



Plesk 8.3 for Linux/Unix Kaspersky Antivirus Module Administrator's Guide

Copyright Notice

ISBN: N/A

SWsoft.

13755 Sunrise Valley Drive

Suite 600

Herndon

VA 20171 USA

Phone: +1 (703) 815 5670

Fax: +1 (703) 815 5675

© Copyright 1999-2007,

SWsoft Holdings, Ltd.

All rights reserved

Distribution of this work or derivative of this work in any form is prohibited unless prior written permission is obtained from the copyright holder.

Patented hosting technology protected by U.S. Patents 7,099,948; 7,076,633.

Patents pending in the U.S.

Linux is a registered trademark of Linus Torvalds.

ASPLinux and the ASPLinux logo are registered trademarks of SWsoft.

RedHat is a registered trademark of Red Hat Software, Inc.

Solaris is a registered trademark of Sun Microsystems, Inc.

X Window System is a registered trademark of X Consortium, Inc.

UNIX is a registered trademark of The Open Group.

Intel, Pentium, and Celeron are registered trademarks of Intel Corporation.

MS Windows, Windows 2003 Server, Windows XP, Windows 2000, Windows NT, Windows 98, and Windows 95 are registered trademarks of Microsoft Corporation.

IBM DB2 is a registered trademark of International Business Machines Corp.

SSH and Secure Shell are trademarks of SSH Communications Security, Inc.

MegaRAID is a registered trademark of American Megatrends, Inc.

PowerEdge is a trademark of Dell Computer Corporation.

Request Tracker is a trademark of Best Practical Solutions, LLC

All other trademarks and copyrights referred to are the property of their respective owners.

Contents

Preface	4
Typographical Conventions	4
Feedback	5
About Kaspersky Antivirus	6
Installing Kaspersky Antivirus	7
Installing License Key	8
Setting Up Antivirus	9
Setting Up Real-time Virus Scanning	10
Setting Up Filtering of Messages Containing Specific File Types	11
Setting Up Automatic Updates for Virus Definitions	12
Switching Antivirus Scanning On and Off	13
Applying Individual Scanning Settings to Mailboxes	14
Applying Individual Filtering Settings to Mailboxes	15
Managing Antivirus Services	16
Viewing Logs	17
Viewing Virus Statistics	18

Preface

In this section:

Typographical Conventions	4
Feedback	5

Typographical Conventions

Before you start using this guide, it is important to understand the documentation conventions used in it.

The following kinds of formatting in the text identify special information.

Formatting convention	Type of Information	Example
Special Bold	Items you must select, such as menu options, command buttons, or items in a list.	Go to the System tab.
	Titles of chapters, sections, and subsections.	Read the Basic Administration chapter.
<i>Italics</i>	Used to emphasize the importance of a point, to introduce a term or to designate a command line placeholder, which is to be replaced with a real name or value.	The system supports the so called <i>wildcard character</i> search.
Monospace	The names of commands, files, and directories.	The license file is located in the http://docs/common/licenses directory.
Preformatted	On-screen computer output in your command-line sessions; source code in XML, C++, or other programming languages.	<pre># ls -al /files total 14470</pre>
Preformatted Bold	What you type, contrasted with on-screen computer output.	<pre># cd /root/rpms/php</pre>
CAPITALS	Names of keys on the keyboard.	SHIFT, CTRL, ALT

KEY+KEY	Key combinations for which the user must press and hold down one key and then press another.	CTRL+P, ALT+F4
---------	--	----------------

Feedback

If you have found a mistake in this guide, or if you have suggestions or ideas on how to improve this guide, please send your feedback to userdocs@swsoft.com. Please include in your report the guide's title, chapter and section titles, and the fragment of text in which you have found an error.

About Kaspersky Antivirus

Kaspersky Antivirus is a program that scans incoming and outgoing mail traffic on your server, and removes malicious and potentially dangerous code from e-mail messages. What makes it an effective solution is that its virus databases are updated with new virus definitions every hour.

To learn more about Kaspersky Antivirus, visit the Web site at http://www.kaspersky.com/anti-virus_linux_mailserver.

To use Kaspersky Antivirus with your Plesk server, you need to install the Kaspersky Antivirus module, purchase a license key and install it through Plesk control panel.

Installing Kaspersky Antivirus

You can install the Kaspersky Antivirus module to the Plesk server in two ways: from the control panel (recommended), and from the command line.

