

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 document will help you in your work and will provide answers regarding this software product.

Note! This document is the property of Kaspersky Lab ZAO (herein also referred to as Kaspersky Lab): all rights to this document are reserved by the copyright laws of the Russian Federation, and by international treaties. Illegal reproduction 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.

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

This document may be amended without additional notification. For the latest version of this document, refer to the Kaspersky Lab website at <http://www.kaspersky.com/docs>.

Kaspersky Lab assumes no liability for the content, quality, relevance, or accuracy of any materials used 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 uses registered trademarks and service marks which are the property of their respective owners.

Revision date: 6/7/11

© 1997-2011 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.....	17
Launching the Web Management Console.....	17
Changing the user password for the Web Management Console.....	17
STARTING AND STOPPING KASPERSKY ANTI-VIRUS	19
MANAGING THE TASKS IN KASPERSKY ANTI-VIRUS	20
Creating an on-demand scan or update task.....	20
Deleting an on-demand scan or update task	21
Manual task management	21
Automatic task management	21
Viewing task state.....	22
Viewing task statistics.....	23
UPDATING KASPERSKY ANTI-VIRUS.....	24
Selecting an update source	25
Updating from local or network folder	25
Using the proxy server.....	27
Last database update rollback.....	27
REAL-TIME PROTECTION.....	29
The structure of predefined security levels in the real-time protection task	29
Creating a protection scope.....	32
Restricting a protection area using masks and regular expressions	33
Exclusion of objects from a protection area	34
Creating a global exclusion area.....	34
Excluding objects from the protection area	35
Exclusion of objects depending on user and group accounts accessing the objects	36
Excluding objects by names of the threats detected in them	36
Selecting interception mode	37
Selecting protection mode	37
Using heuristic analysis	38
Using scan mode depending on user and group accounts accessing the objects.....	38
Selecting actions to perform on detected objects	39
Selecting actions depending on the threat type.....	40
Scan optimization	41
Compatibility with other Kaspersky Lab's applications.....	42

ON-DEMAND SCAN	45
The structure of predefined security levels in on-demand scan tasks	45
Quick scan of files and directories	48
Creating a scan area	50
Restricting a scan area using masks and regular expressions	51
Excluding objects from the scan area	51
Creating a global exclusion area	51
Excluding objects from the scan area	52
Excluding objects by names of the threats detected in them	53
Using heuristic analysis	53
Selecting actions to perform on detected objects	54
Selecting actions depending on the threat type	55
Scan optimization	56
Selecting task priority	57
ISOLATING SUSPICIOUS OBJECTS. DATA BACKUP	58
Viewing statistics of quarantined objects	58
Scanning quarantined objects	59
Placing files to quarantine manually	60
Viewing object IDs	60
Restoring objects	61
Deleting objects	62
MANAGING LICENSES	62
About the License Agreement	63
About licenses for Kaspersky Anti-Virus	63
About Kaspersky Anti-Virus key files	64
Installing the key file	64
Viewing information about a license prior to the key file installation	65
Key file removal	65
Reviewing the license agreement	66
ADMINISTRATOR NOTIFICATIONS. EVENT-BASED ACTIONS	67
Using the internal mailer of Kaspersky Anti-Virus	68
Using Sendmail	69
Generation of notifications	69
Configuring actions	70
Using macros	70
GENERATING REPORTS	72
VIEWING THE PROTECTION STATUS VIA SNMP	73
Configuring interaction via SNMP	73
Structure of the Kaspersky Anti-Virus MIB	74
Description of Kaspersky Anti-Virus MIB objects	76
MANAGING KASPERSKY ANTI-VIRUS FROM THE COMMAND LINE	80
Displaying Kaspersky Anti-Virus command help	82
Starting Kaspersky Anti-Virus	83
Stopping Kaspersky Anti-Virus	83
Restarting Kaspersky Anti-Virus	83
Enabling events output	84

Quick scan of files and directories	84
Rollback of Kaspersky Anti-Virus databases	85
Commands for obtaining reports and statistics	85
Viewing application information.....	85
Viewing Anti-Virus activity reports.....	86
Viewing reports on the most commonly encountered threats.....	87
Commands for managing the Anti-Virus settings and tasks	89
Viewing general settings of Kaspersky Anti-Virus	89
Editing the general settings of Kaspersky Anti-Virus.....	90
Viewing the list of Kaspersky Anti-Virus tasks.....	91
Viewing task state	92
Starting the task	93
Stopping the task	93
Pausing the task	94
Resuming the task	94
Obtaining task settings.....	95
Modifying task settings.....	96
Creating a task.....	97
Deleting tasks	97
Obtaining task schedule settings	98
Modifying task schedule settings	99
Deleting the task schedule	100
Searching for scheduled events.....	100
Licenses management commands	102
Validating a key file prior to installation	102
Viewing information about a license prior to the key file installation.....	103
Viewing information about the installed key files.....	103
Viewing the status of installed licenses	104
Active key file installation	104
Supplementary key file installation.....	105
Active key file removal	105
Supplementary key file removal	105
Quarantine and backup storage management commands	106
Obtaining brief quarantine or backup storage statistics	106
Obtaining information about storage objects.....	106
Obtaining information about one object in the storage.....	107
Restoring objects from the storage	107
Placing an object in quarantine manually.....	108
Deleting one object from the storage	108
Exporting objects from the storage into a specified directory	109
Importing previously exported objects into the storage	109
Clearing the storage.....	110
Logs management commands	111
Obtaining the number of Anti-Virus events, using a filter	111
Obtaining information about Kaspersky Anti-Virus events	111
Viewing the time interval, during which the events will occur that are registered in the log	112
Event log rotation	113
Removing objects from the event log.....	113
Limiting selections using filters	114

Logical expressions	114
Object parameters in quarantine / backup storage	115
Anti-Virus events and their data	118
ANTI-VIRUS CONFIGURATION FILE SETTINGS	126
Rules for editing Kaspersky Anti-Virus INI configuration files	126
Real-time protection and on-demand scan tasks settings	127
Update tasks settings	141
Schedule settings	145
General settings of Kaspersky Anti-Virus	148
Quarantine and backup storage settings	150
Event log settings	151
Settings of notifications and event-based actions.....	152
MANAGING KASPERSKY ANTI-VIRUS VIA KASPERSKY ADMINISTRATION KIT	155
Viewing the server protection status	155
The "Application Settings" dialog box	156
Creating and configuring tasks	156
Creating a task	156
The Local task creation wizard	157
Step 1. Entering general task settings	158
Step 2. Selecting an application and defining task type	158
Step 3. Configuring task settings	158
Step 4. Scheduling the task	158
Step 5. Completing the wizard	159
Updating tasks settings.....	159
Creating a scan area.....	159
Configuring security settings	160
Creating an excluded area.....	160
Selecting an update source.....	161
Selecting the type of updates.....	162
Scheduling a task via Kaspersky Administration Kit	163
Creating a task start rule	163
Configuring task schedule.....	163
Creating and configuring policies.....	165
Creating a policy	166
Configuring a policy	166
Checking connection with Administration Server manually. The klnagchk utility	166
Connecting to Administration Server manually. The klmover utility	167
Tasks settings.....	168
Interception method	169
Protection mode.....	169
Heuristic analysis	169
Action to perform on infected objects.....	170
Action to be performed on suspicious objects.....	171
Actions to be performed on objects depending on the threat type	171
Excluding objects by name	172
Excluding objects by threat name	172
Scan of compound files.....	172
Maximum object scan time.....	173

Maximum size of a scanned object	173
Updates source	173
FTP server mode	174
FTP or HTTP server response wait time	174
Using a proxy server to connect to update sources	174
Proxy server authentication.....	174
Proxy server settings	174
Directory for saving updates	175
Updates type.....	175
KASPERSKY LAB ZAO	176
INFORMATION ABOUT THIRD-PARTY CODE	177

INTRODUCTION

Kaspersky Anti-Virus protects servers running under Linux operating system 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 the 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. 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 Kaspersky 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 disinfecting.

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. 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 disinfected 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/klnagent/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/klnagent/share/man/man1/klnagchk.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>).

