

Kaspersky Anti-Virus 8.0 for Linux File Server

INSTALLATION 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: all rights to this document are protected by the copyright laws of the Russian Federation and by international treaties. Illegal reproduction and distribution of this document or parts hereof result in civil, administrative or criminal liability by applicable law.

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

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

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

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

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

Document revision date: 11/18/2010

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

<http://www.kaspersky.com>

<http://support.kaspersky.com>

CONTENTS

INTRODUCTION.....	5
Application purpose	5
Hardware and software system requirements	5
Obtaining information about Kaspersky Anti-Virus	7
Sources of information for further research.....	7
Contacting the Technical Support Service	9
Discussing Kaspersky Lab's applications on the web forum	9
What's new in version 8.0.....	10
DISTRIBUTION CONTENTS	12
KASPERSKY ANTI-VIRUS INSTALLATION.....	13
Step 1. Installation of the Kaspersky Anti-Virus package	13
Step 2. Installing Network Agent.....	14
KASPERSKY ANTI-VIRUS REMOTE INSTALLATION.....	15
Creating a remote installation task	15
Step 1. Defining the task name.....	16
Step 2. Selecting the task type.....	16
Step 3. Selecting the installation package	16
Step 4. Selecting the remote installation method.....	16
Step 5. Configuring update task settings	16
Step 6. Selecting the installation package for joint deployment	17
Step 7. Configuring the restart settings.....	17
Step 8. Defining the method for selecting computers.....	17
Step 9. Selecting the client computers.....	17
Step 10. Specifying the user account for running tasks	17
Step 11. Scheduling the task launch.....	18
Step 12. Completing task creation	18
Running a remote installation task.....	18
Viewing and configuring the remote installation package settings.....	19
Creating an installation package.....	19
Step 1. Defining the installation package name	20
Step 2. Selecting the application distribution package	20
Step 3. Loading the installation package	20
Step 4. Configuring the real-time protection task	20
Step 5. Configuring update task settings	21
Step 6. Completing creation of an installation package	21
Viewing and configuring the settings of an installation package.....	21
KASPERSKY ANTI-VIRUS INITIAL CONFIGURATION	23
Step 1. Reviewing the license agreement	24
Step 2. Selecting the locale	24
Step 3. Installing the key file	25
Step 4. Configuring proxy server settings	25
Step 5. Downloading Kaspersky Anti-Virus databases.....	25
Step 6. Enabling automatic database updates	26
Step 7. Compiling the kernel module.....	26

- Step 8. Integrating with Samba server.....26
- Step 9. Purpose of the password for access to the Web Management Console27
- Step 10. Starting the real-time protection task.....28
- Step 11. Managing the Web Management Console service28
- Step 12. Access to the Web Management Console interface.....28
- Step 13. Configuring Network Agent settings29
- Starting the automatic initial setup.....29
- Configuring permissions for SELinux and AppArmor systems.....31
- REMOVING KASPERSKY ANTI-VIRUS.....33
- REMOTE UNINSTALLATION OF KASPERSKY ANTI-VIRUS34
- STEPS TO PERFORM AFTER UNINSTALLING KASPERSKY ANTI-VIRUS35
- VERIFYING REAL-TIME PROTECTION AND ON-DEMAND SCAN TASKS OPERATION36
 - Verifying real-time protection task operation.....36
 - Verifying on-demand scan task operation.....36
 - Test virus EICAR and its modifications.....37
- KASPERSKY ANTI-VIRUS FILE LOCATIONS39
- KASPERSKY LAB.....42

INTRODUCTION

This Guide contains a description of the installation procedure for Kaspersky Anti-Virus 8.0 for Linux File Server (hereinafter referred to as the *Kaspersky Anti-Virus* or *application*).

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

IN THIS SECTION

Application purpose.....	5
Hardware and software system requirements.....	5
Obtaining information about Kaspersky Anti-Virus.....	7
What's new in version 8.0.....	10

APPLICATION PURPOSE

Kaspersky Anti-Virus 8.0 for Linux File Server is intended to provide anti-virus protection for file servers that run under Linux and FreeBSD operating systems.

Kaspersky Anti-Virus allows the user to:

- provide real-time server's file system protection against malicious code, i.e. intercept file access requests, analyze them, and disinfect or delete infected objects;
- scan server 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 containing valuable information;
- update application databases using Kaspersky Lab update servers or Administration Server; also, Kaspersky Anti-Virus can be configured to update the databases from a local directory;
- manage the application and modify its operation settings using the control utility, Kaspersky Administration Kit and Web Management Console.

