Avira Managed Email Security (AMES)

User Guide

AVIRA

Table of Contents

1. Product information

Thank you for taking a look at the Avira Managed Email Security (AMES) manual.

This manual will help you get started with AMES, as well as customizing AMES to your specific needs. You will have peace in your inbox in no time.

1.1 Functionality

Avira Managed Email Security (AMES) is a service dedicated to stopping spam or viruses before they reach your company's network. This is achieved by routing the emails to our AMES server cluster. AMES then scans and delivers the malware-free emails to your server.

The most accurate spam scanning technology

For intercepting spam, we use a combination of technologies proven to be extremely effective. Since spammers and virus makers become more skilled every day, we constantly test and implement new methods to keep our lead position in email scanning, and you enjoy the benefits of this without any extra effort.

Configuring AMES

Because we stop spam and viruses "in the cloud", that is also the place where the configuration is done.

You can log in to the AMES interface at https://ames.avira.com.

Currently, the AMES interface is available in the following languages:

- English
- German
- French
- Spanish
- Dutch

AMES saves your language preference in a cookie or tries to match your browser's language. In case of an unsupported language, the AMES interface opens in English.

Release notes

To keep you up to date with the latest developments, we placed a link to the **Release notes** page (available at Partner and domain administrator levels only).

1.2 Licensing AMES

When you let your Avira Partner purchase a license for AMES, you need to choose the number of users. These users correspond to the total number of people in your organization, that are going to use AMES to filter emails.

AMES gives you total freedom to distribute these users across multiple domains, create aliases for them, set filtering rules, etc. but you should always keep your license up to date with the actual users. For more information, see the AMES terms and conditions on our website.

2. Getting started with AMES

You'll find that once your Avira Partner has set up a license for your domain, the rest of the configuration is surprisingly easy.

If you don't have an Avira Partner yet, please take a look at the Avira Partner Locator on our website.

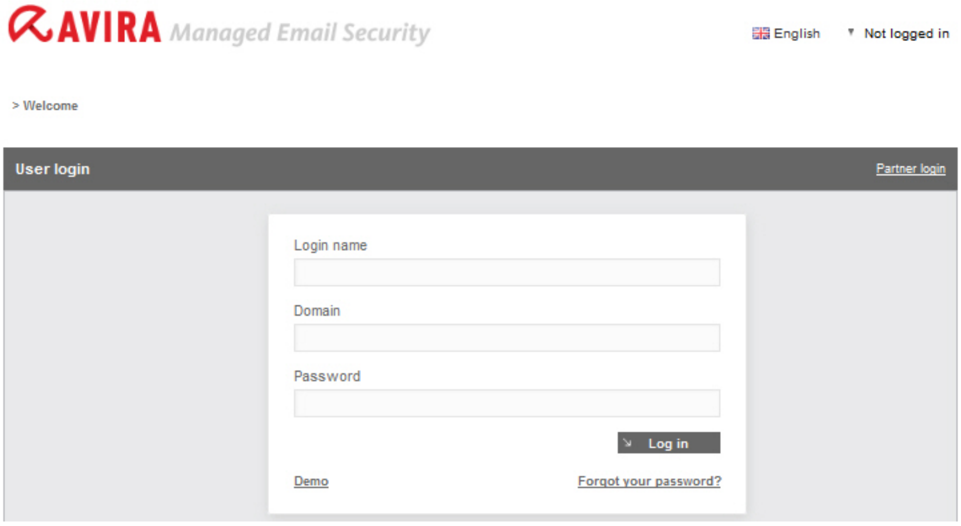
2.1 Adding a new domain to AMES

To add a new domain to AMES, please call your Avira Partner. They will then register your details, request a license and add the domain to AMES.

2.2 Logging in to AMES

The domain is created in AMES and you will receive an **order confirmation email** with the credentials for the AMES account and details such as **DNS MX settings** and **Firewall settings**.

1. Open https://ames.avira.com in your browser, where you'll find the login screen:



2. Fill in your **Login name**, the **Domain** you want to access, and your **Password**.

   These were written in the **order confirmation** your partner received.

3. Click **Login**.

   You will see the AMES **Service License Agreement** (SLA), which you need to read and agree, to continue.

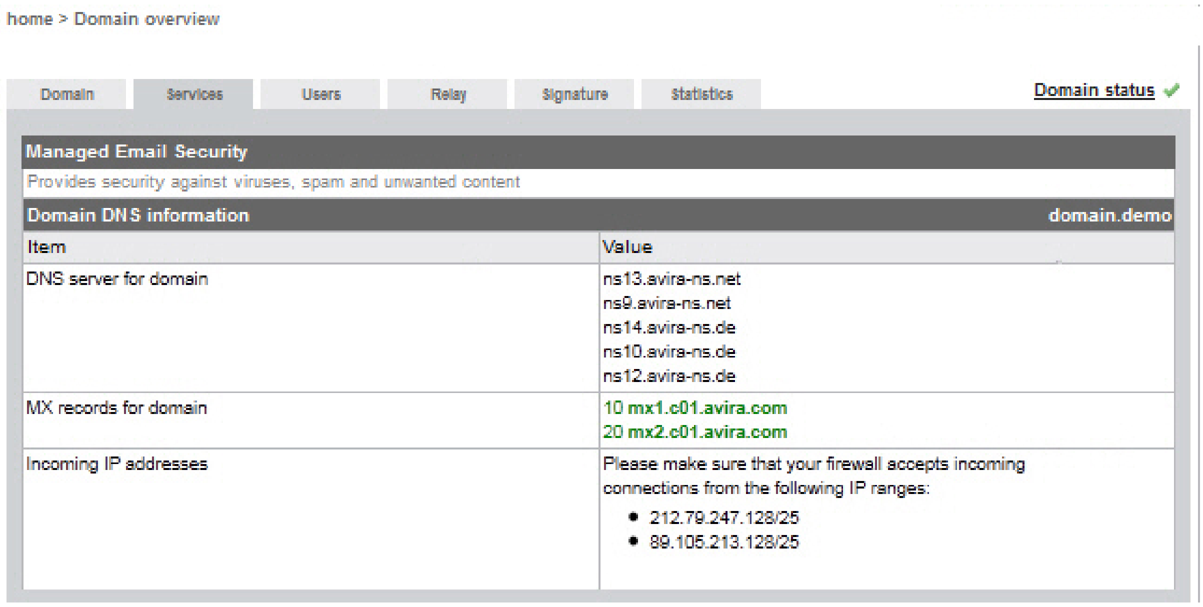
2.3 Configuring the AMES domain

For each new domain, one generic user is created (see "The catch-all user" - page 12) and the **mail delivery** is set to the **currently used mail server**. This means, you can start using AMES without any further configuration and the email flow will not be interrupted.

Normally, your partner carries out the domain configuration for you, but if for some reason you need to do this yourself, we'll guide you in the process.

The Domain status assistant

After logging in to AMES, click the **Services** tab in the **Domain overview**.



Managed Email Security

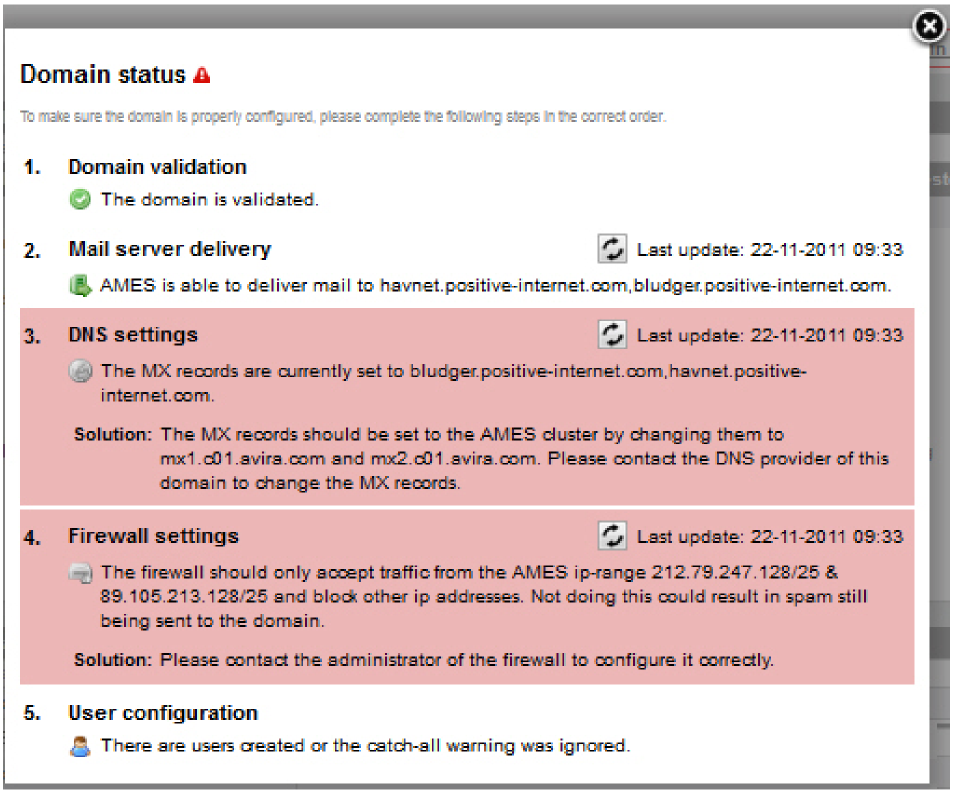
Provides security against viruses, spam and unwanted content

Domain DNS information	domain.demo
Item	Value
DNS server for domain	ns13.avira-ns.net ns9.avira-ns.net ns14.avira-ns.de ns10.avira-ns.de ns12.avira-ns.de
MX records for domain	10 mx1.c01.avira.com 20 mx2.c01.avira.com
Incoming IP addresses	Please make sure that your firewall accepts incoming connections from the following IP ranges: • 212.79.247.128/25 • 89.105.213.128/25

The **Domain status** link opens the 5-step domain activation assistant, which shows the status of each step and eventually displays instructions to complete them:

1. Domain validation
2. Mail server delivery
3. DNS settings

4. Firewall settings
5. User configuration



Domain status ⚠

To make sure the domain is properly configured, please complete the following steps in the correct order.

1. **Domain validation**
   ✓ The domain is validated.

2. **Mail server delivery** — Last update: 22-11-2011 09:33
   AMES is able to deliver mail to havnet.positive-internet.com,bludger.positive-internet.com.

3. **DNS settings** — Last update: 22-11-2011 09:33
   The MX records are currently set to bludger.positive-internet.com,havnet.positive-internet.com.
   Solution: The MX records should be set to the AMES cluster by changing them to mx1.c01.avira.com and mx2.c01.avira.com. Please contact the DNS provider of this domain to change the MX records.

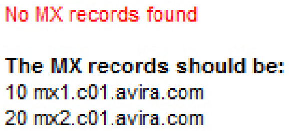
4. **Firewall settings** — Last update: 22-11-2011 09:33
   The firewall should only accept traffic from the AMES ip-range 212.79.247.128/25 & 89.105.213.128/25 and block other ip addresses. Not doing this could result in spam still being sent to the domain.
   Solution: Please contact the administrator of the firewall to configure it correctly.

5. **User configuration**
   There are users created or the catch-all warning was ignored.

Configuring the DNS server

To activate the scanning and filtering of incoming emails, you have to change the **MX-settings** in the DNS server for the domain. The correct records are in the **order confirmation email**.

If correct, the MX records are displayed in green under *Domain DNS information* in the **Services** tab of the **Domain overview**.In case the MX records are not correctly set, a message in red is displayed. For example:



No MX records found

The MX records should be:
10 mx1.c01.avira.com
20 mx2.c01.avira.com

Note
Make sure there is no MX-record with a priority below 10; otherwise emails from your organization will not be scanned and filtered by AMES.

Depending on the Time-To-Live (TTL) settings of your MX records, it might take up to 24 hours before DNS changes become active.

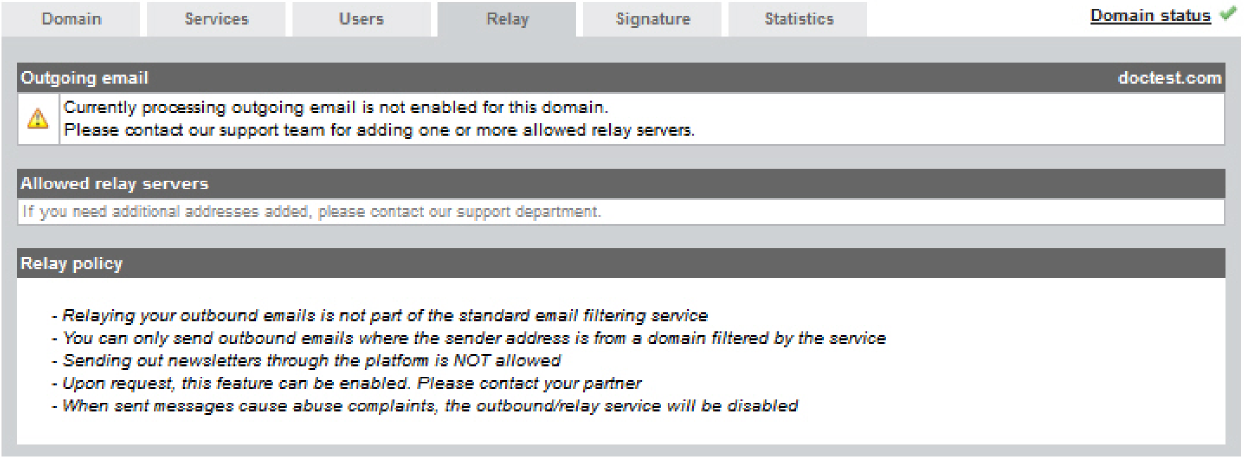
After directing the MX records to the Avira AMES cluster, the managed service is active and will scan and filter the incoming emails. The filtered and scanned emails will be delivered to the regular mailbox.

Configuring security and firewall

After DNS changes are complete and propagated correctly, make sure the receiving mail server accepts only emails coming from the AMES server cluster mentioned in the **order confirmation email**. This can be done through settings in the firewall or mail server itself.

2.4 Scanning outgoing emails

By default, AMES scans only the incoming emails. The relay service (scanning of outgoing emails) is initially deactivated.



Outgoing email — doctest.com

⚠ Currently processing outgoing email is not enabled for this domain.
Please contact our support team for adding one or more allowed relay servers.

Allowed relay servers

If you need additional addresses added, please contact our support department.

Relay policy

- *Relaying your outbound emails is not part of the standard email filtering service*
- *You can only send outbound emails where the sender address is from a domain filtered by the service*
- *Sending out newsletters through the platform is NOT allowed*
- *Upon request, this feature can be enabled. Please contact your partner*
- *When sent messages cause abuse complaints, the outbound/relay service will be disabled*

If you want AMES to scan your outgoing emails for viruses, please contact your Avira partner, to activate the relay feature for your domain.

With enabled relay service, the domain’s administrators will see the amount of filtered outgoing messages.

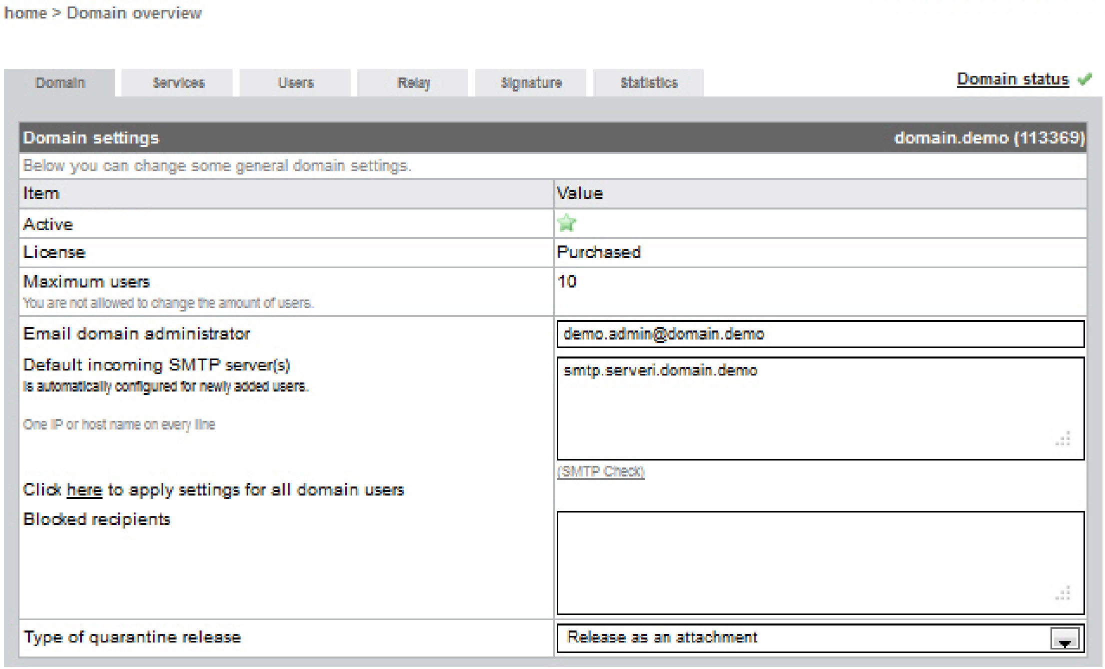
A daily maximum amount of messages is set, depending on the number of users: the amount of users in the domain, multiplied by 50 (never less than 1000 messages). If this limit is reached, the administrators receive a bounce message.

