Avira AntiVir MailGate / Avira MailGate Suite

User Manual

AVIRA

1 About this manual

This chapter contains an overview of the structure and content of this manual.

A brief introduction provides information on the following subjects:

1.1 Introduction

In this manual, we have compiled all of the information you need on Avira AntiVir MailGate and lead you step-by-step through the installation, configuration and use of the software.

The attachment contains a glossary explaining basic terms.

Additional help and information is also available from our website, our Technical Support hotline and our regular newsletter (see Service – Page 110).

Your Avira Team

1.2 Structure of the manual

The manual for your Avira AntiVir MailGate software consists of several chapters containing the following information:

Chapter	Contents
1 About this manual	Structure of the manual, characters and symbols
2 Product information	General information on Avira AntiVir MailGate, its modules, features and system requirements, and on licensing
3 Milter mode	Introduction to milter mode in Avira AntiVir MailGate
4 Installation	Instructions for installing Avira AntiVir MailGate on your system
5 Configuration	Information on the optimal adjustment of Avira AntiVir MailGate components on your system
6 Operation	Commands and parameters for executing the scanner and the queue manager; procedures for identifying viruses and unwanted programs
7 Updates	Updating via the Internet and intranets
8 Service	Avira GmbH Support and service
9 Appendix	Glossary with explanations of technical terms and abbreviations Golden rules for virus protection

1.3 Characters and symbols

The following characters and symbols are used in this manual:

Symbol	Meaning
✓	placed before a condition which must be fulfilled prior to performing an action.
▶	placed before a step which has to be completed.
↳	placed before an event resulting directly from the previous action.
	placed before an alert warning of critical data loss or hardware damage.
	placed before a particularly important piece of information, for example, relating to steps being carried out.
	denotes a tip facilitating the understanding and operation of the Avira AntiVir MailGate.

The following emphases are also used in the text to improve readability and clarity:

Emphasis in the text	Explanation
Ctrl + Alt	Keys or key combinations
/usr/lib/AntiVir/mailgate	Path details and file names
`ls /usr/lib/AntiVir`	User input
Select components Select all	Software interface components, e.g. menu options, window headings or buttons in dialog boxes
http://www.avira.com	URLs
Characters and symbols - Page 4	Cross-references inside the document

1.4 Abbreviations

The following abbreviations are used in this manual:

Abbreviation	Meaning
ACL	Access Control List
FAQs	Frequently Asked Questions
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
MIME	Multipurpose Internet Mail Extensions
MTA	Mail Transport Agent
RFC	Request For Comment
SMTP	Simple Mail Transfer Protocol
VDF	Virus Definition File

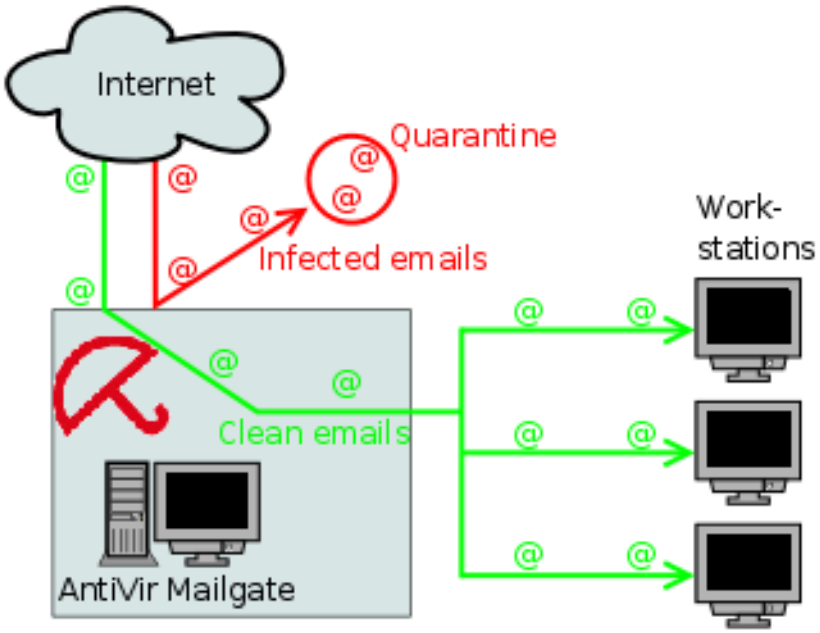
2 Product information

File transfer by email has become such a fixture of modern communications that it's difficult to imagine life without it. However emails often also transfer viruses and unwanted programs.

Many of these viruses and programs are specially developed to attack Windows operating systems. UNIX systems are however exposed to the same danger, as malware is also transmitted by UNIX mail servers. Cyber attacks exploit this fact mercilessly to invade third-party networks. If Windows clients can be infected, the same goes for the computers of their communication partners.

An increasing number of companies and public institutions are now using UNIX. Because the software used is also free, the operating systems can easily become the target of virus programmers. In the future, virus protection for UNIX systems will remain an issue. For this reason we have developed Avira AntiVir MailGate.

Avira AntiVir MailGate scans all incoming and outgoing emails (including attachments) on your UNIX mail server. The software works with a wide range of Mail Transport Agents (MTAs), e.g. Sendmail, Postfix, Exim, Qmail and similar programs. Effective support is provided for many well known distributions - Red Hat, SuSE, Debian, etc.(see 2.4 System requirements).



There are two particularly important things to bear in mind right from the start:

Warning: *The loss of valuable data usually has dramatic consequences. Even the best virus protection software cannot provide one hundred percent protection from data loss.*

▶ *Make regular backups of your data.*

A virus protection program can only provide reliable and effective protection if it is up-to-date.

▶ *Use automatic updates to ensure that your Avira AntiVir MailGate is always up-to-date. This manual will explain how to proceed.*

2.1 Features

Avira AntiVir MailGate supports a wide range of configuration settings which allow you to constantly monitor email traffic on your system.

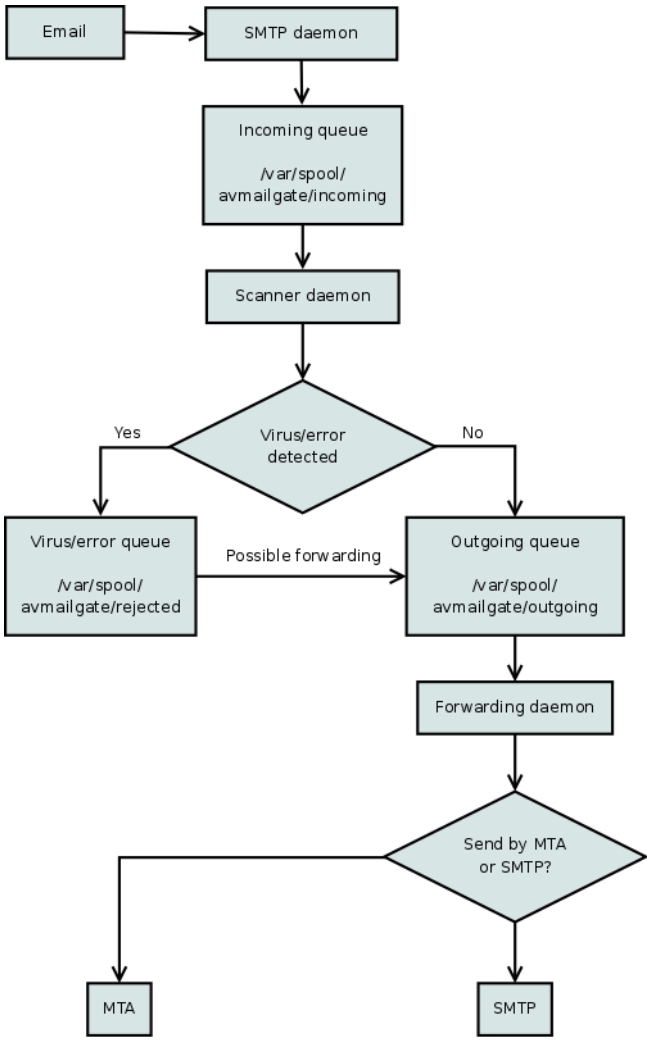
The most important features of Avira AntiVir MailGate:

- Real-time scanning of incoming and outgoing emails
- Scanning for viruses and unwanted programs
- Configurable spam filter (contained in the **Avira MailGate Suite**)
- Scanning of mailboxes
- Isolation of suspicious and infected files
- Configurable notification functions for the administrator, the sender and the recipient of the email
- External reporting via Avira AntiVir MailGate activities in a database
- Automatic Internet updates for MailGate, Scanner, VDF and Engine
- Heuristic detection of macroviruses
- Detection of all conventional archive types (with configurable recursion depth for nested archives)
- Optional: GUI support for integration into the Avira Security Management Center

2.2 Modules and functionality of Avira AntiVir MailGate

Avira AntiVir MailGate is an SMTP scanner which scans all incoming and outgoing emails (including attachments) on your UNIX mail server. The scan is performed extremely quickly and is easy to configure.

As well as SMTP, Avira AntiVir MailGate also supports the Sendmail milter interface.



This storage and forwarding agent divides the work between two programs:

SMTP daemon

The SMTP daemon receives the emails and stores them in the spool directory. The program runs as a separate server using Port 25 (SMTP).

Scanner and forwarding daemon

The forwarding daemon reads the emails in the spool directory, decodes the attachments and starts to scan for viruses and unwanted programs.

Depending on the result of the scan, clean emails are forwarded, whilst infected emails are blocked in the spool directory (rejected).

In accordance with the configuration in avmailgate.conf the program also blocks

suspicious emails in the same directory, e.g. password-protected archives and fragmented emails. The rules for the spam filter are also defined in the same configuration file.

Where necessary, the queue can be scanned with the queue manager avq.
To find out how to scan the spool directory, go to Queue manager avq – Page 96.

Alerts:
If viruses, unwanted programs or suspicious files are detected, the postmaster receives an email detailing the alerts. The alerts can also be sent to the sender and the recipient of the email. The program provides alert templates which you can adapt and apply.

Updater:
The Avira Updater downloads the latest updates from the Avira AntiVir MailGate webservers at regular intervals and installs them (manually or automatically). The module can also send notifications by email.

You can update the entire Avira AntiVir MailGate or just the Scanner.

2.3 Licensing concept

To be able to use Avira AntiVir MailGate, you must purchase a license for the program and agree to the license terms and conditions.
(see http://www.avira.com/en/license-agreement).

Two license models are available for Avira AntiVir MailGate:
- Test version
- Full version

Licensing depends on the number of users on the network who are to be protected by Avira AntiVir MailGate.

The license is issued via the license file hbedv.key. You can obtain this file by email from Avira GmbH. The file contains exact details of which programs are licensed and for what period of time. The same license file can apply for multiple Avira GmbH products.

Test version

30 day test license for Avira AntiVir MailGate.

For further information on the evaluation version, please go to our website http://www.avira.com.

Full version

The scope of the license for the full version comprises:
- Avira AntiVir MailGate-versions for downloading from the Internet
- License file by email to upgrade the test version to the full version
- Detailed installation instructions (digital)
- Four weeks installation support from date of purchase
- Newsletter service (by email)
- Internet update services for program files and VDFs

After installation of an Avira AntiVir MailGate product, you can use the following command to display information on the current license:

```
/usr/lib/AntiVir/mailgate/avlinfo
```

▶ Change the /usr/lib/AntiVir/mailgate directory and access `./avlinfo`

You can obtain further information by using the following command:
`avlinfo -h`

2.4 System requirements

To ensure that Avira AntiVir MailGate functions optimally on your server, the following minimum requirements must be met (depending on factors such as the extent of email traffic, the number and size of attachments, etc. additional memories may be necessary):

The versions for Linux and Solaris use similar installation and application processes (normally only a few file names are different, depending on the target system).

- Computer: x86, SPARC
- Operating system: Linux (with GLIBC 2.2 or higher) or Solaris
- 32 Bit or 64 Bit CPU
  Use with 64 Bit UNIX: Please use the required 32 Bit library. Further details can be found in your UNIX system documentation.
- RAM: 512 MB
- HDD: 1 GB HDD (for unpacking archives)
- Administration via the SMC: libstdc++so.5 for the SMC agent.

The following distributions are officially supported by Avira AntiVir MailGate:

- Red Hat Enterprise Linux 4 Server
- Red Hat Enterprise Linux 5 Server
- Red Hat Enterprise linux 6 Server
- Novell Open Enterprise Server (10.2)
- Novell SUSE Linux Enterprise Server 9 (SLES 9)
- Novell SUSE Linux Enterprise Server 10 - 10.2 (SLES 10)
- Novell SUSE Linux Enterprise Server 11 (SLES 11)
- Debian GNU/Linux 4
- Debian GNU/Linux 5
- Debian GNU/Linux 6
- Ubuntu Server Edition 8
- Ubuntu Server Edition 9
- Ubuntu Server Edition 10
- Ubuntu Server Edition 11
- Sun Solaris 9 (SPARC)
- Sun Solaris 10 (SPARC)

To use Avira AntiVir MailGate on an x86_64 Debian system, a previous installation of lib32nss-mdns is recommended.

2.4.1 Active directory

Avira AntiVir MailGate supports the use of Active Directory on the following platforms:

- Windows Server 2003 SP2
- Windows Server 2003 R2 SP2
- Windows Server 2008
- Windows Server 2008 R2

3 Milter mode

3.1 Overview

To start Avira AntiVir MailGate in milter mode, the following syntax is required (after installation of MailGate) for the `ListenAddress` option in avmailgate.conf:

```
inet:port@{hostname|ip-address}
Example: inet:3333@localhost
```

- or -

```
{unix|local}:/path/to/file
Example:
 unix:/path/to/file
 local:/path/to/file
```

3.2 Functions of Avira AntiVir MailGate (Milter mode)

Avira AntiVir MailGate (Milter mode) is a plug-in for Sendmail available from Version 8.11, which communicates via the Sendmail libmilter interface.

The module scans all incoming and outgoing emails. Infected emails are not forwarded. A status report is displayed in syslog. The sender, recipient and administrator can be notified of an infection.

Functions

Most of the following functions also apply to Avira AntiVir MailGate when it is not running in milter mode.

- All Sendmail functions are still available (e.g. SMTP authentication, Anti-relaying and Anti-spam)
- Simple installation and integration into Sendmail
- Hourly or daily Internet updates for MailGate, Scanner, VDF and Engine
- Scanning incoming and outgoing emails
- Reliable real-time detection of viruses and malware.
- Configurable reactions to detected viruses or malware
- Isolation of infected or suspicious files in a quarantine directory
- Log file as log for email traffic
- Immediate activation of a new VDF
- Heuristic detection of macroviruses
- Configurable alert templates
- Archive scanning

3.3 Integration of Avira AntiVir MailGate (Milter mode) in Sendmail

3.3.1 Requirements

Sendmail Version 8.11 or later with libmilter interface.

Otherwise:

▶ Read the README file in the libmilter directory of the Sendmail kit (http://www.sendmail.org).

▶ Compile the new version of Sendmail with the libmilter interface.

To check whether Sendmail has been compiled with the libmilter interface:

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

3.3.2 Integration

Two options are available for adding Avira AntiVir MailGate (milter mode) to the Sendmail configuration file sendmail.cf

- Changing sendmail.cf directly

- OR -

- Generating sendmail.cf

Changing sendmail.cf directly

▶ Add the following two lines to the configuration file sendmail.cf.

```
Xavmilter, S=inet:3333@localhost, F=R,
T=S:2m;R:2m;E:10m
O InputMailFilters=avmilter
```

Meaning of the values

- F: defines what should happen if the filter is not available:
  - T: emails are temporarily not accepted (Error 4XX)
  - R: emails are rejected (Error 5XX)
- T: defines the following timeouts:
  - C: timeout for creating connection to the filter
  - S: timeout for sending information to the filter
  - R: timeout for reading a response from the filter
  - E: timeout between sending “End of Message” and the response from the filter

Change these values if the log displays the following notification “Milter (avmilter): timeout before data read”

Generating sendmail.cf

▶ Add the relevant lines to the sendmail.mc file
(commands beginning with `INPUT` must be on one line):

For Sendmail 8.11.x:

```
define(`_FFR_MILTER', `true')
INPUT_MAIL_FILTER(`avmilter',`S=inet:3333@localhost,
F=R, T=S:2m;R:2m;E:10m')
```

for Sendmail 8.12.x:

```
INPUT_MAIL_FILTER(`avmilter',`S=inet:3333@localhost,
F=R, T=S:2m;R:2m;E:10m')
```

▶ Generate the file sendmail.cf
Example:

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

4 Installation

You can find the current version of Avira AntiVir MailGate on the Avira website. Avira AntiVir MailGate is available as a compressed archive. You can install the program on your system with the install script.

Requirements

To be able to install Avira AntiVir MailGate you must be logged on as root. An MTA (Sendmail, Postfix, Exim, Qmail etc.) must also be available on your system. Our support service however only deals with problems directly linked to Avira AntiVir MailGate.

This section describes a standard Sendmail installation on a SuSE distribution. If you want to integrate the program into a different MTA or, for example, into Lotus Domino, further information is available in the relevant file (INSTALL.sendmail, INSTALL.exim, INSTALL.qmail, INSTALL.postfix etc.).

This chapter contains the following sections:

If you have also installed Avira AntiVir Server (UNIX) or Avira AntiVir Professional (UNIX) and are configuring and using these products with the aid of the GUI, please note that the GUI is not compatible with the current version (beginning with Version 3) of Avira AntiVir MailGate and Avira AntiVir WebGate.

4.1 Preparing installation files

Downloading program files from the Internet

- Download the current files to your local computer from our website http://www.avira.com. The file name is antivir-mailgate-prof.tgz.
- Copy the file into a directory of your choice (e.g. /tmp) on the computer on which Avira AntiVir MailGate is to be installed.

Extracting the program files

- Change the temporary directory:

```
cd /tmp
```

- Extract the archive for the Avira AntiVir-MailGate kit:
  `tar -xzvf antivir-mailgate-prof.tgz`

  ↳ The folder antivir-mailgate-prof-<Version> will be created in the temporary directory.

4.2 Licensing

In order to execute Avira AntiVir MailGate you require a license (see Licensing concept – Page 9). The license file hbedv.key can be obtained by email. It contains information on the license's scope and period of validity.

Purchasing a license

- Fill out the test license form on our website and you can test Avira AntiVir MailGate for 30 days.
- Contact us by telephone or via sales@avira.com and we will send you a valid license file by email.
- You can also purchase Avira AntiVir MailGate in our online shop.

Copying the license file

- Copy the license file hbedv.key to your installation directory. Example: /tmp/antivir-mailgate-prof-<Version>.

You can copy the license file into the program directory /usr/lib/AntiVir/mailgate *at a later time.*

4.3 Installation with the “install” installation script

You can install Avira AntiVir MailGate automatically using the install script.

To do this, the install script will complete the following steps:

- Check the integrity of the installation files.
- Check authorizations required for installation.
- Search for previously installed versions of Avira AntiVir MailGate on the computer.
- Copy the program file (and overwrite existing files that are no longer needed).
- Copy the configuration files (existing configuration files will be retained).
- Install the Internet Updater.
- Optional: Install GUI support for Avira SMC (Security Management Center).

Preparing installation

✓ The program files have been downloaded from the Internet and extracted.

▶ Log in as **root**. Otherwise you will not have the authorization to perform the installation and the script will issue an error message.

▶ Change the directory in which you extracted the Avira AntiVir MailGate kit. Example:

```
cd /tmp/antivir-mailgate-prof-<Version>
```

Installing Avira AntiVir MailGate

▶ Enter the following:

```
./install
```

↳ The installation script is started.

▶ You have to read and accept the license agreement before the installation can continue.

▶ Close the file with the license agreement with q.

↳ The following query is displayed:

```
Do you agree to the license terms? [n]
```

▶ Enter y and press **Enter**.

↳ The Avira AntiVir MailGate Core Components are installed. The script now

requests the license file path:

```
copying install_list_mailgate to  /usr/lib/AntiVir/mailgate ... done
copying LICENSE to /usr/lib/AntiVir/mailgate/LICENSE-mailgate ... done
1) installing AntiVir Core Components (Engine, Savapi and Avupdate)
copying ...

Enter the path to your key file []
```

▶ Enter the license file path and press **Enter**.

```
copying license key  to  /usr/lib/AntiVir/mailgate/ license-mailgate.key... done


installation of AntiVir Core Components (Engine, Savapi and Avupdate)
complete
```

- OR -
If you want to copy the license file at a later time, just press **Enter**.

↳ The next step installs the automatic Internet Updater. You will then be asked if you wish to create a link for the start script in /usr/sbin:

```
2) Configuring updates
An internet updater is available with AVIRA MailGate (UNIX). It will ensure
that you always have the latest malware detection patterns and engine
updates.

In order to trigger an update you will need to run the command:
   /usr/lib/AntiVir/mailgate/avupdate-mailgate

Would you like to create a link in /usr/sbin for avupdate-mailgate? [y]
```

▶ Press **Enter** to confirm or press n.

↳ You will now be asked whether you wish to create cron jobs for scanner and product updates:

```
Would you like to setup Scanner update as cron task? [y]
Please specify the interval to check.
Recommended values are daily or 2 hours.

available options: d [2]
creating Scanner update cronjob ... done

Would you like to check for MailGate updates once a week? [n] y
creating MailGate update cronjob ... done

setup internet updater complete
```

You can also adjust these options at a later time.

