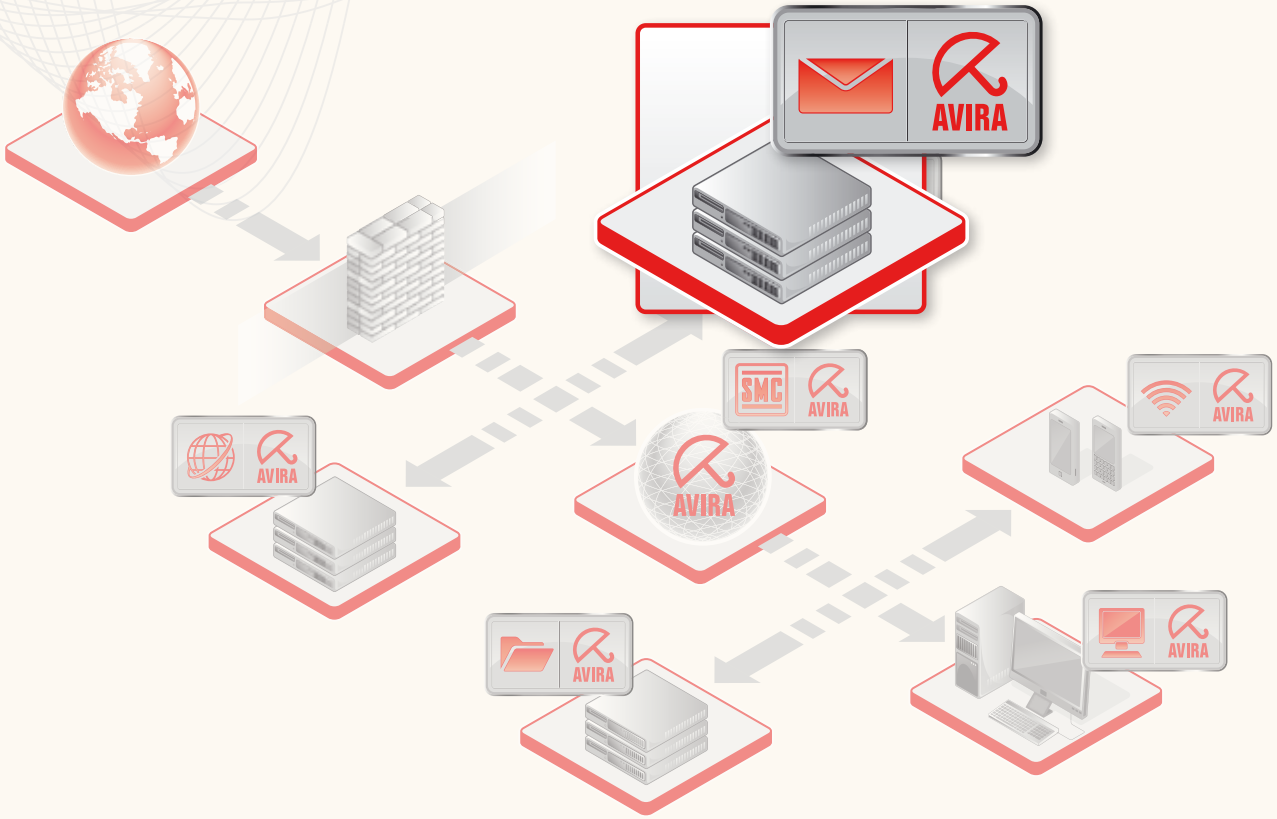
AVIRA
More Than Security

User Manual

Avira AntiVir MailGate | MailGate Suite



www.avira.com

Contents

Chapter 1. About this Manual 3

1.1 Introduction 3
1.2 The Structure of the Manual 4
1.3 Signs and Symbols 4
1.4 Abbreviations 5

Chapter 2. Product Information 6

2.1 Features 7
2.2 Modules and Operating Mode of Avira AntiVir MailGate 8
2.3 Licensing Concept 9
2.4 System Requirements 10

Chapter 3. Milter Mode 11

3.1 Overview 11
3.2 AntiVir MailGate (Milter Mode) Features 12
3.3 AntiVir MailGate (Milter Mode) Integration in Sendmail 12

Chapter 4. Installation 14

4.1 Preparing the Installation Files 15
4.2 Licensing 15
4.3 Installation with the Installation Script "install" 16
4.4 Reinstalling and Uninstalling AntiVir 19
4.5 Further Installation Steps, Depending on the MTA 20
4.6 Testing AntiVir MailGate after Installation 25

Chapter 5. Configuration 26

5.1 MailGate Spool Directories 27
5.2 MailGate Configuration in avmailgate.conf 28
5.3 Spam Filter Configuration (Avira MailGate Suite only) 41
5.4 Scanner Configuration in avmailgate-scanner.conf 46
5.5 Hosts Configuration in avmailgate.acl 47
5.6 Warnings Configuration in avmailgate.warn 48
5.7 Report Templates Configuration 48
5.8 Updater Configuration in avupdate.conf 51

Chapter 6. Operation 53

6.1 Starting and Stopping AntiVir MailGate Manually 53
6.2 Parameters for SMTP and Scanner Daemon 55
6.3 Queue Manager avq 56
6.4 Procedures when Detecting Viruses/Unwanted Programs 59

Chapter 7. Updates 60

7.1 Internet Updates 60

Chapter 8. Service 62

8.1 Support 62
8.2 Online Shop 62
8.3 Contact 63

Chapter 9. Appendix 64

9.1 Glossary 64
9.2 Further Information 65
9.3 Golden Rules for Protection Against Viruses 66

1 About this Manual

In this Chapter you can find an overview of the structure and contents of this manual.

After a short introduction, you can read information about the following issues:

- The Structure of the Manual – Page 4
- Signs and Symbols – Page 4
- Abbreviations – Page 5

1.1 Introduction

We have included in this manual all the information you need on Avira AntiVir MailGate and it will guide you step by step through installation, configuration and operation of the software.

The appendix contains a Glossary, which explains the basic terms.

For further information and assistance, please refer to our website, to the Hotline of our Technical Support and to our regular Newsletter (see Service – Page 62).

Your Avira Team

1.2 The Structure of the Manual

The manual of your AntiVir software consists of a number of Chapters, providing the following information:

Chapter	Contents
1 About this Manual	The structure of the manual, signs and symbols.
2 Product Information	General information on Avira AntiVir MailGate, its modules, features, system requirements and licensing.
3 Milter Mode	Presenting the Milter function mode in Avira AntiVir MailGate.
4 Installation	Instructions to install Avira AntiVir MailGate on your system, using a script or the graphical installation routine.
5 Configuration	Directions for optimum settings of Avira AntiVir MailGate components on your system.
6 Operation	Commands and parameters for running the Scanner and the queue manager; reactions when viruses and unwanted programs are detected.
7 Updates	Running Internet and intranet updates.
8 Service	Avira GmbH Support and Service.
9 Appendix	Glossary of technical terms and abbreviations, Golden Rules for protection against viruses.

1.3 Signs and Symbols

The manual uses the following signs and symbols:

Symbol	Meaning
✓	Used before a condition that must be met prior to performing an action.
▶	Used before a step you have to perform.
↳	Used before the result that directly follows the preceding action.
	Used before an alert if there is a danger of critical data loss or hardware damage.
	Used before a note containing particularly important information, e.g. on the steps to be followed
	Used before a tip that makes it easier to understand and use Avira AntiVir MailGate.

For improved legibility and clear marking, the following types of emphasis are also used in the text:

Emphasis in text	Explanation
Ctrl+Alt	Key or key combination
/usr/lib/AntiVir/avmailgate	Path and file name
`ls /usr/lib/AntiVir`	User entries
Choose component **Select all**	Elements of the software interface such as menu items, window titles and buttons in dialog windows
http://www.avira.com	URLs
Signs and Symbols – Page 4	Cross-reference within the document

1.4 Abbreviations

The manual uses the following abbreviations:

Abbreviation	Meaning
ACL	Access Control List
FAQ	Frequently Asked Question
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

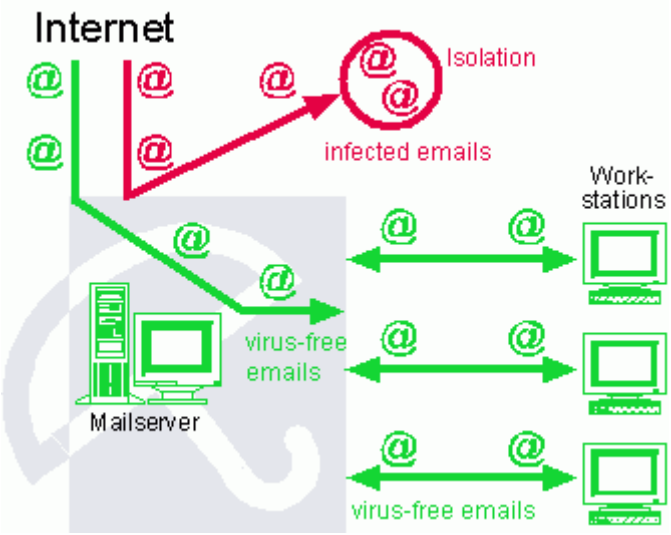
2 Product Information

Email file transfer is a natural part of modern communication and we can no longer imagine everyday life without it. However, emails frequently also transport viruses or unwanted programs.

Many of these viruses/unwanted programs were conceived especially to attack Windows operating systems. But it must be considered that there is also a danger for Open Source systems, because UNIX mail servers also transport malware. This offers an easy opportunity for cyber-attackers to penetrate your network. Windows clients can be infected, and thus computers of their messaging partners can also be affected.

Business users increasingly rely on UNIX. However, with free software entering companies and institutes, the alternative operating systems are increasingly targeted by virus programmers. Therefore, virus protection on UNIX will still be needed in the future. This is why we have developed Avira AntiVir MailGate.

Avira AntiVir MailGate scans all incoming and outgoing emails (including attachments) on your UNIX mail server. The software can operate on a variety of Mail Transport Agents (MTAs), such as Sendmail, Postfix, Exim, Qmail and other programs. It effectively supports common distributions - Red Hat, SuSE, Debian etc (see 2.4 System Requirements).



To start with, two very important tips:

Losing valuable files usually has dramatic consequences. Not even the best antivirus software can fully protect you against data loss.

▶ *Ensure that you make regular back-ups of your files.*

An anti-virus program can only be reliable and effective if kept up to date.

▶ *Ensure that you keep your Avira AntiVir MailGate up to date using automatic updates. You will learn how to do this in this user guide.*

2.1 Features

Avira AntiVir MailGate supports a variety of configuration settings to ensure that you have control of the email traffic on your system.