3. Setting your AMES domains and users

3.1 Making general domain settings

First, you should check the general settings of the new domain.

1. In the **Domain overview**, click the **Domain** tab.



Domain settings	domain.demo (113369)
Below you can change some general domain settings.	
Item	Value
Active	✓
License	Purchased
Maximum users You are not allowed to change the amount of users.	10
Email domain administrator	demo.admin@domain.demo
Default incoming SMTP server(s) is automatically configured for newly added users. One IP or host name on every line	smtp.serveri.domain.demo (SMTP Check)
Click here to apply settings for all domain users	
Blocked recipients	
Type of quarantine release	Release as an attachment

The **Domain status** link opens the 5-step domain activation assistant (see "The Domain status assistant" - page 7).

2. Your partner can activate or deactivate your domain.

   The license type and the maximum number of users for the domain are displayed under *Domain settings*.

3. In the **Email domain administrator** field, type the email address of the domain administrator.

4. Insert the **Default incoming SMTP server(s)**, which will apply to the new users you create.

   Add only one IP address or hostname on each line.

   If you want to assign these servers to all domain users, use the "Click here" link.

5. In case you want to block the email accounts of certain users, but keep their quarantines for a while, add their email addresses in the **Blocked recipients** field.

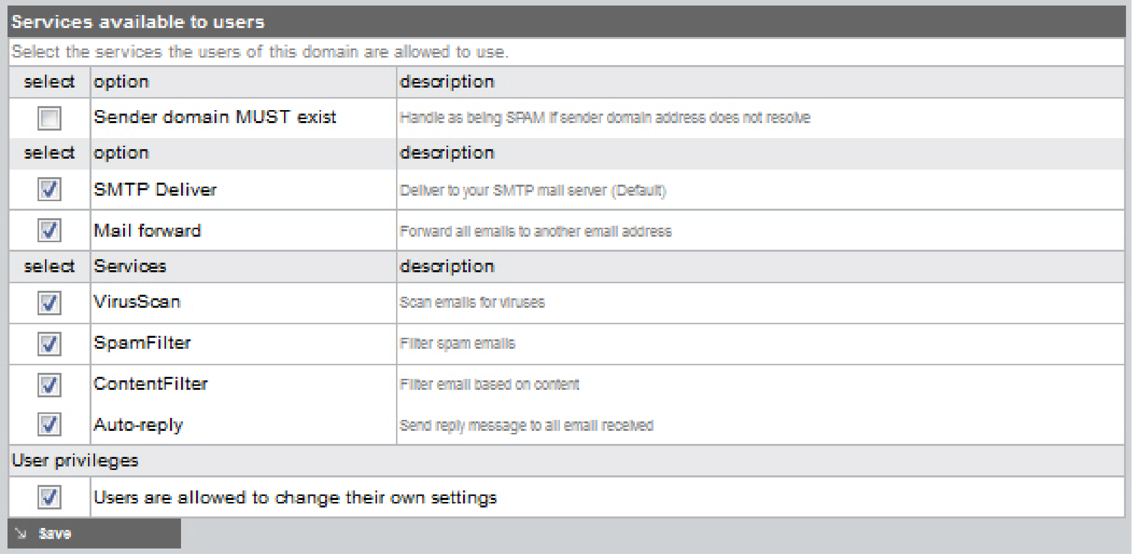
When released from quarantine, blocked emails can be released as attachment or as the original message. To set this behavior for the entire domain, use the option **Type of quarantine release**:

- **Release as the original message** - Send the original message to the users' inboxes.
- **Release as an attachment** - Send the blocked message as attachment to a warning email to the users' inboxes.

3.2 Setting the services available to end-users

1. In the **Domain overview**, click the **Services** tab.

2. Under *Services available to users*, you can enable or disable certain options for all the end-users of the selected domain.



Services available to users

Select the services the users of this domain are allowed to use.

select	option	description
□	Sender domain MUST exist	Handle as being SPAM if sender domain address does not resolve
select	**option**	**description**
☑	SMTP Deliver	Deliver to your SMTP mail server (Default)
☑	Mail forward	Forward all emails to another email address
select	**Services**	**description**
☑	VirusScan	Scan emails for viruses
☑	SpamFilter	Filter spam emails
☑	ContentFilter	Filter email based on content
☑	Auto-reply	Send reply message to all email received
User privileges		
☑	Users are allowed to change their own settings	

- **Sender domain MUST exist** - If the domain of the sender does not resolve, the message is considered spam.
- **SMTP Deliver** - Messages are delivered to the SMTP mail server.
- **Mail forward** - Messages are forwarded to another email address.
- **VirusScan** - Messages are scanned for viruses.
- **SpamFilter** - Messages are scanned for spam.
- **ContentFilter** - Message components are scanned, according to the whitelist/ blacklist content rules.
- **Auto-reply** - The users are allowed to activate the auto-reply service.
- **Users are allowed to change their own settings** - The users can activate virus notifications and schedule quarantine reports.

3.3 Adding new users to a domain

When AMES is configured for your domain, the users you provide have to operate properly. If an email is sent to the email address `test@demo.domain`, the user `test` has to exist, or the email will bounce back to the sender.

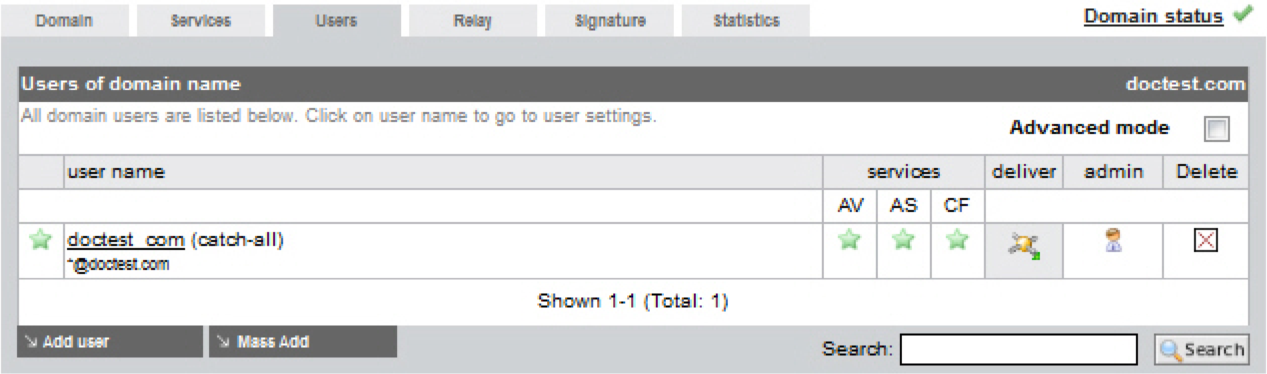
The catch-all user

By default, AMES has one **catch-all user**. A catch-all user is convenient because it receives emails for all users on your domain.

> **Note**
> Avira discourages the use of a "catch-all" setting. The best approach is to create a separate user account in AMES for every user you have. The LDAP feature can reduce the time spent on this task. Please contact your Avira partner for more information.

3.3.1 Adding a new user

1. To add a new user manually, go to the **Domain overview** and click the **Users** tab.



Users of domain name — doctest.com

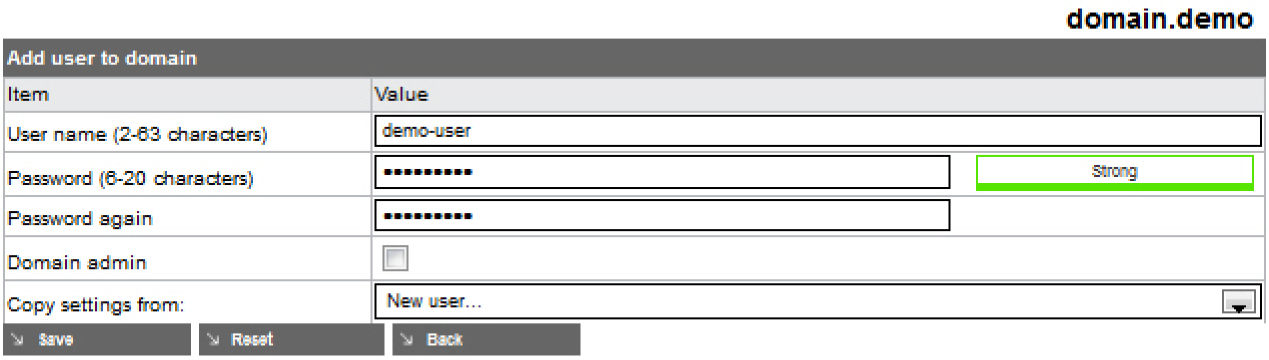
All domain users are listed below. Click on user name to go to user settings.

Advanced mode □

	user name	services			deliver	admin	Delete
		AV	AS	CF			
☆	doctest_com (catch-all) *@doctest.com	☆	☆	☆			☒

Shown 1-1 (Total: 1)

2. Click **Add user** to open the **Add user to domain** dialog:



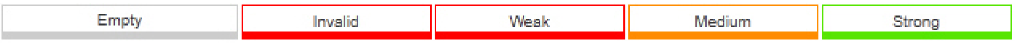
domain.demo

Add user to domain

Item	Value
User name (2-63 characters)	demo-user
Password (6-20 characters)	••••••••••
Password again	••••••••••
Domain admin	□
Copy settings from:	New user...

Each **User name** is considered to be the **primary email address** of that user; any other email address of that specific user is considered an **alias**.

3. Type the **User name** and **Password** for your new user. The password has to be minimum 6 characters long. The password strength is shown as you type:



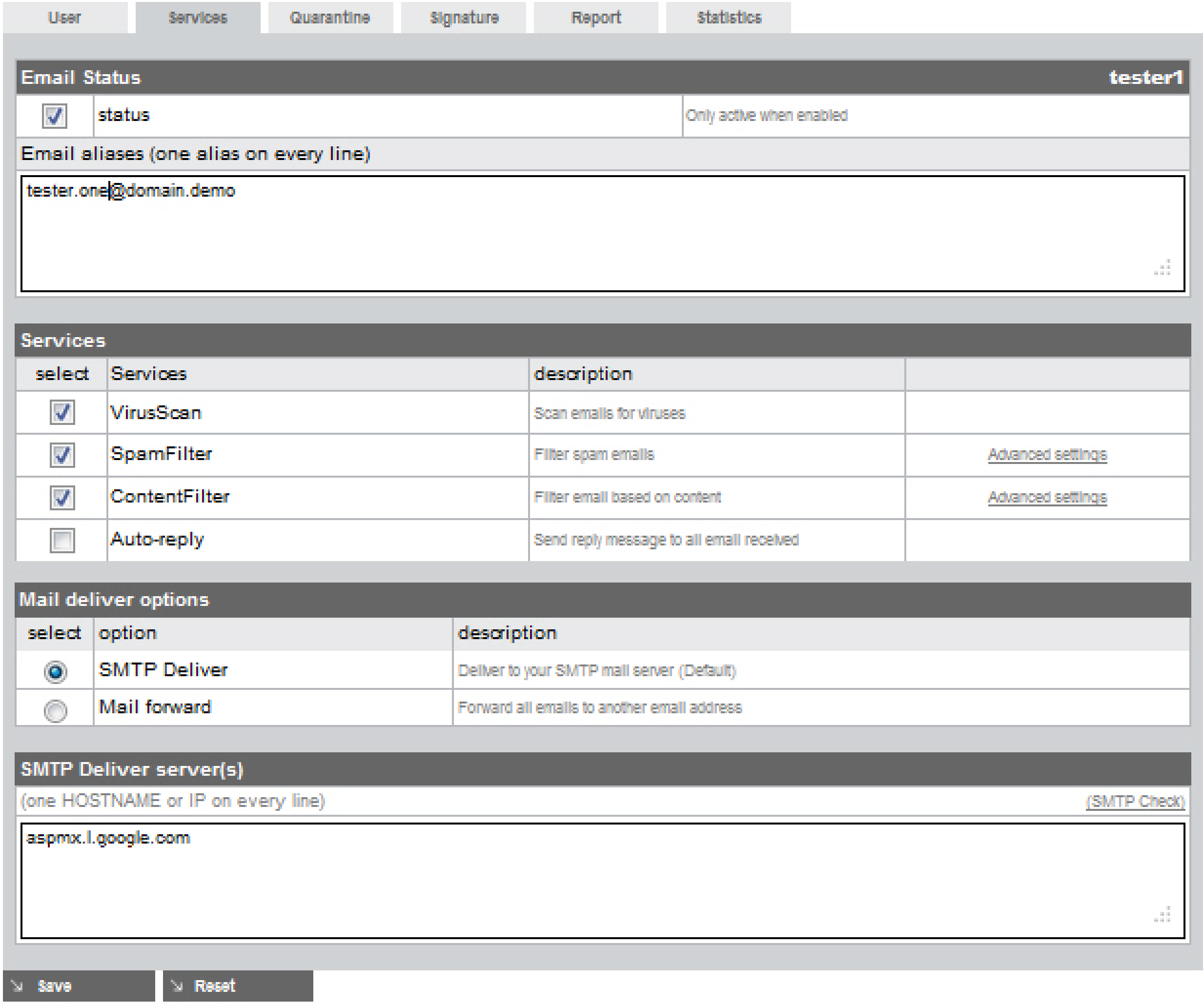
4. If you'd like this user to be able to manage the domain's settings on https://ames.avira.com, enable the **Domain admin** option.

5. You can apply the settings from an existing user, by selecting it from the drop-down list **Copy settings from**.

6. When finished, click **Save**.

   You will be warned that the user is disabled by default. This is done so you can review the settings before they take effect.

7. To enable the user, click its name in the **Users** tab and activate the **status** option and the available services in the **Services** tab:



Email Status		tester1
☑	status	Only active when enabled

Email aliases (one alias on every line)

tester.one@domain.demo

Services

select	Services	description	
☑	VirusScan	Scan emails for viruses	
☑	SpamFilter	Filter spam emails	Advanced settings
☑	ContentFilter	Filter email based on content	Advanced settings
□	Auto-reply	Send reply message to all email received	

Mail deliver options

select	option	description
●	SMTP Deliver	Deliver to your SMTP mail server (Default)
○	Mail forward	Forward all emails to another email address

SMTP Deliver server(s)

(one HOSTNAME or IP on every line) (SMTP Check)

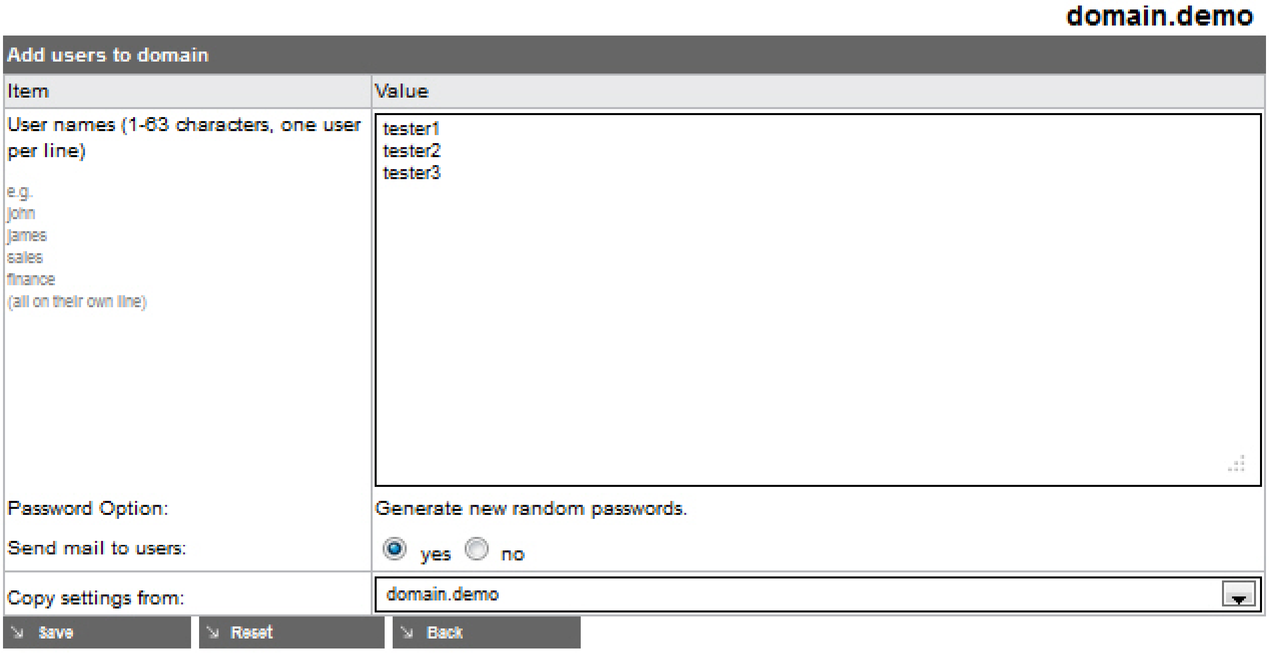
aspmx.l.google.com

- **VirusScan** - Messages are scanned for viruses.
- **SpamFilter** - Messages are scanned for spam.

