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 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.

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. You can find details about the permissions 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 use a Cisco SEG as your message source. It provides visibility only; you cannot 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; Secure Email Threat Defense will not store or use the account. To learn why these rights are required, 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 will be redirected 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 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.

  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 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://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 whether 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.