Avira AntiVir MailGate / Avira MailGate Suite

HowTo

AVIRA

Table of contents

1. Installation

1.1 A closer look at the installation package

You can get the latest Avira AntiVir MailGate installation package at anytime from our website:

http://www.avira.com/en/download/product/avira-antivir-mailgate/

Please unpack the downloaded installation package as follows:

```
gzip -cd antivir-mailgate-prof.tgz | tar xv
```

The created directory contains a couple of essential directories and files which we will look at more closely.

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

The installation directory for Avira AntiVir MailGate is structured as follows:

`bin`	-	Executable files
`cert`	-	Avira certificate
`doc`	-	documentations
`etc`	-	configuration files
`legal`	-	license agreement for 3rd-party tools
`script`	-	shell scripts
`smcpkg`	-	AMC-specific files
`templates`	-	standard templates for MailGate
`vdf`	-	basic virus definitions
`.installrc`	-	product information file
`build.dat`	-	product build version
`install`	-	main installation script
`install_list_webgate`	-	installation files and permissions
`LICENSE`	-	Avira GmbH software license agreement
`LICENSE.DE`	-	Avira GmbH software license agreement
`README`	-	description installation package
`README.uninstall`	-	description uninstall routine
`uninstall`	-	uninstall routine
`uninstall_smcplugin.sh`	-	uninstall script for AMC-plugin

1.2 Interactive installation

You can execute the command-line oriented standard installation as follows:

```
./install
```

If you have already performed an installation at an earlier point in time, you can further accelerate the installation:

```
./install –fast
```

1.3 Automatic installation

If you want to perform a completely automatic (unattended) installation, you can use the installation option that is also used internally by the AMC:

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

All settings for the automatic installation can be found in the mentioned INF-file. Therefore you could also use a copy with your own settings. This would e.g. enable you to perform a major rollout or simply improve your daily tasks.

./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
```

1.4 Standard installation

During the installation you will get queries about the basic configuration.
You can safely use the standard values.

2. Avira AntiVir MailGate in use

2.1 Combination options with MTAs

Avira AntiVir MailGate is a dedicated mail server service with its own queue management. This service can usually communicate with other mail servers via the SMTP-protocol. Therefore, you will get a high number of possible combinations. Avira AntiVir MailGate functions in many cases as a simple mail relay with built-in filter function.

There are currently two special installation options that allow a direct integration into an existing mail server:

- Postfix Content-Filter
- Sendmail Milter

The combination with Postfix has proven itself in the most client cases. Sendmail is used in special cases and particularly on Unix systems like Solaris.

2.1.1 Which alternative should be used when?

Both alternatives can be scaled very well and are used in small installations as well as in the enterprise sector. The respective MTA keeps its main role within the mail traffic and MailGate is integrated via a diversion that can reject threats effectively to the quarantine or block them directly (in the case of Milter).

The big advantage is that all the options are preserved which are otherwise offered by the MTA (SMTP-AUTH etc.). MailGate itself is restricted to basic commands of the SMTP-protocol because of its function.

2.1.2 Avira AntiVir MailGate standalone as a relay

The classical variant - Avira AntiVir MailGate as a simple mail relay - can be particularly interesting in the enterprise sector, because you have much more complex mail structures there.

External branches, high availability and redundancy theoretically require Avira AntiVir MailGate to be installed multiple times. This also increases the administrative overhead. Using Mailgate as a central relay in such an environment has therefore stood its test, e.g. within a company-wide DMZ.

Example:

Internet → external MX → firewall → MailGate (DMZ) → firewall → internal mail relay → internal Infrastructure

2.2 Avira AntiVir MailGate in combination with Postfix

2.2.1 Avira AntiVir MailGate at the front end of Postfix

A variant that is used in relatively rare cases, but can be implemented very easily, is the possibility to use Avira AntiVir MailGate as a local relay at the front end of Postfix.

Scheme for this configuration:

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

You can find a detailed description of the installation of this configuration variant in the Avira AntiVir MailGate manual on page 30 („IP address“) and in chapter 4.5 „Configuring Postfix“

2.2.2 Avira AntiVir MailGate as a content filter

Avira AntiVir MailGate can be integrated in combination with Postfix as a so-called Content Filter. This constellation is the most common solution among our customers. An installation is quite simple. Postfix usually already brings along the support for Content Filter.

Scheme for this configuration:

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

Only the entry for the content filter (the bypass) will be recorded in the main configuration of Postfix (main.cf):

```
„antivir‟ = Port 10024
```

/etc/postfix/main.cf:

```
content_filter=smtp:localhost:10024
```

Below, another TCP-socket will be defined in the service configuration of Postfix. The known mail server service „smtpd“ should scan on top this TCP-socket. It is important to reset the previous globally valid definition for the Content Filter, so it does not cause a mail loop.

