



User Manual

Milter for Sendmail

**Security Solutions
for companies and professional users**



DATENTECHNIK GMBH

Table of contents

1	Introduction	1
1.1	Target groups	1
1.2	Functionality of AntiVir Milter for Linux	1
2	Integrating AntiVir Milter in sendmail	2
2.1	Condition	2
2.2	Integration	2
3	Installing AntiVir Milter	4
3.1	Condition	4
3.2	Installation	4
4	Configuring AntiVir Milter	9
4.1	Functioning of AntiVir Milter	9
4.2	Setting the configuration in avmilter.conf	10
5	Configuring automatic updates	18
5.1	Settings in antivir.conf	18
5.2	AntiVir PGP Public Key - antivir.gpg	19
6	Virus-specific warnings: file avmilter.warn	21
7	Notification templates	22

1 Introduction

1.1 Target groups

This user manual is intended for all users of AntiVir Milter. It contains information for everyone from technically experienced lay people up to the administrator. Basic knowledge of Linux is required in any case.

1.2 Functionality of AntiVir Milter for Linux

AntiVir Milter is a plug-in for sendmail versions 8.11 and up and communicates via the libmilter interface of sendmail.

AntiVir Milter checks all incoming and outgoing emails. Infected emails are blocked. A status message is written to "syslog". The sender, receiver and administrator can be informed about infections.

Functions:

- All sendmail functions can still be used.
Example: SMTP authentication, anti-relaying, anti-spam
- Easy installation and integration into sendmail
- Hourly or daily update of the scan engine and the virus definition file via the Internet
- Checking of incoming and outgoing mails
- Dependable detection of viruses and unwanted programs in real time
- Configurable response to a detected virus or unwanted program
- Isolation of infected and suspicious files in a quarantine directory
- Log file can be used as a protocol via mail traffic
- Immediate activation, if new virus definition file (.vdf) is available
- Heuristic macro-virus detection
- Modifiable templates to create own alert messages
- Scanning in archives (the number of supported archive formats is displayed with `antivir --version`)

2 Integrating AntiVir Milter in sendmail

2.1 Condition

A version of sendmail equal to or greater than 8.11 with the libmilter interface must be present.

If this is not the case:

- ⇒ Read the README file in the libmilter folder in the sendmail package (<http://www.sendmail.org>).
- ⇒ Compile a new version of sendmail with the libmilter interface.

2.2 Integration

AntiVir Milter can then be inserted into the configuration file of sendmail, sendmail.cf, in two ways:

- Editing sendmail.cf directly
- or
- Generating sendmail.cf

2.2.1 Editing sendmail.cf directly

⇒ Enter the following two lines into sendmail.cf:

```
Xavmilter, S=inet:3333@localhost, F=R, T=S:10m;R:10m;E:10m
O InputMailFilters=avmilter
```

2.2.2 Generating sendmail.cf

⇒ Enter the relevant lines into the sendmail.mc file:

with sendmail 8.11.x:

```
define(`_FFR_MILTER', `true')
INPUT_MAIL_FILTER(`avmilter',`S=inet:3333@localhost, F=R,
T=S:10m;R:10m;E:10m')
```

with sendmail 8.12.x:

```
INPUT_MAIL_FILTER(`avmilter',`S=inet:3333@localhost, F=R,
T=S:10m;R:10m;E:10m')
```

⇒ Generate the file sendmail.cf.

Example:

```
m4 sendmail.mc > /etc/mail/sendmail.cf
```

2.2.3 Additional information

When configuring sendmail, we only offer support for problems directly related to AntiVir Milter.

Additional information can be found at <http://www.sendmail.org>.

Information on the libmilter interface can be found at <http://www.milter.org>.

3 Installing AntiVir Milter

3.1 Condition

A version of sendmail equal to or greater than 8.11 with the libmilter interface must be present (see chapter 2.1).

If you wish to check whether sendmail has been compiled with libmilter support:

```
sendmail -d0.10 < /dev/null | grep MILTER
```

3.2 Installation

3.2.1 Selecting the AntiVir Milter package

The names of the AntiVir Milter package is dependent on the operating system:

- Free-BSD: avfbmlt.tgz
- Open-BSD: avobmlt.tgz
- Linux: avlxmlt.tgz

In the following we will describe the installation using a linux system.

