

Phishing Protection for Microsoft O365

Deployment and Configuration Guide

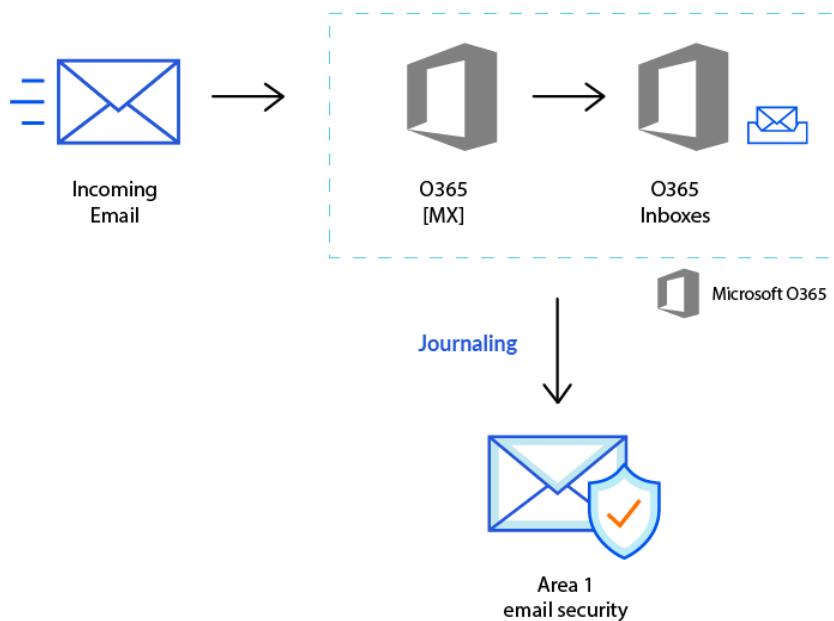
O365 Journaling

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

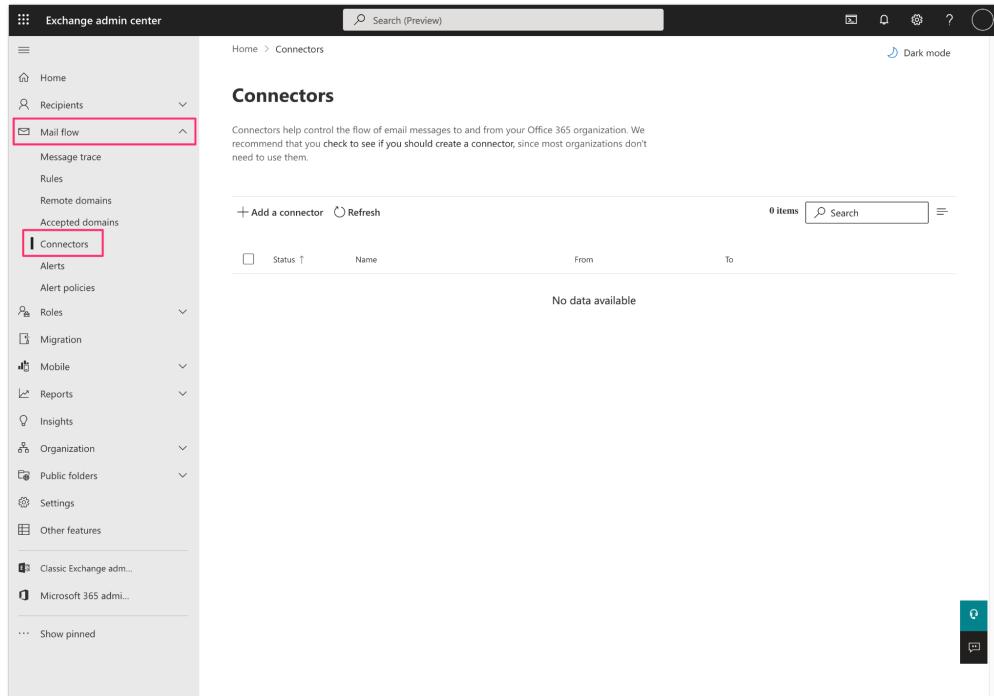
- Step 1: Configure connector for delivery to Area 1 (if required)
- Step 2: Configure Journal Rule

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..

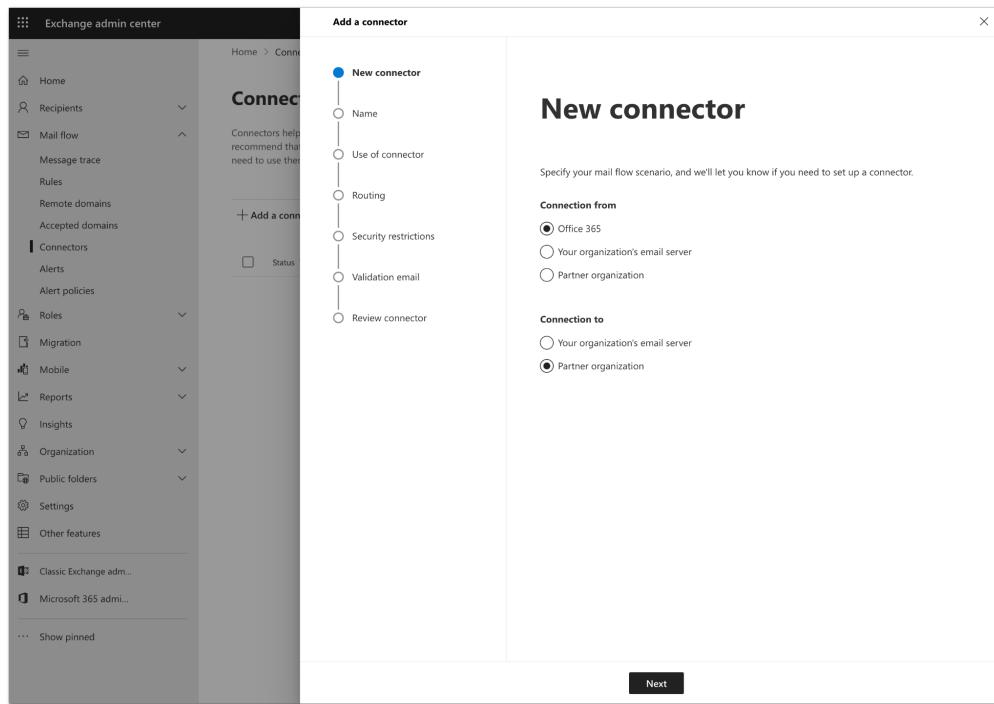
If your email architecture requires outbound messages to traverse your email gateway, you may want to consider configuring a connector to send the journal messages directly to Area 1.

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



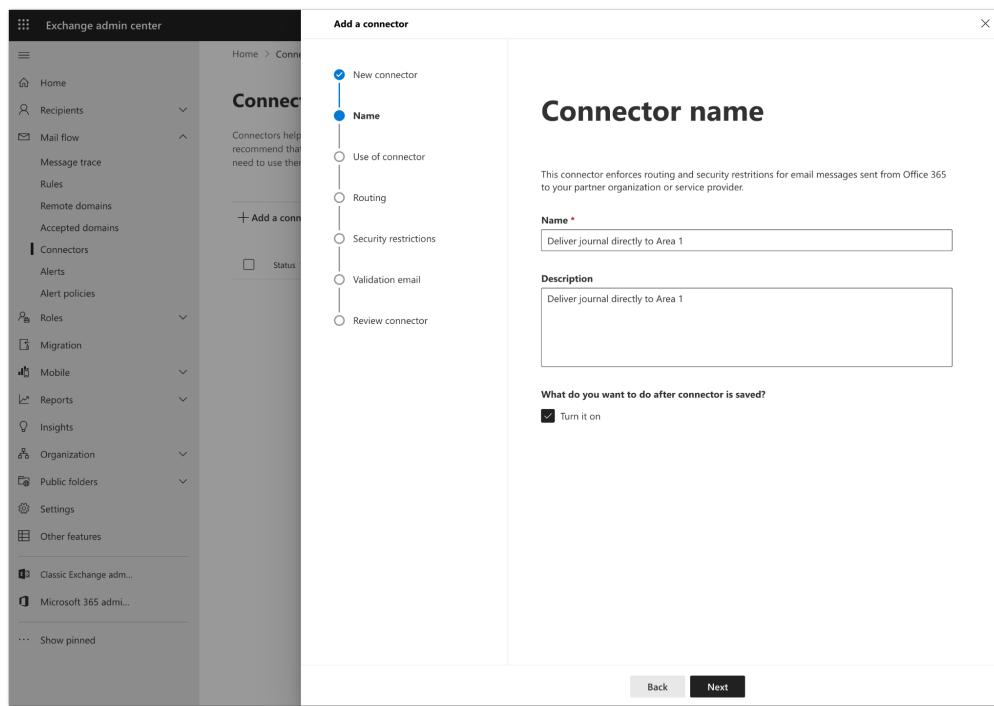
2. Click the **+ Add a connector** button to configure a new connector and configure the connector mail direction as follows:

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



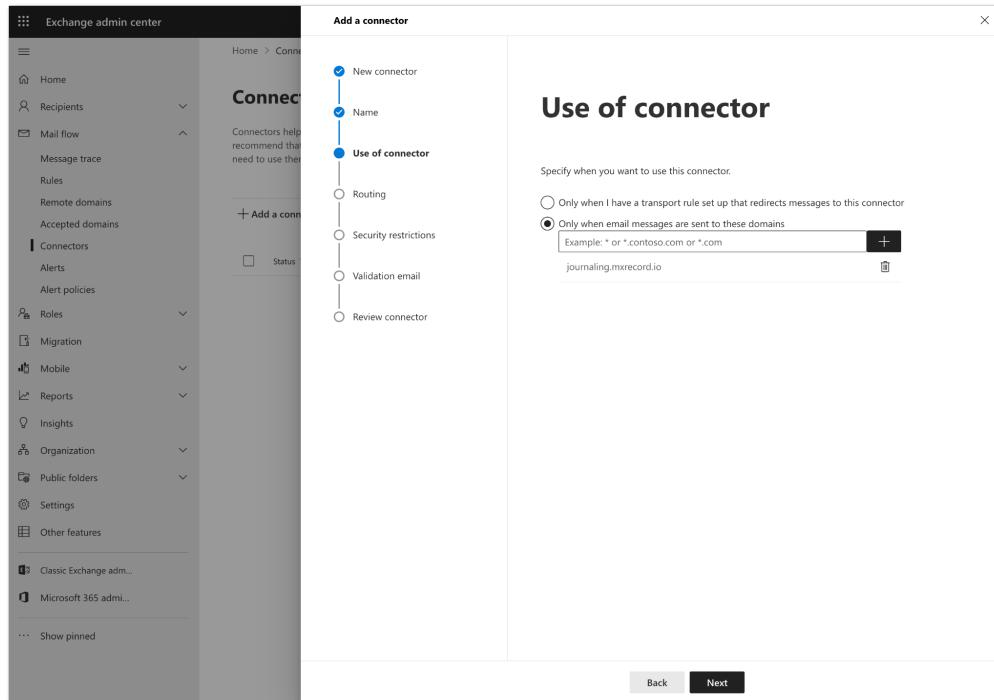
3. Configure the connector name and description:

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



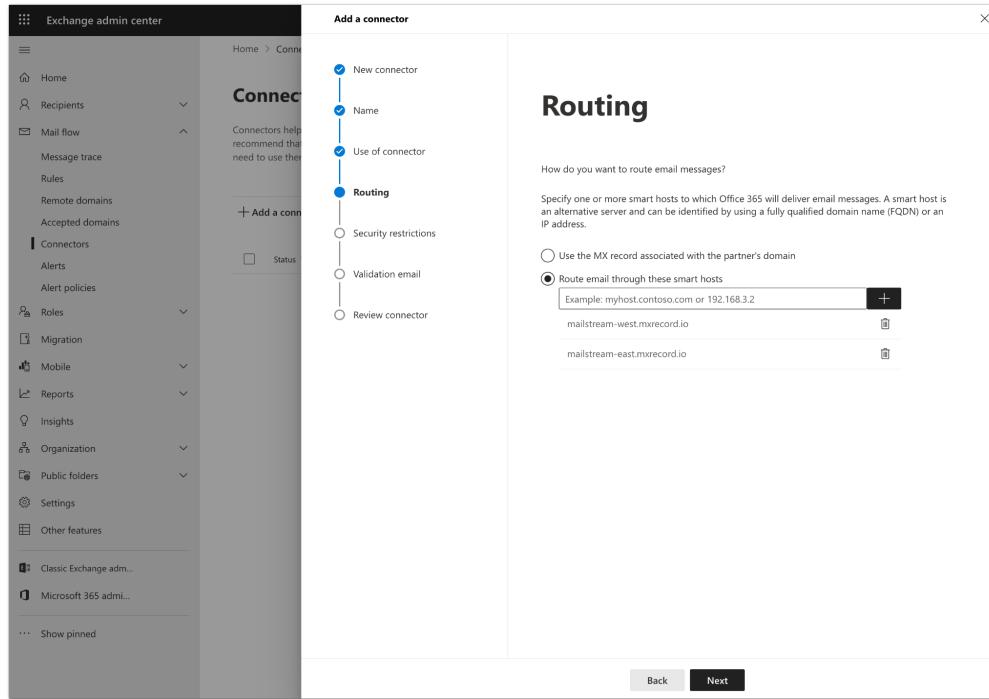
4. Configure the **Use of connector** setting:

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

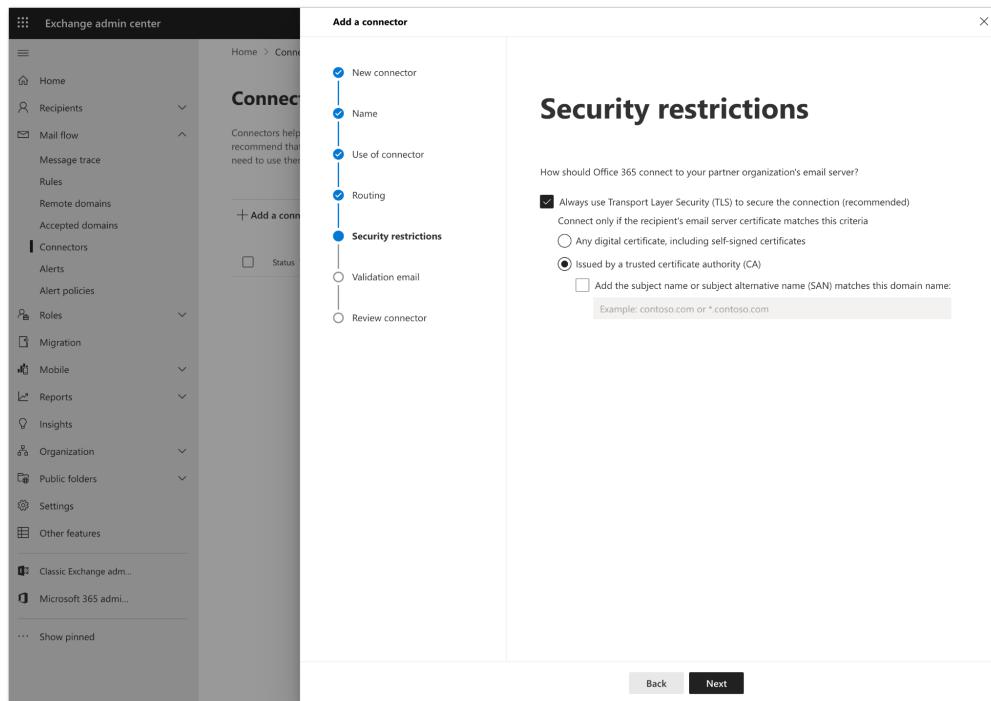
- mailstream-east.mxrecord.io
- mailstream-west.mxrecord.io



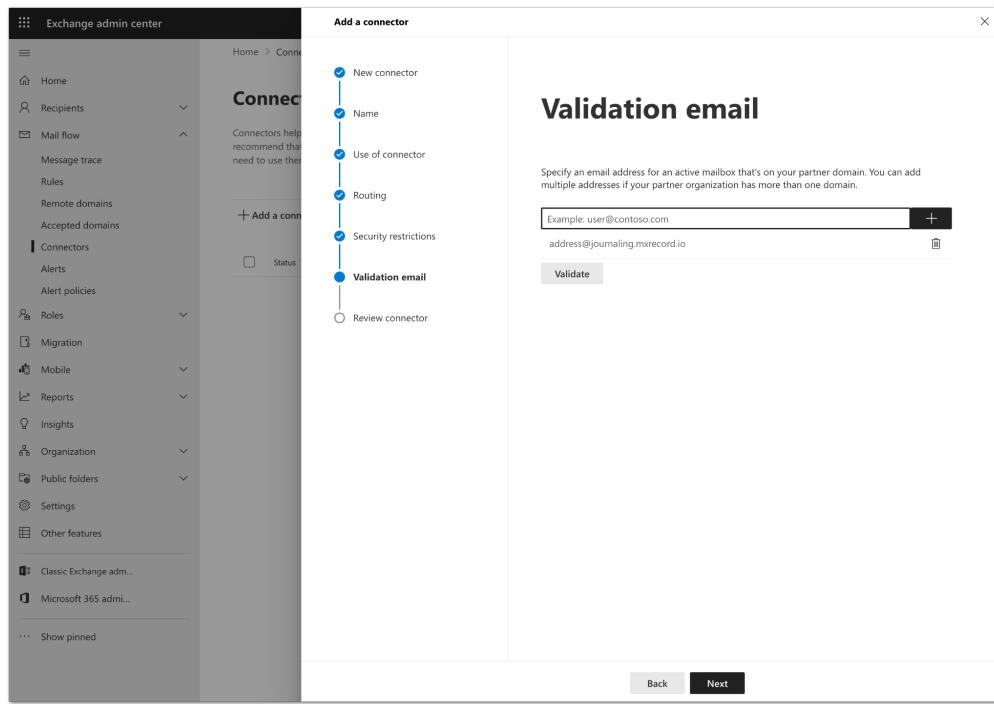
If there is a requirement to enforce traffic through the EU region use the following smarthost instead:

- mailstream-eu1.mxrecord.io

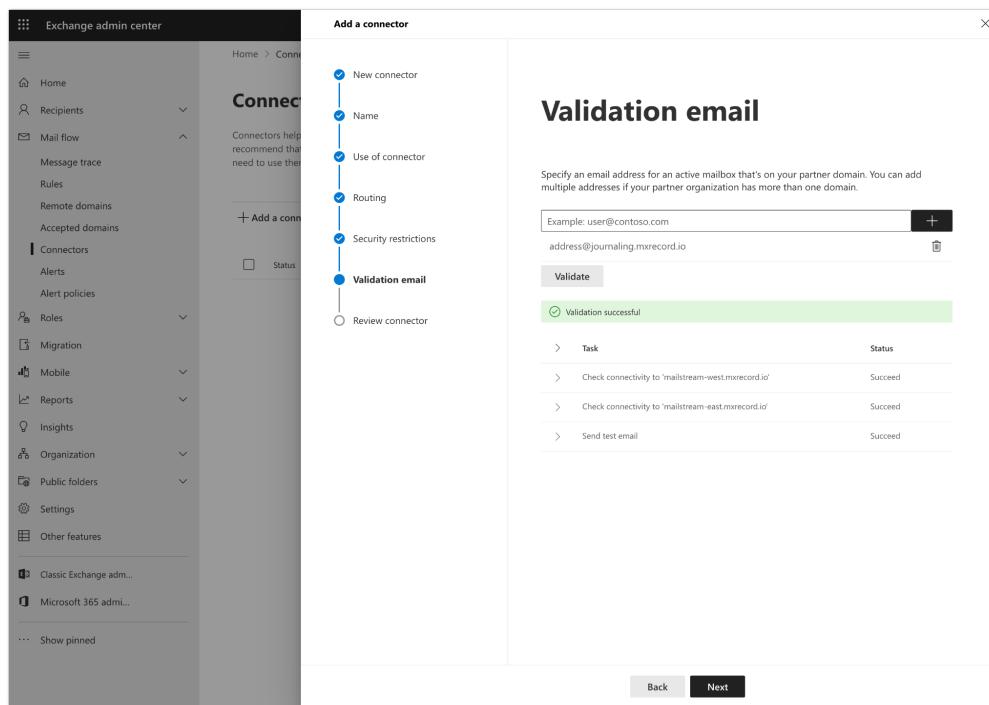
6. Preserve the default TLS configuration:



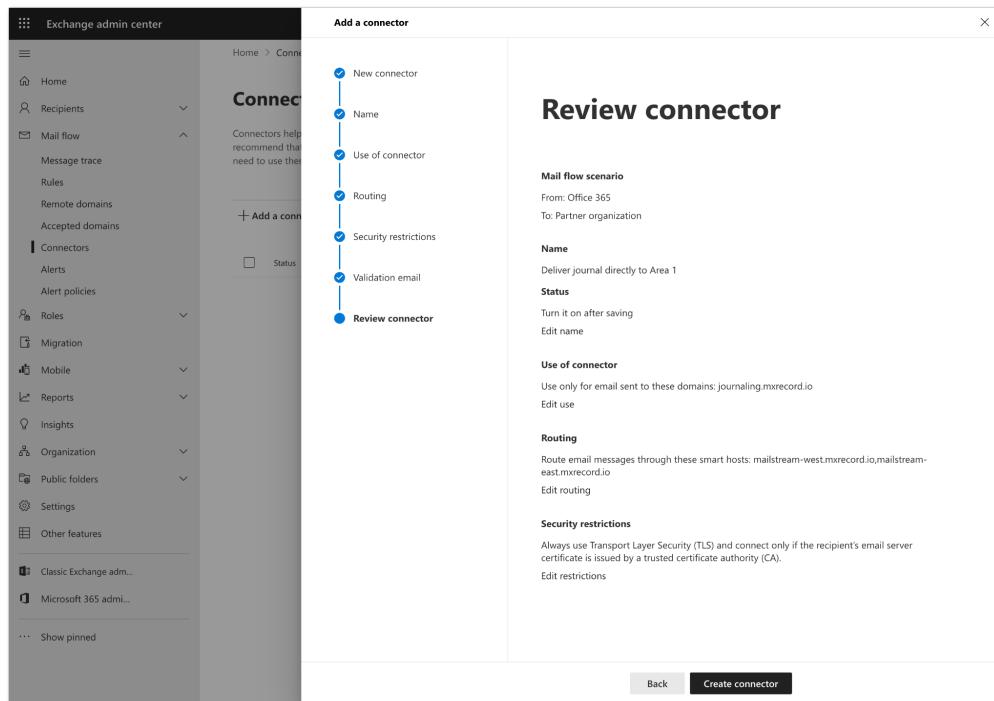
7. Validate the connector by using your tenant's specific journaling address. This address can be found in the Area 1 Horizon portal in the Support > Service Addresses page (<https://horizon.area1security.com/support/service-addresses>):



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 includes sections for Home, Recipients, Mail flow (with sub-options like Message trace, Rules, Remote domains, Accepted domains), Connectors (selected), Alerts, Alert policies, Roles, Migration, Mobile, Reports, Insights, Organization, Public folders, Settings, and Other features. At the bottom of the sidebar are links for "Classic Exchange adm..." and "Microsoft 365 adm...". 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 table with one item:

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

At the top right of the main area are "Dark mode" settings and a search bar. On the far right, there are three small icons.

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.

The screenshot shows the 'Undeliverable reports' section of the 'Settings' page. It includes a description of what undeliverable reports are and a field to enter an email address for sending undeliverable journal reports. A 'Save' button is at the bottom.

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

The screenshot shows the 'Journal rules' configuration page. It has tabs for MRM Retention policies, MRM Retention tags, and Journal rules (which is selected). A note about journaling outside of Microsoft 365 is present. Below, there's a search bar and a table with columns for Name, Status, User, and 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

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

Next Cancel

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

Exchange (legacy) > Create journal rule

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]

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. A modal window titled 'Select a user or group to journal' is open on the right. 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 to the top, with the 'Unpin' button highlighted by a blue arrow. The main navigation bar includes 'Home', 'Users' (which is pinned), 'Active users', 'Contacts', 'Guest users', 'Deleted users', 'Groups' (which is pinned), 'Active groups' (highlighted by a blue arrow), 'Deleted groups', and 'Shared mailboxes'. The title 'Active groups' is displayed prominently. Below it, a note states: 'It can take up to an hour for new distribution groups and mail-enabled security groups to appear in your Active groups list. If you don't see your new group yet, go to the Exchange admin center.' A link 'Learn more about group types' is also present. The top navigation bar has tabs for 'Microsoft 365' (selected), 'Distribution list', 'Mail-enabled security', and 'Security'. At the bottom, there are buttons for 'Add a group', 'Export', and 'Refresh'.

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 title is 'Choose a group type'. It says: 'Choose the group type that best meets your team's needs. Learn more about group types'. Three options are listed: 'Microsoft 365 (recommended)' (disabled), 'Distribution' (selected, highlighted by a blue arrow), and 'Mail-enabled security' (disabled). The 'Distribution' option is described as 'Creates an email address for a group of people.' 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 lists four items under 'Active groups': 'List', 'RBACDistribution', 'test', and 'Test'. A blue arrow points to the 'Test' entry. The table columns include 'Group name', 'Group email', 'Sync status', and 'Created on'. The 'Group name' column is sorted in ascending order.

Group name ↑	Group email	Sync status	Created on
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