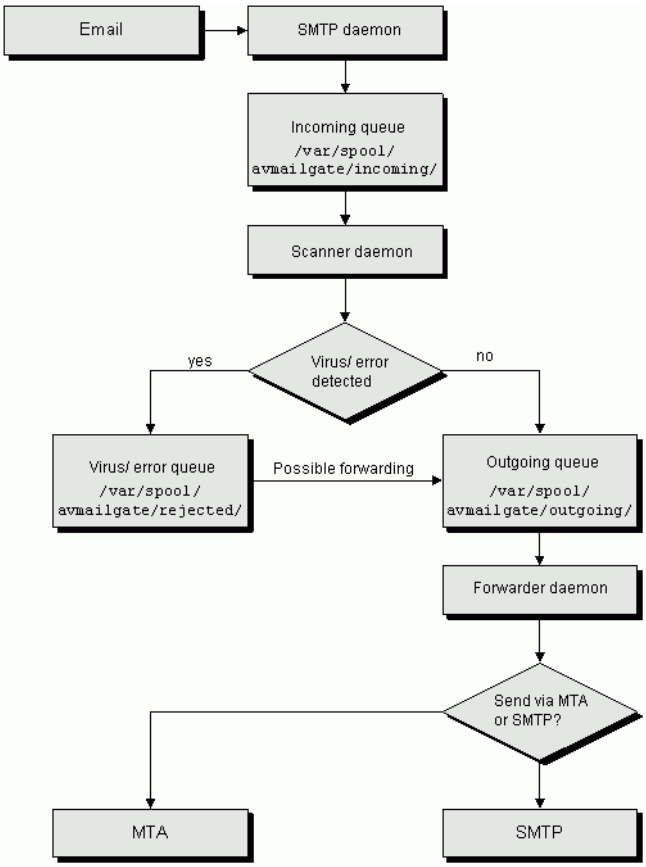
The essential features of Avira AntiVir MailGate are:

- real-time scanning of incoming and outgoing emails;
- scanning for viruses and unwanted programs;
- configurable spam filter (available in **Avira MailGate Suite**);
- scanning of mailboxes;
- isolation of suspicious and infected files;
- configurable notification functions for the administrator and for the email sender and recipient;
- login to the email server logs;
- automatic Internet update for product, scanner, engine and VDFs;
- heuristic detection for macro viruses;
- recognition of all common archive types (with configurable recursion level for nested archives);
- optional: GUI support for integration with Avira Security Management Center.

2.2 Modules and Operating Mode 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 for viruses/unwanted programs (see figure below). The program has a high scanning speed and is easy to configure.

Apart from SMTP, Avira AntiVir MailGate supports the Sendmail Milter interface.



This store and forward agent divides the work between two programs:

SMTP daemon

The SMTP daemon receives the emails and stores them in the spool directory. This program can run as an independent server using port 25 (SMTP) or it can be started by the Internet superdaemons inetd or xinetd.

Scanner and Forwarder daemon

The forwarder daemon reads the emails stored in the spool directory, decodes any attachments and then starts scanning for viruses and unwanted programs.

Depending on the result of the scanning process, clean emails are forwarded, while infected emails are blocked in the spool directory (rejected).

According to the configuration made in avmailgate.conf, the program also blocks suspicious emails, such as password-protected archives and fragmented emails, in the same directory. In the same configuration file you can define rules for the spam filter.

You can scan the queue on-demand using the Queue Manager avq (for scanning the spool directory, see Queue Manager avq – Page 56).

Warnings:
The postmaster receives an email containing detailed alerts when viruses, unwanted programs or suspicious files are detected. The alerts can also be sent to the sender and recipient of the email. The program contains alert templates that you can adjust and use.

Updater:
Avira Updater downloads current updates from the AntiVir web servers and installs them at regular intervals, manually or automatically. It can also send update notifications by email.

You can update Avira AntiVir MailGate entirely or only certain components: signatures, engine, scanner.

2.3 Licensing Concept

You must have a license to use Avira AntiVir MailGate and accept the license terms (see http://www.avira.com/documents/general/pdf/en/avira_eula_en.pdf).

There are 2 license modes for Avira AntiVir MailGate:
- Test version
- Full version

The license depends on the number of users in the network, who are to be protected by Avira AntiVir MailGate.

The license is contained in a license file named hbedv.key. You will receive it by email from Avira GmbH. It contains specific data such as the programs you will use and the period of your license. The same license file may refer to more than one Avira product.

Test Version

30-day test license for Avira AntiVir MailGate.

Details of the evaluation version can be found on our website: http://www.avira.com.

Full Version

The range of full version license includes:
- Avira AntiVir MailGate versions available by Internet download
- license file by email, to convert the test version into a full version
- complete installation instructions (digital)
- four weeks installation support, starting from acquisition date
- newsletter service (per email)
- Internet update service for program files and VDF

After installing an AntiVir product, you can read the information on your current license, using the license tool avlinfo.

▶ Change to /usr/lib/AntiVir and call `./avlinfo`

Use `avlinfo -h` to get information about using this tool.

The license file must have the suffix **.key** *(case insensitive).*

The new scanner backend (savapi) does not display information about the license file, when called with `--version`.

2.4 System Requirements

For Avira AntiVir MailGate to work properly on your server, the following minimum requirements have to be met (additional memory may be required, depending on the email traffic, number and size of attachments etc):

The versions for UNIX Server, UNIX Workstation and Sun Sparc Solaris have similar installation and operating procedures (in general, only some file names may differ, depending on the target operating system).

- Computer: x386, Sparc
- OS: Linux (with GLIBC 2.2 or higher), or Solaris
- CPU: 32-bit or 64-bit UNIX
  Running AntiVir software on 64-bit UNIX systems, requires the ability to execute 32-bit binaries. For instructions about checking and eventually enabling this behavior, please refer to the documentation of your UNIX system.
- 8 MB free hard disk space for product installation
- 20 MB temporary disk space
- 32 MB free memory space (64 MB recommended)
- Administration through Avira SMC: Please consider that the libstdc++so.5 is required for the SMC Agent.

Officially supported distributions for Avira AntiVir MailGate:

- Red Hat Enterprise Linux 5 Server
- Red Hat Enterprise Linux 4 Server
- Novell Open Enterprise Server (10.2)
- Novell Linux Desktop 9 (NLD 9)
- Novell SUSE Linux Enterprise Server 11 (SLES 11)
- Novell SUSE Linux Enterprise Server 10 - 10.2 (SLES 10)
- Novell SUSE Linux Enterprise Server 9 (SLES 9)
- Debian GNU/Linux 4
- Debian GNU/Linux 5 (stable, lenny)
- Ubuntu Server Edition 8
- Ubuntu Server Edition 9 (intrepid)
- Sun Solaris 9 (SPARC)
- Sun Solaris 10 (SPARC)
- Gentoo

3 Milter Mode

3.1 Overview

AntiVir Milter has been a stand-alone product up to now. The product has been available only for Sendmail, using the Sendmail Milter interface. Now, the Milter functionality is integrated in MailGate.

In order to start MailGate in Milter mode, the option `ListenAddress` in avmailgate.conf requires the following syntax (after installing MailGate):

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

– OR –

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

Example:

```
unix:/path/to/file
local:/path/to/file
```

If necessary, the `ForwardTo` entry has to be set to the Sendmail binary. If the default value is correct, the option has to remain unchanged:

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

AntiVir MailGate will no longer use the avmilter.* files for Milter mode. They have to be renamed avmailgate.*

Example: `mv /etc/avmilter.warn /etc/avmailgate.warn`

To migrate from an older Milter installation to the current AntiVir MailGate (Milter mode), the file MILTER_MIGRATION must be used. It is located in the /doc directory of the product kit.

It is recommended to adjust the file avmailgate.conf *instead of renaming the file* avmilter.conf

3.2 AntiVir MailGate (Milter Mode) Features

AntiVir MailGate (Milter mode) is a plug-in for Sendmail, starting with version 8.11, and communicates through Sendmail's libmilter interface.

It scans all incoming and outgoing emails. Infected emails are not forwarded. A status notification is shown in syslog. It can notify senders, recipients and administrators of infections.

Functions

Most of these features also apply to MailGate, even when it is not running in Milter mode.

- All Sendmail features remain available.
  Example: SMTP authentication, anti-relaying and anti-spam
- Simple installation and integration in Sendmail
- Hourly or daily Internet update for scan engine and VDF
- Scanning of incoming and outgoing emails
- Reliable on-access detection of viruses and malware
- Configurable reaction when viruses or malware are detected
- Isolation of infected or suspicious files in a quarantine directory
- Logfile used as email traffic log
- Immediate activation of new VDF
- Heuristic macrovirus detection
- Configurable templates for alerts
- Archive scanning

3.3 AntiVir MailGate (Milter Mode) Integration in Sendmail

3.3.1 Requirements

Sendmail version 8.11 or newer with libmilter interface is required.

Otherwise:

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

▶ Compile the new version of Sendmail with libmilter interface.

To check, if Sendmail with libmilter interface has been compiled:

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

3.3.2 Integration

There are two ways of adding AntiVir MailGate (Milter mode) to Sendmail's configuration file sendmail.cf:

- Directly modify sendmail.cf

– OR –

- generate sendmail.cf

Directly modify sendmail.cf

▶ Insert the following two lines in the configuration file sendmail.cf:

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

Value meaning

- F: determines what should happen if the filter is not available:
  - T: emails are temporarily not accepted (error 4XX)
  - R: emails are rejected (error 5XX)
- T: sets the following timeouts:
  - C: timeout to set up the connection to filter
  - S: timeout while sending information to filter
  - R: timeout while reading an answer from filter
  - E: timeout between sending the "End of message" and the response from the filter

Change these values if the log displays this notification:
"Milter (avmilter): timeout before data read"

Generate sendmail.cf

▶ Insert the corresponding lines in the file sendmail.mc
(commands beginning with `INPUT` must be written in 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 AntiVir MailGate on Avira website. AntiVir is supplied as a packed archive. You can install the program on your system using the install script.

Requirements

You have to be logged in as **root** in order to install AntiVir MailGate. You also need an MTA (Sendmail, Postfix, Exim, Qmail etc.) available on your system. We cannot provide support for problems that do not directly concern AntiVir MailGate.

This section describes an example installation of a standard Sendmail configuration on a SuSE distribution. If you want to integrate the program with another MTA or, for example, with Lotus Domino, you can find further information in the related files (INSTALL.sendmail, INSTALL.exim, INSTALL.qmail, INSTALL.postfix etc.).

This Chapter contains the following sections:

- Preparing the Installation Files – Page 15
- Licensing – Page 15
- Installation with the Installation Script "install" – Page 16
- Reinstalling and Uninstalling AntiVir – Page 19
- Further Installation Steps, Depending on the MTA – Page 20
- Testing AntiVir MailGate after Installation – Page 25

If you have also installed Avira AntiVir Server (UNIX) or Avira AntiVir Professional (UNIX) and you use the Graphical User Interface to configure and operate these products, please note that the GUI is not compatible with the current versions (starting with version 3) of Avira AntiVir MailGate and Avira AntiVir WebGate.

4.1 Preparing the Installation Files

Downloading program files from the Internet

- Download the current files from our website http://www.avira.com to your local computer. The file name is antivir-mailgate-prof-<version>.tar.gz
- Copy the file to a directory of your choice on the computer on which you want to install AntiVir MailGate. For example, in /tmp.

Unpacking program files

- Go to the temporary directory:

  ```
  cd /tmp
  ```

- Unpack the archive for the AntiVir kit:

  ```
  tar -xzvf antivir-mailgate-prof-<version>.tar.gz
  ```

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

4.2 Licensing

You need a license to run AntiVir MailGate (see Licensing Concept – Page 9). The license file hbedv.key is delivered by email. It contains information on the scope and period of the license.

Acquiring the license

- You may test AntiVir MailGate for 30 days, if you fill in the test license form on our website.
- Contact us by telephone or at sales@avira.com to obtain a valid license file by email.
- You can also purchase AntiVir through our Online Shop (for more details, please visit http://www.avira.com).

Copying the license file

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

You can copy the license file later to the program directory /usr/lib/AntiVir/

4.3 Installation with the Installation Script "install"

The install script performs the installation of AntiVir MailGate automatically.

It performs the following tasks:

- checks the integrity of the installation files;
- checks for the required authorizations for installation;
- checks for an existing version of AntiVir MailGate on the computer;
- copies the program files (and overwrites existing, obsolete ones);
- copies configuration files (and keeps existing configuration files);
- installs Avira Updater;
- optional: installs the GUI support for Avira SMC (Security Management Center).

Preparing installation

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

▶ Login as **root**. Otherwise you do not have the required authorization for installation and the script returns an error message.

▶ Go to the directory where you unpacked the AntiVir MailGate kit. For example:

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

Installing AntiVir MailGate

▶ Type:

```
./install
```

↳ The installation script starts.

▶ You must read the license agreement and agree with it for the installation to continue.

▶ Quit the license agreement file with q.

↳ The following question appears:

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

▶ Type y and press **Enter**.

↳ The AntiVir Engine is being installed. Then the script asks for the path to the license file:

```
creating /usr/lib/AntiVir ... done
1) installing AntiVir Core Components (Engine, Savapi and Avupdate)
copying ...

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

▶ Type the path to the license file and press **Enter**

– OR –
If you want to copy the license file later, just click **Enter**.

↳ The next step is installing the automatic Internet Updater. Then you are asked whether a link should be created in /usr/sbin for the start script:

```
2) Configuring updates
An internet updater is available with version 3.1.2-1 of
AVIRA MailGate (UNIX). It will ensure that you always have the latest
virus signatures and engine updates.

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

Please read the README file for more information about updating and
which method best suits you.

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

▶ Confirm with **Enter** or click n.

↳ Then you are asked if you want to create cron jobs for the Scanner and for 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]
creating MailGate update cronjob ... done
setup internet updater complete
```

You can also set these options later.

↳ The script continues, with the installation of the main program:

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

▶ You have to provide the path for the manual pages:

```
Enter the path where the manual pages will be located [/usr/share/man]
```

▶ Confirm the default path with **Enter** or type another one.

↳ The following questions regard the local and relayed hosts:

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

▶ Change the host name, if necessary, and press **Enter**.

↳ The next question is:

```
Enter the hosts and networks that are allowed to relay:
[127.0.0.1/8 192.168.0.0/16]:
```

▶ Change the settings if necessary and press **Enter**.

↳ Then you are asked whether a link should be created in /usr/sbin for the start script:

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

▶ Confirm with **Enter** or click n.

↳ Then you are asked whether AntiVir MailGate should start automatically:

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

▶ Type n and click **Enter**. You can change this option later

– OR –

Confirm the default setting with **Enter**.

↳ The next step installs the SMC plugin, for 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,** if you want to install the SMC plugin (or n and **Enter**, to skip it).

↳ The following message appears, when the script is finished:

```
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, proceed with the installation as described in Further Installation Steps, Depending on the MTA – Page 20.

▶ Finally, you can start AntiVir MailGate:

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

Modified binaries will not run.
For example, if binaries are prelinked: Either disable prelinking or add /usr/lib/AntiVir as an excluded prelink path in /etc/prelink.conf.

Starting with version 3.0.0, a new scanner backend is used. Old scanner specific configuration options, that are not known to MailGate, must be moved from
/etc/avmailgate.conf
to the scanner specific configuration file
/etc/avmailgate-scanner.conf.

It is highly recommended that you perform an update after installation, to ensure up-to-date protection. This can be done by running:

```
/usr/lib/AntiVir/avupdate --product=MailGate
```

For more details on updating, see Updates – Page 60.

4.4 Reinstalling and Uninstalling AntiVir

You can re-launch the install script at any time. There are several possible situations:

- Install a new version (upgrade). The installation script checks the previous version and installs the necessary new components.
  The configuration settings already made are not overwritten, but inherited (see Configuration – Page 26).
- Later installation of some components.
- Activating or deactivating the automatic start of Avira Updater or AntiVir MailGate.

Reinstalling Avira AntiVir MailGate

The steps are the same in all cases:

▶ Open the directory where you unpacked AntiVir MailGate. For example:

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

▶ Type:

```
./install
```

↳ The installation script runs as described above.

▶ Make the changes you need during installation procedure.

AntiVir MailGate is installed with the required settings.

Uninstalling AntiVir

You can use the *uninstall* script, located in the temporary AntiVir directory, to remove Avira AntiVir MailGate. The syntax is:

```
uninstall [--product=productname] [--no-interactive]
 [--force] [--version] [--help]
```

where `productname` is `Mailgate.`

▶ Open the AntiVir directory:

```
cd /usr/lib/AntiVir
```

▶ Type:

```
./uninstall --product=Mailgate
```

↳ The script starts uninstalling the product, asking you step by step, if you want to keep backups for the license file, for the configuration files and logfiles; it can also remove the cronjobs you made for MailGate and Scanner.

▶ Answer the questions with **y** or **n** and press **Enter**.

↳ Avira AntiVir MailGate is removed from your system.

4.5 Further Installation Steps, Depending on the MTA

After installing AntiVir MailGate as described above, you have to make some manual settings, depending on your MTA.

The following part describes Sendmail, Exim, Qmail and Postfix specifics.

Configuring Sendmail

If you are working with Sendmail, we recommend that you use AntiVir MailGate in Milter mode (see Chapter Milter Mode – Page 11). It guarantees full SMTP functionality in Sendmail (such as SMTP authentication).

Configuring Exim

AntiVir MailGate runs with Exim version 3.0 or newer.

▶ To detect your Exim version use the command:
`exim -bV`

There are two ways of integrating AntiVir MailGate with Exim:

- Integrate AntiVir MailGate as a content filter in Exim (recommended)

- Proxy mode

Content Filter

AntiVir MailGate configuration:

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

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

▶ Restart AntiVir MailGate.

Exim configuration:

▶ Modify (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 router entry:

▶ Search for the entry `begin router` in exim.conf 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 transport entry:

▶ Search for `begin transports` in exim.conf 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

AntiVir MailGate configuration:

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

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

▶ Restart AntiVir MailGate.

Exim configuration:

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

```
daemon_smtp_port = 825
```

▶ Restart Exim.

Configuring Qmail

A plugin for Qmail is available, for better integration of AntiVir MailGate into Qmail. Please contact support@avira.com for details.

There are two ways to integrate AntiVir MailGate with Qmail:

- Sendmail wrapper
- Backdoor mechanism

Replace SMTP with SMTP-Backdoor only in the run *file. All the other parameters are just examples.*

Sendmail wrapper

You can use Sendmail wrapper, which was supplied with Qmail, to deliver emails (default). First, go to the Qmail installation folder and activate the wrapper.

▶ Activate the Sendmail wrapper in Qmail:

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

▶ Establish the email forwarding mode. Refer to the file /etc/avmailgate.conf for the following line:
`# Select how mail should be forwarded.`

▶ Change these entries as below:

```
# Send mail by piping it thru 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 smtp-backdoor
```

Backdoor mechanism

The second possibility sets email delivery on port 825, on which Qmail should be active. This is done, for example, with inetd.conf (see Qmail installation package).

▶ Insert the following line in /etc/services:

```
smtp-backdoor 825/tcp
```

▶ Establish the email forwarding mode. Look into the file /etc/avmailgate.conf for:
`# Select how mail should be forwarded.`

▶ Change these entries as below:

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

If you use inetd with Qmail:

▶ Insert the following line in inetd.conf (one line!):

```
smtp-backdoor stream tcp nowait qmaild /var/qmail/bin/
tcp-env tcp-env /var/qmail/bin/qmail-smtpd
```

If you use tcpwrapper with Qmail:

▶ Change the Qmail port in /var/qmail/supervise/qmail-smtpd/run. For example, look 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
```

▶ Edit the lines as follows:

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

Configuring Postfix

There are two ways of integrating AntiVir MailGate with Postfix:

- Integrate AntiVir MailGate as a content filter in Postfix (recommended)
- AntiVir MailGate listens on port 25 and forwards emails to Postfix

Content Filter

From Postfix snapshot 20000520, it is possible to integrate AntiVir MailGate as a content filter. The first release with possible content filtering was 20010228. Proceed as follows:

▶ Make the following entries in etc/services:

```
# Content Filter for postfix
antivir 10024/tcp #Port for smtp daemon
smtp-backdoor 10025/tcp #Port for postfix backdoor
```

▶ Look for the following line in /etc/avmailgate.conf:

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

▶ Change these entries as below:

```
# Select how mail should be forwarded.
# Send mail by piping it thru 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 smtp-backdoor
# The location of the scanner's socket.
# MailGate connects to this socket to perform scan requests.
ScannerListenAddress /var/run/avmailgate/scanner
```

If you use SuSE Mail Server II:

▶ Replace the entry `#AllowSourceRouting NO` with:

```
AllowSourceRouting YES
```

▶ Stop and restart AntiVir MailGate:

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

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

```
# service type private unpriv chroot wakeup maxproc command + args
# (yes) (yes) (yes) (never) (50)
   smtp inet n - n - - smtpd
   For AntiVir Mail daemon
   localhost:smtp-backdoor inet n - n - - smtpd -o content_filter=
   (one line!)
```

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

The entry `smtpd -o content_filter` deactivates the corresponding line in a second Postfix instance (avoids mail loops).

▶ Add into /etc/postfix/main.cf:

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

▶ Restart Postfix:

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

or

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

If Postfix sets the status **deferred** *for emails, after AntiVir MailGate installation:*

▶ Search in main.cf for the line:

```
defer_transports = local
```

▶ Comment it out:

```
# defer_transports = local
```

Listen on port 25

▶ Look in master.cf for:

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

▶ Comment it out:

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

↳ It prevents Postfix from listening on SMTP port. SMTP daemon can listen on this port. Emails forwarded by the SMTP daemon will be processed by the Sendmail wrapper /usr/lib/sendmail (delivered by Postfix).

▶ Restart Postfix:

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

or

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

4.6 Testing AntiVir MailGate after Installation

After installing AntiVir MailGate, it is recommended that you test its functionality. To do this, you can use a test virus, called Eicar, which is recognized by all virus scanners. This will not cause any damage, but it will force the program to react when an email scan is performed, if the installation (and configuration) is correct.

▶ Copy the following string to 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 to a test email for AntiVir MailGate.

▶ Check the reactions in the directory /var/spool/avmailgate/rejected.

▶ Check the messages AntiVir MailGate sent to the logfile or syslog.

5 Configuration

You can adjust AntiVir MailGate for optimum performance on your system. During installation with the install script, some of the settings are suggested and you can make changes at any time.

In this section, you will be guided step by step through the configuration process. It contains the following sections:

- MailGate Spool Directories – Page 27
- MailGate Configuration in avmailgate.conf – Page 28
- Spam Filter Configuration (Avira MailGate Suite only) – Page 41 (This feature is only activated with the license for **Avira MailGate Suite**.)
- Scanner Configuration in avmailgate-scanner.conf – Page 46
- Hosts Configuration in avmailgate.acl – Page 47
- Warnings Configuration in avmailgate.warn – Page 48
- Report Templates Configuration – Page 48
- Updater Configuration in avupdate.conf – Page 51

The configuration files are read when the program starts. It will ignore empty lines or lines beginning with #.

They are provided with default values, which are suitable for most set-ups. Some entries are deactivated or commented out using # and they can be activated by deleting the # sign.

Starting with MailGate 3.0.0, unknown configuration options trigger an error message: WARNING: found an unknown config option ... while parsing the configuration file.

The list of configuration files is shown when you complete the installation:

/etc/avmailgate.conf	(AVIRA MailGate main config)
/etc/avmailgate-scanner.conf	(AVIRA MailGate scanners config)
/etc/avmailgate.acl	(AVIRA MailGate access list)
/etc/avmailgate.ignore	(AVIRA MailGate ignore list)
/etc/avmailgate.scan	(AVIRA MailGate scan list)
/etc/avmailgate.warn	(AVIRA MailGate warn list)
/etc/asmailgate.except	(AVIRA MailGate spamfilter config)
/etc/avira/avupdate.conf	(AVIRA Avupdate options)

The configuration file /etc/antivir.conf is no longer used. Users are strongly recommended to remove this file. All settings for AntiVir MailGate should be done in ***/etc/avmailgate.conf*** *and all settings for the internet updater should be done in* ***/etc/avira/avupdate.conf****.*

Although /etc/antivir.conf will still be read, the software will issue a warning that the file is deprecated.

5.1 MailGate Spool Directories

AntiVir MailGate isolates infected emails in "quarantine". Depending on the configuration, a message about the detection of a virus/unwanted program is sent to postmaster and/or the sender and/or recipient of the email. These parameters can be set in the file avmailgate.conf (see MailGate Configuration in avmailgate.conf – Page 28).

Spool directories

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

- incoming: incoming emails that must be scanned.
- outgoing: scanned emails that can be forwarded.
- rejected: emails containing a virus/unwanted program, or classified as problematic due to a MIME error, for example.

Spool files

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

- data file
- control file

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

The control file has the same ID, but according to its status its name begins with:

- xf-: control file has just been processed;
- qf-: the email is to be subjected to a virus scan;
- Qf-: the email is to be forwarded without scanning;
- vf-: the email contains a virus/unwanted program;
- mf-: the email has a MIME problem.

Example

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

Spool files processing

If there is a virus/unwanted program detection, the directory /var/spool/avmailgate/rejected/ contains:

- df-file
- vf-file or mf-file

These files can be processed by external programs or scripts, such as those set by the `ExternalProgram` parameter (see MailGate Configuration in avmailgate.conf – Page 28).

If no virus/unwanted program is detected, data files and control files are deleted after scanning and sending the email.

5.2 MailGate Configuration in avmailgate.conf

The configuration file avmailgate.conf contains numerous parameters for working with AntiVir MailGate.

Configuration procedure

▶ Edit avmailgate.conf according to your preferences.

▶ Restart MailGate to activate the new settings:

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

The entries in avmailgate.conf are described below, in thematic groups. These entries only influence the actions of AntiVir MailGate and not other AntiVir software.

When changing User, Group, PidDir or ListenAddress, you have to stop MailGate first.

User, Group

Users/Group:

The users and group for MailGate processes (they should not be **root**).

If you modify this parameter, you must also change the value for `User` *and* `Group` *in* /etc/avmailgate-scanner.conf. *See Scanner Configuration in avmailgate-scanner.conf – Page 46*

Default values:

```
User uucp
Group antivir
```

If these are modified, the access rights of the relevant directories must also be changed.

Postmaster

Postmaster:

The email address to receive alerts about concerning viruses/unwanted programs, as well as other notifications:

```
Postmaster postmaster
```

MyHostName

Host name:

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

If not set, the default setting is given by `gethostname(2)`. Otherwise, the default is:

```
MyHostName localhost
```

SpoolDir

Spool directory:

Emails are kept in the sub-directories incoming, rejected and outgoing while being processed.

The spool directory must belong to the user defined under `User` and the associated `Group` and must only be accessed by this user (mode=700).

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

AntiVirDir

AntiVir directory:

The library directory of AntiVir MailGate, including virus definition files antivir*.vdf and the license file. If you use AntiSpam, do not modify the default AntiVir directory:

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

Temporary Dir

Temporary directory:

This directory contains temporary files (such as attachments currently being scanned for viruses or unwanted programs). Sufficient space is required for unpacked attachments. If not set, the TMPDIR environment variable will be used.

If you want to use a single tmp directory for all MailGate components, you can change the option `TemporaryDir` *in* /etc/avmailgate.conf, *and* `ScanTemp` *in* avmailgate-scanner.conf.

Default:

```
TemporaryDir /var/tmp
```

MatchMail AddressFor Local

Check domain name:

This option determines whether the domain names of RECIPIENT, SENDER or BOTH addresses should be matched with the entries in the `local:` section in avmailgate.acl, in order to accept the email.

For more information, see Hosts Configuration in avmailgate.acl – Page 47.
Default is:

```
MatchMailAddressForLocal RECIPIENT
```

SMTPBanner

SMTP message:

Sets the headers sent by MailGate. You can edit the text, for example, if you do not want to reveal the type of security software. Default is:

```
SMTPBanner "AntiVir MailGate"
```

PidDir

PID directory:

This directory saves the PID files for MailGate's main processes. You must stop AntiVir MailGate before changing this parameter.

```
PidDir /var/tmp
```

Syslog Facility

Syslog facility:

It sets the log category that Syslog should apply for MailGate messages.

```
SyslogFacility mail
```

LogFile

Logfile:

It must contain the full path to the log file. Apart from the log file, entries will also be sent to syslog.

If LogFile is set to NO (default), no log file is used. The entries will still be sent to syslog.

```
LogFile NO
```

-or-

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

DebugLevel

Debug output:

It determines the level of debug output written in syslog and, if set, in the logfile.

Possible values: 0 (disabled) - 5 (all messages).

```
DebugLevel 0
```

Listen Address

IP address:

The address and the port on which the SMTP daemon listens. AntiVir MailGate listens on all network cards (by 0.0.0.0) or a specific IP address can be defined. If you are uncertain, you can **keep the default setting**:

```
ListenAddress 0.0.0.0 port 25
```

You can start AntiVir MailGate in Milter mode using a different syntax. For more details, see Chapter Milter Mode – Page 11.

MaxIncoming Connections

Maximum number of simultaneous connections (not in milter mode):

Sets the number of simultaneous connections from remote sites. For example, you can set the maximum number of simultaneously incoming emails to 100. For unlimited connections, use 0 (default setting).

```
MaxIncomingConnections 0
```

SMTP Timeout

SMTP timeout (not in milter mode):

Defines the maximum timeout in seconds for SMTP connections.

```
SMTPTimeout 300
```

MaxMessage Size

Maximum message size (not in milter mode):

A value greater than 0 means that only emails up to the given size are scanned. Larger emails are rejected. If the value is 0, all messages of any size are scanned.

e.g.: 4KB, 3MB, 2GB.

```
MaxMessageSize 0
```

MinFree Blocks

Minimum free system space (not in milter mode):

AntiVir MailGate refuses incoming connections, if the free hard disk space is smaller than the given value.

```
MinFreeBlocks 100
```

Max Recipients PerMessage

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

Defines the maximum number of recipients for an email. The 0 value deactivates this option.

```
MaxRecipientsPerMessage 100
```

RefuseEmpty MailFrom

Reject emails without sender name (not in milter mode):

It is possible to receive messages without the sender's name. The default setting is NO, so that the SMTP server accepts all incoming emails. This default setting should not be changed.

```
RefuseEmptyMailFrom NO
```

RFC2821, RFC821 and RFC2505 recommend that all emails (even without the sender's address) should be accepted by an SMTP server. It is recommended not to change the default setting for the parameter `RefuseEmptyMailFrom`.

AllowSource Routing

Allow source routing (not in milter mode):

Source routing has the following address syntax:

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

This address sets the route for the email: it passes through `ONE` and `TWO` and it is finally delivered to `JOE` on host `THREE`.

This option specifies whether all except `JOE@THREE` should be excluded (`NO`) or whether the address should be retained (`YES`).

```
AllowSourceRouting   NO
```

InEnvelope Addresses BangIs

Exclamation mark in envelope address (not in milter mode):

- If `REFUSED` is set and there is an "!" in the recipient's address, the message is rejected.
- If `IGNORED` is set, "!" is treated as a normal sign in the recipient's address.
- If `INTERPRETED` is set, the recipient's address is transformed into RFC821 standard form. For example, the address
  `hostA!hostB!hostC!user`
  is transformed into

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

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

```
InEnvelopeAddressesBangIs   REFUSED
```

InEnvelope Addresses PercentIs

Percent sign in envelope address (not in milter mode):

If `REFUSED` is set and a '%' sign is in the recipient's address, the message is rejected.

If `IGNORED` is set, '%' is treated as a normal sign in the address.

If `INTERPRETED` is set, the recipient's address is transformed into RFC821 standard form. For example, the address

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

is transformed into

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

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

```
InEnvelopeAddressesPercentIs REFUSED
```

AcceptLoose DomainName

Checking email domain syntax (not in milter mode):

A domain name must contain the following characters only: [-.0-9A-Za-z]
The parameter `AcceptLooseDomainName` also allows incorrect domain names.

If the setting is `NO` and the domain name for message delivery is not correct (depending on source routing), the message is rejected.

If the setting is `YES`, the domain name is not checked. Therefore, even if the domain is incorrect, the email is forwarded.

```
AcceptLooseDomainName NO
```

AddressFilter

Filtering email addresses:

This option can activate/deactivate the address filter. The default setting is `NO`, i.e. no address filter is used with the standard installation.

```
AddressFilter NO
```

To be able to use the address filter, the following files are necessary:

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

and

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

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

The lists are checked. Checking begins with the first list on `FilterTableOrder`. When a match is found, the checking is terminated and the configured action performed.

According to the result, the procedures are:

- if there is no match in the first list, the next list is checked.
- if there is no match in the second list either, the email is scanned.
- if there is a match in the ignore list, the email is not scanned.
- if there is a match in the scan list, the email is scanned.

The email addresses must have Perl-compatible regular expressions, such as:

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

Example:

/etc/avmailgate.ignore contains the following lines:

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

If the address is somebody@somewhere.tld, the email is not scanned.

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

/^virus@firm/ R is equal to /^virus@firm/.

When starting AntiVir MailGate, `maillog` will indicate whether the address filter is active or not:

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

or

```
addressfilter is not active
```

Filter TableOrder

Scanning order of the filter table:

This option can be used only if AddressFilter is active (`AddressFilter YES`). The possible parameters are:

```
FilterTableOrder scan,ignore
```

or

```
FilterTableOrder ignore,scan
```

SMTP Greeting Timeout

Defines the maximum timeout, in seconds, for receiving the greeting message from the remote host (not in milter mode).

```
SMTPGreetingTimeout 300
```

SMTPHelo Timeout

Defines the maximum timeout, in seconds, for receiving a reply to the SMTP HELO

command (not in milter mode).

```
SMTPHeloTimeout 300
```

SMTP MailFrom Timeout

Defines the maximum timeout, in seconds, for receiving a reply to the MAIL FROM command (not in milter mode).

```
SMTPMailFromTimeout 300
```

SMTP Rcpt Timeout

Defines the maximum timeout, in seconds, for receiving a reply to the RCPT TO command (not in milter mode).

```
SMTPRcptTimeout 300
```

SMTP Data Timeout

Defines the maximum timeout, in seconds, for receiving a reply to the DATA command (not in milter mode).

```
SMTPDataTimeout 120
```

SMTP DataBlock Timeout

Defines the maximum timeout, in seconds, for sending individual data blocks (not in milter mode).

```
SMTPDataBlockTimeout 180
```

SMTP DataPeriod Timeout

Defines the maximum timeout, in seconds, for receiving a reply to the final dot of the DATA command and QUIT command after sending the message (not in milter mode).

```
SMTPDataPeriodTimeout 600
```

Max Forwarders

Maximum number for the forwarder:

Maximum number of simultaneous forwarding processes. The value depends on the efficiency of your email system and on the quality of your email connection (default value: 10).

```
MaxForwarders 10
```

ForwardTo

Forwarder:

Defines how emails should be sent (default: by Sendmail).

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

The email can also be sent by SMTP:

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

The SMTP setting applies only to MailGate in SMTP mode. In Milter mode, it can only be forwarded by the program. Therefore, the valid entry is:

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

ScannerListen Address

Scanner location:

Sets the location of the scanner's socket, for MailGate to connect and perform scan

requests.

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

If you modify this parameter, you must also set the same value for `ListenAddress` *in* /etc/avmailgate-scanner.conf. *See* *Scanner Configuration in avmailgate-scanner.conf – Page 46*

Max Attachments

Maximum number of email attachments (MIME):

Defines the maximum number of attachments for a single MIME email.

```
MaxAttachments 100
```

Block Suspicious Mime

Blocking suspicious emails (MIME):

Blocks suspicious MIME emails. An email is classified as suspicious if it exceeds the maximum recursion levels or the maximum attachment number (default setting: NO).

```
BlockSuspiciousMime NO
```

Block Fragmented Message

Blocking fragmented emails:

Blocks fragmented emails. For further information, see "Message Fragmentation and Reassembly", RFC 2046, http://www.faqs.org/rfcs/rfc2046.html, paragraph 5.2.2.1).

```
BlockFragmentedMessage NO
```

BlockPartial Archive

Block partial archive:

If activated (YES), this option blocks mails containing an archive, which is part of a multivolume archive.

```
BlockPartialArchive NO
```

Block Extensions

Blocking emails with certain extensions:
You can configure MailGate to block emails containing attachments with specified file extensions (such as exe, scr, pif). This also applies to archived files.

```
BlockExtensions NO
```

-or-

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

Expose Recipient Alerts

Sending alerts to recipients of suspicious emails:

You can send alerts of viruses and unwanted programs to recipients. The available values are:

- **NO**: the recipient will receive no virus alert.
- **LOCAL**: alert messages are sent only if the recipient is a local user of your domain. Set the option in avmailgate.acl to `local`.
- **YES**: the recipient always receives virus alerts.

```
ExposeRecipientAlerts LOCAL
```

ExposeSenderAlerts

Sending alerts to senders of concerning emails:

You can send alerts about viruses and unwanted programs to senders. The available values are:

- **NO**: the sender will receive no virus alert.
- **LOCAL**: alert messages are sent only if the sender is local user in your domain. Set the option in avmailgate.acl to `local` (not in milter mode).
- **YES**: the sender always receives virus alerts for the concerning emails.

```
ExposeSenderAlerts LOCAL
```

ExposePostmasterAlerts

Sending alerts to postmaster:

Sends alerts about viruses or unwanted programs to the postmaster.

```
ExposePostmasterAlerts YES
```

AlertsUser

Warning recipients:

Name or email address of the recipients to be warned (if a virus/unwanted program is detected in an email):

```
AlertsUser AvMailGate
```

or

```
AlertsUser AvMailGate@domainname
```

AddStatusInBody

Status information in email body:

If the setting is NO, the email contains no additional information (default):

```
AddStatusInBody NO
```

If the setting is YES:

- If a file named `body-state` exists in the template subdirectory of the program, the text from this file is inserted in the mail (see Report Templates Configuration – Page 48).
- `AddStatusInBody` could also take the name of a file. In this case, the contents of the file are added.

MaxMessageSizeStatus

Status text:
If the option `AddStatusInBody` is set to `YES`, no status text is added to an email that exceeds the given size value.

e.g.: 4KB, 3MB, 2GB. Default:

```
MaxMessageSizeStatus 0
```

ForwardAllEmailAsMIME

Forwarding emails as MIME (not in milter mode):

Even if not in MIME, emails can be transformed into MIME emails. They have a MIME header with content type: text/plain, content disposition: inline and content encoding: 7 bit or 8 bit. "Encoding" depends on the original email.

If the setting is NO, non-MIME emails are sent without further processing.

If the setting is YES, non-MIME emails are transformed into MIME emails.

```
ForwardAllEmailAsMIME NO
```

ScanInArchive

Scan in archives:

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

If the setting is YES, all files in archives are unpacked and scanned, depending on the settings for `ArchiveMaxSize`, `ArchiveMaxRecursion` and `ArchiveMaxRatio`.

```
ScanInArchive YES
```

Archive MaxSize

Maximum unpacked size of archived files:

There are some archived files that have useless content but intentionally expand to an "irrational size" when unpacked in order to slow down the computer. This parameter avoids unpacking such archive files.

If the setting is 0, all archived files are unpacked, whatever their size.

If the set value is >0, all archives that do not exceed the given value (in bytes) are unpacked and scanned.

e.g.: 2KB (2 Kilobytes), 3MB (3 Megabytes).

```
ArchiveMaxSize 0
```

ArchiveMax Ratio

Blocking "mail bombs":

Blocks so-called "mail bombs" with a very high compression ratio. You can set the maximum difference between packed and unpacked file size.

The zero value deactivates this option (**not** recommended). The default is 150.

```
ArchiveMaxRatio 150
```

ArchiveMax Recursion

Maximum archive recursion:

If the setting is 0, recursive (nested) archives are unpacked, whatever their recursion depth.

If the set value is >0, all archives that do not exceed the given recursion depth are unpacked. This saves processing time.

```
ArchiveMaxRecursion 20
```

Block Suspicious Archive

Blocking emails with suspicious archives:

If activated (YES), this option blocks archives that exceed one of the settings for `ArchiveMaxSize`, `ArchiveMaxRecursion` and `ArchiveMaxRatio`.

If the option is deactivated (NO), such archives are forwarded, disregarding the settings for `ArchiveMaxSize`, `ArchiveMaxRecursion` and `ArchiveMaxRatio`.

```
BlockSuspiciousArchive NO
```

Block Encrypted Archive

Blocking emails with password-protected archives:

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

If NO is set, emails containing encrypted archives are also delivered.

```
BlockEncryptedArchive   NO
```

Detect...

Detection of other types of unwanted programs:
Besides viruses, there are some other types of harmful or unwanted software, described in avmailgate.conf. You can activate their detection using the following options:

```
DetectADSPY yes
DetectAPPL yes
DetectBDC yes
DetectDIAL yes
DetectGAME no
DetectHIDDENEXT yes
DetectJOKE no
DetectPCK no
DetectPHISH yes
DetectSPR no
```

Heuristics Macro

Macrovirus Heuristics:
Activates the heuristics for macroviruses in documents.

```
HeuristicsMacro yes
```

Heuristics Level

Win32-Heuristics:
Sets the detection level of Win32-Heuristics. Available values are 0 (off), 1 (low), 2 (medium) and 3 (high).

```
HeuristicsLevel 3
```

Block OnError

Blocking emails on scan error:
If set to YES, it blocks emails if an error occurs during scanning attached archives or cause the scan process timeout.

```
BlockOnError NO
```

Block Unsupported Archive

Blocking emails with unsupported archives:
Blocks emails containing archives that are not supported by the scanner.

```
BlockUnsupportedArchive NO
```

RejectAlertMail

Rejecting emails containing alerts:
(Available only in Milter mode) If `RejectAlertMail` is YES, an email containing an alert will be rejected with the message "**Alert found in email**". It will be moved to the quarantine directory depending on the setting of QuarantineAlert.

If `RejectAlertMail` is NO, the email will be accepted and moved to quarantine.

```
RejectAlertMail NO
```

Quarantine Alert

Sending alert emails to quarantine:
(Available only in Milter mode) If `QuarantineAlert` is `YES` and `RejectAlertMail` is `YES`, an email containing an alert will be rejected and the email will be quarantined.

If `QuarantineAlert` is `NO` and `RejectAlertMail` is `YES`, the email will be rejected and not quarantined.

```
QuarantineAlert YES
```

PollPeriod

Scanning queue:

Sets the interval, in seconds, for the program to scan the emails queue for viruses and malware.

```
PollPeriod 60
```

Queue Lifetime

Email lifetime in queue (not in milter mode):
The maximum time for an email to wait in the queue before rejection.
The value can be given in seconds, minutes, hours or days. For example:
10s, 10m, 10h, 10d.

The zero value deactivates the option.

```
QueueLifetime 0
```

Forwarder RetryDelay

The interval for MailGate to retry forwarding an email (not in milter mode).
The value can be given in seconds, minutes, hours or days (see above).

```
ForwarderRetryDelay 30m
```

Throttle Message Count

This option is necessary if too many emails are gathered in the queue and MailGate is restarted (not in milter mode).

In this case, all emails are processed as soon as possible. It can lead to load problems.

The set number is the maximum number of emails to be processed by `ThrottleDelay` (see the example below).

It is important not to accept any more emails while this option is active. These would not be processed immediately.

This option should only be used temporarily.

The option `ThrottleDelay` also has to be set.

```
ThrottleMessageCount 0
```

Throttle Delay

This option sets the number of emails (`ThrottleMessageCount`) to be sent in a time interval, in seconds (not in milter mode). Default: 0, deactivates the option.

```
ThrottleDelay       0
```

Example:

There are 100 emails in the queue. `ThrottleMessageCount` is set to 10 and `ThrottleDelay` to 1. Then a maximum of 10 emails are processed per second.

BounceMessageUser

Recipient for email failure (not in milter mode):

This is the user that receives email failure reports when an email cannot be sent by MTA.

```
BounceMessageUser MAILER-DAEMON
```

BounceMessageSizeBody

Size of the email failure - mail body (not in milter mode):

Sets the size in bytes from the original mail body, to be returned by bounce mail. The value 0 means no limit is set.

e.g.: 4KB, 3MB, 2GB.

```
BounceMessageSizeBody 0
```

BounceMessageSizeHeader

Size of the email failure - mail header (not in milter mode):

Sets the size in bytes from the original mail header, to be returned by bounce mail. The value 0 means no limit is set.

e.g.: 2KB (2 Kilobytes), 3MB (3 Megabytes), 2GB (2 Gigabytes).

```
BounceMessageSizeHeader 0
```

AddXHeader

Adding X header (not in milter mode):

If the setting is YES, the queue ID and information on scan status will be included in the header of the email. For example: **X-AntiVirus: checked by AntiVir MailGate...**
The text cannot be modified.

```
AddXHeader YES
```

AddReceivedByHeader

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

If the setting is YES, the scanned email contains a note on incoming time.

```
AddReceivedByHeader YES
```

MaxHopCount

Avoiding mail loops (not in milter mode):

If more "Received:" lines appear in the header, the email is blocked.

```
MaxHopCount 100
```

ScanTimeout

Maximum time for email scanning:

Defines maximum time for email scanning, in seconds:

```
ScanTimeout 300
```

ExternalProgram

Running an external program or script when a virus/unwanted program is detected:

Calls an external program or script in case of detection. The parameter is the ID of the rejected email (see MailGate Spool Directories – Page 27).

```
ExternalProgram /path/to/program
```

NotifyEndOfLicense

Information on license expiry date:

Sends a message to postmaster, 30 days before license expiration date. The 0 value means no alert.

```
NotifyEndOfLicense 30
```

Add Precedence Header

Adding precedence header:

If the setting is YES, the following line is added in the headers:
Precedence: junk.

Programs that are set to respond automatically to incoming emails (e.g.: vacation) would not react to this report. YES and NO entries can be replaced by specific text.

```
AddPrecedenceHeader    NO
```

AddHeaderToNotice

Adding email header for postmaster:

You can add the headers of the rejected email into the warning message sent to the postmaster. The value is YES or NO.

```
AddHeaderToNotice YES
```

GUISupport

GUI support activation:
You must activate this entry in order for MailGate to communicate with the SMC GUI. Required parameters (default values):

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

If these parameters are missing or not valid, the GUI is not available.

5.3 Spam Filter Configuration (**Avira MailGate Suite** only)

A spam filter is integrated in **Avira MailGate Suite** to filter spam and other unwanted emails. The spam filter opens a connection to the spam database server for every email to check its status. You have to enable the connection on port 55555 via TCP.

The spam filter is currently available for Linux-GLIBC22 and for Solaris Sparc systems. It integrates with AntiVir MailGate through a library (libasmailgate.so).

If the spam filter is active, emails marked as "Outbreak" are blocked. All other emails are just tagged. You can read about these header entries in the MANUAL file (Paragraph "Spam and bulk").

All these options are made in avmailgate.conf.

The spam filter proxy will choose its listen port automatically on startup. Be sure you do not have firewall rules for your loopback device active! This may prevent the proxy from starting up correctly.

Options and parameters for spam filter

Enable SpamCheck

Activates/deactivates spam filter.

```
EnableSpamCheck NO
```

SpamAction

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

- TAG inserts a header line into the email. For example:
  X-AntiVirus-Spam-Check: clean (checked by Avira MailGate: version: 2.1.3-0; spam filter version: 2.0.5/0.2; host: host.your.site)
- BLOCK puts the mail into the "rejected" directory.
- NONE disables any action for spam mail.

```
SpamAction TAG
```

Dangerous Outbreak Action

Performs the set action when emails are not detected by the virus scanner, because of their recent outbreak. If the option is set to BLOCK, no email notification is sent.

```
DangerousOutbreakAction BLOCK
```

Dangerous Attachment Action

Performs the set action when the email attachment may be harmful.

```
DangerousAttachmentAction TAG
```

Dangerous IFrameAction

Performs the set action when detecting a dangerous iframe.

```
DangerousIFrameAction TAG
```

Dangerous Alert Action

Performs the set action when the spam filter classifies emails as dangerous.

```
DangerousAlertAction BLOCK
```

Dangerous Unknown Action

Performs the set action when detecting an unknown danger.

```
DangerousUnknownAction TAG
```

LibAsmailgate

Specifies the path to the spam filter library.

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

Spam Header Name

Defines the spam header to be inserted in the email header. Only the beginning can be changed (`X-Antivirus-Spam-Check`). Example:

```
SpamHeaderName X-Antivirus-Spam-Check
```

Result:

```
X-AntiVirus-Spam-Check: spam (checked by Avira
MailGate: version: 2.1.3-0;spam filter version: 2.0.5/
0.2; host: host.your.site)
```

SpamFilter Exceptions

Defines the list of exceptions for black/white lists and actions.

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

The spam filter actions can be overwritten using the file asmailgate.except. In this file you can specify email addresses and the corresponding actions. Additionally

this file can be used as a black and white list for the spam filter.

Each list consists of an address, given as regular expression. E.g.:

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

The above example treats emails from someone@somewhere.tld as spam, independently of the spam check result. "`blacklist`" is the action for the given address.

For Avira MailGate v 2.1.3, a match in this list concerns all recipients even if the mail was sent to recipients that are not listed. E. g. (in asmailgate.except*):*

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

If Avira MailGate processes a mail to someone@somewhere.tld _and_abc@def.tld and the mail was rated as spam, abc@def.tld will not receive the mail since it was blocked due to the rule for someone@somewhere.tld. This behavior will be changed in a further release.

Actions:

Actions overwrite the settings for the spam filter in avmailgate.conf (except for white and black lists). Several actions can be specified for each address:

- `blacklist` - Treat mail as spam
- `whitelist` - Treat mail as clean
- `block_spam` - If the mail is spam, block it
- `block_dangerous_attachment` - If the mail has a dangerous attachment, block it
- `block_dangerous_alert` - If the mail contains a dangerous alert, block it
- `block_dangerous_iframe` - If the mail contains a dangerous iframe, block it
- `tag_spam` - If the mail is spam, tag it
- `tag_dangerous_attachment` - If the mail has a dangerous attachment, tag it
- `tag_dangerous_alert` - If the mail contains a dangerous alert, tag it
- `tag_dangerous_iframe` - If the mail contains a dangerous iframe, tag it

Example of /etc/asmailgate.except:

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

All mail from spam@somewhere.tld will be treated as spam, independently of the spam check result.

Actions can also be switched off. **Example**:

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

Do not block spam for the given recipient address.

"`r`" is the flag for recipient. It means that the given address should be matched against the recipient address and not against the sender address.

The default (without the "`r`" flag) is to match the address against the sender address.

Another **example**:

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

Don't tag DangerousAttachment and DangerousIFrame mails.

A "DangerousOutbreak" has a higher priority than the black- and whitelisting. If a "DangerousOutbreak" was detected, no check for black- and whitelistings will be performed.

SpamFilter DetectGTUBE

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

An email containing this string should be rated as **spam** by spam filters. Just put this string into the message's body and send it through Avira MailGate. If you get messages similar to the ones below, the spam filter works correctly:

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

GTUBE will not be detected by default. To switch the GTUBE detection on, set this option to YES and restart Avira MailGate.

```
SpamFilterDetectGTUBE NO
```

SpamFilter Startup Timeout

This option specifies how long should Avira MailGate wait for the external spam daemon to come up (in seconds).

```
SpamFilterStartupTimeout 60
```

SpamFilter ServiceConnect Timeout

This option specifies how long should Avira MailGate wait for an answer of a configuration request to the external spam filter daemon (in seconds).

```
SpamFilterServiceConnectTimeout 30
```

SpamFilter ServiceMax Sessions

This option sets the maximum limit of simultaneous running threads of the external spam filter daemon.

```
SpamFilterServiceMaxSessions 50
```

SpamFilter HandleBulk ADVLikeSpam

Option to rate category bulk advertisement as spam.

```
SpamFilterHandleBulkADVLikeSpam NO
```

SpamFilter HandleBulk PornLikeSpam

Option to rate category bulk porn as spam.

```
SpamFilterHandleBulkPornLikeSpam NO
```

SpamFilter ModifySubject

Inserts the spam check result into the "Subject:" header line:
Subject: [spamcheck: spam] this is the original subject text

This is the default message.It can be overridden using a template: "spamfilter-subjects". This template allows you to specify a string for each spam check result. The string for the corresponding spam check result will be used as a replacement for the "Subject:" header line.

A sample template is installed to /usr/lib/AntiVir/templates/examples. Please see the MANUAL for details.

```
SpamFilterModifySubject NO
```

SpamFilter CheckFailed Keep

Re-queue a mail if the spam check failed. The mail will be put back in the queue to be reprocessed later. It will be reprocessed as long as the error persists. At the moment you can't enforce the delivery of a mail that is stuck in the queue.

```
SpamFilterCheckFailedKeep NO
```

OpenMax

Specifies the maximum number of opened files for the Avira MailGate processes. The default value will only be set if the current system value is lower than the default.

```
OpenMax 1024
```

DBSupport

If this option is enabled, MailGate writes statistics into a database. The database consists in two tables: alerts (logs information about each malware alert) and counter (logs the number of different emails processed by MailGate).

Please refer to /usr/lib/AntiVir/MANUAL.avmailgate for more information about the **database support**.

```
DBSupport NO
```

DBodbcIni

If `DBSupport` is active, the ODBC driver manager will use the specified odbc.ini. Default: the installed ODBC driver manager decides which odbc.ini file it loads.

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

DBodbcLib

If `DBSupport` is active, MailGate will load the specified library and use it as the ODBC driver manager. Default: loads one of the following libraries from the default library path in this order: libodbc.so.1, libodbc.so, libiodbc.so

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

DBodbcData Source

If `DBSupport` is active, it connects to the given database source.

```
DBodbcDataSource MailGate
```

DBUpdate Delay

If `DBSupport` is active, it waits for a given interval, before writing the next summed up counters to the database. You can specify the delay in seconds, minutes and hours. Default: write counters to database every full hour.

```
DBUpdateDelay 1h
```

5.4 Scanner Configuration in avmailgate-scanner.conf

A new configuration file has been introduced, starting with MailGate v 3.0.0: avmailgate-scanner.conf. It contains configuration options specific to the new scanner backend. Usually, you don't have to change the options in this file, but there might be a few exceptions.

User, Group

If you change one of these options, you have to make sure that the files avmailgate-scanner.conf and avmailgate.conf contain the same values for these options.

You also have to adapt avmailgate-scanner.conf if you updated from a previous MailGate version (< 3.0.0) and the current settings for `User/Group` differ from the default settings. Defaults:

```
User uucp
Group antivir
```

There are some other changes needed when changing `User/Group`:

In /etc/avmailgate-scanner.conf:

- Change the owner/group of the path given with `ListenAddress` (The option consists of a path and a socket file. Don't forget to stop MailGate before making any changes. If the socket file exists, delete it and only change the owner/group of the directory.)

When changing the user and/or group here, you must also change the options `User` *and* `Group` *in MailGate's configuration file (*/etc/avmailgate.conf*).*

- Adapt the option `SocketPermissions` to the new user/group. See syntax below.

In /etc/avmailgate.conf:

- Change the option `User/Group`
- Change the owner/group of the directory and its sub directories given with `SpoolDir` (default: /var/spool/avmailgate).

Socket Permissions

The owner and permissions of the scanner backend's socket. The scanner backend must run as the same user as MailGate runs.

```
SocketPermissions 0600
```

ListenAddress

ListenAddress (in avmailgate-scanner.conf) and ScannerListenAddress (in avmailgate.conf) specify how the scanner backend can be reached. Both options must point to the same path (the string "unix:" must not be used with the option ScannerListenAddress):

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

In /etc/avmailgate.conf:

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

UseSavapi Proxy

To make scanning processes more efficient, you can use a given pool of scanners. Please note that too many scanners would overload the computer, while too few

would cause unnecessary waiting for applications. Values: 0 or 1. Default:

```
UseSavapiProxy 0
```

PoolScanners

The number of AntiVir scanners set in the pool. Default:

```
PoolScanners 24
```

Pool Connections

The maximum number of simultaneous connections MailGate allows to the scanner pool. Default:

```
PoolConnections 128
```

Syslog Facility

It sets the log category that Syslog should apply for Scanner messages.

```
SyslogFacility mail
```

ReportLevel

The scanner can be set to log on different levels:

- 0 - Log errors
- 1 - Log errors and alerts
- 2 - Log errors, alerts and warnings
- 3 - Log errors, alerts, warnings and debug messages

"alerts" means information about potential malicious code.

Default:

```
ReportLevel 0
```

ScanTemp

The directory used by the scanner to store temporary files, such as unpacked archives, or locked files.

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

If you want to use a single tmp directory for all MailGate components, you can change the option `TemporaryDir` *in* /etc/avmailgate.conf, *and* `ScanTemp` *in* avmailgate-scanner.conf.

Default:

```
ScanTemp /var/tmp
```

LogFileName

Path to the scanner logfile.

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

5.5 Hosts Configuration in avmailgate.acl

Using `local` and `relay` as key words, avmailgate.acl decides which computer is allowed to send emails via AntiVir MailGate. This is established via the sender's or recipient's domain or IP address.

▶ Set the local hosts and/or domains. For example:

```
local: localhost
```

```
local: avira.com
```

▶ Set which hosts and networks may send emails. For example:

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

IP addresses

You can specify IP addresses in various ways:

```
192.168.0.0/16 or 192.168
```

Both have the same meaning. /16 means 16 bit and signifies the first two numbers of the IP address. Therefore, all IP addresses starting with 192.168 are allowed.

Example for /etc/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
```

5.6 Warnings Configuration in avmailgate.warn

Optionally, you can use another file to set the warning messages: /etc/avmailgate.warn. Beside avmailgate.conf, this file controls the alert emails sent to the recipient, sender and postmaster.

A command for this file contains two entries:

- first, the name of the detected virus/unwanted program and it may contain wildcards;
- the second is one or more of the following letters:

 - S: for sender
 - R: for recipient
 - P: for postmaster

Example

The command

```
/klez/ RP
```

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

The settings in avmailgate.warn *will overrule those made in* avmailgate.conf *in the event of specific virus/unwanted program detection.*

5.7 Report Templates Configuration

You can set some report texts as email notifications in the event of virus/unwanted program or suspicious file detection.

- ▶ Copy the example templates in the required language from the templates directory /usr/lib/AntiVir/templates/examples/<language>/ in the directory /usr/lib/AntiVir/templates.
- ▶ Change the directory to /usr/lib/AntiVir/templates. This directory contains the following files:
  patho-administrator
  patho-recipient
  patho-sender
  alert-administrator
  alert-recipient
  alert-sender
- ▶ Write the texts you need in the files listed above. Keep the file structure:
  - the first line is the email subject;
  - an empty line follows (new line);
  - then the text of the email.

Keywords

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

Keyword	**Text**
SENDER	The email address of the infected email sender.
ALERTS	The list of viruses/unwanted programs found in the email. Every line contains a virus name, and the prefix and postfix are repeated.
REASON	The reason for not scanning an email (short sentence).
ADVICE	Advice on problem-solving (~1 line, see REASON)
QUEUEID	Email ID in Avira AntiVir MailGate queue.
SUBJECT	Subject of infected email.
CONCERNING_ FILE_NAMES	Will be replaced with a list of files in which the alerts were detected.
PRODUCT_ VERSION	Product version number.
ENGINE_ VERSION	Scan engine version number.
VDF_VERSION	VDF version number.
VDF_DATE	VDF creation date.

Example for alert-sender

```
SUBJECT: AntiVir ALARM [Your email: "SUBJECT"]
**********AntiVir ALARM**********
AntiVir has discovered the following in the email sent
from your address:
                    ALERTS
This email has not been sent, but isolated on your
server. Please scan your system immediately for possible
virus infection.
Clean your system before sending any more email
messages.
```

5.8 Updater Configuration in avupdate.conf

Updates ensure that AntiVir MailGate components (MailGate, scanner, VDF and engine), which provide security against viruses or unwanted programs, are always kept up to date.

With Avira Updater you can update Avira software on your computers, using Avira update servers.

To configure the update process, use the options in /etc/avira/avupdate.conf described below. All parameters from avupdate.conf can be passed to the Updater via command line. For example:

- parameter in avupdate.conf:

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

- command line:

```
/usr/lib/AntiVir/avupdate.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
```

master-file — Specifies the master.idx file.

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

install-dir — Specifies the installation directory for updated product files.

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

temp-dir — Temporary directory for downloading update files.

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

Setting update email reports

All reports on AntiVir updates are sent to the email address given in avupdate.conf:

mailer — Emails can be sent via `smtp` engine or using `sendmail`:

```
mailer=
```

smtp... — Authentication for smtp connection. Activate the `auth-method` option and then provide the smtp server, port, user and password.

```
auth-method=password
smtp-user=<your_username>
smtp-password=<your_password>
smtp-server=<servername>
smtp-port=<port>
```

notify-when — There are three situations to set for email notifications:

- 0 - no email notifications are sent,

- 1 - email notifications are sent in case of "successful update", "unsuccessful update", or "up to date".
- 2 - email notification only in case of "unsuccessful update".
- 3 - email notification only in case of "successful update" (default).

```
notify-when=
```

email-to The recipient of notification emails.

```
email-to=
```

Logfile settings

log Specify a full path with a filename to which AntiVir Updater will write its log messages.

```
log=/var/log/avupdate.log
```

log-append By default, the logfile is overwritten. You can use this option to append the logfile.

```
log-append
```

Integration into Avira Security Management Center (SMC)

In order to configure updates via Avira Security Management Center (SMC), it is necessary to add the updateplugin package to the SMC repository. Once added, a new product "Avira Updater" will be available for installation on machines administered by the SMC.

The "Avira Updater" product allows updates to be configured for all products installed on computers administered by the SMC. For more details, please refer to the SMC documentation.

6 Operation

After concluding installation and configuration and when AntiVir MailGate is running, MailGate guarantees continuous monitoring of your system. During operation you might have to make occasional changes in settings, as described in Configuration – Page 26.

In some cases, it may be necessary to operate AntiVir MailGate manually or to process the emails filtered by AntiVir MailGate manually.

This Chapter describes:

- Starting and Stopping AntiVir MailGate Manually – Page 53
- Parameters for SMTP and Scanner Daemon – Page 55
- Queue Manager avq – Page 56

In addition, you will find information on:

- Procedures when Detecting Viruses/Unwanted Programs – Page 59

6.1 Starting and Stopping AntiVir MailGate Manually

If you have installed AntiVir MailGate as described in Installation – Page 14, the program is automatically started and stopped by the system.

However, you may need to start and stop AntiVir MailGate manually. Any changes in configuration files must be followed by a restart of the program, for activation.

The script /usr/lib/AntiVir/avmailgate starts and stops the scanner and mailgate daemon.

Since version 3.0.0, MailGate uses a new scanner, which must be started before avmailgate.bin. Therefore, you have to start and stop MailGate with the avmailgate script:

```
/usr/lib/AntiVir/avmailgate start
/usr/lib/AntiVir/avmailgate stop
```

If you use your own script, you should make sure to start the scanner first. See the script "avmailgate" for an example on how you can start the scanner backend.

If you want to pass specific command line options to MailGate, you can add them to the parameter "DAEMONPARAMS" in the script (see Parameters for avmailgate.bin).

You must login as **root** *or you must have the required access rights to start or stop AntiVir MailGate manually.*

Starting AntiVir MailGate

▶ Type:

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

↳ The program starts with the following message:

```
Starting AVIRA AntiVir MailGate...
Starting savapi
```

Stopping AntiVir MailGate

▶ Type:

```
/usr/lib/AntiVir/avmailgate stop
```

↳ The program stops with the following message:

```
Stopping AVIRA AntiVir MailGate...
Stopping: avmailgate.bin
Shutting down Avira MailGate...
Stopping: savapi
```

Restarting AntiVir MailGate

This is used, for example, after making changes in configuration scripts.

▶ Type:

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

↳ The program restarts after showing the following message:

```
Stopping AVIRA AntiVir MailGate...
Stopping: avmailgate.bin
Shutting down Avira MailGate...
Stopping: savapi

Starting AVIRA AntiVir MailGate...
Starting savapi
```

Checking AntiVir MailGate status

▶ Type:

```
/usr/lib/AntiVir/avmailgate status
```

↳ The program shows information on the MailGate daemons:

```
Status: avmailgate.bin running
Status: savapi running
```

6.2 Parameters for SMTP and Scanner Daemon

The following tables describe the possible command line parameters that overrule avmailgate.conf settings.

Syntax:

```
avmailgate.bin [-V|--version] [-i] [-C config-file] [-D
debug-level] [--stop] [--status] [--avq]
```

Parameters for avmailgate.bin

Parameter	Description
`-V or --version`	Displays the version number
`-C config-file`	Defines an alternative configuration file instead of /etc/avmailgate.conf If you specify `-C`, you have to specify `-C` for `--stop` and `--status` too.
`-A acl-file`	Defines an alternative acl file instead of the default /etc/avmailgate.acl
`-i`	The SMTP daemon runs in inetd mode with SMTP conversation via stdin and stdout. For more information, see inetd(8).
`-p port`	Defines the port on which SMTP daemon is listening instead of the normal SMTP port (25).

Another possibility is to add the parameters `-C`, `-A` *and* `-p` *to the variable DAEMONPARAMS="" in the start/stop script* ***/usr/lib/AntiVir/avmailgate***.

The following options are used during debugging:

Parameter	Description
`-D debug-level`	Sets debug level (small integer, 1-5, 5 is most detailed).
`-R remote.host`	Defines the remote host domain name (default: `-i`)
`-r remote-ip-addr`	Defines the remote host IP address (aaa.bbb.ccc.ddd) (default: `-i`)
`-q port`	Defines the remote host TCP port
`--avq`	Calls the queue manager.

6.3 Queue Manager avq

The Queue Manager avq is integrated in avmailgate.bin. The Queue Manager enables manipulation of the AntiVir MailGate spool directory /var/spool/avmailgate/ and its sub-directories. Here you can see and modify the status of the pending emails (see MailGate Spool Directories – Page 27).

Email status in queue

▶ Type:

```
/usr/lib/AntiVir/avmailgate.bin --avq
```

↳ The status for all emails in the queue is displayed.

In the first row you will see the name of the displayed queue. For example:
`Queue: rejected`.

At the end of the list, you will see the number of emails in the queue:
`5 mails in the rejected queue`.

The Queue Manager shows the following status information for the emails:

- `--> Not processed yet`
- `--> OK`
- `--> MIME problem` (Recursion too deep etc.)
- `--> Found e.g. (1x) Eicar Test Signature (type: virus)`

The following status information is displayed, according to the spam filter results (see Report Templates Configuration – Page 48):

- `--> Outbreak detected`
- `--> Dangerous attachment found`
- `--> Dangerous iframe found`
- `--> Dangerous alert found`
- `--> Spam`

You can control the outcome with the following parameters after `--avq` (the Help provides more parameters, which you can call with `--avq --help`).

You can apply the following parameters to the outcome:

Parameter	Description
`--queue=incoming`	Lists the emails in the incoming queue
`--queue=outgoing`	Lists the emails in the outgoing queue
`--list=all`	Lists all queues

`--type=<type>`	Lists all rejected emails of the specific type.
	Other types can be:
	`spam`
	`mal` (malicious mails)
	`dangerous_attachment`
	`dangerous_iframe`
	`dangerous_alert`
	`dangerous_outbreak`
	`alert` (types like worm, virus etc.)

`--type=<notype>`	Lists all rejected emails, except the one specified, if it has the prefix "no": `nospam, nomal`, etc.
`--nosort`	Switches off the sorting. By default, the queue listing is sorted by date (according to the internal timestamp of the queue file), with the newest email in the last position.

Deleting emails from queue

Deleting emails from the queue is important in the event of infected emails. Forwarded emails are automatically deleted from the queue.

You have to delete the emails from the **rejected** *queue manually.*

To delete denied emails immediately, you can use the option `ExternalProgram` *in* avmailgate.conf. *For example:*

```
ExternalProgram /usr/lib/AntiVir/rm_rejected.sh

rm_rejected.sh:
#!/bin/sh
/usr/lib/AntiVir/avmailgate.bin --avq --remove=$1
```

▶ Find out the ID of the email. AntiVir MailGate indicates the ID of the email in its logs and in the email sent to the postmaster.

▶ Type the command (where <ID> is the ID of the infected email):

```
/usr/lib/AntiVir/avmailgate.bin --avq --remove=<ID>
```

↳ The email is deleted from the queue.

You can use the following parameters when deleting:

Parameter	Description
--remove=<ID>	Deletes the email with the given ID.
--remove=all	Deletes all emails. Before deleting, an alert appears to confirm the action.
--flush	Immediately empties the incoming and outgoing queue.

Forcing email forwarding

This procedure may forward potentially dangerous viruses.

▶ Always check which email is going to be forwarded.

▶ Find out the ID of the email. AntiVir MailGate indicates the ID of the infected email in its logs and in the email sent to the postmaster.

▶ Type the command (where <ID> is the ID of the infected email):

```
/usr/lib/AntiVir/avmailgate.bin --avq --deliver=<ID>
```

↳ The email is delivered, whatever the virus scanner reports, and it is deleted from the queue.

6.4 Procedures when Detecting Viruses/Unwanted Programs

If configured correctly, AntiVir MailGate has already automatically carried out all important antivirus tasks on your system:

- Infected emails are not forwarded.
- Infected emails are moved to /var/spool/avmailgate/rejected (or to another directory, specified in avmailgate.conf), where data file (df-) and control file (vf- or mf -) are located. For further information, see MailGate Spool Directories – Page 27.
- Data files can contain emails in which viruses/unwanted programs were detected. These can be directly deleted, together with the control file, or they can be handled using the Queue Manager (--avq).
- According to the avmailgate.conf settings, postmaster can send alerts to senders and/or recipients of infected emails.
- According to the avmailgate.conf settings, infected files can be further processed by external programs or scripts.

These procedures avoid the danger of spreading infection.

You should always perform the following steps:

▶ Try to detect the way the virus/unwanted program infiltrated your system.

▶ Perform targeted scanning on the data storage supports used.

▶ Inform your team, superiors or partners.

▶ Inform your system administrator and security provider.

Submit Infected Files to Avira GmbH

▶ Please send us the viruses, unwanted programs and suspicious files that our product does not yet recognize or detect. Send us the virus or unwanted program packed in an archive (PGP, gzip, WinZIP, PKZip, Arj), attached to an email message, to virus@avira.com.

When packing, use the password **virus**. *In this way, the file will not be deleted by virus scanners on an email gateway.*

7 Updates

With Avira Updater you can update Avira software on your computers, using Avira update servers. The program can be configured either by editing the configuration file (see 5.8 Updater Configuration in avupdate.conf), or by using parameters in the command line.

It is recommended to run the Updater as **root**. If the Updater does not run as **root**, it does not have the necessary rights to restart AntiVir daemons, so the restart has to be made manually, as **root**.

Advantage: any running processes of AntiVir daemons (such as Scanner, Engine, MailGate) are automatically updated with the current antivirus files, without interrupting the running scan processes. It is thus ensured that all files are scanned.

7.1 Internet Updates

Manually

If you want to update AntiVir MailGate or some of its components:

▶ Use the command:

```
/usr/lib/AntiVir/avupdate --product=[product]
```

As `[product]`, you can use:

- `Signatures` - to update only the vdf files.
- `Engine` - to update the engine and the vdf files.
- `Scanner` - (recommended) to update the scanner, engine and vdf files.
- `MailGate` - complete update (MailGate, scanner, engine and vdf files).

If you just want to check for a new AntiVir version without updating AntiVir:

▶ Use the command:

```
/usr/lib/AntiVir/avupdate --check --product=[product]
```

The `[product]` values are the same as above.

Automatic updates with cron daemon

Regular updates are made using cron daemon.

The settings for automatic updates in /etc/crontab **have already been made if**, when installing Avira AntiVir MailGate with the install script, the answer for installing AntiVir Updater and starting it automatically was `yes`.

You can find further information on cron daemon in your UNIX documentation.

To make or change the settings for automatic updates in crontab manually:

▶ Add or edit the entry in /etc/crontab, similar to the example below.

Example: for an hourly update at *:23, enter the following command:
`23 * * * * root /usr/lib/AntiVir/avupdate --product=[product]`

As `[product]`, you can use:
- `Signatures` - to update only the vdf files.
- `Engine` - to update the engine and the vdf files.
- `Scanner` - (recommended) to update the scanner, engine and vdf files.
- `MailGate` - complete update (MailGate, scanner, engine and vdf files).

▶ Start the update process to test the settings:

```
/usr/lib/AntiVir/avupdate --product=[product]
```

where `[product]` takes the same values as above.

↳ If successful, a report will appear in the logfile /var/log/avupdate.log

8 Service

8.1 Support

Support Service

Our website http://www.avira.com contains all the necessary information on our extensive support service.

The expertise and experience of our developers is available to you. The experts from Avira answer your questions and help you with difficult technical problems.

During the first 30 days after you have purchased a license, you can use our **AntiVir Installation Support** by phone, email or by online form.

In addition, we recommend that you also purchase our **AntiVir Classic Support**, with which you can contact and obtain advice from our experts during business hours when technical problems are encountered. The annual fee for this service, which includes eliminating viruses and hoax support, is 20% of the list price of your purchased AntiVir program.

Another optional service is the **AntiVir Premium Support** which, in addition to the scope of the AntiVir Classic Support, allows you to contact expert partners at any time - even after business hours in the case of an emergency. When virus alerts occur, you will receive an SMS on your cellphone.

Forum FAQ

Before you contact our Hotline, we recommend that you visit our user forum at http://forum.antivir.de, as well as the FAQ section on our website.
Your questions may already have been answered for another user and posted on the forum.

Email Support

Support via email can be obtained at http://www.avira.com.

8.2 Online Shop

Would you like to buy our products by mouse-click?

You can visit the Avira Online Shop at http://www.avira.com and buy, upgrade or extend AntiVir licenses quickly and safely. The Online Shop guides you step by step through the order menu. A **multi-lingual Customer Care Center** explains the order process, payment transactions and delivery. Resellers can order by invoice and use a reseller panel.

8.3 Contact

Address
Avira GmbH
Lindauer Strasse 21
D-88069 Tettnang
Germany

Internet
You can find further information on us and our products by visiting http://www.avira.com.

9 Appendix

9.1 Glossary

Term	Meaning
cron (daemon)	A daemon which starts other programs at specified times.
Daemon	A background process for administration on UNIX systems. On average, there are about a dozen daemons running on a computer. These processes usually start up and shut down with the computer.
Demo version	Without a license file, Avira AntiVir MailGate runs as a demo version. An Avira banner is inserted in every email. The automatic update function is not available, so you will have to download new virus definitions and scan engine versions manually from our website.
Eicar	The European Institute for Computer Antivirus Research offers a test virus for testing antivirus programs. More details at: http://www.eicar.org
Logfile	also: Report file. A file containing reports generated by the program during run-time when a certain event occurs.
Malware	Generic term for "foreign bodies" of any type. These can be interferences such as viruses or other software, which the user generally considers as unwanted (see also Unwanted Programs).
MIME	Multipurpose Internet Mail Extensions: Internet extensions for integrating binary files in Internet emails. MIME supports so-called multipart emails, to allow various file types in an email or binary attachments and HTML emails.
MTA	Mail Transfer Agent: a program that sends emails via SMTP. For example, Sendmail, Postfix, Exim.
Quarantine directory	The directory where infected files are stored to block the user's access to them. (for example, rejected)
root	The user with unlimited access rights (such as system administrator on Windows)
Scan engine	AntiVir software module, which controls the search for viruses and unwanted programs.
SAVAPI	Secure AntiVirus Application Programming Interface
Script	A text file containing commands to be executed in UNIX (similar to batch files in DOS).
SMTP	Simple Mail Transfer Protocol: protocol for email communication on the Internet.

Term	Meaning
syslog daemon	A daemon used by programs for logging various information. These reports are written in different logfiles. The syslog daemon configuration is in /etc/antivir.conf.
Unwanted programs	The name for programs that do not directly harm the computer, but are not wanted by the user or administrator or have been installed without their consent. These can be backdoors (BDC), dialers, jokes and games.
VDF (Virus Definition File)	A file with known signatures for viruses and unwanted programs. In many cases it is sufficient for an update to load the most recent version of this file.

9.2 Further Information

You can find further information on viruses, worms, macro viruses and other unwanted programs at http://www.avira.com .

9.3 Golden Rules for Protection Against Viruses

- Always keep boot floppy disks for your network server and for your workstations.
- Always remove floppy disks from the drive after finishing work. Even if they have no executable programs, disks can contain program code in the boot sector and these can serve to carry boot sector viruses.
- Regularly back up your files.
- Limit program exchange: particularly with other networks, mailboxes, Internet and acquaintances.
- Scan new programs before installation and the disk after this. If the program is archived, you can detect a virus only after unpacking and during installation.

If there are other users connected to your computer, you should set the following rules for protection against viruses:

- Use a test computer to check downloads of new software, demo versions or virus-suspicious media (floppies, CD-R, CD-RW, removable drives).
- Disconnect the test computer from the network!
- Appoint a person responsible for virus infection operations and define all steps for virus elimination.
- Draw up an emergency plan as a precaution for preventing damage due to destruction, theft, failure or loss/change due to incompatibility. You can replace programs and storage devices, but not your vital business data.
- Draw up a plan for data protection and recovery.
- Your network must be correctly configured and the access rights must be wisely assigned. This is represents good protection against viruses.

Avira AntiVir MailGate | Avira AntiVir MailGate Suite

Avira GmbH

Lindauer Str. 21
88069 Tettnang
Germany
Telephone: +49 (0) 7542-500 0
Fax: +49 (0) 7542-525 10
Internet: http://www.avira.com

© Avira GmbH. All rights reserved.

This manual was created with great care. However, errors in design and contents cannot be excluded. The reproduction of this publication or parts thereof in any form is prohibited without previous written consent from Avira GmbH.

Errors and technical subject to change.

Issued Q1-2009

AntiVir® is a registered trademark of the Avira GmbH.
All other brand and product names are trademarks or registered trademarks of their respective owners. Protected trademarks are not marked as such in this manual. However, this does not mean that they may be used freely.