CLOUDFLARE
AREA 1 SECURITY

Email Security for Microsoft O365

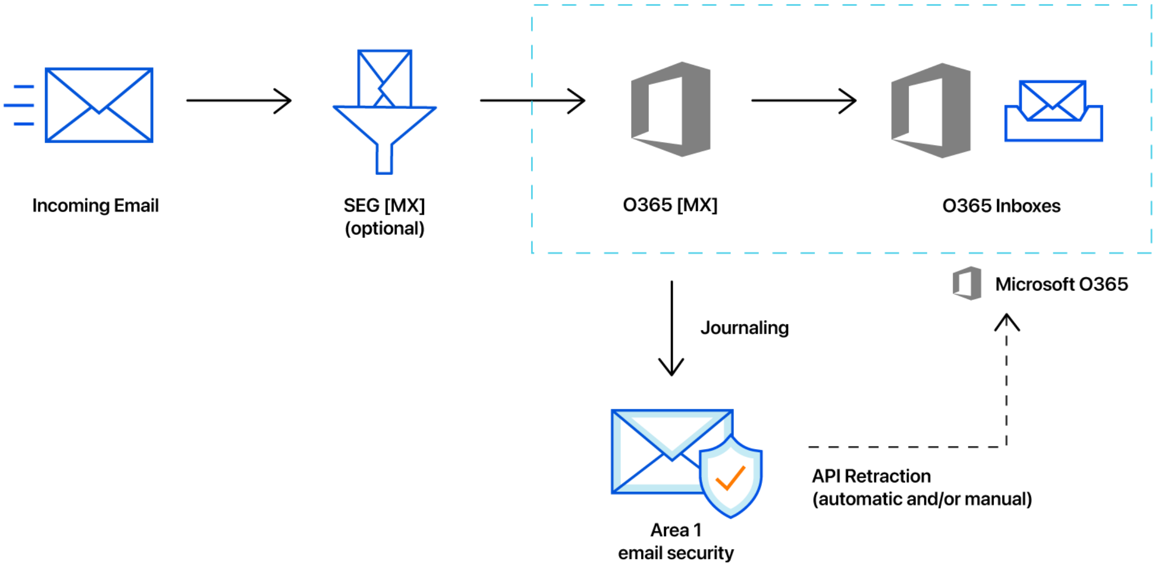
Deployment and Configuration Guide
Automatic Message Retraction

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

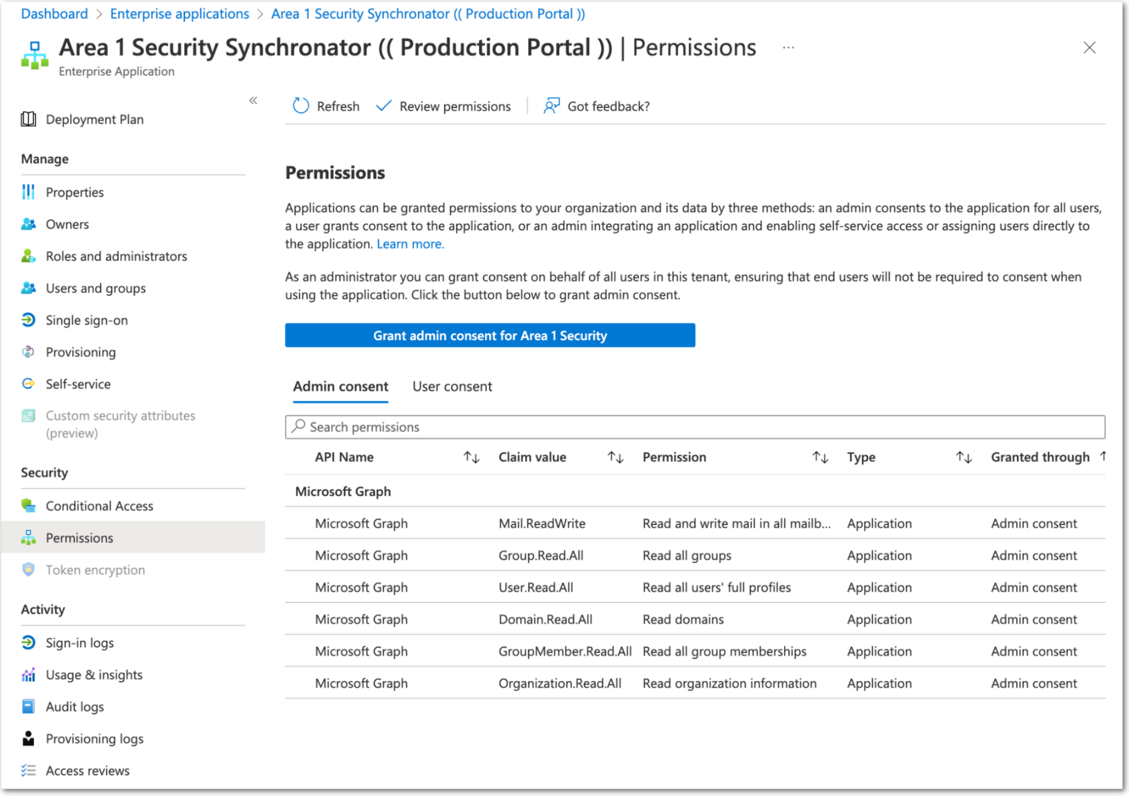
Step 1: Authorize Area 1 with O365 for Retraction

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.



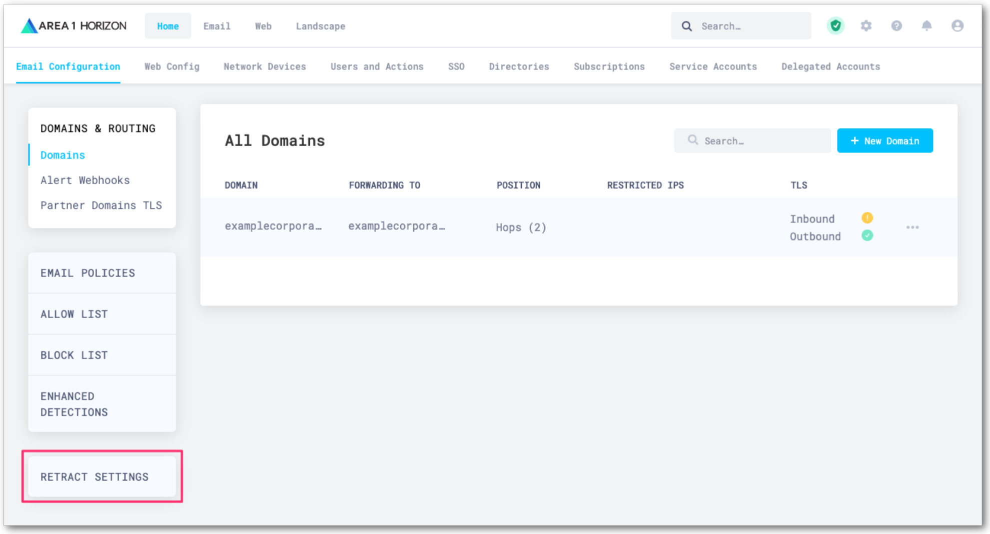
Permissions

Applications can be granted permissions to your organization and its data by three methods: an admin consents to the application for all users, a user grants consent to the application, or an admin integrating an application and enabling self-service access or assigning users directly to the application. Learn more.

As an administrator you can grant consent on behalf of all users in this tenant, ensuring that end users will not be required to consent when using the application. Click the button below to grant admin consent.

API Name ↑↓	Claim value ↑↓	Permission ↑↓	Type ↑↓	Granted through ↑
Microsoft Graph				
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

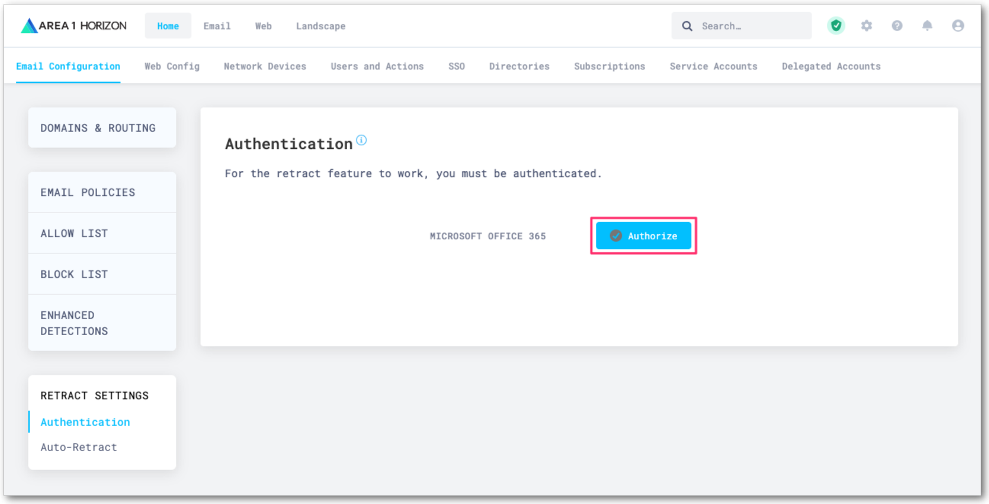
1. From the Area 1 Horizon Portal, access the Email Configuration section (https://horizon.area1security.com/settings/email/routing/domains) and select the **Retraction Settings** option on the left navigation bar:



DOMAIN	FORWARDING TO	POSITION	RESTRICTED IPS	TLS
examplecorpora…	examplecorpora…	Hops (2)		Inbound ● Outbound ✓

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

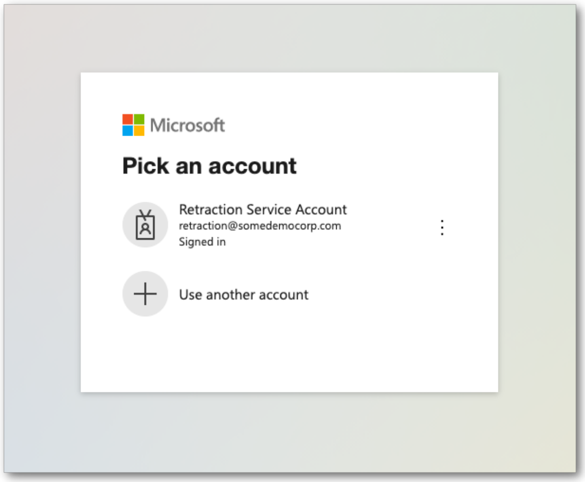
2. In the Retraction Settings section, you will need to authorize Area 1 to execute retractions through O365's Graph API. This is a simple process that requires you to authenticate and authorize Area 1 with O365. Ensure that the account that you will be using to authenticate has the appropriate administrative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



Authentication

For the retract feature to work, you must be authenticated.

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:

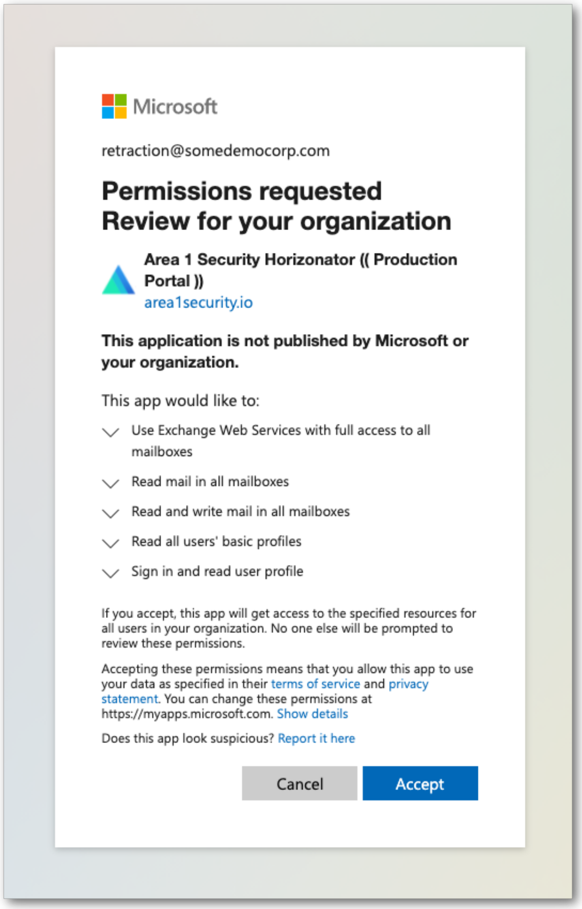


Pick an account

Retraction Service Account
retraction@somedemocorp.com
Signed in

Use another account

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



retraction@somedemocorp.com

Permissions requested
Review for your organization

Area 1 Security Horizonator ((Production Portal))
area1security.io

This application is not published by Microsoft or your organization.

This app would like to:

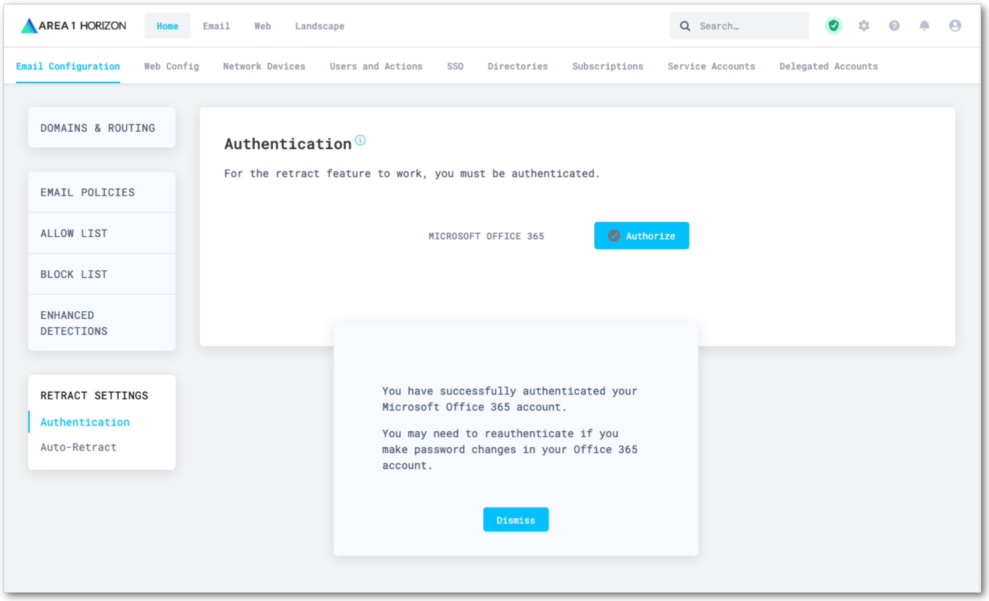
- Use Exchange Web Services with full access to all mailboxes
- Read mail in all mailboxes
- Read and write mail in all mailboxes
- Read all users' basic profiles
- Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

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:



Authentication

For the retract feature to work, you must be authenticated.

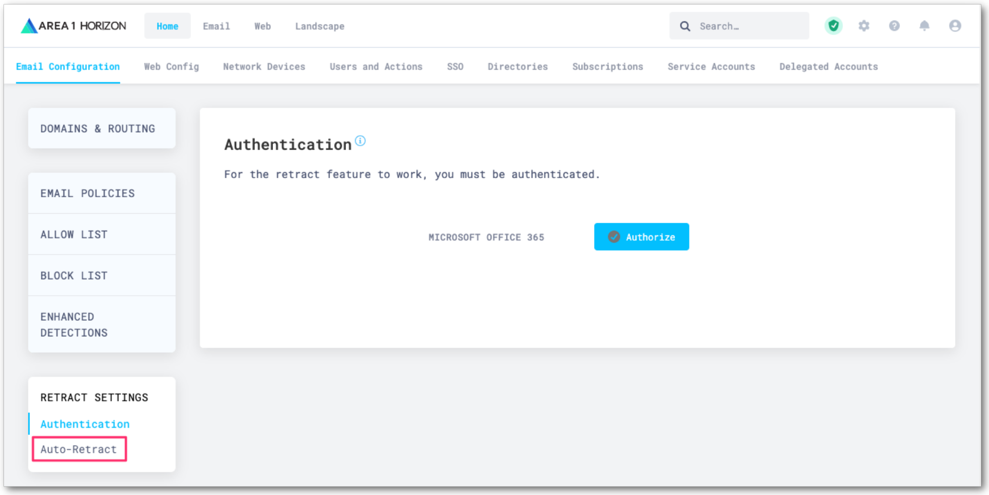
You have successfully authenticated your Microsoft Office 365 account.

You may need to reauthenticate if you make password changes in your Office 365 account.

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.

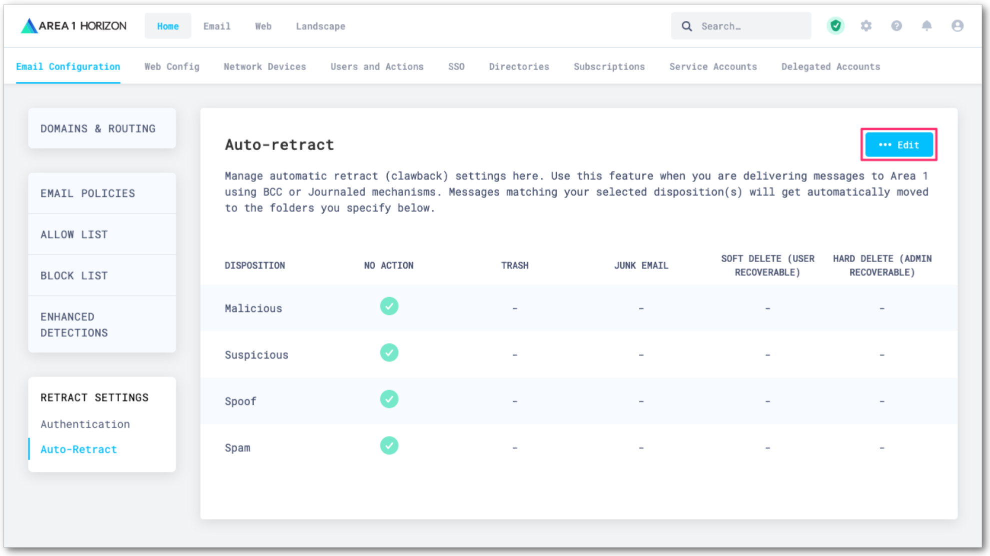
1. Click the **Auto-Retract** option on the left navigation bar to access retraction behavior setting:



Authentication

For the retract feature to work, you must be authenticated.

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

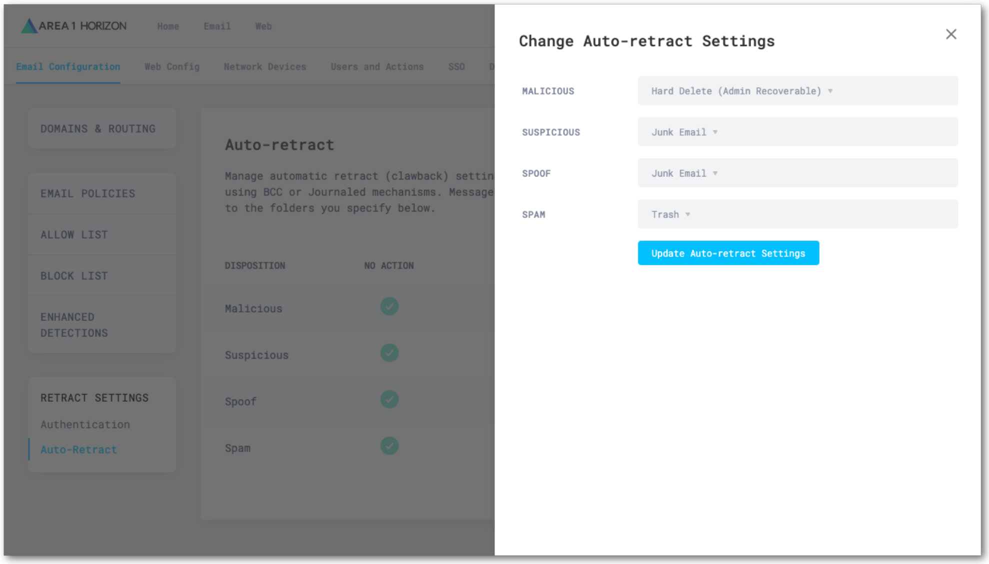


Auto-retract

Manage automatic retract (clawback) settings here. Use this feature when you are delivering messages to Area 1 using BCC or Journaled mechanisms. Messages matching your selected disposition(s) will get automatically moved to the folders you specify below.

DISPOSITION	NO ACTION	TRASH	JUNK EMAIL	SOFT DELETE (USER RECOVERABLE)	HARD DELETE (ADMIN RECOVERABLE)
Malicious	✓	-	-	-	-
Suspicious	✓	-	-	-	-
Spoof	✓	-	-	-	-
Spam	✓	-	-	-	-

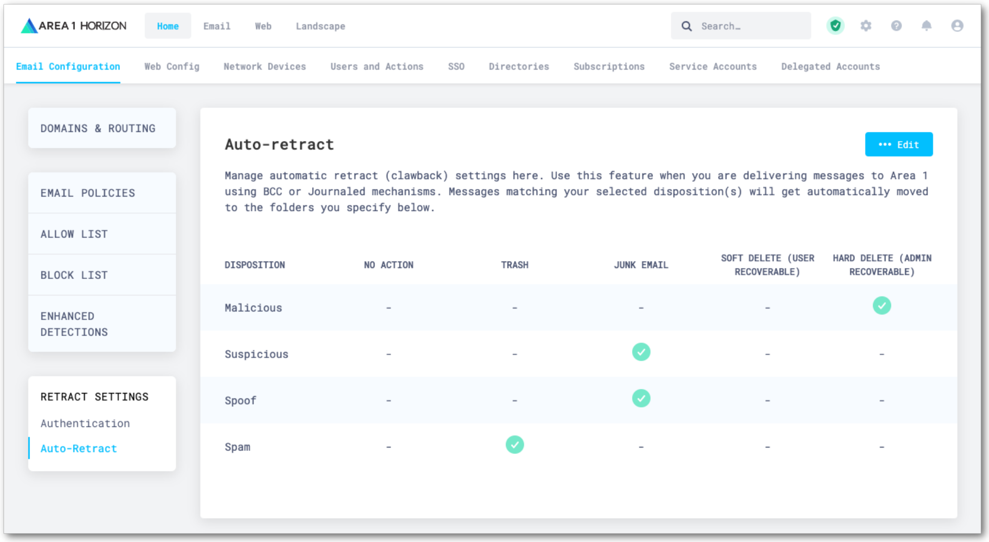
3. Select the appropriate remediation behavior for each dispositions and save your selection by clicking the **Update Auto-retraction Settings**:



Change Auto-retract Settings

MALICIOUS	Hard Delete (Admin Recoverable)
SUSPICIOUS	Junk Email
SPOOF	Junk Email
SPAM	Trash

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



Auto-retract

Manage automatic retract (clawback) settings here. Use this feature when you are delivering messages to Area 1 using BCC or Journaled mechanisms. Messages matching your selected disposition(s) will get automatically moved to the folders you specify below.

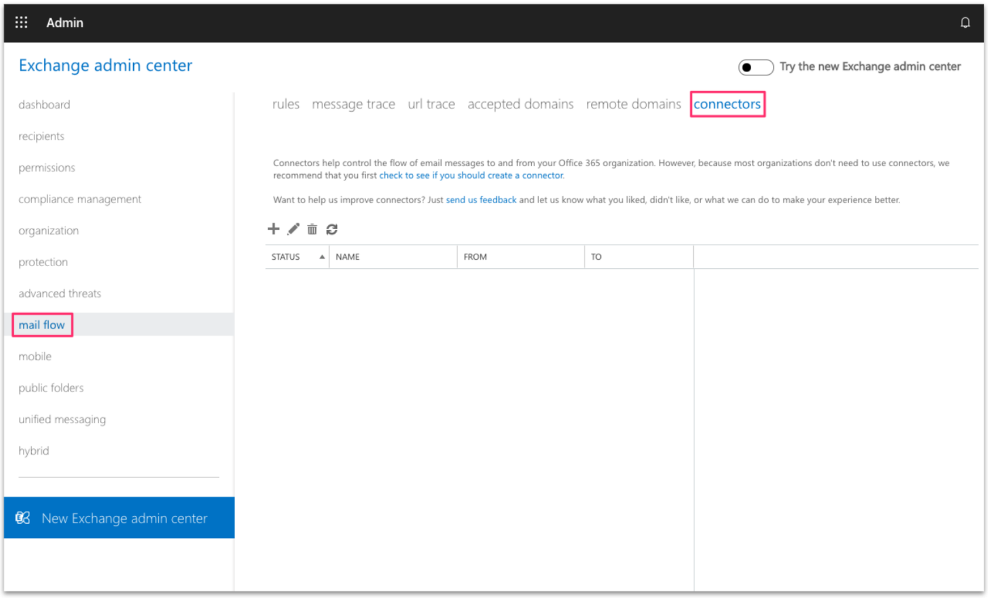
DISPOSITION	NO ACTION	TRASH	JUNK EMAIL	SOFT DELETE (USER RECOVERABLE)	HARD DELETE (ADMIN RECOVERABLE)
Malicious	-	-	-	-	✓
Suspicious	-	-	✓	-	-
Spoof	-	-	✓	-	-
Spam	-	✓	-	-	-

Step 3: 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.

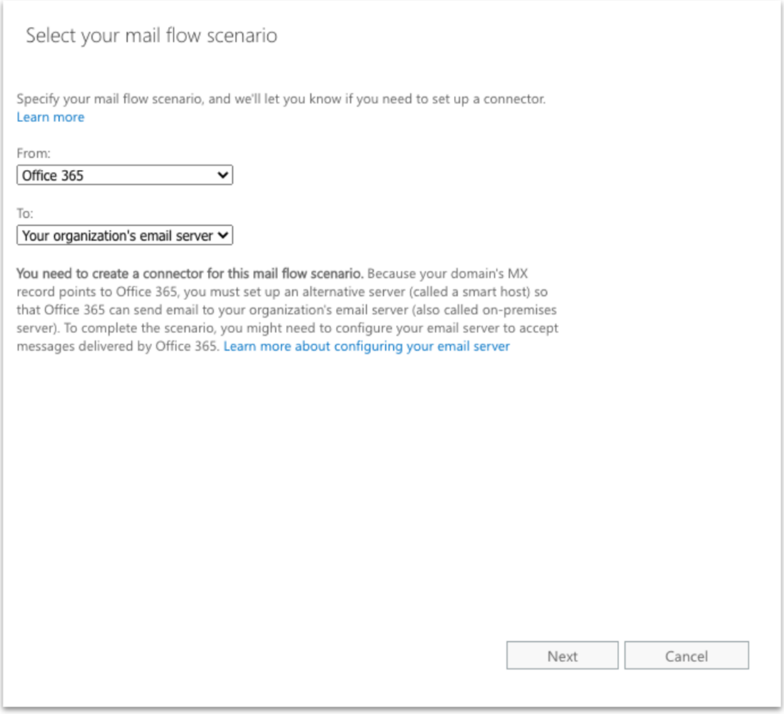


Connectors help control the flow of email messages to and from your Office 365 organization. However, because most organizations don't need to use connectors, we recommend that you first check to see if you should create a connector.

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:** Your organization's email server



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

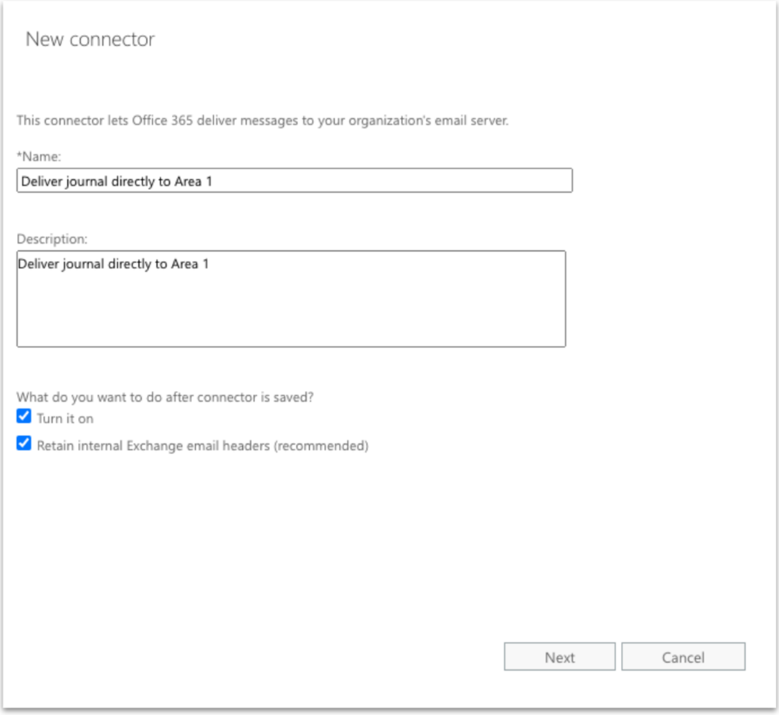
From:
Office 365

To:
Your organization's email server

You need to create a connector for this mail flow scenario. Because your domain's MX record points to Office 365, you must set up an alternative server (called a smart host) so that Office 365 can send email to your organization's email server (also called on-premises server). To complete the scenario, you might need to configure your email server to accept messages delivered by Office 365. Learn more about configuring your email server

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

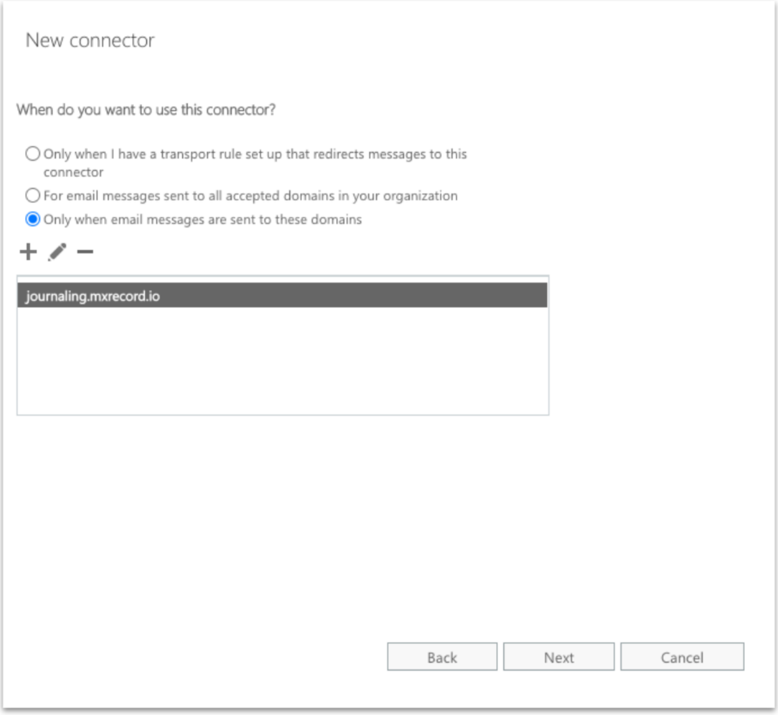
What do you want to do after connector is saved?

☑ 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

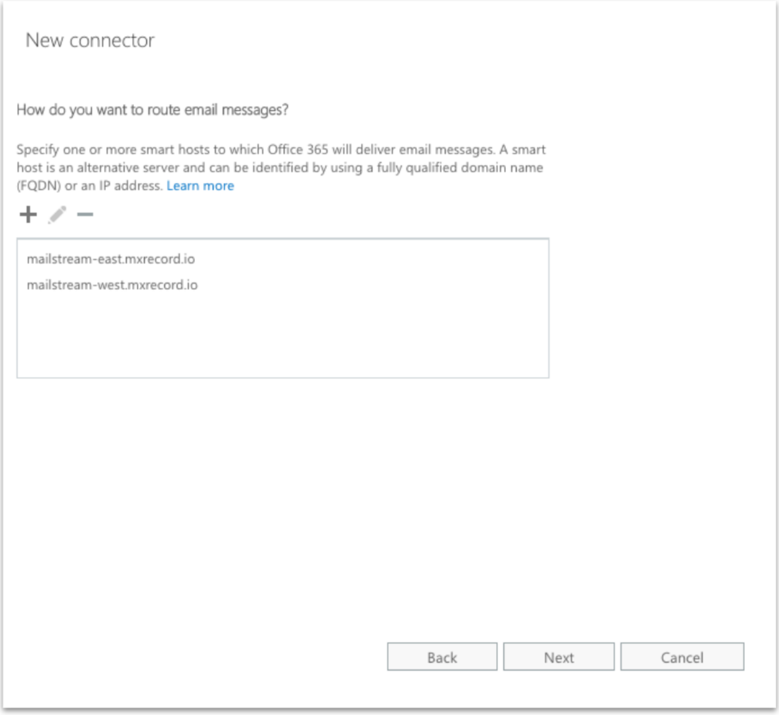
When do you want to use this connector?

○ 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: **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?

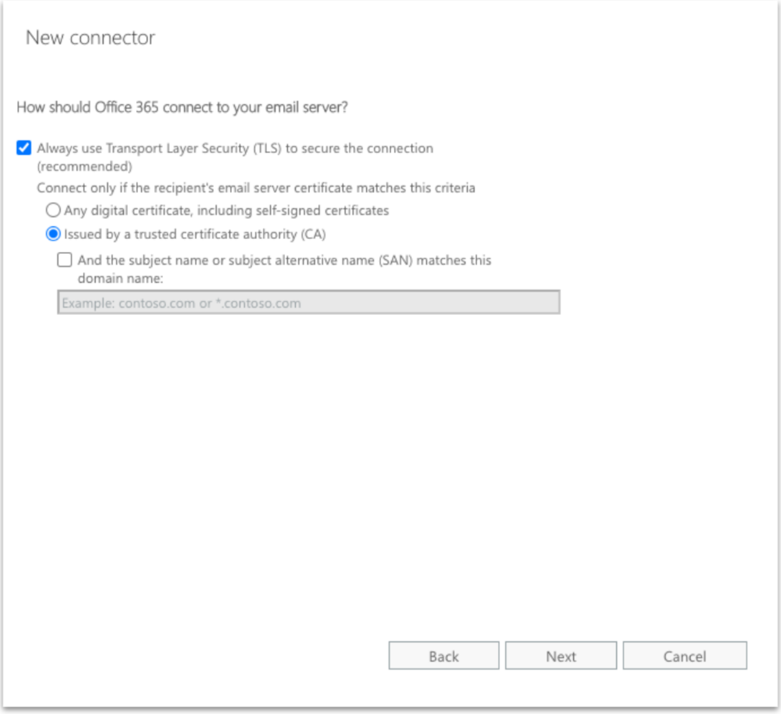
Specify one or more smart hosts to which Office 365 will deliver email messages. A smart host is an alternative server and can be identified by using a fully qualified domain name (FQDN) or an IP address. Learn more

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

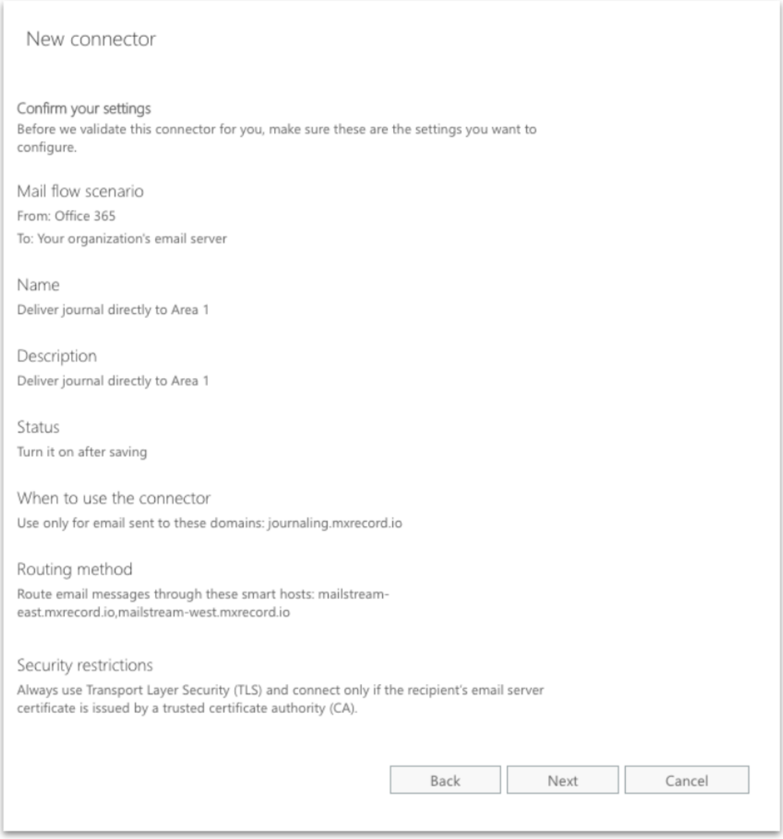
○ Any digital certificate, including self-signed certificates

● 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: Your organization's email server

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

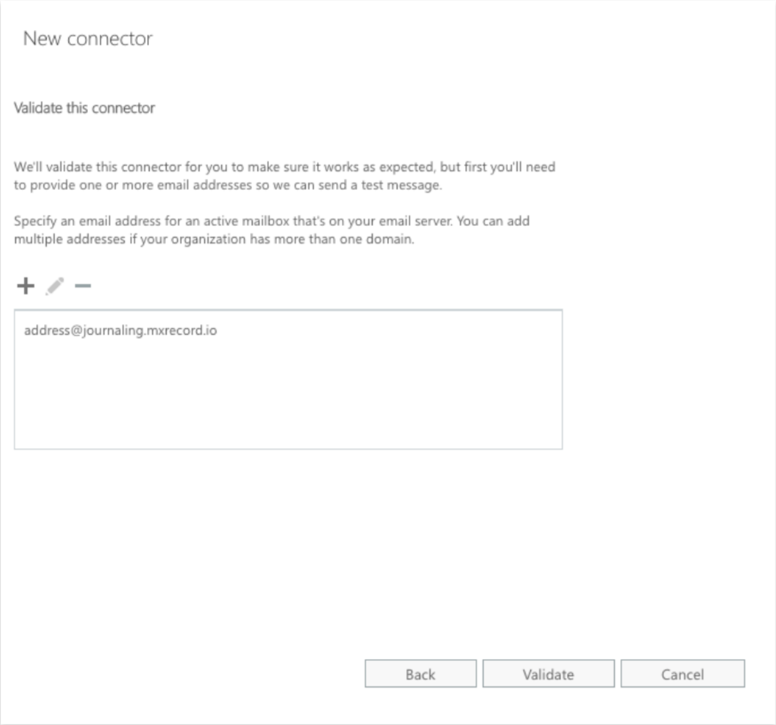
Routing method

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

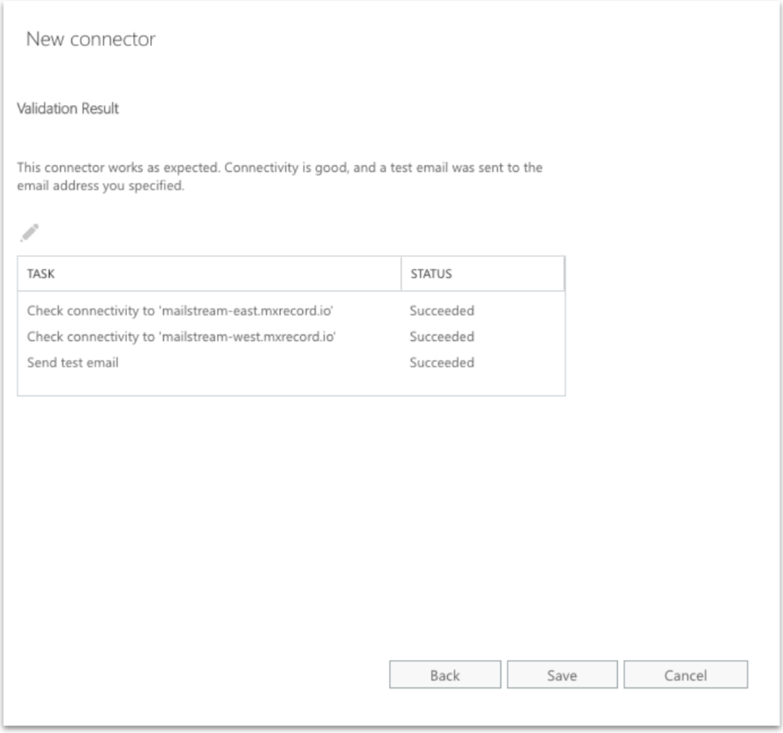
Validate this connector

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:



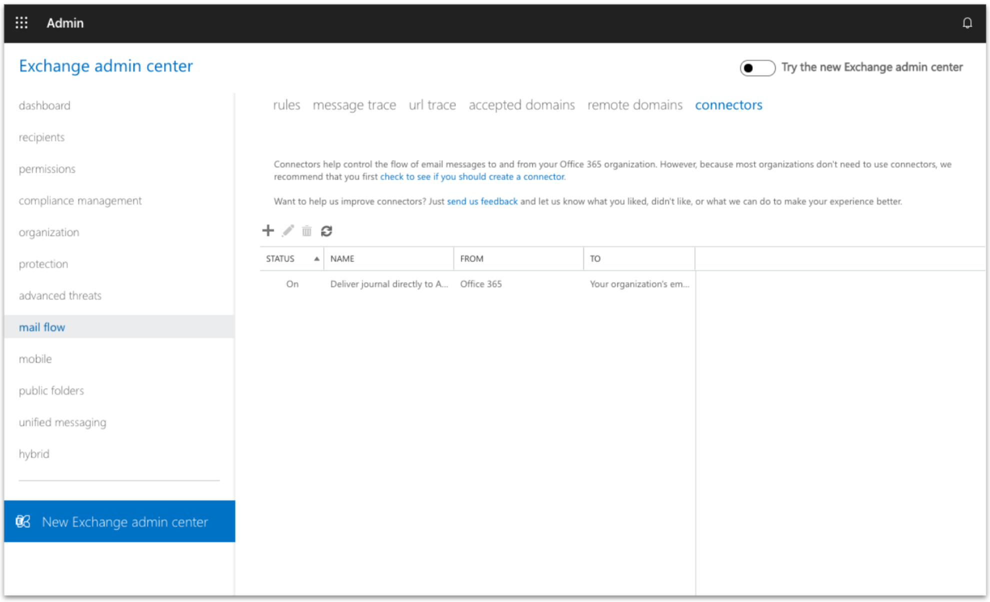
New connector

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:



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.

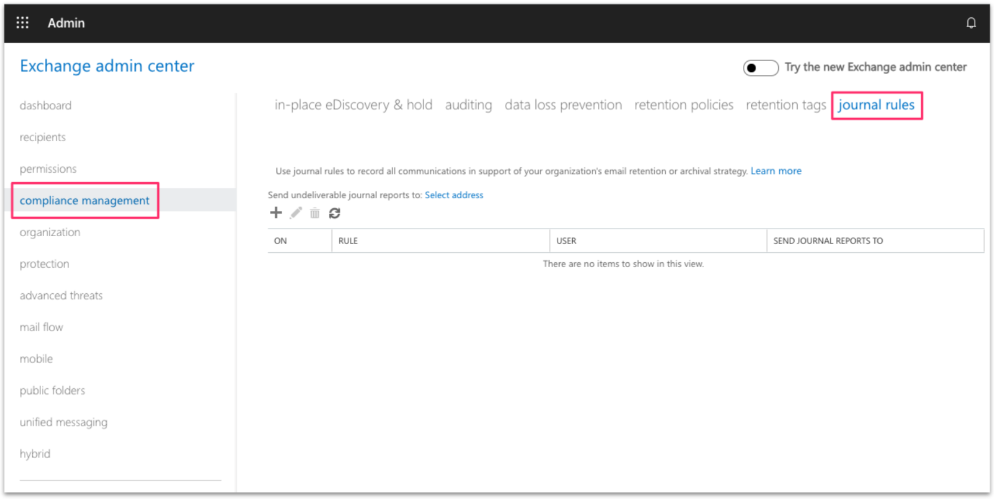
Want to help us improve connectors? Just send us feedback and let us know what you liked, didn't like, or what we can do to make your experience better.

STATUS ▲	NAME	FROM	TO
On	Deliver journal directly to A...	Office 365	Your organization's em...

Step 4: Configure Journal Rule

In order for the auto-retraction to complete, Area 1 must see the messages received by O365. This is configured through a Journal rule:

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



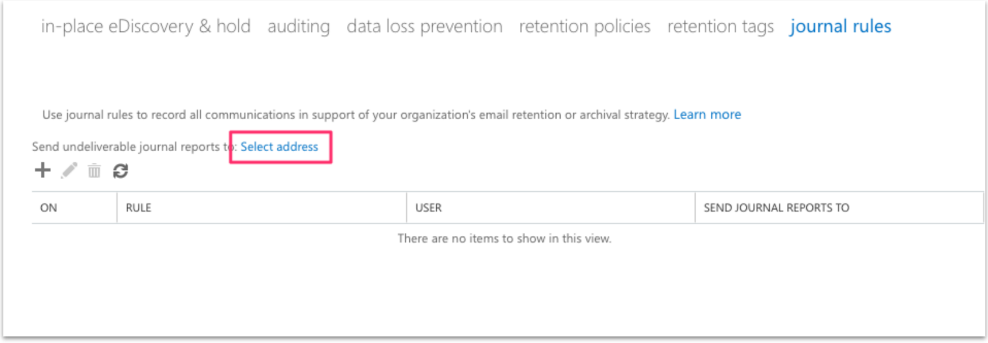
Use journal rules to record all communications in support of your organization's email retention or archival strategy. Learn more

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

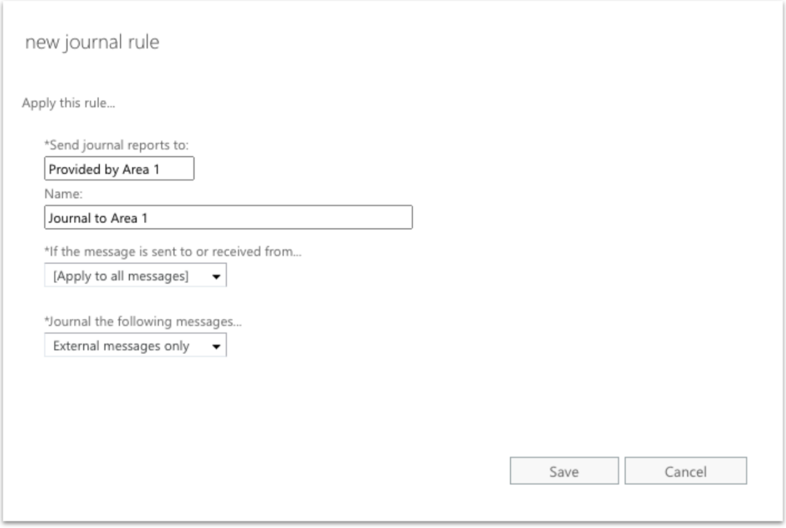
Send undeliverable journal reports to: Select address

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

Note: If you need to limit which users get their messages retracted, you can specify a group of users in the **If the message is sent to or received from...** dropdown. However, from a security perspective, it is recommended that messages for all users be inspected.

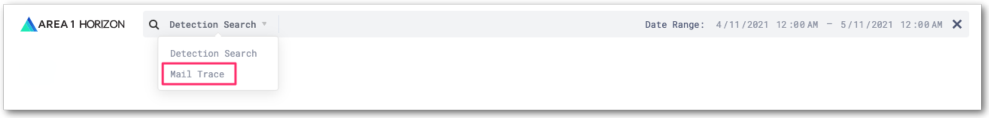
4. Click **Save** to save the journaling rule and acknowledge the warning indicating that the rule will only apply to future messages, once saved the rule is automatically active and may take a few minutes for the configuration to propagate and start to push messages to Area 1.

Now that Area 1 is receiving messages, messages that cause a detection will be automatically remediated based on the behavior configured in Step 2.

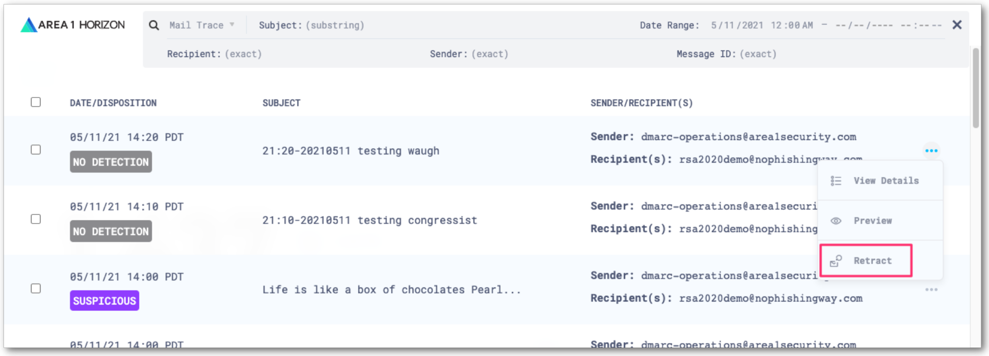
Manual Message Retraction

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:

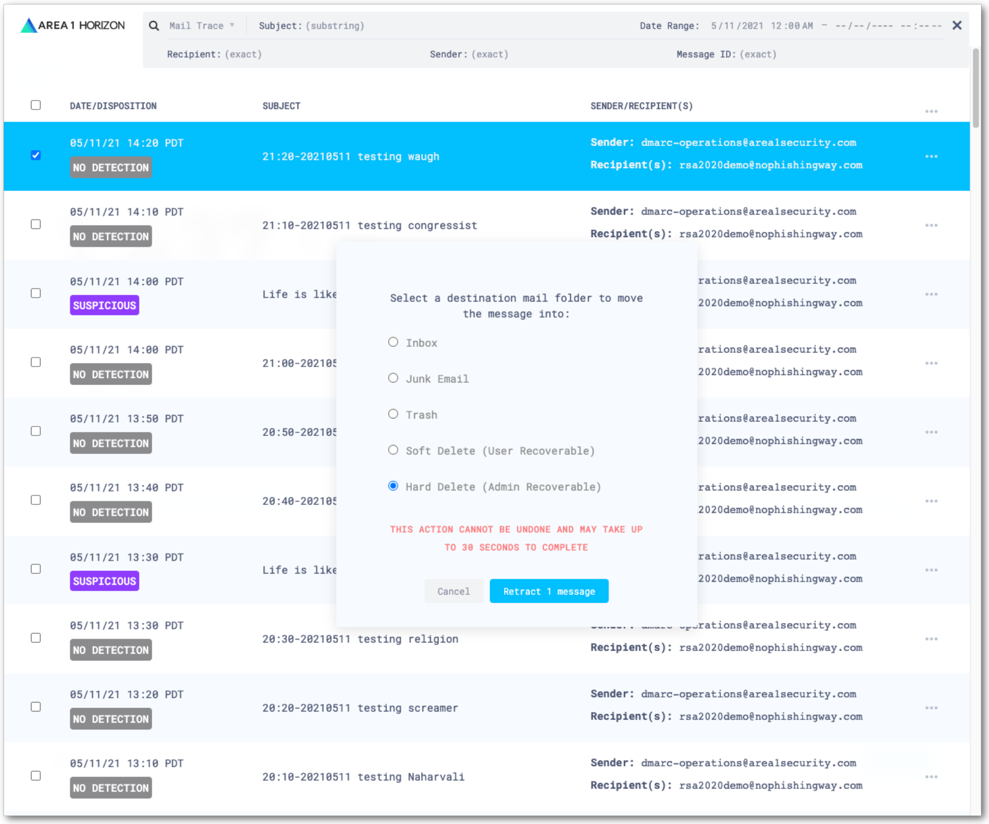


2. This will update the search dialog and allow you to search for the messages to retract, once you have entered the correct search parameters, you will be presented with the messages that match the search criteria. To retract a single message, click the **...** icon associated with the message and select 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:



☐	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@nophishing
☐	05/11/21 14:10 PDT NO DETECTION	21:10-20210511 testing congressist	**Sender:** dmarc-operations@arealsecuri **Recipient(s):** rsa2020demo@nophishing
☐	05/11/21 14:00 PDT SUSPICIOUS	Life is like a box of chocolates Pearl...	**Sender:** dmarc-operations@arealsecuri **Recipient(s):** rsa2020demo@nophishingway.com
	05/11/21 14:00 PDT		**Sender:** dmarc-operations@arealsecurity.com

3. Clicking the **Retract** action, will bring up a dialog giving you the option to decide where you want to retract the message:



Mail Trace ▾ Subject: (substring) Date Range: 5/11/2021 12:00 AM – --/--/---- --:---- ✕

Recipient: (exact) Sender: (exact) Message ID: (exact)

☐	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	rations@arealsecurity.com 2020demo@nophishingway.com	•••
☐	05/11/21 14:00 PDT NO DETECTION	21:00-202105	rations@arealsecurity.com 2020demo@nophishingway.com	•••
☐	05/11/21 13:50 PDT NO DETECTION	20:50-202105	rations@arealsecurity.com 2020demo@nophishingway.com	•••
☐	05/11/21 13:40 PDT NO DETECTION	20:40-202105	rations@arealsecurity.com 2020demo@nophishingway.com	•••
☐	05/11/21 13:30 PDT SUSPICIOUS	Life is like	rations@arealsecurity.com 2020demo@nophishingway.com	•••
☐	05/11/21 13:30 PDT NO DETECTION	20:30-20210511 testing religion	rations@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	•••

Select a destination mail folder to move the message into:

○ Inbox

○ Junk Email

○ Trash

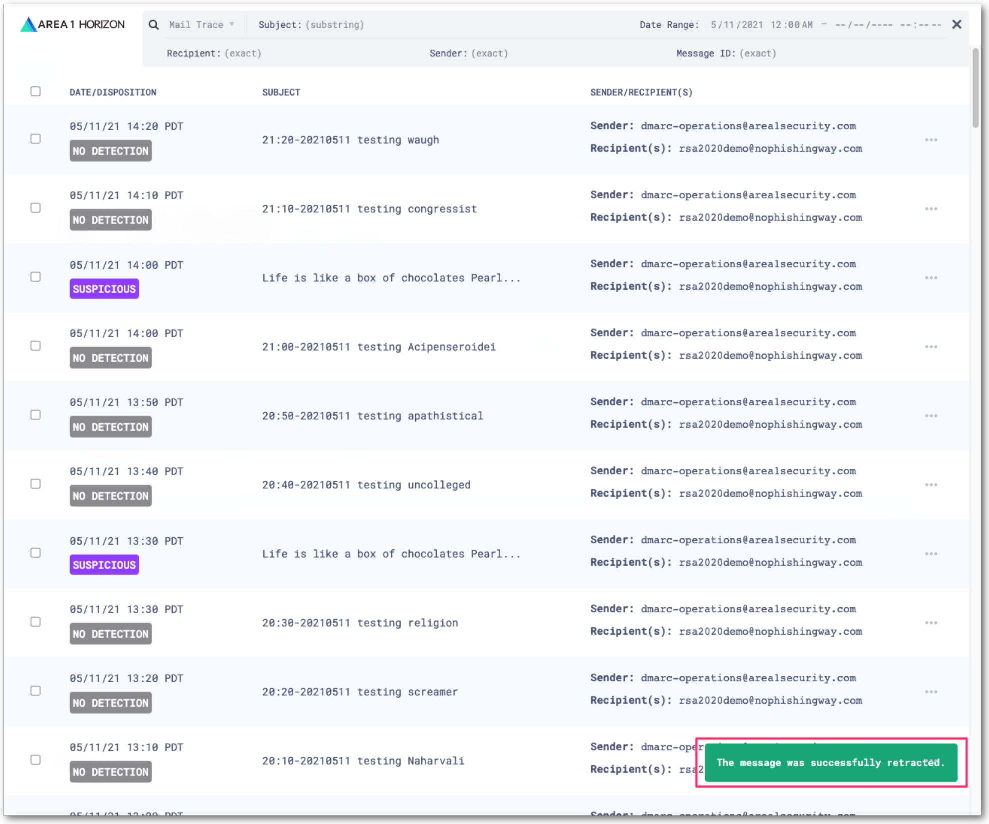
○ Soft Delete (User Recoverable)

● Hard Delete (Admin Recoverable)

THIS ACTION CANNOT BE UNDONE AND MAY TAKE UP TO 30 SECONDS TO COMPLETE

Cancel | Retract 1 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:



Mail Trace ▾ Subject: (substring) Date Range: 5/11/2021 12:00 AM – --/--/---- --:---- ✕

Recipient: (exact) Sender: (exact) Message ID: (exact)

□	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 Acipenseroidei	**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-oper **Recipient(s):** rsa2	
	05/11/21 13:00 PDT		**Sender:** dmarc-operations@arealsecurity.com	

The message was successfully retracted.