Cisco Secure Email Threat Defense User Guide

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.

Set Up Secure Email Threat Defense

Secure Email Threat Defense setup includes the following:

1. Sign-in to Your Account, page 11
2. Indicate if you have a Secure Email Gateway (SEG), page 11
3. Select Your Message Source, Visibility and Remediation, page 11
4. Set Up Your Message Source, page 12
5. Review Your Policy Settings, page 14
6. Import Your Microsoft Email Domains, page 14

These steps assume you meet the **Requirements, page 9.**

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 logged 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.

Indicate if you have a 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 or No, then click **Next**.
2. If you answered Yes, enter your SEG type and header. Click **Next**.

Select Your Message Source, Visibility and Remediation

1. Select your message source: Microsoft O365 or Gateway. If you selected No SEG in the previous step, Microsoft O365 is assumed as your message source.
2. Select your Visibility and Remediation.

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

Microsoft 365 Authentication

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

  Note: If you choose **Read/Write**, you will need to turn on the Automated Remediation Policy in your **Policy Settings, page 17** once your setup is complete. To apply auto-remediation to all internal emails, ensure the **Apply auto-remediation to domains not in the domain list** box on the Policy page is selected.

For Microsoft 365 Authentication mode, Secure Email Threat Defense requests access permissions from Microsoft. These permissions depend on whether you choose Read/Write or Read mode. Details about the permissions can be found in the linked Microsoft documentation.

Both Microsoft Authentication modes request: **Organization.Read.All** and **User.Read**

- https://learn.microsoft.com/en-us/graph/permissions-reference#organizationreadall
- https://learn.microsoft.com/en-us/graph/permissions-reference#userread

Read/Write mode requests: **Mail.ReadWrite**

- https://learn.microsoft.com/en-us/graph/permissions-reference#mailreadwrite

Read mode requests: **Mail.Read**

- https://learn.microsoft.com/en-us/graph/permissions-reference#mailread

No Authentication

This option is available if you are using a Cisco SEG as your message source. It provides visibility only. You will not be able to remediate messages.

3. 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; the account will not be stored or used by Secure Email Threat Defense. For information on why these rights are needed, see Cisco Secure Email Threat Defense FAQ: 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 are redirected back to the Secure Email Threat Defense setup page.
   d. Click **Next**.

Set Up Your Message Source

Complete the steps for your selected 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 needing to pass through the Secure Email Gateway, we recommend adding an outbound connector in Microsoft 365. The connector needs to be added before you set 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

  Note: 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 pre-existing 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, you 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://compliance.microsoft.com/homepage.

   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**.

Review Your Policy Settings

For information on policy settings, see **Policy Settings, page 17**. If you have chosen **Microsoft O365 Authentication: Read/Write** mode, you should verify your **Automated Remediation** settings now. To apply automated remediation to all internal emails, ensure **Apply auto-remediation to domains not in the domain list** is selected. You can turn on the **Automated Remediation Policy** toggle once your domains are imported.

Import Your Microsoft Email Domains

Secure Email Threat Defense imports domains with email capabilities from your Microsoft 365 tenant. Import your domains so you can apply automated remediation to specific domains. Secure Email Threat Defense treats newly imported domains differently depending on if you have the **Apply auto-remediation to domains not in the domain list** box checked or unchecked:

- If **Apply auto-remediation to domains not in the domain list** is checked, auto-remediation is applied to any new domains that are imported.
- If **Apply auto-remediation to domains not in the domain list** is unchecked, auto remediation is not applied to any new domains that are imported.

By default, the **Apply auto-remediation to domains not in the domain list** is unchecked.

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.

Policy Settings

The settings on the **Policy** page determine how mail is handled by Cisco Secure Email Cloud Mailbox. Default settings are applied when you **Set Up Secure Email Threat Defense, page 11**. To change your settings, make the change then click the **Save and Apply** button.

Table 1 Policy Settings

Setting	Description	Options	Default
Message Source	Defines the source for your messages.	■ **Microsoft 365** ■ **Gateway** (for incoming messages only)	Manually selected when you set up Secure Email Threat Defense.
Visibility & Remediation	Defines the type of remediation policy you can apply.	■ **Microsoft 365 Authentication** – **Read/Write** - Allows visibility and on-demand or automated remediation (that is, move or delete suspect messages). Read/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 select **Read**, you need only set the **Attachment Analysis** and **Message Analysis** directions. Remediation policy will not be applied. ■ **No Authentication** Allows Visibility only.	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. **Note:** When you choose **Microsoft 365 Authentication: Read/Write**, you should also verify your **Automated Remediation Policy** settings.
Secure Email Gateway (SEG)	The presence of a Secure Email Gateway (SEG) impacts how Secure Email Threat Defense identifies the Sender IP.	■ Nothing selected (No SEG) ■ **SEG is present** – **Use Cisco SEG default header** (X-IronPort-RemoteIP). – **Use Custom SEG header**. You must add the header you wish to use.	Manually selected when you set up Secure Email Threat Defense. For more information, see Policy Settings with a Gateway, page 19.

Table 1 Policy Settings

Setting	Description	Options	Default
Message Analysis	Messages to be dynamically analyzed, including: ■ Direction of messages ■ Direction of mail attachments to be analyzed by Cisco Secure Malware Analytics ■ Analysis of Spam and Graymail	■ **Direction of Messages** – **Incoming** – **Outgoing** – **Internal** ■ **Direction of Attachments** – **Incoming** – **Outgoing** – **Internal** ■ **Spam and Graymail** – **On** or **Off**	■ **Direction of Messages** – **All** for Microsoft O365 Message Source – **Incoming** for Gateway message source ■ **Direction of Attachments** – **Incoming** ■ **Spam and Graymail** – **Off** for all accounts created after May 9, 2023
Automated Remediation Policy	Remediation actions for messages found to be: ■ **Threats** (BEC, Scam, Phishing, or Malicious) ■ **Spam** ■ **Graymail**	■ **No Action** ■ **Move to Quarantine** ■ **Move to Trash** ■ **Move to Junk** **Note:** If the sender address belongs to a sender allow list in Exchange or if the message has already been remediated by Microsoft 365, remediation actions are not applied.	■ **Automated Remediation Policy** toggle - **Off** ■ Threats - **Move to Quarantine** ■ Spam - **Move to Junk** ■ Graymail - **No Action**
Safe Sender: Do not remediate Microsoft Safe Sender messages with Spam or Graymail verdicts.	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**

Table 1 Policy Settings

Setting	Description	Options	Default
Imported Domains – Domains are imported to help determine message directions. Domains can be excluded from Automated Remediation Policy.			
Apply Auto-Remediation	Applies automated remediation to a specific domain.	**Checked** or **Unchecked**	**Unchecked**. When you turn on **Read/Write** Remediation mode, select these check boxes to apply auto-remediation to specific domains.
Apply auto-remediation to domains not in the domain list above	Applies when a domain is not explicitly listed. For example, if a new domain has been added to your Microsoft 365 account but not imported into Secure Email Threat Defense.	**Checked** or **Unchecked**	**Unchecked**. When you turn on **Read/Write** mode, select this check box to ensure auto-remediation is applied to all internal emails.