Technical Support by email

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 ask your question 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 the problem encountered in detail.
- **Client number and password.** Enter the client number and the password you have received during the registration at the Technical Support service website.
- **Email address.** The Technical Support service will send their answer to this email address.

Technical support by phone

If you have a problem which requires urgent help, you can call your nearest Technical Support office. When you apply to Russian-speaking (<https://support.kaspersky.com/en/PersonalCabinet>) 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 immediate answer, you can discuss it with the Kaspersky Lab experts and other users in our forum 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 WebManagement 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 runs all predefined and custom tasks, schedule settings (see section "Schedule settings" on page [145](#)) which is set to run PS.

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 those custom tasks in the schedule settings (see section "Schedule settings" on page [145](#)) which is set to launch PS, will be launched again.

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

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

➤ To stop *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 server 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 [21](#)):

- **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	20
Deleting an on-demand scan or update task.....	21
Manual task management.....	21
Automatic task management.....	21
Viewing task state	22
Viewing task statistics	23

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 (see section "Creating a task" on page [97](#)).

➤ 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 \  
  
[--file=<configuration file name>] [--file-format=<INI|XML>]
```

The settings for the created task are as follows:

- all local and mounted objects will be scanned;

- scan will be done with default settings.

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>
```

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 <update 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 specify the start time and duration of the task.

The following types of tasks support automatic management:

- real-time protection;

- on-demand scan;
- databases update.

➤ *To schedule a task using a configuration file, perform the following steps:*

1. Save the task scheduling 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. Configure the schedule settings (see page [145](#)).
3. 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>
```

The following example displays the command output:

Example:

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 Kaspersky 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..... [25](#)

Updating from local or network folder..... [25](#)

Using the proxy server [27](#)

Last database update rollback [27](#)

SELECTING AN UPDATE SOURCE

Update source (see page [173](#)) 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 [25](#)).

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 Kaspersky Anti-Virus update package from Kaspersky Lab's update servers, or from a mirror server hosting a current set of updates.
2. The retrieved updates are placed in a shared folder.
3. 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.
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"
[RetranslateUpdatesSettings]
RetranslationFolder="<full path to the created directory>"

```

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

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. 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 server file system. By default, the real-time protection task runs automatically at the start of Kaspersky Anti-Virus. The task runs in the server'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	29
Creating a protection scope	32
Restricting a protection area using masks and regular expressions	33
Exclusion of objects from a protection area.....	34
Selecting interception mode	37
Selecting protection mode.....	37
Using heuristic analysis.....	38
Using scan mode depending on user and group accounts accessing the objects	38
Selecting actions to perform on detected objects.....	39
Selecting actions depending on the threat type.....	40
Scan optimization.....	41
Compatibility with other Kaspersky Lab's applications	42

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 Kaspersky 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="Recommended"
[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="Recommended"
[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="Recommended"

[ScanScope:ScanSettings:AdvancedActions]

Verdict="Riskware"

FirstAction="Skip"

SecondAction="Skip"

```

CREATING A PROTECTION SCOPE

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

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 [33](#)).

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 [38](#));
 - **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 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. 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 ECMA-262 regular expressions.

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

Using 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 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	34
Excluding objects from the protection area	35
Exclusion of objects depending on user and group accounts accessing the objects	36
Excluding objects by names of the threats detected in them.....	36

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 protected area that are specified using Shell masks or ECMA-262 regular expressions.

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

Using regular expressions, you can specify the file path template excluded from the scan by Kaspersky Anti-Virus. 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 server, you can exclude it using the name of the detected or suspected threat. 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 ECMA-262 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 server accessed from remote computers 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 [169](#)) 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 \  
--set-settings 8 --file=<full path to the file>
```

```
--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**, **Deep** or **Recommended** 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

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.
- **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

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.
- **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:*

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

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

- **On-demand scan.** Scans all local objects on the server with the recommended security settings and all the shared objects, regardless of 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 [48](#)) 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	45
Quick scan of files and directories.....	48
Creating a scan area.....	50
Restricting a scan area using masks and regular expressions.....	51
Excluding objects from the scan area	51
Using heuristic analysis.....	53
Selecting actions to perform on detected objects.....	54
Selecting actions depending on the threat type.....	55
Scan optimization.....	56
Selecting task priority	57

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 Kaspersky 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="Recommended"

[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="Recommended"
[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="Recommended"

[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 default scan using the --scan-file command:

```
ScanPriority="System"
```

```

[ScanScope]
UseScanArea=yes
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=yes
HeuristicLevel="Recommended"

```

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 51).

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 ECMA-262 regular expressions.

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

Using 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	51
Excluding objects from the scan area	52
Excluding objects by names of the threats detected in them.....	53

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 this case, Kaspersky Anti-Virus will not scan files or directories from the scan area that are specified using Shell masks or ECMA-262 regular expressions.

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

Using regular expressions, you can specify the file path template excluded from the scan by Kaspersky Anti-Virus. 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.
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 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 server, you can exclude it using the name of the detected or suspected threat. 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 ECMA-262 regular expressions.

➤ *To exclude objects by the name of detected threat, 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 **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 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**, **Deep** or **Recommended** 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.
- **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.
- **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 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 **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 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 **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. 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 **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.

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 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 [115](#)).

IN THIS SECTION

Viewing statistics of quarantined objects.....	58
Scanning quarantined objects.....	59
Placing files to quarantine manually.....	60
Viewing object IDs.....	60
Restoring objects.....	61
Deleting objects.....	62

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 [86](#)), 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 Kaspersky 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 115) 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')"
```

The following example displays the command output:

Example:

```
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')"
```

The following example displays the command output:

Example:

```
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.

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 [115](#)) 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 [172](#)) or **Exclude objects by threat name** (see page [172](#)) 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 [110](#)).

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 [63](#)).

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 [63](#)). 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 [64](#)) 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 [63](#)), as well as your right to use the application and additional services (see page [63](#)).

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 [64](#)): 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 Kaspersky 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 Kaspersky 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 information about the license, 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 64).
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 63).

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 [118](#)). 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 are 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 [59](#)).

IN THIS SECTION

Using the internal mailer of Kaspersky Anti-Virus	68
Using Sendmail	69
Generation of notifications.....	69
Configuring actions	70
Using macros	70

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 [152](#)).

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 [152](#)).

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 [70](#)).

➤ 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 [SmtplibNotifies] 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 [70](#)).

➤ 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%	Danger level	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 [87](#));
- reports on the activity of Kaspersky Anti-Virus components (see page [86](#)).

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.

Kaspersky Anti-Virus 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 Net-SNMP package, update Kaspersky Anti-Virus to latest version.

IN THIS SECTION

Configuring interaction via SNMP	73
Structure of the Kaspersky Anti-Virus MIB	74
Description of Kaspersky Anti-Virus MIB objects	76

CONFIGURING INTERACTION VIA SNMP

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

1. Specify the address of server, on which SNMP manager is running, by using 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** setting.

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

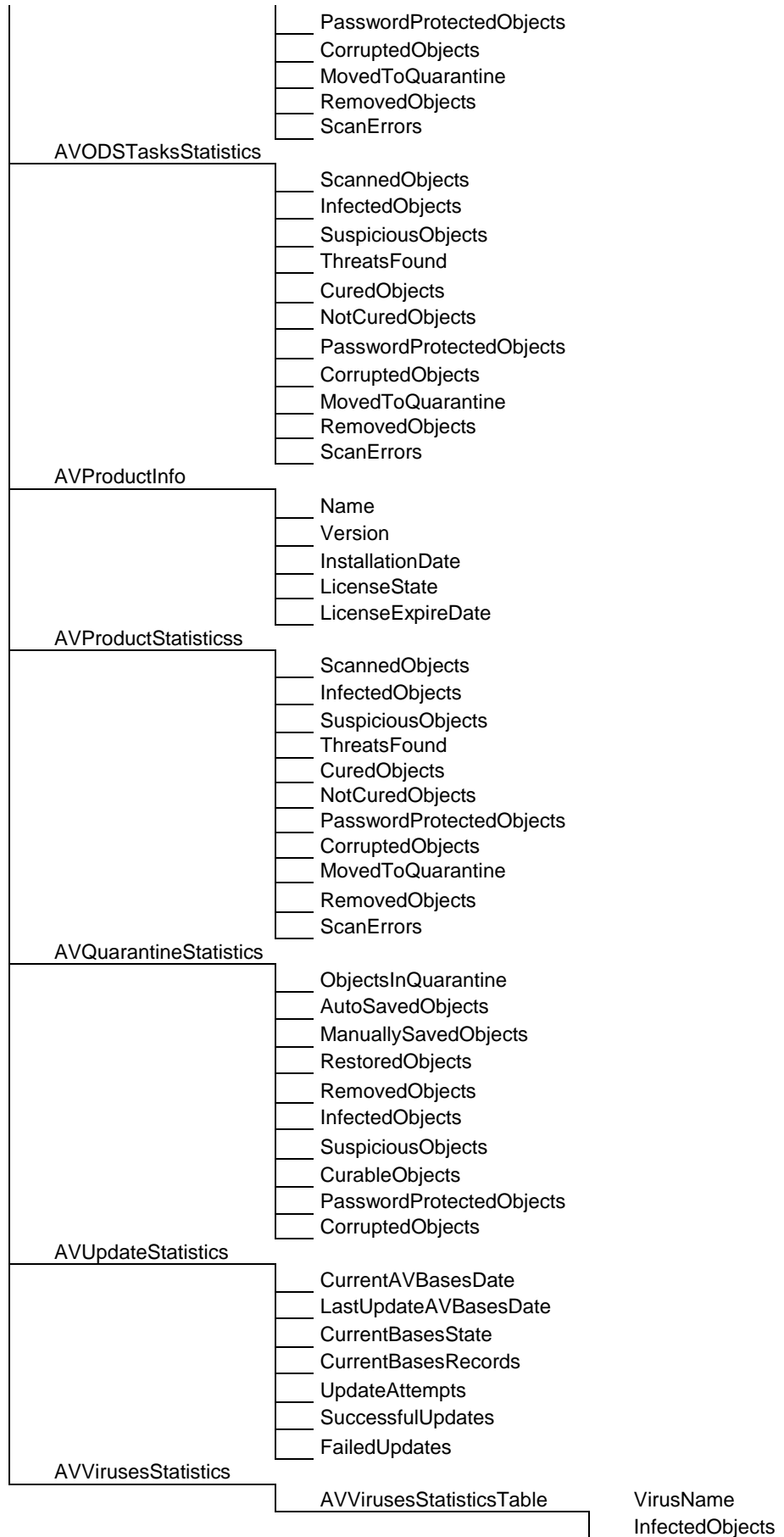
Statistics

AVBackupStatistics

- ObjectsInBackup
- RestoredObjects
- RemovedObjects
- InfectedObjects
- SuspiciousObjects

AVOASTasksStatistics

- ScannedObjects
- InfectedObjects
- SuspiciousObjects
- ThreatsFound
- CuredObjects
- NotCuredObjects



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.
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	The number of malicious programs found.
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	The number of malicious programs found.
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	The number of malicious programs found.
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 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 82)	Displays Kaspersky Anti-Virus command help.
Kaspersky Anti-Virus management commands	
--start-app (see page 83)	Starts Kaspersky Anti-Virus.
--restart-app (see page 83)	Restarts Kaspersky Anti-Virus.
--stop-app (see page 83)	Stops Kaspersky Anti-Virus.
--scan-file (see page 84)	Scans files or directories.
-R (see page 85)	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 85)	Outputs information about Kaspersky Anti-Virus.
-S --get-stat (see page 86)	Creates reports about the operation of Kaspersky Anti-Virus and its components.
-S --top-viruses (see page 87)	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 84)	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 89)	Outputs general Kaspersky Anti-Virus settings.
-T --set-app-settings (see page 90)	Defines general Kaspersky Anti-Virus settings.
-T --get-task-list	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 93)	Starts the task.
-T --stop-task (see page 93)	Stops the task.
-T --suspend-task (see page 94)	Pauses the task.

COMMANDS	DESCRIPTION
-T --resume-task (see page 94)	Resumes the task.
-T --get-settings (see page 95)	Outputs task settings.
-T --set-settings (see page 96)	Defines task settings.
-T --create-task (see page 97)	Creates a task of specified type; imports task settings from the specified configuration file.
-T --delete-task (see page 97)	Deletes the task.
-T --set-schedule (see page 98)	Sets task scheduling settings or imports them from a configuration file.
-T --get-schedule (see page 99)	Outputs task scheduling settings.
-T --del-schedule (see page 100)	Sets task scheduling settings, specified by default.
-T --show-schedule (see page 100)	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 102)	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 (see section "Viewing information about a license prior to the key file installation" on page 103)	Outputs information about the license from the key file without installing the license.
-L --get-installed-keys (see page 103)	Outputs information about installed licenses.
-L --query-status (see page 102)	Outputs the status of installed licenses.
-L --install-active-key (see page 104)	Installs an active license.
-L --install-suppl-key (see page 105)	Installs a supplementary license.
-L --revoke-active-key (see page 105)	Deletes an active license.
-L --revoke-suppl-key (see page 105)	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 106)	Outputs brief storage statistics.
-Q --query (see page 106)	Displays information about storages objects.
-Q --get-one (see page 107)	Displays information about one object in the storage.
-Q --restore (see page 107)	Restores an object from the storage.
-Q --add-object (see page 108)	Places a copy of the object to quarantine.
-Q --remove (see page 108)	Deletes the object from storage.
-Q --export (see page 109)	Exports objects from storage into a specified directory.
-Q --import (see page 109)	Imports objects into the storage from a specified directory, into which they were previously exported.
-Q --mass-remove (see page 110)	Removes some or all objects from the storage.
Logs management commands	

COMMANDS	DESCRIPTION
-E	This prefix indicates that the command is one of a group of commands for managing logs (optional).
-E --count (see page 111)	Outputs the number of events matching the filter defined in the event log or specified rotation file.
-E --query (see page 111)	Outputs information about events matching the filter defined in the event log or specified rotation file.
-E --period (see page 112)	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 113)	Rotates the event log.
-E --remove (see page 113)	Removes events from the log or the specified rotation file.

IN THIS SECTION

Displaying Kaspersky Anti-Virus command help [82](#)

Starting Kaspersky Anti-Virus..... [83](#)

Stopping Kaspersky Anti-Virus..... [83](#)

Restarting Kaspersky Anti-Virus..... [83](#)

Enabling events output..... [84](#)

Quick scan of files and directories..... [84](#)

Rollback of Kaspersky Anti-Virus databases..... [85](#)

Commands for obtaining reports and statistics [85](#)

Commands for managing the Anti-Virus settings and tasks..... [89](#)

Licenses management commands..... [102](#)

Quarantine and backup storage management commands..... [106](#)

Logs management commands..... [111](#)

Limiting selections using filters..... [114](#)

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 Kaspersky Anti-Virus events, or together with the `--start-task` command (start task (see section "Starting the task" on page 93)), 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>]
```

Examples:

- *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
<code>--file <file name></code>	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
<code>--scan-file <path to file or directory></code>	Names of files and directories that will be quickly scanned by Kaspersky Anti-Virus.
<code>--action <action></code>	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. To do this, use the roll back to the previous databases task.

