SpamPanel Email Level

Manual

Version 1 — Last update: March 21, 2014

Table of Contents

Incoming

- [Incoming Spam Quarantine](#)
- [Incoming Log Search](#)
- [Delivery Queue](#)
- [Report Non-Spam](#)
- [Report Spam](#)

Incoming Spam Quarantine

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

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

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

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

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

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 header.

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

Selecting the 'release' button from this page will release this specific message from the quarantine and deliver it to the intended recipient.

Incoming Log Search

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

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

You can search on various strings and options, including, sender, recipient, subject and sender IP.

Date range:	2/25/14 00:00 — 2/27/14 00:00
Message ID:	
Subject:	
Sender:	
Recipient:	@ example.com
Sender IP:	
Sender host:	
Match:	All conditions
Classification:	all
Return partial matches:	☐
Include results from the last minutes:	☐ ❓

Storage period

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

Access

The logs can be easily downloaded or searched from the webinterface.

Delay

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

Information logged

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

It's possible to view the "delivery status" and the "error details" of the message by using the drop down box on the specific message line.
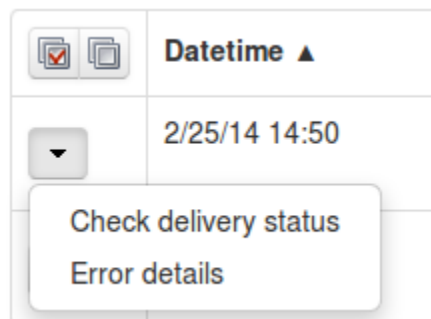
Messages that say 'Accepted' have not necessarily been delivered, it means the message has been accepted for delivery. If immediate delivery fails, the message will be automatically retried. If the destination server rejects the email, a bounce will be generated to the sender.

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

Delivery Queue

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

On this page you have several options:

- Retry to delivery all messages
- View Message
- Delete Message
- Delete and Report as Spam
- Force retry individual message
- Check the Queue Reason
- Check the Retry Time
- Search for messages

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

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

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

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

Server	all ▾

Message ID:	

Time:	

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

Size:	

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

Sender:	alice@example.com

Recipient:	bob@example.com

Match:	⦿ And
	○ Or

Return partial matches:	☐

🔍 Start search

Report Non-Spam

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

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

Report Spam

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

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

Outgoing

- [Outgoing Log Search](#)

Outgoing Log Search

All email connections (spam and not spam) to a domain are logged to the logging server. To make sure a connection can be logged, the "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 ratelimiting is applied because of a flood of connections from a certain IP, or when the sending server is violating certain requirements from the RFC 5321.

Storage period

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

Access

The logs can be easily downloaded or searched from the webinterface.

Delay

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

Information logged

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

> 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.

Archive

- [Search](#)

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 perfomance 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.

Protection Report

- [Periodic User Report](#)

Periodic User Report

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

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

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

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

Whitelist / Blacklist

- [Recipeint Whitelist](#)

Recipient Whitelist

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

To whitelist a specific recipient address, the local part of the address should be entered. For example if your domain is example.com and you add "nofilter" to the recipient whitelist, all emails sent to nofilter@example.com will not be scanned for spam/viruses. To whitelist all recipients for a domain (so all emails sent to the domain are not scanned/blocked), you can enter the wildcard "*" for the local part.

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

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

My Account

User Profile

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

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

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