Kaspersky Endpoint Security 8 for Linux

ADMINISTRATOR'S GUIDE

APPLICATION VERSION: 8.0

KASPERSKY lab

Dear User!

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

Attention! This document is the property of Kaspersky Lab ZAO (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.

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

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

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

Revision date: 5/13/11

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

CONTENTS

INTRODUCTION

Kaspersky Endpoint Security 8 for Linux (hereinafter *Kaspersky Endpoint Security* or *the application*) provides protection for workstations running under the Linux operating system against malware penetrating computers through file exchange.

Kaspersky Endpoint Security scans the computer disks and other mounted devices. It can scan individual directories accessible over SMB/CIFS and NFS as well as remote directories mounted on the workstation using the SMB/CIFS and NFS protocols.

IN THIS SECTION

GENERAL INFORMATION ABOUT KASPERSKY ENDPOINT SECURITY

Kaspersky Endpoint Security 8 for Linux (hereinafter *Kaspersky Endpoint Security* or the *application*) provides protection for workstations running under the Linux operating system 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 computer'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 Endpoint Security 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 Endpoint Security isolates objects that it considers 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 Endpoint Security 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.

- Generate statistics and reports about operational results.
- Update Kaspersky Endpoint Security 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.

  You can manage Kaspersky Endpoint Security:

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

REAL-TIME PROTECTION AND ON-DEMAND SCAN

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

Real-time protection

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

Kaspersky Endpoint Security scans files for multiple types of threats (see section "Programs detectable by Kaspersky Endpoint Security" on page 11). When any application accesses a file on the computer (for example, reads or writes it), Kaspersky Endpoint Security scans files when they are accessed and 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 Endpoint Security detects a malicious program in the file, it will perform the actions you have specified for it, for example, it may attempt to disinfect the file or simply delete it. The program attempting to access the file may only do so if this file is not infected or has been successfully disinfected.

On-demand scan

On-demand scan involves one-time complete or selective scan of files on the computer 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 Endpoint Security.

Scanning symbolic links

The real-time protection and on-demand scan tasks of Kaspersky Endpoint Security scan symbolic links only if the file to which the symbolic link refers is included within scan 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, computer security will be at risk!

Scanning hard links

When Kaspersky Endpoint Security processes a file with more than one hard link depending on actions to be taken with objects the following scenarios are available:

- 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 Endpoint Security 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 Endpoint Security 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 Endpoint Security 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 Endpoint Security assigns the *suspicious* status 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 Endpoint Security isolates found infected and suspicious objects to secure the protected computer from their potential harmful effect.

Moving objects to quarantine

Kaspersky Endpoint Security quarantines detected infected and suspicious objects by moving them from the original location to the quarantine or backup storage directory. Kaspersky Endpoint Security rescans quarantined objects after each update of Kaspersky Endpoint Security databases. Having scanned quarantined objects after databases update, Kaspersky Endpoint Security may acknowledge some of the objects to be not infected. Other objects can be found infected by Kaspersky Endpoint Security.

If you suspect that a certain file may contain a threat while Kaspersky Endpoint Security 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 Endpoint Security places in the quarantine / 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 Endpoint Security 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 computer. You may need to restore an object, for example, if the original infected file contained valuable data but Kaspersky Endpoint Security could not preserve its integrity during disinfection and the information inside became unavailable.

Restoring infected or suspicious objects may lead to computer infection.

PROGRAMS DETECTABLE BY KASPERSKY ENDPOINT SECURITY

Kaspersky Endpoint Security is capable of detecting hundreds of thousands of different programs that represent a threat to computer security, within the computer's file system. Some of those programs impose great menace to the user, others are only dangerous when specific conditions are met. After Kaspersky Endpoint Security 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 Endpoint Security distinguishes the following categories of malicious programs:

- 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). 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, specials 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 THE INFORMATION ABOUT KASPERSKY ENDPOINT SECURITY

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

If you already purchased Kaspersky Endpoint Security, 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 Endpoint Security are available:

- Kaspersky Endpoint Security page at the Kaspersky Lab website;
- documentation;
- manual pages.

Page at the Kaspersky Lab website

http://www.kaspersky.com/endpoint-security-linux

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

Documentation

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

Administrator Guide includes information on how to manage Kaspersky Endpoint Security using command line utility and Kaspersky Administration Kit.

These documents are supplied in PDF format in Kaspersky Endpoint Security distribution package. Alternatively, you can download the documentation files from the Kaspersky Endpoint Security page at Kaspersky Lab website.

Manual pages

The following manual page files contain information about specific aspects of Kaspersky Endpoint Security:

- manage Kaspersky Endpoint Security from the command line:

/opt/kaspersky/kes4lwks/share/man/man1/kes4lwks-control.1.gz;

- Configuring general Kaspersky Endpoint Security settings:

/opt/kaspersky/kes4lwks/share/man/man5/kes4lwks.conf.5.gz;

- configuring the real-time protection task:

/opt/kaspersky/kes4lwks/share/man/man5/kes4lwks-oas.conf.5.gz;

- configuring on-demand scan tasks:

/opt/kaspersky/kes4lwks/share/man/man5/kes4lwks-ods.conf.5.gz;

- configuring update tasks:

/opt/kaspersky/kes4lwks/share/man/man5/kes4lwks-update.conf.5.gz;

- configuring the storage of quarantined objects and the storage of objects backed up before disinfection or removal:

/opt/kaspersky/kes4lwks/share/man/man5/kes4lwks-quarantine.conf.5.gz;

- configuring the event repository:

/opt/kaspersky/kes4lwks/share/man/man5/kes4lwks-events.conf.5.gz;

- description of utility which changes settings for connection with the Kaspersky Administration Kit Administration Server:

/opt/kaspersky/klnagent/share/man/man1/klmover.1.gz;

- description of utility which checks settings for connection with the Kaspersky Administration Kit Administration Server:

/opt/kaspersky/klnagent/share/man/man1/klnagchk.1.gz.

CONTACTING THE TECHNICAL SUPPORT SERVICE

If you have already purchased Kaspersky Endpoint Security, you can obtain information about it from the Technical Support service by phone or via Internet.

Technical Support Service will answer your questions about installing and using the program. If your computer has been infected, they will help eliminate the consequences of malicious programs.

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

Email request to the Technical Support Service

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

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

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

If you are not yet a registered user of Kaspersky Lab applications, you can fill out a registration form (https://support.kaspersky.com/ru/personalcabinet/Registration/Form/?LANG=en). When registering, indicate the application *activation code* or *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". If you do not find an appropriate topic, select "General Question".
- **Application version name and number**.
- **Request text**. Describe the problem you have encountered providing as much detail as possible.
- **Customer ID and password**. Enter the customer ID and password received during registration at the Technical Support Service website.
- **Email address**. The experts of the Technical Support Service will send their reply to your inquiry to that address.

Technical support by phone

If an urgent problem has occurred, you can call the Technical Support Service in your city. Before contacting to the Russian-speaking (http://support.kaspersky.ru/support/support_local) specialists or international (http://support.kaspersky.com/support/international) technical support, please gather the information (http://support.kaspersky.com/support/details) on your computer and set it on antivirus software. This will allow our specialists to help you more quickly.

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.

STARTING AND STOPPING KASPERSKY ENDPOINT SECURITY

Before taking the actions or using the commands described above, make sure that the kes4lwks-supervisor service is running on the computer!

By default, Kaspersky Endpoint Security starts automatically at the operating system startup (on default run levels for each operating system). Kaspersky Endpoint Security runs all predefined and custom tasks, schedule settings (see section "Schedule settings" on page 127) which is set to run PS.

If you stop Kaspersky Endpoint Security, execution of all tasks will be interrupted. After Kaspersky Endpoint Security restart, interrupted custom tasks will not be resumed automatically. Only those custom tasks in the schedule settings (see section "Schedule settings" on page 127) which is set to launch PS, will be launched again.

➧ *To run the Kaspersky Endpoint Security, execute the following command:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --start-app
```

➧ To stop *Kaspersky Endpoint Security*, execute the following command:

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --stop-app
```

➧ *To restart the Kaspersky Endpoint Security, execute the following command:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --restart-app
```

MANAGING KASPERSKY ENDPOINT SECURITY TASKS

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

➨ *To obtain the lists of tasks of Kaspersky Endpoint Security, execute the following command:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --get-task-list
```

The user can manage the following types of tasks (see page 18):

- **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

The Kaspersky Endpoint Security installation creates one task of each type. You can create custom on-demand scan and update tasks (see section "Creating a task" on page 78).

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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 (see section "Default scan settings" on page 38).

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/kes4lwks/bin/kes4lwks-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) and **Custom Scan** (ID=15) tasks).

You cannot delete the real-time protection task.

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control --start-task <task ID>
```

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --stop-task <task ID>
```

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --suspend-task <task ID>
```

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --resume-task <task ID>
```

AUTOMATIC TASK MANAGEMENT

In addition to managing Kaspersky Endpoint Security 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 configure task schedule using the configuration file:

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

   ```
   /opt/kaspersky/kes4lwks/bin/kes4lwks-control --get-schedule <task ID> \
   --file=<full path to the file>
   ```

2. Configure the schedule settings (see page 127).
3. Import the schedule settings into the task:

   ```
   /opt/kaspersky/kes4lwks/bin/kes4lwks-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 Endpoint Security 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/kes4lwks/bin/kes4lwks-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 Endpoint Security tasks. Viewing statistics is available for the following task types:

- **Application** – general operating statistics for Kaspersky Endpoint Security;
- **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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \

--get-stat <task type> [--task-id <task ID>] --export-report=<full path to the file>
```

UPDATING KASPERSKY ENDPOINT SECURITY

During the license period you can download updates for the databases of Kaspersky Endpoint Security.

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 computer, we recommend that you receive database updates regularly.

Kaspersky Lab can also release update packages for Kaspersky Endpoint Security application modules. 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 the Kaspersky Endpoint Security has retrieved the current databases from an Kaspersky Lab's HTTP server; if you have configured automatic database update, Kaspersky Endpoint Security 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 Endpoint Security automatically switches to using databases with previously installed update. If Kaspersky Endpoint Security databases get corrupted, you can roll them back to the previously installed updates.

By default, if Anti-Virus databases have not been updated within a week since Kaspersky Lab had released previous database updates, Kaspersky Endpoint Security will log the *Databases are outdated* (AVBasesAreOutOfDate) event. 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

Update source (see page 154) is a resource containing updates for Kaspersky Endpoint Security 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
--set-settings <update task ID> \
CommonSettings.SourceType=AKServer
```

To reduce Internet traffic, you can configure Kaspersky Endpoint Security database update from the local or network folder (see page 22).

UPDATING FROM LOCAL OR NETWORK FOLDER

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

1. One of the computers on the network retrieves the Kaspersky Endpoint Security 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 Kaspersky Endpoint Security database updates.

➧ *To download updates for Kaspersky Endpoint Security databases to a shared folder on one of the network computers, perform the following steps:*

1. Create a folder, to which Kaspersky Endpoint Security 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/kes4lwks/bin/kes4lwks-control \
   --set-settings <update task ID> \
   --file=<full path to the file>
   ```

5. Start the task using the following command:

   ```
   /opt/kaspersky/kes4lwks/bin/kes4lwks-control --start-task <update task ID>
   ```

Kaspersky Endpoint Security databases will be downloaded to the shared folder.

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

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

   ```
   UpdateType="AllBases"
   [CommonSettings]
   SourceType="Custom"
   UseKLServersWhenUnavailable=yes
   UseProxyForKLServers=no
   UseProxyForCustomSources=no
   PreferredCountry=""
   ProxyServer=""
   ProxyPort=3128
   ProxyBypassLocalAddresses=yes
   ProxyAuthType="NotRequired"
   ProxyAuthUser=""
   ProxyAuthPassword=""
   UseFtpPassiveMode=yes
   ConnectionTimeout=10
   ```

```
[CommonSettings:CustomSources]
Url="/home/bases"
Enabled=yes
[UpdateComponentsSettings]
Action="DownloadAndApply"
```

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
--set-settings <update task ID> \
CommonSettings.ProxyAuthType=Plain \
CommonSettings.ProxyAuthUser=user \
CommonSettings.ProxyAuthPassword=password
```

LAST DATABASE UPDATE ROLLBACK

The Kaspersky Endpoint Security creates backup copies of the original databases before it applies updates. If an update procedure gets interrupted or fails, the Kaspersky Endpoint Security 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 Kaspersky Endpoint Security databases task.

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --start-task 14
```

REAL-TIME PROTECTION

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

You cannot create custom real-time protection tasks.

IN THIS SECTION

DEFAULT PROTECTION SETTINGS

In Kaspersky Endpoint Security for real-time protection task the following default settings are configured.

```
ProtectionType="Full"
TotalScanners=4
[ScanScope]
UseScanArea=yes
AreaMask="*"
UseAccessUser=no
AreaDesc="All objects"
[ScanScope:AreaPath]
Path="/"
[ScanScope:AccessUser]
[ScanScope:ScanSettings]
ScanArchived=no
ScanSfxArchived=no
```

```
ScanMailBases=no
ScanPlainMail=no
ScanPacked=yes
UseTimeLimit=yes
TimeLimit=60
UseSizeLimit=no
SizeLimit=0
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"
```

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 computer 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 27).

Kaspersky Endpoint Security will scan objects in the specified scan areas in the order in which the areas are listed in the configuration file. If you wish to configure different security settings for child and parent directories, place the subdirectory in the list higher, than its parent directory.

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

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

   ```
   /opt/kaspersky/kes4lwks/bin/kes4lwks-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 32);
    - **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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
--set-settings 8 --file=<full path to the file>
```

RESTRICTING A PROTECTION AREA USING MASKS AND REGULAR EXPRESSIONS

By default, Kaspersky Endpoint Security 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 Endpoint Security will scan files or directories from the protection area that are specified using Shell masks or ECMA-262 regular expressions.

