

KASPERSKY LAB

Kaspersky Anti-Virus[®] 5.7 for Linux File Server

ADMINISTRATOR'S GUIDE

KASPERSKY ANTI-VIRUS[®] 5.7 FOR
LINUX FILE SERVER

Administrator's Guide

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

Revision date: September, 2008

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 5.7?	8
1.4. Licensing procedure	8
1.5. Hardware and software system requirements	8
1.6. Distribution kit	10
1.6.1. License Agreement	10
1.6.2. Services for registered users	10
1.7. Conventions used in this document	11
CHAPTER 2. HOW IT WORKS	12
CHAPTER 3. INSTALLING KASPERSKY ANTI-VIRUS	14
3.1. Installing the application on a computer running Linux	14
3.2. Installation procedure	14
3.3. Post-install configuration	15
3.4. Installing Network Agent	16
3.5. Configuring Network Agent	16
3.6. Updating the application to version 5.7	17
3.7. Locating the application files	17
3.8. Completing the setup	19
CHAPTER 4. USING KASPERSKY ANTI-VIRUS	20
4.1. Updating the anti-virus database	20
4.1.1. Automatically updating the anti-virus database	21
4.1.2. On-demand updating of the anti-virus database	23
4.1.3. Creating a network directory to store the anti-virus database	24
4.2. Anti-virus protection of file systems	25
4.2.1. Scan scope	26
4.2.2. Object scan and disinfection mode	27
4.2.3. Actions to be performed on objects	28
4.2.4. On-demand scan of an individual directory	29
4.2.5. Scheduled scan	29

4.2.6. Additional capabilities: using script files	30
4.2.6.1. Disinfection of infected objects in an archive	30
4.2.6.2. Sending notifications to the administrator	31
4.3. Real-time anti-virus protection.....	32
4.4. Managing license keys	33
4.4.1. Viewing license key details.....	33
4.4.2. Renewing your license	35
CHAPTER 5. ADDITIONAL SETTINGS	37
5.1. Configuration of product interaction with Webmin	37
5.2. Optimization of Kaspersky Anti-Virus operation	38
5.3. Moving objects into quarantine	40
5.4. Backing up infected objects	41
5.5. Localization of the date and time format.....	42
5.6. Kaspersky Anti-Virus report generation settings.....	42
CHAPTER 6. ADMINISTERING THE PROGRAM WITH KASPERSKY ADMINISTRATION KIT	45
6.1. Administering the application	47
6.1.1. Configuring application settings.....	48
6.1.1.1. Settings tab, Real-time protection: general settings section.....	49
6.1.1.2. Settings tab, Real-time protection: protection scope section.....	50
6.2. Managing tasks	50
6.2.1. Creating tasks	50
6.2.1.1. Creating local tasks.....	52
6.2.1.2. Creating group tasks.....	54
6.2.1.3. Creating global tasks	54
6.2.2. Configuring specific task settings.....	54
6.2.2.1. On-demand scan task.....	55
6.2.2.2. Anti-virus database update task	56
6.2.3. Starting and stopping tasks	56
6.3. Managing policies	57
6.3.1. Creating policies.....	57
6.3.2. Viewing and editing policy settings	59
6.3.2.1. Configuring the protection scope.....	60
6.3.2.2. Specifying object types to be protected.....	61
6.3.2.3. Configuring actions applied to objects.....	61

6.3.2.4. Specifying additional parameters	61
CHAPTER 7. UNINSTALLING KASPERSKY ANTI-VIRUS.....	62
CHAPTER 8. VERIFYING THE ANTI-VIRUS OPERATION.....	63
APPENDIX A. ADDITIONAL INFORMATION ABOUT THE APPLICATION.....	65
A.1. Kaspersky Anti-Virus configuration file.....	65
A.2. Command line parameters for component kavscanner	73
A.3. Return codes of the kavscanner component	76
A.4. Command line parameters for component kavmonitor	77
A.5. Command line parameters for component licensemanager	78
A.6. Return codes of the licensemanager component.....	78
A.7. Command line parameters for component keepup2date	80
A.8. Return codes of the keepup2date component.....	81
A.9. Command line parameters for component kavmiddleware.....	81
APPENDIX B. FREQUENTLY ASKED QUESTIONS.....	82
APPENDIX C. KASPERSKY LAB	88
C.1. Other Kaspersky Lab Products	89
C.2. Contact Us.....	99
APPENDIX D. LICENSE AGREEMENT.....	100

CHAPTER 1. INTRODUCTION

The constant growth in both the number of computer users, and the volume of e-mail and internet traffic, increases the threat of virus infections and data corruption or theft by malicious computer programs (malware).

The most dangerous sources of malware are:

Internet

The global information network is the main conduit for all types of malware. As a rule, viruses and other malicious programs are located on popular internet websites, disguised as useful software or freeware. Malware can also be located within 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 e-mail databases may contain viruses. Malware can be located either in the message body, or as a message attachment. Commonly, 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.

Viruses targeting Unix-based systems are far less common than those aimed at the Windows Operating System, due to the peculiarities of the two platforms. However, the threat to Unix users is not negligible. Provided below is a detailed description of malware types.

1.1. Computer viruses and malware

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

- **Worms** – malicious programs which spread themselves using network resources. These programs are called "worms" due to their ability to tun-

nel from one computer to another, using networks, e-mail and other channels. This ability allows worms to proliferate extremely quickly.

Worms propagate by penetrating a computer, determining the IP addresses of other nearby computers, and send copies of themselves to these computers. Apart from 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 other than RAM.

- **Viruses** – programs that *infect* other programs by adding their code to the infected program's code, to gain control when the infected files are run. This simple definition helps determine that the major action of a virus 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, or steal confidential information. In the strict sense, Trojan Horses are not viruses since they do not infect programs or data; they are unable to sneak independently into computers and are often distributed disguised as some "useful" software. However, Trojans may inflict far greater damages than 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 File Server (hereinafter referred to as *Kaspersky Anti-Virus*, or *the application*) protects file servers running Linux operating systems.

Kaspersky Anti-Virus for Linux allows the user to:

- *Ensure real-time protection of the file system against malicious code:* intercept and analyze attempts to access files, and disinfect or delete infected objects.

- *Scan objects on demand:* search infected and suspicious files (including files within specified scan scopes); analyze files, and disinfect or delete infected objects.
- *Quarantine suspicious and corrupted objects:* save suspicious files in the quarantine directory.
- *Create a copy of the infected object in the backup storage directory* before attempting to disinfect or deleting the object, allowing a future restoration of the object if it contains valuable information.
- *Update the anti-virus database;* the database is updated from Kaspersky Lab's updates servers. The user can also configure the application so that the database is updated from a local directory.
- *Control and configure Kaspersky Anti-Virus* using the application configuration file, the web-based interface of Webmin or the Kaspersky Administration Kit.

1.3. What's new in version 5.7?

The following features are new in **Kaspersky Anti-Virus 5.7 for Linux File Server** as compared to version 5.5:

- Support for Kaspersky Anti-Virus configuration and management using Kaspersky Administration Kit has been implemented.

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

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:
 - One of the following operating systems for 32-bit platforms:
 - Red Hat Enterprise Linux 5.2 server;
 - Fedora 9;
 - SUSE Linux Enterprise Server 10 SP2;
 - Novel Open Enterprise Server 2;
 - openSUSE Linux 11;
 - Debian GNU/Linux 4 R4;
 - Mandriva Corporate Server 4;
 - Ubuntu 8.04.1 Server Edition;
 - One of the following operating systems for 64-bit platforms:
 - Red Hat Enterprise Linux 5.2 server;
 - Fedora 9;
 - SUSE Linux Enterprise Server 10 SP2;
 - openSUSE Linux 11.
- 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 must be installed.
- Software compilation packages must be installed (gcc, binutils, glibc-devel, make, ld) and preinstalled operating system kernel source code for compiling the *kavmonitor* component.



Please note that Kaspersky Anti-Virus does not support systems running SELinux. Use of SELinux may result in various warnings in the system log file generated by the application.

1.6. Distribution kit

You can purchase Kaspersky Anti-Virus online (for example, visit <http://www.kaspersky.com> and follow the **E-Store** link).

If you buy Kaspersky Anti-Virus online, you will download the application from 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 receipt of your payment.

1.6.1. License Agreement

The License Agreement is a legal contract between you and Kaspersky Lab Ltd., which contains the terms and conditions under 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.

1.6.2. Services for registered users

Kaspersky Lab Ltd. offers 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 receive the following services:






- 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 e-mail;
- information about new Kaspersky Lab products and about new viruses appearing worldwide (this service is provided to users who subscribe to Kaspersky Lab's newsletter).



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

1.7. Conventions 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 user's steps and possible actions
 Task, example	Statement of a problem, example of the demonstration of the application's capabilities
 Solution	Implementation of the task
[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. HOW IT WORKS

To understand how Kaspersky Anti-Virus works, it is useful to know that it comprises a number of application modules, each with a specific function in providing anti-virus protection for your computer.

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 utility for integration with Kaspersky Administration Kit *kavmiddleware*,
- *Remote administration module* used with Webmin application.

There follows a detailed discussion of the application's algorithm, based on an example of real-time protection (that is, using the *kavmonitor* component).

The component operates as follows:

1. When any application on your computer attempts to access a file system object, whether to open, run or close the file, the call is intercepted by *kavmonitor*'s kernel module, and the file is sent for anti-virus scanning.



The ability to intercept the operations of closing a file is not supported:

- in 32-bit operating systems: from kernel versions 2.6.21 and above;
 - in 64-bit operating system: from kernel versions 2.6.18 and above.
2. The intercepted file is processed using a daemon application included in the *kavmonitor* component. The daemon scans the object for viruses and processes, based on settings specified in the configuration file. The treatment includes, but is not limited to, disinfection using the anti-virus database if this option is selected.
 3. After the file has been processed, *kavmonitor* sends to the kernel module the access code (allowed/prohibited) that defines the file status.

4. Based on the object's status, the *kavmonitor* component either allows or blocks access to the file. If access is blocked, the application requesting access to the file will receive an error code indicating that access has been denied.

The file status assigned during scanning 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** – the infected object could not be disinfected.
- **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.

The actions performed on the object in response to each status are defined by the configuration file settings (details see Appendix A on p. 65).