3.2.2 Extracting files

⇒ Extract the avlxmlt.tgz file.

```
tar xzvf avlxmlt.tgz
```

A subdirectory antivir-milter-x.x.x is created (x.x.x represents the current version number).

⇒ Switch to the antivir-milter-x.x.x subdirectory:

```
cd antivir-milter-x.x.x
```

3.2.3 Creating directories and copying files

⇒ Create the folder /usr/lib/AntiVir/. Copy the file vdf/antivir.vdf to the folder /usr/lib/AntiVir/. Ensure that the capitalization of the word "AntiVir" is correct here:

```
mkdir /usr/lib/AntiVir  
cp vdf/antivir.vdf /usr/lib/AntiVir/
```

⇒ Change user to uucp:

```
chown uucp:antivir /usr/lib/AntiVir  
chown uucp:antivir /usr/lib/AntiVir/antivir.vdf
```

⇒ Change group to antivir:

```
chown uucp:antivir /usr/lib/AntiVir
chown uucp:antivir /usr/lib/AntiVir/antivir.vdf
```

⇒ Copy the scan engine bin/antivir to folder /usr/lib/AntiVir.

```
cp bin/antivir /usr/lib/AntiVir
```

⇒ Change users to uucp:

```
chown uucp:antivir /usr/lib/AntiVir/antivir
```

⇒ Change group to antivir:

```
chown uucp:antivir /usr/lib/AntiVir/antivir
```

⇒ Copy files avmilter.conf and antivir.conf to folder /etc:

```
cp etc/avmilter.conf /etc/
cp etc/antivir.conf /etc/
```

⇒ Copy program file bin/avmilter to folder /usr/sbin/:

```
cp bin/avmilter /usr/sbin/
```

⇒ Create a spool folder (preset: /var/spool/avmilter). This folder may only be accessible to antivir or the user specified in /etc/avmilter.conf:

```
mkdir /var/spool/avmilter
cd /var/spool/avmilter/
mkdir incoming
mkdir outgoing
mkdir rejected
chown -R uucp:antivir var/spool/avmilter
chmod -R 700 var/spool/avmilter
```

3.2.4 Copying the license file

If you have a license for commercial or private use:

⇒ Copy the license file hbedv.key to the folder /usr/lib/AntiVir/avmilter.key:

```
cp hbedv.key /usr/lib/AntiVir/avmilter.key
chown uucp:antivir /usr/lib/AntiVir/avmilter.key
chmod 440 /usr/lib/AntiVir/avmilter.key
```

Without a digital licence key, AntiVir Milter is running in demo mode. The following note is then added to the reference line of each e-mail:

- Checked by AntiVir DEMO version -

3.2.5 Integrating AntiVir Milter into sendmail

Edit the configuration file `sendmail.cf` (see chapter 2).

3.2.6 Starting programs

⇒ Start AntiVir Milter with command line options:

```
/usr/sbin/avmilter -p inet:3333@localhost
```

or

⇒ Start AntiVir Milter without command line options:

```
/usr/sbin/avmilter
```

A prerequisite for this input is that you entered `inet:3333@localhost` in parameter `ListenAddress` of `avmilter.conf`.

Another option to let AntiVir Milter communicate with sendmail is the following:

⇒ Start AntiVir Milter with command line options:

```
/usr/sbin/avmilter -p unix:/path/to/file
```

or

⇒ Start AntiVir Milter without command line options:

```
/usr/sbin/avmilter
```

A prerequisite for this input is that you entered `unix:/path/to/file` in parameter `ListenAddress` of `avmilter.conf`.

Note:

If AntiVir Milter is started with the `inet:` option, an internet socket will be used for communication.

If AntiVir Milter is started with the `unix:` option, a local socket will be used.

⇒ Restart sendmail (with SuSE):

```
rcsendmail restart
```

or

```
killall -HUP sendmail
```

3.2.7 Defining further command line options

- ⇒ If required, enter the path to the config files with `-P`:

```
avmilter -P /path/to/configfiles/
```

- ⇒ If required, enter the path to single files:

```
avmilter -W /path/to/milterfiles/avmilter.warn
```

```
avmilter -S /path/to/milterfiles/avmilter.scan
```

```
avmilter -I /path/to/milterfiles/avmilter.ignore
```

```
avmilter -C /path/to/milterfiles/avmilter.conf
```

- ⇒ If you wish detailed entries in the syslog, you can activate the debug mode (level 1–5):

```
avmilter -D5
```

- ⇒ If emails still stored in the Incoming and Outgoing folder are to be processed by AntiVir Milter (**start AntiVir Milter first!**):

```
avmilter -f
```

3.2.8 Automating updates

The periodical execution of updates is controlled via the cron daemon.

- ⇒ Make the corresponding entry in the file `/etc/crontab`.

Example: Add the following line for a hourly update at e.g. 11:00 p.m.:

```
23 * * * * root /usr/lib/AntiVir/antivir --update -q
```

- ⇒ When using a proxy server: Enter the server name and connection in the file `/etc/antivir.conf` (see chapter 5.1).

- ⇒ Test update settings by starting:

```
/usr/lib/AntiVir/antivir --update -q
```

When executed successfully, a message from AntiVir Milter with the scan engine version and VDF version is present in the log file `/var/log/mail`, `/var/log/maillog` or `/var/log/mail.log`.

3.2.9 Checking access authorization

If you change the user and group parameters in `avmilter.conf` (see chapter 4.2):

⇒ Ensure that the following files have the same access authorization:

```
/usr/lib/AntiVir/antivir  
/usr/lib/AntiVir/antivir.vdf  
/usr/lib/AntiVir/avmilter.key
```

⇒ Ensure that the following folders have the same access authorization and that they are accessible to the users or groups defined in `avmilter.conf`:

```
/usr/lib/AntiVir/  
/var/spool/avmilter/  
/var/spool/avmilter/incoming/  
/var/spool/avmilter/outgoing/  
/var/spool/avmilter/rejected/
```

4 Configuring AntiVir Milter

4.1 Functioning of AntiVir Milter

AntiVir Milter ensures that any infected emails are separated from the others ("quarantined") and, depending on the configuration, notifies the user that the virus or unwanted program has cropped up. This method of operation can be set via the file `avmilter.conf`.

AntiVir Milter generates an internal message ID for each email.

First, two files are stored in the directory `incoming`. This directory can be found in the directory specified in `SpoolDir` (default setting: `/var/spool/avmilter`):

- `df-Message-ID`: data file containing the email
- `qf-Message-ID`: control file containing the meta information on the email and indicating that the email is ready for a check for viruses or unwanted programs.

If AntiVir Milter finds a virus or unwanted program, these files are moved to the directory `rejected`. This directory can be found in the directory specified in `SpoolDir` (default setting: `/var/spool/avmilter`). In doing so, the control file `qf-Message-ID` is renamed as:

- `vf-Message-ID` (if the email contains a virus or unwanted program)
- `mf-Message-ID` (if a MIME problem has occurred with the email).

If an infection is present, the following files can be ultimately found in the respective directory (default setting: `/var/spool/avmilter/rejected/`):

- `df-Message-ID`
- `vf-Message-ID` or `mf-Message-ID`

External programs or scripts can access these files, for example by using the `ExternalProgram` directive in `avmilter.conf` (see chapter 4.2).

4.2 Setting the configuration in avmilter.conf

The file `avmilter.conf` contains settable parameters effecting the functioning of AntiVir Milter. Lines beginning with `#` are comments or commands which have been commented out. If parameters are not specified, the standard settings of the following list are used.

User, Group

AntiVir Milter starts under the following user and group:

User	uucp
Group	antivir

If these settings are changed, the access authorization to the affected directories and files must be likewise reset (see chapter 3.2.9).

Postmaster

Receives error messages and alarms on viruses and unwanted programs:

Postmaster	postmaster
------------	------------

MyHostName

FQDN (Fully Qualified Domain Name) of the local host.