Policy Settings with a Gateway

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

Table 2 Suggested Policy Settings with Gateway

Setting Name	Recommended Selection
Secure Email Gateway (SEG)	**SEG is present**, and indicate header
Message Analysis	**Outgoing** and **Internal**
Attachment Analysis	**None**
Remediation Actions	■ Threats - **Move to Quarantine** ■ Spam - **Move to Junk**

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 Set Up Secure Email Threat Defense, page 11.

Switching Your Message Source

To change your message source, navigate to the **Policy** page.

1. Select the radio button for the new 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, page 61 or Configure your Gateway to Stop Sending Messages, page 62.
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 Set Up Your Message Source, page 12.

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.

Messages Page Icons

The following table shows icons used on the Messages page and their meanings.

Table 1 Messages Page Icons

Icon	Name	Description
	Links	Message contains link(s).
	Attachments	Message contains attachment(s).
	Manually Remediated or Manually Reclassified	Message was manually remediated or reclassified. The icon shows next to the Action if the message was remediated and next to the Verdict if the message was reclassified.
	Retrospective Verdict	A Retrospective Verdict was applied. A Retrospective Verdict is one that was applied after the message was first scanned by Secure Email Threat Defense.
	Allowed	Message was allowed based on the item indicated: Allow List, MS Allow List, or Safe Sender.
	Verdict Override	Verdict was overridden based on a Verdict Override message rule.
	Bypass Analysis	Message was not analyzed because of a Bypass Analysis message rule. The type of rule, either Security Mailbox or Phish Test, is indicated.
	BEC	Message has been marked as Business Email Compromise (BEC), either manually or through auto-remediation.
	Scam	Message has been marked as Scam, either manually or through auto-remediation.
	Phishing	Message has been marked as Phishing, either manually or through auto-remediation.

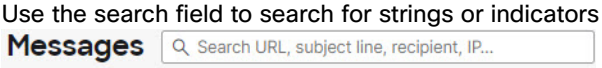
Table 1 Messages Page Icons

Icon	Name	Description
	Malicious	Message has been marked as Malicious, either manually or through auto-remediation.
	Spam	Message has been marked as Spam, either manually or through auto-remediation.
	Graymail	Message has been marked as Graymail. Graymail is mail that has been determined to be marketing, social, or junk.
	Neutral	Message has been marked as Neutral.
	Incoming	Mail received from outside your O365 tenant.
	Internal	Mail sent within your O365 tenant.
	Outgoing	Mail sent to recipients outside of your O365 tenant

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.

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

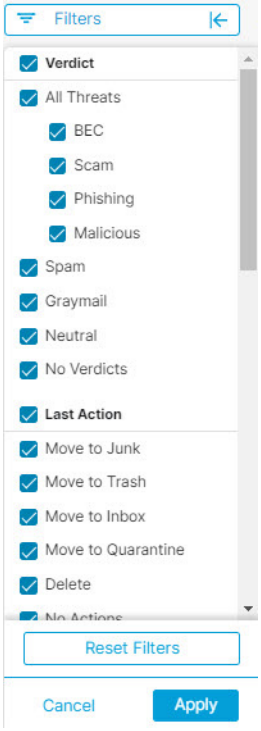


Filter Panel

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 the arrow to expand the filter panel.

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

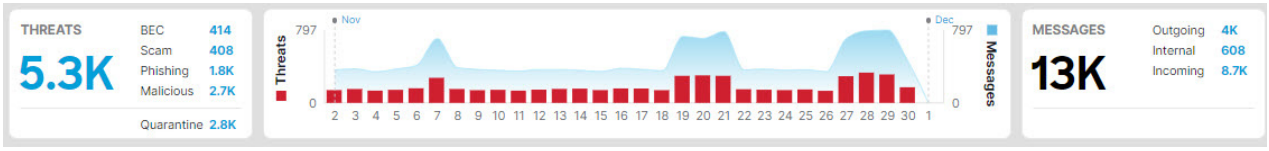


Use the **Reset Filters** button to reset the filters to their defaults.

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
- A Quarantine total you can use to filter for quarantined items
- Message Direction totals you can use to quickly filter by direction



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.

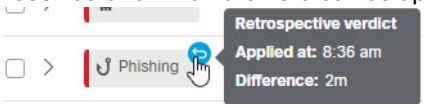
- **Phishing**: These messages have been convicted of fraudulently copying or mimicking legitimate services in an attempt to acquire sensitive information such as user names, passwords, credit card numbers, and more.
- **Malicious**: These messages have been convicted of containing, serving, or supporting 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

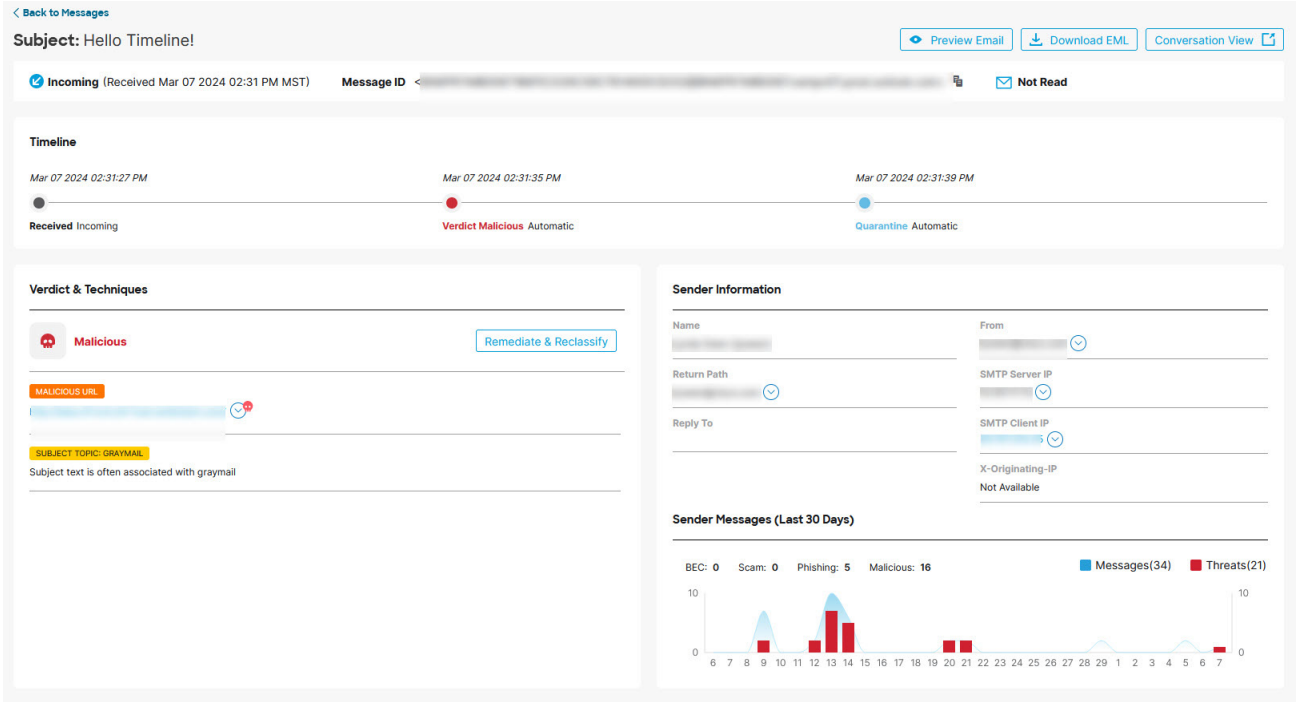
The message report allows you to investigate details about a message. Select the **>** icon or click anywhere on a message row to access the report for that message.

