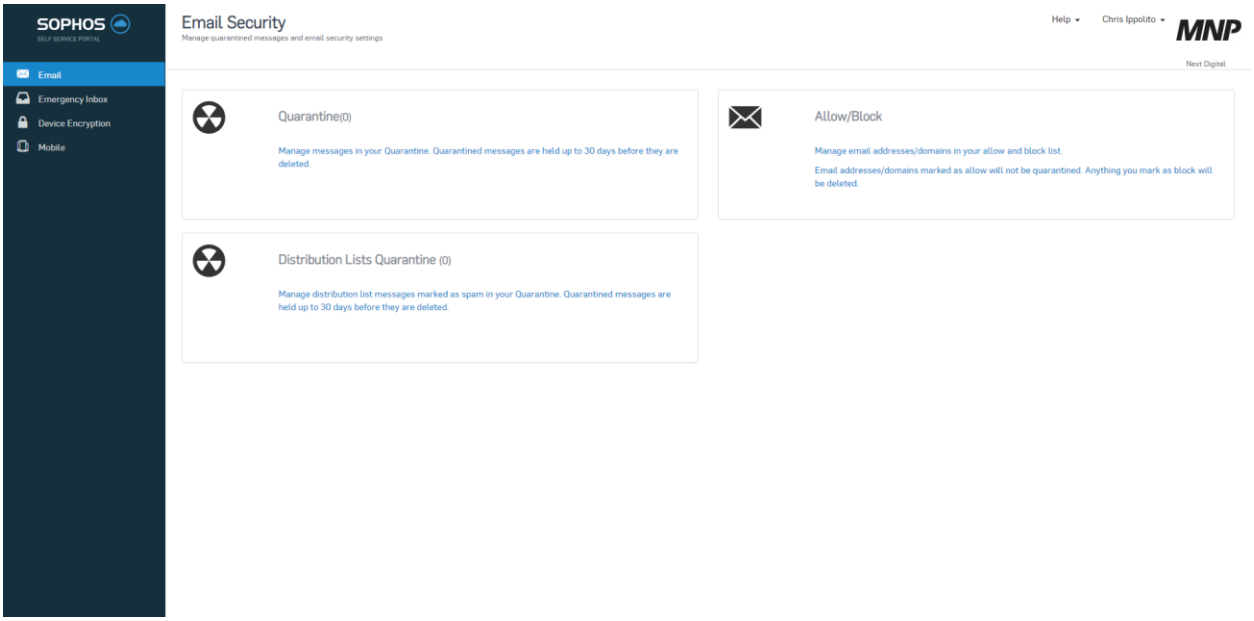
NextGen Email Security

The NextGen 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.

Self Service Account Setup

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 MNP Digital Service Portal.