➤ *To install Kaspersky Antivirus through the control panel:*

- 1 Login as administrator to the control panel.
- 2 Select the **Modules** shortcut in the navigation pane
- 3 Click **Manage Modules**.
- 4 Click **Add new module**.
- 5 Select a module package file, and click **OK**.

➤ *To install Kaspersky Antivirus through the command line:*

- 1 Login as root to the server, where Plesk is installed.
- 2 Run the command
`/plesk_installation_directory/admin/bin/modulemng --install --file=<kaspersky_antivirus_module_filename>`,
where 'plesk_installation_directory' is the directory you installed Plesk to.

Example:

```
/usr/local/psa/admin/bin/modulemng --install --file=/opt/modules/kav.rpm
```

Note: Kaspersky Antivirus module and other modules that come with Plesk are located in the directory `/opt/modules` of Plesk distribution.


In this chapter:

Installing License Key..... 8

Installing License Key

- *To obtain and install a license key for Kaspersky Antivirus:*
- 1 Click the **Server** shortcut in the navigation pane.
 - 2 Click the **License Management** icon in the **System** group.
 - 3 Click **Order New Key**. The SWsoft online store page listing available add-ons opens in a new browser window.
 - 4 On this page, select the check box next to the Kaspersky Antivirus item and click **ADD TO MY BASKET**.
 - 5 Because Plesk add-ons are added to the license keys that already exist, the Plesk Number Checking System page will open. Enter the number of your license key to which you add this feature and click **Submit**.
 - 6 In the next steps, indicate the currency, number of keys, provide contact details, billing address, and payment method, and submit the form. You will be notified by e-mail when your order is processed.

When you receive the e-mail notice, return to the **License Management** screen (**Server >**

License Management) and click  **Retrieve Keys** to retrieve the ordered license key. Plesk License Manager will retrieve the upgraded license key from the SWsoft licensing server and automatically install it to your control panel.

Setting Up Antivirus

After you installed the module and license key, configure antivirus protection and set up automatic updates. You can set the default administrative settings that will apply to all mail accounts on your server, and you can let your users set individual settings for their mail accounts.

In this chapter:

Setting Up Real-time Virus Scanning	10
Setting Up Filtering of Messages Containing Specific File Types	11
Setting Up Automatic Updates for Virus Definitions	12

Setting Up Real-time Virus Scanning

- *To set up virus scanning:*
- 1 Go to **Server > Mail**.
 - 2 In the **Antivirus preferences** group, select the **Kaspersky Antivirus** option. Click **OK**.
 - 3 Go to **Modules > Kaspersky Antivirus**, and click the **Antivirus Engine** link.
 - 4 From the **Use the following set of virus definitions** menu, select the **Extended** item. Compared to the standard set, the extended set contains definitions for different types of malicious code (malware) other than viruses.
 - 5 Under the **Log Settings** group, specify where scanning report should be located and what amount of information should be presented in the report. Click **OK**.
 - 6 Go to **Modules > Kaspersky Antivirus > Server-wide Scanning Settings** tab.
 - 7 To specify what type of mail (incoming, outgoing or both) to scan for viruses, select the respective option from the **Server-wide scanning settings** menu.
 - 8 To allow your users to set individual virus protection settings for their mailboxes, select the **Allow users to customize scanning settings** check box.
 - 9 To specify what to do with infected messages, click **Scanning settings**, and specify the following:
 - a **Add X-header to e-mail**. Leave this selected if you want Kaspersky Antivirus to add headers to scanned e-mail messages. These headers can be used for filtering mail by mail programs.
 - b **Administrator's e-mail**. Specify your e-mail if you want to receive scanning reports.
 - c **Quarantine path**. If you want antivirus to move infected messages to a quarantine directory after disinfection, specify the path to this directory.
 - d **Actions on scanning completed**. Use the items in the **Infected** row to specify what antivirus should do when an infected message is detected.
 - To move such a message with attached file to the quarantine directory, select the **Move object to quarantine** check box.
 - To send a notice to the message sender, select a check box under the **Notify sender** column.
 - To send a notice with the original message to the recipient: under the **Send to recipient** column, select the notice and attach original mail check boxes, and then specify what to do to the attached malicious code by selecting an item from the menu under the **object** column.
 - If you want to send a notice to the administrative address you previously specified, select the respective items under the **Send to administrator** column.

Note: Here you can also specify what to do about the following categories of messages: messages from which malicious code was removed by Kaspersky Antivirus (**Cured** row); messages suspected of being infected with an unknown virus (**Suspicious** row); messages that contain corrupted files (**Corrupted** row); messages that contain code that resembles a known virus (**Warning** row); messages that could not be scanned because antivirus service was stopped or failed due to an internal error (**Error** row); messages that contained password-protected files (**Protected** row).

