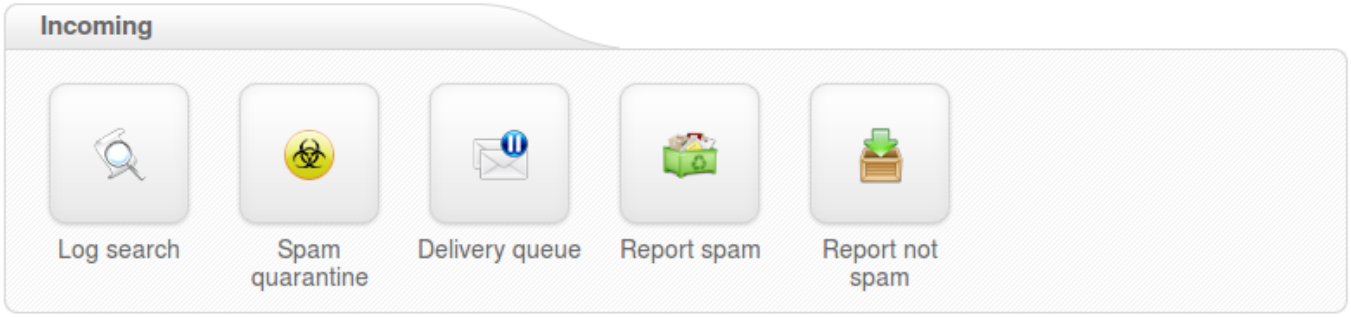
SpamExperts Control Panel Email User Level

1 — Last update: 2016/07/12

SpamExperts

Table of Contents

Incoming



- Incoming Log Search
- Incoming Spam Quarantine
- Delivery Queue
- Report Spam
- Report Non-Spam

Incoming Log Search

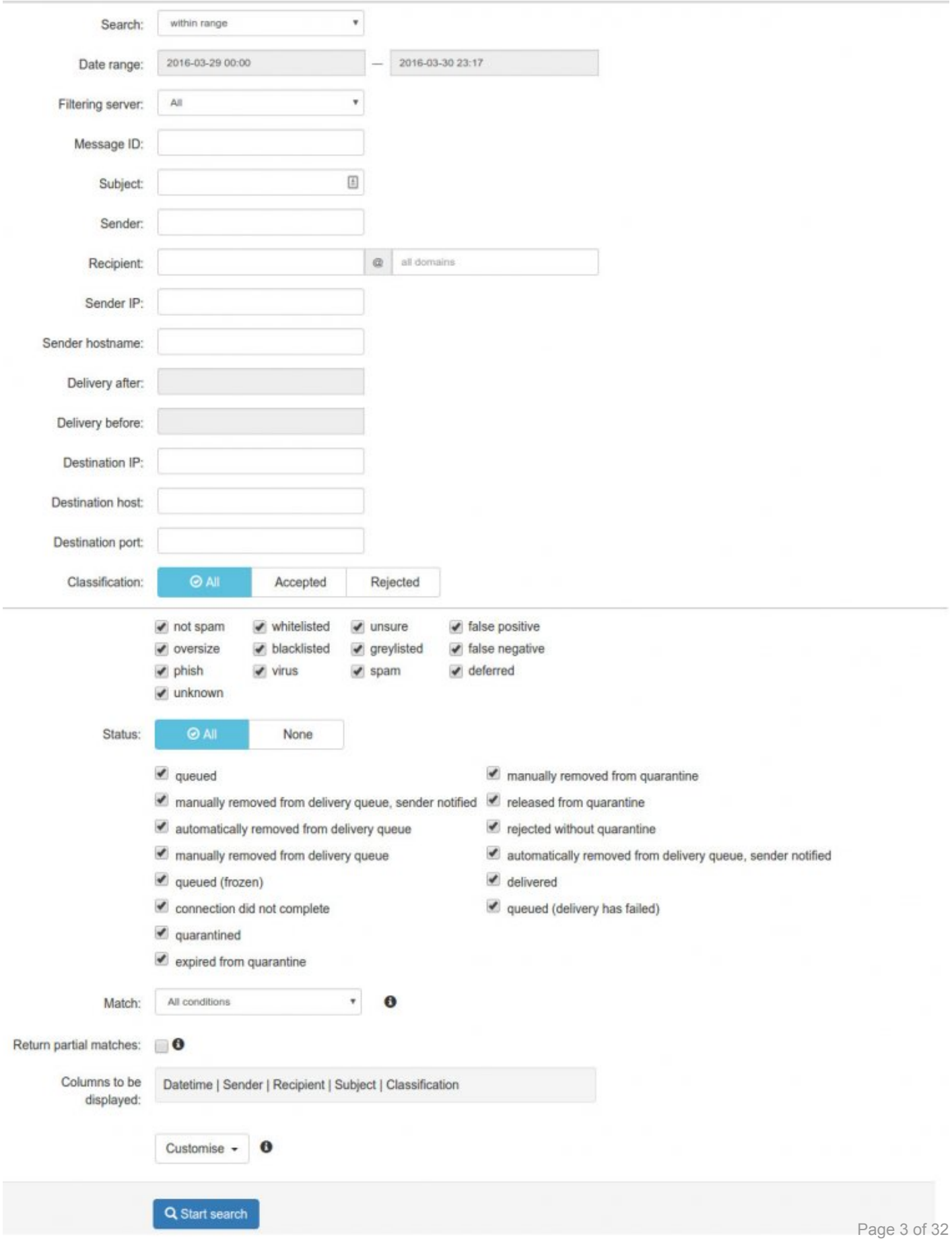
On this page you can view the log of messages that are received, blocked and temporarily rejected.

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.

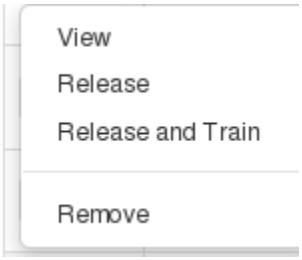
Delay

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 Spam Quarantine

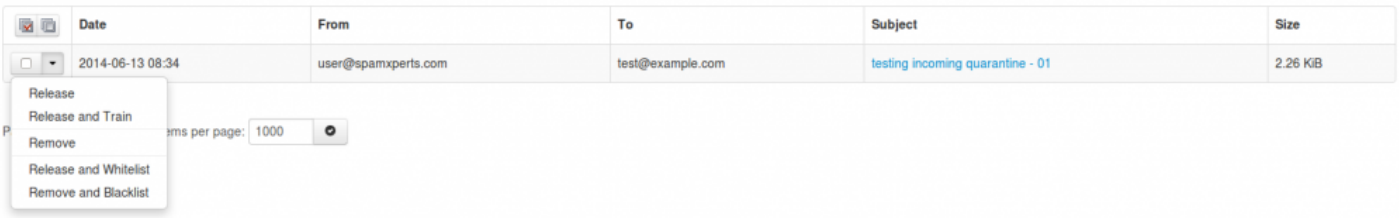
The Spam quarantine interface displays all the incoming quarantined messages.

> * 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.

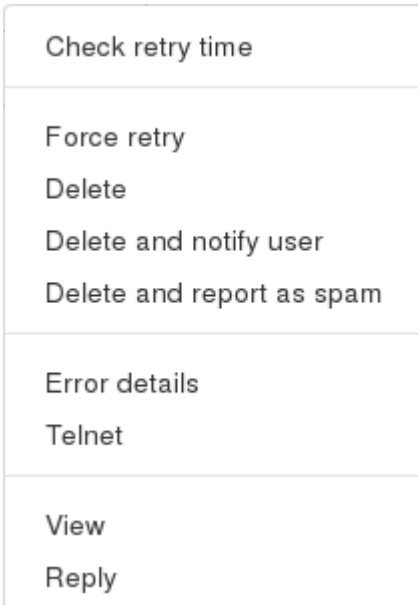
If an attachment is included in the quarantined message, then this can be individually downloaded by clicking on the **'Attachment:'** line in the normal view.

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.