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

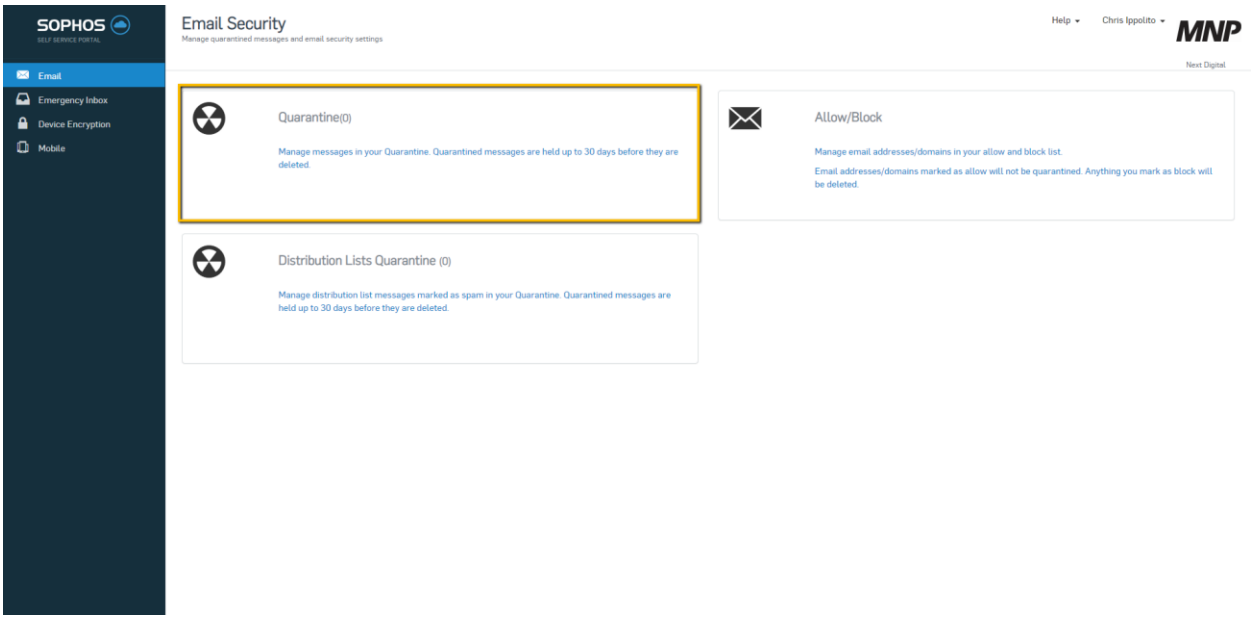


Manage Quarantined Emails

The Quarantine consists of 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 the Quarantine.

1. Click on Quarantine

The Quarantine displays a list of your 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.

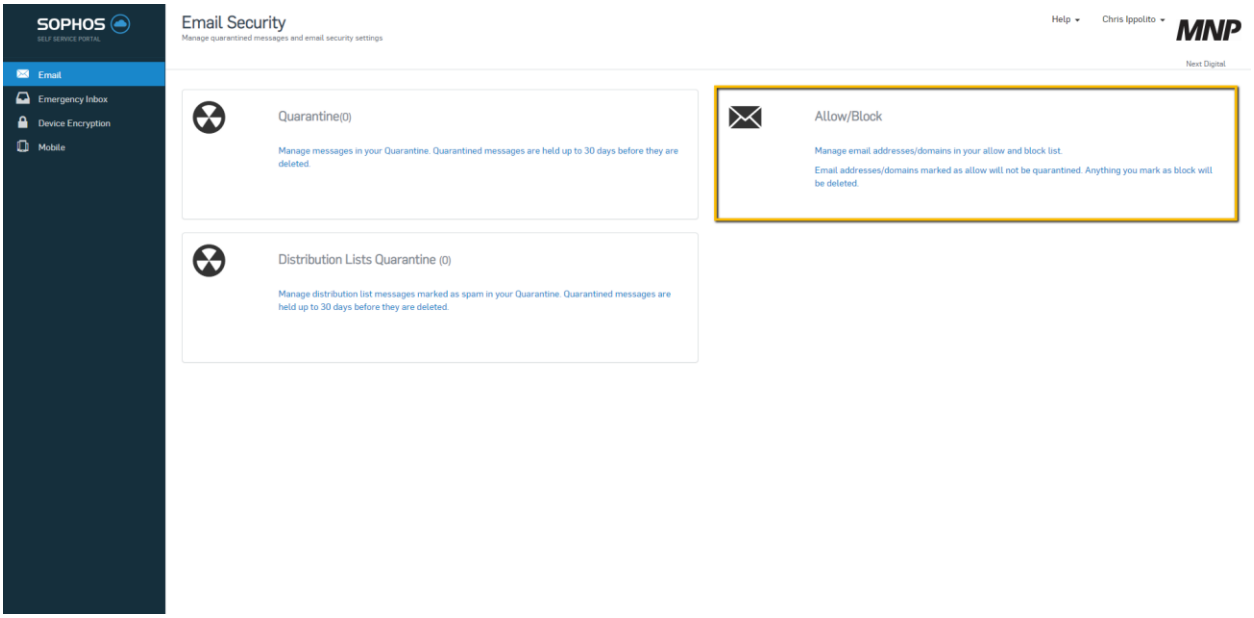
Note: *Quarantined messages are deleted after 30 days.*

Allow/Block

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

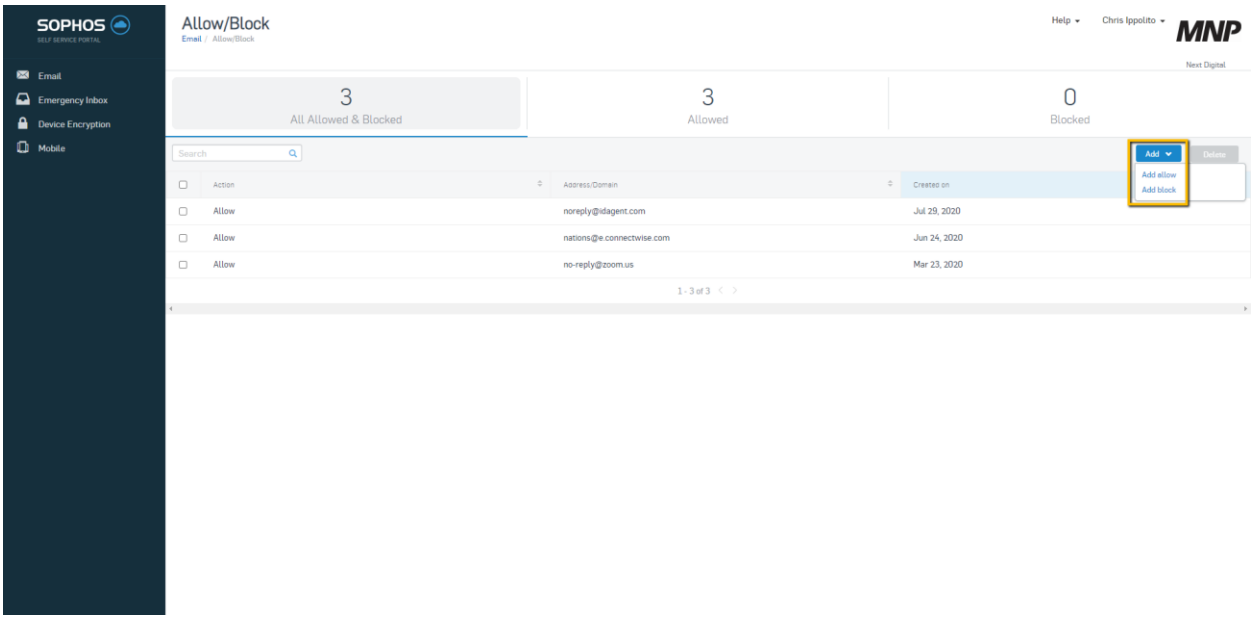
1. Click on Allow/Block.

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 though 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 a dropdown menu that will show the **Add** and **Block** options. Select the action you want to take.



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

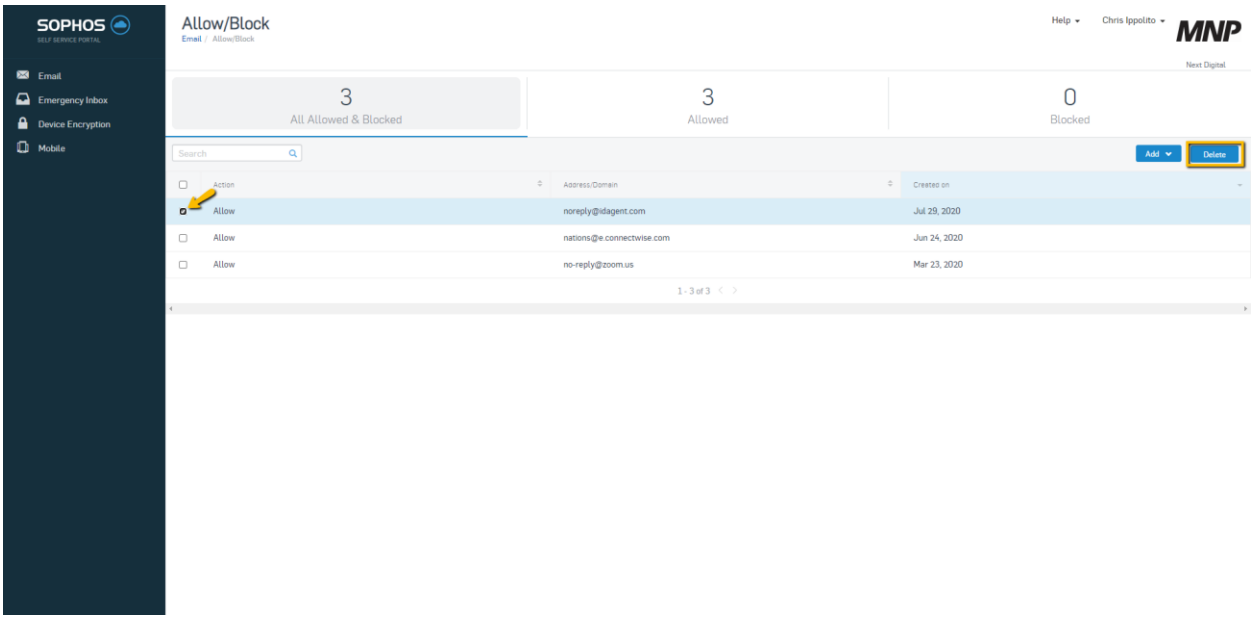
3. Add the email address or domain. You can also override duplicate entries by ticking the **Override duplicates** box.

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.

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.*

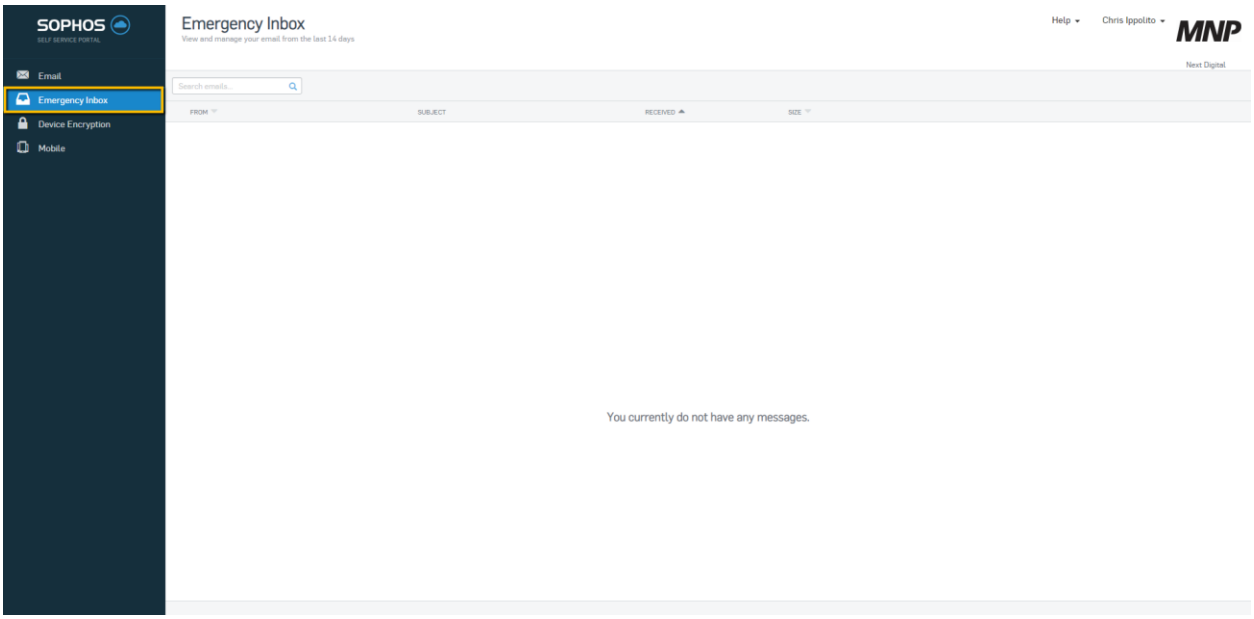
5. If you want to delete addresses or domains from the add or block list, select the items from the list and click Delete.