- **ContentFilter** - Message components are scanned, according to the whitelist/ blacklist content rules.
- **Auto-reply** - The users are allowed to activate the auto-reply service.
- **SMTP Deliver** - Messages are delivered to the SMTP mail server.
- **Mail forward** - Messages are forwarded to another email address.

3.3.2 Adding multiple users to a domain (Mass Add)

1. To add multiple users at once, go to the **Domain overview**, click the **Users** tab and press **Mass Add**.



domain.demo

Add users to domain

Item	Value
User names (1-63 characters, one user per line) e.g. john james sales finance (all on their own line)	tester1 tester2 tester3
Password Option:	Generate new random passwords.
Send mail to users:	● yes ○ no
Copy settings from:	domain.demo

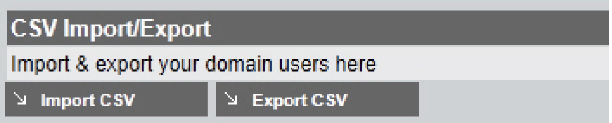
2. Insert the names of the new users, one per line, in the **User names** area.
3. You can apply the settings from an existing user, by selecting it from the drop-down list **Copy settings from**.
4. The **Mass Add** feature generates random passwords and sends them by email to the users, if the option **Send mail to users** is set to **yes**.
5. When finished, click **Save**.

   A message is displayed, with the list of users and passwords added to the domain.
6. Send the new credentials to your new users, if the option **Send mail to users** was set to **no**.

3.4 Import/ Export the list of domain users

Avira-Partners and AMES domain administrators can import/ export the list of the users of a domain in a csv-type file. The file is editable and contains the settings for each user. It can be used to easily add or modify the settings for a large number of users (mass updates).

1. To carry out an import or export of the users' list, go to the **Domain overview**, click the **Domain** tab and scroll down to the *CSV Import/Export* section.



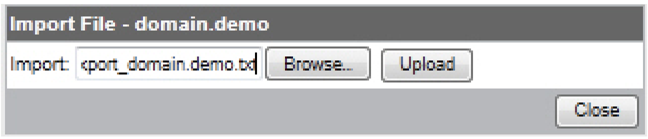
CSV Import/Export

Import & export your domain users here

2. Click **Export CSV** and open the export file in an editor or save it on your system.

   You can make changes to the users' settings in a spreadsheet, as needed.

3. Then you can save the file as .txt and import it into the domain again, by clicking **Import CSV** on the **Domain** tab.

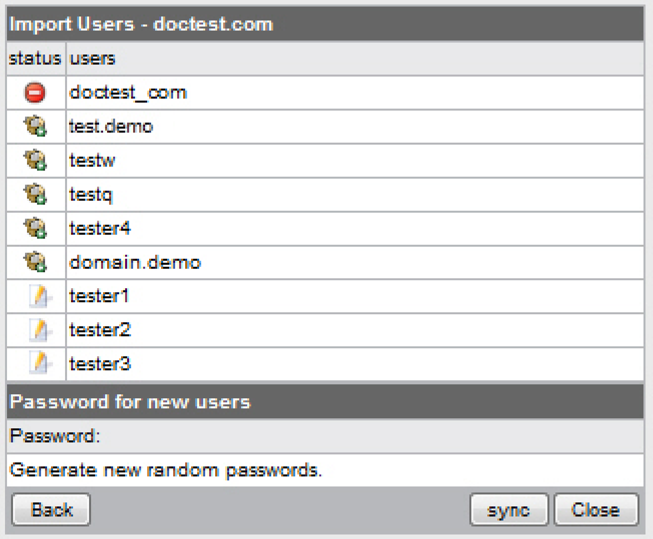


Import File - domain.demo

Import: xport_domain.demo.txt

4. In the **Import File** dialog, select the file from your system and click **Upload**.

5. You can review the list of imported users and click **sync**, to finalize the import and generate new random passwords for all the users.



Import Users - doctest.com

status	users
⊖	doctest_com
✚	test.demo
✚	testw
✚	testq
✚	tester4
✚	domain.demo
✎	tester1
✎	tester2
✎	tester3

Password for new users

Password:

Generate new random passwords.

Status symbols:

✚ - added user

✎ - modified user

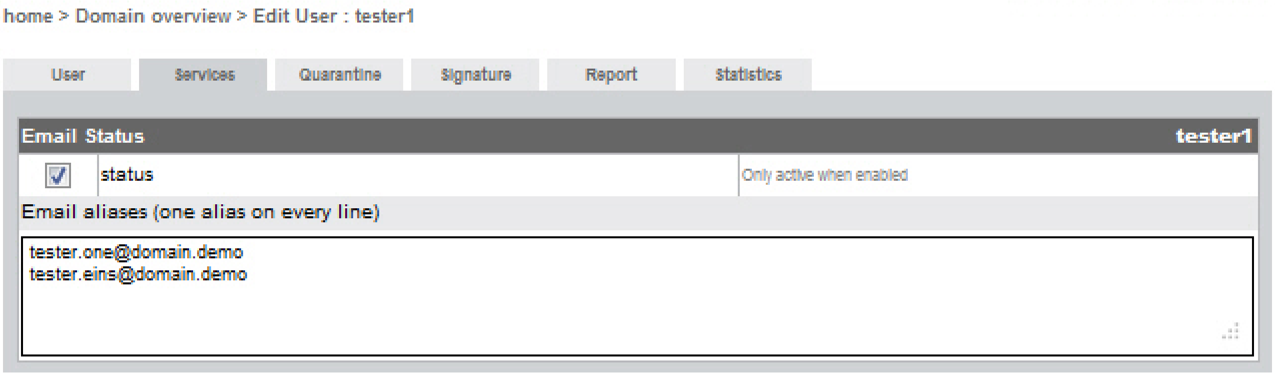
⛔ - deleted user

3.5 Adding a user alias

User aliases can be used to assign multiple email addresses to one user.

1. If you'd like to create an alias, select the user from the **Users** tab.

   The **Services** tab for the selected user opens:



home > Domain overview > Edit User : tester1

Email Status tester1

☑ status Only active when enabled

Email aliases (one alias on every line)

tester.one@domain.demo
tester.eins@domain.demo

2. Add one or more email addresses in the **Email aliases** field (e.g. `tester.one@domain.demo`). Insert each of them on a new line, not separated by other characters.

3. Click **Save** on the bottom of the page when done.

Greylisting

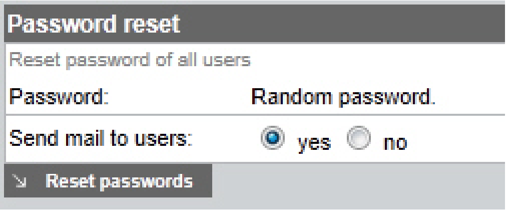
Warning
If you'd like to use a **catch-all address**, use the * placeholder (`*@domain.demo`), but please note:
The use of a so-called catch-all setting, where every combination of characters in front of the domain name is accepted as an email address (`*@example.com`), makes your domain extra vulnerable to spam and viruses. This is why AMES enables **advanced greylisting** for all catch-all users. This technique bounces emails from unknown senders the first time, and will accept only the second or later attempt. Because a lot of spam servers will not try to resend emails, greylisting significantly reduces the amount of emails that must be filtered and scanned.

Note
Since the time it takes for the emails to be re-delivered depends on the sender's mail server, thus delaying the email delivery, Avira discourages the use of a "catch-all" setting. The best approach is to create a separate user account in AMES for every user you have. The **Domain synchronization** feature can really cut the time spent on this task.

3.6 Resetting user passwords

Domain administrators and Avira partners can reset the passwords of all users of a domain, by generating random passwords.

1. To reset all user passwords within a domain, go to the **Domain overview**, click the **Services** tab and scroll down to the *Password reset* section.



Password reset

Reset password of all users

Password: Random password.

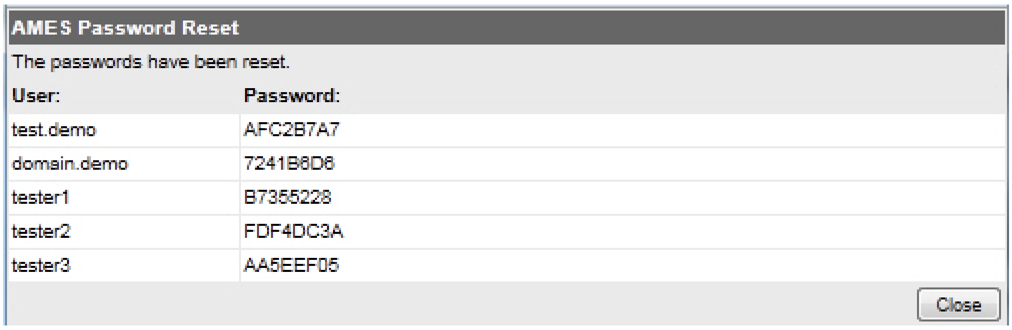
Send mail to users: ● yes ○ no

2. Leave the option **Send mail to users** enabled (**yes**, default setting), if you want to send the new credentials to the users by email.

3. Click **Reset passwords**, to generate the new credentials.

   A list of the generated data is displayed.

4. If you did not enable the option **Send mail to users**, make sure you save this list and send the credentials to each of the users.



AMES Password Reset

The passwords have been reset.

User:	Password:
test.demo	AFC2B7A7
domain.demo	7241B6D6
tester1	B7355228
tester2	FDF4DC3A
tester3	AA5EEF05

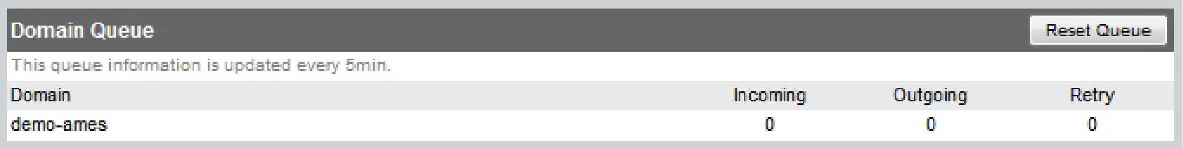
3.7 Synchronization settings (LDAP/ CSV)

These settings are only available to Avira Partners, because of the possible consequences of misconfiguration. Please contact your Avira partner for more information.

3.8 Domain queue information

As Avira-Partner or domain administrator, you can view the statistics of **Incoming**, **Outgoing** and **Retry** queues per domain.

1. Select a domain and click the **Domain** tab. Scroll down to the *Domain Queue* section:



Domain Queue

This queue information is updated every 5min.

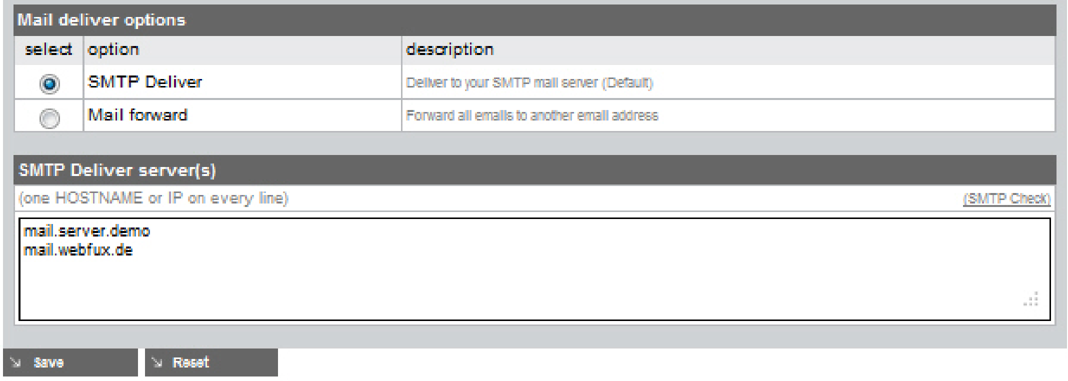
Domain	Incoming	Outgoing	Retry
demo-ames	0	0	0

2. You can use the **Reset Queue** button, to empty the email queue.

3.9 Changing the email delivery options for a user

You can choose between delivery to your SMTP server (default setting) or forwarding the emails to another address (in case you temporary need this service).

1. To change mail delivery settings, select a **User** and go to the **Services** tab.



Mail deliver options

select	option	description
●	SMTP Deliver	Deliver to your SMTP mail server (Default)
○	Mail forward	Forward all emails to another email address

SMTP Deliver server(s)

(one HOSTNAME or IP on every line) (SMTP Check)

```
mail.server.demo
mail.webfux.de
```

2. Under *Mail deliver options*, you can choose between two methods:

   - Activate **SMTP Deliver**.
     Under **SMTP Deliver server(s)**, you can add one or more hosts or IP addresses, to which AMES will deliver the emails.

   - Activate **Mail forward**.
     Under **Forward your email to this address**, you can type one or more email addresses to which AMES will deliver your emails.

3. Click **Save** when done.

3.10 Customizing email signatures

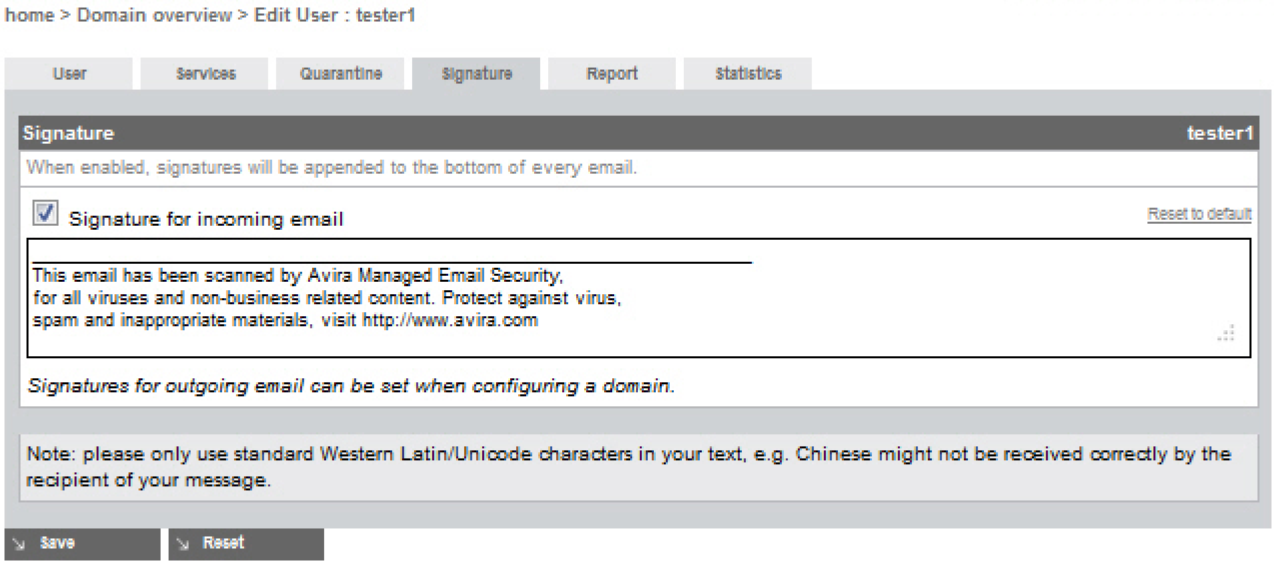
AMES allows you to append a custom message (signature) to the bottom of an outgoing or incoming email.

> **Note**
> Please use only standard Western Latin/ Unicode characters in the signature text.

Adding a signature to incoming emails

You can add a **user-specific** signature to incoming emails.

1. Select the **User** you'd like to add a signature for and go to the **Signature** tab.



Signature tester1

When enabled, signatures will be appended to the bottom of every email.

☑ Signature for incoming email

Reset to default

This email has been scanned by Avira Managed Email Security,
for all viruses and non-business related content. Protect against virus,
spam and inappropriate materials, visit http://www.avira.com

Signatures for outgoing email can be set when configuring a domain.

Note: please only use standard Western Latin/Unicode characters in your text, e.g. Chinese might not be received correctly by the recipient of your message.

2. Activate the option **Signature for incoming email** and write the text in the text area.

   -OR-

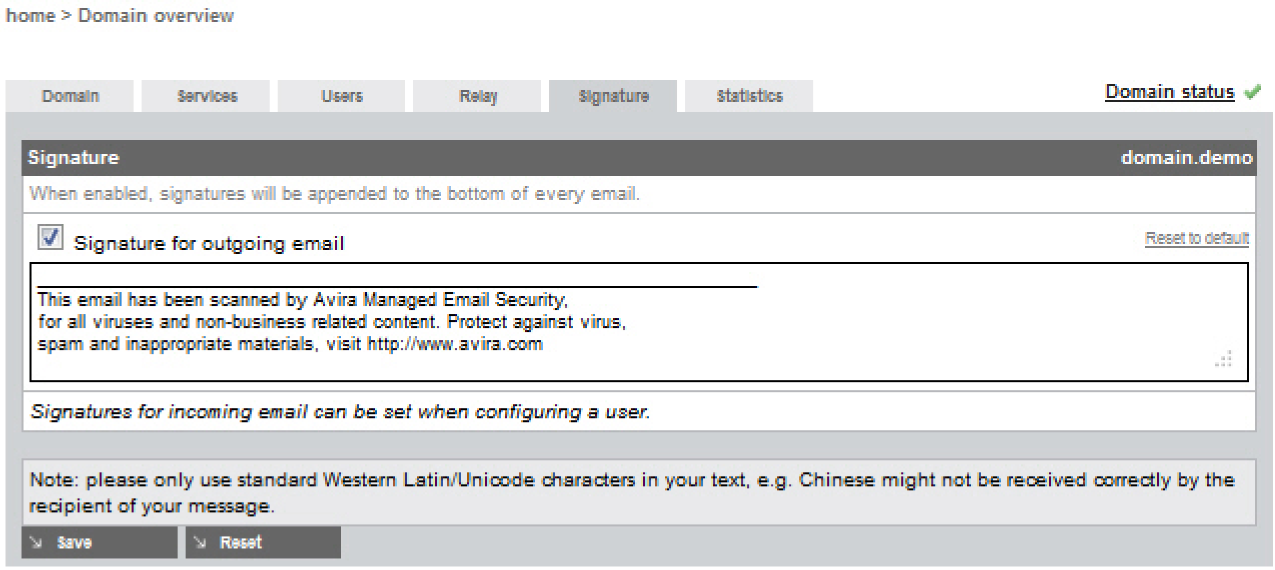
   Click the **Reset to default** link, to use a standard signature.

