

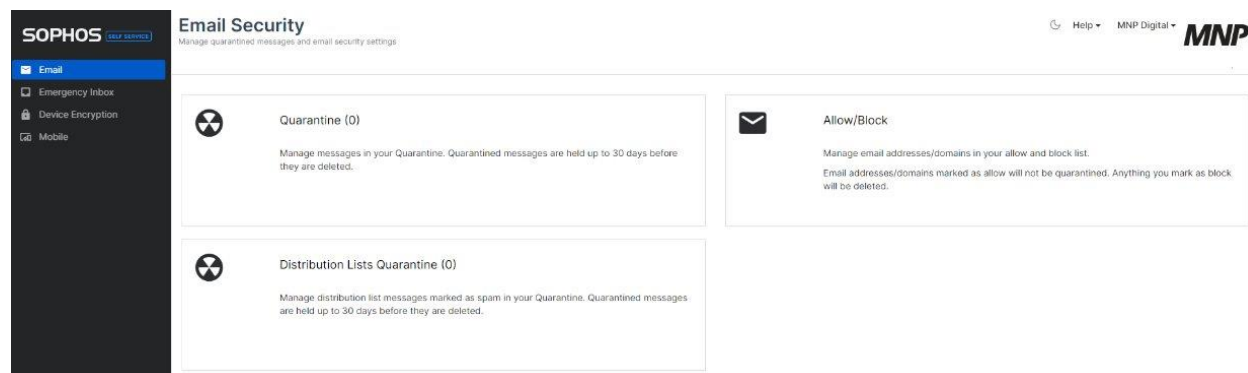
Email security tool

The MNP Digital Managed IT Services email security tool (powered by Sophos) is continuously working to block potential spam emails for you throughout the day. The following day you will receive an email listing the quarantined messages for your review. You also have the option to log into your Self-Service account, where you can view your quarantined messages and manage the allow/blocklists.

Account Setup and Access

You will receive an email invite to access your self-service account. Once set up, you can log in by navigating to <https://central.sophos.com/manage/self-service> or the [Managed Services Client Centre](#).

Below is what you'll see once you log in.

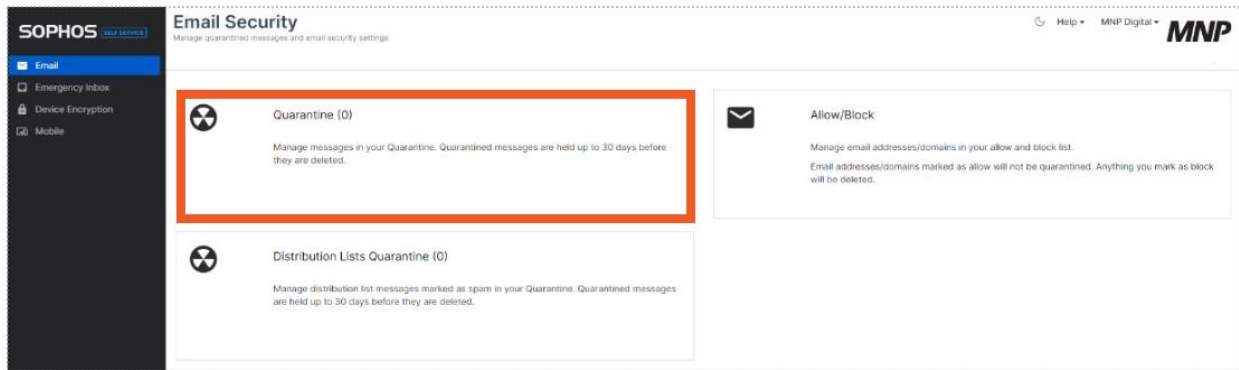


Manage Quarantined Emails

The Quarantine contains emails identified as potential spam. You can review these messages and either 'Release' or 'Delete' them. Releasing a message delivers it to your inbox. Below are the instructions on how to use Quarantine.