10 Click **OK** to save the settings.

Now antivirus scans all mail in accordance with the settings you defined.

If want to set individual settings for a mailbox, refer to the chapter Applying Individual Scanning Settings for Mailboxes (on page 14).

Setting Up Filtering of Messages Containing Specific File Types

In addition to scanning mail for viruses, you can set up Kaspersky Antivirus to filter attached files with specific file name extensions or MIME-types. You can specify the file types that must be delivered without scanning and the file types that must not be scanned and delivered to recipients.

➤ **To specify file types that must not be scanned and delivered:**

- 1** Go to **Modules > Kaspersky Antivirus > Server-wide Scanning Settings > Scanning Settings > Filtering Settings** tab.
- 2** Under the **Black list** group, type the file name extensions or MIME-types, separating them with a coma and a white space.
For example, to filter Windows executable files, specify either `.*\ .exe$` in the **File name** box, or `application/binary` in the **MIME-type** box.
- 3** Specify what to do when the messages containing the blacklisted files arrive: you can choose to remove the message with attachment, move it to quarantine for further inspection, and send the respective notices to sender, recipient, or server administrator.
- 4** To save the settings, click **OK**.

➤ **To specify file types that must be delivered without scanning:**



- 1** Go to **Modules > Kaspersky Antivirus > Server-wide Scanning Settings > Scanning Settings > Filtering Settings** tab.
- 2** Under the **White list** group, type the file name extensions or MIME-types, separating them with a coma and a white space. For example, if you do not want antivirus to scan messages that have attached Microsoft Word documents, specify `.*\ .doc$` in the **File name** box.

- 3 Click **OK** to save the settings.

Setting Up Automatic Updates for Virus Definitions

By default, antivirus is set to update its virus definitions once per day. Updates are downloaded from the official updates server at Kaspersky Labs, which is located in Russia.

➤ *If you want to retrieve updates from another location, or if you want to change the updating schedule:*

- 1 Go to **Modules > Kaspersky Antivirus**. A list of Kaspersky Antivirus services opens.
- 2 Ensure that the updating service is running: the icon  shows to the left of the **KeepUp2Date** link. If not, click the respective  icon.
- 3 In the list of services, click the **KeepUp2Date** link.
- 4 Specify the new updating settings as required, and click **OK** to save the settings.

Switching Antivirus Scanning On and Off

➤ *To switch on server-wide antivirus scanning:*

- 1 Go to **Modules > Kaspersky Antivirus > Server-wide Scanning Settings** tab.
- 2 From the **Server-wide scanning settings** menu, select the type of mail (incoming, outgoing or both) to scan for viruses.
- 3 Click **OK**.

➤ *To switch off server-wide antivirus scanning:*

- 1 Go to **Modules > Kaspersky Antivirus > Server-wide Scanning Settings** tab.
- 2 From the **Server-wide scanning settings** menu, select the **Scanning disabled** option.
- 3 Click **OK**.

Applying Individual Scanning Settings to Mailboxes

- *To apply individual scanning settings to a mailbox:*
- 1 Go to **Domains > domain name > Mail > mail account > Antivirus**.
 - 2 Under **Antivirus preferences**, specify what type of mail to scan for viruses: incoming, outgoing, or both.
 - 3 To specify what to do with infected messages, click **Scanning settings**, and specify the following:
 - a **Add X-header to e-mail**. Leave this selected if you want Kaspersky Antivirus to add headers to scanned e-mail messages. These headers can be used for filtering mail by mail programs.
 - b **Administrator's e-mail**. Specify your e-mail if you want to receive scanning reports.
 - c **Quarantine path**. If you want antivirus to move infected messages to a quarantine directory after disinfection, specify the path to this directory.
 - d **Actions on scanning completed**. Use the items in the **Infected** row to specify what antivirus should do when an infected message is detected.
 - To move such a message with attached file to the quarantine directory, select the **Move object to quarantine** check box.
 - To send a notice to the message sender, select a check box under the **Notify sender** column.
 - To send a notice with the original message to the recipient: under the **Send to recipient** column, select the notice and attach original mail check boxes, and then specify what to do to the attached malicious code by selecting an item from the menu under the **object** column.
 - If you want to send a notice to the administrative address you previously specified, select the respective items under the **Send to administrator** column.
-
- Note:** Here you can also specify what to do about the following categories of messages: messages from which malicious code was removed by Kaspersky Antivirus (**Cured** row); messages suspected of being infected with an unknown virus (**Suspicious** row); messages that contain corrupted files (**Corrupted** row); messages that contain code that resembles a known virus (**Warning** row); messages that could not be scanned because antivirus service was stopped or failed due to an internal error (**Error** row); messages that contained password-protected files (**Protected** row).
-
- 4 Click **OK** to save the settings.