Task start syntax

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

COMMANDS FOR OBTAINING REPORTS AND STATISTICS

IN THIS SECTION

Viewing application information	85
Viewing Anti-Virus activity reports	86
Viewing reports on the most commonly encountered threats.....	87

VIEWING APPLICATION INFORMATION

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

Command syntax

```
kav4fs-control [-S] --app-info [--export-report=<file name>] \
[--report-type=<report file format>]
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
--export-report=<report filename>	Optional key. The file name in which the obtained information 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. You can save the 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.
--report-type=<report file format>	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.

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 filename>] [--report-type=<report file format>] [--use-name]
```

Examples:

➤ *View statistics of the Kaspersky Anti-Virus operation:*

```
/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>	Specify the Anti-Virus component that you want to obtain statistics for. Possible values include: Application – an application; OAS – real-time protection; ODS – on-demand scan; Quarantine – quarantine; Backup – backup storage; Update – update.
--from=<start date>	The report starting date. You can assign the following values: <ul style="list-style-type: none"> • a 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; <div style="border: 1px dashed gray; padding: 5px; margin: 10px 0;"> <p style="color: red; text-align: center;">When specifying the date and time should enclose all the expression in quotation marks, and between the date and time to put a space.</p> </div> <ul style="list-style-type: none"> • a time, formatted as HH:MM:SS, to obtain information starting at the specified time of the current day.

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
	If you do not specify the --from=<start date> argument, the report will collect information from the time the Anti-Virus was installed.
--to=<end date>	<p>The report ending date. You can assign the following values:</p> <ul style="list-style-type: none"> a 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 before the specified time on the specified date; <p style="border: 1px dashed gray; padding: 5px; text-align: center; color: red;">When specifying the date and time should enclose all the expression in quotation marks, and between the date and time to put a space.</p> <ul style="list-style-type: none"> a 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 -N	Task name.

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>]
```

Examples:

- ➡ 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>	<p>The report starting date. You can assign the following values:</p> <ul style="list-style-type: none"> • a 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; <p style="text-align: center; border: 1px dashed gray; padding: 5px; color: red;">When specifying the date and time should enclose all the expression in quotation marks, and between the date and time to put a space.</p> <ul style="list-style-type: none"> • a 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"> • a 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 before the specified time on the specified date; <p style="text-align: center; border: 1px dashed gray; padding: 5px; color: red;">When specifying the date and time should enclose all the expression in quotation marks, and between the date and time to put a space.</p> <ul style="list-style-type: none"> • a 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>
--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 report 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>

COMMANDS FOR MANAGING THE ANTI-VIRUS SETTINGS AND TASKS

IN THIS SECTION

Viewing general settings of Kaspersky Anti-Virus	89
Editing the general settings of Kaspersky Anti-Virus	90
Viewing the list of Kaspersky Anti-Virus tasks	91
Viewing task state	92
Starting the task	93
Stopping the task	93
Pausing the task	94
Resuming the task	94
Obtaining task settings	95
Modifying task settings	96
Creating a task	97
Deleting tasks	97
Obtaining task schedule settings	98
Modifying task schedule settings	99
Deleting the task schedule	100
Searching for scheduled events	100

VIEWING GENERAL SETTINGS OF KASPERSKY ANTI-VIRUS

The `--get-app-settings` command outputs general settings of Kaspersky Anti-Virus (see page [148](#)). 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 [90](#)). 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>]
```

Examples:

➤ *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
--file=<configuration file name> -F <configuration file name>	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. 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.

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 [148](#)).

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 [89](#)).
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>
```

Examples:

➤ *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 will 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: <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	Task status. Available values: <ul style="list-style-type: none"> Stopped – the task is stopped; Stopping – the task is stopping;

	<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> [--use-name]
```

Command example

➔ To 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 <code>kav4fs-control --get-task-list</code> command (see page 91).
--use-name -N	Task name.

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 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: <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);

FIELD	DESCRIPTION
	<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>Complete – the task is completed successfully;</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>Resuming – the task is resuming;</p> <p>Failed – the task has terminated with an error;</p> <p>Interrupted by user – the task execution was interrupted by the user.</p>

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 84), in this case information about events occurring during task execution is displayed.

Command syntax

```
kav4fs-control --start-task <task ID> --[progress] [--use-name]
```

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 91).
--progress	Displays task progress.
--use-name	Task name.
-N	

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]
```

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 91).
--use-name	Task name.
-N	

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]
```

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 91).
--use-name	Task name.
-N	

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 [94](#)).

Command syntax

```
kav4fs-control [-T] --resume-task <task ID> [--use-name]
```

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 91).
--use-name -N	Task name.

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 [96](#)) 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>] -- [--use-name] [--use-name]  
kav4fs-control [-T] --get-settings <task ID> \  
<INI file section name>.<setting value> [--use-name]
```

Examples:

- 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 91).
--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 will 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 -N	Task name.

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]
```

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 91).
--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.

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
--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 the key if the extension of the specified file does not match its format. Possible values: XML, INI.
--use-name -N	Task name.

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>]
```

Example:

- 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>	Optional key. 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 will 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]
```

Example:

➔ *Delete the task with ID=20:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --delete-task 20
```

ARGUMENT	DESCRIPTION AND POSSIBLE VALUES
--delete-task <task ID> -D <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 91).
--use-name -N	Task name.

OBTAINING TASK SCHEDULE SETTINGS

The --get-schedule command outputs the task schedule settings (see page [145](#)). 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 Kaspersky Anti-Virus using the --set-schedule (see section "Modifying task schedule settings" on page [99](#)). Kaspersky Anti-Virus will apply the new schedule settings immediately.

Command syntax

```
kav4fs-control [-T] --get-schedule <task ID> \  
[--file=<configuration file name>] -- [--use-name] [--use-name]  
kav4fs-control [-T] --get-schedule <task ID> <parameter name> [--use-name]
```

Examples:

➔ *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 RuleType setting value in the real-time protection task schedule:*

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --get-schedule 9 RuleType
```

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 -N	Task name.

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 [145](#)).

You can use this command to modify the Anti-Virus settings:

1. Save the schedule settings to a configuration file using the -T --get-schedule (see section "Obtaining task schedule settings" on page [98](#)).
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]
```

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 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 -N	Task name.

DELETING THE TASK SCHEDULE

The -T --del-schedule command sets task scheduling settings, specified by default during the initial configuration of Kaspersky Anti-Virus (see Guide of Kaspersky Anti-Virus 8 for Linux).

Command syntax

```
kav4fs-control -T --del-schedule <task ID> [--use-name]
```

Example:

➤ Set scheduling settings for task with ID=15, specified by default:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control -T --del-schedule 15
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
<task ID>	Identification number of a Kaspersky Anti-Virus task.
--use-name -N	Task name.

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=<end date> --task-id=<task ID> [--use-name]
```

Command examples

The following example displays the command to search for events in the specified time interval and the command output.

Example:

➤ Find events which are scheduled for precise time of the first start within the range from 3/28/11 to 4/1/11:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \  
--show-schedule Time --from=2011-03-28 --to=2011-04-01
```

The command output:

Events number: 2

```
TaskId #9, Event: Start, Date: 2011-04-05 02:00 PM:00, Start Rule: [Daily, 02:00 PM:00;;
1] TaskId #16, Event: Start, Date: 2011-04-06 12:00 AM:00, Start Rule: [Once, 2011-04-06
12:00 AM:00]
```

The following example displays the output of the command to search for events and the command output.

Example:

➤ Search the following scheduled events for the specified task:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control \
--show-schedule Time --task-id="On-demand scan" --use-name
```

The command output:

Events number: 1

```
TaskId #9, Event: Start, Date: 2011-04-25 04:30 PM:00, Start Rule: [Monthly, 04:30 PM:00;
25]
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
<rule type>	<p>Schedule rule type.</p> <p>Available values:</p> <ul style="list-style-type: none"> • Time – rules containing the time for the task start. • StartUp – rules containing a PS condition (at Kaspersky Anti-Virus start). • BasereLoad – rules containing a BR condition (upon database 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; <p style="border: 1px dashed gray; padding: 5px; text-align: center;">When specifying the date and time should enclose all the expression in quotation marks, and between the date and time to put a space.</p> <ul style="list-style-type: none"> • a time, formatted as HH:MM:SS, to obtain information starting at 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>
--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 before the specified time on the specified date; <p style="border: 1px dashed gray; padding: 5px; text-align: center;">When specifying the date and time should enclose all the expression in quotation marks, and between the date and time to put a space.</p> <ul style="list-style-type: none"> • time, formatted as HH:MM:SS, to obtain information up to the specified time of the current day.

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
	If you skip the option --to=<end date>, search will cover a week period since the command execution.
--task-id=<task ID>	Identification number of the task, for which schedule search is performed.
--use-name -N	Task name.

LICENSES MANAGEMENT COMMANDS

IN THIS SECTION

Validating a key file prior to installation	102
Viewing information about a license prior to the key file installation.....	103
Viewing information about the installed key files	103
Viewing the status of installed licenses	104
Active key file installation	104
Supplementary key file installation	105
Active key file removal.....	105
Supplementary key file removal	105

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>
```

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>
```

Example:

➔ Output license information from the `/home/test/00000001.key` file:

```
/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
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.
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 [63](#)).

Command syntax

```
kav4fs-control [-L] --install-active-key <path to key file>
```

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 [63](#)).

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>
```

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.....	106
Obtaining information about storage objects.....	106
Obtaining information about one object in the storage.....	107
Restoring objects from the storage.....	107
Placing an object in quarantine manually.....	108
Deleting one object from the storage.....	108
Exporting objects from the storage into a specified directory.....	109
Importing previously exported objects into the storage.....	109
Clearing the storage.....	110

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>"]
```

Examples:

➤ *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]
```

Examples:

- To displays information about storages 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 displays information about objects from the backup storage:

```
/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 114).
--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]
```

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 -Q --query command (see page 106).
--detailed	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>]
```

Examples:

- 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 106).
<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>
```

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>
```

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 <code>-Q --query</code> command (see page 106).

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 [150](#)).

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>]
```

Examples:

- ◆ 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 114).
--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 [150](#)).

Command syntax

```
kav4fs-control [-Q] --import <directory containing exported objects>
```

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>]
```

Examples:

- *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
<code>--query="<logical expression>"</code>	Creates a filter consisting of a logical expression (see page 114).
<code>--limit=<maximum number of records></code>	Sets a filter: maximum number of records from query, which should be displayed.
<code>--offset=<offset from the query beginning></code>	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 [111](#)
- Obtaining information about Kaspersky Anti-Virus events..... [111](#)
- Viewing the time interval, during which the events will occur that are registered in the log..... [112](#)
- Event log rotation [113](#)
- Removing objects from the event log [113](#)

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 [111](#)).

Command syntax

```
kav4fs-control [-E] --count "<logical expression>" [--db=<rotation file>]
```

Examples:

➤ To obtain the number of Kaspersky Anti-Virus events stored in the event log:

```
/opt/kaspersky/kav4fs/bin/kav4fs-control --count ""
```

➤ To obtain the number of Kaspersky 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 114).
--db=<rotation file>	The rotation file, information in which you wish to view (this file has the extension <code>.db</code>). If you do not provide this modifier, Kaspersky 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 Kaspersky 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>]
```

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 114).
--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, Kaspersky 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 --file-format 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 -F key will 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>]
```

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, Kaspersky 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 [151](#)).

If the RotateMethod setting has the Erase value, Kaspersky 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 Kaspersky 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>]
```

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 114).
--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, Kaspersky Anti-Virus will delete records from Kaspersky Anti-Virus event log.

LIMITING SELECTIONS USING FILTERS

IN THIS SECTION

Logical expressions.....	114
Object parameters in quarantine / backup storage.....	115
Anti-Virus events and their data	118

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 Kaspersky Anti-Virus events: `-E --count "<logical expression>"` (see page [111](#));
- obtaining information about Kaspersky Anti-Virus events: `-E --query "<logical expression>"` (see page [111](#));
- obtaining information about objects in quarantine or in the backup storage: `-Q --query "<logical expression>"` (see page [106](#));
- obtaining concise statistical information about objects in quarantine or in the backup storage: `-Q --get-stat --query "<logical expression>"` (see page [106](#));
- selective removal of objects from the storage: `-Q --mass-remove --query "<logical expression>"` (see page [110](#));
- selective export of objects from quarantine or from the backup storage: `-Q --export --query "<logical expression>"` (see page [109](#)).

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')"
```

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 115). 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.
OrigType Type	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: 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.

FIELD	TYPE	DESCRIPTION AND POSSIBLE VALUES
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 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	<p>OrigThreatName – the name of the threat, based on the Kaspersky Lab classification, found in the object when the object is placed in the storage.</p> <p>ThreatName – the name of the threat detected in a quarantined object after scanning with updated databases.</p> <p>You can use masks with the aid of the 'like' comparison operator.</p>
Compound	i	<p>Indicates, whether the object is a compound object.</p> <p>Possible values include:</p> <ul style="list-style-type: none"> 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.

FIELD	TYPE	DESCRIPTION AND POSSIBLE VALUES
GID	i	The ID (GID) of the group to which the user who created the object belongs.
Mode	i	Access permissions.
AddTime	s	<p>The date and time the object was placed in the storage, formatted as "YYYY-MM-DD HH:MM:SS".</p> <p>If you specify the date but not the time, the time will be specified as 00:00:00.</p> <p>If you specify the time but not the date, the current date will be specified.</p> <p>If you specify the date and time as follows: (AddTime== s"), then the current date and time will be specified.</p>
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
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, 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,

#	EVENT NAME	DESCRIPTION	SETTINGS
			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
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, PersistentTaskId, 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,

#	EVENT NAME	DESCRIPTION	SETTINGS
			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, 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, ObjectActionsCompletedReason, ObjectSource, 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

#	EVENT NAME	DESCRIPTION	SETTINGS
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, 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 Kaspersky 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,

#	EVENT NAME	DESCRIPTION	SETTINGS
			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.
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.

SETTING	TYPE	DESCRIPTION
Error.	s	Type of error. Possible values include: IncorrectUser – non existent user given in the task settings, his/her name is found in the Info field; IncorrectGroup – non existent group given in the task settings, group name is found in the Info field; IncorrectPath – incorrect scan path given in task settings, path is found in the Info field; InterceptorNotFound – on launch of the task, the interceptor module cannot be loaded.
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.
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.

SETTING	TYPE	DESCRIPTION
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.
Path	s	Path to file where events have been moved.
QuarantineId	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.
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);

SETTING	TYPE	DESCRIPTION
		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	<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.

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.....	126
Real-time protection and on-demand scan tasks settings.....	127
Update tasks settings.....	141
Schedule settings.....	145
General settings of Kaspersky Anti-Virus.....	148
Quarantine and backup storage settings.....	150
Event log settings.....	151
Settings of notifications and event-based actions.....	152

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).

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.

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; expressions containing date and time, formatted as “YYYY-MM-DD HH:MM:SS”).

Example:

```
AreaDesc="Scan mail databases"
```

Other values can be entered either with or without quotes.

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.

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 [96](#)) from the configuration file, the comments are ignored. While viewing task settings (see section "Obtaining task settings" on page [95](#)), 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 [95](#)) 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 [96](#)).

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 default settings.

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:ScanSettings:AdvancedActions]

additional 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

...

[ScanScope:ScanSettings:AdvancedActions]

additional 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 [126](#)).

Table 19. Real-time protection and on-demand scan tasks settings

SETTING	DESCRIPTION AND POSSIBLE VALUES
ScanPriority	<p>Task priority.</p> <p>This setting is used only in the on-demand scan tasks and is not used in the real-time protection tasks.</p> <p>You can set one of the predefined task priorities in accordance with process priorities in Linux.</p> <p>Possible values include:</p> <ul style="list-style-type: none"> System (system). Priority of the process running a task is defined by the operating system. High (high). Priority of the process running a task is increased. Medium (medium). Priority of the process running a task remains unchanged. Low (low). Priority of the process running a task is decreased. <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>Kaspersky Anti-Virus includes two components intercepting attempts to access files and scanning those files. They are Samba interceptor (used to scan objects on server accessed from remote computers via the SMB / CIFS protocol) and the kernel level interceptor (scanning objects accessed using other methods).</p> <p>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.</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> <ul style="list-style-type: none"> 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). SambaOnly. Kaspersky Anti-Virus scans objects with the SAMBA interceptor only

SETTING	DESCRIPTION AND POSSIBLE VALUES
	<p>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 Installation Guide of Kaspersky Anti-Virus 8 for Linux).</p> <p>KernelOnly. Kaspersky Anti-Virus scans server objects only using the file interceptor.</p> <p>Make sure that you have specified the kernel interceptor during the initial configuration of Kaspersky Anti-Virus (see Installation Guide of Kaspersky Anti-Virus 8 for Linux).</p> <p>Default value: the operation shall be selected during Kaspersky Anti-Virus installation.</p>
<p>[ScanScope]</p> <p>Scan area.</p>	
<p>AreaDesc</p>	<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 objects.</p>
<p>AreaMask</p>	<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 ECMA-262 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>
<p>UseAccessUser</p>	<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> <ul style="list-style-type: none"> 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; no – scan objects when they are accessed with any permissions. <p>Default value: no.</p>
<p>[ScanScope:AreaPath]</p> <p>Scan scope, path to the directory to scan. You must specify at least one scan area to start the real-time protection task.</p>	

SETTING	DESCRIPTION AND POSSIBLE VALUES
Path	<p>The setting value consists of three elements: <file system type>:<access protocol>:<path to the directory being scanned>, where: <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> <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.</p> <p>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</p>	

SETTING	DESCRIPTION AND POSSIBLE VALUES
<p>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>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.</p>	
UserName	<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>
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>

SETTING	DESCRIPTION AND POSSIBLE VALUES
	<p>no – do no 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>
ScanPlainMail	<p>Kaspersky Anti-Virus scans the files of plain text email messages.</p> <p>yes – scan plain text email messages;</p> <p>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;</p> <p>no – do not scan packed files.</p> <p>Default value: yes.</p>
InfectedFirstAction	<p>First action to be performed on infected objects.</p> <hr/> <p>In real-time protection tasks, before performing the action specified by you on an infected object, Kaspersky Anti-Virus blocks access to the object by applications that attempt to do so.</p> <hr/> <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. Kaspersky Anti-Virus moves the object to quarantine.</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>

SETTING	DESCRIPTION AND POSSIBLE VALUES
	<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> <hr/> <p>In real-time protection tasks, before performing the action specified by you on an object, Anti-Virus moves the object to Quarantine blocks access to the object by applications that attempt to do so.</p> <hr/> <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 disinfected, Kaspersky Anti-Virus will leave the object unchanged.</p> <p>Quarantine. Kaspersky Anti-Virus moves the object to quarantine.</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 disinfected.</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</p>

SETTING	DESCRIPTION AND POSSIBLE VALUES
	<p>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> <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 ECMA-262 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>

SETTING	DESCRIPTION AND POSSIBLE VALUES
<p>ExcludeThreats</p>	<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> <p>You can use shell masks and extended ECMA-262 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>
<p>UseAdvancedActions</p>	<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>
<p>ReportCleanObjects</p>	<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 Kaspersky 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>

SETTING	DESCRIPTION AND POSSIBLE VALUES
	<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 Kaspersky 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 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>Recommended – recommended value.</p> <p>Default value: Recommended.</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>	

SETTING	DESCRIPTION AND POSSIBLE VALUES
Verdict FirstAction SecondAction	<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> <ul style="list-style-type: none"> Virware – viruses and worms; Trojware – Trojans; Malware – other malicious software; Pornware – pornographic software; Adware – advertising software; Riskware – potentially dangerous software. <p>For more information on the types of threats, refer to the section "Programs detectable by Kaspersky Anti-Virus" (on page 11).</p> <p>Example:</p> <pre> UseAdvancedActions=yes [ScanScope:ScanSettings:AdvancedActions] Verdict=Adware FirstAction=Cure SecondAction=Skip [ScanScope:ScanSettings:AdvancedActions] Verdict=Pornware FirstAction=Cure SecondAction=Skip </pre> <p>Default value: not configured.</p>
[ExcludedFromScanScope] Exclusion area.	
AreaDesc	<p>Description of the exclusion area, containing additional information about the exclusion area.</p> <p>Example:</p> <pre> AreaDesc="Exclude separate SAMBA" </pre> <p>Default value: not configured.</p>
AreaMask	<p>You can use this setting to limit the exclusion area specified in the [ExcludedFromScanScope:AreaPath] section.</p> <p>Kaspersky Anti-Virus will only exclude those objects that you specify using Shell masks</p>

SETTING	DESCRIPTION AND POSSIBLE VALUES
	<p>or ECMA-262 regular expressions. Use the re: prefix in regular expressions.</p> <p style="text-align: center;">AreaMask=re:.*\.tar\.gz</p> <p>Default value: not configured.</p>
UseAccessUser	<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>	
Path	<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> <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="text-align: center;">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>	

SETTING	DESCRIPTION AND POSSIBLE VALUES
UserName	<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> <pre>UserName=usr1</pre> <pre>UserName=usr2</pre> <p>Default value: not configured.</p>
UserGroup	<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> <pre>UserGroup=group1</pre> <pre>UserGroup=group2</pre> <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 [95](#)) 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 [96](#)).

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 [126](#)).

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 <code>RetranslationFolder</code> 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 <code>[RetranslateUpdatesSettings]</code> section. It will save the downloaded updates in the directory specified by the <code>RetranslationFolder</code> 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 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 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 Kaspersky Endpoint Security protection of computers in your organization.</p> <p>Custom. Kaspersky Anti-Virus will download updates from the user-defined source, specified in the <code>[CommonSettings:CustomSources]</code> 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 Kaspersky 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>

SETTING	DESCRIPTION AND POSSIBLE VALUES
	<p>no – do not use proxy server to connect to the Kaspersky Lab update servers. 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; no - do not use proxy server to connect to the user-defined update servers. Default value: no.</p>
ProxyPort	<p>Proxy server settings: port. Default value: 3128.</p>
ProxyServer	<p>Proxy server settings: network name or IP address. Default value: not configured.</p>
ProxyBypassLocalAddresses	<p>Using a proxy server when connecting to local update servers. By default, the proxy server is not used for connections to local update servers. Disable this option to implement a connection to a local update servers via a proxy server specified in the <code>ProxyServer</code> parameter.</p> <p>yes – not use proxy server to connect to local update servers; no – use proxy server to connect to local update servers. Default value: yes.</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 <code>ProxyAuthUser</code> and <code>ProxyAuthPassword</code> settings. 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. Default value: not configured.</p>
ProxyAuthPassword	<p>If you enable authentication, specify the password of the user whose rights will be used by Anti-Virus for proxy server access. 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; no – use active FTP server mode. Default value: yes.</p>

SETTING	DESCRIPTION AND POSSIBLE VALUES
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 Kaspersky 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. <p>Default value: DownloadAndApply.</p>
<p>[RetranslateUpdatesSettings]</p> <p>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.</p>	
RetranslationFolder	<p>Specify the directory into which the Anti-Virus will save the downloaded updates.</p> <p>Default value: not configured.</p>
RetranslationComponents	<p>Specify the name of the update you would like to receive if you specified RetranslateComponentsList as your UpdateType setting.</p> <p>You can review the names of update on the Kaspersky Lab Technical Support web site.</p> <p>Example:</p>

SETTING	DESCRIPTION AND POSSIBLE VALUES
	<p>To copy updates for version 6.0.2.551 of Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition:</p> <p>RetranslationComponents=UPDATER</p> <p>RetranslationComponents=AVS</p> <p>RetranslationComponents=BLST</p> <p>RetranslationComponents=KAV6WSEE</p> <p>RetranslationComponents=RT</p> <p>RetranslationComponents=AK6</p> <p>RetranslationComponents=INDEX60</p> <p>Default value: not configured.</p>

SCHEDULE SETTINGS

This section describes configuration file settings that you can use to schedule the task start.

When specifying the settings, follow the rules for editing Kaspersky Anti-Virus INI configuration files (see page [126](#)).

Structure of the schedule INI configuration file

