



# Cisco Secure Email Threat Defense FAQ

최초 게시 날짜: 2021년 4월 26일

최종 업데이트: 02-27-2023





# 목차

- 소개 ..... 3
- 설정 상황 ..... 5
  - Secure Email Threat Defense 를 설정하는 데 Microsoft 365 전역 관리자 권한이 필요한 이유는 무엇입니까? ..... 5
  - Malware Analytics/Threat Grid 에서 환영 이메일을 받은 이유는 무엇입니까? ..... 5
  - 저널 주소를 찾으려면 어떻게 해야 합니까? ..... 5
  - Microsoft 365 테넌트를 등록하려고 할 때 등록 오류가 표시되는 이유는 무엇입니까? ..... 5
  - Cisco 는 저널 데이터를 얼마 동안 보존합니까? ..... 5
  - 사용자를 둘 이상의 Secure Email Threat Defense 인스턴스에 추가할 수 있습니까? ... 5
- 로그인 문제 ..... 7
  - Secure Email Threat Defense 에 로그인하는 동안 발생하는 문제에 대한 자세한 정보를 찾으려면 어떻게 해야 합니까? ..... 7
  - 내 이메일 주소로 로그인할 수 없는 이유는 무엇입니까? ..... 7
  - 비밀번호를 재설정하려면 어떻게 해야 합니까? ..... 7
  - 내 Microsoft 계정으로 SecureX 에 로그인하려고 할 때 400 Bad Request( 잘못된 요청 ) 오류가 표시되는 이유는 무엇입니까? ..... 7
  - SecureX 애플리케이션 포털에서 Secure Email Threat Defense 에 액세스하려면 어떻게 해야 합니까? ..... 7
  - Secure Email Threat Defense 인스턴스 간에 전환하려면 어떻게 해야 합니까? ..... 7
  - Secure Email Threat Defense 의 운영 상태를 어떻게 확인할 수 있습니까? ..... 8
- Secure Email Threat Defense 및 Microsoft 365 ..... 9
  - Secure Email Threat Defense 는 Microsoft 365 에서 허용 목록의 발신자 또는 도메인을 준수합니까? ..... 9
  - Secure Email Threat Defense 이 ( 가 ) 사용자가 Outlook 의 정크 메일에 대해 수행하는 작업을 준수합니까? ..... 9
  - 저널링 크기 제한은 얼마입니까? ..... 9
  - 일부 도메인이 Secure Email Threat Defense 에 표시되지 않는 이유는 무엇입니까? ... 9
  - Microsoft 365 의 저널링에 대한 자세한 내용은 어디에서 확인할 수 있습니까? ... 9
- 메시지 및 검색 ..... 11
  - 메시지가 잘못 분류되었음을 Cisco 에 알리려면 어떻게 해야 합니까? ..... 11
  - 이미 재분류한 발신자로부터 이메일이 계속 수신되는 이유는 무엇입니까? ..... 11

---

혼합 이메일이란 무엇입니까?.....	11
일부 메시지가 혼합으로 분류된 내부 메일 목록으로 전송되는 이유는 무엇입니까?.....	11
일부 메시지가 내 메시지 페이지에 두 번 표시되는 이유는 무엇입니까?.....	11
비공개 수신자란 무엇을 의미합니까?.....	11
지원 .....	13
Secure Email Threat Defense 문서에 액세스하려면 어떻게 해야 합니까?.....	13
고객 지원에 문의하려면 어떻게 합니까?.....	13
새로운 기능에 대한 질문이 있는 경우 어떻게 해야 합니까?.....	13



## 소개

이 문서에는 Cisco Secure Email Threat Defense( 이전 명칭 Cisco Secure Email Cloud Mailbox) 에 대한 FAQ( 자주 묻는 질문 )가 포함되어 있습니다 . Secure Email Threat Defense 사용에 대한 자세한 내용은 [Cisco Secure Email Threat Defense 사용 설명서](#)를 참조하십시오 .





## 설정 상황

Secure Email Threat Defense 를 설정하는 데 Microsoft 365 전역 관리자 권한이 필요한 이유는 무엇입니까?

