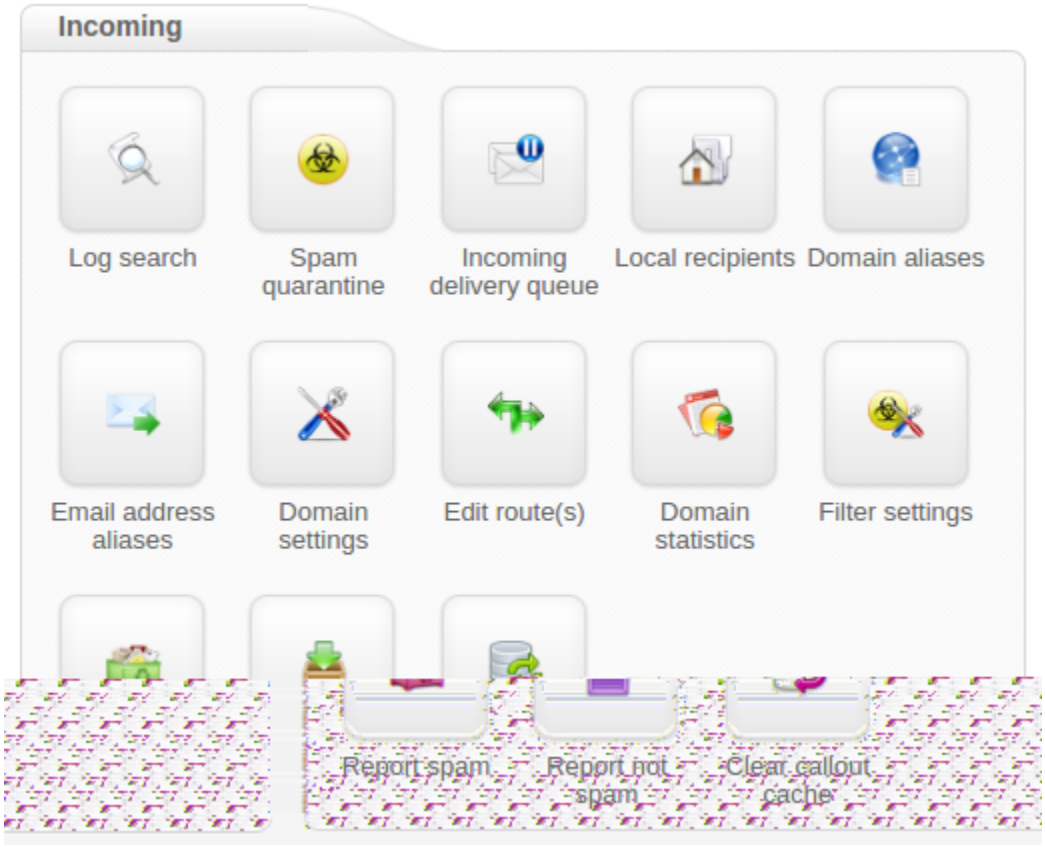
SpamExperts Control Panel Domain Level

1 — Last update: 2016/07/12

SpamExperts

Table of Contents

Incoming



- Incoming Log Search
- Incoming Spam Quarantine
- Delivery Queue
- Local Recipients
- Email Address Aliases
- Domain Aliases
- Domain Settings
- Edit Routes
- Domain Statistics
- Filter settings
  - Manage List of Domains and IP Addresses with Disabled SPF check
- Report Spam
- Report Non-Spam
- Clear Callout Cache

Incoming Log Search

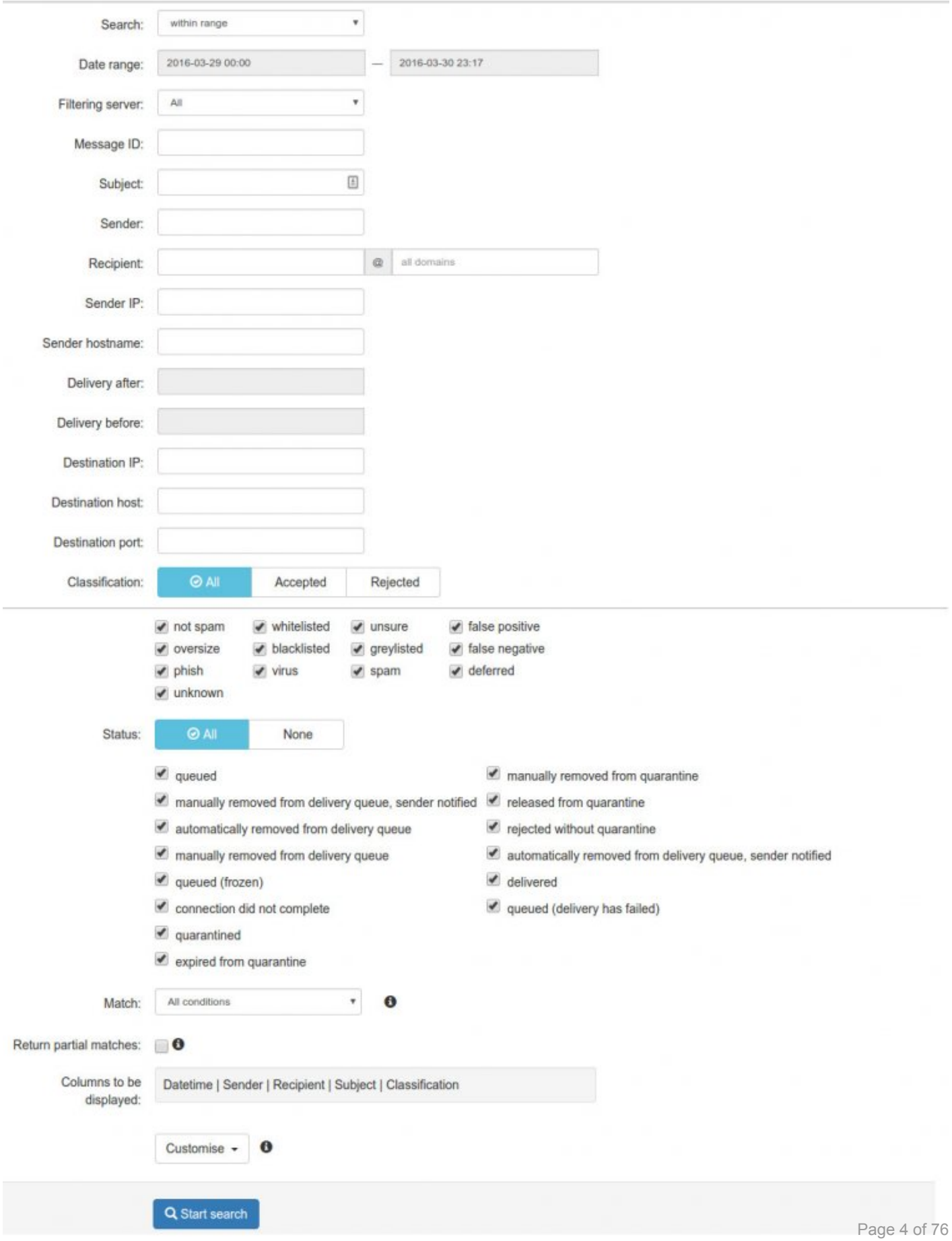
On this page you can view the log of messages that are received, blocked and temporarily rejected.

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 the “RCPT TO” data, to ensure all connections being available from the logging system.

You can search on various strings and options, based on a date range, server, message ID, subject, sender, recipient, sender IP, hostname, delivery before and after, destination IP, destination host, destination port and also classifications such as all, accepted and rejected. The filters include more detailed classifications such as not spam, whitelisted, unsure, false positive, oversize, blacklisted, greylisted, false negative, phish, virus, spam, deferred and unknown.

The message status presents two buttons that select all or none of the following: queued, manually removed from quarantine, manually removed from delivery queue, released from quarantine, automatically removed from delivery queue, rejected without quarantine, manually removed from delivery queue, automatically removed from delivery queue, queued (frozen), delivered, connection did not complete, queued (delivery has failed), quarantined, expired from quarantine.
Users can also select if the search should match all conditions or any conditions, including returning partial matches.

By clicking on the **Customize** button, the displayed columns can be customized and include all of the following: Datetime, Filtering Server, Message ID, Sender Hostname, Sender, Recipient, From, To, CC, Subject, Incoming size, Outgoing size, Delivery date, Destination IP, Destination host, Destination port, Status and Classification.


Search:
within range
Date range:
2016-03-29 00:00
2016-03-30 23:17
Filtering server:
All
Message ID:
Subject:
Sender:
Recipient:
all domains
Sender IP:
Sender hostname:
Delivery after:
Delivery before:
Destination IP:
Destination host:
Destination port:
Classification:
All
Accepted
Rejected
not spam
whitelisted
unsure
false positive
oversize
blacklisted
greylisted
false negative
phish
virus
spam
deferred
unknown
Status:
All
None
queued
manually removed from delivery queue, sender notified
automatically removed from delivery queue
manually removed from delivery queue
queued (frozen)
connection did not complete
quarantined
expired from quarantine
manually removed from quarantine
released from quarantine
rejected without quarantine
automatically removed from delivery queue, sender notified
delivered
queued (delivery has failed)
Match:
All conditions
Return partial matches:
Columns to be displayed:
Datetime | Sender | Recipient | Subject | Classification
Customise
Start search

Storage period

The connections logged are by default accessible for up to 14 days. Optionally it's possible to store the logging for a longer time, this can be configured in the SpamExperts Control Panel.

Access

The logs can be easily downloaded or searched from the Web Interface.

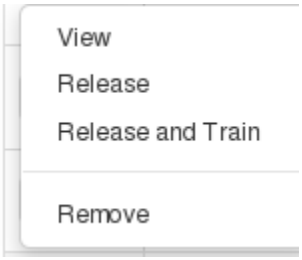
Delay

The logging data is processed every 10 minutes on all filtering nodes. It is possible to view messages waiting for migration by using the "**Latest Results**" option, otherwise there may be a small delay such as a few minutes.

Information logged

- Datetime
- Filtering server
- Message ID
- Sender IP
- Sender hostname
- Sender
- Recipient
- From
- To
- CC
- Subject
- Incoming size
- Outgoing size
- Delivery date
- Destination IP
- Destination host
- Destination port
- Status
- Classification

It's possible to view the message, release, release and train or remove.



Messages that return ‘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 Super-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.

Incoming Spam Quarantine

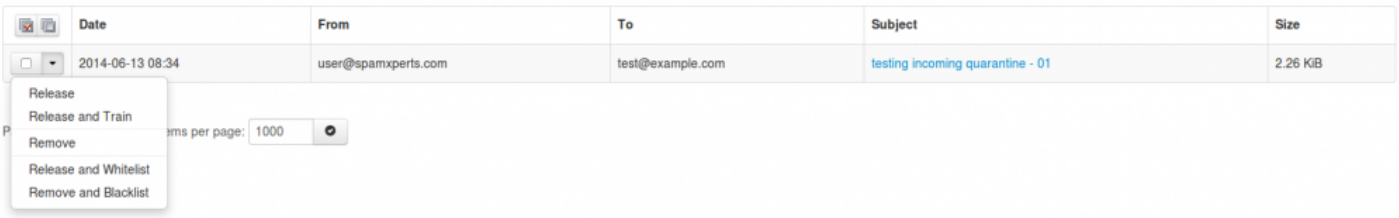
The Spam quarantine interface displays all the incoming quarantined messages.

> * By default, these are stored for 14 days, after which they are purged.

From the quarantine overview, you are able to view the messages and sort or search on specific criteria. The “From:” address us also displayed in the quarantine overview as the sender to resemble the results an email client would show.

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, for example: admin level, domain level or email user level, will not remove these from the other levels. This is by design.



‘**Release and Train**’ will deliver the message to the recipient and train the message as ham into our filtering system. This option is recommended by SpamExperts when releasing the messages from Spam Quarantine so that the filters can be correctly adjusted.

Clicking on the ‘**Release**’ option will release the 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 indented recipient and automatically add the 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 the sender's email address to 'Sender Blacklist'.

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 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 data-sets or save it.

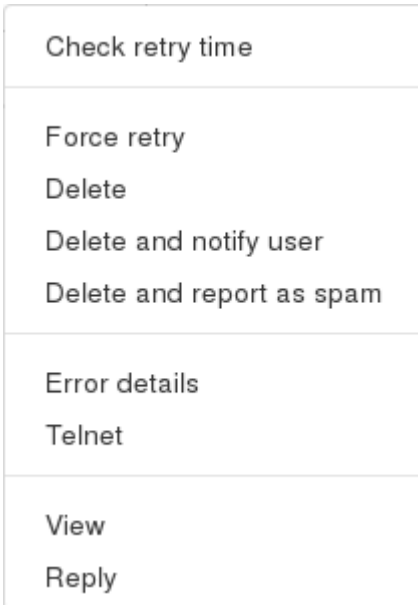
If an attachment is included in the quarantined message, then this can be individually downloaded by clicking on the **'Attachment:'** line in the normal view.

Incoming Delivery Queue

This page shows emails 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 using the drop down menu net to the message:

- 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)
- Reply (reply to the queued message directly from the interface



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

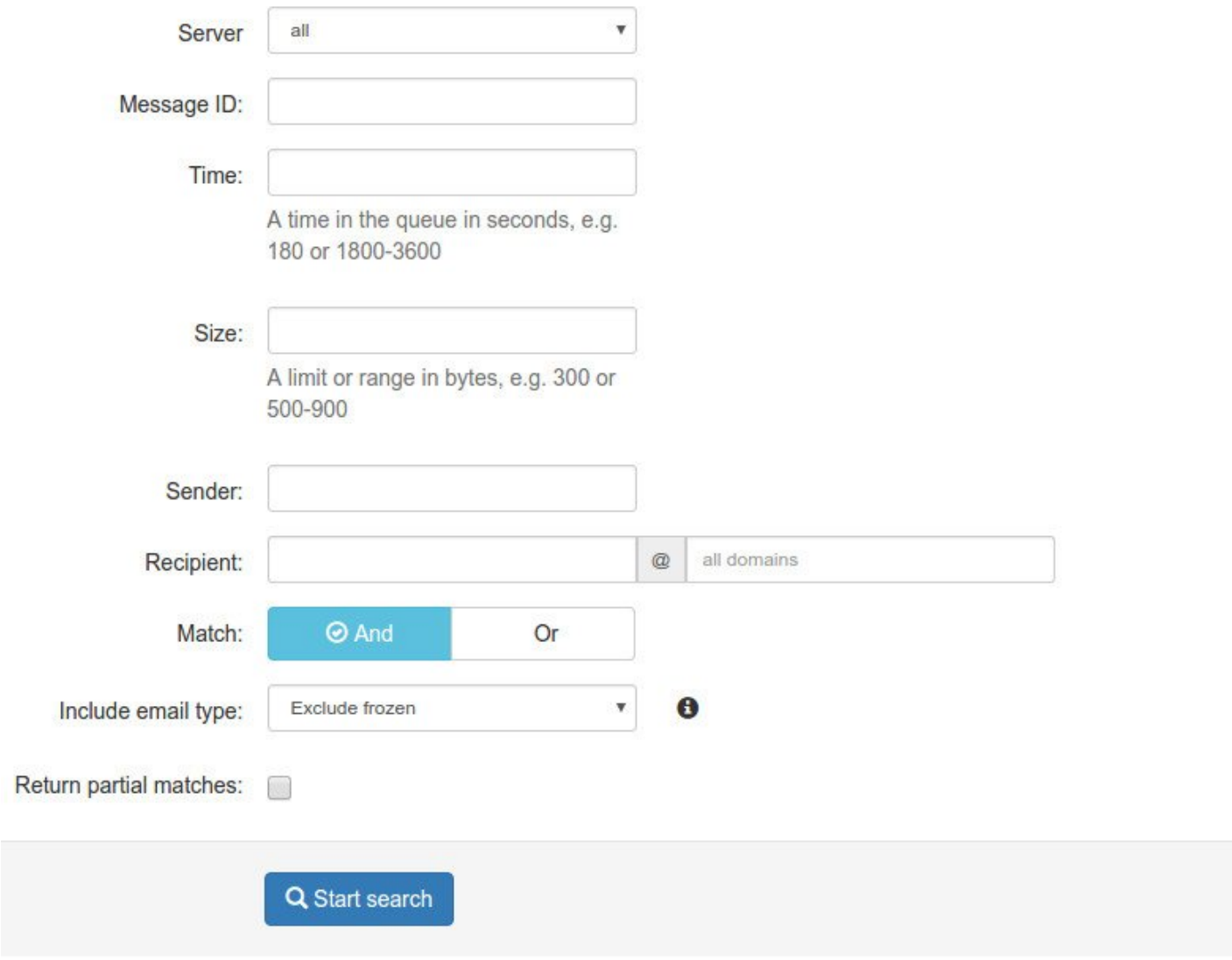
We have also reintroduced the option ‘Error details’ to check the reason why messages are stored in Delivery Queue.

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.

If you choose “Reply”, this allows you to compose and reply to a message to a sender when the message is queued.

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



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.

