

Mail Assure

Email Level User Guide

CONTENTS

Introduction	1
Accessing Mail Assure	1
Using the Log Search	2
Managing the Spam Quarantine	4
Spam Report Email	6
Searching and Restoring from the Archive	9
Archived Email - Bulk Export	9
Managing the Incoming Whitelist and Blacklist	10
View Whitelisted/Blacklisted Senders	10
Add a Sender to the Whitelist or Blacklist	10
Using Webmail when your Mail Server is Down	12
Incoming Delivery Queue	12
Compose Email	12
Network Tools	14
SMTP Tab	14
Manage your Email User Profile	17



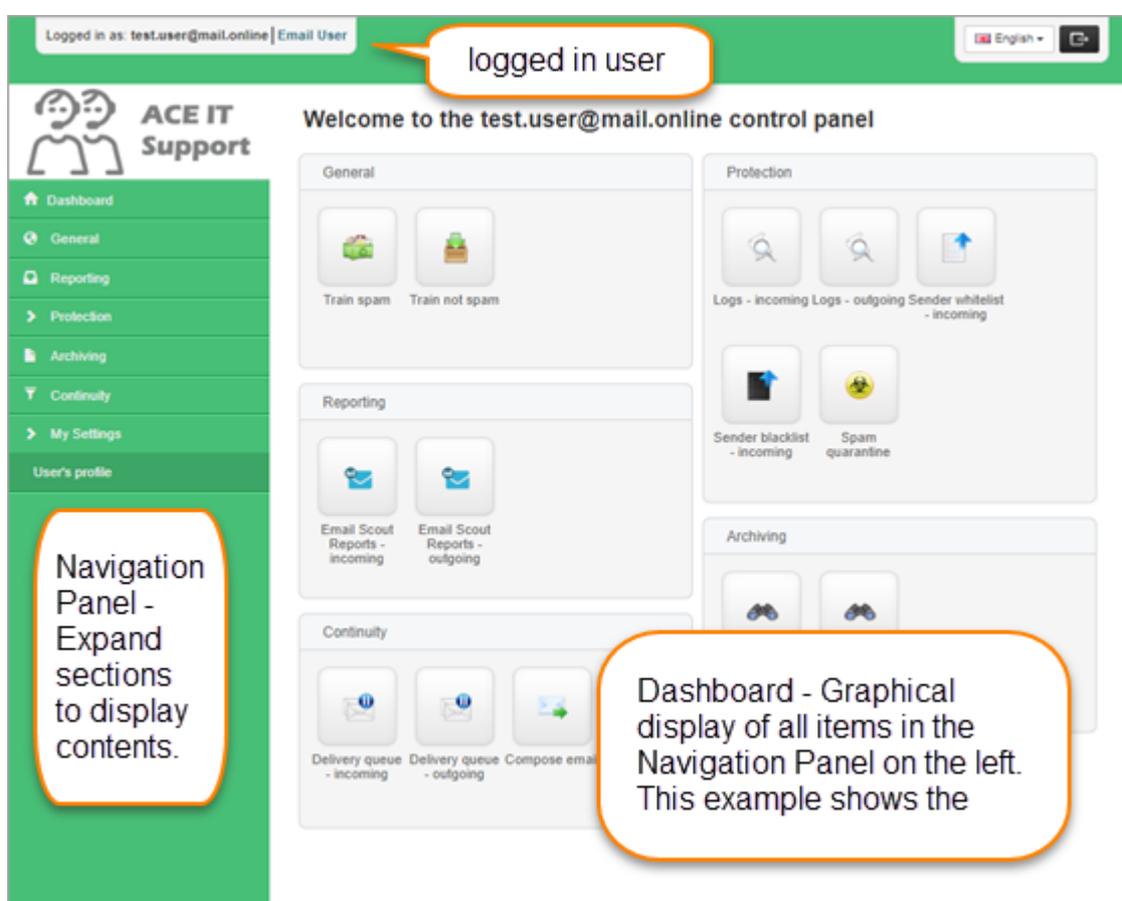
Introduction

This Email Level User Guide describes how you can access the Mail Assure application as an Email Level user - and then go on to perform a variety of tasks including searching for and reporting on specific mail and viewing the spam quarantine.

Accessing Mail Assure

Using the link supplied by your administrator, log into the application using your email address and password.

i If you have forgotten your password or want to add yourself as a Mail Assure user, use the [Retrieve log-in link](#) in the Login page.



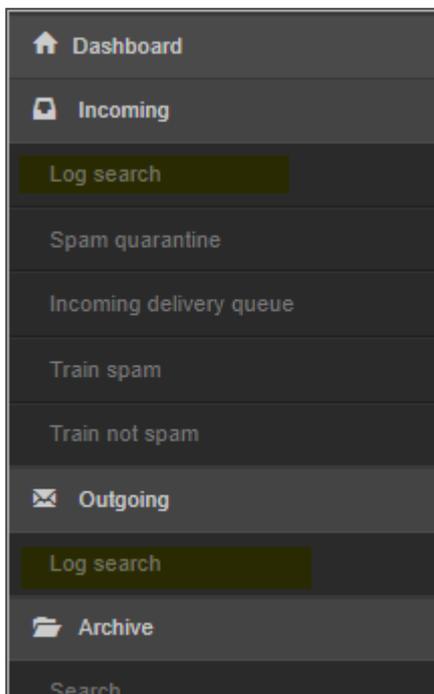
Click on the links in the Navigation panel to expand menu items - and navigate to the relevant section within the application.

Using the Log Search

The Log Search feature allows you to search for, view and report on incoming and outgoing mail that you have sent or received in the previous 32 days.

1. To search logs for incoming mail select **Incoming > Logs**.

Alternatively, to search logs for outgoing mail select **Outgoing > Logs**.



2. Use the **Query Rules** panel to filter your search. Add more queries by clicking on **+ New rule** and select from the filter options available
3. Click **Show Results** to run your search.

A list of emails matching your specified filters is displayed at the bottom of the page, with information on each individual email including sender, delivery status etc.

Using the dropdown to the left of each email, you can perform various actions depending on the message classification. For example, if an email has been placed in the quarantine, you can view, release, release and train, and remove using the dropdown menu to the left of the email.

	Message ID	Timestamp	Sender	Main class	Subject	Status
	1fy9nm-0000 Fm-KG	2018-09-07 06:59		whitelisted	Ace IT Support Report: 20180906 - 20180907 (training.g.co.uk)	delivered
		3-09-06 1		whitelisted	Quarantine Report for (training.co.uk, 2018-09-06 14:01:03.835412)	delivered
		3-09-06 5		unsure	test Thu, 06 Sep 2018 11:45:00 +0100	delivered
		3-09-06 6		unsure	test Thu, 06 Sep 2018 11:06:23 +0100	delivered
		3-09-06 0		unsure	test Thu, 06 Sep 2018 11:00:24 +0100	delivered
		3-09-06 9		unsure	test Thu, 06 Sep 2018 10:58:46 +0100	delivered
		3-09-06 7		unsure	test Thu, 06 Sep 2018 10:57:56 +0100	delivered
	1fxr20-0003Y M-2a	2018-09-06 10:56		phish	test Thu, 06 Sep 2018 10:56:48 +0100	quarantined-expired
	1fxr17-0003q e-EU	2018-09-06 10:56	test@test.com	spam	test Thu, 06 Sep 2018 10:55:51 +0100	quarantined-expired

Alternatively, click in the **Subject** column to open the **Mail Preview** page where you can also perform the same actions on the message and view the message content.

Mail Preview

Normal Plain Raw

Redeliver archived message More actions

Train as spam

Download archived message

Telnet SMTP test

Sender callout

Recipient callout

Whitelist sender

Blacklist sender

Delivery history

Compose Reply

Export as .CSV

from: no-reply@mail.online
to: rice@training.co.uk

Quarantine Report for rice@training.co.uk, 2018-09-06 14:01:03.835412

Sample Report
Ace IT Support

Scout Reports for training.co.uk

Report name: Automatic quarantine report at 14:00 GMT

Report entries: 3

From	Subject
test@test.com	test Thu, 06 Sep 2018 10:56:48 +0100
test@test.com	test Thu, 06 Sep 2018 10:55:51 +0100
test@test.com	test Thu, 06 Sep 2018 10:54:32 +0100

If you no longer wish to receive this automatic report, click here to unsubscribe.

Close

Managing the Spam Quarantine

Access the Spam quarantine to view incoming messages that have been blocked and stored as spam.

As well as being able to access quarantined messages from the Log Search (described in [Using the Log Search](#)), you can also access them directly from the Spam Quarantine:

Select **Protection > Spam quarantine**.

The **Log Search** page is displayed, listing all messages that have been quarantined:

The screenshot shows the 'Log Search' interface. At the top, there is a title 'Log Search ([redacted])' and a descriptive paragraph. Below this is a link 'Export entries as CSV' and a button 'Email me this report'. The main section is 'Query Rules', which includes a dropdown for 'Status' set to 'Quarantined', a dropdown for 'is one of', and a search input field. Below the query rules are options for '+ New rule' and 'Reset rules'. There are also sections for 'Group results by:' and 'Columns to be displayed:'. At the bottom, there is a table with one row of results.

Log Search ([redacted])

All connections that are handled by the filter (other than when the filter is disabled, and those handled by denial of service protection) result in a log entry that records meta-data about the message, its classification, and what happened to it. This information is kept for a period of time controllable at the domain level, and is then purged. There is a short delay, typically well under 10 minutes, before log entries are available here.

[Export entries as CSV](#)

Email me this report

Query Rules

Status is one of

Quick select: [Accepted](#), [Not accepted](#)

+ New rule ✕ Reset rules

Group results by: Columns to be displayed: [Show Results](#)

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

<input type="checkbox"/>	Timestamp	From	To	Subject
<input type="checkbox"/>	2018-07-27 13:01		[redacted]	test Fri, 27 Jul 2018 13:01:31 +0100

In this page you can:

- Search for a quarantined message - Use the **Query Rules** filter at the top of the page.
- Empty spam quarantine - Click on the **Empty spam quarantine** button at the top right of the page.

- Perform actions on individual emails - Use the dropdown to the left of each email to choose from the following actions:
 - Remove from quarantine - Remove messages from the system completely.
 - Release from quarantine - Allow messages to be delivered to the recipient.
 - Release and train from quarantine - Allow messages to be delivered and train the system to recognize future messages from this sender as not spam.
 - Download quarantined message
 - Telnet SMTP test
 - Sender callout
 - Recipient callout
 - Whitelist sender
 - Blacklist sender
 - Whitelist recipient
 - Blacklist recipient
 - Delivery history
 - Compose Reply
 - View email
 - Change action for messages like this
 - Export as .CSV
- Preview quarantined message content - By clicking on the message link in the **Subject** column the **Mail preview** page opens displaying the message. In this page you can view the message in plain text or the original HTML format. You may also be able to perform the following actions:
 - Release quarantined messages - Allow messages to be delivered to the recipient.
 - Release and train messages - Allow messages to be delivered and train the system to recognize future messages from this sender as not spam.
 - Remove messages.
 - Download the message in .eml format

