



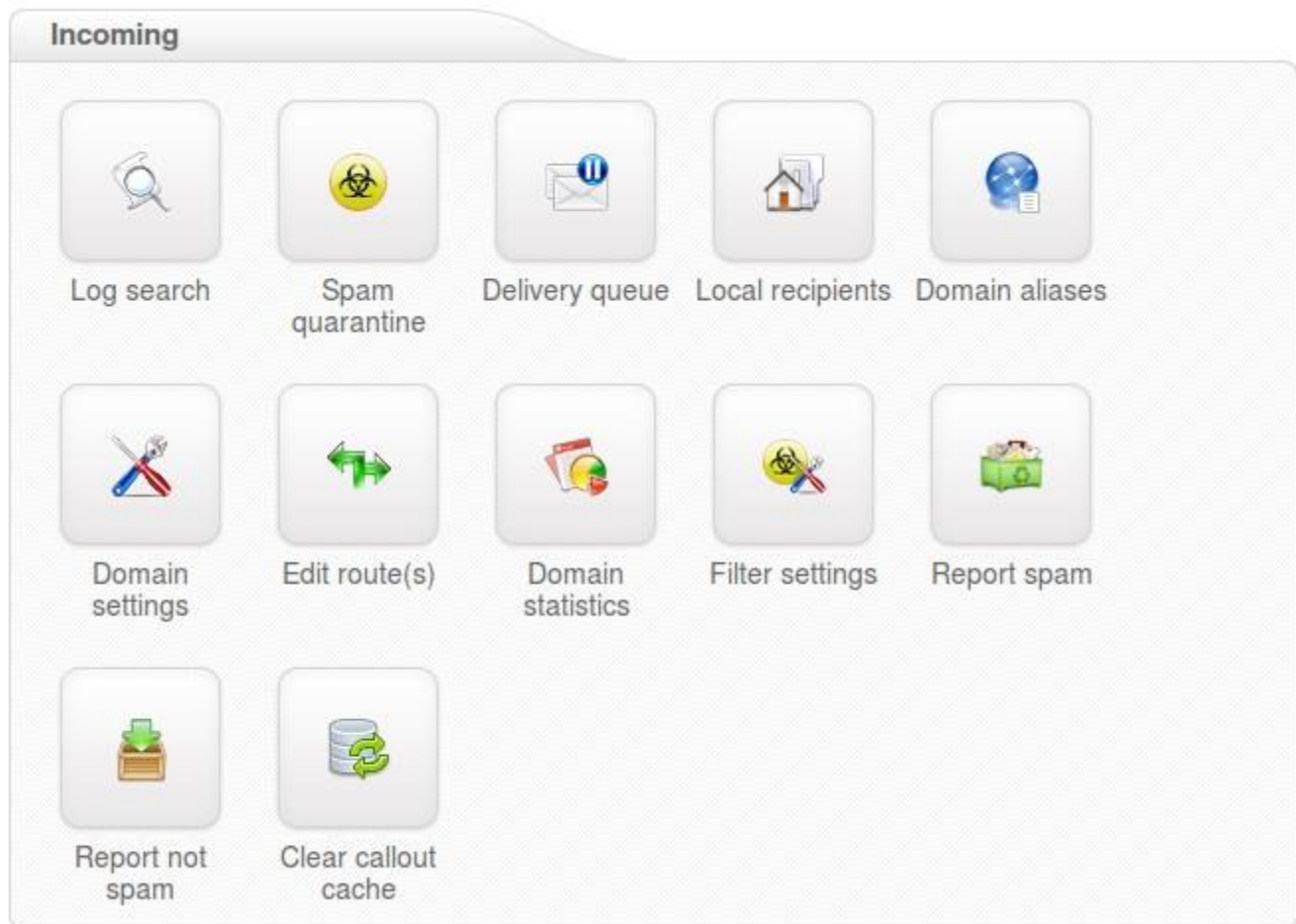
Administrator Guide

Table of Contents

Incoming.....	2
Incoming Spam Quarantine	3
Incoming Log Search	4
Delivery Queue	7
Domain Aliases	9
Domain Settings.....	11
Domain Statistics	12
Edit Routes.....	15
Filter settings.....	17
Manage list of domains and IP addresses with disabled SPF check	20
Local Recipients.....	21
Report Non-Spam	23
Report Spam	24
Clear Callout Cache	25
Blacklist / Whitelist	26
Sender Whitelist.....	27
Recipient Whitelist.....	28
Sender Blacklist	30
Recipient Blacklist.....	32
Outgoing.....	33
Outgoing Log Search	33
Manage Outgoing Users	36
Generate SPF record.....	41
Settings	42
Outgoing User settings	43
Generate DKIM certificate.....	45
Clear Callout Cache (Outgoing).....	46
Archive	47
Search	48
Status	49
Export.....	50
Protection Report	51
On-Demand Domain Report	52
Periodic Domain Report.....	53
Periodic User Report.....	53
Email Restrictions	54

Blocked Extenstions.....	55
Email Size Restriction	55
Webinterface Users.....	56
Manage Email Users.....	57
Manage Permissions	58
My account.....	59
User Profile	60

Incoming



- [Incoming Spam Quarantine](#)
- [Incoming Log Search](#)
- [Delivery Queue](#)
- [Domain Aliases](#)
- [Domain Settings](#)
- [Domain Statistics](#)
- [Edit Routes](#)
- [Filter settings](#)
- [Local Recipients](#)
- [Report Non-Spam](#)
- [Report Spam](#)

Incoming Spam Quarantine

The Spam quarantine interface will show you all the incoming quarantined messages.

By default, these are stored for 28 days, after which they are purged.

From the quarantine overview, you are able to view the messages and sort or search on specific criteria.

It's also possible to mass release and mass delete messages here. Please note that releasing messages has effect on your filtering, so releasing spam/virus/phishing emails may have a negative impact on your filtering quality.

Removing messages from a specific level (i.e. admin level, domain level, email user level) will not remove these from the other levels. This is by design.

	Date	From	To	Subject	Size
<input type="checkbox"/>	2014-06-13 08:34	user@spamxperts.com	test@example.com	testing incoming quarantine - 01	2.26 KiB
<div>Release Release and Train Remove Release and Whitelist Remove and Blacklist</div>					

'Release and Train' will deliver the message to the recipient and train the message as ham into our datasets. This option is recommended by Spam Experts when releasing the messages from Spam Quarantine so that the filters can be correctly adjusted.

Pressing on **'Release'** option from this page will release this specific message from the quarantine and it will only deliver it to the intended recipient.

Choosing **'Release and Whitelist'** will deliver the message to the intended recipient and automatically add sender's email address to 'Sender Whitelist'.

'Remove' will delete the message from Spam Quarantine.

'Remove and Blacklist' will delete the email and automatically add sender's email address to 'Sender Blacklist'.

Mail preview



To view the headers and full raw content of one quarantined messages:

- Click on the subject of the relevant message
- Click the 'Raw' tab
- Click 'Load raw body' at the bottom of the headers

To view the reason for the blocked message, you will need to look for the "Evidence:" line of the raw header and then compare it against our classifications page at – <https://my.spamexperts.com/kb/136/Classifications.html>

At the top or bottom of the raw headers page of the message in Spam Quarantine you can find the option 'Download as eml' which offers you the choice to download that specific spam message in .eml format so that you can afterwards report it to our datasets or save it.

If an attachment is included in the quarantined message, then this can individually be downloaded by clicking on the 'Attachment:' line in the normal view.

Incoming Log Search

Here you can view the log of messages, received, blocked and temporarily rejected.

All email connections (spam and not spam) to a domain are logged to the logging server. To make sure a connection can be logged, the "RCPT TO" information needs to have been received. Connections are generally only temporarily or permanently rejected after receiving this "RCPT TO" data, to ensure all connections being available from the logging system. Connections may not be logged when ratelimiting is applied because of a flood of connections from a certain IP, or when the sending server is violating certain requirements from the RFC 5321.

You can search on various strings and options, including, sender, recipient, subject, message ID, sender host and sender's IP. In the Log Search page you can select the columns that you wish to include in the output by clicking the 'Customize' button. You can select the following columns to be displayed for the filtered messages in the Log Search : Datetime, Host, Sender, Recipient, Sender Hostname, Incoming/ Outgoing Size, Classification, From, To, CC, Subject.