> You can use Shell masks to specify a file name template to be scanned by Kaspersky Endpoint Security.
>
> You can also use regular expressions to specify a template for the file path which Kaspersky Endpoint Security should scan. 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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

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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
--set-settings 8 --file=<full path to the file>
```

EXCLUDING OBJECTS FROM THE PROTECTION AREA

By default, Kaspersky Endpoint Security 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 Endpoint Security will not scan files or directories from the protection 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 Endpoint Security.

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

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

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
--set-settings 8 --file=<full path to the file>
```

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

Kaspersky Endpoint Security 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
   --set-settings 8 --file=<full path to the file>
   ```

EXCLUDING OBJECTS BY NAMES OF THE THREATS DETECTED IN THEM

If Kaspersky Endpoint Security considers a scanned object to be infected or suspicious, it performs the action on this object specified in the task. If you consider this object to be harmless for the protected computer, you can exclude it from the scan scope by the name of threat detected in it. In this case Kaspersky Endpoint Security 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 Endpoint Security 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
   --set-settings 8 --file=<full path to the file>
   ```

SELECTING INTERCEPTION MODE

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

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

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--set-settings 8 ProtectionType=KernelOnly
```

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--set-settings 8 ProtectionType=SambaOnly
```

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--set-settings 8 ProtectionType=Full
```

> If the Samba interceptor is enabled, Kaspersky Endpoint Security will not scan objects that are not accessed using SMB / CIFS.

SELECTING PROTECTION MODE

Protection mode (see page 150) is the condition which triggers the real-time protection task. By default, Kaspersky Endpoint Security 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 Endpoint Security 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 protection task settings to a file using the following command:

   ```
   /opt/kaspersky/kes4lwks/bin/kes4lwks-control \
   --get-settings 8 --file=<full path to the file>
   ```

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

   - **SmartCheck**, to enable the Smart mode;

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

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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 Endpoint 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 these objects 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 tasksettings to a file using the following command:

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
--set-settings 8 --file=<full path to the file>
```

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

Kaspersky Endpoint Security 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
--set-settings 8 --file=<full path to the file>
```

SELECTING ACTION TO PERFORM ON DETECTED OBJECTS

As a result of the scan, Kaspersky Endpoint Security 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 the first action is failed to perform, it will perform the second action.

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

- **Recommended**. Kaspersky Endpoint Security 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 Endpoint Security 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.
- **Cure**. Kaspersky Endpoint Security attempts to disinfect the object, and if disinfection is not possible, it leaves the object intact.
- **Quarantine**. Kaspersky Endpoint Security moves the object to quarantine.
- **Remove**. Kaspersky Endpoint Security creates a backup copy of the object, then removes it.
- **Skip**. Kaspersky Endpoint Security leaves the object intact.

> 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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 the first action is failed to perform, it will perform the second action.

You can specify the following actions:

- **Recommended**. Kaspersky Endpoint Security 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 Endpoint Security 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.

- **Cure**. Kaspersky Endpoint Security attempts to disinfect the object, and if disinfection is not possible, it leaves the object intact.
- **Quarantine**. Kaspersky Endpoint Security moves the object to quarantine.
- **Remove**. Kaspersky Endpoint Security creates a backup copy of the object, then removes it.
- **Skip**. Kaspersky Endpoint Security leaves the object intact.

> 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
   --set-settings 8 --file=<full path to the file>
   ```

SCAN OPTIMIZATION

You can shorten the scan time and speed up Kaspersky Endpoint Security. 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
--set-settings 8 --file=<full path to the file>
```

COMPATIBILITY WITH OTHER KASPERSKY LAB'S APPLICATIONS

To ensure compatibility of the Kaspersky Endpoint Security 8 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 Endpoint Security 8 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/kes4lwks/bin/kes4lwks-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>
```

3. Repeat the section specified above for all mail agents integrated with Kaspersky Anti-Virus for Linux Mail Server.

4. 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"
```

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

   ```
   /opt/kaspersky/kes4lwks/bin/kes4lwks-control \
   --set-settings 8 --file=<full path to the file>
   ```

To configure simultaneous operation of Kaspersky Anti-Virus 8 with Kaspersky Anti-Spam, perform the following steps:

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

   ```
   /opt/kaspersky/kes4lwks/bin/kes4lwks-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-Spam>
   [ExcludedFromScanScope:AccessUser]
   UserName=<name of user who is the owner of the mail queue>
   ```

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

   ```
   /opt/kaspersky/kes4lwks/bin/kes4lwks-control \
   --set-settings 8 --file=<full path to the file>
   ```

To configure simultaneous operation of Kaspersky Anti-Virus 8 with Kaspersky Mail Gateway, perform the following steps:

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

   ```
   /opt/kaspersky/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
   --set-settings 8 --file=<full path to the file>
   ```

ON-DEMAND SCAN

On-demand scan involves one-time complete or selective scan for the malicious programs on the computer. Kaspersky Endpoint Security may run several on-demand scan tasks at the same time.

Kaspersky Endpoint Security includes two predefined on-demand scan tasks:

- **On-demand scan**. Scans all local objects on the computer 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 Endpoint Security allows to scan files and directories quickly (see section "Quick scan of files and directories" on page 39) from the command line.

You can create on-demand scan tasks.

IN THIS SECTION

DEFAULT SCAN SETTINGS

In Kaspersky Endpoint Security for on-demand scan task the following default settings are configured.

```
ScanPriority="System"

[ScanScope]

UseScanArea=yes

AreaMask="*"

AreaDesc="All objects"

[ScanScope:AreaPath]
```

```
Path="/"

[ScanScope:ScanSettings]

ScanArchived=yes

ScanSfxArchived=yes

ScanMailBases=no

ScanPlainMail=no

ScanPacked=yes

UseTimeLimit=no

TimeLimit=120

UseSizeLimit=no

SizeLimit=0

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"
```

QUICK SCAN OF FILES AND DIRECTORIES

Kaspersky Endpoint Security allows to scan files and directories without configuring the scan area (see section "Creating scan area" on page 41). You can define name templates for files and directories being scanned or their paths using Shell masks.

> You can use Shell masks to specify templates for the file or directory name to be scanned by Kaspersky Endpoint Security.

➡ *To scan file or directory:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --scan-file <path to file or directory>
```

➡ *To scan several files or directories:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --scan-file <path to file or director>
<path to file or director> 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/kes4lwks/bin/kes4lwks-control --action <action> --scan-file <path to
file or directory>
```

CREATING A SCAN AREA

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

The on-demand scan task scans objects within the computer 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 42).

Kaspersky Endpoint Security will scan objects in the specified scan areas in the order in which the areas are listed in the configuration file. If you wish to configure different security settings for child and parent directories, 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
   --set-settings <task ID> --file=<full path to the file>
   ```

RESTRICTING A SCAN AREA USING MASKS AND REGULAR EXPRESSIONS

By default, Kaspersky Endpoint Security 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 Endpoint Security will scan files or directories from the protection area that are specified using Shell masks or ECMA-262 regular expressions.

> You can use Shell masks to specify a file name template to be scanned by Kaspersky Endpoint Security.
>
> You can also use regular expressions to specify a template for the file path which Kaspersky Endpoint Security should scan. 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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

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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
   --set-settings <task ID> --file=<full path to the file>
   ```

EXCLUDING OBJECTS FROM THE SCAN AREA

By default, Kaspersky Endpoint Security scans all objects within the scan area.

You can define name and path templates that are excluded from the scan area. In this case, Kaspersky Endpoint Security 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 Endpoint Security.

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

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

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

   ```
   /opt/kaspersky/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
   --set-settings <task ID> --file=<full path to the file>
   ```

EXCLUDING OBJECTS BY NAMES OF THE THREATS DETECTED IN THEM

If Kaspersky Endpoint Security considers a scanned object to be infected or suspicious, it performs the action on this object specified in the task. If you consider this object to be harmless for the protected computer, you can exclude it from the scan scope by the name of threat detected in it. In this case Kaspersky Endpoint Security 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 Endpoint Security 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 theon-demand scan task settings to a file using the following command:

   ```
   /opt/kaspersky/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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 Endpoint 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 these objects 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 on-demand scan task settings to a file using the following command:

   ```
   /opt/kaspersky/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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 Endpoint Security 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 the first action is failed to perform, it will perform the second action.

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

- **Recommended**. Kaspersky Endpoint Security 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 Endpoint Security 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.

- **Cure**. Kaspersky Endpoint Security attempts to disinfect the object, and if disinfection is not possible, it leaves the object intact.

- **Quarantine**. Kaspersky Endpoint Security moves the object to quarantine.
- **Remove**. Kaspersky Endpoint Security creates a backup copy of the object, then removes it.
- **Skip**. Kaspersky Endpoint Security leaves the object intact.

> 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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 the first action is failed to perform, it will perform the second action.

You can specify the following actions:

- **Recommended**. Kaspersky Endpoint Security 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 Endpoint Security 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.
- **Cure**. Kaspersky Endpoint Security attempts to disinfect the object, and if disinfection is not possible, it leaves the object intact.
- **Quarantine**. Kaspersky Endpoint Security moves the object to quarantine.
- **Remove**. Kaspersky Endpoint Security creates a backup copy of the object, then removes it.
- **Skip**. Kaspersky Endpoint Security leaves the object intact.

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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control \
   --set-settings <task ID> --file=<full path to the file>
   ```

SCAN OPTIMIZATION

You can shorten the scan time and speed up Kaspersky Endpoint Security. 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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 computer.

- **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 computer should be decreased during task execution.

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--set-settings <task ID> ScanPriority=<priority>
```

ISOLATING SUSPICIOUS OBJECTS. DATA BACKUP

Kaspersky Endpoint Security isolates objects that it considers 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 Endpoint Security 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 Endpoint Security saves to a storage copies of objects before disinfecting or deleting them.

If an object is a part of a compound object, Kaspersky Endpoint Security will save such compound object entirely in the backup storage. For example, if Kaspersky Endpoint Security 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 96).

IN THIS SECTION

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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control -S --get-stat Quarantine
```

If the start and end dates for the report are not specified (see page 66), the statistics for the whole Kaspersky Endpoint Security operating period.

Table1. 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 Endpoint Security.
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 Endpoint Security 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 Endpoint Security 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 Endpoint Security 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 Endpoint Security may recognize some of the objects as clean (the value of the **Type** field (see page 96) for such objects will change to **Clean**). Other objects can be found infected by Kaspersky Endpoint Security.

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

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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	• 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/kes4lwks/bin/kes4lwks-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 Endpoint Security 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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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 computer 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 Endpoint Security was unable to preserve its integrity and the information in the file became unavailable.
- If, having scanning the quarantined objects after database update, Kaspersky Endpoint Security recognizes the object as not infected (the value of the **Type** field (see page 96) for such objects will change to **Clean**).
- If you consider the object harmless for the computer and wish to use it. To prevent Kaspersky Endpoint Security 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 153) or **Exclude objects by threat name** (see page 153) 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 the quarantine / backup to the original location, execute the following command:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --restore <object ID>
```

- *To restore an object from the quarantine / backup to a specified directory, execute the following command:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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 computer, you can delete it from quarantine or backup.

- *To delete one object from the quarantine / backup, execute the following command:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control -Q \
--mass-remove --query "(OrigType!=s'Backup')"
```

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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 91).

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

License Agreement is a legal contract between an individual or legal entity, who/that lawfully holds in ownership a copy of Kaspersky Endpoint Security, 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 Endpoint Security.

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 Endpoint Security database updates;
- Kaspersky Endpoint Security program modules updates.

To obtain these services, you should purchase and activate a license (see section "About Kaspersky Endpoint Security licenses" on page 55).

ABOUT KASPERSKY ENDPOINT SECURITY LICENSES

License is the right to use Kaspersky Endpoint Security 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 55). 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 Endpoint Security.

  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. After the expiration date of the license, Kaspersky Endpoint Security stops performing all of its functions.

- *Commercial* - a paid license with a validity period of, for example, one year, issued when you purchase Kaspersky Endpoint Security. 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 Endpoint Security 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 Endpoint Security 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 Endpoint Security key files" on page 56) associated with the license.

ABOUT KASPERSKY ENDPOINT SECURITY KEY FILES

Key file – a tool used to activate a corresponding license (see section "About Kaspersky Endpoint Security licenses" on page 55), as well as your right to use the application and additional services (see page 55).

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 = 291days.

INSTALLING THE KEY FILE

You can immediately install two key files (see page 56): 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 Endpoint Security 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 Endpoint Security 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/kes4lwks/bin/kes4lwks-control \
--install-active-key <key filename>
```

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--install-suppl-key <key filename>
```

VIEWING INFORMATION ABOUT A LICENSE PRIOR TO THE KEY FILE INSTALLATION

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

- *To view license information (see page 55), execute the following command:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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 56).
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 Endpoint Security provided for by the license.
License period	License validity period (see page 55).

Example of command output:

```
License info:

      Application name:                 Kaspersky Endpoint Security BO Suite
International Edition. 10-14 Workstation 6 months Beta License

      Key file creation date:           2010-09-03

      Key file expiration date:         2011-04-04

      License number:                   1222-0003F4-0A451011

      License type:                     Beta

      Usage restriction:                10 Workstations

      License period:                   183
```

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/kes4lwks/bin/kes4lwks-control \
--revoke-active-key
```

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--revoke-suppl-key
```

REVIEWING THE LICENSE AGREEMENT

License Agreement is a legal contract between an individual or legal entity, who/that lawfully holds in ownership a copy of Kaspersky Endpoint Security, 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 Endpoint Security.

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/kes4lwks/share/doc/LICENSE`.

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 68);
- reports on the activity of Kaspersky Endpoint Security components (see page 66).

You can use the command line to obtain reports on the activity of any individual product component.

You can perform the following operations:

- generate reports for the specified time intervals;
- save created reports in the files of the following formats: HTML or CSV.

MANAGING KASPERSKY ENDPOINT SECURITY FROM THE COMMAND LINE

Apply the following rules when entering Kaspersky Endpoint Security 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 Kaspersky Endpoint Security commands is provided in the table below.

Table 5. The list of Kaspersky Endpoint Security commands

Commands	**Description**
--help (see page 63)	Displays Kaspersky Endpoint Security command help.
Kaspersky Endpoint Security management commands	
--start-app (see page 64)	Starts Kaspersky Endpoint Security.
--restart-app (see page 64)	Restarts Kaspersky Endpoint Security.
--stop-app (see page 64)	Stops Kaspersky Endpoint Security.
--scan-file (see page 65)	Scans files or directories.
-R (see page 65)	Rolls back to previous databases.
Commands for obtaining Kaspersky Endpoint Security statistics	
-S	This prefix indicates that the command is one of a group of commands for obtaining statistics (optional).
-S --app-info (see page 66)	Displays information about Kaspersky Endpoint Security.
-S --get-stat (see page 66)	Creates reports about the operation of Kaspersky Endpoint Security and its components.
-S --top-viruses (see page 68)	Creates reports on threats that are most commonly encountered on the computer.
-S --clean-stat (see page 69)	Deletes statistics about Kaspersky Endpoint Security operation.
Commands to output events of Kaspersky Endpoint Security	
-W (see page 64)	Enables output of Kaspersky Endpoint Security events.
Commands for managing Kaspersky Endpoint Security settings and tasks	

COMMANDS	DESCRIPTION
-T	This prefix indicates that the command is one of a group of commands for managing the Kaspersky Endpoint Security settings and tasks (optional).
-T --get-app-settings (see page 70)	Outputs general Kaspersky Endpoint Security settings.
-T --set-app-settings (see page 71)	Specifies general Kaspersky Endpoint Security settings.
-T --get-task-list (see section "Viewing Kaspersky Endpoint Security task list" on page 72)	Returns the list of existing Kaspersky Endpoint Security tasks.
-T --get-task-state (see page 73)	Outputs the state of selected task (for example, In progress, Stopped, or Paused).
-T --start-task (see page 75)	Starts the task.
-T --stop-task (see page 75)	Stops the task.
-T --suspend-task (see page 75)	Pauses the task.
-T --resume-task (see page 76)	Resumes the task.
-T --get-settings (see page 76)	Outputs task settings.
-T --set-settings (see page 77)	Defines task settings.
-T --create-task (see page 78)	Creates a task of specified type; imports task settings from the specified configuration file.
-T --delete-task (see page 79)	Deletes the task.
-T --set-schedule (see page 79)	Sets task scheduling settings or imports them from a configuration file.
-T --get-schedule (see page 80)	Outputs task scheduling settings.
-T --del-schedule (see page 81)	Sets task scheduling settings, specified by default.
-T --show-schedule (see page 81)	Searches for past scheduled events.
Licenses management commands	

COMMANDS	DESCRIPTION
-L	This prefix indicates that the command is one of a group of commands for managing licenses (optional).
-L --validate-key (see page 83)	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 84)	Outputs information about the license from the key file without installing the license.
-L --get-installed-keys (see page 85)	Outputs information about installed licenses.
-L --query-status (see page 83)	Outputs the status of installed licenses.
-L --install-active-key (see page 86)	Installs an active license.
-L --install-suppl-key (see page 86)	Installs a supplementary license.
-L --revoke-active-key (see page 87)	Deletes an active license.
-L --revoke-suppl-key (see page 87)	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 87)	Outputs brief storage statistics.
-Q --query (see page 87)	Displays information about storages objects.
-Q --get-one (see page 88)	Displays information about one object in the storage.
-Q --restore (see page 88)	Restores an object from the storage.
-Q --add-object (see page 89)	Places a copy of the object to quarantine.
-Q --remove (see page 89)	Deletes the object from storage.
-Q --export (see page 90)	Exports objects from storage into a specified directory.
-Q --import (see page 90)	Imports objects into the storage from a specified directory, into which they were previously exported.
-Q --mass-remove (see page 91)	Removes some or all objects from the storage.
Logs management commands	
-E	This prefix indicates that the command is one of a group of commands for managing logs (optional).
-E --count (see page 92)	Outputs the number of events matching the filter defined in the event log or specified rotation file.
-E --query (see page 92)	Outputs information about events matching the filter defined in the event log or specified rotation file.
-E --period (see page 93)	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 94)	Rotates the event log.
-E --remove (see page 94)	Removes events from the log or the specified rotation file.

IN THIS SECTION

DISPLAYING KASPERSKY ENDPOINT SECURITY COMMAND HELP

The kes4lwks-control --help command <set of Kaspersky Endpoint Security commands> displays Kaspersky Endpoint Security command help.

Command syntax

```
kes4lwks-control --help [<set of Kaspersky Endpoint Security commands>]
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
<set ofKaspersky Endpoint Security commands>	Specify the set of Kaspersky Endpoint Security commands on which you want to get help. Possible values include: -T [--task-and-settings] – commands managing the tasks and general settings of Kaspersky Endpoint Security; -L [--licenser] – license management commands; -Q [--quarantine-and-backup] are quarantine and backup storage management commands; -S [--statistics] – are statistics management commands for Kaspersky Endpoint Security; -E [--event-log] – are event management commands for Kaspersky Endpoint Security.

STARTING KASPERSKY ENDPOINT SECURITY

Before taking the actions or using the commands described above, make sure that the kes4lwks-supervisor service is running on the computer!

The kes4lwks-control command with --start-app key starts Kaspersky Endpoint Security.

Command syntax

```
kes4lwks-control --start-app
```

STOPPING KASPERSKY ENDPOINT SECURITY

Before taking the actions or using the commands described above, make sure that the kes4lwks-supervisor service is running on the computer!

The kes4lwks-control command with --stop-app key stops Kaspersky Endpoint Security.

Command syntax

```
kes4lwks-control --stop-app
```

RESTARTING KASPERSKY ENDPOINT SECURITY

Before taking the actions or using the commands described above, make sure that the kes4lwks-supervisor service is running on the computer!

The kes4lwks-control command with --restart-app key restarts Kaspersky Endpoint Security.

Command syntax

```
kes4lwks-control --restart-app
```

ENABLING EVENTS OUTPUT

The -W command enables the output of Kaspersky Endpoint Security events. You can use this command either by itself, to output all Kaspersky Endpoint Security events, or together with the --start-task command (start task (see section "Starting the task" on page 75)), so as to output only events associated with the task being executed.

Event name and additional event information will be returned.

Command syntax

```
kes4lwks-control -W [--file=<file name>]
```

Examples:

- *Enable the output of Kaspersky Endpoint Security events:*

  ```
  /opt/kaspersky/kes4lwks/bin/kes4lwks-control -W
  ```

- *Enable saving of Kaspersky Endpoint Security events to a file, save events in a file named 081808.xml in the current* *directory:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
-W --file 081808.xml
```

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

QUICK SCAN OF FILES AND DIRECTORIES

The kes4lwks-control command with --scan-file key performs a quick scan of files and directories.

Command syntax

```
kes4lwks-control --action <action> --scan-file <path to the file or directory>[ <path to
the file or directory> ...]
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
--scan-file <path to file or directory>	Name of file or directory which Kaspersky Endpoint Security will scan quickly.
--action <action>	Optional key. Available values: • **Recommended** – perform recommended action. • **Cure**. • **Quarantine**. • **Remove**. • **Skip**. Default value: **Skip**.

ROLLING BACK THE KASPERSKY ENDPOINT SECURITY DATABASE UPDATES

The Kaspersky Endpoint Security creates backup copies of the original databases before it applies updates. If an update procedure gets interrupted or fails, the Kaspersky Endpoint Security 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 Kaspersky Endpoint Security databases task.

Task start syntax

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control -R
```

COMMANDS FOR OBTAINING REPORTS AND STATISTICS

IN THIS SECTION

VIEWING APPLICATION INFORMATION

The --app-info command outputs the information about Kaspersky Endpoint Security.

Command syntax

```
kes4lwks-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 Endpoint Security name
Version	Kaspersky Endpoint Security version
Install date	Date and time of Kaspersky Endpoint Security latest installation
License state	The license state
License expire date	License expiration date

VIEWING REPORTS ON KASPERSKY ENDPOINT SECURITY OPERATION

The --get-stat command outputs the Kaspersky Endpoint Security operation statistics; allows to create reports about the operation of individual components of Kaspersky Endpoint Security over a specified time period; allows to save reports to a file.

Command syntax

```
kes4lwks-control [-S] --get-stat <Kaspersky Endpoint Security 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:

➧ *To view the operation statistics of Kaspersky Endpoint Security:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --get-stat Application
```

➧ *To view real-time protection statistics for January 2009:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--get-stat OAS --from=2009-01-01 --to=2009-01-31
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES

<Kaspersky Endpoint Security component>	Specify the Kaspersky Endpoint Security component for which you want to view statistics. 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: • 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; When specifying the date and time should enclose all the expression in quotation marks, and between the date and time to put a space. • time, formatted as HH:MM:SS, to obtain information starting at the specified time of the current day. If you do not specify the --from=<start date> argument, the report will collect information from the time the Kaspersky Endpoint Security was installed.

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
--to=<end date>	The report ending date. You can assign the following values: • 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; When specifying the date and time should enclose all the expression in quotation marks, and between the date and time to put a space. • time, formatted as HH:MM:SS, to obtain information up to the specified time of the current day. If you do not specify the --to=<end date> argument, the report will collect information up to the current time.
--task-id=<task ID (only for on-demand scan and update tasks)>	The identification number of the Kaspersky Endpoint Security on-demand scan task. 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. This argument is not used together with --from=<start date> and --to=<end date> keys.
--export-report=<report filename>	Optional key. The file name in which the obtained report will be stored. If you specify only a file name without specifying a path to it, then the configuration file will be created in the current directory. If the file with the name specified already exists at the location pointed at the specified path, such file will be overwritten. If the directory specified does not exist on this drive, the file will not be created. 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.
--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.
--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 computer during the specified time interval. This information is displayed on the console and may be saved in a report file.

Command syntax

```
kes4lwks-control [-S] --top-viruses <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 computer in January 2009, and save a report in the /home/kavreports/2009_01_top_viruses.html file:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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 computer.
--from=<start date>	The report starting date. You can assign the following values: • date, formatted as YYYY-MM-DD (or YYYY/MM/DD or YYYY.MM.DD), to obtain information starting at midnight (00:00) of the specified date; • date and time, formatted as YYYY-MM-DD HH:MM:SS, to obtain information starting at the specified time on the specified date; • time, formatted as HH:MM:SS, to obtain information starting at the specified time of the current day. If you do not specify the --from=<start date> argument, the report will collect information from the time the Kaspersky Endpoint Security was installed.
--to=<end date>	The report ending date. You can assign the following values: • date, formatted as YYYY-MM-DD (or YYYY/MM/DD or YYYY.MM.DD), to obtain information until the specified date, inclusive; • date and time, formatted as YYYY-MM-DD HH:MM:SS, to obtain information up to the specified time on the specified date; • time, formatted as HH:MM:SS, to obtain information up to the specified time of the current day. If you do not specify the --to=<end date> argument, the report will collect information up to the current time.
--export-report=<report filename>	Optional key. The file name in which the obtained report will be stored. If you specify only a file name without specifying a path to it, then the configuration file will be created in the current directory. If the file with the name specified already exists at the location pointed at the specified path, such file will be overwritten. If the directory specified does not exist on this drive, the report file will not be created. 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.
--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.

DELETING KASPERSKY ENDPOINT SECURITY OPERATION STATISTICS

The --clean-stat command deletes statistics about Kaspersky Endpoint Security operation.

COMMANDS FOR MANAGING KASPERSKY ENDPOINT SECURITY SETTINGS AND TASKS

IN THIS SECTION

OBTAINING GENERAL KASPERSKY ENDPOINT SECURITY SETTINGS

The --get-app-settings command outputs the general Kaspersky Endpoint Security settings (see page 130). Using this command, you can also obtain the general settings of Kaspersky Endpoint Security that are defined using command-line arguments.

You can use this command to modify general Kaspersky Endpoint Security, installed on the computer:

1. Save the general Kaspersky Endpoint Security 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 Endpoint Security using the --set-app-settings command (see page 71). Kaspersky Endpoint Security 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 Endpoint Security installed on another computer.

Command syntax

```
kes4lwks-control [-T] \
--get-app-settings [--file=<configuration file name>] [--file-format=<INI|XML>]
kes4lwks-control [-T] --get-app-settings [<parameter name>]
```

Examples:

- *Export general Kaspersky Endpoint Security settings into the file kav_config.xml. Save the file created in the current directory:*

  ```
  /opt/kaspersky/kes4lwks/bin/kes4lwks-control \
  --get-app-settings -F kav_config.xml
  ```

- *Output the TraceLevel setting value:*

  ```
  /opt/kaspersky/kes4lwks/bin/kes4lwks-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 Kaspersky Endpoint Security 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.

MODIFYING GENERAL KASPERSKY ENDPOINT SECURITY SETTINGS

The --set-app-settings command modifies general Kaspersky Endpoint Security settings using command-line arguments or imports them from a specified configuration file (see page 130).

You can use this command to modify general Kaspersky Endpoint Security:

1. Save the general settings of Kaspersky Endpoint Security to a configuration file using the --get-app-settings command (see page 70).

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 Endpoint Security using the --set-app-settings command. Kaspersky Endpoint Security will apply new configuration settings after you stop and then start it again using the --stop-app and --start-app commands or using the --restart-app command.

Command syntax

```
kes4lwks-control [-T] --set-app-settings \
--file=<configuration file name> [--file-format=<INI|XML>]
kes4lwks-control [-T] \
--set-app-settings <setting name>=<setting value> \
<setting name>=<setting value>
```

Examples:

- *Import the general settings into Kaspersky Endpoint Security from the configuration file with the /home/test/kav_config.xml name:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--set-app-settings -F /home/test/kav_config.xml
```

- *Set the level of detail in the "Important events" trace log:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--set-app-settings TraceLevel=Warning
```

KEYS	DESCRIPTION AND POSSIBLE VALUES
--file=<configuration file name> -F <configuration file name>	The name of the configuration file settings of which will be imported into Kaspersky Endpoint Security; 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 KASPERSKY ENDPOINT SECURITY TASK LIST

The --get-task-list command returns the list of existing Kaspersky Endpoint Security tasks.

Command syntax

```
kes4lwks-control [-T] --get-task-list
```

The following information about Kaspersky Endpoint Security 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 Kaspersky Endpoint Security).
Id	Task ID number (ID, alternative name, which Kaspersky Endpoint Security assigns to a task when it is created).

Class	Kaspersky Endpoint Security task type. The setting can assume the following values: • tasks, which users can manage: 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); Rollback – task for rolling back to the previous databases (ID=14); • service tasks: 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); EventStorage – implements the events log service (ID=11);
State	Task status. Available values: 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.

VIEWING TASK STATE

The --get-task-state command returns the status of the specified task (for example, Running, Stopped and Paused).

Command syntax

```
kes4lwks-control [-T] --get-task-state <task ID> [--use-name]
```

Example:

➨ *Obtain the status of the task with ID=9:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --get-task-state 9
```

ARGUMENTS, KEYS	DESCRIPTION AND POSSIBLE VALUES
<task ID>	Specify the task ID number (ID, alternative name, which Kaspersky Endpoint Security assigns to a task being created). To view Kaspersky Endpoint Security tasks ID numbers, use the kes4lwks-control --get-task-list command.
--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 Kaspersky Endpoint Security).
Id	Task ID number (ID, alternative name, which Kaspersky Endpoint Security assigns to a task when it is created).
Class	Kaspersky Endpoint Security task type. The setting can assume the following values: • tasks, which users can manage: 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); Rollback – task for rolling back to the previous databases (ID=14); • service tasks: 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); EventStorage – implements the events log service (ID=11);
State	Task status. Available values: Complete – the task is completed successfully; Stopping – the task is stopping; Started – the task is in progress; Starting – the task is starting; Suspended – the task is suspended; Suspending – the task is suspending; Resuming – the task is resuming; Failed – the task has terminated with an error; Interrupted by user – the task execution was interrupted by the user.

STARTING THE TASK

The --start-task command launches the task with specified ID number. This command can be used with the command-line argument -W (see page 64), in this case information about events occurring during task execution is displayed.

Command syntax

```
kes4lwks-control --start-task <task ID> --[progress] [--use-name]
```

Example:

➨ *Start the task with ID=6:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --start-task 6
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
<task ID>	Specify the task ID number (ID, alternative name, which Kaspersky Endpoint Security assigns to a task being created). To view Kaspersky Endpoint Security tasks ID numbers, use the -T --get-task-list command.
--progress	Displays task progress.
--use-name -N	Task name.

STOPPING THE TASK

The --stop-task command stops the task with specified ID number.

Command syntax

```
kes4lwks-control [-T] --stop-task <task ID> [--use-name]
```

Example:

➨ *Stop the task with ID=6:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --stop-task 6
```

ARGUMENT	DESCRIPTION AND POSSIBLE VALUES
<task ID>	Specify the task ID number (ID, alternative name, which Kaspersky Endpoint Security assigns to a task). To view Kaspersky Endpoint Security tasks ID numbers, use the -T--get-task-list command.
--use-name -N	Task name.

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

```
kes4lwks-control [-T] --suspend-task <task ID> [--use-name]
```

Example:

➧ *Pause the task with ID=9:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --suspend-task 9
```

ARGUMENT	DESCRIPTION AND POSSIBLE VALUES
<task ID>	Specify the task ID number (ID, alternative name, which Kaspersky Endpoint Security assigns to a task). To view Kaspersky Endpoint Security tasks ID numbers, use the kes4lwks-control -T --get-task-list command.
--use-name -N	Task name.

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 75).

Command syntax

```
kes4lwks-control [-T] --resume-task <task ID> [--use-name]
```

Example:

➧ *Resume the task with ID=9:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --resume-task 9
```

ARGUMENT	DESCRIPTION AND POSSIBLE VALUES
<task ID>	Specify the task ID number (ID, alternative name, which Kaspersky Endpoint Security assigns to a task). To view Kaspersky Endpoint Security tasks ID numbers, use the -T --get-task-list command.
--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 77) from this configuration file into the task of a corresponding type on another server.

Command syntax

```
kes4lwks-control [-T] --get-settings <task ID> \
[--file=<configuration file name>] -- [--use-name] [--use-name]
kes4lwks-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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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 Endpoint Security assigns to a task being created). To view Kaspersky Endpoint Security tasks ID numbers, use the -T --get-task-list command.
--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 Endpoint Security 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

```
kes4lwks-control [-T] --set-settings <task ID> \
--file=<configuration file name> [--file-format=<INI|XML>] [--use-name]
kes4lwks-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/kes4lwks/bin/kes4lwks-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 Endpoint Security assigns to a task). To view Kaspersky Endpoint Security tasks ID numbers, use the -T --get-task-list command.
--file=<configuration file name> -F <configuration file name>	The name of the configuration file settings of which will be imported into the task; it includes full path to the file.
--file-format=<INI|XML>	Optional key. By default, the format of the configuration file specified by the -F key 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 Endpoint Security 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

```
kes4lwks-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/kes4lwks/bin/kes4lwks-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. Kaspersky Endpoint Security 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 Endpoint Security 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

```
kes4lwks-control [-T] --delete-task <task ID> [--use-name]
```

Example:

➧ *Delete the task with ID=20:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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 Endpoint Security assigns to a task being created). To view Kaspersky Endpoint Security tasks ID numbers, use the -T --get-task-list command.
--use-name -N	Task name.

OBTAINING TASK SCHEDULE SETTINGS

The --get-schedule command outputs the task schedule settings (see page 127). 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 Endpoint Security using the --set-schedule (see section "Modifying task schedule settings" on page 80). Kaspersky Endpoint Security will apply the new schedule settings immediately.

Command syntax

```
kes4lwks-control [-T] --get-schedule <task ID> \
[--file=<configuration file name>] -- [--use-name] [--use-name]
kes4lwks-control [-T] --get-schedule <task ID> <parameter name> [--use-name]
```

Examples:

➧ *Save Kaspersky Endpoint Security settings to the file on_demand_schedule.xml. Save the file created in the current directory:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--get-schedule 9 -F on_demand_schedule.xml
```

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control \
--get-schedule 9 RuleType
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
<task ID>	The identification number of the Kaspersky Endpoint Security 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 127).

You can use this command to modify Kaspersky Endpoint Security:

1. Save the schedule settings to a configuration file using the -T --get-schedule (see section "Obtaining task schedule settings" on page 79).
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 Endpoint Security using the -T --set-schedule command. Kaspersky Endpoint Security will apply the new schedule settings immediately.

Command syntax

```
kes4lwks-control -T --set-schedule <task ID> --file=<configuration file name> \
[--file-format=<INI|XML>] [--use-name]
kes4lwks-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/kes4lwks/bin/kes4lwks-control -T \
--set-schedule 9 -F /home/test/on_demand_schedule.xml
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
<task ID>	The identification number of the Kaspersky Endpoint Security 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 Endpoint Security (see Guide of Kaspersky Endpoint Security 8 for Linux).

Command syntax

```
kes4lwks-control -T --del-schedule <task ID> [--use-name]
```

Example:

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

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control -T --del-schedule 15
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
<task ID>	The identification number of the Kaspersky Endpoint Security task.
--use-name -N	Task name.

SEARCHING FOR SCHEDULED EVENTS

The -T --show-schedule command searches for scheduled events.

Command syntax

```
kes4lwks-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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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>	Schedule rule type. Available values: • `Time` – rules containing the time for the task start. • `Startup` – rules containing a PS condition (at Kaspersky Endpoint Security start). • `Basereload` – rules containing a BR condition (upon database update).
--from=<start date>	The report starting date. You can assign the following values: • date, formatted as YYYY-MM-DD (or YYYY/MM/DD or YYYY.MM.DD) , to start searching from midnight (00:00) of the specified date; • date and time, formatted as YYYY-MM-DD HH:MM:SS , to obtain information starting at the specified time on the specified date; • time, formatted as HH:MM:SS , to start searching from the specified time of the current day. If you skip the option --from=<start date>, search will begin with the command execution time.
--to=<end date>	The report ending date. You can assign the following values: • date, formatted as YYYY-MM-DD (or YYYY/MM/DD or YYYY.MM.DD) , to search information until the specified date, inclusive; • date and time, formatted as YYYY-MM-DD HH:MM:SS , to search information up to the specified time on the specified date; • time, formatted as HH:MM:SS , to search information up to the specified time of the current day. 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

The kes4lwks-control --validate-key command uses Kaspersky Lab's database to verify if a key file is genuine and is issued for Kaspersky Endpoint Security. This command outputs information about the key file to the console, without installing it.

Command syntax

```
kes4lwks-control [-L] --validate-key <path to key file>
```

Example:

➡ *Validate the license in file /home/test/00000001.key:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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 Endpoint Security name.
Key file creation date	License creation date.
License expiration date	Date when the license validity period completes calculated by Kaspersky Endpoint Security; 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

```
kes4lwks-control [-L] --show-license-info <path to key file>
```

Example:

➡ *Output license information from the /home/test/00000001.key file:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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 Endpoint Security 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 kes4lwks-control --get-installed-keys command outputs information about the installed key files to the console.

Command syntax

```
kes4lwks-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 Endpoint Security 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	Kaspersky Endpoint Security 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 – Kaspersky Endpoint Security performs none of its functions. This mode is activated upon expiration of a trial license.
Detailed license information:	
Application name	Kaspersky Endpoint Security 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

```
kes4lwks-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 Endpoint Security key files" section (see page 55).

Command syntax

```
kes4lwks-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/kes4lwks/bin/kes4lwks-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 Endpoint Security key files" section (see page 55).

If the active key file is not installed, a supplementary key file will be installed as the active key file.

Command syntax

```
kes4lwks-control [-L] --install-suppl-key <path to key file>
```

Example:

➧ *Install a supplementary license from the /home/test/00000002.key file:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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

```
kes4lwks-control [-L] --revoke-active-key
```

SUPPLEMENTARY KEY FILE REMOVAL

The --revoke-suppl-key command removes the installed supplementary key file.

Command syntax

```
kes4lwks-control [-L] --revoke-suppl-key
```

QUARANTINE AND BACKUP STORAGE MANAGEMENT COMMANDS

IN THIS SECTION

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

```
kes4lwks-control [-Q] --get-stat [--query "<logical expression>"]
```

Examples:

- *To view brief quarantine statistics:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control -Q \
--get-stat --query "(OrigType!=s'Backup')"
```

- *To view brief backup storage statistics:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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

```
kes4lwks-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/kes4lwks/bin/kes4lwks-control -Q --query ""
```

➡ *To view information about objects in quarantine and display 51 entries starting with the 50th entry:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control -Q --query "(OrigType!=s'Backup')" \
--limit=50 --offset=50
```

➡ *To displays information about objects from the backup storage:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control -Q --query "(OrigType==s'Backup')"
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
"<logical expression>"	Creates a filter consisting of a logical expression (see page 95).
--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

```
kes4lwks-control [-Q] --get-one <object ID> [--detailed]
```

Example:

➡ *To obtain information about the object with ID=1:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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 87).
--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

```
kes4lwks-control [-Q] --restore <identification number of object in storage> \
[--file=<file name and path to file>]
```

Examples:

➧ *To restore the object with ID=1 to its original location:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --restore 1
```

➧ *To restore the object with ID=1 to the current directory, in a file named restored.exe:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --restore 1 -F restored.exe
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
<object ID>	To obtain the object identification number, you can use the -Q --query command (see page 87).
--file=<file name> -F <file name>	Name of the file in which Kaspersky Endpoint Security will save the object during restoration, it includes the file path. If you do not specify a file path, Kaspersky Endpoint Security will save the file in the current directory. If you omit this argument, Kaspersky Endpoint Security 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

```
kes4lwks-control [-Q] --add-object <file name>
```

Example:

➧ *To place a copy of the /home/sample.exe file to quarantine:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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

```
kes4lwks-control [-Q] --remove <object ID>
```

Example:

➧ *To delete the object with ID=1:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control -Q --remove 1
```

ARGUMENT	DESCRIPTION AND POSSIBLE VALUES
<object ID>	To obtain the object identification number, you can use the -Q --query command (see page 87).

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 computer. The location of the storage directory on the computer is specified in the quarantine and backup storage configuration file (see page 132).

You can use filters to export only selected objects, for example, only quarantined objects.

Command syntax

```
kes4lwks-control [-Q] --export <target 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/kes4lwks/bin/kes4lwks-control -Q\
--export /media/flash128/avpstorage
```

➧ *To export 50 quarantined objects to the /media/flash128/avpstorage directory, starting with the 51st entry:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-control -Q \
--export /media/flash128/avpstorage --query "(OrigType==s'Backup')"
```

ARGUMENT, KEYS	DESCRIPTION AND POSSIBLE VALUES
<destination directory>	Directory in which Kaspersky Endpoint Security stores objects from the backup storage. If the directory does not exist, it will be created. You can specify a directory for remote resources mounted on the computer using SMB/CIFS and NFS.
--query="<logical expression>"	Creates a filter consisting of a logical expression (see page 95).
--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 computer is specified in the quarantine and backup storage configuration file (see page 132).

Command syntax

```
kes4lwks-control [-Q] --import <directory containing exported objects>
```

Example:

- *To import objects from the /media/flash128/avpstorage directory into the storage:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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

```
kes4lwks-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/kes4lwks/bin/kes4lwks-control --mass-remove
```

- *To delete quarantined objects only, 50 entries, starting with the 51st entry:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control -Q --mass-remove \
--query "(OrigType!=s'Backup')" --limit=50 --offset=50
```

- *To delete objects from the backup storage:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control -Q \
--mass-remove --query "(OrigType==s'Backup')"
```

KEYS	DESCRIPTION AND POSSIBLE VALUES
--query="<logical expression>"	Creates a filter consisting of a logical expression (see page 95).
--limit=<maximum number of records>	Sets a filter: maximum number of records from query, which should be displayed.
--offset=<offset from the query beginning>	Sets a filter: maximum number of records from query, which should be skipped from the query beginning.

LOGS MANAGEMENT COMMANDS

IN THIS SECTION

OBTAINING THE NUMBER OF KASPERSKY ENDPOINT SECURITY EVENTS WITH 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 92).

Command syntax

```
kes4lwks-control [-E] --count "<logical expression>" [--db=<rotation file>]
```

Examples:

- *To obtain the number of Kaspersky Endpoint Security events, stored in the trace log:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-control --count ""
```

- *Obtain the number of Kaspersky Endpoint Security events stored in the rotation file EventStorage-2009-12-01-23-57-23.db:*

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-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 95).
--db=<rotation file>	The rotation file, information in which you wish to view (this file has the extension .db). If you do not provide this modifier, Kaspersky Endpoint Security will display the number of events in the log at the moment.

OBTAINING THE INFORMATION ABOUT KASPERSKY ENDPOINT SECURITY EVENTS

The --query command allows obtaining information about Kaspersky Endpoint Security events from Kaspersky Endpoint Security event log or from the rotation file; and it allows saving the obtained information in a file.

Command syntax

```
kes4lwks-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/kes4lwks/bin/kes4lwks-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 95).
--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 Endpoint Security 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. Name of the file in which Kaspersky Endpoint Security 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

```
kes4lwks-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/kes4lwks/bin/kes4lwks-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/kes4lwks/bin/kes4lwks-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 Endpoint Security 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.

If the RotateMethod setting has the Erase value, Kaspersky Endpoint Security deletes information about events from the log.

If the RotateMethod setting has the Move value, Kaspersky Endpoint Security transfers information about events from the log into the RotateMoveFolder directory and saves it in the rotation file.

Command syntax

```
kes4lwks-control [-E] --rotate
```

REMOVING OBJECTS FROM THE EVENT LOG

The --remove command deletes records about events from Kaspersky Endpoint Security log or from the specified rotation file.

You can delete all records, or just several records, by using filters.

Command syntax

```
kes4lwks-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/kes4lwks/bin/kes4lwks-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 95).
--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 Endpoint Security will delete records from Kaspersky Endpoint Security event log.

LIMITING SELECTIONS USING FILTERS

IN THIS SECTION

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 Endpoint Security events: -E --count "<logical expression>" (see page 92);
- obtaining information about the events of Kaspersky Endpoint Security: -E --count "<logical expression>" (see page 92);
- obtaining information about objects in quarantine or in the backup storage: -Q --query "<logical expression>" (see page 87);
- obtaining concise statistical information about objects in quarantine or in the backup storage: -Q --get-stat --query "<logical expression>" (see page 87);
- selective removal of objects from the storage: -Q --mass-remove --query "<logical expression>" (see page 91);
- selective export of objects from quarantine or from the backup storage: -Q --export --query "<logical expression>" (see page 90).

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 96). 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 6. 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.
OrigVerdict Verdict	s	OrigVerdict – type of threat detected in the object when the object was placed in the storage. Verdict – type of threat detected in the quarantined object after scanning with updated databases. Possible values include: 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	OrigDangerLevel – danger level of the threat detected in an object when the object was placed in the storage. DangerLevel – danger level of the threat in the quarantined object after scanning with updated databases. The danger level of an object depends on the type of threat in the object (see section "Programs detectable by Kaspersky Endpoint Security" on page 11). The danger level may assume the following values: 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	OrigDetectCertainty – the state of a detected object upon its placement in the storage. DetectCertainty – the state Kaspersky Endpoint Security assigns to an object in quarantine

FIELD	TYPE	DESCRIPTION AND POSSIBLE VALUES
		after scanning it using updated databases. Possible values include: 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	OrigThreatName – the name of the threat, based on the Kaspersky Lab classification, found in the object when the object is placed in the storage. ThreatName – the name of the threat detected in a quarantined object after scanning with updated databases. You can use masks with the aid of the 'like' comparison operator.
Compound	i	Indicates, whether the object is a compound object. Possible values include: yes – the object is a compound object; no – the object is not compound.
UID	i	The ID (UID) of the user that created the object.
GID	i	The ID (GID) of the group to which the user who created the object belongs.
Mode	i	Access permissions.
AddTime	s	The date and time the object was placed in the storage, formatted as "YYYY-MM-DD HH:MM:SS". If you specify the date but not the time, the time will be specified as 00:00:00. If you specify the time but not the date, the current date will be specified. If you specify the date and time as follows: (AddTime== s"), then the current date and time will be specified.
Size	i	Original size of the object, in bytes.

KASPERSKY ENDPOINT SECURITY EVENTS AND THEIR SETTINGS

You can filter Kaspersky Endpoint Security based on their settings. The following table describes Kaspersky Endpoint Security events, event settings are described in the next table below.

Table 7. Events

№	EVENT NAME	DESCRIPTION	SETTINGS
1	ApplicationStarted	Kaspersky Endpoint Security is running; the event occurs after all tasks necessary for Kaspersky Endpoint Security are started.	Date, EventId, EventType, RuntimeTaskID, TaskId, TaskName, TaskType
2	ApplicationSettingsChanged	General Kaspersky Endpoint Security settings have 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	Updated Kaspersky Endpoint Security databases have been successfully installed.	Date, EventId, EventType, RuntimeTaskID, AVBasesDate, TaskId, TaskName, TaskType
11	AVBasesAreOutOfDate	The Kaspersky Endpoint Security databases are outdated.	Date, EventId, EventType, RuntimeTaskID, TaskId, TaskName, TaskType
12	AVBasesAreTotallyOutOfDate	The Kaspersky Endpoint Security databases are obsolete.	Date, EventId, EventType, RuntimeTaskID, TaskId, TaskName, TaskType
13	AVBasesIntegrityCheckOK	Integrity check of Kaspersky Endpoint Security databases completed successfully.	Date, EventId, EventType, RuntimeTaskID, TaskId, TaskName, TaskType
14	AVBasesIntegrityCheckFailed	Kaspersky Endpoint Security databases failed an integrity check.	Date, EventId, EventType, RuntimeTaskID, TaskId, TaskName, TaskType
15	AVBasesApplied	The Kaspersky Endpoint Security databases are applied.	Date, EventId, EventType, RuntimeTaskID, TaskId, TaskName, TaskType

№	EVENT NAME	DESCRIPTION	SETTINGS
16	UpdateSourceSelected	An update source has been selected.	Date, EventId, EventType, RuntimeTaskID, TaskId, TaskName, TaskType
17	UpdateSourceNotSelected	An update source connection error has occurred.	Date, EventId, EventType, RuntimeTaskID, TaskId, TaskName, TaskType
18	NothingToUpdate	No update is required. This event occurs if the version of the database updates installed on the computer corresponds to or is newer than the version of the database updates on the update source.	Date, EventId, EventType, RuntimeTaskID, TaskId, TaskName, TaskType
19	UpdateError	An error occurred while updating.	Date, EventId, EventType, ModuleName, RuntimeTaskID, TaskId, TaskName, TaskType
20	ModuleDownloaded	A program module has been downloaded.	Date, EventId, EventType, ModuleName, RuntimeTaskID, TaskId, TaskName, TaskType
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,

№	EVENT NAME	DESCRIPTION	SETTINGS
			FileOwnerId, ObjectName, RuntimeTaskID, SkipReason, TaskId, TaskName, TaskType
30	ObjectProcessingError	A processing error has occurred.	Date, EventId, EventType, AccessHost, AccessUser, AccessUserId, FileName, FileOwner, FileOwnerId, ObjectName, ObjectProcessError, RuntimeTaskID, TaskId, TaskName, TaskType
31	ObjectDisinfected	The object has been disinfected.	Date, EventId, EventType, AccessHost, AccessUser, AccessUserId, FileName, FileOwner, FileOwnerId, ObjectName, RuntimeTaskID, TaskId, TaskName, TaskType
32	ObjectNotDisinfected	The object has not been disinfected.	Date, EventId, EventType, AccessHost, AccessUser, AccessUserId, FileName, FileOwner, FileOwnerId, ObjectNotDisinfectedReason, RuntimeTaskID, TaskId, TaskName, TaskType
33	ObjectDeleted	The object has been deleted.	Date, EventId, EventType, AccessHost, AccessUser, AccessUserId, FileName, FileOwner, FileOwnerId, RuntimeTaskID, TaskId, TaskName, TaskType
34	ObjectBlocked	The real-time protection task has denied object access to an accessing application.	Date, EventId, EventType, AccessHost, AccessUser, AccessUserId, FileName, FileOwner, FileOwnerId, RuntimeTaskID, TaskId, TaskName, TaskType
35	ObjectActionsCompleted	Action on infected object completed.	Date, EventId, EventType, AccessHost, AccessUser, AccessUserId, FileName, FileOwner, FileOwnerId, ObjectReason, ObjectSource, ObjectType, RuntimeTaskID, TaskId, TaskName, TaskType
36	ObjectSavedToQuarantine	Object quarantined.	Date, EventId, EventType, DangerLevel, DetectCertainty, FileName, QuarantineId, QuarantineObjectType, RuntimeTaskID, TaskId, TaskName, TaskType, VerdictType
37	ObjectSavedToBackup	The object was placed in Backup.	Date, EventId, EventType, DangerLevel, DetectCertainty, FileName, QuarantineId, QuarantineObjectType, RuntimeTaskID, TaskId, TaskName, TaskType, VerdictType
38	ObjectRemovedFromQuarantine	Object was deleted from quarantine.	Date, EventId, EventType, FileName, QuarantineId, QuarantineObjectType, RuntimeTaskID, TaskId, TaskName, TaskType
39	ObjectRemovedFromBackup	The object has been removed from backup.	Date, EventId, EventType, FileName, QuarantineId, QuarantineObjectType, RuntimeTaskID, TaskId, TaskName,

№	EVENT NAME	DESCRIPTION	SETTINGS
			TaskType
40	ObjectRestoredFromQuarantine	Object restored from Quarantine.	Date, EventId, EventType, FileName, QuarantineId, QuarantineObjectType, RuntimeTaskID, TaskId, TaskName, TaskType
41	ObjectRestoredFromBackup	Object has been restored from backup.	Date, EventId, EventType, FileName, QuarantineId, QuarantineObjectType, RuntimeTaskID, TaskId, TaskName, TaskType
42	QuarantineSizeLimitReached	Quarantine and backup maximum size reached.	Date, EventId, EventType, FileName, RuntimeTaskID, TaskId, TaskName, TaskType
43	QuarantineSoftSizeLimitExceeded	Quarantine size defined by the **QuarantineSoftSizeLimit** setting has been reached.	Date, EventId, EventType, RuntimeTaskId, TaskId, TaskName, TaskType
44	QuarantineObjectCorrupted	Object in Quarantine is corrupted.	Date, EventId, EventType, FileName, QuarantineId, RuntimeTaskID, TaskId, 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 Endpoint Security 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 Endpoint Security databases completed successfully.	Date, EventId, EventType, RuntimeTaskID, TaskId, TaskName, TaskType
54	AVBasesRollbackError	Error while rolling back the Kaspersky Endpoint Security databases.	Date, EventId, EventType, RuntimeTaskID, TaskId, TaskName, TaskType
55	OASTaskError	Real time protection error.	Date, Error, EventId, EventType, Info, RuntimeTaskID, TaskId, TaskName,

№	EVENT NAME	DESCRIPTION	SETTINGS
			TaskType
56	ODSTaskError	Creating an on-demand scan.	Date, Error, EventId, EventType, Info, RuntimeTaskID, TaskId, TaskName, TaskType
57	EventsErased	Events erased.	Date, BeginDate, EndDate, EventId, EventType, Reason, RuntimeTaskID, TaskId, TaskName, TaskType
58	EventsMoved	Events moved.	Date, BeginDate, EndDate, EventId, EventType, Path, Reason, RuntimeTaskID, TaskId, TaskName, TaskType

Table 8. 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	DangerLevel – danger level of the threat detected in an object when the object was placed in the storage. OrigDangerLevel – danger level of the threat in the quarantined object after scanning with updated databases. The danger level of an object depends on the type of threat in the object (see section "Programs detectable by Kaspersky Endpoint Security" on page 11). The danger level may assume the following values: 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.
Date	s	Date and time of the event.
DetectCertainty (OrigDetectCertainty)	s	OrigDetectCertainty – the state of a detected object upon its placement in the storage. DetectCertainty – the state Kaspersky Endpoint Security assigns to an object in quarantine after scanning it using updated databases. The state of the detected object: 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).
EndDate	s	Date before which events are deleted or moved.
Error	s	Type of error. Possible values include: IncorrectUser – non existent user given in the task settings, his/her name is

SETTING	TYPE	DESCRIPTION
		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 Kaspersky Endpoint Security interception occurred.
Info	s	Additional information about the error.
ModuleName	s	The name of the Kaspersky Endpoint Security module related to an 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 – Kaspersky Endpoint Security only has read access rights to the object.
ObjectProcessError	s	The type of error that occurred during object scanning: Unknown InternalError ObjectNotCurable ObjectNoRights ObjectIOError OutOfSpace ObjectNotFound ObjectReadOnly SystemError

ObjectReason	s	Result of activities on the object. Possible values include:
		Cured – object disinfected;
		Removed – object deleted;
		Quarantined – object moved to quarantine;
		Skipped – object skipped;
		AllActionsFailed – all actions on the object ended with an error.

ObjectSource	s	Source of the infected file:

SETTING	TYPE	DESCRIPTION
		LocalFile – local file system; RemoteNfsFile – remote resource accessed by NFS protocol; RemoteSambaFile – remote resource accessed by SMB/CIFS protocol.
ObjectType	s	The object type (whether the object is a compound object or not): Object – the object is not compound; Archive – the object is a compound object.
Path	s	Path to file where events have been moved.
QuarantineId	i	The ID of the object in the storage; is assigned by Kaspersky Endpoint Security.
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	Kaspersky Endpoint Security task type. The setting can assume the following values: • tasks, which users can manage: 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); Rollback – task for rolling back to the previous databases (ID=14); • service tasks: 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);

SETTING	TYPE	DESCRIPTION
		License – implements the license server (ID=5); EventStorage – implements the events log service (ID=11).
ThreatName	s	The name of the threat detected in the object related to the event.
Type (OrigType)	s	OrigType – the state of the object, assigned when the object is placed in the storage. Type – the state of an object in quarantine after it has been scanned using updated databases. Possible values include: 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.

Table 9.

KASPERSKY ENDPOINT SECURITY CONFIGURATION FILES' SETTINGS

You can create Kaspersky Endpoint Security configuration files either in INI or in XML format.

This section describes the structure and settings of Kaspersky Endpoint Security INI configuration files.

IN THIS SECTION

RULES FOR EDITING KASPERSKY ENDPOINT SECURITY .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 Endpoint Security will apply the default value if there is 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).

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 77) from the configuration file, the comments are ignored. While viewing task settings (see section "Obtaining task settings" on page 76), 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 76) 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 77).

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 Kaspersky Endpoint Security 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 Endpoint Security will use for the scan area specified in the [ScanScope:AreaPath] section. If you do not define settings of these sections, Kaspersky Endpoint Security 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]

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

    ...
```

Kaspersky Endpoint Security scans areas in the order specified in the configuration file.

Note that if a file is part of several specified scan areas, Kaspersky Endpoint Security 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

...
```

Kaspersky Endpoint Security 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 Endpoint Security .ini configuration files (see page 107).

Table 10. Real-time protection and on-demand scan tasks settings

SETTING	DESCRIPTION AND POSSIBLE VALUES
`ScanPriority`	Task priority. This setting is used only in the on-demand scan tasks and is not used in the real-time protection tasks. You can set one of the predefined task priorities in accordance with process priorities in Linux. Possible values include: **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. Lower process priority increases the duration of task execution, but it can also affect positively the performance of processes belonging to other active applications. Higher process priority decreases the duration of task execution, but it can also affect negatively the performance of processes belonging to other active applications. Default value: **System**.

SETTING	DESCRIPTION AND POSSIBLE VALUES
`ProtectionType`	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.). This setting is used only in the real-time protection task and is not used in on-demand scan tasks. Kaspersky Endpoint Security contains two components that intercept attempts to access files and scan them: a SAMBA interceptor (used to scan objects on remote computers when they are accessed via SMB/CIFS) and a kernel level interceptor. It scans objects when they are accessed in some other way. The SAMBA interceptor provides, as additional object information, the IP address of the remote computer, on which the application attempted to access the object when it was intercepted by Kaspersky Endpoint Security. If you use the protected computer only as a SAMBA server, you can specify the value SambaOnly. In this case, Kaspersky Endpoint Security will not scan objects that are not accessed via SMB/CIFS. Possible values include: **Full**. Kaspersky Endpoint Security scans computer objects with the SAMBA interceptor when they are accessed via SMB/CIFS. Kaspersky Endpoint Security uses the kernel level interceptor to intercept all other operations on files that are accessible on the protected computer (including files on remote computers). **SambaOnly**. Kaspersky Endpoint Security 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 Endpoint Security (see Installation Guide of Kaspersky Endpoint Security 8 for Linux). **KernelOnly**. Kaspersky Endpoint Security scans computer objects using file interceptor only. Make sure that you have specified the kernel interceptor during the initial configuration of Kaspersky Endpoint Security (see Installation Guide of Kaspersky Endpoint Security 8 for Linux). Default value: the operation shall be selected during Kaspersky Endpoint Security installation.
`[ScanScope]` Scan area.	
`AreaDesc`	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. Example: `AreaDesc="Scan mail databases"` Default value: **All objects**.
`AreaMask`	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. Within the scan area, Kaspersky Endpoint Security will scan only those files or directories specified using Shell masks or ECMA-262 regular expressions. Use the **re:** prefix in regular expressions. If you do not specify this setting, Kaspersky Endpoint Security will scan all objects in the scan area. You can specify several values for this setting.

SETTING	DESCRIPTION AND POSSIBLE VALUES

	Example:
	`AreaMask=re:.*/Documents/`
	`AreaMask=re:.*\.doc`
	`AreaMask=re:\.exe`
	Default value: *.

`UseAccessUser`	This setting determines whether or not to use the settings in the [ScanScope:AccessUser] section (scanning upon access using the permissions of specified users). The setting of this section is applied only in real-time protection tasks. It is not used for on-demand scan tasks. Possible values include: **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. Default value: **no**.
`[ScanScope:AreaPath]` Scan scope, path to the directory to scan. You must specify at least one scan area to start the real-time protection task.	
`Path`	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: **Mounted**. Remote directories mounted on the computer. Using the <access protocol> setting, specify the protocol that provides remote access to the directories. **Shared**. Computer file system resources shared by the SMB/CIFS or NFS protocol. **AllRemotelyMounted**. All remote directories mounted on the computer using SMB/CIFS and NFS protocols. **AllShared**. Computer file system resources shared by the SMB/CIFS and NFS protocols. **<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: **SMB**. The SMB/CIFS protocol. **NFS**. The NFS protocol. **<path to the directory being scanned>**. Full path to the directory being scanned. For peculiarities in the scanning of symbolic and hard links please refer to the section Peculiarities in scanning of symbolic and hard links (see page 9). Examples: `Path=/` – *scan all local computer directories mounted with SMB/CIFS or NFS.* `Path=/home/ivanov` – *scan the /home/ivanov directory.* `Path=Mounted:SMB` – *scan all remote directories mounted using SMB/CIFS*.

SETTING	DESCRIPTION AND POSSIBLE VALUES
	`Path=Mounted:NFS` – *scan all remote directories mounted using NFS*. `Path=Mounted:SMB:/remote-resources/ivanov-windows` – *scan the /remote-resources/ivanov-windows directory, which has been mounted using SMB/CIFS*. `Path=Mounted:NFS:/remote-resources/ivanov-linux` – *scan the /remote-resources/ivanov-windows directory, which has been mounted using NFS*. `Path=Shared:SMB` – *scan all directories in the computer's file system shared by SMB/CIFS*. `Path=Shared:SMB:my_samba_share` – *scan the resource with the name my_samba_share shared by SMB/CIFS*. `Path=Shared:NFS` – *scan all computer directories that are accessible via NFS*. `Path=Shared:NFS:/nfs_shares/my_share`– *scan the resource with the name /nfs_shares/my_share shared by NFS.* Default value: /.
`[ScanScope:AccessUser]` Scan upon access using the permissions of specified users. Kaspersky Endpoint Security 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, Kaspersky Endpoint Security scans objects when they are accessed with any rights. The settings of this section are applied only in real-time protection tasks. They are not used for on-demand scan tasks. 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.	

`UserName`	Kaspersky Endpoint Security 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:
	`UserName=usr1`
	`UserName=usr2`
	Default value: not configured.

`UserGroup`	Group name. Kaspersky Endpoint Security 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:
	`UserGroup=group1`
	`UserGroup=group2`
	Default value: not configured.

`[ScanScope:ScanSettings]` Security settings that Kaspersky Endpoint Security applies when scanning the area specified by the [ScanScope:AreaPath] setting.	
`ScanByAccessType`	Kaspersky Endpoint Security 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): **SmartCheck** (smart mode). Kaspersky Endpoint Security 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 Endpoint Security scans the object a second time only when the process closes it for the last time.

SETTING	DESCRIPTION AND POSSIBLE VALUES
	Open (at an access attempt). Kaspersky Endpoint Security scans the object when an attempt is made to open for reading or for execution or modification. **OpenAndModify** (at an attempt to access or modify). Kaspersky Endpoint Security 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. Default value: **SmartCheck**.
`ScanArchived`	Kaspersky Endpoint Security scans file archives (including SFX self-extracting archives). Please note that Kaspersky Endpoint Security identifies threats in archives, but does not disinfect them. **yes** – scan archives; **no** – do not scan archives. Default values: real-time protection task – **no**; on-demand scan task – **yes**.
`ScanSfxArchived`	Kaspersky Endpoint Security scans self-extracting archives (archives that contain an executable extraction module). **yes** – scan SFX archives; **no** – do no scan SFX archives. Default values: real-time protection task – **no**; on-demand scan task – **yes**.
`ScanMailBases`	Kaspersky Endpoint Security scans email databases of Microsoft Outlook, Outlook Express, The Bat! and other email clients. **yes** – scan email database files; **no** – do not scan email database files. Default value: **no**.
`ScanPlainMail`	Kaspersky Endpoint Security scans the files of plain text email messages. **yes** – scan plain text email messages; **no** – do not scan plain text email messages. Default value: **no**.
`ScanPacked`	Kaspersky Endpoint Security scans executable files packed by binary code packers, such as UPX or ASPack. This type of composite object contains threats more often than others. **yes** – scan packed files; **no** – do not scan packed files. Default value: **yes**.
`InfectedFirstAction`	First action to be performed on infected objects. In real-time protection tasks, before performing the action specified by you on an infected object, Kaspersky Endpoint Security blocks access to the object by applications that

SETTING	DESCRIPTION AND POSSIBLE VALUES
	attempt to do so. Possible values include: **Cure**. Kaspersky Endpoint Security attempts to disinfect the 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 Endpoint Security will leave the object unchanged. **Remove**. Kaspersky Endpoint Security creates a backup copy of the infected object, then removes it. **Recommended** (perform recommended action). Kaspersky Endpoint Security 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, Kaspersky Endpoint Security 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. **Quarantine**. Kaspersky Endpoint Security moves the object to Quarantine. **Skip**. The object will remain intact. Kaspersky Endpoint Security does not attempt to cure or delete the object, but does log information about the object. Default value: **Recommended**.

SETTING	DESCRIPTION AND POSSIBLE VALUES
`InfectedSecondAction`	Second action to be performed on infected objects. The values are the same as for the InfectedFirstAction setting. If Kaspersky Endpoint Security fails to perform the first action, it will perform the second action. 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. If you do not specify a second action, Kaspersky Endpoint Security will use Skip as the second action. Default value: **Skip**.
`SuspiciousFirstAction`	First action to be performed on suspicious objects. In real-time protection tasks, before performing the action specified by you on an object, Kaspersky Endpoint Security blocks access to the object by applications that attempt to do so. Possible values include: **Cure**. Kaspersky Endpoint Security attempts to disinfect the 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 Endpoint Security will leave the object unchanged. **Quarantine**. Kaspersky Endpoint Security moves the object to Quarantine. **Remove**. Kaspersky Endpoint Security creates a backup copy of the object, then removes it. **Recommended** (perform recommended action). Kaspersky Endpoint Security 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, Kaspersky Endpoint Security 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. **Skip**. The object will remain intact. Kaspersky Endpoint Security does not attempt to cure or delete the object, but does log information about the object. Default value: **Recommended**.
`SuspiciousSecondAction`	The values are the same as for the SuspiciousFirstAction setting. If Kaspersky Endpoint Security fails to perform the first action, it will perform the second action. 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. If you do not specify a second action, Kaspersky Endpoint Security will use Skip as the second action. Default value: **Skip**.
`UseSizeLimit`	Determines whether or not to apply the SizeLimit setting (which specifies the maximum size of a scanned object). **yes** – use the SizeLimit setting; **no** – do not use the SizeLimit setting. Default value: **no**.
`SizeLimit`	The maximum size of the objects being scanned (in bytes). Kaspersky Endpoint Security skips an object if its size exceeds the specified value.

SETTING	DESCRIPTION AND POSSIBLE VALUES
	This setting is used together with the UseSizeLimit setting. Specify the maximum object size (in bytes). Possible values: 0 – 2147483647 (approximately 2 GB). **0** – Kaspersky Endpoint Security scans objects of any size. Default value: **0**.
`UseTimeLimit`	Determines whether the TimeLimit setting (which specifies the maximum duration of an object scan) applies. **yes** – use the TimeLimit setting; **no** – do not use the TimeLimit setting. Default values: real-time protection task – **yes**; on-demand scan task – **no**.
`TimeLimit`	Maximum object scan time (sec). The Kaspersky Endpoint Security stops scanning an object if it takes longer than the number of seconds specified by this setting value. This setting is used together with the UseTimeLimit setting. Specify the maximum scan duration for an object in seconds. **0** – the object scan duration is unlimited. Default values: real-time protection task – **60**; on-demand scan task – **120**.
`UseExcludeMasks`	Enables / disables exclusion of objects specified by the ExcludeMasks setting. **yes** – exclude objects specified by the ExcludeMasks setting. **no** – do not exclude objects specified by the ExcludeMasks setting. Default value: **no**.

`ExcludeMasks`	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.
	Example:
	`ExcludeMasks=re:.*\.tar\.gz`
	`ExcludeMasks=re:.*\.avi`
	`ExcludeMasks=re:/.*\.avi$`
	`ExcludeMasks=*.doc`
	Default value: not configured.

`UseExcludeThreats`	Enables / disables exclusion of objects containing the threats, specified by the ExcludeThreats setting. **yes** – exclude objects containing the threats, specified by the ExcludeMasks setting. **no** – do not exclude objects containing the threats, specified by the ExcludeMasks setting.

SETTING	DESCRIPTION AND POSSIBLE VALUES
	Default value: **no**.

`ExcludeThreats`	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.
	E.g., you may be using a utility to collect information about your network. Most Kaspersky Endpoint Security programs refer such utility code to the **Riskware** threats type. To keep Kaspersky Endpoint Security from blocking it, add the full name of the threat contained in the application to the list of excluded threats.
	In order to exclude a single object from the scan, specify the full name of the threat in this object - Kaspersky Endpoint Security line with a conclusion that the object is infected or suspicious.
	You can find the full name of the threat detected in an object in the Kaspersky Endpoint Security log.
	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.
	The setting value is case-sensitive.
	Example:
	Perform no actions on files in which Kaspersky Endpoint Security identifies the threats named NetTool.Linux.SynScan.a and Monitor.Linux.Keylogger.a:
	`ExcludeThreats=not-a-virus:NetTool.Linux.SynScan.a`
	`ExcludeThreats=not-a-virus:Monitor.Linux.Keylogger.a`
	You can use shell masks and extended POSIX regular expressions to specify threat names. Add the re: prefix to regular expressions.
	Perform no actions on files in which Kaspersky Endpoint Security identifies any threats for Linux belonging to the not-a-virus category:
	`ExcludeThreats=re:not-a-virus:.*\.Linux\..*`
	Default value: not configured.

`UseAdvancedActions`	Enables / disables actions to be performed on an object, depending on the type of threat found in the object. If you enable the option, Kaspersky Endpoint Security will apply actions which you will specify in the [ScanScope:ScanSettings:AdvancedActions] section instead of actions specified by InfectedFirstAction, InfectedSecondAction, SuspiciousFirstAction and SuspiciousSecondAction settings. Available values: **yes** – perform the action to be performed on objects, depending on the type of threat; **no** – do not perform the action to be performed on objects, depending on the type of threat. Default value: **yes**.
`ReportCleanObjects`	Enables / disables logging of the information about scanned objects, which Kaspersky Endpoint Security recognizes as clean. You can enable the option, for example, to make sure that an object has been scanned by Kaspersky Endpoint Security. 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.

SETTING	DESCRIPTION AND POSSIBLE VALUES
	Available values: **yes** – log information about clean objects; **no** – do not log information about clean objects. Default value: **no**.
`ReportPackedObjects`	Enables / disables logging of the information about scanned objects that make up a part of compound objects. You can enable the option, for example, to make sure that an object within an archive has been scanned by Kaspersky Endpoint Security. 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. Available values: **yes** – log information about objects scanned within archives; **no** – do not log information about objects scanned within archives. Default value: **no**.
`UseAnalyzer`	Enable / disable Heuristic Analyzer. 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. Available values: **yes** – enable Heuristic Analyzer; **no** – disable Heuristic Analyzer. Default value: **yes**.
`HeuristicLevel`	The level of detail of the heuristic analysis. 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. Available values: **Light** – least detailed scan, minimum system load; **Medium** – medium scan, balanced system load; **Deep** – most detailed scan, maximum system load; **Recommended** – recommended value. Default value: **Recommended**.
`[ScanScope:ScanSettings:AdvancedActions]` A response depending on the type of threat. Using the settings in this section, you can customize a particular reaction of Kaspersky Endpoint Security to objects that contain specified threats.	

`Verdict`
`FirstAction`
`SecondAction`
	Prior to specifying the settings in this section, make sure that the UseAdvancedActions setting is active.
	For the threats specified in the Verdict setting, specify two actions (FirstAction and SecondAction). Kaspersky Endpoint Security will attempt to perform these actions on the

SETTING	DESCRIPTION AND POSSIBLE VALUES

	object if it identifies the specified threat in the object.
	If Kaspersky Endpoint Security fails to perform the first action, it will perform the second action.
	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.
	If you do not specify a second action, Kaspersky Endpoint Security will use Skip as the second action.
	See the values for the FirstAction and SecondAction settings in the descriptions of these sections.
	Possible values for the Verdict setting (type of threat) are:
	Virware – viruses and worms;
	Trojware – Trojans;
	Malware – other malicious software;
	Pornware – pornographic software;
	Adware – advertising software;
	Riskware – potentially dangerous software.
	The values of the Verdict setting are case-sensitive.
	For more information on the types of threats, refer to the section "Programs detectable by Kaspersky Endpoint Security" (on page 11).
	Example:
	`UseAdvancedActions=yes`
	`[ScanScope:ScanSettings:AdvancedActions]`
	`Verdict=Adware`
	`FirstAction=Cure`
	`SecondAction=Skip`
	`[ScanScope:ScanSettings:AdvancedActions]`
	`Verdict=Pornware`
	`FirstAction=Cure`
	`SecondAction=Skip`
	Default value: not configured.

`[ExcludedFromScanScope]` Exclusion area.	
`AreaDesc`	Description of the exclusion area, containing additional information about the exclusion area. Example: AreaDesc="Exclude separate SAMBA" Default value: not configured.
`AreaMask`	You can use this setting to limit the exclusion area specified in the [ExcludedFromScanScope:AreaPath] section. Kaspersky Endpoint Security will only exclude those objects that you specify using Shell masks or ECMA-262 regular expressions. Use the **re:** prefix in regular expressions.

Setting	Description and possible values
	`AreaMask=re:.*\.tar\.gz` Default value: not configured.
`UseAccessUser`	This setting enables and disables the use of settings in the [ExcludedFromScanScope:AccessUser] section (exclusion when attempting access using the rights of specified users). The setting of this section is applied only in real-time protection tasks. It is not used for on-demand scan tasks. Possible values include: **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; **no** – exclude objects when they are accessed with any rights. Default value: not configured.
`[ExcludedFromScanScope:AreaPath]` Exclusion area. Path to the excluded directory.	
`Path`	The setting value consists of three elements: **<file system type>:<access protocol>:<path to the excluded directory>**, where: **<file system type>**. Possible values include: **Mounted**. Remote directories mounted on the computer. Using the <access protocol> setting, specify the protocol that provides remote access to the directories. **Shared**. Computer file system resources shared by the SMB/CIFS or NFS protocol. **AllRemotelyMounted**. All remote directories mounted on the computer using SMB/CIFS and NFS protocols. **AllShared**. Computer file system resources shared by the SMB/CIFS and NFS protocols. **<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: **SMB**. The SMB/CIFS protocol. **NFS**. The NFS protocol. **<path to the excluded directory>**. The full path to the excluded directory. Examples: `Path=Mounted:NFS` – *exclude all remote directories mounted using NFS*. Default value: not configured.
`[ExcludedFromScanScope:AccessUser]` Scanning exclusion when attempting access using the rights of specified users. Kaspersky Endpoint Security 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, Kaspersky Endpoint Security excludes objects when they are accessed with any rights. The settings of this section are applied only in real-time protection tasks. They are not used for on-demand scan tasks.	
`UserName`	Kaspersky Endpoint Security excludes objects only if they are accessed by applications running with the permissions of specified users. You can specify several values for this

SETTING	DESCRIPTION AND POSSIBLE VALUES

	setting, for example:
	`UserName=usr1`
	`UserName=usr2`
	Default value: not configured.

`UserGroup`	Group name. Kaspersky Endpoint Security excludes 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:
	`UserGroup=group1`
	`UserGroup=group2`
	Default value: not configured.

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 76) 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 77).

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 Kaspersky Endpoint Security 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 Endpoint Security 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. Specify the directory in which Kaspersky Endpoint Security 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 Endpoint Security .ini configuration files (see page 107).

Table 11. Update tasks settings

SETTING	DESCRIPTION AND POSSIBLE VALUES
`UpdateType`	Specify the function to be performed by the update task: **AllBases**. Update Kaspersky Endpoint Security databases. **RetranslateProductComponents** (Copy all available Kaspersky Endpoint Security updates). Kaspersky Endpoint Security will save the downloaded updates in the directory specified by the RetranslationFolder setting, without installing them. **RetranslateComponentsList** (Copy only specified updates). Kaspersky Endpoint Security will download only the updates whose names have been specified in the settings of the [RetranslateUpdatesSettings] section. It will save the downloaded updates in the directory specified by the RetranslationFolder setting, without installing them. Using the **RetranslateComponentsList** setting you can download updates of 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 Endpoint Security modules are not installed automatically. Default value: **AllBases**.
`[CommonSettings]` Update source and settings used to connect to it.	
`SourceType`	Specify an update source for Kaspersky Endpoint Security: **KLServers**. Kaspersky Endpoint Security will receive updates from one of the Kaspersky Lab update servers. Updates are downloaded via HTTP or FTP protocols. **AKServer**. Kaspersky Endpoint Security will download updates to the protected computer from the Kaspersky Administration Kit Administration Server installed in the LAN. 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. **Custom**. Kaspersky Endpoint Security will download updates from the user-defined source, specified in the [CommonSettings:CustomSources] section. You can specify directories on FTP or HTTP servers or directories on any device mounted on the computer, including directories on remote computers mounted using SMB/CIFS or NFS. Default value: **KLServers**.

SETTING	DESCRIPTION AND POSSIBLE VALUES
`UseKLServersWhenUnavailable`	You can configure the Kaspersky Endpoint Security to access the Kaspersky Lab's update servers if all user-defined sources are unavailable. **yes** – connect to Kaspersky Lab update servers if all user-defined sources are unavailable; **no** – do not connect to Kaspersky Lab update servers if all user-defined sources are unavailable. Default value: **yes**.
`UseProxyForKLServers`	The option to use a proxy server for connection to the update servers of Kaspersky Lab. **yes** – use proxy server to connect to the Kaspersky Lab update servers; **no** – do not use proxy server to connect to the Kaspersky Lab update servers. Default value: **no**.
`UseProxyForCustomSources`	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. **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**.
`ProxyPort`	Proxy server settings: port. Default value: **3128**.
`ProxyServer`	Proxy server settings: network name or IP address. Default value: not configured.
`ProxyBypassLocalAddresses`	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 `ProxyServer` parameter. **yes** – not use proxy server to connect to local update servers; **no** – use proxy server to connect to local update servers. Default value: **yes**.
`ProxyAuthType`	This setting controls authentication when accessing a proxy server being used for connections to FTP or HTTP update source servers. **NotRequired** (no authentication). Select if authentication is not required to access the proxy server. **Plain** (authentication by login name and password, i.e. basic authentication). Specify the user name and password using ProxyAuthUser and ProxyAuthPassword settings. Default value: **NotRequired**.
`ProxyAuthUser`	If you enable authentication, specify the name of the user whose rights will be used by Kaspersky Endpoint Security for proxy server access. Default value: not configured.
`ProxyAuthPassword`	If you enable authentication, specify the password of the user whose rights will be used by Kaspersky Endpoint Security for proxy server access. Default value: not configured.

SETTING	DESCRIPTION AND POSSIBLE VALUES
`UseFtpPassiveMode`	By default, to connect to update servers using FTP, Kaspersky Endpoint Security uses the passive FTP server mode: it is assumed that a network firewall is used in the corporate LAN. Available values: **yes** – use passive FTP server mode; **no** – use active FTP server mode. Default value: **yes**.
`ConnectionTimeout`	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 Endpoint Security will connect to another specified update source, for example, to another Kaspersky Lab update server if you configured updating from Kaspersky Lab update servers. Specify the response wait time in seconds. Only integers within the range from **0** to **120** can be entered as parameter values. Default value: **10**.
`[CommonSettings:CustomSources]` 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 Endpoint Security will always try the next specified source if the previous source is unavailable. You can configure Kaspersky Endpoint Security to access the Kaspersky Lab update servers if all user-defined sources are unavailable using the UseKLServersWhenUnavailable setting.	
`Url`	Specify the user-defined update source: LAN or WAN directory. Example: `Url=`http: //primer.ru/bases/ – the address of HTTP or FTP server on which the directory containing updates is located. `Url= /home/bases/ –` a directory on the protected computer. Default value: not configured.
`Enabled`	Using this setting you can enable or disable the use of the source specified by URL setting in the current section. **yes** – use the update source; **no** – do not use the update source. Default value: not configured.
`[UpdateComponentsSettings]` Updates download.	
`Action`	The setting is mandatory, its value is DownloadAndApply: • Kaspersky Endpoint Security downloads updates if UpdateType is set to RetranslateProductComponents or RetranslateComponentsList; • Kaspersky Endpoint Security downloads and installs updates if UpdateType is set to AllBases. Default value: DownloadAndApply.
`[RetranslateUpdatesSettings]` Downloading updates from the update source without applying them. Specify the settings of this section if you have selected to download updates without applying them: specified the RetranslateComponentsList value for the UpdateType	

SETTING	DESCRIPTION AND POSSIBLE VALUES
setting.	
`RetranslationFolder`	Specify the directory into which Kaspersky Endpoint Security will save the downloaded updates. Default value: not configured.

`RetranslationComponents`	Specify the name of the update you would like to receive if you specified RetranslateComponentsList as your UpdateType setting.
	You can review the names of update on the Kaspersky Lab Technical Support web site.
	Example:
	To copy updates for version 6.0.2.551 of Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition:
	`RetranslationComponents=UPDATER`
	`RetranslationComponents=AVS`
	`RetranslationComponents=BLST`
	`RetranslationComponents=KAV6WSEE`
	`RetranslationComponents=RT`
	`RetranslationComponents=AK6`
	`RetranslationComponents=INDEX60`
	Default value: not configured.

SCHEDULE SETTINGS

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

When specifying the settings, follow the rules for editing Kaspersky Endpoint Security .ini configuration files (see page 107).

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 12. Schedule settings

SETTING	DESCRIPTION AND POSSIBLE VALUES
`RuleType`	The Starting a scheduled task mode. Possible values include: • `Once` – once; • `Monthly` – monthly; • `Weekly` – weekly;

SETTING	DESCRIPTION AND POSSIBLE VALUES
	• `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 Endpoint Security database update (this alternative is not used in update tasks). • `PS` – at application start. The task will be launched at every Kaspersky Endpoint Security startup. 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: • `yes` – run missed tasks the next time the application is started; • `no` – run only scheduled tasks.

Table 13. 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 14. 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 115 th 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:

Start task at startup Kaspersky Endpoint Security:

```
RuleType=PS
```

KASPERSKY ENDPOINT SECURITY GENERAL SETTINGS

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 Endpoint Security .ini configuration files (see page 107).

Once the general settings of Kaspersky Endpoint Security are changed, restart the Kaspersky Lab Framework service using the command `/opt/kaspersky/kes4lwks/bin/kes4lwks-control --restart-app.`

Table 15. Kaspersky Endpoint Security general settings

SETTING	DESCRIPTION AND POSSIBLE VALUES
`StartWithUser`	Account under which Kaspersky Endpoint Security processes are performed. You cannot modify this setting. Default value: **root**.
`StartWithGroup`	Account under which Kaspersky Endpoint Security processes are performed. You cannot modify this setting. Default value: **default**.
`UpdateFolder`	Path to a directory on protected computer containing the updates directories specified by the AVBasesFolderName and AVBasesBackupFolderName settings. Default value: **/var/opt/kaspersky/kes4lwks/update**.
`AVBasesFolderName`	Directory in which Kaspersky Endpoint Security stores database updates. Default value: **avbases**.
`AVBasesBackupFolderName`	Name of the directory which Kaspersky Endpoint Security 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 Kaspersky Endpoint Security 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 computer 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 computer 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 Kaspersky Endpoint Security saves temporary files it creates. If you specify a different directory, make sure that it allows reading and writing for the account under which Kaspersky Endpoint Security runs. Default value: **/var/run/kes4lwks**.
`TraceEnable`	Maintaining a trace log. Kaspersky Endpoint Security records all events into the trace log. Trace log files are stored in the directory specified by the TraceFolder setting. Possible values include: **yes** – maintain a trace log; **no** – do not maintain a trace log. Default value: **yes**.
`TraceFolder`	Directory in which Kaspersky Endpoint Security stores trace log files. If you specify a different directory, make sure that it allows reading and writing for the account under which Kaspersky Endpoint Security runs.

SETTING	DESCRIPTION AND POSSIBLE VALUES
	Default value: **/var/log/kaspersky/kes4lwks**.
`TraceLevel`	Trace log detail level Possible values include: **Fatal**. Critical events. **Error**. Errors. **Warning**. Important events. **Info**. Information events. **Debug**. Debug information. 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. Please note that the trace file can take up a large amount of disk space. If you do not change the log settings when you enable trace log generation, Kaspersky Endpoint Security will trace Kaspersky Endpoint Security subsystems with the **Debug information** level of detail. Default value: **Error**.
`MaxFileNameLength`	The maximum length of the full path to the scanned file, in bytes. 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. Possible values: **4096 – 33554432**. Default value: **16384**.
`BlockFilesGreaterMaxFileName`	Blocks access to files in which the full path name exceeds the **MaxFileNameLength** value. The on-demand scan task skips such files regardless of the **BlockFilesGreaterMaxFileName** value. Possible values include: **yes** – the real-time protection task blocks access to such files; **no** – the access is not blocked. Default value: **yes**.

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 Endpoint Security .ini configuration files (see page 107).

Table 16. Quarantine and backup storage settings

SETTING	DESCRIPTION AND POSSIBLE VALUES
`QuarantineFolder`	Directory containing the quarantined and backed up objects. You can specify a storage directory that is different from the default directory.

SETTING	DESCRIPTION AND POSSIBLE VALUES
	You can use any directory on any computer device as the storage. Specifying directories located on remote computers, for example, those mounted via SMB/CIFS or NFS, is not recommended. Kaspersky Endpoint Security will start to place objects into the directory specified in this setting both after you have imported the file settings into Kaspersky Endpoint Security using the -T --set-settings command, and after Kaspersky Endpoint Security has been stopped and restarted. If the specified directory does not exist or is not accessible, Kaspersky Endpoint Security will start to use the storage directory set by default. Default value: **/var/opt/kaspersky/kes4lwks/quarantine/**.
`QuarantineSizeLimit`	Maximum storage size. The value of this setting specifies the maximum data volume in the storage. Note that after the maximum storage size has been exhausted, Kaspersky Endpoint Security will stop placing objects to quarantine and will stop backing up objects prior to disinfection and deletion. A QuarantineSizeLimitReached event will be logged, indicating that the maximum storage size has been reached. If the value of this setting is set to 0, the maximum storage size is not defined. Specify a value in bytes. Possible values: 0 – 1,8*10^{19} Default value: **1073741824**.
`QuarantineSoftSizeLimit`	Recommended storage size. The value of this setting specifies the recommended general data volume in the storage. This is an information setting. It does not limit the storage size, but allows the administrator to track the status of the storage. After the recommended storage size has been reached, Kaspersky Endpoint Security will continue to place objects in quarantine and will continue to back up objects prior to disinfection and deletion. A QuarantineSoftSizeLimitExceeded event will be logged, indicating that recommended maximum storage size has been reached. If the value of this setting is set to 0, the recommended maximum storage size is not defined. Specify a value in bytes. Possible values: 0 – 1,8*10^{19} Default value: **858993459**.

EVENT LOG SETTINGS

This section describes the settings of the configuration file of Kaspersky Endpoint Security event log.

When modifying the file settings, follow the rules for editing Kaspersky Endpoint Security .ini configuration files (see page 107).

Table 17. Event log settings

SETTING	DESCRIPTION AND POSSIBLE VALUES
`EventStorageFolder`	Event log directory. Kaspersky Endpoint Security saves information about events and service files of its event log to this directory. You can view information about events stored in these files, using the -E --query command (see page 92). You cannot modify this setting. Default value: **/var/opt/kaspersky/kes4lwks/db/event_storage**.
`RotateMethod`	The Kaspersky Endpoint Security rotates events partially deleting (moving) event information from the EventStorageFolder directory. The RotateMethod setting can take the following values: **Erase**. The Kaspersky Endpoint Security 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. **Move**. When the RotatePeriod elapses or when the data volume exceeds the maximum value defined by the EventStorageMaxSize setting, Kaspersky Endpoint Security transfers information about events from the log into the RotateMoveFolder directory and saves it in the rotation file. 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. During each rotation Kaspersky Endpoint Security saves information about events in a separate file. Created files may differ in size if rotation uses both the RotatePeriod and the EventStorageMaxSize settings or if it is performed by the user manually. A single file size may be up to half of the value defined by EventStorageMaxSize or less (deviations range within 100 KB). You can delete the rotation files or create their backup copies on removable media. Default value: **Erase**.

SETTING	DESCRIPTION AND POSSIBLE VALUES
`RotateMoveFolder`	Directory where Kaspersky Endpoint Security moves information about events if the Move method of events rotation has been selected. 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 Endpoint Security does not move information about events deleting it instead from the EventStorageFolder directory. Default value: not configured.
`RotatePeriod`	Rotation interval, it can take the following values: **Daily**. Kaspersky Endpoint Security rotates events every day at 00:00. **Weekly**. Kaspersky Endpoint Security rotates events every Monday at 00:00. **Monthly**. Kaspersky Endpoint Security rotates events on the 1st day of each month at 00:00. **Never**. The interval for events rotation is not defined. Default value: **Never**.
`EventStorageMaxSize`	Maximum size of the events log directory. When information about events in the EventStorageFolder directory exceeds the size defined by the setting, Kaspersky Endpoint Security rotates events. The setting can be used in combination with the RotatePeriod setting to restrict additionally the size of the event log directory. Specify a value in bytes. **0** – maximum size of the events log directory is not defined. Setting the value to zero or too high is not recommended because large data volume in the EventStorageFolder directory can slow down Kaspersky Endpoint Security. Default value: **10485760**.

MANAGING KASPERSKY ENDPOINT SECURITY USING KASPERSKY ADMINISTRATION KIT

If your organization uses Kaspersky Administration Kit for centralized management of the anti-virus applications, you can control Kaspersky Endpoint Security 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 COMPUTER PROTECTION STATUS

The Administration Console lets you view the protection status of a selected computer and the overall computer status from the point of view of anti-virus security and its accessibility.

➡ *To view protection status of a computer:*

1. In the Administration Console tree, expand the **Managed computers** node and select the group to which the protected computer belongs.
2. Right-click the line with the information about the protected computer 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 computer:

Table 18. Information on computer protection status in the dialog box

FIELD	DESCRIPTION
Computer status	Status of the protected computer 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, *Started*, *Stopped*, *Paused*.
Last on-demand scan	Date and time of the last execution of an on-demand scan task.
Viruses found	The total number of malicious programs (names of threats) detected on the protected computer (counter of detected threats) since the moment when Kaspersky Endpoint Security was installed or since the moment the counter was last reset. In order to reset a counter, press the **Reset** button.

THE "APPLICATION SETTINGS" DIALOG BOX

Using the **Application settings** dialog box you can perform remote management of Kaspersky Endpoint Security or configure it on the selected protected computer.

➡ *To open the **Application settings**dialog box, perform the following steps:*

1. In the Administration Console tree expand the **Managed computers** node.
2. Expand the group containing the protected computer and select the **Client computers** node.
3. Right-click the line with the information about the protected computer in the results pane and select the **Properties** command.
4. In the **<Computer name> Properties** dialog box, on the **Applications** tab select **Kaspersky Endpoint Security 8 for Linux** 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 computer on the **Tasks** tab. Group tasks should be created on the selected group's **Group tasks** node, tasks for specific computers should be created on the **Tasks for specific computers** node.

General information about tasks in Kaspersky Administration Kit can be found in *Kaspersky Administration Kit. Administrator Guide*.

CREATING A TASK

When configuring Kaspersky Endpoint Security via 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 138). 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 new task** link in the tasks pane to start the New task wizard. Further information about creating group tasks is available in the Kaspersky Administration Kit manual.

➧ *To create a task for collections of hosts (Kaspersky Administration Kit task):*

1. Open the Administration Console of Kaspersky Administration Kit.
2. Select the required folder: **Tasks for specific computers**, or **Kaspersky Administration Kit tasks**.
3. Click the **Create a new task** link in the tasks pane to start the New task wizard. Further information about creating Kaspersky Administration Kit tasks and tasks for collections of hosts is available in the Kaspersky Administration Kit manual.

THE LOCAL TASK CREATION WIZARD

The Local task creation wizard can be started from the context menu of a managed computer, or in its properties window.

The wizard consists of a series of screens (steps) navigated using buttons **Back** and **Next**; to close the wizard once it completed its work, use the **Finish** button. To cancel the application at any stage, use the **Cancel** button.

STEP 1. ENTERING GENERAL TASK SETTINGS

At the first stage, specify the task name's in the **Name** field.

STEP 2. SELECTING AN APPLICATION AND DEFINING TASK TYPE

During this stage, you should specify the task's type, and which program will perform the task. Kaspersky Endpoint Security 8 for Linux, or Network Agent.

For Kaspersky Endpoint Security 8 the following tasks can be created:

- Virus scan – checks user-defined areas for the presence of viruses.
- Update – downloads and applies a package containing program updates.
- Update roll-back – rolls back the last program update.
- Key file installation – installs a new license key file, required to enable the program's full functionality.

STEP 3. CONFIGURING TASK SETTINGS

The appearance of the wizard's window at this stage will depend on the task type selected during the previous stage.

The following settings are required for an on-demand scan task:

- specify the scan's scope (see page 140) and the scan settings (see page 141);
- specify any excluded areas (see page 141).

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

- specify the source (see page 142) 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 143).

The task to roll-back updates has no specific settings.

The license key file installation task requires a path to the key file.

➨ *To do that, perform the following actions:*

1. Click the **Browse** button in the Task Creation Wizard window.
2. Select the license key file (with a .key extension) which you received when purchasing Kaspersky Endpoint Security.

STEP 4. SCHEDULING THE TASK

Configure the task schedule settings (see section "Scheduling a task" on page 144). You can configure a schedule for all task types except license installation tasks.

STEP 5. COMPLETING THE WIZARD

The last screen of the wizard will inform you that the task creation wizard has completed successfully.

UPDATING TASKS SETTINGS

After you have created a task you can:

- modify the task settings;
- modify the task schedule, enable or disable scheduled task launches.

➡ *To modify the task settings:*

1. In the Administration Console tree expand the **Managed computers** node and select the group to which the protected computer belongs.
2. Right-click the line with the information about the protected computer 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 by Kaspersky Endpoint Security. 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.

   d. In the **Masks** section, click the **Add** button and in the displayed **Object mask** window, define the file name templates, or path templates, for the objects to be scanned.

> You can use Shell masks to specify a file name template to be scanned by Kaspersky Endpoint Security.

> You can also use regular expressions to specify a template for the file path which Kaspersky Endpoint Security should scan. A regular expression cannot contain the name of the folder which defines the scan or protection area.
>
> Add the **re:** prefix to regular expressions.

e. Click **OK** to save the changes.

4. Click the **OK** button in the **Task settings** window to save the changes.

Kaspersky Endpoint Security 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 Endpoint Security 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 files** section, check the boxes beside the types of composite objects (see page 154) which you want Kaspersky Endpoint Security to scan.
4. In the **Scan optimization** section of the **Settings** tab, specify the maximum scanning duration for an individual object (see page 154) and the maximum size of objects to scan (see page 154).
5. Select the **Actions** tab, and specify the operations to be performed on infected objects (see page 151) and on suspicious objects (see page 152).
6. In the **Exclusion area** section, specify objects to be excluded from scanning by name (see page 153) and objects to be excluded from scanning by the name of the detected threat (see page 153).

> 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 Endpoint Security scans all objects within the scan area.

You can define name and path templates that are excluded from the scan area. In this case, Kaspersky Endpoint Security 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 Endpoint Security.

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

➧ *To define an excluded area:*

1. Open the **Task properties** window.
2. Click the **Add** button on the **Exclusion areas** tab.
3. In the **<New exclusion area>** dialog box which will open:
   a. In the **Area name** field, assign a name to the new area. The name will appear in the list of areas for scanning within the **Exclusion areas** window.
   b. Select the resource type in the dropdown list to the left.

      If you selected a **Shared** or **Remote** resource, you must specify in the right dropdown list the protocol used to remotely access to that resource, whether **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

Update source is a resource containing updates for Kaspersky Endpoint Security databases. Update sources can be HTTP or FTP servers, or local or network folders.

The main updates source is Kaspersky Lab's update servers. These are special Internet sites which contain updates for databases and application modules for all Kaspersky Lab products.

➧ *To choose an update source:*

1. Open the **Task properties** window.
2. Use the **Updates sources** tab to select a source of updates (see page 154).
3. Click **OK** to save the changes.

➧ *To add a custom update source:*

1. Open the **Task properties** window.
2. On the **Updates sources** tab, select **Other directories on the local network or the Web**, and click the **Customize** button.
3. In the **Updates sources** window that will open, press the **Add** button and enter either the path to a directory which contains the updates, or the address of a FTP or HTTP update server.
4. Click **OK** to save the changes.

➧ *To configure the connection to an update source:*

1. Open the **Task properties** window.
2. On the **Updates sources** tab, press the **Connection settings** button.
3. Configure the following settings in the window that will open:
   a. FTP server mode (see page 155)
   b. time to wait for a response from the update source while connected to it (see page 155)
   c. proxy server usage (see page 155)
   d. proxy server settings (see page 156)
   e. authentication required to access proxy server (see page 155)
   f. location of the protected computer
4. Click **OK** to save the changes.

SELECTING THE TYPE OF UPDATES

The Kaspersky Endpoint Security update task performs one of the following actions:

1. Downloads and installs databases.
2. Copies the Kaspersky Endpoint Security modules updates. 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 156) 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 156) 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

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 Endpoint Security starts.

➧ *To create a task start rule:*

1. In the Administration Console tree expand the **Managed computers** node.
2. Expand the group containing the protected computer and select the **Client computers** node.
3. Right-click the line with the information about the protected computer 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 144).
7. Click **OK** to save the changes.

SCHEDULING A TASK

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 Endpoint Security using the **Start** command from the context menu or the analogous point in the **Action** menu.
- **After application update** – launch will 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. Detailed information about tasks in Kaspersky Administration Kit can be found in *Kaspersky Administration Kit. Administrator 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**, task will be run once in two days (one 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**, task will be run every Monday in 03:00 PM.

  By default, the **Day of the week** 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**, 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, the 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 computers where Kaspersky Endpoint Security is installed.

A policy applies all specified settings to all protected computers 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 Endpoint Security 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 Endpoint Security does not apply configuration values that you have not set to 🔓 in the policy's properties. When the effect of the policy is terminated, the settings whose values were modified by the policy retain the values they had while the policy was active.

Using policies, you can configure the real-time protection task settings for Kaspersky Endpoint Security.

IN THIS SECTION

CREATING A POLICY

➡ *To create a policy for a group of servers on which Kaspersky Endpoint Security 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 Endpoint Security 8 for Linux** from the drop-down list.

5. In the **Creating a policy** window, select one of the following policy statuses:

   - **Active policy**, if you want the policy to become active immediately upon creation. If an active policy already exists in the group, this policy will become inactive and the policy you are creating will be activated.

   - **Inactive policy**, if you do not want the created policy to be activated immediately. In this case you will be able to activate the policy at a later time.

   In the following policy creation wizard windows, specify the real-time protection task settings and update settings you require.

6. Use the **Protection areas** window to add one or several protection areas and select the interception method (see page 150).

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 Endpoint Security.

➡ *To configure policy settings in the* ***Policy properties*** *dialog box:*

1. In the Administration Console tree, expand the **Managed computers** node, expand the administration group whose policy settings you want to configure, and then expand the included **Policies** node.

2. In the result pane, open the context menu of the policy whose settings you want to configure and select the **Properties** command.

3. In the **<Policy Name> Properties** dialog box configure the required policy settings and click the **OK** button.

CHECKING CONNECTION WITH ADMINISTRATION SERVER MANUALLY. THE KLNAGCHK UTILITY

The Network Agent distribution kit includes the *klnagchk* utility to check the connection with the Administration Server.

Following installation of the Network Agent, the utility is located in the /opt/kaspersky/klnagent/bin directory and, when launched, performs the following actions in accordance with the keys in use:

- outputs to the screen or records in the log file the connection parameters used by the Network Agent installed on the client computer to connect to the Administration Server;
- outputs to the screen or in the log file the statistics about operation of the Network Agent, since its last launch, and the results of this utility operation;
- attempts to connect the Network Agent to the Administration Server;
- if the connection could not be established, sends an ICMP packet to verify the status of the computer on which the Administration Server is installed.

Utility command line syntax:

```
klnagchk [-logfile <file name>] [-sp] [-savecert <path to the certificate file>] [-
restart]
```

The command line parameters are as follows:

- `-logfile <filename>` – log the connection parameters used by Network Agent to connect to the Administration Server and the results of the utility operation. By default the information will be stored in the stdout.tx. file. If the modifier is not used, the parameters, results and error messages will be printed to the screen.
- `-sp` – display the password used to authenticate the user on the proxy server. This parameter is used if connection to the Administration Server is performed using a proxy server.
- `-savecert <filename>` – save the certificate used to access the Administration Server in the specified file.
- `-restart` – restart the Network Agent after the utility has completed.

CONNECTING TO ADMINISTRATION SERVER MANUALLY. THE KLMOVER UTILITY

The Network Agent distribution kit includes the *klmover* utility to manage the connection to the Administration Server.

Following installation of the Network Agent, the utility is located in the /opt/kaspersky/klnagent/bin directory and, when launched, performs the following actions in accordance with the keys in use:

- connects the Network Agent to the Administration Server using the parameters supplied;
- Logs the results of the operation in the events log file, or displays them on the screen.

Utility command line syntax:

```
klmover [-logfile <file name>] {-address <server address>} [-pn <port number>] [-ps
<SSL port number>] [-nossl] [-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 computer.
- `-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.

- `-nossl` – 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

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

Kaspersky Endpoint Security contains two components that intercept attempts to access files and scan them: a SAMBA interceptor (used to scan objects on remote computers when they are accessed via SMB/CIFS) and a kernel level interceptor. It scans objects when they are accessed in some other way.

The SAMBA interceptor provides, as additional object information, the IP address of the remote computer on which an application attempted an object access when it was intercepted by Kaspersky Endpoint Security.

If you use the protected computer only as a SAMBA server, you can set the **SAMBA only** value. In this case, Kaspersky Endpoint Security will not scan objects that are not accessed via SMB/CIFS.

Possible values include:

- **All operations**. Kaspersky Endpoint Security scans computer objects with the SAMBA interceptor when they are accessed via SMB/CIFS. Kaspersky Endpoint Security uses the kernel level interceptor to intercept all other operations on files that are accessible on the protected computer (including files on remote computers).
- **SAMBA only**. Kaspersky Endpoint Security 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 Endpoint Security (see Installation Guide of Kaspersky Endpoint Security 8 for Linux).
- **File system only**. Kaspersky Endpoint Security scans computer objects without using the SAMBA interceptor.

  Make sure that you have specified the kernel interceptor during the initial configuration of Kaspersky Endpoint Security (see Installation Guide of Kaspersky Endpoint Security 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 Endpoint Security scans such objects.

Select one of the protection modes depending on your requirements to the computer security, on which files are stored on the computer, on the format of the files are stored in and on the information they contain:

- **Smart check**. Kaspersky Endpoint Security 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 Endpoint Security scans the object a second time only when the process closes it for the last time.
- **When opened and modified**. Kaspersky Endpoint Security 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 Endpoint Security 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 Endpoint 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 these objects 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 computer'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 Endpoint Security finds an object infected, it performs the action you have selected.

Select one of the following values:

- **Disinfect**. Kaspersky Endpoint Security attempts to disinfect the object, and if disinfection is not possible, it leaves the object intact.
- **Delete**. Kaspersky Endpoint Security deletes the object.
- **Perform recommended action**. Kaspersky Endpoint Security automatically selects and performs the actions on the object based on the data about the threat detected in the object and about the possibility of disinfecting it, for example, Kaspersky Endpoint Security 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. This action can only be specified as the initial action to be taken on infected objects.
- **Skip**. The object remains intact: Kaspersky Endpoint Security does not try to cure 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 Endpoint Security 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 Endpoint Security was not able to disinfect or delete the object will be recorded in the log.

In the list select two actions that Kaspersky Endpoint Security will try to execute on the object. If Kaspersky Endpoint Security fails to perform the first action, it will perform the second action.

During real-time protection, Kaspersky Endpoint Security 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 Endpoint Security 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 Endpoint Security attempts to disinfect the object, and if disinfection is not possible, it leaves the object intact.
- **Delete**. Kaspersky Endpoint Security deletes suspicious object from the computer.

  > Before deleting the object Kaspersky Endpoint Security places a copy of such object into backup storage. Kaspersky Endpoint Security 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 Endpoint Security was not able to remove the object will be recorded in the log.

- **Perform recommended action**. Kaspersky Endpoint Security 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 Endpoint Security does not attempt to disinfect or delete it, but logs relevant information about the object, including what malware it is suspected to contain.

In the list select two actions that Kaspersky Endpoint Security will try to execute on the object. If Kaspersky Endpoint Security fails to perform the first action, it will perform the second action.

> During real-time protection, Kaspersky Endpoint Security blocks access to an object for any application that attempts to access it, before actual operations with that object.

ACTIONS TO BE PERFORMED ON OBJECTS DEPENDING ON THE THREAT TYPE

The **Action to be performed on objects depending on the threat type** security setting is used in the real-time protection and on-demand scan tasks.

Threats of some types (classes) are more dangerous for the computer than others. For example, Trojans can do much more damage than adware. Using this setting, you can configure different actions to be taken by Kaspersky Endpoint Security with objects found to contain specified threats.

If you specify values for this setting, Kaspersky Endpoint Security will use them instead of the values of the Action on infected object setting (see page 151) and the Action on suspicious object setting (see page 152).

For each type of threat, select from the list two actions which Kaspersky Endpoint Security will perform on each object which presents that threat. If Kaspersky Endpoint Security fails to perform the first action, it will perform the second action.

If possible, Kaspersky Endpoint Security 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 Endpoint Security fails to move an object to backup storage or quarantine, it will not take the next step on the object (for example, disinfecting or deleting it). The object will be considered skipped. You can review the reason for skipping the object in the log.

In the list of threat types, the **Network worms** and **Classical viruses** types are combined under the single name of **Viruses**.

EXCLUDING OBJECTS BY NAME

The **Excluding objects by name** security setting is used in real-time protection and on-demand scan tasks.

By default, Kaspersky Endpoint Security 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 Endpoint Security will not scan files or directories from the protection 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 Endpoint Security.

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

Information on an object's exclusion from scanning is saved in the log.

EXCLUDING OBJECTS BY THREAT NAME

The **Excluding objects by threat name** security setting is used in real-time protection and on-demand scan tasks.

If Kaspersky Endpoint Security considers a scanned object to be infected or suspicious, it performs the action on this object specified in the task. If you consider this object to be harmless for the protected computer, you can exclude it from the scan scope by the name of threat detected in it. In this case Kaspersky Endpoint Security 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 Endpoint Security 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 Endpoint Security 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 according to Kaspersky Endpoint Security, 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 Endpoint Security 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 compound objects that Kaspersky Endpoint Security will scan.

Select one or several values:

- **Scan archives**. Kaspersky Endpoint Security scans file archives (including SFX self-extracting archives). Please note that Kaspersky Endpoint Security identifies threats in archives, but does not disinfect them.
- **Scan SFX archives**. Kaspersky Endpoint Security scans self-extracting archives (archives that include a self-extraction module).
- **Scan mail databases**. Kaspersky Endpoint Security scans Microsoft Office Outlook and Microsoft Outlook Express mail database files.
- **Scan packed objects**. Kaspersky Endpoint Security 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 Endpoint Security 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 Endpoint Security 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 Endpoint Security 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 Endpoint Security 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 Endpoint Security 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 Endpoint Security will download updates to the protected computer from the Kaspersky Administration Kit Administration Server installed in the LAN.

- **Other directories on the local network or the Web**. Kaspersky Endpoint Security 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 computer, including directories on remote computers mounted using SMB/CIFS or NFS protocols.

You can specify one or several user-defined update sources. Kaspersky Endpoint Security will always try the next specified source if the previous source is unavailable.

You can change the order in which Kaspersky Endpoint Security polls custom sources, and also configure it to connect to selected sources on the list only.

You can configure the Kaspersky Endpoint Security to access the Kaspersky Lab's 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, Kaspersky Endpoint Security uses the passive FTP server mode: it is assumed that a network firewall is used in the corporate 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 Endpoint Security 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 Endpoint Security accesses a proxy server when connecting to Kaspersky Lab's update servers.
- Kaspersky Endpoint Security 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 computer.

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 Endpoint Security will download and install database updates.
- **Copy all updates available for the application**. Select this value to download and save all accessible Kaspersky Endpoint Security updates in a directory without applying them.
- **Copy updates for selected modules**. Select this option to download selected updates only. Kaspersky Endpoint Security will save 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 Endpoint Security 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 flagship product, Kaspersky Anti-Virus, reliably protects all types of computer systems against virus attacks, including workstations, file servers, mail systems, firewalls, Internet gateways and hand-held computers. Its easy-to-use management tools maximize the automation of anti-virus protection for computers and corporate networks. A large number of developers worldwide use the Kaspersky Anti-Virus kernel in their products, including Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India), and BorderWare (Canada).

Kaspersky Lab customers benefit from a wide range of additional services that ensure both stable operation of the company's products, and compliance with specific business requirements. We design, implement and support corporate anti-virus systems. Kaspersky Lab's anti-virus database is updated every hour. The company provides its customers with technical support service in several languages.

If you have any questions, please refer them to one of our distributors or directly to Kaspersky Lab ZAO. We will be glad to assist you, via phone or email, in any matters related to our products. You will receive full and comprehensive answers to all your questions.

Kaspersky Lab official site:	http://www.kaspersky.com
Virus Encyclopedia:	http://www.securelist.com
Anti-virus laboratory:	newvirus@kaspersky.com
	(only for sending archives of suspicious objects)
	http://support.kaspersky.ru/helpdesk.html?LANG=en
	(for queries to virus analysts)

INFORMATION ABOUT THIRD-PARTY CODE

Information about third-party code is contained in the file legal_notices.txt, in the application installation folder.