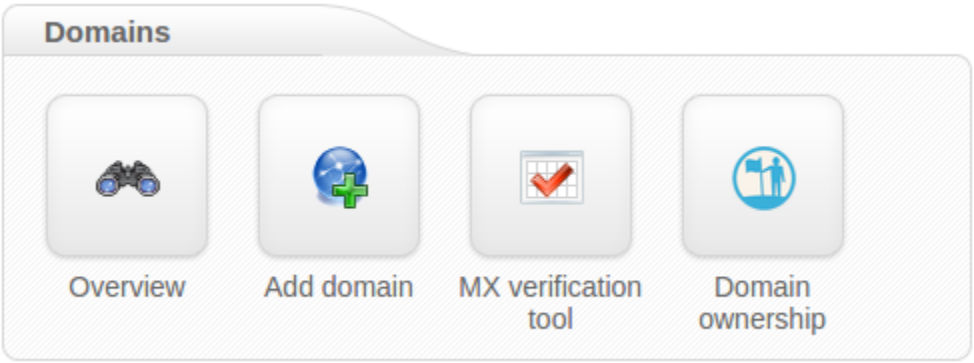
SpamExperts Control Panel Super Administrator Level

2 — Last update: 2016/07/12

SpamExperts

Table of Contents

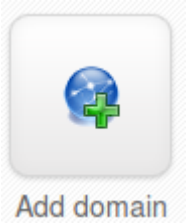
Domains



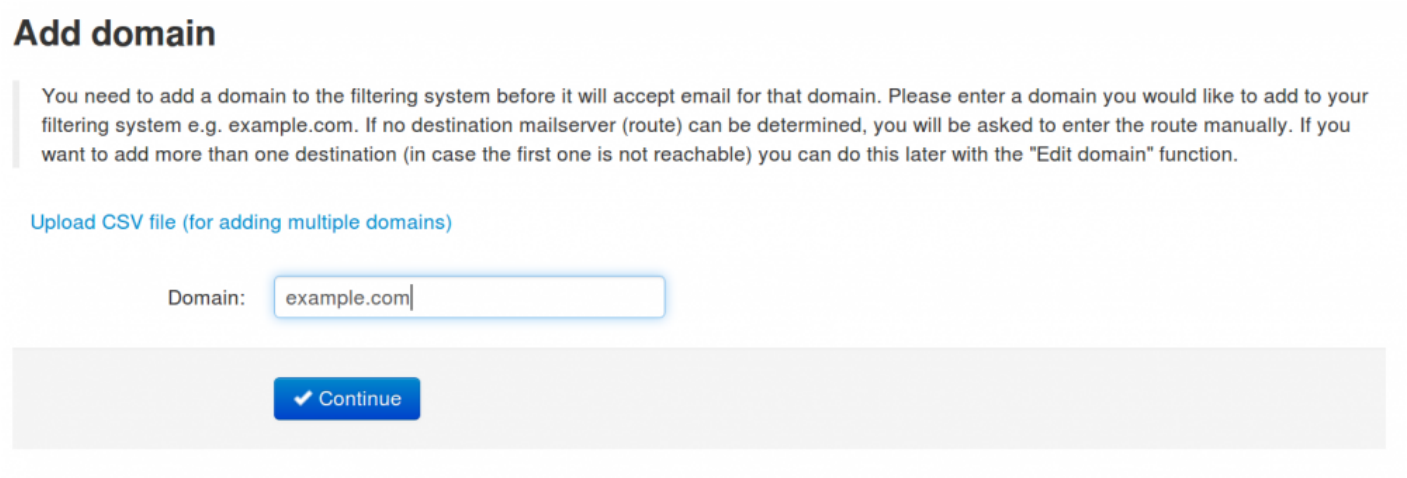
- Overview
- Add Domain
- MX verification Tool
- Domain Ownership

Add Domain

To add a domain, click on the '**Add Domain**' button in the welcome user dashboard. You can optionally upload a Comma Separated Values (CSV) file to add multiple domains at once.



Then type the domain you would like to add to your filtering system, for example: "example.com" and click **Continue**.



If no destination mail server (route) could be determined for the final mail delivery, you are automatically asked to enter the route manually. If you want to add more than 1 route, in case the first one is not reachable, you can do this later by going to **Domain Dashboard** > **Incoming** > **Edit Routes**.

> * Be Advised : Always add the domain to the interface before changing the MX records to the new cluster MX records, because in this way the correct route for the destination mail server will be added automatically and no mail will be rejected.

The domain will appear in the Overview page, after being successfully added.

In the same row with the domain, you will find 3 small icons, as shown below, which will display the status of your services:

- Incoming Filtering
- Outgoing Filtering
- Email Archiving

MX verification Tool

The MX verification tool is used to check if domains present on the server have the correct MX records.

Click on the **Dashboard** → **MX verification tool** under the **Domains** menu section. Enter your valid MX hostname(s) and click **start verification**.

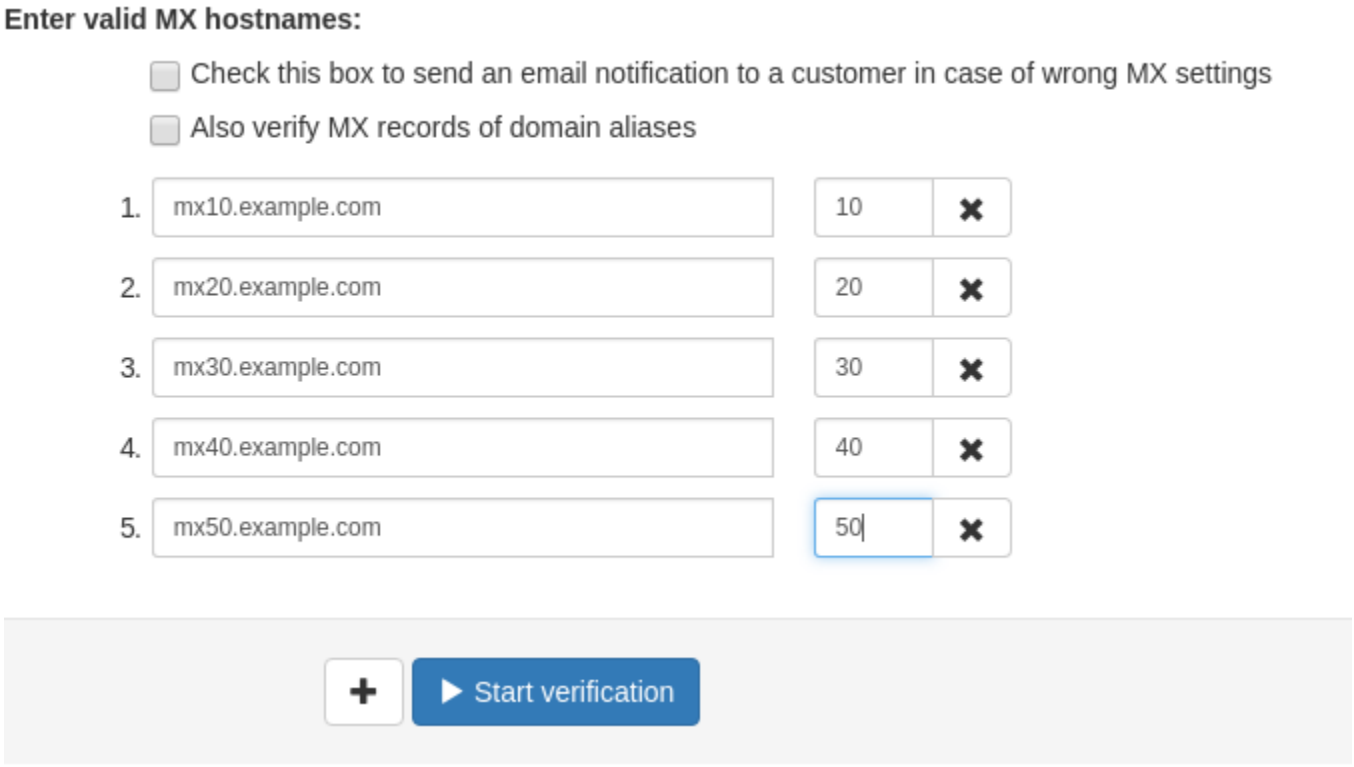
The output will list all the domains present on the system with different MX records.

There are 2 checkbox options available:

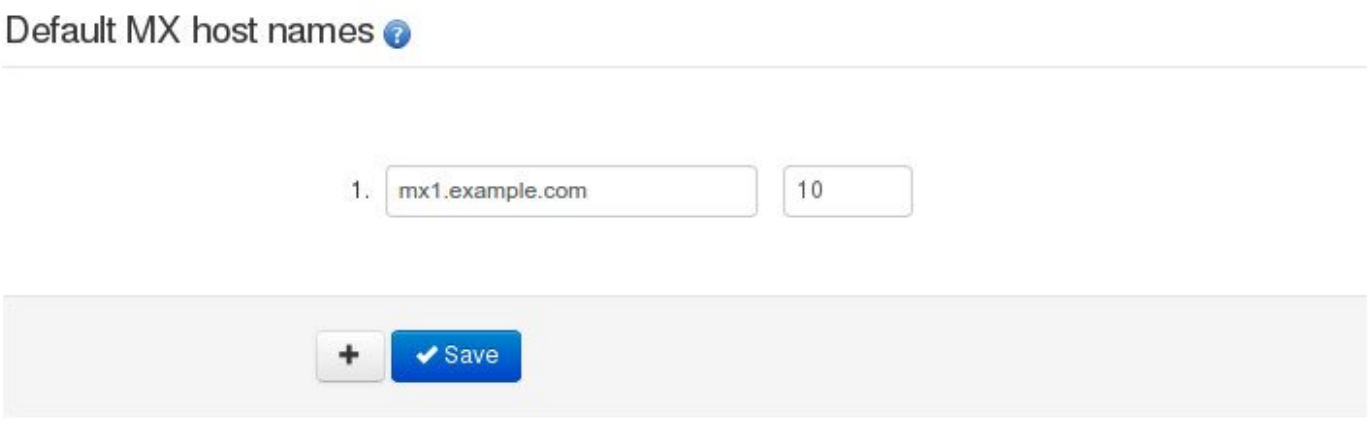
- Check this box to send an email notification to a customer in case of wrong MX settings
- Also verify MX records of domain aliases

> * As a Super-Admin you also have a third checkbox option available, as the Skip Assigned Domain feature is present.

The above are by default unchecked.

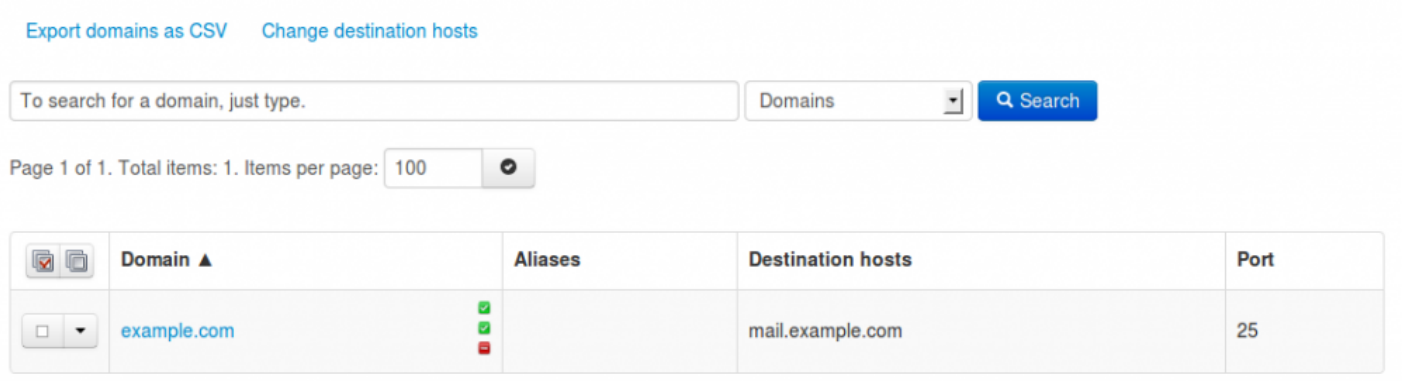


The default MX records can also be set via the "**Default MX host names**" section, from **Server** menu → **Settings**.



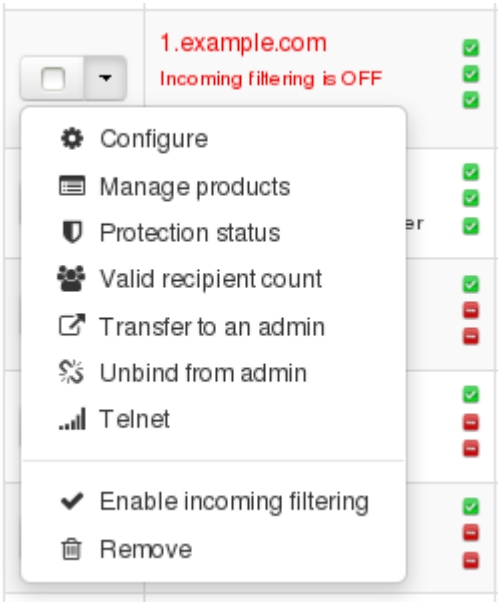
Overview

Domain Overview contains a list of domains, domain aliases, destination routes, and ports for which your email filtering system accepts email. Also active services present on each domain are displayed as small green boxes by each domain name.



You can perform the following functions by clicking on the respective drop down menu, beside each domain:

- Configure (Domain)
- Manage products
- (Check) Protection Status
- (Check) Valid recipient count
- Transfer (the domain) to an admin (on the Cluster)
- Telnet
- Remove (domain)


1.example.com
Incoming filtering is OFF
Configure
Manage products
Protection status
Valid recipient count
Transfer to an admin
Unbind from admin
Telnet
Enable incoming filtering
Remove

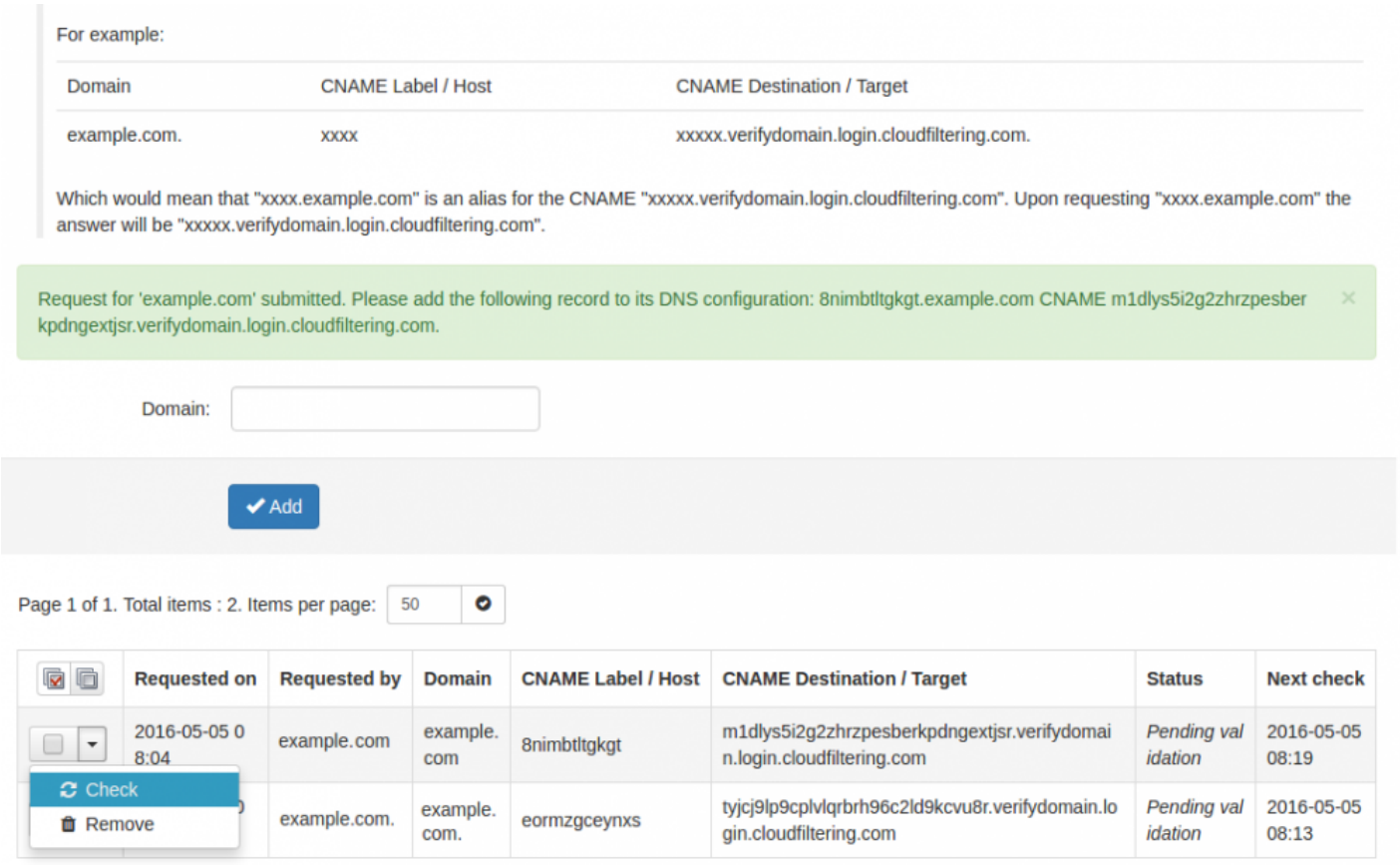
Domain Ownership

Here you can add your domain(s) and we'll verify your ownership. Simply follow the instructions, for example, add a domain "example.com". Then you need to add the CNAME you are provided with.

You will be given for example the following CNAME record: **"dwtzty8kedtw. CNAME 6p6ngfykfnreylqxcslsbut3voabhqqp.verifydomain.login.FILTERINGHOSTNAME.com"**.

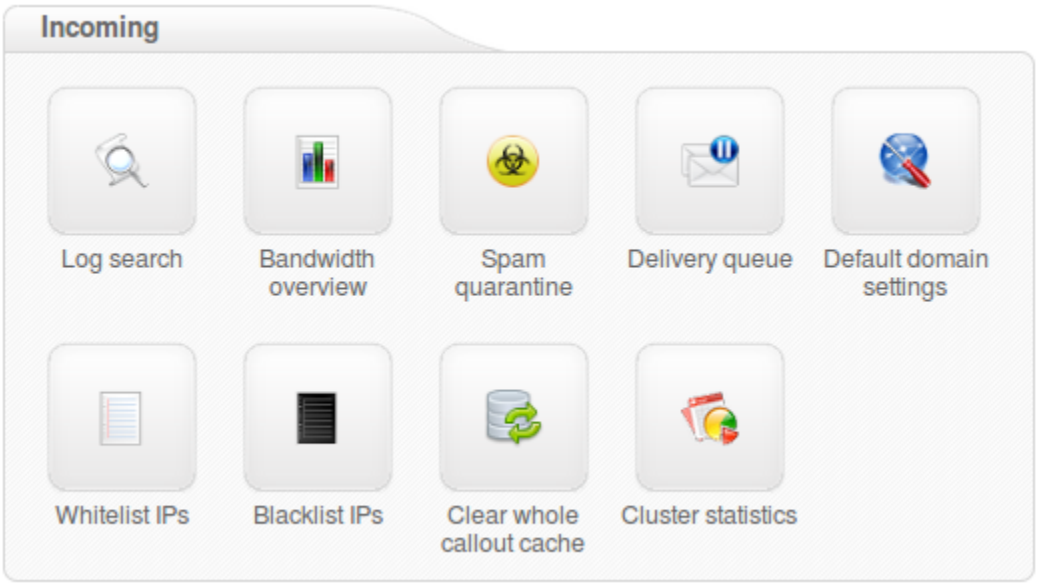
Checks will be performed periodically to validate the domain, until we find your CNAME record in the DNS settings.

Here you can also check if the domain has been validated or remove the domain validation process, by clicking the left-hand side button as shown in the below screenshot and choosing your appropriate action (Check or Remove).



* You should leave the CNAME in place for re-verification. Don’t remove it.

Incoming Filtering



- Incoming Log Search
- Incoming Bandwidth Overview
- Incoming Spam Quarantine
- Incoming Delivery Queue
- Incoming Default Domain settings
    - Incoming Advanced Settings
    - Default Filter settings
        - Manage list of IP addresses with disabled SPF check
- Manage list of IP addresses with disabled SPF check
    - IP whitelist
    - Default Sender Whitelist
    - Default Recipient Whitelist
- Blacklist
    - IP Blacklist
    - Default Sender Blacklist
    - Default Recipient Blacklist
- Clear Whole Callout-Cache
- Incoming Global Statistics

Incoming Log Search

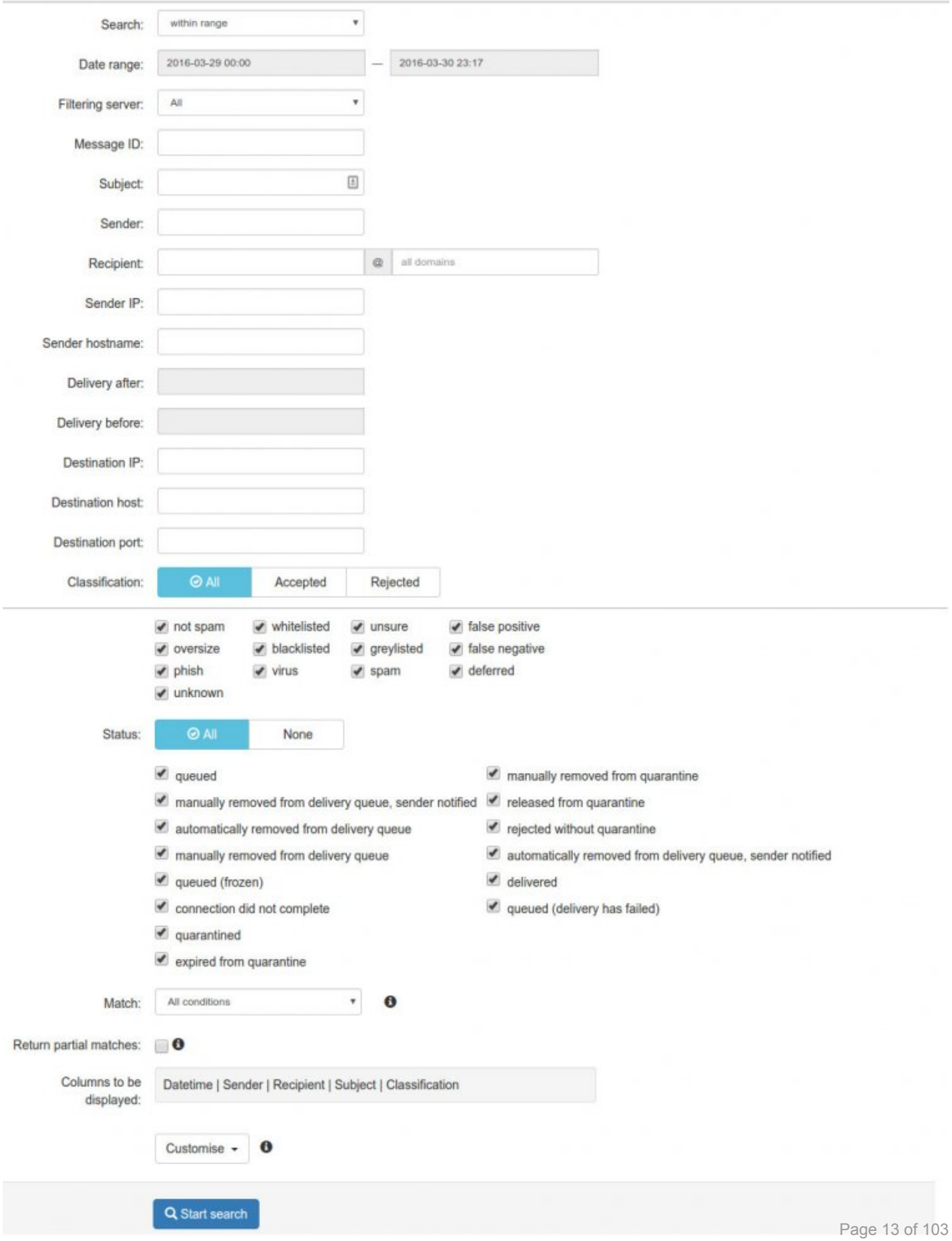
On this page you can view the log of messages that are received, blocked and temporarily rejected.

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 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:
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.

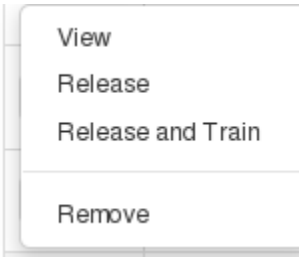
Delay

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.

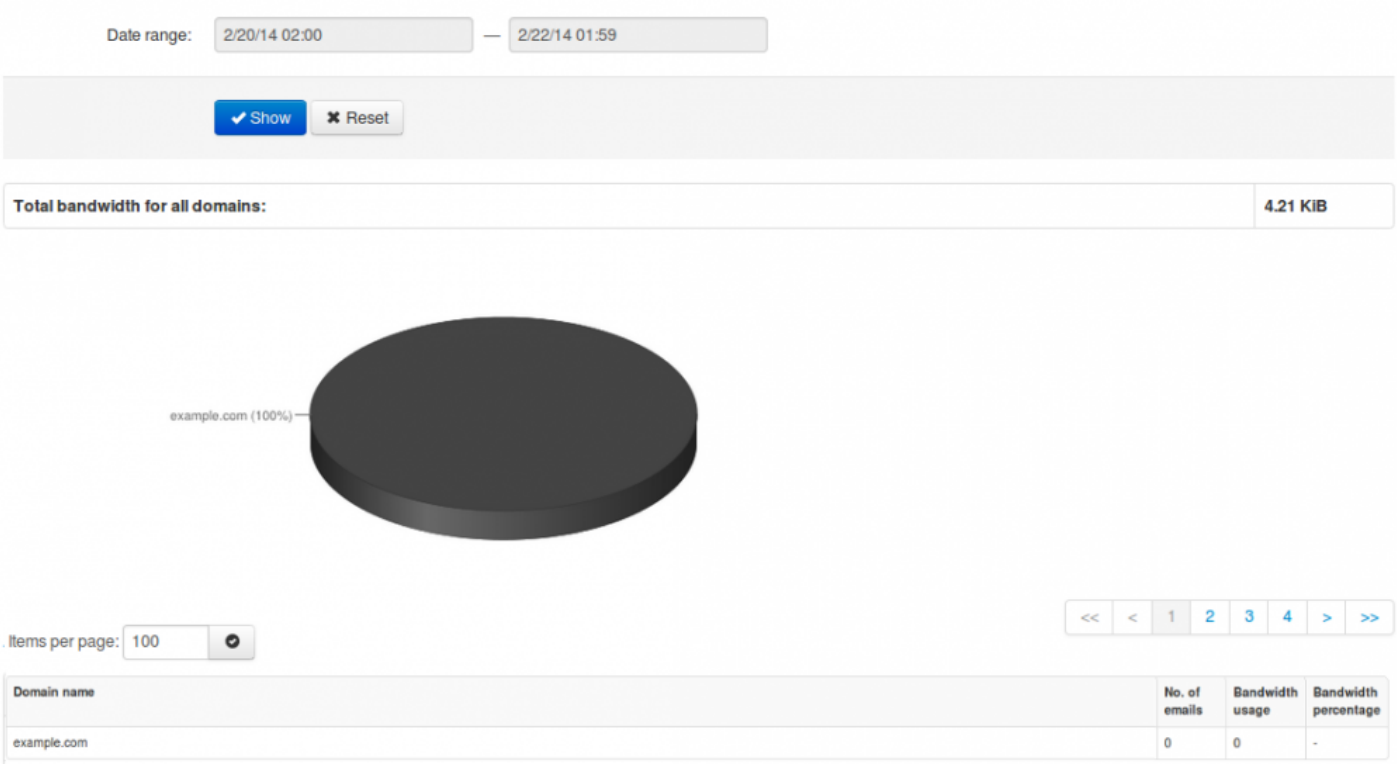


Messages that return ‘Accepted’ have not necessarily been delivered, it means the message has been accepted for delivery. If immediate delivery fails, the message will be automatically retried. If the destination server rejects the email, a bounce will be generated to the sender.

> ! 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 Bandwidth Overview

The Bandwidth Overview feature will display the bandwidth usage per domain for a given time-frame.



Incoming Spam Quarantine

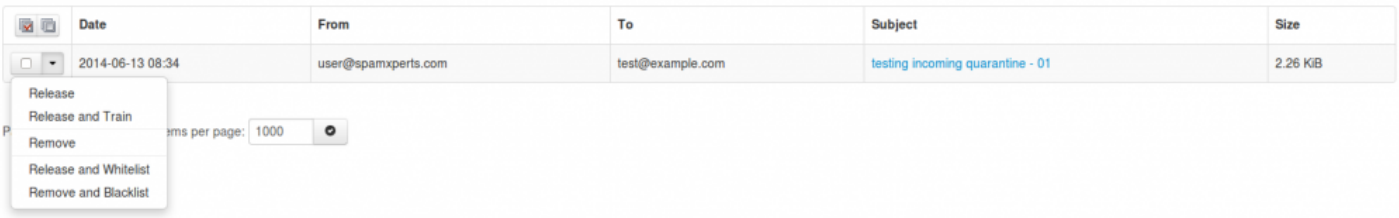
The Spam quarantine interface displays all the incoming quarantined messages.

> * 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.

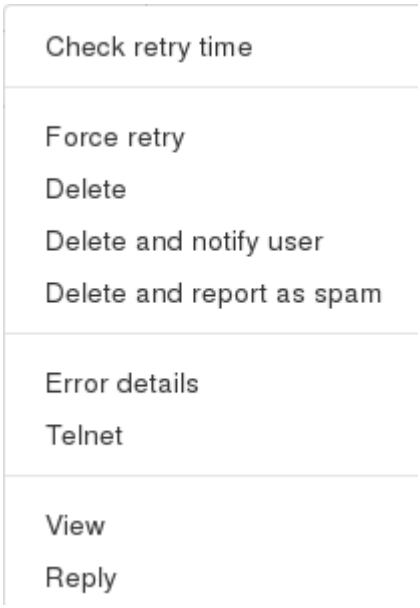
If an attachment is included in the quarantined message, then this can be individually downloaded by clicking on the **'Attachment:'** line in the normal view.

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.

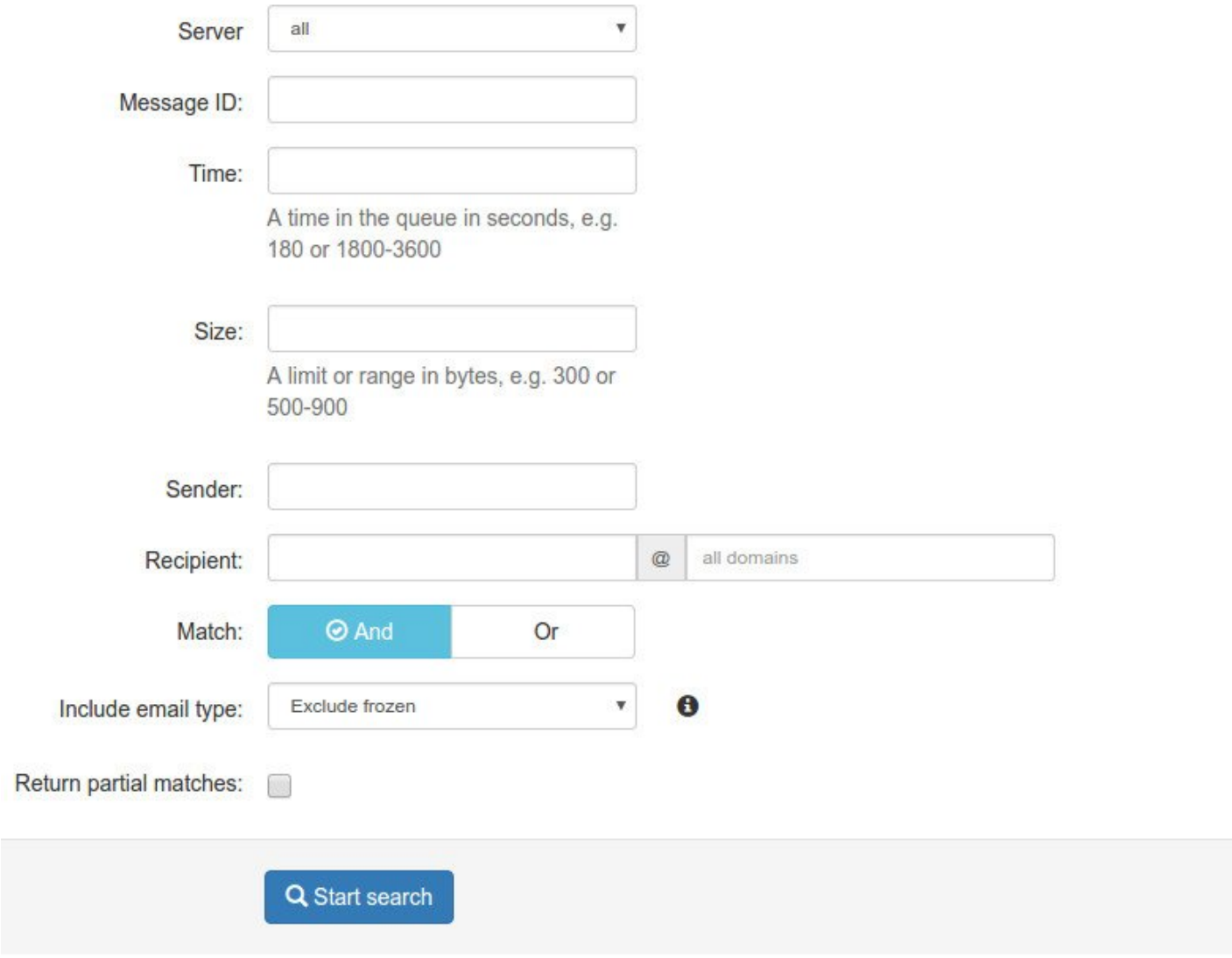
We have also reintroduced the option ‘Error details’ to check the reason why messages are stored in Delivery Queue.

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.

Incoming Default Domain settings

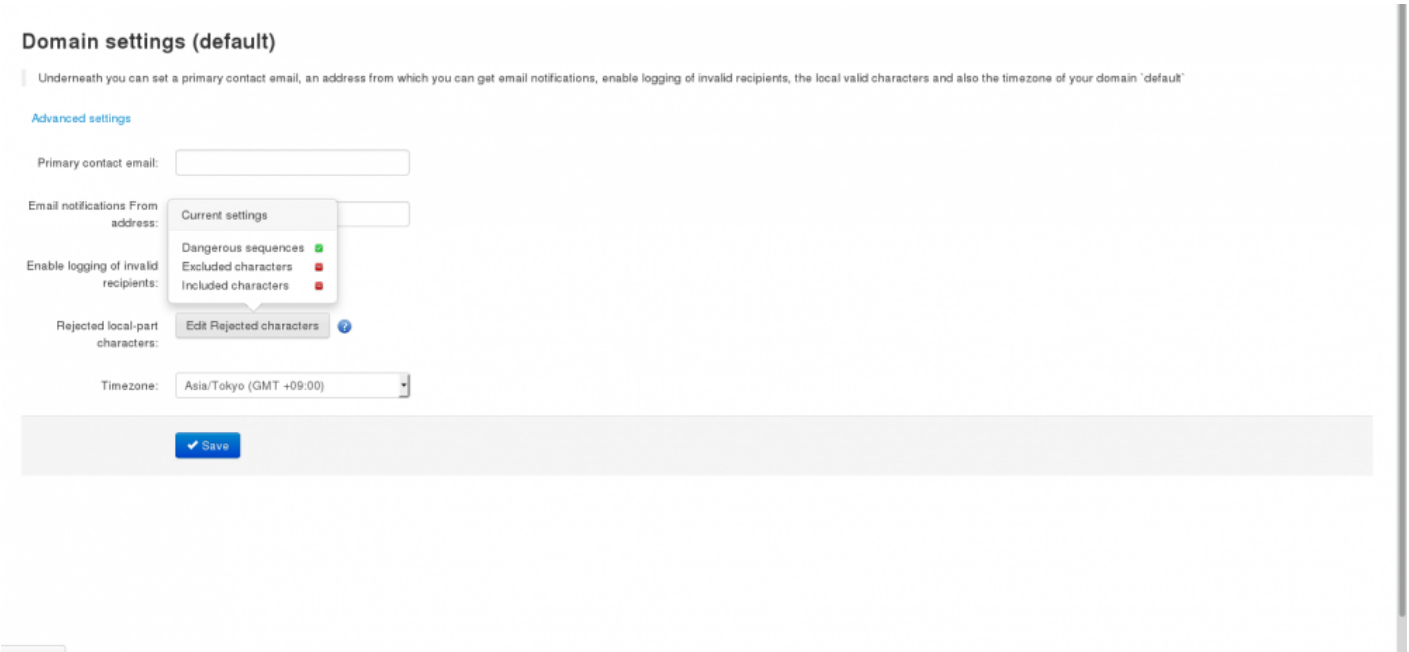
With the default domain settings in the control panel users can control certain domain settings. The default settings apply to all domains that have not yet explicitly set a custom value for the setting yet, and are therefore using the default settings.

In this section users can set the maximum bounces, enable/disable logging for invalid recipients, and set accessible/inaccessible logging days for your domains which are using the default settings.

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. Thus removing a character here will allow that character in the local part.

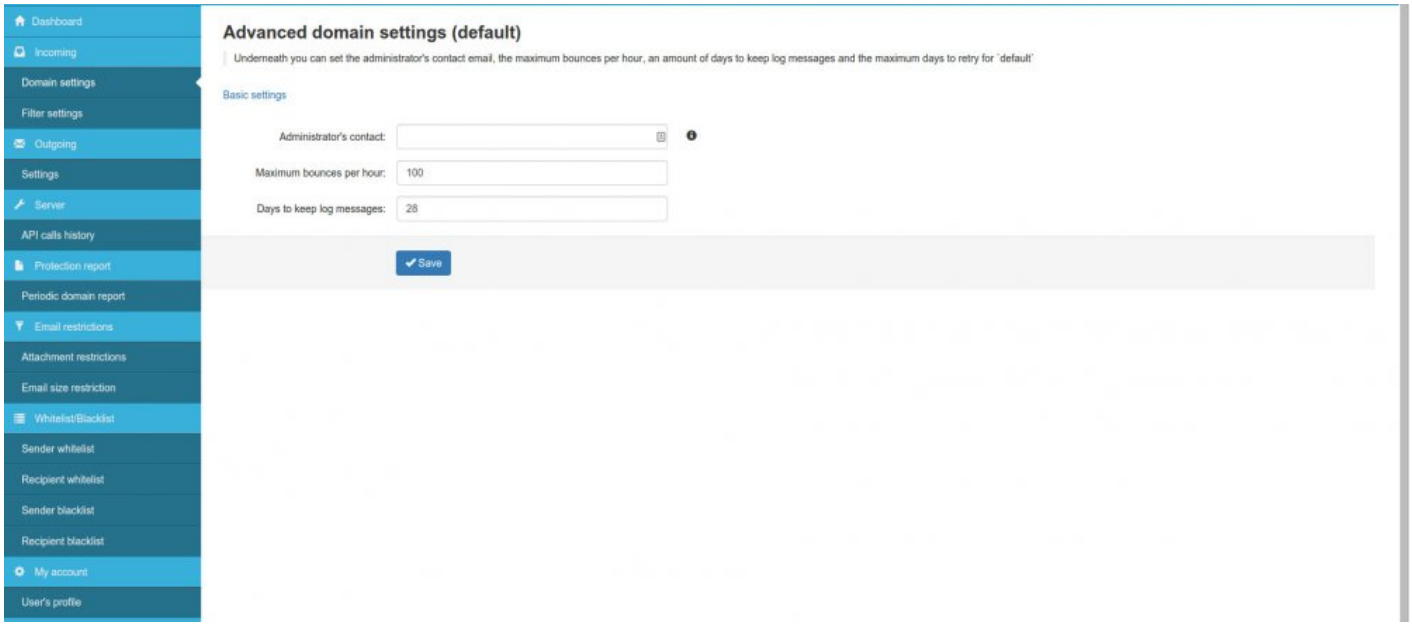
You can “Edit Rejected Characters” by setting up a list of regular expressions. If a local part of the recipient matches any of the regular expressions, then the recipient will be rejected.

While hovering mouse over, you will see your current settings:



Incoming Advanced Settings

By clicking Advanced Settings, users have the ability to set the Administrator contact email address, maximum bounces per hour or how many days log messages are stored.



Filter settings (default)

Here you can set the Default filter settings that are applied to all domains who use the default value and domains that are added after this.

The Default Filter settings are accessible via the following path: **Default Domain Settings → Incoming → Filter Settings**

! Be Advised: The options below will globally apply to all domains that have not yet explicitly set a custom value for the setting yet, and are therefore using the default settings.

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

* Advisory: We do NOT recommend changing the default settings, as they 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 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. This applies globally to all the domains using the default settings.

Skip SPF Check

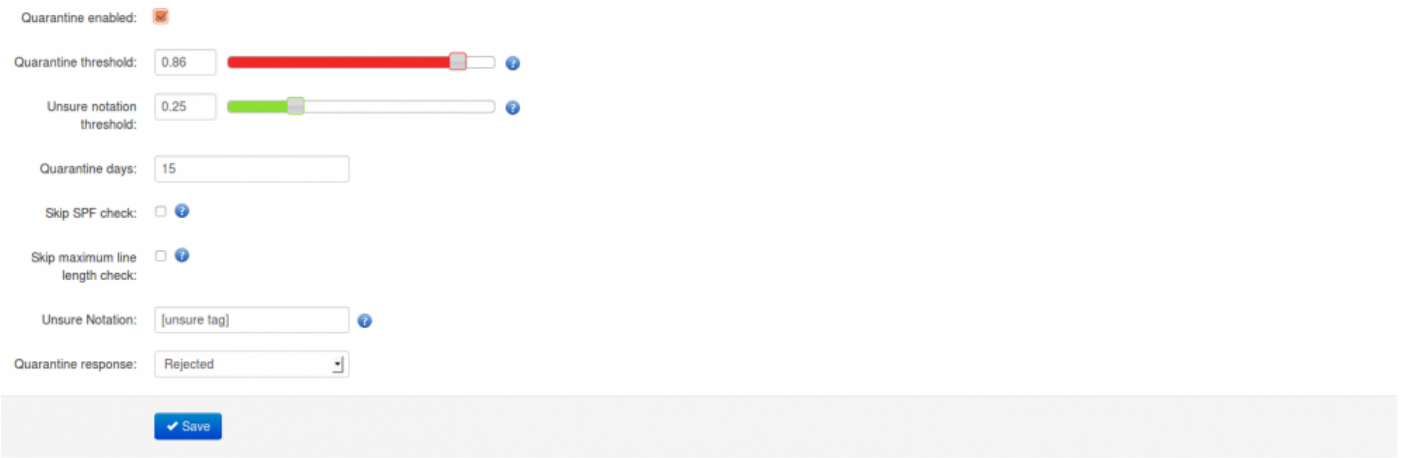
This means that emails for all the domains using the default settings will not be subject to SPF (Sender Policy Framework) checks.

Skip Maximum Line Length

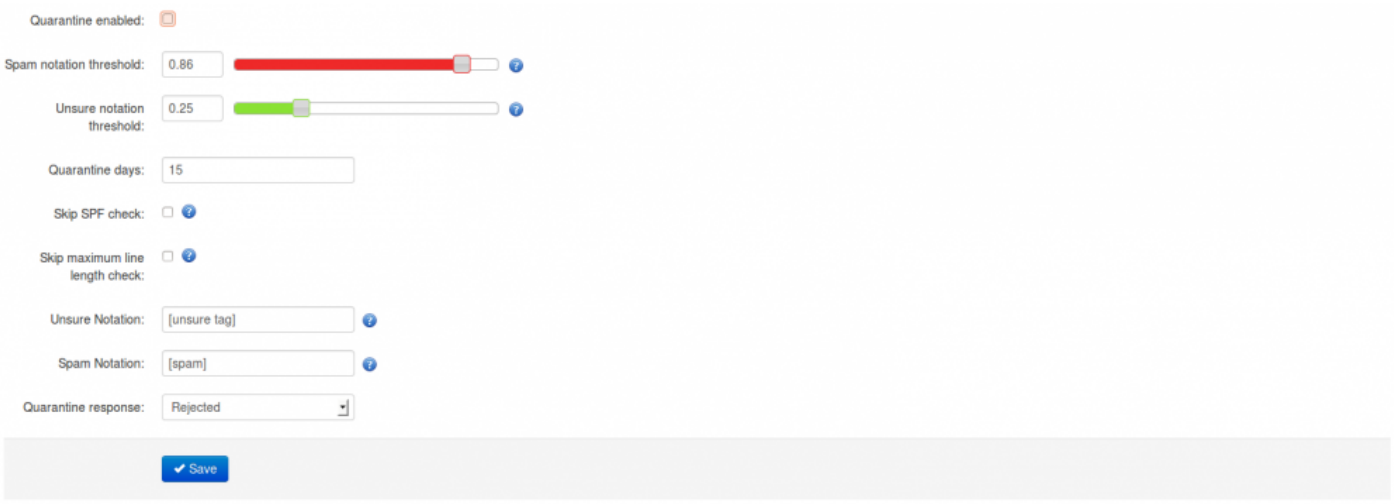
This means that emails for all the domains using the default settings will not be subject the RFC line length checks.