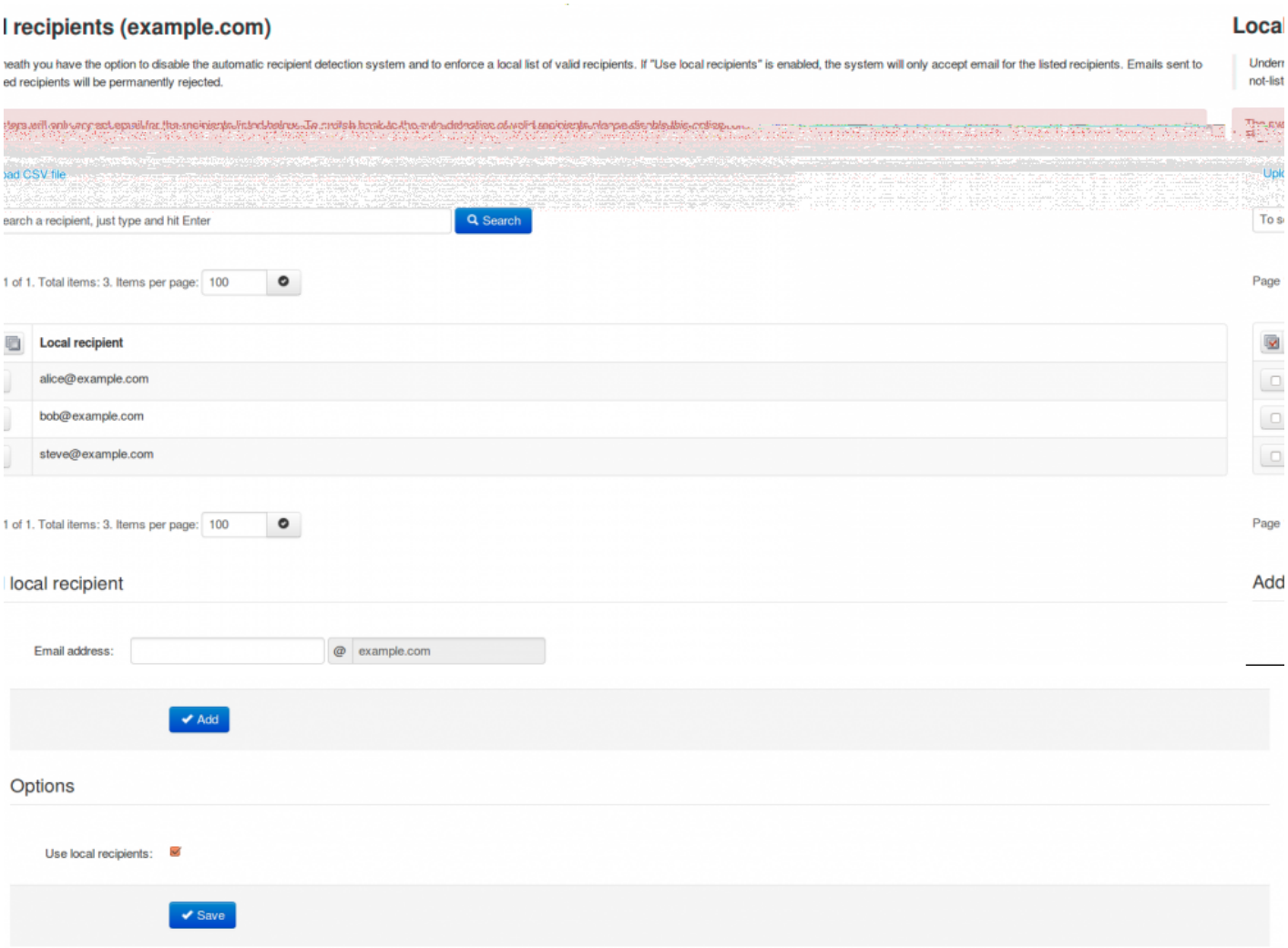
Local Recipients

This feature allows email traffic only to recipients already added on the below list, verifying the existence of an email account before accepting the email for it. For uploading a large list, for example thousands of email addresses, you can use the “Upload CSV file” feature which will automatically add the recipients without having to manually add them one by one.

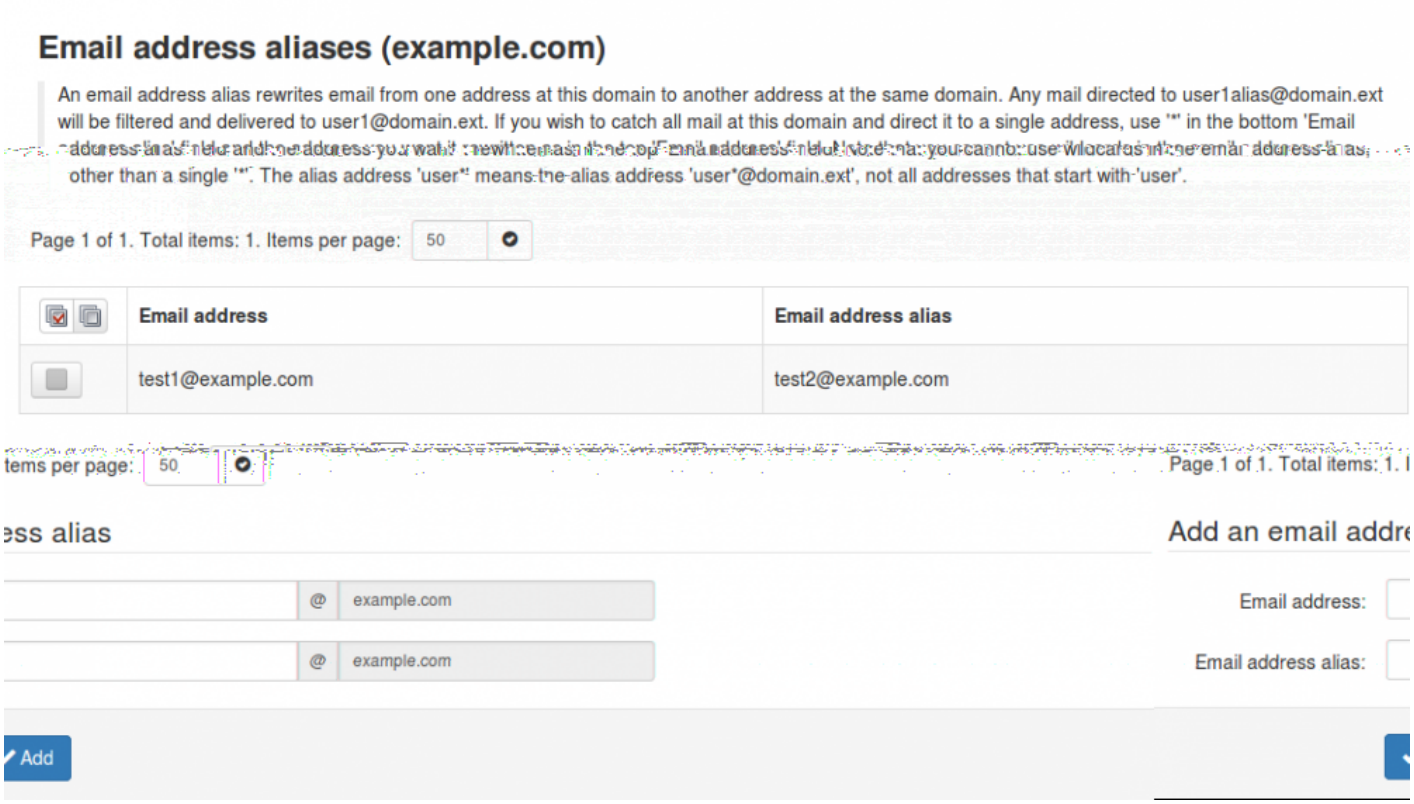
With local recipients you have to add all recipients by hand. If you do not add these users, you will not be able to receive emails on that account.

> ! 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.


l recipients (example.com)
Local
eath 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
ed recipients will be permanently rejected.
Under
not-list
ad CSV file
Upl
earch a recipient, just type and hit Enter
Search
To s
1 of 1. Total items: 3. Items per page: 100
Page
Local recipient
alice@example.com
bob@example.com
steve@example.com
1 of 1. Total items: 3. Items per page: 100
Page
local recipient
Add
Email address:
@
example.com
Add
Options
Use local recipients:
Save

Email Address Aliases

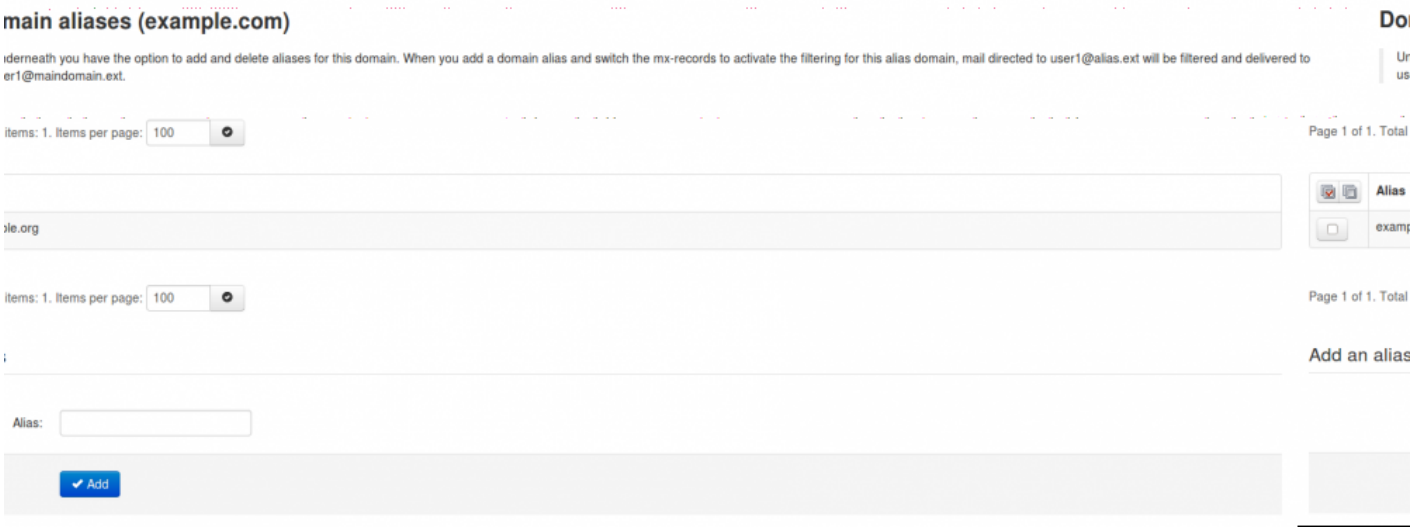


On the Email Address Aliases page you can add aliases for your email addresses

Simply fill in the two fields, “**Email Address**” and “**Email Address Alias**”, and click “**Add**”.

Now the email address alias will appear in the list. By selecting it (tick the checkbox) you can remove the alias.

Domain Aliases



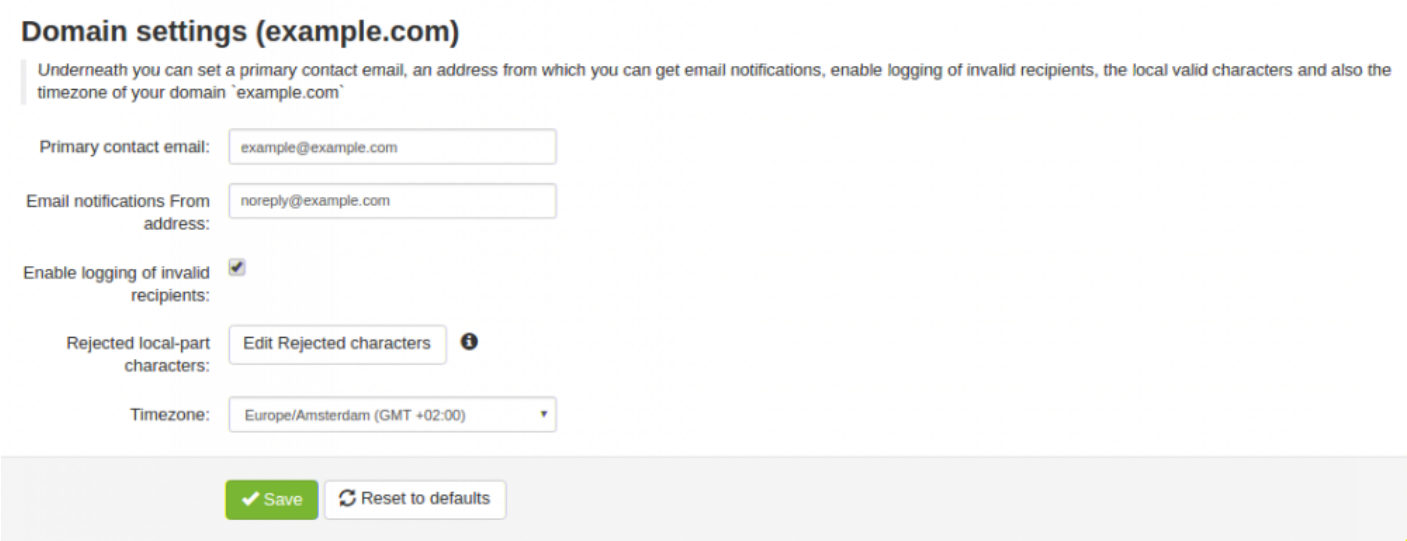
If you have multiple domains, you can make use of the domain aliasing option. Domain aliases can be added to your main domain directly in the web interface. Any email sent to the domain alias will be delivered to the same user on the main domain.

> * Messages delivered to the alais 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.



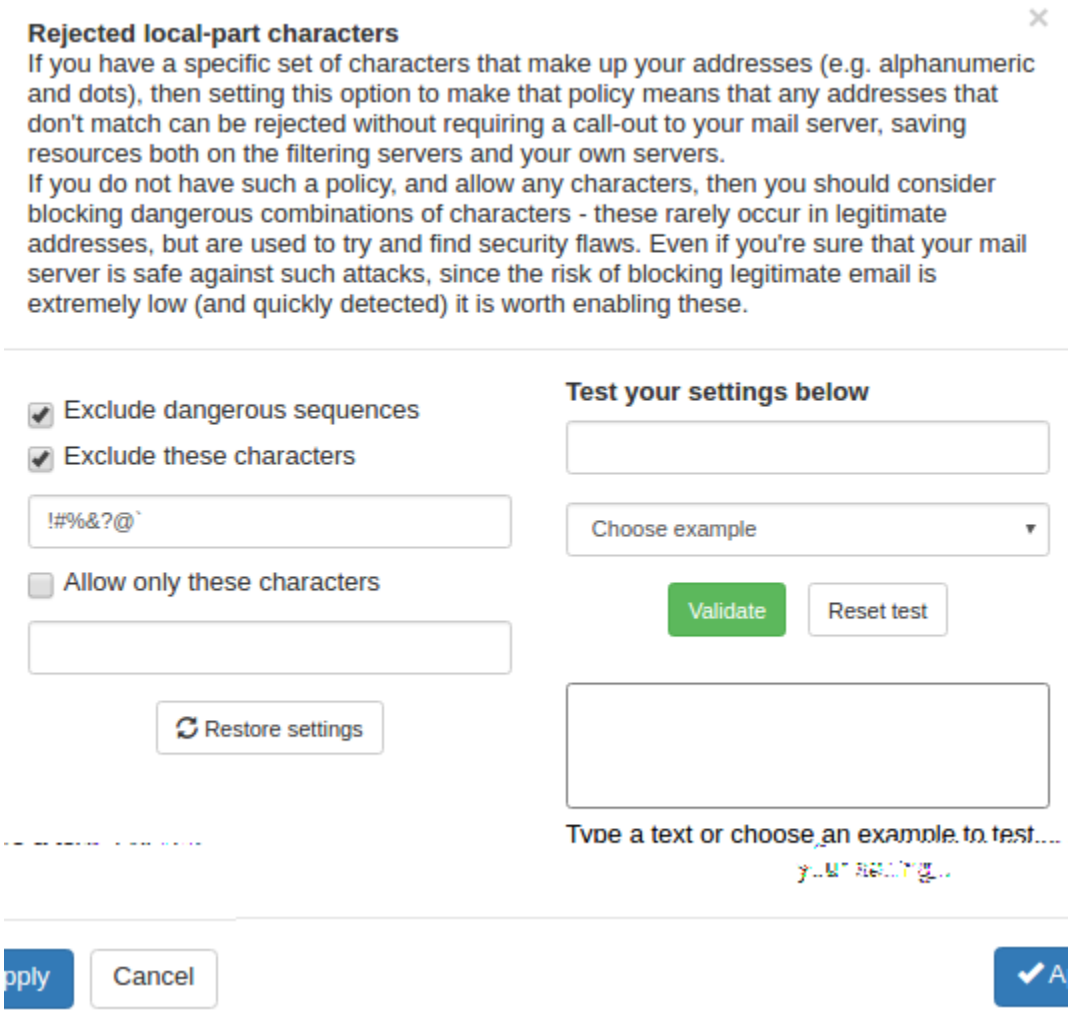
You can set the following options :

Basic Settings:

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

The Rejected local-part characters are the characters that are allowed in the local part (before the @ part) of the email address.

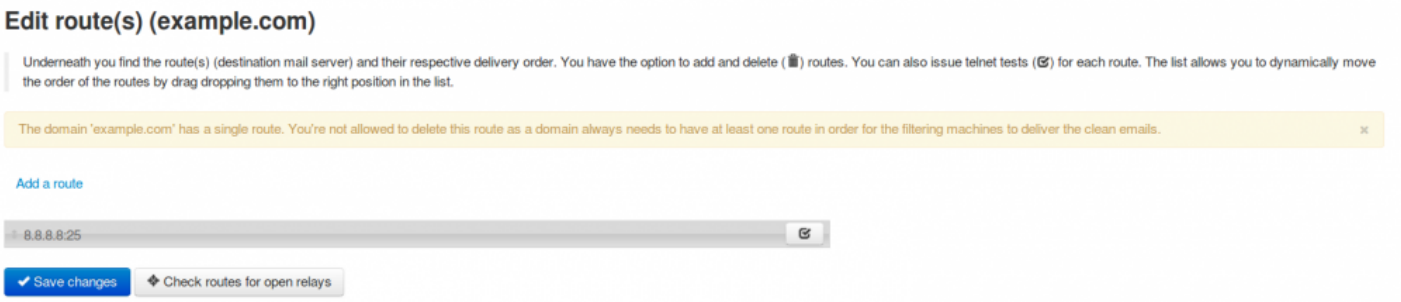
You can **Edit Rejected Characters** by setting up a list of regular expressions. If a local part of the recipient matches any of the regular expressions, then the recipient will be rejected.


