CLOUDFLARE
AREA 1 SECURITY

Email Security for Microsoft O365

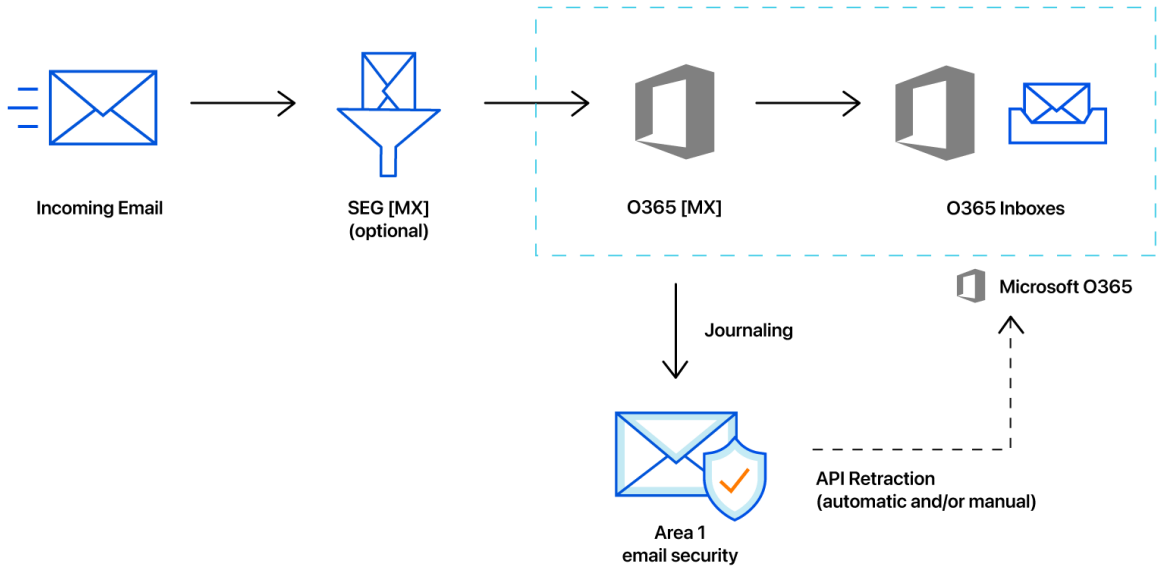
Deployment and Configuration Guide
Automatic Message Retraction

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

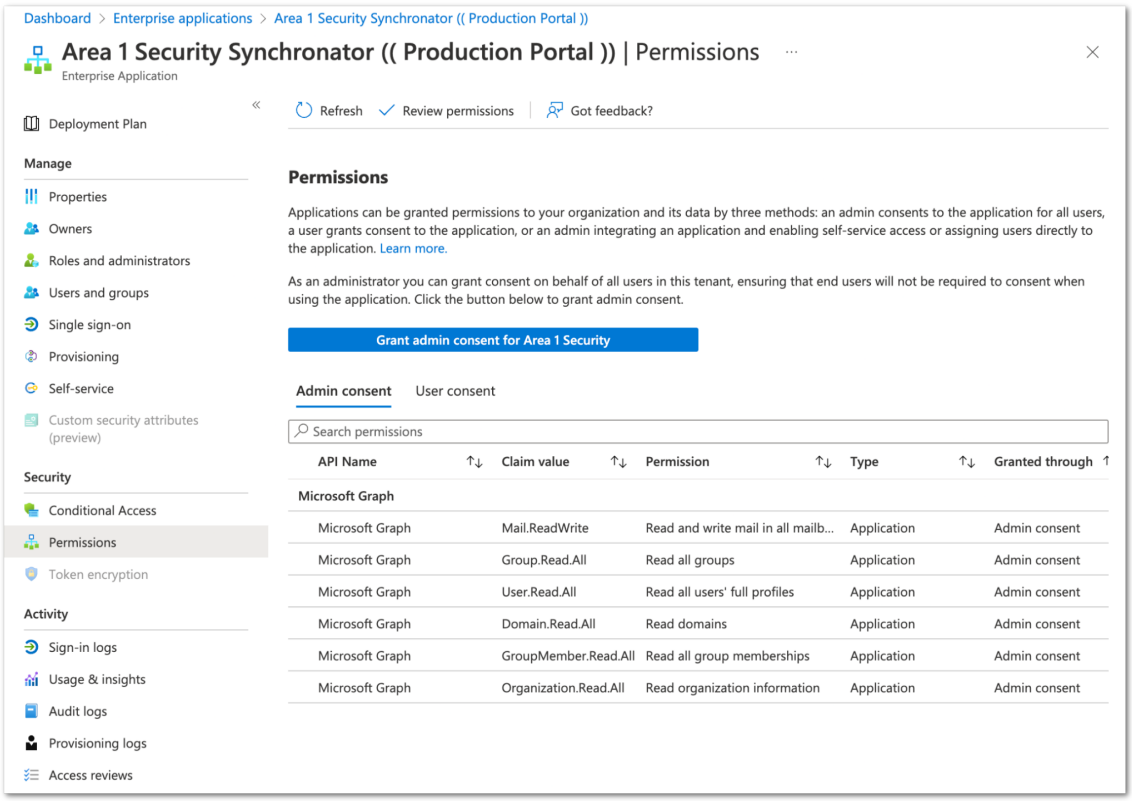
Step 1: Authorize Area 1 with O365 for Retraction

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.

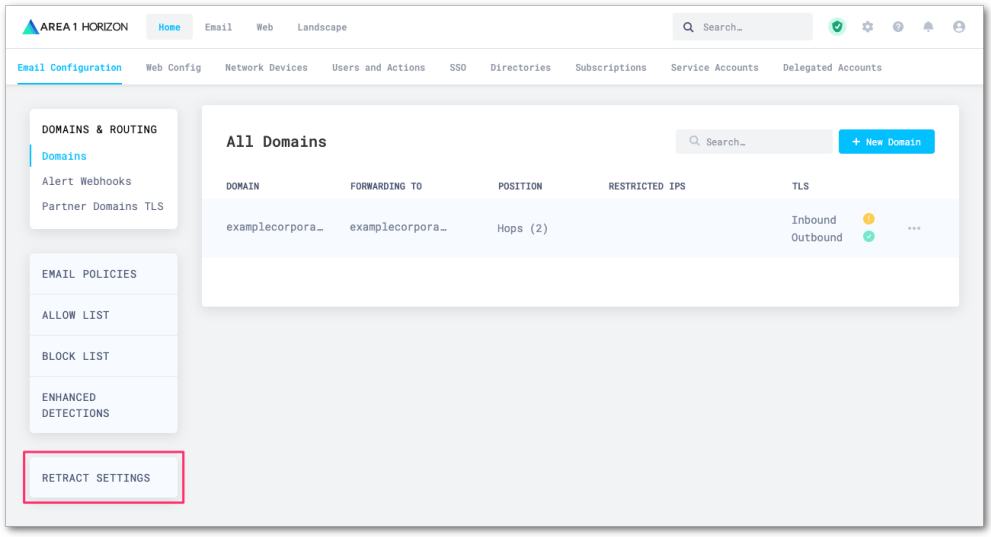
When assigning user roles in the O365 console, you will find these roles under the **Identity** admin roles in the Roles configuration section of the user permissions.

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.

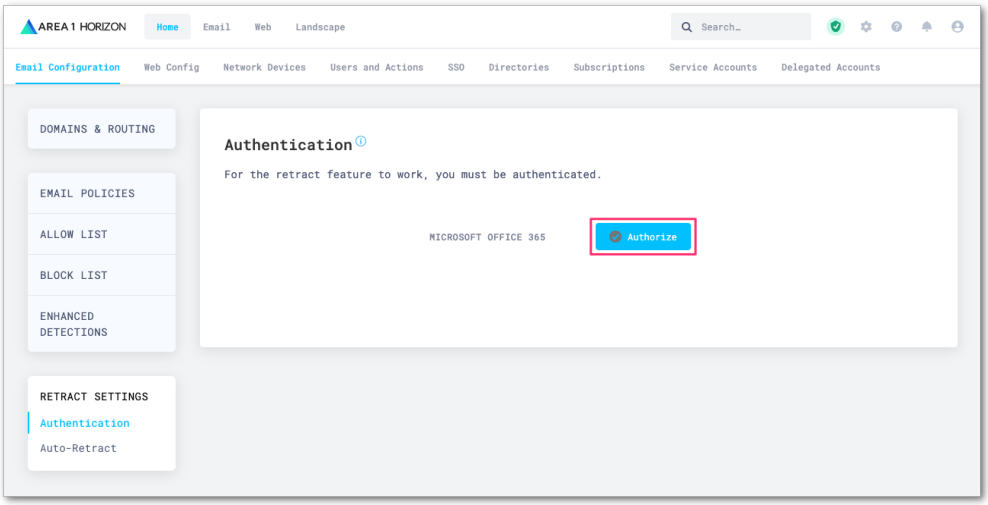


1. From the Area 1 Horizon Portal, access the Email Configuration section (https://horizon.area1security.com/settings/email/routing/domains) and select the **Retraction Settings** option on the left navigation bar:

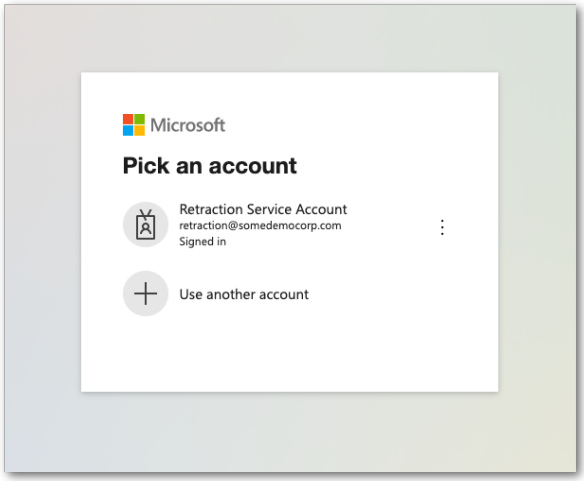


Note: If you do not see the **Retract Settings** option, please contact customer support to enable the feature.

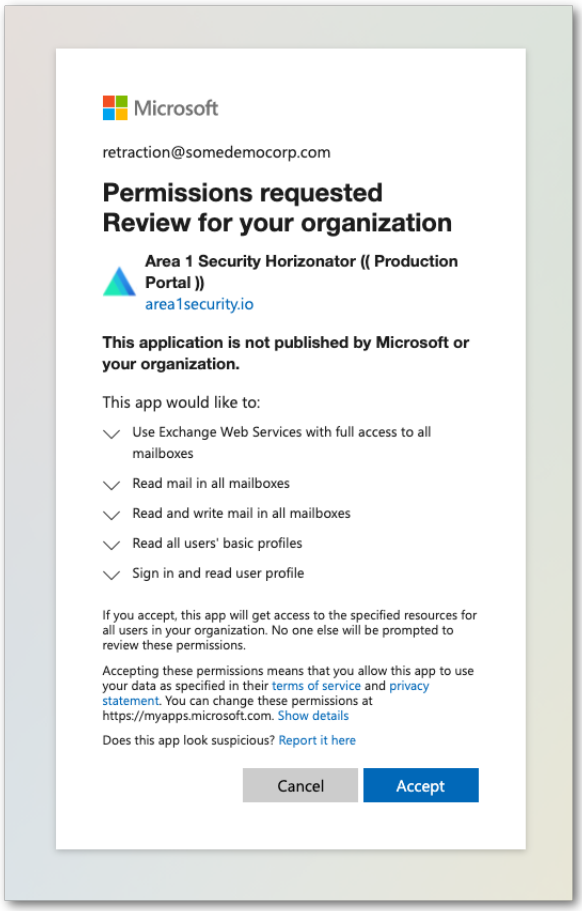
2. In the Retraction Settings section, you will need to authorize Area 1 to execute retractions through O365's Graph API. This is a simple process that requires you to authenticate and authorize Area 1 with O365. Ensure that the account that you will be using to authenticate has the appropriate administrative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



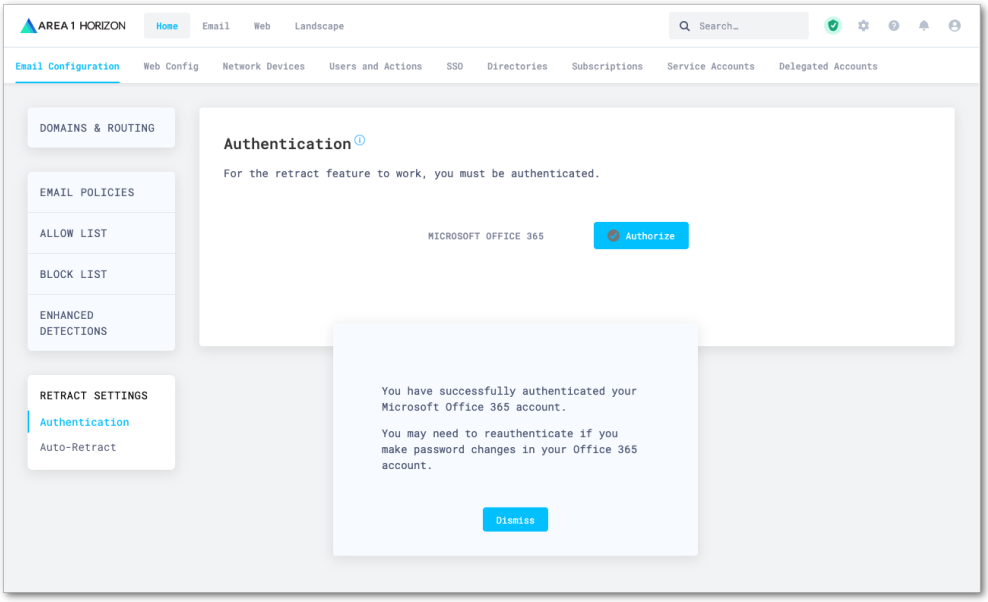
3. The Area 1 Horizon Portal will redirect you to a Microsoft Login page, select or enter the appropriate account to initiate for the authentication process:



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



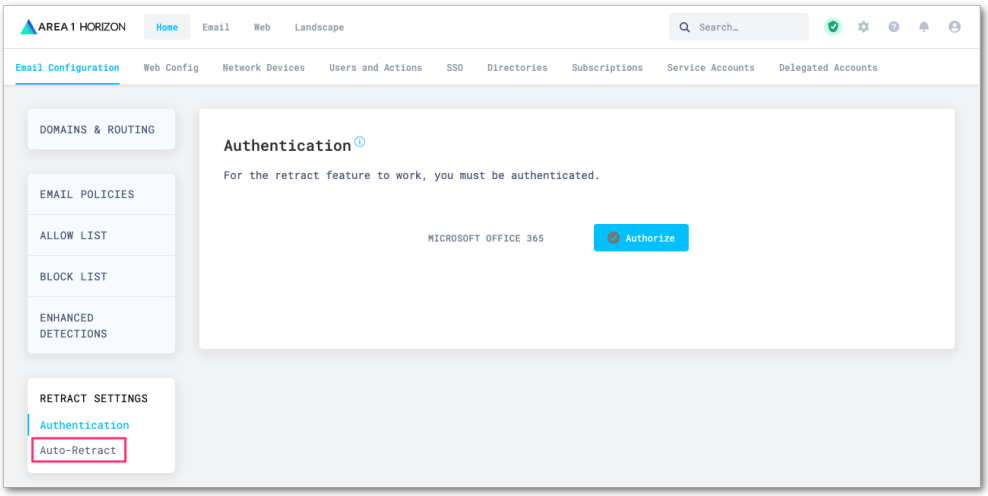
5. Upon authorization, you will be automatically redirected to the Area 1 Portal, with a notification that the authorization successfully completed, you may click **Dismiss** to clear the notification:



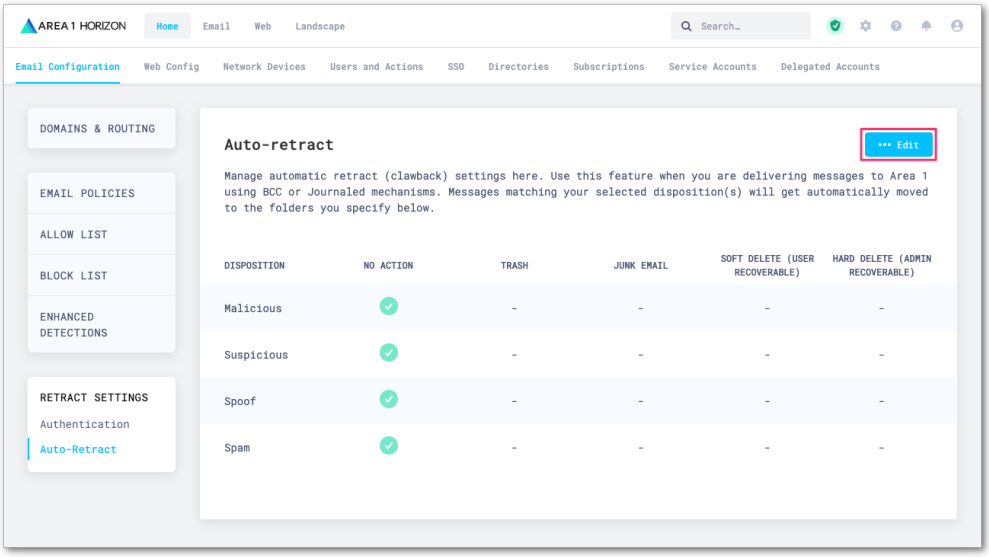
Step 2: Configure Auto-Retraction Actions