Spam Report Email

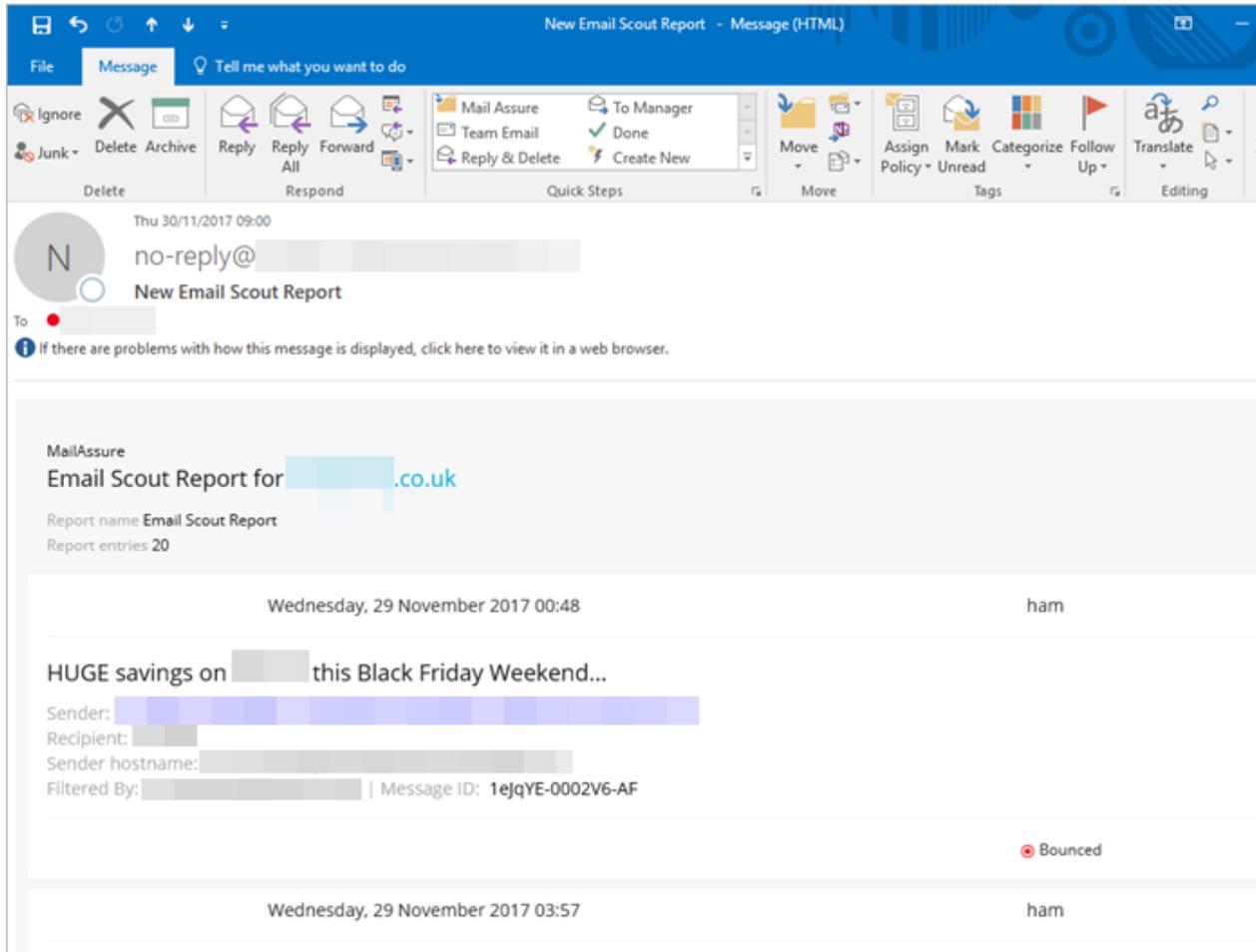
If you want to send a spam report to your email address you can configure this from the Log Search. You can choose to send the report straight-away, or you can schedule the report to be sent hourly, daily, weekly or monthly.

1. To set this up, go to **Incoming > Logs**.
2. In the **Classification** section, select 'spam' to search for spam.
3. Select **Start search** to run the search - all matching spam emails are listed.
4. Select **Email me this report**.
5. Select when you want the report delivered:
 - Right away
 - At given date - Select date and time you want the report to be emailed
 - Repeat - Select the name of the report, and the time and frequency the report will be sent (hourly, daily, weekly or monthly).

