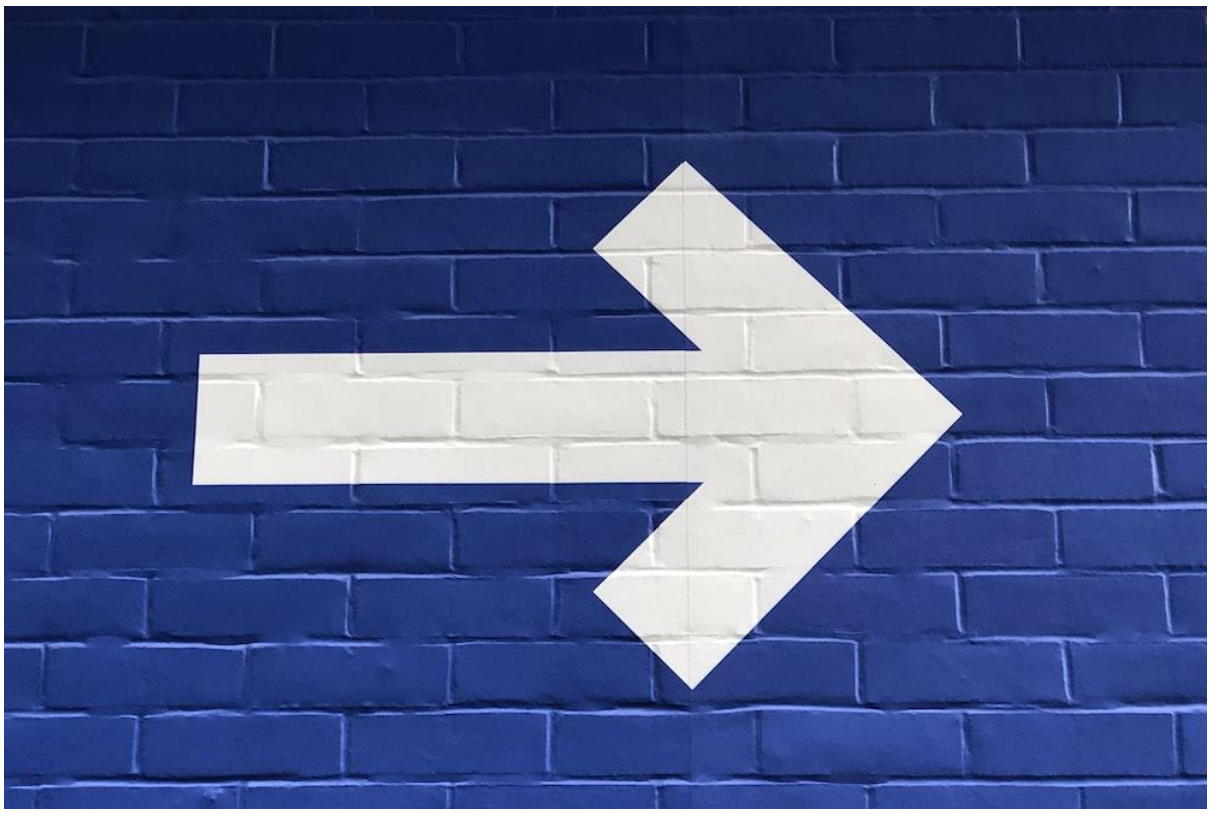
OMSUK Ltd

Important changes to your OMSUK Email Security



We are retiring our existing Email Security platform, Reflexion, and replacing it with a new platform from Mesh Security.

The new platform works in broadly similar ways to our previous platform, but we recommend you read this guide to familiarize yourself with any new changes and what you need to do.

We will be migrating all of our clients over the next month or so.

When is this happening?

We will be migrating clients Individually over the next month or so.

We will be contacting each client via email to let them know when this Is due to happen.

How much will this cost?

They'll be no change to your monthly agreement - the new service Is charged at exactly the same price as our old platform, and we bill in exactly the same way. You pay per email account, per month. You can cancel at any time, only needing to give us 30 days' notice.

How will this affect me?

We are taking every effort to reduce the impact of this change on our clients, however, you'll need to be aware of this change and how to access and use the Email Security Hub - details can be found later in this document.

You won't notice any disruption to your email during or after the transfer as we will manage the entire process for you.

However, following the migration, you'll need to go to a new URL/Link to check your email quarantine. In addition, you'll start to receive daily email digests with a list of any quarantined messages (these were formerly known as daily quarantine emails on our previous platform). These can be disabled but are switched on by default.

What about my block and allow lists?

We have migrated your block and allow lists from our old email security platform into the new platform.

Why are you changing your email security system?

We've been using the same system for a number of years now and after it was acquired by SOPHOS, development of the product stalled and no new updates have been released for the last few months. In addition, we've begun to experience issues that SOPHOS are slow or unwilling to resolve, such as non-delivery of the daily quarantine emails. SOPHOS are trying to encourage their clients to move across to their own email security platform. However, we found the SOPHOS system clunky and difficult to use. We therefore searched for a solution that would be a good fit for our clients and would still offer robust protection and security. We settled on Mesh Security.

What are the benefits?

Financial Fraud Prevention

Analyzes email containing payment requests, banking information and other financial content for signs of fraud and deception.

URL Protect

All URLs are subjected to scanning against real-time threat feeds for known and unknown malicious sites and fake login pages.

Dynamic Content Scanning

Next-gen spam filtering - Text and images in the message body are dynamically scanned for indicators of spam, nefarious intent, and evasive techniques.

4x Antivirus & Antimalware Engines

Multiple award-winning signature-based and heuristicbased scanning engines, detecting known and unknown types of malware, such as ransomware, botnets, and trojans.

Impersonation Detection

Inspects email content, language, tone, and cadence, combined with checks on the sender for matches and/or similarities with the recipient organization visually and phonetically.

Attachment Sandboxing

Unknown and potentially malicious attachments are detonated virtually, protecting against neverbefore-seen, zero-hour threats like polymorphic malware and new variants of ransomware.

End-User Quarantine Digests

Quarantined emails can be released by end users (if permitted) with intuitive, easy-to-use, ultramodern quarantine digests.

DMARC, DKIM, SPF Verification

Inbound emails are subject to DMARC, DKIM, and SPF verification checks, which assist in authenticating the sender.

Outbound Email Scanning

Outgoing emails are scanned for malicious content, spam, and signs of mailbox compromise.

Predictive Threat Intelligence

Mesh utilizes a combination of Passive DNS Sensors, DeepRelationship Analysis, Neural Networks and other information sources to detect abnormalities and predict where future attacks are likely to originate.

Graymail Filtering

Blocks unsolicited marketing emails and no longer wanted newsletters, improving employee productivity.

Built in Microsoft Azure

For maximum reliability and scalability, all Mesh services are built in Microsoft Azure Datacenters, helping you to meet some of the highest data center requirements for compliance and redundancy.

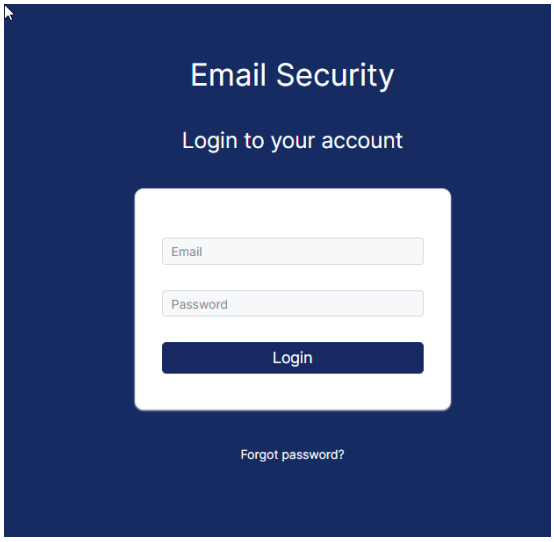
How do I access the new email quarantine?

When spam or potentially malicious messages are detected, they are automatically quarantined.

We will send you a daily digest of any quarantined messages each day.

However, we strongly recommend you review all messages that have been quarantined by visiting the Email Security Hub at the following link:

https://hub-eu.emailsecurity.app/



You can also click on the Manage your Quarantine button In the daily digest emails to access this page.

What Is my login to access the Email Security Hub?

Simply enter your email address and password then click Login to access the Email Security Hub.

What Is my password? How do I reset It?

You should have received an email to set a password for your account. Simply click on this link and set a secure, unique password to access the hub.

Didn't get an email? Click Forgot password? on the sign in page and enter your email address to get a link to reset your password.

Quarantine Digest Emails

1 - INTRODUCTION

Why do I receive a quarantine digest?

We have implemented Mesh's email security platform to protect against threats and spam. To ensure we don't incorrectly block an email you need, a tiny fraction of your email will end up in quarantine. These emails will be shown in quarantine digests.

How often will I receive a quarantine digest?

The frequency is set by your administrator. Regardless of frequency, digests will only be sent if there has been an email quarantined since your last digest.

How long are emails held in quarantine?

Emails are quarantined for 28 days after which they are automatically deleted.

1.1 - CATEGORIES

Threats
Made up of Definite Spam, High Spam, Likely Spam.

Spam
Made up of Infomail, Banned Attachments, Email that exceed the allowed size limit.

Policy
Email considered safe and delivered to your inbox.

Safe
Email considered safe and delivered to your inbox.

1.2 - ACTIONS

Deliver
Release email from quarantine and deliver the email to your inbox.

Preview
View the content of the email before taking an action.

Delete
Delete the email from quarantine. The email is no longer retrievable.

Request
For certain emails quarantined as either threats or policy, users can only request the email is released by their IT admin.

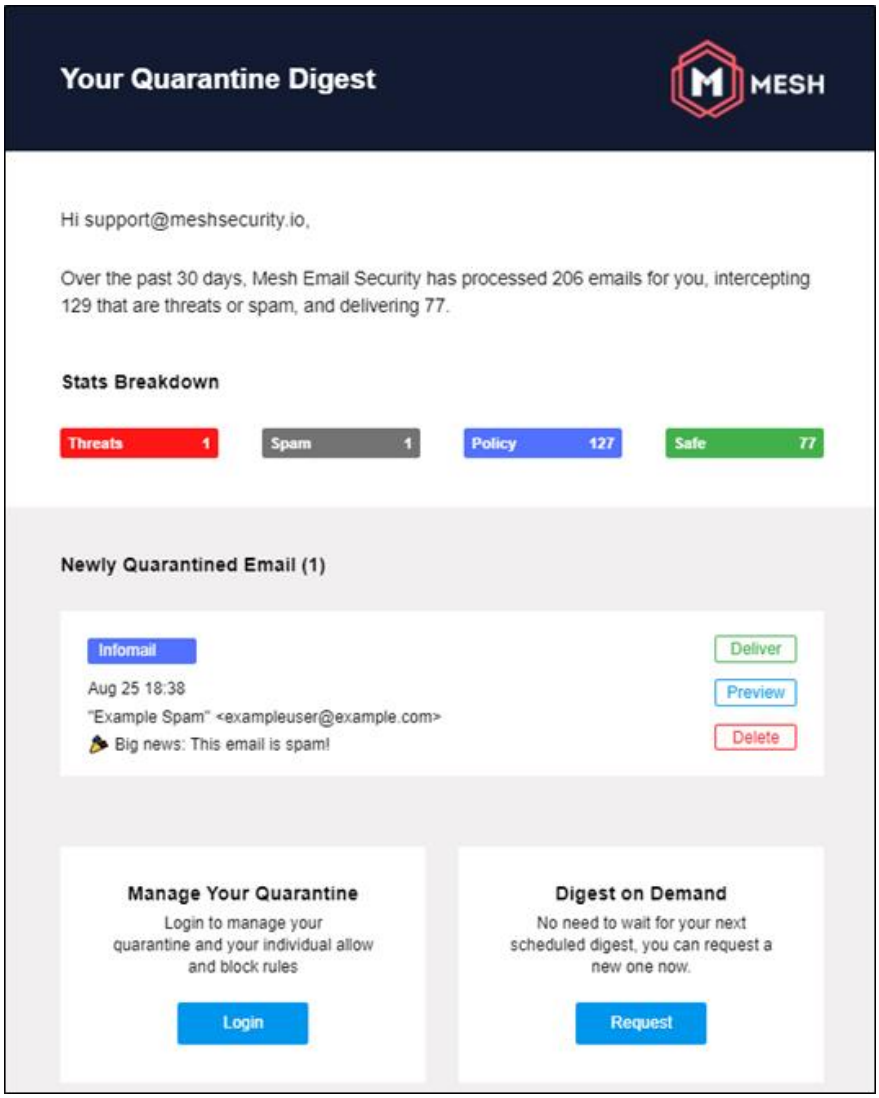


Figure 1: Quarantine Digest

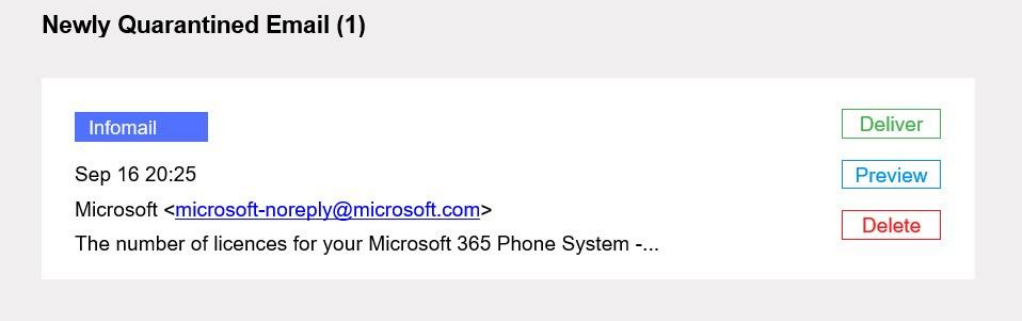


Figure 2: Newly Quarantined Emails

1.3 USING THE DELIVER BUTTON

To deliver emails directly to your inbox from a quarantine digest perform the following:

Step 1:

Click the "Deliver" button for the specific email in the quarantine digest.

Step 2:

A browser window will open stating that the email has been delivered.

Step 3a:

If you wish to allow all future emails from the sender select "Always allow sender".

Step 3b:

If you wish to allow all future from the sender's domain select "Always allow sender domain". You cannot allow entire free-mail domains such as Gmail or Hotmail.

Step 4:

Click "Confirm" if you have selected an option.

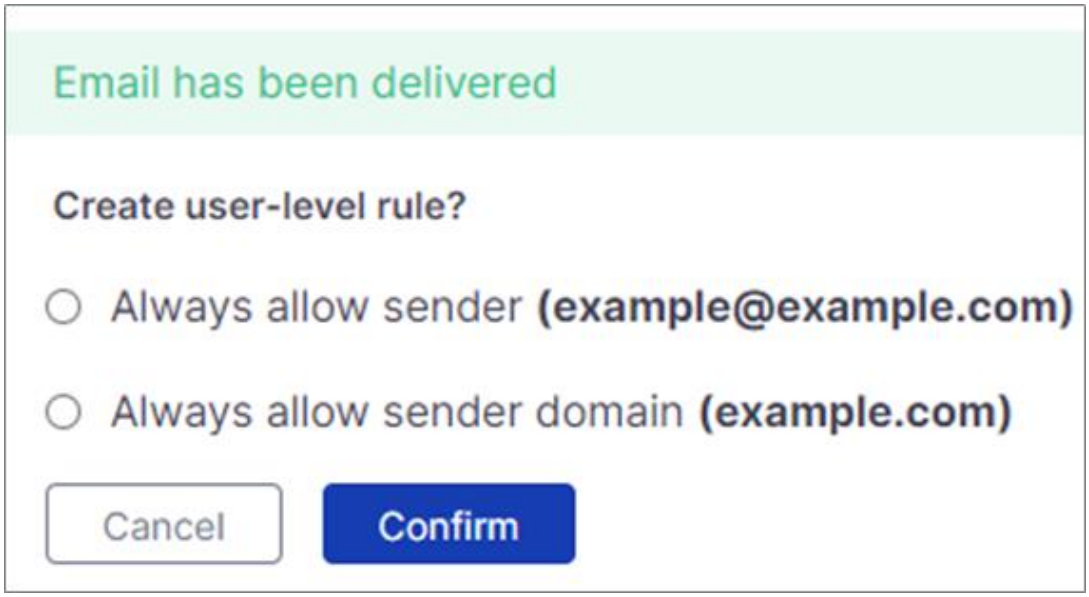


Figure 3: Email delivered

1.4 USING THE PREVIEW BUTTON

Previewing emails allows users to read the email in a secure browser window where all images have been removed and all links are converted to plaintext. In this browser window the choice to either deliver or delete the message is provided.

To preview emails from a quarantine digest, perform the following, click the “Preview” button for the specific email in the quarantine digest. This will open the default browser.

Several options are available in this window.

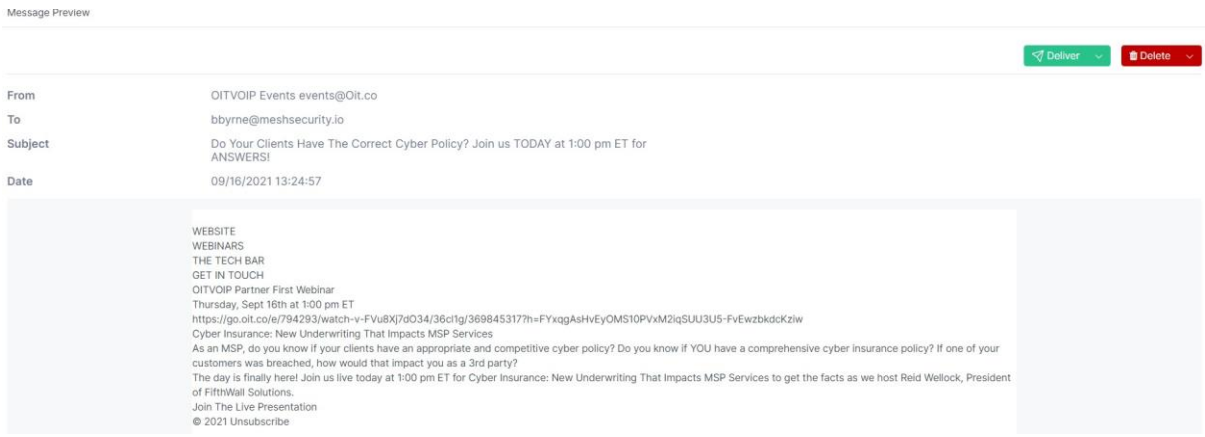


Figure 4: Preview window

1.4.1 DELIVER

Select the “Deliver” option to deliver the email from quarantine to your inbox. If the email that has been quarantined for violating the policy, it can only be delivered by an administrator for security reasons. In this case, clicking on the link sends a deliver request to the domain administrator.

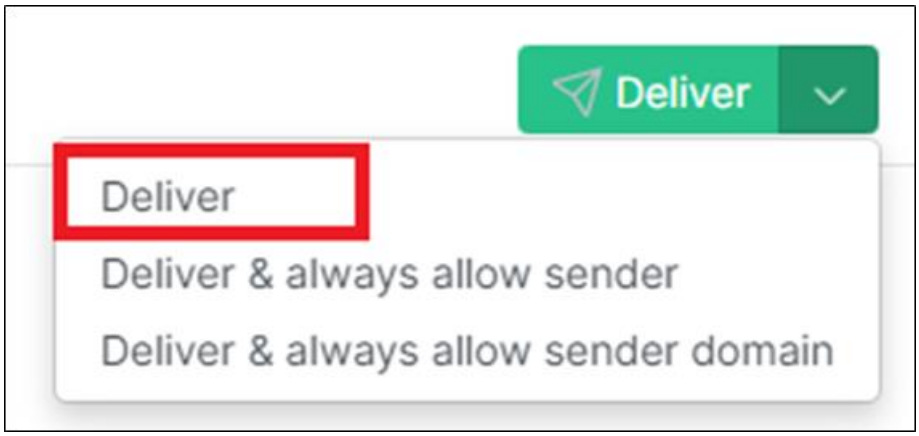


Figure 5: Deliver

1.4.2 DELIVER & ALWAYS ALLOW SENDER

Select the “Deliver” option to deliver the email from quarantine to your inbox. If the email that has been quarantined for violating the policy, it can only be delivered by an administrator for security reasons. In this case, clicking on the link sends a deliver request to the domain administrator.

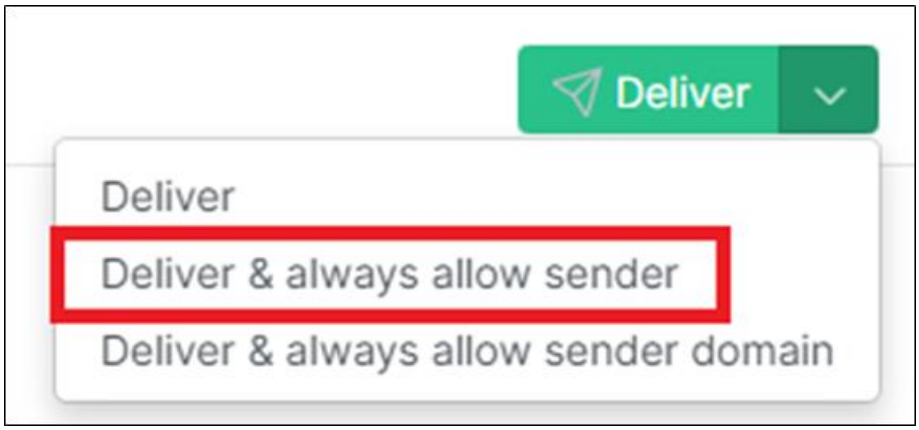


Figure 6: Deliver & always allow sender

1.4.3 DELIVER & ALWAYS ALLOW SENDER DOMAIN

Select the “Deliver & Always Allow Sender Domain” option to allow the sender domain. This adds an allow entry for the specified sender domain and the user’s email address. Emails from the same domain are also allowed in future.

NOTE
For security reasons you cannot always allow your own domain or free domains, such as Gmail, Hotmail, or Yahoo.

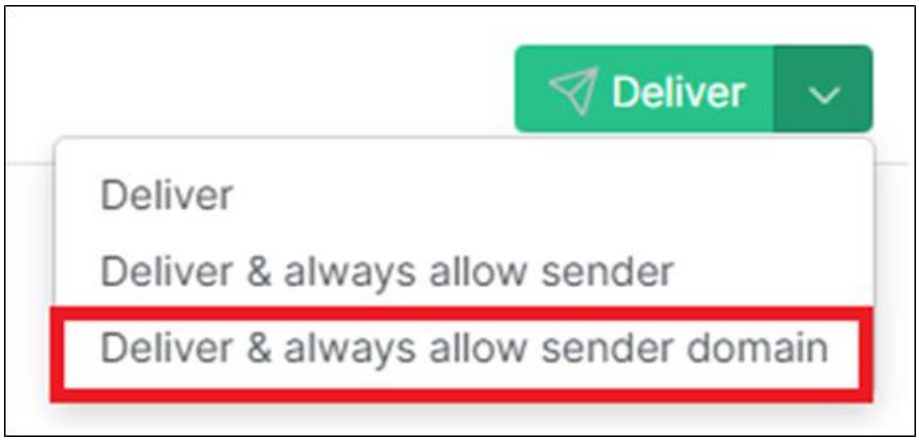


Figure 7: Deliver & always allow sender domain

1.4.4 DELETE

Select the “Delete” option to delete the email from quarantine.

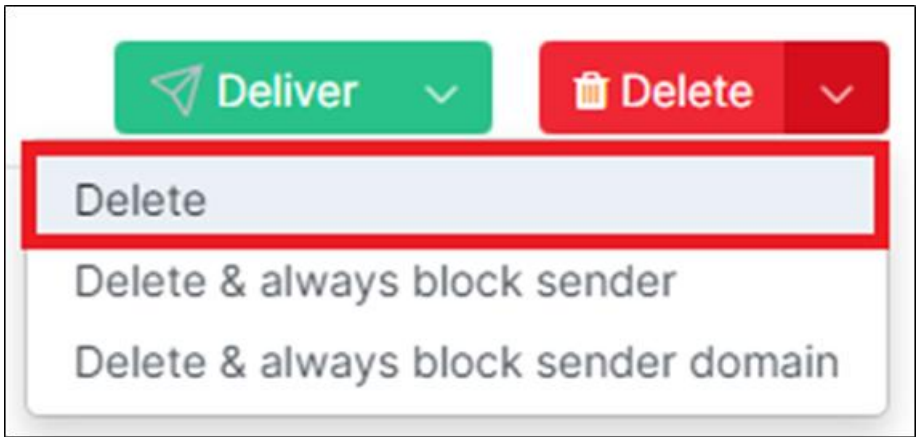


Figure 8: Delete

1.4.5 DELETE & ALWAYS BLOCK SENDER

Select “Deliver & Always Block Sender” to block the sender email address. This adds a block rule entry for the specified sender email address and the user’s email address.

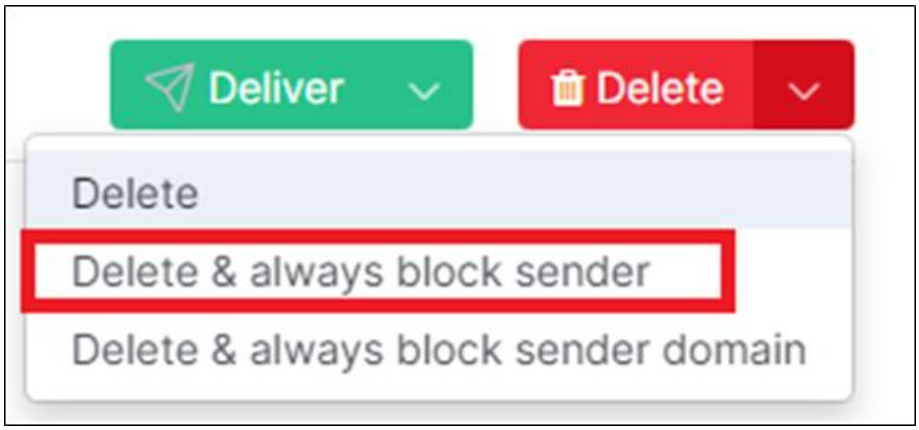


Figure 9: Delete & always block sender

1.4.6 DELETE & ALWAYS BLOCK SENDER DOMAIN

Select “Deliver & Always Block Sender Domain” to block the sender domain. This adds a block rule entry for the specified sender domain and the user’s email address. Email from other addresses at the domain is also blocked.

NOTE
For security reasons you cannot always block free domains, such as Gmail, Hotmail, or Yahoo.

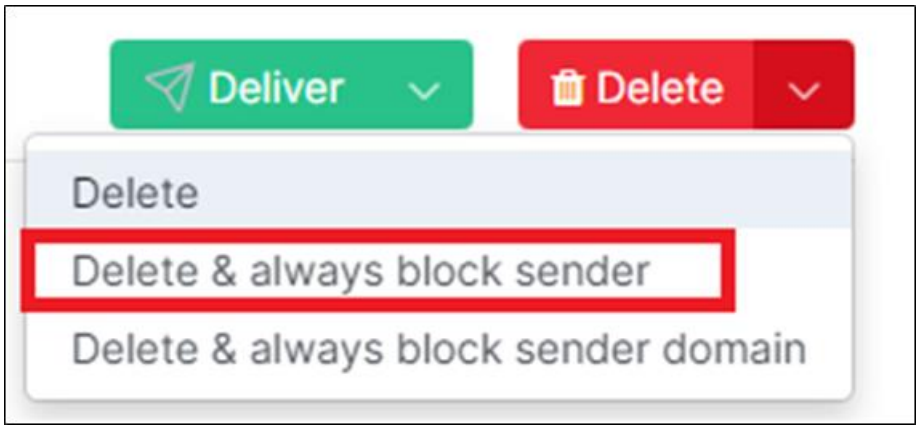


Figure 10: Delete & always block sender domain

1.5 USING THE DELETE BUTTON

To delete emails permanently from quarantine perform the following:

Step 1:

Click the “Delete” button for the specific email in the quarantine digest.

Step 2:

A browser window will open stating that the email has been deleted.

Step 3a:

If you wish to block all future emails from the sender select “Always block sender”.

Step 3b:

If you wish to block all future from the sender’s domain select “Always block sender domain”. You cannot block entire free-mail domains such as Gmail or Hotmail.

Step 4:

Click “Confirm” if you have selected an option.

Figure 11: Email Deleted

1.6 MANAGING YOUR QUARNATINE

The “Manage Your Quarantine” button allows users to login to view their quarantine. Here all emails currently in quarantine are listed. Allow rules and block rules can be created and deleted also.

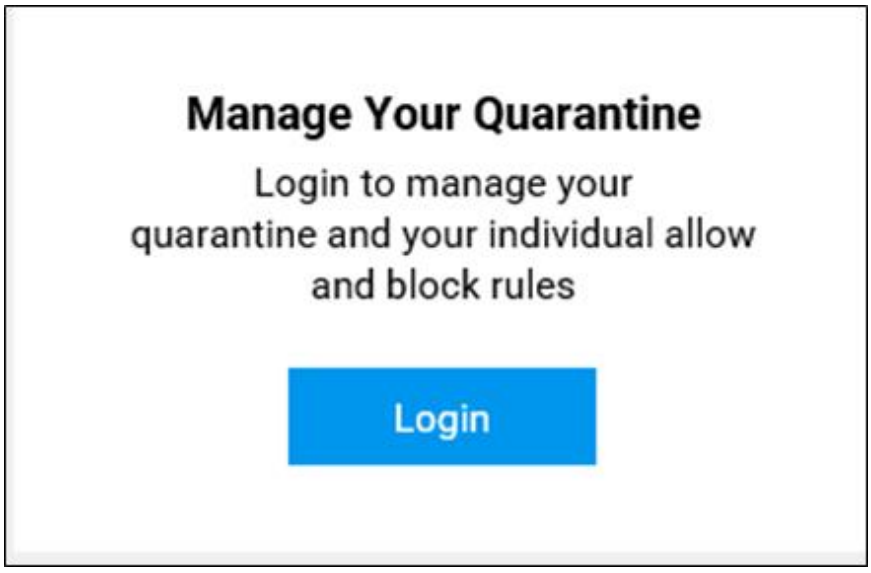


Figure 12: Manage Your Quarantine

1.7 DIGEST ON DEMAND

The Digest on Demand feature allows users to request a brand-new digest on the fly.

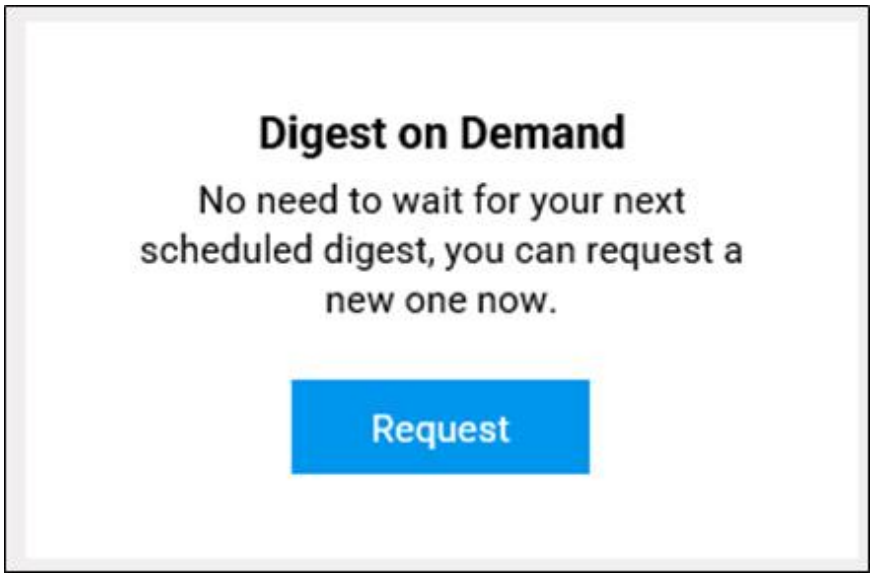


Figure 13: Digest on Demand

Once clicked a browser window will open and advising that a request was sent. Note: If there have been no quarantined emails since the previous period, a digest will not be sent. Maximum of 3 requests per day per user.

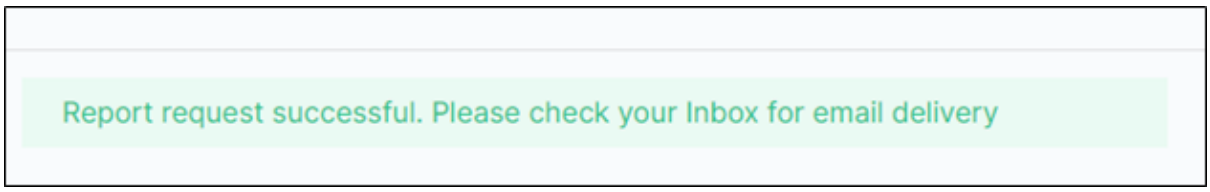


Figure 14: Digest request successful