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

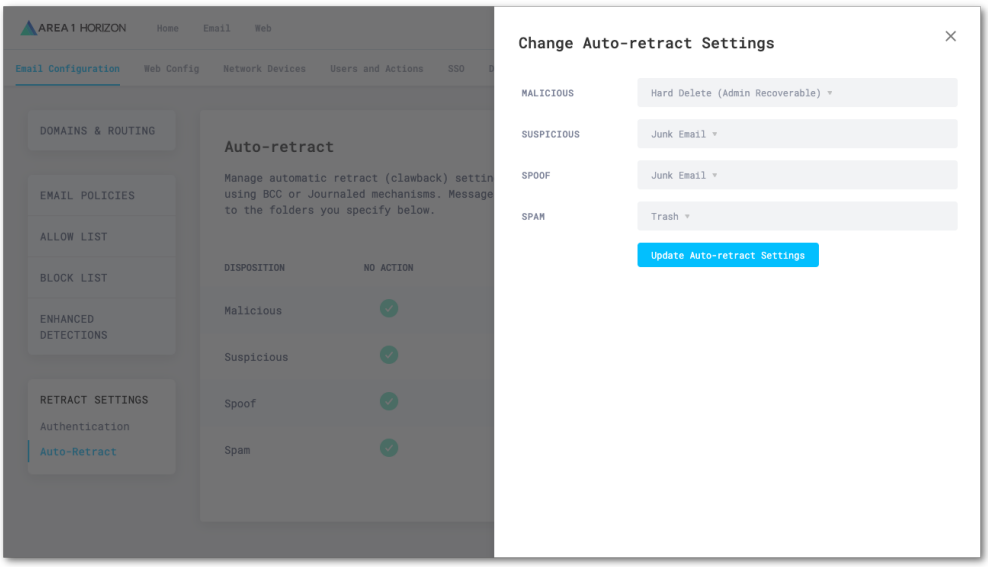
1. Click the **Auto-Retract** option on the left navigation bar to access retraction behavior setting:



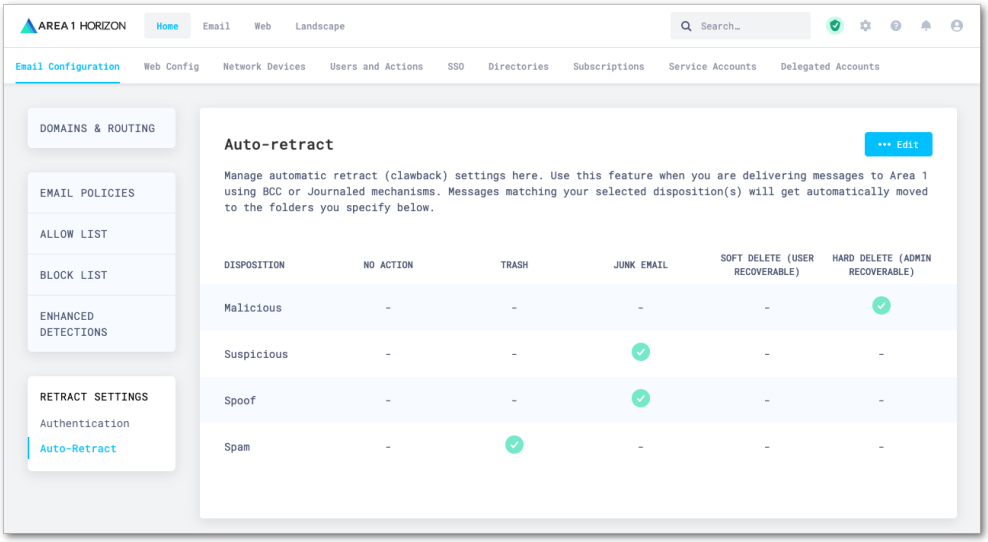
2. By default, no actions are taken against any of the dispositions. To modify the behaviors, click the **Edit** button:



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



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

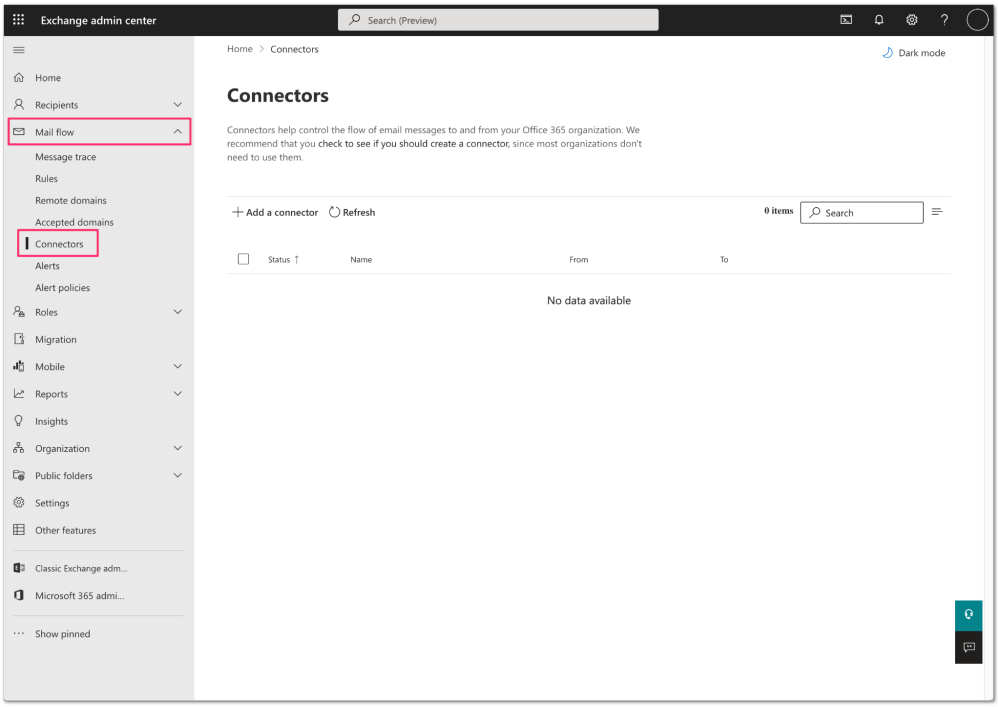


Step 3: Configure connector for delivery to Cloudflare Area 1 (if required)

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

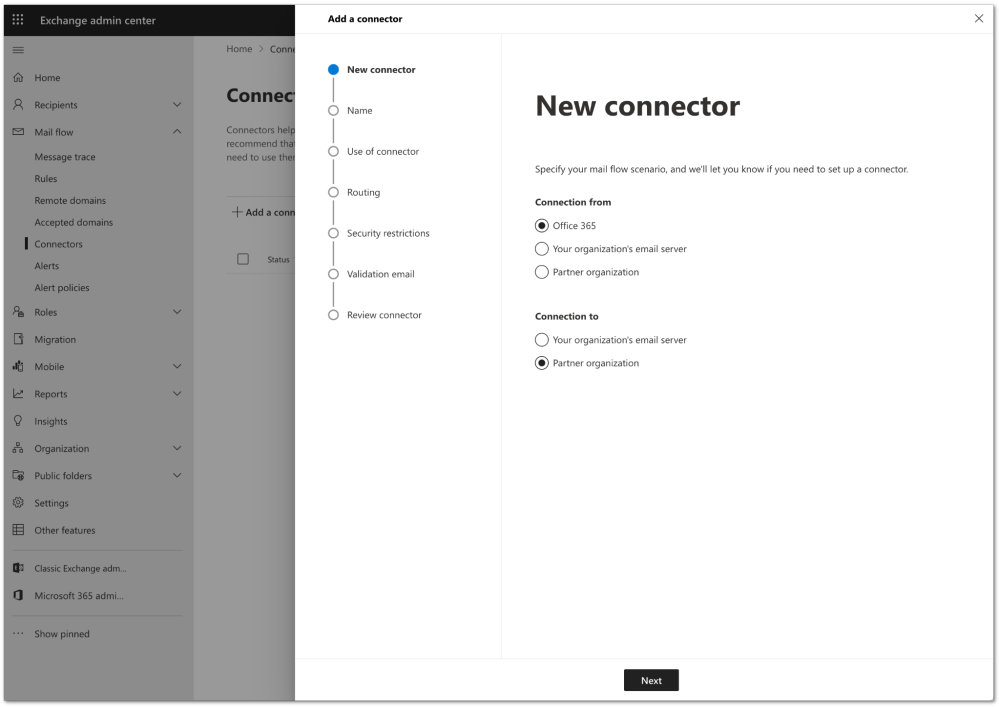
If your email architecture requires outbound messages to traverse your email gateway, you may want to consider configuring a connector to send the journal messages directly to Area 1.