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
- Sender Messages
- Recipient information including Recipients, Envelope Recipients, and Mailboxes
- Links
- Attachments

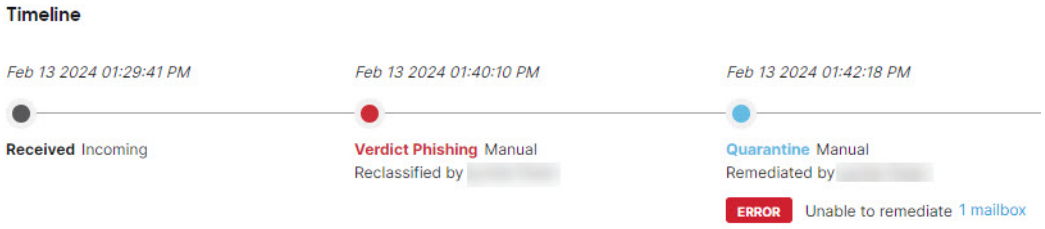
- Email Preview

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



Timeline

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



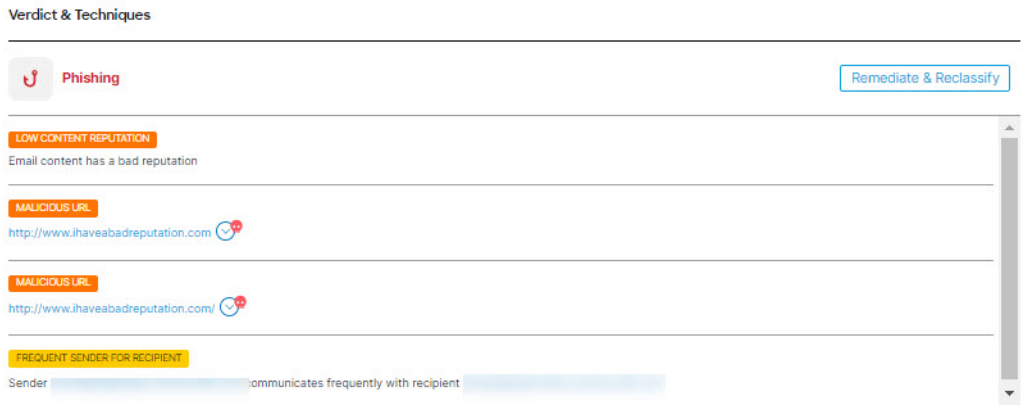
The timeline shows:

- **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

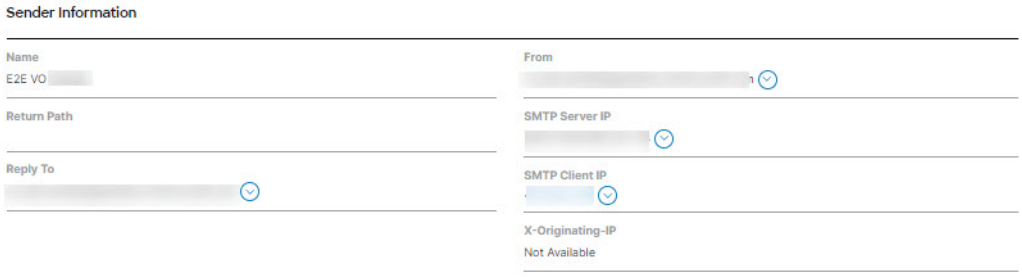
The Verdict and Techniques panel shows a visual representation of the verdict applied to a message and techniques detected that may have contributed to the verdict. Techniques are color coded to indicate their severity. Malicious file names/SHA256 and URLs are shown dynamically when available. Static 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, page 29.



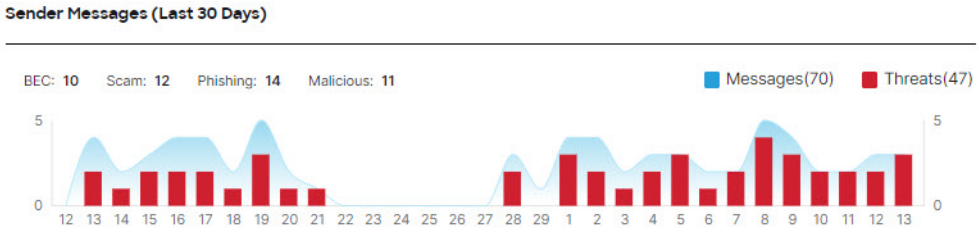
Sender Information

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 and X-Originating IP.



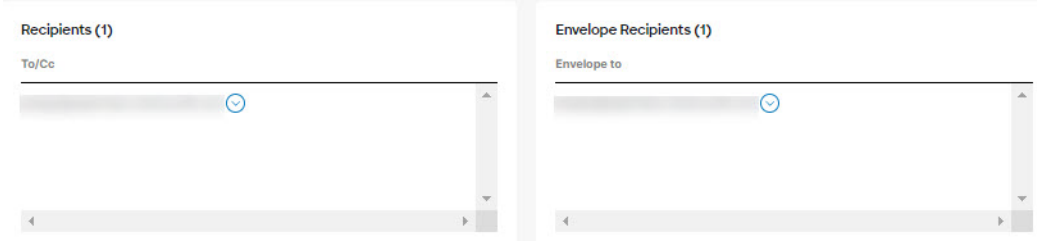
Sender Messages

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.