3. Click **Save**.

Adding a signature to outgoing emails

You can add a **domain-specific** signature to outgoing emails, in case you use the Relay service (see 2.4 Scanning outgoing emails - page 9).

1. Select the **Domain** you'd like to add a signature for and go to the **Signature** tab.



Signature domain.demo

When enabled, signatures will be appended to the bottom of every email.

☑ Signature for outgoing email

Reset to default

This email has been scanned by Avira Managed Email Security,
for all viruses and non-business related content. Protect against virus,
spam and inappropriate materials, visit http://www.avira.com

Signatures for incoming email can be set when configuring a user.

Note: please only use standard Western Latin/Unicode characters in your text, e.g. Chinese might not be received correctly by the recipient of your message.

2. Activate the option **Signature for outgoing email** and write the text in the text area.

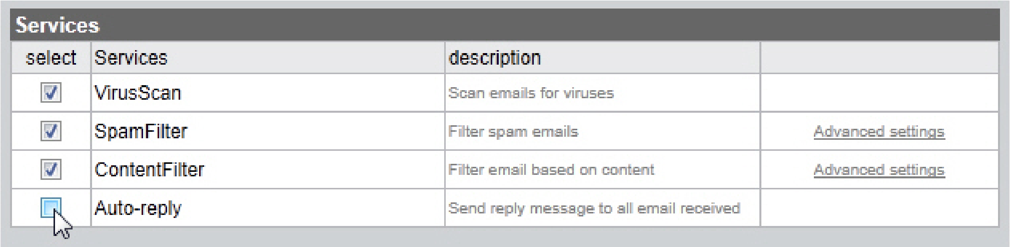
   -OR-

   Click the **Reset to default** link, to use a standard signature.

3. Click **Save**.

3.11 Setting up an automatic reply

1. To set an auto-reply message to the emails received by a user (for example, an "out of office" reply), select the **User**, go to **Services** and activate the **Auto-reply** service:

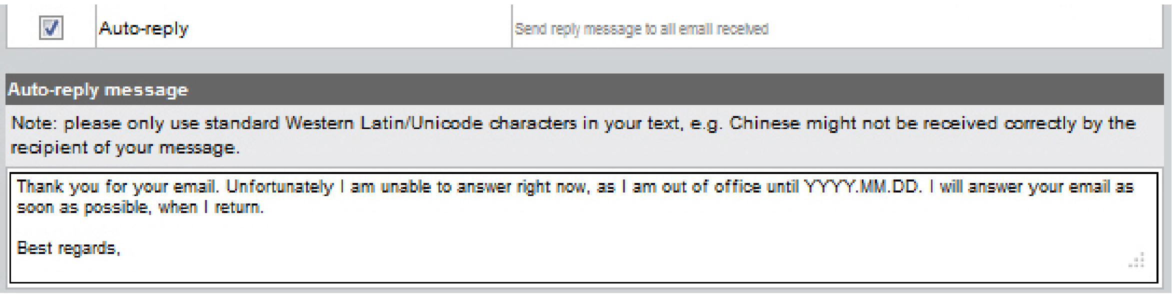


Services

select	Services	description	
☑	VirusScan	Scan emails for viruses	
☑	SpamFilter	Filter spam emails	Advanced settings
☑	ContentFilter	Filter email based on content	Advanced settings
□	Auto-reply	Send reply message to all email received	

Note
If the **Auto-reply** service is not listed for the selected user, the service has to be enabled by a domain administrator or Avira partner (see 3.2 Setting the services available to end-users - page 11).

2. Type the reply message (using standard Western Latin/ Unicode characters) in the **Auto-reply message** text area:



☑	Auto-reply	Send reply message to all email received

Auto-reply message

Note: please only use standard Western Latin/Unicode characters in your text, e.g. Chinese might not be received correctly by the recipient of your message.

Thank you for your email. Unfortunately I am unable to answer right now, as I am out of office until YYYY.MM.DD. I will answer your email as soon as possible, when I return.

Best regards,

3. Click **Save** to apply the change.

4. Quarantine Management

4.1 Configuring the email filters

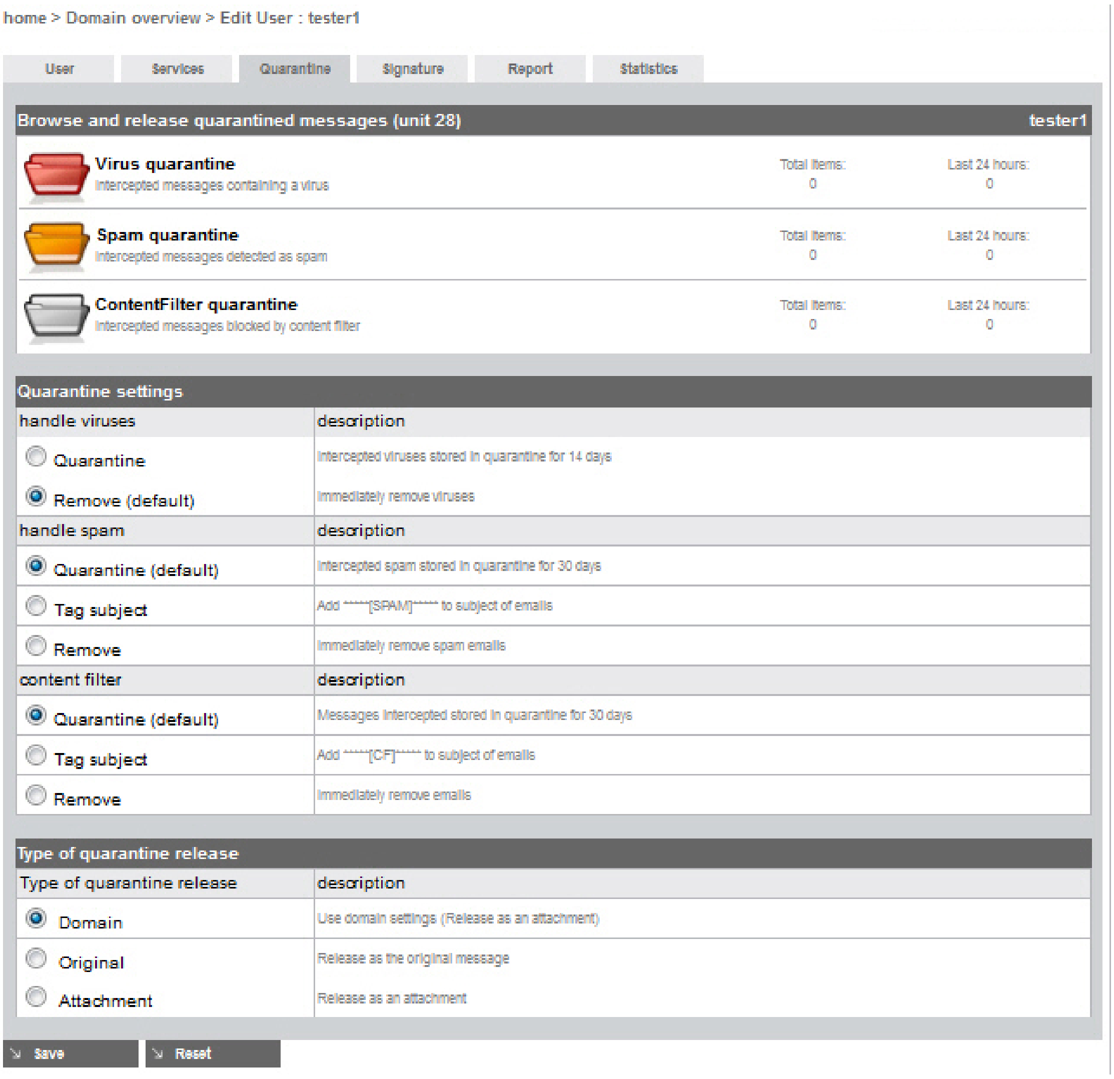
AMES comprises a variety of email filtering and analysis tools. You can configure your AMES account to remove infected emails immediately, to send them to quarantine or just to place a tag in their subject. Furthermore, you can set the heuristic level of the spam control, define advanced spam rules and content filtering rules.

Note
According to their company’s security policy, the domain administrators can configure the filters, the quarantines and the reports, and disable these options for the end-users.

4.1.1 Handling intercepted spam or viruses

By default, AMES sends all spam and filtered emails to quarantine. You may also choose a different behavior, such as to tag the email and then deliver it to the inbox, or even to remove it immediately.

1. Choose a **User** for which you'd like to configure the spam and virus handling and click the **Quarantine** tab.



home > Domain overview > Edit User : tester1

Browse and release quarantined messages (unit 28) tester1

Virus quarantine Intercepted messages containing a virus	Total items: 0	Last 24 hours: 0
Spam quarantine Intercepted messages detected as spam	Total items: 0	Last 24 hours: 0
ContentFilter quarantine Intercepted messages blocked by content filter	Total items: 0	Last 24 hours: 0

Quarantine settings

handle viruses	description
○ Quarantine	Intercepted viruses stored in quarantine for 14 days
● Remove (default)	Immediately remove viruses
handle spam	**description**
● Quarantine (default)	Intercepted spam stored in quarantine for 30 days
○ Tag subject	Add `*****[SPAM]*****` to subject of emails
○ Remove	Immediately remove spam emails
content filter	**description**
● Quarantine (default)	Messages intercepted stored in quarantine for 30 days
○ Tag subject	Add `*****[CF]*****` to subject of emails
○ Remove	Immediately remove emails

Type of quarantine release

Type of quarantine release	description
● Domain	Use domain settings (Release as an attachment)
○ Original	Release as the original message
○ Attachment	Release as an attachment

2. Select the action you want to apply to infected emails, spam emails or filtered content:

   - Under *handle viruses*: select **Quarantine**, if infected emails should be quarantined for 14 days, then deleted; or select **Remove**, if infected emails should be deleted immediately (default setting).

   - Under *handle spam*: select **Quarantine**, if spam emails should be quarantined for 30 days, then deleted (default setting); select **Tag subject**, to mark the subject of spam emails with `******[SPAM]*******` in your inbox; or select **Remove**, if spam emails should be deleted immediately.

   - Under *content filter*: select **Quarantine**, if filtered emails should be quarantined for 30 days, then deleted (default setting); select **Tag subject**, to mark the subject of filtered emails with `******[CF]*******` in your inbox; or select **Remove**, if filtered emails should be deleted immediately.

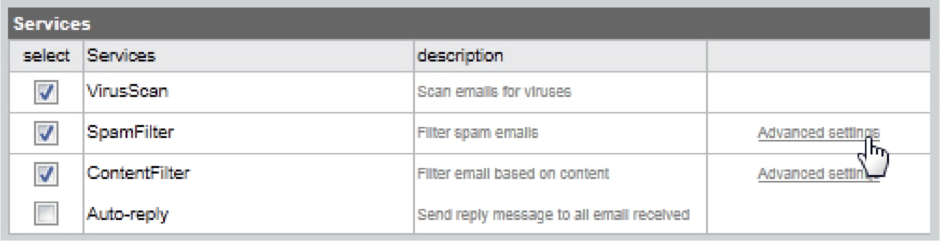
3. When released from quarantine, blocked emails can be released as attachment or as the original message. To set this behavior per user, use the option *Type of quarantine release*:

- **Domain** - Keep the setting made by the domain administrator for the entire domain (see 3.1 Making general domain settings - page 10).
- **Original** - Send the original message in the user's inbox.
- **Attachment** - Send the blocked message as attachment to a warning email to the user's inbox.

4. Click **Save** to save the settings.

4.1.2 Adjusting the filter settings

If you'd like to change the settings for the SpamFilter and/or the ContentFilter, select a **User**, go to the **Services** tab and click on **Advanced settings** for the filter you'd like to adjust.

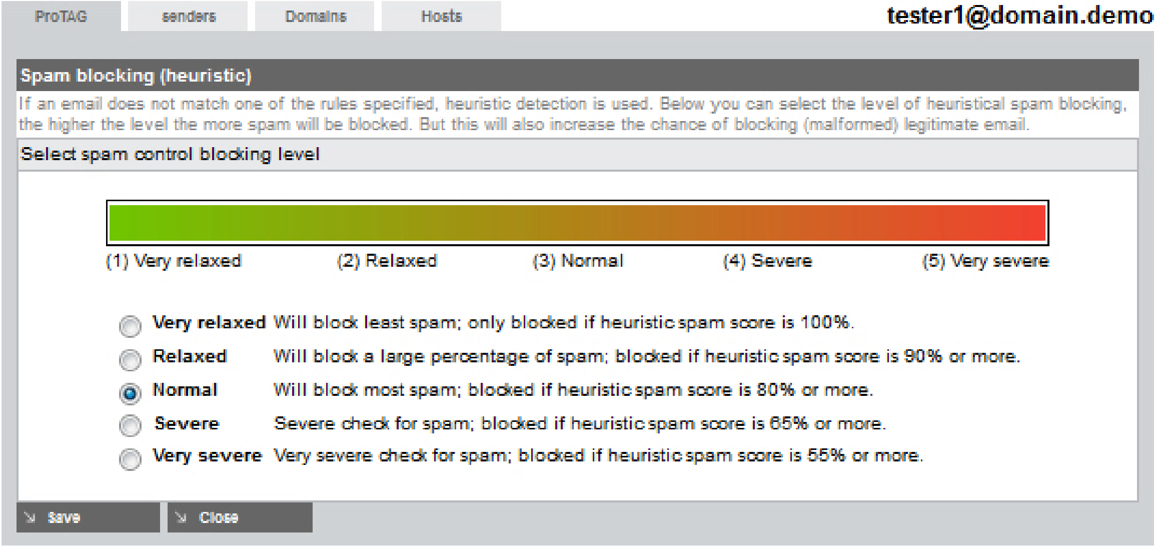


Services

select	Services	description	
☑	VirusScan	Scan emails for viruses	
☑	SpamFilter	Filter spam emails	Advanced settings
☑	ContentFilter	Filter email based on content	Advanced settings
□	Auto-reply	Send reply message to all email received	

SpamFilter

On the **Advanced settings** page, click **ProTAG**. Here you can set the blocking level for the heuristic spam control, which is applied to your incoming emails.



tester1@domain.demo

Spam blocking (heuristic)

If an email does not match one of the rules specified, heuristic detection is used. Below you can select the level of heuristical spam blocking, the higher the level the more spam will be blocked. But this will also increase the chance of blocking (malformed) legitimate email.

Select spam control blocking level

○ **Very relaxed** Will block least spam; only blocked if heuristic spam score is 100%.
○ **Relaxed** Will block a large percentage of spam; blocked if heuristic spam score is 90% or more.
● **Normal** Will block most spam; blocked if heuristic spam score is 80% or more.
○ **Severe** Severe check for spam; blocked if heuristic spam score is 65% or more.
○ **Very severe** Very severe check for spam; blocked if heuristic spam score is 55% or more.

There are five levels of severity for the spam control, based on the heuristic spam score:

- **Very relaxed** - blocks only messages with a heuristic spam score of 100%.
- **Relaxed** - blocks only messages with a heuristic spam score greater than 90%.
- **Normal** - blocks only messages with a heuristic spam score greater than 80%.

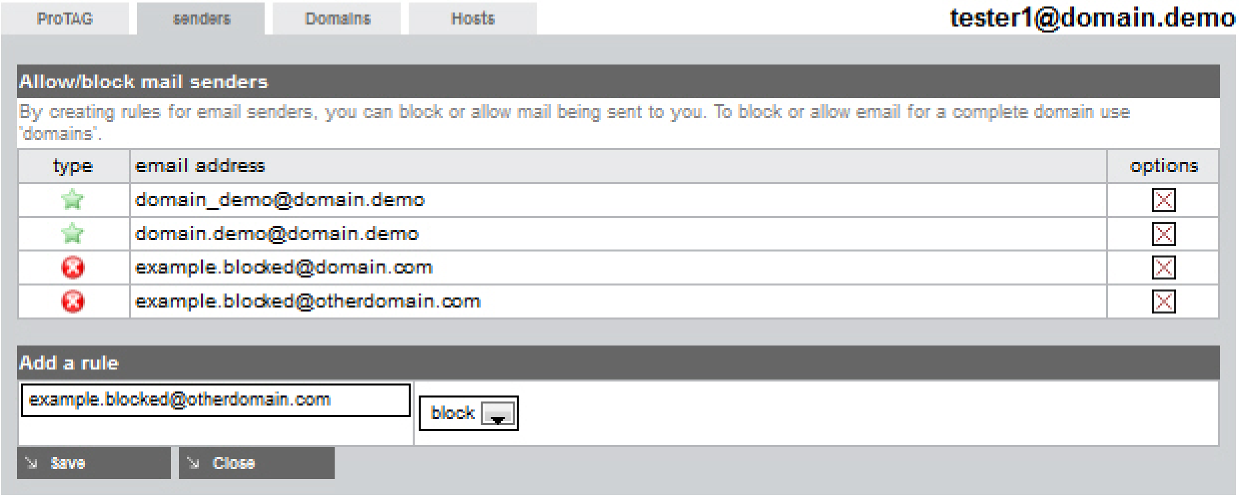
- **Severe** - blocks messages with a heuristic spam score greater than 65%.
- **Very severe** - blocks messages with a heuristic spam score greater than 55%.

The default setting is **Normal**.

> **Note**
> For organizations with a normal rate of spam we recommend the **Normal** level. As a result of setting the SpamFilter to **Severe** or **Very severe**, legitimate email with spam properties might be blocked. That is why we advise that you monitor your Spam quarantine on a regular basis, and schedule a daily spam report.

Using the SpamFilter settings, you can also block or allow certain email senders, domains or hosts.

1. For example, to add rules for email senders, click the **Senders** tab.



Allow/block mail senders

By creating rules for email senders, you can block or allow mail being sent to you. To block or allow email for a complete domain use 'domains'.

type	email address	options
★	domain_demo@domain.demo	☒
★	domain.demo@domain.demo	☒
✖	example.blocked@domain.com	☒
✖	example.blocked@otherdomain.com	☒

Add a rule

example.blocked@otherdomain.com — block

2. Insert the email address of the sender in the field under **Add a rule** (e.g. `example.blocked@otherdomain.com`).

3. Select the rule type: **block** or **allow**.

4. Click **Save**, to add the rule.

   The rules are listed under *Allow/block mail senders*, with type-symbols:
   ✖ block (blacklist) or
   ★ allow (whitelist).

To delete a rule, click the **X** mark in the **options** column and click **OK** in the pop-up window.

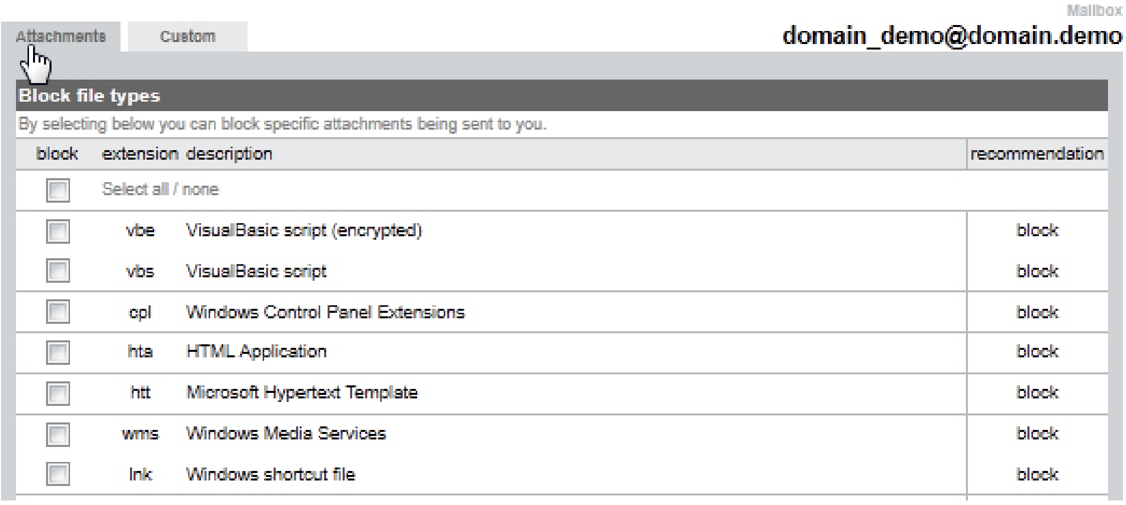
Use the **Domains** and **Hosts** tabs to add rules for blocking or allowing certain domains and IP addresses. The procedure is similar to the one for **Senders**.

> **Note**
> SpamFilter rules are also added when you use the whitelist options **Safe Sender** or **Safe Domain** in the *Email Quarantine Summary*.
> See "Whitelist Options" - page 29.

Content Filter

In the ContentFilter settings, you can set attachment rules or custom rules:

- **Attachments:** Click the checkboxes in the first column of the extensions list, to **block** certain file types.



domain_demo@domain.demo

Block file types

By selecting below you can block specific attachments being sent to you.

block	extension	description	recommendation
□	Select all / none		
□	vbe	VisualBasic script (encrypted)	block
□	vbs	VisualBasic script	block
□	cpl	Windows Control Panel Extensions	block
□	hta	HTML Application	block
□	htt	Microsoft Hypertext Template	block
□	wms	Windows Media Services	block
□	lnk	Windows shortcut file	block

The list contains the following recommendations:

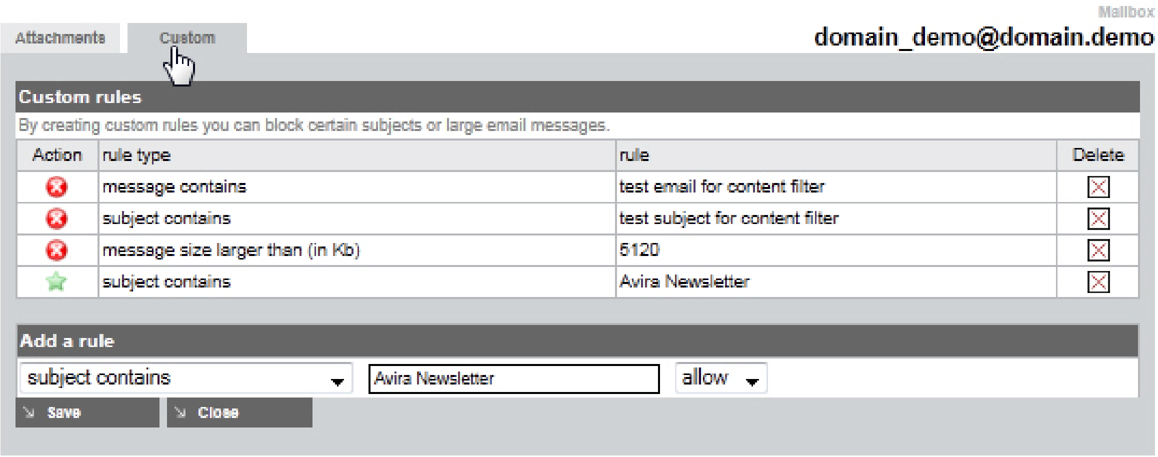
- *block*: you should block this type of attachment.

- *block if unsure*: if you are not sure whether you want to allow this kind of attachment, we recommend that you block it.

- *do not block*: attachments accepted by default; you can block them if you want.

To make the selection easier, you can use the option **Select all/ none**: Use it to select/ deselect all the extensions, and then click the ones you want to block/allow.

- **Custom:** You can create your own rules to **block** or **allow** emails



domain_demo@domain.demo

Custom rules

By creating custom rules you can block certain subjects or large email messages.

Action	rule type	rule	Delete
✖	message contains	test email for content filter	☒
✖	subject contains	test subject for content filter	☒
✖	message size larger than (in Kb)	5120	☒
☆	subject contains	Avira Newsletter	☒

Add a rule

subject contains ▾ | Avira Newsletter | allow ▾

To add a custom rule:

1. Select a filter criterion from the drop-down list:

   - **subject contains:** allows or blocks emails containing a certain subject.
   - **message contains:** allows or blocks emails containing a certain string.
   - **message size larger than:** blocks emails exceeding a maximum message size in Kb.

2. Type the text you want to filter for (e.g. `Avira Newsletter`) or the maximum message size (e.g. `5120`).

3. Select the rule type: **block** or **allow**.

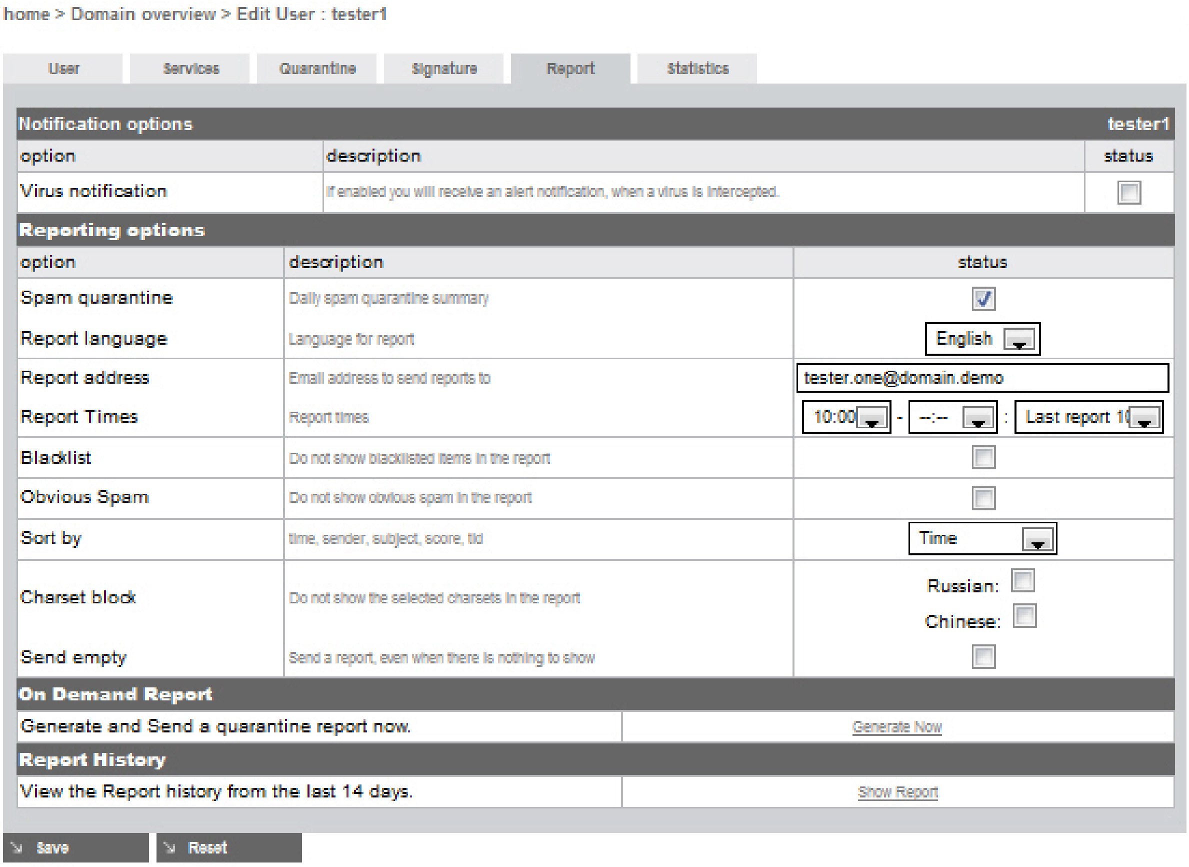
4. Click **Save**, to add the rule.

   The rules are listed under **Custom rules**, with type-symbols:
   ⊗ block (blacklist) or
   ☆ allow (whitelist).

To delete a rule, click the **X** mark in the **Delete** column and click **OK** in the pop-up window.

4.2 Setting up virus and spam notifications

1. To schedule a report, select a **User** then click the **Report** tab.



Notification options		tester1
option	description	status
Virus notification	If enabled you will receive an alert notification, when a virus is intercepted.	□

Reporting options		
option	description	status
Spam quarantine	Daily spam quarantine summary	☑
Report language	Language for report	English
Report address	Email address to send reports to	tester.one@domain.demo
Report Times	Report times	10:00 - --:-- : Last report 10
Blacklist	Do not show blacklisted items in the report	□
Obvious Spam	Do not show obvious spam in the report	□
Sort by	time, sender, subject, score, tid	Time
Charset block	Do not show the selected charsets in the report	Russian: □ Chinese: □
Send empty	Send a report, even when there is nothing to show	□

On Demand Report	
Generate and Send a quarantine report now.	Generate Now

Report History	
View the Report history from the last 14 days.	Show Report

2. Enable **Virus notification**, to receive a warning by email, whenever a virus is intercepted.

3. Enable **Spam quarantine** to receive a daily summary of intercepted spam, according to the settings you make under *Reporting options*:

- **Report language** - currently you can choose between: English, German, Spanish, French and Dutch.
- **Report address** - insert one email address, to which AMES will send virus notifications and spam summary.
- **Report Times** - by default, AMES sends the spam summary twice a day (e.g. `08:00`, `16:00`). You can select different times or disable one of them.
  Further options for the report times:

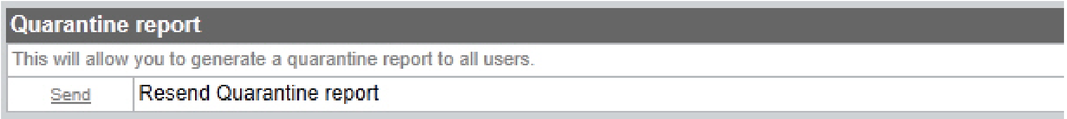
  - `Last report 100` - list of 100 items since the last report.
  - `Last report 500` - list of 500 items since the last report.
  - `Last 100 items` - list of the last 100 items.
  - `Last 500 items` - list of the last 500 items.
- **Blacklist** - AMES does not display the blacklisted items in the summary, if you enable this option.
- **Obvious Spam** - AMES does not display items with a high spam score in the summary, if you enable this option.
- **Sort by** - select a criterion to sort the summary list: `Time`, `Sender`, `Subject`, `Score`, `TLD` (top level domain).
- **Charset block** - AMES does not display **Russian** or **Chinese** charsets in the summary, if you enable these options.
- **Send empty** - AMES sends a report, even if there is nothing to show.

4. When done click **Save**.

> **Warning**
> We advise that you let AMES generate a report on a daily basis, especially when you have just started using AMES or if you use severe filtering settings for spam.

5. Click **Generate Now**, if you want to receive the quarantine summary per email immediately. To view a report history of the last 14 days, click **Show Report**.

As Avira-Partner or AMES domain administrator, you can generate a quarantine report and send it to all users of a domain: Go to the **Domain overview > Services**, scroll down to the *Quarantine report* section and click **Send**.



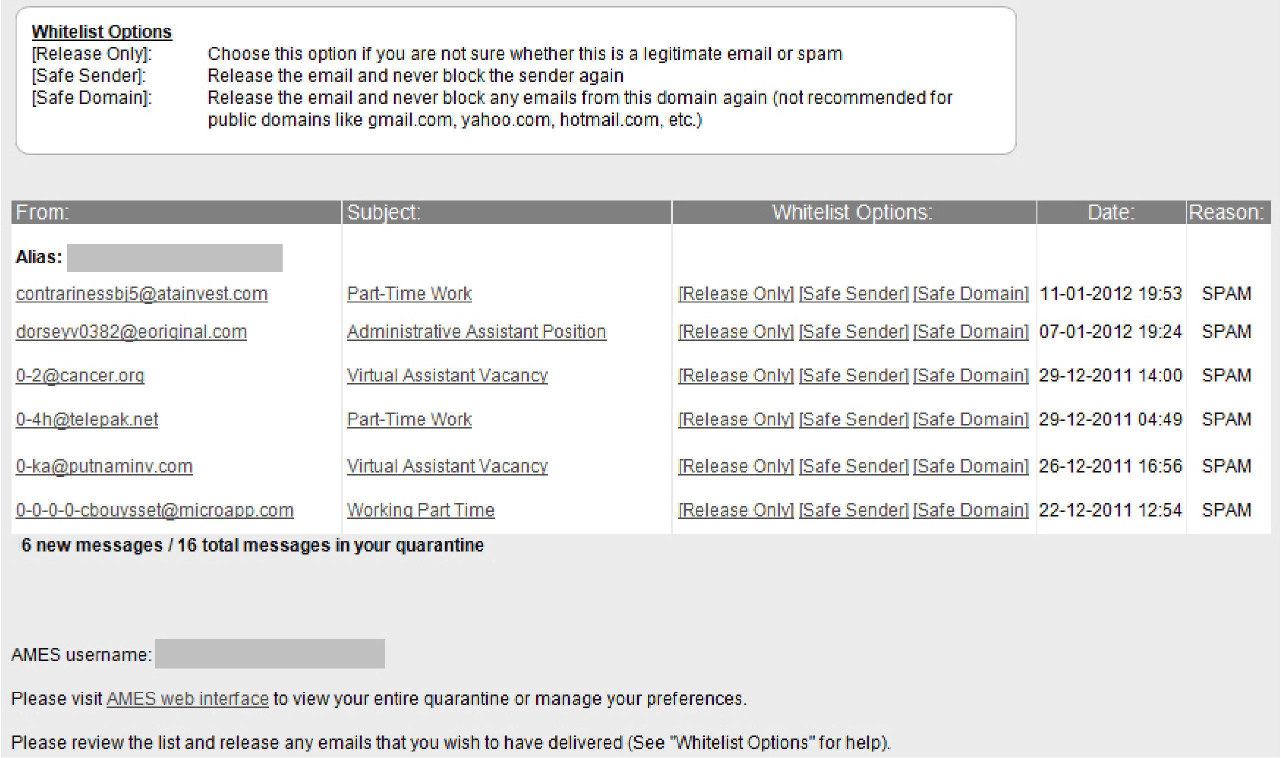
Quarantine report

This will allow you to generate a quarantine report to all users.