```
„smtp-backdoor‟ = Port 10025
```

/etc/postfix/master.cf:

```
localhost:10025 inet n - n - - smtpd -o content_filter=
```

Postfix should then be restarted to apply the configuration. This will complete the configuration in Postfix.

The MailGate configuration is very simple as well:

/etc/avira/avmailgate.conf:

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

At the end a restart of MailGate is required as well to apply the configuration.

2.3 Avira AntiVir MailGate in combination with Sendmail

An interesting variant is the implementation via the Sendmail Milter interface.
Scheme for this configuration:

Internet
|
Sendmail ←→ [MILTER] ←→ MailGate
|
another MTA / Client (MUA)

Tip: With this variant, it is possible to examine mails directly within the SMTP-dialog and to reject them directly in case of a detection, thus enabling a direct „REJECT“. You can find a detailed description of the installation in the Avira AntiVir MailGate manual starting with chapter 3.3 „Integration of Avira AntiVir MailGate (Milter mode) in Sendmail.

2.4 Avira AntiVir MailGate in combination with Avira AntiSpam

The inhouse solution of Avira AntiSpam can be ideally combined with Avira AntiVir MailGate and offers an effective protection from the daily flooding with spam.

A combination is possible as:

- extended content filter
- Standalone operation of both products

2.5 Avira AntiVir MailGate in combination with other MTAs

Avira AntiVir MailGate can basically interact with each mail server which communicates RFC-compliant with SMTP. Typical combinations are:

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

Avira AntiVir MailGate should be configured as a „standalone“ (i.e. relay) operation to combine MailGate with one of those MTAs.

Exemplary schemes for this configuration:

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

Internet → MailGate → Exchange → Client (MUA)

3. Avira MailGate Suite in use

These configurations should be considered beforehand and only be added if needed. The values have to be adopted accordingly.

3.1. Special features of Avira MailGate Suite

Avira MailGate Suite can be purchased as a license upgrade in addition to the normal Avira AntiVir MailGate. This is technically the same product as Avira AntiVir MailGate. However, additional functions will be unlocked by the license upgrade.

Avira MailGate Suite offers currently one additonal complete solution of AntiSpam

You just have to load a new key file contained in Avira MailGate Suite so that you can use the Avira MailGate Suite functionality. Then, you can activate the AntiSpam options in the /etc/avira/avmailgate.conf.

MailGate will be ideally used at the „front“, i.e. as a connective link in the internal or external mail infrastructure.

Exemplary scheme for this configuration:

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

4. Best practices

4.1 Log data

All the resulting log data will be written either into the syslog or into a special log file. There is no monitoring in regards to Avira AntiVir MailGate if the log file reaches a maximum size.

In the Linux and Unix environment there are already for a long time system tools available like „logrotate“. Once configured, they take all your work away and rotate automatically according to own reference values.

4.2 Configuration

You can take the following recommended extended settings below:

Avira AntiVir MailGate (without AntiSpam)

/etc/avira/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
```

Avira MailGate Suite (with AntiSpam)

/etc/avira/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 required)
#
EnableSpamCheck     YES

# Important options:
#
# SpamAction  TAG:
#    enables a user-dependent SpamFiltering,
#    either in the mail client, or in your main mail server
#
# SpamAction  BLOCK:
#    causes a quarantine immediately
#    The quarantine can be read using the AVQ-Manager and
#    managed:
#
#      $ /usr/lib/AntiVir/avmailgate.bin --avq --help
#
SpamAction     TAG

DangerousOutbreakAction  BLOCK
DangerousAttachmentAction     TAG
DangerousAlertAction     BLOCK
DangerousUnknownAction   TAG

# Important: black- and white- list:
SpamFilterExceptions     /etc/avira/asmailgate.except

SpamFilterHandleBulkADVLikeSpam    NO
SpamFilterHandleBulkPornLikeSpam   YES
SpamFilterModifySubject  YES
```

5. Updates

Two types of updates will be set up during the installation to keep your AntiVir installation up to date:

- Scannerupdate (only scanner & engine & VDF)

Product update (MailGate program files)

This can be generally very interesting for you if you consider program updates as a particularly sensitive issue. Thus, you will get the possibility to perform an audit on a separate test system prior to using the new version productively.

The line for that is as follows:

```
/usr/lib/AntiVir/mailgate/avupdate-mailgate --product=Scanner
```

After the installation you will find the settings for the update in the following file:

/etc/cron.d/avira_updater:

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

5.1 Useful settings for an update

Depending on the target group, we recommend for our customers to perform an update at least 2 or 3 times a day.

5.1.1 Medium and large businesses

Example: every hour

/etc/cron.d/avira_updater:

5.1.2 Small businesses

Example: every three hours

/etc/cron.d/avira_updater:

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

5.1.3 Customers with narrowband connections (modem/ISDN):

Example: every 8 hours

/etc/cron.d/avira_updater:

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

5.1.4 Internet service provider

For internet service providers it is of course recommended to look significantly more frequently for new signatures. Therefore, the frequency of update requests should be set considerably higher, e.g. every 15 minutes. This ensures that you always use the latest signatures.

/etc/cron.d/avira_updater:

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

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 Operations GmbH & Co. KG.

Issued Q2-2012

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.

AVIRA

live *free.*™

Avira Operations GmbH & Co. KG
Kaplaneiweg 1
88069 Tettnang
Germany

Telephone: +49 7542-500 0
Facsimile +49 7542-500 3000
www.avira.com