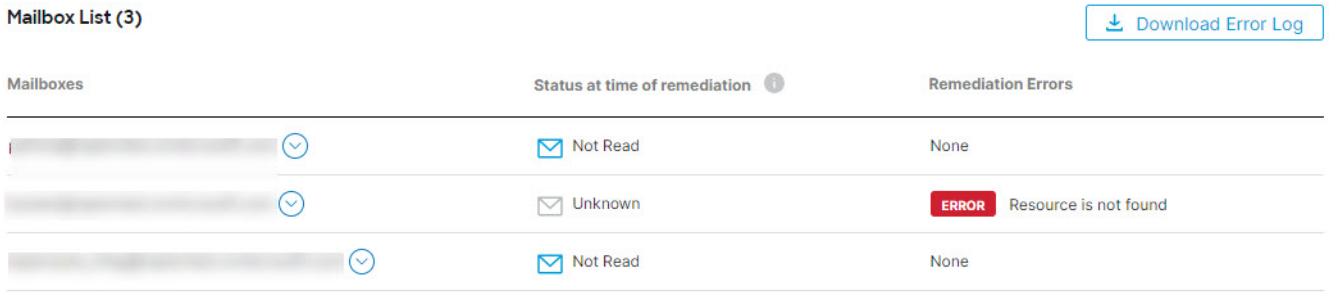
Recipient Information

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



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.

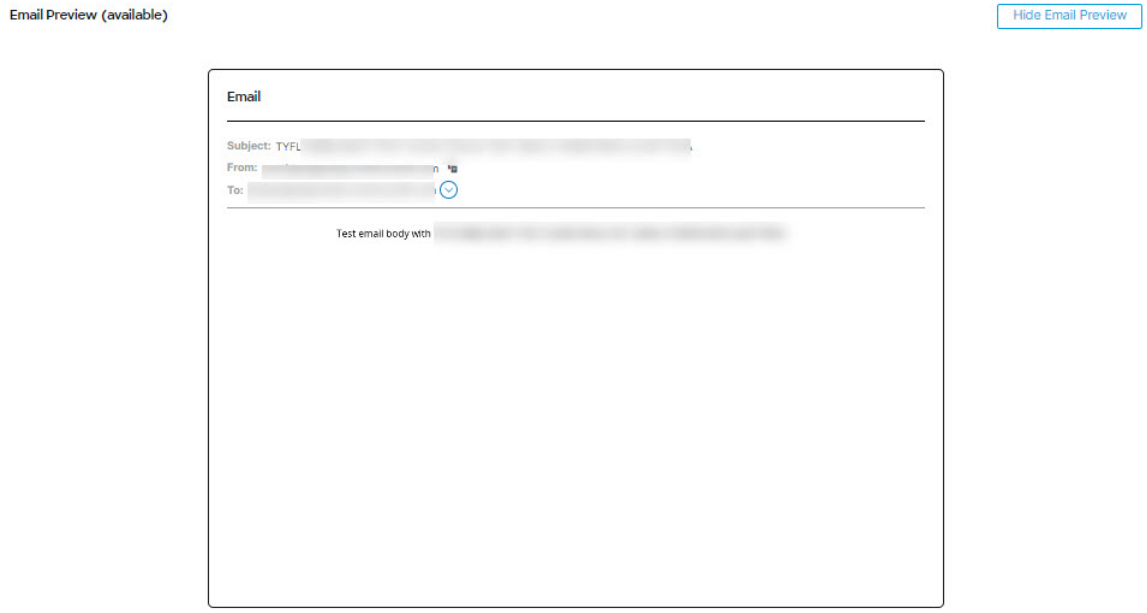


Links and Attachments

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

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.



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

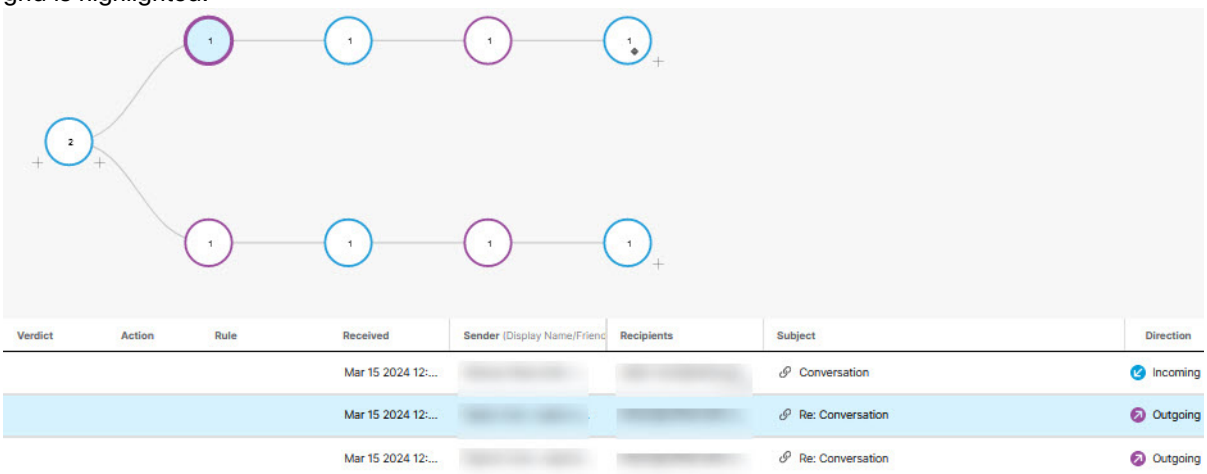
Conversation View

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.

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.



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, page 55.

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. You can also move and reclassify a 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/.

Note: 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 Verdict Override Rules, page 51.

About Hybrid Exchange Accounts

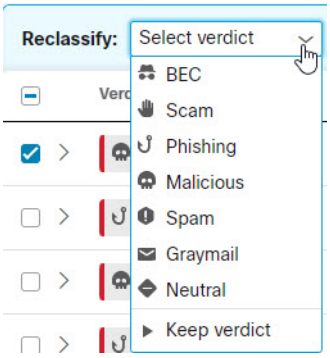
Secure Email Threat Defense can act only on mailboxes located in Exchange Online (O365). If you are in the process of migrating your mailboxes from on-premises Exchange to Exchange Online (O365), remediation (move or deletion) will only work for mailboxes located in Exchange Online (O365). You will not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



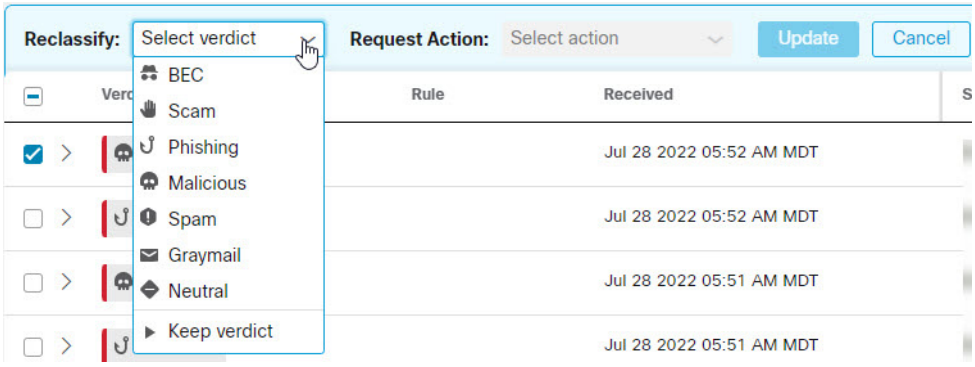
3. Click **Update** to apply the new classification.