Cisco 는 Microsoft 365 자격 증명을 물리적으로 수락하지 않으며 전역 관리자의 자격 증명을 캐시하거나 저장하지도 않습니다 . Secure Email Threat Defense Microsoft 의 API 에 대한 인증 토큰을 발급할 수 있도록 Microsoft 의 Azure 애플리케이션 등록 프로세스로 리디렉션합니다 . 전역 관리자만 이 토큰에 권한을 부여할 수 있습니다 .

자세한 내용은 애플리케이션의 관리자 권한에 대한 Microsoft 설명서를 참조하십시오 .

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent/>

Malware Analytics/Threat Grid 에서 환영 이메일을 받은 이유는 무엇입니까?

최소 Cisco Secure Malware Analytics( 이전 명칭 Threat Grid) 계정은 Secure Email Threat Defense 계정 생성 프로세스의 일부로 생성됩니다 . 새 Malware Analytics 계정이 보유하고 있을 수 있는 기존 Malware Analytics 계정에 연결되지 않았습니다 . Secure Email Threat Defense 설정을 위해 Malware Analytics 계정에 대해 어떤 작업도 수행할 필요가 없습니다 .

저널 주소를 찾으려면 어떻게 해야 합니까?

Secure Email Threat Defense 설정 페이지에 저널 주소가 표시됩니다 . 초기 설정 후 이를 찾아야 하는 경우 , Account Details( 어카운트 세부 정보 ) 섹션의 **Settings( 설정)**( 톱니바퀴 아이콘 ) > **Administration( 관리 )** > **Business( 비즈니스 )** 페이지에서 찾을 수 있습니다 .

Microsoft 365 테넌트를 등록하려고 할 때 등록 오류가 표시되는 이유는 무엇입니까?

이전에 다른 Secure Email Threat Defense 계정에 등록한 테넌트를 등록하려고 하면 권한 부여가 실패합니다 . Secure Email Threat Defense 동일한 Microsoft 테넌트 ID 를 사용하는 여러 계정을 허용하지 않습니다 .

Cisco 는 저널 데이터를 얼마 동안 보존합니까?

각 저널 메시지는 거의 즉시 메타데이터 추출 및 콘텐츠 분석을 거친 후 삭제됩니다 . 저널 메시지에 포함된 모든 첨부 파일은 추가 분석 또는 샌드박싱을 위해 최소 24 시간 동안 보존됩니다 . 저널에서 추출된 메타데이터는 90 일 동안 저장됩니다 .

사용자를 둘 이상의 Secure Email Threat Defense 인스턴스에 추가할 수 있습니까?

동일한 SecureX 로그인 계정을 사용하여 여러 Secure Email Threat Defense 인스턴스에 액세스할 수 있습니다 . 이렇게 하면 로그아웃한 후 별도의 계정으로 다시 로그인할 필요 없이 각 인스턴스를 더 쉽게 추적할 수 있습니다 .

**Settings( 설정)**( 톱니바퀴 아이콘 ) > **Administration( 관리 )** > **Users( 사용자 )** 에서 새 사용자를 생성하여 추가 인스턴스에 사용자를 추가합니다 . Secure Email Threat Defense 동일한 SecureX 로그인을 사용하는 계정은 사용자 메뉴에서 사용할 수 있습니다 . 이 액세스는 동일한 지역 ( 북미 또는 유럽 ) 의 Secure Email Threat Defense 계정으로 제한됩니다 .







## 로그인 문제

Secure Email Threat Defense 에 로그인하는 동안 발생하는 문제에 대한 자세한 정보를 찾으려면 어떻게 해야 하나요?

Secure Email Threat Defense 사용자 인증 관리를 위해 Cisco 의 SecureX 로그인 SSO 솔루션을 사용합니다. FAQ 를 포함하여 SecureX 로그인에 대한 자세한 내용은 [Cisco SecureX 로그인 빠른 시작 가이드](#)를 참조하십시오.

내 이메일 주소로 로그인할 수 없는 이유는 무엇입니까?