↳ The script continues to install the main program:

```
3) installing main program
copying doc/antivir_mailgate_en.pdf to /usr/lib/AntiVir/mailgate ... done
copying ...
```

↳ The next queries relate to hosts handled as local, and those hosts which are allowed to relay via Avira AntiVir MailGate emails:

```
Enter the hosts and/or domains that are local
[<hostname>]:
```

▶ When appropriate, change the host names and press **Enter**.

↳ The next query is displayed:

```
Please enter the hosts and networks that are allowed to relay. When running
MailGate in content filter mode (SMTP), the address suggested below will be
sufficient. You can change this settings by editing the file
 /etc/avira/avmailgate.acl
afterwards

[127.0.0.1/8]:
```

↳ You will now be asked if you wish to create a link for the start script in /usr/sbin:

```
Would you like to create a link in /usr/sbin for avmailgate? [y]
```

▶ Press **Enter** to confirm or press n.

↳ You will now be asked if Avira AntiVir MailGate should be started automatically at system start-up:

```
Please specify if boot scripts should be set up.
Set up boot scripts [y]:
```

▶ Enter n and press **Enter**. You can change this option at a later time.

- OR -

Confirm the default setting by pressing **Enter**.

↳ The next step installs the SMC plugin for the Avira Security Management Center:

```
installation of main program complete

4) activate SMC support
If you are going to use AVIRA Security Management Center (SMC) to manage
this software remotely you need this

 Would you like to activate SMC support? [y]
```

▶Press **Enter** to install the SMC plugin, or n and **Enter** to skip the installation.

↳ The following message is displayed when the script has ended:

```
Installation of the following features complete:
   AntiVir Core Components (Engine, Savapi and Avupdate)
   AVIRA Internet Updater
   AVIRA MailGate
   AntiVir SMC plugin
```

▶ Depending on your MTA, continue the installation as described in Other installation steps depending on the MTA – Page 19.

▶ Avira AntiVir MailGate is installed under

```
/usr/lib/AntiVir/mailgate
```

.

▶ You can now start Avira AntiVir MailGate:

```
/usr/lib/AntiVir/mailgate/avmailgate start
```

***Warning**: Modified binary files cannot start.*

For example, with prelink: either deactivate prelink, or enter /usr/lib/AntiVir/mailgate as an exception in the configuration file /etc/prelink.conf.

***Warning**: From Version 3.0.0 onwards, a new Scanner backend has been used. If you have been using a MailGate version older than 3.0.0, please note that in the current MailGate version, some scanner-specific configuration options are now specified in avmailgate-scanner.conf and not in avmailgate.conf.*

We recommend that you perform an update immediately after installation to ensure all protection mechanisms are up-to-date. To do this, execute the following command:

```
/usr/lib/AntiVir/mailgate/avupdate-mailgate
```

Further information on updates is available in Updates – Page 108.

4.4 Reinstalling or uninstalling Avira AntiVir MailGate

You can re-access the installation script at any time. This enables the following procedures:

- Installation of a new version (upgrade). The installation script first checks the previous version and installs the requisite new components. The existing configuration settings are not overwritten but inherited (Configuration – Page 24).
- Subsequent installation of individual components.
- Enabling and disabling of Avira Updater and Avira AntiVir MailGate automatic start-up.

Reinstalling Avira AntiVir MailGate

The procedure is the same in all cases:

- Change the temporary directory in which you extracted Avira AntiVir MailGate, for example:
  `cd /tmp/antivir-mailgate-prof-<version>/`
- Enter:
  `./install`

  ↳ The installation script starts as described for the initial installation (Installing Avira AntiVir MailGate – Page 15).
- Change the relevant settings during installation.

  ↳ Avira AntiVir MailGate is installed with the new settings.

Uninstalling Avira AntiVir MailGate

If you want to uninstall Avira AntiVir MailGate, you can use the *uninstall* script. It is available in the installation directory.

- Change the directory in which you have installed Avira AntiVir MailGate:
  `cd /usr/lib/AntiVir/mailgate`
- Enter:

  `./uninstall --product=Mailgate`

  ↳ The script uninstalls the product. It asks whether you want to keep a copy of the license file, if you want to backup the configuration files and log files; it can also delete the cron jobs for updating MailGate or Scanner.
- Answer by entering ***y*** or ***n*** and confirm by pressing ***Enter***.

  ↳ Avira AntiVir MailGate is uninstalled.

4.5 Other installation steps depending on the MTA

After the installation of Avira AntiVir MailGate described above, you must define some settings manually, depending on which MTA you are using.

The following section describes the features specific to Sendmail, Exim, Qmail and Postfix.

Configuring Sendmail

If you are working with Sendmail, it is recommended that you use Avira AntiVir MailGate in milter mode (see Chapter Milter mode – Page 10). This mode ensures full SMTP functionality in Sendmail(e.g. SMTP authentication).

Configuring Exim

Avira AntiVir MailGate runs with Exim Version 3.0 or higher.

▶ The following command enables you to find out which Exim version you are using:
`exim -bV`

There are two options for integrating Avira AntiVir MailGate into Exim:
- Integration of Avira AntiVir MailGate as a content filter in Exim (recommended)
- Proxy mode

Content filter

Configuration of Avira AntiVir MailGate:

▶ Change (or add) the following entries in avmailgate.conf:

```
ListenAddress 127.0.0.1 port 10024
ForwardTo SMTP: 127.0.0.1 port 10025
```

▶ Restart Avira AntiVir MailGate.

Configuration of Exim:

▶ Change (or add) the following entries in exim.conf:

```
# Listen on all interfaces on port 25
# and on 127.0.0.1 port 10025
local_interfaces = 0.0.0.0.25 : 127.0.0.1.10025
```

Add an entry for the Router:

▶ Inexim.conf, search for `begin router` and add the following entries:

```
# Router for AntiVir MailGate
antivir_mailgate:
 debug_print = "R: AntiVir MailGate for
    $local_part@$domain"
 driver = manualroute
 transport = antivir_mailgate_transport
 route_list = "* localhost byname"
 self = send
 # do not call this router in the second instance of Exim
 condition = ${if !eq {$interface_port}{10025}{1}{0}}
```

Add an entry for the transport:

▶ In exim.conf, search for `begin transports` and add the following lines:

```
# Transport for AntiVir MailGate
antivir_mailgate_transport:
        driver = smtp
        # connect to port 10024
        port = 10024
        allow_localhost
```

▶ Restart Exim.

Proxy mode

Configuration of Avira AntiVir MailGate:

▶ Change (or add) the following entries in avmailgate.conf:

```
ListenAddress 0.0.0.0 port 25
ForwardTo SMTP: 127.0.0.1 port 825
```

▶ Restart Avira AntiVir MailGate.

Configuration of Exim:

▶ Change (or add) the following entries in exim.conf:

```
daemon_smtp_port = 825
```

▶ Restart Exim.

Configuring Qmail

A plugin is available in Qmail to enhance the integration of Avira AntiVir MailGate. Details are available from support@avira.com.

There are two options for integrating Avira AntiVir MailGate into Qmail:

- Sendmail wrapper
- Backdoor procedure

Replace SMTP with `825` in the `run` file only. All other parameters are examples only.

Sendmail wrapper

Sendmail wrapper

You can use the Sendmail wrapper, delivered with Qmail, to deliver emails (default). First change the Qmail installation folder and enable the wrapper.

▶ Enable the Sendmail wrapper in Qmail:

```
ln -s /var/qmail/bin/sendmail /usr/lib/sendmail
ln -s /var/qmail/bin/sendmail /usr/sbin/sendmail
```

▶ Set up the email relay mode. Find the following line in the file /etc/avira/avmailgate.conf:

```
# Select how mail should be forwarded.
```

▶ Change the appropriate entries as follows:

```
# Send mail by piping it through sendmail (this is the default)
ForwardTo /usr/sbin/sendmail -oem -oi
# Or if you want the mail to be sent by SMTP
# ForwardTo SMTP: localhost port 825
```

Backdoor procedure

Backdoor procedure

The second options involves setting up email delivery via port 825 on which Qmail should be enabled. This is achieved, e.g. with the aid of the file inetd.conf (see Qmail installation package).

▶ Set up the email relay mode. In /etc/avira/avmailgate.conf, search for the following line:

```
# Select how mail should be forwarded.
```

▶ Change the appropriate entries as follows:

```
# ForwardTo /usr/sbin/sendmail -oem -oi
# Or if you want the mail to be sent by SMTP
ForwardTo SMTP: localhost port 825
```

If you are using inetd with Qmail:

▶ Add the following line (1 line!) to inetd.conf:

```
825 tcp nowait qmaild /var/qmail/bin/tcp-env tcp-env /var/qmail/
bin/qmail-smtpd
```

If you are using tcpwrapper with Qmail:

▶ Change the Qmail port in /var/qmail/supervise/qmail-smtpd/run. For example, search for the following lines:

```
/usr/bin/tcpserver -D -R -v -p -x /etc/tcprules.d/qmail-smtp.cdb \
-u $QMAILDUID -g $NOFILESGID 0 smtp /var/qmail/bin/qmail-smtpd 2>&1
```

▶ Change the lines as follows:

```
/usr/bin/tcpserver -D -R -v -p -x /etc/tcprules.d/qmail-smtp.cdb \
-u $QMAILDUID -g $NOFILESGID 0 825 /var/qmail/bin/qmail-smtpd 2>&1
```

Configuring Postfix

There are two options for integrating Avira AntiVir MailGate into Postfix:

- Integration of Avira AntiVir MailGate as a content filter in Postfix (recommended)
- Avira AntiVir MailGate is listening on port 25 and relays emails to Postfix

Content filter

Perform the following steps:

▶ In /etc/avira/avmailgate.conf, search for the following line:

```
# Select how mail should be forwarded.
```

▶ Change the appropriate entries as follows:

```
# Select how mail should be forwarded.
# Send mail by piping it through sendmail (this is the default)
# ForwardTo /usr/sbin/sendmail -oem -oi
# Or if you want the mail to be sent by SMTP
ForwardTo SMTP: localhost port 10025
# Set the network interface the SMTP daemon will listen on.
ListenAddress 127.0.0.1 port 10024
```

If you are using SuSE Mail Server II:

▶ Replace the entry `#AllowSourceRouting NO` with the following:

```
AllowSourceRouting YES
```

▶ Close Avira AntiVir MailGate and then restart it:

```
/etc/init.d/avmailgate restart
```

▶ Add the following entry to /etc/postfix/master.cf:

```
# For AntiVir maildaemon
localhost:10025 inet n - n - - smtpd -o content_filter=
```

▶ Ensure that the first symbol in the table is not a space or tab character.

The parameter `-o content_filter` prevents emails from being repeatedly sent back and forth between Avira AntiVir MailGate and Postfix.

▶ Add the following entries to /etc/postfix/main.cf:

```
# AntiVir integration
content_filter = smtp:[127.0.0.1]:10024
```

This setting avoids needless MX lookups.

▶ Restart Postfix:

```
/etc/init.d/postfix restart
```

or

```
/etc/init.d/postfix reload
```

After installation of Avira AntiVir MailGate, if Postfix gives emails the status **deferred**, *perform the following steps:*

▶ In main.cf, search for the following line:

```
defer_transports = local
```

▶ Comment out the line:

```
# defer_transports = local
```

Listening on port 25

▶ In master.cf, search for the following line:

```
smtp inet n - n - - smtpd
```

▶ Comment out the line:

```
# smtp inet n - n - - smtpd
```

↳ This will prevent Postfix from listening on the SMTP port (25), thereby ensuring that the SMTP daemon of Avira AntiVir MailGate will listen on the SMTP port (25).

▶ Restart Postfix:

```
/etc/init.d/postfix restart
```

or

```
/etc/init.d/postfix reload
```

4.6 Testing Avira AntiVir MailGate after installation

After you have installed Avira AntiVir MailGate you should check it is functioning correctly. For this purpose you can use the Eicar test virus, which is detected by all virus scanners. The virus does not cause any damage, but triggers a program reaction when scanning the email if everything has been installed and configured correctly.

- Copy the following character string into a file:
  X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

  - OR -
  Download the Eicar file from the website http://www.eicar.com.
- Send this file as an attachment in a test email to Avira AntiVir MailGate.
- Check the reaction in the directory /var/spool/avmailgate/rejected.
- Check the messages which Avira AntiVir MailGate has sent to the log file or to syslog.

5 Configuration

You can adapt Avira AntiVir MailGate to ensure optimal performance on your system. Some settings are recommended during installation with the install script. You can change these settings at any time.

This section takes you step-by-step through the configuration process.
The following subject areas are covered:

The configuration files are read at program start-up. Empty lines and lines beginning with "#" are ignored.

The files contain default settings suitable for most configurations. Some entries are disabled or commented out with "#" symbol. These entries can be enabled by deleting the "#" symbol.

From Avira AntiVir MailGate 3.0.0 onwards, invalid configuration options trigger an error message:
"Error at line ... in /etc/avira/avmailgate.conf".

At the end of installation, the list of configuration files is displayed:

/etc/avira/avmailgate.conf	(MailGate-Main configuration)
/etc/avira/avmailgate-scanner.conf	(Scanner configuration)
/etc/avira/avmailgate.acl	(MailGate-Access list)
/etc/avira/avmailgate.ignore	(MailGate-Ignore list)
/etc/avira/avmailgate.scan	(MailGate-Scan list)
/etc/avira/avmailgate.warn	(MailGate-Alert list)
/etc/avira/asmailgate.except	(MailGate-Spam filter configuration)
/etc/avira/avupdate-mailgate.conf	(Options for Avira avupdate)

5.1 Avira AntiVir MailGate-Spool directories

Avira AntiVir MailGate places infected emails in "quarantine". Depending on the configuration, the postmaster and/or sender and/or recipient of the email are notified that a virus or unwanted program has been detected.
The parameters are defined in the file avmailgate.conf (see Avira AntiVir MailGate

configuration in avmailgate.conf – Page 26).

Spool directories

Spool directories

The spool directory (default: /var/spool/avmailgate/) contains three sub-directories:

- incoming: incoming emails which must be scanned.
- outgoing: scanned emails which can be forwarded.
- rejected: emails containing a virus or unwanted program or which have been classified as problematic (for example due to a MIME error).

Spool files

Spool files

In these directories, every email is represented by two files:

- Data file
- Control file

The name of the data file begins with df- and contains an ID (e.g. 32557-0BE692EB).

The control file has the same ID. Depending on the status, its name begins with:

- xf-: the control file has just been edited.
- qf-: the email must be scanned for viruses.
- Qf-: the email can be forwarded without scanning.
- vf-: the email contains a virus or unwanted program.
- mf-: there is a MIME problem in the email.

Example

Example:

- Data file: df-32557-0BE692EB
- Corresponding control file: qf-32557-0BE692EB

Editing spool files

Editing spool files

If a virus or unwanted program has been discovered, the directory /var/spool/avmailgate/rejected/ contains the following files:

- df-file
- vf- or mf-file

These files can be edited by external programs or scripts (e.g. those in the parameter `ExternalProgram`, seeAvira AntiVir MailGate configuration in avmailgate.conf – Page 26).

If no virus or unwanted program is discovered, the data files and control files are deleted after the email has been scanned and sent.

5.2 Avira AntiVir MailGate configuration in avmailgate.conf

The configuration file avmailgate.conf contains numerous parameters for working with Avira AntiVir MailGate. If a parameter is not specified, the default value is used. Please note, that not all parameters have a default value. The options are keywords, followed by whitespaces and value. The keywords ar not case sensitive.

Value types

Value types

- Characters: a sequence of one or more characters. If you want the value to start or stop with whitespace, you have to put the value into “quotation marks”.
- Path: the file path, as e.g. `/usr/lib/AntiVir/mailgate/avmailgate`.
- Option: given options, as e.g. `RECIPIENT | SENDER | BOTH`.
- Number: a decimal number.
  Minimum value allowed: -2147483648
  Maximum value allowed: 2147483647
- Non-negative number: a non-negative decimal number, 0 or greater.
  Minimum value allowed: 0
  Maximum value allowed: 4294967295
- Boolean: a boolean value, either YES or NO.
- Size: a decimal number, optionally followed by suffixes as B (bytes), K (kilobytes), M (megabytes) or G (gigabytes). If no suffix is given, the value is interpreted as bytes.
  Minimum value allowed: 0
  Maximum value allowed: 4294967295 bytes

  If suffix G is used, the maximum value allowed is: 3
  If suffix M is used, the maximum value allowed is: 4095
  If suffix K is used, the maximum value allowed is: 4194303
- Timespan: a decimal number, optionally followed by suffixes as s (seconds), m (minutes), h (hours) or d (days). If no suffix is given, the value is interpreted as seconds.

Configuration process

Configuration process

▶ Adapt avmailgate.conf to meet your requirements.

▶ Restart Avira AntiVir MailGate to put changed settings into effect:

```
/usr/lib/AntiVir/mailgate/avmailgate restart
```

The entries in avmailgate.conf are described in the following sections. Thematically related entries are grouped together. Entries relate only to Avira AntiVir MailGate and have no effect on any other AntiVir software.

If you change User, Group, PidDir or ListenAddress, you have to close Avira AntiVir MailGate beforehand.

You can use the following command

```
./avmailgate.bin --dump-config
```

to display the currently valid configuration values, excluding all existing comments in the configuration file and disabled configuration settings.

User, Group

User/Group

The user and group for Avira AntiVir MailGate processes (should not be root).

If you change this parameter, you also have to change the value for `User` *and* `Group` *in* /etc/avira/avmailgate-scanner.conf *(see Scanner configuration in avmailgate-scanner.conf – Page 84).*

Syntax:

```
User "characters"
Group "characters"
```

Default settings:

```
User uucp
Group antivir
```

If you change these settings, you also have to adapt the access rights for the spool directory (configuration option `SpoolDir`) and for

```
/usr/lib/AntiVir/mailgate/gui
```

Postmaster

Postmaster

This parameter specifies the email address to which the virus/unwanted program alerts and other notifications are sent:

Syntax:

```
Postmaster    "characters"
```

Default:

```
Postmaster    postmaster.
```

An example of value may be:

```
Postmaster virusmaster@admins.department.example.com
```

MyHostName

Hostname

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

Syntax:

```
MyHostName "characters"
```

Example:

```
MyHostName FooBarBaz
```

If this option is not assigned, the default setting is determined by `gethostname(2)`. Otherwise the default setting is:

```
MyHostName localhost
```

SpoolDir

Spool directory

During processing emails are placed in the sub-directories incoming, rejected and outgoing. The default directory is created by the install script. If you change the option SpoolDir you have to create the sub-directories incoming, outgoing and rejected by yourself.

The spool directory and the sub-directories incoming, outgoing and rejected must belong to the user and group specified in User, Group User, Group. Access can only be granted by these users (mode=700).

Syntax:

```
SpoolDir "path"
```

Example:

```
SpoolDir  /var/spool/FooBarBaz
```

Default:

```
SpoolDir /var/spool/avmailgate
```

AntiVirDir

AntiVir directory

The library directory of Avira AntiVir MailGate, containing virus definition files (*.vdf) and the license file.

Syntax:

```
AntiVirDir "path"
```

Example:

```
AntiVirDir /usr/lib/AntiVir/FooBarBaz
```

If you are using AntiSpam, you should not change the AntiVir default directory:

```
AntiVirDir /usr/lib/AntiVir/mailgate
```

TemporaryDir

Temporary directory

This directory contains temporary files (e.g. attachments which have just been scanned for viruses or unwanted programs). You must have enough available disk space for extracted attachments. If this option is not assigned, the environment variable TMPDIR is used.

If all Avira AntiVir MailGate components are using a common temporary directory, change the options `TemporaryDir` *in* /etc/avira/avmailgate.conf *and* `ScanTemp` *in* avmailgate-scanner.conf.

Syntax:

```
TemporaryDir "path"
```

Example:

```
TemporaryDir  /var/FooBarBaz
```

Default:

```
TemporaryDir /var/tmp
```

MatchMailAddressForLocal

Check domain names

This option determines whether the domain names of RECIPIENT-, SENDER- or BOTH-addresses should be compared with the entries in the `local:` section of the file avmailgate.acl, before an email is accepted.

Syntax:

```
MatchMailAddressForLocal "option"
MatchMailAddressForLocal  RECIPIENT | SENDER | BOTH
```

Example:

```
MatchMailAddressForLocal  RECIPIENT
```

For further information, refer to Host configuration in avmailgate.acl – Page 87.
Default:

```
MatchMailAddressForLocal RECIPIENT
```

SMTPBanner

SMTP-Banner (not in milter mode)

Defines the header sent by Avira AntiVir MailGate. You can change the text, for example if you do not want to disclose the type of security software being used.

Syntax:

```
SMTPBanner "characters"
```

Example:

```
SMTPBanner FooBarBaz
```

Default:

```
SMTPBanner “AntiVir MailGate”
```

PidDir

PID directory

The PID files for Avira AntiVir MailGate main processes are saved in this directory. You have to close Avira AntiVir MailGate before changing this parameter.

Syntax:

```
PidDir "path"
```

Example:

```
PidDir  /var/FooBarBaz
```

Default:

```
PidDir /var/tmp
```

Syslog facility

Syslog facility

This option defines the log category syslog uses for Avira AntiVir MailGate messages.

Syntax:

```
SyslogFacility "characters"
```

Example:

```
SyslogFacility local0
```

Default:

```
SyslogFacility mail
```

LogFile

Log file

This option must contain the full path of the log file. Entries in the log file are also sent to syslog.