Read/Write Remediation Mode

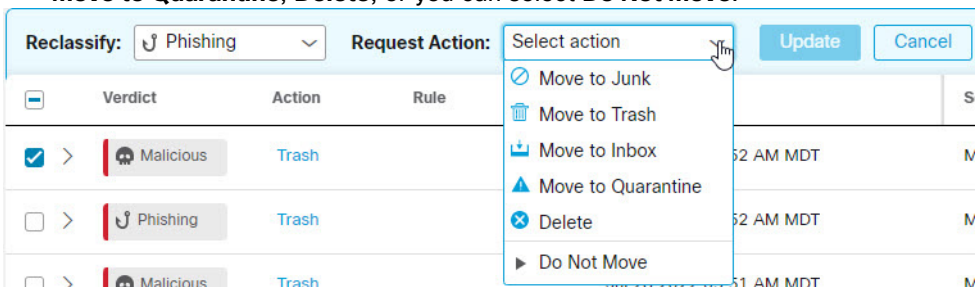
If you are in Read/Write remediation mode, you can move suspicious messages out of user Inboxes and into their Junk or Trash, or to a Quarantine folder they cannot access. Similarly, if you determine a message that was moved to Junk, Trash, or Quarantine is not suspicious, you can move it back to user 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**.



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**.



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

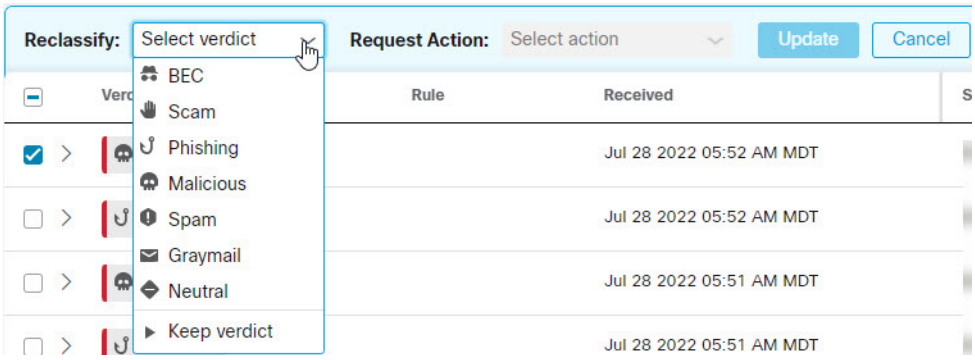
If a message has been moved, it is indicated in the **Last Action** column.

Note: 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.

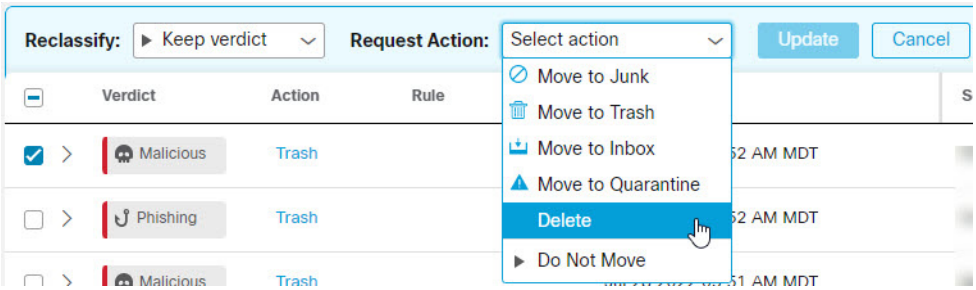
Delete Messages

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**.



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



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.

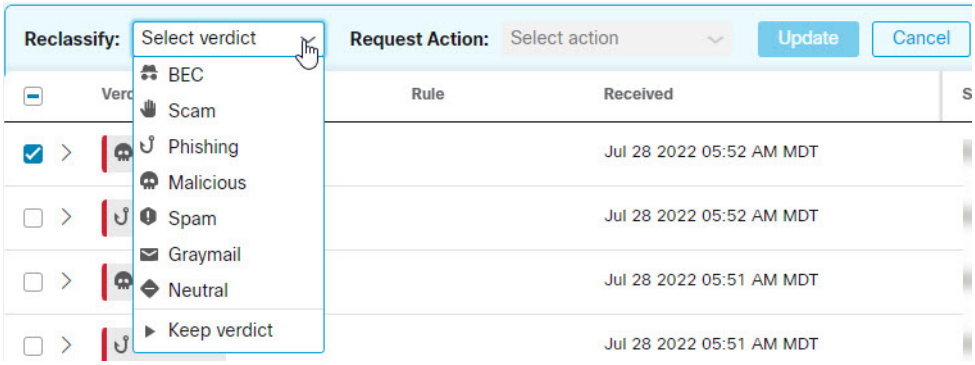
Quarantine Messages

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.

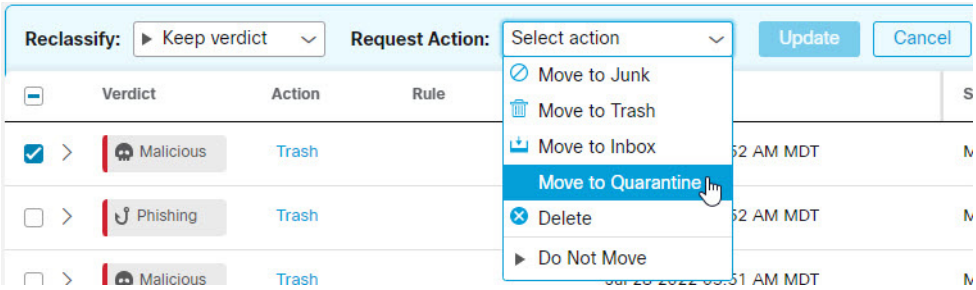
To manually move messages to quarantine:

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**.



