

KASPERSKY LAB

---

Kaspersky Anti-Virus® 5.5  
for Samba Servers

ADMINISTRATOR'S  
MANUAL

KASPERSKY ANTI-VIRUS® 5.5 FOR SAMBA SERVERS

---

# Administrator's manual

© Kaspersky Lab Ltd.

<http://www.kaspersky.com>

Revision date: November 2006

# Contents

CHAPTER 1. INTRODUCTION .....	5
1.1. Computer viruses and malware .....	5
1.2. The purpose and main features of Kaspersky Anti-Virus .....	6
1.3. Hardware and software system requirements .....	8
1.4. Distribution kit .....	9
1.5. Help desk for registered users .....	10
1.6. Adopted conventions.....	10
CHAPTER 2. INTERNAL ARCHITECTURE OF KASPERSKY ANTI-VIRUS FOR SAMBA SERVERS .....	12
2.1. Component structure.....	12
2.2. Algorithm of operation .....	12
CHAPTER 3. INSTALLATION OF KASPERSKY ANTI-VIRUS .....	14
3.1. Software installation to a server running Linux.....	14
3.2. Software installation to a server running FreeBSD .....	14
3.3. Installation process.....	15
3.4. Configuring the application.....	15
3.5. Locations of product files.....	16
3.6. Upgrading your Samba server.....	19
3.7. Uninstalling Kaspersky Anti-Virus.....	19
CHAPTER 4. POST-INSTALL CONFIGURATION.....	21
4.1. Default product settings.....	21
4.2. Installing the anti-virus databases.....	22
4.3. Setting the product up for work with Webmin.....	22
4.4. Recommended operation modes .....	23
4.4.1. Optimal operation mode .....	23
4.4.2. Top performance mode.....	24
4.4.3. Top reliability mode.....	25
4.4.4. Scanning mode for frequently modified files.....	26

---

CHAPTER 5. USING KASPERSKY ANTI-VIRUS FOR SAMBA SERVERS.....	28
5.1. Anti-Virus Database Updating.....	28
5.1.1. Automatic updating of the anti-virus databases.....	30
5.1.2. On-demand update of the anti-virus databases.....	31
5.1.3. Creation of a network directory for storage and downloading of anti-virus databases.....	32
5.2. Real-time anti-virus protection of Samba servers.....	33
5.2.1. Setup of user's notifications.....	34
5.2.1.1. Monitoring with notifications through smbclient.....	34
5.2.1.2. Monitoring with e-mail notifications.....	35
5.3. Anti-Virus protection of file systems.....	35
5.3.1. On-demand scanning of files.....	36
5.3.2. Scheduled scanning of a directory (cron).....	37
5.3.3. Additional opportunities: using scripts.....	37
5.3.3.1. E-mail notification of administrator.....	37
CHAPTER 6. ADDITIONAL SETUP.....	39
6.1. Tuning real-time anti-virus protection.....	39
6.1.1. Scope of monitoring.....	39
6.1.2. File scanning and disinfection mode.....	40
6.1.3. File operations.....	41
6.1.4. Quarantine for infected objects.....	41
6.1.5. Backup copying of objects.....	42
6.2. Setup of anti-virus protection for server file systems.....	43
6.2.1. Scanning area.....	43
6.2.2. File scanning and disinfection mode.....	44
6.2.3. File operations.....	45
6.2.4. Backup mode settings.....	45
6.3. Optimizing Kaspersky Anti-Virus for Samba Servers.....	46
6.4. Restarting Kaspersky Anti-Virus for Samba Servers.....	48
6.5. Localization of displayed date and time format.....	49
6.6. Reporting parameters in Kaspersky Anti-Virus.....	50
CHAPTER 7. LICENSE KEYS MANAGEMENT.....	52
7.1.1. Viewing license key information.....	52
7.1.2. License extension.....	53

---

7.1.3. License key removal.....	54
CHAPTER 8. CHECKING CORRECT OPERATION OF THE ANTI-VIRUS .....	56
CHAPTER 9. FREQUENTLY ASKED QUESTIONS.....	58
APPENDIX A. ADDITIONAL INFORMATION ABOUT THE APPLICATION .....	63
A.1. Kaspersky Anti-Virus configuration file.....	63
A.2. Command line options for the kavsamba component.....	71
A.3. Kavsamba return codes.....	71
A.4. Command line options for the kavscanner component.....	72
A.5. Kavscanner return codes.....	75
A.6. Command line options for the licensemanager component.....	76
A.7. Licensemanager return codes.....	76
A.8. Command line options for the keepup2date component .....	77
A.9. keepup2date return codes.....	78
APPENDIX B. KASPERSKY LAB.....	79
B.1. Other Kaspersky Lab Products .....	80
B.2. Contact Us.....	86
APPENDIX C. LICENSE AGREEMENT .....	87

---

# CHAPTER 1. INTRODUCTION

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

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

## **Internet**

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

## **E-mail messages**

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

## **Software vulnerabilities**

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

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

## 1.1. Computer viruses and malware

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

**Worms** – malicious programs that belong to this category use network resources for distribution. These programs were called "worms" due to their ability to tunnel from one computer to another, using networks, email

and other channels. Due to this ability, worms can proliferate extremely fast.

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

**Viruses** –programs that *infect* other programs by adding their code to the infected program's code in order to gain control when infected files are run. This simple definition helps determine that the major action a virus performs is *infecting* computer programs. Viruses spread somewhat slower than worms.

**Trojan horses or Trojans** – perform unauthorized actions on infected computers, for instance, depending on the particular conditions, they can erase information on hard drives, "freeze" the system, steal confidential information, etc. In the strict sense, Trojan Horses are not viruses as they do not infect programs or data; they are unable to sneak independently into computers and therefore are distributed by impostors disguised as some "useful" software. However, Trojans may inflict far greater damages compared to a regular virus attack.

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



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

## 1.2. The purpose and main features of Kaspersky Anti-Virus

**Kaspersky Anti-Virus® 5.5 for Samba Servers** software application (hereinafter also called **Kaspersky Anti-Virus**) performs anti-virus scanning of objects for Samba servers running Linux or FreeBSD operating systems.

The application accomplishes two-level scanning of server file systems both in real-time and in the on-demand scanning mode. If malicious code is detected Kaspersky Anti-Virus can cure or block the infected objects efficiently in order to prevent further spreading of epidemics providing timely notifications to system administrators about such accidents.



The application also employs iChecker™ – an intellectual technology, which allows considerable increase of file scanning speed.

Kaspersky Anti-Virus for Samba Servers is a package of anti-virus components performing the following functions:

- *Real-time protection of Samba file server from malicious code (**On-Access Scanner**).*
- *On-demand searching and neutralization of malicious code in the server file system (**On-Demand Scanner**).*
- *Notifications to the administrator about detection of infected or suspicious objects.*
- *Maintaining the current status of the anti-virus databases (**keepup2date**).*
- *Local and remote administration using a web administration module (**Webmin**).*

Besides, Kaspersky Anti-Virus offers the following additional functionality to its users:

- An opportunity to run user-defined scripts in cases, when events of the “an infected file was detected” type occur.
- An opportunity to move infected (or suspicious) objects to a special storage location (quarantine).
- Preserving the original infected object prior to its disinfection (Backup) with an opportunity to restore it in a non-standard situation.
- Saving information about already scanned files in an operational cache, which allows a considerable increase of file scanning speed during subsequent access to such files (the cache preserves the information until application restart).
- An opportunity to restrict the maximum number of files for simultaneous real-time scanning while adding the rest of the requested files to a scanning queue.
- An opportunity to suspend automatically the anti-virus background file scanning, when the server load exceeds the user-defined level – and resume operation, when the server load reaches an acceptable level.
- An opportunity to define any combination of “scanning on access” and “scanning on saving” modes for each public directory.
- An opportunity to define selectively individual anti-virus protection settings for each public directory.

- The least loaded updates' server of Kaspersky Lab is detected during the updating of the anti-virus databases. Besides, in cases of line disconnection the updating process after reconnection resumes its work from the place where it left off.
- An opportunity to roll back both the updates to anti-virus databases and application updates.

## 1.3. Hardware and software system requirements

Operation of **Kaspersky Anti-Virus for Samba Servers** requires:

- Intel Pentium® 133 MHz CPU or better.
- 64 MB RAM.
- 100 MB of disk space for application installation and storage of temporary files.
- Software requirements:
  - One of the following operating systems for a 32-bit platform:
    - RedHat Linux 9.0.
    - RedHat Enterprise Linux Advanced Server 4 UPD3.
    - SUSE Linux Enterprise Server 9.0 SP3.
    - SUSE Linux Professional 10.1.
    - Debian GNU/Linux 3.1 R2.
    - Mandriva 2006.
    - FreeBSD 4.11.
    - FreeBSD 5.4.
    - FreeBSD 6.1.
  - One of the following operating systems for a 64-bit platform:
    - RedHat Enterprise Linux Advanced Server 4 UPD3.
    - RedHat Fedora Core 5.
    - SUSE Linux Professional 10.1.
    - SUSE LES 9 SP3.
  - The Webmin program ([www.webmin.com](http://www.webmin.com)) for remote administration of Kaspersky Anti-Virus.

- Perl language interpreter, version 5.0 or newer ([www.perl.org](http://www.perl.org)).
- Installed Samba server 2.2.7 and newer or 3.0.0-3.0.23c.



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

Besides, if your server uses protection based on File System Access Control Lists (ACLs), you will have to configure Samba server to support that functionality.

## 1.4. Distribution kit

You can purchase Kaspersky Anti-Virus either from our distributors (retail box) or in our Internet-shop ([www.kaspersky.com](http://www.kaspersky.com), **Buy online** section).

When purchasing a retail box you will receive the following distribution kit:

- A sealed envelope with an installation CD (or a set of floppy disks) containing software product files.
- Administrator's guide.
- Register card (with the serial number)
- License key.
- License agreement.



Before you unseal the envelope containing the CD (or floppy disks), be sure to thoroughly review the license agreement.

When purchasing Kaspersky Anti-Virus in the Web-shop you download the product from Kaspersky Lab's website. The distribution file contains the product and the license key.

The License Agreement (LA) is a legal agreement between you (either an individual or a single entity) and the manufacturer (Kaspersky Lab Ltd.) describing the terms on which you may employ the anti-virus product, which you have purchased.



**Make sure to read the terms of the LA!**

If you do not agree to the terms of this LA, Kaspersky Lab is not willing to license the software product to you and you should return the unused product to your Kaspersky Anti-Virus dealer for a full refund, making sure the envelope with CD (or diskettes) is sealed.

If you unsealed the envelope, you have agreed to all the terms of the LA.

## 1.5. Help desk for registered users

Kaspersky Lab offers a large service package enabling legal users to efficiently employ Kaspersky Anti-Virus.

If you register and purchase a subscription you will be provided with the following services for the period of your subscription:




- daily virus definition database updates via e-mail;
- product upgrades;
- phone and e-mail advice on matters related to your software installation, configuration and performance;
- information about new Kaspersky Lab products and new computer viruses (for those who subscribe to our newsletter).





Kaspersky Lab does not give advice on the performance and use of your operating system or various other technologies.

## 1.6. Adopted conventions

The text in this document uses various styles depending upon its purpose. The table below lists adopted conventions used in the text.

Style	Purpose
<b>Bold type</b>	Menu titles, menu items, window titles, parts of dialog boxes, etc.
 <b>Note.</b>	Additional information, notes.
 <b>Attention!</b>	Information that should be paid special attention.
 <i>In order to perform the action,</i>  1. Step 1. 2. ...	Procedure description for user's steps and possible actions.

Style	Purpose
 Task, example	Statement of problem, example for using the software features.
 Solution	Solution to a defined problem.
<b>[key]</b> – key purpose.	Command line keys.
Text of information messages and the command line	Text of configuration files, information messages and the command line.

---

# CHAPTER 2. INTERNAL ARCHITECTURE OF KASPERSKY ANTI-VIRUS FOR SAMBA SERVERS

Before we describe the features of Kaspersky Anti-Virus for Samba Servers let us discuss its internal architecture in detail. That will allow better understanding of the Anti-Virus operation algorithm.

## 2.1. Component structure

Kaspersky Anti-Virus for Samba Servers consists of the following components:

- *kavsamba* (or an On-Access Scanner);
- *kavscanner* (or an On-Demand Scanner);
- *keepup2date*.

The *kavsamba* component, in its turn, includes the *kavsamba.so* and *kavsamba* modules. The *kavsamba.so* is implemented in the form of a dynamic library integrated into Samba server and intercepting attempts to access files through that Samba server. The *kavsamba* module is a daemon process analyzing the files provided by the *kavsamba.so* files and processing them in accordance with the current settings. Data exchange between the module and the daemon process is accomplished through a local socket (Unix Domain sockets).

The *kavscanner* component is designed for anti-virus protection of file systems. Server file systems or individual directories are scanned according to the administrator's demand or the schedule (depending upon selected settings).

The *keepup2date* component updates the anti-virus databases used during scanning and disinfection and also downloads patches to the package programs.

## 2.2. Algorithm of operation

Here we shall review internal architecture of the product in terms of real-time anti-virus protection since the on-demand scanning process is fairly simple and does not require any special coverage.

So the used algorithm of operation is as follows:

1. If a user attempts to access a file through Samba server the request is intercepted by the server itself and transferred to the *kavsamba.so* module.
2. The *kavsamba.so* module sends the data pertaining to the request (file name, its full path, ID of the user who requested the file, computer domain name) to the *kavsamba* component through IPC using binary protocol.
3. The *kavsamba* module scans the requested object for viruses and processes it in accordance with the settings in the configuration file (including the use of anti-virus databases, if that option is enabled).
4. Upon completion of file scanning and processing *kavsamba.so* receives from *kavsamba* the access code (granted/denied), which determines the file status.
5. In accordance with the object status *kavsamba.so* transfers to the Samba server a permit to access the object or blocks the latter.

Access to a file is blocked if the latter is infected or looks suspicious (Infected, CureFailed, Warning, Suspicion). In all other cases access to the file is granted.

---

# CHAPTER 3. INSTALLATION OF KASPERSKY ANTI-VIRUS

Prior to beginning the installation of Kaspersky Anti-Virus we recommend the following preparations for your system:

- Make sure that your system conforms to the hardware and software requirements for installation of the Kaspersky Anti-Virus (please see section 1.3 on p. 7).
- Enter the system as superuser (**root**).

## 3.1. Software installation to a server running Linux

Kaspersky Anti-Virus for computers running Linux is distributed in two variants of installation packages:

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



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

```
rpm -i <package_file_name>
```



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

```
dpkg -i <package_file_name>
```

## 3.2. Software installation to a server running FreeBSD

The installation package of Kaspersky Anti-Virus is supplied in a pkg package for servers running FreeBSD operating system.



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

```
pkg_add <package_name>
```

## 3.3. Installation process



For several reasons the process of installation may terminate with an error code. In such cases make sure that your computer conforms to the hardware and software requirements (please see section 1.3 on p. 7) and that you have logged into the system with root privileges.

The application is installed to a server in several stages:

1. Copying the installation package files to a server.
2. Configuration of the *keepup2date* component.
3. Installation (updating) of the anti-virus databases.



Ensure that the anti-virus databases are installed before you begin using the product. The procedure of anti-virus scanning and disinfection depends upon the records in the anti-virus databases containing descriptions of all currently known viruses and cure methods for infected objects. Scanning and processing of files cannot be performed without anti-virus databases!

Please note also that automatic configuration of the application will not be performed if the anti-virus databases are not installed.

4. License key installation.

If a license key is not installed, configuration will not be performed and it will be impossible to use the application. However, if the key is missing temporarily (for example, the product has been purchased via the Internet and the license key hasn't been received by e-mail yet) you can install it after installation, before beginning to actually use the product.

5. Installation of a Webmin module.

Remote control module for the Webmin package will be installed only if Webmin has a standard path. After module installation you will receive respective recommendations for its setup to work with the application.

## 3.4. Configuring the application

System configuration is performed immediately upon copying the installation package files to server. Depending upon the package manager the configuration stage will either start automatically or (if the package manager does not allow using interactive packages like *.rpm*, for example) require some additional

actions on the user's part. A respective message will appear on-screen in that case.

The process of configuring the application consists of the following stages:

- Search for an installed Samba server and checking its version for conformity with the software requirements.
- Search and modification of the Samba server configuration file.
- Checking the Samba server configuration file for presence of VFS objects. If the Samba server configuration file contains lines indicating VFS objects in use, they will be commented.



If you are using FreeBSD with Samba server versions 3.0-3.0.9, incorrect handling of VFS modules is possible because of certain specific peculiarities of the operating system.

To ensure proper interaction between the application and VFS objects, you are advised to upgrade your Samba server version or install a patch for Samba server (please see [https://bugzilla.samba.org/show\\_bug.cgi?id=2100](https://bugzilla.samba.org/show_bug.cgi?id=2100) for details about the patch).

If the system configuration requires some additional information (e.g., the path to the Samba server configuration file) the respective questions will be output to server console. Entry of incorrect responses will abort the configuration process.

If the above configuration stages complete successfully, the application will be ready for work, no additional notifications will be produced. The configuration file supplied with the product package contains all settings necessary to start working.



Please keep in mind that you have to restart the Samba server before you can proceed to further work.

## 3.5. Locations of product files

After Kaspersky Anti-Virus installation its files will be placed in the following locations (provided that all default paths suggested during the procedure are accepted):

### In Linux:

*/etc/opt/kaspersky/* – the directory containing the configuration file of Kaspersky Anti-Virus and other files with various settings:

*kav4samba.conf* – configuration file.

*/var/opt/kaspersky/kav4samba/bases* and */var/opt/kaspersky/kav4samba/licenses* – the directories containing the anti-virus databases and license keys respectively.

*/opt/kaspersky/kav4samba* – the main directory of the Anti-Virus containing:

- /bin/* – the directory for executable files of all the components included into Kaspersky Anti-Virus for Samba Servers:
  - kav4samba-kavscanner* – executable file of the kavscanner component responsible for anti-virus protection of file servers (On-Demand Scanner).
  - kav4samba-licensemanager* – executable file of the licensemanager component used for operations with license keys.
  - kav4samba-keepup2date* – executable file of the keepup2date component updating the anti-virus databases.
- /sbin/kav4samba-kavsamba* – executable file of the kavsamba real-time protection component (On-Access Scanner).
- /lib/bin/setup/kavsamba\_setup.pl* – the script used to integrate the product with your Samba server.
- /share/man* – directory containing man files.



In order to enable using the reference system of Kaspersky Anti-Virus (manual pages), add the */opt/kaspersky/kav4samba/share/man* path to the **MANPATH** environment variable.

*/opt/kaspersky/kav4samba/lib/* – directory containing Samba modules for 32-bit operating systems.

*/opt/kaspersky/kav4samba/lib64/* – directory containing Samba modules for 64-bit operating systems.

*/opt/kaspersky/kav4samba/share/contrib/kavsamba.wbm* – directory containing the plug-in module for Webmin.

*/opt/kaspersky/kav4samba/share/contrib/vox.sh* – script for disinfection of archives.

*/opt/kaspersky/kav4samba/share/doc/* – directory containing licenses and Samba documentation.

*/opt/kaspersky/kav4samba/src/* – directory containing the source code of the Samba plug-in module.

*/var/opt/kaspersky/kav4samba/bases/* – directory containing the anti-virus databases.

*/var/opt/kaspersky/kav4samba/bases.backup/* – directories containing backup copies of the anti-virus databases (for a database roll-back, if necessary).

*/var/log/kaspersky /* – directory containing the log files generated by the application components.

**In FreeBSD:**

*/usr/local/etc/kaspersky/* – the directory containing the configuration file of Kaspersky Anti-Virus and other files with various settings:

*kav4samba.conf* – configuration file.

*kav4samba.conf.default* – configuration file containing the default settings.

*/var/db/kaspersky/kav4samba/bases/* and

*/var/db/kaspersky/kav4samba/licenses/* – the directories containing the anti-virus databases and license keys respectively.

*/usr/local/* – system directory where the administrator installs programs. Kaspersky Anti-Virus adds to the directory executable files of all its components:

*kav4samba-kavscanner* – executable file of the kavscanner component responsible for anti-virus protection of file servers (On-Demand Scanner).

*kav4samba-licensemanager* – executable file of the licensemanager component used for operations with license keys.

*kav4samba-keepup2date* – executable file of the keepup2date component updating the anti-virus databases.

*/usr/local/sbin/kav4samba-kavsamba* – executable file of the kavsamba real-time protection component (On-Access Scanner).

*/usr/local/libexec/kaspersky/kav4samba/setup/kavsamba\_setup.pl* – the script used to integrate the product with your Samba servers.

*/usr/local/man/* – directory containing man files.

*/usr/local/lib/kaspersky/kav4samba/* – directory containing Samba modules for 32-bit operating systems.

*/usr/local/share/kav4samba/contrib/kavsamba.wbm* – directory containing the plug-in module for Webmin.

*/usr/local/share/kav4samba/contrib/vox.sh* – script for disinfection of archives.

*/usr/local/share/doc/kav4samba/* – directory containing licenses and Samba documentation.

*/usr/local/src/kav4samba/* – directory containing the source code of the Samba plug-in module.

*/var/db/kaspersky/kav4samba/bases.backup/* – directories containing backup copies of the anti-virus databases (for a database roll-back, if necessary).

*/var/log/kaspersky/* – directory containing the log files generated by the application components.



In all further discussions of sample tasks we shall assume that Kaspersky Anti-Virus is installed on a server running Linux.

## 3.6. Upgrading your Samba server



*The distribution package of Kaspersky Anti-Virus contains binary VFS modules for supported Samba versions.*

*If you have a new Samba Server version unsupported by Kaspersky Anti-Virus, you can rebuild the VFS module of the application manually.*

*In order to do that perform the following steps:*

If you are running Linux, enter the following in the command line:

```
cd /opt/kaspersky/kav4samba/src
./configure --with-sambasrc=<path_to_samba>
&& make
```

where <path\_to\_samba> stands for the path to the source code of the Samba Server modules.

If you are running FreeBSD, enter the following in the command line:

```
cd /usr/local/src/kav4samba
./configure --with-sambasrc=<path_to_samba> && make
```

where <path\_to\_samba> stands for the path to the source code of the Samba Server modules.

An updated version of the VFS module will be created in the **/lib** subdirectory. The administrator will have to configure and install the module then.

## 3.7. Uninstalling Kaspersky Anti-Virus

The procedure of uninstalling Kaspersky Anti-Virus for Samba Servers requires the following:

- Superuser privileges (**root** or another user with UID=0). If you have no such privileges at the moment of uninstall procedure you'll have to enter the system as **root**.
- Stopped Samba server.



**The uninstaller routine does not stop the Samba server on its own!**

Kaspersky Anti-Virus removal will be performed automatically. The uninstall procedure uses different methods depending upon the distribution package type.



*If you installed Kaspersky Anti-Virus for Samba Servers using its .rpm package enter the following in the command line to begin uninstalling:*

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



*If you installed Kaspersky Anti-Virus for Samba Servers using its .deb package enter the following in the command line to begin uninstalling:*

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



The control scripts cannot be deleted automatically in Debian GNU/Linux because of certain peculiarities of that operating system. As soon as the uninstall procedure completes, the administrator will have to remove the `/opt/kaspersky/kav4samba/lib/bin/kav4samba` script manually from the system.



*If you installed Kaspersky Anti-Virus for Samba Servers using its pkg package enter the following in the command line to begin uninstalling:*

```
pkg_delete <package_name>
```

No additional notifications are output if the uninstall procedure completes successfully.



If you have installed the remote administration plug-in for **Webmin**, it should be removed manually.

To do so, open the **Webmin Modules** tab in the main Webmin window and select in the **Delete Modules** list the **KAV for Samba Servers** line. Then click the **Delete Selected Modules** button.

---

# CHAPTER 4. POST-INSTALL CONFIGURATION

The installation routine performs analysis of the system, where Kaspersky Anti-Virus is being installed to and defines some parameters of its configuration automatically. Several parameters of the product configuration file are defined by default as most convenient for work with the Anti-Virus (please see section 4.1 on p. 21).



Prior to beginning work with the product we recommend installing or updating its anti-virus databases if you haven't done so during installation!

In addition, you should configure Kaspersky Anti-Virus for work with the Webmin package.

This chapter is devoted to discussing the default settings of Kaspersky Anti-Virus and detailed review of the configuration necessary for product operation.

## 4.1. Default product settings

All parameters pertaining to the operation of Kaspersky Anti-Virus are recorded in its default configuration file.



You can create your own configuration files and use them both for current tasks and as the default configuration.

Let us review closely the default parameters defined in that file. Based on the information in this section you can determine whether Kaspersky Anti-Virus needs additional tuning (please see Chapter 6 on p. 39) for its more efficient integration in your corporate environment.

The default configuration of Kaspersky Anti-Virus suggests that the real-time protection component (*kavsamba*) begins working at the start of the operating system. Starting the on-demand scanning component (*kavscanner*) without additional command line keys forces *anti-virus scanning* of server directories and file systems beginning with the current one.

If infected, suspicious or corrupted files are discovered, respective notifications are output to console and appended to the report file.



Please note that discovered infected files ARE NOT CURED BY DEFAULT!

## 4.2. Installing the anti-virus databases

Kaspersky Anti-Virus detects viruses and cures infected objects using the records in its anti-virus databases. These databases contain descriptions of all currently known malicious programs and methods of their disinfection. Therefore maintaining the updated status of the anti-virus databases is an essential task.



New viruses appear every day. Therefore, you should update the anti-virus databases **immediately** after product installation because the databases included into the distribution package may be outdated by that time.

In order to update the anti-virus databases, you have to start the *keepup2date* component. Enter the following in the command line:

```
/path/to/kav4samba-keepup2date
```

The anti-virus databases will be copied from the Kaspersky Lab updates' servers to a special directory defined in the configuration file.

## 4.3. Setting the product up for work with Webmin

If you plan to configure Kaspersky Anti-Virus remotely we recommend that you set it up for work with the Webmin package.

For example, Webmin may be used for restriction of access to the program through a system of user passwords.

All Anti-Virus settings modified remotely through Webmin are saved to the default configuration file of the application.



*If you wish to create an alternative configuration file using Webmin, you'll have to perform the following actions:*

1. Copy the data from the existing configuration file to a new one saving it under a different name. Then modify the new (alternative) configuration file in accordance with your tasks.
2. Specify the alternative configuration file name in the **Full path to KAV config** parameter entry field of the **Config edit** tab.



Please refer to Webmin documentation for details about different settings of that program. In addition, you can use Webmin help to resolve questions about the plug-in module for remote product administration.

Configuration and start of various tasks discussed further **do not** include descriptions of procedures necessary for remote management within Webmin!

## 4.4. Recommended operation modes

Kaspersky Lab recommends several variants of setup depending upon server load in order to achieve the most efficient operation of Kaspersky Anti-Virus for Samba Servers. Let us review those variants in detail.

### 4.4.1. Optimal operation mode

This mode ensures optimal balance between server performance and established protection level.



*In order to define the optimal mode of operation enter the following changes to the configuration file:*

- Set the file cache size to be approximately equal to the number of files accessible through the Samba server. We recommend proceeding from the assumption that a clear file record in the cache requires about 50 bytes (**FileCacheSize**) parameter in the **[samba.options]** section).
- Set the following parameter values in the **[path]** section:  

```
IcheckerDbFile=/var/opt/kaspersky/kav4samba/ichecker.db
```
- Set the following parameter values in the **[samba.options]** section:  

```
Packed=yes  
Archives=yes  
SelfExtArchives=yes  
MailBases=yes  
MailPlain=yes  
Heuristic=yes  
Cure=yes  
Ichecker=yes  
CheckFilesLimit=20  
BgCheckFilesLimit=5  
BgSheduleTime=10
```

HashType=md5

- Set the following parameter values in the **[samba.path]** section:
 

```
BackupPath=/var/opt/kaspersky/kav4samba/infected
SambaConfigFile=/etc/samba/smb.conf
```
- Set the following parameter values in the **[samba.actions]** section:
 

```
OnInfected=MovePath /tmp/infected
OnSuspicion=MovePath /tmp/suspicious
OnWarning=MovePath /tmp/warning
```
- Set the following parameter values in the **[samba.shares]** section:
 

```
CheckOnOpen=yes
CheckOnClose=yes
```



Please make sure that the **iChecker** technology has been also enabled for the *kavscanner* component (section **[scanner.options]**, parameter **Ichecker=yes**). Besides, the *kavsamba* and *kavscanner* components must use the same options for the **Packed, Archives, SelfExArchives, MailBases, MailPlain, and Heuristic** parameters (**[scanner.options]** and **[samba.options]** sections).

## 4.4.2. Top performance mode

This mode provides for maximum application performance, however, reliability of anti-virus protection is somewhat decreased.

It is recommended to switch off scanning of archives and checking of files being closed. Thus the application will not scan archives, which may be infected. Infected objects may also be saved to the server; such objects will be scanned only when accessed for opening (if users attempt to access the objects for reading).



*In order to set the mode up you should enter the following modifications to the configuration file:*

- Set the following parameter values in the **[samba.options]** section:
 

```
Ichecker=no
FileCacheSize=15000
CheckFilesLimit=0
HashType=crc32
```
- Set the following parameter values in the **[samba.shares]** section:

```
CheckOnOpen=yes
CheckOnClose=no
```

### 4.4.3. Top reliability mode

This variant of program settings accomplishes maximum reliability of server protection since files are scanned during reading and writing, however, the application performance will be slightly lower.



*In order to set the mode up you should enter the following modifications to the configuration file:*

- Set the following parameter values in the **[samba.options]** section:

```
Packed=yes
Archives=yes
SelfExtArchives=yes
MailBases=yes
MailPlain=yes
Heuristic=yes
Cure=yes
Ichecker=yes
FileCacheSize=0
CheckFilesLimit=0
BgCheckFilesLimit=0
BgSheduleTime=0
HashType=md5
```

- Set the following parameter value in the **[samba.path]** section:

```
BackupPath=/var/opt/kaspersky/kav4samba/infected
```

- Set the following parameter values in the **[samba.actions]** section:

```
OnInfected=remove
OnSuspicion=remove
OnWarning=remove
```



Please make sure that the **iChecker** technology has been also enabled for the *kavscanner* component (section **[scanner.options]**, parameter **IChecker=yes**). Besides, the *kavsamba* and *kavscanner* components must use the same options for the **Packed**, **Archives**, **SelfExtArchives**, **MailBases**, **MailPlain**, and **Heuristic** parameters (**[scanner.options]** and **[samba.options]**)

sections).

#### 4.4.4. Scanning mode for frequently modified files

This mode is recommended for setting up anti-virus protection of shared directories, where files are frequently updated.

The difference between the mode for checking frequently modified files and the **recommended mode** (please see section 4.4.1 on p. 23) is manifested in the suggestion to skip scanning of files in shared directories after their recording (*public* directory in the example discussed below).

It is recommended to switch off scanning of files being closed for such directories. In that case directory contents will be scanned for virus presence either when a user attempts to access it or during background scanning.

General settings for all other directories will be similar to the **recommended mode**.



*In order to set the mode up you should enter the following modifications to the configuration file:*

- Set the following parameter value in the **[path]** section:  
IcheckerDbFile=  
/var/opt/kaspersky/kav4samba/ichecker.db
- Set the following parameter values in the **[samba.options]** section:  
Packed=yes  
Archives=yes  
SelfExtArchives=yes  
MailBases=yes  
MailPlain=yes  
Heuristic=yes  
Cure=yes  
Ichecker=yes  
FileCacheSize=20000  
CheckFilesLimit=20  
BgCheckFilesLimit=5  
BgScheduleTime=10  
HashType=md5

- Set the following parameter value in the **[samba.path]** section:  
BackupPath=/var/opt/kaspersky/kav4samba/infected  
SambaConfigFile=/etc/samba/smb.conf
- Set the following parameter values in the **[samba.actions]** section:  
OnInfected=remove  
OnSuspicion=remove  
OnWarning=remove
- Set the following parameter values in the **[samba.shares]** section:  
CheckOnOpen=yes  
CheckOnClose=yes
- Set the following parameter values in the **[samba.shares:public]** section:  
CheckOnOpen=yes  
CheckOnClose=no

---

# CHAPTER 5. USING KASPERSKY ANTI-VIRUS FOR SAMBA SERVERS

Anti-virus security is accomplished both in real time and in on-access mode. Let us review those opportunities in detail.

*Real-time protection* is accomplished by means of the *kavsamba* component that intercepts attempts to access files for opening through a Samba server and through background scanning of files being closed. Files are tested for presence of viruses and processed in accordance with software settings. Access to dangerous files is blocked.

During *on-demand scanning* performed by the *kavscanner* component you can order scanning of any file types (including e-mail databases, compressed files, etc.), present in a computer. Scanning results will be used to treat infected files according to the settings in the configuration file.

Besides, the opportunity to *update the anti-virus databases* using the *keepup2date* component is an important aspect of anti-virus security. The component performs both remote and local updating of the anti-virus databases and application modules.



Please note that in all examples for the *kavsamba* component discussed below Kaspersky Anti-Virus must be restarted after making modifications to its configuration file. Please see details on methods for restarting the application in section 6.4 on p.48.

## 5.1. Anti-Virus Database Updating

The application's *keepup2date* component performs the essential function of maintaining the current status of the anti-virus databases, which Kaspersky Anti-Virus uses to scan for infected objects and cure them. They can be downloaded from the servers, where updates available from Kaspersky Lab are stored. For example, such as:

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

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

<ftp://downloads1.kaspersky-labs.com/> and others.

A list of addresses, from which updates can be downloaded, can be found in the *updcfg.xml* file included into the product package.

During the updating procedure the *keepup2date* component accesses the list, picks up an address and attempts to download the anti-virus databases from the server. If the update cannot be obtained from the selected address, the component will switch to the next address and retry downloading the databases.



Updates for anti-virus databases are made available on Kaspersky Lab's update servers several times an hour.

Upon successful update the updater performs the command specified as the value for the **PostUpdateCmd** parameter in the **updater.options]** section of the configuration file). By default the command will initiate reloading of the anti-virus databases. Invalid modification of that parameter may prevent the application from using the updated databases or make it function incorrectly.



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

If your LAN has a rather complicated structure we recommend downloading the updates from the respective servers once every day; the updates should be placed then in a certain network directory and your local network computers should be set up to use that directory as the source of anti-virus database updates. Please see details on task creation for that purpose in section 5.1.3 on p. 32.

The updating procedure can be set up using **cron** (please see section 5.1.1 on p. 30) or the command line (please see section 5.1.2 on p. 31).



We strongly recommend updating your anti-virus databases at least once every hour!

The updating procedure can be set up using **cron** (please see section 5.1.1 on p. 30) or the command line (please see section 5.1.2 on p. 31).

Kaspersky Anti-Virus 5.5 also features an opportunity to select the set of the anti-virus databases, which the product will use, in order to ensure optimal anti-virus security.

*Standard databases* are anti-virus databases containing detailed descriptions of all currently known viruses, methods of their detection and disinfection. These databases are used by default.

*Extended databases* are anti-virus databases that contain also information about potentially dangerous software (RiskWare) and programs that transfer advertisements (AdWare).

Riskware programs contain vulnerabilities that may be exploited for organization of hacker attacks, installation of unauthorized software, etc.

Adware programs are installed together with third party software and start displaying advertisements in additional windows or forcing the user to visit the advertiser's web site. Besides unsolicited advertisement information, such programs also increase considerably the load on communication lines and the traffic.

Standard anti-virus databases are sufficient for normal operation. Extended anti-virus databases are used to ensure higher level of protection. The use of extended anti-virus databases increases the computational resources required to scan the data.

### 5.1.1. Automatic updating of the anti-virus databases

You can schedule regular automatic updating of the anti-virus databases using the cron utility.



**Task:** schedule automatic daily updating of the anti-virus databases to run every 3 hours. The system log should be updated with operational application errors only. A general log of all starts of the task should be created, with no information output to console.



**Solution:** in order to accomplish the task you should perform the following actions:

1. Define respective parameter values in the configuration file for the application, e.g.:

```
[updater.options]
KeepSilent=yes
[updater.report]
Append=yes
ReportLevel=4
```

2. Edit the file containing the rules for the **cron** process (**crontab -e**) by adding the following line into it:

```
0 0-23/3 * * */opt/kaspersky/kav4samba/bin/kav4samba-keepup2date
```



**Task:** configure downloading of updates for the anti-virus databases from the update servers of Kaspersky Lab. The address of the source update server should be automatically picked from the list included with the *keepup2date* component.



**Solution:** in order to accomplish the task you should perform the following actions:

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



**Task:** configure downloading of updates for the anti-virus databases from an administrator-defined address. The updating procedure should be interrupted if updates cannot be retrieved from that address.



**Solution:** in order to accomplish the task you should perform the following actions:

Assign the **Yes** value to the **UseUpdateServerUrl** and **UseUpdateServerUrlOnly** parameters in the **[updater.options]** section. Besides, the **UpdateServerUrl** parameter must contain the address of the source address server.



**Task:** configure downloading of updates for the anti-virus databases from an administrator-defined address. If updates cannot be retrieved from the address, the databases should be downloaded from an address included in the list of update servers included into the package of Kaspersky Anti-Virus.



**Solution:** in order to accomplish the task you should perform the following actions:

Assign the **Yes** value to the **UseUpdateServerUrl** parameter and the **No** value to the **UseUpdateServerUrlOnly** parameter in the **[updater.options]** section. Besides, the **UpdateServerUrl** parameter must contain the address of the source address server.

## 5.1.2. On-demand update of the anti-virus databases

You can start the procedure for updating the anti-virus databases at any time from the command line.



**Task:** update the anti-virus databases saving the results to the */tmp/updatesreport.log* file.



**Solution:** in order to accomplish the task you should enter the following in the command line:

```
# kav4samba-keepup2date -l /tmp/updatesreport.log
```

If you need to update anti-virus databases on several computers it should be more convenient to download the databases from the updates' servers once, save them to a certain directory and then update all computers using that directory as source instead of downloading the files over and over again.



**Task:** set up updating of the anti-virus databases from the **/home/bases** network directory; if the directory is inaccessible or empty, the updating procedure should use the servers of Kaspersky Lab. Results should be output to the **report.txt** file.



**Solution:** in order to accomplish the task you should perform the following actions:

1. Define respective parameter values in the configuration file for the application:

```
[updater.options]
```

```
UpdateServerUrl=/home/bases
```

```
UseUpdateServerUrl=yes
```

```
UseUpdateServerUrlOnly=no
```

2. Enter the following in the command line:

```
# kav4samba-keepup2date -l /tmp/report.txt
```

### 5.1.3. Creation of a network directory for storage and downloading of anti-virus databases

In order to ensure correct updating of the anti-virus databases from a network directory, you should reproduce in that directory the file structure of the sites acting as sources of updates provided by Kaspersky Lab. Let us examine the task closely.



**Task:** create a network directory for subsequent storage of anti-virus databases to be downloaded to local network computers.



**Solution:** in order to accomplish the task you should perform the following actions:

1. Create a local directory.
2. Launch the *keepup2date* program as follows:

```
# kav4samba-keepup2date -u <dir>
```

where `<dir>` stands for a full path to the created directory.

3. Provide network reading access to the directory for LAN computers.



**Task:** configure updating of the anti-virus databases through a proxy server.



**Solution:** in order to accomplish the task you should perform the following actions:

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

or:

1. Assign the **Yes** value to the **UseProxy** parameter in the **[updater.options]** section of the configuration file.
2. Define the **http\_proxy** environment variable in the **http://username:password@ip\_address:port** format. Please note, that the variable will only be used in cases when the **UseProxy** parameter in the **[updater.options]** section is missing or is set to **Yes**.

## 5.2. Real-time anti-virus protection of Samba servers

Real-time anti-virus protection of Samba servers is accomplished by the *kavsamba* component tracking attempts to access files through a Samba server. *Kavsamba* starts as an operating system daemon. After the built-in anti-virus core of the component analyses a requested file, *kavsamba* makes a decision on further work with such file (whether access should be granted/blocked).

Disinfection of infected objects is off by default, i.e. if infected, suspicious or corrupted objects are discovered they will be blocked and relevant information will be included into anti-virus report.



All settings of the *kavsamba* component are grouped in the **[samba.\*]** sections of the application configuration file.

You can additionally activate disinfection of infected objects, their transfer to a separate directory, etc. It requires corresponding modifications to the settings stored in the configuration file. Please see details in section 6.1.3. on p.41.

## 5.2.1. Setup of user's notifications

Since *kavsamba* operates in background, nothing is displayed on the console except for its start output and help information. Additional setup of notifications may be performed through e-mail messages or the **smbclient** standard utility. Let us review those opportunities in detail.

### 5.2.1.1. Monitoring with notifications through smbclient

Installation of a Samba server automatically installs the **smbclient** utility delivering **winpopup** messages to client computers. In Windows operating system such messages (**winpopup**) are displayed on the user's screen if the Messenger service is started.

That opportunity is useful for notification of users (administrators) about attempts to access an infected file through a Samba server.

Let us examine such method of notification using the following example:



**Task:** Display of an on-screen notification for the user if an attempt of accessing an infected file through a Samba server takes place.



**Solution:** in order to accomplish the task you should perform the following actions:

1. Define the action to be performed over infected files. To do so add into the **[samba.notify]** section of the configuration file the following line indicating the action:

```
OnInfected=exec echo "%USER%
%FULLPATH%/FILENAME% is infected by %VIRUSNAME%"
| smbclient -M %USERHOST%
```

2. Restart Kaspersky Anti-Virus.

### 5.2.1.2. Monitoring with e-mail notifications

In case of monitoring with e-mail notifications attempts of accessing an infected or suspicious file are reported in an e-mail message sent to a specified address.



**Task:** Notification of administrator about user's attempt to access an infected or suspicious file via Samba server.



**Solution:** in order to accomplish the set task you should perform the following actions:

1. Define the action to be performed over infected objects. To do so add into the **[samba.notify]** section of the configuration file the following line indicating the action:

```
OnInfected=exec echo "%USER%
%FULLPATH%/%FILENAME% from %USERHOST% is infected
by %VIRUSNAME%" | mail -s 'Virus notification'
spam-virus@localhost.ru
OnWarning=exec echo "%USER% %FULLPATH%/%FILENAME%
from %USERHOST% is probably infected by
%VIRUSNAME%" | mail -s 'Virus notification' spam-
virus@localhost.ru
OnSuspicion=exec echo "%USER%
%FULLPATH%/%FILENAME% from %USERHOST% is probably
infected by %VIRUSNAME%" | mail -s 'Virus
notification' spam-virus@localhost.ru
```



Keep in mind that you will have to perform a cold restart of Kaspersky Anti-Virus (see section 6.4 on p. 48).

## 5.3. Anti-Virus protection of file systems



On-demand anti-virus scanning can only be initiated by the **root** user!

Anti-virus protection of server file systems is performed by the *kavscanner* component scanning server files for presence of viruses and processing infected and/or suspicious objects in accordance with its settings. Objects' processing may be either purely informational (output of information to a report and server

console, administrator notification), or force object modification (disinfection, transfer to a separate directory, removal).



All settings of the *kavscanner* component are grouped in the **[scanner.\*]** section of the application configuration file.



By default *kavscanner* only notifies user/administrator about the infected objects it has discovered. Please see details on additional setup for actions to be performed over files in section 6.2.3 on p. 45.

On-demand scanning of your server file systems may be invoked by the administrator from the command line or scheduled using the standard **cron** utility. You can order scanning of whole file systems or an individual directory. Sectors of block devices can also be scanned.

Further we shall discuss in detail most typical tasks of anti-virus protection for server file systems.



The process of scanning a whole computer for virus presence is quite a resource-consuming task. Please note that during the procedure the server will slow down, therefore it is recommended to perform scanning when the server load is at the lowest level.

### 5.3.1. On-demand scanning of files

One of the goals accomplished by the Kaspersky Anti-Virus is scanning for virus presence and disinfection of files in an individual directory of a server.



**Task:** start of recursive scanning for **/tmp** directory with automatic disinfection of all infected objects. All objects, which cannot be disinfected are to be deleted.

Results of component activity (start date, detailed information about all files except for those containing no viruses) are to be output to a report file *kavscanner-current\_date.log*, which must be saved to the same directory.



**Solution:** in order to accomplish the set task you should enter the following in the command line:

```
#!/kav4samba-kavscanner -rlq
-o kavscanner-`date +%F`.log -i3 -ePASBME -j3 -mCn
/tmp
```

## 5.3.2. Scheduled scanning of a directory (cron)

The **cron** utility for scheduled programs' launch can be used for automatic performance of any tasks by the Kaspersky Anti-Virus for Samba Servers, including scheduled scanning of a specified directory.



**Task:** daily scanning for virus presence must be started at 0 hrs. 00 min for the **/home** directory, the routine must use scanning parameters defined in the `/etc/kav/kavscanner.cron` file



**Solution:** in order to accomplish the task you should perform the following actions:

1. Create `/etc/kav/kavscanner.cron` configuration file and record all required scanning parameters to it.
2. Modify the file, which defines rules for cron (**crontab -e**): add the following line:

```
0 0 * * * /path/to/kav4samba-kavscanner -c
/etc/kav/kavscanner.cron /home
```

## 5.3.3. Additional opportunities: using scripts

Kaspersky Anti-Virus offers an opportunity for additional processing of objects, which have passed anti-virus scanning, using various standard Unix/Linux commands and scripts. Such tools help experienced administrators to define at their discretion actions to be performed over objects with different status and thus extend Kaspersky Anti-Virus functionality.

### 5.3.3.1. E-mail notification of administrator

Kaspersky Anti-Virus allows setting up of standard Unix/Linux tools for system administrator notifications about discovered infected, suspicious or corrupted files.



**Task:** set up notification of administrator about infected files and archives discovered in the server file system during each server scanning performed in accordance with the parameters stored in the application configuration file.



**Solution:** in order to accomplish the task you should perform the following actions:

Define rules for processing of simple objects and container objects in the application configuration file:

```
[scanner.object]
```

```
OnInfected=exec echo %FULLPATH%/FILENAME% is  
infected by %VIRUSNAME% | mail -s kav4samba-  
kavscanner admin@localhost.ru
```

```
[scanner.container]
```

```
OnInfected=exec echo archive %FULLPATH%/FILENAME% is  
infected, viruses list is in the attached file %LIST%  
| mail -s kav4samba-kavscanner -a %LIST%  
admin@localhost.ru
```

---

# CHAPTER 6. ADDITIONAL SETUP

This section describes in detail additional setup of Kaspersky Anti-Virus functionality. Unlike the required settings made during the installation process (please see section 3.3 on p.15), and essential for product functioning, additional setup is performed at the administrator's discretion. Those settings extend product functionality and allow its adjustment for operation within corporate framework of a specific enterprise.

## 6.1. Tuning real-time anti-virus protection

As it has been noted above, real-time anti-virus protection of Samba servers is accomplished by the *kavsamba* component.

Configuration of the component provides for an opportunity to adjust the following parameters:

- Scope of monitoring: the path and objects to be monitored (please see section 6.1.1. on p. 39).
- File scanning and disinfection mode (please see section 6.1.2 on p.40).
- Actions to perform over files (please see section 6.1.3. on p. 41).
- Backup copy mode (please see section 6.1.5 on p.42).
- Creation of reports and notifications (please see section 6.5 on p.49).

### 6.1.1. Scope of monitoring

The monitoring area of the *kavsamba* component includes the *path* and *objects of monitoring*.

The *monitoring path* means all file systems accessible to a user through the Samba server. The path can be restricted only by means of excluding some directories or files in the application configuration file (or its alternative) (section **[samba.options]**, parameters **ExcludeMask** and **ExcludeDirs**).

*Monitoring objects* (types of files to be scanned for virus presence) are also defined only by the parameters in the **[samba.options]** section of the configuration file .



You cannot define or restrict the monitoring area from the command line at the start of the *kavsamba* component. Such an option is implemented only for ant-virus scanning of the server file systems (*kavscanner* component).

## 6.1.2. File scanning and disinfection mode

*Kavsamba* supports the following file access operations: open and close. On opening all non-empty files are scanned; a file being closed is scanned if any modifications have been made to it.

By default disinfection of intercepted infected files is off, it means that a user (and/or administrator) is only notified about discovery of viruses or suspicious objects. Notification is accomplished by messages output to a report file (please see section 6.6 on p.50). Access to such objects is blocked automatically.

Disinfection of infected objects is switched on in the configuration file (section **[samba.options]**, parameter **Cure=yes**). If after file scanning *kavsamba* discovers its infection (i.e. file status is **Infected**), it will act in accordance with the settings in its configuration file (please see section 6.1.3 on p.41).

Resulting from the scanning (and disinfection) procedure a file is assigned one of the following status variants:

- **Clear** – the file is not infected.
- **Infected** – the file is infected.
- **Cured** – the file has been successfully disinfected.
- **CureFailed** – file disinfection has failed.
- **Warning** – file code resembles a known virus.
- **Suspicion** – file infection with an unknown virus is suspected.
- **Protected** – the file cannot be scanned because it is encrypted.
- **Corrupted** – the file is damaged.

Access to a file is either blocked (**Infected**, **CureFailed**, **Warning**, **Suspicion**) or granted (any other status) depending upon its status.



Files with **CureFailed** status are treated according to the actions defined for infected objects!

Please note that in order to speed up scanning of container objects (archives) the *kavsamba* component stops its work assigning the **Infected** status to a whole archive immediately when the first virus is discovered inside. It means also that even if the object is infected with several viruses *kavsamba* will log only one of them.

### 6.1.3. File operations

Performance of some actions can be defined for files with **Infected**, **Suspicious**, **Warning**, **Cured**, **Protected**, **Corrupted** or **Error** status, here belong such actions as:

- *Transfer to a certain directory* – transfer of files with a specified status to a certain directory, *regular* and *recursive transfer* is possible.
- *File removal* from file system.
- *Running a certain command* – files processing using standard Linux commands, scripts, etc.

Please note that the *kavsamba* component does not differentiate actions to be performed over files and container objects. Therefore a report may contain several names of viruses discovered in an object.

You can set up the rules for objects processing as follows:

- Define the rules in the application configuration file, if they are planned as default actions (**[samba.actions]** section).
- Define the rules for processing in an alternative configuration file and use it during component start.

Please note that the **/homes** shared directory is virtual. It points to the home directories of all users. Individual settings of anti-virus protection cannot be specified for such directories.



Therefore, the product uses the settings in the **[samba.shares]** section to define the protection parameters for user home directories. If anti-virus scanning is disabled in the **[samba.shares]** section, user home directories will be unprotected.

### 6.1.4. Quarantine for infected objects

The existing opportunity for transfer of infected files to a separate directory is used for quarantine of infected objects (**[samba.actions]** section, **MovePath** parameter). Transfer is performed in cases, when file disinfection has failed (for instance, when out of three viruses discovered in a file only two have been removed successfully).



Administrator can set up transfer of objects to different directories depending upon file status.

If it is planned to preserve and keep such directory, we recommend that you exclude it from the scanning area using the **ExcludeDirs** parameter (**[samba.options]** section) in the configuration file.



**Task:** scan for virus presence all files requested through a Samba server and cure them, if they are infected. If the disinfection procedure fails, infected objects must be transferred with their full paths to the **/tmp/infected** directory.



**Solution:** in order to accomplish the task you should perform the following actions:

1. Turn on the cure mode for infected objects in the application configuration file (**Cure=yes** in the **[samba.options]** section).
2. Define rules for isolation of infected objects. In order to do so add the following settings in the **[samba.actions]** section of the configuration file:  

```
OnInfected=MovePath /tmp/infected
```
3. Perform a cold restart of Kaspersky Anti-Virus (see section 6.4 on p. 48).

## 6.1.5. Backup copying of objects

If scanned files turn out to be infected while removal from file system is defined as an action to be performed over infected objects, loss of some important data is possible. In order to avoid that Kaspersky Anti-Virus offers an opportunity to copy files to backup storage.

Prior to file disinfection or removal its copy is saved in backup storage (**[samba.path]** section, **BackupPath** parameter). It allows preserving a backup copy (and restore the file if necessary) in case the file itself is damaged during disinfection. Such files are saved to backup with full paths. Subsequent recording of the same file to backup storage automatically replaces earlier file copy with a newer one.

Please note that file backup is off by default and therefore the path to the directory for storage of backup copies is not specified. You'll have to define the path personally to enable that feature.



If an object is removed from file system, its backup copy will be preserved until it is deleted by the administrator.

## 6.2. Setup of anti-virus protection for server file systems

Anti-virus protection of server file systems is performed by the *kavscanner* component. Default parameters of *kavscanner* operation are stored in the application configuration file (**[scanner]** section); they are set for the most thorough scanning of file systems accessible from a workstation, where the product is installed. All available files are scanned for virus presence, including:

- Packed files.
- Archives.
- Self-extracting archives.
- E-mail databases.
- Plain e-mail messages.

The whole collection of parameters pertaining to anti-virus protection of server file systems can be subdivided into groups, which define:

- Scanning area (please see section 6.2.1 on p. 43) (that parameter is similar to the monitoring area for real-time protection).
- File scanning and cure mode (please see section 6.2.2 on p. 44).
- Actions to be performed over files (please see section 6.2.3 on p. 45).

Let us review in detail setup of each parameters' group.

### 6.2.1. Scanning area

Scanning area may be conventionally subdivided into two parts:

- *Scanning path* is a list of directories and files for anti-virus scanning.
- *Scanning objects* are file types, which will be scanned for virus presence (archives, e-mail messages, etc.).

By default all objects of accessible file systems are scanned beginning with the current directory.



Scanning of all server file systems requires entering the root directory first or specifying the scanning area in the command line.

You can redefine scanning path using the following methods:

- Enumeration of directories and files with their absolute or relative (to the current directory) paths separated by spaces in the command line at component start.

- Definition of scanning paths in a text file with a subsequent command to use the file with the **-@ <file\_name>** key. Each object in such file is specified in a new line with its absolute path.



If the command line contains both a scanning path and a text file with a list of objects for scanning, first the objects listed in the command line will be scanned, and then the objects from the file will be processed.

- Restriction of default paths (everything beginning with the current directory) or of the paths listed in the command line by entering masks for files and directories to be excluded from the scanning area (**[scanner.options]** section, parameters **ExcludeMask** and **ExcludeDirs**) in the configuration file.
- Disabling *recursive scanning of directories* (**[scanner.options]** section, **Recursion** parameter or **-r** key).
- Creation of an alternative configuration file with subsequent command to use it by the **-c <file\_name>** key at component start.

Default scanning objects are also defined in the application configuration file (**[scanner.options]** section) and can be redefined:

- by command line keys at component start
- when an alternative configuration file is used.

## 6.2.2. File scanning and disinfection mode

File scanning and disinfection mode for the *kavscanner* component is totally similar to that of the *kavsamba* component except for the fact that *kavscanner* performs various actions including operations with files having **Corrupted** status (please see details on the actions in section 6.1.3 on p.41).

Please remember that disinfection is off by default and files are just scanned for virus presence with notifications about infected, suspicious or corrupted objects output to the console and scanning log.

Each file receives a certain status (**Clear**, **Infected**, **Warning**, etc.) after its scanning for virus presence, whereupon the application handles the file in accordance with the settings in its configuration file.

Please remember that if disinfection is on (**[scanner.options]** section, parameter **Cure=yes**) disinfection of files with the **Infected** status will be attempted.

## 6.2.3. File operations

Depending upon file status different operations may be applicable to it. By default discovery of files with a certain status results only in notifications output to console and added to logs.

However, you can set up certain actions to be performed over files with **Infected**, **Suspicious**, **Warning**, **Cured**, **Protected**, **Corrupted** and **Error** status, similar to the *kavsamba* component:

- *Transfer to a certain directory* – transfer of files with a specified status to a certain directory, *regular* and *recursive transfer* is possible.
- *File removal* from file system.
- *Running a certain command* – files processing using standard Unix/Linux commands, scripts, etc.

While scanning server file systems, Kaspersky Anti-Virus distinguishes between a *simple* object (file) and *container* object (consisting of several objects – archive). Actions to be performed over such objects are also different; they are allocated separate sections in the configuration file. Section **[scanner.object]** is devoted to simple objects, section **[scanner.container]** – to container objects.

Various operations are possible for self-extracting archives: if an archive itself is infected, it is viewed as a simple object, but if archived objects inside it contain viruses – it is treated as a compound one. Respective operations with the archive are determined by parameters from different sections of the configuration file.

You can select an action to be performed over specific files using the following methods:

- Define the actions in the application configuration file, if they are planned for default use (**[scanner.object]** and **[scanner.container]** sections).
- Indicate the actions in an alternative configuration file and use it at the component start.
- Define the actions for the current session using the command line keys at the start of the *kavscanner* component.

## 6.2.4. Backup mode settings

The possibilities for tuning the settings of backup used in anti-virus protection of file systems are identical to those described in section 6.1.5 on p. 42 for real-time anti-virus protection. Therefore we shall not discuss those settings here in detail.



**Task:** scanning for virus presence of all directories and files listed in the */tmp/download.lst* file and their disinfection. In case of disinfection fail-

ure discovered infected objects must be transferred with their full paths to the **/tmp/infected** directory, suspicious objects – to the **/tmp/suspicious** directory, warnings – to the **/tmp/warning** directory.



**Solution:** in order to accomplish the task you should perform the following actions:

1. Create `scan_sample.conf` alternative configuration file.
2. Make sure that disinfection of infected objects is on (**Cure=yes** in the **[scanner.options]** section).
3. Set up the rules for processing of infected objects. To do so add into the **[scanner.object]** and **[scanner.container]** sections of the `scan_sample.conf` configuration file the following settings:

```
OnInfected=MovePath /tmp/infected
OnSuspicion=MovePath /tmp/suspicious
OnWarning=MovePath /tmp/warning
```

4. Enter the following in the command line:

```
# kav4samba-kavscanner -@/tmp/downloads.lst -c
sample_scan.conf
```

## 6.3. Optimizing Kaspersky Anti-Virus for Samba Servers

Kaspersky Anti-Virus for Samba Servers offers several efficient methods for optimization of its operations in order to decrease server load. Let us examine them closely.



*Use of iChecker database and a cache of scanned files.*

The software uses some technologies that allow to do without scanning of a file anew each time a user tries to access it; instead it just compares the file to previously gathered data on it, when possible. The algorithm for object (file) scanning for virus presence is as follows:

During initial scanning of any file the information about it (name, checksum) is appended to one of the following databases:

- iChecker database includes information about scanned uninfected files of identified formats. Such a database contains information about scanned objects provided both by the *kavsamba* and the *kavscanner* components.

- Scanned files' cache is a database containing information on all the checked files. The database contains information only on components scanned by the *kavsamba* component; it exists in RAM and is not saved after *kavsamba* completes its work.

If during the scanning procedure information about a file is not added to the iChecker database (the file is not clear or has an unsupported format), it is sent to the cache.

Each subsequent user's accesses to a file force its search first in the iChecker database, then (if the object hasn't been found in the first database) – in the cache. File name serves as search criterion. If such file is found in any of the bases, its information will be compared with the data stored in the base. The file is considered to be unchanged and is not scanned for virus presence provided its current condition is completely identical to its description in a relevant database.

If no data can be found for the requested file in the iChecker database or in the cache, complete file scanning for viruses is performed.



If you have changed the set of anti-virus databases being used while working with the application, the information from the iChecker database should be removed manually (complete path to the database is defined by the **IcheckerDbFile** parameter in the **[path]** section of the application configuration file).

The requirement is determined by the fact that the database may contain records of infected objects that have not been detected using the standard anti-virus databases but have been revealed using the extended database. The application does not rescan files that are found in the iChecker database and so computer infection may be possible.



*Background scanning.*

Since data search in the above-mentioned bases is very fast, it decreases the load on server and provides an opportunity for further improvement of its efficient use by means of *background file scanning*.

While running Kaspersky Anti-Virus determines its load and, if the level does not exceed its defined limit, performs background scanning of files from shared directories located on a Samba server as well as files modified in the process of work.

The load is defined by the maximum number of files allowed for simultaneous scanning (**CheckFilesLimit** parameters in the **[samba.options]** section). The number of files allowed for simultaneous background scanning can also be defined (**BgCheckFilesLimit** parameter in the **[samba.options]** section) as well

as the time interval after which the Anti-Virus requests a new file for scanning (**BgSheduleTime** parameter in the **[samba.options]** section).

If the number of files to be scanned exceeds the allowed maximum newly arriving files are added into a queue for scanning later, when the load falls below an acceptable level.

In that case users who requested scanning of files will have to expect a response slightly longer than anticipated. After scanning completion a file is removed from the queue without additional notifications.



If the frequency of requests is not specified (**BgSheduleTime=0**), background scanning will not be performed.

Thus the maximum allowed server load can be established and maintained.

## 6.4. Restarting Kaspersky Anti-Virus for Samba Servers



Access to the **[samba.shares]** protected by the Anti-Virus will be blocked during any restart of Kaspersky Anti-Virus.

Several variants are available for restarting the Anti-Virus:

- A "warm" restart is recommended after updating of the anti-virus databases.

In that case just the anti-virus databases are reloaded, and all connections are preserved. The *kavsamba* component is not restarted, so its file cache, etc. remains intact.

A "warm" reboot is accomplished by entering the following in the command line:

For Linux distributions:

```
/etc/init.d/kav4samba reload_avbase
```

For FreeBSD distributions:

```
/usr/local/etc/rc.d/kav4samba.sh reload_avbase
```

In that case the *kavsamba* process receives a **SIGUSR1** signal.

- A complete "cold" restart must be performed if modifications are made to the configuration file or settings or when a new license key is installed.

In that case the program reads again its configuration file and databases terminating all user connections since the application actually first stops its operation and then restarts.

Restarting is accomplished by entering the following in the command line:

For Linux distributions:

```
/etc/init.d/kav4samba reload
```

For FreeBSD distributions:

```
/usr/local/etc/rc.d/kav4samba.sh reload
```

In that case the *kavsamba* process receives a **SIGHUP** signal.

- Forced termination of Kaspersky Anti-Virus operation is accomplished by entering the following in the command line:

For Linux distributions:

```
/etc/init.d/kav4samba stop
```

For FreeBSD distributions:

```
/usr/local/etc/rc.d/kav4samba.sh stop
```

The command will send to the *kavsamba* process a **SIGTERM** signal terminating *kavsamba* operation and closing all its branched copies, and then the Anti-Virus terminates correctly.



We strongly recommend that you do not terminate the activity of the *kavsamba* process with the **kill -9** command. That command will terminate the process, however, several temporary and working files will remain in the system; they can be removed only manually. Some applications identify the process as an active one if those files are present in a system.

## 6.5. Localization of displayed date and time format

While working Kaspersky Anti-Virus compiles reports for each of its components as well as various notifications for users and administrators. Such information is always supplemented with the date and time of its output.

By default Kaspersky Anti-Virus uses the date and time formats corresponding to the strftime standard:

**%H:%M:%S** – format of time output (hh.mm.ss).

**%d/%m/%y** – format of date output (dd.mm.yy).

The administrator may change the date and time format. Localization of formats is performed in the **[locale]** section of the application configuration file. For example, you can define the following formats:

**%I:%M:%S %P** – for time output in twelve-hour format (**TimeFormat** parameter).

**%y/%m/%d** and **%m/%d/%y** – for date output (**DateFormat** parameter) (yy.mm.dd and mm.dd.yy respectively).

## 6.6. Reporting parameters in Kaspersky Anti-Virus

Results of operations performed by all components of the Kaspersky Anti-Virus are summarized in a report output to a log file.



Results of anti-virus processing of server file systems are also output to console. By default the information output to a report and on-screen is identical. If you wish to see on the console information different from that in a report log, you'll need to perform some additional setup.

You can adjust the volume of output information by modifying the *level of report details*.

**The level of details** is a number, which determines how specific the information about components operation in the report should be. Each higher level includes the information from the previous one and some additional data.

The table below contains a summarized description of all levels possible for report details.

Levels	Level description	Meaning
0	Critical errors	Information about critical errors only (i.e. errors, which cause program termination because some actions cannot be performed). For example, component infection or an error while checking or loading databases and license keys.
1	Errors	Information about other errors including those, which do not force termination of components' activity, for example, information about an error encountered during file scanning.
2	Warning	Information about errors, which can result in termination of application activity, for example,

Levels	Level description	Meaning
		insufficient available disk space.
3	Info, Notice	Important informational messages; for example: information telling whether a component is started, path to the configuration file, scanning area, information about anti-virus databases, license keys, and resulting statistics.
4	Activity	Messages about scanning of files in accordance with the level of details defined for the scanning report.
10	Debug	All debugging messages, for example, the content of the configuration file.

Information about fatal errors in component operation is output always despite the defined level of details. Level 4 set by default is optimal for component operation.

---

# CHAPTER 7. LICENSE KEYS MANAGEMENT

The right to use Kaspersky Anti-Virus for Samba servers is restricted in terms of duration (as a rule, the period of license validity lasts for one year from the date of product purchase). When the license to use Kaspersky Anti-Virus expires, the application will continue its operation, but it will be unable to further update its anti-virus databases. The Anti-Virus will continue to cure infected objects, but it will use its old databases.

A license key entitles you to use the product and contains all the required data pertaining to the license, which you have purchased, such as license type, expiration date, information about distributors, etc.

Besides the right to use the product during the period of license validity you are entitled to the following:

- round-the-clock technical support
- anti-virus database updates issued *every hour*
- product updates (patches)
- new product versions (upgrades)
- timely notifications about new viruses.

When the license expires, the above services are discontinued automatically. Kaspersky Anti-Virus will continue scanning of server file systems but it will use only anti-virus databases, which were current as of the date of license expiry. The feature of anti-virus database updating will become unavailable. An attempt to update the anti-virus databases manually will render the application unusable.

Therefore it is essential to review regularly the information in the license key and control the date of its expiry.

## 7.1.1. Viewing license key information

You can review information about installed license keys in the logs produced by the *kavscanner* and *kavsamba* components since both of them load the information from the license keys during start.

Moreover, Kaspersky Anti-Virus contains a special *licensemanager* component, which allows not only reviewing more detailed information about the keys but also retrieving some analytical data.

All the information may be output to a server console or viewed remotely from any computer on your network through Webmin interface.



*In order to review the information about all installed license keys*

enter the following in the command line:

```
#./kav4samba-licensemanager -s
```

The following information will be output to server console:

```
Kaspersky license manager Version 5.5  
Copyright (C) Kaspersky Lab. 1997-2006.  
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
```



*In order to review the information about an installed license key*

enter, for example, the following in the command line:

```
#./kav4samba-licensemanager -k 00053E3D.key
```

The following information will be output to server console:

```
Kaspersky license manager Version 5.5  
Copyright (C) Kaspersky Lab. 1997-2006  
Portions Copyright (C) Lan Crypto  
Serial 0038-000419-0003D3EA, "Kaspersky Anti-Virus  
for Linux", expires 04-07-2003 in 28 days
```

## 7.1.2. License extension

Extension of your license to use Kaspersky Anti-Virus entitles you to restoration of complete product functionality including updates to the anti-virus databases. Besides, you will be granted further access to services.

The period of license validity depends on the type of licensing that you have selected during product purchase.



*In order to extend your license to use Kaspersky Anti-Virus for Samba Servers you'll need to:*

contact the company, where you have purchased the product and acquire an extension for your license to use Kaspersky Anti-Virus

or.

extend the license duration directly through Kaspersky Lab having sent a message to the Sales Department ([sales@kaspersky.com](mailto:sales@kaspersky.com)) or fill a respective form in the **eStore → Renew or Upgrade Your License** section of our website ([www.kaspersky.com](http://www.kaspersky.com)). After payment you will receive a license key sent to the e-mail address, indicated in your order form.

The purchased license key has to be installed using the *licensemanager* utility (**LicensePath** parameter of the program configuration file).



*In order to install a new key you'll need to:*

enter, for example, the following in the command line:

```
#!/kav4samba-licensemanager -a 00053E3D.key
```

The following information will be output to server console:

```
Kaspersky license manager. Version  
5.5.0.0/RELEASE  
Copyright (C) Kaspersky Lab. 1998-2006.  
Key file 00053E3D.key is successfully registered
```

We recommend updating your anti-virus databases after the procedure.

If you wish to install a new license key before the current one expires you can install it as an additional key. An additional key begins working when the subscription period of the active key expires. The period of a reserved key validity is calculated beginning from the moment of its activation.

Installation of an additional key is accomplished in accordance with the standard method similar to the installation of the main key. After that a license key information request will output to server console information about both the active and the reserved keys.

### 7.1.3. License key removal



*In order to remove all installed license keys,*

enter the following in the command line:

```
#!/kav4samba-licensemanager -da
```

The following information will be output to server console:

```
Kaspersky license manager. Version  
5.5.0.0/RELEASE  
Copyright (C) Kaspersky Lab. 1998-2006.  
Active key was successfully removed
```



*In order to remove your additional key,*

enter, for example, the following in the command line:

```
#./kav4samba-licensemanager -dr
```


The following information will be output to server console:

```
Kaspersky license manager. Version  
5.5.0.0/RELEASE  
Copyright (C) Kaspersky Lab. 1998-2006.  
Additional key was successfully removed
```

---

# CHAPTER 8. CHECKING CORRECT OPERATION OF THE ANTI-VIRUS

When the installation and setup of Kaspersky Anti-Virus are complete we recommend checking the settings and correct operation of the program using a test “virus” and modifications thereof.

The test “virus” has been specifically developed by  (The European Institute for Computer Antivirus Research) for checking the operation of anti-virus products.

The test “virus” IS NOT A VIRUS and it contains no code, which might harm your computer; at that most products of anti-virus vendors identify it as a virus.



Never use real viruses to test the operational integrity of anti-virus products!

The test “virus” can be downloaded from the official site of **EICAR** at: [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm). If you have no Internet access, you can create a test “virus” manually. To do so enter the line below in any text editor and save it to a file under the name **eicar.com**:

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

The file, which you have downloaded from **EICAR** site or created in a text editor as described above, contains the body of a standard test “virus”. The Anti-Virus detects it, assigns the **Infected** incurable type to it and performs an action defined by the administrator for objects belonging to such type.

In order to test the Anti-Virus reaction to the detection of objects belonging to other types you may modify the contents of the standard test “virus” by adding one of the prefixes below (please see Table 1).



You can check correct operation of Kaspersky Anti-Virus using modifications of EICAR “virus” if your anti-virus databases are dated Oct. 24, 2003 or later only (cumulative update – October 2003).

Table 1. Test “virus” modifications

Prefix	Object type
No prefix, standard test	<b>Infected</b> . The object is not cured.

Prefix	Object type
"virus"	
CORR–	<b>Corrupted.</b> The object is damaged.
SUSP–	<b>Suspicious</b> (unknown virus code).
WARN–	<b>Warning</b> (modified code of a known virus).
ERRO–	<b>Error.</b> The object caused an error during scanning.
CURE–	<b>Cured.</b> The object is cured; at that the text in the "virus" body is changed to CURED.
DELE–	The object is deleted automatically.

The first column of the table contains the prefixes, which should be added to the line beginning of the standard test "virus" (e.g. CORR–X50!P%@AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H\*). The second column contains the types of objects identified by the anti-virus application as a result of their addition. Actions performed over each object are defined by Anti-Virus settings selected by the administrator.

---

# CHAPTER 9. FREQUENTLY ASKED QUESTIONS

This chapter is devoted to the most frequently asked users' questions pertaining to installation, setup and operation of the Kaspersky Anti-Virus; here we shall try to answer them in detail.



**Question:** *Is it possible to use Kaspersky Anti-Virus with anti-virus products of other vendors?*

We recommend uninstalling anti-virus products of other vendors prior to installation of Kaspersky Anti-Virus to avoid software conflicts.



**Question:** *Kaspersky Anti-Virus does not rescan a file. Why?*

Indeed, Kaspersky Anti-Virus does not rescan files which have not changed since their last scan.

That has become possible due to new iChecker™ technology. The application implements the technology using a database of object checksums.



**Question:** *why does Kaspersky Anti-Virus cause a certain decrease of server performance noticeably loading the CPU?*

Virus detection is a purely computational (mathematical) problem connected with structural analysis, checksum calculation and mathematical data conversions. Therefore processor time is the main resource consumed by the anti-virus software. At that each new virus added into the anti-virus database increases the overall scanning time. That is a forced compensation for security and safety of your data.

Unlike other anti-virus products, which speed up scanning by means of excluding from their databases less easily detectable or less frequent (in the geographic location of the anti-virus vendor) viruses as well as file formats that require complicated analysis (e.g. PDF), Kaspersky Lab believes that the purpose of its anti-virus is establishment of real anti-virus security for its users instead of imaginary, since you cannot be semi-protected. Besides, "partial protection" is even worse than no protection at all (because in the latter case users take personal precautions).

Kaspersky Anti-Virus makes its users feel maximum protection. Of course, Kaspersky Anti-Virus software package allows experienced users to accelerate anti-virus scanning to the detriment of overall security by disabling scanning of various file types, but we do not recommend doing so to users, who want the best protection.

For the purpose of maximum user protection Kaspersky Anti-Virus recognizes more than 40 types of archives and installation packages demonstrating its capability to detect viruses in more than 350 different file formats. It is essential for anti-virus security because harmful executable code may be hidden inside files in any recognized format. However, one cannot but admit that despite the daily growth in the number of viruses detected by Kaspersky Anti-Virus (approximately 30 new viruses daily) as well as the ever increasing number of recognized file formats, each subsequent version of our product functions faster than the previous one. That is achieved through the use of new unique technologies, such as iChecker, developed at Kaspersky Lab. In that case a file is checked for viruses only once - during the initial scanning. During all subsequent scans the file is not checked for virus presence provided that it remains unchanged. Thus the anti-virus performance increases drastically after the first file scanning.



Question: *why is a license key required? Can my Anti-Virus work without it?*

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

If you haven't yet made a decision whether you wish to buy Kaspersky Anti-Virus, we can provide to you a trial key, which will work for two weeks or one month. The key will be blocked when that period expires.



Question: *what happens when a license to use the product expires?*

When your license to use Kaspersky Anti-Virus expires the software will continue operation, however, you will have no access to anti-virus database updates. The anti-virus software will cure infected objects, but it will use its old databases only.

Downloading of anti-virus databases from the Kaspersky Lab site using the *keepup2date* component will be impossible. If you download the databases by means other than the *keepup2date* component Kaspersky Anti-Virus will not work.

Therefore we cannot guarantee your protection against new virus infections.



**Question:** *the license key to Kaspersky Anti-Virus is recorded on a floppy disk. What should I do if my computer has no floppy disk drive?*

This problem has several solutions.

You can write an e-mail with a description of your problem to the Sales Department of Kaspersky Lab ([sales@kaspersky.com](mailto:sales@kaspersky.com)). Please mention in the message the date and place where you purchased Kaspersky Anti-Virus and its complete registration number. Managers of the Sales department will send your key file to your e-mail address.

You can read the floppy disk contents on another computer equipped with a floppy disk drive and then record it to another media, which your computer can read. Select that medium during installation of Kaspersky Anti-Virus as the source of your license key.

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



**Question:** *my Anti-Virus does not function.*

*What should I do?*

First of all check whether a solution to your problem is described in this document and, in particular, in this section or at our site (**Services → Knowledge base → Kaspersky Anti-Virus 5.5 for Samba Servers**).

We also recommend contacting the company, from which you have purchased your Kaspersky Anti-Virus or writing a letter to the Technical Support Service (<http://www.kaspersky.com/helpdesk.html>).



**Question:** *can an intruder deliberately replace the anti-virus databases?*

An intruder may be able to download the anti-virus databases from the Kaspersky Lab site and copy them to the directory, where they should be stored, but Kaspersky Anti-Virus will not use such databases during its work!

All anti-virus databases have unique signatures verified by Kaspersky Anti-Virus while accessing the bases. If a signature does not correspond to the one assigned at the Kaspersky Lab and the databases are dated

after the date of license expiry, Kaspersky Anti-Virus will not use such databases.



**Question:** *are the X architecture processors supported (PowerPC, SPARC, Alpha, PA-RISC etc.)?*

The current version of the product does not support processors of those types.



**Question:** *will the Kaspersky Anti-Virus for Unix work with my Linux distribution?*

Kaspersky Anti-Virus 5.5 has been tested with RedHat, Debian, SuSE and Mandriva Linux distributions and Kaspersky Anti-Virus packages have been compiled specifically for the listed distributions.

Users of distributions that are not included into the list supported by Kaspersky Lab may experience incorrect product operation. That is first of all determined by the operating system specifics. For example, your OS distribution may use a different version of a certain library or its system initialization scripts may have a non-standard location. In such case the Technical Support of the Kaspersky Lab will be unable to help you.



**Question:** *how do I decompress a .tgz or .tar.gz archive?*

Archives belonging to .tgz or .tar.gz types are decompressed using the following command:

```
tar zxvf <archive_name>
```



**Question:** *can I control Kaspersky Anti-Virus using the Network Control Centre for Windows?*

Network Control Centre for Windows cannot be used for operations with Kaspersky Anti-Virus for Unix. In this version of the product we have provided for an opportunity to control the software remotely via a special Webmin module.



**Question:** *how do I save software console output to a file?*

One of possible solutions is described below:

enter the following in the command line:

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

where:

`some_app` means the software, the standard output and error messages of which you would like to have saved to a file;

`text_file` – full path to the file, where the information will be recorded.

For example:

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

In that case standard output messages as well as error messages from the *keepup2date* component will be output to the *updater.log* file in the current directory.

---

# APPENDIX A. ADDITIONAL INFORMATION ABOUT THE APPLICATION

This appendix contains a description of the folder tree of the Kaspersky Anti-Virus after installation, its configuration file and command line options of applications components and their return codes. A script file for disinfection of archives is provided as an example.

## A.1. Kaspersky Anti-Virus configuration file

Kaspersky Anti-Virus package includes the *kav4sambaservers.conf* configuration file containing the settings for the application's operation. Here we shall discuss in detail each section of that file. Default values of configuration file settings will be mentioned where applicable.

The **[path]** section contains essential parameters that define the paths to critical application files:

**BasesPath** – full path to the anti-virus databases.

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

**IcheckerDbFile** – full path to the folder containing the database of files scanned using the iChecker technology.

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

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



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

The **[samba.options]** section contains the settings of real-time anti-virus protection:

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

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

**Packed=yes** – scanning mode for packed files. In order to disable the mode, set the parameter to **no**.

**Archives=yes** – scanning mode for archives. In order to disable the mode, set the parameter to **no**.

**SelfExtArchives=yes** – scanning mode for self-extracting archives. In order to disable the mode, set the parameter to **no**. If the archive scan mode is enabled (**Archives=yes**), then self-extracting archives will be scanned even if the **SelfExtArchives** parameter is set to **no**.

**MailBases=yes** – mail database scan mode. In order to disable the mode, set the parameter to **no**.

**MailPlain=yes** – scanning mode for plain text mail messages. In order to disable the mode, set the parameter to **no**.

**Heuristic=yes** – mode for using heuristic code analyzer during the scan. In order to disable the mode, set the parameter to **no**.

**Cure=no** – cure mode for infected objects. In order to enable the mode, set the parameter to **yes**.

**Ichecker=yes** – instruction to use the iChecker technology for anti-virus scanning. In order to disable the mode, set the parameter to **no**.

**FileCacheSize** – the number of records about clean objects in file cache.

**BgCheckFilesLimit** – maximum number of objects that can be scanned simultaneously in the background mode. Background scanning will not be performed if the parameter is set to **0**.

**BgSheduleTime** – time interval after which the application starts background anti-virus scanning of a new file from shared directories (seconds).

**HashType=md5|crc32** – hash type used. Default type: **md5**.

**UseAVbasesSet=standard|extended** – the set of anti-virus databases that the application uses. The **extended** set contains, in addition to records of the **standard** set, signatures of riskware, such as adware, remote administration programs, etc.

The **[samba.path]** section contains parameters that define the paths to essential files of the kavsamba components:

**BackupPath=path** – full path to the folder containing backup copies of the objects scanned.

**SambaConfigFile=path** – full path to the configuration file of the Samba server.

**PidFile=path** – full path to the PID file of the kavsamba component.

The **[samba.shares]** section contains parameters that determine the settings of file

scanning in public folders:

**CheckOnOpen** – anti-virus file scan upon a request to open it.

**CheckOnClose** – anti-virus file scan at saving.

Sections of the **[samba.shares:SHARENAME]** type *can be created* in the configuration file; they must contain the parameters that define the settings of anti-virus protection for an individual shared directory (e.g., for the **SHARENAME** directory):

**CheckOnOpen** – anti-virus file scan upon a request to open it.

**CheckOnClose** – anti-virus file scan at saving.



If you have specified individual protection parameters for a shared directory, then access to it will be blocked while Kaspersky Anti-Virus is not running.

The **[samba.actions]** section contains parameters that define the actions performed over specific object types:

**OnInfected=action** – actions to be performed upon detection of an infected file. If the disinfection mode for infected files is turned on, then the specified action will be performed over objects that could not be disinfected.

**OnSuspicion=action** – actions to be performed in case when the application detects a suspicious file resembling a virus that is yet unknown to Kaspersky Lab.

**OnWarning=action** – actions to be performed in case when the application detects a file resembling a known virus.

**OnCured=action** – actions in case of detection and successful disinfection of an infected object.

**OnProtected=action** – actions upon detection of a password-protected encrypted object. Such objects cannot be scanned.

**OnCorrupted=action** – actions upon detection of a damaged file.

**OnError=action** – actions to be performed if a system error occurs while scanning an object.

Syntax of the **action** parameter consists of two parts: an action and an additional option delimited by a space. The value of the additional parameter is specified in quotes. E.g.: **OnInfected=move /tmp/infected**

An action can take one of the following values:

- *move* <directory> – move a file to the <directory>.
- *movePath* <directory> – move a file to the <directory> recursively (using an absolute path).
- *remove* – delete file.

- o *exec <parameter>* – apply to the object an action defined by the <parameter> value.

The following macros can be used as an additional action parameter:

- o %VIRUSNAME% – name of the detected virus.
- o %FULLPATH% – full directory path.
- o %FILENAME% – file name without path.

The **[samba.notify]** section contains parameters that determine delivery of notifications upon detection of specific object types:

**OnInfected=action** – notification upon detection of an infected file.

**OnSuspicion=action** – notification upon detection of a suspicious file resembling a virus that is yet unknown to Kaspersky Lab.

**OnWarning=action** – notification upon detection of a file resembling a known virus.

**OnCured=action** – notification in case of detection and successful disinfection of an infected object.

**OnProtected=action** – notification upon detection of a password-protected object. Such objects cannot be scanned.

**OnCorrupted=action** – notification upon detection of a damaged file.

**OnError=action** – notification upon a system error that may occur while scanning.

An action can take one of the following values:

- o *move <directory>* – move a file to the <directory>.
- o *movePath <directory>* – move a file to the <directory> recursively (using an absolute path).
- o *remove* – delete file.
- o *exec <parameter>* – apply to the object an action defined by the <parameter> value.

The following macros can be used as an additional action parameter:

- o %USER% – name of the user requesting the file.
- o %USERIP% – IP of the user requesting the file.
- o %USERHOST% – host of the user requesting the file.
- o %VIRUSNAME% – name of the detected virus.
- o %FULLPATH% – full directory path.
- o %FILENAME% – filename without path.

The **[samba.report]** section contains report generation parameters for the kavsamba component:

**ReportFileName** – name of the report file where the component logs the results of its activity.

**ReportMaxSize** – report file size (bytes).

**ReportLevel** – level of details in the report.

**Append=yes** – mode for appending new messages to the report file. In order to disable the mode, set the parameter to **no**.

**ShowOK=yes** – mode for logging messages about clean files into the report. In order to disable the mode, set the parameter to **no**.

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

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

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

**Packed=yes** – scanning mode for packed files. In order to disable the mode, set the parameter to **no**.

**Archives=yes** – scanning mode for archives. In order to disable the mode, set the parameter to **no**.

**SelfExtArchives=yes** – scanning mode for self-extracting archives. In order to disable the mode, set the parameter to **no**. If the archive scan mode is enabled (**Archives=yes**), then self-extracting archives will be scanned even if the **SelfExtArchives** parameter is set to **no**.

**MailBases=yes** – mail database scan mode. In order to disable the mode, set the parameter to **no**.

**MailPlain=yes** – scanning mode for plain text mail messages. In order to disable the mode, set the parameter to **no**.

**Heuristic=yes** – mode for using heuristic code analyzer during the scan. In order to disable the mode, set the parameter to **no**.

**Recursion=yes** – mode for recursive scanning of folders during the anti-virus scan. In order to disable the mode, set the parameter to **no**.

**Ichecker=yes** – instruction to use the iChecker technology for anti-virus scanning. In order to disable the mode, set the parameter to **no**.

**Cure=no** – cure mode for infected objects. In order to enable the mode, set the parameter to **yes**.

**UseAVbasesSet=standard|extended** – the set of anti-virus databases that the application uses. The **extended** set contains, in addition to records of the **standard** set, signatures of riskware, such as adware, remote administration programs, etc.

**FollowSymlinks** – the mode used for work with symbolic links. When set to **yes**, the option forces opening of all symlinks. If it is set to **no**, symbolic links to directories will be left unopened.

**MaxLoadAvg** – numeric parameter reflecting the server load. If the load exceeds the specified value, the anti-virus scanning stops for a while. It

will resume as soon as the server load returns to the level defined by the parameter.

The **[scanner.path]** section contains parameters that define the paths to essential files of the kavscanner component:

**BackupPath=path** – full path to the folder containing backup copies of the objects scanned.

The **[scanner.object]** section contains parameters that define the actions performed over specific object types during anti-virus protection of file servers:

**OnInfected=action** – actions to be performed upon detection of an infected file. If the disinfection mode for infected files is turned on, then the specified action will be performed over objects that could not be disinfected.

**OnSuspicion=action** – actions to be performed in case when the application detects a suspicious file resembling a virus that is yet unknown to Kaspersky Lab.

**OnWarning=action** – actions to be performed in case when the application detects a file resembling a known virus.

**OnCorrupted=action** – actions upon detection of a damaged file.

**OnCured=action** – actions in case of detection and successful disinfection of an infected object.

**OnProtected=action** – actions upon detection of a password-protected encrypted object. Such objects cannot be scanned.

**OnError=action** – actions to be performed if a system error occurs while scanning an object.

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>* – apply to the object the action defined by the *<parameter>* value.

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

- %LIST% – filename or the list of infected, suspicious and corrupted files found in a container. The file format is as follows: **<virus name>\t<filename>**.
- %FULLPATH% – full path to the container.
- %FILENAME% – filename without path.
- %CONTAINERTYPE% – container type as a line.

The **[scanner.container]** section contains parameters that define the actions applied to archives during anti-virus protection of server file systems:

**OnCorrupted=action** – actions upon detection of a damaged container.

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

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

**OnWarning=action** – actions to be performed in case when the application detects a file resembling a known virus within a container.

**OnCured=action** – actions in case of detection and successful disinfection of an infected object within a container.

**OnProtected=action** – actions upon detection of a password-protected encrypted object inside a container. Such objects cannot be scanned.

**OnError=action** – actions to be performed if a system error occurs while scanning a container.

Syntax of the actions that are applied to the objects listed above is similar to that for objects described above in the **[scanner.object]** section.

The **[scanner.report]** section contains report generation parameters for the kavscanner component:

**ReportFileName** – name of the report file where the component logs the results of its activity.

**ReportLevel=4** – report file size.

**Append=yes** – mode for appending new messages to the report file. In order to disable the mode, set the parameter to **no**.

**ShowOK=yes** – mode for logging messages about clean files into the report. In order to disable the mode, set the parameter to **no**.

**ShowContainerResultOnly=no** – logging of the results of archive scanning in the report in short format. Set the parameter to **yes** to add a brief report.

**ShowObjectResultOnly=no** – logging of the results of object scanning in the report in short format. Set the parameter to **yes** to add a brief report.

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

**AVBasesTestPath** – full path to the directory where the anti-virus databases are stored.

**BackUpPath** – full path to an existing directory where earlier anti-virus databases will be preserved during update.

The **[updater.options]** section contains the settings of the keepup2date component:

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

**UseUpdateServerUrlOnly=no** – the mode for using just the address specified by the **UpdateServerUrl** parameter for updating of the anti-virus databases. If the parameter is set to **no**, then after a failed update attempt the application will pick another address from its list of update servers.

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

**RegionSettings=ru** – the code of the user's region (two initial letters of the region's name); this code is used to select a Kaspersky Lab's updates server that would suit best for downloading the updates to the anti-virus databases.

**ConnectTimeout=30** – network timeout for updating the anti-virus databases (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 update servers.

**UseProxy** – mode for proxy server use for connection to a Kaspersky Lab's updates server. If the parameter is set to **no**, the proxy server will not be used. If it is set to **yes**, the proxy server address defined by the **ProxyAddress** parameter. If the value of the **ProxyAddress** setting is not defined, the value of the **http\_proxy** environment variable will be used. If the environment variable is not defined, no proxy server will be used.

**ProxyAddress** – address of the proxy server used for connection. This parameter 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 taken from the environment variable **http\_proxy**.

The **[updater.report]** section contains report generation parameters for the keepup2date component:

**Append=yes** – mode for appending new messages to the report file. In order to disable the mode, set the parameter to **no**.

**ReportFileName** – name of the report file where the component logs the results of its activity.

**ReportLevel=4** – level of details in the reports.

## A.2. Command line options for the kavsamba component

The configuration file parameters can be redefined using command line options, when you are launching the application from the command line. Let us examine them closely.

Help options:	
<b>-h</b>	Display on the console help information about the kavsamba component.
<b>-v</b>	Display program version.
Configuration options:	
<b>-c (-y) &lt;path_to_file&gt;</b>	Use an alternative <b>&lt;path_to_file&gt;</b> configuration file.

## A.3. Kavsamba return codes

The kavsamba component may return any of the following codes while running:

<b>0</b>	The component is running.
<b>64</b>	License information is missing or no license keys have been found using the path specified in the configuration file.
<b>65</b>	The configuration file could not be loaded.
<b>70</b>	The kavsamba component is damaged.

## A.4. Command line options for the kavscanner component

The configuration file parameters can be redefined using command line options, when you are launching the application from the command line. Let us examine them closely.

Help options:	
<b>-h</b>	Display on the console help information about the kavscanner component.
<b>-v</b>	Display program version.
Configuration options:	
<b>-c (-C) &lt;path_to_file&gt;</b>	Use an alternative <b>&lt;path_to_file&gt;</b> configuration file.
<b>-g&lt;path_to_file&gt;</b>	Write the list of all known viruses registered in the anti-virus databases into the <b>&lt;path_to_file&gt;</b> file.
<b>-f</b>	Ignore corrupted signature of the kavscanner component and attempt to disinfect the component.
Scanning options:	
<b>-e &lt;option&gt;</b>	Change the default scan option. The following modes may be used as an <b>&lt;option&gt;</b> :
<b>P/p</b>	Enable/disable scanning of packed files.
<b>A/a</b>	Enable/disable scanning of archives.
<b>S/s</b>	Enable/disable scanning of self-extracting archives.
<b>B/b</b>	Enable/disable scanning of mail databases.
<b>M/m</b>	Enable/disable scanning of plain text mail messages.
<b>E/e</b>	Enable/disable heuristic code analyzer.

