
New features of Kaspersky Anti-Virus for Unix

Version 4.0.0.0

Keeper

In order to correctly perform checking of the mail traffic it is required to load the following programs before the mailer's start: *kavdaemon*, *kavucc*, *kavkeeper*. At that the *kavdaemon* and the *kavucc* programs must be started before *kavkeeper*.

Scanner and Daemon

1. New command line switches:

-AE[-]

disables extraction of self-extracting archives.

-AS[-]

disables checking for viruses in OLE objects embedded in examined files.

2. The **-W[file path]** option is extended. Now you can define an absolute or relative path to the required log file.
3. There is a new feature allowing you to include or exclude links from the location to be scanned (the **[Object]** section **Names** parameter in the *defUnix.prf* file). The links processing rules are defined by the **[Options]** section **Symlincs** parameter.

For example, if the **[Object]** section **Names** parameter of the *defUnix.prf* file enables the program to scan the **/home/user/mydoc** link, and **Symlincs=0**, the files and folders available via this link will be ignored.

Version 4.0.0.1

Updater

New command line switches:

-g[=base]

specifies the database named **base** to be used as storage for the program performance settings. The default setting is **base=defUnix**.

-gd[q]

sets the program to save settings that follow this switch to the default database. **q** is an optional element that defines whether to launch the Updater program during this session or not. More precisely:

- **-gdq** saves the defined settings to the default database and disables the program start;
- **-gd** saves the defined settings to the default database and starts the program with these settings.

For example, if you enter the following on your command line:

```
./kavupdater -gd  
-uik=http://www.kaspersky.com/updates -ws
```

the program will start updating anti-virus databases from the specified URL, whereupon the results will be saved to the system log.

If next time you start the program by using the following string in the command line:

```
./kavupdater
```

the updating operation will be performed from **http://www.kaspersky.com/updates** (the URL defined previously), and the program performance results will be saved to the system log. This URL will be used because the **gd** command line switch specified during the previous start saved the program performance settings to the default database.

-l[q]

displays settings defined in the command line after this switch on your screen. **q** is an optional element that defines whether to launch the Updater program during this session or not. More precisely:

- **-lq** displays the defined settings on your screen and disables the database updating operation;
- **-l** displays the defined settings on your screen and starts the Updater program.

Version 4.0.1.0

Daemon

1. New extension for the socket writing mode 3. This mode allows the program to write command strings to a socket during the check and is used if the objects are checked without being intermediately saved onto the disk. Now this command line parameter may include the file name and looks similar to the following:

```
<3>date_and_time:<switch|length|filename>
```

where:

- | – is the section separator;
- switch** is the value acquired using the **ftok()** function;
- length** is the size of the shared memory;
- filename** is the name of the file to be checked.



This extension allows you to be more specific about the examined objects to be logged. You can also use the switch without this extension, i.e. omit the file name in the command line!

2. The **CopyEqual** parameter is added to the following *defUnix.prf* file sections: **[ActionWithInfected]**, **[ActionWithCorrupted]** and **[ActionWithSuspicion]**. The **Yes** value in this line enables the program to copy temporary files with identical names by appending appropriate **sequence number to the file name**.

Version 4.0.2.0

All programs

Access to the program settings' database and multi-user access locking are implemented.

Control Centre

New command line switches:

-r[=[hostname:]port]

allows management of the Control Centre program from a remote computer.

-ms=server

defines the server from which the traffic quota depletion notifications will be sent.

-mf=from

defines the address from which the traffic quota depletion notifications will be sent.

-mt=to

defines the destination address for the traffic quota depletion notifications.

-mat=Mb

defines the traffic quota in Mb.

**-cp[w]="prgname -a:arg[:arg1[...]] -u=username
-e=hour:min"**

starts the **prgname** program with the defined settings,

where:

prgname is the name of the **prgname** program executable file.

-a:arg[:arg1[...]] is the **prgname** program performance settings.

-u=username is the user name under which the **prgname** program should be started.

-e=hour:min is the **prgname** program performance time. When this time expires the program will be closed.

w an the optional element that activates program termination waiting mode, and screens and logs the program exit code.

-cpt

verifies whether the **prgname** program was started by the **-cp[w]** command line switch.

-cpk

terminates execution of the **prgname** program started by the **-cp[w]** command line switch.

Keeper

New features of the **kldbedit** utility. Now you can import the binary database with Keeper settings into a text file, then edit it

and export again into the binary format. This mode of operation does not require use of the WebTuner program.

Version 4.0.2.1

Scanner and Daemon

1. A new value can be assigned to the **[ActionWithInfected]** section **InfectedFiles** parameter of the *defUnix.prf* file. 4 in the **InfectedFiles** line allows you to rename infected files, if you preset the program to copy these files to the directory defined in the **InfectedFlder** line. Also, renaming the program changes the file extension to the one defined in the **ChangeExt** line.
2. New command line switch - **-I4** – allows you to implement the above described function on the command line.
3. New section is added to the *defUnix.prf* profile. This section is named **[Mail]** and includes the following notification settings:

SendMail – enables the program to notify about infected objects detected. Type Yes to enable notifications, or No to disable them.

SendOnEach – notifies about every infected object separately. Type Yes to enable notifications, or No to disable them.

SendAtEnd – notifies about all the infected objects detected. Type Yes to enable notifications, or No to disable them.



The **SendOnEach** and **SendAtEnd** modes are mutually exclusive and cannot be both enabled.

SMTPServer – defines the smtp server, from which the notifications will be sent. The general form of the string is:
smtp:server_name.domain.ru(com and etc.)

SendFrom – defines the address, from which the notifications will be sent.

SendTo – defines the destination address for the notifications. You may use the address mask in this line.

CC – defines the destination addresses for the notification copies.

For example, this section may look similar to the following:

```
[Mail]
SendMail=Yes
SendOnEach=Yes
SendAtEnd=No
SMTPServer=smtp:anton.localhost.ru
SendFrom=anton@localhost.ru
```

```
SendTo=*@mydomain.com  
CC=admin@mydomain.com
```

WebTuner and Keeper

New macroinstructions can be used to create notifications for administrators, senders and recipients:

- **%SENDER%** – inserts the infected message sender address in the notification text.
- **%RECIPIENT%** – inserts the infected message recipient address in the notification text.
- **%KAVANSWER%** – inserts the infected-message-detected report from Daemon in the notification text.

Version 4.0.2.2

All programs

Now when you display the performance report file the program searches for the file with the same name. This feature is implemented to avoid the data loss resulting from use of the name of an existing report file for the new report file.

Updater

New command line switches:

-gu

cleans the configuration database.

-gdu

saves the program performance settings to the configuration database with pre-cleaning of this database.

Version 4.0.4.0

Daemon

1. Daemon can be started from the command line as well as from the */etc/rc.d/init.d/kavd* startup file. This file allows you to automatically start the daemon process every time your system is started. To enable the automatic start of your daemon process, you should place the *kavd* script in the */etc/rc.d/init.d/* directory and add the corresponding symbolic

link (using the *ntsysv* and *chkconfig* utilities, or the `ln -s` command) to the required startup level.

2. For the daemon process to automatically disinfect infected objects, you should specify the `-I2` switch in the command line or in the *kavd* script-file (the **DPARMS** parameter) respectively.

Keeper

Keeper is a client of the daemon process and uses the Daemon program to disinfect infected messages (their bodies and attachments), therefore in order to disinfect infected messages you should set the Daemon program the appropriate way. The following operation sequences can be suggested:

Alternative 1: if your Daemon was started from the command line, you should:

1. stop your mailing system;
2. kill all the daemon processes:
/kavdaemon -ka
3. redefine the Keeper settings using the WebTuner or the *kldbedit* utilities (for details see the corresponding User Guides: Kaspersky Anti-Virus for Linux/Sun Solaris/xBSD Mail Server);
4. start the Daemon program with the disinfection feature enabled:
/kavdaemon -I2
5. start Keeper;
6. start your mailing system.

Alternative 2: if your Daemon was started using the `/etc/rc.d/init.d/kavd` script at the system start, you should:

1. define the following switch in the `/etc/rc.d/init.d/kavd` file:
DPARMS="-I2"
2. redefine the Keeper settings using the WebTuner or the *kldbedit* utilities (for details see the corresponding User Guides: Kaspersky Anti-Virus for Linux/Sun Solaris/xBSD Mail Server);
3. restart your operating system.