Cisco Secure Email Threat Defense User Guide

Table of Contents

Introduction

Cisco Secure Email Threat Defense is an integrated cloud-native security solution for Microsoft 365 that focuses on simple deployment, easy attack remediation, and superior visibility.

Requirements

The following are required to successfully set up and use Cisco Secure Email Threat Defense:

- You have purchased Secure Email Threat Defense and received a welcome email.
- The latest version of one of the following browsers:
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox
- If your Message Source is Microsoft 365 or your Visibility & Remediation mode uses Microsoft 365 Authentication:
  - A Microsoft 365 account with Global Admin rights.
  - An email address in your Microsoft 365 environment capable of receiving undeliverable journal reports. The email address used will not be journaled; do not use an address you want Secure Email Threat Defense to analyze.

Setup for Journal Message Sources

Secure Email Threat Defense setup for journal message sources includes the following:

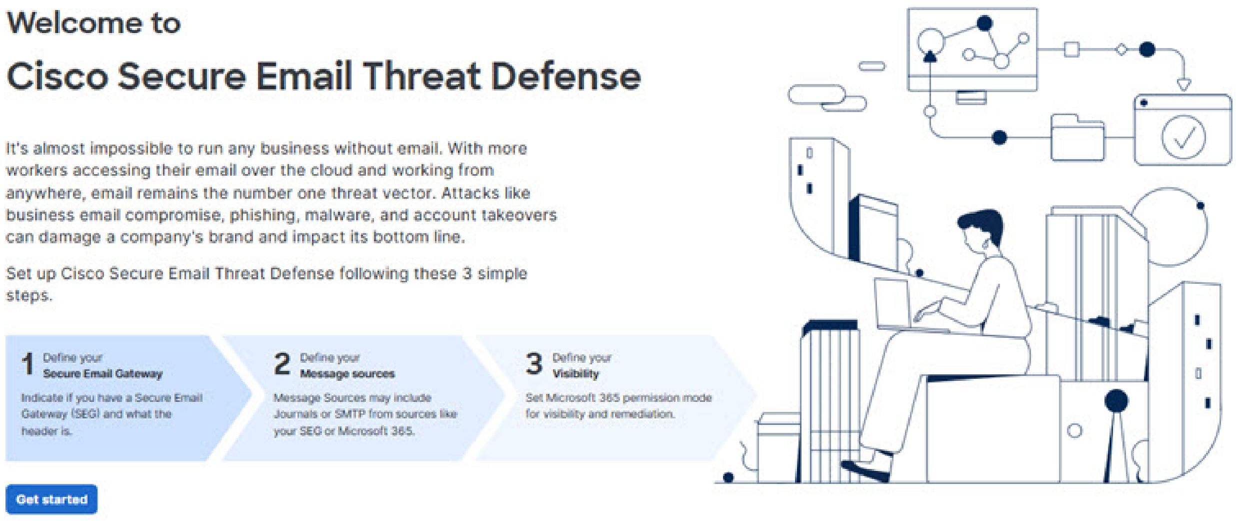
1. **Sign in to Your Account**
2. **Define Your Secure Email Gateway (SEG)**
3. **Define Your Message Sources**
4. **Define Your Visibility**
5. **Set up Your Message Source**
6. **Import Your Microsoft Email Domains and Review your Policy Configuration**

These steps assume you meet the **Requirements**.

Sign in to Your Account

1. Follow the directions in the welcome email from Cisco to set up your user account.

   Secure Email Threat Defense uses Cisco Security Cloud Sign On to manage user authentication. For information on Security Cloud Sign On, see https://cisco.com/go/securesignon. If you are an existing SecureX Threat Response, Cisco Secure Malware Analytics (formerly Threat Grid), or Cisco Secure Endpoint (formerly AMP) customer, sign in with your existing credentials. If you are not an existing user, you will need to create a new Security Cloud Sign On account.
2. Once you have successfully signed in, accept the Terms and Conditions.
3. You now have access to the **Welcome to Cisco Secure Email Threat Defense** page. Follow the setup wizard as described in the following sections.



Welcome to

Cisco Secure Email Threat Defense

It's almost impossible to run any business without email. With more workers accessing their email over the cloud and working from anywhere, email remains the number one threat vector. Attacks like business email compromise, phishing, malware, and account takeovers can damage a company's brand and impact its bottom line.

Set up Cisco Secure Email Threat Defense following these 3 simple steps.

1 Define your **Secure Email Gateway**
Indicate if you have a Secure Email Gateway (SEG) and what the header is.

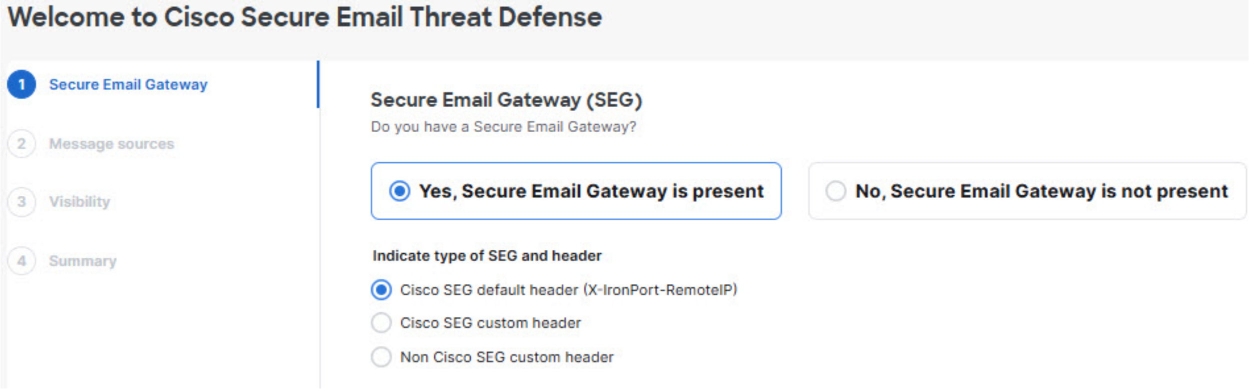
2 Define your **Message sources**
Message Sources may include Journals or SMTP from sources like your SEG or Microsoft 365.

3 Define your **Visibility**
Set Microsoft 365 permission mode for visibility and remediation.

Define Your Secure Email Gateway (SEG)

Regardless of your message source (chosen in the next section), it is important to indicate that a Secure Email Gateway (SEG) is present and which header can be used to identify it in incoming journals so Secure Email Threat Defense can determine the true originating sender of a message. Without this configuration, it may appear that all messages come from the SEG, which could result in false positive convictions..

1. Indicate if a Secure Email Gateway (SEG) is present by selecting **Yes, Secure Email Gateway is present** or **No, Secure Email Gateway is not present**.



Welcome to Cisco Secure Email Threat Defense

1 Secure Email Gateway
2 Message sources
3 Visibility
4 Summary

Secure Email Gateway (SEG)
Do you have a Secure Email Gateway?

● Yes, Secure Email Gateway is present ○ No, Secure Email Gateway is not present

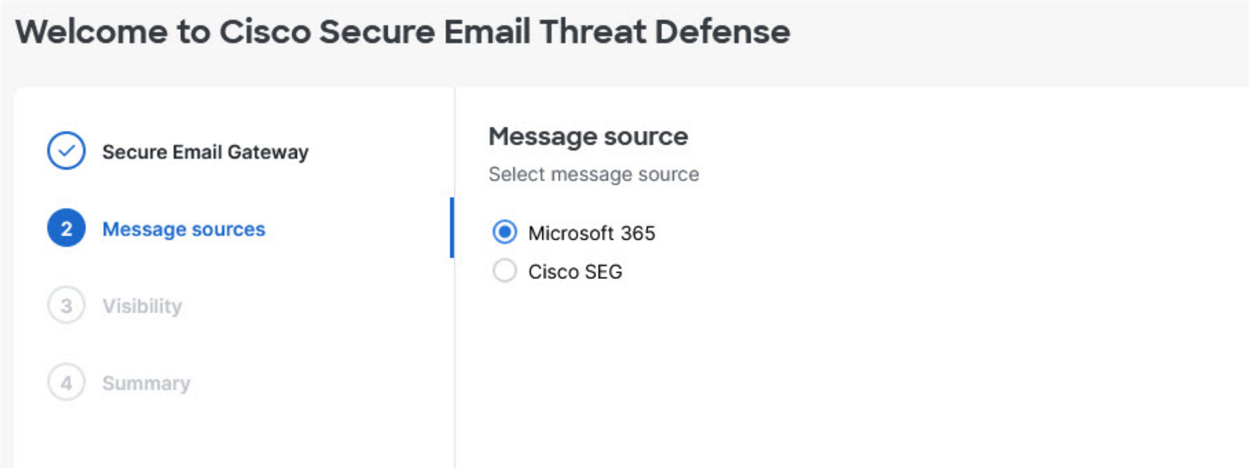
Indicate type of SEG and header
● Cisco SEG default header (X-IronPort-RemoteIP)
○ Cisco SEG custom header
○ Non Cisco SEG custom header

2. If you answered Yes, enter your SEG type and header.

3. Click **Next**.

Define Your Message Sources

1. Select your message source: Microsoft 365 or Cisco SEG. If you selected No SEG in the previous step, Microsoft 365 is assumed as your message source and the wizard skips this step.



Welcome to Cisco Secure Email Threat Defense

✓ Secure Email Gateway
2 Message sources
3 Visibility
4 Summary

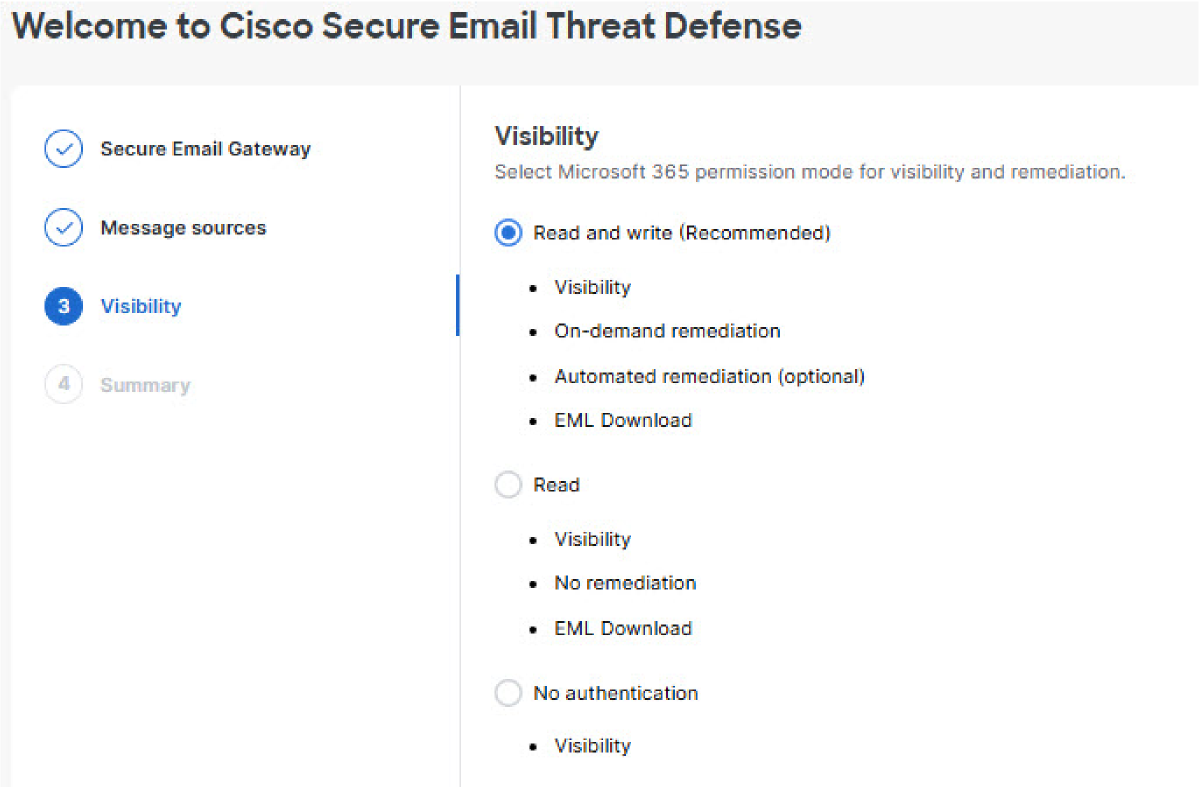
Message source
Select message source
● Microsoft 365
○ Cisco SEG

2. Click Next.

Define Your Visibility

1. Select your Microsoft 365 permission mode for visibility and remediation.

   The visibility defines the type of remediation policy you can apply. The options available will differ depending on your previous selections.



Welcome to Cisco Secure Email Threat Defense

✓ Secure Email Gateway

✓ Message sources

3 Visibility

4 Summary

Visibility

Select Microsoft 365 permission mode for visibility and remediation.

● Read and write (Recommended)

- Visibility
- On-demand remediation
- Automated remediation (optional)
- EML Download

○ Read

- Visibility
- No remediation
- EML Download

○ No authentication

- Visibility

Microsoft 365 Authentication

- **Read and Write** – Allows visibility and on-demand or automated remediation (that is, move or delete suspect messages). Read and write permissions will be requested from Microsoft 365.
- **Read** – Allows visibility only, no remediation. Read-only permissions will be requested from Microsoft 365.

> If you choose Read and Write, you will need to turn on the remediation policy in your Configuration Settings once your setup is complete. To apply auto-remediation to all internal emails, ensure the Apply Policy to domains not in the list above box on the **Configuration** > **Mail flow configuration** > **Domains** panel is selected.

For Microsoft 365 Authentication mode, Secure Email Threat Defense requests access permissions from Microsoft. These permissions depend on whether you choose Read and Write or Read mode. You can find details about the permissions in the linked Microsoft documentation.

Table 1. Microsoft Graph API Permissions

MS Graph API Permission	ETD Mode	ETD Usage
Mail.Read	Read	▪ EML download ▪ Reclassification feedback
Mail.ReadWrite	Read and Write	▪ All Mail.Read usages ▪ Remediation ◦ Create quarantine folders ◦ Move messages ◦ Delete messages
User.Read	All	Default requesting user permission
Domain.Read.All	All	Import mail servers
Organization.Read.All	All	Import domains
User.Read.All	All	▪ Recipient validation ▪ Group based policy exceptions
Group.Read.All	All	▪ Recipient validation ▪ Group based policy exceptions
GroupMember.Read.All	All	Group based policy exceptions

2. If you chose Microsoft 365 Authentication, connect to Microsoft 365.
   a. Click **Next** to connect to Microsoft 365.
   b. Log in to your Microsoft 365 account, as prompted. This account must have Global Admin rights; Secure Email Threat Defense will not store or use the account. To learn why these rights are required, see Why are Microsoft 365 Global Admin rights required to set up Secure Email Threat Defense?.
   c. Click **Accept** to accept the permissions for the Secure Email Threat Defense app. You will be redirected to the Secure Email Threat Defense setup page.
   d. Click **Next**.

Set up Your Message Source

A summary page provides instructions to set up your message source to send your email data to Secure Email Threat Defense. Complete the steps below for your message source.

1. Microsoft O365 Message Source
2. Gateway Message Source

Microsoft O365 Message Source

If you selected Microsoft O365 as your message source, you must configure Microsoft 365 to send journals to Secure Email Threat Defense. To do this, you add a journal rule. If you have a Gateway in place, add a connector in Microsoft 365 before adding your journal rule.

1. **For users with a Secure Email Gateway (SEG)**: Add a connector in Microsoft 365. To ensure journals are sent directly from Microsoft 365 to Secure Email Threat Defense without passing through the Secure Email Gateway, we recommend adding an outbound connector in Microsoft 365. You need to add the connector before setting up journaling. From the Microsoft 365 Exchange Admin Center, create a new connector by using the following settings in the **Add a connector** wizard:
   - **Connection from**: Office 365.
   - **Connection to**: Partner organization.
   - **Connector name**: Outbound to Cisco Secure Email Threat Defense (select the **Turn it on** check box).
   - **Use of connector**: Only when email messages are sent to these domains (add **mail.cmd.cisco.com** for North American environments, **mail.eu.cmd.cisco.com** for European environments, **mail.au.etd.cisco.com** for Australian environments, or **mail.in.etd.cisco.com** for Indian environments).
   - **Routing**: Use the MX record associated with the partner’s domain.
   - **Security restrictions**: Always use Transport Layer Security (TLS) to secure the connection (recommended); Issued by a trusted certificate authority (CA).
   - **Validation email**: Your journal address from the Secure Email Threat Defense setup page.

   > The connector validation may fail if your O365 tenant is already configured with conditional mail routing using an Exchange transport rule to route outbound mail to an existing connector. While journal messages are system-privileged and are not affected by transport rules, the connector validation test email is not privileged and is affected by transport rules.

   To overcome this validation issue, locate the preexisting transport rule and add an exception for your Secure Email Threat Defense journal address. Wait for this change to be effective, then retest the new connector validation.
2. Configure Microsoft 365 to send journals to Secure Email Threat Defense. To do this, add a journal rule.

a. Copy your journal address from the Secure Email Threat Defense setup page. If you need to repeat this process later, you can also find your journal address on the Administration page.

b. Go to your Microsoft Purview compliance portal: https://purview.microsoft.com/.

c. Navigate to **Solutions** > **Data lifecycle management** > **Exchange (legacy)** > **Journal rules**.

d. If you haven’t already done so, add an Exchange recipient to the **Send undeliverable journal reports to** field, then click **Save**. The email address used will not be journaled; do not use an address you want Secure Email Threat Defense to analyze. If you do not have a recipient you want to use for this purpose, you will need to create one.

e. Return to the **Journal rules** page. Click the **+** button to create a new journal rule.

f. Paste the journal address from the Secure Email Threat Defense setup page into the **Send journal reports to** field.

g. In the **Journal rule name** field, enter **Cisco Secure Email Threat Defense**.

h. Under **Journal messages sent or received from**, select **Everyone**.

i. Under **Type of message to journal**, select **All messages**.

j. Click **Next.**

k. Review your choices, then click **Submit** to finish creating your rule.

3. Return to the Secure Email Threat Defense setup page. Click **Review Policy**.

Gateway Message Source

If you selected Gateway as your message source, enable your Cisco Secure Email Cloud Gateway’s Threat Defense Connector to send messages to Secure Email Threat Defense.

1. Copy your Message Intake Address from the Secure Email Threat Defense setup page. If you need to repeat this process later, you can find your Message Intake address on the Administration page.
2. From the Secure Email Cloud Gateway UI, select **Security Services** > **Threat Defense Connector**.
3. Select the **Enable Threat Defense Connector** checkbox.
4. Enter the Message Intake Address you copied from Secure Email Threat Defense in step 1.
5. Click **Submit** to commit your changes.
6. Return to the Secure Email Threat Defense setup page. Click **Review Policy**.

Import Your Microsoft Email Domains and Review your Policy Configuration

When the setup wizard is complete, you will be on a Summary page for the wizard. Click **Review policy** to review your policy configuration. For information on policy settings, see Configuration Settings.

Secure Email Threat Defense imports domains with email capabilities from your Microsoft 365 tenant. Go to the **Configuration** > **Mail flow configuration** > **Domains** panel to import your domains so you can apply automated remediation to specific domains. Secure Email Threat Defense treats newly imported domains differently depending on whether you have the **Unlisted domains** setting on or off:

- If the **Unlisted domains** setting is **Apply policy to domains not listed above**, your policy is applied to any new domains that are imported.
- If the **Unlisted domains** setting is **Do not apply policy to domains not listed above**, your policy is not applied to any new domains that are imported.

By default, the Unlisted domains setting is set to Do not apply policy to domains not listed above. If you have chosen Microsoft 365 Read and Write as your message source and visibility, you should set this setting to Apply policy to domains not listed above as soon as you have imported your current domains.

See more:

1. Manual Import
2. Automatic Import

Manual Import

To manually import your Microsoft 365 email domains (recommended when you set up Secure Email Threat Defense for the first time):

1. Navigate to the **Policy** page.
2. Click the **Update Imported Domains** button to import your domains into Secure Email Threat Defense.
3. Use the check box next to each domain to adjust the automated remediation setting for that domain.
4. We recommend also selecting **Apply auto-remediation to domains not in the domain list** to ensure auto-remediation is applied to all internal emails and to any domains that are automatically imported later.
5. Click **Save and Apply**.

Automatic Import

Domains are automatically imported every **24** hours to ensure the list is up-to-date

Setup for SMTP Message Sources

> ⓘ SMTP message sources are available for new customers with a Secure Email Threat Defense advantage license.

Secure Email Threat Defense setup includes the following:

1. Sign in to Your Account
2. Define Your Secure Email Gateway (SEG)
3. Define Your Message Source
4. Define Your Visibility
5. Set up Your Message Source
6. Integrate with Microsoft 365
7. Review Your Policy Settings

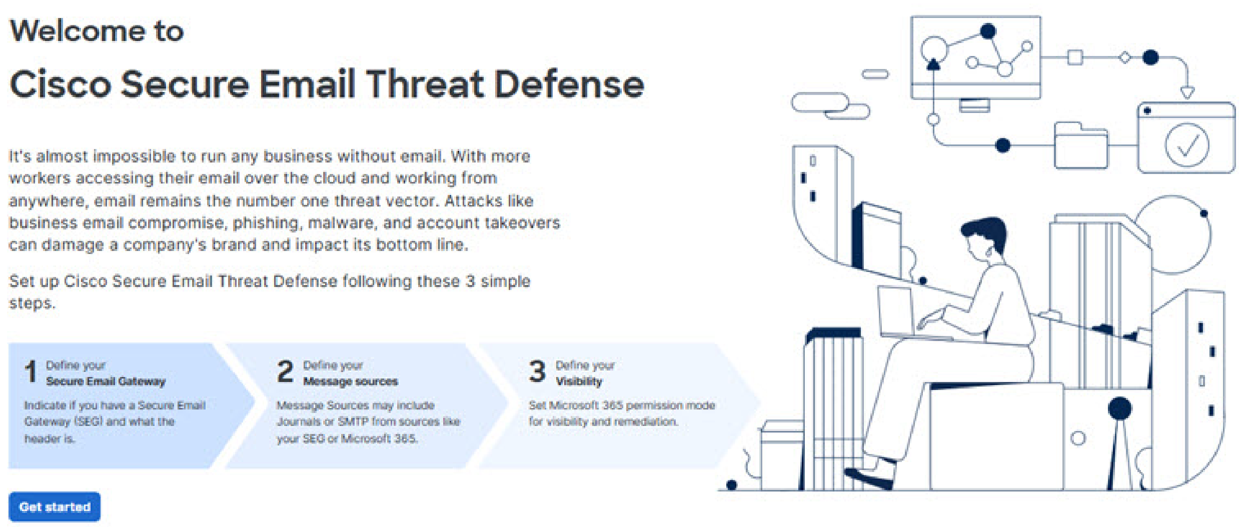
These steps assume you meet the Requirements.

Sign in to Your Account

1. Follow the directions in the welcome email from Cisco to set up your user account.

   Secure Email Threat Defense uses Cisco Security Cloud Sign On to manage user authentication. For information on Security Cloud Sign On, see https://cisco.com/go/securesignon. If you are an existing SecureX Threat Response, Cisco Secure Malware Analytics (formerly Threat Grid), or Cisco Secure Endpoint (formerly AMP) customer, sign in with your existing credentials. If you are not an existing user, you will need to create a new Security Cloud Sign On account.

2. Once you have successfully signed in, accept the Terms and Conditions.
3. You now have access to the **Welcome to Cisco Secure Email Threat Defense** page. Follow the setup wizard as described in the following sections.



Welcome to

Cisco Secure Email Threat Defense

It's almost impossible to run any business without email. With more workers accessing their email over the cloud and working from anywhere, email remains the number one threat vector. Attacks like business email compromise, phishing, malware, and account takeovers can damage a company's brand and impact its bottom line.

Set up Cisco Secure Email Threat Defense following these 3 simple steps.

1 Define your **Secure Email Gateway**
Indicate if you have a Secure Email Gateway (SEG) and what the header is.

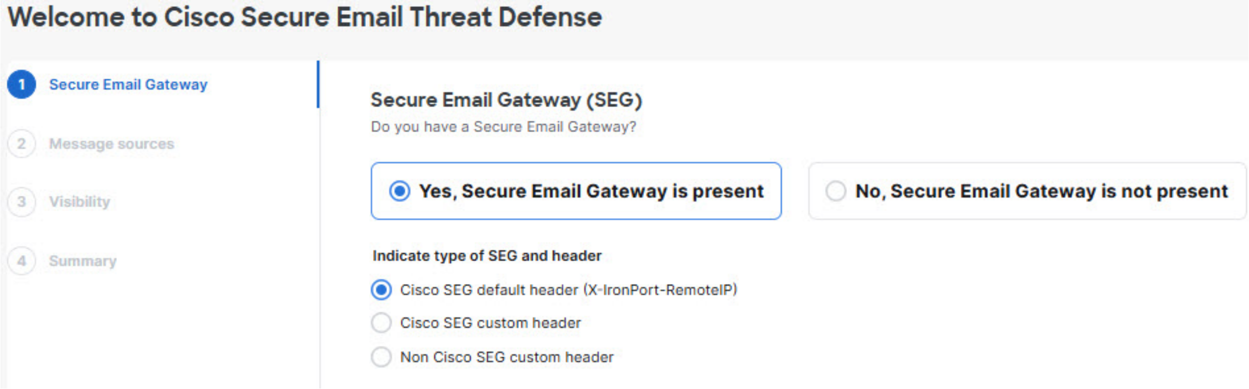
2 Define your **Message sources**
Message Sources may include Journals or SMTP from sources like your SEG or Microsoft 365.

3 Define your **Visibility**
Set Microsoft 365 permission mode for visibility and remediation.

Define Your Secure Email Gateway (SEG)

Regardless of your message source (chosen in the next section), it is important to indicate that a Secure Email Gateway (SEG) is present and which header can be used to identify it in incoming journals so Secure Email Threat Defense can determine the true originating sender of a message. Without this configuration, it may appear that all messages come from the SEG, which could result in false positive convictions..

1. Indicate if a Secure Email Gateway (SEG) is present by selecting **Yes, Secure Email Gateway is present** or **No, Secure Email Gateway is not present**.



Welcome to Cisco Secure Email Threat Defense

Secure Email Gateway (SEG)
Do you have a Secure Email Gateway?

● Yes, Secure Email Gateway is present
○ No, Secure Email Gateway is not present

Indicate type of SEG and header
● Cisco SEG default header (X-IronPort-RemoteIP)
○ Cisco SEG custom header
○ Non Cisco SEG custom header

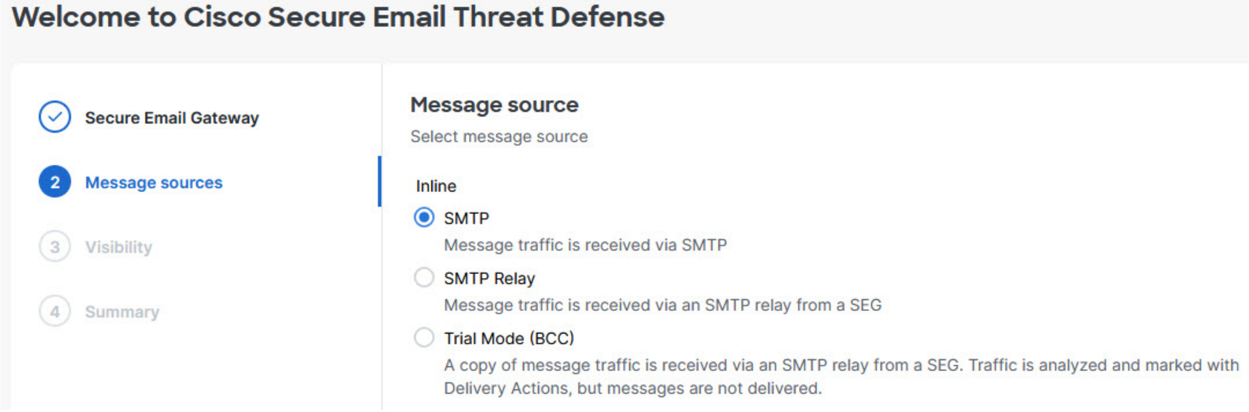
2. If you answered Yes, enter your SEG type and header.

3. Click **Next**.

Define Your Message Source

Select your SMTP/Inline Mode message source:

- **SMTP** - Message traffic is received via SMTP from your mail provider.
- **SMTP Relay** - Message traffic is received via an SMTP relay from a SEG. Add the IP addresses of your email gateway that you expect traffic from.
- **Trial Mode (BCC)** - A copy of message traffic is received via an SMTP relay from a SEG. Traffic is analyzed and marked with delivery actions, but messages are not delivered to user mailboxes. Define the IP addresses that you expect traffic from.



Welcome to Cisco Secure Email Threat Defense

Message source

Select message source

Inline

● SMTP

Message traffic is received via SMTP

○ SMTP Relay

Message traffic is received via an SMTP relay from a SEG

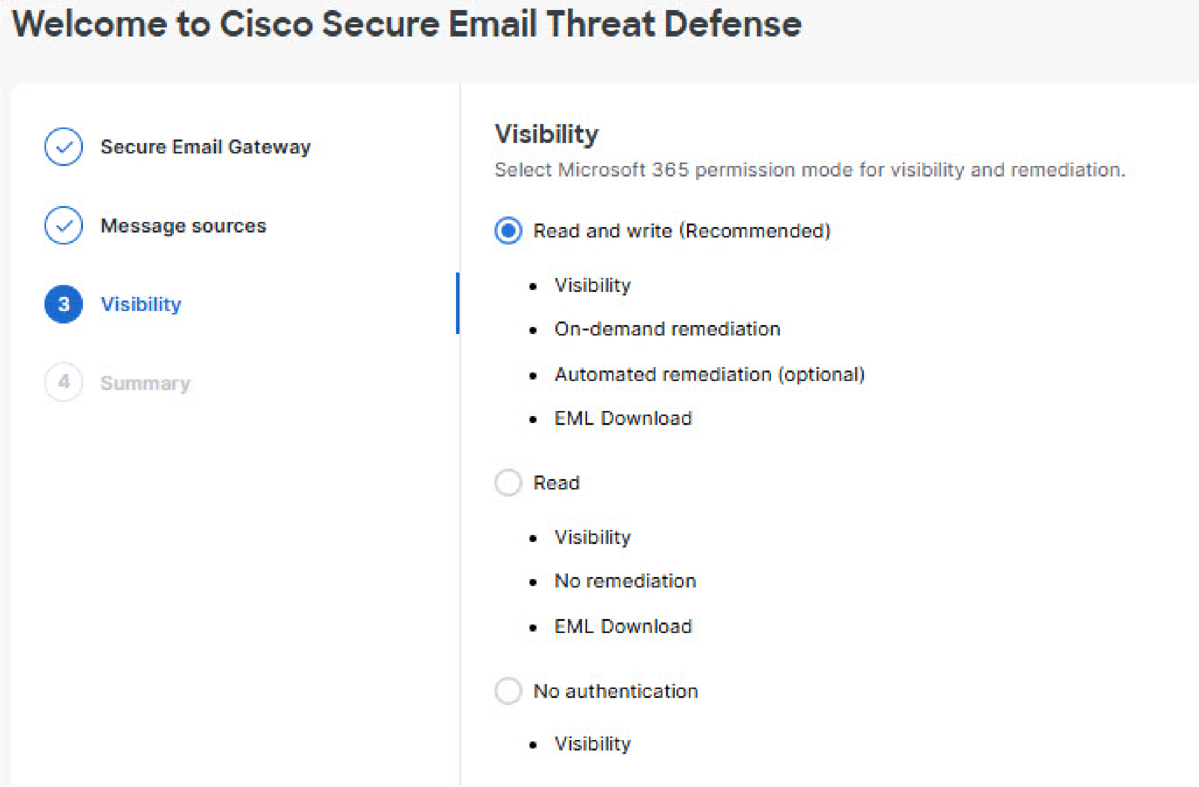
○ Trial Mode (BCC)

A copy of message traffic is received via an SMTP relay from a SEG. Traffic is analyzed and marked with Delivery Actions, but messages are not delivered.

Define Your Visibility

1. Select your Microsoft 365 permission mode for visibility and remediation.

   The visibility defines the type of remediation policy you can apply.



Welcome to Cisco Secure Email Threat Defense

Visibility

Select Microsoft 365 permission mode for visibility and remediation.

● Read and write (Recommended)

- Visibility
- On-demand remediation
- Automated remediation (optional)
- EML Download

○ Read

- Visibility
- No remediation
- EML Download

○ No authentication

- Visibility

Microsoft 365 Authentication

- **Read and Write** – Allows visibility and on-demand or automated remediation (that is, move or delete suspect messages). Read and write permissions will be requested from Microsoft 365.
- **Read** – Allows visibility only, no remediation. Read-only permissions will be requested from Microsoft 365.

> ⓘ If you choose Read and Write, you will need to turn on the remediation policy in your **Configuration Settings** once your setup is complete. To apply auto-remediation to all internal emails, ensure the Apply Policy to domains not in the list above box on the **Configuration** > **Mail flow configuration** > **Domains** panel is selected.

For Microsoft 365 Authentication mode, Secure Email Threat Defense requests access permissions from Microsoft. These permissions depend on whether you choose Read and Write or Read mode. You can find details about the permissions in the linked Microsoft documentation.

Table 1. Microsoft Graph API Permissions

MS Graph API Permission	ETD Mode	ETD Usage
Mail.Read	Read	▪ EML download ▪ Reclassification feedback
Mail.ReadWrite	Read and Write	▪ All Mail.Read usages ▪ Remediation ◦ Create quarantine folders ◦ Move messages ◦ Delete messages
User.Read	All	Default requesting user permission
Domain.Read.All	All	Import mail servers
Organization.Read.All	All	Import domains
User.Read.All	All	▪ Recipient validation ▪ Group based policy exceptions
Group.Read.All	All	▪ Recipient validation ▪ Group based policy exceptions

MS Graph API Permission	ETD Mode	ETD Usage
GroupMember.Read.All	All	Group based policy exceptions

2. If you chose Microsoft 365 Authentication, connect to Microsoft 365.
   a. Click **Next** to connect to Microsoft 365.
   b. Log in to your Microsoft 365 account, as prompted. This account must have Global Admin rights; Secure Email Threat Defense will not store or use the account. To learn why these rights are required, see **Why are Microsoft 365 Global Admin rights required to set up Secure Email Threat Defense?**.
   c. Click **Accept** to accept the permissions for the Secure Email Threat Defense app. You will be redirected to the Secure Email Threat Defense setup page.
   d. Click **Next**.

Set up Your Message Source

Complete the steps below to set up your message source to send email data to Secure Email Threat Defense.

- **SMTP**
- **SMTP Relay**
- **Trial Mode (BCC)**

SMTP

> Before you complete these steps, import and verify your domains on the Configuration page as described in **User Added Domains**

For an Inline/SMTP message source, you need to set up your mail host to send traffic to Secure Email Threat Defense. This involves changing your DNS MX record and DNS TXT record. The steps will vary depending on your provider

1. To allow Secure Email Threat Defense to receive incoming email on behalf of your domain, update your DNS MX record to point to your Secure Email Threat Defense environment. The destination depends on where your Secure Email Threat Defense instance is hosted.

Table 1. DNS MX Record Settings by Region

Environment	DNS Record
North America	mx.us.etd.cisco.com

Environment	DNS Record
Europe	mx.eu.etd.cisco.com
India	mx.in.etd.cisco.com
Australia	mx.au.etd.cisco.com
United Arab Emirates	mx.ae.etd.cisco.com
Beta	mx.beta.etd.cisco.com

2. Configure your domain to enable Secure Email Threat Defense to deliver incoming email to mailboxes. IP addresses for each region are mentioned below, however we recommend retrieving the updated list of IPs using the corresponding host name.

   Example: **dig host.<region>.etd.cisco.com** retrieves the corresponding IPs for the region.

Table 2. Regional Host Names and IPs

Region/Environment	Host Name	IPs
North America	host.us.etd.cisco.com	▪ 3.233.202.39 ▪ 52.4.38.100 ▪ 52.21.33.60 ▪ 3.218.110.126
Europe	host.eu.etd.cisco.com	▪ 18.158.246.66 ▪ 3.122.146.98 ▪ 3.121.252.9
India	host.in.etd.cisco.com	▪ 13.126.150.150 ▪ 15.207.156.30 ▪ 13.235.117.17
Australia	host.au.etd.cisco.com	▪ 3.24.0.238 ▪ 52.65.229.190 ▪ 52.62.51.239
United Arab Emirates	host.ae.etd.cisco.com	▪ 40.172.72.5 ▪ 40.172.180.89 ▪ 40.172.203.161

Region/Environment	Host Name	IPs
Beta	host.beta.etd.cisco.com	▪ 3.83.181.165 ▪ 3.212.52.157 ▪ 35.171.255.176 ▪ 34.237.73.142

3. Configure your DNS TXT record

Table 3. TXT Record Settings by Region

Region/Environment	TXT Record
North America	`v=spf1 include:spf.us.etd.cisco.com -all`
Europe	`v=spf1 include:spf.eu.etd.cisco.com -all`
India	`v=spf1 include:spf.in.etd.cisco.com -all`
Australia	`v=spf1 include:spf.au.etd.cisco.com -all`
United Arab Emirates	`v=spf1 include:spf.ae.etd.cisco.com -all`
Beta	`v=spf1 include:spf.beta.etd.cisco.com -all`

4. In Secure Email Threat Defense, go to **Configuration** > **Analysis configuration** > **Domains** > **Imported Domains** and click **Update Lis**t. Verify that the expected domains are imported and can accept traffic.

SMTP Relay

For this message source setting, traffic is received via an SMTP relay from a SEG. You will have defined the IP addresses you expect email from in the initial Secure Email Threat Defense setup.

The exact steps to direct mail from your SEG will depend on your system. To receive incoming email relayed from your SEG/MTA, complete the following:

1. Set up connection limits for all connections made to Secure Email Threat Defense:
   - Messages are accepted over TLS 1.2 only
   - Maximum messages per connection is 10
2. For Secure Email Threat Defense to be able to process Relay messages, the Sender IP needs to be present as a header in the email. Add the following headers:

X-CSE-ClientIP - IP of the sender who sent the mail to the SEG\MTA.

3. Redirect messages to one of the following hosts based on your Region/Environment.

Table 1. MX Record Settings by Region

Region/Environment	DNS Record
North America	mx.us.etd.cisco.com
Europe	mx.eu.etd.cisco.com
India	mx.in.etd.cisco.com
Australia	mx.au.etd.cisco.com
United Arab Emirates	mx.ae.etd.cisco.com
Beta	mx.beta.etd.cisco.com

4. Configure your domain to enable Secure Email Threat Defense to deliver incoming email to mailboxes. IP addresses for each region are mentioned below, however we recommend retrieving the updated list of IPs using the corresponding host name

   Example: **dig host.<region>.etd.cisco.com** retrieves the corresponding IPs for the region.

Table 2. Regional Host Names and IPs

Region/Environment	Host Name	IPs
North America	host.us.etd.cisco.com	▪ 3.233.202.39 ▪ 52.4.38.100 ▪ 52.21.33.60 ▪ 3.218.110.126
Europe	host.eu.etd.cisco.com	▪ 18.158.246.66 ▪ 3.122.146.98 ▪ 3.121.252.9
India	host.in.etd.cisco.com	▪ 13.126.150.150 ▪ 15.207.156.30 ▪ 13.235.117.17
Australia	host.au.etd.cisco.com	▪ 3.24.0.238 ▪ 52.65.229.190

Region/Environment	Host Name	IPs
		▪ 52.62.51.239
United Arab Emirates	host.ae.etd.cisco.com	▪ 40.172.72.5 ▪ 40.172.180.89 ▪ 40.172.203.161
Beta	host.beta.etd.cisco.com	▪ 3.83.181.165 ▪ 3.212.52.157 ▪ 35.171.255.176 ▪ 34.237.73.142

Trial Mode (BCC)

For this message source setting, a copy of message traffic is received via an SMTP relay from a SEG. Traffic is analyzed and marked with delivery actions, but messages are not delivered to user mailboxes. You will have defined the IP addresses you expect email from in the initial Secure Email Threat Defense setup.

To enable Secure Email Threat Defense to receive incoming email BCC-ed from your existing SEG/MTA, complete the following steps. The exact steps will vary depending on your setup.

1. Set up connection limits for all connections made to Secure Email Threat Defense:
    - Messages are accepted over TLS 1.2 only
    - Maximum messages per connection is 10
    - When your message source receives an error when sending BCC traffic to Secure Email Threat Defense, it should not bounce the email back to the sender.
2. For Secure Email Threat Defense to be able to process BCC messages, a set of headers need to be present in the emails. Add the following headers:
    - `X-CSE-ClientIP` - IP of the sender (Sending MTA) who sent the mail to the SEG/MTA
    - `X-CSE-MailFrom` - The "mail from" address
    - `X-CSE-RcptTo` - The "rcpt to" addresses
    - `X-CSE-MsgDirection` - "Incoming"
3. Configure the email address to BCC emails to Secure Email Threat Defense. The BCC email address takes the following format:

    <tenant_id>@inbound-bcc-domain

    where **tenant_id** is the Secure Email Threat Defense tenant id of the customer and **inbound-bcc-domain** is one of the following based on the region:

Table 1. Inbound BCC Domains

Region/Environment	DNS Record
North America	bcc-in.us.etd.cisco.com
Europe	bcc-in.eu.etd.cisco.com
India	bcc-in.in.etd.cisco.com
Australia	bcc-in.au.etd.cisco.com
United Arab Emirates	bcc-in.ae.etd.cisco.com
Beta	bcc-in.beta.etd.cisco.com

Integrate with Microsoft 365

If you are integrating with Microsoft 365, complete the following steps in the Microsoft 365 Exchange Admin Center.

1. Add a connector to accept inbound email from Secure Email Threat Defense. To do so, navigate to the Microsoft 365 Exchange Admin Center https://admin.exchange.microsoft.com/#/connectors, and add a connector for inbound traffic from Secure Email Threat Defense by using the following settings in the **Add a connector** wizard:
   a. **Connection from**: Partner organization.
   b. **Connection to**: Office 365.
   c. **Connector name**: Inbound from Cisco Secure Email Threat Defense (select the **Turn it on** check box).
   d. **Identify partner organization**: By verifying that the IP address of the sending server matches one of the following IP addresses, which belong to your partner organization. Add the IP addresses for your region here.
   e. **Security restrictions**: Reject email messages if they aren’t sent over TLS.
2. In Microsoft 365 Exchange Admin center https://admin.exchange.microsoft.com/#/transportrules, create a Transport Mail Rule to bypass spam filtering for inbound mail from Secure Email Threat Defense:
   a. **Name**: Bypass Spam Filter for SMTP Source.
   b. **Apply this rule if**: The sender IP addresses is in any of the following ranges. Add the IP addresses for your mail server here.

   c. **Do the following**: Modify the message properties: Set the spam confidence level (SCL) to -1.
   d. **Rule Mode**: Enforce
   e. **Severity**: Low
   f. **Stop processing more rules**: selected
   g. **Match sender address in message**: Header or Envelope

3. In Microsoft 365 Exchange Admin center, create a Mail Rule to Send Threats to MS Quarantine:
   a. **Name**: Quarantine Rule.
   b. **Apply this rule if**: The message headers matches these text patterns: X-CSE-Quarantine = true.
   c. **Do the following**: Redirect the message to: hosted quarantine.
   d. **Rule Mode**: Enforce
   e. **Severity**: Medium
   f. **Stop processing more rules**: selected
   g. **Match sender address in message**: Header
4. In Microsoft 365 Exchange Admin center, create a Mail Rule to send Spam and Graymail to the Junk folder:
   a. **Name**: Junk Rule.
   b. **Apply this rule if**: The message headers matches these text patterns: X-CSE-Junk = true.
   c. **Do the following**: Modify the message properties: Set the spam confidence level (SCL) to 9.
   d. **Rule Mode**: Enforce
   e. **Severity**: High
   f. **Stop processing more rules**: selected
   g. **Match sender address in message**: Header

Review Your Policy Settings

When your setup is complete, you will be on a Summary page for the wizard. Click **Review policy** to review your policy configuration. For information on policy settings, see Configuration Settings.

CIDR Ranges and NAT IP Addresses

For SMTP/Inline mode, after Secure Email Threat Defense has analyzed your traffic, message traffic will be sent from the CIDR ranges and IP addresses documented in this section. We recommend you add the specified IP ranges to your allow list to ensure seamless service operation and connectivity.

CIDR Ranges

The following CIDR ranges are used for NAT IPs:

- North America: 3.41.135.128/27
- North America(backup): 18.98.16.128/27
- Europe: 18.96.45.96/28
- Europe(backup): 3.40.131.112/28
- India: 18.96.227.160/28
- India(backup): 18.99.161.64/28
- Australia: 3.44.64.80/28
- Australia(backup): 18.99.192.224/28
- United Arab Emirates: 18.96.96.48/28
- United Arab Emirates(backup): 3.40.131.128/28

IPs Assigned Per Environment

Beta	North America	Europe	India	Australia	United Arab Emirates
3.41.135.139	3.41.135.128	18.96.45.100	18.96.227.160	3.44.64.80	18.96.96.48
3.41.135.141	3.41.135.129	18.96.45.101	18.96.227.161	3.44.64.81	18.96.96.49
3.41.135.144	3.41.135.130	18.96.45.102	18.96.227.162	3.44.64.82	18.96.96.50
3.41.135.145	3.41.135.131	18.96.45.103	18.96.227.163	3.44.64.83	18.96.96.51
3.41.135.146	3.41.135.132	18.96.45.104	18.96.227.164	3.44.64.84	18.96.96.52
3.41.135.147	3.41.135.133	18.96.45.105	18.96.227.165	3.44.64.85	18.96.96.53
3.41.135.149	3.41.135.134	18.96.45.106	18.96.227.166	3.44.64.86	18.96.96.54
3.41.135.150	3.41.135.135	18.96.45.107	18.96.227.167	3.44.64.87	18.96.96.55
	3.41.135.136	18.96.45.96	18.96.227.168	3.44.64.88	18.96.96.56
	3.41.135.137	18.96.45.97	18.96.227.169	3.44.64.89	18.96.96.57
	3.41.135.138	18.96.45.98	18.96.227.170	3.44.64.90	18.96.96.58
	3.41.135.140	18.96.45.99	18.96.227.171	3.44.64.91	18.96.96.59
	3.41.135.142				
	3.41.135.143				
	3.41.135.148				

Beta	North America	Europe	India	Australia	United Arab Emirates
	3.41.135.151				

Configuration Settings

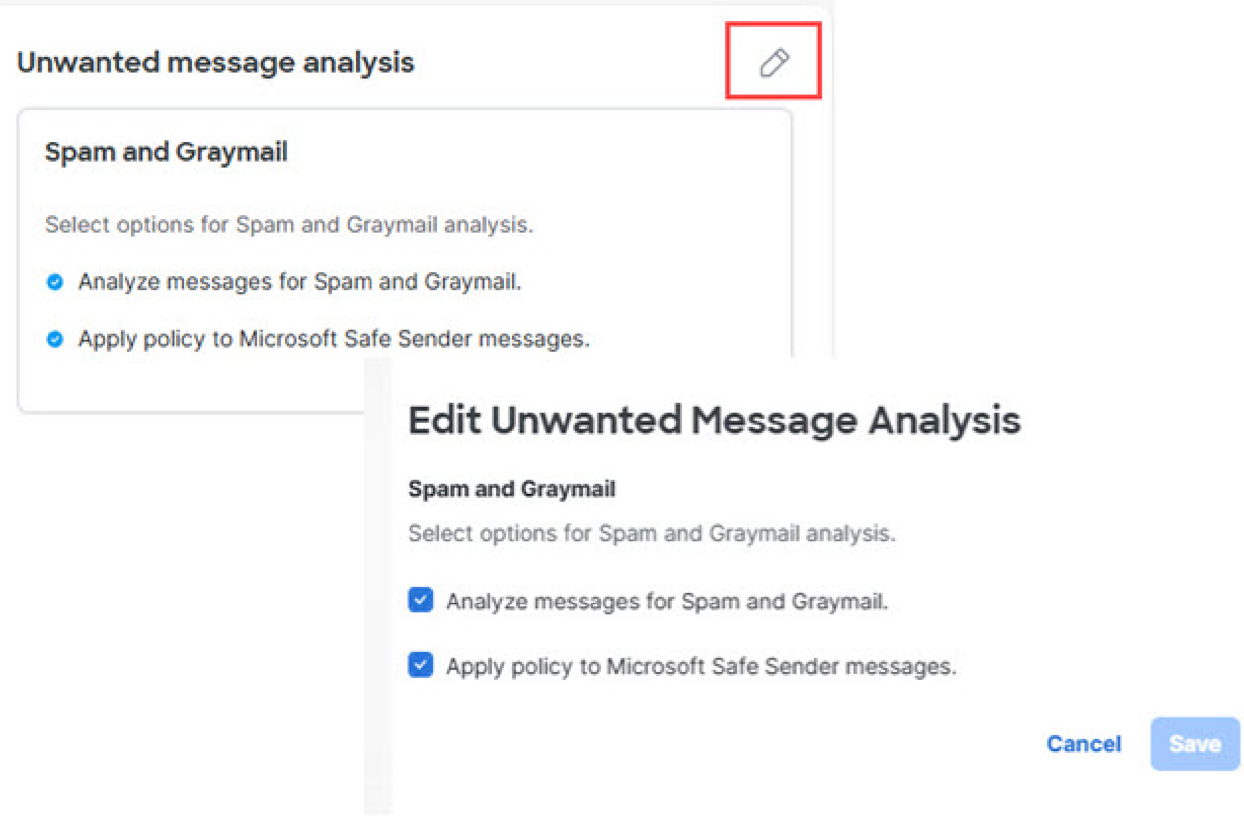
This chapter describes settings that were previously referred to as **Policy Settings**

The settings on the Configuration pages determine how Secure Email Threat Defense handles mail. Default settings are applied when you Secure Email Threat Defense. Be sure to review your settings to make sure Secure Email Threat Defense is handling your mail in the way you want it to.

Configuration settings are split the following areas:

- Mail flow configuration
- Connection handling
- Global settings
- Policy configuration

Edit items on these pages by clicking the pencil icon in the top right corner of a panel, or at the end of a row. After you click the pencil, you are taken to a dialog or workflow to make changes to those settings. For example:



Unwanted message analysis

Spam and Graymail

Select options for Spam and Graymail analysis.

- ✓ Analyze messages for Spam and Graymail.
- ✓ Apply policy to Microsoft Safe Sender messages.

Edit Unwanted Message Analysis

Spam and Graymail

Select options for Spam and Graymail analysis.

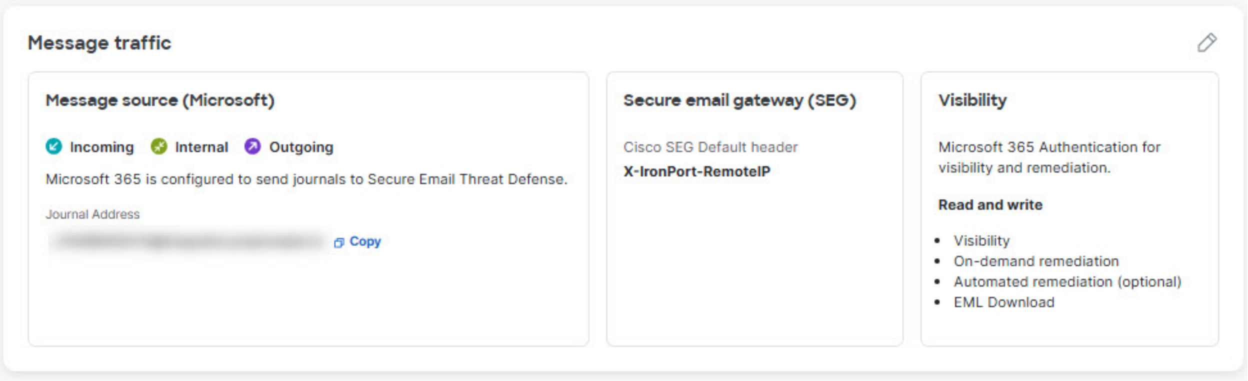
☑ Analyze messages for Spam and Graymail.

☑ Apply policy to Microsoft Safe Sender messages.

Mail Flow Configuration

The Mail flow configuration page shows your message sources and Microsoft 365 visibility, and information related to your domains.

The Message traffic panel houses settings for message sources and Microsoft 365 authentication and visibility. Your Microsoft journal address or Secure Email Gateway (SEG) Message intake address is also accessible from this panel. Click the pencil icon to change these settings. This takes you to a workflow to make changes.



Message traffic

Message source (Microsoft)

✓ Incoming ✓ Internal ✓ Outgoing

Microsoft 365 is configured to send journals to Secure Email Threat Defense.

Journal Address

[redacted] Copy

Secure email gateway (SEG)

Cisco SEG Default header

X-IronPort-RemoteIP

Visibility

Microsoft 365 Authentication for visibility and remediation.

Read and write

- Visibility
- On-demand remediation
- Automated remediation (optional)
- EML Download

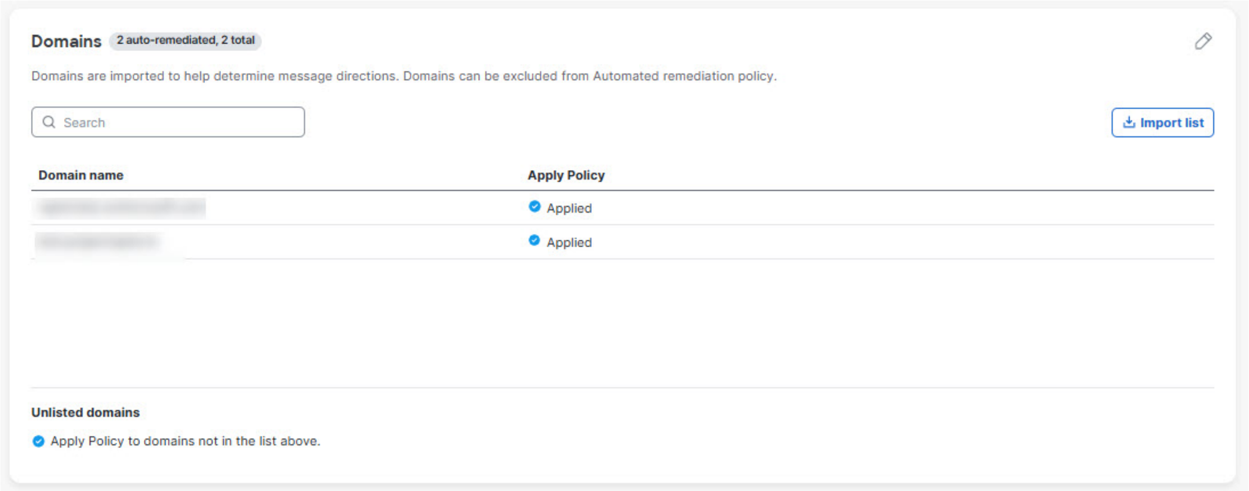
Table 1 Mail Flow Configuration Settings

Setting	Description	Options	Default
Message Source	Defines the source for your messages.	▪ **Microsoft 365** ▪ **Secure email gateway (SEG)** (for incoming messages only)	Manually selected when you set up Secure Email Threat Defense.
Visibility	Defines the type of remediation policy you can apply.	▪ **Microsoft 365 Authentication** ○ **Read and Write** - Allows visibility and on-demand or automated remediation (that is, move or delete suspect messages). Also allows EML downloads. Read and write permissions will be requested from Microsoft 365. ○ **Read** - Allows visibility only, no remediation or EML downloads. Read-only permissions will be requested from Microsoft 365.	Manually selected when you set up Secure Email Threat Defense. If you change your Microsoft 365 Authentication setting, you will be redirected to reset your Microsoft 365 permissions. You may also be directed to set up journaling; you can skip this step if you have already set up journaling. i When you choose

Setting	Description	Options	Default
		ⓘ If you select **Read**, you need only set the **Attachment Analysis** and **Message Analysis** directions. Remediation policy will not be applied. - **No Authentication** - Allows Visibility only.	ⓘ **Microsoft 365 Authentication: Read and Write**, you should also verify your **Configuration Settings with a Gateway** settings.
Secure Email Gateway (SEG)	The presence of a Secure Email Gateway (SEG) impacts how Secure Email Threat Defense identifies the Sender IP.	- **No, Secure Email Gateway is not present** - **Yes, Secure Email Gateway is present** ○ **Cisco SEG default header** (`X-IronPort-RemoteIP`) ○ **Cisco SEG custom header** (indicate header) ○ **Non Cisco SEG custom header** (indicate header)	Manually selected when you set up Secure Email Threat Defense. For more information, see Configuration Settings with a Gateway.
Domains – Domains are imported to help determine message directions. Domains are automatically imported from Microsoft 365 every 24 hours. Domains can be excluded from automated remediation policies.			
Auto-Remediation	Applied to the domains not in the domains list.	**Checked** or **Unchecked**	**Unchecked**. When you turn on **Read and Write** visibility, select this check box.

Imported Domains

The Domains panel lists your email domains. Imported domains help determine message direction. Specific domains can be excluded from automated remediation policies. The domains list is automatically updated every 24 hours or you can click **Import list** to refresh your Microsoft domains immediately.



Domains 2 auto-remediated, 2 total

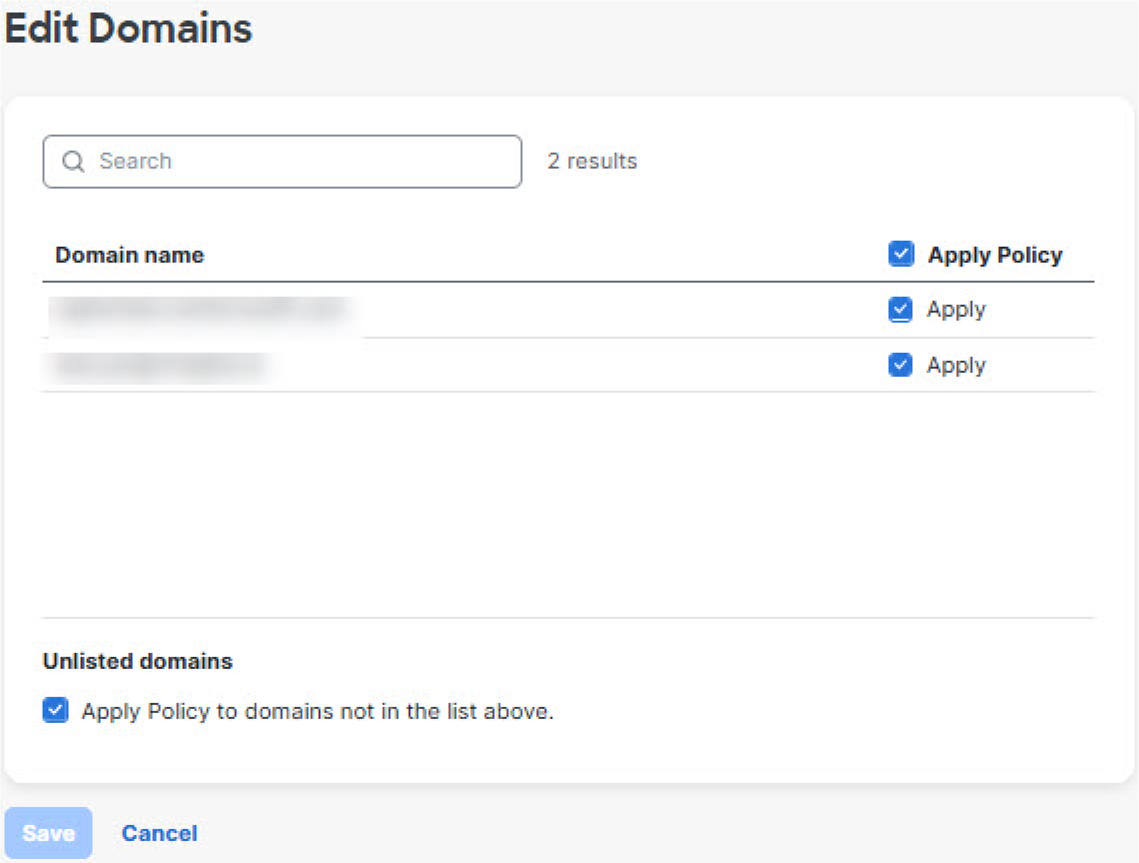
Domains are imported to help determine message directions. Domains can be excluded from Automated remediation policy.

Domain name	Apply Policy
[redacted]	● Applied
[redacted]	● Applied

Unlisted domains

● Apply Policy to domains not in the list above.

Click the pencil icon in the top right corner of the Domains panel to adjust which domains you want to apply your policies to and if you want to apply policies to domains not in the list. Domains might not be in your list if they haven't been imported yet.



Edit Domains

2 results

Domain name	☑ Apply Policy
[redacted]	☑ Apply
[redacted]	☑ Apply

Unlisted domains

☑ Apply Policy to domains not in the list above.

Configuring Secure Email Threat Defense as a First Hop

For information on configuring Secure Email Threat Defense as a first point of delivery, see **Configuring a Relay Host Server**.

Configuring a Relay Host Server

In SMTP/Inline mode, you can configure Secure Email Threat Defense as a first point of delivery (also know as first hop) in your mail flow. By adding a relay host server, Secure Email Threat Defense analyzes your mail, then delivers your messages to your relay host for further analysis, rather than to the end user's mailboxes.

1. Navigate to **Configuration** > **Mail flow configuration** > **Domains** > **Imported domains**.
2. Click the pencil icon to open the **Edit Domains** page.
3. In the **Primary Relay Host Name or IP** field, enter a relay host name or IP to forward messages to instead of using the imported mail server.
4. Click **Save**. This returns you to the Domains panel. You can see your newly added server under Mail server host name, and the Mail Server Type is marked as Manually Configured.

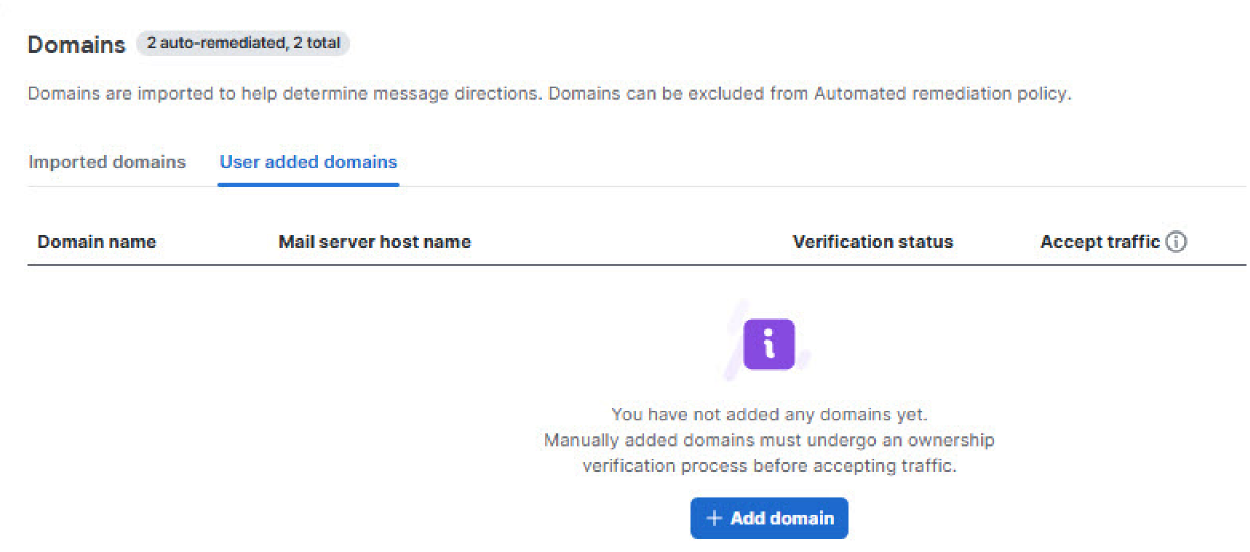
User Added Domains

Use the **User added domains** tab to specify custom domain names and mail servers. This can be used to add non-Microsoft domains or to add Microsoft domains without giving Secure Email Threat Defense Read or Write access to your Microsoft business. If you are using a non-Microsoft SMTP message source, add your domains here.

To add a domain, you must specify the domain name and primary mail host and then complete an owner verification process before you can direct traffic to Secure Email Threat Defense. Secure Email Threat Defense can analyze and apply delivery instructions to your messages but cannot remediate messages once they have been delivered.

To add and verify a domain:

1. Navigate to **Configuration** > **Mail flow configuration** > **Domains** > **User added domains** tab.



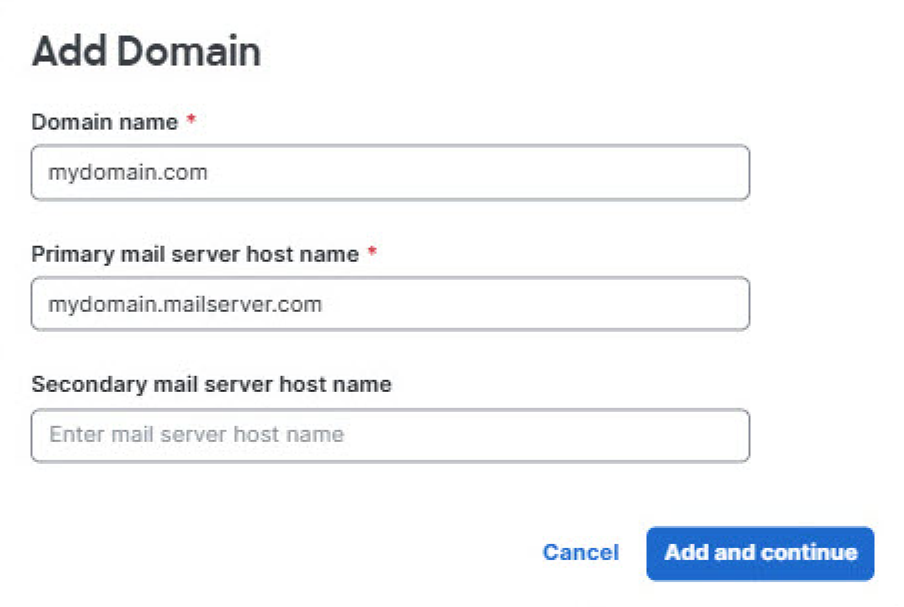
Domains 2 auto-remediated, 2 total

Domains are imported to help determine message directions. Domains can be excluded from Automated remediation policy.

Domain name	Mail server host name	Verification status	Accept traffic ⓘ

You have not added any domains yet.
Manually added domains must undergo an ownership verification process before accepting traffic.

2. Click the **Add domain** button.
3. Enter the Domain name and Primary mail server host name (and Secondary mail server host name, if applicable).



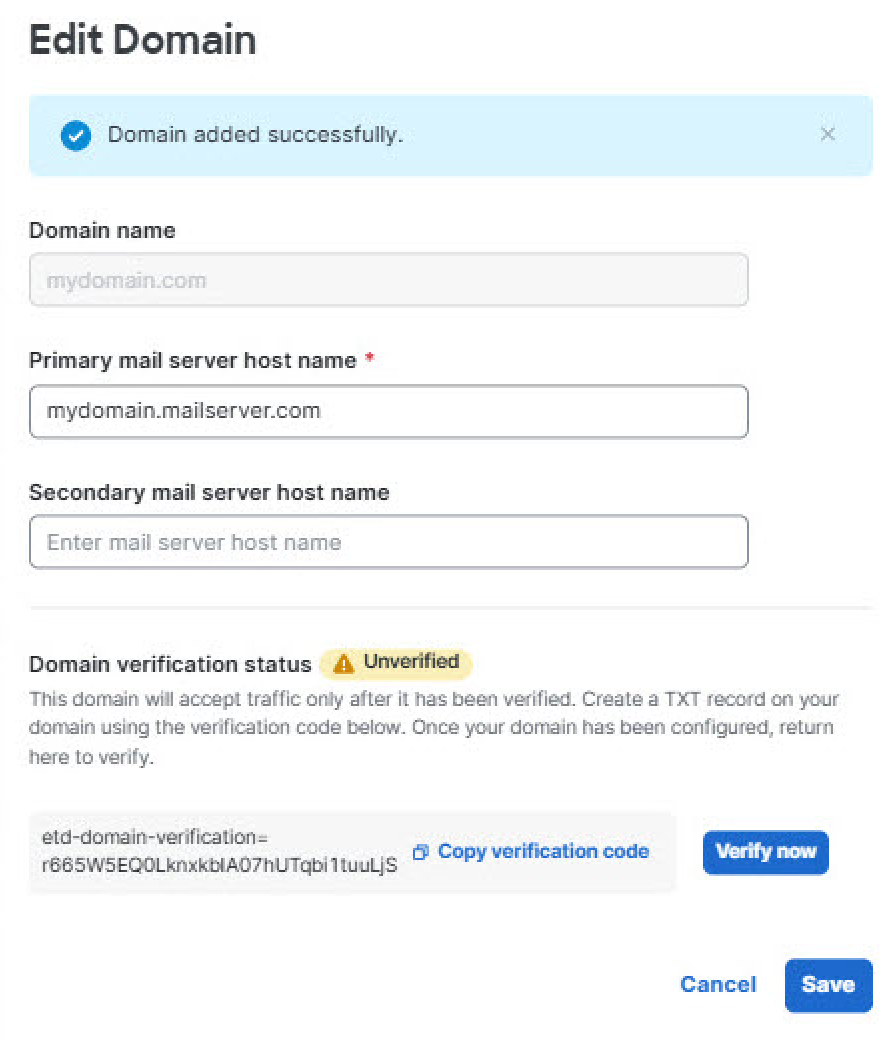
Add Domain

Domain name *: mydomain.com

Primary mail server host name *: mydomain.mailserver.com

Secondary mail server host name: Enter mail server host name

4. Click the **Add and continue** button. The domain is added. You must now verify your ownership.
5. To verify your domain, copy the verification code and create a TXT record on your domain using the code. The steps for doing this will depend on your domain host.



Edit Domain

Domain added successfully.

Domain name

mydomain.com

Primary mail server host name *

mydomain.mailserver.com

Secondary mail server host name

Enter mail server host name

Domain verification status ⚠ Unverified

This domain will accept traffic only after it has been verified. Create a TXT record on your domain using the verification code below. Once your domain has been configured, return here to verify.

etd-domain-verification=
r665W5EQ0LknxkblA07hUTqbi1tuuLjS

6. Once the TXT record is added to your domain, return to Secure Email Threat Defense and click the **Verify now** button. This performs a DNS lookup to verify the record, and the status is changed to Verified when it is successful.
7. Select the accept traffic check box if you are ready to accept traffic from the newly added domain.
8. Click **Save**.
9. After your domain is added and verified, configure your DNS MX record and DNS TXT records to send traffic to Secure Email Threat Defense. The destination depends on where your Secure Email Threat Defense instance is hosted.

Table 1. DNS Record Settings

Environment	DNS Record	Type
North America	mx.us.etd.cisco.com	A
Europe	mx.eu.etd.cisco.com	A
India	mx.in.etd.cisco.com	A
Australia	mx.au.etd.cisco.com	A
United Arab Emirates	mx.ae.etd.cisco.com	A
Beta	mx.beta.etd.cisco.com	A

Switching Your Message Source

To change your message source, navigate to the **Configuration** > **Mail flow configuration** page.

1. Click the pencil icon to be taken to a wizard that will walk you through the steps to change your message source.
2. A notice indicating you are switching your message source appears. Click **Continue**.
3. The Switch Message Source dialog appears. You need to configure your previous message source to stop sending messages to Secure Email Threat Defense. For details on how to do this, see Delete Your Secure Email Threat Defense Journal Rule or Configure your Gateway to Stop Sending Messages.
4. Select the checkbox indicating you have stopped sending journals or messages from your previous source, then click **Next**.
5. Configure your new message source using the Message Intake Address or Journal Address shown in the dialog. The steps for setting up each type of message source are detailed in .

Connection Handling

> ⓘ Connection handling is applicable to SMTP/Inline message sources.

Use the **Configuration** > **Connection handling** tab to create rules to allow or block hostnames/FQDNs and IP addresses at the connection level.

See also:

- Add a New Allow or Block Rule
- Edit an Existing Allow or Block Rule

Add a New Allow or Block Rule

1. Select **Configuration** > **Connection handling**.
2. Select the category of rule you want to create: Allow list or Block list.
3. Click the **New allow rule** or **New block rule** button.
4. Create a Rule name and a Short description for the rule, then click **Create rule**. Your rule is created.
5. Now, add Connections to your rule. Click **Add connections**.
6. Enter the items you want to allow or block, separated by commas. This can include hostnames/FQDNs and IP addresses.
7. Click **Save** to finish creating the rule.

Your items are added as separate connections in your list. This gives you granular control over each entry if you need to edit them in the future.

Edit an Existing Allow or Block Rule

1. Select **Configuration** > **Connection handling**.
2. Select the category of rule you want to edit: Allow list or Block list.
3. Click the pencil icon in the row you want to edit.
4. To edit the Rule Name or short description, click the **Edit** button, make your changes, then click **Save**.
5. To edit a connection, click the pencil icon in the row you want to edit. In the Edit Allowed/Blocked Connections dialog, make your changes, then click **Save**.
6. To add an additional connection to your rule, click Add connections. In the Add Allowed/Blocked Connections dialog, enter the hostnames/FQDNs and IP addresses you want to add, then click **Save**.

Delete an Allow or Block Rule

To delete a rule:

1. Select **Configuration** > **Connection handling**.
2. Select the type of rule you want to delete: Allow list or Block list.
3. Click the delete icon next to the rule you want to delete.

Your rule is deleted.

Blocked Connection Logs

There are several ways to see logs for connections you have blocked:

- Navigate to **Insights** > **Blocked Connection Logs** to see a graphical representation of items that have been blocked.
- Export the Blocked Connection Logs to CSV by clicking the **Export** button on the Blocked Connection Logs page.
- View the Blocked Connection entries in the Audit Log CSV export, accessible from **Administration** > **Business** > **Audit Logs**.

Global Settings

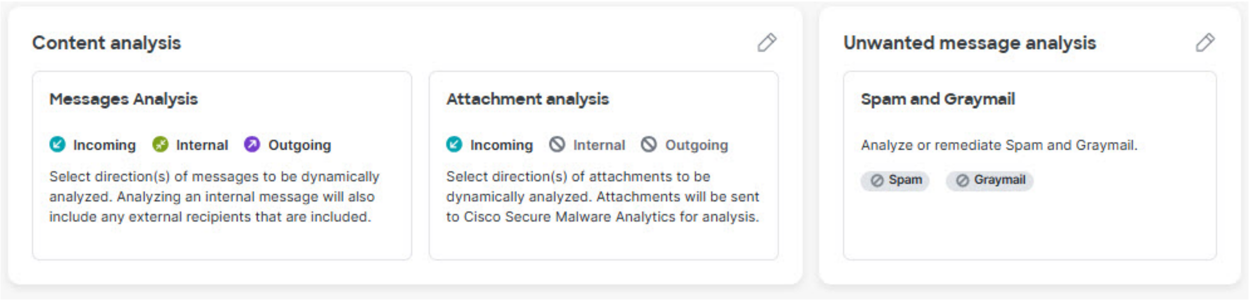
The Global settings page is where you define which content you want to analyze.

See also:

- Content Analysis
- Message Bypass Rules
- Add a New Message Bypass Rule
- Edit a Message Bypass Rule
- Enable or Disable a Message Bypass Rule
- Delete a Message Bypass Rule
- URL Rules
- Data Loss Prevention (DLP)

Content Analysis

The Content analysis panel shows which directions of messages and attachments you want Secure Email Threat Defense to analyze. The Unwanted message analysis panel shows your settings for analysis and remediation of Spam and Graymail messages. Click the pencil in the top right corner of each panel to edit your settings.



Content analysis

Messages Analysis

✓ Incoming ✓ Internal ✓ Outgoing

Select direction(s) of messages to be dynamically analyzed. Analyzing an internal message will also include any external recipients that are included.

Attachment analysis

✓ Incoming ⊘ Internal ⊘ Outgoing

Select direction(s) of attachments to be dynamically analyzed. Attachments will be sent to Cisco Secure Malware Analytics for analysis.

Unwanted message analysis

Spam and Graymail

Analyze or remediate Spam and Graymail.

⊘ Spam ⊘ Graymail

Table 2 Global settings

Setting	Description	Options	Default
Content Analysis	■ **Messages Analysis**. Direction of messages to be dynamically analyzed. ■ **Attachment Analysis**. Direction of mail attachments to be dynamically analyzed.	■ **Direction of Messages** ◦ **Incoming** ◦ **Internal** ◦ **Outgoing** ■ **Direction of Attachments** ◦ **Incoming** ◦ **Internal Outgoing**	■ **Direction of Messages** ◦ **All** for Microsoft O365 Message Source ◦ **Incoming** for Gateway message source ■ **Direction of Attachments** ◦ **Incoming**
Unwanted Message Analysis	Analyze messages for Spam and Graymail	**Checked** or **Unchecked**	**Checked** for all accounts created after November 4, 2025.
Safe Sender: Apply policy to Microsoft Safe Sender messages	Messages tagged by Microsoft in the journal header as Safe Sender and with Secure Email Threat Defense verdicts of Spam or Graymail will not be remediated if this box is checked.	**Checked** or **Unchecked**	**Unchecked**

Message Bypass Rules

For legacy customers, these rules were previously accessible from **Administration** > **Message Rules** > **Bypass Analysis**. Existing bypass rules have been relocated to **Configuration** > **Global settings > Message bypass rules**.

Message bypass rules allow you to bypass analysis for Phish test senders or Security mailbox recipients that match the rule criteria. Messages that meet the rule criteria will bypass all engine analysis so you can process your security tests without engines interfering. Attachments and links are not opened or scanned by Secure Email Threat Defense.

If a Message bypass rule is created for testing, the rule should be reconsidered after an appropriate period of time to prevent vulnerabilities.

Phish Test rules:

- Apply to all incoming messages from the specified sender email addresses, sender domains, or IP addresses (IPv4), or CIDR addresses); messages will not be analyzed.

  > We recommend only using sender IP addresses/CIDR criteria to bypass specific sender infrastructure; IP addresses are not as easily spoofed as sender email addresses or domains. If you use sender email addresses or domains criteria, they will only match against the **EnvelopeFrom** email address.

- Can have up to 50 criteria per rule.

Security Mailbox rules:

- Apply to incoming messages for the specified recipient email addresse(s); messages will not be analyzed.

  > Security Mailbox rules are only applied if all the recipients on an email are included in the rule. If other recipients are copied or included as a BCC (blind carbon copy), the message will not bypass the analysis engines. It is important you specify all possible addresses that are expected in the **EnvelopeTo** and **DeliveredTo** fields. These fields are parsed differently and may have different values.

- Can have up to 50 criteria per rule.

There is a limit of 20 active Message Bypass rules. Rules can be deactivated or deleted.

Advisory on Creating and Using Message Bypass Rules

Note the following important caveats when creating and using Message bypass rules.

- A Message bypass rule bypasses all scanning and protections for messages that match the rule conditions. Do not use these rules for any use-cases other than customer employee security awareness training (Phish Test) or for end-mailbox-user reporting to an organization’s Security Mailbox. These are the only supported scenarios for Message bypass rules. For other scenarios, use allow/block lists or Policy configuration exceptions.
- It is strongly advised to use only the dedicated Sender IP Addresses/CIDR blocks provided by your Phish Test vendor as the basis of Message bypass rules
- Be aware if your Phish Test vendor is unable to provide dedicated Sender IP Addresses/CIDR blocks; the usage of Sender Domain or Email Address in a Message bypass rule opens you up to bypassing potentially spoofed messages.
- Do not use Sender Domain or Email Address in a Message bypass rule unless you have separately validated that sender email authentication is strongly enforced by your organization’s upstream edge email controls, and the specified Sender Domain or Sender Email Address exactly matches the final Return-Path header on all messages intended to match the Message bypass rule.

Add a New Message Bypass Rule

Complete the following steps to create a new rule:

1. Select **Configuration** > **Global settings**.
2. On the **Message bypass rules** panel, select the **Phish test senders** tab or the **Recipients (Security mailboxes)** tab.
3. Click the **New Phish Test Rule** or **New Security Mailbox Rule** button.
4. Create a rule name. Each rule must have a unique name.
5. For a Phish Test rule, select a criteria type: Email Addresses, Domains, IP Addresses, or CIDR addresses. Then, enter your items, separated by commas.
6. For a Security Mailbox rule, enter your recipient email addresse(s), separated by commas. Be sure to include all possible recipient addresses expected to be in the **EnvelopeTo** and **DeliveredTo** fields, as they may differ. Your rule will only fire if all the recipients on the message are included in the rule.
7. Click **Save** to finish creating the rule.

Your rule is added to the list. It may take up to 20 minutes for the change to take effect.

> ⓘ If a Message bypass rule is created for testing, the rule should be reconsidered after an appropriate period of time to prevent vulnerabilities.

Edit a Message Bypass Rule

To edit a rule:

1. Select **Configuration** > **Global settings**.
2. On the **Message bypass rules** panel, select the type of rule you want to edit.
3. Click the pencil icon next to the rule you want to edit.
4. Make your desired changes, then click **Save**.

Your rule is updated. It may take up to 20 minutes for the change to take effect.

Enable or Disable a Message Bypass Rule

To enable or disable an existing rule:

1. Select **Configuration** > **Global settings**.
2. On the **Message bypass rules** panel, select the type of rule you want to edit.
3. Click the pencil icon next to the rule you want to edit.
4. Switch the **Rule** status toggle to **Inactive** or **Active**.
5. Click **Save**.

The status of your rule is updated. It may take up to 20 minutes for the change to take effect.

Delete a Message Bypass Rule

To delete a rule:

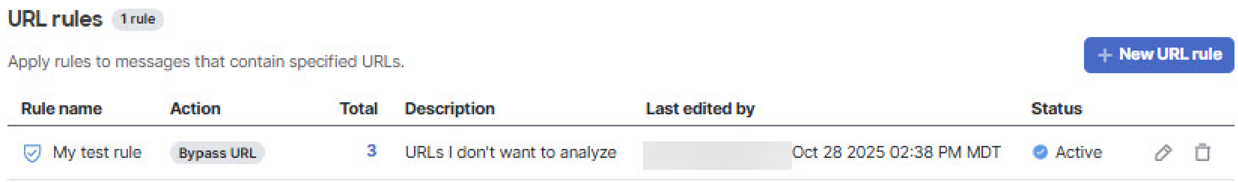
1. Select **Configuration** > **Global settings**.
2. On the Message bypass rules panel, select the type of rule you want to edit.
3. Click the delete icon next to the rule you want to delete.

Your rule is deleted.

URL Rules

URL rules apply to messages that contain specified URLs. Currently, Bypass URL is the only action that can be applied with this rule type. For example, if you do not want URLs that point to your company intranet to be analyzed, you can create a URL rule to bypass analysis of your intranet URLs. The messages are fully scanned aside from the specified URLs.

URL rules can be created on the **Configuration** > **Global Settings** > **URL rules** panel.



URL rules 1 rule

Apply rules to messages that contain specified URLs.

Rule name	Action	Total	Description	Last edited by	Status
My test rule	Bypass URL	3	URLs I don't want to analyze	[redacted] Oct 28 2025 02:38 PM MDT	Active

Add a New URL rule

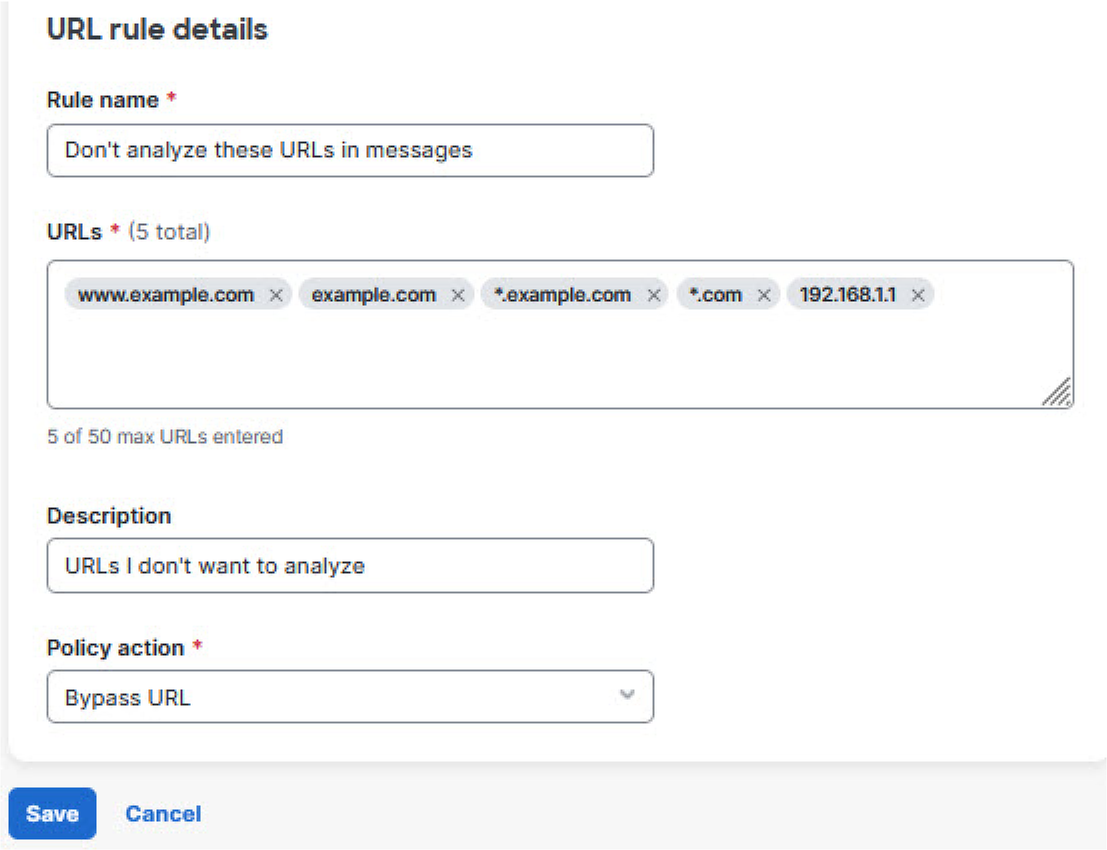
Complete the following steps to create a new URL rule:

1. Select **Configuration** > **Global settings**.
2. On the **URL rules** panel, click the **New URL rule** button.
3. Create a rule name. Each rule must have a unique name.
4. Enter the URLs you want to bypass analysis of.

   The following bullets provide examples of valid formats. Note that path/query parameters are not supported.

   - Domain: example.com, www.example.com
   - Wildcard subdomain: *.example.org
   - Wildcard domain: *.com
   - IPv4 address: 192.168.1.1
   - IPv6 address: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
5. Enter a short description for the rule.

6. Select what policy action you want to apply. **Bypass URL** is the only option currently available.
7. Click **Save**.



URL rule details

Rule name *

Don't analyze these URLs in messages

URLs * (5 total)

www.example.com × example.com × *.example.com × *.com × 192.168.1.1 ×

5 of 50 max URLs entered

Description

URLs I don't want to analyze

Policy action *

Bypass URL

Your rule is added to the list. It may take up to 20 minutes for the change to take effect.

Edit a URL Rule

To edit a rule:

1. Select **Configuration** > **Global settings**.
2. On the **URL rules** panel, click the pencil icon next to the rule you want to edit.
3. Make your desired changes, then click **Save**.

Your rule is updated. It may take up to 20 minutes for the change to take effect.

Enable or Disable a URL Rule

To enable or disable an existing rule:

1. Select **Configuration** > **Global settings**.
2. On the **URL rules** panel, click the pencil icon next to the rule you want to edit.

3. Switch the **Rule** status toggle to **Inactive** or **Active**.
4. Click **Save**.

The status of your rule is updated. It may take up to 20 minutes for the change to take effect.

Delete a URL Rule

To delete a rule:

1. Select **Configuration** > **Global settings**.
2. On the **URL rules** panel, click the delete icon next to the rule you want to delete.

Your rule is deleted.

Data Loss Prevention (DLP)

> i DLP is available for Cisco Secure Access customers with Secure Email Threat Defense advantage and premier licenses.

Secure Email Threat Defense uses centralized Cisco Secure Access Data Loss Prevention (DLP) services. To access the Data loss prevention settings navigate to **Configuration** > **Global settings**.

To integrate Secure Access DLP with Secure Email Threat Defense, there are three tasks:

1. Generate API keys with a "DLP as A Service" scope from within Cisco Secure Access. For details, see Cisco Secure Access Help: Add API Key.
2. Use the generated credentials to Enable DLP in Secure Email Threat Defense. For details, see **Enable DLP**.
3. Add an email rule to the DLP policy in Secure Access. For details, see Cisco Secure Access Help: Add an Email Rule to the Data Loss Prevention Policy.

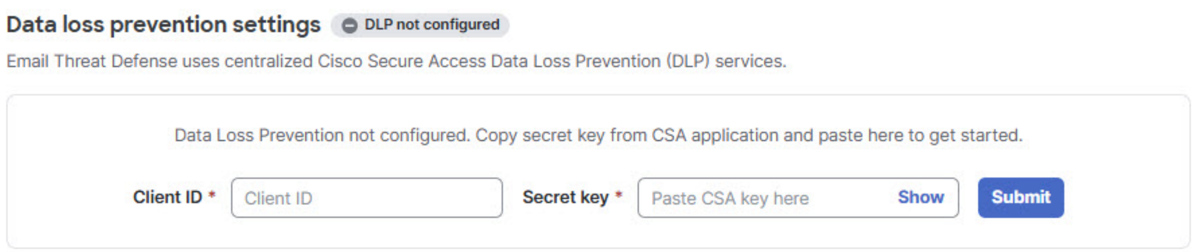
Generate Cisco Secure Access DLP API Keys

Before you can enable DLP in Secure Email Threat Defense, generate API keys with a "DLP as A Service" scope from within Cisco Secure Access. For details, see Cisco Secure Access Help: Add API Key.

Enable DLP

Complete the following steps to enable DLP in Secure Email Threat Defense:

1. Select **Configuration** > **Global settings**.
2. On the **Data loss prevention settings** panel, enter the Client ID and Secret key that you generated in **Generate Cisco Secure Access DLP API Keys**.



Data loss prevention settings

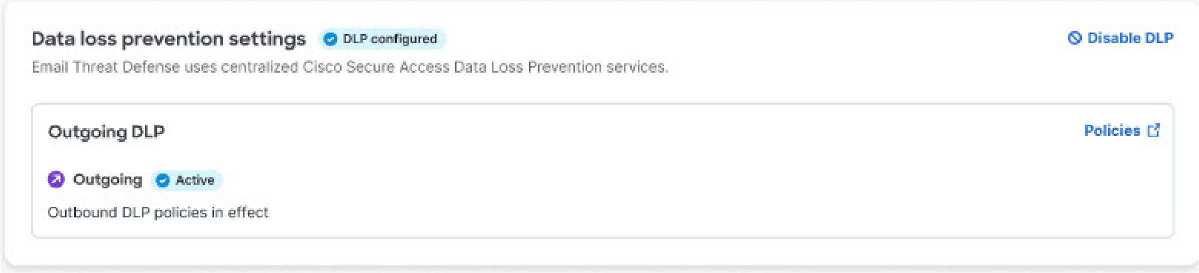
Email Threat Defense uses centralized Cisco Secure Access Data Loss Prevention (DLP) services.

Data Loss Prevention not configured. Copy secret key from CSA application and paste here to get started.

Client ID * Client ID

Secret key * Paste CSA key here

3. Click **Submit**. DLP is now enabled.



Data loss prevention settings

Email Threat Defense uses centralized Cisco Secure Access Data Loss Prevention services.

Outgoing DLP

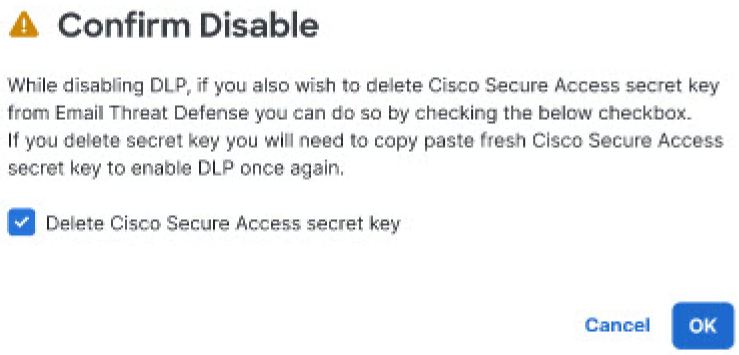
Outbound DLP policies in effect

4. In Cisco Secure Access, add an email rule to the Data Loss Prevention Policy. For details, see Cisco Secure Access Help: Add an Email Rule to the Data Loss Prevention Policy.

Disable DLP

To disable DLP:

1. Select **Configuration** > **Global settings**.
2. On the **Data loss prevention settings** panel, click **Disable DLP**.
3. A confirmation dialog is displayed. A checkbox provides the option to delete your keys as you disable the feature.
4. Click **OK**. DLP is now disabled.



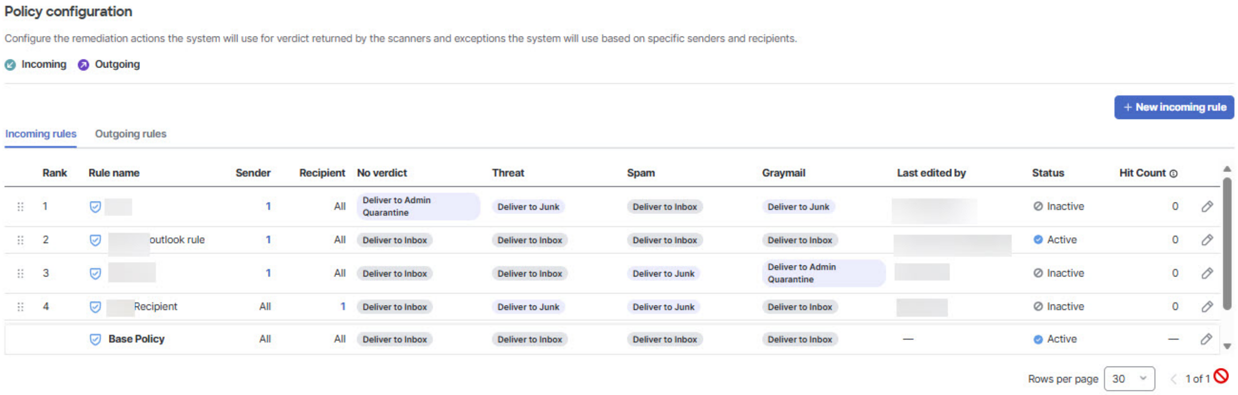
Confirm Disable

While disabling DLP, if you also wish to delete Cisco Secure Access secret key from Email Threat Defense you can do so by checking the below checkbox.
If you delete secret key you will need to copy paste fresh Cisco Secure Access secret key to enable DLP once again.

☑ Delete Cisco Secure Access secret key

Policy Configuration

The Policy configuration page is where you configure remediation actions the system will use for verdicts returned by the scanners as well as exceptions the system will use based on specific senders and recipients.



Policy configuration

Configure the remediation actions the system will use for verdict returned by the scanners and exceptions the system will use based on specific senders and recipients.

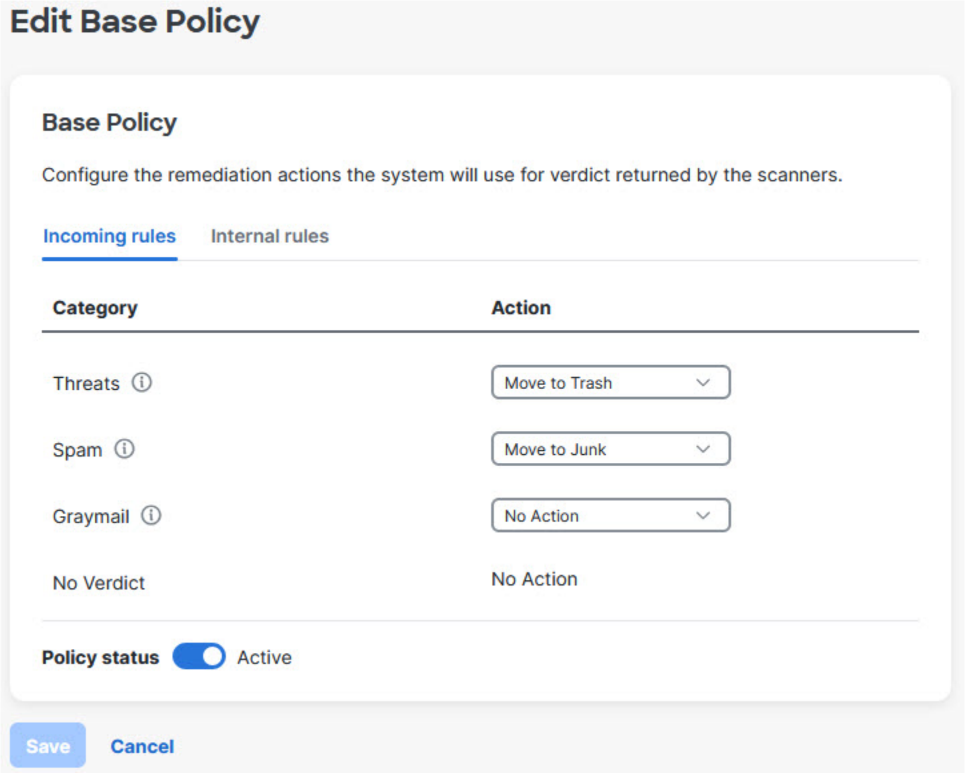
Rank	Rule name	Sender	Recipient	No verdict	Threat	Spam	Graymail	Last edited by	Status	Hit Count
1	[redacted]	1	All	Deliver to Admin Quarantine	Deliver to Junk	Deliver to Inbox	Deliver to Junk	[redacted]	Inactive	0
2	[redacted] outlook rule	1	All	Deliver to Inbox	Deliver to Inbox	Deliver to Inbox	Deliver to Inbox	[redacted]	Active	0
3	[redacted]	1	All	Deliver to Inbox	Deliver to Inbox	Deliver to Junk	Deliver to Admin Quarantine	[redacted]	Inactive	0
4	[redacted] Recipient	All	1	Deliver to Inbox	Deliver to Junk	Deliver to Junk	Deliver to Inbox	[redacted]	Inactive	0
	Base Policy	All	All	Deliver to Inbox	Deliver to Inbox	Deliver to Inbox	Deliver to Inbox	—	Active	—

Base Policy

The Base Policy defines your default remediation actions. You can indicate different actions for different types of messages (Threats, Spam, and Graymail) and different message directions.

Click the pencil icon at the right side of the **Configuration** > **Policy Configuration** > **Base Policy** row to be taken to the Edit Base Policy dialog where you can make adjustments for different directions and message categories. You can set different policies by message direction.

Internal message settings also apply to outgoing messages in a sender’s mailbox. For example, if bob@yourcompany.com sends a message to a recipient outside of your domain, the Internal message settings apply to the message in his sent messages folder.



Edit Base Policy

Base Policy

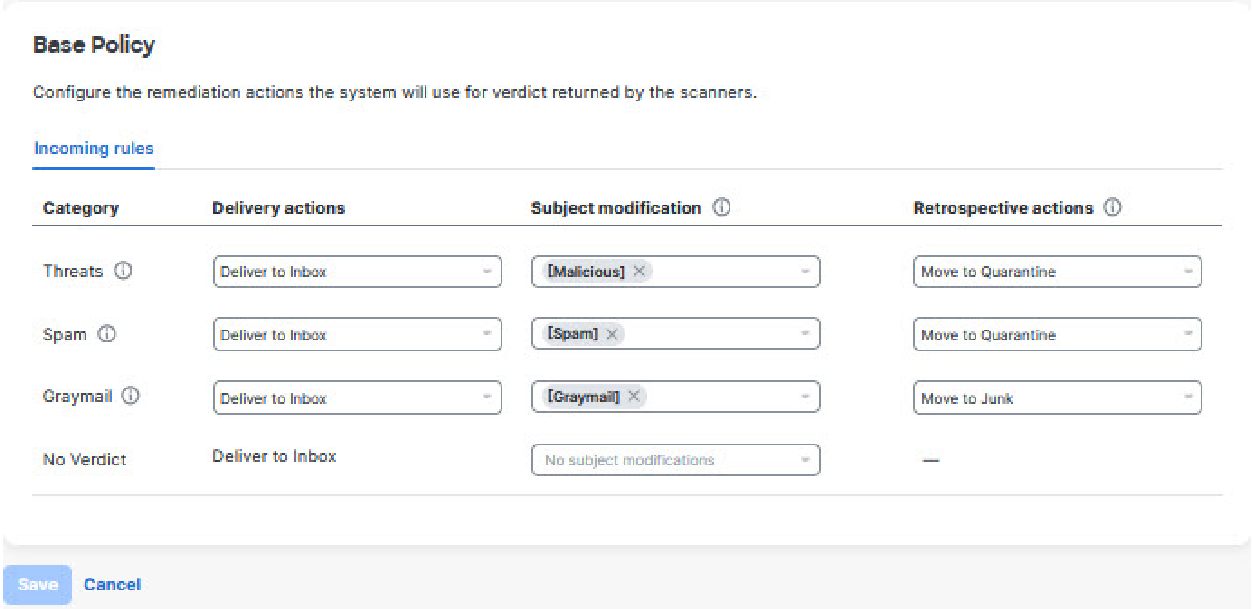
Configure the remediation actions the system will use for verdict returned by the scanners.

Category	Action
Threats	Move to Trash
Spam	Move to Junk
Graymail	No Action
No Verdict	No Action

Policy status: Active

For SMTP/Inline message sources, you can also define the following as part of your Base Policy:

- Subject modifications to be pre-pended to subject lines when Delivery actions are applied. The options include [Spam], [Graymail], [Marketing], [Bulk], [External], [Malicious], and [Potentially harmful].
- Retrospective actions to be applied if a retrospective verdict is reached by the analysis engines



Base Policy

Configure the remediation actions the system will use for verdict returned by the scanners.

Incoming rules

Category	Delivery actions	Subject modification	Retrospective actions
Threats	Deliver to Inbox	[Malicious]	Move to Quarantine
Spam	Deliver to Inbox	[Spam]	Move to Quarantine
Graymail	Deliver to Inbox	[Graymail]	Move to Junk
No Verdict	Deliver to Inbox	No subject modifications	—

Policy Configuration Settings

Setting	Description	Options	Default
Base Policy (Journal Sources)	Default remediation actions for messages found to be: - **Threats** (BEC, Scam, Phishing, or Malicious) - **Spam** - **Graymail**	- **Move to Trash** - **Move to Junk** - **Move to Quarantine** - **No Action** If the sender address belongs to a sender allow-list in Exchange or the message has already been remediated by Microsoft 365, remediation actions are not applied.	- Threats - **Move to Quarantine** - Spam - **Move to Junk** - Graymail - **No Action**
Base Policy (SMTP/Inline Sources)	Default actions for messages found to be: - **Threats** (BEC, Scam, Phishing, or Malicious) - **Spam** - **Graymail**	- **Deliver to Inbox** - **Deliver to Junk** - **Deliver to Quarantine** - **Drop**	Base Policy defaults: - Threats - **Deliver to Quarantine** - Spam - **Deliver to Quarantine** - Graymail - **Deliver to Junk**

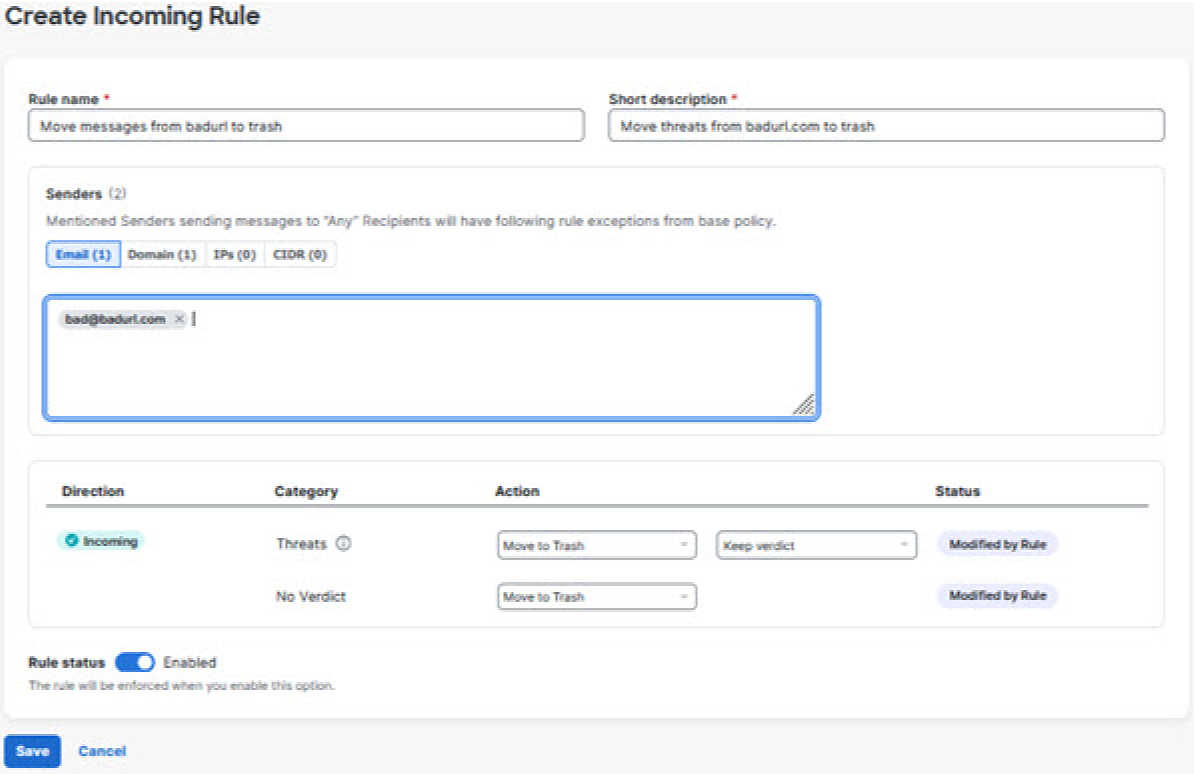
Setting	Description	Options	Default
			Retrospective Verdict Policy defaults: ▪ Threats - **Move to Quarantine** ▪ Spam - **Move to Quarantine** ▪ Graymail - **Move to Junk**

Policy Exceptions

You can create policy exception rules by senders (all Message sources) or recipients (SMTP Message sources). These rules act as exceptions to your base policy. Rules are applied in a ranked order; drag and drop the items in the list to reorder them.

Create exceptions to your base policy by creating policy exception rules.

1. Go to **Configuration** > **Policy configuration**.
2. Select the tab for the direction you want the rule to apply to. For these steps we'll use incoming as an example.
3. Click the **New incoming rule** button.
4. Create a Rule name and a Short description for the rule.
5. Under **Apply to**, select Sender or Recipient. For Journal message sources, Sender is already selected as the only option.
6. Click the category of item you want to add, then enter the senders or recipients you want the rule to apply to.
   - For sender rules, this can be in the form of email addresses, domains, IP addresses, or CIDR block.
   - For recipient rules, this can be an email address, domain, or **Supported Microsoft Groups**.
7. Select actions you want to apply as exceptions to your base policy. For example, you may want to move all messages from a certain sender to trash, regardless of the verdict.
8. Click **Save**.



Create Incoming Rule

Rule name *: Move messages from badurl to trash

Short description *: Move threats from badurl.com to trash

Senders (2)

Mentioned Senders sending messages to "Any" Recipients will have following rule exceptions from base policy.

Email (1) | Domain (1) | IPs (0) | CIDR (0)

bad@badurl.com ×

Direction	Category	Action		Status
Incoming	Threats ⓘ	Move to Trash	Keep verdict	Modified by Rule
	No Verdict	Move to Trash		Modified by Rule

Rule status: Enabled

The rule will be enforced when you enable this option.

Your rule is created.

Supported Microsoft Groups

Secure Email Threat Defense's integration with Microsoft groups supports the following:

- Microsoft 365 Groups
- Security Groups
- Mail-enabled security groups
- Distribution groups

Dynamic distribution groups are not supported.

Configuration Settings with a Gateway

If you have a Cisco Email Security appliance or similar gateway in place, consider using the following policy settings.

Table 4. Suggested Policy Settings with Gateway

Setting Name	Recommended Selection
Secure Email Gateway (SEG)	**Yes, Secure Email Gateway is present**, and indicate header

Setting Name	Recommended Selection
Message Analysis	**Unwanted message analysis (Spam and Graymail)** off
Remediation Actions	**Threats - Move to Quarantine**

It is important to indicate that a Secure Email Gateway (SEG) is present and which header can be used to identify it in incoming journals so Secure Email Threat Defense can determine the true originating sender of a message. Without this configuration it may appear that all messages come from the SEG, which could result in false positive convictions.

For information on verifying or configuring the header on Cisco Secure Email Cloud Gateway (formerly CES) or Cisco Secure Email Gateway (formerly ESA), see https://docs.ces.cisco.com/docs/configuring-asyncos-message-filter-to-add-sender-ip-header-for-cloud-mailbox.

If you are using Microsoft 365 as your message source, we also recommend bypassing your appliance so journals are sent directly from Microsoft 365 to Secure Email Threat Defense. You can do this by adding a connector in Microsoft 365, as described in **Setup for Journal Message Sources**.

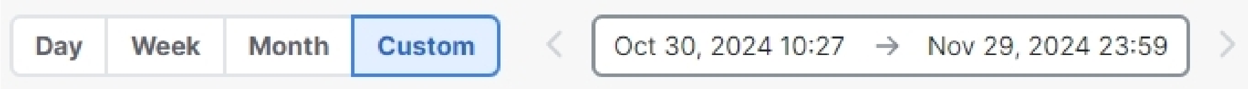
Messages

The Messages page shows your messages and search results and allows you to look for possible compromises. You can display up to 100 messages per page.

In this chapter:

Search and Filter

Use the calendar control to show data for a defined time period (most recent Day, Week, or Month), or a Custom time frame within the last 90 days.



Oct 30, 2024 10:27 → Nov 29, 2024 23:59

Use the search field to search for strings or indicators of interest, such as hashes or URLs.

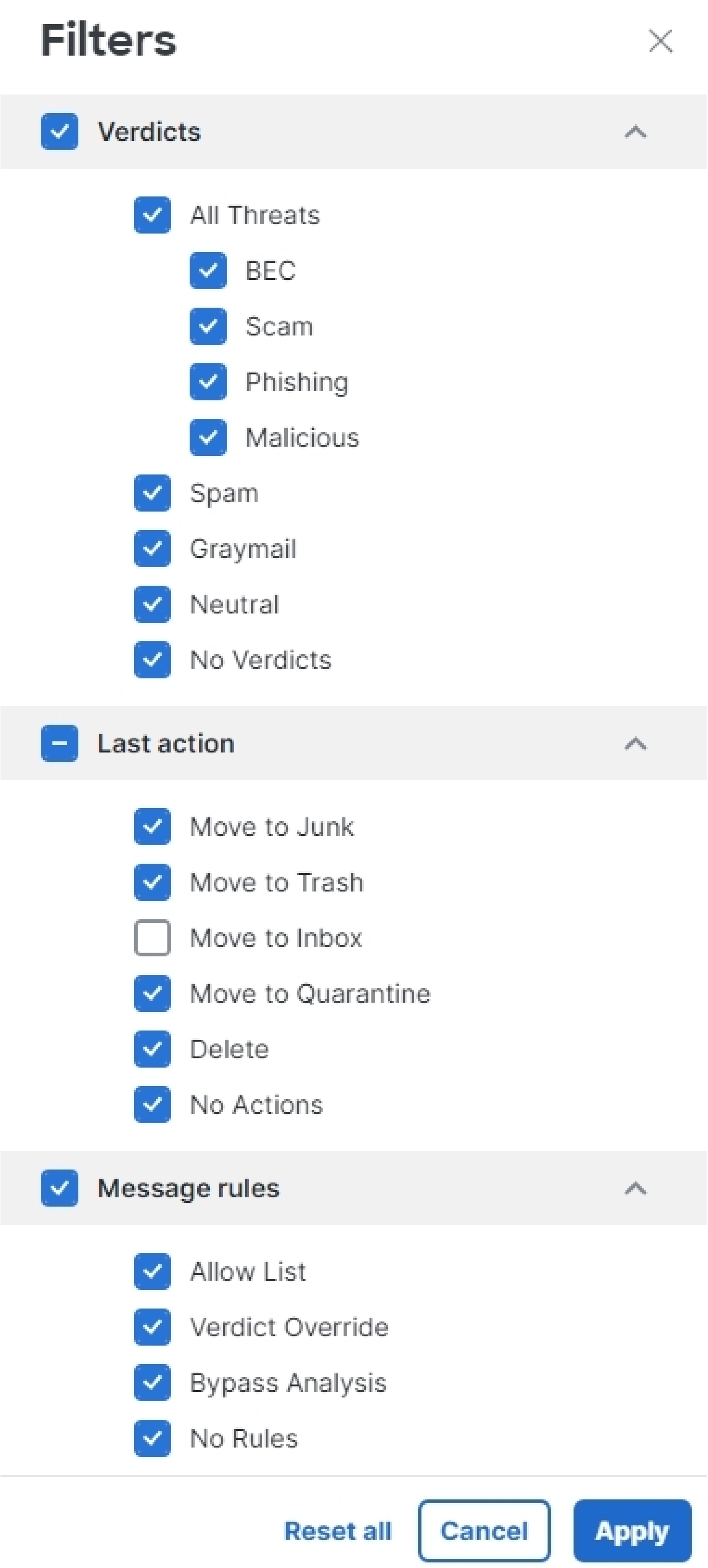
Search Messages for a URL, subject line, recipient, or IP

Filter Panel

Use the filter panel to refine your search. For example, you may want to see all mail sent from a specific sender, mail with a specific verdict, mail with attachments or links, mail that has been reclassified, mail that has been moved to Junk, and so on.

1. Click **Filters** to expand the filter panel.

2. Make your selections, then click **Apply**. Note that you must have at least one item selected under Verdict.



Filters

☑ Verdicts

- ☑ All Threats
  - ☑ BEC
  - ☑ Scam
  - ☑ Phishing
  - ☑ Malicious
- ☑ Spam
- ☑ Graymail
- ☑ Neutral
- ☑ No Verdicts

⊟ Last action

- ☑ Move to Junk
- ☑ Move to Trash
- □ Move to Inbox
- ☑ Move to Quarantine
- ☑ Delete
- ☑ No Actions

☑ Message rules

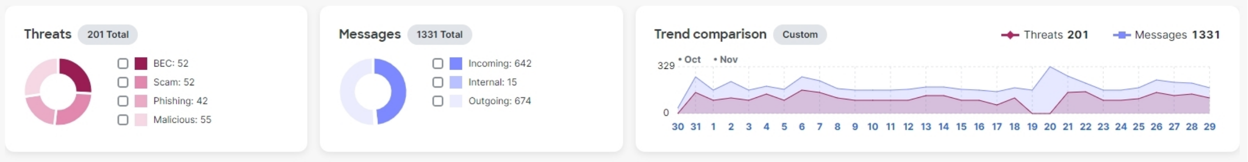
- ☑ Allow List
- ☑ Verdict Override
- ☑ Bypass Analysis
- ☑ No Rules

Use the **Reset all** button to reset the filters to their defaults.

Messages Graph and Quick Filter

The messages graph and quick filter across the top of the Messages page provides a graphical view of your message traffic. Use this graph to quickly filter your messages. The graph includes:

- A Threat and category breakout to view totals and easily filter for threats.
- Message Direction totals you can use to quickly filter by direction.
- The comparison of trends for the selected date range.



To hide these charts to free up screen space, click **Hide Charts** next to the calendar controls. Similarly, click **Show Charts** to show them when they have been hidden.

Verdicts

Secure Email Threat Defense applies the following threat verdicts to messages:

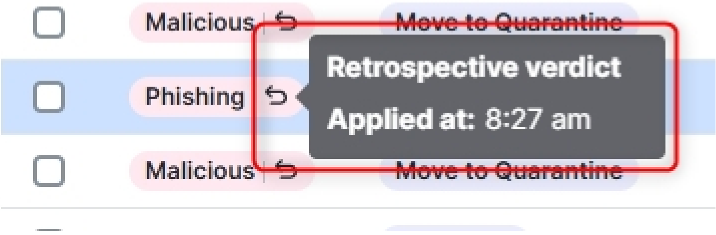
- **BEC**: Business Email Compromises (BEC) are sophisticated scams that use social engineering and intrusion techniques to cause financial damage to the organization.
- **Scam**: Scams are focused on causing financial harm to individuals using techniques such as lottery or extortion fraud.
- **Phishing**: These messages have been convicted of fraudulently copying or mimicking legitimate services in an attempt to acquire sensitive information such as user names, passwords, credit card numbers, and more.
- **Malicious**: These messages have been convicted of containing, serving, or supporting the delivery or propagation of malicious software.

Retrospective Verdicts

A retrospective verdict is one that was applied to a message sometime after the message was first scanned by Secure Email Threat Defense.

A retrospective verdict in Secure Email Threat Defense is slightly different that in other Cisco security products. Although Secure Email Threat Defense is not an inline mail processor, it does have a fixed time range for completing its initial analysis of a message. Newer content engines that have longer analysis times, such as Talos' Deep URL Analysis, are treated as a retrospective verdict. As the verdict is delayed, so is the remediation. Thus, Secure Email Threat Defense tags these convictions distinctly.

Retrospective verdicts are indicated on the Messages page next to the Verdict with a blue icon. Hover your cursor over the icon to see the time the retrospective verdict was applied and the difference between when the message was received and when the verdict was applied.



Retrospective Verdict Email Notifications

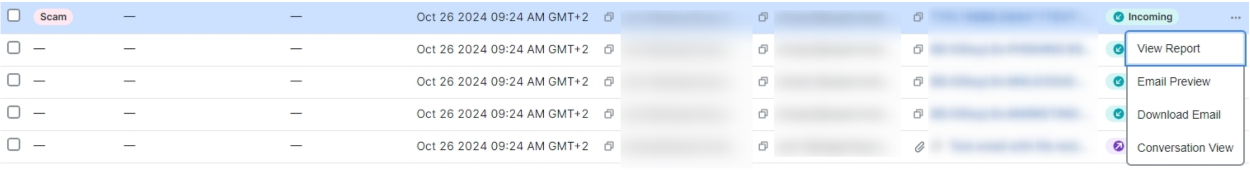
To turn email notifications for retrospective verdicts on or off:

1. Select **Administration** > **Business**.
2. Under **Preferences**, select or deselect >**Send Notifications for Retrospective Verdicts**.

Retrospective verdicts email notifications are sent to the specified notification email address if the check box is selected. These notifications are turned on by default.

Message Report

The message report allows you to investigate details about a message. Select **...** > **View Report** or click anywhere on a message row to access the report for that message.

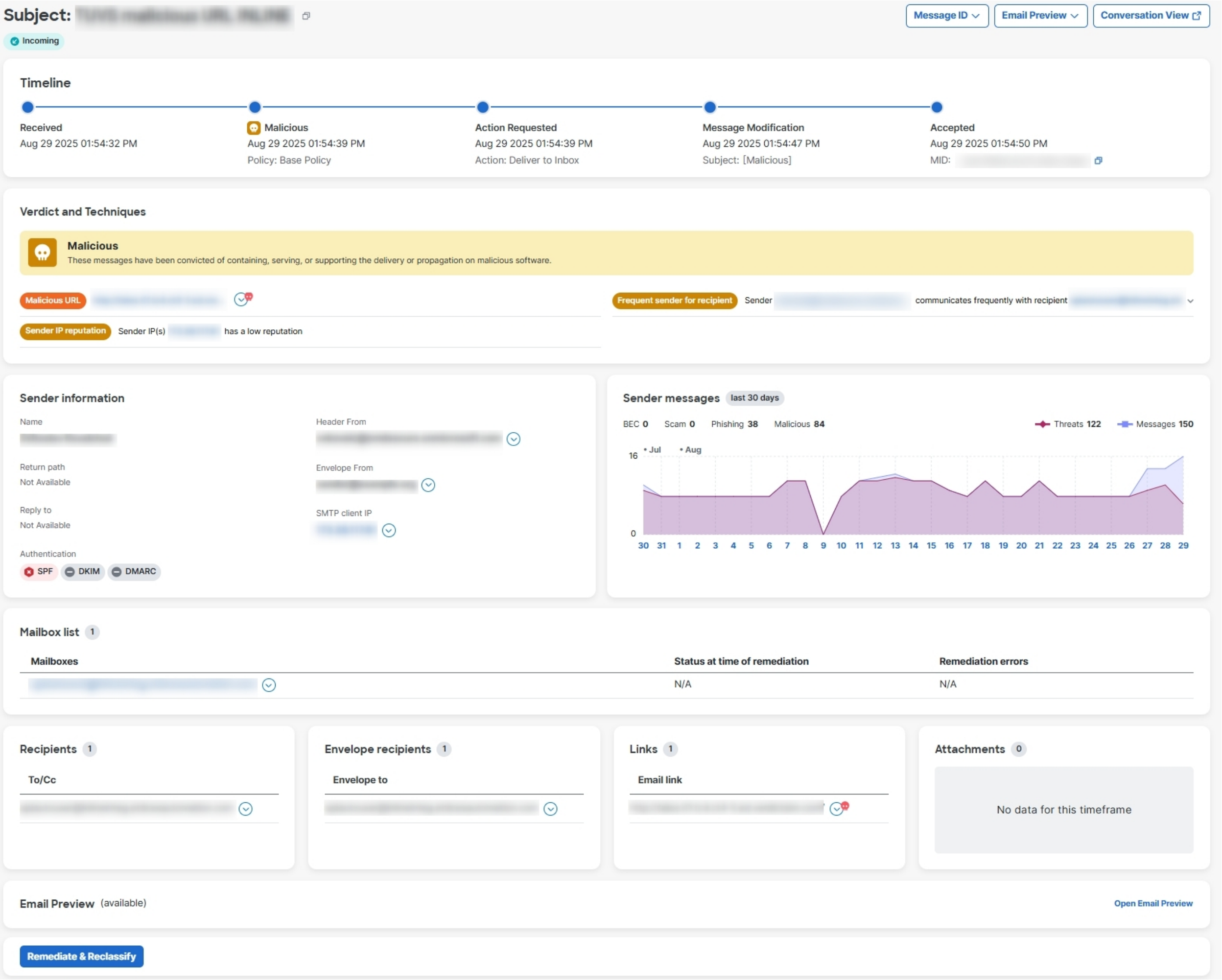


□	Scam	—	—	Oct 26 2024 09:24 AM GMT+2				Incoming ...
□	—	—	—	Oct 26 2024 09:24 AM GMT+2				
□	—	—	—	Oct 26 2024 09:24 AM GMT+2				
□	—	—	—	Oct 26 2024 09:24 AM GMT+2				
□	—	—	—	Oct 26 2024 09:24 AM GMT+2				

The message report shows details about a message including:

- Message direction, Microsoft Message ID, and if the message was read at the time of remediation
- Timeline
- Verdict and Techniques
- Sender Information (including authentication errors for SMTP message sources)
- Sender Messages
- Recipient information including Recipients, Envelope Recipients, and Mailboxes
- Links
- Attachments
- Email Preview

The message report also gives access to Conversation View and EML Downloads.



Subject: [redacted]

Incoming

Timeline

Received	Malicious	Action Requested	Message Modification	Accepted
Aug 29 2025 01:54:32 PM	Aug 29 2025 01:54:39 PM	Aug 29 2025 01:54:39 PM	Aug 29 2025 01:54:47 PM	Aug 29 2025 01:54:50 PM
	Policy: Base Policy	Action: Deliver to Inbox	Subject: [Malicious]	MID: [redacted]

Verdict and Techniques

Malicious
These messages have been convicted of containing, serving, or supporting the delivery or propagation on malicious software.

Malicious URL [redacted]

Frequent sender for recipient Sender [redacted] communicates frequently with recipient [redacted]

Sender IP reputation Sender IP(s) [redacted] has a low reputation

Sender information

Name
[redacted]

Header From
[redacted]

Return path
Not Available

Envelope From
[redacted]

Reply to
Not Available

SMTP client IP
[redacted]

Authentication
SPF DKIM DMARC

Sender messages last 30 days

BEC 0 Scam 0 Phishing 38 Malicious 84

Mailbox list 1

Mailboxes	Status at time of remediation	Remediation errors
[redacted]	N/A	N/A

Recipients 1

To/Cc
[redacted]

Envelope recipients 1

Envelope to
[redacted]

Links 1

Email link
[redacted]

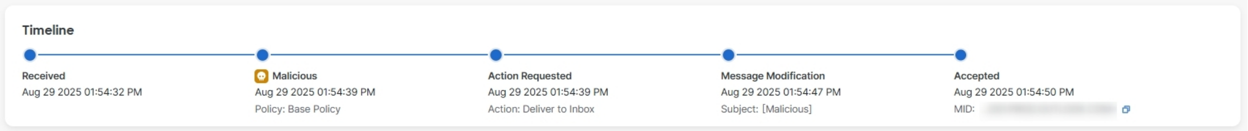
Attachments 0

No data for this timeframe

Email Preview (available)

Timeline

The Timeline for a message is shown on the messages report.



Timeline

Received	Malicious	Action Requested	Message Modification	Accepted
Aug 29 2025 01:54:32 PM	Aug 29 2025 01:54:39 PM	Aug 29 2025 01:54:39 PM	Aug 29 2025 01:54:47 PM	Aug 29 2025 01:54:50 PM
	Policy: Base Policy	Action: Deliver to Inbox	Subject: [Malicious]	MID: [redacted]

The timeline shows:

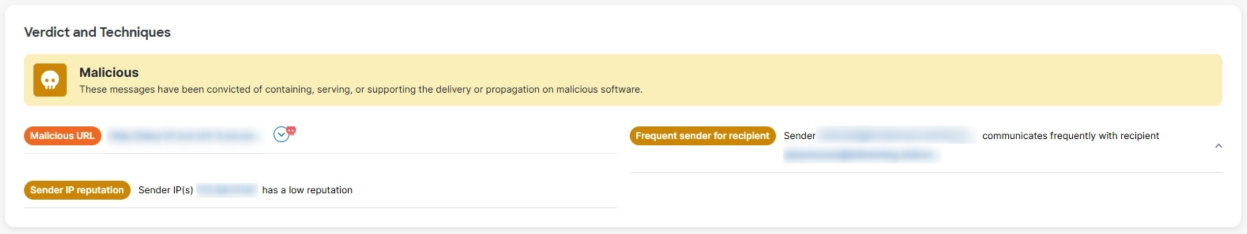
- **Received**: when a message was received and details about the message direction
- **Rule**: information about any message rule that was applied
- **Verdict**: information about any verdict that was rendered or applied and who performed the action

- **Action**: information about any action that was taken on the message and who performed the action. This includes:
  - Where and how a message was moved
  - Information about any remediation errors on the message and which mailboxes had the errors

Verdict and Techniques

The Verdict and Techniques panel shows a visual representation of the verdict applied to a message and techniques detected that may have contributed to the verdict. Techniques are color coded to indicate their severity. Malicious file names/SHA256 and URLs are shown dynamically when available. Static descriptions are shown when dynamic text is not possible.

You can remediate and/or reclassify a message directly from this panel. Click the Remediate & Reclassify button, then follow the directions provided in **Move and Reclassify Messages**.



Verdict and Techniques

Malicious
These messages have been convicted of containing, serving, or supporting the delivery or propagation on malicious software.

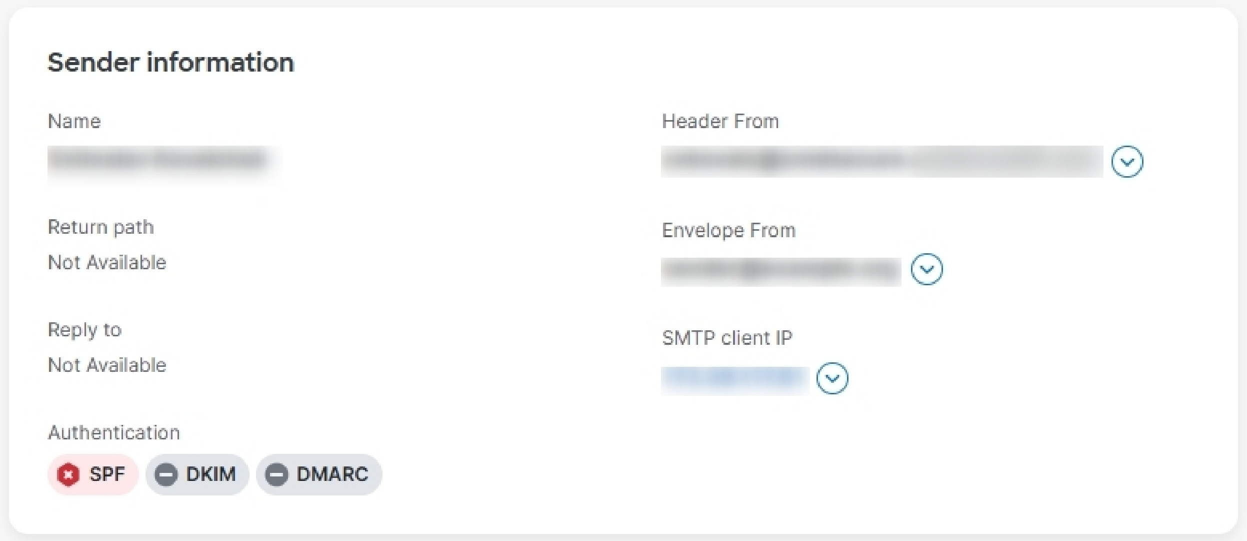
Malicious URL [redacted]

Frequent sender for recipient Sender [redacted] communicates frequently with recipient [redacted]

Sender IP reputation Sender IP(s) [redacted] has a low reputation

Sender Information

The Sender Information panel shows information known about the sender of the message including name, email address, return path, reply to, SMTP server and client IPs, X-Originating IP, and SPF, DKIM, and DMARC authentication errors. For more information on Authentication errors, see **Authentication Error Codes**. Mouse-over the Authentication indicators to see details about the errors.



Sender information

Name
[redacted]

Header From
[redacted]

Return path
Not Available

Envelope From
[redacted]

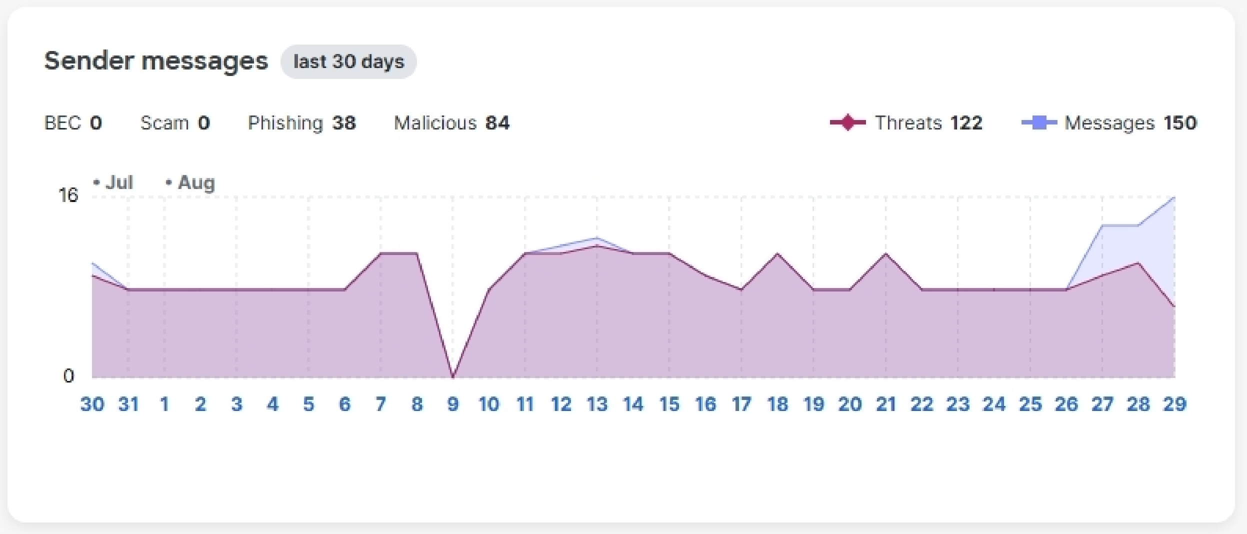
Reply to
Not Available

SMTP client IP
[redacted]

Authentication
SPF DKIM DMARC

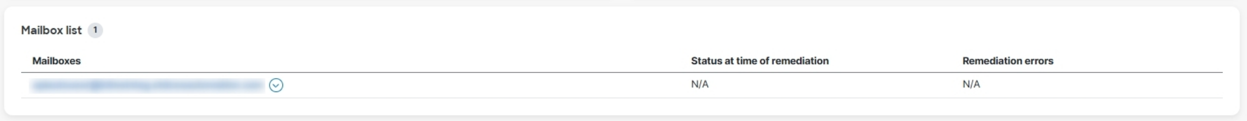
Sender Messages

The Sender Messages graph shows the total messages sent and total threat messages sent by the sender of the message over the last 30 days. This can help you quickly see if there is any pattern of threat messages from the user.



Mailbox List

The Mailbox List shows a list of end-user mailboxes that received incoming and internal messages. The list also shows if the message was read prior to the last remediation action and any remediation errors on the message. Remediation errors can occur if a user deleted or moved a messages before the system tried to remediate it.

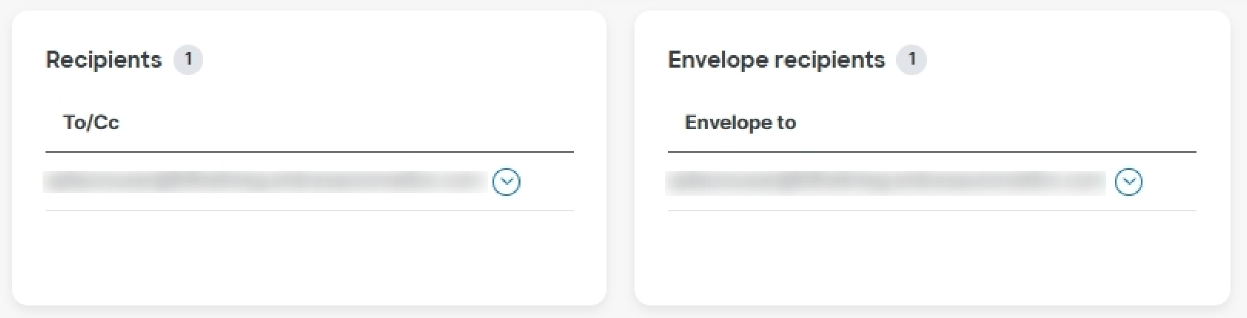


Mailbox list 1

Mailboxes	Status at time of remediation	Remediation errors
[redacted]	N/A	N/A

Recipient Information

The Recipients and Envelope Recipients panels show information about who the message was sent to.



Recipients 1

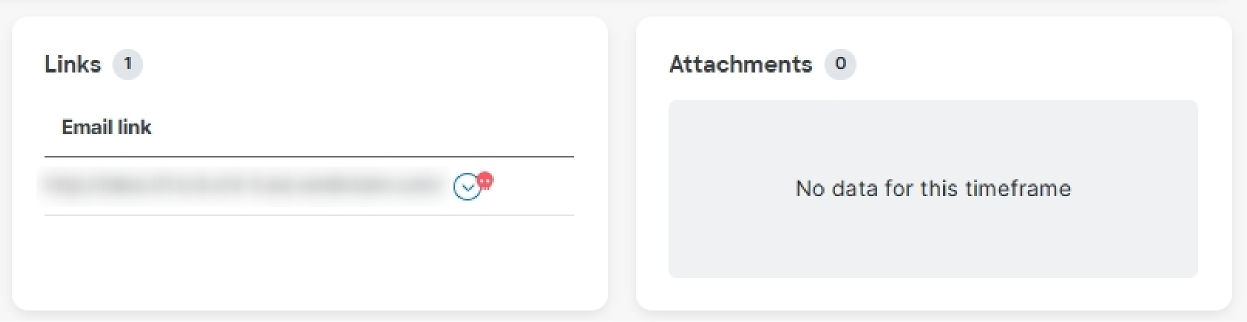
To/Cc
[redacted]

Envelope recipients 1

Envelope to
[redacted]

Links and Attachments

The Links and Attachment panels show information about links and attachments found in the message.



Links 1

Email link

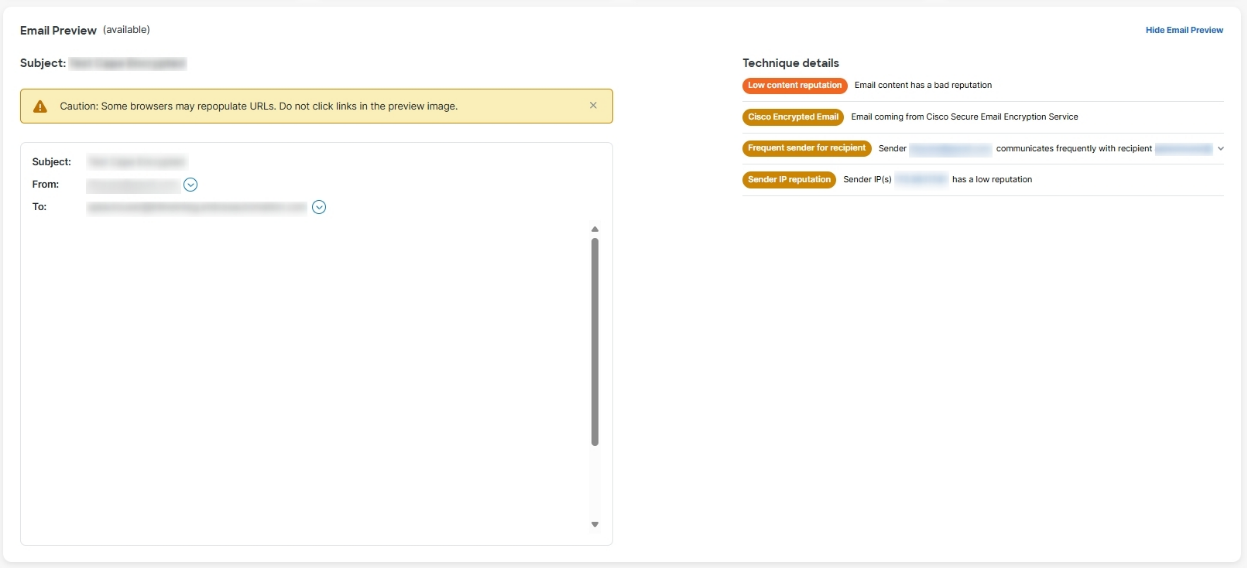
[redacted]

Attachments 0

No data for this timeframe

Email Preview

The Email Preview allows super-admin and admin users to request and see a message as it appears to the end-user without needing to download the EML file. The message is shown as an image. Click the **Open Email Preview** button to see the preview.



Email Preview (available)

Subject: [redacted]

Caution: Some browsers may repopulate URLs. Do not click links in the preview image.

Subject: [redacted]

From: [redacted]

To: [redacted]

Technique details

Low content reputation — Email content has a bad reputation

Cisco Encrypted Email — Email coming from Cisco Secure Email Encryption Service

Frequent sender for recipient — Sender [redacted] communicates frequently with recipient [redacted]

Sender IP reputation — Sender IP(s) [redacted] has a low reputation

An audit log record is created when a user previews a message. The audit log is available for download from **Administration** > **Business** > **Preferences**.

Conversation View

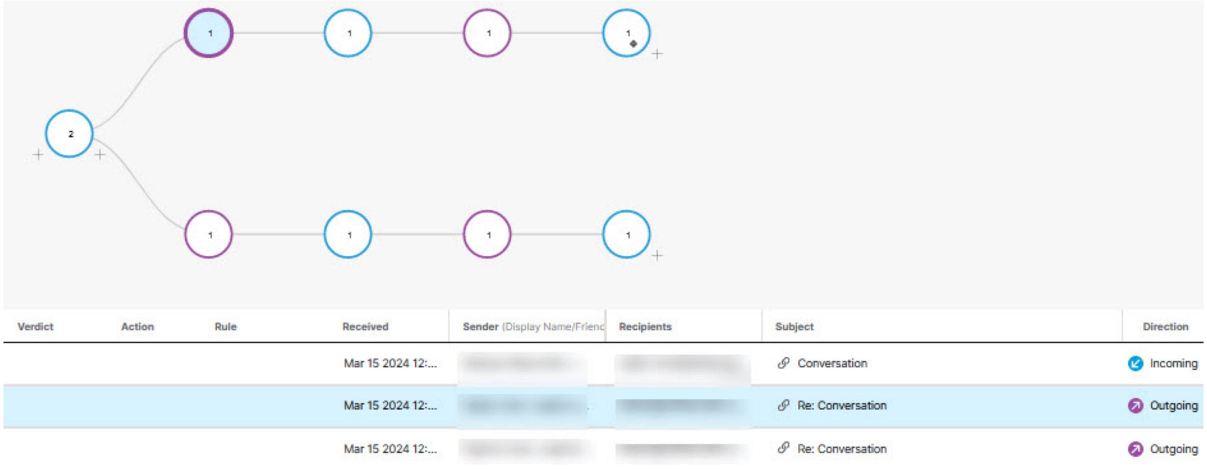
Conversation view provides a holistic view of a conversation. Use the conversation view to track the messages in a conversation and gain a complete understanding of the mail flow. This can be useful in determining where a threat originated and how it spread within your organization.

When you are in the message report, click the **Conversation View** button on the top right of the page to see messages that are connected to a specific email.

Conversation View

Click the **+** icons to expand nodes of the conversation so you can see messages that came earlier or later in the conversation. Nodes that are expanded are added to the message grid shown below the nodes. Nodes and messages are color-coded to indicate direction: Incoming, Outgoing, or Internal.

The number within the node circle indicates how many addresses the message was sent to. An icon within a node indicates if a threat was detected or a verdict was applied. When you select a node, the corresponding message in the grid is highlighted.



Verdict	Action	Rule	Received	Sender (Display Name/Frienc	Recipients	Subject	Direction
			Mar 15 2024 12:...	[redacted]	[redacted]	Conversation	Incoming
			Mar 15 2024 12:...	[redacted]	[redacted]	Re: Conversation	Outgoing
			Mar 15 2024 12:...	[redacted]	[redacted]	Re: Conversation	Outgoing

XDR Pivot Menu

If your Secure Email Threat Defense business is integrated with Cisco XDR you can access the XDR pivot menu from within the message report. For information about integrating with XDR, see XDR.

Authentication Error Codes

The following email authentication failure codes are shown in the UI for SPF, DKIM, and DMARC.

SPF

Error Code	Key	Value
spf_1	No SPF Record	SPF signature validation failed as domain owners have not published any SPF record.
spf_2	IP Mismatch	SPF validation failed as sender IP (1.1.1.1) does not match with the IP list configured in DNS (SPF Record)

Error Code	Key	Value
spf_3	Malformed DNS Record	SPF validation failed as SPF record is malformed (RFC violation)
spf_4	Unsupported Attributes	SPF validation failed as SPF record contains attributes not supported by Secure Email Threat Defense
spf_5	DNS Failure	SPF validation failed as Secure Email Threat Defense could not retrieve SPF records from DNS
spf_6	Sender Domain Retreival Failed	SPF validation failed as Secure Email Threat Defense could not retrieve the Sender domain
spf_7	SPF Soft Fail	SPF validation resulted in a Soft Fail
spf_8	SPF Neutral	SPF validation resulted in a Neutral verdict

DKIM

Error Code	Key	Value
dkim_1	No Verification Keys	DKIM signature validation failed as email is signed whereas domain owners have not published any verification keys
dkim_2	Body Hash Failed | Header Hash Failed	DKIM signature validation failed as email hash does not match with hash generated by domain owners published signing keys
dkim_3	Malformed DKIM Signature	DKIM signature validation failed as signature is malformed (RFC violation)
dkim_4	Signature Expired	DKIM signature validation failed as signature in the email expired (timed out)
dkim_5	Key Malformed	DKIM signature validation failed as Public Key is malformed (RFC violation)
dkim_6	Key Size Mismatch	DKIM signature validation failed as signature key size does not match with Secure Email Threat Defense supported key sizes
dkim_7	DNS Failure	DKIM signature validation failed as Secure Email Threat Defense could not retrieved the DKIM keys from DNS
dkim_8	None	DKIM validation not performed as Email is not signed

Error Code	Key	Value
dkim_9	Sender Domain Retrieval Failed	DKIM validation failed as Secure Email Threat Defense could not retrieve the Sender domain from the email headers

DMARC

Error Code	Key	Value
dmarc_1	No DMARC Record	DMARC signature validation failed as domain owners have not published any DMARC record
dmarc_2	Malformed DNS Record	DMARC validation failed as DMARC record is malformed (RFC violation)
dmarc_3	Sender Domain Retrieval Failed	DMARC validation failed as Secure Email Threat Defense could not retrieve the Sender domain from the email headers
dmarc_4	DNS Failure	DMARC validation failed as Secure Email Threat Defense could not retrieve DMARC records from DNS

dmarc_5	DMARC Failed	spf = “fail”; dkim = “fail”
		spf = “pass”; dmarc_spf_align =“fail”
		dkim = “pass”; dmarc_dkim_align = “fail”

SMTP server will include the following custom header in the outer envelope:

Header	Value (JSON) - Sample

X-CSE-Auth-Failure-Data	{
	"spf": "spf_1",
	"dkim": "dkim_1",
	"dmarc": "dmarc_5",
	"dmarc_failed_reason: "spf=pass; dmarc_spf_align=fail; dkim=fail"
	“dmarc_action” : “quarantine”,
	"spf_ts": 1755751374,
	"dkim_ts": 1755751378,
	"dmarc_ts": 1755751380
	}

Move and Reclassify Messages

Use the Messages page to move or reclassify messages if you think they have been incorrectly classified:

- You can move or reclassify up to 100 messages at a time by changing the number of messages displayed per page.
- To move more than 100 and up to 50, 000 messages, see **Bulk Move and Reclassify Messages**.
- You can also move and reclassify a single message directly from the Verdict & Techniques panel of the Message Report page.

You can also move and reclassify messages using the Remediation and Reclassification API. See the API guide for details https://developer.cisco.com/docs/message-search-api/.

> Reclassifying only affects the verdict on the selected message(s). It does not indicate any change in action on future messages from the selected sender or based on the message content. The message will be queued for review by Cisco Talos. Talos may use the feedback to influence future classifications. For false positive messages, consider adding **Policy Exceptions**.

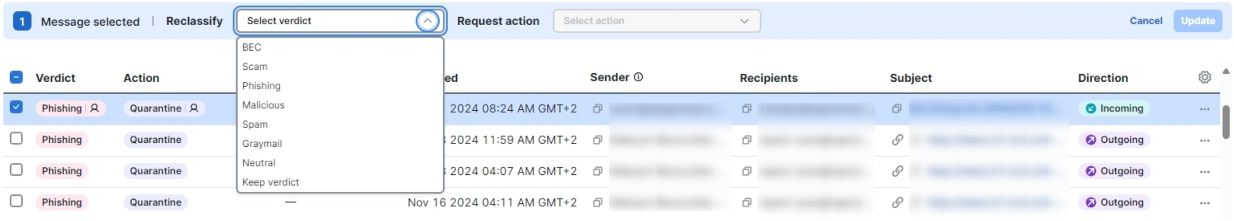
About Hybrid Microsoft Exchange Accounts

Secure Email Threat Defense can act only on mailboxes located in Exchange Online (O365). If you are in the process of migrating your mailboxes from on-premises Exchange to Exchange Online (O365), remediation (move or deletion) will only work for mailboxes located in Exchange Online (O365). You will not be notified that the remediation for on-premises Exchange mailboxes has failed.

Read Remediation Mode

If you are in Read mode, you can reclassify (apply a different verdict to) messages.

1. Select the message(s) you want to reclassify.
2. Select a verdict from the drop-down menu. You can reclassify the messages as **BEC**, **Scam**, **Phishing**, **Malicious**, **Spam**, **Graymail**, or **Neutral** or you can select **Keep verdict**.



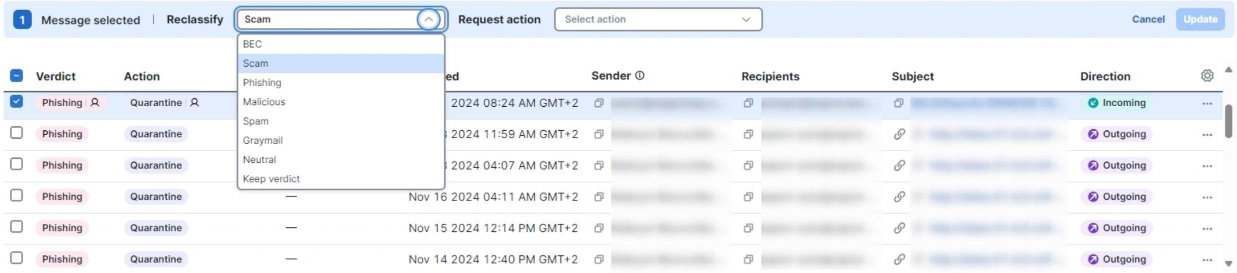
Verdict	Action		ed	Sender	Recipients	Subject	Direction
☑ Phishing	Quarantine		2024 08:24 AM GMT+2	[redacted]	[redacted]	[redacted]	Incoming
□ Phishing	Quarantine		2024 11:59 AM GMT+2	[redacted]	[redacted]	[redacted]	Outgoing
□ Phishing	Quarantine		2024 04:07 AM GMT+2	[redacted]	[redacted]	[redacted]	Outgoing
□ Phishing	Quarantine	—	Nov 16 2024 04:11 AM GMT+2	[redacted]	[redacted]	[redacted]	Outgoing

3. Click **Update** to apply the new classification.

Read/Write Remediation Mode

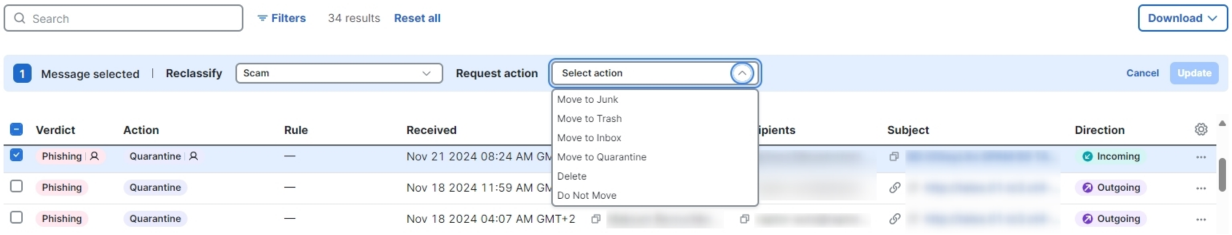
If you are in Read/Write remediation mode, you can move suspicious messages out of user Inboxes and into their Junk or Trash, or to a Quarantine folder they cannot access. Similarly, if you determine a message that was moved to Junk, Trash, or Quarantine is not suspicious, you can move it back to user Inboxes. You can also Delete messages entirely. This process also allows you to reclassify (apply a different verdict to) messages.

1. Select the message(s) you want to move or reclassify.
2. Select a verdict from the Reclassify drop-down menu. You can reclassify the messages as **BEC**, **Scam**, **Phishing**, **Malicious**, **Spam, Graymail**, or **Neutral**, or you can select **Keep verdict**.



Verdict	Action		ed	Sender	Recipients	Subject	Direction
☑ Phishing	Quarantine		2024 08:24 AM GMT+2	[redacted]	[redacted]	[redacted]	Incoming
□ Phishing	Quarantine		2024 11:59 AM GMT+2	[redacted]	[redacted]	[redacted]	Outgoing
□ Phishing	Quarantine		2024 04:07 AM GMT+2	[redacted]	[redacted]	[redacted]	Outgoing
□ Phishing	Quarantine	—	Nov 16 2024 04:11 AM GMT+2	[redacted]	[redacted]	[redacted]	Outgoing
□ Phishing	Quarantine	—	Nov 15 2024 12:14 PM GMT+2	[redacted]	[redacted]	[redacted]	Outgoing
□ Phishing	Quarantine	—	Nov 14 2024 12:40 PM GMT+2	[redacted]	[redacted]	[redacted]	Outgoing

3. Select an action from the Request Action drop-down menu. You can **Move to Junk**, **Move to Trash**, **Move to Inbox**, **Move to Quarantine**, **Delete**, or you can select **Do Not Move**.



Verdict	Action	Rule	Received		ipients	Subject	Direction
☑ Phishing	Quarantine	—	Nov 21 2024 08:24 AM GM		[redacted]	[redacted]	Incoming
□ Phishing	Quarantine	—	Nov 18 2024 11:59 AM GM		[redacted]	[redacted]	Outgoing
□ Phishing	Quarantine	—	Nov 18 2024 04:07 AM GMT+2	[redacted]	[redacted]	[redacted]	Outgoing

4. Click **Update** to apply the new classification and take action on the messages.

If a message has been moved, it is indicated in the **Action** column.

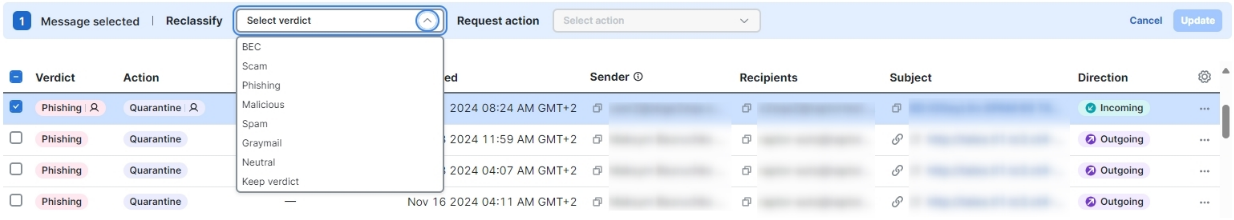
> For outgoing and internal message, the Move to Inbox action moves the message to the Sent folder of the initial sender of the message, instead of to their Inbox.

Delete Messages

Super-admin and admin users can permanently delete messages from mail boxes using the Delete action in the Reclassify/Remediate workflow. Deleted messages are moved to the **recoverableitemspurges** folder. This folder is not accessible to users and Secure Email Threat Defense cannot restore deleted messages to Inboxes.

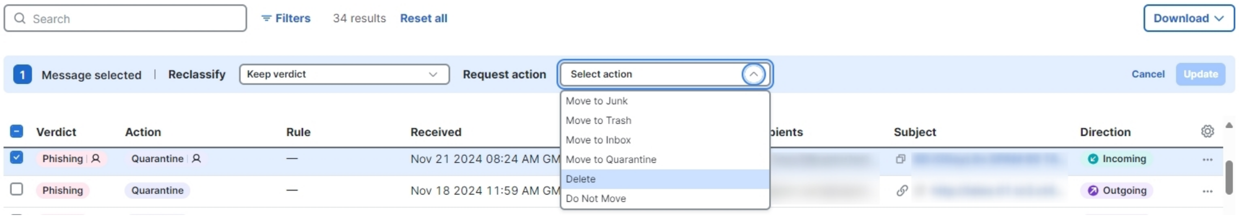
1. Select the message(s) you want to delete.

2. Select a verdict from the Reclassify drop-down menu. You can reclassify the messages as **BEC**, **Scam**, **Phishing**, **Malicious**, **Spam**, **Graymail**, or **Neutral**, or you can select **Keep verdict**.



☐	Verdict	Action	ed	Sender ⓘ	Recipients	Subject	Direction
☑	Phishing	Quarantine	2024 08:24 AM GMT+2	[redacted]	[redacted]	[redacted]	Incoming
☐	Phishing	Quarantine	2024 11:59 AM GMT+2	[redacted]	[redacted]	[redacted]	Outgoing
☐	Phishing	Quarantine	2024 04:07 AM GMT+2	[redacted]	[redacted]	[redacted]	Outgoing
☐	Phishing	Quarantine	Nov 16 2024 04:11 AM GMT+2	[redacted]	[redacted]	[redacted]	Outgoing

3. Select **Delete** from the Request Action drop-down menu.



☐	Verdict	Action	Rule	Received	ients	Subject	Direction
☑	Phishing	Quarantine	—	Nov 21 2024 08:24 AM GM	[redacted]	[redacted]	Incoming
☐	Phishing	Quarantine	—	Nov 18 2024 11:59 AM GM	[redacted]	[redacted]	Outgoing

4. Click **Update** to delete the message(s).

5. A Confirm Deletion dialog indicates that messages cannot be recovered and verifies that you want to continue. Click **Delete** to continue.

Delete is indicated in the **Last Action** column.

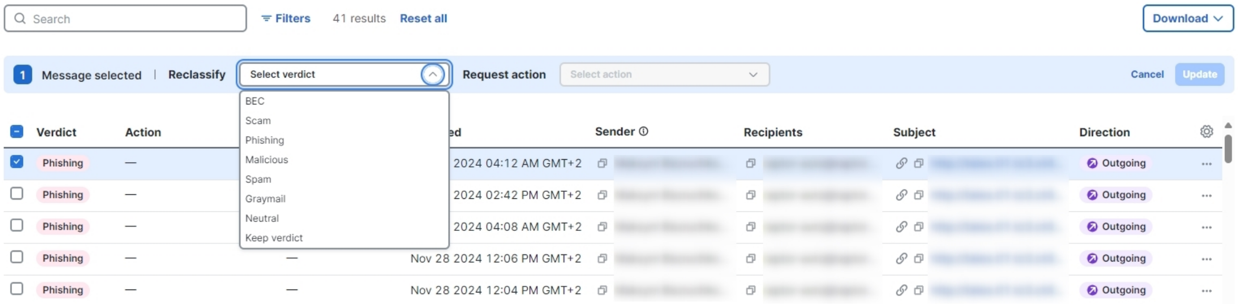
Quarantine Messages

Quarantine folders are created automatically for each mailbox and are hidden from Outlook users. The secret folder name is visible to Super-admin and admin users on the **Administration** > **Business** page. In Outlook, messages in the quarantine folder are automatically purged according to your Deleted Items purge settings. Secure Email Threat Defense cannot restore messages back to user Inboxes after they are purged from the quarantine folder.

To manually move messages to quarantine:

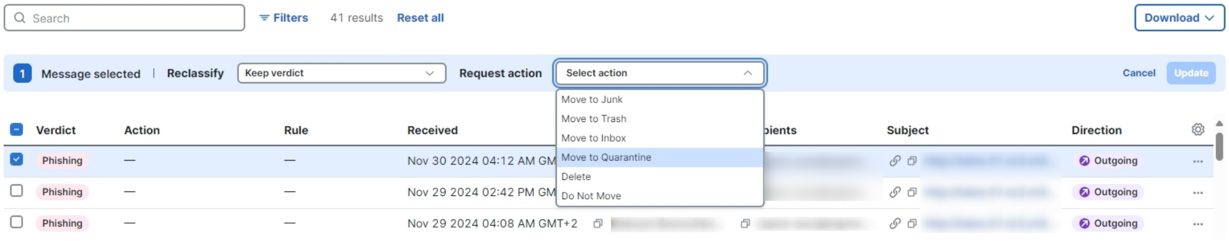
1. Select the message(s) you want to move to quarantine.

2. Select a verdict from the Reclassify drop-down menu. You can reclassify the messages as **BEC**, **Scam**, **Phishing**, **Malicious**, **Spam**, **Graymail**, or **Neutral**, or you can **Keep verdict**.



Verdict	Action		...ed	Sender	Recipients	Subject	Direction
☑ Phishing	—		2024 04:12 AM GMT+2	[redacted]	[redacted]	[redacted]	Outgoing
□ Phishing	—		2024 02:42 PM GMT+2	[redacted]	[redacted]	[redacted]	Outgoing
□ Phishing	—		2024 04:08 AM GMT+2	[redacted]	[redacted]	[redacted]	Outgoing
□ Phishing	—	—	Nov 28 2024 12:06 PM GMT+2	[redacted]	[redacted]	[redacted]	Outgoing
□ Phishing	—	—	Nov 28 2024 12:04 PM GMT+2	[redacted]	[redacted]	[redacted]	Outgoing

3. Select **Move to Quarantine** from the Request Action drop-down menu.



Verdict	Action	Rule	Received	...pients	Subject	Direction
☑ Phishing	—	—	Nov 30 2024 04:12 AM GM	[redacted]	[redacted]	Outgoing
□ Phishing	—	—	Nov 29 2024 02:42 PM GM	[redacted]	[redacted]	Outgoing
□ Phishing	—	—	Nov 29 2024 04:08 AM GMT+2	[redacted]	[redacted]	Outgoing

4. Click **Update** to quarantine the message(s).

Move to Quarantine is indicated in the **Last Action** column.

Understanding Secure Email Threat Defense Labels

Secure Email Threat Defense automatically classifies incoming emails to protect you from various threats. Knowing these labels helps you quickly identify and respond appropriately to potential dangers in your inbox. Consider these definitions when manually reclassifying or remediating messages.

Table 1. Label Classification

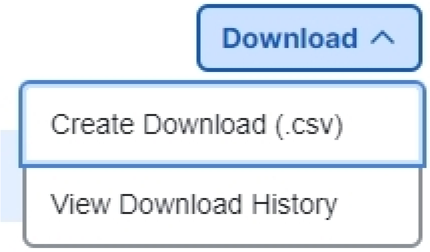
Label	Description	Examples
Spam	These are unsolicited, often irrelevant bulk messages, typically for advertising or spreading non-targeted misinformation. They are generally harmless but unwanted.	An email from a low-reputation journal inviting you to publish, which upon verification, is not listed in reputable academic databases like Web of Science or DOAJ.
BEC (Business Email Compromise)	Highly targeted attacks where senders impersonate colleagues or trusted business contacts (like HR or management) to trick you into revealing sensitive information or taking urgent actions. Always verify unexpected internal requests, especially those asking for financial transfers or	An email appearing to be from your HR department asking you to open a PDF about new vacation plans or scan a QR code, or an urgent request from a "Sales Manager" for an order, where the sender's email address doesn't match the real company domain.

Label	Description	Examples
	confidential data.	
Scam	Fraudulent emails designed to deceive recipients into providing personal information, financial details, or other sensitive data, often by exploiting emotions like excitement or urgency.	A blackmail email demanding cryptocurrency to keep a secret, a "lucky winner" notification for a lottery you never entered, or a fake PayPal payment confirmation with a suspicious transaction ID.
Phishing	Emails disguised as legitimate entities (e.g., your bank, an online service, or even a personal email provider) aiming to steal your login credentials or personal data. These often use deceptive communication, create urgency, and contain links to spoofed websites.	An email asking you to disclose your personal Gmail credentials because your account is "about to be suspended" if you don't verify immediately by clicking a link.
Malicious	Emails crafted with the intent to harm the recipient or achieve unauthorized access, often containing links that lead to dangerous websites.	An email with an embedded malicious link that, if clicked, redirects you to a website which has been identified as harmful; an email with an attachment named `InvoiceID20250237713.exe` or an email containing an SVG HTML Landing attachment designed to install executable files.
Graymail	Emails you have consented to receive at some point (e.g., newsletters, promotional offers, updates from companies) but might now consider unwanted or irrelevant. These are legitimate but not always desired.	A newsletter from a business intelligence software company that you once subscribed to, featuring a *Download Guide* button, but you no longer find it useful.
Neutral	Legitimate, non-threatening emails. These are typically expected communications from known contacts or organizations, containing no suspicious elements, pressure tactics, or requests for sensitive information.	A personal or professional correspondence from a colleague, an update from a subscribed service you still value, or a continuation of an established email thread.

Download Search Results

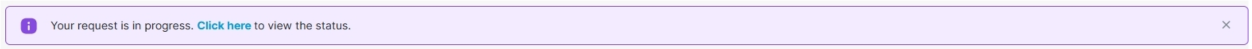
You can download a CSV file of the data for messages in your search results. Downloads are limited to 10,000 messages. Complete the following steps to download your data:

1. Click the Download button and select **Create Download (.csv)**.



A banner indicating that your request is in progress appears.

2. Click the text to be taken to the **Downloads: Messages** page.

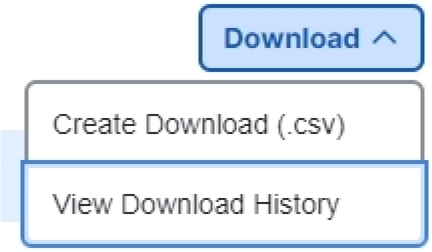


Your request is in progress. Click here to view the status.

3. When your download is ready, download your file by clicking the Download icon under the Actions column.

Download History

Your download history is kept for 90 days. Click the Download button and select **View Download History** to go to the **Downloads: Messages** page.



This page shows you the date range, who requested the download, the date it was initiated, and the status. Download your file by selecting the Download icon under the Actions column.

Downloads

The pages accessible from the **Download** menu in the upper-right corner of the screen allow you to create and manage:

- Search result message data CSVs
- Remediation error log CSVs
- EML download requests

Messages

You can download the search result message data in CSV format if you need to leverage email data for security, compliance, analytical, or management purposes. The CSV organizes the data by the following attributes:

- Message ID
- Verdict (BEC, scam, phishing, malicious, spam, graymail, neutral, or no verdict)
- Last Action (quarantine, junkmail, trash, or inbox)
- Remediation Method (automatic, manual, or API)
- Retrospective Verdict (TRUE or FALSE)
- Received (date and time)
- Display Name
- Sender
- Reply to
- Return Path
- Envelope From
- Sending IP
- Receiving IP
- X-Originating IP
- Recipients
- Subject
- Attachments
- URLs
- Direction (incoming, outgoing, or internal)
- Rule Name
- Rule Type

- Source
- Delivered to
- Envelope to
- Sender Authentication (SPF, DKIM, DMARC pass/fail, reason, and DMARC action (SMTP/Inline message sources only)

You can download message data in two ways:

- From the Messages page, as described in Download Search Results. Use this option if you want to download specific filtered data or data for a longer time period. It will create a CSV file of the data for messages in the current search and filter results.
- From the **Downloads** > **Messages (CSV)** tab, as described below. This is useful if you want to download all message data from a specific time period such as the Last 24 hours, Last 7 days, or a specific day or week.

To create and download a CSV of your message data from the Downloads page:

1. Select **Downloads** > **Messages (CSV)**.
2. Click **Create CSV**.
3. In the dialog that displays, select the date range you want to create a download for, then click **Create CSV**.
4. When your download is ready, download the file by clicking the Download icon under the Actions column.

EML Downloads

Super-admin and admin users can request EML downloads from the expanded message view. Small downloads happen immediately; larger downloads are available from the Downloads page until they are downloaded or for 7 days, whichever comes first. Files can be downloaded one time from the Downloads page. You can reach the Downloads page directly from **Downloads** > **Download EML**.

To request and download an EML file:

1. From the message report, click the **Request EML Download** button. Smaller messages are downloaded immediately.
2. For slower downloads, a banner indicating that your request is in progress appears. Click the text to be taken to the **Downloads: Download EML** page.
3. When your download is ready, download your file by clicking the Download icon under the Actions column.

Remediation Error Log

If a remediation error occurs, a notification is shown under the Notifications (bell icon) menu. The remediation error log allows you to investigate any remediation failures for individual mailboxes. For example, a Move to Trash request could be unsuccessful if the message had already been deleted by the mailbox owner. The remediation error log would show this as Resource is not found.

The remediation error log is a CSV file that organizes the data by the following attributes:

- Request ID
- Timestamp
- User Email ID
- Folder Request
- Mailbox
- Action Type
- Reason

You can request an error log download directly from a notification by expanding the notification and clicking the **Request Download** button.

Alternatively, complete the following steps to create and download a remediation error log:

1. Select **Downloads** > **Remediation Error Log**.
2. Click **Create CSV**.
3. In the dialog that displays, select the date range you want to create a download for, then click **Create CSV**.
4. When your download is ready, download the file by clicking the Download icon under the Actions column.

Insights

In this chapter:

1. Trends
2. Impact Report
3. Blocked Connection Logs

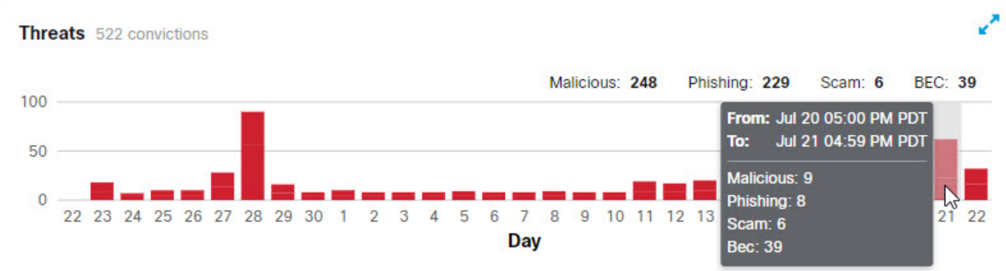
Trends

The Trends page shows graphical information about your email data. View Trends by selecting **Insights** > **Trends**.

- Use the calendar control to show data for a specific Day, Week, or Month.
- Click data of interest in the graphs to be taken to the data details on the Messages page.
- Click legend items to be taken to the relevant data on the Messages page. For example, click Incoming to see all Incoming messages that are currently showing on the chart.
- Download your trend data by clicking the download ⤓ button. The results are exported as a CSV file that includes:
  - an hourly roll-up of the past 90 days of data if you are viewing the last 24 hours or a specific day
  - 24-hour roll-ups of the past 90 days of data if you are viewing the last 30 days
- Print your Trends charts or save as PDF by clicking the print 🖨 button.

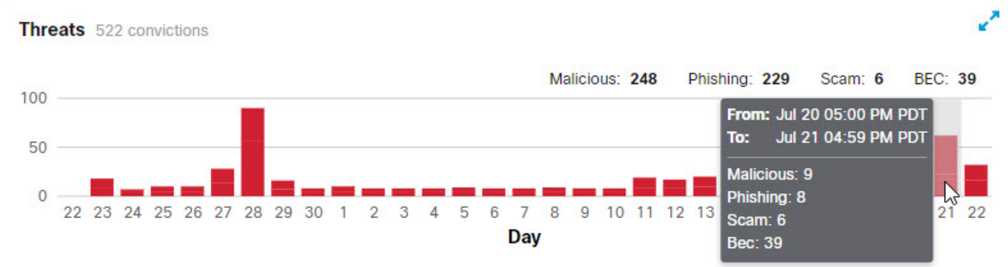
About Timezones

Each bar on a Day chart shows the data for one hour. These charts are based in your browser's local timezone.



Each bar on a Week or Month chart shows the data for one 24-hour day. The day is based on UTC 00:00 through 11:59 p.m. and then converted to your browser's local time.

For example, if you are in Pacific Daylight Time (PDT) UTC−07:00, a bar on a Month chart would show from July 20 5:00 p.m. through July 21 4:59 p.m. Pacific.

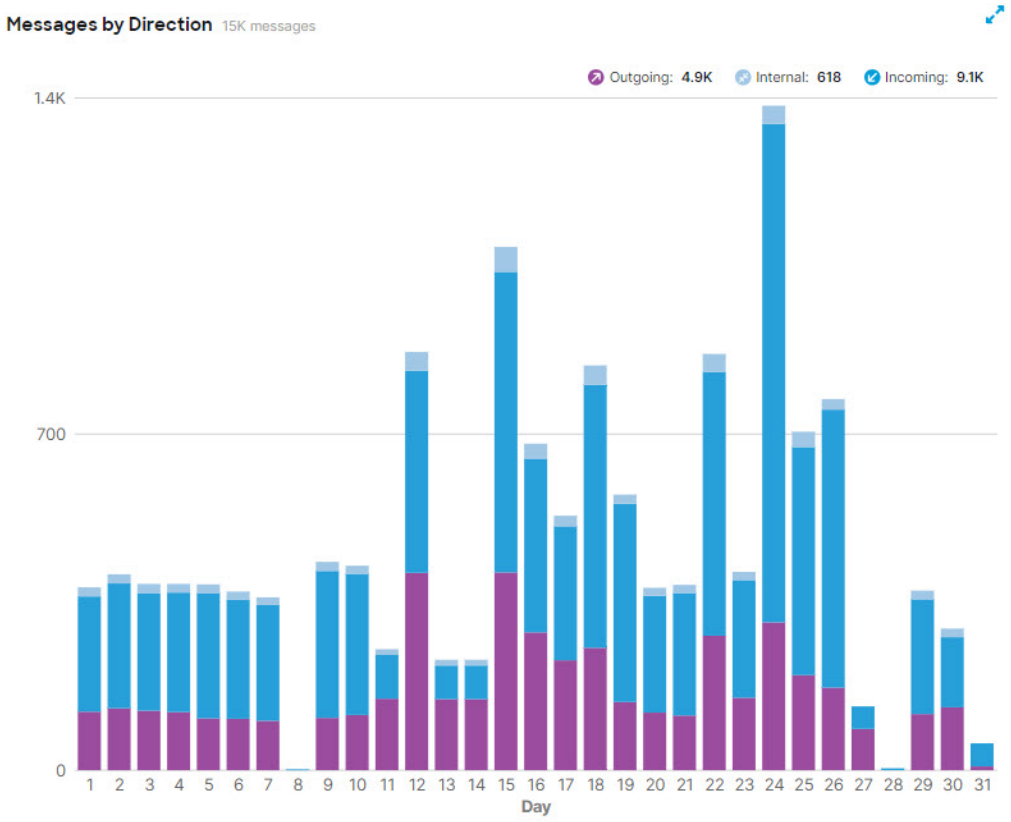


Messages by Direction

The Messages by Direction graph shows your total email traffic. Mail is divided into the following categories:

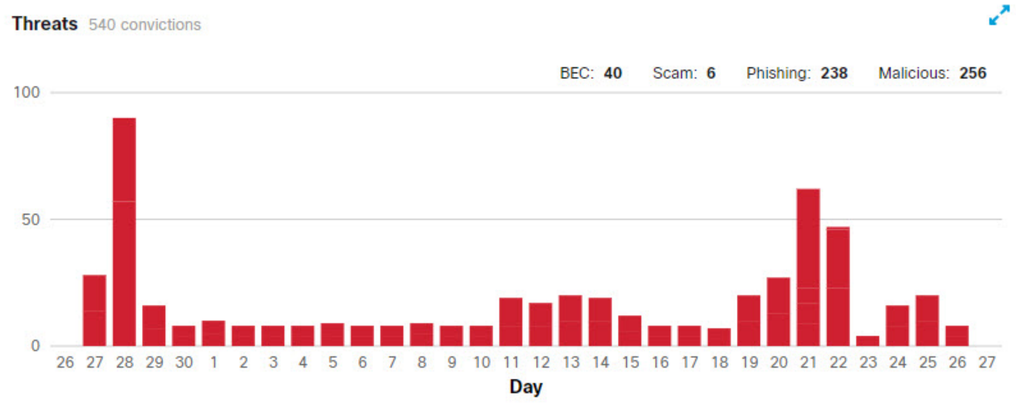
- **Outgoing**: mail sent to recipients outside of your O365 tenant
- **Internal**: mail sent within your O365 tenant
- **Incoming**: mail received from outside your O365 tenant

The legend shows the number of messages in each category.



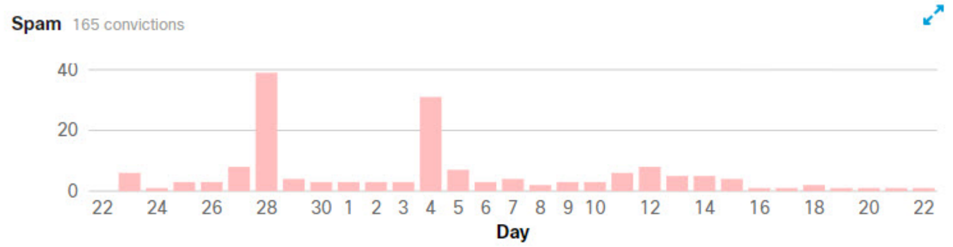
Threats

The Threats graph shows a snapshots of messages that were determined to be threats. This includes BEC, Scam, Phishing, and Malicious. The legend shows the number of messages in each category. Click the data to be taken to the Messages page.



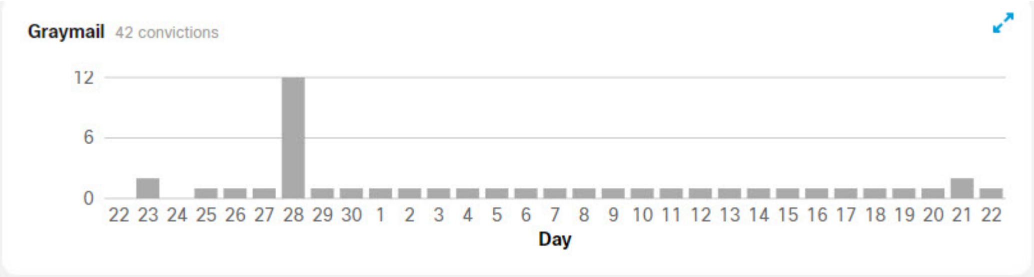
Spam

The Spam graph shows a snapshot of messages that were determined to be Spam. The legend shows the total number of messages determined to be Spam.



Graymail

The Graymail graph shows a snapshot of messages that were determined to be Graymail. The legend shows the total number of messages determined to be Graymail.

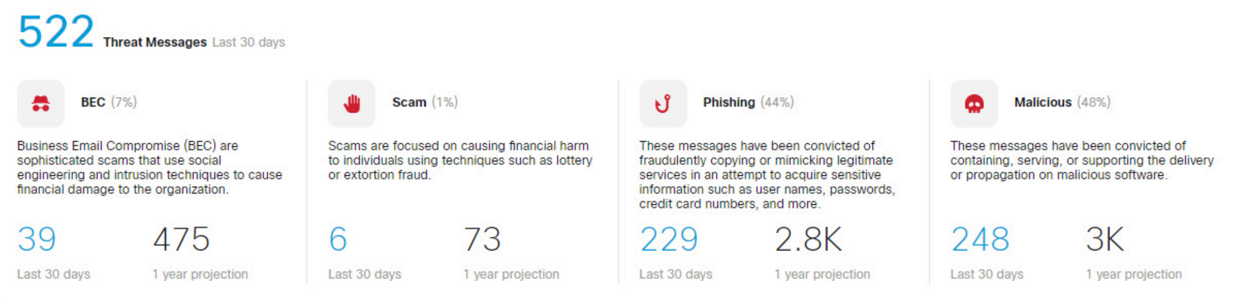


Impact Report

The Impact Report shows the benefits Secure Email Threat Defense provided over the last 30 days. Select **Insights** > **Impact Report** to see the report. Click data of interest in the report to be taken to the data details on the Messages page.

Data shown includes:

- Threat messages caught by Secure Email Threat Defense in the selected 30 day period, and a 1-year projection of this data. The 1-year projection is calculated as the daily average multiplied by 365.



522 **Threat Messages** Last 30 days

BEC (7%)

Business Email Compromise (BEC) are sophisticated scams that use social engineering and intrusion techniques to cause financial damage to the organization.

39 Last 30 days

475 1 year projection

Scam (1%)

Scams are focused on causing financial harm to individuals using techniques such as lottery or extortion fraud.

6 Last 30 days

73 1 year projection

Phishing (44%)

These messages have been convicted of fraudulently copying or mimicking legitimate services in an attempt to acquire sensitive information such as user names, passwords, credit card numbers, and more.

229 Last 30 days

2.8K 1 year projection

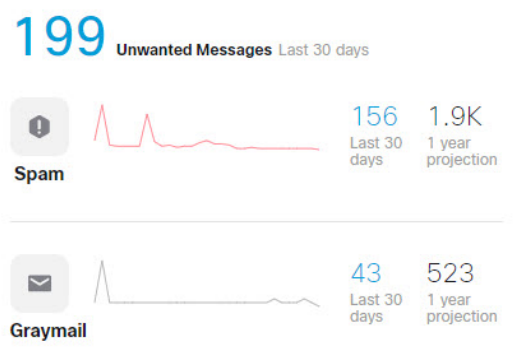
Malicious (48%)

These messages have been convicted of containing, serving, or supporting the delivery or propagation on malicious software.

248 Last 30 days

3K 1 year projection

- Unwanted Messages. This chart shows Spam and Graymail in the selected 30 day period, and a 1-year projection of this data. The 1-year projection is calculated as the daily average multiplied by 365.



199 **Unwanted Messages** Last 30 days

Spam

156 Last 30 days

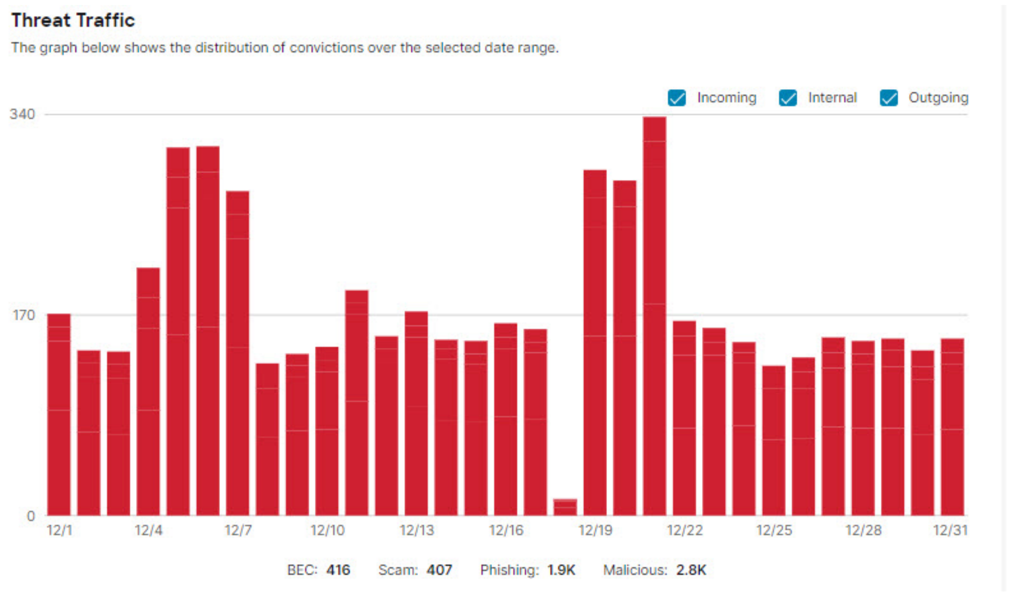
1.9K 1 year projection

Graymail

43 Last 30 days

523 1 year projection

- Threat Traffic. This chart shows convictions over the selected 30 day period. You can filter this chart by direction.

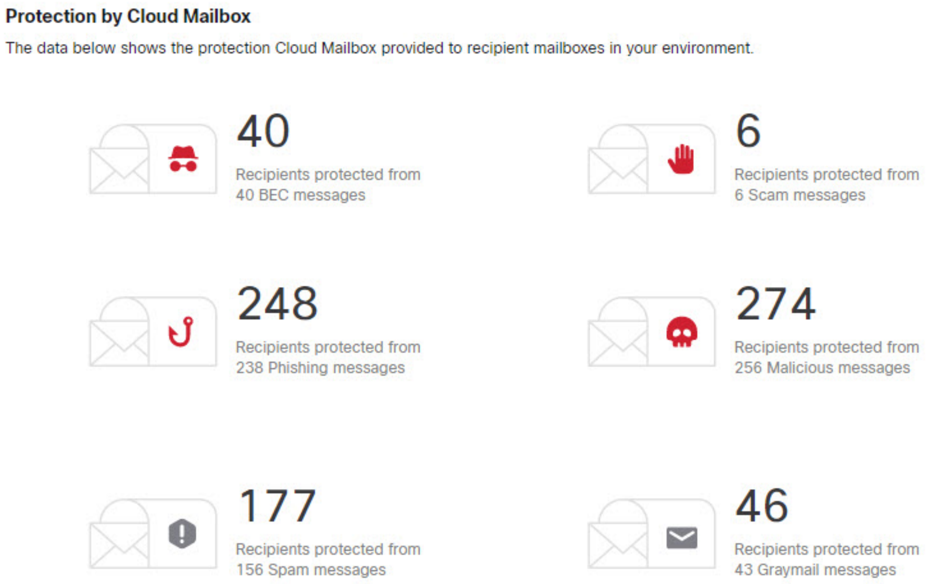


Threat Traffic

The graph below shows the distribution of convictions over the selected date range.

BEC: **416** Scam: **407** Phishing: **1.9K** Malicious: **2.8K**

- Protection by Secure Email Threat Defense. This chart shows the protection Secure Email Threat Defense provided to recipient mailboxes in your environment.



Protection by Cloud Mailbox

The data below shows the protection Cloud Mailbox provided to recipient mailboxes in your environment.

40
Recipients protected from
40 BEC messages

6
Recipients protected from
6 Scam messages

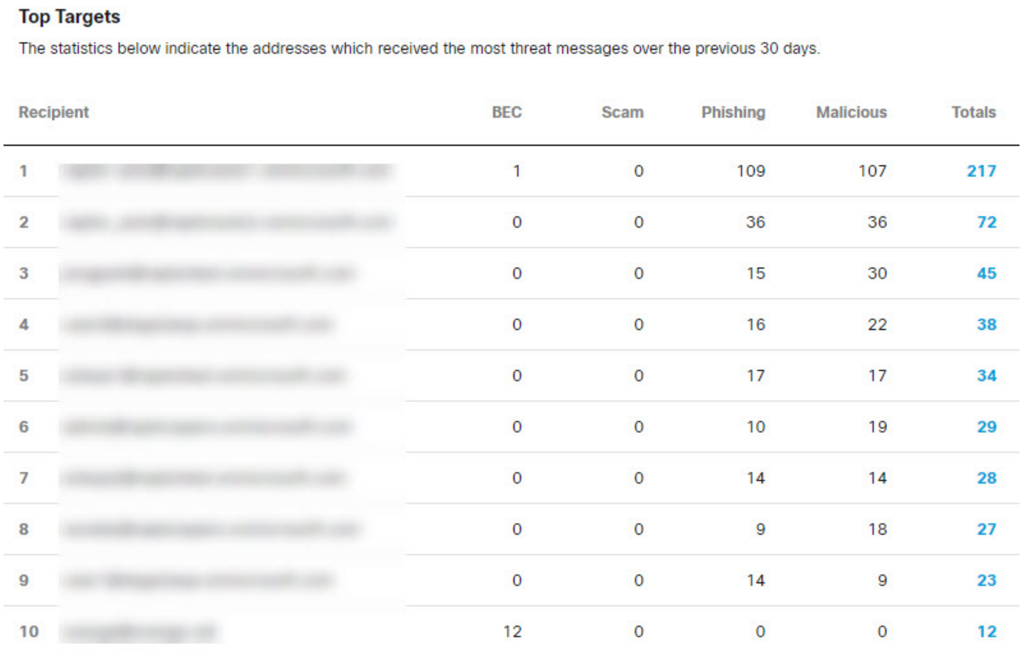
248
Recipients protected from
238 Phishing messages

274
Recipients protected from
256 Malicious messages

177
Recipients protected from
156 Spam messages

46
Recipients protected from
43 Graymail messages

- Top Targets. This chart shows the top ten internal targets of threat messages over the selected 30 day period.

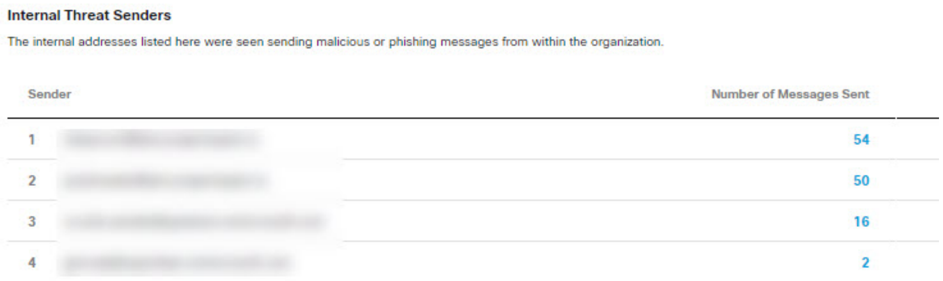


Top Targets

The statistics below indicate the addresses which received the most threat messages over the previous 30 days.

	Recipient	BEC	Scam	Phishing	Malicious	Totals
1	[redacted]	1	0	109	107	217
2	[redacted]	0	0	36	36	72
3	[redacted]	0	0	15	30	45
4	[redacted]	0	0	16	22	38
5	[redacted]	0	0	17	17	34
6	[redacted]	0	0	10	19	29
7	[redacted]	0	0	14	14	28
8	[redacted]	0	0	9	18	27
9	[redacted]	0	0	14	9	23
10	[redacted]	12	0	0	0	12

- Internal Threat Senders. This chart shows the top ten internal senders of threat messages.



Internal Threat Senders

The internal addresses listed here were seen sending malicious or phishing messages from within the organization.

	Sender	Number of Messages Sent
1	[redacted]	54
2	[redacted]	50
3	[redacted]	16
4	[redacted]	2

Blocked Connection Logs

> Connection handling and Blocked connection logs are applicable to SMTP/Inline message sources. SMTP message source configurations are available for customers with a Secure Email Threat Defense advantage license.

The Blocked Connection Logs report at **Insights** > **Blocked Connection Logs** shows a graphical representation of connections that have been blocked based on IP Reputation and Block Lists.

You can export the Blocked Connections Logs data to CSV by clicking the **Export** button. Blocked Connection data is also shown in the Audit Log CSV export, accessible from **Administration** > **Business** > **Audit Logs**.

High Impact Personnel List

Important personnel, such as members of executive leadership teams, are at risk of being impersonated in an attempt to compromise other targets. The high impact personnel list helps Secure Email Threat Defense defend your organization from impersonation attacks.

Access the high impact personnel list from **Administration** > **High Impact Personnel**.

Admins should create a list of up to 500 people to be sent to Cisco Talos for higher scrutiny on Display Name and Sender Email Address. Deviations from the configured information for an individual will be identified as a Technique in the Verdict Details panel of convicted messages.

Add a User to the High Impact Personnel List

Complete the following steps to add a user to the high impact personnel list:

1. Select **Administration** > **High Impact Personnel**.
2. Click **New HIP contact**.
3. Enter the user's information. First Name, Last Name, and Email Address are required.
4. Click **Save** to finish adding the user to the list.

Update a User's Information in the High Impact Personnel List

Complete the following steps to edit a user's information in the high impact personnel list:

1. Select **Administration** > **High Impact Personnel**.
2. In the furthest right column, click the **Edit** (pencil) button on the row of the user whose information you want to update.
3. Update the user's information as needed. First Name, Last Name, and Email Address are required.
4. Click **Save** to finish editing the user's information.

Remove a User from the High Impact Personnel List

Complete the following steps to remove a user from the high impact personnel list:

1. Select **Administration** > **High Impact Personnel**.
2. In the furthest right column, click the **Delete** button on the row of the user you want to delete.
3. Click **Delete** in the Confirm Removal dialog to complete the action.

Manage Users

Manage your user accounts from the **Administration** > **Users** page.

Secure Email Threat Defense uses Cisco Security Cloud Sign On (formerly SecureX sign-on) for user authentication management. For information on Security Cloud Sign On, see https://cisco.com/go/securesignon.

> If you are an existing Cisco XDR, Cisco Secure Malware Analytics (formerly Threat Grid), or Cisco Secure Endpoint (formerly AMP) customer, be sure to sign in with your existing Security Cloud Sign On credentials. If you are not an existing user, you must create a new Security Cloud Sign On account

Although Security Cloud Sign On allows you to sign on with other types of accounts, we recommend using a Security Cloud Sign On account to keep your Cisco security product accounts connected.

Multi-Account Access

You can access multiple Secure Email Threat Defense instances using the same Security Cloud Sign On account. This makes it easier to keep track of each instance without having to log out and log back in using a separate Security Cloud Sign On account.

Add a user to additional Secure Email Threat Defense instances by following the steps in **Create a New User**. Accounts using the same Security Cloud Sign On account will be available from their User menu. Note that this access is limited to Secure Email Threat Defense instances in the same region (North America, Europe, Australia, or India).

User Roles

Role-based access control (RBAC) allows you to have users with different levels of control or access within the application. Secure Email Threat Defense users can be created in the roles described in the following table.

User Roles

Role	Description
super-admin	These users have access to all features in Secure Email Threat Defense. They can alter settings and policies, reclassify and remediate messages, download EML files, and view email message previews.
admin	These users have all the capabilities of super-admins, except they cannot create, edit, or delete super-admin or admin users.
analyst	These users can use the search and insight capabilities. They can reclassify and remediate

Role	Description
	messages, but cannot delete messages from user mailboxes. They cannot make changes to the account setup or policies or create, edit, or delete new users. They also cannot download EML files or view email message previews.
read-only	These users can use the search and insight capabilities. They cannot reclassify or remediate messages, make changes to the account setup or policies, or create new users. They also cannot download EML files or view email message previews.

Access to Features by Role

Feature Group	Feature	Role
Administration	Add/Edit Users	■ super-admin ■ admin
	Create/Edit/Delete Admins	super-admin
Business	Toggle Google Analytics	■ super-admin ■ admin
	View Notification Email	■ super-admin ■ admin
	Edit Retro Notification Email	■ super-admin ■ admin
	Download Audit Logs	■ super-admin ■ admin ■ analyst ■ read-only
	View Quarantine Folder	■ super-admin ■ admin
	View Notifications	■ super-

Feature Group	Feature	Role
		admin admin analyst read-only
Policy	Edit Policy	super-admin admin
	Import Domains	super-admin admin
	Modify Message Rules	super-admin admin analyst
Search	Search from Home Page	super-admin admin analyst read-only
Messages	View Expansion	super-admin admin analyst read-only
	View Reports	super-admin admin analyst read-only
	Download EML	super-admin admin

Feature Group	Feature	Role
	View Email Preview	- super-admin - admin
Reclassify and Remediate	Reclassify	- super-admin - admin - analyst
	Move Message	- super-admin - admin - analyst
	Quarantine Message	- super-admin - admin - analyst
	Delete Message	- super-admin - admin
	View Remediation Error Log	- super-admin - admin - analyst - read-only
Cisco XDR	Authorize Dashboard	- super-admin - admin
	Authorize Ribbon	- super-admin - admin - analyst - read-only

Feature Group	Feature	Role
API	Access API Tab	super-admin admin
	Access API Key	super-admin admin
	Generate API Credentials	super-admin admin

Create a New User

Complete the following steps to create a new user:

1. Select **Administration** > **Users**.
2. Click **Add New User**.
3. Enter the user's credentials, select a role, then click **Create**.

> ℹ The user's email address *must* match the one they use for their Security Cloud Sign On account.

The user receives an email with the subject **Welcome to Cisco Secure Email Threat Defense**. They must follow the directions in the email to set up a Security Cloud Sign On account (if they do not already have one) and log in.

Edit a User

You can update a user's role. You cannot edit a user's email address. If a user changes their name, they must update it in their Security Cloud Sign On account.

To edit a user's role:

1. Select **Administration** > **Users**.
2. Click the pencil under the Action column.
3. In the Edit User dialog, select a new role for the user, then click **Save changes**.

Delete a User

Complete the following steps to delete a user:

1. Select **Administration** > **Users**.
2. Click the X icon under the Action column.
3. Click **Delete** in the Confirm Deletion dialog to complete the action.

A status message shows the deletion is complete. This deletes the user’s account from Secure Email Threat Defense, but does not delete their Security Cloud Sign On account. If you want to delete a user from multiple Secure Email Threat Defense instances, you must complete these steps for each instance.

User Settings

Settings for individual user profiles are accessible from **User** (profile icon) > **User Settings**.

Details

The Details section includes your user name, role, and organization.

Preferences

The Preferences section includes your XDR Ribbon authorization and theme appearance settings.

XDR Ribbon

Secure Email Threat Defense is integrated with Cisco XDR ribbon. The ribbon allows you to navigate between Cisco security products, access casebook, search observables, and view incidents. XDR ribbon is authorized per user. For more information, see **Cisco XDR**.

Themes

You can choose to view Secure Email Threat Defense with a light or dark background. To switch the mode, go to **User** (profile icon)> **User Settings** > **Preferences** > **Theme**. Images in this guide are usually shown in the light theme.

Administration Settings

The administration settings described in this section are accessible from **Administration** > **Business**.

Account

The Account section shows the following:

- Microsoft 365 tenant ID
- Journal Address
- Business ID
- Quarantine Folder ID
- Support Subscription ID

License

The License section shows the following:

- License Type
- Seat Count
- Start Date (for standalone businesses that are not part of a Suite)
- End Date (for standalone businesses that are not part of a Suite)

Preferences

The Preferences section includes your Notification Email address, access to Audit Logs, your Google Analytics settings, and your business-level Cisco XDR integration authorization.

Notification Emails

The notification email address is the address Secure Email Threat Defense sends notification emails to. For example, we may send notifications about updates to the system, new features, scheduled maintenance, and so on. This is initially set to the email address of your first user.

Retrospective Verdicts

You cab choose to receive notifications for retrospective verdicts to your notification email address by selecting the **Send Notifications for Retrospective Verdicts** checkbox. An email will be sent when a retrospective verdict is applied to messages.

User Management Actions

You can choose to receive notifications for user management actions at the second email address in the Preferences section. User management actions include changes to users such as a user being created, updated, or deleted.

Audit Logs

Audit logs keep track of all security events, trace security incidents, and visualize their impact. You can export the audit logs for the last three months (separately for each month) in a CSV file. To download audit logs, select a date range from the drop-down and then click **Download CSV**. The CSV provides information on the event category, time and date, action performed, user email and IP, and event status and metadata.

Google Analytics

Google Analytics is initially enabled or disabled when you set up Secure Email Threat Defense and accept the Terms and Conditions. When enabled, Cisco collects non-personally-identifiable usage data, including but not limited to sender, recipient, subject, and URLs, and may share that data with Google Analytics. This data allows us to better understand the way Secure Email Threat Defense meets your needs.

Cisco XDR

Secure Email Threat Defense is integrated with Cisco XDR. XDR allows you to see Secure Email Threat Defense information alongside data from your other Cisco security products. For more information on this setting, see **XDR**.

Message Rules

> The rules in this chapter are for Journal traffic sources only. Equivalent rules for SMTP/Inline traffic sources can be created on the Configuration pages. See Configuration Settings for more information.

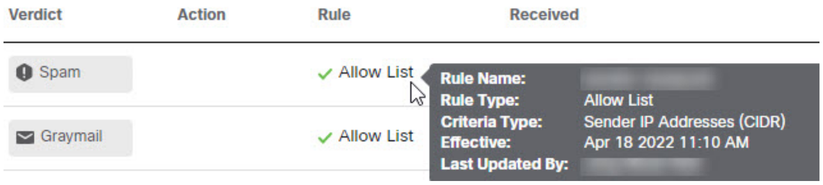
> **Message rules are deprecated and will be removed in a future release**. Your rules are still available and functioning, but you cannot add new rules.
> You should recreate any Message Rule functionality using the new Policy exceptions rules under **Configuration** > **Policy settings**. Once your rules are migrated, Policy exceptions will take precedence over message rules. For information on creating Policy exceptions, see Policy Exceptions.

Message rules allow you to specify that some types of messages should not be remediated or scanned.

> Allow List and Verdict Override rules are not available for businesses in No Authentication mode.
> Bypass Analysis rules have been renamed and migrated to **Global settings** > **Message bypass rules**.

Create and manage your message rules from the **Administration** > **Message Rules** page.

Message bypass rules take precedence over Allow List and Verdict Override rules. If a message is affected by a rule, it is indicated in the Rule column of the Messages page. Hover your cursor over the item in the Rule column to see which rule was applied.



Verdict	Action	Rule	Received
Spam		✓ Allow List	
Graymail		✓ Allow List	

Rule Name: [redacted]
Rule Type: Allow List
Criteria Type: Sender IP Addresses (CIDR)
Effective: Apr 18 2022 11:10 AM
Last Updated By: [redacted]

> Rules do not automatically apply to sub-domains. Domains are matched *exactly* as indicated in a rule.

Allow List Rules

Allow List rules allow you to prevent remediation of Threat, Spam, and/or Graymail messages from specific sender email addresses, sender domains, or sender IP addresses. Messages will still be analyzed but auto-remediation will not be applied. For example, if Secure Email Threat Defense determines items from a certain sender are Spam, but you want to keep the items in user Inboxes, you can create an Allow List rule to override any policy that would remediate such messages. An Allow List rule acts an exception to your overall policy settings. Messages that match an Allow List rule still appear on the Impact report.

Allow List rules:

- Apply to Threats, Spam, and/or Graymail.
- Specify allowed sender email addresses, sender domains, or sender IP addresses (IPv4 or CIDR block).
- Can have up to 50 criteria per rule. That is, 50 email addresses, domains, or addresses.

There is a limit of 20 active rules. Rules can be deactivated or deleted.

Verdict Override Rules

Verdict Override rules allow you to override Threat, Spam, and/or Graymail verdicts that match the criteria specified by the rule. Messages are marked with a Neutral verdict and are not remediated. Messages where the verdict was overridden do not appear on the Impact report.

Verdict Override rules:

- Apply to Threats, Spam, and/or Graymail.
- Specify allowed sender email addresses, sender domains, or sender IP addresses (IPv4 or CIDR block).
- Can have up to 50 criteria per rule. That is, 50 email addresses, domains, or IP addresses.

There is a limit of 20 active rules. Rules can be deactivated or deleted.

Add Message Rules

> **Message rules are deprecated and will be removed in a future release**. Your rules are still available and functioning, but you cannot create new rules.
> You should recreate any Message Rule functionality using the new Policy exceptions rules under **Configuration** > **Policy settings**. Once your rules are migrated, Policy exceptions will take precedence over message rules. For information on creating Policy exceptions, see **Policy Exceptions**.

The steps for adding message rules differ slightly depending on the category of rule.

Add a New Allow List or Verdict Override Rule

Complete the following steps to create a new rule:

1. Select **Administration** > **Message Rules**.
2. Select the category of rule you want to create: **Allow List** or **Verdict Override**.
3. Click the **Add New Rule** button.
4. Create a rule name. Each rule must have a unique name.

5. Select a criteria type. You can select Sender Email, Sender Domain, Sender IP Addresses (IPv4), or Sender IP Addresses (CIDR).
6. Enter the items you want to allow or override, separated by commas.
7. Select Spam, Graymail, and/or Threats, depending on which verdicts you want to allow.
8. Click **Submit** to finish creating the rule.

Your rule is added to the list. It may take up to 20 minutes for the change to take effect.

Edit a Rule

> **Message rules are deprecated and will be removed in a future release**. Your rules are still available and functioning, but you cannot add new rules.
> You should recreate any Message Rule functionality using the new Policy exceptions rules under **Configuration** > **Policy settings**. Once your rules are migrated, Policy exceptions will take precedence over message rules. For information on creating Policy exceptions, see Policy Exceptions.

Note that only enabled rules can be edited. To edit a rule:

1. Select **Administration** > **Message Rules**.
2. Select the type of rule you want to edit.
3. Under the Actions column, click the pencil icon next to the rule you want to edit.
4. Make your desired changes, then click **Save Changes**.

Your rule is updated. It may take up to 20 minutes for the change to take effect.

Enable or Disable a Rule

To enable or disable an existing rule:

1. Select **Administration** > **Message Rules**.
2. Select the type of rule you want to enable or disable.
3. Under the Actions column, click the enable or disable icon next to the rule you want to change the status of.

The status of your rule is updated. It may take up to 20 minutes for the change to take effect.

Delete a Rule

To delete a rule:

1. Select **Administration** > **Message Rules**.
2. Select the type of rule you want to delete.

3. Under the Actions column, click the delete icon next to the rule you want to delete.

Your rule is deleted.

Microsoft Allow Lists and Safe Senders

Secure Email Threat Defense honors senders and domains added to your spam filter allow lists in Microsoft 365 for Spam and Graymail messages. MS Allow lists are honored for BEC and Scam verdicts but not for Malicious or Phishing verdicts. For more information, see **Secure Email Threat Defense and Microsoft 365**.

Microsoft Allow lists are not always honored by Secure Email Threat Defense if your organization allows individual users to configure allow lists in their mailbox and a message happens to fall in a user’s allow list. If you want Secure Email Threat Defense to honor these settings, deselect the **Apply policy to Microsoft Safe Sender messages** check box on the **Configuration** > **Global settings** > **Unwanted message analysis** panel. Safe Sender flags are respected for Spam and Graymail verdicts, but are not respected for Threat verdicts. That is, Safe Sender messages with Spam or Graymail verdicts will not be remediated.

Cisco XDR

Cisco XDR connects Cisco security products into an integrated platform. Secure Email Threat Defense is integrated with Cisco XDR and Cisco XDR ribbon.

- XDR allows you to view and act on Secure Email Threat Defense information alongside data from your other Cisco security products.
- XDR ribbon allows you to navigate between Cisco security products, access casebook, search observables, and view incidents.

For details on XDR not provided in this document, see the Cisco XDR documentation: https://docs.xdr.security.cisco.com/

XDR

Secure Email Threat Defense provides the following tiles that can be viewed in a Cisco XDR dashboard:

- Messages by Direction: Shows your total email traffic by direction. Mail is divided into Outgoing, Internal, and Incoming.
- Threats: Shows a snapshot of messages that were determined to be BEC, Scam, Phishing, or Malicious.
- Spam: Shows a snapshot of messages that were determined to be Spam.
- Graymail: Shows a snapshot of messages that were determined to be Graymail.

For information on the XDR dashboard, see the Cisco XDR documentation: https://docs.xdr.security.cisco.com/

Authorize Cisco XDR for Secure Email Threat Defense

Before you can authorize Cisco XDR for Secure Email Threat Defense, you must have a Cisco XDR account and be part of a Cisco XDR organization. For more information, see the Cisco XDR documentation: https://docs.xdr.security.cisco.com/

> A Secure Email Threat Defense account can only be integrated with one Cisco XDR organization at a time.

Secure Email Threat Defense super-admin and admin users can authorize the Cisco XDR module for their Secure Email Threat Defense instance:

1. Select **Administration** > **Business**.
2. Under **Preferences** > **Extended Detection and Response**, click **Authorize XDR Integration**.
3. Complete the authorization flow.

A banner appears, stating that XDR configuration was successful.

You can now add Secure Email Threat Defense tiles to your XDR dashboard. For information on how to do this, see the Cisco XDR documentation: https://docs.xdr.security.cisco.com/Content/Control-Center/configure-dashboards.htm

Revoke XDR Authorization for Secure Email Threat Defense

> ⓘ Any super-admin or admin user can perform this task. It does not have to be performed by the user who authorized XDR for the Secure Email Threat Defense instance.

To revoke XDR authorization:

1. Select **Administration** > **Business**.
2. Under **Preferences** > **Extended Detection and Response**, click **Revoke Authorization**.

A banner appears, stating that XDR configuration was successfully updated.

XDR Ribbon

The XDR ribbon is located in the lower portion of the page, and persists as you move between Secure Email Threat Defense and other Cisco security products in your environment. Any Secure Email Threat Defense user can authorize the XDR Ribbon for their use. Use the ribbon to navigate between your Cisco security applications, access casebook, search observables, and view incidents.

For information on XDR Ribbon, see the Cisco XDR documentation: https://docs.xdr.security.cisco.com/Content/Ribbon/ribbon.htm

Pivot Menu

When you authorize the ribbon, XDR pivot menus are added within the Secure Email Threat Defense message report. These menus give you a central point of access to additional information about each observable, depending on which Cisco security products you have purchased.

Similarly, Secure Email Threat Defense’s integration with XDR allows you to use the pivot menu to access Secure Email Threat Defense from XDR. Observables you can pivot from include:

- Email Address
- Email Message ID
- Email Subject
- File Name
- Sender IP

  - SHA 256
  - URL

Use the pivot menu to:

- Quarantine messages with a specific observable directly from the pivot menu. Items quarantined in this way indicate in Secure Email Threat Defense that they were manually remediated using XDR/by an XDR user.

  > ℹ Quarantine from the pivot menu is limited to 100 messages.

- Move the messages you quarantined back to the inbox.

  > ℹ Moving from quarantine to the inbox is also limited to 100 messages.

- Initiate a search in Secure Email Threat Defense.

For more information on XDR pivot menus, see the XDR documentation: https://docs.xdr.security.cisco.com/Content/pivot-menu.htm

Authorize XDR Ribbon

XDR ribbon is authorized at the user level. You can authorize the ribbon from within the ribbon or from the User Preferences menu.

> ℹ Your XDR account needs to be activated before you can authorize the ribbon. You can do this by following the instructions in XDR or by integrating any other modules in XDR.

Authorize from within XDR Ribbon

To authorize your XDR ribbon from within the ribbon:

1. Click **Get XDR** in the XDR ribbon.
2. In the Grant Application Access dialog, click **Authorize Secure Email Threat Defense Ribbon**.

Your XDR ribbon is now authorized. A banner appears, stating that XDR configuration was successfully updated.

Authorize from Secure Email Threat Defense User Settings

To authorize your XDR ribbon from the User Settings menu:

1. Select **User** (profile icon) > **User Settings**.
2. Under **Preferences** > **XDR Ribbon**, click **Authorize XDR Ribbon**.

3. In the Grant Application Access dialog, click **Authorize Cisco Secure Email Threat Defense Ribbon**.

Your XDR ribbon is now authorized. A banner appears, stating that XDR configuration was successfully updated.

Revoke XDR Ribbon Authorization

XDR ribbon is authorized at the user level. You can revoke authorization from within the ribbon or from the User Preferences menu.

Revoke Authorization from within XDR Ribbon

To revoke your XDR ribbon authorization from within the ribbon,

1. Select **Settings** > **Authorization** > **Revoke** in the XDR ribbon.
2. In the Revoke dialog, click **Confirm**.

XDR ribbon is no longer authorized for your Secure Email Threat Defense user account.

Revoke Authorization from Secure Email Threat Defense User Settings

To revoke your XDR ribbon authorization from the User Settings menu:

1. Select **User** (profile icon) > **User Settings**.
2. Under **Preferences** > **XDR Ribbon**, click **Revoke Authorization**.

XDR ribbon is no longer authorized for your Secure Email Threat Defense user account. A banner appears, stating that XDR configuration was successfully updated.

API

The Secure Email Threat Defense API allows you to programmatically access and consume data in a secure and scalable manner. For more information, see the API documentation https://developer.cisco.com/docs/message-search-api/.

Cisco Security Cloud App for Splunk

Cisco Secure Email Threat Defense integrates with Splunk through the Cisco Security Cloud App, providing a centralized platform for monitoring and analysis. To configure the integration between Secure Email Threat Defense and Splunk, see the Cisco Security Cloud App for Splunk User Guide.

Deactivate Secure Email Threat Defense

This chapter contains information on how to deactivate Secure Email Threat Defense for:

1. Message Source: Microsoft 365
2. Message Source: Gateway

Message Source: Microsoft 365

To deactivate Secure Email Threat Defense when you have Microsoft as your message source, there are two main tasks:

1. Delete your Secure Email Threat Defense journal entry from Microsoft 365 Admin Center
2. Delete the Secure Email Threat Defense application from your Microsoft Azure tenant

Delete Your Secure Email Threat Defense Journal Rule

To delete your Secure Email Threat Defense journal rule:

1. Go to your Microsoft 365 Admin Center https://admin.microsoft.com/AdminPortal/Home.
2. Navigate to **Admin centers** > **Compliance** > **Data lifecycle management** > **Exchange (legacy)** > **Journal rules**.
3. Select the Secure Email Threat Defense journal rule, then click **Delete**. Select **Yes** to confirm you want to delete the journal rule.

Delete the Secure Email Threat Defense Application from Azure

To delete the Secure Email Threat Defense application from Azure:

Go to portal.azure.com.

1. Search for and select **Enterprise applications**.
2. If you are using an older view in Azure, this may be called **App registrations**.
3. Locate and select the **Cisco Secure Email Threat Defense** and/or **Cisco Secure Email Threat Defense (Read Only)** application.
4. In the left pane, select **Properties**.
5. Click the **Delete** button, then select **Yes** to confirm you want to delete the Secure Email Threat Defense app.

Message Source: Gateway

To deactivate Secure Email Threat Defense when you are using a Gateway as your message source, there are two main tasks:

- Configure your Gateway to stop sending messages to Secure Email Threat Defense
- Delete the Secure Email Threat Defense application from your Microsoft Azure tenant (not necessary for No Authentication mode)

Configure your Gateway to Stop Sending Messages

To configure your Gateway to stop sending messages to Secure Email Threat Defense:

1. In your Secure Email Cloud Gateway console, go to **Security Services** > **Threat Defense Connector**.
2. Set **Threat Defense Connector** to **Disabled**.

Delete the Secure Email Threat Defense Application from Azure

To delete the Secure Email Threat Defense application from Azure:

1. Go to portal.azure.com.
2. Search for and select **Enterprise applications**.

   If you are using an older view in Azure, this may be called **App registrations**.
3. Locate and select the **Cisco Secure Email Threat Defense** and/or **Cisco Secure Email Threat Defense (Read Only)** application.
4. In the left pane, select **Properties**.
5. Click the **Delete** button, then select **Yes** to confirm you want to delete the Secure Email Threat Defense app.

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: http://www.cisco.com/c/en/us/support/index.html
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Copyright Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html.