Search:

Date range: — or

Filtering server:

Message ID:

Subject:

Sender:

Recipient: @

Sender IP:

Sender host:

Classification:

<input checked="" type="checkbox"/> not spam	<input checked="" type="checkbox"/> whitelisted	<input checked="" type="checkbox"/> unsure	<input checked="" type="checkbox"/> false positive
<input checked="" type="checkbox"/> oversized	<input checked="" type="checkbox"/> blacklisted	<input checked="" type="checkbox"/> greylisted	<input checked="" type="checkbox"/> phishing
<input checked="" type="checkbox"/> virus	<input checked="" type="checkbox"/> spam	<input checked="" type="checkbox"/> deferred	<input checked="" type="checkbox"/> unknown

Match:

Return partial matches: ☐

Columns to be displayed: Datetime | Sender | Recipient | Classification | Subject

Storage period

The connections logged are by default accessible for up to 28 days. Optionally it's possible to store the logging for a longer time, this can be configured in Spampanel.

Access

The logs can be easily downloaded or searched from the web interface.

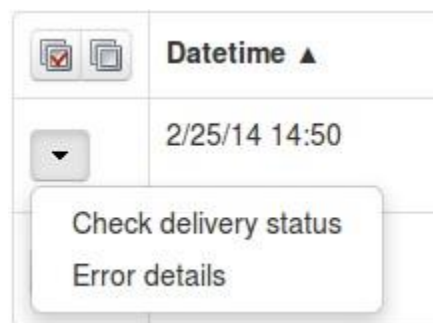
Delay

The logging data is processed every 10 minutes on all filtering nodes. The average delay for the connections to be visible in the log search is therefore 5 minutes.

Information logged

- Date/time
- Server (email ID)
- Sender hostname/IP
- Sender address
- Recipient address
- Subject
- Incoming Size
- Outgoing Size
- Classification

It's possible to view the “delivery status” and the “error details” of the message by using the drop down box on the specific message line.



Messages that say 'Accepted' have not necessarily been delivered, it means the message has been accepted for delivery. If immediate delivery fails, the message will be automatically retried. If the destination server rejects the email, a bounce will be generated to the sender.


For admin users: We advise not to use the global log search for large amounts of data without specifying a domain name, as this can cause delays in the interface when dealing with large amounts of domains and data.

Delivery Queue

This page shows the email that cannot be temporarily delivered to the destination mail server. Messages that end up here will only be due to temporary issues (4XX error) with the destination mail servers.

On this page you have several options:

- Retry to delivery all messages (Apply to Selected – Force Retry option)
- View Message (View option)
- Delete Message (Delete option)
- Delete and Report as Spam (Delete and report as spam option)
- Force retry individual message (Force Retry option)
- Check the Queue Reason (Error Details option)
- Check the Retry Time (check option under Retry time)
- Search for messages (Delivery Queue page)

	Server	Message ID	In queue	Size	Sender	Recipient	Frozen	Retry time
<input type="checkbox"/>	demo1.spambrand.com	1XX0MhP-00019x-12	9 hours	1.85 KiB	noreplyfrom@demo1.spambrand.com	test@example.com	Yes	check

Force retry

Delete

Delete and report as spam

Error details

View

Per page: 100

You can view the content/raw headers of a queued message by pressing the dropdown black arrow on the selected message and View.

We have also reintroduced the option ‘Error details’ to check the reason why messages are stored in Delivery Queue.

It is possible to execute “bulk removal” on selected messages by putting a tick in the check box of the selected messages and choose “Remove messages” from the actions at the bottom of the screen.

Choosing the “Delete & Report as Spam” option will report the selected message(s) to the training server and delete the message from the queue.

It’s also possible to search the delivery queue using the search option in the interface:

Server:

Message ID:

Time:
A time in the queue in seconds, e.g. 180 or 1800-3600

Size:
A limit or range in bytes, e.g. 300 or 500-900

Sender:

Recipient:

Match: ☒ And
☐ Or

Include email type: ?

Return partial matches: ☐



When a message cannot be delivered to its recipients nor returned to its sender, the message is marked as “frozen”, and only occasional delivery attempts are made before eventually giving up on the message. You can now search the Delivery Queue for all the queued messages (including frozen messages), or only ones that are “frozen”, or only normal messages excluding frozen messages.

Domain Aliases

Domain aliases (example.com)

Underneath you have the option to add and delete aliases for this domain. When you add a domain alias and switch the mx-records to activate the filtering for this alias domain, mail directed to user1@alias.ext will be filtered and delivered to user1@maindomain.ext.

Page 1 of 1. Total items: 1. Items per page: 100

	Alias
	example.org

Page 1 of 1. Total items: 1. Items per page: 100

Add an alias

Alias:

 Add

If you have multiple domains, you can make use of the domain aliasing option. Domain aliases can be added to your main domain directly in the web interface. Any email sent to the domain alias will be delivered to the same user on the main domain.

Messages delivered to the alias domain will be re-written at SMTP level to the main domain, so the local email part **MUST** exist on the main domain.

Alias domains don't have separate access to the control panel. Since all SMTP traffic to the domain alias is rewritten to the main domain, any changes/lookups on the main domain will simply include the alias domain traffic as if it was sent directly to the main domain. If you are searching for a specific email sent to a domain alias using the log search, the recipient will therefore show as user@maindomain.

Domain Settings

With the Domain Settings in the Control Panel you can control certain domain settings. The settings apply to the particular domain that have not yet explicitly set a custom value for the setting yet.

You can set the following options:

Basic Settings:

- Primary Contact Email for that domain
- Email notifications From address
- Enable/disable logging for invalid recipients
- Rejected local-part characters
- Timezone

Advanced Settings:

- Administrator's Contact
- Maximum bounces per hour
- Days to keep log messages
- Maximum days to retry
- Disable catch-all check
- Block password attachments • Block dangerous attachments:

At this section (Spam Panel – domain level – Domains Settings page) you can set the maximum bounces, enable/disable logging for invalid recipients, and set accessible/inaccessible logging days for your domain.

The Rejected local-part characters are the characters that are allowed in the local part (before the @ part) of the email address. As regex is used, anything inside the [] is not allowed. So removing a character here will allow that character in the local part.

When having the 'Block password attachments' option enabled in Domains Settings page – Advanced Settings, the system will check all ZIP files attached to a message, and if any are password-protected, then the message will be rejected.

The 'Block dangerous attachments' option allows you to control whether messages containing executables files in the attachment should be blocked or not.

In Spam Panel – domain level – Domains Settings page – Advanced Settings we've added the option to skip the "catch-all" checks for your filtered domains which is useful when activating the 'Automatically activate for all recipients' option in the Periodic User Reports especially when you are using Microsoft Exchange 2013.

Domain settings (example.com)

Underneath you can set a primary contact email, an address from which you can get email notifications, enable logging of invalid recipients, the local valid characters and also the timezone of your domain

Advanced settings

Primary contact email:

Email notifications From address:

Enable logging of invalid recipients: ☒

Rejected local-part characters:

Timezone:

Advanced domain settings (example.com)

Underneath you can set the administrator's contact email, the maximum bounces per hour, an amount of days to keep log messages and the maximum days to retry for 'example.com'

Basic settings

Administrator's contact:

Maximum bounces per hour:

Days to keep log messages:

Maximum days to retry:

Disable catch-all check: ☐

Block password attachments: ☐

Block dangerous attachments: ☐

Domain Statistics

!https://cdn.manula.com/user/1814/img/large/domain-statistics2.png!Here you can view the statistics for a given timeframe (Hours, Days, Weeks, Months, Years).

Statistics are displayed for:

- Spam ratio (of total messages)
- General accuracy
- Not Spam messages
- Unsure messages
- Spam messages blocked
- Viruses blocked
- Whitelisted
- Blacklisted

Domain statistics (example.com)

Underneath you can view the statistics for a given timeframe.