Send	Resend Quarantine report

4.3 Managing the quarantines directly from your email account

Once the daily summary report is activated, the user receives an email every day, as scheduled, with the list of eventual new spam messages.



Whitelist Options

[Release Only]: Choose this option if you are not sure whether this is a legitimate email or spam

[Safe Sender]: Release the email and never block the sender again

[Safe Domain]: Release the email and never block any emails from this domain again (not recommended for public domains like gmail.com, yahoo.com, hotmail.com, etc.)

From:	Subject:	Whitelist Options:	Date:	Reason:
Alias: [redacted]				
contrarinessbj5@atainvest.com	Part-Time Work	[Release Only] [Safe Sender] [Safe Domain]	11-01-2012 19:53	SPAM
dorseyv0382@eoriginal.com	Administrative Assistant Position	[Release Only] [Safe Sender] [Safe Domain]	07-01-2012 19:24	SPAM
0-2@cancer.org	Virtual Assistant Vacancy	[Release Only] [Safe Sender] [Safe Domain]	29-12-2011 14:00	SPAM
0-4h@telepak.net	Part-Time Work	[Release Only] [Safe Sender] [Safe Domain]	29-12-2011 04:49	SPAM
0-ka@putnaminv.com	Virtual Assistant Vacancy	[Release Only] [Safe Sender] [Safe Domain]	26-12-2011 16:56	SPAM
0-0-0-0-cbouysset@microapp.com	Working Part Time	[Release Only] [Safe Sender] [Safe Domain]	22-12-2011 12:54	SPAM

6 new messages / 16 total messages in your quarantine

AMES username: [redacted]

Please visit AMES web interface to view your entire quarantine or manage your preferences.

Please review the list and release any emails that you wish to have delivered (See "Whitelist Options" for help).

Whitelist Options

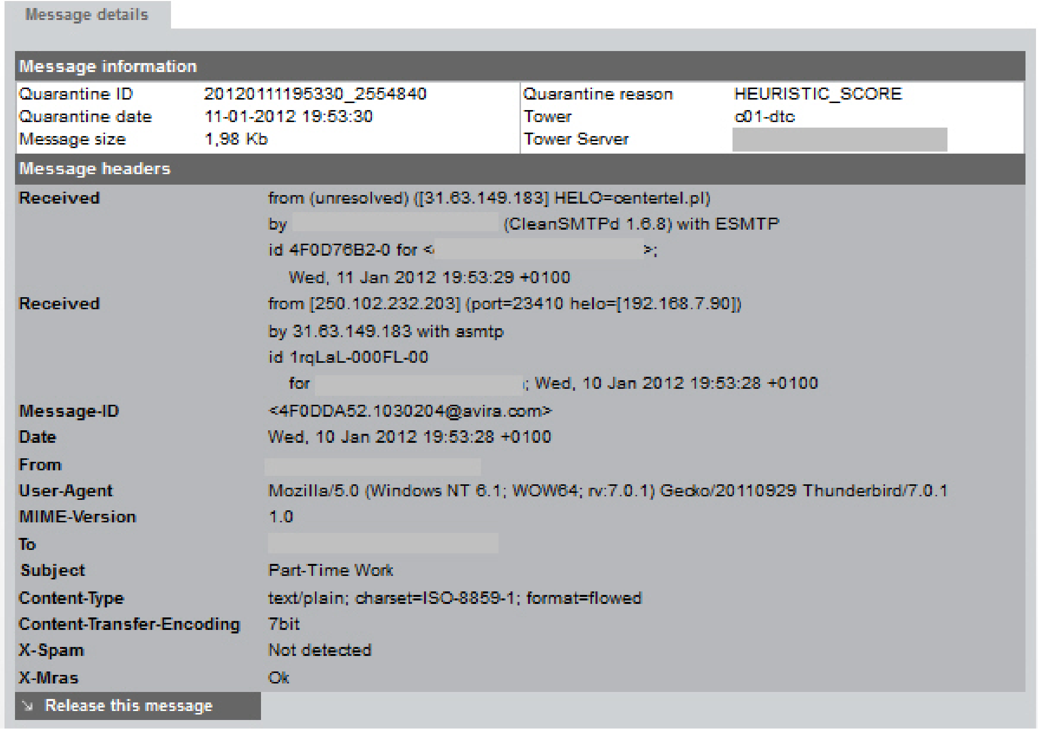
You can manage your quarantine directly from your email client, by using the links in the **Whitelist Options** column of the Quarantine Summary:

- Click **Release Only**, to deliver the quarantined email to your inbox.
- Click **Safe Sender**, to deliver the quarantined email to your inbox and to add the sender to the whitelist of your AMES SpamFilter, so the sender will never be blocked again.
- Click **Safe Domain**, to deliver the quarantined email to your inbox and to add the sender's domain to the whitelist of your AMES SpamFilter, so the domain will never be blocked again.

Warning
It is not recommended to use the **Safe Domain** option for public domains, such as gmail.com, yahoo.com, hotmail.com, etc.

If you wish to view your entire quarantine or manage your preferences, you can click the link to the **AMES web interface**, which opens the login page to your AMES account.

You can first check the details of the quarantined message, by clicking its subject (e.g. `Part-Time Work`) in the **Subject** column of the Quarantine Summary.



Message information

Quarantine ID	20120111195330_2554840	Quarantine reason	HEURISTIC_SCORE
Quarantine date	11-01-2012 19:53:30	Tower	c01-dtc
Message size	1,98 Kb	Tower Server	[redacted]

Message headers

Received	from (unresolved) ([31.63.149.183] HELO=centertel.pl) by [redacted] (CleanSMTPd 1.6.8) with ESMTP id 4F0D76B2-0 for < [redacted] >; Wed, 11 Jan 2012 19:53:29 +0100

Received	from [250.102.232.203] (port=23410 helo=[192.168.7.90])
	by 31.63.149.183 with asmtp
	id 1rqLaL-000FL-00
	for [redacted]; Wed, 10 Jan 2012 19:53:28 +0100

Message-ID	<4F0DDA52.1030204@avira.com>
Date	Wed, 10 Jan 2012 19:53:28 +0100
From	[redacted]
User-Agent	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:7.0.1) Gecko/20110929 Thunderbird/7.0.1
MIME-Version	1.0
To	[redacted]
Subject	Part-Time Work
Content-Type	text/plain; charset=ISO-8859-1; format=flowed
Content-Transfer-Encoding	7bit
X-Spam	Not detected
X-Mras	Ok

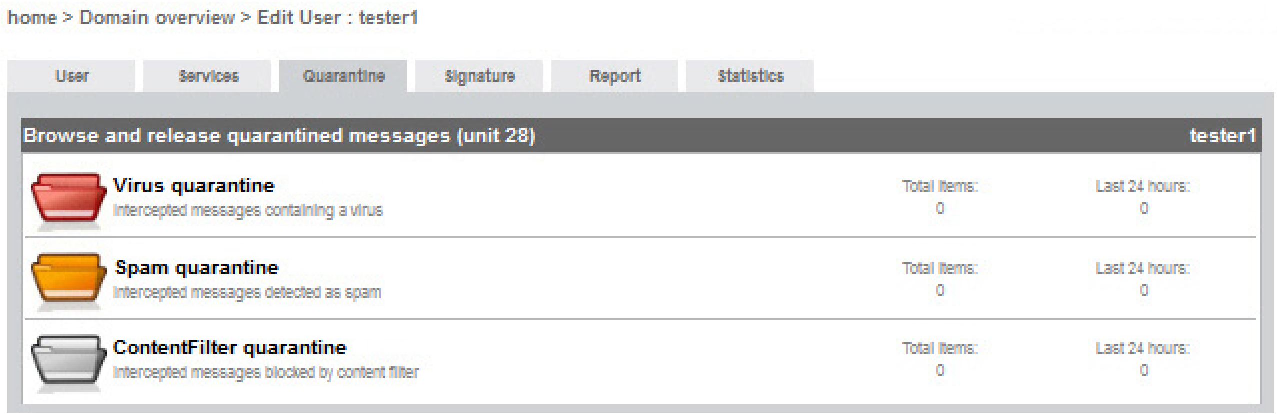
After checking the message details, like *Quarantine reason* and *Message headers*, you can still decide to release the message from quarantine, by clicking **Release this message**.

If the **Virus notification** feature is enabled, the user receives a warning by email, each time a virus is detected in an incoming message. The warning contains details about the infected message and a link to the malware description on the Avira website.

The user can check the **Virus quarantine** in the AMES account, to delete or release the quarantined email within 14 days.

4.4 Managing the quarantines from your AMES account

To open the quarantine, select a **User** then go to the **Quarantine** tab.



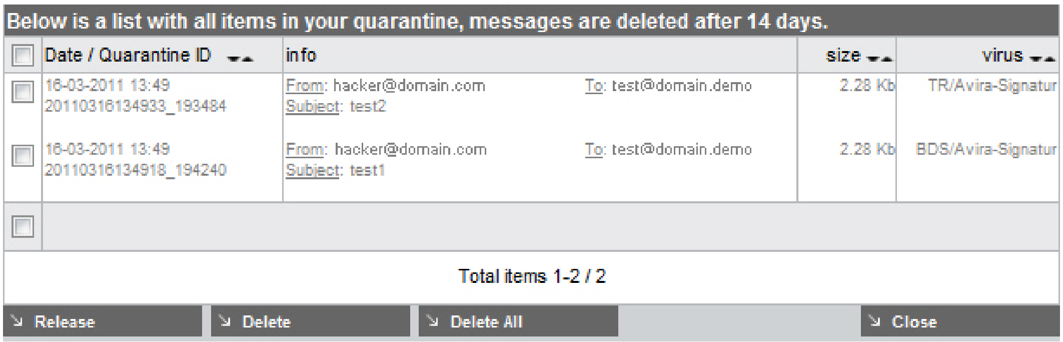
Browse and release quarantined messages (unit 28) tester1

Virus quarantine Intercepted messages containing a virus	Total items: 0	Last 24 hours: 0
Spam quarantine Intercepted messages detected as spam	Total items: 0	Last 24 hours: 0
ContentFilter quarantine Intercepted messages blocked by content filter	Total items: 0	Last 24 hours: 0

AMES has three different quarantines, for different types of filtering. Click the name of each quarantine, to check its contents.

Virus quarantine

If your account is set to quarantine infected emails for 14 days, the **Virus quarantine** stores all emails with virus signatures.



Below is a list with all items in your quarantine, messages are deleted after 14 days.

□	Date / Quarantine ID	info		size	virus
□	16-03-2011 13:49 20110316134933_193484	From: hacker@domain.com Subject: test2	To: test@domain.demo	2.28 Kb	TR/Avira-Signatur
□	16-03-2011 13:49 20110316134918_194240	From: hacker@domain.com Subject: test1	To: test@domain.demo	2.28 Kb	BDS/Avira-Signatur
□					

Total items 1-2 / 2

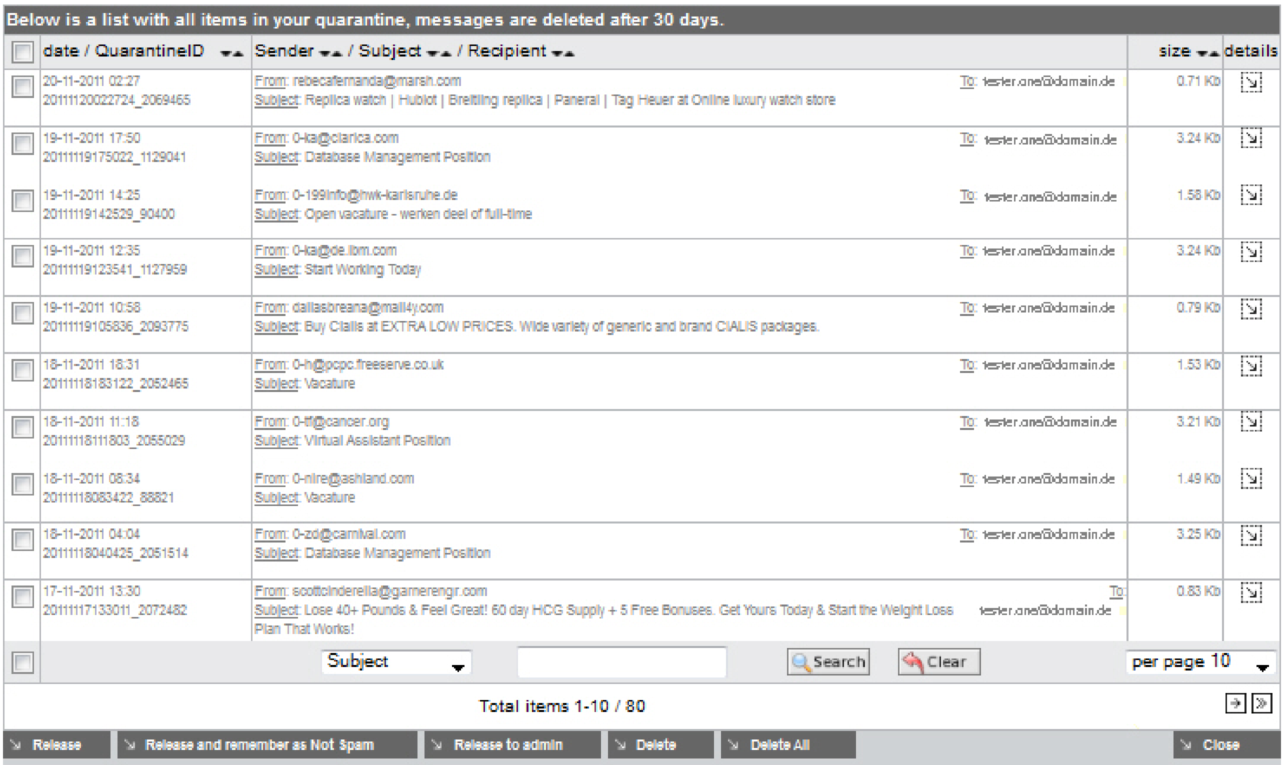
To delete specific emails, select the items in the list and click **Delete.** To delete all the messages in this quarantine, click **Delete All**. AMES will automatically delete infected emails older than 14 days.

Warning

If you doubt whether a specific email contains a virus, do not release it. The virus filtering in AMES is almost never wrong. In case you decide an email is not infected, select it and click **Release** to deliver it to your inbox.

Spam quarantine

If your account is set to quarantine spam emails for 30 days, the **Spam quarantine** stores all intercepted spam emails.



Below is a list with all items in your quarantine, messages are deleted after 30 days.

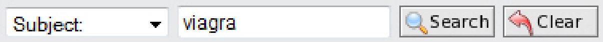
□	date / QuarantineID	Sender / Subject / Recipient		size	details
□	20-11-2011 02:27 20111120022724_2069465	From: rebecafernanda@marsh.com Subject: Replica watch | Hublot | Breitling replica | Panerai | Tag Heuer at Online luxury watch store	To: tester.one@domain.de	0.71 Kb	↘
□	19-11-2011 17:50 20111119175022_1129041	From: 0-ka@clarica.com Subject: Database Management Position	To: tester.one@domain.de	3.24 Kb	↘
□	19-11-2011 14:25 20111119142529_90400	From: 0-199info@hwk-karlsruhe.de Subject: Open vacature - werken deel of full-time	To: tester.one@domain.de	1.58 Kb	↘
□	19-11-2011 12:35 20111119123541_1127959	From: 0-ka@de.ibm.com Subject: Start Working Today	To: tester.one@domain.de	3.24 Kb	↘
□	19-11-2011 10:58 20111119105836_2093775	From: dallasbreana@mail4y.com Subject: Buy Cialis at EXTRA LOW PRICES. Wide variety of generic and brand CIALIS packages.	To: tester.one@domain.de	0.79 Kb	↘
□	18-11-2011 18:31 20111118183122_2052465	From: 0-h@pcpc.freeserve.co.uk Subject: Vacature	To: tester.one@domain.de	1.53 Kb	↘
□	18-11-2011 11:18 20111118111803_2055029	From: 0-tf@cancer.org Subject: Virtual Assistant Position	To: tester.one@domain.de	3.21 Kb	↘
□	18-11-2011 08:34 20111118083422_88821	From: 0-nlre@ashland.com Subject: Vacature	To: tester.one@domain.de	1.49 Kb	↘
□	18-11-2011 04:04 20111118040425_2051514	From: 0-zd@carnival.com Subject: Database Management Position	To: tester.one@domain.de	3.25 Kb	↘
□	17-11-2011 13:30 20111117133011_2072482	From: scottcinderella@garnerengr.com Subject: Lose 40+ Pounds & Feel Great! 60 day HCG Supply + 5 Free Bonuses. Get Yours Today & Start the Weight Loss Plan That Works!	To: tester.one@domain.de	0.83 Kb	↘

□ Subject ▾ Search Clear per page 10 ▾

Total items 1-10 / 80

To delete specific emails, select the items in the list and click **Delete.** To delete all the messages in this quarantine, click **Delete All**. AMES will automatically delete spam emails after 30 days.

You can also filter the list by ID, sender, recipient or subject, using the **Search** feature: Select the filter criterion in the drop-down list (**QuarantineID**, **Sender**, **Recipient**, **Subject**), insert the string you are searching for (e.g. `viagra`) and press **Search**. If you want to delete the filter string and return to the initial list, click **Clear**.



Subject: ▾ viagra

To release selected emails from the quarantine:

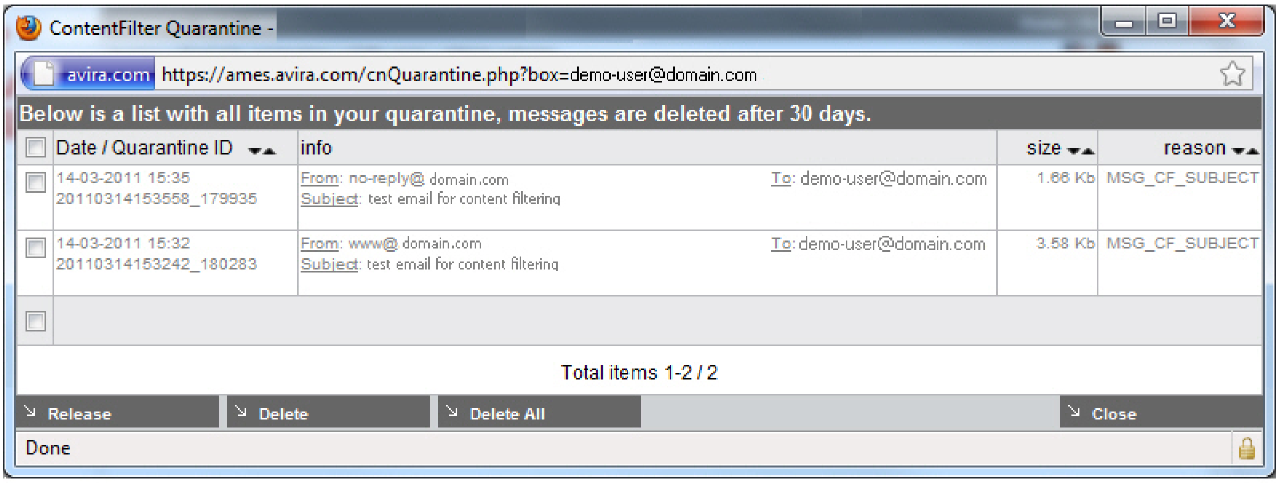
- Click **Release**, to deliver the selected email to your inbox.
- Click **Release and remember as Not Spam**, to deliver the selected emails to your inbox and no longer recognize emails from these senders as spam. Note, that this action will reduce the effectiveness of the spam filtering.
- Click **Release to admin**, to deliver the selected emails to your domain administrator, who can check them for you.

Note

You can completely rely on AMES default settings, but if needed, you can customize them. If you set the spam filter too high, your spam quarantine could also intercept **ham**. 'Ham' is email falsely identified as spam. If you get ham in your quarantine, or receive emails falsely tagged as spam in your email client, you might want to check the Advanced settings of the SpamFilter (see "SpamFilter" - page 24).

Content Filter quarantine

In the **ContentFilter quarantine** you will find all blocked emails, based on size, attachment or your own customized rules.



ContentFilter Quarantine -

avira.com https://ames.avira.com/cnQuarantine.php?box=demo-user@domain.com

Below is a list with all items in your quarantine, messages are deleted after 30 days.

□	Date / Quarantine ID	info	size	reason
□	14-03-2011 15:35 20110314153558_179935	From: no-reply@ domain.com To: demo-user@domain.com Subject: test email for content filtering	1.66 Kb	MSG_CF_SUBJECT
□	14-03-2011 15:32 20110314153242_180283	From: www@ domain.com To: demo-user@domain.com Subject: test email for content filtering	3.58 Kb	MSG_CF_SUBJECT
□				

Total items 1-2 / 2

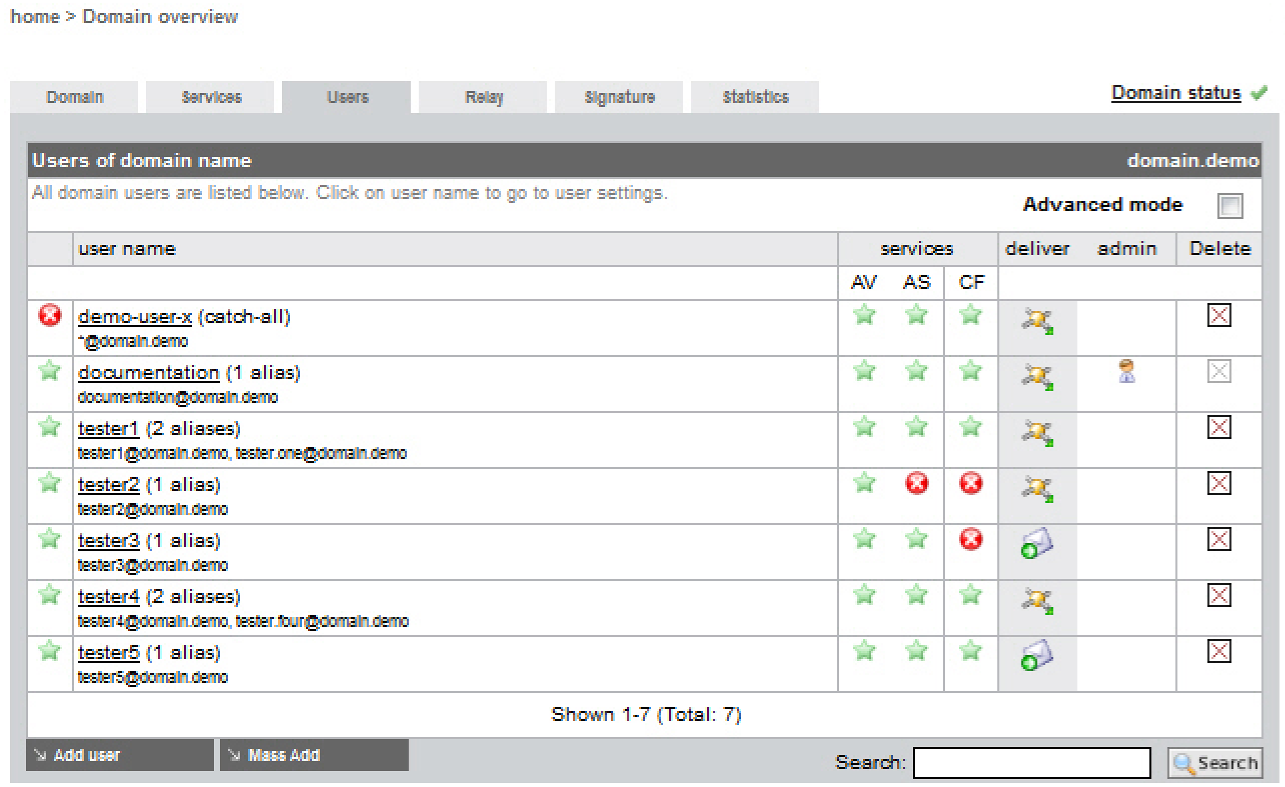
If you decide to deliver a selected email to your inbox, click **Release.**

To delete specific emails, select the items in the list and click **Delete.** To delete all the messages in this quarantine, click **Delete All**. AMES will automatically delete content-blocked emails after 30 days.

5. User management

As Avira partner or AMES domain administrator, you can manage all the users of a domain in the **Domain overview**, on the **Users** tab.

The default view displays a list of the users and the services status for each user:



home > Domain overview

Users of domain name — domain.demo

All domain users are listed below. Click on user name to go to user settings.

Advanced mode □

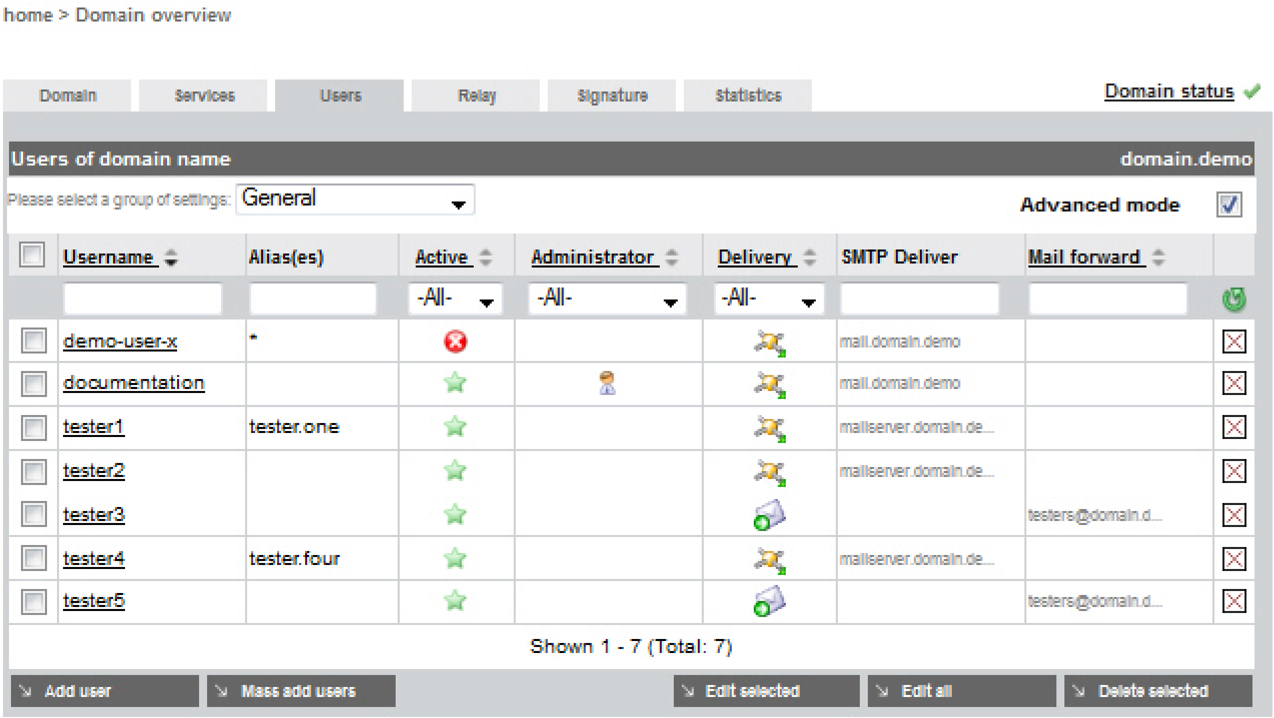
	user name	services			deliver	admin	Delete
		AV	AS	CF			
✖	demo-user-x (catch-all) *@domain.demo	★	★	★	⇄		☒
★	documentation (1 alias) documentation@domain.demo	★	★	★	⇄	👤	☒
★	tester1 (2 aliases) tester1@domain.demo, tester.one@domain.demo	★	★	★	⇄		☒
★	tester2 (1 alias) tester2@domain.demo	★	✖	✖	⇄		☒
★	tester3 (1 alias) tester3@domain.demo	★	★	✖	✉		☒
★	tester4 (2 aliases) tester4@domain.demo, tester.four@domain.demo	★	★	★	⇄		☒
★	tester5 (1 alias) tester5@domain.demo	★	★	★	✉		☒

Shown 1-7 (Total: 7)

- active ★ or inactive user ✖;
- user’s name and aliases (clicking a user’s name, takes you to the user level of the AMES interface);
- active services: VirusFilter (AV), SpamFilter (AS), ContentFilter (CF);
- email delivery method (SMTP ⇄ or Forward ✉);
- symbol for domain administrators 👤.

5.1 User management in advanced mode

If you enable the **Advanced mode** option, you can easily configure the services for single or multiple users in just three steps.



Users of domain name domain.demo

Please select a group of settings: General

Advanced mode ☑

☐	Username	Alias(es)	Active	Administrator	Delivery	SMTP Deliver	Mail forward	
			-All-	-All-	-All-			
☐	demo-user-x	*	✗			mail.domain.demo		☒
☐	documentation		★	👤		mail.domain.demo		☒
☐	tester1	tester.one	★			mailserver.domain.de...		☒
☐	tester2		★			mailserver.domain.de...		☒
☐	tester3		★				testers@domain.d...	☒
☐	tester4	tester.four	★			mailserver.domain.de...		☒
☐	tester5		★				testers@domain.d...	☒

Shown 1 - 7 (Total: 7)

1. **First, select the group of settings** from the drop-down list above the table:

   - General

   - Services

   - Filter options

   - Blacklist

   - Whitelist

   - Report general

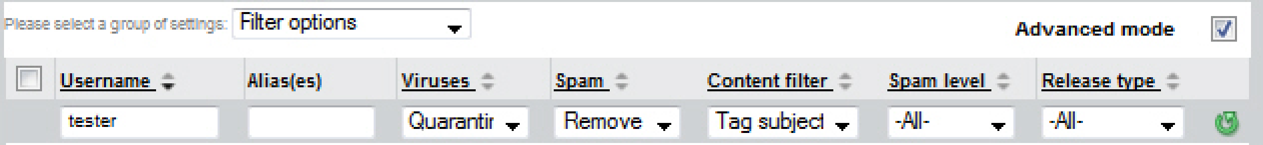
   - Report content

2. **Then, select the users you want to edit**:

   Click the checkboxes in the first column, to select the users. You can use the checkbox in the table header, to select or deselect all users.

   To sort the users list by the contents of a column, click the column header once or twice: one of the two grey arrows in the header turns black ⬍ , to indicate the ascending or descending sort order.

To filter the list by certain criteria, use one or more fields below the column headers.



Please select a group of settings: Filter options

Advanced mode ☑

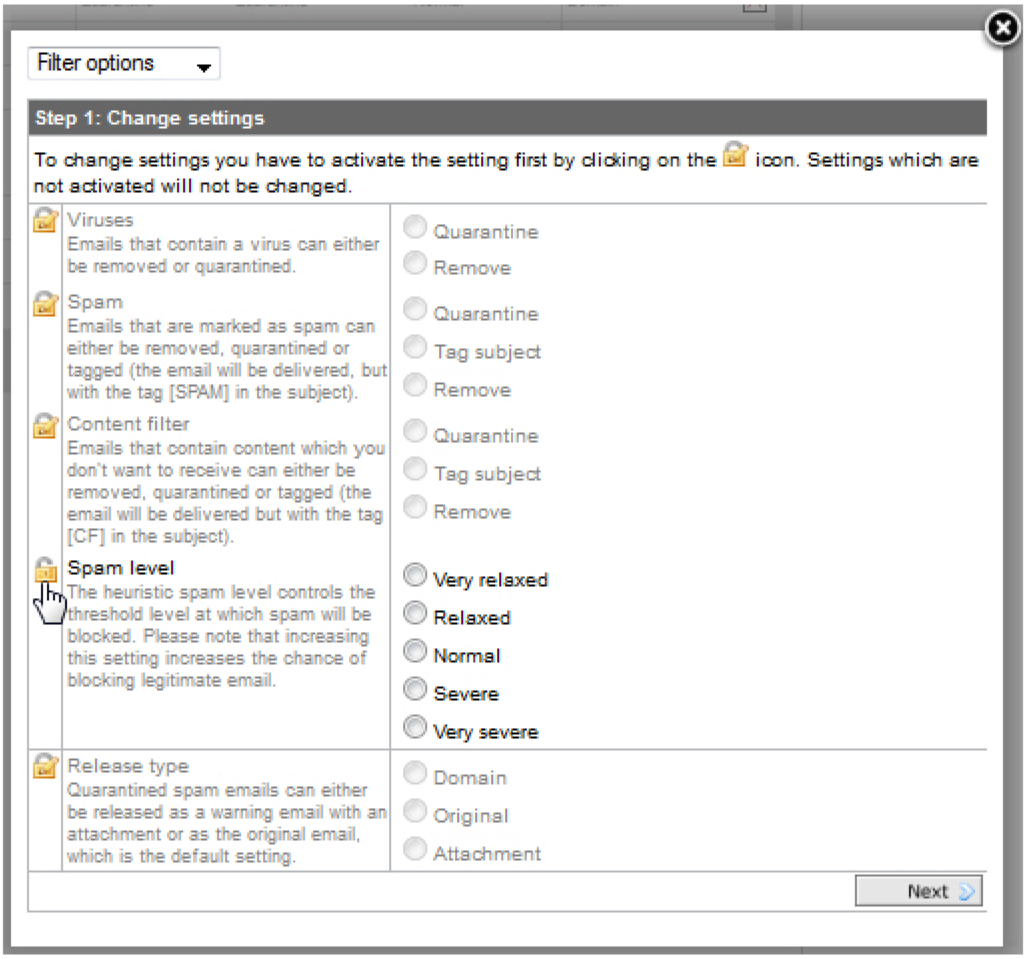
☐	Username	Alias(es)	Viruses	Spam	Content filter	Spam level	Release type
	tester		Quarantir	Remove	Tag subject	-All-	-All-

To clear all the filters and display the entire users list again, click the **Reset filters** button.

3. **Finally, make the changes to the users' settings**:

   If you just want to delete the selected users, click **Delete selected** then press **OK** to confirm the action.

   Click the **Edit selected** button, to start editing the services for the selected users. You can directly click **Edit all**, if the changes should apply to all users in the list.



Filter options

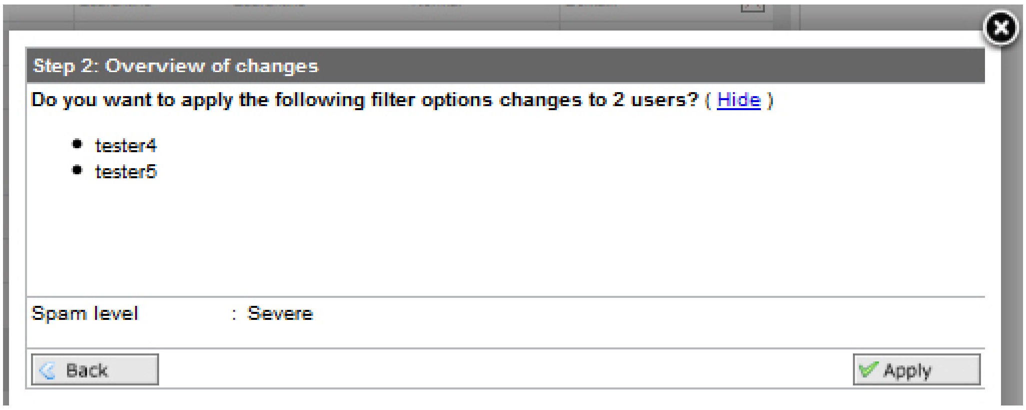
Step 1: Change settings

To change settings you have to activate the setting first by clicking on the icon. Settings which are not activated will not be changed.

Viruses Emails that contain a virus can either be removed or quarantined.	○ Quarantine ○ Remove
Spam Emails that are marked as spam can either be removed, quarantined or tagged (the email will be delivered, but with the tag [SPAM] in the subject).	○ Quarantine ○ Tag subject ○ Remove
Content filter Emails that contain content which you don't want to receive can either be removed, quarantined or tagged (the email will be delivered but with the tag [CF] in the subject).	○ Quarantine ○ Tag subject ○ Remove
Spam level The heuristic spam level controls the threshold level at which spam will be blocked. Please note that increasing this setting increases the chance of blocking legitimate email.	○ Very relaxed ○ Relaxed ○ Normal ○ Severe ○ Very severe
Release type Quarantined spam emails can either be released as a warning email with an attachment or as the original email, which is the default setting.	○ Domain ○ Original ○ Attachment

4. Click the **Edit** icons in the first column of the settings sheet and select the option you want to activate for the selected users.

5. Click **Next** to review the changes.



Step 2: Overview of changes

Do you want to apply the following filter options changes to 2 users? (Hide)

- tester4
- tester5

Spam level : Severe

6. You can click **Show** or **Hide**, to display or to hide the list of selected users in the overview window.

7. Click **Apply**, then **Close**.

   The changes you made will be updated in the **Users** view.

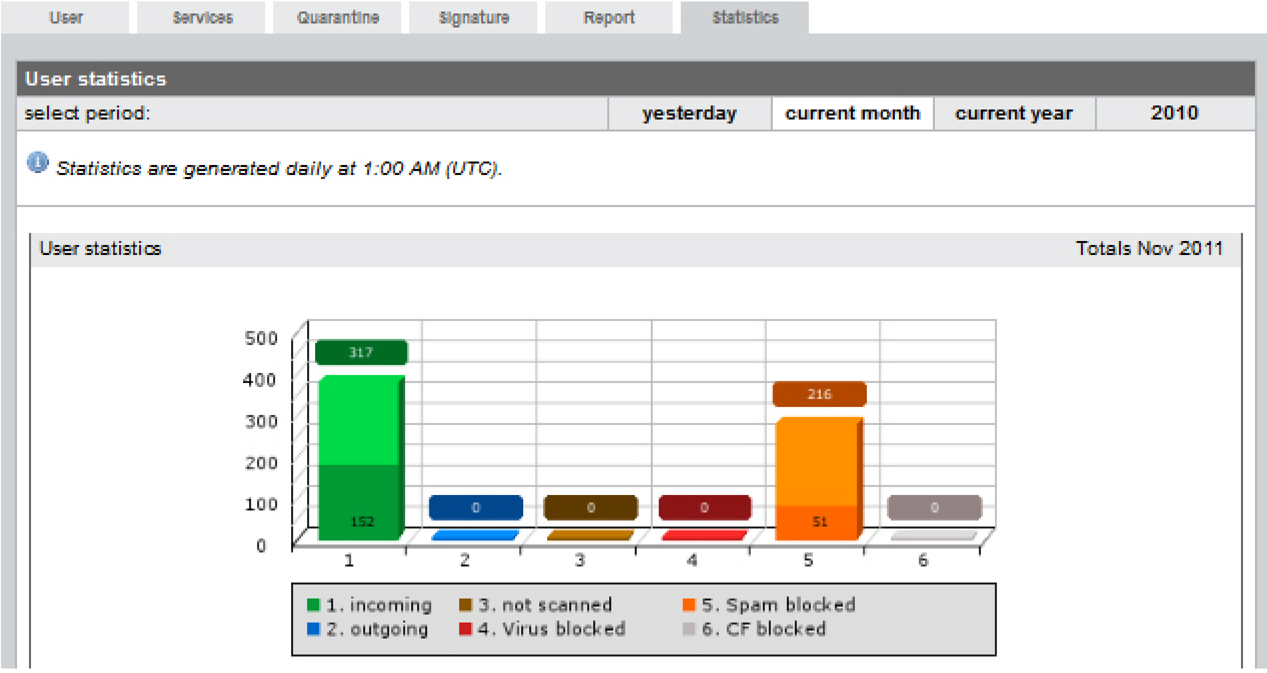
Overview of the settings available in Advanced mode

Groups of settings	Settings	Options
General	(See 3.3 Adding new users to a domain - page 12)	
	Active	Yes / No
	Administrator	Yes / No
	Delivery	SMTP Deliver (+ hostname or IP) Mail forward (+ email address)
Services	(See 3.3 Adding new users to a domain - page 12)	
	VirusScan	Enabled / Disabled
	SpamFilter	Enabled / Disabled
	ContentFilter	Enabled / Disabled
Filter options	(See 4.1 Configuring the email filters - page 22)	
	Viruses	Quarantine / Remove
	Spam	Quarantine Tag subject Remove
	Content filter	Quarantine Tag subject Remove

Groups of settings	Settings	Options
	Spam level	Very relaxed Relaxed Normal Severe Very severe
	Release type	Domain Original Attachment
Blacklist / Whitelist	(See 4.1.2 Adjusting the filter settings - page 24)	
	Senders	Add entries / Delete entries (+ sender addresses)
	Domains	Add entries / Delete entries (+ sender domains)
	Hosts	Add entries / Delete entries (+ hosts)
Report general	(See 4.2 Setting up virus and spam notifications - page 27)	
	Virus notification	Enabled / Disabled
	Quarantine report	Enabled / Disabled
	Language	English / German
	Recipient	Use the box address of each user Use a general address for all users (+ email address)
	Report Times	Time of day
Report content	(See 4.2 Setting up virus and spam notifications - page 27)	
	Report contents	Last report 100 Last report 500 Last 100 items Last 500 items
	Blacklisted	Show / Hide
	Obvious Spam	Show / Hide
	Character-set	None Russian Chinese Both
	Empty report	Enabled / Disabled

6. Statistics

AMES creates statistics regarding the scanned emails, intercepted viruses, spam and filtered content, **per domain** and **per user**. Click the **Statistics** tab, to check them out.



Statistics are generated daily at 1:00 AM (UTC).

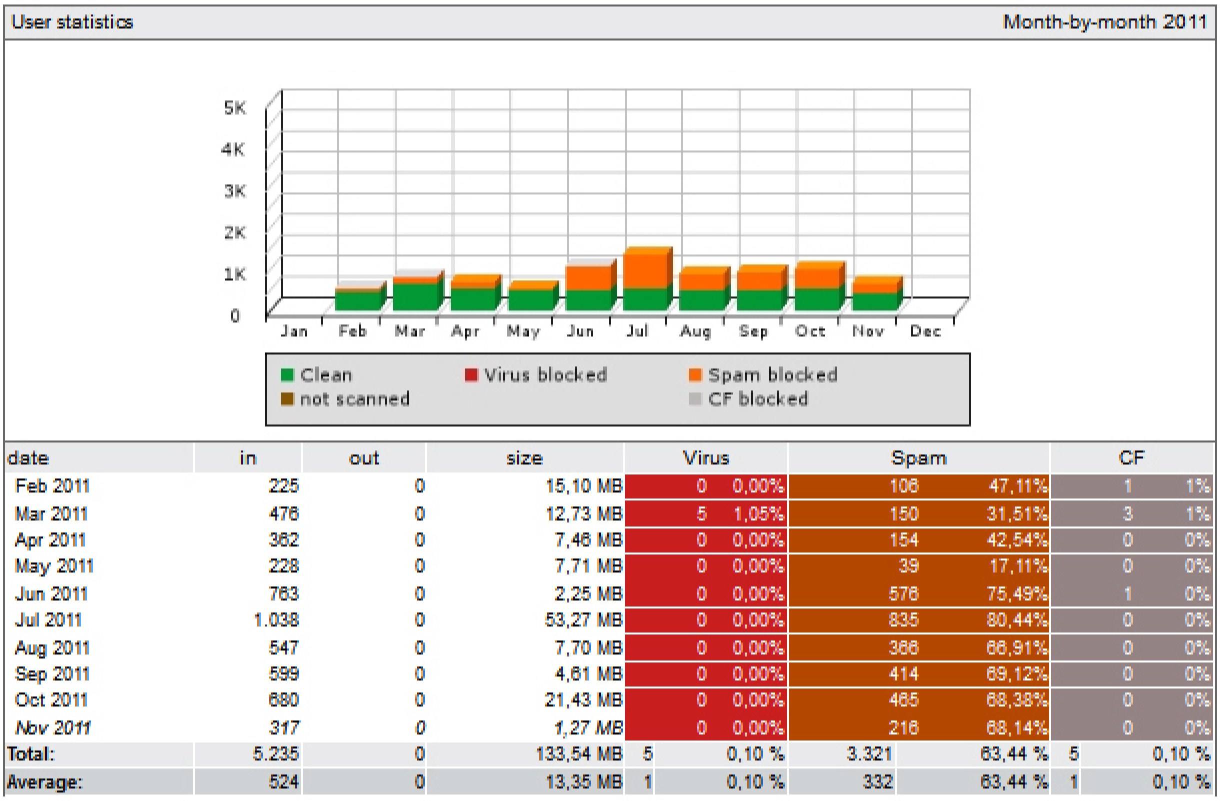
The information about the processed emails is divided into:

- **incoming** (green) - the amount of incoming emails; the dark-green segment represents the incoming emails, for which greylisting was NOT applied. Greylisting is only applied to catch-all users. See "Greylisting" - page 17.
- **outgoing** (blue) - the amount of outgoing emails, if the relay service is enabled. See 2.4 Scanning outgoing emails - page 9.
- **not scanned** (brown) - the amount of not scanned emails, due to disabled filters.
- **Virus blocked** (red) - the amount of emails intercepted by the Virus Filter.
- **Spam blocked** (orange) - the amount of emails intercepted by the Spam Filter, including blacklisted items; the dark-orange segment represents the emails stored in the spam quarantine.
- **CF blocked** (grey) - the amount of emails intercepted by the Content Filter.

> **Note**
> Statistics are generated daily at 1:00 AM (UTC).

You can change the time range of the statistics, using the **select period** menu: **yesterday**, **current month**, **last month**, **current year**, or the previous year.

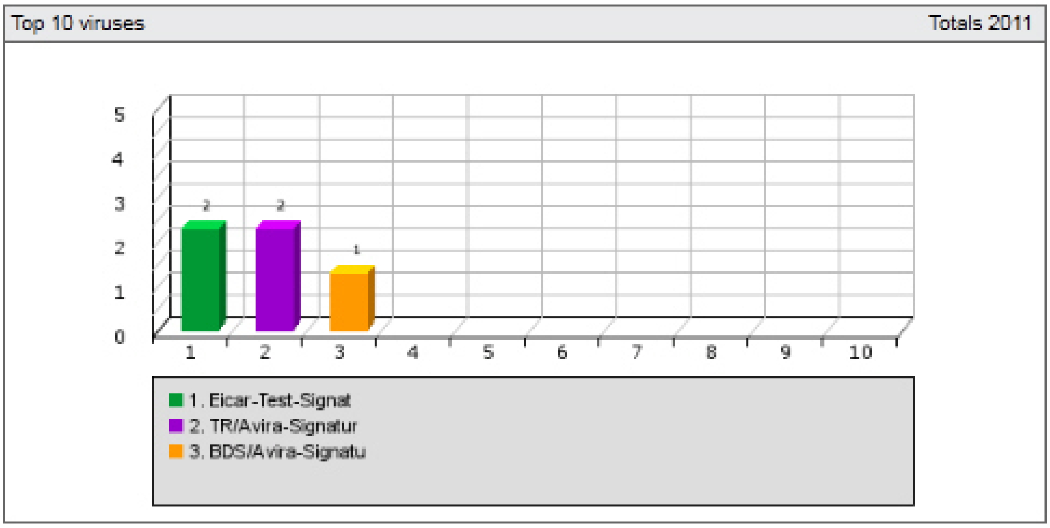
If you select for example, the current month, **day-by-day statistics** are also available for the selected user or domain. Similarly, if you select a year, you can see **month-by-month statistics**, for a user or domain.



User statistics Month-by-month 2011

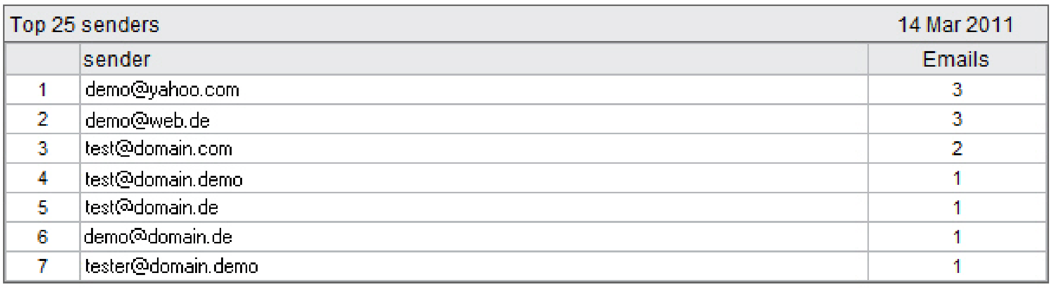
date	in	out	size	Virus		Spam		CF	
Feb 2011	225	0	15,10 MB	0	0,00%	106	47,11%	1	1%
Mar 2011	476	0	12,73 MB	5	1,05%	150	31,51%	3	1%
Apr 2011	362	0	7,46 MB	0	0,00%	154	42,54%	0	0%
May 2011	228	0	7,71 MB	0	0,00%	39	17,11%	0	0%
Jun 2011	763	0	2,25 MB	0	0,00%	576	75,49%	1	0%
Jul 2011	1.038	0	53,27 MB	0	0,00%	835	80,44%	0	0%
Aug 2011	547	0	7,70 MB	0	0,00%	366	66,91%	0	0%
Sep 2011	599	0	4,61 MB	0	0,00%	414	69,12%	0	0%
Oct 2011	680	0	21,43 MB	0	0,00%	465	68,38%	0	0%
Nov 2011	*317*	*0*	*1,27 MB*	0	0,00%	216	68,14%	0	0%
Total:	5.235	0	133,54 MB	5	0,10 %	3.321	63,44 %	5	0,10 %
Average:	524	0	13,35 MB	1	0,10 %	332	63,44 %	1	0,10 %

You can also check the report on the **Top 10 viruses** that have been intercepted by AMES in the selected period.

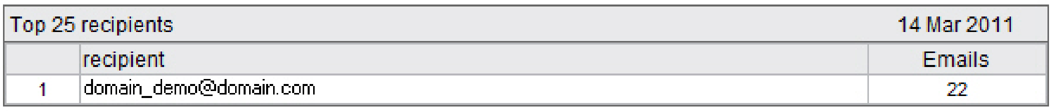


Top 10 viruses Totals 2011

Further statistics display the **Top 25 senders** and **Top 25 recipients** of emails during the selected period.



Top 25 senders		14 Mar 2011
	sender	Emails
1	demo@yahoo.com	3
2	demo@web.de	3
3	test@domain.com	2
4	test@domain.demo	1
5	test@domain.de	1
6	demo@domain.de	1
7	tester@domain.demo	1



Top 25 recipients		14 Mar 2011
	recipient	Emails
1	domain_demo@domain.com	22

7. Support

Support service

All necessary information on our comprehensive support service can be obtained from our website http://www.avira.com.

FAQs

Please also read the FAQ section on our website.
Your questions may already have been asked and answered by other users in this section.

Please contact your Avira Partner - they will be more than willing to help you with any further questions regarding Avira products.

Contact

Address

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

Internet

You can find further information about us and our products at the following address:
http://www.avira.com

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 Q1-2012

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