<b>-R/r</b>	Enable/disable recursive scanning.
<b>-S/s</b>	Enable/disable symlink opening mode.
<b>-l</b>	Scan local file systems only.
Report generation options:	
<b>-q</b>	Do not print messages to the screen.
<b>-o &lt;name&gt;</b>	Specify the filename for the file into which the report on component activity will be logged. If the filename is not specified, the report will not be generated.
<b>-j&lt;number&gt;</b>	Specify the amount of details in the report. The following detail levels may be used as an <b>&lt;option&gt;</b> :
<b>1</b>	Enable/disable output of messages about other errors.
<b>2</b>	Enable/disable output of informational messages.
<b>3</b>	Enable/disable output of messages related to scanning.
<b>10</b>	Enable/disable output of debugging messages.
<b>-x&lt;option&gt;</b>	Specify the amount of details in the scanning report output to console. The following detail levels may be used as an <b>&lt;option&gt;</b> :
<b>O/o</b>	Short/extended format for messages about simple object scanning.
<b>C/c</b>	Short/extended format for messages about archive scanning.
<b>N/n</b>	Enable/disable output of messages about clean files to the console.
<b>P/p</b>	Enable/disable printing messages about the current operation of the component to the screen.
<b>-m&lt;option&gt;</b>	Specify the amount of details for the scan report logged to the report file. The following modes may be used as an <b>&lt;option&gt;</b> :

<b>O/o</b>	Short/extended format for messages about simple object scanning.
<b>C/c</b>	Short/extended format for messages about archive scanning.
<b>N/n</b>	Enable/disable output of messages about clean files to the report file.
File options:	
<b>-p&lt;option&gt; &lt;file_name&gt;</b>	Save the list of objects into the specified file; save each object with the full path in a new line. The following modes may be used as an <b>&lt;option&gt;</b> :
<b>i</b>	Save the list of infected objects into the <b>&lt;file_name&gt;</b> file.
<b>s</b>	Save the list of suspicious objects into the <b>&lt;file_name&gt;</b> file.
<b>c</b>	Save the list of corrupted objects into the <b>&lt;file_name&gt;</b> file.
<b>w</b>	Save to the <b>&lt;file_name&gt;</b> file a list of objects containing code that resembles known viruses.
<b>-@ &lt;filelist.lst&gt;</b>	Scan objects with the path specified in the <b>&lt;filelist.lst&gt;</b> file.
File processing options (the use of these modifiers in the command line overrides the execution of actions defined in the configuration file):	
<b>-i0</b>	Scan for viruses only.
<b>-i1</b>	Cure infected objects; skip if disinfection is impossible.
<b>-i2</b>	Cure infected objects. If disinfection is impossible and if the object is a simple one - delete it; do not delete infected objects from a container.
<b>-i3</b>	Cure infected objects. If disinfection is impossible and if the object is a simple one - delete it; if the infected object is located in a container - delete the entire container.

<b>-i4</b>	Delete infected objects and containers.
------------	---

## A.5. Kavscanner return codes

The kavscanner component may return any of the following codes while running:

<b>0</b>	No viruses found.
<b>5</b>	All infected objects have been cured.
<b>10</b>	Password-protected archives have been detected.
<b>15</b>	Corrupted files have been detected.
<b>20</b>	Suspicious files have been detected.
<b>21</b>	Files containing code that resembles known viruses have been detected.
<b>25</b>	Infected files have been detected.
<b>30</b>	System error during file scanning.
<b>50</b>	The anti-virus databases could not be loaded (the path specified in the configuration file is not found).
<b>55</b>	Anti-virus databases are corrupted.
<b>60</b>	The Anti-Virus database date stamp is beyond the license key period.
<b>64</b>	License information is missing or no license keys have been found using the path specified in the configuration file.
<b>65</b>	Configuration file could not be loaded.
<b>66</b>	Invalid configuration file option.
<b>70</b>	The kavscanner component is damaged.
<b>75</b>	The kavscanner component is damaged and cannot be cured.

## A.6. Command line options for the licensemanager component

Help options:	
<b>-h</b>	Display on the console help information about the <i>licensemanager</i> component.
<b>-v</b>	Display program version.
Command line options for managing license keys:	
<b>-s</b>	Output information about all installed license keys to the console.
<b>-c (-C) &lt;path_to_file&gt;</b>	Use the <path_to_file> alternative configuration file.
<b>-k &lt;path_to_file&gt;</b>	Display information about the <path_to_file> key on the screen.
<b>-a &lt;path_to_file&gt;</b>	Install the <path_to_file> license key.
<b>-d &lt;a r&gt;</b>	Remove all license keys / remove an additional license key.

## A.7. Licensemanager return codes

The licensemanager component may return any of the following codes while running:

<b>0</b>	The component has successfully loaded license key information and completed its operation.
<b>30</b>	System error has occurred during component operation.
<b>64</b>	License information is missing or no license keys have been found using the path specified in the configuration file.
<b>65</b>	Configuration file could not be loaded.

<b>66</b>	Invalid configuration file option.
-----------	------------------------------------

## A.8. Command line options for the keepup2date component

Help options:	
<b>-v</b>	Output the version to the console and exit the component.
<b>-h</b>	Output to the console help information about the command line options supported by the component and exit.
<b>-s</b>	Output to the console a complete list of update servers including the region code.
Update options:	
<b>-r</b>	Rollback of the last update to the previous version.
<b>-k</b>	Do not execute the <b>PostUpdateCmd</b> command after a successful anti-virus database update.
<b>-q</b>	The mode of the component operation in which no system messages will be printed to the screen.
<b>-e</b>	The mode of the component operation in which only messages about critical errors will be printed to the screen.
<b>-x &lt;path_to_file&gt;</b>	Copy all updates of the anti-virus database into the <b>&lt;path_to_file&gt;</b> local folder.
<b>-g &lt;URL&gt;</b>	Address for updating the anti-virus databases. When this option is specified, the updater will use the address.
<b>-d &lt;path_to_file&gt;</b>	Use the component's PID file located in the <b>&lt;path_to_file&gt;</b> local folder.
Report generation options:	

<b>-l &lt;path_to_file&gt;</b>	Log work results in the <path_to_file> file.
--------------------------------	--

## A.9. keepup2date return codes

The *keepup2date* component may return any of the following codes while running:

<b>0</b>	The anti-virus database does not need to be updated.
<b>1</b>	The anti-virus database has been updated successfully.
<b>10</b>	Critical error occurred; the updating process will be terminated.
<b>12</b>	Error occurred while rolling back to the last update of the anti-virus databases.
<b>30</b>	The <b>PostUpdaterCmd</b> command could not be executed after the databases had been updated.
<b>60</b>	License information is missing or no license key was found using the path specified in the configuration file.
<b>75</b>	The configuration file cannot be loaded or contains errors.

---

## APPENDIX B. KASPERSKY LAB

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

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

Today, Kaspersky Lab employs more than 250 specialists, each of whom is proficient in anti-virus technologies, with 9 of them holding M.B.A. degrees, 15 holding Ph.Ds, and two experts holding membership in the Computer Anti-Virus Researchers Organization (CARO).

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

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

Kaspersky Lab's customers benefit from a wide range of additional services that ensure both stable operation of the company's products, and compliance with specific business requirements. Kaspersky Lab's anti-virus database is updated every 3 hours. The company provides its customers with a 24-hour technical support service, which is available in several languages to accommodate its international clientele.

## B.1. Other Kaspersky Lab Products

### **Kaspersky Lab News Agent**

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

The product performs the following functions:

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

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

### **Kaspersky® OnLine Scanner**

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

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

### **Kaspersky® OnLine Scanner Pro**

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

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

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

### **Kaspersky Anti-Virus® 6.0**

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

The program provides for complex anti-virus checks including:

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

Proactive protection offers the following features:

- **Control of changes within file system.** The program allows users to create a list of applications, which it will control on a per component basis. It helps protect application integrity against the influence of malicious software.
- **Monitoring of processes in random-access memory.** Kaspersky Anti-Virus 6.0 in a timely manner notifies users whenever it detects dangerous, suspicious or hidden processes or in case when unauthorized changes in standard processes occur.
- **Monitoring of changes in OS registry** due to internal system registry control.
- **Blocking of dangerous VBA macros** in Microsoft Office documents.
- **System restoration** after malicious spyware influence accomplished due to recording of all changes in the registry and computer file system and an opportunity to perform their roll-back at user's discretion.

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

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

The anti-virus protection feature includes:

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

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

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

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

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

## Kaspersky® Security for PDA

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

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

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

## Kaspersky Anti-Virus Mobile

Kaspersky® Anti-Virus Mobile provides for anti-virus protection of mobile devices running Symbian OS or Microsoft Windows Mobile. The software allows the user to perform complex anti-virus scanning including:

- **On-demand scanning** of mobile device's memory, individual folder or a specific file. If an infected objects is detected, it is relocated to Quarantine directory or deleted.
- **Real-time scanning:** the product scans automatically all incoming objects or objects being modified as well as all accessed files.
- **Scheduled scanning** of data preserved in memory of a mobile device.
- **Protection against SMS and MMS spam.**

## Kaspersky Anti-Virus® Business Optimal

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

Kaspersky Anti-Virus® Business Optimal guarantees full-scale anti-virus protection<sup>1</sup> for:

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

---

<sup>1</sup> Depending on the type of distribution kit.

- *E-mail systems* including Microsoft Exchange 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail, and Qmail.
- *Internet gateways*: CheckPoint Firewall –1; Microsoft ISA Server 2000 Standard Edition, and Microsoft ISA Server 2004 Standard Edition.

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

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

### **Kaspersky® Corporate Suite**

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

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

- Workstations running Windows 98/ME, Windows NT/2000/XP, and Linux;
- *File servers* running Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Microsoft Windows 2003 Server, Novell Netware, FreeBSD, and Linux; Samba *file servers*.
- E-mail clients, including Microsoft Exchange Server 5.5/2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim and Qmail.
- Internet-gateways: CheckPoint Firewall –1, Microsoft ISA Server 2000 Enterprise Edition, Microsoft ISA Server 2004 Enterprise Edition.
- Hand-held computers (PDAs), running Symbian OS, Windows CE and Palm OS, and also smartphones running Microsoft Windows Mobile 2003 for Smartphone and Microsoft Smartphone 2002.

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

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

### **Kaspersky® Anti-Spam**

Kaspersky® Anti-Spam is a cutting-edge software suite that is designed to help organizations with small- and medium-sized networks wage war against the onslaught of undesired e-mail (spam). The product combines the revolutionary

technology of linguistic analysis with modern methods of e-mail filtration, including RBL lists and formal letter features. Its unique combination of services allows users to identify and wipe out up to 95% of unwanted traffic.

Installed at the entrance to a network, 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 by samples provided by the Company's linguistic laboratory specialists.

### **Kaspersky SMTP Gateway**

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

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

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

### **Kaspersky® Mail Gateway**

Kaspersky Mail Gateway is a comprehensive solution that provides complete protection for users of mail systems. This application installed between the corporate network and the Internet scans all components of e-mail messages for the presence of viruses and other malware (Spyware, Adware, etc.) and performs centralized anti-spam filtration of e-mail stream. This solution also includes some additional mail traffic filtration features for e-mail filtering by names and MIME types of attached files as well as tools that help decrease the load on mail systems and prevent hacker attacks

### **Kaspersky Anti-Virus® for Proxy Server**

Kaspersky Anti-Virus® for Proxy Server is an anti-virus solution for protection of HTTP web traffic passing proxy servers. The application scans in real time Internet traffic protecting computers from penetration of malicious software during Web surfing and checking files downloaded from the Internet.

### **Kaspersky Anti-Virus® for MIMESweeper for SMTP**

Kaspersky Anti-Virus® for MIMESweeper for SMTP provides for fast anti-virus scanning of SMTP traffic on servers using Clearswift MIMESweeper.

The software is implemented as an anti-virus plug-in for Clearswift MIMESweeper for SMTP that scans incoming and outgoing e-mail processing it in real time.

## B.2. Contact Us

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

Technical support	Please find the technical support information at <a href="http://www.kaspersky.com/supportinter.html">http://www.kaspersky.com/supportinter.html</a>
General information	WWW: <a href="http://www.kaspersky.com">http://www.kaspersky.com</a> <a href="http://www.viruslist.com">http://www.viruslist.com</a> Email: <a href="mailto:sales@kaspersky.com">sales@kaspersky.com</a>

---

# APPENDIX C. LICENSE AGREEMENT

## End User License Agreement

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

### 3. Support.

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

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

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

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

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

(iv) "Support Services" means:

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

(b) Free software updates, including version upgrades;

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

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

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

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

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

#### 6. Limited Warranty.

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

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

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

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

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

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

#### 7. Limitation of Liability.

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

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

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

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

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

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

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