Rejected local-part characters
If you have a specific set of characters that make up your addresses (e.g. alphanumeric and dots), then setting this option to make that policy means that any addresses that don't match can be rejected without requiring a call-out to your mail server, saving resources both on the filtering servers and your own servers.
If you do not have such a policy, and allow any characters, then you should consider blocking dangerous combinations of characters - these rarely occur in legitimate addresses, but are used to try and find security flaws. Even if you're sure that your mail server is safe against such attacks, since the risk of blocking legitimate email is extremely low (and quickly detected) it is worth enabling these.
Exclude dangerous sequences
Exclude these characters
!#%&?@`
Allow only these characters
Restore settings
Test your settings below
Choose example
Validate
Reset test
Type a text or choose an example to test....
pply
Cancel
A

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.

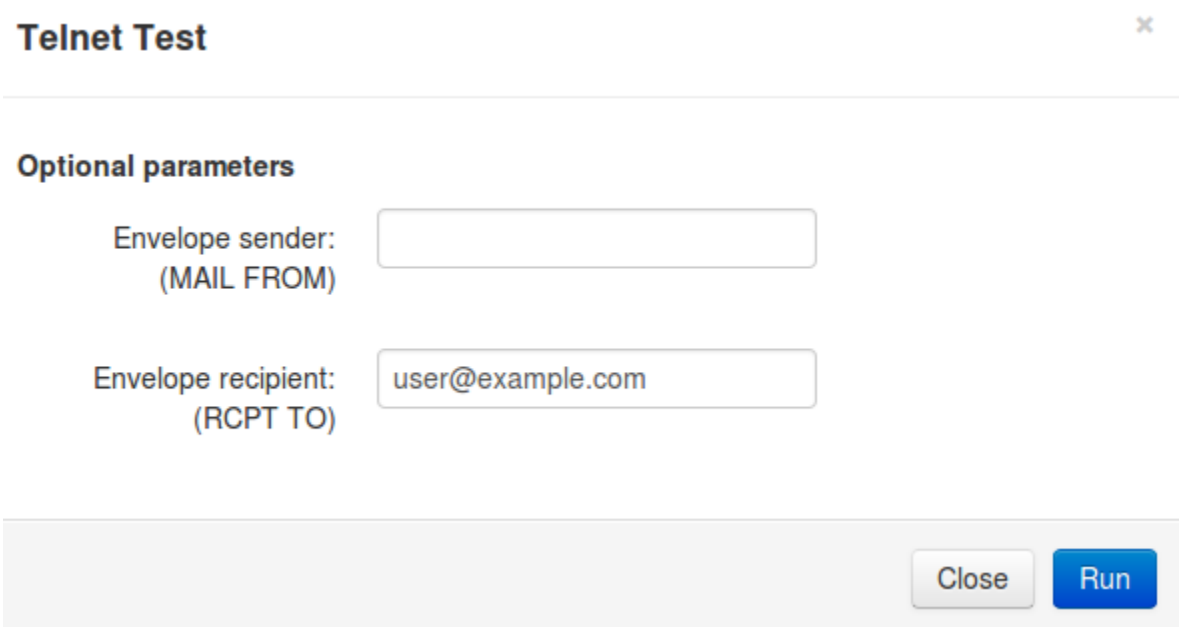


Whenever there are temporary problems with the first route (e.g. 4xx temporary rejects), we'll automatically try delivery to the second route. If there are permanent failures with a route (e.g. hostname not resolvable) we'll directly start queuing email and won't try the next route.

> * 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.

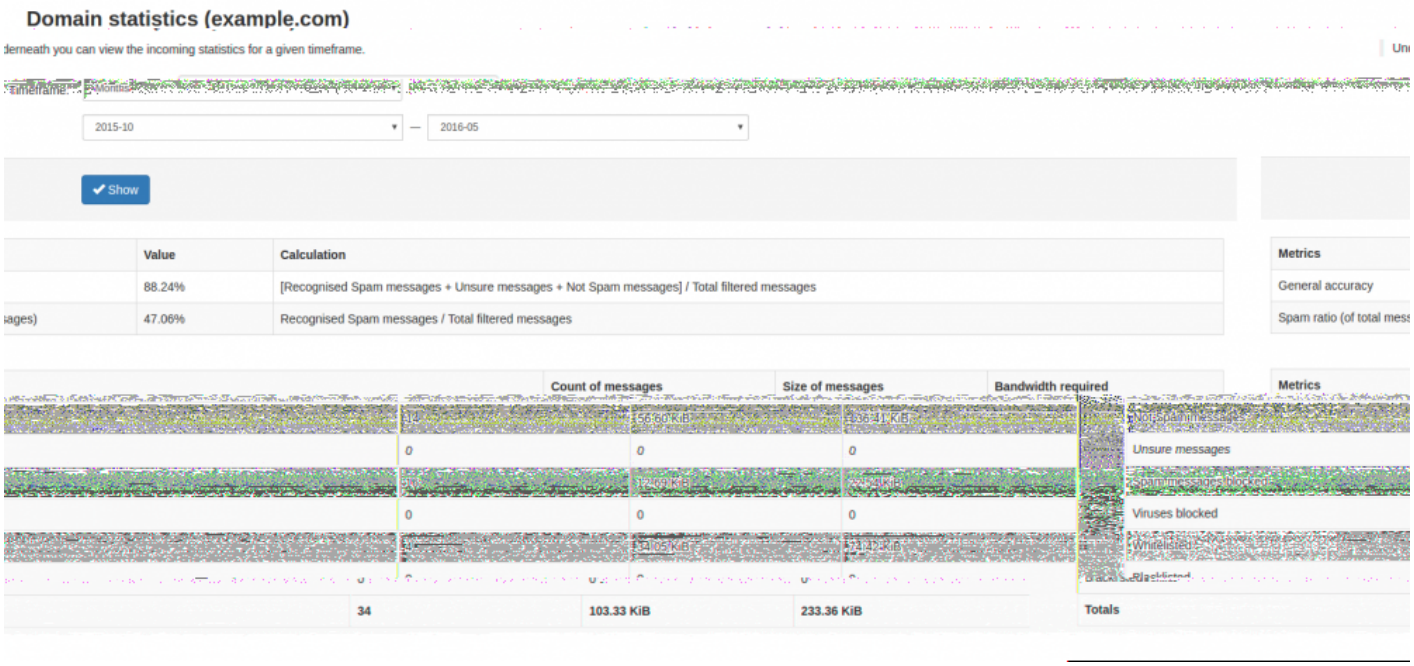
On this page you can now perform telnet tests for recipient callouts by pressing on the following icon next to the destination route:

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 the sender's email address (which can be blank if you want to use empty mail from address eg: 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

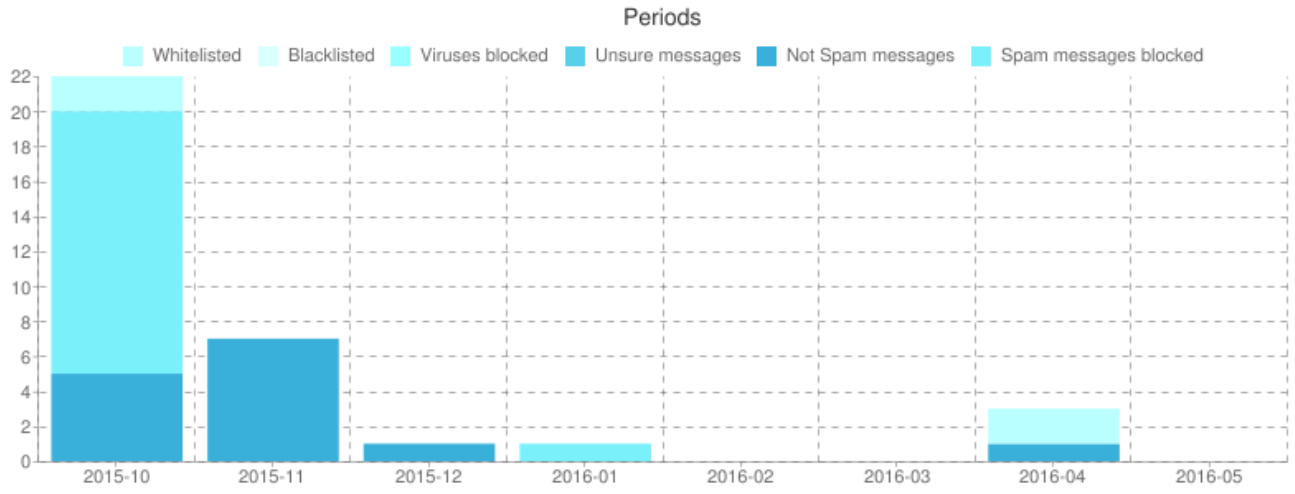
Domain Statistics

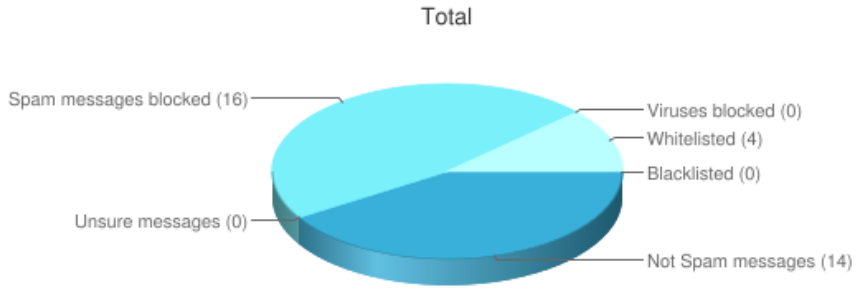
Here you can view the statistics for a given time-frame (Hours,Days,Weeks,Months,Years) of your incoming email traffic.



Statistics are displayed for :

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


Periods
Whitelisted
Blacklisted
Viruses blocked
Unsure messages
Not Spam messages
Spam messages blocked
22
20
18
16
14
12
10
8
6
4
2
0
2015-10
2015-11
2015-12
2016-01
2016-02
2016-03
2016-04
2016-05


Total
Spam messages blocked (16)
Viruses blocked (0)
Whitelisted (4)
Blacklisted (0)
Unsure messages (0)
Not Spam messages (14)

Filter settings

On this page 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.

> ! Be Advised: 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 0.3.

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.

Skip SPF Check

With this option enabled, emails for your domain will not be subject to SPF (Sender Policy Framework) checks.

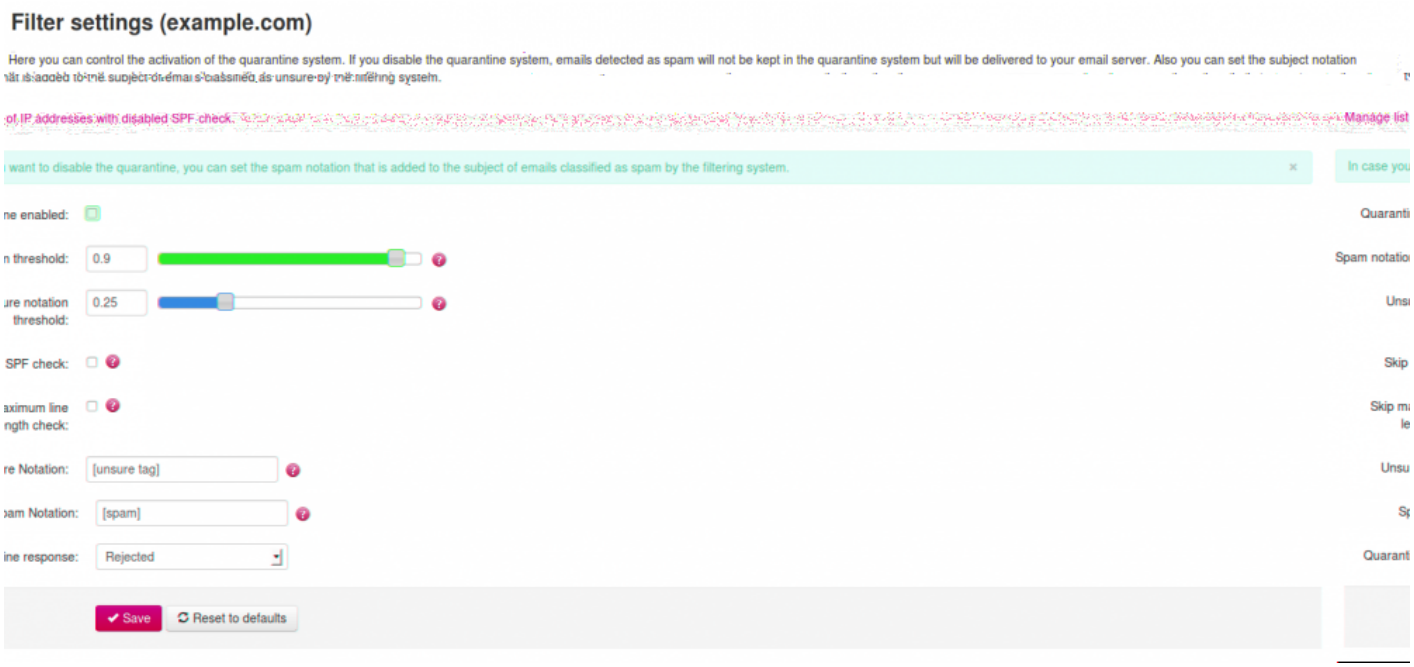
Skip Maximum Line Length

With this option enabled, emails for your domain will not be subject the RFC line length checks.

Quarantine Response

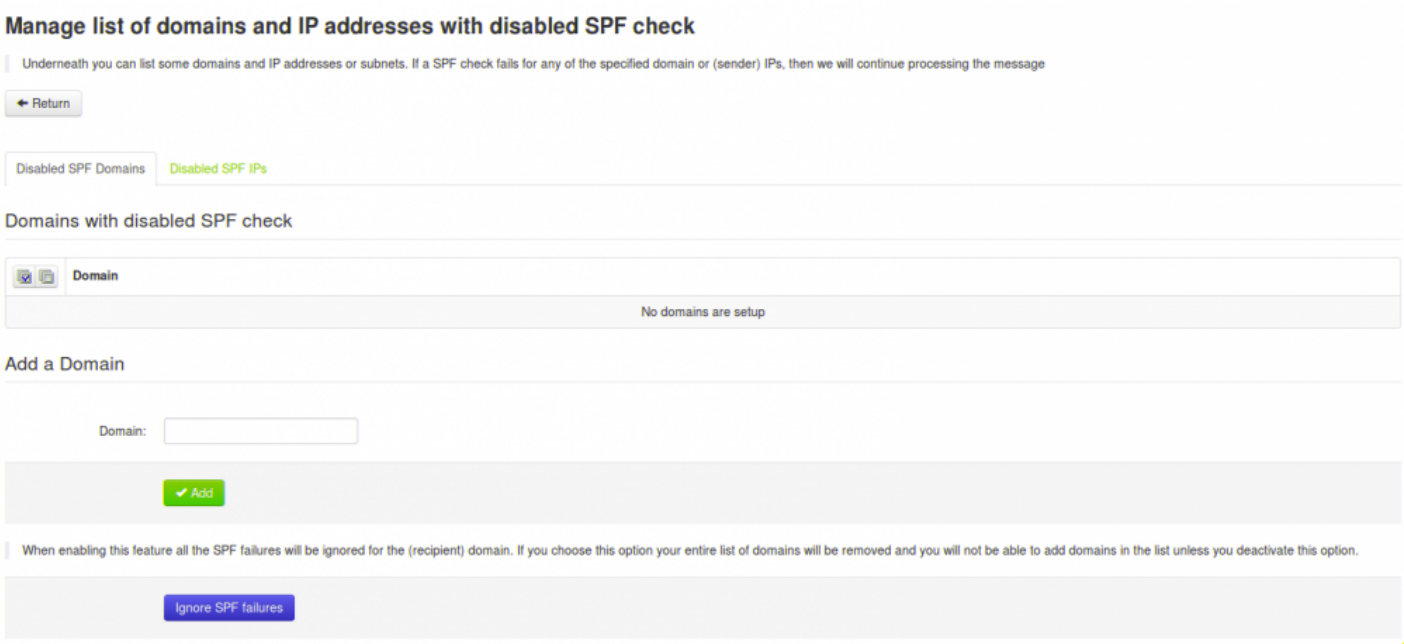
This you can set if you, for example, do not want senders to receive a bounce message when their mail gets blocked and quarantined. If you set it to Accept the message, the SMTP response would be 2xx accept however the message would still be blocked and shows in the Spam Quarantine. Since that technically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

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
of IP addresses with disabled SPF check.
Manage list
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.
In case you
ne enabled:
Quaranti
n threshold:
0.9
Spam notatio
ure notation threshold:
0.25
Unsı
SPF check:
Skip
aximum line ngth check:
Skip m
le
re Notation:
[unsure tag]
Unsu
pam Notation:
[spam]
Sp
ine response:
Rejected
Quarant
Save
Reset to defaults

Manage list of domains and IP addresses with disabled SPF check

On this page you can set the list of domains/IP addresses to skip the SPF (Sender Policy Framework) check.
Other checks still apply when adding IP addresses here.
This is particularly useful when dealing with forwarding servers or when you wish to ignore all the SPF failures for the (recipient) domain.




anage 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
abled SPF Domains
Disabled SPF IPs
addresses with disabled SPF check
IP address
No IP addresses are setup
d an IP
IP address:
Add
More actions
Reset all to default

Report Spam

With this option you can drag and drop or upload spam messages that passed the filter for immediate training to the systems.

