
Email Security for Microsoft O365

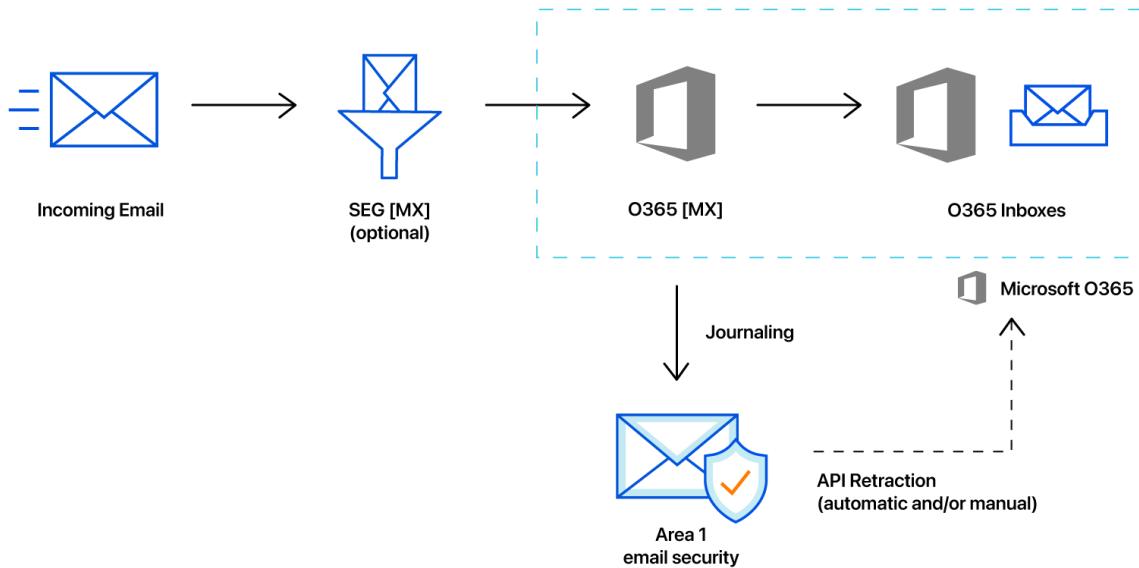
Deployment and Configuration Guide
Automatic Message Retraction

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 Synchronizer) 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 Azure Active Directory Admin Center interface. The left sidebar navigation includes: Dashboard, Enterprise applications, Area 1 Security Synchronizer ((Production Portal)), Manage (Properties, Owners, Roles and administrators, Users and groups, Single sign-on, Provisioning, Self-service, Custom security attributes (preview)), Security (Conditional Access, Permissions, Token encryption), Activity (Sign-in logs, Usage & insights, Audit logs, Provisioning logs, Access reviews). The main content area is titled 'Area 1 Security Synchronizer ((Production Portal)) | Permissions'. It features a 'Refresh' button, a 'Review permissions' link, and a 'Got feedback?' link. A large blue button labeled 'Grant admin consent for Area 1 Security' is prominently displayed. Below it, tabs for 'Admin consent' and 'User consent' are visible, with 'Admin consent' being the active tab. A search bar labeled 'Search permissions' is present. A table lists permissions granted to Microsoft Graph:

API Name	Claim value	Permission	Type	Granted through
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

- 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:

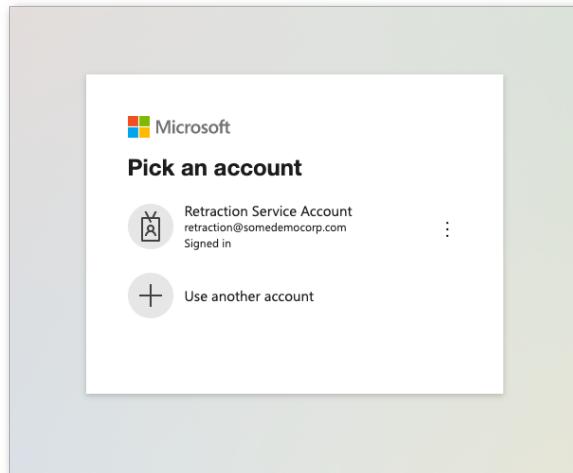
The screenshot shows the 'Email Configuration' section of the Area 1 Horizon portal. On the left, a sidebar lists several categories: DOMAINS & ROUTING (Domains, Alert Webhooks, Partner Domains TLS), EMAIL POLICIES (ALLOW LIST, BLOCK LIST, ENHANCED DETECTIONS), and RETRACT SETTINGS. The 'RETRACT SETTINGS' option is highlighted with a red box. The main panel displays a table titled 'All Domains' with columns: DOMAIN, FORWARDING TO, POSITION, RESTRICTED IPS, and TLS. Two domains are listed: 'examplecorpora...' and 'examplecorpora...'. Under 'TLS', for the first domain, 'Inbound' is marked with a yellow exclamation icon and 'Outbound' is marked with a green checkmark. A '...' button is also present.

