CLOUDFLARE
AREA 1 SECURITY

Phishing Protection for Microsoft O365

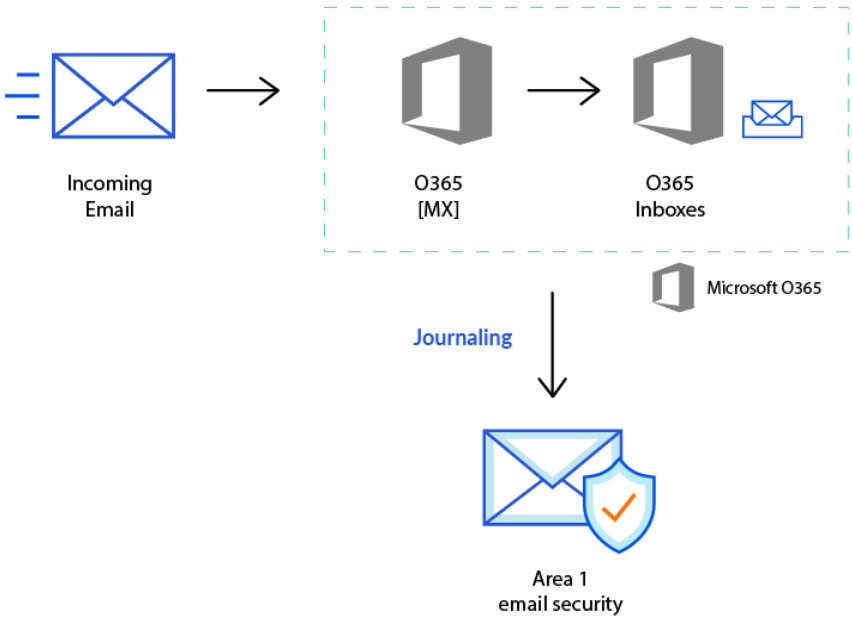
Deployment and Configuration Guide
O365 Journaling

Cloudflare Area 1 Overview

Phishing is the root cause of upwards of 90% of security breaches that lead to financial loss and brand damage. Cloudflare Area 1 is a cloud-native service that stops phishing attacks, the #1 cybersecurity threat, across all traffic vectors - email, web and network.

With globally distributed sensors and comprehensive attack analytics, Area 1 cloud email security 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 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

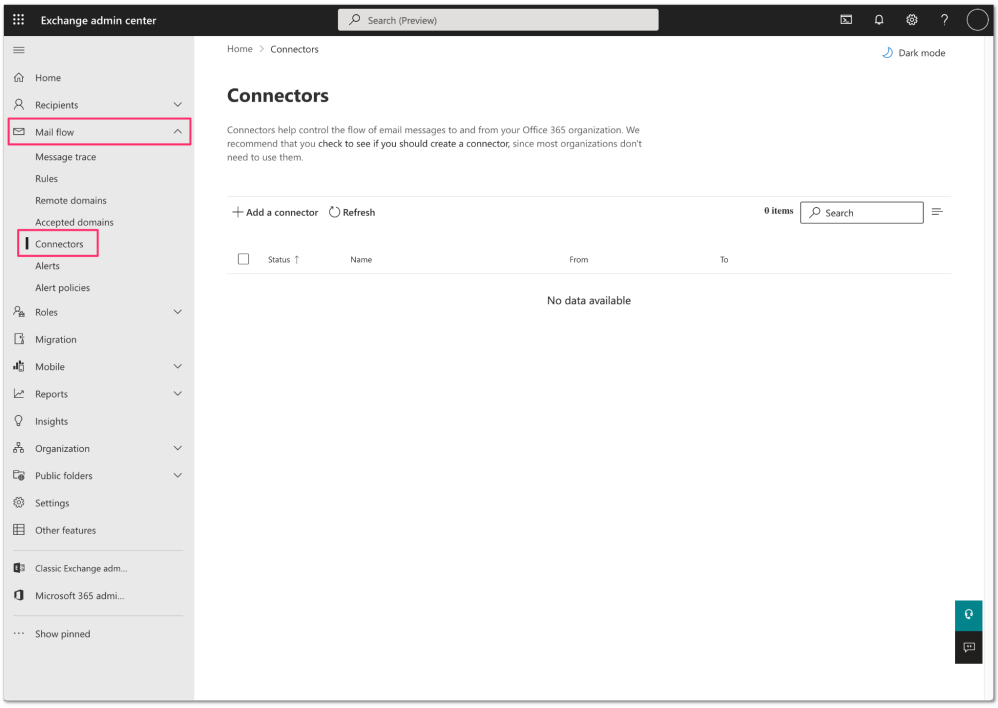
- Step 1: Configure connector for delivery to Area 1 (if required)
- Step 2: Configure Journal Rule

Step 1: 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..