The emails should be in **.eml**, **.txt** or **.msg** format and it must contain the full headers, including the SpamExperts additional headers.

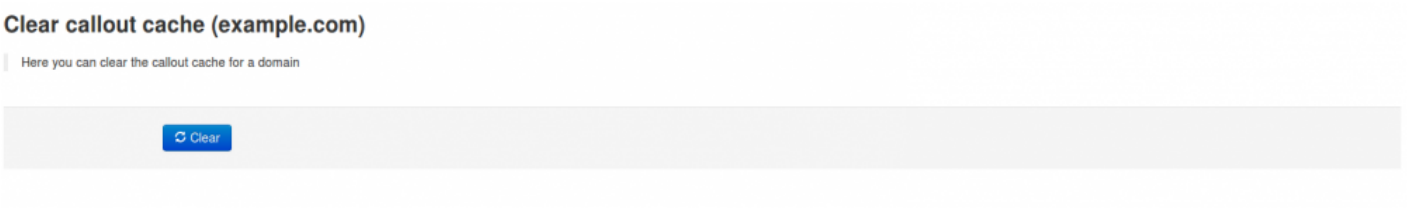
Report Not Spam

With this option you can drag and drop or upload messages you wish to classify as not spam (ham) for training.

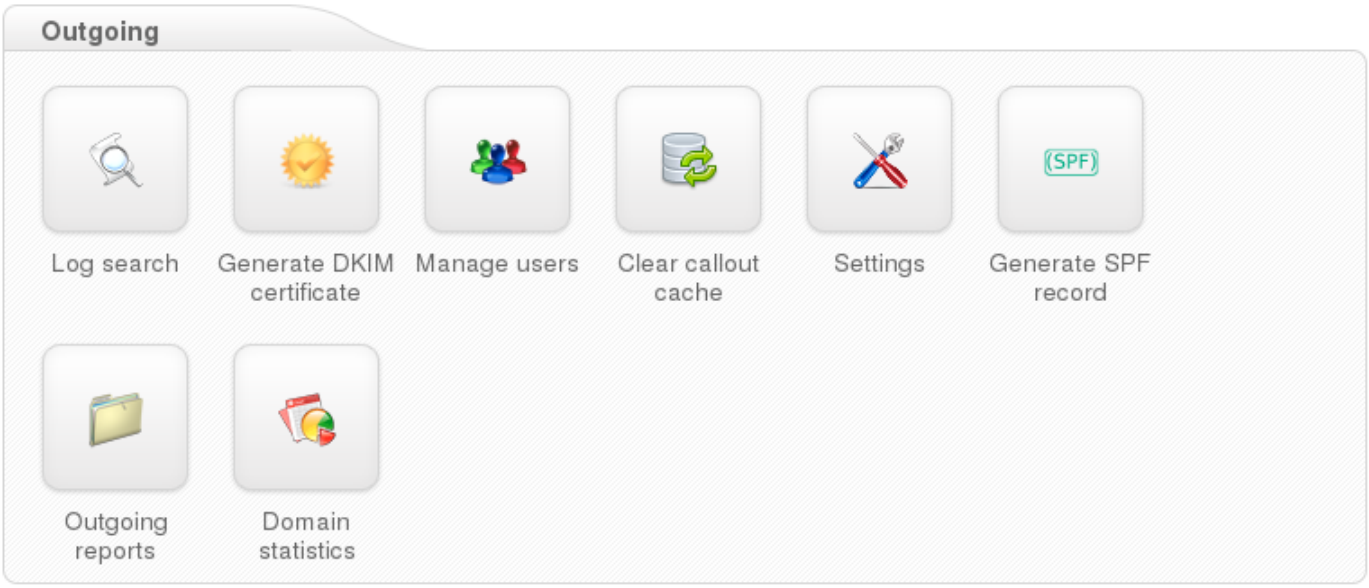
The emails must be in **.eml** / **.txt** format and it must contain the full headers, including the SpamExperts additional headers.

Clear Callout Cache

On this page 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.



Outgoing



- Outgoing Log Search
- Generate DKIM certificate
- Manage Outgoing Users
- Clear Callout Cache
- Settings
- Generate SPF record
- Outgoing Reports
- Domain Statistics

Outgoing Log Search

All email connections, spam and not spam, to a domain are logged to the logging server. To ensure a connection can be logged, the **“RCP 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 rate limiting is applied because of a flood of connections from a certain IP address, or when the sending server is violating certain requirements from the RFC 5321.

You can search on various strings and options, based on a date range, server, message ID, subject, sender, recipient, sender IP, hostname, delivery before and after, destination IP, destination host, destination port and also classifications such as all, accepted and rejected. The filters include more detailed classifications such as not spam, whitelisted, unsure, false positive, oversize, blacklisted, greylisted, false negative, phish, virus, spam, deferred and unknown.

The message status presents two buttons that select all or none of the following: queued, manually removed from quarantine, manually removed from delivery queue, released from quarantine, automatically removed from delivery queue, rejected without quarantine, manually removed from delivery queue, automatically removed from delivery queue, queued (frozen), delivered, connection did not complete, queued (delivery has failed), quarantined, expired from quarantine.
Users can also select if the search should match all conditions or any conditions, including returning partial matches.

By clicking on the **Customize** button, the displayed columns can be customized and include all of the following: Datetime, Filtering Server, Message ID, Sender Hostname, Sender, Recipient, From, To, CC, Subject, Incoming size, Outgoing size, Delivery date, Destination IP, Destination host, Destination port, Status and Classification.

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 “set” 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:
within range
Date range:
2016-04-19 00:00
2016-04-20 14:25
Filtering server:
All
Message ID:
Subject:
Sender:
example@example.com
User:
example.com
Recipient:
User identification:
Sender IP:
Sender hostname:
Delivery after:
Delivery before:
Destination IP:
Destination host:
Destination port:
Classification:
All
Accepted
Rejected
not spam
whitelisted
unsure
false positive
oversize
blacklisted
locked
false negative
phish
virus
spam
deferred
unknown
Status:
All
None
queued
manually removed from quarantine
manually removed from delivery queue, sender notified
released from quarantine
automatically removed from delivery queue
rejected without quarantine
manually-removed from-delivery queue-
automatically removed from delivery queue, sender-notified
queued (frozen)-
delivered
connection did not complete
queued (delivery has failed)
quarantined
expired from quarantine
Match:
All conditions
Return partial matches:
lumns to be displayed:
Datetime | User | User identification | Sender | Recipient | Subject | Classification
Customise
Start search
Reset
Export

Storage period

The connections logged are by default accessible for up to 30 days. Optionally it's possible to store the logging for a longer time. This can be configured in SpamExperts Control Panel.

Access

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

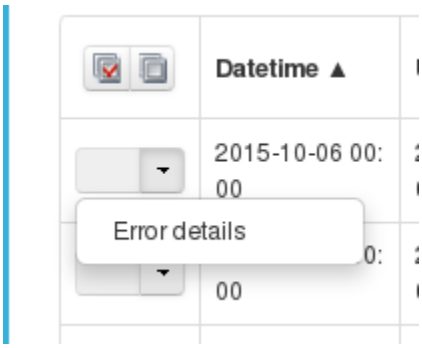
Delay

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 around 5 minutes.

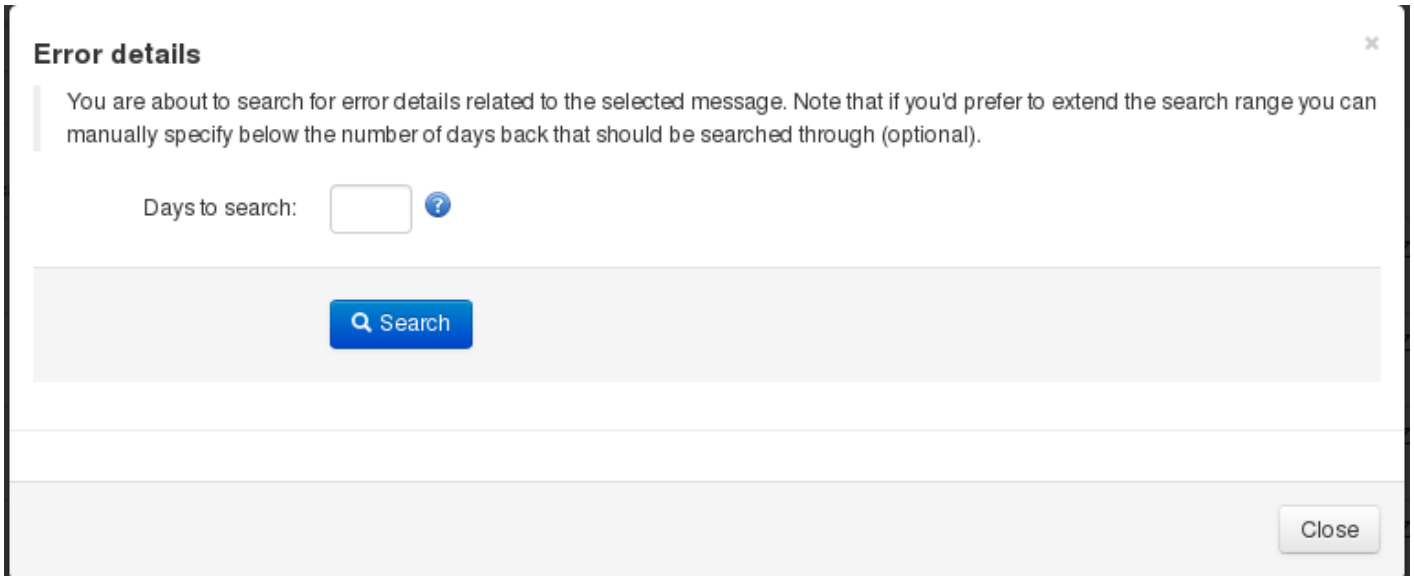
Information logged

- Datetime
- Filtering server
- Message ID
- Sender IP
- Sender hostname
- User
- User identification
- Sender
- Recipient
- From
- To
- CC
- Subject
- Incoming size
- Outgoing size
- Delivery date
- Destination IP
- Destination host
- Destination port
- Status
- Classification

It's possible to view the **"error details"** of the message by using the drop down box on the specific message line.



Here you can manually specify the number of days that should be searched through, starting from 1 and up to 31.



! For Super-Admins: 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 many domains and large amounts of data.

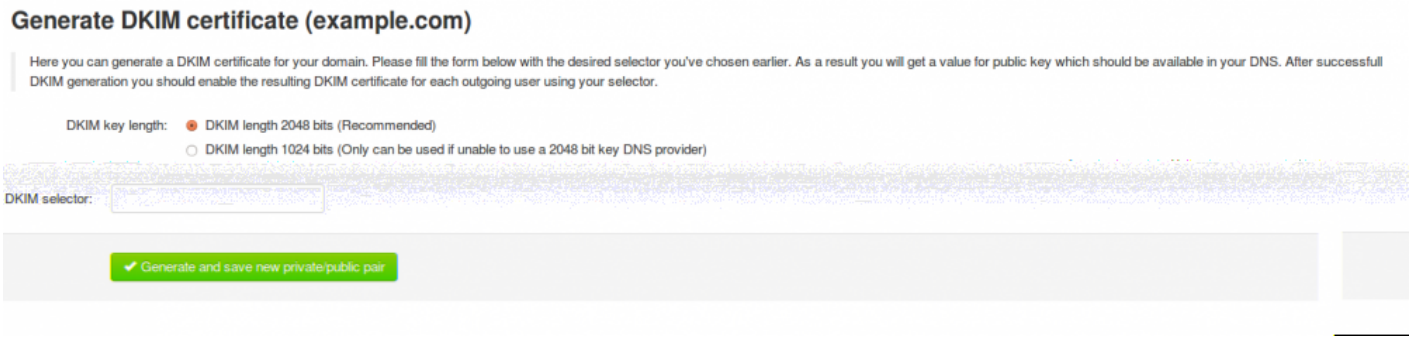
Generate DKIM certificate

On this page can generate a DKIM (DomainKeys Identified Mail) 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.

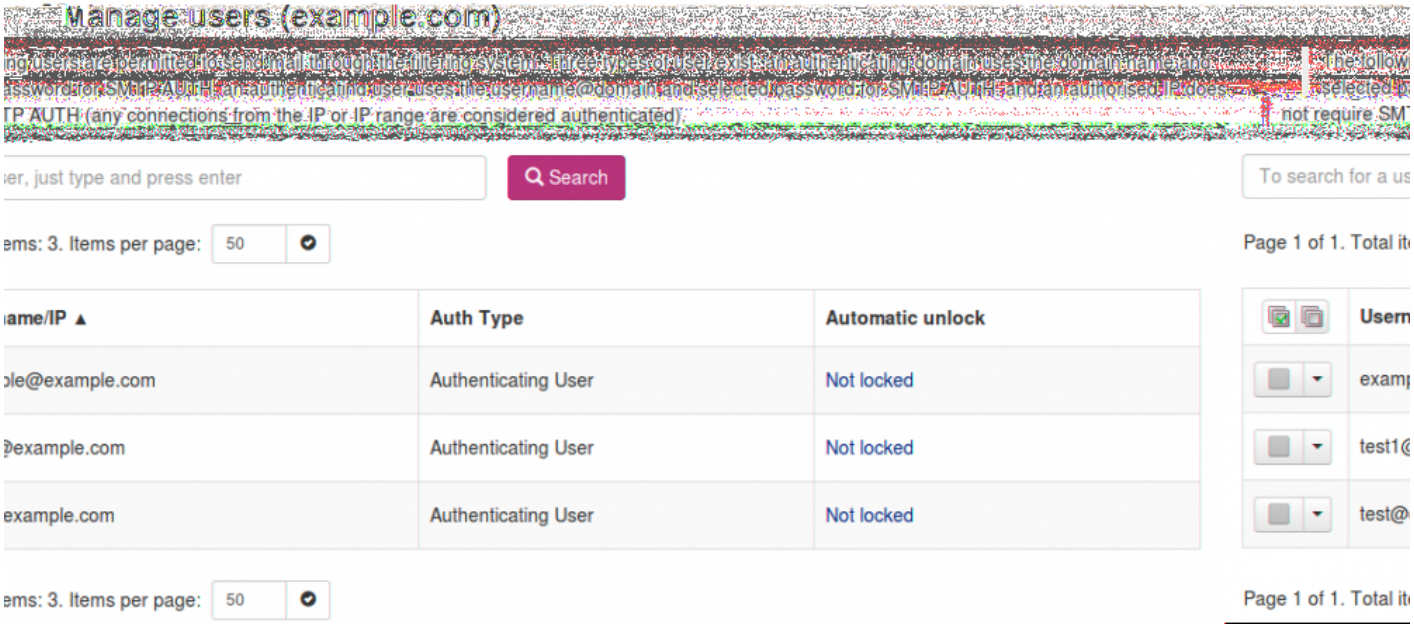
The key lengths that can be chosen are:

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

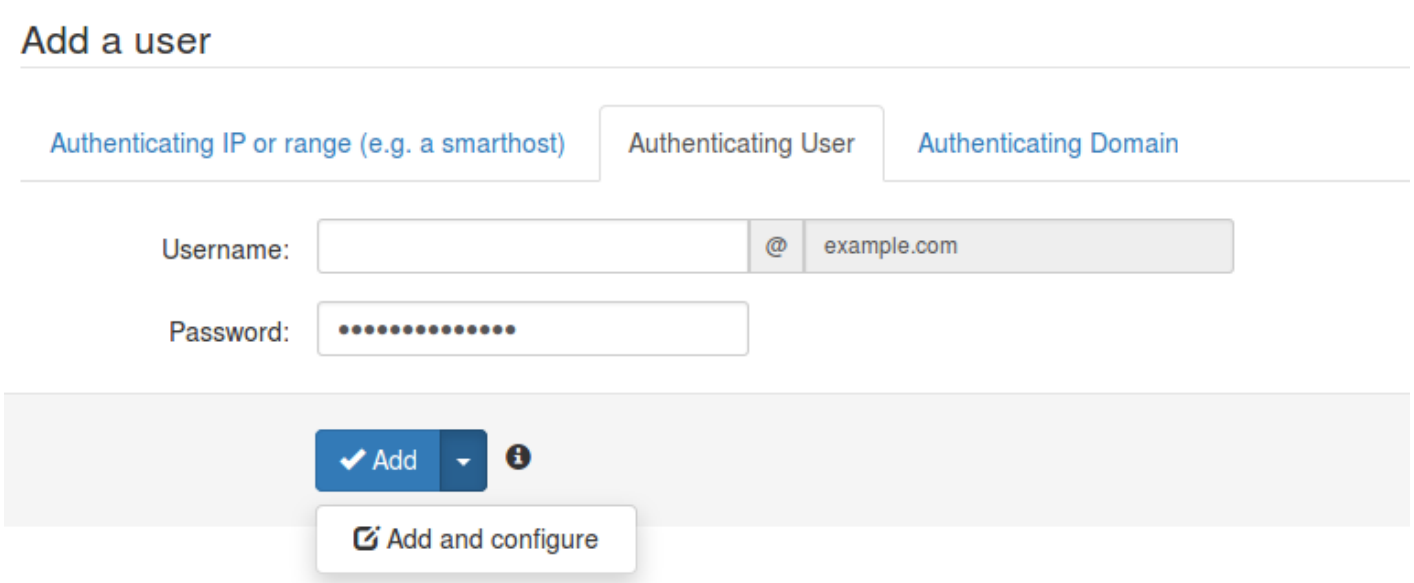


Manage Outgoing Users

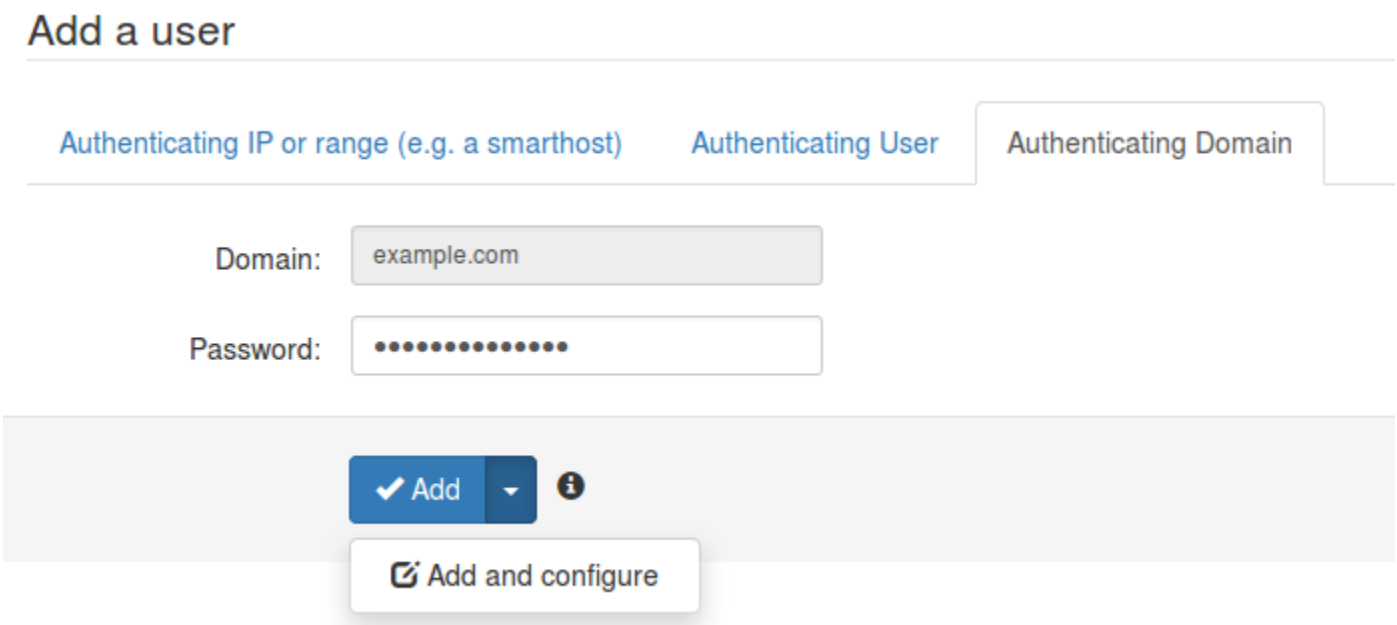
This feature enables you to create and manage outgoing users.



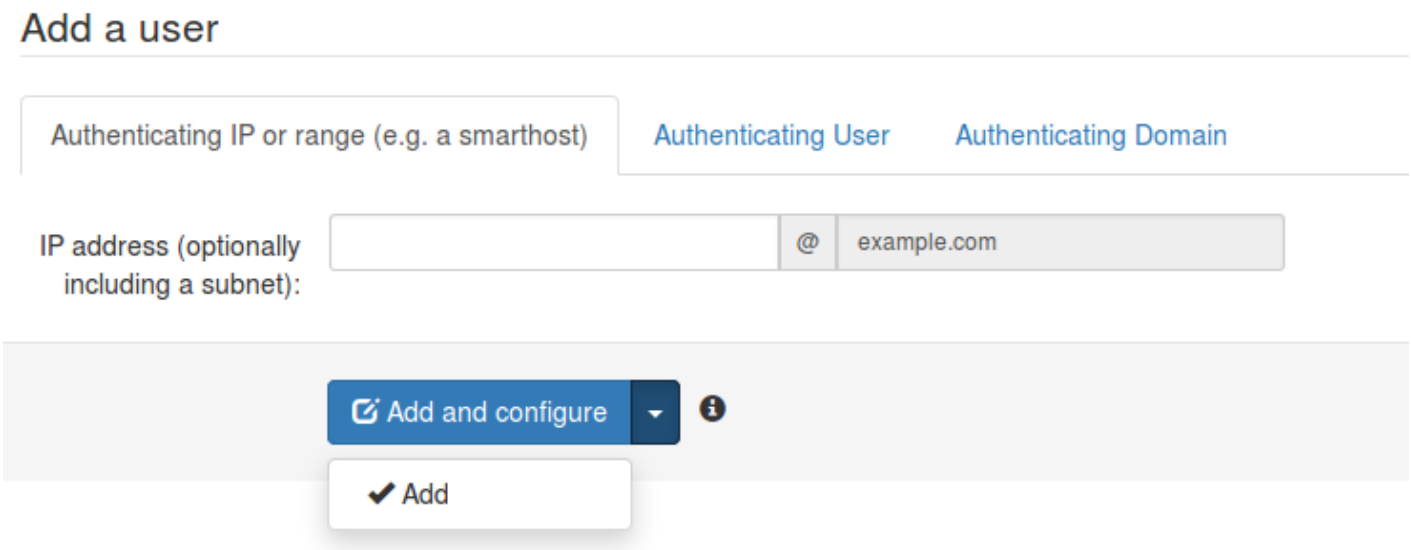
When adding Outgoing Users you can choose from:



“**Authenticating User**” – which means that the SMTP AUTH username will be ‘Username@out.example.com’, 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 using SMTP AUTH.

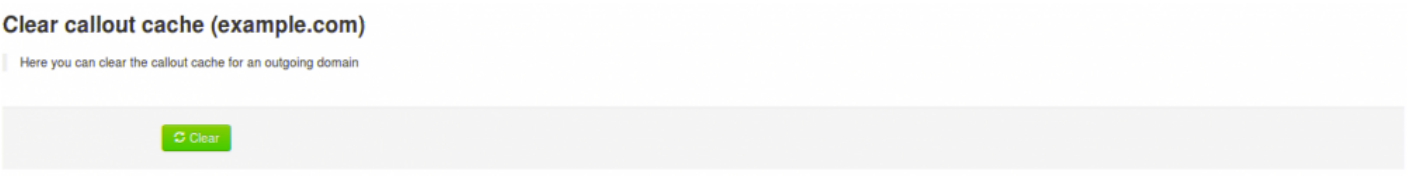
By editing the outgoing user you can manage the settings applied to that specific outgoing user:

- **Password**: Set the password for the per username authenticated outgoing user (N/A for IP outgoing users).
- **Identification Method**: Here you can choose from: “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 per month sent by the user.
- **Outgoing Limit per week**: the limit for outgoing messages per week sent by the user.
- **Outgoing Limit per hour**: the limit for outgoing messages per hour sent by all the user.
- **Outgoing Limit per minute**: the limit for outgoing messages per 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. (**Not Applicable at Domain Level**)
- **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). (**Not Applicable at Domain Level**)
- **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.

Clear Callout Cache (Outgoing)

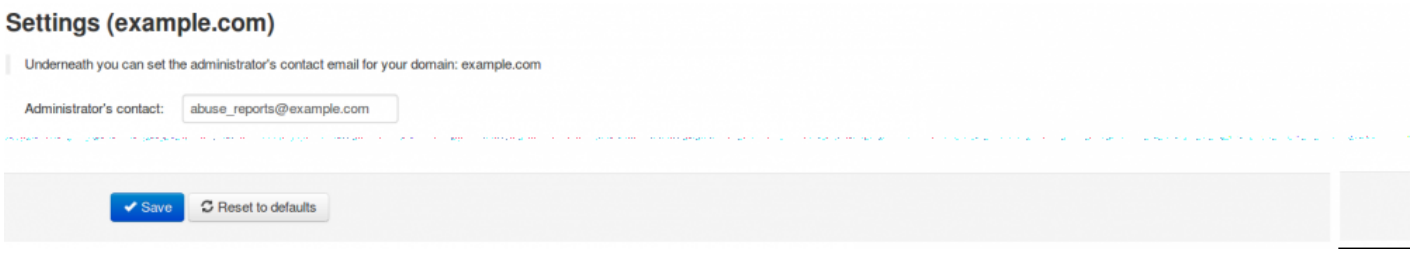
On this page you can clear the callout cache for an outgoing domain.



Settings

On this page you can set the administrator's contact email for the domain.

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



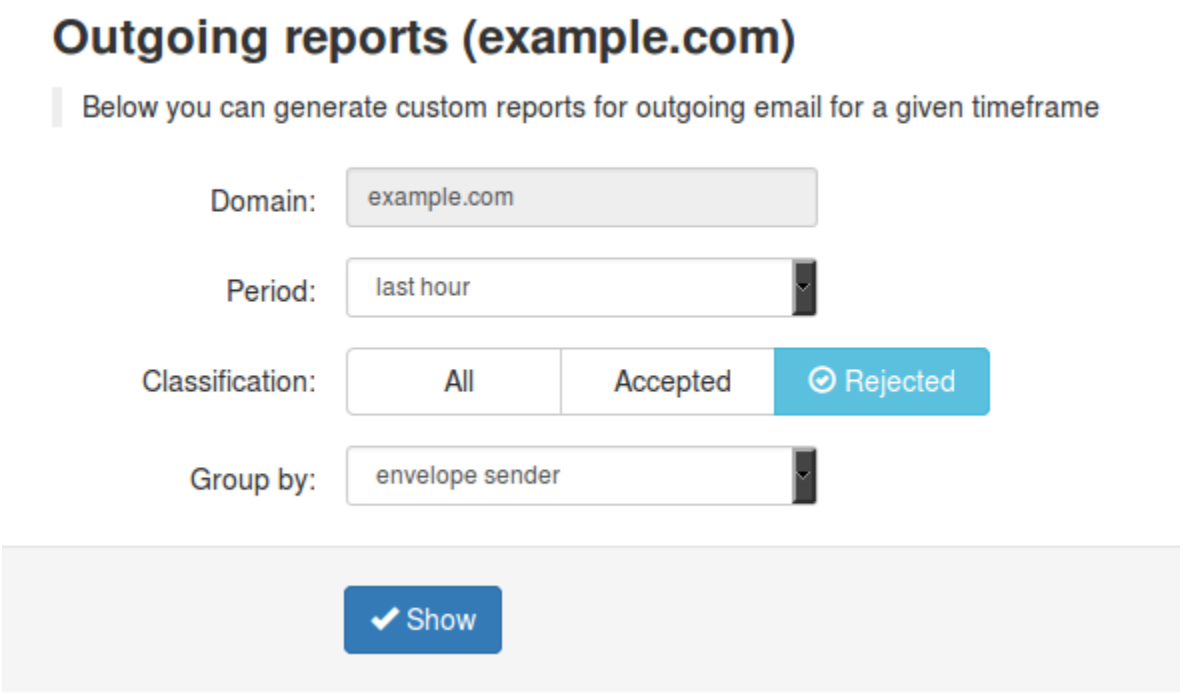
Generate SPF record

On this page you can generate a SPF record.

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

Outgoing Reports

With the Outgoing Reports function you can generate custom reports for outgoing email for a given time frame.

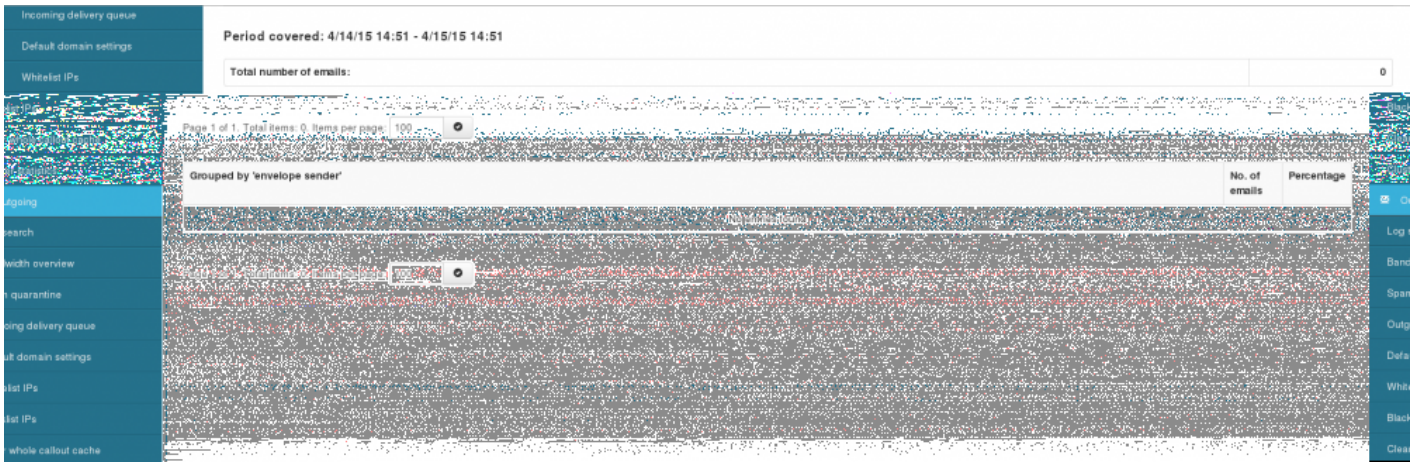


You can see from these reports the number of messages sent for a time frame ranging from last hour up to the last seven days.

If you select a Domain you can:

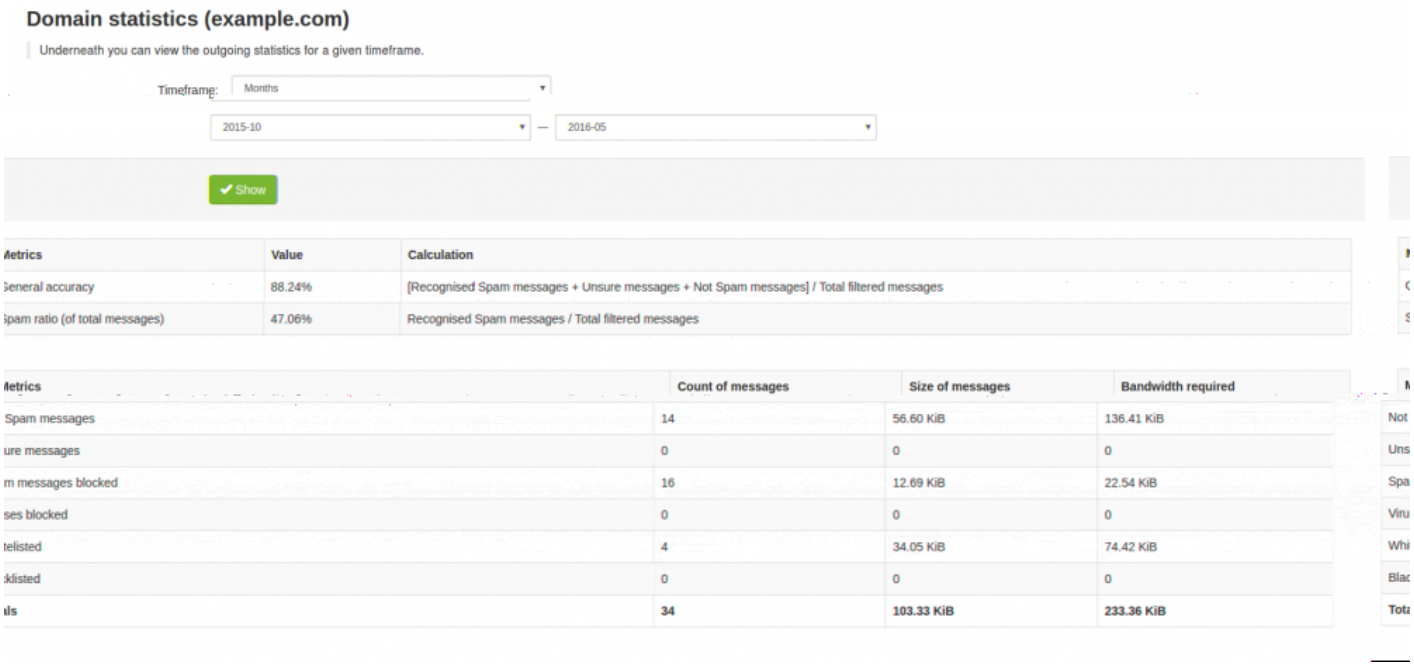
- Select the **Period** – from Last hour to Last 7 Days
- Sort the messages by their **Classification** – All, Accepted, Rejected
- **Group by** identity, envelope sender or from header

The report will show the total number of messages sent for the selected period, the number of messages sent by each sender and a percentage.


Incoming delivery queue
Default domain settings
Whitelist IPs
Period covered: 4/14/15 14:51 - 4/15/15 14:51
Total number of emails:
0
Grouped by 'envelope sender'
No. of emails
Percentage

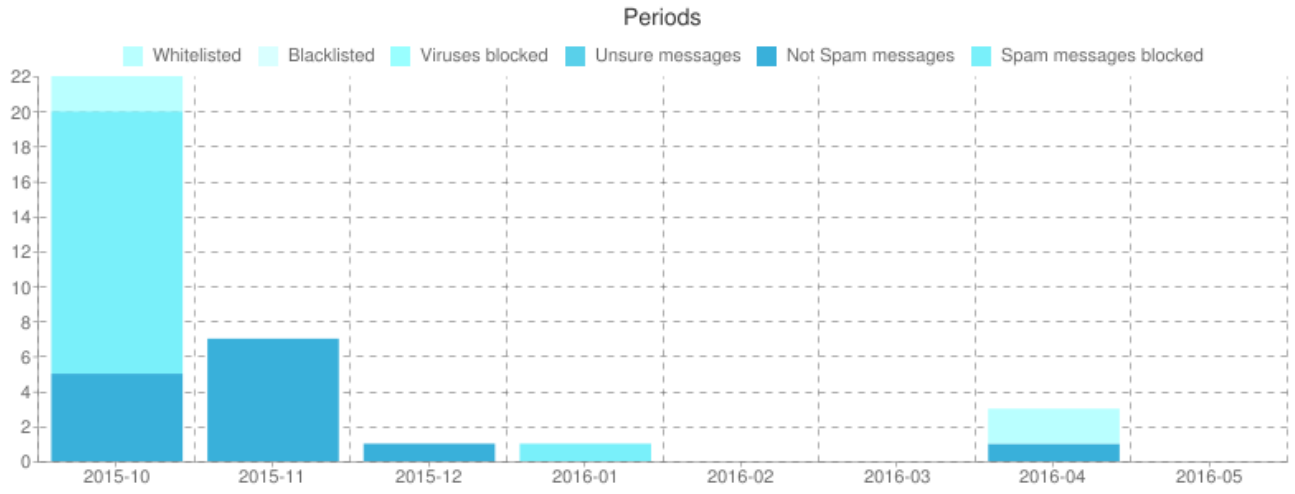
Domain Statistics (Outgoing)

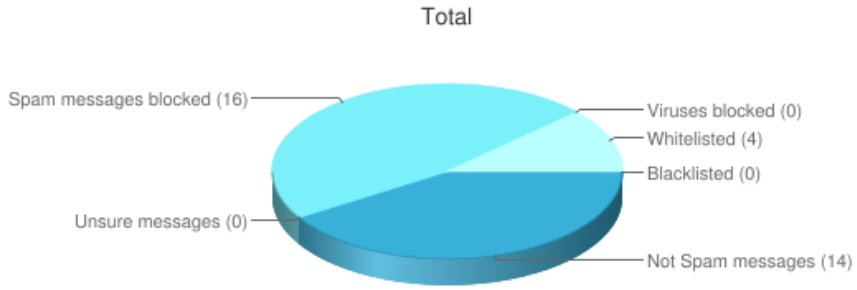
Here you can view the statistics for a given time-frame (Hours,Days,Weeks,Months,Years) of your outgoing email traffic.



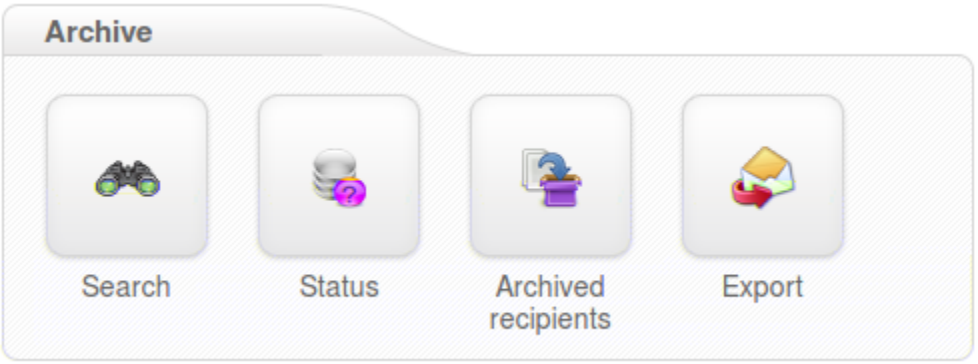
Statistics are displayed for :

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


Periods
Whitelisted
Blacklisted
Viruses blocked
Unsure messages
Not Spam messages
Spam messages blocked
22
20
18
16
14
12
10
8
6
4
2
0
2015-10
2015-11
2015-12
2016-01
2016-02
2016-03
2016-04
2016-05


Total
Spam messages blocked (16)
Viruses blocked (0)
Whitelisted (4)
Blacklisted (0)
Unsure messages (0)
Not Spam messages (14)

Archive



- Search
- Status
- Archived Recipients
- Export

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’, can not 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’.

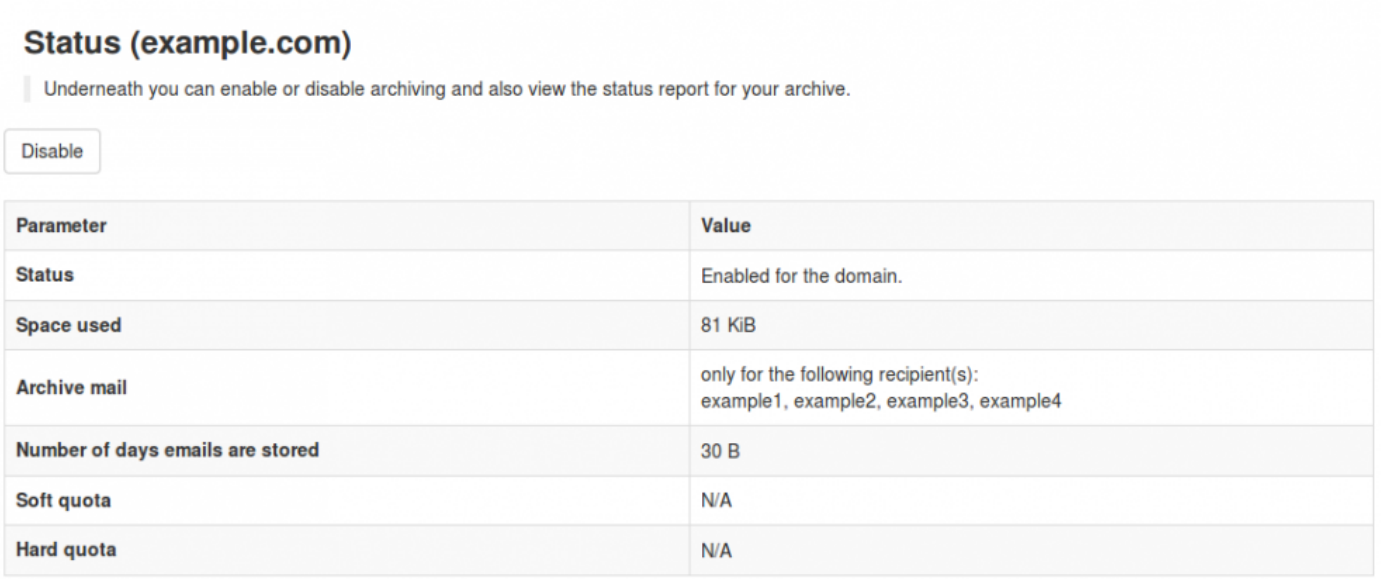
All archived emails are indexed including readable attachments. They can be searched using any search string.

Status

On this page you can check the status of your Archiving service.

As a domain user you can check the following:

- Space Used
- Archived email for recipients
- Number of days emails are stored
- Soft quota
- Hard quota



Status (example.com)

Underneath you can enable or disable archiving and also view the status report for your archive.

Disable

Parameter	Value
Status	Enabled for the domain.
Space used	81 KiB
Archive mail	only for the following recipient(s): example1, example2, example3, example4
Number of days emails are stored	30 B
Soft quota	N/A
Hard quota	N/A

As a Super-Admin you will see the following parameters, including the ones from above if you go to your domain (Super-Admin Dashboard – Overview – Select a domain – Archiving – Status).

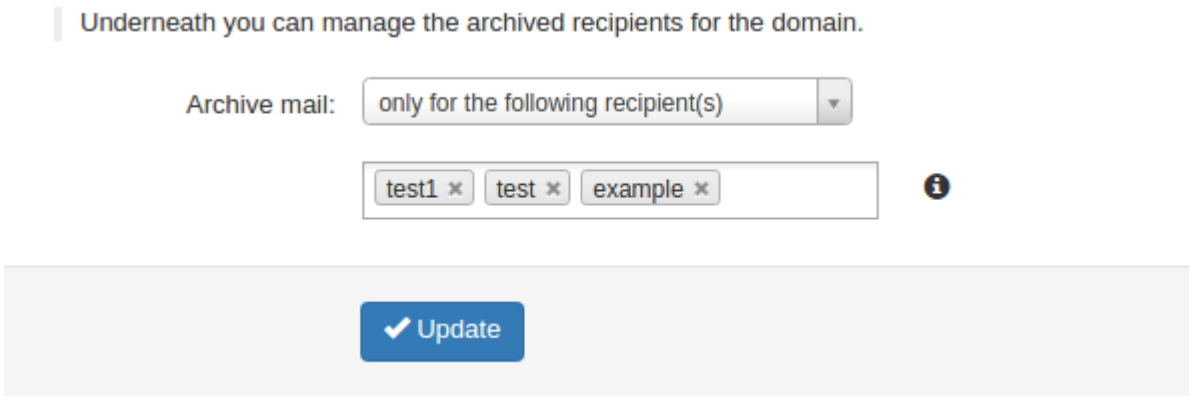
- Number of days emails are stored
- Soft quota
- Hard quota

Parameter	Value
Number of days emails are stored	0

Archived Recipients

On this page you can manage the archived recipients for your domain.

You have the options to manage all recipients, a list of specific recipients, or all recipients except a list of recipients.

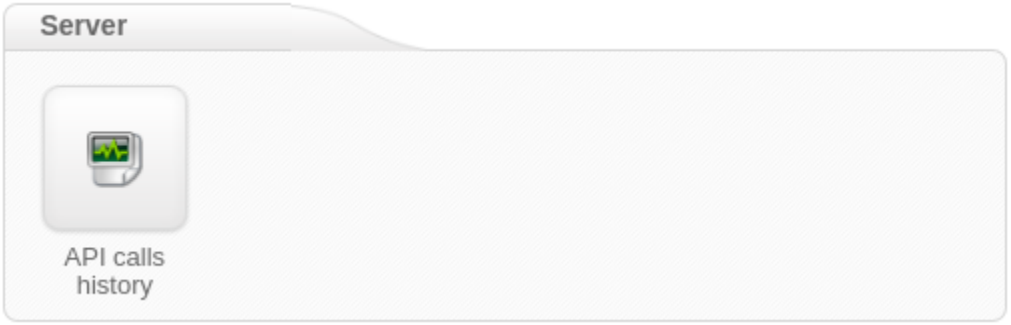


> **!** Be Advised: The list should be separated by a space ( ) or a comma (,). Also, please provide only the local part of the recipient's email address. For example only add "**test**" from the "**test@example.com**" email address.

Export

Using the Export feature 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.

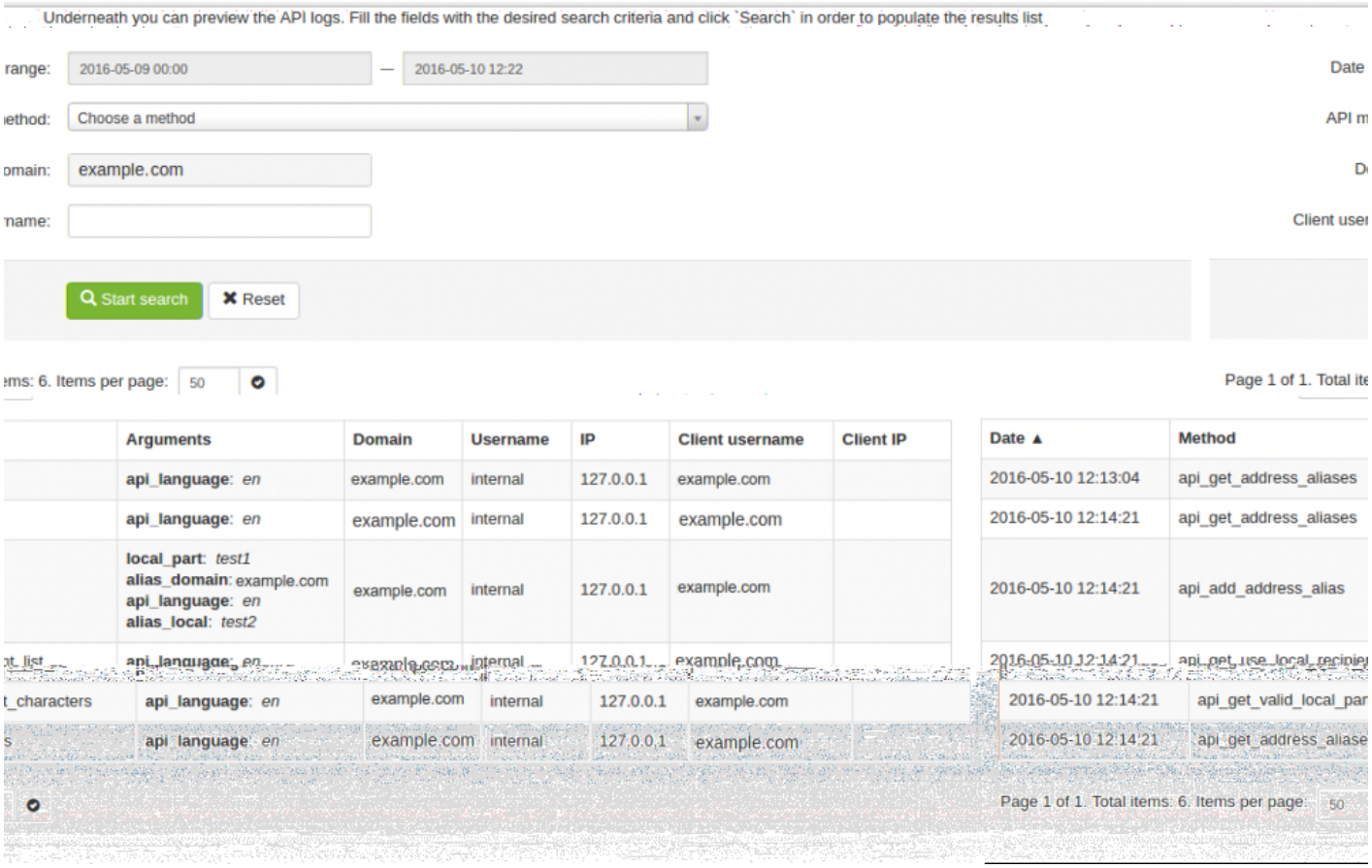
Server



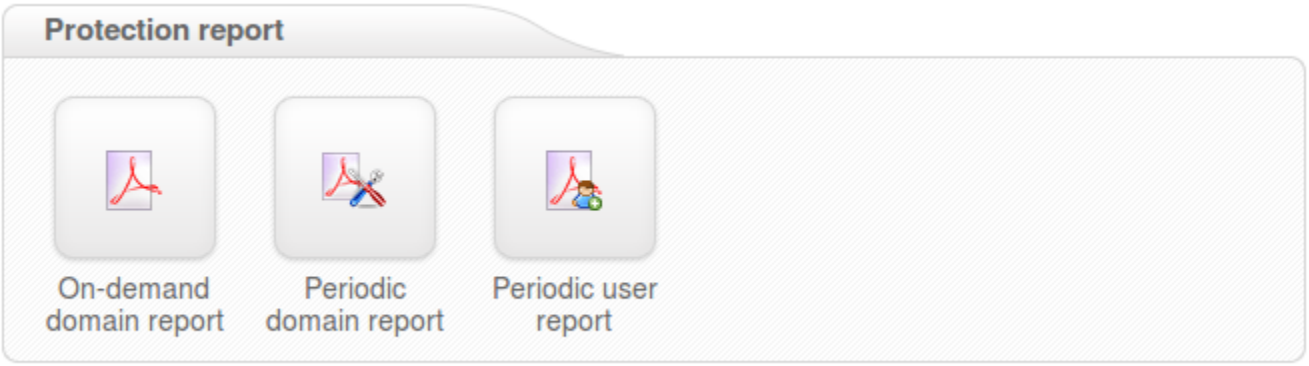
- API Calls History

API Calls History

Here you can check the history of the SpamExperts Control Panel API calls by selecting a time-frame, type of API call and client username.

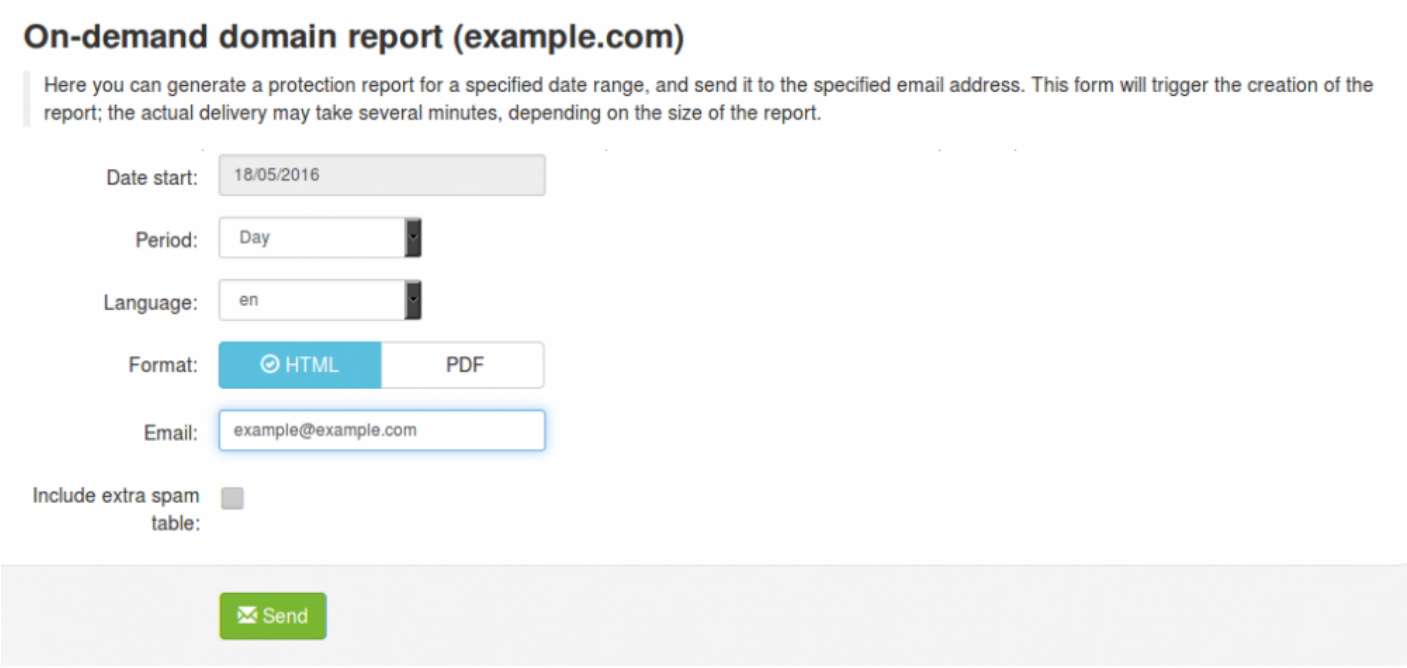


Protection Report



- On-Demand Domain Report
- Periodic Domain Report
- Periodic User Reports

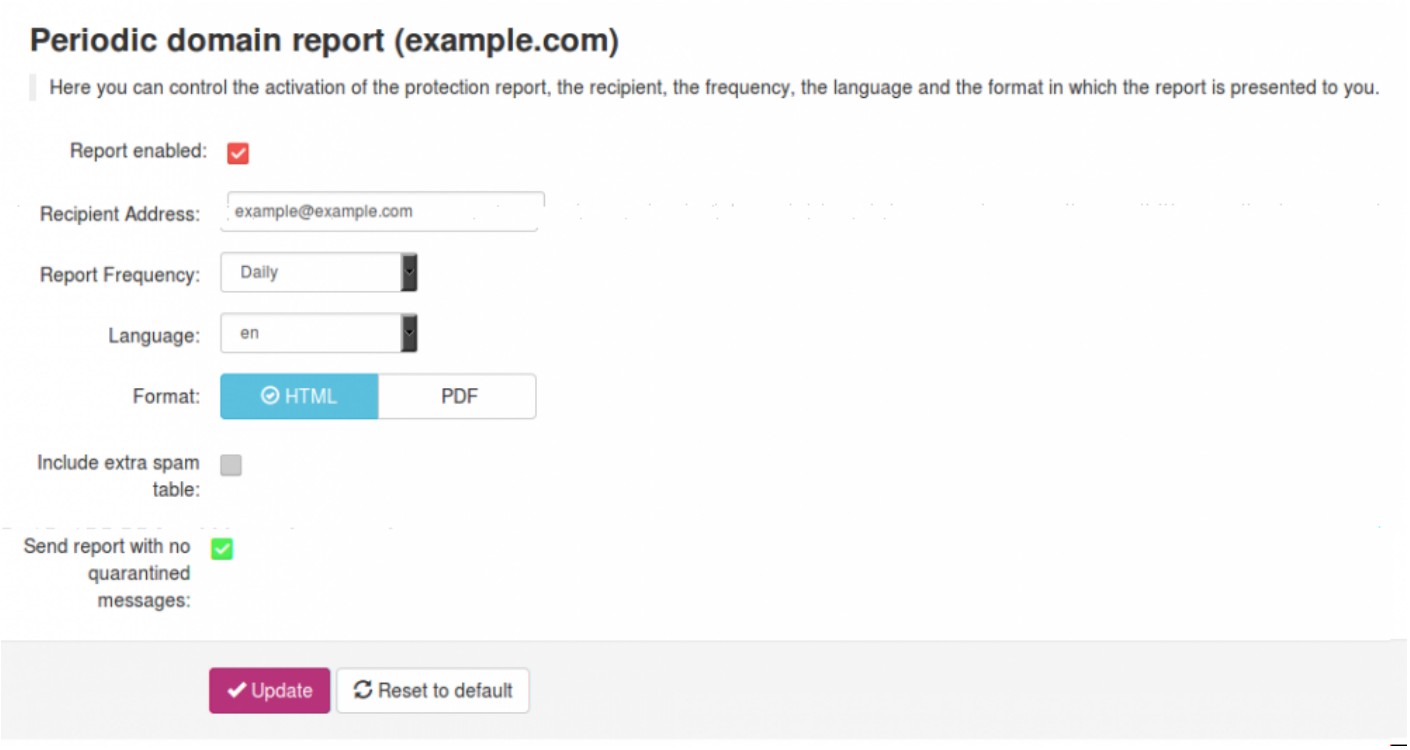
On-Demand Domain Report



Using 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 of messages that were rejected but not quarantined.

Periodic Domain Report



A daily or weekly report can be generated for your 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

As domain user, 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 a 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 users a welcome email in the beginning to let them know their personal quarantine has been activated, and if they would like to log in and 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 available for use.

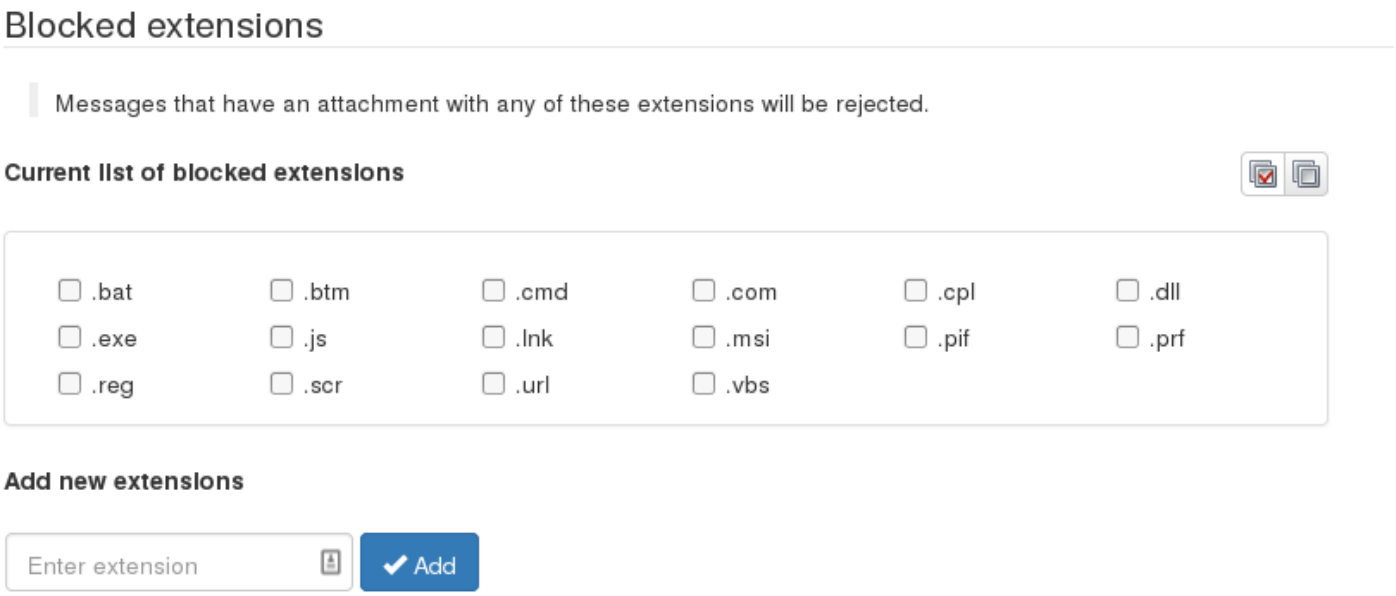
! In the **SpamExperts Control Panel – Domain Level – Domains Settings** page – **Advanced Settings** we've added the option to **skip the "catch-all"** checks for your filtered domains, which is useful when activating the '**Automatically activate for all recipients**' option in the **Periodic User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

Email Restrictions

- Attachment Restrictions
- Email Size Restrictions

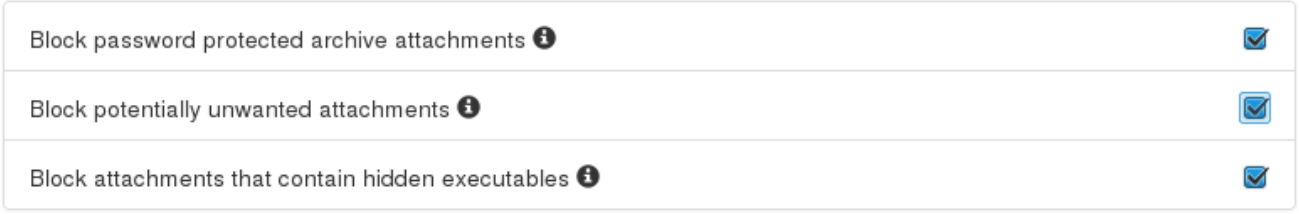
Attachment restrictions

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.



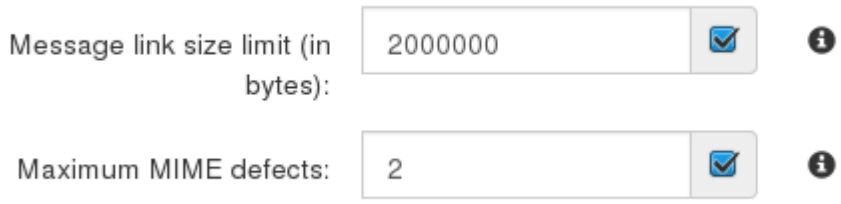
Restricted Options:

here you are able to enable/disable messages that are likely to be dangerous. for example, compressed archives that have executables within a zip file, compressed archives that are password protected , and attachments that are classified as PUA (This can be attachments that have runtime packers for example)



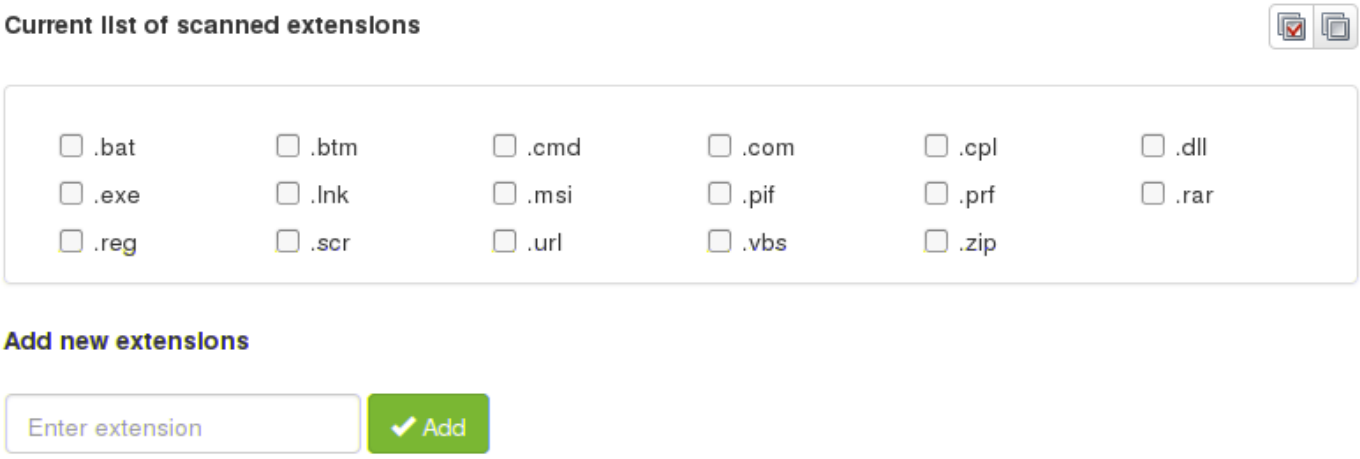
Additional restrictions:

The additional restrictions options allows to to configure how many mime parts are allowed for a message, and the “message link size limit”. The message link size limit refers to the “scanned link extensions” below. As malware will often be of a small size, we would recommend to set this to around 2MB maximum.

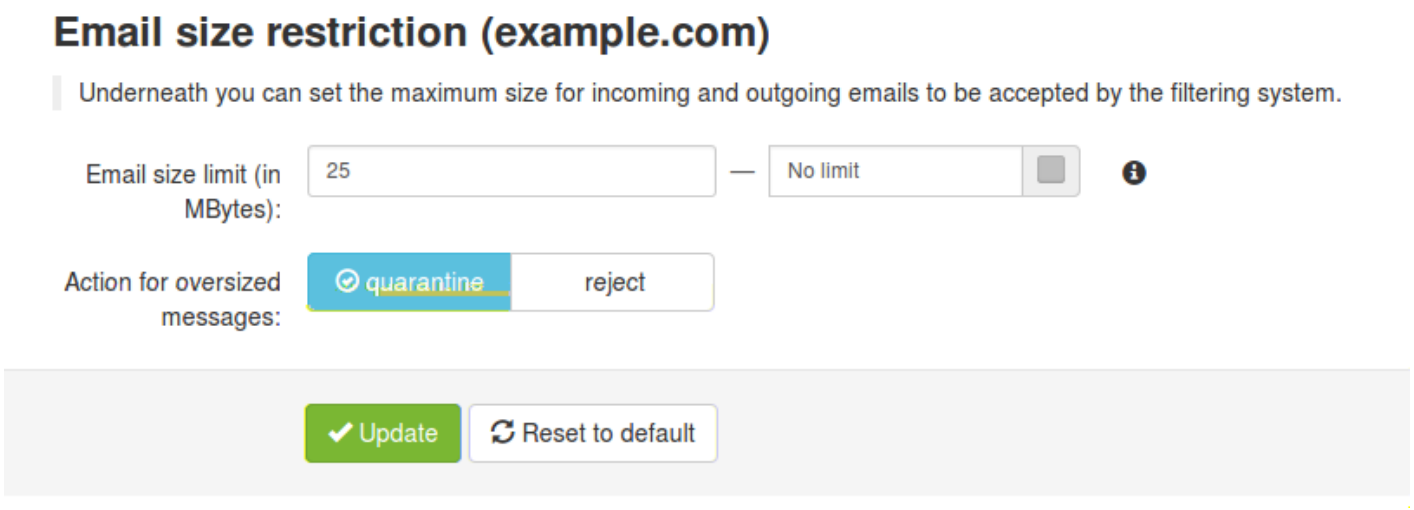


Scanned link extensions:

By default when a message is sent with a link inside the email, the content of this link is not downloaded. Here you can configure this. For example, you can add “.zip” and “.rar” to this list, and if a message is sent with “http://example.com/mybadfile.zip”, then the “mybadfile.zip” will be downloaded and scanned. We recommend to never add things like “.php”, “.html” etc to this list.

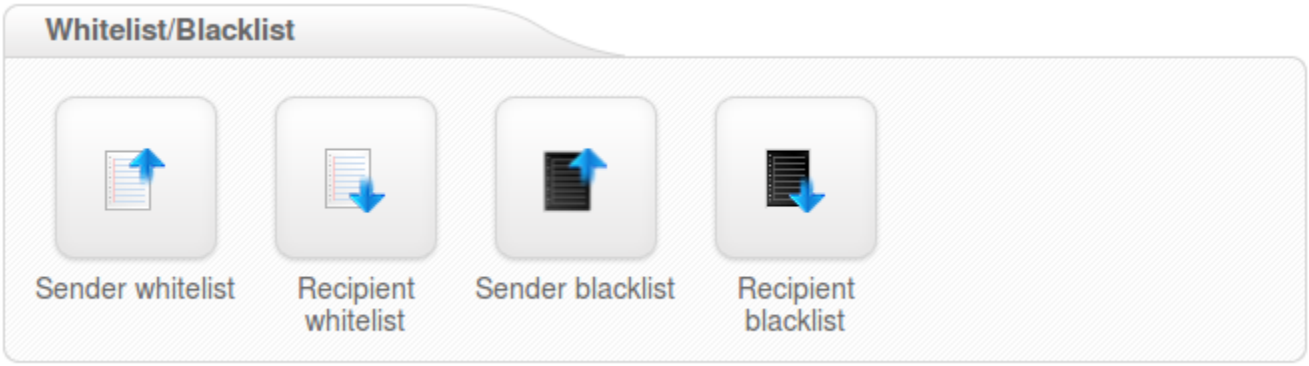


Email Size Restriction



By default the system applies no limits to the email size, and uses the size set by the destination mailserver. 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.

Blacklist / Whitelist



- Sender Whitelist
- Recipeint Whitelist
- Sender Blacklist
- Recipient Blacklist

Sender Whitelist

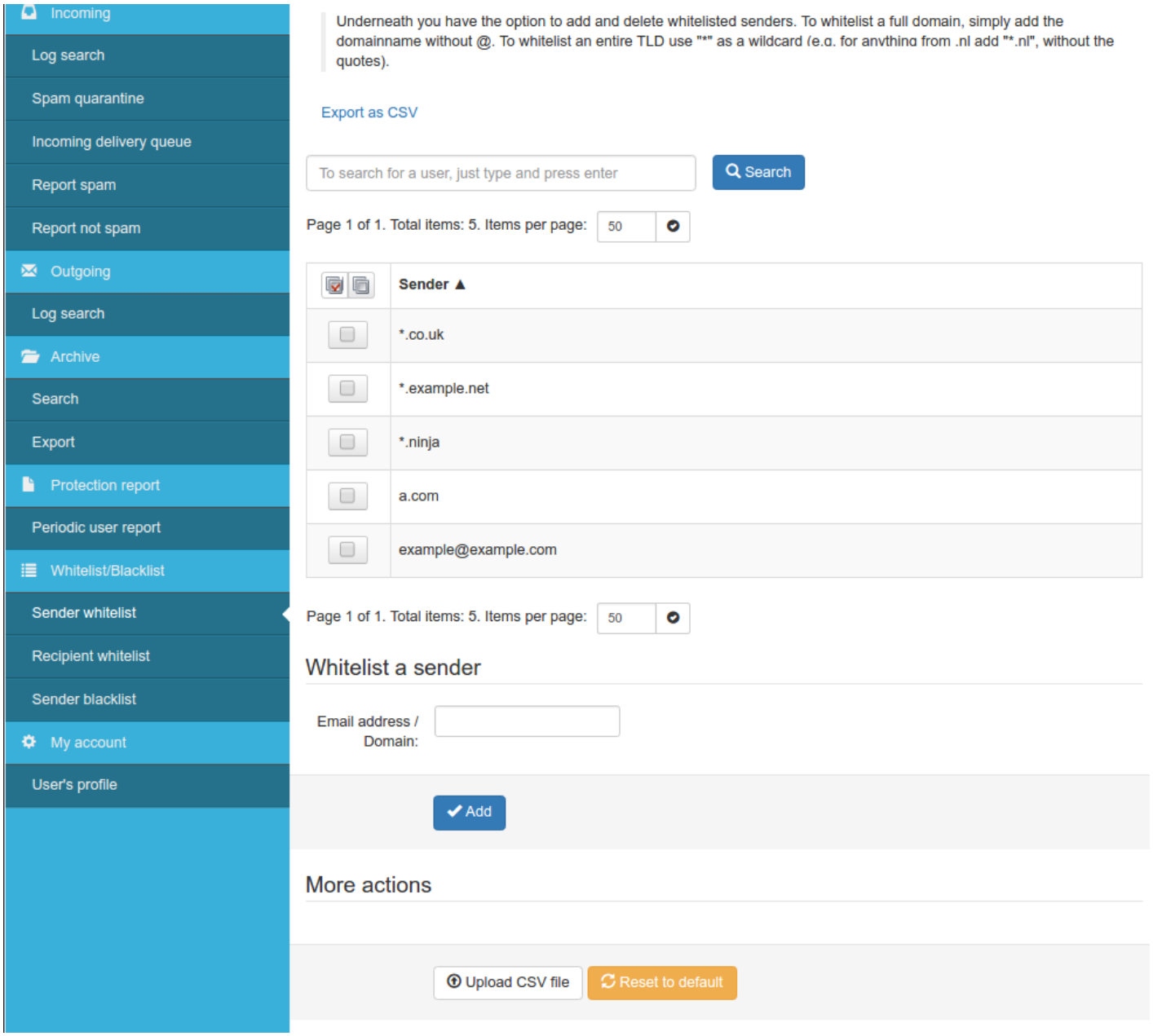
* Whitelisting the sender(s) at this section will apply to all the users on this domain when logged in as domain user.

* When logged in as email user, you can whitelist senders for your own email account.

To allow the domain administrator or email user 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 and the **From** address that is visible to recipients. The **MAIL FROM** might be different from the **From:** address, as if you check the headers of an email, the "**envelope-from**" address specifies the actual sender address.

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 @). You can also use the wildcard support to whitelist a whole TLD, such as "*.net".



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

! Be Advised: All filtering checks are disabled for whitelisted recipients. We recommend to use only the recipient whitelist for exceptional cases such as special **abuse@** or **postmaster@** recipients.

* As email user the whitelisting is limited to your own account, as you can only whitelist/unwhitelist your account.

! The following part is addressed only to domain users.

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/malware. 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.

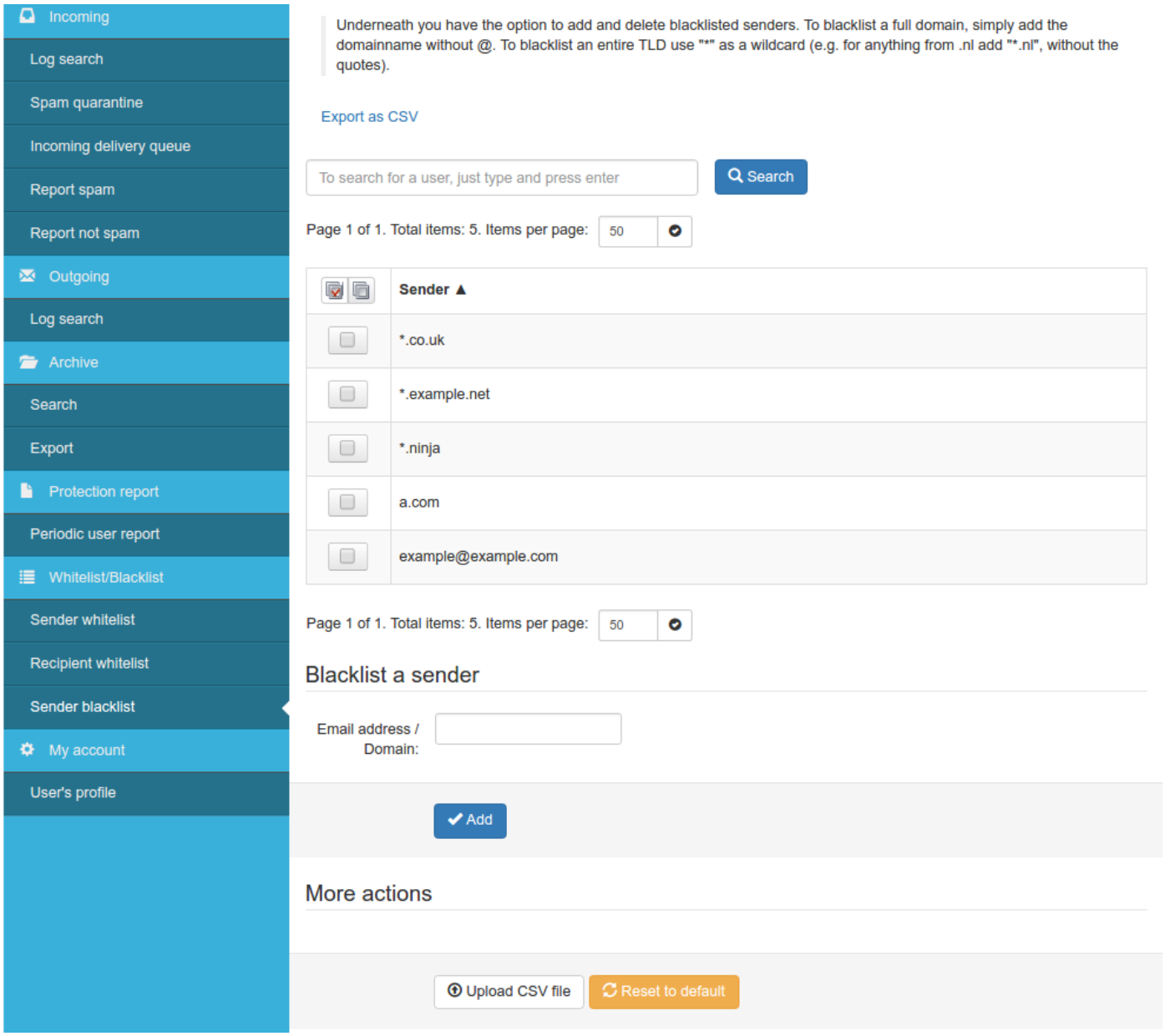
* Blacklisting the sender(s) at email user level will apply and is limited to all accounts or domains that send emails to that specific email user address.

To allow the domain administrator or email user 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 and the **From** address that is visible to recipients. The **MAIL FROM** might be different from the **From:** address, as 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.

! If you blacklist a **From:** address that is different that the **MAIL FROM** (envelope-from) the message will be quarantine, NOT rejected.

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 @). You can also use the wildcard support to blacklist a whole TLD, such as "*.net".



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

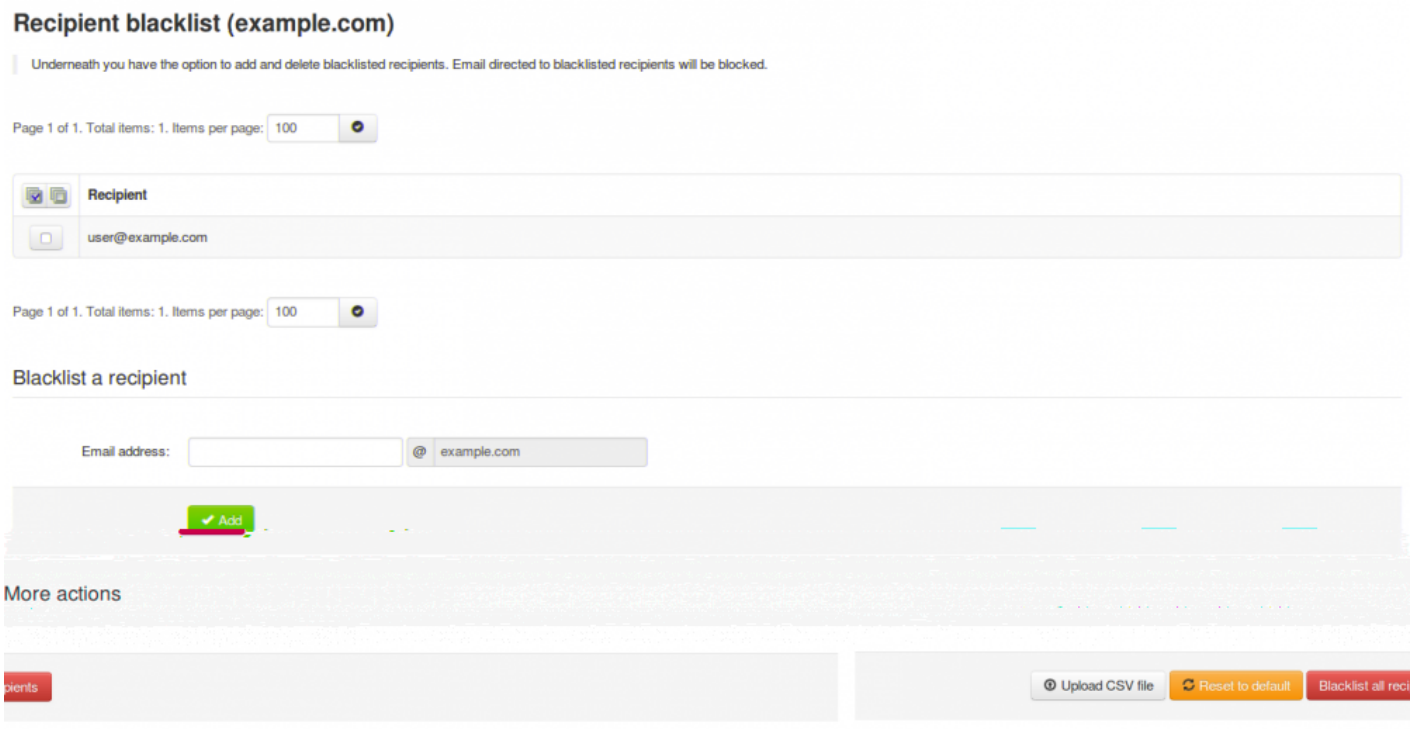
* Blacklisting the recipient(s) at this section will apply to all users on this domain.

Emails to recipients listed on the blacklist will be automatically rejected.

! Be Advised: The messages are rejected, 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.

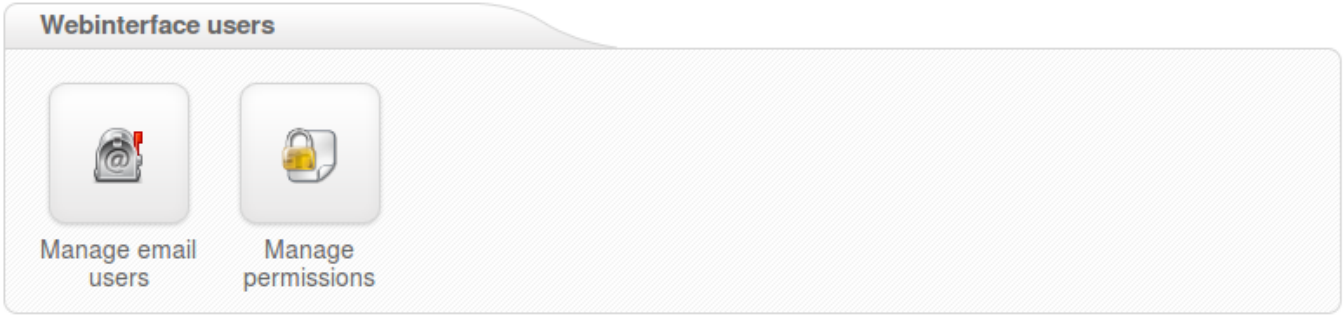
To blacklist a specific recipient address, the local part of the address should be entered. For example if your domain is example.com and you add “nofilter” to the recipient blacklist, all emails sent to nofilter@example.com will be rejected. To blacklist all recipients for a domain (so all emails sent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



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

Webinterface Users



- Manage Email Users
- Manage Permissions

Manage Email Users

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

Please ensure 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.

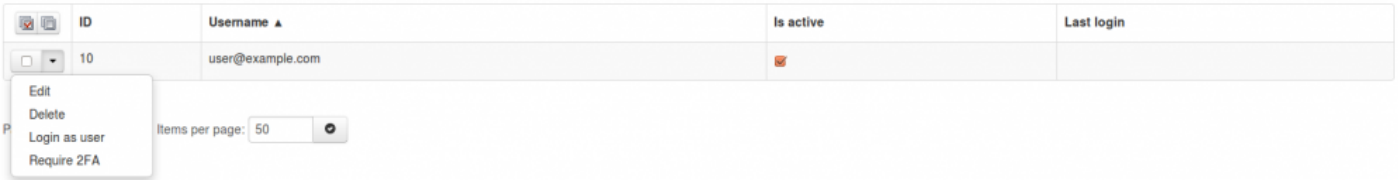
You may also upload a Comma Separated Values (CSV) file. Each line in the file must contain at least four columns, the username, the domain, the password and the status.

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 drop-down black arrow you have several options such as:

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



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.

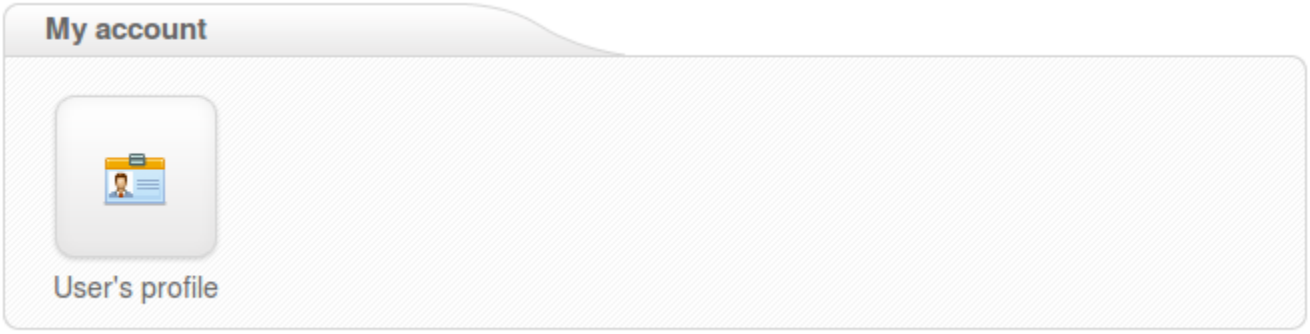
Manage Permissions

In this section you can manage specific permissions for available user roles and for individual pages for user levels.

The permissions are for the following:

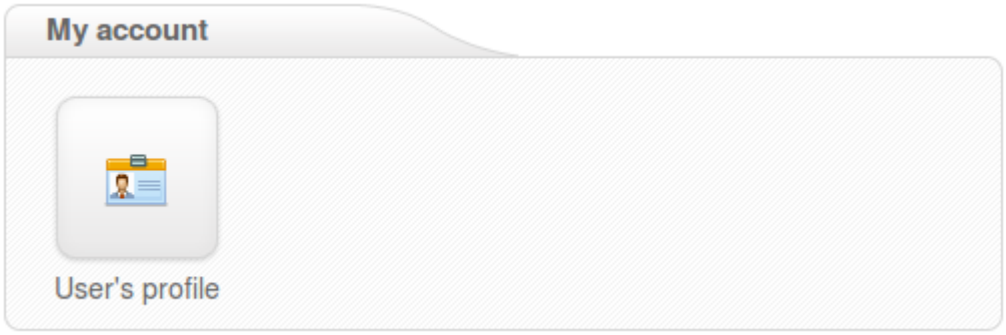
- Incoming
    - Log search
    - Include results from the last minutes
    - Spam quarantine
    - Incoming delivery queue
    - Report spam
    - Report not spam
- Outgoing
    - Log search
    - Include results from the last minutes
    - Reason of locking
- Archive
    - Search
    - Export
- Protection report
    - Periodic user report
    - Enable for recipient
        - Whitelist/Blacklist
    - Sender whitelist
    - Upload CSV Sender whitelist
    - Recipient whitelist
    - Sender blacklist
    - Upload CSV Sender blacklist
- My account
    - User’s profile

My account



- User Profile

User Profile



In this section 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 as well.

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)

User's profile

Here you can manage your account settings.
We recommend you to use a password manager that automatically creates and remembers your password.

Username: admin

Old password:

New password:

Confirm new password:

Email:

Save

Two Step Authentication

You can enable Two Step Authentication to further 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.

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

Compose email

The following page allows you to compose an email directly from the interface. This isn't intended to be a full email client, but you are able to set and change the To, CC, and BCC addresses, use rich formatting, and insert links into messages.