Timeframe:

Days

2/21/14

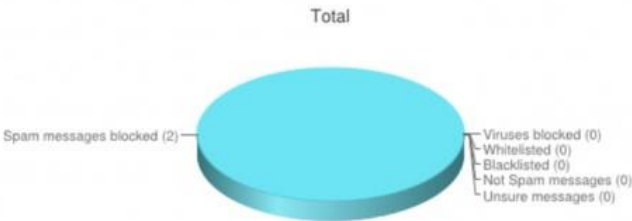
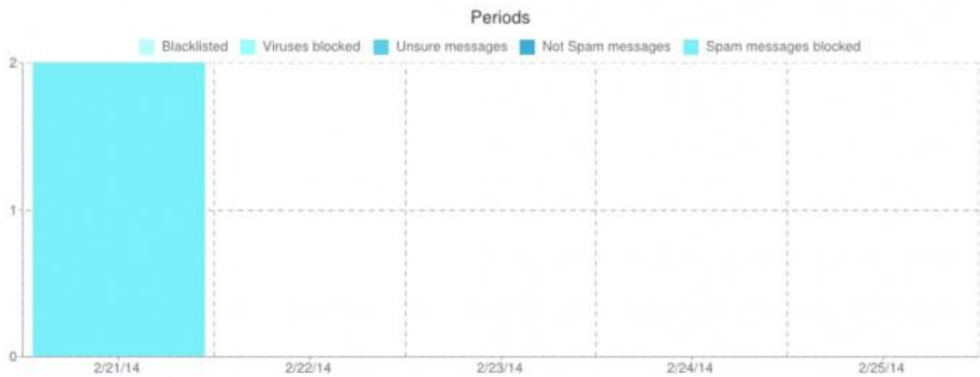
 —

2/25/14

✓ Show

Metrics	Value	Calculation
General accuracy	100.00%	[Recognised Spam messages + Unsure messages + Not Spam messages] / Total filtered messages
Spam ratio (of total messages)	100.00%	Recognised Spam messages / Total filtered messages

Metrics	Count of messages	Size of messages	Bandwidth required
Not Spam messages	0	0	0
Unsure messages	0	0	0
Spam messages blocked	2	2.02 KiB	4.21 KiB
Viruses blocked	0	0	0
Whitelisted	0	0	0
Blacklisted	0	0	0
Totals	2	2.02 KiB	4.21 KiB



Edit Routes

With this function you edit the route(s) (destination mail server) and their respective delivery order.

You have the option to add and delete routes. Also, the list allows you to dynamically move the order of the routes by drag dropping them to the right position in the list.

Edit route(s) (example.com)

Underneath you find the route(s) (destination mail server) and their respective delivery order. You have the option to add and delete (🗑️) routes. You can also issue telnet tests (🔍) for each route. The list allows you to dynamically move the order of the routes by drag dropping them to the right position in the list.

The domain 'example.com' has a single route. You're not allowed to delete this route as a domain always needs to have at least one route in order for the filtering machines to deliver the clean emails. x

Add a route

8.8.8.8:25



✓ Save changes

⚙️ Check routes for open relays

Whenever there are temporary problems with the first route (e.g. 4xx temporary rejects), we'll automatically try delivery to the second route (etcetera). If there are permanent failures with a route (e.g. hostname not resolvable) we'll directly start queuing email and won't try the next route.

We recommend not to use your own fallback system, and instead use the filtering cluster to queue your emails if there are problems with your main destination route.

In Spam Panel – domain level – Edit Routes page you can now perform telnet tests for recipient callouts by pressing on the following icon next to the destination route:



By performing this web interface telnet test, you can verify the existence of recipient's email address on the destination mail server (the one set in Edit Routes page). For fulfilling the recipient callout test you will be requested to type sender's email address (which can be blank if you want to use empty mail from address e.g.: MAILFROM:<>) and you'll also need to input recipient's email address for which the destination server accepts email (recipient's email address which needs to be verified if exists or not on the destination mail server).

Telnet Test



Optional parameters

Envelope sender:
(MAIL FROM)

Envelope recipient:
(RCPT TO)

user@example.com

Close

Run

Filter settings

Here you can set the filter settings that are applied to the domain and its users.

With the Filter settings function, you can control the activation of the quarantine system. This is available via the control panel.

Note: We do NOT recommend changing the defaults settings, the default settings are automatically tuned to provide optimal filtering.

Threshold

The Quarantine Threshold slider (in red) indicates what score you have set for spam messages. The higher the score the means the higher the threshold our systems detect and flag the message as spam. We recommend setting this level to 0.90 to avoid any mail delivery problems.

The Unsure Notation Threshold slider (in green) indicates at what threshold our systems classify the message as unsure, the higher the number set here, the higher threshold our systems have to reach before we class it as unsure. The default here should be 0.1

When a message gets blocked using this method, you can see the combined score in the headers of the email. For example:

X-BrandedHostname-Evidence: Combined (0.96)

Quarantine days

Here you can set the number of days for how long you wish to store the spam emails in the Spam Quarantine. This applies globally to all the domains using the default settings.

Skip SPF Check

This means that emails for all the domains using the default settings will not be subject to SPF (Sender Policy Framework) checks.

Skip Maximum Line Length

This means that emails for all the domains using the default settings will not be subject the RFC line length checks.

Quarantine Response


This you can set if you, for example, do not want senders to receive a bounce message when their mail gets blocked and quarantined. If you set it to Accept the message, the SMTP response would be 2xx accept however the message would still be blocked and shows in the Spam Quarantine. Since that technically breaks with the SMTP RFC specification, it's not recommended.


Filter settings (example.com)

Here you can control the activation of the quarantine system. If you disable the quarantine system, emails detected as spam will not be kept in the quarantine system but will be delivered to your email server. Also you can set the subject notation that is added to the subject of emails classified as unsure by the filtering system.

[Manage list of IP addresses with disabled SPF check](#)

Quarantine enabled: ☒

Quarantine threshold: 

Unsure notation threshold: 

Skip SPF check: ☐

Skip maximum line length check: ☐

Unsure Notation:

Quarantine response:

If you disable the quarantine system, emails detected as spam will not be kept in the quarantine system but will be delivered to your destination email server. Under “Spam notation” you can mark these messages with a specific subject notation. Note that we do NOT return a 5xx reject message for messages classified as spam if the quarantine has been disabled, we do return a 5xx reject message for messages classified as spam if the quarantine is enabled. Every email gets a special header added “X-Recommended-Action: accept” or “X-Recommended-Action: reject”. You can filter the message based on this header if quarantine is disabled.

Filter settings (example.com)

Here you can control the activation of the quarantine system. If you disable the quarantine system, emails detected as spam will not be kept in the quarantine system but will be delivered to your email server. Also you can set the subject notation that is added to the subject of emails classified as unsure by the filtering system.

[Manage list of IP addresses with disabled SPF check](#)

In case you want to disable the quarantine, you can set the spam notation that is added to the subject of emails classified as spam by the filtering system.

Quarantine enabled: ☒

Spam notation threshold: 

Unsure notation threshold: 

Skip SPF check: ☐

Skip maximum line length check: ☐

Unsure Notation:

Spam Notation:

Quarantine response:

Manage list of domains and IP addresses with disabled SPF check

Here you can set the list of domains/IP's to skip the SPF (Sender Policy Framework) check.

Other checks still apply when adding IP's here.

This is particularly useful when dealing with forwarding servers or when you wish to ignore all the SPF failures for the (recipient) domain.

Manage list of domains and IP addresses with disabled SPF check

Underneath you can list some domains and IP addresses or subnets. If a SPF check fails for any of the specified domain or (sender) IPs, then we will continue processing the message

[← Return](#)

Disabled SPF Domains Disabled SPF IPs

Domains with disabled SPF check

 Domain

No domains are setup

Add a Domain

Domain:

[✓ Add](#)

When enabling this feature all the SPF failures will be ignored for the (recipient) domain. If you choose this option your entire list of domains will be removed and you will not be able to add domains in the list unless you deactivate this option.

[Ignore SPF failures](#)

Manage list of domains and IP addresses with disabled SPF check

Underneath you can list some domains and IP addresses or subnets. If a SPF check fails for any of the specified domain or (sender) IPs, then we will continue processing the message

[← Return](#)

Disabled SPF Domains Disabled SPF IPs

IP addresses with disabled SPF check

 IP address

No IP addresses are setup

Add an IP

IP address:

[✓ Add](#)

More actions

[↺ Reset all to default](#)

Local Recipients

In normal setups, the cluster is doing cached recipient callouts to verify existence of a mailbox before accepting email for it. In some cases, for instance you have a very large domain with thousands of mailboxes or in situations that requires this, you can switch to “Local Recipients” instead.

With local recipients you have to add all recipients by hand. If you do not add these users, you will not be able to receive emails on that account.

We highly recommend only using this feature in specific cases, in normal cases this is not necessary to use.

Therefore, you have the option to disable the automatic recipient detection system and to enforce a local list of valid recipients. If “Use local recipients” is enabled, the system will only accept email for the listed recipients. Emails sent to not-listed recipients will be permanently rejected.

