Konfigurieren von sicherem E-Mail-Gateway für richtlinienbasiertes Journaling zum Schutz vor E-Mail-Bedrohungen

Inhalt

Einleitung

In diesem Dokument werden die Schritte zur Konfiguration des sicheren E-Mail-Gateways (SEG) zur Durchführung von richtlinienbasiertem Journaling für den sicheren E-Mail-Schutz vor Bedrohungen (SETD) beschrieben.

Voraussetzungen

Die Kenntnis der allgemeinen Einstellungen und Konfiguration des Cisco Secure Email Gateway (SEG) ist von Vorteil.

Verwendete Komponenten

Diese Konfiguration erfordert beides:

- Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 und höher
- Cisco Email Threat Defense (SETD)-Instanz.
- Threat Defence Connector (TDC). "Die definierte Verbindung zwischen den beiden Technologien."

"Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen aller Befehle verstehen."

Überblick

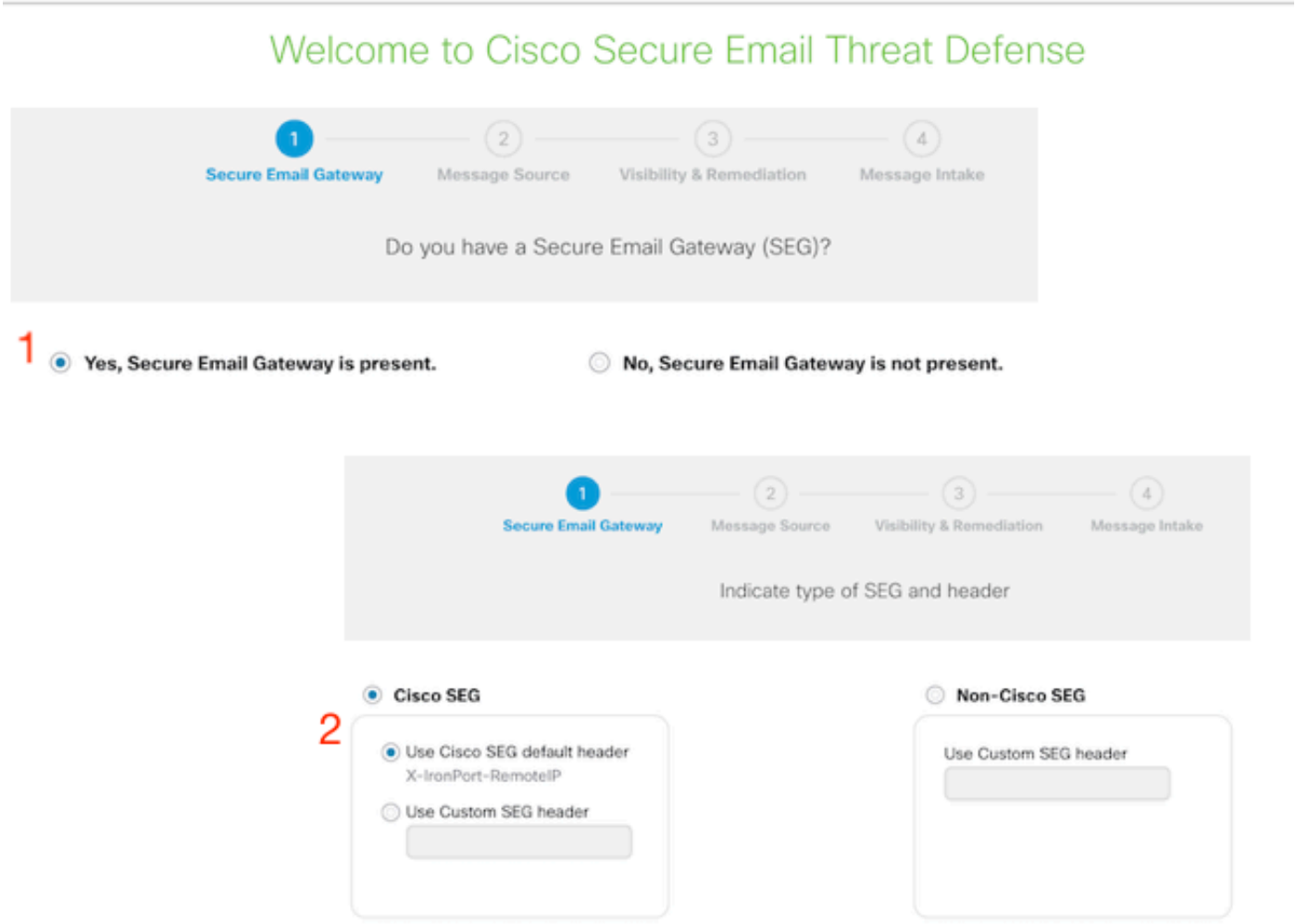
Die Cisco SEG kann für zusätzlichen Schutz in SETD integriert werden.

- Die SEG-Journalaktion überträgt die vollständige E-Mail für alle unschädlichen Nachrichten.
- Die SEG bietet die Möglichkeit, eingehende E-Mail-Flows basierend auf einer Übereinstimmung pro E-Mail-Policy auszuwählen.
- Die Option "SEG pro Richtlinie" bietet drei Optionen: "Keine Suche", "Standard-Nachrichteneingangsadresse" oder "Benutzerdefinierte Nachrichteneingangsadresse".
    - Die Standardeingangsadresse stellt das primäre SETD-Konto dar, das E-Mails für eine bestimmte Kontoinstanz akzeptiert.
    - Die benutzerdefinierte Nachrichteneingangsadresse stellt ein zweites SETD-Konto dar, das E-Mails für verschiedene definierte Domänen akzeptiert. Dieses Szenario gilt für komplexere SETD-Umgebungen.
- Journalnachrichten haben eine SEG Message ID (MID) und eine Destination Connection ID DCID
- Die Zustellungswarteschlange enthält einen Wert ähnlich einer Domäne, "the.tdc.queue", um SETD-Übertragungszähler zu erfassen.
    - Die aktiven Zähler für "the.tdc.queue" können hier angezeigt werden: cli>tophosts oder SEG Reporting > Delivery Status (nicht CES).
    - "the.tdc.queue" steht für den Threat Defense Connector (TDC), der einem Zieldomänennamen entspricht.

Konfigurieren

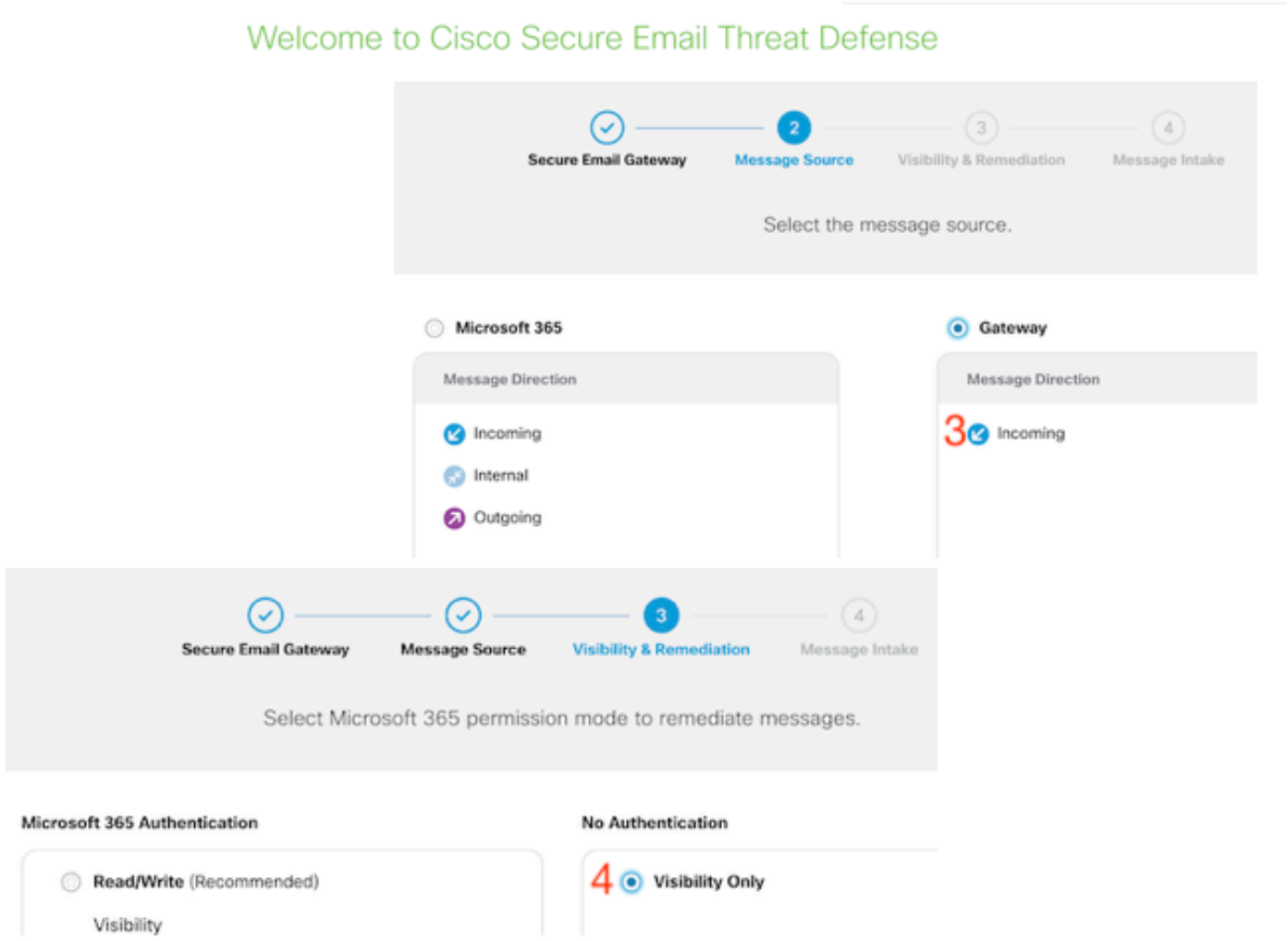
SETZEN Sie die ersten Einrichtungsschritte, um die "Message Intake Address" zu erzeugen.

1. Ja, Secure Email Gateway ist vorhanden.
2. Cisco SEG

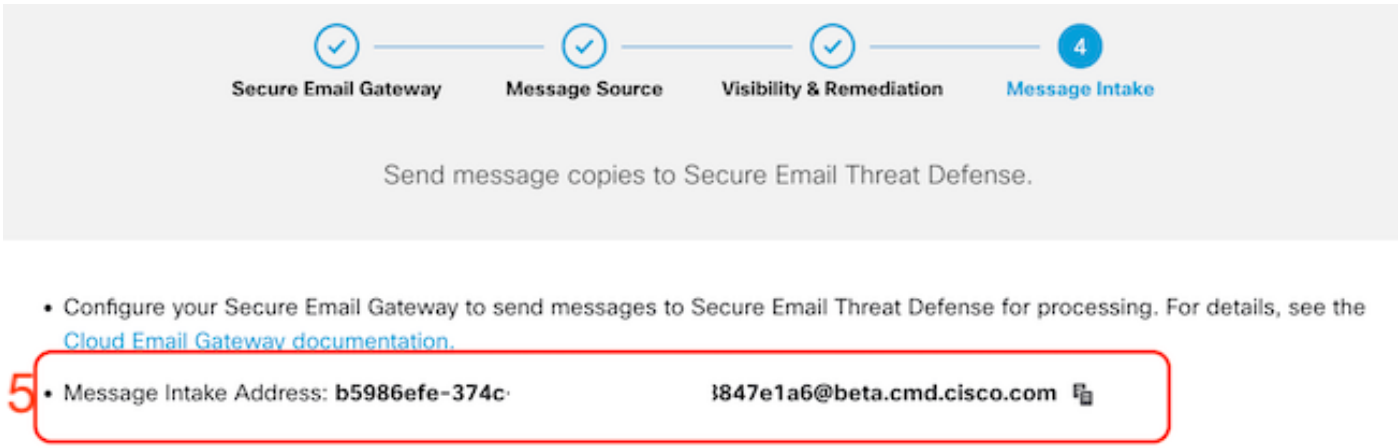


3. Richtung der Nachricht = Eingehend.

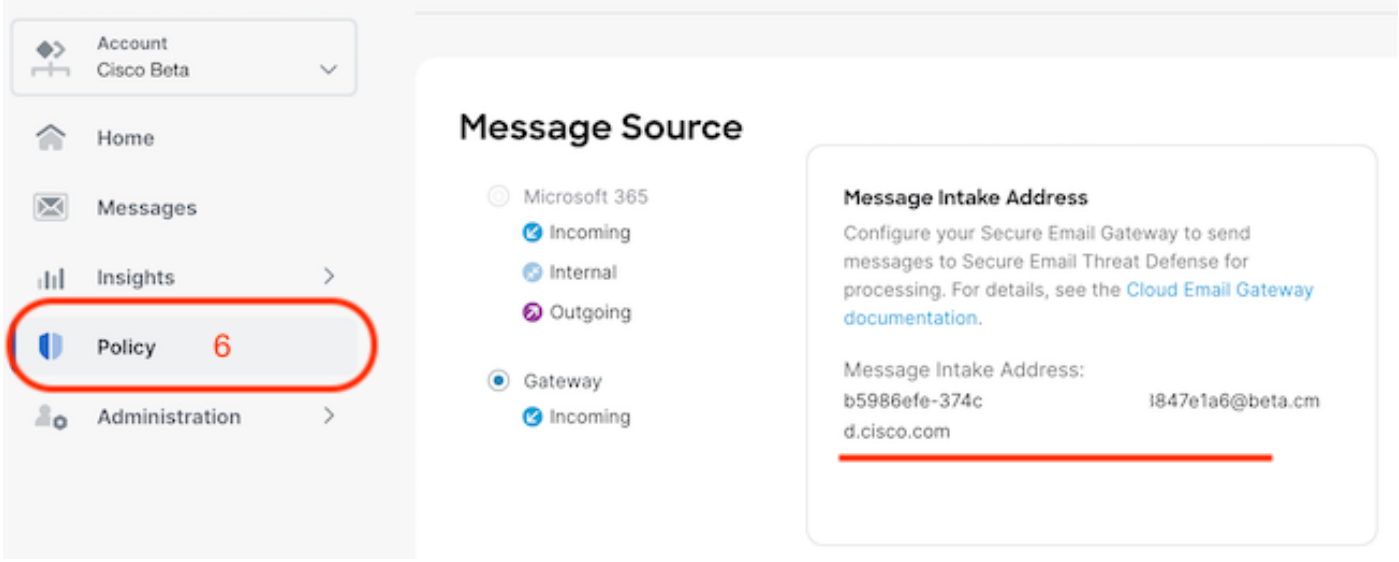
4. Keine Authentifizierung = Nur Transparenz.



5. Die Nachrichteneingangsadresse wird angezeigt, nachdem Schritt 4 akzeptiert wurde.



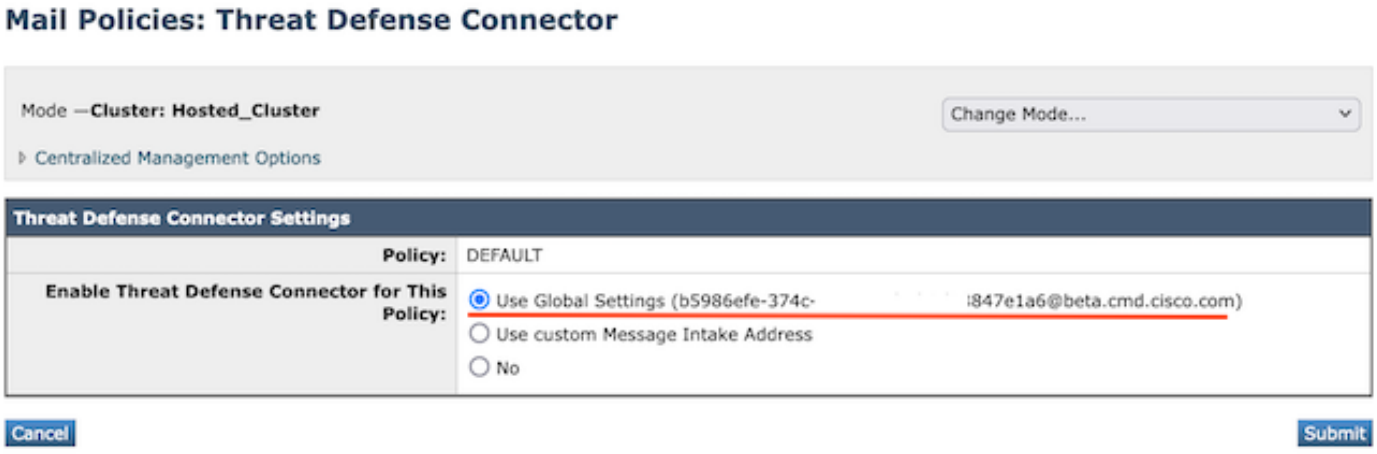
6. Wenn Sie die Nachrichteneingangsadresse nach der Einrichtung abrufen müssen, navigieren Sie zum Menü Richtlinie.



Wechseln Sie zur SEG WebUI, und navigieren Sie zu Security Services > Threat Defense Connector Settings.

Navigieren Sie zu Mail-Policys:

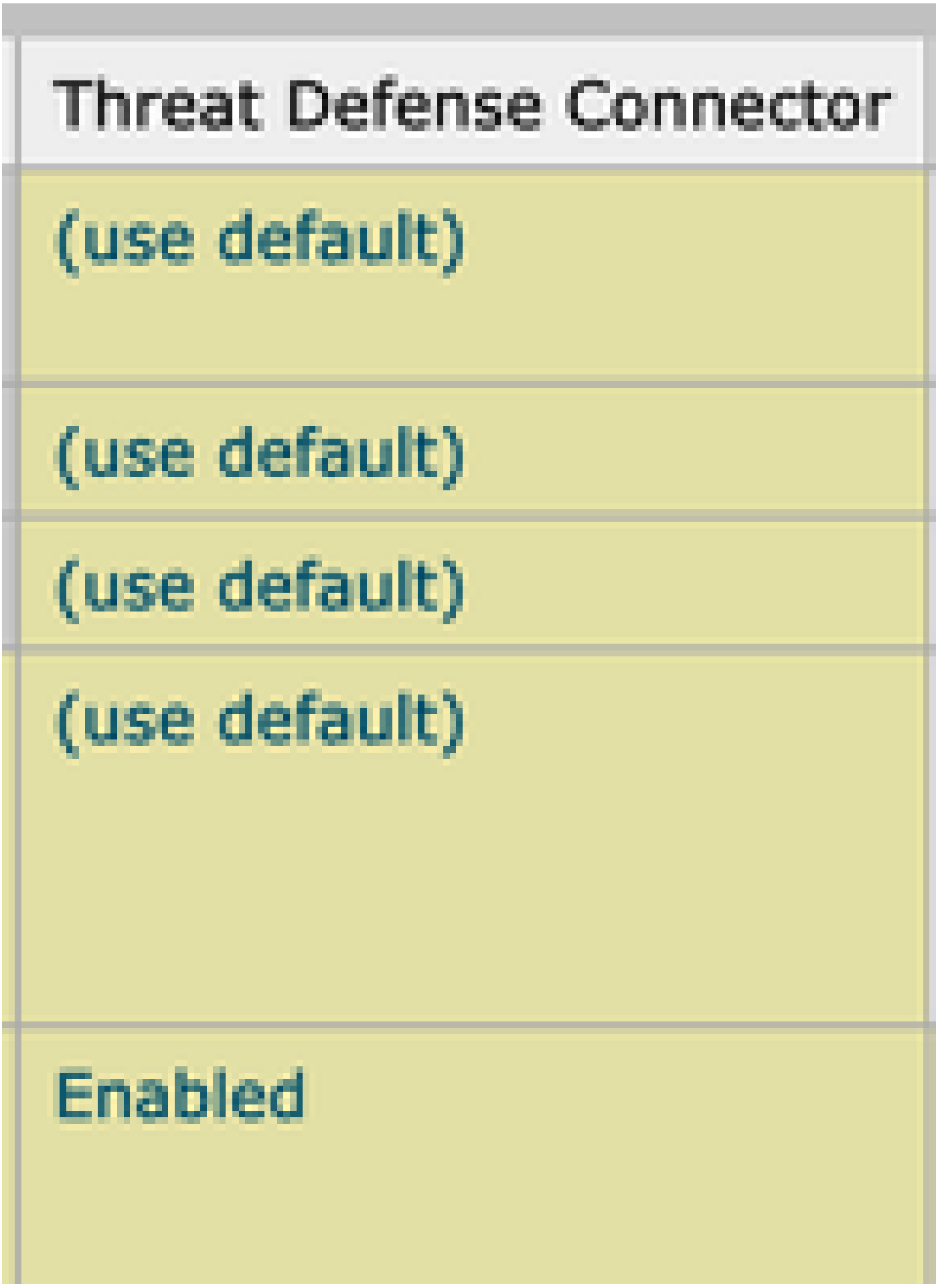
- Richtlinien für eingehende Mails
  - Der letzte Service auf der rechten Seite ist "Threat Defence Connector".
- Der Einstellungslink zeigt zum ersten Mal die Konfiguration "Disabled" (Deaktiviert) an.



Die benutzerdefinierte Nachrichteneingangsadresse wird mithilfe einer sekundären SETD-Instanz aufgefüllt.

Hinweis: Bei Verwendung der benutzerdefinierten Einzugsadresse ist es wichtig, die Abgleichkriterien für die Mail-Richtlinie zu konfigurieren, um den richtigen Domänenverkehr zu erfassen.

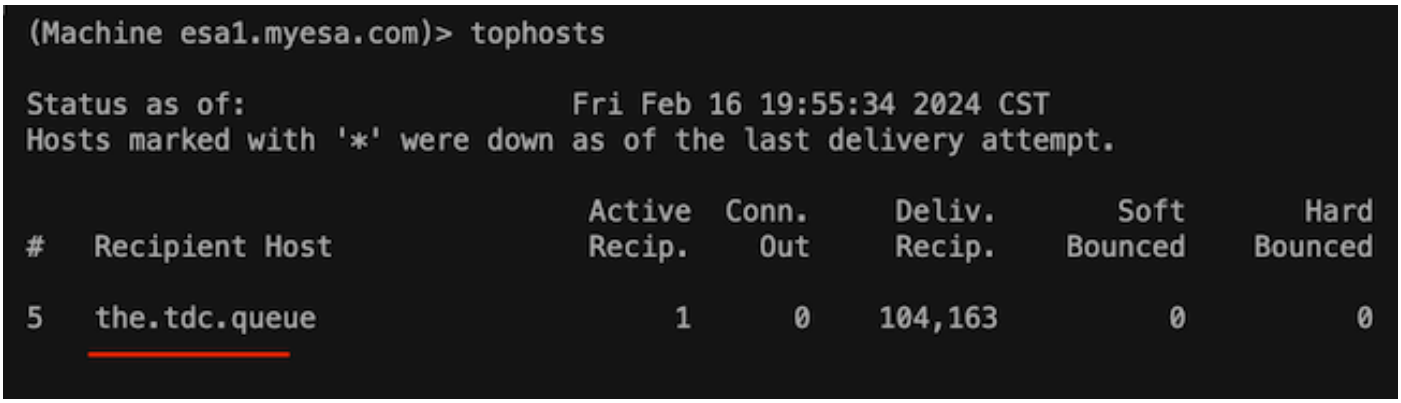
Die letzte Ansicht der Einstellung zeigt den Wert "Enabled" (Aktiviert) für den konfigurierten Service an.


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

Überprüfung

Sobald alle Schritte abgeschlossen sind, wird die E-Mail in das SETD Dashboard eingefügt.

Der SEG CLI-Befehl > tophosts zeigt die .tdc.queue-Zähler für aktive Zustellungen an.



Fehlerbehebung

TDC-Verbindungsverhalten:

- Mindestens 3 Verbindungen werden geöffnet, wenn Einträge in der Zielwarteschlange vorhanden sind.
- Weitere Verbindungen werden dynamisch über dieselbe Logik für reguläre E-Mail-Zielwarteschlangen hergestellt.
- Offene Verbindungen werden geschlossen, wenn die Warteschlange leer wird oder nicht genügend Einträge in der Zielwarteschlange vorhanden sind.
- Wiederholungen werden gemäß dem Wert in der Tabelle durchgeführt.
- Nachrichten werden aus der Warteschlange entfernt, nachdem die Wiederholungsversuche beendet wurden oder wenn sich die Nachricht zu lange in der Warteschlange befindet (120 Sek.)

Threat Defence Connector - Wiederholungsmechanismus

Fehlerfall	Erneut versuchen	Anzahl der Wiederholungen
SMTP 5xx-Fehler (außer 503/552)	Nein	–
SMTP 4xx-Fehler (einschließlich 503/552)	Ja	1
TLS-Fehler	Nein	–
Allgemeines Netzwerk \ Verbindungsfehler, DNS-Fehler usw.	Ja	1

Beispiel für TDC-E-Mail-Protokolle basierend auf den Zustellungsergebnissen

TDC-bezogene Protokolleinträge enthalten den Wert "TDC:" vor dem Protokolltext.

Das Beispiel zeigt eine normale TDC-Lieferung.

```
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
```

Das Beispiel zeigt einen Lieferfehler an, da die Meldung nach Ablauf des 120-Sekunden-Timeouts nicht zugestellt werden kann.

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

Das Beispiel zeigt einen Zustellungsfehler aufgrund eines TLS-Fehlers an.

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

In diesem Beispiel wird eine ungültige SETD-Journaladresse angezeigt, die zu einem Hard Bounce führt.

```
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) :
```

Die Nachrichtenverfolgung zeigt lediglich eine einzige Zeile an, die die erfolgreiche Zustellung der Nachricht an SETD anzeigt.

In diesem Beispiel wird aufgrund eines TLS-Fehlers ein Zustellungsfehler angezeigt.

16. Februar 2024 21:19:24 Uhr (GMT-06:00)	TDC: Die Nachricht 14501404 wurde mit Cisco Secure Email Threat Defense zum Scannen erfolgreich zugestellt.

Zugehörige Informationen

- Email Security - Einrichtungsleitfaden
- Cisco Secure Email Gateway Launch-Website für Support-Leitfäden
- ETD-Benutzerhandbuch

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.