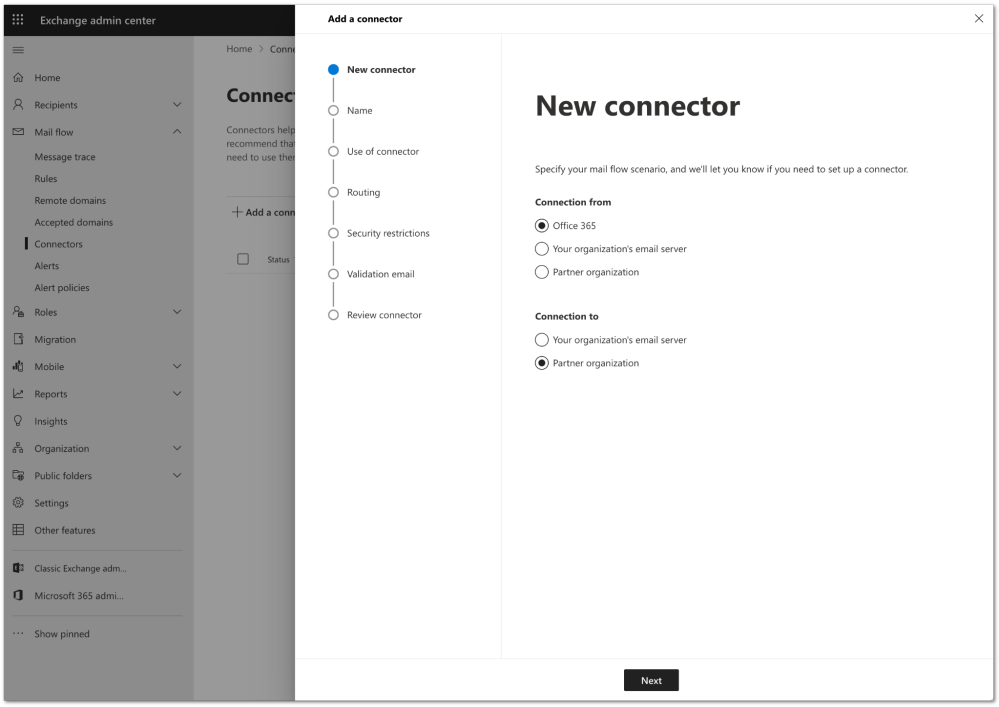
If your email architecture requires outbound messages to traverse your email gateway, you may want to consider configuring a connector to send the journal messages directly to Area 1.

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



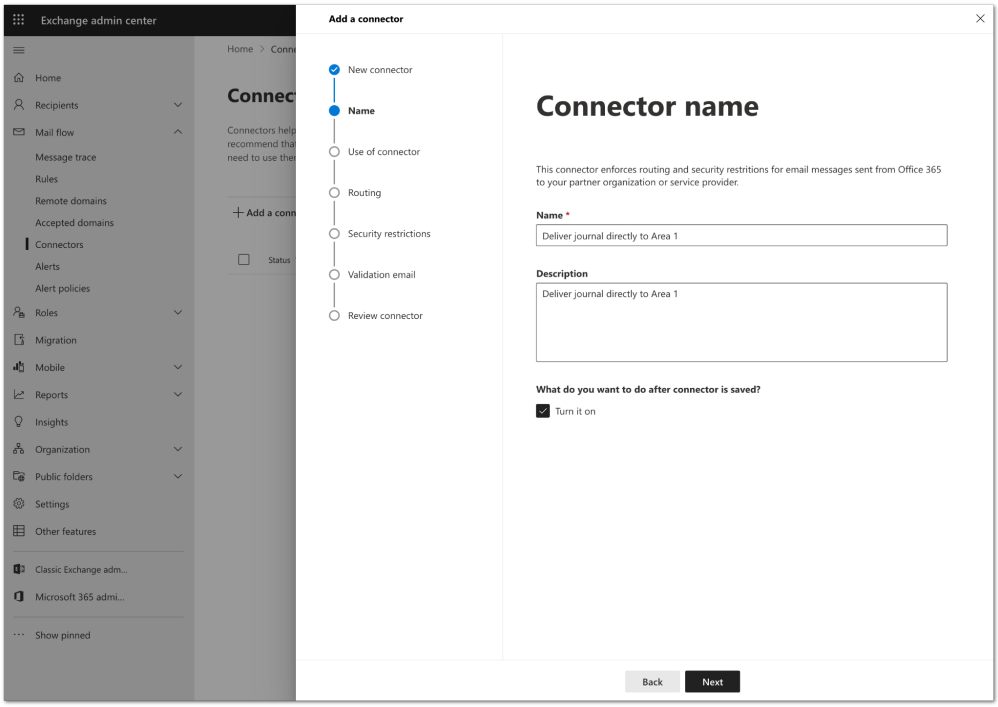
2. Click the **+ Add a connector** button to configure a new connector and configure the connector mail direction as follows:

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



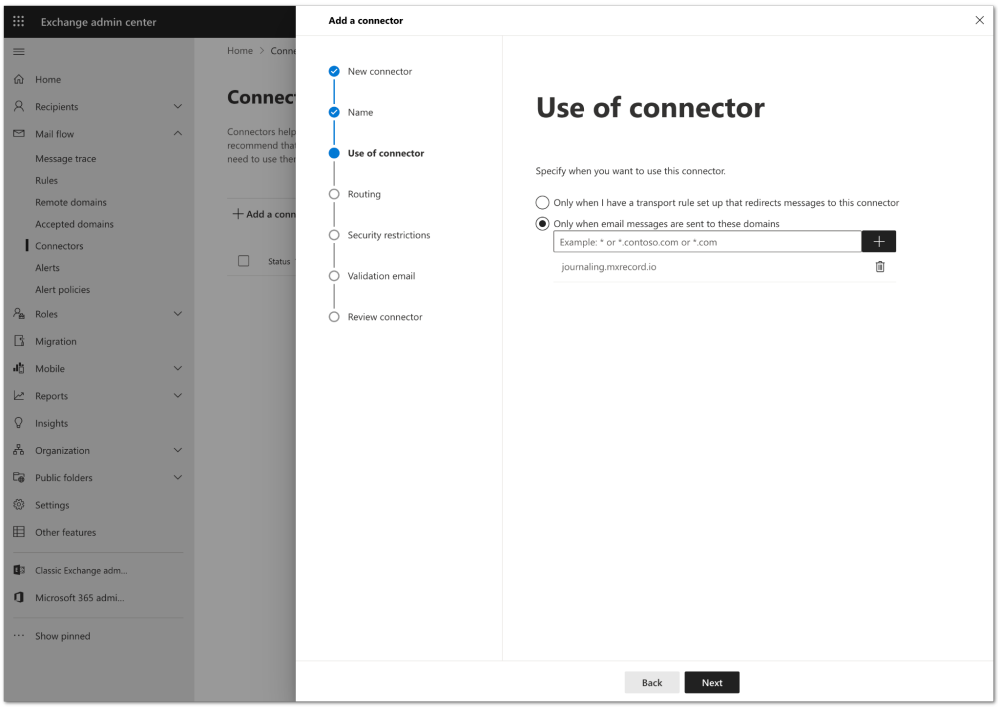
3. Configure the connector name and description:

