

Avira **AntiVir** MailGate

Support
August 2010



www.avira.com

Errors in design and contents cannot be excluded
© Avira GmbH

Contents

- 1 Installation 3**
 - 1.1 The installation package 3
 - 1.2 Tips for the Installation..... 4
 - 1.3 Installation options 5
- 2 MailGate in action..... 6**
 - 2.1 MailGate in connection with postfix..... 6
 - 2.2 MailGate in connection with Sendmail 7
 - 2.3 MailGate in connection with Avira AntiSpam..... 8
 - 2.4 MailGate in connection with further MTAs..... 8
- 3 MailGate Suite in Action 9**
 - 3.1 Characteristics of the MailGate Suite..... 9
- 4 Best practices 9**
 - 4.1 Logging..... 9
 - 4.2 Configuration10
 - 4.3 Updates12

1 Installation

1.1 The installation package

You find the current installation package for Avira AntiVir MailGate on our website:

http://www.avira.de/de/downloads/avira_antivir_mailgate.html

Please, decompress the installation package:

```
$ gzip -cd antivir-mailgate-prof.tgz | tar xvf
```

The directory contains important directories and files which are described in the following.

```
$ cd antivir-mailgate-prof-<Version>
```

```
antivir-mailgate-prof-3.0.0-7-0 #
```

```
.installrc  
LICENSE  
LICENSE.DE  
README  
bin  
contrib  
doc  
etc  
install  
legal  
pgp  
script  
smcpgk  
templates  
vdf
```

The installation directory is structured as follows:

Install	- Main installation script
.installrc	- Product information file
LICENSE	- Avira GmbH Software License Agreement
doc/RELEASE_NOTES	- important changes in this version
README	- Description installation package
doc/	- Documentations
pgp/	- PGP key and instructions
bin/	- Executable files
vdf/	- Basic virus definitions
legal/	- License agreement for 3 rd party parts
etc/	- Configuration files
script/	- Shell Scripts
smcpkg/	- SMC-specific files
templates/	- Applied Templates
contrib/	- 3rd-Party Software

1.2 Tips for the Installation

You can start the command line related, interactive default installation as follows:

```
$ ./install
```

In case you have already executed an installation before, you can accelerate the installation:

```
$ ./install --fast
```

Unattended Installation

If you want to proceed a completely automatic (unattended) installation, you can use the installation type of the SMC:

```
$ ./install --fast --inf=./smcpkg/setup.inf
```

All settings for the automatic installation are located in the given INF file. You could use a copy of your own settings and e.g. proceed a larger rollout or simplify your daily work.

./smcpkg/setup.inf:

```
SAVAPI3_ADDLINK=y
MAILGATE_ADDLINK=y
MAILGATE_AUTOSTART=y
MAILGATE_MANPAGESDIR=" "
MAILGATE_LOCALACL="`hostname -f` `hostname -d`"
MAILGATE_RELAYACL="127.0.0.1/8 192.168.0.0/16"
UPDATER_INSTALL=y
UPDATER_ADDLINK=y
UPDATER_ADDCRONJOB=y
UPDATER_CYCLE_SIG_EN=2h
UPDATER_CYCLE_PROD=y
UPDATER_CYCLE=2
UPDATER_EMAILTO=n
SMC_INSTALL=1
ANTIVIR_CONFIG=n
LICENSE_AGREEMENT=y
```

Default installation

During the installation you receive questions concerning the basic configuration. You can use the default values without hesitation.

1.3 Installation options

MailGate is a mail server service with an own queue management. It can communicate with other mail servers (MTAs) via the SMTP protocol. Therefore there is a multitude of possible combinations. In a lot of cases MailGate works as a simple mail relay with integrated filter functions.

There are two special installation options, which allow a direct integration into an existing mail server.

Postfix Content-Filter
Sendmail Milter

The combination with postfix has proven itself in most customer cases. Sendmail is used in more special cases and first of all on Unix system like solaris.

Which option should be used in which cases?

Both options can be adjusted very easily to different hardware types. They are used in small networks but also in large enterprises. The respective MTA keeps the main tasks concerning the mail traffic. MailGate is integrated via a redirection which is able to move threats into the quarantine or to block them directly (via sendmail milter).

The big advantage is that all options which are usually offered by the MTA (SMTP-AUTH etc.) are maintained. But the functions of MailGate are limited to the basic commands of the SMTP protocol.

MailGate „Standalone“ as Relay

The classic option – MailGate as simple mail relay – can be very interesting in large enterprises as the mail structures in large enterprises can be quite complex.

Circumstances like the administration of subsidiaries, the need for a good availability and redundancies require several installations of MailGate. So the administrative effort increases. Therefore MailGate should be used as a central relay, e.g. in a company-wide DMZ.

An example:

Internet → external MX → Firewall → MailGate (DMZ) → Firewall
→ internal mail relay → internal infrastructure

2 MailGate in action

2.1 MailGate in connection with postfix

MailGate in front of Postfix

The possibility to use MailGate as a local relay in front of postfix is quite rarely used but easily to configure.

Procedure for this configuration:

Internet → MailGate → Postfix → another MTA / Client (MUA)

You find a detailed installation description of this configuration options in the MailGate Manual on page 30 (supervise port 25)

MailGate as Content Filter

MailGate can be used in connection with postfix as a so-called content filer. This constellation is the most frequent solution among our customers. An installation is relatively easy. Usually postfix already contains the support for content filter.

Procedure for this configuration:

Internet → Postfix →[REDIRECTION]→ MailGate →[FORWARD]→
→ Postfix Backdoor → another MTA / Client (MUA)



In the main configuration of postfix (main.cf) only the entry for the content filter (the redirection) is entered:

"antivir" = Port 10024

/etc/postfix/main.cf:

```
content_filter=smtpl:localhost:10024
```

In the following a further TCP socket is defined. On this TCP socket the known mail server service "smtpd" shall listen. Thereby it is important that the definition for the content filter which was valid before is reset so that no mail loop is generated.

"smtp-backdoor" = Port 10025

/etc/postfix/master.cf:

```
localhost:10025 inet n - n - - smtpd -o content_filter=  
Postfix should be rebooted afterwards so that the new configuration is active. Now the configuration in postfix is done.
```

The MailGate configuration is also very simple.

/etc/avmailgate.conf:

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

Afterwards a reboot of MailGate is necessary in order to assume the configuration.

2.2 MailGate in connection with Sendmail

An interesting option is the integration via sendmail milter interface.

Procedure for this configuration:

```
Internet  
|  
Sendmail ↔ [MILTER] ↔ MailGate  
|  
further MTA / Client (MUA)
```

Tip: This option allows you to check an email directly in the SMTP dialogue. In case of a detection the email can be rejected directly. That means a direct "REJECT" is possible.

You find detailed installation instructions in the MailGate manual from page 15 on.

2.3 MailGate in connection with Avira AntiSpam

The in-house solution of Avira AntiSpam can be ideally combined with MailGate and offers an effective protection against the daily spam flood.

A combination is possible as:

- extended content filter
- stand alone of both products

2.4 MailGate in connection with further MTAs

MailGate can communicate with every mail server which speaks SMTP in an RFC-conform way.

Typical combinations are:

- MailGate + Exim
- MailGate + Qmail
- MailGate + Exchange

In order to combine MailGate with one of these MTAs, MailGate should be configured for a standalone (relay) operation.

Procedure examples for this configuration:

Internet → MailGate → Exim → further MTA / Client (MUA)

Internet → MailGate → Exchange → Client (MUA)

3 MailGate Suite in Action

3.1 Characteristics of the MailGate Suite

The MailGate suite can be purchased as license upgrade to the usual MailGate license. It is the same product. Additional functions are activated by the license upgrade.

The Avira AntiVir MailGate Suite offers an additional AntiSpam solution.

If you want to use the MailGate Suite functionalities only a new key file has to be installed, which activates the MailGate Suite. Afterwards you can activate the AntiSpam option in the `/etc/avmailgate.conf`.

We recommend you to use the MailGate Suite as the first instance in the internal or external mail infrastructure.

Example procedure for this configuration:

```
Internet → MailGate Suite → further MTA / Client (MUA)
```

4 Best practices

4.1 Logging

All log files are written into the syslog or into a special log file. MailGate doesn't have a limitation for the maximum size of the log file.

On Linux and Unix systems tools like "logrotate" have been developed which rotate automatically depending on the values which you have configured.

4.2 Configuration

We recommend you the following extended settings:

MailGate (without AntiSpam)

/etc/avmailgate.conf:

MatchMailAddressForLocal	BOTH
LogFile	/var/log/avmailgate.log
MaxIncomingConnections	1024
ScanInArchive	YES
ArchiveMaxSize	128MB
ArchiveMaxRatio	150
ArchiveMaxRecursion	20
BlockSuspiciousArchive	YES
BlockUnsupportedArchive	YES
BlockEncryptedArchive	NO
BlockOnError	NO
ExposePostmasterAlerts	YES
ExposeRecipientAlerts	LOCAL
ExposeSenderAlerts	LOCAL
HeuristicsMacro	
HeuristicsLevel	3
DetectADSPY	yes
DetectAPPL	no
DetectBDC	yes
DetectDIAL	yes
DetectGAME	no
DetectHIDDENEXT	yes
DetectJOKE	no
DetectPCK	yes
DetectPHISH	yes
DetectSPR	no
AddXHeader	YES
AddReceivedByHeader	YES
OpenMax	2048

MailGate Suite (with AntiSpam)

/etc/avmailgate.conf:

```
MatchMailAddressForLocal      BOTH
LogFile                        /var/log/avmailgate.log
MaxIncomingConnections         1024
ScanInArchive                  YES
ArchiveMaxSize                 128MB
ArchiveMaxRatio                150
ArchiveMaxRecursion            20
BlockSuspiciousArchive         YES
BlockUnsupportedArchive        YES
BlockEncryptedArchive          NO
BlockOnError                   NO

ExposePostmasterAlerts        YES
ExposeRecipientAlerts         LOCAL
ExposeSenderAlerts            LOCAL

HeuristicsMacro
HeuristicsLevel                3

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

AddXHeader                     YES
AddReceivedByHeader           YES

OpenMax                        2048

#
# Anti-Spam Configuration (MailGate Suite License necessary)
#
EnableSpamCheck                YES

# Important Options:
#/necessary/
# SpamAction TAG:
#   allows a user-dependent Spamfiltering,
#   in the mail client or in the main mail server
#
# SpamAction BLOCK:
```



```
# the mail is moved to quarantine at once
# the quarantine can be outread and administered via the
# AVQ-Manager
#
# $ /usr/lib/AntiVir/avmailgate.bin --avq --help
#
SpamAction TAG

DangerousOutbreakAction BLOCK
DangerousAttachmentAction TAG
DangerousAlertAction BLOCK
DangerousUnknownAction TAG

# Important: Black- and Whitelist:
SpamFilterExceptions /etc/asmaligate.except

SpamFilterHandleBulkADVLikeSpam NO
SpamFilterHandleBulkPornLikeSpam YES
SpamFilterModifySubject YES
```

4.3 Updates

In order to keep your AntiVir installation up-to-date you can configure two different modes of updates during the installation:

Scanner update (only scanner & engine & VDF)
Product update (MailGate program files)

You find the settings for the updates in the following file after the installation:
/etc/cron.d/avira_updater:

```
36 */2 * * * root /usr/lib/AntiVir/avupdate --product=Scanner
39 11 * * Tue root /usr/lib/AntiVir/avupdate --
product=mailgate
```

Reasonable values for an update

Depending on usage we recommend our customers to proceed an update at least 2 or 3 times a day.

Large enterprises:

Example: hourly update

/etc/cron.d/avira_updater:

```
* */1 * * * root /usr/lib/AntiVir/avupdate --product=Scanner
```



Small Business:

Example: 3 hour interval

/etc/cron.d/avira_updater:

```
* */3 * * * root /usr/lib/AntiVir/avupdate --product=Scanner
```

Customers with narrow strip connections (Modem/ISDN):

Example: 8 hour interval

/etc/cron.d/avira_updater:

```
* */8 * * * root /usr/lib/AntiVir/avupdate --product=Scanner
```

Internet Service Providers

It is recommended for internet service providers to download the current signatures more frequently, e.g. every 15 minutes. Thereby you can make sure to use always the latest signatures.

/etc/cron.d/avira_updater:

```
*/15 * * * * root /usr/lib/AntiVir/avupdate --product=Scanner
```

Pattern update

Furthermore you have the possibility to execute only an engine and VDF update. The guard product files and the central scanner service (SAVAPI) are not updated.

This can be interesting for you in case you are considering program updates as especially sensitive. Thereby you have the possibility to proceed an audit on a separate test system before you implement the new version in the productive network.

The command has to be entered as follows:

```
$ /usr/lib/AntiVir/avupdate --product=Signatures
```