CHAPTER 3. INSTALLING KASPERSKY ANTI-VIRUS

We recommend that you perform this system check before installing Kaspersky Anti-Virus:

- Make sure that your system meets the hardware and software requirements for Kaspersky Anti-Virus (see 1.5 on p. 8).
- 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 the following format:

- **.rpm** – for systems that support RPM Package Manager
- **.deb** – for Debian-based OS distributions.



To start the installation of Kaspersky Anti-Virus from a .rpm package, type the following at the command line:

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



To start the installation of Kaspersky Anti-Virus from a .deb package, type the following at the command line:

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

3.2. Installation procedure

The installation consists of two parts. The first part includes the following steps:

1. Creation of the kluser user and klusers group.
2. Unpacking of the files from distribution package to target computer.

3. Registration of required services depending upon the host system.
4. Setting up default parameters in configuration files of the product components.

3.3. Post-install configuration

Post-install configuration is the second part of Kaspersky Anti-Virus setup. To initiate product configuration, use the *postinstall.pl* script located in the */opt/kaspersky/kav4fs/lib/bin/setup* directory.



During installation to a computer running Debian the post-install configuration script will be launched automatically.

After script start, you will be offered to perform the following steps:

1. Specify the path to your license key file.
2. Configure the parameters of the proxy server used for connection to the Internet in the following format:

```
http://<IP of the proxy server>:<port>
```

or

```
http://<user_name>:<password>@<IP of the proxy server>:  
<port>,
```

depending upon authorization necessity for the proxy. The updating component of the application (*keepup2date*) uses the value for connection to the servers of Kaspersky Lab and downloading updates to the anti-virus databases.

If you do not use a proxy for connection to the Internet, set the parameter to **no**.

3. Download the anti-virus databases from the servers of Kaspersky Lab. Enter **yes** or **no** depending upon your wish to perform the update immediately.
4. Configure interaction with Webmin.
5. Start compilation of the *kavmonitor* module. During the stage your computer will compile the libraries required for *kavmonitor* operation. If the kernel source code is not located in the default directory, enter the following in the command line to compile the *kavmonitor* component:

```
# /opt/kaspersky/kav4fs/src/kavmon.pl -b [PATH]
```

where [PATH] stands for the path to the kernel source code.

3.4. Installing Network Agent

If you plan to manage the application remotely using Kaspersky Administration Kit, the Network Agent has to be installed.



To initiate Network Agent installation from its .rpm package, enter the following in the command line:

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



To initiate Network Agent installation from its .deb package, enter the following in the command line:

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

3.5. Configuring Network Agent

After installation, the Network Agent has to be configured for its proper interaction with Kaspersky Administration Kit. To start configuration, run the *postinstall.pl* script located in the */opt/kaspersky/klnagent/lib/bin/setup* directory.



During Network Agent installation to a computer running Debian the post-install configuration script will be launched automatically.

After script start, you will be offered to perform the following steps:

1. Specify the DNS name or IP address of your Administration Server.
2. Specify the port number for the Administration Server.
3. Specify the SSL port number of the Administration Server.
4. Define whether the SSL connection should be used for data transfer.
5. Specify the default administration group name.

3.6. Updating the application to version 5.7



The upgrading procedure works correctly for version 5.5-27.

The *kavmonitor* service has to be stopped before upgrading. To do that, enter the following in the command line:

```
# /etc/init.d/kav4fs stop
```



To initiate Kaspersky Anti-Virus upgrade from its *.rpm* package, enter the following in the command line:

```
# rpm -U <distribution_package_filename>
```



To initiate Kaspersky Anti-Virus upgrade from its *.deb* package, enter the following in the command line:

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

Upon completion of the upgrade procedure, the configuration file of product version 5.5 will be replaced with its counterpart for version 5.7. Add necessary modifications to the configuration file manually.

3.7. Locating the application files



The default locations of Kaspersky Anti-Virus files on a server running Linux OS are as follows:

/etc/opt/kaspersky/ – directory containing the Kaspersky Anti-Virus configuration file:

kav4fs.conf – configuration file.

/opt/kaspersky/kav4fs/ – main directory of Kaspersky Anti-Virus, containing:

/bin/ – a directory 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/ – directory containing auxiliary files of Kaspersky Anti-Virus.

/setup/ – directory containing the scripts required for application configuration:

postinstall.pl – script for post-install product configuration.

uninstall.pl – application removal script.

setup.pl – application configuration script.

/sbin/ – directory containing auxiliary services of Kaspersky Anti-Virus:

kav4fs-kavmonitor – executable file of the anti-virus protection component.

kav4fs-kavmiddleware – executable file of the remote administration component *kavmiddleware*.

/src/ – directory containing the application's anti-virus kernel module.

/opt/kaspersky/kav4fs/share/contrib/kav4fs.wbm – plug-in to Webmin application.

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

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

/opt/kaspersky/kav4fs/share/man/ – directory containing manual files.

/var/opt/kaspersky/kav4fs/bases/ – directory containing the anti-virus database.

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

/var/opt/kaspersky/kav4fs/licenses – directory containing license information.



To connect the help system of Kaspersky Anti-Virus (manual pages), assign the value ***/opt/kaspersky/kav4fs/share/man*** to the **MANPATH** environment variable.



On a server running Linux OS, the default locations of Network Agent files after Kaspersky Anti-Virus installation are as follows:

/opt/kaspersky/klnagent/ – main Network Agent directory containing:

/bin/ – directory where the executable files of Network Agent utility programs are stored, including:

klmover – this utility manually connects the client computer to the Administration Server (see the Kaspersky Administration Kit Reference Book for more information on using this utility).

klnagchk – this utility checks the manual connection to the *Administration Server* (see the Kaspersky Administration Kit Reference Book for more information on using this utility).

/lib/ – directory containing auxiliary files of the *Network Agent*.

/bin/setup – directory containing configuration scripts for *Network Agent*.

/share/man/ – directory containing manual files.

/sbin/ – directory containing the executable file of the *Network Agent* service.

3.8. Completing the setup

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

CHAPTER 4. USING KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus allows you to specify the anti-virus protection system of your computer, at the level either of individual files or of the entire file system.

The application's functionality can be packaged into tasks that the administrator can perform using the application. Tasks implemented using Kaspersky Anti-Virus can be divided into the following groups:

- Updating the anti-virus database, which is used for detecting viruses and disinfecting infected objects (see 4.1 on p. 20).
- Anti-virus protection of the computer's file system, using scheduled and/or on-demand scans (see 4.2 on p. 25).
- Real-time anti-virus protection (see 4.3 on p. 31).

This chapter describes these typical tasks. Within the context of a specific company's network, the administrator may combine these tasks and make them more appropriate to business needs.

4.1. Updating the anti-virus database

Updating the anti-virus database is performed by the *keepup2date* component, and is an integral factor in full-fledged anti-virus protection. The default source used for updating the anti-virus database is Kaspersky Lab's updates servers. The list of these 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 in the application's distribution kit. To view the list of update servers, enter the following in the command line:

```
# /opt/kaspersky/kav4fs/bin/kav4fs-keepup2date -s
```

During the update process, the *keepup2date* component selects the first address from this list and attempts to download the anti-virus database from the server. The current computer location (as the two-lettered code of the country according to the ISO 3166-1 standard) can be specified via the **RegionSettings** parameter

in the **[updater.options]** section of the application configuration file. In this case the *keepup2date* component starts choosing the update servers, marked as belonging to the specified region. If the update cannot be performed from the address selected, the component switches to the next URL and makes another attempt.



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



You can use a server that does not belong to Kaspersky Lab as an update source. Databases of Kaspersky Anti-Virus on the server can be released earlier than the ones installed on your computer. In case of an update from such server, the outdated databases will replace more current records.

After a successful update, a command, specified by the **PostUpdateCmd** parameter of the configuration file's **[updater.options]** section, is executed. By default this command automatically reloads the anti-virus database. If an invalid change is made to this 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.*]** section of the configuration file.

If the structure of your local area network is complex, you are advised to download updates to the anti-virus database from the updates servers every hour, place them in a network directory, and configure local computers throughout the network to use this directory as their update source. For details on the creation of a network directory, see 4.1.3 on p. 24.

The update may be scheduled using the **cron** utility (see 4.1.1 on p. 21) or it may be performed on-demand by the administrator who can run this task manually from the command line (see 4.1.2 on p. 23).



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

4.1.1. 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 hour. Only record application errors in the system log. Maintain the general log for all tasks started, and do not print any information to the screen.



Solution: to perform this task, do the following:

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

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

2. Edit the configuration file for the cron (**crontab -e**) process by entering the following line:

```
0 0-23/1 * * * /opt/kaspersky/bin/kav4fs-keepup2date
```



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



Solution: to perform this task, do the following:

Assign the value **No** to the **UseUpdateServerUrl** setting in the **[updater.options]** section of the application's configuration file.



Task: configure the component to download updates to 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: to perform this task, do the following:

Assign the value **Yes** to both 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 component to download updates to the anti-virus database from a specified URL. If the download cannot be performed from this URL, update the database from the URLs specified in the list included in the *keepup2date* component.



Solution: to perform this task, do the following:

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

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

You can start the update of the anti-virus database from the command line at any time. To do that, type the following command:

```
# /opt/kaspersky/kav4fs/bin/kav4fs-keepup2date
```



Task: start the update of the anti-virus database and record the results in the file */tmp/updatesreport.log*.



Solution: to implement this task enter at the command line:

```
# /opt/kaspersky/kav4fs/bin/kav4fs-keepup2date -l  
/tmp/updatesreport.log
```

The most convenient way to update the anti-virus database on several computers is to download the updates once from the updates servers, place the updates in a network directory and then direct the computers to treat this directory as their update source.



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



Solution: 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 at the command line:

```
# /opt/kaspersky/kav4fs/bin/kav4fs-keepup2date -l
/tmp/report.txt
```

4.1.3. Creating a network directory to store the anti-virus database

To ensure that the anti-virus database is correctly updated from the network directory, the directory must contain the same file structure as Kaspersky Lab's updates servers. Provided below is a detailed discussion of this task.



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



Solution: to perform this task, do the following:

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

```
# /opt/kaspersky/kav4fs/bin/kav4fs-keepup2date -u
<dir>
```

where <dir> is the full path to the local directory.

3. Grant local computers read-only network access to this catalog.



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



Solution: to perform this task, do the following:

1. Assign the 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 format **http://username:password@ip_address:port**. The values **ip address** and **port** are mandatory, while **username** and **password** are necessary only if the proxy server requires authorization.

or:

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

4.2. Anti-virus protection of file systems

The *kavscanner* component provides anti-virus protection of the computer's file systems, by scanning files and processing infected and suspicious objects according to 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 scan the entire file system, an individual directory or a single file. All protection settings may be divided into groups that define:

- Scan scope (see 4.2.1 on p. 26).
- How objects are to be scanned and disinfected (see 4.2.2 on p. 27).
- Actions to be performed on objects (see 4.2.3 on p. 28).
- Settings used to generate the report on the operation's outcome (see 5.6 on p. 42).

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

- As a one-time task - from the command line (see 4.2.4 on p. 29).
- According to the schedule using the **cron** application (see 4.2.5 on p. 29).



An 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 recommend that no other heavy application should run at the same time. To avoid such problems, we recommend that you scan individual selected catalogs.

4.2.1. Scan scope

The scan scope can be roughly divided into two parts:

- *scan path* – the list of directories and objects to be searched for viruses;
- *scan objects* – types of objects to be scanned for viruses (archives, etc.)

By default all objects of all available file systems are scanned, starting with the current directory.



To scan all file systems of the computer, you have to switch to the root directory, or specify the scan scope at the command line as `"/`.

You can redefine the scan path by the following methods:

- Listing at the command line (using a space as a separator) all directories and files to be scanned, using absolute or relative (relative to the current directory) paths.
- List the scan paths in a text file, and specify this file to be used by using the parameter `-@<filename>` in the command line. Each object in this file should be entered on a new line, using its absolute path only.



If you specified at the command line both scan paths and a text file containing a list of the scan objects, only the paths indicated in the file will be scanned. The paths entered at the command line will be ignored.

- Restrict paths which are accepted by default (all, starting with the current directory) or listed in the command line, by entering in the **kav4fs.conf** configuration file masks of files and directories that will be excluded from the scan scope (**[scanner.options]** section, settings **ExcludeMask** and **ExcludeDirs**).

- Turn off the *recursive scan of the catalogs* (**[scanner.options]** section, the **Recursion** setting or command line parameter **-r**).
- Create an alternative configuration file and specify this file to be used using the command line parameter **-c <filename>** at component startup.

The 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 parameters at component startup;
- by using an alternative configuration file.

4.2.2. Object scan and disinfection mode

The settings of this mode are very important, because they determine whether the application will cure infected files when they are detected.

By default disinfection is turned off: the default behaviour is to scan objects and to notify about detected viruses and other suspicious or corrupted files by printing messages to the screen and in the report (see 5.6 on p. 42).

As a result of an anti-virus scan, each object will be assigned a status from 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).
- **Error** – an error has occurred while scanning the object.

With the disinfection mode turn on (section **[scanner.options]**, setting **Cure = yes**) only objects with the **Infected** status will be sent for anti-virus processing. As a 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. Files with this status will be processed according to rules specified for infected objects.
- **Error** – error occurred during the object scan.

4.2.3. Actions to be performed on objects

The actions to be performed on an object depend on the object's status (see Chapter 2, on p. 12). The default action is only to provide notification about the detection of infected or suspicious objects. However, for objects with **Infected**, **Suspicious**, **Warning**, **Error**, **Protected** and **Corrupted** status you can configure further responses, including:

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

Please note that Kaspersky Anti-Virus discriminates 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, with section **[scanner.object]** for simple objects, and section **[scanner.container]** for container objects.



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

You can select actions to be performed on 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 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 startup does not have to be specified!

- You can specify them for the current work session using command line parameters when starting the *kavscanner* component.

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

4.2.4. On-demand scan of an individual directory

One of the commonest tasks implemented by Kaspersky Anti-Virus is the anti-virus scan and disinfection of an individual directory.



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

Create the files *infected.lst*, *suspicion.lst*, *corrupted.lst* and *warning.lst* to record 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 in the report file *kav4fs-kavscanner-current_date-pid.log* that will be created in the current directory.



Solution: to implement this task, enter at the command line:

```
# /opt/kaspersky/kav4fs/bin/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
```

4.2.5. Scheduled scan

Kaspersky Anti-Virus tasks can be scheduled to run using the **cron** application.



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



Solution: to perform this task, do the following:

1. Create the configuration file `/etc/kav/scanhome.conf` and specify the 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 * * * /opt/kaspersky/kav4fs/bin/kav4fs-
kavscanner -c /etc/kav/scanhome.conf /home
```

4.2.6. Additional capabilities: using script files

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

4.2.6.1. Disinfection of infected objects in an archive

Kaspersky Anti-Virus detects, but does not disinfect, suspicious and infected files packed in archives. However, infected files packed in archives can be disinfected by using an additional script file. The next example shows how to disinfect `tar` and `zip` archives using the script file `vox.sh`, which is included in the Kaspersky Anti-Virus distribution package.

When started, the scripts unpacks the archive being scanned, runs an anti-virus scan and processes the individual objects, and then repacks the scanned files. It assumes that the necessary archiving utilities have been installed on the system.



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



Solution: to perform this task, do the following:

Enter at the command line:

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

4.2.6.2. Sending notifications to the administrator

Using standard Unix tools, you can specify that notifications are sent to the administrator upon detection of infected, suspicious or corrupted objects in the computer's file systems.



Task: configure administrator notification when infected files and archives are detected during file systems scans performed using the settings specified in the **kav4fs.conf** configuration file. Enable resolving of the symbolic links to the checked objects.



Solution: to perform this task, do the following:

Enter these rules for processing simple objects and container objects in the 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% ad-
min@localhost.com
```



Before launching the example, make sure that the **mail** utility is located at this utility's standard installation path in the operating system.

4.3. Real-time anti-virus protection

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



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

The *kavmonitor* component is configured so that when another program requires access to a file (opening, closing or executing), *kavmonitor* performs an anti-virus scan: if the action is to close the file, it will be scanned only if it has been altered. By default, all object types specified by the user will be scanned for viruses and malware, except:

- archives
- self-extracting archives
- mail databases
- e-mail messages.



If a symbolic link is scanned, the link's target object will be checked. This occurs even if the target object is excluded from protection.

If a symbolic link is added to the **IncludeDirs** list, then it will not be resolved by the *kavmonitor* component.

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



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

For objects with the status **Infected**, **Suspicious**, **Warning**, **Error**, **Protected** and **CureFailed**, you can configure responses following scanning, including:

- *moving to a directory* – moving objects with a certain status to a directory; *simple* and *recursive* (with restoration of the full path) *moving* is available;
- *deleting object* from the file system;
- *performing a command* – processing of files using standard Unix script files, or similar.

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

You can also configure additional settings:

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



Avoid making changes to the **[monitor.*]** section of the application configuration file if remote administration of application via Kaspersky Administration Kit is planned. These sections' parameters are overridden by the settings made via Kaspersky Administration Kit.

4.4. Managing license keys

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

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

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

4.4.1. Viewing license key details

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

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

All information will be printed to the screen.



To view information about all license keys,

Enter at the command line:

```
#/opt/kaspersky/kav4fs/bin/kav4fs-licensemanager -s
```

Information similar to the following will be printed to the screen:

```
Kaspersky license manager Version 5.7
Copyright © Kaspersky Lab 1997-2007.
Portions Copyright (C) Lan 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
```



To view information about a specific key,

Enter at the command line:

```
# /opt/kaspersky/kav4fs/bin/kav4fs-licensemanager -k
<key filename>
```

where `<key filename>` is the name of the license key file, for instance, `0003D3EA.key`.

The following information will be printed to the screen:

```
Kaspersky license manager Version 5.7
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
```

4.4.2. Renewing your license

Renewal of your Kaspersky Anti-Virus license grants you the right for to restore the application's full functionality: that is, to update the anti-virus database, and resume the additional services listed in 4.3 on p. 32.

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



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, by sending a request directly to our Sales Department (sales@kaspersky.com), or filling out a form at our website (<http://www.kaspersky.com>), section **eStore -> Renewal**. Upon 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 give you considerable discounts when you renew your license for our products. 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.



To install your new license key,

Enter at the command line:

```
# /opt/kaspersky/kav4fs/bin/kav4fs-licensemanager -a  
<key filename>
```

After this we recommend that you update your anti-virus database (see 4.1 on p. 20).



To remove a license key,

Enter at the command line:

```
# /opt/kaspersky/kav4fs/bin/kav4fs-licensemanager -da
```

to remove the active license key, or

```
# /opt/kaspersky/kav4fs/bin/kav4fs-licensemanager -dr
```

to remove the additional license key.

CHAPTER 5. ADDITIONAL SETTINGS

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

5.1. Configuration of product interaction with Webmin

If you plan to manage Kaspersky Anti-Virus remotely, you are advised to configure it to be used with the Webmin package.

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

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



To create an alternative configuration file using Webmin, you must:

1. Copy data from the existing configuration file into a new file and save this new file under a different name. Then you can 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 text field marked **Full path to KAV config**.



For more details about configuring the Webmin application, see the documentation for that product. Additionally, if you have questions regarding the remote administration plug-in of the application, you may refer to the Webmin online documentation.

Further in this guide, **remote operations via Webmin are not discussed!**

5.2. Optimization of Kaspersky Anti-Virus operation

To reduce the load on the computer's processor, and increase the speed of anti-virus processing, Kaspersky Anti-Virus offers effective optimization methods. This section gives 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 repeatedly scan a file every time it is accessed and, if possible, restrict the work to merely comparing it to the existing information about it. The algorithm for scanning objects (files) for viruses is as follows:

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 selected 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 *kavmonitor*. The cache consists of two levels. The first level stores information about **clean files** that are accessed relatively often. This cache is located in the kernel module, which considerably reduces the time needed to access it. If the application detects data about the requested file 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 is performed on the second level that contains information **about all scanned files**. Both cache databases exist in RAM and will not persist after the application is closed.

Therefore, if during a scan, information about a file is not added to the iChecker database (in which case 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 a file, a search will be performed first in the first-level cache, then in the iChecker database and in the second-level cache. The search is based on the filename. If the 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 requested file is not detected in either the iChecker database or the 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 **iCheckerDbFile** parameter in the **[path]** section of the application's configuration file.

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



Limiting the load on the processor.

Scanning the computer's file systems may take a long time, depending upon the amount of data stored. In this case, the load on the processor is considerably increased while it continues to perform other tasks. Therefore it is desirable to have a tool that pauses the anti-virus scan once a specified load threshold has been exceeded.

Kaspersky Anti-Virus has such a mechanism. In version 5.7 setting **MaxLoadAvg** has been added to the **[scanner.options]** section of the configuration file. If this setting is turned on, *kavscanner* pauses before scanning each new file until the value of the processor **load average** decreases to the specified level.

Additionally, you can restrict the number of objects being simultaneously scanned in real-time mode, using the **CheckFileLimit** setting in the **[monitor.options]** section of the application's configuration file. This can decrease the processor load, and increase the speed of scanning of some objects.

One more step decreasing the load on system resources is *kavmiddleware* disabling. The service provides for interaction between Kaspersky Anti-Virus and Kaspersky Administration Kit. If you do not use the application features binding it to Kaspersky Administration Kit, you can stop the *kavmiddleware* service. To do that, enter the following in the command line:

```
# /etc/init.d/kavmiddleware stop
```

5.3. Moving objects into quarantine

You can configure Kaspersky Anti-Virus so that all infected objects will be moved to a separate quarantine directory.

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

If you plan to keep the directory of these isolated objects within the computer's file system, you are advised to exclude it from the scope of future scans by specifying the full path to it as the value for setting **ExcludeDirs** in the **[scanner.options]** section of the configuration file.

The rest of this section discusses the task of isolating infected objects detected during scans of the computer's file system.



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



Solution: to perform this task, do the following:

1. To specify actions on 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 at the command line:

```
# /opt/kaspersky/kav4fs/bin/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 directory `/tmp/infected` to reading and writing only. This can be achieved using standard Unix tools (command **chmod**). The task implementation should be modified as follows:

Enter the following line in the sections **[scanner.object]** and **[scanner.container]** of the application's 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 all files for which access is attempted, and disinfect infected objects. If disinfection is not successful, move the infected objects with full paths into the directory **/tmp/infected**.



Solution: to perform this task, do the following:

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

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

5.4. Backing up infected objects

If scanned files were infected, and deletion from the file system is specified for infected objects, there is a risk of losing important data. To avoid this risk, Kaspersky Anti-Virus includes the ability to copy files to backup storage.

*Before the attempt to disinfect or delete an object, a copy of the object will be automatically created in the backup directory (section **[monitor.path]**, settings **BackupPath**). This creates a backup copy, with the possibility of restoring the original file if the object is corrupted during disinfection. The object with the full path will be copied into backup storage. If an object is saved twice in the backup storage, the older copy of the object will be automatically overwritten by the newer one.*

Please note: by default no files are copied to the backup directory, and the location of the backup directory is not defined in the configuration file.

To turn on this mode, manually specify the path to the directory 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 directory until it is deleted by the administrator.



Actions specified for infected objects in the configuration file settings are not performed on files in the backup directory.

5.5. Localization of the date and time format

During its operation, Kaspersky Anti-Virus generates reports for each of its components and sends notifications to its 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 have the same format as the UNIX **strftime** function:

%H:%M:%S – time format.

%d/%m/%y – date format.

The administrator can alter the time and the date formats. Localization of these 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** and **month/day/year** respectively.

5.6. Kaspersky Anti-Virus report generation settings

Results of the operation of all components of Kaspersky Anti-Virus are logged in report files.



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

To record the application's activity in the system log, set the **ReportFileName** parameter in the **[monitor.report]**, **[scanner.report]**, and **[updater.report]** sections to **syslog**. The information is recorder at the **daemon syslog's** facility.

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

The detail level is a number that determines the level of detail of the information about the operation of components which is logged in the report. Each

successive level includes information of the previous level complemented by some additional information.

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

Level	Level description	Explanation
0	Critical errors	Information about critical errors only. For example, the component is infected, or an error occurred during verification, or loading of the database or the license keys. Critical errors information is marked with 'F' symbol in the log file.
1	Errors	Information about other errors including those that cause the component to close: for example, object scan error information. Non-critical errors are marked with 'E' symbol in the log file.
2	Warning	Information about errors that may cause the application to close: for example, information about insufficient free disk space or license key expiration. Such messages are marked with 'W' symbol in the log file.
3	Info, Notice	Important informational messages: for example, information stating whether the component is running, the path to the configuration file, scan scope, information about the anti-virus database, about license keys, and statistical info about the results. Informational messages are marked with 'I' symbol in the log file.
4	Activity	Messages about current application activity (for example, the name of the object being scanned). Such messages are marked with 'A' symbol in the log file.
9	Debug	Debug messages. Such messages are marked with 'D' symbol in the log file.

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



By default, logging to a file is disabled for the on-demand scan or update tasks launched via the Kaspersky Administration Kit.

Specify the report detail level and report storage directory via the **ReportLevel** and **ReportsDir** parameters in the **[middleware.options]** section of the application's configuration file to enable logging.

CHAPTER 6. ADMINISTERING THE PROGRAM WITH KASPERSKY ADMINISTRATION KIT

The **Kaspersky Administration Kit** enables central management of the key administrative tasks in operating a company network's security system.

Kaspersky Anti-Virus 5.7 is one of the suite of Kaspersky Lab products which can be managed either locally, at the command line (the method is described herein above), or remotely, using Kaspersky Administration Kit if the computer is a part of a centralized remote administration system.

The deployment procedure for the application has two steps:

- deploy *Administration Server* in the network, and install *Administration Console* on the administrator's workstation. For details, see the Administrator's Guide for implementing Kaspersky Administration Kit;
- deploy the Kaspersky Anti-Virus 5.7 and *Network Agent* on the networked computers which are to be remotely administered.

Figure 1 shows the interface to *Administration Console*, which allows you to administer the application remotely through Kaspersky Administration Kit. It provides a standard **MMC-integrated interface** (Microsoft Management Console), and allows the administrator to perform these functions:

- remotely configure Kaspersky Anti-Virus on networked computers
- update the Kaspersky Anti-Virus database
- view information about the application's operation on client computers.

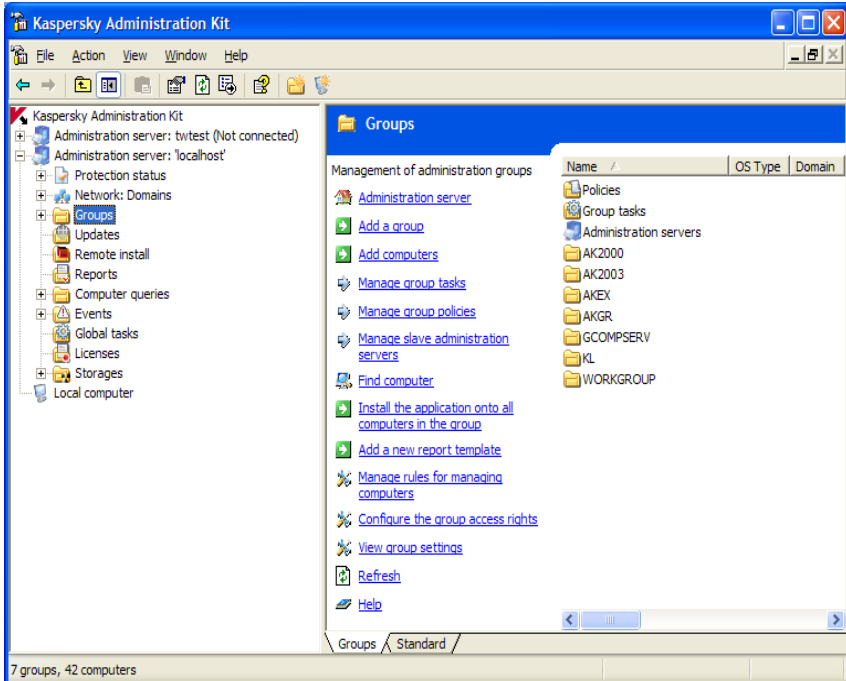


Figure 1. Kaspersky Administration Kit Administration Console

When administering the application centrally through Kaspersky Administration Kit, the administrator determines settings for policies, tasks, and for the application. Protection is designed around these settings.

Application settings are a set of general settings for application operation, including general protection settings and protection scope settings.

A **task** is a specific action performed by the application. Tasks for Kaspersky Anti-Virus are of several types, including:

- on-demand scan tasks
- anti-virus database update tasks.

Each specific task has a set of Kaspersky Anti-Virus settings, called the *task settings*, which are used when the task is performed.

The key feature of centralized administration is the grouping of remote computers, which are managed by creating and configuring group policies.

A **policy** refers to a collection of settings for Kaspersky Anti-Virus operation within a logical network group of computers.

A policy allows you to manage the complete functionality of the application, since it contains both application settings and settings for all types of tasks, except for settings that are specified individually for a specific computer (for example, task schedules).

The policy may also restrict modifications to the application's or task's settings.

6.1. Administering the application

The Kaspersky Administration Kit enables the complete remote administration of Kaspersky Anti-Virus on individual client computers, including: starting and pausing scans, general configuration such as enabling and disabling protection, and configuring settings for report creation.

To manage application settings:

1. Select the group that contains the target client computer in the list of **Groups** (see Figure 1).
2. In the result pane, select the client computer for which you need to modify application settings. In the context menu or in the **Actions** menu, select the **Properties** command.
3. The **Applications** tab on the client computer properties window (see Figure 2) displays a complete list of Kaspersky Lab applications installed on the client computer.
4. Select **Kaspersky Anti-Virus 5.7 for Linux Workstation and File Server**. The following buttons are available beneath the list:
 - **Events** – view a list of events that have occurred during application operation on the server or a client computer, and were recorded on the administration server.
 - **Statistics** – view statistical information about application operation.
 - **Properties** – configure the application in the **Kaspersky Anti-Virus 5.7 for Linux Workstation and File Server settings** window that opens.

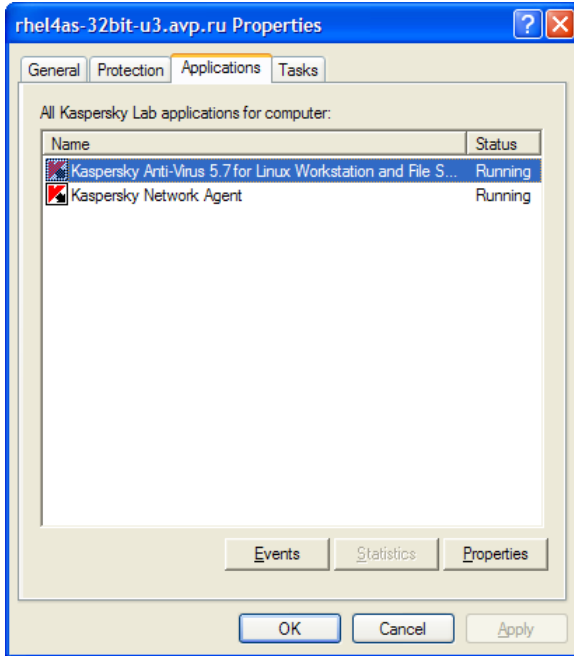


Figure 2. List of Kaspersky Lab applications

6.1.1. Configuring application settings

To view or modify application settings:

1. Open the properties window for the client computer on the **Applications** tab (see Figure 2).
2. Select **Kaspersky Anti-Virus 5.7 for Linux Workstation and File Server**. Click the **Properties** button to open the application settings window.

All the tabs, except the **Settings** tab, are standard for Kaspersky Administration Kit. For more on the standard tabs, see section "Viewing information about the client computer" of the Kaspersky Admin Kit's Administrator's Guide.

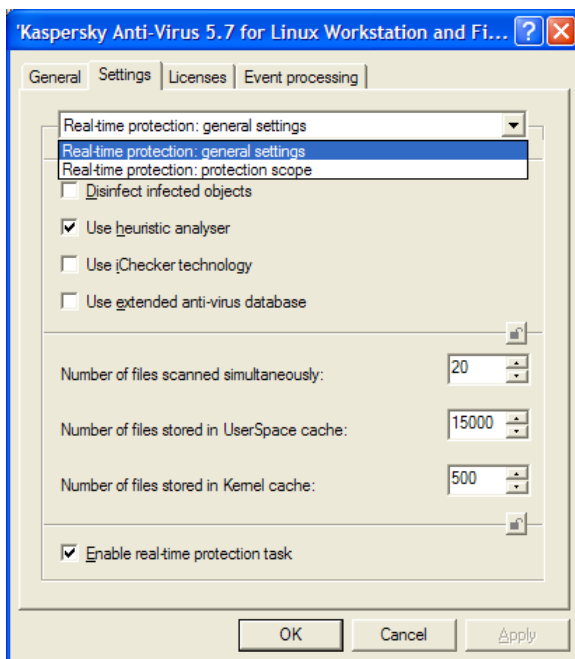


Figure 3. Configuring Kaspersky Anti-Virus settings.
Settings tab



If a policy prevents alteration to some settings (see 6.3.1 on pg. 57) the corresponding controls will be disabled.

On the **Settings** tab, you can configure general protection settings and protection scope settings. The following sections describe this process in more detail.

6.1.1.1. Settings tab, Real-time protection: general settings section

On the **Protection: general settings** section, you can:

- enable/disable real-time protection of the host computer
- enable/disable disinfection of infected objects
- enable/disable the heuristic analyzer and the iChecker technology

- configure application performance settings (the number of simultaneously scanned files, number of files preserved in Kernel and UserSpace cache).

6.1.1.2. Settings tab, Real-time protection: protection scope section

On the **Protection: protection scope** section, you can:

- configure the trusted area (choose directories to exclude from scanning)
- specify filename masks to exclude from scanning (defined as standard shell masks)
- configure the protected area (the list of directories to scan)
- select the types of objects to scan.

6.2. Managing tasks

This section describes creating and configuring tasks for Kaspersky Anti-Virus.

Centralized administration with Kaspersky Administration Kit allows you to create and use the following tasks:

- on-demand scan task
- anti-virus database update task.

6.2.1. Creating tasks

You can create your own tasks for scanning and updating of the anti-virus database.

To view the list of the tasks created for a client computer:

1. Select the group that contains the target client computer in the **Groups** directory (see Figure 1).
2. In the result pane, select the computer for which you want to view a list of local tasks. Use the **Tasks** command from the context menu or the **Actions** menu. The **Properties** window of the client computer will open.
3. The **Tasks** tab of the **Properties** window (see Figure 4) displays a complete list of tasks created for that client computer.

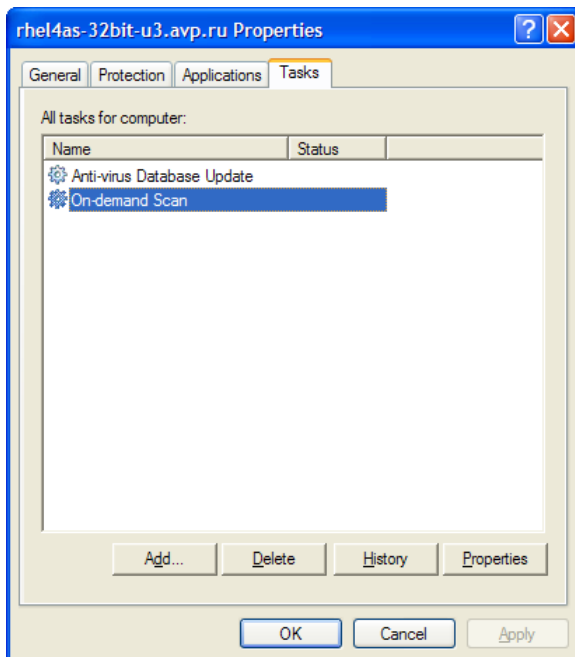


Figure 4. List of application tasks

When working with the application through Kaspersky Administration Kit, you can create:

- local tasks, configured for individual computers
- group tasks, configured for computers which are all members of a single network group
- global tasks, configured for a selected subset of all client computers from all network groups

You can modify task settings, monitor their performance, copy and move tasks from one group to another, and also delete them, using the standard commands **Copy/Paste**, **Cut/Paste**, and **Delete** from the context menu, or the same commands from the **Action** menu.