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 your NextGen Email Security self-service account 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.



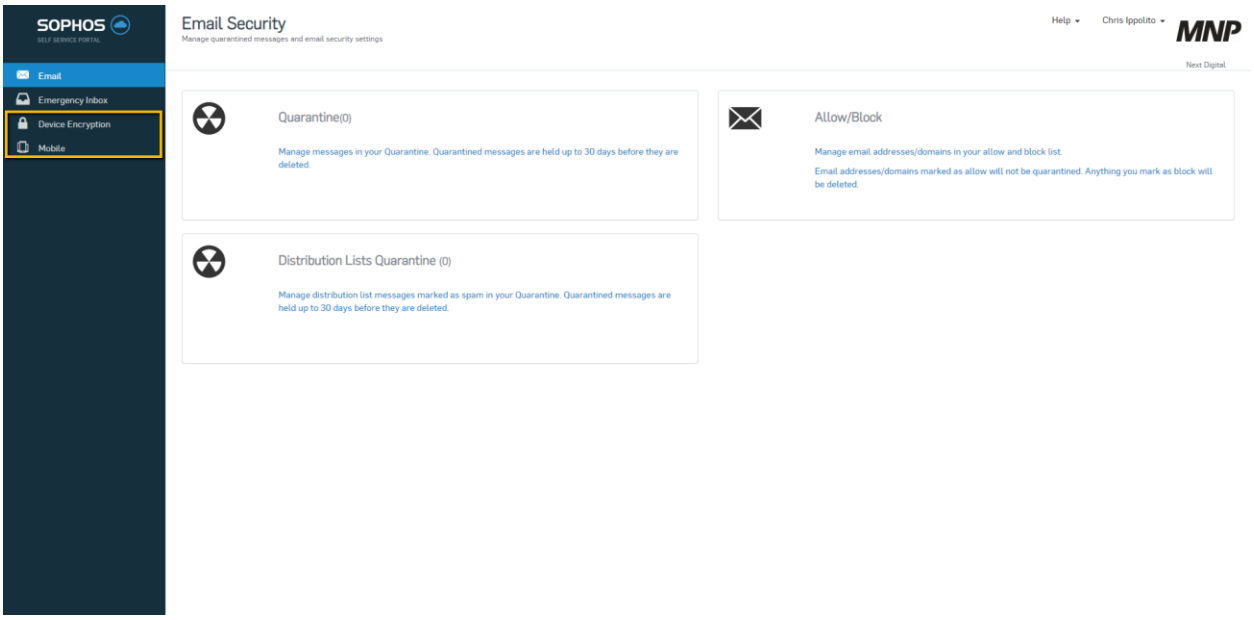
Device Encryption and Mobile

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

With **Device Encryption**, you can retrieve a recovery key to unlock your computer when you have forgotten your logon password (BitLocker PIN, password, USB key, or macOS password).

With **Mobile**, you enroll your device with Sophos Mobile.

You can also remotely locate, lock or wipe your devices and reset your password without having to contact the helpdesk.



NextGen 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: This banner is green. It shows that the email sender is in the allowed list and passed verification.

Unknown: This banner is yellow. It shows that email sender is outside your organization and didn't fail verification.

Untrusted: This banner is orange. It shows that the email sender is outside your organization and failed verification.

NextGen 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.

Additional Resources

Please visit https://www.mnp.ca/en/cx-knowledge-base for additional resources such as how to request support.