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



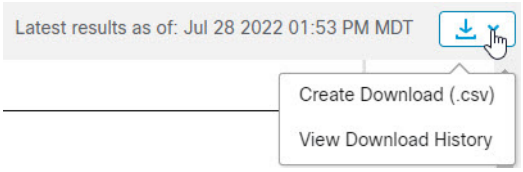
4. Click **Update** to quarantine the message(s).

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

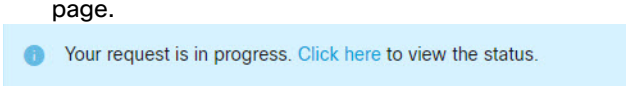
Download Search Results

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)**.



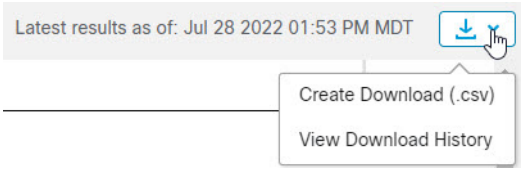
2. A banner indicating that your request is in progress appears. Click the text to be taken to the **Downloads: Messages** page.



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.

Download Search Results

Downloads

The pages accessible from the **Downloads** menu allow you create and/or manage:

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

Messages

You can download message data in two ways:

- From the Messages page, as described in Download Search Results, page 32. 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** 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**.
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. When you have a message expanded, 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*.

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

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

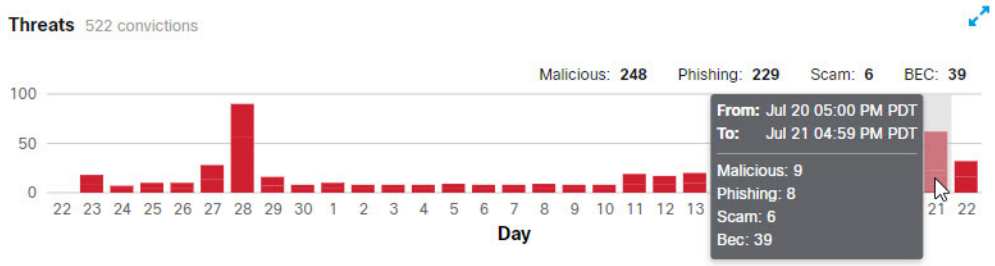
Trends

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.

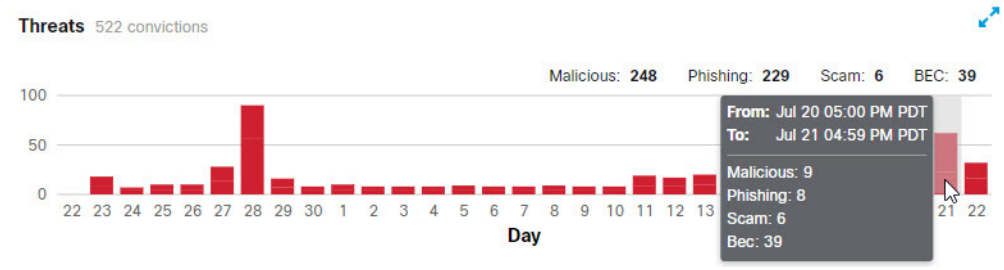
About Timezones

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

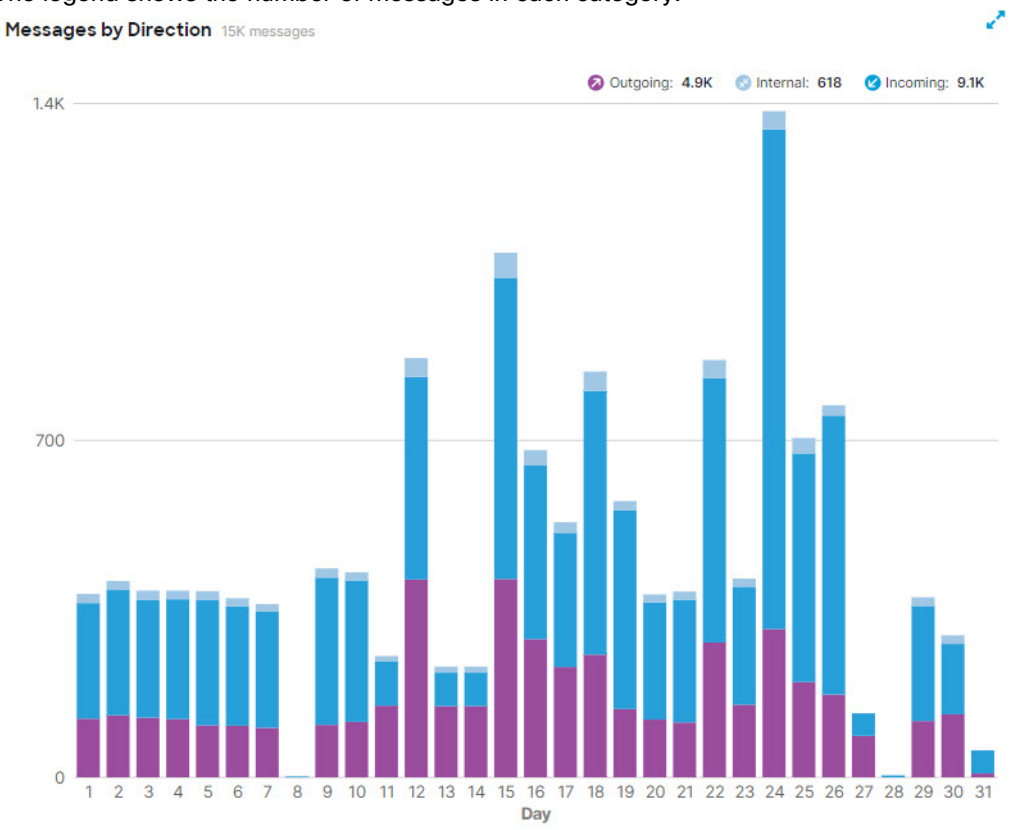


Messages by Direction

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

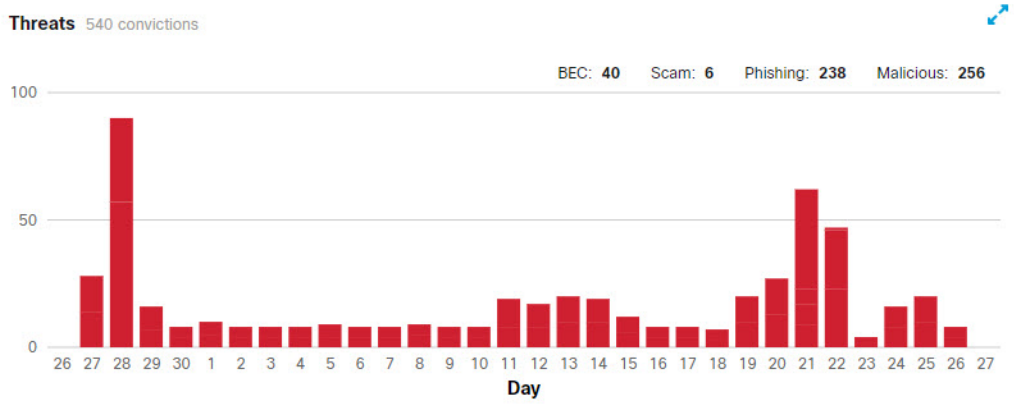
- **Outgoing**: mail sent to recipients outside of your O365 tenant
- **Internal**: mail sent within your O365 tenant
- **Incoming**: mail received from outside your O365 tenant

The legend shows the number of messages in each category.