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



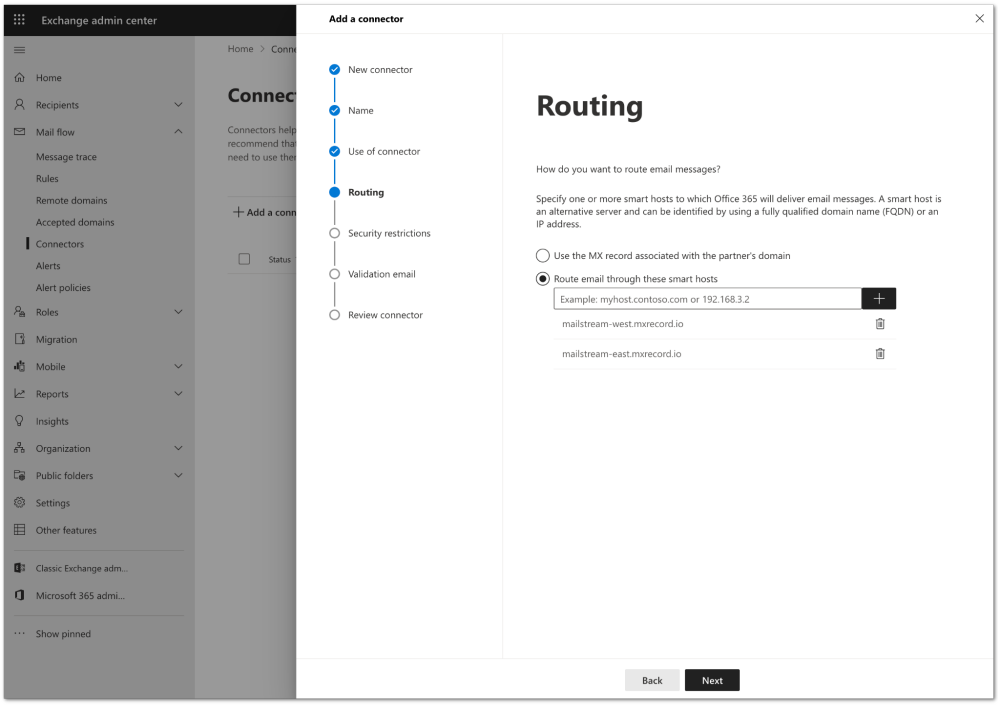
4. Configure the **Use of connector** setting:

   - 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:

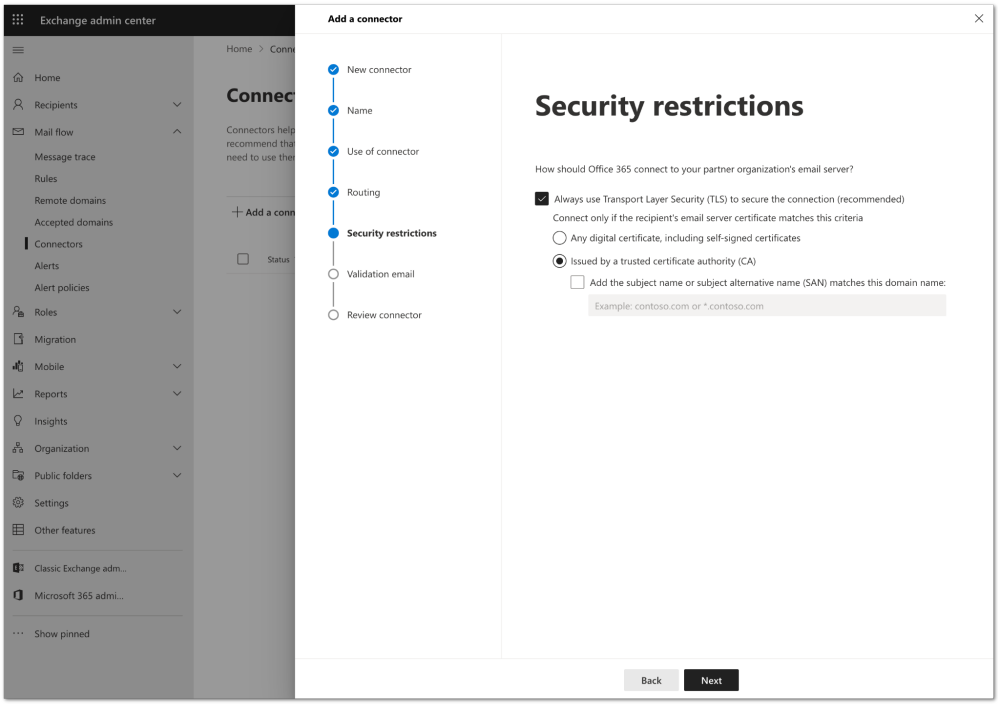
    - mailstream-east.mxrecord.io
    - mailstream-west.mxrecord.io