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 shown in the Spam Quarantine. Since that technically breaks with the SMTP RFC specification, it's not recommended (however some clients prefer to overrule it).



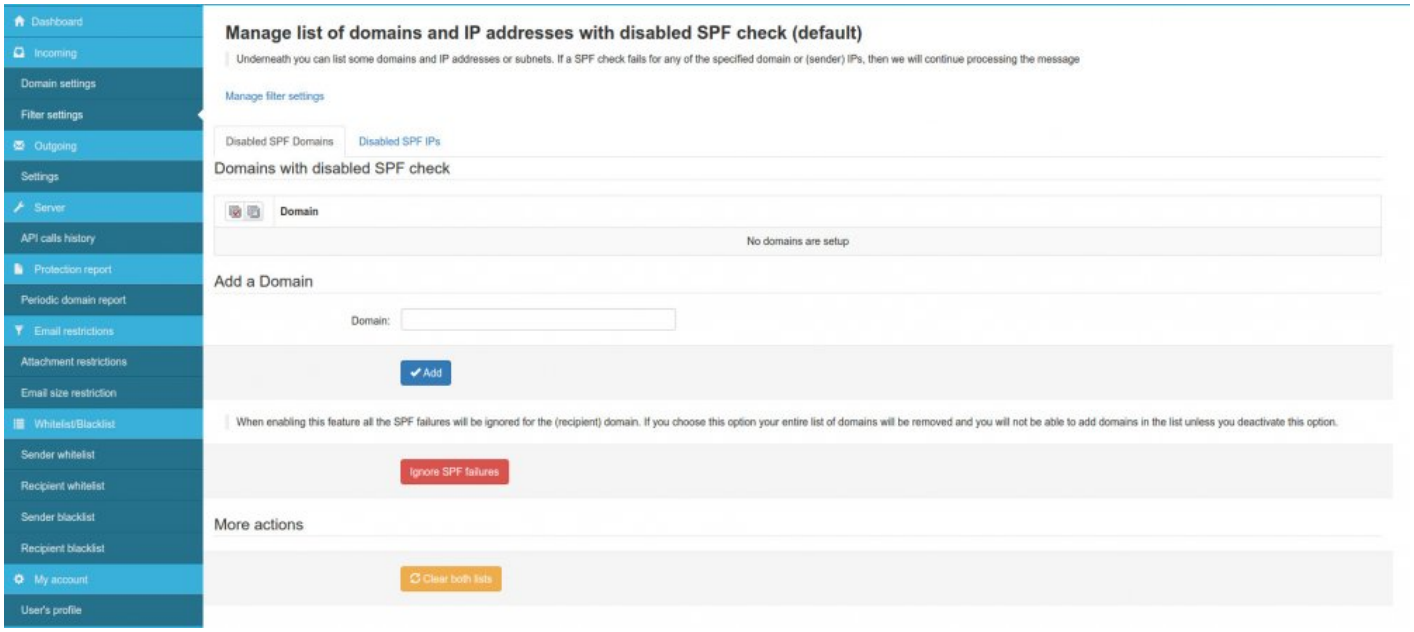
If you disable the quarantine system, emails detected as spam will not be kept in the quarantine system but will be delivered to your destination email server. Under "Spam Notation" you can mark these messages with a specific subject notation. Note that we do NOT return a 5xx reject message for messages 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.


Quarantine enabled:
Spam notation threshold:
0.86
Unsure notation threshold:
0.25
Quarantine days:
15
Skip SPF check:
Skip maximum line length check:
Unsure Notation:
[unsure tag]
Spam Notation:
[spam]
Quarantine response:
Rejected
Save

Manage list of IP addresses with disabled SPF check

Here you can set the list of domains or IP addresses to skip the SPF (Sender Policy Framework) check.

This is particularly useful when dealing with forwarding servers.



Other checks still apply when adding IP addresses here.

Whitelist

As a Super-Admin you can access 3 types of whitelists:

- IP Whitelist
- Default Sender Whitelist
- Default Recipient Whitelist

IP whitelist

The Incoming IP whitelist can be used to SKIP certain filtering methods. Hence if you skip a filtering method which is actually reducing the spam score, such as content check, chances of messages being blocked may increase by skipping certain filters. Therefore we recommend only to skip checks for very specific situations to overrule the overall system, and to avoid messages being falsely blocked.

The following filtering checks are able to be skipped:

- Skip temporary rejection by DNSBL
- Skip rate limit
- Skip greylisting
- Skip content checks
- Skip DNS checks
- Skip DNSBL checks
- Skip EHLO checks

Sender Whitelist (default)

Default Domain Settings → Whitelist/Blacklist *→ *Sender Whitelist

> * Whitelisting the sender(s) at this section will apply globally to all domains that have not yet explicitly set a custom value for the setting, and are therefore using the default settings.

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. This may be different than the **"From:"** header in the email. 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 using only 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 in general wrongly blocking a sender, you can always contact our customer support so we can research what problem is causing the rejection and resolve it.

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 **"*@"**.

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 (default)

Default Domain Settings → Whitelist/Blacklist *→ *Recipient Whitelist

> * Whitelisting the recipient(s) at this section will apply globally to all domains that have not yet explicitly set a custom value for the setting, and are therefore using the default settings.

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, malware or viruses. To whitelist all recipients for a domain, so that all emails sent to the domain are not scanned/blocked, you can enter a wildcard “*” for the local part.

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

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

Blacklist

As a Super-Admin you can access 3 types of blacklists:

- IP Blacklist
- Default Sender Blacklist
- Default Recipient Blacklist

IP Blacklist

Traffic from IP addresses listed on the IP blacklist will get immediately rejected. The messages are NOT quarantined. All messages from blacklisted IP addresses are rejected with a 5xx SMTP error code, so legitimate sending SMTP servers will generate a bounce message to the sender. You have the option to add, edit and delete IP addresses, as well as adding a reason for why you blacklisted the respective IP address/range.

Sender Blacklist (default)

Default Domain Settings → Whitelist/Blacklist *→ *Sender Blacklist

> * Blacklisting the sender(s) at this section will apply globally to all domains that have not yet explicitly set a custom value for the setting, and are therefore using the default settings.

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 than 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 "@".

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 (default)

- Default Domain Settings* → **Whitelist/Blacklist *→ *Recipient Blacklist.**

> * Blacklisting the recipient(s) at this section will apply globally to all domains that have not yet explicitly set a custom value for the setting yet, and are therefore using the default settings.

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 a 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

Clear Whole Callout-Cache

On this page you can clear the callout cache for all domains. By default we cache server responses to 2 hours. For example, if you change a route of a domain you will need to clear the calllout cache for that domain if you do not want to wait for the 2 hour cache to expire.

* We recommended to clear the callout cache only at domain level of the domain that is having issues instead of clearing the callout cache globally.

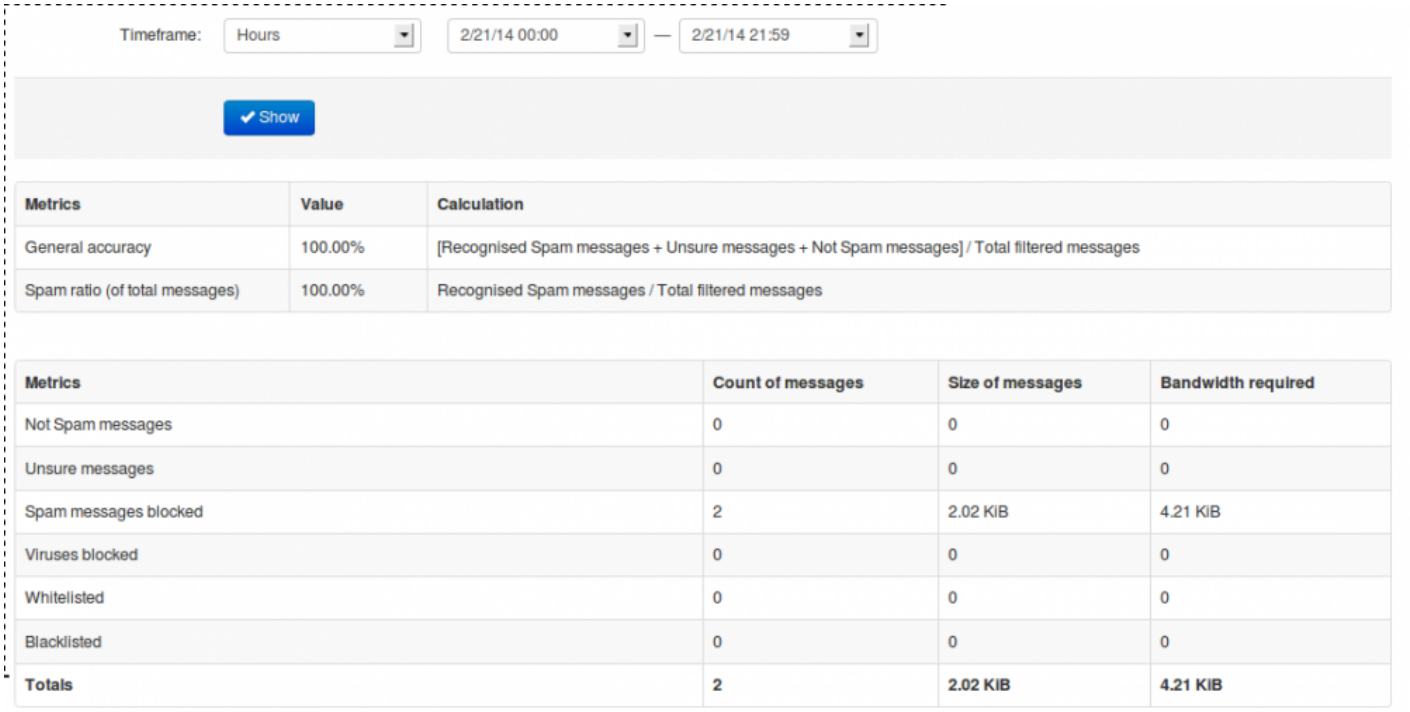
Clear

Incoming Global Statistics

With the Incoming Global Statistics users can view the incoming statistics for a given time-frame (Hours,Days,Weeks,Months,Years).

Statistics are displayed for :

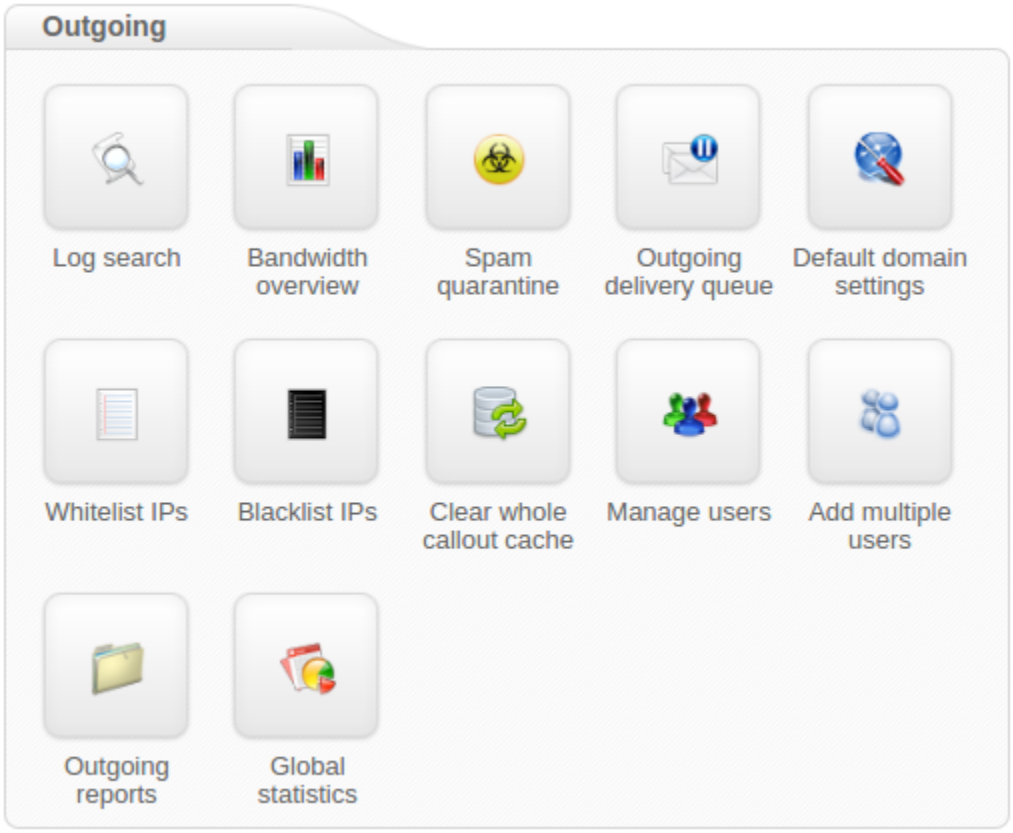
- General accuracy
- Spam ratio (of total messages)
- Not Spam messages
- Unsure messages
- Spam messages blocked
- Viruses blocked
- Whitelisted
- Blacklisted



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**

Outgoing Filtering



- Outgoing Log Search
- Outgoing Bandwidth Overview
- Outgoing Spam Quarantine
- Outgoing Delivery Queue
- Outgoing Default Domain Settings
- Outgoing IP whitelist
- Outgoing IP Blacklist
- Global Outgoing Callout Cache
- Manage Outgoing Users
- Add Multiple Users
- Outgoing Reports
- Outgoing Global Statistics

Outgoing Log Search

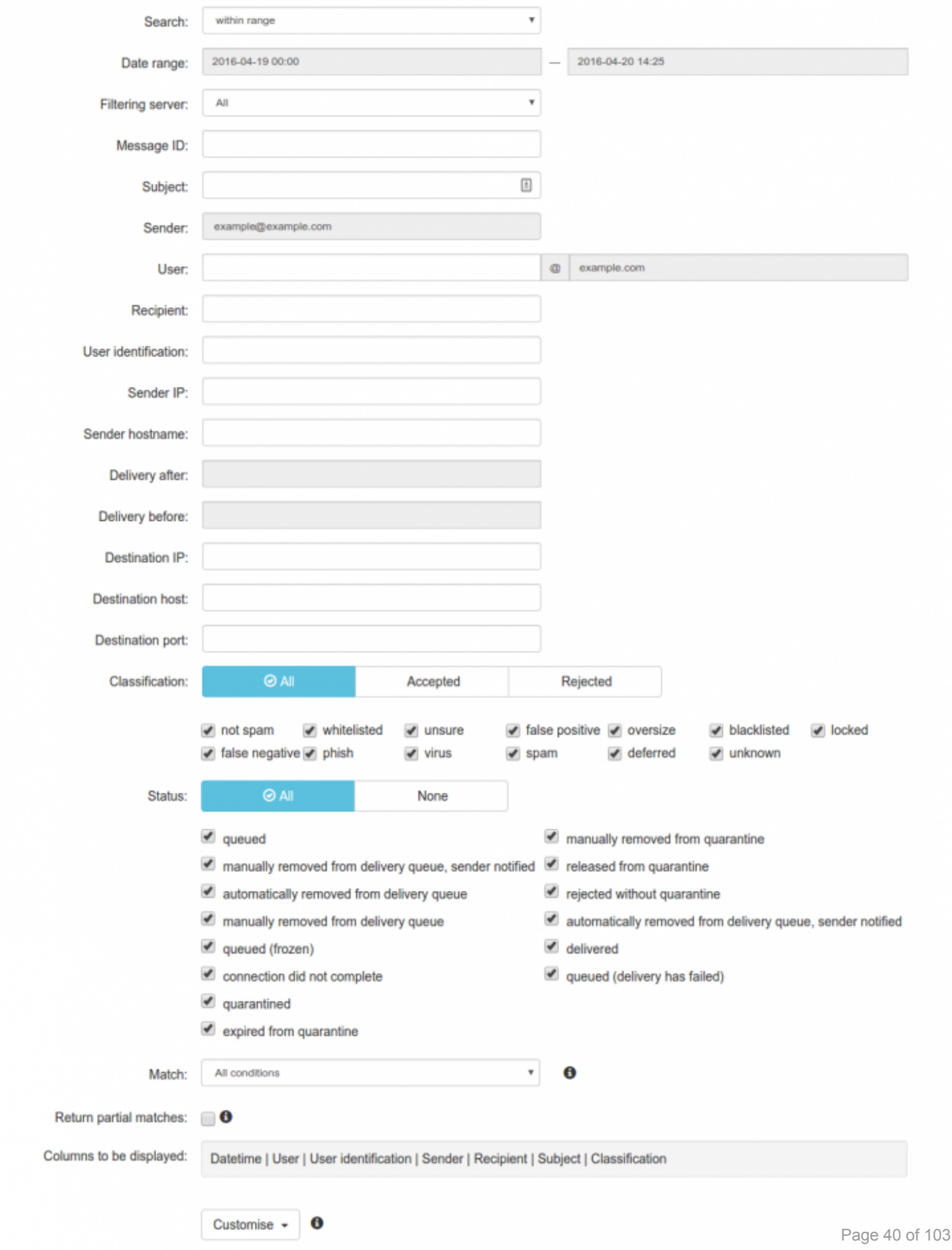
All email connections, spam and not spam, to a domain are logged to the logging server. To ensure a connection can be logged, the **“RCP TO”** information needs to have been received. Connections are generally only temporarily or permanently rejected after receiving this **“RCPT TO”** data, to ensure 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 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 | 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.

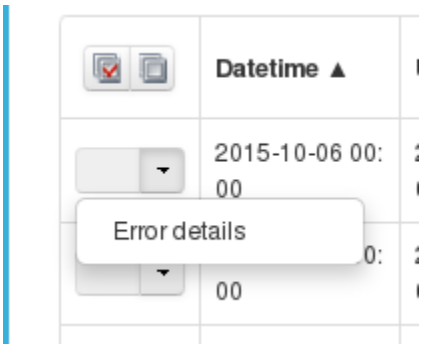
Delay

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.

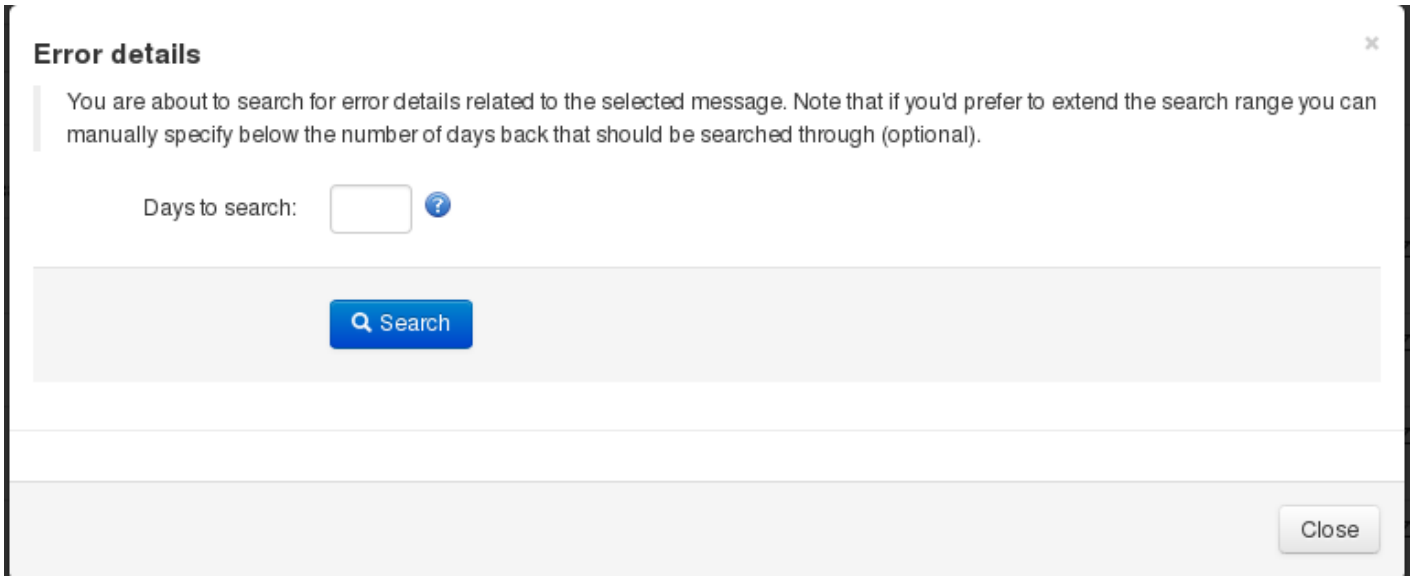
Information logged

- 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.



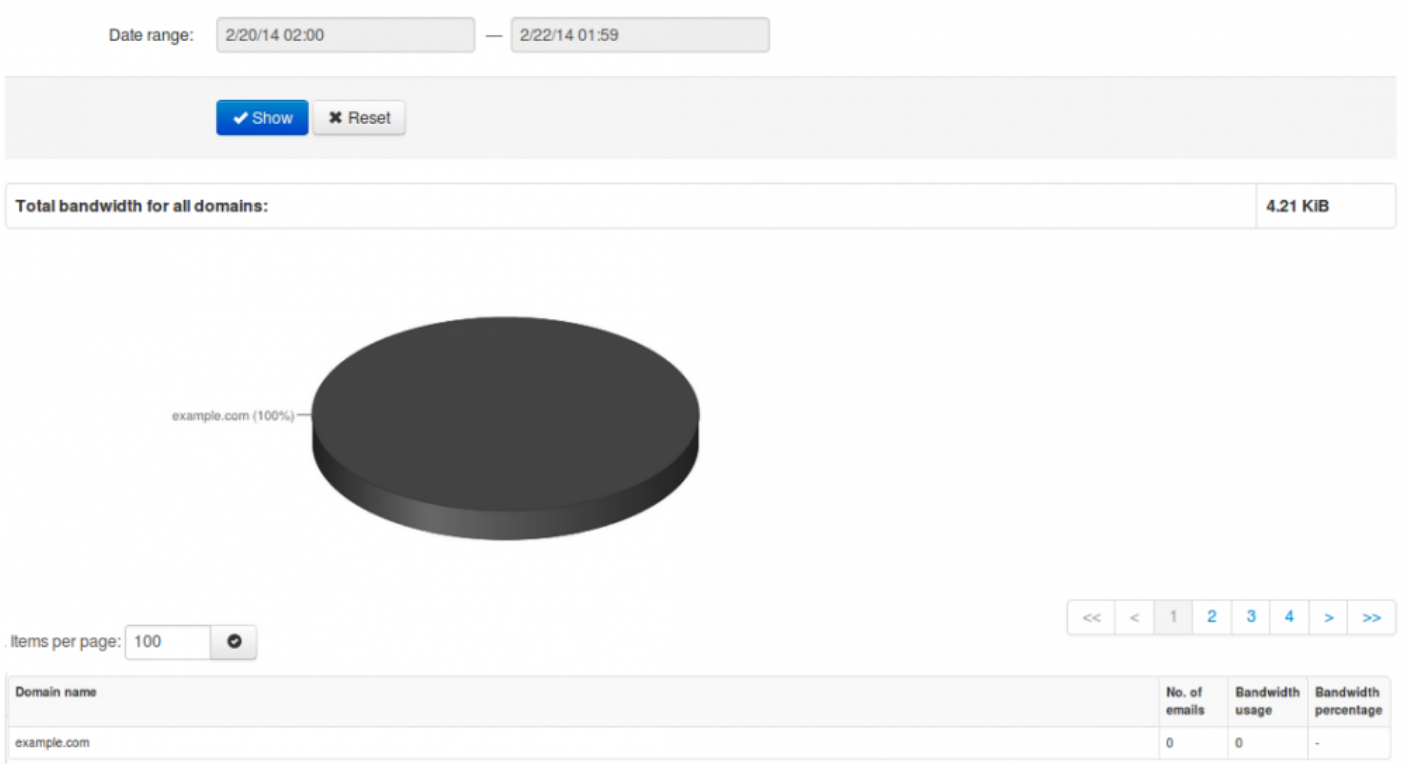
Here you can manually specify the number of days that should be searched through, starting from 1 and up to 31.



