

KASPERSKY LAB

Kaspersky Anti-Virus® 5.5 for Linux
and FreeBSD Mail Servers

ADMINISTRATOR'S
GUIDE

KASPERSKY ANTI-VIRUS® 5.5 FOR
LINUX AND FREEBSD MAIL SERVERS

Administrator's guide

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

Revision date: July 2007

Contents

CHAPTER 1. KASPERSKY ANTI-VIRUS 5.5 FOR LINUX AND FREEBSD MAIL SERVERS.....	6
1.1. What's new in version 5.5	7
1.2. Hardware and software requirements	8
1.3. Distribution kit	9
1.4. Services for registered users	10
CHAPTER 2. TYPICAL PATTERNS OF APPLICATION DEPLOYMENT	11
2.1. Internal architecture of Kaspersky Anti-Virus	11
2.2. Operation on the same server as the mail server	13
2.3. Operation on a dedicated server.....	14
CHAPTER 3. INSTALLING KASPERSKY ANTI-VIRUS	17
3.1. Installing the application to a server running Linux.....	17
3.2. Installing the application to a server running FreeBSD.....	18
3.3. Installation procedure	18
3.4. Configuring the application.....	19
CHAPTER 4. POST-INSTALLATION SETUP	20
4.1. Default application settings	20
4.2. Installing / updating the anti-virus databases.....	22
4.3. Using Webmin plug-in for Kaspersky Anti-Virus management	22
4.4. Manual integration with mail systems	23
4.4.1. Integration with Sendmail	23
4.4.2. Integration with Qmail.....	24
4.4.3. Integration with Postfix.....	25
4.4.4. Integration with Exim	25
4.4.5. Configuring Kaspersky Anti-Virus for integration with a mail system.....	26
CHAPTER 5. WORKING WITH KASPERSKY ANTI-VIRUS.....	28
5.1. Updating Kaspersky Anti-Virus databases.....	28
5.1.1. Database update from Kaspersky Lab servers	29
5.1.2. Scheduling anti-virus database updates using cron.....	30

5.1.3. Manual updating of the anti-virus databases	30
5.1.4. Creating and using a local source of updates	31
5.1.5. Updating the anti-virus databases via a proxy server	32
5.2. Antiviral protection of the server's mail traffic	32
5.2.1. Delivering clean and disinfected messages	33
5.2.2. Delivery of all messages	34
5.2.3. Delivery of messages containing password-protected archives	36
5.2.4. Blocking message delivery	36
5.2.5. Complementary filtration of messages by attachment types	38
5.3. Anti-virus protection of file systems	40
5.3.1. On-demand scanning	41
5.3.2. Scheduled directory scans using cron	41
5.3.3. Advanced options: using scripts	42
5.3.3.1. Cleaning infected archives	42
5.3.3.2. E-mail notification of administrator	42
5.3.4. Moving objects to Quarantine	43
5.3.5. Backup of processed objects	44
5.4. Product key management	45
5.4.1. Licensing mechanism	45
5.4.2. Viewing the product key information	46
5.4.3. Key validity extension	48
CHAPTER 6. ADVANCED SETTINGS	49
6.1. Setting up antiviral protection of mail traffic	49
6.1.1. Forming user groups	50
6.1.2. Message check and disinfection mode	51
6.1.3. Actions on objects	52
6.1.4. Notifying senders, recipients, and administrators	54
6.2. Configuring anti-virus protection for server file systems	56
6.2.1. Scanning area	56
6.2.2. File scanning and disinfection mode	57
6.2.3. Operations on files	58
6.2.4. Backup mode	59
6.3. Optimizing Kaspersky Anti-Virus	59
6.3.1. Using iChecker database	60
6.3.2. Reducing the server load	60
6.4. Configuring the <i>aveserver</i> process	60

6.4.1. Aveserver reloading.....	61
6.4.2. Forced <i>aveserver</i> termination	62
6.5. Scanning of POP3 mail from external mailboxes.....	62
6.6. Additional features for Postfix.....	64
6.6.1. DSN extension support	64
6.6.2. 8bit-MIME extension support	65
6.6.3. X-Forward extension support.....	65
6.6.4. Incoming SMTP support in <i>smtpscanner</i>	65
6.7. Localization of displayed date and time format	66
6.8. Event logging parameters in Kaspersky Anti-Virus	66
6.8.1. Format of messages about scanning.....	68
6.8.2. The format of messages output to the console	70
6.8.3. Anti-virus statistics of the application	70
6.8.4. Additional data fields in messages.....	71
CHAPTER 7. UNINSTALLING KASPERSKY ANTI-VIRUS.....	72
CHAPTER 8. TESTING THE OPERATION OF KASPERSKY ANTI-VIRUS.....	73
CHAPTER 9. FREQUENTLY ASKED QUESTIONS.....	75
APPENDIX A. KASPERSKY LAB.....	81
A.1. Other Kaspersky Lab Products	82
A.2. Contact Us.....	90
APPENDIX B. LICENSE AGREEMENT.....	91

CHAPTER 1. KASPERSKY ANTI-VIRUS 5.5 FOR LINUX AND FREEBSD MAIL SERVERS

Kaspersky Anti-Virus® 5.5 for Linux and FreeBSD Mail Servers (hereinafter referred to as *Kaspersky Anti-Virus*) is designed for anti-virus processing of mail traffic and file systems of servers running the Linux or FreeBSD operating systems, and using the Sendmail, Postfix, Qmail, or Exim mail programs.

This application allows the user to:

- *Check for viruses* incoming and outgoing mail messages, as part of the server's SMTP traffic.
- *Detect* infected, suspicious, corrupted, and password-protected files, as well as files that cannot be scanned.
- *Cure* infected objects in file systems and mail messages.
- *Quarantine* all infected, suspicious, and corrupted objects of the server file system and its mail traffic. Password-protected files can also be quarantined, as well as files that cannot be scanned.
- *Process mail traffic* according to rules preset for groups of senders and recipients.
- *Provide secondary filtering of mail traffic* by name and type of attached files, and use individual processing rules for the filtered objects.
- *Notify* the sender, recipient, and group administrator about mail messages that contain infected, suspicious, and other objects.
- *Update the anti-virus databases* using Kaspersky Lab's update servers as the source.

The anti-virus database is used to search for and clean infected objects. During the scan each file is analyzed for the presence of viruses by comparing the file's code with code stored in the database which are specific to individual viruses. If the file is infected, the application disinfects it, again using information stored in the database.

New viruses appear daily, and therefore the experts at Kaspersky Lab recommend updating the anti-virus database hourly to maintain the application in up-to-date condition.

- *Scan for viruses* all mounted file systems.
- *Configure Kaspersky Anti-Virus* via the web-based interface provided by the Webmin program and the application configuration file.

1.1. What's new in version 5.5

Version 5.5 of Kaspersky Anti-Virus for Linux and FreeBSD Mail Servers features the following improvements over version 5.0:

- The *keepup2date* component uses new technologies to download updates to the anti-virus databases and application modules, cutting down on network traffic. Integrity checks for downloaded databases ensure secure application operation.
- A backup storage area preserves copies of suspicious or infected objects prior to their disinfection or removal. This allows the recovery of the original data if errors occur during object disinfection.
- The iChecker technology and double-level caching of scanned objects have been implemented to decrease server load during anti-virus scanning.
- The Webmin application can now be used to remotely view both statistics of virus activity for a specified period, and data on the types of viruses detected during an anti-virus scan.
- The option to restrict the number of objects scanned simultaneously in the background has been added, to optimize server load.
- A list of detectable viruses can now be generated.
- The option to select the current protocol (SMTP or LMTP) for operation of the *smtpscanner* component has been added.
- It is now possible to notify e-mail senders about message delivery when the SMTP protocol is used.
- The option has been added to save, for each message, the names of detected viruses and the message identification code in the event log file produced by the *smtpscanner* component.
- The application licensing policy has been changed. In particular, it is no longer necessary to create and maintain a list of protected users; this list is automatically generated and maintained by the application now.
- The active anti-virus databases (standard databases, extended or paranoid set) can be specified individually for each application component.

- A new macro, which inserts all headers from the original message, has been added for use with notifications.
- The application setup and removal procedures have been simplified considerably. In particular, the application correctly removes its traces from configuration files during the uninstall procedure.
- Installation has been made faster by enabling the application to import configuration settings from earlier versions (4.0 or 5.0).
- The installer now correctly detects the presence of, and integrates the application with, Kaspersky Anti-Spam, and restores the previous configuration during the uninstall procedure.
- Support for the DSN, 8bit-MIME, X-Forward extensions and SMTP as an incoming transfer protocol has been added.
- The application now features an opportunity to append additional information about the results of anti-virus scanning and processing to the headers of scanned messages.

1.2. Hardware and software requirements

The minimum system requirements for **Kaspersky Anti-Virus** are:

- Hardware requirements:
 - Intel Pentium-class processor
 - 32 Mb of RAM or more
 - 100 Mb or more of available hard disk space.
- Software requirements:
 - One of the following operating systems:
 - Red Hat Linux 9.0
 - Red Hat Enterprise Linux Advanced Server 3
 - Fedora Core 3
 - SuSE Linux Enterprise Server 9.0
 - SuSE Linux Professional 9.2
 - Mandrake Linux 10.1
 - Debian GNU/Linux 3.0 updated (r4)

- FreeBSD 4.10 or 5.3
- One of the following mail systems:
 - sendmail 8.x,
 - qmail 1.03,
 - postfix 1.0 or higher,
 - exim 4.0.
- Perl version 5.0 or higher (www.perl.org) for Kaspersky Anti-Virus installation, and the which utility for installation of the application.
- The Webmin utility (www.webmin.com) 1.070 or higher for remote administration of the application.

1.3. Distribution kit

You can purchase Kaspersky Anti-Virus either from our distributors (retail box) or in our Internet-shop (www.kaspersky.com, **E-Store** section).

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

A sealed envelope with an installation CD containing software application files

Administrator's guide

Product key included into the distribution package or recorded to an individual floppy disk

License agreement.

Please read the license agreement carefully before opening the CD envelope.

Opening the sealed envelope of the installation CD or installing the application on a computer confirms your acceptance of all terms and conditions of the license agreement.

If you purchase our application from a web shop, you download it from the Kaspersky Lab site; the copy also contains this manual. Your product key is either included into the installation file or sent to you by e-mail after payment.

The license agreement constitutes a legal agreement between you and Kaspersky Lab containing the terms and conditions subject to which you may use the purchased software.

Please read the license agreement carefully!

If you do not agree with the terms of the license agreement, you may return the box with Kaspersky Anti-Virus to the distributor, where you have purchased it; you will be refunded the amount you've paid for subscription, provided the CD envelope remains sealed.

1.4. Services for registered users

Kaspersky Lab offers its legal users a broad range of services maximizing the efficiency of Kaspersky Anti-Virus software.

By purchasing a subscription you become a registered software user entitled to the following services throughout the license period:

- Software upgrades for this software application.
- Consultations regarding issues pertaining to installation, configuration and use of this software. You can contact the Technical Support service for consulting using any of the following methods:
- Make a phone call to Technical Support.
- Create and send a request using the Technical Support web site (<http://www.kaspersky.com/helpdesk>) or your personal user cabinet.
- notifications about new software products from Kaspersky Lab, and about new virus outbreaks. This service is provided to users who have subscribed to the Kaspersky Lab e-mail newsletter service.

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

CHAPTER 2. TYPICAL PATTERNS OF APPLICATION DEPLOYMENT

Depending on the initial architecture of the mail server, there are several options for deploying Kaspersky Anti-Virus for Linux and FreeBSD Mail Servers:

- *On the same server with the e-mail software.* This option is used when the server is hosting a Sendmail, Qmail, Postfix or Exim mail software (see section 2.2 on page 13).
- *On a dedicated server as a secondary filter.* This option is recommended when the primary mail server is running an unsupported operating and/or mail system (see section 2.3 on page 14).
- *As a filter for external mail services.* This option is useful when mail server users have their mailboxes on external servers, in order to provide antiviral protection of downloaded mail messages (see section 6.5 on page 62).

In all these cases, Kaspersky Anti-Virus can both filter mail traffic and scan all mounted file systems.

Prior to studying the above deployment patterns in detail, we shall review the internal architecture of Kaspersky Anti-Virus in order to fully understand its operational algorithm.

2.1. Internal architecture of Kaspersky Anti-Virus

When using Kaspersky Anti-Virus, it is important to understand its operational algorithm.

This section reviews the application's internal architecture, concentrating on mail traffic scanning, since the process of scanning server file systems is comparatively straightforward and does not require a special in-depth study.

It should be noted that Kaspersky Anti-Virus is only capable of scanning mail for viruses, and does not constitute a mail agent capable of receiving and routing mail traffic. This must be carried out by a mail system installed on the server, with which the anti-virus program is integrated after installation.

In the following examples illustrating internal operation of Kaspersky Anti-Virus for Linux and FreeBSD after its integration with the mail system, the Sendmail mail server will be used as an example.

In the process of anti-virus integration into the Sendmail server, an additional configuration file `sendmail.cf.listen` is created.

When started with this configuration file, Sendmail receives mail traffic and passes it to Kaspersky Anti-Virus for scanning. If started with the original configuration file (`sendmail.cf`), it delivers mail messages received from the application.

Thus, mail messages are scanned using the following algorithm:

1. Sendmail receives e-mail via the SMTP protocol (configuration file `sendmail.cf.listen`). Sendmail creates a queue, in which it stores the incoming mail and passes it via the LMTP or SMTP protocol to the `smtpscanner` component for scanning.
2. The `smtpscanner` component processes the mail traffic according to the defined settings. Mail message scanning and cleaning is carried out as follows:
 - a. `smtpscanner` passes the file name for the mail message to the `aveserver` component using the local socket.
 - b. `aveserver` scans and disinfects the object using the anti-virus databases.
 - c. `smtpscanner` receives from `aveserver` a return code that defines the status of the file.
 - d. Depending on the object status, `smtpscanner` processes it according to the configuration file.
3. The processed mail traffic, with notifications regarding the results of scanning and cleaning, is transferred via the SMTP protocol to the Sendmail server (with `sendmail.cf` configuration file), which delivers this mail traffic to local users or routes it to other mail servers.

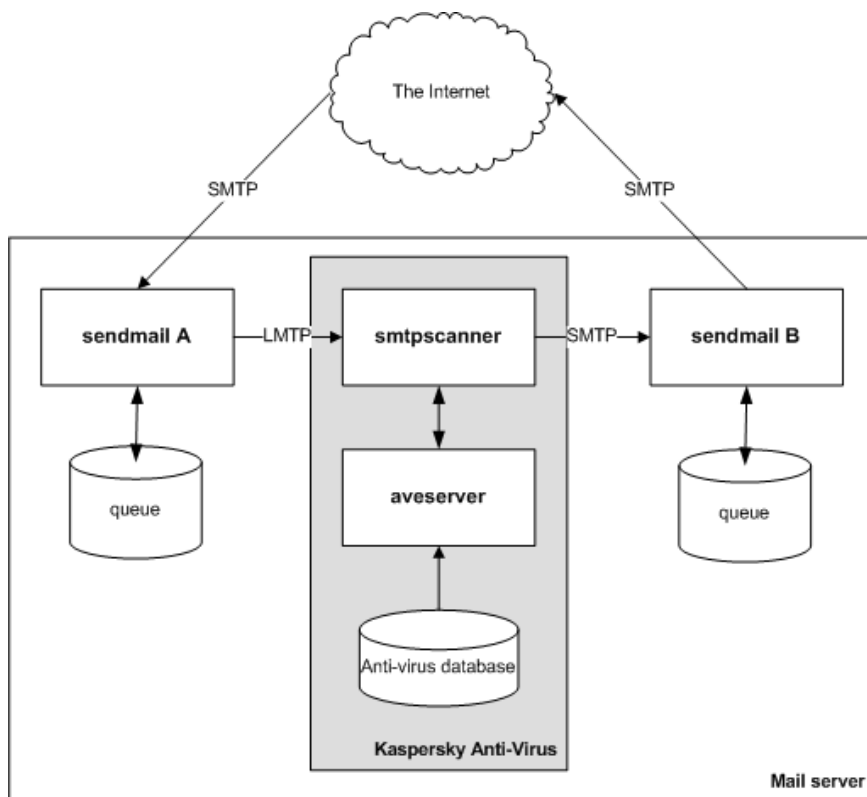


Figure 1. Internal architecture of Kaspersky Anti-Virus for Linux and FreeBSD Mail Servers

2.2. Operation on the same server as the mail server

In this document, the operation and configuration of Kaspersky Anti-Virus are described only for the case of installation on one server with a mail system.

The installation and operation of Kaspersky Anti-Virus on the same server as the mail software is only possible with supported operating systems (Linux or FreeBSD), and with supported mail systems (Sendmail, Qmail, Postfix or Exim).

This configuration is recommended for mail servers operating with average load.

Let us take a detailed look at the operation of Kaspersky Anti-Virus on the same server as any of the above mentioned mail systems (see Figure 2). The sequence of processing incoming and outgoing mail is identical, and consists of the following stages:

1. The stream of mail messages comes in from other servers, or from the LAN, via the SMTP protocol.
2. The mail system receives the mail traffic and passes it to Kaspersky Anti-Virus for scanning.
3. The application processes the mail traffic according to the specified settings, and returns it to the mail system along with an additional set of notifications.
4. The mail system routes the mail traffic further.

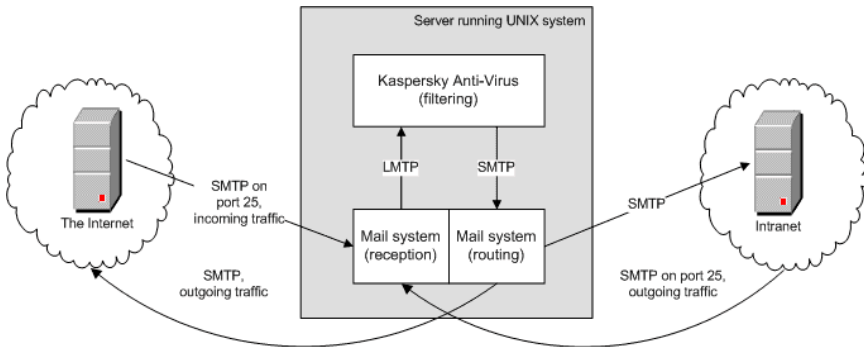


Figure 2. Diagram of Kaspersky Anti-Virus operation on the same server with mail system

Based on the above diagram, during installation or post-installation configuration of Kaspersky Anti-Virus, the following settings must be adjusted:

- Define the port which Kaspersky Anti-Virus will use.
- Set the mail system port that the program will use to receive mail from Kaspersky Anti-Virus after filtering.

2.3. Operation on a dedicated server

Kaspersky Anti-Virus for Linux and FreeBSD Mail Servers can scan and provide anti-virus processing, for mail traffic even if your mail server is running another operating system, for example Microsoft Windows Server 2003.

In this situation, Kaspersky Anti-Virus must be installed on a dedicated server running Linux or FreeBSD.

In order to receive mail traffic and forward it to the Windows mail server, a mail system (Sendmail, Qmail, Postfix or Exim) must also be installed on the dedicated server. Then Kaspersky Anti-Virus should be installed and integrated with the mail system (see section 4.4 on page 23).

With this layout, the operation has the following sequence (see Figure 3):

1. Mail traffic is received by the server running an operating system belonging to the Unix family.
2. The mail system (e.g., Postfix) forwards it to Kaspersky Anti-Virus via the LMTP or SMTP protocol for scanning.
3. Checked mail with notifications created by the anti-virus is passed back to the mail system, which in turn forwards it to the main mail server for delivery or further routing.

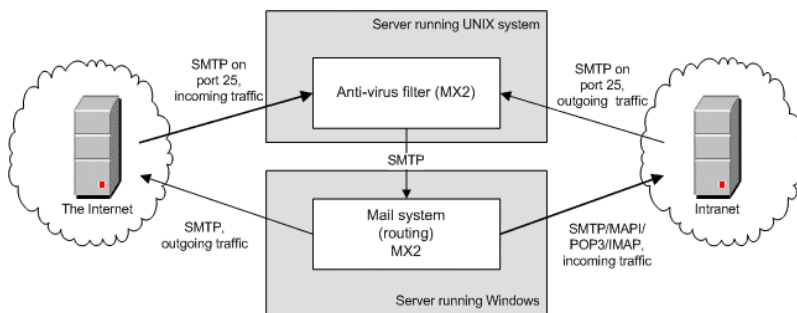


Figure 3. Diagram of Kaspersky Anti-Virus operation on a dedicated server

On the above diagram, the server with Kaspersky Anti-Virus installed is the primary server since it receives mail stream and resends it, while the server with Microsoft Exchange Server is the secondary one, which only delivers mail.

However, if prior to installation of Kaspersky Anti-Virus your mail server had been used to screen messages by senders' IP addresses, then the server with Kaspersky Anti-Virus must be defined as secondary. The reason is that if you make the server hosting Kaspersky Anti-Virus the primary one, all the mail messages will be received by the secondary server (with IP filtering) from the same IP address, making filtering impossible.

If there are mail servers within your LAN, then the MX-records or forwarding parameters must point to the primary server, not the secondary one.

- Primary filter (MX1) settings:

- Name of the host server where the filter is installed:
mx1.yourhost.domain
- Host server name for mail forwarding: mx2.yourhost.domain:25
- Secondary filter (MX2) settings:
 - Name of the host server where the filter is installed:
mx2.yourhost.domain
 - Host server name from which the mail is received:
mx1.yourhost.domain

CHAPTER 3. INSTALLING KASPERSKY ANTI-VIRUS

Before installing Kaspersky Anti-Virus for Linux and FreeBSD, you are advised to make the following preparations for your system:

- Make sure your system meets the hardware and software requirements listed in section 1.2 on page 8. If any recommended application has not been installed yet, you are advised to install it, or else a part of the application's functionality will be unavailable.
- Make backup copies of configuration files of the mail system installed on your server.
- Set up an Internet connection.
- **Stop the mail server** into which Kaspersky Anti-Virus will be integrated.
- Log in to the system as **root**.

We advise that you install the application in off hours or when the mail traffic has the lowest intensity!

3.1. Installing the application to a server running Linux

Kaspersky Antivirus is distributed in two different installation packages (rpm or deb).

To initiate installation of Kaspersky Anti-Virus from the .rpm package, enter the following on the command line:

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

To initiate installation of Kaspersky Anti-Virus from the .deb package, enter the following on the command line:

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

3.2. Installing the application to a server running FreeBSD

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

To initiate installation of Kaspersky Anti-Virus from the .pkg package, enter the following on the command line:

```
# pkg_add <package_name>
```

3.3. Installation procedure

If the installation process terminates with an error, please check that your computer meets the hardware and software requirements (see section 1.2 on p. 8) and that you have logged in to the system as **root**.

To install the application on a server, follow the steps below:

1. Copy application files to server.
2. Install product key.

If the key is not installed, work with the application will be impossible. If you have no product key at the time of installation (for example, if you purchased the application via the Internet and have not received the key by e-mail yet), you can install the key after the setup procedure but before you actually start using the application.

3. Configure the *keepup2date* component.
4. Update the anti-virus databases.

Ensure that the anti-virus databases are updated after application setup. The databases contain descriptions of all currently known viruses and cure methods for infected objects. Scanning and processing of files cannot be performed without the anti-virus databases!

Automatic configuration of the application will not be performed if the anti-virus databases are not installed.

5. Install the Webmin module.

The Webmin module for remote software management can be installed correctly only if the Webmin application is located in the default directory. After Webmin is installed, you will receive detailed instructions on how to configure the module to work with the application.

These steps are examined in more detail in the following sections.

3.4. Configuring the application

As soon as the product files are copied to the server, the installer initiates system configuration. Depending upon the package manager being used, the configuration procedure will be started automatically (e.g., RPM) or, if the manager does not support interactive scripts, the administrator may have to do that manually. In the latter case the installer will display an appropriate notification.

The configuration procedure consists of the following steps:

- Searching for an installed mail server, and comparing its version with the software requirements.
- Searching for the mail server configuration file, and modify it.

If additional information becomes necessary during configuration (e.g., the path to the mail server's configuration file), the installer will issue requests for information to the server's console. Entry of invalid answers will terminate the process.

If these configuration steps finish successfully, the application is ready to work; the installer will not produce additional notifications. The configuration file bundled with the installation package contains all parameters required to start operation.

Please make sure to restart the mail server before you begin using the application.

CHAPTER 4. POST- INSTALLATION SETUP

During installation, the system onto which you install Kaspersky Anti-Virus is analyzed and some of the application's configuration parameters are set automatically to the most suitable values for the system (see section 4.1 on page 20).

Before you begin using the application, update the anti-virus databases if it has not been done during the installation, and scan the server's file systems for viruses.

To begin working with the program, you need to do the following:

- Integrate Kaspersky Anti-Virus with the mail system installed on your server (see section 4.4.5 on page 26).
- Create a list of protected users whose mail will be scanned for viruses and disinfected, if necessary (see section 5.4.1 on page 45).

In addition, you are advised to set up Kaspersky Anti-Virus for joint operation with the Webmin package.

This chapter describes the default settings of Kaspersky Anti-Virus and takes a look at the configuration required to use the application.

Examples further demonstrate paths typical for Linux distributions.

4.1. Default application settings

All the parameters of Kaspersky Anti-Virus for Linux and FreeBSD are stored in the default configuration file `/etc/kav/5.5kav4mailservers.conf`.

You can create your own configuration files.

Below you can find the default configuration file settings. Information about additional settings that may be necessary to use the application are described in another section (see Chapter 6 on page 49).

By default the Anti-Virus does not cure infected files: such files are deleted without disinfection.

ANTI-VIRUS PROTECTION OF THE SERVER'S MAIL TRAFFIC

Anti-virus protection of mail traffic is impossible until Kaspersky Anti-Virus is integrated with the mail system. The settings explained below determine the application's operation by default once it has been integrated with the mail system.

The `[smtpscan.group:default]` section of the `kav4mailservers.conf` configuration file defines the presence of the `default` group, which includes all the protected users of the mail server associated with no special scanning rules. The group sets the following rules for anti-virus scanning and processing of the mail traffic:

- Incoming and outgoing mail messages are scanned.
- If infected mail messages are detected the application disinfects them.

Disinfected mail messages are delivered to the recipients and to the group administrator (default address: `postmaster@localhost`) along with notifications stating that the messages contained viruses and were successfully disinfected. Similar messages are sent to the senders of the messages.

If a message fails to be disinfected, it is deleted, and an appropriate notification is sent to the recipient, the sender, and group administrator.

All notifications regarding mail message scanning, disinfection, deletion, quarantine etc. are by default sent from the `MAILER-DAEMON@localhost` address.

- During anti-virus scanning of mail traffic, any suspicious or corrupted files, and mail messages that cannot be scanned, are deleted. Appropriate notifications are sent to the recipient, the sender, and the group administrator.
- All actions taken by the application are logged in the report file.

Please note that the `aveserver` process must be running to enable anti-virus scanning of mail traffic. If this process is disabled, all incoming mail traffic is automatically queued for scanning and processing. Information about this is saved in the application log file. See section 6.4 on page 60.

ANTI-VIRUS PROTECTION OF THE SERVER'S FILE SYSTEMS

The default settings for Kaspersky Anti-Virus are such that when the `kavscanner` component is launched without any command line switches, it recursively scans server file systems for viruses, beginning with the current directory.

If any infected, suspicious or corrupted files are found, corresponding messages will be sent to the console and added to the report file.

4.2. Installing / updating the anti-virus databases

You are advised to install/update the anti-virus database immediately after installing the application.

To do so, please run the *keepup2date* component:

```
# /opt/kav/5.5/kav4mailservers/bin/keepup2date
```

The anti-virus databases will be downloaded from Kaspersky Lab's update servers and stored in the directory specified in the configuration file.

Experts at Kaspersky Lab recommend that you update the anti-virus database every hour since efficient operation of the Anti-Virus requires its up-to-date status. For more information regarding database updating refer to the sections 5.1.2 - 5.1.3 on page 30 - 30.

4.3. Using Webmin plug-in for Kaspersky Anti-Virus management

If you plan to control Kaspersky Anti-Virus remotely, it must be configured for work with the Webmin utility.

For example, Webmin may be used for restricting access to the program by setting user passwords. For further details regarding configuring Webmin, please refer to the documentation supplied with it.

Anti-Virus settings modified remotely from 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:

- 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 as required.
- Specify the alternative configuration file name in the **Full path to KAV config** parameter field of the **Config edit** tab.

4.4. Manual integration with mail systems

If the application has not been integrated automatically during its installation (see section 3.4 on page 19), you can perform the integration procedure manually.

The integration procedure consists of configuring your mail system for work with Kaspersky Anti-Virus (see sections 4.4.1-4.4.4 on pages 23-25), setting up the application for work with the mail system (see section 4.4.5 on page 26) and start of the e-mail system with new configuration.

Users whose accounts are employed to launch and operate the mail system must have the rights to read configuration files of the respective mail system.

The following sub-sections contain the details of manual integration of Kaspersky Anti-Virus with supported mail systems.

4.4.1. Integration with Sendmail

To configure Kaspersky Anti-Virus for work with Sendmail, the following steps are required:

1. Copy `sendmail.cf` to the `sendmail.cf.listen` file.
2. In the new `sendmail.cf.listen` file create the following rule:

```
SParseLocal=98
R$*[tab_character] $#smtpscanner $@$1 $:$1
```

- Add `smtpscanner` description in the file:

```
Msmtpscanner,
P=
/opt/kav/5.5/kav4mailservers/bin/smtpscanner,
F=PCXmz9, S=EnvFromSMTP, R=EnvToSMTP,
E=\r\n, L=2040,
T=SMTP,
A=smtpscanner
```

3. Configure Kaspersky Anti-Virus as required for the integration (see section 4.4.5 on page 26).

Add the following two processes to the start-up scripts:

```
/usr/sbin/sendmail -bd -q10m -C \
/etc/mail/sendmail.cf.listen
```

```
/usr/sbin/sendmail -C /etc/mail/sendmail.cf
```

If Sendmail version 8.12 is used in configuration with `submit.cf`, add the following processes to the start-up scripts:

```
/usr/sbin/sendmail -bd -q10m \  
-C /etc/mail/sendmail.cf.listen  
  
/usr/sbin/sendmail \  
-C /etc/mail/sendmail.cf  
  
/usr/sbin/sendmail -C /etc/mail/submit.cf
```

After Kaspersky Anti-Virus integration with Sendmail, use the `kavsend-mail.sh` script included into the application package to start the mail system and anti-virus scanning of e-mail messages.

4.4.2. Integration with Qmail

When Kaspersky Anti-Virus is integrated with Qmail mail system its *smtpscanner* component replaces the *qmail-queue* program. To send messages or place them in the queue, *smtpscanner* calls the original *qmail-queue* program.

To configure Kaspersky Anti-Virus for work with Qmail, the following steps are required:

1. Rename the *qmail-queue* file in the `/var/qmail/bin/` directory to *queue.kav55*.
2. Copy the *qmail-queue* file from the `/opt/kav/5.5/kav4mailservers/bin/` directory to the `/var/qmail/bin` directory or create a symbolic link to that file.
3. Set the following permissions to access the *qmail-queue* and *queue.kav55* files:

```
16 -rws-x-x 1 qmailq qmail 12688 Mar 24  
13:56 queue.kav55  
316 -rwx-x-x 1 qmailq qmail 315612 Apr  
14 11:29 qmail-queue
```

4. Configure Kaspersky Anti-Virus as required for the integration (see section 4.4.5 on page 26).
5. Restart the mail system.

If your Qmail system uses the `softlimit` utility, you should either increase the amount of available memory, or disable memory limitations. Otherwise difficulties may be possible while scanning large e-mail messages.

4.4.3. Integration with Postfix

To configure Kaspersky Anti-Virus for work with Postfix, the following steps are required:

1. Add the following line to the Postfix mail system configuration file `main.cf`:
`content_filter = lmtp:localhost:10025`
2. Add the following lines to the Postfix mail system configuration file `master.cf`:
`localhost:10025 inet n n n -
 10 spawn user=kluser
 argv=/opt/kav/bin/smtpscanner
localhost:10026 inet n - n - 10
 smtpd -o content_filter=-o
 myhostname=localhost`
3. Create the `/var/spool/filter` directory.
4. Create the `kluser` user, include the account in the `filter` group with `/var/spool/filter` specified as home directory.
5. Modify the rights to access the `/var/spool/filter` directory accordingly and keep in mind that `smtpscanner` will work using the permissions assigned for the `kluser` account:

```
mkdir /var/spool/filter  
groupadd filter  
useradd kluser -s /bin/false -d /var/spool\  
/filter -g filter  
chown kluser.filter /var/spool/filter
```

6. Configure Kaspersky Anti-Virus as required for the integration (see section 4.4.5 on page 26).
7. Restart the mail system.

4.4.4. Integration with Exim

To configure Kaspersky Anti-Virus for work with Exim, the following steps are required:

1. Copy the configuration file, (as a rule, `exim.conf`) to `exim.conf.listen`.
2. Edit the `exim.conf.listen` file as follows:
 - add these lines in the TRANSPORT CONFIGURATION section:

```
kav_lmtp_transport:
driver = lmtp
command = /opt/kav/bin/smtpscanner
```

- define local mail delivery parameters in the ROUTERS CONFIGURATION section:

```
localuser:
driver=accept
transport=kav_lmtp_transport
```

set the parameters for remote mail delivery:

```
lookuphost:
driver=dnslookup
transport=kav_lmtp_transport
```

3. Configure Kaspersky Anti-Virus for the integration as required (see section 4.4.5 on page 26).
4. Add the following two processes to the start-up scripts:

```
exim -q10m -bd -C /etc/exim/exim.conf.listen
exim -C /etc/exim/exim.conf
```

If you need to launch the *smtpscanner* component on behalf of another user account, compile the Exim mail system with altered values for the EXIM_GID and EXIM_UID parameters. For more details please refer to the documentation supplied with the Exim mail system).

After Kaspersky Anti-Virus integration with Exim, use the *kavexim.sh* script included into the application package to start the mail system and perform anti-virus scanning of e-mail messages.

4.4.5. Configuring Kaspersky Anti-Virus for integration with a mail system

To integrate Kaspersky Anti-Virus with a mail system, the Anti-Virus settings need to be configured, too.

Required settings are entered directly in the configuration file of the application.

To configure Kaspersky Anti-Virus for operation with a mail system, the following steps must be performed:

- Specify the address to send notifications from:

```
NotifyFromAddress=<e-mail address>
```

- Define the mail receipt and delivery settings in the **[smtpscan.general]** section. The parameters use the following syntax: **protocol:host:port**, where:

- **protocol** is the protocol, which will be used for mail sending (**smtp** or **lmtp**)
- **host** is the name of the host or its IP address, from which the mail will be sent, or the name of the mail program.
- **port** – port number (port 25 by default).

E.g., the line can look as follows:
smtp:localhost:25 or **lmtp:(local.mail -l)**

- For Sendmail:

```
ForwardMailer=smtp: (/usr/sbin/sendmail -bs \  
-C /etc/mail/sendmail.cf)
```

- For Qmail:

```
ForwardMailer=qmail: (/var/qmail/bin/qmail-queue)
```

- For Postfix:

```
ForwardMailer=smtp:localhost:10026
```

- For Exim:

```
ForwardMailer=smtp: (exim -bs \  
-C/etc/exim/exim.conf)
```

- For the group of users specify the following settings in the **[smtpscan.group:default]** section of the configuration file:

```
AdminAddress=<e-mail_address>  
AdminNotify=yes
```

- In the **[smtpscan.limits]** section set the maximum scanning duration (in seconds), e.g.:

```
MaxCheckTime=60
```

CHAPTER 5. WORKING WITH KASPERSKY ANTI-VIRUS

With Kaspersky Anti-Virus you can organize complete antiviral protection of your server from a file stored on the server for incoming and outgoing mail traffic, including mail collected from external mail services.

Kaspersky Anti-Virus allows administrators to create management tasks for the application. The tasks can be divided into three groups:

1. Update of the anti-virus databases used to scan for viruses and clean any infected objects.
2. Antiviral protection of the server's mail traffic.
3. Antiviral protection of the server's file systems.

Each of these groups consists of more specific tasks that use particular functions of the application. Further we shall discuss the most typical tasks, their configuration and launch from the command line.

Before running tasks dealing with anti-virus scanning of mail, the *aveserver* process must be launched if it was not started when the operating system booted.

5.1. Updating Kaspersky Anti-Virus databases

The application's *keepup2date* component performs the essential function of maintaining the current status of the anti-virus databases, which are used by Kaspersky Anti-Virus while scanning for, and cleaning, infected objects. They can be downloaded from Kaspersky Lab's update servers, at these addresses:

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

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

<ftp://downloads1.kaspersky-labs.com/updates/> , and other servers.

A full list of addresses from which updates can be downloaded, can be found in the *updcfg.xml* file included in the application package. The list will be updated automatically on a regular basis.

Manual editing of the *updcfg.xml* file is not allowed!

During the updating procedure the *keepup2date* component accesses the list of servers in this file, selects a server and attempts to download the anti-virus databases from it. If the attempt to use the server for updating fails, *keepup2date* repeats the process using the next address. After a successful update the application restarts automatically by default (**PostUpdateCmd** parameter in the **[updater.options]** section).

All settings for the *keepup2date* component are stored in the **[updater.*]** sections of the configuration file.

If the structure of your LAN is rather complicated, you are advised to download the anti-virus database updates to a network directory and configure other network computers to copy the updates from that directory.

We strongly recommend that you update the anti-virus databases every hour!

The updating procedure can be scheduled using the **cron** service (see section 5.1.2 on page 30), or the administrator may choose to run it manually from the command line (see section 5.1.3 on page 30).

5.1.1. Database update from Kaspersky Lab servers

The anti-virus databases can be updated from several sources.

To configure the program to download updates from one of Kaspersky Lab servers listed in a special file:

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

To configure the program to download updates from a user-defined server and terminate updating if this server cannot be accessed:

Assign the **yes** values to the **UseUpdateServerUrl** and **UseUpdateServerUrlOnly** parameters in the **[updater.options]** section. Besides, the **UpdateServerUrl** parameter should contain the updates' server address.

*To configure the program to download updates from a user-defined server and, if that server is unavailable, try to update from servers listed in the *keepup2date* component's file:*

Assign the **yes** value to the **UseUpdateServerUrl** parameter in the **[updater.options]** section; the **UseUpdateServerUrlOnly** parameter should be assigned the **no** value. Besides, the **UpdateServerUrl** parameter should contain the updates' server address.

5.1.2. Scheduling anti-virus database updates using cron

You can schedule regular automatic anti-virus database updates using the **cron** service.

Task: set up automatic daily anti-virus database updating scheduled to run every 3 hours. An update server should be selected randomly. The *aveserver* process must be automatically restarted after the database update. Only update errors should be recorded in the system log. Keep a general log of all runs of the task. Output no information to the console.

Solution: in order to accomplish the task, do the following:

1. Define the appropriate values in the application configuration file, e.g.:

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

2. Run the following command

```
# crontab -e
```

and modify the file, which defines rules for the **cron** daemon, adding the following line:

```
0 */3 * * * /opt/kav/5.5/kav4mailservers/bin/keepup2date
```

5.1.3. Manual updating of the anti-virus databases

An update of Kaspersky Anti-Virus databases can be initiated from the command line at any time.

Example

Start the update procedure for the anti-virus databases and report the results in the */tmp/updatesreport.log* file.

To perform the task, you should launch the *keepup2date* component from the command line as follows:

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

5.1.4. Creating and using a local source of updates

To ensure that updates to the anti-virus databases are distributed correctly from a shared network directory in your LAN to local computers, the structure within the network directory must be identical to the structure of Kaspersky Lab's update servers.

Example:

Create a network directory to be used as a source of updates by LAN computers. To accomplish the task, perform the following steps:

1. Create a local directory.
2. Launch the *keepup2date* component:

```
# keepup2date -u rdir
```

where *rdir* stands for a complete path to the created directory.
3. Grant computers on the LAN network access to that directory.

Downloading of updates from a network directory is only supported in Kaspersky Lab applications of versions 5.0 and 5.5.

If you need to update anti-virus databases on several computers, you can configure distribution of updates from a network directory. Such approach allows you to avoid multiple downloads of the same databases from the Internet. Instead, you can download them once to a public directory which other computers will use then as a source.

Example:

Configure updating of the anti-virus databases from the **/mnt/bases** local directory. If the directory is inaccessible or empty, the databases should be updated from Kaspersky Lab servers. Updater operation results must be recorded to the event log.

To accomplish the task, you should perform the following steps:

1. Define the following settings in the configuration file:

```
[updater.options]
UpdateServerUrl=/mnt/bases
UseUpdateServerUrl=yes
UseUpdateServerUrlOnly=no
(or use the -g /mnt/bases option)
```

2. Launch the *keepup2date* component as follows:

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

5.1.5. Updating the anti-virus databases via a proxy server

Example:

Set up updating of the anti-virus databases through a proxy server.

To accomplish the task, you should perform the following steps:

2. Assign the value **yes** to the **UseProxy** parameter in the **[updater.options]** section of the configuration file.
3. Ensure that the **ProxyAddress** parameter in the **[updater.options]** section of the configuration file contains a valid 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 obligatory while **username** and **password** have to be specified only in cases, when the proxy requires authentication.

or:

1. Assign the value **yes** to the **UseProxy** parameter in the **[updater.options]** section of the configuration file.
2. Specify the **http_proxy** environment variable in the following format: **http://username:password@ip_address:port**. This variable will be taken into account only if the **UseProxy** parameter in the **[updater.options]** section is either missing or set to **yes**.

5.2. Antiviral protection of the server's mail traffic

Anti-virus filtering of mail traffic, either incoming, outgoing, or in transit, is the chief task of Kaspersky Anti-Virus. It is implemented by the *smtpscanner* component.

This component protects users against infected mail messages, and delivers clean and disinfected messages to them with notifications regarding every message check-up.

The option of additional filtering according to the type of the attachment makes it possible to decrease the server load during mail traffic processing.

All the settings of the *smtpscanner* component are grouped in the [smtpscanner.*] sections of the *kav4mailservers.conf* configuration file.

The most typical tasks for antiviral protection of mail traffic are reviewed in the following sections.

Please keep in mind that the *aveserver* process must be running to enable anti-virus scanning of mail traffic.

5.2.1. Delivering clean and disinfected messages

This method of configuring Kaspersky Anti-Virus is used when you do not intend to divide the users into groups of senders and recipients. This is convenient, for example, when you need to deliver only clean and disinfected mail messages for all server accounts.

Example:

Task:

- Scan the entire mail traffic of the server for viruses and clean all infected messages.
- Delete infected messages that cannot be cleaned.
- Deliver disinfected messages to the recipients.
- Notify senders, recipients, and administrators about disinfected, deleted, suspicious, and corrupted messages, as well as messages that cannot be checked. Attach unchanged infected objects to the administrator's notifications.
- Record all actions in the */tmp/report.log* file.

Solution: to accomplish the task:

1. Set the following parameters for the **default** group:

```
[smtpscanner.group:default]
Check=yes
AdminAddress=<e-mail_address>
AdminNotify=yes
```

```
AdminAction=unchanged
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=yes
RecipientAction=remove
CuredRecipientNotify=yes
CuredRecipientAttachReport=yes
CuredRecipientAction=cured
```

Please refer to section 6.1.3 on page 52 for detailed description of actions over messages.

The `Sender*`, `Recipient*` and `Admin*` parameters define the rules for processing all object types except for objects with the status `Clear`. Any rules set for a certain object have higher priority. Thus, in this example all the object types will be removed from the recipient's mails (`RecipientAction=remove`), except for the `Cured` object (`CuredRecipientAction=cured`).

2. Configure logging of the component work results to the `/tmp/report.log` file:

```
[smtpscan.report]
ShowOk=yes
ReportFileName=/tmp/report.log
ReportFilePermission=0660
```

5.2.2. Delivery of all messages

In some situations, all messages must be delivered to a certain user group, including infected ones.

Example:

Task:

- Scan all mail traffic for viruses.
- Clean any infected messages for all users except for those included in the **urgent** group.
- Move mail messages that fail to be disinfected, as well as suspicious and corrupted mails, to the Quarantine directory for all users except those included in the **urgent** group.
- Notify senders, recipients, and administrators about blocked, disinfected, deleted, suspicious and corrupted messages, as well as about messages that fail to be checked. Attach unchanged infected objects to the administrator's notifications.
- Deliver all messages, including infected ones, to the recipients in the **urgent** group, with obligatory notification about possible virus infection.

To accomplish the task:

1. Specify the following configuration settings for the **default** group:

```
[smtpscan.group:default]
Check=yes
QuarantinePath=/var/db/Quarantine
Quarantine=yes
InfectedQuarantine=yes
SuspiciousQuarantine=yes
CorruptedQuarantine=yes
ErrorQuarantine=yes
ProtectedQuarantine=yes
AdminAddress=<e-mail_address>
AdminNotify=yes
AdminAction=unchanged
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=yes
RecipientAction=remove
CuredRecipientNotify=yes
CuredRecipientAttachReport=yes
CuredRecipientAction=cured
```

Please refer to section 6.1.3 on page 52 for detailed description of actions over messages.

2. Set the **urgent** group configuration in the following way:

```
[smtpscan.group:urgent]
Check=yes
Quarantine=no
AdminAddress=<e-mail_address>
AdminNotify=yes
AdminAction=unchanged
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=yes
RecipientAction=unchanged
```

5.2.3. Delivery of messages containing password-protected archives

E-mail messages quite frequently contain an attachment including a password-protected archive. Kaspersky Anti-Virus does not cure infected files inside password-protected archives. Therefore by default the application delivers messages with password-protected archives without scanning. In such cases, the Anti-Virus generates a message notifying that the archive has not been scanned. By default, the notification is delivered to message recipient and the administrator.

To disable notification about delivery of an unchecked archive:

- Assign **no** to the **ProtectedRecipientAttachReport** parameter in the **[smtpscan.group:default]** section of the application configuration file. That will disable delivery of notifications to recipients.
- Assign **no** to the **ProtectedAdminNotify** parameter in the **[smtpscan.group:default]** of the application configuration file. That will disable delivery of notifications to group administrator.

5.2.4. Blocking message delivery

Usually, the administrator has to block the delivery of some messages.

One such situation is when a mail message containing important data is suspected of being infected by a virus. The data might get lost during disinfection. In this situation the mail message should be isolated and, for example, sent to Kaspersky Lab's experts for analysis.

Task:

- Scan the entire mail traffic of the server for viruses and clean all infected messages.
- Block the delivery of infected, suspicious, corrupted, and password-protected messages, as well as those that cannot be scanned.
- Deliver only clean or disinfected messages to the recipients.
- Notify senders, recipients, and administrators about blocked, disinfected, deleted, suspicious, and corrupted messages, as well as about messages that cannot be checked. Attach unchanged infected objects to the administrator's notifications.

Solution: to accomplish the task:

Define the following settings in the *kav4mailservers.conf* configuration file:

```
[smtpscan.group:default]
Check=yes
QuarantinePath=/var/db/Quarantine
Quarantine=yes
InfectedQuarantine=yes
SuspiciousQuarantine=yes
CorruptedQuarantine=yes
ErrorQuarantine=yes
ProtectedQuarantine=yes
AdminAddress=<e-mail_address>
AdminNotify=yes
AdminAction=unchanged
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=yes
RecipientAction=remove
CuredRecipientNotify=yes
CuredRecipientAttachReport=yes
CuredRecipientAction=cured
```

Please refer to section 6.1.3 on page 52 for detailed description of actions over messages.

5.2.5. Complementary filtration of messages by attachment types

Quite often, mail messages have attachments that have a serious chance of containing a virus (e.g., .exe files). In order to prevent infection experts at Kaspersky Lab recommend filtering mail traffic by the name and/or type of such objects, and relocate the attachments to a separate directory for further analysis.

Task:

- For the **users** group:
 - Scan the group's mail messages for viruses.
 - Filter out any .exe files attached to mail messages. Quarantine these separated files.
 - Clean any infected mail messages. If the attempt to disinfect an object fails, delete it from the message, but deliver it unchanged to the group administrator.
 - Notify the group administrator and the recipients about quarantined objects.
 - Notify the administrator, the senders, and the recipients about deleted, infected, corrupted, and password-protected objects, and about messages that cannot be scanned.
- For all other recipients:
 - Scan all mail traffic for viruses, and clean all infected messages.
 - Quarantine infected messages that cannot be cured, suspicious and corrupted messages and objects, and any objects that fail to be scanned.
 - Deliver disinfected messages to the recipients.
 - Deliver password-protected files to the recipients with notification regarding their possible virus infection.
 - Notify the senders, the recipients, and the administrator about deleted, infected, corrupted, and quarantined messages, and about messages that cannot be scanned. Attach unchanged objects of all types to the administrator's notifications.

In order to accomplish the task, do the following:

1. Define the following configuration settings for the **users** group:

```
[smtpscan.group:users]
Check=yes
QuarantinePath=/var/db/Quarantine
Quarantine=yes
AdminAddress=<e-mail_address>
AdminNotify=yes
AdminAction=unchanged
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=yes
RecipientAction=remove
FilterByName=.*\.exe$
FilteredQuarantine=yes
FilteredRecipientNotify=yes
CuredRecipientNotify=yes
CuredRecipientAttachReport=yes
CuredRecipientAction=cured
ProtectedRecipientNotify=yes
ProtectedRecipientAction=unchanged
ProtectedRecipientAttachReport=no
ProtectedSenderNotify=no
ProtectedAdminNotify=no
```

Please refer to section 6.1.3 on page 52 for detailed description of actions over messages.

2. Define the following configuration settings for the **default** group:

```
Check=yes
QuarantinePath=/var/db/Quarantine
Quarantine=yes
InfectedQuarantine=yes
SuspiciousQuarantine=yes
CorruptedQuarantine=yes
ErrorQuarantine=yes
AdminAddress=<e-mail_address>
```

```
AdminNotify=yes
AdminAction=unchanged
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=no
RecipientAction=remove
ProtectedRecipientNotify=yes
ProtectedRecipientAttachReport=yes
ProtectedRecipientAction=unchanged
CuredRecipientNotify=yes
CuredRecipientAttachReport=yes
CuredRecipientAction=cured
```

Please refer to section 6.1.1 on page 50 for details regarding creation of the list of user groups.

5.3. Anti-virus protection of file systems

Server file systems are protected against viruses by the *kavscanner* component which scans server files for viruses, and processes infected and/or suspicious objects in accordance with the defined settings. The processing may be either purely informational (information sent to an event log and the server console, or to the administrator), or it may modify the object (disinfection, relocation to quarantine, or removal).

All the settings of the *kavscanner* component are grouped in the [scanner.*] sections of the *kav4mailservers.conf* configuration file.

Single on-demand scan of your server file systems may be invoked from the command line or scheduled using the standard **cron** service. The range of the file system to be scanned can be specified, from the whole file system or down to individual directories or files.

Scanning a whole server for viruses is a resource-consuming task. Please keep in mind that while it is running, the server's overall performance drops, and therefore running any other processes at the same time is not recommended. To avoid these problems, you are advised to scan individual directories instead.

5.3.1. On-demand scanning

Kaspersky Anti-Virus enables scanning for, and disinfection of, files in a specified server directory.

Task: start recursively scanning of the `/tmp` directory, automatically disinfecting all infected objects. Objects which cannot be disinfecting are to be deleted.

The results of component activity (start date, detailed information about all files except for those containing no viruses) are to be stored in a log file `kavscanner-<current_date>.log` in the same directory.

Solution: in order to accomplish the task you should start the `kavscanner` component in the command line as follows:

```
# kavscanner -Rlq -okavscanner-`date +%F`.log -i3\ -  
ePASBME -j3 -mCn /tmp
```

If the scanning procedure reveals an infected object inside an archive, the whole archive will be deleted!

5.3.2. Scheduled directory scans using cron

The standard Unix scheduling `cron` service can be used for regular scanning of a specified directory.

Task: schedule daily scanning for virus presence to start at 0 hrs. 00 min. in the `/home` directory, using scanning parameters defined in the `/etc/kav/kavscanner.conf` configuration file.

Solution: to accomplish the task, perform the following steps:

1. Create the `/etc/kav/kavscanner.cron` configuration file with all the required scanning parameters.
2. Run the following command

```
crontab -e
```

and modify the file which sets the tasks for `cron` daemon adding to it the following line:

```
0 0 * * */opt/kav/5.5/kav4mailservers/bin\  
/kavscanner -c /etc/kav/kavscaner.conf /home
```

5.3.3. Advanced options: using scripts

Kaspersky Anti-Virus enables additional processing of objects which have passed through anti-virus analysis, by using standard Unix/Linux commands and scripts. These tools allow experienced administrators to extend the functionality of Kaspersky Anti-Virus by defining different actions to be applied to objects of different status.

5.3.3.1. Cleaning infected archives

Disinfection of archives requires the presence of installed archivers for operations with them.

Kaspersky Anti-Virus does not perform disinfection of compressed infected files; it just discovers suspicious and infected objects inside archives. However, this capability can be implemented using an additional script. Please see below an example illustrating disinfection of *tar*, *rar*, *tgz* and *zip* archives using the *vox.sh* script, which is included in the distribution package of Kaspersky Anti-Virus.

Task: scan all *tar* and *zip* archives accessible on a server and attempt disinfection of all the infected objects they contain using the *vox.sh* script. Use */etc/kav/kavscanner.conf.in* as a configuration file, where script use for disinfection of archives should be specified prior to the scanning procedure.

List all infected objects with their full paths in the */tmp/infected_archive.lst* file. Store a report of the component's activity in the */tmp/logfile.log* file.

Solution: in order to accomplish the task, do the following:

1. Create an alternative *kavscanner.conf.in* file.
2. Define the rules for processing infected objects in the **[scanner.container]** section of that file:

```
OnInfected=exec /opt/kav/5.5/kav4mailservers\  
/contrib/vox.sh %FULLPATH%/%FILENAME%
```

3. Run the *kavscanner* component as follows:

```
# kavscanner -c kavscanner.conf.in -ePASE -qR\  
-o /tmp/logfile.log -j3\  
-pi/tmp/infected_archive.lst /
```

5.3.3.2. E-mail notification of administrator

Standard Unix/Linux tools can be configured to notify the administrator about infected, suspicious or corrupted files discovered within server file systems.

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

Solution: in order to accomplish the task, do the following:

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

```
[scanner.object]
OnInfected=exec echo %FULLPATH%/FILENAME% is\
infected by %VIRUSNAME% | mail -s kavscanner\
admin@<e-mail_address>

[scanner.container]
OnInfected=exec echo archive %FULLPATH%/FILENAME%\
is infected, viruses list is in the attached file\
%LIST% | mail -s kavscanner -a %LIST% \
admin@<e-mail_address>
```

5.3.4. Moving objects to Quarantine

Kaspersky Anti-Virus can be configured to move all infected objects found within the server's file system to Quarantine.

Such an approach can be used, for example, if during the antiviral scanning of a directory an infected file containing important data is detected. Since part of the data may get lost during disinfection, an appropriate approach may be to isolate the infected object in Quarantine for subsequent sending to Kaspersky Lab for analysis. Suspicious objects should be quarantined, too.

If you intend to keep the Quarantine directory within the server's file system, we advise that you exclude it from the target area for subsequent scans by specifying its full path in the **ExcludeDir** parameter of the application configuration file. Quarantined files are stored in encrypted form being thus unable to harm the computer file system.

Task: scan all the objects listed in the */tmp/download.lst* file, moving any infected objects with their full paths to the */tmp/infected* directory. Use heuristic code analysis. Disable recursive scanning. Record information about infected, suspicious, and corrupted objects to the event log.

Solution: in order to accomplish the task, do the following:

1. Define the following actions to be performed on infected objects in the **[scanner.object]** and **[scanner.container]** sections of the configuration file:

```
OnInfected=movePath /tmp/infected
```

2. Disable the disinfection mode (**Cure=no**) if it was enabled.
3. Run the *kavscanner* component as follows:

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

Please refer to section 6.2.3 on page 58 for details on actions over files.

In order to define several actions in a rule for processing of infected objects, enumerate them using the «;» character as a separator (please see the example below).

Example:

Access to the files within the */tmp/infected* directory must be restricted to their reading and writing.

The task should be accomplished using standard Unix tools (**chown** and **chmod** commands). Modify the rule for processing of infected objects in the **[scanner.object]** and **[scanner.container]** sections (please see above) of the configuration file as follows:

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

5.3.5. Backup of processed objects

If infected files are automatically deleted as the default action for infected files, valuable data may be lost. Data are also at risk during disinfection. To avoid this, Kaspersky Anti-Virus offers the option to copy infected files to a backup storage directory.

Prior to an object's disinfection or removal, the application can be configured to automatically copy it to the backup storage directory, specified by the **BackupPath** parameter in the **[scanner.path]** section. It allows you to preserve a backup copy (and restore the original file, if necessary) if a file gets damaged during disinfection. Files are stored in an encrypted form. Subsequent recording of the same file to backup storage automatically replaces its earlier copy with a newer one.

By default the backup mode is off and the path to the for backup storage directory is not defined. The path must be specified in the configuration file to enable backup mode.

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

5.4. Product key management

A product key entitles you to use the application and also contains data pertaining to the purchased product, such as key type, expiration date, the number of protected users or protected traffic volume (depending on the key type), information about the distributors, etc.

During the period of key validity you are entitled to the following services:

- twenty-four-hour technical support;
- hourly updates of anti-virus databases;
- application updates (patches);
- new application versions (upgrades);
- timely notifications about new viruses.

When the key expires, these services are discontinued automatically. Kaspersky Anti-Virus will continue scanning server file systems and mail traffic but it will use only the anti-virus databases which were current when the license expired, as the function of anti-virus database updating will become unavailable. The administrators will be notified about the expiry of the license.

It is essential therefore to review regularly the information in the key and control the date of its expiration.

5.4.1. Licensing mechanism

Kaspersky Anti-Virus 5.5 uses a new licensing technology. During installation on a server the administrator has to specify a list of domains for which the application should protect the e-mail. Licenses may be issued:

- for a certain volume of scanned traffic,
- for a certain number of protected user accounts.

In the first case the licensed traffic will include the total amount of messages which the application received, scanned and assigned the **Clean** status to (i.e. contained no viruses).

In the second case the application will view as a licensed user any sender and/or recipient of an uninfected message scanned by the application.

The application will notify the administrator 14 days before the key expires. The notification will be sent once every 24 hours and during each application restart.

An identical notification mechanism is provided for cases of key expiry, and when email traffic exceeds the licensed traffic volume.

However, if the traffic volume exceeds the licensed volume by more than 10 percent, a corresponding notification will be sent to the administrator each time the application detects a message with a status other than **Clean**.

Correct functioning of the licensing mechanism requires the following actions:

Define the **LicenseDomain** parameter in the **[smtpscan.license]** section. The parameter determines the masks of protected domains. The value of the parameter must include all mail domains protected by Kaspersky Anti-Virus. Domain names must be specified in POSIX regexp format, listed in a single line, delimited with commas.

Please note that the "." character has its own meaning in POSIX regexp format, so it should be entered after "\" characters.

5.4.2. Viewing the product key information

Information about installed license keys can be reviewed in the event logs produced by the *kavscanner*, *kavmonitor* and *keepup2date* components, since each of them loads the information from the keys when they are launched.

Moreover, Kaspersky Anti-Virus contains a special *licensemanager* component, which allows you to review more detailed information about the keys together with some analytical data.

For example, if you have purchased Kaspersky Anti-Virus with a license based on the MAIL TRAFFIC VOLUME, the *licensemanager* component will enable you to keep track of used traffic volume and will inform you about the amount (in Mb) of licensed mail traffic currently remaining.

You can also view information about the amount of traffic processed during the day (by hours) and thus see when the load reaches its maximum. This information may be useful if, for example, you experience any problem with the application and wish to consult technical support.

If you purchased the application with a license based on the NUMBER OF USERS, you can view the total number of purchased product keys.

All of the above information can be output to the server's console.

In order to review information about all product keys, run the licensemanager component using the command line:

```
# licensemanager -s
```

The component will return information about installed keys, similar to the following:

```
Kaspersky license manager Version 5.5
Copyright (C) Kaspersky Lab. 1998-2005.
License file 0003D3EA.key, serial 0038-000419-
0003D3EA, "Kaspersky Anti-Virus for Unix Mail
Server", expires 04-07-2003 in 28 days
License file 0003E3E8.key, serial 011E-000413-
0003E3E8, "Kaspersky Anti-Virus for Unix Mail Server
 (license per e-mail address)", expires 25-01-2004 in
 234 days
```

In order to review the information about a specific license key, launch the `licensemanager` component indicating the key file name by entering, for example, the following in the command line:

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

Information similar to the following will be output to the console:

```
Kaspersky license manager Version 5.5
Copyright (C) Kaspersky Lab. 1998-2005.
Serial 0038-000419-0003D3EA, "Kaspersky Anti-Virus
for Unix Mail Server", expires 04-07-2003 in 28 days
```

In order to view information regarding licensed mail traffic or the number of protected users, launch the `licensemanager` component with the `-i` option in the command line:

```
licensemanager -i
```

Information similar to the following will be output:

- If the license is based on the **NUMBER OF USERS**:

```
Kaspersky license manager for Linux. Version
5.5.0/RELEASE #68
Copyright (C) Kaspersky Lab, 1997-2005.
Portions Copyright (C) Lan Crypto

License users units: 5
Users units used: 0
Users units left: 5
```

- If the license is based on the **MAIL TRAFFIC VOLUME**:

```
Kaspersky license manager Version 5.5
```

```
Copyright (C) Kaspersky Lab. 1998-2005.  
Daily traffic statistic(Bytes):  
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0  
License traffic units: 10 (MB)  
Traffic units used: 0 (MB)  
Traffic units left: 10 (MB)
```

5.4.3. Key validity extension

Extension of your key for Kaspersky Anti-Virus extends or restores complete application functionality, including additional services listed in section 5.3.5 on page 44.

In order to extend the validity of your key for Kaspersky Anti-Virus you'll need to:

contact the company from which you purchased the application and acquire an extension for your Kaspersky Anti-Virus key.

or:

extend the key validity directly through Kaspersky Lab by sending an email message to the Sales Department (sales@kaspersky.com), or fill in the appropriate form at the **E-Store** → **Renew Your License** section of our site (www.kaspersky.com). After payment you will receive a product key sent to the e-mail address indicated in your order form.

The new key must be installed. To do so, copy it to the directory assigned for keys storage, and specified by the **LicensePath** parameter of in the **[path]** section of the configuration file, and restart the server.

After this, you are advised to update your anti-virus databases (see section 5.1 on page 28).

CHAPTER 6. ADVANCED SETTINGS

This section describes some advanced settings of Kaspersky Anti-Virus. Unlike the required settings made during installation process (see Chapter 4 on page 20), without which the product cannot be used, advanced settings are used at the administrator's discretion to extend the application's functionality and tailor it to fulfill particular business needs.

Kaspersky Anti-Virus performs anti-virus scanning based on its settings in the `kav4mailservers.conf` configuration file. You can edit the file.

6.1. Setting up antiviral protection of mail traffic

When scanning mail traffic for viruses, the main criteria used to select rules for processing mail messages are the sender's and the recipient's addresses, and the parameters of the group they are part of. Therefore, it is of utmost importance that the addresses are placed in the proper groups.

Whether or not a message belongs to a certain group is determined by the presence of both the sender's and the recipient's address in that group. The program looks through the group's address list and searches for both addresses. When the combination of these two addresses (sender-recipient) is detected in the group under analysis, the message is processed according to the rules for this group.

*The presence of a line with the address of a message in the group is checked according to **POSIX regex**.*

By default, the configuration file includes the **[smtpscan.group:default]** group, which defines the rules of processing mail messages. Since the group initially contains no names of senders or recipients, the rules described in it are applied to all messages. You can change the parameters of the **default** group or create new groups.

If other groups have been added to the configuration file (see section 6.1.1 on page 50), the sequence of mail message processing will be as follows:

- The program checks if the sender and recipient addresses belong to the groups defined by the administrator. If the message addresses belong to an existing group, this message will be processed according to the rules of that group.

- If the addresses of the sender and the recipient of the processed message fall into several groups, the program will use the parameters of the first one.
- If these addresses are not part of any address group defined by the administrator, then the message will be processed according to the rules specified in the **default** group.

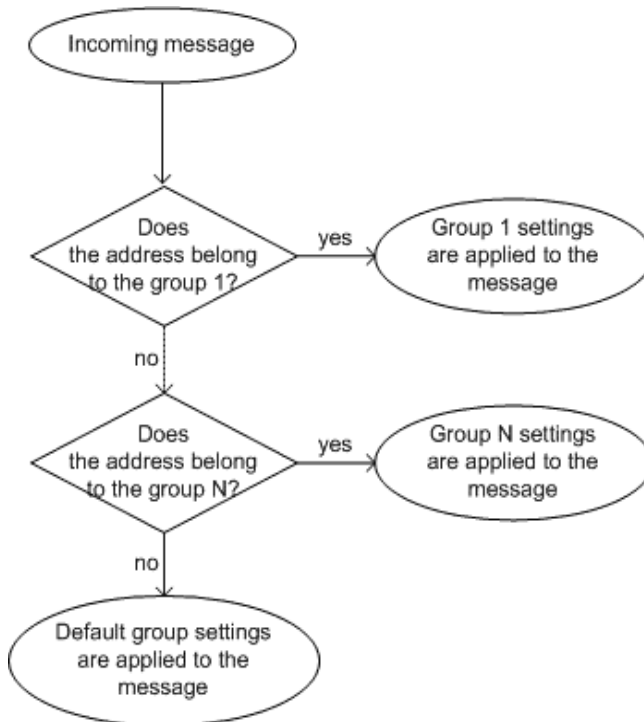


Figure 4. Mail message processing

6.1.1. Forming user groups

By default, the configuration file of Kaspersky Anti-Virus contains the **[smtpscan.group:default]** group including all the server's senders and recipients. It uses the following rules for mail message processing:

- Check all messages.
- Clean all infected files that are detected.

- Deliver only clean and disinfected mail messages.
- Messages that fail to be disinfected, as well as suspicious, corrupted, or password-protected messages and those that cannot be scanned shall only be delivered to the group administrator.
- Notify the senders, the recipients, and the group administrator about infected, cleaned, suspicious, corrupted, and password-protected messages and those that cannot be scanned.

If you want Kaspersky Anti-Virus to process mail messages for different senders and recipients using different rules, you will have to create groups for them.

In order to create a new group,

1. In the configuration file create section **[smtpscan.group:<group_name>]**.
2. Define the addresses, or address masks, of the recipients and senders to be included in the group. To do so, list them as the values of the **Senders** and **Recipients** parameters, delimited by commas.

The **POSIX regex** standard is used to specify masks.

If you do not define the value of either **Recipients** OR **Senders** parameter it will be automatically set as **.*@.*** (all addresses).

In version 5.5 of Kaspersky Anti-Virus the **kavadministrators** group has been introduced into the configuration file. During application setup, the installer automatically adds to the group all addresses of administrators listed in the **/var/qmail/alias/postmaster** directory.

In cases when an administrator address is modified later (e.g., **AdminAddress** parameter in the **[smtpscan.group:default]** or another group), the new administrator address, and all other addresses using it as an alias, must be added to the list of values for the **Recipients** parameter of the **[smtpscan.group:kavadministrators]** group.

The procedure is important if the system is set up to deliver infected e-mail messages to the administrator,

6.1.2. Message check and disinfection mode

To scan the mail traffic of a certain group of senders and recipients for viruses, the server's administrator must enable the appropriate mode in the group's parameters.

To do so, set the parameter **Check=yes** in the *kav4mailservers.conf* configuration file for the respective group.

When Check mode is enabled, all mail messages attributed to the group by the criterion of sender/recipient are scanned by Kaspersky Anti-Virus for viruses. However, infected mail messages will not be cleaned.

To *ENABLE THE CURE MODE* for infected messages it is necessary to specify in the group at least one parameter for disinfected (**Cured**) objects. For example, if you specify:

```
[smtpscan.group:account]
Check=yes
CuredRecipientNotify=yes
```

there will be these results:

- All mail messages for senders and recipients included in the **account** group will be checked for viruses.
- Any infected objects that are detected will be cleaned.
- The recipients will receive appropriate notifications regarding the disinfected objects.

6.1.3. Actions on objects

The following aspects determine the actions to be taken with mail messages:

- Object's status assigned after scanning (see section 6.2.2 on page 57).
- The action specified for a certain object status in the configuration file.

An object is assigned its status by the *aveserver* process immediately after it is scanned for viruses. The action to be applied to the object after scanning is set by the server's administrator.

Kaspersky Anti-Virus® allows actions to be specified for mail message objects that are delivered to the recipients and the group administrator. For message senders, ONLY notifications can be sent.

The following actions can be specified for mail message objects:

- **Remove** – remove object from the message.
- **Unchanged** – leave the object unchanged. In this case the object will not be cured and will be delivered in its original form.
- **Cured** –deliver only clean or disinfected objects.

You can specify *common actions* for all object types, or specify individual actions for each type.

To set common actions for all the object types,

Set the desired values for the parameters **AdminAction** and **RecipientAction**. These parameters define actions for all object types. E. g.:

```
AdminAction=unchanged
RecipientAction=remove
```

All attachments to mail messages for the group will be delivered to the administrator unchanged, but they will be removed from the recipients' messages.

To set individual actions for different types of objects,

Specify the desired actions as values for the parameters **<object_type>AdminAction** and **<object_type>RecipientAction**.

E. g.,

```
AdminAction=unchanged
RecipientAction=remove
CuredRecipientAction=cured
```

In this case, all mail messages, irrespectively of the object type, will be delivered to the group administrator unchanged, while the recipient will only receive disinfected messages. All other types of objects will be removed from mail messages.

Besides the above actions, application can **move objects to the Quarantine directory**.

To move objects from a mail message to the Quarantine directory,

Define the following parameters in the group configuration file:

```
QuarantinePath=/var/db/Quarantine
Quarantine=yes
SuspiciousQuarantine=yes
CorruptedQuarantine=yes
ErrorQuarantine=yes
```

6.1.4. Notifying senders, recipients, and administrators

Kaspersky Anti-Virus allows delivery of notifications for mail message senders, recipients and group administrators regarding objects of all statuses (suspicious, infected, cleaned, corrupted etc.) Sending of notifications is regulated by the following configuration parameters:

- **RecipientNotify** – notification to the recipient of the mail message.
- **SenderNotify** – notification to the sender of the mail message.
- **AdminNotify** – notification to the group administrator.

The above parameters define how notifications are sent about objects of any status. To set notifications to be sent for objects with specific statuses, enable the following modes:

- **<object_status>RecipientNotify**
- **<object_status>SenderNotify**
- **<object_status>AdminNotify.**

In this case, notification will only be sent regarding the objects with the specified status.

For example, if you need the application to send notifications to the administrator and the sender regarding objects with any status, and to the recipient regarding only infected, cleaned, and corrupted objects, you should specify the following settings in the group:

```
InfectedRecipientNotify=yes
CuredRecipientNotify=yes
CorruptedRecipientNotify=yes
SenderNotify=yes
AdminNotify=yes
```

It is also necessary to specify the address they will be sent from (**NotifyFromAddress** parameter in the section [**smtpscan.general**]).

By default, Kaspersky Anti-Virus enables notifications for objects of any status. All these notifications contain a **general text** based on the */etc/kav/5.5/template_notify_main* template included in the distribution kit.

If you wish to edit the text of the notification you can either:

- Edit the text of the template supplied with the program.

- Create a new template file and specify the full path to it as the value of the **Template** parameter in the **[smtpscan.notify]** section.

In the text of the template you can use the following macros, which will be automatically replaced by the corresponding value depending on the status assigned to those objects after their anti-virus scanning:

- **%VERSION%** – version of Kaspersky Anti-Virus.
- **%SENDER%** – message sender address.
- **%RECIPIENT%** – list of all message recipients separated with line feed character.
- **%MSGID%** – message ID number.

%VIRUSNAME% – text description of the problem. You can translate this text into any language by entering the corresponding lines for every object status in the **[locale]** section.

%SUBJECT% – inserts the contents of the **Subject** field from the original e-mail message.

%DATETIME% – date and time the message was processed. The format of time and date representation can be edited too (see section 6.5 on page 62).

- **%HEADERS%** – original message headers.
- **%ACTION%** – description of actions performed over the attached message objects. The macro is used in all templates except for notifications to message senders. The following actions are possible:
 - `attachement not modified` – attachment remained unchanged.
 - `attachement cured` – attachment was infected and has been cured successfully.
 - `attachment removed` – attachment has been removed.
 - `attachments cured and removed` – some of the attachments have been cured and delivered to the recipient, some of them have been removed.

These macros can also be used to create message subjects.

The notification generation parameters (MIME type, message subject, codepage etc.) are grouped under the section **[smtpscan.notify]** of the configuration file.

6.2. Configuring anti-virus protection for server file systems

All the parameters for the protection for server's file systems can be subdivided into groups that determine:

- Scan area (see section 6.2.1 on page 56).
- File scanning and disinfection mode (see section 6.2.2 on page 57).
- Operations on files (see section 6.2.3 on page 58).
- Parameters for generation of the event log about application activity (see section 6.5 on page 62).

The following sections discuss each of each of these groups of settings in turn.

6.2.1. Scanning area

The scanning area may be conveniently subdivided into the following parts:

- The list of target directories and files for anti-virus scanning.
- The list of file types which will be scanned for the presence of viruses (archives, e-mail messages, etc.).

By default all accessible file system objects are scanned, beginning with the current directory.

Scanning the entire server file system requires to enter the root first or indicate scanning area in the command line.

The list of directories and files that must be scanned can be defined using the following methods:

- Enumerating directories and files with their absolute or relative (to the current directory) paths, separated by spaces in the command line, when the component starts.
- Defining scanning paths in a text file, with the subsequent command to use the file issued via the `-@ <file_name>` command line option. Each object in the file is listed on 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, the application will only process the objects listed in the file.

- Restricting default paths (both listed in the command line and in the text file), can be accomplished by entering masks for files and directories to be excluded from the scanning area, using the parameters **ExcludeMask** and **ExcludeDirs** in the **[scanner.options]** section of the *kav4mailservers.conf* configuration file.
- Disabling *recursive scanning of directories* (**[scanner.options]** section, parameter **Recursion** or **-r** key).
- Creating an alternative configuration file, with a subsequent command to use it issued via the **-c <file_name>** command line option when the component starts.

The default list of objects for scanning is also specified in the *kav4mailservers.conf* configuration file (**[scanner.options]** section) and can be redefined:

- by command line options when the component is started.
- when an alternative configuration file is used.

6.2.2. File scanning and disinfection mode

Disinfection of infected files revealed while scanning is an essential aspect of anti-virus protection.

The option to disinfect objects is disabled by default, which means that when scanning the application will only provide notification that viruses, suspicious or corrupted objects have been discovered, by sending a message to the console and to its event log (see section 6.5 on page 62).

As a result of the scanning procedure, each object is assigned one of the following status values:

- **Clean** – no viruses detected.
- **Infected** – the file is infected.
- **Warning** – the file code resembles a known virus.
- **Suspicious** – the file infection with an unknown virus is suspected.
- **Corrupted** – the file is damaged.
- **Protected** – the file is password-protected and cannot be scanned.

When disinfection mode is enabled (**[scanner.options]** section, parameter **Cure=yes**) only files with **Infected** status are sent for anti-virus processing. Following disinfection a file is assigned one of the following status values:

- **Cured** – the file has been successfully disinfected.

- **CureFailed** – file disinfection has failed. These files will be treated according to the rules defined for infected objects.

6.2.3. Operations on files

Certain actions may be applied to files depending upon their status assigned after anti-virus scanning (see section 6.2.2 on page 57). By default, the application only outputs notifications about detected files with a certain status to the console and records the information to its event log.

Some actions can be defined specifically for files with **Infected**, **Suspicious**, **Warning** or **Corrupted** status:

- *transfer to a specified directory* – relocation of files with a defined status to a specified directory, *regular* or *recursive transfer* is possible;
- *removal* of the file from the file system;
- *execution of a certain command* – processing of files using standard Unix commands, scripts, etc.

For **Protected** and **Cured** files the application just outputs its notifications to the console and to the event log.

Please note that Kaspersky Anti-Virus distinguishes between a simple object (file) and a compound object (containers consisting of several objects, e.g. archive). The actions to be performed on these two types of objects are also different, and are allocated separate sections in the configuration file. The **[scanner.object]** section is devoted to simple objects, and the section **[scanner.container]** is for to compound 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. These two separate operations on the archive are determined by parameters from different sections of the configuration file!

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

- Specify the actions in the application configuration file if they are to be used as default actions (**[scanner.object]** and **[scanner.container]** sections).
- Indicate the actions in an alternative configuration file and use it when the component starts.
- Define the actions for the current session using the command line options when the *kavscanner* component is started.

The syntax defining actions is similar for simple objects and containers.

6.2.4. Backup mode

This section examines the backup mode settings, using the task below as an example.

Task: scan for viruses all objects within the directories and files listed in */tmp/download.lst*, and disinfect them. If disinfection fails to relocate infected objects with their complete paths to the */tmp/infected* directory; move suspicious objects to */tmp/suspicious*; output notifications to */tmp/warning*.

Solution: to accomplish the task, you should do the following:

1. Create an alternative configuration file: *scan_sample.conf*.
2. Enable the disinfection mode for infected objects, if it has been disabled (**Cure=yes** in the **[scanner.options]** section).
3. Set the rules for processing of infected objects. To do so, add the following settings to the **[scanner.object]** and **[scanner.container]** sections of the *scan_sample.conf* configuration file:

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

4. Run the *kavscanner* component using the command line as follows:

```
# kavscanner -@ /tmp/downloads.lst -c \  
scan_simple.conf
```

6.3. Optimizing Kaspersky Anti-Virus

Kaspersky Anti-Virus offers several efficient methods for optimization of its operations.

These technologies are only employed while scanning objects within the server's file system. Their use is regulated by corresponding parameters in the **[scanner.options]** section of the application configuration file.

6.3.1. Using iChecker database

The application avoids scanning files anew each time they are accessed, by checking to see whether the file has changed since it was last scanned. The algorithm for object (file) scanning for virus presence is as follows:

- After initial scanning of any file the information about it (name, checksum) is appended to the common iChecker database, which includes information about scanned **clean** files of identified formats scanned by the *kavscanner* component.
- All subsequent user's accesses of a file force a search for the file name in the iChecker database first. File name is used as a search criterion. If the file is found in the iChecker database, its current condition will be compared with the data stored in the database. The file is considered to be unchanged, and is correspondingly not rescanned, if its current condition is completely identical to the stored information.

If no data can be found for the requested file in either the iChecker database or the cache, the file is scanned for viruses and the databases updated with the results.

6.3.2. Reducing the server load

Scanning server file systems may require considerable time if the data volume is large. If current tasks are also running at the same time, the server load may grow noticeably. As the server must be able to perform its usual tasks, so it is useful to suspend anti-virus scanning on a server when a certain load limit is exceeded.

In order to accomplish the goal, the **MaxLoadAvg** parameter has been added to the **[scanner.options]** section of the application configuration file. If the parameter value is specified, *kavscanner* checks the current server load value (*load average*) before scanning each new file. If the value exceeds the figure specified in the configuration file, the scanner will suspend its work until the **load average** value decreases to the specified threshold.

6.4. Configuring the *aveserver* process

Anti-virus processing of mail traffic is carried out by means of two components - *aveserver* and *smtpscanner* - interacting with each other.

Aveserver is launched during the operating system start-up. A connection with *aveserver* is established immediately when *smtpscanner* accesses this process.

The *aveserver* process is controlled by parameters in the **[aveserver.options]** section of the *kav4mailservers.conf* configuration file:

- **DetachFromTerminal** – the process is disconnected from the terminal immediately after startup. This mode should be enabled, since system boot will not proceed until the process disconnects. The mode is enabled by default (value is **yes**). The mode should only be disabled (value is **no**) when the process is controlled by a program such as **SVC**.
- **StartupMode** – enables switching of the process to the background mode provided that **DetachFromTerminal=yes**. The **fast** value means that the daemon switches to the background mode immediately after loading the configuration file, returning the code **0**. The **normal** value switches the process to the background mode only after loading the anti-virus databases and the license keys to memory.

The visual speed of launching the process in the fast mode is higher, but the possibility exists that the daemon will fail to load because of some fatal error, in which case nothing will be output to the console.

- **LocalSocketPermission** – the octonary permission with which the socket is created. By default, **LocalSocketPermission=0666**.

6.4.1. Aveserver reloading

The *aveserver* process is automatically reloaded immediately after the anti-virus databases are updated, if the appropriate setting is enabled in the configuration file.

The process is reloaded by the following command.

```
# kill -HUP <process_PID>
```

After its execution the process receives the **SIGHUP** signal, at which, the parent process reloads the configuration file, the product keys, and the databases or, if the path to the file is set incorrectly, terminates and leaves the corresponding message in the event log. All active connections of the process with client programs remain active until they are closed.

Such reloading of the *aveserver* process is necessary, for example, after you have edited the configuration file, added a new key, or manually updated the anti-virus databases.

6.4.2. Forced *aveserver* termination

If you need to force the termination of the *aveserver* process, use the following command:

```
# kill <process_PID>
```

The command will send the **SIGTERM** signal to the process. This signal will end the operation of *aveserver* and close all the copies it created.

We strongly recommend that you do not use the command `kill -9` to end the operation of the *aveserver* process. This command will indeed terminate the process, but will leave a number of temporary and work files that can only be deleted manually. Some applications (like Webmin) use these files to detect if the process is running or not.

6.5. Scanning of POP3 mail from external mailboxes

Nowadays, external mailboxes on web mail servers are widely used. Often mail is delivered from such servers by clients using POP3 while Kaspersky Anti-Virus only scans SMTP mail traffic. However, it is necessary to prevent infection while downloading e-mail from external e-mail services.

In order to ensure antiviral protection of external mail, the following configuration is required:

1. Disable the default POP3 port 110, and configure the gateway to function as a proxy server for POP3 using the **fetchmail** package. This package downloads mail messages from external servers and sends them to a mail system via SMTP. Then the messages are scanned by Kaspersky Anti-Virus.

Filtering mail from external mailboxes requires a local SMTP server and a local user account on the computer where the **fetchmail** package is installed.

Fetchmail is usually requires the following configuration: every user in the \$HOME directory has a file `.fetchmailrc`, containing at least the following lines:

```
set postmaster "user"  
set bouncemail  
set no spambounce
```

```
set properties ""
poll mail.that.is.free.ru with proto POP3
    user 'remote_user' there with password
    'pass12345' is 'user' here
poll mail2.that.is.free.ru with proto POP3
    user 'remote_user2' there with password
    'pass123452' is 'user' here
```

where:

- **user** is the user's name on the local network
- **mail.that.is.free.ru** and **mail2.that.is.free.ru** are names of the hosts from which we need to collect mail.
- **remote_user** and **remote_user2** are logins for the servers *mail.that.is.free.ru* and *mail2.that.is.free.ru*, respectively.
- **pass12345** and **pass123452** are passwords for the *remote_user* and *remote_user2* mail accounts.

With these settings, the **fetchmail** program will collect mail messages from the hosts *mail.that.is.free.ru* and *mail2.that.is.free.ru* and send them to the local SMTP for the *user*.

No fields (*From*, *To* or any other) will be altered in the messages, and only one more header *Received* will be added by **fetchmail**. Mail messages received by the user will look as if they were received in the usual way.

2. Configure the user's cron service, via crontab, to launch **fetchmail**, for example, every 10-15 minutes.

In order to automate the process of setting up the **fetchmail** program for other users who use external mailboxes, the following data is necessary:

- Name of the external host, from which **fetchmail** will collect mail messages.
- Login for the external host account.
- Password for the account.

In addition, in every user's home directory there must be a file *.fetchmailrc* with the following content:

```
set postmaster "user"
set bouncemail
set no spambounce
set properties ""
```

The following script file may be used for adding mailbox records:

```
#!/bin/bash
echo "poll $1 with proto POP3 " >>$HOME/.fetchmailrc
echo "user '$2' with password '$3' is '$4' \
here">>$HOME/.fetchmailrc
```

If you run this script file with the following parameters:

```
pop.mail.ru dan secret admin
```

then messages for the user *dan@mail.ru* will be forwarded to the address *admin@your_host.your_domain*.

6.6. Additional features for Postfix

Kaspersky Anti-Virus offers a number of additional features when used with Postfix e-mail system:

- Support for the DSN SMTP extension (RFC 3461, RFC 3885) (see section 6.6.1 on p. 64).
- Support for the 8bit-MIME SMTP extension (RFC 1652) (see section 6.6.2 on p. 65).
- Support for the X-Forward SMTP extension (see section 6.6.3 on p. 65).

These protocol extensions can be configured at the administrator's discretion.

6.6.1. DSN extension support

The `smtpscanner` component supports the DSN extension of the SMTP protocol. Support for this extension allows the component to preserve the parameters of a mail message assigned to the latter by an incoming e-mail system. `Smtpscanner` in that case does not analyze the parameters transferring them instead without modifications to a routing mail system.

In order to enable DSN support:

Define the following parameter in the `[smtpscan.general]` section of the application configuration file:

```
EHL0supportDSN=yes
```

Prior to enabling the option, make sure that the routing mail system supports the DSN extension.

6.6.2. 8bit-MIME extension support

The 8bit-MIME extension is frequently used when a mail system works with national encodings using SMTP because basic version of the protocol does not support transfer of messages in languages using non-ASCII characters. Therefore support for that extension has been added in Kaspersky Anti-Virus 5.5.

If your external mail system does not support the 8bit-MIME extension, Kaspersky Anti-Virus must be configured appropriately, too.

In order to enable 8bit-MIME support:

Define the following parameter in the **[smtpscan.general]** section of the application configuration file:

```
EHL0support8BITMIME=yes
```

Kaspersky Anti-Virus functions no matter whether the support for the 8bit-MIME is enabled or disabled.

6.6.3. X-Forward extension support

Kaspersky Anti-Virus features support for the X-Forward extension for Postfix.

In order to enable X-Forward support:

- Use the SMTP protocol in case of Anti-Virus integration with Postfix (refer to section 4.4.5 on p. 28 for details).
- Define the following parameters in the **[smtpscan.general]** section of the application configuration file:

```
EHL0supportXFORWARD=yes
```

```
EHL0attrsXFORWARD=NAME ADDR PROTO HELO
```

6.6.4. Incoming SMTP support in smtpscanner

The smtpscanner component can receive incoming traffic using LMTP or SMTP.

In order to enable SMTP support in smtpscanner, perform the following actions:

- Assign the **smtp** value to the **Protocol** parameter in the **[smtpscan.general]** section of the application configuration file.

- Change the protocol value from lmtpt to smtp under the smtp service in Postfix configuration file (*master.cf*).
- Restart the mail system.

6.7. Localization of displayed date and time format

While working, Kaspersky Anti-Virus compiles reports for each of its components, and notifications for users and administrators which are always supplemented with the date and time at which they occurred.

By default, Kaspersky Anti-Virus uses time and date formats conforming to those used by the C function `strftime`:

- `%H:%M:%S` – displayed time format.
- `%d/%m/%y` – displayed date format.

An administrator may change the date and time format through parameters in the **[locale]** section of the *kav4mailservers.conf* configuration file. Examples of possible formats include:

- `%I:%M:%S %P` – for time output in twelve-hour format (**TimeFormat** parameter) with an am/pm indication.
- `%y/%m/%d` and `%m/%d/%y` – for date output (**DateFormat** parameter) in the *year/month/date* or *month/date/year* formats respectively.

6.8. Event logging parameters in Kaspersky Anti-Virus

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

Results of anti-virus scanning of server file systems are also output to the console. By default the information output to an event log and to the console is identical. Additional configuration is needed to display different information on the console from that in the event log (see section 6.8.2 on page 70 for details).

The amount of output information can be altered by changing the *report detail level*.

The **level of detail** is a number that sets the level of verbosity for information regarding the components' work. Each subsequent level (higher numbers) includes information of the previous level together with some additional data.

The possible levels of event log details are listed in the table below.

Levels	Level name	Meaning
	Fatal errors	Information regarding critical errors, which terminate the program due to impossibility of executing an action. For example, the application component is infected, or a vital action failed, such as scanning, database loading, or product key loading failed.
1	Errors	Information about other errors, including those not causing components to terminate, e.g. information regarding a file scanning failure.
2	Warning	Information about errors, which can cause termination of product operation (e.g., information about insufficient free disk space).
3	Info, Notice	Information telling whether a component is running or not, the path to the configuration file, scan area, information regarding anti-virus databases, product keys, and the resulting statistics.
4	Activity	Messages regarding object scanning according to the level of detail set for the scanning event log (see section 6.8.1 on page 68).
10	Debug	All debug messages, for example, configuration file contents.

Information regarding fatal errors in component operation is output regardless of the selected level of detail. The optimal level of detail is **4**, which is set by default.

The general format used to output information according to any of the above levels of detail is as follows:

```
[date time level_of_detail] STRING
```

where:

- `[date time level_of_detail]` is the parameter generated by the system, and contains the date and the time (in the format set by the administrator) and the report level of detail (the first letter of the level of detail).

The time and date formats can be changed in the **[locale]** section of the *kav4mailservers.conf* configuration file (see section 6.7 on page 66).

- `STRING` – a line of the event log, which may have different formats depending on the type of message. The following message types exist:
 - Messages about scanning (see section 6.8.1 on page 68).
 - Other messages (regarding a component start, anti-virus database loading, return codes etc.).
 - Messages output to the console (see section 6.8.2 on page 70).

Below is a detailed explanation of each message type and format.

6.8.1. Format of messages about scanning

Messages about scanning are only generated by the *kavscanner* and *aveserver* components.

The report format regarding file scanning depends on the object type (simple or container) to which it belongs.

For simple objects, messages about scanning look as follows:

- Extended message format (**ShowObjectResultOnly=no**):

```
"file_name" result [virus_name]
```

- Short message format (**ShowObjectResultOnly=yes**):

```
"file_name" result
```

where:

- `virus_name` is the name of the virus for the events CURED, INFECTED, CUREFAILED, WARNING, and SUSPICIOUS. For other events this field is left blank.
- `result` – the status assigned to the file after scanning and disinfection. A full list of possible results is provided in the table below.

With compound objects (archives) the messages can also have an extended or brief format:

- Extended message format (**ShowContainerResultOnly=no**):

```
"archive_name"
```

```
"file_name" result [virus_name]
```

```
"file_name" result [virus_name]
```

- Short message format (**ShowContainerResultOnly=yes**):

```
"file_name" result
```

Event/Result	Value
OK	The file is not infected.
CURED (only with disinfection enabled) mode	The file had been infected and was successfully cleaned.
INFECTED	The file is infected by one or more viruses. No request for disinfection.
CUREFAILED (only with disinfection enabled) mode	The file is infected by one or more viruses. Request for disinfection is present, but disinfection of the file is impossible.
WARNING	The code of the file is similar to that of a known virus.
SUSPICIOUS	The file is suspected of being infected by an unknown virus.
ERROR	The file cannot be checked due to an error (e.g. if a corrupted archive was processed)
PROTECTED	The file cannot be checked because it is password-protected.
CORRUPTED	The file is corrupted.

6.8.2. The format of messages output to the console

Messages are output to the console by the *kavscanner* and *keepup2date* components.

The output of the information by the *kavscanner* component to the console is governed by the presence of the `-q` option (quiet) in the command line when launching the component. If the option is used, the information will not be output to the console. Output of the messages regarding operation of the *keepup2date* component to the console is enabled by the configuration file parameter **KeepSilent=no**.

By default, the format and the contents of the information displayed on the screen are exactly the same as those included in the event log.

The contents of the information output to the console by the *kavscanner* component can be configured by including the **[display]** section in the configuration file (*kav4mailservers.conf* or the alternative one).

In this section, the parameters determine whether or not to display information about scanning objects in the archive (**ShowContainerResultOnly**), uninfected files (**ShowOK**), and the results of the component's current operation (**ShowProgress**).

The scanning log detail level is adjusted by the `-x<option>` option provided that the **[display]** section is present.

6.8.3. Anti-virus statistics of the application

Kaspersky Anti-Virus features an opportunity for collection and reviewing of statistics on virus activity for a specified period. The functionality is available via the web-based interface offered by Webmin.

To set up automatic collection of anti-virus statistics, perform the following steps:

- Assign the value below to the **AVStatistics** parameter in the **[smtpscan.report]** section of the application configuration file:

```
AVStatistics=\n/var/log/kav/5.5/kav4mailservers/smtpscanner.stat
```

- Configure the script collecting statistics from the log file to run at regular time intervals as necessary:

```
perl /usr/libexec/webmin/kavms5.5/parse_avstat.pl \  
-sd=/var/db/kav/5.5/kav4mailservers/proc_avstat\  
/var/log/kav/5.5/kav4mailservers/smtpscanner.stat
```

- Review the updated statistical information within Webmin after launching the above-mentioned script only.

If Webmin is installed at a path different from the default, then the `/usr/libexec/webmin/kavms5.5/parse_avstat.pl` path must be modified accordingly!

6.8.4. Additional data fields in messages

The application allows addition of supplementary information to message headers. The data may include information on application version, the last update to the anti-virus databases, time and results of anti-virus scanning of the current message.

Addition of such information to message header is defined by the **AddXHeaders** parameter in the **[smtpscan.group:default]** section of the configuration file.

Header format:

```
X-Anti-Virus: <application name and version >, bases:  
<last update of the anti-virus databases in YYYYMMDD  
format> #<number of records in the anti-virus data-  
bases>, check: <scan date in YYYYMMDD format> <status  
after scanning or not_checked>
```

E.g.:

```
X-Anti-Virus:Kaspersky Anti-Virus for Unix Mail Serv-  
ers version 5.5/RELEASE, bases: 20041101 #102746,  
check: 20041210 clean
```

CHAPTER 7. UNINSTALLING KASPERSKY ANTI-VIRUS

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

- superuser privileges (**root**).
- Installation log file. Names and sizes of the files installed as parts of Kaspersky Anti-Virus must be exactly the same as specified in the installation log file.
- The *aveserver* process must be stopped.
- The mail service must be stopped.

If you installed Kaspersky Anti-Virus using its .rpm package enter the following in the command line to begin the uninstall procedure:

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

If you installed Kaspersky Anti-Virus using its .deb package enter the following in the command line to begin the uninstall procedure:

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

If you installed Kaspersky Anti-Virus using its .pkg package enter the following in the command line to begin the uninstall procedure:

```
# pkg-delete <package_name>
```

The application will be uninstalled automatically. No additional notifications are output in case of successful completion of software removal.

CHAPTER 8. TESTING THE OPERATION OF KASPERSKY ANTI-VIRUS

After installing and adjusting Kaspersky Anti-Virus, you can test the correctness of its settings and operation using a series of test "viruses".

The test virus was specially designed by the European Institute for Computer Antivirus Research organization, [eicar](http://www.eicar.org) for testing anti-virus products.

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

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

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

The file downloaded from the **EICAR** website contains the body of a standard test "virus". The application will detect it, assign the **Infected** status to it and apply the action defined by the administrator for handling objects of this status.

To test the response of the application to other types of objects, modify the body of this standard test "virus" by adding one of the prefixes (please see the table below).

Prefix	Object type
No prefix, standard test "virus"	Infected. The object cannot be disinfected.
CORR-	Corrupted.
SUSP-	Suspicious (unknown viral code).
WARN-	Warning (modified code of a known virus).
ERRO-	Error while scanning the object.

Prefix	Object type
CURE–	Cured. The object is disinfected; the text of the "virus" body is changed for CURE.
DELE–	The object is automatically deleted.

The first table column lists prefixes to be added at the beginning of the string of the standard test "virus". The second column of this table contains the status assigned by the application after the prefix has been added. The actions for each status of object are defined by anti-virus application settings customized 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 Kaspersky Anti-Virus; here we shall try to answer them in detail.

Constantly growing Knowledge Base containing answers to frequently asked questions is available at Kaspersky Lab web site: http://support.kaspersky.com/unix_mail_server. You can use it to find answers to the questions that are not mentioned below. You can also use online HelpDesk form to send a request to the Technical Support service (<http://www.kaspersky.com/helpdesk>).

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 and iStreams technology. The application implements the technology using a database of file checksums and file checksum storage in alternate NTFS streams.

Question: Why does Kaspersky Anti-Virus cause a certain decrease in computer performance, noticeably loading the CPU?

Virus detection is a computationally intensive mathematical problem requiring structural analysis, checksum calculation and mathematical data conversions. Processor time is therefore the main resource consumed by the Anti-Virus, and each new virus added to the anti-virus database increases the overall scanning time.

Other anti-virus products speed up scanning by excluding from their databases both viruses which are less easily detectable or less frequent (e.g. in a specific geographic location), and file formats that require complicated analysis (e.g., PDF). Kaspersky Lab believes that the purpose of anti-virus protection is to establish real and complete anti-virus security for its users.

Experienced users can, of course, accelerate anti-virus scanning by disabling scanning of various file types. However, please keep in mind that it will decrease the overall security level.

Kaspersky Anti-Virus recognizes more than 700 formats of archived and packed files. This is essential for anti-virus security because harmful executable code may be hidden inside files of any recognized format. However, despite the daily growth in the number of viruses detected by Kaspersky Anti-Virus (approximately 30 new viruses appear daily) as well as the ever increasing number of recognized file formats, this new version of our application functions faster than previous ones. That is achieved through the use of new unique technologies, such as iChecker™, developed at Kaspersky Lab.

***Question:** Why do I need a key file? Will my copy of the Anti-Virus work without it?*

No, Kaspersky Anti-Virus does not work without a product key.

If you are still deciding whether or not to purchase Kaspersky Anti-Virus, we can provide you with a temporary key file (trial key), which will only work either for two weeks or for a month. When this period expires, the key will be blocked.

***Question:** What happens when the key validity period expires?*

After expiration of the key, Kaspersky Anti-Virus will continue operating, but anti-virus database updating will be disabled. The anti-virus application will continue cleaning infected objects but it will be using the old anti-virus databases.

If such a situation arises, contact either the company from which you purchased Kaspersky Anti-Virus, or Kaspersky Lab directly, for key extension.

***Question:** My installation of Kaspersky Anti-Virus does not work.*

What should I do?

First of all check **whether the *aveserver* component is running**, or a solution to your problem is described in this document and, in particular, in this section or in the Knowledge Base of Kaspersky Lab site (http://support.kaspersky.com/unix_mail_server).

In addition, we recommend that you apply for support to the distributor from whom you purchased Kaspersky Anti-Virus, or write to Kaspersky Lab's Technical Support (<http://www.kaspersky.com/helpdesk>).

To make sure your request is answered as soon as possible, follow these suggestions:

1. In the message header, specify your server's operating system, the name of the component you are experiencing problems with, and briefly describe the problem. For example:
Linux, Webmin, no access to settings of the licensed users' list.
2. At the beginning of the message, specify the exact versions of the operating system and Kaspersky Anti-Virus.
3. Clearly describe the problem in brief. Keep in mind that, when reading your mail, the support service officers do not yet know about your problem. They can only help after fully understanding and reproducing it.
4. Send the following data, packed into one archive, to the Technical Support Service:
 - All the configuration files of your mail agent (MTA)
 - Files from the */etc/kav/* directory
 - Mail system event log file
 - The anti-virus component event log, for example, */var/log/aveserver.log*;
 - The information output to the console by the command **ps -ax**
 - The key file.
5. Make sure to specify in your mail if your computer system contains any of the following:
 - SCSI controller;
 - a very old or very new processor, or more than one processor;
 - less than 64 MB or more than 2 GB of RAM.
6. Specify the approximate amount of daily traffic and whether or not the server has peak loads.

Question: What are the hourly updates for?

A few years ago viruses were transmitted on floppy disks, and adequate computer protection could be achieved by installation of an anti-virus program followed by infrequent updates to its anti-virus database. However, recent virus epidemics spread around the world in a matter of hours, and anti-virus protection with old databases may be helpless

against a new threat. In order to resist new viruses, you should update the anti-virus databases daily.

Every year Kaspersky Lab increases the frequency of its updates issued for the anti-virus databases. Currently they are released every hour.

Updating of the application modules is an additional feature that allows both correction of discovered vulnerabilities and addition of new functions.

***Question:** What are the changes to the updating service of version 5.0?*

The Kaspersky Lab 5.0 application suite features a new updating service which has been developed in accordance with the requests of our users. It automates the whole updating procedure, from the preparation of updates in Kaspersky Lab to the moment that relevant files are updated on clients' computers.

Advantages of the new updating service include:

Ability to resume downloading of files after disconnection. Upon reconnection only files which have not been downloaded are retrieved.

Cumulative updates are now half the size. A cumulative update contains the whole anti-virus database; therefore its size considerably exceeds that of typical updates. The new service employs a special technology which allows using an already existing anti-virus database for a cumulative update.

Accelerated downloading from the Internet. Kaspersky Anti-Virus locates a Kaspersky Lab's update server located in your region. Furthermore, servers are allocated according to their performance, so you will not be sent to an overloaded server while there is another idle server available.

Use of key black lists. Unlicensed and illegal users are now prevented from using the updating service. Protected users therefore do not suffer from inability to contact overloaded updates' servers.

Corporate enterprises can now create a local updates' server. This feature is designed for organizations where a single LAN unites computers protected by Kaspersky Lab applications. Any computer on the LAN can be turned into an updates' server that retrieves updates from the Internet and shares them with the other networked computers.

Is it possible for an intruder to replace the anti-virus database?

Every anti-virus database has a unique signature checked by Kaspersky Anti-Virus when accessing the database. If the signature is wrong or the date of the database is later than that of the key expiration, Kaspersky Anti-Virus will not use it.

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

Version 5.5 of Kaspersky Anti-Virus for Unix Mail Servers has been tested with RedHat, Debian and SuSE distributions and Kaspersky Anti-Virus packages have been compiled specifically for the listed distributions.

Please see the supported OS versions in section 1.2 on page 8.

If your distribution is 100 percent compatible with a supported one (for example, ASPLinux is compatible with Red Hat Linux), then the probability of critical problems is very low.

Users of distributions that are not included in the list supported by Kaspersky Lab may experience incorrect application operation, which will be caused by specific details of the operating system. For example, your OS distribution may use a different version of a library or its system initialization scripts may have a non-standard location. In such cases, Kaspersky Lab's Technical Support service will be unable to help you.

Question: *Everything worked fine until I installed Kaspersky Anti-Virus for Unix Mail Servers and integrated it with the Postfix mail system. After that, mail messages stopped being delivered and the following error was logged in maillog:*

```
Sep 23 15:17:03 server postfix/lmtp[1678]:  
8238C38987: to=<user@server.org  
<mailto:user@server.org>>, relay=none, delay=1,  
status=bounced (localhost: host not found)
```

What should I do?

Such a problem may appear in the following cases:

- Your DNS has no localhost domain, which is required by RFC 2606. Configure your DNS as the RFC advises. For more detailed information please refer to this page: <http://www.ietf.org/rfc/rfc2606.txt>.
- Localhost is not defined in the file `/etc/hosts`. Normally, it should be set to **localhost=127.0.0.1**. Edit the hosts file, specifying this address for localhost.
- The `/etc/hosts` file contains no localhost IP address. Add the following line to the `/etc/hosts` file:

```
127.0.0.1      localhost
```

Question: *Can Network Control Centre for Windows be used to control Kaspersky Anti-Virus?*

It is impossible to use Network Control Centre for Windows when working with Kaspersky Anti-Virus for Unix Mail Servers. In this version of the application we provide an option to configure it remotely using a special module for the Webmin package.

Question: *How can I save the program's console output to a file?*

To save the information output to the console by Kaspersky Anti-Virus, you can either make the appropriate settings in the configuration file or type the following at the command line:

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

where:

`some_app` – means the application module for which you want to save to file the standard output and error messages.

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

E.g.:

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

In this case the 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. Kaspersky Lab

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

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

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

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

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

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

A.1. Other Kaspersky Lab Products

Kaspersky Anti-Virus® Personal

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

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

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

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

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

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

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

Kaspersky Anti-Virus® Personal Pro

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

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

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

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

Kaspersky® Anti-Hacker

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

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

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

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

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

Kaspersky® Personal Security Suite

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

Kaspersky Personal Security Suite has the following features:

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

Kaspersky Lab News Agent

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

The product performs the following functions:

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

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

Kaspersky® OnLine Scanner

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

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

Kaspersky® OnLine Scanner Pro

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 Microsoft ActiveX® technology. 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® Business Optimal

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

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

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

¹ 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.

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

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

Kaspersky® Corporate Suite

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

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

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

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

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

Kaspersky® Anti-Spam

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

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

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

Kaspersky® SMTP Gateway

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

Kaspersky Security® for Microsoft Exchange 2003

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

Kaspersky® Mail Gateway

Kaspersky Mail Gateway is a comprehensive solution that provides complete protection for users of mail systems. This application installed between the corporate network and the Internet scans all components of e-mail messages for the presence of viruses and other malware (Spyware, Adware, etc.) and

performs centralized anti-spam filtration of e-mail stream. This solution also includes some additional mail traffic filtration features.

A.2. Contact Us

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

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

Appendix B. License agreement

Standard 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. IF YOU HAVE BROKEN THE CD'S SLEEVE OR OPENED THE BOX, YOU WILL NOT BE ENTITLED TO RETURN THE SOFTWARE FOR REFUND. SOFTWARE FOR HOME USE (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY SECURITY FOR PDA) PURCHASED AS A DOWNLOAD VIA THE INTERNET MAY BE RETURNED FOR A FULL REFUND WITHIN 14 DAYS AFTER PURCHASE FROM KASPERSKY LAB, IT'S AUTHORIZED DISTRIBUTOR OR RESELLER. OTHER PRODUCTS ARE NON REFUNDABLE. 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 unauthorised 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 one (1) year 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 attached to this Agreement,

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 90 days from first download or installation the Software 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 (v) 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. Liability

(i) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for (i) the tort of deceit, (ii) 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, (iii) any breach of the obligations implied by s.12 Sale of Goods Act 1979 or s.2 Supply of Goods and Services Act 1982 or (iv) any liability which cannot be excluded by law.

(ii) Subject to paragraph (i), 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 paragraph (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. The construction and interpretation of this Agreement shall be governed in accordance with the laws of England and Wales. The parties hereby submit to the jurisdiction of the courts of England and Wales save that Kaspersky Lab as claimant shall be entitled to initiate proceedings in any court of competent jurisdiction.

9. (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), 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).