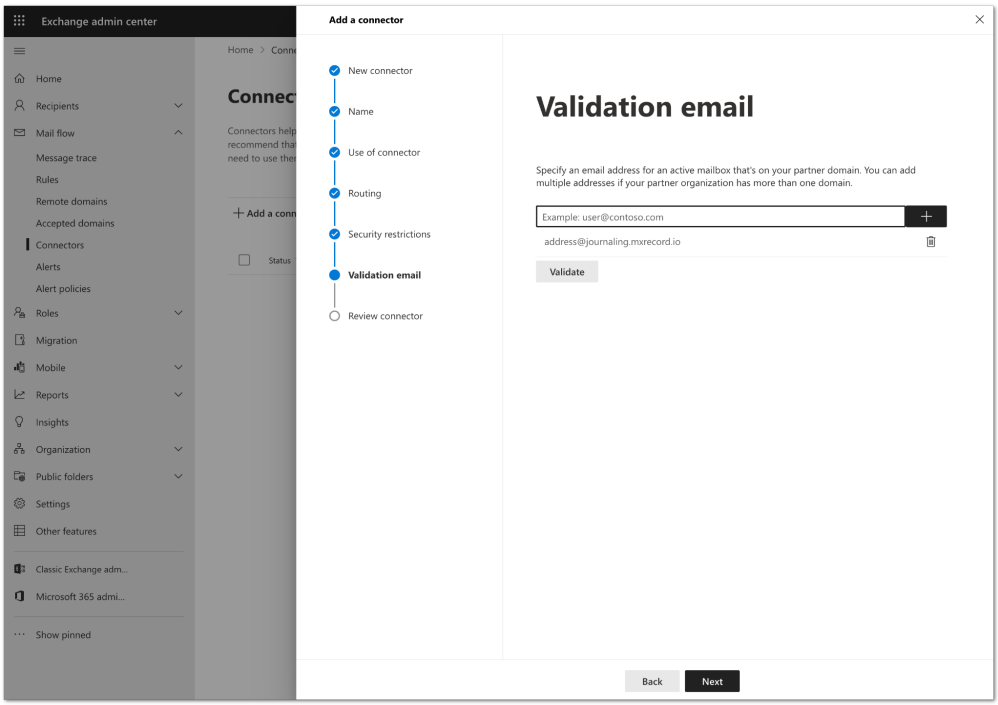
If there is a requirement to enforce traffic through the EU region use the following smarthost instead:

- mailstream-eu1.mxrecord.io

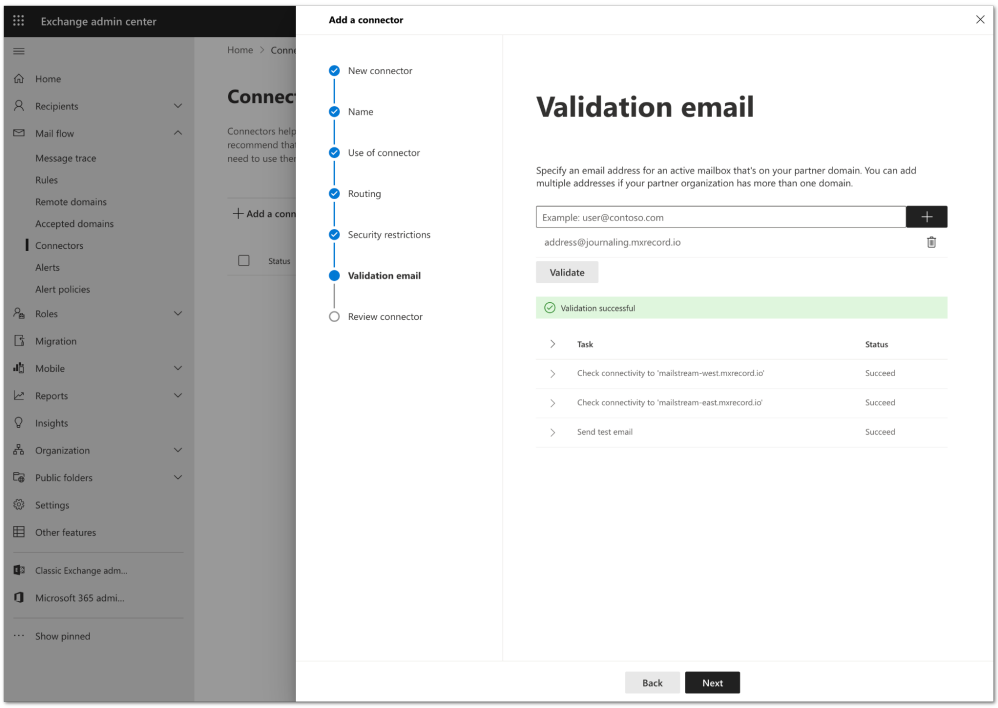
6. Preserve the default TLS configuration:



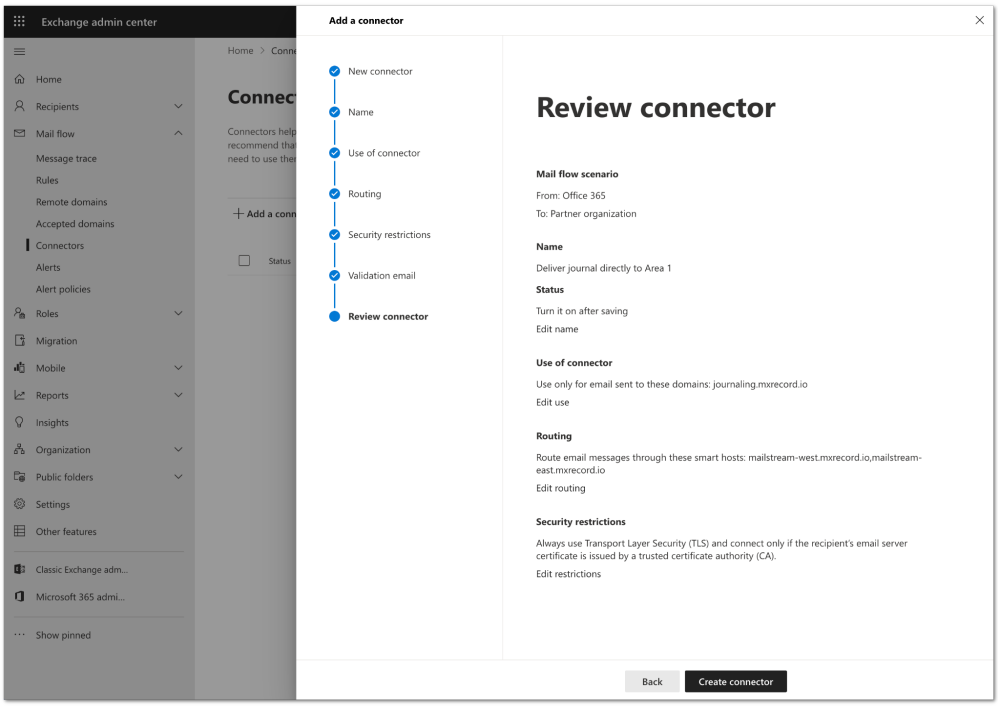
7. Validate the connector by using your tenant's specific journaling address. This address can be found in the Area 1 Horizon portal in the Support > Service Addresses page (https://horizon.area1security.com/support/service-addresses):



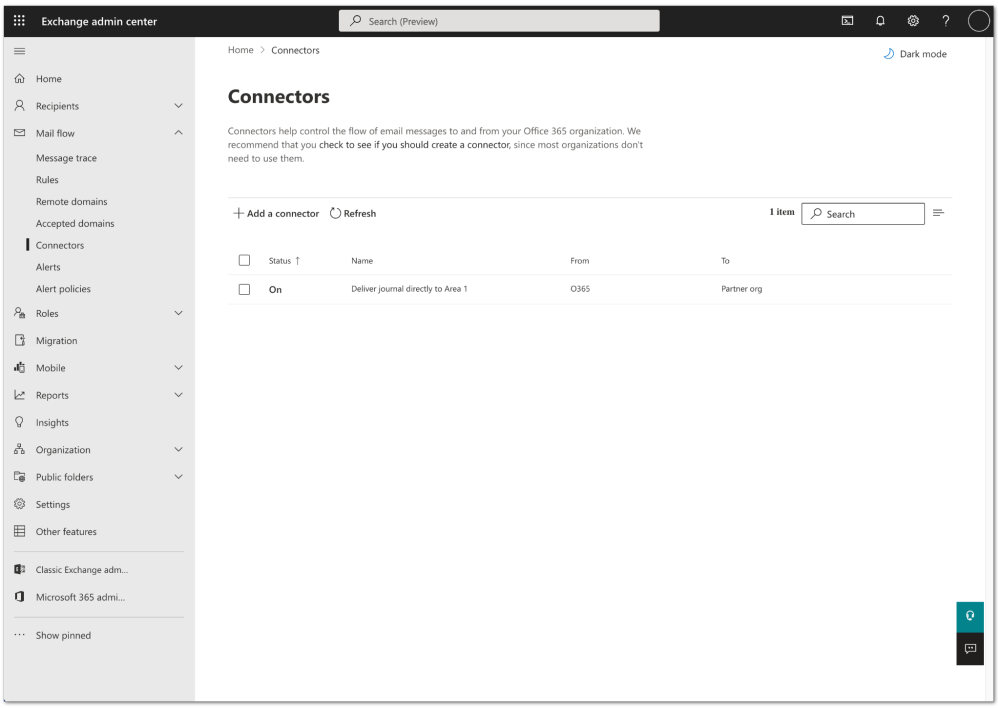
9. Once the validation completes, you should receive a **Succeeded** status for all the tasks:



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

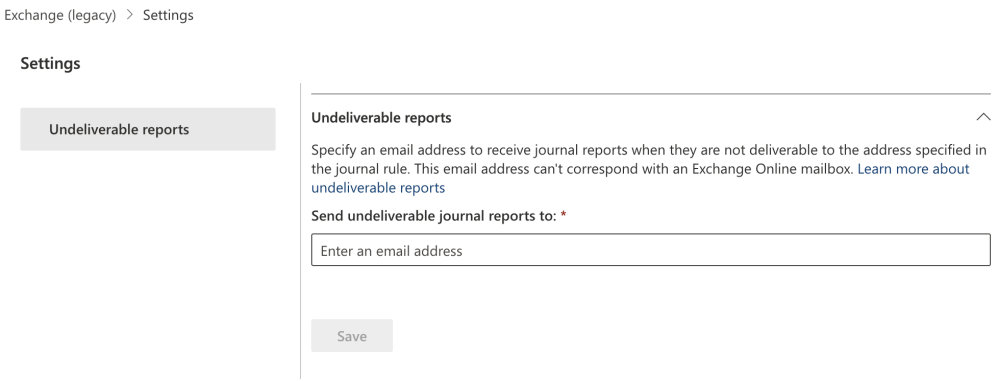


10. Once saved, the connector will be active:

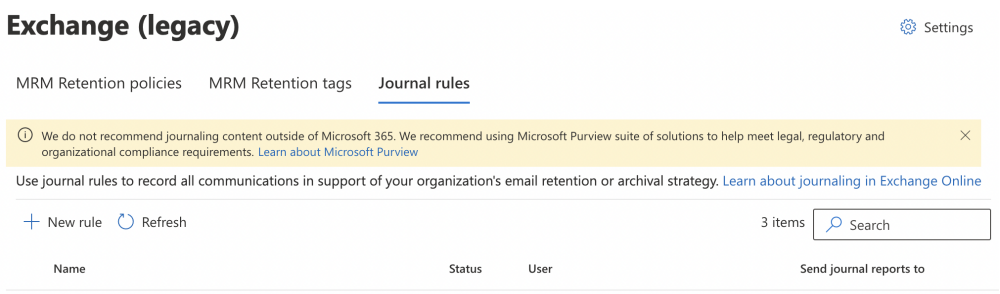


Step 2: Configure Journal Rule

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.



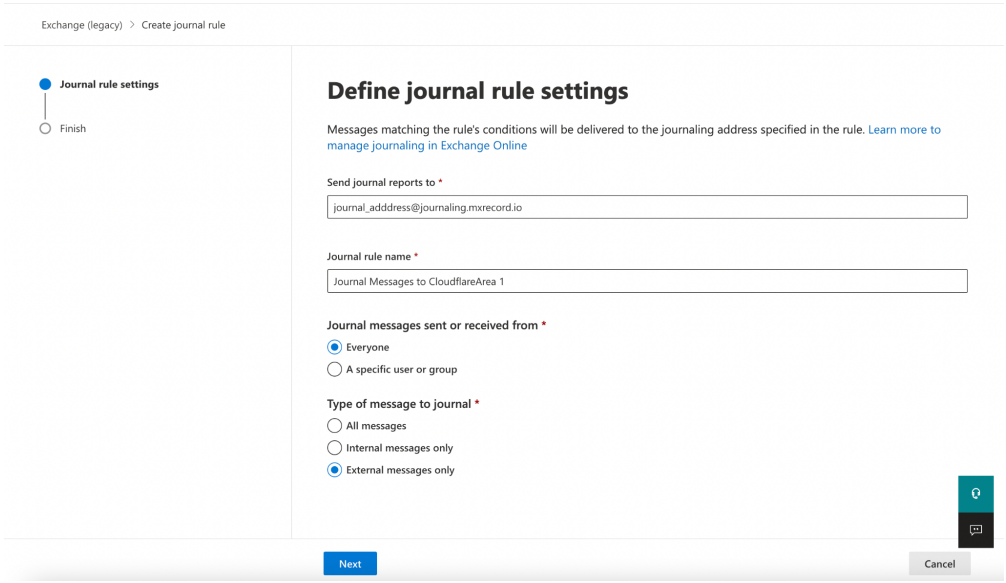
6. Select **New rule t**o configure a journaling rule, and configure the journaling rule as follows then select **Next**:

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

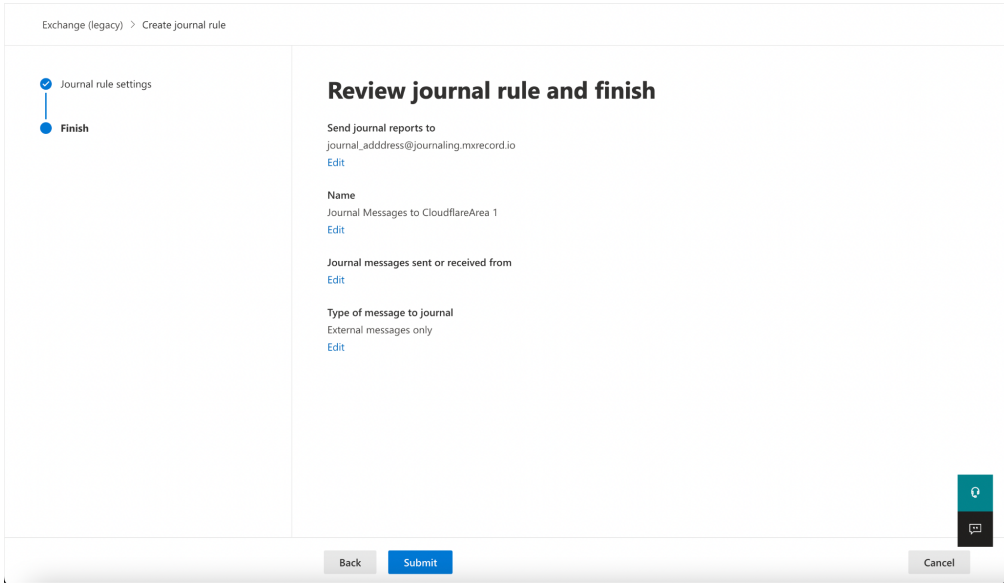
      https://horizon.area1security.com/support/service-addresses

- 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**.



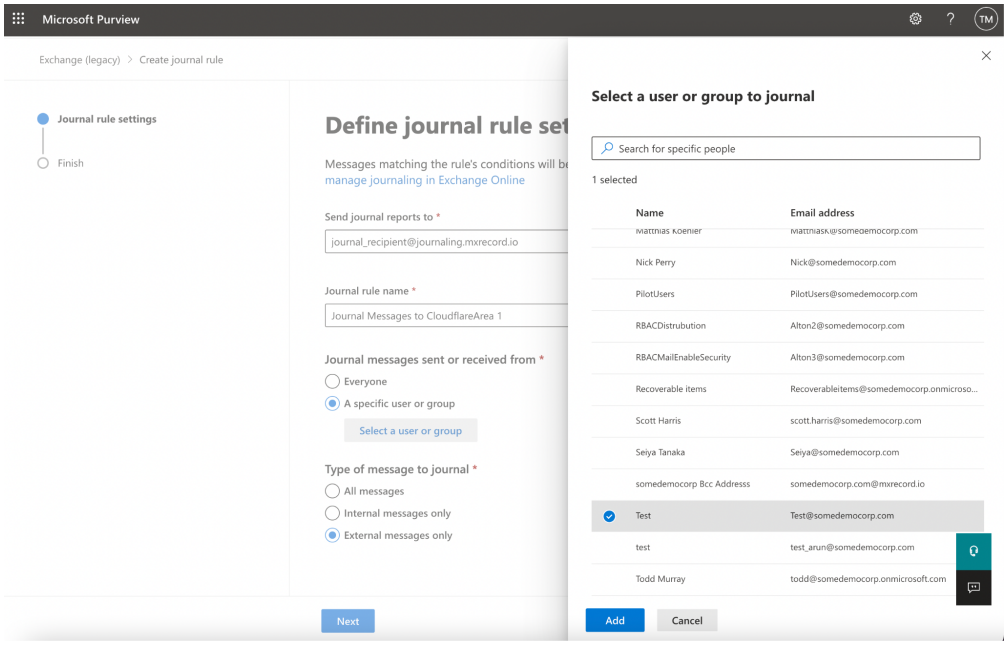
8. Click **Done.** Once saved the rule is automatically active and may take a few minutes for the configuration to propagate and start to push messages to Cloudflare Area 1.

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]

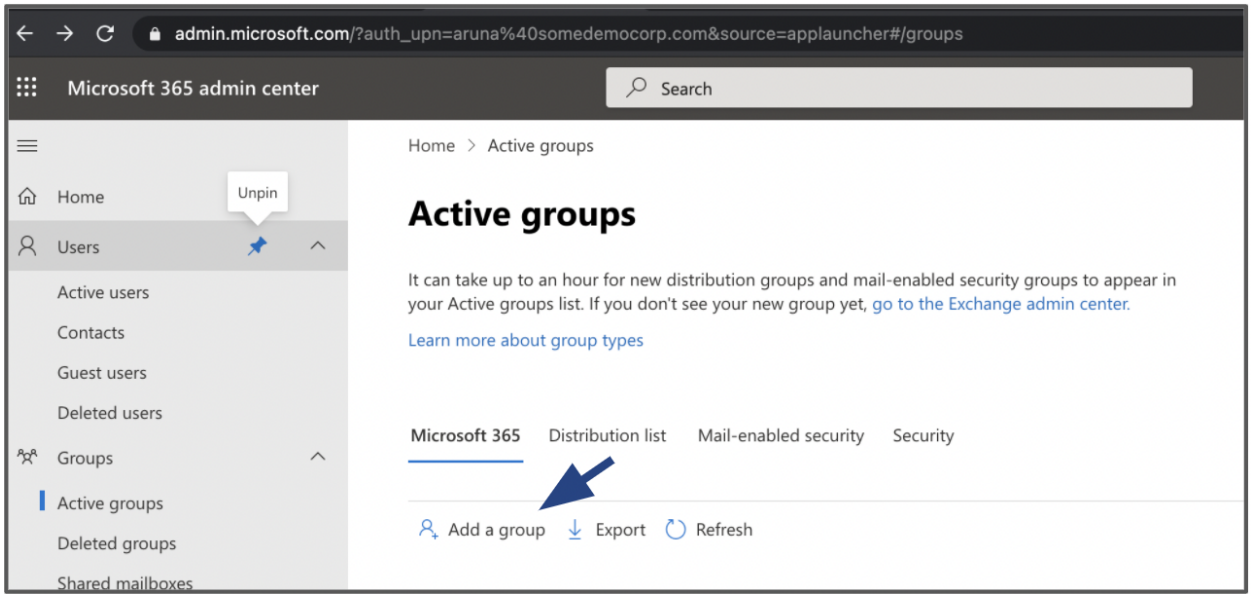


- From the window that pops up with the list of users/groups, select the corresponding distribution group.

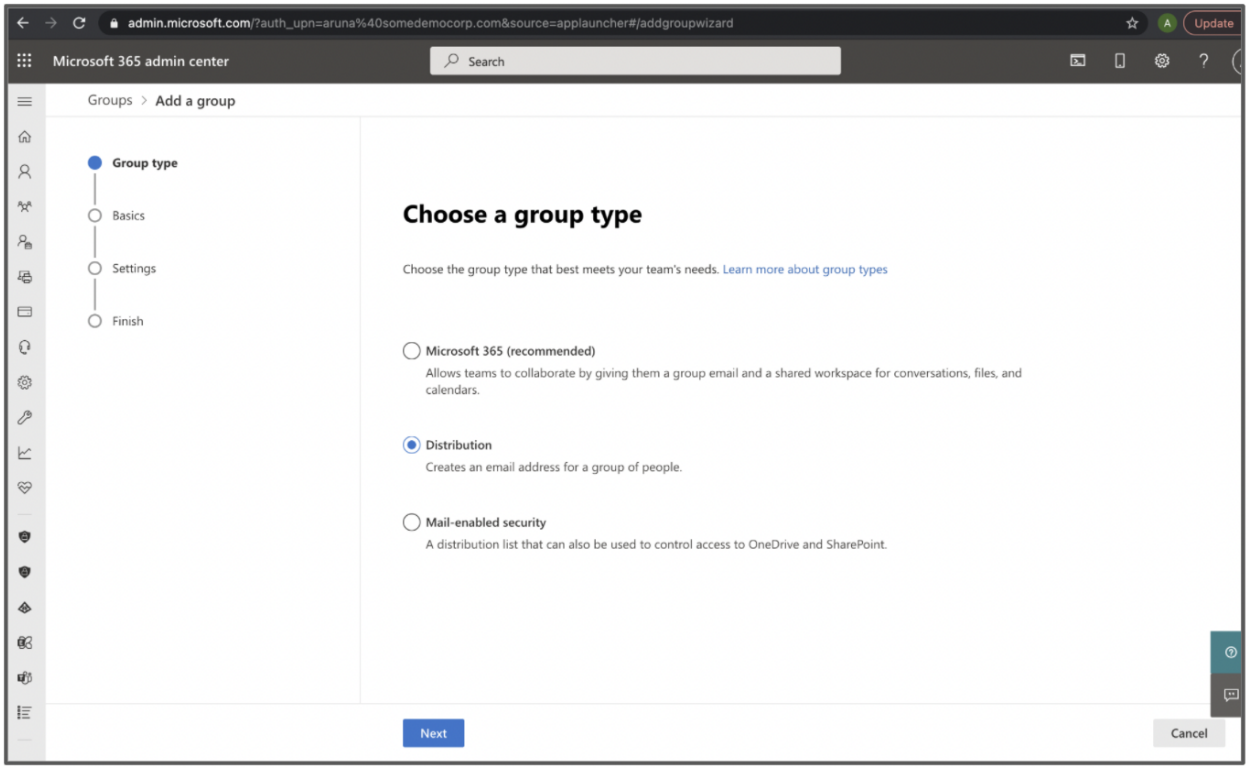
Creating distribution group in O365

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

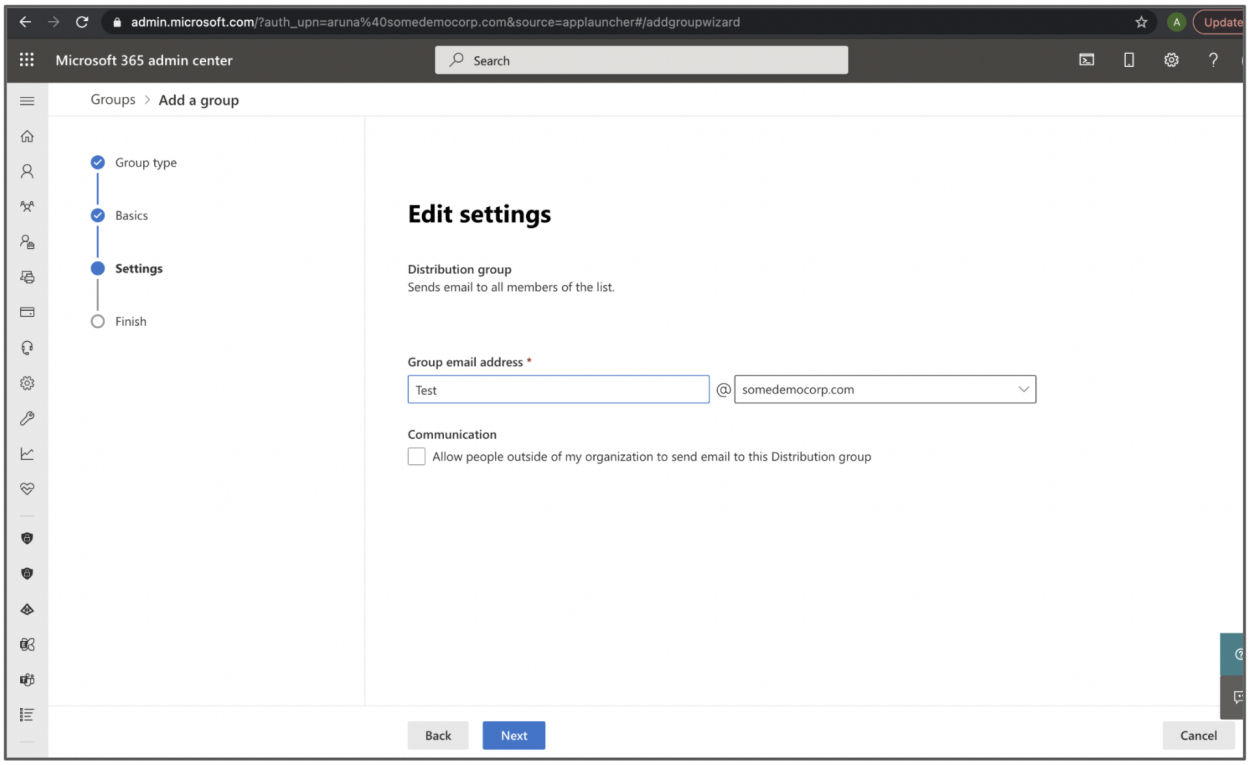
Navigate to: Microsoft Exchange Admin Center > Home > Active Groups



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: