CLOUDFLARE
AREA 1 SECURITY

Phishing Protection for Microsoft O365

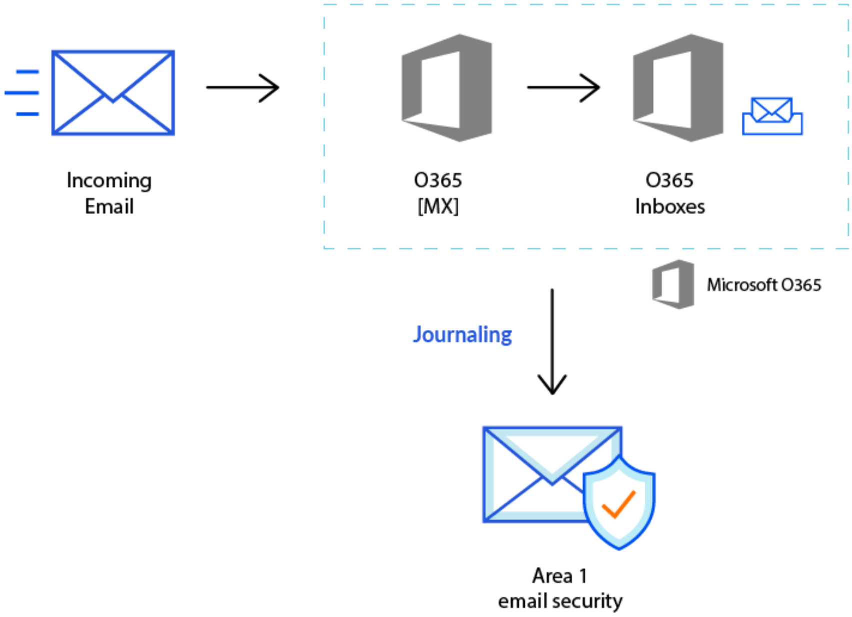
Deployment and Configuration Guide
O365 Journaling

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

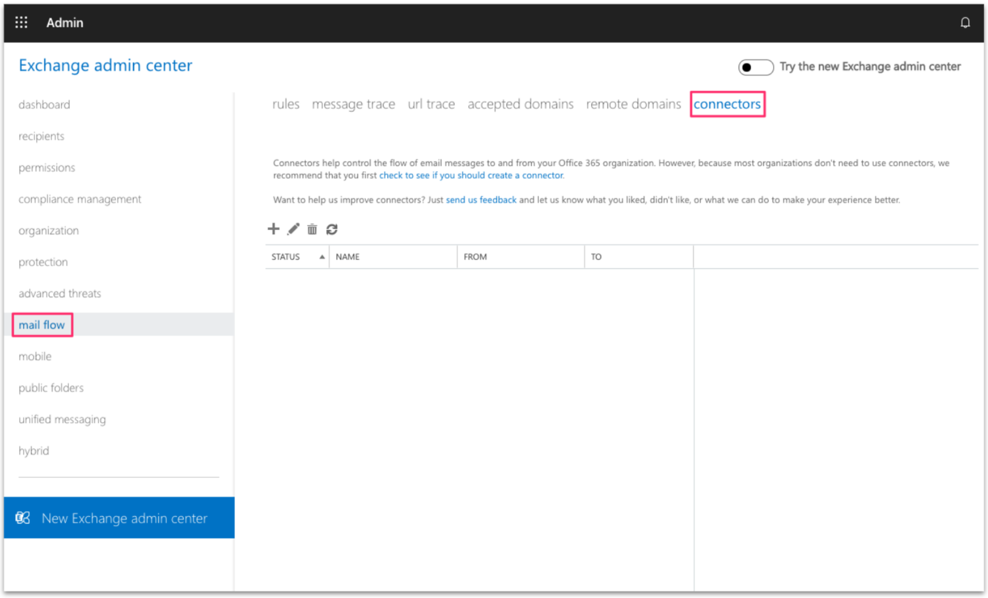
- Step 1: Configure connector for delivery to Area 1 (if required)
- Step 2: Configure Journal Rule

Step 1: Configure connector for delivery to 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. From the Exchange admin center, select the **connectors** configuration section from the **mail flow** configuration panel. Click the **+** button to configure a new connector.

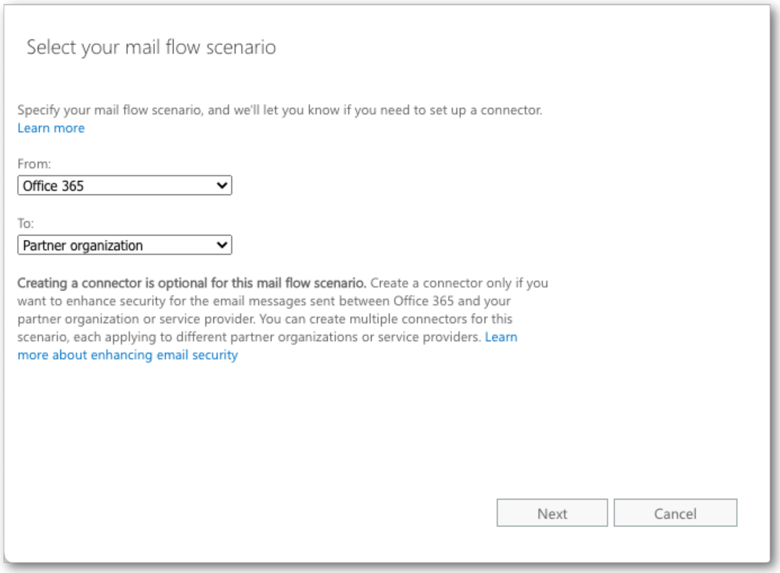


Connectors help control the flow of email messages to and from your Office 365 organization. However, because most organizations don't need to use connectors, we recommend that you first check to see if you should create a connector.