! 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.

Outgoing Bandwidth Overview

On this page you will find an overview of the outgoing bandwidth usage per domain for a given time-frame and the total Outgoing bandwidth used:



Outgoing Spam Quarantine

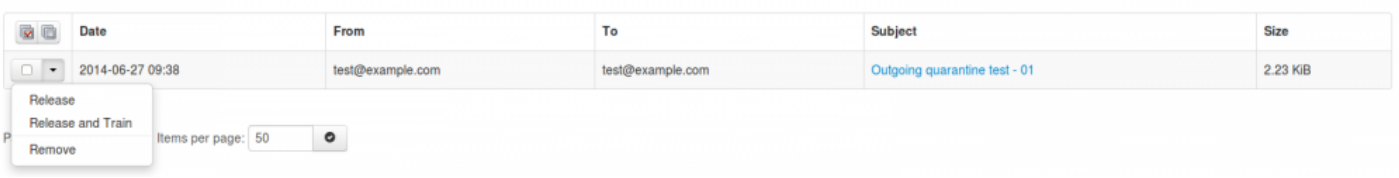
! The Global Outgoing Spam Quarantine is only available to Super-Administrators. Administrators, Domain & Email users do not have access to the Outgoing Spam Quarantine. Only administrators can release emails from here.

The Global Outgoing Spam quarantine, will show you all the Outgoing quarantined messages for all domains on the system.

* 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.

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



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

'**Remove**' will delete the message from the Outgoing Spam Quarantine.

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

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

If a Attachment is included in the quarantined message, then this can individually be downloaded by clicking on the ‘Attachment:’ line in the normal view.

Outgoing Delivery Queue

On this page you can view the emails that are currently in the queue, excluding frozen emails that failed to bounce because of an invalid sender

The emails are queued only if the destination server is not accepting them. You can also force the delivery of queued messages if the issues on the destination mail server have been fixed.

The delivery queue also automatically retries to deliver the emails.

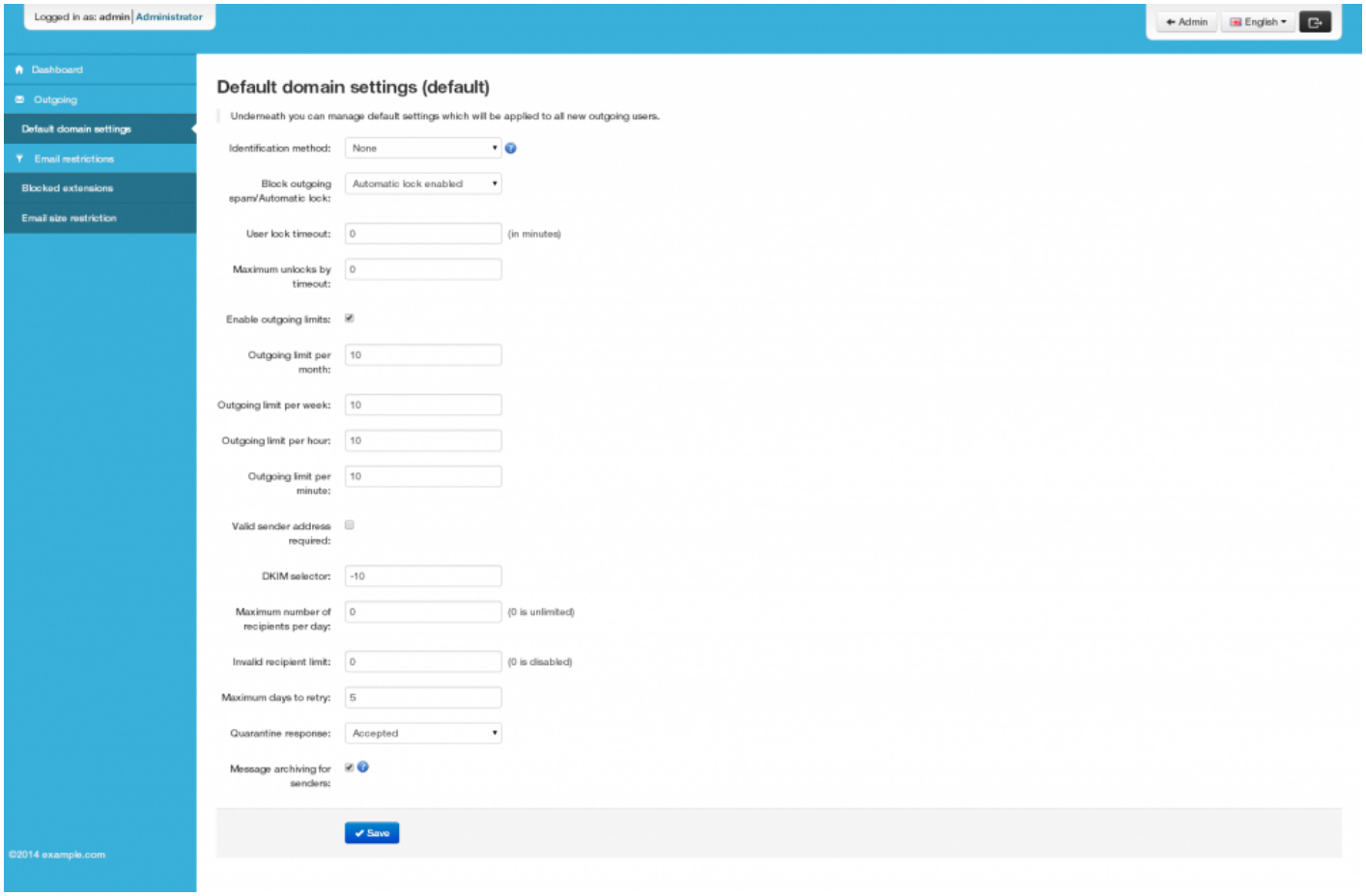
You can search the emails in queue by multiple criteria:

- Server
- Message ID
- Time
- Size
- Sender
- Recipient

You also have the option to match you searches and/or exclude frozen emails, include frozen emails or both, but also return partial matches.

Outgoing Default Domain Settings

On this page you can control certain default domain settings. The default settings apply to all domains that have not yet explicitly set a custom value for the setting, and are therefore using the default settings.

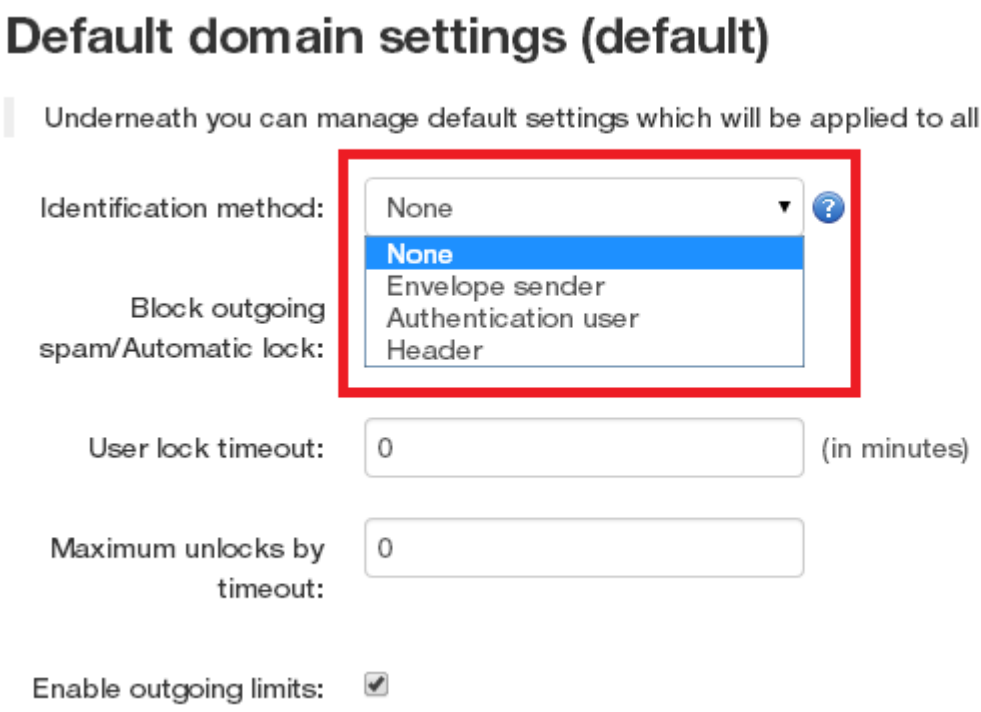


With Default Domain Settings you can manage the default settings which will be applied to all new outgoing users:

- **Identification Method**: Here you can choose either, “envelope sender” , “authentication user” or “Header” for the identification method.
- **Block outgoing spam/Automatic lock**: The option ‘Automatic Lock Enabled’ will lock the user and stop the respective 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 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**: 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 a 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), is a new "Identification method" choice.

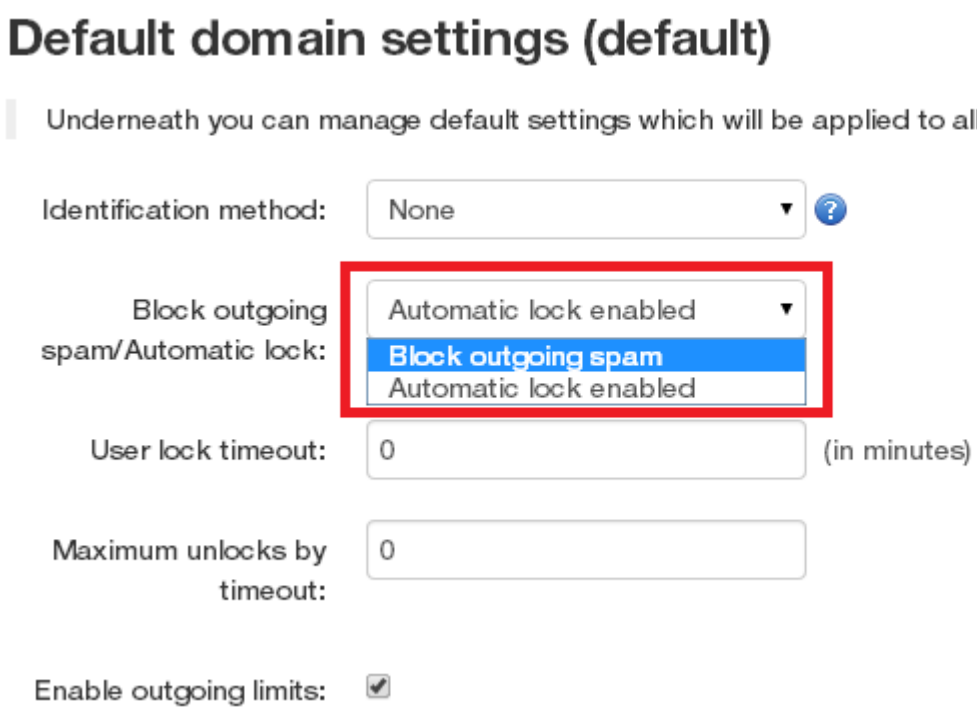


As can be seen in the above screenshot, you have three choices:

1. The **“envelope sender”**, or **MAIL FROM** value. If your system enforces this, then it 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”**. By choosing 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 has been automatically/manually unlocked.



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 failed, i.e. a 4xx code, 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.

Outgoing IP whitelist

The Outgoing Whitelist feature allows you to whitelist specific checks when used for the outgoing filtering. You can also specify a reason for whitelisting a specific IP/range.

- Sender validation skipped
- MX/A DNS check skipped
- Required FROM domain check skipped
- Content checks skipped

Outgoing IP Blacklist

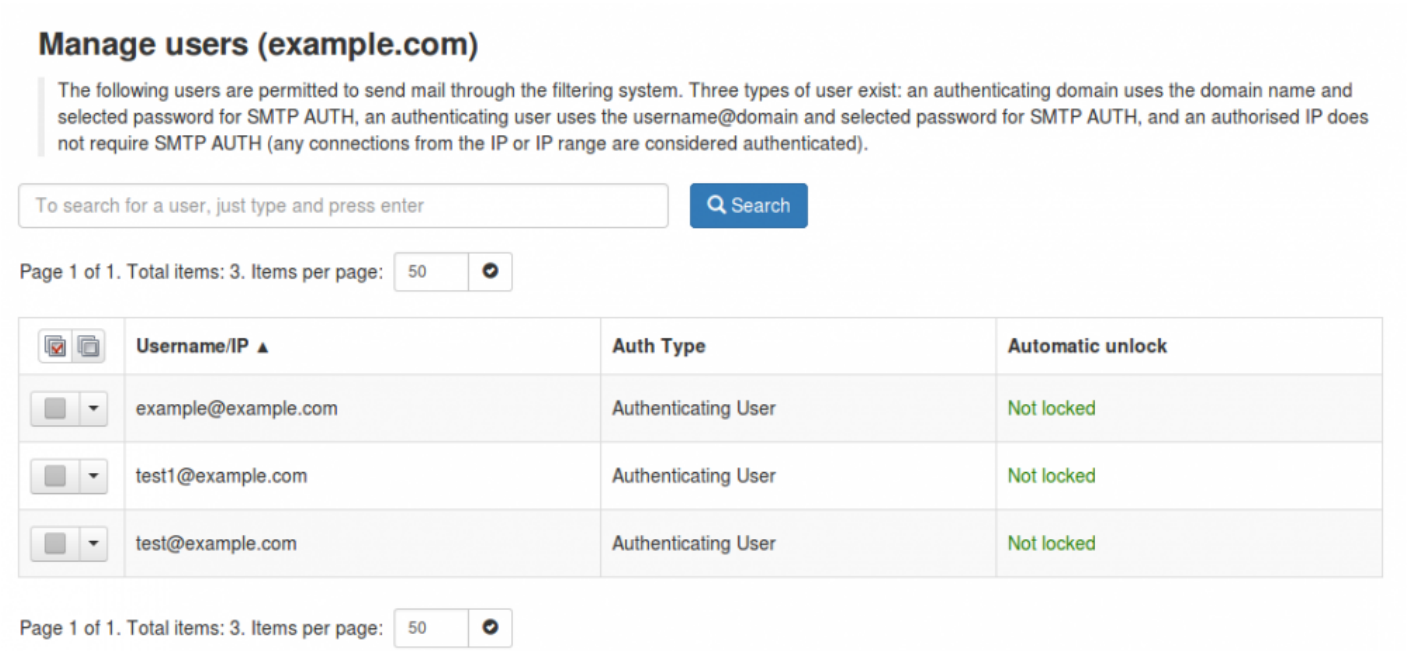
Traffic from IP addresses listed on the IP blacklist will get immediately rejected. The messages are NOT quarantined. The messages are rejected with a 5xx SMTP error code, so legitimate sending SMTP servers will generate a bounce message to the sender. You have the option to add, edit and delete IP addresses, as well as specify a reason for blacklisting the IP address.

Global Outgoing Callout Cache

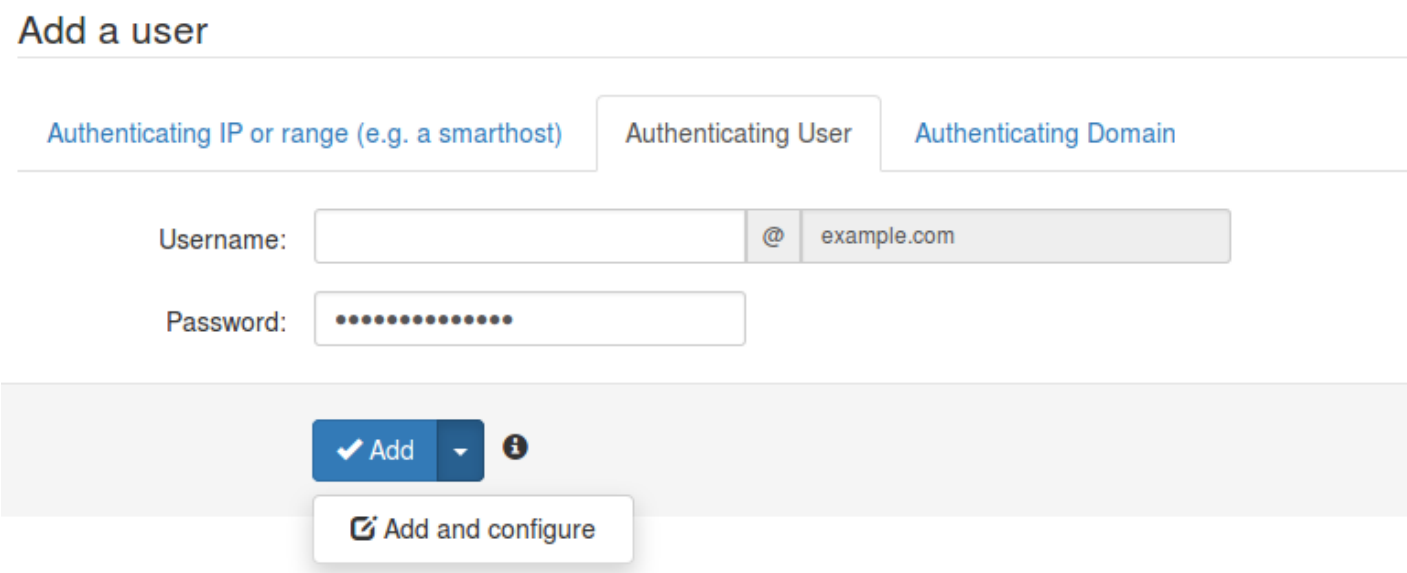
On this page you can clear the callout cache for all outgoing domains. By default we cache server responses to 2 hours.

Manage Outgoing Users

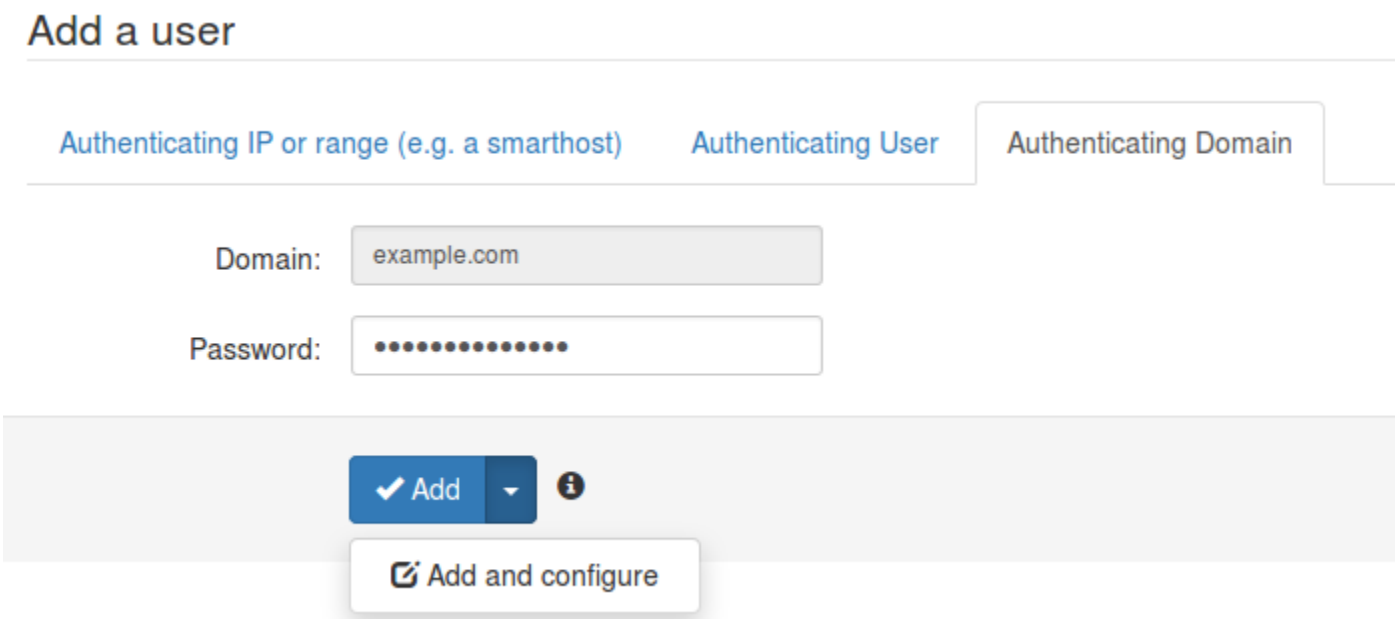
This feature enables you to create and manage outgoing users.