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

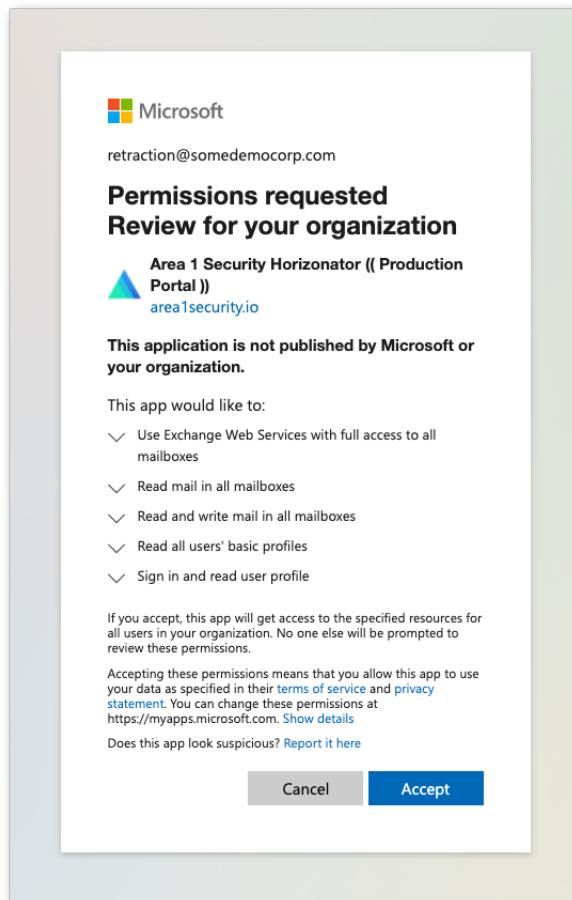
2. In the Retraction Settings section, you will need to authorize Area 1 to execute retractions through O365's Graph API. This is a simple process that requires you to authenticate and authorize Area 1 with O365. Ensure that the account that you will be using to authenticate has the appropriate administrative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

The screenshot shows the 'Email Configuration' section of the Area 1 Horizon Portal. On the left, there is a sidebar with several tabs: 'DOMAINS & ROUTING', 'EMAIL POLICIES', 'ALLOW LIST', 'BLOCK LIST', 'ENHANCED DETECTIONS', 'RETRACT SETTINGS', 'Authentication' (which is currently selected), and 'Auto-Retract'. The main content area is titled 'Authentication' and contains the message: 'For the retract feature to work, you must be authenticated.' Below this, it says 'MICROSOFT OFFICE 365' and features a blue 'Authorize' button. The 'Authorize' button is highlighted with a red rectangular box.

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:

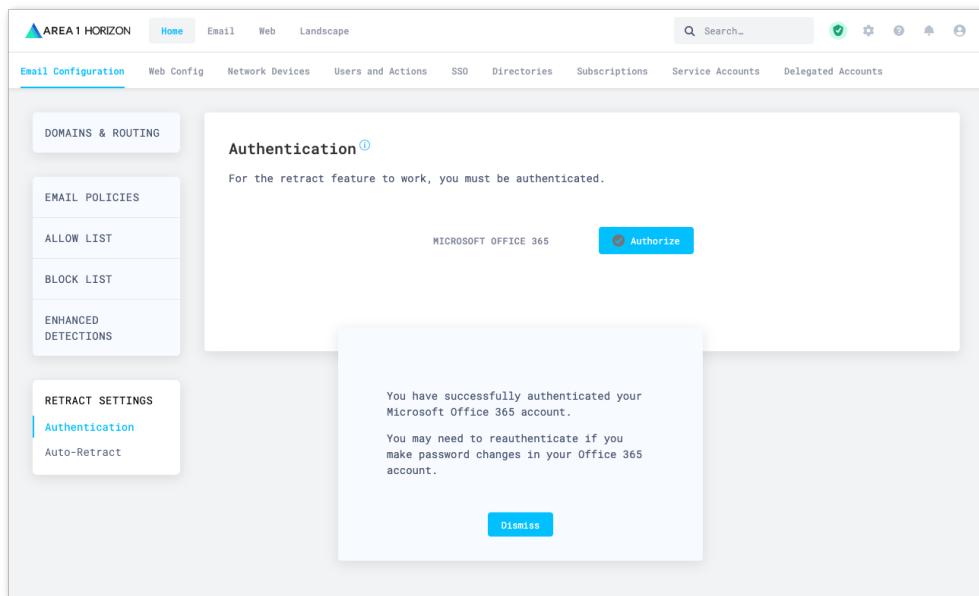


Does this app look suspicious? [Report it here](#)

Cancel

Accept

- 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.

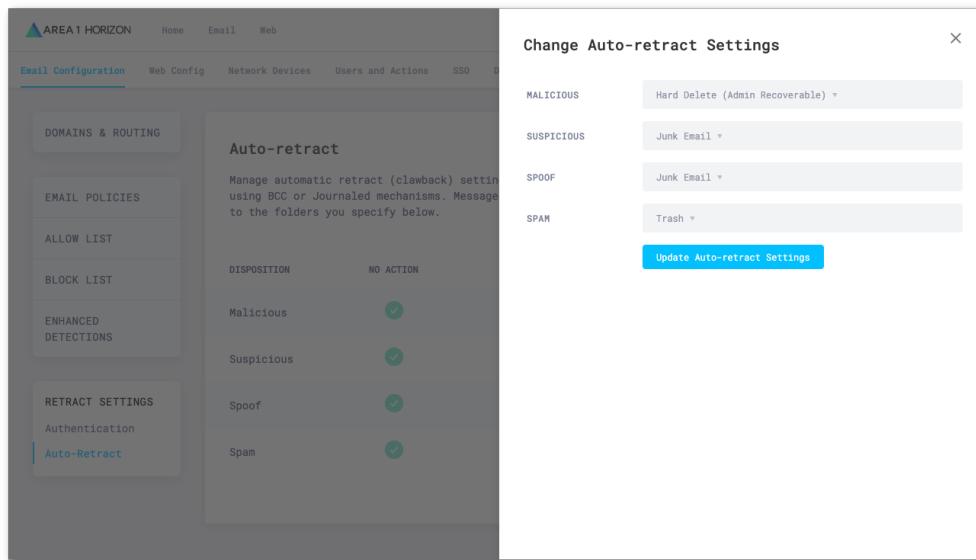
1. Click the **Auto-Retract** option on the left navigation bar to access retraction behavior setting:

The screenshot shows the 'Email Configuration' section of the Area 1 Horizon interface. On the left, there's a sidebar with 'RETRACT SETTINGS' selected, which contains 'Authentication' and 'Auto-Retract'. The main panel is titled 'Authentication' and contains a message: 'For the retract feature to work, you must be authenticated.' Below this is a 'MICROSOFT OFFICE 365' section with an 'Authorize' button. The 'Auto-Retract' button in the sidebar is highlighted with a red box.

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

The screenshot shows the 'Email Configuration' section of the Area 1 Horizon interface. On the left, there's a sidebar with 'RETRACT SETTINGS' selected, which contains 'Auto-Retract'. The main panel is titled 'Auto-retract' and contains a table for managing automatic retract (clawback) settings. The table has columns for 'DISPOSITION', 'NO ACTION', 'TRASH', 'JUNK EMAIL', 'SOFT DELETE (USER RECOVERABLE)', and 'HARD DELETE (ADMIN RECOVERABLE)'. Rows in the table include 'Malicious', 'Suspicious', 'Spoof', and 'Spam', each with a green checkmark in the 'NO ACTION' column. An 'Edit' button in the top right corner of the main panel is highlighted with a red box.

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



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

Auto-retract						... Edit
DISPOSITION	NO ACTION	TRASH	JUNK EMAIL	SOFT DELETE (USER RECOVERABLE)	HARD DELETE (ADMIN RECOVERABLE)	
Malicious	-	-	-	-	-	<input checked="" type="checkbox"/>
Suspicious	-	-	<input checked="" type="checkbox"/>	-	-	
Spoof	-	-	<input checked="" type="checkbox"/>	-	-	
Spam	-	<input checked="" type="checkbox"/>	-	-	-	

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..

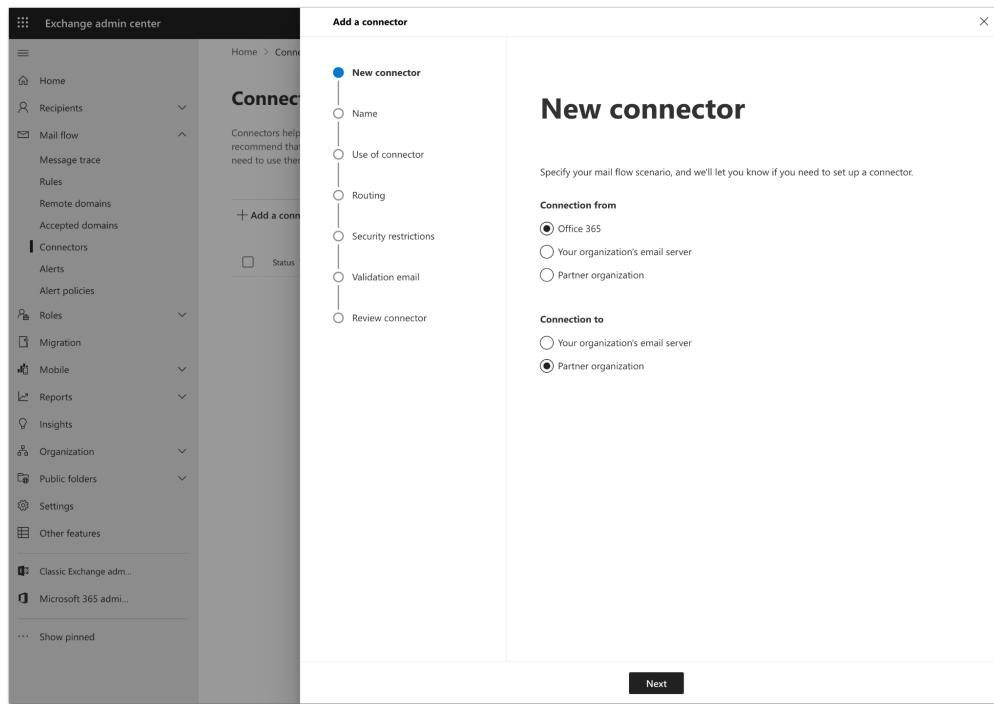
If your email architecture requires outbound messages to traverse your email gateway, you may want to consider configuring a connector to send the journal messages directly to Area 1.

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

The screenshot shows the Exchange admin center interface. The left sidebar has a 'Mail flow' section with several options: Message trace, Rules, Remote domains, Accepted domains, Connectors (which is selected and highlighted with a red box), Alerts, Alert policies, Roles, Migration, Mobile, Reports, Insights, Organization, Public folders, Settings, and Other features. Below this are pinned items for Classic Exchange admin and Microsoft 365 admin. At the bottom of the sidebar is a 'Show pinned' link. The main content area is titled 'Connectors' and contains a brief description: 'Connectors help control the flow of email messages to and from your Office 365 organization. We recommend that you check to see if you should create a connector, since most organizations don't need to use them.' Below this is a button '+ Add a connector' and a search bar. A table header row is visible with columns for Status, Name, From, and To. A message 'No data available' is displayed below the table. The top right corner of the main content area has a 'Dark mode' switch.