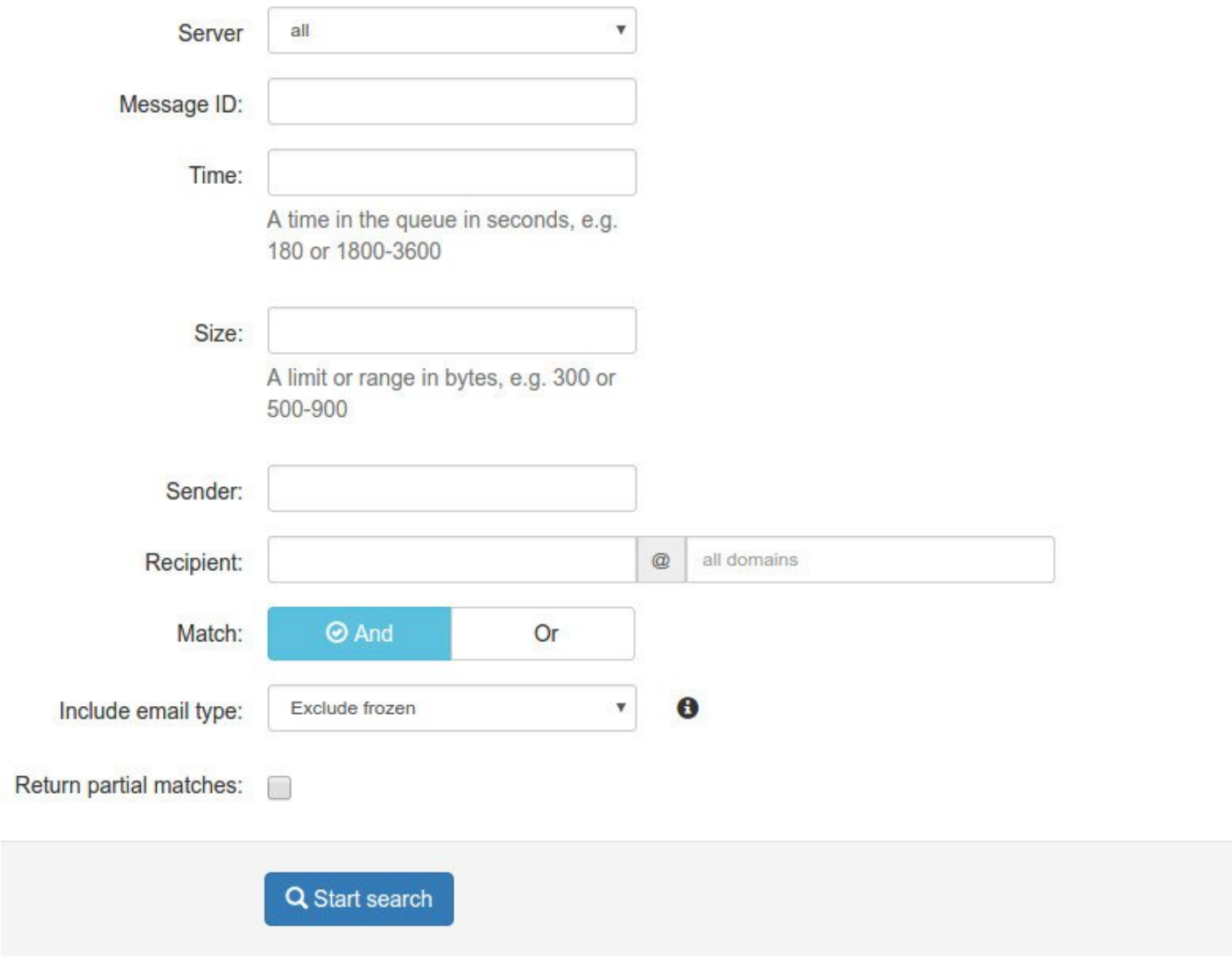
We have also reintroduced the option ‘Error details’ to check the reason why messages are stored in Delivery Queue.

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.