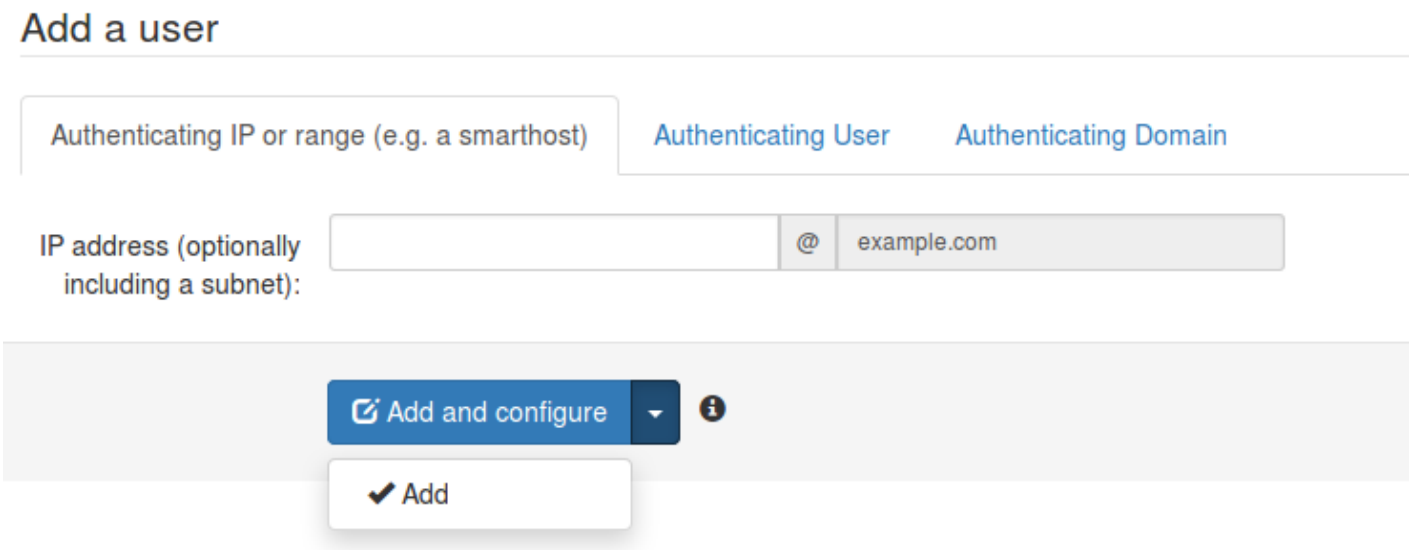
When adding Outgoing Users you can choose from:



“**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.

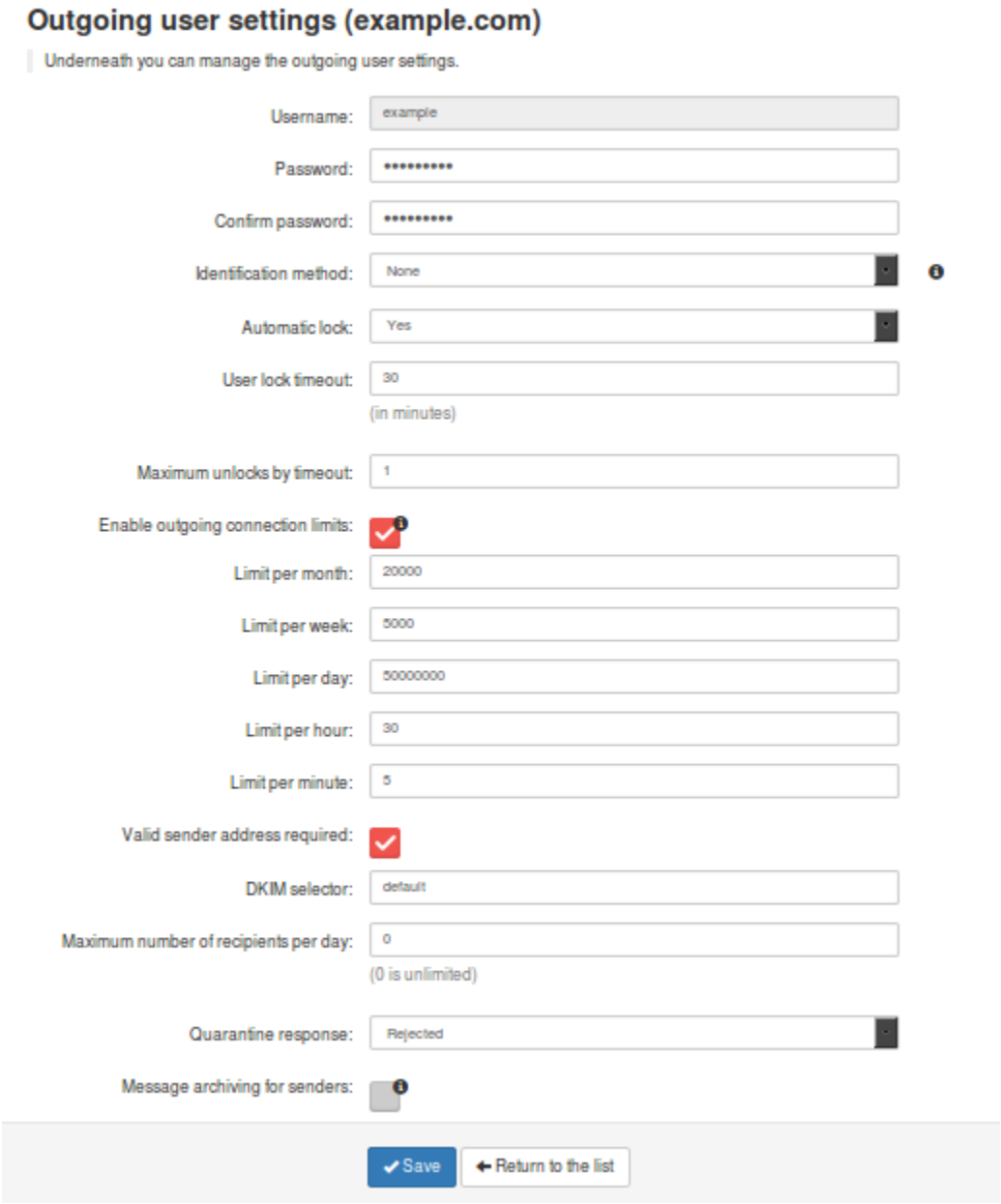


“**Authenticating Domain**” – which means that the domain name is the username for authentication, with the configured password.



“**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.

Add Multiple Users

With this option you have the ability to add multiple users via a .csv (Comma Seperated Values) file. Each line must contain 3 columns: username, domain, password.

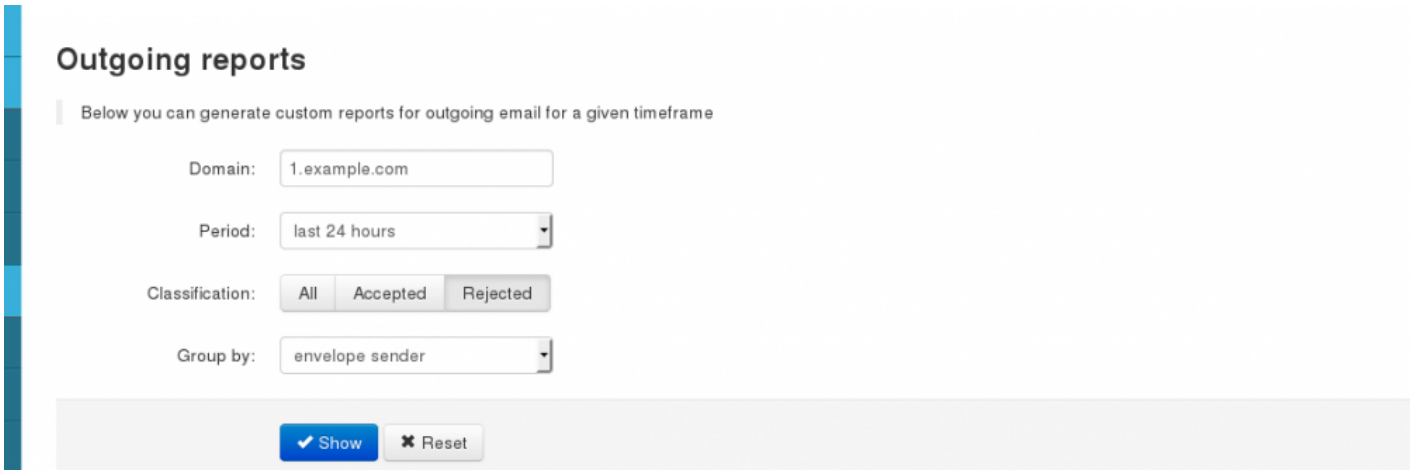
An example .csv file would be: **user1,example.com,Mypassword321**

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

The .csv file must be less that 9MB.

Outgoing Reports

On this page you can generate custom outgoing email reports for a given time frame.

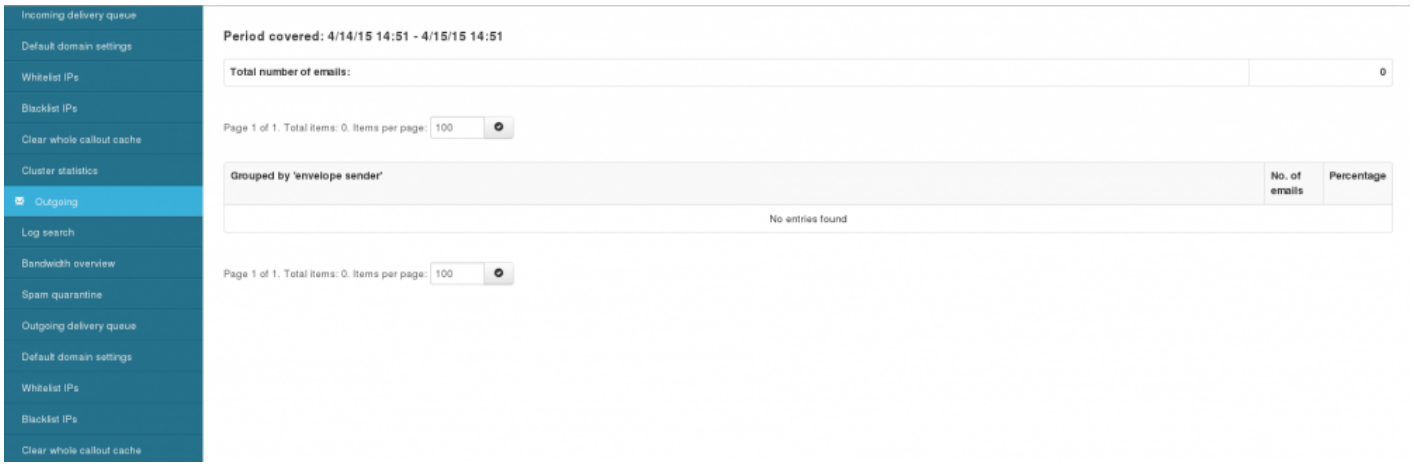


You can see from these reports the number of messages sent for a time frame ranging from last hour up to the last seven days.

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.

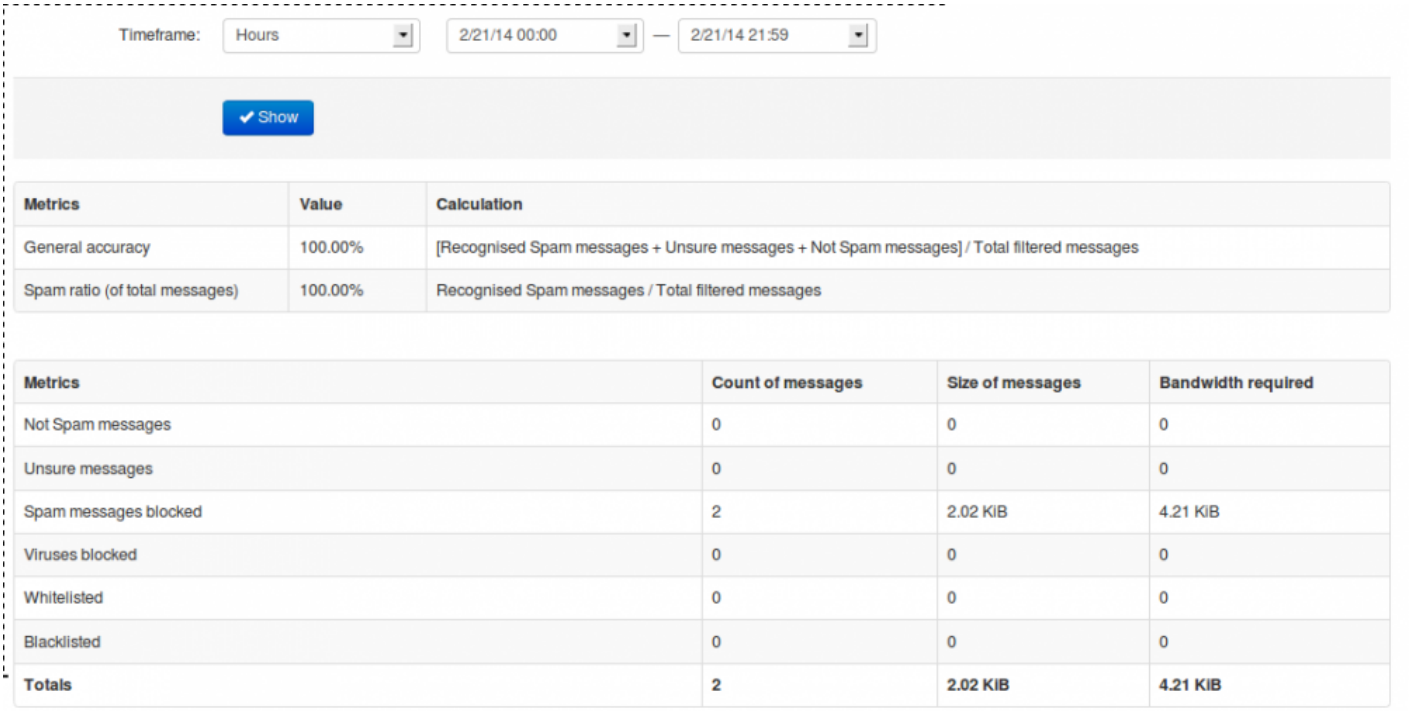

Incoming delivery queue
Default domain settings
Whitelist IPs
Blacklist IPs
Clear whole callout cache
Cluster statistics
Outgoing
Log search
Bandwidth overview
Spam quarantine
Outgoing delivery queue
Default domain settings
Whitelist IPs
Blacklist IPs
Clear whole callout cache
Period covered: 4/14/15 14:51 - 4/15/15 14:51
Total number of emails:
0
Page 1 of 1. Total items: 0. Items per page: 100
Grouped by 'envelope sender'
No. of emails
Percentage
No entries found
Page 1 of 1. Total items: 0. Items per page: 100

Outgoing Global Statistics

With the Outgoing Global Statistics users can view the outgoing statistics for a given time-frame (Hours,Days,Weeks,Months,Years).

Statistics are displayed for :

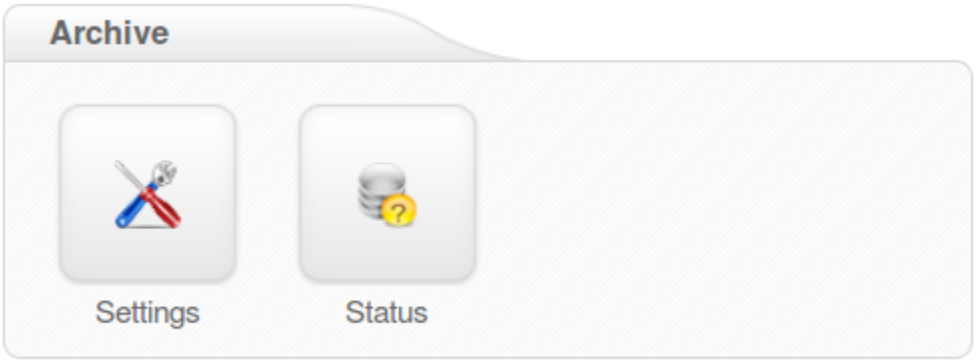
- General accuracy
- Spam ratio (of total messages)
- Not Spam messages
- Unsure messages
- Spam messages blocked
- Viruses blocked
- Whitelisted
- Blacklisted



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**

Email Archiving



- Settings
- Status

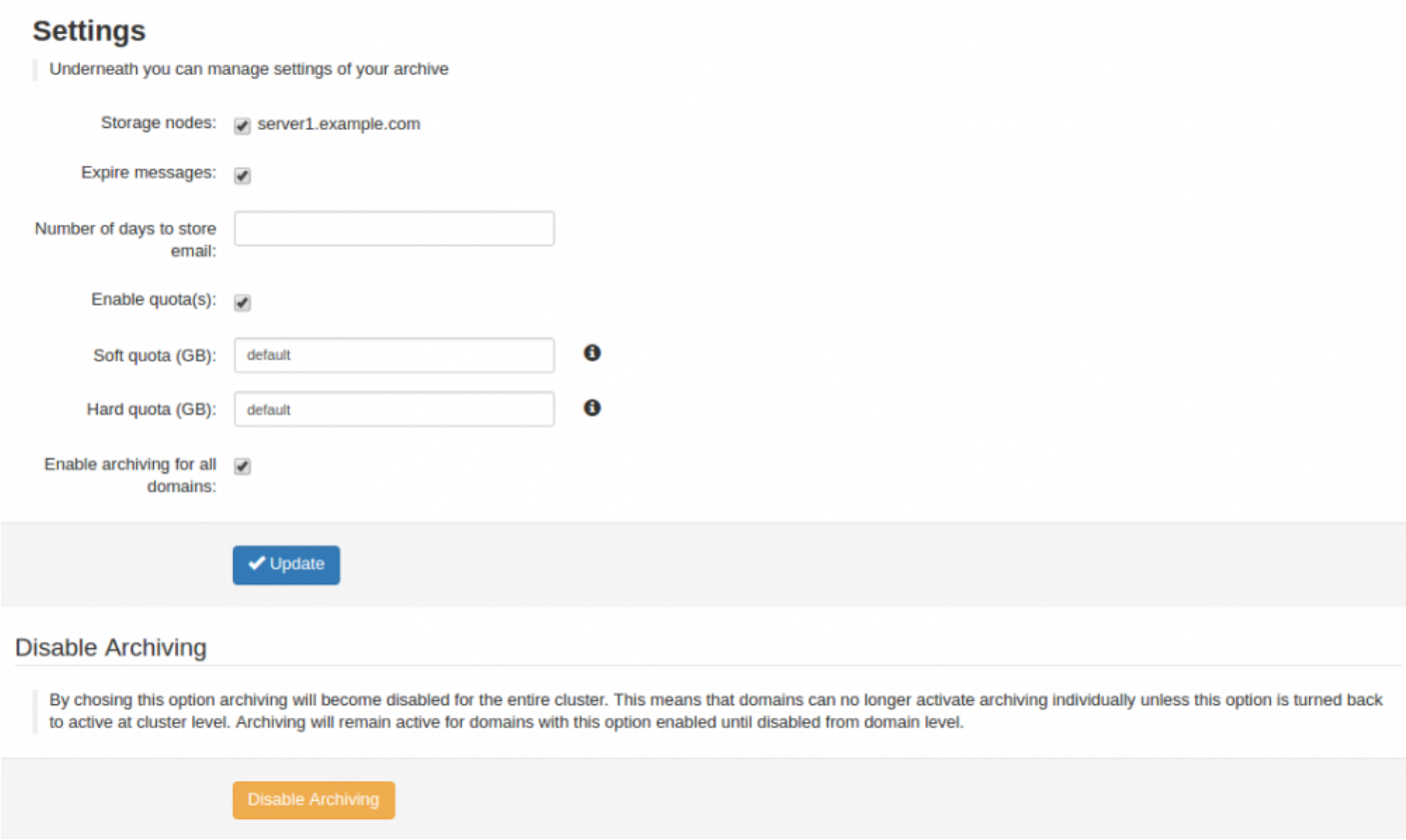
Settings

You can select which node(s) you wish to use for storage, and the number of days to store the archived emails for. This must be set before you can start using the archiving service.
On the Archive Settings page manage in the SpamExperts Control Panel – Super-Administrator level – Archiving Settings you can manage quotas for the archive product within the web interface. Two types of quota are available (you may use neither, either one, or both). The “soft” quota sends an email message to the contact address for the domain (and a CC to the admin address for the domain) warning the user that they have reached the specified limit. The “hard” quota deletes the oldest messages in the archive when the limit is reached, to make room for new messages.

You can also choose what type of Storage when multiple nodes are used.

- Striping
- Mirroring

There is also an option to enable/disable archiving for all domains at once.

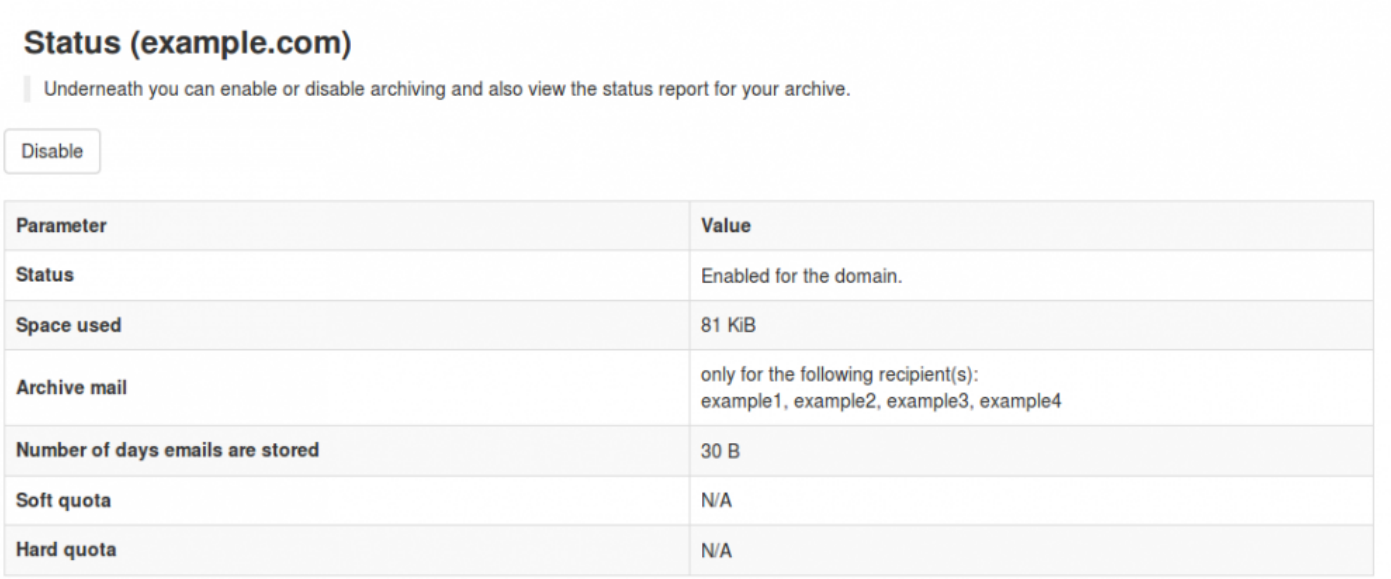


Status

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



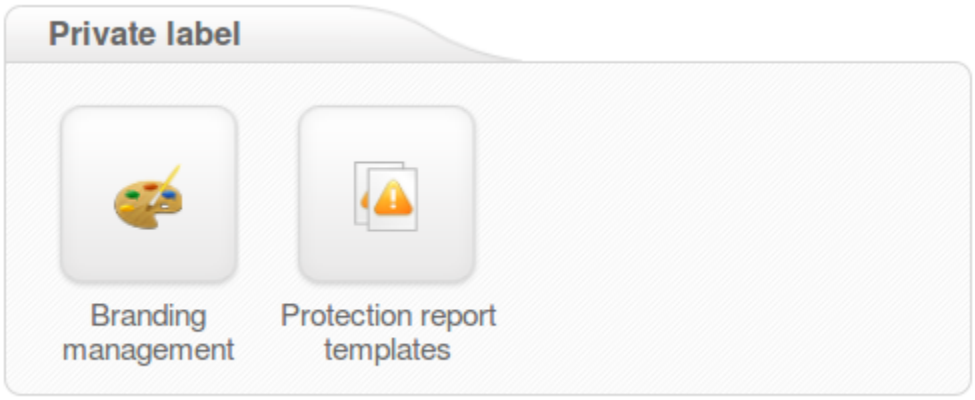
Parameter	Value
Status	Enabled for the domain.
Space used	81 KiB
Archive mail	only for the following recipient(s): example1, example2, example3, example4
Number of days emails are stored	30 B
Soft quota	N/A
Hard quota	N/A

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

Private Label

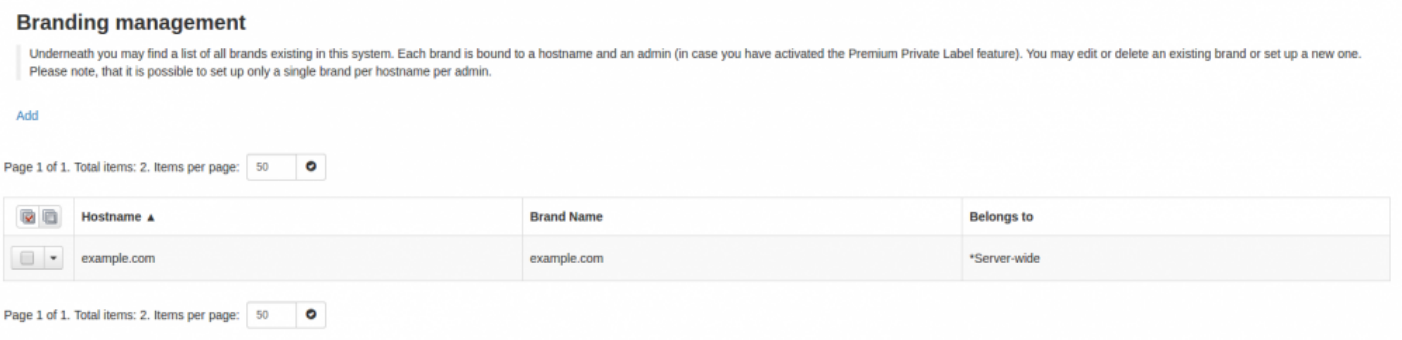


- Branding Management
- Protection Report Template

Branding Management

With branding enabled, you the opportunity to fully customize the software with your own branding and logo to suit your requirements. Specially designed for the ISP's, Hosting companies and Enterprises, our branding options include custom email headers, web interface, customized protection reports & copyright notices.

To edit or delete a brand, just click the drop-down button from the left side of your branding name and select your action.

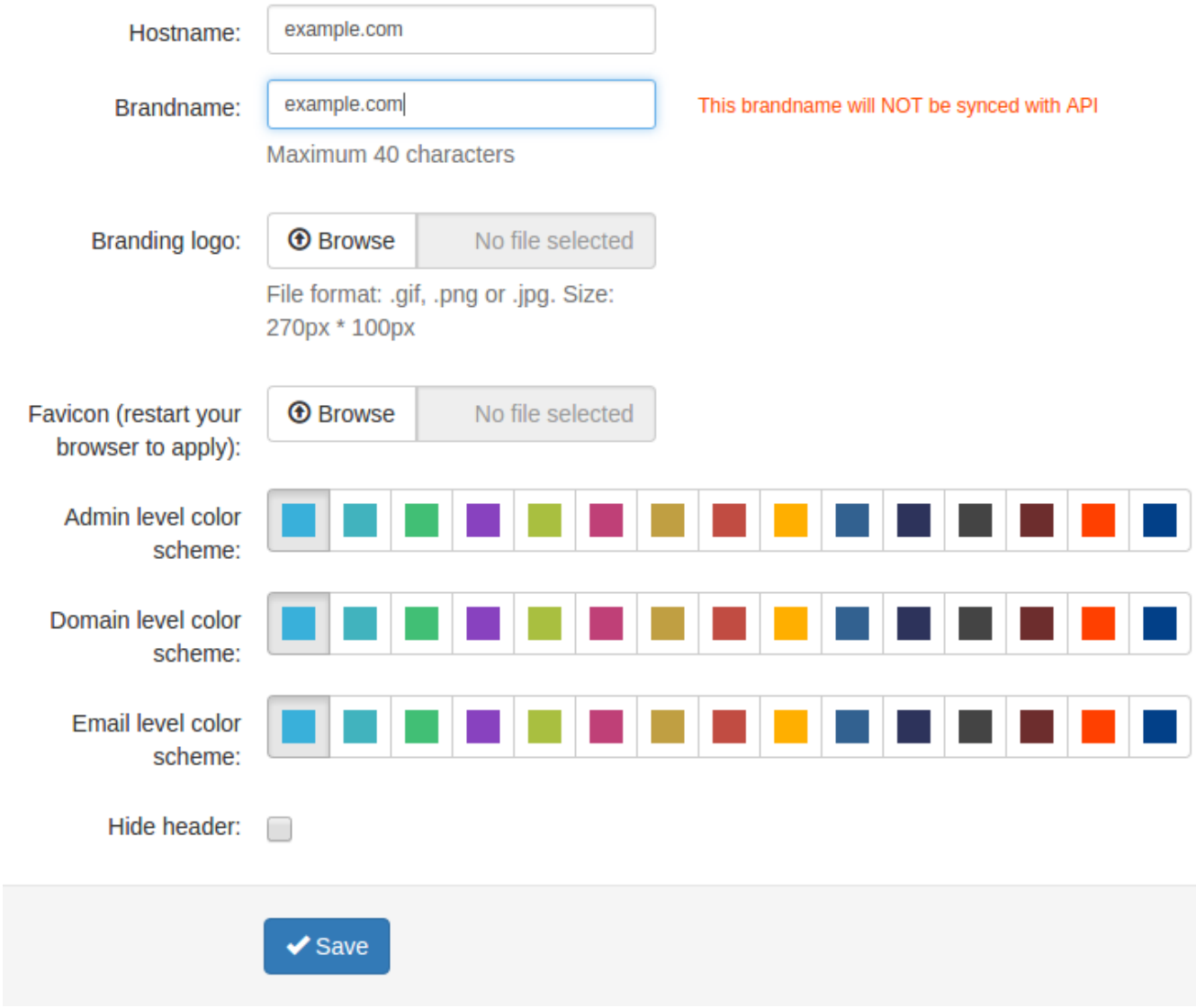


The following options can be branded with Private Label:

- Set your own Control Panel logo/favicon/color scheme
- Choose your own custom MX records
- Manage the protection report templates
- Create your own Control Panel login URL
- Set the name of the classification tags included in the email header

The "Premium Private Label" option allows you to have multiple brands within a cluster, each administrator can define his/her own branding.

- Set your own Control Panel logo/favicon/color scheme
- Manage the protection report templates
- Choose your own custom MX records
- Create your own Control Panel login URL
- Set the name of the classification tags included in the email header


Hostname:
example.com
Brandname:
example.com
This brandname will NOT be synced with API
Maximum 40 characters
Branding logo:
Browse
No file selected
File format: .gif, .png or .jpg. Size: 270px * 100px
Favicon (restart your browser to apply):
Browse
No file selected
Admin level color scheme:
Domain level color scheme:
Email level color scheme:
Hide header:
Save

Protection Report Template

The content of the HTML report may be customized via the API/webinterface. By default, it includes the quarantined messages table, but does not include the table of messages that were rejected without quarantine, this setting can be adjusted to show both tables.

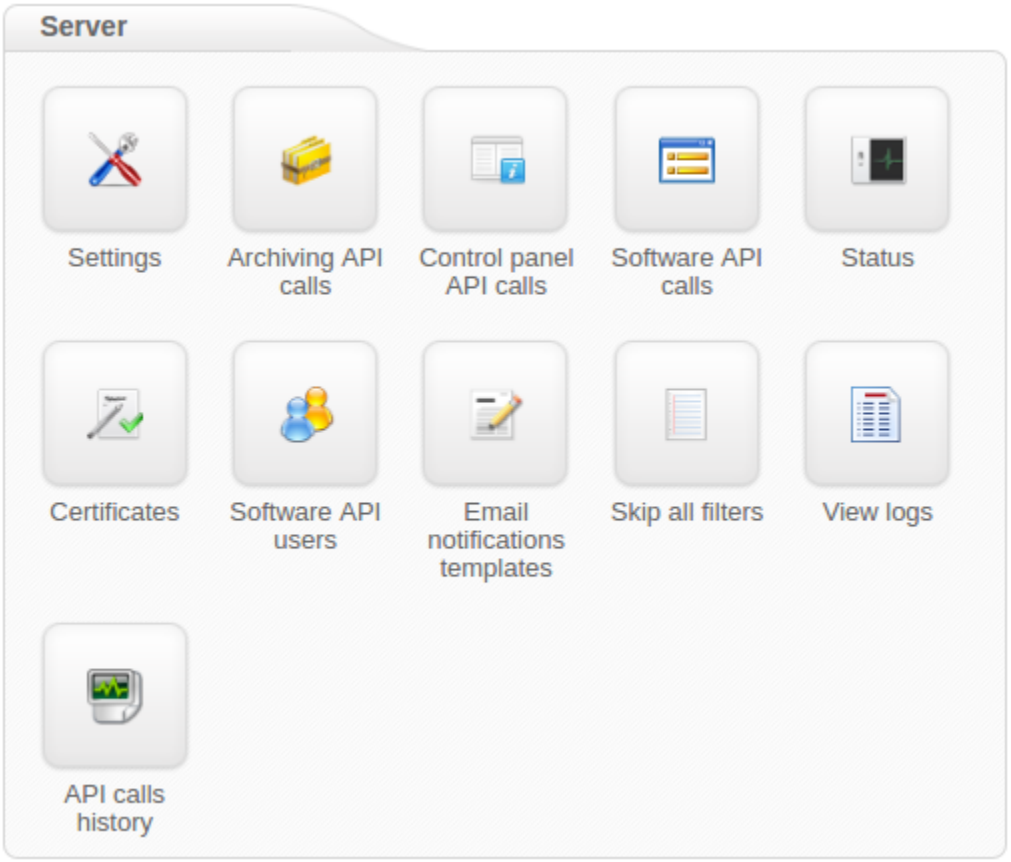
Customization of Protection Template Report:

Here you can create or edit existing protection reports, so they can be tailored to suit your specific needs. You can customize the following:

- Language
- Email Subject
- From address
- Reply-To address
- Sender address
- Attachment filename
- PDF body
- HTML body
- Domain name
- Welcome email subject
- Welcome email text
- Non-black report color
- Long date format
- Short date format
- Quarantine Hostname
- HTML Stylesheet
- HTML TR template
- HTML TH template
- HTML TD template
- Show subjects as links in the message view.

It is possible to set a different Logo on the “Protection Reports” that in the “Branding Management” section.

Server



- Server Settings
- Archiving API calls
- Control Panel API Calls
- Software API calls
- Server Status
- Certificates
- Software API Users
- Email Notifications Template
- Skip All Filters
- API Calls History

Server Settings

Within the control panel there are a number of settings that can be changed, including: the default settings for the products you have purchased, the administrator's contact, the contact URL that will be used in case of a 'contact us' button and the logout URL that will be used in case of a 'logout' button. Also you can choose the date and time format and your timezone. If you want to use one or more additional languages, you can choose them here also.

On this page you can also choose if your products will be by default enabled for domains or users.

Admin users have the ability cu customize the following settings:

- Download the 1-click Log in script
- Administrator's contact
- Contact Us URL
- Logout URL
- Timezone
- Date and time format
- Default Language
- Force secure (HTTPS) connections
- Default Items per page
- Email notifications From address
- Email notifications To address
- APS to Control Panel access message
- You can set your default MX hostnames

Super-Admin users can use the following features on this page, including the ones described above for admins:

- Auto-enable sub-admins for all admins
- Auto-enable release spam messages for all admins
- Session timeout
- Force clear the web-interface cache (this is auto-cleared approximately every 5 minutes)
- Force DNS cache clear
- SSH Allowed IP's
- IP addresses allowed.
- IP ranges allowed for user submission
- Choose your preferred cluster update day and time

- You can set your default MX hostnames

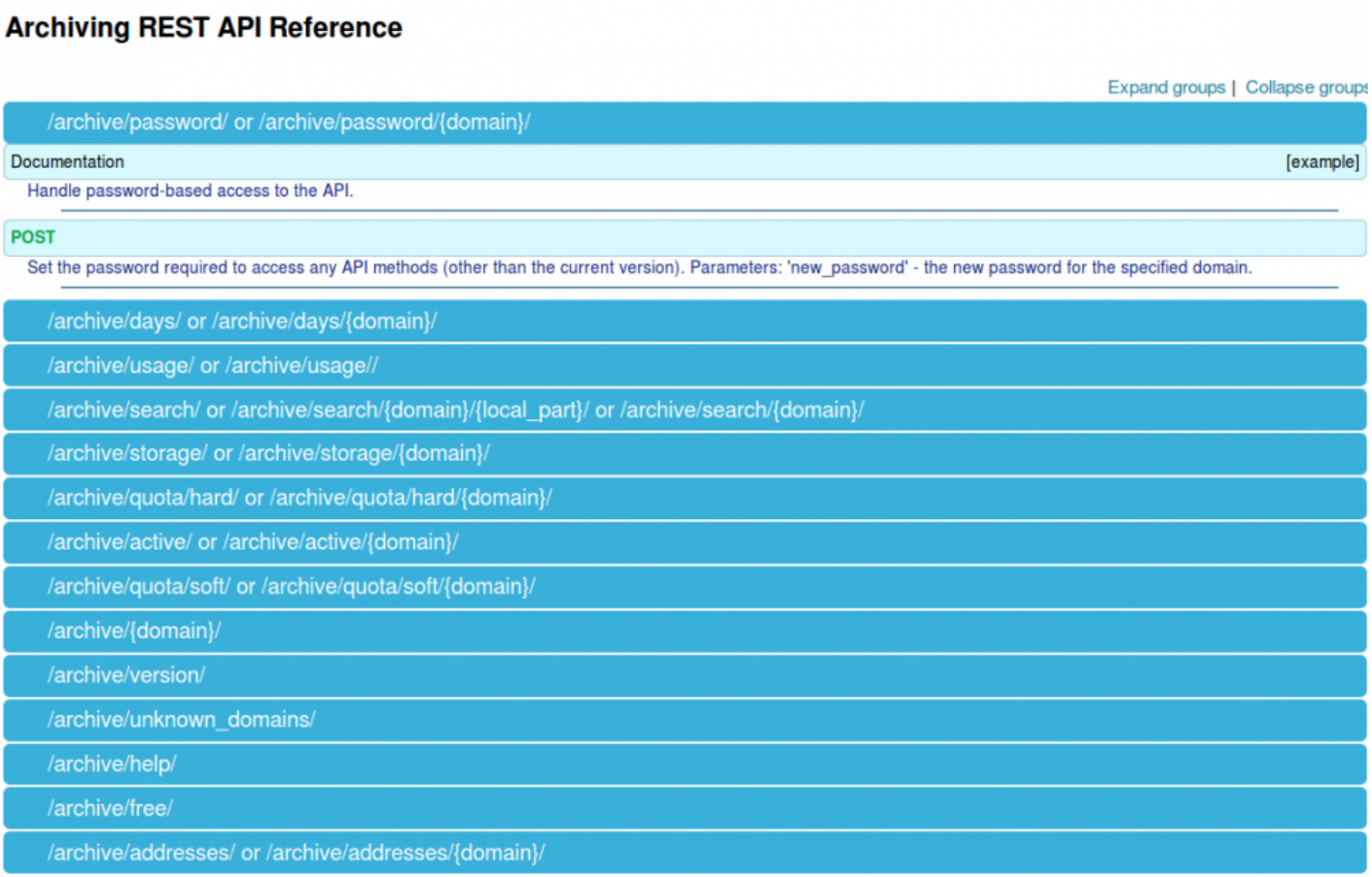
Archiving API calls

Clicking the “Archiving API calls” tab will direct you to the help page. Here it will give you a comprehensive guide to all the archiving calls used.

The Archiving API allows you to automate the process for setting the number of days for messages to be be archived, get overall information about usage of the archive for specific domains, search/delete messages to the appropriate storage nodes, set the storage system for the domain, set the archive hard/soft quota, access messages in the archive of a domain, get the arching API version, control the behavior of the API when messages are submitted for an unknown domain, get dynamically generated documentation for this API, get data about space free on the used storage nodes.

Your Archiving API username is your Super-Admin username.

Example Archiving API calls:



Control Panel API Calls

Clicking the “Control Panel API calls” function will direct you to the help page. Here it will give you a comprehensive guide to all the calls used.

The Control Panel API allows you to automate the process of adding/removing domains to admin accounts, allowing your customers/admins/sub-admins to use a one-click-login solution and modify the settings of the domains in the system. You can also use this account with our range of add-ons.

Your API username is your Admin username.

> ! The option enable Control Panel API must be enabled from the user settings, Dashboard > Webinterface Users > Manage Super-Admins/Admins.

Example Control Panel API calls:

- /api/domain/add/domain//[destinations//][aliases//]
- /api/domain/edit/[domain//]destinations//
- /api/domain/exists/[domain//]
- /api/domain/getbandwidthusage/domain//since//until//

General notes

While doing API requests you may tell the API which output format to use.
The plaintext format is used by default. To set an output format you need to pass an additional parameter - 'format'.
The resulting request URI should look like:

http://demo1.spambrand.com/api/controller/action/format/<*format_id*>/param1/value/param2/value/etc.

Currently the following format IDs are supported:

- plain
- json

Expand groups | Collapse groups

Resellers

Authentication

Software API calls

The Software API allows you to configure your cluster at a much more refined level than from the interface. These calls can be used in custom scripts and add-ons and in your custom integration.

Clicking the “Software API calls” function will direct you to the API documentation page.

For example:

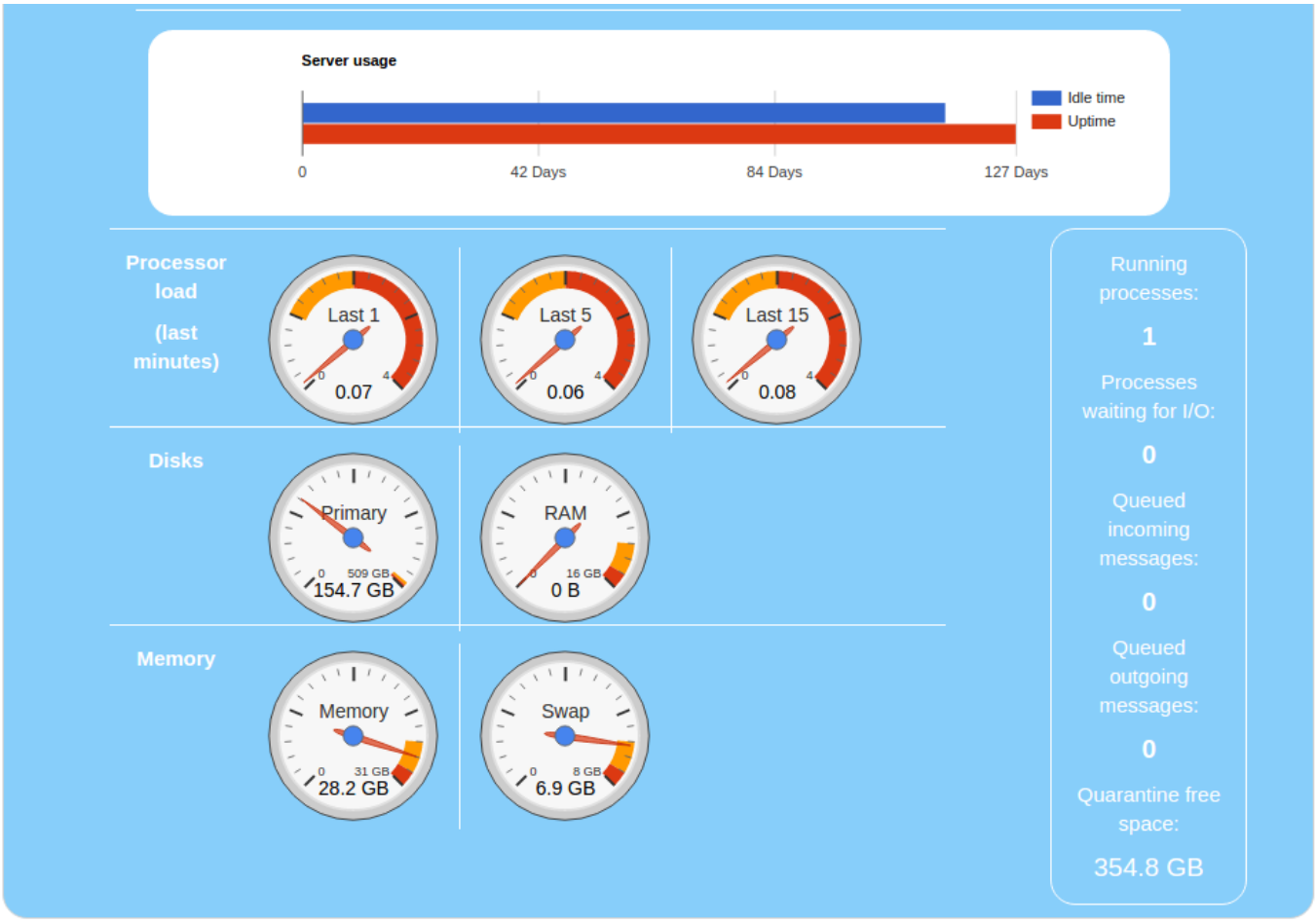
- api_add_domain_alias(domain, alias)
- api_add_incoming_domain(domain, destination)
- api_add_local_recipient(domain, local_part)
- api_get_administrator_contact(domain)
- api_get_administrator_from(domain)

To view all API calls click the Expand All Categories link:

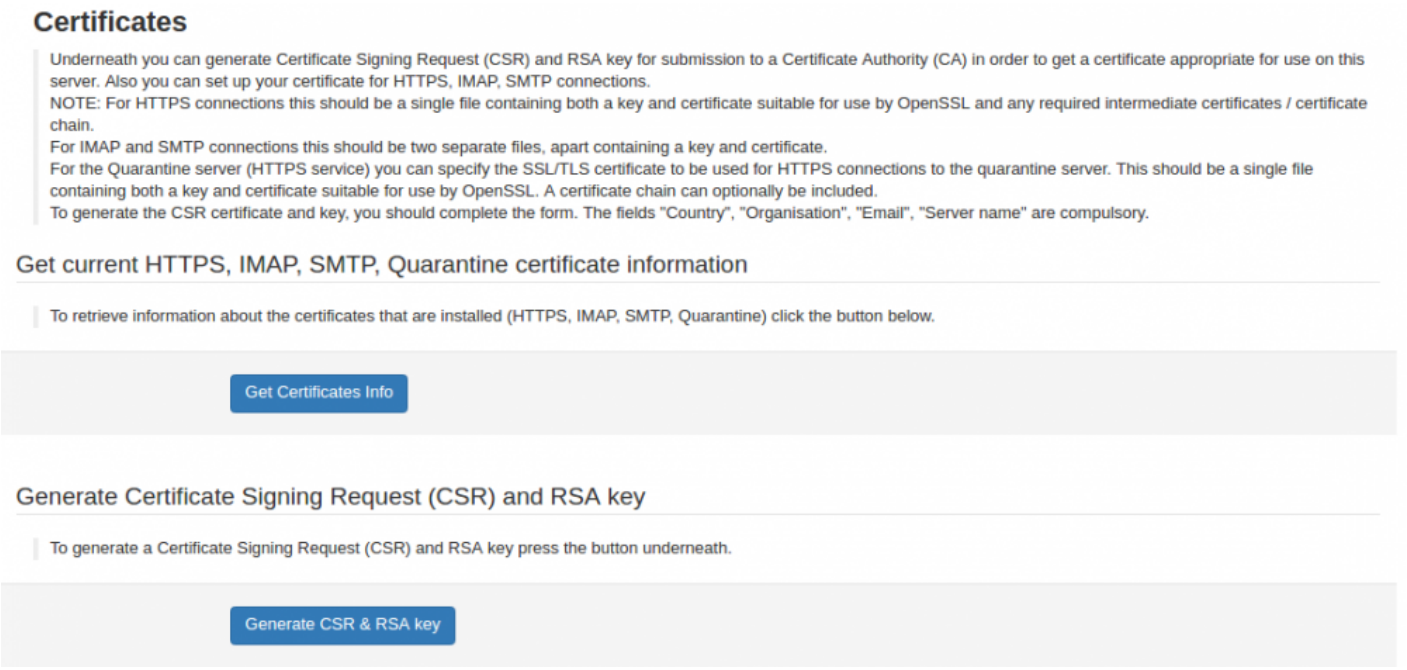
Server Status

Here you will see a graphical interface providing detailed informations and the status of your server(s), including:

- Load
- Uptime
- Idle time
- Free Memory
- Swap Used
- Number of running processes
- Free Disk Space
- Number of queued incoming & outgoing messages
- Quarantine free space



Certificates

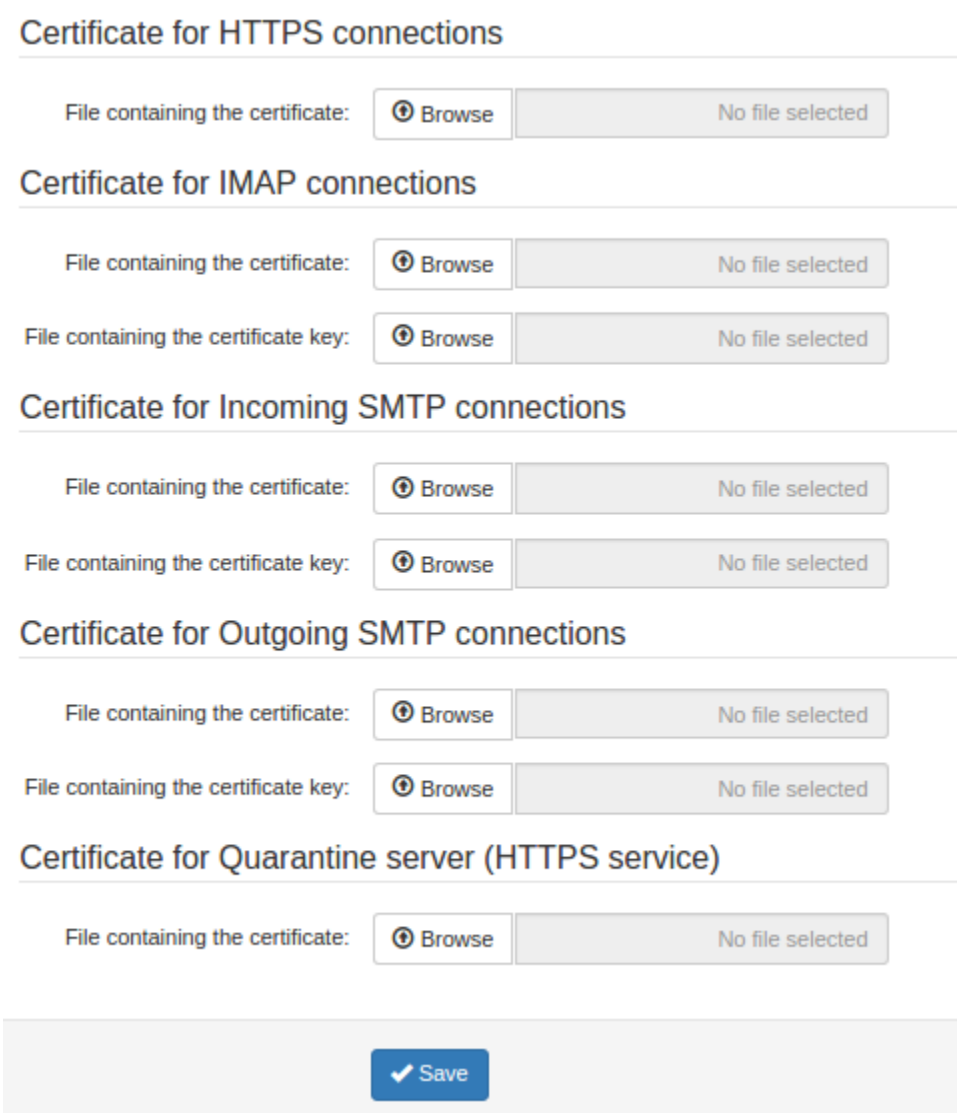


With the “Certificates” option from within the SpamExperts Control Panel you can generate the CSR (Certificate Signing Request). This allows you to set up your certificate for HTTPS, IMAP, SMTP connections.

> * For specific instructions on how to generate the CSR, create, upload and use the certificates please check our Knowledgebase article.

To generate CSR certificate and key you should fill the form. Fields “Country”, “Organisation”, “Email”, “Server name” binding on filling.

If your certificate uses a chain (root certificate), it should be included in the files.


Certificate for HTTPS connections
File containing the certificate:
Browse
No file selected
Certificate for IMAP connections
File containing the certificate:
Browse
No file selected
File containing the certificate key:
Browse
No file selected
Certificate for Incoming SMTP connections
File containing the certificate:
Browse
No file selected
File containing the certificate key:
Browse
No file selected
Certificate for Outgoing SMTP connections
File containing the certificate:
Browse
No file selected
File containing the certificate key:
Browse
No file selected
Certificate for Quarantine server (HTTPS service)
File containing the certificate:
Browse
No file selected
Save

Software API Users

On this page you can create a new Software API user and set the permissions for specific Software API Calls he can use or select one of existing API user(s) to manage it’s settings.

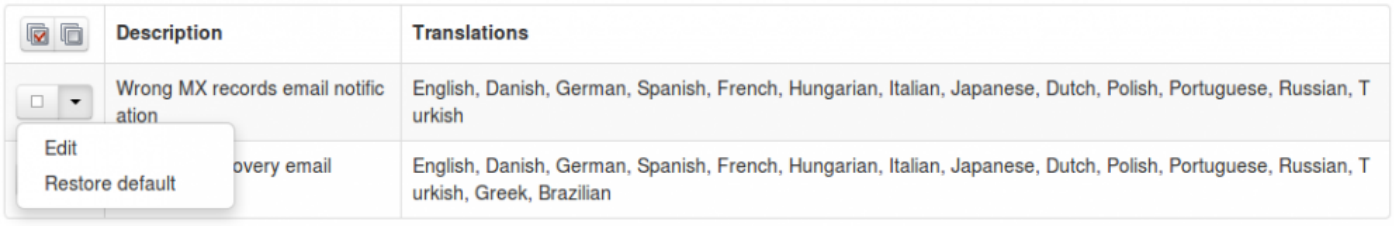
If you are using Interface Administrator IP restrictions then the restriction will also apply to the API users.

Email Notifications Template

On this page you can manage available email notification templates which can be sent out by your control panel. This option lets you edit the templates in various languages for:

- Wrong MX records email notification
- Password recovery email

The template variables that can be used are: %(domain), %(actual_mx_records), %(required_mx_records)



Skip All Filters

Here you can set an IP address to **skip ALL filtering stages**.

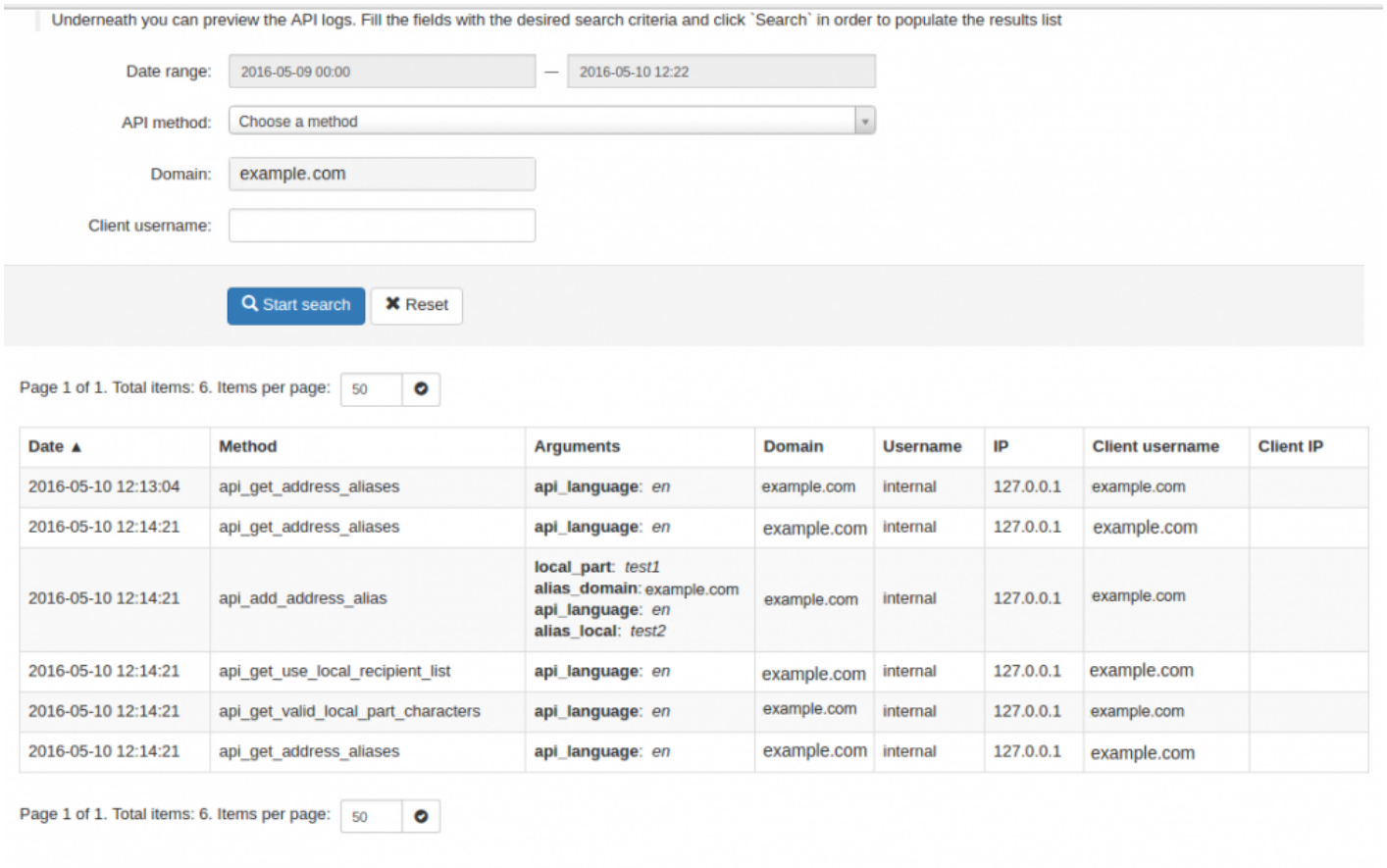
> ! This should only be used in emergency cases, as any messages to and from the IP addresses listed here will not be monitored, logged or filtered.

View Logs

On this page you can examine debug level logs. In some cases when the debug log is too large, you can download and examine it locally.

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.

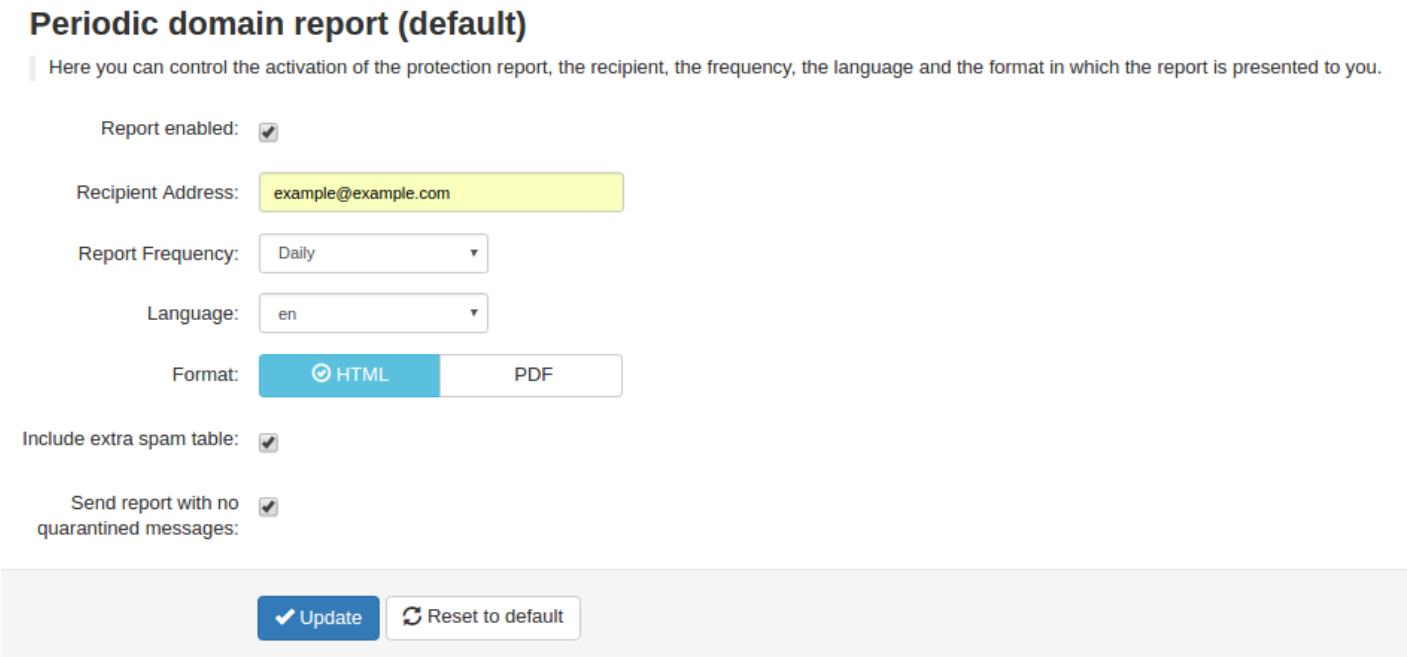


Date ▲	Method	Arguments	Domain	Username	IP	Client username	Client IP
2016-05-10 12:13:04	api_get_address_aliases	**api_language**: *en*	example.com	internal	127.0.0.1	example.com	
2016-05-10 12:14:21	api_get_address_aliases	**api_language**: *en*	example.com	internal	127.0.0.1	example.com	
2016-05-10 12:14:21	api_add_address_alias	**local_part**: *test1* **alias_domain**: example.com **api_language**: *en* **alias_local**: *test2*	example.com	internal	127.0.0.1	example.com	
2016-05-10 12:14:21	api_get_use_local_recipient_list	**api_language**: *en*	example.com	internal	127.0.0.1	example.com	
2016-05-10 12:14:21	api_get_valid_local_part_characters	**api_language**: *en*	example.com	internal	127.0.0.1	example.com	
2016-05-10 12:14:21	api_get_address_aliases	**api_language**: *en*	example.com	internal	127.0.0.1	example.com	

Page 1 of 1. Total items: 6. Items per page: 50

Protection Report

Default Periodic Domain Report



To access the Default Periodic Domain Report, go to: **Incoming** – **Default Domain Settings** – **Protection Report** (on the left hand side menu) – **Periodic Domain Report**.

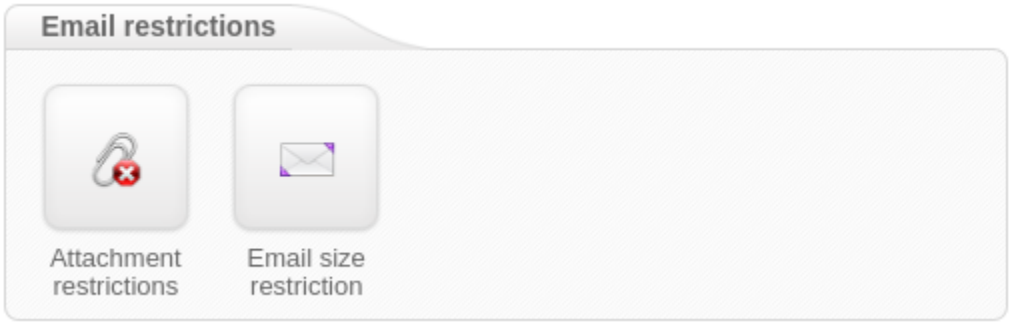
A daily or weekly report can be generated for your domain(s) and be delivered via email. Multiple recipients can be separated with a comma. A report can also be generated on-demand from the API/web interface.

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

The PDF/HTML 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. A similar table is also included with the messages that were quarantined, including links to release each message directly.

! Settings defined here will also affect other users and other domains as it sets the **DEFAULT** periodic domain report.

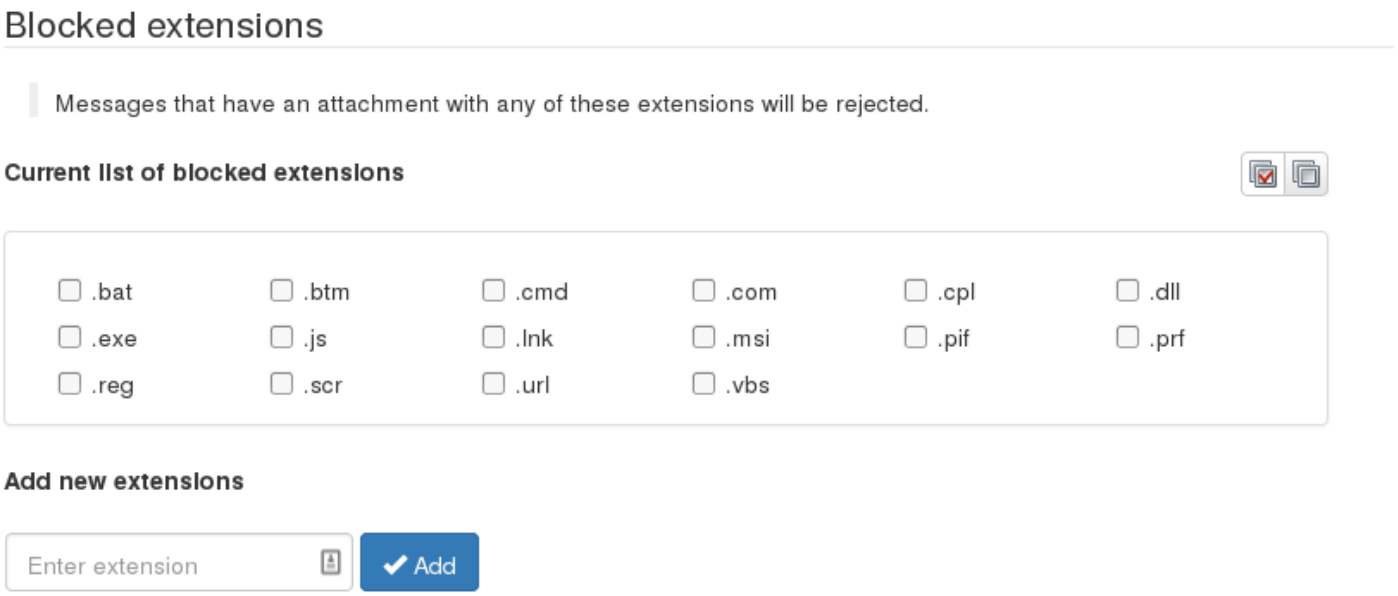
Email Restrictions



- Attachment Restrictions
- Email Size Restrictions

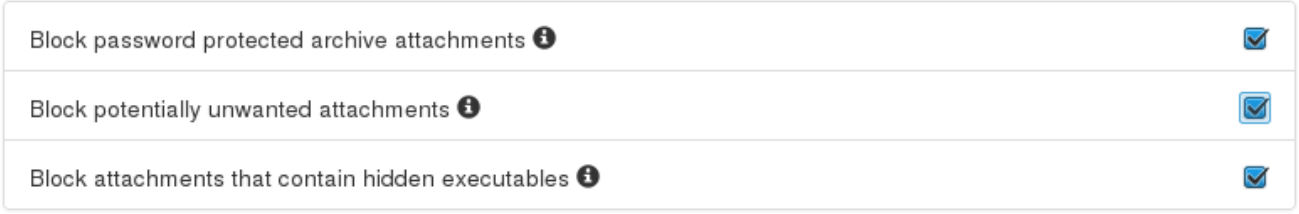
Attachment restrictions (default)

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.



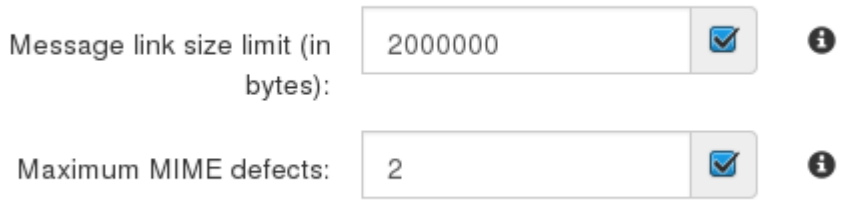
Restricted Options:

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)



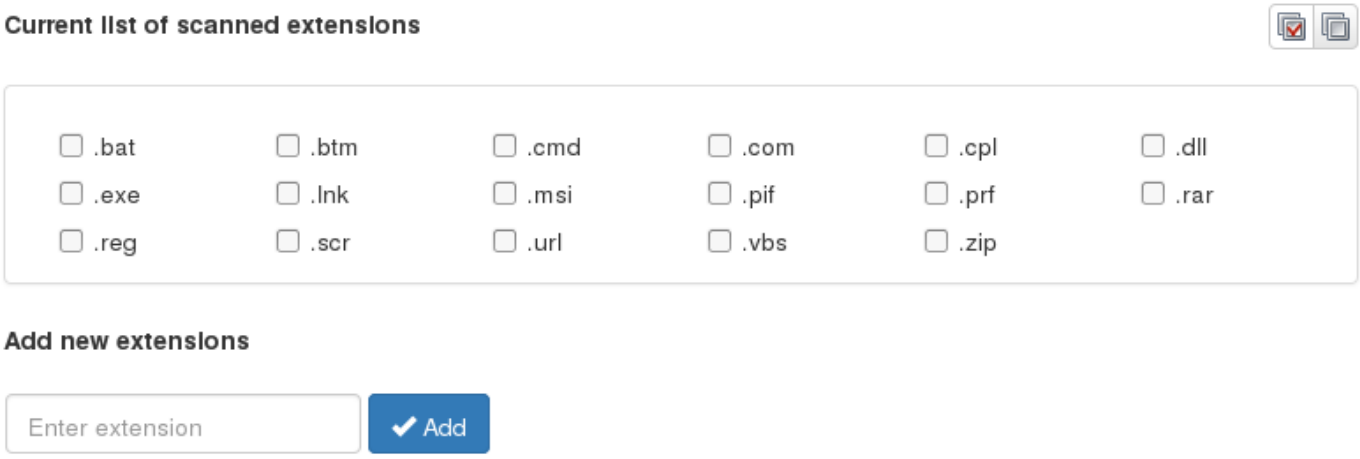
Additional restrictions:

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.

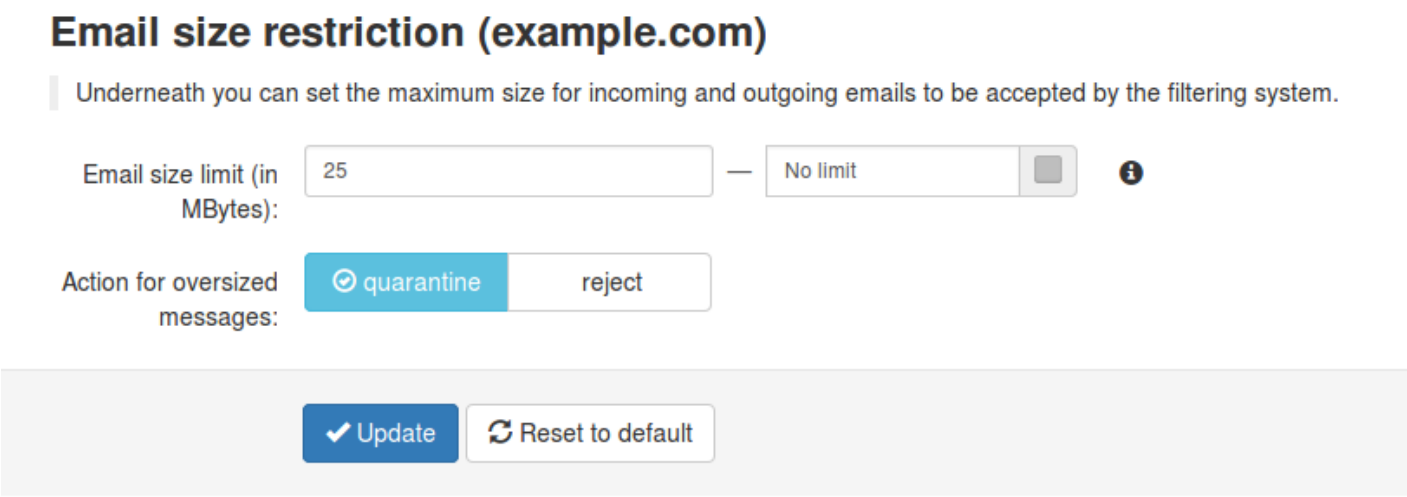


Scanned link extensions:

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.



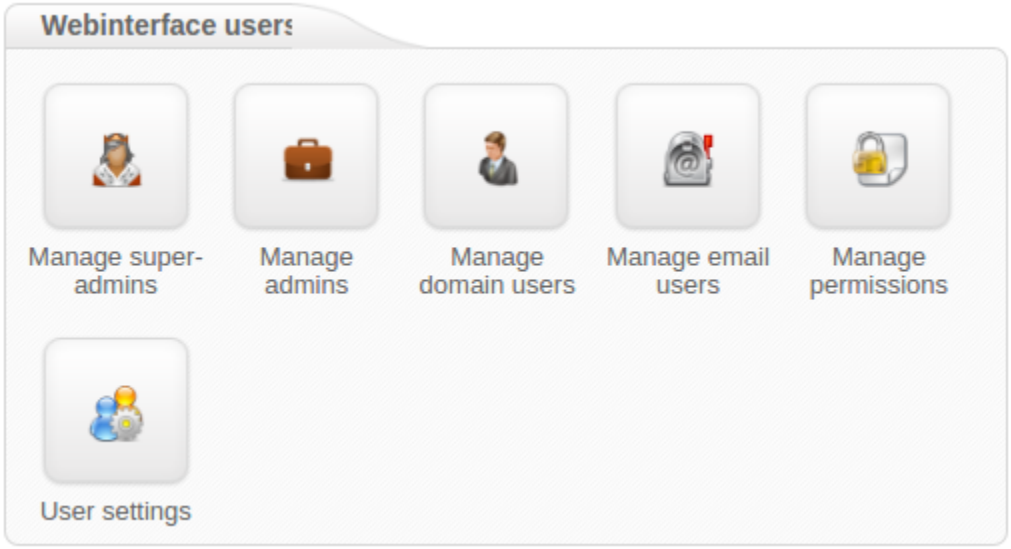
Email Size Restriction (default)



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.

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

Webinterface Users

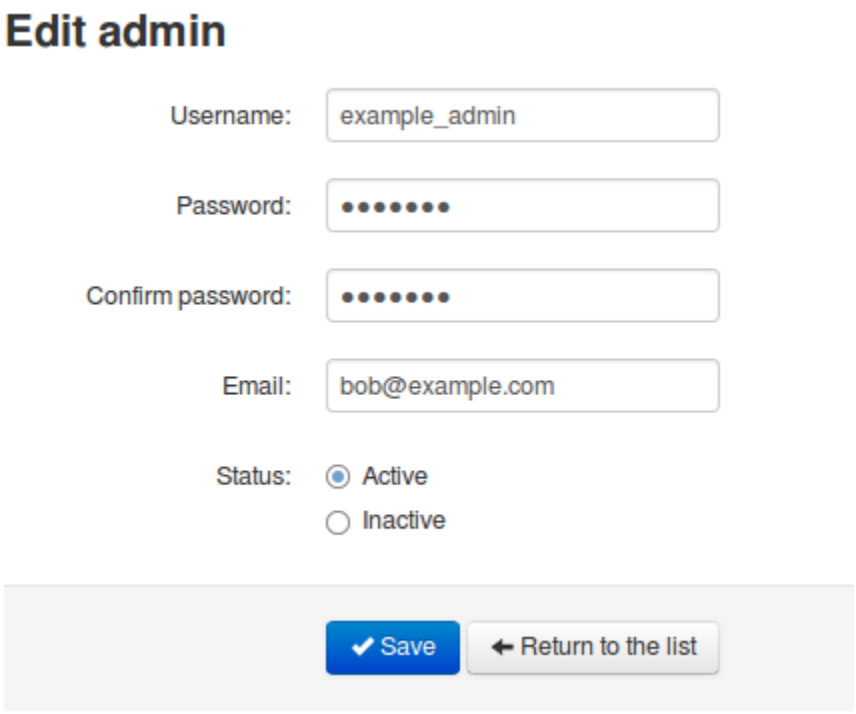


- Manage Super Administrators
- Manage Administrators
- Manage Domain Users
- Manage Email Users
- Manage Permissions
- User Settings

Manage Super Administrators

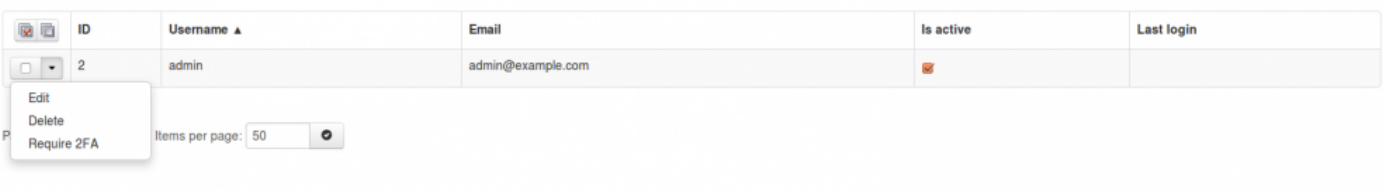
With this option you can manage who has super-administrator access to the SpamExperts Control Panel. You can either add the super-administrator(s) one by one via the **Add** button or you can **Upload a Comma Separated Values (CSV) file** to add multiple users at once. Each line in the file must contain at least four columns, the username, the password, the email and the status.

Please ensure when setting the password, that it contains lower case letters, at least one upper case letter or one digit, no spaces, and is 6-25 characters in length.



If you select an Administrator in ‘Manage Administrators’ and press the drop-down black arrow you have several options such as:

- Edit Administrator
- Delete Administrator
- Require 2FA



With Require 2FA a Super-Administrator, Administrator or Domain user can require specific users, or all users, to use 2-factor authentication. 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.

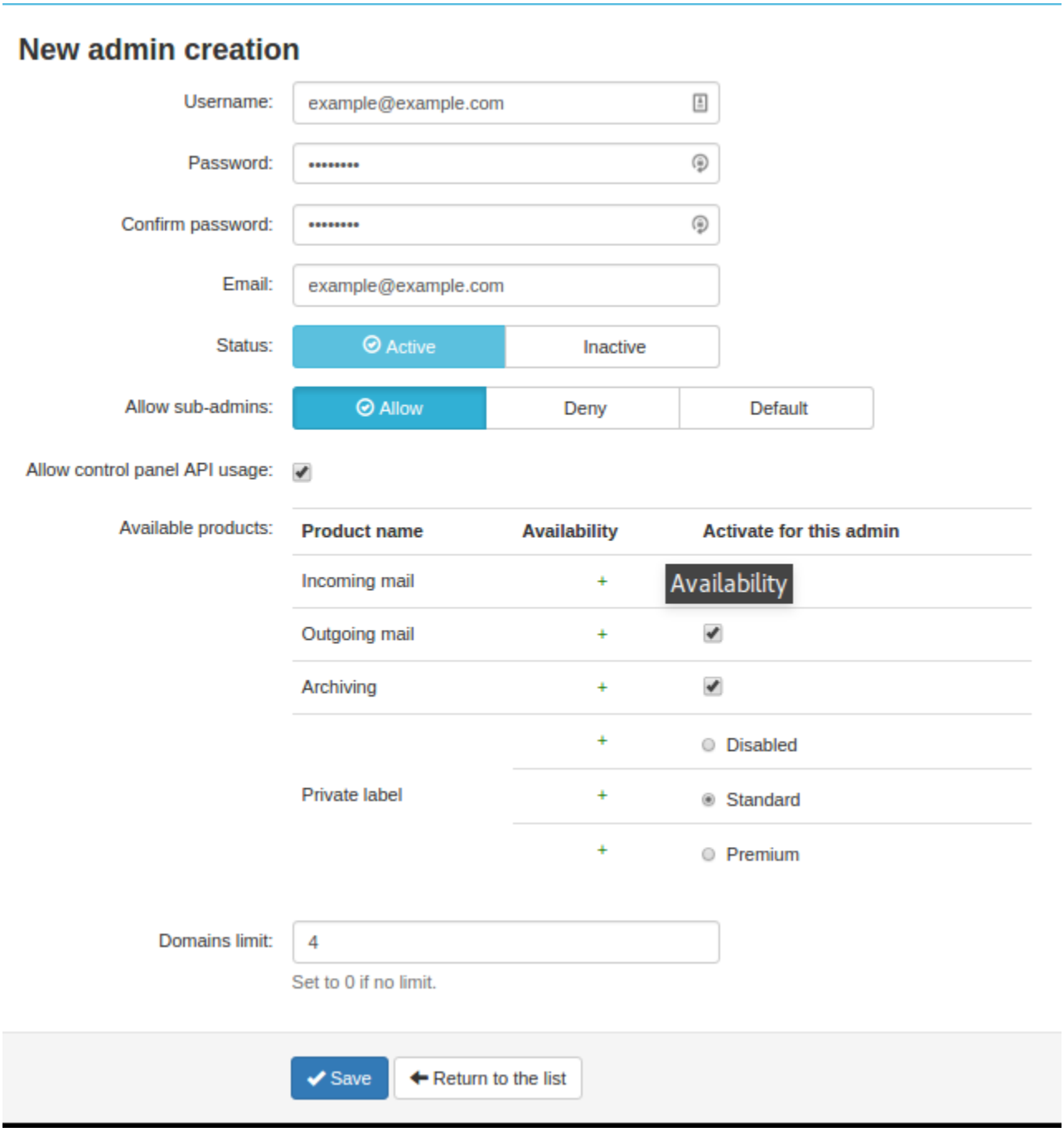
In the Control Panel – 'Manage Super-Admins' page you can set each Super-Administrator's status as Active/Inactive or you can also view the last login date of each admin.

Manage Administrators

With this option you can manage your Administrators to have access to the Control Panel and configure their specified products and services.

You are able to set the following options and services per administrator:

- Incoming mail
- Outgoing mail
- Archiving
- Private label
- Domain Limits
- Control Panel API usage
- Allow Sub-admins

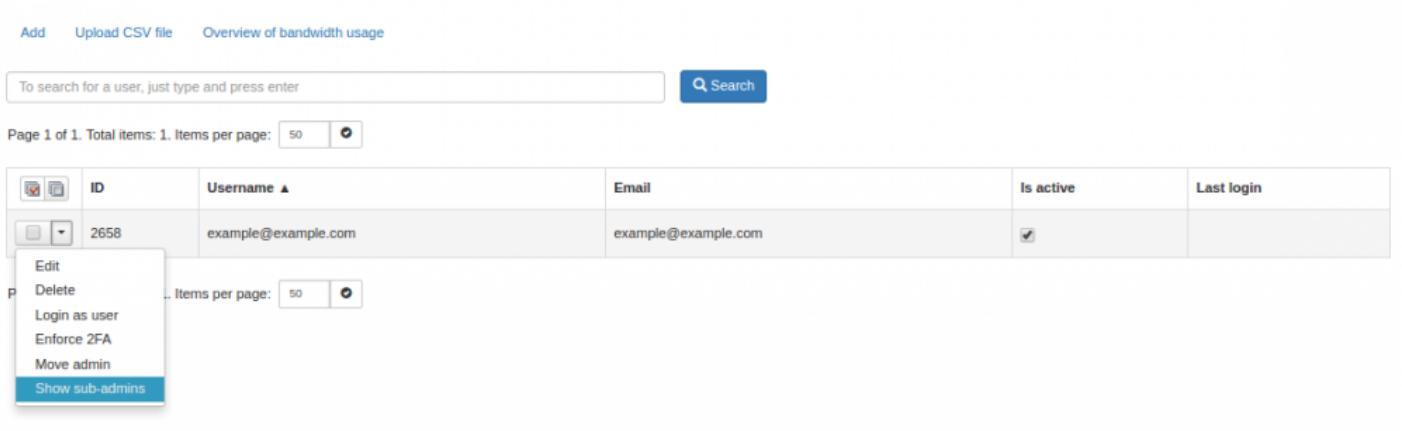


You can either add the Administrator(s) one by one – Add button or you can upload a Comma Separated Values (CSV) file to add multiple users at once. Each line in the CSV file must contain at least four columns, the username, the password, the email, the status and the domain's limit (domain's limit should be set to 0 if there is no limit).

Please ensure that when setting the password, the password contains lower case letters, at least one upper case letter or one digit, no spaces, and is between 6-25 characters in length.

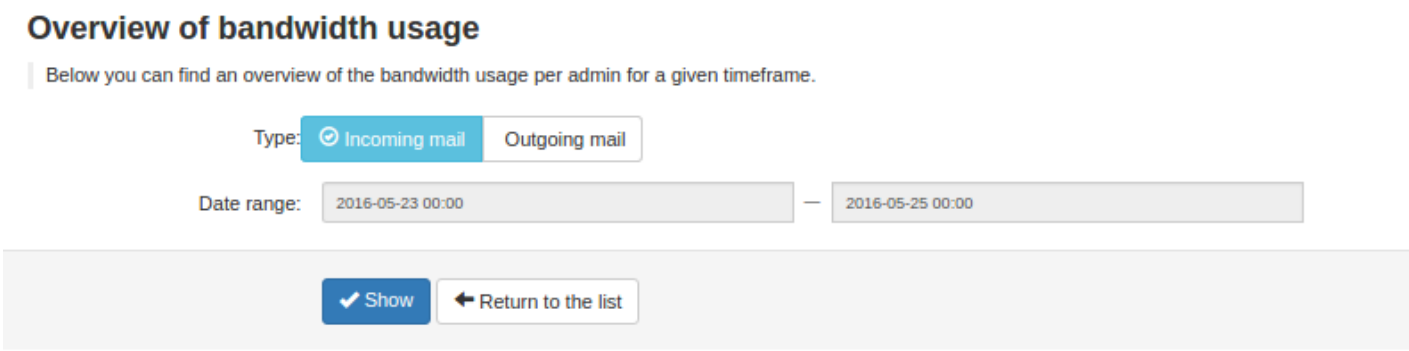
If you select an Administrator and choose the drop-down arrow you have several options such as:

- Edit Administrator
- Delete Administrator
- Login as Administrator
- Require 2FA
- Bind Domains to this Administrator (you can bind/unbind domains to the selected Re-Seller)



With Require 2FA a Super Administrator or Administrator 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.

At the top of the page there is an option "Overview of bandwidth usage" where you can find an overview of the bandwidth usage for incoming/outgoing email per admin for a given time-frame.



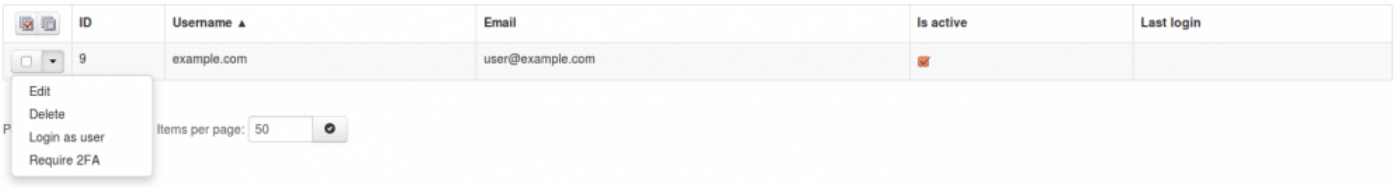
Manage Domain Users

With this function you can manage the domain users. These users can login using their domain and the set password to manage their domain specific settings.You can either add individual users or multiple users at a time by uploading a CSV file.

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.

If you select a Domain user and choose the drop-down arrow you have several options such as:

- Edit Domain user
- Delete Domain user
- Login as Domain user
- Require 2FA



With Require 2FA an Administrator 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.

> **!** Be Advised: When deleting a user, please ensure you remove the domain also. If it is not possible to remove the domain, then change the status of the user to inactive.

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.

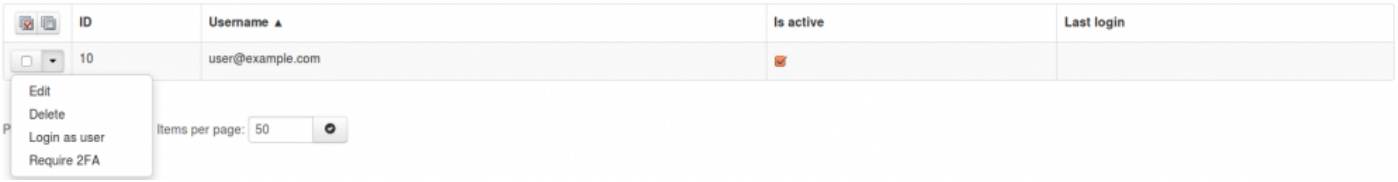
You may also upload a Comma Separated Values (CSV) file. Each line in the file must contain at least four columns, the username, the domain, the password and the status.

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

User Settings

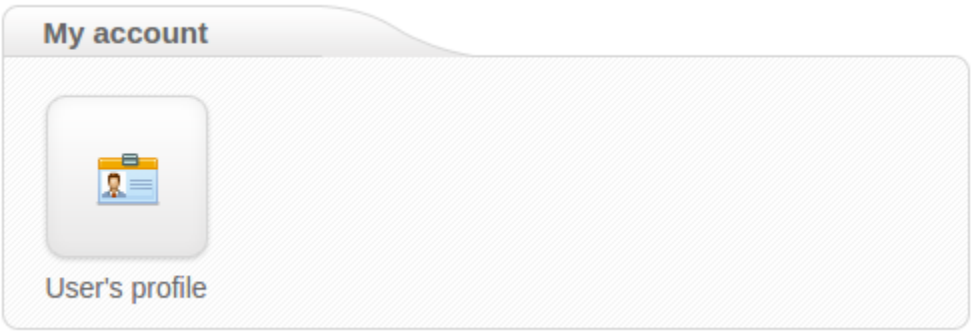
On this page you have the option to configure the global password policy for all your users.

You can customize the following elements of the password policy:

- Minimum number of characters
- Minimum number of digits
- Minimum number of lowercase characters
- Minimum number of uppercase characters
- Minimum number of punctuation characters
- Allow spaces
- Allow dictionary words

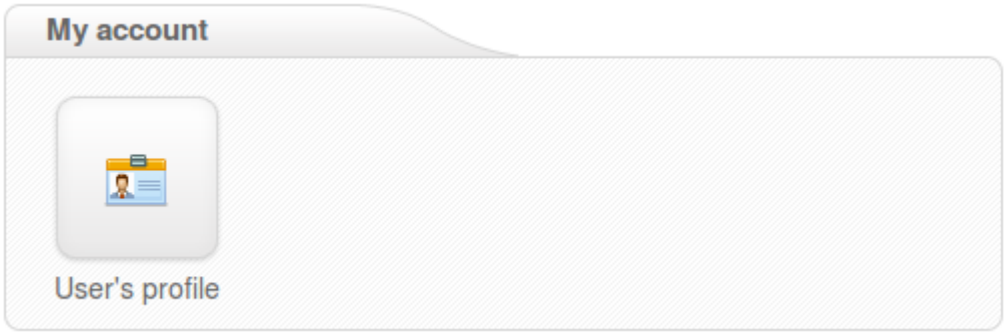
As a Super-Admin you also have the option to enforce Two-Factor Authentication (2FA) for user types, such as super-admins, admins, domain users or email users.

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.