The default setting, if not defined in the configuration file, is the hostname returned by `gethostname(2)`. If this fails, "localhost" is set:

MyHostName	localhost
------------	-----------

SpoolDir

Spool directory of AntiVir Milter. During processing, emails are placed in the subdirectories incoming, rejected and outgoing (see chapter 4.1).

The SpoolDir must be owned by User:Group (as specified above) and must be accessible to only this user (mode = 0700):

SpoolDir	/var/spool/avmilter
----------	---------------------

AntiVirDir

The directory where the AntiVir main program, the virus definition file `antivir.vdf`, and the license key are stored:

AntiVirDir	/usr/lib/AntiVir
------------	------------------

TemporaryDir

The directory where the temporary files are stored (for example, attachments while being checked for viruses and unwanted programs). It needs enough space to hold uncompressed attachments for each forwarder:

```
TemporaryDir          /var/tmp
```

or

```
TemporaryDir          /tmp
```

ListenAddress

To start AntiVir Milter without command line options, you can for example enter `inet:3333@localhost` or `unix:/path/to/file` here.

```
ListenAddress          inet:3333@localhost
```

or

```
ListenAddress          unix:/path/to/file
```

ForwardTo

Selects the binary of sendmail and the arguments for how to call sendmail:

```
ForwardTo              /usr/lib/sendmail -oem -oi
```

MaxAttachments

Sets the maximum number of attachments allowed for a single MIME mail:

```
MaxAttachments         100
```

BlockSuspiciousMime

Stops delivery of "suspicious" MIME mails. A MIME mail is considered "suspicious" if `MaxNestingLevel` or `MaxAttachments` (see above) has been reached:

```
BlockSuspiciousMime    NO
```

BlockFragmentedMessage

Blocks mails which are delivered as a fragmented message.

(For further information see "Message Fragmentation and Reassembly", RFC 2046, <http://www.faqs.org/rfcs/rfc2046.html>, chapter 5.2.2.1):

```
BlockFragmentedMessage NO
```

ExposeRecipientAlerts

Sends alerts on viruses and unwanted programs to recipient(s):

```
ExposeRecipientAlerts  NO
```

ExposeSenderAlerts

Sends alerts on viruses and unwanted programs to sender:

ExposeSenderAlerts NO

ExposePostmasterAlerts

Sends alerts on viruses and unwanted programs to postmaster (only available in commercial mode):

ExposePostmasterAlerts YES

AlertsUser

User name or mail address of sender of alerts (if viruses or unwanted programs were found in a mail):

AlertsUser AntiVir

or

AlertsUser AntiVir@mailserver.mydomain.tld

RejectAlertMail

If RejectAlertMail is set to YES, a mail containing a virus or unwanted program will be blocked on SMTP level. The sender receives the message "557 Alert found in mail".

If RejectAlertMail is set to NO, the mail will be accepted and moved to the quarantine directory:

RejectAlertMail NO

QuarantineAlert

If the two options RejectAlertMail and QuarantineAlert are set to YES, an email containing a virus or an unwanted program will be blocked on SMTP level, but stored nevertheless in the directory for rejected emails. Only the postmaster will receive an email message. The sending of an email message is dependent on the settings in the ExposePostmasterAlerts option.

QuarantineAlert YES

ScanInArchive

If ScanInArchive is set to NO, no files in an archive will be scanned.

If ScanInArchive is set to YES, all files in archives will be extracted and scanned, depending on the restrictions given with ArchiveMaxSize, ArchiveMaxRecursion and ArchiveMaxRatio:

ScanInArchive YES

ArchiveMaxSize (old: MaxFileSizeInArchive)

If ArchiveMaxSize is 0, all files in an archive will be unpacked, independent of their unpacked size.

If ArchiveMaxSize is > 0, only files with an unpacked size up to MaxFileSizeInArchive (in bytes) will be unpacked.

Currently, the old notation is still accepted; but future versions will no longer accept it.

```
ArchiveMaxSize          0
```

ArchiveMaxRecursion (old: MaxRecursionDepthInArchive)

If ArchiveMaxRecursion is 0, recursive archives will be unpacked with an unlimited recursion depth.

If ArchiveMaxRecursion is > 0, recursive archives will be unpacked up to the set recursion depth.