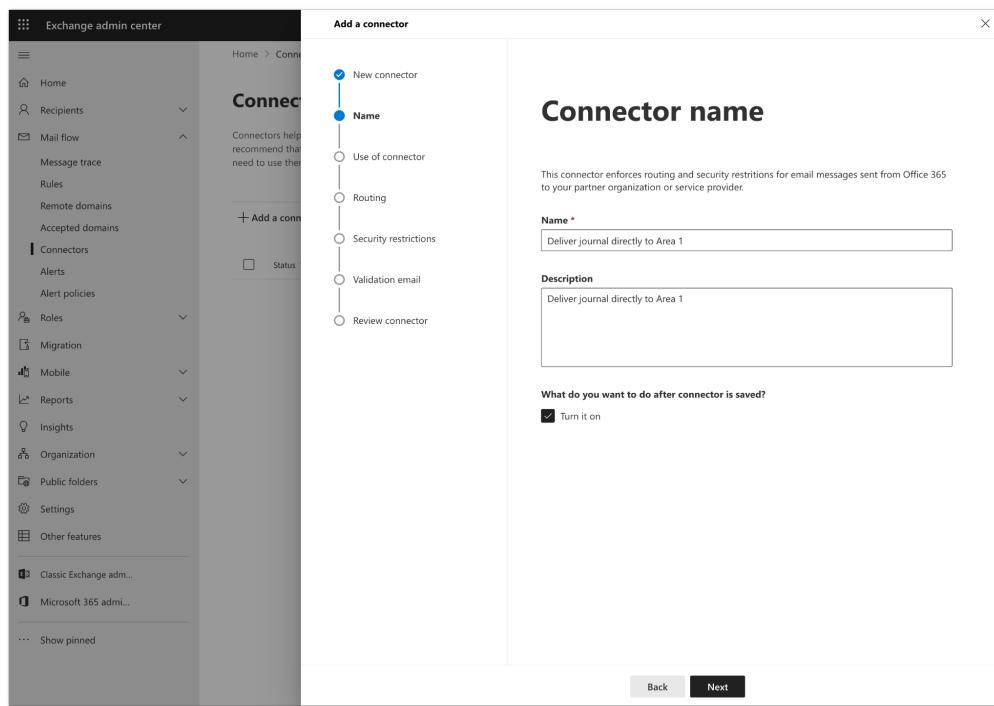
2. Click the **+ Add a connector** button to configure a new connector and configure the connector mail direction as follows:

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



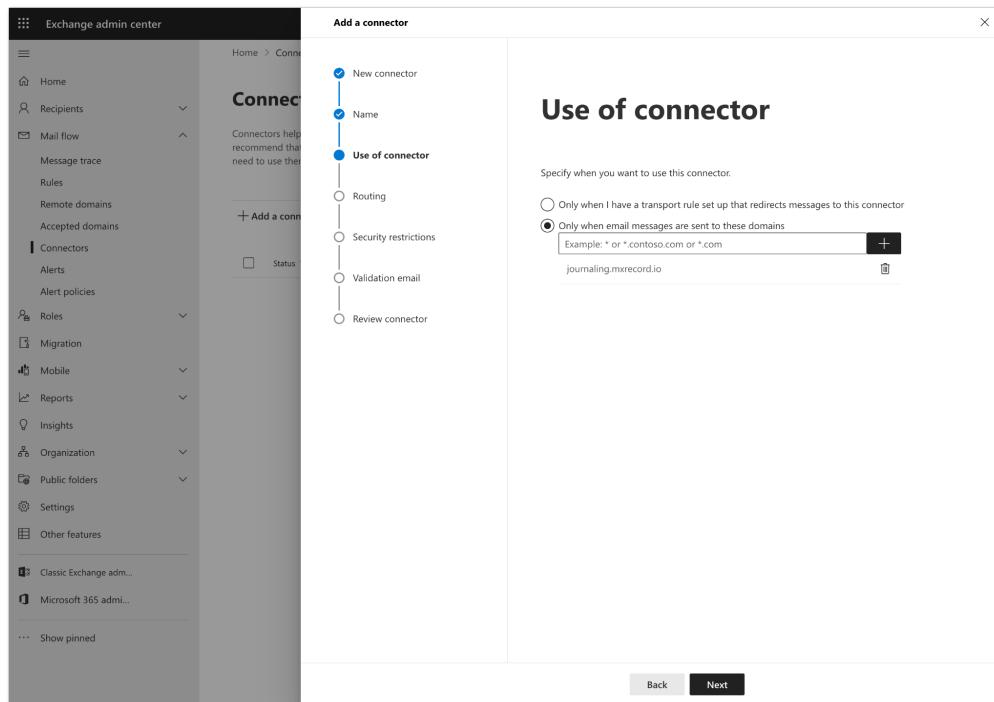
3. Configure the connector name and description:

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



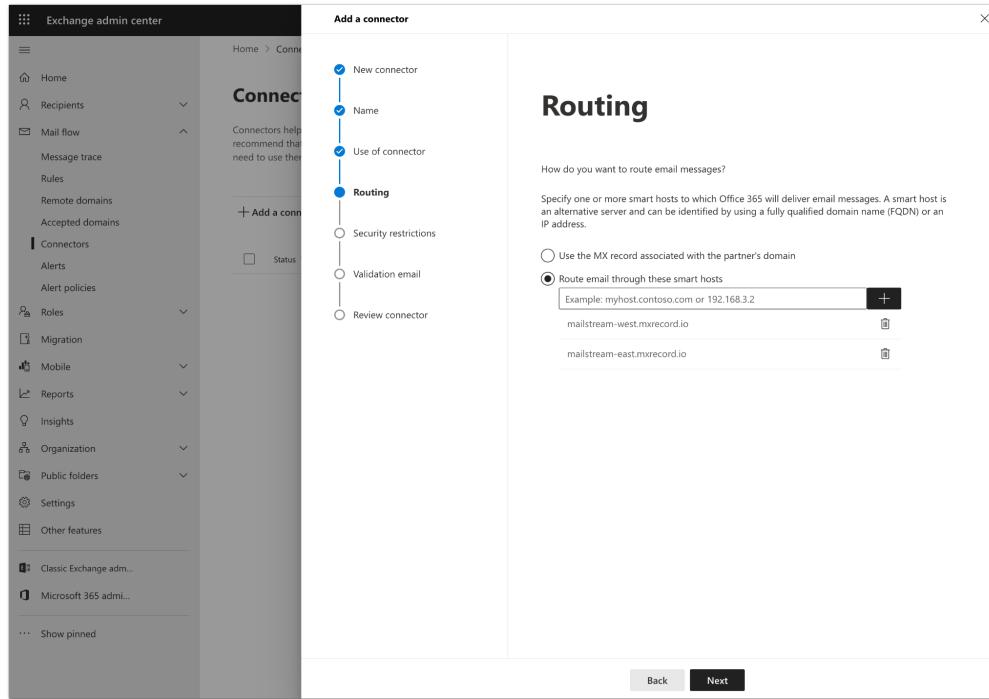
4. Configure the **Use of connector** setting:

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



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:

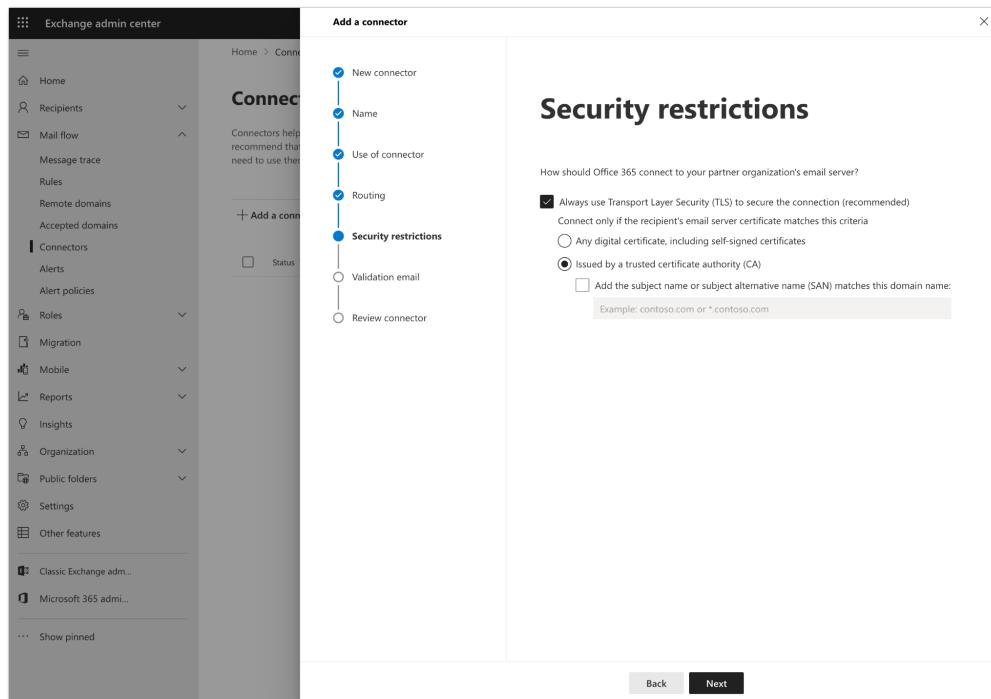
- mailstream-east.mxrecord.io
- mailstream-west.mxrecord.io



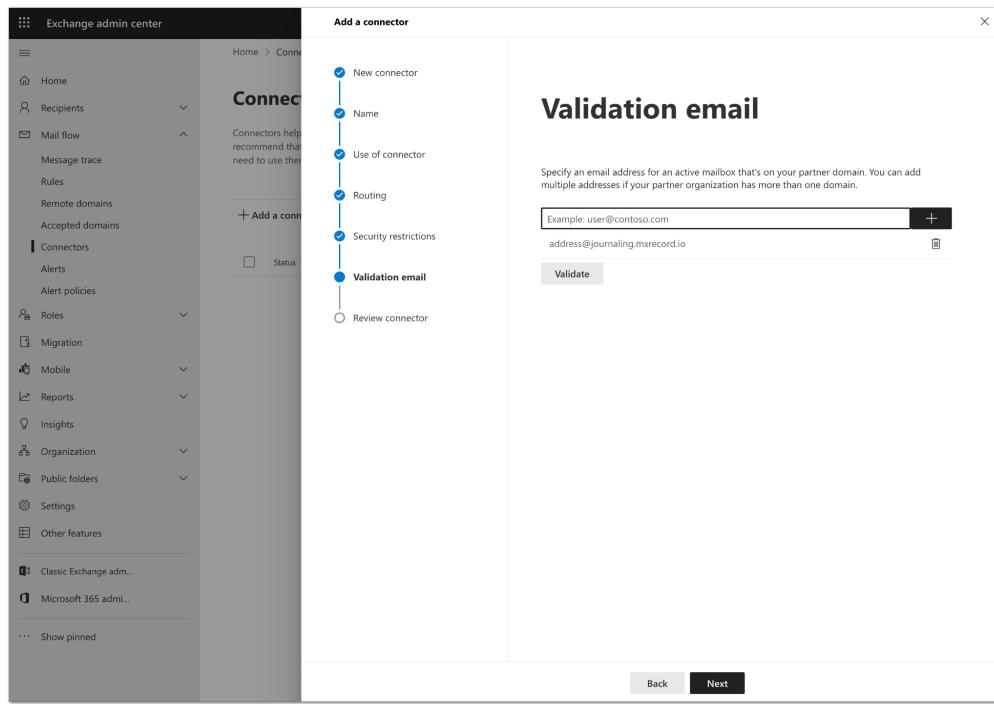
If there is a requirement to enforce traffic through the EU region use the following smarthost instead:

- mailstream-eu1.mxrecord.io

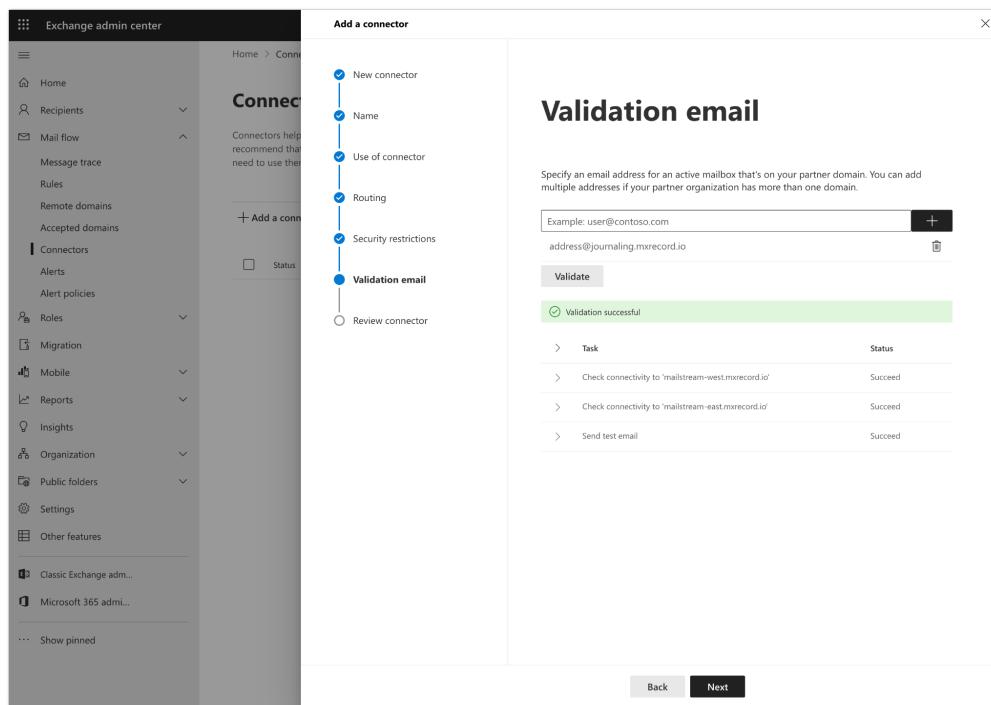
6. Preserve the default TLS configuration:



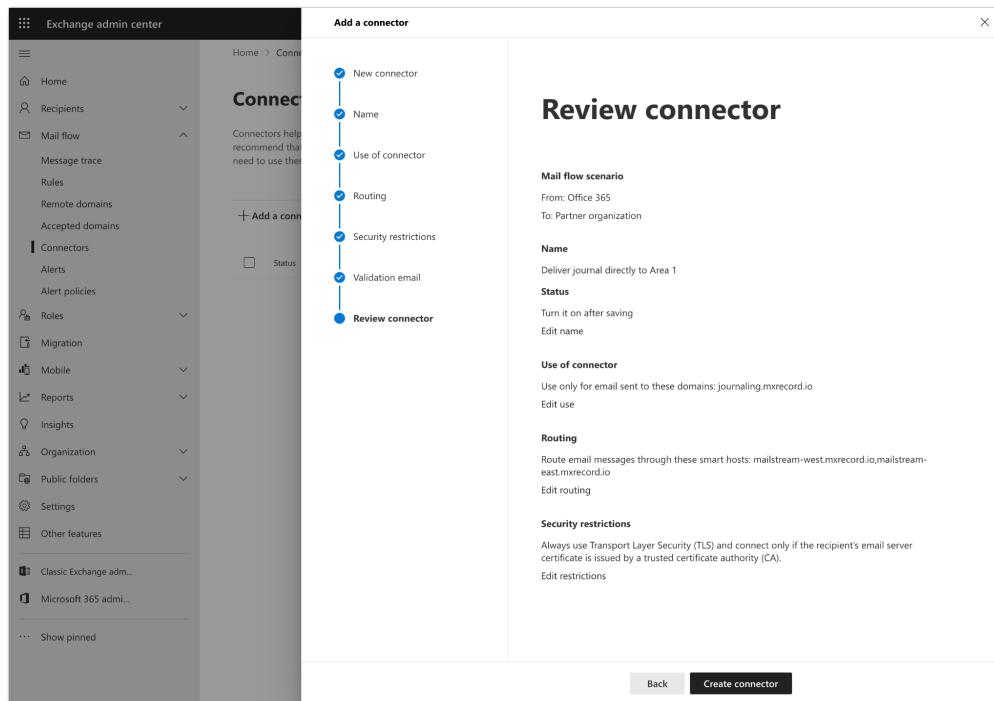
7. Validate the connector by using your tenant's specific journaling address. This address can be found in the Area 1 Horizon portal in the Support > Service Addresses page (<https://horizon.area1security.com/support/service-addresses>):



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



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



10. Once saved, the connector will be active:

The screenshot shows the Exchange admin center interface. The left sidebar is titled "Exchange admin center" and contains a navigation menu with the following items: Home, Recipients, Mail flow (with sub-options: Message trace, Rules, Remote domains, Accepted domains), Connectors (selected), Alerts, Alert policies, Roles, Migration, Mobile, Reports, Insights, Organization, Public folders, Settings, Other features, Classic Exchange adm..., Microsoft 365 adm..., and Show pinned. The main content area is titled "Connectors" and includes a sub-header: "Connectors help control the flow of email messages to and from your Office 365 organization. We recommend that you check to see if you should create a connector, since most organizations don't need to use them." Below this is a table with one item:

<input type="checkbox"/>	Status	Name	From	To
<input type="checkbox"/>	On	Deliver journal directly to Area 1	O365	Partner org

At the top right of the main content area, there is a "Dark mode" toggle switch, a search bar with the placeholder "Search (Preview)", and a "1 item" indicator.

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)



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 rule name *

Journal messages sent or received from *

Everyone
 A specific user or group

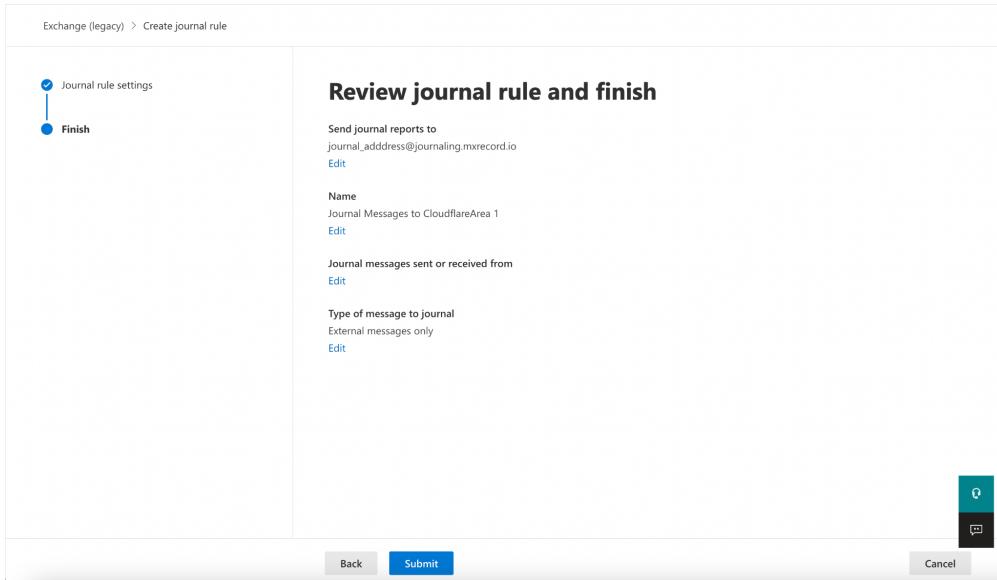
Type of message to journal *

All messages
 Internal messages only
 External messages only

 **Submit**

 **Cancel**

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



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 Jounaled 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]**

The screenshot shows the Microsoft Purview interface for creating a journal rule. On the left, there's a navigation pane with 'Journal rule settings' selected. The main area is titled 'Define journal rule set'. It includes fields for 'Send journal reports to' (set to 'journal_recipient@journaling.mxrecord.io'), 'Journal rule name' (set to 'Journal Messages to CloudflareArea 1'), and 'Journal messages sent or received from' (with 'A specific user or group' selected). Below these are options for 'Type of message to journal' (with 'External messages only' selected). At the bottom of this panel are 'Next' and 'Cancel' buttons. To the right, a modal window titled 'Select a user or group to journal' is open. It has a search bar and a list of users with one item selected: 'Test'. There are 'Add' and 'Cancel' buttons at the bottom of the modal.

- 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

The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar is pinned, with 'Unpin' highlighted. The main content area is titled 'Active groups'. It includes a note about distribution groups appearing within an hour, a link to the Exchange admin center, and tabs for Microsoft 365, Distribution list, Mail-enabled security, and Security. Below the tabs are buttons for 'Add a group', 'Export', and 'Refresh'. A blue arrow points to the 'Add a group' button.

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

The screenshot shows the 'Add a group' wizard. On the left, a sidebar lists steps: Group type (selected), Basics, Settings, and Finish. The main panel is titled 'Choose a group type' with the sub-instruction 'Choose the group type that best meets your team's needs. Learn more about group types'. It lists three options: 'Microsoft 365 (recommended)', 'Distribution' (which is selected), and 'Mail-enabled security'. A blue arrow points to the 'Distribution' option. At the bottom are 'Next' and 'Cancel' buttons.