Report Spam

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

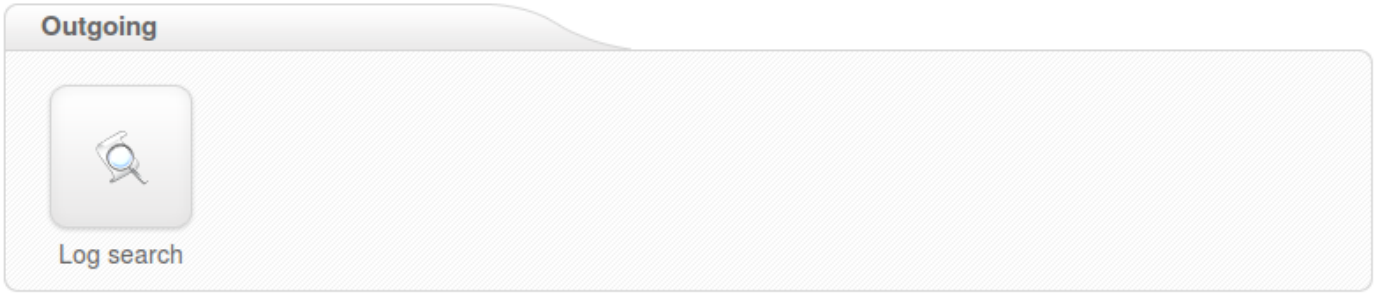
The emails should be in **.eml**, **.txt** or **.msg** format and it must contain the full headers, including the SpamExperts additional headers.

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.

Outgoing



- Outgoing Log Search

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.

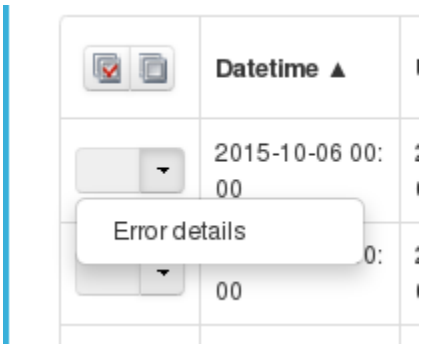
Delay

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.