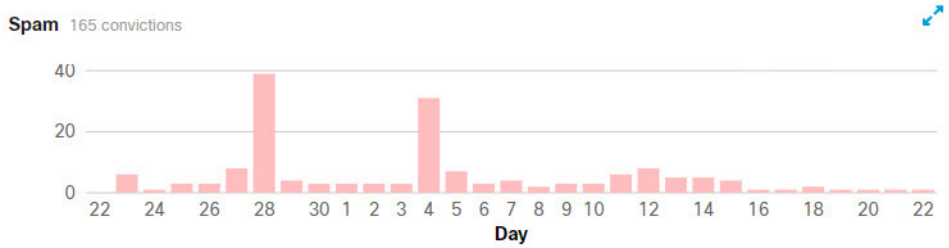
Threats

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.



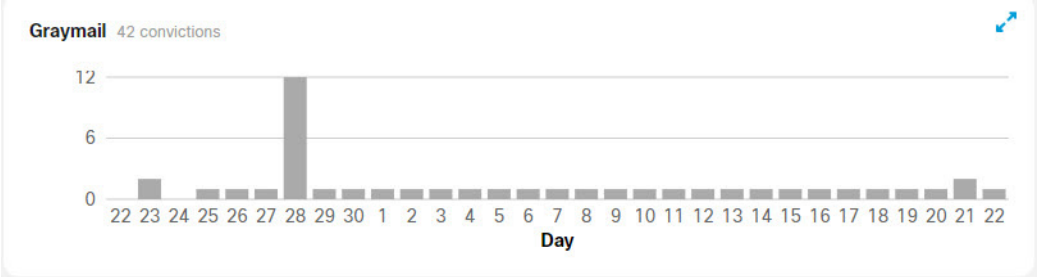
Spam

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.

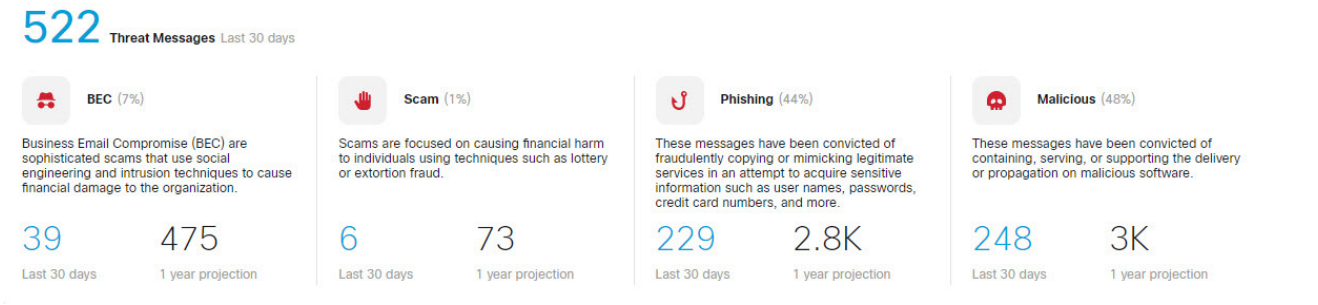


Impact Report

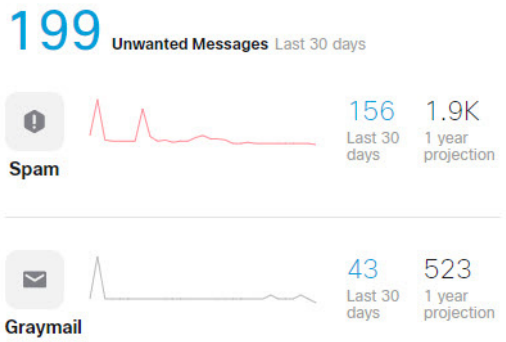
The Impact Report shows the benefits Secure Email Threat Defense provided over the last 30 days. Select **Insights** > **Impact Report** to see the report. Click data of interest in the report to be taken to the data details on the Messages page.

Data shown includes:

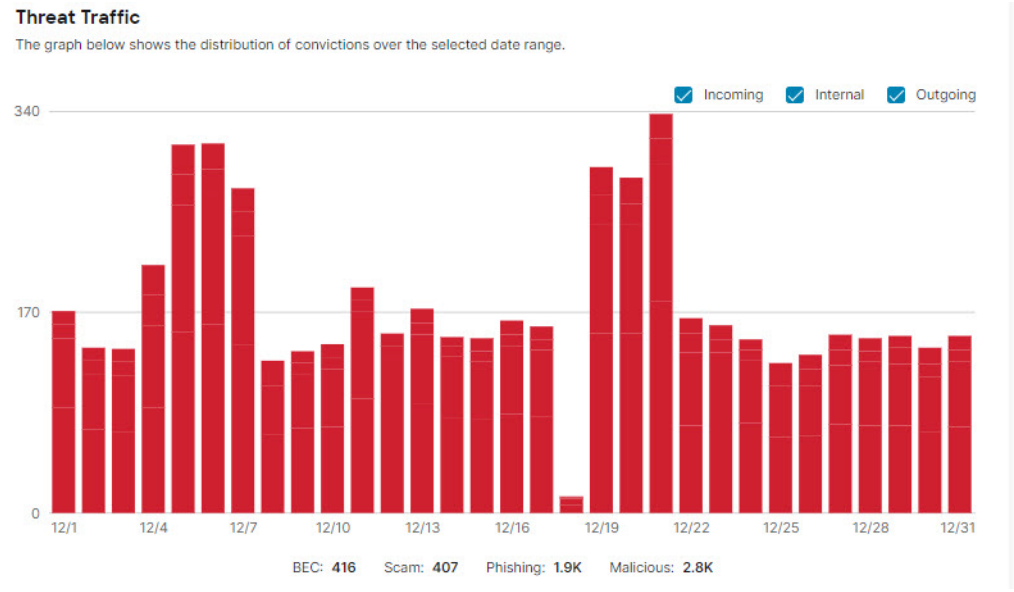
- Threat messages caught by Secure Email Threat Defense in the selected 30 day period, and a 1-year projection of this data. The 1-year projection is calculated as the daily average multiplied by 365.