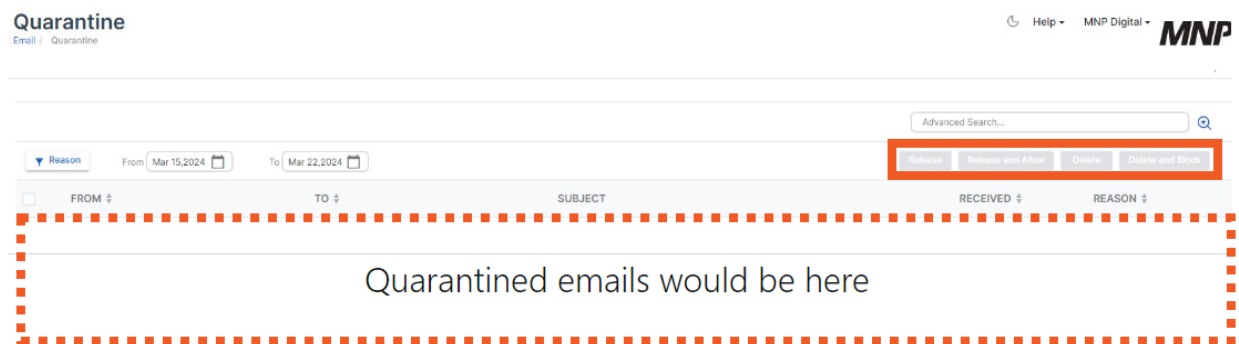
1. Click on Quarantine

The Quarantine lists emails that have been identified as potential spam. The sender, recipient, subject, time and date are shown for each email.



2. Select a subject to view the quarantined email message and choose whether you want to Release or Delete it.

Note: Quarantined messages are deleted after 30 days.

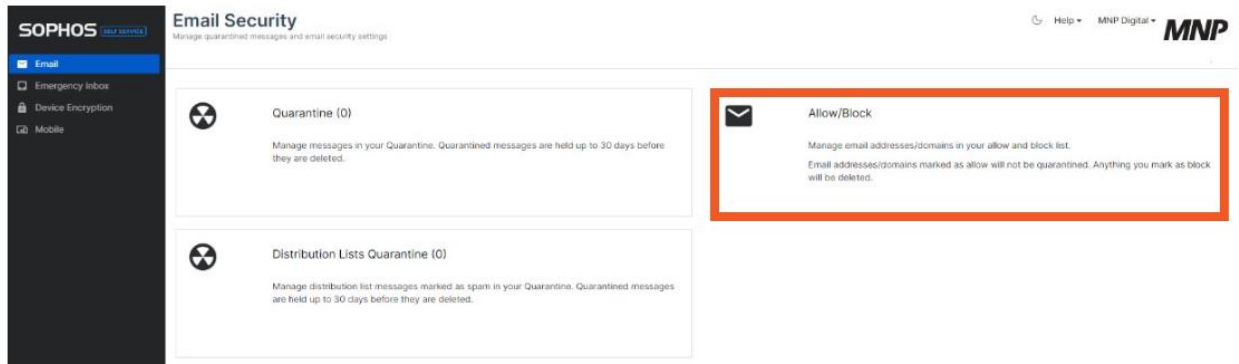


Allow/Block

You can manage which email addresses and domains are allowed or blocked using Allow/Block.

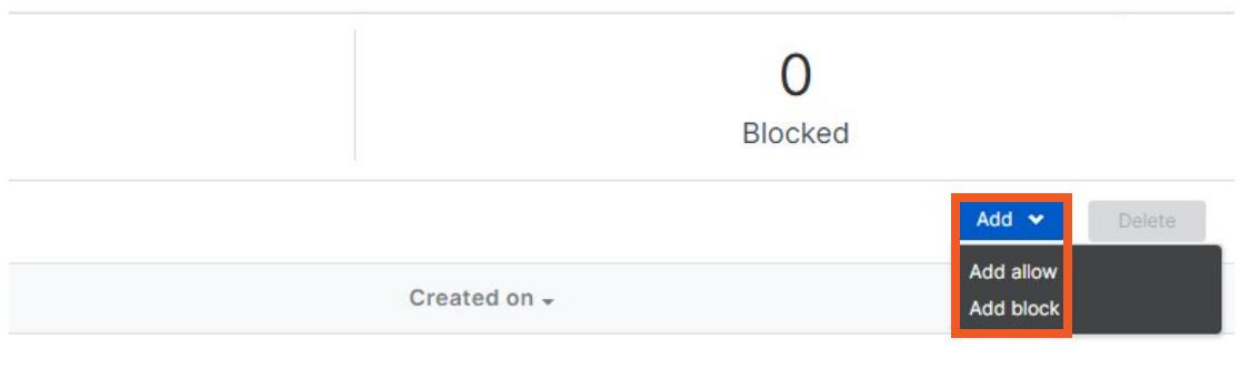
1. Click on Allow/Block.

Allow/Block displays a page to add email addresses or domains you want to allow or block. If you have already added some, a list is displayed. You can filter your results by using the Search field.



Note: Only personal items added through your self-service account are displayed here. Company-wide allows/blocks will not be shown in your self-service account.

2. Click Add to display the options Add and Block. Select the action you want to take.



A window will appear with a text box where you can add the email address or domain.

3. Add the email address or domain. You can also override duplicate entries by ticking the Override duplicates box.

If you add the same email address or domain to both the allow and block lists, Override duplicates will be based on the most recent option you choose.

Add allow ×

Email address or domain *

i.e. example.com, name@example.com. Wildcards are not supported.

Override duplicates i

Cancel
Save

4. Click Save to confirm your choice. Click Cancel if you do not want to save the settings.

Note: The spam detection function will not be carried out for email addresses and domains on your self-service account Allow list.

5. If you want to delete addresses or domains from the add or block list, select the items from the list and click Delete.

Allow/Block

Email / Allow/Block

Help ▾ MNP Digital ▾

0

All Allowed & Blocked

0

Allowed

0

Blocked

Search

Add ▾
Delete

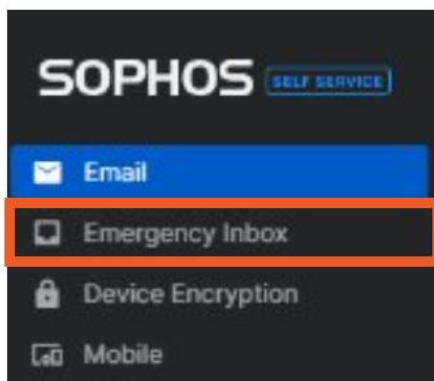
<input type="checkbox"/>	Action ▾	Address/Domain ▾	Created on ▾
Allow/Block list would be here			

A window will appear with the list of email addresses that you chose to delete. To confirm your selection, click Delete, otherwise click Cancel.

Emergency Inbox

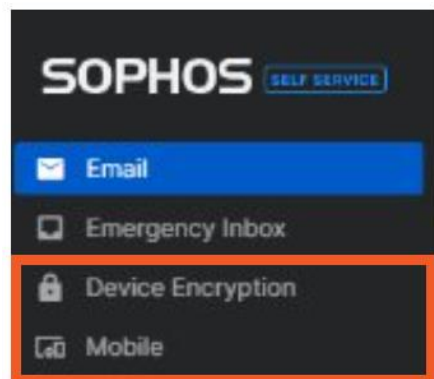
The Emergency Inbox may be used when you cannot access your email client (e.g. Outlook or Gmail). Suppose there's an outage affecting access to your email service provider, such as Microsoft 365 or Google Workspace. In that case, you can log into the email security tool and view your Emergency Inbox. The Emergency Inbox will hold all incoming emails until the service is

restored. Meaning you could view any critical emails you're waiting for even though your email service provider is down.



Device Encryption and Mobile

Device Encryption and Mobile functions are used if your organization leverages Sophos device management service.



Email Security – Smart Banners

Smart Banners will display at the top of inbound email messages to show if the email is trusted. Email recipients can add senders to their Allow and Block lists from within the email.

Trusted: Email sender is in the allowed list and passed verification.

A horizontal green banner with a thin black border. Inside the banner, the text reads: "This sender is trusted."

Unknown: Email sender is outside your organization and didn't fail verification.

Caution! This message was sent from outside your organization.

[Allow sender](#) | [Block sender](#)

Untrusted: Email sender is outside your organization and failed verification.

Warning! This message was sent from outside your organization and we were unable to verify the sender.

[Allow sender](#) | [Block sender](#)

Email Security – Sender Checks

Sender Checks are used to verify the authenticity of an email's origin.

When an email is received, it looks at the address of the sending mail server. If this check fails, the Subject line of the email will include the following prefix:

[CAUTION: SUSPECT SENDER]

This prefix indicates that the email could not be from whom it says it is. Before responding to the email, you should verify that it is authentic.