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 shows a navigation tree with 'Groups' selected. The main area is titled 'Edit settings' for a 'Distribution group'. It includes fields for 'Group email address' (set to 'Test'@'somedemocorp.com') and 'Communication' (with an unchecked checkbox for sending email outside the organization). At the bottom are 'Back', 'Next', and 'Cancel' buttons.

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

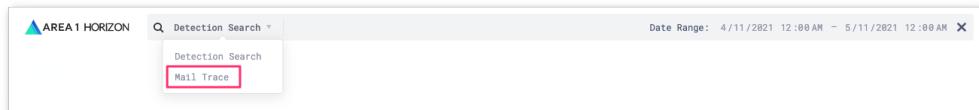
The screenshot shows the 'Active groups' page in the Microsoft 365 admin center. The left sidebar shows a navigation tree with 'Groups' selected. The main area is titled 'Active groups' and lists four items: 'List', 'RBACDistribution', 'test', and 'Test'. A blue arrow points to the 'Test' entry in the 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.

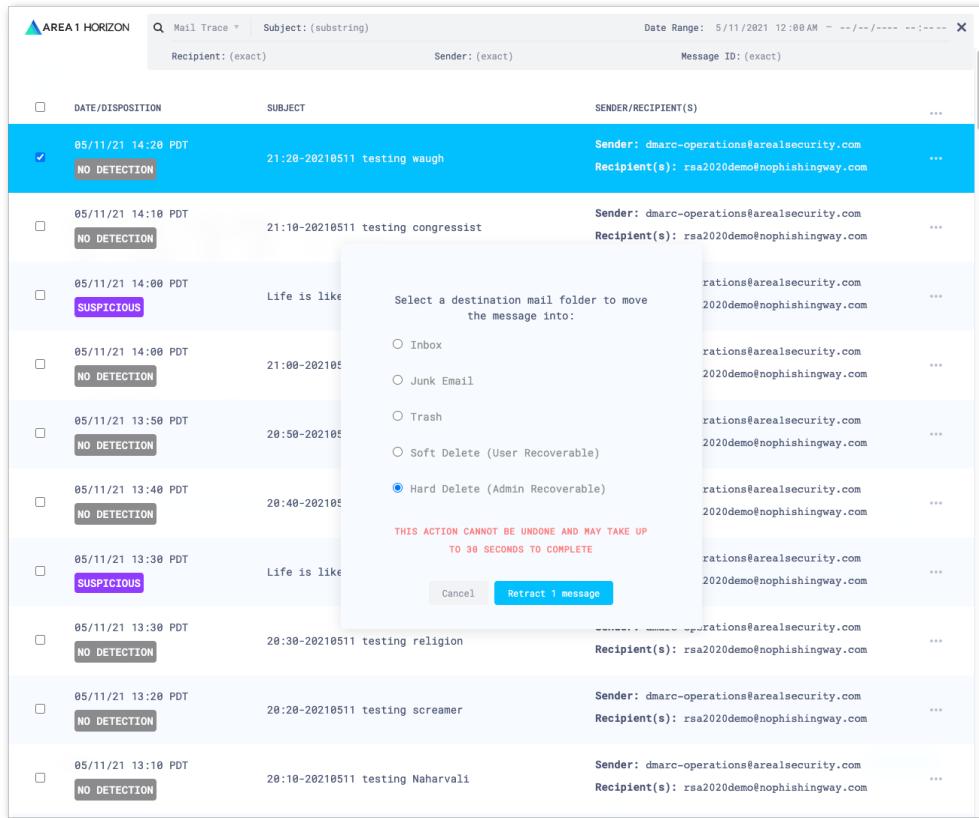
1. To manually retract a message, you will first need to find the message to retract. Access the Mail Trace search function by clicking the Search bar on top of the portal and using the dropdown to change the search type to Mail Trace:



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:



- 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:

The screenshot shows a list of messages in the Mail Trace interface. Each message row includes the date and time, subject, and detection status (e.g., NO DETECTION, SUSPICIOUS). The last message in the list has a green box at the bottom right containing the text "The message was successfully retracted.".

DATE/DISPOSITION	SUBJECT	SENDER/RECIPIENT(S)
05/11/21 14:20 PDT NO DETECTION	21:20-20210511 testing waugh	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com
05/11/21 14:10 PDT NO DETECTION	21:10-20210511 testing congressist	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com
05/11/21 14:00 PDT SUSPICIOUS	Life is like a box of chocolates Pearl...	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com
05/11/21 14:00 PDT NO DETECTION	21:00-20210511 testing Acipenseroidae	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com
05/11/21 13:50 PDT NO DETECTION	20:50-20210511 testing apathistical	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com
05/11/21 13:40 PDT NO DETECTION	20:40-20210511 testing uncolleged	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com
05/11/21 13:30 PDT SUSPICIOUS	Life is like a box of chocolates Pearl...	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com
05/11/21 13:30 PDT NO DETECTION	20:30-20210511 testing religion	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com
05/11/21 13:20 PDT NO DETECTION	20:20-20210511 testing screamer	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com
05/11/21 13:10 PDT NO DETECTION	20:10-20210511 testing Naharvali	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com

The message was successfully retracted.