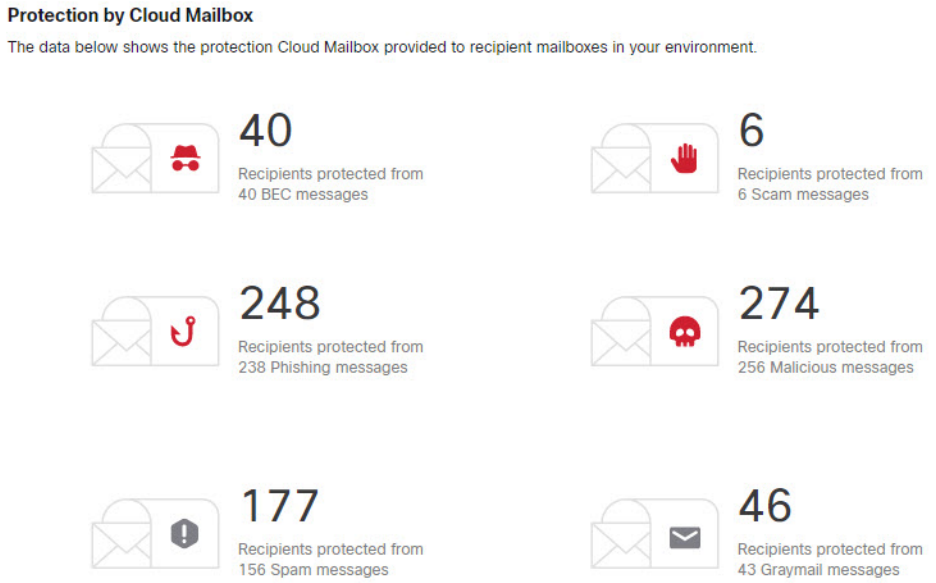
- Unwanted Messages. This chart shows Spam and Graymail in the selected 30 day period, and a 1-year projection of this data. The 1-year projection is calculated as the daily average multiplied by 365.



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



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



- 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

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.

Admins should create a list of up to 100 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 the **Add New Personnel** button.
3. Enter the user's information. First Name, Last Name, and Email Address are required.
4. Click **Submit** 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. Under the Actions column, click the **Edit** (pencil) button.
3. Update the user's information as needed. First Name, Last Name, and Email Address are required.
4. Click **Submit** 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. Under the Actions column, click the **Delete** button.
3. Click **Delete** to in the Confirm Removal dialog to complete the action.

Remove a User from the High Impact Personnel List

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.

Note: 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, page 46. 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.

Table 1 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 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.

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**.

   Note: 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, page 55.

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.

Preferences

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 setting, and your business-level Cisco XDR integration authorization.

Notification Email

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.

You can choose whether or not to send notifications for retrospective verdicts to your notification email address. An email will be sent when a retrospective verdict is applied to messages.

Audit Logs

You can download audit logs for the previous 3 months as CSV files. Select a date range from the drop-down, then click **Download CSV**.

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 **Cisco XDR, page 55**.

Message Rules

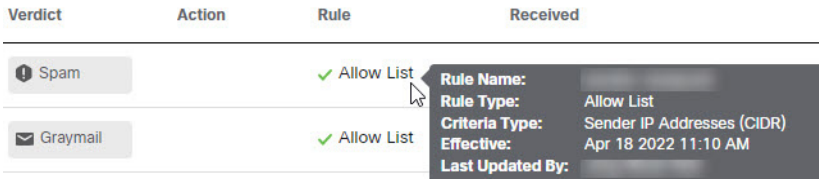
Message rules allow you to specify that some types of messages should not be remediated or scanned. You can create:

- Allow List rules
- Verdict Override rules
- Bypass Analysis rules

Note: Allow List and Verdict Override rules are not available for businesses in No Authentication mode.

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

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



Note: 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.

Bypass Analysis Rules

Bypass Analysis rules allow you to bypass analysis for Phish Test or Security Mailbox messages that match the 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.

Note: If a Bypass Analysis 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 block); messages will not be analyzed.

  Note: 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.

- 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.

  Note: Security Mailbox rules are applied if the specified recipient is the only recipient of the message. If other recipients are copied or included as a BCC (blind carbon copy), the message will not bypass the analysis engines.

- Can have up to 50 criteria per rule.

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

Advisory on Creating and Using Bypass Rules

Note the following important caveats when creating and using Bypass Rules.

- A Bypass Rule bypasses all scanning and protections for messages that match the rule conditions. Do not use Bypass 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 Bypass Rules. For all other scenarios only Verdict Override or Allow Rules are supported.
- It is strongly advised to use only the dedicated Sender IP Addresses/CIDR blocks provided by your Phish Test vendor as the basis of 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 Bypass Rule opens you up to bypassing potentially spoofed messages.
- Do not use Sender Domain or Email Address in a 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 Bypass Rule.

Add Message Rules

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.

Add a New Bypass Analysis Rule

Complete the following steps to create a new rule:

1. Select **Administration** > **Message Rules**.
2. Select **Bypass Analysis**.
3. Click the **Add New Rule** button.
4. Create a rule name. Each rule must have a unique name.
5. Select which rule type you want to create: **Phish Test** or **Security Mailbox**.
6. For a Phish Test rule, select a criteria type: Sender Email Addresses, Sender Domains, Sender IP Addresses (IPv4), or IP Addresses (CIDR). Then, enter your items, separated by commas.

   For a Security Mailbox rule, enter your recipient email addresse(s), separated by commas.
7. 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.

Note: If a Bypass Analysis rule is created for testing, the rule should be reconsidered after an appropriate period of time to prevent vulnerabilities. See for important caveats to keep in mind when creating and using Bypass Rules.

Edit a Rule

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 not honored for Malicious or Phishing verdicts. For more information, see Cisco Secure Email Threat Defense FAQ: 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, select the **Do not remediate Microsoft Safe Sender messages with Spam or Graymail verdicts** check box on the Policy page. Safe Sender flags are respected for Spam and Graymail verdicts, but are not respected for Malicious and Phishing 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/

Note: 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

Note: 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.
  - **Note:** Quarantine from the pivot menu is 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.

Note: Your XDR account needs to be activated before you can authorize the ribbon. You can do this by following the instructions in Authorize Cisco XDR for Secure Email Threat Defense, page 55 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/.

Deactivate Secure Email Threat Defense

Message Source: Microsoft 365

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

- Delete your Secure Email Threat Defense journal entry from Microsoft 365 Admin Center
- 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#/homepage.
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:

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

   Note: 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**.

   Note: 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.

Frequently Asked Questions (FAQ)

Frequently asked questions are available in the Cisco Secure Email Threat Defense FAQ.