If LogFile is set to NO (default setting), no log file is used. Entries are however still sent to syslog.

Syntax:

```
LogFile "path"
```

Example:

```
LogFile /var/log/avmailgate.log
```

Default:

```
LogFile NO
```

LogAlertsFor EachRecipient

LogAlertsForEachRecipient

This option determines whether Avira AntiVir MailGate inputs an entry in the log file per infected email or per recipient.

Syntax:

```
LogAlertsForEachRecipient "YES | NO"
```

Default:

```
LogAlertsForEachRecipient NO
```

DebugLevel

Debug messages

This option determines whether or how detailed debug messages are registered in syslog or, if enabled, in the log file.

The detail accuracy can be set to the levels 0-5. A value of 0 means no debug messages are logged and a value of 5 means all are.

Syntax:

```
DebugLevel "non-negative number"
```

Example:

```
DebugLevel 2
```

Default:

```
DebugLevel 0
```

ListenAddress

IP address

The network interface address and port the SMTP daemon will listen on. Avira AntiVir MailGate is listening by default on 0.0.0.0:25 (all network interfaces port

25), it can be configured with a particular network interface address.

Syntax:

for SMTP mode:

```
ListenAddress "characters" port "number"
```

for milter mode:

```
ListenAddress "characters":"number"@"characters"
```

The default value will only be accepted if IPv4 support is enabled. If you disable IPv4 support, you have to specify a valid IPv6 address here (See configuration option InetProtocols – Page 54).

Default:

```
ListenAddress 0.0.0.0 port 25
```

Examples

for SMTP mode:

```
ListenAddress 192.168.5.20 port 25
```

for milter modus:

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

If you are unsure, you can use the default setting:

```
ListenAddress 0.0.0.0 port 25
```

With another syntax you can start Avira AntiVir MailGate in milter mode. For further information, refer to Milter mode – Page 10. Currently milter mode only works with IPv4.

If you enable only IPv6 support using the option InetProtocols, you have to specify IPv6 addresses for the ListenAddress and ForwardTo options, as well as in the avmailgate.acl file.

MaxIncoming Connections

Maximum number of simultaneous connections (not in milter mode)

This option defines the number of simultaneous client connections that Avira AntiVir MailGate will accept. The default setting 0 indicates there is no limit to the number.

Syntax:

```
MaxIncomingConnections "non-negative number"
```

Example:

```
MaxIncomingConnections 10
```

Default:

```
MaxIncomingConnections 0
```

SMTPTimeout

SMTP-Timeout (not in milter mode)

This option defines the maximum timeout for SMTP connections (in seconds).

Syntax:

```
SMTPTimeout "non-negative number"
```

Example:

```
SMTPTimeout 60
```

Default:

```
SMTPTimeout 300
```

EnableLegacy Quarantine

EnableLegacyQuaratine

You can use this option to select which Quarantine Manager you want to use.

Quarantine Manager Classic is the default:

```
EnableLegacyQuarantine Yes
```

If you want to change to the new feature Quarantine Manager Advanced, change this parameter to:

```
EnableLegacyQuarantine No
```

Further details on the Quarantine Manager can be found in Chapter 6.4 - Quarantine management – Page 98.

MaxMessage Size

Maximum message size (not in milter mode)

A value greater than 0 means that only emails that do not exceed the specified size are scanned. Larger emails are rejected. The value 0 means that emails of any size are scanned.

Syntax:

```
MaxMessageSize "number""GB|MB|KB"
```

Examples:

```
MaxMessageSize 4 KB, 3 MB, 2 GB.
```

Default:

```
MaxMessageSize 0
```

MinFreeBlocks

Minimum free system memory (not in milter mode)

Avira AntiVir MailGate denies incoming connection if free hard disk space falls below the specified value.

Syntax:

```
MinFreeBlocks "non-negative number"
```

Example:

```
MinFreeBlocks 50
```

Default:

```
MinFreeBlocks 100
```

Max Recipients PerMessage

Maximum number of recipients per email (not in milter mode)

This option defines the maximum number of recipients for an email.

The setting 0 disables this option, resulting in an unlimited number of recipients for an email.

Syntax:

```
MaxRecipientsPerMessage "non-negative number"
```

Example:

```
MaxRecipientsPerMessage 50
```

Default:

```
MaxRecipientsPerMessage 100
```

RefuseEmptyMailFrom

Refuse emails without sender names (not in milter mode)

Some emails do not contain sender names. With the default setting NO the SMTP server accepts all incoming emails. This setting should not be changed.

Syntax:

```
RefuseEmptyMailFrom "YES | NO"
```

Default:

```
RefuseEmptyMailFrom NO
```

Standards RFC2821, RFC821 and RFC2505 recommend that an SMTP server should accept all emails, even those without sender addresses. The default setting for the parameter `RefuseEmptyMailFrom` *should therefore not be changed.*

AllowSourceRouting

Allow source routing (not in milter mode)

The following address syntax is used for source routing:

```
@ONE,@TWO:JOE@THREE
```

This address defines the route of the email. It is sent via `ONE` and `TWO` to `JOE` at host `THREE`.

This option determines whether all receivers, with the exception of `JOE@THREE` should be excluded (`NO`) or whether the address should be retained (`YES`).

Syntax:

```
AllowSourceRouting "YES | NO"
```

Default:

```
AllowSourceRouting NO
```

InEnvelopeAddressesBangIs

Exclamation marks in envelope addresses (not in milter mode)

- If the parameter is set to `REFUSED` and the recipient address contains an exclamation mark, the message is refused.
- If the setting is `IGNORED` exclamation marks in recipient addresses are treated as normal characters.
- If the setting is `INTERPRETED` the recipient address is converted to the RFC821 standard format. For example the address
  `hostA!hostB!hostC!user`
  becomes
  `hostA,@hostB:user@hostC`

If source routing is enabled, the email is sent to hostA, otherwise it is sent to hostC.

Syntax:

```
InEnvelopeAddressesBangIs "option"
```

Example:

```
InEnvelopeAddressesBangIs IGNORED | REFUSED | INTERPRE-
TED
```

Default:

```
InEnvelopeAddressesBangIs REFUSED
```

InEnvelope Addresses PercentIs

Percentage signs in envelope addresses (not in milter mode)

If the parameter is set to `REFUSED` and the recipient address contains an percentage sign, the message is refused.

If the setting is `IGNORED` percentage signs in addresses are treated as normal characters.

If the setting is `INTERPRETED` the recipient address is converted to the RFC821 standard format. For example the address

```
user%hostC%hostB@hostA
```

becomes

```
@hostA,@hostB:user@hostC
```

If source routing is enabled, the email is sent to hostA, otherwise it is sent to hostC.

Syntax:

```
InEnvelopeAddressesPercentIs "option"
```

Example:

```
InEnvelopeAddressesPercentIs IGNORED | REFUSED |
INTERPRETED
```

Default:

```
InEnvelopeAddressesPercentIs REFUSED
```

AcceptLoose DomainName

Check syntax of email domains (not in milter mode)

A domain name should only contain the following characters: [-.0-9A-Za-z] The parameter `AcceptLooseDomainName` also allows domain names which violate this rule.

The setting `NO` means that a message is rejected if the domain name for the message delivery is incorrect (depending on source routing).

If the setting is `YES` the domain name is not scanned. The email is forwarded in all cases.

Syntax:

```
AcceptLooseDomainName "YES | NO"
```

Default:

```
AcceptLooseDomainName    NO
```

AddressFilter

Filter email addresses

This option enables or disables the address filter. If the setting is `NO` (default setting) the default installation does not use an address filter.

Syntax:

```
AddressFilter "YES | NO"
```

Default:

```
AddressFilter NO
```

You need the following files to use the address filter:

```
/etc/avira/avmailgate.ignore
```

and

```
/etc/avira/avmailgate.scan
```

These files contain lines with email addresses and optionally the flags S/s (sender) and/or R/r (recipient). The specified email addresses are only scanned by the SMTP protocol (MAIL FROM and RCPT TO). The email addresses in the email headers are ignored.

The lists are scanned. The checking begins with the first list in `FilterTableOrder`. If there is accordance, the check is ended and the scheduled action is carried out.

The following options are available, depending on the result:

- If there is no accordance in the first list, the next list is scanned.
- If there is also no accordance in the second list, the email is scanned.
- If there is accordance in the ignore list, the email is not scanned.
- If there is accordance in the scan list, the email is scanned.

The email addresses can contain regular expressions in Perl format, e.g.

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

Example:

/etc/avira/avmailgate.ignore contains the following lines:

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

The email is not scanned if the address is somebody@somewhere.tld.

The email is not scanned if the recipient address is virus@firm*. In this case, the R-flag is optional:

/^virus@firm/ R is equivalent to */^virus@firm/*.

When Avira AntiVir MailGate is started, log entries will be made which indicate whether the address filter is active or inactive :

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

or

```
addressfilter is not active
```

Assign recipient addresses to groups

To draw up detailed statistics on email traffic, it is useful to assign recipients to groups. This can be done either with the aid of an ActiveDirectory server or a simple text file.

To use an ActiveDirectory server, the ActiveDirectoryURI configuration option (see ActiveDirectoryServerURI – Page 37) must be set to the URI at which the ActiveDirectory server can be reached.

If no ActiveDirectory server is available or if this is not to be used, the ActiveDirectoryServerURI must refer to the text file being used. In this case, a plain file name such as

/etc/avira/avmailgate.groups

must be specified.

Please do not use multiple file paths, but a unique single path.

In this file, the email addresses are assigned to the required group with the aid of regular expressions. The regular expressions used are specified in the PCRE syntax.

Lines beginning with a hash symbol (#) are ignored.

Every line begins with the keyword “grp”, followed by a space. The space is followed by a regular expression in perl-format. Another space and the group name form the final element. All addresses corresponding to the specified regular expression are assigned to this group name.

Example:

```
grp /^person\d+@example.com$/ groupOne
```

In this case, all addresses beginning with the element ‘person’, followed by one or more numbers and ‘@example.com’ are assigned to the group ‘groupOne’.

It is not possible to specify both a filename and one or more Active Directory server URIs.

Mapping of email addresses to organizational units

With the help of an ActiveDirectory server Avira AntiVir MailGate generates a list of names of organizational units that the given user belongs to.

The following description applies to the use of an ActiveDirectory server. If you have entered a text file to the ActiveDirectoryServerURI the following is not valid.

The sequence of the list has the following order:

- The list starts with the organizational units listed in the memberOf attribute of the ActiveDirectory record associated with the user. They are sorted alphabetically.
- The following entry contains the specified Distinguished Name of the primary group of the user, sorted alphabetically.
- The next entry lists the Distinguished Name of the parent elements of the ActiveDirectory record associated with the user. All inner lists are sorted alphabetically.

If the options ActiveDirectoryGroupBlackList or ActiveDirectoryGroup WhiteList are configured, Avira AntiVir MailGate uses the mentioned template for list entries. This might remove one or more items from the list. The first item of the resulting list is considered as the organizational unit of the user.

The following configuration options are available:

ActiveDirectory Support

ActiveDirectory Support

This option enables and disables the function. It is disabled by default and can be activated by

```
ActiveDirectorySupport YES
```

Syntax:

```
ActiveDirectorySupport "YES | NO"
```

Default:

```
ActiveDirectorySupport NO
```

The assignment of email addresses to organizational units can now be carried out by the Active Directory Server.

***Warning**: If, during configuration of the InetProtocols you turn off IPv4 support, both ActiveDirectory and SNMP support are automatically disabled, as they are based on IPv4. The following features of Avira AntiVir MailGate require IPv4: Milter mode, ActiveDirectory support and SNMP support.*

ActiveDirectory ServerURI

Access to the ActiveDirectory server

This option determines how the ActiveDirectory server can be accessed.
A file path can also be specified if you wish to use a text file rather than an Active Directory server to assign groups.

Syntax:

```
ActiveDirectoryServerURI "characters"
```

Default:

```
ActiveDirectoryServerURI ldap://my.ad-server.com:389
```

A valid LDAP-URI for an ActiveDirectory server is established as follows:

Example:

```
ActiveDirectoryServerURI /path/to/file
```

If you specify an absolute filename such as:

```
ActiveDirectoryServerURI /etc/avira/avmailgate.groups
```

in this config option, no ActiveDirectory server is needed. A list of mappings from email addresses to group names is read from the given file instead.

Multiple LDAP-URIs can also be specified. In this case, the individual URIs must be separated by a space and should have the same login credentials.

Example:

```
ActiveDirectoryServerURI ldap://my.ad-server1.com
ldap://my.ad-server2.com ldap://my.ad-server3.com
```

It is not possible to specify both a filename and one or more ActiveDirectory server URIs.

ActiveDirectory BaseDN

ActiveDirectoryBaseDN

This option defines the branching of the ActiveDirectory tree at which the email address scan is to be initiated. When configuring ActiveDirectory support this parameter is mandatory.

Syntax:

```
ActiveDirectoryBaseDN "characters"
```

Default:

```
ActiveDirectoryBaseDN
```

Example:

```
ActiveDirectoryBaseDN dc=example,dc=com
```

ActiveDirectory Login

ActiveDirectoryLogin

This option specifies the user name for logging in to the ActiveDirectory Server. The user name must be designated a Distinguished Name.

Syntax:

```
ActiveDirectoryLogin "characters"
```

Default:

```
ActiveDirectoryLogin
```

Example:

```
ActiveDirectoryLogin
cn=Administrator,cn=Users,dc=mail,dc=example,dc=com
```

If no `ActiveDirectoryLogin` is specified, Avira AntiVir MailGate will issue anonymous queries. If your ActiveDirectory server does not allow anonymous queries, however, the queries will fail.

ActiveDirectory Password

ActiveDirectoryPassword

This option specifies the password for the `ActiveDirectoryLogin`.

Syntax:

```
ActiveDirectoryPassword "characters"
```

Example:

```
ActiveDirectoryPassword secret
```

Default:

```
ActiveDirectoryPassword ""
```

Only a single value (login or password) for the `ActiveDirectoryLogin` and `ActiveDirectoryPassword` may be specified in the avmailgate.conf file.

This option is without effect if no `ActiveDirectoryLogin` has been specified.

ActiveDirectory UseTLS

ActiveDirectoryUseTLS

The `ActiveDirectoryUseTLS` option enables TLS encryption of all ActiveDirectory connections. You can enable TLS encryption by setting the option to `YES`:

```
ActiveDirectoryUseTLS YES
```

Syntax:

```
ActiveDirectoryUseTLS "YES | NO"
```

Default:

```
ActiveDirectoryUseTLS NO
```

***Warning:** To use TLS encryption, the appropriate file must be specified under `ActiveDirectoryCACertificates`. Please make sure that the registered hostname in `ActiveDirectoryServerURI` is the same as the one recorded in the certificate file.*

ActiveDirectory CACertificates

ActiveDirectoryCACertificates

This option contains the path to the file which contains the certificates of all certificate authorities recognized by Avira AntiVir MailGate. All certificates have to be Base64-encoded.

Syntax:

```
ActiveDirectoryCACertificates "path"
```

Example:

```
ActiveDirectoryCACertificates /etc/known_cas.crt
```

ActiveDirectory SASLAuth Mechanism

ActiveDirectorySASLAuthMechanisms

This option defines the authentication procedure for the ActiveDirectory server. Options are `PLAIN` and `DIGEST-MD5`.

Syntax:

```
ActiveDirectorySASLAuthMechanism "option"
```

Default:

```
ActiveDirectorySASLAuthMechanism PLAIN
```

The default setting PLAIN may constitute a security risk in that in this case the authentication is sent to the server as plaintext. This could allow third parties with access to the traffic on the network to obtain your login data.
We therefore advise you to use PLAIN only when authentication is carried out via a TLS-encrypted connection.

***Warning**: If DIGEST-MD5 is used, the authentication as administrator may fail.*

ActiveDirectory SearchTimeout

ActiveDirectorySearchTimeout

This option defines how many milliseconds should elapse before a search is terminated (if no response has been sent).

Syntax:

```
ActiveDirectorySearchTimeout "non-negative number"
```

Example:

```
ActiveDirectorySearchTimeout 1000
```

Default:

```
ActiveDirectorySearchTimeout 30000
```

ActiveDirectory BindTimeout

ActiveDirectoryBindTimeout

This option defines how many milliseconds should elapse before Active Directory logins (bind operations) are terminated.

Syntax:

```
ActiveDirectoryBindTimeout "non-negative number"
```

Example:

```
ActiveDirectoryBindTimeout 1000
```

Default:

```
ActiveDirectoryBindTimeout 5000
```

ActiveDirectory CacheSize

ActiveDirectoryCacheSize

This option defines how many LDAP queries should be cached by Avira AntiVir MailGate. The advantage of this is that identical queries are not sent to the ActiveDirectory server as the program can instead access the results

stored in the cache. In this way future queries can be processed faster.

Syntax:

```
ActiveDirectoryCacheSize "non-negative number"
```

Example:

```
ActiveDirectoryCacheSize 812
```

Default:

```
ActiveDirectoryCacheSize 1024
```

There is a limit to the number of entries that can be stored. The cache capacity depends on the size of the RAM and the length of the search results.

ActiveDirectory CacheTTL

ActiveDirectoryCacheTTL

This option establishes how long the LDAP queries should be stored in the cache. The setting `0` disables this option.

Syntax:

```
ActiveDirectoryCacheTTL "timespan"
```

Example:

```
ActiveDirectoryCacheTTL 10m
```

Default:

```
ActiveDirectoryCacheTTL 30m
```

If Avira AntiVir MailGate receives an email within 30 minutes with a recipient for which a query already exists in the cache, the program reads this entry without having to also communicate with the Active Directory Server.

ActiveDirectory CheckUser AccountControl

ActiveDirectoryCheckUserAccountControl

This option determines that, when scanning email addresses, only active Active Directory accounts are delivered as search results, i.e. blocked accounts are excluded from the search results. The group assignment cannot be determined for inactive accounts. In this case the option Reject Unknown Recipients – Page 42 applies.

Syntax:

```
ActiveDirectoryCheckUserAccountControl "YES | NO"
```

Default:

```
ActiveDirectoryCheckUserAccountControl YES
```

ActiveDirectory GroupBlackList

ActiveDirectoryGroupBlackList

This option can determine which organizational units are included in the database. The function Reject Unknown Recipients remains unchanged.

Syntax:

```
ActiveDirectoryGroupBlackList "characters"
```

Default:

```
ActiveDirectoryGroupBlackList
```

The names of the organizational units are entered in a list in the form of Distinguished Names and separated by semi-colons.

Example:

```
ActiveDirectoryGroupBlackList FirstDN; SecondDN
```

The listed organizational units are ignored by the recipient search. This makes it possible to exclude specific organizational units from database statistics.

The `ActiveDirectoryGroupBlackList` settings are overridden by the `ActiveDirectoryGroupWhiteList` settings.

ActiveDirectory Group WhiteList

ActiveDirectoryGroup WhiteList

This option can determine which organizational units are included in the database. The function Reject Unknown Recipients remains unchanged.

Syntax:

```
ActiveDirectoryGroupWhiteList "characters"
```

Default:

```
ActiveDirectoryGroupWhiteList
```

The names of the organizational units are entered in a list in the form of Distinguished Names and separated by semi-colons.

Example:

```
ActiveDirectoryGroupWhiteList FirstDN; SecondDN
```

The names of the units listed are scanned during the recipient search. This makes it possible to include these units exclusively in the database statistics.

The `ActiveDirectoryGroupWhiteList` settings override the `ActiveDirectoryGroupBlackList` settings.

Reject Unknown Recipients

RejectUnknownRecipients

This option ensures that emails to recipients not in the directory trigger a non-temporary error (SMTP Code 550: “Requested action not taken: mailbox unavailable”). Temporary errors in contrast trigger a temporary error message (SMTP - Code 450: “Requested mail action not taken: mailbox unavailable”). An SMTP reply consists of a three digit number followed by some text. The first digit denotes whether the response is good, bad or incomplete at which 4xx is a temporary negative reply and 5xx is a permanent negative reply. The second digit encodes responses in specific categories, at which x5x indicates errors concerning mail-system. The third digit gives a finer gradation of meaning in each category.

Syntax:

```
RejectUnknownRecipients "YES | NO"
```

Default:

```
RejectUnknownRecipients NO
```

The setting has no effect if ActiveDirectorySupport is disabled.

Filter TableOrder

Filter table scan sequence

This option can only be used when AddressFilter is enabled (`AddressFilter YES`).

Syntax:

```
FilterTableOrder "option"
```

The possible parameters are:

```
FilterTableOrder scan,ignore
```

or

```
FilterTableOrder ignore,scan
```

Default:

```
FilterTableOrder scan,ignore
```

SMTP Greeting Timeout

SMTPGreetingTimeout (not in milter mode)

This option defines the maximum timeout (in seconds) for receiving the greeting message from the remote host.

Syntax:

```
SMTPGreetingTimeout "non-negative number"
```

Example:

```
SMTPGreetingTimeout 100
```

Default:

```
SMTPGreetingTimeout 300
```

SMTPHelo Timeout

SMTPHeloTimeout (not in milter mode)

This option defines the maximum timeout (in seconds) for a response to the SMTP commands HELO and EHLO.