HARDWARE AND SOFTWARE SYSTEM REQUIREMENTS

In order for Kaspersky Anti-Virus to operate, the system must meet the following hardware and software requirements:

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

- 2 GB available on the hard drive to install Kaspersky Anti-Virus and store temporary and log files.
- Software requirements:
 - One of the following 32-bit operating systems:
 - Red Hat Enterprise Linux 5.5 Server;
 - Red Hat Enterprise Linux 6 Server;
 - Fedora 13;
 - CentOS-5.5;
 - SUSE Linux Enterprise Server 10 SP3;
 - SUSE Linux Enterprise Server 11 SP1;
 - Novell Open Enterprise Server 2 SP2;
 - openSUSE Linux 11.3;
 - Mandriva Enterprise Server 5.1;
 - Ubuntu 10.04 LTS Server Edition;
 - Debian GNU/Linux 5.0.5;
 - FreeBSD 7.3, 8.1.
 - One of the following 64-bit operating systems:
 - Red Hat Enterprise Linux 5.5 Server;
 - Red Hat Enterprise Linux 6 Server;
 - Fedora 13;
 - CentOS-5.5;
 - SUSE Linux Enterprise Server 10 SP3;
 - SUSE Linux Enterprise Server 11 SP1;
 - Novell Open Enterprise Server 2 SP2;
 - openSUSE Linux 11.3;
 - Ubuntu 10.04 LTS Server Edition;
 - Debian GNU/Linux 5.0.5;
 - FreeBSD 7.3, 8.1.
 - one of the following web browsers (for management via Web Management Console):
 - Microsoft Internet Explorer 7;
 - Microsoft Internet Explorer 8;
 - Mozilla FireFox 3.x.

- Perl interpreter: version 5.0 or later, see <http://www.perl.org>
- Installed packages for compiling programs (gcc, binutils, glibc (64-bit operating systems use 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 Anti-Virus modules.

OBTAINING INFORMATION ABOUT KASPERSKY ANTI-VIRUS

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

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

SOURCES OF INFORMATION FOR FURTHER RESEARCH

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

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

Page at the Kaspersky Lab website

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

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

Documentation

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

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

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

Manual pages

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

- managing Kaspersky Anti-Virus from the command line:
 - for Linux – `/opt/kaspersky/kav4fs/share/man/man1/kav4fs-control.1.gz`;
 - for FreeBSD – `/usr/local/man/man1/kav4fs-control.1.gz`;
- configuring general settings for Kaspersky Anti-Virus:

- for Linux – */opt/kaspersky/kav4fs/share/man/man5/kav4fs.conf.5.gz*;
- for FreeBSD – */usr/local/man/man5/kav4fs.conf.5.gz*;
- configuring the real-time protection task:
 - for Linux – */opt/kaspersky/kav4fs/share/man/man5/kav4fs-oas.conf.5.gz*;
 - for FreeBSD – */usr/local/man/man5/kav4fs-oas.conf.5.gz*;
- configuring on-demand scan tasks:
 - for Linux – */opt/kaspersky/kav4fs/share/man/man5/kav4fs-ods.conf.5.gz*;
 - for FreeBSD – */usr/local/man/man5/kav4fs-ods.conf.5.gz*;
- configuring update tasks:
 - for Linux – */opt/kaspersky/kav4fs/share/man/man5/kav4fs-update.conf.5.gz*;
 - for FreeBSD – */usr/local/man/man5/kav4fs-update.conf.5.gz*;
- configuring the storage of quarantined objects and the storage of objects backed up before disinfection or removal:
 - for Linux – */opt/kaspersky/kav4fs/share/man/man5/kav4fs-quarantine.conf.5.gz*;
 - for FreeBSD – */usr/local/man/man5/kav4fs-quarantine.conf.5.gz*;
- configuring notifications:
 - for Linux – */opt/kaspersky/kav4fs/share/man/man5/kav4fs-notifier.conf.5.gz*;
 - for FreeBSD – */usr/local/man/man5/kav4fs-notifier.conf.5.gz*;
- configuring SNMP-Agent:
 - for Linux – */opt/kaspersky/kav4fs/share/man/man5/kav4fs-snmp.conf.5.gz*;
 - for FreeBSD – */usr/local/man/man5/kav4fs-snmp.conf.5.gz*;
- configuring the event repository:
 - for Linux – */opt/kaspersky/kav4fs/share/man/man5/kav4fs-events.conf.5.gz*;
 - for FreeBSD – */usr/local/man/man5/kav4fs-events.conf.5.gz*;
- description of utility which changes the Web Management Console's user password:
 - for Linux – */opt/kaspersky/kav4fs/share/man/man1/kav4fs-wmconsole-passwd.1.gz*;
 - for FreeBSD – */usr/local/man/man1/kav4fs-wmconsole-passwd.1.gz*;
- description of utility which changes settings for connection with the Kaspersky Administration Kit Administration Server:
 - for Linux – */opt/kaspersky/klnagent/share/man/man1/klmover.1.gz*;
- description of utility which checks settings for connection with the Kaspersky Administration Kit Administration Server:

- for Linux – `/opt/kaspersky/klagent/share/man/man1/klagchk.1.gz`.

CONTACTING THE TECHNICAL SUPPORT SERVICE

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

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

Technical Support by email

You may submit 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 may submit your question in Russian, English, German, French, or Spanish.

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

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

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

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

- **Request type.** Select the topic most similar to the problem you have encountered, e.g.: "Product installation / removal problem", or "Virus scan / removal problem".
- **Kaspersky Anti-Virus version name and number.**
- **Text of request.** Describe in detail the problem encountered.
- **Client number and password.** Enter the client number and the password received during the registration at the Technical Support service website.
- **Email address.** The Technical Support service will send their answer to this email address.

Technical support by phone

If you have a problem which requires urgent help, you may call your nearest Technical Support office. When you apply to Russian-speaking (http://support.kaspersky.ru/support/support_local) or international (<http://support.kaspersky.ru/support/international>) Technical Support specialists, please remember to provide the Kaspersky Anti-Virus information (<http://support.kaspersky.ru/support/details>), so that our specialists could help you as soon as possible.

DISCUSSING KASPERSKY LAB'S APPLICATIONS ON THE WEB FORUM

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

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

WHAT'S NEW IN VERSION 8.0

Let's take a closer look at the new features in Kaspersky Anti-Virus 8.0 for Linux File Server.

New protection features:

- Kaspersky Anti-Virus 8.0 combines the capabilities of previous application versions, i.e. Kaspersky Anti-Virus 5.7 for Linux File Server 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 and backup storage capabilities have been expanded:
 - Objects are stored in encrypted form.
 - New administrative capabilities allow you to:
 - 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 or backup storage in an archive (to reduce the amount of used disk space);
 - import objects from the archive into the quarantine or backup storage.
 - A new feature allows you to manage the quarantine and backup storage using Web Management Console.

New features to manage the operation of Kaspersky Anti-Virus:

- Centralized management of the Kaspersky Anti-Virus life cycle and performance of on-demand scan, real-time protection, and Kaspersky Anti-Virus database update tasks.
- Centralized storage of Kaspersky Anti-Virus operation settings.
- Kaspersky Anti-Virus 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 POSIX extended regular expressions.

- A list of users / groups, the file operations of whom 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.
- Actions to perform on objects may be specified based on the type of detected threat.
- The schedule for running / stopping tasks may be configured in detail.

New in Kaspersky Anti-Virus monitoring, reporting, and operation statistics:

- The following Kaspersky Anti-Virus monitoring features have been expanded:
 - tools for obtaining the following categories of information:
 - general information about the application;
 - information about the Kaspersky Anti-Virus databases version;
 - information about the license state;
 - information about the status of Kaspersky Anti-Virus components;
 - information about tasks results;
 - information about the state of the quarantine and backup storage;
 - tools for notifying administrators of the protected server about events related to Kaspersky Anti-Virus operation, such as:
 - Kaspersky Anti-Virus database obsolescence;
 - license expiration;
 - violation of the licensing agreement terms;
 - the occurrence of critical errors in Kaspersky Anti-Virus operation;
 - tools for retrospective analysis of Kaspersky Anti-Virus operation that enable you to:
 - collect, process, and store the statistics on Kaspersky Anti-Virus operation;
 - display the Kaspersky Anti-Virus operation statistics collected over a user-specified period of time;
 - search events based on criteria specified by the user;
 - audit the following aspects of application operation: creating / running / stopping Kaspersky Anti-Virus tasks, modifying Kaspersky Anti-Virus settings, user actions on objects in the quarantine and backup storage, etc.;
 - tools for creating reports on Kaspersky Anti-Virus operation, based on collected statistics, and tools for exporting reports (HTML, PDF and XLS formats are supported);
 - monitoring Kaspersky Anti-Virus operation and virus activity. Information is located in a centralized repository of Kaspersky Anti-Virus events. Kaspersky Anti-Virus 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 Anti-Virus distribution are shown in the table below.

Table 1. Kaspersky Anti-Virus packages

PACKAGE	PURPOSE
kav4fs-<version_number>.i386.rpm kav4fs_<version_number>_i386.deb kav4fs-<version_number>.tgz	Contains the main Kaspersky Anti-Virus files. This package can be installed both on 32-bit and 64-bit operating systems.
klagent-<version_number>.i386.rpm klagent_<version_number>_i386.deb	This package contains Network Agent (a utility that connects Kaspersky Anti-Virus to Kaspersky Administration Kit).
kav4fs-rpm.tar.gz kav4fs-deb.tar.gz	Contains the files kav4fs.kpd and akinstall.sh used in the remote installation procedure for Kaspersky Anti-Virus using Kaspersky Administration Kit.
klagent-rpm.tar.gz klagent-deb.tar.gz	Contains the files klagent.kpd and akinstall.sh used in the remote installation procedure for Administration Console using Kaspersky Administration Kit.

The main package of Kaspersky Anti-Virus includes the Web Management Console component.

KASPERSKY ANTI-VIRUS INSTALLATION

Kaspersky Anti-Virus is distributed in packages in `.tgz`, `.deb` and `.rpm` formats.

The installation process includes several steps:

1. Installation of the Kaspersky Anti-Virus package.
2. Installation of the Network Agent package (installation of this package is necessary to manage Kaspersky Anti-Virus using Kaspersky Administration Kit).

IN THIS SECTION

Step 1. Installation of the Kaspersky Anti-Virus package	13
Step 2. Installing Network Agent	14

STEP 1. INSTALLATION OF THE KASPERSKY ANTI-VIRUS PACKAGE

Before installing Kaspersky Anti-Virus 8.0 for Linux File Server, de-install Kaspersky Anti-Virus 5.5 for Samba Servers and Kaspersky Anti-Virus 5.7 for Linux File Server if either or both are installed on the server.

You must have **root** privileges to initiate installation of the Kaspersky Anti-Virus package.

