

Kaspersky Security 8.0 for Linux Mail Server



Administrator's Guide

APPLICATION VERSION: 8.0 MAINTENANCE PACK 1, CRITICAL FIX 1

Dear User,

Thank you for choosing our product. We hope that you will find this documentation useful and that it will provide answers to most questions that may arise.

Attention! This document is the property of Kaspersky Lab ZAO (herein also referred to as Kaspersky Lab): all rights to this document are reserved by the copyright laws of the Russian Federation, and by international treaties. Illegal reproduction or distribution of this document or parts hereof will result in civil, administrative, or criminal liability under applicable law.

Any type of reproduction or distribution of any materials, including translations, is allowed only with the written permission of Kaspersky Lab.

This document and related graphic images can be used exclusively for informational, non-commercial, or personal use.

This document may be amended without prior notice. You can find the latest version of this document on the Kaspersky Lab website, at <http://www.kaspersky.com/docs>.

Kaspersky Lab assumes no liability for the content, quality, relevance, or accuracy of any materials used herein the rights to which are owned by third parties, or for any potential damages associated with the use of such documents.

Document revision date: 04/17/2015

© 2015 Kaspersky Lab ZAO. All Rights Reserved.

<http://www.kaspersky.com>
<http://support.kaspersky.com>

TABLE OF CONTENTS

ABOUT THIS GUIDE	8
In this document	8
Document conventions	10
SOURCES OF INFORMATION ABOUT THE APPLICATION.....	12
Sources of information for independent research	12
Discussing Kaspersky Lab applications on the Forum.....	13
KASPERSKY SECURITY 8.0 FOR LINUX MAIL SERVER	14
What's new	15
Distribution kit.....	15
Hardware and software requirements.....	15
APPLICATION ARCHITECTURE.....	18
Main components	18
Operation algorithm	19
INSTALLING AND REMOVING THE APPLICATION.....	20
Preparing to install.....	20
Upgrading from a previous version of the application	21
Installing Kaspersky Security on top of the previous version	22
Installing the Kaspersky Security web interface on top of the previous version	23
Updating Kaspersky Security settings.....	24
Updating Kaspersky Security web interface settings	25
Installing the application	25
Installing the Kaspersky Security package.....	25
Installing the Kaspersky Security localization package	26
Installing the Kaspersky Security web interface package on the same computer with Kaspersky Security	27
Installing the Kaspersky Security web interface package on a separate computer.....	28
Preparing Kaspersky Security for operation	30
Starting initial configuration of Kaspersky Security manually	30
Starting automatic initial configuration of Kaspersky Security.....	39
Preparing Kaspersky Security web interface for operation	44
Starting initial configuration of Kaspersky Security web interface manually	44
Starting automatic initial configuration of the web interface of Kaspersky Security.....	48
Removing Kaspersky Security.....	50
Actions after removing Kaspersky Security	51
CONNECTING TO KASPERSKY SECURITY WEB INTERFACE	51
MANUAL INTEGRATION OF KASPERSKY SECURITY WITH MAIL SERVERS AND AMAVIS INTERFACE.....	53
About manual integration.....	53
Manual Integration with Sendmail server	54
Integration using the .mc file	55
Integration using the .cf file	56
Manual Integration with Exim mail server	57
After-queue integration by rerouting.....	57
Before-queue integration using dynamic linking.....	60
Manual Integration with QMail server	63

Manual integration with a Postfix mail server	64
After-queue integration.....	64
Before-queue integration.....	66
Integration using the Milster protocol	68
Manual integration with the Amavis interface.....	69
APPLICATION LICENSING	71
About the license	71
About the End User License Agreement.....	72
About the license certificate.....	72
About the key.....	72
About the key file.....	73
About data provision.....	73
Viewing information about the license and added keys	74
Adding a key.....	74
Removing the key.....	74
STARTING AND STOPPING THE APPLICATION	76
SERVER PROTECTION STATUS	77
BASIC PRINCIPLES	78
About scan and content filtering statuses	78
About message processing rules.....	79
Message processing algorithm	79
About black and white lists of addresses.....	80
Creating message processing rules.....	81
Viewing the list of message processing rules	83
About actions on objects.....	83
About Kaspersky Security tasks	84
Viewing the list of application tasks	85
About information X-headers	86
ANTI-SPAM PROTECTION	87
About Anti-Spam protection.....	87
About external Anti-Spam message scanning services.....	87
Enabling and disabling the Anti-Spam engine	88
Enabling and disabling Anti-Spam scanning of messages for a rule	89
Configuring general Anti-Spam scan settings.....	89
Configuring Anti-Spam scan settings for a rule.....	90
Configuring Anti-Spam Quarantine settings.....	93
Limiting the size of messages to be scanned for spam	93
ANTI-VIRUS PROTECTION.....	95
About Anti-Virus protection	95
Enabling and disabling the Anti-Virus engine	95
Enabling and disabling Anti-Virus scanning for a rule.....	96
Configuring general Anti-Virus scan settings	97
Configuring the processing of a message that cannot be disinfected	98
Configuring Anti-Virus scan settings for a rule.....	99
Excluding messages from Anti-Virus scanning by attachment format	100
Excluding messages from Anti-Virus scanning by attachment name.....	101

Limiting the size of objects to be scanned for viruses	102
ANTI-PHISHING PROTECTION	103
About Anti-Phishing protection.....	103
Enabling and disabling the Anti-Phishing engine.....	103
Enabling and disabling Anti-Phishing scanning of messages for a rule	104
Configuring general Anti-Phishing scan settings.....	105
Configuring Anti-Phishing scan message processing settings.....	105
CONTENT FILTERING OF MESSAGES	107
About content filtering.....	107
Enabling and disabling content filtering of messages	107
Enabling and disabling content filtering of messages for a rule	108
Configuring content filtering by message size.....	109
Configuring content filtering by attachment name.....	109
Configuring content filtering by attachment format.....	110
UPDATING KASPERSKY SECURITY DATABASES.....	112
About database updates	112
Checking database state	112
About update sources.....	114
Selecting an update source	114
Configuring the proxy server settings	116
Configuring the update task schedule.....	117
Update task schedule settings	117
Updating databases manually.....	119
ADVANCED CONFIGURATION OF KASPERSKY SECURITY	121
Configuring global black and white lists of addresses.....	121
Setting the number of scanning streams	123
Importing / exporting settings.....	123
INTEGRATION WITH AN EXTERNAL DIRECTORY SERVICE USING THE LDAP PROTOCOL	124
About integration with an external directory service.....	124
Configuring Kaspersky Security integration with an external directory service with the help of user scripts	125
Requirements for user scripts	125
Searchemail user script	126
Searchusers user script.....	127
Getuseraccount user script.....	127
Login user script	128
Configuring the application connection to an external directory service using the LDAP protocol	128
Checking the application connection to an external directory service using the LDAP protocol	129
Adding senders / recipients from an external user service to rules.....	129
Adding personal black and white lists of addresses.....	131
Managing untrusted certificates	132
USING THE APPLICATION VIA THE SNMP PROTOCOL.....	134
About receiving runtime information via the SNMP protocol.....	134
Configuring interaction with the application via the SNMP protocol	134
Getting the ID of the SNMP process	135
Enabling information exchange via the SNMP protocol	135
Calling MIB objects	136

Enabling / disabling event traps	136
Viewing the MIB structure using the snmpwalk command	136
MANAGING COMPANY EMPLOYEE ACCOUNTS	137
Configuring settings of a company employee account.....	137
Activating and deactivating a company employee account.....	137
Configuring settings of a company employee account.....	138
Configuring the transmission of infected messages placed in Backup to users.....	138
BACKUP	140
About Backup	140
Viewing statistics of message copies in Backup	141
Filtering the details of message copies in Backup	141
Deleting message copies from Backup.....	142
Saving messages from Backup to file	142
Delivering messages from Backup to recipients	142
Configuring Backup size	143
EMAIL NOTIFICATIONS	144
About email notifications	144
Enabling delivery of email notifications about objects	145
Specifying additional email addresses for delivery of email notifications about objects	146
Configuring delivery of email event notifications to the administrator	147
Editing templates of email event notifications	148
Using macros in templates of email event notifications	149
RUNTIME REPORTS AND STATISTICS	152
Viewing runtime statistics	152
Creating reports	152
Creating on-demand reports	153
Configuring scheduled reports	155
EVENT LOG	156
About the event log	156
Changing the system log category for storing events	158
Configuring event logging in the event log	158
TRACE LOG.....	160
About the trace log.....	160
Enabling the trace log.....	161
Configuring the level of detail of the trace log.....	161
Configuring the location of the trace log	162
Configuring the rotation of trace files	162
TESTING THE APPLICATION OPERATION	164
About the EICAR test file	164
About the types of the EICAR test file.....	164
Testing anti-virus protection of messages using the EICAR test file.....	165
ADMINISTRATION OF THE APPLICATION THROUGH KASPERSKY SECURITY CENTER.....	167
About managing the application via Kaspersky Security Center.....	167
Configuring administration of the application through Kaspersky Security Center.....	167
Installing Network Agent	168
Configuring Network Agent settings.....	168

Installing the Kaspersky Security administration plug-in	169
Checking the connection to Kaspersky Security Center.....	169
Starting and stopping Kaspersky Security on a client computer	169
Managing tasks.....	170
About tasks for Kaspersky Security 8.0 for Linux Mail Server	170
Creating a local task.....	171
Creating a group task.....	171
Creating a task for a set of computers	172
Editing task settings	172
Viewing general information on the operation of Kaspersky Security in a cluster	174
CONTACTING THE TECHNICAL SUPPORT SERVICE	175
Technical support by phone.....	175
Technical Support via Kaspersky CompanyAccount	175
Using a trace file and AVZ script.....	176
Extended diagnostics of application operation.....	176
APPENDICES	177
Application file locations on a computer running Linux	177
Application file locations on a computer running FreeBSD	178
KASPERSKY LAB.....	180
INFORMATION ABOUT THIRD-PARTY CODE.....	181
TRADEMARK NOTICES.....	182
INDEX	183

ABOUT THIS GUIDE

This document is the Administrator's Guide to installing, configuring, and using the Kaspersky Security 8.0 for Linux® Mail Server (hereinafter also "Kaspersky Security"). This document is intended for application administrators. The Guide is intended for technical specialists who carry out the installation and administration of Kaspersky Security and provide support for organizations that use Kaspersky Security.

This Guide is intended to:

- Explain how to install and use Kaspersky Security.
- Provide readily available information on issues related to the operation of Kaspersky Security.
- Describe additional sources of information about the application and ways of receiving technical support.

IN THIS SECTION:

In this document.....	8
Document conventions.....	10

IN THIS DOCUMENT

This document includes the following sections:

Sources of information about the application (see page [12](#))

This section describes sources of information about the application and lists websites that you can use to discuss the application's operation.

Kaspersky Security 8.0 for Linux Mail Server (page [14](#))

This section contains information on the purpose, key features, and composition of the application. It shows the function of each part of the package supplied and a range of services available to registered users of the application. This section contains hardware and software requirements which the computer must meet for the installation of Kaspersky Security.

Application architecture (see page [18](#))

This section describes Kaspersky Security and the logic of their interaction.

Installing and removing the application (page [20](#))

This section contains step-by-step instructions for application installation and removal.

Connecting to Kaspersky Security web interface (see page [51](#))

This section describes how you can connect to start using the application web interface.

Manual integration of Kaspersky Security with mail servers and Amavis interface (see page [53](#))

This section contains information about how to manually integrate Kaspersky Security 8.0 for Linux Mail Server with Exim, Postfix, Sendmail, QMail, and Amavis.

Application licensing (see page [71](#))

This section provides information about general terms related to the application activation. Read this section to learn more about the purpose of the License Agreement, ways of activating the application, and license renewal.

Starting and stopping the application (see page [76](#))

This section describes how you can start and stop the application.

Mail server protection status (see page [77](#))

This section contains information about how to check the level of protection of the mail server and related problems.

Basic operating principles (see page [78](#))

This section contains a description of the basic concepts and principles of using the application, and information about how to configure it.

Anti-Spam email protection (see page [87](#))

This section contains information about Anti-Spam protection of messages and how to configure it.

Anti-Virus email protection (see page [95](#))

This section contains information about Anti-Virus protection of messages and how to configure it.

Anti-Phishing email protection (see page [103](#))

This section contains information about Anti-Phishing protection of messages and how to configure it.

Content filtering of email (see page [107](#))

This section contains information about content filtering of messages and how to configure it.

Kaspersky Security database updates (see page [112](#))

This section contains information on how to update application databases.

Kaspersky Security advanced settings (see page [121](#))

This section contains information on how to configure additional settings for the application.

Integration with an external directory service (see page [124](#))

This section describes how you can integrate Kaspersky Security with an external directory service that supports the LDAP protocol and use custom scripts to search for information in the external directory service.

Managing the application via SNMP (see page [134](#))

This section contains information about how to use Kaspersky Security via the SNMP protocol and configure runtime trap events.

Managing company employee accounts (see page [137](#))

This section describes how you can manage accounts of company employees and configure their settings.

Backup (see page [140](#))

This section contains information about Backup and how to use it.

Email notifications (see page [144](#))

This section contains information about mail notifications and how to configure them.

Runtime reports and statistics (see page [152](#))

This section contains information about reports and statistics on the operation of the application.

Event log (see page [156](#))

This section contains information about the Event log and how to configure it.

Trace log (see page [160](#))

This section contains information about the Trace log and how to configure it.

Application testing (see page [164](#))

This section provides information about how to ensure that the application detects viruses and their modifications and performs the correct actions on them.

Administering the application through Kaspersky Security Center (see page [167](#))

This section describes how you can manage Kaspersky Security 8.0 for Linux Mail Server through Kaspersky Security Center.

Contacting Technical Support (see page [175](#))

This section provides information about how to obtain technical support and the requirements for receiving help from Technical Support.

Annexes (see page [177](#))

This section provides information that complements the document text.

Kaspersky Lab ZAO (see page [180](#))

This section provides information about Kaspersky Lab ZAO.

Information on third-party code (see page [181](#))

This section provides information about the third-party code used in the application.

Trademark notices (on page [182](#))

This section lists trademarks of third-party manufacturers that were used in the document.

Index

This section allows you to quickly find required information within the document.

DOCUMENT CONVENTIONS

This document uses the following conventions (see table below).

Table 1. Document conventions

SAMPLE TEXT	DESCRIPTION OF DOCUMENT CONVENTION
Note that...	Warnings are highlighted in red and boxed. Warnings show information about actions that may have unwanted consequences.
We recommend that you use...	Notes are boxed. Notes provide additional and reference information.
Example: ...	Examples are given in blocks on a yellow background titled as "Example".
<i>Update means...</i> The <i>Databases are out of date</i> event occurs.	The following elements are italicized in the text: <ul style="list-style-type: none"> • New terms. • Names of application statuses and events.
Press ENTER . Press ALT+F4 .	Names of keyboard keys appear in bold and are capitalized. Names of keys that are connected by a + (plus) sign indicate the use of a key combination. These keys have to be pressed simultaneously.
Click the Enable button.	Names of application interface elements, such as entry fields, menu items, and buttons, are set off in bold.
➡ <i>To configure a task schedule:</i>	Introductory phrases of instructions are italicized and are accompanied by the arrow sign.
In the command line, type help. The following message then appears: Specify the date in dd:mm:yy format.	The following types of text content are set off with a special font: <ul style="list-style-type: none"> • Text in the command line. • Text of messages that the application displays on screen. • Data to be entered using the keyboard.
<User name>	Variables are enclosed in angle brackets. Instead of a variable, the corresponding value should be inserted, with angle brackets omitted.

SOURCES OF INFORMATION ABOUT THE APPLICATION

This section lists the sources of information about the application.

You can select the most suitable information source, depending on the issue's level of importance and urgency.

IN THIS SECTION:

Sources of information for independent research.....	12
Discussing Kaspersky Lab applications on the Forum	13

SOURCES OF INFORMATION FOR INDEPENDENT RESEARCH

You can use the following sources to find information about the application:

- Application page on the Kaspersky Lab website
- Application page on the Technical Support website (Knowledge Base).
- Kaspersky Security 8.0 for Linux Mail Server web interface help. The web interface lets you manage Kaspersky Security through a browser.
- Documentation.

If you cannot find the solution to an issue on your own, we recommend that you contact Technical Support at Kaspersky Lab.

An Internet connection is required to use information sources on the Kaspersky Lab website.

Application page on the Kaspersky Lab website

The Kaspersky Lab website features an individual page for each application.

On the page (<http://www.kaspersky.com/linux-mail-security>), you can view general information about the application, its functions and features.

The Kaspersky Lab website (<http://www.kaspersky.com/linux-mail-security>) contains a link to a section describing the product and how to obtain a license or extend an existing one.

The application's Knowledge Base page at the Technical Support Service website.

Knowledge Base is a section on the Technical Support website that provides advice on using Kaspersky Lab applications. The Knowledge Base comprises reference articles grouped by topics.

On the page of the application in the Knowledge Base (<http://support.kaspersky.com/klms8>), you can read articles that provide useful information, recommendations, and answers to frequently asked questions on how to purchase, install, and use the application.

Articles may provide answers to questions that are out of scope of Kaspersky Security, being related to other Kaspersky Lab applications. They also may contain news from the Technical Support Service.

Web interface help

Help provides information on managing protection, configuring the application, and performing common user tasks using the web-interface of Kaspersky Security 8.0 for Linux Mail Server (hereinafter the "web interface").

Documentation

The application distribution kit includes documents that help to install and activate the application on local area network computers, configure application settings, and find tips on using the application.

- *To connect Kaspersky Security manual pages under the Linux operating system,*

add the following string to the `/etc/manpath.config` configuration file:

```
MANPATH /opt/kaspersky/klms/share/man
```

- *To connect Kaspersky Security manual pages under the FreeBSD™ operating system,*

add the following string to the `/etc/manpath.config` (or `man.conf`) configuration file:

```
MANDATORY_MANPATH /usr/local/man
```

DISCUSSING KASPERSKY LAB APPLICATIONS ON THE FORUM

If your question does not require an immediate answer, you can discuss it with the Kaspersky Lab experts and other users in our forum (<http://forum.kaspersky.com>).

In this forum you can view existing topics, leave your comments, create new topics.

KASPERSKY SECURITY 8.0 FOR LINUX

MAIL SERVER

Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1 protects incoming and outgoing email messages (or "messages") against malware, spam and phishing, and provides content filtering. Kaspersky Security runs under Linux and FreeBSD operating systems, and can be used on high-load mail servers.

The Application allows:

- Scan incoming and outgoing email messages for spam, phishing, and malware, detect and block mail attachments intended for a restricted number of recipients or attachments that target software vulnerabilities.
- Neutralize threats detected in files and email messages, disinfect objects.
- Save message copies in Backup before their anti-virus processing and filtering.
- Save messages from Backup to file and deliver messages to recipients from Backup.
- Process mail in accordance with the rules defined for groups of senders and recipients.
- Perform content filtering of messages by size and attachments by name, type, and size.
- Specify user accounts and user groups from Microsoft® Active Directory® and OpenLDAP in mail filtering rules.
- Notify the sender, recipients, and administrator about detected messages containing objects that are infected, probably infected, password-protected, or inaccessible for scanning.
- Update Anti-Virus, Anti-Spam, and Anti-Phishing databases from Kaspersky Lab update servers or custom resources (http and ftp servers) according to schedule or on demand.
- Generate application runtime statistics and reports.
- Getting application runtime info and statistics via SNMP as well as enabling / disabling event traps.
- Scan mail server file systems for malware on demand.
- Configure the settings and manage the application using the standard tools of the operating system from the command line or using a web-based interface.
- Manage the operation of a group of mail servers with Kaspersky Security 8.0 for Linux Mail Server installed via Kaspersky Security Center 10 SP1.

All commands and paths in the document are specified for the Linux operating system. Information about application file locations on computers with the FreeBSD operating system is available in the "Application file locations on a computer running FreeBSD section (see page [178](#))".

If you copy any code strings from the Guide to the mail server configuration file, be sure to delete the backslashes (\) and their trailing LFs.

IN THIS SECTION:

What's new	15
Distribution kit.....	15
Hardware and software requirements	15

WHAT'S NEW

Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1 delivers the following new features:

- More operating systems are now supported.
- Support of the Apache 2.4 web server has been implemented.
- Kaspersky Security Center 10 SP1 is now supported.
- The Delete Attachment operation has been added for the Content Filter component of the application.
- It is now possible to send several messages at once from Backup via the web interface.
- It is now possible to filter messages by rule ID in the web interface.

DISTRIBUTION KIT

You can purchase the application through Kaspersky Lab's online stores (for example, <http://www.kaspersky.com>, in the **Online Shop** section) or partner companies.

The content of the distribution kit may differ depending on the region, in which the application is distributed.

If Kaspersky Security is purchased through an online store, the application is copied from the store's website. Information required to activate the application is sent to you by email after payment.

HARDWARE AND SOFTWARE REQUIREMENTS

Kaspersky Security has the following hardware and software requirements:

- Minimum hardware requirements:
 - Intel® Xeon® 3040 processor or Core™ 2 Duo 1.86 GHz or faster.
 - 2 GB RAM.
 - At least 4 GB available for swap.
 - 4 GB available on the hard drive to install application and store temporary and log files.
- Software requirements:
 - One of the following 32-bit operating systems:

- Red Hat Enterprise Linux® 6.6 Server.
- SUSE Linux Enterprise Server 11 SP3.
- CentOS-6.6.
- Ubuntu Server 12.04.4 LTS.
- Ubuntu Server 14.04 LTS.
- Debian GNU / Linux 7.7.
- Debian GNU / Linux 6.0.10.
- FreeBSD 8.3.
- FreeBSD 9.3.
- FreeBSD 10.1.
- One of the following 64-bit operating systems:
 - Red Hat Enterprise Linux 6.6 Server.
 - Red Hat Enterprise Linux 7.
 - SUSE Linux Enterprise Server 11 SP3.
 - SUSE Linux Enterprise Server 12.
 - CentOS-6.6.
 - CentOS-7.
 - Ubuntu Server 12.04 LTS.
 - Ubuntu Server 14.04 LTS.
 - Debian GNU / Linux 6.0.10.
 - Debian GNU / Linux 7.7.
 - FreeBSD 8.3.
 - FreeBSD 9.3.
 - FreeBSD 10.1.
- Availability of the following packages of 32-bit libraries on 64-bit operating systems:
 - ia32-libs for Debian and Ubuntu
 - libgcc.i686, glibc.i686 for RHEL and CentOS
 - libgcc-32bit, glibc-32bit for SUSE.
 - lib32 for FreeBSD 64bit;
 - compat9x for FreeBSD 10.
- Kaspersky Security requires the Perl 5 programming language of version 5.8.5 or later.

Kaspersky Security supports integration with the following mail servers:

- Exim-4.71 or later
- Postfix-2.5 or later
- Sendmail-8.14 or later.

To run the Kaspersky Security web interface, one of the following browsers must be installed on the computer:

- Mozilla™ Firefox™ 34 or later.
- Microsoft Internet Explorer® 11 or later.
- Google Chrome™ 39 or later.

To enable the operation of the Kaspersky Security web interface, an Apache 2.4 web server must be installed on the computer hosting the web interface.

APPLICATION ARCHITECTURE

This section describes Kaspersky Security and the logic of their interaction.

IN THIS SECTION:

Main components.....	18
Operation algorithm.....	19

MAIN COMPONENTS

Kaspersky Security includes the following components:

- *Filter* – receives and forwards mail messages to/from the application's mail server. Kaspersky Security includes several filters used in accordance with the mail server and the type of integration with Kaspersky Security:
 - Milter.
 - Smtproxy.
 - Dfunc.
 - Qmail-queue binary.
- Klms-watchdog – the main component for processing mail messages. It consists of the following modules:
 - Scan Logic is a module that controls message scanning (hereinafter also "Scan Logic module"). It includes a MIME parser and content filter.
 - AV-engine – scans messages for viruses (hereinafter "the Anti-Virus engine").
 - AS-engine – scans messages for spam (hereinafter "the Anti-Spam engine").
 - AP-engine – scans messages for phishing threats (hereinafter "the Anti-Phishing engine").
 - Updater – updates Anti-Virus, Anti-Spam, and Anti-Phishing databases.
 - Backup – allows messages to be restored to their original form with no changes.
 - Auth – interfaces with user registration systems.
 - Statistics – collects statistical information.
 - Settings-manager – stores task and rule settings for processing messages in the database; exports and imports these settings and notifies other modules of any changes.
 - Facade – allows the application to interface with utilities and administration systems.
 - Licenser – manages keys.
 - Notifier – generates messages with notifications of importance to the administrator.
 - Event_manager – delivers notifications about events to other application modules.

- Sntp_sender – sends notifications.
- Task manager – controls the start/stop sequence of other modules.
- Klms-postgres – a database storing application settings, statistics for reports, and metadata of objects in Backup. Metadata of objects in backup may be stored in a database that is stored externally (outside the application).
- Klms-control– a utility used to set application settings (task settings and message processing rules (see section "About message processing rules" on page [79](#)), view runtime statistics, manage Backup, and run tasks.

OPERATION ALGORITHM

The application runs according to the following algorithm:

1. The filter receives a message from the mail server and forwards it to the Scan Logic module.
2. The Scan Logic message scanning control module determines the rule by which the application will process the email message (see section "About message processing rules" on page [79](#)).
3. The application scans the message in accordance with the settings for the rule. If all scans are set to run in accordance with the rule settings, the application performs them in the following order:
 - a. Anti-Spam scan.
 - b. Anti-Phishing scan (see section "About Anti-Phishing email protection" on page [103](#)).
 - c. Content filtering (see section "About content filtering of messages" on page [107](#)).
 - d. Anti-Virus scan.
4. Based on the results of message scanning, Scan Logic adds a status tag at the beginning of the message subject (Subject field) and adds an information X-header (see section "About information X-headers" on page [86](#)) to the message header.
5. After all scans have been completed, depending on the status assigned to the message, the application performs an action (see section "About actions on objects" on page [83](#)) configured in the settings of the message processing rule. Infected objects are treated by default, and cured if possible.
6. After scanning and processing, Scan Logic forwards the message to the filter.
7. The filter forwards the processed message with notifications on the scan and disinfection results to the mail server.
8. The mail server delivers the message to local users or routes it to other mail servers.

INSTALLING AND REMOVING THE APPLICATION

This section contains step-by-step instructions for application installation and removal.

IN THIS SECTION:

Preparing to install.....	20
Upgrading from a previous version of the application.....	21
Installing the application.....	25
Preparing Kaspersky Security for operation.....	30
Preparing Kaspersky Security web interface for operation.....	44
Removing Kaspersky Security.....	50
Actions after removing Kaspersky Security.....	51

PREPARING TO INSTALL

Before installing the Kaspersky Security package:

- make sure that your computer meets hardware and software requirements (see section "Hardware and software requirements" on page [15](#));
- download the Kaspersky Linux Mail Security installation package in TGZ, TXZ, DEB, or RPM format from the website of an online store to your computer (see section "Distribution kit" on page [15](#));
- install the glibc package (64-bit operating systems require the 32-bit version of glibc).

Before installing Kaspersky Security on a computer running the Debian or Ubuntu operating system, you need to execute the following command: `# locale-gen en_US.UTF-8`.

The installation package for the Kaspersky Security web interface is required only if you want to manage the application through the browser.

Before you install the Kaspersky Security web interface package:

- make sure that your computer meets the hardware and software requirements.
- download the installation package for the Kaspersky Security web interface in .deb or .rpm format from the Online Shop (the installation package for the web interface is required only if you want to manage the application through the browser).
- install the following Apache modules: mod_ssl, mod_include, mod_dir, mod_expires (if not already installed) and enable them using the command: `# a2enmod` (if not already enabled).

```
# a2enmod ssl
```

```
# a2enmod include
# a2enmod dir
# a2enmod expires
```

For the localization packages to work correctly, the system has to support the corresponding languages.

For example, if you need to install the Russian localization package `klms-l10n-ru_<version_number>_i386.deb` under Debian GNU/Linux 6.0, make sure that the system supports the Russian language before installing it.

➤ To view the list of supported languages, execute the following command:

```
# locale -a
```

If the Russian language is not on this list, you have to install it.

➤ To install the Russian language, execute the following command:

```
# dpkg-reconfigure locales
```

You can now proceed to installing the `klms-l10n-ru_<version_number>_i386.deb` package.

Follow the same steps for any localization.

UPGRADING FROM A PREVIOUS VERSION OF THE APPLICATION

The process of upgrading Kaspersky Security 8.0 for Linux Mail Server from the previous version to Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1 includes several stages:

1. Installing the Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1 package (see section "Installing Kaspersky Security on top of the previous version" on page [22](#)) on top of the package with the previous version of Kaspersky Security 8.0 for Linux Mail Server.
2. Updating Kaspersky Security settings (see page [24](#)) using the application settings update script.
3. Installing the Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1 web interface package (see section "Installing Kaspersky Security web interface on top of the previous version" on page [23](#)) on top of the package with the previous version of the Kaspersky Security 8.0 for Linux Mail Server web interface.

Steps 1 and 3 can be performed simultaneously if Kaspersky Security and the application web interface are installed on the same mail server.

4. Updating Kaspersky Security web interface settings (see page [25](#)) using the application web interface settings update script.
5. Installing Kaspersky Security language packages (see section "Preparing to install" on page [20](#)) over the language packages of the previous application version.

After Kaspersky Security is upgraded, the threat detection statistics, reports, and objects in Backup and Anti-Spam Quarantine are preserved.

If localization packages were installed for the previous version of Kaspersky Security, before upgrading remove the localization packages by executing one of the following commands:

```
# rpm -e klms_<packagename> for a localization package in RPM format;
# dpkg -r klms_<packagename> for a localization package in DEB format;
# pkg_delete_<packagename> for a localization package of the FreeBSD operating system.
```

IN THIS SECTION:

Installing Kaspersky Security on top of the previous version.....	22
Installing the Kaspersky Security web interface on top of the previous version	23
Updating Kaspersky Security settings	24
Updating Kaspersky Security web interface settings.....	25

INSTALLING KASPERSKY SECURITY ON TOP OF THE PREVIOUS VERSION

This section describes the procedure for installing the Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1 package on top of the package with the previous version of Kaspersky Security 8.0 for Linux Mail Server on computers running under Linux and FreeBSD operating systems.

Installing Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1 on a computer running under the Linux operating system

- *To install Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1 from an RPM package on a 32-bit or 64-bit operating system, execute the following command:*

```
# rpm -U klms-<version_number>.i386.rpm
```

- *To install Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1 from a DEB package on a 32-bit operating system, execute the following command:*

```
# dpkg -i klms_<version_number>_i386.deb
```

- *To install Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1 from a DEB package on a 64-bit operating system, execute the following command:*

```
# dpkg --force-architecture -i klms_<version_number>_i386.deb
```

After running the command, the application is installed automatically.

Installing Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1 on a computer running under the FreeBSD operating system

Prior to installing Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1 on a computer running under the FreeBSD operating system, remove the previous version of Kaspersky Security 8.0 for Linux Mail Server.

- *To remove the previous version of Kaspersky Security 8.0 for Linux Mail Server, execute the following command:*

```
# pkg_delete klms_<version_number>
```

Do not run the klms-cleanup script after removing the previous version of Kaspersky Security 8.0 for Linux Mail Server, as doing so will erase the configured application settings.

- To install Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1 from a TGZ package on a 32-bit or 64-bit FreeBSD 8 operating system, execute the following command:

```
# pkg_add klms-<version_number>.tgz
```

- To install Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1 from a TXZ package on a 32-bit FreeBSD 9 operating system, execute the following command:

```
# pkg add klms-<version_number>.txz
```

- To install Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1 from a TXZ package on a 64-bit FreeBSD 9 operating system or a 32-bit or 64-bit FreeBSD 10 operating system, execute the following command:

```
# pkg add -f klms-<version_number>.txz
```

After running the command, the application is installed automatically.

After installing the application package, install the Kaspersky Security localization package (see section "Installing the Kaspersky Security localization package" on page [26](#)).

After installing Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1, run the Kaspersky Security settings update script (see section "Updating Kaspersky Security settings" on page [24](#)).

INSTALLING THE KASPERSKY SECURITY WEB INTERFACE ON TOP OF THE PREVIOUS VERSION

This section describes the procedure for installing the Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1 web interface package on top of the web interface package of the previous version of Kaspersky Security 8.0 for Linux Mail Server on computers running under Linux and FreeBSD operating systems.

Installing the Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1 web interface on a computer running under the Linux operating system

- To install the Kaspersky Security web interface from an RPM package on a 32-bit operating system, execute the following command:

```
# rpm -U klmsui-<version_number>.i386.rpm
```

- To install the Kaspersky Security web interface from an RPM package on a 64-bit operating system, execute the following command:

```
# rpm -U klmsui-<version_number>.x86_64.rpm
```

- To install the Kaspersky Security web interface from a DEB package on a 32-bit operating system, execute the following command:

```
# dpkg -i klmsui_<version_number>_i386.deb
```

- To install the Kaspersky Security web interface from a DEB package on a 64-bit operating system, execute the following command:

```
# dpkg -i klmsui_<version_number>_amd64.deb
```

After the command is executed, the application web interface is installed automatically.

Installing the Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1 web interface on a computer running under the FreeBSD operating system

Prior to installing the web interface of Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1 on a computer running under the FreeBSD operating system, remove the web interface of previous version of Kaspersky Security 8.0 for Linux Mail Server.

- *To remove the web interface of the previous version of Kaspersky Security 8.0 for Linux Mail Server, execute the following command:*

```
# pkg_delete klmsui-<version_number>
```

- *To install the web interface of Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1 on the FreeBSD 8 operating system, execute the following command:*

```
# pkg_add klmsui-<version_number>.tgz
```

- *To install the web interface of Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1 on the FreeBSD 9 operating system, execute the following command:*

```
# pkg add klmsui-<version_number>.txz
```

- *To install the web interface of Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1 on the FreeBSD 10 operating system, execute the following command:*

```
# pkg add -f klmsui-<version_number>.txz
```

After the command is executed, the application web interface is installed automatically.

After installing the web interface of Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1, run the Kaspersky Security web interface settings update script (see section "Updating the Kaspersky Security web interface settings" on page [25](#)).

UPDATING KASPERSKY SECURITY SETTINGS

After installing Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1, run the Kaspersky Security settings update script. The Kaspersky Security settings update script is included in the Kaspersky Security installation package.

The configured application settings and mail server integration settings are preserved on computers running under the Linux operating system after the previous version of Kaspersky Security 8.0 for Linux Mail Server is upgraded to Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1. You have to update the values of Kaspersky Security settings that have been added or modified in Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1.

The application has to be integrated with the mail server again manually or automatically on computers running under the FreeBSD operating system after the previous version of Kaspersky Security 8.0 for Linux Mail Server is upgraded to Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1.

- *To run the Kaspersky Security settings update script, execute the following command:*

- under Linux:

```
# /opt/kaspersky/klms/bin/klms-upgrade.pl
```

- under FreeBSD:

```
# /usr/local/bin/klms-upgrade.pl
```

The script prompts you to specify the values of Kaspersky Security settings one step at a time.

When the previous version of Kaspersky Security 8.0 for Linux Mail Server is upgraded to Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1, the settings cannot be updated automatically using a file with saved answers.

UPDATING KASPERSKY SECURITY WEB INTERFACE SETTINGS

After installing the web interface of Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1, run the Kaspersky Security web interface settings update script. The Kaspersky Security web interface settings update script is included in the Kaspersky Security web interface installation package.

➤ To run the Kaspersky Security web interface settings update script, execute the following command:

- under Linux:


```
# /opt/kaspersky/klmsui/bin/klmsui-upgrade.pl
```
- under FreeBSD:


```
# /usr/local/bin/klmsui-upgrade.pl
```

When the web interface of the previous version of Kaspersky Security 8.0 for Linux Mail Server is upgraded to Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1, the settings cannot be updated automatically using a file with saved answers.

INSTALLING THE APPLICATION

The installation includes several steps:

1. Installing the Kaspersky Security package" on page [25](#)).

You must have root privileges to initiate installation of the Kaspersky Security package.

2. Installing the Kaspersky Security web interface package (see section "Installing the Kaspersky Security web interface package on the same computer with Kaspersky Security" on page [27](#)).

Installation of this package is required if you want to manage the application through the browser. The Kaspersky Security web interface package can be installed on the same computer with the Kaspersky Security package or on a separate computer.

IN THIS SECTION:

Installing the Kaspersky Security package	25
Installing the Kaspersky Security localization package	26
Installing the Kaspersky Security web interface package on the same computer with Kaspersky Security	27
Installing the Kaspersky Security web interface package on a separate computer	28

INSTALLING THE KASPERSKY SECURITY PACKAGE

Kaspersky Security is distributed in packages of TGZ, TXZ, DEB, and RPM formats.

- To install Kaspersky Security from an .rpm package, execute the following command:

```
# rpm -i klms-<version_number>.i386.rpm
```

- To install Kaspersky Security from a .deb package on a 32-bit operating system, execute the following command:

```
# dpkg -i klms_<version_number>_i386.deb
```

- To install Kaspersky Security from a .deb package on a 64-bit operating system, execute the following command:

```
# dpkg --force-architecture -i klms_<version_number>_i386.deb
```

- To install Kaspersky Security from a package of TGZ format on a 32-bit or 64-bit FreeBSD 8 operating system, execute the following command:

```
# pkg_add klms-<version_number>.tgz
```

- To install Kaspersky Security from a TXZ package on a 32-bit FreeBSD 9 operating system, execute the following command:

```
# pkg add klms-<version_number>.txz
```

- To install Kaspersky Security from a TXZ package on a 64-bit FreeBSD 9 operating system or a 32-bit or 64-bit FreeBSD 10 operating system, execute the following command:

```
# pkg add -f klms-<version_number>.txz
```

After the command is executed, the application is installed automatically.

After installing the application package, install the Kaspersky Security localization package (see section "Installing the Kaspersky Security localization package" on page [26](#)).

After installing Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1, run the Kaspersky Security settings update script (see section "Updating Kaspersky Security settings" on page [24](#)).

INSTALLING THE KASPERSKY SECURITY LOCALIZATION PACKAGE

This section describes the procedure for installing the localization package of Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1 on computers running under Linux and FreeBSD operating systems.

Installing the Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1 localization package on a computer running under the Linux operating system

- To install localization package of RPM format on a 32-bit or 64-bit operating system, execute the following command:

```
# rpm -i klms_ru-<version_number>.noarch.rpm
```

- To install a localization package from a DEB package on a 32-bit or 64-bit operating system, execute the following command:

```
# dpkg -i klms-110n-ru_<version_number>_all.deb
```

Installing the Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1 localization package on a computer running under the FreeBSD operating system

- To install localization package of TGZ format on a 32-bit or 64-bit FreeBSD 8 operating system, execute the following command:

```
# pkg_add klms_ru-<version_number>.tgz
```

- To install a localization package of TXZ format on a 32-bit FreeBSD 9 operating system, execute the following command:

```
# pkg add klms_ru-<version_number>.txz
```

- To install a localization package of TXZ format on a 64-bit FreeBSD 9 operating system or a 32-bit or 64-bit FreeBSD 10 operating system, execute the following command:

```
# pkg add -f klms_ru-<version_number>.txz
```

After installing the localization package, you have to run the Kaspersky Security settings update script (see section "Updating Kaspersky Security settings" on page [24](#)).

INSTALLING THE KASPERSKY SECURITY WEB INTERFACE PACKAGE ON THE SAME COMPUTER WITH KASPERSKY SECURITY

The Kaspersky Security web interface can be installed from DEB, RPM, TGZ or TXZ packages on the same computer with Kaspersky Security.

- To install the web interface from a .deb package on a 32-bit operating system, execute the following command:

```
# rpm -i klmsui-<version_number>.i386.rpm
```

- To install the web interface from a .deb package on a 64-bit operating system, execute the following command:

```
# rpm -i klmsui-<version_number>.x86_64.rpm
```

- To install the web interface from a .deb package on a 32-bit operating system, execute the following command:

```
# dpkg -i klmsui_<version_number>_i386.deb
```

- To install the web interface from a .deb package on a 64-bit operating system, execute the following command:

```
# dpkg -i klmsui_<version_number>_amd64.deb
```

- To install the web interface from a TGZ package on the FreeBSD 8 operating system, execute the following command:

```
# pkg_add klmsui-<version_number>.tgz
```

- To install the web interface from a TXZ package on the FreeBSD 9 operating system, execute the following command:

```
# pkg add klmsui-<version_number>.txz
```

- To install the web interface from a TXZ package on the FreeBSD 10 operating system, execute the following command:

```
# pkg add -f klmsui-<version_number>.txz
```

After installing the web interface of Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1, run the Kaspersky Security web interface settings update script (see section "Updating the Kaspersky Security web interface settings" on page [25](#)).

INSTALLING THE KASPERSKY SECURITY WEB INTERFACE PACKAGE ON A SEPARATE COMPUTER

The Kaspersky Security web interface can be installed on a separate computer. To configure interaction between Kaspersky Security and the web interface:

1. Install the Kaspersky Security web interface package (see section "Installing the Kaspersky Security web interface package" on page [28](#)).
2. Configure the Facade module supporting application interaction with utilities and administration systems (see section "Configuring the Facade module supporting application interaction with utilities and administration systems" on page [29](#)).
3. Configure the connection of the Kaspersky Security web interface to an Apache server (see section "Configuring the connection of the Kaspersky Security web interface to an Apache server" on page [29](#)).

After installing the web interface of Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 Critical Fix 1, run the Kaspersky Security web interface settings update script (see section "Updating the Kaspersky Security web interface settings" on page [25](#)).

IN THIS SECTION:

Installing the Kaspersky Security web interface package.....	28
Configuring the Facade module supporting application interaction with utilities and administration systems.....	29
Configuring the connection of the Kaspersky Security web interface to an Apache server	29

INSTALLING THE KASPERSKY SECURITY WEB INTERFACE PACKAGE

The Kaspersky Security web interface can be installed from DEB, RPM, TGZ or TXZ packages.

- *To install the web interface from a .deb package on a 32-bit operating system, execute the following command:*

```
# rpm -i klmsui-<version_number>.i386.rpm
```

- *To install the web interface from a .deb package on a 64-bit operating system, execute the following command:*

```
# rpm -i klmsui-<version_number>.x86_64.rpm
```

- *To install the web interface from a .deb package on a 32-bit operating system, execute the following command:*

```
# dpkg -i klmsui_<version_number>_i386.deb
```

- *To install the web interface from a .deb package on a 64-bit operating system, execute the following command:*

```
# dpkg -i klmsui_<version_number>_amd64.deb
```

- *To install the web interface from a TGZ package on the FreeBSD 8 operating system, execute the following command:*

```
# pkg_add klmsui-<version_number>.tgz
```

- *To install the web interface from a TXZ package on the FreeBSD 9 operating system, execute the following command:*

```
# pkg add klmsui-<version_number>.txz
```

- To install the web interface from a TXZ package on the FreeBSD 10 operating system, execute the following command:

```
# pkg add -f klmsui-<version_number>.txz
```

CONFIGURING THE FACADE MODULE SUPPORTING APPLICATION INTERACTION WITH UTILITIES AND ADMINISTRATION SYSTEMS

- To configure the Facade module that enables the application to interact with utilities and administration systems:

1. Export the Facade task settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--get-settings <Facade task ID> -f <name of the settings file> or
```

```
# /opt/kaspersky/klms/bin/klms-control \
--get-settings Facade -n -f <name of the settings file>
```

2. Open the XML file to edit the task settings.
3. In the <port> </port> section, specify the port for interaction with the Kaspersky Security web interface.
4. In the <interfaceAddress> </interfaceAddress> section, specify the IP address of the computer where the Kaspersky Security web interface is installed.
5. Save the changes made.
6. Import the Facade task settings from an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--set-settings <Facade task ID> -f <name of the settings file>
```

or

```
# /opt/kaspersky/klms/bin/klms-control \
--get-settings Facade -n -f <name of the settings file>
```

CONFIGURING THE CONNECTION OF THE KASPERSKY SECURITY WEB INTERFACE TO AN APACHE SERVER

- To configure the connection of the *Kaspersky Security web interface* to an Apache web server on a computer running a Linux operating system:

1. Open the /etc/apache2/conf.d/klmsui.conf file with Kaspersky Security web interface settings.
2. Specify the IP address of the mail server and the port of the Facade module in the line FastCgiExternalServer /opt/kaspersky/klmsui/share/htdocs/cgi-bin/klwi -host 127.0.0.1:2711.

- To configure the connection of the *Kaspersky Security web interface* to an Apache web server on a computer running a Debian operating system:

1. Open the /etc/httpd/conf.d/klmsui.conf file with Kaspersky Security web interface settings.
2. Specify the IP address of the mail server and the port of the Facade module in the line FastCgiExternalServer /opt/kaspersky/klmsui/share/htdocs/cgi-bin/klwi -host 127.0.0.1:2711.

- To configure the connection of the *Kaspersky Security web interface* to an Apache web server on a computer running a FreeBSD operating system:
 1. Open the `/usr/local/etc/apache24/Includes/klmsui.conf` file with Kaspersky Security web interface settings.
 2. Specify the IP address of the mail server and the port of the Facade module in the line `FastCgiExternalServer /opt/kaspersky/klmsui/share/htdocs/cgi-bin/klwi -host 127.0.0.1:2711`.

PREPARING KASPERSKY SECURITY FOR OPERATION

After the installation, Kaspersky Security needs to be configured.

Kaspersky Security initial configuration consists of a series of steps in the form of a script. The initial configuration script for Kaspersky Security is included in the installation package.

Initial configuration of Kaspersky Security settings can be performed manually or automatically using a file with saved answers.

IN THIS SECTION:

Starting initial configuration of Kaspersky Security manually	30
Starting automatic initial configuration of Kaspersky Security	39

STARTING INITIAL CONFIGURATION OF KASPERSKY SECURITY MANUALLY

- To start initial configuration of Kaspersky Security manually, execute the following command:

- under Linux:

```
# /opt/kaspersky/klms/bin/klms-setup.pl
```

- under FreeBSD:

```
# /usr/local/bin/klms-setup.pl
```

The initial configuration script prompts you to specify information needed to configure Kaspersky Security one step at a time.

IN THIS SECTION:

Step 1. Selecting the language for viewing the License Agreement and the Kaspersky Security Network Statement	31
Step 2. Reviewing the License Agreement.....	31
Step 3. Participating in Kaspersky Security Network.....	32
Step 4. Selecting the backup directory	33
Step 5. Backup connection settings	33
Step 6. Selecting the socket.....	33
Step 7. Using the Kaspersky Security web interface	34
Step 8. Selecting the TCP port for interaction with the Kaspersky Security web interface	34
Step 9. Assigning a password to access the web interface	34
Step 10. Selecting the type of integration with the mail server	35
Step 11. Configuring the proxy server settings.....	38
Step 12. Adding a key	38
Step 13. Updating the databases	39

STEP 1. SELECTING THE LANGUAGE FOR VIEWING THE LICENSE AGREEMENT AND THE KASPERSKY SECURITY NETWORK STATEMENT

At this step you can select the language in which the text of the License Agreement and the Kaspersky Security Network Statement will be displayed. To do so, enter the number of the relevant language from the proposed list.

Language selection is available if additional localization packages are installed in the operating system. If no additional localization packages are installed, the text of the License Agreement and the Kaspersky Security Network Statement are displayed in the English language.

STEP 2. REVIEWING THE LICENSE AGREEMENT

At this step, you have to accept or decline the terms of the License Agreement.

➤ *To view the License Agreement:*

1. Press **ENTER**.

The text of the License Agreement is displayed. To move through the text, use the cursor control keys or the **B** and **F** keys (to move backward or forward one screen, respectively). To view help, press the **H** key.

2. Press the **Q** key to exit the viewing mode.
3. Do one of the following:
 - To accept the License Agreement, enter yes (or y).
 - To reject the License Agreement, enter no (or n).

4. Press **ENTER**.

If you rejected the License Agreement, initial configuration is discontinued.

You can also view the text of the License Agreement by opening the relevant file. The file with the text of the End User License Agreement is located at the following path:

- for the application installed on a computer running under Linux: /opt/kaspersky/klms/share/doc/LICENSE, for the web interface: /opt/kaspersky/klmsui/share/doc/LICENSE;
- for the application installed on a computer running under FreeBSD: /usr/local/share/doc/klms/LICENSE, for the web interface: /opt/kaspersky/klmsui/share/doc/LICENSE.

STEP 3. PARTICIPATING IN KASPERSKY SECURITY NETWORK

At this step you need to accept or decline participation in Kaspersky Security Network (KSN).

Kaspersky Security Network (KSN) is an infrastructure of online services that provides access to the online Kaspersky Lab Knowledge Base, which contains information about the reputation of files, web resources, and software. Data from Kaspersky Security Network ensures faster response by Kaspersky Security to new threats, improves the performance of some protection components, and reduces the risk of false positives.

Thanks to users who participate in Kaspersky Security Network, Kaspersky Lab is able to promptly gather information about types and sources of new threats, develop solutions for neutralizing them, and minimize the number of false positives. Participation in Kaspersky Security Network also lets you access reputation statistics for applications and websites.

If you participate in Kaspersky Security Network, Kaspersky Security performance statistics are submitted to Kaspersky Lab. These statistics are sent automatically.

No personal data is collected, processed, or stored.

Participation in Kaspersky Security Network is voluntary. You are prompted to decide during initial configuration of Kaspersky Security, but you can change your decision at any time later.

► *To accept or reject participation in Kaspersky Security Network:*

1. Press **ENTER**.

The text of the Kaspersky Security Network Statement opens. To move through the text, use the cursor control keys or the **B** and **F** keys (to move backward or forward one screen, respectively). To view help, press the **H** key.

2. Press the **Q** key to exit the viewing mode.
3. Do one of the following:
 - To accept the terms of the Kaspersky Security Network Statement, type yes (or y).
 - To reject the terms of the Kaspersky Security Network Statement, type no (or n).
4. Press **ENTER**.

To be able to access KSN, allow outbound TCP connections through port 443 on the computer where Kaspersky Security is installed.

You can also view the text of the Kaspersky Security Network Statement straight from the file. The file with the text of the Kaspersky Security Network Statement is located at the following path:

- for the application installed on a computer running under Linux: `/opt/kaspersky/klms/share/doc/LICENSE_ksn`.
- for the application installed on a computer running under FreeBSD: `/usr/local/share/doc/klms/LICENSE_ksn`.

STEP 4. SELECTING THE BACKUP DIRECTORY

At this step, you can specify the directory where backup copies of mail messages processed by Kaspersky Security are to be stored, or select the default directory.

➤ *To specify the backup directory:*

1. Specify the full path to the directory for storing the backup copies of mail messages.
2. Press **ENTER**.

➤ *To accept the default backup directory,*

press **ENTER**.

The default path is `/var/opt/kaspersky/klms/backup`.

STEP 5. BACKUP CONNECTION SETTINGS

At this step, you can specify the settings for connecting the application to Backup database or select the default connection settings.

You can use an external database as Backup. Kaspersky Security supports PostgreSQL databases of version 9.1 or later.

➤ *To specify Backup connection settings:*

1. Specify Backup connection settings in the following format:
`[dbname=<database name> user=<user name> host=<database socket>]`
2. Press **ENTER**.

➤ *To select default Backup connection settings,*

press **ENTER**.

The proposed default connection settings are as follows: `[dbname=backup user=kluser host=/var/run/klms]`.

STEP 6. SELECTING THE SOCKET

During this step, you need to specify the socket that Scan Logic uses to listen for incoming connections from the filter.

➤ *To specify the socket:*

1. Specify the IP address and port number or the NIX™ socket that Scan Logic will use to listen for incoming connections as follows: `inet:<port>@<IP address>` (for a network socket) or `unix:<path to UNIX socket>` (for UNIX sockets).

A UNIX socket is proposed by default: `unix: /var/run/klms/klms_scanner_sock`

2. Press **ENTER**.

STEP 7. USING THE KASPERSKY SECURITY WEB INTERFACE

At this step, you can specify whether or not you want to use the Kaspersky Security web interface.

- *To use the Kaspersky Security web interface,*
type yes (or y) and press **Enter**.

The Kaspersky Security web interface is disabled by default.

STEP 8. SELECTING THE TCP PORT FOR INTERACTION WITH THE KASPERSKY SECURITY WEB INTERFACE

This step is displayed if you enabled the Kaspersky Security web interface at the previous step.

At this step, you can specify the number of the TCP port to be used by Kaspersky Security for interaction with the web interface.

- *To specify the number of the TCP port for interaction with the Kaspersky Security web interface,*
enter the port number and press **ENTER**.

The default option is 2711.

STEP 9. ASSIGNING A PASSWORD TO ACCESS THE WEB INTERFACE

At this step, you can specify the Administrator account password for access to the web-based interface of the application.

If you do not specify a password for access to the web interface at this step, you can do so later using the utility `/opt/kaspersky/klms/bin/klms-control --set-web-admin-password`.

- *To enter a password for access to the web-interface, perform the following steps:*

1. Enter yes.
The default option is no.
2. Press **ENTER**.
3. Specify the password for the Administrator account.

The password must be at least eight characters long and must meet at least three of the following conditions:

- Contain at least one upper-case character
 - Contain at least one lower-case character
 - Contain at least one special character
 - Contain at least one numeral
4. Confirm the password.
 5. Press **ENTER**.

STEP 10. SELECTING THE TYPE OF INTEGRATION WITH THE MAIL SERVER

At this step you need to run the setting scenario.

➤ *To run the setting scenario execute the following command:*

```
# /opt/kaspersky/klms/bin/klms-setup.pl
```

After that you need to select the type of integration of Kaspersky Security with the mail server: automatic or manual.

Kaspersky Security can be integrated with the following mail servers:

- Exim.
- Postfix.
- Sendmail.
- QMail.

➤ *To perform automatic integration of Kaspersky Security with the mail server:*

1. Enter the number specified next to the name of the mail server.
2. Press **ENTER**.
3. Depending on which server you selected at step 1 of the instructions, perform the actions described in the sections that follow:
 - Integration with Sendmail server (see page [36](#));
 - Integration with Exim server (see page [36](#));
 - Integration with Postfix server (see page [37](#));
 - Integration with QMail server (see page [36](#)).

If you choose not to integrate the application with the mail server at this step automatically, you can perform manual integration later (see section "Manual integration of Kaspersky Linux Mail Security with mail servers and Amavis interface" on page [53](#)).

➤ *To decline automatic integration of Kaspersky Security with the mail server:*

1. Enter the number specified next to the option Manual integration.
2. Press **ENTER**.

IN THIS SECTION:

Integrating with Qmail server.....	36
Integrating with Sendmail server	36
Integrating with Exim mail server.....	36
Integrating with Postfix mail server	37

INTEGRATING WITH QMAIL SERVER

The application performs integration with the QMail server automatically.

If the initial configuration script cannot find the path to the directory containing the qmail executable file during installation, perform the following instructions.

➤ *To specify the path to the directory containing the qmail executable file:*

1. Specify the full path to the directory containing the qmail executable file.
2. Press **ENTER**.

If the initial configuration script cannot find the standard qmail user account during installation, specify the user account with the rights to start the qmail service.

➤ *To specify the qmail user account:*

1. Specify the user account with the rights to start the qmail service.
2. Press **ENTER**.

INTEGRATING WITH SENDMAIL SERVER

➤ *To integrate Kaspersky Security with Sendmail:*

1. Select the method for integration with the Sendmail server:
 - If you want changes to be made to the .mc file and then use that file to create the .cf file during integration, enter 1.
 - If you want changes to be made to the .cf configuration file during integration, enter 2.

The default option is 1.

2. Press **ENTER**.
3. Specify the IP address and port number or the UNIX socket that the filter will use to listen for incoming connections as follows: inet:<port>@<IP address> (for network sockets) or unix:<path to UNIX socket> (for UNIX sockets).

The UNIX socket `unix:/var/opt/kaspersky/klms/klms_milter` is proposed by default.

4. Press **ENTER**.
5. Select the action that the Sendmail server must take on the message in case of filter error:
 - If you want Sendmail to accept the message without scanning, enter 2 to select the accept option.
 - If you want Sendmail to reject the message, enter 1 to select the reject option.
 - If you want Sendmail to notify the sender of the temporary inability to accept the message, enter 3 to select the tempfail option.

The default option is tempfail.

6. Press **ENTER**.

INTEGRATING WITH EXIM MAIL SERVER

➤ *To integrate Kaspersky Security with Exim:*

1. Select the type of integration with the Exim mail server:

- If you want to perform a before-queue integration of Kaspersky Security with Exim using dynamic linking (dlfunc), enter 1.

Make sure that Exim supports dlfunc-based content filtering. To do so, run the `exim -bV` command. The following represents a positive result: `Expand_dfunc`.

- If you want to perform after-queue integration of Kaspersky Security with Exim via SMTP by rerouting, enter 2.

The default option is 1 (if Exim supports dlfunc-based content filtering).

2. Press **ENTER**.
3. If your choice is 2, do the following:
 - a. Specify the port number where the `smtp_proxy` filter will listen for messages from the mail server.
The default option is 10025.
 - b. Press **ENTER**.
 - c. Specify the port number where the message will go after being scanned.
The default option is 10026.
 - d. Press **ENTER**.

INTEGRATING WITH POSTFIX MAIL SERVER

➤ *To integrate Kaspersky Security with Postfix:*

1. Select the type of integration with the Postfix mail server:
 - To perform before-queue integration of Kaspersky Security with Postfix, enter 1.
 - To perform after-queue integration of Kaspersky Security with Postfix, enter 2.
 - To integrate Kaspersky Security with Postfix using Milter functions, enter 3.

The default option is 3.
2. Press **ENTER**.
3. Specify the IP address and port number or UNIX socket that the `smtp_proxy` filter will use to listen for messages from the mail server as follows: `inet:<port>@<IP address>` (for network sockets) or `unix:<path to UNIX socket>` (for UNIX sockets).
 - If you selected 1 at Step 1, the UNIX socket `unix` is proposed by default.
 - If you selected 2 at Step 2, only the network socket in `inet:<port>@<IP address>` format is available. The network socket `inet:10025@127.0.0.1` is proposed by default.
 - If you selected 3 at Step 1 of the wizard, the UNIX socket `unix:/var/run/klms/klms_milter_sock` is proposed by default.
4. Press **ENTER**.
5. If you entered 2 at Step 1, specify the port number to which the message will be forwarded after being scanned.
The default option is 10026.

6. Press **ENTER**.
7. If you entered 3 at Step 1, select the action that Postfix must take on the message in case of filter error:
 - If you want Postfix to accept the message without scanning, enter 2 to select the accept option.
 - If you want Postfix to reject the message, enter 1 to select the reject option.
 - If you want Postfix to reply to the message sender, enter 3 to select the tempfail option.

The default option is tempfail.
8. Press **ENTER**.

STEP 11. CONFIGURING THE PROXY SERVER SETTINGS

If you access the Internet via a proxy server, you can configure it at this step. An Internet connection is required to download the Anti-Virus and Anti-Spam databases from Kaspersky Lab's update servers. If you choose not to configure the proxy server at this step, you can configure the proxy server later (see section "Configuring the proxy server" on page [116](#)) without using the initial configuration script.

If you do not use a proxy server to connect to the Internet, press **ENTER**.

➤ *To specify that a proxy server should be used,*

type yes (or y) and press **Enter**.

You will be prompted to specify the FQDN (fully qualified domain name) and port or IP address and port of the proxy server.

➤ *To specify the IP address and port of the proxy server,*

enter the proxy server address in the IP_address_of_proxy_server:port format and press **Enter**.

➤ *To specify the FQDN and port of the proxy server,*

enter the proxy server FQDN in FQDN_of_proxy_server:port format and press **Enter**.

You will be prompted to choose whether or not authentication is required upon connecting to the proxy server:

- If authentication is not required, type no (or n) and press **Enter**.
- If authentication is required, type yes (or y) and press **Enter**.

➤ *To specify the authentication login and password:*

1. Enter the proxy server login name and press **Enter**.

You will be prompted to set a password.

2. Enter the password for accessing the proxy server and press **Enter**.

The proxy server will be configured with authentication.

STEP 12. ADDING A KEY

At this step, you can specify the path to the key file. The key file contains information used to verify the right to use Kaspersky Linux Mail Security and calculate the application usage time (see section "About key file" on page [73](#)). You can add a key during initial configuration of Kaspersky Linux Mail Security or add it later (see section "Adding a key" on page [74](#)) without using the initial configuration script.

➤ *To add a key during initial configuration:*

1. Specify the full path to the key file.
2. Press **ENTER**.

➤ *To not add a key:*

1. Enter a blank line.
2. Press **ENTER**.

If no key is added, Kaspersky Security does not protect the computer.

STEP 13. UPDATING THE DATABASES

At this step, Anti-Virus and Anti-Spam databases of the application are updated automatically.

The database update schedule is configured by default, with the application databases updated once every 5 minutes.

STARTING AUTOMATIC INITIAL CONFIGURATION OF KASPERSKY SECURITY

Initial configuration of Kaspersky Security can be performed in automatic mode.

A file with saved answers can be created using the `--create-auto-install=<full path to the configuration file>` parameter when running the initial application configuration script.

Possible values should be typed using lower-case characters.

➤ *To start initial configuration of Kaspersky Security in automatic mode, execute the following command:*

- under Linux:

```
/opt/kaspersky/klms/bin/klms-setup.pl \
```

```
--auto-install=<full path to the configuration file with the saved answers>
```

- under FreeBSD:

```
/usr/local/bin/klms-setup.pl \
```

```
--auto-install=<full path to the configuration file with the saved answers>
```

The settings of the configuration file with answers are given in the following table.

Table 2. Parameters of the Kaspersky Security initial configuration file with answers

SETTING	DESCRIPTION	AVAILABLE VALUES
EULA_AGREED	Required setting. Acceptance of the terms of the License agreement.	yes
KSN_AGREED	Required setting. Acceptance of the terms of the Kaspersky Security Network Statement.	yes no
KEY_FILE	Optional setting. Path to the key file.	<path> Case sensitive.
BACKUP_CUSTOM_PATH	Optional setting. Custom path to Backup. If the line with this setting is skipped, the default path to Backup is used (/var/opt/kaspersky/klms/backup).	<path> Case sensitive.
BACKUP_CUSTOM_DB	Optional setting. Custom path for connecting to the Backup database. If the line with this setting is skipped, the default setting is used (dbname=backup user=kluser host=/var/run/klms). Kaspersky Security supports PostgreSQL databases of version 9.1 or later.	<connection_string> Case sensitive.
SCANNER_SOCKET	Optional setting. Socket used by the scanner. If the line with this parameter is skipped, the parameter retains its default value (unix:/var/run/klms/klms_scanner_sock).	inet:port@IP unix:<path_to_socket> Case sensitive.
MTA	Required setting. Type of integration with the mail server.	postfix exim sendmail qmail manual
POSTFIX_INTEGRATION_TYPE	Required setting. Type of integration with the Postfix mail server.	prequeue afterqueue milter
POSTFIX_MILTER_SOCKET	Optional setting. Socket used for integration with the Postfix mail server via the Milter protocol. If the line with this setting is skipped, the setting takes the value inet:10025@127.0.0.1. The setting is ignored if: <ul style="list-style-type: none"> • The value of the MTA setting is not equal to "postfix". • The value of the POSTFIX_INTEGRATION_TYPE setting is not equal to "milter". 	inet:port@IP unix:<path_to_socket> Case sensitive.

SETTING	DESCRIPTION	AVAILABLE VALUES
POSTFIX_SMTP_PROXY_SOCKET	<p>Optional setting.</p> <p>Socket used for integration with the Postfix mail server with "after-queue" and "before-queue" integration types.</p> <p>If the line with this setting is skipped, the setting takes the value <code>inet:10025@127.0.0.1</code>.</p> <p>The setting is ignored if:</p> <ul style="list-style-type: none"> The value of the MTA setting is not equal to "postfix". The value of the POSTFIX_INTEGRATION_TYPE setting is equal to "milter". 	<p><code>inet:port@IP unix:<path_to_socket></code></p> <p>Case sensitive.</p>
POSTFIX_FORWARD_PORT	<p>Optional setting.</p> <p>TCP port for forwarding scanned messages in the case of integration with the Postfix mail server.</p> <p>If the line with this setting is skipped, the setting takes the value "10026".</p> <p>The setting is ignored if the value of the MTA setting is not equal to "postfix".</p>	<p><port></p>
POSTFIX_FAILTYPE	<p>Optional setting.</p> <p>Default action on a message in the case of integration with the Postfix mail server via the Milter protocol.</p> <p>If the line with this setting is skipped, the setting takes the value "Tempfail".</p> <p>The setting is ignored if:</p> <ul style="list-style-type: none"> The value of the MTA setting is not equal to "postfix". The value of the POSTFIX_INTEGRATION_TYPE setting is not equal to "milter". 	<p>accept reject tempfail</p>
EXIM_INTEGRATION_TYPE	<p>The setting is required if the MTA value is equal to "exim".</p> <p>Type of integration with the Exim mail server.</p> <p>If the line with this setting is skipped, the setting takes the value "dlfunc" (if the Exim version has been compiled with support of dynamic linking).</p> <p>The setting is ignored if the value of the MTA setting is not equal to "exim".</p>	<p>dlfunc afterqueue</p>

SETTING	DESCRIPTION	AVAILABLE VALUES
EXIM_FORWARD_PORT	<p>Optional setting.</p> <p>TCP port for forwarding scanned messages in the case of integration with the Exim mail server.</p> <p>If the line with this setting is skipped, the setting takes the value "10026".</p> <p>The setting is ignored if the value of the MTA setting is not equal to "exim".</p>	<port>
EXIM_FILTER_PORT	<p>Optional setting.</p> <p>Port to be monitored by the scanner when filtering messages arriving from the Exim mail server.</p> <p>If the line with this setting is skipped, the setting takes the value "10025".</p> <p>The setting is ignored if the value of the MTA setting is not equal to "exim".</p>	<port>
SENDMAIL_USES_MC	<p>Optional setting.</p> <p>Enables the option to edit or compile a file with the .mc extension, or edit a file with the .cf extension.</p> <p>If the line with this setting is skipped, the setting takes the value "1".</p> <p>The setting is ignored if the value of the MTA setting is not equal to "sendmail".</p>	0 1
SENDMAIL_MILTER_SOCKET	<p>Optional setting.</p> <p>Socket used for integration with the Sendmail mail server via the Milter protocol.</p> <p>If the line with this setting is skipped, the setting takes the value inet:10025@127.0.0.1.</p> <p>The setting is ignored if:</p> <ul style="list-style-type: none"> • The value of the MTA setting is not equal to "sendmail". • The value of the SENDMAIL_USES_MC setting is not equal to 1. 	inet:port@IP unix:<path_to_socket> Case sensitive.

SETTING	DESCRIPTION	AVAILABLE VALUES
SENDMAIL_FAILTYPE	<p>Optional setting.</p> <p>Default action on a message in the case of integration with the Sendmail mail server via the Milter protocol.</p> <p>If the line with this setting is skipped, the setting takes the value "tempfail".</p> <p>The setting is ignored if:</p> <ul style="list-style-type: none"> • The value of the MTA setting is not equal to "sendMail". • The value of the SENDMAIL_USES_MC setting is not equal to 1. 	accept reject tempfail
QMAIL_BIN_DIR	<p>Optional setting.</p> <p>Path to the Qmail directory.</p> <p>If the line with this setting is skipped, the setting takes the value "var/qmail/bin".</p> <p>The setting is ignored if the value of the MTA setting is not equal to "qmail".</p>	<p><path></p> <p>Case sensitive.</p>
QMAIL_USER	<p>Optional setting. The default value is "qmaild".</p> <p>Specifies the user login for the Qmaild service.</p> <p>The line with the setting is ignored if the value of the MTA setting is not equal to "qmail".</p>	<p><login></p> <p>Case sensitive.</p>
USE_UI	<p>Optional setting.</p> <p>Enables the option to use the web interface for managing the application.</p> <p>If the line with this setting is skipped, the setting takes the value "no".</p>	yes no
WEB_UI_PORT	<p>Optional setting.</p> <p>TCP port for Kaspersky Security interaction with the Apache server.</p> <p>If the line with this setting is skipped, the setting takes the value "2711".</p> <p>The setting is ignored if the value of the USE_UI setting is equal to "no".</p>	<port>
WEB_UI_IFACE_ADDR	<p>Optional setting.</p> <p>Specifies the IP address of the host on which the Kaspersky Security web interface is installed.</p> <p>The setting is ignored if the value of the USE_UI setting is equal to "no".</p>	

SETTING	DESCRIPTION	AVAILABLE VALUES
WEB_PASSWORD	<p>Optional setting.</p> <p>Administrator password for accessing the web interface of the application.</p> <p>If the line with this setting is skipped, the Administrator password is not specified.</p> <p>If the password specified in the line is not subject to validation, the Administrator password is not specified.</p> <p>The password will not be saved in the file with answers if this password as specified during the execution of the klms-setup.pl script.</p>	<p><password></p> <p>Case sensitive.</p>

PREPARING KASPERSKY SECURITY WEB INTERFACE FOR OPERATION

After Kaspersky Security web interface has been installed, you need to perform an initial configuration.

Initial configuration of the Kaspersky Security web interface consists of a series of steps in the form of a script for the user's convenience. The initial configuration script should be started after the Kaspersky Security web interface has been installed. The initial configuration script for the Kaspersky Security web interface is included in the installation package.

Initial configuration of the web interface of Kaspersky Security can be performed manually or automatically.

IN THIS SECTION:

Starting initial configuration of Kaspersky Security web interface manually	44
Starting automatic initial configuration of the web interface of Kaspersky Security	48

STARTING INITIAL CONFIGURATION OF KASPERSKY SECURITY WEB INTERFACE MANUALLY

➤ To start initial configuration of the Kaspersky Security web interface manually, execute the following command:

- under Linux:


```
# /opt/kaspersky/klmsui/bin/klmsui-setup.pl
```
- under FreeBSD:


```
# /usr/local/bin/klmsui-setup.pl
```

The Administrator account is used for access to the Kaspersky Security web-interface. The password for this account is defined during initial configuration of Kaspersky Security (see section "Step 9. Assigning a password to access the web interface" on page [34](#)).

The Kaspersky Security web interface initial configuration script then prompts you to specify information one step at a time.

IN THIS SECTION:

Step 1. Selecting the License Agreement language.....	45
Step 2. Reviewing the License Agreement.....	45
Step 3. Selecting an Apache web server.....	46
Step 4. Selecting an Apache server virtual host.....	46
Step 5. Selecting a socket to interact with Kaspersky Security	47
Step 6. Selecting a certificate to access the web interface.....	47

STEP 1. SELECTING THE LICENSE AGREEMENT LANGUAGE

At this step you can select the language in which the text of the License Agreement will be displayed. To do so, enter the number of the relevant language from the proposed list.

Language selection is available if additional localization packages are installed in the operating system. If no additional localization packages have been installed, the text of the License Agreement is displayed in English.

STEP 2. REVIEWING THE LICENSE AGREEMENT

At this step, you have to accept or decline the terms of the License Agreement.

➔ *To view the License Agreement:*

1. Press **ENTER**.

The text of the License Agreement is displayed. To move through the text, use the cursor control keys or the **B** and **F** keys (to move backward or forward one screen, respectively). To view help, press the **H** key.

2. Press the **Q** key to exit the viewing mode.
3. Do one of the following:
 - To accept the License Agreement, enter yes (or y).
 - To reject the License Agreement, enter no (or n).
4. Press **ENTER**.

If you rejected the License Agreement, initial configuration is discontinued.

You can also view the text of the License Agreement by opening the relevant file. The file with the text of the End User License Agreement is located at the following path:

- for the application installed on a computer running under Linux: `/opt/kaspersky/klms/share/doc/LICENSE`, for the web interface: `/opt/kaspersky/klmsui/share/doc/LICENSE`;
- for the application installed on a computer running under FreeBSD: `/usr/local/share/doc/klms/LICENSE`, for the web interface: `/opt/kaspersky/klmsui/share/doc/LICENSE`.

STEP 3. SELECTING AN APACHE WEB SERVER

Before installing the web interface package for Kaspersky Security, you need to install the following Apache modules: `mod_ssl`, `mod_include`, `mod_dir`, `mod_expires` (if not already installed) and enable them using the command `a2enmod` (if not already enabled):

```
# a2enmod ssl  
  
# a2enmod include  
  
# a2enmod dir  
  
# a2enmod expires
```

At this step, you can specify the Apache web server to be used by Kaspersky Security.

The initial configuration script for the application web interface automatically determines the location of the configuration and executable files of the Apache service and displays information about the Apache web server that is located.

If the initial configuration script for the application web interface correctly identified the location of the configuration and executable files of the Apache server, you need to confirm it.

If the initial configuration script for the web interface did not correctly locate the configuration and executable files for the Apache service, or if you do not want to use the selected Apache web server, you need to manually specify the location of the Apache service files of the Apache web server that you want to use.

➤ *To confirm the location of the Apache service files:*

1. Enter yes (or y).
2. Press **ENTER**.

➤ *To specify the location of the Apache service files:*

1. Enter no (or n).
2. Press **ENTER**.
3. Specify the full path to the Apache executable file.
4. Press **ENTER**.
5. Specify the full path to the Apache configuration file.
6. Press **ENTER**.
7. Specify the full path to the Apache run script.
8. Press **ENTER**.

STEP 4. SELECTING AN APACHE SERVER VIRTUAL HOST

At this step, you need to specify a virtual host for the Apache web server.

➤ *To specify the virtual host:*

1. Do one of the following:

- If the Apache server virtual host is defined by its name, enter name.
- If the Apache server virtual host is defined by its port number, enter port.

This option is selected by default.

- If the Apache server virtual host is defined by its directory, enter dir.

When using the Apache web server virtual host defined by its directory, Kaspersky Security uses the connection settings specified in the Apache configuration file. An insecure HTTP connection is established by default. You can manually configure the Apache web server virtual host to use an encrypted SSL connection.

2. Press **ENTER**.
3. Do one of the following:
 - If you selected the name option at step 1, enter the name of the virtual host for the Apache web server.
 - If you selected the port option at step 1, enter the port number of the virtual host for the Apache web server.
The default option is 9045.
 - If you selected the dir option at step 1, enter the path to the directory where files of the Kaspersky Security web interface will be stored.
The klms directory is offered by default.
4. Press **ENTER**.

STEP 5. SELECTING A SOCKET TO INTERACT WITH KASPERSKY SECURITY

At this step, you need to specify a socket (IP address and port number) to enable interaction between the Apache web server and Kaspersky Security.

► *To specify an IP address and port number to enable interaction between the Apache web server and Kaspersky Security:*

1. Enter the IP address and port number in the format <IP address>:<port>.
The default network socket is: 127.0.0.1:2711.
2. Press **ENTER**.

STEP 6. SELECTING A CERTIFICATE TO ACCESS THE WEB INTERFACE

At this step, you need to specify a certificate to access the Kaspersky Security web interface.

You can create a new certificate or specify the path to a private key file and the path to an existing certificate on the computer.

► *To create a new certificate to access the web interface of the application:*

1. Enter new.
2. Press **ENTER**.

A new certificate is created.

➤ *To specify the path to a private key file and the path to an existing certificate:*

1. Type file and press **ENTER**.
2. Specify the path to the private key file and press **ENTER**.
3. Specify the path to the certificate file and press **ENTER**.

STARTING AUTOMATIC INITIAL CONFIGURATION OF THE WEB INTERFACE OF KASPERSKY SECURITY

Initial configuration of the web interface of Kaspersky Security can be performed in automatic mode. A file with saved answers can be created using the `--create-auto-install=<full path to the configuration file>` parameter when running the initial application configuration script.

Possible values should be typed using lower-case characters.

➤ *To start initial configuration of the Kaspersky Security web interface in automatic mode, execute the following command:*

- under Linux:

```
/opt/kaspersky/klmsui/bin/klmsui-setup.pl \
```

```
--auto-install=<full path to the configuration file with the saved answers>
```

- under FreeBSD:

```
/usr/local/bin/klmsui-setup.pl \
```

```
--auto-install=<full path to the configuration file with the saved answers>
```

The settings of the configuration file with answers are given in the following table.

Table 3. Settings of the Kaspersky Security web interface configuration file with answers

SETTING	DESCRIPTION	AVAILABLE VALUES
WEB_EULA_AGREED	Required setting. Acceptance of the terms of the License agreement.	yes
APACHE_BIN	Required setting. Path to the directory of the Apache web server.	<path> Case sensitive.
APACHE_CONF_D	Required setting. Path to the settings directory of the Apache web server.	<path> Case sensitive.
APACHE_INIT_D	Required setting. Path to the startup script of the Apache web server.	<path> Case sensitive.
VHOST_TYPE	Required setting. Method of configuration of the virtual server of the Apache web server.	name port dir
VHOST_PORT	Required setting if the value of the VHOST_TYPE setting is equal to "port". Number of the port on the virtual server of the Apache web server.	<port>
VHOST_DIR	Required setting if the value of the VHOST_TYPE setting is equal to "dir". Specifies the path to the folder with the files of the Kaspersky Security web interface.	<url_subdir>
VHOST_HOST	Required setting if the value of the VHOST_TYPE setting is equal to "name". Specifies the name of the virtual Apache web server.	<hostname>
UI_HOST	Required setting. Specifies a socket (IP address and port number) to enable interaction between the Apache web server and Kaspersky Security.	<host:port>
CERT_TYPE	Required setting. Type of certificate. If the type is set to "new", the certificate is created by the initial configuration script. The type "keep" is included in the list and selected by default if the certificate already exists.	new file keep
CERT_KEY	Required setting if the value of the CERT_TYPE setting is equal to "file". Path to the private key to the Apache web server.	<path> Case sensitive.

SETTING	DESCRIPTION	AVAILABLE VALUES
CERT_CRT	Required setting if the value of the CERT_TYPE setting is equal to "file". Path to the certificate of the Apache web server.	<path> Case sensitive.
IGNORE_APACHE_ARCH	Optional setting. Specifies whether or not to ignore the error when the klmsui-setup.pl script cannot determine the bit value of the installed Apache server. If the bit value of the server cannot be determined and the key value is set to "yes", integration continues.	yes no

REMOVING KASPERSKY SECURITY

➤ To remove Kaspersky Security installed from an .rpm package, execute the following command:

```
# rpm -e <PRODUCT_BIN>
```

You can remove Kaspersky Security, installed from a .deb package in one of the following ways:

- remove the application, but keep data created and used by the application during run time.
- remove the application completely, including all files and directories.

➤ To remove Kaspersky Security installed from an .deb package, execute the following command:

```
# dpkg -r <PRODUCT_BIN>
```

If necessary, you can later delete all files and folders remaining after removal of the application (see section "Actions after removing Kaspersky Security" on page [51](#)).

➤ To remove Kaspersky Security installed from a .deb-package completely (including all files and directories), execute the following command:

```
# dpkg -P klms
```

➤ To remove Kaspersky Security installed on a computer running under FreeBSD 8, execute the following command:

```
# pkg_delete klms-<version_number>
```

➤ To remove Kaspersky Security installed on a computer running under FreeBSD 9 or FreeBSD 10, execute the following command:

```
# pkg delete klms-<version_number>
```

The application is removed automatically. Kaspersky Security is removed and integration with the mail server is canceled.

ACTIONS AFTER REMOVING KASPERSKY SECURITY

When Kaspersky Security has been removed (see section "Removing Kaspersky Security" on page [50](#)) data such as application settings, messages in Backup, executable service files, help files, database updates, reports, log files, and sockets may remain on the computer.

Kaspersky Security includes scripts to delete files and directories that remain following removal of the application.

➤ *To delete data that remains when the application is removed:*

1. Enter the following command:

- under Linux:

```
# /var/opt/kaspersky/<PRODUCT_BIN>/cleanup.sh
```

- under FreeBSD:

```
# /var/db/kaspersky/klms/cleanup.sh
```

2. Enter yes to confirm deletion of data remaining after the removal of Kaspersky Security.

CONNECTING TO KASPERSKY SECURITY WEB INTERFACE

After preparing the web interface of Kaspersky Security for operation (see section "Preparing Kaspersky Security for operation" on page [30](#)), you can connect to the web interface.

➤ *To connect to the Kaspersky Security web interface:*

1. Type the following address in the address line of the web browser:

```
https://<IP address of Kaspersky Security>:<port>.
```

You specified the address when installing the application (see section "Installing the application" on page [25](#)).
Default port number: 9045.

A web interface login page opens, prompting you to enter the user name and password of the web address administrator (see figure below).



Figure 1. Authorization in the Kaspersky Security web interface

2. In the **User name** field, type Administrator.
3. In the **Password** field, enter the password specified at the stage of Preparing Kaspersky Security for operation (see section "Preparing Kaspersky Security for operation" on page [30](#)).
4. Click the **Log on** button.

The main page of the Kaspersky Security web interface opens.

MANUAL INTEGRATION OF KASPERSKY SECURITY WITH MAIL SERVERS AND AMAVIS INTERFACE

This section contains information about how to manually integrate Kaspersky Security with Exim, Postfix, Sendmail, QMail, as well as with the Amavis interface.

IN THIS SECTION:

About manual integration	53
Manual Integration with Sendmail server	54
Manual Integration with Exim mail server	57
Manual Integration with QMail server	63
Manual integration with a Postfix mail server	64
Manual integration with the Amavis interface	69

ABOUT MANUAL INTEGRATION

If you choose not to integrate the application with a mail server automatically during initial configuration (see section "Step 10. Selecting the type of integration with the mail server" on page [35](#)), you must integrate Kaspersky Security with a mail server manually.

You can integrate Kaspersky Security with the following mail servers manually:

- Exim (see section "Manual integration with Exim mail server" on page [57](#)).
- Postfix (see section "Manual integration with Postfix mail server" on page [64](#)).
- Sendmail (see section "Manual integration with Sendmail mail server" on page [54](#)).
- QMail (see section "Manual integration with QMail mail server" on page [63](#)).
- Amavis (see section "Manual integration with the Amavis interface" on page [69](#)).

Kaspersky Security supports integration with mail servers through the klms service, which receives processing requests from the mail server.

If the application is integrated with the mail server manually, you need to:

- enter the klms server in the operating system registry.
- modify the configuration file of the mail server.

Under FreeBSD you can configure the klms service to start automatically at operating system startup.

➔ To configure the *klms* service to start automatically on FreeBSD startup,

add the following strings to the */etc/rc.conf* configuration file:

```
klmsdb_enable=YES
```

```
klms_enable=YES
```

For Exim and Postfix mail servers, Kaspersky Security supports both before-queue and after-queue integration. In the case of before-queue integration, messages are forwarded to Kaspersky Security for scanning before insertion in the mail server queue, while after-queue integration sends messages to Kaspersky Security for scanning after they are inserted in the mail server queue.

The Kaspersky Security filter and the mail server communicate via sockets.

Sockets must be assigned based on the following rules:

- `inet:<port>@<ip_address>` for network sockets;
- `unix:<socket_path>` for UNIX sockets.

Example:

```
scanner=inet:5555@127.0.0.1 for network sockets
```

```
scanner=unix:/var/run/klms/scanner_sock for UNIX sockets
```

The following two conditions must be met when using a socket:

- when defining a network socket, the port number must be above 1024.
- when defining a UNIX socket, the filter and *kluser* must have the rights to access the socket.

MANUAL INTEGRATION WITH SENDMAIL SERVER

Sendmail provides the Milter API interface for integration with third-party filters. Kaspersky Security receives messages from Sendmail and transmits them back by calling Milter API functions. Messages are sent for scanning before insertion in the mail queue (before-queue integration).

To integrate the application with a Sendmail server, you to modify the Sendmail configuration file manually.

In the `[global]` section set the true value for the `header-guard` setting of the *klms_filter.conf* filter settings file.

You can make changes to the Sendmail configuration file as follows:

- by modifying the `.cf` configuration file.
- by modifying the `.mc` file and then creating the `.cf` file from it using the `m4` macro processor.

If you modify the `.cf` file only, all modifications will be lost on any subsequent creation of the `.cf` file from the `.mc` file.

IN THIS SECTION:

Integration using the <code>.mc</code> file	55
Integration using the <code>.cf</code> file	56

INTEGRATION USING THE .MC FILE

➤ To integrate Kaspersky Security with Sendmail using the .mc file:

1. Back up the .mc file.
2. Add the following strings to the .mc file:

```
dnl #KLMS-milter-begin-filter dnl

define(`_FFR_MILTER', `true')dnl
INPUT_MAIL_FILTER(`KLMS_Milter', `S=$filter_socket,${fail_type}T=S:3m;R:5m;E:10m') \
dnl
```

```
dnl #KLMS-milter-end-filter dnl
```

where `$filter_socket` stands for the IP address and port number or the UNIX socket that the filter uses to listen for incoming connections as follows: `inet:<port>@<IP address>` (for a network socket) or `unix:<path to UNIX socket>` (for UNIX sockets).

`{fail_type}` defines the action to be taken by the Sendmail server on messages if the filter works incorrectly. `{fail_type}` can take the values "F=R", "F=A," or "F=T,". R means reject, A means accept, and T means tempfail. If you replace `{fail_type}` with an empty line, the message will be skipped. The recommended option is tempfail.

Example:

```
INPUT_MAIL_FILTER(`KLMS_Milter', `S=inet:10025@127.0.0.1,F=T,T=S:3m;R:5m;E:10m')dnl
```

3. Compile the .cf configuration file according to your operating system settings.
4. Stop the klms service.
5. Open the file `/etc/opt/kaspersky/klms/klms_filters.conf` (under Linux) or `/usr/local/etc/kaspersky/klms/klms_filters.conf` (under FreeBSD).
6. In the [global] section, specify the path to the sendmail file in the following line:


```
sendmail-path=<path to sendmail file>
```
7. Specify the IP address and port number or UNIX socket where the filter will listen for incoming connections in the following string of the [milter] section of the `/etc/opt/kaspersky/klms/klms_filters.conf` file (under Linux) or `/usr/local/etc/kaspersky/klms/klms_filters.conf` (under FreeBSD):

```
socket=<IP address and port number> or <path to UNIX socket>
```

Example:

```
socket=inet:10025@127.0.0.1
```

8. Open the file `/var/opt/kaspersky/klms/installer.dat` (under Linux) or `/var/db/kaspersky/klms/installer.dat` (under FreeBSD).
9. Add the following lines to the file:

```
SENDMAIL_MILTER=1
```

```
SENDMAIL_USES_MC=1 if you have compiled the .mc file, 0 if not.
```

```
START_MILTER=1
```

10. Start the klms service.
11. Restart Sendmail.

INTEGRATION USING THE .CF FILE

➤ To integrate Kaspersky Security with Sendmail using the .cf file:

1. Create the backup copy of the sendmail.cf file.
2. Add the following strings to the sendmail.cf file:

```
#KLMS-milter-begin-filter
O InputMailFilters=KLMS_Milter
O Milter.macros.connect=j, _, {daemon_name}, {if_name}, {if_addr}
O Milter.macros.helo={tls_version}, {cipher}, \
{cipher_bits}, {cert_subject}, {cert_issuer}
O Milter.macros.envfrom=i, {auth_type}, \
{auth_authen}, {auth_ssf}, {auth_author}, \
{mail_mailer}, {mail_host}, {mail_addr}
O Milter.macros.envrcpt={rcpt_mailer}, {rcpt_host}, {rcpt_addr}
#KLMS-milter-end-filter
#KLMS-milter-begin-socket
XKLMS_Milter, S=${filter_socket},${fail_type}T=S:3m;R:5m;E:10m
#KLMS-milter-end-socket
```

where `$filter_socket` stands for the IP address and port number or the UNIX socket that the filter uses to listen for incoming connections as follows: `inet:<port>@<IP address>` (for a network socket) or `unix:<path to UNIX socket>` (for UNIX sockets).

`${fail_type}` defines the action to be taken by the Sendmail server on messages if the filter works incorrectly.

`${fail_type}` can take the values "F=R", "F=A," or "F=T,". R means reject, A means accept, and T means tempfail.

If you replace `${fail_type}` with an empty line, the message will be skipped. The recommended option is tempfail.

Example:

```
INPUT_MAIL_FILTER(`KLMS_Milter',`S=inet:10025@127.0.0.1,F=T,T=S:3m;R:5m;E:10m')dnl
```

3. Stop the klms service.
4. Open the file `/etc/opt/kaspersky/klms/klms_filters.conf` (under Linux) or `/usr/local/etc/kaspersky/klms/klms_filters.conf` (under FreeBSD).
5. In the `[global]` section, specify the path to the sendmail file in the following line:


```
sendmail-path=<path to sendmail file>
```


- Specify the IP address and port number or UNIX socket where the filter will listen for incoming connections in the following string of the [milter] section of the /etc/opt/kaspersky/klms/klms_filters.conf file (under Linux) or /usr/local/etc/kaspersky/klms/klms_filters.conf (under FreeBSD):

socket=inet:<port>@<IP address> or <UNIX socket>

Example:

socket=inet:10025@127.0.0.1

- Open the file /var/opt/kaspersky/klms/installer.dat (under Linux) or /var/db/kaspersky/klms/installer.dat (under FreeBSD).
- Add the following lines to the file:


```
SENDMAIL_MILTER=1
```

SENDMAIL_USES_MC=1 if you have compiled the .mc file, 0 if not.

```
START_MILTER=1
```
- Start the klms service.
- Restart Sendmail.

MANUAL INTEGRATION WITH EXIM MAIL SERVER

Kaspersky Security supports 2 methods for manual integration with Exim:

- After-queue integration via SMTP by rerouting. With after-queue integration, all messages that are forwarded via the computer go to Kaspersky Security for scanning after they have been inserted in the Exim mail server queue.
- Before-queue integration via dfunc. With before-queue integration, messages go to Kaspersky Security for scanning before insertion in the Exim mail server queue.

IN THIS SECTION:

After-queue integration by rerouting.....	57
Before-queue integration using dynamic linking.....	60

AFTER-QUEUE INTEGRATION BY REROUTING

When "after-queue" integration is used and messages are rerouted to Kaspersky Security for scanning and then returned to the Exim mail server, the following conditions must be satisfied:

- The filter must be configured to intercept messages from the Exim mail server via socket-in. This socket must be specified in the configuration of the application.
- The filter must forward messages to Scan Logic for scanning via the scanner socket. This socket must be specified in the configuration of the application.
- The filter must return messages to the Exim mail server via socket-out. This socket must be specified in the configuration of the application.

When after-queue integration with the Exim mail server is used for rerouting, socket-in, scanner, and socket-out must point to a network socket.

Depending upon the specific distribution of the operating system, you have to modify one or several configuration files of the Exim mail server. For example, in Debian and Ubuntu Exim configuration may consist of several files in the `/etc/exim/conf.d` directory or a single file only.

➤ *To perform after-queue integration of Kaspersky Security with Exim by rerouting:*

1. Make a backup copy of the Exim configuration file (files).
2. In the [routers] section of Exim configuration file(s), add after the line

```
begin routers
```

add the following lines:

```
#klms-filter-begin-2
```

```
klms_dnslookup:
```

```
driver = dnslookup
```

```
domains = ! +local_domains
```

```
ignore_target_hosts = 0.0.0.0 : 127.0.0.0/8
```

```
verify_only
```

```
pass_router = smtp_proxy
```

```
no_more
```

```
klms_system_aliases:
```

```
driver = redirect
```

```
allow_fail
```

```
allow_defer
```

```
data = ${lookup{$local_part}lsearch{/etc/aliases}}
```

```
verify_only
```

```
pass_router = smtp_proxy
```

```
klms_localuser:
```

```
driver = accept
```

```
check_local_user
```

```
verify_only
```

```
pass_router = smtp_proxy
```

```
cannot_route_message = Unknown user
```

```
failed_address_router:
```

```
driver = redirect
```

```
verify_only
```

```
condition = "{0}"
```

```
allow_fail
```

```
data = :fail: Failed to deliver to address
```

```
no_more
```

```
smtp_proxy:
```

```
driver = manualroute
```

```
condition = "${if or {{eq {$interface_port}{$forward_port}} \\  
  {eq {\$received_protocol}{spam-scanned}} \\  
  {0}{1}}"
```

```
transport = smtp_proxy
```

```
route_list = "*" localhost byname"
```

```
self = send
```

```
#klms-filter-end-2
```

where \$forward_port is the port number of the socket where the message will go after being scanned by Kaspersky Security.

3. In the [transports] section of Exim configuration file(s), add after the line

```
begin transports
```

```
add the following lines:
```

```
#klms-filter-begin-3
```

```
smtp_proxy:
```

```
driver = smtp
```

```
port = $scanner_port
```

```
delay_after_cutoff = false
```

```
allow_localhost
```

```
#klms-filter-end-3
```

where \$scanner_port stands for the port, which filter uses to wait for messages.

4. In the main Exim configuration file (`exim.conf` or `update-exim.conf.conf`), specify the substring in the form `127.0.0.1.$forward_port` as follows:

```
dc_local_interfaces=<IP address1>.<port1>:127.0.0.1.$forward_port
```

or

```
local_interfaces=<IP address1>.<port1>:127.0.0.1.$forward_port
```

where the `127.0.0.1.$forward_port` substring is required to enable Exim to accept processed messages from the filter and listen for data on `$forward_port`.

5. Compile the Exim configuration file (files) according to your operating system settings.
6. Open the file `/var/opt/kaspersky/klms/installer.dat` (under Linux) or `/var/db/kaspersky/klms/installer.dat` (under FreeBSD).
7. Add the following lines to the file:

```
EXIM_INTEGRATION_TYPE= after-queue
```

```
START_SMTP_PROXY=1
```

8. Open the file `/etc/opt/kaspersky/klms/klms_filters.conf` (under Linux) or `/usr/local/etc/kaspersky/klms/klms_filters.conf` (under FreeBSD).
9. In the `[smtp_proxy]` section, specify the following settings:

```
socket-in=inet:$scanner_port@127.0.0.1
```

```
socket-out=inet: $forward_port@127.0.0.1
```

10. Set the `true` value in the `[global]` section for the `header-guard` setting.
11. Restart the `klms` service.
12. Restart Exim mail server.

BEFORE-QUEUE INTEGRATION USING DYNAMIC LINKING

To use the "before-queue" integration method, you have to specify that `dlfunc` support is required when compiling the corresponding dynamic library from the source code. Repositories of some Linux distributions contain compiled Exim versions already, in other cases manual compiling is required.

In case of manual compilation, you have to add the following lines to Makefile:

```
EXPAND_DLFUNC=yes
```

```
EXTRALIBS= -export-dynamic
```

When before-queue integration via a dynamic library is used, the filter must transfer messages for scanning to ScanLogic through ServiceSocket. This socket must be specified in the configuration of the application.

Depending upon the specific distribution of the operating system, you have to modify one or several configuration files of the Exim mail server. For example, in Debian and Ubuntu Exim configuration may consist of several files in the `/etc/exim/conf.d` directory or a single file only.

➤ *To integrate before_queue integration with Exim using a dynamic library:*

1. Make sure that Exim supports `dlfunc`-based content filtering. To do so, run the `exim -bV` command.

The following represents a positive result: Expand_dfunc.

2. Make a backup copy of the Exim configuration files.
3. Modify the access control list for acl_smtp_data. To do that, find in the Exim configuration file(s) the line that looks like:

acl_smtp_data = acl_check_data (the line may contain another access control list instead of acl_check_data)

and after the line

acl_check_data: (or line containing another access control list)

add the following lines:

```
#klms-filter-begin
```

```
warn set acl_m_klms_headers =
```

```
set acl_m_klms_result =
```

```
set acl_m_klms_answer = ${dfunc{LIBDIR/libklms-exim.so}{scan}{${spool_directory}/input}}
```

```
defer condition = ${if eq {$acl_m_klms_answer}{}}{yes}{no}}
```

```
log_message = LMS check failed (empty answer)
```

```
message = Temporary local problem - please try later
```

```
defer condition = ${if match {$acl_m_klms_answer}{\N^451\N}}{yes}{no}}
```

```
log_message = LMS check defer: ${if match {$acl_m_klms_answer} \
```

```
{\N^451 Mail processing aborted(.+\n?.*\n)*$\N}{$1}}\
```

```
 ${if eq {$acl_m_klms_result}{}}{, result is \
```

```
'$acl_m_klms_result'}\
```

```
 , temporary file $acl_m_klms_tempfile
```

```
message = Temporary local problem - please try later
```

```
defer condition = ${if match {$acl_m_klms_answer}{\N^452\N}}{yes}{no}}
```

```
log_message = LMS check defer: ${if match {$acl_m_klms_answer} \
```

```
{\N^452 Mail processing timed out(.+\n?.*\n)*$\N}{$1}}\
```

```
 ${if eq {$acl_m_klms_result}{}}{, result is \
```

```
'$acl_m_klms_result'}\
```

```
 , temporary file $acl_m_klms_tempfile
```

```
message = Temporary local problem - please try later
```

```
deny condition = ${if match {$acl_m_klms_answer}{\N^550\N}}{yes}{no}}
```

```
log_message = LMS check reject: ${if match {$acl_m_klms_answer} \
```

```
{\N^550 Rejected by malware filter(.+\n?.*\n)*$\N}{$1}}\
```

```

    ${if eq {$acl_m_klms_result}{}}{, result is \
'$acl_m_klms_result'}\
    , temporary file $acl_m_klms_tempfile
deny condition = ${if match {$acl_m_klms_answer}{\N^554\N}{yes}{no}}
    log_message = LMS check reject: ${if match {$acl_m_klms_answer} \
{\N^554 Mail processing failed(.+\n?.*\n)*\N}{$1}}\
    ${if eq {$acl_m_klms_result}{}}{, result is \
'$acl_m_klms_result'}\
    , temporary file $acl_m_klms_tempfile
    message = ${if match {$acl_m_klms_answer} \
{\N^554 Mail processing failed(.+\n?.*\n)*\N} \
{Mail processing failed:$1}}
warn condition = ${if match {$acl_m_klms_answer}{\N^250\N}{yes}{no}}
    logwrite = LMS check accept: ${if match {$acl_m_klms_answer} \
{\N^250 (.+)\N}{$1}} \
    ${if eq {$acl_m_klms_result}{}}{, result is \
'$acl_m_klms_result'}
    set acl_m_klms_answer =
warn condition = ${if eq {$acl_m_klms_answer}{no}{yes}}
    logwrite = LMS check: $acl_m_klms_answer

```

#klms-filter-end

where LIBDIR – path to the libklms-exim.so library:

- for FreeBSD (32-bit) - /usr/local/lib/kaspersky/klms/libklms-exim.so,
 - for FreeBSD (64-bit) - /usr/local/lib/kaspersky/klms/compat64/libklms-exim.so,
 - for Linux (32-bit) - /opt/kaspersky/klms/lib/libklms-exim.so,
 - for Linux (64-bit) - /opt/kaspersky/klms/lib64/libklms-exim.so.
4. Compile the .so module according to the settings of your operating system (optional).
 5. Add the user kluser to the group to which the exim process belongs.
 6. In the [global] section set the false value for the header-guard setting of the *klms_filter.conf* filter settings file.
 7. Open the file /var/opt/kaspersky/klms/installer.dat (under Linux) or /var/db/kaspersky/klms/installer.dat (under FreeBSD).

8. Add the following line to the file:

```
EXIM_INTEGRATION_TYPE=dlfunc
```

9. Restart the klms service.
10. Restart Exim mail server.

The Kaspersky Security installation package contains a compiled dynamically loaded dlfunc library for all operating systems supported by the application. The source files required for the dlfunc library are located in the directory /opt/kaspersky/klms/share/src/dlfunc (under Linux) or /usr/local/share/klms/src/dlfunc (under FreeBSD).

In some cases, manual compilation is required.

➤ *To perform a manual compilation of the dynamically loaded dlfunc library:*

1. Install the source libraries of the Exim mail server.
2. Install the libevent library (version 2.0.10 or higher).
3. Install the boost library (version 1.47.0 or higher).
4. Open the folder /opt/kaspersky/klms/share/src/dlfunc (for Linux) or the folder /usr/local/share/klms/src/dlfunc (for FreeBSD)
5. Execute the command `./configure --with-exim=<path to exim headers> --with-boost=<path to boost> --with-libevent=<path to libevent>`
6. Execute the following command: `# make`.

The libklms-exim.so file appears in the current folder.

MANUAL INTEGRATION WITH QMAIL SERVER

The QMail server does not support the integration of extensions. To integrate Kaspersky Security with QMail server manually, replace the original executable file with the /opt/kaspersky/klms/lib/bin/kavklms-qmail (under Linux) or /usr/local/libexec/kaspersky/klms/klms-qmail (under FreeBSD) queue file supplied with Kaspersky Security for Linux Mail Server. This file supports message filtering and transmits messages back to the original qmail-queue file for subsequent delivery. Rename the original qmail-queue file to qmail-queue-real.

Messages are sent for scanning before insertion in the mail queue (before-queue filtering).

➤ *To integrate Kaspersky Security with QMail manually:*

1. Specify /var/qmail/bin/sendmail as the sendmail-path parameter's value in the [global] section of the klms_filters.conf file.
2. Copy the /var/qmail/bin/qmail-queue file to the /var/qmail/bin/qmail-queue-real folder using the following command:

```
#cp -fp /var/qmail/bin/qmail-queue /var/qmail/bin/qmail-queue-real
```

3. Copy the filter file from the Kaspersky Security distribution kit to the qmail folder using the following command:

- under Linux:

```
#cp -fp /opt/kaspersky/klms/libexec/qmail-queue /var/qmail/bin/qmail-queue
```

- under FreeBSD:

```
#cp -fp /usr/local/libexec/kaspersky/klms/qmail-queue /var/qmail/bin/qmail-queue
```

- Set the following access rights for the `qmail-queue` and `qmail-queue-real` files:

```
# ls -la /var/qmail/bin/qmail-queue*
```

```
-rws--s--x 1 qmaild klusers 2287242 Feb 19 20:53 /var/qmail/bin/qmail-queue
```

```
-rws--x--x 1 qmailq qmail 19288 June 27 2013 /var/qmail/bin/qmail-queue-real
```

- In the filter settings file `klms_filter.conf`, go to the `[global]` section and make sure that the `header-guard` setting has its value set to `true`.
- Restart Kaspersky Security:

```
service klms restart
```

MANUAL INTEGRATION WITH A POSTFIX MAIL SERVER

Kaspersky Security supports 3 methods for integration with Postfix:

- After-queue integration. With after-queue integration, all messages that are forwarded via the protected computer go to the application for scanning after they have been inserted in the Postfix mail server queue.
- Before-queue integration. With before-queue integration, messages go to the application for scanning before insertion in the Postfix mail server queue.
- Integration using the Milter protocol. In this case, messages are forwarded to the application for scanning via the Milter protocol.

IN THIS SECTION:

After-queue integration.....	64
Before-queue integration.....	66
Integration using the Milter protocol	68

AFTER-QUEUE INTEGRATION

When "after-queue" integration is used and messages are forwarded to Kaspersky Security for scanning and then returned to the Postfix mail server, the following conditions must be satisfied:

- The filter must be configured to intercept messages from the Postfix mail server via `socket-in`. This socket must be specified in the configuration of the application.
- The filter must forward messages to Scan Logic for scanning via the `scanner` socket. This socket must be specified in the configuration of the application.
- The filter must return messages to the Postfix mail server via `socket-out`. This socket must be specified in the configuration of the application.

When Kaspersky Security is integrated with the Postfix mail server, `socket-in`, `scanner`, and `socket-out` can point to a network socket or to a local one.

► To perform after-queue integration of Kaspersky Security with Postfix:

- Open the configuration file `main.cf`.

2. Add the following strings to the end of the main.cf file:

```
#klms-begin-afterqueue-filter

content_filter =klms_postfix-afterqueue:$sock_postfix_format

#klms-end-afterqueue-filter
```

where \$sock_postfix_format stands for the IP address and port number or the UNIX socket that the filter uses to listen for incoming connections as follows: inet:<IP address>:<port> (for a network socket) or unix:<path to UNIX socket> (for UNIX sockets).

3. Open the configuration file master.cf.
4. Add the following strings to the end of the master.cf file:

```
#klms-begin-afterqueue-filter

klms_postfix-afterqueue\tunix - - \n - 10 smtp
-o smtp_send_xforward_command=yes
127.0.0.1:$forward_port\tinet\tn - n - 10 smtpd
-o content_filter=
-o receive_override_options=no_unknown_recipient_checks,\
no_header_body_checks,no_address_mappings
-o smtpd_helo_restrictions=
-o smtpd_client_restrictions=
-o smtpd_sender_restrictions=
-o smtpd_recipient_restrictions=permit_mynetworks,reject
-o mynetworks=127.0.0.0/8,[::1]/128
-o smtpd_authorized_xforward_hosts=127.0.0.0/8,[::1]/128

#klms-end-afterqueue-filter
```

where the string

127.0.0.1:\$forward_port\tinet\tn - n - 10 smtpd is required to enable Postfix to accept processed messages from the filter and listen for data on \$forward_port.

5. Open the file /var/opt/kaspersky/klms/installer.dat (under Linux) or /var/db/kaspersky/klms/installer.dat (under FreeBSD).
6. Add the following lines to the file:


```
POSTFIX_INTEGRATION_TYPE=afterqueue

START_SMTP_PROXY =1
```
7. Open the file /etc/opt/kaspersky/klms/klms_filters.conf (under Linux) or /usr/local/etc/kaspersky/klms/klms_filters.conf (under FreeBSD).
8. In the [global] section set the false value for the header-guard setting.

- In the [smtp_proxy] section, specify the following settings:

socket-in=<IP address and port number> or <UNIX socket> specified at Step 2 of the wizard for \$sock_postfix_format

socket-out=inet: \$forward_port@127.0.0.1

in the format inet:<port>@<IP address> (for a network socket) or unix:<path to UNIX socket> (for a UNIX socket).

Example:

socket-in=inet:10025@127.0.0.1

socket-out=inet: 10026@127.0.0.1

- Restart the klms service.

- Restart Postfix.

BEFORE-QUEUE INTEGRATION

When "before-queue" integration is used and messages are forwarded to Kaspersky Security for scanning and then returned to the Postfix mail server, the following conditions must be satisfied:

- The filter must be configured to intercept messages from the Postfix mail server via socket-in. This socket must be specified in the configuration of the application.
- The filter must forward messages to Scan Logic for scanning via the scanner socket. This socket must be specified in the configuration of the application.
- The filter must return messages to the Postfix mail server via socket-out. This socket must be specified in the configuration of the application.

When Kaspersky Security is integrated with the Postfix mail server, socket-in, scanner, and socket-out can point to a network socket or to a local one.

➡ To perform before-queue integration of Kaspersky Security with Postfix:

- Open the configuration file master.cf.

- In the master.cf file, after the line

```
smtp inet n - n - - smtpd
```

add the following lines:

```
#klms-postfix-prequeue-start
```

```
-o smtpd_proxy_filter=$sock_postfix_format
```

```
-o smtpd_proxy_options=speed_adjust (for integration with Postfix 2.7 or higher)
```

```
#klms-postfix-prequeue-end
```

where \$sock_postfix_format stands for the IP address and port number or the UNIX socket that the filter uses to listen for incoming connections as follows: inet:<IP address>:<port> (for a network socket) or unix:<path to UNIX socket> (for UNIX sockets).

- Add the following strings in the end of the master.cf configuration file:

```
#klms-begin

klms_postfix-prequeue unix - - n - 10 smtp

-o smtp_send_xforward_command=yes

127.0.0.1:$forward_port\tinet\tn - n - 10 smtpd

-o receive_override_options=no_unknown_recipient_checks, \
no_header_body_checks,no_address_mappings

-o smtpd_helo_restrictions=

-o smtpd_client_restrictions=

-o smtpd_sender_restrictions=

-o smtpd_recipient_restrictions=permit_mynetworks,reject

-o mynetworks=127.0.0.0/8,[:1]/128

-o smtpd_authorized_xforward_hosts=127.0.0.0/8,[:1]/128

#klms-end
```

where the string

127.0.0.1:\$forward_port\tinet\tn - n - 10 smtpd is required to enable Postfix to accept processed messages from the filter and listen for data on \$forward_port.

4. Open the file /var/opt/kaspersky/klms/installer.dat (under Linux) or /var/db/kaspersky/klms/installer.dat (under FreeBSD).

5. Add the following lines to the file:

```
POSTFIX_INTEGRATION_TYPE= prequeue

START_SMTP_PROXY =1
```

6. Open the file /etc/opt/kaspersky/klms/klms_filters.conf (under Linux) or /usr/local/etc/kaspersky/klms/klms_filters.conf (under FreeBSD).

7. In the [global] section set the false value for the header-guard setting.

8. In the [smtp_proxy] section, specify the following settings:

socket-in=<IP address and port number> or <UNIX socket> specified at Step 2 of the wizard for \$sock_postfix_format

socket-out=inet: \$forward_port@127.0.0.1

in the format inet:<port>@<IP address> (for a network socket) or unix:<path to UNIX socket> (for a UNIX socket).

Example:

```
socket-in=inet:10025@127.0.0.1
```

```
socket-out=inet: 10026@127.0.0.1
```

9. Restart the klms service.

- Restart Postfix.

INTEGRATION USING THE MILTER PROTOCOL

When integration based on Milter functionality is used to transfer messages to the application for scanning and return them to the Postfix mail server, the following conditions must be observed:

- The filter must be configured to intercept messages from the Postfix mail server via socket. This socket must be specified in the configuration of the application.
- The filter must forward messages to Scan Logic for scanning via the scanner socket. This socket must be specified in the configuration of the application.

When Kaspersky Security is integrated with the Postfix mail server, socket and scanner can point to a network socket or to a local one.

➔ To integrate Kaspersky Security with Postfix using the Milter protocol:

- Enter the following command:

```
postconf -e $milter_socket
```

where `$milter_socket` stands for the IP address and port number or the UNIX socket where the filter will listen for incoming connections, as follows: `inet:port@IP address` (for network sockets) or `unix:<path to UNIX socket>` (for UNIX sockets).

- Open the configuration file `main.cf`.
- Add the following strings to the end of the `main.cf` file:

```
#lms-milter-begin

milter_connect_macros = j _ {daemon_name} {if_name} {if_addr}

milter_helo_macros = {tls_version} {cipher} {cipher_bits} {cert_subject} \
{cert_issuer}

milter_mail_macros = i {auth_type} {auth_authen} {auth_ssf} {auth_author} \
{mail_mailer} {mail_host} {mail_addr}

milter_rcpt_macros = {rcpt_mailer} {rcpt_host} {rcpt_addr}

milter_default_action = $fail_type

milter_protocol = 3

milter_connect_timeout=180

milter_command_timeout=180

milter_content_timeout=600

#lms-milter-end
```

where `$fail_type` can take the values: `reject`, `accept` or `tempfail`.

`fail_type` defines the action to be taken by the Postfix mail server on messages if the filter works incorrectly.

- reject – reject the message.
- accept – skip without scanning.
- tempfail – send temporary error notification to message sender.

The recommended option is tempfail.

4. Open the file `/var/opt/kaspersky/klms/installer.dat` (under Linux) or `/var/db/kaspersky/klms/installer.dat` (under FreeBSD).

5. Add the following lines to the file:

```
POSTFIX_INTEGRATION_TYPE= milter
```

```
START_MILTER=1
```

6. Open the file `/etc/opt/kaspersky/klms/klms_filters.conf` (under Linux) or `/usr/local/etc/kaspersky/klms/klms_filters.conf` (under FreeBSD).

7. Specify the IP address and port number or UNIX socket that the filter will use to listen for incoming connections in the following string of the `[milter]` section:

`socket=<IP address and port number> or <UNIX socket> specified at Step 1 for $milter_socket`

in the format `inet:<port>@<IP address>` (for a network socket) or `unix:<path to UNIX socket>` (for a UNIX socket).

Example:

```
socket=inet:10025@127.0.0.1
```

8. In the `[global]` section set the false value for the header-guard setting.
9. Restart the klms service.
10. Restart Postfix.

MANUAL INTEGRATION WITH THE AMAVIS INTERFACE

➡ *To integrate Kaspersky Security with Amavis manually:*

1. Add the kluser user to the amavis group (or to the group specified via the `$daemon_group` parameter of `/etc/amavisd.conf`) with the following command:

```
gpasswd -a kluser amavis
```

2. Add the account of the amavis user (or user specified in the `$daemon_user` setting of the `amavisd.conf` configuration file (hereinafter `/etc/amavisd.conf`)) to the klusers user group using the following command:

```
gpasswd -a amavis klusers
```

3. Open the `amavisd` file (hereinafter – `/usr/local/sbin/amavisd`)
4. Comment out the following lines to the `@spam_scanners` section:

```
@spam_scanners = (  
  
#[ 'SpamdClient', 'Amavis::SpamControl::SpamdClient' ],
```

5. Under the SUSE Linux 11 SP2 operating system, add the kluser account to the vscan user group. The vscan user group should be the primary group for the kluser account.
6. Under the SUSE Linux 11 SP2 operating system, add the vscan account to the klusers user group. The klusers user group should be the primary group for the vscan account.
7. Specify the rds_asp socket, where the KLRDS task is listening for incoming messages, in the following lines of the /usr/local/sbin/amavisd file for SpamdClient Perl module:

```
package Amavis::SpamControl::SpamdClient ...

my($spamd_handle) = Amavis::IO::RW->new(

['/var/run/klms/rds_asp'], Eol => "\015\012", Timeout => 30);
```

8. Open the amavisd.conf configuration file (hereinafter – /etc/amavisd.conf) for editing.
9. Make the following changes to the @av_scanners and @spam_scanners sections of the opened file:

```
@av_scanners = (

['Kaspersky Security 8.0 for Linux Mail Server',

\ask_daemon, ["nCONTSCAN {} \n", "/var/run/klms/rds_av"],

qr/\bOK$/m, qr/\bFOUND$/m,

qr/^\.*?: (?!Infected Archive)(.*) FOUND$/m ], ); ...

@spam_scanners = (

['SpamdClient', 'Amavis::SpamControl::SpamdClient' ], );
```

10. We recommend setting a 1500 KB limit on the maximum message size when using the Anti-Spam scan. To do so, set the following value in this string:

```
$sa_mail_body_size_limit = 1500000;
```

11. Restart the amavisd using the following command:

```
/etc/init.d/amavisd restart
```

During integration with the Amavis interface, you can specify the settings of Kaspersky Security only using the command line. Settings specified using the web interface of Kaspersky Security (such as the response timeout when attempting to connect to KSN) will not apply.

APPLICATION LICENSING

This section covers the main aspects of application licensing.

IN THIS SECTION:

About the license.....	71
About the End User License Agreement	72
About the license certificate	72
About the key	72
About the key file.....	73
About data provision.....	73
Viewing information about the license and added keys.....	74
Adding a key	74
Removing a key.....	74

ABOUT THE LICENSE

A *license* is a time-limited right to use the application, granted under the End User License Agreement.

A current license entitles you to the following kinds of services:

- Use of the application in accordance with the terms of the End User License Agreement
- Getting technical support

The scope of services and application usage term depend on the type of license under which the application is activated.

The following license types are provided:

- *Trial* – a free license intended for trying out the application.

A trial license is usually of limited duration. As soon as the license expires, all Kaspersky Security features are disabled. To continue using the application, you need to purchase a commercial license.

You can activate the application under a trial license only once.

- *Commercial* – a pay-for license that is provided when you buy the application.

When the commercial license expires, the application continues running with limited functionality (for example, Kaspersky Security database updates are not available). To continue using Kaspersky Security in fully functional mode, you must renew your commercial license.

We recommend renewing the license before its expiration to ensure maximum protection of your computer against security threats.

ABOUT THE END USER LICENSE AGREEMENT

The *End User License Agreement* is a binding agreement between you and Kaspersky Lab ZAO, stipulating the terms on which you may use the application.

You are advised to carefully read the End User License Agreement before using the application.

You can view the terms of the License Agreement in the following ways:

- During installation of Kaspersky Security.
- By reading the license.txt file. This file is included in the application's distribution kit.

By confirming that you agree with the End User License Agreement when installing the application, you signify your acceptance of the terms of the End User License Agreement. If you do not accept the terms of the End User License Agreement, you must abort application installation and must not use the application.

ABOUT THE LICENSE CERTIFICATE

The *License Certificate* is a document provided with the key file or activation code.

The License Certificate contains the following license information:

- License number
- Details of the license holder
- Information about the application that can be activated using the license
- Limitation on the number of licensing units (devices on which the application can be used under the license)
- License start date
- License expiration date or license validity period
- License type

ABOUT THE KEY

A *key* is a sequence of bits with which you can activate and subsequently use the application in accordance with the terms of the End User License Agreement. A key is generated by Kaspersky Lab. The key is displayed in the application or website interface as an alphanumeric sequence. You can add a key to the application by using a *key file*.

Kaspersky Lab can black-list a key over violations of the End User License Agreement. If the key has been black-listed, you have to add a different key to continue using the application.

There are two types of keys: active and additional.

An *active key* is the key that is currently used by the application. A trial or commercial license key can be added as the active key. The application cannot have more than one active key.

An *additional key* is a key that entitles the user to use the application, but is not currently in use. An additional key becomes active automatically when the current active key stops working, for example due to license expiry. An additional key can be added only if the active key is available. A trial license key cannot be added as an additional key.

Kaspersky Security uses keys of the following types:

- *Fully-functional key.* When a key is added, the application works in full-functionality mode, performing scans for spam, phishing, viruses and other types of malware.
- *Key for Anti-Virus protection.* When this key is added, the application scans messages for viruses and other threats but does not scan messages for spam. The status label assigned by the application to a message following a spam scan contains information about limited functionality.
- *Key for Anti-Spam and Anti-Phishing protection.* When this key is added, the application scans messages for spam and phishing but does not scan messages for viruses and other threats. The status label assigned by the application to a message following a scan for viruses and other threats contains information about limited functionality.

The type of additional key should match the type of the previously added active key. If the type of the additional key does not match the type of a previously added active key, the available application functionality changes when the additional key becomes active.

Anti-Spam and Anti-Virus databases are updated regardless of key type.

ABOUT THE KEY FILE

A *key file* is a file with the .key extension that you receive from Kaspersky Lab. Key files are designed to activate the application by adding a key.

You receive a key file at the email address that you provided when you bought Kaspersky Security or ordered the trial version of Kaspersky Security.

You do not need to connect to Kaspersky Lab activation servers in order to activate the application with a key file.

You can recover a key file if it is accidentally deleted. You may need a key file to register with Kaspersky CompanyAccount.

To recover a key file, do one of the following:

- Contact Kaspersky Lab Technical Support (<http://support.kaspersky.com/>).
- Obtain a key file on the Kaspersky Lab website (<https://activation.kaspersky.com>) based on your existing activation code.

ABOUT DATA PROVISION

According to the terms of the License Agreement that you have accepted, you consent to the automatic transmission to Kaspersky Lab of the information enumerated in the License Agreement under "Data Provision" (see section "Step 2. Reviewing the License Agreement" on page [31](#)). This is needed to improve the level of mail server security.

If you agree to participate in Kaspersky Security Network, information collected during the operation of Kaspersky Security on the computer is automatically forwarded to Kaspersky Lab. The list of data that is transmitted is provided in the Kaspersky Security Network Statement (see section "Step 3. Participating in Kaspersky Security Network" on page [32](#)).

Information retrieved is protected by Kaspersky Lab pursuant to the requirements stipulated by the existing legislation. Kaspersky Lab uses any retrieved information as general statistics only. General statistics are automatically generated using original collected information and do not contain any private data or other confidential information. Kaspersky Lab uses the latest methods for protecting the privacy of data it collects. Original collected data is stored in encrypted form and deleted as new data is accumulated. General statistics are stored indefinitely.

VIEWING INFORMATION ABOUT THE LICENSE AND ADDED KEYS

You can view information about the license, such as its validity period and expiration date.

- To view information about the license, execute the following command:

```
# /opt/kaspersky/klms/bin/klms-control \
--licenser --query-status
```

- To view information about all added keys, enter the following at the command line:

```
# /opt/kaspersky/klms/bin/klms-control \
--licenser --get-installed-keys
```

ADDING A KEY

You can add keys with two statuses: active and supplementary. You can use the application as soon as you add an active key. After adding an active key, you can add a supplementary key. The supplementary key automatically becomes active on expiration of the license. This ensures that protection is maintained in the period between expiration and renewal of the license.

If you add an active key when one has already been added for Kaspersky Security, the new key replaces the previously installed one. The key installed earlier is removed.

If you add a supplementary key when one has already been added for Kaspersky Security, the new key replaces the previously installed one. The supplementary key installed earlier is removed.

- To add an active key, execute the following command:

```
# /opt/kaspersky/klms/bin/klms-control --licenser --install-active-key <key file name>
```

- To add a supplementary key, execute the following command:

```
# /opt/kaspersky/klms/bin/klms-control --licenser --install-additional-key <key file name>
```

REMOVING THE KEY

If you remove the active key and a supplementary key has been added for Kaspersky Security, the supplementary key automatically becomes active.

- To remove the active key, execute the following command:

```
# /opt/kaspersky/klms/bin/klms-control \
--licenser --revoke-active-key
```

- To remove the supplementary key, execute the following command:

```
# /opt/kaspersky/klms/bin/klms-control \
--licenser --revoke-additional-key
```

If you remove the active and supplementary keys, you cannot use the full functionality of the application.

STARTING AND STOPPING THE APPLICATION

Starting the application

By default, Kaspersky Security starts automatically when the operating system is booted (at the default level of execution for each operating system).

At first startup and subsequent restarts, the product automatically creates folders required for normal operation of the product in the `/var/log` and `/tmp` folders. Modifying these folders manually can cause the product to malfunction.

Stopping the application

If required, you can stop the application. To stop the application, first stop the `klms` service and then the database.

- *To stop the `klms` service under a Linux operating system, execute the following command:*

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

- *To stop the database under a Linux operating system, execute the following command:*

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

- *To stop the `klms` service under a FreeBSD operating system, execute the following command:*

```
# /usr/local/etc/rc.d/klms stop
```

- *To stop the database under a FreeBSD operating system, execute the following command:*

```
# /usr/local/etc/rc.d/klmsdb stop
```

SERVER PROTECTION STATUS

The protection status of the mail server indicates whether or not there are currently any security issues affecting the level of security.

Not only detected malicious programs and spam are classified as security issues in this instance, but also:

- using outdated databases (see section "About database updates" on page [112](#));
- disabling the Anti-Spam engine (see section "Enabling and disabling the Anti-Spam engine" on page [88](#));
- disabling the Anti-Virus engine (see section "Enabling and disabling the Anti-Virus engine" on page [95](#));
- disabling the Anti-Phishing engine (see section "Enabling and disabling the Anti-Phishing engine" on page [103](#)).

To ensure that Kaspersky Security is protecting the mail server:

- check that the klms service is running.
- checking the state of databases (see section "Checking database state" on page [112](#));
- if you have configured integration with an external directory service (LDAP, Active Directory), check the connection between the application and the user service (see section "Checking the application connection to an external directory service using the LDAP protocol" on page [129](#)).

► *To verify that the klms service is running:*

1. Execute the command:

```
# /opt/kaspersky/klms/bin/klms-control --is-program-started
```

2. Execute the command:

```
# echo $?
```

If Kaspersky Security is running, 0 is returned; if the application is not running, 1 is returned.

BASIC PRINCIPLES

This section contains a description of the basic concepts and principles of using the application, and information about how to configure it.

IN THIS SECTION:

About scan and content filtering statuses	78
About message processing rules	79
Message processing algorithm.....	79
About black and white lists of addresses.....	80
Creating message processing rules	81
Viewing the list of message processing rules	83
About actions on objects	83
About Kaspersky Security tasks	84
Viewing the list of application tasks	85
About information X-headers.....	86

ABOUT SCAN AND CONTENT FILTERING STATUSES

Based on the results of scanning for spam, the Anti-Spam engine assigns one of the following Anti-Spam scan statuses to messages:

- *Clean* – the message contains no spam.
- *Spam* – the application unambiguously recognizes the message as spam.
- *Probable Spam* – the message may contain spam.
- *Blacklisted* – the sender's email address or IP address is contained in the black list of addresses.
- *Massmail* – the message belongs to a mass mailing campaign.
- *Error* – the scan returned an error.

Based on the results of scanning for viruses, the Anti-Virus engine assigns one of the following Anti-Virus scan statuses to messages:

- *Clean* – the object is not infected.
- *Infected* – the object is infected; either it cannot be disinfected, or disinfection has not been attempted.
- *Disinfected* – the object is disinfected.
- *Probably infected* – the object is probably infected with an unknown virus or a new modification of a known virus.

- *Encrypted* – the object cannot be scanned because it is encrypted.
- *Corrupted* – the object is damaged or an error occurred during the scan.

Based on the Anti-Phishing scan results, the Anti-Phishing engine assigns one of the following status labels to the message:

- *Clean* – the message does not contain phishing URLs, images or text that could trick users into disclosing confidential data to fraudsters, or links to websites with malware.
- *Phishing* – the application has found the message to contain images or text that could trick users into disclosing confidential data to fraudsters.
- *Malicious link* – the application has found the message to contain links to websites with malware.
- *Error* – the scan returned an error.

As a result of content filtering, the Scan Logic message scanning control module assigns one of the following content filtering statuses to messages:

- *Clean* – the message does not violate the content filter settings.
- *BannedFileName* – the message contains an attachment with a banned name.
- *BannedFileFormat* – the message contains an attachment having a banned file format.
- *SizeExceeded* – the message exceeds the maximum allowed size.

ABOUT MESSAGE PROCESSING RULES

A *message processing rule* (or rule) is a group of settings for multiple pairs of addresses of senders and recipients; Kaspersky Security applies the rule to all messages whose sender and recipient match one of the pairs. For a rule to be assigned to a message, the addresses of the sender and recipient must be specified in the rule settings.

By default, the application contains the following preset message processing rules:

- *WhiteList* – process messages from the white list.
- *BlackList* – process messages from the black list.
- *Default* – process messages according to the predefined settings.

When processing an email, the application checks each rule for the "sender - recipient" pair of addresses beginning with the highest-priority rule (1). If no match is found, the application checks the pair of addresses of the rule with the next highest priority (2). As soon as it finds the "sender - recipient" pair of addresses in any rule, the application applies the processing settings configured in that rule to the message.

If none of the rules contains the "sender - recipient" pair of addresses, the message is processed according to the preset settings of the Default rule.

You can customize the settings of each message processing rule.

MESSAGE PROCESSING ALGORITHM

The application processes mail message according to the following algorithm:

1. Scan Logic message scanning control module determines which message processing rules (see section "About message processing rules" on page [79](#)) apply to a message, judging by the combination of the sender and

recipient addresses, and chooses the rule with the highest priority. If no rule is found for the address pair, the application processes the message in accordance with the Default rule.

2. If the message is addressed to several recipients whose addresses belong to different rules, several virtual copies of the message are created in accordance with the number of rules. Each copy of the message is processed as per the rule assigned to the address of the recipient.
3. The further actions taken by the application depend on the settings of the selected message processing rule.
 - If the rule specifies that messages are to be scanned for spam, the Scan Logic module forwards the mail message to Anti-Spam engine for scanning.

The Anti-Spam engine scans the message and assigns one of the spam scan status labels to it. Information about the status assigned is contained in the special information X-header X-KLMS-AntiSpam-Status (see section "About information X-headers" on page [86](#)), which Scan Logic adds to the message after it is processed. Based on the results of message scanning, the Scan Logic module also adds a status tag at the beginning of the message subject (Subject field).

- If the rule specifies that messages are to be scanned for phishing threats, the Scan Logic module forwards the mail message to the Anti-Phishing engine for scanning.

The Anti-Phishing engine scans the message and assigns one of the phishing scan status labels to it. Information about the status assigned is contained in the special information X-header X-KLMS-AntiPhishing (see section "About information X-headers" on page [86](#)), which Scan Logic adds to the message after it is processed. Based on the results of message scanning, the Scan Logic module also adds a status tag at the beginning of the message subject (Subject field).

- If the rule specifies that messages are to be filtered for content, the Scan Logic module performs content filtering of the message by size, name, and format of attachments.

As a result of content filtering, Scan Logic assigns one of the following content filtering status labels to messages:

- If the rule specifies that messages are to be scanned for viruses, the Scan Logic module forwards the mail message to the Anti-Virus engine for scanning.

The mail format analyzer (MIME, RFC2822, UUE) built into the Anti-Virus engine parses the individual objects of the message: body, attachments, and others. Every object received is sent to Anti-Virus engine for scanning.

Anti-Virus first scans messages as one object and then one message part at a time and assigns one of the anti-virus scan status labels to the message. Based on the results of message scanning, the Scan Logic module adds a status tag at the beginning of the message subject (Subject field).

4. Depending on the status assigned, the application performs actions (see section "About actions on objects" on page [83](#)) on messages in accordance with the message processing rule.

ABOUT BLACK AND WHITE LISTS OF ADDRESSES

Black and white lists of addresses can be used to fine-tune the mail system's response to messages that are not spam officially (such as news feeds). Black lists of addresses can also be used to configure the application to block messages containing new types of threats and spam before Kaspersky Security databases have been updated.

There are two types of black and white lists of addresses:

- *Personal*. Contain the addresses of senders for a single recipient (see section "Adding personal black and white lists of addresses" on page [131](#)). A personal white list of addresses allows messages to pass through without anti-spam scanning. The messages are still scanned for phishing, viruses, and other threats, and content filtering is also performed.
- *Global*. Contain the addresses of senders and recipients. You can specify such lists in the preset BlackList and WhiteList message processing rules (see section "About message processing rules" on page [79](#)). You can also

create rules (see section "Configuring global black and white lists of addresses" on page [121](#)), specifying the addresses of senders and recipients whose messages should be rejected without scanning or allowed to pass without scanning. A global white list of addresses allows messages to pass through without scanning for spam, viruses, and phishing threats.

Messages whose sender and recipients have their addresses on a global black or white list of addresses are processed as follows:

- If the addresses of the sender and recipients of a message are on a global black list of addresses, the application rejects the message. The message does not reach the mail server of Kaspersky Security.
- If the addresses of the sender and recipients of a message are on a global white list of addresses, the application refers the message for further scanning, bypassing scanning by the Anti-Spam, Anti-Virus, and Anti-Phishing components.
- If the addresses of the sender and recipients of a message are both on the global white list and the global black list of addresses, the application processes the message according to a rule with a higher priority.

A message is processed according to the rule of a personal white list or personal black list of addresses if the rules of the global black list and global white list of addresses do not apply to it.

A message whose sender has his address on a personal black or white list of addresses is processed as follows:

- If the message sender's address is on a personal black list of addresses and one of the addresses of the message recipients belongs to the owner of the personal black list of addresses, the message is not delivered to the recipient who owns the personal black list. Depending on the action configured for messages from senders on a personal black list, the message is either deleted or quarantined.
- If the sender's address is on a personal white list of addresses, the message is delivered to the recipient depending on the results of scanning for viruses, phishing threats, and content filtering.
- If the sender's address is both on a personal white list and black list of addresses, the message is processed according to the rules of the personal white list of addresses.

CREATING MESSAGE PROCESSING RULES

➔ *To create a new rule:*

1. To create a new rule, use the command:

```
# /opt/kaspersky/klms/bin/klms-control --create-rule <rule name>
```

2. Set the rule priority using the command:

```
# /opt/kaspersky/klms/bin/klms-control \  
--set-rule-priority <rule ID> --before <rule ID>
```

The value can be set using any natural number.

3. Export rule settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \  
--get-rule-settings <rule ID> -f <rule settings file name> or  
--get-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

4. Open the XML file to edit the rule settings.

- In the <belongingCriteria> section, specify the addresses of the sender and recipient in the <sender> and <recipient> settings, respectively.

If you need to add several sender and recipient email addresses, each new email address must be in a separate <item> section, typed in a new string of the settings file.

Example:

```
<belongingCriteria>
<sender>
<item>
  <type>EMailMask</type>
  <value>*</value>
</item>
<item>
  <type>CIDR</type>
  <value>172.16.10.145</value>
</item>
</sender>
<recipient>
<item>
  <type>ExternalAccount</type>
  <value>CN=test10,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=sbs2k8,DC=local</value>
</item>
</recipient>
</belongingCriteria>
```

At least one of the sender, recipient values must be specified. If the description of the rule does not contain a sender or recipient value, the application applies the rule with the next highest priority.

You can use the symbols "*" and "?" to create an address mask, and regular expressions beginning with the prefix "re:".

Regular expressions are not case-sensitive.

- In the <ScanSettings> section, specify 1 as the value of the <active> setting to activate the rule.
- Specify the rule mode. To do so, in the <ScanSettings> section use one of the following values for the <ruleAction> setting:
 - Scan, if you want the application to process messages according to the configured scan settings;

- Skip (skip without scanning), if you want the application to process messages according to this rule in the same way as it does according to the rule of the global white list of addresses (see section "Configuring global black and white lists of addresses" on page [121](#));
 - Reject (reject without scanning), if you want the application to process messages according to this rule in the same way it does according to the rule of the global black list of addresses.
8. If necessary, configure the settings of Anti-Spam scanning (see section "Configuring Anti-Spam scan settings for a rule" on page [90](#)), Anti-Virus scanning, and content filtering (see section "Configuring Anti-Virus scan settings for a rule" on page [109](#)).

If the values of these settings have not been configured for a rule, the default settings are used.

9. Save the changes made.
10. To import rule settings from an XML file, use the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--set-rule-settings <rule ID> -f <rule settings file name> or
--set-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

You can later view the list of created rules (see section "Viewing the list of message processing rules" on page [83](#)).

VIEWING THE LIST OF MESSAGE PROCESSING RULES

You can view the list of all preset and newly created rules.

➤ *To view the list of rules, execute the following command:*

```
# /opt/kaspersky/klms/bin/klms-control --get-rule-list
```

The application displays the list of rules,

with the following information:

- Rule name
- Rule ID
- Rule priority
- Rule status (active or inactive)

ABOUT ACTIONS ON OBJECTS

Depending on the status assigned to messages based on the results of Anti-Virus and Anti-Spam scanning and content filtering, Kaspersky Security performs actions on messages and the objects that they contain. The application records the result of scanning in the event log (see section "About the event log" on page [156](#)).

In the rule settings, you can specify actions to be performed by the application on messages with a certain status.

The settings that define the actions can take the following values:

- Skip – deliver message to recipient with no changes.
- Reject – do not deliver message to recipient. If you select this action, the sending mail server receives a return code in response, indicating the occurrence of an error during delivery. The message is not delivered to the recipient.
- DeleteMessage – delete message. If you select this operation, the sending mail server receives a notification that the message has been received; however, the message is not delivered to the recipient.
- DeleteAttachment – delete attachment (applied only after an anti-virus scan).
- Cure – cure infected object (applied only after an anti-virus scan). When this action is selected, the application attempts to cure the infected object. If disinfection is impossible, the Reject, Delete Message or Delete Attachment action specified in the rule settings is applied to the object. If the administrator has not specified the action in the rule settings, the application performs the DeleteAttachment action.

ABOUT KASPERSKY SECURITY TASKS

Some of **Kaspersky Security functionality is implemented in the form of Tasks**. For instance, the Anti-Virus database update task UpdaterAVS (hereinafter also "Anti-Virus database update task") and the Anti-Spam database update task UpdaterASP (hereinafter also "Anti-Spam database update task") download and install Anti-Virus and Anti-Spam database updates. The scheduled report generation tasks DailyReport, WeeklyReport, and MonthlyReport generate application reports for a day, week, and month. The Notifier task forms notifications about events occurring during the operation of the application.

Kaspersky Security includes the following tasks:

- Auth (ID=1).
- Backup (ID=2).
- ScanLogic (ID=3).
- Facade (ID=4).
- AvServer (ID=5).
- AspServer (ID=6).
- EventManager (ID=7).
- Licenser (ID=8).
- Notifier (ID=9).
- Statistics (ID=10).
- Updater (ID=11).
- AspMoebius (ID=13).
- AspQuarantine (ID=14).
- SntpSender (ID=15).
- Snmp (ID=16).
- DailyReport (ID=17).

- WeeklyReport (ID=18).
- MonthlyReport (ID=19).
- EventLogger (ID=20).
- ScanServer (ID=21).
- KLRDS (ID=22).
- Ksn (ID=23).

Most of them are system tasks not to be configured by the administrator.

Kaspersky Security tasks can have one of the following statuses:

- *Started* – a running task.
- *Starting* – a task being launched.
- *Stopped* – a task that has stopped.
- *Failed* – a task that has ended with an error.

VIEWING THE LIST OF APPLICATION TASKS

➡ To view the list of application tasks, execute the following command:

```
# /opt/kaspersky/klms/bin/klms-control --get-task-list
```

The application displays the list of tasks.

The following task details are shown:

- Number of tasks.
- Task names.
- Task IDs.
- Task performance state (see section "About Kaspersky Security tasks" on page [84](#)).

The following example shows how task details are displayed (task name, task ID, task state, and task run ID):

Example:

Name: Notifier

ID: 9

State: Started

Runtime ID: 7

ABOUT INFORMATION X-HEADERS

After scanning message, the Scan Logic message scanning control module adds special information X-headers to the message header, such as:

- X-KLMS-Rule-ID: 1 – list of message processing rule IDs.
- X-KLMS-Message-Action: attachment removed, AntiVirus – action taken by the application on the message.
- X-KLMS-AntiVirus: Kaspersky Security 8.0 for Linux Mail Server, version 8.0.1.517, bases: 2013/11/19 06:41:00 – release date of anti-virus databases.
- X-KLMS-AntiSpam-Method: none – the method used to identify spam.
- X-KLMS-AntiSpam-Rate: 0 – rating assigned to the message by the Anti-Spam engine.
- X-KLMS-AntiSpam-Status: not_detected – status assigned to the message by the Anti-Spam engine based on the Anti-Spam scan results.
- X-KLMS-AntiSpam-Envelope-From: someemail@example.com – message sender.
- X-KLMS-AntiPhishing: Clean, 2013/11/13 18:22:56 – a general header for messages processed by the Anti-Phishing engine.

ANTI-SPAM PROTECTION

This section contains information about Anti-Spam protection of messages and how to configure it.

IN THIS SECTION:

About Anti-Spam protection	87
About external Anti-Spam message scanning services.....	87
Enabling and disabling the Anti-Spam engine.....	88
Enabling and disabling Anti-Spam scanning of messages for a rule.....	89
Configuring general Anti-Spam scan settings	89
Configuring Anti-Spam scan settings for a rule	90
Configuring Anti-Spam Quarantine settings	93
Limiting the size of messages to be scanned for spam	93

ABOUT ANTI-SPAM PROTECTION

One of the main tasks of Kaspersky Security is to filter out unwanted messages (spam) in the mail traffic of the server.

Messages are scanned for spam by the Anti-Spam engine. Anti-Spam engine scans each message for signs of spam. First, Anti-Spam engine scans the attributes of the message, such as sender and recipient addresses, size, and headers (including the From and To fields). Second, Anti-Spam engine analyzes the message content (including the Subject header) and attached files. Anti-Spam engine is enabled by default. If required, you can disable the Anti-Spam engine or disable Anti-Spam scanning for any rule. You also can limit the size of messages (see section "Limiting the size of messages to be scanned for spam" on page [93](#)) to be scanned for spam.

Depending on the sensitivity level, the application assigns messages in which spam or probable spam has been detected the specific statuses in accordance with the spam rating calculated by Anti-Spam. *Spam rating* is a whole number from 0 to 100 that reflects the number of times Anti-Spam engine was actuated in processing the message. The application also takes into account the responses from the DNSBL, SURBL and UDS servers and SPF technology to assign the spam rating.

Based on the scan results, the Anti-Spam engine assigns the message one of the spam scan statuses and adds a status tag at the beginning of the message subject (Subject field).

Depending on the status assigned to the message, the application performs an action (see section "About actions on objects" on page [83](#)) on the message in accordance with the message processing rule. You can specify actions to be performed by the application on messages with a certain status. The default action performed on messages is Skip.

ABOUT EXTERNAL ANTI-SPAM MESSAGE SCANNING SERVICES

To ensure more thorough Anti-Spam filtering of email messages, Kaspersky Security supports external services:

- DNSBL. Servers that host public lists of IP addresses identified in the distribution of spam.

- SURBL. SURBL is a list of hyperlinks to the resources advertised by spam senders.

During spam rating calculation, the application considers the weight assigned to each responding DNSBL and SURBL server.

- Reputation filtering. A cloud service that uses technologies for determining the reputation of messages.

The reputation filtering increases the accuracy of detection of spam messages. The high accuracy of spam detection is achieved owing to the high speed with which information about new types of spam is updated in the cloud service.

On detecting a potential spam message, Kaspersky Security temporarily places it in Anti-Spam Quarantine. The message remains in Anti-Spam Quarantine for the specified period of time, such as 30 minutes. When the Anti-Spam Quarantine period elapses, Kaspersky Security rescans the message. After re-scanning the message, the application can change its status to one of the following: *Spam / Massmail / Probable Spam / Clean*.

- SPF. SPF (Sender Policy Framework) allows validation of the sender's domain to make sure it is not forged. Domains use SPF to authorize certain computers to send mail on their behalf. If the sender of a message is not included in the list of authorized senders, the spam rating of the message is increased
- Enforced Anti-Spam Updates Service – instant update system for anti-spam signatures.

ENABLING AND DISABLING THE ANTI-SPAM ENGINE

You can enable or disable the Anti-Spam engine. Anti-Spam engine is enabled by default.

► *To enable or disable the Anti-Spam engine:*

1. Export the ScanLogic task settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--get-settings <ScanLogic task ID> -f <name of the settings file> or
# /opt/kaspersky/klms/bin/klms-control \
--get-settings ScanLogic -n -f <name of the settings file>
```

2. Open the XML file to edit the task settings.
3. In the <asSettings> section, specify one of the following values for the <enableAsScan> setting:

- 1, to enable the Anti-Spam engine;
- 0, to disable the Anti-Spam engine.

By default, the value is set to 1.

4. Save the changes made.
5. Import the ScanLogic task settings from an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--set-settings <ScanLogic task ID> -f <name of the settings file> or
# /opt/kaspersky/klms/bin/klms-control \
--set-settings ScanLogic -n -f <name of the settings file>
```


ENABLING AND DISABLING ANTI-SPAM SCANNING OF MESSAGES FOR A RULE

You can enable or disable Anti-Spam scanning of messages for any message processing rule.

➤ *To enable or disable Anti-Spam scanning of messages for a rule:*

1. Export rule settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--get-rule-settings <rule ID> -f <rule settings file name> or
--get-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

2. Open the XML file to edit the rule settings.
3. In the <engineSettings> subsection of the <asScanSettings> section, specify one of the following values of the <enableScan> setting:
 - 1, to enable Anti-Spam scanning of messages for this rule;
 - 0, to disable Anti-Spam scanning of messages for this rule.
4. Save the changes made.

5. To import rule settings from an XML file, use the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--set-rule-settings <rule ID> -f <rule settings file name> or
--set-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

CONFIGURING GENERAL ANTI-SPAM SCAN SETTINGS

You can configure general Anti-Spam scan settings. These settings apply to all message processing rules according to which the application performs scanning of messages for spam.

➤ *To configure general Anti-Spam scan settings:*

1. Export the ScanLogic task settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--get-settings <ScanLogic task ID> -f <name of the settings file> or
--get-settings ScanLogic -n -f <name of the settings file>
```

2. Open the XML file of the ScanLogic task to edit the task settings.
3. In the <asSettings> section, specify the values of the relevant Anti-Spam scan settings:

- In the <enableReputationFiltering> subsection, specify the value 1 to enable reputation filtering (see section "Configuring Anti-Spam Quarantine settings" on page 93) or 0 to disable reputation filtering. If the value in the <useKsnStatus> subsection is set to 0, reputation filtering is disabled.

Reputation filtering is enabled by default.

- In the <scanTimeLimit> subsection, specify the maximum duration of Anti-Spam scanning of a message in seconds. If the message has not been scanned during this time, the application issues an *Error* verdict — the message scan has returned an error.

The default maximum duration of Anti-Spam scanning of a message is 30 seconds.

- In the <useKsnStatus> subsection, specify the value 1 if you want the application to use information from Kaspersky Security Network when issuing a verdict on the message, or 0 if you do not want the application to use information from Kaspersky Security Network.

The use of information from Kaspersky Security Network is enabled by default.

- In the <useEnforcedAntiSpamUpdatesService> subsection, specify the value 1 to enable the Enforced Anti-Spam Updates service or 0 to disable the service.

The Enforced Anti-Spam Updates service is enabled by default.

- In the <externalServices> subsection, specify the relevant values for the following nodes:
 - <dnsTimeout> – the maximum time during which the application waits for a response from DNS servers (in seconds). The default value is 10 seconds.
 - <dnsblList> – the list of DNSBL servers from which the application will request information about the message being scanned. Each DNSBL server must be specified in the following format: <item>Server name or IP address</item>.
 - <surblList> – the list of SURBL servers from which the application will request information about the message being scanned. Each SURBL server must be specified in the following format: <item>Server name or IP address</item>.

4. Save the changes made.

5. Import the ScanLogic task settings from an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \  
  
--set-settings <ScanLogic task ID> -f <name of the settings file> or  
  
--set-settings ScanLogic -n -f <name of the settings file>
```

CONFIGURING ANTI-SPAM SCAN SETTINGS FOR A RULE

► To configure the Anti-Spam scan message processing settings:

1. Export rule settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \  
  
--get-rule-settings <rule ID> -f <rule settings file name> or  
  
--get-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

2. Open the XML file to edit the rule settings.

3. Specify the preferred action to be taken by the application (see section "About actions on objects" on page [83](#)) on messages. To do so, in the <asScanSettings>-section, specify the value Skip, DeleteMessage or Reject for the following settings:

- <spamAction>, if the message has the status *Spam*;
- <probableSpamAction>, if the message has the status *ProbableSpam*;
- <blacklistedAction>, if the message has the status *Blacklisted*;
- <massMailAction>, if the message has status as *MassMail*.

The default action for all statuses is Skip.

4. If you selected the DeleteMessage action at the previous step of the sequence, you can configure the application to move a message copy to Backup before deleting the message (see section "About Backup" on page [140](#)). To do so, in the <asScanSettings> section, specify the value 1 for the following settings:

- <backupSpam>, if the message has the status *Spam*;
- <backupProbableSpam>, if the message has the status *ProbableSpam*;
- <backupBlacklisted>, if the message has the status *Blacklisted*;
- <backupMassMail>, if the message has status as *MassMail*.

The default value for all statuses is set to 0 – do not move a message copy to Backup.

5. If you selected Skip at Step 3 of the sequence, you can edit the text of the tag added to the Subject field of the message. To do so, in the <asScanSettings> section, specify the text of the stamp as the value for the following settings:

- <spamMark>, if the message has the status *Spam*;
- <probableSpamMark>, if the message has the status *ProbableSpam*;
- <blacklistedMark>, if the message has the status *Blacklisted*;
- <massMailMark>, if the message has status as *MassMail*.

6. In the <maxSizeLimit> subsection, specify the maximum size of messages (in bytes) to be scanned by Anti-Spam. The value 0 is interpreted as the absence of a limit on the maximum message size.

By default, the value is set to 1.5 MB.

7. In the <externalServices> subsection, specify the external services (see section "About external Anti-Spam message scanning services" on page [87](#)) to be used by the application when scanning messages:

- <useDns> – enables / disables the use of external services when scanning messages. When the value is set to 0, the use of all external services is disabled.

The use of external services is enabled by default.

- <useSpf> – enables / disables the SPF technology when scanning messages.

SPF technology is enabled by default.

- <useSurbl> – enables / disables the use of a custom list of SURBL servers when scanning messages. You can specify the list of SURBL servers when configuring general Anti-Spam scan settings (see section "Configuring general Anti-Spam scan settings" on page [89](#)).

The SURBL service is enabled by default.

- <useSurbIDefaultList> – enables / disables message scanning with use of SURBL servers whose list is provided with application database updates.

The use of the standard list of SURBL servers is enabled by default.

- <useDnsbl> – enables / disables the use of a custom list of DNSBL servers when scanning messages. You can specify the list of DNSBL servers when configuring the general Anti-Spam scanning settings.

The use of the custom list of DNSBL servers is enabled by default.

- <useDnsblDefaultList> – enables / disables message scanning with use of DNSBL servers whose list is provided with application database updates.

The use of the standard list of DNSBL servers is enabled by default.

- <dnsHostInDns> – enables / disables the scanning of DNS for the address of the message sender.

The scanning of DNS for the address of the message sender is enabled by default.

- <dnsDynamicResolvedFrom> – enables / disables the scanning of the message sender against the database of bot nets. The scan uses a reverse DNS lookup of the sender's IP address.

If your mail server has users connected via a dial-up link, enabling this scan is not recommended.

The scanning of the message sender against the database of bot nets is disabled by default.

8. In the <advancedOptions> subsection, specify the values of additional Anti-Spam scan settings:

- <parseRtf> – enables / disables the scanning of RTF attachments.

The scanning of RTF attachments is disabled by default.

- <useGsg> – enables / disables enables graphics analysis technology during scanning.

Graphics analysis technology is enabled by default.

- <disableLangChinese> – enables / disables a higher spam rating for messages written in Chinese.

A higher spam rating for messages written in Chinese is disabled by default.

- <disableLangKorean> – enables / disables a higher spam rating for messages written in Korean.

A higher spam rating for messages written in Korean is disabled by default.

- <disableLangThai> – enables / disables a higher spam rating for messages written in Thai.

A higher spam rating for messages written in Thai is disabled by default.

- <disableLangJapanese> – enables / disables a higher spam rating for messages written in Japanese.

A higher spam rating for messages written in Japanese is disabled by default.

- <disableLangCyrillic> – enables / disables a higher spam rating for messages written in Cyrillic font.

A higher spam rating for messages written in Cyrillic font is disabled by default.

9. Save the changes made.

10. To import rule settings from an XML file, use the command:

```
# /opt/kaspersky/klms/bin/klms-control \
```

--set-rule-settings <rule ID> -f <rule settings file name> or

--set-rule-settings <rule name> -n -f <rule settings file name>

The <rule name> should be enclosed in double quotes if it contains blanks.

CONFIGURING ANTI-SPAM QUARANTINE SETTINGS

You can specify the period for keeping a message in Anti-Spam Quarantine and the maximum size of Anti-Spam Quarantine.

➤ *To configure the Anti-Spam Quarantine settings:*

1. Export the rule settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control --get-settings AspQuarantine -n -f <name of the settings file>
```

2. Open the XML file for editing.
3. Specify the maximum size of Anti-Spam Quarantine in the <MaxQuarantineSize> section. The size is specified in bytes.
4. Specify the period of time for keeping messages in Anti-Spam Quarantine in the <MaxObjectTimeout> section. Time period is specified in seconds.
5. Save the changes made.
6. Import Anti-Spam quarantine settings from an XML file using the command

```
# /opt/kaspersky/klms/bin/klms-control --set-settings -n -f <name of the settings file>
```

LIMITING THE SIZE OF MESSAGES TO BE SCANNED FOR SPAM

You can set the maximum size of messages to be scanned for spam.

➤ *To limit the size of messages to be scanned for spam:*

1. Export the ScanLogic task settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
```

```
--get-settings <ScanLogic task ID> -f <name of the settings file> or
```

```
--get-settings ScanLogic -n -f <name of the settings file>
```

2. Open the XML file of the ScanLogic task to edit the task settings.
3. Specify the maximum size of a message that should be scanned (0 – no size restriction). To this end, in the <engineSettings> subsection of the <asScanSettings> section, for the <maxSizeLimit> setting specify a value not exceeding 1073741824 bytes (or 1 GB).
4. Save the changes made.
5. Import the ScanLogic task settings from an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
```

```
--set-settings <ScanLogic task ID> -f <name of the settings file> or
```

```
--set-settings ScanLogic -n -f <name of the settings file>
```

ANTI-VIRUS PROTECTION

This section contains information about Anti-Virus protection of messages and how to configure it.

IN THIS SECTION:

About Anti-Virus protection.....	95
Enabling and disabling the Anti-Virus engine.....	95
Enabling and disabling Anti-Virus scanning for a rule.....	96
Configuring general Anti-Virus scan settings.....	97
Configuring the processing of a message that cannot be disinfected.....	98
Configuring Anti-Virus scan settings for a rule.....	99
Excluding messages from Anti-Virus scanning by attachment format.....	100
Excluding messages from Anti-Virus scanning by attachment name.....	101
Limiting the size of objects to be scanned for viruses.....	102

ABOUT ANTI-VIRUS PROTECTION

One of the main tasks of Kaspersky Security is to scan email messages for the presence of viruses and other threats, and cure infected objects using information from the current (latest) version of the Anti-Virus databases (see section "About database updates" on page [112](#)).

Messages are scanned for viruses and other threats by Anti-Virus engine. Anti-Virus engine scans the body of the message and all attached files in any format (attachments) using the Anti-Virus databases. Anti-Virus module also allows detecting and blocking email attachments that have been intended for a limited scope of recipients and created to perpetrate attacks aimed at software vulnerabilities. Based on the scan results, Anti-Virus assigns the message one of the virus scan statuses and adds a tag with the status at the beginning of the message subject (Subject field).

Depending on the status assigned to the message, the application performs an action (see section "About actions on objects" on page [83](#)) configured in the settings of the rule applied to the message. You can specify actions to be performed by the application on messages with a certain status. Before processing a message, the application saves its copy in Backup (see section "About Backup" on page [140](#)).

You can specify the maximum size of attachments to be scanned (see section "Limiting the size of objects to be scanned for viruses" on page [102](#)) and specify objects to be excluded from Anti-Virus scanning. The application can exclude from scanning attachments of particular formats (see section "Excluding messages from Anti-Virus scanning by attachment format" on page [100](#)) or attachments with specific names (see section "Excluding messages from Anti-Virus scanning by attachment name" on page [101](#)).

ENABLING AND DISABLING THE ANTI-VIRUS ENGINE

You can enable or disable the Anti-Virus engine. The Anti-Virus engine is enabled by default.

► *To enable or disable Anti-Virus engine:*

1. Export the ScanLogic task settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
```

```
--get-settings <ScanLogic task ID> -f <name of the settings file> or
```

```
--get-settings ScanLogic -n -f <name of the settings file>
```

- Open the XML file of the ScanLogic task to edit the task settings.
- In the <avSettings> section, specify one of the following values for the <enableAvScan> setting:
 - 1, to enable the Anti-Virus engine;
 - 0, to disable the Anti-Virus engine.

By default, the value is set to 1.

- Save the changes made.
- Import the ScanLogic task settings from an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
```

```
--set-settings <ScanLogic task ID> -f <name of the settings file> or
```

```
--set-settings ScanLogic -n -f <name of the settings file>
```

ENABLING AND DISABLING ANTI-VIRUS SCANNING FOR A RULE

You can enable or disable Anti-Virus scanning of messages for any message processing rule.

➤ *To enable or disable Anti-Virus scanning of messages for a rule:*

- Export rule settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
```

```
--get-rule-settings <rule ID> -f <rule settings file name> or
```

```
--get-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

- Open the XML file to edit the rule settings.
- In the <engineSettings> subsection of the <avScanSettings> section, specify one of the following values of the <enableScan> setting:
 - 1, to enable Anti-Virus scanning of messages for this rule;
 - 0, to disable Anti-Virus scanning of messages for this rule.

- Save the changes made.
- To import rule settings from an XML file, use the command:

```
# /opt/kaspersky/klms/bin/klms-control \
```

```
--set-rule-settings <rule ID> -f <rule settings file name> or
```



```
--set-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

CONFIGURING GENERAL ANTI-VIRUS SCAN SETTINGS

You can configure general Anti-Virus scan settings. These settings apply to all message processing rules according to which the application performs Anti-Virus scanning of messages.

➤ To configure general Anti-Virus scan settings:

1. Export the ScanLogic task settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--get-settings <ScanLogic task ID> -f <name of the settings file> or
--get-settings ScanLogic -n -f <name of the settings file>
```

2. Open the XML file of the ScanLogic task to edit the task settings.
3. In the <avSettings> section, specify the values of the relevant Anti-Virus scan settings:

- In the <scanTimeLimit> subsection, specify the maximum duration of Anti-Virus scanning of a message in seconds. If the message has not been scanned during the specified time, the application labels it as *Corrupted* – the object is damaged or an error occurred while scanning the object.

The default maximum duration of Anti-Virus scanning of a message is 180 seconds.

- In the <maxNestingLevel> subsection, specify the maximum nesting level of objects during Anti-Virus scanning. Nested objects include message attachments and archives packed inside other archives. For example, if the maximum object nesting level is set to 1, the application scans the message and its attachments of the first nesting level during an Anti-Virus scan. If these objects are found to contain threats, the application scans all attachments and objects of the first nesting level contained in them.

The default maximum nesting level for objects is 32.

- In the <useAnalyzer> subsection, specify the value 1 to enable the use of Heuristic Analyzer during Anti-Virus scanning, or 0 to disable Heuristic Analyzer.

The use of Heuristic Analyzer is enabled by default.

- In the <heuristicLevel> subsection, specify the level of heuristic analysis to be used during Anti-Virus scanning of messages. The following levels are available: Light, Medium, and Deep.

The default heuristic analysis level is set to Medium.

4. Save the changes made.
5. Import the ScanLogic task settings from an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--set-settings <ScanLogic task ID> -f <name of the settings file> or
--set-settings ScanLogic -n -f <name of the settings file>
```

CONFIGURING THE PROCESSING OF A MESSAGE THAT CANNOT BE DISINFECTED

You can configure the actions to be taken by the application when processing messages with objects that cannot be disinfected:

Messages with objects are recognized as messages that cannot be disinfected in the following cases:

- The application could not perform the DeleteAttachment action for the <InfectedFirstAction> rule setting.
- The application could not perform the DeleteAttachment action for the <InfectedSecondAction> rule setting.
- The application could not perform the DeleteAttachment action for the <corruptedAction> or <encryptedAction> rule setting.

► *To configure the settings for processing messages with objects that cannot be disinfected:*

1. Export the ScanLogic task settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--get-settings <ScanLogic task ID> -f <name of the settings file> or
--get-settings ScanLogic -n -f <name of the settings file>
```

2. Open the XML file of the ScanLogic task to edit the task settings.
3. In the <avSettings> section, go to the <emergencyAction> subsection and specify one of the following actions to be taken by the application on objects that could not be disinfected:

- RejectMessage if you want the application to reject a message with an object that cannot be disinfected.
- DeleteMessage if you want the application to delete a message with an object that cannot be disinfected.

The default action is DeleteMessage.

4. In the <avSettings> section, go to the <backupEmergency> subsection and specify one of the options for saving in Backup the messages with objects that could not be disinfected:

- 1 if you want the application to save in Backup a copy of the message being deleted.
- 0 if you want the application to delete the message without saving its copy.

By default, the value is set to 1.

5. Save the changes made.
6. Import the ScanLogic task settings from an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--set-settings <ScanLogic task ID> -f <name of the settings file> or
--set-settings ScanLogic -n -f <name of the settings file>
```

CONFIGURING ANTI-VIRUS SCAN SETTINGS FOR A RULE

► To configure Anti-Virus scan message processing settings:

1. Export rule settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--get-rule-settings <rule ID> -f <rule settings file name> or
--get-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

2. Open the XML file to edit the rule settings.
3. Specify the preferred action to be taken by the application on infected messages (messages with *Infected* status and messages with *Probably Infected* status that contain potentially malicious objects). To do so, in the <avScanSettings> section, specify the value Skip, Cure, DeleteMessage, DeleteAttachment or Reject for the <infectedFirstAction> setting:

The default action is Cure.

4. Specify the preferred action to be performed on infected messages (with *Infected* status) that cannot be disinfected. To do so, in the <avScanSettings> section, specify the value DeleteMessage, DeleteAttachment or Reject for the <infectedSecondAction> setting:

The default action is DeleteAttachment.

5. Specify the preferred action to be taken on messages with *Corrupted* and *Encrypted* status. To do so, in the <avScanSettings> section, specify the value Skip, DeleteMessage, DeleteAttachment or Reject for the following settings:

- <corruptedAction>, if the message has the status *Corrupted*;
- <encryptedAction>, if the message has the status *Encrypted*;

The default action for all statuses is Skip.

6. If you selected the DeleteMessage or DeleteAttachment actions at the previous steps of the sequence, you can configure the application to move a message copy to Backup before deleting the message (see section "About Backup" on page [140](#)). To do so, in the <asScanSettings> section, specify the value 1 for the following settings:

- <backupInfected>, if an infected or probably infected message is detected;
- <backupCorrupted>, if the message has the status *Corrupted*;
- <backupEncrypted>, if the message has the status *Encrypted*.

7. The default setting for messages with *Corrupted* and *Encrypted* status is 0 – do not save message copy in Backup.

8. If you selected Skip, Cure, or DeleteAttachment, at Steps 3-6 of the sequence, you can edit the text of the tag added to the Subject field of the message. To do so, in the <avScanSettings> section, specify the text of the stamp as the value for the following settings:

- <infectedMark>, if the message has status as *Infected* or *Probably Infected*;
- <disinfectedMark>, if the message is *Disinfected*;
- <corruptedMark>, if the message has the status *Corrupted*;

- `<encryptedMark>`, if the message has the status *Encrypted*;
9. Save the changes made.
 10. To import rule settings from an XML file, use the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--set-rule-settings <rule ID> -f <rule settings file name> or
--set-rule-settings <rule name> -n -f <rule settings file name>
```

The `<rule name>` should be enclosed in double quotes if it contains blanks.

If the attachment contains an archive with objects having different scan statuses, all objects of the message or the entire attachment are subject to one (most severe) action depending on all scan statuses assigned to objects in the archive.

EXCLUDING MESSAGES FROM ANTI-VIRUS SCANNING BY ATTACHMENT FORMAT

Kaspersky Security can exclude attachments of certain formats from Anti-Virus scanning of messages.

➤ To exclude attachments of certain formats from Anti-Virus scanning of messages:

1. Export rule settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--get-rule-settings <rule ID> -f <rule settings file name> or
--get-rule-settings <rule name> -n -f <rule settings file name>
```

The `<rule name>` should be enclosed in double quotes if it contains blanks.

2. Open the XML file to edit the rule settings.
3. In the `<engineSettings>` subsection of the `<avScanSettings>` section, specify 1 as the value of each relevant setting corresponding to the file format inside the `<excludedFormats>` subsection:
 - If executable files need to be excluded from scanning, in the `<executableCategory>` subsection specify the value 1 for the settings corresponding to the executable file formats that you want to exclude from scanning.
 - If document files need to be excluded from scanning, in the `<officeCategory>` subsection specify the value 1 for the settings corresponding to the document file formats that you want to exclude from scanning.
 - If multimedia files need to be excluded from scanning, in the `<multimediaSubcategory>` subsection specify the value 1 for the settings corresponding to the file formats that you want to exclude from scanning.
 - If image attachments need to be excluded from scanning, in the `<imageCategory>` subsection specify the value 1 for the settings corresponding to the file formats that you want to exclude from scanning.
 - If archived objects need to be excluded from scanning, in the `<archiveCategory>` subsection specify the value 1 for the settings corresponding to the file formats that you want to exclude from scanning.
 - If database files need to be excluded from the scan, in the `<databaseCategory>` subsection specify the value 1 for the settings corresponding to the file formats that you want to exclude from scanning.

4. Save the changes made.
5. To import rule settings from an XML file, use the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--set-rule-settings <rule ID> -f <rule settings file name> or
--set-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

EXCLUDING MESSAGES FROM ANTI-VIRUS SCANNING BY ATTACHMENT NAME

Kaspersky Security can exclude attachments with certain names from Anti-Virus scanning of messages.

► To exclude attachments with certain names from Anti-Virus scanning of messages:

1. Export rule settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--get-rule-settings <rule ID> -f <rule settings file name> or
--get-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

2. Open the XML file to edit the rule settings.
3. Specify the names of attachments to be excluded from scanning. To do so, in the <engineSettings> subsection of the <avScanSettings> section, specify the file name masks as the values of the <excludedNames> setting.

You can use the "*" and "?" symbols to create a name mask.

If you need to add several file names, each file name must be in a separate <item> section, typed in a new string of the settings file.

Example:

```
<excludedNames>
  <item>*.iso</item>
</excludedNames>
```

4. Save the changes made.
5. To import rule settings from an XML file, use the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--set-rule-settings <rule ID> -f <rule settings file name> or
--set-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

LIMITING THE SIZE OF OBJECTS TO BE SCANNED FOR VIRUSES

You can specify the maximum size of objects to be scanned for viruses and other threats.

➤ *To restrict the size to be scanned for viruses and other threats:*

1. Export rule settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \  
  
--get-rule-settings <rule ID> -f <rule settings file name> or  
  
--get-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

2. Open the XML file to edit the rule settings.
3. Specify the maximum size that should be scanned (0 - no size restriction). To this end, in the <engineSettings> subsection of the <avScanSettings> section, specify for the <maxSizeLimit> setting a value not exceeding 1073741824 bytes (or 1 GB).
4. Save the changes made.
5. To import rule settings from an XML file, use the command:

```
# /opt/kaspersky/klms/bin/klms-control \  
  
--set-rule-settings <rule ID> -f <rule settings file name> or  
  
--set-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

ANTI-PHISHING PROTECTION

This section contains information about Anti-Phishing protection of messages and how to configure it.

IN THIS SECTION:

About Anti-Phishing protection	103
Enabling and disabling the Anti-Phishing engine.....	103
Enabling and disabling Anti-Phishing scanning of messages for a rule.....	104
Configuring general Anti-Phishing scan settings	105
Configuring Anti-Phishing scan message processing settings	105

ABOUT ANTI-PHISHING PROTECTION

One of the tasks of Kaspersky Security is to filter out phishing threats and links to websites with malware from messages passing through the mail server. *Phishing* applies to messages with phishing URLs, containing images or text that could trick users into disclosing confidential data to fraudsters.

The Anti-Phishing engine scans messages for phishing threats and links to websites with malware. The Anti-Phishing engine analyzes the message content (including the Subject header) and attached files.

Based on the Anti-Phishing scan results, the application assigns the message one of the Anti-Phishing scan statuses and adds a status tag at the beginning of the message subject. The message status tag ("Subject" field) can be configured in the rule settings (see section "Configuring Anti-Phishing scan message processing settings" on page [105](#)).

Depending on the status assigned to the message, the application performs an action (see section "Configuring Anti-Phishing scan message processing settings" on page [105](#)) on the message in accordance with the message processing rule. You can specify actions to be performed by the application on messages with a certain status. The default action taken by the application on messages is Skip, with messages delivered to users unchanged.

The Anti-Phishing engine is enabled by default. If required, you can disable the Anti-Phishing engine or disable Anti-Phishing scanning for any rule.

ENABLING AND DISABLING THE ANTI-PHISHING ENGINE

You can enable or disable the Anti-Phishing engine. The Anti-Phishing engine is enabled by default.

► *To enable or disable the Anti-Phishing engine:*

1. Export the ScanLogic task settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \  
  
--get-settings <ScanLogic task ID> -f <name of the settings file> or  
  
--get-settings ScanLogic -n -f <name of the settings file>
```

2. Open the XML file of the ScanLogic task to edit the task settings.
3. In the <apSettings> section, specify one of the following values for the <enableAsScan> setting:

- 1, to enable the Anti-Phishing engine;
- 0, to disable the Anti-Phishing engine.

By default, the value is set to 1.

4. Save the changes made.
5. Import the ScanLogic task settings from an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--set-settings <ScanLogic task ID> -f <name of the settings file> or
--set-settings ScanLogic -n -f <name of the settings file>
```

ENABLING AND DISABLING ANTI-PHISHING SCANNING OF MESSAGES FOR A RULE

You can enable or disable Anti-Phishing scanning of messages for any message processing rule.

➤ *To enable or disable Anti-Phishing scanning of messages for a rule:*

1. Export rule settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--get-rule-settings <rule ID> -f <rule settings file name> or
--get-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

2. Open the XML file to edit the rule settings.
3. In the <engineSettings> subsection of the <apScanSettings> section, specify one of the following values of the <enableScan> setting:
 - 1, to enable Anti-Phishing scanning of messages for this rule;
 - 0, to disable Anti-Phishing scanning of messages for this rule.

4. Save the changes made.
5. To import rule settings from an XML file, use the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--set-rule-settings <rule ID> -f <rule settings file name> or
--set-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

CONFIGURING GENERAL ANTI-PHISHING SCAN SETTINGS

You can configure general Anti-Phishing scan settings. These settings apply to all message processing rules according to which the application performs scanning of messages.

➤ *To configure general Anti-Phishing scan settings:*

1. Export the ScanLogic task settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--get-settings <ScanLogic task ID> -f <name of the settings file> or
--get-settings ScanLogic -n -f <name of the settings file>
```

2. Open the XML file of the ScanLogic task to edit the task settings.

3. In the <apSettings> section, specify the values of the relevant Anti-Phishing scan settings:

- In the <scanTimeLimit> subsection, specify the maximum duration of Anti-Phishing scanning of a message in seconds. If the message has not been scanned during this time, the application issues an *Error* verdict — the message scan has returned an error.

The default maximum duration of scanning is 30 seconds.

- In the <enableHeuristic> subsection, specify the value 1 to enable Heuristic Analyzer during Anti-Phishing scanning, or 0 to disable Heuristic Analyzer.

The use of Heuristic Analyzer is enabled by default.

- In the <useKsnStatus> subsection, specify the value 1 if you want the application to use information from Kaspersky Security Network when issuing a phishing verdict on the message, or 0 if you do not want the application to use information from Kaspersky Security Network.

The use of information from Kaspersky Security Network is enabled by default.

4. Save the changes made.

5. Import the ScanLogic task settings from an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--set-settings <ScanLogic task ID> -f <name of the settings file> or
--set-settings ScanLogic -n -f <name of the settings file>
```

CONFIGURING ANTI-PHISHING SCAN MESSAGE PROCESSING SETTINGS

➤ *To configure the Anti-Phishing scan message processing settings:*

1. Export rule settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--get-rule-settings <rule ID> -f <rule settings file name> or
```

```
--get-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

2. Open the XML file to edit the rule settings.
3. Specify the preferred action to be taken by the application (see section "About actions on objects" on page [83](#)) on messages. To do so, in the <apScanSettings> section specify the value Skip, DeleteMessage or Reject for the <phishingAction> setting if the message has status as *Phishing* or *Malicious link*.

The default action is Skip.

4. If you selected the DeleteMessage action at the previous step of the sequence, you can configure the application to move a copy of the message found to contain a phishing threat to Backup before deleting the message (see section "About Backup" on page [140](#)). To do so, in the <apScanSettings> section, specify the value 1 for the <backupPhishing> setting.
5. If you selected Skip at Step 3 of the sequence, you can edit the text of the tag added to the Subject field of the message. To do so, in the <apScanSettings> section, specify the text of the stamp as the value for the following settings:
 - <phishingMark>, if the message has *Phishing* status;
 - <maliciousMark>, if the message has *Malicious link* status.

6. Save the changes made.
7. To import rule settings from an XML file, use the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--set-rule-settings <rule ID> -f <rule settings file name> or
--set-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

CONTENT FILTERING OF MESSAGES

This section contains information about content filtering of messages and how to configure it.

IN THIS SECTION:

About content filtering.....	107
Enabling and disabling content filtering of messages.....	107
Enabling and disabling content filtering of messages for a rule.....	108
Configuring content filtering by message size	109
Configuring content filtering by attachment name	109
Configuring content filtering by attachment format.....	110

ABOUT CONTENT FILTERING

Kaspersky Security can perform content filtering of messages that pass through the mail server.

Content filtering of messages is performed in the following ways:

- by message size (see section "Configuring content filtering by message size" on page [109](#));
- by mask of attachment names (see section "Configuring content filtering by attachment name" on page [109](#));
- by attachment format (see section "Configuring content filtering by attachment format" on page [110](#)).

You can specify the maximum size of messages, mask undesirable file names, and specify undesirable file formats.

As a result of content filtering, the message scanning control module assigns one of the content filtering statuses to the message.

Depending on the status assigned to the message, the application performs an action (see section "About actions on objects" on page [83](#)) configured in the settings of the rule applied to the message. You can specify actions to be performed by the application on messages with a certain status. The program rejects messages by default.

By default, content filtering of messages is disabled. You can enable content filtering of messages by the application or enable content filtering of messages for any rule (see section "Enabling and disabling content filtering of messages for a rule" on page [108](#)).

ENABLING AND DISABLING CONTENT FILTERING OF MESSAGES

You can enable or disable content filtering of messages by the application. By default, content filtering of messages is disabled.

➤ *To enable or disable content filtering of messages:*

1. Export the ScanLogic task settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
```

```
--get-settings <ScanLogic task ID> -f <name of the settings file> or
```

```
--get-settings ScanLogic -n -f <name of the settings file>
```

2. Open the XML file of the ScanLogic task to edit the task settings.
3. In the <cfSettings> section, specify one of the following values for the <enableCfScan> setting:
 - 1, to enable content filtering of messages;
 - 0, to disable content filtering of messages.
4. Save the changes made.
5. Import the ScanLogic task settings from an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
```

```
--set-settings <ScanLogic task ID> -f <name of the settings file> or
```

```
--set-settings ScanLogic -n -f <name of the settings file>
```

ENABLING AND DISABLING CONTENT FILTERING OF MESSAGES FOR A RULE

You can enable or disable content filtering of messages for any message processing rule.

➤ *To enable or disable content filtering of messages for a rule:*

1. Export rule settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
```

```
--get-rule-settings <rule ID> -f <rule settings file name> or
```

```
--get-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

2. Open the XML file to edit the rule settings.
3. In the <engineSettings> subsection of the <cfScanSettings> section, specify one of the following values of the <enableScan> setting:
 - 1, to enable content filtering of messages for this rule;
 - 0, to disable content filtering of messages for this rule.
4. Save the changes made.
5. To import rule settings from an XML file, use the command:

```
# /opt/kaspersky/klms/bin/klms-control \
```

```
--set-rule-settings <rule ID> -f <rule settings file name> or
```

```
--set-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

CONFIGURING CONTENT FILTERING BY MESSAGE SIZE

► To configure content filtering by message size, do the following:

1. Export rule settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--get-rule-settings <rule ID> -f <rule settings file name> or
--get-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

2. Open the XML file to edit the rule settings.
3. Enable content filtering of messages. To do so, in the <engineSettings> subsection of the <cfScanSettings> section, specify the value 1 for the <enableScan> setting.
4. Specify the maximum allowed message size (0 - no size restriction). To this end, in the <engineSettings> subsection of the <cfScanSettings> section, specify a value for the <maxAllowedSize> setting not exceeding 1073741824 bytes (or 1 GB).
5. Specify the preferred action to be taken by the application (see section "About actions on objects" on page [83](#)) on messages exceeding the specified size. To do so, in the <cfScanSettings> section, specify the value Skip, DeleteMessage or Reject for the <sizeExceededAction> setting:

The default action is Reject.

6. If necessary, you can configure the application to move messages exceeding the specified size to Backup (see section "About Backup" on page [140](#)). To do so, in the <cfScanSettings> section, specify the value 1 for the <backupSizeExceeded> setting.
7. Save the changes made.
8. To import rule settings from an XML file, use the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--set-rule-settings <rule ID> -f <rule settings file name> or
--set-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

CONFIGURING CONTENT FILTERING BY ATTACHMENT NAME

► To configure content filtering of messages by attachment name:

1. Export rule settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--get-rule-settings <rule ID> -f <rule settings file name> or
```

```
--get-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

2. Open the XML file to edit the rule settings.
3. Enable content filtering of messages. To do so, in the <engineSettings> subsection of the <cfScanSettings> section, specify the value 1 for the <enableScan> setting.
4. Specify the names of attached files that are banned. To do so, in the <engineSettings> subsection of the <cfScanSettings> section, specify the file name masks as the values of the <bannedFileNames> setting.

You can use the "*" and "?" symbols to create a name mask.

If you need to add several file names, each file name must be in a separate <item> section, typed in a new string of the settings file.

Example:

```
<bannedFileNames>
  <item>*.exe</item>
</bannedFileNames>
```

5. Specify the preferred action to be taken by the application (see section "About actions on objects" on page [83](#)) on messages with attachments that have banned names. To do so, in the <cfScanSettings> section, specify the value Skip, DeleteMessage, DeleteAttachment or Reject for the <bannedFileNameAction> setting.

The default action is Reject.

6. If necessary, you can configure the application to move copies of messages with attachments that have banned names to Backup (see section "About Backup" on page [140](#)). To do so, in the <cfScanSettings> section, specify the value 1 for the <backupBannedFileName> setting.
7. Save the changes made.
8. To import rule settings from an XML file, use the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--set-rule-settings <rule ID> -f <rule settings file name> or
--set-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

CONFIGURING CONTENT FILTERING BY ATTACHMENT FORMAT

➤ *To configure content filtering of messages by attachment format:*

1. Export rule settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--get-rule-settings <rule ID> -f <rule settings file name> or
```

```
--get-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

2. Open the XML file to edit the rule settings.
3. Enable content filtering of messages. To do so, in the <engineSettings> subsection of the <cfScanSettings> section, specify the value 1 for the <enableScan> setting.
4. Specify the formats of attached files that are banned. To do so, in the <engineSettings> subsection of the <cfScanSettings> section, specify the value 1 for each setting corresponding to file formats inside the <bannedFileFormat> subsection.
 - To block the sending of executable files, in the <executableCategory> subsection specify the value 1 for the settings corresponding to the executable file formats that you want to block.
 - To block the sending of document files, in the <officeCategory> subsection specify the value 1 for the settings corresponding to the file formats that you want to block.
 - To block the sending of multimedia files, in the <multimediaSubcategory> subsection specify the value 1 for the settings corresponding to the file formats that you want to block.
 - To block the sending of image attachments, in the <imageCategory> subsection specify the value 1 for the settings corresponding to the file formats that you want to block.
 - To block the sending of archived objects, in the <archiveCategory> subsection specify the value 1 for the settings corresponding to the file formats that you want to block.
 - To block the sending of database files, in the <databaseCategory> subsection specify the value 1 for the settings corresponding to the file formats that you want to block.
5. Specify the preferred action to be taken by the application (see section "About actions on objects" on page [83](#)) on messages with attachments of banned formats. To do so, in the <cfScanSettings> section, specify the value Skip, DeleteMessage, DeleteAttachment or Reject for the <bannedFileFormatAction> setting.

The default action is Reject.

6. If necessary, you can configure the application to move copies of messages with attachments of banned formats to Backup (see section "About Backup" on page [140](#)). To do so, in the <cfScanSettings> section, specify the value 1 for the <backupBannedFileFormat> setting.
7. Save the changes made.
8. To import rule settings from an XML file, use the command:

```
# /opt/kaspersky/klms/bin/klms-control \
```

```
--set-rule-settings <rule ID> -f <rule settings file name> or
```

```
--set-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

UPDATING KASPERSKY SECURITY DATABASES

This section contains information about updating Anti-Virus, Anti-Spam, and Anti-Phishing databases.

IN THIS SECTION:

About database updates	112
Checking database state	112
About update sources	114
Select update source.....	114
Configuring the proxy server settings	116
Configuring the update task schedule	117
Update task schedule settings.....	117
Manual database update.....	119

ABOUT DATABASE UPDATES

Anti-Virus databases, Anti-Spam databases, and Anti-Phishing databases (hereafter also "databases") are files containing records that can be used to detect malicious code in scanned objects. These records contain information about the control sections of malicious code and algorithms used for disinfecting objects that contain such threats.

Virus analysts at Kaspersky Lab detect hundreds of new threats daily, create records to identify them, and include them in *database updates packages* (or update packages). Update packages consist of one or several files containing records to identify threats that were detected since the previous update package was released. In order to minimize the risk of infecting the protected server, we recommend that you receive database update packages regularly.

As long as the license is in effect, you can receive database update packages from Kaspersky Lab's website automatically on schedule, or download and install them manually.

During installation, Kaspersky Security downloads the latest databases from one of Kaspersky Lab's update servers. If you have configured automatic database updates, Kaspersky Security runs updates according to schedule (with a frequency of once per 5 minutes).

Kaspersky Security periodically and automatically checks for new update packages on Kaspersky Lab's update servers. By default, if the Kaspersky Security databases have not been updated for a week since Kaspersky Lab released the last updates, Kaspersky Security logs the event *Databases are out of date*. If the databases have not been updated for two weeks, Kaspersky Security logs the event *Databases are extremely out of date*. You can configure administrator notifications about these events.

CHECKING DATABASE STATE

Databases can exist in one of the three states:

- Up to date (UpToDate)

- Outdated (Outdated)
- Obsolete (Obsoleted)

➤ *To check the state of Anti-Virus databases:*

```
# /opt/kaspersky/klms/bin/klms-control --get-avs-bases-info
```

The application keeps the following information on Anti-Virus databases:

- state of Anti-Virus databases: up to date (UpToDate), outdated (Outdated), or obsolete (Obsoleted).
- Number of records.
- Anti-Virus database release date;
- The time when Anti-Virus databases were installed in the application.

The following example shows the command output:

Example:

```
<root>
  <status>UpToDate</status>
  <recordCount>8095519</recordCount>
  <publishingTime>Fri Jun 11 16:40:00 2012</publishingTime>
  <installTime>Fri Jun 11 4:53:12 PM 2012</installTime>
</root>
```

➤ *To check the state of Anti-Spam databases:*

```
# /opt/kaspersky/klms/bin/klms-control --get-asp-bases-info
```

The application shows the following information about Anti-Spam databases:

- state of Anti-Spam databases: up to date (UpToDate), outdated (Outdated), or obsolete (Obsoleted).
- Anti-Spam database release date;
- The time when Anti-Spam databases were installed in the application.

The following example shows the command output:

Example:

```
<root>
  <status>UpToDate</status>
  <publishingTime>Fri Jun 8 11:40:36 2012</publishingTime>
  <installTime>Fri Jun 8 11:50:12 AM 2012</installTime>
</root>
```

- To check the state of Anti-Phishing databases:

```
# /opt/kaspersky/klms/bin/klms-control --get-aph-bases-info
```

The application shows the following information about Anti-Phishing databases:

- state of Anti-Phishing databases: up to date (UpToDate), outdated (Outdated), or obsolete (Obsoleted).
- Anti-Phishing database release date;
- The time when Anti-Phishing databases were installed in the application.

The following example shows the command output:

Example:

```
<root>
  <status>UpToDate</status>
  <publishingTime>Fri Jun 8 11:40:36 2012</publishingTime>
  <installTime>Fri Jun 8 11:50:12 AM 2012</installTime>
</root>
```

ABOUT UPDATE SOURCES

Updates source is a resource containing updates for Kaspersky Security databases.

The main update source is Kaspersky Lab's update servers. These are special Internet sites which contain updates for databases and application modules for all Kaspersky Lab products. If you use a proxy server to connect to the Internet, you should configure its settings.

To reduce the amount of Internet traffic, you can configure Kaspersky Security databases from a *custom update source*. In addition, HTTP or FTP servers or local directories on the user's computer can serve as custom updates sources.

If Kaspersky Security is managed using Kaspersky Security Center, you can specify Kaspersky Security Center as the update source.

SELECTING AN UPDATE SOURCE

Kaspersky Lab update servers or custom update sources can be specified as update sources for the Anti-Virus and Anti-Spam database update tasks (see section "About update sources" on page [114](#)).

Kaspersky Security does not support updates from HTTP and FTP servers with authentication.

- To select a custom update source:

1. To export update task settings to an XML file, use the command:

```
# /opt/kaspersky/klms/bin/klms-control \
  --get-settings <update task ID> -f <file name> or
  --get-settings Updater -n -f <file name>
```

2. Open the XML file to edit the task settings.
3. In the <updateCommonSettings> section, specify Custom as the value of the sourceType setting:

```
<sourceType>Custom</sourceType>
```
4. In the <customSources> subsection, specify the custom update source (a local folder on the computer or HTTP/FTP server).

If you need to add several custom update sources, each new custom update source must be in a separate <item> section, typed in a new string of the settings file.

Example:

```
<updateCommonSettings>
  <sourceType>Custom</sourceType>
  <customSources>
    <item>
      ftp://172.16.10.145/xz6
    </item>
    <item>
      http://172.16.10.145/xz6
    </item>
  </customSources>
```

5. Save the changes made.
6. To import settings from an XML file to an update task, use the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--set-settings <update task ID> -f <file name> or
--set-settings Updater -n -f <file name>
```

➡ *To select Kaspersky Lab's update servers as an update source:*

1. To export update task settings to an XML file, use the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--get-settings <update task ID> -f <file name> or
--get-settings Updater -n -f <file name>
```

2. Open the XML file to edit the task settings.
3. In the <updateCommonSettings> section, specify KLServers as the value of the sourceType setting:

```
<sourceType>KLServers</sourceType>
```

4. Save the changes made.

- To import settings from an XML file to an update task, use the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--set-settings <update task ID> -f <file name> or
--set-settings Updater -n -f <file name>
```

- *To select Kaspersky Security Center as an update source:*

- To export update task settings to an XML file, use the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--get-settings <update task ID> -f <file name> or
--get-settings Updater -n -f <file name>
```

- Open the XML file to edit the task settings.
- In the <updateCommonSettings> section, specify SCServer as the value of the sourceType setting:

```
<sourceType>SCServer</sourceType>
```

- Save the changes made.
- To import settings from an XML file to an update task, use the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--set-settings <update task ID> -f <file name> or
--set-settings Updater -n -f <file name>
```

CONFIGURING THE PROXY SERVER SETTINGS

If you use a proxy server to connect to the Internet, you should configure its settings.

- *To enable configure the settings of a proxy server for accessing update sources:*

- Export the Kaspersky Security general settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--get-app-settings -f <file name>
```

- Open the XML file to edit the task settings.
- Enable the use of a proxy server for accessing update sources. To do so, specify the values in the following subsections of the <proxySettings> section:

- In the <enable> subsection, specify the value 1 to enable the use of a proxy server.

The proxy server usage option is enabled by default.

- In the <serverAddress> subsection, specify the name or IP address of the proxy server.

- In the <port> subsection, specify the port number for connecting to the proxy server.

The default port number is 8080.

- d. In the <authenticationType> subsection, specify the value NotRequired if authentication is not required to connect to the proxy server, or Plain if authentication is required.
- e. If the connection to the proxy server requires authentication, specify the user name and password in the <user> and <password> subsections.
- f. In the <proxyBypassLocalAddresses> subsection, specify the value 1 to disable the use of a proxy server for local company addresses, or 0 to enable the use of a proxy server for local company addresses.

By default, the value is set to 1.

4. Save the changes made.
5. To import settings from an XML file, use the command:

```
# /opt/kaspersky/klms/bin/klms-control \  
  
--set-app-settings -f <file name>
```

CONFIGURING THE UPDATE TASK SCHEDULE

If you did not configure a scheduled update of databases (see section "Step 13. Configuring databases updates" on page [39](#)) while preparing the application for operation, you can configure the schedule of the Anti-Virus and Anti-Spam database update tasks manually.

➔ *To configure the update task startup schedule:*

1. To export update task settings to an XML file, use the command:

```
# /opt/kaspersky/klms/bin/klms-control \  
  
--get-settings <update task ID> -f <file name> or  
  
--get-settings Updater -n -f <file name>
```

2. Open the XML file to edit the task settings.
3. In the <schedule> section, specified the preferred settings (see section "Update task schedule settings" on page [117](#)).
4. Save the changes made.
5. To import settings from an XML file to an update task, use the command:

```
# /opt/kaspersky/klms/bin/klms-control \  
  
--set-settings <update task ID> -f <file name> or  
  
--set-settings Updater -n -f <file name>
```

UPDATE TASK SCHEDULE SETTINGS

The <schedule> section of the file containing the database update task settings is structured as follows:

```
<schedule>  
  
  <ruleType>Once|Monthly|Weekly|Daily|Hourly|Minutely|Manual</ruleType>  
  
  <startByTime>
```

```
<year><year></year>  
<month><month></month>  
<day>day of month|day of week</day>  
<hour><hours></hour>  
<min><minutes></min>  
<sec><seconds></sec>  
<dayOfMonth><day of month></dayOfMonth>  
<dayOfWeek><day of week></dayOfWeek>  
<timePeriod><1></timePeriod>  
</startByTime>  
<randInterval><minutes></randInterval>  
<execTimeLimit><minutes></execTimeLimit>  
<runMissed><0|1></runMissed>  
</schedule>
```

Table 4. Update task schedule settings

SETTING	DESCRIPTION AND POSSIBLE VALUES
ruleType	The Starting a scheduled task mode. Possible values include: <ul style="list-style-type: none"> • Once – once. • Monthly – monthly. • Weekly – weekly. • Daily – every N day. • Hourly – every N hour. • Minutely – every N minutes. • Manual – manually.
startByTime	Start time. If you do not specify a start time, the current system date and / or time is set by default (see table below).
randInterval	Randomize the task launch within a time interval (in minutes) to equalize the load on the mail server while multiple scheduled tasks are running simultaneously. Format – [0;999].
execTimeLimit	Limit the duration of the task interval (in minutes). Format – [0;999].
runMissed	Run missed tasks. Possible values include: <ul style="list-style-type: none"> • 1 – run missed tasks the next time the application is started; • 0 – run only scheduled tasks.

Table 5. Field values of the startByTime setting

SETTING	THE STARTBYTIME SETTING VALUE
<year>	year [present year -1;present year +10]
<month>	month [JAN FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC]
<day>,<dayOfMonth>	day of month [1;31]
<hour>	hour [00;23]
<min>	minutes [00;59]
<sec>	seconds [00;59]
<dayOfWeek>	day of week [MON TUE WED THU FRI SAT SUN]
<timePeriod>	time period [0-999], where 0 indicates the start period is not set

UPDATING DATABASES MANUALLY

If you have not configured scheduled database updates (see section "Configuring the update task schedule" on page [117](#)), you can update the Anti-Virus, Anti-Spam and Anti-Phishing databases manually.

➤ To update the Kaspersky Security databases manually:

```
klms-control --start-task Updater -n --progress
```


ADVANCED CONFIGURATION OF KASPERSKY SECURITY

This section describes how to perform an advanced configuration of Kaspersky Security.

IN THIS SECTION:

Configuring global black and white lists of addresses	121
Setting the number of scanning streams	123
Importing / exporting settings	123

CONFIGURING GLOBAL BLACK AND WHITE LISTS OF ADDRESSES

The settings of global black and white lists of addresses are contained in the preset BlackList (ID=2) and WhiteList (ID=3) message processing rules.

In addition, when creating a new rule (see section "Creating message processing rules" on page [81](#)), you can specify one of the rule modes: reject messages without scanning (in which case the application processes messages according to this rule in the same way as it does according to the BlackList rule) or skip messages without scanning (in which case the application processes messages according to this rule in the same way as it does according to the WhiteList rule).

➤ *To configure a global black or white list of addresses:*

1. Export the rule settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \  
  
--get-rule-settings <rule ID> -f <rule settings file name> or  
  
--get-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

To export the settings of the BlackList rule, execute the command

```
# /opt/kaspersky/klms/bin/klms-control \  
  
--get-rule-settings BlackList -n -f <name of the rule settings file>
```

To export the settings of the WhiteList rule, execute the command

```
--get-rule-settings WhiteList -n -f <name of the rule settings file>
```

2. Open the XML file to edit the rule settings.
3. Make the required changes in the <belongingCriteria> section, specifying the addresses of the sender and recipient in the <sender> and <recipient> settings, respectively.

If you need to add several sender and recipient email addresses, each new email address must be in a separate <item> section, typed in a new string of the settings file.

Example:

```
<belongingCriteria>
  <sender>
    <item>
      <type>EMailMask</type>
      <value>*</value>
    </item>
    <item>
      <type>CIDR</type>
      <value>172.16.10.145</value>
    </item>
  </sender>
  <recipient>
    <item>
      <type>ExternalAccount</type>
      <value>CN=test10,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=sbs2k8,DC=local</value>
    </item>
  </recipient>
</belongingCriteria>
```

You can use the symbols "*" and "?" to create an address mask, and regular expressions beginning with the prefix "re:".

Regular expressions are not case-sensitive.

4. In the <ScanSettings> section, specify 1 as the value of the <active> setting to activate the rule.
5. Save the changes made.
6. To import rule settings from an XML file, use the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--set-rule-settings <rule ID> -f <rule settings file name> or
--set-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

SETTING THE NUMBER OF SCANNING STREAMS

The number of scanning streams is set to enable you to correctly balance the load on the mail server processors.

➤ *To set the number of scanning streams:*

1. Export the ScanLogic task settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--get-settings <ScanLogic task ID> -f <name of the settings file> or
--get-settings ScanLogic -n -f <name of the settings file>
```

2. Open the XML file of the ScanLogic task to edit the task settings.
3. In the <scanThreads> section, change the number of scan threads. The default number of scan threads is eight.
4. Save the changes made.
5. Import the ScanLogic task settings from an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--set-settings <ScanLogic task ID> -f <name of the settings file> or
--set-settings ScanLogic -n -f <name of the settings file>
```

IMPORTING / EXPORTING SETTINGS

You can export task settings and other application settings to a file for use during installation of the application on a different mail server.

➤ *To export Kaspersky Security task settings to a file, execute the following command:*

```
# /opt/kaspersky/klms/bin/klms-control --export-settings -f <name of the settings file>
```

➤ *To import Kaspersky Security task settings from a file, execute the following command:*

```
# /opt/kaspersky/klms/bin/klms-control --import-settings -f <name of the settings file>
```

➤ *To export Kaspersky Security rule settings to a file, execute the following command:*

```
# /opt/kaspersky/klms/bin/klms-control --export-rules -f <name of the settings file>
```

➤ *To import Kaspersky Security rule settings from a file, execute the following command:*

```
# /opt/kaspersky/klms/bin/klms-control --import-rules -f <name of the settings file>
```

INTEGRATION WITH AN EXTERNAL DIRECTORY SERVICE USING THE LDAP PROTOCOL

This section describes how you can integrate Kaspersky Security with an external directory service that supports the LDAP protocol and use custom scripts to search for information in the external directory service.

IN THIS SECTION:

About integration with an external directory service	124
Configuring Kaspersky Security integration with an external directory service with the help of user scripts	125
Requirements for user scripts.....	125
Searchemail user script.....	126
Searchusers user script.....	127
Getuseraccount user script	127
Login user script.....	128
Configuring the application connection to an external directory service using the LDAP protocol	128
Checking the application connection to an external directory service using the LDAP protocol	129
Adding senders / recipients from an external user service to rules	129
Adding personal black and white lists of addresses	131
Managing untrusted certificates.....	132

ABOUT INTEGRATION WITH AN EXTERNAL DIRECTORY SERVICE

Kaspersky Security supports integration with the Active Directory external directory service and other external LDAP services.

Integration with an external directory service is required to perform the following tasks:

- Add senders / recipients from an external user service to message processing rules.
- Allow users to maintain personal black and white lists of addresses.
- Allow the recipient to view the recipient's messages in Backup.

Integration with an external directory service is performed with the help of user scripts (see section "Configuring integration of Kaspersky Security with an external directory service with the help of user scripts" on page [125](#)).

CONFIGURING KASPERSKY SECURITY INTEGRATION WITH AN EXTERNAL DIRECTORY SERVICE WITH THE HELP OF USER SCRIPTS

The following user scripts are used to integrate Kaspersky Security with an external directory service:

- searchemail – used for determining the IDs of an email message, list of user groups, sender, and recipient;
- searchusers – used for searching a user in an external directory service and for searching a user in custom white and black lists of addresses;
- getuseraccount – used for substituting user accounts with names while viewing a rule. If the script was started but did not perform its function, the rule displays the user IDs only;
- login – used during authorization of a user from an external directory service;
- checkconnection – used to check the availability of an external directory service. The results of user script operation are displayed in the Kaspersky Security web interface window on the **Monitoring** tab.

User scripts should be run for the user kluser. Any supported language can be used to write the user scripts.

➤ *To configure Kaspersky Security integration with an external directory service with the help of user scripts:*

1. Copy user scripts to one of the following folders:

- /etc/kaspersky/klms/scripts for a Linux operating system.
- /usr/local/etc/kaspersky/klms/scripts for a FreeBSD operating system.

2. Export the Auth task settings to an XML file using the command:

```
klms-control --get-settings Auth -n -f auth_settings.xml
```

3. Set the type of integration with the external directory service to user integration in the Auth task settings file with the following command:

```
sed -i 's|<integrationType>.*</integrationType>|<integrationType>Custom</integrationType>|g' auth_settings.xml
```

4. Import Auth task settings from the XML-file to the program with the following command:

```
klms-control --set-settings Auth -n -f auth_settings.xml
```

REQUIREMENTS FOR USER SCRIPTS

Kaspersky Security has the following requirements for user scripts:

- Data sent to a user script and retrieved as a result of script execution should end with a line that does not contain characters, but contains ".\n".
- If data requested during user script execution has not been located, the script should return an empty line with a period ".\n".
- Data should be sent to the user script looking the way the user entered it. Data input should be screened to avoid the injection of code.

- User scripts have a specific name.
- Error messages during user script execution should be returned to the console as messages with the "+++ ERROR " start line containing a blank. For example, "+++ ERROR cannot connect to DB\n".
- All IDs are line values, which is why they can appear as both words and numerals.
- All user scripts can run using either parallel data requests or sequential data requests. For example, searchemail can be run several times (task Auth, setting processPool -> processNumber), in which case data will be retrieved from the external directory service in parallel. This works only when the setting processPool -> processNumber of the task Auth is greater than "1".

When sequential data requests are used, the searchmail user script is started once. As soon as the user script has transmitted data, it awaits the next request. This means that the user script keeps working until the application itself stops it.

SEARCHEMAIL USER SCRIPT

The following table contains the characteristics of the searchemail user script.

Table 6. Characteristics of the searchemail user script

DATA INPUT FORMAT	DATA OUTPUT FORMAT	USAGE EXAMPLES		
		DESCRIPTION	DATA INPUT	DATA OUTPUT
email\n .n	userID1\n group1 ID\n group2 ID\n ... groupN ID\n .n	The user account belongs to only one user group.	user@example.com .	userID1 managerGroup .
		The user account does not exist.	hacker@example.com .	.
		An error has occurred.	onemoreuser@example.com	ERROR connection lost .

SEARCHUSERS USER SCRIPT

The following table contains the characteristics of the searchusers user script.

Table 7. Characteristics of the searchusers user script

DATA INPUT FORMAT	DATA OUTPUT FORMAT	USAGE EXAMPLES		
		DESCRIPTION	DATA INPUT	DATA OUTPUT
any search line\n .n	UserID1\n nameOfField1 valueOfField1\n nameOfField2 valueOfField2\n ... nameOfFieldN valueOfFieldN\n \n userID2\n nameOfField1 valueOfField1\n nameOfField2 valueOfField2\n ... nameOfFieldN valueOfFieldN\n \n userIDN\nn	The administrator needs to find users whose last name is Brown. As a result of user script execution, the administrator gets two accounts: John and Santa.	Brown .	userID1 name John Brown email john@example.com phone 1871 login john userID2 name Santa Brown email presents@example.com phone 1500 login santa .
		There are no accounts matching the requested line.	hacker .	.

GETUSERACCOUNT USER SCRIPT

The following table contains the characteristics of the getuseraccount user script.

Table 8. Characteristics of the getuseraccount script

DATA INPUT FORMAT	DATA OUTPUT FORMAT	USAGE EXAMPLES		
		DESCRIPTION	DATA INPUT	DATA OUTPUT
userID\n .n	nameOfField1 valueOfField1\n nameOfField2 valueOfField2\n ... nameOfFieldN valueOfFieldN\n .n	The administrator needs to retrieve the details of the userID1 account.	userID1 .	name John Brown email john@example.com phone 1871 .

LOGIN USER SCRIPT

The following table contains the characteristics of the login user script.

Table 9. Characteristics of the login user script

DATA INPUT FORMAT	DATA OUTPUT FORMAT	USAGE EXAMPLES		
		DESCRIPTION	DATA INPUT	DATA OUTPUT
userLogin\n userPassword\n .\n	nameOfField1 valueOfField1\n nameOfField2 valueOfField2\n ... nameOfFieldN valueOfFieldN\n .\n	Successful operating system login.	John 123456 .	userID1 .
		Operating system login error.	hacker password .	ERROR wrong login or password .

CONFIGURING THE APPLICATION CONNECTION TO AN EXTERNAL DIRECTORY SERVICE USING THE LDAP PROTOCOL

➔ To configure the connection of the application with an external directory service using the LDAP protocol:

1. Export the Auth task settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control --get-settings 1 -f <name of the settings file>
```

2. Open the XML file for editing.
3. Specify the preferred type of integration between the application and the external directory service via LDAP in the <integrationType>: <LDAPGeneric> section (for integration with LDAP) or <AD> (for integration with Active Directory).
4. Depending on the type of integration, specify the values of the following settings in the <LDAPGeneric> or <AD> sections:
 - <host> – address of the server with the openLDAP or Active Directory service, depending on the type of integration selected in the <integrationType> section;
 - <connectionType> – the type of connection to Active Directory or server with the openLDAP service: TLS, LDAP via SSL or without encryption;
 - <port> – port of the server with the openLDAP or Active Directory service, depending on the type of connection selected in the <connectionType> section;
 - <bindDn> – administrator account;
 - <password> – administrator password;
 - <searchBase> – account search database.

Example of the <AD> integration type parameters in use:

```
<host><IP address></host>
<port>389</port>
<bindDn>user@companyname.com</bindDn>
<password>123456</password>
<searchBase>dc=companyname,dc=com</searchBase>
```

Example of the <LDAPGeneric> integration type parameters in use:

```
<host>IP address</host>
<port>389</port>
<bindDn>cn=admin,dc=site</bindDn>
<password>123456</password>
<searchBase>dc=site</searchBase>
```

5. Specify the timeout for establishing a connection to the openLDAP or Active Directory service in the <netTimeoutInSeconds> section. If the server does not respond during the specified time, the "Can not contact LDAP server" result is returned.
6. Save the changes made.
7. Import the Auth task settings from an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control --set-settings 1 -f <name of the settings file>
```

We recommend using an unprivileged user account when configuring the application connection to an external directory service using LDAP.

CHECKING THE APPLICATION CONNECTION TO AN EXTERNAL DIRECTORY SERVICE USING THE LDAP PROTOCOL

- To check the application connection to an external directory service using LDAP:

```
# /opt/kaspersky/klms/bin/klms-control --test-ldap-settings-connection
```

The response "Auth task connected successfully" indicates a positive result.

ADDING SENDERS / RECIPIENTS FROM AN EXTERNAL USER SERVICE TO RULES

- To add a sender / recipient from an external directory service to a message processing rule:

1. Export the rule settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
```

```
--get-rule-settings <rule ID> -f <name of the rule settings file>
```

2. Open the XML file for editing.
3. Create new <item> section in the <sender> subsection (to add a sender) or <recipient> subsection (to add a recipient) of the <belongingCriteria> section.

If you need to add several sender and recipient email addresses, each new email address must be in a separate <item> section, typed in a new string of the settings file.

Both the message sender and recipient must be specified in the rule.

4. In the <type> subsection, set the ExternalAccount value.
5. In the <value> subsection, set the CN value from LDAP settings.

Example:

```
<belongingCriteria>
  <sender>
    <item>
      <type>EMailMask</type>
      <value>*</value>
    </item>
  </sender>
  <recipient>
    <item>
      <type>ExternalAccount</type>
      <value>CN=test10,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=sbs2k8,DC=local</value>
    </item>
  </recipient>
</belongingCriteria>
```

6. Save the changes made.
7. Import the rule settings from an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
```

```
--set-rule-settings <rule ID> -f <name of the rule settings file>
```

ADDING PERSONAL BLACK AND WHITE LISTS OF ADDRESSES

When application integration with an external directory service via LDAP is enabled, users are able to maintain their personal black and white lists of senders' addresses.

► *To add a personal black or white list of addresses:*

1. Get a sample rule settings file and save it to an XML file, for example `personal_user1.xml`, with the following command:

```
# /opt/kaspersky/klms/bin/klms-control --personal --sample > personal_user1.xml
```

Sample rule settings file.

Example:

```
<root>
  <blackList>
    <item></item>
  </blackList>
  <whiteList>
    <item></item>
  </whiteList>
</root>
```

2. Use the `<item>` subsection of the `<blackList>` section to add senders' addresses to the black list of addresses, and the `<item>` subsection of the `<whiteList>` section to add senders' addresses to the white list of addresses.

If you need to add several senders' addresses, each new email address must be specified in a separate `<item>` section in a new line of the settings file.

Example:

```

<root>

  <blackList>

    <item>

      user1@mycompany.com

    </item>

    <item>

      user2@mycompany.com

    </item>

  </blackList>

  <whiteList>

    <item>

      administrator@mycompany.com

    </item>

  </whiteList>

</root>

```

3. Save this personal black or white list of addresses for the relevant external directory service user account (for example, for the account `cn=user1001,ou=users,dc=site` user account) using the command:

```

# /opt/kaspersky/klms/bin/klms-control --personal \

--set-settings 'cn=user1001,ou=users,dc=site' -f personal_user1.xml

```

You can specify the e-mail address of a user instead of the user's account.

```

# /opt/kaspersky/klms/bin/klms-control --personal \

--set-settings <email> -f personal_user1.xml

```

MANAGING UNTRUSTED CERTIFICATES

If you have established an encrypted connection of the application to an external directory service via the LDAP protocol (using the `<connectionType/>` parameter in the `settings.xml` file (see section "Configuring the application connection to an external directory service using the LDAP protocol" on page [128](#))), Kaspersky Security requests a certificate from the server with the openLDAP or Active Directory service. You can configure the way Kaspersky Security should respond to a situation in which Active Directory or a server with the openLDAP service does not send a certificate to Kaspersky Security or sends an untrusted certificate.

The response of Kaspersky Security to a missing certificate or an untrusted certificate is configured using the `TLS_REQCERT <level>` setting. This setting is located in the configuration file: `/etc/opt/kaspersky/klms/ldap.conf`. The format of the `ldap.conf` file depends on the LDAP library used.

The TLS_REQCERT parameter can take the following values:

- **Never.** Kaspersky Security does not request a certificate from Active Directory or the server with the openLDAP service.
- **Allow.** Kaspersky Security requests a certificate from Active Directory or the server with the openLDAP service. If the certificate has not been sent or an untrusted certificate has been sent, the TLS session continues. This is the default value.
- **Try.** Kaspersky Security requests a certificate from Active Directory or the server with the openLDAP service. If the certificate is not sent, the TLS session continues. If an untrusted certificate is sent, the TLS session is interrupted.
- **Demand / hard.** The demand and hard values are equivalent. Kaspersky Security requests a certificate from Active Directory or the server with the openLDAP service. If the certificate is missing or an untrusted certificate has been sent, the TLS session is interrupted.

After changing the value of the TLS_REQCERT parameter and saving the ldap.conf file, restart Kaspersky Security to apply changes.

USING THE APPLICATION VIA THE SNMP PROTOCOL

This section contains information about how to use Kaspersky Security via the SNMP protocol and configure runtime trap events.

IN THIS SECTION:

About receiving runtime information via the SNMP protocol	134
Configuring interaction with the application via the SNMP protocol.....	134

ABOUT RECEIVING RUNTIME INFORMATION VIA THE SNMP PROTOCOL

You can use the SNMP protocol to gain access to the following categories of information about Kaspersky Security:

- general information
- runtime statistics since installation
- information about runtime events

Read-only access is granted.

The application uses an SNMP agent to interact via the SNMP protocol. The SNMP agent supports the AgentX protocol (version 1). Any SNMP agent that supports AgentX can be used as an SNMP manager. Kaspersky Security works with SNMP managers that support SNMP v2, v2c, v3.

If you plan to take meter readings with utilities from the Net-SNMP package, you need to upgrade the Net-SNMP package to the latest version.

CONFIGURING INTERACTION WITH THE APPLICATION VIA THE SNMP PROTOCOL

You can perform the following actions:

- Get the ID of the SNMP process.
- Enable information exchange via SNMP.
- Call MIB objects.
- Enable / disable event traps.
- View the MIB structure using the snmpwalk command.

IN THIS SECTION:

Getting the ID of the SNMP process	135
Enabling information exchange via the SNMP protocol.....	135
Calling MIB objects.....	136
Enabling / disabling event traps.....	136
Viewing the MIB structure using the snmpwalk command	136

GETTING THE ID OF THE SNMP PROCESS

To configure interaction with the application via SNMP, you have to get the ID of the SNMP process.

➤ *To get the ID of the SNMP process:*

```
# /opt/kaspersky/klms/bin/klms-control --get-task-list
```

ENABLING INFORMATION EXCHANGE VIA THE SNMP PROTOCOL

➤ *To enable information exchange with the application via the SNMP protocol:*

1. Configure the address of the SNMP master agent by specifying the following value in the snmpd.conf file:

```
master agentx
```

```
AgentXSocket tcp:0.0.0.0:705
```

2. Export the SNMP task settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
```

```
--get-settings <SNMP task ID> -f <file name>
```

3. Open the XML file to edit the task settings.
4. Specify the address of the SNMP master agent in the following section:

```
<masterAgentAddress>tcp:127.0.0.1:705</masterAgentAddress>
```

5. Enable the use of the SNMP protocol by specifying the value 1 in the <enableSNMP> <enableSNMP /> section.
6. Save the changes made.

7. Import the settings from the XML file to the SNMP task using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
```

```
--set-settings <SNMP task ID> -f <file name>
```

After importing the settings, restart Kaspersky Security to apply the changes.

You can now call MIB objects in Kaspersky Security and receive information via the SNMP protocol using OID objects. Kaspersky Security is distributed with MIB files containing the symbol names of MIB objects, events, and their settings. When Kaspersky Security is installed, the MIB files are located in the directory: /opt/kaspersky/klms/share/snmp-mibs.

CALLING MIB OBJECTS

- *To be able to access the MIB objects of Kaspersky Security, allow the SNMP master agent to access the MIB files of Kaspersky Security. To do so, execute the following commands:*

```
# echo "mibdirs +/opt/kaspersky/klms/share/snmp-mibs" >> snmp.conf
```

```
# echo "mibs all" >> snmp.conf
```

ENABLING / DISABLING EVENT TRAPS

The SNMP protocol provides access to runtime statistics and event traps that occur in the operation of Kaspersky Security. You can enable / disable Kaspersky Security traps.

- *To enable / disable Kaspersky Security event traps:*

1. Export the SNMP task settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \  
  
--get-settings <SNMP task ID> -f <file name>
```

2. Open the XML file to edit the task settings.
3. Assign the value 1 to the trapsEnable setting.
4. Save the changes made.
5. Import the settings from the XML file to the SNMP task using the command:

```
# /opt/kaspersky/klms/bin/klms-control \  
  
--set-settings <SNMP task ID> -f <file name>
```

VIEWING THE MIB STRUCTURE USING THE SNMPWALK COMMAND

- *To view the MIB structure in Kaspersky Security using the snmpwalk command,*

add the following string to the snmpd.conf configuration file:

```
view systemview included .1.3.6.1.4.1.23668.1463
```


MANAGING COMPANY EMPLOYEE ACCOUNTS

This section describes how you can manage accounts of company employees and configure their settings.

IN THIS SECTION:

About a company employee account	137
Activating and deactivating a company employee account	137
Configuring settings of a company employee account	138
Configuring the transmission of infected messages placed in Backup to users	138

CONFIGURING SETTINGS OF A COMPANY EMPLOYEE ACCOUNT

Company employee accounts are intended for company employees tasked with analyzing and managing personal black and white lists of addresses and copies of messages placed in Backup (for example, for Helpdesk employees). This account gives an employee access only to settings and contents of Backup and personal black and white lists of addresses.

ACTIVATING AND DEACTIVATING A COMPANY EMPLOYEE ACCOUNT

➔ *To activate or deactivate a company employee account:*

1. Export the application's general settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control --get-app-settings -f <name of the settings file>
```
2. Open the XML file to edit the settings.
3. In the <helpdesk> section, specify one of the following values for the <enable> parameter:
 - 1, to activate accounts for company employees;
 - 0, to deactivate accounts for company employees.
4. Save the changes made.
5. Import the application's general settings from an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control --set-app-settings -f <name of the settings file>
```

CONFIGURING SETTINGS OF A COMPANY EMPLOYEE ACCOUNT

➤ *To configure the settings of a company employee account:*

1. Export the application's general settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control --get-app-settings -f <name of the settings file>
```

2. Open the XML file to edit the settings.
3. To allow or block employees working under the account being configured to access personal white and black lists of addresses, specify one of the following values for the <accessBlackWhiteList> parameter in the <helpdesk> section:

- 1, to allow access to personal black or white lists;
- 0, to block access to personal black or white lists.

4. Save the changes made.

5. Import the application's general settings from an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control --set-app-settings -f <name of the settings file>
```

6. To specify the name for a company employee account, run the following command:

```
# /opt/kaspersky/klms/bin/klms-control --set-web-helpdesk-login <login-name>, where <login-name> is the account name.
```

7. To specify the password for a company employee account, run the following command:

```
# /opt/kaspersky/klms/bin/klms-control --set-web-helpdesk-password <password>, where <password> is the password.
```

The names and passwords of all accounts for using the application are located at the following path:
/var/opt/kaspersky/klms/db/passwd.

CONFIGURING THE TRANSMISSION OF INFECTED MESSAGES PLACED IN BACKUP TO USERS

➤ *To configure the transmission of infected messages placed in Backup to users:*

1. Export the Backup settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control --get-settings Backup -n -f <name of the settings file>
```

2. Open the XML file to edit the settings.

3. In the <root> section, specify one of the following values for the <allowAvThreatsRestoration> parameter:

- 1, to allow users working under the company employee account to send infected messages placed in Backup to users;

- 0, to block users working under the company employee account from sending infected messages placed in Backup to users.
4. Save the changes made.
 5. Import the Backup settings from an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control --set-settings Backup -n -f <name of the settings file>
```

BACKUP

This section contains information about Backup and how to use it.

IN THIS SECTION:

About Backup.....	140
Viewing statistics of message copies in Backup.....	141
Filtering the details of message copies in Backup.....	141
Deleting message copies from Backup.....	142
Saving messages from Backup to file	142
Delivering messages from Backup to recipients.....	142
Configuring Backup size.....	143

ABOUT BACKUP

Kaspersky Security places copies of messages in *Backup*. Copies of messages are stored in Backup in unreadable format and therefore do not compromise your computer's security.

Kaspersky Security places copies of the following messages in Backup:

- After scanning by the Anti-Virus engine: copies of messages, before an attempt is made to cure or delete the messages, or delete an attachment using the actions Cure, DeleteMessage or DeleteAttachment.
- After scanning by the Anti-Spam engine: copies of messages assigned *Spam / Probable spam / Blacklisted* status, before attempting to delete them using the DeleteMessage action, provided that the application is configured to move messages to Backup when processing them according to a rule (see section "Configuring Anti-Spam scan settings for a rule" on page [90](#)).
- After scanning by the Anti-Phishing engine: copies of messages assigned *Phishing / Malicious link* status, before attempting to delete them using the DeleteMessage action, provided that the application is configured to move messages to Backup when processing them according to a rule (see section "Configuring Anti-Phishing scan message processing settings" on page [105](#)).
- After content filtering: copies of messages that violate the content filtering criteria, provided that the processing rule is configured to place copies of such messages in Backup when content filter criteria are violated by size (see section "Configuring content filtering by message size" on page [109](#)) / attachment name (see section "Configuring content filtering by attachment name" on page [109](#)) / attachment format (see section "Configuring content filtering by attachment format" on page [110](#)).

Copies of messages are placed in Backup together with attachments.

The default maximum Backup space is 1 GB. As soon as this threshold value is exceeded, the application starts to delete the oldest messages from Backup. When the amount of occupied space is again below the threshold value, the application stops deleting messages from Backup. You can change the maximum size of Backup (see section "Configuring the size of Backup" on page [143](#)).

You can perform the following actions on copies of messages in Backup:

- view the statistics of message copies in Backup (see section "Viewing statistics of message copies in Backup" on page [141](#));
- filter the details of message copies in Backup (see section "Filtering the details of message copies in Backup" on page [141](#));
- delete message copies from Backup (see section "Deleting message copies from Backup" on page [142](#));
- deliver messages from Backup to recipients (see section "Delivering messages from Backup to recipients" on page [142](#)). Any email address, including one that is not present in the "To" field of the message, can be specified as the recipient's email address.
- Save messages from Backup to file (see section "Saving messages from Backup to file" on page [142](#)).

The local area network administrator can be held liable for unauthorized access to information transmitted in messages stored in Backup.

VIEWING STATISTICS OF MESSAGE COPIES IN BACKUP

You can view statistics of message copies in Backup: the total number of message copies currently in Backup, and the total disk space that they occupy.

➤ *To view statistics of message copies in Backup:*

```
# /opt/kaspersky/<PRODUCT_BIN>/bin/<PRODUCT_BIN>-control --backup --statistics
```

FILTERING THE DETAILS OF MESSAGE COPIES IN BACKUP

You can filter the details of message copies in Backup to get information on the message copies you need.

➤ *To filter the details of message copies in Backup:*

```
# /opt/kaspersky/klms/bin/klms-control --backup --query \  
--message-id <message ID> --from <sender's email address> \  
--to <recipient's email address> --subject <subject> \  
--limit <maximum number of messages>
```

The application shows information about message copies in Backup, such as:

- IP address of the message sender
- Email address of the message sender
- Time when the message was sent
- Time when the message was received
- Message subject
- Attachments
- Message scan and content filtering statuses

DELETING MESSAGE COPIES FROM BACKUP

You can delete message copies from Backup in several ways:

- Delete one message copy.
- Delete copies of all messages processed according to one rule.
- Delete all copies of messages matching the specified filtration criteria (see section "Filtering the details of message copies in Backup" on page [141](#)).

➤ *To delete one message copy from Backup, execute the following command:*

```
# /opt/kaspersky/klms/bin/klms-control --backup --remove \  
--message-id <message ID>
```

➤ *To delete copies of all messages processed according to one rule, execute the following command:*

```
# /opt/kaspersky/klms/bin/klms-control --backup --remove --\  
rule-id <rule ID>
```

➤ *To delete all copies of messages matching the specified filtration criteria, execute the following command:*

```
# /opt/kaspersky/klms/bin/klms-control --backup --query \  
--message-id <message ID> --from <sender's email address> \  
--to <recipient's email address> --subject <subject> \  
--limit <maximum number of messages> --mass-remove
```

SAVING MESSAGES FROM BACKUP TO FILE

You can save a message from Backup to file on the computer. You may need to save a message to file if, for example, you want to open the message in your email client later.

Saving infected and probably infected messages poses a security threat to your computer.

➤ *To save a message from Backup to a file, execute the following command:*

```
# /opt/kaspersky/klms/bin/klms-control --backup \  
--save --message-id <message ID> --rule-id <rule ID> -file <file name>
```

DELIVERING MESSAGES FROM BACKUP TO RECIPIENTS

If you consider a message in Backup to be safe, you can deliver the message from Backup to the recipients.

Delivering infected and probably infected messages from Backup could pose a security threat to computers.

➤ *To deliver a message from Backup to its recipients, execute the following command:*

```
# /opt/kaspersky/klms/bin/klms-control --backup \  
--deliver --message-id <message ID> --rule-id <rule ID>
```

```
--deliver --message-id <message ID> --rule-id <rule ID> --recipients <recipient's email address> <recipient's email address>
```

CONFIGURING BACKUP SIZE

➤ *To configure the size of Backup:*

1. Export the Backup task settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \  
  
--get-settings Backup -n -f <name of the settings file>
```

2. Open the XML file to edit the rule settings.
3. In the <maxSize> section, specify the maximum size in bytes that Backup can take up on the hard drive.

When the specified value is exceeded, the application attempts to remove old copies of messages from Backup.

4. Import the rule settings from an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \  
  
--set-settings Backup -n -f <name of the settings file>
```

EMAIL NOTIFICATIONS

This section contains information about mail notifications and how to configure them.

IN THIS SECTION:

About email notifications	144
Enabling delivery of email notifications about objects	145
Specifying additional email addresses for delivery of email notifications about objects	146
Configuring delivery of email event notifications to the administrator	147
Editing templates of email event notifications.....	148
Using macros in templates of email event notifications	149

ABOUT EMAIL NOTIFICATIONS

An *email notification* (or notification) is an email message containing a description of a processed message. The application sends the notification to the recipients or sender of the processed message, or to the mail server administrator. Besides a description of the email message, the notification contains a description of objects deleted from the message. The application also includes the text of the source message in notifications for recipients.

You can configure the delivery of email notifications (see section "Enabling delivery of email notifications about objects" on page [145](#)) about infected or corrupted objects, object scanning errors, or violations of content filtering criteria, to the administrator or the message sender or recipient, and to email addresses you specify (see section "Specifying additional email addresses for delivery of email notifications about objects" on page [146](#)).

Various events occur during the operation of Kaspersky Security. They reflect changes in the status of Kaspersky Security. You can configure the delivery of event notifications to the administrator by email (see section "Configuring delivery of email event notifications to the administrator" on page [147](#)).

The application provides two types of email notifications:

- notifications about objects.
- administrator notifications about events.

Administrator notifications are available for the following events:

- *License expired*, which occurs when the license validity period has expired.
- *License expires soon*, which occurs when the license validity period is about to expire.
- *Key is blocked*, which occurs if the key is in the black list.
- *Databases are out of date*, which occurs if the Anti-Virus or Anti-Spam databases are out of date.
- *Databases are extremely out of date*, which occurs if the Anti-Virus or Anti-Spam databases are obsolete.
- *Error purging Backup*, which occurs when automatic deletion of messages in Backup returns an error.
- *Backup is almost full*, which occurs when Backup is running out of space.

- *Error placing messages in Backup*, which occurs when an attempt to place a message in Backup returns an error.

Kaspersky Security contains templates of notifications for the mail server administrator, or for the sender or recipient of a message. You can edit these notification templates (see section "Editing templates of email event notifications" on page [148](#)).

ENABLING DELIVERY OF EMAIL NOTIFICATIONS ABOUT OBJECTS

➔ *To enable delivery of notifications:*

1. Export rule settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--get-rule-settings <rule ID> -f <rule settings file name> or
--get-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

2. Open the XML file to edit the rule settings.
3. In one of the following subsections of the <notificationSettings> section:
 - <admin> for delivery of notifications to the administrator,
 - <sender> for delivery of notifications to the sender,
 - <recipient> for delivery of notifications to the recipient,
 - <additional> for delivery of notifications to the additional email addresses you specified (see section "Specifying additional email addresses for delivery of email notifications about objects" on page [146](#)).

specify the value 1 for the following settings:

- <enableInfected> for notifications about infected objects.
 - <enableEncrypted> for notifications about encrypted objects.
 - <enableCorrupted> for notifications about corrupted objects or errors during scanning of an object.
 - <enableCFFail> for notifications about violations of the content filter settings;
 - <enablePhishing> to send notifications about phishing threats detected.
4. Save the changes made.
 5. To import rule settings from an XML file, use the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--set-rule-settings <rule ID> -f <rule settings file name> or
--set-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

SPECIFYING ADDITIONAL EMAIL ADDRESSES FOR DELIVERY OF EMAIL NOTIFICATIONS ABOUT OBJECTS

➤ To specify additional email addresses for delivery of email notifications about objects:

1. Export rule settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--get-rule-settings <rule ID> -f <rule settings file name> or
--get-rule-settings <rule name> -n -f <rule settings file name>
```

The <rule name> should be enclosed in double quotes if it contains blanks.

2. Open the XML file to edit the rule settings.
3. In the <additional> subsection of the <notificationSettings> section, specify the list of email addresses for delivery of notifications with the following settings:
 - <emailListInfected> for notifications about infected objects.
 - <emailListEncrypted> for notifications about encrypted objects.
 - <emailListCorrupted> for notifications about corrupted objects or errors during scanning of an object.
 - <emailListCFFail> for notifications about violations of the content filter settings;
 - <emailListPhishing> for notifications about detected phishing URLs.

If you need to add several email addresses for sending notifications, each new address must be in a separate <item> section in a new line of the settings file.

Example:

```
<additional>
  <options>
    <enableInfected>0</enableInfected>
    <enableCorrupted>1</enableCorrupted>
    <enableEncrypted>0</enableEncrypted>
    <enableCFFail>0</enableCFFail>
    <enablePhishing>0</enablePhishing>
  </options>
  <emailListInfected />
  <emailListCorrupted>
```

```

    <item>
      administrator@mycompany.com
    </item>
  </emailListCorrupted>
  <emailListEncrypted />
  <emailListCFFail />
  <emailListPhishing />
</additional>

```

4. Save the changes made.
5. To import rule settings from an XML file, use the command:

```

# /opt/kaspersky/klms/bin/klms-control \
--set-rule-settings <rule ID> -f <rule settings file name> or
--set-rule-settings <rule name> -n -f <rule settings file name>

```

The <rule name> should be enclosed in double quotes if it contains blanks.

CONFIGURING DELIVERY OF EMAIL EVENT NOTIFICATIONS TO THE ADMINISTRATOR

You can configure the delivery of email notifications about application events (see section "About email notifications" on page [144](#)) to the administrator. To do so, you need to specify the administrator's address for delivery of notifications and enable delivery of notifications. You can also specify the address from which the application is to send administrator notifications.

➤ *To configure the delivery of email event notifications to the administrator:*

1. Export the application's general settings to an XML file using the command:


```
# /opt/kaspersky/klms/bin/klms-control --get-app-settings -f <file name>
```
2. Open the XML file to edit the settings.
3. In the <adminEmailAddresses> section, specify the email addresses of the administrator to which notifications are to be sent.
4. In the <replyEmailAddress> section, you can specify the address from which notifications are to be sent.

The default email address is klms@localhost.

5. Save the changes made.
6. Import the application's general settings from an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control --set-app-settings -f <file name>
```

- Export the settings of the Notifier module to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control --get-settings 9 -f <file name>
```

- Open the XML file to edit the settings.

- In the <notificationFlags> section, specify the value 1 for the following settings:

- <antiVirusBasesOutdated> and <antiVirusBasesObsoleted> for sending notifications about the *antiVirusBasesOutdated* event;
- <antiSpamBasesOutdated> and <antiSpamBasesObsoleted> for sending notifications about the *antiSpamBasesOutdated* event;
- <messageBackupFailed> for notifications about *messageBackupFailed* events.
- <backupCleanupFailed> for notifications about *backupCleanupFailed* events.
- <backupAlmostFull> for notifications about *backupAlmostFull* events.
- <licenseExpiresSoon> for notifications about *licenseExpiresSoon* events.
- <licenseExpired> for notifications about *licenseExpired* events.
- <licenseBlacklisted> for notifications about *licenseBlacklisted* events;
- <externalDirectoryServicesError> for sending notifications about the *externalDirectoryServicesError* event.

- Save the changes made.

- Import the settings from an XML file to the Notifier module using the command:

```
# /opt/kaspersky/klms/bin/klms-control --set-settings 9 -f <file name>
```

EDITING TEMPLATES OF EMAIL EVENT NOTIFICATIONS

➔ To edit an email event notification template:

- Export the settings of the Notifier module to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control --get-settings 9 -f <file name>
```

- Open the XML file to edit the settings.

- In the <notificationTemplates> section, edit the text of the relevant event notification template. You can edit the template text using macros (see section "Using macros in templates of email event notifications" on page [149](#)).

If, while editing a template text, you use line breaks or characters that may cause errors during analysis by the XML parser, you must use the following format: `CDATA: <tag><![CDATA[...]]></tag>`.

The text fragment inside `<![CDATA[...]>`, is not analyzed by the XML parser, and is perceived as an ordinary string that contains only character data and no markup.

- Save the changes made.

- Import the settings from an XML file to the Notifier module using the command:

```
# /opt/kaspersky/klms/bin/klms-control --set-settings 9 -f <file name>
```

USING MACROS IN TEMPLATES OF EMAIL EVENT NOTIFICATIONS

Macro is a substitution element used in event notification templates. In the text of a notification generated on the basis of a template, a macro is substituted for a certain value.

Macro syntax: %MACRO_NAME%

The following macros can be used in notification texts (see table below).

Table 10. Macros for event notification templates

MACRO	DESCRIPTION	EVENT FOR WHICH THE MACRO IS USED
%SERVER_NAME%	Mail server name.	<i>antiVirusBasesOutOfDate, antiVirusBasesObsolete, antiSpamBasesOutOfDate, antiSpamBasesObsolete, messageBackupFailed, severalMessagesBackupFailed, severalBackupCleanupAttemptsFailed, backupAlmostFull, licenseExpiresSoon, licenseExpired, licenseBlacklisted</i>
%PRODUCT_NAME%	Application name.	<i>antiVirusBasesOutOfDate, antiVirusBasesObsolete, antiSpamBasesOutOfDate, antiSpamBasesObsolete, messageBackupFailed, severalMessagesBackupFailed, severalBackupCleanupAttemptsFailed, backupAlmostFull, licenseExpiresSoon, licenseExpired, licenseBlacklisted</i>
%BASES_ISSUE_DATE%	Anti-Virus or Anti-Spam database release date.	<i>antiVirusBasesOutOfDate, antiVirusBasesObsolete, antiSpamBasesOutOfDate, antiSpamBasesObsolete</i>
%OUTDATED_DAYS%	Number of days since the last update of Anti-Spam or Anti-Spam databases.	<i>antiVirusBasesOutOfDate, antiVirusBasesObsolete, antiSpamBasesObsolete</i>
%OUTDATED_HOURS%	Number of hours since last update of Anti-Spam databases.	<i>antiSpamBasesOutOfDate</i>
%SMTP_MESSAGE_ID%	Message header.	<i>messageBackupFailed, scanStatusAlertForAdmin, scanStatusAlertForOthers</i>
%MESSAGES_COUNT%	Number of messages that could not be placed in Backup or total number of messages in Backup.	<i>severalMessagesBackupFailed, backupAlmostFull</i>
%MINUTES%	Time during which attempts were made to place messages in Backup or automatically delete messages from it.	<i>severalMessagesBackupFailed, severalBackupCleanupAttemptsFailed</i>
%ATTEMPTS%	Number of attempts to automatically delete messages from Backup.	<i>severalBackupCleanupAttemptsFailed</i>
%MESSAGES_SIZE%	Total size of messages in Backup in megabytes.	<i>backupAlmostFull</i>
%MAX_BACKUP_SIZE%	Maximum size of Backup.	<i>backupAlmostFull</i>
%LICENSE_NUMBER%	License key.	<i>licenseExpiresSoon, licenseExpired, licenseBlacklisted</i>
%EXPIRATION_DAYS%	Number of days before expiration of the license.	<i>licenseExpiresSoon</i>
%EXPIRATION_DATE%	License expiration date.	<i>licenseExpired</i>
%SENDER%	Email address of message sender.	<i>scanStatusAlertForAdmin, scanStatusAlertForRecipient, scanStatusAlertForOthers</i>
%ALL_RECIPIENTS%	Addresses of all recipients of source message.	<i>scanStatusAlertForAdmin, scanStatusAlertForSender, scanStatusAlertForOthers</i>
%AFFECTED_RECIPIENTS%	Addresses of the original message recipients who should be advised of the event described in the notification.	<i>scanStatusAlertForAdmin, scanStatusAlertForOthers, messageBounce</i>

MACRO	DESCRIPTION	EVENT FOR WHICH THE MACRO IS USED
%AFFECTED_RULES%	Original message processing rules that are conditioned by the event described in the notification.	<i>scanStatusAlertForAdmin,</i> <i>scanStatusAlertForOthers</i>
%MESSAGE_ID%	ID of message in the application.	<i>scanStatusAlertForAdmin,</i> <i>scanStatusAlertForOthers</i>
%SUBJECT%	Subject (Subject field) of source message.	<i>scanStatusAlertForAdmin,</i> <i>scanStatusAlertForSender,</i> <i>scanStatusAlertForRecipient,</i> <i>scanStatusAlertForOthers</i>
%DATE%	Message processing date.	<i>scanStatusAlertForAdmin,</i> <i>scanStatusAlertForSender,</i> <i>scanStatusAlertForRecipient,</i> <i>scanStatusAlertForOthers</i>
%MESSAGE_ACTION%	Action taken by the application on the email message.	<i>scanStatusAlertForAdmin,</i> <i>scanStatusAlertForSender,</i> <i>scanStatusAlertForRecipient,</i> <i>scanStatusAlertForOthers</i>
%DATA_BEGIN%	Service macro to designate the beginning of the list of macros to be attached.	<i>scanStatusAlertForAdmin,</i> <i>scanStatusAlertForSender,</i> <i>scanStatusAlertForRecipient,</i> <i>scanStatusAlertForOthers</i>
%DATA_END%	Service macro to designate the end of the list of macros to be attached.	<i>scanStatusAlertForAdmin,</i> <i>scanStatusAlertForSender,</i> <i>scanStatusAlertForRecipient,</i> <i>scanStatusAlertForOthers</i>
%OBJECT_NAME%	Name of attachment.	<i>scanStatusAlertForAdmin,</i> <i>scanStatusAlertForSender,</i> <i>scanStatusAlertForRecipient,</i> <i>scanStatusAlertForOthers</i>
%OBJECT_SIZE%	Size of attachment.	<i>scanStatusAlertForAdmin,</i> <i>scanStatusAlertForSender,</i> <i>scanStatusAlertForRecipient,</i> <i>scanStatusAlertForOthers</i>
%STATUS%	Message status.	<i>scanStatusAlertForAdmin,</i> <i>scanStatusAlertForSender,</i> <i>scanStatusAlertForRecipient,</i> <i>scanStatusAlertForOthers</i>
%OBJECT_ACTION%	Action taken by the application on the attachment.	<i>scanStatusAlertForAdmin,</i> <i>scanStatusAlertForSender,</i> <i>scanStatusAlertForRecipient,</i> <i>scanStatusAlertForOthers</i>

RUNTIME REPORTS AND STATISTICS

This section contains information about reports and statistics on the operation of the application.

IN THIS SECTION:

Viewing runtime statistics.....	152
Creating reports.....	152

VIEWING RUNTIME STATISTICS

► To view statistics on the operation of the application, execute the following command:

```
# /opt/kaspersky/klms/bin/klms-control --dashboard
```

You can view monthly (option --month), weekly (option --week), daily (option --day), or hourly (option --hour) statistics.

Monthly and weekly statistics are given per day; daily statistics per hour; hourly statistics every 5 minutes.

The application displays information as per the following table:

Table 11. Runtime statistics

NAME	VALUE
threat	Total number of infected, probably infected, corrupted, or encrypted messages, and messages for which Anti-Virus scanning returned an error.
phishing	The total number of messages containing phishing threats or links to websites with malware.
spam	Total number of messages containing spam or potential spam, and messages from undesirable senders.
content	Total number of messages that triggered the application during content filtering by message size, attachment name or format.
notScanned	Total number of messages that have not been processed for some reason (for example, messages have been excluded from scanning by the administrator, the license has expired, the Anti-Virus engine, Anti-Spam engine, Anti-Phishing engine, or content filtering has been disabled).
clean	Total number of messages scanned by the application and identified as not infected, not containing spam or phishing, and not violating the content filter settings.
total	Total number of messages processed by the application.

CREATING REPORTS

Kaspersky Security can generate reports and statistics on the operation of the application.

You can create reports in the following ways:

- on demand (see section "Creating on-demand reports" on page [153](#));

- by schedule (see section "Configuring scheduled reports" on page [155](#)).

You can create on-demand reports for the following periods:

- today
- this month
- this year
- last couple of days
- last seven days
- last month
- last year
- exact time

The application stores on-demand reports in the directory `/var/opt/kaspersky/klms/reports/`.

You can create scheduled reports for the following periods:

- day (DailyReport task, ID=17)
- week (WeeklyReport task, ID=18)
- month (MonthlyReport task, ID=19)

The stores scheduled reports in the following directories:

- daily reports: `/var/opt/kaspersky/klms/reports/daily`
- weekly reports: `/var/opt/kaspersky/klms/reports/weekly`
- monthly reports: `/var/opt/kaspersky/klms/reports/monthly`

IN THIS SECTION:

Creating on-demand reports [153](#)

Configuring scheduled reports..... [155](#)

CREATING ON-DEMAND REPORTS

➡ *To create an on-demand report, execute the following command:*

```
# /opt/kaspersky/klms/bin/klms-control --report
```

You can create a report for the following periods:

- today (option `--today`).
- this month (option `--this-month`).
- this year (option `--this-year`).

- last few days (option `--last-days <ndays>`, where `<ndays>` is the number of days; 1 by default).
- last week (option `--last-week`).
- last month (option `--last-month`).
- last year (option `--last-year`).
- exact time (option `--exact-time YYYY [.MM [.DD]]`, where YYYY is the year, MM is the month, DD is the day) If you use the full date format for an exact-time report, you can specify a report period using the option `--ndays <ndays>`, where `<ndays>` is the number of days from the date specified for which you want to get a report.

The following example illustrates how to create a report for the previous month.

Example:

The current month is May 2012. You need a report for April 2012.

Execute the following command:

```
# /opt/kaspersky/klms/bin/klms-control --report --last-month
```

The application creates a report for April 2012.

The following example illustrates how to create a report for an exact time.

Example:

You need a report for 4 May 2012.

Execute the following command:

```
# /opt/kaspersky/klms/bin/klms-control --report --exact-time 2012.05.04
```

The application creates a report for this one day.

The following example illustrates how to create a report for an exact period.

Example:

You need a report for 6 days starting 4 May 2012.

Execute the following command:

```
# /opt/kaspersky/klms/bin/klms-control --report --exact-time 2012.05.04 --ndays 6
```

The application creates a report for the period from 4 May through 9 May.

Different language options are available for all reports (option `--lang`). The list of languages depends on the application localization packages installed. The default language is English.

The following example illustrates how to create a report in Russian.

Example:

You need a report for today in Russian.

Execute the following command:

```
# /opt/kaspersky/klms/bin/klms-control --report --today --lang ru_RU
```

The application generates a report for today in Russian.

In addition, you can configure the delivery of on-demand reports by email. To do so, use the option `--deliver`.

The following example illustrates how to configure the delivery of a report for the current month.

Example:

You need to create and deliver a report for this month.

Execute the following command:

```
# /opt/kaspersky/klms/bin/klms-control --report --this-month \
--deliver <recipient's email address> <recipient's email address> ...
```

The application creates a report for this month and delivers it to the email addresses of the recipients that you specified.

CONFIGURING SCHEDULED REPORTS

➡ *To configure the generation of scheduled reports:*

1. Export DailyReport (ID=17), WeeklyReport (ID=18), or MonthlyReport (ID=19) task settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--get-settings <task ID> -f <file name>
```

2. Open the XML file to edit the task settings.
3. Specify 1 as the value of the `<enableReport>` setting to enable the generation of scheduled reports.
4. Specify the settings of the report generation schedule:
 - `<dayOfMonth>` – day of month [1;31] (for MonthlyReport task)
 - `<dayOfWeek>` – day of week [MON | TUE | WED | THU | FRI | SAT | SUN] (for WeeklyReport task)
 - `<hour>` – hours [00;23] (for DailyReport, WeeklyReport, or MonthlyReport task)
 - `<min>` – minutes [00;59] (for DailyReport, WeeklyReport, or MonthlyReport task)

5. If you want to enable the delivery of scheduled reports by email:
 - in the `<sendOptions>` section, specify the value 1 for the `<enableSend>` setting.
 - in the `<recipientsAddresses>` section, specify the email addresses to which scheduled reports are to be sent.

6. Specify the language of the scheduled reports using the `<lang>` setting. The list of languages depends on the application localization packages installed.

7. Save the changes made.

8. Import the settings from an XML file to a DailyReport, WeeklyReport, or MonthlyReport task using the command:

```
# /opt/kaspersky/klms/bin/klms-control \
--set-settings <task ID> -f <file name>
```

EVENT LOG

This section contains information about the Event log and how to configure it.

IN THIS SECTION:

About the event log	156
Changing the system log category for storing events.....	158
Configuring event logging in the event log	158

ABOUT THE EVENT LOG

Various events occur during the operation of Kaspersky Security. They reflect changes in the status of Kaspersky Security. Information about these events is stored in the *Event log*.

The application keeps the Event log in the system log of the operating system (syslog) in the Mail category. If necessary, you can change the category of the system log in which the application should log events. The application designates Kaspersky Security events with the abbreviation KLMS to distinguish them from other events stored in the Mail category.

Events can have the following levels of importance:

- Error – events involving application errors.
- Info – informational events. At this level, the log stores email addresses of senders and receivers, the IP address of the computer transmitting the message, as well as detailed information on message scan results.

By default, the application logs only error events (i.e., events with the Error level of importance) in the event log (see table below). You can configure all application events to be recorded in the log.

Table 12. Events in the event log

EVENT	DESCRIPTION	IMPORTANCE LEVEL
<i>RuleSettingsChangedEvent</i>	Message processing rule settings have been changed.	Info
<i>TaskSettingsChangedEvent</i>	Task settings have been changed.	Info
<i>MessageProcessedEvent</i>	Message has been processed.	Info
<i>MessageNotProcessedEvent</i>	Message has not been processed.	Info
<i>MessageQuarantinedEvent</i>	Messages has been placed in Backup.	Info
<i>ProductStartEvent</i>	Application has been started.	Info
<i>ScheduledReportError</i>	Error creating scheduled report.	Error
<i>ScheduledReportGenerated</i>	Scheduled report has been generated.	Info
<i>BackupLimitReachedEvent</i>	Backup limit size has been reached.	Info
<i>BackupRestoreAvThreatEvent</i>	Message from Backup has been saved to file or sent to recipients.	Info
<i>BackupAddErrorEvent</i>	Error adding message to Backup.	Error
<i>BackupRotateErrorEvent</i>	Error automatically freeing up space in Backup.	Error
<i>AvUpdateErrorEvent</i>	Error updating Anti-Virus databases.	Error
<i>AvBasesLoadError</i>	Error loading Anti-Virus databases.	Error
<i>AspUpdateErrorEvent</i>	Error updating Anti-Spam databases.	Error
<i>ApUpdateErrorEvent</i>	Error updating Anti-Phishing databases.	Error
<i>AvBasesAttachedEvent</i>	Anti-Virus databases have been updated.	Info
<i>ApBasesAttachedEvent</i>	Anti-Phishing databases have been updated.	Info
<i>AspBasesAttachedEvent</i>	Anti-Spam databases have been updated.	Info
<i>NothingToUpdateEvent</i>	No update required.	Info
<i>AvBasesOutdatedEvent</i>	Anti-Virus databases are out of date.	Info
<i>AspBasesOutdatedEvent</i>	Anti-Spam databases are out of date.	Info
<i>ApBasesOutdatedEvent</i>	Anti-Phishing databases are out of date.	Info
<i>AvBasesObsoleteEvent</i>	Anti-Virus databases are obsolete.	Info
<i>AspBasesObsoleteEvent</i>	Anti-Spam databases are obsolete.	Info
<i>ApBasesObsoleteEvent</i>	Anti-Phishing databases are obsolete.	Info
<i>AvBasesAppliedEvent</i>	Anti-Virus databases have been downloaded.	Info
<i>AspBasesAppliedEvent</i>	Anti-Spam databases have been downloaded.	Info
<i>ApBasesAppliedEvent</i>	Anti-Phishing databases have been downloaded.	Info
<i>LicenseBlacklistedEvent</i>	Key is in the black list of keys.	Error
<i>LicenseExpiredEvent</i>	License has expired.	Error
<i>LicenseExpiresSoonEvent</i>	License expires soon.	Info
<i>LicenseErrorEvent</i>	Key related error.	Error
<i>LicenseInstalledEvent</i>	Key has been added.	Info
<i>LicenseRevokedEvent</i>	Key has been deleted.	Info
<i>TaskCrashEvent</i>	Process returned an error.	Error
<i>TaskRestartEvent</i>	Process has been restarted.	Info

In PostgreSQL, the **Log** level is higher than the **Error** level. For details, see <http://www.postgresql.org/docs/9.1/static/runtime-config-logging.html#RUNTIME-CONFIG-SEVERITY-LEVELS>

CHANGING THE SYSTEM LOG CATEGORY FOR STORING EVENTS

➤ To change the syslog category for storing events:

1. Export the Event log settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control --get-settings 20 -f <file name>
```

2. Open the XML file to edit the settings.
3. Specify the value of the <facility> setting to indicate the syslog category where the application is to log events.

The default category is Mail.

4. Save the changes made.
5. Import the Event log settings from an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control --set-settings 20 -f <file name>
```

CONFIGURING EVENT LOGGING IN THE EVENT LOG

➤ To configure the logging of events in the event log:

1. Export the Event log settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control --get-settings EventLogger -n \  
-f <file name>
```

2. Open the XML file to edit the settings.
3. Specify the level of importance of events that the application is to record in the Event log. To do so, specify one of the following values for the <logLevel> setting:

- Error – events involving application errors (this is the default value).
- Info – informational events In this case the program writes to event log informational events and error events.

4. Save the changes made.
5. Import the Event log settings from an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control --set-settings \  
<ID of the EventLogger task> -f <file name>
```

Kaspersky Security installed on a computer running the FreeBSD operating system cannot record symbols that have encoding other than ASCII in the event log. For this reason, any text having encoding other than ASCII is displayed incorrectly when recorded in the event log.

➡ *For text having encoding other than ASCII to be displayed correctly in the event log, execute the following commands:*

1. `echo 'syslogd_flags="-s -8" >> /etc/rc.conf.`
2. `/etc/rc.d/syslogd restart.`

TRACE LOG

This section contains information about the Trace log and how to configure it.

IN THIS SECTION:

About the trace log	160
Enabling the trace log.....	161
Configuring the level of detail of the trace log	161
Configuring the location of the trace log	162
Configuring the rotation of trace files.....	162

ABOUT THE TRACE LOG

If a problem occurs during the operation of Kaspersky Security (for example, Kaspersky Security or an individual task has crashed) and you would like to diagnose it, you can create a trace log that saves all application events and send it to the Support Service.

By default, trace log files are stored in the directory `/var/log/kaspersky/klms`. You can specify the location of the trace log on the hard drive (see section "Configuring the location of the trace log" on page [162](#)).

You can specify the level of detail of the trace log (see section "Configuring the level of detail of the trace log" on page [161](#)).

The following levels of detail of the trace log are available for selection:

- Fatal – critical errors.
- Error – events involving application errors.
- Warning – important events. The value of the smtp header that could not be decoded is recorded in the trace log.
- Info – informational events
- Debug – debugging information The trace log records the message subjects and addresses of senders and recipients, attachment names, and other information about processed messages, as well as the full details of message search queries. The log also records data from external sources and all links to web resources contained in the messages. When *mlter* is used, the trace log records all message headers.

The highest level of detail is Debug, at which all events are recorded in the trace log; the lowest level of detail is Fatal, at which only critical events are recorded in the trace log. The default level of detail is set to Error.

At the Debug level, the trace log takes up a large amount of disk space and main contain confidential user information.

ENABLING THE TRACE LOG

➤ *To enable or disable the trace log:*

1. Export the application's general settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control --get-app-settings -f <file name>
```

2. Open the XML file to edit the settings.
3. In the <tracerSettings> section, specify one of the following values for the <Enable> setting:

- 1, to enable the trace log;
- 0, to disable the trace log.

4. Save the changes made.
5. Import the application's general settings from an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control --set-app-settings -f <file name>
```

6. Restart the application. Execute the following command:

```
# /etc/init.d/klms restart
```

CONFIGURING THE LEVEL OF DETAIL OF THE TRACE LOG

➤ *To configure the level of detail of the trace log:*

1. Export the application's general settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control --get-app-settings -f <file name>
```

2. Open the XML file to edit the settings.
3. Specify the level of detail of the trace log. In the <tracerSettings> section, specify one of the following values for the <level> setting:

- Fatal – critical errors.
- Error – events involving application errors.
- Warning – important events.
- Info – informational events
- Debug – debugging information

4. Save the changes made.
5. Import the application's general settings from an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control --set-app-settings -f <file name>
```

6. Restart the application. Execute the following command:

```
# /etc/init.d/klms restart
```

CONFIGURING THE LOCATION OF THE TRACE LOG

➤ *To configure the location of the trace log:*

1. Export the application's general settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control --get-app-settings -f <file name>
```

2. Open the XML file to edit the settings.
3. You can specify the location of the trace log on the hard drive. To do so, specify one of the following values as a <destination> value for the <tracerSettings> setting:

- Files, if you want the application to keep the trace log in a separate file in the directory /var/log/kaspersky/klms (this is the default value).
- Syslog, if you want the application to record all events in the system log of the operation system.

4. Save the changes made.

5. Import the application's general settings from an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control --set-app-settings -f <file name>
```

6. Restart the application. Execute the following command:

```
# /etc/init.d/klms restart
```

CONFIGURING THE ROTATION OF TRACE FILES

You can configure the settings of rotation of trace files, such as maximum trace file size and number of trace files to be saved. When these limits are exceeded, the old trace files are overwritten with new trace files. The trace file rotation settings make it possible to limit the volume of memory that can be taken up by the trace log.

➤ *To configure the trace file rotation settings:*

1. Export the application's general settings to an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control --get-app-settings -f <file name>
```

2. Open the XML file to edit the settings.

3. Specify the trace file rotation settings. To do so, specify the values of the following settings in the <tracerSettings> section:

- a. Specify one of the following values in the <rotationPeriod> subsection:

- NoRotation. Old trace files are overwritten with new trace files when the values of the <rotationFileSize> setting or the <maxFileCount> setting are exceeded.
- Monthly. Old trace files are overwritten with new trace files monthly when the values of the <rotationFileSize> setting or the <maxFileCount> setting are exceeded.
- Weekly. Old trace files are overwritten with new trace files weekly when the values of the <rotationFileSize> setting or the <maxFileCount> setting are exceeded.
- Daily. Old trace files are overwritten with new trace files daily when the values of the <rotationFileSize> setting or the <maxFileCount> setting are exceeded.

- Hourly. Old trace files are overwritten with new trace files hourly when the values of the <rotationFileSize> setting or the <maxFileCount> setting are exceeded.

The default value is NoRotation.

- b. In the <rotationFileSize> subsection, specify the maximum size of the trace file (in bytes). When this limit is exceeded, the old trace file is overwritten with a new trace file.

By default, the value is set to 100 MB.

- c. In the <maxFileCount> subsection, specify the maximum number of trace files that can be stored at any one time. When the number of trace files exceeds this limit, the trace files are overwritten with new files.

By default, the value is set to 10.

4. Save the changes made.
5. Import the application's general settings from an XML file using the command:

```
# /opt/kaspersky/klms/bin/klms-control --set-app-settings -f <file name>
```

TESTING THE APPLICATION OPERATION

This section provides information about how to ensure that the application detects viruses and their modifications and performs the correct actions on them.

IN THIS SECTION:

About the EICAR test file.....	164
About the types of the EICAR test file	164
Testing anti-virus protection of messages using the EICAR test file	165

ABOUT THE EICAR TEST FILE

You can make sure that the application detects viruses and disinfects infected files by using the *EICAR test file*. The EICAR test file has been developed by the European Institute for Computer Antivirus Research (EICAR) in order to test the functionality of anti-virus applications.

The EICAR test file is not a virus. The EICAR test file does not contain any program code that could damage your computer. However, a major part of anti-virus applications identify the EICAR test file as a virus.

The EICAR test file is not intended for testing the functionality of the heuristic analyzer or searching for malware at the system level (rootkits).

Do not use real viruses to test the functionality of anti-virus applications! This may damage your computer.

Do not forget to resume the anti-virus protection of Internet traffic and files after you have finished with the EICAR test file.

ABOUT THE TYPES OF THE EICAR TEST FILE

You can test the application's functioning by creating various modifications of the EICAR test file. The application detects the EICAR test file (or a modification of it) and assigns it a status depending on the results of the scan. The application takes specified actions on the EICAR test file if they had been selected in the settings of the component that has detected the EICAR test file.

The first column of the table (see the table below) contains prefixes that you can use when creating modifications of the EICAR test file. The second column lists all possible statuses assigned to the file, based on the results of the scan by the application. The third column indicates how the application processes files with the specified status.

Table 13. Modifications of the EICAR test file

Prefix	File status	File processing information
No prefix, standard test virus.	Infected. File contains code of a known virus. File cannot be disinfected.	The application identifies this file as a file containing a virus that cannot be disinfected. The action set for infected files is applied to the file. By default, the application displays an on-screen notification that the file cannot be disinfected.
CURE-	Infected. File contains code of a known virus. File can be disinfected.	The file contains a virus that can be disinfected or deleted. The application disinfects the file; the text of the virus body is replaced with the word CURE. The application displays an on-screen notification that a disinfected file has been detected.
DELE-	Infected. File contains code of a known virus. File cannot be disinfected.	The application identifies the file as a virus that cannot be disinfected, and deletes it. The application displays an on-screen notification that the disinfected file has been deleted.
WARN-	Probably infected. File contains code of an unknown virus. File cannot be disinfected.	File is probably infected. The application applies the action set for probably infected files on the file. By default, the application displays an on-screen notification that a probably infected file has been detected.
SUSP-	Probably infected. File contains modified code of a known virus. File cannot be disinfected.	The application detected a partial correspondence of a section of file code with a section of code of a known virus. When a probably infected file is detected, the application databases do not contain a description of the full code of the virus. The application applies the action set for probably infected files on the file. By default, the application displays an on-screen notification that a probably infected file has been detected.
CORR-	Corrupted.	The application does not scan this type of file because its structure is damaged (for example, the file format is invalid). You can find the information that the file has been processed in the report on the application's operation.
ERRO-	Scan error.	An error occurred during the scan of a file. The application could not access the file, since the integrity of the file has been breached (for example, no end to a multivolume archive) or there is no connection to it (if the file is scanned on a network drive). You can find the information that the file has been processed in the report on the application's operation.

TESTING ANTI-VIRUS PROTECTION OF MESSAGES USING THE EICAR TEST FILE

You can test the effectiveness of anti-virus scanning of messages using an EICAR test file or one of the varieties of the EICAR test file.

➤ To test anti-virus protection of messages using the EICAR test file:

1. You can download this EICAR test file from EICAR's official website at http://www.eicar.org/anti_virus_test_file.htm.
2. Save the EICAR test file.
3. Send an email message with the EICAR test file to a computer with Kaspersky Security installed.

Kaspersky Security informs you that a threat has been detected and blocks the attempt to save the object.

➡ *To test anti-virus protection of messages using one of the EICAR test files:*

1. You can download this EICAR test file from EICAR's official website at http://www.eicar.org/anti_virus_test_file.htm.
2. Save the EICAR test file.
3. Add one of the prefixes to the head of the EICAR test file (see section "About the types of the EICAR test file" on page [164](#)).

You can use any text or hypertext editor to do this.

4. Save the resulting file under a name corresponding to the type of the EICAR file. For example, by adding the DELE- prefix, save the resulting file under the name eicar_dele.com.
5. Send an email message with the eicar_dele.com file in the attachment to a computer with Kaspersky Security installed.

Kaspersky Security informs you that a threat has been detected and performs the action configured in the scan settings.

ADMINISTRATION OF THE APPLICATION THROUGH KASPERSKY SECURITY CENTER

This section describes how you can manage Kaspersky Security 8.0 for Linux Mail Server through Kaspersky Security Center.

IN THIS SECTION:

About managing the application via Kaspersky Security Center	167
Configuring administration of the application through Kaspersky Security Center	167
Starting and stopping Kaspersky Security on a client computer.....	169
Managing tasks	170
Viewing general information on the operation of Kaspersky Security in a cluster	174

ABOUT MANAGING THE APPLICATION VIA KASPERSKY SECURITY CENTER

Kaspersky Security Center is designed for centrally managing and monitoring mail servers with Kaspersky Security installed by performing the primary administrative tasks. Kaspersky Security Center supports interaction through all network configurations that use the TCP/IP protocol.

Kaspersky Security Center supports the following operations in administering Kaspersky Security installed on mail servers:

- Adding the active or additional key.
- Running the Kaspersky Security database update task.
- View information about the protection status of a cluster of mail servers.
- Start and stop Kaspersky Security.

CONFIGURING ADMINISTRATION OF THE APPLICATION THROUGH KASPERSKY SECURITY CENTER

To configure the process of administering Kaspersky Security via Kaspersky Security Center:

1. Install Kaspersky Security Center Network Agent (see section "Installing Network Agent" on page [168](#)). Network Agent comes in a separate installation package together with the Kaspersky Security installation package.
2. Configure Network Agent settings using the initial configuration script (see section "Configuring Network Agent settings" on page [168](#)),
3. Install the Kaspersky Security administration plug-in (see the section "Installing Kaspersky Security administration plug-in" on page [169](#)).

IN THIS SECTION:

Installing Network Agent.....	168
Configuring Network Agent settings	168
Installing the Kaspersky Security administration plug-in.....	169
Checking the connection to Kaspersky Security Center.....	169

INSTALLING NETWORK AGENT

You must have root privileges to initiate installation of Network Agent.

- To install Network Agent from an RPM package, execute the following command:

```
# rpm -i klnagent-<version_number>.i386.rpm
```

- To install Network Agent from a DEB package on a 32-bit operating system, execute the following command:

```
# dpkg -i klnagent_<version_number>_i386.deb
```

- To install Network Agent from a DEB package on a 64-bit operating system, execute the following command:

```
# dpkg -i --force-architecture klnagent_<version_number>_i386.deb
```

After the command has been executed, Network Agent is installed automatically.

After installation, configure the settings of Network Agent (see section "Configuring Network Agent settings" on page [168](#)).

CONFIGURING NETWORK AGENT SETTINGS

- To configure Network Agent settings:

1. Execute the command `# /opt/kaspersky/klnagent/lib/bin/setup/postinstall.pl`.

The Network Agent initial configuration script starts.

2. After launching the script, do the following:

- a. Specify the DNS name or IP address of the Administration Server of Kaspersky Security Center.
- b. Specify the port number of the Administration Server or the default port number (14000).
- c. Specify the SSL port number of the Administration Server or the default port number (13000).
- d. Specify whether the SSL connection should be used for data transfer. By default, the SSL connection is enabled.
- e. Specify if you want to use Network Agent as a gateway for connecting to Kaspersky Security Center. By default, the connection to Kaspersky Security Center is established directly without using a gateway.

For details on configuring Network Agent, see the *Administrator's Guide for Kaspersky Security Center*.

INSTALLING THE KASPERSKY SECURITY ADMINISTRATION PLUG-IN

➤ To install the Kaspersky Security administration plug-in

1. Run the klcfginst.msi file from the folder with the Kaspersky Security installation package.
2. Wait for the Installation Wizard to finish.

CHECKING THE CONNECTION TO KASPERSKY SECURITY CENTER

After installing and configuring Network Agent, you can check the connection of Kaspersky Security to the Administration Server of Kaspersky Security Center using the klnagchk utility.

➤ To check the connection to Kaspersky Security Center, execute the following command:

```
# /opt/kaspersky/klnagent/bin/klnagchk
```

The klnagchk utility displays the results of the connection check.

If problems occurred during the connection check, look for a solution in the *Administrator's Guide for Kaspersky Security Center*.

STARTING AND STOPPING KASPERSKY SECURITY ON A CLIENT COMPUTER

➤ To start or stop Kaspersky Security on a client computer:

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Managed computers** folder of the console tree, open the folder with the name of the administration group to which the relevant client computer belongs.
3. In the results pane, select the **Computers** tab.
4. In the list of client computers, select the computer on which you want to start or stop Kaspersky Security.
5. Do one of the following:

- Right-click to display the context menu of the client computer. Select **Properties**.
- In the **Actions** menu, select **Computer properties**.


A client computer properties window opens.

6. In the client computer properties window, select the **Applications** section.

A list of Kaspersky Lab applications that are installed on the client computer appears in the right part of the client computer properties window.

7. Select the application Kaspersky Security 8.0 for Linux Mail Server.


8. Do the following:

- To start Kaspersky Security, click the  button on the right of the list of Kaspersky Lab applications or do the following:

- a. Right-click to display the context menu of Kaspersky Security 8.0 for Linux Mail Server and select **Properties**, or click the **Properties** button under the list of Kaspersky Lab applications.

The **Kaspersky Security 8.0 for Linux Mail Server application settings** window opens on the **General** tab.

- b. Click the **Start** button.

- To stop Kaspersky Security, click the  button on the right of the list of Kaspersky Lab applications or do the following:

- a. Right-click to display the context menu of Kaspersky Security 8.0 for Linux Mail Server and select **Properties**, or click the **Properties** button under the list of applications.

The **Kaspersky Security 8.0 for Linux Mail Server application settings** window opens on the **General** tab.

- b. Click the **Stop** button.

MANAGING TASKS

This section describes how you can manage tasks for Kaspersky Security 8.0 for Linux Mail Server. View the *Kaspersky Security Center Administrator Guide* for details on the concept of task management through Kaspersky Security Center.

IN THIS SECTION:

About tasks for Kaspersky Security 8.0 for Linux Mail Server	170
Creating a local task.....	171
Creating a group task.....	171
Creating a task for a set of computers.....	172
Editing task settings	172

ABOUT TASKS FOR KASPERSKY SECURITY 8.0 FOR LINUX MAIL SERVER

Kaspersky Security Center controls the activity of Kaspersky Lab applications on client computers by means of tasks.

You can create the following types of tasks to administer Kaspersky Security 8.0 for Linux Mail Server through Kaspersky Security Center:

- Local tasks that are configured for a separate client computer
- Group tasks that are configured for client computers within one or more administration groups
- Tasks for sets of computers outside administration groups

Tasks for sets of computers outside administration groups apply only to client computers that are specified in the task settings. If new client computers are added to a set of computers for which a task is configured, this task does not apply to these new computers. To apply the task to these computers, create a new task or edit the settings of the existing task.

You can manage the key addition task by managing Kaspersky Security 8.0 for Linux Mail Server remotely via Kaspersky Security Center. While performing this task, the application adds a key for application activation, including an additional key.

You can manage tasks as follows:

- Start a task

If Kaspersky Security 8.0 for Linux Mail Server is running (see section "Starting and stopping Kaspersky Security on a client computer" on page 169) on a client computer, you can start a task on this client computer through Kaspersky Security Center. If Kaspersky 8.0 for Linux Mail Server is stopped, the running tasks are aborted, and it is no longer possible to manage tasks on this client computer through Kaspersky Security Center.

- Create new tasks
- Edit task settings

CREATING A LOCAL TASK

➔ *To create a local task:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Managed computers** folder of the console tree, open the folder with the name of the administration group to which the relevant client computer belongs.
3. In the results pane, select the **Computers** tab.
4. In the list of client computers, select a computer for which you want to create a local task.
5. Do one of the following:
 - Right-click to display the context menu of the client computer. Select **Properties**.
 - In the **Actions** menu, select **Computer properties**.

A client computer properties window opens.

6. Select the **Tasks** tab.
7. Click the **Add** button.
The Task Wizard starts.
8. Follow the instructions of the Task Wizard.

CREATING A GROUP TASK

➔ *To create a group task:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the console tree, open the **Managed computers** folder.
3. In the results pane, select the **Tasks** tab.
4. Do one of the following:

- Click the **Create task** button.
- Right-click to display the context menu. Select **Create→Task**.

The Task Wizard starts.

5. Follow the instructions of the Task Wizard.

CREATING A TASK FOR A SET OF COMPUTERS

➤ *To create a task for a set of computers:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the console tree, open the **Tasks for sets of computers** folder.
3. Do one of the following:
 - Click the **Create task** button.
 - Right-click to display the context menu. Select **Create → Task**.

The Task Wizard starts.

4. Follow the instructions of the Task Wizard.

EDITING TASK SETTINGS

The Kaspersky Security task settings that you can configure through Kaspersky Security Center are identical to the task settings that you can configure through the local interface of Kaspersky Security. You can configure the task settings when you create a task or edit its settings after the task is created.

➤ *To edit the settings of a local task:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Managed computers** folder of the console tree, open the folder with the name of the administration group to which the relevant client computer belongs.
3. In the results pane, select the **Computers** tab.
4. In the list of client computers, select the computer for which you want to configure Kaspersky Security settings.
5. Do one of the following:
 - Right-click to display the context menu of the client computer. Select **Properties**.
 - In the **Actions** menu, select **Computer properties**.

A client computer properties window opens.

6. Select the **Tasks** section.

A list of local tasks appears in the right part of the window.

7. Select the necessary local task in the local tasks list.
8. Do one of the following:

- Right-click to display the context menu of the task. Select **Properties**.
- Click the **Properties** button.

The **<Local task name> properties** window opens.

9. In the **<Local task name> task properties** window, select the **Settings** section.
10. Edit the local task settings.
11. To save your changes, in the **Properties: <Local task name>** window, click **OK**.

➤ *To edit the settings of a group task:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Managed computers** folder, open the folder with the name of the necessary administration group.
3. In the results pane, select the **Tasks** tab.

A list of group tasks appears in the lower part of the tasks pane.

4. Select the necessary group task in the group tasks list.
5. Do one of the following:
 - Right-click to display the context menu of the task. Select **Properties**.
 - On the right of the group tasks list, click the **Edit task settings** button.

The **Properties: <Group task name>** window opens.

6. In the **Properties: <Group task name>** window, select the **Settings** section.
7. Edit the group task settings.
8. To save your changes, in the **Properties: <Group task name>** window, click **OK**.

➤ *To edit the settings of a task for a set of computers:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Tasks for sets of computers** folder of the console tree, select a task for a set of computers whose settings you want to edit.
3. Do one of the following:
 - Right-click to display the context menu of the task for a set of computers. Select **Properties**.
 - On the right of the list of tasks for sets of computers, click the **Edit task settings** button.

The **Properties: <Name of the task for a set of computers>** window opens.

4. In the **Properties: <Name of the task for a set of computers>** window, select the **Settings** section.
5. Edit the settings of the task for a set of computers.
6. To save your changes, in the **Properties: <Name of the task for a set of computers>** window, click **OK**.

Except for the **Settings** tab, all tabs in the task properties window are identical to those that are used in Kaspersky Security Center. Consult the *Kaspersky Security Center Administrator Guide* for their detailed description. The **Settings**

tab contains settings that are specific to Kaspersky Security. The content of the tab varies depending on the task type that is selected.

VIEWING GENERAL INFORMATION ON THE OPERATION OF KASPERSKY SECURITY IN A CLUSTER

► *To view general information on the operation of Kaspersky Security 8.0 for Linux Mail Server in a cluster:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Managed computers** folder of the console tree, open the **Security for Linux Mail Server** folder.
3. Open the **Clusters and server arrays** folder.
4. In the details pane, select the cluster for whose computers you want to view information on the operation of Kaspersky Security 8.0 for Linux Mail Server.
5. Right-click to open the context menu of the cluster. Select **Properties**.

The cluster properties window opens.

6. Select the **Dashboard** section.

A table with information on the operation of Kaspersky Security 8.0 for Linux Mail Server for each computer in the cluster appears in the right part of the window. More details about managing clusters are available in the *Administrator's Guide for Kaspersky Security Center*.

CONTACTING THE TECHNICAL SUPPORT SERVICE

This section describes the ways to get technical support and the terms on which it is available.

IN THIS SECTION:

Technical support by phone	175
Technical Support via Kaspersky CompanyAccount	175
Using a trace file and AVZ script	176
Extended diagnostics of application operation	176

TECHNICAL SUPPORT BY PHONE

If an urgent issue arises, you can call Kaspersky Lab Technical Support representatives (<http://support.kaspersky.com/support/contacts>).

Before contacting Technical Support, you are advised to read the technical support rules (<http://support.kaspersky.com/support/rules>). These rules contain information about the working hours of Kaspersky Lab Technical Support and about the information that you must provide so that Kaspersky Lab Technical Support specialists can help you.

TECHNICAL SUPPORT VIA KASPERSKY COMPANYACCOUNT

Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>) is a web service for companies that use Kaspersky Lab applications. The Kaspersky CompanyAccount web service is designed to facilitate interaction between users and Kaspersky Lab specialists via online requests. You can use Kaspersky CompanyAccount to track the status of your online requests and store a history of them as well.

You can register all of your organization's employees under a single account on Kaspersky CompanyAccount. A single account lets you centrally manage electronic requests from registered employees to Kaspersky Lab and also manage the privileges of these employees via Kaspersky CompanyAccount.

The Kaspersky CompanyAccount web service is available in the following languages:

- English
- Spanish
- Italian
- German
- Polish
- Portuguese

- Russian
- French
- Japanese

To learn more about Kaspersky CompanyAccount, visit the Technical Support website (http://support.kaspersky.com/faq/companyaccount_help).

USING A TRACE FILE AND AVZ SCRIPT

After you report a problem to Kaspersky Lab Technical Support specialists, they may ask you to generate a report with information about the operation of Kaspersky Security and send it to Kaspersky Lab Technical Support. Kaspersky Lab Technical Support specialists may also ask you to create a *trace file*. The trace file allows you to trace the process of performing application commands step by step and determine the stage of application operation at which an error occurs.

After analyzing the data you send, Kaspersky Lab Technical Support specialists can create an AVZ script and send it to you. By running AVZ scripts, it is possible to analyze active processes for threats, scan the computer for threats, disinfect or delete infected files, and create system scan reports.

EXTENDED DIAGNOSTICS OF APPLICATION OPERATION

To perform extended diagnostics of problems in the operation of the application, you can use certain application administration commands. These commands are not described in the Administrator's Guide for Kaspersky Security 8.0 for Linux Mail Server. A Technical Support representative will send you these commands if necessary.

APPENDICES

This section provides information that complements the document text.

IN THIS SECTION:

Application file locations on a computer running Linux.....	177
Application file locations on a computer running FreeBSD.....	178

APPLICATION FILE LOCATIONS ON A COMPUTER RUNNING LINUX

After Kaspersky Security has been installed on a computer running a Linux operating system, the application files are arranged as follows by default:

`/etc/opt/kaspersky/klms` : this directory contains the Kaspersky Security configuration files:

- `kavscanner_defaults.conf` – configuration file of the kavscanner utility;
- `klms_filters.conf` – configuration file of the mail agent's filter.

`/opt/kaspersky/klms/` – root folder of Kaspersky Security, which includes:

`/opt/kaspersky/klms/bin/` – folder containing the executable files of Kaspersky Security:

- `klms-control` – executable file of the Kaspersky Security control utility;
- `klms-setup.pl` – initial configuration script for Kaspersky Security;

`/opt/kaspersky/klms/lib/` – folder containing Kaspersky Security libraries;

`/opt/kaspersky/klms/lib64/` – folder containing additional 64-bit libraries of Kaspersky Security;

`/opt/kaspersky/klms/libexec/` – folder containing service executable files of Kaspersky Security;

`/opt/kaspersky/klms/libexec/cleanup.sh` – script for cleaning up data remaining after Kaspersky Security removal;

`/opt/kaspersky/klms/share/` – folder storing font files, files of the Kaspersky Security help system (manual pages), localization packages, source code of Kaspersky Security modules, MIB files, and files with the text of the End User License Agreement:

`/opt/kaspersky/klms/share/man/` – folder storing files of the Kaspersky Security help system (manual pages);

`/opt/kaspersky/klms/share/locale` – folder storing localization packages;

`/opt/kaspersky/klms/share/src/` – folder storing source code of Kaspersky Security modules;

`/opt/kaspersky/klms/share/snmp-mibs/` – folder storing MIB files of Kaspersky Security.

`/opt/kaspersky/klmsui/lib/` – folder storing libraries of the Kaspersky Security web interface.

`/opt/kaspersky/klmsui/bin/klmsui-setup.pl` – initial configuration script for the web interface of Kaspersky Security.

`/opt/kaspersky/klmsui/share/htdocs` – folder storing all hml resources of the Kaspersky Security web interface.

`/opt/kaspersky/klmsui/libexec/` – folder storing service executable files of the Kaspersky Security web interface:

`/opt/kaspersky/klmsui/libexec/cleanup.sh` – script for cleaning up data remaining after removal of the Kaspersky Security web interface;

`/opt/kaspersky/klmsui/libexec/mod_klwi.so` – module of the Apache web server.

`/var/opt/kaspersky/klms/` – folder storing Kaspersky Security data:

`/var/opt/kaspersky/klms/backup` – Backup for message copies;

`/var/opt/kaspersky/klms/reports/` – on-demand reports;

`/var/opt/kaspersky/klms/reports/weekly` – scheduled weekly reports;

`/var/opt/kaspersky/klms/reports/daily` – scheduled daily reports;

`/var/opt/kaspersky/klms/reports/monthly` – scheduled monthly reports;

`/var/opt/kaspersky/klms/postgresql/` – Kaspersky Security database;

`/var/opt/kaspersky/klms/update/` – folder storing Kaspersky Security update packages;

`/var/opt/kaspersky/klms/update/asbases` – folder storing Anti-Spam database update packages downloaded from update sources;

`/var/opt/kaspersky/klms/update/avbases` – folder storing Anti-Virus database update packages downloaded from update sources;

`/var/opt/kaspersky/klms/update/asbases` – folder storing compiled Anti-Spam databases;

`/var/opt/kaspersky/klms/update/avbases-backup` – folder storing backup copies of Anti-Virus database update packages;

`/var/opt/kaspersky/klms/update/asbases-backup` – folder storing backup copies of Anti-Spam database update packages.

`/var/log/kaspersky/klms/` – folder storing trace files of Kaspersky Security.

`/var/run/klms/` – folder storing service files of Kaspersky Security.

APPLICATION FILE LOCATIONS ON A COMPUTER RUNNING FREEBSD

After Kaspersky Security has been installed on a computer running a FreeBSD operating system, the application files are arranged as follows by default:

`/usr/local/libexec/kaspersky/klms` – folder containing Kaspersky Security libraries;

`/usr/local/lib/kaspersky/klms` – folder containing Kaspersky Security libraries;

`/usr/local/bin/` – folder containing the executable files of Kaspersky Security:

`/usr/local/bin/kavscanner` – configuration file of the kavscanner utility;

`/usr/local/bin/klms-control` – executable file of the Kaspersky Security control utility;

`/usr/local/bin/klms-disable_content_reputation.pl` – script for disabling content filtering and clearing the quarantine.

`/usr/local/bin/klms-setup.pl` – initial configuration script for Kaspersky Security;

`/usr/local/bin/klms-uninstall_filters.pl` – script for disintegrating from the mail server;

`/usr/local/etc/rc.d/klms` – application launch script;

`/usr/local/etc/rc.d/klmsdb` – database launch script;

`/usr/local/man/` – folder storing files of the Kaspersky Security help system (manual pages);

`/usr/local/share/doc/klms/` – folder storing font files, images, localization packages, files with the text of the End User License Agreement, MIB files, source code of modules:

`/usr/local/share/klms/fonts` – folder storing font files;

`/usr/local/share/klms/images` – folder storing images;

`/usr/local/share/klms/locale` – folder storing localization packages;

`/usr/local/share/klms/snmp-mibs` – folder storing the MIB files of Kaspersky Security;

`/usr/local/share/klms/srcsrc/` – folder storing source code of Kaspersky Security modules.

`/var/db/kaspersky` – folder storing application files and data:

`/var/db/kaspersky/klms/cleanup.sh` – script for cleaning up data remaining after Kaspersky Security removal;

`/var/db/kaspersky/klms/backup` – folder storing copies of Backup messages;

`/var/db/kaspersky/klms/postgresql` – Kaspersky Security database;

`/var/db/kaspersky/klms/reports` – on-demand reports;

`/var/db/kaspersky/klms/reports/daily` – scheduled daily reports;

`/var/db/kaspersky/klms/reports/monthly` – scheduled monthly reports;

`/var/db/kaspersky/klms/reports/weekly` – scheduled weekly reports.

`/var/db/kaspersky/klms/update` – folder storing Kaspersky Security update packages:

`/var/db/kaspersky/klms/update/asbases` – folder storing Anti-Spam database update packages downloaded from update sources;

`/var/db/kaspersky/klms/update/asbases-backup` – folder storing backup copies of Anti-Spam database update packages;

`/var/db/kaspersky/klms/update/avbases` – folder storing Anti-Virus database update packages downloaded from update sources;

`/var/db/kaspersky/klms/update/avbases-backup` – folder storing backup copies of Anti-Virus database update packages;

`/var/db/kaspersky/klms/update/aspbases` – folder storing compiled Anti-Spam databases.

`/var/log/kaspersky/klms/` – folder storing trace files of Kaspersky Security.

KASPERSKY LAB

Kaspersky Lab software is internationally renowned for its protection against viruses, malware, spam, network and hacker attacks, and other threats.

In 2008, Kaspersky Lab was rated among the world's top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky Lab is the preferred developer of computer protection systems among home users in Russia, according to the COMCON survey "TGI-Russia 2009".

Kaspersky Lab was founded in Russia in 1997. Today, it is an international group of companies headquartered in Moscow with five regional divisions that manage the company's activity in Russia, Western and Eastern Europe, the Middle East, Africa, North and South America, Japan, China, and other countries in the Asia-Pacific region. The company employs more than 2000 qualified specialists.

PRODUCTS. Kaspersky Lab's products provide protection for all systems—from home computers to large corporate networks.

The personal product range includes anti-virus applications for desktop, laptop, and tablet computers, and for smartphones and other mobile devices.

Kaspersky Lab delivers applications and services to protect workstations, file and web servers, mail gateways, and firewalls. Used in conjunction with Kaspersky Lab's centralized management system, these solutions ensure effective automated protection for companies and organizations against computer threats. Kaspersky Lab's products are certified by the major test laboratories, are compatible with the software of many suppliers of computer applications, and are optimized to run on many hardware platforms.

Kaspersky Lab's virus analysts work around the clock. Every day they uncover hundreds of new computer threats, create tools to detect and disinfect them, and include them in the databases used by Kaspersky Lab applications. *Kaspersky Lab's Anti-Virus database is updated hourly; and the Anti-Spam database every five minutes.*

TECHNOLOGIES. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. This is one of the reasons why many third-party software developers have chosen to use the Kaspersky Anti-Virus engine in their own applications. Those companies include SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), CommuniGate Systems (USA), Openwave Messaging (Ireland), D-Link (Taiwan), M86 Security (USA), GFI Software (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), Netasq+Arkoon (France), NETGEAR (USA), Parallels (USA), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Many of the company's innovative technologies are patented.

ACHIEVEMENTS. Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. For example, in 2010 Kaspersky Anti-Virus received several top Advanced+ awards in a test administered by AV-Comparatives, a respected Austrian anti-virus laboratory. But Kaspersky Lab's main achievement is the loyalty of its users worldwide. The company's products and technologies protect more than 300 million users, and its corporate clients number more than 200,000.

Kaspersky Lab official site:

<http://www.kaspersky.com>

Virus encyclopedia:

<http://www.securelist.com>

Virus Lab:

<http://newvirus.kaspersky.com> (for analyzing suspicious files and websites)

Kaspersky Lab web forum:

<http://forum.kaspersky.com>

INFORMATION ABOUT THIRD-PARTY CODE

Information about third-party code is contained in the file legal_notices.txt, in the application installation folder.

TRADEMARK NOTICES

Registered trademarks and service marks are the property of their respective owners.

Apache and Apache feather logo are trademarks of Apache Software Foundation.

Active Directory, Microsoft, and Internet Explorer are trademarks of Microsoft Corporation registered in the United States of America and elsewhere.

Linux is a trademark of Linus Torvalds, registered in the USA and elsewhere.

Sendmail and other names and product names are trademarks or registered trademarks of Sendmail, Inc.

The FreeBSD mark is the registered trademark of the FreeBSD Foundation.

Intel, Xeon, Core are trademarks of Intel Corporation registered in the United States of America and elsewhere.

Red Hat Enterprise Linux is a trademark of Red Hat Inc. registered in the United States of America and elsewhere.

Novell is a trademark of Novell Inc. registered in the USA and elsewhere.

Debian is a registered trademark of Software in the Public Interest, Inc.

Mozilla, Firefox are trademarks of the Mozilla Foundation.

Google Chrome is a trademark owned by Google, Inc.

UNIX is a trademark registered in the USA and elsewhere and used under license granted by X/Open Company Limited.

INDEX

A

About a company employee account	137
configuring	138
activating and deactivating	137
Actions on objects	83
Active Directory	
integration	128
After-queue	
integration with Postfix mail server	64
Amavis	
integration with the interface	69
Anti-Phishing	103
configuring	105
enabling and disabling	103
Anti-Spam	87
enabling / disabling	88
message size limitations	93
Anti-Virus	
configuring	97
enabling / disabling	95
excluding messages from scanning by attachment format	100
excluding messages from scanning by attachment name	101
message that cannot be disinfected	98
Anti-Virus	95
Apache	
connecting to the web server	29
AVZ script	176

B

Backup	140
maximum size	143
Before-queue	
integration with Postfix mail server	66

C

Content filtering	107
enabling and disabling	107
Content filtering by attachment format	110
Content filtering by attachment name	109
Content filtering by message size	109

D

Databases	112
manual update	119
select update source	114
sources of update	114

E

EICAR	164
Email notifications	144
configuring	147
templates editing	148
Event log	156

configuring	158
Exim	
integration with mail server	57
F	
Facade	
application interaction with utilities and administration systems.....	29
H	
Hardware and software requirements	15
I	
Installing the application package.....	25
Installing the localization package	26
Installing the web interface package	28
K	
KASPERSKY.....	180
Kaspersky Security Network	32
enabling and disabling	32
Key	72
adding.....	74
removing.....	74
L	
LDAP protocol	
configuring	128
License.....	71
activation code	
License	
key.....	72
key file	73
License Agreement.....	72
viewing information about the license and added keys	74
M	
Message processing rules.....	79
configuring Anti-Phishing.....	105
configuring Anti-Spam	90
configuring Anti-Virus.....	99
configuring content filtering.....	108
creating rules	81
delivering messages from Backup.....	142
finding message copies	141
saving messages to file	142
MIB	
objects	136
structure.....	136
Milter	
protocol for integration with the Postfix mail server.....	68
N	
Notifications.....	144
P	
Postfix	
integration with mail server	64
Preparing.....	20

Q

QMail	
integration with mail server	63

S

Sendmail	
integration with mail server	54
SNMP protocol	134
enabling	135
event traps	136
process ID	135

T

Tracing	
trace file	176

U

Upgrading from a previous version of the application.....	21
---	----