Local recipients (example.com)

Underneath you have the option to disable the automatic recipient detection system and to enforce a local list of valid recipients. If "Use local recipients" is enabled, the system will only accept email for the listed recipients. Emails sent to not-listed recipients will be permanently rejected.

The system will only accept email for the recipients listed below. To switch back to the auto-detection of valid recipients please disable this option. ✕

[Upload CSV file](#)

To search a recipient, just type and hit Enter

Search

Page 1 of 1. Total items: 3. Items per page: 100 ⌵

	Local recipient
	alice@example.com
	bob@example.com
	steve@example.com

Page 1 of 1. Total items: 3. Items per page: 100 ⌵

Add local recipient

Email address:

@ example.com

✓ Add

Options

Use local recipients: ☒

✓ Save

Report Non-Spam

With this option you can drag drop or upload messages you wish to classify as non-spam (ham) for training.

These must be in .eml . / .txt format and it must contain the full headers, including the Spamexperts additional headers.

Report Spam

At this section you can drag drop or upload spam messages that passed the filter for immediate training to the systems.

These must be in .eml / .txt format and it must contain the full headers, including the Spamexperts additional headers.

Customers can download report SPAM by downloading the Outlook Plugin, please see links below:

32-bit - http://syndication.globalmicro.co.za/downloads/software/SpamReport_Outlook_32bit.msi

64-bit - http://syndication.globalmicro.co.za/downloads/software/SpamReport_Outlook_64bit.msi

Clear Callout Cache

At this section you can manually clear the domain's callout cache.

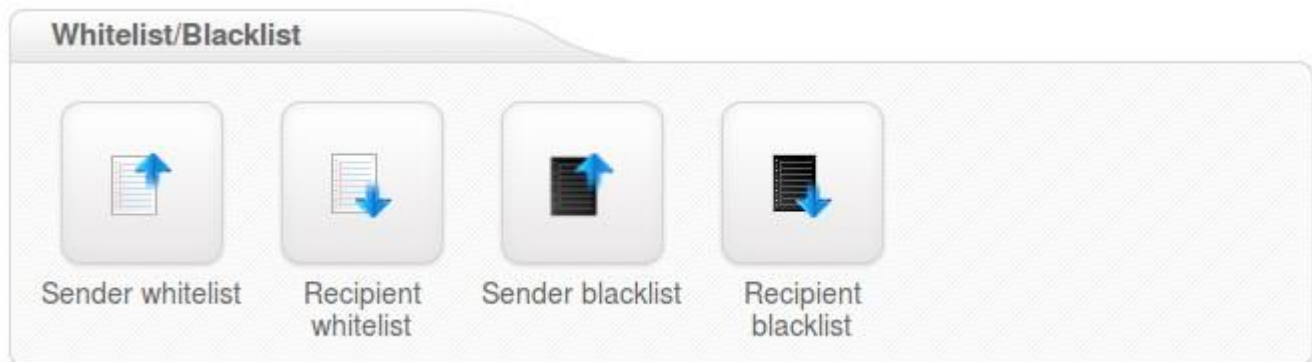
This is extremely useful to be cleared after changing the domain routes, DNS records and for removing the bad/good responses from the destination mail server.

Clear callout cache (example.com)

Here you can clear the callout cache for a domain

 Clear

Blacklist / Whitelist



- [Sender Whitelist](#)
- [Recipient Whitelist](#)
- [Sender Blacklist](#)
- [Recipient Blacklist](#)

Sender Whitelist

Whitelisting the sender(s) at this section will apply to all the users on this domain.

To allow the domain administrator to remain in control over the filtering, it's possible to whitelist a sender. The check works based on the MAIL FROM provided by the sender at SMTP level, or the "From:" header in the email.

All filtering checks are disabled for whitelisted senders. We recommend only using the sender whitelist if the system would otherwise wrongly block email from a certain sender. Spammers often use fake senders matching the recipient domain, or domains the recipient may have received emails from before, to try and bypass the filtering in that way. In addition, if the system is generally wrongly blocking a sender, you can always contact our customer support so we can research what problem is causing the rejection and resolve that issue.

You can whitelist a specific sending email address, or a full sending domain. To whitelist all senders from a domain, you should only enter the domain (without *@).

Sender whitelist (example.com)

Underneath you have the option to add and delete whitelisted senders. To whitelist a full domain, simply add the domainname without @.

Page 1 of 1. Total items: 4. Items per page: 100

 Sender
<input type="checkbox"/> a.com
<input type="checkbox"/> b.com
<input type="checkbox"/> c.om
<input type="checkbox"/> example@senderdomain.com

Page 1 of 1. Total items: 4. Items per page: 100

Whitelist a sender

Email address /
Hostname:

 Add

More actions

 Upload CSV file

 Reset to default

If you want to add multiple whitelisted senders at once you can upload a Comma Separated Values (CSV) file. Each line in the file must contain one column: emailaddress. Example CSV file content:

user1@example.com

user2@otherdomain.example.com example.com

Recipient Whitelist

All filtering checks are disabled for whitelisted recipients. We recommend only using the recipient whitelist for exceptional cases such as special abuse@ or postmaster@ recipients.

To whitelist a specific recipient address, the local part of the address should be entered. For example, if your domain is example.com and you add “nofilter” to the recipient whitelist, all emails sent to nofilter@example.com

will not be scanned for spam/viruses. To whitelist all recipients for a domain (so all emails sent to the domain are not scanned/blocked), you can enter the wildcard "*" for the local part.

You can optionally also upload a Comma Separated Values (CSV) file to add multiple whitelisted recipients at once (this is only available for domain users). Each line in the file must contain one column: emailaddress.

Example CSV file content:

```
user1@example.com user2@otherdomain.example.com
```

Sender Blacklist

Blacklisting the sender(s) at this section will apply to all users on this domain.

To allow the domain administrator to remain in control over the filtering, it's possible to blacklist a sender. The check works based on the MAIL FROM provided by the sender at SMTP level, this may be different from the "From:" header in the email. If you check the headers of an email, the "envelope-from" address specifies the actual sender address.


Emails from senders listed on the blacklist will be automatically rejected. The messages are NOT quarantined. The messages are rejected with a 5xx SMTP error code, so legitimate sending SMTP servers will generate a bounce message to the sender.

You can blacklist a specific sending email address, or a full sending domain. To blacklist all senders from a domain, you should only enter the domain (without *@).

Sender blacklist (example.com)

Underneath you have the option to add and delete blacklisted senders. To blacklist a full domain, simply add the domainname without @.

Page 1 of 1. Total items: 1. Items per page: 100

	Sender
	user@example.com

Page 1 of 1. Total items: 1. Items per page: 100

Blacklist a sender

Email address /
Hostname:

 Add

More actions

 Upload CSV file

 Reset to default

You can upload a Comma Separated Values (CSV) file to add multiple blacklisted senders at once. Each line in the file must contain one column: emailaddress. Example CSV file content:

```
user1@example.com
```

```
user2@otherexample.com example.net
```

Recipient Blacklist

Blacklisting the recipient(s) at this section will apply to all users on this domain.

Emails to recipients listed on the blacklist will be automatically rejected. The messages are NOT quarantined. The messages are rejected with a 5xx SMTP error code, so legitimate sending SMTP servers will generate a bounce message to the sender.

To blacklist a specific recipient address, the local part of the address should be entered. For example, if your domain is example.com and you add “nofilter” to the recipient blacklist, all emails sent to nofilter@example.com will be rejected. To blacklist all recipients for a domain (so all emails sent to the domain will be rejected), you can enter the wildcard “*” for the local part.

Recipient blacklist (example.com)

Underneath you have the option to add and delete blacklisted recipients. Email directed to blacklisted recipients will be blocked.