 All repeat reports that you create are known as Email Scout Reports and are listed in the page accessed by clicking the **Email Scout Reports** button.

6. In the **Subject** field enter the subject you that you wish to see in the subject line of the email.
7. In the **Sender** field, enter the name you wish to see as the sender of the email.
8. Click **Save**.

The email you receive contains a list of emails that match the report filters.



The subject line may contain a link. When clicked this will open a web page in your browser containing the message content which can be viewed in Plain text or Raw (which displays the message headers):



The **Available Actions** dropdown has the following options:

- Blacklist Sender
- Release
- Whitelist Sender
- Remove
- Release and Train - Releases the email for delivery and trains the system to recognize this message as NOT spam in the future
- Unsubscribe - unsubscribe from receiving this spam report

Searching and Restoring from the Archive

If you need to restore an email from your Archive, it is recommended that you use the Log Search facility described in [Using the Log Search](#).

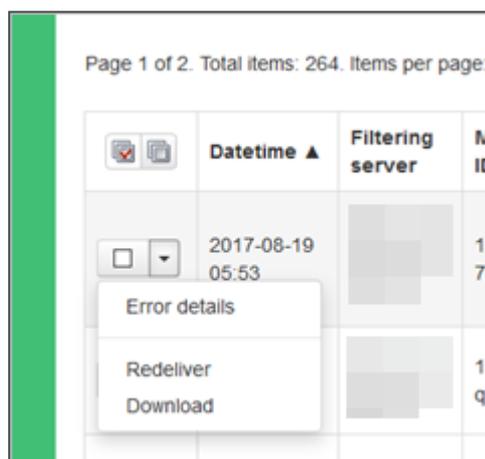
1. Select **Incoming > Logs**.
2. Use the filters available to search for specific messages.
3. Select the **Return only archived messages** option.
4. Click **Start search**.

All matching archived messages are listed at the bottom of the page.

If you want to preview the message, click in the **Subject** column to open the message in the **Mail preview** page.

i Archive users are able to preview every email in the delivery logs. Non-Archive users will only be able to preview quarantined emails.

5. Click on the dropdown to the left of the message and select **Redeliver** to redeliver the message to your mailbox or **Download** to download the individual message in a zipped archive.



Archived Email - Bulk Export

If you want to perform a bulk export of Archived messages:

1. Select **Archiving > Export**.
2. Specify the **Date range**.
3. Enter the destination email address in the **Destination email** field.
4. Click **Export**.

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

Managing the Incoming Whitelist and Blacklist

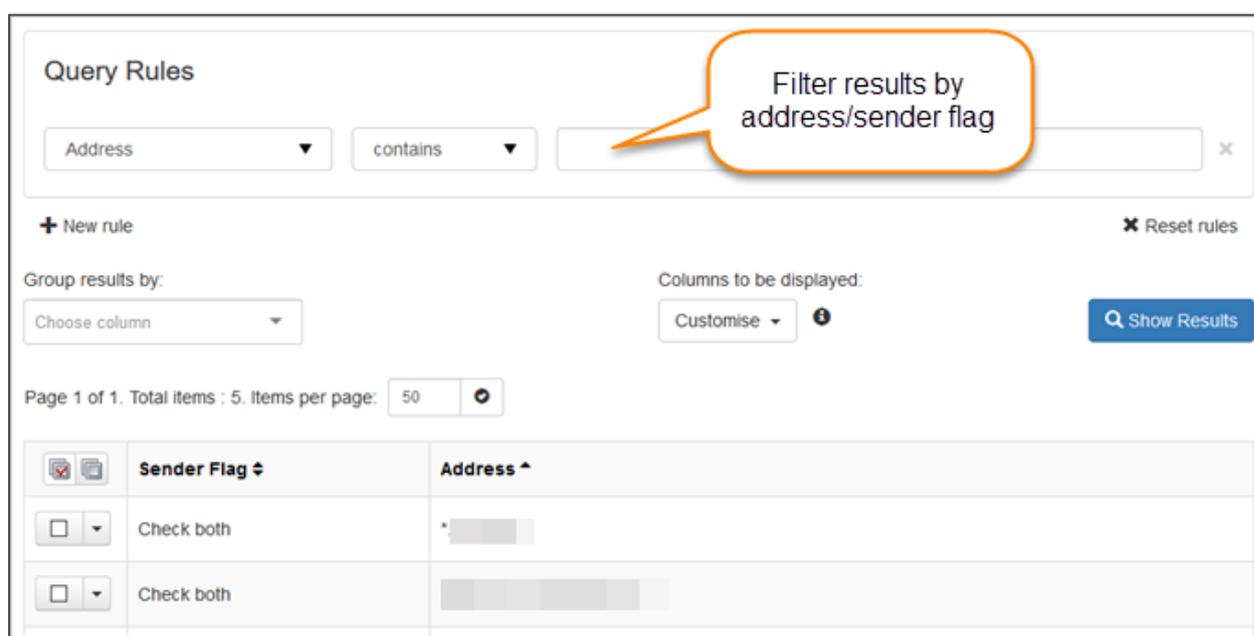
Use the Whitelist to list trusted email addresses. Incoming mail from whitelisted senders (which may normally be identified as spam) will always be allowed. Conversely, use the Blacklist to block incoming mail from known spammers.

You can whitelist/blacklist email addresses and domains.

View Whitelisted/Blacklisted Senders

To check which whitelist/blacklist rules are set up in your system:

1. Select **Protection > Sender whitelist - incoming** or **Protection > Sender blacklist - Incoming**.
2. Click on **Show Results** to display all listed senders.
3. To filter for specific whitelisted/blacklisted addresses, use the **Query Rules** panel to filter your search:



The screenshot shows the 'Query Rules' interface. At the top, there is a search bar with a dropdown menu set to 'Address', a 'contains' operator, and a text input field. A callout bubble points to the text input field with the text 'Filter results by address/sender flag'. Below the search bar, there are buttons for '+ New rule' and 'x Reset rules'. There are also dropdown menus for 'Group results by:' (set to 'Choose column') and 'Columns to be displayed:' (set to 'Customise'). A 'Show Results' button is visible. At the bottom, there is a table with two columns: 'Sender Flag' and 'Address'. The table contains two rows, both with 'Check both' in the 'Sender Flag' column and a redacted address in the 'Address' column. The page status is 'Page 1 of 1. Total items : 5. Items per page: 50'.

Add a Sender to the Whitelist or Blacklist

1. Select **Protection > Sender whitelist - incoming** to access the Whitelist or **Protection > Sender blacklist - Incoming** for the Blacklist.
2. Click on **+ Add whitelist sender** or **+Add blacklist sender** to open the relevant popup:

Add whitelist sender [X]

Sender Flag

Apply to Envelope Sender Apply to From: Address Apply to both

Address *

3. Choose which address you want to apply by selecting from the following **Sender Flags**:
 - Apply to Envelope Sender - The SMTP Envelope from address
 - Apply to From: Address - The MIME message address
 - Apply to both

i It is recommended that you select **Apply to both**. This will whitelist/blacklist the sender address at SMTP and email header level. For example, if a spammer tries to change the sender email address in an email, the system will be able to check the before and after address.

4. In the **Address** field, enter the email address or domain you want to whitelist/blacklist.
5. Click **Save**.

Using Webmail when your Mail Server is Down

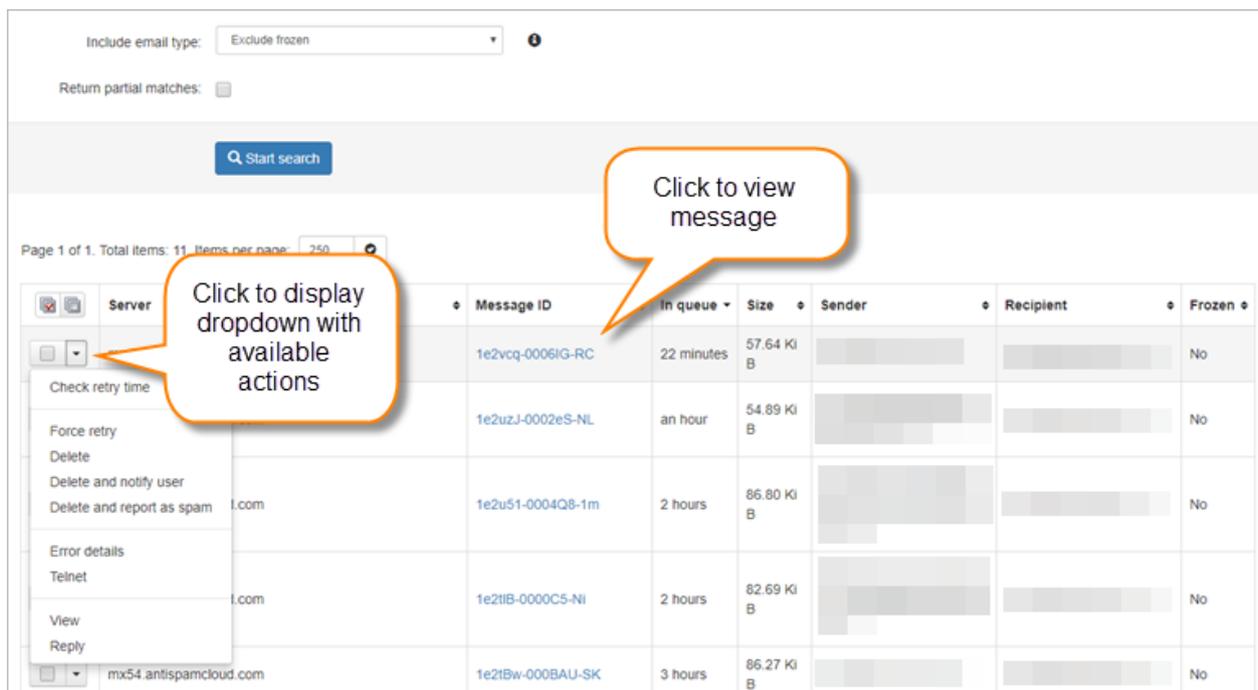
If you are having problems with your local mail environment and mail cannot be delivered to your mailbox, you can use the system's continuity functionality to continue working. There are two features available that allow you to do this:

- Incoming Delivery Queue
- Compose Email

Incoming Delivery Queue

The Incoming Delivery Queue stores emails that are not being accepted by the destination server (your mail server administrator should be able to check why these emails are not being accepted). The system stores these messages and attempts to re-deliver queued messages automatically for 14 days.

1. Select **Incoming > Incoming delivery queue**. to display a list of queued messages.
2. If you need to, use the filters to search for a specific email.
3. Click on the dropdown to the left of a message or click in the **Message ID** column to view or reply to a message:



Compose Email

Use the Compose Email feature to send emails when your mail server is down.

1. Select **Continuity > Compose email**.

Compose email ([redacted] .xyz)

You can add multiple recipients by typing an address and pressing enter to add another one

To Cc/Bcc

Subject

Message

Formats - A - A - B / E E E ■

■ ■ 🔗

Powered by TinyMCE

✓ Send Message ✕ Reset

2. Entered the recipient, subject and message content and click on **Send Message**.

Network Tools

The **Network tools** page allows you to test mail transfer using various tools:

- Ping - tests the reachability of hosts
- [SMTP Tab](#)
- Traceroute - Displays the route and transit time for connections between servers in the cluster and a specified destination
- Dig - Used to query Domain Name System (DNS) servers. You can query a specific name server or leave blank to use the Control Panel's default name server.

You can access this page from the Admin, Domain and Email Level Control Panels from **Continuity > Network Tools**.

SMTP Tab

Use the SMTP tab to test mail transfer using the SMTP protocol with the following checks:

- Sender callout - If you are seeing problems with sender verification, you can see exactly what the sender's mail server responds with when the address is checked.
- Recipient callout - If you are seeing delivery problems, you can see exactly what the destination's mail server responds with when the recipient is specified.
- Open relay check - You can see whether a mail server appears to be an "open relay", accepting mail for any destination.
- Catch-all check - You can see whether a mail server appears to be a "catch-all" for a specified domain, accepting mail for any address at that domain.
- Telnet test - You can check the full SMTP delivery process to a destination, to see exactly how the destination responds in answer to each of the SMTP commands, and the final message content. The tool will go as far as the information provided. If a recipient is not provided, then the connection will end after "MAIL FROM", and if a message is not provided, then the connection will end after "RCPT TO". If you have a message in the DATA section, this will send an email to the specified recipient.

To test deliverability issues from a specific server in the cluster, or IP assigned to a server, select the relevant IP. If left blank, then one of the control panel IPs will be used.

You can access this page from the Admin, Domain and Email Level Control Panels from **Continuity > Network Tools**.

The following fields/options are available:

Field/Option	Description
Hostname	You must either enter a server hostname here or enter the Envelope sender for any checks to run.
EHLO	Name of the EHLO/HELO that you want to use in the SMTP transaction.

Field/Option	Description
Envelope Sender	Enter the envelope sender to initiate a sender callout.
Envelope Recipient	<p>Enter the envelope recipient to initiate a recipient callout.</p> <p>Using the Catch all option you can see whether a mail server appears to be a 'catch-all' for a specified domain, accepting mail for any address at that domain.</p>
Data	If you want to send data to the envelope-recipient e.g. the content of the SMTP transaction and not just a callout.
Timeout, per SMTP command	How long you want the SMTP commands to last (e.g. for slower mta's there may be a need to set this higher before it times out)
Interface	Choose what IP you do the verification from. For example, if you want to do a sender verification check from a certain IP, choose the IP address from those available. If it is the default , then it uses the interfaces server IP/hostname (master.antispamcloud.com).
Prefer TLS	Try to use STARTTLS to perform the test over a secure connection.
Data only for Exchange servers	Some versions of Microsoft Exchange do not support doing a sender or recipient callout in the usual manner. If you select this option and the server appears to be a Microsoft Exchange Server, the tool will send a suitable test message in DATA. You should generally use this when doing a 'callout' check, but be aware that if the recipient is valid they will receive the test email message.

Field/Option	Description
	<p> If Data only for Exchange servers is unchecked, Default message is unchecked and there is nothing in the data part then no DATA is sent.</p>

Manage your Email User Profile

The **User Profile** page allows you to manage your profile settings.

From the Email Level Control Panel, select **My Settings > User profile**.

The **User's profile** page is displayed:

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.

Email:

This account is configured to use LDAP authentication so the option to change the password is not available

Features preview: Active Inactive

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 \(Windows Phone\)](#)

Notification

Send an email notification when your account is accessed from a new / different IP or location than usual.

From this page you can perform the following tasks:

- Change your password - You need your old password in order to do this.

i If LDAP authentication is configured, this option will not be available.

- Enable/disable the feature preview option which shows upcoming system features.

- Configure two step authentication - This enables a two step login process which entails entering a code as well as your username and password. Download the necessary app on your phone to generate the code you need:
 - [Download Google Authenticator \(Android/iPhone/Blackberry\)](#)
 - [Download Authenticator \(Windows Phone\)](#)
- Enable email notification when your account is accessed from a new location or IP address.

After making any changes, click **Save**.