Want to help us improve connectors? Just send us feedback and let us know what you liked, didn't like, or what we can do to make your experience better.

2. Configure the connector mail direction as follows:

   - **From**: Office 365
   - **To:** Partner Organization



Select your mail flow scenario

Specify your mail flow scenario, and we'll let you know if you need to set up a connector.
Learn more

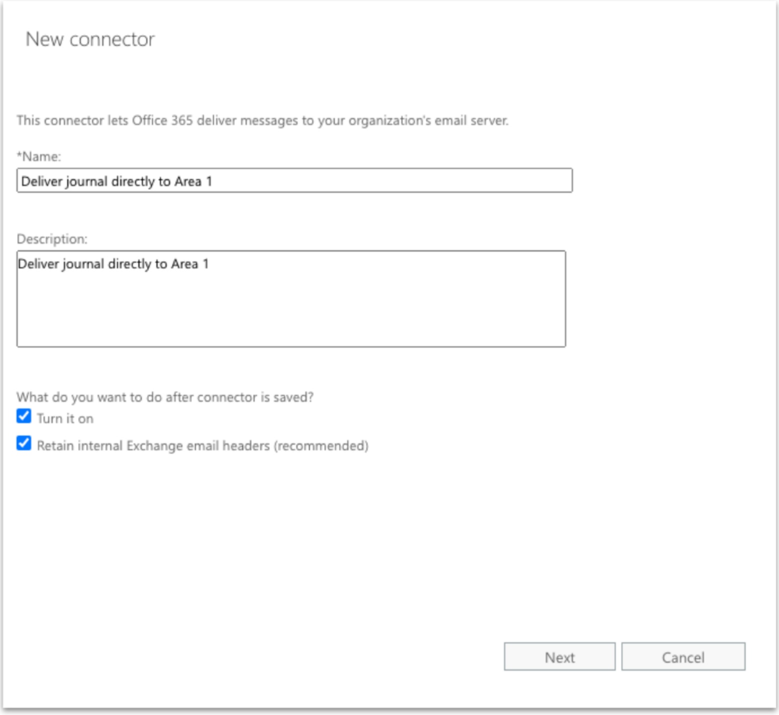
From:
Office 365

To:
Partner organization

Creating a connector is optional for this mail flow scenario. Create a connector only if you want to enhance security for the email messages sent between Office 365 and your partner organization or service provider. You can create multiple connectors for this scenario, each applying to different partner organizations or service providers. Learn more about enhancing email security

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
    - Select the **Retain internal Exchange email headers (recommended)** checkbox



New connector

This connector lets Office 365 deliver messages to your organization's email server.

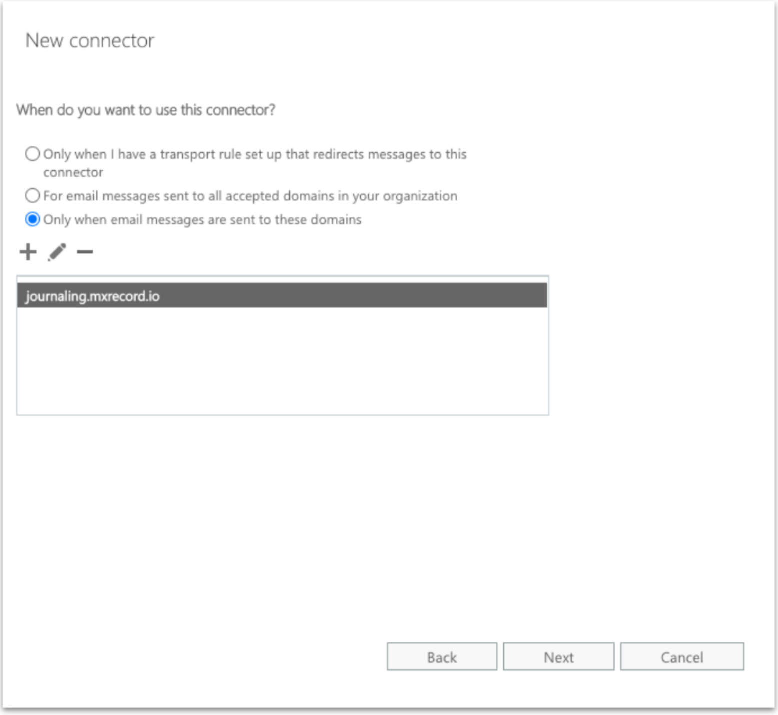
*Name:
Deliver journal directly to Area 1

Description:
Deliver journal directly to Area 1

What do you want to do after connector is saved?
☑ Turn it on
☑ Retain internal Exchange email headers (recommended)

4. Configure the **When do you want to use this connector?** setting:

    - Select **Only when email messages are sent to these domains** option
    - Click the **+** button and add the entry **journaling.mxrecord.io** in the configuration pop-up.



New connector

When do you want to use this connector?

○ Only when I have a transport rule set up that redirects messages to this connector

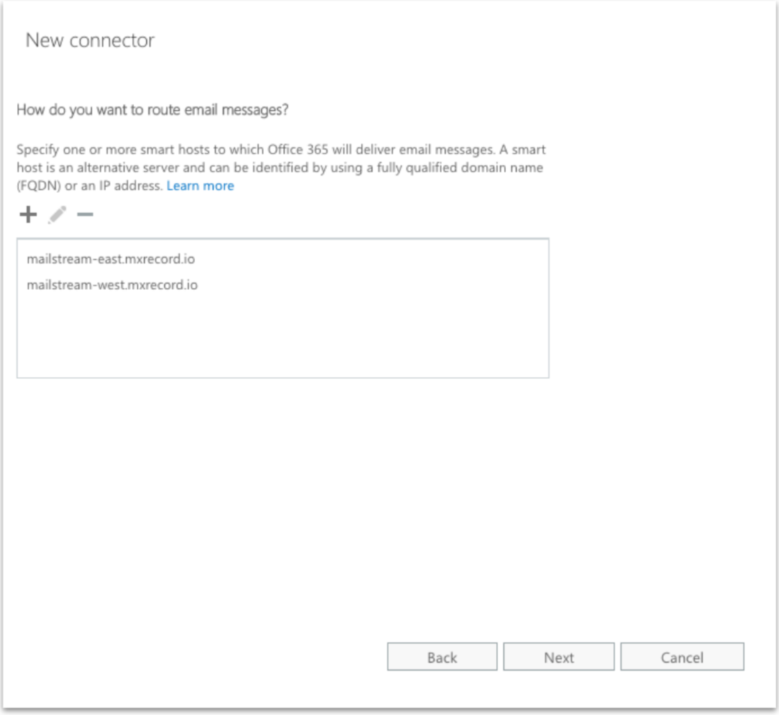
○ For email messages sent to all accepted domains in your organization

● Only when email messages are sent to these domains

journaling.mxrecord.io

5. Configure the **How do you want to route email messages?** setting by specifying the following smarthosts:

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



New connector

How do you want to route email messages?

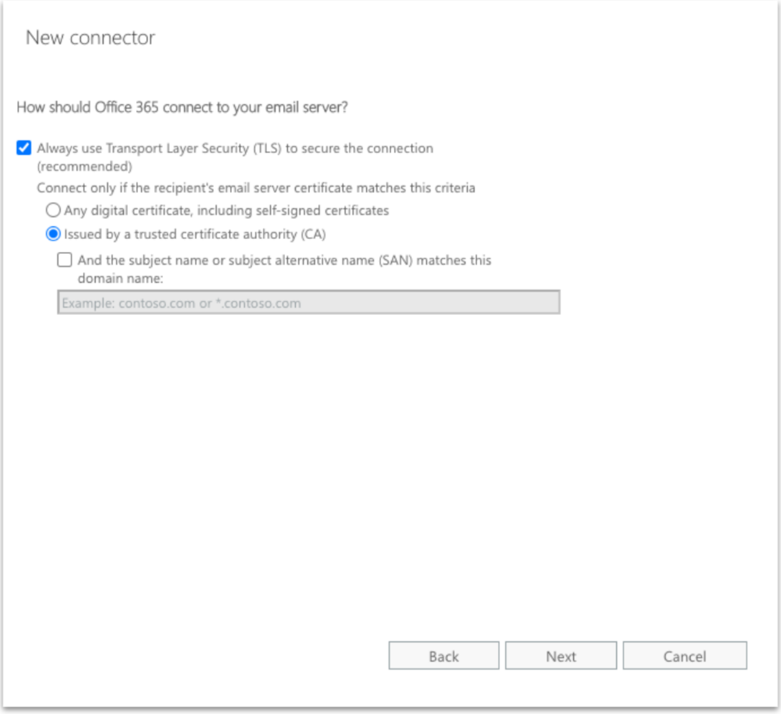
Specify one or more smart hosts to which Office 365 will deliver email messages. A smart host is an alternative server and can be identified by using a fully qualified domain name (FQDN) or an IP address. Learn more

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

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

- mailstream-eu1.mxrecord.io

6. Preserve the default TLS configuration:



New connector

How should Office 365 connect to your 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

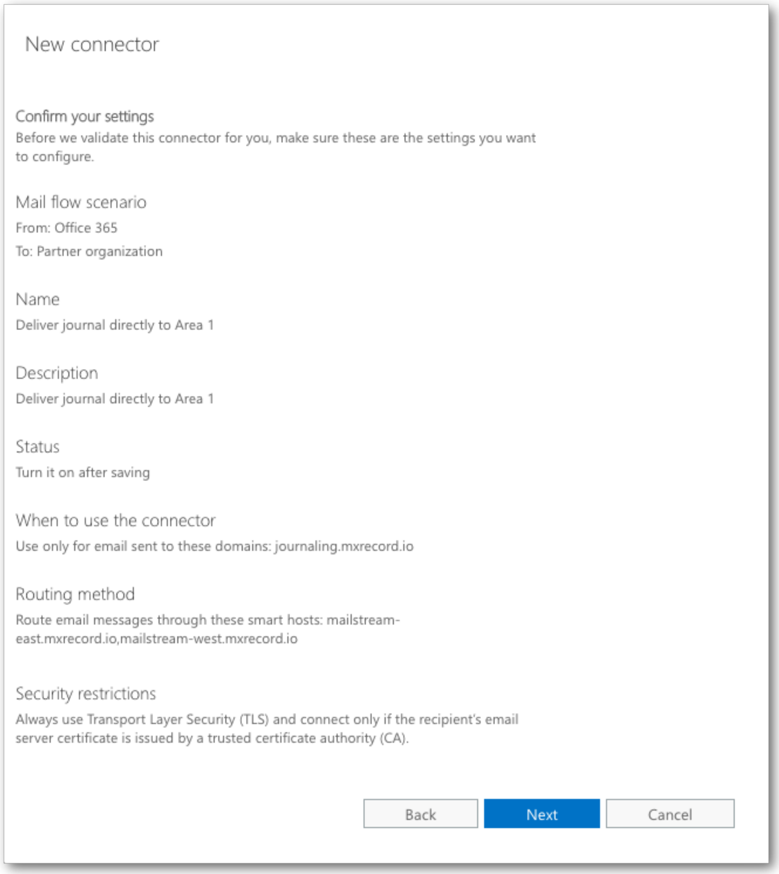
○ Any digital certificate, including self-signed certificates

● Issued by a trusted certificate authority (CA)

□ And the subject name or subject alternative name (SAN) matches this domain name:

Example: contoso.com or *.contoso.com

7. Confirm the connector configuration:



New connector

Confirm your settings

Before we validate this connector for you, make sure these are the settings you want to configure.

Mail flow scenario

From: Office 365

To: Partner organization

Name

Deliver journal directly to Area 1

Description

Deliver journal directly to Area 1

Status

Turn it on after saving

When to use the connector

Use only for email sent to these domains: journaling.mxrecord.io

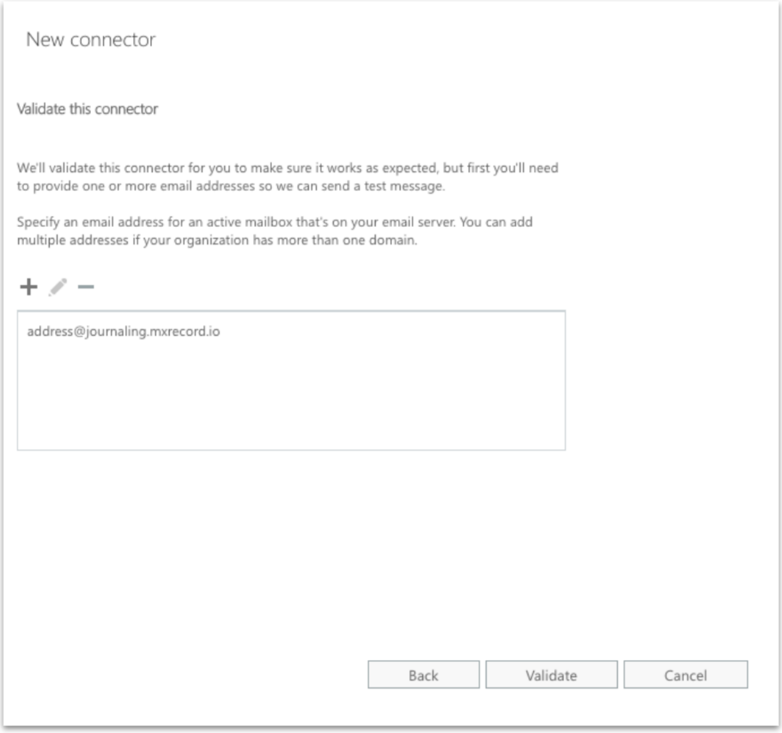
Routing method

Route email messages through these smart hosts: mailstream-east.mxrecord.io,mailstream-west.mxrecord.io

Security restrictions

Always use Transport Layer Security (TLS) and connect only if the recipient's email server certificate is issued by a trusted certificate authority (CA).

8. Validate the connector by using the provided journaling address:



New connector

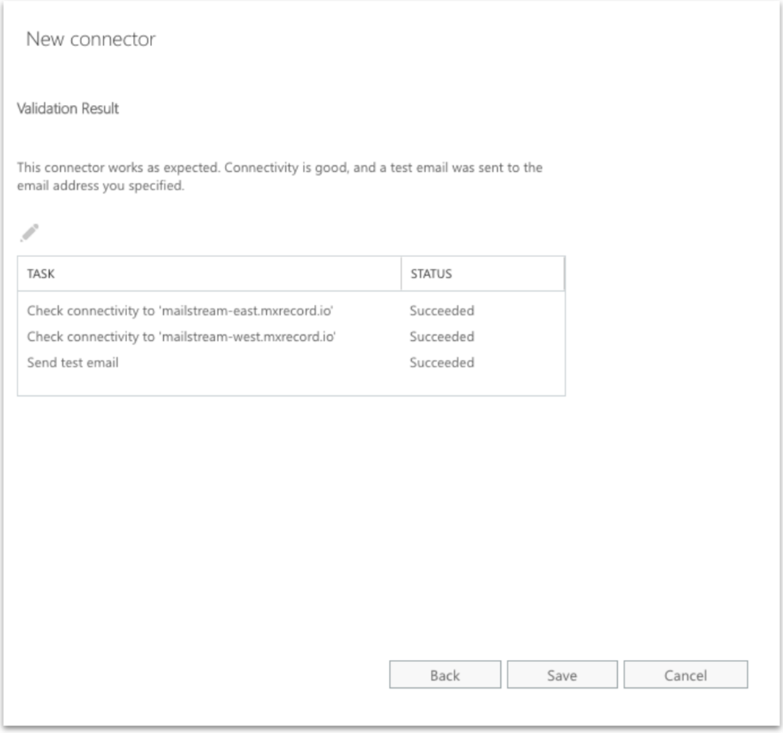
Validate this connector

We'll validate this connector for you to make sure it works as expected, but first you'll need to provide one or more email addresses so we can send a test message.

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

address@journaling.mxrecord.io

9. Once the validation completes, you should receive a **Succeeded** status for all 3 tasks and you can **save** this new connector:



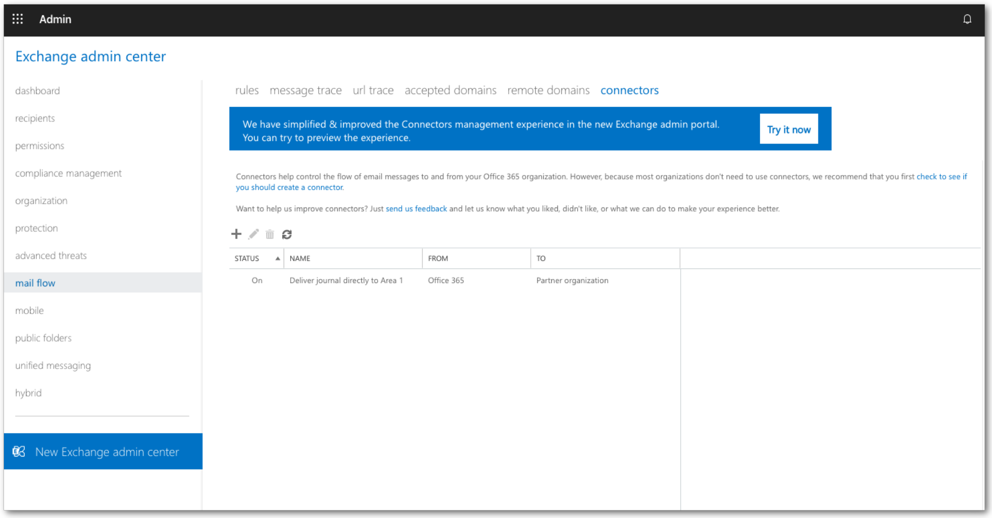
New connector

Validation Result

This connector works as expected. Connectivity is good, and a test email was sent to the email address you specified.

TASK	STATUS
Check connectivity to 'mailstream-east.mxrecord.io'	Succeeded
Check connectivity to 'mailstream-west.mxrecord.io'	Succeeded
Send test email	Succeeded

10. Once saved, the connector will be active:



We have simplified & improved the Connectors management experience in the new Exchange admin portal.
You can try to preview the experience.

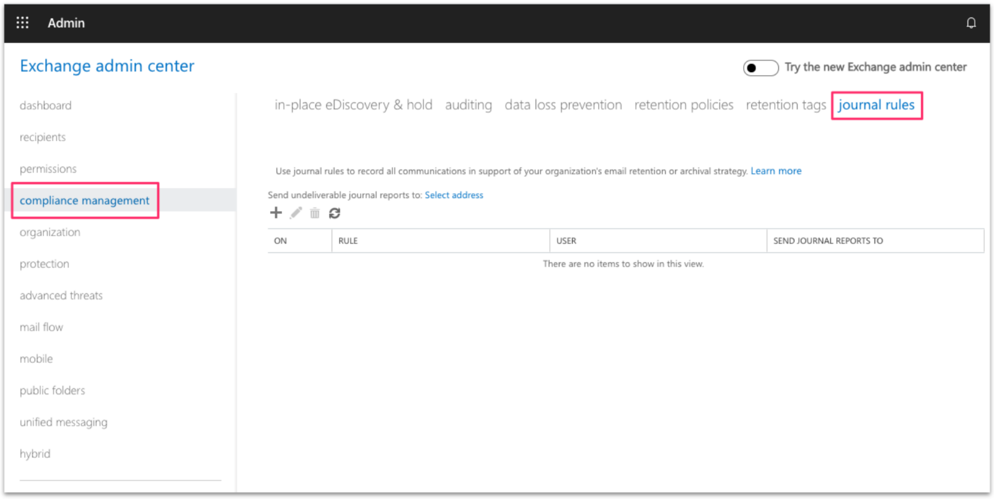
Connectors help control the flow of email messages to and from your Office 365 organization. However, because most organizations don't need to use connectors, we recommend that you first check to see if you should create a connector.

Want to help us improve connectors? Just send us feedback and let us know what you liked, didn't like, or what we can do to make your experience better.

STATUS ▲	NAME	FROM	TO
On	Deliver journal directly to Area 1	Office 365	Partner organization

Step 2: Configure Journal Rule

1. From the Exchange admin center, select the **journal rules** configuration section from the **compliance management** configuration panel.



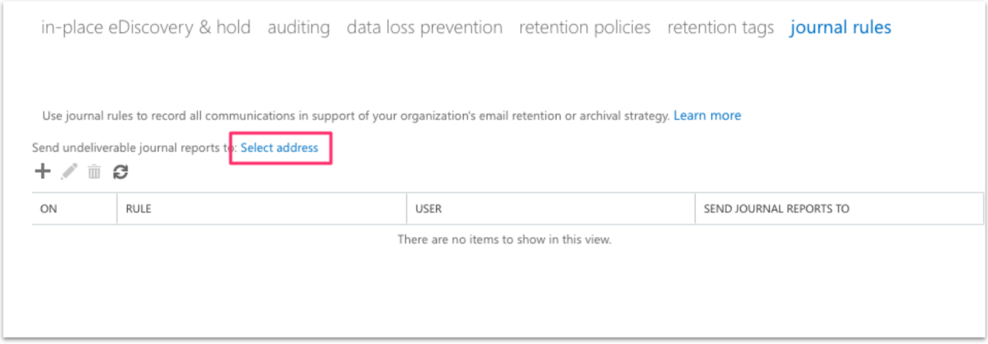
Use journal rules to record all communications in support of your organization's email retention or archival strategy. Learn more

Send undeliverable journal reports to: Select address

ON	RULE	USER	SEND JOURNAL REPORTS TO

There are no items to show in this view.

2. If you do not have an **undeliverable journal reports** address already configured, click on the **Select address** link to specify a mailbox that should receive any delivery bounces. Without a configured address, you will not be able to save the journal rule.



Use journal rules to record all communications in support of your organization's email retention or archival strategy. Learn more

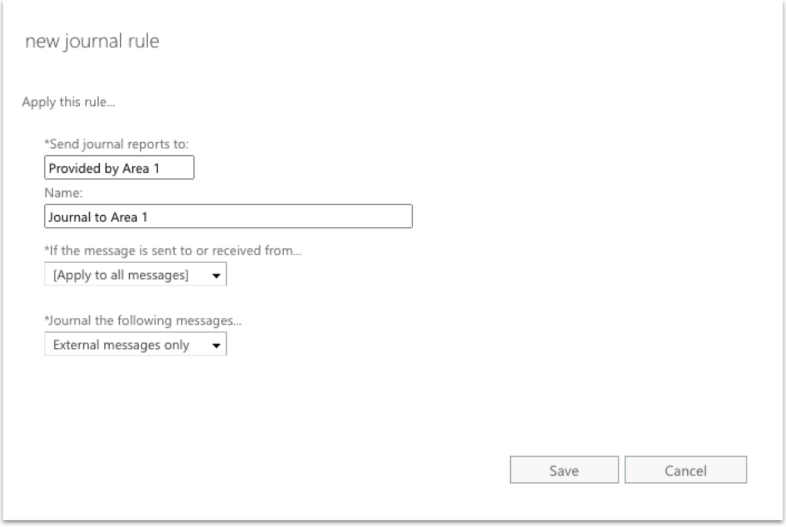
Send undeliverable journal reports to: Select address

ON	RULE	USER	SEND JOURNAL REPORTS TO

There are no items to show in this view.

3. Click on the **+** button to configure a journaling rule, and configure the journaling rule as follows:

    - **Send journal reports to:** This address will be provided by Area 1
    - **Name:** Journal Messages to Area 1
    - **If the message is sent to or received from…:** [Apply to all messages]
    - **Journal the following messages…:** External messages only



new journal rule

Apply this rule...

*Send journal reports to:
Provided by Area 1

Name:
Journal to Area 1

*If the message is sent to or received from...
[Apply to all messages]

*Journal the following messages...
External messages only

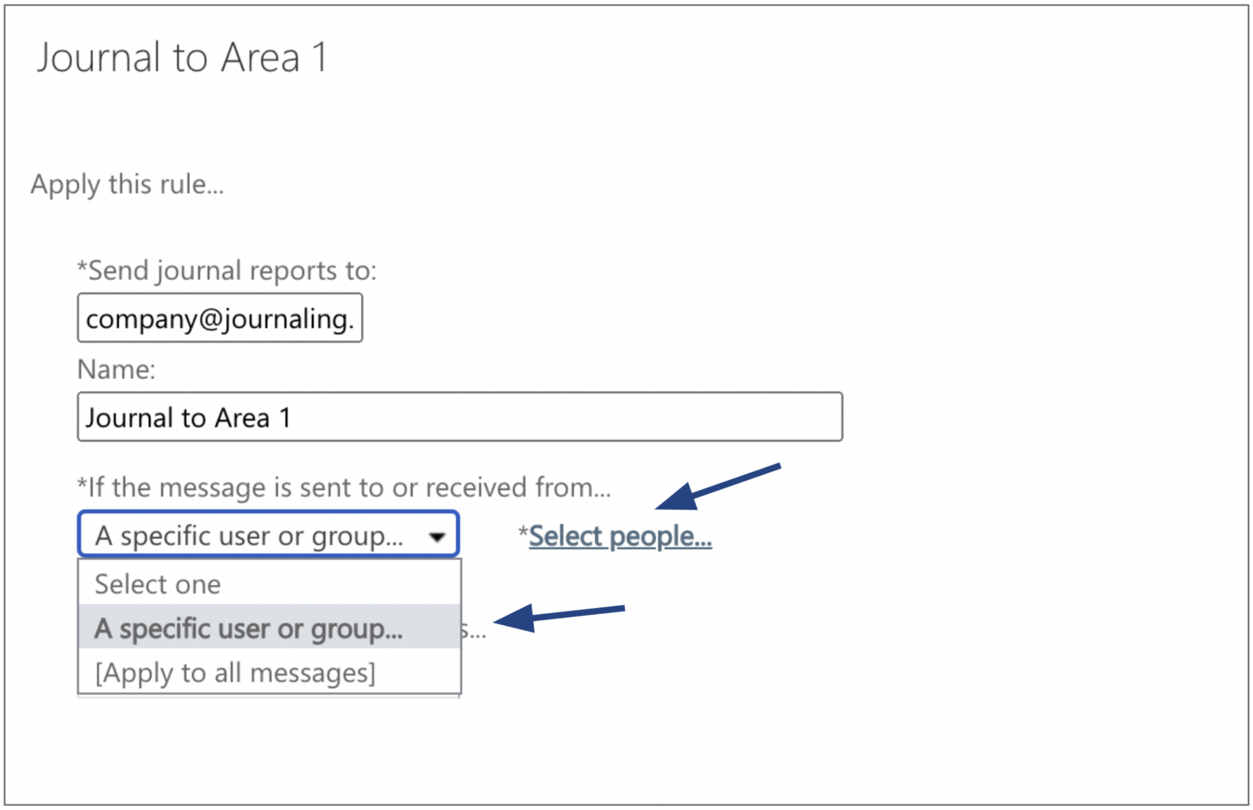
4. Click **Save** to save the journaling rule and acknowledge the warning indicating that the rule will only apply to future messages, once saved the rule is automatically active and may take a few minutes for the configuration to propagate and start to push messages to Area 1.

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

- **If the message is sent to or received from…:** [A specific user or group]



Journal to Area 1

Apply this rule...

*Send journal reports to: company@journaling.

Name: Journal to Area 1

*If the message is sent to or received from...

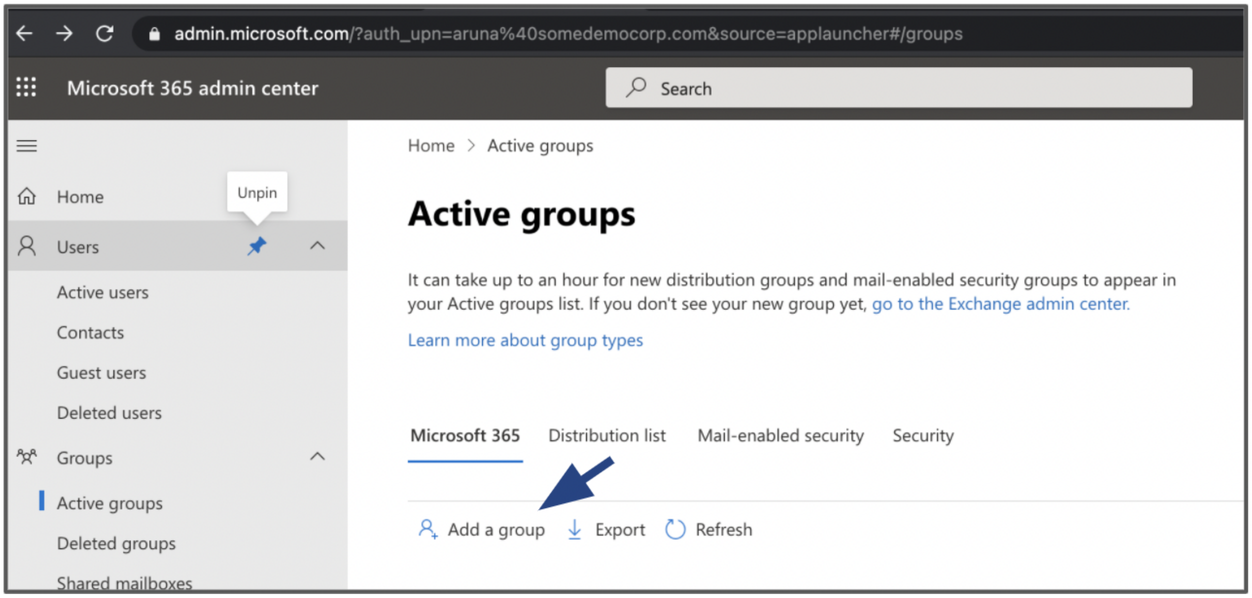
A specific user or group... *Select people...

- 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

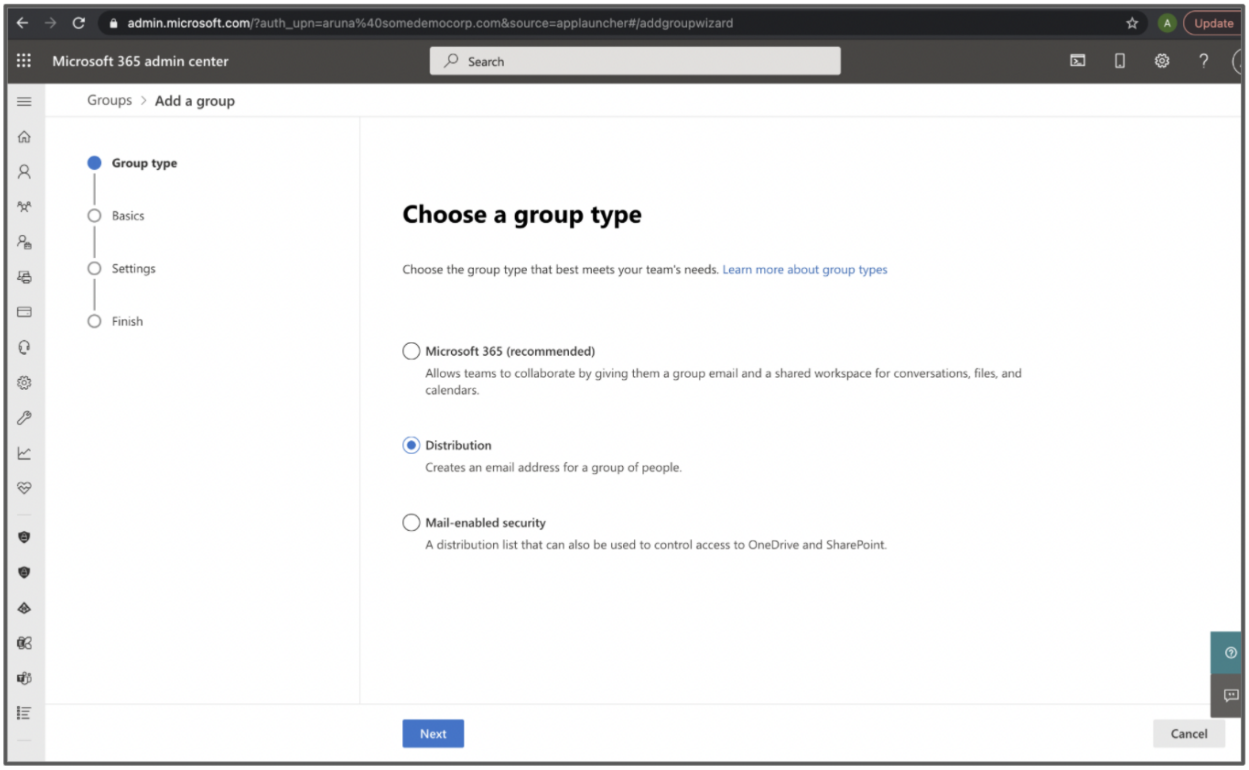


Active groups

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.

Learn more about group types

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



admin.microsoft.com/?auth_upn=aruna%40somedemocorp.com&source=applauncher#/addgroupwizard
Update
Microsoft 365 admin center
Search
Groups > Add a group
Group type
Basics
Settings
Finish

Choose a group type

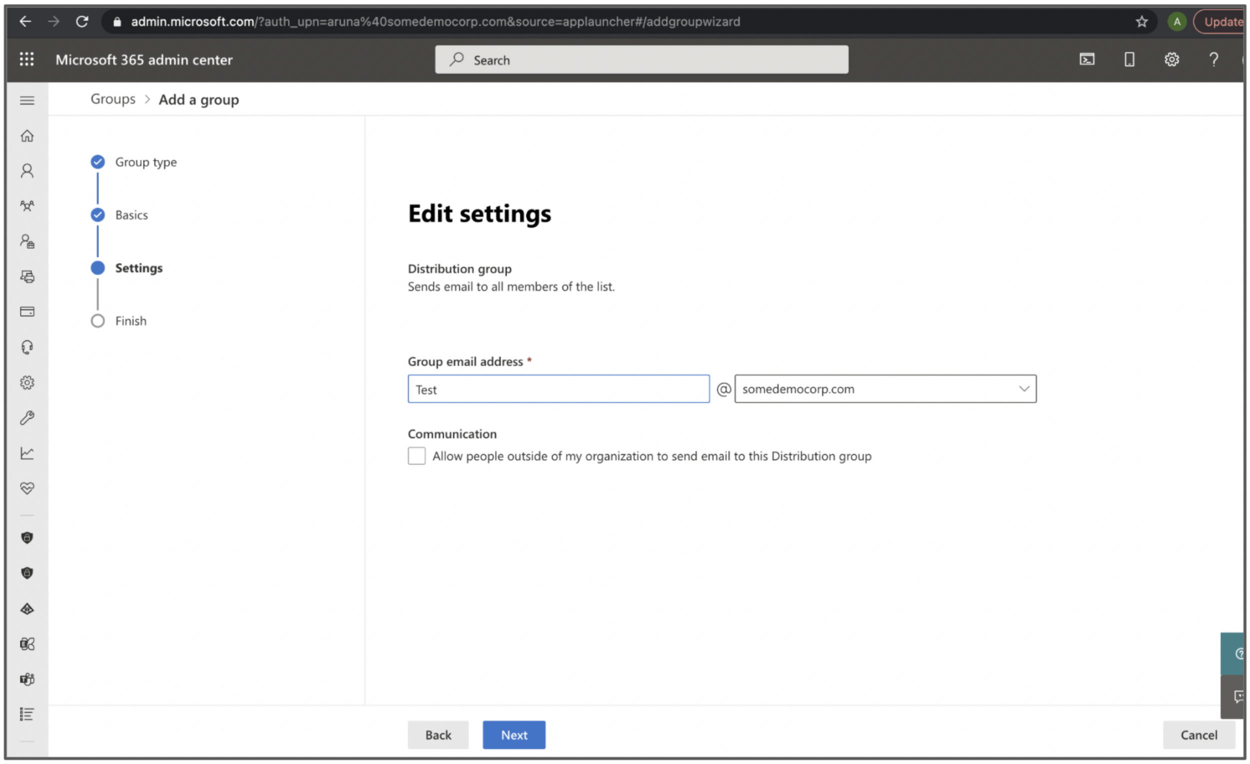
Choose the group type that best meets your team's needs. Learn more about group types

○ Microsoft 365 (recommended)
Allows teams to collaborate by giving them a group email and a shared workspace for conversations, files, and calendars.

● Distribution
Creates an email address for a group of people.

○ Mail-enabled security
A distribution list that can also be used to control access to OneDrive and SharePoint.

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


admin.microsoft.com/?auth_upn=aruna%40somedemocorp.com&source=applauncher#/addgroupwizard
Update
Microsoft 365 admin center
Search
Groups > Add a group
Group type
Basics
Settings
Finish
Back
Next
Cancel

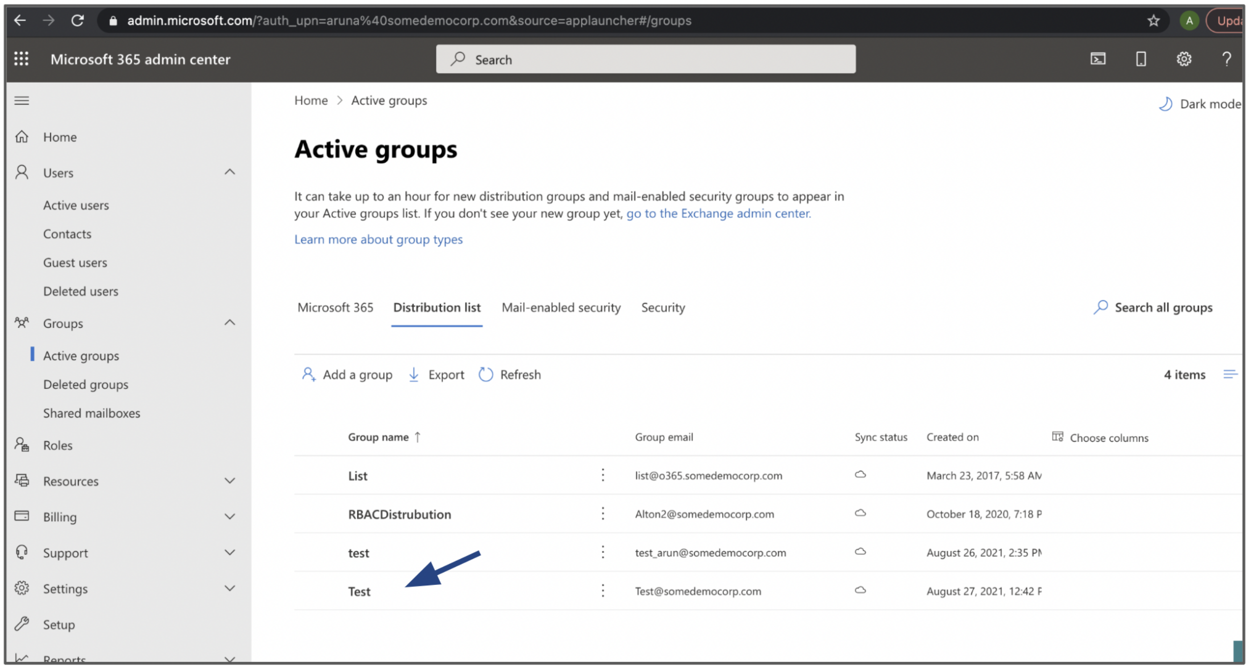
Edit settings

Distribution group
Sends email to all members of the list.

Group email address *
Test @ somedemocorp.com

Communication
□ Allow people outside of my organization to send email to this Distribution group

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



Active groups

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.

Learn more about group types

Group name ↑	Group email	Sync status	Created on
List	list@o365.somedemocorp.com	☁	March 23, 2017, 5:58 AN
RBACDistrubution	Alton2@somedemocorp.com	☁	October 18, 2020, 7:18 P
test	test_arun@somedemocorp.com	☁	August 26, 2021, 2:35 PI
Test	Test@somedemocorp.com	☁	August 27, 2021, 12:42 F