Page 1 of 1. Total items: 1. Items per page: 100

Recipient
user@example.com

Page 1 of 1. Total items: 1. Items per page: 100

Blacklist a recipient

Email address: @ example.com

✓ Add

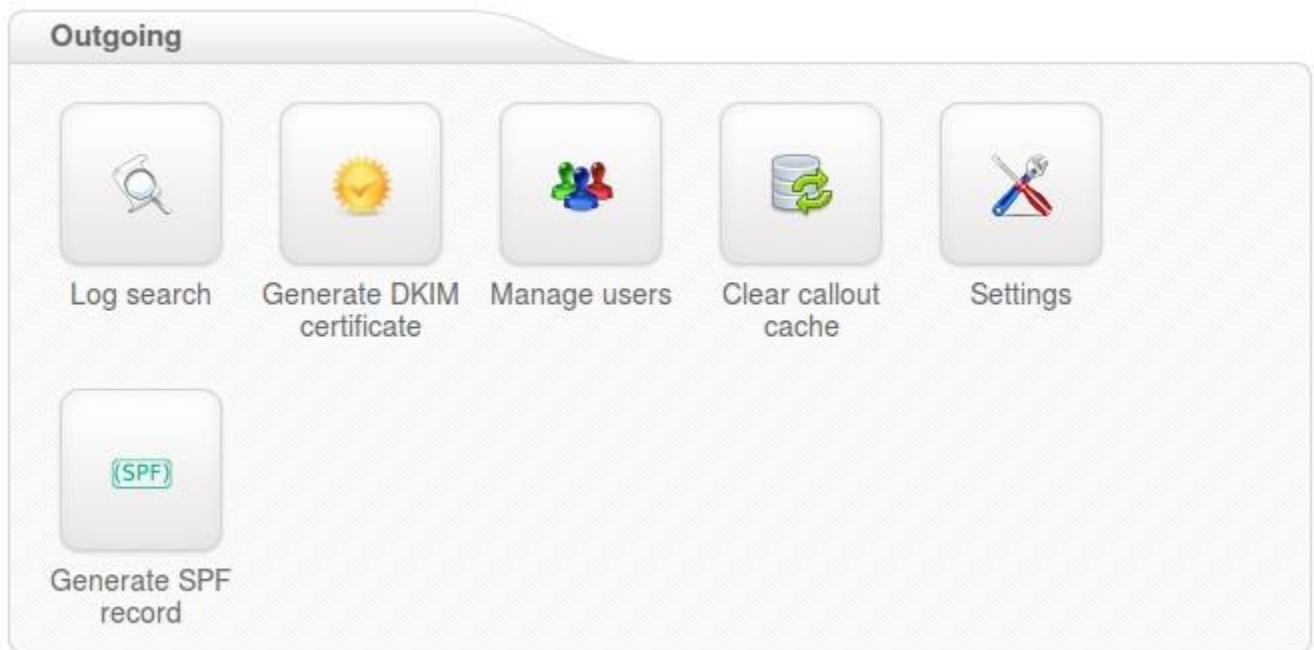
More actions

Upload CSV file Reset to default Blacklist all recipients

You can optionally also upload a Comma Separated Values (CSV) file to add multiple blacklisted recipients at once. Each line in the file must contain one column: emailaddress. Example CSV file content:

user1@example.com user2@otherdomain.example.com

Outgoing



- [Outgoing Log Search](#)
- [Manage Outgoing Users](#)
- [Generate SPF record](#)
- [Settings](#)
- [Outgoing User settings](#)
- [Generate DKIM certificate](#)

Outgoing Log Search

All email connections (spam and not spam) to a domain are logged to the logging server. To make sure a connection can be logged, the “RCPT TO” information needs to have been received. Connections are generally only temporarily or permanently rejected after receiving this “RCPT TO” data, to ensure all connections being available from the logging system. Connections may not be logged when ratelimiting is applied because of a flood of connections from a certain IP, or when the sending server is violating certain requirements from the RFC 5321.

You can search on various strings and options, including, sender, outgoing user, recipient, subject, message ID, sender host and sender’s IP. In the Log Search page you can select the columns that you wish to include in the output by clicking the ‘Customize’ button. You can select the following columns to be displayed for the filtered messages in the Log Search : Datetime, Filtering Server, Message ID, Outgoing User, User Identification,

Sender, Recipient, Sender IP, Sender Hostname, Incoming/Outgoing Size, Classification, From, To, CC, Subject.

In the outgoing log search, you can now include in your results the identification of the end-user, if you have that configured. As a reminder: when you are creating or editing an outgoing user, you can “tell” the software to identify users by their authentication username, the envelope sender, or by searching for a username in a message header. We strongly recommend that everyone using a “smarthost” configuration do this, so that we are able to provide you with detailed information about which of your end-users are causing problems.

Search:

Date range: — or ☐

Filtering server:

Message ID:

Subject:

Sender:

User: @

Recipient:

Sender IP:

Sender host:

Classification:

<input checked="" type="checkbox"/> not spam	<input checked="" type="checkbox"/> whitelisted	<input checked="" type="checkbox"/> unsure	<input checked="" type="checkbox"/> false positive
<input checked="" type="checkbox"/> oversize	<input checked="" type="checkbox"/> blacklisted	<input checked="" type="checkbox"/> locked	<input checked="" type="checkbox"/> phish
<input checked="" type="checkbox"/> virus	<input checked="" type="checkbox"/> spam	<input checked="" type="checkbox"/> deferred	<input checked="" type="checkbox"/> unknown

Match: ⓘ

Return partial matches: ☐ ⓘ

Columns to be displayed: Datetime | User | Sender | Recipient | Classification | Subject

ⓘ

Storage period

The connections logged are by default accessible for up to 28 days. Optionally it's possible to store the logging for a longer time, this can be configured in Spampanel.

Access

The logs can be easily downloaded or searched from the web interface.

Delay

The logging data is processed every 10 minutes on all filtering nodes. The average delay for the connections to be visible in the log search is therefore 5 minutes.

Information logged

- Date/time
- Server (email ID)
- Sender hostname/IP
- Sender address
- Recipient address
- Classification

It's possible to view the "delivery status" of the message by using the drop down box on the specific message line.



We advise not to use the global log search for large amounts of data without specifying a domain name, as this can cause delays in the interface when dealing with large amounts of domains and data.

Manage Outgoing Users

With this option you can create/manage outgoing users.

When adding Outgoing Users, you can either choose from:

“**Authenticating User**” which means that the SMTP AUTH username will be

‘Username@outgoingdomain.ext’, and the password will be ‘Password’ set for this outgoing user.

“**Authenticating Domain**” which means that the domain name is the username for authentication (with the configured password).



“**Authenticating IP or range**” will be an IP outgoing user (without a password) and any connection from that IP will be considered authenticated without needing to use SMTP AUTH.

By editing the outgoing user, you can manage the settings which will be applied to that specific outgoing user:

Manage users (example.com)

Underneath you can manage outgoing users. The SMTP AUTH username will be 'Username@example.com, and the password will be 'Password'. If the 'Username' field is left blank, then the SMTP AUTH username will be equal to the domain name. If the 'Password' field is left blank, then the 'Username' must be an IP address, and any connection from that IP will be considered authenticated without needing to use SMTP AUTH.

Page 1 of 1. Total items: 1. Items per page:

 	Username ▲	Automatic unlock
<input type="checkbox"/>	test@example.com	Not locked

Edit

Lock

Page 1 of 1. Total items: 1. Items per page:

Add a user

Authenticating IP or range (e.g. a smarthost)

Authenticating User

Authenticating Domain

Username: @

Password:

Outgoing user settings (example.com)

Underneath you can manage the outgoing user settings.

IP range:

Identification method:

Automatic lock:

User lock timeout: (in minutes)

Maximum unlocks by timeout:

Enable outgoing limits: ☐

Outgoing limit per month:

Outgoing limit per week:

Outgoing limit per hour:

Outgoing limit per minute:

Valid sender address required: ☐

DKIM selector:

Maximum number of recipients per day: (0 is unlimited)

Invalid recipient limit: (0 is disabled)

Quarantine response:

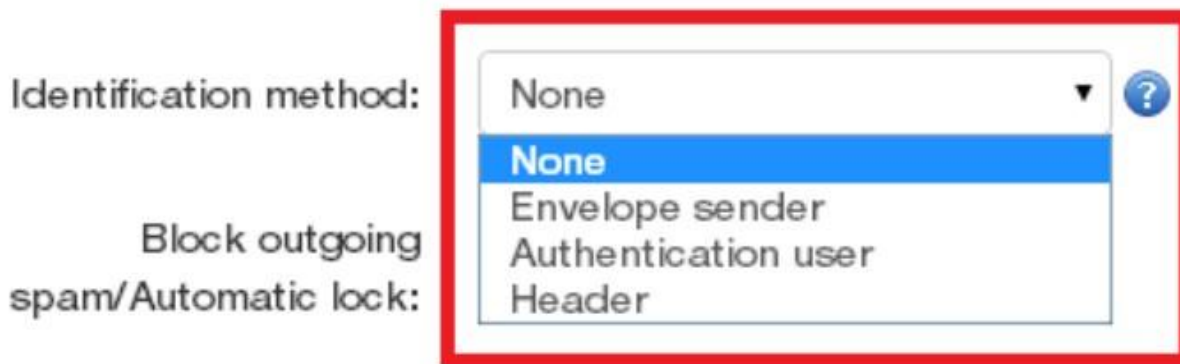
Message archiving for senders: ☐

[Save](#) [Return to the list](#)