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

➤ To install Kaspersky Anti-Virus from `.rpm`-package, execute the following command:

```
# rpm -i kav4fs-<version_number>.i386.rpm
```

➤ To install Kaspersky Anti-Virus from `.deb`-package, execute the following command:

```
# dpkg -i kav4fs_<version_number>_i386.deb
```

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

```
# dpkg -i --force-architecture kav4fs_<version_number>_i386.deb
```

➤ To install Kaspersky Anti-Virus on a server running FreeBSD, execute the following command:

```
# pkg_add kav4fs-<version_number>.tgz
```

➤ To enable Web Management Console and Kaspersky Anti-Virus services start after you install them to a server running FreeBSD, add to the `/etc/rc.conf` configuration file the following strings:

```
kav4fs_supervisor_enable="YES"
kav4fs_wmconsole_enable="YES"
```

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

The post-installation Kaspersky Anti-Virus configuration script should be started (see page [23](#)) after the application has been installed from .rpm-package.

STEP 2. INSTALLING NETWORK AGENT

Installation of the Network Agent package (installation of this package is required to manage Kaspersky Anti-Virus using Kaspersky Administration Kit):

You must have root privileges to initiate installation of the Kaspersky Administration kit. .

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

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

➤ *To install Network Agent from .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 (see page [29](#)) after Network Agent has been installed from .rpm-package.

KASPERSKY ANTI-VIRUS REMOTE INSTALLATION

You can install Kaspersky Anti-Virus remotely via the Administration Console in Kaspersky Administration Kit. To install Kaspersky Anti-Virus remotely, create a remote installation task (see section "Creating a remote installation task" on page [15](#)) 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 must be installed and configured (see page [29](#)). To successfully complete the remote installation, Administration Console must be started on a protected server.

Installation packages (see section "Creating an installation package" on page [19](#)) are used to create a remote installation task. 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 [23](#)). 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 using 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 remote installation task	15
Running a remote installation task	18
Viewing and configuring the remote installation package settings	19
Creating an installation package	19
Viewing and configuring the settings of an installation package.....	21

CREATING A REMOTE INSTALLATION TASK

➤ *To create a remote installation 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 **New** → **Task** or the analogous point in the **Action** menu.

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

THE WIZARD'S STEPS

Step 1. Defining the task name [16](#)

Step 2. Selecting the task type..... [16](#)

Step 3. Selecting the installation package..... [16](#)

Step 4. Selecting the remote installation method [16](#)

Step 5. Configuring update task settings..... [16](#)

Step 6. Selecting the installation package for joint deployment..... [17](#)

Step 7. Configuring the restart settings [17](#)

Step 8. Defining the method for selecting computers [17](#)

Step 9. Selecting the client computers [17](#)

Step 10. Specifying the user account for running tasks [17](#)

Step 11. Scheduling the task launch [18](#)

Step 12. Completing task creation [18](#)

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 **Application deployment**.

STEP 3. SELECTING THE INSTALLATION PACKAGE

Specify the installation package that will be installed during execution of the given task. 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 [19](#)) using the Installation Package Creation Wizard.

STEP 4. SELECTING THE REMOTE INSTALLATION METHOD

Select the **Push install** option.

STEP 5. CONFIGURING UPDATE TASK SETTINGS

In this step, you will be 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 Network Agent along with this application**, and then select the required installation package.

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

click the **Create** button.

This will start the New Package Wizard (see section "Creating an installation package" on page [19](#)). Follow the wizard's instructions.

STEP 7. CONFIGURING THE RESTART SETTINGS

Define the operations that should be performed if server 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;
- **Prompt user for action** – 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 client computers for installation will be selected using the data collected by the Administration Server during corporate network discovery;
- **I want to define computer addresses (IP, DNS or NETBIOS) 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 **Managed computers** folder) and the computers not included in the groups (the **Unassigned computers** folder).

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 txt 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 server. To import the list from a file, you need to specify the txt file with a list of addresses of servers 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 this, do the following:
 - Define the procedure for the task launch 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, this 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 [19](#)).

RUNNING 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 **OS reboot** tabs.

Remote installation tasks are configured in the same way as the properties of any of the tasks. Let's take a closer look at the settings specific for this task type on the **Settings** tab. You 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 launched 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 Anti-Virus distribution disk.

➤ To make a Kaspersky Anti-Virus distribution disk, do the following:

1. Unpack the kav4fs-rpm.tar.gz or kav4fs-deb.tar.gz archive (depending on the package manager used in the operating system of the protected server) in a folder accessible to Administration Server in Kaspersky Administration Kit.
2. Copy the kav4fs-<version_number>.i386.rpm or kav4fs_<version_number>_i386.deb package to the same folder (depending on the package manager used in the operating system of the protected server).

➤ 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 **New** → **Installation package** or the corresponding point in the **Action** menu.

This opens the New Package Wizard. Follow the wizard's instructions.

THE WIZARD'S STEPS

Step 1. Defining the installation package name	20
Step 2. Selecting the application distribution package	20
Step 3. Loading the installation package.....	20
Step 4. Configuring the real-time protection task	20
Step 5. Configuring update task settings.....	21
Step 6. Completing creation of an installation package.....	21

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 Kaspersky Lab's installation package**. 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 [21](#)) 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

In 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.

Further in this step, you will be 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 Anti-Virus 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/kav4fs/lib/samba/kav4fs-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

In this step, you will be asked to specify the task update settings. The following update sources are available:

- **Do not change;**
- **Kaspersky Administration Kit 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. The update source can be an HTTP or FTP server, or a local or network folder.

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 SETTINGS OF AN INSTALLATION PACKAGE

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

1. Go to 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 during generation of the installation package (see section "Creating an installation package" on page [19](#)). If required, they can be changed.

The **Update** tab contains update task settings: selection of update source and user update source configuration. These settings are configured during generation of the installation package (see section "Creating an installation package" on page [19](#)). 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 change the key file.

KASPERSKY ANTI-VIRUS INITIAL CONFIGURATION

After Kaspersky Anti-Virus has been installed on the server, you will need to configure Kaspersky Anti-Virus initial settings.

If Kaspersky Anti-Virus initial configuration has not been performed, the server'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 Anti-Virus databases,
- compiling the kernel modules.

➡ *To run the Kaspersky Anti-Virus initial configuration script manually, execute the following command:*

for Linux:

```
# /opt/kaspersky/kav4fs/bin/kav4fs-setup.pl
```

You can perform the actions required to start a real-time protection task using Kaspersky Anti-Virus management tools. For detailed information, please refer to Kaspersky Anti-Virus 8.0 for Linux File Server Administrator's Guide.

IN THIS SECTION

Step 1. Reviewing the license agreement	24
Step 2. Selecting the locale	24
Step 3. Installing the key file	25
Step 4. Configuring proxy server settings	25
Step 5. Downloading Kaspersky Anti-Virus databases	25
Step 6. Enabling automatic database updates	26
Step 7. Compiling the kernel module	26
Step 8. Integrating with Samba server	26
Step 9. Purpose of the password for access to the Web Management Console	27
Step 10. Starting the real-time protection task	28
Step 11. Managing the Web Management Console service	28
Step 12. Access to the Web Management Console interface	28
Step 13. Configuring Network Agent settings	29
Starting the automatic initial setup	29
Configuring permissions for SELinux and AppArmor systems	31

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 Anti-Virus configuration will terminate.

STEP 2. SELECTING THE LOCALE

At this stage you need to specify the locale that will be used by Kaspersky Anti-Virus.

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 Anti-Virus 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 Anti-Virus 8.0 for Linux File Server.

If no license has been installed, the Kaspersky Anti-Virus will not provide server 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 Anti-Virus 8.0 for Linux File Server 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 Anti-Virus 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 of the following formats:
 - `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 Anti-Virus" section in Kaspersky Anti-Virus 8.0 for Linux File Server Administrator's Guide.

STEP 5. DOWNLOADING KASPERSKY ANTI-VIRUS DATABASES

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

➔ *To upload Kaspersky Anti-Virus to the server,*

respond **yes**.

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

The default answer is **yes**.

If Kaspersky Anti-Virus databases have not been uploaded, Kaspersky Anti-Virus will not provide anti-virus protection of the server.

You can start Kaspersky Anti-Virus databases update without using the script. To obtain information on starting a Kaspersky Anti-Virus database update, please refer to the "Updating Kaspersky Anti-Virus" section in the Kaspersky Anti-Virus 8.0 for Linux File Server Administrator's Guide.

STEP 6. ENABLING AUTOMATIC DATABASE UPDATES

In this step, you will be asked to enable or disable automatic updating of Kaspersky Anti-Virus databases.

➤ *To enable automatic databases updates,*

respond **yes**.

By default, updating of Kaspersky Anti-Virus databases is scheduled to run every 30 minutes.

You can enable the automatic Kaspersky Anti-Virus database updates without using the initial configuration script. To obtain information on setting up the Kaspersky Anti-Virus database update schedule, please refer to the "Modifying task schedule settings. -T --set-schedule" and "Schedule settings" sections in Kaspersky Anti-Virus 8.0 for Linux File Server Administrator's Guide.

STEP 7. COMPILING THE KERNEL MODULE

In this step, you are 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/kav4fs/bin/kav4fs-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 server'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 Anti-Virus 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.

➤ *Perform the following actions to configure protection for a Samba server manually:*

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

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 blocking of the Samba resources after the real-time protection task termination,*

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/kav4fs/bin/kav4fs-setup.pl --samba
```

STEP 9. PURPOSE OF THE PASSWORD FOR ACCESS TO THE WEB MANAGEMENT CONSOLE

In this step, you will be asked to enter a password for access to the Web Management Console.

➤ *To enter a password for access to the Web Management Console, perform the following steps:*

1. Enter **yes**.
2. Enter and re-enter the password.

If you have not specified a password for access to the Web Management Console on this stage, you can do it later using the */opt/kaspersky/kav4fs/bin/kav4fs-wmconsole-passwd* utility.

The default answer is **no**.

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;
- downloading Kaspersky Anti-Virus databases;
- compiling the kernel modules or integration with the Samba server.

To obtain information on the task management, please refer to the "Task management" section in Kaspersky Anti-Virus 8.0 for Linux File Server Administrator Guide.

STEP 11. MANAGING THE WEB MANAGEMENT CONSOLE SERVICE

You must have **root** privileges to manage the Web Management Console service.

The remote administration component Web Management Console is included in the Kaspersky Anti-Virus distribution package. By default, the Web Management Console component is not launched during the system boot sequence or the Anti-Virus startup.

➤ To start the Web Management Console service, execute the following command:

```
# /etc/init.d/kav4fs-wmconsole start
```

➤ To stop the Web Management Console service, execute the following command:

```
# /etc/init.d/kav4fs-wmconsole stop
```

Use the **chkconfig** utility (on RPM systems) or the **update-rc.d** utility (on DEB systems) to set up the automatic start of the Web Management Console service.

STEP 12. ACCESS TO THE WEB MANAGEMENT CONSOLE INTERFACE

Web Management Console provides its web interface for managing the Kaspersky Anti-Virus.

➤ To access the Web Management Console interface:

1. Launch web browser.
2. Enter the following URL in the address bar:

```
http://DNS_name_or_IP_address_of_protected_server:9080
```

3. Enter the user password specified during the Kaspersky Anti-Virus initial configuration.

The Web Management Console component accesses the protected server with the **kluser** privileges.

STEP 13. CONFIGURING NETWORK AGENT SETTINGS

You must configure Network Agent settings if you plan to manage Kaspersky Anti-Virus 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 THE AUTOMATIC INITIAL SETUP

You can perform the initial setup of Kaspersky Anti-Virus in automatic mode.

➤ To start the initial setup in automatic mode, run the following command:

for Linux:

```
/opt/kaspersky/kav4fs/bin/kav4fs-setup.pl \  
--auto-install=<full path to the initial setup configuration file>
```

for FreeBSD:

```
/usr/local/bin/kav4fs-setup.pl \  
--auto-install=<full path to the initial setup configuration file>
```

The settings of the initial setup configuration file are shown in the table below.

Table 2. Settings of the initial setup configuration file

SETTING	DESCRIPTION	POSSIBLE VALUES:
EULA_AGREED	Mandatory setting. I accept the terms of the License Agreement	yes
SERVICE_LOCALE	Locale used when working with Kaspersky Anti-Virus	Locale in the format specified in RFC 3066
INSTALL_KEY_FILE	Full path to the key file	

SETTING	DESCRIPTION	POSSIBLE VALUES:
UPDATER_SOURCE	Updates source	<ul style="list-style-type: none"> • AKServer – use Kaspersky Administration Kit Administration Server as update source; • KLServers – use Kaspersky Lab servers as update source; • URL of the update source;
UPDATER_PROXY	Address of the proxy server used to establish the Internet connection	<ul style="list-style-type: none"> • URL of the proxy server; • no – do not use any proxy server;
UPDATER_EXECUTE	Running the databases update task during the configuration process	<ul style="list-style-type: none"> • yes – run the update task; • no – do not run the update task;
UPDATER_ENABLE_AUTO	Enabling / disabling the automatic run of the databases update task	<ul style="list-style-type: none"> • yes – enable the automatic run of the update task; • no – disable the automatic run of the update task;
RTP_BUILD_KERNEL_MODULE	Mandatory setting. Starting the kernel module compilation	<ul style="list-style-type: none"> • yes – compile the kernel module; • no – do not compile the kernel module;
RTP_BUILD_KERNEL_SRCS	Path to the kernel source codes	<ul style="list-style-type: none"> • auto – automatic search; • path to the source codes;
RTP_SAMBA_ENABLE	Mandatory setting. Integrating with Samba server	<ul style="list-style-type: none"> • yes – perform integration using the values of the settings RTP_SAMBA_CONF, RTP_SAMBA_VFS, RTP_SAMBA_VFS_MODULE; • no – do not perform integration; • auto – define the paths to the Samba server components automatically;
RTP_SAMBA_CONF	Full path to the Samba server configuration file (<i>smf.conf</i>)	
RTP_SAMBA_VFS	Full path to the directory containing the VFS modules for the Samba server	
RTP_SAMBA_VFS_MODULE	Full path to the VFS module of Kaspersky Anti-Virus that should be set as processing module	
RTP_START	Running the real-time protection task when the configuration is complete	<ul style="list-style-type: none"> • yes – run the real-time protection task; • no – do not run the real-time protection task;

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

Install the package `polycoreutils-python` before using the `audit2allow` utility.

➤ To create an SELinux module with rules required to run Kaspersky Anti-Virus, do the following:

1. Switch SELinux to permissive mode:

```
# setenforce Permissive
```

2. Check the performance of the real-time protection task (see page [36](#)).
3. Create a rules module on the basis of blocking records:

```
# audit2allow -l -M kav4fs -i\ /var/log/audit/audit.log
```

Ensure that the generated list contains only rules relating to Kaspersky Anti-Virus.

4. Load the new rules module:

```
# semodule -i kav4fs.pp
```

5. Switch SELinux to enforcing mode:

```
# setenforce Enforcing
```

If new audit messages related to Kaspersky Anti-Virus appear, the rules module file needs to be updated.

➤ To update the rules module file, do the following:

```
# audit2allow -l -M kav4fs -i /var/log/audit/audit.log
```

```
# semodule -u kav4fs.pp
```

Additional information is provided in the following guides:

- Red Hat Enterprise Linux: "Red Hat Enterprise Linux Deployment Guide", chapter 44. Security and SELinux.
- Fedora: Fedora SELinux Project Pages.
- Debian GNU/Linux: "Configuring the SELinux Policy Guide" from the `selinux-doc` "Documentation for Security-Enhanced Linux".

➤ To update the AppArmor profiles required to run Kaspersky Anti-Virus, do the following:

1. Switch all rules for applications to "complain" mode:

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

```
# /etc/init.d/apparmor reload
```

2. Restart `kav4fs`:

```
# /etc/init.d/kav4fs-supervisor restart
```

3. Check the performance of the real-time protection task (see page [36](#)).

4. Run the profile update utility:

```
# aa-logprof
```

5. Reload the AppArmor rules:

```
# /etc/init.d/apparmor reload
```

6. Switch all rules for applications to "enforcing" mode:

```
# aa-enforce /etc/apparmor.d/*
```

```
# /etc/init.d/apparmor reload
```

If new audit messages related to Kaspersky Anti-Virus appear, the steps described in points 3 and 4 should be repeated.

Additional information is provided in the following guides:

- openSUSE and SUSE Linux Enterprise Server: "Novell AppArmor Quick Start", "Novell AppArmor Administration Guide".
- Ubuntu: "Ubuntu Server Guide", chapter 8. Security.

REMOVING KASPERSKY ANTI-VIRUS

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

- *To remove Kaspersky Anti-Virus installed from .rpm-package, execute the following command:*

```
# rpm -e kav4fs
```

- *To remove Kaspersky Anti-Virus installed from .deb-package, execute the following command:*

```
# dpkg -r kav4fs
```

- *To remove Kaspersky Anti-Virus installed on server under FreeBSD operating system, execute the following command:*

```
# pkg_delete kav4fs
```

In doing so, all Kaspersky Anti-Virus tasks will be stopped.

- *To remove the Network Agent from .rpm-package, execute the following command:*

```
# rpm -e klnagent
```

- *To remove Network Agent from .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.

REMOTE UNINSTALLATION OF KASPERSKY ANTI-VIRUS

Remote uninstallation of Kaspersky Anti-Virus using Kaspersky Administration Kit is performed by running a remote uninstallation task.

➤ *To create a remote uninstallation task for Kaspersky Anti-Virus, do the following:*

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 **New** → **Task** or the analogous point in the **Action** menu.

This will launch the New Task 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 **Advanced** folder and select **Product deinstallation task**.
6. Specify the application that should be removed in the **Settings** window. To do this, in the **Uninstall the application supported by Kaspersky Administration Kit** dropdown list, select **Kaspersky Anti-Virus 8.0 for Linux File Server**.
7. In the **Remote uninstall method** window, select **Forced uninstall**.
8. In the **Settings** window under the **Force uploading uninstall utility** settings, select the **Using Network Agent** checkbox.
9. Complete the task creation process as for a remote installation task (see page [15](#)).

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

➤ *To execute a remote de-installation task for Kaspersky Anti-Virus manually, 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.

STEPS TO PERFORM AFTER UNINSTALLING KASPERSKY ANTI-VIRUS

After deleting Kaspersky Anti-Virus (see page [33](#)), the following information remains on the server:

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

Kaspersky Anti-Virus includes scripts that delete files and directories remaining on the server after uninstallation of Kaspersky Anti-Virus.

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

1. Enter the following command:
 - for Linux: # `/var/opt/kaspersky/kav4fs/cleanup.sh`
 - for FreeBSD: # `/var/db/kaspersky/kav4fs/cleanup.sh`
2. Confirm deletion of information remaining after Kaspersky Anti-Virus has been uninstalled by entering **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 Anti-Virus, 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	36
Verifying on-demand scan task operation	36
Test virus EICAR and its modifications	37

VERIFYING REAL-TIME PROTECTION TASK OPERATION

This section describes how to make sure the Anti-Virus 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 server.

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

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

```
# /opt/kaspersky/kav4fs/bin/kav4fs-control --start-task 8
```

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

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

4. Anti-Virus 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 Anti-Virus 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 server.

➤ 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/kav4fs/bin/kav4fs-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 server.

During the scan, Anti-Virus will assign the **Infected** status to the file if you leave the *eicar.com* file unmodified. Anti-Virus 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 [37](#))).

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

```
# /opt/kaspersky/kav4fs/bin/kav4fs-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/kav4fs/bin/kav4fs-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/kav4fs/bin/kav4fs-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 server (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 server. However, anti-virus applications of most vendors identify a threat in it.

The file containing this test virus is called *eicar.com*. You may 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 server 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, Anti-Virus 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 Anti-Virus 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 ANTI-VIRUS ACTION
No prefix	Anti-Virus assigns the Infected status to the object.
WARN-	The Anti-Virus 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 Anti-Virus 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-	The Anti-Virus assigns the status Suspicious (detected using the Heuristic Analyzer).
CURE-	The Anti-Virus assigns the Infected status and attempts to disinfect the file. If disinfection is successful, the body of the virus is replaced by the word "CURE".
CORR-	Anti-Virus assigns the Corrupted status to the object.

KASPERSKY ANTI-VIRUS FILE LOCATIONS

After Kaspersky Anti-Virus is installed on a server running Linux, the files of the distribution package will be located in the following default directories:

/opt/kaspersky/kav4fs/ – main directory of Kaspersky Anti-Virus, containing:

bin/ – directory that contains executable files of all Kaspersky Anti-Virus components:

kav4fs-control – executable file for the product control component;

kav4fs-setup.pl – script for post-install product configuration;

kav4fs-wmconsole-passwd – executable file for the password changing utility of Web Management Console.

lib/ – directory that contains supplemental Kaspersky Anti-Virus modules:

samba/ – the compiled Samba module directory.

lib64/ – directory that contains supplemental Kaspersky Anti-Virus' 64-bit modules:

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

libexec/ – the Kaspersky Anti-Virus support file directory;

src/ – the Kaspersky Anti-Virus' module source code directory:

kernel/ – the Kaspersky Anti-Virus kernel module library directory;

samba/ – the Samba module library directory for Kaspersky Anti-Virus.

/opt/kaspersky/kav4fs/share/doc/ – Kaspersky Anti-Virus documentation files:

LICENSE – license agreement;

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

/opt/kaspersky/kav4fs/share/man/ – the man file directory.

/opt/kaspersky/kav4fs/share/snmp-mibs/ – the Kaspersky Anti-Virus mib-files directory.

/etc/init.d/ – directory that contains control scripts of the Web Management Console and Kaspersky Lab Framework:

kav4fs-wmconsole – the control script for the Web Management Console service;

kav4fs-supervisor – the control script for the Kaspersky Lab Framework service.

/etc/opt/kaspersky/ – directory that contains the configuration files of the Web Management Console and Kaspersky Lab Framework:

kav4fs-wmconsole.conf – the configuration file of the Web Management Console;

kav4fs-supervisor.conf – the configuration file of the Kaspersky Lab Framework.

/var/opt/kaspersky/kav4fs/ – the Kaspersky Anti-Virus data directory:

db/ – Kaspersky Anti-Virus databases;

update/ – the Kaspersky Anti-Virus updates directory;

quarantine/ – quarantine storage.

/var/log/kaspersky/kav4fs/ – the Kaspersky Anti-Virus log file directory.

/var/run/kav4fs/ – the Kaspersky Anti-Virus temporary file directory.

To connect to the Kaspersky Anti-Virus manual pages, add the following lines to the shell configuration file:

```
MANPATH="$MANPATH:/opt/kaspersky/kav4fs/share/man/:"
export MANPATH
```

After Kaspersky Anti-Virus is installed on a server running FreeBSD, the files of the distribution package will be located in the following default directories:

/usr/local/bin/ – directory that contains executable files of all Kaspersky Anti-Virus components:

kav4fs-control – executable file for the product control component;

kav4fs-setup.pl – script for post-install product configuration;

kav4fs-wmconsole-passwd – executable file for the password changing utility of Web Management Console.

/usr/local/lib/kaspersky/kav4fs/ – directory that contains supplemental Kaspersky Anti-Virus modules:

samba/ – the compiled Samba module directory.

lib64/ – directory that contains supplemental Kaspersky Anti-Virus' 64-bit modules:

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

libexec/ – the Kaspersky Anti-Virus support file directory;

src/ – the Kaspersky Anti-Virus' module source code directory:

kernel/ – the Kaspersky Anti-Virus kernel module library directory;

samba/ – the Samba module library directory for Kaspersky Anti-Virus.

/usr/local/share/doc/kav4fs/ – Kaspersky Anti-Virus documentation files:

LICENSE – license agreement;

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

/usr/local/man/ – the man file directory.

/usr/local/share/kav4fs/snmp-mibs/ – the Kaspersky Anti-Virus mib-files directory.

/usr/local/etc/rc.d/ – directory that contains control scripts of the Web Management Console and Kaspersky Lab Framework:

kav4fs-wmconsole – the control script for the Web Management Console service;

kav4fs-supervisor – the control script for the Kaspersky Lab Framework service.

/usr/local/etc/kaspersky/ – directory that contains the configuration files of the Web Management Console and Kaspersky Lab Framework:

kav4fs-wmconsole.conf – the configuration file of the Web Management Console;

kav4fs-supervisor.conf.default – the configuration file of the Kaspersky Lab Framework.

/var/db/kaspersky/kav4fs/ – the Kaspersky Anti-Virus data directory:

db/ – Kaspersky Anti-Virus databases;

update/ – the Kaspersky Anti-Virus updates directory;

quarantine/ – quarantine storage.

/var/log/kaspersky/kav4fs/ – the Kaspersky Anti-Virus log file directory.

/var/run/kav4fs/ – the Kaspersky Anti-Virus temporary file directory.

To connect to the Kaspersky Anti-Virus manual pages, add the following lines to the */etc/manpath.config* configuration file:

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

KASPERSKY LAB

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 1000 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 24-hour technical support service in several languages.

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

Kaspersky Lab 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)