Kaspersky Endpoint Security 8 for Linux

INSTALLATION GUIDE

APPLICATION VERSION: 8.0

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.

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: 5/11/11

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

CONTENTS

INTRODUCTION

This Guide contains a description of the installation procedure for Kaspersky Endpoint Security 8 for Linux (hereinafter referred to as the *Kaspersky Endpoint Security* or *application*).

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

IN THIS SECTION

APPLICATION PURPOSE

Kaspersky Endpoint Security 8 for Linux is intended to provide anti-virus protection for workstations that run under Linux operating systems.

Kaspersky Endpoint Security allows to:

- provide real-time file system protection against malicious code, i.e. intercept file access requests, analyze them, and disinfect or delete infected objects;
- scan workstation objects on demand, i.e. search for infected and suspicious files in specified scan areas, analyze them, and disinfect or delete infected objects;
- quarantine infected and suspicious objects;
- create copies of infected objects in backup storage before disinfection or deletion, so as to be able to recover objects that contain valuable information;
- update application databases using Kaspersky Lab update servers or Administration Server; also, Kaspersky Endpoint Security can be configured to update the databases from a local directory;
- manage the application and configure it using the management utility, Kaspersky Administration Kit.

HARDWARE AND SOFTWARE SYSTEM REQUIREMENTS

In order to ensure Kaspersky Endpoint Security runs correctly, the system must meet the following hardware and software requirements:

- Minimum hardware requirements:
  - processor Intel Pentium® II 400 MHz or higher;
  - 512 MB RAM;
  - at least 1 GB available for swap;

        - 2 GB available on the hard drive to install Kaspersky Endpoint Security and store temporary and log files.

- Software requirements:
    - One of the following 32-bit operating systems:
        - Red Hat Enterprise Linux 5.5 Desktop;
        - Fedora 13;
        - CentOS-5.5;
        - SUSE Linux Enterprise Desktop 10 SP3;
        - SUSE Linux Enterprise Desktop 11 SP1;
        - openSUSE Linux 11.3;
        - Mandriva Linux 2010 Spring;
        - Ubuntu 10.04 LTS Desktop Edition;
        - Debian GNU/Linux 5.0.5.
    - One of the following 64-bit operating systems:
        - Red Hat Enterprise Linux 5.5 Desktop;
        - Fedora 13;
        - CentOS-5.5;
        - SUSE Linux Enterprise Desktop 10 SP3;
        - SUSE Linux Enterprise Desktop 11 SP1;
        - openSUSE Linux 11.3;
        - Ubuntu 10.04 LTS Desktop Edition;
        - Debian GNU/Linux 5.0.5.
    - Perl interpreter: version 5.0 or higher, see http://www.perl.org
    - Installed packages to compile programs (gcc, binutils, glibc (64-bit operating systems require the 32-bit version of glibc), glibc-devel, make, ld), as well as the installed source code of the operating system kernel to compile Kaspersky Endpoint Security modules.

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.

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

Email request to the Technical Support Service

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

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

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

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

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

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

- **Request type**. Select the topic, which is the closest to the problem you have encountered, e.g.: "Product installation / removal problem", or "Virus scan / removal problem".
- **Kaspersky Endpoint Security version name and number**.
- **Request text**. Describe in detail the problem encountered.
- **Customer ID and password**. Enter the customer ID and password received during registration at the Technical Support Service website.
- **Email address**. The experts of the Technical Support Service will send their reply to your inquiry to that address.

Technical support by phone

If an urgent problem has occurred, you can always call the Technical Support Service in your city. When you apply to Russian-speaking (http://support.kaspersky.ru/support/support_local) or international (http://support.kaspersky.com/support/international) Technical Support specialists, please remember to provide the

Kaspersky Endpoint Security information (http://support.kaspersky.com/support/details), so that our specialists could help you as soon as possible.

DISCUSSION OF KASPERSKY LAB'S APPLICATIONS IN WEB FORUM

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

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

WHAT'S NEW IN VERSION 8

Let's take a closer look at the new features in Kaspersky Endpoint Security 8 for Linux.

New protection features:

- Kaspersky Endpoint Security 8 for Linux combines the capabilities of previous application versions, i.e. Kaspersky Anti-Virus 5.7 for Linux Workstations and Kaspersky Anti-Virus 5.5 for Samba Servers, by using two types of file operation interception: a kernel level (kernel module) interceptor and a Samba interceptor;
- Quarantine / backup storage administrative capabilities have been expanded, which allow:
  - add objects to quarantine manually;
  - search for quarantined objects (by object attributes);
  - delete found objects;
  - restore found objects;
  - rescan objects;
  - save part of the quarantine / backup storage in an archive (to reduce the amount of used disk space);
  - import objects from the archive into the quarantine / backup storage.

New features to manage the operation of Kaspersky Endpoint Security:

- Centralized management of the Kaspersky Endpoint Security life cycle and performance of on-demand scan, real-time protection, and Kaspersky Endpoint Security database update tasks.
- Centralized storage of Kaspersky Endpoint Security operation settings.
- Kaspersky Endpoint Security operation settings are no longer stored in text configuration files. Text files are used only for importing and exporting settings from the central repository of settings.
- Multiple scan areas may be specified in a single task, which enables the user to:
  - specify scan settings for each area individually;
  - specify scan areas by:
    - full path within file system;
    - device name;
    - network access type (Shared, Mounted);

        - network access protocol (SMB / CIFS, NFS);
        - network resource name (Samba share name, NFS shared folder);
    - the scan area description supports ECMA-262 regular expressions;
- a list of users / groups, whose file operations the real-time protection task will scan, may be defined for the scan area.
- Multiple exclusion rules may be specified for a single scan area.
- Remote management via Kaspersky Administration Kit is available.
- You can manage the computer using the local management interface where you can perform the following actions:
    - view computer protection status with installed Kaspersky Endpoint Security;
    - start and manage computer scan and database update tasks;
    - view statistics for on-demand scan and real-time protection tasks;
    - view events in the events log.
- Actions to perform on objects may be specified based on the type of detected threat.
- A schedule for starting / stopping tasks may be configured in detail.

New in Kaspersky Endpoint Security monitoring, reporting, and operation statistics:

- The following Kaspersky Endpoint Security monitoring features have been expanded:
    - tools for obtaining the following categories of information:
        - general information about the application;
        - information about the Kaspersky Endpoint Security databases version;
        - information about the license state;
        - information about the status of Kaspersky Endpoint Security components;
        - information about tasks results;
        - information about the state of the quarantine / backup storage;
    - tools for retrospective analysis of Kaspersky Endpoint Security operation that enable you to:
        - collect, process, and store the statistics on Kaspersky Endpoint Security operation;
        - display the Kaspersky Endpoint Security operation statistics collected over a user-specified period of time;
        - search the events based on criteria specified by the user;
        - audit the following aspects of application operation: creating / starting / stopping Kaspersky Endpoint Security tasks, modifying Kaspersky Endpoint Security settings, user actions on objects in the quarantine and backup storage, etc.;
    - tools for creating reports on Kaspersky Endpoint Security operation, based on collected statistics, and tools for exporting reports (HTML, CSV formats are supported);
    - monitoring Kaspersky Endpoint Security operation and virus activity. Information is located in a centralized repository of Kaspersky Endpoint Security events. Kaspersky Endpoint Security provides its own tools for searching, displaying, and analyzing data on its operation, as well as the capability of using external resources.

DISTRIBUTION CONTENTS

The contents of the Kaspersky Endpoint Security distribution are shown in the table below.

Table 1. Kaspersky Endpoint Security packages

PACKAGE	**PURPOSE**
kes4lwks-<version_number>.i386.rpm **kes4lwks_<version_number>_i386.deb**	Contains the main Kaspersky Endpoint Security files. This package can be installed both on 32-bit and 64-bit operating systems.
klnagent-<version_number>.i386.rpm **klnagent_<version_number>_i386.deb**	Contains the Network Agent (a utility that connects Kaspersky Endpoint Security with Kaspersky Administration Kit).
kes4lwks-rpm.tar.gz **kes4lwks-deb.tar.gz**	Contains the files kes4lwks.kpd and akinstall.sh used in the remote installation procedure for Kaspersky Endpoint Security using Kaspersky Administration Kit.
klnagent-rpm.tar.gz **klnagent-deb.tar.gz**	Contains the files klnagent.kpd and akinstall.sh used in the remote installation procedure for Administration Console using Kaspersky Administration Kit.

INSTALLING KASPERSKY ENDPOINT SECURITY

Kaspersky Endpoint Security is distributed in packages in *.deb* and *.rpm* formats.

The installation process includes several steps:

1. Installing the Kaspersky Endpoint Security package.
2. Installation of the Network Agent package (installation of this package is necessary to manage Kaspersky Endpoint Security using Kaspersky Administration Kit).

IN THIS SECTION

STEP 1. INSTALLING THE KASPERSKY ENDPOINT SECURITY PACKAGE

Before you install Kaspersky Endpoint Security 8 for Linux, remove Kaspersky Anti-Virus 5.5 for Samba Servers or Kaspersky Anti-Virus 5.7 for Linux Workstations, installed on the computer.

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

Before installing Kaspersky Endpoint Security, you need to install the glibc package (64-bit operating systems require the 32-bit version of glibc).

➡ *To install Kaspersky Endpoint Security from .rpm-package, execute the following command:*

```
# rpm -i kes4lwks-<version_number>.i386.rpm
```

➡ *To install Kaspersky Endpoint Security from .deb-package, execute the following command:*

```
# dpkg -i kes4lwks_<version_number>_i386.deb
```

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

```
# dpkg -i --force-architecture kes4lwks_<version_number>_i386.deb
```

After entering the command, the installation will be performed automatically.

After the Kaspersky Endpoint Security installations from the .rpm-package is completed, run the post-installation script (see section "Kaspersky Endpoint Security initial configuration" on page 22).

STEP 2. INSTALLING NETWORK AGENT

Installation of Network Agent is required if you plan to manage Kaspersky Endpoint Security using Kaspersky Administration Kit.

You must have **root** privileges to initiate installation of Network Agent.

➧ *To install Network Agent installed from an .rpm-package, execute the following command:*

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

➧ *To install Network Agent installed from a .deb-package, execute the following command:*

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

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

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

After entering the command, the installation will be performed automatically.

Post-installation Network Agent configuration script should be started after Network Agent has been installed from .rpm-package.

INSTALLING KASPERSKY ENDPOINT SECURITY REMOTELY

You can install Kaspersky Endpoint Security remotely via the Administration Console in Kaspersky Administration Kit. To install Kaspersky Endpoint Security remotely, create a remote installation task (see section "Creating a deployment task" on page 14) for a cluster of computers.

The application is installed using the *push install* method (see Kaspersky Administration Kit 8.0 Implementation Guide). Push install allows you to remotely install applications on specific client computers of a logical network. While starting the task, the Administration Server copies installation files from the shared folder to a temporary folder on each client computer, and runs the setup program on these computers.

Network Agent is a component that provides for Administration Console connection with client computers. Therefore, it should be installed and configured properly. To successfully complete the remote installation, the Network Agent must be started on a protected computer.

Installation packages (see section "Creating an installation package" on page 18) are used to create an installation package. An installation package is a set of files required to install the application and contains settings for both the installation and the initial set-up process (see page 22). The installation package can be created before or during the creation of the remote installation task. The same installation package can be reused many times.

Please note that for the operating system that use dpkg the installation package must be based on the deb-package, while operating systems using RPM must be based on the .rpm-package.

All the installation packages created for an Administration Server are located in the **Repositories** → **Installation packages** folder of the console tree.

IN THIS SECTION

CREATING A DEPLOYMENT TASK

➡ *To create a deployment task for selected computers using push install:*

1. Connect to the necessary Administration Server.
2. Select the **Tasks for specific computers** folder in the console tree.
3. Open the context menu and select **Create** → **Task** or the analogous point in the **Action** menu.

This will launch the Task Creation Wizard. Follow the wizard's instructions.

THE WIZARD'S STEPS

STEP 1. DEFINING THE TASK NAME

Enter the task name in the **Name** field.

STEP 2. SELECTING THE TASK TYPE

In the **Kaspersky Administration Kit** node select the **Application deployment** task type.

STEP 3. SELECTING THE INSTALLATION PACKAGE

Specify the installation package that will be installed when the task is performed. Select the necessary package from the list of packages created for the Administration Server or use the **New** button to create a new installation package. New installation packages are created (see section "Creating an installation package" on page 18) using the Installation Package Creation Wizard.

STEP 4. SELECTING THE REMOTE INSTALLATION METHOD.

Select the **Push install** option.

STEP 5. DEFINING THE TASK SETTINGS

At this step you are asked to specify whether the application needs to be re-installed if it is already installed on the client computer. Check the **Do not install application if it is already installed** box, if you do not want the application to be re-installed on the computer (by default, the box is checked).

STEP 6. SELECTING THE INSTALLATION PACKAGE FOR JOINT DEPLOYMENT

If you wish to install the Administration Console together with the application, enable the option to **Install Administration Agent along with this application**, and then select the required installation package.

➧ *To create a new Network Agent installation package,*

in the task creation wizard's window, click the **Create** button.

This will start the New Package Wizard (see section "Creating an installation package" on page 18). Follow the wizard's instructions.

STEP 7. CONFIGURING THE RESTART SETTINGS

Define the operations that should be performed if computer restart is required after application setup. The following options are available:

- **Do not restart the computer**;
- **Restart the computer** – if you select this option, the operating system will only be restarted if necessary;
- **Ask the user** – if you select this option, you will need to configure the settings for notifying the user of a computer restart.

Select the option **Do not restart computer**.

STEP 8. DEFINING THE METHOD FOR SELECTING COMPUTERS

Define the method for selecting computers for which a task has been created:

- **I want to select computers using Windows Networking** – in this case the computers for deployment will be selected using the data collected by the Administration Server while polling the corporate network;
- **I want to select computers using addresses (IP address, NetBIOS or DNS name) input manually** – in this case the name or IP addresses of the client computers must be selected or input manually.

STEP 9. SELECTING THE CLIENT COMPUTERS

If the computers are selected using data collected while polling the network, a list is generated in the wizard window. To make a selection, check the boxes by the names of the client computers from the administration groups (the **Controllable computers** node) and the computers not included in the groups (the **Undistributed computers** node).

If computers are selected manually, then the list of addresses is generated by entering the NetBIOS or DNS names, or IP addresses (or a range of IP addresses) of the computers, or by importing the list from a text file in which every address must be specified in a new line. Generate the list of addresses by clicking the **Add**, **Delete** or **Add IP range** buttons, or import the list from a txt file by clicking the **Import** button. An IP address (or range of IP addresses), or a NetBIOS or DNS name can be used as the address of a computer. To import the list from a file, you need to specify the text file with a list of addresses of computers to be added.

STEP 10. SPECIFYING THE USER ACCOUNT FOR RUNNING TASKS

Since files are copied to the client computers by the Administration Console, you do not need to add a user account. Administration Console performs all operations to copy and install files using the **Local system** account rights.

STEP 11. SCHEDULING THE TASK LAUNCH

Create the task launch schedule.

- In the **Scheduled start** drop-down list, select the necessary mode for task launch:
  - **Manually**;
  - **Every N hours**;
  - **Daily**;
  - **Weekly**;
  - **Monthly**;
  - **Once** – in this case the deployment task will be started on computers only once, irrespective of its results;
  - **Immediately** – start the task immediately after the wizard finishes;
  - **On completing another task** – in this case the deployment task will only be started after completion of the specified task.
- Configure the schedule settings in the group of fields that corresponds to the selected mode.
- Configure additional task start settings (they depend upon the selected scheduling mode). To do that, perform the following actions:
  - 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.
  - Check the **Run missed tasks** box to make 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**, **Once**, or **Immediately**.
  - If this box is not checked, only scheduled tasks will be started on the client computers, and for **Manually**, **Once**, and **Immediately** – on hosts visible on the network only. By default, the box is unchecked.

STEP 12. COMPLETING TASK CREATION

When the wizard is complete, the task you created will be added to the **Tasks for specific computers** folder in the console tree and displayed in the results pane. If necessary, you can modify its settings (see page 18).

STARTING A REMOTE INSTALLATION TASK

➧ *To start a remote installation task manually for a cluster of computers, do the following:*

1. Connect to the necessary Administration Server.
2. Select the **Tasks for specific computers** folder in the console tree.
3. In the results pane, select the required task in the list.
4. Open the context menu and select **Start** or the analogous point in the **Action** menu.

VIEWING AND CONFIGURING THE REMOTE INSTALLATION PACKAGE SETTINGS

➧ *To view the properties of the remote installation task and modify its settings, do the following:*

1. Select the **Tasks for specific computers** folder in the console tree.
2. In the results pane, select the required task in the list.
3. Open the context menu and select **Properties** or the analogous point in the **Action** menu.

This opens the **Properties <Name of task>** window that consists of the **General**, **Notification**, **Client computers**, **Schedule**, **Settings**, **Account** and **Restart OS** tabs.

Remote installation tasks are configured in the same way as the properties of any of the tasks. Let us examine closely the settings specific for this task type on the **Settings** tab. On this tab you can define:

- the method for delivery of the files necessary for application setup to client computers and specify the maximum number of simultaneous connections;
- the number of installation attempts when a task is started according to the schedule;
- whether or not to reinstall the application if it is already installed on the client computer;
- whether running applications should be closed before the installation starts;
- whether the operating system version should be checked for compliance with the hardware requirements before application installation.

CREATING AN INSTALLATION PACKAGE

Before creating an installation package, you need to make a Kaspersky Endpoint Security distribution disk.

➧ *To make a Kaspersky Endpoint Security distribution disk, do the following:*

1. Unpack the kes4lwks-rpm.tar.gz or kes4lwks-deb.tar.gz archive (depending on the package manager used in the operating system of the protected computer) in a folder accessible to Administration Server in Kaspersky Administration Kit.
2. Copy the kes4lwks-<version_number>.i386.rpm or kes4lwks_<version_number>_i386.deb package to the same folder (depending on the package manager used in the operating system of the protected computer).

➧ *To create an installation package, do the following:*

1. Connect to the necessary Administration Server.
2. Select the **Repositories** → **Installation packages** folder in the console tree.
3. Open the context menu and select **Create** → **Installation package** or the analogous point in the **Action** menu.

This opens the Installation Package Creation Wizard. Follow the wizard's instructions.

THE WIZARD'S STEPS

STEP 1. DEFINING THE INSTALLATION PACKAGE NAME

Enter the name of the installation package in the **Name** field.

STEP 2. SELECTING THE APPLICATION DISTRIBUTION PACKAGE

At this step you are asked to specify the application to be installed.

In the dropdown list select the option: **Create installation package for Kaspersky Lab application**. Click the **Select** button and select the file with the .kpd extension. The application name and version number fields will be populated automatically.

Installation package settings are generated by default depending on the application to install. You can modify them (see page 20) after creating a package in its properties window.

STEP 3. LOADING THE INSTALLATION PACKAGE

To load the newly generated installation package to the Administration Server, click the **Next** button.

STEP 4. CONFIGURING THE REAL-TIME PROTECTION TASK

At this step you have the option to compile the kernel module of the operating system. This compiles the kernel module necessary for operation of the real-time protection task. The following options are available:

- **Do not compile real-time protection module**;
- **Compile module, search for the kernel source codes automatically** – if this option is selected, the kernel source codes will be found automatically;
- **Compile module, specify path to the kernel source code** – if this option is selected, you need to manually specify the full path to the source codes of the operating system (for example, */lib/modules/2.6.27.39-0.2-default*). Click the **Additional** button to specify the full path to the kernel source codes.

At this step you are asked to define the settings for integration with the Samba server. The following options are available:

- **Do not install Samba interceptor**;
- **Automatic integration with Samba-server** – if this option is selected, Kaspersky Endpoint Security will be automatically integrated with the Samba server;

- **Integrate with Samba-server, specify settings manually** – if this option is selected, you need to manually specify the settings for integration with the Samba server. Click the **Additional** button to specify the following settings for integration with the Samba server:
  - full path to the configuration file of the Samba server (for example, */etc/samba/smb.conf*);
  - directory for the Samba VFS modules (for example, */usr/lib/samba/vfs*);
  - name of the VFS module being installed (for example, */opt/kaspersky/kes4lwks/lib/samba/kes4lwks-smb-vfs21.so*).

Select the **Start real-time protection task after setup** checkbox if you want the task to run immediately after installation.

STEP 5. CONFIGURING UPDATE TASK SETTINGS

At this step you are asked to specify the task update settings. The following update sources are available:

- **Do not change**;
- **Kaspersky Administration Server**;
- **Kaspersky Lab's update servers**;
- **Other update sources**.

  If you have selected this option, click the **Additional** button to configure the user update source. Update sources can be HTTP or FTP servers, or local or network folders.

Select the **Start update immediately after installation** checkbox if you want the update task to run immediately after installation.

STEP 6. COMPLETING CREATION OF AN INSTALLATION PACKAGE

As a result, the installation package will be created; it will appear in the results pane of the **Repositories** → **Installation packages** folder. You can modify the installation package settings in its properties window.

VIEWING AND CONFIGURING THE PROPERTIES OF AN INSTALLATION PACKAGE

➧ *To view the installation package settings and modify the settings, do the following:*

1. Select the **Repositories** → **Installation packages** folder in the console tree.
2. In the results pane select the required installation package.
3. Open the context menu and select **Properties** or the analogous point in the **Action** menu.
4. This opens the **Properties <Name of installation package>** window that consists of the **General**, **Real-time protection**, **Update** and **License** tabs.

The **General** tab contains general information about the package. It includes the following data:

- Installation package name (you can modify it).
- Name and version of the application for which the package has been created.

- Package size.
- Creation date.
- Path to the installation package folder.

The **Real-time protection** tab contains real-time task settings: settings for the compilation of the kernel module of the operating system required to run the real-time protection task, and settings for integration with the Samba server. These settings are configured at the stage of generating an installation package (see section "Creating an installation package" on page 18). If required, they can be changed.

The **Update** tab contains update task settings: the selection of update source and user update source configuration. These settings are configured at the stage of generating an installation package (see section "Creating an installation package" on page 18). If required, they can be changed.

The **License** tab contains information about the application license for which the installation package has been generated. On this tab you can add or modify the key file.

KASPERSKY ENDPOINT SECURITY INITIAL CONFIGURATION

After Kaspersky Endpoint Security has been installed on the computer, you will need to configure Kaspersky Endpoint Security initial settings.

If Kaspersky Endpoint Security initial configuration has not been performed, the computer's anti-virus protection will not work.

Initial configuration consists of a series of steps that are implemented as a script, for the user's convenience. The initial configuration script is executed automatically upon completion of application installation on the computer. If the package manager used by the operating system does not support interactive scripts, the initial configuration script will have to be invoked manually.

Real-time protection task is started upon completion of the initial configuration process. A necessary condition for this is the completion of the following actions:

- installing the key file;
- downloading Kaspersky Endpoint Security database updates;
- compiling the kernel modules.

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

for Linux:

```
# /opt/kaspersky/kes4lwks/bin/kes4lwks-setup.pl
```

You can perform the actions required to start a real-time protection task using Kaspersky Endpoint Security management tools. For detailed information, please refer to Kaspersky Endpoint Security 8 for Linux Administrator's Guide.

IN THIS SECTION

STEP 1. REVIEWING THE LICENSE AGREEMENT

In this step, you must either agree or decline the terms of the License Agreement.

You can review the text of the agreement using the *less* utility. To move through the text, use the cursor control key or the **b** and **f** keys (to move backward or forward one screen, respectively). To obtain help, use the **h** key. To finish your review, use the **q** key.

After exiting the viewing mode, enter **yes** (or **y**) to agree with the license agreement terms and conditions. If you do not agree with the license agreement terms, enter **no** (or **n**).

If you do not agree with the terms and conditions of the license agreement, Kaspersky Endpoint Security configuration will terminate.

STEP 2. SELECTING THE LOCALE

At this stage you need to specify the locale that will be used by Kaspersky Endpoint Security.

The locale is set in the format specified in RFC 3066.

➡ *To obtain a full list of locale values, use the following command:*

```
# locale -a
```

The default locale is **en_US.utf8**.

STEP 3. INSTALLING THE KEY FILE

In this step, you must install a key file. The key file contains information that is used to verify the right to use Kaspersky Endpoint Security and defines the period of its use.

➡ *To install a key file,*

indicate the complete path to the key file or the path to the directory that contains key files.

If the specified directory contains several key files, the application will install the first file suitable for Kaspersky Endpoint Security 8 for Linux.

If no license has been installed, the Kaspersky Endpoint Security will not provide computer anti-virus protection.

You can install a key file without using the initial configuration script. To obtain information on key file installation, please refer to the "Managing licenses" section in Kaspersky Endpoint Security 8 for Linux Administrator's Guide.

STEP 4. CONFIGURING PROXY SERVER SETTINGS

In this step, configure the proxy server settings. This is necessary if a proxy server is used to connect to the Internet. An Internet connection is required to download Kaspersky Endpoint Security databases from update servers.

➡ *To configure the proxy server, perform the following steps:*

- If you use a proxy server to connect to the Internet, specify the address of the proxy server using one:
  - `proxy_server_IP:port_number`, if no authentication is required to connect to the proxy server;
  - `user_name:password@proxy_server_IP:port_number`, if authentication is required to connect to the proxy server.
- If you do not use a proxy server to connect to the Internet, respond **no**.

The default answer is **no**.

You can configure the proxy server settings without using the initial configuration script. To obtain information on setting up a proxy server, please refer to the "Updating Kaspersky Endpoint Security" section in Kaspersky Endpoint Security 8 for Linux Administrator's Guide.

STEP 5. DOWNLOADING KASPERSKY ENDPOINT SECURITY DATABASE UPDATES

In this step, you will be asked to upload Kaspersky Endpoint Security databases to the computer. Computer data is protected using databases that contain descriptions of threat signatures and methods of countering them. Kaspersky Endpoint Security uses these to scan and disinfect dangerous objects. The databases are added to every hour with records of new threats.

➡ *To upload Kaspersky Endpoint Security to the computer,*

respond **yes**.

If you don't want to download databases now, respond **no**.

The default answer is **yes**.

If Kaspersky Endpoint Security databases have not been uploaded, Kaspersky Endpoint Security will not provide anti-virus protection of the computer.

You can start Kaspersky Endpoint Security databases update without using the script. To obtain information on starting database updates, please refer to the "Updating Kaspersky Endpoint Security" section in Kaspersky Endpoint Security 8 for Linux Administrator's Guide.

Step 6. Enabling automatic database updates

In this step, you will be asked to enable or disable automatic updating of Kaspersky Endpoint Security databases.

➡ *To enable automatic databases updates,*

enter **yes**.

By default, updating of Kaspersky Endpoint Security databases is scheduled to run every 30 minutes.

You can enable the automatic Kaspersky Endpoint Security database updates without using the initial configuration script. To obtain information on setting up the Kaspersky Endpoint Security database update schedule, please refer to the "Modifying task schedule settings. -T --set-schedule" and "Schedule settings" sections in Kaspersky Endpoint Security 8 for Linux Administrator Guide.

Step 7. Compiling the kernel module

In this step, you will be asked to initiate compilation of the kernel module. This compiles the kernel module necessary for operation of the real-time protection task.

If the script finds the operating system's kernel source code in the default directory, the found path will be used by default. Otherwise, you will be asked to enter the path to the kernel source codes.

You can perform compilation of the kernel module, without repeating the previous script steps.

➡ *To perform compilation of the kernel module, without running the initial configuration, execute the following command:*

```
# /opt/kaspersky/kes4lwks/bin/kes4lwks-setup.pl \

--build=<path to the kernel source codes>
```

If compilation of the kernel module was not performed, the real-time protection task will not scan operations on local or mounted objects of the computer's system file.

Step 8. Integrating with Samba server

Integration with the Samba server is performed during this step. The procedure involves the following actions:

- a search is performed for an installed Samba server and its version is checked to make sure it suits the software requirements;
- the Samba server configuration file is found and modified;
- the Samba server configuration file is checked for VFS modules.

If VFS modules are specified in the Samba server configuration file at the time of Kaspersky Endpoint Security installation, these modules will be disabled.

The initial configuration script searches for installed Samba servers. Afterward, you will be asked to configure protection for the found servers either automatically or manually. Enter **Y** to automatically configure protection for a Samba server. This is the default mode. Enter **N** if an incorrect Samba server was found, or if you want to configure protection for the Samba server manually.

➧ *To configure Samba server protection manually, perform the following steps:*

If you enter a blank line in response to the initial configuration script prompt, the process for configuring the protection of Samba server will be paused.

1. Specify the path to the directory containing the *smbd* file.
2. Specify the path to the directory containing the Samba server configuration file (*smb.conf*).
3. Specify the path to the directory containing the VFS modules for the Samba server.

Upon completion of integration, the Samba server service must be restarted manually.

If the real-time protection task is stopped after the integration with the Samba server has been completed, access to the Samba resources will be blocked.

➧ *To avoid having access to Samba resources blocked after stopping the real-time protection task,*

add the following line to the `[global]` section of the */etc/samba/smb.conf* configuration file:

```
kavsamba:access_on_error = yes
```

You can perform integration with the Samba server, without repeating the previous script steps.

➧ *To perform integration with the Samba server, without running the initial configuration, execute the following command:*

```
# /opt/kaspersky/kes4lwks/bin/kes4lwks-setup.pl --samba
```

STEP 9. STARTING GRAPHICAL INTERFACE AUTOMATICALLY

On this stage, specify whether you want to start graphical interface automatically at system startup.

➧ *To start graphical interface automatically at system startup,*

respond **yes**.

If you do not want to start graphical interface automatically at system startup, enter **no**.

The default answer is **yes**.

STEP 10. STARTING THE REAL-TIME PROTECTION TASK

In this step, a real-time protection task is started if the following actions have been performed:

- the license has been installed;
- Kaspersky Endpoint Security database updates have been downloaded;
- compiling the kernel modules or integration with the Samba server.

To obtain information on task management, please refer to the "Managing tasks" section in Kaspersky Endpoint Security 8 for Linux Administrator's Guide.

STEP 11. CONFIGURING NETWORK AGENT SETTINGS

You must configure Network Agent settings if you plan to manage Kaspersky Endpoint Security using Kaspersky Administration Kit. The configuration process is implemented as a script.

➧ *To run the Network Agent configuration script, execute the following command:*

```
# /opt/kaspersky/klnagent/lib/bin/setup/postinstall.pl
```

After launching the script, you will be asked to perform the following actions:

1. Specify the DNS name or IP address of your Administration Server.
2. Specify the Administration Server port number or use default port number (14000).
3. Specify the SSL port number of the Administration Server or use default port number (13000).
4. Define whether the SSL connection should be used for data transfer. By default, SSL connection is enabled.

To obtain detailed information on setting up Network Agent, please refer to Kaspersky Administration Kit Administrator Guide.

STARTING AUTOMATIC INITIAL CONFIGURATION

Initial setup of Kaspersky Endpoint Security can be performed in automatic mode.

➧ *To start initial setup in automatic mode, execute the following command:*

for Linux:

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-setup.pl \
--auto-install=<full path to initial setup configuration file>
```

for FreeBSD:

```
/usr/local/bin/kes4lwks-setup.pl \
--auto-install=<full path to initial setup configuration file>
```

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

Table 2 Initial configuration file settings

SETTING	DESCRIPTION	AVAILABLE VALUES
EULA_AGREED	Required setting. I agree with the conditions of the license agreement	**yes**

SETTING	DESCRIPTION	AVAILABLE VALUES
SERVICE_LOCALE	The locale used by Kaspersky Endpoint Security	The locale in the format specified in RFC 3066
INSTALL_KEY_FILE	Full path to the key file	
UPDATER_SOURCE	Updates source	• **AKServer** – use the Kaspersky Administration Kit server as the update source; • **KLServers** – use the Kaspersky Lab servers as the update source; • URL of the update source;
UPDATER_PROXY	Address of the proxy server used to connect to the Internet	• URL of the proxy server; • **no** – do not use a proxy server;
UPDATER_EXECUTE	Start database update task during setup	• **yes** – start update task; • **no** – do not start update task;
UPDATER_ENABLE_AUTO	Enable / disable automatic start of database update task	• **yes** – enable automatic start of update task; • **no** – disable automatic start of update task;
RTP_BUILD_KERNEL_MODULE	Required setting. Starting compilation of kernel module	• **yes** – compile kernel module; • **no** – do not compile kernel module;
RTP_BUILD_KERNEL_SRCS	Path to the kernel source codes	• **auto** – automatic search; • path to the source codes;
RTP_SAMBA_ENABLE	Required setting. Integrating with Samba server	• **yes** – integrate using the settings RTP_SAMBA_CONF, RTP_SAMBA_VFS, RTP_SAMBA_VFS_MODULE; • **no** – do not integrate; • **auto** – automatically determine paths to Samba server components;
RTP_SAMBA_CONF	Full path to Samba server configuration file (*smb.conf*)	
RTP_SAMBA_VFS	Full path to the directory containing the VFS modules for the Samba server	
RTP_SAMBA_VFS_MODULE	Full path to VFS module of Kaspersky Endpoint Security to be installed as the module handler	
RTP_START	Start real-time protection on setup completion	• **yes** – start real-time protection task; • **no** – do not start real-time protection task;
GUI_ENABLE	Starting graphical interface automatically at system startup.	• **yes** – to start graphical interface automatically; • **no** – not to start graphical interface automatically;

Enter parameter values in the **parameter name=value** format (spaces between parameter name and its value are not processed).

CONFIGURING PERMISSIONS FOR SELINUX AND APPARMOR SYSTEMS

Kaspersky Endpoint Security is incompatible with SELinux and Novell AppArmor.

➧ *To switch SELinux to permissive mode, execute the following command:*

```
# setenforce Permissive
```

➧ *To switch all the AppArm to"complain" mode, execute the following command:*

```
# aa-complain /etc/apparmor.d/*
# /etc/init.d/apparmor reload
```

REMOVING KASPERSKY ENDPOINT SECURITY

If you want to restore quarantined files, do that before uninstalling Kaspersky Endpoint Security. Otherwise, it will not be possible to restore files from quarantine.

➧ *To remove Kaspersky Endpoint Security, installed from .rpm-package, execute the following command:*

```
# rpm -e kes4lwks
```

➧ *To remove Kaspersky Endpoint Security, installed from .deb-package, execute the following command:*

```
# dpkg -r kes4lwks
```

➧ *To remove Kaspersky Endpoint Security on a computer running FreeBSD execute the following command:*

```
# pkg_delete kes4lwks
```

All Kaspersky Endpoint Security tasks will be stopped.

➧ *To delete Network Agent installed from an .rpm-package, execute the following command:*

```
# rpm -e klnagent
```

➧ *To delete Network Agent installed from a .deb-package, execute the following command:*

```
# dpkg -r klnagent
```

The uninstallation procedure is performed automatically. Upon completion of the procedure, a confirmation message will be displayed on the screen.

UNINSTALLING KASPERSKY ENDPOINT SECURITY REMOTELY

Remote uninstallation of Kaspersky Endpoint Security using Kaspersky Administration Kit is performed by running a remote uninstallation task.

➡ *To create a remote uninstallation task for Kaspersky Endpoint Security, perform the following actions:*

1. Connect to the necessary Administration Server.
2. Select the **Tasks for specific computers** folder in the console tree.
3. Open the context menu and select **Create** → **Task** or the analogous point in the **Action** menu.

   This will launch the Task Creation Wizard.
4. In the **Task name** window enter the name of the task in the **Name** field.
5. In the **Task type** window in the **Kaspersky Administration Kit** node, open the **More** folder and select **Remote uninstallation of application**.
6. Specify the application that should be removed in the **Settings** window. To do this, in the **Remove application supported by Kaspersky Administration Kit** dropdown list, select **Kaspersky Endpoint Security 8 for Linux**.
7. In the **Remote uninstallation method** window, select **Push uninstallation**.
8. In the **Settings** window under the **Force download of uninstallation utility** settings, select the **Using Administration Console** checkbox.
9. Complete the task creation process as for a remote installation task (see page 14).

The task that you have created will start in accordance with its schedule.

➡ *To start a remote uninstallation task for Kaspersky Endpoint Security manually, perform the following actions:*

1. Connect to the necessary Administration Server.
2. Select the **Tasks for specific computers** folder in the console tree.
3. In the results pane, select the required task in the list.
4. Open the context menu and select **Start** or the analogous point in the **Action** menu.

STEPS TO PERFORM AFTER YOU UNINSTALL KASPERSKY ENDPOINT SECURITY

After you remove Kaspersky Endpoint Security (see page 30), the following information remains on the computer:

- Kaspersky Endpoint Security databases;
- license repository databases;
- event repository databases;
- Kaspersky Endpoint Security operation settings databases;
- files in the backup storage and quarantine;
- log files.

Kaspersky Endpoint Security includes scripts that delete files and directories remaining on the server after uninstallation of Kaspersky Endpoint Security.

➧ *To run these scripts, perform the following steps:*

1. Enter the following command:
   - for Linux: `# /var/opt/kaspersky/kes4lwks/cleanup.sh`
   - for FreeBSD: `# /var/db/kaspersky/kav4fs/cleanup.sh`
2. Confirm deletion of information remaining after uninstallation of Kaspersky Endpoint Security, by responding **yes**. To keep the information and stop the script execution, enter **no**.

VERIFYING REAL-TIME PROTECTION AND ON-DEMAND SCAN TASKS OPERATION

After installing and initial configuration of Kaspersky Endpoint Security, you can make sure that real-time protection and the on-demand scan tasks are properly configured.

IN THIS SECTION

VERIFYING REAL-TIME PROTECTION TASK OPERATION

This section describes how to make sure the Kaspersky Endpoint Security real-time protection task detects infected and suspicious objects when they are accessed and performs the actions on such objects that are specified in the task.

➡ *To check operation of the real-time protection task, perform the following steps:*

1. Download the *eicar.com* file from EICAR site at http://www.eicar.org/anti_virus_test_file.htm. Save it on the protected computer.

   If you want to verify how Kaspersky Endpoint Security detects suspicious files, add the "SUSP-" prefix to the line of text in the file (for more detail, see section "EICAR test virus and its modifications").

2. Start the real-time protection task, if it was stopped, using the following command:

   ```
   # /opt/kaspersky/kes4lwks/bin/kes4lwks-control --start-task 8
   ```

3. Open the *eicar.com* file for reading, using the following command:

   ```
   # cat <full_path_to_eicar.com>
   ```

4. Kaspersky Endpoint Security will intercept attempts to access the file, check the file, and block access to it. The following message will be displayed on the console:

   ```
   "cat: <full_path_to_eicar.com>: Permission denied"
   ```

5. Enter the following command:

   ```
   # echo $?
   ```

   The real-time protection task has successfully handled access to the *eicar.com* file if this command returns a nonzero value.

VERIFYING ON-DEMAND SCAN TASK OPERATION

This section describes how to make sure that Kaspersky Endpoint Security detects infected and suspicious objects in the scan area specified in the on-demand scan task, and then performs the actions specified in the task on the found objects.

You can verify the "On-demand scan" function by performing either the **Full computer scan** task or another user-defined on-demand scan task.

You will need to save the *eicar.com* file on the protected computer.

➧ *To verify operation of an on-demand scan task, perform the following step:*

1. Stop the real-time protection task using the following command:

   ```
   # /opt/kaspersky/kes4lwks/bin/kes4lwks-control --stop-task 8
   ```

2. Download the *eicar.com* file from the EICAR web page at http://www.eicar.org/anti_virus_test_file.htm and save it on the protected computer.

   During the scan, Kaspersky Endpoint Security will assign the **Infected** status to the file if you leave the eicar.com file unmodified. Kaspersky Endpoint Security will assign the **Suspicious**, status if you modify the line of text in the file *eicar.com* , appending the "SUSP-" prefix (for more details, see section "Test virus EICAR and its modifications" (see page 34)).

3. Create an on-demand scan task using the following command:

   ```
   # /opt/kaspersky/kes4lwks/bin/kes4lwks-control \

   --create-task <task_name> --use-task-type=ODS
   ```

   The ID of the created task will be displayed on the console.

4. Add the directory containing the *eicar.com* file to the scan area of the created task using the following command:

   ```
   # /opt/kaspersky/kes4lwks/bin/kes4lwks-control \

   --set-settings <ID_of_the_created_task> \

   ScanScope.AreaPath.Path=<path_to_the_directory_containing_eicar.com>
   ```

5. Start the created task using the following command:

   ```
   # /opt/kaspersky/kes4lwks/bin/kes4lwks-control \

   --start-task <ID_of_the_created_task> -W
   ```

6. Review the results of the task's operation on the console.

The on-demand scan task is properly configured if the *eicar.com* file has been deleted from the protected computer (on condition that the task settings specify the action to perform on infected objects as **Disinfect, delete if disinfection is not possible**).

TEST VIRUS EICAR AND ITS MODIFICATIONS

Test virus is designed for verification of the operation of the anti-virus applications. It is developed by The European Institute for Computer Antivirus Research (EICAR).

> The test virus is not a malicious program. It does not contain program code that may inflict damage to your computer. However, anti-virus applications of most vendors identify a threat in it.

File containing this test virus is called eicar.com. You can download it from the http://www.eicar.org/anti_virus_test_file.htm page at the EICAR organization's official web site.

Before saving the file in a computer directory, make sure that real-time file protection is disabled for the directory.

The eicar.com file contains a text line. While scanning the file, Kaspersky Endpoint Security will identify a "threat" in this line of text, assign it the status **Infected**, and perform the action specified in the task.

You can also use the eicar.com file in order to check how Kaspersky Endpoint Security reacts when threats of other types are detected. To do it, open the file using a text editor, add one of the prefixes listed in the table below to the file content, and save the file under a new name.

Table 3. Prefixes

PREFIX	**FILE STATUS AFTER THE SCAN AND KASPERSKY ENDPOINT SECURITY ACTION**
No prefix	Kaspersky Endpoint Security assigns the **Infected** status to the object.
WARN-	The Kaspersky Endpoint Security assigns the status **Warning** to the object (the object's code partly coincides with the code of a known threat).
ERRO-	An error occurred when scanning the object. Kaspersky Endpoint Security could not access the object: the integrity of the object has been violated (for example, a multivolume archive has no end) or there is no connection to it (if the object is being scanned on a network resource).
SUSP-	Kaspersky Endpoint Security assigns the **Suspicious** status to the object (detected using the Heuristic Analyzer).
CURE-	Kaspersky Endpoint Security assigns the **Infected** status to the object and attempts to disinfect the file. If disinfection is successful, the body of the virus is replaced by the word "CURE".
CORR-	Kaspersky Endpoint Security assigns the **Corrupted** status to the object.

KASPERSKY ENDPOINT SECURITY FILE LOCATIONS

After Kaspersky Endpoint Security is installed on a computer running Linux operating system, the files of the distribution package will be located in the following default directories:

/opt/kaspersky/kes4lwks/ – main directory of Kaspersky Endpoint Security, containing:

bin/ – directory that contains executable files of all Kaspersky Endpoint Security components:

kes4lwks-control – executable file for the product control component;

kes4lwks-qtgui – executable file for graphical interface;

kes4lwks-setup.pl – script for post-install Kaspersky Endpoint Security configuration.

lib/ – directory that contains supplemental Kaspersky Endpoint Security modules:

samba/ – the compiled Samba module directory.

lib64/ – directory that contains supplemental Kaspersky Endpoint Security' 64-bit modules:

samba/ – the compiled 64-bit Samba module directory.

libexec/ – the Kaspersky Endpoint Security support file directory;

src/ – the Kaspersky Endpoint Security module source code directory:

kernel/ – the Kaspersky Endpoint Security kernel module library directory;

samba/ – the Samba module library directory for Kaspersky Endpoint Security.

/opt/kaspersky/kes4lwks/share/doc/ – Kaspersky Endpoint Security documentation files:

LICENSE – license agreement.

LICENSE.GPL – the license agreement for the kernel and Samba modules.

/opt/kaspersky/kes4lwks/share/man/ – the man file directory.

/etc/init.d/ – directory that contains management scripts of Kaspersky Lab Framework:

kes4lwks-supervisor – the control script for the Kaspersky Lab Framework service.

/etc/opt/kaspersky/ – directory that contains the configuration file of Kaspersky Lab Framework:

kes4lwks-supervisor.conf – the configuration file of the Kaspersky Lab Framework.

/var/opt/kaspersky/kes4lwks/ – the Kaspersky Endpoint Security data directory:

db/ – Kaspersky Endpoint Security databases;

update/ – the Kaspersky Endpoint Security updates directory;

quarantine/ – quarantine storage.

/var/log/kaspersky/kes4lwks/ – the Kaspersky Endpoint Security log file directory;

/var/run/kes4lwks/ – the Kaspersky Endpoint Security temporary file directory.

To connect to the Kaspersky Endpoint Security manual pages, add the following lines to the shell configuration file:

```
MANPATH="$MANPATH:/opt/kaspersky/kes4lwks/share/man/:"

export MANPATH
```

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.

The Kaspersky Lab website:	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)