Syntax:

```
SMTPHeloTimeout "non-negative number"
```

Example:

```
SMTPHeloTimeout 100
```

Default:

```
SMTPHeloTimeout 300
```

SMTP MailFrom Timeout

SMTPMailFromTimeout (not in milter mode)

This option defines the maximum timeout (in seconds) for a response to the command MAIL FROM.

Syntax:

```
SMTPMailFromTimeout "non-negative number"
```

Example:

```
SMTPMailFromTimeout 100
```

Default:

```
SMTPMailFromTimeout 300
```

SMTP RcptTimeout

SMTPRcptTimeout (not in milter mode)

This option defines the maximum timeout (in seconds) for a response to the command RCPT TO.

Syntax:

```
SMTPRcptTimeout "non-negative number"
```

Example:

```
SMTPRcptTimeout 100
```

Default:

```
SMTPRcptTimeout 300
```

SMTP DataTimeout

SMTPDataTimeout (not in milter mode)

This option defines the maximum timeout (in seconds) for a response to the command DATA.

Syntax:

```
SMTPDataTimeout "non-negative number"
```

Example:

```
SMTPDataTimeout 100
```

Default:

```
SMTPDataTimeout 120
```

SMTP DataBlock Timeout

SMTPDataBlockTimeout (not in milter mode)

This option defines the maximum timeout (in seconds) when sending individual data blocks.

Syntax:

```
SMTPDataBlockTimeout "non-negative number"
```

Example:

```
SMTPDataBlockTimeout 100
```

Default:

```
SMTPDataBlockTimeout 180
```

SMTP DataPeriod Timeout

SMTPDataPeriodTimeout (not in milter mode)

This option defines the maximum timeout (in seconds) for a response to the concluding period of the commands DATA and QUIT after sending the message.

Syntax:

```
SMTPDataPeriodTimeout "non-negative number"
```

Example:

```
SMTPDataPeriodTimeout 100
```

Default:

```
SMTPDataPeriodTimeout 600
```

Max Forwarders

Maximum number of forwarding processes (not in milter mode)

This option defines the maximum number of simultaneous forwarding processes. The optimal value depends on the efficiency of your email system and the quality of the email connection.

Syntax:

```
MaxForwarders "non-negative number"
```

Example:

```
MaxForwarders 5
```

Default:

```
MaxForwarders 10
```

ForwardTo

Forwarding

This option defines how emails are sent (Default setting: by Sendmail).

Default:

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

The emails can also be sent by SMTP.

Syntax:

```
ForwardTo   SMTP: "characters" port "characters"
```

or

```
ForwardTo   SMTP: "characters" port "number"
```

E.g.:

```
ForwardTo   SMTP: localhost port 825
```

or

```
ForwardTo   SMTP: localhost port smtp
```

The SMTP setting is only active if Avira AntiVir MailGate is running in SMTP mode. In milter mode, emails can only be forwarded by the program. In this case the correct entry is:

```
ForwardTo /path/to/file
```

If you enable only IPv6 support using the option InetProtocols, you have to specify IPv6 addresses for the ListenAddress, ForwardTo and ForwardTo2 options, as well as in the avmailgate.acl file.

ForwardTo2

ForwardTo2

This option can be used to set up an alternate SMTP forwarding server which can be used if the primary forwarding server, defined by ForwardTo fails.

Syntax:

```
ForwardTo2 "characters"
```

Example:

```
ForwardTo2 SMTP: smtp.example.com port 25
```

Avira AntiVir MailGate uses this setting when no connection to the primary forwarding server can be established, the status code 421 is received in response to a SMTP command or if no response is received within the specified time (Timeout).

UsePipelining InSMTPClient

UsePipelining

UsePipeliningInSMTPClient: This configuration option determines whether the SMTP client integrated into Avira AntiVir MailGate uses SMTP extension Pipelining (according to RFC 2920).

Syntax:

```
UsePipeliningInSMTPClient "YES | NO"
```

Default:

```
UsePipeliningInSMTPClient NO
```

To enable this option, an SMTP server must be set up as a forwarding agent using the ForwardTo option and support extension Pipelining. This option significantly accelerates the delivery of emails, in particular if Avira AntiVir MailGate is installed on a system other than the SMTP forwarding server.

ScannerListen Address

ScannerListenAddress

The location of the scanner's socket. Avira AntiVir MailGate connects to this specified socket to perform scan requests.

Syntax:

```
ScannerListenAddress "path"
```

Default:

```
ScannerListenAddress /var/run/avmailgate/scanner
```

If you change this parameter, you must also change the value for `ListenAddress` *in* /etc/avira/avmailgate-scanner.conf *(see Scanner configuration in avmailgate-scanner.conf – Page 84).*

Max Attachments

Maximum number of email attachments (MIME)

An email is classed as suspicious if it exceeds the maximum number of attachments (Default setting: `100`).
See also `BlockSuspiciousMime`.

Syntax:

```
MaxAttachments "non-negative number"
```

Example:

```
MaxAttachments 50
```

Default:

```
MaxAttachments 100
```

Block Suspicious Mime

Block suspicious emails (MIME)

This option lets you block suspicious MIME emails. An email is classed as suspicious based on the `MaxAttachments` setting. (Default setting: NO).

Syntax:

```
BlockSuspiciousMime "YES | NO"
```

Default:

```
BlockSuspiciousMime NO
```

Block Fragmented Message

Block fragmented emails

This parameter is used to block fragmented emails. Further information can be found in “Message Fragmentation and Reassembly” in RFC 2046 (http://www.faqs.org/rfcs/rfc2046.html, Section 5.2.2.1).

Syntax:

```
BlockFragmentedMessage "YES | NO"
```

Default:

```
BlockFragmentedMessage NO
```

BlockPartial Archive

Block partial archives

If this option is enabled (YES), emails with archives which are part of a multivolume archive are blocked.

Syntax:

```
BlockPartialArchive   "YES | NO"
```

Default:

```
BlockPartialArchive NO
```

Block Extensions

Block emails with specific extensions

Avira AntiVir MailGate can be configured to block emails containing attachments with specific file extensions (e.g. exe, scr or pif). The block also applies to archived files. Each extension is separated by a semicolon. If this parameter is set to NO, MailGate allows extensions of any kind.

Syntax:

```
BlockExtensions "extension1; extension2 | NO"
```

Default:

```
BlockExtensions NO
```

Example:

```
BlockExtensions exe;scr;pif
```

Each individual file extension should not exceed 120 characters.

Expose Recipient Alerts

Send alerts to recipients of suspicious emails

You can send alerts relating to viruses and unwanted programs to the recipient.
Possible values:

- NO: the recipient receives no virus alert.
- LOCAL: Alarm messages are only sent when the recipient is a local user in your domain. Set the option in avmailgate.acl to`local`. Note, that `local` has no effect in milter mode.
- YES: the recipient always receives a virus alert.

Syntax:

```
ExposeRecipientAllerts "option"
ExposeRecipientAlerts YES | NO | LOCAL
```

Default:

```
ExposeRecipientAlerts LOCAL
```

Expose SenderAlerts

Send alerts to senders of suspicious emails

You can send alerts relating to viruses and unwanted programs to the sender.
Possible values:

- NO: the sender receives no virus alert.
- LOCAL: Alert messages are only sent when the sender is a local user in your domain. Set the option in avmailgate.acl to`local`. Note, that `local` has no effect in milter mode.
- YES: the sender of a suspicious email always receives a virus alert.

Syntax:

```
ExposeSenderAlerts "option"
ExposeSenderAlerts YES | NO | LOCAL
```

Default:

```
ExposeSenderAlerts LOCAL
```

Expose Postmaster Alerts

Send alerts to the postmaster

You can send alerts relating to viruses and unwanted programs to the postmaster.

Syntax:

```
ExposePostmasterAlerts YES | NO
```

Default:

```
ExposePostmasterAlerts YES
```

AlertsUser

Alert recipients

Specifies the sender address of notification emails, if unwanted programs or viruses are detected.

Syntax:

```
AlertsUser "characters"
```

Default:

```
AlertsUser AvMailGate
```

***Warning**: If, during configuration of the InetProtocols you turn off IPv4 support, both ActiveDirectory and SNMP support are automatically disabled, as they are based on IPv4. The following features of Avira AntiVir MailGate require IPv4: Milter mode, ActiveDirectory support and SNMP support*

SNMP Recipient

SNMP Recipient

Avira AntiVir MailGate can be configured in such a way that administrators are notified via SNMP traps of events, e.g. virus detections. A specification for these traps is supplied in MIB format in the files AVIRA-MIB.txt and AVIRA-MAILGATE-V0-MIB.txt.

Syntax:

```
SNMPRecipient hostname|IP address[:port]
```

Default:

```
SNMPRecipient ""
```

Example, insert:

```
SNMPRecipient localhost:162
```

into *avmailgate.conf* to specify the hostname or IP address to which the SNMP traps are to be sent. This information can be optionally supplemented with a colon, followed by the required port number, if, for example, the default port is not being used.

The setting SNMPRecipient is only active if SNMP notifications are enabled in Notification Mechanisms.

SNMPSender

Set up sender for SNMP traps

This option can be used to define which IP address is specified as the sender address in SNMP traps. If a hostname is specified, this will be used to determine the IP address being used by means of DNS-lookup.

Syntax:

```
SNMPSender "IP address|hostname"
```

Example:

```
SNMPSender 192.168.1.100
```

The setting SNMPSender is only active if SNMP notifications are enabled in Notification Mechanisms.

SNMP Community

SNMP Community

Applications that support SNMP can be grouped on the basis of community membership. Information on community membership is restricted to 255 characters.

Syntax:

```
SNMPCommunity "characters"
```

Default:

```
SNMPCommunity Avira
```

The setting SNMPCommunity is only active if SNMP notifications are enabled in Notification Mechanisms.

Notification Mechanisms

NotificationMechanisms

As soon as Avira AntiVir MailGate identifies a problem, an email notification can be sent to the postmaster. These problems include, for example, MailGate is trying to scan an email and the connection to SAVAPI fails.

Syntax:

```
NotificationMechanisms "characters"
```

Valid options:

```
NotificationMechanisms EMAIL; SNMP | NONE
```

Default:

```
NotificationMechanisms EMAIL
```

If the configuration is set to

```
EMAIL
```

a notification is sent by email.

If the configuration is set to

```
EMAIL;SNMP
```

a notification is sent by email and via SNMP traps.

If the configuration is set to

```
NONE
```

no notification is sent.

Example:

```
NotificationMechanisms EMAIL;SNMP
```

Email notifications are enabled by default. SNMP traps are disabled by default. In order to send SNMP traps, you have to specify a valid SNMP Recipient .

Please use the Postmaster configuration option to specify whom notifications should be sent to.

AddStatusInBody

Status information in the text of the email

You may insert additional information in the body of emails.

Syntax:

```
AddStatusInBody "YES | NO"
AddStatusInBody /path/to/file
```

Default:

```
AddStatusInBody NO
```

If the setting is NO, no status information is inserted in the body of the emails.

If the setting is YES the following options are available:

- If a file called `body-state` exists in the templates sub-directory of the program, the text from this file is inserted into the email (see Configuring report templates – Page 88).
- With `AddStatusInBody` you can also assign the name to a file. In this case the content of the assigned file is used.

`AddStatusinBody` modifies the emails just before they are forwarded, i.e. only clean emails will be modified.

MaxMessageSizeStatus

Statustext

If the `AddStatusInBody` option is set to `YES` no status text is added to an email that exceeds the specified size. You can enter the size in `gigabytes (GB)`, `megabytes (MB)`, `kilobytes (KB)` or `bytes`. Please note that values larger than 2000 MB (2GB) are not allowed.

Syntax:

```
MaxMessageSizeStatus "size"
```

Examples:

```
MaxMessageSizeStatus 4KB,3MB
```

Default:

```
MaxMessageSizeStatus 0
```

ForwardAllEmailAsMIME

Forward emails as MIME (not in milter mode)

Emails that are not in MIME format can be converted to this format. You then have at your disposal a MIME header with content type: text/plain, content disposition: inline and content encoding: 7 bit or 8 bit. The encryption depends on the original email.

If the setting is NO, emails that are not in MIME format are sent without further processing.

If the setting is YES, these emails are converted to MIME format.

Syntax:

```
ForwardAllEmailAsMIME  "YES | NO"
```

Default:

```
ForwardAllEmailAsMIME NO
```

ScanInArchive

Scan archives

If the setting is NO, archives are not scanned for viruses and unwanted programs.

If the setting is YES, all archived files are extracted and scanned. For this the settings in `ArchiveMaxSize`, `ArchiveMaxRecursion` and `ArchiveMaxRatio` apply.

Syntax:

```
ScanInArchive     "YES | NO"
```

Default:

```
ScanInArchive YES
```

Archive MaxSize

Maximum size of archived files when extracted

There are some archived files with worthless content which, when extracted, "expand" to a significant size with the explicit intention of compromising computer performance. This parameter prevents such archive files from being extracted.

If the setting is 0, all archived files are extracted irrespective of size.

If the setting is >0, all archives which do not exceed the specified size (in bytes) are extracted and scanned.

If MailGate is running in Milter mode and the value of the option ArchiveMaxSize is set lower than 5120 bytes, MailGate will print and log the following warning message:

Warning: The value of the ArchiveMaxSize option (n) is lower than the recommended minimum value (5120). This may lead to MailGate's notification emails being blocked. It is strongly recommended to increase the value to 5120 or higher.
Whereat (n) is the configuration value of ArchiveMaxSize.

Syntax:

```
ArchiveMaxSize "size"
```

Examples:

```
ArchiveMaxSize 2KB (2 kilobytes), 3MB (3 megabytes)
```

Default:

```
ArchiveMaxSize 0
```

ArchiveMax Ratio

Block "Mail-bombs"

It is possible to block so-called "Mail-bombs" which have a very high compression

rate. You can specify the maximum difference between the compressed and uncompressed file size.

The setting 0 disables the option (**not** recommended). The default setting is 150.

Syntax:

```
ArchiveMaxRatio "non-negative number"
```

Example:

```
ArchiveMaxRatio 100
```

Default:

```
ArchiveMaxRatio 150
```

ArchiveMax Recursion

Maximum recursion depth in archives

If the setting is 0, recursive (nested) archives are extracted irrespective of their recursion depth.

If the setting is >0, all archives that do not exceed the specified recursion depth are extracted. This reduces processing time.

Syntax:

```
ArchiveMaxRecursion "non-negative number"
```

Example:

```
ArchiveMaxRecursion 10
```

Default:

```
ArchiveMaxRecursion 20
```

Block Suspicious Archive

Block emails with suspicious archives

If this option is enabled (YES), archives that Avira AntiVir MailGate has classified as suspicious are blocked.
All archives that cannot be fully scanned are deemed suspicious. Any archives that exceed limit values specified in `ArchiveMaxSize`, `ArchiveMaxRecursion` and `ArchiveMaxRatio` are also deemed to be suspicious.

Syntax:

```
BlockSuspiciousArchive    "YES | NO"
```

If this option is disabled (NO), suspicious archives are also forwarded.

Default:

```
BlockSuspiciousArchive NO
```

Block Encrypted Archive

Block emails with password-protected archives

If the setting is `YES`, emails containing password-protected files in archives are rejected.

Syntax:

```
BlockEncryptedArchive    "YES | NO"
```

If the setting is `NO`, emails with encrypted archives are also delivered.

Default:

```
BlockEncryptedArchive NO
```

Encrypted EmailAction

Handling encrypted emails

Avira AntiVir MailGate can deal with encrypted emails in three different ways.

Syntax:

```
EncryptedEmailAction "option"
```

Default:

```
EncryptedEmailAction IGNORE
```

1. The email is delivered/forwarded without a log entry or notification (default).
   ```
   EncryptedEmailAction IGNORE
   ```
2. The email is delivered/forwarded and the postmaster is notified.
   ```
   EncryptedEmailAction NOTIFY_POSTMASTER
   ```
3. The email is classified as suspicious. i.e. it is not delivered/forwarded.
   ```
   EncryptedEmailAction TREAT_AS_SUSPICIOUS
   ```

In order to receive notifications of the arrival of encrypted emails, it is necessary to specify `EMAIL` *in* Notification Mechanisms.

`EncryptedEmailAction` *can only be used with fully encrypted emails. The option does not work with emails in which, for example, only the attachment is encrypted.*

InetProtocols

InetProtocols

It is possible to use IPv6 in addition to the default IPv4. You can also choose to use IPv6 on its own.

Syntax:

```
InetProtocols "characters"
```

Default:

```
InetProtocols IPv4
```

To do this, change the default setting

```
InetProtocols IPv4
```

to meet your requirements, e.g. to

```
InetProtocols IPv4 ; IPv6
```

If you enable only IPv6 support, you have to specify IPv6 addresses for the ListenAddress *and* ForwardTo *options, as well as in the* avmailgate.acl *file.*

***Warning**: If you turn off IPv4 support, both ActiveDirectory support and SNMP support are automatically disabled, as these are based on IPv4. The following features of Avira AntiVir MailGate require IPv4:*
Milter mode, ActiveDirectory support and SNMP support.

Detecting

Detecting other unwanted programs

As well as viruses, other harmful or unwanted software is described in avmailgate.conf. The following options can be used to enable detection of this software and the corresponding default values are:

Default:

- `DetectADSPY yes`
  Detects software that displays advertising pop-ups or software that sends user's specific data to third parties.
- `DetectAPPL no`
  Detects applications of dubious origin and applications that might be hazardous to use.
- `DetectBDC yes`
  Detects control software for backdoors. In general these are harmless.
- `DetectDIAL yes`
  Detects dial-up programs for connections that charge a fee. Dial-up programs might cause huge costs.
- `DetectGAME no`
  Detects games that causes no damage on your computer.
- `DetectHIDDENEXT yes`
  Detects files that have an executable file extension which is hidden behind a harmless one.
- `DetectJOKE no`
  Detects harmless joke programs.
- `DetectPCK yes`
  Detects files that have been compressed with an unusual runtime compression tool. Please make sure that the source of these files is trustworthy.
- `DetectPHISH yes`
  Detects faked emails that are supposed to prompt the user to reveal confidential information as user accounts, passwords or online-banking data on certain websites.
- `DetectSPR no`
  Detects software that may be able to compromise the security of your system, initiate unwanted program activities, damage your privacy or spy out your user behaviour.

Heuristics Macro

Macrovirus heuristics

This option enables heuristics for macroviruses in documents and allows to detect malware before you had a chance to perform an update.

Syntax:

```
Heuristicsmacro "YES | NO"
```

Default:

```
HeuristicsMacro YES
```

Heuristics Level

Win32 heuristics

This option defines the detection level of Win32 heuristics. Permitted values are `0` (Off), `1` (Low), `2` (Medium) and `3` (High).

Syntax:

```
HeuristicsLevel "non-negative number"
```

Example:

```
HeuristicsLevel 1
```

Default:

```
HeuristicsLevel 3
```

Block OnError

Block emails in the case of scan errors

If the setting is YES, emails are blocked if an error occurs when scanning archives in the attachment or if the scan process is terminated by a timeout.

Syntax:

```
BlockOnError "YES | NO"
```

Default:

```
BlockOnError NO
```

Block Unsupported Archive

Block emails with unsupported archives

Emails with archives which the Scanner does not support are blocked.

Syntax:

```
BlockUnsupportedArchive "YES | NO"
```

Default:

```
BlockUnsupportedArchive NO
```

Reject AlertMail

Reject emails containing alerts (only in milter mode)

If `RejectAlertMail` is set to `YES`, emails containing an alert with the message "Alert found in email" are rejected and placed in the quarantine directory (depending on the QuarantineAlert setting).

Syntax:

```
RejectAlertMail "YES | NO"
```

If `RejectAlertMail` is set to `NO`, the email is accepted and placed in the quarantine directory.

Default:

```
RejectAlertMail NO
```

Quarantine Directory

Rejected emails are moved to the quarantine directory. You have to remove the

files manually from this directory. To remove all rejected emails you can use the following option (6.4 Quarantine management and the option **AlertAction** below)

```
avmailgate.bin --avq --remove=all
```

Quarantine Alert

Place alert emails in quarantine (only in milter mode)

If both `QuarantineAlert` and `RejectAlertMail` are set to `YES`, emails containing an alert are rejected and placed in quarantine.

If `QuarantineAlert` is set to `NO` and `RejectAlertMail` is set to `YES`, the email is rejected and not placed in quarantine.

Syntax:

```
QuarantineAlert "YES | NO"
```

Default:

```
QuarantineAlert YES
```

AlertAction

AlertAction

This option determines whether infected or suspicious emails will be moved to the quarantine directory or will be deleted immediately. Independent from your settings of `EnableLegacyQuarantine` the following values are accepted:

- `QUARANTINE` Alerts and suspicious emails will be sent to the quarantine directory.
- `DELETE_ALERTS` Alert emails will be deleted. Suspicious emails will be sent to quarantine.
- `DELETE_ALL` Alerts as well as suspicious emails will be deleted.

Syntax:

```
AlertAction "option"
```

Default:

```
AlertAction QUARANTINE
```

Enhanced QueueHandling

Limit queue length

(Not available in milter mode) Both the queue load for `incoming` and `outgoing` emails can be limited. You may activate this feature separately for each queue.

The specified parameters for the incoming emails queue are:

Syntax:

```
IncomingHighFillLevel "non-negative number"
IncomingLowFillLevel "non-negative number"
```

For the outgoing emails queue:

Syntax:

```
OutgoingHighFillLevel "non-negative number"
OutgoingLowFillLevel "non-negative number"
```

Default for all parameters is:

```
0
```

A maximum (`HighFillLevel`) and minimum (`LowFillLevel`) threshold value are defined for this purpose. As soon as the maximum value is reached, any other emails are rejected with a temporary error message (SMTP Code 452: insufficient system storage). Depending on the performance and load of the system, the number of emails might slighty exceed the given threshold. By setting a valid treshold value you specify at what level the incoming or outgoing queue is "congested" or is "available". New connections are not accepted until the number of emails in the queue drops to the minimum value (`LowFillLevel`) or below this value.
On startup, each queue's status is reset to "available". If the number of emails in a queue is greater or equal to the defined `HighFillLevel`, the queue is considered as "congested". If the number of emails in a queue is less or equal to its `LowFillLevel`, the queue is considered as "available". If the number of emails in a queue is less than the `HighFillLevel` but larger than the `LowFillLevel` and the queue's previous state was "congested", its state remain unchanged. To change this status the number of emails has to drop to the `LowFillLevel` again.

On a restart, Avira AntiVir MailGate will accept new emails regardless to the previous state. The system does not recall a previous "congested" state of a queue.

When the set threshold value is reached, the postmaster is informed by SNMP trap or email with the aid of the Notification Mechanisms function.

The number of emails counted will also contain those created by Avira AntiVir MailGate itself.

The following statements are valid:

- The threshold value for both `HighFillLevel` and `LowFillLevel` is 0 (default).
- The threshold value for `HighFillLevel` is greater than that for `LowFillLevel`.

If invalid statements are made, Avira AntiVir MailGate will not start.

PollPeriod

Scan queue (not in milter mode)

This option defines the interval at which the program scans the email queue for viruses and malware (in seconds).

Syntax:

```
PollPeriod "non-negative number"
```

Example:

```
PollPeriod 30
```

Default:

```
PollPeriod 60
```

Queue Lifetime

Storage time for emails in the queue (not in milter mode)

The maximum time an email spends in the queue before it is rejected. The value can be specified in seconds, minutes, hours or days. Examples: 10s, 10m, 10h, 10d.

Syntax:

```
QueueLifetime "timespan"
```

Example:

```
QueueLifetime 1h
```

The setting 0 disables this option.

Default:

```
QueueLifetime 0
```

Forwarder RetryDelay

Set up the forwarding interval (not in milter mode)

This option enables you to set the maximum interval at which Avira AntiVir MailGate attempts to re-forward the email. If the `ForwarderRetryDelay` value is less than the `PollPeriod` value, MailGate will forward the email at the interval set for `PollPeriod`. I.e. the forwarding interval is whichever is the greater, the `ForwarderRetryDelay` value or the `PollPeriod` value.

Syntax:

```
ForwarderRetryDelay "timespan"
```

Example:

```
ForwarderRetryDelay 1h
```

You can specify the value in seconds (`s`), minutes (`m`), hours (`h`) or days (`d`).

Default:

```
ForwarderRetryDelay 30m
```

Each time Avira AntiVir MailGate uses `ForwarderRetryDelay` to attempt to forward the emails in the queue, the maximum storage time for these emails is checked. The value specified for `QueueLifetime` should therefore be a multiple of the `ForwarderRetryDelay` value.

Example:

```
QueueLifetime 3d
ForwarderRetryDelay 30m
```

Throttle Message count

Maximum number of emails for processing (not in milter mode)

This option is necessary when too many emails have accumulated in the queue and Avira AntiVir MailGate is restarted.

In this case, all emails are processed as quickly as possible. This can cause load problems.

The value specified is the maximum number of emails processed by

ThrottleDelay (see the following example).

It is important that no other emails are accepted while this option is enabled. These emails would not be processed immediately.

This option should only be used on a temporary basis.

The ThrottleDelay option must also be defined.

Syntax:

```
ThrottleMessageCount "non-negative number"
```

Default:

```
ThrottleMessageCount 0
```

Throttle Delay

Maximum number of emails for sending (not in milter mode)

This option defines how many emails (ThrottleMessageCount) are sent in a specified period (in seconds). Default setting: 0 (disables the option).

Syntax:

```
ThrottleDelay "non-negative number"
```

Default:

```
ThrottleDelay 0
```

Example:

There are 100 emails in the queue. ThrottleMessageCount is set to 10, ThrottleDelay to 1. This setting allows a maximum of 10 emails to be processed per second.

Bounce MessageUser

Sender for undeliverable ("Bounce") emails (not in milter mode)

The user specified by the sender of an email which cannot be delivered by the MTA.

Syntax:

```
BounceMessageUser "characters"
```

Default:

```
BounceMessageUser MAILER-DAEMON
```

or

```
BounceMessageUser MAILER-DAEMON@domainname
```

Bounce Message SizeBody

Extent of the content of the bounce-email (not in milter mode)

Defines the extent to which the original email text is reproduced in the bounce-email (in bytes). The value 0 means there is no upper limit.

Syntax:

```
BounceMessageSizeBody "number""GB|MB|KB"
```

Examples:

```
BounceMessageSizeBody 4KB, 3MB, 2GB.
```

Default:

```
BounceMessageSizeBody 0
```

Bounce Message SizeHeader

Length of the bounce-email header (not in milter mode)

Defines the extent to which the original email header is reproduced by the bounce-email (in bytes). The value 0 means there is no upper limit.

Syntax:

```
BounceMessageSizeHeader "number""GB|MB|KB"
```

Examples:

```
BounceMessageSizeHeader 2KB (2 kilobytes), 3MB (3
megabytes), 2GB (2 gigabytes)
```

Default:

```
BounceMessageSizeHeader 0
```

AddXHeader

Add X-header

If the setting is YES, the queue ID and scan-status information are added to the email header. Example: **X-AntiVirus: checked by AntiVir MailGate...** The text cannot be changed.

Syntax:

```
AddXHeader "YES | NO"
```

Default:

```
AddXHeader YES
```

AddReceived ByHeader

Add "Received:" stamp to header (not in milter mode)

If the setting is YES, the scanned email contains information on the entry time.

Syntax:

```
AddReceivedByHeader YES | NO
```

Default:

```
AddReceivedByHeader YES
```

MaxHop count

Avoid mail loops

If the header contains more "Received" lines than specified in this option, the email is blocked.

Syntax:

```
MaxHopCount "non-negative number"
```

Example:

```
MaxHopCount 50
```

Default:

```
MaxHopCount 100
```

ScanTimeout

Maximum time for email scan

This option defines the maximum time for the email scan (in seconds).

Syntax:

```
ScanTimeout "non-negative number"
```

Example:

```
ScanTimeout 100
```

Default:

```
ScanTimeout 300
```

External Program

Execute an external program or script if a virus/unwanted program is discovered

Accesses an external program or script if a virus/unwanted program is detected. The parameter is the ID of the rejected email (see Avira AntiVir MailGate-Spool directories – Page 24).

Syntax:

```
ExternalProgram "path"
```

Example:

```
ExternalProgram /path/to/program
ExternalProgram /dir/my_own_script
```

Default:

```
None
```

NotifyEnd OfLicense

Information on the license expiry date

Sends a message to the postmaster every day before the license expiry date (in days). If the value is 0 no message is sent.

Syntax:

```
NotifyEndOfLicense "number"
```

Example:

```
NotifyEndOfLicense 15
```

Default:

```
NotifyEndOfLicense 30
```

Add Precedence Header

Add precedence header

If the setting is YES, the following line is added to the header of the notification email:
Precedence: junk.

Programs which respond automatically to incoming emails (e.g. vacation) do not react to this report. The entries YES and NO can be replaced by special text.

Syntax:

```
AddPrecedenceHeader "option"
```

```
AddPrecedenceHeader "YES | NO | custom text"
```

Default:

```
AddPrecedenceHeader NO
```

AddHeaderToNotice

Add email header for postmaster

You can include the header of a rejected email in the alert message sent to the postmaster. Possible values are `YES` and `NO`.

Syntax:

```
AddHeaderToNotice "YES | NO"
```

Default:

```
AddHeaderToNotice YES
```

GUISupport

Enabling GUI support

This option must be enabled to ensure Avira AntiVir MailGate can communicate with the
SMC-GUI. Required parameters (Default settings):

Syntax:

```
GuiSupport "YES | NO"
```

Default:

```
GuiSupport NO
GuiCAFile /usr/lib/AntiVir/mailgate/gui/cert/
cacert.pem
GuiCertFile /usr/lib/AntiVir/mailgate/gui/cert/
server.pem
GuiCertPass antivir_default
GuiRandFile /path/to/file
```

You also have to make sure that the following ports are open:

```
udp: 59411
tcp: 50360
```

If these parameters are missing or invalid, the GUI will not be available.

OpenMax

OpenMax

This option defines the maximum number of open files for Avira AntiVir MailGate processes. The default value is only set when the current system value is below the default value.

```
OpenMax 1024
```

If the value specified here is less than 1, Avira AntiVir MailGate ensures that at least 1024 files can be opened at the same time.

If the specified value is greater than 0, MailGate uses this value to define the maximum number of files which may be opened.

It is usually not necessary to change this value.

Syntax:

```
OpenMax "non-negative number"
```

Example:

```
OpenMax 1
```

Default:

```
OpenMax 0
```

5.2.1 Database support

Since version 3.1.0, Avira AntiVir MailGate supports the logging of statistics to a database.

For details on how to set up the database and other requirements, see Setup below. The database consists of two tables, called `alerts` and `counter`.

`Alerts` table contains information about each blocked alert.

This means that each alert is logged even if it occurred in the same mail.

`Counter` table contains summarized information about emails which were processed.

The Avira AntiVir MailGate package also contains sample files to be used with OpenOffice. See section OpenOffice.

Requirements

This is a list of version numbers of MySQL servers, MySQL ODBC drivers and ODBC driver managers which should be compatible:

MySQL 5.0.70
MySQL ODBC driver 3.51.11
iODBC 3.52.4

Setup

Before you enable database support, you have to install an ODBC driver manager and set it up. There are two driver managers available:

iODBC - www.iodbc.org (recommended)
unixODBC - www.unixodbc.org

Below is a description on how to install and set up ODBC on Debian 5.0 (please consult the distribution or driver manager manual on how to install and set up ODBC if you use another operating systems).

***Warning**: Avira AntiVir MailGate is a 32-bit binary and can't use a 64-bit shared object.This means it will not be able to use a 64-bit ODBC driver manager.*

For 64-bit machines you should make sure that the ODBC connector is a 32-bit shared object. For details about how to set up database support in Avira AntiVir MailGate on a 64-bit machine, see the file README.db-support-SLES10-SP2-64bit.

This file contains an example setup for ODBC on SuSE Linux Enterprise 10 SP2.

1. Set up the database

If you haven't already set up a user with access rights to the database, you should set one up now.
Please consult your database's manual for information on how to add a user to your database and grant the user access.

See the file /usr/lib/AntiVir/mailgate/create-db.sql for details on the database layout. The database layout is the script to create a MySQL database.

You can use this script to create the database (example for MySQL, with the server running on the specified host):

```
# mysql -u <db user> -p -h <your sql server host name>
< create-db.sql
```

Enter password.

In order to have the latest layout for the Avira AntiVir MailGate database you can upgrade the database by using the following script:

```
/usr/lib/AntiVir/mailgate/upgrade-db.sql
```

Columns added by the use of this script will not be available until MailGate has been restarted.

2. Install iODBC

You should choose a thread safe library. Please consult the distribution manual to check if your ODBC library was built with thread support.

```
# apt-get install libiodbc2
```

3. Install the corresponding database driver for your database

You should choose a thread safe driver. Please consult the distribution manual to check if your ODBC driver is thread safe.

Example for MySQL ODBC driver:

```
# apt-get install libmyodbc
```

4. Set up odbc.ini (see 5. for an example odbc.ini)

There are different ways to perform the setup:

- Create and/or edit /etc/odbc.ini
  or
- Copy /etc/avira/avmailgate-odbc.ini to /etc/odbc.ini and edit it
  or
- Edit /etc/avira/avmailgate-odbc.ini and set the configuration option "DBodbcIni" in /etc/avira/avmailgate.conf to "/etc/avira/avmailgate-odbc.ini"

If you want to configure the odbc.ini path from the Avira Security Manager Center (SMC) please notice that it is not possible to define the file via the SMC GUI. You may copy the path manually to the client, for example with the help of SCP or WinSCP or you may use the file copy function of the SMC. Please make sure that the file has the appropriate write permission. You can set the permission manually via SSH or you may use the chmod-workaround: /bin/chmod a+w/usr/lib/AntiVir/agent/mailgate-odbc.ini.

If you don't specify "DBodbcIni" in /etc/avira/avmailgate.conf, the library decides where to search for the odbc.ini.

The library might also use a different odbc.ini file if the specified file exists but is not readable/writable by the user MailGate is running as.

5. Sample odbc.ini

This is an example of a minimal odbc.ini file.

Please consult the documentation of your database driver for details on the available options.

[MailGate]
Driver = /usr/lib/odbc/libmyodbc.so
Server = hostname.of.my.sql.server
User = username
Password = password
Database = mailgate

[MailGate]: The DSN used by Avira AntiVir MailGate
Driver: This is the path to the driver's library
Server: Database server
User: Username for accessing the database
Password: Username's password
Database: Name of the database to use

6. Enable database support in avmailgate.conf

Set `DBSupport` to YES in /etc/avira/avmailgate.conf.

7. Test your ODBC setup

You can use the tool `avmg_stats` to check database connectivity. The utility `avmg_stats` is started by Avira AntiVir MailGate when `DBSupport` or `GuiSupport` is enabled. First of all `avmg_stats` parses the configuration file (/etc/avira/avmailgate.conf) for validation. It is used by Avira AntiVir MailGate to log to the database and it is used by the SMC to get information from MailGate. The client uses `avmg_stats` to interrogate the database.

```
/usr/lib/AntiVir/mailgate/gui/bin/avmg_stats -S
```

If successful, the tool will print the following:

```
$ /usr/lib/AntiVir/mailgate/gui/bin/avmg_stats -S
Using these settings:
ODBC ini:     <using system's odbc.ini.>
ODBC library: libodbc.so.1
ODBC source:  MailGate

Preparing connection ...
=> OK
Connecting ...
=> OK
Disconnecting ...
=> OK

Successfully verified database connectivity!
```

... and something similar if errors occur (example for MySQL, the error message may vary depending on the error type):

```
Using these settings:
ODBC ini:     <using system's odbc.ini.>
ODBC library: libodbc.so.1
ODBC source:  MailGate

Preparing connection ...
=> OK
Connecting ...
Failed to connect to ODBC data source (error code: -2)
([MySQL][ODBC 3.51 Driver]Lost connection to MySQL server at 'reading
initial communication packet', system error: 111)
```

Print CSV list

Avira AntiVir MailGate is able to print the tables' contents as a CSV (comma separated value) list. By default only the `alerts` table is printed. You can choose another table using the command line option `-t`.

The first line of the resulting list contains the column names. All other lines are the table's rows. The results are not sorted.

Example:

Print the "alerts" table:

```
# /usr/lib/AntiVir/mailgate/gui/bin/avmg_stats -o csv
```

Print the "counter" table:

```
# /usr/lib/AntiVir/mailgate/gui/bin/avmg_stats -o csv
-t counter
```

CSV separator:

Specify a field separator using one character:

```
-o csv:s
```

You must quote the separator for it to be interpreted by the shell.

Example:

Print the "alerts" table and separate by ";":

```
# /usr/lib/AntiVir/mailgate/gui/bin/avmg_stats -o
csv:';'
```

Time ranges:

You can limit the result to only list rows within a specific time range:

```
-R "YYYY-MM-DD HH:MM:SS/YYYY-MM-DD HH:MM:SS"
```

Example:

Print the "alerts" table limited to a specific time range:

```
# /usr/lib/AntiVir/mailgate/gui/bin/avmg_stats -o csv -
R "2009-05-15 00:00:00/2009-05-15 15:35:43"
```

This will list all alerts which were logged between 2009-05-15 00:00:00 and 2009-05-15 15:35:43

`Alerts` table description

When a mail is blocked, information about the alert(s) is immediately written to

the database.

Column	Description
id	This column has no special meaning. It's just an auto-incremented number.
reason	The reason why the mail was blocked. The following reasons exist: Alert - scanner found malware Spam - spam filter detected spam or another category (see "Spam filter" for details about categories) Error - an error occurred during the scan Incomplete - not completely scanned Encrypted - mail contains an encrypted attachment Extension - mail contains an attachment with a forbidden filename extension Limit - a limit was reached Suspicious - <not yet available> (not yet used) Unsupported - An archive with an unsupported compression method Unknown reason - reason is unknown (not yet used) ***Note**: other reasons may appear in this column in the future after product updates.*
alertname	Depends on reason: Alert - the name of the alert All other reasons - A detailed description of the reason
queueid	Queue ID of the mail
alerttype	Depends on reason: Alert - adware, backdoor, trash, dialer, heuristic, joke, program, riskware, trojan, virus, worm *(**Note**: other categories may appear in this column. The categories depend on the scanner and may change, or new ones may become available after a scanner update).* All other reasons - short description of the alertname

Column	Description
filename	The name of the file in which the alert was found. Depends on reason: Alert - file name of the file which caused the alert All other reasons - column contains "<no file name available>" ***Note**: The file name is limited to 100 characters. If truncated, the file name gets " ..." appended.*
action	Contains only `quarantined` at the moment.
source	The sender's mail address (limited to 40 characters). If truncated, the address gets " ..." appended.
alerturl	Unused ("")
missed	Due to internal buffer limits, it may be that not every alert can be written to the database. If this happens, the column "missed" contains the count of alert information which could not be written to the database.
product	Contains the product's name "MailGate".
rcpt	This column will store the recipient of an email as follows: - only the first recipient of an email, if `DBStoreAlertsForEachRecipient` is disabled. - every recipient of an email, if `DBStoreAlertsForEachRecipient` is enabled and the alerts table contains one row for each recipient.
vdf	Version information of the VDF which was used for scanning.
engine	Version information of the engine which was used for scanning.
hostname	The value of "MyHostName" (/etc/avira/avmailgate.conf). If "MyHostName" is not set, the value returned from gethostname(). If gethostname() fails, "localhost".

Column	Description
ou	If ActiveDirectorySupport is activated and a group look-up has been processed, the found value will be added to this column
date	The date and time the statistics daemon received the alert information. Date and time are the values received from `localtime_r`(). The format is YYYY-MM-DD HH:MM:SS. *"Date notes" for details on storing the date.*

`Counter` table description

The rows in the counter table are written periodically. The default setting is every completed hour.

You can change the delay between entries using the configuration option `DBUpdateDelay` in /etc/avira/avmailgate.conf.

Example:

```
DBUpdateDelay 30m
```

Write information to the database every 30 minutes
Possible units are: no unit/s=seconds, m=minutes, h=hours

Column	Description
id	This column has no special meaning. It's just an autoincremented number.
accepted	Count of mails accepted by the SMTP daemon
clean	Count of clean mails
alerts	Count of malware found
spam	Count of spam (blocked and not blocked) ***Note**: blocked mails also appear in the `alerts` table.*
sent	Count of mails successfully forwarded ***Note**: notification mails are counted also.*
notify_admin	Count of postmaster notifications
notify_sender	Count of sender notifications
notify_recipient	Count of recipient notifications
total_size	Summary of the mails' sizes
errors	Count of mails which caused an error while processing
incomplete	Count of mails which could not be scanned completely

Column	Description
unsupported	Count of mails which contained an unsupported compression method
encrypted	Count of mails with encrypted attachments
extension	Count of mails with a file attached whose file name contains a forbidden extension
limits	Count of mails which reached an archive limit while processing
unknown	Unused (0)
product	The product's name "MailGate"
ou	If ActiveDirectorySupport is activated and a group look-up has been processed, the found organizational units with their counts of processed emails are listed here
hostname	The value of "MyHostName" (/etc/avira/avmailgate.conf). If "MyHostName" is not set, the value returned from gethostname(). If gethostname() fails, "localhost".
date	The date and time when the counter results were compiled and written to the database. Date and time are the values received from localtime_r(). The format is YYYY-MM-DD HH:MM:SS. ***Note**: See Date notes for details on storing the date.*

Date notes

The date column contains the local date/time of the server Avira AntiVir MailGate is running on. The database script creates the date column as `DATETIME` data type.

Please note that there is no conversion of the date/time. The database server is not expected to convert date/time since the data type of the date column is `DATETIME` and not `TIMESTAMP`.

OpenOffice

The below description requires ODBC to be configured correctly on the machine on which you're running OpenOffice.

Please see section Setup on how to set up ODBC. You can also consult your operating system's documentation on how to set up ODBC.

The Avira AntiVir MailGate package contains two OpenOffice files "MailGate.odb"

and "Alerttype+Counter.ods" in the "doc" directory. These files can be used to add a database to OpenOffice and to receive information currently stored in the database.

MailGate.odb contains database information:
- An ODBC data source is used (called "MailGate")
- The username and password is "mailgate"

Additionally the file contains a macro which automatically registers the database in OpenOffice. See Macro for details. (This works only for OpenOffice 3.1 or later).

Alerttype+Counter.ods:
- Contains a set of data received from the database. The data can be refreshed to get the latest database content.
- Contains sample charts

Macro

The macro is used to automatically register the database when opening the odb-document. This macro only works with OpenOffice 3.1 (or later).

This is the macro embedded in "MailGate.odb":

```
***** BASIC *****
' The purpose of this macro is to register a database if it isn't already registered.
' The macro is linked to the "Open Document" event.
' This means it is always executed when opening the document.

Sub Main
Dim DatabaseName as String
Dim DatabaseCtx as Object
DatabaseName = "MailGate"

' Get context to access datasource
DatabaseCtx = CreateUnoService("com.sun.star.sdb.DatabaseContext")

' Check if database is already registered
If not DatabaseCtx.hasByName (DatabaseName) Then
Dim URL as String
    Dim DB as Object
URL = thisComponent.getURL
DB = DatabaseCtx.getByName (URL)
' Register database
DatabaseCtx.registerObject (DatabaseName, DB)
End If
End Sub
```

OpenOffice < 3.1

This section describes how to use the OpenOffice files with OpenOffice < 3.1.

Versions of OpenOffice < 3.1 are not able to use the embedded macro in "MailGate.odb". Thus you have to add the database manually.

▶ 1. Copy "MailGate.odb" from the package to your hard disk. (The file must exist if you want to use Alertype+Counter.ods in the future).

▶ 2. Start OpenOffice

▶ 3. Ignore the warning about macro security

▶ 4. Add the database manually:

↳ Tools -> Options

↳ OpenOffice.org Base -> Databases

↳ New

▶ Browse for "MailGate.odb"

↳ OK

↳ OK

▶ 5. Continue with "6." in the below section

OpenOffice 3.1

This section describes how to use the OpenOffice files with OpenOffice 3.1.

▶ 1. Copy "MailGate.odb" from the package to your hard disk (The file must exist if you want to use "Alertype+Counter.ods" in the future).

▶ 2. Start OpenOffice

▶ 3. Lower macro security:

↳ Tools -> Options

↳ OpenOffice.org -> Security

↳ Macro Security -> Medium

↳ OK

↳ OK

▶ 4. Open MailGate.odb:

↳ File -> Open -> MailGate.odb

↳ Enable Macros

5. The database should now be available in OpenOffice.

To verify the existence of the database use:

↳ Tools -> Options

↳ OpenOffice.org Base -> Databases

There should be an entry "MailGate".

↳ Cancel

▶ 6. You can now use the document "Alerttype+Counter.ods" to view the current database contents and to create or use the existing charts:

↳ File -> Open -> Alerttype+Counter.ods

Refresh data:

- Right-click into the data you'd like to refresh (one of the cells: A3,D3,G3)
- (Enter username and password for the database if asked)
- Choose "Refresh"

If there's data available in the database, you should see some counters or even alert types in "alerttype" if a mail was quarantined since Avira AntiVir MailGate with database support was started.

The counter charts are updated automatically if any of the counters change.

The alerttype chart must be updated manually if there are new types:

- Double-click the alerttype chart
- Right-click the chart "Data ranges"
- Either change the rows manually or use the button with the green arrow to choose new alerttypes.

Do not select the cells A3 and B3. Only select the cells containing the alert type and the counter.

↳ OK

The chart should contain the new alert type.

- 7. You may want to set the macro security level to "High":
  - ↳ Tools -> Options
  - ↳ OpenOffice.org -> Security
  - ↳ Macro Security -> High
  - ↳ OK
  - ↳ OK

Options

DBSupport **DBSupport**

If you enable this option, Avira AntiVir MailGate enters statistics in a database. The database consists of two tables: alerts (logged information on each malware detection) and counter (counts the emails MailGate processes).

Syntax:

```
DBSupport "YES | NO"
```

Default:

```
DBSupport NO
```

If you want to enable the `DBSupport` change the parameter value to `YES` and make sure that the following ports are open if you are working on the loopback interface:

```
udp: 59411
tcp: 50360 (only for SMC user)
```

If you are using DBSupport together with exceptions for the SpamFilter (SpamFilterExceptions) it could happen that the entries in the database look inconsistent. If a single email has different sender or recipient addresses or its sender/recipient is not available in SpamFilterExceptions, the email will be multiplied. Because of this multiplication factor the database's table `counter` may now contain a row with fields that seem to be inconsistent:

accepted	1
clean	2

DBodbcIni

DBodbcIni

If you have enabled the `DBSupport` option, the ODBC driver manager uses the specified odbc.ini file. Default setting: the installed ODBC driver manager decides which odbc.ini file to load.

Syntax:

```
DBodbcIni "path"
```

Example:

```
DBodbcIni /path/to/odbc.ini
```

DBodbcLib

DBodbcLib

If you have enabled the `DBSupport` option Avira AntiVir MailGate loads the library specified here and uses it as the ODBC driver manager. Default setting: one of the following files is loaded in sequence from the default library path: libodbc.so.1, libodbc.so, libiodbc.so

Syntax:

```
DBodbcLib "path"
```

Example:

```
DBodbcLib /path/to/odbc-library
```

DBodbcData Source

DBodbcDataSource

If you have enabled the `DBSupport` option, the specified database is connected as the source.

Syntax:

```
DBodbcDataSource "characters"
```

Default:

```
DBodbcDataSource MailGate
```

DBUpdate Delay

DBUpdateDelay

If you have enabled the `DBSupport` option, the statistics are recorded in the database at regular intervals. You can enter the interval in seconds (s), minutes (m) or hours (h). Default: to the whole hour.

Syntax:

```
DBUpdateDelay "timespan"
```

Default:

```
DBUpdateDelay 1h
```

DBStoreAlertsForEachRecipient

DBStoreAlertsForEachRecipient

If this option is enabled, there will be one row in the `alerts` table for each recipient of an email. If it is disabled, there will be only one row per email which will mention the first recipient. Default: only write one row per email to the `alerts` table.

Syntax:

```
DBStoreAlertsForEachRecipient "YES | NO"
```

Default:

```
DBStoreAlertsForEachRecipient NO
```

DBLog CleanMails

DBLogCleanMails

This option enables information on clean, harmless emails to be stored in the database.

The information is recorded in the categories `reason`, `queueid`, `action`, `source`, `product`, `vdf`, `engine`, (`ou`) and `date`. `reason` is set to `clean` and `action` to `processed`.

Syntax:

```
DBLogCleanMails "YES | NO"
```

Default:

```
DBLogCleanMails NO
```

5.3 Configuring the spam filter (for **Avira MailGate Suite** only)

The spam filter integrated into the Avira MailGate Suite filters out spam and other unwanted emails. For each email, the spam filter opens a connection to the spam database server to check your spam status. You have to activate the connection on port 55555 via TCP.

If the spam filter is enabled, emails highlighted as “Outbreak” are blocked. All other emails are only tagged.

All other options are set up in avmailgate.conf.

Options and parameters for the spam filter

Enable SpamCheck

EnableSpamCheck

Enables or disables the spam filter.

Syntax:

```
EnableSpamCheck "YES | NO"
```

Default:

```
EnableSpamCheck NO
```

SpamAction

SpamAction

Defines an action for spam emails: BLOCK, TAG, NONE.

Syntax:

```
SpamAction "option"
```

- TAG adds a header line to the email. Example:
  X-AntiVirus-Spam-Check: clean (checked by Avira MailGate: version: 3.2.1.16; spam filter version: 3.2.0/2.3; host: host.your.site)
- BLOCK moves the email to the rejected directory.
- NONE disables all actions for spam emails.

Default:

```
SpamAction TAG
```

Dangerous Outbreak Action

DangerousOutbreakAction

Performs the specified action if emails are not detected by the virus scanner due to an outbreak. Valid options are TAG, BLOCK and NONE.

Syntax:

```
DangerousOutbreakAction "option"
```

- TAG adds a header line to the email. Example:
  X-AntiVirus-Spam-Check: clean (checked by Avira MailGate: version: 3.2.1.16; spam filter version: 3.2.0/2.3; host: host.your.site)
- BLOCK moves the email to the rejected directory.
- NONE disables all actions for dangerous outbreaks.

Default:

```
DangerousOutbreakAction BLOCK
```

Dangerous Attachment Action

DangerousAttachmentAction

Performs the specified action if an email attachment may be dangerous. Valid options are TAG, BLOCK and NONE. The attachments are identified by their suffixes:
.ade, .adp, .bas, .bat, .bhx, .ceo, .cer, .chm, .cmd, .com, .cpl, .crt, .exe, .hlp, .hta, .inf, .ins, .isp, .js, .jse, .lnk, .mde, .mim, .msc, .msi, .msp, .mst, .ole, .pcd, .pi, .pif, .reg, .scr, .sct, .shb, .shs, .vb, .vbe, .vbs, .wmd, .wmz, .wsc, .wsf, .xxe

Syntax:

```
DangerousAttachmentAction "option"
```

- TAG adds a header line to the email. Example:
  X-AntiVirus-Spam-Check: clean (checked by Avira MailGate: version: 3.2.1.16; spam filter version: 3.2.0/2.3; host: host.your.site)
- BLOCK moves the email to the rejected directory.

- NONE disables all actions for dangerous attachments.

Default:

```
DangerousAttachmentAction TAG
```

Dangerous IFrameAction

DangerousIFrameAction

Performs the specified action if a dangerous IFRAME is discovered. Valid options are TAG, BLOCK and NONE.

Syntax:

```
DangerousFrameAction "option"
```

- TAG adds a header line to the email. Example:
  X-AntiVirus-Spam-Check: clean (checked by Avira MailGate: version: 3.2.1.16; spam filter version: 3.2.0/2.3; host: host.your.site)
- BLOCK moves the email to the rejected directory.
- NONE disables all actions for dangerous iFrames.

Default:

```
DangerousIFrameAction TAG
```

Dangerous Alert Action

DangerousAlertAction

Performs the specified action if the spam filter classifies an email as dangerous. Valid options are TAG, BLOCK and NONE.

Syntax:

```
DangerousAlertAction "option"
```

- TAG adds a header line to the email. Example:
  X-AntiVirus-Spam-Check: clean (checked by Avira MailGate: version: 3.2.1.16; spam filter version: 3.2.0/2.3; host: host.your.site)
- BLOCK moves the email to the rejected directory.
- NONE disables all actions for dangerous alerts.

Default:

```
DangerousAlertAction BLOCK
```

Dangerous Unknown Action

DangerousUnknownAction

Performs the specified action if an unknown danger is discovered. Valid options are TAG, BLOCK and NONE.

Syntax:

```
DangerousUnknownAction "option"
```

- TAG adds a header line to the email. Example:
  X-AntiVirus-Spam-Check: clean (checked by Avira MailGate: version: 3.2.1.16; spam filter version: 3.2.0/2.3; host: host.your.site)
- BLOCK moves the email to the rejected directory.
- NONE disables all actions for dangerous unknown.

Default:

```
DangerousUnknownAction TAG
```

LibAsmailgate

LibAsmailgate

Specifies the path to the spam filter library.

Syntax:

```
LibAsmailgate "path"
```

Default:

```
LibAsmailgate /usr/lib/AntiVir/mailgate/
libasmailgate.so
```

Spam HeaderName

SpamHeaderName

Specifies the spam header to be added to the email header. Only the beginning of the text can be changed (`X-AntiVirus-Spam-Check`).

Syntax:

```
SpamHeaderName "characters"
```

Default:

```
SpamHeaderName X-AntiVirus-Spam-Check
```

Result:

```
X-AntiVirus-Spam-Check: spam (checked by Avira
MailGate: version: 3.2.1.16; spam filter version:
3.2.0/2.3; host: host.your.site);id=5506-x4KZ25
```

SpamFilter Exceptions

SpamFilterExceptions

Defines the list of exceptions for blacklists/whitelists and the related actions.

Syntax:

```
SpamFilterExceptions "path"
```

Default:

```
SpamFilterExceptions /etc/avira/asmailgate.except
```

The spam filter actions can be overwritten using the asmailgate.except file. In this file, you can specify the email addresses and related actions. The file can also be used as a blacklist/whitelist for the spam filter.

Each list consists of an address in the form of a regular expression, e.g.:

```
/^someone@somewhere\.tld$/i blacklist
```

This example treats emails from someone@somewhere.tld as spam, irrespective of the result of the spam check. `Blacklist` is the action for the specified address.

In Avira MailGate v 2.1.3, an accordance in this list relates to all recipients, including those not included in the list. Example (in asmailgate.except*):*

```
/^someone@somewhere\.tld$/i r block_spam
```

If Avira MailGate processes an email addressed to someone@somewhere.tld and abc@def.tld which has been classified as spam, abc@def.tld does not receive the email, as it has been blocked by the rule which applies to someone@somewhere.tld. This behavior will be changed in future versions.

Actions:

Actions have priority over spam filter settings in avmailgate.conf (with the exception of blacklists/whitelists). Multiple actions can be defined for each address:

- `blacklist` - email is treated as spam
- `whitelist` - email is treated as clean
- `block_spam` - email is blocked if it has been classified as spam
- `block_dangerous_attachment` - email is blocked if it has a dangerous attachment
- `block_dangerous_alert` - email is blocked if it contains a dangerous alert
- `block_dangerous_iframe` - email is blocked if it has a dangerous IFRAME
- `tag_spam` - email is tagged if it has been classified as spam
- `tag_dangerous_attachment` - email is tagged if it has a dangerous attachment
- `tag_dangerous_alert` - email is tagged if it contains a dangerous alert
- `tag_dangerous_iframe` - email is tagged if it contains a dangerous IFRAME

Example for /etc/avira/asmailgate.except:

```
/^spam@somewhere\.tld$/i blacklist
```

Emails from spam@somewhere.tld are treated as spam irrespective of the result of the spam check.

Actions can also be disabled. **Example**:

- in /etc/avira/avmailgate.conf:
  `SpamAction BLOCK`
- in /etc/avira/asmailgate.except:
  `/^me@here\.tld$/i r !block_spam`

Spam is not blocked for the specified recipient address.

`r` is the flag for recipient. It means that the specified address should not be compared with the sender address but with the recipient address.

In the default setting (without the flag `r`) the address is compared with the sender address.

A further **example**:

- in /etc/avira/avmailgate.conf:
  `DangerousAttachmentAction TAG`
  `DangerousIFrameAction TAG`
- in /etc/avira/asmailgate.except:
  `/^me@here\.tld$/i r !tag_dangerous_attachment !tag_dangerous_iframe`

DangerousAttachment emails and DangerousIFrame emails are not tagged.

The status "DangerousOutbreak" has a higher priority than entries in blacklists and whitelists. In the case of a "DangerousOutbreak" blacklists and whitelists are not checked.

SpamFilter DetectGTUBE

SpamFilterDetectGTUBE

The GTUBE test string can be used to test the integrated spam filter.
You can find this string and a complete RFC-822 email at:
http://spamassassin.apache.org/gtube/

An email containing this string should be classified as **spam** by spam filters. Simply copy the string into the text of the message and send it via Avira AntiVir MailGate. The spam filter is working correctly if you receive the following message:

```
...
spam filter: result=spam; action=tagged; id=15025-btMzMR
spam filter: spam mail detected (queue id: 15025-btMzMR)
...
```

GTUBE is not detected by default. To enable GTUBE detection, set this option to YES and restart Avira AntiVir MailGate.

Syntax:

```
SpamFilterDetectGTUBE "YES | NO"
```

Default:

```
SpamFilterDetectGTUBE NO
```

SpamFilter Startup Timeout

SpamFilterStartupTimeout

This option defines how long Avira AntiVir MailGate should wait until the external spam daemon boots up (in seconds).

Syntax:

```
SpamFilterStartupTimeout "non-negative number"
```

Default:

```
SpamFilterStartupTimeout 60
```

SpamFilter ServiceConnect Timeout

SpamFilterServiceConnectTimeout

This option defines how long Avira AntiVir MailGate should wait until a response to a configuration request arrives from the external spam filter daemon (in seconds).

Syntax:

```
SpamFilterServiceConnectTimeout "non-negative number"
```

Default:

```
SpamFilterServiceConnectTimeout 30
```

SpamFilter ServiceMax Sessions

SpamFilterServiceMaxSessions

This option defines the maximum number of simultaneously running connections to the external spam filter daemon.

Syntax:

```
SpamFilterServiceMaxSessions "non-negative number"
```

Default:

```
SpamFilterServiceMaxSessions 50
```

SpamFilter HandleBulk ADVLikeSpam

SpamFilterHandleBulkADVLikeSpam

You can use this option to classify junk mail as spam.

Syntax:

```
SpamFilterHandleBulkADVLikeSpam "YES | NO"
```

Default:

```
SpamFilterHandleBulkADVLikeSpam NO
```

SpamFilter HandleBulk PornLikeSpam

SpamFilterHandleBulkPornLikeSpam

You can use this option to classify emails with pornographic content as spam.

Syntax:

```
SpamFilterHandleBulkPornLikeSpam "YES | NO"
```

Default:

```
SpamFilterHandleBulkPornLikeSpam NO
```

SpamFilter ModifySubject

SpamFilterModifySubject

This option inserts the result of the spam check in the "subject" header line.
Subject: [spamcheck: spam] Original subject text

This is the default message. It can be overwritten using a template: "spamfilter-subjects". In this template, you can specify a string for each spam check result. The relevant string replaces the "subject" header line.

A sample template is available in /usr/lib/AntiVir/mailgate/templates/examples.

Syntax:

```
SpamFilterModifySubject "YES | NO"
```

Default:

```
SpamFilterModifySubject NO
```

SpamFilter CheckFailed Keep

SpamFilterCheckFailedKeep

If the spam check fails, the email is sent back to the queue to be rechecked. The email is processed as long as the error occurs. At present you cannot force the forwarding of a blocked email in the queue.

Syntax:

```
SpamFilterCheckFailedKeep "YES | NO"
```

Default:

```
SpamFilterCheckFailedKeep NO
```

5.4 Scanner configuration in avmailgate-scanner.conf

From Avira AntiVir MailGate 3.0.0 onwards, a new configuration file has been

introduced: avmailgate-scanner.conf. This file contains special configuration options for the new Scanner backend. The options in this file need to be changed only in a few exceptional cases.

User Group

User, Group

If you change one of these options, you must ensure that the files avmailgate-scanner.conf and avmailgate.conf contain identical values for these options.

You must also adapt avmailgate-scanner.conf if you have updated from an earlier MailGate version (< 3.0.0) and the current `User/Group` settings are different from the default settings.

Syntax:

```
User "characters"
Group "characters"
```

Default:

```
User uucp
Group antivir
```

Example:

```
User FooBarBaz
Group FooBar
```

If you make changes to `User/Group` you have to make certain other changes:

In /etc/avira/avmailgate-scanner.conf:

- Change the owner or group of the path specified in `ListenAddress` (Note: The option consists of a path and a socket file. Close Avira AntiVir MailGate before you make changes. If the socket file exists, delete it and change only the directory owner or group.)

If you change the user and/or group at this point, you must also change the `User` *and* `Group` *options in the MailGate configuration file* /etc/avira/avmailgate.conf.

In /etc/avira/avmailgate.conf:

- Change the option `User/Group`.
- Change the owner or group of the directory specified in `SpoolDir` and its sub-directories (Default setting: /var/spool/avmailgate).

Socket Permissions

SocketPermissions

The owner and authorizations for the socket of the Scanner backend. The Scanner backend must use the same user identification as Avira AntiVir MailGate.

```
SocketPermissions 0600
```

ListenAddress

ListenAddress

The `ListenAddress` (in avmailgate-scanner.conf) and `ScannerListenAddress` (in avmailgate.conf) options define how the Scanner backend is reached. Both options must reference the same path (the “unix:” string cannot be used in the ScannerListenAddress option):

```
ListenAddress unix:/var/run/avmailgate/scanner
ScannerListenAddress /var/run/avmailgate/scanner
```

PoolScanners

PoolScanners

A pool of scanners is used to ensure scans are performed more efficiently. The `PoolScanners` option defines the size of this pool.
Please note however that too many scanners may overload the computer, whilst too few causes higher waiting times for the applications.

Syntax:

```
PoolScanners "non-negative number"
```

Default:

```
PoolScanners 24
```

Pool Connections

PoolConnections

The maximum number of simultaneous connections Avira AntiVir MailGate allows for the scanner pool. Default setting:

Syntax:

```
PoolConnections "non-negative number"
```

Default:

```
PoolConnections 128
```

SyslogFacility

SyslogFacility

This option defines the log category syslog uses for scanner messages.

Syntax:

```
SyslogFacility "characters"
```

Default:

```
SyslogFacility mail
```

ReportLevel

ReportLevel

The scanner set up can establish various protocol levels:

- 0 - Errors
- 1 - Errors and alerts
- 2 - Errors, alerts and warnings
- 3 - Errors, alerts, warnings and debug messages

An “alert” contains information on potentially harmful code.

Syntax:

```
ReportLevel "non-negative number"
```

Default:

```
ReportLevel 0
```

ScanTemp

ScanTemp

The directory in which the scanner places temporary files, e.g. extracted archives or blocked files.

The Scanner backend does not recognize the environment variable "TMPDIR".

If all Avira AntiVir MailGate components are using a common temporary directory, change the options `TemporaryDir` *in* /etc/avira/avmailgate.conf *and* `ScanTemp` *in* avmailgate-scanner.conf.

Default:

```
ScanTemp /var/tmp
```

LogFileName

LogFileName

The path of the Scanner log file.

```
LogFileName /path/to/logfile
```

5.5 Host configuration in avmailgate.acl

avmailgate.acl uses the keywords `local` and `relay` to decide which computers can send emails via Avira AntiVir MailGate. The domain or IP address of the sender or recipient are used in this process.

▶ Define the local hosts and/or domains. Example:

```
local: localhost
local: avira.com
```

▶ Define which hosts and networks can send emails. Example:

```
relay: 127.0.0.1/8 192.168.0.0/16
```

IP addresses

IP addresses

IP addresses can be specified in various ways:

```
192.168.0.0/16 or 192.168
```

Both variations have the same meaning. /16 means 16 Bit and denotes the first two numbers of the IP address. All IP addresses beginning with 192.168 are therefore allowed.

Example for /etc/avira/avmailgate.acl:

```
# Access lists for AVIRA MailGate
# These hosts and/or domains are local.
local: localhost 127.0.0.1
local: avira.com
# These hosts and networks are allowed to relay.
relay: 127.0.0.1/8 192.168.0.0/16
```

If you enable only IPv6 support using the option InetProtocols, you have to specify IPv6 addresses for the ListenAddress and ForwardTo options, as well as in the avmailgate.acl file.

5.6 Configuration of warnings in avmailgate.warn

You have the option of using another file to define alert messages: /etc/avira/avmailgate.warn. Together with avmailgate.conf this file controls the alert messages sent to the recipient, sender and postmaster.

A command in this file is composed of two elements:

- The name of the detected virus or unwanted program appears at the beginning. Wildcards can also be used.
- The second element consists of one or more of the following letters:

- S: for sender
- R: for recipient
- P: for postmaster
- T: to send an SNMP trap

Example **Example:**

The command

```
/klez/ RP
```

instructs Avira AntiVir MailGate to send an alert email to the recipient and the postmaster if the virus called Klez is detected.

If a special virus or unwanted program is detected, the settings in avmailgate.warn *have priority over those in* avmailgate.conf.

5.7 Configuring report templates

You can define the texts used as email notifications when software viruses, unwanted programs or suspicious files are discovered.

▶ Copy the sample templates in the appropriate language from the templates directory/usr/lib/AntiVir/mailgate/templates/examples/<Language>/ into the directory /usr/lib/AntiVir/mailgate/templates.

▶ Change the directory in /usr/lib/AntiVir/mailgate/templates. This directory contains the following files:
patho-administrator
patho-recipient
patho-sender
alert-administrator
alert-recipient
alert-sender

▶ Type the required texts into the abovementioned files. Retain the structure of the file:
- The first line is the subject of the email.
- This is followed by an empty line (new line).
- The conclusion forms the text of the email.

Keywords

Keywords

The files alert-* and patho-* can contain the following keywords which are replaced by the appropriate text:

Keyword	Text
SENDER	The email address of the sender of the infected email.
ALERTS	The list of viruses and unwanted programs detected in the email. Each line contains the name of a virus. Prefix and Postfix are repeated.
REASON	The reason why an email has not been scanned (in brief).
ADVICE	Troubleshooting information (approx. 1 line, see REASON).
QUEUEID	The ID of the email in the Avira AntiVir MailGate queue.
SUBJECT	The subject of the infected email.
CONCERNING_ FILE_NAMES	This keyword is replaced by a list of files in which the alerts were detected.
PRODUCT_ VERSION	The product version number.
ENGINE_ VERSION	The version number of the scan engine.
VDF_VERSION	The VDF version number.
VDF_DATE	The VDF creation date.

Example for alert-sender

Example for alert-sender

```
SUBJECT: AntiVir ALERT [Your email: "SUBJECT"]
**********************AntiVir ALERT*******************
AntiVir has discovered the following viruses/unwanted
programs in an email with your sender address::
                      ALERTS
The email has not been sent and has been isolated
on your server. Check your system immediately for
a possible virus infection.
Clean your system before you send any more email
messages.
```

5.8 Updater configuration in avupdate-mailgate.conf

Updates ensure that the Avira AntiVir MailGate components (MailGate, Scanner, VDF and Engine) that are responsible for protecting you against viruses and unwanted programs are always up-to-date.

The Avira Updater lets you update the Avira software on your computer using Avira update servers.

To configure an update task, use the options in /etc/avira/avupdate-mailgate.conf described later in this document. All parameters in avupdate-mailgate.conf can be transferred to the Updater in the command line. Example:

- Parameter in avupdate-mailgate.conf:

```
temp-dir=/tmp
```

- Command in the command line:

```
/usr/lib/AntiVir/mailgate/avupdate-mailgate.bin
--temp-dir=/tmp
```

internet-srvs — The list of Internet update servers.

```
internet-srvs=http://dl1.pro.antivir.de, http://
dl2.pro.antivir.de, http://dl3.pro.antivir.de
```

intranet-srvs — The list of intranet update servers.

```
intranet-svrs=http://iumserver:7080
```

master-file — The master.idx file

```
master-file=/idx/master.idx
```

install-dir — The installation directory for updated product files.

```
install-dir=/usr/lib/AntiVir
```

temp-dir — Temporary directory for downloaded update files.

```
temp-dir=/tmp/avira_update
```

Creating email update reports

All reports on Avira AntiVir MailGate updates are sent to the email addresses specified in
avupdate-mailgate.conf:

mailer — The reports can be sent via `smtp` or via `sendmail`:

Default:

```
mailer=smtp
```

smtp... — Authentication of the smtp connection. Enable the `auth-method` option and specify the smtp server, the port, the user and the password.

```
auth-method=password
smtp-user=<Your_Username>
smtp-password=<Your_Password>
smtp-server=<Servername>
smtp-port=<Port>
```

notify-when — Email notifications can be assigned four values:

- 0 - No email notifications are sent.
- 1 - Email notifications are sent in the following cases: “Update successful”, “Update unsuccessful” and “Up-to-date”.
- 2 - An email notification is only sent for “Update unsuccessful”.
- 3 - An email notification is only sent for “Update successful”.

Default:

```
notify-when=3
```

email-to — The recipient of the email notifications.

Default:

```
email-to=root@localhost
```

Log file settings

log — Specify the full path and name of the file in which Avira AntiVir Updater records its log messages.

```
log=/var/log/avupdate-mailgate.log
```

log-append — The log file is overwritten by default. You can use this option to append the log messages to the end of the log file.

```
log-append
```

Setting intranet updates

If you prefer to use an intranet update instead of the default Internet one, you have to configure some parameters in avupdate-mailgate.conf (see intranet-srvs) or you

have to provide them in the command line:

`intranet-srvs`

Specifies a comma separated list of Avira IUM servers.

`product-root`

Specifies the root of the update on the IUM server (set to `/update`).

`intranet`

Specifies that the update will be made from the intranet rather than from the Internet.

Example:

```
intranet-svrs=http://iumserver:7080
product-root=/update
intranet
```

With the Avira Internet Update Manager (IUM) you can automatically download updates for a large number of your Avira products from the internet. The individual client computers in your network do not have to download updates from the Internet themselves, instead IUM will create a mirror located in your internal network. For more information, please refer to the Avira IUM user manual (http://www.avira.com/).

Setting fallback update servers

If you like to set up fallback update servers, for example in case the intranet servers do not work appropriately and you like to update from Internet servers, you can do a setup by adding the option `peak-handling-srvs` in the configuration file or in the command line. The option has the same syntax as `intranet-srvs`.

Example:

```
peak-handling-srvs=http://dl1.pro.antivir.de,
http://dl2.pro.antivir.de, dl3.pro.antivir.de
```

Integration in Avira Security Management Center (SMC)

To configure updates via the Avira Security Management Center (SMC), you must add the package with the update plugin to the SMC repository. The new product “Avira Updater” is then available for installation purposes on computers administered by SMC.

The product “Avira Updater” facilitates the configuration of updates for all products installed on SMC computers. Further information is available in the SMC documentation.

6 Operation

After completing installation and configuration and after starting Avira AntiVir MailGate, the program ensures that your system is constantly monitored. In the course of the usage process, occasional changes to the configuration may be required. The Chapter Configuration – Page 24 contains explanations relating to this.

In some cases, it is necessary to operate Avira AntiVir MailGate manually or to manually process the files filtered by Avira AntiVir MailGate.

This chapter describes the follow topics:

- Starting and stopping Avira AntiVir MailGate manually – Page 93
- Parameters for the SMTP and Scanner daemon – Page 95
- Queue manager avq – Page 96

You can also find information on

- Procedures for identifying viruses or unwanted programs – Page 107

6.1 Starting and stopping Avira AntiVir MailGate manually

If you have installed Avira AntiVir MailGate according to the description in Installation – Page 13 it is started and stopped automatically by the system.

In certain cases, however, Avira AntiVir MailGate has to be started and stopped manually. Any changes to the configuration files are not enabled until the program is restarted.

The script /usr/lib/AntiVir/mailgate/avmailgate starts and stops the Scanner and the Avira AntiVir MailGate daemon.

From Version 3.0.0 onwards, Avira AntiVir MailGate uses a new scanner which has to be started before avmailgate.bin. For this reason, MailGate must be started and stopped with the aid of the script "avmailgate":

```
/usr/lib/AntiVir/mailgate/avmailgate start
/usr/lib/AntiVir/mailgate/avmailgate stop
```

If you are using your own script, you should note that the Scanner is started first. In the script "avmailgate" you will find an example of how the Scanner backend can be started.

If you want to transfer specific command line options to Avira AntiVir MailGate, you can add them to the "DAEMONPARAMS" parameter in the script (see Parameters for avmailgate.bin).

To be able to start or stop Avira AntiVir MailGate manually, you must be logged on as the root *user or be assigned the necessary access rights.*

Starting Avira AntiVir MailGate

▶ Enter the following:

```
/usr/lib/AntiVir/mailgate/avmailgate start
```

↳ The program is started with the following message:

```
Starting AVIRA AntiVir MailGate...
Starting savapi
```

Stopping Avira AntiVir MailGate

▶ Enter the following:

```
/usr/lib/AntiVir/mailgate/avmailgate stop
```

↳ The program is stopped with the following message:

```
Stopping AVIRA AntiVir MailGate...
Stopping: avmailgate.bin
Shutting down Avira MailGate...
Stopping: savapi
```

Restarting Avira AntiVir MailGate

Avira AntiVir MailGate must be restarted if, for example, changes have been made to the configuration script.

▶ Enter the following:

```
/usr/lib/AntiVir/mailgate/avmailgate restart
```

↳ The program first displays the following message and then restarts:

```
Stopping AVIRA AntiVir MailGate...
Stopping: avmailgate.bin
Shutting down Avira MailGate...
Stopping: savapi

Starting AVIRA AntiVir MailGate...
Starting savapi
```

Checking the Avira AntiVir MailGate status

▶ Enter the following:

```
/usr/lib/AntiVir/mailgate/avmailgate status
```

↳ The program displays information on the Avira AntiVir MailGate daemon:

```
Status: avmailgate.bin running
Status: savapi running
```

6.2 Parameters for the SMTP and Scanner daemon

The following tables describe the possible command line parameters which override the settings in avmailgate.conf.

Syntax:

```
avmailgate.bin [ -V | --version ] [ -C config file ] [ -A
ACL file ] [-p milter listen address ] [ --start ] [ --stop
] [ --status ] [--avq ] [ --dump-config ] [--test-active-
directory] [ --runtime-versions ] [--rebuild-quarantine
-db] [ -D debug level ]
```

Parameters for avmailgate.bin

Parameter	Description
`-V or --version`	Displays the version number.
`-C config-file`	Uses another configuration file instead of /etc/avira/avmailgate.conf. If you specify `-C` here, you must do the same for `--stop` and `--status`.
`-A ACL-file`	Uses another ACL file instead of the default setting /etc/avira/avmailgate.acl
`-p milter listen address`	Enables milter mode and sets the milter `ListenAddress` to the given value (address and port the SMTP daemon should connect to).
`--start`	Starts Avira AntiVir MailGate.
`--stop`	Shuts Avira AntiVir MailGate down.
`--status`	Indicates whether Avira AntiVir MailGate is running.
`--avq`	Calls up the queue manager.
`--dump-config`	Displays the configuration values that are currently valid, excluding all comments in the configuration file and disabled configuration settings.

Parameter	Description
`--test-active-directory`	Verifies the configuration settings that are related to the ActiveDirectorySupport. This option tests the ActiveDirectory server connection, runs a query for a given email address and prints a list of the related organizational units. Errors will be reported on stdout and to the log files. Use this command to troubleshoot Avira AntiVir MailGate's ActiveDirectorySupport. *If the same email address is set for several users, this command may return the same organizational unit several times.*
`--runtime-versions`	Displays version information on the Scanner currently being used. Example: AVE:8.2.1.172 VDF:7.10.4.134 SAVAPI:3.0.5.22 AVE is the version number of the scan engine. VDF is the version number of the sample file. SAVAPI is the version number of the scan service.
`--rebuild-quarantine-db`	Rebuilds the quarantine database from existing quarantine files. This command line is only useful if you are using the Quarantine Manager Advanced. The parameter value for `EnableLegacyQuarantine` must be set to NO.

A further option is to add the parameters `-C`, `-A` and `-p` to the variable DAEMONPARAMS in the start-/stop script ***/usr/lib/AntiVir/mailgate/avmailgate***.

The following options are used for debugging:

Parameter	Description
`-D debug-level`	Defines the accuracy with which debug messages are logged. (Levels 0-5, 0 = no logging, 5 = detailed logging).

6.3 Queue manager avq

The queue manager avq is integrated into avmailgate.bin. It facilitates the handling of Avira AntiVir MailGate spool directories "incoming" and "outgoing" in /var/spool/avmailgate/.
The status of emails that have not yet been dealt with and have been moved to quarantine can be displayed and changed here (see Avira AntiVir MailGate-Spool directories – Page 24).

The list can be controlled with the aid of the following parameters for `--avq` (further parameters can be found in the Help, which you can access with `--avq --help`). If no command is given, the content of the "rejected" queue will be listed.

The following parameters control the list:

Parameter	Description
`--queue=incoming`	The emails in the “incoming” queue are listed.
`--queue=outgoing`	The emails in the “outgoing” queue are listed.
`--queue=rejected`	The emails in the "rejected" queue are listed.
`--list=all`	Displays all emails in the rejected, incoming and outgoing queue. The first column shows the status of the email. The second column displays the queue ID. The third column shows the size of the email in bytes. The fourth column displays the arrival time of the email and the last column shows the names of the sender and of the recipient. Please see example below.
`--nosort`	Disables the sorting. The emails in the queue are sorted by default according to date (according to the timestamp of the waiting file): the most recent email takes the last position.

Example:

```
v 2402-mhLKEG 838 TUE MAY 17 12:16:56 Sender: test@example.com
                                      Recipients: test@example.com
```

The email with the queue ID 2402-mhLKEG is 838 bytes large and is classified as `v`. The possible status classifications are:

Status	Description
`v`	found malware
`m`	found suspicious mail
`y`	mail is being processed
`q`	mail is ready for process
`f`	forced delivery
`x`	mail is in process

6.4 Quarantine management

Avira AntiVir MailGate provides two different quarantine managers: the original Quarantine Manager Classic and the more recent Quarantine Manager Advanced. Only one of these managers can be used at a time, enabling one disables the other.

***Warning**: The two quarantine managers are not compatible. In consequence, emails sent to quarantine by one quarantine manager cannot be converted to the format of the other quarantine manager.*

6.4.1 Quarantine Manager Classic

If you want to work with the classic form of quarantine manager, retain the preset parameter in the configuration file. The default setting is:

```
EnableLegacyQuarantine Yes
```

Email status in quarantine

▶ Enter the following:

```
/usr/lib/AntiVir/mailgate/avmailgate.bin --avq
```

↳ The status of all emails in quarantine is displayed.

The first line contains the name of the quarantine displayed. Example:

```
Queue: rejected.
```

At the end of the list the number of emails in quarantine is established:

```
5 mails in the rejected queue.
```

The quarantine manager displays the following status information for each email:

- `--> Not processed yet`
- `--> OK`
- `--> MIME problem` (recursion to deep, etc.)
- `--> Found e.g. (1x) Eicar Test Signature (type: virus)`

The following status information is displayed, depending on the result of the spam filter (see Configuring report templates – Page 88):

- `--> Outbreak detected`
- `--> Dangerous attachment found`
- `--> Dangerous iframe found`
- `--> Dangerous alert found`
- `--> Spam`

The list can be controlled with the aid of the following parameters for `--avq` (further parameters can be found in the Help, which you can access with `--avq --help`).

The following parameters control the list:

Parameter	Description
`--list=all`	All queues are listed.
`--nosort`	Disables the sorting. The emails in the queue are by default sorted according to date (according to the timestamp of the waiting file): the most recent email takes the last position.
`--flush`	Flushes incoming and outgoing queue.

Deleting emails from the queue

Emails in the rejected *queue have to be deleted manually.*

To delete rejected emails immediately, you can use the option `AlertAction` *in* avmailgate.conf.

In order to delete rejected emails manually, proceed as follows (see also *Quarantine Manager Advanced – Page 100)**:*

▶ Ascertain the queue ID of the email. Avira AntiVir MailGate includes this queue-ID in its logs and in the email which is sent to the postmaster.

Example:

```
Avira MailGate has detected the following in a mail sent
through your server:
 (1x) Eicar-Test-Signature (type: virus)
The mail was not delivered.
It has been quarantined with the following queue id:
 13881-wS6dUU
```

▶ Enter the following command (<ID> is the ID of the infected email):

```
/usr/lib/AntiVir/mailgate/avmailgate.bin --avq
--remove=<ID>
```

↳ The email is deleted from the queue.

You can control the delete process using the following parameters:

Parameter	Description
`--remove=<ID>`	Deletes the email with the specified ID.

`--remove=all`	Deletes all emails. The user is prompted to confirm the action:
	`# ./avmailgate.bin --avq --remove=all`
	`All mails in the directory "/var/spool/avmailgate/rejected/" will be deleted.`
	`Are you sure? [y/N] y`
	`Removing vf-14375-AZ2SEl`
	`Removing df-14375-AZ2SEl`

Forcing email forwarding

***Warning**: This process may result in potentially harmful viruses being forwarded*

▶ Always take care over which type of email should be forwarded.

▶ Ascertain the ID of the infected email. Avira AntiVir MailGate includes this ID in its logs and in the email which is sent to the postmaster.

The mail was not delivered.

```
The mail was not delivered.
It has been quarantined with the following queue id:
13881-wS6dUU
```

▶ Enter the following command (<ID> is the ID of the infected email):

```
/usr/lib/AntiVir/mailgate/avmailgate.bin --avq --
deliver=<ID>
```

↳ The email is delivered and deleted from quarantine irrespective of the result of the virus scan.

6.4.2 Quarantine Manager Advanced

Quarantine Manager Advanced is disabled by default. To enable this manager, you have to edit the configuration file

```
/etc/avira/avmailgate.conf
```

Set the option

```
EnableLegacyQuarantine
```

to `NO` and save the change. Start Avira AntiVir MailGate.

The Quarantine Manager Advanced is not available in milter mode.

The syntax for calling the Quarantine Management Tool is as follows:

```
# avqmc-mgt [ARGUMENTS] [COMMANDS] [COMMANDS ARGUMENTS]
```

6.4.3 Functions of the quarantine tool avqmc-mgt

The following arguments are available:

```
avqmc-mgt[ -f ] [ -m ] [ -h, --help ] [--print-alert-types]
[-u <username> ] [ --version ] [ --force-root ]
```

Argument	Description
`-f`	Will execute a command, e.g. `deliver`, immediately. You will not be asked to reconfirm the command.
`-m`	Displays information on the email placed in quarantine, separated by commas and in machine-readable form.
`-h, --help`	Provides a short description of the management daemon and the available commands and parameters.
`--print-alert-types`	Prints a list of known alert types. You can search for a specific alert type by using the command `avqmc-mgt search alert_type=`
`-u <username>`	Enables a user to make a direct choice, instead of having the choice determined by avqmd- Socket Permissions.
`avqmd --version`	Displays the version number of the `avqmd` binary.
`avqmc-mgt --version`	Displays the version number of the `avqmc-mgt` binary.
`--force-root`	By default `avqmc-mgt` switches to whomever owns the socket of the quarantine management daemon. `--force-root` prevents a switch of users, therefore `avqmc-mgt` runs as `root`.
	*Please use this option with caution! It is intended solely for debugging purposes.*

The following commands and command arguments are available:

```
avqmc-mgt[ list ] [ view <ID> ] [ count ] [delete all ] [
delete <ID>] [ delete <date> ][ reprocess <ID> ] [ deliver
<ID> ] [ search ]
```

Command/argument	Description
`list`	Displays a list of quarantined emails.
`view <ID>`	Displays the email with the specified ID.
`count`	Displays the number of quarantined emails.
`delete all`	Deletes all emails from quarantine.
`delete <ID>`	Deletes the email with the specified ID.
`delete <date>`	Deletes emails quarantined at a certain date and time or during a specified period.
`reprocess <ID>`	Sends an email to be reprocessed with Avira AntiVir MailGate.
`deliver <ID>`	Forces the delivery of an email with the specified ID.
`search`	Enables you to search the quarantine database.

Displaying the quarantine database

You can use the command

```
avqmc-mgt
```

to display information on all emails placed in quarantine, e.g.

```
...
ID: 62
 Queue-ID: 16113-Gw2lMB
 Quarantine date: Thu Sep 23 18:25:20 CEST 2010
 (2010-09-23)
 Envelope sender: Sender@example.com
 Envelope recipient: Recipient@example.com
 Subject: Subject
 Message-ID: 2010-09-23.5338@Sender
 Date: Thu, 23 Sep 2010 18:25:20 +0200
 To: Sender@example.com
 From: Recipient@example.com
 Alert: W32/Avira-signature (virus) (2)
 AVE version: 8.2.4.2
 VDF version: 7.10.4.182
ID: 63
...
```

Every email contains two IDs, a database ID (e.g. `62`) and a queue ID (e.g. `16113-Gw2lMB`). The database ID is assigned chronologically according

to the time log of the email in quarantine. The queue ID is static and linked to a specific email.

```
ID: 62
Queue ID: 16113-Gw2lMB
```

In addition, the date and time at which an email was moved to quarantine is displayed, as well as the basic data of the email (sender, recipient, subject, send date and message ID) and the scan result.

The reason why the email was placed in quarantine is specified (`Alert`). Viruses, worms, malware and other factors which have caused the email to be sent to quarantine are sorted by name and listed with details of their type and the number of alerts of the type that were detected in the email.

```
Alert: W32/Avira-signature (virus) (2)
```

If you are using the enhanced quarantine management utility, the output contains the following file:

```
Alert: Eicar-Test_Signature (virus) (3)
Alert: HIDDENTEXT/Worm.Gen (heuristic) (1)
```

In this location, you will also find the version number of the AVE and VDF (for definition of terms refer to 9.3 Glossary) with which the email scan was performed.

```
AVE version: 8.2.4.2
VDF version: 7.10.4.182
```

Displaying an email placed in quarantine

You can use the assigned ID to display emails placed in quarantine.
To do this, use the command:

```
avqmc-mgt view <ID>
```

For example, the command

```
avqmc-mgt view 62
```

shows you the email with the database ID 62. You can use the command

```
avqmc-mgt view 16113-Gw2lMB
```

to view the email with the queue ID `16113-Gw2lMB`.
The email is displayed in its entirety. The functionality of the view command does not equate to that of a Mail-Client. Quarantine Manager Advanced uses the program set by the variables `$PAGER` to display the emails.

If no program has been specified, `/usr/bin/less` is called by default. If this cannot be found, the Manager tries to call `/usr/bin/more`. If this also fails, an error occurs.

Displaying the number of emails placed in quarantine

Enter the command

```
avqmc-mgt count
```

to display the number of emails placed in quarantine.

Deleting emails placed in quarantine

There are various options for deleting emails placed in quarantine.

To delete all emails from quarantine, use the command

```
avqmc-mgt delete all
```

If you want to delete a specific email, you can enter the following command:

```
avqmc-mgt delete <ID>
```

Use the appropriate database or queue ID.

You can also delete an email based on the quarantine date.

The quarantine date of each email is contained in the information provided for all emails placed in quarantine, which you can access using the command `avqmc-mgt`:

```
Quarantine date: Thu Sep 23 18:25:20 CEST 2010 (2010-09-23)
```

Use the command:

```
avqmc-mgt delete date:<YYYY-MM-DD>
```

If you therefore want to delete all emails placed in quarantine on 23 September 2010, enter the following:

```
avqmc-mgt delete date:2010-09-23
```

You can also add an exact time of day and delete all emails placed in quarantine at this time.

```
avqmc-mgt delete date:<YYYY-MM-DD>T<HH:MM:SS>
```

Example: You can use

```
avqmc-mgt delete date:2010-09-23T09:30:00
```

to delete all emails placed in quarantine on 23.09.2010 at 09:30 hrs.

Alternatively, you can also delete all emails placed in quarantine during a specified period. To do this, extend the command as follows:

```
avqmc-mgt delete date:<YYYY-MM-DD>/<YYYY-MM-DD>
```

If you therefore enter:

```
avqmc-mgt delete date:2010-10-21/2010-10-24
```

you delete all emails placed in quarantine between 21.10.2010 at 23:59 hrs and 24.10.2010 at 00:00 hrs. The delete period in this case would therefore comprise 4 whole days.

This command can also be extended by specifying an exact time in the form of hours, minutes and seconds:

```
avqmc-mgt delete date:<YYYY-MM-DD[T<HH:MM:SS>]>[/
<YYYY-MM-DD [T<HH:MM:SS>]>]
```

Example:

```
avqmc-mgt delete date:2010-10-21T08:30:00/2010-10-
24T22:30:00
```

In this way, all emails placed in quarantine between 21.10.2010 at 08:30 hrs and 24.10.2010 at 22:30 hrs are deleted.

If there are no problems executing the command, you will receive a confirmation to that effect in the command line.

Rescanning emails placed in quarantine

The command

```
avqmc-mgt reprocess <ID>
```

e.g.

```
avqmc-mgt reprocess 62 or reprocess 16113-Gw2lMB
```

sends an email to be reprocessed with Avira AntiVir MailGate. This option can be used, for example, if you suspect that a false positive has been reported and the email has been moved to quarantine in error.

With this command the email is resent by Avira AntiVir MailGate and deleted from quarantine. If the email is again placed in quarantine after the scan process it is given a new database ID but retains the same queue ID.

Forcing delivery of a quarantined email

***Warning**: This process may result in the forwarding of dangerous malware.*

If an email is moved to quarantine due to a false positive or on the basis of specific settings (e.g. archive depth or attachment size), you can force delivery of this email.

To do this, use the command

```
avqmc-mgt deliver
```

in combination with the appropriate database or queue ID, e.g.:

`avqmc-mgt deliver 62` or `avqmc-mgt deliver 16113-Gw2lMB`

You will be asked to confirm the forced delivery:

> You are trying to send emails that might contain malware! Do you wish to continue anyhow? `[y/N]`

Using the argument `-f` in the command

```
avqmc-mgt -f deliver 62
```

will send the emails without confirmation message.

Searching quarantine

You can search the quarantine database using the following commands:

```
avqmc-mgt search <search-key>=<search-value>
```

Either `alert-type` or `alert-name` can be specified as the `search-key`
The `search-value` defines this type or the name more exactly.

Example for a search based on a specific alert type:

```
avqmc-mgt search alert-type=virus
```

Example for a search based on a specific alert name:

```
avqmc-mgt search alert-name=Eicar
```

In addition **?** can be used as a wildcard for a symbol, e.g.:

```
avqmc-mgt search alert-name=Eica?
```

The symbol ***** can be used as a wildcard for any character sequence, for example for the following search:

```
avqmc-mgt search alert-name=*Signatur
```

The list of `alert-types`, *against which a search can be performed is dynamic and may change at any time.*

Rebuild the quarantine database

With the following command line option you can rebuild the quarantine database from existing quarantine files:

```
--rebuild-quarantine-db
```

This could be useful if you deleted the database file and you want to restore it. Please take note of the following:

1. The rebuild has to be done manually:

```
# /usr/lib/AntiVir/mailgate/avmailgate.bin --rebuild
-quarantine-db
```

2.Avira AntiVir MailGate must not run during the rebuild process.

3. Before rebuilding the database file will be deleted. You will be asked to confirm the deletion before rebuilding process starts.

Example:

```
The database file avqm.db will be deleted before it gets rebuilt.
Do you wish to continue? [y/N) y
Processing sub directory virus ...
Successfully added existing files to the database.
Database has been rebuilt.
```

Errors will be reported as follows:

```
Processing sub directory virus ...
Failed to process quarantine file 55f5a870.qua
No quarantine files found to be added to the database.
Please check your daemon log files syslog  for details.
```

6.5 Procedures for identifying viruses or unwanted programs

If you have configured Avira AntiVir MailGate correctly, all important anti-virus tasks are performed automatically in your system:

- Infected emails are not forwarded.
- Infected emails are moved to /var/spool/avmailgate/rejected (or to another directory specified in avmailgate.conf), which contains the data file (df-) and the control file (vf- or mf-). For further information, refer to Avira AntiVir MailGate-Spool directories – Page 24.
- Data files may contain emails in which viruses or unwanted programs have been detected. These files can be deleted directly, together with the control file or processed using the queue manager (--avq).
- Depending on the settings in avmailgate.conf, the postmaster can send alerts to the senders and/or recipients of infected emails.
- Depending on the settings in avmailgate.conf, infected emails can be further processed by external programs or scripts.

These processes reduce the danger of an infection spreading.

The following steps should always be carried out:

▶ Try to discover how the virus or unwanted program has invaded your system.

▶ Perform a systematic scan of any data media involved.

▶ Notify your team, your supervisor and your business partners.

▶ Notify your systems administrator and your security provider.

Sending infected files to Avira GmbH

▶ Send us any viruses, unwanted programs and suspicious files which have not yet been detected or discovered by our products. The virus or unwanted program should be compressed (PGP, gzip, WinZIP, PKZip, Arj) and sent as an email attachment to virus@antivir.com.

When compressing, use the password virus. *This will ensure that the file is not deleted by email gateway virus scanners.*

7 Updates

The Avira Updater lets you update the Avira software on your computer using Avira update servers. The program can be configured either by editing the configuration file (see 5.8 Updater configuration in avupdate-mailgate.conf) or via parameters in the command line.

We recommend that you execute the Updater as **root**. If the Updater is not executed as **root** it will not have the required authorizations for rebooting the Avira AntiVir MailGate daemon and the reboot will have to be performed as **root** manually.

The advantage of this is that all running processes of Avira AntiVir MailGate daemons (e.g. Scanner and MailGate) are automatically updated with the latest anti-virus files without interrupting the running scan processes.
This ensures that all files are scanned.

7.1 Internet updates

Manual

If you want to update Avira AntiVir MailGate or any of its components:

▶ Use the following command:

```
/usr/lib/AntiVir/mailgate/avupdate-mailgate
--product=[Product]
```

You can enter the following as the `[Product]`:

- `Scanner` - (recommended) the scanner components like engine and vdf files are updated.
- `MailGate` - full update (MailGate, Scanner, Engine and VDF files).

If you only want to search for a new Avira AntiVir MailGate version without updating Avira AntiVir MailGate:

▶ Use the following command:

```
/usr/lib/AntiVir/mailgate/avupdate-mailgate
--check --product=[Product]
```

The values for `[Product]` are the same as in the example above.

Automatic updates with the cron daemon

Regular updates are performed with the cron daemon.

The relevant settings for the cron daemon **are already available if** you answered `Yes` to the question of whether Avira AntiVir Updater should be installed and automatically started during installation of Avira AntiVir MailGate with the install script.

Further information on the cron daemon can be found in your

UNIX documentation.

To manually define or change the settings for automatic updates in the cron configuration:

▶ Add the required entry to the file /etc/cron.d/avira_updater or edit it (see the following example).

Example: To perform the update hourly (always at *:23), enter the following command:

```
23 * * * * root /usr/lib/AntiVir/mailgate/avupdate-mailgate
--product=[Product]
```

You can enter the following as the `[Product]`:

- `Scanner` - (recommended) der Scanner is updated.
- `MailGate` - full update (MailGate, Scanner, Engine and VDF files).

▶ Start the update process to check the settings:

```
/usr/lib/AntiVir/mailgate/avupdate-mailgate
--product=[Product]
```

The values for `[Product]` are the same as in the example above.

↳ If the update has been successful, a report is created in the log file /var/log/avupdate-mailgate.log.

8 Service

8.1 FAQs

8.1.1 How to watch for SNMP traps on Debian 5

1.) Install the snmpd package:

```
$ apt-get install snmpd
```

2.) Copy the MIB files from the Avira AntiVir MailGate package to /usr/share/snmp/mibs:

```
$ cp antivir-mailgate-prof-<Version>/etc/AVIRA-*-MIB.txt
/usr/share/snmp/mibs
```

3.) Configure snmpd in such way that the Avira AntiVir MailGate MIB files are read:

```
$ echo "+mibs AVIRA-MIB" >> /etc/snmp/snmp.conf
$ echo "+mibs AVIRA-MAILGATE-V0-MIB" >> /etc/snmp/
snmp.conf
```

4.) Configure snmpd by editing /etc/snmp/snmptrapd.conf.

First we need to tell it to accept Avira AntiVir MailGate's SNMP traps:

```
$ echo "authCommunity log,execute,net SNMP_COMMUNITY"
>>
/etc/snmp/snmptrapd.conf
```

Replace SNMP_COMMUNITY by the value of the SNMPCommunity config option

(defaults to `Avira`).

Next we can ask snmptrapd to execute a custom program everytime a given SNMP trap is received.

For example, we might use the following line

```
traphandle AVIRA-MAILGATE-V0-MIB::mgtAlert /usr/local/
bin/mailgate_alert
```

to make snmptrapd run `/usr/local/bin/mailgate_alert` everytime the mgtAlert trap is received.

For example, `/usr/local/bin/mailgate_alert` might look like this:

```
#!/bin/bash

read host
read ip
vars=

name=
klass=
qid=

while read oid val
do
  if [ "$oid" = "AVIRA-MAILGATE-V0-MIB::mgtMalwareName.0" ]
  then
    name=$val
  fi

  if [ "$oid" = "AVIRA-MAILGATE-V0-MIB::mgtMalwareClass.0" ]
  then
    klass=$val
  fi

  if [ "$oid" = "AVIRA-MAILGATE-V0-MIB::mgtQueueItemID.0" ]
  then
    qid=$val
  fi
done

echo "MailGate found $name (classification: $klass) in $qid"
```

5.) Run `snmptrapd -f` and wait for Avira AntiVir MailGate to send the mgtAlert trap. (You could try to send the Eicar test virus through Avira AntiVir MailGate to trigger this). You should then see the following output in the terminal where you started `snmptrapd`:

```
MailGate found "Eicar-Test-Signature" (classification:
"virus") in "XXX"
```

(where XXX is replaced by the queue ID of the mail)

8.2 Support

Support service

Support service

All necessary information on our comprehensive support service can be obtained from our website http://www.avira.com.

Forum FAQs

Forum and FAQs

Before you contact the hotline, we recommend that you visit our user forum

at http://forum.avira.com/.
Please also read the FAQs section on our website.
Your question may already have been asked and answered by other users in this section.

Email support

Email support

You can obtain support by email from support@avira.com

8.3 Contact

Address
Avira GmbH
Kaplaneiweg 1
D-88069 Tettnang
Germany

Internet
You can find further information about us and our products at http://www.avira.com.

9 Appendix

9.1 Sent SNMP traps

mgtUp:

Avira AntiVir MailGate has been started.

mgtDown:

Avira AntiVir MailGate has been stopped.

mgtSmtpServerDown:

The SMTP server (avgated) has unexpectedly closed, i.e. it has been shut down by a signal or closed with the exit code other than 0.

mgtSmtpSessionDown:

An SMTP session has unexpectedly closed, i.e. it has been shut down by a signal or closed with the exit code other than 0. Transmitted parameters: The exit code and the received signal. One of these parameters is set to 0.

mgtForwarderDown:

The forwarding server (avgatefwd) has unexpectedly closed, i.e. it has been shut down by a signal or closed with the exit code other than 0.

mgtForwarderSessionDown:

The forwarding process has unexpectedly closed, i.e. it has been shut down by a signal or closed with the exit code other than 0. Transmitted parameters: The exit code and the received signal. One of these parameters is set to 0.

mgtCannotForwardMail:

The forwarding process was unable to send emails.

mgtAlert:

The Scanner has detected malware. Transmitted parameters: Malware name, assignment and ID of the queue element in which the malware was detected.

These SNMP notifications must be expressly enabled by the user by adapting /etc/avira/avmailgate.warn.

mgtSuspicious:

The Scanner was unable to complete the scan process and the email has therefore been classed as suspicious. Transmitted parameters: The reason the Scanner has classified the email as suspicious and the ID of the relevant queue element.

mgtMalwareScannerUnreach:

No connection to the malware Scanner could be established.

mgtQuarantineDaemonDown:

The Quarantine Daemon has unexpectedly closed, i.e. it has been shut down by a signal or closed with an exit code other than 0.

mgtScannerSpamCheckerUnreach:

No connection to the spam filter (e.g. Expurgate) could be established.

mgtLicenseWillExpireSoon:

The license expires in less than N days (the number N is defined with the NotifyEnd OfLicense – Page 62 option). Transmitted parameters:
Number of days the license is still valid for.

mgtLicenseExceeded:

Avira AntiVir MailGate is being used to process the mail of a larger number of users than the license provides for(Purchasing a license – Page 14).

mgtQueueReachedHighFillLevel:

The incoming or outgoing queue reaches its high fill level. An integer identifies the queue for which the trap is sent. The trap will be sent only if the feature QueueFillLevel is enabled(see Enhanced QueueHandling – Page 57).

mgtQueueReachedLowFillLevel:

After reaching the high fill level, the incoming or outgoing queue reaches the low fill level again. An integer identifies the queue for which the trap is sent. The trap will be sent only if the feature QueueFillLevel is enabled(see Enhanced QueueHandling – Page 57).

9.2 Sent Notification Emails (via NotificationMechanism)

Notification Emails

The SMTP Server (avgated) has terminated unexpectedly , i.e. it was brought down by a signal or it exited with an exit code other than 0.

A child process of the SMTP server process (avgated) has terminated unexpectedly, i.e. it was brought down by a signal or it exited with an exit code other than 0.

A forwarder daemon process (avgatefwd) has terminated unexpectedly , i.e. it was brought down by a signal or it exited with an exit code other than 0.

A forwarder session process has terminated unexpectedly , i.e. it was brought down by a signal or it exited with an exit code other than 0.

Avira AntiVir MailGate cannot connect to the malware scanner (SAVAPI) .

The quarantine daemon has terminated unexpectedly , i.e. it was brought down by a signal or it exited with an exit code other than 0.

Avira AntiVir MailGate cannot connect to the spam filter (eXpurgate) .

The incoming or outgoing queue reaches its high fill level (only sent if the feature QueueFillLevel is enabled).

The incoming or outgoing queue reaches its low fill level (only sent if the feature QueueFillLevel is enabled).

An encrypted email has been found (only sent if the configuration option EncryptedEmailOption is set to `NOTIFY_POSTMASTER`.)

9.3 Glossary

Term	Meaning
AVE (Anti Virus Engine)	AVE refers to the engine the virus scanner uses to scan the emails for potentially dangerous programs.
cron (daemon)	A daemon which starts other programs at a specified time.
Daemon	A systems administration process in UNIX that runs in the background. On average several dozen daemons are executed on one computer. These processes are normally started and shut down together with the computer.
Eicar	The European Institute for Computer Antivirus Research provides a test virus for testing anti-virus programs. For further information, refer to http://www.eicar.org
IUM	Avira Internet Update Manager
Log file	Also: Report file. A file with reports generated by the program during runtime when specific events occur.
Malware	An umbrella term for “foreign bodies” of all kinds. These can be incidents, such as viruses, or other software which the user considers unwanted (see also “Unwanted programs”).
MIME	Multipurpose Internet Mail Extensions: Internet extensions, the purpose of which is to integrate binary files in emails. MIME supports so-called multipart emails. This enables different file types in one email, binary attachments and HTML emails.
MTA	Mail Transport Agent: a program that sends emails by SMTP. Examples: Sendmail, Postfix, Exim.
Quarantine directory	The directory in which infected files are deposited to prevent user access (e.g. rejected).
root	A user with unrestricted access rights (e.g. the system administrator in Windows).
SAVAPI	Secure AntiVirus Application Programming Interface
Scan engine	The Avira AntiVir MailGate software module which controls the scan for viruses and unwanted programs.
Script	A text file with commands which are executed by UNIX (similar to a batch file in DOS).

SMC	Avira Security Management Center.
SMTP	Simple Mail Transfer Protocol: A protocol for email communications on the Internet.
syslog daemon	A daemon which is used by programs to log different information. The reports are written in different log files.
Unwanted programs	An umbrella term for programs which are installed without the agreement of the user or administrator and are therefore unwanted, although they do not cause any direct damage to the computer. These include backdoors (BDCs), dialers, jokes and games.
VDF (Virus Definition File)	A file with specific rules, for identifying malware. In many cases an update will suffice to download the latest version of this file.

9.4 Further information

For further information on viruses, worms, macroviruses and other unwanted programs, go to http://www.avira.com.

9.5 Golden rules for virus protection

- Create boot disks for your network servers and workstations.
- Always remove the disks from the drive when you finish work. Even disks without executable programs may contain program code in the boot sector and therefore carry a boot sector virus.
- Make regular backups of your data.
- Limit the exchange of programs. This applies especially to other networks, mailboxes, the Internet and friends.
- Scan new programs before installation and then perform a disk scan. If the program is zipped, a virus will not usually become evident until it is unzipped and installed.

If other people have access to your computer, you should adhere to the following rules to protect yourself from viruses.

- Make a test computer available on which you can scan software downloads, demo versions and suspect data media (disks, CD-Rs, CD-RWs, removable drives).
- Remove the test computer from the network!

- Appoint a Data Protection Officer who is responsible for handling virus infections, and set out the steps to be taken to remove a virus.
- Draw up an emergency plan. Such a plan can help prevent damage due to willful destruction, theft, outages or losses/changes due to incompatibilities. Programs and memory devices can be replaced, but data that a company relies on for its economic survival cannot.
- Draw up a protection and recovery plan for your data.
- Ensure your network is properly configured and use common sense when assigning access rights.

  These measures will help optimize your virus protection.

Issued Q2-2011

AVIRA

live free.™

Avira GmbH
Kaplaneiweg 1
88069 Tettnang
Germany

Telephone: +49 7542-500 0
Facsimile +49 7542-500 3000
www.avira.com