The task settings on each computer are determined by the group policy, task settings and application settings on that computer.

6.2.1.1. Creating local tasks

To create a local task:

1. From the **Groups** list (see Figure 1), select the group which contains the client computer for which you want to create a local task.
2. Select the target computer from the list of group's computers, and use the **Properties** command from the context menu or the **Tasks** item from the **Action** menu. The **Properties: <computer name>** window will open, displaying the properties of the client computer..
3. The **Tasks** tab (see Figure 4) displays a list of tasks created for that computer. To add a new local task, click the **Add** button; to change task settings, click the **Properties** button. To delete a selected task from the list, click the **Delete** button.

When you press the **Add** button, a task creation wizard will start up. The wizard provides a series of windows which can be navigated using the **Back** and **Next** buttons. You can finish the wizard by pressing **Finish**. The **Cancel** button will stop the Wizard at any point.

The following sections describe how to create a task using the wizard.

Step 1. Entering general data on the task

The first window is introductory. Here you must specify the name of the task in the **Name** field.

Step 2. Selecting an application and task type

From the **Application name** list view, select **Kaspersky Anti-Virus 5.7 for Linux Workstation and File Server**. Select the task type from the **Task type** list. The following task types are available for Kaspersky Anti-Virus:

- On-demand scan
- Anti-virus database update

Step 3. Configuring settings for the selected task type

Depending on the task type selected in the previous step, the contents of the following windows can vary.

CONFIGURING SETTINGS FOR AN ON-DEMAND SCAN TASK

For on-demand scanning tasks, you must specify:

- the types of objects to be scanned
- the scan scope specified as a colon-delimited list of paths to the objects to scan
- the actions that will be applied to infected objects when they are detected
- any additional parameters, such as whether to use the heuristic analyzer, the iChecker™ technology, the extended anti-virus database or whether to launch the new task as a full computer scan task.

CONFIGURING SETTINGS FOR AN ANTI-VIRUS DATABASE UPDATE TASK

For the anti-virus database update task, you must specify:

- the source to download updates from. You can use the update servers of Kaspersky Lab or specify a user-defined source.
- whether passive FTP mode is required
- the connection timeout (in seconds).

You can enable / disable using a proxy server and configure its settings in the dialog that opens after clicking the **Configure proxy server**.

Step 4. Setting up a schedule

In the **Task schedule** window, you can configure a schedule that will be used to run the task.

In the **Schedule** drop-down list, select the type of schedule for the task. The central part of the window, containing data entry fields, will change its appearance in response to your selection.

For more details on configuring task schedules, see the Administrator's Guide for Kaspersky Administration Kit.

Step 5. Finishing creating a task

The last window of the wizard will inform you that you have successfully creating a task.

6.2.1.2. Creating group tasks

To create a group task:

1. Select the group for which you want to create a task from the console tree (see Figure 1).
2. Select the group's list of **Tasks**, open the context menu, and select the **Create→Task** command, or use the same command on the **Action** menu. The task creation wizard will start, similar to the local task create wizard (for more, see 6.2.1.1 on pg. 52). Follow its instructions.

When the wizard is finished, the task will be added to the list of **Tasks** for that group and all its sub-groups, and will be visible in the results pane.

6.2.1.3. Creating global tasks

To create a global task:

1. Select the **Global tasks** node from the console tree (see Figure 1), open the context menu, and select the **Create→Task** command, or use the same command on the **Action** menu.
2. The task creation wizard will start, similar to the local task creation wizard (for more, see 6.2.1.1 on pg. 52). The only difference is in selecting the networked client computers to which the task will apply.
3. Select from the network the computers that will run the task. You can select computers from different folders or select an entire folder (for more details, see the Administrator's Guide for Kaspersky Administration Kit).



Global tasks are only performed on a selected set of computers. If new client computers are added to a group with computers for which a remote installation task has been created, this task will not run for them. You must create a new task or make corresponding changes to the settings of the existing task.

When the wizard is finished, a global task will be added to the **Global tasks** node of the console tree, and will be visible in the results pane.

6.2.2. Configuring specific task settings

To view and modify the settings for client computer tasks:

1. Open the properties window for the client computer on the **Tasks** tab (see Figure 4).

2. Select the task from the list and click the **Properties** button. The task settings window will open (see Figure 5).

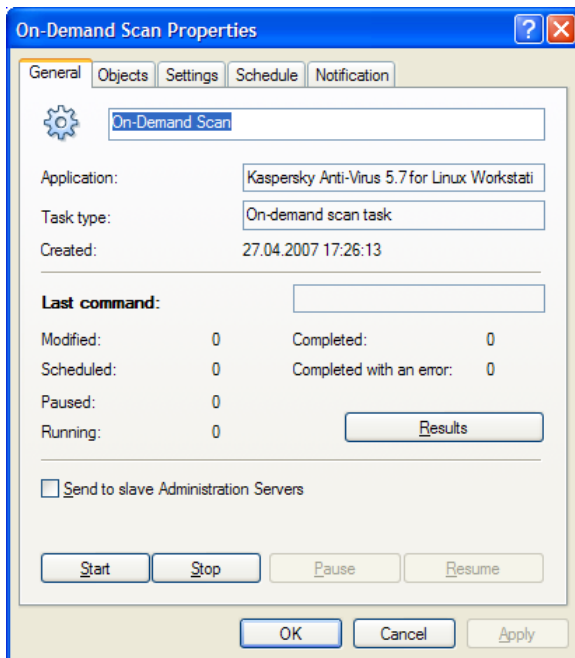


Figure 5. Configuring task settings

The following tabs are the same for all tasks:

- **General** – view general information about a task, about starting the task, or pausing it.
- **Schedule** – create a schedule for running tasks.
- **Notifications** – configure notifications on the results of tasks (for more details, see the Administrator’s Guide for Kaspersky Administration Kit).

6.2.2.1. On-demand scan task

Besides the parameters specified during task creation, the following task settings can be customized for on-demand scan tasks:

- the types of objects to be scanned

- the trusted zone – a list of objects and objects' name masks excluded from scanning
- whether to scan local file systems only
- whether to scan directories recursively
- whether to resolve symbolic links during scan
- whether the current task should be launched as a full computer scan task.

6.2.2.2. Anti-virus database update task

The update task settings include:

- the source to download updates from. You can use the update servers of Kaspersky Lab or specify a user-defined source.
- regional settings. When the current computer's location is specified the update will be performed from the update servers of the specified region.
- whether passive FTP mode is required
- the connection timeout (in seconds).

You can enable / disable using a proxy server and configure its settings in the dialog that opens after clicking the **Configure proxy server**.

6.2.3. Starting and stopping tasks

Tasks are started, paused and resumed automatically, either according to a schedule or manually, using commands from the context menu or from the View Task Settings window.

To start/stop a task manually:

Select the necessary task from the results window, open the context menu, and select **start/stop**, or use the same commands on the **Action** menu.

You can initiate the same operations for all task types from the task settings window on the **General** tab (see Figure 5), using the command buttons **Start**, **Stop**.



Tasks will start on the client computer only if the corresponding application is running. When the application is stopped, all started tasks will be terminated.

6.3. Managing policies

Setting up policies allows you to apply universal application and task settings to a group of client computers.

This section includes information on creating and configuring policies for Kaspersky Anti-Virus.

6.3.1. Creating policies

To create a policy for Kaspersky Anti-Virus:

1. In the **Groups** directory (see Figure 1), select the group of computers for which you need to create a policy.
2. Select the list of **Policies** for the selected group, open the context menu, and use the **Create→Policy** command, which will start the policy creation wizard.

Policies are created by the policy wizard. The wizard provides a series of windows which can be navigated using the **Back** and **Next** buttons. You can finish the wizard by pressing **Finish**. The **Cancel** button will stop the Wizard at any point.

The following sections describe how to create a task using the wizard.



During each step of creating a policy (Step 3 - Step 5), the settings entered can be locked with the  button. If settings are locked, they cannot be edited when the policy is used on client computers.

Step 1. Entering general data on the policy

The first step of the wizard is introductory. Here you must specify the name of the policy in the **Name** field of the first wizard window. Then select **Kaspersky Anti-Virus 5.7 for Linux Workstation and File Server** from the **Application name** dropdown list.

Step 2. Selecting policy status

In this dialog you should specify the policy status setting the corresponding switch to the required position and thus making the policy active, inactive or applicable for mobile users (enforced after computer disconnection from network).



You can create several policies for a single application within a group, but only one of them can be active.

Step 3. Configuring policy settings

Application settings are subdivided in two categories:

- general settings
- the settings of protection scope and protected objects.

General settings include:

- real-time protection settings
- action applied to revealed infected objects (you can enable/disable disinfection of such objects)
- whether to use the heuristic analyzer and iChecker™ technology.

Protection settings include:

- trusted area (list of directories excluded from scanning)
- masks of files excluded from scanning (defined as standard shell masks)
- list of object types to be protected.

The lists of directories and object masks are colon-delimited.

Step 4. Finishing creating a policy

The final window of the wizard tells you that you have successfully created a policy.

Once the wizard is completed, the Kaspersky Anti-Virus policy will be added to the **Policies** directory for the corresponding group, and will be visible in the results panel.

You can edit the settings of the new policy, and set restrictions on modifying its settings using the **.** button for each settings group. Locked settings will not be available for alteration in the application or task properties. The policy will be applied to client computers the first time the clients synchronize with the server.

You can copy, delete or move policies from one group to another using the standard commands **Copy/Paste**, **Cut/Paste**, and **Delete** from the context menu, or using the same commands from the Action menu.

6.3.2. Viewing and editing policy settings

At the editing stage, you can modify the policy, and also block modification to settings in nested group policies and in application and task settings.

1. Select the computer group for which settings are to be edited from the console tree in the **Groups** list (see Figure 1).
2. Select the **Policies** item for the group: the results pane will display all the policies created for the group.
3. Select the policy to edit from the list of policies for **Kaspersky Anti-Virus 5.7 for Linux Workstation and File Server** (the application name is specified in the **Application** field).
4. Select the **Properties** command from the context menu for the selected policy. A policy settings window will open for the application, containing several tabs.

The **General**, **Enforcement**, and **Events** tabs are standard for Kaspersky Administration Kit (for more details, see the Administrator's Guide for the program).

The **Settings** tab (see Figure 6) contains sections with settings specific to Kaspersky Anti-Virus. Details of these sections follow.

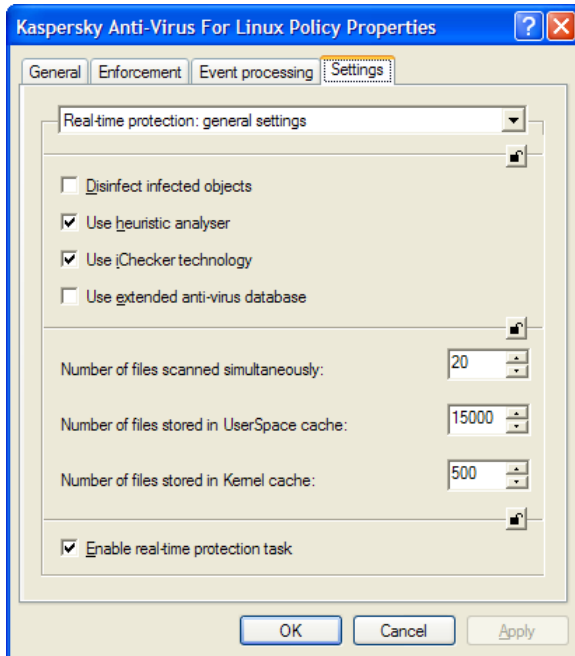



Figure 6. Configuring policy settings



When editing policy settings, use the  button to lock data entered for the policy. In future, blocked settings will not be available for alteration in the application or task properties..

6.3.2.1. Configuring the protection scope

You can use the **Protection: scope and objects' types** section of the **Settings** tab to:

- define the trusted area (directories to be excluded from scanning)
- specify name masks for files to be excluded from protection (defined as standard shell masks)
- specify the scan scope (list of directories that should be scanned).

The lists of directories and object masks are colon-delimited.

6.3.2.2. Specifying object types to be protected

You can specify which object types will be protected in the **Protection: scope and objects' types** section of the **Settings** tab.

You can choose to scan:

- packed executables
- archives
- self-extracting archives
- e-mail databases
- plain e-mail.

6.3.2.3. Configuring actions applied to objects

You can use the **Protection: general settings** section of the **Settings** tab to:

- enable / disable disinfection of objects affected by malware
- enable / disable real-time protection
- enable / disable the heuristic analyzer
- enable / disable the iChecker™ technology
- enable / disable the use of an extended anti-virus database.

6.3.2.4. Specifying additional parameters

There are some additional parameters, which can be set in the **Protection: general settings** section of the **Settings** tab, including:

- the number of simultaneously scanned files
- the number of files stored in the UserSpace cache
- the number of files stored in the Kernel cache.

CHAPTER 7. UNINSTALLING KASPERSKY ANTI-VIRUS

To uninstall Kaspersky Anti-Virus you will need:

- Privileged user rights (**root**). If you are going to uninstall the application and do not have such rights, you will have to log in to the system as the **root** user.
- Installation process report file.
- The filenames and sizes of the installed Kaspersky Anti-Virus files must 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. To do that, type the following in the command line:

```
# /etc/init.d/kav4fs stop
```

Then you will have to uninstall the application and Network Agent.



If you installed Kaspersky Anti-Virus and Network Agent from .rpm packages, enter the following in the command line to initiate their removal:

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




If you installed Kaspersky Anti-Virus and Network Agent from .deb packages, enter the following in the command line to initiate their removal:

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

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

CHAPTER 8. VERIFYING THE ANTI-VIRUS OPERATION

After Kaspersky Anti-Virus is installed and configured, you are advised to 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.

The file downloaded from the **EICAR** website or created as described above contains the body of a standard test "virus". Kaspersky Anti-Virus will detect it, assign it the **Infected** non-disinfectable status 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)
WARN–	Suspicious (modified code of a known virus)

Prefix	Object type
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 the prefixes to be added at the beginning of the string of the standard test “virus”: for example,

```
CORR–X5O!P%@AP[4\^PZX54(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 the prefix. The actions for each type of object are defined by the application settings configured by the administrator.

APPENDIX A.

ADDITIONAL INFORMATION ABOUT THE APPLICATION

This Appendix contains the description of the directory tree of Kaspersky Anti-Virus after installation, the configuration file and the command line parameters of the components and their return codes. The 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 the most important files without which the application will not function.

BasesPath– full path to the anti-virus database.

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

IcheckerDbFile– full path to the directory that stores the database checked using 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 **[network]** contains *kavmiddleware* connection settings:



You should not change this parameter value during regular application use.

MiddlewareAddress=/var/run/kav4fs/kavmiddleware.socket – configuration of the *kavmiddleware* connection to *Network Agent* and *kavmonitor*.

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

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

Packed=yes – packed files scan mode. To disable scanning of packed files, assign the value **no** to this setting.

Archives=no – archives scan mode. To disable the scanning of archive files, assign the value **no** to this setting.

SelfExtArchives=no – self-extracting archives scan mode. 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 **SelfExtArchives** is assigned the value **no**.

MailBases=no – e-mail database scan mode. To disable this mode assign value **no** to this setting.

MailPlain=no – scan of e-mail messages in plain text format. To disable this mode assign value **no** to this setting.

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

Cure=no – mode for disinfecting infected objects. To enable this mode, assign the value **yes** to this setting.

Ichecker=no – the mode for the use of the iChecker technology during the anti-virus scan. 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 simultaneously.

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, including adware and remote administration programs.

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 directory containing 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 real-time anti-virus protection.

OnInfected=action – actions to be performed when an infected file is detected. 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 when a suspicious file is detected. The file contains code which resembles a virus, but one not known yet to Kaspersky Lab.

OnWarning=action – actions to be performed in case of a detection of a file containing code 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 when a password-protected object is detected. Such objects cannot be scanned.

OnCorrupted=action – actions to be performed when a corrupted file is detected.

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

The syntax of the **action** setting consists of two parts: the action itself and an optional parameter separated by 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* <directory> – move file into <directory>.
- *movePath* <directory> – move file to <directory> recursively (with the absolute path).
- *remove* – delete the file.
- *exec* <parameter> – perform on the object the action defined by the value <parameter>.

The following values can be passed as the *exec* action parameters:

- %VIRUSNAME% – name of the detected threat or the error name.
- %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 string.
-

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

ReportLevel=4 – report detail level (see 5.6 on p. 42).

ReportFileName – a name of the file into which results of the component operation are logged. If the **syslog** value is specified, the information is recorded into the system log at the daemon **facility**.

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. 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. 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 directories that are excluded from the scan; by default all directories 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. 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 – e-mail database scan mode. In order to disable this mode assign value **no** to this setting.

MailPlain=yes – scan e-mail messages in plain text format. To disable this mode assign value **no** to this setting.

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

Recursion=yes – mode for recursive scanning of directories 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**), self-extracting archives will be scanned even if the **SelfExtArchives** setting is assigned the value **no**.

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 and remote administration programs.

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 settings for 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 – a name of the report file into which results of the component operation will be logged. If the **syslog** value is specified, the information is recorded into the system log at the daemon **facility**.

ReportLevel=4 – report detail level (see 5.6 on p. 42).

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 on 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 if infected objects are detected 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 if a suspicious object is detected inside a container.

OnWarning=action – actions to be performed if a suspicious object is detected inside a container: that is, an object the code of which resembles the code of a known virus.

OnCured =action – actions to be performed if a container contains 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=action – actions to be performed if an error occurred during the container scan.

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

Section **[scanner.object]** contains settings that define actions to be performed on 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 if a suspicious file is detected. The file's code resembles the code of a virus not known yet to Kaspersky Lab.

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

OnError=action – 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 **[monitor.actions]**.

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. To display short format results, assign the value **yes** to this setting.

ShowObjectResultOnly=no – the mode of displaying the results of the scan of a simple object in short format on the screen. To display short results, assign value **yes** 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, including the process of downloading of the anti-virus database, or information about the scan of the current file. 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 directory for backup copies of 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 directory.

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

Section **[updater.report]** contains the settings for 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 – name of the file into which results of the component operation will be logged. If the **syslog** value is specified, the information is recorded into the system log at the daemon **facility**.

ReportLevel=4 – report detail level (see 5.6 on p. 42).

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 the setting is assigned value **yes**, the proxy server 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 the address specified in the setting **UpdateServerUrl** for updating the anti-virus database. If this setting is assigned value **no**, then in case of an unsuccessful update of the anti-virus database 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 in the application installation package will start automatic reloading of the updated anti-virus database by the application. We do not recommend changing the value of this setting.

RegionSettings=ru the code of the user's region; this code is used to select the 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.

Section **[middleware.options]** contains the settings of the *kavmiddleware* service:



You should not change these parameters' values during regular application use.

ScannerExe=/opt/kaspersky/kav4fs/bin/kav4fs-kavscanner – path to the executable file of the *kavscanner* component.

Keepup2dateExe=/opt/kaspersky/kav4fs/bin/kav4fs-keepup2date – path to the executable file of the *keepup2date* component.

LicensemanagerExe=/opt/kaspersky/kav4fs/bin/kav4fs-licensemanager – path to the executable file of the *licensemanager* component.

MonitorlnitdScript=/etc/init.d/kav4fs – path to the script for managing the *kavmonitor* service.

DirToStoreFiles=/var/opt/kaspersky/kav4fs/middleware – path to the *kavmiddleware* service file.

ReportLevel=0 – report detail level (see 5.6 on p. 42).

ReportsDir=/var/log/kaspersky/kav4fs – path to the application component's report files.

A.2. Command line parameters for component *kavscanner*

Settings of the configuration file can be overridden from the command line at application startup using command line parameters. A detailed discussion of these parameters 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 e-mail databases;

M/m Enable/disable the scan of plain text e-mail messages;

E/e Enable/disable heuristic code analyzer.

-R/r Enable/disable recursive scan;

-S/s Enable/disable the mode of opening symbolic links;

-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. Information about component activity will also be output to the console. Specify `syslog` as the **<name>** parameter value to log into system log.

-j<level> Specify the report detail level based on the amount of information contained in this report. The following detail level may be used as the **<level>**:

1 Enable display of messages about other errors;

- | | |
|--------------------------|--|
| 2 | Enable display of information messages; |
| 3 | Enable 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> : |
| 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 in 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 which are specified in the file **<filelist.lst>**.

File processing options (the use of these parameters 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, then delete it; do not delete infected objects from the container.
- i3** Disinfect infected object; if disinfection is not possible and if the object is simple object, then delete it; if the infected object is located in the container, then 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 have been detected that contain code resembling the code of known viruses;

- 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 was 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 parameters 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 parameters for component licensemanager

Help options:

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

License key management 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(a|r)** Remove active (**-da** option) or additional (**-dr** option) 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.
- 70** Component licensemanager is corrupted.

A.7. Command line parameters 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 parameters supported by the component, and close the component;
-s	Print the list of the updates servers to the screen;
Operation options:	
-r	Rollback 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 directory <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 directory <path_to_file> .
Report generation options:	

<code>-l<path_to_file></code>	Log the results of the component's operation in file <code><path_to_file></code> .
-------------------------------------	--

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 <code>PostUpdateCmd</code> 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.

A.9. Command line parameters for component `kavmidware`

Опции помощи:	
<code>-v</code>	Print to the screen the version of the application and close the component.;
<code>-h</code>	Print to the screen help information about the command line parameters supported by the component, and close the component.

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?

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 files. 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.

Other anti-virus software vendors try to reduce the overall scan time by cutting the number or types of files scanned – 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 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 detectable file format 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 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 an 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 directory on your hard drive and select this directory as the license key source directory during the Kaspersky Anti-Virus installation.



Question: *My installation of Kaspersky Anti-Virus does not work. What should I do?*

First of all, try to locate the description of your problem and its solution 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://support.kaspersky.com>.



Question: Why are daily updates 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, 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 application's modules that ensures detected vulnerabilities are repaired, 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 users' feedback and marketing requirements. Additionally, the developers had a task to increase the processability of the entire updates pro-

cedure 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 size of cumulative updates has been cut 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, which 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 overloaded servers.
- For 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 to receive updates from the internet, place them into a local directory and provide access to this directory 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 5.7 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 Linux.

Details on the supported operating systems see 1.5 on p. 8.

The application may perform improperly when run under versions not included in the list of versions supported by Kaspersky Lab. This is, firstly, 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 maximum number of processes started by *kavmonitor* is limited 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 monitor processes always exceeds 1 (by default 20 processes 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 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 file the information which 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 at 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,

```
# /opt/kaspersky/kav4fs/bin/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`.



Question: How can I see the results of application activity after launching the application task via the Kaspersky Administration Kit?

Logging of the application activity launched via Administration Kit is disabled by default.

Make the following changes to the application's configuration file to enable saving of the application tasks results to a file:

- specify the report detail level (see 5.6 on p. 42) via the **ReportLevel** parameter in the **[middleware.options]** section.
- specify the report storage directory.

One of the following files will be created in the specified directory:

- `kavscanner_middleware.log` – upon completion of the on-demand scan task;
- `keepup2date_middleware.log` – upon completion of the update task.



Question: why mail server working on the same computer with the file server, protected by Kaspersky Anti-Virus, can't send a letter?

If there is a mail or Samba server working on the same computer with the file server, then it is possible that infected file is to processed by this server. The `kavmonitor` component will detected the threat before it is processed and prevent access to it.

If data, processed by mail or other server is protected via anti-virus application, then such situations can be avoided. You are recommended to add the temporary files and queue directories to the **ExcludeDirs** list of the **[monitor.options]** section of the application configuration file.

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. The company's products consistently 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. Our databases are 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 Lab News Agent

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

News Agent enables users to;

- See the current virus forecast .in the system tray
- Subscribe to and unsubscribe from news feeds
- Retrieve news from each selected feed at the specified interval and receive notifications about fresh news
- Review news on the selected feeds
- Review the list of feeds and their status
- Open full article text in your browser

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

Kaspersky® OnLine Scanner

This program is a free service provided to the visitors of Kaspersky Lab's corporate website. The service delivers an efficient online anti-virus scan of your computer. Kaspersky OnLine Scanner runs directly from your browser. This way, users receive quick responses to questions regarding potential infections on their computers. Using the service, visitors can:

- Exclude archives and e-mail databases from scanning
- Select standard/extended 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 available to the visitors of Kaspersky Lab's corporate website. The service delivers an efficient online anti-virus scan of your computer and disinfects 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 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), regardless 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, folders, 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:

- **Controls modifications within the 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.
- **Monitors 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 active processes occur.
- **Monitors changes in OS registry** due to internal system registry control.
- **Blocks dangerous VBA macros** in Microsoft Office documents.
- **Performs system restore** after malware attacks by logging all changes to the registry and computer file system and rolls them 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 major information- threats (viruses, hackers, spam and spyware). A single interface enables fusers to configure and manage all the program's components.

The anti-virus protection features include:

- **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), regardless of the mail client being used. The program includes plug-ins for popular e-mail clients (such as Microsoft Office Out-

look, Microsoft Outlook Express/Windows Mail, 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, folders or drives. In addition, the application can perform anti-virus analysis exclusively for critical areas of the operating system and Microsoft Windows start-up objects.
- **Proactive protection:** the program constantly monitors 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 ensured by recognition of phishing attacks, thereby preventing confidential data leaks (above all passwords, bank account and credit card numbers) and blocking execution of dangerous scripts on web pages, pop-up windows and advertisement banners. The **autodialer blocking** feature helps identify software that attempts to use your modem for hidden unauthorized connections to paid phone services and blocks 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 network 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 to Stealth Mode, the system blocks all network activity except for a few transactions allowed in user-defined rules.

The program employs an all-inclusive 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 learning algorithm
- Recognition of spam sent in image files

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 well as files when attempts are made to access them
- **Protection from text message spam**

Kaspersky Anti-Virus for File Servers

This software package provides reliable protection for file systems on servers running Microsoft Windows, Novell NetWare, Linux and Samba from all types of malware. The suite includes the following Kaspersky Lab applications:

- [Kaspersky Administration Kit](#).
- [Kaspersky Anti-Virus for Windows Server](#).
- [Kaspersky Anti-Virus for Linux File Server](#).
- [Kaspersky Anti-Virus for Novell Netware](#).
- [Kaspersky Anti-Virus for Samba Server](#).

Features and functionality:

- *Protects server file systems in real time*: All server files are scanned when opened or saved on the server
- *Prevents virus outbreaks*;
- *On-demand scans* of the entire file system or individual files and folders;
- *Use of optimization technologies* when scanning objects in the server file system;
- *System rollback after virus attacks*;
- *Scalability of the software package* within the scope of system resources available;
- *Monitoring of the system load balance*;
- *Creating a list of trusted processes* whose activity on the server is not subject to control by the software package;
- *Remote administration* of the software package, including centralized installation, configuration, and administration;
- *Saving backup copies of infected and deleted objects* in case you need to restore them;
- *Quarantining suspicious objects*;
- *Send notifications on events* in program operation to the system administrator;

- *Log detailed reports;*
- *Automatically update program databases.*

Kaspersky Open Space Security

Kaspersky Open Space Security is a software package with a new approach to security for today's corporate networks of any size, providing centralized protection information systems and support for remote offices and mobile users.

The suite includes four programs:

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Specifics on each program are given below.

Kaspersky WorkSpace Security is a program for centralized protection of workstations inside and outside of corporate networks from all of today's Internet threats (viruses, spyware, hacker attacks, and spam).

Features and functionality:

- Comprehensive protection from viruses, spyware, hacker attacks, and spam;
- Proactive Defense from new malicious programs whose signatures are not yet added to the database;
- Personal Firewall with intrusion detection system and network attack warnings;
- Rollback for malicious system modifications;
- Protection from phishing attacks and junk mail;
- Dynamic resource redistribution during complete system scans;
- Remote administration of the software package, including centralized installation, configuration, and administration;
- Support for Cisco[®] NAC (Network Admission Control);
- Scanning of e-mail and Internet traffic in real time;
- Blocking of popup windows and banner ads when on the Internet;
- Secure operation in any type of network, including Wi-Fi;

- Rescue disk creation tools that enable you to restore your system after a virus outbreak;
- An extensive reporting system on protection status;
- Automatic database updates;
- Full support for 64-bit operating systems;
- Optimization of program performance on laptops (Intel® Centrino® Duo technology);
- Remote disinfection capability (Intel® Active Management, Intel® vPro™).

Kaspersky Business Space Security provides optimal protection of your company's information resources from today's Internet threats. Kaspersky Business Space Security protects workstations and file servers from all types of viruses, Trojans, and worms, prevents virus outbreaks, and secures information while providing instant access to network resources for users.

Features and functionality:

- Remote administration of the software package, including centralized installation, configuration, and administration;
- *Support for Cisco® NAC (Network Admission Control);*
- *Protection of workstations and file servers from all types of Internet threats;*
- *iSwift technology to avoid rescanning files within the network;*
- *Distribution of load among server processors;*
- *Quarantining suspicious objects from workstations;*
- *Rollback for malicious system modifications;*
- *scalability of the software package within the scope of system resources available;*
- *Proactive Defense* for workstations from new malicious programs whose signatures are not yet added to the database;
- *Scanning of e-mail and Internet traffic* in real time;
- *Personal Firewall* with intrusion detection system and network attack warnings;
- *Protection while using Wi-Fi networks;*
- *Self-Defense from malicious programs;*
- *Quarantining suspicious objects;*

- *automatic database updates.*

Kaspersky Enterprise Space Security

This program includes components for protecting linked workstations and servers from all today's Internet threats. It deletes viruses from e-mail, keeping information safe while providing secure access to network resources for users.

Features and functionality:

- Protection of workstations and file servers from viruses, Trojans, and worms;
- Protection of Sendmail, Qmail, Postfix and Exim mail servers;
- Scanning of all e-mails on Microsoft Exchange Server, including shared folders;
- Processing of e-mails, databases, and other objects for Lotus Domino servers;
- Protection from phishing attacks and junk mail;
- preventing mass mailings and virus outbreaks;
- scalability of the software package within the scope of system resources available ;
- Remote administration of the software package, including centralized installation, configuration, and administration;
- Support for Cisco ® NAC (Network Admission Control);
- Proactive Defense for workstations from new malicious programs whose signatures are not yet added to the database ;
- Personal Firewall with intrusion detection system and network attack warnings ;
- Secure operation while using Wi-Fi networks;
- Scans Internet traffic in real time;
- Rollback for malicious system modifications;
- Dynamic resource redistribution during complete system scans;
- Quarantining suspicious objects ;
- An extensive reporting system on protection system status;
- automatic database updates.

Kaspersky Total Space Security

This solution monitors all inbound and outbound data streams (e-mail, Internet, and all network interactions). It includes components for protecting workstations and mobile devices, keeps information safe while providing secure access for users to the company's information resources and the Internet, and ensures secure e-mail communications.

Features and functionality:

- *Comprehensive protection from viruses, spyware, hacker attacks, and spam* on all levels of the corporate network, from workstations to Internet gateways;
- Proactive Defense for workstations from new malicious programs whose signatures are not yet added to the database ;
- *Protection of mail servers and linked servers*;
- *Scans Internet traffic* (HTTP/FTP) entering the local area network in real time;
- scalability of the software package within the scope of system resources available ;
- *Blocking access from infected workstations*;
- *Prevents virus outbreaks*;
- *Centralized reporting on protection status*;
- Remote administration of the software package, including centralized installation, configuration, and administration;
- *Support for Cisco® NAC* (Network Admission Control);
- *Support for hardware proxy servers*;
- *Filters Internet traffic* using a trusted server list, object types, and user groups;
- *iSwift technology to avoid rescanning files within the network* ;
- Dynamic resource redistribution during complete system scans;
- Personal Firewall with intrusion detection system and network attack warnings ;
- *Secure operation for users on any type of network*, including Wi-Fi;
- *Protection from phishing attacks and junk mail*;
- *Remote disinfection capability* (Intel® Active Management, Intel® vPro™);
- *Rollback for malicious system modifications*;

- *Self-Defense from malicious programs;*
- *full support for 64-bit operating systems;*
- *automatic database updates.*

Kaspersky Security for Mail Servers

This program is for protecting mail servers and linked servers from malicious programs and spam. The program includes application for protecting all standard mail servers (Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix and Exim) and also enables you to configure a dedicated e-mail gateway. The solution includes:

- [Kaspersky Administration Kit.](#)
- [Kaspersky Mail Gateway.](#)
- [Kaspersky Anti-Virus for Lotus Notes/Domino.](#)
- [Kaspersky Anti-Virus for Microsoft Exchange.](#)
- [Kaspersky Anti-Virus for Linux Mail Server.](#)

Its features include:

- *Reliable protection from malicious or potentially dangerous programs;*
- *Junk mail filtering;*
- *Scans incoming and outgoing e-mails and attachments;*
- *Scans all e-mails on Microsoft Exchange Server for viruses, including shared folders;*
- *Processes e-mails, databases, and other objects for Lotus Notes/Domino servers;*
- *Filters e-mails by attachment type;*
- *Quarantines suspicious objects;*
- *Easy-to-use administration system for the program;*
- *Prevents virus outbreaks;*
- *Monitors protection system status using notifications;*
- *Reporting system for program operation;*
- *scalability of the software package within the scope of system resources available ;*
- *automatic database updates.*

Kaspersky Security for Internet Gateways

This program provides secure access to the Internet for all an organization's employees, automatically deleting malware and riskware from the data incoming on HTTP/FTP. The solution includes:

- [Kaspersky Administration Kit](#).
- [Kaspersky Anti-Virus for Proxy Server](#).
- [Kaspersky Anti-Virus for Microsoft ISA Server](#).
- [Kaspersky Anti-Virus for Check Point FireWall-1](#).

Its features include:

- *Reliable protection from malicious or potentially dangerous programs;*
- *Scans Internet traffic (HTTP/FTP) in real time;*
- *Filters Internet traffic using a trusted server list, object types, and user groups;*
- *Quarantines suspicious objects;*
- *Easy-to-use administration system;*
- *Reporting system for program operation;*
- *Support for hardware proxy servers;*
- Scalability of the software package within the scope of system resources available ;
- *Automatic database updates.*

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam is a cutting-edge software suite 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 Anti-Virus® for MIMESweeper

Kaspersky Anti-Virus® for MIMESweeper provides high-speed scanning of traffic on servers running Clearswift MIMESweeper for SMTP / Clearswift MIMESweeper for Exchange / Clearswift MIMESweeper for Web.

The program is a plug-in and scans for viruses and processes inbound and outbound e-mail traffic 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

End User License Agreement

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

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

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

In accordance with the legislation, regarding KASPERSKY SOFTWARE intended for individual consumers (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, kaspersky anti-spam personal, kaspersky security suite personal, KASPERSKY SECURITY FOR PDA) purchased on line from the KASPERSKY LAB Internet Web Site, customer shall have a period of 7 working days as from the delivery of product to make return of it to the Merchant for exchange or refund, provided the software is NOT unsealed.

Regarding the Kaspersky software intended for individual consumers (KASPERSKY Anti-virus PERSONAL, KASPERSKY Anti-virus PERSONAL PRO, KASPERSKY Anti-hacker, kaspersky anti-spam personal, kaspersky security suite personal, KASPERSKY SECURITY FOR PDA) not purchased online via Internet, this software neither will be returned nor exchanged except for contrary provisions from the partner who sells the product. In this case, Kaspersky LAB will not be held by the partner's clauses.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3. Support.

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

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

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

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

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

(iv) "Support Services" means:

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

(b) Free software updates, including version upgrades;

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

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

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

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

information, but without limitation to the foregoing shall use best endeavours to maintain the security of the Key Identification File.

6. Limited Warranty.

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

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

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

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

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

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

7. Limitation of Liability.

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

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

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

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

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

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