# Secure Email Gateway Per-Policy 저널링을 Secure Email Threat Defense로 구성

## 목차



## 소개

이 문서에서는 SED(Secure Email Threat Defense)를 위한 정책별 저널링을 수행하도록 SEG(Secure Email Gateway)를 구성하는 단계를 설명합니다.

## 사전 요구 사항

Cisco SEG(Secure Email Gateway) 일반 설정 및 컨피그레이션에 대한 사전 지식은 유용합니다.

### 사용되는 구성 요소

이 설정에는 두 가지가 모두 필요합니다.

- Cisco SEG(Secure Email Gateway) AsyncOS 15.5.1 이상
- Cisco SETD(Email Threat Defense) 인스턴스
- TDC(Threat Defense Connector) "두 기술 간의 정의된 연결"

"이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 가동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다."

## 개요

Cisco SEG는 추가 보호를 위해 SETD와 통합할 수 있습니다.

- SEG 저널 작업은 모든 정상 메시지에 대한 전체 이메일을 전송합니다.
- SEG는 Per-Mail-Policy 일치를 기반으로 수신 메일 흐름을 선택적으로 선택하는 옵션을 제공합니다.
- SEG Per Policy 옵션은 No Scan(검사 없음), Default Message Intake address(기본 메시지 수

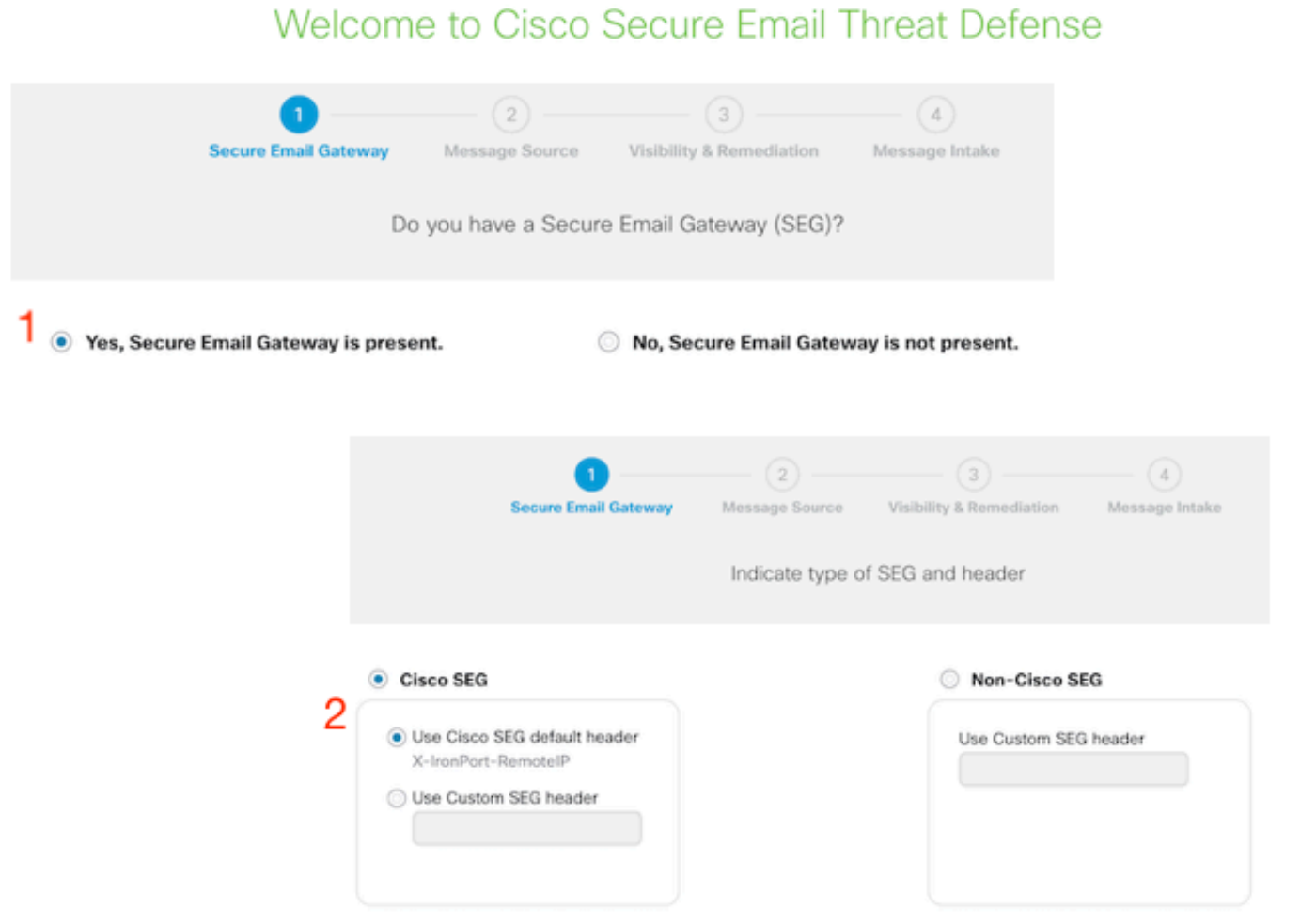
신 주소) 또는 Custom Message Intake Address(사용자 지정 메시지 수신 주소)의 3가지 선택 사항을 허용합니다.
    - Default Intake Address(기본 수신 주소)는 특정 계정 인스턴스에 대한 메일을 수락하는 기본 SETD 계정을 나타냅니다.
    - Custom Message Intake Address(맞춤형 메시지 수신 주소)는 서로 다른 정의된 도메인에 대한 메일을 수락하는 두 번째 SETD 어카운트를 나타냅니다. 이 시나리오는 좀 더 복잡한 SETD 환경에 적용됩니다.
- 저널된 메시지에는 SEG [메시지 ID(MID) 및 대상 연결 ID DCID가 있습니다.]
- Delivery Queue에는 SETD 전송 카운터를 캡처하기 위해 "the.tdc.queue" 도메인과 유사한 값이 포함되어 있습니다.
    - "the.tdc.queue" 활성 카운터는 cli>tophosts 또는 SEG Reporting > Delivery Status (non-CES)에서 확인할 수 있습니다.
    - "the.tdc.queue"는 대상 도메인 이름과 동일한 TDC(Threat Defense Connector)를 나타냅니다.

# 구성

"메시지 수신 주소"를 생성하기 위한 SETD 초기 설정 단계

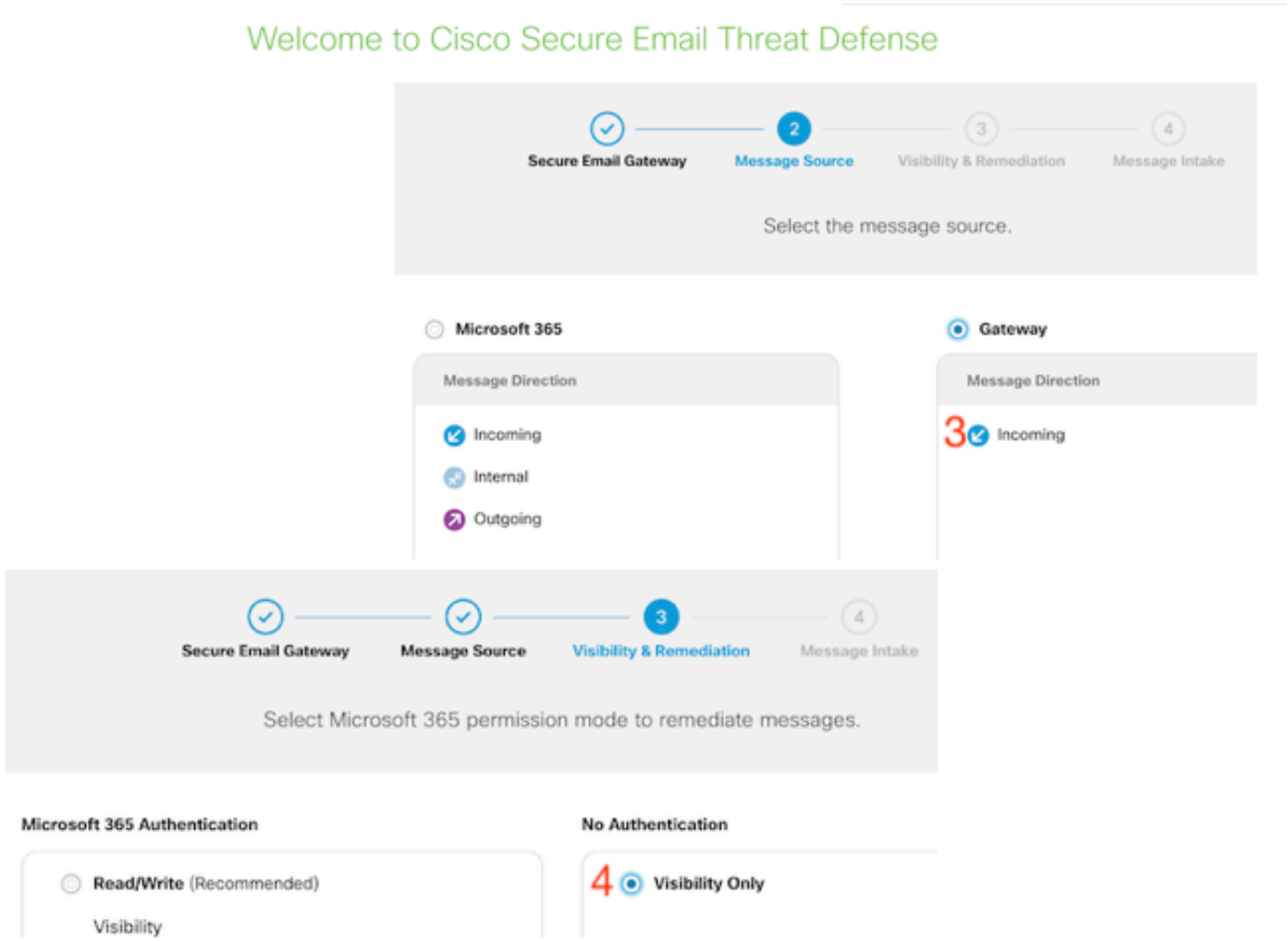
1. 예, Secure Email Gateway가 있습니다.
2. Cisco SEG

---

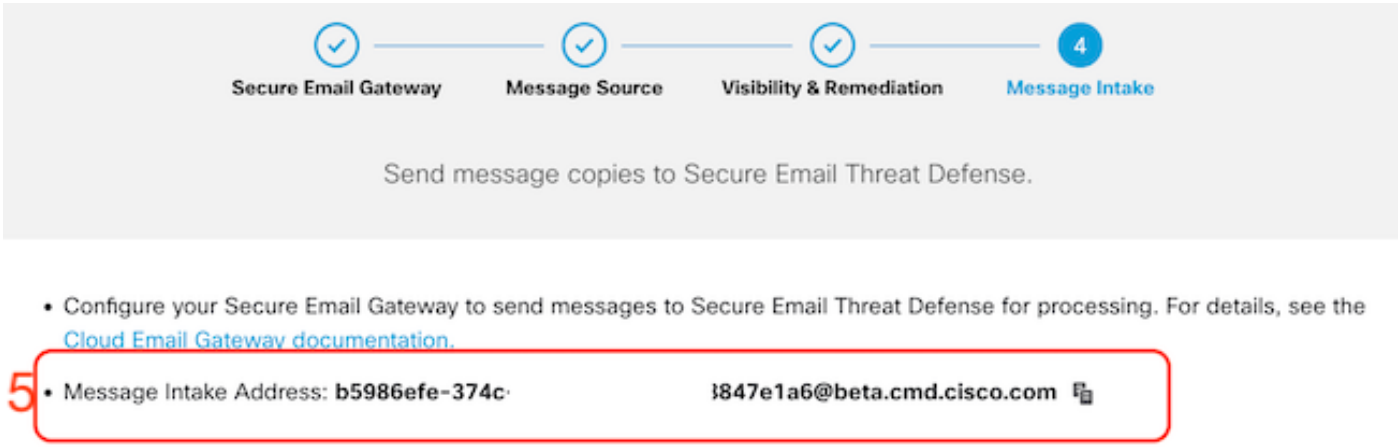


3. 메시지 방향 = 수신

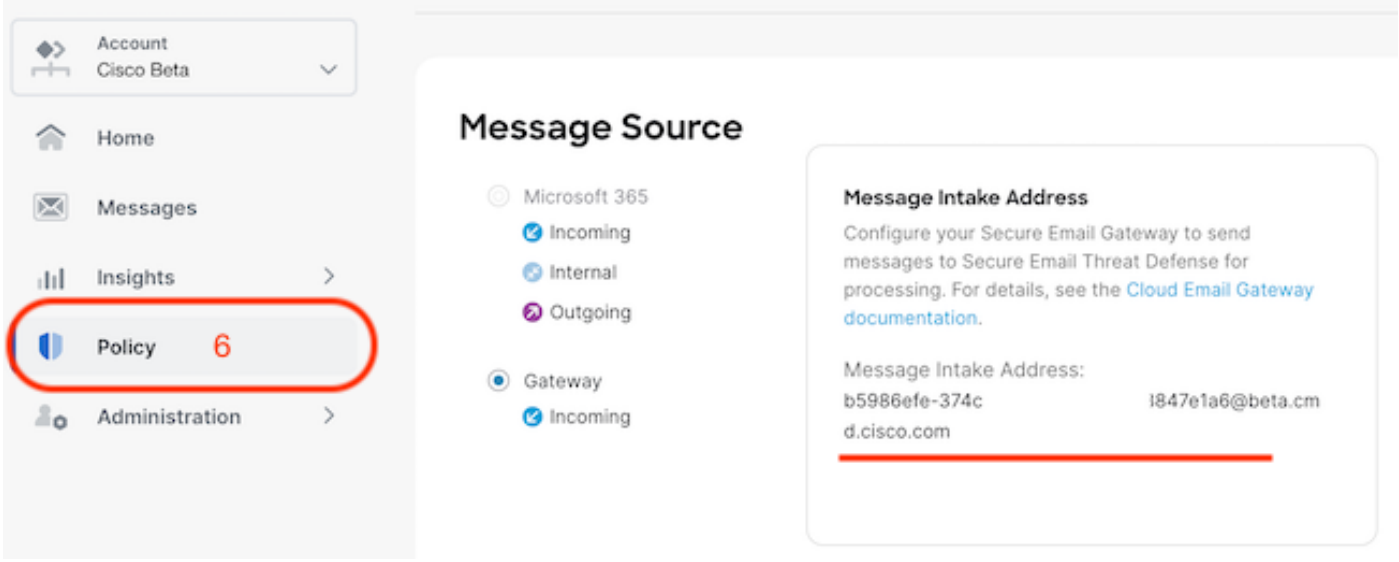
4. 인증 없음 = 가시성만




5. 4단계가 수락된 후 메시지 수신 주소가 표시됩니다.



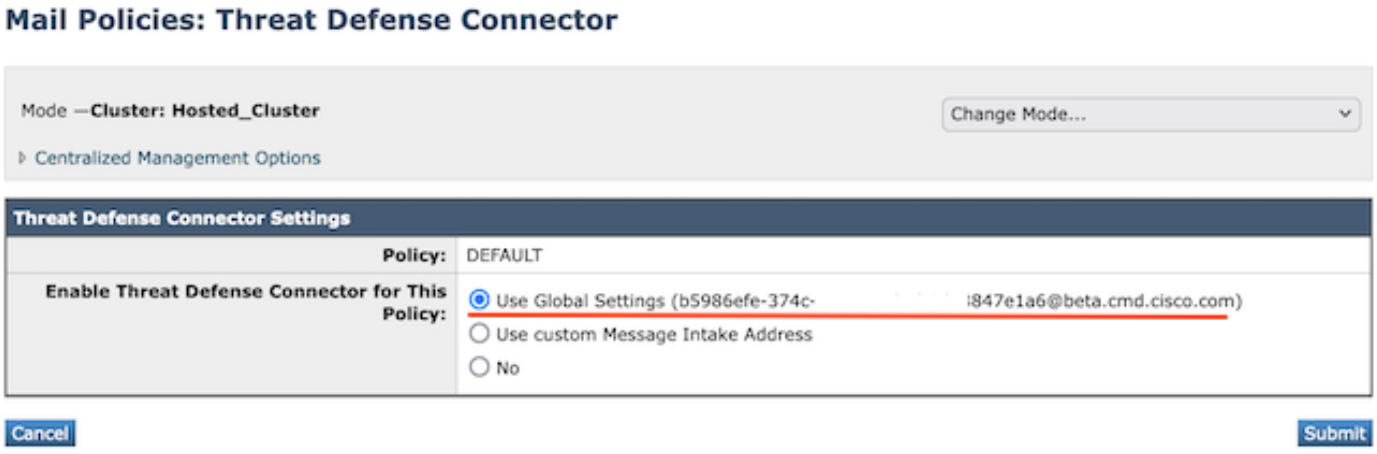

6. 설정 후 메시지 수신 주소를 검색해야 하는 경우 정책 메뉴로 이동합니다.




SEG WebUI로 전환하려면 Security Services(보안 서비스) > Threat Defense Connector Settings(Threat Defense 커넥터 설정)로 이동합니다.


Mail Policies(메일 정책):

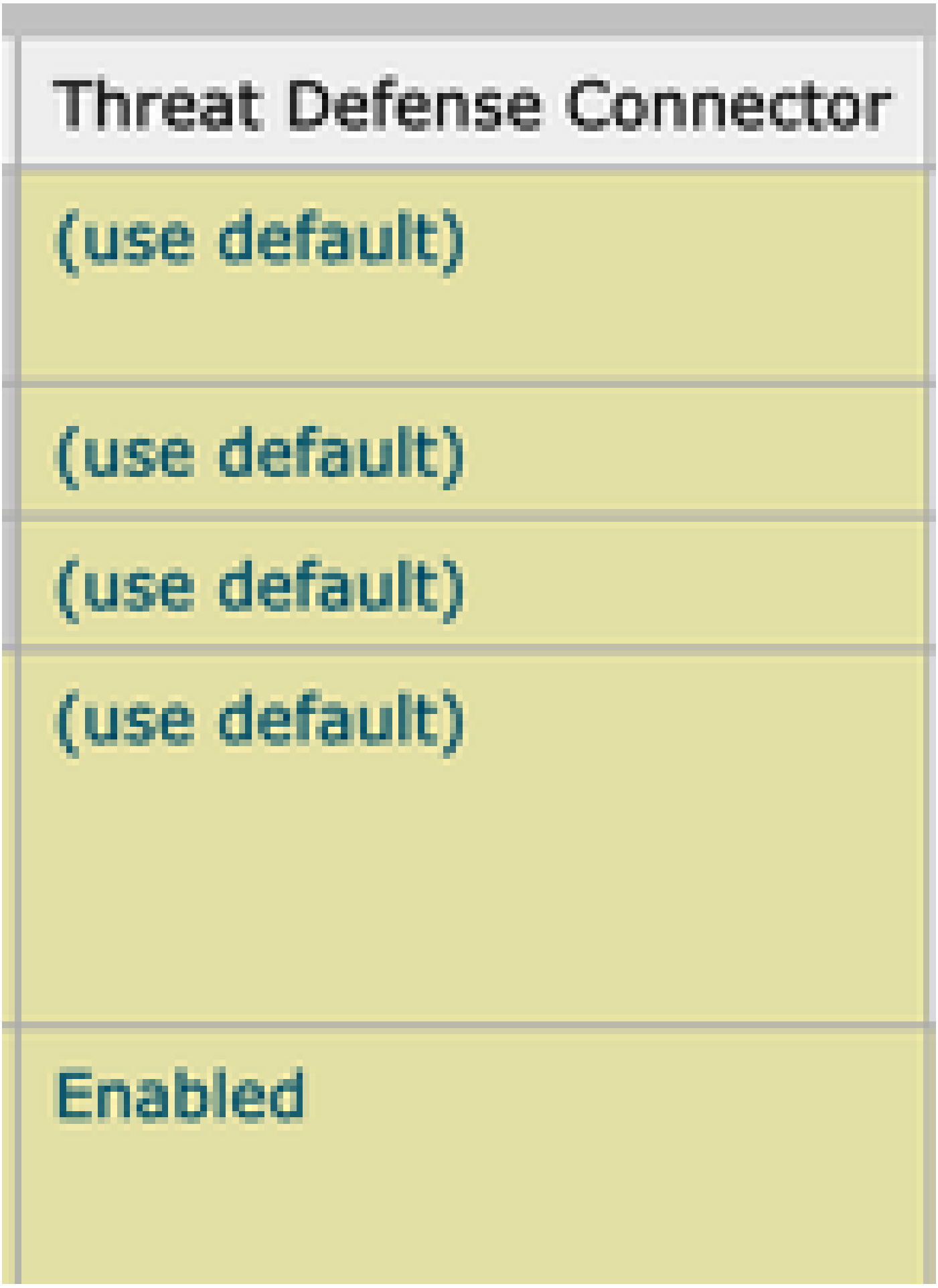
- 수신 메일 정책
  - 오른쪽의 마지막 서비스는 "Threat Defense Connector"입니다.
- 설정 링크는 첫 컨피그레이션에 대해 "Disabled(비활성화됨)"로 표시됩니다.




맞춤형 메시지 수신 주소는 보조 SETD 인스턴스를 사용하여 채워집니다.


참고: Custom Intake Address(맞춤형 수신 주소)를 활용하여 메일 정책 일치 기준을 구성하여 올바른 도메인 트래픽을 캡처하는 것이 중요합니다.

설정의 최종 보기에는 구성된 서비스에 대해 "Enabled(활성화됨)" 값이 표시됩니다.


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

## 다음을 확인합니다.

모든 단계가 완료되면 이메일에 SETD 대시보드가 입력됩니다.

SEG CLI 명령 > tophosts는 활성 전달에 대한.tdc.queue 카운터를 표시합니다.

```
(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
```

## 문제 해결

TDC 연결 동작:

- 대상 큐에 항목이 있을 때 최소 3개의 연결이 열립니다
- 추가 연결은 일반 이메일 대상 대기열에 대해 동일한 논리를 사용하여 동적으로 생성됩니다.
- 열린 연결은 큐가 비어 있거나 대상 큐에 충분한 항목이 없으면 닫힙니다.
- 재시도는 테이블의 값에 따라 수행됩니다.
- 메시지가 대기열에서 너무 오래(120초) 또는 재시도가 모두 완료된 후 메시지가 대기열에서 제거됩니다.

Threat Defense 커넥터 재시도 메커니즘

| 오류 사례 | 다시 시도 완료 | 재시도 횟수 |
|---|---|---|
| SMTP 5xx 오류(503/552 제외) | 아니요 | 해당 없음 |
| SMTP 4xx 오류(503/552 포함) | 예 | 1 |
| TLS 오류 | 아니요 | 해당 없음 |
| 일반 네트워크 \ 연결 오류, DNS 오류 등 | 예 | 1 |

제공 결과를 기반으로 한 샘플 TDC 메일 로그

TDC 관련 로그 엔트리는 로그 텍스트 이전의 TDC: 값을 포함한다.

이 샘플은 정상적인 TDC 전달을 나타냅니다.

```
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
```

이 샘플은 120초 시간 초과가 만료된 후 전달할 수 없는 메시지로 인해 전달 오류를 표시합니다

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

샘플은 TLS 오류로 인해 전달 오류를 나타냅니다.

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

이 샘플은 잘못된 SETD 저널 주소를 나타냅니다. 그러면 하드 반송이 발생합니다.

```
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) :
```

메시지 추적은 SETD에 메시지를 성공적으로 전달했음을 나타내는 한 줄만 표시합니다.

이 샘플은 TLS 오류로 인해 배달 오류를 표시합니다.

| | |
|---|---|
| 2024년 2월 16일 21:19:24 (GMT -06:00) | TDC: Cisco Secure Email Threat Defense를 사용한 스캐닝에 대한 메시지 14501404이 성공적으로 제공되었습니다. |

## 관련 정보

- 이메일 보안 설정 가이드
- Cisco Secure Email Gateway 시작 페이지 - 지원 가이드
- ETD 사용 설명서

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.