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



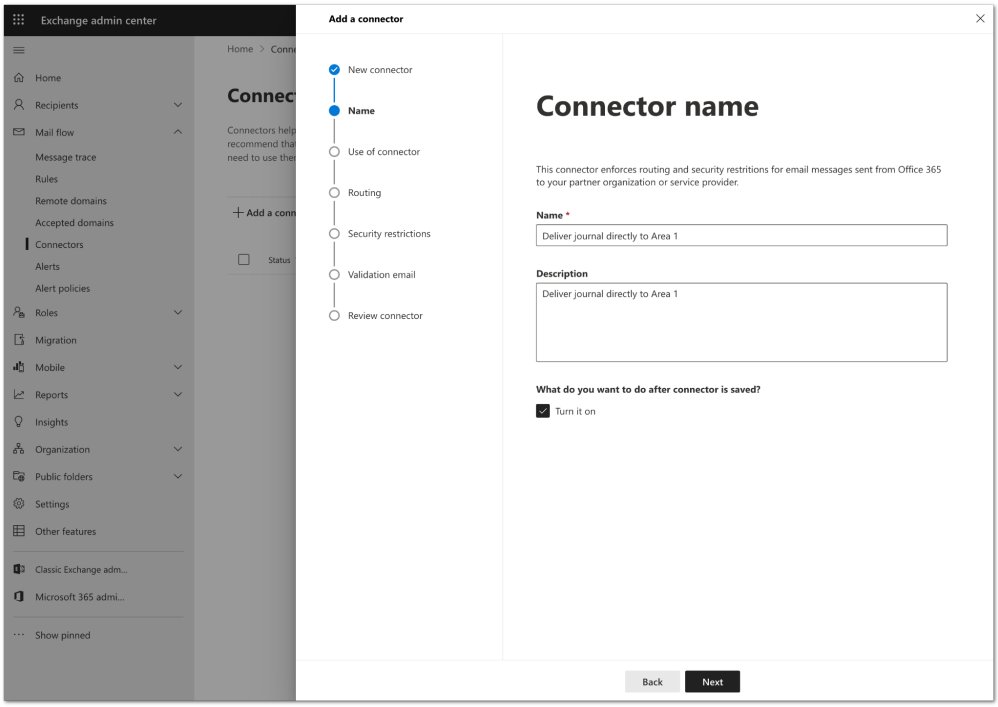
2. Click the **+ Add a connector** button to configure a new connector and configure the connector mail direction as follows:

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



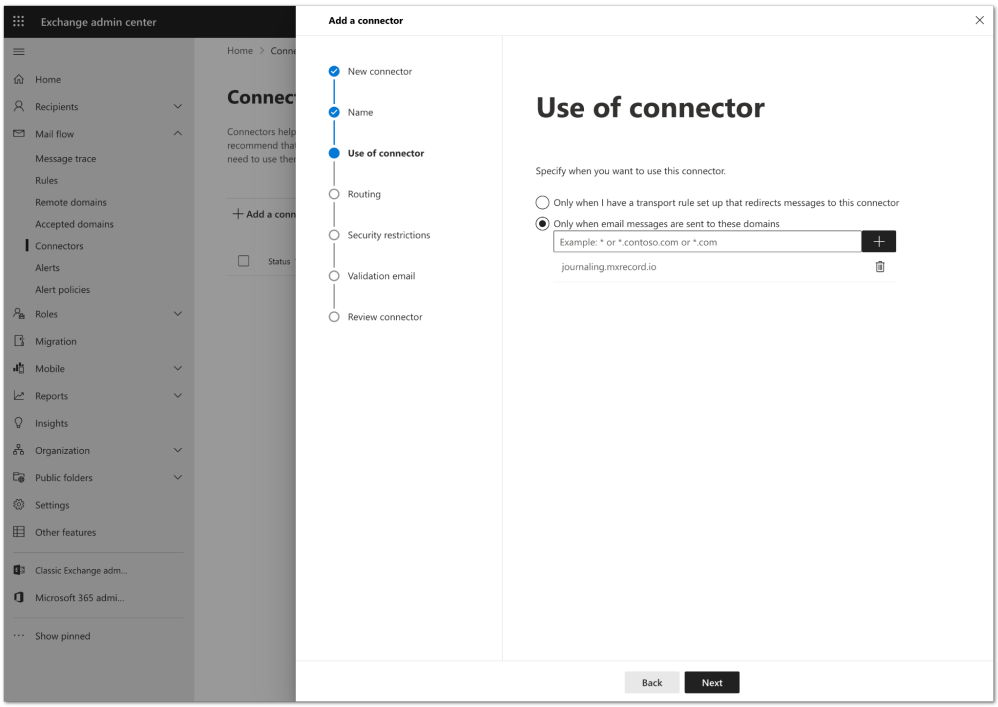
3. Configure the connector name and description:

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



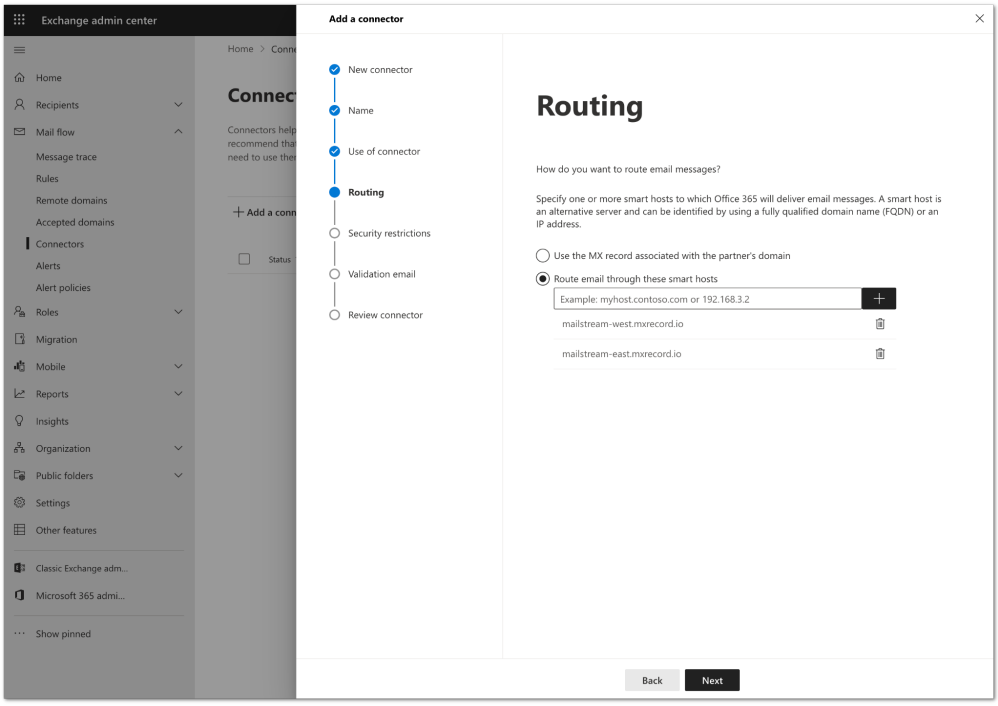
4. Configure the **Use of connector** setting:

   - Select **Only when email messages are sent to these domains** option
   - Enter **journaling.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:

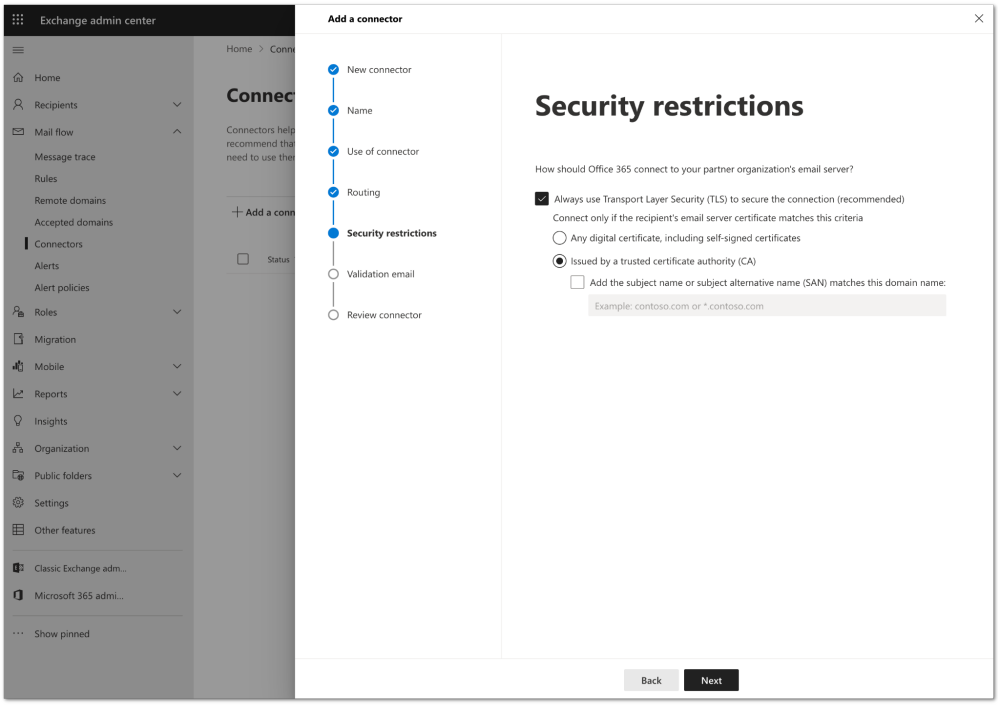
    - mailstream-east.mxrecord.io
    - mailstream-west.mxrecord.io



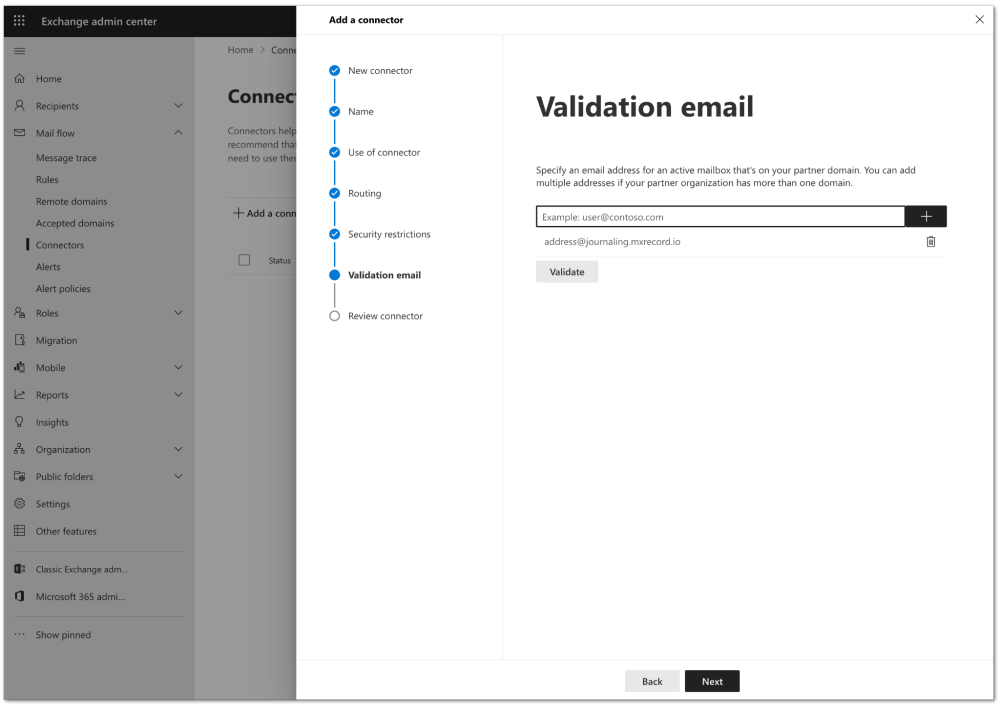
If there is a requirement to enforce traffic through the EU region use the following smarthost instead:

- mailstream-eu1.mxrecord.io

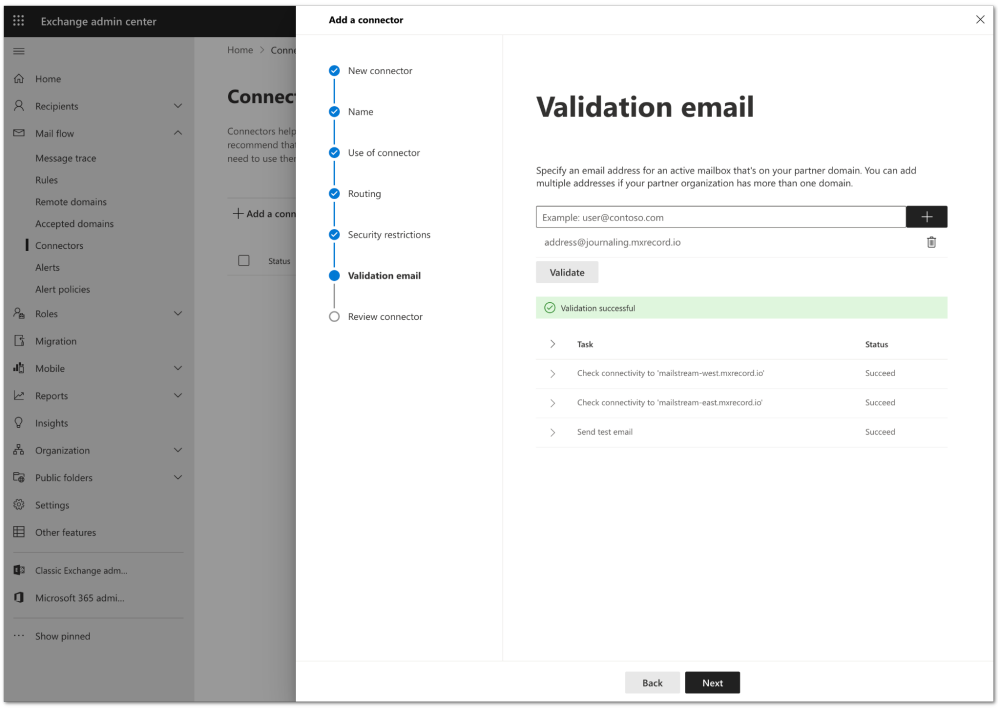
6. Preserve the default TLS configuration:



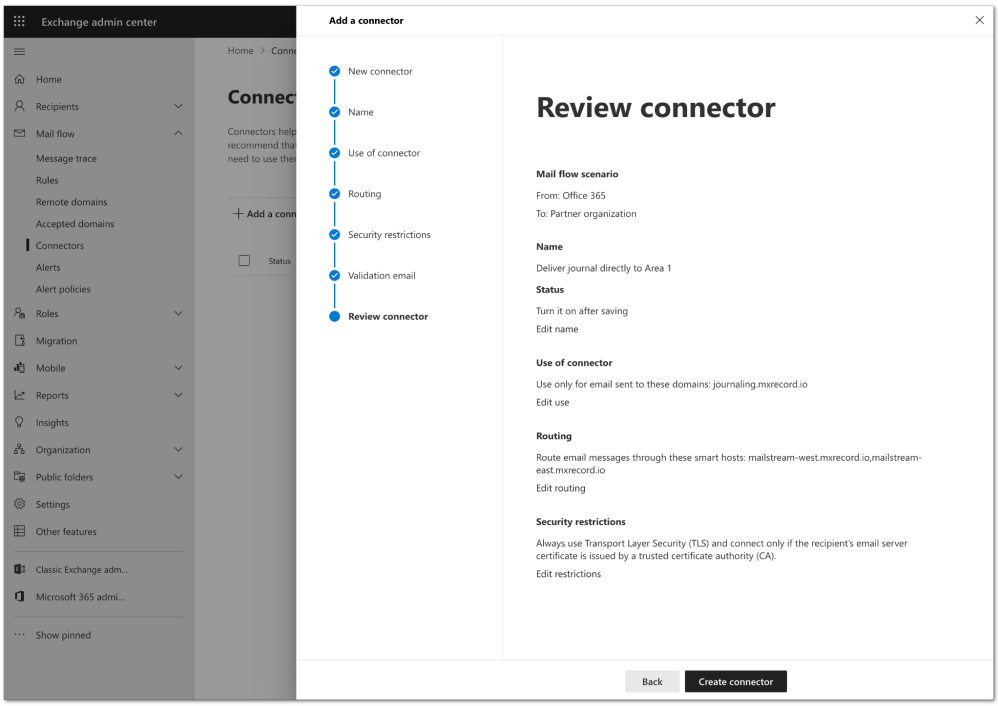
7. Validate the connector by using your tenant's specific journaling address. This address can be found in the Area 1 Horizon portal in the Support > Service Addresses page (https://horizon.area1security.com/support/service-addresses):



