Configure Secure Email Gateway Per-Policy Journaling to Secure Email Threat Defense

Contents

Introduction

This document describes steps to configure the Secure Email Gateway (SEG) to perform Per-Policy Journaling for Secure Email Threat Defense (SETD).

Prerequisites

Prior knowledge of the Cisco Secure Email Gateway (SEG) general settings and configuration is beneficial.

Components Used

This setup requires both;

- Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 and newer
- Cisco Email Threat Defense (SETD) Instance.
- Threat Defense Connector (TDC). "The defined connection between the two technologies."

"The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command."

Overview

The Cisco SEG is capable of integrating with SETD for additional protection.

- The SEG journal action transfers the complete email for all clean messages.
- The SEG provides the option of selectively choosing incoming mail flows based on a Per-Mail-Policy match.
- The SEG Per Policy option allows 3 choices; No Scan, Default Message Intake address, or Custom Message Intake Address.
  - The Default Intake Address represents the primary SETD Account accepting mail for a specific account instance.
  - The Custom Message Intake Address represents a second SETD Account accepting mail for

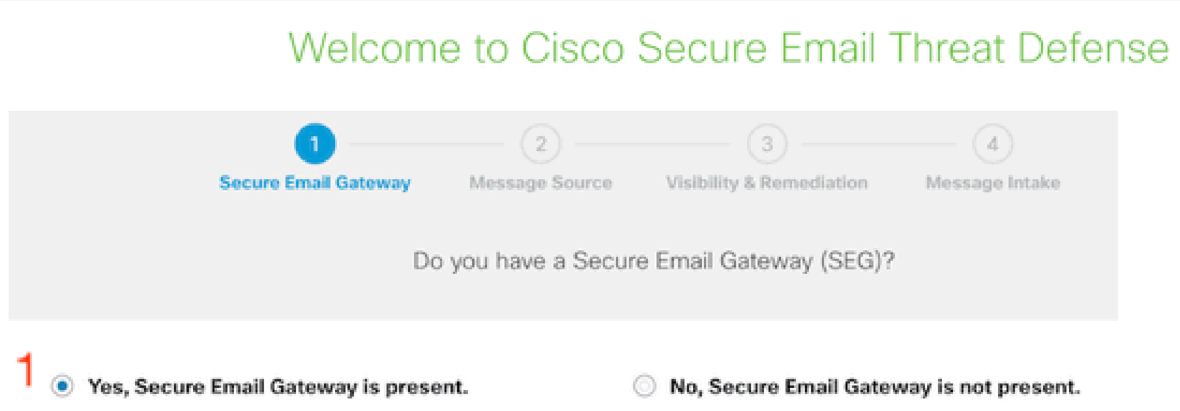
different defined domains. This scenario applies to more complex SETD Environments.

- Journaled messages have an SEG Message ID(MID) and Destination Connection ID DCID
- The Delivery Queue contains a value similar to a domain, "the.tdc.queue", to capture SETD transfer counters.
  - "the.tdc.queue" active counters can be viewed here: cli>tophosts or SEG Reporting > Delivery Status (non-CES).
  - "the.tdc.queue" represents the Threat Defense Connector (TDC) equivalent to a destination domain name.

Configure

SETD initial setup steps to generate the "Message Intake Address."

