

KASPERSKY LAB

Kaspersky Anti-Virus[®] 5.5
for Check Point[™] Firewall-1[®]

Administrator's Guide

KASPERSKY ANTI-VIRUS[®] 5.5 FOR CHECK POINT[™]
FIREWALL-1[®]

Administrator's Guide

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

Revision date: November, 2006

Table of Contents

CHAPTER 1. INTRODUCTION	6
1.1. Computer viruses and malicious software.....	6
1.2. Purpose, main functions and structure of Kaspersky Anti-Virus.....	8
1.3. What's new in version 5.5?	10
1.4. Software and hardware requirements	11
1.5. Distribution kit	12
1.5.1. License Agreement.....	13
1.6. Services provided for registered users	13
1.7. Formatting conventions.....	13
CHAPTER 2. OPERATION OF KASPERSKY ANTI-VIRUS.....	15
2.1. Deploying the application	15
2.2. Deployment of anti-virus protection	15
2.3. Anti-virus protection system maintenance.....	17
CHAPTER 3. INSTALLING AND REMOVING THE APPLICATION	18
3.1. Installing the application	18
3.1.1. First-time installation	19
3.1.2. Reinstalling the application.....	22
3.2. Removing the application.....	22
CHAPTER 4. INTEGRATION OF KASPERSKY ANTI-VIRUS WITH CHECK POINT™ FIREWALL-1®	23
4.1. Registering Security Server with Check Point™ Firewall-1®	23
4.2. Obtaining a Security Server certificate.....	32
CHAPTER 5. STARTING USING THE APPLICATION.....	34
5.1. Starting the application	34
5.2. Application interface	34
5.2.1. Main application window	34
5.2.2. Shortcut menu	36
5.3. Creating the list of monitored servers	37
5.4. Connecting the Management Console to the server	38
5.5. Connecting the Security Server to Check Point™ Firewall-1®	39
5.6. Minimum required settings.....	46

5.7. Protection without additional configuration	47
5.8. Verifying the application performance	48
5.8.1. Test “virus” EICAR and its modifications	48
5.8.2. Testing the HTTP traffic protection	49
5.8.3. Testing the SMTP traffic protection.....	49
5.8.4. Testing the FTP traffic protection	50
CHAPTER 6. UPDATING THE ANTI-VIRUS DATABASE.....	51
6.1. Downloading updates from the internet.....	54
6.2. Installing updates from a network folder	55
6.3. Automatic updates.....	56
6.4. Updating the anti-virus database in the manual mode.....	57
CHAPTER 7. ANTI-VIRUS PROTECTION	58
7.1. Anti-virus objects processing	60
7.1.1. Actions performed with objects transferred via HTTP protocol.....	61
7.1.2. Actions performed with objects transferred via FTP protocol	62
7.1.3. Actions performed with objects transferred via SMTP protocol	62
7.2. Anti-Virus protection level.....	63
7.3. Enabling and disabling the anti-virus protection. Selecting the anti-virus protection level	63
7.4. Scanning HTTP traffic	65
7.5. Scanning FTP traffic.....	70
7.6. Scanning SMTP traffic.....	73
7.7. Anti-virus scan efficiency.....	75
CHAPTER 8. BACKUP STORAGE	79
8.1. Viewing the backup storage.....	80
8.2. Backup storage filter	81
8.3. Restoring objects from the backup storage.....	84
8.4. Deleting objects from the backup storage	86
8.5. Configuring the backup storage settings	87
CHAPTER 9. REPORTS.....	89
9.1. Creating reports	91
9.2. Creating the report template	92
9.3. Viewing reports.....	95
CHAPTER 10. APPLICATION EVENT LOG.....	98

10.1. Configuring the diagnostics level	99
10.2. Configuring log files settings	101
CHAPTER 11. LICENSE KEYS	102
11.1. License information	104
11.2. License key details	105
11.3. License-related notifications.....	107
11.4. Installing the license key	107
11.5. Removing a license key	108
CHAPTER 12. NOTIFICATIONS	110
CHAPTER 13. FREQUENTLY ASKED QUESTIONS.....	114
A.1.1.1. NOTIFICATION SETTINGS	118
A.1.1.2. GLOSSARY	122
A.1.1.3. KASPERSKY LAB.....	126
A.2. Other Kaspersky Lab Products	127
A.3. Contact Us.....	134
A.3.1.1. LICENSE AGREEMENT.....	136

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 books 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.

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

1.1. Computer viruses and malicious software

The constant growth in the number of computer users and new possibilities of data exchange between them via e-mail or internet result in the increased threat of virus infections and data corruption or theft by malicious computer programs.

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

- **Worms** – malicious programs that belong to this category use network resources for distribution. These programs were called "worms" due to their ability to tunnel from one computer to another, using networks, email and other channels. Due to this ability, worms can proliferate extremely fast.

Worms penetrate a computer, determine IP addresses of other computers, and send copies of themselves to these computers. Apart from the network addresses, worms often use data contained in the address books of e-mail client applications installed on the infected machine. Sometimes worms create work files on disks, but they also can function without utilizing any resources of the infected computer except RAM.

- **Viruses** –programs that infect other programs by adding their code to the infected program's code in order to gain control when infected files are run. This simple definition helps determine that the major action a virus performs is *infecting* computer programs. Viruses spread somewhat slower than worms.
- **Trojan horses** – perform unauthorized actions on infected computers, for instance, depending on the particular conditions, they can erase information on hard drives, "freeze" the system, steal confidential information, etc. In the strict sense, Trojan Horses are not viruses as they do not infect programs or data, and are unable to sneak independently into computers and are distributed by malicious users as some "useful" software. However, Trojans may inflict far greater damages compared to a regular virus attack.

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

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

- **Adware** - code that, without the user's knowledge, is included into a program's code in order to display advertising messages. As a rule, adware is integrated into freeware programs. The advertising component is located in the interface. Adware programs are often used to gather users' personal information and send it to the developer, change browser's settings (browser's home page, search page, security levels, etc.) and create traffic that is not controlled by the user. All this may lead to the infringement of the security policies and further to direct financial losses.
- **Riskware** - programs that are not supposed to perform any malicious functions, but contain security breaches and errors and therefore can be used by intruders as auxiliary components of malicious programs. This type of software includes, for example remote administration programs, IRC client programs, FTP programs and various utilities used for ending or hiding running processes.
- **Spyware** - software used to obtain unauthorized access to user's data, for tracking actions performed on this computer or gathering information about the contents of the hard drive. Such programs help the intruder not only gather information, but also gain control over the user's computer. Spyware programs are often distributed along with freeware and installed on the user's computer without the user's knowledge. This type of software includes keyboard spies, password hacking programs and software used for gathering confidential information (for example credit card numbers).

- **Automatic dialers** (Pornware) - programs that establish modem connection with various pay-per-visit internet (as a rule, pornographic) websites.
- **Hacking tools** - tools used by hackers to obtain access to the user's computer. This type of software includes various illegal vulnerability scanners, password hacking programs and other types of software used to hack network resources or to obtain unauthorized access to the system under attack.

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



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

1.2. Purpose, main functions and structure of Kaspersky Anti-Virus

Kaspersky Anti-Virus® for Check Point™ Firewall-1® (hereinafter referred to as **Kaspersky Anti-Virus**) is a system that provides anti-virus monitoring of files transmitted over HTTP, FTP and SMTP protocols via Check Point™ Firewall-1® firewall that ensures high quality protection of corporate networks against malware.

Kaspersky Anti-Virus is controlled using special user interface incorporated into Microsoft Management Console (hereinafter - **MMC**).

The application performs the following functions:

- performs anti-virus scan and processing of data streams transmitted via HTTP and FTP protocols. Depending on the settings, the application will skip or attempt to disinfect a malicious object, block access to it and notify about detection of such objects.
- passes over disinfected files to the client that requested this HTTP or FTP stream.
- scans incoming and outgoing e-mail messages transmitted via SMTP protocol and all attached files for the presence of malicious code in the real-time format. Depending on the settings selected, the application will pass infected messages, delete them or attach to them a warning message.

- creates list of objects that will not be scanned for viruses.
- saves backup copies of objects to a special storage before disinfecting, deleting or blocking the object for the consequent restoring which prevents the loss of data. Configurable filters allow to easily locate the original copies of objects.
- notifies user requesting an object that contains malicious code.
- notifies about the results of the anti-virus object scan, anti-virus database updates, report creation, forthcoming expiration of the license and change of the application status by launching external programs including scripts written by the administrator. This feature allows the administrator to setup notifications about the above events in a most convenient way.
- updates the anti-virus database from internet or from the local folder either in the manual or automatic mode. Internet updates can be performed from the Kaspersky Lab's FTP and HTTP internet servers.



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

As new viruses are created daily, it is extremely important that you maintain your anti-virus database up-to-date.

The anti-virus database at the Kaspersky Lab's servers is updated on an **hourly** basis. We recommend that you update your anti-virus database with the same frequency (see Chapter 6, page 51).

- Maintains events log and creates reports about the results of the anti-virus scan on a regular basis. The application allows creating reports using built-in templates at the required time interval.
- Allows 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.).
- Manages license keys

Kaspersky Anti-Virus 5.5 for Check Point™ Firewall-1® includes the following components:

- **Security server** that provides the anti-virus functionality and updating of the anti-virus database and includes administrative services for remote management, configuring and ensuring the integrity of the application and of the data stored.
- **Management Console** that provides the user interface for managing the administrative services of the application and allows installing the application, configuring settings and managing the server component. The man-

agement module is implemented as the extension of the Microsoft Management Console (MMC).

1.3. What's new in version 5.5?

Kaspersky Anti-Virus 5.5 for Check Point™ Firewall-1® has the following distinctions from the previous version:

- Completely revised intuitive graphical interface implemented according to the Microsoft Management Console standards. Using the new interface, the administrator can start using the application without the need to configure any preliminary settings. Additionally, this interface offers a wide range of options for configuring the customized application management environment that can be adapted to the conditions of any particular corporate network to the maximum possible extent.
- The use of extended set of the anti-virus database for scanning objects helps protect traffic not only against malware, but also against potentially dangerous programs (riskware), such as spyware, adware, automatic dialing programs, hacking software and joke programs.
- The possibility to select anti-virus protection levels has been implemented which enables the administrator to adjust the security level of the stream passing through the firewall and the Anti-Virus load during the scan.
- Configurable filters allow to easily locate the original copies of objects for example for their subsequent restoration.
- A new feature has been added that allows user to scale the application based on the number of processors installed on the computer on which the application is residing. In order to enhance the efficiency of the application (increasing the number of objects that can be analyzed at the same time) several instances of the anti-virus kernel can be launched and run simultaneously.
- The possibility to control the size of the queue of the objects to be scanned allows a more precise control of the Anti-Virus load depending on the amount of data being scanned.
- A possibility to scan objects in RAM without using the disk subsystem has been added, which considerably increases the efficiency of the application.
- Due to the support of AMON and ELA protocols a deeper level of Kaspersky Anti-Virus integration with Check Point™ Firewall-1® has been achieved, which allows transferring information about Kaspersky Anti-Virus operation and viewing it using standard Check Point™ Firewall-1® tools.
- The logging capability has been drastically improved. The application now allows logging registered events into the Microsoft Windows application

log and in the application's logs. An ability to configure the degree of information completeness and the extent of detail has been added. Logs can be viewed using the Microsoft Windows **Events Viewer** tool and standard text editors, such as **Notepad**.

- An ability to create regular extended reports about the anti-virus scan results. Reports can be created either in the automatic mode or by the administrator's request. The reports maintaining system ensures fast, convenient and consistent method of accessing information using standard tools, such as for example, Microsoft Internet Explorer.
- Controlling the application from the command line is not supported.

1.4. Software and hardware requirements

Kaspersky Anti-Virus is used with Check Point™ Firewall-1® (versions NG, NG AI and NGX).

For the installation and operation of the application components the software and hardware of your computer must comply with the following minimum requirements:

Management server:

- Hardware requirements:
 - processor Intel Pentium 300 MHz or higher;
 - about 512 MB free RAM;
 - about 20 MB of free disk space for the application installation (not counting the size of the backup storage and other service folders);
 - at least 1 GB of free disk space for temporary storage of data copied from the internet before the anti-virus scan and for the backup files storage.
- Software requirements:
 - Microsoft Windows 2000 Professional with Service Pack 4 or higher installed;
 - Microsoft Windows XP Professional Edition with Service Pack 2 or higher installed;
 - Microsoft Windows 2000 Server with Service Pack 4 or higher installed;
 - Microsoft Windows 2000 Advanced Server with Service Pack 4 or higher installed;
 - Microsoft Windows Server 2003 Standard Edition or higher;

- Microsoft Windows Server 2003 Enterprise Edition or higher.

Management console:

- Hardware requirements:
 - processor Intel Pentium II 300 MHz or higher;
 - 256 MB RAM;
 - 10 MB free disk space.
- Software requirements:
 - Microsoft Windows 2000 Professional with Service Pack 4 or higher installed;
 - Microsoft Windows XP Professional Edition with Service Pack 2 or higher installed;
 - Microsoft Windows 2000 Server with Service Pack 4 or higher installed;
 - Microsoft Windows 2000 Advanced Server with Service Pack 4 or higher installed;
 - Microsoft Windows Server 2003 Standard Edition or higher;
 - Microsoft Windows Server 2003 Enterprise Edition or higher.

1.5. Distribution kit

You can purchase Kaspersky Anti-Virus either from our dealers (retail box) or online (for example, visit <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 on the installation CD or on a special diskette;
- License Agreement



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

If you buy Kaspersky Anti-Virus online, you will have to 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.

1.5.1. License Agreement

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



Read the License Agreement carefully!

If you do not agree with the terms of the license agreement, you can return Kaspersky Anti-Virus to your dealer for a full refund. In this case, the envelope with the installation CD must remain sealed.

By opening the sealed 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 use Kaspersky Anti-Virus more efficiently .

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






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



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

1.7. Formatting conventions

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

Format feature	Meaning/Usage
Bold font	Titles of menus, menu items, windows, dialog boxes and their elements, etc.
 Note	Additional information, notes
 Attention!	Information requiring special attention
 <i>In order to perform,</i> Step 1. ...	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
 Solution	Implementation of the task
[key] – modifier name.	Command line modifier
Information messages and command line text	Text of configuration files, information messages and command line

CHAPTER 2. OPERATION OF KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus 5.5 for Check Point™ Firewall-1® acts as a filter: processes data, transferred over HTTP, FTP and SMTP protocols, identifies monitored objects, analyzes them for the presence of malicious code and blocks attempts of infected files and web documents to penetrate the local network.

2.1. Deploying the application

The structure of Kaspersky Anti-Virus 5.5 for Check Point™ Firewall-1® includes two components. The anti-virus functionality is performed by the server component, called the Security Server. The user interface is provided by the Management Console.

The process of Kaspersky Anti-Virus deployment is identical for the local and the distributed Check Point™ Firewall-1® configuration.

The Security Server component is a CVP server. It is integrated into the Check Point™ Firewall-1® application in accordance with OPSEC™ standards and by default supports protected data transfer protocol.

The Security Server can be installed either on one computer with Check Point™ Firewall-1® or on any other computer connected via a TCP/IP protocol with the computer where Check Point™ Firewall-1® is installed.

The Security Server installation option depends on the operating system installed on the computer with Check Point™ Firewall-1®, on whether this computer system complies with the server component installation requirements or on the traffic transferred via Check Point™ Firewall-1®.

It should be noted that when processing a large amount of data traffic, Kaspersky Anti-Virus may somewhat slow down the computer and this may affect the throughput of Check Point™ Firewall-1®. Therefore we recommend installing the Security Server on a dedicated computer for networks with large amount of traffic.

2.2. Deployment of anti-virus protection



In order to create anti-virus protection system using Kaspersky Anti-Virus 5.5 for Check Point™ Firewall-1®:

1. Install the Security Server component on the computer that has a TCP/IP connection to the computer where the Check Point™ Firewall-1® application is installed. The installation is performed from the installation CD.

If there are several Check Point™ Firewall-1® servers installed in the network, each server shall have its own Security Server component installed.

It is also possible to install several Security Server components to scan data received from a single Check Point™ Firewall-1® application. In this case, data distribution between the anti-virus servers will be performed by the firewall. The anti-virus scan results for each Security Server, namely,

- backup storage content;
- information included into the reports;
- the group of events registered in the Windows logs and in the application's logs;

will be provided only for objects forwarded to this Security Server by Check Point™ Firewall-1®.



The number of instances of Kaspersky Anti-Virus installed in the network will be determined by the number of installed Security Servers.

2. Perform integration of Kaspersky Anti-Virus and Check Point™ Firewall-1® (see Chapter 4, page 23) for each of the installed Security Servers.
3. Install the Management Console on the computer that has a TCP/IP network connection with the computer on which the Security Server is installed. The Management Console provides a centralized access to all network resources from a single administrator's workstation; therefore, it is sufficient to install this component on one computer only. However, if several administrators are working together, the Management Console can be installed on each administrator's computer.
4. Create the list of monitored servers (see section 5.3, page 37).
5. Connect the Management Console to the servers (see section 5.4, page 38).
6. Configure settings for connecting to Check Point™ Firewall-1® (see section 5.5, page 39) for each server.
7. Configure the anti-virus protection system for each server:

- Fine-tune the anti-virus database update settings (see Chapter 6, page 51).
- Verify the correctness of the settings and of the Anti-Virus operation using a test "virus" **EICAR** (see section 5.8, page 48).
- Configure the event logs and reports settings (see Chapter 10, page 98 and Chapter 9, page 89).
- Configure notifications about the results of anti-virus object scan, anti-virus database updates, report creation, forthcoming expiration of the license, change of the application status (see Chapter 12 on page 110).

2.3. Anti-virus protection system maintenance

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

- updating the anti-virus database on a regular basis;
- reviewing the application work logs and anti-virus scan result reports.

CHAPTER 3. INSTALLING AND REMOVING THE APPLICATION

Before the installation of Kaspersky Anti-Virus, make sure that the software and hardware of the computers used meet the installation requirements. The minimum allowable configuration is described in section 1.4, page 2.



For installation of Kaspersky Anti-Virus 5.5 for Check Point™ Firewall-1® the local administrator's rights are required for the computer on which the installation is performed.



Updating from previous versions of Kaspersky Anti-Virus for Check Point™ Firewall to version 5.5 is not available.

3.1. Installing the application

The setup wizard will offer you to install the application components of Kaspersky Anti-Virus 5.5 for Check Point™ Firewall-1®, Security Server and Management Console, on the computer on which the setup wizard is run. You can select either complete or custom installation of the application or repair an invalid installation of Kaspersky Anti-Virus.

After the Management Console is installed, Kaspersky Anti-Virus group and a shortcut icon to run it will appear in the **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 Anti-Virus 5.5 for Check Point™ Firewall-1®**;
- launch – **automatic**;
- profile - **Local system**.

You can review the properties of the **Security Server** and monitor its operation using standard Microsoft Windows administration tool - **Computer Management/Services**. Information about the operation of the **Security Server** is registered and saved in the Windows application log on the computer on which the Security Server is installed and in the Kaspersky Anti-Virus application logs.

3.1.1. First-time installation

In order to install Kaspersky Anti-Virus, run the executable file from the installation CD. The installation process will be facilitated by the setup wizard. Setup wizard will offer you to configure the installation settings and start the installation. Following below is a detailed discussion of each step of the application installation.



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

Step 1. Verifying the version of the installed operating system

Before the installation begins, the setup wizard will verify whether your computer complies with the minimum hardware and software requirements. If these requirements are not met, the installation will not be performed.

If your system does not comply with the software requirements, update your operating system to the required version, install all required Service Packs and start the installation of Kaspersky Anti-Virus one more time.

Step 2. Greeting and License Agreement

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

Step 3. Selecting the type of the installation

During this step, select the installation type: complete or custom.

In order to install on your computer both the Security Server and the Management Console, select the Complete option. The application will be installed into the default folder (Program files\Kaspersky Lab\Kaspersky Anti-Virus for Check Point™ Firewall).

If you wish to install only one component of the application or to change the default installation folder, use the custom type of the installation. In this case, you will be offered to select the required component and specify path to the installation folder.

Step 4. Selecting application components to be installed

If you selected the custom installation option, specify application components to be installed on your computer. You can also change the default folder into which they will be installed.

You can select either both components or only the Administration console to be installed. The Security server will not be installed without the Console.

By default, you will be offered to install both components (the Security Server and the Management Console) into the Program files\Kaspersky Lab\Kaspersky Anti-Virus for Check Point™ Firewall folder. If this folder does not exist, it will be created automatically. You can change the installation folder using the Browse button.



If your system does not comply with the minimum hardware or software requirements for the installation of the Security Server, you will be offered to install only the Management Console.

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

Step 5. Selecting the data folder

During the installation of the Security Server, the setup wizard will create service folders and databases required for the application to work. These folders and databases include:

- temporary files and backup storage folders;
- folder to store the anti-virus database used by the application;
- reports storage folder;
- logs storage folders;
- backup storage database;
- report statistics database.



The data folder must be excluded from the scan scope of any anti-virus applications installed on your computer.

Specify the folder to store the service data. By default you will be offered to create folder **Program files\Kaspersky Lab\Kaspersky Anti-Virus for Check Point™ Firewall\DataFolder**. You can change the path to the folder using the **Browse** button.

After the application is installed, you will be able to change the path to the data folder using the Kaspersky Anti-Virus Management Console, in the anti-virus protection settings window (the **General** tab of the **Anti-Virus protection** window). The new value will apply at the Security Server restart.

Note that databases used by the application are created only once, during the installation of the Security Server.



If you decide change the application data folder, then in order to ensure the correct data transfer into the new folder, the entire content of the old folder shall be copied, including the subfolders structure and the names of the subfolders shall remain intact.

If the integrity of the data folder structure has been affected, the Security Server will not run and, consequently, Kaspersky Anti-Virus will not work.

Step 6. Launching the installation

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

Step 7. Installing license key

During the installation of the Security Server, you will be offered to install the license key for Kaspersky Anti-Virus 5.5 for Check Point™ Firewall-1®.

You can also install the license key later using the Management Console, however, note that without the license key the anti-virus functionality of the application will not be available and you will only be able to launch the Management Console.

During this step, Kaspersky Anti-Virus 5.5 for Check Point™ Firewall-1® license key will be installed. The license key is your personal "key" that contains all service information required for the full-featured functionality of the application and additional reference information, namely:

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

Install the current license key in the window that will open. In order to do this, press the **add** button in the corresponding section. Specify the license key file (*.key) to be installed using the standard Windows Select file dialog box. As a result, the selected license key will be installed as the current license key for Kaspersky Anti-Virus.



You can use your license key used with the previous application version - Kaspersky Anti-Virus 4.0 as the license key for Kaspersky Anti-Virus 5.5 for Check Point™ Firewall-1® if it is still valid.

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

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

Step 8. Completing the installation

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

3.1.2. Reinstalling the application

You have to reinstall Kaspersky Anti-Virus if the first-time installation appeared to be incorrect or if the executable files were corrupted during the operation.



*In order to reinstall the application select the **Repair** option in the window that will open.*

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

3.2. Removing the application

You can remove Kaspersky Anti-Virus for Check Point™ Firewall-1® from your computer using standard Windows Add/Remove Programs tool or the application distribution kit. This will remove all installed Kaspersky Anti-Virus components, namely the Security Server and the Management Console, from your computer.



In order to remove Kaspersky Anti-Virus for Check Point™ Firewall-1® using the distribution kit:

run the executable file from the installation CD and select the **Remove** option in the window that will open.

CHAPTER 4. INTEGRATION OF KASPERSKY ANTI-VIRUS WITH CHECK POINT™ FIREWALL-1®

The process of integration of Kaspersky Anti-Virus with Check Point™ Firewall-1® is a standard procedure for OPSEC™ applications and involves two steps:

1. Registration of the Security Server with Check Point™ Firewall-1® as an OPSEC™ application.
2. Obtaining the Security Server certificate.

After Kaspersky Anti-Virus is integrated with Check Point™ Firewall-1®, connect the Security Server to Check Point™ Firewall (see section 5.5, page 39).



If traffic passing through the firewall is sent to several servers, each server must be integrated with Security Check Point™ Firewall-1®.

4.1. Registering Security Server with Check Point™ Firewall-1®

Registering OPSEC™ applications is described in detail in the Check Point™ Guides. Provided below is the procedure of configuring the settings that are specific to Kaspersky Anti-Virus. The configuration process must be performed from the Check Point™ Firewall-1® management console (**Check Point™ SmartDashboard™**).



In order to register the Security Server with Check Point™ Firewall-1® as an OPSEC™ application:

1. Create a new network object (**Network Objects/New Nodes/Host**) for the computer on which the Security Server is installed. Specify the network name and the IP address of this computer in the window that will open (see Figure 1)

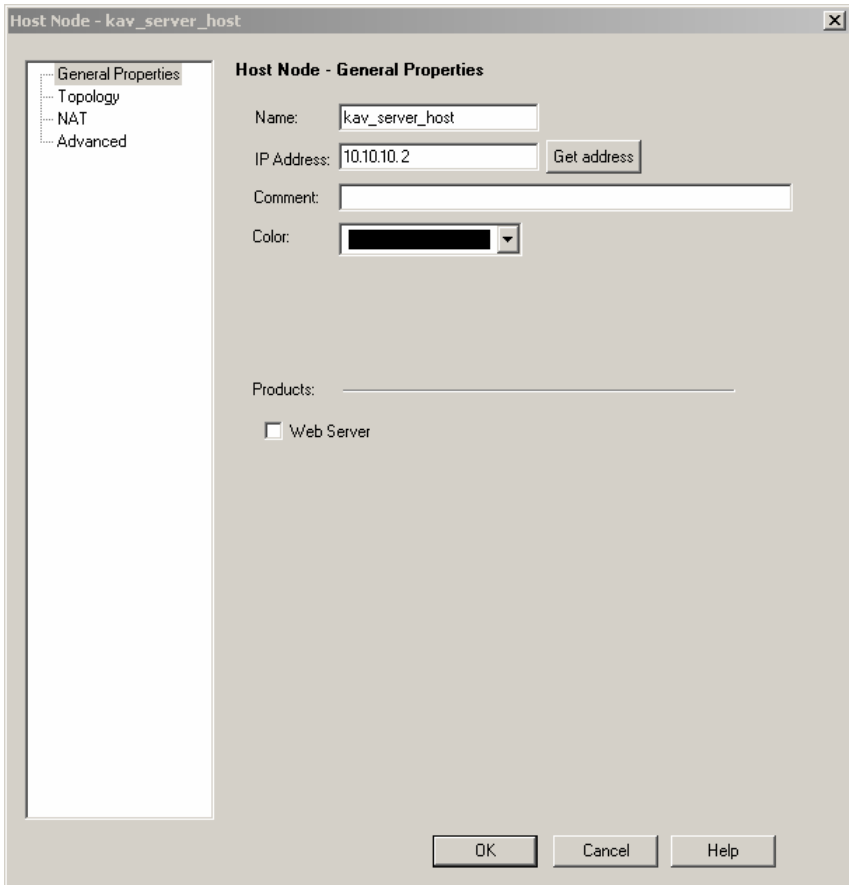


Figure 1. Creating a **Security Server** network object

2. When creating a new object, that is an OPSEC™ application (OPSEC™ Application/New) in the General tab of the OPSEC™ Application Properties settings configuration window (see Figure 2), perform the following:
 - Using the **Name** entry field, enter the name of the OPSEC™ application that will be used for addressing to the Security Server of the Check Point™ Firewall-1® services.
 - Select the Security Server network object created earlier from **Host** the drop-down list;

- In the **Server Entities** and **Client Entities** sections, select CVP, AMON and ELA as protocols supported by the application.



Configuring the protocols settings is not required. Kaspersky Anti-Virus uses the default Check Point™ Firewall-1® settings.

If the configuration of Check Point™ Firewall-1® interaction with OPSEC™ applications is different from the standard configuration, setup the settings as required.

The screenshot shows the 'OPSEC Application Properties - kav_server' dialog box. It has three tabs: 'General', 'CVP Options', and 'AMON Options'. The 'General' tab is active. The 'Name' field contains 'kav_server'. The 'Comment' field is empty. The 'Color' field is set to black. The 'Host' field contains 'kav_server_host' and has a 'New...' button next to it. Below these fields is the 'Application properties' section, which includes 'Vendor' (set to 'User defined'), 'Product', and 'Version' dropdown menus. An 'Activate...' button is located below the application properties. The 'Server Entities' section has a list with checkboxes for 'CVP' (checked), 'UFP' (unchecked), and 'AMON' (checked). The 'Client Entities' section has a list with checkboxes for 'ELA' (checked), 'LEA' (unchecked), 'SAM' (unchecked), 'CPMI' (unchecked), 'DMI' (unchecked), and 'UAA' (unchecked). The 'Description' field contains 'Event Logging API'. The 'Secure Internal Communication' section has a 'Communication...' button and a 'DN:' field. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Figure 2. Creating an OPSEC™ application

3. Setup a secure connection of the Security Server to Check Point™ Firewall-1® (Secure Internal Communications). The following will be created as the result:
 - key to obtain a Security Server certificate;
 - a Security Server certificate;
 - a Security Server SIC name (OPSEC™ application's SIC name).



The Security Server SIC name will be displayed in the OPSEC™ **Application Properties** window, in the **DN** field (section **Secure Internal Communication**).

4. Describe protocols that will be subject to the anti-virus scan.

Kaspersky Anti-Virus scans the data passing through the firewall via HTTP, FTP and SMTP protocols. Create the following:

- a URI resource for transferring the HTTP protocol data for scanning;
- an FTP resource for transferring the FTP protocol data for scanning;
- an SMTP resource for transferring the SMTP protocol data for scanning;

When describing the resources, specify the following parameters in order to enable Check Point™ to transfer data to the Anti-Virus to perform the scan:

- to create URI, FTP and SMTP resources check the **Use CVP (Content Vectoring Protocol)** box on the **CVP** tab (see Figure 3) and select the name of the OPSEC™ application corresponding to the Security Server in the **CVP server** field;

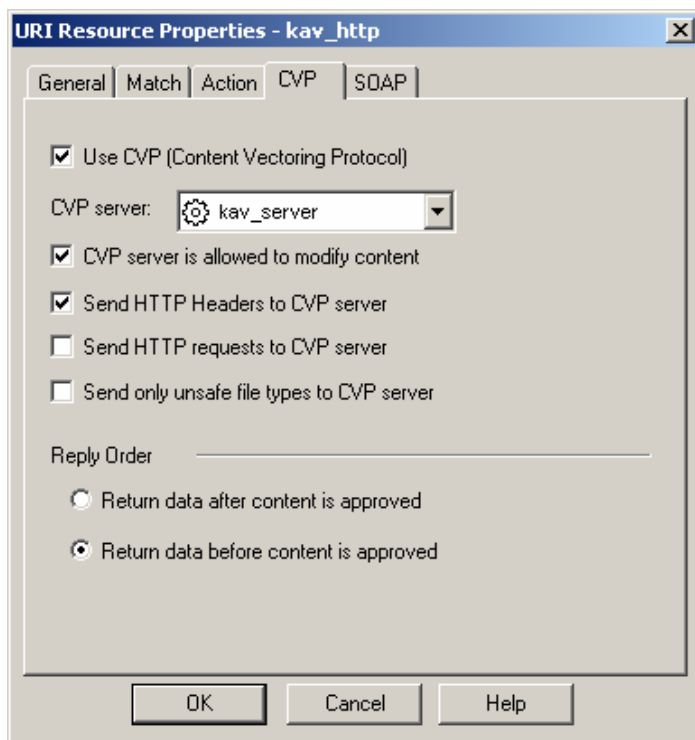


Figure 3. Creating a URI-resource.
The **CVP** tab

- to create an FTP resource check the **GET** and the **PUT** boxes in the **Methods** section on the **Match** tab (see Figure 4);

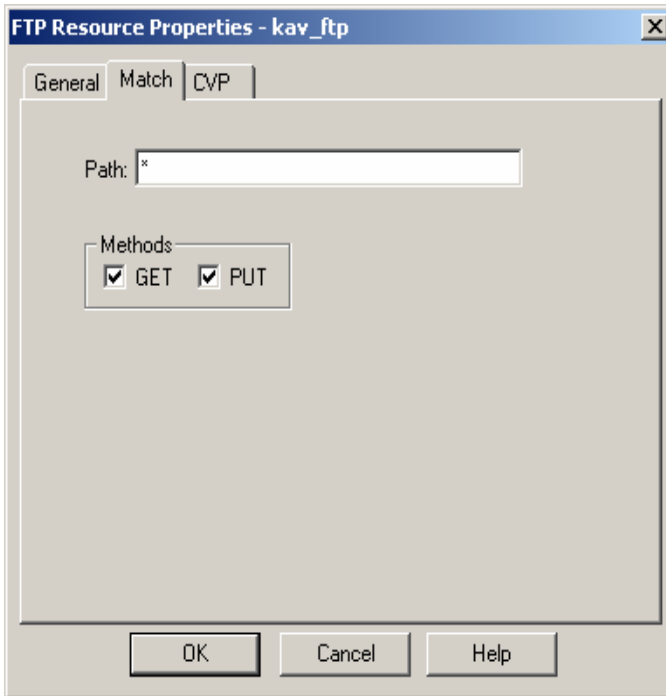


Figure 4. Creating an FTP resource.
The **Match** tab

- to create a URI resource, select the **Enforce URI capabilities** option in the **Use this resource to** section on the **General** tab (see Figure 5).

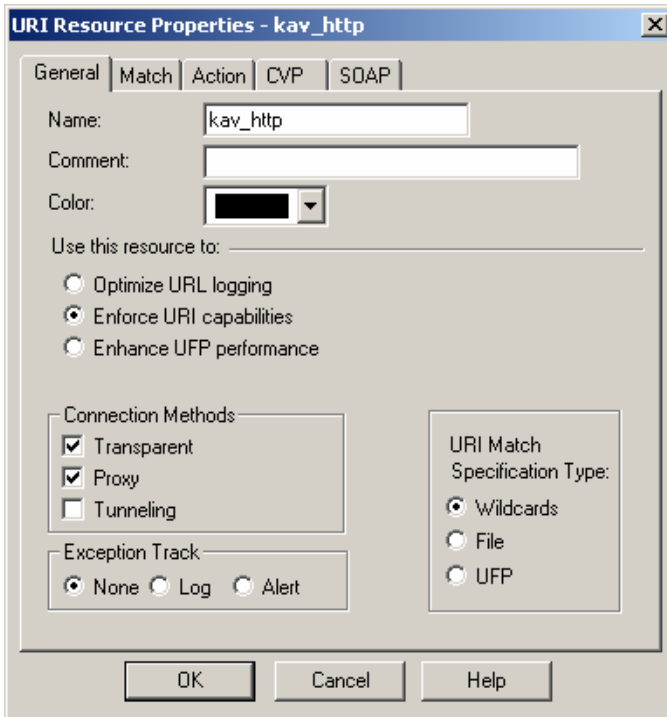


Figure 5. Creating a URI resource.
The **General** tab

In order to increase the efficiency of the anti-virus scan, specify the following settings values on the **CVP** tab (see Figure 3):

- Check the **CVP server is allowed to modify content** box for URI-, SMTP- and FTP-resources.

This parameter controls the possibility of disinfection and replacement of objects detected during the anti-virus scan (see section 7.1, page 60).



If the box is not checked, disinfection (as well as replacement for HTTP and SMTP objects) will not be performed. Such objects will be identified as infected and blocked by Check Point™ Firewall-1®.

- Check the **Send HTTP Headers to CVP server** box for the URI resource and the **Send SMTP Headers to CVP server** box - for the SMTP resource.

- Select the **Return data before content is approved** option in the **Reply Order** section for URI, SMTP and FTP resource.

This parameter determines the possibility of early data transfer to the user before this data is scanned (see section 7.4, page 65).



If this option is not selected for the URI and FTP resources, then early data transfer will not be performed during the scan of objects transferred over HTTP and FTP protocols.



Please take into account the following restrictions when creating a SMTP resource:

- the size of messages redirected by Check Point™ Firewall-1® for the anti-virus scan displayed in the **Do not send mail larger than** field on the **Action2** tab (see Figure 6);
- the size of messages passing through Check Point™ Firewall-1® (**Network Objects/ Check Point™ /Advanced/SMTP**) displayed in the **Don't accept mail larger than** field (see Figure 7).

The specified values must match the traffic parameters. Messages with the size exceeding the restrictions will not be processed by Check Point™ Firewall-1® and, therefore, will not be submitted to the anti-virus scan and will not be delivered to the user.

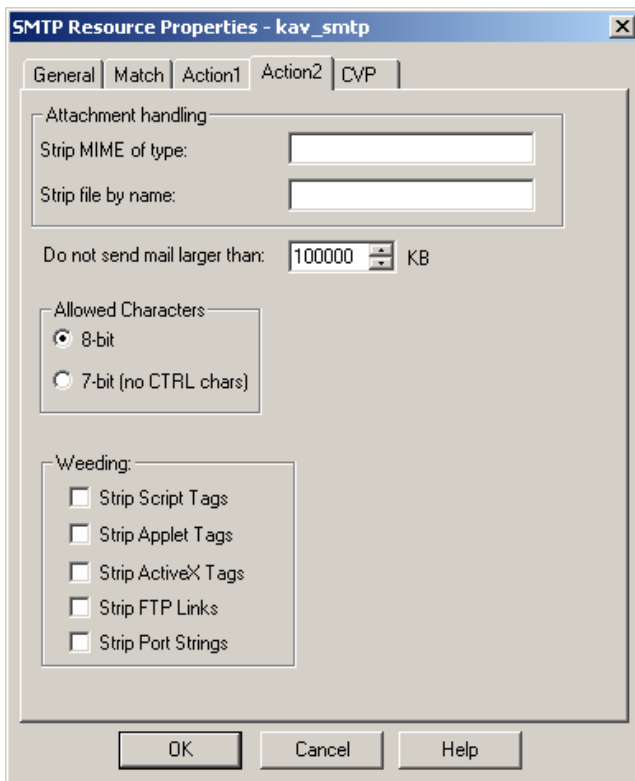


Figure 6. Configuring the SMTP resource settings.
The **Action2** tab

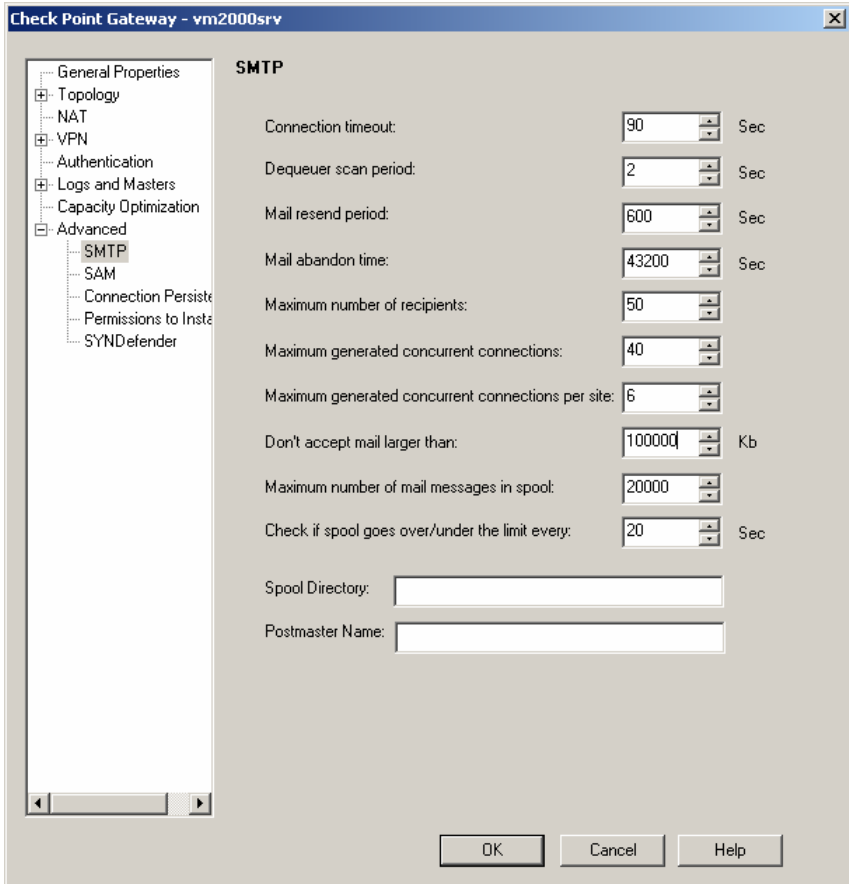


Figure 7. Configuring the settings of Check Point™ Firewall-1®.
Restricting the message size

4.2. Obtaining a Security Server certificate

Obtaining the certificate is a standard procedure for applications integrated with Check Point™ Firewall-1®. This procedure is performed using special utility ***opsec_pull_cert.exe*** designed for obtaining certificates and included into the Kaspersky Anti-Virus distribution kit. After installation of the Security server this utility will be located in the component installation folder, subfolder **OpsecTools**.

The settings will be assigned values set during the registration of the Security Server with Check Point™ Firewall-1® (see section 4.1, page 23).



In order to obtain the Security Server certificate:

run executable file **opsec_pull_cert.exe** included into the Kaspersky Anti-Virus distribution kit on the computer on which the Security Server is installed using the command line with the following keys:

```
opsec_pull_cert.exe -h <IP address> -n <OPSEC™ application name> -p <modifier> -o <path to the certificate file >
```

where:

<IP address> - IP address of the computer on which Check Point™ Firewall-1® is installed;

< OPSEC™ application name> - the name of the OPSEC™ application, assigned for the Security Server during the registration with Check Point™ Firewall-1®;

<modifier> - the modifier used for obtaining the Security Server certificate specified when the settings for secure connection to Check Point™ Firewall-1® were configured;

<path to the certificate file> - full path to the file where the Security Server certificate received from Check Point™ Firewall-1® will be saved. This file must be saved in a local folder on the computer on which the Security Server is installed. According to the default Anti-Virus settings the certificate file will be stored as file **opsec.p12** in the application data folder in service folder **OpsecDir**. We recommend using this value for this setting.



If setting **-o <path to the certificate file>** is not used, the certificate file will be saved as **opsec.p12** in the folder from which **opsec_pull_cert.exe** utility was run.

We recommend to move the certificate file to the application data folder in **service** folder **OpsecDir** as this will allow to avoid additional configuration when connecting the Security server to Check Point™ Firewall-1® (see section 5.5 on page 39).

After the action performed by this utility is completed successfully, the full path to the certificate file and the SIC name of the Security Server will be displayed on the screen.

CHAPTER 5. STARTING USING THE APPLICATION

5.1. Starting the application

The server part of the application, the Security Server, is launched automatically at the startup of the operating system on the computer on which the Security System is installed. If the settings used for the interaction of the Security Server with Check Point™ Firewall-1® have been configured (see section 5.5, page 39) and the anti-virus protection has been enabled (see section 7.1, page 60), it will start functioning immediately after the server component is started.

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



In order to start the Management Console:

select the **Management Console** item in the programs group **Kaspersky Anti-Virus 5.5 for Check Point™ Firewall** from the standard **Start / Programs** Windows menu. This programs group is created only on the administrator's workstations when the Management Console is installed.

5.2. Application interface

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

5.2.1. Main application window

The main application window (see Figure 8) contains a menu, a toolbar, a view pane and a results pane. The menu provides the window management functions as well as the access to the help system. The set of buttons on the toolbar ensures the direct access to some frequently accessed items of the main menu. The display pane presents the **Kaspersky Anti-Virus 5.5 for Check Point™ Firewall-1®** namespace in the form of the console tree, the results pane displays the list of elements of the object selected in the tree.

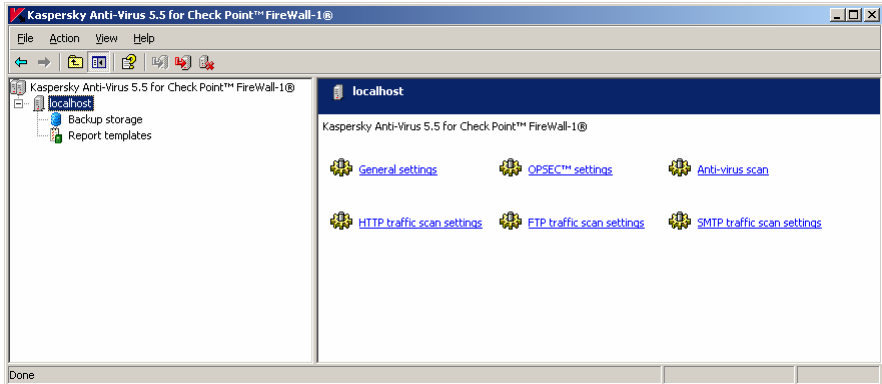


Figure 8. Main application window

The Kaspersky Anti-Virus 5.5 for Check Point™ Firewall-1® namespace contains the list of monitored servers (that is, computers that are monitored by Kaspersky Anti-Virus via this console) in the form of nodes.

Immediately after the installation of the Management Console the namespace does not contain any elements.

After being added to the console tree, the monitored server will be displayed as a node with name <Computer Name>. The settings configuration and controlling Kaspersky Anti-Virus application is performed using hyperlinks in the results pane.

- [General settings](#) – used for viewing general settings of Kaspersky Anti-Virus operation, license details and information about installed license keys, renewing the license and the configuring the application operation diagnostics settings and notification settings.
- [OPSEC™ settings](#) – used for viewing and configuring Check Point™ Firewall-1® interaction settings.
- [Anti-virus scan](#)– used to control the anti-virus protection, configure the reception settings, anti-virus database updates settings, manually update the database, create automatic the updating schedule, configure the efficiency of the Kaspersky Anti-Virus operation.
- [HTTP traffic scan settings](#)– used to configure the HTTP traffic scan settings.
- [FTP traffic scan settings](#)– used to configure the FTP traffic scan settings.
- [SMTP traffic scan settings](#)– used to configure the SMTP traffic scan settings.

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

- **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 working with reports; contains templates used to create the anti-virus scan reports.

5.2.2. Shortcut menu

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

Object	Command	Purpose
Kaspersky Anti-Virus 5.5 for Check Point™ Firewall-1®	Add a server	Add to the console tree a computer where Kaspersky Anti-Virus will be controlled using the console.
<Computer name>	Disconnect from the server	Disconnect the computer with the Security Server installed from the Management Console.
	Connect to the server	Connect the computer with the Security Server installed to the Management Console.
	Remove the server from the console tree	Remove the computer from the list of servers on which Kaspersky Anti-Virus is controlled using the Management Console.
Backup storage	New filter	Create and configure a new filter used to search for objects located in the backup storage.
Report templates	New report template	Create a new report template.

Additional shortcut menu commands are also provided for report templates and for the backup storage:

- using the **Create a report** command you can create a report based on the selected template and save it as a file;
- using the **View report** command you can display the last report created based on the selected template;
- the **Get file** command is used to obtain the original copy of the object that had been saved before this object was processed by the Anti-Virus.

5.3. Creating the list of monitored servers

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



In order to add a new server to the list of monitored servers,

1. Select the Kaspersky Anti-Virus 5.5 for Check Point™ Firewall-1® node in the console tree, open the shortcut menu and select the Add a server command or use the analogous item from the Action menu. This will open an Adding a server window (see Figure 9).
2. Specify a computer with the Security Server component installed. If the server component is installed on the same computer as the Management Console, select Local computer. In order to add one of the computers installed in the network, select Remote computer and specify the name computer's name in the entry field. You can enter the name manually (select IP address, full domain name (FQDN in the following format **<domain name>.<Computer name>**), the computer's name in the MS Windows network (NetBIOS name) or select the computer using the **Browse** button.



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

The connection is established using DCOM protocol.

In order to establish connection between the Management Console and the Security Server when adding the server, check the **Connect now** box (details see section 5.4. page 38).



The Security Server component must be installed on the selected computer in order to ensure connection.

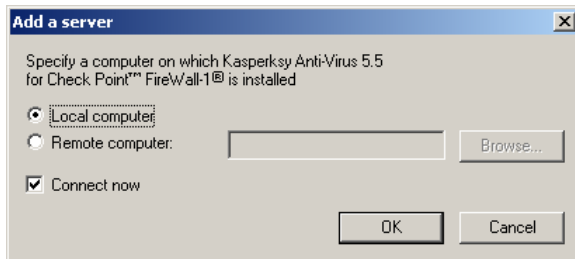




Figure 9. The **Adding a server** dialog box

As a result, the computer that you selected will be displayed as a <Computer name> node in the console tree. The local computer will be displayed as the localhost.

If the connection with the Security Server was successfully established, the  icon will appear next to the monitored and the node structure will include nested folders: Backup Storage and Report Templates. If the connection have not been established or could not be established, the server will be flagged with the  icon. You can connect to such server only manually (details see section 5.4. page 38).



In order to remove a server from the list of monitored 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 server from the console tree** command or use the corresponding item in the **Action** menu.

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

5.4. Connecting the Management Console to the server


In order to be able to configure and manage Kaspersky Anti-Virus 5.5 for Check Point™ Firewall-1® using the console, you have to connect to the Security Server

component installed on the monitored server. The application will then receive information from the server and display it as the console tree.



In order to connect to the Security Server

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

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

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. Select the required option.



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

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

5.5. Connecting the Security Server to Check Point™ Firewall-1®

On order to ensure that Kaspersky Anti-Virus scans data transferred via Check Point™ Firewall-1®, the settings for the interaction between the two applications shall be configured.



If the settings for the interaction between Kaspersky Anti-Virus and Check Point™ Firewall-1® are not configured, the anti-virus traffic scan will not be performed.

The interaction between Check Point™ Firewall-1® and application being integrated with it, is maintained by the Secure Internal Communications (SIC) system. Applications are connected to Check Point™ Firewall-1® using a **secure protocol**. Applications authentication is performed based on the *certificate* and the *SIC name* of the application (OPSEC™ application's SIC name). These settings are configured during the integration of Kaspersky Anti-Virus with Check Point™ Firewall-1® (see section 4.1, page 23).



Connecting applications using a secured protocol is recommended by Check Point™ company.

By default, Kaspersky Anti-Virus uses a secured connection protocol and the default Check Point™ Firewall-1® settings.

The interaction between the applications is provided using three protocols. CVP and AMON protocols are used by the Security Server when it is expecting the incoming connection from Check Point™ Firewall-1® and ELA protocol is used by the Security Server to initiate a connection to Check Point™ Firewall-1®.



CVP and AMON protocols are supported by the Security Server, while ELA protocol support is provided by Check Point™ Firewall-1®.

The interaction settings are configured from the administrator's workstation using the Kaspersky Anti-Virus Management Console.

The configuration process is not affected by the computer on which the Security Server is installed (dedicated computer or the computer with Check Point™ Firewall-1®). The steps you will have to perform in order to configure the settings will be the same:



In order to configure the settings for interaction between the Security Server and Check Point™ Firewall-1®:

1. Select the node corresponding to the required server in the console tree and follow the **OPSEC™ settings** link in the results pane.
2. In the **Connection** tab of the **OPSEC™ settings** window that will open (see Figure 10) specify the values for the settings used for connection via CVP, AMON and ELA protocols.



By default the Secure server is connected to Check Point™ Firewall-1® using a secure connection. In order to configure it you will have to specify values for the settings used for connection using protocols CVP and AMON and the path to the certificate file.

In order to ensure that the Secure server transfers to Check Point™ Firewall-1® information about its operation, for example, events registered in the operation of the Anti-Virus, you will have to configure the settings for data transmission using the ELA protocol.



The default secure connection type for each protocol corresponds to the default settings used by Check Point™ Firewall-1® starting with version NG. We recommend that you change these settings only in case of necessity.

For **CVP** and **AMON** protocols specify the following:

- the port number on the Security Server that will be used to receive requests for connection from Check Point™ Firewall-1®. By default, these are port 18181 for CVP protocol and port 18193 for AMON protocol.
- the type of authentication used for connection. Select the required value from the drop-down list:
 - **none** - non-secure ("clear") connection;
 - **sslca** – a protocol based on cryptographic certificates is used, the data will be encrypted.
 - **sslca clear** – a protocol based on cryptographic certificates is used, the data will not be encrypted.
 - **auth_opsec** – an internal Check Point™ protocol is used, the data will not be encrypted;
 - **ssl_opsec** – a SSL-based protocol is used, the data will be encrypted.
 - **ssl_clear_opsec** – a SSL-based protocol is used, the data will not be encrypted.

If the list does not contain the required value, enter it manually.



If protocols that require keys for encryption are used for authentication, the key files must be located in the application data folder in the OPSEC™ service folder.

- **SIC-Security server name**, specified during the registration of the Security Server with Check Point™ Firewall-1® (see section 4.1 on page 23).



You can view the SIC name of the Security Server using the Check Point™ Firewall-1® Management Console. It will be displayed in the **OPSEC™ Application Properties** window, in the **DN** field (section **Secure Internal Communication**).



If a non-secure connection is used, the **SIC-Security Server name** does not have to be specified.

For **ELA** protocol specify the following:

- the number of the port that will be used by Check Point™ Firewall-1® to receive information from Kaspersky Anti-Virus (by default it is port 18187);
- the type of authentication used for connection (see above);

- **ELA Server:** NetBIOS name or the full domain name (FQDN) or the IP address of the computer, on which Check Point™ Firewall-1® is installed,
- **ELA SIC-Server name.** the internal SIC name of Check Point™ Firewall-1® to which the Security Server will be connected;



You can view the internal Check Point™ Firewall-1® SIC name using the Check Point™ Firewall-1® management console. It is displayed in the settings configuration window of Check Point™ Firewall-1® (**Network Objects/ Check Point™ / GeneralProperties**) in the **DN** field, section **Secure Internal Communication**.

Specify the full path to the Security Server certificate file received from Check Point™ Firewall-1® (see section 4.2 on page 32) in the **Path to the SSLCA certificate file** field. By default the certificate file will be saved on the server in the application data folder in the **OpsecDir** service folder with filename **opsec.p12**. Therefore if the path to the file specified is a relative path, the application will search for it in **<Data folder>\OpsecDir**.

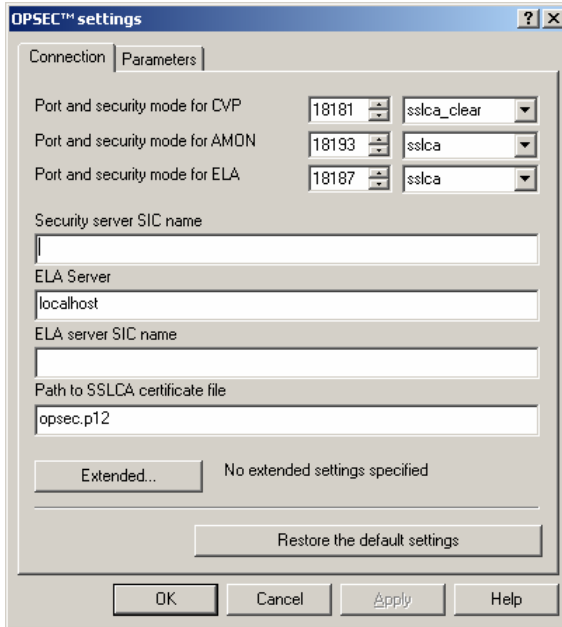


Figure 10. Configuring OPSEC™ settings
The **Connection** tab

In order to specify settings required to configure connection between Kaspersky Anti-Virus and Check Point™ Firewall-1® that are not included in the Connection tab, press the **Advanced** button.

This will open the **Configuring additional OPSEC™ settings** window (see Figure 11). Enter the description of the required settings and press the **OK** button.

An example of such settings for CVP and AMON protocols is the IP address on which the Security Server is expecting connection with Check Point™ Firewall-1®. If this setting is not specified, the Security Server will await connection on all IP addresses available on it.

Example:

```
cvp_server      ip          10.10.10.2
amon_server    ip          10.10.10.2
```



For detailed information about secure connection types and default values for various versions of Check Point™ Firewall-1® visit the Check Point™ corporate website at:

http://www.opsec.com/developer/gw_comm_mode.html

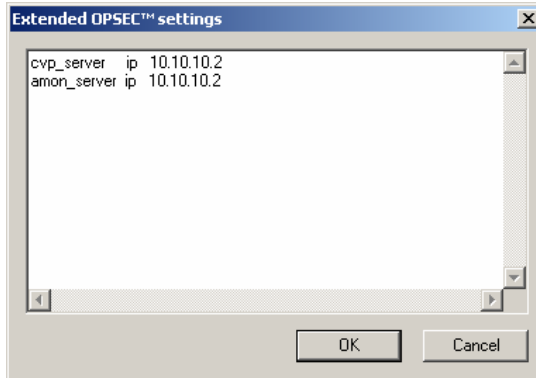


Figure 11. Configuring additional OPSEC™ settings

3. Select the **Parameters** tab (see Figure 12). This tab displays settings used to control the data exchange between the Security Server and Check Point™ Firewall-1®. Specify the required values.
 - Specify the maximum time (in seconds) the Security Server will wait for the data to be received from Check Point™ Firewall-1® in the **Connection timeout** field in the **General** section. If no information has been received within this period of time, the Security Server will disconnect from Check Point™ Firewall-1®. The connection will be established later when Check Point™ Firewall-1® transfers data subject to anti-virus processing. The default value is 120 seconds.
 - Establish the frequency (in seconds) for the Security Server to issue the confirmation signal used to maintain the connection with Check Point™ Firewall-1® in the **Confirm connection every** field of the **General** section. The suggested default value is 5 seconds.
 - In order to ensure the output of registered Anti-Virus operation events into the Check Point™ Firewall-1® event logs and to ensure notification about such events using Check Point™ Firewall-1® tools, check the **Notify about events via ELA protocol** box. After this:
 - Select the option to determine the way notifications will be made from the **Notification type** drop-down list. Select the

Do not notify option if you do not want notifications to be issued.

- Specify the frequency for the Security Server to attempt to restore the connection with Check Point™ Firewall-1® if the connection fails, in the **Try to connection every** field.

Information about the events that happened while the connection was out, will be transferred to Check Point™ Firewall-1® immediately after the connection is restored.



Information about the following events will be sent to the Check Point™ Firewall-1® application:

- updating of anti-virus database,
- forthcoming expiration of the license;
- change of the application status (start/stop of the Security server, changes in the application functionality).

By default the **Notify about events via ELA protocols** box is not checked.

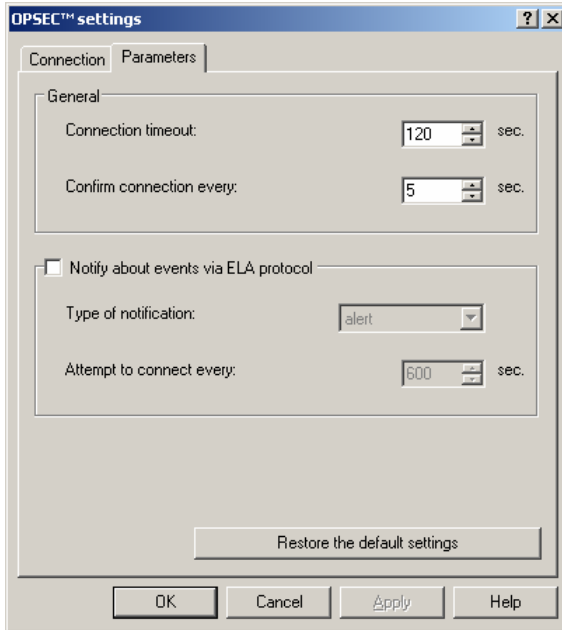


Figure 12. OPSEC™ setting configuration.
The **Parameters** tab

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

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

5.6. Minimum required settings

After the settings for the interaction with Check Point™ Firewall-1® are configured, Kaspersky Anti-Virus will start working with the minimum set of settings, most of which are default optimum settings recommended by the Kaspersky Lab's experts. If necessary, depending on the network properties and the characteristics of the computer on which the Security 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 connection settings in order to receive updates.

The application is configured from the administrator's workplace. It can be performed irrespective of whether Check Point™ Firewall-1® is running.

5.7. Protection without additional configuration

The anti-virus protection will start operating immediately after the parameters for the interaction between Kaspersky Anti-Virus and Check Point™ Firewall-1 are configured. The default operation mode of the Anti-Virus is as follows:

- The application scans objects for the presence of all malware known by the moment (with standard anti-virus protection level selected).
- The anti-virus protection will cover all data transferred via HTTP, FTP and SMTP protocols.
- The scan scope will include objects of all formats, except container objects with the level of nesting above 32.
- The maximum time allowed for scanning one object is 1800 seconds;
- If an infected object is detected when scanning HTTP traffic, the application will attempt to disinfect this object and will pass it if the object was disinfected and if it can not be disinfected, the application will block access to it and display an information message of the following format:

```
Kaspersky Anti-Virus 5.5 for Check Point™ Firewall-1®
```

```
Requested address "<path to the resource>" contains an infected object  
<virus name>. Access to the resource has been blocked.
```

Suspicious, protected and corrupted objects detected will be delivered to the user intact.

- If an infected object is detected when scanning FTP traffic, the application will attempt to disinfect this object and will pass if the object was disinfected and if it can not be disinfected, the application will block access to it and displays an FTP client connection error message:

Suspicious, protected and corrupted objects detected will be delivered to the user intact.

- If an infected object is detected while scanning SMTP traffic, the application will:
 - save a copy of the original message along with all attached files in the backup storage;
 - delete all files attached to the message;
 - replace the body of the message with an information message of the following format:

```
Kaspersky Anti-Virus 5.5 for Check Point™ Firewall-1®
```

The message sent by you contains an **infected** object **<virus name>**. The message has been blocked.

Suspicious, protected and corrupted objects will be delivered to the user intact.

- The anti-virus database is updated hourly via internet from the Kaspersky Lab's HTTP and FTP updates servers.
- The anti-virus protection report will not be created.

5.8. Verifying the application performance

After Kaspersky Anti-Virus is installed and configured, we recommend that you verify the correctness of its settings and operation using a test "virus" and its modifications. A separate test shall be performed for each protocol.

5.8.1. Test "virus" EICAR and its modifications

This test "virus" was designed by  (The European Institute for Computer Antivirus Research) specifically 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.



Before you download the test "virus", you must disable the anti-virus protection (see section 7.3, page 63), because otherwise *anti_virus_test_file.htm* will be identified by the Anti-Virus as an infected object received via HTTP protocol and processed accordingly.

Do not forget to enable the anti-virus protection immediately after you download the test "virus".

If you have no internet connection, you can create your own test "virus". To create a test "virus," type the following in any text editor and save the file as **ecar.com**:

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

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

5.8.2. Testing the HTTP traffic protection



In order to detect viruses in the data stream transferred via HTTP protocol:

download the test “virus” from the official website of the **EICAR** organization at http://www.eicar.org/anti_virus_test_file.htm.

When attempting to download the test “virus”, Kaspersky Anti-Virus will detect this object, identify it as an infected object that cannot be disinfected, and will perform an action **specified** in the HTTP traffic settings for this type of objects. By default, (see section 5.7, page 47), if you attempt to download the test “virus” connection with the website will be terminated and the browser will display a message informing the user that this object is infected with virus *EICAR-Test-File*.

5.8.3. Testing the SMTP traffic protection

In order to detect viruses in the data streams transferred using SMTP protocol, you can use the mail system that uses this protocol to transfer data.



In order to do this:

1. Create a **plain text** message using a mail client installed on your computer.



Message that contains a test virus will not be scanned if it is created in the RTF or HTML format!

2. Copy the text of the standard or modified “virus” in the beginning of the message or attach a file containing the test “virus” to the message.
3. Send the message to the administrator.
4. Read the message received at this address.

Kaspersky Anti-Virus will detect this object, identify it as infected and will perform an action specified in the SMTP traffic scan settings as the default action for this type of objects (see section 5.7, page 47):

- all attached objects will be deleted;
- the body of the message will be replaced with an information message about the detected virus *EICAR-Test-File*;
- a copy of the original message along with all attached files will be saved in the backup storage;

5.8.4. Testing the FTP traffic protection



In order to detect viruses in the data stream transferred via FTP protocol:

1. Copy the test "virus" to a location that you can access using FTP protocol.
2. Try to download *ecar* "virus" from this location.

Kaspersky Anti-Virus will detect this object, identify it as an infected object that cannot be disinfected, and will perform an action specified in the FTP traffic settings for this type of objects. Thus, if you are using the default settings (see section 5.7, page 47), the Anti-Virus will disconnect from this location when the test "virus" is attempted to be downloaded and a connection error message will be displayed.

CHAPTER 6. UPDATING THE ANTI-VIRUS DATABASE

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

Kaspersky Lab's anti-virus database contains the description of the following objects categories:

- a. All currently known malicious programs.
- b. Programs that do not contain malicious code as it is commonly understood, but may impose a moral threat, inflict financial damage or facilitate the theft of confidential information. This software category includes:
 - adware;
 - various harmless utilities that can be used by malicious software and intruders;
 - automatic dialing programs that connect the user's computer to commercial internet sites;
 - automatic dialing programs that connect the user's computer to porn websites;
 - automatic porn files downloading programs;
 - keyboard spies;
 - password hacking programs;
 - backdoor programs,
- c. Joke programs and programs with "bizarre" content or form programs that affect the system in a way that cannot be qualified as beneficial. This type of software include:
 - programs that cause unexpected video or sound effects;
 - programs that cause problems in the system operation;
 - virus simulators.
- d. Programs that do not contain malicious code and do not inflict any damage to the computer, but can be a part of the environment used for development of malicious software. This software category includes:
 - software hacking programs, key generators, credit card numbers generators;
 - Java classes;
 - programs that collect information about the system security (anti-virus software installed, firewalls, etc.)
 - network utilities (scanners, etc.)

Categories of objects that will be detected by the Anti-Virus in the traffic passing through the firewall will be determined by the selected level of the anti-virus protection (see section 7.2, page 63).

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

The application copies anti-virus database updates via internet from the Kaspersky Lab's updates servers or from a network updates folder specified by the server administrator. The use of the particular resource depends on the settings. The updates folder can be set up as a public access folder that will be used to store downloaded updates for the following Kaspersky Lab's applications: Kaspersky Administration Kit 5.0, Kaspersky Anti-Virus 5.0 for Windows Workstations and Kaspersky Anti-Virus 5.0 for File Servers (see section 6.2, page 55).

Updates are downloaded either according to the schedule or manually. In order to download the anti-virus database from the internet, your computer must be connected to the internet. Kaspersky Anti-Virus downloads updates from the dedicated update servers and then installs the required file on your computer. Kaspersky Anti-Virus allows configuring the notification about the results of the anti-virus database update (see Chapter 12 on page 110).

Information about the anti-virus database used by the application can be viewed by following the [General settings](#) link on the **General tab** in the **General settings** window (see Figure 40). The following information is provided:

- number of records in the anti-virus database;
- date and time of the anti-virus database creation.



In order to update the Kaspersky Anti-virus database:

1. Select the node corresponding to the required server in the console tree and follow the [Anti-virus scan](#) link in the results pane.
2. Specify the source of updates in the **Updates** tab of the **Anti-virus scan** window (see Figure 13) that will open. You can select update from the internet and configure the connection settings or select update from the network folder (details see section 6.1, page 54 and section 6.2, page 55).

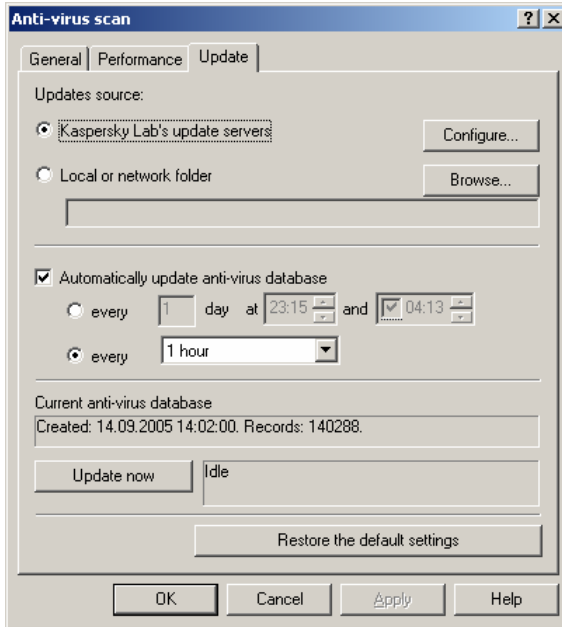


Figure 13. Anti-virus database updates settings window.
Configuring internet updates downloading

3. For automatic updates, create an updates downloading schedule (details see section 6.3, page 56). If updates are required immediately, press the **Update now** button (details see section 6.4, page 57) to download the updates manually.



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

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

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

6.1. Downloading updates from the internet



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

1. Select the node corresponding to the required server in the console tree and follow the Anti-virus scan link in the results pane.
2. Go to the Updates tab in the Anti-virus scan window that will open (see Figure 13) and select Kaspersky Lab's updating servers (default option) as the source of updates.
3. After this press the Configure settings button and specify the network connection settings in the Internet updating setting window that will open (see Figure 14):

Internet updating settings

Automatically select the updates server

Use the specified server:

Use proxy

Address: Port:

Use authentication

Username:

Password:

Use passive FTP mode

OK Cancel Help

Figure 14. Network connection settings

- Specify the server from which the updates will be downloaded. Select the **Automatically select the update server** option to ensure that the application selects a server from those recommended by Kaspersky Lab or select the **Use the specified server** and enter the address of an HTTP or an FTP updates server.

- 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 **User Name** and the **Password** fields.
 - If you would like to use the passive mode for updating from an FTP server, check the **Use the passive FTP mode** box, if you need to use the active mode – uncheck this box. We recommend using the passive mode.
4. After you are done with the settings, press the **OK** button in the Internet update settings in order to apply the changes.
 5. Press the Apply or the **OK** button on the **Updates** tab.

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

6.2. Installing updates from a network folder

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

Kaspersky Anti-Virus 5.0 for Windows Workstations and Kaspersky Anti-Virus 5.0 for File Servers also allow users to save updates downloaded from the internet into a public folder and to use this folder as the local updates source.



In order to ensure successful updates, the computer on which the Security Server is installed, shall have the rights for reading from this public folder.



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

1. Select the node corresponding to the required server in the console tree and follow the Anti-virus scan link in the results pane.
2. Go to the Updates tab in the Anti-virus scan window that will open (see Figure 15), select the Local or network folder option as the

updates source and enter the path to the required folder in the corresponding field manually or using the **Browse** button.

3. After you are done with the settings, press the Apply or the OK button.

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

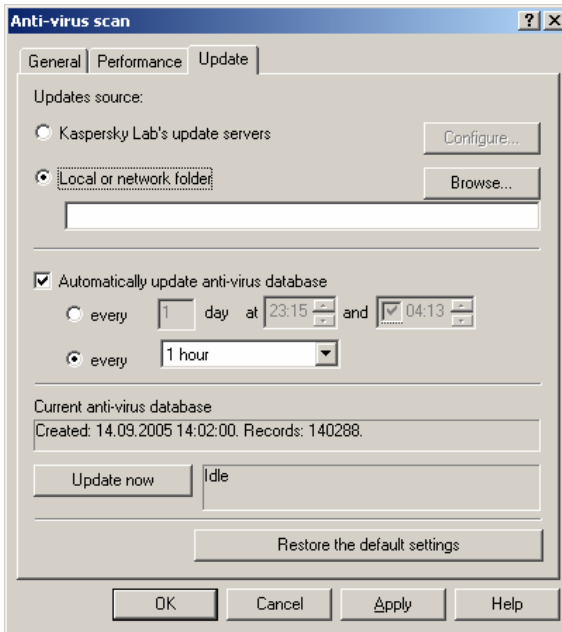


Figure 15. Configuring updates from the local folder

6.3. Automatic updates



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

1. Select the node corresponding to the required server in the console tree and follow the Anti-virus scan link in the results pane.
2. Check the Update the anti-virus database automatically box in the General tab of the Anti-virus updates window (see Figure 13) that will open and create a schedule for receiving the updates. In order to do this select the required schedule option and specify the required frequency, the updates interval unit and the update time.

3. After you are done with the settings, press the Apply or the OK button.

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

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

6.4. Updating the anti-virus database in the manual mode



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

1. Select the node corresponding to the required server in the console tree and follow the [Anti-virus scan](#) link in the results pane.
2. Press the Update **now** button on the **Updates** tab of the **Anti-virus scan** window (see Figure 13) that will open.



The **Update now** button is not available if the anti-virus is being updated at the moment or if this function of your application has been disabled due to the violation of the license terms (see Chapter 11, page 102).

As a result, the application will immediately update the anti-virus database in accordance with the specified settings.

CHAPTER 7. ANTI-VIRUS PROTECTION

The main task of Kaspersky Anti-Virus is scanning mail traffic passing through Check Point™ Firewall-1® and disinfecting or blocking e-mail messages using the information contained in the current (latest) version of the anti-virus database.

Depending on the anti-virus protection level (see section 7.1, page 60) the application can detect:

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

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



If you transfer software through the firewall, you have to exclude such software category from the objects subject to be scanned.

If the anti-virus server protection is enabled (details see section 7.3, page 63), then starting and stopping of the traffic scan will be performed simultaneously with the startup and shutdown of the computer on which the Security Server is installed.

All objects transferred through the firewall will be scanned in the real-time mode. By default HTTP, FTP and SMTP traffic will be processed. If required (for example, if the traffic arriving to Check Point™ Firewall-1® has already been scanned by another anti-virus application) the scan of any of the above protocols can be disabled.

Depending on the settings specified for each protocol in the anti-virus settings, the application will:

- select objects to be scanned;
- scan and analyze the object using the anti-virus database;
- pass clean objects to the user and process other objects in accordance with the current settings; a copy of the object can be saved in the backup storage before it is processed.

Kaspersky Anti-Virus allows the user to configure notifications about the results of the anti-virus scan of objects (see Chapter 12 on page 110).

When scanning e-mail messages transferred via SMTP protocol the program scans the body of the message and all attached files of any format.

It is to be noted that Kaspersky Anti-Virus distinguishes between simple objects (the message body, simple attachment, for example an executable file) and containers (consisting of several objects, for example an archive, a message with another message attached to it or an MS Word file that contains macros). In order to decrease the load on the server, containers with the nesting level above a specified value can be excluded from the anti-virus scan.

An additional list of objects to be excluded from the anti-virus scan can be created for data transferred via HTTP and FTP protocols. Such list can include archives, packed executable files and some other types of files.

When scanning multi-volume archives downloaded from the source in parts, Kaspersky Anti-Virus will treat and process each volume and each part as an individual object. In this case, the application can detect malicious code only if such code is fully located in one of the volumes. Malicious objects split into parts can not be detected. In this situation, the malicious code may propagate after the object is restored as one entity.



Multi-volume archives and objects downloaded in parts can be scanned after they are saved to the hard drive using, for example, Kaspersky Anti-Virus for Windows Workstations.

For HTTP protocol Kaspersky Anti-Virus provides an option of blocking access to objects that are transferred in parts (see section 7.4, page 65). This option is not provided for FTP protocol and in order to minimize the possibility of infection using the method described above, we recommend disabling the ability to download information by parts in the settings of Check Point™ Firewall-1®.

For data requested via HTTP protocol, Kaspersky Anti-Virus blocks access to objects that do not satisfy the requirements of this protocol (for example, no headings). Such objects will not be sent for anti-virus processing nor will they be delivered to the user. However, if required, there is a provision for a transfer of data that does not include service information to the user. In this case the object will be sent for anti-virus processing, processed and delivered to the user according to the anti-virus scan settings selected for HTTP traffic.

Anti-virus scan increases the time required to deliver the information to the user. Therefore, there is a provision for transferring unscanned data that still can rule out the possibility of the delivery of infected objects when processing objects transferred via HTTP and FTP protocols (see section 7.4, page 65). This method involves transferring of unscanned data in parts at maximum allowed intervals that make it possible to hold parts of downloaded information before the object has been scanned. If, as the result of the anti-virus scan, it appears that the

object is not infected, the rest of the information will be transferred to the user. Otherwise, the application will break the connection with the source and display a message informing the user that the information can not be downloaded. The object will be processed using the anti-virus scan settings and information about such objects will be logged in the events log and in the report.

The results of the scan are cached during a certain period of time that allows reducing the number of repeated scans of the object (see section 7.4, page 65).

Kaspersky Anti-Virus allows simultaneous scan of several objects. 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 (see section 7.7, page 75).

The mode of scanning objects in RAM allows scanning objects without saving them to a work folder on the hard drive. Depending on the scan settings, the application can simultaneously scan up to 1000 objects up to 1024 KB each in the RAM without using the disk subsystem (see section 7.7, page 75).

The use of objects queue (see section 7.7, page 75) allows increasing or decreasing the throughput of Kaspersky Anti-Virus and thus - adjusting the load depending on the traffic passing through the firewall.

7.1. Anti-virus objects processing

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

- **Clean** – the object does not contain malicious or potentially dangerous code.
- **Infected** – the object contains at least one malicious or potentially dangerous object.
- **Suspicious** – object's code is similar to the code of a known malicious or potentially dangerous object.
- **Protected** – object is password-protected.
- **Corrupted**– object is corrupted.

The application can disinfect, block objects detected during an anti-virus scan or pass them to the user without making changes to them.

You can configure notifications about the detection of infected, suspicious, protected and corrupted objects (see Chapter 12 on page 110). No notification is made about objects that are not infected.

Before the processing, a copy of the object can be saved in the backup storage to be restored or deleted later.

The disinfection option is provided only for **infected** objects transferred via HTTP or FTP protocols. A special processing procedure can be used for **non-disinfectable** objects.

7.1.1. Actions performed with objects transferred via HTTP protocol

The following actions can be performed to disinfect **infected** objects detected during the scan of data transferred via HTTP protocol.

- *Disinfect* – disinfect and pass the object to the user, once disinfecting. If the object cannot be disinfecting, apply the action specified for objects that cannot be disinfecting.
- *Disinfect, save a copy* - disinfect, pass the object to the use once disinfecting, save a copy of the original object in the backup storage. If the object cannot be disinfecting, apply the action specified for objects that cannot be disinfecting.

The following actions can be performed to process **infected, non-disinfectable, suspicious, protected** and **corrupted** objects.

- *Skip, make no changes* – pass the object to the user without making changes to it;
- *Replace with text* – block access to the object, display in the browser window an informational message generated based on a replacement template.
- *Replace with text, save a copy* – block access to the object, display in the browser window an informational message generated based on a replacement template, save a copy of the original object in the backup storage.

Copies of clean and skipped objects can also be saved in the backup storage.

7.1.2. Actions performed with objects transferred via FTP protocol

The following actions can be performed to disinfect **infected** objects detected during the scan of data transferred via FTP protocol.

- *Disinfect* – disinfect and pass the object to the user, once disinfecting. If the object cannot be disinfecting, apply the action specified for objects that cannot be disinfecting.
- *Disinfect, save a copy* - disinfect, pass the object to the use once disinfecting, save a copy of the original object in the backup storage. If the object cannot be disinfecting, apply the action specified for objects that cannot be disinfecting.

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

- *Skip, make no changes* – pass the object to the user without making changes to it;
- *Block* – block access to the object; as a result, a data transfer error message will be displayed in the FTP client window.
- *Block, save a copy* - block access to the object, save a copy of the original object in the backup storage. As a result, a data transfer error message will be displayed in the FTP client window.

Copies of clean and skipped objects can also be saved in the backup storage.

7.1.3. Actions performed with objects transferred via SMTP protocol

The following actions can be applied to process **infected, suspicious, protected and corrupted** objects detected as the result of an anti-virus scan of information transferred via SMTP protocol.

- *Skip, make no changes* – pass the object to the user without making changes to it.
- *Replace with text* – replace all files attached to the message, replace the message body with the informational message generated based on a replacement template.
- *Replace with text, save a copy* - delete all files attached to the message, replace the message body with an informational message generated based on the replacement template, save a copy of the original message (the message body and all attached files) in the backup storage.

The selected action will be applied to the entire message irrespective of whether an infected, suspicious, protected or corrupted object is detected in the message body or in one of the attached files.

Copies of clean and skipped objects can also be saved in the backup storage.

7.2. Anti-Virus protection level

Kaspersky Anti-Virus allows detecting all currently known at the moment malicious and potentially dangerous programs in the traffic passing through the firewall. Description of these programs and methods used for disinfection of infected objects are contained in the Kaspersky Lab's anti-virus database (see Chapter 6, page 51). Categories of objects detected by Kaspersky Anti-Virus 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 Updating the anti-virus database list on page 51.
- **Redundant anti-virus protection level:** protection against all currently known malicious and potentially dangerous programs included under 'b', 'c' and 'd' in the Updating the anti-virus database list on page 51.

7.3. Enabling and disabling the anti-virus protection. Selecting the anti-virus protection level

If the anti-virus protection is enabled, the anti-virus scan of the traffic passing through the firewall will be commenced and stopped at the startup and shutdown of the operating system on the computer with the Security Server installed. By default scan is provided for HTTP, FTP and SMTP protocols. In order to lower the load on the server you can disable scanning of a specific traffic individually in the settings for each protocol.

The objects will be scanned in accordance with the anti-virus protection level selected.

If anti-virus protection is disabled, no scan will be performed for the traffic transferred via any of the protocols.



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



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

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. Select one of the following options in the **Anti-Virus protection** group on the **General** tab (see Figure 16) in the **Anti-Virus protection** window that will open:
 - **Disabled** in order to disable the anti-virus scan of information passing through the firewall.
 - **Standard anti-virus protection, Extended anti-virus protection** or **Redundant anti-virus protection** in order to enable anti-virus protection and apply the required protection level.



The use of the extended or the redundant anti-virus protection level may affect the speed of your Anti-Virus operation. Besides, some programs that you use may be treated as risk-ware.

3. In order to apply the changes, press the **Apply** or the **OK** button. The anti-virus protection will then be enabled/disabled within a couple of minutes.

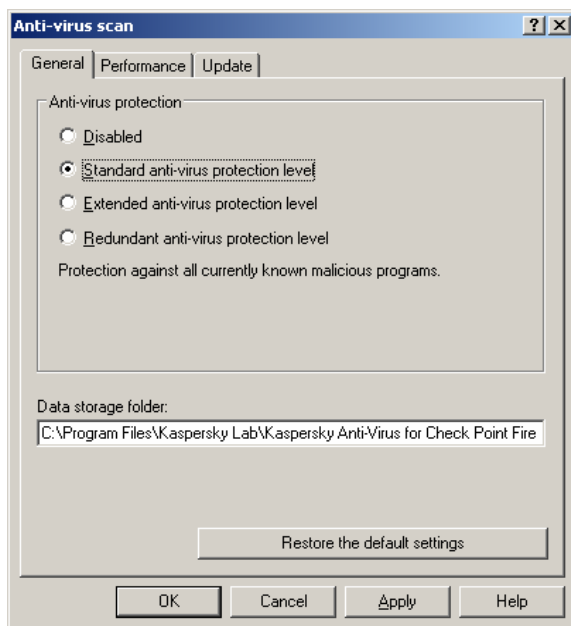


Figure 16. Enabling anti-virus protection

7.4. Scanning HTTP traffic



In order to configure the settings for scanning data transferred via HTTP protocol:

1. Select the node corresponding to the required server in the console tree and follow the [HTTP traffic settings](#) link in the results pane.

Configure the anti-virus operation settings for scanning HTTP traffic on the tabs of the **HTTP traffic scan settings** window that will open (see Figure 17).

2. On the Settings tab (see Figure 17) check the Scan HTTP traffic in order to enable scanning. After this specify the values of the settings that control:
 - transfer of unscanned data to the user if the object scan takes a long time;
 - object scan when the object is accessed again;

- transfer of information, downloaded from the source in parts, to the user.
- Transfer of data that does not include service information to the user.

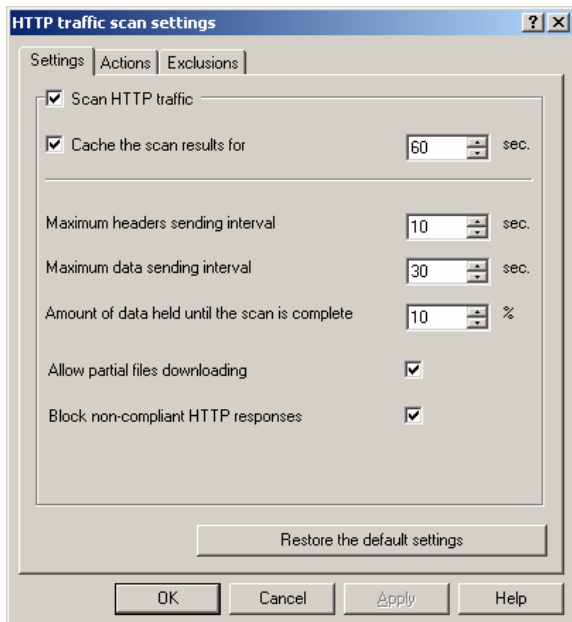


Figure 17. HTTP traffic scan settings
The **Settings** tab

- In order to minimize the number of repeated scans of the object, check the **Cache the scan result for** box and specify time (in seconds) during which the program will hold the result of the scan in memory. When the user tries to access the object again within the specified interval, the access to the object will be granted or the user will receive a notification about the result of the last scan of this object. By default the box is checked and the interval value is 60 seconds.
- In order to ensure that the client program that requested the stream does not break connection with the source and does not display a connection error message, Kaspersky Anti-Virus, during the entire time of the scan, transfers the service information (as a rule, HTTP protocol headers) and small data packets at a specified interval. Specify (in seconds) the time interval for sending next data packet in the **Maximum header**

sending interval field. The value of this setting is set based on the parameters of the client program and shall not exceed the time period after which the client displays a message about the failed attempt to connect to the specified address. The suggested default value is 10 seconds.

- Specify the maximum allowed timeout for the user to wait for the next data packet in the **Maximum data sending interval** field (the default value is 30 seconds). This setting determines the speed with which the real data will be delivered to the user.
- Specify the percentage of the total volume of the unscanned data that will be held until the scan is complete in the **Amount of data to be held until the scan is complete** field. The greater the value of this setting, the less will be the possibility of infection when passing unscanned data to the user. The suggested default value is 10%.
- In order to allow delivery of files downloaded in parts to the user, check the **Allow partial files downloading** box. If this box is not checked, the application will break the connection with the source and display a message informing the user that the information can not be downloaded. By default this box is checked.
- In order to ensure that objects that do not include standard HTTP protocol service information are scanned for viruses and delivered to the user, uncheck the **Block non-compliant HTTP responses** box. Objects will be processed in accordance with the scan settings selected for HTTP traffic. If the box is checked (default option), non-standard HTTP responses will be blocked, will not be sent for anti-virus scanning and therefore will not be delivered to the user.

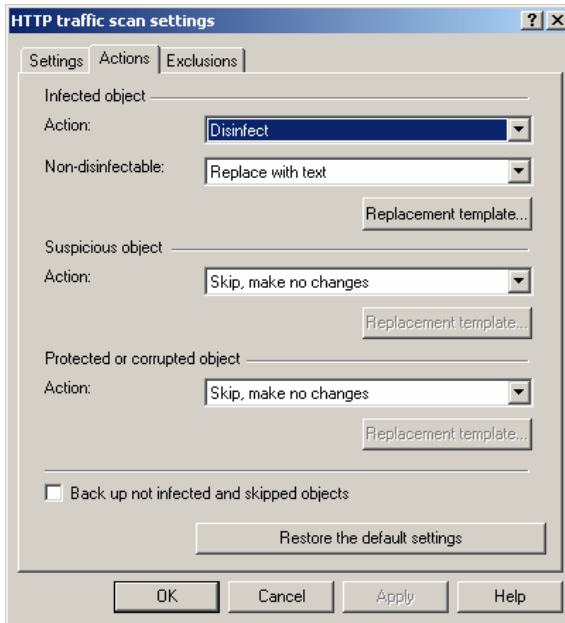


Figure 18. HTTP traffic scan settings.
The **Actions** tab

3. Specify which actions will be performed upon detection of infected, suspicious, protected and corrupted objects on the **Actions** tab (see Figure 18). Determine the order of processing for each status individually. In order to do this, select the required action from the drop-down list in the corresponding section.

If you select an action that involves replacement of the object, you must create a replacement template. In order to do this, press the **Notification template** button and enter the notification text in the window that will open (see Figure 19). The text of the notification may include information about the virus detected, HTTP address of the infected object and information about the connection error occurred. To include this information add corresponding substitution macros to the template selecting them from the drop-down list accessible via the **Macros** button.

To save copies of clean objects and unchanged files, select the **Save copies of clean and passed objects** check box.



When the **Save copies of clean and passed objects** check box is selected, the **Disinfect, save a copy** action will be applied to all infected objects instead of the **Disinfect** action. The original copies of disinfected objects and the objects that cannot be disinfected will also be saved if the **Skip, make no changes** action is selected for such objects.

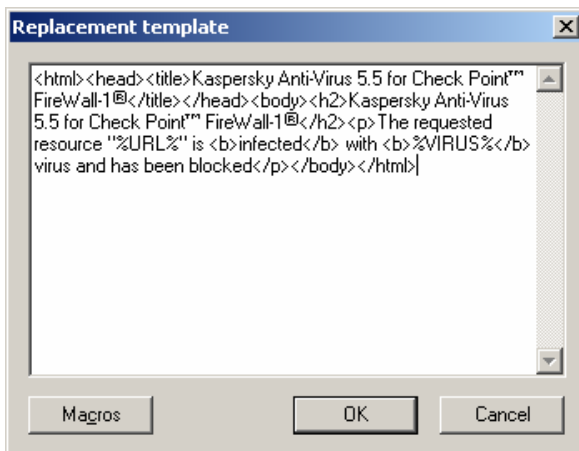


Figure 19. Creating the replacement template

4. On the **Exclusions** tab (see Figure 20) provide the list of objects that will not be scanned for the presence of malicious code. In order to do this, check boxes next to the corresponding types of objects in the list.

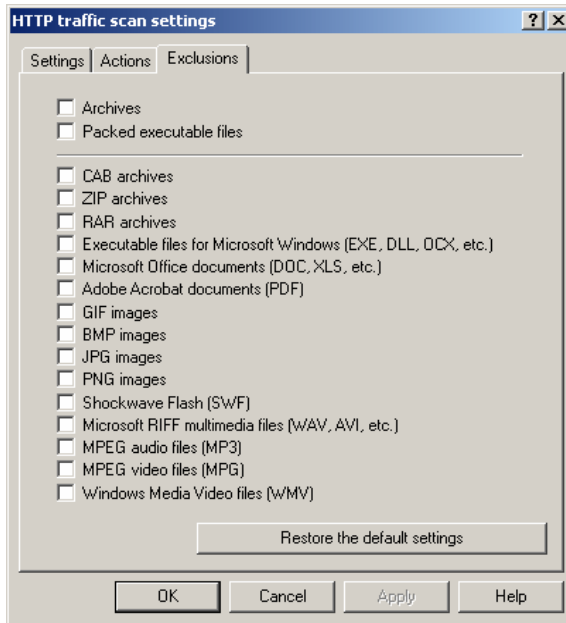


Figure 20. HTTP traffic scan settings
The **Exclusions** tab

5. 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.



In order to disable scanning data transferred via HTTP protocol:

uncheck the **Scan HTTP traffic** box on the **Settings** tab of the **HTTP scan settings** window (see Figure 17) and press the **Apply** or the **OK** button.

7.5. Scanning FTP traffic



In order to configure the settings for scanning data transferred via FTP protocol:

1. Select the node corresponding to the required server in the console tree and follow the [FTP traffic settings](#) link in the results pane.

This will open the **FTP scan settings** window (see Figure 21). Configure the anti-virus operation settings for scanning FTP traffic on the tabs of this window.

The settings are configured similarly to the settings used for HTTP traffic. (see section 7.4, page 65).

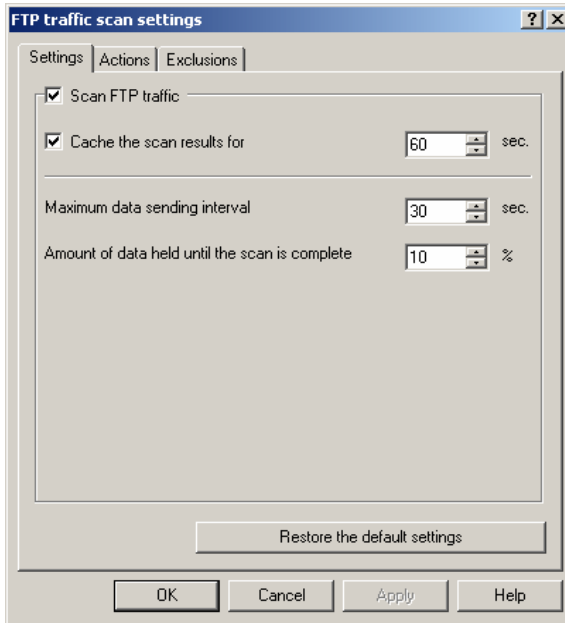


Figure 21. FTP traffic scan settings
The **Settings** tab

2. In order to ensure that the scan will be performed, check the Scan FTP traffic box (see Figure 21). After this specify values for the settings controlling the transfer of unscanned data to the user if the object scan takes a long time.
3. Specify which actions will be performed upon detection of infected, suspicious, protected and corrupted objects on the **Actions** tab (see Figure 21).

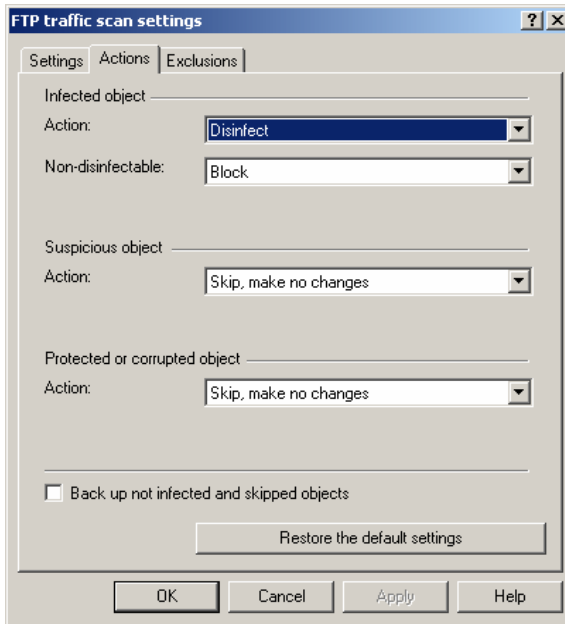


Figure 22. FTP traffic scan settings.
The **Actions** tab

4. On the **Exclusions** tab (see Figure 23) provide the list of objects that will not be scanned for the presence of malicious code. In order to do this, check boxes next to the corresponding types of objects in the list

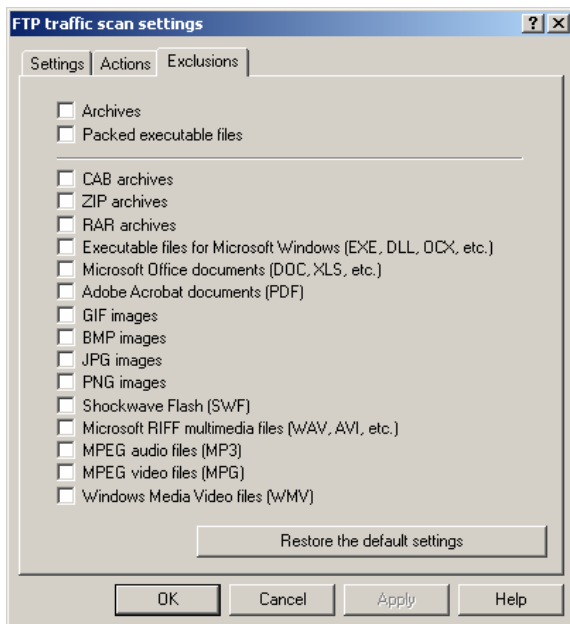


Figure 23. FTP traffic scan settings.
The **Exclusions** tab

5. 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.



In order to disable scanning data transferred via FTP protocol:

uncheck the **Scan FTP traffic** box on the **Settings** tab of the **FTP scan settings** window (see Figure 21) and press the **Apply** or the **OK** button.

7.6. Scanning SMTP traffic



In order to configure the settings for scanning data transferred via SMTP protocol:

1. Select the node corresponding to the required server in the console tree and follow the [SMTP traffic settings](#) link in the results pane. This will open the **SMTP scan settings** window (see Figure 25).

2. In order to ensure that traffic will be scanned, check the **Scan SMTP traffic** box (see Figure 24) on the **Settings** tab.



Figure 24 SMTP traffic scan settings
The **Settings** tab

3. Specify which actions will be performed upon detection of infected, suspicious, protected and corrupted objects on the Actions tab (see Figure 25). The settings are configured similarly to the settings used for HTTP traffic (see section 7.4, page 65).

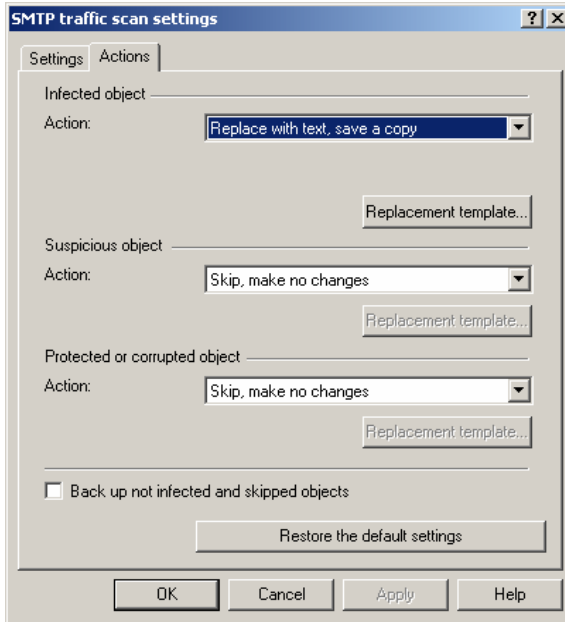


Figure 25 SMTP traffic scan settings
The **Actions** tab

- 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.



In order to disable scanning data transferred via SMTP protocol:

uncheck the **Scan SMTP traffic** box on the **Settings** tab of the **SMTP scan settings** window (see Figure 24) and press the **Apply** or the **OK** button.

7.7. Anti-virus scan efficiency



In order to configure the application's operation efficiency settings:

- Select the node corresponding to the required server in the console tree and follow the Anti-virus protection link in the results pane.

2. Select the Performance tab in the Anti-virus protection window that will open (see Figure 26) and specify the values for the settings displayed on this tab.

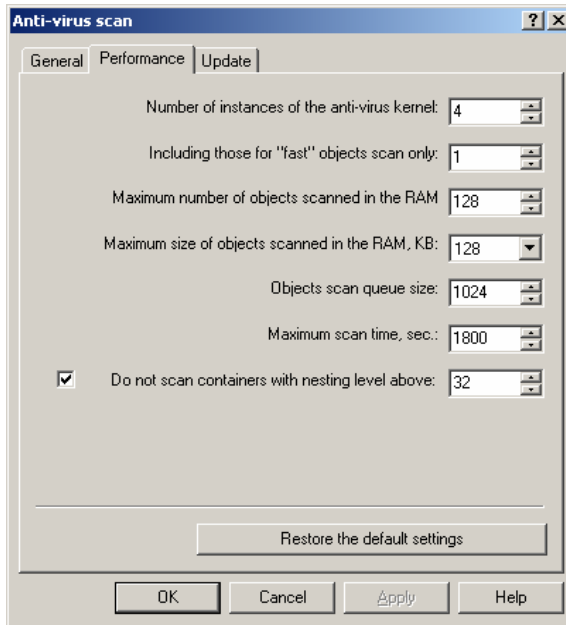


Figure 26. Kaspersky Anti-Virus Performance settings

- Number of instances of the anti-virus kernel running simultaneously. By default 4 instances will be created and will be running simultaneously. You can set this value in the range between 1 to 32. Microsoft recommends that you set up a value that is not greater than 4 multiplied by the number of the processors on the computer on which the Security Server is installed.
- The number of anti-virus kernel instances reserved for processing working ("fast") traffic. This setting allows to reduce the effect the scan of larger objects has on the Kaspersky Anti-Virus throughput. The suggested default value is 1.

"Fast" objects are only HTTP traffic objects that comply with the following criteria:

- text objects less than 2 MB;
- *html* files less than 2 MB;

- graphic objects less than 2 MB;
- all other objects (except applications) less than 256 KB.
- The maximum number of objects scanned in RAM without saving to the working folder on the hard drive. You can set this value in the range between 1 to 1000. The suggested default value is 128.
- The maximum number of objects being scanned in RAM in KB. Select the required value from the drop-down list.



If the queue is full or if the size of the object is above the specified limit, the object will be saved and scanned in the work folder located in the application data folder.

All files over 1024 KB are saved to be processed in the working folder.



The values of the settings used for scanning objects in RAM shall be determined based on the characteristics of the hardware of the computer on which the Security Server is installed.

The total volume of the objects being scanned shall not exceed the amount of free RAM.

- The size of the queue of objects to be scanned - the maximum number of objects being scanned and waiting to be scanned in the working folder on the hard drive. You can set this value in the range between 1 to 16383. The suggested default value is 1024.



If the queue is full, an object will not be scanned, but will be classified as clean and sent to the client that requested this object.

- The maximum time for scanning one object (in seconds). Specify the value within the range from 0 to 86400 seconds (inclusive). The default value is 1800 seconds.



If the object could not be scanned within the specified time period, it will be classified as clean and sent to the client that requested this object.

In order to exclude containers from the scan scope, check the **Do not scan containers with nesting level above** box and enter the desired value (the default value is 32). The application will scan all nested objects within the container including the specified level.

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



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

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

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



The settings for scanning objects in RAM will be applied only after the restart of the operating system of the computer on which the Security server is installed or after stopping and starting of Kaspersky Anti-Virus 5.5 for Check Point™ Firewall-1® service manually via the **Computer Management/Services** Windows utility.

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

CHAPTER 8. BACKUP STORAGE

Kaspersky Anti-Virus allows saving a backup copy of an infected object before processing. A copy of such object is created in the *backup storage*. Later such object stored in the backup storage can be restored (see section 8.3, page 84) or deleted (see section 8.4, page 86). The ability to restore objects may prove very useful, for example, if during the disinfection process some data was lost, if the object was deleted by mistake or if another disinfection attempt is required using an updated anti-virus database, for example, by Kaspersky Anti-Virus for Windows Workstations.



A backup copy of the object will be created only if it is provided for by the selected anti-virus protection settings:

When a backup copy of an object transferred via HTTP protocol or FTP protocol is created, the application will place the object that was attempted to be accessed into the backup storage. For objects transferred via SMTP protocol, the application will save the message body and all attachments irrespective of where the malicious object was detected.

The backup storage is a service folder. It is created in the application's data folder during the installation of the Security Server.

The amount of information that can be stored in the backup storage may be restricted by the following parameters: backup storage size or objects storage period. By default the maximum storage size is 1024 MB and the objects storage period equals 30 days. The administrator can alter the values of these restriction parameters (details see section 8.5, page 87)

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

- deletes objects for which the storage period has expired;
- if the available space is still insufficient to place the object in the backup storage, the application will free the required space by deleting "older" objects;



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 (see section 8.1, page 80), configuring its settings (see section 8.5, page 87) and managing backup copies of objects (see section 8.3, page 84 and section 8.4, page 86) functions are available via the **Backup storage** folder (see Figure 27). This folder is included into the structure of each node reflecting the monitored server.

For convenient viewing, search for information in the backup storage and for structuring the storage the application includes configurable user filters (see section 8.2, page 81). Filters, created for the backup storage, can be viewed in the **Backup Storage** folder as subfolders under names assigned by the administrator when the filters were created.

8.1. Viewing the backup storage



In order to view the backup storage:

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

After this a table containing the full list of all objects contained in the backup storage will appear in the results pane (see Figure 27).

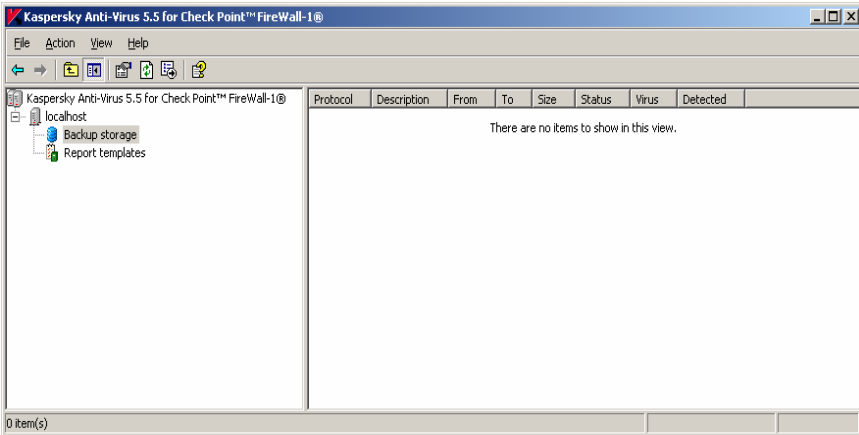


Figure 27. Viewing the backup storage

The following information is provided for each object in the table:

- **Protocol.** The type of protocol that was scanned when the object was detected.
- **Description.** HTTP, FTP address of the source of the subject of the message for objects transferred via SMTP protocol.
- **From.** IP address of the source where the object is located or e-mail address of the sender for objects transferred via SMTP protocol.

- **To.** IP address of the computer from which the object was requested or e-mail address of the recipient for objects transferred via SMTP protocol.
- **Size.** Object's size in bytes.
- **Status.** Status assigned to the object as a result of the anti-virus scan: **infected**, **disinfected**, **suspicious**, **protected/corrupted** (see section 7.1, page 60).



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

- **Virus.** The name of the detected virus or suspicious software (will be displayed only for objects with the **infected**, **disinfected** or **suspicious** status).
- **Time detected.** Exact date and time when the object was detected by Kaspersky Anti-Virus.

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

8.2. 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. Select the **Backup Storage** folder in the console tree and use the **New Filter** command in the shortcut menu or the analogous item under the **Action** menu. This will open a filter settings configuration window (see Figure 28).

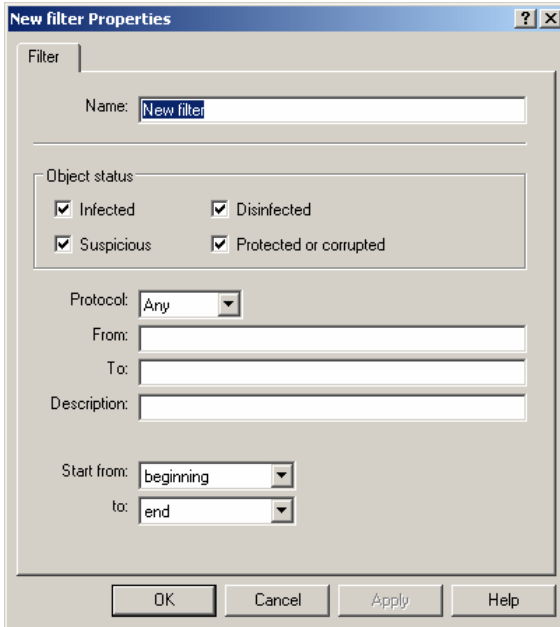


Figure 28. Creating a filter

2. Specify a name under which the filter will be saved in the Backup Storage folder.
3. Specify the parameter values that will be used to perform the search for (filtering of) objects stored in the backup storage. You can specify any number of parameters. The only mandatory parameter is the filter name.

The following information about the object can be used to configure the parameters:

- object status (multiple values can be selected);
- the type of protocol that was scanned when the object was detected. In order to view information for all protocols, select the **Any** option from the drop-down list;
- IP address of the source where the object is located or e-mail address of the sender for objects transferred via SMTP protocol;
- IP address of the computer from which the object was requested or e-mail address of the recipient for objects transferred via SMTP protocol;

- HTTP, FTP address of the source of the subject of the message for objects transferred via SMTP protocol;
 - time interval during which the object was detected.
4. After you are done with the settings press the **Apply** or the **OK** button. 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 criteria will be displayed in the results pane.

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



In order to change the filter parameters:

1. Select the filter you wish 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 29).

The image shows a dialog box titled "New filter Properties" with a standard Windows-style title bar (minimize, maximize, close buttons). The dialog is divided into several sections:

- Filter**: A tabbed section with a "Name:" label and a text input field containing "New filter".
- Object status**: A section containing four checked checkboxes: "Infected", "Disinfected", "Suspicious", and "Protected or corrupted".
- Protocol**: A dropdown menu currently set to "Any".
- From:** An empty text input field.
- To:** An empty text input field.
- Description:** An empty text input field.
- Start from:** A dropdown menu set to "beginning".
- to:** A dropdown menu set to "end".

At the bottom of the dialog, there are four buttons: "OK", "Cancel", "Apply", and "Help".

Figure 29. Configuring filter

2. Change the values of the filter's parameters as required.
3. In order to apply the changes, press the Apply or the OK button. For exit without saving the changes made, press the Cancel button.

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



In order to delete a filter:

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

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



As 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.

8.3. 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 27). You can use filters for searching for the object (see section 8.2, page 81).
3. Open the shortcut menu and use the Get file or the analogous command under the Action menu.
4. As the result a warning message will be displayed (see Figure 30) prompting you to confirm that you wish to proceed with the restoring. Press the Yes button to restore the object.
5. In a window that will open (see Figure 31) specify the folder to which you wish to save the object restored, and if required, enter or modify the object's name.

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



We recommend that you restore only objects with the **suspicious** or **protected/corrupted** status. During the next scan, for example with Kaspersky Anti-Virus for Windows Workstations using the updated version of the anti-virus database, you may be able to disinfect this object or detect in it a new virus not known before.

Restoring other objects may result in infecting your computer!

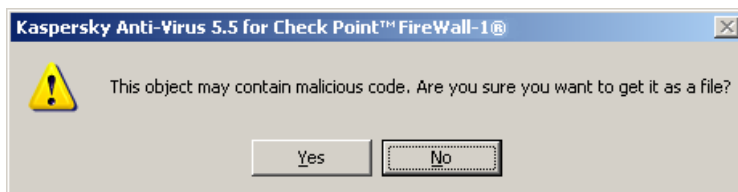


Figure 30. Confirming object restoring

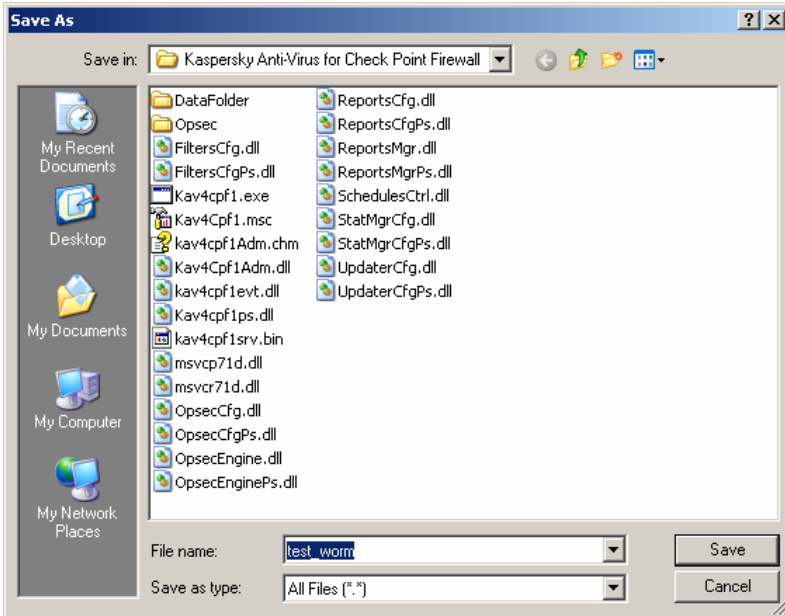


Figure 31. Restoring an object from the backup storage

8.4. Deleting objects from the backup storage

The following objects are automatically deleted from the backup storage:

- objects for which the storage period has expired;
- "older" objects if there is the maximum size of the backup storage has been reached and there is not enough space for storing a new object. The application will then delete the number of older objects required to free the space needed.

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



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

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

2. Select the object you wish to delete in the table displaying the content of the backup storage (see Figure 27). You can use filters for searching for the object (see section 8.2, page 81).
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 table reflecting the content of the backup storage.

8.5. 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 settings of the backup storage,

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 Properties:Backup storage window that will open (see Figure 32) specify the values for the settings.

Specify in the **Maximum storage size** field the total maximum size of objects that can be stored in the backup storage. The default this value is 1024 MB.

In the **Maximum object storage period** field specify the maximum number of days the objects will be stored in the backup storage. The suggested default value is 30 days.

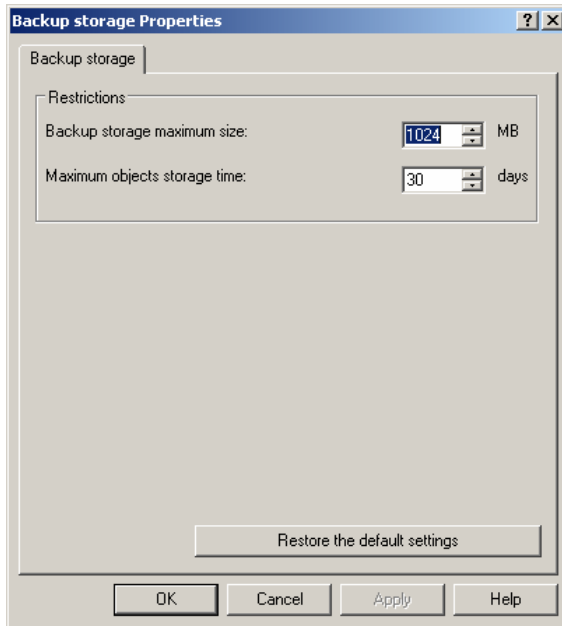


Figure 32. Configuring the backup storage settings

4. In order to apply the changes, press the **Apply** or the **OK** button. For exit without saving the changes made, press the **Cancel** button.

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

CHAPTER 9. REPORTS

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

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

- general scan results
 - the total number of scanned objects;
 - the total size of all scanned objects (in bytes);
- malicious objects detected;
- sources of infected objects;
- performance data of the anti-virus scan:
 - average processing speed (number of objects per second);
 - average processing speed (bytes per second);
 - the maximum scan speed achieved.

Reports are created automatically in accordance with the schedule or by request and are saved as *html* pages in the reports storage folder. The filename reflects the date and the time when the report was created in the following format **<DD.MM.YYYY_HH-MM-SS>**. Kaspersky Anti-Virus provides a possibility to configure notifications about the results of report creation (see Chapter 12 on page 110).

The default storage location for the reports is the **Reports** folder. This folder is located in the application's data folder. Any other folder selected by the administrator can be used to store reports (see section 9.2, page 92). The period for the reports storage on the server and the reports storage folder size are not limited. Reports are deleted manually using the file system.

Reports are viewed using the default system browser (see section 9.3, page 95).

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 the folder to store the report.

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

The list of the report templates created is displayed in the form of a table in the results pane (see Figure 33).

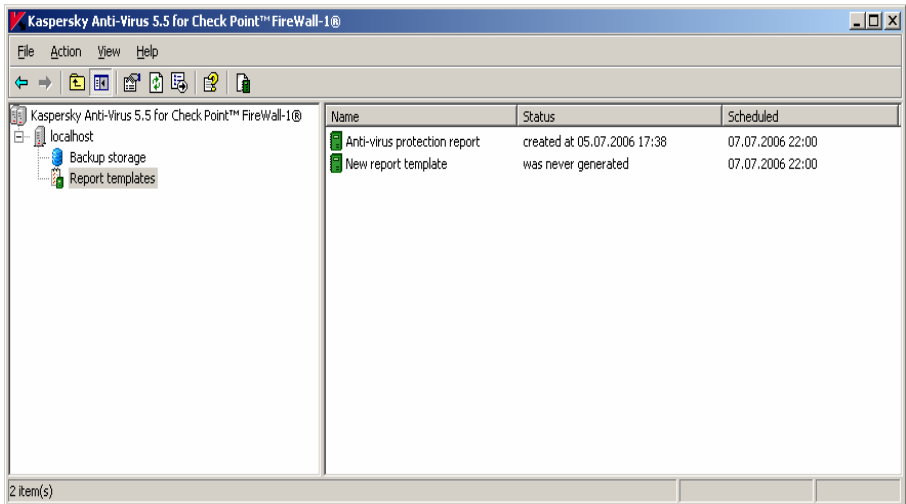


Figure 33. The **Report templates** folder

Apart from the template name the table contains the following information for each template:

- **Status:** status of the report created based on the template.
- **Expected:** date and time of creation of the next report according to the schedule or on-demand, if the automatic report creation is disabled.

Depending on current stage of the report creation, the report status may have one of the following values:

- **being created since <time and date for scheduled report generation>;**
- **created <date and time of the report creation>;**
- **was not created;**
- **error;**
- **creation error at <date and time of the error >.**

Detailed information about report template settings is provided in the settings window accessible through the Properties shortcut menu command (details see section 9.2, page 92).

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

9.1. Creating reports



In order to create an anti-virus scan report:

1. Create a report template (see section 9.2, page 92) or select an existing template.
2. Check the Create report box on the General tab of the report template configuration window (see Figure 35).

As a result, a new report will be created within intervals specified in the schedule.

In order to view the results of the anti-virus scan, open the report for the corresponding reporting period (see section 9.3, page 95).

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



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

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 33).
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 reports** box in the **General** tab of the report template settings window (see Figure 35) is checked.

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

The information about the sources of infected objects and malicious objects detected displayed in reports is limited by 10 lines. You can view ten most infected sources and top ten types of detected malicious objects.



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

1. 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 Properties: Report templates window that will open (see Figure 34):

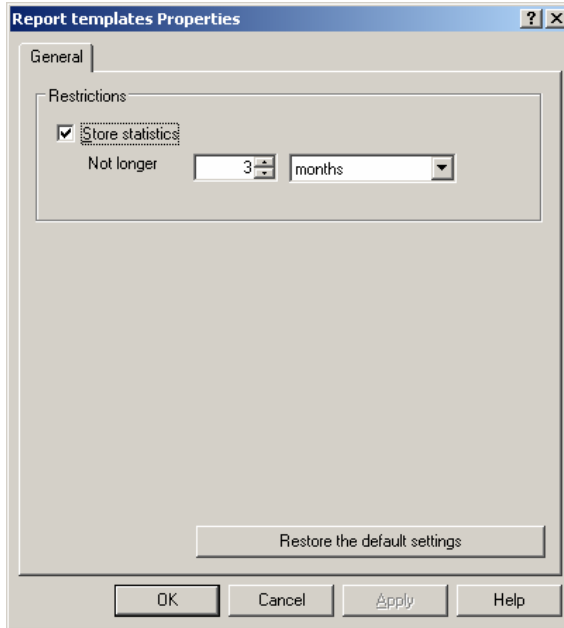


Figure 34. Configuring the reports settings

- Check the **Store statistics** box.
 - Specify the information storage period and select the time unit.
4. After you have made the changes, press the **Apply** or the **OK** button to apply the new settings. The settings will change within one hour after the changes have been applied. For exit without saving the changes made, press the **Cancel** button.

9.2. Creating the report template



In order to create a new report template.

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

2. Open the shortcut menu and use the Create a report template or the analogous command under the Action menu.
3. As a result, a report template settings window <New report template> will open (see Figure 35); this window consists of the following tabs: General and Parameters. Specify the required value for the settings in the tabs as follows:

Perform the following in the **General** tab (see Figure 35):

- Enter the template name in the **Name** field.
- Specify whether reports will be automatically created based on this template. In order to do this, check (or uncheck) the **Create reports** box.
- If required, enter a more detailed description of the report to be created based on this template in the **Description** field.
- After this, specify the folder into which reports will be saved. By default, it is the **Reports** folder located on the server in the application's data folder. You also manually select a different folder. If a folder with such name does not exist, it will be created by the application.

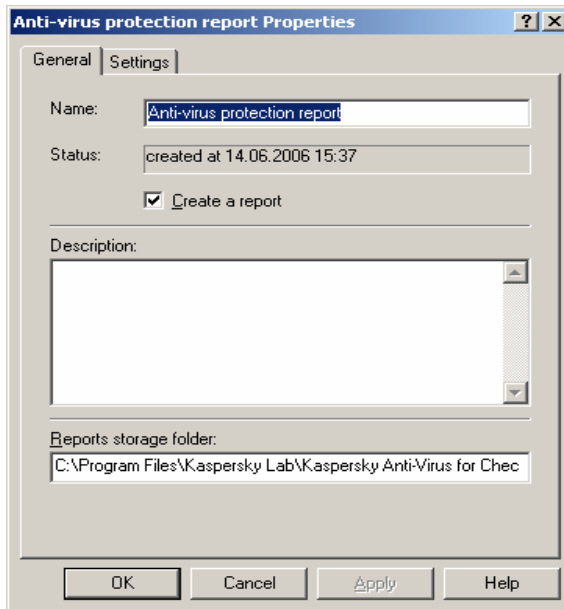


Figure 35. Report template.
The **General** tab

Specify the reporting period and the report creation schedule settings in the **Settings** tab (see Figure 36).

- The following options are available when specifying the reporting period:
 - specify the time interval. 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 the exact date for the beginning and the end of the reporting period. In order to do this, select the **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 weekdays** or **Monthly, on the specified day**. Configure the schedule settings in accordance with the selected frequency.
 - Specify the time when reports will be created in the **Generate report at** field.
4. After you are done with the settings press the **Apply** or the **OK** button.

As a result:

- The report template will be added to the **Report templates** folder and will be displayed as a table in the results pane.
- If the **Create reports** box in the **General** tab is checked, the application will create reports according to the time specified in the schedule and with the specified frequency. Reports can also be created by the administrator's request.

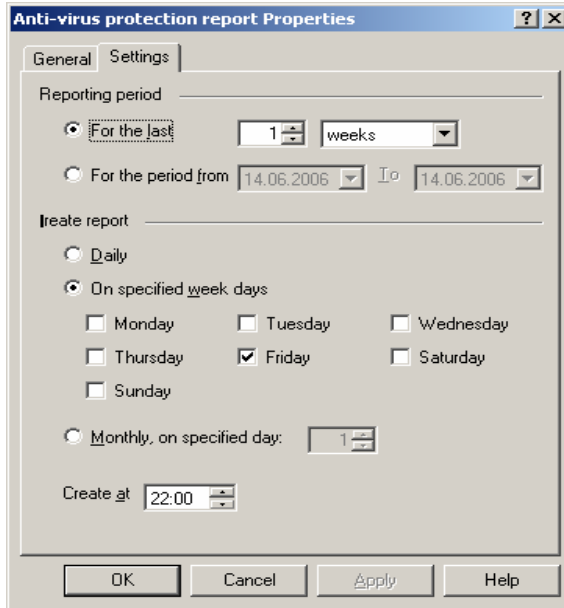


Figure 36. Report template.
The **Settings** tab

9.3. Viewing reports



In order to view a report using the file system:

1. Enter the folder where the logs are stored. By default, it is the Reports folder located on the server in the application's data folder.
2. Select and open an html file with the name corresponding to the date and time of report creation in the following format **<DD.MM.YYYY_HH-MM-SS>**.

As a result the system default browser will be loaded. The required report about the anti-virus scan results will be displayed in the main window of the browser (see Figure 37). Immediately after loading, the report displays general results of the scan. The reporting period will be specified in the heading.

Kaspersky Anti-Virus 5.5 for Check Point™ Firewall-1®
Anti-virus scanning report for period: from 28.06.2006 17:38:54
to 05.07.2006 17:38:54

- General scan results
- Sources of infected objects
- Malicious object types
- Scanning performance

General scanning results

Number of objects scanned

	HTTP	FTP	SMTP	Total
Not infected	0	0	0	0
Cured	0	0	0	0
Infected	0	0	0	0
Suspicious	0	0	0	0
Corrupted/Protected	0	0	0	0
Total	0	0	0	0

Total amount of objects scanned, bytes

	HTTP	FTP	SMTP	Total
Not infected	0	0	0	0
Cured	0	0	0	0
Infected	0	0	0	0
Suspicious	0	0	0	0
Corrupted/Protected	0	0	0	0
Total	0	0	0	0

Figure 37. Viewing reports General scan results

The left frame of the report contains the list of the report's sections (table of contents); the heading and the content of the selected section are displayed in the right frame.

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



In order to view a report using the Management Console:

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 33).

3. Open the shortcut menu and use the **View report** or the analogous command under the **Action** menu.
4. As the result the last report created based on the selected template will be displayed. Reports are viewed using the default system browser.
5. If no reports were created based on the selected template an information message will be displayed (see Figure 38). In this case create a report and try to view it again using the console.

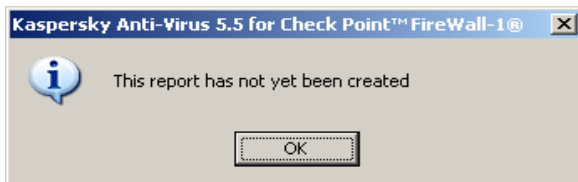


Figure 38. Notification that no report based on the selected template were created

CHAPTER 10. APPLICATION EVENT LOG

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

The degree of the completeness of the information entered into the logs depends on the diagnostics levels selected in the application's settings (see section 10.1, page 99).

Events registered in the Windows application log can be viewed using standard Microsoft Windows tool Events viewer. For Kaspersky Anti-Virus the Source column contains line Kav4Cpf1.



In order to ensure that the events registered in the logs are displayed correctly, you must select a language that matches the language version of the Anti-Virus in the Language for non-Unicode programs section of the Regional and Language Options standard Microsoft Windows tool.

The application provides for two types of logs: the application operation log and the anti-virus scan results log.

Depending on the type, the log files have the following naming convention:

Kav4Cpf1_DATE.log – Kaspersky Anti-Virus log that contains information about the application's operation provided with the extent of detail that was specified by the date the information was logged. The *DATE* part in the filename shall be replaced with the date the log was created on in the **YYYYMMDD** format. For example, *Kav4Cpf1_20050410.log*.

If, by the time when new data must be entered into the log, the log is not accessible for writing, for example, if it is opened for editing by the administrator, Kaspersky Anti-Virus will create a new file with a postfix added to the filename. For example, *Kav4Cpf1_20050410_1.log*.

virusDATE.log – Kaspersky Anti-Virus log that includes information about the results of the anti-virus scan.

By default, a new log is created on a monthly basis. The file storage period is not restricted, but the number of files of the same type is limited (maximum three by default). If this maximum allowable number is exceeded at the time a new log file is created, the oldest log file of the same format will be deleted. The frequency for creating new log files and the maximum number of logs can be modified (see section 10.2, page 101).

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

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

By default, logs are stored in the Logs folder. This folder is created in the application's data folder during the installation of the Security Server component. Any other folder selected by the administrator can be used to store logs (see section 10.2, page 101).

Kaspersky Anti-Virus logs' settings can be modified in the Diagnostics tab of the application settings window General parameters (see Figure 39). This window is accessible via the General parameters link.

10.1. Configuring the diagnostics level

For each component of the program, there is a set of diagnostic messages that will be entered into the logs. The information volume and the extent of detail will be determined by the diagnostics level selected for the particular group of messages.

For following diagnostics level are provided:

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



In order to configure the diagnostics level,

1. Select the node corresponding to the required server in the console tree and follow the General settings link in the results pane.
2. Go to the Diagnostics tab in the General settings window that will open (see Figure 39).

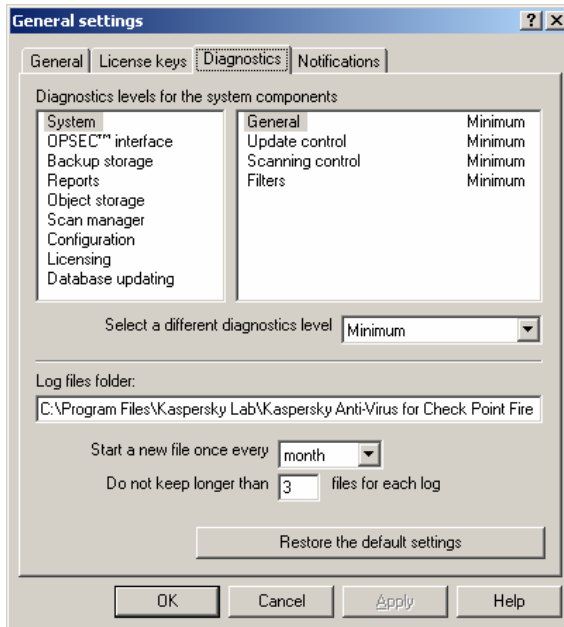


Figure 39. The **Diagnostics** tab

- The **Diagnostics level for system components** section located in the tab contains a table. The left part of the table contains the list of all components included into the structure of the program. The right section of the table displays the groups of the diagnostic messages for the selected component and the diagnostics level for each of the groups.



Only diagnostic messages of group **Scan Results** for the **Filters** component will be entered into the results log.

Messages of this group are not registered in the application's operation log.

Select the component in the left part of the table and then select the required group of diagnostic messages in the right part of the table. Select the desired diagnostics level using the drop-down list.

Specify the required diagnostics level for each program component. You can select the diagnostics level for all or several components at the same time selecting components using the <Shift> and <Ctrl+Shift> keys or using the mouse.

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

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

10.2. Configuring log files settings



In order to configure logs files settings,

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 parameters window that will open (see Figure 39).
3. Enter the path to the new folder in the Log files folder field.
4. Select the frequency for creating logs in the **Start a new file once** field by selecting the required value from the drop-down list.
5. Specify the number of log files of the same format that can be stored by the application. In order to do this, specify the desired value in the Store not more than [NN] files for each log field.
6. After you are done with the settings, press the Apply or the OK button.

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

CHAPTER 11. LICENSE KEYS

When you purchase Kaspersky Anti-Virus, you enter into a license agreement with Kaspersky Lab Ltd. Based on this agreement you are entitled to use this software during the specified period of time to protect the mail traffic received and requested from the number of workstations specified in the license.

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

- the anti-virus functionality of the application;
- *hourly* anti-virus database update;
- application updates (patches);
- 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 application verifies the validity of the license agreement by the **license key** that is an integral part of any Kaspersky Lab's product.



Without the license key the management services will be the only Kaspersky Anti-Virus functionality available to you.

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

- the functionality of the application will be restricted;
- a record about the violation detected will be entered into the events logs;
- information about the violation of the license agreement terms will be sent to the Check Point™ Firewall-1® application. If the application has the notification settings configured, a corresponding notification will be issued using Check Point™ Firewall-1® functionality.

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

A warning message will be issued by a Check Point™ Firewall-1® utility two weeks prior to the license expiration date. This message contains information

about the expiration date of the currently installed license key. Notification period can be changed (see section 11.3 on page 107).

Kaspersky Anti-Virus settings also provide for a possibility to configure notifications of the forthcoming expiration of the license and restrictions of the application's functionality (see Chapter 12 on page 110).

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



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



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

1. Contact the dealer you originally purchased the product from and buy a new license key for the use of Kaspersky Anti-Virus 5.5 for Check Point™ Firewall-1®.

or:

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

2. Install the license key (see section 11.4, page 107).



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

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

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

11.1. License information



In order to view the license:

1. Select the node corresponding to the required server in the console tree and follow the General settings link in the results pane.
2. Go to the General tab in the General parameters window that will open (see Figure 40).

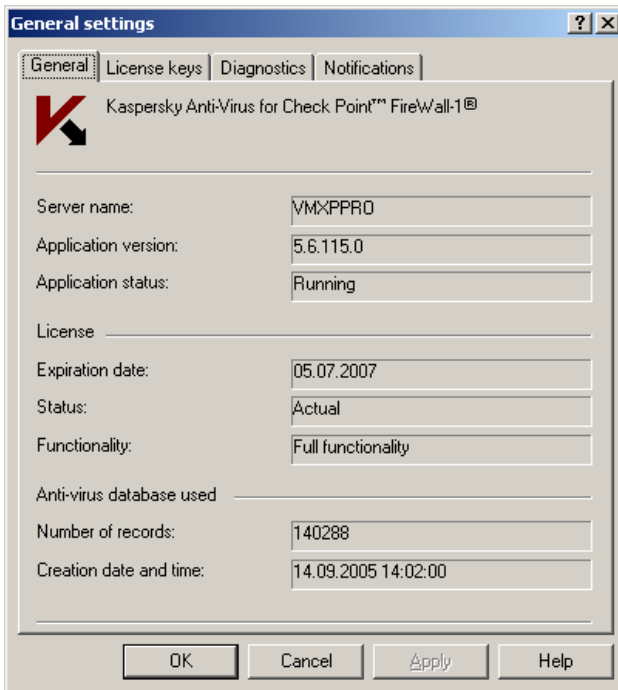


Figure 40. Viewing license information

The tab contains the following information:

- the name of the computer on which the Kaspersky Anti-Virus Security Server component is installed;
- the number of the application version installed;
- the current status of the Server Security component;

- license expiry date:
- the status of the current license key.
- application functionality available based on the current license key:
 - **All functions.** The application operates as provided for in the license agreement.
 - **Updating function is not available.** The anti-virus database updating feature is not available. The application performs the anti-virus scan and disinfects infected objects found based on the outdated version of the anti-virus database. Your license may be expired.
 - **Management services only.** In this case, only management services used to configure the application settings, particularly, license key installation will be available. This may be caused by exceeding the license restriction on the number of protected workstations or by the expiration of the trial license key.
 - **Update only.** Only anti-virus database updating feature is available. The anti-virus database may have been corrupted, therefore the anti-virus scan cannot be performed.
- information about the anti-virus database used by the application.

11.2. License key details



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

1. Select the node corresponding to the required server in the console tree and follow the [General settings](#) link in the results pane.
2. Go to the **General** tab in the **General settings** window that will open (see Figure 41).

This tab contains detailed information about the current and the backup license keys installed and about the license-related notifications settings.

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

- Status.

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

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

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

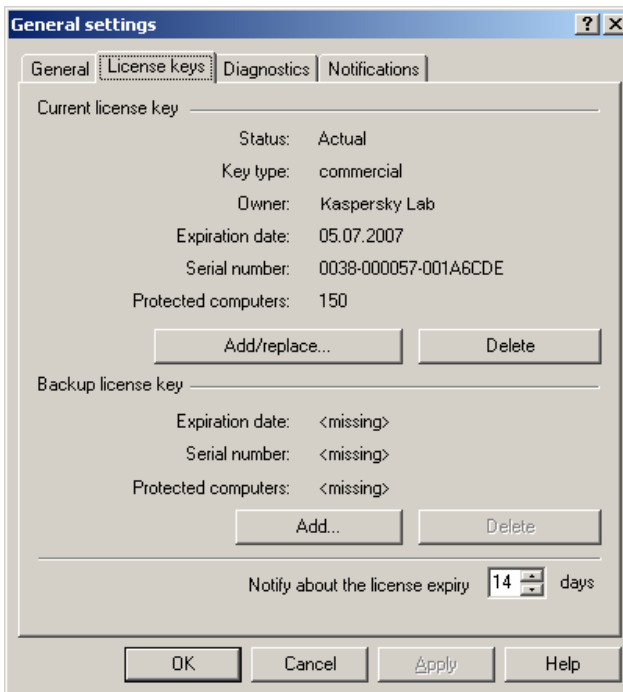


Figure 41. Viewing license key details
Configuring the license-related notifications settings

11.3. License-related notifications

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

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

- the current license key expires in several days;
- the license key has expired;
- the current license key was found in the black list;

A corresponding entry will be registered in the application log and the information will be sent to the Check Point™ Firewall-1® application.

If the Check Point™ Firewall-1® application has the notification settings configured, a corresponding notification will be issued using Check Point™ Firewall-1® functionality. There is also a possibility to configure notifications about the forthcoming license expiration in the Anti-Virus settings (see Chapter 12 on page 110).

By default a notification is issued 14 days prior to the license expiration date. You can configure the notification to be issued at an earlier or a later date.



In order to a configure license expiration notification period,

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 41).

In the **Notify about license expiration () before** field specify the number of days prior to the license key expiration you want the license-relation notification to be issued.

3. Press the **Apply** or the **OK** button.

11.4. Installing the license key

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



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

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

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



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

1. Select the node corresponding to the required server in the console tree and follow the General settings link in the results pane.
2. Go to the License keys tab in the General settings window that will open (see Figure 41).
3. On the License keys tab:
 - if you are installing or replacing the current license key, press the **Add/Replace button** in the **Current license key** section.
 - if you are installing or replacing the backup license key, press the **Add button** in the **Current license key** section.
4. Specify the license key file (*.key) to be installed in the file select dialog box that will open.



After the trial key expires a second trial key cannot be installed.

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

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

11.5. Removing a license key



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



In order to remove a license key,

1. Select the node corresponding to the required server in the console tree and follow the General settings link in the results pane.
2. Go to the License keys tab in the General settings window that will open (see Figure 41).
3. On the License keys tab:
 - if you are removing the backup license key, press the **Remove** button in the **Backup license key** section.
 - if you are removing the current license key, press the **Remove** button in the **Current license key** section.
4. Confirm the removal of the license key in the warning message that will be displayed on your screen.

As a result, information in the fields of the corresponding sections will be updated.
5. Close the General **settings** window using the **Apply** or the **OK** button.

CHAPTER 12. NOTIFICATIONS

Notifications about events registered in the operation of the Kaspersky Anti-Virus application can be configured by the use of the in-built notification feature of Check Point™ Firewall-1®. For this the following features must be configured:

- Settings of interaction of the Security Server with Check Point™ Firewall-1® via ELA protocol (see section 5.5 on page 39). These settings are available in the **Advanced** tab of the **OPSEC™ settings** window (see Figure 12).
- Check Point™ Firewall-1® notifications about events of Kaspersky Anti-Virus.

Check Point™ Firewall-1® can issue notifications about the following events of Kaspersky Anti-Virus:

- **Updating the anti-virus database** (successful or resulting in an error).
- **Forthcoming expiration of the license** (when the time of the notification about the license expiration is reached (see section 11.3 on page 107).
- **Change of the application status** (starting and stopping of the Security server, restriction of the application functionality at the expiration of the license, restoration of the functionality after the license is renewed).

Additionally, Kaspersky Anti-Virus allows the possibility to automatically launch applications specified by the administrator on the Security Server when certain types of events are registered during the operation of the application.

You can assign an external application or a script file to be launched to the following types of events:

- **Anti-virus object scan:** detection of an infected, suspicious, protected or corrupted object (no notification will be issued in case of a detection of clean objects).
- **Updating the anti-virus database:** after an update of the anti-virus database irrespective of the result of such update (success or error).
- **Report creation:** after creation of a report based on a template (whether successful or resulting in an error).
- **Forthcoming expiration of the license:** when the license expiration notification period is approaching. By default this period is 14 days after the expiration of the license and it can be changed (see section 11.3 on page 107). You can review the value specified for this setting on the **License keys** tab in the **General settings** window (see Figure 41).
- **Change of the application status:** for the following changes of the application status: starting and stopping of the Security Server, restriction of

the application functionality at the expiration of the license, restoration of the functionality after the license is renewed.



In order to configure notifications made via Kaspersky Anti-Virus:

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 **Notifications** tab in the **General settings** window that will open (see Figure 42).
3. On this tab, in the field corresponding to the required event specify the full path to the module that will be launched on the Security Server when a specific event is occurred. If required, enter also the required command line keys.



If the path to the file contains space symbols, the entire path shall be provided in double quotes. The command line keys shall be specified after the closing quotes.

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

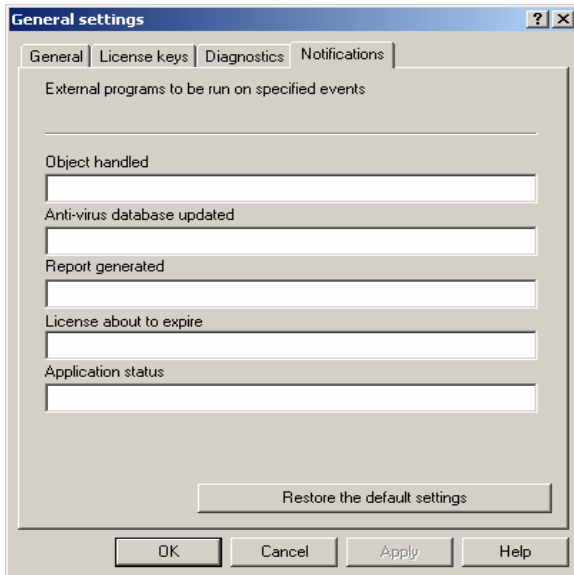


Figure 42. Configuring notifications via Kaspersky Anti-Virus

An example of a program to be launched is a script file **alert.js** included in the application distribution package. After the installation of the Security Server file **alert.js** is saved into the component installation folder in the service folder **Scripts**. You can use this file in its original form (having configured the distribution settings), enter changes into this file or write and use your own script files or other executable modules to issue notifications about events.

As the result of execution of **alert.js** an e-mail message will be sent to the address specified by the administrator; the message will contain the following information about the event:

- description of the events - in the body of the message;
- event type - added to the message header;
- message for event **Report creation** will contain an attached report file (if the report was successfully created).

Address of the sender and the recipient, address and number of the SMTP server port and the message subject are specified in the script variables. These settings must be configured before **alert.js** file is used in order to ensure its correct execution.



*In order to assign certain values to the variables of script file **alert.js**:*

1. Open **alert.js** for editing.
2. Specify values for the following variables at the beginning of the file:
 - `g_smtpServer = "<SMTP-server_address>";`
IP address or a different network address of the computer can be used as the address.
 - `g_smtpPort = 25;`
Number of the communication port of the SMTP server. By default port 25 will be used.
 - `g_mailFrom = "<notification_sender_e-mail_address>";`
 - `g_mailTo = "<notification_recipient_e-mail_address>";`
You can enter several addresses separated by commas.
 - `g_mailSubject = "<message_subject>";`
The message subject can be specified at the user's discretion.
3. Save changes you have made to the file.

Kaspersky Anti-Virus transfers information about events and [applications launched] using the Microsoft Windows environment variables. Each type of

events has its own set of variables, the complete list of variables is provided in Appendix A on page 118.

CHAPTER 13. FREQUENTLY ASKED QUESTIONS

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



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

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



Question: Why does Kaspersky Anti-Virus cause a certain decrease in my computer performance and impose a considerable load on the processor?

The process of virus detection is a computational (mathematical) task that involves analysis of structures, checksum calculation and mathematical data transformation. Therefore, the main resource consumed by the anti-virus software is the processor time. Moreover, each new virus added into the anti-virus database adds to the overall scanning time.

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

Kaspersky Anti-Virus allows experienced users to accelerate the anti-virus scanning process by the way of disabling scanning of various file types. However, note that this lowers the security level.

Kaspersky Anti-Virus can detect over 700 formats of archived and compressed files. This is very important for the anti-virus security as each of detectable file formats may contain executable malicious code.



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

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

If you are still undecided whether or not to purchase Kaspersky Anti-Virus, we can provide you with a temporary key file (trial key), which will

only work either for two weeks or for a month. When this period expires, the key will be blocked.



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

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

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



Question: My Anti-Virus does not work.

What should I do?

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

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

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

1. In the subject of your message, indicate your operating system, the name of the Kaspersky Lab's product you are using and the problem you encountered. For example, MS Windows 2000 Pro, SP4, Kaspersky Anti-Virus 5.5 for **Check Point™ Firewall-1®**, anti-virus database update cannot be performed.
2. Use plain text format for your message.
3. At the beginning of your message, indicate:
 - the version of your operating system and service packs installed;
 - Check Point™ Firewall-1® version and service packs installed;
 - the version of your Kaspersky Anti-Virus copy and the number of your license.
4. Briefly, but clearly describe the problem. Bear in mind that the support specialists have no previous knowledge of your problem

- and can only help you if they fully understand it and have been able to reproduce it.
5. Forward to the technical support service the following data packed in one archive:
 - the current application events logs produced with the **Debug** diagnostic level for each application module;
 - your license key.
 6. Make sure that you have specified the following conditions in your message:
 - your processor is too old or very new or you have several processors;
 - RAM less than 256 MB or in excess of 2 GB.
 7. Indicate the approximate daily mail traffic and load peaks if applicable.



Question: Why daily updates are required?

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

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

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



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

All anti-virus databases are supplied with a unique signature verified by Kaspersky Anti-Virus when the program 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, Kaspersky Anti-Virus 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 MS 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:

The network settings should always be configured in the update service settings.

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

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

APPENDIX A. NOTIFICATION SETTINGS

This section contains description of settings passed to the application launched in order to issue notification about a Kaspersky Anti-Virus event (see Chapter 12 on page 110).

Settings are passed using Microsoft Windows environment variables. Provided below is the list of events that cause the application to be launched and the list of variables being passed for each event.

Event description	Settings passed
Anti-virus object scan	
Anti-virus object scan completed	<pre>kav4cpfl_event = "object" kav4cpfl_scan = "cured" "infected" "suspicious" "other" "cured" - disinfected "infected" - infected "suspicious" - suspicious "other" - protected/corrupted kav4cpfl_id = <internal_object_id> (number) kav4cpfl_time = <scan_completion_date_and_time> kav4cpfl_object = <object_URL > or <mail_id> kav4cpfl_size = <object_size_in_bytes> kav4cpfl_protocol = "HTTP" "FTP" "SMTP" kav4cpfl_source = <object_source_server_IP_address> kav4cpfl_destination = <object_recipient_server_IP_address> kav4cpfl_subject = <message_subject> (for SMTP only) kav4cpfl_from = <message_sender> (for SMTP only)</pre>

Event description	Settings passed
	kav4cpfl_to = <message_recipient> (for SMTP only) kav4cpfl_virus = <virus_name> or <empty> kav4cpfl_error = <er- ror_description> or <empty>
Object anti-virus scan notifications queue overflow	kav4cpfl_event = "overflow" kav4cpfl_number = <num- ber_of_missed_notifications> kav4cpfl_time = <event_occurrence_time>
Anti-virus database updating	
Anti-virus database update completed successfully	kav4cpfl_event = "update" kav4cpfl_bases = <date_and_time_of_creation_of_ant i- vi- rus_database_used_by_application> kav4cpfl_error = <empty> kav4cpfl_time = <event_occurrence_time>
Anti-virus database update resulted in an error Anti-virus database was rolled back to the previous version	kav4cpfl_event = "update" kav4cpfl_bases = <date_and_time_of_creation_of_ant i- vi- rus_database_used_by_application> kav4cpfl_error = <er- ror_description> kav4cpfl_time = <event_occurrence_time>
Anti-virus database update resulted in an error No current anti-virus database exists.	kav4cpfl_event = "update" kav4cpfl_bases = <empty> kav4cpfl_error = <er- ror_description> kav4cpfl_time = <event_occurrence_time>

Event description	Settings passed
Report creation	
Report created successfully.	<pre>kav4cpfl_event = "report" kav4cpfl_title = <report_name> (specified in the report settings) kav4cpfl_path = <path_to_report_file> kav4cpfl_error = <empty> kav4cpfl_time = <event_occurrence_time></pre>
Error creating report. Report has not been created	<pre>kav4cpfl_event = "report" kav4cpfl_title = <report_name> (specified in the report settings) kav4cpfl_path = <empty> kav4cpfl_error = <error_description> kav4cpfl_time = <event_occurrence_time></pre>
Forthcoming expiration of the license	
License expiration notification period specified in the Kaspersky Anti-Virus settings has been reached	<pre>kav4cpfl_event = "license" kav4cpfl_time = <event_occurrence_time> kav4cpfl_days = <number_of_days_left_before_license_expiration></pre>
Change of the application status	
<p>Kaspersky Anti-Virus operates in full mode, as provided for in the license agreement.</p> <p>Event occurs at the Security Server startup if the application functionality is not restricted and when the application functionality</p>	<pre>kav4cpfl_event = "status" kav4cpfl_error = <empty> kav4cpfl_time = <event_occurrence_time></pre>

Event description	Settings passed
is restored as the result of the license renewal.	
<p>Only management functionality is available.</p> <p>The event occurs in case of a violation of the license agreement, trial key expiration or anti-virus database corruption.</p>	<pre>kav4cpfl_event = "status" kav4cpfl_error = "disabled" kav4cpfl_time = <event_occurrence_time></pre>
<p>Security Server component not started or not initialized</p>	<pre>kav4cpfl_event = "status" kav4cpfl_error = "failed" kav4cpfl_time = <event_occurrence_time></pre>
<p>Security Server component stopped (for example, because the computer turned off).</p>	<pre>kav4cpfl_event = "status" kav4cpfl_error = "shutdown" kav4cpfl_time = <event_occurrence_time></pre>

APPENDIX B. GLOSSARY

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

A

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

Anti-virus database – database, created by Kaspersky Lab's specialists, that contains 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.

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

Application data folder – the folder in which service folder and databases required for the application to operate are stored. If you change the data folder, all information stored in this folder must be saved to the new location.

B

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

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

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

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

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

C

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

D

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

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

I

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

K

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

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

L

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

License period – a period of time for which you are granted the right to use all features of Kaspersky Anti-Virus. The license period is determined by the license key; a standard license period is one year after the license key is installed. After the license expires, the application functionality will be restricted.

M

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

Monitored object - any file, moved over HTTP, FTP or SMTP protocol through the firewall.

N

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

R

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

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

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

S

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**.

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

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 not known yet by Kaspersky Lab.

T

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

V

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.

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.

APPENDIX C. KASPERSKY LAB

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

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

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

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

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

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

C.1. Other Kaspersky Lab Products

Kaspersky Anti-Virus® Personal

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

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

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

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

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

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

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

Kaspersky Anti-Virus® Personal Pro

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

unique second-generation heuristic analyzer efficiently detects unknown viruses. A simple and convenient interface allows users to configure the program quickly making work with it easier than ever.

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

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

Kaspersky® Anti-Hacker

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

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

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

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

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

Kaspersky® Personal Security Suite

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

Kaspersky Personal Security Suite has the following features:

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

Kaspersky Lab News Agent

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

The product performs the following functions:

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

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

Kaspersky® OnLine Scanner

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

- Exclude archives and e-mail databases from scanning.
- Select standard/extended anti-virus databases for scanning.

- Save a report on the scanning results in txt or html formats.

Kaspersky® OnLine Scanner Pro

This program is a subscription service available to visitors of the corporate website allowing to perform efficient anti-virus scan of your computer and disinfection of infected files online. Kaspersky OnLine Scanner Pro is executed in the web browser using the Microsoft ActiveX® technology. While scanning the user can:

- exclude archives and mail databases from the scan scope;
- select standard / extended anti-virus database to be used for scanning;
- save reports with the scan results in txt and html format.

Kaspersky Anti-Virus® 6.0

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

The program provides for complex anti-virus checks including:

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

Proactive protection offers the following features:

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

- **System restoration** after malicious spyware influence accomplished due to recording of all changes in the registry and computer file system and an opportunity to perform their roll-back at user's discretion.

Kaspersky® Internet Security 6.0

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

The anti-virus protection feature includes:

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

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

Kaspersky® Internet Security 6.0 **registers attempts to scan the ports of your computer**, which frequently precede network attacks, and successfully defends against typical hacker attacks. The program uses **defined rules as a basis** for control over all network transactions tracking all **incoming and outgoing data packets**. **Stealth mode** (owing to the SmartStealth™ technology) **prevents computer detection from outside**. When you switch into that mode, the system will block all network activity except for a few transactions allowed in user-defined rules.

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

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

Kaspersky® Security for PDA

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

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

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

Kaspersky Anti-Virus® Business Optimal

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

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

- *Workstations* running Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation and Linux.
- *File servers* running Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Microsoft Windows 2003 Server, Novell Netware, FreeBSD and OpenBSD, Linux, Samba Servers.
- *E-mail systems* including Microsoft Exchange 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail, and Qmail.
- *Internet gateways*: Check Point™ Firewall –1® ; Microsoft ISA Server 2000 Standard Edition.

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

¹ Depending on the type of distribution kit.

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

Kaspersky® Corporate Suite

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

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

- *Workstations* running Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation and Linux;
- *File servers* running Microsoft Windows NT 4.0 Server, Microsoft Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD, Linux and Samba Servers;
- *E-mail systems*, including Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim and Qmail;
- *Internet gateways: Check Point™ FireWall-1®*; Microsoft ISA Server 2004 Enterprise Edition;
- *Hand-held computers* (PDAs), running Windows CE and Palm OS, and also smartphones running Microsoft Windows Mobile 2003 for Smartphone and Microsoft Smartphone 2002.

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

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

Kaspersky® Anti-Spam

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

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

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

Kaspersky® SMTP Gateway

Kaspersky® SMTP-Gateway for Linux/Unix is a solution designed for anti-virus processing of e-mail transmitted via SMTP. The application contains a number of additional tools for filtering e-mail traffic by name and MIME type of attachments and a number of tools reducing the load on the mail system and preventing hacker attacks. DNS Black List support provides protection against e-mails coming from servers entered in these lists as sources distributing unwanted e-mail (spam).

Kaspersky Security® for Microsoft Exchange 2003

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

Kaspersky® Mail Gateway

Kaspersky Mail Gateway is a comprehensive solution that provides complete protection for users of mail systems. This application installed between the corporate network and the Internet scans all components of e-mail messages for the presence of viruses and other malware (Spyware, Adware, etc.) and performs centralized anti-spam filtration of e-mail stream. This solution also includes some additional mail traffic filtration features.

C.2. Contact Us

If you have any questions, comments, or suggestions, please refer them to one of our distributors or directly to Kaspersky Lab. We will be glad to assist you in

any matters related to our product by phone or via email. All of your recommendations and suggestions will be thoroughly reviewed and considered.

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

© Partial copyright for information relating to Check Point products 2005 Check Point Software Technologies Ltd. All rights reserved. Check Point, Application Intelligence, the Check Point logo, FireWall-1, OPSEC and SmartDashborard are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The Check Point products described in this document is protected by U.S. Patent No. 5,606,668, 5,835,726, 6,496,935, 6,873,988 and 6,850,943 and may be protected by other U.S. patents, foreign patents or pending applications.

APPENDIX D. LICENSE AGREEMENT

End User License Agreement

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

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

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

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

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

THIS CASE, KASPERSKY LAB WILL NOT BE HELD BY THE PARTNER'S CLAUSES.

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

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

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

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

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

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

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

steps to achieve interoperability, provided that you only reverse engineer or decompile the Software to the extent permitted by law.

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

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

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

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

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

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

described herein. Upon any termination or expiration of this Agreement, you must immediately destroy all copies of the Software and the Documentation. You may terminate this Agreement at any point by destroying all copies of the Software and the Documentation.

3. Support.

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

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

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

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

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

(iv) "Support Services" means:

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

(b) Free software updates, including version upgrades;

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

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

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

5. Confidentiality. You agree that the Software and the Documentation, including the specific design and structure of individual programs and the Key Identification File, constitute confidential proprietary information of Kaspersky Lab. You shall not disclose, provide, or otherwise make available such confidential information in any form to any third party without the prior written consent of Kaspersky Lab.

You shall implement reasonable security measures to protect such confidential information, but without limitation to the foregoing shall use best endeavours to maintain the security of the Key Identification File.

6. Limited Warranty.

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

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

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

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

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

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

7. Limitation of Liability.

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

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

(whether such losses or damage were foreseen, foreseeable, known or otherwise):

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

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

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

(iii) The liability of Kaspersky Lab for Misrepresentation as a fundamental matter, including a matter fundamental to the maker's ability to perform its obligations under this Agreement, shall be subject to the limitation of liability set out in paragraph 7(iii).