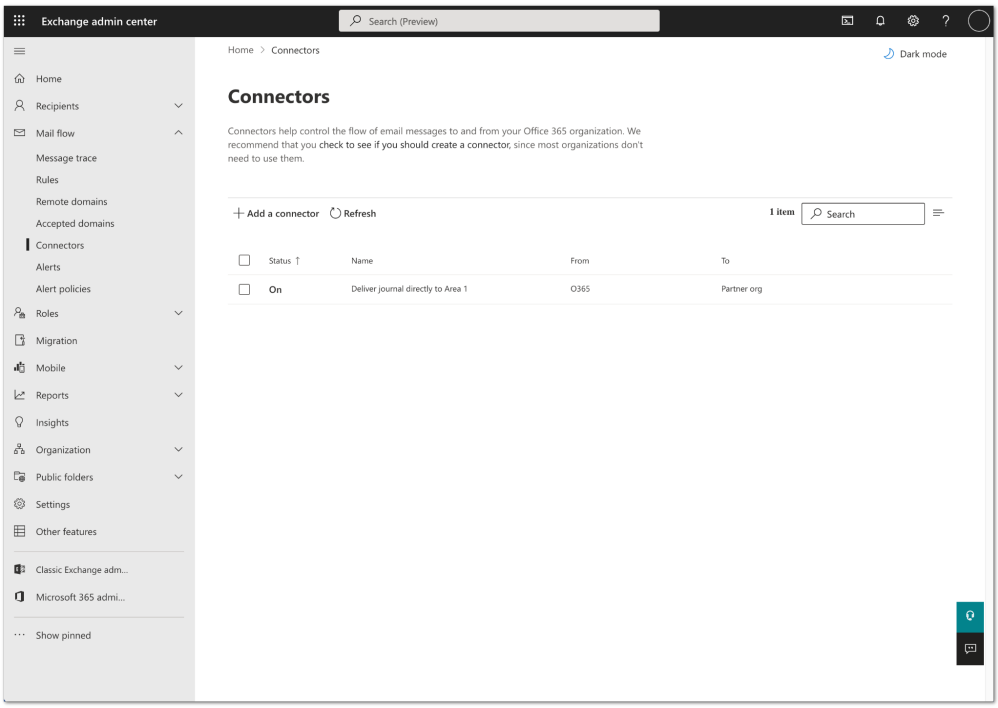
9. Once the validation completes, you should receive a **Succeeded** status for all the tasks:



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



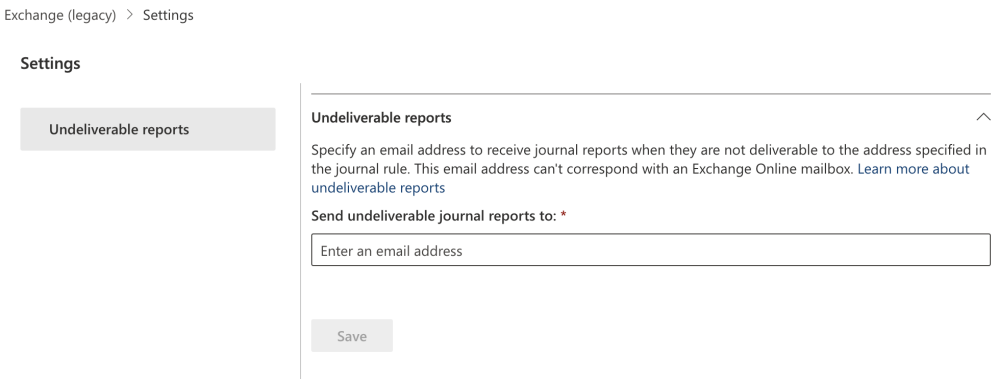
10. Once saved, the connector will be active:



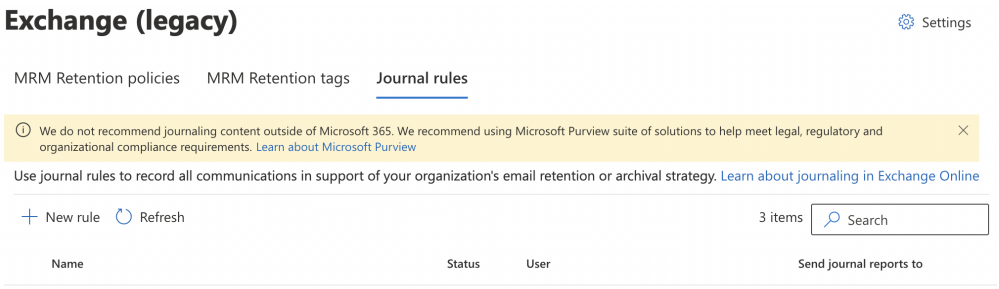
Step 4: Configure Journal Rule

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.



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



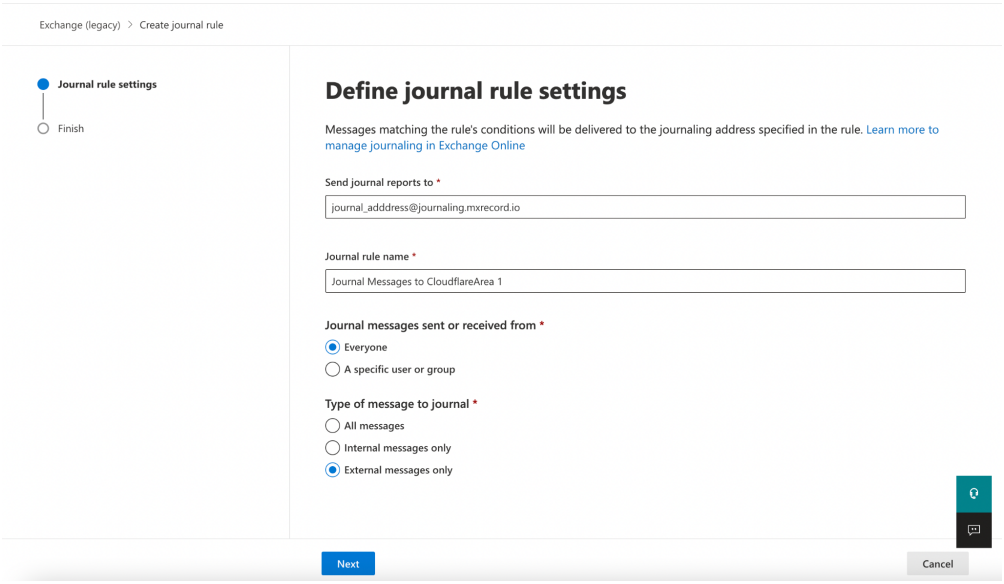
6. Select **New rule t**o configure a journaling rule, and configure the journaling rule as follows then select **Next**:

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

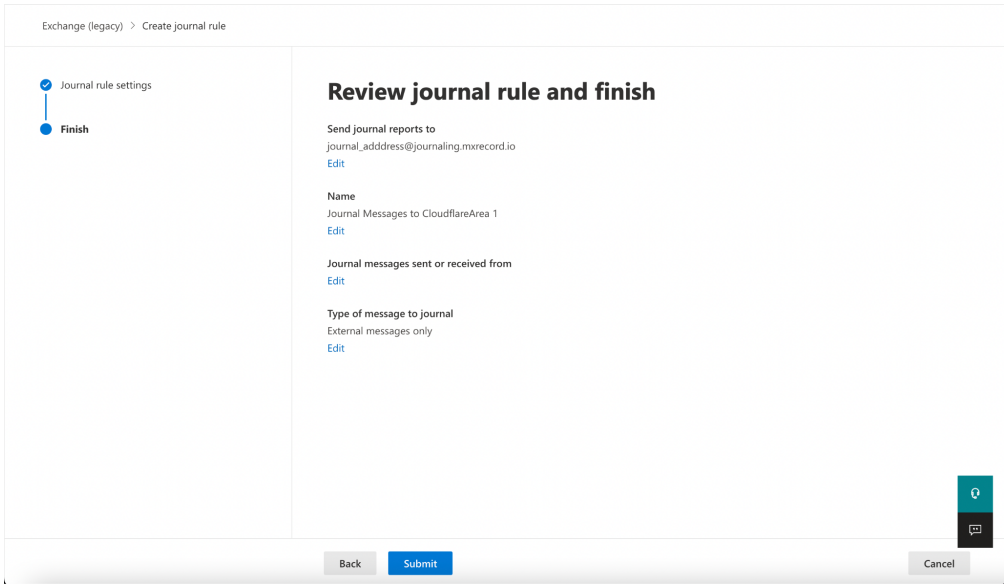
https://horizon.area1security.com/support/service-addresses