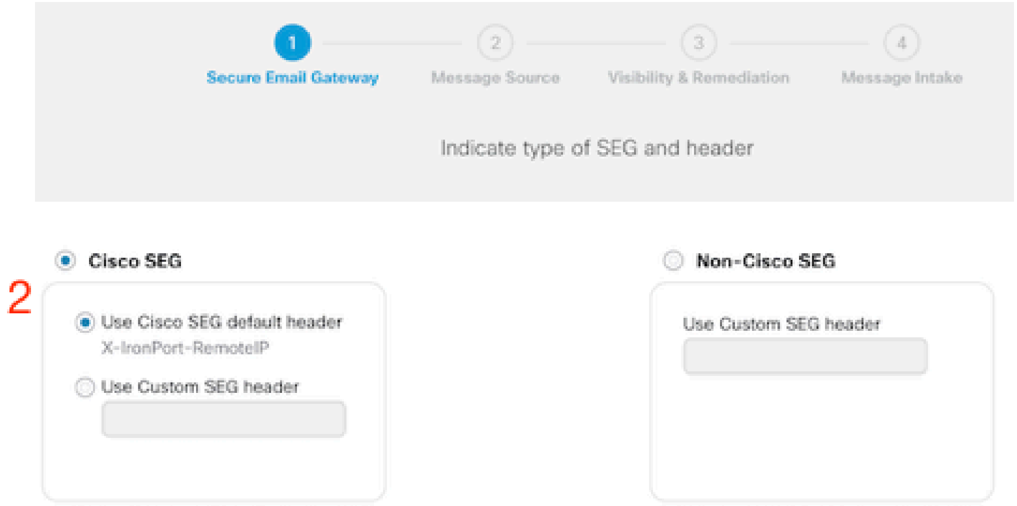
1. Yes, Secure Email Gateway is present.
2. Cisco SEG



Welcome to Cisco Secure Email Threat Defense

Do you have a Secure Email Gateway (SEG)?

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



Indicate type of SEG and header

● Cisco SEG

● Use Cisco SEG default header X-IronPort-RemoteIP

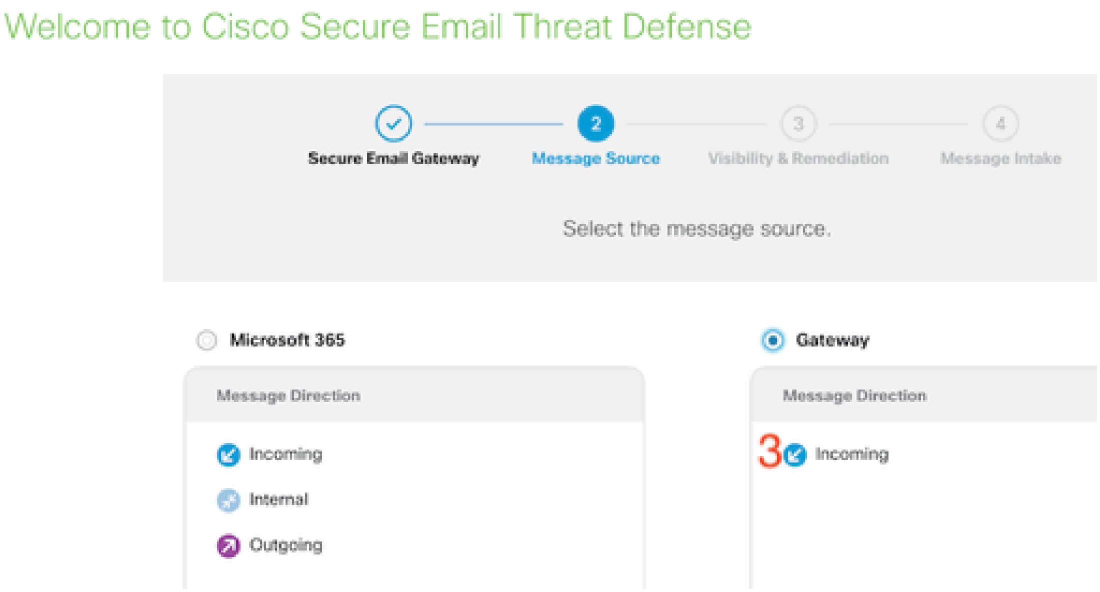
○ Use Custom SEG header

○ Non-Cisco SEG

Use Custom SEG header

3. Message Direction = Incoming.

4. No Authentication = Visibility Only.



Select the message source.

○ Microsoft 365

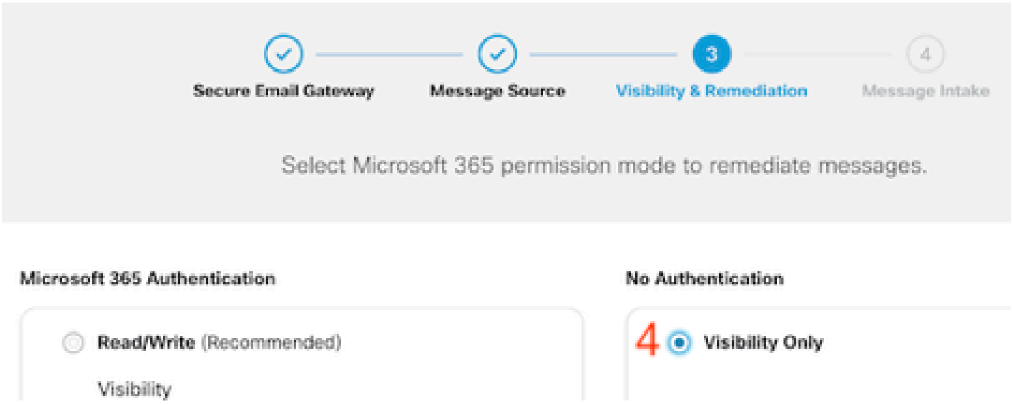
Message Direction

- Incoming
- Internal
- Outgoing

● Gateway

Message Direction

- Incoming



Select Microsoft 365 permission mode to remediate messages.

Microsoft 365 Authentication

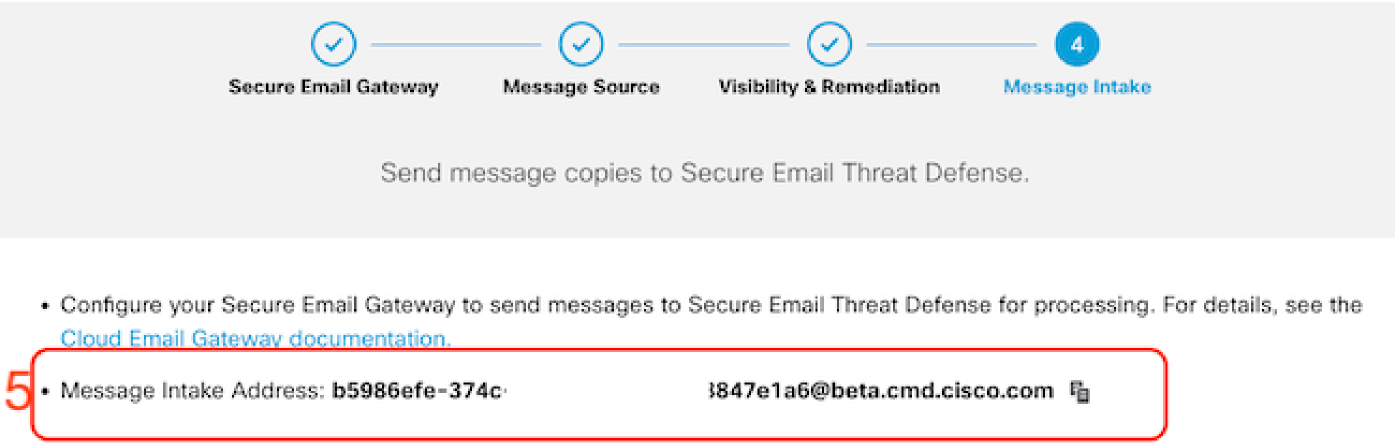
○ Read/Write (Recommended)

Visibility

No Authentication

● Visibility Only

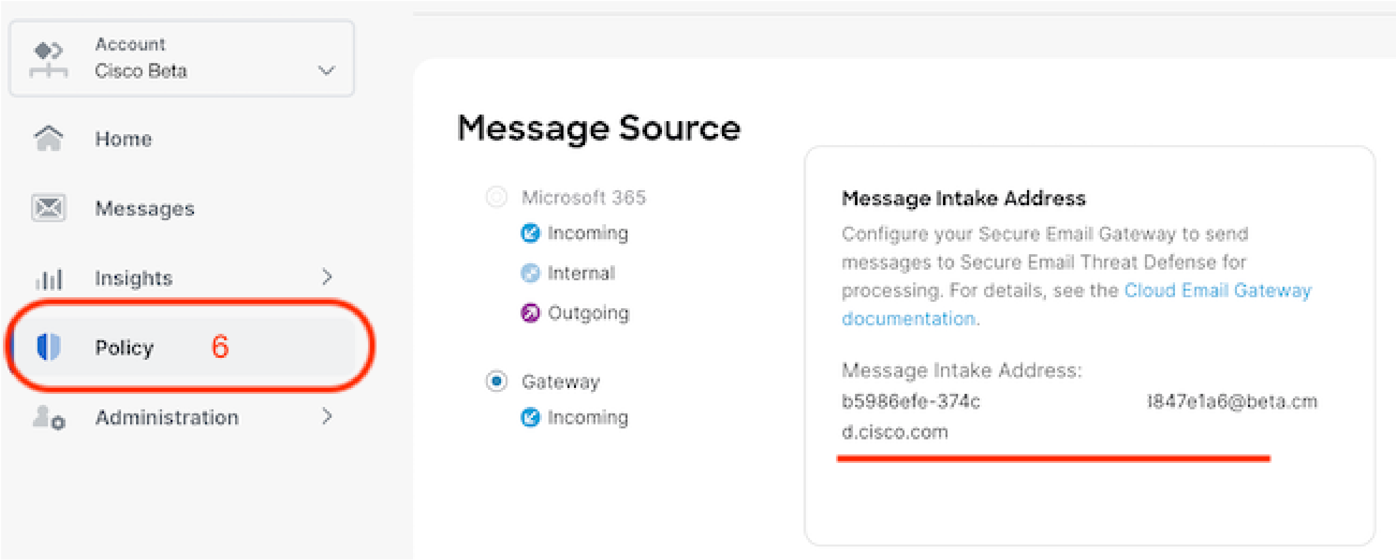
5. The Message Intake Address is presented after step 4 has been accepted.



Send message copies to Secure Email Threat Defense.

- Configure your Secure Email Gateway to send messages to Secure Email Threat Defense for processing. For details, see the Cloud Email Gateway documentation.
- Message Intake Address: b5986efe-374c[redacted]3847e1a6@beta.cmd.cisco.com

6. If you need to retrieve the Message Intake Address post setup, navigate to the Policy menu.



Message Source

○ Microsoft 365
Incoming
Internal
Outgoing

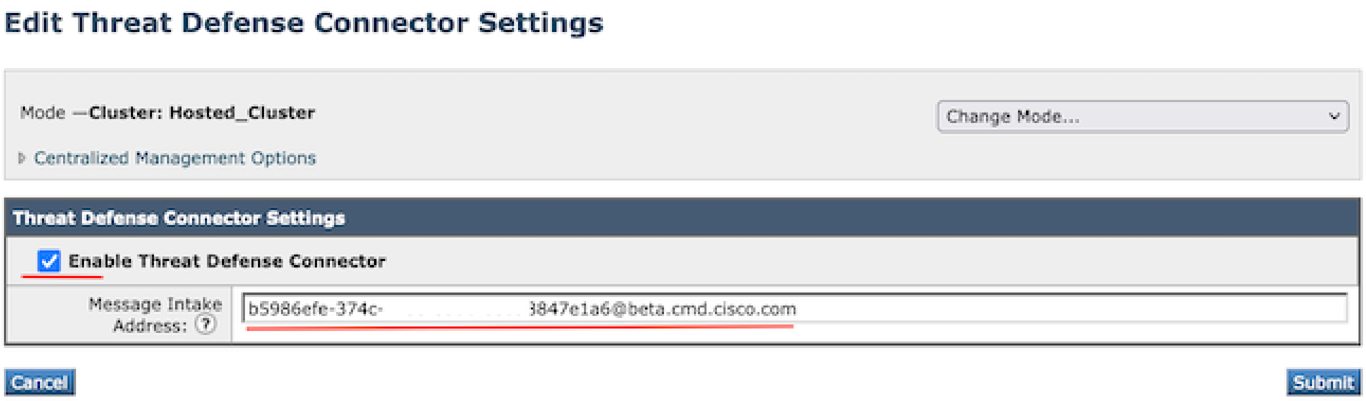
● Gateway
Incoming

Message Intake Address

Configure your Secure Email Gateway to send messages to Secure Email Threat Defense for processing. For details, see the Cloud Email Gateway documentation.

Message Intake Address:
b5986efe-374c 1847e1a6@beta.cmd.cisco.com

Transitioning to the SEG WebUI, Navigate to Security Services > Threat Defense Connector Settings.



Edit Threat Defense Connector Settings

Mode —**Cluster: Hosted_Cluster**

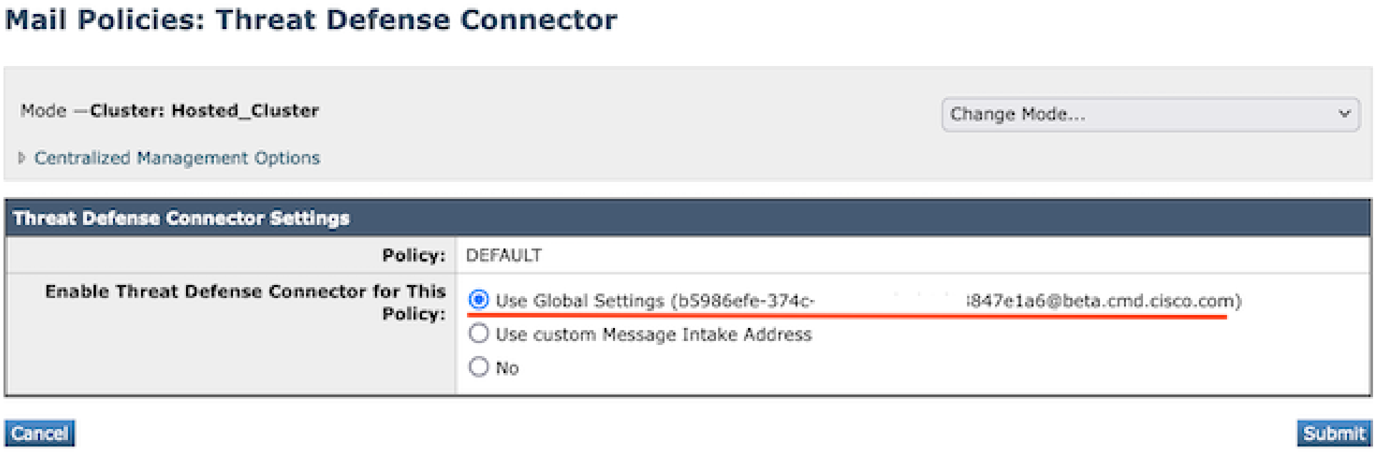
Threat Defense Connector Settings

☑ **Enable Threat Defense Connector**

Message Intake Address: b5986efe-374c- 3847e1a6@beta.cmd.cisco.com

Navigate to Mail Policies:

- Incoming Mail Policies
    - The last service to the right is "Threat Defense Connector."
- The settings link displays, "Disabled," for the first time configuration.



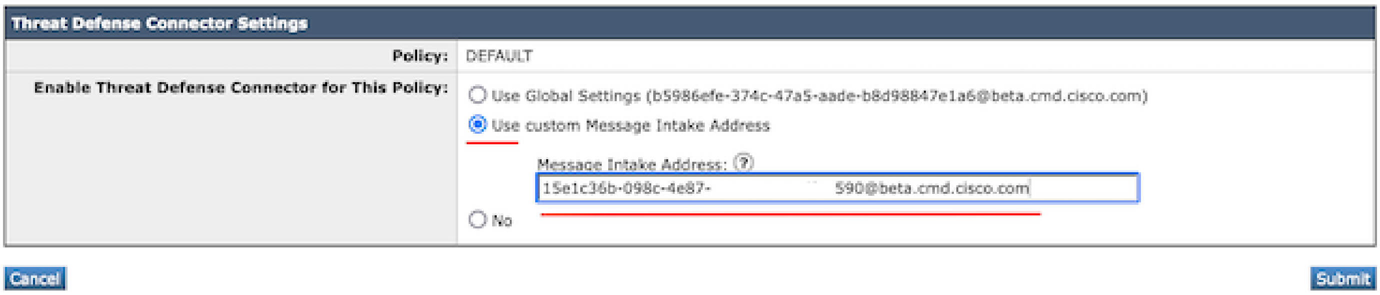
Mail Policies: Threat Defense Connector

Mode —**Cluster: Hosted_Cluster**

Threat Defense Connector Settings

Policy:	DEFAULT
Enable Threat Defense Connector for This Policy:	● Use Global Settings (b5986efe-374c- 1847e1a6@beta.cmd.cisco.com) ○ Use custom Message Intake Address ○ No

The Custom Message Intake Address would populate using a secondary SETD instance.

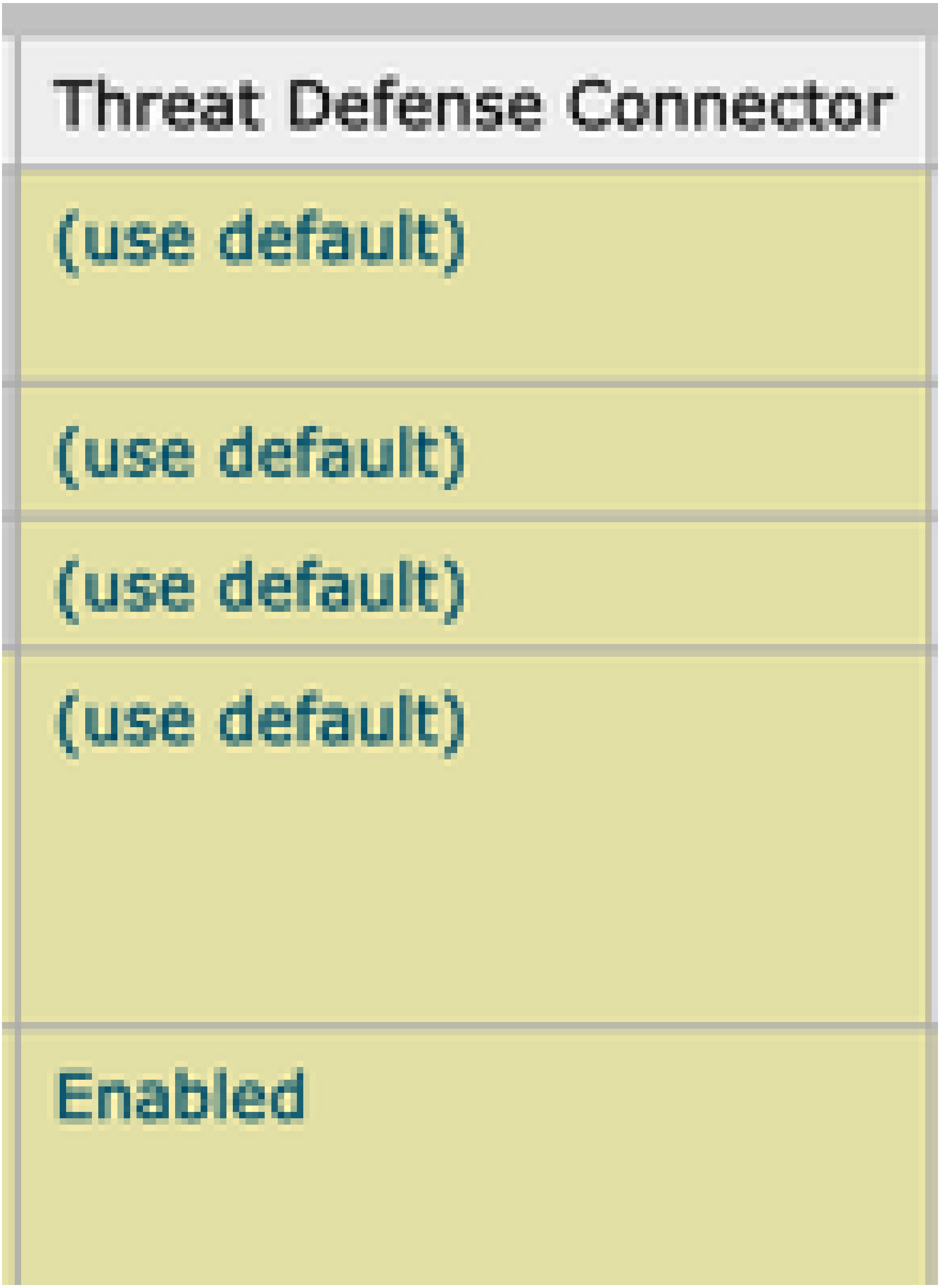


Threat Defense Connector Settings

Policy:	DEFAULT
Enable Threat Defense Connector for This Policy:	○ Use Global Settings (b5986efe-374c-47a5-aade-b8d98847e1a6@beta.cmd.cisco.com) ● Use custom Message Intake Address Message Intake Address: 15e1c36b-098c-4e87- 590@beta.cmd.cisco.com ○ No

Note: It is important when utilizing the Custom Intake Address to configure the Mail Policy match criteria to capture the correct domain traffic.

The final view of the setting presents the value "Enabled," for the configured service.

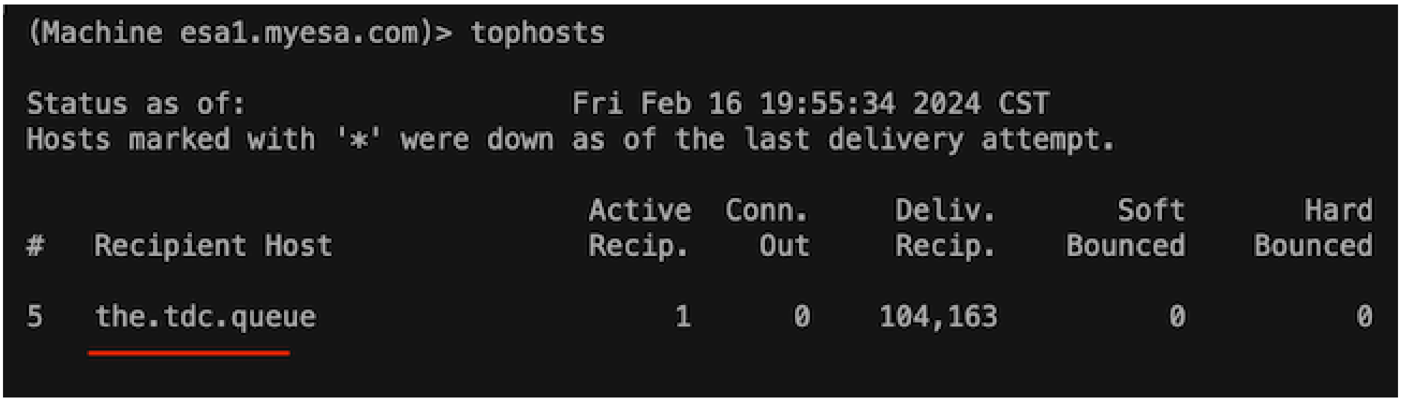


Threat Defense Connector
(use default)
(use default)
(use default)
(use default)
Enabled

Verify

Once all steps have been completed, the email populates the SETD Dashboard.

The SEG CLI command > tophosts displays the.tdc.queue counters for active deliveries.



```
(Machine esa1.myesa.com)> tophosts

Status as of:                   Fri Feb 16 19:55:34 2024 CST
Hosts marked with '*' were down as of the last delivery attempt.

                                 Active   Conn.     Deliv.      Soft      Hard
#   Recipient Host               Recip.     Out     Recip.   Bounced   Bounced

5   the.tdc.queue                     1       0    104,163         0         0
```

Troubleshoot

TDC Connection Behavior:

- A minimum of 3 connections are opened when there are entries present in the destination queue
- Further connections are spawned dynamically using the same logic for regular email destination queues.
- Open connections are closed once the queue becomes empty or there are not enough entries present in the Destination queue.
- Retries are performed as per the value in the table.
- Messages are removed from the queue after retries are exhausted or if the message is in the queue for too long (120sec)

Threat Defense Connector Retry Mechanism

Error Case	Retry Done	Number of Retries
SMTP 5xx errors (except 503/552)	No	N/A
SMTP 4xx errors (including 503/552)	Yes	1
TLS Errors	No	N/A
General Network \ Connection errors, DNS errors, and so on.	Yes	1

Sample TDC mail logs based on the delivery results

TDC-related log entries contain the TDC: value preceding the log text.

The sample presents a normal TDC delivery.

```
Fri Feb 16 21:19:22 2024 Info: TDC: MID 14501404 with Message-ID '<O7afv777xxreILg2OQ@gostrt-sstp-0>' e
Fri Feb 16 21:19:23 2024 Info: TDC: New SMTP DCID 4566150 interface 10.13.0.99 address 10.10.55.171 por
Fri Feb 16 21:19:23 2024 Info: DCID 4566150 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES128-GCM-SH
Fri Feb 16 21:19:23 2024 Info: TDC: Delivery start DCID 4566150 MID 14501404
Fri Feb 16 21:19:24 2024 Info: TDC: MID 14501404 successfully delivered for scanning with Cisco Secure
Fri Feb 16 21:19:24 2024 Info: Message finished MID 14501404 done
```

The sample presents a delivery error due to the undeliverable message after the 120-second timeout expired

```
Wed Nov 29 09:03:05 2023 Info: TDC: Connection Error: DCID 36 domain: the.tdc.queue IP: 10.10.0.3 port:
```

The Sample presents a delivery error due to a TLS Error.

```
Fri Feb 14 04:10:14 2024 Info: TDC: MID 1450012 delivery failed to Cisco Secure Email Threat Defense:TL
```

This sample presents an invalid SETD Journal Address resulting in a hard bounce.

```
Wed Nov 29 09:07:16 2023 Info: TDC: MID 171 with Message-ID '<20231129090720.24911.11947@vm21bsd0050.cs
dress test@esa.example.com
Wed Nov 29 09:07:16 2023 Info: DNS Error esa.example.com MX - NXDomain
Wed Nov 29 09:07:16 2023 Info: TDC: Hard bounced - 5.1.2 - Bad destination host ('000', 'DNS Hard Error
Wed Nov 29 09:07:16 2023 Info:
TDC: MID 171 delivery failed to Cisco Secure Email Threat Defense: Hard Bounced.
Wed Nov 29 09:07:16 2023 Info: Bounced: DCID 0 MID 171 to RID 0 - Bounced by destination server with re
(MX) :
```

Message Tracking simply displays a single line indicating the successful delivery of the message to SETD.

This sample presents a delivery error due to a TLS Error.

16 Feb 2024 21:19:24 (GMT -06:00)	TDC: Message 14501404 was successfully delivered for scanning with Cisco Secure Email Threat Defense.

Related Information

- Email Security Setup Guide
- Cisco Secure Email Gateway Launch Page to Support Guides
- ETD User Guide