- **Password:** Set the password for the per username authenticated outgoing user (N/A for IP outgoing users).
- **Identification Method:** Here you can choose either, “envelope sender” , “authentication user” or “Header” for the identification method.
- **Automatic lock:** The option ‘Automatic Lock Enabled’ will lock the user and stop that outgoing user from sending any more email when SPAM is seen, the administrator will receive an alert when this happens and give you the option to unlock the user.
- **User Lock timeout:** the timeout for locking the user in minutes after the spam messages are sent.
- **Maximum Unlocks by timeout:** setup the maximum number of unlocks by timeout.
- **Enable Outgoing Limits:** Enabled/Disabled
- **Outgoing Limit per month:** the limit for outgoing messages/month sent by the user.
- **Outgoing Limit per week:** the limit for outgoing messages/week sent by the user.
- **Outgoing Limit per hour:** the limit for outgoing messages/hour sent by all the user.
- **Outgoing Limit per minute:** the limit for outgoing messages/minute sent by the user.
- **Valid Sender Address Required:** Enabled/Disabled – valid sender’s email address check.
- **DKIM Selector:** Here you can set the default DKIM selector.
- **Maximum number of recipients per day:** the maximum number of recipients the user can send emails to.
- **Invalid Recipient limit:** the limit assigned for sending emails to invalid recipients.
- **Maximum days to retry:** set the maximum number of days the message will be retried for delivery (this applies to messages stuck in the delivery queue).

- **Quarantine Response:** Rejected/Accepted – “Rejected” legitimate senders will receive a bounce message when their mail gets blocked and quarantined. “Accepted” the SMTP response would be ‘Accept’ and the message would still be blocked and shown in the quarantine but the sender won’t receive a bounce message.
- **Message archiving for senders:** Enabled/Disabled – for archiving messages for envelope from sending domains.

It’s now possible to manage the outgoing user identification system. In the “Default Domain Settings” (Outgoing section) or “in Outgoing user settings” (Manage Outgoing Users – Edit), there is a new “Identification method” choice.



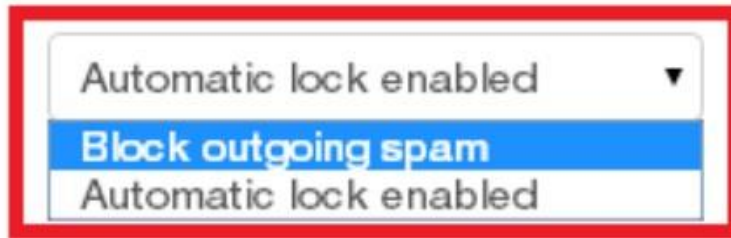
As can be seen in the screen shot above you have three choices:

1. The “envelope sender” (or MAIL FROM value). If your system enforces this, then this is likely your best choice.
2. The “authentication user”. In this case, the identity will match the outgoing user’s authentication details. This is the best choice when you are providing unique usernames and passwords to each outgoing user, rather than using a smarthost system.
3. “Header”. If you choose this option, you are able to add any number of identification headers that we should search for in the message. For example, you might have a system that adds an “X-Client-ID” header, which uniquely identifies each of your end users. For each header, you may choose to either use the entire header value as the identity, or you can provide a regular expression that extracts out a part of the value to use. You may also choose to have our software remove the header after we have found the identity, if you don’t want this to be available to the recipient of the message.

The option below ‘Block Outgoing Spam’ will block the spam messages in the Outgoing Spam Quarantine as opposed to ‘Automatic Lock Enabled’ option which will lock the user and stop that outgoing user from sending any more emails when Spam messages are detected. Please be aware that if you are using IP authenticated users and use the ‘Automatic Lock Enabled’ option for that specific IP outgoing user, this will lock the whole

server not allowing any users to relay outgoing messages until the IP outgoing user was automatically/manually unlocked.

Block outgoing
spam/Automatic lock:



If the user is locked, then:

1. A notification message is sent to the administrator
2. Authentication succeeds, and the connection is processed as normal until DATA, when the message is temporarily (i.e. with a 4xx code) failed, with an error message indicating that the account is locked and the administrator must be contacted (providing the contact address from the API). Email to the administrator address is always accepted, even for locked users.
3. The message is stored in the quarantine IMAP system, under the “global” user’s account for review by the administrator

Users may be unlocked:

1. Automatically after a fixed period of time with a maximum of X times (configurable via the API)
2. Manually via the API

Generate SPF record

The system automatically generates the SPF record string along with the current status on the domain. For the SPF Record to become function able it has to be added at the DNS Registrar / Edit Zone page as a TXT Record.

Generate SPF record (example.com)

The required SPF record string should be generated below along with the current status on the domain.

SPF Record String:	v=spf1 a:demo1.brand.com -all
SPF Record Status (example.com):	<ul style="list-style-type: none">Servers missing from SPF record:demo1.brand.com

Settings

At this section you can set the administrator's contact email for the domain.

This address is predominately used for ARF (Abuse Report Feedback) reports.

Settings (example.com)

Underneath you can set the administrator's contact email for your domain: example.com

Administrator's contact:

✓ Save

↺ Reset to defaults

Outgoing User settings

Here you can control the outgoing user settings.

This can be found by editing the outgoing user:

 Username ▲	Automatic unlock
 bob@example.com	Not locked

Edit

Lock

Page 1 of 1. Items per page: 100

- **Password:** Set up the password globally.
- **Block outgoing spam/Automatic lock:** The option 'Automatic Lock Enabled' will lock the user and stop that outgoing user from sending any more email when SPAM is seen (as opposed to 'block', which will only block the SPAM messages individually), the administrator will receive an alert when this happens and give you the option to unlock the user.
- **User Lock timeout:** the timeout for locking the user in minutes after the spam messages are sent.
- **Maximum Unlocks by timeout:** setup the maximum number of unlocks by timeout.
- **Enable Outgoing Limits:** Enabled/Disabled
- **Outgoing Limit per month:** the limit for outgoing messages/month sent by the user.
- **Outgoing Limit per week:** the limit for outgoing messages/week sent by the user.
- **Outgoing Limit per hour:** the limit for outgoing messages/hour sent by all the user.
- **Outgoing Limit per minute:** the limit for outgoing messages/minute sent by the user.
- **Valid Sender Address Required:** Enabled/Disabled – valid sender's email address check.
- **DKIM Selector:** Here you can set the default DKIM selector.
- **Maximum number of recipients per day:** the maximum number of recipients the user can send emails to.
- **Invalid Recipient limit:** the limit assigned for sending emails to invalid recipients.
- **Maximum days to retry:** set the maximum number of days the message will be retried for delivery (this applies to messages stuck in the delivery queue).
- **Quarantine Response:** Rejected/Accepted – "Rejected" legitimate senders will receive a bounce message when their mail gets blocked and quarantined. "Accepted" the SMTP response would be 'Accept' and the message would still be blocked and shown in the quarantine but the sender won't receive a bounce message.

It's also possible to manually lock the outgoing user here in case of issues. This can also be done via the drop down box

Generate DKIM certificate

Here you can generate a DKIM certificate for your domain. You will need to choose the desired selector that you chose earlier in the outgoing users section. As a result, you will get a value for public key which should be available in your DNS.

After successful DKIM generation you should enable the resulting DKIM certificate for each outgoing user using your selector.

The key lengths that can be chosen are:

- DKIM length 2048 bits (Recommended)
- DKIM length 1024 bits (Only can be used if unable to use a 2048 bit key DNS provider)

Generate DKIM certificate (example.com)

Here you can generate a DKIM certificate for your domain. Please fill the form below with the desired selector you've chosen earlier. As a result you will get a value for public key which should be available in your DNS. After successful DKIM generation you should enable the resulting DKIM certificate for each outgoing user using your selector.