- 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



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



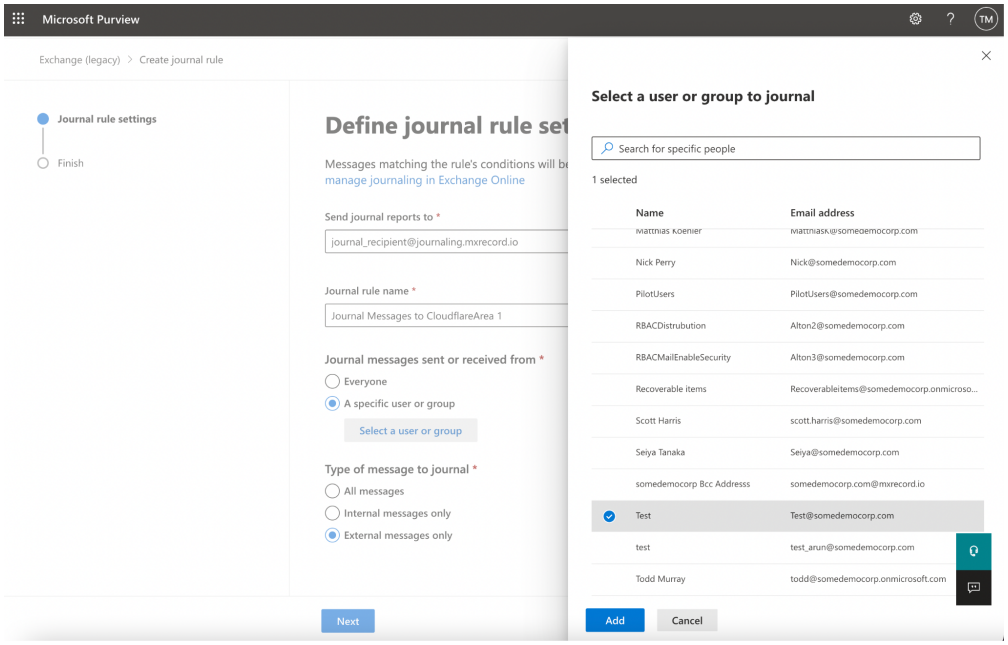
8. Click **Done.** Once saved the rule is automatically active and may take a few minutes for the configuration to propagate and start to push messages to Cloudflare Area 1.

You can now access the Cloudflare Area 1 portal and you should see the number of messages processed counter increment as 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]

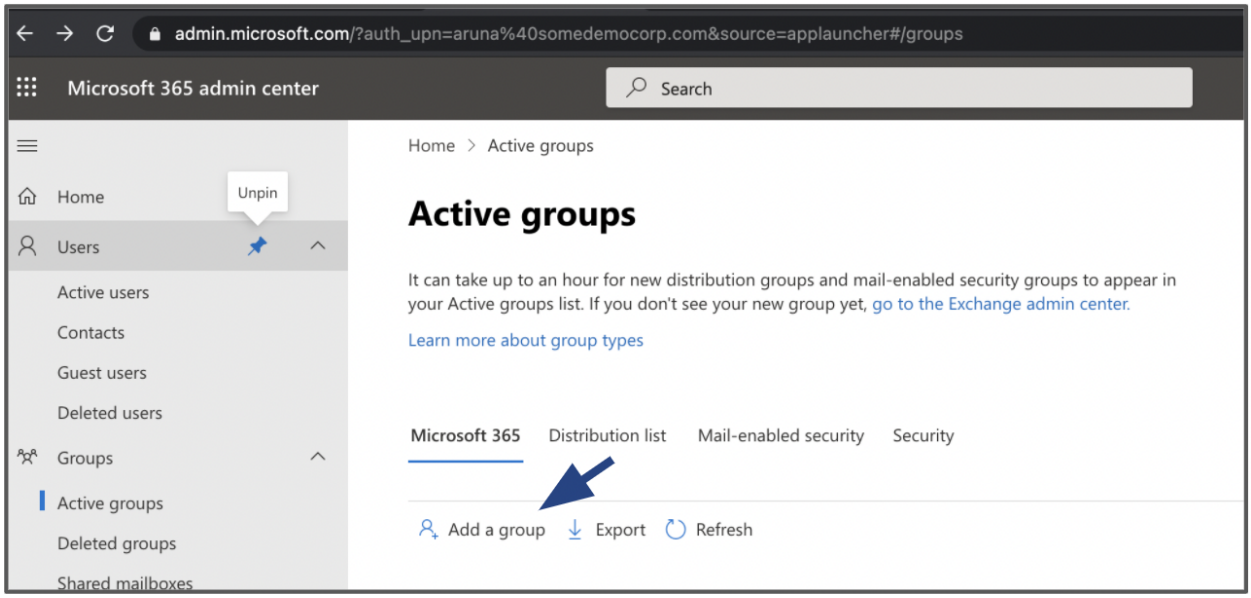


- From the window that pops up with the list of users/groups, select the corresponding distribution group.