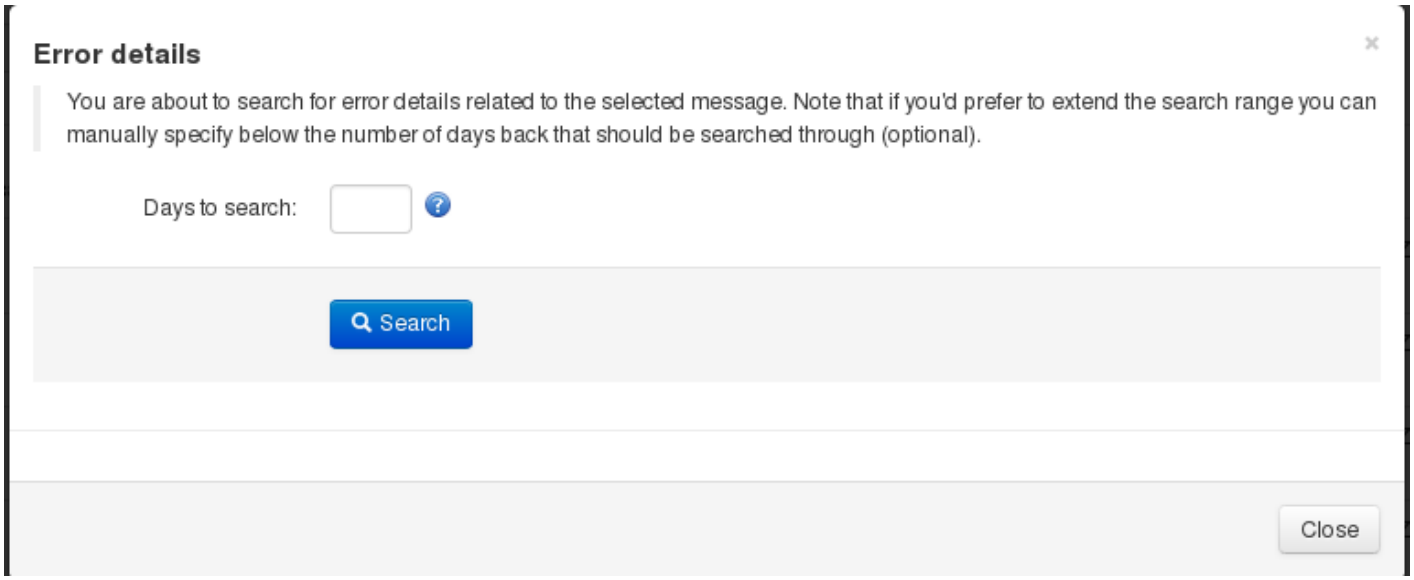
Information logged

- 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.

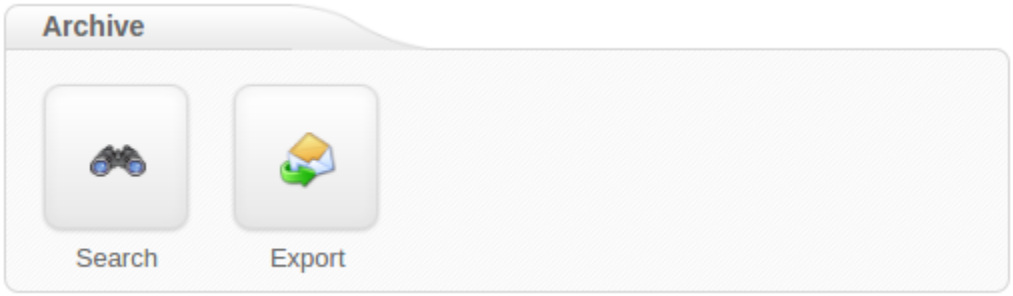


Here you can manually specify the number of days that should be searched through, starting from 1 and up to 31.



! 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.

Archive



- Search
- 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).

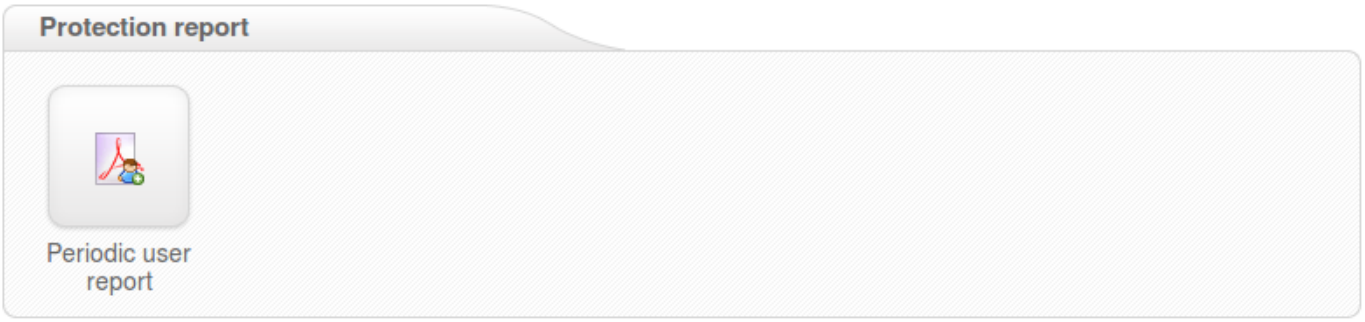
For example, a query that uses all of these operators is: ‘(cat -dog) | (cat -mouse)’. This will find messages that include ‘cat’, but not ‘dog’ or messages that include ‘cat’, but not ‘mouse’.

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

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.

Protection Report



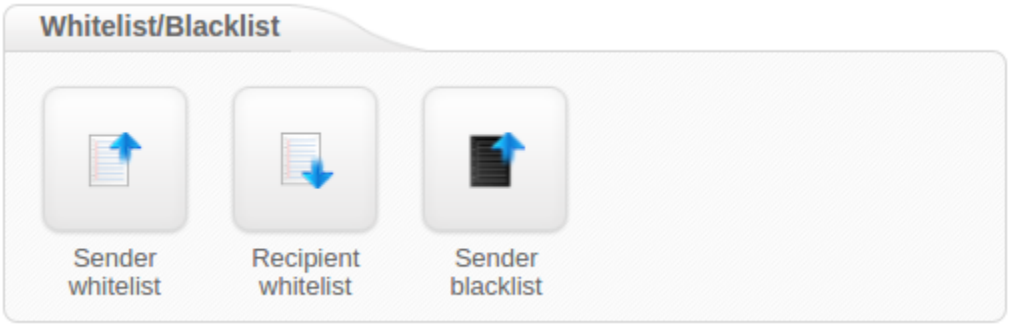
- Periodic User Report

Periodic User Report

As email user here you can enable **Periodic Protection Reports** for your account if it's not already enabled, and configure the email address where the report should be sent.

To enable the **Periodic User Report**, click the "**Add a recipient**" button, and configure the email address that will receive the periodic user report, frequency, language, format and click "**Enable**".

Whitelist / Blacklist



- Sender Whitelist
- Recipient Whitelist
- Sender Blacklist

Sender Whitelist

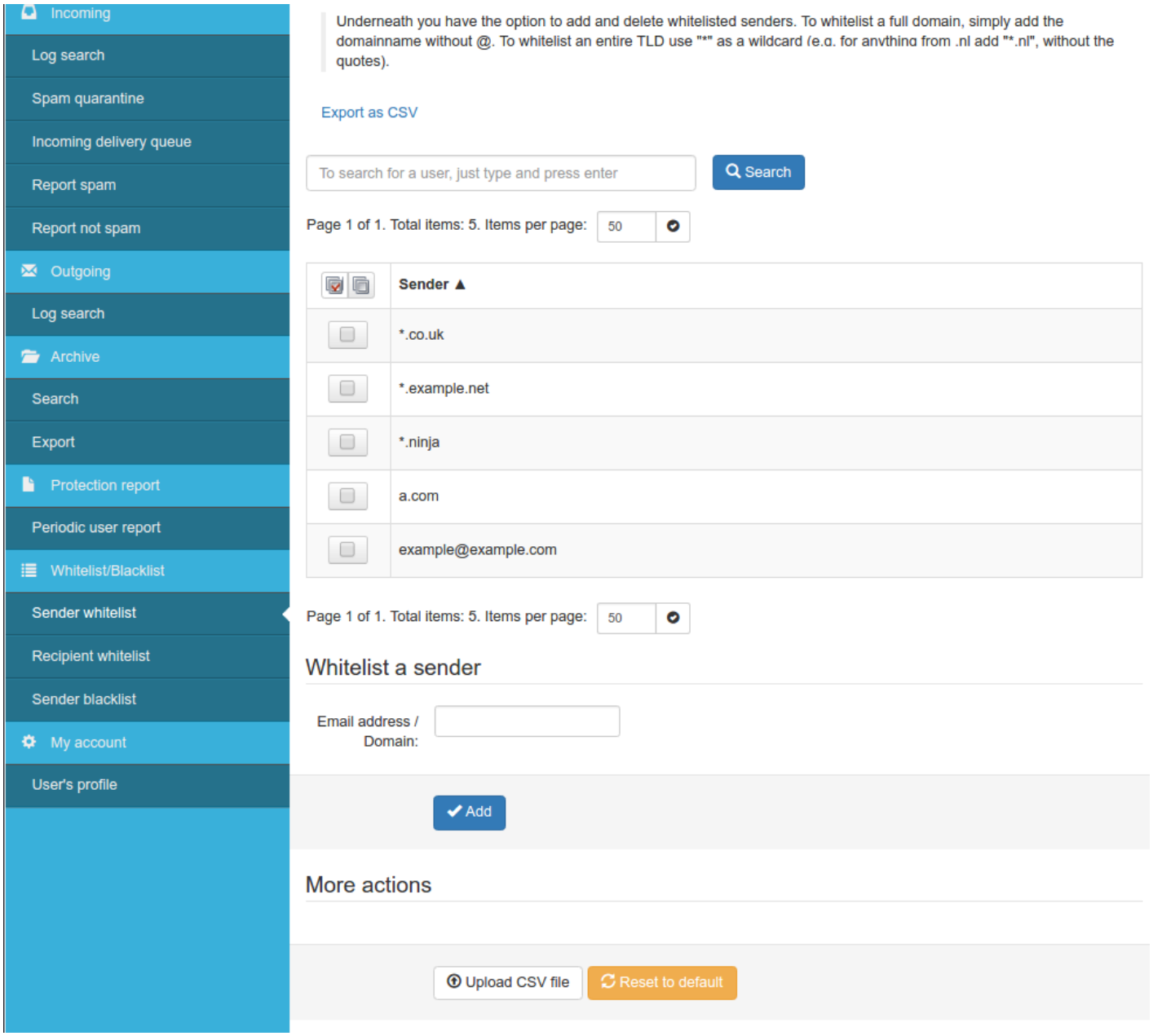
* Whitelisting the sender(s) at this section will apply to all the users on this domain when logged in as domain user.

* 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.

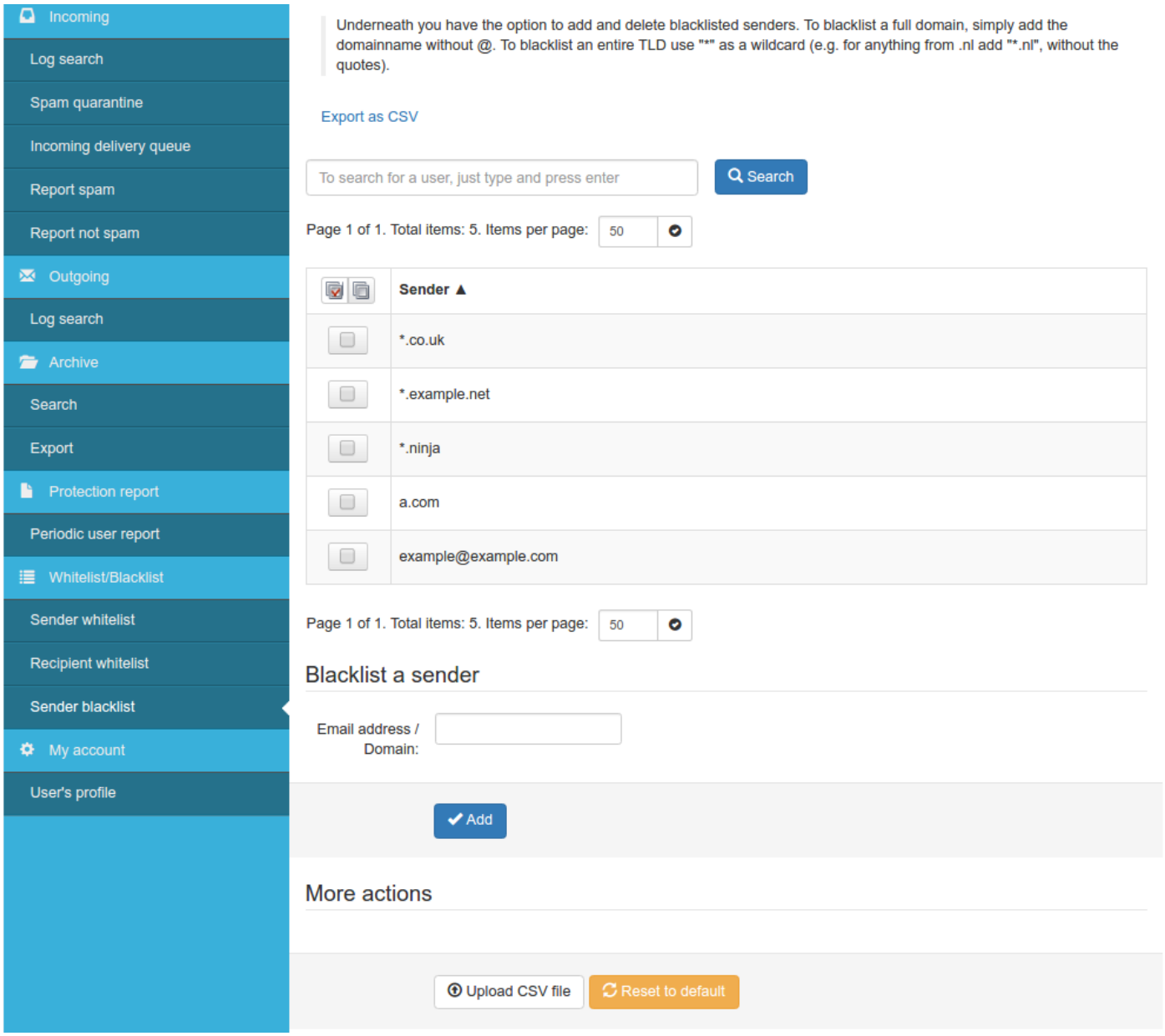
* Blacklisting the sender(s) at email user level will apply and is limited to all accounts or domains that send emails to that specific email user address.

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.

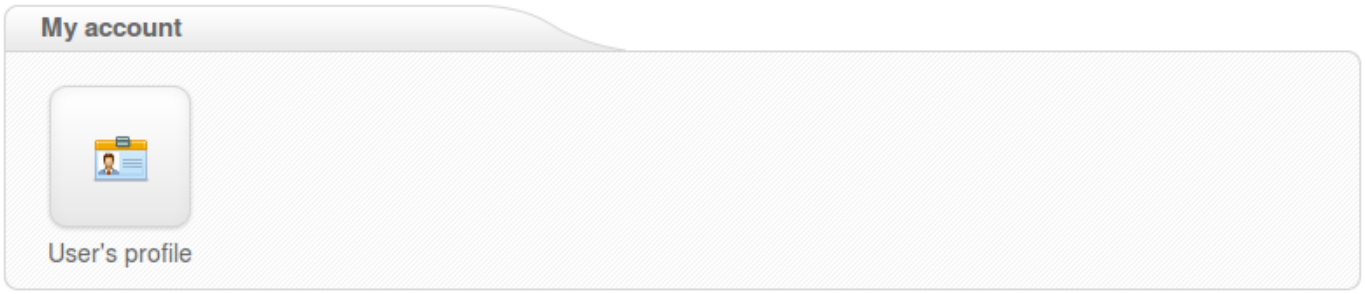
You can blacklist a specific sending email address, or a full sending domain. To blacklist all senders from a domain, you should only enter the domain (without @). You can also use the wildcard support to blacklist a whole TLD, such as "*.net".



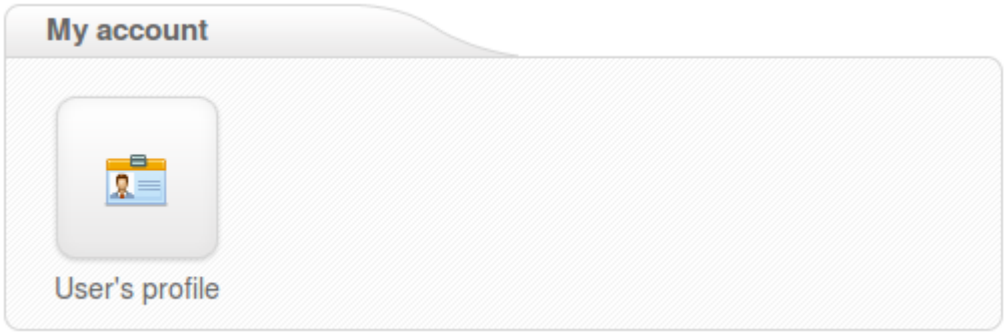
You can upload a Comma Separated Values (CSV) file to add multiple blacklisted senders at once. Each line in the file must contain one column: **emailaddress**. Example CSV file content:

user1@example.com
user2@otherexample.com
example.net

My Account



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.