Currently, the old notation is still accepted; but future versions will no longer accept it.

```
ArchiveMaxRecursion     20
```

ArchiveMaxRatio

ArchiveMaxRatio stops so-called mail bombs with a very high compression.

If ArchiveMaxRatio is set to 0, this option is turned off. This setting is **not** recommended.

```
ArchiveMaxRatio         150
```

BlockSuspiciousArchive

If BlockSuspiciousArchive is set to YES, delivery of mails can be stopped – depending on the settings in ArchiveMaxSize, ArchiveMaxRecursion, and ArchiveMaxRatio.

If BlockSuspiciousArchive is set to NO, delivery of mails containing archives with a suspicious recursion depth isn't stopped:

```
BlockSuspiciousArchive  NO
```

BlockEncryptedArchive

If BlockEncryptedArchive is set to YES, delivery of mails containing encrypted files in archives is stopped.

If BlockEncryptedArchive is set to NO, delivery of mails containing encrypted files in archives is not stopped:

```
BlockEncryptedArchive   NO
```

AddXHeader

If AddXHeader is set to YES, information about scanning status is added to the header of checked mail. E.g.: "X-AntiVirus: Checked by ..." (only available in commercial mode):

```
AddXHeader          YES
```

ModifySubject

Adds the string "- Checked by AntiVir -" to the existing subject of a mail:

```
ModifySubject        NO
```

ScanTimeout

Specifies the scan time of mail, in seconds, when scanning of mails is stopped:

```
ScanTimeout          300
```

ExternalProgram

Calls external program or script if a virus or unwanted program was found. The argument is the ID of the rejected message (see chapter 4.1):

```
ExternalProgram       /dir/my_own_script
```

NotifyEndOfLicense

If an email message (with default text) is to notify the postmaster a certain number of days before the license expires, this option specifies the number of days (default setting: 10 days). The value 0 switches off this option.

You can also define an individual text for the email message. To do so, the file /etc/avmilter.license has to be defined.

```
NotifyEndOfLicense    10
```

AddressFilter

This option activates/deactivates the address filter. Default setting is NO, i.e. during standard installation no address filter is used.

```
AddressFilter          YES
```

To be able to use the address filter, the following files have to be available:

```
/etc/avmilter.ignore
```

and

```
/etc/avmilter.scan
```

These files contain email addresses (line-by-line), and – optionally – the flags *S/s* (sender address) and/or *R/r* (recipient address). The defined email addresses are checked using the SMTP protocol only (MAIL FROM and RCPT TO). Email addresses in email headers are not taken into account.

Incoming mail is checked if it matches these lists. The list standing first in the FilterTableOrder is checked first. If matches are found, further checking of lists is aborted and the configured action is carried out.

Depending on the result, the following actions are triggered:

- If there is no match to the first list, the next list will be checked.
- If there is still no match, the email will be scanned.
- If there is a match to the ignore list, the email will not be scanned.
- If there is a match to the scan list, the email will be scanned.

The email addresses have to be Perl-compatible, regular expressions, e.g.:

```
/abc/
/^abc/
/xyz/i
/^abc@def\.tld/
```

Example:

/etc/avmilter.ignore contains the following lines:

```
/^someone@somewhere\.tld$/ SR
/^virus@company/ R
/^abc@def.*\.tld/i
```

If the address of the sender or recipient is `someone@somewhere.tld`, the email will not be scanned.

If the address of the recipient is `virus@company*`, , the email will not be scanned. The flag *R* is optional in this case: `/^virus@company/ R` is equivalent to `/^virus@company/`.

When starting AntiVir Milter there will be an entry in maillog indicating whether the address filter is active or not:

```
addressfilter is active
table order is: ignore,scan
```

or

```
addressfilter is not active
```

FilterTableOrder

This option is only relevant if the address filter is active (AddressFilter YES).

Possible parameters:

scan, ignore

or

ignore, scan

AddPrecedenceHeader

This option is exclusively available with a licence for commercial use. If YES is set, the email sent in response to a detected virus will be marked with the string "Precedence: junk". Programs automatically responding to incoming mail (e. g. vacation) will not react to this notification mail. The entry YES or NO can be replaced by an individual text.

AddPrecedenceHeader YES

AddHeaderToNotice

Specifies if the original header of the infected email is to be included into the email message to the postmaster. Possible settings are YES or NO.

AddHeaderToNotice NO

UseProxy

Scans are more efficient if carried out using the Proxy option in SAVAPI, if a defined pool of AV scanners is used. As this pool increases data throughput, the size of the pool has to be exactly defined: Too many scanners need too many resources without an increased performance; an insufficient number of scanners makes the SAVAPI applications wait unefficiently long. Possible settings: YES or NO.

UseProxy NO

ProxyScanners

Number of AV scanners in the pool (see also UseProxy).

ProxyScanners 8

ProxyConnections

Number of maximum permissible simultaneous connections among AntiVir Milter and scanners from the pool.

ProxyConnections 32

LogFile

The LogFile setting has to contain the complete path to the log file. Besides the entries written to the Log file, entries are also send to the syslog.

If LogFile is set to NO, no separate log file is used. However, entries are send to the syslog.

```
LogFile                                /var/log/avmilter.log
```

or

```
LogFile                                NO
```

RejectOnEngineError

If a scanning error occurs, the email will be rejected. Possible settings are YES or NO.

```
RejectOnEngineError                   YES
```

UseTemplates

Specifies whether or not existing templates are to be used. Possible settings are YES and NO (see chapter 7 Notification templates).

```
UseTemplates                          YES
```

5 Configuring automatic updates

With an automatic update those components of AntiVir Milter which ensure protection against viruses and unwanted programs (vdf file and scan engine) are brought up to date.

5.1 Settings in antivir.conf

The file `/etc/antivir.conf` contains settable parameters effecting the automatic update of the scan engine and the virus definition file.

Lines beginning with `#` are comments or commands which have been commented out.

Email Notification

To receive email notifications of updates you must specify the email address to which the notification will be sent. There is no default value for this directive:

```
EmailTo                                root@localhost
```

Logfile

Updates may also be logged to a specified file (in addition to syslog). You must specify the file. There is no default value for this directive:

```
LogTo                                  /var/log/antivir.log
```

Proxy Configuration

If your machine uses an HTTP proxy server, you must specify the proxy configuration settings in order to make Internet updates. There are no default values for these directives. Example:

```
HTTPProxyServer                        proxy.domain.com
HTTPProxyPort                          8080
HTTPProxyUsername                      username
HTTPProxyPassword                     password
```

Syslog Configuration

Regardless of the above configuration settings, AntiVir will always log important information using syslog. It is possible to specify which syslog facility and priority you would like AntiVir to use. If not given, default values are:

```
SyslogFacility                        user
SyslogPriority                         notice
```

GnuPG

AntiVir supports GnuPG (<http://www.gnupg.org>) in order to verify the authenticity of Internet update files. In order for AntiVir updater to utilize GnuPG, it must know where the GnuPG binary is located (see chapter 5.2). If you use GnuPG, be aware that all updates will fail until the AntiVir public key (antivir.gpg) has been added to your keyring and signed:

```
GnuPGBinary
```

If you are utilizing GnuPG, you may also specify options that your particular setup might need. Normally no options are required:

```
GnuPGOptions
```

5.2 AntiVir PGP Public Key – antivir.gpg

AntiVir supports GnuPG to verify the authenticity of files downloaded using the AntiVir internet updater. In order to make use of this feature (which is highly recommended), you will need to take the following steps. This needs to be done only once.

⇒ Get GnuPG.

You can download it from the GnuPG website (<http://www.gnupg.org>). If you are new to GnuPG and PGP, it is recommended that you read over the GnuPG handbook and learn the concepts of PGP and how it can be safely and securely used.

⇒ Generate your own PGP key.

If you are not familiar with GnuPG and PGP, read the GnuPG handbook.

⇒ Add the AntiVir PGP Public Key to your keyring:

```
gpg --import antivir.gpg
```

⇒ Check the key's fingerprint to make sure that it is the correct AntiVir PGP Public Key:

```
gpg --fingerprint support@antivir.de
```

This will show the 40-character fingerprint. Make sure it matches the fingerprint displayed on the AntiVir web site (<http://www.antivir.de>) or verify the fingerprint with somebody who uses GnuPG with AntiVir.

⇒ Sign the AntiVir PGP Public Key to declare that you trust that this is a valid key:

```
gpg --sign-key support@antivir.de
```

⇒ Verify that everything is set up correctly:

You can do this by checking the fingerprint on the antivir binary:

⇒ Go into the bin directory from the installation files and you should see two files:

- antivir
- antivir.asc

⇒ Check the signature with:

```
gpg --verify antivir.asc antivir
```

If everything passes this check without error, you are ready to use GnuPG with AntiVir updater.

⇒ Activate GnuPG in AntiVir by adding the GnuPGBinary directive to the /etc/antivir.conf file. This directive takes as its argument the full path to your GnuPG binary. Typically, it would look like this:

```
GnuPGBinary /usr/local/bin/gpg
```

⇒ Restart AntiVir updater to let the new settings become effective:

```
/usr/lib/antivir/avupdater restart
```

Note:

Currently only engine or program updates utilize GnuPG. VDF file updates will not use GnuPG.

6 Virus-specific warnings: file avmilter.warn

As an option, you can define a file `/etc/avmilter.warn`. This file specifies – beyond the settings in `avmilter.conf` – the sending of email warnings to sender, recipient and postmaster.

A line of this file consists of two entries: The first entry is the name of the detected virus or unwanted program, resp. This entry may contain wildcards. The second entry consists of one or more of the following entries:

- S: for Sender
- R: for Recipient
- P: for Postmaster

Example:

```
/klez/ RP
```

instructs AntiVir Milter to send an email warning to recipient and postmaster, if a virus has been detected containing the name element **klez**.

Note:

The settings in `avmilter.warn` suspend the settings in `avmilter.conf` (`Expose*Alerts`) for the specified viruses and unwanted programs.

7 Notification templates

If you are running a commercial or private license, you have the possibility to define your own message in virus und pathological notification mails.

⇒ Create the directory `/usr/lib/AntiVir/templates/`.

⇒ Copy the sample template files from archive directory `templates` to `/usr/lib/AntiVir/templates/`.

⇒ Set the access rights:

```
chown -R uucp:antivir /usr/lib/AntiVir/templates
```

⇒ Change to the directory `/usr/lib/AntiVir/templates/`. This directory contains the following files:

- patho-administrator
- patho-recipient
- patho-sender
- virus-administrator
- virus-recipient
- virus-sender

⇒ Edit all files and insert your own messages. Pay attention to the format of these files. The first line is the subject of a mail. After this line there must follow an empty line (new line), then the body.

Keywords

The virus-* and patho-* files may contain the following keywords which will be replaced by the corresponding text:

Keyword	Replacing text
LICENSE	Centered license text (one or two lines)
SENDER	Email address of the sender of the bad email
VIRUSES	List of viruses and unwanted programs found in the bad email, one per line, the prefix and postfix substring being repeated on each line
REASON	Cause explaining why the email could not be scanned (one short sentence)
ADVICE	Suggestion as to what the sender can do to eliminate the problem (see REASON) (about one line)
QUEUEID	ID of the message in the AvMilterGate queue
SUBJECT	Subject of the infected mail

Example

For example see the file virus-recipient:

Subject: AntiVir ALERT [your mail: "SUBJECT"]

*****AntiVir ALERT*****

LICENSE

AntiVir has detected the following in email from your address:

VIRUSES

This mail was not delivered, but isolated on your server. Please check your system immediately for viruses and unwanted programs.

Please remove any potential viruses and unwanted programs from your computer before sending a new mail with attachments.



Program & Documentation
Copyright © 2004
H+BEDV Datentechnik GmbH
All rights reserved

Editor:
H+BEDV Datentechnik GmbH
D-88069 Tettnang, Lindauer Strasse 21

Phone: +49 (0) 7542 / 500 0
Fax: +49 (0) 7542 / 52510

Internet: <http://www.antivir.de>
<http://www.hbedv.com>

Version December 2004