```
RuleType=Once|Monthly|Weekly|Daily|Hourly|Minutely|Manual|PS|BR
[StartTime=<date time>; <day of the month|day of the week>; <run period>]
[RandomInterval=<minutes>]
[ExecuteTimeLimit=<minutes>]
[RunMissedStartRules=yes|no]
```

Table 21. Schedule settings

SETTING	DESCRIPTION AND POSSIBLE VALUES
RuleType	<p>The Starting a scheduled task mode.</p> <p>Possible values include:</p> <ul style="list-style-type: none"> • Once – once; • Monthly – monthly; • Weekly – weekly; • Daily – every N day; • Hourly – every N hour; • Minutely – every N minutes; • Manual – manually; • BR – after databases update. The task will be started after each successful Kaspersky Anti-Virus database update (this alternative is not used in update tasks). • PS – at application start. The task will be launched at every Anti-Virus startup.

SETTING	DESCRIPTION AND POSSIBLE VALUES
	For the real-time protection task is only available values of the Manual and PS.
StartTime	Start time. If you specify a start time, by default, the current system date and / or time is set. The format of this parameter depends on the parameter RuleType, see the table below.
RandomInterval	Distribute a task to start at random in the interval (in minutes) to equalize the load on the server while running to schedule multiple tasks. Format – [0;999].
ExecuteTimeLimit	Limit the duration of the task interval (in minutes). Format – [0;999].
RunMissedStartRules	Run the missed tasks. Possible values include: <ul style="list-style-type: none"> • yes – run missed tasks the next time the application is started; • no – run only scheduled tasks.

Table 22. Parameters of the mode for task launch and start time

THE RULETYPE SETTING VALUE	THE STARTTIME SETTING VALUE FORMAT
Once	<date time>
Monthly	<time>; <day of month>
Weekly	<time>; <day of week>
Daily	<time>;;<start period>
Hourly	<date time>;;<start period>
Minutely	<time>;;<start period>
Manual	Not used
BR	Not used
PS	Not used

The <start time> setting has the following format.

[<year>/][<month>/][<day of month>] [hh]:[mm]:[ss]; [<day of month>|<day of week>]; [<start period>]

Table 23. Field values of the start time parameter

FIELD	THE STARTTIME SETTING VALUE
<year>	[present year -1present year +10]
<month>	JAN FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC
<day of the month>	[1;31]
hh	hour [00;23]
mm	minutes [00;59]
ss	seconds [00;59]
<day of the week>	MON TUE WED THU FRI SAT SUN
<start period>	[0-999], where 0 – start period is not set

Examples

The following example displays a task start in the "Once" mode.

Example:

Start the task March 30, 2011 at 10:00 am:

```
RuleType="Once"
StartTime="2011/Mar/30 10:00 AM:00"
```

The following example displays a task start in the "Monthly" mode.

Example:

Start the task every month 15th day at 12:00 am:

```
RuleType=Monthly
StartTime=12:00 AM:00; 15
```

The following example displays a task start in the "Weekly" mode.

Example:

Start task every week on Monday at 00:00:

```
RuleType=Weekly
StartTime=00:00:00; Mon
```

The following example displays a task start in the "Every N day" mode.

Example:

Start a task in a day at 12:30 am:

```
RuleType=Daily
StartTime=12:30 AM:00;; 2
```

The following example displays a task start in the "Every N hour" mode.

Example:

Start task every 3 hours, starting at the specified time:

```
RuleType=Hourly
StartTime=2011/Apr/01 12:00 AM:00;; 3
```

The following example displays a task start in the "Every N minutes" mode.

Example:

Start task every 10 minutes, starting at the specified time:

```
RuleType=Minutely
StartTime=02:30 PM:00;; 10
```

The following example displays a task start after databases update.

Example:

Start task after databases update:

```
RuleType=BR
```

The following example displays a task start at the program starts.

Example:

To start a task at Kaspersky Anti-Virus startup:

```
RuleType=PS
```

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 [126](#)).

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 24. 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

SETTING	DESCRIPTION AND POSSIBLE VALUES
	<p>account under which Kaspersky Anti-Virus runs.</p> <p>Default value: /var/run/kav4fs.</p>
TraceEnable	<p>Maintaining a trace log.</p> <p>Kaspersky Anti-Virus records all events into the trace log. Trace log files are stored in the directory specified by the TraceFolder setting.</p> <p>Possible values include:</p> <ul style="list-style-type: none"> yes – maintain a trace log; no – do not maintain a trace log. <p>Default value: yes.</p>
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 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 [126](#)).

Table 25. 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> <hr/> <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 <code>QuarantineSizeLimitReached</code> event will be logged, indicating that the maximum storage size has been reached.</p> <hr/> <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.</p> <hr/> <p>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 <code>QuarantineSoftSizeLimitExceeded</code> event will be logged, indicating that the recommended storage size has been reached.</p> <hr/> <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 [126](#)).

Table 26. 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 -E --query command (see page 111).</p> <p>You cannot modify this setting.</p> <p>Default value: <code>/var/opt/kaspersky/kav4fs/db/event_storage</code>.</p>
RotateMethod	<p>Kaspersky Anti-Virus rotates events partially deleting (moving) event information from the EventStorageFolder directory. The RotateMethod setting can take the following values:</p> <p>Erase. Kaspersky 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, Kaspersky 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 Kaspersky Anti-Virus saves information about events in a separate file.</p> <p>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, Kaspersky 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. Kaspersky Anti-Virus rotates events every day at 00:00.</p> <p>Weekly. Kaspersky Anti-Virus rotates events every Monday at 00:00.</p> <p>Monthly. Kaspersky 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</p>

SETTING	DESCRIPTION AND POSSIBLE VALUES
	<p>defined by the setting, Kaspersky 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> <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 [126](#)).

Table 27. Settings of notifications and event-based actions

SETTING	DESCRIPTION AND POSSIBLE VALUES
EnableSmtп	<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>
[CommonSmtпSettings]	
General notification settings	
Sender	<p>The 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> <p style="padding-left: 40px;">DefaultRecipients=admin1@example.com</p> <p style="padding-left: 40px;">DefaultRecipients=admin2@example.com</p> <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>

SETTING	DESCRIPTION AND POSSIBLE VALUES
	<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 [CommonSmtpSettings:InternalMailerSettings] section.</p> <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> <p>-t – mandatory argument (instruction to use the list of recipients from message);</p> <p>-i – optional argument (instruction to disable interpreting a single dot (.) in a line as a message end character).</p> <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 recipients list rule sets from what list the recipients will receive the message.</p> <p>Local. Message will be sent to recipients from the local list;</p> <p>Global. Message will be sent to recipients from the global list.</p> <p>Both. Messages will be sent to recipients from both lists;</p> <p>Default value: Global.</p>

SETTING	DESCRIPTION AND POSSIBLE VALUES
Subject	The message "Subject" field. If you skip the setting, the "Subject" field will contain the event. Default value: not configured.
Body	Message body. You can add macros (see section "Using macros" on page 70). 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 .
[Actions] Settings for event-based actions. Create a separate [Actions] section for each event, for which you wish to configure an action.	
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 Kaspersky 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 70). 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	155
The "Application Settings" dialog box.....	156
Creating and configuring tasks.....	156
Creating a task.....	156
The Local task creation wizard.....	157
Updating tasks settings	159
Scheduling a task via Kaspersky Administration Kit.....	163
Creating and configuring policies	165
Checking connection with Administration Server manually. The klnagchk utility.....	166
Connecting to Administration Server manually. The klmover utility.....	167
Tasks settings	168

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** 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 name> Properties** dialog box open the **Protection** tab.

The **Protection** tab displays the following information about the protected server:

Table 28. Information on server protection status in the 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, Stopped, Paused</i> .
Last full scan date	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, click 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**, perform the following steps:

1. In the Administration Console tree expand the **Managed computers** node.
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's 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 [157](#)). 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 task pane to start the New task wizard. Further information about creating group tasks is available in the Kaspersky Administration Kit Reference Guide.

➤ *To create a task for specific computers (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 task pane to start the New task wizard. Further information about creating Kaspersky Administration Kit tasks and tasks for specific computers is available in the Kaspersky Administration Kit Reference Guide.

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 Workstation 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 rollback – 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 [159](#)) and the scan settings (see page [160](#));
- specify any excluded areas (see page [160](#)).

The following settings are required for a task which updates the database and program modules:

- specify the source (see page [161](#)) 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 [162](#)).

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 this, do the following:*

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

Configure the task schedule settings (see section "Scheduling a task" on page [163](#)). 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, 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, 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 **SMB/CIFS** 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.

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 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.

- d. 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 [172](#)) 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 [173](#)) and the maximum size of objects to scan (see page [173](#)).
5. Select the **Actions** tab, and specify the operations to be performed on infected objects (see page [170](#)) and on suspicious objects (see page [171](#)).
6. In the **Exclusion area** section, specify objects to be excluded from scanning by name (see page [172](#)) and objects to be excluded from scanning by the name of the detected threat (see page [172](#)).

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 this case, Kaspersky Anti-Virus will not scan files or directories from the scan area that are specified using Shell masks or ECMA-262 regular expressions.

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

Using regular expressions, you can specify the file path template excluded from the scan by Kaspersky Anti-Virus. 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 **SMB/CIFS** 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

Updates source is a resource containing updates for Kaspersky Anti-Virus database. The update source can be an HTTP or FTP server, or a local or network folder.

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 [173](#)).
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, click 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 [174](#))
 - b. time to wait for a response from the update source while connected to it (see page [174](#))
 - c. proxy server usage (see page [174](#))
 - d. proxy server settings (see page [174](#))
 - e. authentication required to access proxy server (see page [174](#))
 - f. location of 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 [175](#)) 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 [175](#)) 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 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 in the task creation wizard 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.

IN THIS SECTION

Creating a task start rule	163
Configuring task schedule	163

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, 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 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. Configure the task schedule (see section "Scheduling a task" on page [163](#)).
7. Click **OK** to save the changes.

CONFIGURING TASK SCHEDULE

In the **Scheduled start** drop-down list, select the necessary mode for task launch:

- **Every N hours.**
- **Every N minutes.**
- **Every N day.**
- **Weekly.**
- **Monthly.**
- **Once.**

- **Manually** – launch will be performed manually from the main application window of Kaspersky Anti-Virus using the **Start** command from the context menu or the analogous point in the **Action** menu.
- **After application update** – launch will be performed after each databases update.
- **At application start.**
- **When new updates are downloaded to the repository** – launch will be performed automatically after the Administration Server obtains updates.
- **On virus outbreak.**
- **On completing another task.**

Here are all startup modes, used in the Kaspersky Administration Kit tasks. Depending on the type of selected task, some of specified options may be missing. General information about tasks in Kaspersky Administration Kit can be found in *Kaspersky Administration Kit. Administrator's Guide*.

After selecting the task start mode you should specify the frequency of its run in the fields block corresponding to the selected mode. Depending on the selected mode the following values are specified:

- For the **Every N hours** task start mode you must specify frequency in hours in the **Every** field, and in the **Plan for** – date and time of the first task start.

For example, if you specify the **2** value in the **Every** field, and in the **Plan for** field – **April 3, 2011 . 03:00 PM:00**, then the task will run every two hours starting at 03:00 PM April 3, 2011.

The default frequency is set to **6**, as well as the date and start time is automatically put down the current system date and time of your computer.

- For the **Every N minutes** task start mode you must specify frequency in minutes in the **Every** field, and in the **Plan for** – time of the first task start.

For example, if you specify the **30** value in the **Every** field, and in the **Plan for** field– **03:00 PM:00**, then the task will run every half hour from 03:00 PM of the day.

The default frequency is set to **30**, as well as start time is automatically put down the current system time of your computer.

- For the **Every N day** task start mode you must specify frequency in days in the **Every** field, and in the **Start time** – time when the task should run on the specified dates.

For example, if you specify the **2** value in the **Every** field, and in the **Start time** field– **03:00 PM:00**, the task will be run once in two days (every other day) in 03:00 PM.

The default frequency is set to **1**, as well as start time is automatically put down the current system time of your computer.

- For the **Weekly** task start mode you must specify day of week in the **Every** field, on which the task should be run, and in the **Start time** – time when the task should run on the specified day of week.

For example, if you specify the **Monday** value in the **Every** field, and in the **Start time** field– **03:00 PM:00**, the task will be run every Monday in 03:00 PM.

By default, the **Every** field is set to **Sunday**, as well as start time is automatically put down the current system time of your computer.

- For the **Weekly** task start mode you must specify day of week in the **Every** field, on which the task should be run, and in the **Start time** – time when the task should run on the specified day of month.

For example, if you specify the **20** value in the **Every** field, and in the **Start time** field– **03:00 PM:00**, the task will be run every month Monday the twentieth day in 03:00 PM.

By default, the **Every** field is set to **1**, and in the **Start time** field – the current system time of computer.

- For the **Once** task start mode you must specify day in the **Start day** field, on which the task should be run, and in the **Start time** field – task start time on the specified day.

The values of these fields are automatically put down and correspond to the current system date and time of your computer, but you can change them.

- For the **On virus outbreak** mode you must specify the types of programs, for which the *Virus attack* event should be taken into account at task start. To do this, check the boxes by the selected types of programs.
- If the task will start after the completion of another task, in the **Task name** field you must specify, what the task is to be completed, by clicking the **Select** button. In the **Execution result** field specify the mode to complete task.

You can also configure additional task start settings (they depend upon the selected scheduling mode):

- Define the procedure for the task startup if the client computer is unavailable (turned off, disconnected from the network, etc.) or if the application is not running at the time specified by the schedule.

If the **Run the missed tasks** box is checked, the system attempt to start the task the next time the application is started on this client computer. The task will be started immediately following the host's registering with the network if the task launch schedule is set to **Manually** and **Once**.

If this box is not checked, only scheduled tasks will be started on the client computers, and for **Manually**, **Once** – on hosts visible on the network only. By default, this box is unchecked.

- Define deviation from the scheduled time, during which the task will be run on client computers. This feature is provided in order to solve the problem of simultaneous access to a large number of client computers to the Administration Server at task start.



You must select the **Distribute a task to start at random in the interval (in minutes)** check box and specify time interval in minutes, during which Server is attempted to access that the client computers attempts not to simultaneous access Administration Server at task start. By default, this box is unchecked.

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 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 the real-time protection task settings for Kaspersky Anti-Virus.

IN THIS SECTION

Creating a policy	166
Configuring a policy.....	166

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 the administration group for whose computers you want to create the policies for.
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 " * < : > ? \ |).
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 you require.

6. Use the **Protection areas** window to add one or several protection areas and select the interception method (see page [169](#)).
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 the real-time protection task 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 *klmagchk* utility to check the connection with the Administration Server.

Following installation of the Network Agent, the utility is located in the `/opt/kaspersky/klmagent/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.

- `-noss1` – 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	169
Protection mode	169
Heuristic analysis	169
Action to perform on infected objects	170
Action to be performed on suspicious objects	171
Actions to be performed on objects depending on the threat type	171
Excluding objects by name.....	172
Excluding objects by threat name	172
Scan of compound files	172
Maximum object scan time.....	173
Maximum size of a scanned object	173
Updates source	173
FTP server mode	174
FTP or HTTP server response wait time	174
Using a proxy server to connect to update sources	174
Proxy server authentication.....	174
Proxy server settings.....	174
Directory for saving updates.....	175
Updates type	175

INTERCEPTION METHOD

The **Scan on file access type** security setting is used only in real-time protection task.

Kaspersky Anti-Virus includes two components intercepting attempts to access files and scanning those files. They are Samba interceptor (used to scan objects on server accessed from remote computers 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.

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 Installation Guide of Kaspersky Anti-Virus 8 for Linux).

- **File system only.** Kaspersky Anti-Virus scans server objects without using the SAMBA interceptor.

Make sure that you have specified the kernel interceptor during the initial configuration of Kaspersky Anti-Virus (see Installation Guide of Kaspersky Anti-Virus 8 for Linux).

PROTECTION MODE

The **Protection mode** security setting is used only in the 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;**
- **Recommended.**

Default value: **Recommended.**

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.

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, Kaspersky 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.
- **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. 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, Kaspersky 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 **Actions by 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 [170](#)) and the Action on suspicious object setting (see page [171](#)).

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 **Exclude objects by name or regular expression** 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 protected area that are specified using Shell masks or ECMA-262 regular expressions.

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

Using regular expressions, you can specify the file path template excluded from the scan by Kaspersky Anti-Virus. 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 **Exclude 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 server, you can exclude it using the name of the detected or suspected threat. 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 ECMA-262 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 ECMA-262 regular expressions. Regular ECMA-262 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 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 Kaspersky Endpoint Security 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 main 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/virlab/helpdesk.html?LANG=en>
(for queries to virus analysts)

INFORMATION ABOUT THIRD-PARTY CODE

The legal_notices.txt file contains the information about third-party code, located in the application setup folder.