DKIM key length: ☒ DKIM length 2048 bits (Recommended)
☐ DKIM length 1024 bits (Only can be used if unable to use a 2048 bit key DNS provider)

DKIM selector:

✓ Generate and save new private/public pair

Clear Callout Cache (Outgoing)

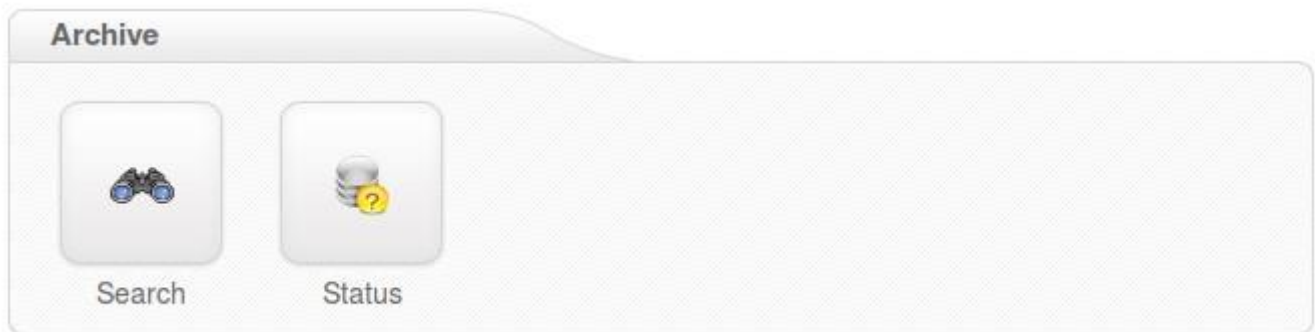
At this section you can clear the callout cache for an outgoing domain.

Clear callout cache (example.com)

Here you can clear the callout cache for an outgoing domain

 Clear

Archive



- [Search](#)
- [Status](#)

Search

Here you can search messages that match the specified criteria that have been archived. You can set the text to be found in the field 'query'. Also you can choose the mode.

It may be 'all', 'any', 'boolean' or 'phrase'. The Boolean mode allows the '&' (and), '|' (or), '-' '!' (not) operators and grouping '(' and ')' to be used in the query.

There is implicit '&', so 'cat dog' is the same as 'cat & dog'. 'or' operator precedence is higher than 'and'. Queries like '-dog', cannot be evaluated (for performance reason).

For example, a query that uses all of these operators is: '(cat -dog) | (cat -mouse)'. This will find messages that include 'cat', but not 'dog' or messages that include 'cat', but not 'mouse'.

All archived emails are indexed including readable attachments. They can be searched using any search string.

Status

Here is the status of the Archiving service, including:

- Space Used
- Free Space Available
- Number of days emails are stored

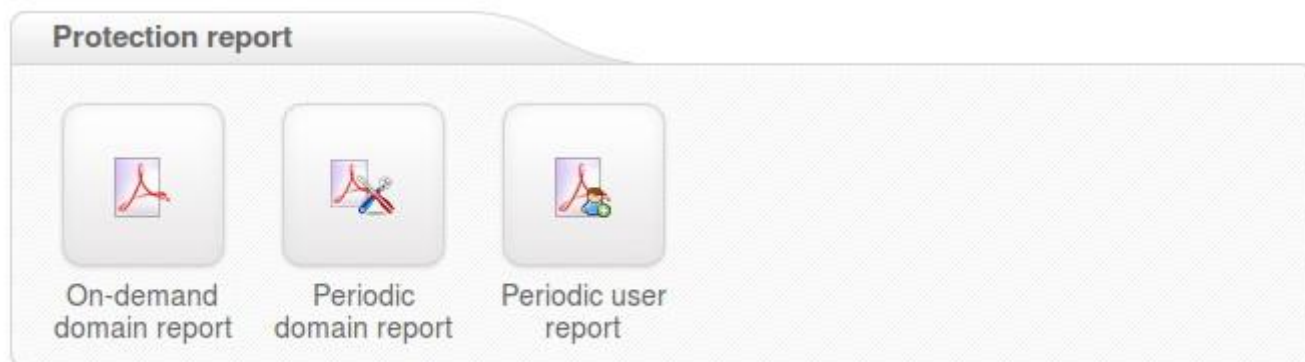
Parameter	Value
Number of days emails are stored	0

Export

Using the Export will allow you to get emailed copies of the archived mail.

All the archived emails from the specified period will be emailed to the destination email address as individual files in a zip archive.

Protection Report



- [On-Demand Domain Report](#)
- [Periodic Domain Report](#)
- [Periodic User Reports](#)

On-Demand Domain Report

On-demand domain report (example.com)

Here you can generate a protection report for a specified date range, and send it to the specified email address. This form will trigger the creation of the report; the actual delivery may take several minutes, depending on the size of the report.

Date start:

Period:

Language:

Format: ☒ HTML
☐ PDF

Email:

Include extra spam table: ☐

 Send

With this feature you can generate a Protection Domain Report for a specified date range, and send it to a specified email address. The format of the report can be either HTML or PDF format.

The “Include extra spam table” is only used in the PDF reports, and this adds a table of messages that were rejected but not quarantined.

Periodic Domain Report

Periodic domain report (example.com)

Here you can control the activation of the protection report, the recipient, the frequency, the language and the format in which the report is presented to you.

Report enabled: ☒

Recipient Address:

Report Frequency:

Language:

Format: ☒ HTML
☐ PDF

Include extra spam table: ☒

Send report with no quarantined messages: ☒

A daily or weekly report can be generated for each domain (or for specific recipients at a domain) and is delivered via email. Multiple recipients can be separated with a comma. A report can also be generated on demand from the API/web interface.

The report can be sent as a PDF attachment or as inline HTML. The PDF report outlines a summary of the spam and viruses that the filtering service has protected the domain (or address) from receiving, and also includes information about the total volume of mail processed for the said domain.

The PDF report also includes a detailed table (for auditing purposes) of messages that were rejected but not quarantined; this table is configured by default but may be disabled via the API/web interface – it will be very large for some domains. A similar table is also included with the messages that were quarantined, including links to release each message directly.

Settings defined here will mean that users on this domain will also take these values.

Periodic User Report

With this option you can enable periodic protection reports based on users. You can add users, either individually or via the .csv upload function for multiple users (multiple upload is only available for domain users). Only ASCII characters are supported for the local part.

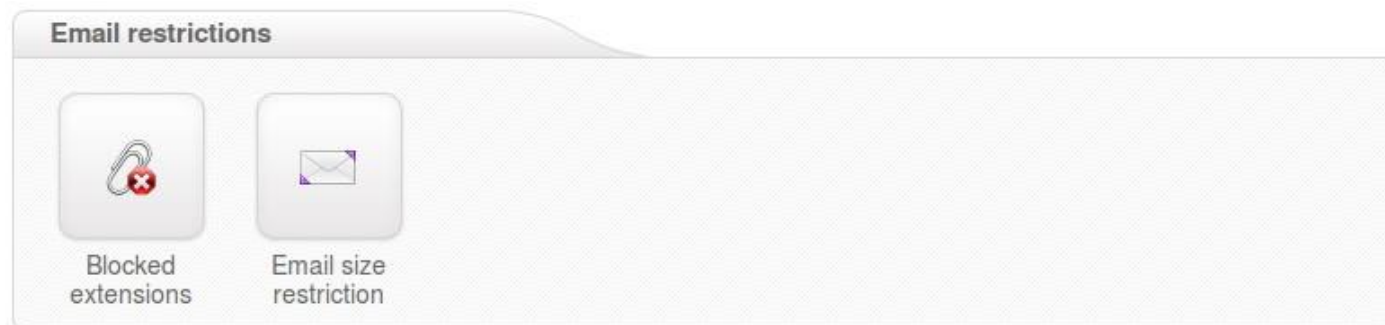
The report will contain an overview of the quarantined messages for the specific user, including links to release each message directly.

The option “Automatically activate for all recipient” will automatically add users to the user report list, and then once added, send them a daily or weekly report on the spam received. It will also send the end user a welcome email in the beginning to let them know their personal quarantine has been activated, and if they would like to log in to see this, they can do it using the login link in the email.

Please note: If your domain has “Catch-All” enabled, then this option will not be able to be enabled

In Spam Panel – domain level – Domains Settings page – Advanced Settings we’ve added the option to skip the “catch-all” checks for your filtered domains which is useful when activating the ‘Automatically activate for all recipients’ option in the Periodic User Reports especially when you are using Microsoft Exchange 2013.

Email Restrictions



- [Blocked Extensions](#)
- [Email Size Restrictions](#)

Blocked Extensions

Blocked extensions (example.com)

Underneath you can specify which emails should be blocked based on the extension of the files attached.

