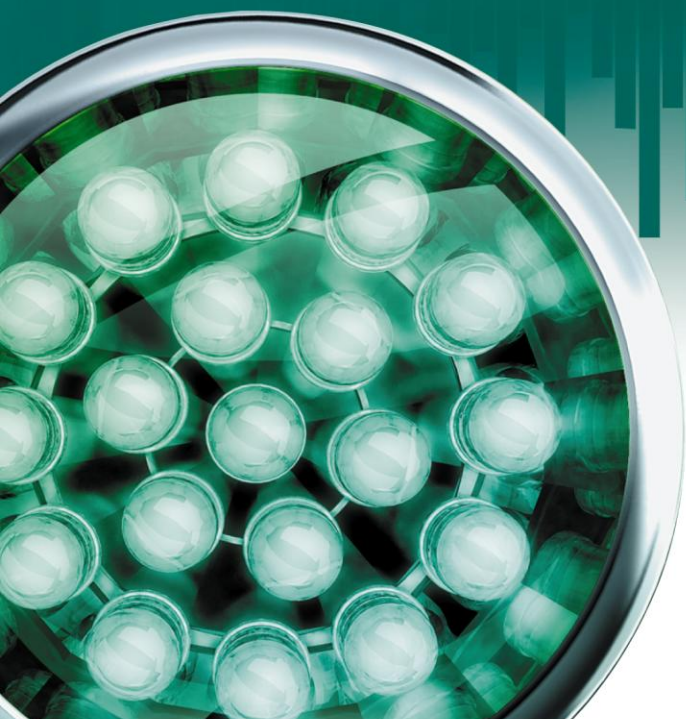


Kaspersky Anti-Virus 8.0 for Linux File Server

ADMINISTRATOR'S GUIDE

APPLICATION VERSION: 8.0



KASPERSKY lab

Dear User!

Thank you for choosing our product. We hope that this documentation will help you in your work and will provide answers regarding this software product.

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

All materials may only be duplicated, regardless of form, or distributed, including in translation, with the written permission of Kaspersky Lab ZAO.

This document and graphic images related to it may be used exclusively for informational, non-commercial, and personal purposes.

The document can be modified without prior notification. For the latest version of this document, refer to the Kaspersky Lab website at <http://www.kaspersky.com/docs>.

Kaspersky Lab ZAO assumes no liability for the content, quality, relevance, or accuracy of any materials used in this document for which the rights are held by third parties, or for any potential damages associated with the use of such documents.

This document involves the registered trademarks and service marks which are the property of their respective owners.

Document revision date: 11/10/2010

© 1997-2010 Kaspersky Lab ZAO. All Rights Reserved.

<http://www.kaspersky.com>

<http://support.kaspersky.com>

CONTENTS

INTRODUCTION.....	8
General information on Kaspersky Anti-Virus	8
Real-time protection and on-demand scan	9
Peculiarities in scanning of symbolic and hard links	9
About infected, suspicious objects and objects with the status "Warning"	10
About backup and quarantine	10
Programs detectable by Kaspersky Anti-Virus	11
Obtaining information about Kaspersky Anti-Virus	13
Sources of information for further research.....	13
Contacting the Technical Support Service	15
Discussion of Kaspersky Lab's applications in web forum	16
WORKING WITH KASPERSKY WEB MANAGEMENT CONSOLE.....	16
Launching the Web Management Console.....	16
Changing the user password for the Web Management Console.....	17
STARTING AND STOPPING KASPERSKY ANTI-VIRUS	18
MANAGING THE TASKS IN KASPERSKY ANTI-VIRUS	19
Creating an on-demand scan or update task.....	19
Deleting an on-demand scan or update task	20
Manual task management	20
Automatic task management	20
Viewing task state.....	21
Viewing task statistics.....	22
UPDATING KASPERSKY ANTI-VIRUS.....	23
Selecting an update source	24
Updating from local or network folder	24
Using the proxy server.....	26
Last database update rollback.....	26
REAL-TIME PROTECTION.....	27
The structure of predefined security levels in the real-time protection task	27
Creating a protection scope.....	30
Restricting a protection area using masks and regular expressions	31
Exclusion of objects from a protection area	32
Creating a global exclusion area.....	32
Excluding objects from the protection area	33
Exclusion of objects depending on user and group accounts accessing the objects	34
Excluding objects by names of the threats detected in them	34
Selecting interception mode	35
Selecting protection mode	35
Using heuristic analysis	36
Using scan mode depending on user and group accounts accessing the objects.....	36
Selecting actions to perform on detected objects	37
Selecting actions depending on the threat type.....	38
Scan optimization	39
Compatibility with other Kaspersky Lab's applications.....	40

ON-DEMAND SCAN	43
The structure of predefined security levels in on-demand scan tasks	43
Quick scan of files and directories	46
Creating a scan area	48
Restricting a scan area using masks and regular expressions	49
Excluding objects from the scan area	49
Creating a global exclusion area	50
Excluding objects from the scan area	50
Excluding objects by names of the threats detected in them	51
Using heuristic analysis	52
Selecting actions to perform on detected objects	52
Selecting actions depending on the threat type	53
Scan optimization	55
Selecting task priority	55
ISOLATING SUSPICIOUS OBJECTS. DATA BACKUP	57
Viewing statistics of quarantined objects	57
Scanning quarantined objects	58
Placing files to quarantine manually	59
Viewing object IDs	59
Restoring objects	60
Deleting objects	61
MANAGING LICENSES	61
About the License Agreement	62
About licenses for Kaspersky Anti-Virus	62
About Kaspersky Anti-Virus key files	63
Installing the key file	63
Viewing information about a license prior to the key file installation	64
Key file removal	65
Reviewing the license agreement	65
ADMINISTRATOR NOTIFICATIONS. EVENT-BASED ACTIONS	66
Using the internal mailer of Kaspersky Anti-Virus	67
Using Sendmail	68
Generation of notifications	68
Configuring actions	69
Using macros	69
GENERATING REPORTS	71
VIEWING THE PROTECTION STATUS VIA SNMP	72
Configuring interaction via SNMP	72
Structure of the Kaspersky Anti-Virus MIB	73
Description of Kaspersky Anti-Virus MIB objects	75
MANAGING KASPERSKY ANTI-VIRUS FROM THE COMMAND LINE	79
Displaying Kaspersky Anti-Virus command help	81
Starting Kaspersky Anti-Virus	82
Stopping Kaspersky Anti-Virus	82
Restarting Kaspersky Anti-Virus	82
Enabling events output	82

Quick scan of files and directories	83
Rollback of Kaspersky Anti-Virus databases	83
Commands for obtaining reports and statistics	84
Viewing application information.....	84
Viewing Anti-Virus activity reports.....	84
Viewing reports on the most commonly encountered threats.....	86
Commands for managing the Anti-Virus settings and tasks	87
Viewing general settings of Kaspersky Anti-Virus	87
Editing the general settings of Kaspersky Anti-Virus.....	88
Viewing the list of Kaspersky Anti-Virus tasks.....	89
Viewing task state	90
Starting the task	91
Stopping the task	92
Pausing the task	92
Resuming the task	93
Obtaining task settings.....	93
Modifying task settings.....	94
Creating a task.....	95
Deleting tasks	96
Obtaining task schedule settings	96
Modifying task schedule settings	97
Searching for scheduled events.....	98
Licenses management commands	99
Validating a key file prior to installation	99
Viewing information about a license prior to the key file installation.....	100
Viewing information about the installed key files.....	101
Viewing the status of installed licenses	102
Active key file installation	102
Supplementary key file installation.....	102
Active key file removal	103
Supplementary key file removal	103
Quarantine and backup storage management commands	103
Obtaining brief quarantine or backup storage statistics	104
Obtaining information about storage objects.....	104
Obtaining information about one object in the storage	105
Restoring objects from the storage	105
Placing an object in quarantine manually.....	105
Deleting one object from the storage	106
Exporting objects from the storage into a specified directory	106
Importing previously exported objects into the storage	107
Clearing the storage.....	107
Logs management commands	108
Obtaining the number of Anti-Virus events, using a filter	108
Obtaining information about Kaspersky Anti-Virus events	109
Viewing the time interval, during which the events will occur that are registered in the log	110
Event log rotation	110
Removing objects from the event log.....	110
Limiting selections using filters	111
Logical expressions	111

Object parameters in quarantine/backup storage	112
Anti-Virus events and their data	114
ANTI-VIRUS CONFIGURATION FILE SETTINGS	123
Rules for editing Kaspersky Anti-Virus INI configuration files	123
Real-time protection and on-demand scan tasks settings	124
Update tasks settings	137
Schedule settings	141
Start rules.....	142
Stop rules.....	143
Pause rules	144
Specifying exact time	145
General settings of Kaspersky Anti-Virus	145
Quarantine and backup storage settings	147
Event log settings	148
Settings of notifications and event-based actions.....	150
MANAGING KASPERSKY ANTI-VIRUS VIA KASPERSKY ADMINISTRATION KIT	153
Viewing the server protection status	153
The "Application Settings" dialog box	154
Creating and configuring tasks	154
Creating a task	154
The Local task creation wizard	155
Step 1. Entering general task settings	156
Step 2. Selecting an application and defining task type	156
Step 3. Configuring task settings	156
Step 4. Scheduling the task	156
Step 5. Completing the wizard	157
Updating tasks settings.....	157
Creating a scan area.....	157
Configuring security settings	158
Creating an excluded area	158
Selecting an update source.....	159
Selecting the type of updates	160
Scheduling a task via Kaspersky Administration Kit	161
Creating a task start rule	161
Creating a task stop rule	161
Creating a task pause rule	162
Creating and configuring policies.....	163
Creating a policy	164
Configuring a policy	164
Checking connection with Administration Server manually. The klnagchk utility	165
Connecting to Administration Server manually. The klmover utility	165
Tasks settings.....	166
Interception method	167
Protection mode.....	167
Heuristic analysis	168
Action to perform on infected objects	168
Action to be performed on suspicious objects.....	169
Actions to be performed on objects depending on the threat type	170

Excluding objects by name	170
Excluding objects by threat name	170
Scan of compound files.....	171
Maximum object scan time.....	171
Maximum size of a scanned object.....	172
Updates source.....	172
FTP server mode	172
FTP or HTTP server response wait time.....	172
Using a proxy server to connect to update sources	173
Proxy server authentication.....	173
Proxy server settings	173
Directory for saving updates	173
Updates type.....	173
KASPERSKY LAB ZAO	175
INFORMATION ABOUT THIRD-PARTY CODE	176
Program code.....	176
APACHE 1.3.41	177
EXPAT 1.95.8	183
GSOAP	183
JQUERY 1.3.2	188
LIBHARU 2.1.0	189
LIBXML2-2.6.32.....	189
LIBXSLT-1.1.23	189
LIBPCRE 7.4.....	190
ZLIB 1.2.3	191
BOOST 1.39.0	191
LIBACL 2.2.45-1	191
ATTR 2.4.38-1	191
LIBPNG 1.2.44.....	192
LIBUTF.....	192
LZMALIB 4.43.....	192
NET-SNMP 5.5	192
SQLITE 3.6.17	196
DEJAVU SANS 2.31	196
PROTOTYPE-1.6.0.3.....	198
Distributed program code	198
REDIRFS 0.10 (MODIFIED)	198
Other information.....	198

INTRODUCTION

Kaspersky Anti-Virus protects file servers running under Linux and FreeBSD operating systems against malware penetrating computers through file exchange.

Kaspersky Anti-Virus scans the server disks and other mounted devices. It can scan individual directories accessible over SMB/CIFS and NFS as well as remote directories mounted on the server using the SMB/CIFS and NFS protocols.

All command examples listed in this document are valid for Linux operating systems.

IN THIS SECTION

General information on Kaspersky Anti-Virus.....	8
Obtaining information about Kaspersky Anti-Virus.....	13

GENERAL INFORMATION ON KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus 8.0 for Linux File Server (hereinafter Kaspersky Anti-Virus or the application) provides protection for servers running under Linux and FreeBSD operating systems against malware that penetrates the file system through a network connection or a removable device.

The application can:

- Scan file system objects located on the server's local drives, as well as shared and distributed resources accessed via the SMB/CIFS and NFS protocols.

File system objects can be scanned both in real-time or on demand.

- Detect infected and suspicious objects.

If an object is found to contain code from a known threat, Kaspersky Anti-Virus assigns it the *infected* status. If it is not possible to determine for sure whether or not an object is infected, it is classified as *suspicious*.

- Neutralize threats detected in files.

Depending on the type of threat, the application automatically selects the action required to neutralize it: disinfect infected object, move suspicious object to Quarantine, delete object or skip, i.e. leave object unchanged.

- Move suspicious objects to Quarantine.

Kaspersky Anti-Virus isolates objects, which it recognizes as suspicious. The application places such objects to quarantine, i.e., it moves them from their original location into a special storage, in which they are stored in encrypted form for security purposes. After every database update, Kaspersky Anti-Virus automatically runs a scan of objects in Quarantine. Some of them can be considered not infected and restored from Quarantine.

- Save backup copies of files before they are processed. Restore files from backup copies.
- Manage tasks and their settings.

The application provides four types of user-controllable tasks: real-time protection, on-demand scan, scan of objects in Quarantine, and update. The tasks of other types are system tasks and are not intended to be managed by the user.

- Notifies the administrator about events due to a change in the anti-virus protection status of the server and the general status of Kaspersky Anti-Virus.
- Uses Shell scripts to configure actions to be executed automatically as a result of certain events.
- Generate statistics and reports about operational results.
- Monitor the server's protection status through the SMTP protocol.
- Update anti-virus databases from Kaspersky Lab's update servers or from a user-specified source by schedule or on demand.

The databases are used to find and treat infected files. Based on the records they contain, each file is scanned for threats: the code of the file is matched against code that resembles a particular threat.

- Configure settings and control tasks both locally through the computer's standard operating system, or remotely from any computer in a local network or across the Internet.

Kaspersky Anti-Virus can be managed in several ways:

- through the command bar;
- by modifying the application's configuration file;
- through the Web Management Console;
- using the Kaspersky Administration Kit.

REAL-TIME PROTECTION AND ON-DEMAND SCAN

The following functions can be used to ensure server protection: *real-time protection* and *on-demand scan*.

Real-time protection

By default, the real-time protection task starts automatically along with Kaspersky Anti-Virus at the server startup and keeps on running continuously in the background mode. Kaspersky Anti-Virus scans files when they are accessed.

Kaspersky Anti-Virus checks files for various types of malware (see section "Programs detectable by Kaspersky Anti-Virus" on page [11](#)). When any application accesses a file on the server (for example, reads or writes it), Kaspersky Anti-Virus intercepts the operation on the file. It checks the file for the presence of malware using its databases (see section "About infected, suspicious objects and objects with the status "Warning" " on page [10](#)). If Kaspersky Anti-Virus detects a malicious program in the file, it will perform the actions you have specified for it, for example, it may attempt to disinfect the file or simply delete it. The program attempting to access the file may only do so if this file is not infected or has been successfully disinfected.

On-demand scan

On-demand scan involves one-time complete or selective scan of files on the server for the presence of threats.

PECULIARITIES IN SCANNING OF SYMBOLIC AND HARD LINKS

The following peculiarities in scanning of symbolic and hard links may be found during Kaspersky Anti-Virus scan.

Scanning symbolic links

Kaspersky Anti-Virus' Real time protection and on-demand scans only check symbolic links if the file that the symbolic link goes to is included in the scanned area.

If the file, which is accessed using a symbolic link, is not included in the protection area of the task, it will not be scanned by the application trying to access this file. If such file contains malicious code, server security will be at risk!

Scanning hard links

When Kaspersky Anti-Virus processes file which has more than one hard link, there are the following scenarios available depending on the action selected:

- If **Quarantine** (move to quarantine) is selected, the processed hard link will be moved to quarantine, and other hard links will not be processed;
- if the **Remove** action is selected, the processed hard link is removed, other hard links is processed;
- if the **Cure** action is selected – Kaspersky Anti-Virus either will disinfect the source file or it will replace the processed hard link by the clean copy of the source file. The created copy will have the name of the processed hard link.

When restoring the file from quarantine or backup, a copy of the source file is created with the name of the quarantined hard link (backup). Connections to other hard links are not restored.

ABOUT INFECTED, SUSPICIOUS OBJECTS AND OBJECTS WITH THE STATUS "WARNING"

Kaspersky Anti-Virus contains a set of databases. Databases are files containing records that are used to detect the malicious code of hundreds of thousands of known potential threats in objects being scanned. These records contain information about the control sections of the threats' code and algorithms used for disinfecting the objects in which these threats are contained.

If Kaspersky Anti-Virus detects (in an object being scanned) sections of code that fully match the control code sections of a threat based on the information provided in the databases, it will consider such object *infected*.

Kaspersky Anti-Virus will assign the status "Warning" to the detected object if it contains a section of code that partially coincides with a control code section from a known threat (in accordance with certain conditions). At the same time, a false alarm may occur.

Kaspersky Anti-Virus assigns the status *suspicious* to objects detected by its Heuristic Analyzer. The Heuristic Analyzer detects malicious objects based on their behavior. The code in such an object cannot be said to partially or completely match the code of a known threat, but it does contain instructions or sequences of instructions that are peculiar to threats.

ABOUT BACKUP AND QUARANTINE

Kaspersky Anti-Virus isolates found infected and suspicious objects to secure the protected server from their potential harmful effect.

Moving objects to quarantine

Kaspersky Anti-Virus quarantines detected infected and suspicious objects by moving them from the original location to the quarantine or backup storage directory. Objects are stored in the directory in encrypted format. Kaspersky Anti-Virus rescans quarantined objects after each update of Kaspersky Anti-Virus databases. Having scanned quarantined objects, Kaspersky Anti-Virus may recognize some of the objects as not infected. Other objects can be found infected by Kaspersky Anti-Virus.

If you suspect that a certain file may contain a threat while Kaspersky Anti-Virus recognizes it as clean, you can manually place such object in quarantine to check it later using updated databases.

Backup copying of objects before disinfection or deletion

Kaspersky Anti-Virus places in the quarantine or backup directory copies of infected and suspicious objects prior to disinfecting or deleting them. Such objects may be missing in the original location if they were deleted, or they may be stored in a modified form if Kaspersky Anti-Virus disinfecting them.

You can restore an object from the quarantine or backup directory at any moment to its original location or to any other directory specified on the server. You may need to restore an object, for example, if the original infected file contained valuable data but Kaspersky Anti-Virus could not preserve its integrity during disinfection and the information inside became unavailable.

Restoring infected or suspicious objects may lead to server infection.

PROGRAMS DETECTABLE BY KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus is capable of detecting hundreds of thousands of different programs that represent a threat to computer security, within the server's file system. Some of those programs impose great menace to the user, others are only dangerous when specific conditions are met. After Kaspersky Anti-Virus detects a malicious program in an object, it will assign it a certain category characterized by a certain severity level (high, medium, or low).

Kaspersky Anti-Virus distinguishes the following categories of malicious program:

- viruses and worms (Virware);
- Trojan programs (Trojware);
- other malicious software (Malware);
- pornographic software (Pornware);
- advertising software (Adware);
- potentially dangerous software (Riskware).

A brief description of the threats is provided below. For a more detailed description of malicious programs and their classification please visit the Kaspersky Lab Virus Encyclopedia (<http://www.viruslist.com/en/viruses/encyclopedia>).

Viruses and worms (Virware)

Danger level: high

This category includes classic viruses and network worms.

Classic viruses infect files of other programs or data. It adds its own code to such files in order to gain control when these files are being opened. Once a classic virus penetrates a system, it activates itself upon a certain event and performs its harmful operations.

Classic viruses differ depending on their environment and method they use for infecting other objects.

The term environment refers to areas of a computer, an operating system or an application, penetrated by the virus code. Based on the environment, file, boot, macro and script viruses are distinguished.

The term method of infection refers to various methods of implanting malicious code into the objects being infected. There are numerous types of viruses using various methods of infection. Overwriting viruses write their code over the code of the file being infected, thus erasing its content. The infected file stops working and cannot be restored. Parasitic viruses modify file code, leaving such files fully or partially operating. Companion viruses do not modify files, creating duplicates of them instead. When such infected file is launched, the control will be overtaken by its duplicate, which is the virus. There exist virus links as well as viruses infecting object modules (OBJ), compiler libraries (LIB), program source texts, etc.

The code of a network worm, after it penetrates the system, gets activated and performs its malicious action in a manner similar to that of the classic virus code. The network worm received its name due to its ability to tunnel from one computer to another - to send copies of itself through various information channels.

Propagation method is the main attribute used to differentiate between various types of network worms. Worms of various types can spread via email, instant messaging programs, IRC channels, file exchange networks, etc. Besides, there are network worms spreading their copies within network resources. Malicious programs infect operating systems exploiting their internal vulnerabilities and security breaches in applications running in those systems; they also penetrate public resources or may accompany other threats.

Many network worms spread at a very high rate.

In addition to the damage they inflict to the infected computer, network worms discredit the owner of such computer, cause additional charges for network traffic, and clutter up Internet channels.

Trojan programs (Trojware)

Danger level: high

Trojan programs (Trojan, Backdoor, Rootkit and other classes) perform the actions not authorized by the users of computers, for example, they steal passwords, access Internet resources, download and install other malicious programs.

Unlike worms and viruses, Trojan programs do not create copies of themselves penetrating files and infecting them. They sneak into a computer, for example, via e-mail or using a web browser when the user visits an "infected" website. Trojan programs are started with the user's participation. They begin performing their malicious actions right after they are started.

However, Trojans may inflict far greater damage as compared to a regular virus attack.

Backdoor programs are considered to be most dangerous among Trojans. Their functionality resembles that of remote administration utilities. They install themselves in a computer secretly from the users and enable intruders to control the infected computer remotely.

Another type of Trojan is the Rootkit. Like other Trojan programs, Rootkits permeate the system without the user's knowledge. Although they do not perform any malicious actions, they camouflage other malware and its activities and thus extend the existence of such programs in the infected system. Rootkits may hide files or processes in the memory of an infected computer and also conceal intruder's access to the system.

Other malicious software (Malware)

Danger level: medium

Other malicious programs do not impose any threat to the computer on which they are executed, yet they can be used to organize network attacks on remote computers, hack other computers, create other viruses or Trojans.

Malicious software belonging to this category is very diverse. Thus, it includes programs performing *network attacks* (DoS (Denial-of-Service) class), which send multiple requests to remote computers, which cause these servers to fail. *Hoaxes* (BadJoke, Hoax types) alarm users with virus-like messages: they can "detect" a virus in a clean file or display a message about disk formatting, which will not take place in effect. *Encrypting programs* (FileCryptor, PolyCryptor classes) encrypt other malicious programs to prevent them from being detected during an anti-virus scan. *Constructors* (Constructor class) allow to generate original texts of viruses, object modules, or infected files. *Spam utilities* (SpamTool class) collect email addresses on an infected computer or turn such computer into a spam-sending machine.

Pornographic software (Pornware)

Danger level: medium

Pornographic programs are included in a "not-a-virus" class of programs. They have functions, which may inflict damage to the user only if special conditions are met.

Such programs are concerned with the display of pornographic information to the user. Depending on the behavior of the programs, three types are distinguished: automatic dialers (Porn-Dialer), downloaders (Porn-Downloader), and tools (Porn-Tool). Porn dialers connect to pay-per-visit pornographic Internet resources using a modem, pornographic downloaders download pornography to the user's computer. Pornographic tools are programs related to the search and display of pornographic materials (for example, special toolbars for browsers or special video players).

Advertising software (Adware)

Danger level: medium

Adware programs are included in a "not-a-virus" class. They are built-in into other programs without the user's knowledge to display advertising messages in their interface. In many cases adware programs, in addition to displaying advertising messages, gather users' personal information and send it to their developer, change browser's settings (browser home page, search page, security levels, etc.) and create traffic that is not controlled by the user. In addition to the violation of security rules, activities of adware may cause direct financial losses.

Riskware

Danger level: low

Potentially dangerous applications are included in a "not-a-virus" class of programs. Such programs may be legally purchased and used in daily operations by the users, for example, system administrators.

Some remote management programs, such as Remote Administrator, and programs for obtaining network information are considered potentially dangerous.

OBTAINING INFORMATION ABOUT KASPERSKY ANTI-VIRUS

Kaspersky Lab provides various sources of information about Kaspersky Anti-Virus. Select a source most convenient for you depending on the importance and urgency of your question.

If you have already purchased Kaspersky Anti-Virus, you can contact the Technical Support service. If your question does not require an immediate answer, you can discuss it with the Kaspersky Lab experts and other users in our forum at <http://forum.kaspersky.com>.

SOURCES OF INFORMATION FOR FURTHER RESEARCH

The following sources of information about Kaspersky Anti-Virus are available:

- Kaspersky Anti-Virus page at the Kaspersky Lab website;
- documentation;
- manual pages.

Page at the Kaspersky Lab website

<http://www.kaspersky.com/anti-virus-linux-file-server>

This page contains general information about the application, its functionality and peculiarities. You can purchase Kaspersky Anti-Virus or extend the period of its use in our online store.

Documentation

Installation Guide describes the purpose of Kaspersky Anti-Virus, requirements to the hardware and software for the installation and operation of Kaspersky Anti-Virus, instructions for its installation, verification of its operability and initial setup.

Administrator's Guide contains information about how to manage Kaspersky Anti-Virus using the command line utility, Kaspersky Web Management Console and Kaspersky Administration Kit.

These documents are supplied in PDF format in Kaspersky Anti-Virus distribution package. Alternatively, you can download the documentation files from the Kaspersky Anti-Virus page at Kaspersky Lab's website.

Manual pages

You can review the following manual pages files to obtain information about Kaspersky Anti-Virus:

- managing Kaspersky Anti-Virus from the command line:
 - for Linux – `/opt/kaspersky/kav4fs/share/man/man1/kav4fs-control.1.gz`,
 - for FreeBSD – `/usr/local/man/man1/kav4fs-control.1.gz`;
- configuring general settings for Kaspersky Anti-Virus:
 - for Linux – `/opt/kaspersky/kav4fs/share/man/man5/kav4fs.conf.5.gz`,
 - for FreeBSD – `/usr/local/man/man5/kav4fs.conf.5.gz`;
- configuring the real-time protection task:
 - for Linux – `/opt/kaspersky/kav4fs/share/man/man5/kav4fs-oas.conf.5.gz`,
 - for FreeBSD – `/usr/local/man/man5/kav4fs-oas.conf.5.gz`;
- configuring on-demand scan tasks:
 - for Linux – `/opt/kaspersky/kav4fs/share/man/man5/kav4fs-ods.conf.5.gz`,
 - for FreeBSD – `/usr/local/man/man5/kav4fs-ods.conf.5.gz`;
- configuring update tasks:
 - for Linux – `/opt/kaspersky/kav4fs/share/man/man5/kav4fs-update.conf.5.gz`,
 - for FreeBSD – `/usr/local/man/man5/kav4fs-update.conf.5.gz`;
- configuring the storage of quarantined objects and the storage of objects backed up before disinfection or removal:
 - for Linux – `/opt/kaspersky/kav4fs/share/man/man5/kav4fs-quarantine.conf.5.gz`,
 - for FreeBSD – `/usr/local/man/man5/kav4fs-quarantine.conf.5.gz`;
- configuring notifications:
 - for Linux – `/opt/kaspersky/kav4fs/share/man/man5/kav4fs-notifier.conf.5.gz`,
 - for FreeBSD – `/usr/local/man/man5/kav4fs-notifier.conf.5.gz`;
- configuring SNMP-Agent:

- for Linux – */opt/kaspersky/kav4fs/share/man/man5/kav4fs-snmp.conf.5.gz*;
- for FreeBSD – */usr/local/man/man5/kav4fs-snmp.conf.5.gz*;
- configuring the event repository:
 - for Linux – */opt/kaspersky/kav4fs/share/man/man5/kav4fs-events.conf.5.gz*;
 - for FreeBSD – */usr/local/man/man5/kav4fs-events.conf.5.gz*;
- description of utility which changes the Web Management Console's user password:
 - for Linux – */opt/kaspersky/kav4fs/share/man/man1/kav4fs-wmconsole-passwd.1.gz*;
 - for FreeBSD – */usr/local/man/man1/kav4fs-wmconsole-passwd.1.gz*;
- description of utility which changes settings for connection with the Kaspersky Administration Kit Administration Server:
 - for Linux – */opt/kaspersky/klagent/share/man/man1/klmover.1.gz*;
- description of utility which checks settings for connection with the Kaspersky Administration Kit Administration Server:
 - for Linux – */opt/kaspersky/klagent/share/man/man1/klmagchk.1.gz*.

CONTACTING THE TECHNICAL SUPPORT SERVICE

If you have already purchased Kaspersky Anti-Virus, you can obtain information about it from the Technical Support Service by telephone or online.

Before contacting the Technical Support service, please read the Support rules for Kaspersky Lab's products (<http://support.kaspersky.com/support/rules>).

Email request to the Technical Support Service

You can ask your question to the Technical Support Service specialists by filling out the web form of Request to Kaspersky Lab Technical Support at <http://support.kaspersky.com/helpdesk.html>.

You can send your inquiry in Russian, English, German, French or Spanish.

In order to send an email message with your question, you must indicate the **client number** obtained from the Technical Support website during registration along with your **password**.

If you are not yet a registered user of Kaspersky Lab applications, you can fill out a registration form (<https://support.kaspersky.com/ru/personalcabinet/Registration/Form/?LANG=en>). During registration, specify the key file name.

The Technical Support service will reply to your request in your Personal Cabinet (<https://support.kaspersky.com/en/PersonalCabinet>) and to the email address you have specified in your request.

Describe the problem you have encountered in the request web form providing as much detail as possible. Specify the following information in the mandatory fields:

- **Request type.** Select the topic, which is the closest to the problem you have encountered, e.g.: "Product installation / removal problem", or "Virus scan / removal problem".
- **Kaspersky Anti-Virus version name and number.**

- **Request text.** Describe in detail the problem encountered.
- **Customer ID and password.** Enter the customer ID and password received during registration at the Technical Support Service website.
- **Email address.** The experts of the Technical Support Service will send their reply to your inquiry to that address.

Technical support by phone

If an urgent problem has occurred, you can always call the Technical Support Service in your city. When you apply to Russian-speaking (http://support.kaspersky.ru/support/support_local) or international (<http://support.kaspersky.ru/support/international>) Technical Support specialists, please remember to provide the Kaspersky Anti-Virus information (<http://support.kaspersky.ru/support/details>), so that our specialists could help you as soon as possible.

DISCUSSION OF KASPERSKY LAB'S APPLICATIONS IN WEB FORUM

If your question does not require an urgent answer, you can discuss it with Kaspersky Lab's specialists and other users in our forum located at <http://forum.kaspersky.com>.

In this forum you can view existing topics, leave your comments, create new topics and use the search engine.

WORKING WITH KASPERSKY WEB MANAGEMENT CONSOLE

Kaspersky Web Management Console (hereinafter also referred to as the Web Management Console) is a tool for managing Kaspersky Anti-Virus using a web browser.

You can perform the following actions through the Web Management Console:

- Display the operational and protection status of the server running Kaspersky Anti-Virus, and generate corresponding reports
- Manage and configure Kaspersky Anti-Virus

The Web Management Console is included in the distribution package of Kaspersky Anti-Virus. For more details about starting and configuring the Web Management Console see *Kaspersky Anti-Virus 8.0 for Linux File Server. Installation Guide*.

The **admin** account is used for access to the Kaspersky Web Management Console. The password for this account is specified during initial configuration of Kaspersky Anti-Virus. This account may be used for simultaneous access to the Web Management Console from multiple computers.

If two users open the web console window on different computers at the same time and modify the same parameter of Kaspersky Anti-Virus, the product will apply the parameter value saved last.

LAUNCHING THE WEB MANAGEMENT CONSOLE

You can launch the Web Management Console in the browser on a protected computer or another computer located in the same network segment with the server and compliant with the hardware and software requirements.

➤ *To open the Kaspersky Anti-Virus web console, perform the following steps:*

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

`http://<IP address or domain name of the protected server>:9080`

2. On the **Logon** page enter the Web Management Console user password and press **Log on**.

At the first Web Management Console logon you should enter the user password defined during initial configuration of Kaspersky Anti-Virus.

If you have not specified a password for access to the Web Management Console during the Kaspersky Anti-Virus initial configuration, you can do it using the `/opt/kaspersky/kav4fs/bin/kav4fs-wmconsole-passwd` utility.

CHANGING THE USER PASSWORD FOR THE WEB MANAGEMENT CONSOLE

Default settings of the account used to access the Web Management Console are as follows:

- User name – **admin**.
- Password for this account is specified during initial configuration of Kaspersky Anti-Virus.

You can change the user password, if necessary.

➤ *To edit the Web Management Console user password, perform the following steps:*

1. In the left part of Kaspersky Anti-Virus web console, select the **General settings** section.
2. In the **Current password** field enter the user password used at present.
3. In the **New password** field define the new user password and re-enter it in the **Confirm new password** field.
4. Press the **Change password** button.

STARTING AND STOPPING KASPERSKY ANTI-VIRUS

Before taking the actions or using the commands described above, make sure that the `kav4fs-supervisor` service is running on the computer!

By default, Kaspersky Anti-Virus starts automatically at the operating system startup (on default runlevels for each operating system). Kaspersky Anti-Virus launches all predefined and custom tasks scheduled to run according to the PS start rule (see page [142](#)).

If you stop the Kaspersky Anti-Virus, execution of all tasks will be interrupted. After Kaspersky Anti-Virus restart, interrupted custom tasks will not be resumed automatically. Only the custom tasks scheduled to run according to the PS start rule (see page [142](#)) will be launched again.

➤ To start *Kaspersky Anti-Virus*, execute the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --start-app
```

➤ To pause *Kaspersky Anti-Virus*, execute the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --stop-app
```

➤ To restart *Kaspersky Anti-Virus*, execute the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --restart-app
```

MANAGING THE TASKS IN KASPERSKY ANTI-VIRUS

Task is a Kaspersky Anti-Virus component, implementing part of the program functionality. For example, the real-time protection task implements protection of the files in real time, the update task downloads and installs Kaspersky Anti-Virus database updates, etc.

➤ To list Kaspersky Anti-Virus tasks, execute the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --get-task-list
```

The user can manage the following types of tasks (see page [20](#)):

- **OAS**, real-time protection tasks;
- **ODS**, on-demand scan tasks;
- **QS**, tasks which scan quarantined objects;
- **Update**, update tasks.

The tasks of other types are system tasks and are not intended to be managed by the user. You can only modify their operation settings.

IN THIS SECTION

Creating an on-demand scan or update task	19
Deleting an on-demand scan or update task.....	20
Manual task management.....	20
Automatic task management.....	20
Viewing task state	21
Viewing task statistics	22

CREATING AN ON-DEMAND SCAN OR UPDATE TASK

The Kaspersky Anti-Virus installation creates one task of each type. You can create custom on-demand scan and update tasks.

➤ To create an on-demand scan task, execute the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--create-task <task name> --use-task-type=ODS
```

The settings for the created task are as follows:

- All local and mounted objects will be scanned.

- The scan's security level will be **Recommended** (see page [43](#)).

You can create an on-demand scan task with the required set of parameters. To do that, specify the full path to the file containing the task settings, using the `--file` key of the `--create-task` command.

- *To create an update task, execute the following command:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--create-task <task name> --use-task-type=Update \
--file=<path to the file containing the task settings>
```

The update task will be created successfully, only if the path to the file containing the task settings was specified.

DELETING AN ON-DEMAND SCAN OR UPDATE TASK

You can delete update tasks and on-demand scan tasks (except **Quarantine scan** (ID=10) and **On-Demand Scan** (ID=9) tasks).

You cannot delete the real-time protection task.

- *To delete the task, execute the following command:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --delete-task <task ID>
```

MANUAL TASK MANAGEMENT

The actions described in this section are available for the OAS, ODS, QS, and Update task types.

You can pause and resume any task except for update tasks.

You can run several on-demand scan tasks simultaneously.

- *To start a task, execute the following command:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --start-task <task ID>
```

- *To stop a task, execute the following command:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --stop-task <task ID>
```

- *To pause a task, execute the following command:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --suspend-task <task ID>
```

- *To resume a task, execute the following command:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --resume-task <task ID>
```

AUTOMATIC TASK MANAGEMENT

In addition to managing Kaspersky Anti-Virus tasks manually, you can use automatic task management. To do so, create a task schedule.

Task schedule is a set of rules that define the task start time, pause time and stop time.

The following types of tasks support automatic management:

- Real-time protection tasks support start, stop and pause rules.
- On-demand scan tasks support start, stop and pause rules.
- Database updates – start rules only are available for this type of task.

➡ *To configure task schedule using the configuration file:*

1. Save the real-time protection task settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --get-schedule <task ID> \  
--file=<full path to the file>
```

2. Assign the value **yes** to the **Enabled** setting.
3. Configure the schedule settings (see page [141](#)).
4. Import the schedule settings into the task:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --set-schedule <task ID> \  
--file=<full path to the file>
```

VIEWING TASK STATE

One of the aspects of task management is monitoring the task state.

Kaspersky Anti-Virus tasks may have one of the following states:

- **Started** – the task is in progress;
- **Starting** – the task is starting;
- **Stopped** – the task is stopped;
- **Stopping** – the task is stopping;
- **Suspended** – the task is suspended;
- **Suspending** – the task is suspending;
- **Resumed** – the task has been resumed;
- **Resuming** – the task is resuming;
- **Failed** – the task has terminated with an error;
- **Interrupted by user** – the task execution was interrupted by the user.

➡ *To view the task state, execute the following command:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --get-task-state <task ID>
```

Example of command output:

Name: On-demand scan

Id: 9

Class: ODS

State: Stopped

VIEWING TASK STATISTICS

You can obtain the operating statistics for Kaspersky Anti-Virus tasks. Viewing statistics is available for the following task types:

- **Application** – general operating statistics for Kaspersky Anti-Virus.
- **Quarantine** – quarantine statistics.
- **OAS** – statistics for the real-time protection task.
- **ODS** – statistics for the on-demand scan tasks.
- **Backup** – backup storage statistics.
- **Update** – statistics for update tasks.

For the ODS and Update task types, it is necessary to specify the task ID. If the task ID is not specified, general statistics for the selected task type will be provided.

➤ *To view task statistics, execute the following command:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-stat <task type> [--task-id <task ID>]
```

You can specify the period, for which statistics is displayed.

The date and time of the beginning and end of the period are specified in format [YYYY-MM-DD] [HH24:MI:SS].

➤ *To obtain statistics for a specific period, execute the following command:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-stat <task type> \  
--from=<beginning of period> --to=<end of period>
```

If the value of the <beginning of period> setting is not specified, statistics will be collected since the task start. If the value of the <end of period> setting is not specified, statistics will be collected until the present moment.

You can save task statistics to files in two formats: HTML and CSV. By default, the file format is set by the file extension.

➤ *To save statistics to a file, execute the following command:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-stat <task type> [--task-id <task ID>] \  
--export-report=<full path to the file>
```

UPDATING KASPERSKY ANTI-VIRUS

During the license period you can download updates for the databases of Kaspersky Anti-Virus.

Databases are files containing records that are used to detect the malicious code of known threats in scanned objects. These records contain information about the control sections of the threats' code and algorithms used for disinfecting the objects in which these threats are contained.

Virus analysts at Kaspersky Lab detect hundreds of new threats daily, create records to identify them, and include them in database updates. *Database updates* are one or several files, which contain records identifying threats that have been detected since the previous update had been released. To minimize the risk of infecting the server, we recommend that you receive database updates regularly.

Kaspersky Lab can release Anti-Virus module update packages. Update packages are classified as urgent (or critical) or routine. Urgent update packages remove vulnerabilities and fix errors; routine updates add new functions or improve existing ones.

Within the validity period of your license you can download updates from the web site of Kaspersky Lab and install them manually.

You can also automatically set module updates for other Kaspersky Lab applications.

Database updates

During installation Kaspersky Anti-Virus has retrieved the current databases from an Kaspersky Lab's HTTP server; if you have configured automatic database update, Kaspersky Anti-Virus starts the update according to the schedule (once every 30 minutes) using the predefined update task (ID=6).

You can configure the preinstalled update task and create user-defined update tasks.

If update downloading is interrupted or terminates with an error, Kaspersky Anti-Virus automatically switches to using databases with previously installed update. If Kaspersky Anti-Virus databases get corrupted, you can roll them back to the previously installed updates.

By default, if Kaspersky Anti-Virus databases have not been updated for a week since the moment when Kaspersky Lab had released the last installed updates, the Anti-Virus logs the event *Databases are outdated* (AVBasesAreOutOfDate). If the databases have not been updated within two weeks, it registers the event *Databases are obsolete* (AVBasesAreTotallyOutOfDate).

Copying database and module updates. Distributing updates

You can download updates to each protected computer or use one computer as an intermediary by copying all updates onto it and then distributing them to the computers. And if you use Kaspersky Administration Kit application for the centralized administration of computer protection in an enterprise, you can use Kaspersky Administration Kit administration server as an intermediary for updates distribution.

To save database updates on an intermediary computer without applying them, configure *updates distribution* in the update task.

IN THIS SECTION

Selecting an update source	24
Updating from local or network folder	24

Using the proxy server [26](#)

Last database update rollback [26](#)

SELECTING AN UPDATE SOURCE

Update source (see page [172](#)) is a resource containing updates for Anti-Virus databases. Update sources can be HTTP or FTP servers, or local or network folders.

The main updates 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.

➤ *To select Kaspersky Lab's update servers as your update source,, execute the following command:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--set-settings <update task ID> \  
CommonSettings.SourceType=KLServers
```

➤ *To select Kaspersky Administration Kit server as an update source, execute the following command:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--set-settings <update task ID> \  
CommonSettings.SourceType=AKServer
```

To reduce Internet traffic, you can configure Anti-Virus database update from the local or network folder (see page [24](#)).

UPDATING FROM LOCAL OR NETWORK FOLDER

The procedure of retrieving updates from a local folder is arranged as follows:

1. One of the computers on the network retrieves the Anti-Virus update package from Kaspersky Lab's update servers, or from a mirror server hosting a current set of updates. The retrieved updates are placed in a shared folder.
2. Other computers on the network access the shared folder to retrieve Anti-Virus database updates.

➤ *To download updates for Kaspersky Anti-Virus databases to a shared folder on one of the network computers, perform the following steps:*

1. Create a folder, to which Kaspersky Anti-Virus will download database updates.
2. Provide shared access to the created folder.
3. Create a configuration file that contains the following setting values:

```
UpdateType="RetranslateProductComponents"  
[CommonSettings]  
SourceType="KLServers"  
UseKLServersWhenUnavailable=yes  
UseProxyForKLServers=no  
UseProxyForCustomSources=no  
PreferredCountry=""  
ProxyServer=""
```



```
ProxyPort=3128
ProxyBypassLocalAddresses=yes
ProxyAuthType="NotRequired"
ProxyAuthUser=""
ProxyAuthPassword=""
UseFtpPassiveMode=yes
ConnectionTimeout=10
[UpdateComponentsSettings]
Action="DownloadAndApply"
[RetranslateUpdatesSettings]
RetranslationFolder="<full path to the created directory>"
```

4. Import the settings from configuration file into the task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings <update task ID> \
--file=<full path to the file>
```

5. Start the task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --start-task <update task ID>
```

Kaspersky Anti-Virus databases will be downloaded to the shared folder.

➤ *To specify the shared folder as an update source for other network computers, perform the following steps:*

1. Create a configuration file that contains the following setting values:

```
UpdateType="AllBases"
[CommonSettings]
SourceType="Custom"
UseKLServersWhenUnavailable=yes
UseProxyForKLServers=no
UseProxyForCustomSources=no
PreferredCountry=""
ProxyServer=""
ProxyPort=3128
ProxyBypassLocalAddresses=yes
ProxyAuthType="NotRequired"
ProxyAuthUser=""
ProxyAuthPassword=""
UseFtpPassiveMode=yes
ConnectionTimeout=10
[CommonSettings:CustomSources]
Url="/home/bases"
Enabled=yes
[UpdateComponentsSettings]
Action="DownloadAndApply"
```

2. Import the settings from configuration file into the task using the following command:

```

/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings <update task ID> \
--file=<full path to the file>

```

USING THE PROXY SERVER

If you use a proxy server to connect to the Internet, you must configure its settings.

- *To enable using a proxy server to access Kaspersky Lab's update servers,, execute the following command:*

```

/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings <update task ID> \
CommonSettings.UseProxyForKLServers=yes \
CommonSettings.ProxyBypassLocalAddresses=yes \
CommonSettings.ProxyServer=proxy.company.com \
CommonSettings.ProxyPort=3128

```

- *To enable using a proxy server to access custom update sources, execute the following command:*

```

/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings <update task ID> \
CommonSettings.UseProxyForCustomSources=yes \
CommonSettings.ProxyBypassLocalAddresses=yes \
CommonSettings.ProxyServer=proxy.company.com \
CommonSettings.ProxyPort=3128

```

- *To specify authentication settings for connection to the proxy server, execute the following command:*

```

/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings <update task ID> \
CommonSettings.ProxyAuthType=Plain \
CommonSettings.ProxyAuthUser=user \
CommonSettings.ProxyAuthPassword=password

```

LAST DATABASE UPDATE ROLLBACK

Before applying the database updates, Anti-Virus creates backup copies of the previous databases. If an update procedure gets interrupted or fails, Anti-Virus automatically reverts to the previous database version containing updates installed earlier.

If you encounter problems after database update, you can roll back the databases to the previous version. To do this, use the roll back to the previous databases task.

- *To roll back to the previous databases, execute the following command:*

```

/opt/kaspersky/kav4fs/bin/kav4fs-control --start-task 14

```

REAL-TIME PROTECTION

The real-time protection task prevents infection of the computer's file system. By default, the real-time protection task runs automatically at the start of Kaspersky Anti-Virus. The task runs in the computer's RAM, scanning all files that are opened, saved, or executed. You can stop, start, pause and resume it.

You cannot create custom real-time protection tasks.

IN THIS SECTION

The structure of predefined security levels in the real-time protection task	27
Creating a protection scope	30
Restricting a protection area using masks and regular expressions	31
Exclusion of objects from a protection area.....	32
Selecting interception mode	35
Selecting protection mode.....	35
Using heuristic analysis.....	36
Using scan mode depending on user and group accounts accessing the objects	36
Selecting actions to perform on detected objects.....	37
Selecting actions depending on the threat type.....	38
Scan optimization.....	39
Compatibility with other Kaspersky Lab's applications	40

THE STRUCTURE OF PREDEFINED SECURITY LEVELS IN THE REAL-TIME PROTECTION TASK

Kaspersky Lab specialists distinguish three security levels. The decision of which level to select must be taken on your own based on the operation conditions and the current situation. You will be invited to select one of the following security levels:

- **Low**

The **Low** security level can be selected on a server if the network has other computer security tools besides Anti-Virus on servers and workstations, for example, firewalls are configured and security policies are established for the network users.

The following settings will be applied at the **Low** security level during the scan:

```
[ScanScope:ScanSettings]
```

```
ScanArchived=no
```

```
ScanSfxArchived=no
```

```

ScanMailBases=no
ScanPlainMail=no
ScanPacked=yes
UseTimeLimit=yes
TimeLimit=60
UseSizeLimit=yes
SizeLimit=8388608
ScanByAccessType="SmartCheck"
InfectedFirstAction="Cure"
InfectedSecondAction="Remove"
SuspiciousFirstAction="Quarantine"
SuspiciousSecondAction="Skip"
UseAdvancedActions=yes
UseExcludeMasks=no
UseExcludeThreats=no
ReportCleanObjects=no
ReportPackedObjects=no
UseAnalyzer=yes
HeuristicLevel="Light"
[ScanScope:ScanSettings:AdvancedActions]
Verdict="Riskware"
FirstAction="Skip"
SecondAction="Skip"

```

- **Recommended**

The **Recommended** security level is set by default. Experts of Kaspersky Lab deem it sufficient for protection of file servers in most networks. The level provides an optimal combination of protection and the load on protected servers.

The following settings will be applied at the **Recommended** security level during the scan:

```

[ScanScope:ScanSettings]
ScanArchived=no
ScanSfxArchived=no
ScanMailBases=no
ScanPlainMail=no

```

```

ScanPacked=yes
UseTimeLimit=yes
TimeLimit=60
UseSizeLimit=no
SizeLimit=8388608
ScanByAccessType="SmartCheck"
InfectedFirstAction="Recommended"
InfectedSecondAction="Skip"
SuspiciousFirstAction="Recommended"
SuspiciousSecondAction="Skip"
UseAdvancedActions=yes
UseExcludeMasks=no
UseExcludeThreats=no
ReportCleanObjects=no
ReportPackedObjects=no
UseAnalyzer=yes
HeuristicLevel="Light"
[ScanScope:ScanSettings:AdvancedActions]
Verdict="Riskware"
FirstAction="Skip"
SecondAction="Skip"

```

- **High**

Use the **High** security level if you have high requirements to the security of your computer network.

The following settings will be applied at the **High** security level during the scan:

```

[ScanScope:ScanSettings]
ScanArchived=no
ScanSfxArchived=yes
ScanMailBases=no
ScanPlainMail=no
ScanPacked=yes
UseTimeLimit=yes
TimeLimit=60

```

```

UseSizeLimit=no

SizeLimit=8388608

ScanByAccessType="SmartCheck"

InfectedFirstAction="Cure"

InfectedSecondAction="Remove"

SuspiciousFirstAction="Quarantine"

SuspiciousSecondAction="Skip"

UseAdvancedActions=yes

UseExcludeMasks=no

UseExcludeThreats=no

ReportCleanObjects=no

ReportPackedObjects=no

UseAnalyzer=yes

HeuristicLevel="Light"

[ScanScope:ScanSettings:AdvancedActions]

Verdict="Riskware"

FirstAction="Skip"

SecondAction="Skip"

```

CREATING A PROTECTION SCOPE

Note the peculiarities (see page [9](#)) in scanning of symbolic and hard links.

By default, the real-time protection task scans all files that are opened, modified, and saved within the local server file system.

You can extend or narrow down the protection area by adding or removing objects to be scanned, or by changing the type of files to be scanned (see page [31](#)).

Kaspersky Anti-Virus will scan objects in the specified areas in the order, in which they are listed in the configuration file or in its Web Management Console. If you wish to specify the security settings of the subdirectory to be different from the security settings of the parent directory, place the subdirectory in the list higher, than its parent directory.

➤ *To extend a protected area, perform the following steps:*

1. Save the real-time protection task settings to a file using the following command:

```

/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-settings 8 --file=<full path to the file>

```

2. Add the following sections to the created file:

- [ScanScope] which contains the following settings:
 - **AreaMask** which defines the name mask of objects to be scanned;
 - **UseAccessUser** which enables the scan mode depending on user and group accounts accessing the objects (see page [36](#));
 - **AreaDesc** which defines the name of protection area.
- [ScanScope:AreaPath] which contains the **Path** setting.
- [ScanScope:AccessUser] which contains settings that define accounts whose file operations will be intercepted by the real-time protection task.
- [ScanScope:ScanSettings] which contains scan settings for the area to be added.

All settings must be assigned in the [ScanScope:ScanSettings] section.

3. Import settings from file to the real-time protection task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--set-settings 8 --file=<full path to the file>
```

➡ To narrow down a protected area, perform the following steps:

1. Save the protection task settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-settings 8 --file=<full path to the file>
```

2. Delete from the created file the following sections, defining protection area:

- [ScanScope];
- [ScanScope:AreaPath];
- [ScanScope:AccessUser];
- [ScanScope:ScanSettings].

3. Import settings from file to the real-time protection task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--set-settings 8 --file=<full path to the file>
```

RESTRICTING A PROTECTION AREA USING MASKS AND REGULAR EXPRESSIONS

By default, Kaspersky Anti-Virus scans all objects within a protected area.

You can specify templates for the names or paths of the files to scan. In this case, Kaspersky Anti-Virus will only scan files or directories from the protected area that are specified using Shell masks or POSIX extended regular expressions.

Using Shell masks, you can specify the file name template to scan by Kaspersky Anti-Virus.

Using extended regular expressions, you can specify the file path template to scan by Kaspersky Anti-Virus. A regular expression cannot contain the name of the folder which defines the scan or protection area.

➤ To specify file name or path templates for the files to be scanned, perform the following steps:

1. Save real-time protection task settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-settings 8 --file=<full path to the file>
```

2. Specify the value of the **AreaMask** setting in the [ScanScope] section which defines the protection area.

3. Import settings from file to the real-time protection task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--set-settings 8 --file=<full path to the file>
```

EXCLUSION OF OBJECTS FROM A PROTECTION AREA

By default, the real-time protection task scans all objects that are included in protection areas defined for this task.

You can exclude several objects from the scan. To do that, you can create four types of exclusions:

- exclusion of objects from a protection area: in this case the specified objects will only be excluded from the selected protected area;
- global exclusion of objects: in this case the specified objects will be excluded from all protection areas defined for the task;
- exclusion of objects depending on user and group accounts accessing the objects: in this case the objects will be excluded from the protection area when they are accessed by specific accounts;
- exclusion of objects by the name of the threat detected in them.

IN THIS SECTION

Creating a global exclusion area	32
Excluding objects from the protection area	33
Exclusion of objects depending on user and group accounts accessing the objects	34
Excluding objects by names of the threats detected in them.....	34

CREATING A GLOBAL EXCLUSION AREA

You can create a global exclusion area. Objects included in this area will be excluded from all areas defined for the real-time protection task.

➤ To create a global exclusion area, perform the following steps:

1. Save the real-time protection task settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-settings 8 --file=<full path to the file>
```


2. Add the following sections to the created file:

- [ExcludedFromScanScope], which contains the following settings:
 - **AreaMask**, which defines templates of object names to be excluded from the scan;
 - **UseAccessUser**, which enables the exclusion mode depending on user and group accounts accessing the objects;
 - **AreaDesc**, which defines a unique name for exclusion area;
- [ExcludedFromScanScope:AreaPath], which contains the **Path** setting that defines the path to the objects to be excluded from the scan.
- [ExcludedFromScanScope:AccessUser], which contains settings that define accounts whose file operations will be excluded from the scan.

3. Import settings from file to the real-time protection task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--set-settings 8 --file=<full path to the file>
```

EXCLUDING OBJECTS FROM THE PROTECTION AREA

By default, Kaspersky Anti-Virus scans all objects within a protected area.

You can define name and path templates that are excluded from the protection area. In this case, Kaspersky Anti-Virus will not scan files or directories from the protection area that are specified using Shell masks or POSIX extended regular expressions.

You can use Shell masks to specify a file name template excluded from scanning by Kaspersky Anti-Virus.

You can also use extended regular expressions to specify a template for the paths to files which Kaspersky Anti-Virus should not scan. The regular expression should not contain the name of the directory containing excluded object.

➤ *To exclude objects from the protection area, perform the following steps:*

1. Save the real-time protection task settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-settings 8 --file=<full path to the file>
```

2. Open the created file for editing.

3. Assign the value **yes** to the **UseExcludeMasks** setting in the [ScanScope:ScanSettings] section.

4. Specify file name or path templates using the **ExcludeMasks** setting in the [ScanScope:ScanSettings] section.

To specify several file name or path templates, repeat the **ExcludeMasks** setting value the required number of times.

5. Import settings from file to the real-time protection task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--set-settings 8 --file=<full path to the file>
```

EXCLUSION OF OBJECTS DEPENDING ON USER AND GROUP ACCOUNTS ACCESSING THE OBJECTS

Kaspersky Anti-Virus allows excluding of objects from the protection area if they are accessed by applications running under the specified user or group accounts.

➤ *To exclude objects from the protection area depending on user and group accounts accessing the objects, perform the following steps:*

1. Save the real-time protection task settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-settings 8 --file=<full path to the file>
```

2. Open the created file for editing.
3. Assign the value **yes** to the **UseAccessUser** setting in the [ExcludedFromScanScope] section;
4. Specify the user name, under which file operations will not be scanned, using the **UserName** setting in the [ExcludedFromScanScope:AccessUser] section;
5. Specify the group name, under which file operations will not be scanned, using the **UserGroup** setting in the [ExcludedFromScanScope:AccessUser] section.

If you wish to specify several user names or group names, specify values for the **UserName** and **UserGroup** settings the required number of times in one section.

6. Import settings from file to the real-time protection task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--set-settings 8 --file=<full path to the file>
```

EXCLUDING OBJECTS BY NAMES OF THE THREATS DETECTED IN THEM

If Kaspersky Anti-Virus considers a scanned object to be infected or suspicious, it performs the action on this object specified in the task. If you consider this object to be harmless for the protected computer, you can exclude it from the scan scope by the name of threat detected in it. In this case Kaspersky Anti-Virus considers such objects as not infected and does not scan them.

The full name of the threat may contain the following information:

<threat class>:<threat type>.<brief name of operating system>.<threat name>.<threat modification code>. For example, **not-a-virus:NetTool.Linux.SynScan.a**.

You can find the full name of the threat detected in an object in the Kaspersky Anti-Virus log.

You can also find the full name of the threat detected in a software product at the Virus Encyclopedia web site (see the Virus Encyclopedia section at <http://www.viruslist.com>). To find the type of a threat, enter the name of the product in the **Search** field.

When specifying threat name templates, you can use Shell masks and POSIX extended regular expressions.

➤ *To exclude objects by the name of detected threat, perform the following steps:*

1. Save the real-time protection task settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-settings 8 --file=<full path to the file>
```

2. Open the created file for editing.
3. Assign the value **yes** to the **UseExcludeThreats** setting in the [ScanScope:ScanSettings] section.
4. Specify the threat name template using the **ExcludeThreats** setting in the [ScanScope:ScanSettings] section.

To specify several threat name templates, repeat the **ExcludeThreats** setting value the required number of times.

5. Import settings from file to the real-time protection task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 8 --file=<full path to the file>
```

SELECTING INTERCEPTION MODE

Kaspersky Anti-Virus includes two components intercepting attempts to access files and scanning those files. They are Samba interceptor (used to scan objects on remote computers accessed via the SMB / CIFS protocol) and the kernel level interceptor (scanning objects accessed using other methods).

The Samba interceptor provides, as additional object information, the IP address of the remote computer on which an application attempted to access an object when it was intercepted by Kaspersky Anti-Virus.

- *To enable the kernel level interceptor, execute the following command:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 8 ProtectionType=KernelOnly
```

- *To enable a Samba interceptor, execute the following command:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 8 ProtectionType=SambaOnly
```

- *To enable both interceptors, execute the following command:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 8 ProtectionType=Full
```

If the Samba interceptor is enabled, Kaspersky Anti-Virus will not scan objects that are not accessed using SMB / CIFS.

SELECTING PROTECTION MODE

Protection mode (see page [167](#)) is the condition which triggers the real-time protection task. By default, Kaspersky Anti-Virus uses smart mode, which determines whether the object is to be scanned based on the actions performed on it. For example, when working with a Microsoft Office document, Kaspersky Anti-Virus scans the file when it is first opened and last closed. Intermediate operations that overwrite the file do not cause it to be scanned.

- *To change the object protection mode, perform the following steps:*

1. Save the real-time protection task settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
```

```
--get-settings 8 --file=<full path to the file>
```

2. Open the created file for editing and assign one of the following values to the **ScanByAccessType** setting in the [ScanScope:ScanSettings] section:

- **SmartCheck**, to enable the Smart mode;
- **Open**, to enable protection mode at an attempt to access the file;
- **OpenAndModify**, to enable protection mode at an attempt to open and modify the file.

3. Import settings from file to the real-time protection task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--set-settings 8 --file=<full path to the file>
```

USING HEURISTIC ANALYSIS

Objects are scanned using databases which contain descriptions of all known malware and the corresponding disinfection methods. Kaspersky Internet Security compares each scanned object with the database's records to determine firmly if the object is malicious, and if so, into which class of malware it falls. This approach is called *signature analysis* and is always used by default.

Since new malicious objects appear daily, there is always some malware which is not described in the databases, and which can only be detected using a *heuristic analysis*. This method presumes the analysis of the actions an object performs within the system. If these actions are indicative of a malicious object, the object is likely to be classed as malicious or suspicious. Consequently, new threats are identified before they become known to virus analysts.

Additionally you can set the detail level for scans. It sets the balance between the thoroughness of searches for new threats, the load on the operating system's resources and the time required for scanning. The higher the detail level, the more resources the scan will require, and the longer it will take.

◆ *To use the heuristic analysis and set the detail level for scans:*

1. Save the real-time protection task settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-settings 8 --file=<full path to the file>
```

2. Open the created file for editing and assign values to the following settings:

- the value **yes** to the **UseAnalyzer** setting in the [ScanScope:ScanSettings] section;
- one of the values: **Light**, **Medium** or **Deep** for the **HeuristicLevel** setting in the [ScanScope:ScanSettings] section.

3. Import settings from file to the real-time protection task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--set-settings 8 --file=<full path to the file>
```

USING SCAN MODE DEPENDING ON USER AND GROUP ACCOUNTS ACCESSING THE OBJECTS

Kaspersky Anti-Virus offers an opportunity to scan objects if they are accessed by applications running with the permissions of the specified users or specified groups.

➤ To enable the object scan mode depending on user and group accounts accessing the objects, perform the following steps:

1. Save the real-time protection task settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-settings 8 --file=<full path to the file>
```

2. Open the created file for editing and assign values to the following settings:

- the value **yes** to the **UseAccessUser** setting in the [ScanScope] section;
- user account, under which file operations will be scanned to the **UserName** setting in the [ScanScope:AccessUser] section;
- group account, under which file operations will be scanned to the **UserGroup** setting in the [ScanScope:AccessUser] section.

If you wish to specify several user names or group names, specify values for the **UserName** and **UserGroup** settings the required number of times in one section.

3. Import settings from file to the real-time protection task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--set-settings 8 --file=<full path to the file>
```

SELECTING ACTIONS TO PERFORM ON DETECTED OBJECTS

Kaspersky Anti-Virus blocks access to the detected object irrespective of the selected action.

As a result of the scan, Kaspersky Anti-Virus assigns one of the following statuses to the object:

- *infected*, if code of a known virus is detected in the object;
- *suspicious*, if the scan cannot determine whether the object is infected or not. This means that the application detected a sequence of code in the file from an unknown virus, or modified code from a known virus.

You can specify two actions to perform on objects with each status. If Kaspersky Anti-Virus fails to perform the first action, it will perform the second action.

You can specify the following actions to perform on detected objects:

- **Recommended.** Kaspersky Anti-Virus automatically selects and performs actions on the object based on data about the threat detected in the object and about the possibility of disinfecting it. For example, Kaspersky Anti-Virus will immediately remove Trojans since they do not incorporate themselves into other files and do not infect them; therefore they do not need to be disinfecting.
- **Cure.** Kaspersky Anti-Virus attempts to disinfect the object, and if disinfection is not possible, it leaves the object intact.
- **Quarantine.** Kaspersky Anti-Virus moves the object to quarantine, where it is stored in encrypted form.
- **Remove.** Kaspersky Anti-Virus deletes the object after making a backup copy.
- **Skip.** Kaspersky Anti-Virus leaves the object unchanged.

The **Recommended** action can be selected only as the first action.

If **Skip** was selected as the first action, the second action can be **Skip** only.

If **Recommended** or **Remove** was selected as the first action, **Quarantine** cannot be selected as the second action.

➔ To specify actions to be performed on infected objects, perform the following steps:

1. Save the real-time protection task settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-settings 8 --file=<full path to the file>
```

2. Open the created file for editing and assign values to the following settings:

- **InfectedFirstAction** in the [ScanScope:ScanSettings] section;
- **InfectedSecondAction** in the [ScanScope:ScanSettings] section;

3. Import settings from file to the real-time protection task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 8 --file=<full path to the file>
```

➔ To specify actions to be performed on suspicious objects, perform the following steps:

1. Save the real-time protection task settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-settings 8 --file=<full path to the file>
```

2. Open the created file for editing and assign values to the following settings:

- **SuspiciousFirstAction** in the [ScanScope:ScanSettings] section;
- **SuspiciousSecondAction** in the [ScanScope:ScanSettings] section;

3. Import settings from file to the real-time protection task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 8 --file=<full path to the file>
```

SELECTING ACTIONS DEPENDING ON THE THREAT TYPE

Kaspersky Anti-Virus blocks access to the detected object irrespective of the selected action.

You can specify operations for the following types of threats:

- **Virware** – viruses;
- **Trojware** – Trojan programs;
- **Malware** – programs which cannot harm your computer directly, but can be used by developers of malicious code or various malicious programs;
- **Adware** – advertising software;

- **Pornware** – programs which download pornographic material or pornography sites without the user's permission;
- **Riskware** – harmless programs which could be used for malicious purposes. An example of such software is Remote Administrator utility.

You can specify two actions for each threat type. If Kaspersky Anti-Virus fails to perform the first action, it will perform the second action.

You can specify the following actions:

- **Recommended.** Kaspersky Anti-Virus automatically selects and performs actions on the object based on data about the threat detected in the object and about the possibility of disinfecting it. For example, Kaspersky Anti-Virus will immediately remove Trojans since they do not incorporate themselves into other files and do not infect them; therefore they do not need to be disinfecting.
- **Cure.** Kaspersky Anti-Virus attempts to disinfect the object, and if disinfection is not possible, it leaves the object intact.
- **Quarantine.** Kaspersky Anti-Virus moves the object to quarantine, where it is stored in encrypted form.
- **Remove.** Kaspersky Anti-Virus deletes the object after making a backup copy.
- **Skip.** Kaspersky Anti-Virus leaves the object unchanged.

The **Recommended** action can be selected only as the first action.

If **Skip** was selected as the first action, the second action can be **Skip** only.

If **Recommended** or **Remove** was selected as the first action, **Quarantine** cannot be selected as the second action.

➡ To specify actions to perform on the threat of specific type, perform the following steps:

1. Save the real-time protection task settings to a file using the following command:


```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-settings 8 --file=<full path to the file>
```
2. Open the created file for editing.
3. Assign the value **yes** to the **UseAdvancedActions** setting in the `[ScanScope:ScanSettings]` section.
4. Add the `[ScanScope:ScanSettings:AdvancedActions]` section to the configuration file.
5. Specify the threat type using the **Verdict** setting in the `[ScanScope:ScanSettings:AdvancedActions]` section.
6. Specify actions to be performed on the threat of selected type using the **FirstAction** and **SecondAction** settings in the `[ScanScope:ScanSettings:AdvancedActions]` section.
7. Import settings from file to the real-time protection task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 8 --file=<full path to the file>
```

SCAN OPTIMIZATION

You can reduce the scan time and speed up Kaspersky Anti-Virus. To do so, you can specify two types of restrictions:

- restriction on the scan duration: once the specified time period elapses, the object scan will be stopped;
- restriction on the maximum size of the object to scan: objects larger than the specified limit will be skipped during the scan.

➤ *To impose a time restriction on the scan duration, perform the following steps:*

1. Save the real-time protection task settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-settings 8 --file=<full path to the file>
```

2. Open the created file for editing and assign values to the following settings:

- the value **yes** to the **UseTimeLimit** setting in the [ScanScope:ScanSettings] section;
- maximum object scan time (in seconds) – to the **TimeLimit** setting in the [ScanScope:ScanSettings] section.

3. Import settings from file to the real-time protection task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--set-settings 8 --file=<full path to the file>
```

➤ *To enable restriction on the maximum size of the object to scan, perform the following steps:*

1. Save the real-time protection task settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-settings 8 --file=<full path to the file>
```

2. Open the created file for editing and assign values to the following settings:

- the value **yes** to the **UseSizeLimit** setting in the [ScanScope:ScanSettings] section;
- maximum object size (in bytes) – to the **SizeLimit** setting in the [ScanScope:ScanSettings] section.

3. Import settings from file to the real-time protection task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--set-settings 8 --file=<full path to the file>
```

COMPATIBILITY WITH OTHER KASPERSKY LAB'S APPLICATIONS

To ensure compatibility of the Kaspersky Anti-Virus 8.0 with Kaspersky Anti-Virus for Linux Mail Server, Kaspersky Anti-Spam, and Kaspersky Mail Gateway, you should exclude support directories of these programs from being scanned in the real-time protection task.

➤ *To configure simultaneous operation of the Kaspersky Anti-Virus 8.0 and Kaspersky Anti-Virus for Linux Mail Server, perform the following steps:*

1. Save the real-time protection task settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-settings 8 --file=<full path to the file>
```

2. Add the following section to the created file:


```
[ExcludedFromScanScope]
AreaMask="*"
UseAccessUser=yes
[ExcludedFromScanScope:AreaPath]
Path=<path to directory of the mail queue of mail agent integrated with Kaspersky
Anti-Virus for Linux Mail Server>
[ExcludedFromScanScope:AccessUser]
UserName=<name of user who is the owner of the mail queue>
```

- Repeat the section specified above for all mail agents integrated with Kaspersky Anti-Virus for Linux Mail Server.
- To exclude from the scan the temporary directory for Kaspersky Anti-Virus for Linux Mail Server filter and services, add the following section to the created file:

```
[ExcludedFromScanScope]
AreaMask="*"
UseAccessUser=yes
[ExcludedFromScanScope:AreaPath]
Path="/var/tmp"
[ExcludedFromScanScope:AccessUser]
UserName="kluser"
```

- Import settings from file to the real-time protection task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 8 --file=<full path to the file>
```

➡ *To configure simultaneous operation of Kaspersky Anti-Virus 8.0 with Kaspersky Anti-Spam, perform the following steps:*

- Save the real-time protection task settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-settings 8 --file=<full path to the file>
```

- Add the following section to the created file:

```
[ExcludedFromScanScope]
AreaMask="*"
UseAccessUser=yes
[ExcludedFromScanScope:AreaPath]
Path=<path to directory of the mail queue of mail agent integrated with Kaspersky
Anti-Spam>
[ExcludedFromScanScope:AccessUser]
UserName=<name of user who is the owner of the mail queue>
```

- Repeat the section specified above for all mail agents integrated with Kaspersky Anti-Spam.
- Import settings from file to the real-time protection task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 8 --file=<full path to the file>
```

- To configure simultaneous operation of Kaspersky Anti-Virus 8.0 with Kaspersky Mail Gateway, perform the following steps:

1. Save the real-time protection task settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-settings 8 --file=<full path to the file>
```

2. To exclude from the scan the Kaspersky Mail Gateway queue directory, add the following section to the created file:

```
[ExcludedFromScanScope]  
AreaMask="*"\  
UseAccessUser=yes  
[ExcludedFromScanScope:AreaPath]  
Path="/var/spool/kaspersky/mailgw"  
[ExcludedFromScanScope:AccessUser]  
UserName="kluser"
```

3. Import settings from file to the real-time protection task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--set-settings 8 --file=<full path to the file>
```

ON-DEMAND SCAN

An on-demand scan involves one-time complete or selective scan for the malicious programs on the computer.

Kaspersky Anti-Virus may run several on-demand scan tasks at the same time.

Kaspersky Anti-Virus includes three predefined on-demand scan tasks:

- **On-demand scan.** Scans all local objects on the computer with the recommended security settings.
- **Scan of all shared objects.** Scans all shared objects regardless of the access protocol.
- **Scanning quarantined objects.** Scans quarantined objects. By default, this task starts automatically after each database update.

Kaspersky Anti-Virus can also perform a quick scan of files and directories (see section "Quick scan of files and directories" on page [46](#)) from the command line.

You can create on-demand scan tasks.

IN THIS SECTION

The structure of predefined security levels in on-demand scan tasks	43
Quick scan of files and directories.....	46
Creating a scan area.....	48
Restricting a scan area using masks and regular expressions.....	49
Excluding objects from the scan area	49
Using heuristic analysis.....	52
Selecting actions to perform on detected objects.....	52
Selecting actions depending on the threat type.....	53
Scan optimization.....	55
Selecting task priority	55

THE STRUCTURE OF PREDEFINED SECURITY LEVELS IN ON-DEMAND SCAN TASKS

Kaspersky Lab specialists distinguish three security levels. The decision of which level to select must be taken on your own based on the operation conditions and the current situation. You will be invited to select one of the following security levels:

- **Low**

The **Low** security level can be selected on a server if the network has other computer security tools besides Anti-Virus on servers and workstations, for example, firewalls are configured and security policies are established for the network users.

The following settings will be applied at the **Low** security level during the scan:

```
[ScanScope:ScanSettings]

ScanArchived=no

ScanSfxArchived=no

ScanMailBases=no

ScanPlainMail=no

ScanPacked=yes

UseTimeLimit=yes

TimeLimit=60

UseSizeLimit=yes

SizeLimit=8388608

ScanByAccessType="SmartCheck"

InfectedFirstAction="Cure"

InfectedSecondAction="Remove"

SuspiciousFirstAction="Quarantine"

SuspiciousSecondAction="Skip"

UseAdvancedActions=yes

UseExcludeMasks=no

UseExcludeThreats=no

ReportCleanObjects=no

ReportPackedObjects=no

UseAnalyzer=yes

HeuristicLevel="Light"

[ScanScope:ScanSettings:AdvancedActions]

Verdict="Riskware"

FirstAction="Skip"

SecondAction="Skip"
```

- **Recommended**

The **Recommended** security level is set by default. Experts of Kaspersky Lab deem it sufficient for protection of file servers in most networks. The level provides an optimal combination of protection and the load on protected servers.

The following settings will be applied at the **Recommended** security level during the scan:

```
[ScanScope:ScanSettings]
ScanArchived=no
ScanSfxArchived=no
ScanMailBases=no
ScanPlainMail=no
ScanPacked=yes
UseTimeLimit=yes
TimeLimit=60
UseSizeLimit=no
SizeLimit=8388608
ScanByAccessType="SmartCheck"
InfectedFirstAction="Recommended"
InfectedSecondAction="Skip"
SuspiciousFirstAction="Recommended"
SuspiciousSecondAction="Skip"
UseAdvancedActions=yes
UseExcludeMasks=no
UseExcludeThreats=no
ReportCleanObjects=no
ReportPackedObjects=no
UseAnalyzer=yes
HeuristicLevel="Light"
[ScanScope:ScanSettings:AdvancedActions]
Verdict="Riskware"
FirstAction="Skip"
SecondAction="Skip"
```

- **High**

Use the **High** security level if you have high requirements to the security of your computer network.

The following settings will be applied at the **High** security level during the scan:

```
[ScanScope:ScanSettings]
ScanArchived=no
ScanSfxArchived=yes
ScanMailBases=no
ScanPlainMail=no
ScanPacked=yes
UseTimeLimit=yes
TimeLimit=60
UseSizeLimit=no
SizeLimit=8388608
ScanByAccessType="SmartCheck"
InfectedFirstAction="Cure"
InfectedSecondAction="Remove"
SuspiciousFirstAction="Quarantine"
SuspiciousSecondAction="Skip"
UseAdvancedActions=yes
UseExcludeMasks=no
UseExcludeThreats=no
ReportCleanObjects=no
ReportPackedObjects=no
UseAnalyzer=yes
HeuristicLevel="Light"
[ScanScope:ScanSettings:AdvancedActions]
Verdict="Riskware"
FirstAction="Skip"
SecondAction="Skip"
```

QUICK SCAN OF FILES AND DIRECTORIES

Kaspersky Anti-Virus can perform a quick scan of files and directories without the need to configure a scan area. You can define name templates for files and directories being scanned or their paths using Shell masks.

Shell masks can be used to define a name template for a file or directory to be scanned by Kaspersky Anti-Virus.

➤ *To scan file or directory:*

```
opt/kaspersky/kav4fs/bin/kav4fs-control --scan-file <path to file or directory>
```

➤ *To scan several files or directories:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --scan-file <path to file or directory>  
<path to file or directory> etc.
```

Configuration for running files and directories scan using the --scan-file command:

```
ScanPriority="System"  
  
[ScanScope]  
  
AreaMask="*"
AreaDesc="Scan one file"  
  
[ScanScope:AreaPath]  
Path="<path to scanned files and directories>"  
  
[ScanScope:ScanSettings]  
  
ScanArchived=yes  
ScanSfxArchived=yes  
ScanMailBases=yes  
ScanPlainMail=yes  
ScanPacked=yes  
  
UseTimeLimit=no  
TimeLimit=120  
  
UseSizeLimit=no  
SizeLimit=0  
  
InfectedFirstAction="Skip"  
InfectedSecondAction="Skip"  
SuspiciousFirstAction="Skip"  
SuspiciousSecondAction="Skip"  
  
UseAdvancedActions=no  
UseExcludeMasks=no  
UseExcludeThreats=no  
ReportCleanObjects=no  
ReportPackedObjects=no
```

```
UseAnalyzer=no
```

```
HeuristicLevel="Medium"
```

By default, all detected objects will be skipped and the corresponding data will be recorded in the report. You can specify one of the following actions performed on detected objects: **Recommended**, **Cure**, **Quarantine**, **Remove**, **Skip**.

➤ *To specify actions on detected objects:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --action <action> --scan-file <path to file or directory>
```

CREATING A SCAN AREA

Note the peculiarities (see page 9) in scanning of symbolic and hard links.

The on-demand scan task scans objects within the server file system that are included in the *scan area*. You can extend or narrow down the scan area by adding or removing objects to be scanned, or by changing the type of files to be scanned (see page 49).

Kaspersky Anti-Virus will scan objects in the specified areas in the order, in which they are listed in the configuration file or in its Web Management Console. If you wish to specify the security settings of the subdirectory to be different from the security settings of the parent directory, place the subdirectory in the list higher, than its parent directory.

➤ *To extend a scan area, perform the following steps:*

1. Save the on-demand scan task settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-settings <task ID> --file=<full path to the file>
```

2. Add the following sections to the created file:

- [ScanScope] which contains the following settings:
 - **AreaMask** which defines the name mask of objects to be scanned;
 - **AreaDesc** which defines the name of protection area.
- [ScanScope:AreaPath] which contains the **Path** setting.
- [ScanScope:ScanSettings] which contains scan settings for the area to be added.

All settings must be assigned in the [ScanScope:ScanSettings] section.

3. Import settings from file to the on-demand scan task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--set-settings <task ID> --file=<full path to the file>
```

➤ *To narrow down a scan area, perform the following steps:*

1. Save the on-demand scan task settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-settings <task ID> --file=<full path to the file>
```

2. Delete from the created file the following sections, defining protection area:

- [ScanScope];
 - [ScanScope:AreaPath];
 - [ScanScope:ScanSettings].
3. Import settings from file to the on-demand scan task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings <task ID> --file=<full path to the file>
```

RESTRICTING A SCAN AREA USING MASKS AND REGULAR EXPRESSIONS

By default, Kaspersky Anti-Virus scans all objects within a protected area.

You can specify templates for the names or paths of the files to scan. In this case, Kaspersky Anti-Virus will only scan files or directories from the protected area that are specified using Shell masks or POSIX extended regular expressions.

Using Shell masks, you can specify the file name template to scan by Kaspersky Anti-Virus.

Using extended regular expressions, you can specify the file path template to scan by Kaspersky Anti-Virus. A regular expression cannot contain the name of the folder which defines the scan or protection area.

➤ *To specify file name or path templates for the files to be scanned, perform the following steps:*

1. Save the on-demand scan task settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-settings <task ID> --file=<full path to the file>
```

2. Specify the value of the **AreaMask** setting in the [ScanScope] section which defines the protection area.
3. Import settings from file to the on-demand scan task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings <task ID> --file=<full path to the file>
```

EXCLUDING OBJECTS FROM THE SCAN AREA

By default, the on-demand scan task scans all objects included in the scan areas defined for this task.

You can exclude several objects from the scan. To do that, you can create three types of exclusions:

- exclusion of objects from a scan area: in this case the specified objects will only be excluded from the selected scan area;
- global exclusion of objects: in this case the specified objects will be excluded from all scan areas defined for the task;
- exclusion of objects by the name of the threat detected in them.

IN THIS SECTION

Creating a global exclusion area	50
Excluding objects from the scan area	50
Excluding objects by names of the threats detected in them.....	51

CREATING A GLOBAL EXCLUSION AREA

You can create a global exclusion area. Objects included in this area will be excluded from all areas defined for the on-demand scan task.

➤ *To create a global exclusion area, perform the following steps:*

1. Save the on-demand scan task settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-settings <task ID> --file=<full path to the file>
```

2. Add the following sections to the created file:

- [ExcludedFromScanScope], which contains the following settings:
 - **AreaMask**, which defines templates of object names to be excluded from the scan;
 - **AreaDesc**, which defines a unique name for exclusion area.
- [ExcludedFromScanScope:AreaPath], which contains the **Path** setting that defines the path to the objects to be excluded from the scan.

3. Import settings from file to the on-demand scan task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings <task ID> --file=<full path to the file>
```

EXCLUDING OBJECTS FROM THE SCAN AREA

By default, Kaspersky Anti-Virus checks all objects within a scan area.

You can define name and path templates that are excluded from the scan area. In that case Kaspersky Anti-Virus will not check files or directories within the scan area if they match the specified Shell masks or extended POSIX regular expressions.

You can use Shell masks to specify a file name template excluded from scanning by Kaspersky Anti-Virus.

You can also use extended regular expressions to specify a template for the paths to files which Kaspersky Anti-Virus should not scan. The regular expression should not contain the name of the directory containing excluded object.

➤ *To exclude objects from the scan area, perform the following steps:*

1. Save the on-demand scan task settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-settings <task ID> --file=<full path to the file>
```

2. Open the created file for editing.
3. Assign the value **yes** to the **UseExcludeMasks** setting in the [ScanScope:ScanSettings] section.

- Specify file name or path templates using the **ExcludeMasks** setting in the [ScanScope:ScanSettings] section.

To specify several file name or path templates, repeat the **ExcludeMasks** setting value the required number of times.

- Import settings from file to the on-demand scan task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--set-settings <task ID> --file=<full path to the file>
```

EXCLUDING OBJECTS BY NAMES OF THE THREATS DETECTED IN THEM

If Kaspersky Anti-Virus considers a scanned object to be infected or suspicious, it performs the action on this object specified in the task. If you consider this object to be harmless for the protected computer, you can exclude it from the scan scope by the name of threat detected in it. In this case Kaspersky Anti-Virus considers such objects as not infected and does not scan them.

The full name of the threat may contain the following information:

<threat class>:<threat type>.<brief name of operating system>.<threat name>.<threat modification code>. For example, **not-a-virus:NetTool.Linux.SynScan.a**.

You can find the full name of the threat detected in an object in the Kaspersky Anti-Virus log.

You can also find the full name of the threat detected in a software product at the Virus Encyclopedia web site (see the Virus Encyclopedia section at <http://www.viruslist.com>). To find the type of a threat, enter the name of the product in the **Search** field.

When specifying threat name templates, you can use Shell masks and POSIX extended regular expressions.

➔ *To exclude objects by the name of detected threat, perform the following steps:*

- Save the on-demand scan task settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-settings <task ID> --file=<full path to the file>
```

- Open the created file for editing.
- Assign the value **yes** to the **UseExcludeThreats** setting in the [ScanScope:ScanSettings] section.
- Specify the threat name template using the **ExcludeThreats** setting in the [ScanScope:ScanSettings] section.

To specify several threat name templates, repeat the **ExcludeThreats** setting value the required number of times.

- Import settings from file to the on-demand scan task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--set-settings <task ID> --file=<full path to the file>
```

USING HEURISTIC ANALYSIS

Objects are scanned using databases which contain descriptions of all known malware and the corresponding disinfection methods. Kaspersky Internet Security compares each scanned object with the database's records to determine firmly if the object is malicious, and if so, into which class of malware it falls. This approach is called *signature analysis* and is always used by default.

Since new malicious objects appear daily, there is always some malware which is not described in the databases, and which can only be detected using a *heuristic analysis*. This method presumes the analysis of the actions an object performs within the system. If these actions are indicative of a malicious object, the object is likely to be classed as malicious or suspicious. Consequently, new threats are identified before they become known to virus analysts.

Additionally you can set the detail level for scans. It sets the balance between the thoroughness of searches for new threats, the load on the operating system's resources and the time required for scanning. The higher the detail level, the more resources the scan will require, and the longer it will take.

➤ *To use the heuristic analysis and set the detail level for scans:*

1. Save the on-demand scan task settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-settings <task ID> --file=<full path to the file>
```

2. Open the created file for editing and assign values to the following settings:

- the value **yes** to the **UseAnalyzer** setting in the [ScanScope:ScanSettings] section;
- one of the values: **Light**, **Medium** or **Deep** for the **HeuristicLevel** setting in the [ScanScope:ScanSettings] section.

3. Import settings from file to the on-demand scan task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--set-settings <task ID> --file=<full path to the file>
```

SELECTING ACTIONS TO PERFORM ON DETECTED OBJECTS

As a result of the scan, Kaspersky Anti-Virus assigns one of the following statuses to the object:

- *infected*, if code of a known virus is detected in the object;
- *suspicious*, if the scan cannot determine whether the object is infected or not. This means that the application detected a sequence of code in the file from an unknown virus, or modified code from a known virus.

You can specify two actions to perform on objects with each status. If Kaspersky Anti-Virus fails to perform the first action, it will perform the second action.

You can specify the following actions to perform on detected objects:

- **Recommended.** Kaspersky Anti-Virus automatically selects and performs actions on the object based on data about the threat detected in the object and about the possibility of disinfecting it. For example, Kaspersky Anti-Virus will immediately remove Trojans since they do not incorporate themselves into other files and do not infect them; therefore they do not need to be disinfecting.
- **Cure.** Kaspersky Anti-Virus attempts to disinfect the object, and if disinfection is not possible, it leaves the object intact.

- **Quarantine.** Kaspersky Anti-Virus moves the object to quarantine, where it is stored in encrypted form.
- **Remove.** Kaspersky Anti-Virus deletes the object after making a backup copy.
- **Skip.** Kaspersky Anti-Virus leaves the object unchanged.

The **Recommended** action can be selected only as the first action.

If **Skip** was selected as the first action, the second action can be **Skip** only.

If **Recommended** or **Remove** was selected as the first action, **Quarantine** cannot be selected as the second action.

➔ To specify actions to be performed on infected objects, perform the following steps:

1. Save the on-demand scan task settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-settings <task ID> --file=<full path to the file>
```

2. Open the created file for editing and assign values to the following settings:

- **InfectedFirstAction** in the [ScanScope:ScanSettings] section;
- **InfectedSecondAction** in the [ScanScope:ScanSettings] section.

3. Import settings from file to the on-demand scan task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--set-settings <task ID> --file=<full path to the file>
```

➔ To specify actions to be performed on suspicious objects, perform the following steps:

1. Save the on-demand scan task settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-settings <task ID> --file=<full path to the file>
```

2. Open the created file for editing and assign values to the following settings:

- **SuspiciousFirstAction** in the [ScanScope:ScanSettings] section;
- **SuspiciousSecondAction** in the [ScanScope:ScanSettings] section.

3. Import settings from file to the on-demand scan task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--set-settings <task ID> --file=<full path to the file>
```

SELECTING ACTIONS DEPENDING ON THE THREAT TYPE

You can specify operations for the following types of threats:

- **Virware** – viruses;
- **Trojware** – Trojan programs;
- **Malware** – programs which cannot harm your computer directly, but can be used by developers of malicious code or various malicious programs;

- **Adware** – advertising software;
- **Pornware** – programs which download pornographic material or pornography sites without the user's permission;
- **Riskware** – harmless programs which could be used for malicious purposes. An example of such software is Remote Administrator utility.

You can specify two actions for each threat type. If Kaspersky Anti-Virus fails to perform the first action, it will perform the second action.

You can specify the following actions:

- **Recommended.** Kaspersky Anti-Virus automatically selects and performs actions on the object based on data about the threat detected in the object and about the possibility of disinfecting it. For example, Kaspersky Anti-Virus will immediately remove Trojans since they do not incorporate themselves into other files and do not infect them; therefore they do not need to be disinfecting.
- **Cure.** Kaspersky Anti-Virus attempts to disinfect the object, and if disinfection is not possible, it leaves the object intact.
- **Quarantine.** Kaspersky Anti-Virus moves the object to quarantine, where it is stored in encrypted form.
- **Remove.** Kaspersky Anti-Virus deletes the object after making a backup copy.
- **Skip.** Kaspersky Anti-Virus leaves the object unchanged.

The **Recommended** action can be selected only as the first action.

If **Skip** was selected as the first action, the second action can be **Skip** only.

If **Recommended** or **Remove** was selected as the first action, **Quarantine** cannot be selected as the second action.

➤ To specify actions to perform on the threat of specific type, perform the following steps:

1. Creating an on-demand scan on a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-settings <task ID> --file=<full path to the file>
```

2. Open the created file for editing.
3. Assign the value **yes** to the **UseAdvancedActions** setting in the [ScanScope:ScanSettings] section.
4. Add the [ScanScope:ScanSettings:AdvancedActions] section to the configuration file.
5. Specify the threat type using the **Verdict** setting in the [ScanScope:ScanSettings:AdvancedActions] section.
6. Specify actions to be performed on the threat of selected type using the **FirstAction** and **SecondAction** settings in the [ScanScope:ScanSettings:AdvancedActions] section.
7. Import settings from file to the on-demand scan task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--set-settings <task ID> --file=<full path to the file>
```

SCAN OPTIMIZATION

You can reduce the scan time and speed up Kaspersky Anti-Virus. To do so, you can specify two types of restrictions:

- restriction on the scan duration: once the specified time period elapses, the object scan will be stopped;
- restriction on the maximum size of the object to scan: objects larger than the specified limit will be skipped during the scan.

➔ *To impose a time restriction on the scan duration, perform the following steps:*

1. Save the on-demand scan settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-settings <task ID> --file=<full path to the file>
```

2. Open the created file for editing and assign values to the following settings:

- the value **yes** to the **UseTimeLimit** setting in the [ScanScope:ScanSettings] section;
- maximum object scan time (in seconds) – to the **TimeLimit** setting in the [ScanScope:ScanSettings] section.

3. Import settings from file to the on-demand scan task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--set-settings <task ID> --file=<full path to the file>
```

➔ *To enable restriction on the maximum size of the object to scan, perform the following steps:*

1. Creating an on-demand scan to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-settings <task ID> --file=<full path to the file>
```

2. Open the created file for editing and assign values to the following settings:

- the value **yes** to the **UseSizeLimit** setting in the [ScanScope:ScanSettings] section;
- maximum object size (in bytes) – to the **SizeLimit** setting in the [ScanScope:ScanSettings] section.

3. Import settings from file to the on-demand scan task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--set-settings <task ID> --file=<full path to the file>
```

SELECTING TASK PRIORITY

By default, all on-demand scan tasks are executed with the priority defined by the system when the task is launched. You can assign one of the following priorities to the task:

- **System.** Priority of the process is defined by the operating system.
- **High.** Decreases the duration of task execution, but it can also affect negatively the performance of processes belonging to other active applications.

Select this option if the task should be performed as soon as possible, despite the possible load on the protected server.

- **Medium.** Priority of the process changes from System to the value recommended by Kaspersky Lab.
- **Low.** Increases the duration of task execution, but it can also affect negatively the performance of processes belonging to other active applications.

Select this option if the load on the protected server should be decreased during task execution.

➡ *To change the priority of the on-demand scan task, execute the following command:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--set-settings <task ID> ScanPriority=<priority>
```


ISOLATING SUSPICIOUS OBJECTS. DATA BACKUP

Kaspersky Anti-Virus isolates objects, which it recognizes as suspicious. The application places such objects to quarantine, i.e., it moves them from their original location into a special storage, in which they are stored in encrypted form for security purposes.

The default storage volume is 1 GB. Once the limit is exceeded, objects will not be added to the storage.

After each database update Kaspersky Anti-Virus automatically scans all quarantined objects. Some of them can be considered not infected and restored from Quarantine. Besides, you can restore objects from Quarantine manually.

Restoring infected or suspicious objects may lead to computer infection.

Kaspersky Anti-Virus saves to a storage encrypted copies of objects before disinfecting or deleting them.

If an object is a part of a compound object, Kaspersky Anti-Virus will save such compound object entirely in the backup storage. For example, if the Anti-Virus has found one of the objects in a mail database to be infected, the entire mail database is backed up.

An object placed in Quarantine or Backup is described using a number of settings (see page [112](#)).

IN THIS SECTION

Viewing statistics of quarantined objects.....	57
Scanning quarantined objects	58
Placing files to quarantine manually	59
Viewing object IDs.....	59
Restoring objects	60
Deleting objects.....	61

VIEWING STATISTICS OF QUARANTINED OBJECTS

You can obtain brief and detailed statistics of quarantined objects.

➤ *To view brief statistics, execute the following command:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q --get-stat --query  
"(OrigType!=s'Backup') "
```

The command returns the number of objects stored in quarantine at the moment and total disk space, which they occupy.

➤ *To view detailed statistics, execute the following command:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -S --get-stat Quarantine
```

If the start and end dates of the report are not specified (see page 84), the statistics will be shown from the moment Kaspersky Anti-Virus was installed.

Table 1. Statistics fields of quarantined objects

FIELD	DESCRIPTION
Quarantined objects	The total number of quarantined objects.
Auto saved objects	The number of objects quarantined by Kaspersky Anti-Virus.
Manually saved objects	The number of objects quarantined by user.
Restored objects	Number of objects restored from the quarantine.
Removed objects	Number of objects deleted from the quarantine.
Infected objects	The number of infected objects (see section "About infected, suspicious objects and objects with the status "Warning" on page 10): a) that were assigned the Infected status after the quarantined object was scanned, and b) that Anti-Virus placed to Quarantine based on the value of the Action to perform depending on threat type setting.
Suspicious objects	The number of suspicious objects (see section "About infected, suspicious objects and objects with the "Warning" status" on page 10).
Curable objects	The number of objects in the storage that Kaspersky Anti-Virus considers infected and curable.
Password protected objects	Number of password-protected objects.
Corrupted objects	The number of corrupted objects.
False detected objects	The number of objects that were assigned the False alarm status, because after scanning using updated databases, quarantined objects were acknowledged to be not infected.

SCANNING QUARANTINED OBJECTS

By default, Kaspersky Anti-Virus executes the **Quarantine scan** task after each database update. Task settings are described in the table below. You cannot modify them.

Having scanned quarantined objects after database update, Kaspersky Anti-Virus may recognize some of the objects as clean (the value of the **Type** field (see page 112) for such objects will change to **Clean**). Other objects can be found infected by Kaspersky Anti-Virus.

You may start the **Scanning quarantined objects** task manually.

➤ To start the **Quarantine scan** task,, execute the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --start-task 10
```

Table 2. The **Quarantine scan** task settings

THE "QUARANTINE SCAN" TASK SETTINGS	VALUE
ID	10
Scan area	Quarantined objects
Default schedule	After databases update
Security settings	Common for the entire scan area. You cannot modify them. The table below contains setting values.

Table 3. Security settings in the **Quarantine scan** task

SECURITY SETTINGS	VALUE
Action to perform on infected objects	Skip
Action to be performed on suspicious objects	Skip
Excluding objects by name	No
Excluding objects by threat name	No
Maximum object scan time	600 sec
Maximum size of a scanned object	Not specified
Scan of compound files	<ul style="list-style-type: none"> • Archives • SFX-archives • Packed objects

PLACING FILES TO QUARANTINE MANUALLY

If you suspect that a file is infected, it can be placed to quarantine manually. A file placed to quarantine is harmless.

➤ To place a file to quarantine manually, execute the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--add-object <full path to the file>
```

VIEWING OBJECT IDS

Using the **-Q** modifier in commands described in this section is mandatory.

When the object is placed in the storage, Kaspersky Anti-Virus assigns a numeric identifier to it. This identifier is used to perform actions on quarantined and backed up objects.

➤ To obtain identifiers of quarantined objects, execute the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q --query "(OrigType!=s'Backup')"
```

Example of command output:

```
Objects returned: 1
```

```
Object ID: 1
```

```

Filename: /home/corr/eicar.com

Object type: UserAdded

Compound object: no

UID: 0

GID: 0

Mode: 644

AddTime: 2009-03-29 09:20 PM:32

Size: 73

```

➔ *To obtain identifiers of backed up objects, execute the following command:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q --query "(OrigType==s'Backup')"
```

Example of command output:

Objects returned: 2

Object ID: 1

```

Filename: /home/cur/eicar.com

Object type: Backup

Compound object: no

UID: 0

GID: 0

Mode: 644

AddTime: 2009-03-29 10:24 PM:50

Size: 73

```

To perform actions on objects, use the value of the **Object ID** field.

RESTORING OBJECTS

Restoring infected or suspicious objects may lead to server infection.

Kaspersky Anti-Virus stores objects in the quarantine / backup storage in encrypted form to ensure the protected server safety from their potential harmful effect.

You can restore any object from the quarantine / backup. This may be required in the following cases:

- If the original file that appeared to be infected contained important information and during disinfection Kaspersky Anti-Virus was unable to preserve its integrity and the information in the file became unavailable.
- If, having scanning the quarantined objects after database update, Kaspersky Anti-Virus recognizes the object as not infected (the value of the **Type** field (see page [112](#)) for such objects will change to **Clean**).

- If you consider the object harmless for the server and wish to use it. To prevent Kaspersky Anti-Virus from isolating this object during subsequent scans, you can exclude the object from being scanned in the real-time protection and on-demand scan tasks. To do so, specify the object as a value for the **Exclude objects by file name** security setting (see page [170](#)) or **Exclude objects by threat name** (see page [170](#)) in these tasks.

You can select where to save the restored object: in its original location or in a directory you specify.

During restoration you can save the object under a different name.

Date and time when the file restored from quarantine was created differs from the date and time of the original file.

- *To restore an object from quarantine or backup to the original location, execute the following command:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --restore <object ID>
```

- *To restore an object from quarantine or backup to the specified folder, execute the following command:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--restore <object ID> -F <file name and path>
```

DELETING OBJECTS

Using the **-Q** modifier in commands described in this section is mandatory.

If you are sure that a quarantined or backed up object is harmless for the server, you can delete it from quarantine or backup.

- *To delete an object from quarantine or backup, execute the following command:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q \  
--remove <object ID>
```

Besides, you can delete all objects from quarantine or backup.

- *To delete all objects from quarantine, execute the following command:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q \  
--mass-remove --query "(OrigType!=s'Backup')"
```

- *To delete all objects from backup, execute the following command:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q \  
--mass-remove --query "(OrigType==s'Backup')"
```

You can empty the quarantine or backup partially using the special command arguments **-Q --mass-remove** (see page [107](#)).

MANAGING LICENSES

As far as Kaspersky Lab's application licensing is concerned, it is important to know about the following concepts:

- the License Agreement;
- license;

- key file;
- activation code;
- application activation.

These concepts are indissolubly interconnected and form a single licensing scheme.

Provided below is the detailed description of each concept.

ABOUT THE LICENSE AGREEMENT

The *License Agreement* is a legal contract between an individual or legal entity, who/that lawfully holds in ownership a copy of Kaspersky Anti-Virus, and Kaspersky Lab ZAO. The License Agreement is included in each Kaspersky Lab's application kit. It contains detailed information about the rights and limitations to use Kaspersky Anti-Virus.

In accordance with the License Agreement, by purchasing and installing a Kaspersky Lab's application, you obtain a right of perpetual use of its copy.

Kaspersky Lab is delighted to offer you additional services:

- technical support;
- Kaspersky Anti-Virus database update;
- Anti-Virus program modules update.

To obtain these services, you should purchase and activate a license (see section "About Kaspersky Anti-Virus licenses" on page [62](#)).

ABOUT LICENSES FOR KASPERSKY ANTI-VIRUS

License is the right to use Kaspersky Anti-Virus and related additional services provided by Kaspersky Lab and its partners.

Each license is characterized by license period and type.

License validity period is the period of time over which you are able to use the additional services (see section "About the licensing agreement" on page [62](#)). The range of services depends on the license type.

The following types of licenses are provided:

- *Trial* - a free license with a limited validity period, for example, 30 days, intended to acquaint users with Kaspersky Anti-Virus.

The trial license can only be used once!

It is supplied with the trial version of the application. You cannot contact Technical Support if you only have a trial license. On expiry of the validity period, Kaspersky Anti-Virus ceases all its functions.

- *Commercial* - a paid license with a validity period of, for example, one year, issued when you purchase Kaspersky Anti-Virus. This license comes with certain restrictions, for example, on the number of computers it can be used for or the amount of daily traffic that can be scanned.

Under clause 3.6 of the license agreement, if Kaspersky Anti-Virus is purchased for use on more than one computer, the validity period of the license shall begin when the application is activated on the first computer.

All functions and additional services are available during the validity period of a commercial license.

When the commercial license expires, Kaspersky Anti-Virus continues to perform all of its functions; additional services, however, are not provided. As before, you will be able to scan your computer for viruses and use the protection components, but using only the anti-virus databases you had when the license expired. Consequently, Kaspersky Lab does not guarantee 100% protection for your computer against new viruses after expiry of the license validity period.

To use the application and its additional services, you should purchase a commercial license and activate it.

The activation of a license is performed using the installation of a key file (see section "About Kaspersky Anti-Virus key files" on page [63](#)) associated with the license.

ABOUT KASPERSKY ANTI-VIRUS KEY FILES

Key file – a tool used to activate a corresponding license (see section "About Kaspersky Anti-Virus licenses" on page [62](#)), as well as your right to use the application and additional services (see page [62](#)).

The key file is included in the application distribution kit, if you purchase it from the Kaspersky Lab's distributors, or is sent to you by mail, if you purchase the application in the Kaspersky Lab's eStore.

The key file contains the following information:

- Period of license validity.
- License type (trial or commercial).
- License restrictions (for example, the number of hosts for which the license is valid, or the volume of protected mail traffic).
- Technical Support Service contact information.
- Validity period.

The *key file validity period* is the key file "shelf life", assigned to the key file when it is created. It is a time period after which the key file becomes invalid, and activation of the associated license is unavailable.

Let us examine, how the key file validity period and the license period are connected as an example.

Example:

License period: 300 days

The key write date is 9/1/2010.

Validity period of the key file: 300 days

The key file installation date (license activation date) is 9/10/2010, which is 9 days after the key write date.

Result:

The calculated license validity period is 300 days-9 days = 291 days.

INSTALLING THE KEY FILE

You can immediately install two key files (see page [63](#)): an active key file and a supplementary key file. The active key file takes effect from its installation. The supplementary key file automatically takes effect immediately after the end of the active key file validity period.

If you install the key file as the active key file, although there is an active key file in Anti-Virus already, the new key file will replace the previously installed one. The key file installed earlier will be removed.

If you install the key file as a supplementary key file, although there is a supplementary key file in Anti-Virus already, the new key file will replace the previously installed one. The key file installed earlier will be removed.

- To install a key file as an active key, execute the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--install-active-key <key filename>
```

- To install a key file as a supplementary key, execute the command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--install-suppl-key <key filename>
```

VIEWING INFORMATION ABOUT A LICENSE PRIOR TO THE KEY FILE INSTALLATION

You can view license information stored in the key file before its installation.

- To view license information (see page [62](#)), execute the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--show-license-info <full path to the file>
```

This command outputs the following license information (see the table below).

Table 4. License information

FIELD	DESCRIPTION
Application name	The name of the application for which the key file was written.
Key file creation date	Key file write date (see page 63).
Key file expiration date	License expiration date.
License number	The license serial number.
License type	License type: trial or commercial.
Usage restriction	Number of objects defined in restriction. Restriction to use Kaspersky Anti-Virus provided for by the license.
License period	License validity period (see page 62).

Example of command output:

License info:

```
Application name:           Kaspersky BusinessSpace Security International Edition.  
10-14 User 1 year NFR License: Kaspersky Anti-Virus Suite for WS and FS
```

```
Key file creation date:    2009-05-28
```

```
Key file expiration date: 2010-08-27
```

```
License number:           0038-000451-05B74DD4
```


License type:	Commercial
Usage restriction:	10
License period:	365

KEY FILE REMOVAL

You can remove the key file. If you remove the active key file, the supplementary key file will automatically become active.

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

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--revoke-active-key
```

- *To remove a supplementary key file, execute the following command:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--revoke-suppl-key
```

REVIEWING THE LICENSE AGREEMENT

The License Agreement is a legal contract between an individual or legal entity, who/that lawfully holds in ownership a copy of Kaspersky Anti-Virus, and Kaspersky Lab ZAO. The License Agreement is included in each Kaspersky Lab's application kit. It contains detailed information about the rights and limitations to use Kaspersky Anti-Virus.

In accordance with the License Agreement, by purchasing and installing a Kaspersky Lab's application, you obtain a right of perpetual use of its copy.

- *To view the provision of the License Agreement,*

open the file `/opt/kaspersky/kav4fs/share/doc/LICENSE` using a text editor.

ADMINISTRATOR NOTIFICATIONS. EVENT-BASED ACTIONS

While Kaspersky Anti-Virus is running, various events occur (see page [114](#)). They reflect the changes in the status of anti-virus protection of the server and Kaspersky Anti-Virus in general. You can configure administrator notifications about those events by email.

You may also use Shell scripts to configure actions that will be performed when certain events occur.

Notifications delivery and performance of actions is available for the following events:

- **ApplicationStarted**, which occurs when Kaspersky Anti-Virus is started;
- **ApplicationShutdown**, which occurs when Kaspersky Anti-Virus is stopped;
- **ThreatDetected**, which occurs when a malicious object is detected;
- **LicenseExpired**, which occurs upon license expiration;
- **LicenseExpiresSoon**, which occurs at the approach of license expiration;
- **LicenseError**, which occurs when the licensing subsystem reports an error;
- **AVBasesAttached**, which occurs upon successful Kaspersky Anti-Virus database update;
- **AVBasesAreOutOfDate**, which occurs if Kaspersky Anti-Virus database is outdated;
- **AVBasesAreTotallyOutOfDate**, which occurs if Kaspersky Anti-Virus database is totally outdated;
- **UpdateError**, which occurs when Kaspersky Anti-Virus database update reports an error;
- **RetranslationError**, which occurs when Kaspersky Anti-Virus database update copying reports an error;
- **LicenseInstalled**, which occurs upon successful key file installation;
- **LicenseRevoked**, which occurs upon key file removal;
- **AVBasesIntegrityCheckFailed**, which occurs when integrity check of Kaspersky Anti-Virus database reports an error;
- **ObjectNotProcessed**, which occurs if the object was not processed;
- **ObjectProcessingError**, which occurs when object processing reports an error;
- **ObjectDisinfected**, which occurs if the object was successfully disinfected;
- **ObjectDeleted**, which occurs if the object was successfully deleted;
- **QuarantineSizeLimitReached**, which occurs when the maximum allowed size of quarantine or backup is reached;
- **QuarantineSoftSizeLimitReached**, which occurs when the recommended size of quarantine or backup is reached;
- **QuarantineObjectAddFailed**, which occurs when placing the object to quarantine reports an error;
- **QuarantineObjectAdded**, which occurs when the object is successfully placed to quarantine;

- **QuarantineObjectRemoved**, which occurs when the object is successfully removed from quarantine;
- **QuarantineObjectRestored**, which occurs when the object is successfully restored from quarantine;
- **QuarantineThreatDetected**, which occurs when a malicious object is detected in a quarantined object;
- **QuarantineObjectProcessingError**, which occurs when processing of a quarantined object reports an error;
- **QuarantineObjectCurable**, which occurs if a quarantined object can be disinfected;
- **QuarantineFalseDetect**, which occurs if a previously quarantined object was considered not infected as the result of scanning quarantined objects (see page [58](#)).

IN THIS SECTION

Using the internal mailer of Kaspersky Anti-Virus	67
Using Sendmail	68
Generation of notifications.....	68
Configuring actions	69
Using macros	69

USING THE INTERNAL MAILER OF KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus provides an in-built mail program for sending notifications.

➤ *To use an in-built mail program for sending notifications, perform the following steps:*

1. Save notification settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-settings 7 --file=<path to the file>
```

2. Open the created file for editing and make the following changes in it:

- Assign the value **yes** to the **EnableSmtp** setting.
- Assign the value **Internal** to the **Mailer** setting in the [CommonSmtpSettings] section.
- Specify the default recipients' addresses using the **DefaultRecipients** setting in the [CommonSmtpSettings] section.
- Specify the SMTP-server address using the **SmtpServer** setting in the [CommonSmtpSettings:InternalMailerSettings] section.

3. Import the settings from the file into the task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 7 --file=<path to the file>
```

For a detailed description of the notification settings please refer to the "Settings of notifications and event-based actions" section (see page [150](#)).

USING SENDMAIL

If Sendmail is used on your server to send email, you can also use it for Kaspersky Anti-Virus notifications.

For successful delivery of notifications, Sendmail should be configured correctly.

➤ To use Sendmail for delivery of notifications, perform the following steps:

1. Save notification settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-settings 7 --file=<path to the file>
```

2. Open the created file for editing and make the following changes in it:

- Assign the value **yes** to the **EnableSmtp** setting.
- Assign the value **Sendmail** to the **Mailer** setting in the [CommonSmtpSettings] section.
- Specify the default recipients' addresses using the **DefaultRecipients** setting in the [CommonSmtpSettings] section.
- Specify the path to the Sendmail executable file using the **SendmailPath** setting in the [CommonSmtpSettings] section.

3. Import the settings from the file into the task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--set-settings 7 --file=<path to the file>
```

For a detailed description of the notification settings please refer to the "Settings of notifications and event-based actions" section (see page [150](#)).

GENERATION OF NOTIFICATIONS

To send notifications, you have to create the message text and specify the email addresses of its recipients. You can use macros in the message text (see page [69](#)).

➤ To generate notifications, perform the following steps:

1. Save notification settings to a file using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-settings 7 --file=<path to the file>
```

2. Open the created file for editing and make the following changes in it:

- a. Add to the file the [SmtpNotifies] section, which contains the following settings:

- **Recipients**, which defines notification recipients if a local list of recipients is used. Repeat the setting value the required number of times to create a list of recipients;
- **UseRecipientList**, which defines the list of notification recipients;
- **Subject**, which defines the Subject field of notification;
- **Body**, which defines the text of notification;

- **EventName**, which defines the name of event that will trigger notification;
 - **Enable**, which enables / disables notification.
- b. Repeat the [Smtplib] section for all events, notifications about which will be sent.
3. Save changes.
4. Import the settings from the file into the task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 7 --file=<path to the file>
```

CONFIGURING ACTIONS

You can create Shell scripts for execution of operations in case of a specified event. You can use macros in the script text (see page [69](#)).

➤ To create a script, which is triggered by an event, perform the following steps:

1. Save notification settings to a file using the following command:


```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-settings 7 --file=<path to the file>
```
2. Open the created file for editing and make the following changes in it:
 - a. Add to the file the [Actions] section, which contains the following settings:
 - **Command**, which defines the script text;
 - **EventName**, which defines the name of event that will trigger the script;
 - **Enable**, which enables or disables execution of the action.
 - b. Repeat the [Actions] section for all events, which will trigger execution of scripts.
3. Save changes.
4. Import the settings from the file into the task using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-settings 7 --file=<path to the file>
```

USING MACROS

The following macros described in the table below can be used in message and script texts.

Table 5. Macros

MACRO	DESCRIPTION	EVENT
%NOW%	Time when event has occurred	The macro is used for all events
%HOST_NAME%	Name of the server where an event has occurred	The macro is used for all events

MACRO	DESCRIPTION	EVENT
%OBJECT%	Name of infected object	Threat found, Object not processed, Error processing object, Object disinfected, Object deleted, Quarantine and backup maximum size reached, Error processing quarantined object, Object quarantined, Object deleted from quarantine/backup, Object restored from quarantine/backup, Threat found in quarantined object, Error processing quarantined object, Quarantined object rendered curable, False detection: quarantined object non-infected
%SOURCE%	Name of computer - source of infected object	Threat found, Object not processed, Error processing object, Object disinfected, Object deleted
%VERDICT%	Status of the object found	Threat found, Object quarantined, Threat found in quarantined object
%THREAT_NAME%	Name of threat	Threat found, Threat found in quarantined object
%DANGER%	Severity	Threat found, Object quarantined, Threat found in quarantined object
%RECORDS%	Number of records in the product databases	Databases updated
%DAYS_LEFT%	Days remaining until the license expires	License expires soon
%REASON%	Error cause	License error, Update error, Error copying updates, Databases integrity check failed, Object not processed, Error processing object, Error processing quarantined object
%DAYS_PASSED%	Days passed since the last database update	Databases are outdated, Databases are obsolete
%SERIAL%	License serial number	License installed, License deleted
%OBJECT_SIZE%	Object size	Quarantine and backup maximum size reached, Object quarantined, Object deleted from quarantine/backup, Object restored from quarantine/backup
%SIZE_LIMIT%	Maximum size of quarantine and backup storage	Quarantine and backup recommended size reached
%ACTUAL_SIZE%	Current size of quarantine and backup storage	Quarantine and backup recommended size reached
%DESCRIPTION%	Description	Error processing quarantined object
%OBJECT_TYPE%	Object type	Object quarantined, Object deleted from quarantine/backup, Object restored from quarantine/backup

GENERATING REPORTS

You can generate the following reports:

- about the number of malicious objects detected in the largest number of objects on the computers (see page [86](#));
- reports on the activity of Kaspersky Anti-Virus components (see page [84](#)).

You can use the command line to obtain reports on the activity of any individual product component. The Web Management Console allows you to produce reports containing summarized information about the **Real-time protection** and **On-demand scan** components.

You can perform the following operations:

- generate reports for the specified time intervals;
- view reports in separate Web Management Console windows;
- save created reports to files in the following formats:
 - in the command line – to HTML or CSV;
 - in the Web Management Console – to PDF or XLS.

VIEWING THE PROTECTION STATUS VIA SNMP

SNMP protocol provides access to the following categories of information about Kaspersky Anti-Virus:

- general Information;
- activity statistics collected since the time of Kaspersky Anti-Virus installation;
- information about events occurring while Kaspersky Anti-Virus is running.

Access to the information is provided for reading only.

Interaction via SNMP is implemented in Kaspersky Anti-Virus using SNMP-Agent. The product allows using as SNMP manager any SNMP agent that supports the AgentX protocol.

The application can interact with SNMP managers supporting SNMP v2, v2c, v3. SNMP agent implemented in the application supports AgentX version 1.

If you plan to read counters using utilities from the Net-SNMP package, update it to the latest version.

IN THIS SECTION

Configuring interaction via SNMP	72
Structure of the Kaspersky Anti-Virus MIB	73
Description of Kaspersky Anti-Virus MIB objects	75

CONFIGURING INTERACTION VIA SNMP

➤ To enable data exchange over SNMP, perform the following steps:

1. Enter the address of the server, on which SNMP manager is running with the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
  
--set-settings 12 \  
  
MasterAgentXAddress=tcp:<SNMP_manager_IP_address_or_DNS_name>:705
```

This address can be obtained from the configuration file of the SNMP-manager.

2. Start the **SNMP plugin** task (ID=12) of Kaspersky Anti-Virus if it is not running, using the following command:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --start-task 12
```

Then you will be able to access MIB objects of Kaspersky Anti-Virus and obtain information over SNMP using OID objects. Kaspersky Anti-Virus package includes MIB files containing symbolic names of objects, events and their

settings. After Kaspersky Anti-Virus installation MIB files can be found in the `/opt/kaspersky/kav4fs/share/snmp-mibs` directory.

➤ To use symbolic names for access to the MIB objects of Kaspersky Anti-Virus,

provide to the SNMP master agent access to the MIB files of Kaspersky Anti-Virus.

To view the structure of Kaspersky Anti-Virus MIB using the `snmpwalk` command, add the following line to the configuration file `snmpd.conf`:

```
view systemview included .3/1/06.4/1/01.23668.1046
```

SNMP allows access to the activity statistics and traps for the events occurring during operation of Kaspersky Anti-Virus. You can enable or disable traps in Kaspersky Anti-Virus.

➤ To enable or disable event traps in Kaspersky Anti-Virus,

assign the value **yes/no** to the **TrapsEnable** parameter.

STRUCTURE OF THE KASPERSKY ANTI-VIRUS MIB

KAV4LinuxFS

Events

- ApplicationStartedEvent
- ApplicationSettingsChangedEvent
- LicenseInstalledEvent
- LicenseNotInstalledEvent
- LicenseRevokedEvent
- LicenseNotRevokedEvent
- LicenseExpiredEvent
- LicenseExpiresSoonEvent
- LicenseErrorEvent
- AVBasesAttachedEvent
- AVBasesAppliedEvent
- AVBasesAreOutOfDateEvent
- AVBasesAreTotallyOutOfDateEvent
- AVBasesIntegrityCheckFailedEvent
- AVBasesRollbackCompletedEvent
- AVBasesRollbackErrorEvent
- NothingToUpdateEvent
- ModuleNotDownloadedEvent
- RetranslationErrorEvent
- ThreatDetectedEvent
- ObjectDisinfectedEvent
- ObjectDeletedEvent
- TaskStateChangedEvent
- ObjectMovedToQuarantineEvent
- UpdateErrorEvent

Statistics

AVBackupStatistics	ObjectsInBackup
	RestoredObjects
	RemovedObjects
	InfectedObjects
	SuspiciousObjects
AVOASTasksStatistics	ScannedObjects
	InfectedObjects
	SuspiciousObjects

	<ul style="list-style-type: none"> ThreatsFound CuredObjects NotCuredObjects PasswordProtectedObjects CorruptedObjects MovedToQuarantine RemovedObjects ScanErrors
AVODSTasksStatistics	
	<ul style="list-style-type: none"> ScannedObjects InfectedObjects SuspiciousObjects ThreatsFound CuredObjects NotCuredObjects PasswordProtectedObjects CorruptedObjects MovedToQuarantine RemovedObjects ScanErrors
AVProductInfo	
	<ul style="list-style-type: none"> Name Version InstallationDate LicenseState LicenseExpireDate
AVProductStatistics	
	<ul style="list-style-type: none"> ScannedObjects InfectedObjects SuspiciousObjects ThreatsFound CuredObjects NotCuredObjects PasswordProtectedObjects CorruptedObjects MovedToQuarantine RemovedObjects ScanErrors
AVQuarantineStatistics	
	<ul style="list-style-type: none"> ObjectsInQuarantine AutoSavedObjects ManuallySavedObjects RestoredObjects RemovedObjects InfectedObjects SuspiciousObjects CurableObjects PasswordProtectedObjects CorruptedObjects
AVUpdateStatistics	
	<ul style="list-style-type: none"> CurrentAVBasesDate LastUpdateAVBasesDate CurrentBasesState CurrentBasesRecords UpdateAttempts SuccessfulUpdates FailedUpdates
AVVirusesStatistics	

AVVirusesStatisticsTable

VirusName

InfectedObjects

DESCRIPTION OF KASPERSKY ANTI-VIRUS MIB OBJECTS

The database of Kaspersky Anti-Virus objects in the SNMP tree has been assigned the following character name: *iso.org.dod.internet.private.enterprises.kaspersky.kav4LinuxFS*. Character names of Kaspersky Anti-Virus MIB objects are shown in the tables below.

Character names are specified in relation to the Kaspersky Anti-Virus identifier.

Kaspersky Anti-Virus events

Table 6. Kaspersky Anti-Virus events

CHARACTER NAME	DESCRIPTION
Events.ApplicationStartedEvent	Kaspersky Anti-Virus is running; this event occurs after all services necessary for the Anti-Virus operation are started.
Events.ApplicationSettingsChangedEvent	General settings of Kaspersky Anti-Virus have been changed.
Events.LicenseInstalledEvent	The key file has been installed.
Events.LicenseNotInstalledEvent	The key file has not been installed.
Events.LicenseRevokedEvent	The key file has been successfully deleted.
Events.LicenseNotRevokedEvent	The key file has not been deleted.
Events.LicenseExpiredEvent	The license period has expired.
Events.LicenseExpiresSoonEvent	The license period will soon expire.
Events.LicenseErrorEvent	A licensing system error has occurred.
Events.AVBasesAttachedEvent	Kaspersky Anti-Virus databases have been successfully downloaded to the server.
Events.AVBasesAppliedEvent	Kaspersky Anti-Virus databases have been successfully connected and are being used.
Events.AVBasesAreOutOfDateEvent	Kaspersky Anti-Virus databases are outdated.
Events.AVBasesAreTotallyOutOfDateEvent	Kaspersky Anti-Virus databases are obsolete.
Events.AVBasesIntegrityCheckFailedEvent	Kaspersky Anti-Virus databases are damaged.
Events.AVBasesRollbackCompletedEvent	Rollback to the previous version of Kaspersky Anti-Virus database completed successfully.
Events.AVBasesRollbackErrorEvent	Error while rolling back to the previous version of Kaspersky Anti-Virus database.
Events.NothingToUpdateEvent	No update required.
Events.UpdateErrorEvent	An error occurred while updating.
Events.ModuleNotDownloadedEvent	An error occurred while downloading an updated program module.
Events.RetranslationErrorEvent	Distribution error.
Events.TaskStateChangedEvent	Task status has changed.
Events.ThreatDetectedEvent	A threat has been detected.
Events.ObjectDeletedEvent	The object has been deleted.

CHARACTER NAME	DESCRIPTION
Events.ObjectDisinfectedEvent	The object has been disinfected.
Events.ObjectMovedToQuarantineEvent	Object quarantined.

All statistics is collected since the Kaspersky Anti-Virus installation.

Backup storage statistics

Table 7. Backup storage statistics

CHARACTER NAME	DESCRIPTION
Statistics.AVBackupStatistics.ObjectsInBackup	Number of objects in the storage.
Statistics.AVBackupStatistics.RestoredObjects	Number of objects restored from the storage.
Statistics.AVBackupStatistics.RemovedObjects	Number of objects deleted from the storage.
Statistics.AVBackupStatistics.InfectedObjects	Number of infected objects in the storage.
Statistics.AVBackupStatistics.SuspiciousObjects	Number of suspicious objects in the storage.

The number of objects in the storage refers not to the number of objects located in it, deleted or restored from it at the given moment, but to the number of objects placed in it, deleted and restored from it during the period of gathering statistics.

Statistics of the real-time protection task

Table 8. Statistics of the real-time protection task operation

CHARACTER NAME	DESCRIPTION
Statistics.AVOASTasksStatistics.ScannedObjects	The number of scanned objects.
Statistics.AVOASTasksStatistics.ThreatsFound	Total number of detected malicious programs.
Statistics.AVOASTasksStatistics.InfectedObjects	The number of infected objects.
Statistics.AVOASTasksStatistics.SuspiciousObjects	The number of suspicious objects.
Statistics.AVOASTasksStatistics.CuredObjects	The number of objects cured.
Statistics.AVOASTasksStatistics.MovedToQuarantine	The number of objects transferred to quarantine.
Statistics.AVOASTasksStatistics.RemovedObjects	The number of deleted objects.
Statistics.AVOASTasksStatistics.NotCuredObjects	The number of objects that could not be cured.
Statistics.AVOASTasksStatistics.ScanErrors	The number of errors that have occurred during the scan.
Statistics.AVOASTasksStatistics.PasswordProtectedObjects	Number of password-protected objects.
Statistics.AVOASTasksStatistics.CorruptedObjects	The number of corrupted objects

On-demand scan tasks statistics

Statistics of the on-demand scan tasks is collected for all tasks.

Table 9. Statistics of the on-demand scan tasks

CHARACTER NAME	DESCRIPTION
Statistics.AVODSTasksStatistics.ScannedObjects	The number of scanned objects.
Statistics.AVODSTasksStatistics.ThreatsFound	Total number of detected malicious programs.
Statistics.AVODSTasksStatistics.InfectedObjects	The number of infected objects.
Statistics.AVODSTasksStatistics.SuspiciousObjects	The number of suspicious objects.
Statistics.AVODSTasksStatistics.CuredObjects	The number of objects cured.
Statistics.AVODSTasksStatistics.MovedToQuarantine	The number of objects transferred to quarantine.
Statistics.AVODSTasksStatistics.RemovedObjects	The number of deleted objects.
Statistics.AVODSTasksStatistics.NotCuredObjects	The number of objects that could not be cured.
Statistics.AVODSTasksStatistics.ScanErrors	The number of errors that have occurred during the scan.
Statistics.AVODSTasksStatistics.PasswordProtectedObjects	Number of password-protected objects.
Statistics.AVODSTasksStatistics.CorruptedObjects	The number of corrupted objects

Kaspersky Anti-Virus statistics

Table 10. General information about the application

CHARACTER NAME	DESCRIPTION
Statistics.AVProductInfo.Name	Application name.
Statistics.AVProductInfo.Version	Program version.
Statistics.AVProductInfo.InstallDate	Application installation date.
Statistics.AVProductInfo.LicenseState	The license state.
Statistics.AVProductInfo.LicenseExpireDate	License expiration date.

Statistics of the Kaspersky Anti-Virus operation

Table 11. Statistics of the application operation

CHARACTER NAME	DESCRIPTION
Statistics.AVProductStatistics.ScannedObjects	The number of scanned objects.
Statistics.AVProductStatistics.ThreatsFound	Total number of detected malicious programs.
Statistics.AVProductStatistics.InfectedObjects	The number of infected objects.
Statistics.AVProductStatistics.SuspiciousObjects	The number of suspicious objects.
Statistics.AVProductStatistics.CuredObjects	The number of objects cured.
Statistics.AVProductStatistics.MovedToQuarantine	The number of objects transferred to quarantine.
Statistics.AVProductStatistics.RemovedObjects	The number of deleted objects.
Statistics.AVProductStatistics.NotCuredObjects	The number of objects that could not be cured.
Statistics.AVProductStatistics.ScanErrors	The number of errors that have occurred during the scan.
Statistics.AVProductStatistics.PasswordProtectedObjects	Number of password-protected objects.
Statistics.AVProductStatistics.CorruptedObjects	The number of corrupted objects

Quarantine statistics

Table 12. Quarantine statistics

CHARACTER NAME	DESCRIPTION
Statistics.AVQuarantineStatistics.ObjectsInQuarantine	The number of objects in quarantine.
Statistics.AVQuarantineStatistics.AutoSavedObjects	The number of automatically quarantined objects.
Statistics.AVQuarantineStatistics.ManuallySavedObjects	The number of manually quarantined objects.
Statistics.AVQuarantineStatistics.RestoredObjects	Number of objects restored from the quarantine.
Statistics.AVQuarantineStatistics.RemovedObjects	Number of objects deleted from the quarantine.
Statistics.AVQuarantineStatistics.InfectedObjects	The number of infected objects in quarantine.
Statistics.AVQuarantineStatistics.SuspiciousObjects	The number of suspicious objects in quarantine.
Statistics.AVQuarantineStatistics.CuredObjects	The number of cured objects in quarantine.
Statistics.AVQuarantineStatistics.PasswordProtectedObjects	The number of password-protected objects in quarantine.
Statistics.AVQuarantineStatistics.CorruptedObjects	The number of corrupted objects in quarantine.
Statistics.AVQuarantineStatistics.FalseDetectedObjects	The number of falsely recognized objects in quarantine.

The number of objects in quarantine refers not to the number of objects located in it, deleted or restored from it at the given moment, but to the number of objects placed in it, deleted and restored from it during the period of gathering statistics.

Update statistics

Table 13. Update statistics

CHARACTER NAME	DESCRIPTION
Statistics.AVUpdateStatistics.CurrentAVBasesDate	Issue date of the current Kaspersky Anti-Virus database.
Statistics.AVUpdateStatistics.LastUpdateAVBasesDate	Date of the most recent update of the Kaspersky Anti-Virus database.
Statistics.AVUpdateStatistics.CurrentBasesState	Kaspersky Anti-Virus database state.
Statistics.AVUpdateStatistics.CurrentBasesRecords	Number of records in the Kaspersky Anti-Virus databases.
Statistics.AVUpdateStatistics.UpdateAttempts	Number of update attempts.
Statistics.AVUpdateStatistics.SuccessfulUpdates	Number of successful update attempts.
Statistics.AVUpdateStatistics.UpdateManualStops	Number of manual update stops.
Statistics.AVUpdateStatistics.FailedUpdates	Number of incomplete updates due to errors.

Virus activity statistics

Table 14. Virus activity statistics

CHARACTER NAME	DESCRIPTION
Statistics.AVVirusesStatistics.AVVirusesStatisticsTable.AVVirusName	Name of a virus.
Statistics.AVVirusesStatistics.LastUpdateAVBasesDate	Number of objects, in which a virus was

CHARACTER NAME	DESCRIPTION
	detected.

MANAGING KASPERSKY ANTI-VIRUS FROM THE COMMAND LINE

Apply the following rules when entering the Anti-Virus commands:

- Please remember that commands are case-sensitive.
- Delimit the keys with the space character.
- Using brief (literal) command or key name, enter the value immediately following the command or a space. Using full command or key name, enter the value following the symbol "equal to" (=) or a space.

The list of Anti-Virus commands is provided in the table below.

Table 15. List of Kaspersky Anti-Virus commands

COMMANDS	DESCRIPTION
--help (see page 81)	Displays Kaspersky Anti-Virus command help.
Kaspersky Anti-Virus management commands	
--start-app (see page 82)	Starts Kaspersky Anti-Virus.
--restart-app (see page 82)	Restarts Kaspersky Anti-Virus.
--stop-app (see page 82)	Stops Kaspersky Anti-Virus.
--scan-file (see page 83)	Scans files or directories.
-R (see page 83)	Rolls back to previous databases.
Commands for obtaining Anti-Virus statistics	
-S	This prefix indicates that the command is one of a group of commands for obtaining statistics (optional).
-S --app-info (see page 84)	Outputs information about Kaspersky Anti-Virus.
-S --get-stat (see page 84)	Creates reports about the operation of Kaspersky Anti-Virus and its components.
-S --top-viruses (see page 86)	Creates reports on threats that are most commonly encountered on the server.
-S --clean-stat	Deletes statistics about Kaspersky Anti-Virus operation.
Kaspersky Anti-Virus event display commands	
-W (see page 82)	Enables output of Kaspersky Anti-Virus events.
Commands for managing the Anti-Virus settings and tasks	
-T	This prefix indicates that the command is one of a group of commands for managing the Kaspersky Anti-Virus settings and tasks (optional).
-T --get-app-settings (see page 87)	Outputs general Kaspersky Anti-Virus settings.
-T --set-app-settings (see page 88)	Defines general Kaspersky Anti-Virus settings.

COMMANDS	DESCRIPTION
-T --get-task-list (see page 89)	Returns the list of existing Kaspersky Anti-Virus tasks.
-T --get-task-state	Outputs the state of selected task (for example, In progress, Stopped, or Paused).
-T --start-task (see page 91)	Starts the task.
-T --stop-task (see page 92)	Stops the task.
-T --suspend-task (see page 92)	Pauses the task.
-T --resume-task (see page 93)	Resumes the task.
-T --get-settings (see page 93)	Outputs task settings.
-T --set-settings (see page 94)	Defines task settings.
-T --create-task (see page 95)	Creates a task of specified type; imports task settings from the specified configuration file.
-T --delete-task (see section "Deleting tasks" on page 96)	Deletes the task.
-T --set-schedule (see page 96)	Sets task scheduling settings or imports them from a configuration file.
-T --get-schedule (see page 97)	Outputs task scheduling settings.
-T --del-schedule	Deletes the task schedule.
-T --show-schedule (see page 98)	Searches for past scheduled events.
Licenses management commands	
-L	This prefix indicates that the command is one of a group of commands for managing licenses (optional).
-L --validate-key (see page 99)	Authenticates the license using the Kaspersky Lab database and outputs information from a key file to the console without installing the license.
-L --show-license-info	Outputs information about the license from the key file without installing the license.
-L --get-installed-keys (see page 101)	Outputs information about installed licenses.
-L --query-status (see page 99)	Outputs the status of installed licenses.
-L --install-active-key (see page 102)	Installs an active license.
-L --install-suppl-key (see page 102)	Installs a supplementary license.
-L --revoke-active-key (see page 103)	Deletes an active license.
-L --revoke-suppl-key (see page 103)	Deletes a supplementary license.
Quarantine and backup storage management commands	
-Q	This prefix indicates that the command is one of a group of commands for managing the quarantine and backup storage (optional).
-Q --get-stat (see page 104)	Outputs brief storage statistics.
-Q --query (see page 104)	Displays information about storages objects.
-Q --get-one (see page 105)	Displays information about one object in the storage.

COMMANDS	DESCRIPTION
-Q --restore (see page 105)	Restores an object from the storage.
-Q --add-object (see page 105)	Places a copy of the object to quarantine.
-Q --remove (see page 106)	Deletes the object from storage.
-Q --export (see page 106)	Exports objects from storage into a specified directory.
-Q --import (see page 107)	Imports objects into the storage from a specified directory, into which they were previously exported.
-Q --mass-remove (see page 107)	Removes some or all objects from the storage.
Logs management commands	
-E	This prefix indicates that the command is one of a group of commands for managing logs (optional).
-E --count (see page 108)	Outputs the number of events matching the filter defined in the event log or specified rotation file.
-E --query (see page 109)	Outputs information about events matching the filter defined in the event log or specified rotation file.
-E --period (see page 110)	Outputs to the console the time interval, during which events will occur that are stored in the event log or the specified rotation file.
-E --rotate (see page 110)	Rotates the event log.
-E --remove (see page 110)	Removes events from the log or the specified rotation file.

DISPLAYING KASPERSKY ANTI-VIRUS COMMAND HELP

The `kav4fs-control --help` command displays Kaspersky Anti-Virus command help.

Command syntax

```
kav4fs-control --help [<set of Anti-Virus commands>]
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
<set of Kaspersky Anti-Virus commands>	<p>Specify the set of Anti-Virus commands about which you want to receive information. Possible values include:</p> <ul style="list-style-type: none"> -T [--task-and-settings] – commands managing the tasks and general settings of Kaspersky Anti-Virus; -L [--licenser] – license management commands; -Q [--quarantine-and-backup] are quarantine and backup storage management commands; -S [--statistics] – commands managing the Anti-Virus statistics; -E [--event-log] are application event management commands.

STARTING KASPERSKY ANTI-VIRUS

Before taking the actions or using the commands described above, make sure that the kav4fs-supervisor service is running on the computer!

The kav4fs-control --start-app command starts Kaspersky Anti-Virus.

Command syntax

```
kav4fs-control --start-app
```

STOPPING KASPERSKY ANTI-VIRUS

Before taking the actions or using the commands described above, make sure that the kav4fs-supervisor service is running on the computer!

The kav4fs-control --stop-app command stops Kaspersky Anti-Virus.

Command syntax

```
kav4fs-control --stop-app
```

RESTARTING KASPERSKY ANTI-VIRUS

Before taking the actions or using the commands described above, make sure that the kav4fs-supervisor service is running on the computer!

The kav4fs-control --restart-app command starts Kaspersky Anti-Virus.

Command syntax

```
kav4fs-control --restart-app
```

ENABLING EVENTS OUTPUT

The -W command enables output of Kaspersky Anti-Virus events. You can use this command either by itself, to output all Anti-Virus events, or together with the --start-task command (see page 91), so as to output only events associated with the task being executed.

Event name and additional event information will be returned.

Command syntax

```
kav4fs-control -W [--file=<file name>]
```

Command example

➤ *Enable output of Kaspersky Anti-Virus events:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -W
```

- Enable saving of the Anti-Virus events to a file, for example, save events in a file named 081808.xml in the current directory:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
-W --file 081808.xml
```

KEY	DESCRIPTION AND POSSIBLE VALUES
--file <file name>	The log file name in which the information about Anti-Virus events will be stored. The saved log file has XML format.

QUICK SCAN OF FILES AND DIRECTORIES

The command kav4fs-control with the key --scan-file performs a quick scan of files and directories.

Command syntax

```
kav4fs-control --action <action> --scan-file <path to the file or directory>[ <path to  
the file or directory> ...]
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
--scan-file <path to file or directory>	Names of files and directories that will be quickly scanned by Kaspersky Anti-Virus.
--action <action>	Optional key. Available values: <ul style="list-style-type: none"> • Recommended – perform recommended action. • Cure. • Quarantine. • Remove. • Skip. Default value: Skip .

ROLLBACK OF KASPERSKY ANTI-VIRUS DATABASES

The Kaspersky Anti-Virus creates backup copies of the original databases before it applies updates. If an update procedure gets interrupted or fails, the Kaspersky Anti-Virus automatically reverts to the previous database version containing updates installed earlier.

If you encounter problems after database update, you can roll back the databases to the previous version.

The rollback to previous database version task performs a rollback to the back-up copy of the Kaspersky Anti-Virus databases.

Task start syntax

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -R
```

COMMANDS FOR OBTAINING REPORTS AND STATISTICS

IN THIS SECTION

Viewing application information	84
Viewing Anti-Virus activity reports	84
Viewing reports on the most commonly encountered threats	86

VIEWING APPLICATION INFORMATION

The `--app-info` command displays information about Kaspersky Anti-Virus.

Command syntax

```
kav4fs-control [-S] --app-info
```

This command outputs the following information:

FIELD	DESCRIPTION
Name	Kaspersky Anti-Virus name
Version	Kaspersky Anti-Virus version
Install date	Date and time of the last Anti-Virus installation
License state	The license state
License expire date	License expiration date

VIEWING ANTI-VIRUS ACTIVITY REPORTS

The `--get-stat` command displays Anti-Virus operating statistics to the console, permits generation of reports on the operation of individual Anti-Virus components over a specified time period, and allows reports to be saved in a file.

Command syntax

```
kav4fs-control [-S] --get-stat <Kaspersky Anti-Virus component> \
[--from=<start date>][--to=<end date>] \
[--task-id=<ID task (only for on-demand scan and update)>] \
[--export-report=<report file name>] [--report-type=<report file format>] \
[--use-name]
```

Command example

- *To view the operation statistics of Kaspersky Anti-Virus:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-stat Application
```

- *To view real-time protection statistics for January 2009:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
```

--get-stat OAS --from=2009-01-01 --to=2009-01-31

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
<Kaspersky Anti-Virus component>	<p>Specify the Anti-Virus component that you want to obtain statistics for. Possible values include:</p> <ul style="list-style-type: none"> Application – an application; OAS – real-time protection; ODS – on-demand scan; Quarantine – quarantine; Backup – backup storage; Update – update.
--from=<start date>	<p>The report starting date. You can assign the following values:</p> <ul style="list-style-type: none"> • date, formatted as YYYY-MM-DD (or YYYY/MM/DD or YYYY.MM.DD), to obtain information starting at midnight (00:00) of the specified date; • date and time, formatted as YYYY-MM-DD HH:MM:SS, to obtain information starting at the specified time on the specified date; • time, formatted as HH:MM:SS, to obtain information starting at the specified time of the current day. <p>If you do not specify the --from=<start date> argument, the report will collect information from the time the Anti-Virus was installed.</p>
--to=<end date>	<p>The report ending date. You can assign the following values:</p> <ul style="list-style-type: none"> • date, formatted as YYYY-MM-DD (or YYYY/MM/DD or YYYY.MM.DD), to obtain information until the specified date, inclusive; • date and time, formatted as YYYY-MM-DD HH:MM:SS, to obtain information up to the specified time on the specified date; • time, formatted as HH:MM:SS, to obtain information up to the specified time of the current day. <p>If you do not specify the --to=<end date> argument, the report will collect information up to the current time.</p>
--task-id=<task ID (only for on-demand scan and update tasks)>	<p>The identification number of the Kaspersky Anti-Virus on-demand scan task.</p> <p>The report will include statistics from the on-demand scan or update task having the specified ID number for the period since the most recent start of the task.</p> <p>This argument is not used together with --from=<start date> and --to=<end date> keys.</p>
--export-report=<report filename>	<p>Optional key. The file name in which the obtained report will be stored. If you specify only a file name without specifying a path to it, then the configuration file will be created in the current directory. If the file with the name specified already exists at the location pointed at the specified path, such file will be overwritten. If the directory specified does not exist on this drive, the file will not be created.</p> <p>You can save the report file in HTML or CSV format and assign it the HTML or CSV extension. If you additionally describe the file format using the --report-type key, you can assign the file any extension.</p>
--report-type=<report file format>	<p>Optional key. By default, the format of the file specified by the --export-report key will be determined by its extension. Specify this key if you specified any file extension other than HTML or CSV. Possible key values: HTML, CSV.</p>
--use-name	<p>Optional key. Task name.</p> <p>This argument is not used together with --task-id=<task ID>.</p>

VIEWING REPORTS ON THE MOST COMMONLY ENCOUNTERED THREATS

The `--top-viruses` command displays information about which malicious programs were found in greatest numbers on the server during the specified time interval. This information is displayed on the console and may be saved in a report file.

Command syntax

```
kav4fs-control [-S] --top-viruses <the number of malicious programs> \
[--from=<start date>][--to=<end date>][--export-report=<file name>] \
[--report-type=<report file format>]
```

Command example

- ◆ To obtain information on the five most commonly encountered malicious programs found on the server in January 2009, and save a report in the `/home/kavreports/2009_01_top_viruses.html` file:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--top-viruses 5 --from=2009-01-01 --to=2009-01-31 \
--export-report=/home/kavreports/2009_01_top_viruses.html
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
<the number of malicious programs>	The number of malicious programs. The report will include information only on the specified number of malicious programs most commonly encountered on the server.
--from=<start date>	The report starting date. You can assign the following values: <ul style="list-style-type: none"> • date, formatted as YYYY-MM-DD (or YYYY/MM/DD or YYYY.MM.DD), to obtain information starting at midnight (00:00) of the specified date; • date and time, formatted as YYYY-MM-DD HH:MM:SS, to obtain information starting at the specified time on the specified date; • time, formatted as HH:MM:SS, to obtain information starting at the specified time of the current day. If you do not specify the <code>--to=<end date></code> argument, the report will collect information up to the current time.
--to=<end date>	The report ending date. You can assign the following values: <ul style="list-style-type: none"> • date, formatted as YYYY-MM-DD (or YYYY/MM/DD or YYYY.MM.DD), to obtain information until the specified date, inclusive; • date and time, formatted as YYYY-MM-DD HH:MM:SS, to obtain information up to the specified time on the specified date; • time, formatted as HH:MM:SS, to obtain information up to the specified time of the current day. If you do not specify the <code>--from=<start date></code> argument, the report will collect information from the time the Anti-Virus was installed.
--export-report=<report filename>	Optional key. The file name in which the obtained report will be stored. If you specify only a file name without specifying a path to it, then the configuration file will be created in the current directory. If the file with the name specified already exists at the location pointed at the specified path, such file will be overwritten. If the directory specified does not exist on this drive, the report file will not be created. <p>You can save the report file in HTML or CSV format and assign it the HTML or CSV extension. If you additionally describe the file format using the <code>--report-type</code> key, you can assign the file any extension.</p>

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
<the number of malicious programs>	The number of malicious programs. The report will include information only on the specified number of malicious programs most commonly encountered on the server.
--report-type=<report file format>	Optional key. By default, the format of the file specified by the --export-report key shall be determined by its extension. Specify this key if you specified any file extension other than HTML or CSV. Possible key values: HTML, CSV.

COMMANDS FOR MANAGING THE ANTI-VIRUS SETTINGS AND TASKS

IN THIS SECTION

Viewing general settings of Kaspersky Anti-Virus	87
Editing the general settings of Kaspersky Anti-Virus	88
Viewing the list of Kaspersky Anti-Virus tasks	89
Viewing task state	90
Starting the task	91
Stopping the task	92
Pausing the task	92
Resuming the task	93
Obtaining task settings	93
Modifying task settings	94
Creating a task	95
Deleting tasks	96
Obtaining task schedule settings	96
Modifying task schedule settings	97
Searching for scheduled events	98

VIEWING GENERAL SETTINGS OF KASPERSKY ANTI-VIRUS

The --get-app-settings command outputs general settings of Kaspersky Anti-Virus (see page [145](#)). Using this command, you can also obtain the general settings of Kaspersky Anti-Virus that are defined using command-line arguments.

You can use this command to modify general settings of Kaspersky Anti-Virus installed on the server:

1. Save general Anti-Virus settings to a configuration file using the --get-app-settings command.
2. Open the configuration file created, modify the required settings and save the changes made.

3. Import the settings from the configuration file into Kaspersky Anti-Virus using the `--set-app-settings` command (see page [88](#)). Kaspersky Anti-Virus will apply new configuration settings after you stop and then start it again using the `--stop-app` and `--start-app` commands.

You can use the configuration file created to import the settings into Kaspersky Anti-Virus installed on another server.

Command syntax

```
kav4fs-control [-T] \
--get-app-settings [--file=<configuration file name>] \
--file-format=<INI|XML>
kav4fs-control [-T] --get-app-settings <setting name>
```

Command example

- *Export general Anti-Virus settings into the file with `kav_config.xml` name. Save the file created in the current directory:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-app-settings -F kav_config.xml
```

- *Output the `TraceLevel` setting value:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--get-app-settings TraceLevel
```

KEYS	DESCRIPTION AND POSSIBLE VALUES
<code>--file=<configuration file name></code> <code>-F <configuration file name></code>	<p>Name of the configuration file in which the Anti-Virus settings will be saved. If you specify only a file name without specifying a path to it, then the configuration file will be created in the current directory. If the file with the name specified already exists at the location pointed at the specified path, such file will be overwritten. If the directory specified does not exist on this drive, the configuration file will not be created.</p> <p>You can save the configuration file in XML or INI format. You can assign to the file XML or INI extension or, if you provide an additional description of the file format using the <code>--file-format</code> key, you can assign any extension to the file.</p>
<code>--file-format=<INI XML></code>	<p>Optional key. By default, the format of the configuration file specified by the <code>-F</code> key shall be determined by its extension. Specify this key if the configuration file's extension will be different from its format. Possible values: XML, INI.</p>

EDITING THE GENERAL SETTINGS OF KASPERSKY ANTI-VIRUS

The `--set-app-settings` command modifies general Anti-Virus settings using command-line arguments or imports them from a specified configuration file (see page [145](#)).

You can use this command to modify the general settings of Kaspersky Anti-Virus:

1. Save the general settings of Kaspersky Anti-Virus to a configuration file using the `--get-app-settings` command (see page [87](#)).
2. Open the configuration file created, modify the required settings and save the changes made.
3. Import the settings from a configuration file into the Anti-Virus using the `--set-app-settings` command. Kaspersky Anti-Virus will apply new configuration settings after you stop and then start it again using the `--stop-app` and `--start-app` commands or with the help of the `--restart-app` command.

Command syntax

```
kav4fs-control [-T] --set-app-settings \
--file=<configuration file name> \
--file-format=<INI|XML>
kav4fs-control [-T] \
--set-app-settings <setting name>=<setting value> \
<setting name>=<setting value>
```

Command example

➤ *Import the general settings into the Anti-Virus from the configuration file with the /home/test/kav_config.xml name:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-app-settings -F /home/test/kav_config.xml
```

➤ *Set the level of detail in the "Important events" trace log:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--set-app-settings TraceLevel=Warning
```

KEYS	DESCRIPTION AND POSSIBLE VALUES
--file=<configuration file name> -F <configuration file name>	Name of the source configuration file, which will be imported into the Anti-Virus; it includes full path to the file.
--file-format=<INI XML>	Optional key. By default, the format of the configuration file specified by the -F key shall be determined by its extension. Specify the key if the format of the configuration file does not match its extension. Possible values: XML, INI.

VIEWING THE LIST OF KASPERSKY ANTI-VIRUS TASKS

The --get-task-list command returns the list of existing Kaspersky Anti-Virus tasks.

Command syntax

```
kav4fs-control [-T] --get-task-list
```

The following information about Kaspersky Anti-Virus tasks will be displayed:

FIELD	DESCRIPTION
Name	Task name; the user defines the name of a custom task when it is created (names of system tasks are assigned by the Anti-Virus).
Id	Task ID number (ID, alternative name, which Kaspersky Anti-Virus assigns to a task being created).
Class	Type of a Kaspersky Anti-Virus task. The setting can assume the following values: <ul style="list-style-type: none"> tasks, which users can manage: <ul style="list-style-type: none"> Update – predefined update task (ID=6); OAS – real-time protection task (ID=8); ODS – predefined on-demand scan task (ID=9); QS – task for scanning of quarantined objects (ID=10); service tasks:

	<p>EventManager – implements message exchange within the program (ID=1);</p> <p>AVS – anti-virus scan service task (ID=2);</p> <p>Quarantine – manages quarantine and backup (ID=3);</p> <p>Statistics – collects statistics (ID=4);</p> <p>License – implements the license server (ID=5);</p> <p>Notifier – controls delivery of notifications and performance of configured actions upon specified events (ID=7);</p> <p>EventStorage – implements the events log service (ID=11);</p> <p>Snmp plugin – provides for delivery of information about the program via SNMP (ID=12).</p>
State	<p>Task status. Available values:</p> <p>Stopped – the task is stopped;</p> <p>Stopping – the task is stopping;</p> <p>Started – the task is in progress;</p> <p>Starting – the task is starting;</p> <p>Suspended – the task is suspended;</p> <p>Suspending – the task is suspending;</p> <p>Resumed – the task has been resumed;</p> <p>Resuming – the task is resuming;</p> <p>Failed – the task has terminated with an error.</p>

VIEWING TASK STATE

The --get-task-state command returns the status of the specified task (for example, Running, Stopped and Paused).

Command syntax

```
kav4fs-control [-T] --get-task-state <task ID>
```

Command example

➤ Obtain the status of the task with ID=9:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-task-state 9
```

ARGUMENT	DESCRIPTION AND POSSIBLE VALUES
<task ID>	Specify the task ID number (ID, alternative name, which Kaspersky Anti-Virus assigns to a task being created). To view the Kaspersky Anti-Virus task ID numbers, use the kav4fs-control --get-task-list command (see page 89).

The following information about the task will be displayed:

FIELD	DESCRIPTION
Name	Task name; the user defines the name of a custom task when it is created (names of system tasks are assigned by the Anti-Virus).
Id	Task ID number (ID, alternative name, which Kaspersky Anti-Virus assigns to a task being

FIELD	DESCRIPTION
	created).
Class	<p>Type of a Kaspersky Anti-Virus task. The setting can assume the following values:</p> <ul style="list-style-type: none"> tasks, which users can manage: <ul style="list-style-type: none"> Update – predefined update task (ID=6); OAS – real-time protection task (ID=8); ODS – predefined on-demand scan task (ID=9); QS – task for scanning of quarantined objects (ID=10); service tasks: <ul style="list-style-type: none"> EventManager – implements message exchange within the program (ID=1); AVS – anti-virus scan service task (ID=2); Quarantine – manages quarantine and backup (ID=3); Statistics – collects statistics (ID=4); License – implements the license server (ID=5); Notifier – controls delivery of notifications and performance of configured actions upon specified events (ID=7); EventStorage – implements the events log service (ID=11); Snmp plugin – provides for delivery of information about the program via SNMP (ID=12).
State	<p>Task status. Available values:</p> <ul style="list-style-type: none"> Complete – the task is completed successfully; Stopping – the task is stopping; Started – the task is in progress; Starting – the task is starting; Suspended – the task is suspended; Suspending – the task is suspending; Resuming – the task is resuming; Failed – the task has terminated with an error; Interrupted by user – the task execution was interrupted by the user.

STARTING THE TASK

The `--start-task` command launches the task with specified ID number. This command can be used with the command-line argument `-W` (see page [82](#)), in this case information about events occurring during task execution is displayed.

Command syntax

```
kav4fs-control --start-task <task ID> --[progress] [--use-name]
```

Command example

➤ *Start the task with ID=6:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --start-task 6
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
<task ID>	Specify the task ID number (ID, alternative name, which Kaspersky Anti-Virus assigns to a task being created). To view Kaspersky Anti-Virus task ID numbers, use the -T --get-task-list command (see page 89).
--progress	Displays task progress.
--use-name	Optional key. Task name. This argument is not used together with --task-id=<task ID>.

STOPPING THE TASK

The --stop-task command stops the task with specified ID number.

Command syntax

```
kav4fs-control [-T] --stop-task <task ID> [--use-name]
```

Command example

➤ *Stop the task with ID=6:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --stop-task 6
```

ARGUMENT	DESCRIPTION AND POSSIBLE VALUES
<task ID>	Specify the task ID number (ID, alternative name, which Kaspersky Anti-Virus assigns to a task). To view Kaspersky Anti-Virus task ID numbers, use the kav4fs-control -T--get-task-list command (see page 89).
--use-name	Optional key. Task name. This argument is not used together with --task-id=<task ID>.

PAUSING THE TASK

The --suspend-task command pauses the task with specified ID number. You can pause real-time protection and on-demand scan tasks. You cannot pause update tasks.

Command syntax

```
kav4fs-control [-T] --suspend-task <task ID> [--use-name]
```

Command example

➤ *Pause the task with ID=9:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --suspend-task 9
```

ARGUMENT	DESCRIPTION AND POSSIBLE VALUES
<task ID>	Specify the task ID number (ID, alternative name, which Kaspersky Anti-Virus assigns to a task). To view Kaspersky Anti-Virus task ID numbers, use the kav4fs-control -T --get-task-list command (see page 89).
--use-name	Optional key. Task name.

ARGUMENT	DESCRIPTION AND POSSIBLE VALUES
	This argument is not used together with --task-id=<task ID>.

RESUMING THE TASK

The --resume-task command resumes the task having the specified identification number that had been suspended using the --suspend-task command (see page [92](#)).

Command syntax

```
kav4fs-control [-T] --resume-task <task ID> [--use-name]
```

Command example

- *Resume the task with ID=9:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --resume-task 9
```

ARGUMENT	DESCRIPTION AND POSSIBLE VALUES
<task ID>	Specify the task ID number (ID, alternative name, which Kaspersky Anti-Virus assigns to a task). To view Kaspersky Anti-Virus task ID numbers, use the -T --get-task-list command (see page 89).
--use-name	Optional key. Task name. This argument is not used together with --task-id=<task ID>.

OBTAINING TASK SETTINGS

The --get-settings command outputs all settings for a specified task or its settings defined in the command line options.

You can export task settings to the configuration file on one computer, and import settings (see section "Modifying task settings" on page [94](#)) from this configuration file into the task of a corresponding type on another server.

Command syntax

```
kav4fs-control [-T] --get-settings <task ID> \  
[--file=<configuration file name>] --file-format=<INI|XML> [--use-name]  
kav4fs-control [-T] --get-settings <task ID> \  
<INI file section name>.<setting value> [--use-name]
```

Command example

- *Export the settings of the task with ID=9 into the /home/test/configkavscanner.xml file:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-settings 9 -F /home/test/configkavscanner.xml
```

- *Export the settings of the task with ID=9 into the configkavscanner.xml file, located in the current directory:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-settings 9 --file=configkavscanner.xml
```

- Output to the console the value of the Path setting from the AreaPath subsection of the ScanScope section, defined in the on-demand scan task:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-settings 9 ScanScope.AreaPath.Path
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
--get-settings <task ID>	Specify the task ID number (ID, alternative name, which Kaspersky Anti-Virus assigns to a task being created). To view Kaspersky Anti-Virus task ID numbers, use the -T --get-task-list command (see page 89).
--file=<configuration file name> -F <configuration file name>	The name of the configuration file in which the task settings will be saved. If you specify only a file name without specifying a path to it, then the configuration file will be created in the current directory. If the file with the name specified already exists at the location pointed at the specified path, such file will be overwritten. If the directory specified does not exist, the configuration file will not be created. You can save the configuration file in XML or INI format. You can assign to the file XML or INI extension or, if you provide an additional description of the file format using the --file-format key, you can assign any extension to the file.
--file-format=<INI XML>	Optional key. By default, the format of the configuration file specified by the -F key shall be determined by its extension. Specify this key if you specified any file extension other than XML or INI. Possible key values: XML, INI.
--use-name	Optional key. Task name. This argument is not used together with --task-id=<task ID>.

MODIFYING TASK SETTINGS

The --set-settings command defines the configuration file task settings using command-line arguments or imports them from the specified configuration file.

You can import the settings from the configuration file into the task being executed. Kaspersky Anti-Virus will apply new configuration settings immediately in the real-time protection task and at the next task launch in the tasks of all other types.

Command syntax

```
kav4fs-control [-T] --set-settings <task ID> \  
--file=<configuration file name> --file-format=<INI|XML> [--use-name]  
kav4fs-control [-T] --set-settings <task ID> \  
<setting name>=<setting value> <setting name>=<setting value> \  
[--use-name]
```

Command example

- Import the settings from the /home/test/config_fridayscan.xml configuration file into the task with ID=9:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --set-settings 9 \  
--file=/home/test/config_fridayscan.xml
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
--set-settings <task ID>	Specify the task ID number (ID, alternative name, which Kaspersky Anti-Virus assigns to a task). To view Kaspersky Anti-Virus task ID numbers, use the -T --get-task-list command (see page 89).

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
--file=<configuration file name> -F <configuration file name>	The name of the configuration file settings of which will be imported into the task; it includes full path to the file.
--file-format=<INI XML>	Optional key. By default, the format of the configuration file specified by the -F key shall be determined by its extension. Specify the key if the extension of the specified file does not match its format. Possible values: XML, INI.
--use-name	Optional key. Task name. This argument is not used together with --task-id=<task ID>.

CREATING A TASK

The --create-task command creates a Kaspersky Anti-Virus task for the specified component; imports the settings from the specified configuration files into the task. The command returns an ID number of the task created.

You can create new on-demand scan and update tasks.

Command syntax

```
kav4fs-control [-T] --create-task <task name> \  
--use-task-type=<task type> --file=<configuration file name> \  
--file-format=<INI|XML>
```

Command examples

- Create an on-demand scan task with the Fridayscan name; import settings from the /home/test/config_kavscanner.xml configuration file into the task:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--create-task Fridayscan --use-task-type=ODS \  
--file=/home/test/config_kavscanner.xml
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
--create-task <task name> -C <task name>	Assign a name to the task. The name may contain any number of ASCII characters.
--use-task-type=<task type>	Mandatory key. Specify the type of the task being created. Available values: ODS – on-demand scan task; Update – update task.
--file=<configuration file name> -F <configuration file name>	Mandatory key for creating the Kaspersky Anti-Virus update task. Specify a full path to the existing configuration file. Anti-Virus imports the settings described in this file into the task.
--file-format=<INI XML>	Optional key. By default, the format of the configuration file specified by the -F key shall be determined by its extension. Specify the key if the extension of the specified configuration file does not match its format. Possible values: XML, INI.

DELETING TASKS

The `--delete-task` command deletes the Kaspersky Anti-Virus task with the specified ID number. You can delete on-demand scan tasks (except for the **Quarantine scan** task) and update tasks.

You cannot delete the real-time protection task.

Command syntax

```
kav4fs-control [-T] --delete-task <task ID> [--use-name]
```

Command examples

➤ *Delete the task with ID=20:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --delete-task 20
```

ARGUMENT	DESCRIPTION AND POSSIBLE VALUES
<code>--delete-task <task ID></code> <code>-D <task ID></code>	Specify the task ID number (ID, alternative name, which Kaspersky Anti-Virus assigns to a task being created). To view Kaspersky Anti-Virus task ID numbers, use the <code>-T --get-task-list</code> command (see page 89).
<code>--use-name</code>	Optional key. Task name. This argument is not used together with <code>--task-id=<task ID></code> .

OBTAINING TASK SCHEDULE SETTINGS

The `--get-schedule` command outputs the task schedule settings (see page [141](#)). Using this command, you can also obtain the task schedule settings that are defined using command-line arguments.

You can use this command to modify task schedule:

1. Save the schedule settings to a configuration file using the `-T --get-schedule` command.
2. Open the configuration file created, modify the required settings and save the changes made.
3. Import the settings from the configuration file into Anti-Virus using the `--set-schedule` command (see page [96](#)). Kaspersky Anti-Virus will apply the new schedule settings immediately.

Command syntax

```
kav4fs-control [-T] --get-schedule <task ID> \  
[--file=<configuration file name>] --file-format=<INI|XML> [--use-name]  
kav4fs-control [-T] --get-schedule <task ID> <setting name> [--use-name]
```

Command example

➤ *Save Kaspersky Anti-Virus settings into the file with `on_demand_schedule.xml` name. Save the file created in the current directory:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-schedule 9 -F on_demand_schedule.xml
```

➤ *Output `StratRules` setting value in the real-time protection task schedule:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--get-schedule 8 StartRules
```


ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
<task ID>	Identification number of a Kaspersky Anti-Virus task.
--file=<configuration file name> -F <configuration file name>	The name of the configuration file in which the schedule settings will be saved. If you specify only a file name without specifying a path to it, then the configuration file will be created in the current directory. If the file with the name specified already exists at the location pointed at the specified path, such file will be overwritten. If the directory specified does not exist on this drive, the configuration file will not be created. You can save the configuration file in XML or INI format. You can assign to the file XML or INI extension or, if you provide an additional description of the file format using the --file-format key, you can assign any extension to the file.
--file-format=<INI XML>	Optional key. By default, the format of the configuration file specified by the -F key will be determined by its extension. Specify this key if the configuration file's extension will be different from its format. Possible values: XML, INI.
--use-name	Optional key. Task name. This argument is not used together with --task-id=<task ID>.

MODIFYING TASK SCHEDULE SETTINGS

The -T --set-schedule command modifies task schedule settings using command-line arguments or imports them from a specified configuration file (see page [141](#)).

You can use this command to modify the Anti-Virus settings:

1. Save schedule settings to a configuration file using the -T --get-schedule command (see page [97](#)).
2. Open the configuration file created, modify the required settings and save the changes made.
3. Import the settings from the configuration file into the Anti-Virus using the -T --set-schedule command. Kaspersky Anti-Virus will apply the new schedule settings immediately.

Command syntax

```
kav4fs-control -T --set-schedule <task ID> --file=<configuration file name> \  
--file-format=<INI|XML> [--use-name]  
kav4fs-control -T --set-schedule <task ID> \  
<setting name>=<setting value> <setting name>=<setting value> \  
[--use-name]
```

Command example

- Import the schedule settings from configuration file named /home/test/on_demand_schedule.xml into the task with ID=9:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -T \  
--set-schedule 9 -F /home/test/on_demand_schedule.xml
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
<task ID>	Identification number of a Kaspersky Anti-Virus task.
--file=<configuration file name> -F <configuration file name>	Name of the configuration file, from which the schedule parameters will be imported into the task. The file name includes its full path.
--file-format=<INI XML>	Optional key. By default, the format of the configuration file specified by the -F key will

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
	be determined by its extension. Specify this key if the configuration file's extension will be different from its format. Possible values: XML, INI.
--use-name	Optional key. Task name. This argument is not used together with --task-id=<task ID>.

SEARCHING FOR SCHEDULED EVENTS

The -T --show-schedule command searches for scheduled events.

Command syntax

```
kav4fs-control -T --show-schedule <rule type> --from=<start date> \
--to=<date> --action=<action> --task-id=<task ID> [--use-name]
```

Command example

- Find events pertaining to task stop that are scheduled for precise time within the range from 28.03.2009 to 01.04.2009:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--show-schedule Time --from=2009-03-28 \
--to=2009-04-01 --action=Stop
```

Example of command output

Events number: 1

```
TaskId #9, Event: Stop, Date: 2009-03-30 12:00:00, Enabled, Stop Rule: [StopAt
2009/Mar/30:12:00 CanRunAfter 1800]
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
<rule type>	Schedule rule type. Available values: <ul style="list-style-type: none"> Time – rules containing the precise time (see page 145) for the task start, stop or pause. Startup – rules containing a PS condition (at Anti-Virus start). Basereload – rules containing a BR condition (upon database update).
--from=<start date>	The report starting date. You can assign the following values: <ul style="list-style-type: none"> date, formatted as YYYY-MM-DD (or YYYY/MM/DD or YYYY.MM.DD), to obtain information starting at midnight (00:00) of the specified date; date and time, formatted as YYYY-MM-DD HH:MM:SS, to obtain information starting at the specified time on the specified date; time, formatted as HH:MM:SS, to obtain information starting at the specified time of the current day. <p>If you skip the option --to=<end date>, search will cover a week period since the command execution.</p>

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
--to=<end date>	<p>The report ending date. You can assign the following values:</p> <ul style="list-style-type: none"> • date, formatted as YYYY-MM-DD (or YYYY/MM/DD or YYYY.MM.DD), to obtain information until the specified date, inclusive; • date and time, formatted as YYYY-MM-DD HH:MM:SS, to obtain information up to the specified time on the specified date; • time, formatted as HH:MM:SS, to obtain information up to the specified time of the current day. <p>If you skip the option --from=<start date>, search will begin with the command execution time.</p>
--action=<action>	<p>Action performed by a rule.</p> <p>Available values:</p> <ul style="list-style-type: none"> • Start – task start rules. • Stop – task stop rules. • Suspend – task pause rules. • Resume – task resumption rules.
--task-id=<task ID>	<p>Identification number of the task, for which schedule search is performed.</p>
--use-name	<p>Optional key. Task name.</p> <p>This argument is not used together with --task-id=<task ID>.</p>

LICENSES MANAGEMENT COMMANDS

IN THIS SECTION

Validating a key file prior to installation	99
Viewing information about a license prior to the key file installation	100
Viewing information about the installed key files	101
Viewing the status of installed licenses	102
Active key file installation	102
Supplementary key file installation	102
Active key file removal.....	103
Supplementary key file removal	103

VALIDATING A KEY FILE PRIOR TO INSTALLATION

The kav4fs-control --validate-key command uses Kaspersky Lab's database to verify if a key file is genuine and is issued for Kaspersky Anti-Virus. This command outputs information about the key file to the console, without installing it.

Command syntax

```
kav4fs-control [-L] --validate-key <path to key file>
```

Command example

➔ *Validate the license in file /home/test/00000001.key:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--validate-key /home/test/00000001.key
```

ARGUMENT	DESCRIPTION AND POSSIBLE VALUES
<path to key file>	Path to the key file; if the key file is located in the current directory. It will be enough to specify the name of the file.

This command outputs the following license information.

FIELD	DESCRIPTION
Application name	Kaspersky Anti-Virus name.
Key file creation date	License creation date.
License expiration date	Date when the license validity period completes calculated by Kaspersky Anti-Virus; it is the date when the license validity period will expire if you activate it at the moment, but not later than the date after which the key file becomes invalid.
License number	License number.
License type	License type: trial or commercial.
Usage restriction	Usage restriction. If any; the number of objects defined in the restriction.
License period	License validity period (in days) since the moment of the license release.

VIEWING INFORMATION ABOUT A LICENSE PRIOR TO THE KEY FILE INSTALLATION

The --show-license-info command outputs license information to the console without installing the key file.

Command syntax

```
kav4fs-control [-L] --show-license-info <path to key file>
```

Command example

➔ *Output license information from the /home/test/00000001.key file to the console:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--show-license-info /home/test/00000001.key
```

ARGUMENT	DESCRIPTION AND POSSIBLE VALUES
<path to key file>	Path to the key file; if the key file is located in the current directory. It will be enough to specify the name of the file.

This command outputs the following license information.

FIELD	DESCRIPTION
-------	-------------

FIELD	DESCRIPTION
Application name	Kaspersky Anti-Virus name.
Key file creation date	License creation date.
Key file expiration date	This date denotes the end of the key file "shelf life", i.e. the date on which the key file becomes invalid. This date is specified when the license is issued.
License number	License number.
License type	License type: trial or commercial.
Usage restriction	Usage restriction. If any; the number of objects defined in the restriction.
License period	License validity period (in days) since the moment of the license release.

VIEWING INFORMATION ABOUT THE INSTALLED KEY FILES

The `kav4fs-control --get-installed-keys` command outputs information about the installed key files to the console.

Command syntax

```
kav4fs-control [-L] --get-installed-keys
```

The command displays the following information about the installed key files.

FIELD	DESCRIPTION
Activation date	License activation date.
Expiration date	The date, on which the license expires, calculated by Kaspersky Anti-Virus when the license is installed. This date occurs at the end of the license validity period after the license becomes active, but not later than the key file expiration date.
Aggregate expiration date	The end date of the combined active and supplementary license validity period.
Days remaining until aggregate expiration	The number of days remaining until the end of the combined active and supplementary license validity period.
License status	The license status; may have one of the following values: Valid – the license is valid; Expired – the license has expired; Blacklisted – the license has been blacklisted; Trial period is over – the license trial period has expired.
Functionality	Anti-Virus functionality; may have one of the following values: Full functionality – the application is fully functional. Functioning without updates – the application is functioning without updates. This mode is activated upon expiration of a commercial license. No features – Anti-Virus performs none of its functions. This mode is activated upon expiration of a trial license.
Detailed license information:	
Application name	Kaspersky Anti-Virus name.
Key file creation date	Date when the key file was issued.

FIELD	DESCRIPTION
Key file expiration date	This date denotes the end of the key file "shelf life", i.e. the date on which the key file becomes invalid. This date is specified when the license is issued.
License number	License number.
License type	License type: trial or commercial.
Usage restriction	Usage restriction. If any; the number of objects defined in the restriction.
License period	License validity period (in days) since the moment of the license release.

VIEWING THE STATUS OF INSTALLED LICENSES

The `--query-status` command outputs the status of installed licenses to the console.

Command syntax

```
kav4fs-control [-L] --query-status
```

ACTIVE KEY FILE INSTALLATION

The `--install-active-key` command installs the active key file. For details on key files please refer to the "About Kaspersky Anti-Virus key files" section (see page [62](#)).

Command syntax

```
kav4fs-control [-L] --install-active-key <path to key file>
```

Command example

◆ *Install a license as an active license from the `/home/test/00000001.key` file:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--install-active-key /home/test/00000001.key
```

ARGUMENT	DESCRIPTION AND POSSIBLE VALUES
<path to key file>	Path to the key file; if the key file is located in the current directory. It will be enough to specify the name of the file.

SUPPLEMENTARY KEY FILE INSTALLATION

The `--install-suppl-key` command installs a supplementary key file. For details on key files please refer to the "About Kaspersky Anti-Virus key files" section (see page [62](#)).

If the active key file is not installed, a supplementary key file will be installed as the active key file.

Command syntax

```
kav4fs-control [-L] --install-suppl-key <path to key file>
```

Command example

➤ *Install a supplementary license from the /home/test/00000002.key file:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--install-suppl-key /home/test/00000002.key
```

ARGUMENT	DESCRIPTION AND POSSIBLE VALUES
<path to key file>	Path to the key file; if the key file is located in the current directory. It will be enough to specify the name of the file.

ACTIVE KEY FILE REMOVAL

The --revoke-active-key command removes the installed active key file.

Command syntax

```
kav4fs-control [-L] --revoke-active-key
```

SUPPLEMENTARY KEY FILE REMOVAL

The --revoke-suppl-key command removes the installed supplementary key file.

Command syntax

```
kav4fs-control [-L] --revoke-suppl-key
```

QUARANTINE AND BACKUP STORAGE MANAGEMENT COMMANDS

IN THIS SECTION

Obtaining brief quarantine or backup storage statistics.....	104
Obtaining information about storage objects	104
Obtaining information about one object in the storage	105
Restoring objects from the storage	105
Placing an object in quarantine manually	105
Deleting one object from the storage	106
Exporting objects from the storage into a specified directory	106
Importing previously exported objects into the storage	107
Clearing the storage	107

OBTAINING BRIEF QUARANTINE OR BACKUP STORAGE STATISTICS

The `--get-stat` command displays the number of objects and the overall volume of data currently in the storage.

Command syntax

```
kav4fs-control [-Q] --get-stat [--query "<logical expression>"]
```

Command example

- *To view brief quarantine statistics:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q \  
--get-stat --query "(OrigType!=s'Backup')"
```

- *To view brief backup storage statistics:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q \  
--get-stat --query "(OrigType==s'Backup')"
```

OBTAINING INFORMATION ABOUT STORAGE OBJECTS

The `--query` command displays information about objects currently in the storage. You can use filters.

Command syntax

```
kav4fs-control [-Q] --query "<logical expression>" \  
[--limit=<maximum number of records>] \  
[--offset=<offset from the query beginning>][--detailed]
```

Command example

- *To view information about storage objects:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q --query ""
```

- *To view information about objects in quarantine and display 51 entries starting with the 50th entry:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q --query "(OrigType!=s'Backup') " \  
--limit=50 --offset=50
```

- *To view information about backup storage objects:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q --query "(OrigType==s'Backup')"
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
"<logical expression>"	Creates a filter consisting of a logical expression (see page 111).
--limit=<maximum number of records>	Sets a filter: maximum number of records from query, which should be displayed.
--offset=<offset from the query beginning>	Sets a filter: maximum number of records from query, which should be skipped from the query beginning.
--detailed	Displays additional service information about objects in the repository.

OBTAINING INFORMATION ABOUT ONE OBJECT IN THE STORAGE

The `--get-one` command displays information about the storage object having the specified identification number.

Command syntax

```
kav4fs-control [-Q] --get-one <object ID> [--detailed]
```

Command example

- To obtain information about the object with ID=1:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --get-one 1
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
<object ID>	To obtain the object identification number, you can use the <code>-Q --query</code> command (see page 104).
<code>--detailed</code>	Displays additional service information about object in the repository.

RESTORING OBJECTS FROM THE STORAGE

The `--restore` command restores the object having the specified identification number from the storage.

Date and time when the file recovered from quarantine was created differs from the date and time of the original file.

Command syntax

```
kav4fs-control [-Q] --restore <identification number of storage object> \  
[--file=<file name and path to file>]
```

Command example

- To restore the object with ID=1 to its original location:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --restore 1
```

- To restore the object with ID=1 to the current directory, in a file named `restored.exe`:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --restore 1 -F restored.exe
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
<object ID>	To obtain the object identification number, you can use the <code>-Q --query</code> command (see page 104).
<code>--file=<file name></code> <code>-F <file name></code>	Name of the file in which Kaspersky Anti-Virus will save the object during restoration, it includes the file path. If you do not specify a file path, Anti-Virus will save the file in the current directory. If you omit this argument, Anti-Virus will save the object in its original location under its original name.

PLACING AN OBJECT IN QUARANTINE MANUALLY

The `--add-object` command places a copy of the object to quarantine.

Command syntax

```
kav4fs-control [-Q] --add-object <file name>
```

Command example

- *To place a copy of the /home/sample.exe file to quarantine:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--add-object /home/sample.exe
```

ARGUMENT	DESCRIPTION AND POSSIBLE VALUES
<file name>	The name of the file, a copy of which you want to place to quarantine, includes the file path.

DELETING ONE OBJECT FROM THE STORAGE

The --remove command deletes the object having the specified identification number from the storage.

Command syntax

```
kav4fs-control [-Q] --remove <object ID>
```

Command example

- *To delete the object with ID=1:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q --remove 1
```

ARGUMENT	DESCRIPTION AND POSSIBLE VALUES
<object ID>	To obtain the object identification number, you can use the -Q --query command (see page 104).

EXPORTING OBJECTS FROM THE STORAGE INTO A SPECIFIED DIRECTORY

The --export command exports objects from the storage to a specified directory. You may need to export objects from the storage to free space on the server. The location of the storage directory on the server is specified in the quarantine and backup storage configuration file (see page [147](#)).

You can use filters to export only selected objects, for example, only quarantined objects.

Command syntax

```
kav4fs-control [-Q] --export <destination directory> \  
[--query "<logical expression>"] \  
[--limit=<maximum number of records>] \  
[--offset=<offset from the query beginning>]
```

Command example

- *To export all objects from the storage to the /media/flash128/avpstorage directory:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q\  
--export /media/flash128/avpstorage
```

- To export 50 quarantined objects to the `/media/flash128/avpstorage` directory, starting with the 51st entry:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q \  
--export /media/flash128/avpstorage --query "(OrigType!=s'Backup') " \  
--limit=50 --offset=50
```

- To export all backed-up objects to the `/media/flash128/avpstorage` directory:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q \  
--export /media/flash128/avpstorage \  
--query "(OrigType==s'Backup') "
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
<destination directory>	The directory where Anti-Virus will save objects from the storage. If the directory does not exist, it will be created. You can specify a directory for remote resources mounted on the server using SMB/CIFS and NFS.
--query="<logical expression>"	Creates a filter consisting of a logical expression (see page 111).
--limit=<maximum number of records>	Sets a filter: maximum number of records from query, which should be displayed.
--offset=<offset from the query beginning>	Sets a filter: maximum number of records from query, which should be skipped from the query beginning.

IMPORTING PREVIOUSLY EXPORTED OBJECTS INTO THE STORAGE

The `--import` command imports previously exported objects into the storage.

The location of the storage directory on the server is specified in the quarantine and backup storage configuration file (see page [147](#)).

Command syntax

```
kav4fs-control [-Q] --import <directory containing exported objects>
```

Command example

- To import objects from the `/media/flash128/avpstorage` directory into the storage:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q\  
--import /media/flash128/avpstorage
```

CLEARING THE STORAGE

The `--mass-remove` command clears the storage, deleting either all or part of the contents.

Before executing this command, stop the real-time protection task and any on-demand scan tasks.

Command syntax

```
kav4fs-control [-Q] --mass-remove \  
[--query="<logical expression>"] \  
[--limit=<maximum number of records>] \  
[--offset=<offset from the query beginning>]
```

Command example

- *To delete all objects from the storage:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --mass-remove
```

- *To delete quarantined objects only, 50 entries, starting with the 51st entry:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
-Q --mass-remove --query "(OrigType!=s'Backup') " \  
--limit=50 --offset=50
```

- *To delete objects from the backup storage:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -Q \  
--mass-remove --query "(OrigType==s'Backup') "
```

KEYS	DESCRIPTION AND POSSIBLE VALUES
--query="<logical expression>"	Creates a filter consisting of a logical expression (see page 111).
--limit=<maximum number of records>	Sets a filter: maximum number of records from query, which should be displayed.
--offset=<offset from the query beginning>	Sets a filter: maximum number of records from query, which should be skipped from the query beginning.

LOGS MANAGEMENT COMMANDS

IN THIS SECTION

Obtaining the number of Anti-Virus events, using a filter [108](#)

Obtaining information about Kaspersky Anti-Virus events..... [109](#)

Viewing the time interval, during which the events will occur that are registered in the log..... [110](#)

Event log rotation [110](#)

Removing objects from the event log [110](#)

OBTAINING THE NUMBER OF ANTI-VIRUS EVENTS, USING A FILTER

The --count command outputs to the console the number of events that are stored in the event log or in the specified rotation file, using filters. This command allows estimating the data volume to be output if you enter the -E --query command (see page [109](#)).

Command syntax

```
kav4fs-control [-E] --count "<logical expression>" [--db=<rotation file>]
```

Command example

- *To obtain the number of Anti-Virus events stored in the event log:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --count ""
```

- To obtain the number of Anti-Virus events stored in the rotation file `EventStorage-2009-12-01-23-57-23.db`:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --count "" \  
--db=EventStorage-2009-12-01-23-57-23.db
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
"<logical expression>"	Creates a filter consisting of a logical expression (see page 111).
--db=<rotation file>	The rotation file, information in which you wish to view (this file has the extension .db). If you do not provide this modifier, Anti-Virus will display the number of events in the log at the moment.

OBTAINING INFORMATION ABOUT KASPERSKY ANTI-VIRUS EVENTS

The `--query` command allows obtaining information about Kaspersky Anti-Virus events from the Anti-Virus event log or from the rotation file; and it allows saving the obtained information in a file.

Command syntax

```
kav4fs-control -E --query "<logical expression>" \  
[--db=<rotation file name>][--limit=<maximum number of records>] \  
[--offset=<offset from the query beginning>][--file=<log filename>]\  
[--file-format=<log file format>]
```

Command example

- To view information on the most recent 50 quarantine events:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
-E --query "(TaskType == s'Quarantine')" --limit=50
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
"<logical expression>"	Creates a filter consisting of a logical expression (see page 111).
--db=<rotation file name>	The rotation file, information about events in which you wish to obtain (this file has the extension .db). If you do not provide this modifier, Anti-Virus will display the information from the event log.
--limit=<maximum number of records>	Sets a filter: maximum number of records from query, which should be displayed.
--offset=<offset from the query beginning>	Sets a filter: maximum number of records from query, which should be skipped from the query beginning.
--file=<log filename> -F <log filename>	Optional key. The file name in which the Anti-Virus events will be saved. If you specify only a file name without specifying a path to it, then the log file will be created in the current directory. If the file with the name specified already exists at the location pointed at the specified path, such file will be overwritten. If the directory specified does not exist on this drive, the log file will not be created. You can save log file in XML or INI format. You can assign to the log file XML or INI extension or, if you provide an additional description of the log file format using the <code>--file-format</code> key, you can assign any extension to the log file.
--file-format=<log file format>	Optional key. By default, the format of the log file specified by the <code>-F</code> key shall be determined by its extension. Specify this key if the log file extension will be different from its format. Possible values: XML, INI.

VIEWING THE TIME INTERVAL, DURING WHICH THE EVENTS WILL OCCUR THAT ARE REGISTERED IN THE LOG

This command allows you to know the time interval during which the events occur that are stored in the event log or in the specified rotation file.

Command syntax

```
kav4fs-control [-E] --period [--db=<rotation file>]
```

Command examples

- *To view the time interval during which the events occur that are stored in the event log or in the specified rotation file:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --period
```

- *To view the time interval during which the events occur that are stored in the event log or in the specified rotation file EventStorage-2009-12-01-23-57-23.db:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--period --db=EventStorage-2009-12-01-23-57-23.db
```

ARGUMENT AND KEYS	DESCRIPTION AND POSSIBLE VALUES
--db=<rotation file>	The rotation file (this file has the extension .db), information about which you wish to obtain. If you do not provide this modifier, Anti-Virus will display the information about the event log.

EVENT LOG ROTATION

The --rotate command performs forced rotation of events in the log in accordance with the RotateMethod and RotateMoveFolder settings configured in the event log configuration file (see page [148](#)).

If the RotateMethod setting has the Erase value, Anti-Virus deletes information about events from the log.

If the RotateMethod setting has the Move value, Kaspersky Anti-Virus transfers information about events from the log into the RotateMoveFolder directory and saves it in the rotation file.

Command syntax

```
kav4fs-control [-E] --rotate
```

REMOVING OBJECTS FROM THE EVENT LOG

The --remove command deletes records about events from Anti-Virus log or from the specified rotation file.

You can delete all records, or just several records, by using filters.

Command syntax

```
kav4fs-control [-E] --remove "<logical expression>" \  
[--db=<rotation file>]
```

Command example

➤ To delete from the event log only records about the events related to assigning the detected objects the status "not infected" (the ReportCleanObjects setting was enabled):

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
-E --remove "(EventType==s'ObjectProcessed') and \
(ObjectReason==s'ObjectClean'))"
```

ARGUMENT AND KEYS	DESCRIPTION AND POSSIBLE VALUES
"<logical expression>"	Creates a filter consisting of a logical expression (see page 111).
--db=<rotation file>	Rotation file, the records from which you wish to delete (this file has the extension .db). If you do not provide this modifier, Anti-Virus will delete records from Anti-Virus event log.

LIMITING SELECTIONS USING FILTERS

IN THIS SECTION

Logical expressions..... [111](#)

Object parameters in quarantine/backup storage..... [112](#)

Anti-Virus events and their data [114](#)

LOGICAL EXPRESSIONS

You can use logical expressions as an argument or a --query parameter in the following commands, in order to limit the information selected by the command:

- obtaining information about the number of Anti-Virus events: -E --count "<logical expression>" (see page [108](#));
- obtaining information about Anti-Virus events: -E --query "<logical expression>" (see page [109](#));
- obtaining information about objects in quarantine or in the backup storage: -Q --query "<logical expression>" (see page [104](#));
- obtaining concise statistical information about objects in quarantine or in the backup storage: -Q --get-stat --query "<logical expression>" (see page [104](#));
- selective removal of objects from the storage: -Q --mass-remove --query "<logical expression>" (see page [107](#));
- selective export of objects from quarantine or from the backup storage: -Q --export --query "<logical expression>" (see page [106](#)).

You can specify several filters, combining their effect using logical "AND" or "OR" operators. Enclose each filter in parenthesis and enclose each logical expression in quotes.

You can sort event (object) information by any field in ascending or descending order.

Syntax

```
"(<field> <comparison operator> <type>'<value>') {<field> <order>}"
"((<field> <comparison operator> <type>'<value>') <logical operator> (<field> <comparison
```

```
operator> <type>'<value>')) {<field> <order>}"
```

Example

➤ Obtain information about quarantined objects having the danger level High:

```
-Q --query "(DangerLevel == s'High')"
```

The following table presents a description of and possible values for logical expression elements.

ELEMENTS	DESCRIPTION AND POSSIBLE VALUES
<comparison operator>	> is greater than < is less than like matches the specified pattern == is equal to != is not equal to >= is greater than or equal to <= is less than or equal to
<logical operator>	and logical "AND" or logical "OR"
{<field><order>}	Event output order. The option is not used with the -E --query command. You can sort events on any field in ascending or descending order. For the -Q --query, -Q --get-stat and -Q --mass-remove commands you can specify as fields the parameters of objects in storage (see page 112). The order can assume the following values: a ascending d descending
<type>	i numerical s line-oriented (string)

OBJECT PARAMETERS IN QUARANTINE/BACKUP STORAGE

You can filter objects in the quarantine/backup storage by the fields described in the following table.

Table 16. Object parameters in quarantine/backup storage

FIELD	TYPE	DESCRIPTION AND POSSIBLE VALUES
Filename	s	The file name and a full path to the file. You can use masks with the aid of the 'like' comparison operator.

FIELD	TYPE	DESCRIPTION AND POSSIBLE VALUES
OrigType Type	s	<p>OrigType – the state of the object, assigned when the object is placed in the storage.</p> <p>Type – the state of an object in quarantine after it has been scanned using updated databases.</p> <p>Possible values include:</p> <ul style="list-style-type: none"> Clean – not infected; Backup – is a backup copy; Infected – infected; UserAdded – added by a user; Error – an error has occurred while scanning the object; PasswordProtected – is password-protected; Corrupted – is corrupted; Curable – the object may be disinfected.
OrigVerdict Verdict	s	<p>OrigVerdict – type of threat detected in the object when the object was placed in the storage.</p> <p>Verdict – type of threat detected in the quarantined object after scanning with updated databases.</p> <p>Possible values include:</p> <ul style="list-style-type: none"> Virware – classic viruses and network worms; Trojware – Trojan programs; Malware – other malicious programs; Adware – advertising software; Pornware – pornographic software; Riskware – potentially dangerous software.
OrigDangerLevel DangerLevel	s	<p>OrigDangerLevel – danger level of the threat detected in an object when the object was placed in the storage.</p> <p>DangerLevel – danger level of the threat in the quarantined object after scanning with updated databases.</p> <p>The danger level of an object depends on the type of threat in the object (see section "Programs detectable by Kaspersky Anti-Virus" on page 11). The danger level may assume the following values:</p> <ul style="list-style-type: none"> High. The object may contain a threat of the network worm, classical virus, or Trojan type. Medium. The object may contain some other malicious program, adware, or a program with pornographic content. Low. The object may contain a threat of riskware type. Info. The object is quarantined by the user.
OrigDetectCertainty DetectCertainty	s	<p>OrigDetectCertainty – the state of a detected object upon its placement in the storage.</p> <p>DetectCertainty – the state Anti-Virus assigns to an object in quarantine after scanning it using updated databases.</p> <p>Possible values include:</p> <ul style="list-style-type: none"> Sure – object is classified as infected; Suspicion – object is classified as suspicious (the object has been found using the

FIELD	TYPE	DESCRIPTION AND POSSIBLE VALUES
		Heuristic Analyzer); Warning – object has the status "Warning" (the object code partly coincides with the code of a known threat; a false alarm may occur).
OrigThreatName ThreatName	s	OrigThreatName – the name of the threat, based on the Kaspersky Lab classification, found in the object when the object is placed in the storage. ThreatName – the name of the threat detected in a quarantined object after scanning with updated databases. You can use masks with the aid of the 'like' comparison operator.
Compound	i	Indicates, whether the object is a compound object. Possible values include: yes – the object is a compound object; no – the object is not compound.
UID	i	The ID (UID) of the user that created the object.
GID	i	The ID (GID) of the group to which the user who created the object belongs.
Mode	i	Access permissions.
AddTime	s	The date and time the object was placed in the storage, formatted as "YYYY-MM-DD HH:MM:SS". If you specify the date but not the time, the time will be specified as 00:00:00. If you specify the time but not the date, the current date will be specified. If you specify the date and time as follows: (AddTime== s"), then the current date and time will be specified.
Size	i	Original size of the object, in bytes.

ANTI-VIRUS EVENTS AND THEIR DATA

You can filter Anti-Virus events based on their settings. The following table describes Anti-Virus events, event settings are described in the next table below.

Table 17. Events

#	EVENT NAME	DESCRIPTION	SETTINGS
1	ApplicationStarted	Kaspersky Anti-Virus is running; the event occurs after all tasks necessary for the Anti-Virus are started.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
2	ApplicationSettingsChanged	General settings of Kaspersky Anti-Virus have been changed.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
3	LicenseInstalled	The license is installed.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType

#	EVENT NAME	DESCRIPTION	SETTINGS
4	LicenseNotInstalled	A license installation error has occurred.	Date, EventId, EventType, RuntimeTaskId, KeySerial, TaskName, TaskType
5	LicenseRevoked	The license has been successfully revoked.	Date, EventId, EventType, RuntimeTaskId, KeySerial, TaskName, TaskType
6	LicenseNotRevoked	A license revocation error has occurred.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
7	LicenseExpired	The license period has expired.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
8	LicenseExpiresSoon	The license period will soon expire.	Date, EventId, EventType, RuntimeTaskId, DaysLeft, TaskName, TaskType
9	LicenseError	Licensing subsystem internal error.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
10	AVBasesAttached	Kaspersky Anti-Virus databases have been installed successfully after an update.	Date, EventId, EventType, RuntimeTaskId, AVBasesDate, TaskId, TaskName, TaskType
11	AVBasesAreOutOfDate	Kaspersky Anti-Virus databases are outdated.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
12	AVBasesAreTotallyOutOfDate	Kaspersky Anti-Virus databases are obsolete.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
13	AVBasesIntegrityCheckOK	Integrity check of Kaspersky Anti-Virus databases completed successfully.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
14	AVBasesIntegrityCheckFailed	Kaspersky Anti-Virus databases are damaged.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
15	AVBasesApplied	Kaspersky Anti-Virus databases applied.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
16	UpdateSourceSelected	An update source has been selected.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
17	UpdateSourceNotSelected	An update source connection error has occurred.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
18	NothingToUpdate	No update is required. This event occurs if the version of the database updates installed on the computer corresponds to or is newer than the version of the database updates on the update source.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
19	UpdateError	An error occurred while updating.	Date, EventId, EventType, ModuleName, RuntimeTaskId, TaskId, TaskName, TaskType
20	ModuleDownloaded	A program module has been downloaded.	Date, EventId, EventType, ModuleName, RuntimeTaskId, TaskId, TaskName, TaskType

#	EVENT NAME	DESCRIPTION	SETTINGS
21	ModuleNotDownloaded	A program module downloading error has occurred.	Date, EventId, EventType, ModuleName, RuntimeTaskId, TaskId, TaskName, TaskType
22	ModuleRetranslated	Program module has been successfully copied for distribution.	Date, EventId, EventType, ModuleName, RuntimeTaskId, TaskId, TaskName, TaskType
23	ModuleNotRetranslated	A program module copying error has occurred.	Date, EventId, EventType, ModuleName, RuntimeTaskId, TaskId, TaskName, TaskType
24	TaskStateChanged	The task state has changed.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskState, TaskType
25	TaskSettingsChanged	The task settings have changed.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
26	PackedObjectDetected	A packed object has been detected.	Date, EventId, EventType, AccessHost, AccessUser, AccessUserId, PackerName, FileName, FileOwner, FileOwnerId, ObjectName, ObjectSource, RuntimeTaskId, TaskId, TaskName, TaskType
27	ThreatDetected	A threat has been detected.	Date, EventId, EventType, AccessHost, AccessUser, AccessUserId, DetectCertainty, FileName, FileOwner, FileOwnerId, ObjectName, RuntimeTaskId, TaskId, TaskName, TaskType, ThreatName, VerdictType
28	ObjectProcessed	The object has been processed.	Date, EventId, EventType, AccessHost, AccessUser, AccessUserId, FileName, FileOwner, FileOwnerId, ObjectName, ProcessResult, RuntimeTaskId, TaskId, TaskName, TaskType
29	ObjectNotProcessed	The object has not been processed.	Date, EventId, EventType, AccessHost, AccessUser, AccessUserId, FileName, FileOwner, FileOwnerId, ObjectName, RuntimeTaskId, SkipReason, TaskId, TaskName, TaskType
30	ObjectProcessingError	A processing error has occurred.	Date, EventId, EventType, AccessHost, AccessUser, AccessUserId, FileName, FileOwner, FileOwnerId, ObjectName, ObjectProcessError, RuntimeTaskId, TaskId, TaskName, TaskType
31	ObjectDisinfected	The object has been disinfected.	Date, EventId, EventType, AccessHost, AccessUser, AccessUserId, FileName, FileOwner, FileOwnerId, ObjectName, RuntimeTaskId, TaskId, TaskName, TaskType
32	ObjectNotDisinfected	The object has not been disinfected.	Date, EventId, EventType, AccessHost, AccessUser, AccessUserId, FileName, FileOwner, FileOwnerId,

#	EVENT NAME	DESCRIPTION	SETTINGS
			ObjectNotDisinfectedReason, RuntimeTaskId, TaskId, TaskName, TaskType
33	ObjectDeleted	The object has been deleted.	Date, EventId, EventType, AccessHost, AccessUser, AccessUserId, FileName, FileOwner, FileOwnerId, RuntimeTaskId, TaskId, TaskName, TaskType
34	ObjectBlocked	The real-time protection task has denied object access to an accessing application.	Date, EventId, EventType, AccessHost, AccessUser, AccessUserId, FileName, FileOwner, FileOwnerId, RuntimeTaskId, TaskId, TaskName, TaskType
35	ObjectActionsCompleted	Action on infected object completed.	Date, EventId, EventType, AccessHost, AccessUser, AccessUserId, FileName, FileOwner, FileOwnerId, ObjectReason, ObjectSource, ObjectType, RuntimeTaskId, TaskId, TaskName, TaskType
36	ObjectSavedToQuarantine	Object quarantined.	Date, EventId, EventType, DangerLevel, DetectCertainty, FileName, QuarantineId, QuarantineObjectType, RuntimeTaskId, TaskId, TaskName, TaskType, VerdictType
37	ObjectSavedToBackup	The object was placed in Backup.	Date, EventId, EventType, DangerLevel, DetectCertainty, FileName, QuarantineId, QuarantineObjectType, RuntimeTaskId, TaskId, TaskName, TaskType, VerdictType
38	ObjectRemovedFromQuarantine	Object was deleted from quarantine.	Date, EventId, EventType, FileName, QuarantineId, QuarantineObjectType, RuntimeTaskId, TaskId, TaskName, TaskType
39	ObjectRemovedFromBackup	The object has been removed from backup.	Date, EventId, EventType, FileName, QuarantineId, QuarantineObjectType, RuntimeTaskId, TaskId, TaskName, TaskType
40	ObjectRestoredFromQuarantine	Object restored from Quarantine.	Date, EventId, EventType, FileName, QuarantineId, QuarantineObjectType, RuntimeTaskId, TaskId, TaskName, TaskType
41	ObjectRestoredFromBackup	Object has been restored from backup.	Date, EventId, EventType, FileName, QuarantineId, QuarantineObjectType, RuntimeTaskId, TaskId, TaskName, TaskType
42	QuarantineSizeLimitReached	Quarantine and backup maximum size reached.	Date, EventId, EventType, FileName, RuntimeTaskId, TaskId, TaskName, TaskType
43	QuarantineSoftSizeLimitExceeded	Quarantine size defined by the QuarantineSoftSizeLimit setting has been reached.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
44	QuarantineObjectCorrupted	Object in Quarantine is corrupted.	Date, EventId, EventType, FileName, QuarantineId, RuntimeTaskId, TaskId,

#	EVENT NAME	DESCRIPTION	SETTINGS
			TaskName, TaskType
45	QuarantineObjectCurable	Quarantined object can be disinfected.	Date, EventId, EventType, FileName, QuarantineId, RuntimeTaskId, TaskId, TaskName, TaskType
46	QuarantineObjectFalseDetect	After scanning of quarantined object Anti-Virus has recognized a suspicious or infected object as clean.	Date, EventId, EventType, FileName, QuarantineId, RuntimeTaskId, TaskId, TaskName, TaskType
47	QuarantineObjectPasswordProtected	Quarantined object password protected.	Date, EventId, EventType, FileName, QuarantineId, RuntimeTaskId, TaskId, TaskName, TaskType
48	QuarantineObjectProcessingError	Error while processing quarantined object.	Date, EventId, EventType, FileName, QuarantineId, RuntimeTaskId, TaskId, TaskName, TaskType
49	QuarantineThreatDetected	Quarantined object infected.	Date, EventId, EventType, DetectCertainty, FileName, QuarantineId, RuntimeTaskId, TaskId, TaskName, TaskType, VerdictType
50	ObjectAddToQuarantineFailed	Error adding object to quarantine.	Date, EventId, EventType, Description, FileName, RuntimeTaskId, TaskId, TaskName, TaskType
51	ObjectAddToBackupFailed	Error while adding an object to storage.	Date, EventId, EventType, Description, FileName, RuntimeTaskId, TaskId, TaskName, TaskType
52	RetranslationError	Error while copying updates.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
53	AVBasesRollbackCompleted	Rollback of Kaspersky Anti-Virus databases completed successfully.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
54	AVBasesRollbackError	Error while rolling back the databases of Kaspersky Anti-Virus.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
55	OASTaskError	Real time protection error.	Date, Error, EventId, EventType, Info, RuntimeTaskId, TaskId, TaskName, TaskType
56	ODSTaskError	Creating an on-demand scan.	Date, Error, EventId, EventType, Info, RuntimeTaskId, TaskId, TaskName, TaskType
57	EventsErased	Events erased.	Date, BeginDate, EndDate, EventId, EventType, Reason, RuntimeTaskId, TaskId, TaskName, TaskType
58	EventsMoved	Events moved.	Date, BeginDate, EndDate, EventId, EventType, Path, Reason, RuntimeTaskId, TaskId, TaskName, TaskType

Table 18. Events settings

SETTING	TYPE	DESCRIPTION
AccessHost	s	Name of remote computer if file is accessed by SMB/CIFS protocol.

SETTING	TYPE	DESCRIPTION
AccessUser	s	Name of user initiating access to file.
AccessUserId	i	ID of the user initiating access to file.
AVBasesDate	s	Release date of the latest installed database updates.
BeginDate	s	Date from when events are deleted or moved.
DangerLevel	s	<p>DangerLevel – danger level of the threat detected in an object when the object was placed in the storage.</p> <p>OrigDangerLevel – danger level of the threat in the quarantined object after scanning with updated databases.</p> <p>The danger level of an object depends on the type of threat in the object (see section "Programs detectable by Kaspersky Anti-Virus" on page 11). The danger level may assume the following values:</p> <p>High. The object may contain a threat of the network worm, classical virus, or Trojan type.</p> <p>Medium. The object may contain some other malicious program, adware, or a program with pornographic content.</p> <p>Low. The object may contain a threat of riskware type.</p> <p>Info. The object is quarantined by the user.</p>
Date	s	Date and time of the event.
DetectCertainty (OrigDetectCertainty)	s	<p>OrigDetectCertainty – the state of a detected object upon its placement in the storage.</p> <p>DetectCertainty – the state Anti-Virus assigns to an object in quarantine after scanning it using updated databases.</p> <p>The state of the detected object:</p> <p>Sure – object is classified as infected;</p> <p>Suspicion – object is classified as suspicious (the object has been found using the Heuristic Analyzer);</p> <p>Warning – object has the status "Warning" (the object code partly coincides with the code of a known threat; a false alarm may occur).</p>
EndDate	s	Date before which events are deleted or moved.
Error.	s	<p>Type of error. Possible values include:</p> <p>IncorrectUser – non-existent user given in the task settings, his/her name is found in the Info field;</p> <p>IncorrectGroup – non-existent group given in the task settings, group name is found in the Info field;</p> <p>IncorrectPath – incorrect scan path given in task settings, path is found in the Info field;</p> <p>InterceptorNotFound – on launch of the task, the interceptor module cannot be loaded.</p>
Filename	s	Full file name.
FileOwner	s	Name of user who is the owner of the file.
FileOwnerId	i	ID of the user who owns the file.
Host	s	The network name of the remote computer (mounted via SMB/CIFS) that accessed the object when Anti-Virus interception occurred.
Info	s	Additional information about the error.

SETTING	TYPE	DESCRIPTION
ModuleName	s	Name of Kaspersky Anti-Virus module that has generated the event.
ObjectName	s	The name of the object related to an event.
ObjectNotDisinfectedReason	s	The reason why an object was not disinfected: Unknown – the reason is unknown; InternalError – the task experienced an internal error; ObjectNotCurable – an object of this type cannot be disinfected; ObjectNotFound – the object was not found; ObjectReadOnly – the Anti-Virus only has read access rights to the object.
ObjectProcessError	s	The type of error that occurred during object scanning: Unknown InternalError ObjectNotCurable ObjectNoRights ObjectIOError OutOfSpace ObjectNotFound ObjectReadOnly SystemError
ObjectReason	s	Result of activities on the object. Possible values include: Cured – object disinfected; Removed – object deleted; Quarantined – object moved to quarantine; Skipped – object skipped; AllActionsFailed – all actions on the object ended with an error.
ObjectSource	s	Source of the infected file: LocalFile – local file system; RemoteNfsFile – remote resource accessed by NFS protocol; RemoteSambaFile – remote resource accessed by SMB/CIFS protocol.
ObjectType	s	The object type (whether the object is a compound object or not): Object – the object is not compound; Archive – the object is a compound object.
Path	s	Path to file where events have been moved.
QuarantinedId	i	The identifier assigned by Anti-Virus to an object in the storage.
Reason	s	Reason why events are moved or deleted: Date – move or deletion made by date; Manual – move or deletion made by user command; Size – move or deletion made by size of database.

SETTING	TYPE	DESCRIPTION
RuntimeTaskId	i	Unique identifier of a task session during which the event occurred. It is refreshed at every task launch.
TaskName	s	Name of the task during which the event occurred.
TaskState	s	Task state: Stopped – the task is stopped; Stopping – the task is stopping; Started – the task is in progress; Starting – the task is starting; Suspended – the task is suspended; Suspending – the task is suspending; Resumed – the task has been resumed; Resuming – the task is resuming; Failed – the task has terminated with an error.
TaskType	s	Type of a Kaspersky Anti-Virus task. The setting can assume the following values: <ul style="list-style-type: none"> • tasks, which users can manage: <ul style="list-style-type: none"> Update – predefined update task (ID=6); OAS – real-time protection task (ID=8); ODS – predefined on-demand scan task (ID=9); QS – task for scanning of quarantined objects (ID=10); • service tasks: <ul style="list-style-type: none"> EventManager – implements message exchange within the program (ID=1); AVS – anti-virus scan service task (ID=2); Quarantine – manages quarantine and backup (ID=3); Statistics – collects statistics (ID=4); License – implements the license server (ID=5); Notifier – controls delivery of notifications and performance of configured actions upon specified events (ID=7); EventStorage – implements the events log service (ID=11); Snmp plugin – provides for delivery of information about the program via SNMP (ID=12).
ThreatName	s	The name of the threat detected in the object related to the event.
Type (OrigType)	s	OrigType – the state of the object, assigned when the object is placed in the storage. Type – the state of an object in quarantine after it has been scanned using updated databases. Possible values include: <ul style="list-style-type: none"> Clean – not infected; Backup – is a backup copy; Infected – infected;

SETTING	TYPE	DESCRIPTION
		UserAdded – added by a user; Error – an error has occurred while scanning the object; PasswordProtected – is password-protected; Corrupted – is corrupted; Curable – the object may be disinfected.

ANTI-VIRUS CONFIGURATION FILE SETTINGS

You can create Anti-Virus configuration files either in INI or in XML format.

This section describes the structure and settings of Anti-Virus INI configuration files.

IN THIS SECTION

Rules for editing Kaspersky Anti-Virus INI configuration files.....	123
Real-time protection and on-demand scan tasks settings.....	124
Update tasks settings.....	137
Schedule settings.....	141
General settings of Kaspersky Anti-Virus.....	145
Quarantine and backup storage settings.....	147
Event log settings.....	148
Settings of notifications and event-based actions.....	150

RULES FOR EDITING KASPERSKY ANTI-VIRUS INI CONFIGURATION FILES

The following rules must be observed when editing the configuration file:

- If a setting belongs to a section, place it in this section only. Preserve the order and nesting of sections. You can place the settings in any order within one section.
- If you omit any setting, Kaspersky Anti-Virus will apply the default value if any.
- Place section names in rectangular brackets [].
- Enter parameter values in the **parameter name=value** format (spaces between parameter name and its value are not processed).

For example:

```
[ScanScope]
AreaDesc="Scan sdc"
AreaMask=re:\.exe
```

- Some parameters can take only one value while others can take several values. If you need to specify several values, repeat the setting as many times as many values you wish to specify, for example:

```
AreaMask=re:home/.*/Documents/
```

```
AreaMask=re:.*\.doc
```

- Settings names are not case sensitive.
- Values for settings of the following types are case sensitive:
 - names (masks, regular expressions) of scanned objects and exclusion objects;
 - names (masks, regular expressions) of threats;
 - user names;
 - user group names.

Other setting values are not case sensitive.

- You can assign Boolean setting values as follows: **yes – no, true – false** or **1 – 0**.
- Put in quotes the text values containing spaces (for example, names of files, directories and their paths):

```
AreaDesc="Scan mail databases"
```

Other values can be entered either with or without quotes, for example:

```
AreaMask="re:home/.*/Documents/"
```

```
AreaMask=re:home/.*/Documents/
```

- A single quote at the beginning or at the end of line will be considered an error.
- If the text value is in quotes, any printable characters within this value, including quotes, the space and tab characters, are part of this value. For example:

```
AreaDesc="Scanning "useless" documents"
```

- The space and tab characters will be ignored in the following cases:
 - before the first quote and after the last quote of the text value;
 - at the beginning and at the end of text value, which is not in quotes.
- You can use comments. A comment is a line starting with the character ; or #. While importing task settings (see section "Modifying task settings" on page [94](#)) from the configuration file, the comments are ignored. While viewing task settings (see section "Obtaining task settings" on page [93](#)), the comments are not displayed.

REAL-TIME PROTECTION AND ON-DEMAND SCAN TASKS SETTINGS

This section describes the settings that you can import into real-time protection and on-demand scan tasks.

You can use a configuration file with the described settings to change the settings of an existing real-time protection (on-demand scan) task, or to create a new task.

To change the settings of an existing task, you need to export the task settings into a file (see page [93](#)) open the file in any text editor, modify the settings as required, save the file, and then import the settings from the file into the task (see page [94](#)).

Structure of the real-time protection (on-demand scan) task INI configuration file

The real-time protection (on-demand scan) task configuration file consists of a set of sections. The file sections describe one or several scan areas and the security settings used by the Anti-Virus when scanning the specified areas.

The [ScanScope] section contains the name of the scan area and limits the scan area.

The [ScanScope:AreaPath] section describes the path to the directory being scanned. Its format differs from the format of other sections of the INI configuration file. You must specify at least one scan area to start the task.

The [ScanScope:ScanSettings] section and its [ScanScope:ScanSettings:AdvancedActions] subsection describe the security settings that Kaspersky Anti-Virus will use for the scan area specified in the [ScanScope:AreaPath] section. If you do not define settings of these sections, Kaspersky Anti-Virus will scan the specified area using security settings corresponding to the predefined **Recommended** security level.

If you want to specify several scan areas, first specify section settings for [ScanScope], [ScanScope:AreaPath], [ScanScope:AccessUser] (only for real-time protection) and [ScanScope:ScanSettings] for one area, then repeat this step for each additional area:

[ScanScope]

area 1

...

[ScanScope:AreaPath]

the path to the directory specified in area 1

...

[ScanScope:AccessUser]

(only for real-time protection tasks) list of area 1 users

...

[ScanScope:ScanSettings]

security settings for area 1

...

[ScanScope]

area 2

...

[ScanScope:AreaPath]

area 2: the path to the directory specified in area 2

...

[ScanScope:AccessUser]

(only for real-time protection tasks) list of area 2 users

...

[ScanScope:ScanSettings]

security settings for area 2

...

Anti-Virus scans areas in the order specified in the configuration file.

Note that if a file is part of several specified scan areas, Kaspersky Anti-Virus will scan it only once, using the security settings specified in the first scan area in which this file appears.

You may need to configure the security settings of the subdirectory which may be different from the security settings of the parent directory. For example, you want to scan the /home/ directory using the regular expression re:.*\doc and delete infected objects found there, and scan objects in the /home/dir1/ subdirectory using the regular expression re:.*\doc and disinfect infected objects found there.

The scan areas should be specified in the configuration file as follows:

[ScanScope]

Subdirectory

AreaMask="re:.*\doc"

[ScanScope:AreaPath]

/home/dir1/

[ScanScope:ScanSettings]

InfectedFirstAction=Cure

...

[ScanScope]

Parent directory

AreaMask="re:.*\doc"

[ScanScope:AreaPath]

/home/

[ScanScope:ScanSettings]

InfectedFirstAction=Remove

...

Anti-Virus will attempt to cure the infected re:.*\doc files in the /home/dir1/ directory and will delete remaining infected re:.*\doc files in the /home/ directory.

A description of configuration file settings, their possible values, and their default values are shown in the table below.

When specifying the file settings, follow the rules for editing Kaspersky Anti-Virus INI configuration files (see page [123](#)).

Table 19. Real-time protection and on-demand scan tasks settings

SETTING	DESCRIPTION AND POSSIBLE VALUES
ScanPriority	Task priority. This setting is used only in the on-demand scan tasks and is not used in the real-time protection tasks.

SETTING	DESCRIPTION AND POSSIBLE VALUES
	<p>You can set one of the predefined task priorities in accordance with process priorities in Linux.</p> <p>Possible values include:</p> <p>System (system). Priority of the process running a task is defined by the operating system.</p> <p>High (high). Priority of the process running a task is increased.</p> <p>Medium (medium). Priority of the process running a task remains unchanged.</p> <p>Low (low). Priority of the process running a task is decreased.</p> <p>Lower process priority increases the duration of task execution, but it can also affect positively the performance of processes belonging to other active applications.</p> <p>Higher process priority decreases the duration of task execution, but it can also affect negatively the performance of processes belonging to other active applications.</p> <p>Default value: System.</p>
ProtectionType	<p>Protection mode. Use of a SAMBA interceptor to scan objects accessed using SMB/CIFS. Use of a kernel level interceptor to scan objects accessed using other protocols (NFS, FTP, etc.).</p> <p>This setting is used only in the real-time protection task and is not used in on-demand scan tasks.</p> <p>Anti-Virus contains two components that intercept attempts to access files and scan them: a SAMBA interceptor (used to scan objects on remote computers when they are accessed via SMB/CIFS) and a kernel level interceptor. It scans objects when they are accessed in some other way.</p> <p>The SAMBA interceptor provides, as additional object information, the IP address of the remote computer, on which the application attempted to access the object when it was intercepted by Kaspersky Anti-Virus.</p> <p>If you use the protected server only as a SAMBA server, you can specify the value SambaOnly. In this case, Kaspersky Anti-Virus will not scan objects that are not accessed via SMB/CIFS.</p> <p>Possible values include:</p> <p>Full. Kaspersky Anti-Virus scans server objects with the SAMBA interceptor when they are accessed via SMB/CIFS. Kaspersky Anti-Virus uses the kernel level interceptor to intercept all other operations on files that are accessible on the protected server (including files on remote computers).</p> <p>SambaOnly. Kaspersky Anti-Virus scans objects with the SAMBA interceptor only when they are accessed via SMB/CIFS.</p> <p>Make sure that you have specified the SAMBA VFS password during the initial configuration of Kaspersky Anti-Virus (see section Step 7. Integrating with Samba server" in the Installation Guide of Kaspersky Anti-Virus 8.0 for Linux File Server).</p> <p>KernelOnly. Kaspersky Anti-Virus scans server objects only using the file interceptor.</p> <p>Make sure that you have specified the SAMBA VFS password during the initial configuration of Kaspersky Anti-Virus (see section Step 6. Compiling the kernel module" in the Installation Guide of Kaspersky Anti-Virus 8.0 for Linux File Server).</p> <p>Default value: the operation shall be selected during Kaspersky Anti-Virus installation.</p>
[ScanScope]	Scan area.

SETTING	DESCRIPTION AND POSSIBLE VALUES
AreaDesc	<p>Description of scan area containing additional information about the scan area. The maximum length of the line, defined by this setting, is equal to 4096 characters.</p> <p>Example:</p> <pre>AreaDesc="Scan mail databases"</pre> <p>Default value: All local objects.</p>
AreaMask	<p>Using this setting you can limit the scan area specified in the [ScanScope:AreaPath] section. The maximum length of the line, defined by this setting, is equal to 4096 characters.</p> <p>Within the scan area, Anti-Virus will scan only those files or directories specified using Shell masks or POSIX extended regular expressions. Use the re: prefix in regular expressions.</p> <p>If you do not specify this setting, Anti-Virus will scan all objects in the scan area.</p> <p>You can specify several values for this setting.</p> <p>Example:</p> <pre>AreaMask=re:.*\Documents/ AreaMask=re:.*\.doc AreaMask=re:\.exe</pre> <p>Default value: *.</p>
UseAccessUser	<p>This setting determines whether or not to use the settings in the [ScanScope:AccessUser] section (scanning upon access using the permissions of specified users).</p> <p>The setting of this section is applied only in real-time protection tasks. It is not used for on-demand scan tasks.</p> <p>Possible values include:</p> <p>yes – exclude objects only if they are accessed by applications running with the permissions of users, specified by the settings in the [ScanScope:AccessUser] section;</p> <p>no – scan objects when they are accessed with any permissions.</p> <p>Default value: not configured.</p>
[ScanScope:AreaPath]	
Scan scope, path to the directory to scan. You must specify at least one scan area to start the real-time protection task.	
Path	<p>The setting value consists of three elements:</p> <p><file system type>:<access protocol>:<path to the directory being scanned>, where:</p> <p><file system type>. Possible values include:</p> <p>Mounted. Remote directories mounted on the server. Using the <access protocol> setting, specify the protocol that provides remote access to the directories.</p> <p>Shared. Server file system resources shared by the SMB/CIFS or NFS protocol.</p> <p>AllRemotelyMounted. All remote directories mounted on the server using SMB/CIFS and NFS protocols.</p> <p>AllShared. Server file system resources shared by the SMB/CIFS and NFS protocols.</p>

SETTING	DESCRIPTION AND POSSIBLE VALUES
	<p><access protocol>. Protocol that provides remote access to the specified resources. This setting is used only when <file system type> has the Mounted or Shared value. Possible values include:</p> <p>SMB. The SMB/CIFS protocol.</p> <p>NFS. The NFS protocol.</p> <p><path to the directory being scanned>. Full path to the directory being scanned. For peculiarities in the scanning of symbolic and hard links please refer to the section Peculiarities in scanning of symbolic and hard links (see page 9).</p> <p>Examples:</p> <p><i>Path=/ – scan all local server directories; scan directories mounted using SMB/CIFS and NFS.</i></p> <p><i>Path=/home/ivanov – scan the /home/ivanov directory.</i></p> <p><i>Path=Mounted:SMB – scan all remote directories mounted using SMB/CIFS.</i></p> <p><i>Path=Mounted:NFS – scan all remote directories mounted using NFS.</i></p> <p><i>Path=Mounted:SMB:/remote-resources/ivanov-windows – scan the /remote-resources/ivanov-windows directory, which has been mounted using SMB/CIFS.</i></p> <p><i>Path=Mounted:NFS:/remote-resources/ivanov-linux – scan the /remote-resources/ivanov-windows directory, which has been mounted using NFS.</i></p> <p><i>Path=Shared:SMB – scan all directories in the server's file system shared by SMB/CIFS.</i></p> <p><i>Path=Shared:SMB:my_samba_share – scan the resource with the name my_samba_share shared by SMB/CIFS.</i></p> <p><i>Path=Shared:NFS – scan all server directories that are accessible via NFS.</i></p> <p><i>Path=Shared:NFS:/nfs_shares/my_share – scan the resource with the name /nfs_shares/my_share shared by NFS.</i></p> <p>Default value: /.</p>
<p>[ScanScope:AccessUser]</p>	<p>Scan upon access using the permissions of specified users.</p> <p>Anti-Virus scans objects only if they are accessed by applications running with the permissions of users and groups, specified by the settings in this section. If section settings are not specified, Anti-Virus scans objects when they are accessed with any rights.</p> <p>The settings of this section are applied only in real-time protection tasks. They are not used for on-demand scan tasks.</p> <p><i>If the settings in this section point to a non-existent user or group, the real-time protection task scans objects when an attempt to access them is made by any user or group.</i></p>
<p>UserName</p>	<p>Anti-Virus scans objects only if they are accessed by applications running with the permissions of specified users. You can specify several values for this setting, for example:</p> <p>UserName=usr1</p> <p>UserName=usr2</p> <p>Default value: not configured.</p>

SETTING	DESCRIPTION AND POSSIBLE VALUES
UserGroup	<p>Group name. Anti-Virus scans objects only if they are accessed by applications running with the permissions of specified groups. You can specify several values for this setting, for example:</p> <p>UserGroup=group1</p> <p>UserGroup=group2</p> <p>Default value: not configured.</p>
<p>[ScanScope:ScanSettings]</p> <p>Security settings that Anti-Virus applies when scanning the area specified by the [ScanScope:AreaPath] setting.</p>	
ScanByAccessType	<p>Anti-Virus scans objects for the following type of access to them (used only in the real-time protection task and not in on-demand scan tasks):</p> <p>SmartCheck (smart mode). Kaspersky Anti-Virus scans a file when an attempt is made to open it, and rescans it when an attempt is made to close it if the file has been modified. If a process accesses an object multiple times in the course of its operation and changes it, Kaspersky Anti-Virus scans the object a second time only when the process closes it for the last time.</p> <p>Open (at an access attempt). Kaspersky Anti-Virus scans the object when an attempt is made to open for reading or for execution or modification.</p> <p>OpenAndModify (at an attempt to access or modify). Kaspersky Anti-Virus scans a file when an attempt is made to open it, and rescans it when an attempt is made to close it if the file has been modified.</p> <p>Default value: SmartCheck.</p>
ScanArchived	<p>Kaspersky Anti-Virus scans file archives (including SFX self-extracting archives). Please note that Kaspersky Anti-Virus identifies threats in archives, but does not disinfect them.</p> <p>yes – scan archives;</p> <p>no – do not scan archives.</p> <p>Default values:</p> <p>real-time protection task – no;</p> <p>on-demand scan task – yes.</p>
ScanSfxArchived	<p>Anti-Virus scans self-extracting archives (archives that contain an executable extraction module).</p> <p>yes – scan SFX archives;</p> <p>no – do not scan SFX archives.</p> <p>Default values:</p> <p>real-time protection task – no;</p> <p>on-demand scan task – yes.</p>
ScanMailBases	<p>Anti-Virus scans email databases of Microsoft Outlook, Outlook Express, The Bat! and other email clients.</p> <p>yes – scan email database files;</p> <p>no – do not scan email database files.</p> <p>Default value: no.</p>

SETTING	DESCRIPTION AND POSSIBLE VALUES
ScanPlainMail	<p>Kaspersky Anti-Virus scans the files of plain text email messages.</p> <p>yes – scan plain text email messages; no – do not scan plain text email messages.</p> <p>Default value: no.</p>
ScanPacked	<p>Kaspersky Anti-Virus scans executable files packed by binary code packers, such as UPX or ASPack. This type of composite object contains threats more often than others.</p> <p>yes – scan packed files; no – do not scan packed files.</p> <p>Default value: yes.</p>
InfectedFirstAction	<p>First action to be performed on infected objects.</p> <p>In real-time protection tasks, before performing the action specified by you on an infected object, Anti-Virus blocks access to the object by applications that attempt to do so.</p> <p>Possible values include:</p> <p>Cure. Anti-Virus attempts to disinfect an object after it saves a copy of the object in the backup storage. If disinfection is not possible, for example, if the type of object or the type of threat in the object cannot be disinfecting, Kaspersky Anti-Virus will leave the object unchanged.</p> <p>Remove. Kaspersky Anti-Virus removes the infected object having first created a backup copy.</p> <p>Recommended (perform recommended action). Kaspersky Anti-Virus automatically selects and performs the action on the object based on the data about the threat detected in the object and about the possibility of disinfecting it, for example, the Anti-Virus will immediately remove Trojans since they do not incorporate themselves into other files and do not infect them; therefore they do not need to be disinfecting.</p> <p>Quarantine. Anti-Virus moves the object to Quarantine, where it is stored in encrypted form.</p> <p>Skip. The object will remain intact. Anti-Virus does not attempt to cure or delete the object, but does log information about the object.</p> <p>Default value: Recommended.</p>
InfectedSecondAction	<p>Second action to be performed on infected objects.</p> <p>The values are the same as for the InfectedFirstAction setting.</p> <p>If Kaspersky Anti-Virus fails to perform the first action, it will perform the second action.</p> <p>If you select Skip or Remove as a first action, then you need not specify a second action. We recommend specifying two actions as other values.</p> <p>If you do not specify a second action, Anti-Virus will use Skip as the second action.</p> <p>Default value: Skip.</p>
SuspiciousFirstAction	<p>First action to be performed on suspicious objects.</p> <p>In real-time protection tasks, before performing the action specified by you on an object, Anti-Virus blocks access to the object for applications that attempt to do so.</p> <p>Possible values include:</p> <p>Cure. Anti-Virus attempts to disinfect an object after it saves a copy of the object in the backup storage. If disinfection is not possible, for example, if the type of object or the type of threat in the object cannot be disinfecting, Kaspersky Anti-Virus will leave</p>

SETTING	DESCRIPTION AND POSSIBLE VALUES
	<p>the object unchanged.</p> <p>Quarantine. Anti-Virus moves the object to Quarantine, where it is stored in encrypted form.</p> <p>Remove. Kaspersky Anti-Virus removes the object having first created a backup copy.</p> <p>Recommended (perform recommended action). Kaspersky Anti-Virus automatically selects and performs the action on the object based on the data about the threat detected in the object and about the possibility of disinfecting it, for example, the Anti-Virus will immediately remove Trojans since they do not incorporate themselves into other files and do not infect them; therefore they do not need to be disinfecting.</p> <p>Skip. The object will remain intact. Anti-Virus does not attempt to cure or delete the object, but does log information about the object.</p> <p>Default value: Recommended.</p>
SuspiciousSecondAction	<p>The values are the same as for the SuspiciousFirstAction setting.</p> <p>If Kaspersky Anti-Virus fails to perform the first action, it will perform the second action.</p> <p>If you select Skip or Remove as a first action, then you need not specify a second action. We recommend specifying two actions as other values.</p> <p>If you do not specify a second action, Anti-Virus will use Skip as the second action.</p> <p>Default value: Skip.</p>
UseSizeLimit	<p>Determines whether or not to apply the SizeLimit setting (which specifies the maximum size of a scanned object).</p> <p>yes – use the SizeLimit setting;</p> <p>no – do not use the SizeLimit setting.</p> <p>Default value: no.</p>
SizeLimit	<p>The maximum size of the objects being scanned (in bytes). If an object to be scanned is larger than the specified value, the Anti-Virus will skip the object.</p> <p>This setting is used together with the UseSizeLimit setting.</p> <p>Specify the maximum object size (in bytes). Possible values: 0 – 2147483647 (approximately 2 GB).</p> <p>0 – Anti-Virus scans objects of any size.</p> <p>Default value: 0.</p>
UseTimeLimit	<p>Determines whether the TimeLimit setting (which specifies the maximum duration of an object scan) applies.</p> <p>yes – use the TimeLimit setting;</p> <p>no – do not use the TimeLimit setting.</p> <p>Default values:</p> <p>real-time protection task – yes;</p> <p>on-demand scan task – no.</p>
TimeLimit	<p>Maximum object scan time (sec). The Anti-Virus stops scanning an object if it takes longer than the number of seconds specified by this setting value.</p> <p>This setting is used together with the UseTimeLimit setting.</p> <p>Specify the maximum scan duration for an object in seconds.</p> <p>0 – the object scan duration is unlimited.</p>

SETTING	DESCRIPTION AND POSSIBLE VALUES
	<p>Default values:</p> <p>real-time protection task – 60;</p> <p>on-demand scan task – 120.</p>
UseExcludeMasks	<p>Enables / disables exclusion of objects specified by the ExcludeMasks setting.</p> <p>yes – exclude objects specified by the ExcludeMasks setting.</p> <p>no – do not exclude objects specified by the ExcludeMasks setting.</p> <p>Default value: no.</p>
ExcludeMasks	<p>Exclude objects by name, mask, or regular expression. You can use this parameter to exclude individual files from being scanned in a given area, or exclude several files at one time using Shell masks and POSIX extended regular expressions. Use the re: prefix in regular expressions.</p> <p>Example:</p> <pre>ExcludeMasks=re:.*\.tar\.gz ExcludeMasks=re:.*\.avi ExcludeMasks=re:/*\.avi\$ ExcludeMasks=*.doc</pre> <p>Default value: not configured.</p>
UseExcludeThreats	<p>Enables / disables exclusion of objects containing the threats, specified by the ExcludeThreats setting.</p> <p>yes – exclude objects containing the threats, specified by the ExcludeMasks setting.</p> <p>no – do not exclude objects containing the threats, specified by the ExcludeMasks setting.</p> <p>Default value: no.</p>
ExcludeThreats	<p>Exclude objects by the name of the threats detected in them. Before specifying a value for this setting, make sure that the UseExcludeThreats setting is active.</p> <p>E.g., you may be using a utility to collect information about your network. Most Kaspersky Anti-Virus programs refer such utility code to the Riskware threats type. To keep Kaspersky Anti-Virus from blocking it, add the full name of the threat contained in the application to the list of excluded threats.</p> <p>In order to exclude a single object from the scan, specify the full name of the threat in this object - the Anti-Virus line with a conclusion that the object is infected or suspicious.</p> <p>You can find full name of the threat identified in an object in the Kaspersky Anti-Virus log.</p> <p>You can also find the full name of the threat identified in a software product at the Virus Encyclopedia web site at Viruslist.com (see the Virus Encyclopedia section at http://www.viruslist.com). To find the name of a threat, enter the name of the product in the Search field.</p> <p>The setting value is case-sensitive.</p> <p>Example :</p> <p><i>Perform no actions on files in which the Anti-Virus identifies the threats named NetTool.Linux.SynScan.a and Monitor.Linux.Keylogger.a:</i></p> <pre>ExcludeThreats=not-a-virus:NetTool.Linux.SynScan.a ExcludeThreats=not-a-virus:Monitor.Linux.Keylogger.a</pre>

SETTING	DESCRIPTION AND POSSIBLE VALUES
	<p>You can use shell masks and extended POSIX regular expressions to specify threat names. Add the re: prefix to regular expressions.</p> <p><i>Perform no actions on files in which the Anti-Virus identifies any threats for Linux belonging to the not-a-virus category:</i></p> <pre>ExcludeThreats=re:not-a-virus:.*\.Linux\..*</pre> <p>Default value: not configured.</p>
UseAdvancedActions	<p>Enables / disables actions to be performed on an object, depending on the type of threat found in the object.</p> <p>If you enable the option, Kaspersky Anti-Virus will apply actions which you will specify in the [ScanScope:ScanSettings:AdvancedActions] section instead of actions specified by InfectedFirstAction, InfectedSecondAction, SuspiciousFirstAction and SuspiciousSecondAction settings.</p> <p>Available values:</p> <p>yes – perform the action to be performed on objects, depending on the type of threat;</p> <p>no – do not perform the action to be performed on objects, depending on the type of threat.</p> <p>Default value: yes.</p>
ReportCleanObjects	<p>Enables / disables logging of the information about scanned objects, which Kaspersky Anti-Virus recognizes as clean.</p> <p>You can enable the option, for example, to make sure that an object has been scanned by Anti-Virus.</p> <hr/> <p>Enabling the option for a long time is not recommended because recording of big data volumes to the log can decrease the operating system performance.</p> <hr/> <p>Available values:</p> <p>yes – log information about clean objects;</p> <p>no – do not log information about clean objects.</p> <p>Default value: no.</p>
ReportPackedObjects	<p>Enables / disables logging of the information about scanned objects that make up a part of compound objects.</p> <p>You can enable the option, for example, to make sure that an object within an archive has been scanned by Anti-Virus.</p> <hr/> <p>Enabling the option for a long time is not recommended because recording of big data volumes to the log can decrease the operating system performance.</p> <hr/> <p>Available values:</p> <p>yes – log information about objects scanned within archives;</p> <p>no – do not log information about objects scanned within archives.</p> <p>Default value: no.</p>
UseAnalyzer	<p>Enable / disable Heuristic Analyzer.</p> <p>The Heuristic Analyzer scans the standard sequence of operations allowing the nature of the file to be determined with a reasonable degree of certainty. The advantage of using this method is that new threats are detected before virus analysts have</p>

SETTING	DESCRIPTION AND POSSIBLE VALUES
	<p>encountered them.</p> <p>Available values:</p> <p>yes – enable Heuristic Analyzer</p> <p>no – disable Heuristic Analyzer</p> <p>Default value: yes.</p>
HeuristicLevel	<p>The level of detail of the heuristic analysis.</p> <p>This level sets the balance between the thoroughness of searches for new threats, the load on the operating system's resources and the time required for scanning. The higher the detail level, the more resources it will require and the longer it will take.</p> <p>Available values:</p> <p>Light – least detailed scan, minimum system load</p> <p>Medium – medium scan, balanced system load</p> <p>Deep – most detailed scan, maximum system load</p> <p>Default value: Light.</p>
<p>[ScanScope:ScanSettings:AdvancedActions]</p> <p>A response depending on the type of threat.</p> <p>Using the settings in this section, you can customize a particular reaction of Kaspersky Anti-Virus to objects that contain specified threats.</p>	
<p>Verdict</p> <p>FirstAction</p> <p>SecondAction</p>	<p>Prior to specifying the settings in this section, make sure that the UseAdvancedActions setting is active.</p> <p>For the threats specified in the Verdict setting, specify two actions (FirstAction and SecondAction). Anti-Virus will attempt to perform these actions on the object if it identifies the specified threat in the object.</p> <p>If Kaspersky Anti-Virus fails to perform the first action, it will perform the second action.</p> <p>If you select Skip or Remove as a first action, then you need not specify a second action. We recommend specifying two actions as other values.</p> <p>If you do not specify a second action, Anti-Virus will use Skip as the second action.</p> <p>See the values for the FirstAction and SecondAction settings in the descriptions of these sections.</p> <p>Possible values for the Verdict setting (type of threat) are:</p> <p>Virware – viruses and worms;</p> <p>Trojware – Trojans;</p> <p>Malware – other malicious software;</p> <p>Pornware – pornographic software;</p> <p>Adware – advertising software;</p> <p>Riskware – potentially dangerous software.</p> <p>The values of the Verdict setting are case-sensitive.</p> <p>For more information on the types of threats, refer to the "Programs detectable by Kaspersky Anti-Virus" section (on page 11).</p> <p>Example:</p> <p>UseAdvancedActions=yes</p>

SETTING	DESCRIPTION AND POSSIBLE VALUES
	<p>[ScanScope:ScanSettings:AdvancedActions]</p> <p>Verdict=Adware</p> <p>FirstAction=Cure</p> <p>SecondAction=Skip</p> <p>[ScanScope:ScanSettings:AdvancedActions]</p> <p>Verdict=Pornware</p> <p>FirstAction=Cure</p> <p>SecondAction=Skip</p> <p>Default value: not configured.</p>
<p>[ExcludedFromScanScope]</p> <p>Exclusion area.</p>	
<p>AreaDesc</p>	<p>Description of the exclusion area, containing additional information about the exclusion area.</p> <p>Example:</p> <p>AreaDesc="Exclude separate SAMBA"</p> <p>Default value: not configured.</p>
<p>AreaMask</p>	<p>You can use this setting to limit the exclusion area specified in the [ExcludedFromScanScope:AreaPath] section.</p> <p>Anti-Virus will only exclude those objects that you specify using Shell masks or POSIX extended regular expressions. Use the re: prefix in regular expressions.</p> <p>AreaMask=re:.*\.tar\.gz</p> <p>Default value: not configured.</p>
<p>UseAccessUser</p>	<p>This setting enables and disables the use of settings in the [ExcludedFromScanScope:AccessUser] section (exclusion when attempting access using the rights of specified users).</p> <p>The setting of this section is applied only in real-time protection tasks. It is not used for on-demand scan tasks.</p> <p>Possible values include:</p> <p>yes – exclude objects only if they are accessed by applications running with the permissions of users, specified by the settings in the [ExcludedFromScanScope:AccessUser] section;</p> <p>no – exclude objects when they are accessed with any rights.</p> <p>Default value: not configured.</p>
<p>[ExcludedFromScanScope:AreaPath]</p> <p>Exclusion area. Path to the excluded directory.</p>	
<p>Path</p>	<p>The setting value consists of three elements:</p> <p><file system type>:<access protocol>:<path to the excluded directory>, where:</p> <p><file system type>. Possible values include:</p> <p>Mounted. Remote directories mounted on the server. Using the <access protocol> setting, specify the protocol that provides remote access to the directories.</p>

SETTING	DESCRIPTION AND POSSIBLE VALUES
	<p>Shared. Server file system resources shared by the SMB/CIFS or NFS protocol.</p> <p>AllRemotelyMounted. All remote directories mounted on the server using SMB/CIFS and NFS protocols.</p> <p>AllShared. Server file system resources shared by the SMB/CIFS and NFS protocols.</p> <p><access protocol>. Protocol that provides remote access to the specified resources. This setting is used only when <file system type> has the Mounted or Shared value. Possible values include:</p> <p>SMB. The SMB/CIFS protocol.</p> <p>NFS. The NFS protocol.</p> <p><path to the excluded directory>. The full path to the excluded directory.</p> <p>Examples:</p> <p style="padding-left: 40px;">Path=Mounted:NFS – <i>exclude all remote directories mounted using NFS.</i></p> <p>Default value: not configured.</p>
	<p>[ExcludedFromScanScope:AccessUser]</p> <p>Scanning exclusion when attempting access using the rights of specified users.</p> <p>Kaspersky Anti-Virus will exclude objects from scanning only if they are accessed by applications with the user and group rights specified by the settings in this section. If section settings are not specified, Anti-Virus scans objects when they are accessed with any rights.</p> <p>The settings of this section are applied only in real-time protection tasks. They are not used for on-demand scan tasks.</p>
<p>UserName</p>	<p>Anti-Virus scans objects only if they are accessed by applications running with the permissions of specified users. You can specify several values for this setting, for example:</p> <p style="padding-left: 40px;">UserName=usr1</p> <p style="padding-left: 40px;">UserName=usr2</p> <p>Default value: not configured.</p>
<p>UserGroup</p>	<p>Group name. Anti-Virus excludes objects only if they are accessed by applications running with the permissions of specified users. You can specify several values for this setting, for example:</p> <p style="padding-left: 40px;">UserGroup=group1</p> <p style="padding-left: 40px;">UserGroup=group2</p> <p>Default value: not configured.</p>

UPDATE TASKS SETTINGS

This section describes the settings of the update task configuration file. You can review it to create new update tasks and modify settings in the existing tasks.

To change the settings of an existing task, you need to export the task settings into a file (see page 93) open the file in any text editor, modify the settings as required, save the file, and then import the settings from the file into the task (see page 94).

The structure of the INI configuration file of the update tasks

Configuration file of the update tasks consists of the set of settings and sections. File sections describe the function performed by the update task, update source and settings used to connect to it.

Using the UpdateType setting, select the function which will be performed by the update task. This is a mandatory setting.

In the [UpdateComponentsSettings] section specify whether you wish to download the updates specified by the UpdateType setting or only receive information about their availability. This is a mandatory setting.

The [CommonSettings] section defines the type of the update source and the settings used to connect to it. Using settings in this section specify whether you wish Anti-Virus to use the proxy server when it connects to various types of update sources and specify the proxy server settings.

The [CommonSettings:CustomSources] section is required if you have selected user-defined sources as the update source. Here you should specify the address of the user-defined update source. If you wish to specify several user-defined update sources, define each source in a separate [CommonSettings:CustomSources] section. Kaspersky Anti-Virus will connect to the user-defined update sources using the connection settings described in the [CommonSettings] section.

The [RetranslateUpdatesSettings] section is required if you have selected downloading of updates without their installation using the UpdateType setting. Using this section specify the directory into which Anti-Virus will save the specified updates. If you selected copying only specified updates, also specify the names of the databases and modules whose updates you want the update task to obtain.

The table below contains a description of the configuration file settings, possible and default values of these settings.

When specifying the file settings, follow the rules for editing Kaspersky Anti-Virus INI configuration files (see page [123](#)).

Table 20. Update tasks settings

SETTING	DESCRIPTION AND POSSIBLE VALUES
UpdateType	<p>Specify the function to be performed by the update task:</p> <p>AllBases. Update the databases of Kaspersky Anti-Virus.</p> <p>RetranslateProductComponents (Copy all accessible Anti-Virus updates). Kaspersky Anti-Virus will save the downloaded updates in the directory specified by the RetranslationFolder setting, without installing them.</p> <p>RetranslateComponentsList (Copy only specified updates). Kaspersky Anti-Virus will download only the updates whose names have been specified in the settings of the [RetranslateUpdatesSettings] section. It will save the downloaded updates in the directory specified by the RetranslationFolder setting, without installing them.</p> <p>Using the RetranslateComponentsList setting you can download updates of other Kaspersky Lab applications if you wish to use the protected server as an intermediary for distributing updates.</p> <p>You can review the names of update components in the document http://support.kaspersky.com/downloads/updater/update_components_21112008.pdf, which is available on the Kaspersky Lab Technical Support web site.</p> <p>Critical updates for Kaspersky Anti-Virus modules are not installed automatically.</p> <p>Default value: AllBases.</p>
<p>[CommonSettings]</p> <p>Update source and settings used to connect to it.</p>	
SourceType	<p>Specify an update source for Kaspersky Anti-Virus:</p> <p>KLServers. Kaspersky Anti-Virus will receive updates from one of the Kaspersky Lab update servers. Updates are downloaded via HTTP or FTP</p>

SETTING	DESCRIPTION AND POSSIBLE VALUES
	<p>protocols.</p> <p>AKServer. Kaspersky Anti-Virus will download updates to the protected server from the Kaspersky Administration Kit administration server installed in the LAN.</p> <p>You can select this update source if you use Kaspersky Administration Kit application for centralized administration of anti-virus protection of computers in your organization.</p> <p>Custom. Kaspersky Anti-Virus will download updates from the user-defined source, specified in the [CommonSettings:CustomSources] section. You can specify directories on FTP or HTTP servers or directories on any device mounted on the server, including directories on remote computers mounted using SMB/CIFS or NFS.</p> <p>Default value: KLServers.</p>
UseKLServersWhenUnavailable	<p>You can configure the Anti-Virus to access the Kaspersky Lab update servers if all user-defined sources are unavailable.</p> <p>yes – connect to Kaspersky Lab update servers if all user-defined sources are unavailable;</p> <p>no – do not connect to Kaspersky Lab update servers if all user-defined sources are unavailable.</p> <p>Default value: yes.</p>
UseProxyForKLServers	<p>The option to use a proxy server for connection to the update servers of Kaspersky Lab.</p> <p>yes – use proxy server to connect to the Kaspersky Lab update servers;</p> <p>no – do not use proxy server to connect to the Kaspersky Lab update servers.</p> <p>Default value: no.</p>
UseProxyForCustomSources	<p>Using a proxy server when connecting to user-defined update sources. Enable this setting if you need access to the proxy server to connect to any of the user-defined FTP or HTTP servers.</p> <p>yes - use proxy server to connect to the user-defined update servers;</p> <p>no - do not use proxy server to connect to the user-defined update servers.</p> <p>Default value: no.</p>
ProxyPort	<p>Proxy server settings: port.</p> <p>Default value: 3128.</p>
ProxyServer	<p>Proxy server settings: network name or IP address.</p> <p>Default value: not configured.</p>
ProxyAuthType	<p>This setting controls authentication when accessing a proxy server being used for connections to FTP or HTTP update source servers.</p> <p>NotRequired (no authentication). Select if authentication is not required to access the proxy server.</p> <p>Plain (authentication by login name and password, i.e. basic authentication). Specify the user name and password using ProxyAuthUser and ProxyAuthPassword settings.</p> <p>Default value: NotRequired.</p>
ProxyAuthUser	<p>If you enable authentication, specify the name of the user whose rights will be used by Anti-Virus for proxy server access.</p>

SETTING	DESCRIPTION AND POSSIBLE VALUES
	Default value: not configured.
ProxyAuthPassword	<p>If you enable authentication, specify the password of the user whose rights will be used by Anti-Virus for proxy server access.</p> <p>Default value: not configured.</p>
UseFtpPassiveMode	<p>By default, to connect to update servers using FTP, the Anti-Virus uses the passive FTP server mode: it is assumed that a network firewall is used in the enterprise LAN.</p> <p>Available values:</p> <p>yes – use passive FTP server mode;</p> <p>no – use active FTP server mode.</p> <p>Default value: yes.</p>
ConnectionTimeout	<p>This setting specifies the time to wait for a response from an update source, i.e. FTP server or HTTP server, while attempting to connect to it. If response from the update source is not received within the specified interval, Kaspersky Anti-Virus will connect to another specified update source, for example, to another Kaspersky Lab update server if you configured updating from Kaspersky Lab update servers.</p> <p>Specify the response wait time in seconds. Only integers within the range from 0 to 120 can be entered as parameter values.</p> <p>Default value: 10.</p>
<p>[CommonSettings:CustomSources]</p> <p>If you selected SourceType=Custom, specify the user-defined update type using the settings of this section. You can specify several user-defined update sources. Define each source in a separate section. Kaspersky Anti-Virus will always try the next specified source if the previous source is unavailable.</p> <p>You can configure the Anti-Virus to access the Kaspersky Lab update servers if all user-defined sources are unavailable using the UseKLServersWhenUnavailable setting.</p>	
Url	<p>Specify the user-defined update source: LAN or WAN directory.</p> <p>Example:</p> <p>Url=http://primer.ru/bases/ – the address of HTTP or FTP server on which the directory containing updates is located.</p> <p>Url= /home/bases/ – a directory on the protected server.</p> <p>Default value: not configured.</p>
Enabled	<p>Using this setting you can enable or disable the use of the source specified by URL setting in the current section.</p> <p>yes – use the update source;</p> <p>no – do not use the update source.</p> <p>Default value: not configured.</p>
<p>[UpdateComponentsSettings]</p> <p>Updates download.</p>	
Action	<p>The setting is mandatory, its value is DownloadAndApply:</p> <ul style="list-style-type: none"> • Kaspersky Anti-Virus downloads updates if UpdateType is set to RetranslateProductComponents or RetranslateComponentsList; • Kaspersky Anti-Virus downloads and installs updates if UpdateType is set to AllBases.

SETTING	DESCRIPTION AND POSSIBLE VALUES
	Default value: DownloadAndApply .
[RetranslateUpdatesSettings]	
Downloading updates from the update source without applying them. Specify the settings of this section if you have selected to download updates without applying them: specified the RetranslateComponentsList value for the UpdateType setting.	
RetranslationFolder	Specify the directory into which the Anti-Virus will save the downloaded updates. Default value: not configured.
RetranslationComponents	Specify the name of the update you would like to receive if you specified RetranslateComponentsList as your UpdateType setting. You can review the names of update components in the document http://support.kaspersky.com/downloads/updater/update_components_21112008.pdf , which is available on the Kaspersky Lab Technical Support web site. Example: <i>To copy updates for version 6.0.2.551 of Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition:</i> RetranslationComponents=UPDATER RetranslationComponents=AVS RetranslationComponents=BLST RetranslationComponents=KAV6WSEE RetranslationComponents=RT RetranslationComponents=AK6 RetranslationComponents=INDEX60 Default value: not configured.

SCHEDULE SETTINGS

This section describes configuration file settings that you can use to schedule the tasks.

When specifying the settings, follow the rules for editing Kaspersky Anti-Virus INI configuration files (see page [123](#)).

Structure of the schedule INI configuration file

Enable=yes | no

StartRules=<start_rule>;<start_rule_2>;...<start_rule_n>

[StopRules=<stop_rule>;<stop_rule_2>;...<stop_rule_n>]

[SuspendRules=<pause_rule>;<pause_rule_2>;...<pause_rule_n>]

Table 21. Schedule settings

SETTING	DESCRIPTION AND POSSIBLE VALUES
Enable	Enables / disables scheduled task launch. Possible values include: yes – enable starting a scheduled task; no – disable starting a scheduled task.
StartRules	List of task start rules (see page 142). Separate values with a semicolon (";").
StopRules	List of task stop rules (see page 143). Separate values with a semicolon (";").
SuspendRules	List of task pause rules (see page 144). Separate values with a semicolon (";").

IN THIS SECTION

Start rules..... [142](#)

Stop rules..... [143](#)

Pause rules [144](#)

Specifying exact time [145](#)

START RULES

You can specify one or several start rules.

Syntax

```
<start_rule>=PS
<start_rule>=BR
<start_rule>=<exact time>
```

Examples

- ◆ *Start a task on the 10th day of each month and on the last day of each month at 8:45 PM:*

```
Enable=yes
StartRules=10::; -1:20:45
```

- ◆ *Start a task every Monday in December 2009 at 12:00 AM:*

```
Enable=yes
StartRules=2009/Dec/Mon::
```

- ◆ *Start a task every day at 1:00 PM:*

```
Enable=yes
StartRules=:01:00 PM
```

➤ *Start a task every 30 minutes:*

```
Enable=yes
StartRules=:30
```

Table 22. Start rule settings

SETTING	DESCRIPTION AND POSSIBLE VALUES
<start_rule>	Conditions for starting a task. You can specify several conditions for starting a task. For example, in order to configure an on-demand scan task to run twice per month, you will have to create two start rules.
BR	After databases update. The task will be started after each successful Anti-Virus database update (this alternative is not used in update tasks).
PS	At application startup. The task will be launched at every Anti-Virus startup.
<exact time>	Specify a date and time for starting a task (see page 145).

STOP RULES

You can specify one or several stop rules.

Syntax

```
<stop_rule>=StopAfter <amount of time in minutes> CanRunAfter <amount of time in minutes>
<stop_rule>=StopAt <exact time> CanRunAfter <amount of time in minutes>
<stop_rule>=StopAt <exact time> CanRunAt <exact time>
```

Examples

➤ *Stop a task 10 minutes after it was started and do not allow it to start again for 10 minutes after stopping:*

```
Enable=yes
StopRules=StopAfter 10 CanRunAfter 10
```

➤ *Stop a task at 12:00 AM on Wednesday and do not allow it to start again until 6:45 PM on Wednesday:*

```
Enable=yes
StopRules=StopAt Wed:: CanRunAt Wed:18:45
```

Table 23. Stop rule settings

SETTING	DESCRIPTION AND POSSIBLE VALUES
<stop_rule>	You can use a stop rule to specify the maximum duration of task execution. Additionally you can use a stop rule to specify a time interval in which the task may not be started per a schedule. At the end of the specified time it will not be resumed. If the next scheduled task start time occurs during the specified interval, said task will not be considered as having been missed.
StopAfter	Maximum duration of the task execution, minutes. If a task is going to run longer than the number of minutes you have specified in this setting, it will be stopped by the Anti-Virus. A task terminated this way will not be considered skipped.

	<p>This feature does not apply to update tasks.</p> <p>Specify the number of minutes.</p> <p>Separate the value with a space.</p>
StopAt	<p>Task stop time.</p> <p>Specify time in <exact time> format (see page 145).</p> <p>Separate the value with a space.</p>
CanRunAfter	<p>Amount of time in minutes after the task is stopped, specified in the StopAfter setting. During this time the task cannot be restarted.</p> <p>If this setting is not specified in the pause rule, the task may be started immediately after stopping (the default setting value is 0).</p> <p>Separate the value with a space.</p>
CanRunAt	<p>The time at which the task may be run again per the schedule. Specify time in <exact time> format (see page 145).</p> <p>Separate the value with a space.</p>

PAUSE RULES

You can specify one or several pause rules.

Syntax

```
<pause_rule>=PauseAfter <amount of time in minutes> ResumeAfter <amount of time in minutes>
<pause_rule>=PauseAt <exact time> ResumeAfter <amount of time in minutes>
<pause_rule>=PauseAt <exact time> [ResumeAt <exact time>]
```

Examples

- Start task at 00:00; pause task from 10:00 to 18:00:

```
Enable=yes
StartRules=:00:00
SuspendRules=PauseAt 10:00 AM ResumeAt 06:00 PM
```

Table 24. Pause rule settings

SETTING	DESCRIPTION AND POSSIBLE VALUES
<pause_rule>	<p>You can use a pause rule to specify a time interval in which the task will be paused. At the conclusion of the specified length of time, Kaspersky Anti-Virus will resume the task. You may need to pause a task for some interval of time during the day (for example, between 10:00 and 18:00).</p> <p>If the next scheduled task start time occurs during the specified interval, said task will not be considered as having been missed.</p> <p>Pause rules do not apply to update tasks.</p>
PauseAfter	<p>Maximum duration of the task execution, minutes.</p> <p>If a task is going to run longer than the number of minutes you have specified in this setting, it will be stopped by the Anti-Virus. A task terminated this way will not be considered skipped.</p> <p>Separate the value with a space.</p>

SETTING	DESCRIPTION AND POSSIBLE VALUES
PauseAt	Task pause time. Specify time in <exact time> parameter format (see page 145). Separate the value with a space.
ResumeAfter	Duration of the task pause, minutes. The Anti-Virus will resume the task upon expiration of the specified time interval since the task pause. If this setting is not specified in the pause rule, the task may be resumed immediately after pausing (the default setting value is 0). Separate the value with a space.
ResumeAt	Task resumption time. Specify time in <exact time> parameter format (see page 145). Separate the value with a space.

SPECIFYING EXACT TIME

The <exact time> setting has the following format.

[<year> /] [<month> /] [<day of the month> | <day of the week>] : [hh] : [mm]

Fields of the <exact time> setting are described in the following table:

FIELD	VALUE
<year>	[1900;2100]
<month>	JAN FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC
<day of the month>	[-1;31], where -1 denotes the last day of the month, 0 – the day of the month is not specified.
<day of the week>	MON TUE WED THU FRI SAT SUN Weekend Working days
hh	hour [00;23]
mm	If you specified a value for hh, this value is in the range [00,59]. If you did not specify a value for hh, this value is in the range [0,24*60]. You can assign the following values: :23:30 specifies "at 11:30 PM". If not specified (or if specified as ::), the task will be started/stopped/paused/resumed at 12:00 AM. ::90 specifies "every 1.5 hr".

GENERAL SETTINGS OF KASPERSKY ANTI-VIRUS

The table below contains a description of the configuration file settings, possible and default values of these settings.

When specifying the file settings, follow the rules for editing Kaspersky Anti-Virus INI configuration files (see page [123](#)).

Once the general settings of Kaspersky Anti-Virus are changed, restart the Kaspersky Lab Framework service using the

`/opt/kaspersky/kav4fs/bin/kav4fs-control --restart-app` command.

Table 25. General settings of Kaspersky Anti-Virus

SETTING	DESCRIPTION AND POSSIBLE VALUES
StartWithUser	Account under which the processes of Kaspersky Anti-Virus are running. You cannot modify this setting. Default value: root .
StartWithGroup	Account under which the processes of Kaspersky Anti-Virus are running. You cannot modify this setting. Default value: default .
UpdateFolder	Path to a directory on protected server containing the updates directories specified by the AVBasesFolderName and AVBasesBackupFolderName settings. Default value: /var/opt/kaspersky/kav4fs/update .
AVBasesFolderName	Directory in which Kaspersky Anti-Virus stores database updates. Default value: avbases .
AVBasesBackupFolderName	Name of the directory which Anti-Virus uses as a service directory when it updates the databases. If you specify a different directory, make sure that it allows reading and writing for the account under which the Anti-Virus runs. Default value: avbases-backup .
SambaConfigPath	Directory in which the SAMBA configuration file is stored. By default, a standard path to the directory of the SAMBA configuration file on the server is specified. You must specify this setting if the Samba configuration file is stored in the location different from the standard location. Default value: /etc/samba/smb.conf .
NfsExportPath	Directory in which the NFS configuration file is stored. By default, a standard path to the directory of the NFS configuration file on the server is specified. You must specify this setting if the NFS configuration file is stored in the location different from the standard location. Default value: /etc/exports .
TempFolder	Full path to the directory in which the Anti-Virus saves temporary files it creates. If you specify a different directory, make sure that it allows reading and writing for the account under which Kaspersky Anti-Virus runs. Default value: /var/run/kav4fs .
TraceEnable	Maintaining a trace log. Kaspersky Anti-Virus records all events into the trace log. Trace log files are stored in the directory specified by the TraceFolder setting. Possible values include: yes – maintain a trace log; no – do not maintain a trace log. Default value: yes .

SETTING	DESCRIPTION AND POSSIBLE VALUES
TraceFolder	<p>Directory in which Kaspersky Anti-Virus stores trace log files.</p> <p>If you specify a different directory, make sure that it allows reading and writing for the account under which Kaspersky Anti-Virus runs.</p> <p>Default value: /var/log/kaspersky/kav4fs.</p>
TraceLevel	<p>Trace log detail level</p> <p>Possible values include:</p> <ul style="list-style-type: none"> Fatal. Critical events. Error. Errors. Warning. Important events. Info. Information events. Debug. Debug information. <p>The most detailed level is Debug information which writes all events to the log, and the least detailed is Critical events level, which only writes critical events to the log.</p> <p>Please note that the trace file can take up a large amount of disk space.</p> <p>If you enable the trace file and do not modify the settings, Kaspersky Anti-Virus traces the Kaspersky Anti-Virus subsystem with the Debug information level of detail.</p> <p>Default value: Error.</p>
MaxFileNameLength	<p>The maximum length of the full path to the scanned file, in bytes.</p> <p>If the length of the file being scanned exceeds this value, the scan task will skip such file and if the BlockFilesGreaterMaxFileName setting is assigned to the yes value, the real-time protection task will block the access to such file.</p> <p>Possible values: 4096 – 33554432.</p> <p>Default value: 16384.</p>
BlockFilesGreaterMaxFileName	<p>Blocks access to files in which the full path name exceeds the MaxFileNameLength value.</p> <p>The on-demand scan task skips such files regardless of the BlockFilesGreaterMaxFileName value.</p> <p>Possible values include:</p> <ul style="list-style-type: none"> yes – the real-time protection task blocks access to such files; no – the access is not blocked. <p>Default value: yes.</p>

QUARANTINE AND BACKUP STORAGE SETTINGS

This section describes the configuration file settings that you can use to customize the settings of the quarantine and the backup storage.

A description of configuration file settings, their possible and default values are shown in the table below.

When specifying the file settings, follow the rules for editing Kaspersky Anti-Virus INI configuration files (see page [123](#)).

Table 26. Quarantine and backup storage settings

SETTING	DESCRIPTION AND POSSIBLE VALUES
QuarantineFolder	<p>Directory containing the quarantined and backed up objects.</p> <p>You can specify a storage directory that is different from the default directory.</p> <p>You can use any directory on any server device as the storage. Specifying directories located on remote computers, for example, those mounted via SMB/CIFS or NFS, is not recommended.</p> <p>Kaspersky Anti-Virus will start to place objects into the directory specified in this setting both after you have imported the file settings into Anti-Virus using the <code>-T --set-settings</code> command, and after the Anti-Virus has been stopped and restarted.</p> <p>If the specified directory does not exist or is not accessible, the Anti-Virus will start to use the storage directory set by default.</p> <p>Default value: <code>/var/opt/kaspersky/kav4fs/quarantine/</code>.</p>
QuarantineSizeLimit	<p>Maximum storage size.</p> <p>The value of this setting specifies the maximum data volume in the storage.</p> <p>Note that after the maximum storage size has been exhausted, Kaspersky Anti-Virus will stop placing objects to quarantine and will stop backing up objects prior to disinfection and deletion. A QuarantineSizeLimitReached event will be logged, indicating that the maximum storage size has been reached.</p> <p>If the value of this setting is set to 0, the maximum storage size is not defined.</p> <p>Specify a value in bytes.</p> <p>Possible values: 0 – 1,8*10¹⁹</p> <p>Default value: 1073741824.</p>
QuarantineSoftSizeLimit	<p>Recommended storage size.</p> <p>The value of this setting specifies the recommended general data volume in the storage.</p> <p>This is an information setting. It does not limit the storage size, but allows the administrator to track the status of the storage. After the recommended storage size has been reached, the Anti-Virus will continue to place objects in quarantine and will continue to back up objects prior to disinfection and deletion. A QuarantineSoftSizeLimitExceeded event will be logged, indicating that the recommended storage size has been reached.</p> <p>If the value of this setting is set to 0, the recommended maximum storage size is not defined.</p> <p>Specify a value in bytes.</p> <p>Possible values: 0 – 1,8*10¹⁹</p> <p>Default value: 858993459.</p>

EVENT LOG SETTINGS

This section contains a description of the settings in the configuration file for Kaspersky Anti-Virus event log.

While changing the file settings, follow the rules for editing Kaspersky Anti-Virus INI configuration files (see page [123](#)).

Table 27. Event log settings

SETTING	DESCRIPTION AND POSSIBLE VALUES
EventStorageFolder	<p>Event log directory. Kaspersky Anti-Virus saves information about events and service files of its event log to this directory.</p> <p>You can view information about events stored in these files, using the <code>-E --query</code> command (see page 109).</p> <p>You cannot modify this setting.</p> <p>Default value: <code>/var/opt/kaspersky/kav4fs/db/event_storage</code>.</p>
RotateMethod	<p>The Anti-Virus rotates events partially deleting (moving) event information from the EventStorageFolder directory. The RotateMethod setting can take the following values:</p> <p>Erase. The Anti-Virus deletes information about events from the log when the RotatePeriod elapses or when the data volume exceeds the maximum value defined by the EventStorageMaxSize setting.</p> <p>Move. When the RotatePeriod elapses or when the data volume exceeds the maximum value defined by the EventStorageMaxSize setting, the Anti-Virus transfers information about events from the log into the RotateMoveFolder directory and saves it in the rotation file.</p> <p>The rotation file name contains the earliest time of event registered in the file; its format is EventStorage-YYYY-MM-DD-hh-mm-ss.db.</p> <p>During each rotation the Anti-Virus saves information about events in a separate file. Created files may differ in size if rotation uses both the RotatePeriod and the EventStorageMaxSize settings or if it is performed by the user manually. A single file size may be up to half of the value defined by EventStorageMaxSize or less (deviations range within 100 KB).</p> <p>You can delete the rotation files or create their backup copies on removable media.</p> <p>Default value: Erase.</p>
RotateMoveFolder	<p>Directory where Kaspersky Anti-Virus moves information about events if the Move method of events rotation has been selected.</p> <p>The directory must be located on the same hard drive partition and have the same mount point with the EventStorageFolder directory. It must exist and be accessible for writing. If these conditions are not met, Anti-Virus does not move information about events deleting it instead from the EventStorageFolder directory.</p> <p>Default value: not configured.</p>
RotatePeriod	<p>Rotation interval, it can take the following values:</p> <p>Daily. The Anti-Virus rotates events every day at 00:00.</p> <p>Weekly. The Anti-Virus rotates events every Monday at 00:00.</p> <p>Monthly. The Anti-Virus rotates events on the 1st day of each month at 00:00.</p> <p>Never. The interval for events rotation is not defined.</p> <p>Default value: Never.</p>
EventStorageMaxSize	<p>Maximum size of the events log directory.</p> <p>When information about events in the EventStorageFolder directory exceeds the size defined by the setting, Anti-Virus rotates events. The setting can be used in combination with the RotatePeriod setting to restrict additionally the size of the event log directory.</p> <p>Specify a value in bytes.</p>

SETTING	DESCRIPTION AND POSSIBLE VALUES
	<p>0 – maximum size of the events log directory is not defined.</p> <p>Setting the value to zero or too high is not recommended because large data volume in the EventStorageFolder directory can slow down Kaspersky Anti-Virus.</p> <p>Default value: 1073741824.</p>

SETTINGS OF NOTIFICATIONS AND EVENT-BASED ACTIONS

This section contains a description of the settings in the configuration file for notifications and event-based actions.

While changing the file settings, follow the rules for editing Kaspersky Anti-Virus INI configuration files (see page [123](#)).

Table 28. Settings of notifications and event-based actions

SETTING	DESCRIPTION AND POSSIBLE VALUES
EnableSntp	<p>Enables/disables delivery of notifications by email.</p> <p>yes – email delivery of notifications is enabled.</p> <p>no – email delivery of notifications is disabled.</p> <p>Default value: no.</p>
EnableActions	<p>Enables/disables execution of event-based actions.</p> <p>yes – execution of event-based actions is enabled.</p> <p>no – execution of event-based actions is disabled.</p> <p>Default value: no.</p>
[CommonSntpSettings]	
General notification settings	
Sender	<p>Email address of the sender.</p> <p>Default value: not configured.</p>
DefaultRecipients	<p>Recipient address from the global list. The product can send to the recipients from the list any notifications about events described in a file.</p> <p>You can specify several recipients: repeat the setting the number of times corresponding to the number of addresses that you wish to add.</p> <p>Example:</p> <pre>DefaultRecipients=admin1@example.com DefaultRecipients=admin2@example.com</pre> <p>You can enable or disable the list individually for every notification using the UseRecipientList setting.</p> <p>Default value: not configured.</p>
Mailer	<p>Email program used to send notifications. The setting can assume the following values:</p> <p>Internal. Internal mailer of Kaspersky Anti-Virus. Kaspersky Anti-Virus features an internal mail program for delivery of notifications via SMTP. You can select that option if authentication is not required to send email. Define the mailer settings in the [CommonSntpSettings:InternalMailerSettings] section.</p>

SETTING	DESCRIPTION AND POSSIBLE VALUES
	<p>Sendmail. The Sendmail application. You can select it if Sendmail is installed and configured on the protected server. Define additionally the SendmailPath setting.</p> <p>Default value: Internal.</p>
SendmailPath	<p>Path to the Sendmail executable file, it includes the following Sendmail settings:</p> <ul style="list-style-type: none"> -t – mandatory argument (instruction to use the list of recipients from message); -i – optional argument (instruction to disable interpreting a single dot (.) in a line as a message end character). <p>Default value: /usr/sbin/sendmail -t -i.</p>
<p>[CommonSmtpSettings:InternalMailerSettings]</p> <p>Settings of the internal Kaspersky Anti-Virus mailer.</p>	
SmtpServer	<p>SMTP server address.</p> <p>Default value: not configured.</p>
SmtpPort	<p>SMTP server port.</p> <p>Default value: 25.</p>
SmtpQueueFolder	<p>Directory where the queue of outgoing messages will be stored.</p> <p>Default value: /var/opt/kaspersky/kav4fs/db/notifier.</p>
ConnectionTimeout	<p>Time during which server response will be expected (seconds).</p> <p>Default value: 10.</p>
<p>[SmtpNotification]</p> <p>Settings for event notifications, message text. Create a separate [SmtpNotification] section for each event, for which you wish to configure notifications.</p>	
Recipients	<p>"Local" list of recipients: they will only receive the message described in the current [SmtpNotification] section.</p> <p>You can specify several recipients: repeat the setting the number of times corresponding to the number of addresses that you wish to add.</p> <p>Example:</p> <pre>Recipients=admin3@example.com Recipients=admin4@example.com</pre> <p>You can enable or disable the list individually for every notification using the UseRecipientList setting.</p> <p>Default value: not configured.</p>
UseRecipientList	<p>The rule for using the list of recipients. It defines the list of recipients, which will be used to send the message:</p> <ul style="list-style-type: none"> Local. Message will be sent to recipients from the local list. Global. Message will be sent to recipients from the global list. Both. Messages will be sent to recipients from both lists. <p>Default value: Global.</p>
Subject	<p>"Subject" field of the message.</p> <p>If you skip the setting, the "Subject" field will contain the event.</p> <p>Default value: not configured.</p>
Body	<p>Message body. You can add macros (see section "Using macros" on page 69).</p>

SETTING	DESCRIPTION AND POSSIBLE VALUES
	Default value: not configured.
EventName	Event that will be reported in notification. Default value: not configured.
Enable	Enables/disables notification delivery: yes – notification delivery is enabled. no – notification delivery is disabled. Default value: no .
<p>[Actions]</p> <p>Settings for event-based actions. Create a separate [Actions] section for each event, for which you wish to configure an action.</p>	
Command	Shell script with the corresponding instructions executed when an event occurs. E.g., you can configure delivery of SMS notifications or instant messaging notifications (such as jabber), integrate the Anti-Virus with various monitoring systems. You can modify the firewall settings or even disable Samba server in case of a virus outbreak (multiple "Threat found" events). You can add macros to the scripts (see section "Using macros" on page 69). Default value: not configured.
EventName	Event that will trigger the specified action. Default value: not configured.
Enable	Enables/disables execution of the action described in the current [Actions] section: yes – action execution is enabled. no – action execution is disabled. Default value: no .

MANAGING KASPERSKY ANTI-VIRUS VIA KASPERSKY ADMINISTRATION KIT

If your organization uses Kaspersky Administration Kit for centralized management of the anti-virus applications, you can control Kaspersky Anti-Virus on the protected servers and configure it using Kaspersky Administration Kit Administration Console.

The Administration Console allows you to examine the computer's protection status and edit the computer's general protection settings. You can also create tasks for on-demand scans, for updating the application, and for installing key files.

IN THIS SECTION

Viewing the server protection status	153
The "Application Settings" dialog box.....	154
Creating and configuring tasks.....	154
Creating a task.....	154
The Local task creation wizard.....	155
Updating tasks settings	157
Scheduling a task via Kaspersky Administration Kit.....	161
Creating and configuring policies	163
Checking connection with Administration Server manually. The klnagchk utility.....	165
Connecting to Administration Server manually. The klmover utility.....	165
Tasks settings	166

VIEWING THE SERVER PROTECTION STATUS

The Administration Console lets you view the protection status of a selected server and the overall server status from the point of view of Anti-Virus security and its accessibility.

◆ *To view protection status of a server:*

1. In the Administration Console tree open the **Managed computers** folder and select the group to which the protected server belongs.
2. Right-click the line with the information about the protected server in the results pane and select the **Properties** command.
3. In the **<Computer name> properties** dialog box open the **Protection** tab.

The **Protection** tab displays the following information about the protected server:

Table 29. Information on server protection status in the <Computer name> Properties dialog box

FIELD	DESCRIPTION
Computer status	Status of the protected server from the point of view of anti-virus security. For more details about statuses refer to the Kaspersky Lab Technical Support website, Article code 987.
Real-time protection status	Displays the real-time protection status, for example, <i>Started</i> , <i>Stopped</i> , <i>Paused</i> .
Last on-demand scan	Date and time of the last execution of an on-demand scan task.
Viruses found	The total number of malicious programs (names of threats) detected on the protected server (counter of detected threats) since the moment when Kaspersky Anti-Virus was installed or since the moment the counter was last reset. In order to reset a counter, press the Reset button.

THE "APPLICATION SETTINGS" DIALOG BOX

Using the **Application settings** dialog box you can perform remote management of Kaspersky Anti-Virus or configure it on the selected protected server.

➤ To open the *Application settings* dialog box:

1. In the Administration Console tree open the **Managed computers** folder.
2. Expand the group containing the protected server and select the **Client computers** folder.
3. Right-click the line with the information about the protected server in the results pane and select the **Properties** command.
4. In the <Computer name> **Properties** dialog box, on the **Applications** tab select **Kaspersky Anti-Virus 8.0 for Linux File Server** in the list of installed applications and click the **Properties** button.

CREATING AND CONFIGURING TASKS

You can create local tasks, tasks for several selected computers and group tasks of the following types:

- update;
- databases update rollback;
- on-demand scan;
- key file installation.

You create local tasks for a selected protected server on the **Tasks** tab. Group tasks should be created on the selected group's **Group tasks** folder, tasks for selected hosts should be created in the **Tasks for specific computers** folder.

General information about tasks in Kaspersky Administration Kit can be found in *Kaspersky Administration Kit. Administrator Guide*.

CREATING A TASK

When configuring Kaspersky Anti-Virus by Kaspersky Administration Kit, you can create tasks of the following types:

- local tasks, for an individual client computer;
- group tasks, for client computers of specified administration groups;
- tasks for specific computers, which may include computers from one or more groups;
- Kaspersky Administration Kit tasks – specific tasks of the Update server: tasks downloading updates, backup copying tasks and reporting tasks.

Tasks for specific computers are only performed by a set of computers. For example, if you add new client computers to a group for which a remote deployment task has been created, the task will not run on those new machines. You have either to create a new task or modify the existing task's settings.

You can perform the following operations with tasks:

- configure tasks;
- monitor a task's performance;
- copy or move a task from one group to another, or delete it, using the standard context menu commands **Copy / Paste, Cut / Paste** and **Delete**, or the corresponding items from the **Action** menu.
- import and export tasks.

Detailed information about using tasks can be found in the Kaspersky Administration Kit manual.

➤ *To create a local task:*

1. Open the computer properties window of the required client computer on the **Tasks** tab.
2. Click the **Add** button.
3. The New task wizard will start (see page [155](#)). Follow its instructions.

➤ *To create a group task, perform the following actions:*

1. Open the Administration Console of Kaspersky Administration Kit.
2. In the **Managed computers** folder, open the required group, which is represented by a subfolder.
3. In the selected group, open the **Group tasks** subfolder which lists the group's existing tasks.
4. Click the **Create a task** link in the tasks pane to start the New task wizard. Further information about creating group tasks is available in the Kaspersky Administration Kit manual.

➤ *To create a task for collections of hosts (Kaspersky Administration Kit task):*

1. Open the Administration Console of Kaspersky Administration Kit.
2. Select the required folder: **Tasks for specific computers**, or **Kaspersky Administration Kit tasks**.
3. Click the **Create a task** link in the tasks pane to start the New task wizard. Further information about creating Kaspersky Administration Kit tasks and tasks for collections of hosts is available in the Kaspersky Administration Kit manual.

THE LOCAL TASK CREATION WIZARD

The Local task creation wizard can be started from the context menu of a managed computer, or in its properties window.

The wizard consists of a series of screens (steps) navigated using buttons **Back** and **Next**; to close the wizard once it completed its work, use the **Finish** button. To cancel the application at any stage, use the **Cancel** button.

STEP 1. ENTERING GENERAL TASK SETTINGS

At the first stage, specify the task name's in the **Name** field.

STEP 2. SELECTING AN APPLICATION AND DEFINING TASK TYPE

During this stage, you should specify the task's type, and which program will perform the task: Kaspersky Anti-Virus 8.0 for Linux File Server, or Network Agent.

For Kaspersky Anti-Virus 8.0 the following tasks can be created:

- Virus scan – checks user-defined areas for the presence of viruses.
- Update – downloads and applies a package containing program updates.
- Update roll-back – rolls back the last program update.
- Key file installation – installs a new license key file, required to enable the program's full functionality.

STEP 3. CONFIGURING TASK SETTINGS

The appearance of the wizard's window at this stage will depend on the task type selected during the previous stage.

The following settings are required for an on-demand scan task:

- specify the scan's scope (see page [157](#)) and the scan settings (see page [158](#));
- specify any excluded areas (see page [158](#)).

The following settings are required for a task which updates the database and program modules:

- specify the source (see page [159](#)) from which the updates will be downloaded, and the settings for connection to the source;
- specify the type of updates to be downloaded (see page [160](#)).

The task to roll-back updates has no specific settings.

The license key file installation task requires a path to the key file.

➡ *To do that, perform the following actions:*

1. In the task creation wizard's window, click the **Browse** button.
2. Select the license key file (with a .key extension) which you received when purchasing Kaspersky Anti-Virus.

STEP 4. SCHEDULING THE TASK

To configure the task schedule, please refer to the section "Scheduling tasks via Kaspersky Administration Kit" on page [161](#)). You can configure a schedule for all task types except license installation tasks.

STEP 5. COMPLETING THE WIZARD

The last screen of the wizard will inform you that the task creation wizard has completed successfully.

UPDATING TASKS SETTINGS

After you have created a task you can:

- modify the task settings;
- modify the task schedule, enable or disable scheduled task launches.

➔ *To modify the task settings:*

1. In the Administration Console tree, expand the **Managed computers** node and select the group to which the protected server belongs.
2. Right-click the line with the information about the protected server in the results pane and select the **Properties** command.
3. In the **Computer properties** dialog box, on the **Tasks** tab, open the context menu for the task you want to configure, and select the **Properties** command.
4. Make the required changes to the settings in the **Task properties** window.
5. Click **OK** to save the changes.

CREATING A SCAN AREA

The term *scan area* refers to the set of objects which will be scanned, such as file system objects. All scan tasks, whether real-time protection tasks or on-demand scan tasks, have a specified scan area.

➔ *To define a scan area:*

1. Open the **Task properties** window.
2. Select the **Settings** tab, and click the **Add** button in the **Scan areas** section.
3. In the **<New scan area>** dialog box which will open:
 - a. In the **Area name** field, assign a name to the new area. The name will appear in the list of areas for scanning, within the **Scan areas** window.
 - b. Select the resource type in the dropdown list to the left.

If you selected a **Shared** or **Remote** resource, you must specify in the right dropdown list the protocol used to remotely access to that resource, whether **Samba** or **Nfs**.

- c. In the path entry field enter the path to the scanned directory.

If you selected a **Shared** or **Remote** resource type, you may specify the path to the directory or the name of the resource, for example, **MySamba**. If you selected **All shared** or **All remote**, leave the path entry field blank.

- d. In the **Masks** section, click the **Add** button and in the displayed **Object mask** window, define the file name templates, or path templates, for the objects to be scanned.

Using Shell masks, you can specify the file name template to scan by Kaspersky Anti-Virus.

Using extended regular expressions, you can specify the file path template to scan by Kaspersky Anti-Virus. A regular expression cannot contain the name of the folder which defines the scan or protection area.

Add the **re:** prefix to regular expressions.

- e. Click **OK** to save the changes.
4. Click the **OK** button in the **Task settings** window to save the changes.

Kaspersky Anti-Virus will scan objects in the scan areas in the order in which the areas are listed. If you wish to configure different security settings for child and parent directories, place the subdirectory in the list higher, than its parent directory.

Use the **Move Up** and **Move Down** buttons to move lines in which paths are specified to the top or bottom of the list.

CONFIGURING SECURITY SETTINGS

The default scan settings used by Kaspersky Anti-Virus for all scan tasks are those recommended by Kaspersky Lab. You can reconfigure the security settings as you require.

➔ *To configure the security settings for a scan area:*

1. Open the **Task properties** window.
2. Select the scan area on the **Settings** tab, and click the **Properties** button in the **Scan areas** section.
3. In the window that will open, select the **Settings** tab. In the **Scan of compound objects** section, check the boxes beside the types of composite objects (see page [171](#)) which you want Kaspersky Anti-Virus to scan.
4. In the **Scan optimization** section of the **Settings** tab, specify the maximum scanning duration for an individual object (see page [171](#)) and the maximum size of objects to scan (see page [172](#)).
5. Select the **Actions** tab, and specify the operations to be performed on infected objects (see page [168](#)) and on suspicious objects (see page [169](#)).
6. In the **Exclusion area** section, specify objects to be excluded from scanning by name (see page [170](#)) and objects to be excluded from scanning by the name of the detected threat (see page [170](#)).

The excluded area specified for a particular scan area will only apply to that scope.

7. Click **OK** to save the changes.

CREATING AN EXCLUDED AREA

By default, Kaspersky Anti-Virus checks all objects within a scan area.

You can define name and path templates that are excluded from the scan area. In that case Kaspersky Anti-Virus will not check files or directories within the scan area if they match the specified Shell masks or extended POSIX regular expressions.

You can use Shell masks to specify a file name template excluded from scanning by Kaspersky Anti-Virus.

You can also use extended regular expressions to specify a template for the paths to files which Kaspersky Anti-Virus should not scan. The regular expression should not contain the name of the directory containing excluded object.

➤ *To define an excluded area:*

1. Open the **Task properties** window.
2. Click the **Add** button on the **Exclusion areas** tab.
3. In the **<New exclusion area>** dialog box which will open:
 - a. In the **Area name** field, assign a name to the new area. The name will appear in the list of areas for scanning within the **Exclusion areas** window.
 - b. Select the resource type in the dropdown list to the left.

If you selected a **Shared** or **Remote** resource, you must specify in the right dropdown list the protocol used to remotely access to that resource, whether **Samba** or **Nfs**.
 - c. In the path entry field enter the path to the excluded directory.

If you selected a **Shared** or **Remote** resource type, you may specify the path to the directory or the name of the resource, for example, **MySamba**. If you selected **All shared** or **All remote**, leave the path entry field blank.
 - d. In the **Masks** section, click the **Add** button and in the displayed **Object mask** window, define the file name templates, or path templates, for the objects to exclude from scanning.
 - e. Click **OK** to save the changes.
4. Click the **OK** button in the **Task settings** window to save the changes.

SELECTING AN UPDATE SOURCE

Update source (see page [172](#)) is a resource containing updates for Anti-Virus databases. Update sources can be HTTP or FTP servers, or local or network folders.

The main updates 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.

➤ *To choose an update source:*

1. Open the **Task properties** window.
2. Use the **Updates sources** tab to select a source of updates (see page [172](#)).
3. Click **OK** to save the changes.

➤ *To add a custom update source:*

1. Open the **Task properties** window.
2. On the **Updates sources** tab, select **Other directories on the local network or the Web**, and click the **Customize** button.
3. In the **Updates sources** window that will open, press the **Add** button and enter either the path to a directory which contains the updates, or the address of a FTP or HTTP update server.
4. Click **OK** to save the changes.

➤ *To configure the connection to an update source:*

1. Open the **Task properties** window.

2. On the **Updates sources** tab, press the **Connection settings** button.
3. Configure the following settings in the window that will open:
 - a. FTP server mode (see page [172](#))
 - b. time to wait for a response from the update source while connected to it (see page [172](#))
 - c. proxy server usage (see page [173](#))
 - d. proxy server settings (see page [173](#))
 - e. authentication required to access proxy server (see page [173](#))
 - f. location of the protected computer
4. Click **OK** to save the changes.

SELECTING THE TYPE OF UPDATES

A Kaspersky Anti-Virus update task performs one of the following operations:

1. Downloads and installs databases.
2. Downloads updates to Kaspersky Anti-Virus' program modules. The updated modules are only copied to the specified directory; no actual installation of the files is performed.
3. Copy updates for selected modules. The task will only retrieve updates specified in the list. No actual installation of the modules will be performed.

➔ *To choose the type of updates, perform the following steps:*

1. Open the **Task properties** window.
2. On the **Updates type** tab, select the type of updates (see page [173](#)) from the dropdown list.
3. If you selected **Copy all updates available for the application**, specify the directory where the updates will be stored (see page [173](#)) in the **Target directory**.
4. If you selected **Copy updates for selected modules** according to a list:
 - a. Click the **Add** button in the **Updates components list**.
 - b. Enter the required update name in the displayed window.

You can review the names of update components in the document http://support.kaspersky.com/downloads/updater/update_components_21112008.pdf, which is available on the Kaspersky Lab Technical Support web site.

- c. Click **OK** to save the changes.
 - d. Repeat the a-c cycle as many times as necessary.
5. Click **OK** to save the changes.

SCHEDULING A TASK VIA KASPERSKY ADMINISTRATION KIT

You can specify the schedule of a task when you create the task or later, using the **Task properties** dialog box. This section describes how to specify a schedule in the **Task properties** dialog box. Task scheduling is performed similarly in the task creation wizard.

CREATING A TASK START RULE

You can create *task start rules*: a one-off task launch at a specified time on a certain day; a regular task launch with a specified frequency, such as weekly or monthly; launching a task after every database update, or every time Kaspersky Anti-Virus starts.

➔ *To create a task start rule:*

1. In the Administration Console tree, expand the **Managed computers**.
2. Expand the group containing the protected server and select the **Client computers** folder.
3. Right-click the line with the information about the protected server in the results pane and select the **Properties** command.
4. In the **Computer properties** dialog box open the **Tasks** tab. Open the context menu of the task you want to configure and select the **Properties** command.
5. In the **Task properties** dialog box open the **Schedule** tab.
6. Enable the task schedule by selecting the option **Run on schedule** in the lower part of the window.
7. Click the **Add** button, and in the **Create new start rule** window that will open:
 - a. Select the rule type from the dropdown list:
 - **At specified time**, to configure the start of the task at a specified date or at a specified interval, for example, weekly.
 - **After databases update**, to start a task each time databases are updated.
 - **At Anti-Virus startup**, to start a task each time Kaspersky Anti-Virus is started.
 - b. If you selected the **At specified time** mode:
 - Select **Once** and enter the exact date and time when the task should start.
 - Select **Periodically**, and specify how often the task should run: after a specified interval (in minutes), or at a defined time of day, daily, weekly, monthly or yearly.
 - c. Click **OK** to save the changes.
8. Click **OK** to save the changes.

CREATING A TASK STOP RULE

You can specify when to stop a task using task stop rules. Additionally, you can specify the time interval during which the task may not be restarted per its schedule, for example, *stop the task at 8:00 AM on Monday and do not restart it until 6:00 PM Friday*.

➤ *To create a task stop rule:*

1. In the Administration Console tree open the **Managed computers** folder and select the group to which the protected server belongs.
2. Right-click the line with the information about the protected server in the results pane and select the **Properties** command.
3. In the **Computer properties** dialog box open the **Tasks** tab. Open the context menu of the task you want to configure and select the **Properties** command.
4. In the **Task properties** dialog box open the **Schedule** tab.
5. Enable the task schedule by selecting the option **Run on schedule** in the lower part of the window.
6. Click the **Add** button, and in the **Create new start rule** window that will open:
 - a. Select the rule type from the dropdown list:
 - **Pause and resume after specified duration.** Kaspersky Anti-Virus will stop the task after the specified time has elapsed after its start. Additionally you can specify an amount of time after the task was stopped, during which the task will not be restarted.
 - **Stop at specified time; allow to start after specified duration.** Kaspersky Anti-Virus will launch the task at the time you specified. Additionally you can specify an amount of time after the task was stopped, during which the task will not be restarted.
 - **Stop and allow to start at specified time.** Kaspersky Anti-Virus will stop a task at the specified time; you can specify a time interval, during which the task cannot be restarted.
 - b. If you selected the **Pause and resume after specified duration** mode:
 - In the **Stop after the task has run for, min** field, enter the maximum time allowed for the task to run (minutes).
 - Specify the amount of time during which the task may not be started in the **After the task has stopped, allow to start in, min** field.
 - c. If you selected the **Stop at specified time; allow to start after specified duration** mode:
 - In the **Task to stop at** field, enter the date and time at which the task will be stopped.
 - In the **After the task has stopped, allow to start again in, min** field, specify the time delay before the task can be restarted.
 - d. If you have selected the **Stop and allow to start at specified time** mode, perform the following steps:
 - In the **Stop the task at** field, enter the date and time at which the task will be stopped.
 - In the **Allow to start again at** field, enter the date and time after which the task can be restarted according to its schedule.
 - e. Click **OK** to save the changes.
7. Click **OK** to save the changes.

CREATING A TASK PAUSE RULE

If you start a task after a task stop rule has been applied (see page [161](#)), the task will restart from the beginning. A task pause rule allows you to resume a task from the point at which it was suspended.

➤ *To create a task pause rule:*



1. In the Administration Console tree, expand the **Managed computers** node and select the group to which the protected server belongs.
2. Right-click the line with the information about the protected server in the results pane and select the **Properties** command.
3. In the **Computer properties** dialog box open the **Tasks** tab. Open the context menu of the task you want to configure and select the **Properties** command.
4. In the **Task properties** dialog box open the **Schedule** tab.
5. Enable the task schedule by selecting the option **Run on schedule** in the lower part of the window.
6. Click the **Add** button, and in the **New pause rule for the task** window that will open:
 - a. Select the rule type from the dropdown list:
 - **Pause and resume after specified duration.** Kaspersky Anti-Virus will pause the task after the specified time has elapsed after its start. Additionally you can specify an amount of time after the task was paused, during which the task will not be restarted.
 - **Pause at specified time; resume after specified duration.** Kaspersky Anti-Virus will pause the task at the time you specified. Additionally you can specify an amount of time after the task was paused, during which the task will not be restarted.
 - **Pause and resume at specified time.** Kaspersky Anti-Virus will pause a task at the specified time; you can specify a time interval or exact time when the task can be restarted.
 - b. If you selected the **Pause and resume after specified duration** mode:
 - In the **Stop after the task has run for, min** field, enter the maximum time allowed for the task to run (minutes).
 - Specify the amount of time during which the task may not be started in the **After the task has stopped, allow to start in, min** field.
 - c. If you selected the **Pause at specified time; resume after specified duration** mode:
 - In the **Task to pause at** field, enter the date and time at which the task will be paused.
 - In the **After the task has stopped, allow to start again in, min** field, specify the time delay before the task can be restarted.
 - d. If you selected the **Pause and resume at specified time** mode:
 - In the **Task to pause at** field, enter the date and time at which the task will be paused.
 - Under the **Task resume time** heading, specify the date and time when Kaspersky Anti-Virus may restart the task by schedule.
 - e. Click **OK** to save the changes.
7. Click **OK** to save the changes.

CREATING AND CONFIGURING POLICIES

You can create global Kaspersky Administration Kit policies for managing protection on several servers where Kaspersky Anti-Virus is installed.

A policy applies all specified settings to all protected servers in one administration group.

You can create several policies for one administration group and enforce them in turns. The Administration Console assigns the **active** status to the policy in effect for a group at any given time.

While the policy is active, Kaspersky Anti-Virus applies the configuration values that you have set to  in the policy's properties instead of the values that were active for these settings before the policy took effect. Kaspersky Anti-Virus does not apply configuration values that you have not set to  in the policy's properties. When the effect of the policy is terminated, the settings whose values were modified by the policy retain the values they had while the policy was active.

Using policies, you can configure general Kaspersky Anti-Virus settings and update settings.

IN THIS SECTION

Creating a policy	164
Configuring a policy.....	164

CREATING A POLICY

➤ *To create a policy for a group of servers on which Kaspersky Anti-Virus is installed:*

1. In the Administration Console tree, expand the **Managed computers** node, expand administration group for whose servers you want to create the policies.
2. In the context menu of the **Policies** subnode, select the **Create** → **Policy** command.

This will open a policy creation wizard window.

3. In the **Policy name** window, enter the name of the policy being created in the input field (the name may not contain the characters " * < : > ? V |).
4. In the **Application** window, select **Kaspersky Anti-Virus 8.0 for Linux File Server** in the dropdown list.
5. In the **Creating a policy** window, select one of the following policy statuses:
 - **Active policy**, if you want the policy to become active immediately upon creation. If an active policy already exists in the group, this policy will become inactive and the policy you are creating will be activated.
 - **Inactive policy**, if you do not want the created policy to be activated immediately. In this case you will be able to activate the policy at a later time.

In the following policy creation wizard windows, specify the real-time protection task settings and update settings you require.

6. Use the **Protection areas** window to add one or several protection areas and select the interception method (see page [167](#)).
7. If necessary, use the **Exclusion areas** window to add one or several areas that do not need protection.
8. Click the **Finish** button in the **Completing the New Policy Wizard** window.

CONFIGURING A POLICY

You can use the **Properties** dialog window of an existing policy to configure general and update settings for Kaspersky Anti-Virus.

➤ To configure policy settings in the **Policy properties** dialog box:

1. In the Administration Console tree, expand the **Managed computers** node, expand the administration group whose policy settings you want to configure, and then expand the included **Policies** node.
2. In the result pane, open the context menu of the policy whose settings you want to configure and select the **Properties** command.
3. In the **<Policy Name> Properties** dialog box configure the required policy settings and click the **OK** button.

CHECKING CONNECTION WITH ADMINISTRATION SERVER MANUALLY. THE KLNAGCHK UTILITY

The Network Agent distribution kit includes the *klnagchk* utility to check the connection with the Administration Server.

Following installation of the Network Agent, the utility is located in the `/opt/kaspersky/klnagent/bin` directory and, when launched, performs the following actions in accordance with the keys in use:

- outputs to the screen or records in the log file the connection parameters used by the Network Agent installed on the client computer to connect to the Administration Server;
- outputs to the screen or in the log file the statistics about operation of the Network Agent, since its last launch, and the results of this utility operation;
- attempts to connect the Network Agent to the Administration Server;
- if the connection could not be established, sends an ICMP packet to verify the status of the computer on which the Administration Server is installed.

Utility command line syntax:

```
klnagchk [-logfile <file name>] [-sp] [-savecert <path to the certificate file>] [-restart]
```

The command line parameters are as follows:

- `-logfile <filename>` – log the connection parameters used by Network Agent to connect to the Administration Server and the results of the utility operation. By default the information will be stored in the `stdout.tx` file. If the modifier is not used, the parameters, results and error messages will be printed to the screen.
- `-sp` – display the password used to authenticate the user on the proxy server. This parameter is used if connection to the Administration Server is performed using a proxy server.
- `-savecert <filename>` – save the certificate used to access the Administration Server in the specified file.
- `-restart` – restart the Network Agent after the utility has completed.

CONNECTING TO ADMINISTRATION SERVER MANUALLY. THE KLMOVER UTILITY

The Network Agent distribution kit includes the *klmover* utility to manage the connection to the Administration Server.

Following installation of the Network Agent, the utility is located in the `/opt/kaspersky/klnagent/bin` directory and, when launched, performs the following actions in accordance with the keys in use:

- Connects the Network Agent to the Administration Server using the parameters supplied.
- Logs the results of the operation in the events log file, or displays them on the screen.

Utility command line syntax:

```
klmover [-logfile <file name>] {-address <server address>} [-pn <port number>] [-ps <SSL port number>] [-nossll] [-cert <path to certificate file>] [-silent] [-dupfix]
```

The command line parameters are as follows:

- `-logfile <file name>` – log the results of the utility operation to the specified file; if the key is not used, the results and error messages are output to stdout.
- `-address <server address>` – the address of the Administration Server for connection. The address can be represented by IP address, NetBIOS or DNS name of the server.
- `-pn <port number>` – number of the port that will be used for an unsecured connection to the Administration Server. The default value is 14000.
- `-ps <SSL port number>` – number of the port that will be used for a secured connection to the Administration Server using the Secure Sockets Layer (SSL) protocol. By default, port 13000 will be used.
- `-nossll` – use an unsecured connection to the Administration Server; if no modifier is used, a secure connection between the Network Agent and Administration Server will be established using the SSL protocol.
- `-cert <full path to the certificate file>` – use the specified certificate file for authentication when accessing the new Administration Server. If no modifier is used, the Network Agent will receive the certificate on its first connection to the Administration Server.
- `-silent` – launch the utility in non-interactive mode. This modifier can be useful, for instance, when launching the utility from the startup script when registering the user.
- `-dupfix` – this modifier is used if the Network Agent was installed using a method other than the regular installation from a distribution package. For example, it could have been restored from a drive image.

TASKS SETTINGS

IN THIS SECTION

Interception method	167
Protection mode	167
Heuristic analysis	168
Action to perform on infected objects	168
Action to be performed on suspicious objects	169
Actions to be performed on objects depending on the threat type	170
Excluding objects by name.....	170
Excluding objects by threat name	170
Scan of compound files	171
Maximum object scan time.....	171

Maximum size of a scanned object	172
Updates source	172
FTP server mode	172
FTP or HTTP server response wait time	172
Using a proxy server to connect to update sources	173
Proxy server authentication.....	173
Proxy server settings.....	173
Directory for saving updates.....	173
Updates type	173

INTERCEPTION METHOD

The **Scan on file access type** security setting is used only in real-time protection task.

Anti-Virus contains two components that intercept attempts to access files and scan them: a SAMBA interceptor (used to scan objects on remote computers when they are accessed via SMB/CIFS) and a kernel level interceptor. It scans objects when they are accessed in some other way.

The SAMBA interceptor provides, as additional object information, the IP address of the remote computer on which an application attempted an object access when it was intercepted by Kaspersky Anti-Virus.

If you use the protected computer only as a SAMBA server, you can set the **SAMBA only** value. In this case, Kaspersky Anti-Virus will not scan objects that are not accessed via SMB/CIFS.

Possible values include:

- **All operations.** Kaspersky Anti-Virus scans server objects with the SAMBA interceptor when they are accessed via SMB/CIFS. Kaspersky Anti-Virus uses the kernel level interceptor to intercept all other operations on files that are accessible on the protected server (including files on remote computers).
- **SAMBA only.** Kaspersky Anti-Virus scans objects with the SAMBA interceptor only when they are accessed via SMB/CIFS.

Make sure that you have specified the SAMBA VFS password during the initial configuration of Kaspersky Anti-Virus (see section Step 7. Integrating with Samba server" in the Installation Guide of Kaspersky Anti-Virus 8.0 for Linux File Server).

- **File system only.** Kaspersky Anti-Virus scans server objects without using the SAMBA interceptor.

Make sure that you have specified the SAMBA VFS password during the initial configuration of Kaspersky Anti-Virus (see section Step 6. Compiling the kernel module" in the Installation Guide of Kaspersky Anti-Virus 8.0 for Linux File Server).

PROTECTION MODE

The **Protection mode** security setting is used only in the real-time protection task.

The setting of this section is applied only in real-time protection task. It determines the type of access to the objects that ensures that Kaspersky Anti-Virus scans such objects.

Select one of the protection modes depending on your requirements to the server security, on which files are stored on the server, on the format of the files are stored in and on the information they contain:

- **Smart check.** Kaspersky Anti-Virus scans a file when an attempt is made to open it, and rescans it when an attempt is made to close it if the file has been modified. If a process accesses an object multiple times in the course of its operation and changes it, Kaspersky Anti-Virus scans the object a second time only when the process closes it for the last time.
- **When opened and modified.** Kaspersky Anti-Virus scans a file when an attempt is made to open it, and rescans it when an attempt is made to close it if the file has been modified.
- **When opened.** Kaspersky Anti-Virus scans the object when an attempt is made to open for reading or for execution or modification.

The default value is **Smart check**.

HEURISTIC ANALYSIS

The **Heuristic analysis** security setting is applied to real-time protection tasks and on-demand scan tasks.

Objects are scanned using databases which contain descriptions of all known malware and the corresponding disinfection methods. Kaspersky Internet Security compares each scanned object with the database's records to determine firmly if the object is malicious, and if so, into which class of malware it falls. This approach is called *signature analysis* and is always used by default.

Since new malicious objects appear daily, there is always some malware which is not described in the databases, and which can only be detected using a *heuristic analysis*. This method presumes the analysis of the actions an object performs within the system. If these actions are indicative of a malicious object, the object is likely to be classed as malicious or suspicious. Consequently, new threats are identified before they become known to virus analysts.

Additionally you can set the detail level for scans. It sets the balance between the thoroughness of searches for new threats, the load on the operating system's resources and the time required for scanning. The higher the detail level, the more resources the scan will require, and the longer it will take.

Select the **Heuristic analysis** check box to enable heuristic analysis.

Select one of the following values in accordance with your security requirements and the speed of the server's file exchange system:

- **Light scan;**
- **Medium;**
- **Deep scan.**

Default value: **Medium**.

ACTION TO PERFORM ON INFECTED OBJECTS

The **Action on infected object** security setting is used in real-time protection and on-demand scan tasks.

When Kaspersky Anti-Virus finds an object infected, it performs on it the action you have selected.

Select one of the following values:

- **Disinfect.** Kaspersky Anti-Virus attempts to disinfect the object, and if disinfection is not possible, it leaves the object intact.
- **Delete.** Kaspersky Anti-Virus removes the object.

- **Perform recommended action.** Kaspersky Anti-Virus automatically selects and performs the action on the object based on the data about the threat detected in the object and about the possibility of disinfecting it, for example, Anti-Virus will immediately remove Trojans since they do not incorporate themselves into other files and do not infect them; therefore they do not need to be disinfecting. This action can only be specified as the initial action to be taken on infected objects.
- **Skip.** The object remains intact: Kaspersky Anti-Virus does not attempt to disinfect or delete it. Information about the identified object will be recorded in the log.
- **Quarantine.** The object will be moved to a quarantine, in which it is stored in encrypted form.

Before modifying an object (through disinfection or removal), Kaspersky Anti-Virus saves a copy of the original object in the Backup storage area. If a copy of the object cannot be made, no attempt is made to disinfect or delete the object, which remains unchanged. Information concerning why Kaspersky Anti-Virus was not able to disinfect or delete the object will be recorded in the log.

Select from the list two actions which Kaspersky Anti-Virus will perform on the object. If Kaspersky Anti-Virus fails to perform the first action, it will perform the second action.

During real-time protection, Anti-Virus blocks access to an object for any application that attempts to access it, before actual operations with that object.

ACTION TO BE PERFORMED ON SUSPICIOUS OBJECTS

The **Action on suspicious object** security setting is used in real-time protection and on-demand scan tasks.

When Kaspersky Anti-Virus finds an object suspicious, it performs with it the action you have selected.

Select one of the following values:

- **Quarantine.** The object will be moved to a quarantine, in which it is stored in encrypted form.
- **Disinfect.** Kaspersky Anti-Virus attempts to disinfect the object, and if disinfection is not possible, it leaves the object intact.
- **Delete.** Kaspersky Anti-Virus removes a suspicious object from the server.

Before deleting the object Kaspersky Anti-Virus places a copy of such object into backup storage, in which objects are stored in encrypted form. Kaspersky Anti-Virus does not delete an object if it cannot first create a copy of the object in Backup. The object will remain intact. Information concerning why Kaspersky Anti-Virus was not able to remove the object will be recorded in the log.

- **Perform recommended action.** Kaspersky Anti-Virus selects and performs the action with the object based on the data about how dangerous the threat detected in the object is.
- **Skip.** The object is not altered: Kaspersky Anti-Virus does not attempt to disinfect or delete it, but logs relevant information about the object, including what malware it is suspected to contain.

Select from the list two actions which Kaspersky Anti-Virus will perform on the object. If Kaspersky Anti-Virus fails to perform the first action, it will perform the second action.

During real-time protection, Anti-Virus blocks access to an object for any application that attempts to access it, before actual operations with that object.

ACTIONS TO BE PERFORMED ON OBJECTS DEPENDING ON THE THREAT TYPE

The **Action to be performed on objects depending on the threat type** security setting is used in the real-time protection and on-demand scan tasks.

Threats of some types (classes) are more dangerous for the computer than others. For example, Trojans can do much more damage than adware. Using this setting, you can configure different actions to be taken by Kaspersky Anti-Virus with objects found to contain specified threats.

If you specify values for this setting, Kaspersky Anti-Virus will use them instead of the values of the Action on infected object setting (see page [168](#)) and the Action on suspicious object setting (see page [169](#)).

For each type of threat, select from the list two actions which Kaspersky Anti-Virus will perform on each object which presents that threat. If Kaspersky Anti-Virus fails to perform the first action, it will perform the second action.

If possible, Kaspersky Anti-Virus will apply selected actions both to infected and to suspicious objects.

If you select **Skip** as the first action, the second action will not be available.

If Kaspersky Anti-Virus fails to move an object to backup storage or quarantine, it will not take the next step on the object (for example, disinfecting or deleting it). The object will be considered skipped. You can review the reason for skipping the object in the log.

In the list of threat types, the **Network worms** and **Classical viruses** types are combined under the single name of **Viruses**.

EXCLUDING OBJECTS BY NAME

The **Excluding objects by name** security setting is used in real-time protection and on-demand scan tasks.

By default, Kaspersky Anti-Virus scans all objects within a protected area.

You can define name and path templates that are excluded from the protection area. In this case, Kaspersky Anti-Virus will not scan files or directories from the protection area that are specified using Shell masks or POSIX extended regular expressions.

You can use Shell masks to specify a file name template excluded from scanning by Kaspersky Anti-Virus.

You can also use extended regular expressions to specify a template for the paths to files which Kaspersky Anti-Virus should not scan. The regular expression should not contain the name of the directory containing excluded object.

Information on an object's exclusion from scanning is saved in the log.

EXCLUDING OBJECTS BY THREAT NAME

The **Excluding objects by threat name** security setting is used in real-time protection and on-demand scan tasks.

If Kaspersky Anti-Virus considers a scanned object to be infected or suspicious, it performs the action on this object specified in the task. If you consider this object to be harmless for the protected computer, you can exclude it from the scan scope by the name of threat detected in it. In this case Kaspersky Anti-Virus considers such objects as not infected and does not scan them.

The full name of the threat may contain the following information:

<threat class>:<threat type>.<brief name of operating system>.<threat name>.<threat modification code>. For example, **not-a-virus:NetTool.Linux.SynScan.a**.

You can find the full name of the threat detected in an object in the Kaspersky Anti-Virus log.

The complete names of threats identified in a program can also be found at the Virus Encyclopedia web site (see section Virus Encyclopedia - <http://www.viruslist.com>). To find the type of a threat, enter the name of the product in the **Search** field.

When specifying threat name templates, you can use Shell masks and POSIX extended regular expressions.

To exclude objects infected by a specific threat from scanning, specify either the threat's full name or a threat name template.

For example, you use a network information utility; Kaspersky Anti-Virus blocks it, classifying its code as a **Riskware** type of threat. You can add the complete name of a threat posed by a program to the list of excluded threats, for example, **not-a-virus:NetTool.Linux.SynScan.a**.

You can specify threat names using Shell masks or POSIX extended regular expressions. Regular POSIX expressions should be identified by the **re:** prefix.

For example, to skip files containing any threats to Linux which belong to the not-a-virus class, enter: **re:not-a-virus:.*\Linux\.***.

SCAN OF COMPOUND FILES

The **Check compound objects** security setting is used in real-time protection and on-demand scan tasks.

Processing composite objects is very time consuming. By default, Kaspersky Anti-Virus scans only composite objects of the types that are most susceptible to infection and that, when infected, are most harmful for the computer. Composite objects of other types are not scanned.

This setting allows the user, depending on the user's security requirements, to select the types of composite objects that Kaspersky Anti-Virus will scan.

Select one or several values:

- **Scan archives.** Kaspersky Anti-Virus scans file archives (including SFX self-extracting archives). Please note that Kaspersky Anti-Virus identifies threats in archives, but does not disinfect them.
- **Scan SFX archives.** Anti-Virus scans self-extracting archives (archives that contain an extraction module).
- **Scan mail databases.** Kaspersky Anti-Virus scans Microsoft Office Outlook and Microsoft Outlook Express mail database files.
- **Scan packed objects.** Kaspersky Anti-Virus scans executable files packed by binary code packers, such as UPX or ASPack. This type of composite object contains threats more often than others.
- **Scan mail formats.** Kaspersky Anti-Virus scans the files of plain text email messages.

MAXIMUM OBJECT SCAN TIME

The **Skip object if scan takes longer than** security level is applied to real-time protection tasks and on-demand scan tasks.

Kaspersky Anti-Virus stops scanning an object if the procedure takes longer than a specified time (in seconds). Information on an object's exclusion from scanning is saved in the log.

MAXIMUM SIZE OF A SCANNED OBJECT

The **Skip objects larger than** setting is used in real-time protection and on-demand scan tasks.

Kaspersky Anti-Virus skips an object if its size exceeds the specified value (in bytes). Information about skipped objects is stored in the log.

Possible values: 0-2147483647 (around 2 GB).

UPDATES SOURCE

You can select the source that Kaspersky Anti-Virus will use to obtain updates, depending on the update plan in effect at your company.

You can specify one of the following as the update source:

- **Kaspersky Lab's update servers.** Kaspersky Anti-Virus will download updates from one of the Kaspersky Lab update servers. Updates are downloaded via HTTP or FTP protocols.
- **Kaspersky Administration Server.** You can select this update source, if Kaspersky Administration Kit is used to centrally manage anti-virus protection in your organization. Kaspersky Anti-Virus will download updates to the protected server from the Kaspersky Administration Kit administration server installed in the LAN.
- **Other directories on the local network or the Web.** Kaspersky Anti-Virus will download updates from the source you have specified. You can specify directories on FTP or HTTP servers or directories on any device mounted on the server, including directories on remote computers mounted using SMB/CIFS or NFS protocols.

You can specify one or several user-defined update sources. Kaspersky Anti-Virus will always try the next specified source if the previous source is unavailable.

You can change the order in which Kaspersky Anti-Virus polls custom sources, and also configure it only to connect to selected sources on the list.

You can specify the order in which Kaspersky Anti-Virus will use the Kaspersky Lab update servers if all user-defined sources are unavailable.

Default value: Kaspersky Lab's update servers.

FTP SERVER MODE

By default, to connect to update servers using FTP, the Anti-Virus uses the passive FTP server mode: it is assumed that a network firewall is used in the enterprise LAN.

Default value: use passive FTP mode.

FTP OR HTTP SERVER RESPONSE WAIT TIME

This setting specifies the time to wait for a response from an update source FTP server or HTTP server while attempting to connect to it. If an update source does not respond within the specified time interval, Kaspersky Anti-Virus contacts the next update source on the list. For example, it will contact another Kaspersky Lab update server, if you have configured it to update from the servers of Kaspersky Lab.

Specify the response wait time in seconds. You can only use integers as the value for this setting.

Default value: **10 sec.**

USING A PROXY SERVER TO CONNECT TO UPDATE SOURCES

This parameter enables or disables the option to use a proxy server to connect to update sources.

If you have specified Kaspersky Lab's update servers as the source of updates, you should select the option **Use proxy server to connect to Kaspersky Lab's update servers** if you access the Internet via a proxy server.

If you use a proxy server to connect to a custom FTP or HTTP server, select the option **Use proxy server to connect to custom update sources**.

Default values:

- Kaspersky Anti-Virus accesses a proxy server when connecting to Kaspersky Lab's update servers.
- Kaspersky Anti-Virus does not use a proxy server when connecting to user-defined update sources (either HTTP or FTP servers or user-specified computers). It is assumed that these sources are located on the local network.

PROXY SERVER AUTHENTICATION

This setting enables authentication when accessing a proxy server being used for connections to FTP or HTTP update source servers.

Enable the **Use authentication** mode and specify **Name** and **Password**.

Default value: no authentication required to connect to a proxy server.

PROXY SERVER SETTINGS

If you have enabled the use of a proxy server to connect to an update source, specify the proxy server settings.

Specify the IP address or the server's DNS name (for example, proxy.mycompany.com) and the port.

Default value: not configured.

DIRECTORY FOR SAVING UPDATES

This setting is used if the update process uses either of these options: **Copy all updates available for the application** or **Copy updates for selected modules**. Using this setting specify the directory into which the update files will be saved.

You can specify a directory on any disk mounted on the server.

Default value: not configured.

UPDATES TYPE

You can use this setting to select a function to be performed by the update task.

Select one of the following values:

- **Update databases only**. Kaspersky Anti-Virus will download and install database updates.
- **Copy all updates available for the application**. Select this value to download and save all accessible Kaspersky Anti-Virus updates in a directory without applying them.

- **Copy updates for selected modules.** Select this option to download selected updates only. Kaspersky Anti-Virus will save the downloaded updates in the specified directory without installing them.

You can download updates for other Kaspersky Lab applications if you wish to use the protected computer as an intermediary for distributing updates. You can review the names of update components in the document http://support.kaspersky.com/downloads/updater/update_components_21112008.pdf, which is available on the Kaspersky Lab Technical Support web site.

Critical updates for Kaspersky Anti-Virus modules are not installed automatically.

Default value: **Update databases only.**

KASPERSKY LAB ZAO

Kaspersky Lab was founded in 1997. Today it is the leading Russian developer of a wide range of high-performance information security software products, including anti-virus, anti-spam and anti-hacking systems.

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

Today, Kaspersky Lab employs over a thousand highly qualified specialists, including 10 MBA degree holders and 16 PhD degree holders. All Kaspersky Lab's senior anti-virus experts are members of the Computer Anti-Virus Researchers Organization (CARO).

Our company's most valuable assets are the unique knowledge and collective expertise accumulated during fourteen years of continuous battle against computer viruses. Thorough analysis of computer virus activities enables the company's specialists to anticipate trends in the development of malware, and to provide our users with timely protection against new types of attacks. This advantage is the basis of Kaspersky Lab's products and services. The company's products remain one step ahead of other vendors in delivering comprehensive anti-virus coverage to our clients.

Years of hard work have made the company one of the top anti-virus software developers. Kaspersky Lab was the first to develop many modern anti-virus software standards. The company's flagship product, Kaspersky Anti-Virus, reliably protects all types of computer systems against virus attacks, including workstations, file servers, mail systems, firewalls, Internet gateways and hand-held computers. Its easy-to-use management tools maximize the automation of anti-virus protection for computers and corporate networks. A large number of developers worldwide use the Kaspersky Anti-Virus kernel in their products, including Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India), and BorderWare (Canada).

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

If you have any questions, please refer them to one of our distributors or directly to Kaspersky Lab ZAO. We will be glad to assist you, via phone or email, in any matters related to our products. You will receive full and comprehensive answers to all your questions.

Kaspersky Lab official site: <http://www.kaspersky.com>

Virus Encyclopedia: <http://www.securelist.com>

Anti-virus laboratory: newvirus@kaspersky.com
(only for sending archives of suspicious objects)
<http://support.kaspersky.ru/helpdesk.html?LANG=en>
(for queries to virus analysts)

INFORMATION ABOUT THIRD-PARTY CODE

Third-party code was used during the application development.

IN THIS SECTION

Program code.....	176
Distributed program code.....	198
Other information	198

PROGRAM CODE

Information on the third-party code used when creating the application.

IN THIS SECTION

APACHE 1.3.41	177
EXPAT 1.95.8	183
GSOAP	183
JQUERY 1.3.2.....	188
LIBHARU 2.1.0.....	189
LIBXML2-2.6.32	189
LIBXSLT-1.1.23.....	189
LIBPCRE 7.4.....	190
ZLIB 1.2.3.....	191
BOOST 1.39.0.....	191
LIBACL 2.2.45-1.....	191
ATTR 2.4.38-1.....	191
LIBPNG 1.2.44.....	192
LIBUTF	192
LZMALIB 4.43	192
NET-SNMP 5.5	192
SQLITE 3.6.17	196
DEJAVU SANS 2.31	196

APACHE 1.3.41

Apache License

Version 2.0, January 2004

<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purpose of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or addition to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license

to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

- (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
- (b) You must cause any modified files to carry prominent notices stating that You changed the files; and
- (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
- (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole,

provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly

negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APACHE HTTP SERVER SUBCOMPONENTS:

The Apache HTTP Server includes a number of subcomponents with separate copyright notices and license terms. Your use of the source code for the these subcomponents is subject to the terms and conditions of the following licenses.

For the MD5 Message-Digest library component:

Copyright (C) 1995, Board of Trustees of the University of Illinois

(C) Copyright 1993,1994 by Carnegie Mellon University

All Rights Reserved.

Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Carnegie Mellon University not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Carnegie

Mellon University makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (c) 1991 Bell Communications Research, Inc. (Bellcore)

Permission to use, copy, modify, and distribute this material for any purpose and without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies, and that the name of Bellcore not be used in advertising or publicity pertaining to this material without the specific, prior written permission of an authorized representative of Bellcore.

BELLCORE MAKES NO REPRESENTATIONS ABOUT THE ACCURACY OR SUITABILITY OF THIS MATERIAL FOR ANY PURPOSE. IT IS PROVIDED "AS IS",

WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES.

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

"THE BEER-WARE LICENSE" (Revision 42):

<phk@login.dknet.dk> wrote this file. As long as you retain this notice you can do whatever you want with this stuff. If we meet some day, and you think this stuff is worth it, you can buy me a beer in return. Poul-Henning Kamp

For the expat-lite library component:

Copyright (c) 1998, 1999 James Clark. Expat is subject to the Mozilla Public License Version 1.1. Alternatively you may use expat under the GNU General Public License instead.

For the regex library component:

Copyright 1992, 1993, 1994 Henry Spencer. All rights reserved.

This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it, subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from flaws in it.
2. The origin of this software must not be misrepresented, either by explicit claim or by omission. Since few users ever read sources, credits must appear in the documentation.
3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software. Since few users ever read sources, credits must appear in the documentation.
4. This notice may not be removed or altered.

For the expat xml parser library component:

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd and Clark Cooper

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

For the mod_mime_magic component:

Copyright (c) 1996-1997 Cisco Systems, Inc.

This software was submitted by Cisco Systems to the Apache Group in July 1997. Future revisions and derivatives of this source code must acknowledge Cisco Systems as the original contributor of this module. All other licensing and usage conditions are those of the Apache Group.

Some of this code is derived from the free version of the file command originally posted to comp.sources.unix. Copyright info for that program is included below as required.

Copyright (c) Ian F. Darwin, 1987. Written by Ian F. Darwin.

This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it freely, subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from flaws in it.

2. The origin of this software must not be misrepresented, either by explicit claim or by omission. Since few users ever read sources, credits must appear in the documentation.
3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software. Since few users ever read sources, credits must appear in the documentation.
4. This notice may not be removed or altered.

For the mod_imap component: "macmartinized" polygon code copyright 1992 by Eric Haines, erich@eye.com

For the zb test and ab support components:

This program is Copyright (C) Zeus Technology Limited 1996.

This program may be used and copied freely providing this copyright notice is not removed.

This software is provided "as is" and any express or implied warranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall Zeus Technology Ltd. be liable for any direct, indirect, incidental, special, exemplary, or consequential damaged (including, but not limited to, procurement of substitute good or services; loss of use, data, or profits; or business interruption) however caused and on theory of liability. Whether in contract, strict liability or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

NOTICE

Apache HTTP Server

Copyright 2006 The Apache Software Foundation.

This product includes software developed at

The Apache Software Foundation (<http://www.apache.org/>).

Portions of this software were developed at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign.

This software contains code derived from the RSA Data Security Inc. MD5 Message-Digest Algorithm, including various modifications by Spyglass Inc., Carnegie Mellon University, and Bell Communications Research, Inc (Bellcore).

This work includes the Expat xml parsing library Copyright (c) 1998, 1999 James Clark, distributed under and subject to the Mozilla Public License Version 1.1.

This work includes the regex library Copyright 1992, 1993, 1994 Henry Spencer, all rights reserved.

EXPAT 1.95.8

Copyright (C) 1998, 1999, 2000, Thai Open Source Software Center Ltd and Clark Cooper

Copyright (C) 2001, 2002, 2003, 2004, 2005, 2006, Expat maintainers

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

GSOAP

gSOAP license

"Part of the software embedded in this product is gSOAP software.

Portions created by gSOAP are Copyright (C) 2001-2004 Robert A. van Engelen, Genivia inc. All Rights Reserved.

THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY GENIVIA INC AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

gSOAP Public License

1.1.1 Version 1.3a

The gSOAP public license is derived from the Mozilla Public License (MPL1.1). The sections that were deleted from the original MPL1.1 text are 1.0.1, 2.1.(c),(d), 2.2.(c),(d), 8.2.(b), 10, and 11. Section 3.8 was added. The modified sections are 2.1.(b), 2.2.(b), 3.2 (simplified), 3.5 (deleted the last sentence), and 3.6 (simplified).

1.2 1 DEFINITIONS.

1.0.1.

1.1. "Contributor"

means each entity that creates or contributes to the creation of Modifications.

1.2. "Contributor Version"

means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. "Covered Code"

means the Original Code, or Modifications or the combination of the Original Code, and Modifications, in each case including portions thereof.

1.4. "Electronic Distribution Mechanism"

means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. "Executable"

means Covered Code in any form other than Source Code.

1.6. "Initial Developer"

means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.

1.7. "Larger Work"

means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1.8. "License"

means this document.

1.8.1. "Licensable"

means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. "Modifications"

means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

A.

Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.

B.

Any new file that contains any part of the Original Code, or previous Modifications.

1.10. "Original Code"

means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.10.1. "Patent Claims"

means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. "Source Code"

means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the

Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. "You" (or "Your")

means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

1.3 2 SOURCE CODE LICENSE.

2.1. The Initial Developer Grant.

The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:

(a)

under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and

(b)

under patents now or hereafter owned or controlled by Initial Developer, to make, have made, use and sell ("offer to sell and import") the Original Code, Modifications, or portions thereof, but solely to the extent that any such patent is reasonably necessary to enable You to utilize, alone or in combination with other software, the Original Code, Modifications, or any combination or portions thereof.

(c)

(d)

2.2. Contributor Grant.

Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license

(a)

under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and

(b)

under patents now or hereafter owned or controlled by Contributor, to make, have made, use and sell ("offer to sell and import") the Contributor Version (or portions thereof), but solely to the extent that any such patent is reasonably necessary to enable You to utilize, alone or in combination with other software, the Contributor Version (or portions thereof).

(c)

(d)

1.4 3 DISTRIBUTION OBLIGATIONS.

3.1. Application of License.

The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section 2.2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with

every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.5.

3.2. Availability of Source Code.

Any Modification created by You will be provided to the Initial Developer in Source Code form and are subject to the terms of the License.

3.3. Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters.

(a) Third Party Claims.

If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs.

If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the LEGAL file.

(c) Representations.

Contributor represents that, except as disclosed pursuant to Section 3.4(a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

3.5. Required Notices.

You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor.

3.6. Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Section 3.1-3.5 have been met for that Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. If you distribute executable versions containing Covered Code as part of a product, you must reproduce the notice in Exhibit B in the documentation and/or other materials provided with the product.

3.7. Larger Works.

You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

3.8. Restrictions.

You may not remove any product identification, copyright, proprietary notices or labels from gSOAP.

1.5 4 INABILITY TO COMPLY DUE TO STATUTE OR REGULATION.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the LEGAL file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

1.6 5 APPLICATION OF THIS LICENSE.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A and to related Covered Code.

1.7 6 VERSIONS OF THE LICENSE.

6.1. New Versions.

Grantor may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2. Effect of New Versions.

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License.

6.3. Derivative Works.

If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrase "gSOAP" or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the gSOAP Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

1.8 7 DISCLAIMER OF WARRANTY.

COVERED CODE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, OF FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS, AND ANY WARRANTY THAT MAY ARISE BY REASON OF TRADE USAGE, CUSTOM, OR COURSE OF DEALING. WITHOUT LIMITING THE FOREGOING, YOU ACKNOWLEDGE THAT THE SOFTWARE IS PROVIDED "AS IS" AND THAT THE AUTHORS DO NOT WARRANT THE SOFTWARE WILL RUN UNINTERRUPTED OR ERROR FREE. LIMITED LIABILITY THE ENTIRE RISK AS TO RESULTS AND PERFORMANCE OF THE SOFTWARE IS ASSUMED BY YOU. UNDER NO CIRCUMSTANCES WILL THE AUTHORS BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES OF ANY KIND OR NATURE WHATSOEVER, WHETHER BASED ON CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, ARISING OUT OF OR IN ANY WAY RELATED TO THE SOFTWARE, EVEN IF THE AUTHORS HAVE BEEN ADVISED ON THE POSSIBILITY OF SUCH DAMAGE OR IF SUCH DAMAGE COULD HAVE BEEN REASONABLY FORESEEN, AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY EXCLUSIVE REMEDY PROVIDED. SUCH LIMITATION ON DAMAGES INCLUDES, BUT IS NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOST PROFITS, LOSS OF DATA OR SOFTWARE, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION OR IMPAIRMENT OF OTHER GOODS. IN NO EVENT WILL THE AUTHORS BE LIABLE FOR THE COSTS OF PROCUREMENT OF SUBSTITUTE SOFTWARE OR SERVICES. YOU ACKNOWLEDGE THAT THIS SOFTWARE IS NOT DESIGNED FOR USE IN ON-LINE EQUIPMENT IN HAZARDOUS ENVIRONMENTS SUCH AS OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR

CONTROL, OR LIFE-CRITICAL APPLICATIONS. THE AUTHORS EXPRESSLY DISCLAIM ANY LIABILITY RESULTING FROM USE OF THE SOFTWARE IN ANY SUCH ON-LINE EQUIPMENT IN HAZARDOUS ENVIRONMENTS AND ACCEPTS NO LIABILITY IN RESPECT OF ANY ACTIONS OR CLAIMS BASED ON THE USE OF THE SOFTWARE IN ANY SUCH ON-LINE EQUIPMENT IN HAZARDOUS ENVIRONMENTS BY YOU. FOR PURPOSES OF THIS PARAGRAPH, THE TERM "LIFE-CRITICAL APPLICATION" MEANS AN APPLICATION IN WHICH THE FUNCTIONING OR MALFUNCTIONING OF THE SOFTWARE MAY RESULT DIRECTLY OR INDIRECTLY IN PHYSICAL INJURY OR LOSS OF HUMAN LIFE. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED CODE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

1.9 8 TERMINATION.

8.1.

This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2.

8.3.

If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken into account in determining the amount or value of any payment or license.

8.4.

In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

1.10 9 LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED CODE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

1.11 10 U.S. GOVERNMENT END USERS.

1.12 11 MISCELLANEOUS.

1.13 12 RESPONSIBILITY FOR CLAIMS.

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

JQUERY 1.3.2

Copyright (c) 2009 John Resig, <http://jquery.com/>.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LIBHARU 2.1.0

Copyright (C) 1999-2006 Takeshi Kanno

Copyright (C) 2007-2008 Antony Dovgal

LIBXML2-2.6.32

Copyright (C) 1998-2003 Daniel Veillard

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE DANIEL VEILLARD BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of Daniel Veillard shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from him.

LIBXSLT-1.1.23

Licence for libxslt except libxslt

Copyright (C) 2001-2002 Daniel Veillard. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE DANIEL VEILLARD BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of Daniel Veillard shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from him.

Licence for libexslt

Copyright (C) 2001-2002 Thomas Broyer, Charlie Bozeman and Daniel Veillard.

All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of the authors shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from him.

LIBPCRE 7.4

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 5 of PCRE is distributed under the terms of the "BSD" license, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

Copyright (c) 1997-2004 University of Cambridge

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

ZLIB 1.2.3

Copyright (C) 1995-2004, Jean-loup Gailly and Mark Adler

BOOST 1.39.0

Copyright (C) 2008, Beman Dawes, Rene Rivera

LIBACL 2.2.45-1

Copyright (C) 2002, Andreas Gruenbacher <agruen@suse.de>, SuSE Linux AG

ATTR 2.4.38-1

Copyright (C) 2000-2002, 2004, Silicon Graphics, Inc

Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 2 of the License

Distributed under the terms of the [GNU] Lesser General Public License as published by the Free Software Foundation, version 2.1 of the License

LIBPNG 1.2.44

Copyright (C) 2004, 2006-2009, Glenn Randers-Pehrson

LIBUTF

Copyright (C) 2002, Lucent Technologies

Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. IN PARTICULAR, NEITHER THE AUTHORS NOR LUCENT TECHNOLOGIES MAKE ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

LZMALIB 4.43

NET-SNMP 5.5

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) ----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) ----

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) ----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR

BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) ----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara,

California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) ----

Copyright (c) 2003-2008, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) ----

Copyright (c) 2004, Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) ----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003

oss@fabasoft.com

Author: Bernhard Penz

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 8: Apple Inc. copyright notice (BSD) ----

Copyright (c) 2007 Apple Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of Apple Inc. ("Apple") nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND

FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL APPLE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 9: ScienceLogic, LLC copyright notice (BSD) ----

Copyright (c) 2009, ScienceLogic, LLC

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of ScienceLogic, LLC nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

SQLITE 3.6.17

DEJAVU SANS 2.31

Copyright (C) 2003, Bitstream, Inc

Copyright (C) 2006, Tavmjong Bah

Fonts are © Bitstream (see below). DejaVu changes are in public domain. Explanation of copyright is on Gnome page on Bitstream Vera fonts. Glyphs imported from Arev fonts are © Tavmjong Bah (see below)

Bitstream Vera Fonts Copyright

Copyright (c) 2003 by Bitstream, Inc. All Rights Reserved. Bitstream Vera is a trademark of Bitstream, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of the fonts accompanying this license ("Fonts") and associated documentation files (the "Font Software"), to reproduce and distribute the Font Software, including without limitation the rights to use, copy, merge, publish, distribute, and/or sell copies of the Font Software, and to permit persons to whom the Font Software is furnished to do so, subject to the following conditions:

The above copyright and trademark notices and this permission notice shall be included in all copies of one or more of the Font Software typefaces.

The Font Software may be modified, altered, or added to, and in particular the designs of glyphs or characters in the Fonts may be modified and additional glyphs or characters may be added to the Fonts, only if the fonts are renamed to names not containing either the words "Bitstream" or the word "Vera".

This License becomes null and void to the extent applicable to Fonts or Font Software that has been modified and is distributed under the "Bitstream Vera" names.

The Font Software may be sold as part of a larger software package but no copy of one or more of the Font Software typefaces may be sold by itself.

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL BITSTREAM OR THE GNOME FOUNDATION BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

Except as contained in this notice, the names of Gnome, the Gnome Foundation, and Bitstream Inc., shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Font Software without prior written authorization from the Gnome Foundation or Bitstream Inc., respectively. For further information, contact: fonts at gnome dot org.

Arev Fonts Copyright

Original text

Copyright (c) 2006 by Tavmjong Bah. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of the fonts accompanying this license ("Fonts") and associated documentation files (the "Font Software"), to reproduce and distribute the modifications to the Bitstream Vera Font Software, including without limitation the rights to use, copy, merge, publish, distribute, and/or sell copies of the Font Software, and to permit persons to whom the Font Software is furnished to do so, subject to the following conditions:

The above copyright and trademark notices and this permission notice shall be included in all copies of one or more of the Font Software typefaces.

The Font Software may be modified, altered, or added to, and in particular the designs of glyphs or characters in the Fonts may be modified and additional glyphs or characters may be added to the Fonts, only if the fonts are renamed to names not containing either the words "Tavmjong Bah" or the word "Arev".

This License becomes null and void to the extent applicable to Fonts or Font Software that has been modified and is distributed under the "Tavmjong Bah Arev" names.

The Font Software may be sold as part of a larger software package but no copy of one or more of the Font Software typefaces may be sold by itself.

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL TAVMJONG BAH BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

Except as contained in this notice, the name of Tavmjong Bah shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Font Software without prior written authorization from Tavmjong Bah. For further information, contact: tavmjong@free.fr.

PROTOTYPE-1.6.0.3

Copyright (C) 2005-2008, Sam Stephenson

DISTRIBUTED PROGRAM CODE

The structure of this product includes the third-party binary code.

IN THIS SECTION

REDIRFS 0.10 (MODIFIED)..... [198](#)

REDIRFS 0.10 (MODIFIED)

Copyright (C) 2008-2010, Frantisek Hrbata

Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 3 of the License

OTHER INFORMATION

Additional information about third-party code

Agava-C program library, developed by OOO "R-Alpha", is used to check digital signature.

The Software may include some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar free software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code ("Open Source Software"). If such licenses require that for any software, which is distributed to someone in an executable binary format, that the source code also be made available to those users, then the source code should be made available by sending the request to source@kaspersky.com or the source code is supplied with the Software.

=====

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the

software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright

notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of

the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details

type `show w'. This is free software, and you are welcome

to redistribute it under certain conditions; type `show c'

for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision'

(which makes passes at compilers) written

by James Hacker.

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the [GNU Lesser General Public License](#) instead of this License.

=====

GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <<http://fsf.org/>>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

- a) The work must carry prominent notices stating that you modified it, and giving a relevant date.
- b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".
- c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.
- d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

- a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.
- b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.
- c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.
- d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.
- e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

- a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or
- b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or
- c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or
- d) Limiting the use for publicity purposes of names of licensors or authors of the material; or
- e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or
- f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <<http://www.gnu.org/licenses/>>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>

This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.

This is free software, and you are welcome to redistribute it

under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, your program's commands might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school, if any, to sign a "copyright disclaimer" for the program, if necessary. For more information on this, and how to apply and follow the GNU GPL, see <http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License. But first, please read <http://www.gnu.org/philosophy/why-not-lgpl.html>.

=====

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its

contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the library's name and an idea of what it does.

Copyright (C) year name of author

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either

version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

signature of Ty Coon, 1 April 1990

Ty Coon, President of Vice

That's all there is to it!

=====