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.