[+ Add extension](#)

 Extension
 bat
 btm
 cmd
 com
 cpl
 dll
 exe
 msi
 pif

More actions

 Reset to default

You can specify which emails should be blocked based on the extension of the files attached. There is a list of some extensions added by default but you can add whatever extension type you want. If a file extension will be blocked the email message which contained the attachment will be placed in the SPAM Quarantine.


Email Size Restriction


Email size restriction (example.com)

Underneath you can set the maximum size for incoming and outgoing emails to be accepted by the filtering system.

Email size limit (in MBytes): — ☐ 

Action for oversized messages:

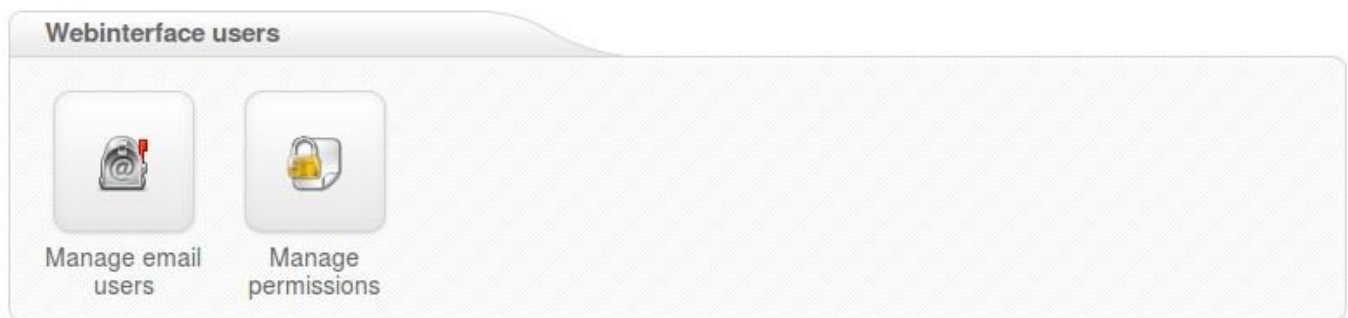
 Update

 Reset to default

By default, the system applies no limits to the email size, and uses the size set by the destination mail server. You can however set the maximum size for incoming and outgoing emails to be accepted by the filtering system. If the message exceeds the set up limit, it can either Rejected and stored in the Spam Quarantine or it can be Rejected with 5xx code (and not stored in Spam Quarantine) depending on how you set this up.

Please make sure that the recipient server can also receive the email size set by the filtering system

Web interface Users



- [Manage Email Users](#)
- [Manage Permissions](#)

Manage Email Users

With this function you can manage email users. These users can log into the Spampanel with their email address to see their own quarantine, and manage their specific email settings.

Please make sure that the domain you are creating the email for already exists on the server, and when setting the password, the password must contain lower case letters, at least one upper case letter or one digit, no spaces, and must be 6-25 characters in length.

Only ASCII characters are supported for the local part.

You may also upload a Comma Separated Values (CSV) file. Each line in the file must contain at least four columns, the username, the domain, the password and the status.

The password must contain lower case letters, at least one upper case letter or one digit, no spaces, and must be 6-25 characters in length.

As a higher level user, you also have the ability to “Login as user”

If you select an Email user in ‘Manage Email Users’ page and press the dropdown black arrow you have several options such as:

- Edit Email User
- Delete Email User
- Login as the Email User
- Require 2FA

	ID	Username 	Is active	Last login
	10	user@example.com		
<div><div><div>Edit</div><div>Delete</div><div>Login as user</div><div>Require 2FA</div></div><div>Items per page: 50 </div></div>				

With Require 2FA an Administrator or Reseller or Domain user can require specific users, or all users, to use 2FA. If a user didn't previously have this enabled, they will be prompted to set it up on their first login after it's requested.

Manage Permissions

Here you can set specific permission settings per user level role

Login & Password recovery settings

Manage:

User role	Login allowed	Password recovery allowed
Administrator	<input type="checkbox"/>	<input type="checkbox"/>
Reseller	<input type="checkbox"/>	<input type="checkbox"/>
Domain	<input type="checkbox"/>	<input type="checkbox"/>
Email	<input type="checkbox"/>	<input type="checkbox"/>

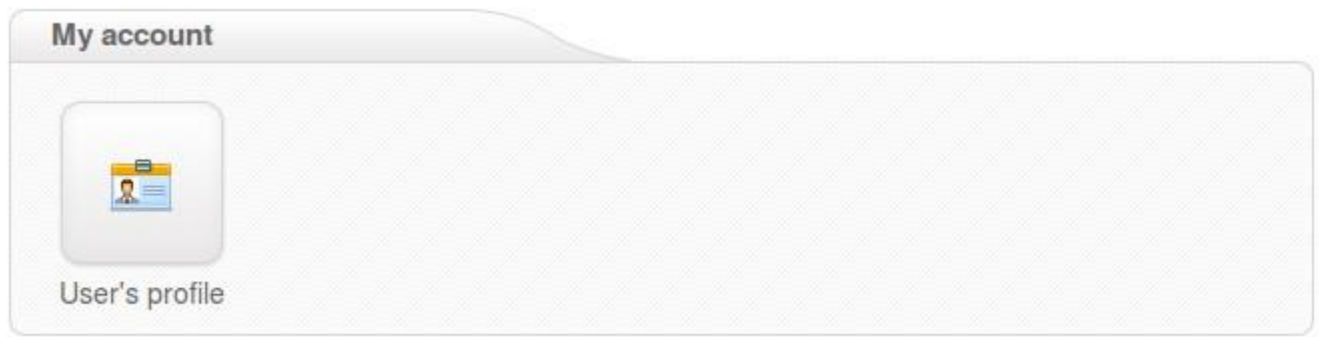
✓ Save

With these settings you can manage permissions for available user's roles.

Individual page permissions

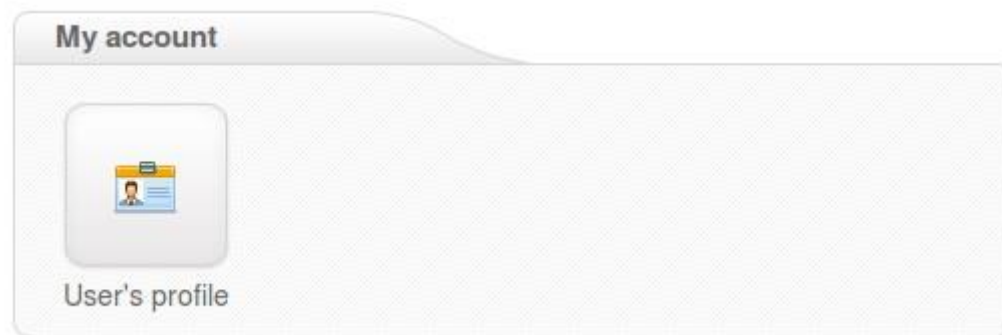
	Admin	Reseller	Domain	Email	Guest
Domains					
— Add domain	<input type="checkbox"/>	<input type="checkbox"/>			
— Upload CSV file	<input type="checkbox"/>	<input type="checkbox"/>			
— MX verification tool	<input type="checkbox"/>	<input type="checkbox"/>			
— Overview	<input type="checkbox"/>	<input type="checkbox"/>			
— Change destination(s)	<input type="checkbox"/>	<input type="checkbox"/>			
— Move domains to	<input type="checkbox"/>	<input type="checkbox"/>			
Incoming					
— Bandwidth overview (bandwidth)	<input type="checkbox"/>	<input type="checkbox"/>			
— Blacklist IPs (blacklistip)	<input type="checkbox"/>	<input type="checkbox"/>			
— Blacklisted IP edit (blacklistipedit)	<input type="checkbox"/>	<input type="checkbox"/>			
— Clear callout cache (clearcalloutcache)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
— Clear whole callout cache (clearglobalcalloutcache)	<input type="checkbox"/>				
— Cluster statistics	<input type="checkbox"/>				
— Default domain settings (defaultdomainsettings)	<input type="checkbox"/>				
— Delivery queue (deliveryqueue)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

My account



- [User Profile](#)

User Profile



Here you can edit the user's profile and enable Two Step Authentication to increase the security of your account. This means an additional device (like a mobile phone) will be required in order to log in, so even if someone knows your password they will not be able to take control of your account without your device.

For Two Step Authentication you should be able to use any app that supports the Time-based One-Time Password (TOTP) protocol, including:

- Google Authenticator (Android/iPhone/BlackBerry)
- Authenticator (Windows Phone 7)

Enable Two Step Authentication