Now antivirus scans all mail coming to and from this mailbox in accordance with the settings you defined.

Applying Individual Filtering Settings to Mailboxes

- *To specify file types that must not be scanned and delivered:*
 - 1 Go to **Domains > domain name > Mail > mail account > Antivirus Scanning Settings > Filtering Settings** tab.
 - 2 Under the **Black list** group, type the file name extensions or MIME-types, separating them with a comma and a white space.
For example, to filter Windows executable files, specify either `.*\ .exe$` in the **File name** box, or `application/binary` in the **MIME-type** box.
 - 3 Specify what to do when the messages containing the blacklisted files arrive: you can choose to remove the message with attachment, move it to quarantine for further inspection, and send the respective notices to sender, recipient, or server administrator.
 - 4 To save the settings, click **OK**.

- *To specify file types that must be delivered without scanning:*
 - 1 Go to **Domains > domain name > Mail > mail account > Antivirus > Scanning Settings > Filtering Settings** tab.
 - 2 Under the **White list** group, type the file name extensions or MIME-types, separating them with a comma and a white space. For example, if you do not want antivirus to scan messages that have attached Microsoft Word documents, specify `.*\ .doc$` in the **File name** box.
 - 3 Click **OK** to save the settings.

Managing Antivirus Services



Kaspersky Antivirus deploys and uses the following services on your system:

- SMTP Scanner
- Kaspersky Antivirus Engine
- KeepUp2Date

SMTP scanner and Kaspersky Antivirus Engine check the mail for viruses and provide mail filtering. The KeepUp2Date service retrieves and installs updates for virus definitions.

➤ **To view the status of these services and start, stop or restart them if required:**

- 1 Go to **Modules > Kaspersky Antivirus**. A list of services opens.




An icon in the **S** (status) column shows  if a service is running, and  if a service is stopped.

Note:

To view the real-time mail scanning log, click an icon in the L column to the left of the **SMTP Scanner** link.

To view the log for virus definitions updates, click an icon in the L column to the left of the **KeepUp2Date** link.

To view the information about the number of virus definitions and license keys used, click an icon in the L column to the left of the **Kaspersky Antivirus Engine** link.

- 2 To start, stop, or restart a service, click the icon , , or , respectively.

In this chapter:

Viewing Logs..... 17

Viewing Logs

➤ *To view the real-time mail scanning log:*

- 1 Go to **Modules > Kaspersky Antivirus**.
- 2 Click the **SMTP Scanner** link.
- 3 Under the **Tools** group, click **View Log**.
- 4 To specify the number of last log entries you want to view, type the number into the respective box and click **Apply**.
- 5 To update the information on the screen, click **Refresh**.
- 6 To remove all log entries, click **Clear Log**.

➤ *To view the log for virus definitions updates:*

- 1 Go to **Modules > Kaspersky Antivirus**.
- 2 Click the **KeepUp2Date** link.
- 3 Under the **Tools** group, click **View Log**.
- 4 To specify the number of last log entries you want to view, type the number into the respective box and click **Apply**.
- 5 To update the information on the screen, click **Refresh**.
- 6 To remove all log entries, click **Clear Log**.

➤ *To view the information about the number of virus definitions and license keys used:*

- 1 Go to **Modules > Kaspersky Antivirus**.
- 2 Click the **Kaspersky Antivirus Engine** link.
- 3 Under the **Tools** group, click **View Log**.
- 4 To specify the number of last log entries you want to view, type the number into the respective box and click **Apply**.
- 5 To update the information on the screen, click **Refresh**.
- 6 To remove all log entries, click **Clear Log**.

Viewing Virus Statistics

- *To view the information about viruses detected and removed by Kaspersky Antivirus:*
 - 1 Go to **Modules > Kaspersky Antivirus**.
 - 2 Click **Virus Statistics**.
 - 3 Select the period for which you want to view virus statistics.
 - 4 If you want to view more detailed information about viruses, or e-mail addresses of e-mail senders or recipients, click the respective tab.