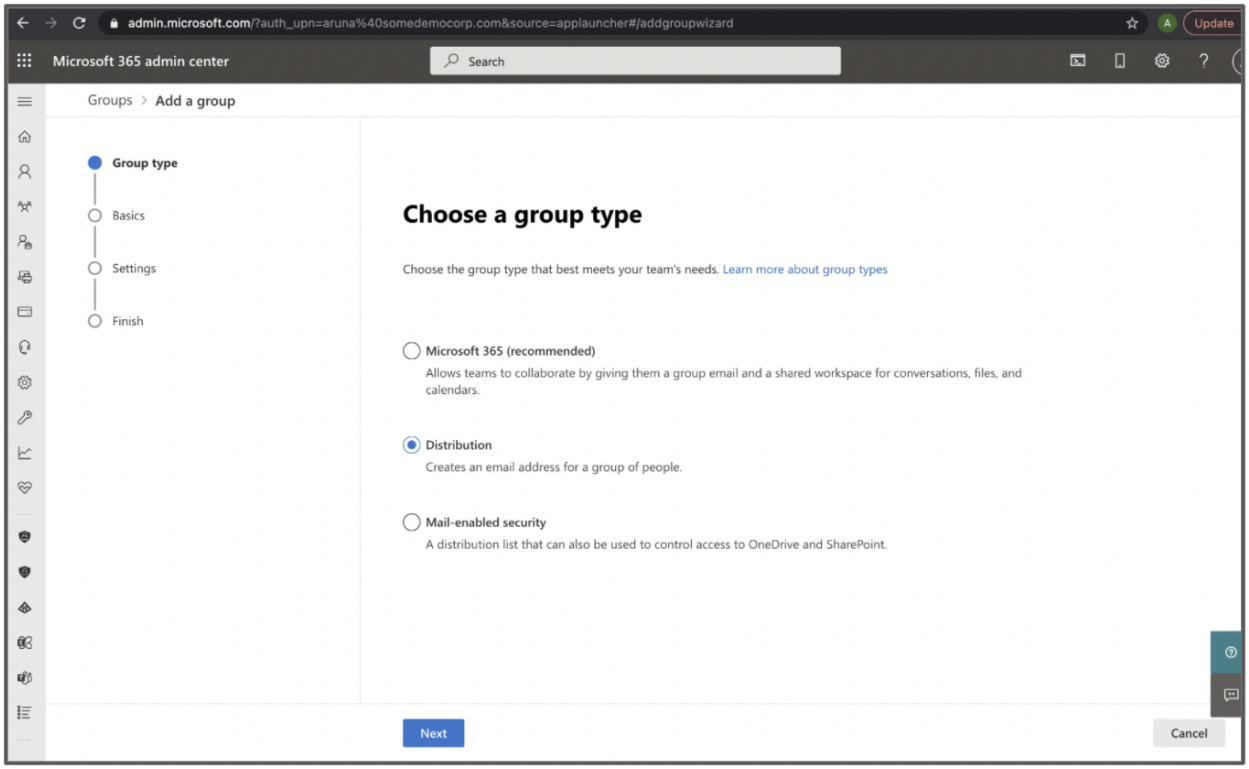
Creating distribution group in O365

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

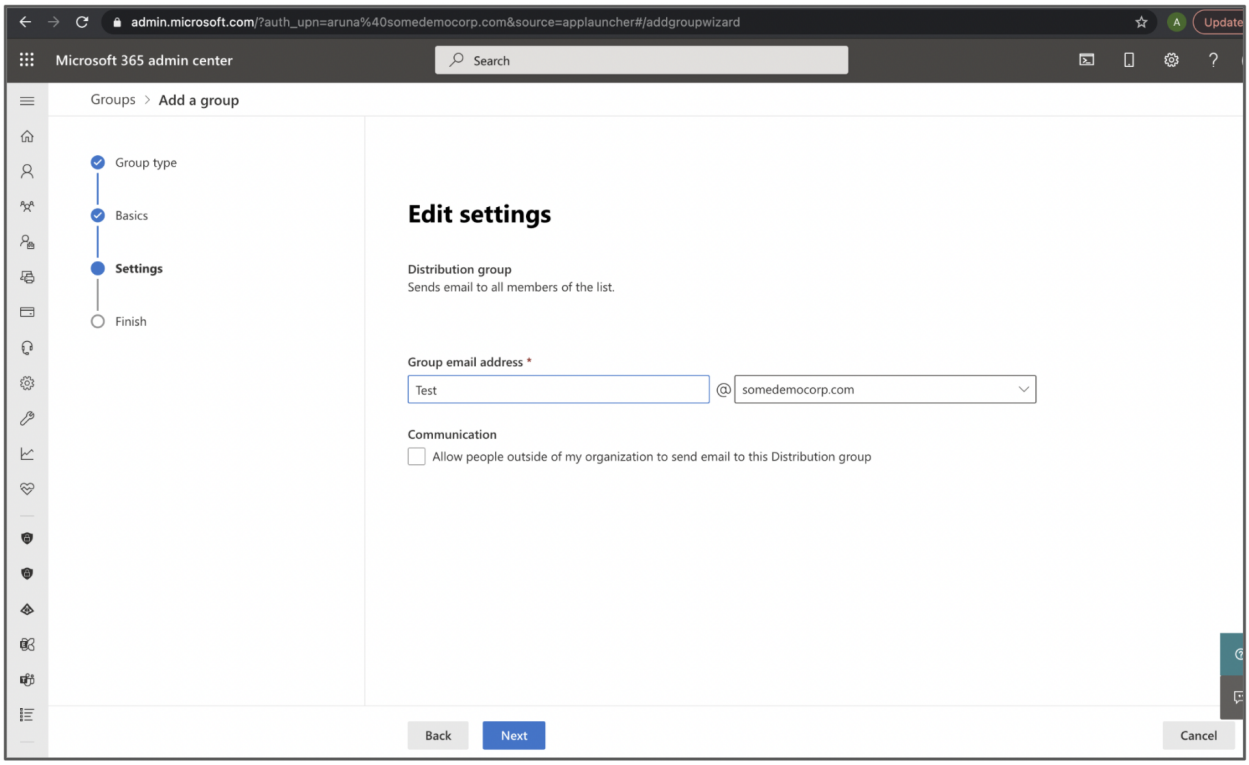
Navigate to: Microsoft Exchange Admin Center > Home > Active Groups



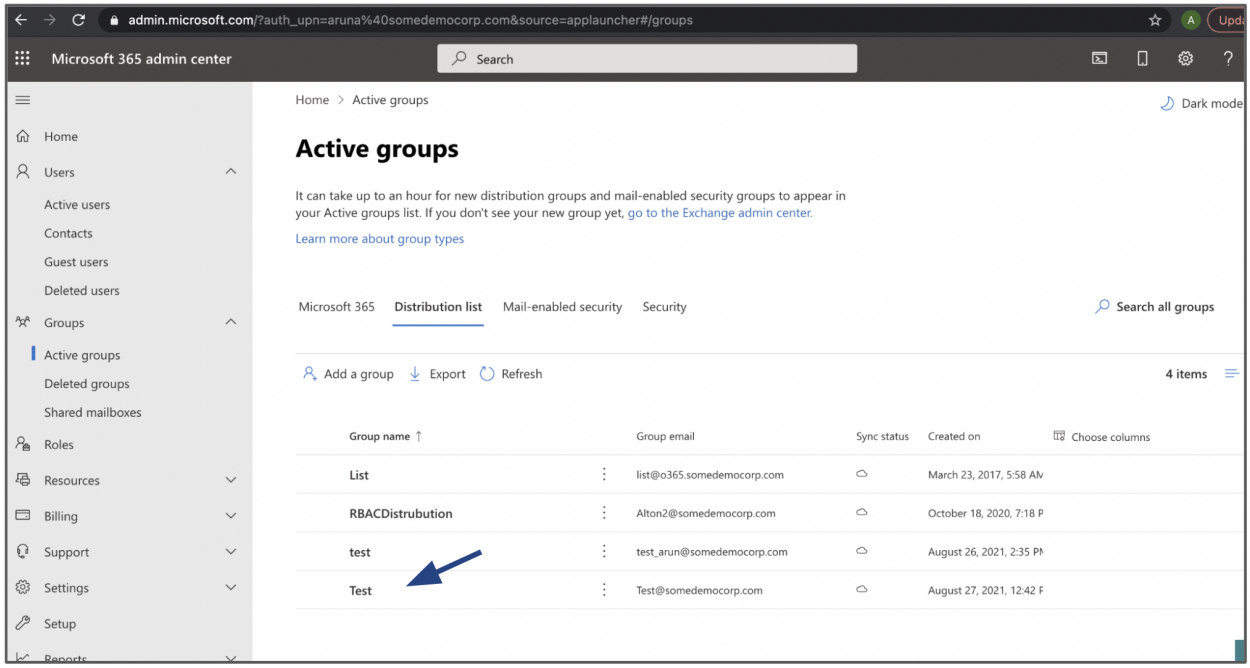
Click ‘Add a group’ > Select ‘Distribution’ > Click Next



Enter a group name > Click Next > And hit ‘Create Group’



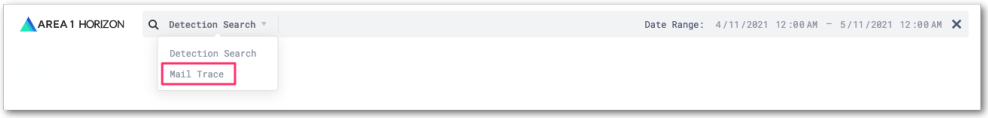
Navigate to the corresponding distribution group created and add the users:



Manual Message Retraction

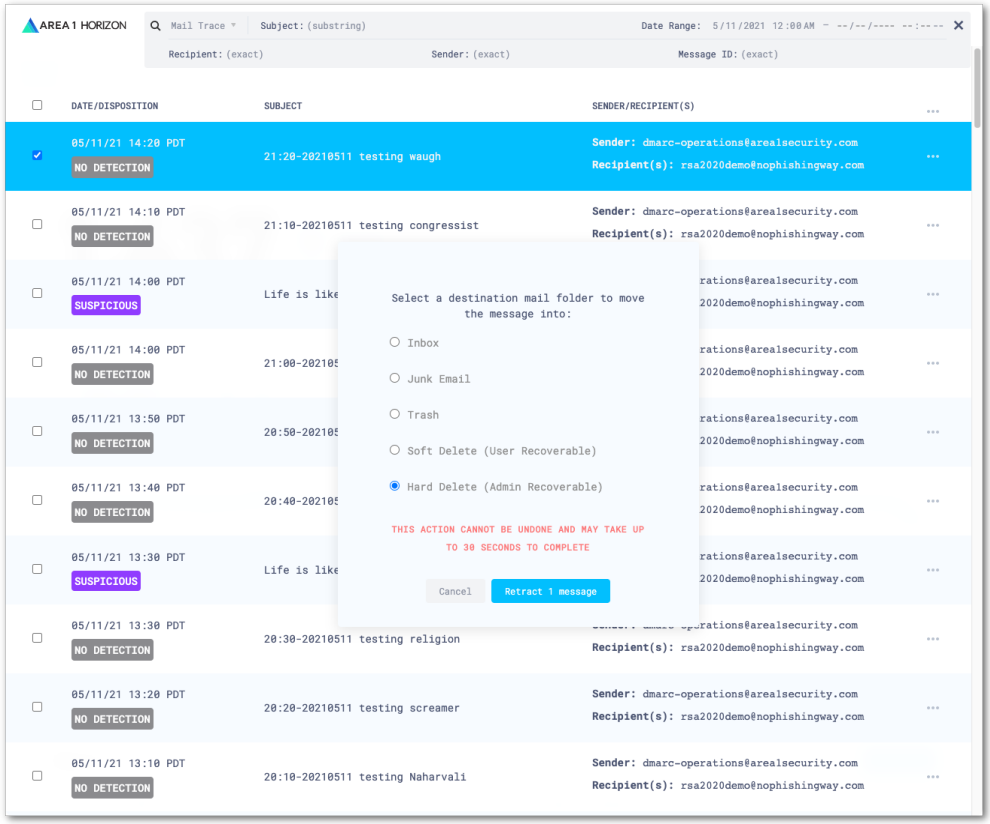
When retraction is enabled, this also allows you to manually retract messages that were not automatically retracted, for example a message was inadvertently sent to a few recipients and you've been requested to retract the message from their inbox.

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: