

Email Security for Microsoft O365

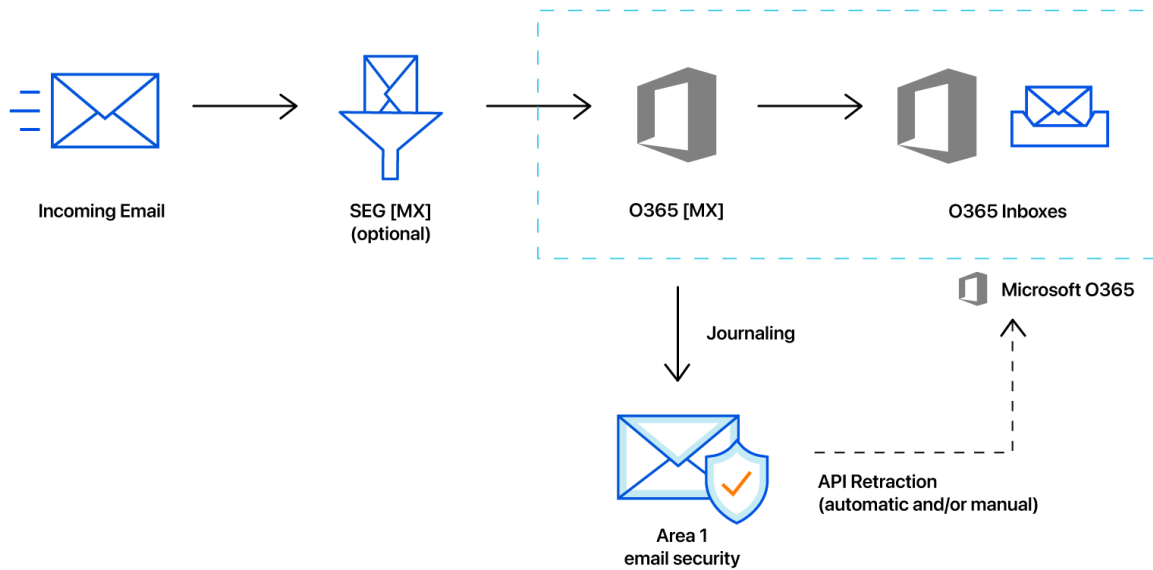
Deployment and Configuration Guide
Automatic Message Retraction

Area 1 Horizon Overview

Phishing is the root cause of 95% of security breaches that lead to financial loss and brand damage. Area 1 Horizon is a cloud based service that stops phishing attacks, the #1 cybersecurity threat, across all traffic vectors - email, web and network.

With globally distributed sensors & comprehensive attack analytics, Area 1 Horizon proactively identifies phishing campaigns, attacker infrastructure, and attack delivery mechanisms during the earliest stages of a phishing attack cycle. Using flexible enforcement platforms, Area 1 Horizon allows customers to take preemptive action against these targeted phishing attacks across all vectors - email, web and network; either at the edge or in the cloud.

Email Flow



Configuration Steps

- Step 1: Authorize Area 1 with O365 for Retraction
- Step 2: Configure Auto-Retraction Actions
- Step 3: Configure connector for delivery to Area 1 (if required)
- Step 4: Configure Journaling Rule
- Manual Retractions

Step 1: Authorize Area 1 with O365 for Retraction

For message retraction to successfully execute, Area 1 Horizon needs to be authorized to make API calls into O365 Graph API architecture. The account used to authorize will require the **"Privileged role admin"** role.

When assigning user roles in the O365 console, you will find these roles under the **Identity** admin roles in the Roles configuration section of the user permissions.

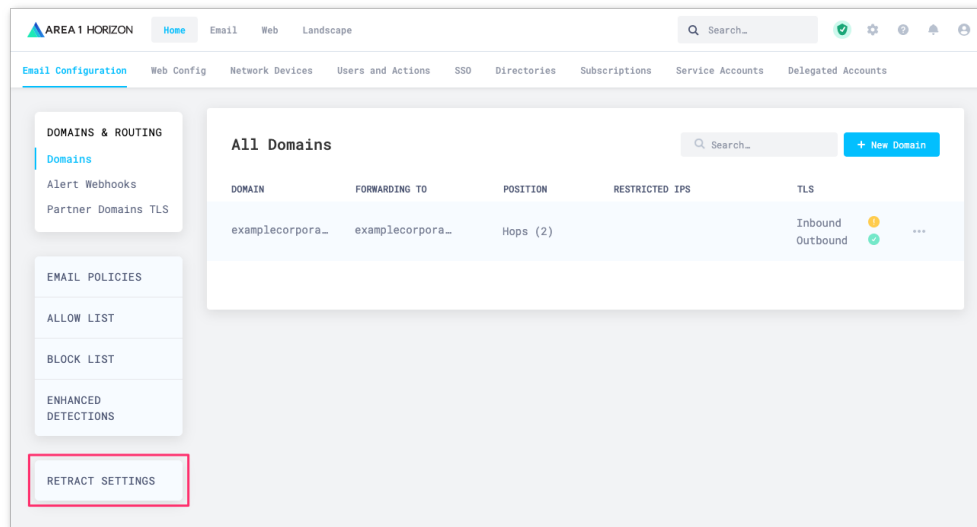
How does the Authorization work?

The authorization process grants the Horizon Portal access to the Azure environment with the least applicable privileges required to function as shown in the screenshot below. The Enterprise Application that we register (Area 1 Security Synchronator) is not tied to any administrator account. Inside of the Azure Active Directory admin center you can review the Permissions granted to the application under the Enterprise Application section.

The screenshot shows the 'Permissions' page for the 'Area 1 Security Synchronator ((Production Portal))' Enterprise Application in the Azure Active Directory admin center. The left sidebar contains navigation links for 'Deployment Plan', 'Manage' (Properties, Owners, Roles and administrators, Users and groups, Single sign-on, Provisioning, Self-service, Custom security attributes), 'Security' (Conditional Access, Permissions, Token encryption), and 'Activity' (Sign-in logs, Usage & insights, Audit logs, Provisioning logs, Access reviews). The main content area has a 'Permissions' section with a description of how permissions are granted and a 'Grant admin consent for Area 1 Security' button. Below this, there are tabs for 'Admin consent' and 'User consent', with 'Admin consent' selected. A search bar is present above a table of permissions.

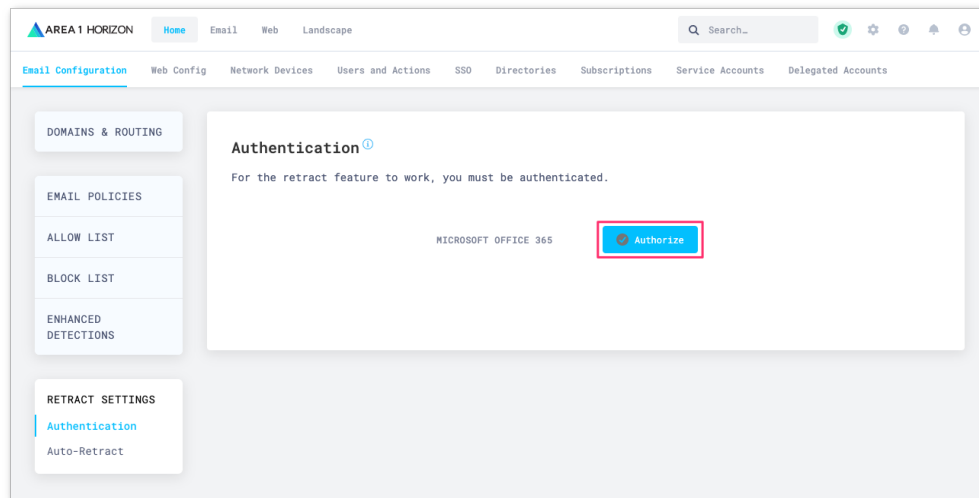
API Name	Claim value	Permission	Type	Granted through
Microsoft Graph				
Microsoft Graph	Mail.ReadWrite	Read and write mail in all mailb...	Application	Admin consent
Microsoft Graph	Group.Read.All	Read all groups	Application	Admin consent
Microsoft Graph	User.Read.All	Read all users' full profiles	Application	Admin consent
Microsoft Graph	Domain.Read.All	Read domains	Application	Admin consent
Microsoft Graph	GroupMember.Read.All	Read all group memberships	Application	Admin consent
Microsoft Graph	Organization.Read.All	Read organization information	Application	Admin consent

1. From the Area 1 Horizon Portal, access the Email Configuration section (<https://horizon.area1security.com/settings/email/routing/domains>) and select the **Retraction Settings** option on the left navigation bar:

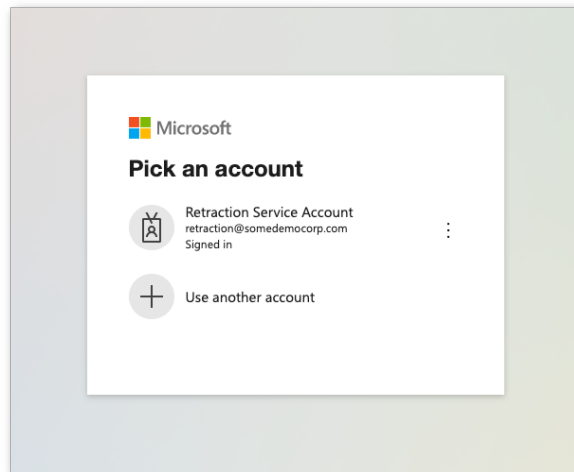


Note: If you do not see the **Retract Settings** option, please contact customer support to enable the feature.

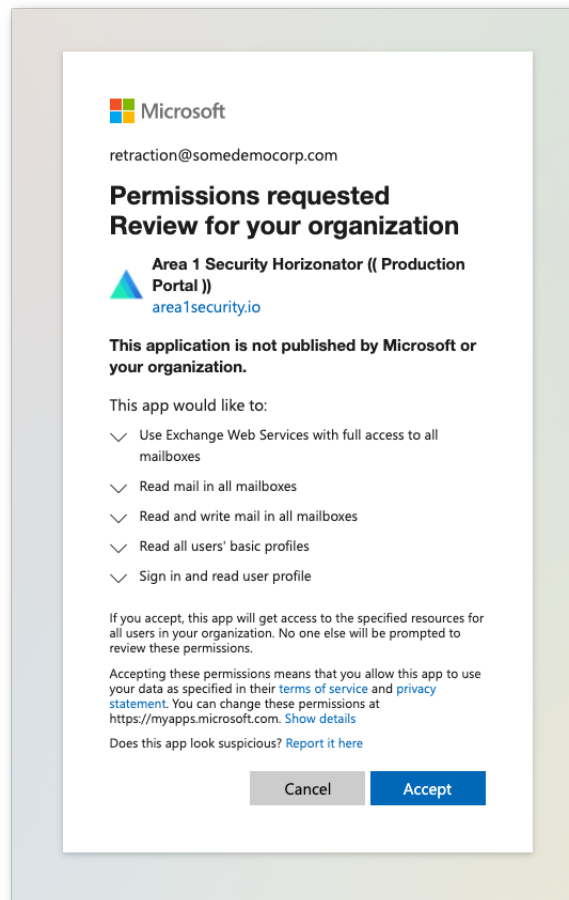
2. In the Retraction Settings section, you will need to authorize Area 1 to execute retractions through O365's Graph API. This is a simple process that requires you to authenticate and authorize Area 1 with O365. Ensure that the account that you will be using to authenticate has the appropriate administrative roles assigned. Click the **Authorize** button to start the process:



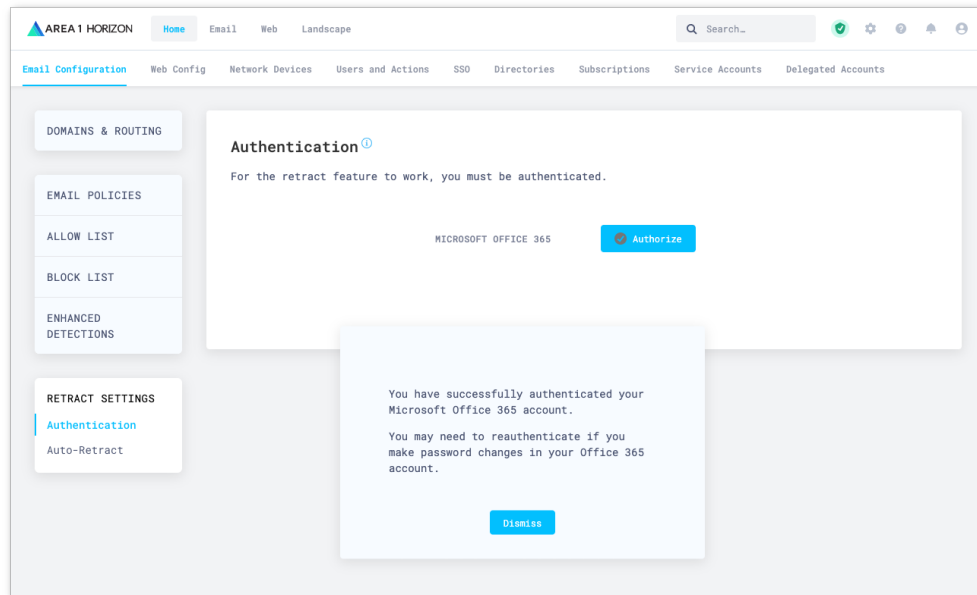
3. The Area 1 Horizon Portal will redirect you to a Microsoft Login page, select or enter the appropriate account to initiate for the authentication process:



4. Once authenticated, you will receive a dialog explaining the requested permissions, click on the **Accept** button to authorize the change:



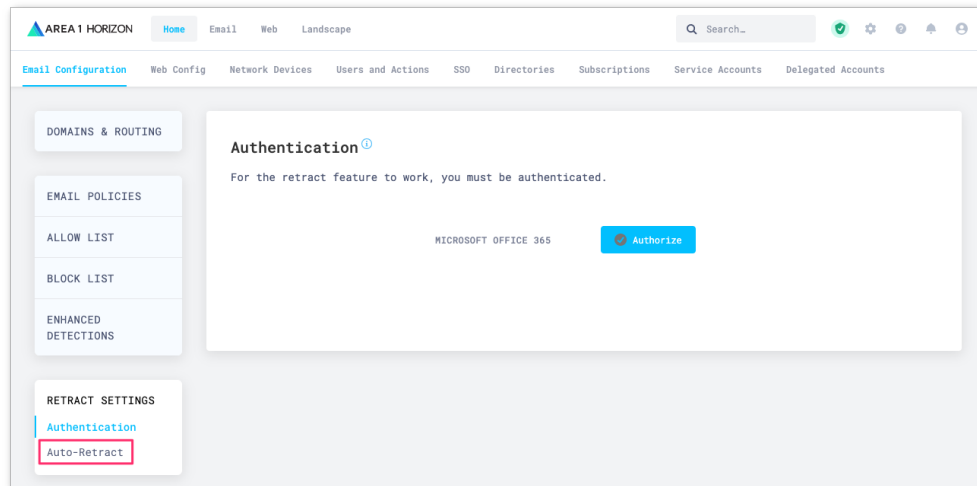
5. Upon authorization, you will be automatically redirected to the Area 1 Portal, with a notification that the authorization successfully completed, you may click **Dismiss** to clear the notification:



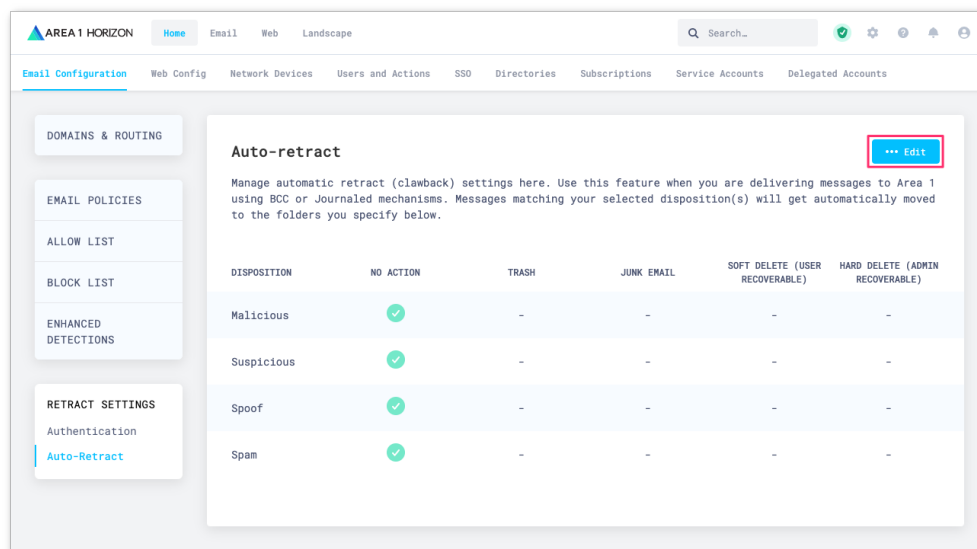
Step 2: Configure Auto-Retraction Actions

Now that Area 1 has been authorized to retract messages from O365 inboxes, you need to configure the retraction behavior for each disposition.

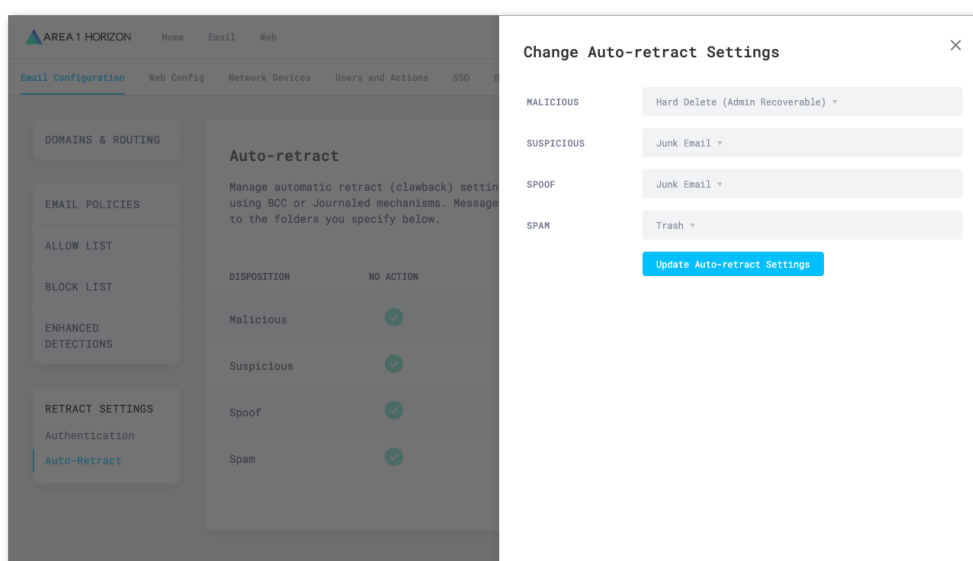
1. Click the **Auto-Retract** option on the left navigation bar to access retraction behavior setting:



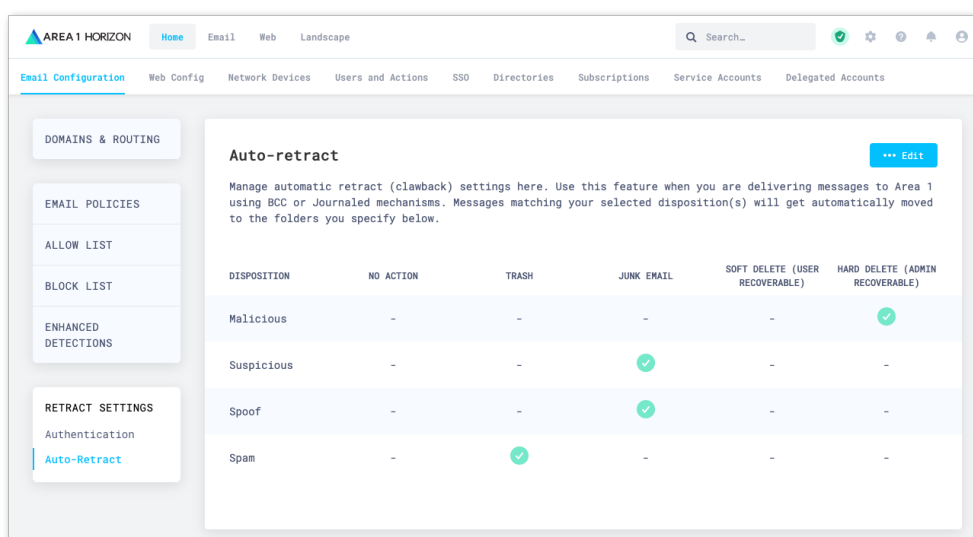
2. By default, no actions are taken against any of the dispositions. To modify the behaviors, click the **Edit** button:



3. Select the appropriate remediation behavior for each disposition and save your selection by clicking the **Update Auto-retraction Settings**:



4. Once saved, the configuration table will update with the selected behaviors:

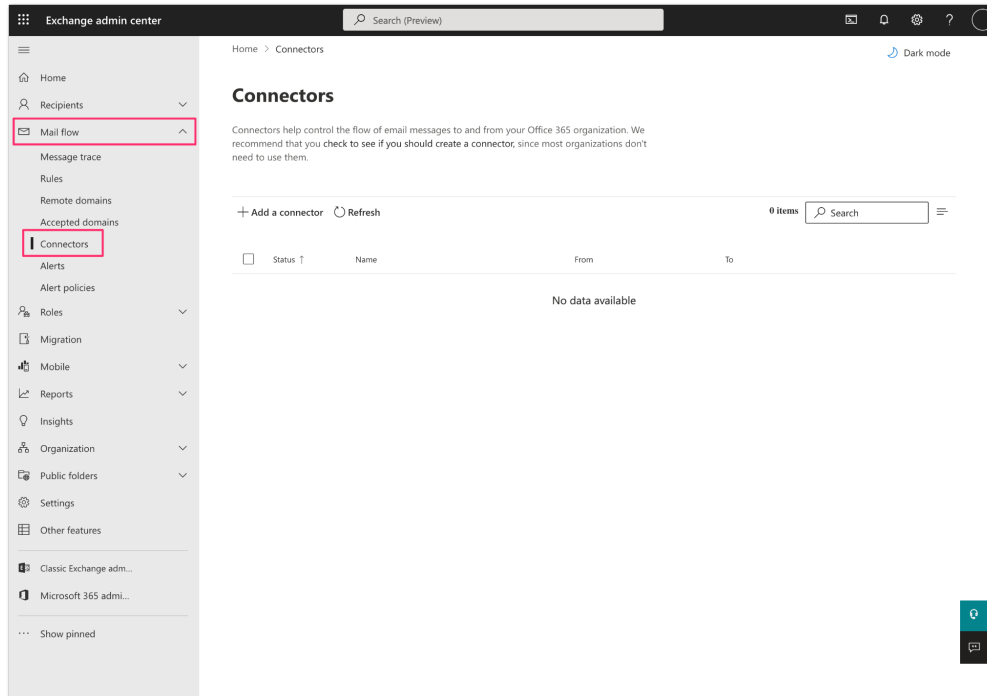


Step 3: Configure connector for delivery to Cloudflare Area 1 (if required)

If your email architecture does not include an outbound gateway, you can skip and proceed to the next step of this configuration guide..

If your email architecture requires outbound messages to traverse your email gateway, you may want to consider configuring a connector to send the journal messages directly to Area 1.

1. Open the Exchange admin center, and access the **Connectors** configuration under the **Mail flow** menu at <https://admin.exchange.microsoft.com/#/connectors>



2. Click the **+ Add a connector** button to configure a new connector and configure the connector mail direction as follows:

- **Connection From:** Office 365
- **Connection to:** Partner Organization

The screenshot shows the 'Exchange admin center' interface with the 'Add a connector' wizard open. The left sidebar contains navigation links: Home, Recipients, Mail flow, Message trace, Rules, Remote domains, Accepted domains, Connectors, Alerts, Alert policies, Roles, Migration, Mobile, Reports, Insights, Organization, Public folders, Settings, Other features, Classic Exchange admin center, and Microsoft 365 admin center. The main content area is titled 'Add a connector' and shows a progress bar with steps: New connector (selected), Name, Use of connector, Routing, Security restrictions, Validation email, and Review connector. The 'New connector' step is active, displaying the title 'New connector' and the instruction 'Specify your mail flow scenario, and we'll let you know if you need to set up a connector.' Below this, there are two sections: 'Connection from' and 'Connection to'. In the 'Connection from' section, 'Office 365' is selected with a radio button. In the 'Connection to' section, 'Partner organization' is selected with a radio button. A 'Next' button is located at the bottom right of the wizard.

3. Configure the connector name and description:

- **Name:** Deliver journal directly to Area 1
- **Description:** Deliver journal directly to Area 1
- Select the **Turn it on** checkbox

Exchange admin center

Home > Connectors

Connectors

Connectors help recommend the need to use the

+ Add a connector

☐ Status

Add a connector

☒ New connector

Name

☐ Use of connector

☐ Routing

☐ Security restrictions

☐ Validation email

☐ Review connector

Connector name

This connector enforces routing and security restrictions for email messages sent from Office 365 to your partner organization or service provider.

Name *

Deliver journal directly to Area 1

Description

Deliver journal directly to Area 1

What do you want to do after connector is saved?

☒ Turn it on

Back Next

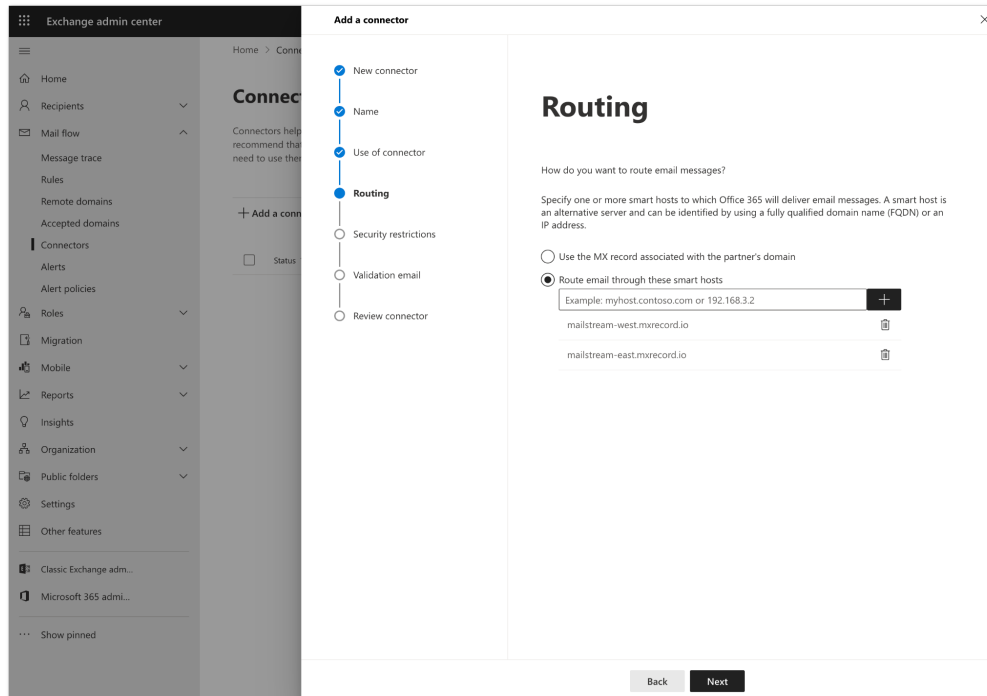
4. Configure the **Use of connector** setting:

- Select **Only when email messages are sent to these domains** option
- Enter **journaling.mxrecord.io** in the text field and click **+** to add domain.

The screenshot shows the 'Exchange admin center' interface with the 'Add a connector' wizard open. The wizard has a progress bar with steps: New connector, Name, Use of connector (current), Routing, Security restrictions, Validation email, and Review connector. The 'Use of connector' step is active, showing the title 'Use of connector' and the instruction 'Specify when you want to use this connector.' There are two radio button options: 'Only when I have a transport rule set up that redirects messages to this connector' and 'Only when email messages are sent to these domains'. The second option is selected. Below the options is a text input field with the placeholder 'Example: * or *.contoso.com or *.com' and a '+' button to add domains. The domain 'journaling.mxrecord.io' has been entered in the field. At the bottom of the wizard are 'Back' and 'Next' buttons.

5. Configure the **Routing** setting by selecting the **Route email through these smart hosts** and specifying the following smarthosts. Click the **+** button after each hosts to add them to the configuration:

- mailstream-east.mxrecord.io
- mailstream-west.mxrecord.io



If there is a requirement to enforce traffic through the EU region use the following smarthost instead:

- mailstream-eu1.mxrecord.io

6. Preserve the default TLS configuration:

The screenshot shows the 'Exchange admin center' interface with the 'Add a connector' wizard open. The wizard is at the 'Security restrictions' step, which is highlighted in the progress bar. The progress bar shows the following steps: New connector, Name, Use of connector, Routing, Security restrictions (current), Validation email, and Review connector. The 'Security restrictions' section asks 'How should Office 365 connect to your partner organization's email server?' and provides three options: 'Always use Transport Layer Security (TLS) to secure the connection (recommended)' (checked), 'Connect only if the recipient's email server certificate matches this criteria', and 'Any digital certificate, including self-signed certificates'. Below these options, there is a checkbox for 'Issued by a trusted certificate authority (CA)' and a checkbox for 'Add the subject name or subject alternative name (SAN) matches this domain name:'. An example domain 'contoso.com or *.contoso.com' is provided. At the bottom of the wizard, there are 'Back' and 'Next' buttons.

Exchange admin center

Home > Connectors

Add a connector

Connectors help recommend the need to use the

+ Add a connector

Status

Progress bar: New connector, Name, Use of connector, Routing, **Security restrictions**, Validation email, Review connector

Security restrictions

How should Office 365 connect to your partner organization's email server?

- ☒ Always use Transport Layer Security (TLS) to secure the connection (recommended)
Connect only if the recipient's email server certificate matches this criteria
- ☐ Any digital certificate, including self-signed certificates
- ☒ Issued by a trusted certificate authority (CA)
- ☐ Add the subject name or subject alternative name (SAN) matches this domain name:
Example: contoso.com or *.contoso.com

Back Next

7. Validate the connector by using your tenant's specific journaling address. This address can be found in the Area 1 Horizon portal in the Support > Service Addresses page (<https://horizon.area1security.com/support/service-addresses>):

The screenshot shows the 'Exchange admin center' interface with the 'Add a connector' wizard open. The wizard has a progress bar on the left with steps: New connector, Name, Use of connector, Routing, Security restrictions, Validation email (current step), and Review connector. The 'Validation email' step is active, showing a title 'Validation email' and instructions: 'Specify an email address for an active mailbox that's on your partner domain. You can add multiple addresses if your partner organization has more than one domain.' Below the instructions is a text input field with a placeholder 'Example: user@contoso.com' and a '+' button. The field contains the address 'address@journaling.mxrecord.io' and a 'Validate' button. At the bottom of the wizard are 'Back' and 'Next' buttons.

9. Once the validation completes, you should receive a **Succeeded** status for all the tasks:

Exchange admin center

Home > Connectors

Connectors help recommend the need to use them.

+ Add a connector

Status

Roles

Migration

Mobile

Reports

Insights

Organization

Public folders

Settings

Other features

Classic Exchange admin center

Microsoft 365 admin center

Show pinned

Add a connector

New connector

Name

Use of connector

Routing

Security restrictions

Validation email

Review connector

Validation email

Specify an email address for an active mailbox that's on your partner domain. You can add multiple addresses if your partner organization has more than one domain.

Example: user@contoso.com

address@journaling.msrecord.io

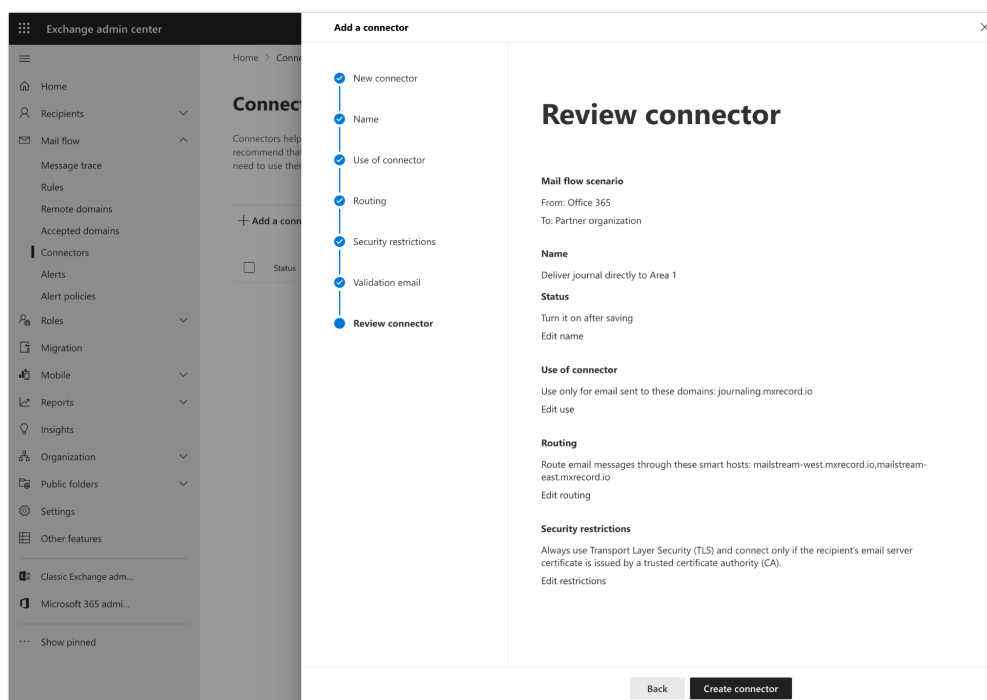
Validate

Validation successful

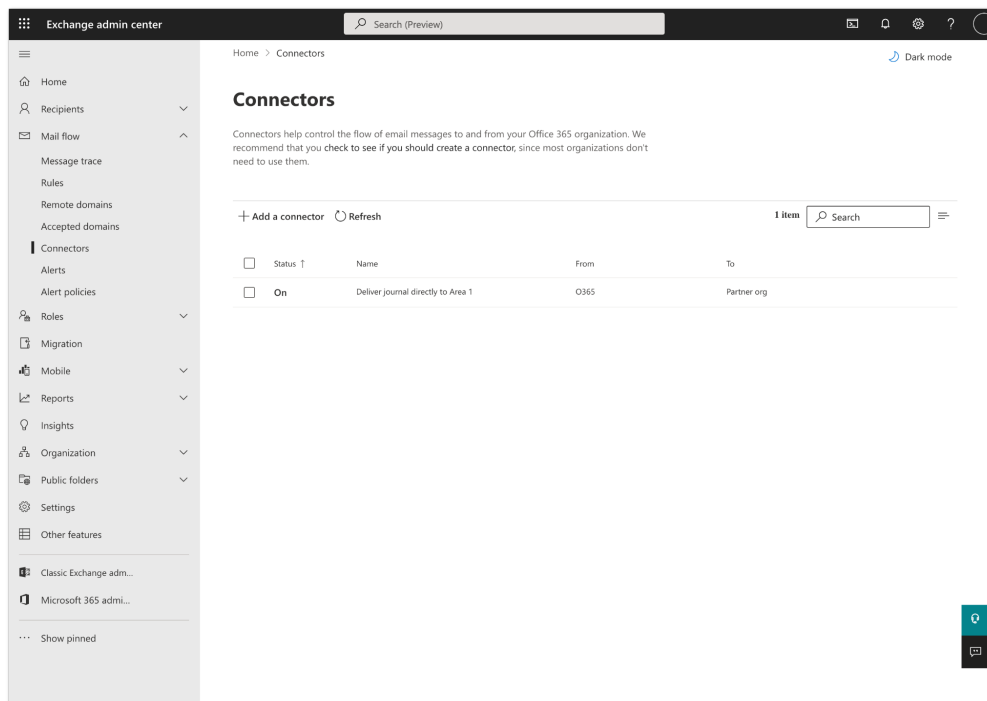
Task	Status
Check connectivity to 'mailstream-west.msrecord.io'	Succeed
Check connectivity to 'mailstream-east.msrecord.io'	Succeed
Send test email	Succeed

Back Next

- Review the configuration and click the **Create connector** button to save the configuration:



10. Once saved, the connector will be active:



Step 4: Configure Journal Rule

1. Open the Microsoft Purview compliance portal at <https://compliance.microsoft.com/homepage>
2. From the Purview compliance portal under the left menu, select **Data lifecycle management**, then select **Exchange (legacy)**
3. From the **Exchange (legacy)** page, select the **Settings** in the top right.



4. Enter the email address for a valid User account and select **Save**. Note: you cannot use a Team or Group address.

Exchange (legacy) > Settings

Settings

Undeliverable reports

Undeliverable reports ^

Specify an email address to receive journal reports when they are not deliverable to the address specified in the journal rule. This email address can't correspond with an Exchange Online mailbox. [Learn more about undeliverable reports](#)

Send undeliverable journal reports to: *

Enter an email address

Save

5. Select **Exchange (legacy)** in the menu or breadcrumbs near the top, then select the **Journal Rules** configuration section.

Exchange (legacy) Settings

MRM Retention policies MRM Retention tags Journal rules

ⓘ We do not recommend journaling content outside of Microsoft 365. We recommend using Microsoft Purview suite of solutions to help meet legal, regulatory and organizational compliance requirements. [Learn about Microsoft Purview](#)

Use journal rules to record all communications in support of your organization's email retention or archival strategy. [Learn about journaling in Exchange Online](#)

+ New rule Refresh 3 items Search

Name	Status	User	Send journal reports to
------	--------	------	-------------------------

6. Select **New rule** to configure a journaling rule, and configure the journaling rule as follows then select **Next**:

- Send journal reports to: This address is specific to each customer tenant and can be found in your Portal at

<https://horizon.area1security.com/support/service-addresses>

- If you are located in the EU or GDPR applies to your organization please ensure you are using a Connector with the smarthost set to mailstream-eu1.mxrecord.io as per the start of this guide.
- Journal Rule Name: Journal Messages to CloudflareArea 1
- Journal messages sent or received from: Everyone
- Type of message to journal: External messages only

Exchange (legacy) > Create journal rule

● Journal rule settings

○ Finish

Define journal rule settings

Messages matching the rule's conditions will be delivered to the journaling address specified in the rule. [Learn more to manage journaling in Exchange Online](#)

Send journal reports to *

journal_address@journaling.mxrecord.io

Journal rule name *

Journal Messages to CloudflareArea 1

Journal messages sent or received from *

☒ Everyone

☐ A specific user or group

Type of message to journal *

☐ All messages

☐ Internal messages only

☒ External messages only

Next Cancel

7. Verify the information is correct then select **Submit**.

Exchange (legacy) > Create journal rule

Journal rule settings

Finish

Review journal rule and finish

Send journal reports to
journal_address@journaling.mxrecord.io
[Edit](#)

Name
Journal Messages to CloudflareArea 1
[Edit](#)

Journal messages sent or received from
[Edit](#)

Type of message to journal
External messages only
[Edit](#)

Back

Submit

Cancel

8. Click **Done**. Once saved the rule is automatically active and may take a few minutes for the configuration to propagate and start to push messages to Cloudflare Area 1.

You can now access the Cloudflare Area 1 portal and you should see the number of messages processed counter increment as Journaled messages are sent to Cloudflare Area 1.

Restricting the Journal rule to specific users/groups:

Another option is to apply the Journal rule created in above step to some messages, the following can be enforced:

- **Journal messages sent or received from:** [A specific user or group]

Microsoft Purview

Exchange (legacy) > Create journal rule

Journal rule settings

Finish

Define journal rule settings

Messages matching the rule's conditions will be journalized. [Manage journaling in Exchange Online](#)

Send journal reports to *

journal_recipient@journaling.mxrecord.io

Journal rule name *

Journal Messages to CloudflareArea 1

Journal messages sent or received from *

☐ Everyone

☒ A specific user or group

Select a user or group

Type of message to journal *

☐ All messages

☐ Internal messages only

☒ External messages only

Next

Select a user or group to journal

Search for specific people

1 selected

Name	Email address
wattnias.koenier	wattnias.k@someemocorp.com
Nick Perry	Nick@someemocorp.com
PilotUsers	PilotUsers@someemocorp.com
RBACDistribution	Alton2@someemocorp.com
RBACMailEnableSecurity	Alton3@someemocorp.com
Recoverable items	RecoverableItems@someemocorp.onmicroso...
Scott Harris	scott.harris@someemocorp.com
Seiya Tanaka	Seiya@someemocorp.com
someemocorp Bcc Address	someemocorp.com@mxrecord.io
<input checked="" type="checkbox"/> Test	Test@someemocorp.com
test	test_arun@someemocorp.com
Todd Murray	todd@someemocorp.onmicrosoft.com

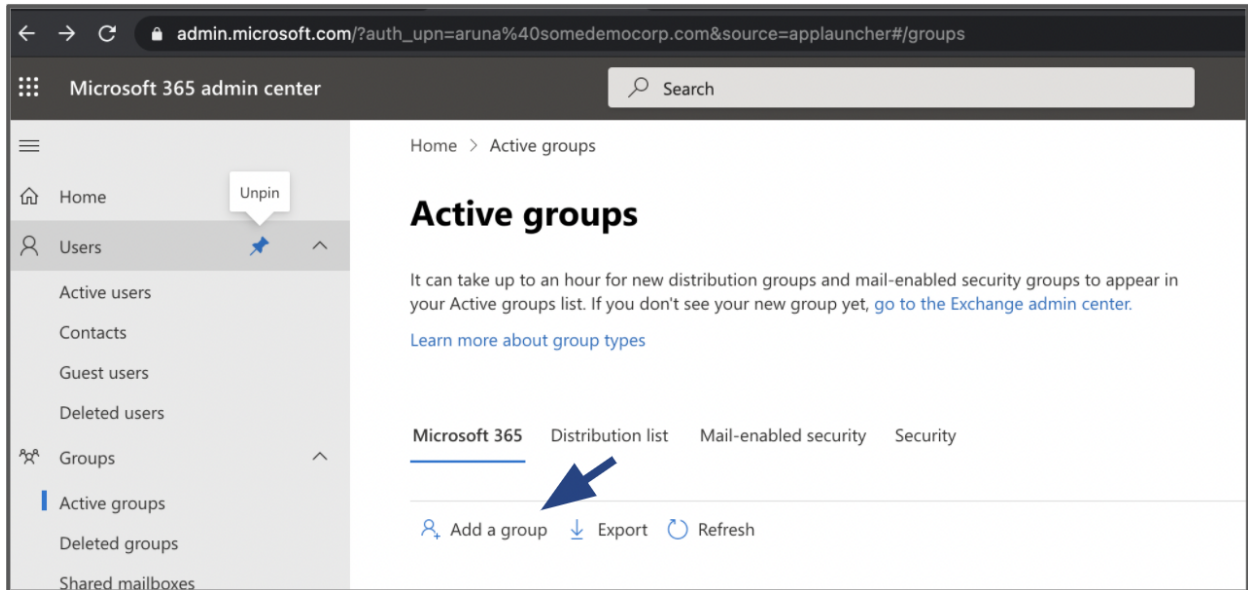
Add Cancel

- From the window that pops up with the list of users/groups, select the corresponding distribution group.

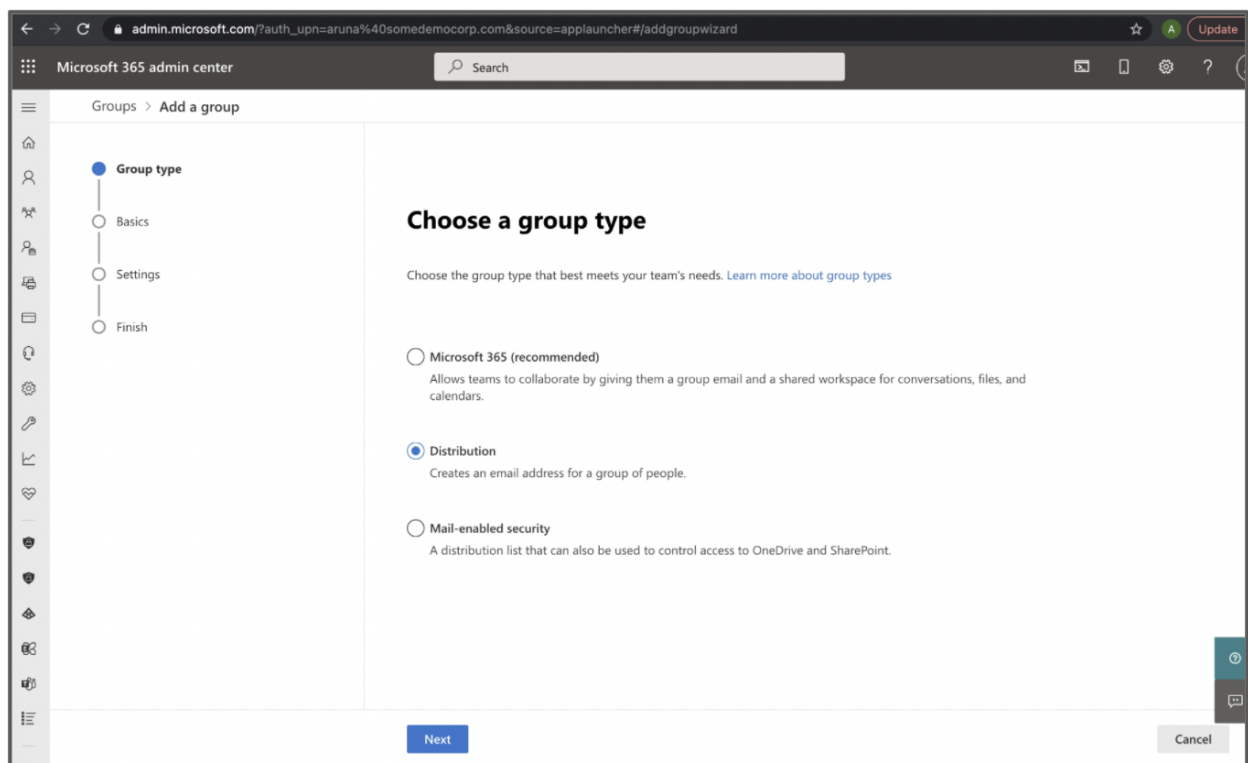
Creating distribution group in O365

If you do not have a distribution group yet, you can follow the below steps to create one.

Navigate to: Microsoft Exchange Admin Center > Home > Active Groups



Click 'Add a group' > Select 'Distribution' > Click Next



Enter a group name > Click Next > And hit 'Create Group'

The screenshot shows the 'Add a group' wizard in the Microsoft 365 admin center. The left sidebar indicates the progress: 'Group type' (checked), 'Basics' (checked), 'Settings' (active), and 'Finish' (disabled). The main content area is titled 'Edit settings' and shows the 'Distribution group' settings. The 'Group email address' field is set to 'Test' with a dropdown menu showing 'somedemocorp.com'. Below this, there is a 'Communication' section with a checkbox 'Allow people outside of my organization to send email to this Distribution group' which is currently unchecked. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

Navigate to the corresponding distribution group created and add the users:

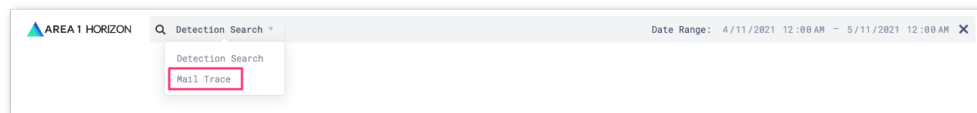
The screenshot shows the 'Active groups' page in the Microsoft 365 admin center. The left sidebar shows the navigation menu with 'Groups' > 'Active groups' selected. The main content area shows a list of distribution groups. A blue arrow points to the 'Test' group in the list.

Group name ↑	Group email	Sync status	Created on	Choose columns
List	list@o365.somedemocorp.com	☁	March 23, 2017, 5:58 AM	
RBACDistribution	Alton2@somedemocorp.com	☁	October 18, 2020, 7:18 PM	
test	test_arun@somedemocorp.com	☁	August 26, 2021, 2:35 PM	
Test	Test@somedemocorp.com	☁	August 27, 2021, 12:42 PM	

Manual Message Retraction

When retraction is enabled, this also allows you to manually retract messages that were not automatically retracted, for example a message was inadvertently sent to a few recipients and you've been requested to retract the message from their inbox.

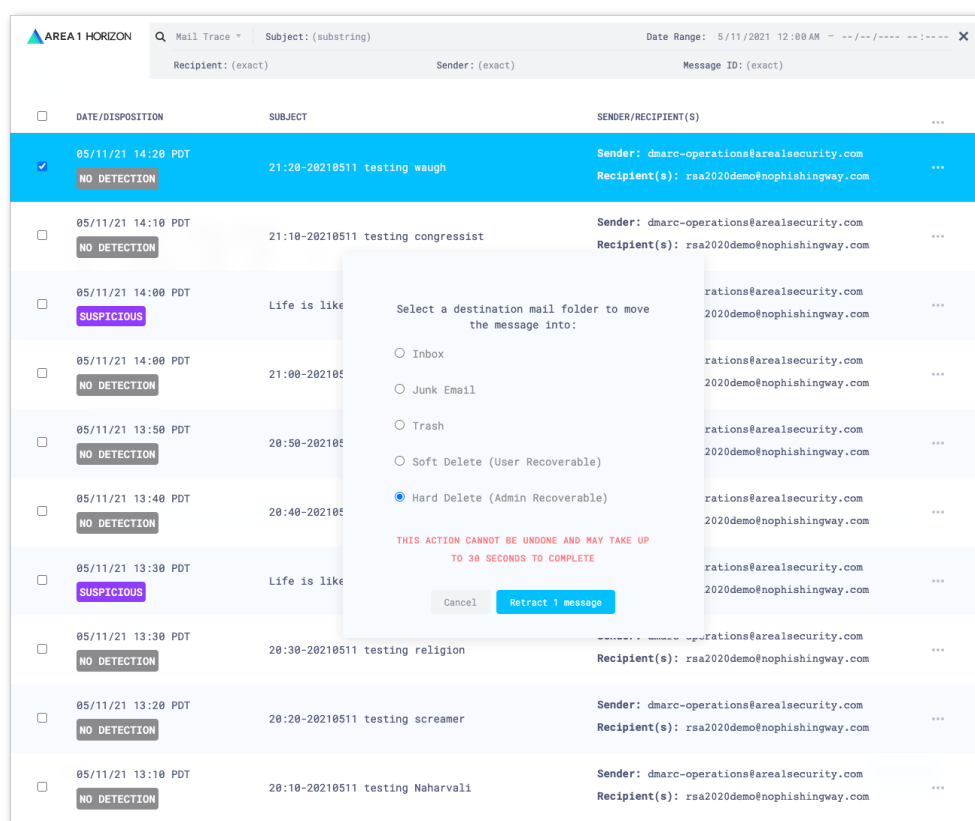
1. To manually retract a message, you will first need to find the message to retract. Access the Mail Trace search function by clicking the Search bar on top of the portal and using the dropdown to change the search type to Mail Trace:



2. This will update the search dialog and allow you to search for the messages to retract, once you have entered the correct search parameters, you will be presented with the messages that match the search criteria. To retract a single message, click the ... icon associated with the message and select the **Retract** option. If you'd like to retract multiple messages, you can select the messages in question by clicking the associated checkbox on the left side of the results:



3. Clicking the **Retract** action, will bring up a dialog giving you the option to decide where you want to retract the message:



4. Once you click the **Retract Message** button, if the message was successfully retracted, you will receive a positive confirmation on the lower right corner of the Portal:

