

KASPERSKY LAB

Kaspersky Anti-Virus® 5.5 for Linux and FreeBSD
Workstation and File Server

ADMINISTRATOR'S GUIDE

KASPERSKY ANTI-VIRUS[®] 5.5 FOR
LINUX AND FREEBSD WORKSTATION AND FILE SERVER

Administrator's Guide

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

Revision date: September, 2006

Table of Contents

CHAPTER 1. INTRODUCTION	6
1.1. Computer viruses and malware	6
1.2. Purpose and major functionality of Kaspersky Anti-Virus	7
1.3. What's new in version 5.5?	8
1.4. Licensing procedure	9
1.5. Hardware and software system requirements	9
1.6. Distribution kit	11
1.7. Services for registered users	11
1.8. Conventions used in this document.....	12
CHAPTER 2. APPLICATION ALGORITHM.....	14
CHAPTER 3. INSTALLING KASPERSKY ANTI-VIRUS	16
3.1. Installing the application on a computer running Linux	16
3.2. Installing the application on a computer running FreeBSD.....	17
3.3. Installation procedure	17
3.4. Updating the application to version 5.5.....	18
3.5. Installing the license key.....	18
3.6. Locating the application files	19
3.7. Completing the setup	22
CHAPTER 4. POST-INSTALLATION APPLICATION CONFIGURATION	23
4.1. Default application configuration	23
4.2. Installing the anti-virus database.....	24
4.3. Configuration for using Kaspersky Anti-Virus together with Webmin.....	24
CHAPTER 5. USING KASPERSKY ANTI-VIRUS	26
5.1. Updating the anti-virus database	26
5.1.1. New capabilities of the updating component	27
5.1.2. Automatically updating the anti-virus database	28
5.1.3. On-demand updating of the anti-virus database	30
5.1.4. Creating a network folder for storing and downloading of the anti-virus database.....	31

5.2. Anti-virus protection of file systems.....	32
5.2.1. Scan scope	33
5.2.2. Objects scan and disinfection mode	34
5.2.3. Actions to be performed with objects	34
5.2.4. On-demand scan of an individual folder	36
5.2.5. Scheduled scan	36
5.2.6. Additional capabilities: using script files	37
5.2.6.1. Disinfection of infected objects in the archive	37
5.2.6.2. Sending notifications to the administrator	38
5.3. Real-time anti-virus protection	38
5.4. Managing license keys.....	39
5.4.1. Viewing license key details.....	40
5.4.2. Renewing your license	41
CHAPTER 6. ADDITIONAL SETTINGS.....	43
6.1. Optimization of Kaspersky Anti-Virus operation	43
6.2. Moving objects into the quarantine folder.....	45
6.3. Object backup copying mode	46
6.4. Localization of the date and time format.....	47
6.5. Kaspersky Anti-Virus report generation settings	47
CHAPTER 7. UNINSTALLING KASPERSKY ANTI-VIRUS.....	50
CHAPTER 8. VERIFYING THE ANTI-VIRUS OPERATION.....	51
APPENDIX A. ADDITIONAL INFORMATION ABOUT THE APPLICATION	53
A.1. Kaspersky Anti-Virus configuration file.....	53
A.2. Command line modifiers for component kavscanner	60
A.3. Return codes of the kavscanner component	63
A.4. Command line modifiers for component kavmonitor	64
A.5. Command line modifiers for component licensemanager	64
A.6. Return codes of the licensemanager component.....	65
A.7. Command line modifiers for component keepup2date.....	66
A.8. Return codes of the keepup2date component.....	67
APPENDIX B. FREQUENTLY ASKED QUESTIONS	68
APPENDIX C. KASPERSKY LAB.....	74
C.1. Other Kaspersky Lab Products	75

C.2. Contact Us..... 83

APPENDIX D. LICENSE AGREEMENT 84

CHAPTER 1. INTRODUCTION

The constant growth in the number of computer users and new the 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.

Among the sources of malware penetrating users' computers the most dangerous are:

Internet

Global information network is the main source of distribution of all types of malware. As a rule, viruses and other malicious programs are located on popular internet websites disguising themselves as useful software or freeware. Malware can be located within numerous scripts that automatically run when a website is loaded in the user's browser.

E-mail messages

E-mail messages delivered to the user's mailbox and stored in the e-mail databases may contain viruses. Malware can be located either in the attachments to messages or in the body of a message. As a rule, infected e-mail messages contain viruses or mail worms. When you open an e-mail message or save an attached file to your hard drive, you may infect data stored in your computer.

Software vulnerabilities

In most cases hackers' attacks are attempted using "software holes". Such vulnerabilities allow hackers to obtain remote access to your computer and, therefore, to your data, your LAN resources and other sources of information.

In the Unix-based systems viruses are far less common compared, for example, to the Windows Operating System due to the peculiarities of the two platforms. However, this does not mean that Unix users encounter no threat. Provided below is a detailed description of malware types.

1.1. Computer viruses and malware

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 or Trojans** – 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; they are unable to sneak independently into computers and therefore are distributed by impostors disguised as some "useful" software. However, Trojans may inflict far greater damages compared to a regular virus attack.

Recently, *worms and Trojans* have become the most widespread type of malware in the Unix-based systems.



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 and major functionality of Kaspersky Anti-Virus

Kaspersky Anti-virus® for Linux and FreeBSD Workstation and File Server (hereinafter *Kaspersky Anti-Virus, the application*) is designed to provide protection of file servers and workstations running Linux or FreeBSD operating systems.

Kaspersky Anti-Virus for Linux and FreeBSD allows to:

- *Ensure real-time protection of the file system against malicious code:* intercept and analyze attempts to access files, disinfect and delete infected objects.
- *Scan objects on-demand:* search infected and suspicious files (including files in the specified scan scopes); analyze files; disinfect or delete infected objects.
- *Quarantine suspicious and corrupted objects:* save suspicious files in the quarantine folder.
- Create a copy of the infected object in the backup storage before attempting to disinfect or deleting such object for the possible restoration of the object if it contains valuable information.
- *Update the anti-virus database;* the database is updated from the Kaspersky Lab's updates servers. The user can also configure the application so that the database is updated from the local folder.
- *Control and configure Kaspersky Anti-Virus* using the application configuration file and web-based interface Webmin.

1.3. What's new in version 5.5?

The following changes have been introduced to **Kaspersky Anti-Virus 5.5 for Linux an FreeBSD Workstation and File Server** as compared to version 5.0:

- A new component *kavmonitor* that ensures anti-virus protection of files in the real-time mode has been added to the application.
- New technologies for receiving updates of the anti-virus database and application modules have been introduced, including integrity check and check of the usability of the downloaded database. This helps considerably save the network traffic.
- The ability to select the type of the anti-virus database to download (standard or extended database set) has been added. Using this option you can individually select the database set to be used by each individual component.
- The application installation and removal procedure have been simplified.
- Importing of the settings of the previous Anti-virus version (5.0) has been made available. This allows to considerably accelerate the process of creating an operational configuration.
- A possibility to create a backup storage to store copies of suspicious and infected objects before such objects are disinfecting or deleted. This helps

avoid the loss of the original data if the object is corrupted during the disinfection.

- In order to reduce the load on the processor when performing the anti-virus scan a database usage iChecker™ technology and double-level caching of scanned objects have been introduced.
- The ability to limit the number of objects scanned at a time in the background mode, which allows to optimize load on the computer has been added.
- The ability to generate lists of viruses detected has been added.
- The set of possible actions performed when objects of various statuses are detected has been extended.
- 64-bit platform support by the application has been implemented.
- On-demand anti-virus scan options have been enhanced.

1.4. Licensing procedure

Kaspersky Anti-Virus licensing policy imposes restrictions on the use of the application based on the usage period (as a rule, a one-year period since the date when the application was purchased).

1.5. Hardware and software system requirements

In order to run Kaspersky Anti-Virus the system must comply with the following software and hardware requirements:

- Hardware requirements:
 - Processor Intel Pentium® 133 MHz or higher;
 - 64 MB RAM.
 - 100 MB free hard drive space for installation of the application and storage of temporary files.
- Software requirements:
 - For 32-bit platform - one of the following operating systems:
 - RedHat Linux 9.0.

- RedHat Enterprise Linux Advanced Server 4 UPD3.
- RedHat Fedora Core 5.
- SUSE Linux Enterprise Server 9.0 SP3.
- Novell Linux Desktop 9.
- SUSE Linux Professional 10.1.
- Debian GNU/Linux version 3.1 R2.
- Mandriva 2006.
- FreeBSD version 4.11.
- Mandriva 2006 FreeBSD version 4.11.
- FreeBSD version 5.4.
- FreeBSD version 6.1.
- For 64-bit platform - one of the following operating systems:
 - RedHat Enterprise Linux Advanced Server 4 UPD3.
 - RedHat Fedora Core 5.
 - SUSE Linux Professional 10.1.
 - SLES 9 SP3.
- Webmin program (www.webmin.com) – for remote administration of Kaspersky Anti-Virus.
- Perl interpreter - version 5.0 or higher (www.perl.org).
- The *which* utility installed.
- Software compilation packages installed (gcc, binutils, glibc-devel, make, ld) and preinstalled operating system kernel code for using the *kavmonitor* component.



Please note that Kaspersky Anti-Virus does not support operation under SE Linux. The use of SE Linux may cause various warnings to appear in the application report system file.

1.6. 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 written on a special disk;
- A registration card (containing the serial number of the product);
- License Agreement.



Before you open the envelope with the CD make sure that you have carefully read the License Agreement.

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

License Agreement

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 (or floppy disks) must remain sealed.

By opening the sealed envelope containing the installation CD (or floppy disks) you accept all terms and conditions of the License Agreement.

1.7. Services for registered users

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

After purchasing your license, 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.

1.8. Conventions used in this document

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> 1. Step 1. 2. ...	Description of the successive user's steps and possible actions
 Task, example	Statement of a problem, example of the demonstration of the application's capabilities

Format feature	Meaning/Usage
 Solution	Implementation of the task
[modifier] – purpose of the modifier	Command line modifiers
Information messages and command line text	Text of configuration files, information messages and command line

CHAPTER 2. APPLICATION ALGORITHM

Before reviewing the functional capabilities of Kaspersky Anti-Virus, a detailed discussion of its internal architecture is required. This will help obtain a comprehensive understanding of the algorithm used in the Anti-Virus operation.

Kaspersky Anti-Virus includes:

- On-demand anti-virus scan component *kavscanner*;
- Real-time anti-virus scan component *kavmonitor*;
- Anti-virus database update module *keepup2date*;
- License key management utility *licensemanager*;
- *Remote administration module* used with Webmin application.

Provided below is a detailed discussion of the application operation algorithm based on an example of real-time protection (that is, using the *kavmonitor* component).

The operation procedure provides as follows:

1. When any application on your computer attempts to access an object of the file system (request to open, run or close a file) such call will be intercepted by the *kavmonitor* component kernel module and sent for anti-virus scanning.
2. The intercepted file will then be processed using a daemon application included into the *kavmonitor* component. The daemon scans the object for viruses and processes it based on the settings specified in the configuration file (including, but not limited to, disinfection using the anti-virus database if this option is selected).
3. After the file has been processed, the kernel module will send to *kavmonitor* the access code (allowed/prohibited) that defines the file status.
4. Based on the object's status the *kavmonitor* component allows access to the file or blocks it (in this case the application requesting access to such file will receive an error code (Access denied)).

The file status assigned during the scan (and processing) can be one of the following:

- **Clean** – the object is not infected.

- **Infected** – the object is infected.
- **Cured** – infected object has been successfully disinfected.
- **CureFailed** – could not disinfect infected object.
- **Warning** – object code resembles the code of a known virus.
- **Suspicion** – the object is suspected of being infected with an unknown virus.
- **Protected** – the object cannot be scanned because it is encrypted.
- **Corrupted** – the object is corrupted.
- **Error** – a system error occurred during the object scan.

Actions performed with the object of each particular status are defined by the configuration file settings (details see Appendix A on page 53).

CHAPTER 3. INSTALLING KASPERSKY ANTI-VIRUS

We recommend that you perform a system check as described below before installing Kaspersky Anti-Virus.

- Make sure that your system meets the hardware and software requirements for the installation of Kaspersky Anti-Virus (see section 1.5 on page 9). If any of the applications, for example Perl are not installed, we recommend that you install them, otherwise a part of the Anti-Virus functionality will not be available.
- Configure your internet connection.
- Log in as **root**.

3.1. Installing the application on a computer running Linux

Kaspersky Anti-Virus for computers running Linux OS is available in either of the two formats:

- **.rpm** – for systems that support RPM Package Manager;
- **.deb** – for Debian distribution packages.



In order to start the installation of Kaspersky Anti-Virus from a rpm package, enter the following in the command line:

```
# rpm -i <distribution_package_filename>
```



In order to start the installation of Kaspersky Anti-Virus from a deb-package, enter the following in the command line:

```
# dpkg -i <distribution_package_filename>
```

3.2. Installing the application on a computer running FreeBSD

For computers running FreeBSD operating system the distribution package of Kaspersky Anti-Virus is supplied in the form of a **pkg** package.



In order to start the installation of Kaspersky Anti-Virus from a pkg package, enter the following in the command line:

```
pkg_add <package_name>
```

3.3. Installation procedure

The application installation is performed *automatically* and includes the following steps:

1. Copying the distribution files to the computer.
2. Installing the license key.

If the license key is not installed, your copy of Kaspersky Anti-Virus will not work.

If the key is temporarily not available (for example, if you purchased the application online and the e-mail with the license key has not been yet received), you can install the license key later, before you start using the application (details about installation of the license key see section 5.4 on page 39).

3. Configuring the anti-virus database update component *keepup2date*;
4. Installing (updating) the anti-virus database.



Do not forget to install the anti-virus database before you start using the application. Scanning and processing files is impossible without the anti-virus database!

5. Installing the Webmin module.

The remote administration module will be installed only if *the default paths were used during the installation of the Webmin package*. After the installation of the module you will receive the corresponding recommendations regarding its configuration for the joint operation with the application.



When working under Linux operating system you must remember that during the update of the operating system kernel module you also must update the *kavmonitor* component's kernel module.

3.4. Updating the application to version 5.5

After the installation of the application the system will be inspected to check if any versions of Kaspersky Anti-Virus below 5.5 are installed on your computer.

If an application of a previous version has been detected, *some existing version's settings* will be imported into the configuration file of version 5.5.



The distribution package of the previous version of Kaspersky Anti-Virus will not be removed during the installation process. This must be done by the administrator.

A part of standard parameters of the configuration file (for example, path to the anti-virus database storage folder) *will not be exported* but will be defined during the installation.

Additionally, some changes have been introduced to the logics of some components' operation and some options have been added to version 5.5 as compared with version 5.0. Therefore we recommend that you verify whether the configuration file is filled out correctly before you start using the application.

3.5. Installing the license key

During this stage of the installation the current folder will be searched for a license key - a file (with *.key* extension) that is required for Kaspersky Anti-Virus to operate. This file allows access to the full functionality of the application. You cannot use Kaspersky Anti-Virus before you install the license key.

If the license key was found, corresponding information will be displayed on the screen and the installation process will proceed to the next stage - installation of the anti-virus database.

If the license key was not found, the administrator will be prompted to specify full path to it. If you do not have the key, you have to cancel the prompt to specify the path to it and proceed with the installation.

Once you receive the license key, install it immediately (details see section 5.4 on page 39).

3.6. Locating the application files



After the installation of Kaspersky Anti-Virus onto a workstation running Linux OS the distribution package files by default will be located as follows:

/etc/opt/kaspersky/ – a folder that contains Kaspersky Anti-Virus configuration file:

kav4ws.conf – configuration file.

/opt/kaspersky/kav4ws/ – main folder of Kaspersky Anti-Virus that contains:

/bin/ – a folder that contains executable files of all Kaspersky Anti-Virus components:

kav4ws-kavscanner – executable file of the anti-virus protection component;

kav4ws-keepup2date – executable file of the anti-virus database update component;

kav4ws-licensemanager – executable file of the license keys management component.

/lib/ – folder that stores auxiliary files of Kaspersky Anti-Virus.

/man/ – folder that stores man files.

/sbin/ – folder that stores auxiliary services of Kaspersky Anti-Virus:

kav4ws-kavmonitor – executable file of the anti-virus protection component.

/src/ – folder that stores the application's anti-virus kernel module.

/opt/kaspersky/kav4ws/share/contrib/kav4ws.wbm – plugin to Webmin application.

/opt/kaspersky/kav4ws/share/contrib/vox.sh – script *vox.sh*, used for disinfecting archives.

/opt/kaspersky/kav4ws/share/doc/LICENSE – license agreement.

/var/opt/kaspersky/kav4ws/bases – folder that stores the anti-virus database.

/var/opt/kaspersky/kav4ws/bases.backup – folder that stores the anti-virus database that was up-to-date before the last update.



In order to connect the help system of Kaspersky Anti-Virus (manual pages), assign value */opt/kaspersky/kav4ws/man* to the *MANPATH* environment variable.



After the installation of Kaspersky Anti-Virus onto a workstation running FreeBSD operating system the distribution package files by default will be located as follows:

`/usr/local/etc/kaspersky/` – folder that contains Kaspersky Anti-Virus configuration file:

`kav4ws.conf` – configuration file.

`/usr/local/bin/` – folder that contains executable files of all Kaspersky Anti-Virus components:

`kav4ws-kavscanner` – executable file of the anti-virus protection component;

`kav4ws-keepup2date` – executable file of the anti-virus database update component;

`kav4ws-licensemanager` – executable file of the license keys management component.

`/usr/local/sbin/` – folder that stores auxiliary services of Kaspersky Anti-Virus:

`kav4ws-kavmonitor` – executable file of the anti-virus protection component.

`/usr/local/man/` – folder that stores man files.

`/usr/local/src/kav4ws/` – folder that stores the application's anti-virus kernel module.

`/usr/local/share/kav4ws/contrib/kav4ws.wbm` – plugin to Webmin application.

`/usr/local/share/kav4ws/contrib/vox.sh` – script `vox.sh`, used for disinfecting archives.

`/usr/local/share/doc/kav4ws/LICENSE` – license agreement.

`/var/db/kaspersky/kav4ws/bases` – folder that stores the anti-virus database.

`/var/db/kaspersky/kav4ws/bases.backup` – folder that stores the anti-virus database that was up-to-date before the last update.



After the installation of Kaspersky Anti-Virus onto a server running Linux OS the distribution package files by default will be located as follows:

`/etc/opt/kaspersky/` – a folder that contains Kaspersky Anti-Virus configuration file:

`kav4fs.conf` – configuration file.

`/opt/kaspersky/kav4fs/` – main folder of Kaspersky Anti-Virus that contains:

`/bin/` – a folder that contains executable files of all Kaspersky Anti-Virus components:

`kav4fs-kavscanner` – executable file of the anti-virus protection component;

kav4fs-keepup2date – executable file of the anti-virus database update component;

kav4fs-licensemanager – executable file of the license keys management component.

/lib/ – folder that stores auxiliary files of Kaspersky Anti-Virus.

/man/ – folder that stores man files.

/sbin/ – folder that stores auxiliary services of Kaspersky Anti-Virus:

kav4ws-kavmonitor – executable file of the anti-virus protection component.

/src/ – folder that stores the application's anti-virus kernel module.

/opt/kaspersky/kav4fs/share/contrib/kav4fs.wbm – plugin to Webmin application.

/opt/kaspersky/kav4fs/share/contrib/vox.sh – script *vox.sh*, used for disinfecting archives.

/opt/kaspersky/kav4fs/share/doc/LICENSE – license agreement.

/var/opt/kaspersky/kav4fs/bases – folder that stores the anti-virus database.

/var/opt/kaspersky/kav4fs/bases.backup – folder that stores the anti-virus database that was up-to-date before the last update.



In order to connect the help system of Kaspersky Anti-Virus (manual pages), assign value */opt/kaspersky/kav4ws/man* to the *MANPATH* environment variable.



After the installation of Kaspersky Anti-Virus onto a server running FreeBSD operating system the distribution package files by default will be located as follows:

/usr/local/etc/kaspersky/ – folder that contains Kaspersky Anti-Virus configuration file:

kav4fs.conf – configuration file.

/usr/local/bin/ – folder that contains executable files of all Kaspersky Anti-Virus components:

kav4fs-kavscanner – executable file of the anti-virus protection component;

kav4fs-keepup2date – executable file of the anti-virus database update component;

kav4fs-licensemanager – executable file of the license keys management component.

/usr/local/sbin/ – folder that stores auxiliary services of Kaspersky Anti-Virus:

kav4ws-kavmonitor – executable file of the anti-virus protection component.

/usr/local/man/ – folder that stores man files.

/usr/local/src/kav4fs/ – folder that stores the application's anti-virus kernel module.

/usr/local/share/kav4fs/contrib/kav4fs.wbm – plugin to Webmin application.

/usr/local/share/kav4fs/contrib/vox.sh – script *vox.sh*, used for disinfecting archives.

/usr/local/share/doc/kav4fs/LICENSE – license agreement.

/var/db/kaspersky/kav4fs/bases – folder that stores the anti-virus database.

/var/db/kaspersky/kav4fs/bases.backup – folder that stores the anti-virus database that was up-to-date before the last update.



In the future for the purpose of our examples we will use the names of the components accepted for the installation on a server running Linux OS.

3.7. Completing the setup

If the installation process completed correctly a *corresponding message* will be displayed on the screen. The configuration file included into the application distribution kit contains all settings necessary to start using it.

However, there are certain settings that are not determined during the installation procedure. Yet, these settings help using Kaspersky Anti-Virus functionality in full-scale. Therefore, we recommend that you perform the post-installation configuration after the installation procedure has been completed (see Chapter 4 on page 23).

CHAPTER 4. POST- INSTALLATION APPLICATION CONFIGURATION

The installation process includes the analysis of the system on which Kaspersky Anti-Virus is installed and some settings of its configuration are determined automatically. Besides, some settings of the application's configuration file are configured by default to provide most convenient mode of the Anti-Virus operation (see section 4.2 on page 24).

Provided below is a discussion of the default Kaspersky Anti-Virus settings and the settings that *the administrator is recommended to select before using the application*.

4.1. Default application configuration

All settings that define the functioning of Kaspersky Anti-Virus are stored in the **kav4fs.conf** configuration file used by default.

Kaspersky Anti-Virus configuration is as follows:

- Once the operating system is started, Kaspersky Anti-Virus starts up automatically. The application intercepts all calls to the file system and analyzes them. Once infected, suspicious or corrupted objects have been detected, Kaspersky Anti-Virus prints out the corresponding messages into the **kavmonitor.log** report file.
- When an on-demand scan is started without using any additional command line modifiers, the anti-virus scan of the computer's folders and file systems will be performed starting with the current folder. Messages with the results of the scan will be printed to the screen and into the **kavscanner.log** report file.



Note that by default infected objects are not disinfected or quarantined!

4.2. Installing the anti-virus database

Kaspersky Anti-Virus performs anti-virus scanning and disinfects infected objects based on the records in the anti-virus database. Anti-virus database contains description of all currently known malicious programs and methods of disinfection of objects infected with them. Therefore, it is extremely important to keep your anti-virus database up-to-date.



New viruses appear every day. We recommend that you make sure to 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.

Kaspersky Anti-Virus updates the anti-virus database using the *keepup2date* component. In order start the updating process, enter the following in the command line:

```
/path/to/ kav4fs-keepup2date
```

The anti-virus database will be then downloaded from the updates server of Kaspersky Lab into a special folder specified in the configuration file.

4.3. Configuration for using Kaspersky Anti-Virus together with Webmin

If you plan to use remote administration of Kaspersky Anti-Virus, we recommend to configure it to be used in conjunction with Webmin package.

By using Webmin you can, for example, restrict access to the application's functionality by setting up a system of passwords for the users.

By default all settings of the Anti-Virus configured remotely using the Webmin program are saved in the default configuration file of the application.



If you wish to create an alternative configuration file using the Webmin program, you must:

1. Copy data from the existing configuration file into a new file and save this new file under a different name. After this you will have to

modify the new (alternative) configuration file so that it fits your purpose.

2. Specify the name of the alternative configuration file on the **Config edit** tab in the entry field for the **Full path to KAV config** setting.



For more details about various issues on configuring the Webmin application see the documentation for this product. Additionally, if you have questions regarding the remote administration of the application, you may refer to the Webmin online documentation.

Later, when you review the settings and run tasks, the operation **will not be performed** remotely through the Webmin program!

CHAPTER 5. USING KASPERSKY ANTI-VIRUS

Using Kaspersky Anti-Virus you can arrange the anti-virus protection system of your computer: from an individual file to the entire file system.

The functionality of the application is comprised of tasks that the administrator can perform using the application. All tasks implemented using Kaspersky Anti-Virus can be divided into the following groups:

- Updating of the anti-virus database used for detecting viruses and disinfecting infected objects (details see section 5.1 on page 26).
- Anti-virus protection of the computer's file systems (scheduled and/or on-demand scan) (details see section 5.2 on page 32).
- Real-time anti-virus protection (protection in the real-time mode (details see section 5.3 on page 38).

This chapter contains description of typical tasks that are implemented during the use of Kaspersky Anti-Virus. Within the context of a specific company's network the administrator may combine these tasks and make them more complex.

5.1. Updating the anti-virus database

Updating of the anti-virus database performed by the *keepup2date* component of the application is an integral factor of the full-fledged anti-virus protection. The source used for updating the anti-virus database used Kaspersky Anti-Virus when it searches for and disinfects infected objects are the Kaspersky Lab's updates servers. The list of such servers includes:

<http://downloads1.kaspersky-labs.com/>

<http://downloads2.kaspersky-labs.com/>

<ftp://downloads1.kaspersky-labs.com/>, etc.

The list of URL's from which you can download the updates is contained in the *updcfg.xml* file included into the application's distribution kit.

During the update process the *keepup2date* component selects the address from this list and attempts to download the anti-virus database from the server. If the

update cannot be performed from the address selected, the component switches to the next URL and makes another attempt.



Updates of the anti-virus database are uploaded to the Kaspersky Lab's updates servers on an hourly basis.

After the successful update a command specified as the value for the **PostUpdateCmd** parameter of the **[updater.options]** section in the configuration file is executed. By default this command starts an automatic reload of the anti-virus database. In case of an invalid change of the above setting the application may fail to use the updated database or will function improperly.



All settings of the *keepup2date* component are grouped in the **[updater.*]** options of the configuration file.

If the structure of your local area network is complex enough, we recommend that you download the updates of the anti-virus database from the updates servers every hour, place them into a network folder and configure the local computers throughout the network to copy the database from this folder. Details on the creation of a network folder see section 5.1.4 on page 31.

The update may be scheduled using the **cron** utility (see section 5.1.2 on page 28) or it may be performed on-demand by the administrator who can run this task manually from the command line (see section 5.1.3 on page 30).



We strongly recommend that you configure the anti-virus database updates to be performed every hour!

5.1.1. New capabilities of the updating component

In version 5.5. of Kaspersky Anti-Virus as opposed to the previous versions the anti-virus database update component has been upgraded. Some existing functions in the new component have been upgraded and some new capabilities have been added as follows:

- the ability to automatically select the closest geographical region to be used for downloading updates, based on the region specified in the configuration file;
- the ability to download and install incremental updates when a cumulative update is available, which allows to save the network traffic;
- in case of a disconnection while the anti-virus database is downloaded or if the updates server was swapped after the connection had been restored, the component will automatically start downloading the

remaining part of the anti-virus database rather than starting a new download;

- checking the integrity of the downloaded database;
- the analysis of the completeness of the anti-virus database and downloading only those elements of the database that have been modified or newly added. This ability also contributes to the savings of the network traffic;
- the ability to start an anti-virus database reload command specified by the user immediately after a successful update;
- the ability to roll back to the previous version of the anti-virus database;
- the wget application is not required now for the operation of the new component;
- the ability to select the type of the anti-virus database to download (standard or extended database set).

Standard database – anti-virus database that contains detailed description of all viruses existing at the moment and methods used for their detection and disinfection. This type of anti-virus database is used by default.

Extended database – anti-virus database that, in addition to information about viruses, contains information RiskWare and AdWare.

RiskWare programs contain vulnerabilities that may be used for hackers' attacks, installation of unauthorized software, etc.

AdWare programs are installed together with some other software and then display advertising messages, open pop-up windows containing advertisements or force the user to visit the advertiser's website. Apart from enforced advertising, such programs considerably load the communication channels and increase the traffic.

For regular operation mode it is sufficient to select standard anti-virus database. Extended anti-virus database is used to ensure a higher information protection level. The use of more complete sets of anti-virus database increases the consumption of resources during the scan.

5.1.2. Automatically updating the anti-virus database

You can schedule regular automatic updates of the anti-virus database by modifying the configuration file.



Task: configure automatic anti-virus database updates to be performed every 3 hours. Enter only application errors in the system log. Maintain the general log for all tasks started, do not print any information to the screen.



Solution: in order to perform this task, do the following:

1. Specify the corresponding values for the settings in the application's configuration file, for example:

```
[updater.options]
KeepSilent=yes
[updater.report]
Append=yes
ReportLevel=1
```

2. Edit file that defines the rules for the operation of the cron (**crontab-e**) process by entering the following line:

```
0 0-23/3 * * * /opt/kaspersky/bin/kav4fs-keepup2date
```



Task: configure the downloading of the anti-virus database updates from the Kaspersky Lab's updates servers. Automatically select the URL of the updates server from the list included into the *keepup2date* component.



Solution: in order to perform this task, do the following:

Assign value **No** to the **UseUpdateServerUrl** setting in the **[updater.options]** section.



Task: configure the download of the anti-virus database from the URL specified by the administrator. If the download cannot be performed from this URL, abort the downloading process.



Solution: in order to perform this task, do the following:

Assign **Yes** value to the **UseUpdateServerUrl** and **UseUpdateServerUrlOnly** settings of the **[updater.options]** value. Additionally, the **UpdateServerUrl** setting must contain the URL of the updates server.



Task: configure the download of the anti-virus database from the URL specified by the administrator. If the download cannot be performed from this URL, update the database from the URL specified in the list of the internal Kaspersky Lab's updates list.



Solution: in order to perform this task, do the following:

Assign value **Yes** to the **UseUpdateServerUrl** setting of the **[updater.options]** section and assign value **No** to the **UseUpdateServerUrlOnly** setting. Additionally, the **UpdateServerUrl** setting must contain the URL of the updates server.

5.1.3. On-demand updating of the anti-virus database

You can start the update of the anti-virus database from the command line at any moment.



Task: start the update of the anti-virus database and save the results to file `/tmp/updatesreport.log`.



Solution: in order to implement this task enter in the command line:

```
# kav4fs-keepup2date -l /tmp/updatesreport.log
```

If you need to update the anti-virus database on several computers, the most convenient way to do it is to download it once from the updates servers, place it into a network folder and then update the database from this folder rather than downloading the database from internet again and again.



Task: arrange updating of the anti-virus database from the network folder **/home/bases** and if this folder is not accessible or empty, update the anti-virus database from the Kaspersky Lab's servers. Print the results into the **report.txt** report file.



Solution: in order to perform this task, do the following:

1. Specify the corresponding values for the settings in the application's configuration file:

```
[updater.options]
UpdateServerUrl=/home/bases
UseUpdateServerUrl=yes
UseUpdateServerUrlOnly=no
```

2. Enter in the command line:

```
# kav4fs-keepup2date -l /tmp/report.txt
```

5.1.4. Creating a network folder for storing and downloading of the anti-virus database

In order to ensure that the updates of the anti-virus database from the network folder are performed correctly, you have to create in this folder a file structure that is analogous to the structure of the Kaspersky Lab's updates servers. Provided below is a detailed discussion of this task.



Task: create a network folder from which the anti-virus database updates will be copied to the local computers within the network.



Solution: in order to perform this task, do the following:

1. Create a local folder.
2. Start the *keepup2date* component as follows:

```
# kav4fs-keepup2date -u <dir>
```

where *<dir>* – full path to the folder created.
3. Grant the local computers read-only network access to this folder.



Task: configure the anti-virus database update to be performed via a proxy server.



Solution: in order to perform this task, do the following:

1. Assign value **Yes** to the **UseProxy** setting of the **[updater.options]** section.
2. Make sure that the **ProxyAddress** setting in the **[updater.options]** section of the configuration file contains the URL of the proxy server. The address must be specified in the following format: **http://username:password@ip_address:port**. Values **ip address** and **port** are mandatory while **username** and **password** are specified only if the proxy server requires authorization.

or:

1. Assign value **Yes** to the **UseProxy** setting of the **[updater.options]** section.

2. Specify environment variable **http_proxy** using format **http://username:password@ip_address:port**. Note that the environment variable will be considered only if the **UseProxy** setting of the **[updater.options]** section is missing or is assigned value **Yes**.

5.2. Anti-virus protection of file systems

The anti-virus protection of the computer's file systems is performed using the *kavscanner* component that performs the scan and processes infected and suspicious objects based on its settings.



All settings of the *kavscanner* component are grouped in the **[scanner.*]** options of the application's configuration file.



By default, only the **root** user can launch an on-demand scan.

You can perform the scan of the entire file system or of an individual folder or object. All protection settings may be divided into groups that define:

- Scan scope (see section 5.2.1 on page 33).
- Objects scan and disinfection mode (see section 5.2.2 on page 34).
- Actions to be performed with the objects (see section 5.2.3 on page 34).
- Settings used for generation of the report about the operation result (section 6.5 on page 47).

The scan of your computer's file systems may be started:

- As a one-time task - from the command line (see section 5.2.4 on page 36).
- According to the schedule using the **cron** application (see section 5.2.5 on page 36).



Anti-virus scan of the entire computer is a process that requires considerable resources. It should be noted that when you start this task, your computer's efficiency will be reduced, therefore we do not recommend to run any other processes at the same time. In order to avoid such problems, we recommend that you scan individual selected folders.

5.2.1. Scan scope

The scan scope can be roughly divided into two parts:

- *scan path* – the list of folders and objects in which the search for viruses will be performed;
- *scan objects* – types of objects that will be scanned for viruses (archives, etc.)

By default all objects of all available file systems will be scanned, starting with the current folder.



In order to scan all file systems of the computer, you have to switch to the root folder or specify the scan scope in the command line `/`.

You can redefine the scan path by the following methods:

- At the startup of the component list in the command line (using a space as a separator) folders and files with absolute or relative (relative to the current folder) paths to them.
- Specify the scan paths in the text file and specify this file to be used using modifier `-@<filename>` in the command line. Each object in this file shall be entered in a new line with the absolute path to it.



If you specified in the command line both the scan path and the text file with the list of the scan objects, the area indicated in the file will be scanned. The path entered in the command line will be ignored.

- Restrict paths accepted by default (all, starting with the current folder) or listed in the command line by entering into the **kav4fs.conf** configuration file masks of files and folders that will be excluded from the scan scope (**[scanner.options]** section, settings **ExcludeMask** and **ExcludeDirs**).
- Turn off the *recursive scan of the folders* (**[scanner.options]** section, the **Recursion** setting or modifier **-r**).
- Create an alternative configuration file and specify this file to be used using modifier **-c <filename>** at the component startup.

Default scan objects are specified in the **kav4fs.conf** configuration file (**[scanner.options]** section) and they can be redefined.

- directly in this file;
- using command line modifiers at the component startup;
- by using an alternative configuration file.

5.2.2. Objects scan and disinfection mode

The settings of this mode are a very important scan option, because they determine whether the application will disinfect infected files detected during the scan.

By default this options is turned off because it only provides for the scan of object and for notifying about detected viruses and other suspicious or corrupted files by printing the messages to the screen and into the report (see section 6.5 on page 47).

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

- **Clean** – no viruses detected (the object is not infected).
- **Infected** – the object is infected.
- **Warning** – object code resembles the code of a known virus.
- **Suspicious** – the object is suspected of being infected with an unknown virus.
- **Corrupted**– the object is corrupted.
- **Protected** – the object cannot be scanned because it is encrypted (password-protected).

With the disinfection mode turn on (section **[scanner.options]**, setting **Cure = yes**) only object with status **Infected** will be sent for anti-virus processing. As the result of the disinfection, the object will be assigned a status from those listed below:

- **Cured** – the object has been successfully disinfected.
- **CureFailed** – the object could not be disinfected. File with such status will be processed according to rules specified for infected objects.
- **Error** – error occurred during the object scan.

5.2.3. Actions to be performed with objects

Which actions will be applied to an object depends on the object's status (see Chapter 2 on page 14). By default notification will be performed only about detection of objects with a specific status. However for objects with **Infected**,

Suspicious, Warning, Error, Protected and **Corrupted** status you can configure performing of some actions, including:

- *moving to a folder* – moving objects with a certain status to a folder; *simple* and *recursive* moving is available.
- *deleting object* from the file system;
- *performing a command* – processing of files using standard Unix, script files, etc.

It should be noted that Kaspersky Anti-Virus discriminate between simple objects (files) and container objects (consisting of several objects, for example, an archive). Actions performed with such objects are also discriminated; in the configuration files these actions are located in different sections. For simple objects – section **[scanner.object]**, for container objects– section **[scanner.container]**.



Actions performed with self-extracting archives can be different: if the archive is infected, it will be viewed as a simple object; if objects within the archives are infected, the object will be viewed as a container. Therefore actions to be performed with the archives, depending on the case, will be determined by the settings specified in different sections of the configuration file.

You can select an action to be performed with an object using several methods as follows:

- You can specify them in the **kav4fs.conf** configuration file if you plan to use these actions as default actions (sections **[scanner.object]** and **[scanner.container]**).
- Specify actions in the alternative configuration file and use this file at the component startup.



If no configuration file is specified in the command line at the component startup, the operating settings will be taken from the **kav4fs.conf** file. The use of this file at the startup does not have to be specified!

- You can specify them for the current work session using the command line modifiers at the startup of the *kavscanner* component.

Actions for both simple and container objects use the same syntax (sections **[scanner.object]** and **[scanner.container]**).

5.2.4. On-demand scan of an individual folder

One of the most commonly used tasks implemented by Kaspersky Anti-Virus is anti-virus scan and disinfection of an individual folder.



Task: start an anti-virus scan of folder **/tmp** with automatic disinfection of all infected objects detected. Delete all objects that could not be disinfected.

Create files *infected.lst*, *suspicion.lst*, *corrupted.lst* and *warning.lst* in which you can save the filenames of all infected, suspicious and corrupted objects detected during the scan.

The results of the component operation (starting date, information about all files, except clean files) will be printed only into the report file *kav4fs-kavscanner-current_date-pid.log* that you must save in the same folder.



Solution: in order to implement this task enter in the command line:

```
# kav4fs-kavscanner -rlq -pi/tmp/infected.lst
-ps/tmp/suspicion.lst -pc/tmp/corrupted.lst
-pw/tmp/warning.lst -o /tmp/kav4fs-kavscanner-`date
"+%Y-%m-%d-$$"`.log -i3 -ePASBMe -j3 -mCn /tmp
```

5.2.5. Scheduled scan

Scheduled programs startup, including Kaspersky Anti-Virus tasks, is performed using **cron** application.



Task: Run an anti-virus scan of **/home** folder every day at 0:00; use the scan settings specified in the configuration file */etc/kav/scanhome.conf*.



Solution: in order to perform this task, do the following:

1. Create configuration file */etc/kav/scanhome.conf* and specify all required scan settings in this file.
2. Edit file that defines the rules for the operation of the cron (**crontab-e**) process by entering the following line:

```
0 0 * * * /path/to/kav4fs-kavscanner -c
/etc/kav/scanhome.conf /home
```

5.2.6. Additional capabilities: using script files

Kaspersky Anti-Virus offers additional processing of objects during the antiviral analysis by using various standard Unix commands and script files. Using these tools experienced administrators can independently define actions to be performed with objects of different statuses and thus, expand the functionality of Kaspersky Anti-Virus.

5.2.6.1. Disinfection of infected objects in the archive

Kaspersky Anti-Virus does not disinfect infected files packed into archives; it only detects suspicious and infected objects within such archives. However, the ability to disinfect infected files packed into archives can be implemented by using an additional script file. This document contains an example of disinfection of *tar* and *zip* archives using script file *vox.sh*. This script is included into the Kaspersky Anti-Virus distribution package.

When started, the script will unpack the archive being scanned, run an anti-virus scan and processing of individual objects, and then pack the scanned files. Therefore necessary archiver utilities have to be installed in the system.



Task: scan all *tar* and *zip* archives, using script *vox.sh*.



Solution: in order to perform this task, do the following:

Enter in the command line:

```
# /opt/kaspersky/kav4fs/share/contrib/vox.sh <archive-path>
```

5.2.6.2. Sending notifications to the administrator

Using standard Unix tool, you can configure notifications to be sent to the administrator upon detection of infected, suspicious or corrupted objects in the computer's file systems.



Task: configure administrator notification in case of detection of infected files and archives in the file systems during each computer scan performed using the settings specified in the **kav4fs.conf** configuration file. Enable the mode of opening symlinks.



Solution: in order to perform this task, do the following:

Specify the following rules for processing simple objects and container objects in configuration file **kav4fs.conf**:

```
[scanner.options]
FollowSymlinks=yes
[scanner.object]
OnInfected=exec echo %FULLPATH%/%FILENAME% is
infected by %VIRUSNAME% |
mail -s kav4fs-kavscanner admin@localhost.ru
[scanner.container]
OnInfected=exec echo archive %FULLPATH%/%FILENAME% is
infected, viruses list is in the attached file %LIST%
| mail -s kav4fs-kavscanner -a %LIST%
admin@localhost.ru
```



Before launching the example the user must make sure that the **mail** utility is located at the location pointed at by this utility's standard installation path in the operating system.

5.3. Real-time anti-virus protection

Real-time anti-virus protection of the computer's file system is performed using the *kavmonitor* component.



All settings of the *kavmonitor* component are contained in the **[monitor.*]** section of the application's configuration file.

The *kavmonitor* component is configured so that when performing any action requiring access to the file (opening, closing or running), component *kavmonitor* performs an anti-virus scan (when closed, the file will be scanned only if it has been altered). By default all objects requested by the user will be scanned for viruses and malware, including:

- packed files;
- archives;
- self-extracting archives;
- mail databases;
- e-mail message.

Based on the results of the scan anti-virus object processing will be performed using the settings specified in the application's configuration file.



By default the infected objects disinfection mode is disabled! In order to configure this option assign value **Yes** to the **Cure** setting in section **[monitor.options]** of the application's configuration file.

For objects with **Infected**, **Suspicious**, **Warning**, **Error**, **Protected** and **CureFailed** status you can configure performing of some actions, including:

- *moving to a folder* – moving objects with a certain status to a folder; *simple* and *recursive* (with restoration of the full path) *moving* is available.
- *deleting object* from the file system;

You can configure rules for processing objects by defining them in the application's configuration file (section **[monitor.actions]**).

You can also configure additional settings:

- Using settings **ExcludeDirs** and **ExcludeMask** define folders that must be excluded from the scan.
- Use the heuristic code analyzer and the iChecker technologies.
- Reduce the server load using by defining the maximum number of objects that can be scanned at the same time.

5.4. Managing license keys

The license key gives you the right to use the application and contains all required information pertaining to the license, that you have purchased, such as: type of the license, license expiration date, dealer details, etc.

In addition to the right of using the application during the license period you obtain:

- 24/7 technical support;
- new updates of the anti-virus database on an hourly basis;
- application updates (patches);
- receiving new versions of the application (upgrades);
- up-to-date information about new viruses.

Upon the expiration of the license you will automatically lose the right to receive the above services. Kaspersky Anti-Virus will continue performing anti-viral file processing, but it will use the anti-virus database that was up-to-date as of the license expiration date. The anti-virus database updating function will not be available.

Therefore, it is extremely important to regularly review the report files that contain the license key details and keep track of the license expiration date.

5.4.1. Viewing license key details

You can view information about installed license keys in the reports about operation of components *kavscanner*, *kavmonitor* and *keepup2date* because at the startup each of these components loads information about these keys.

Apart from this, Kaspersky Anti-Virus provides for a special component *licensemanager* that allows you to view not only the full information about the keys, but also receive some analytical data.

All information may be printed to the screen.



In order to view information about all license keys,

Enter in the command line:

```
kav4fs-licensemanager -s
```

Information will be printed to the screen as follows:

```
Kaspersky license manager Version 5.5  
Copyright © Kaspersky Lab 1997-2007.  
Portions Copyright (C) Ian Crypto
```

```
License file 0003D3EA.key, serial 0038-000419-0003D3EA, "Kaspersky Anti-Virus for Unix", expires 04-07-2003 in 28 days
```

```
License file 0003E3E8.key, serial 011E-000413-0003E3E8, "Kaspersky Anti-Virus for Linux File Srv (licence per e-mail address)", expires 25-01-2004 in 234 days
```



In order to view information about a specific key,

Enter in the command line:

```
kav4fs-licensemanager -k 0003D3EA.key
```

The following information will be printed to the screen:

```
Kaspersky license manager Version 5.5  
Copyright (C) Kaspersky Lab. 1997-2007.  
Portions Copyright (C) Lan Crypto  
Serial 0038-000419-0003D3EA, "Kaspersky Anti-Virus  
for Linux", expires 04-07-2003 in 28 days
```

5.4.2. Renewing your license

Renewal of your Kaspersky Anti-Virus license grants you the right for to restore the full-featured functionality of the application - update the anti-virus database. Besides, additional services listed in section 5.3 on page 39 will be resumed.

The license period depends on the type of licensing that you selected when you purchased the application.



In order to renew your Kaspersky Anti-Virus license,

contact the dealer you purchased the application from and renew your license for the use of Kaspersky Anti-Virus.

or:

renew your license key directly at Kaspersky Labs; in order to do it, send a request directly to our Sales Department (sales@kaspersky.com) or fill out a form at our website (<http://www.kaspersky.com>), section **eStore** -> **Renewal**. Upon the receipt of your payment, we will send a new license key to the e-mail address specified in your order.



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 our offers visit Kaspersky Lab's corporate website and go to **Products → Sales and special offers**.

You must install the license key that you purchased.



In order to install your new license key,

Enter in the command line:

```
kav4fs-licensemanager -a <key filename>
```

After this we recommend that you update your anti-virus database (see section 5.1 on page 26).



In order to remove a license key,

Enter in the command line:

```
kav4fs-licensemanager -d <key filename>
```

CHAPTER 6. ADDITIONAL SETTINGS

This chapter contains information about additional settings of Kaspersky Anti-Virus. These additional settings are used to extend the functionality of the application and its adaptation to the conditions of a specific company.

6.1. Optimization of Kaspersky Anti-Virus operation

In order to reduce the load on the processor and increase the speed of the anti-virus processing of objects, Kaspersky Anti-Virus offers effective methods for optimization of its operation. Provided below is a detailed discussion of these features.



The use of the iChecker database and double-level caching of scanned files.

The application uses several technologies that make it unnecessary to scan a file each time you attempt to access it and, if possible, restrict the work to mere comparing it to the existing information about it. The algorithm of scanning object (file) for viruses includes the following:

After the primary scan of any file, information about it (name, checksum) is registered in one of the following databases:

- iChecker database – common database that includes information about scanned **non-infected** files of some formats. This database contains information about objects scanned by *kavmonitor* and *kavscanner*.
- The cache of scanned files - database that contains information about files scanned by the *kavmonitor* files. The cache consists of two levels: the first level stores information about **clean files**, that are accessed relatively often. The first-level cache is located in the kernel module that allows to considerably decrease the time needed to access it. If the application detects data about the file requested in the first-level cache, it automatically assigns the **Clean** status to the object and no further anti-virus scan will be performed. If the first-level cache does not contain the required information a search will be performed on the second level that

contains information **about all scanned files**. Both cache databases exist in the RAM and will not persist after the application is closed.

Therefore, if during the scan information about the files is not added to the iChecker database (the file is clean or its format is not supported by this technology), it will be added to the cache.

During each attempt to access the file performed by the user, a search will be performed first in the first-level cache, then (if the object has not been detected in the first database) - in the iChecker database and in the second-level cache. The search is based on the filename. If such file is found in any of the databases, the file information will be compared with the information stored in the database. If the current state and its description in the database are completely identical, the file will be deemed unaltered and will not be checked for viruses.

If information about the file requested is not detected either in the iChecker database nor in cache, a full anti-virus scan of the file will be performed.



If you switched the anti-virus database set while working with Kaspersky Anti-Virus, you will have to manually delete information from the iChecker database (the full path to the database is defined in the **lcheckerDbFile** parameter in the **[path]** section of the application's configuration file).

This must be done because the database may contain infected objects not detected using the standard anti-virus database, but detected using the extended set. Files information about which is contained in the iChecker database will not be rescanned which may result in an infection of your computer.



Limiting the load on the processor.

The scan of the computer's file systems may take considerable time if you have considerable amount of data stored. In this case the load on the processor will be considerably increased. At the same time the processor will have to perform current tasks, therefore it would be desirable to have a tool that would pause the anti-virus scan once the specified load threshold has been exceeded.

Kaspersky Anti-Virus has such mechanism. In version 5.5 setting **MaxLoadAvg** has been added to section **[scanner.options]** of the configuration file. If this setting is turned on, *kavscanner*, when scanning each new file, will read the current value of the processor **load average** and if this value exceeds the value specified in the configuration file, *kavscanner* pauses the scan until the value of **load average** decreases to the specified level.

Additionally, you can restrict the number of objects scanned at the same time in the real-time mode using setting **CheckFileLimit** of section **[monitor.options]** of

the application's configuration file. This allows to decrease the load on the processor and increase the speed of scanning of some objects.

6.2. Moving objects into the quarantine folder

You can configure operation of Kaspersky Anti-Virus so that all infected objects will be moved to a separate folder.

This ability can be used, for example, *if the object could not be disinfected* (for example, only two viruses were removed out the three viruses the file is infected with), but the file itself contains valuable information.

If you plan to store the folder with such isolated objects within the computer's file system, we recommend to exclude it from the scope of future scans by specifying the full path to it as the value for setting **ExcludeDirs** in section **[scanner.options]** of the configuration file.

Provided below is a discussion of tasks of isolation of infected objects detected during the process of the on-demand anti-virus scan of the computer's file system and during the scan in the real-time mode.



Task: scan for viruses all objects listed in file `/tmp/download.lst` and move infected objects detected with full paths to these objects to folder `/tmp/infected`. Print information about infected, suspicious and corrupted objects into the report file.



Solution: in order to perform this task, do the following:

1. To specify actions with the infected objects, enter the following line in sections **[scanner.object]** and **[scanner.container]** of the configuration file:

```
OnInfected=MovePath /tmp/infected
```

2. Turn off disinfection mode (**Cure = no**) if it is turned on.
3. Enter in the command line:

```
# kav4fs-kavscanner -@/tmp/download.lst -ePASBME  
-rq  
-i0 -o /tmp/report.log -j3 -mCn
```

Now the task will be made more complex by imposing a requirement to restrict access to the files in folder `/tmp/infected` to reading and writing only. This can be

achieved using standard Unix tools (command **chmod**). Therefore, the task implementation procedure shall be modified as follows:

Enter the following line in sections **[scanner.object]** and **[scanner.container]** of the applications' configuration file to specify the rules for processing infected objects:

```
OnInfected=exec mv %FULLPATH%/%FILENAME%
/tmp/infected/%FILENAME%; chmod -x
/tmp/infected/%FILENAME%
```



Task: scan for viruses all files attempted to be accessed, disinfect infected objects. If the disinfection is not successful, move the infected objects with full paths to them into folder **/tmp/infected**.



Solution: in order to perform this task, do the following:

1. Turn on the disinfection mode for infected objects (**Cure = yes** in section **[monitor.options]** in the configuration file).
2. Specify the rules for isolation of infected objects. In order to do it, configure the setting in section **[monitor.actions]** of the configuration file as follows:

```
OnInfected=MovePath /tmp/infected
```

6.3. Object backup copying mode

If the files scanned were infected and deletion from the file system is indicated as the action to be performed with infected objects, there is a risk of losing some important data. In order to avoid it, Kaspersky Anti-Virus includes the ability to copy files to the backup storage.

Before the attempt to disinfect or delete an object its copy will be automatically created in the backup storage (section **[monitor.path]**, settings **BackupPath**). This allows to create a backup copy (and, if required, to restore the original file) if the object is corrupted during the disinfection. The object with the full path will be saved into the backup storage. If an object is saved twice into the backup storage, the older copy of the object will be automatically replaced with the newer one.

Please note: by default the mode of saving into the backup storage is turned off and, therefore, the path to the folder in which the backup copies are supposed to be stored, is not defined.

In order to turn on this mode, manually specify the path to the folder in which backup copies of the objects will be stored.



If you delete an object from the file system, its copy will be kept in the backup storage until it is deleted by the administrator.



Actions specified for infected objects in the configuration file settings will not be performed with files stored in the backup storage!

6.4. Localization of the date and time format

During its operation, Kaspersky Anti-Virus generates reports for each of its components and various notifications sent to the users and administrators. This information is always stamped with the date and the time it was created.

The default date and time formats used by Kaspersky Anti-Virus are in conformity with the strftime standard:

%H:%M:%S – time format.

%d/%m/%y – date format.

The administrator can alter the time and the date formats. Localization of the formats can be performed in section **[locale]** of the configuration file. For example, you can specify the following formats:

%I:%M:%S %P – in order to display time in "twelve-hour format" (**TimeFormat** setting) with indication of AM/PM.

%y/%m/%d and **%m/%d/%y** – in order to display date (**DateFormat** setting) in format year/month/day и month/day/year respectively.

6.5. Kaspersky Anti-Virus report generation settings

Results of the operation of all components of Kaspersky Anti-Virus are logged into the report that is printed into a file.



Results of the anti-virus processing of the computer's file systems will also be printed to the screen. By default information printed into the report and to the screen will be duplicated. If you wish to display on the screen information that will be different from the information logged into the report file, you will have to configure additional settings.

If you wish the application to record its activity in the system log, set the **ReportFileName** parameter in the **[monitor.report]**, **[scanner.report]**, and **[updater.report]** sections to **syslog**.

The level of detail of the information logged/displayed can be adjusted by altering the *report detail level*.

The detail level is presented as a number that determines the detail level of the information about the operation of the components to be logged into the report. Each next level includes information of the previous level complemented by some additional information.

The table below lists all possible levels of the report detail.

Level	Level description	Explanation
	Critical errors	Information about critical errors only (that is errors that cause the application to close due to impossibility to perform any action). For example, the component is infected or an error occurred during the verification or loading of the database or the license keys.
1	Errors	Information about other errors including those that cause the component to close, for example, object scan error information.
2	Warning	Information about errors that may cause the application to close (for example information about insufficient free disk space).
3	Info, Notice	Important informational messages, for example: information stating whether the component is running, path to the configuration file, scan scope, information about the anti-virus database, about license keys, statistical info about the results.
4	Activity	Messages about objects scan in accordance with the scan level detail level.

Information about the critical errors in the operation of the component will always be included, irrespective of the selected detail level. The optimum level is level 4 selected by default.

CHAPTER 7. UNINSTALLING KASPERSKY ANTI-VIRUS

In order to be able to uninstall Kaspersky Anti-Virus you will need:

- Privileged user rights (**root**). If, at the moment you are going to uninstall the application, you do not have such rights, you will have to log in into the system as the **root** user.
- Installation process report file.
- The filenames and sizes of the installed Kaspersky Anti-Virus files shall fully correspond to those indicated in the installation report file.
- Before you start the application installation process, you will have to stop the **kavmonitor** component.



If you used Kaspersky Anti-Virus rpm package during the installation, enter the following in the command line in order to start the removal process:

```
rpm -e <package_name>
```



If you used Kaspersky Anti-Virus deb package during the installation, enter the following in the command line in order to start the removal process:

```
dpkg -r <package_name>
```




If you used Kaspersky Anti-Virus pkg package during the installation, enter the following in the command line in order to start the removal process:

```
pkg_delete <package_name>
```

The removal procedure will be performed automatically. Upon the completion of the procedure a corresponding message will be displayed on the screen.

CHAPTER 8. VERIFYING THE ANTI-VIRUS OPERATION

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

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

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



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

You can download this test "virus" from the official website of the **EICAR** organization at http://www.eicar.org/anti_virus_test_file.htm. If you have no internet connection, you can create your own test "virus". To create a test "virus," type the following in any text editor and save the file as **icar.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". The Anti-Virus will detect it, assign it the **Infected** non-disinfectable category and apply the action defined by the administrator for processing objects of this type.

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

Table. Modifying the test "virus"

Prefix	Object type
No prefix, standard test "virus"	Infected. Non-disinfectable object.
CORR-	Corrupted.
SUSP-	Suspicious (unknown virus code)

Prefix	Object type
WARN–	Suspicious (modified code of a known virus)
ERRO–	Not analyzed due to an error.
CURE–	Disinfected. The object will be disinfected; the text of the “virus” body will be replaced with the word “CURE”
DELE–	The object will be automatically deleted

The first table column lists prefixes to be added at the beginning of the string of the standard test “virus” (for example, CORR–X5O!P%#@AP[4PZX54(P^)^7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*). The second column of this table contains the types of objects identified by the anti-virus application after you have added a prefix. The actions for each type of objects are defined by the Anti-Virus settings configured by the administrator.

APPENDIX A.

ADDITIONAL INFORMATION ABOUT THE APPLICATION

This Appendix contains the description of the folder tree of the Kaspersky Anti-Virus after the installation, configuration file and the modifiers of the command line of the components and their return codes; script file for disinfecting archives is provided as an example.

A.1. Kaspersky Anti-Virus configuration file

The Kaspersky Anti-Virus package includes the **kav4fs.conf** configuration file that contains the settings for the application's operation. This section contains a detailed discussion of each section of the file settings. In the description of the file settings default values will be indicated, if such default values are provided.

Section **[path]** includes settings that define paths to most important files without which the application will not function.

BasesPath– full path to the anti-virus database.

LicensePath– full path to the folder that contains the license keys.

IcheckerDbFile– full path to the folder that stores the database checked using the iChecker technologies.

Section **[locale]** contains settings that determine the date and time formats:

TimeFormat=%H:%M:%S – time display format according to the strftime standard.



You can change the time display format to the twelve-hour format (am, pm): **%I:%M:%S %P**

DateFormat=%d/%m/%y – date display format according to the strftime standard.



You can change the date display format, for example, to the following: **%y/%m/%d** or **%m/%d/%y**.

Section **[monitor.options]** contains real-time anti-virus scan settings:

ExcludeDirs=mask1:mask2:...:maskN – masks of folders that are excluded from the scan; by default all folders will be scanned.

ExcludeMask=mask1:mask2:...:maskN – file masks that will be excluded from the scan; by default all files will be scanned.

IncludeDirs=mask1:mask2:...:maskN – masks of folders that will be scanned.

Packed=yes – packed files scan mode. In order to disable this mode assign value **no** to this setting.

Archives=yes – archives scan mode. In order to disable this mode assign value **no** to this setting.

SelfExtArchives=yes – self-extracting archives scan mode. In order to disable this mode assign value **no** to this setting. If the archive scan mode is enabled (**Archives=yes**), then self-extracting archives will be scanned even if the **SelfExtArchives** setting has value **no** assigned to it.

MailBases=yes – mail database scan mode. In order to disable this mode assign value **no** to this setting.

MailPlain=yes – scan of mail messages in format plain.text . In order to disable this mode assign value **no** to this setting.

Heuristic=yes – mode for using heuristic code analyzer during the scan. In order to disable this mode assign value **no** to this setting.

Cure=no – mode for disinfecting infected objects. In order to enable this mode assign value **yes** to this setting.

Ichecker=yes – the mode for the use of the iChecker technology during the anti-virus scan. In order to disable this mode assign value **no** to this setting.

FileCacheSize – size of file cache (in MB).

KernelCacheSize – the size of cache stored by the anti-virus kernel (in MB).

CheckFileLimit=20 – the maximum number of objects that can be scanned at the same time.

HashType=md5 – the type of hash used.

UseAVbasesSet=standard|extended – the set of anti-virus database used by the application. The **extended** set contains, in addition to records contained in the **standard** set, signatures of riskware, such as: adware, remote administration programs, etc.

Section **[monitor.path]** includes settings that define paths to most important files without which the kavmonitor module will not function.

BackupPath= path – full path to the folder that stores backup copies of the objects scanned.

PidFile=path – full path to pid file of the kavmonitor component.

Section **[monitor.actions]** contains settings that define actions to be performed with objects of certain types during the real-time anti-virus protection.

OnInfected=action – actions to be performed in case of a detection of an infected file. If the mode of disinfection of infected files is turned on, then the specified action will be performed with objects that could not be disinfected.

OnSuspicion=action – actions to be performed in case of a detection of a suspicious file code of which resembles code of a virus not known yet to Kaspersky Lab.

OnWarning=action – actions to be performed in case of a detection of a file the code of which resembles the code of a known virus.

OnCured=action – actions to be performed in case of a detection and successful disinfection of an infected object.

OnProtected=action – actions to be performed in case of a detection of a password-protected object. Such objects cannot be scanned.

OnCorrupted=action – actions to be performed in case of a detection of a corrupted file.

OnError=actions – actions to be performed if a system error occurred during the object scan.

Section **[monitor.report]** contains the settings of generating reports about the results of the kavmonitor component operation.

ReportLevel=4 – report detail level.

ReportFileName – filename of the file into which results of the component operation will be logged.

Append=yes – mode for appending new messages to the report file. In order to disable this mode assign value **no** to this setting.

ShowOK=yes – mode for logging messages about clean files into the report. In order to disable this mode assign value **no** to this setting.

Section **[scanner.options]** contains settings for scanning the server's file systems:

Archives=yes – archives scan mode. In order to disable this mode assign value **no** to this setting.

Cure=no – mode for disinfecting infected objects. In order to enable this mode assign value **yes** to this setting.

ExcludeDirs=mask1:mask2:...:maskN – masks of folders that are excluded from the scan; by default all folders will be scanned.

ExcludeMask=mask1:mask2:...:maskN – file masks that will be excluded from the scan; by default all files will be scanned.

Heuristic=yes – mode for using heuristic code analyzer during the scan. In order to disable this mode assign value **no** to this setting.

LocalFS=no – mode for scanning only the local file system. In order to enable this mode assign value **yes** to this setting.

MailBases=yes – mail database scan mode. In order to disable this mode assign value **no** to this setting.

MailPlain=yes – scan of mail messages in format plain.text . In order to disable this mode assign value **no** to this setting.

Packed=yes – packed files scan mode. In order to disable this mode assign value **no** to this setting.

Recursion=yes – mode for recursive scanning of folders during the anti-virus scan. In order to disable this mode assign value **no** to this setting.

SelfExtArchives=yes – self-extracting archives scan mode. In order to disable this mode assign value **no** to this setting. If the archive scan mode is enabled (**Archives=yes**), then self-extracting archives will be scanned even if the **SelfExtArchives** setting has value **no** assigned to it.

Ichecker=yes – the mode for the use of the iChecker technology during the anti-virus scan. In order to disable this mode assign value **no** to this setting.

UseAVbasesSet=standard|extended – the set of anti-virus database used by the application. The **extended** set contains, in addition to records contained in the **standard** set, signatures of riskware, such as: adware, remote administration programs, etc.

FollowSymlinks – the option controls handling of symbolic links. If the parameter is set to **yes**, the application will follow the links that point to directories while scanning.

MaxLoadAvg – maximum processor load.

Section **[scanner.report]** contains the settings of generating reports about the results of the kavscanner component operation.

Append=yes – mode for appending new messages to the report file. In order to disable this mode assign value **no** to this setting.

ReportFileName – filename of the file into which results of the component operation will be logged.

ReportLevel=4 – report detail level.

ShowOK=yes – mode for logging messages about clean files into the report. In order to disable this mode assign value **no** to this setting.

ShowContainerResultOnly=no – the mode of displaying the results of the archive scan in short format. In order to display short report assign value **yes** to this setting.

ShowObjectResultOnly=no – the mode of displaying the results of the scan of a simple object in short format. In order to display short format assign value **yes** to this setting.

Section **[scanner.container]** includes settings that determine actions to be performed with archives during the anti-virus protection of the server's file systems.

OnCorrupted=action – actions to be performed in case of a detection of a corrupted container.

OnInfected=action – actions to be performed in case of a detection of an infected objects in the container. If the mode of disinfection of infected files is turned on, then the specified action will be performed with containers that could not be disinfected after all other actions with the objects of the container have been completed.

OnSuspicion=action – actions to be performed in case of a detection of a suspicious object inside a container.

OnWarning=action – actions to be performed in case of a detection inside a container of an object the code of which resembles the code of a known virus.

OnCured =action – actions to be performed in case of a detection inside a container of an infected file that was successfully disinfected.

OnProtected=action – actions to be performed in case of a detection of a password-protected object. Such objects cannot be scanned.

OnError=actions – actions to be performed if an error occurred during the container scan.

The syntax of the **action** setting consists of two parts: the action itself and an optional parameter divided with a space. The value of the optional parameter is entered in quotes. For example, **OnInfected=move "/tmp/infected"**

The action may accept one of the following values:

- *move* <folder> – move file into <folder>.
- *movePath* <folder> – move file to <folder> recursive (with the absolute path).
- *remove* – delete the file.
- *exec* <parameter> – perform with the object action defined by the value <parameter>.

The following is used as macros of the optional parameter of the *exec* action for the containers:

- %LIST% – filename or the list of infected, suspicious and corrupted files found in the container. The file format is as follows: **<virus name>\t<filename>**.
- %FULLPATH% – full path to the container.

- **%FILENAME%** – filename without the path.
- **%CONTAINERTYPE%** – container type as a line.

Section **[scanner.object]** contains settings that define actions to be performed with simple objects of certain types during the anti-virus protection of file servers.

OnCorrupted=action – actions to be performed in case of a detection of a corrupted file.

OnInfected=action – actions to be performed in case of a detection of an infected file. If the mode of disinfection of infected files is turned on, then the specified action will be performed with objects that could not be disinfected.

OnSuspicion=action – actions to be performed in case of a detection of a suspicious file code of which resembles code of a virus not known yet to Kaspersky Lab.

OnWarning=action – actions to be performed in case of a detection of a file the code of which resembles the code of a known virus.

OnCured=action – actions to be performed in case of a detection and successful disinfection of an infected object.

OnProtected=action – actions to be performed in case of a detection of a password-protected object. Such objects cannot be scanned.

OnError=actions – actions to be performed if an error occurred during the object scan.

Syntax of the actions that are performed with the objects listed above is similar to that for containers described above in section **[scanner.container]**.

Section **[scanner.display]** contains settings for printing the report to the screen:

ShowContainerResultOnly=no – the mode of displaying the results of the archive scan in short format on the screen. In order to display short format assign value **no** to this setting.

ShowObjectResultOnly=no – the mode of displaying the results of the scan of a simple object in short format on the screen. In order to display short report assign value **no** to this setting.

ShowOK=yes – mode for printing messages about clean files to the screen. In order to disable this mode assign value **no** to this setting.

ShowProgress=yes – mode of displaying on the screen information about the current component operation (the process of downloading of the anti-virus database, information about the scan of the current file). In order to disable this mode assign value **no** to this setting.

Section **[scanner.path]** contains parameters that determine paths to files without which the kavscanner module will not function:

BackupPath= path – full path to the backup storage folder for backup copies of the objects being scanned by the component.

Section **[updater.path]** includes settings that define paths to the files required for the operation of the anti-virus database updating component:

AVBasesTestPath – full path to the anti-virus database storage folder.

BackUpPath – full path to the anti-virus database backup copy storage folder.

Section **[updater.report]** contains the settings of generating reports about the results of the keepup2date component operation.

Append=yes – mode for appending new messages to the report file. In order to disable this mode assign value **no** to this setting.

ReportFileName – filename of the file into which results of the component operation will be logged.

ReportLevel=4 – report detail level.

Section **[updater.options]** contains the settings of the keepup2date component operation:

KeepSilent=no – mode for printing information about operation of the *keepup2date* component to the screen. In order to disable this mode assign value **yes** to this setting.

ProxyAddress – address of the proxy server used for the connection. This setting is specified in the following format: **http://username:password@url:port**; The **username** and/or the **password** settings are not mandatory for the proxy server address. If the address is not specified, its value will be imported from the environment variable **http_proxy**.

UseProxy – mode for the use of the proxy server for connecting with the Kaspersky Lab's updates server. If the setting is assigned value **no**, the proxy server will not be used. If this setting is assigned value **yes**, the proxy sever address defined by setting **ProxyAddress** will be used. If the value of the **ProxyAddress** setting is not defined, the value of the **http_proxy** environment variable will be used. If the value of the environment variable is not defined, the proxy server will not be used.

UseUpdateServerUrl=no the mode for the use of address defined by setting **UpdateServerUrl** for updating.

UseUpdateServerUrlOnly=no the mode for using only address specified in setting **UpdateServerUrl** for updating of the anti-virus database. If this setting is assigned value **no**, then in case of an unsuccessful update of the anti-virus data-

base from address **UpdateServerUrl**, another address from the list of the updates servers will be used.

UpdateServerUrl=no http://url/ | ftp://url/ | /local_path/ – address for updating the anti-virus database.

PostUpdateCmd – command executed immediately after the anti-virus database update has been successfully completed. The value specified in the configuration file included into the application installation package will start automatic reading of the updated anti-virus database by the application. We do not recommend changing the value of this setting.

RegionSettings= the code of the user's region; this code is used to select a Kaspersky Lab's updates server that would suit best for downloading the updates of the anti-virus database.

ConnectTimeout=30 network timeout for updating the anti-virus database (in seconds). If, during the indicated period the data is not received from the server, another server will be selected from the list of Kaspersky Lab's updates servers.

PassiveFtp=no using passive FTP mode for connection.

A.2. Command line modifiers for component kavscanner

Settings of the configuration file can be redefined from the command line at the application startup using the command line modifiers. A detailed discussion of these modifiers is provided below.

Help options:

- h** Display help information about the kavscanner component to the screen;
- v** Display the application version.

Configuration options:

- c (-C) <path_to_file>** Use alternative configuration file **<path_to_file>**;
- g<path_to_file>** Place the list of all known viruses, records of which are contained in the anti-virus database, into file **<path_to_file>**
- f** Ignore corrupted signature of the kavscanner component and attempt to disinfect the component.

Scanning options:

- e <option>** Change the default scan option. The following modes may be used as an **<option>**:
- P/p** Enable/disable the scan of packed files;
 - A/a** Enable/disable the scan of archives;
 - S/s** Enable/disable the scan of self-extracting archives;
 - B/b** Enable/disable the scan of mail databases;
 - M/m** Enable/disable the scan of plain text format messages;
 - E/e** Enable/disable heuristic code analyzer.
- R/r** Enable/disable recursive scan;
- S/s** Enable/disable the mode of opening symlinks;
- l** Scan local file systems only.

Report generation options:

- q** Do not print messages to the screen;
- o <name>** Specify the filename for the file into which report about the operation of the component will be logged; if the filename is not specified, the report will not be generated;
- j<number>** Specify the report detail level based on the amount of information contained in this report. The following detail level may be used as an **<option>**:
- 1** Enable/disable display of messages about other errors;
 - 2** Enable/disable display of information messages;
 - 3** Enable/disable display of messages about scan;
- x <option>** Specify detail level for the scan report printed to the screen. The following detail level may be used as an **<option>**:

following detail level may be used as an **<option>**:

- | | |
|------------|--|
| O/o | Short/extended format for messages about scan of a simple object; |
| C/c | Short/extended format for messages about scan of an archive; |
| N/n | Enable/Disable printing messages about clean files to the screen. |
| P/p | Enable/Disable printing messages about the current operation of the component to the screen. |
- m <option>** Specify detail level for the scan report printed into the report file. The following modes may be used as an **<option>**:
- | | |
|------------|--|
| O/o | Short/extended format for messages about scan of a simple object; |
| C/c | Short/extended format for messages about scan of an archive; |
| N/n | Enable/Disable printing messages about clean files to the report file. |

File options:

- p<option>**
<file_name> Save the list of objects into the specified file; save each object with the full path in a new line. The following modes may be used as an **<option>**:
- | | |
|----------|---|
| i | Save the list of infected objects into file <file_name> ; |
| s | Save the list of suspicious objects into file <file_name> ; |
| c | Save the list of corrupted objects into file <file_name> ; |
| w | Save the list of object the code of which resembles the code of a know virus to file <file_name> . |
- @ <filelist.lst>** Scan objects path to which is specified in file **<filelist.lst>**.

File processing options (the use of these modifiers in the command line cancels the execution of actions defined in the configuration file):

- i0** Scan for viruses only;
- i1** Disinfect infected objects; skip if disinfection is not possible;
- i2** Disinfect infected object; if disinfection is not possible and if the object is a simple object - delete it; do not delete infected objects from the container.
- i3** Disinfect infected object; if disinfection is not possible and if the object is a simple object - delete it; if the infected object is located in the container – delete the entire container.
- i4** Delete infected objects and containers.

A.3. Return codes of the kavscanner component

During its operation the kavscanner component may return the following codes:

- 0** No viruses found;
- 5** All infected objects have been disinfected;
- 10** Password-protected archives detected;
- 15** Corrupted files detected;
- 20** Suspicious files detected;
- 21** Files that contain code that resembles the code of known viruses detected;
- 25** Infected files detected;
- 30** System error occurred during the file scan;

- 50 Unable to load the anti-virus database (path specified in the configuration file, not found);
- 55 The anti-virus database has been corrupted;
- 60 The Anti-Virus database date stamp is beyond the license key period;
- 64 License information is missing or no license keys have been found at the location path to which was specified in the configuration file;
- 66 Invalid configuration file option
- 65 Unable to load configuration file;
- 70 The kavscanner component has been corrupted;
- 75 The kavscanner component has been corrupted and cannot be fixed.

A.4. Command line modifiers for component kavmonitor

Help options:

- h Display help information about the component to the screen;
- v Display the application version.

Configuration options:

- c<path_to_file> Use alternative configuration file <path_to_file>;

A.5. Command line modifiers for component licensemanager

Help options:

- h** Display help information about the *licensemanager* component to the screen;

License keys managing options:

- s** Display information about all installed license keys to the screen;
- c (-C) <path_to_file>** Use alternative configuration file **<path_to_key_file>**;
- k<path_to_file>** Display information about key **<path_to_key_file>** on the screen;
- a<path_to_file>** Install the license key **<path_to_key_file>**;
- d<path_to_file>** Remove license key.

A.6. Return codes of the *licensemanager* component

During its operation the *licensemanager* component may return the following codes:

- 0** The component successfully loaded information about the license key and successfully completed its operation.
- 30** System error occurred during the component's operation;
- 64** License information is missing or no license keys were found at the path specified in the configuration file;
- 65** Unable to load configuration file;
- 66** Invalid configuration file option.

A.7. Command line modifiers for component keepup2date

Help options:	
-v	Print to the screen the version of the application and close the component.
-h	Print to the screen help information about the command line modifiers supported by the component and close the component;
-s	Print the list of the updates servers to the screen;
Operation options:	
-r	Rollback of the last update to the previous version;
-k	Do not execute PostUpdateCmd command after the anti-virus database update has been successfully completed.
-q	The mode of the component operation during which no system messages will be printed to the screen.
-e	The mode of the component operation during which only messages about critical errors will be printed to the screen.
-x<path_to_file>	Copy all updates of the anti-virus database into local folder <path_to_file> ;
-g <URL>	Address for updating the anti-virus database. When this modifier is specified, the update will be performed from this address.
-d<path_to_file>	Use pid-file of the component, located in local folder <path_to_file> .
Report generation options:	
-l<path_to_file>	Log the results of the component's operation in file <path_to_file> .

A.8. Return codes of the **keepup2date** component

During its operation the *keepup2date* component may return the following codes:

0	The anti-virus database does not need to be updated;
1	The anti-virus database has been updated successfully;
10	Critical error occurred, the updating process will be terminated;
12	Error occurred during the rollback to the last update of the anti-virus database;
30	Could not run command PostUpdateCmd after the anti-virus database update;
60	License information is missing or no license keys were found at the path specified in the configuration file;
75	Unable to load the configuration file or settings error.

APPENDIX B. 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: Kaspersky Anti-Virus does not rescan file. Why?

In fact, Kaspersky Anti-Virus does not rescan file that have not been modified since the last scan.

This is possible due to the use of new technology iChecker™. This technology is implemented utilizing the objects' checksums database.



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. However, each new version of the product works faster than the previous version, despite the daily increase in the total number of viruses detectable with Kaspersky Anti-Virus (about 30 new viruses daily) and the continuous increase in the number of formats that can be processed. This is possible due to the use of new unique technologies, such as iChecker™, developed by Kaspersky Lab.



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 bases 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: The Kaspersky Anti-Virus license key is written on a floppy disk. What should I do if I do not have a floppy drive?

This problem can be resolved in several ways.

You can describe the problem in a message that you should send to the Kaspersky Lab's Sales Department (sales@kaspersky.com). Please make sure to indicate the date and the place of the purchase of Kaspersky Anti-Virus and its full registration number. Managers of the Sales Department will send the license key file to the e-mail address you provided in this message.

You can also read the content of the floppy disk on another computer equipped with a floppy drive and write it to a medium readable on your computer. Select this drive as the license key source drive during the Kaspersky Anti-Virus installation.

You can also read the content of the floppy disk on another computer equipped with a floppy drive and send the license key file to your e-mail address. Receive the message on your computer, save the file in any folder on your hard drive and select this folder as the license key source folder during the Kaspersky Anti-Virus installation.



Question: *My Anti-Virus does not work.*

What should I do?

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

We also recommend that you contact the dealer you purchased your copy of Kaspersky Anti-Virus from or refer to the Knowledge Base at Kaspersky Lab's website (<http://www.kaspersky.ru/faq>).



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 every year. Now the anti-virus database is updated at the server every three hours.

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



Question: What changed in the update service starting with version 5.0?

The new Kaspersky Lab's range of products, starting with version 5.0, features a new update service. This service was developed based on the users' feedback and marketing requirements. Additionally, the developers had a task to increase the processability of the entire updates procedure starting with creation of updates at Kaspersky Lab through file updates at the user's side.

The advantages of the new update service are as follows:

- Resuming downloading in case of a disconnection. *Now you do not have to download over again those updates that you already received if a disconnection from the network occurred.*
- The cumulative updates size has been decreased in half. The cumulative update contains the entire anti-virus database, therefore its size considerably exceeds the size of a regular update. The new service uses a special technology that allows using the database you already have for the cumulative update.
- Downloading updates from the internet has become faster. Now Kaspersky Anti-Virus selects the Kaspersky Lab's updates server located in your region. Additionally, the load on the server will be distributed in accordance with their throughput, it means that you will not be connected to an overloaded server while another server is idle.
- The use of key "black lists". This allows preventing updates to be performed by those users who do not have license for using Kaspersky Anti-Virus. Therefore properly licensed users will not suffer from the servers overload.

- For the corporate products, the ability to create local updates servers has been implemented. This function is needed for organizations that use a single local area network comprised of computers protected by Kaspersky Lab's applications. In this case any computer may be used as the updates server that will receive update from the internet, place them into a local folder and provide access to this folder to all other computers in the network.



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 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: will Kaspersky Anti-virus work under my Linux OS version?

Kaspersky Anti-Virus 5.5 was tested for operation under RedHat, Debian and SUSE and Mandriva Linux OS and the Kaspersky Anti-Virus distribution packages were issued exactly for these flavors of Unix.

Details on the supported operating systems see section 1.5 on page 9.

The application may perform improperly when run under versions not included into the list of version supported by Kaspersky Lab. This is, first of all, related to the specifics of the operating system. For example your operating system may use a different library version or non-standard location of the system initialization scripts. In this case, Kaspersky Lab's Technical Support Service will not be able to help you.



Question: Why does the *kavmonitor* component start several processes at the same time?

The number of processes started by *kavmonitor* is defined by the **CheckFileLimit** setting of the application's configuration file and determines the number of files processed at the same time. Therefore the number of the monitor processes always exceeds 1 (by default 20 proc-

esses will be started). If there are no files to be scanned, the processes do not consume any system resources.



Question: Is it possible to control Kaspersky Anti-Virus using Network Control Centre for Windows?

Controlling Kaspersky Anti-Virus for Linux and FreeBSD Workstation and File Server using Network Control Centre for Windows is impossible. In this version we provided for the ability to remotely configure the application using a special module for Webmin package.



Question: How can I save to a file the content of what the application prints to the screen?

In order to save information that Kaspersky Anti-Virus prints to the screen during its operation, you have to configure the corresponding setting in the configuration file or enter the following in the command line:

```
$ some_app > ./text_file 2>&1
```

where:

`some_app` – application the standard input and output error messages of which you wish to save into the file;

`text_file` – full path to the file in which the information will be stored.

For example,

```
$kav4fs-keepup2date > ./updater.log 2>&1
```

In this case, standard output messages and error messages of the `keepup2date` component will be logged into file `updater.log`.

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 Office Outlook and Microsoft Outlook Express
- protection of your computer from unauthorized access, and also from network hacker attacks from your LAN or the Internet.

Kaspersky Lab News Agent

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

The product performs the following functions:

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

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

Kaspersky® OnLine Scanner

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

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

Kaspersky® OnLine Scanner Pro

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

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

Kaspersky Anti-Virus® 6.0

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

The program provides for complex anti-virus checks including:

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

Proactive protection offers the following features:

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

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

Kaspersky® Internet Security 6.0

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

The anti-virus protection feature includes:

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

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

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

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

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

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

Kaspersky® Security for PDA

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

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

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

Kaspersky Anti-Virus Mobile

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

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

Kaspersky Anti-Virus® Business Optimal

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

Kaspersky Anti-Virus® Business Optimal guarantees full-scale anti-virus 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 Linux; *Samba* file storage
- *E-mail systems* including Microsoft Exchange 2000/2003, Lotus Notes/Domino, postfix, exim, sendmail, and qmail mail systems
- *Internet gateways*: CheckPoint Firewall –1; Microsoft ISA Server 2000 Standard Edition, Microsoft ISA Server 2004 Standard Edition

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

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

Kaspersky® Corporate Suite

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

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

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

¹ Depending on the type of distribution kit.

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

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

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

Kaspersky® Anti-Spam

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

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

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

Kaspersky Security® for Microsoft Exchange 2003

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

Kaspersky® Mail Gateway

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

Kaspersky Anti-Virus® for Proxy Servers

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

Kaspersky Anti-Virus® for MIMESweeper for SMTP

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

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

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 e-mail. Rest assured that all of your recommendations and suggestions will be thoroughly reviewed and considered.

Technical support	Please find the technical support information at http://www.kaspersky.com/supportinter.html Helpdesk: www.kaspersky.com/helpdesk.html
General information	WWW: http://www.kaspersky.com http://www.viruslist.com E-mail: info@kaspersky.com

APPENDIX D. LICENSE AGREEMENT

Standard End User License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (“AGREEMENT”), FOR THE LICENSE OF KASPERSKY INTERNET SECURITY (“SOFTWARE”) PRODUCED BY KASPERSKY LAB (“KASPERSKY LAB”).

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

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

IN ACCORDANCE WITH THE LEGISLATION, REGARDING KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS PURCHASED ONLINE FROM THE KASPERSKY LAB OR ITS PARTNER’S INTERNET WEB SITE, CUSTOMER SHALL HAVE A PERIOD OF FOURTEEN (14) WORKING DAYS AS FROM THE DELIVERY OF PRODUCT TO MAKE RETURN OF IT TO THE MERCHANT FOR EXCHANGE OR REFUND, PROVIDED THE SOFTWARE IS NOT UNSEALED.

REGARDING THE KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS NOT PURCHASED ONLINE VIA INTERNET, THIS SOFTWARE NEITHER WILL BE RETURNED NOR EXCHANGED EXCEPT FOR CONTRARY PROVISIONS FROM THE PARTNER WHO SELLS THE PRODUCT. IN THIS CASE, KASPERSKY LAB WILL NOT BE HELD BY THE PARTNER’S CLAUSES.

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

All references to “Software” herein shall be deemed to include the software activation code with which you will be provided by Kaspersky Lab as part of the Kaspersky Internet Security 6.0.

1. *License Grant.* Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, Kaspersky Lab hereby grants you the non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the "Documentation") for the term of this Agreement solely for your own internal business purposes. You may install one copy of the Software on one computer.

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

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

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

1.1.3 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 (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.

2. Support.

(i) Kaspersky Lab will provide you with the support services (“Support Services”) as defined below for a period of one year since the moment of activation on:

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

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

Support Services shall become available after Software activation. Kaspersky Lab’s technical support service is also entitled to demand from the End User additional registration for identifier awarding for Support Services rendering.

Until Software activation and/or obtaining of the End User identifier (Customer ID) technical support service renders only assistance in Software activation and registration of the End User.

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

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

(iv) “Support Services” means:

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

(b) Updates of network attacks database;

(c) Updates of anti-spam database;

(d) Free software updates, including version upgrades;

(e) Technical support via Internet and hot phone-line provided by Vendor and/or Reseller;

(f) Virus detection and disinfection updates in 24-hours period.

(v) Support Services are provided only if and when you have the latest version of the Software as available on the official

Kaspersky Lab website (www.kaspersky.com) installed on your computer.

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

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

5. *Limited Warranty.*

- (i) Kaspersky Lab warrants that for six (6) months from first download or installation the Software purchased on a physical medium will perform substantially in accordance with the functionality described in the Documentation when operated properly and in the manner specified in the Documentation.
- (ii) You accept all responsibility for the selection of this Software to meet your requirements. Kaspersky Lab does not warrant that the Software and/or the Documentation will be suitable for such requirements nor that any use will be uninterrupted or error free.
- (iii) Kaspersky Lab does not warrant that this Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.
- (iv) Your sole remedy and the entire liability of Kaspersky Lab for breach of the warranty at paragraph (i) will be at Kaspersky Lab option, to repair, replace or refund of the Software if reported to Kaspersky Lab or its designee during the warranty period. You shall provide all information as may be reasonably necessary to assist the Supplier in resolving the defective item.

- (v) The warranty in (i) shall not apply if you (a) make or cause to be made any modifications to this Software without the consent of Kaspersky Lab, (b) use the Software in a manner for which it was not intended, or (c) use the Software other than as permitted under this Agreement.
- (vi) The warranties and conditions stated in this Agreement are in lieu of all other conditions, warranties or other terms concerning the supply or purported supply of, failure to supply or delay in supplying the Software or the Documentation which might but for this paragraph (vi) have effect between the Kaspersky Lab and your or would otherwise be implied into or incorporated into this Agreement or any collateral contract, whether by statute, common law or otherwise, all of which are hereby excluded (including, without limitation, the implied conditions, warranties or other terms as to satisfactory quality, fitness for purpose or as to the use of reasonable skill and care).

6. *Limitation of Liability.*

- (i) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for (a) the tort of deceit, (b) death or personal injury caused by its breach of a common law duty of care or any negligent breach of a term of this Agreement, or (c) any other liability which cannot be excluded by law.
- (ii) Subject to paragraph (i) above, Kaspersky Lab shall bear no liability (whether in contract, tort, restitution or otherwise) for any of the following losses or damage (whether such losses or damage were foreseen, foreseeable, known or otherwise):
 - (a) Loss of revenue;
 - (b) Loss of actual or anticipated profits (including for loss of profits on contracts);
 - (c) Loss of the use of money;
 - (d) Loss of anticipated savings;
 - (e) Loss of business;
 - (f) Loss of opportunity;
 - (g) Loss of goodwill;
 - (h) Loss of reputation;

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

7. This Agreement contains the entire understanding between the parties with respect to the subject matter hereof and supersedes all and any prior understandings, undertakings and promises between you and Kaspersky Lab, whether oral or in writing, which have been given or may be implied from anything written or said in negotiations between us or our representatives prior to this Agreement and all prior agreements between the parties relating to the matters aforesaid shall cease to have effect as from the Effective Date.