SecureX 로그인에 사용 중인 이메일 주소가 Secure Email Threat Defense 계정과 연결된 이메일과 일치하는지 확인하십시오. 일부 고객은 여러 이메일 주소를 사용하는 SecureX 로그인 계정을 보유하고 있을 수 있습니다. Secure Email Threat Defense 단일 사용자에게 대해 여러 이메일 주소를 지원하지 않습니다. Secure Email Threat Defense 계정을 생성할 때 사용한 이메일 주소를 사용하여 로그인해야 합니다. 어떤 이메일 주소가 사용되었는지 모르는 경우 Secure Email Threat Defense 관리자에게 문의하십시오.

비밀번호를 재설정하려면 어떻게 해야 하나요?

SecureX 로그인 프로세스 중에 비밀번호를 입력하라는 메시지가 표시됩니다. **Forgot password(비밀번호 분실)** 를 클릭하여 **Reset Password(비밀번호 재설정)** 페이지로 이동합니다.

내 Microsoft 계정으로 SecureX 에 로그인하려고 할 때 400 Bad Request(잘못된 요청) 오류가 표시되는 이유는 무엇입니까?

Microsoft 365에서는 계정에 이름과 성이 정의되어 있지 않아도 됩니다. 성이 없는 Microsoft 계정으로 인증을 시도하면 SecureX 로그인에서 다음 오류를 반환합니다.

*400 잘못된 요청 사용자를 만들 수 없습니다. 필수 속성이 누락되었습니다.*

이 문제를 해결하려면 Microsoft 365 계정에 이름과 성이 모두 정의되어 있는지 확인하십시오.

SecureX 애플리케이션 포털에서 Secure Email Threat Defense 에 액세스하려면 어떻게 해야 하나요?

SecureX 애플리케이션 포털에서 Secure Email Threat Defense 에 액세스하려면 해당 지역 (북미 또는 유럽)에서 Secure Email Threat Defense 아이콘을 찾습니다.

Secure Email Threat Defense 인스턴스 간에 전환하려면 어떻게 해야 하나요?

동일한 SecureX 로그인 계정을 사용하여 여러 Secure Email Threat Defense 인스턴스에 액세스할 수 있습니다. 이렇게 하면 로그아웃한 후 별도의 계정으로 다시 로그인할 필요 없이 각 인스턴스를 더 쉽게 추적할 수 있습니다. Secure Email Threat Defense 사용자 메뉴에서 동일한 SecureX 로그인을 사용하는 계정을 사용할 수 있습니다. 이는 동일한 지역 (북미 또는 유럽)의 계정으로 제한됩니다.

## Secure Email Threat Defense 의 운영 상태를 어떻게 확인할 수 있습니까 ?

Secure Email Threat Defense 가 다운될 수 있거나 문제의 가능성이 있는 것으로 의심되는 경우, <https://ciscosecureemailthreatdefense.statuspage.io> 에서 상태 페이지를 확인하십시오.



# Secure Email Threat Defense 및 Microsoft 365

## Secure Email Threat Defense 는 Microsoft 365 에서 허용 목록의 발신자 또는 도메인을 준수합니까?

예. Secure Email Threat Defense 는 스팸 및 그레이메일 메시지에 대해 Microsoft 365 의 스팸 필터 허용 목록에 추가된 발신자 및 도메인을 준수합니다. MS 허용 목록은 악성 또는 피싱 판정에 적용되지 않습니다.

기본 Exchange 관리 센터에서는 **Exchange admin center(Exchange 관리 센터) > protection( 보호 ) > spam filter( 스팸 필터 )** 에서 액세스할 수 있습니다.

새로운 Microsoft 365 보안 센터에서는 <https://security.microsoft.com/antispam> 에서도 이 설정에 액세스할 수 있습니다.

Microsoft 의 MSAllowList 헤더에 대한 최근 변경 사항으로 인해, 조직에서 개별 사용자가 사서함에서 허용 목록을 구성하도록 허용하고 메시지가 사용자의 허용 목록에 포함되는 경우 Secure Email Threat Defense 에서 Microsoft 허용 목록이 항상 적용되는 것은 아닙니다. Secure Email Threat Defense 에서 이러한 설정을 준수하도록 하려면 Policy( 정책 ) 페이지에서 **Do not remediate Microsoft Safe Sender messages with Spam or Graymail verdicts(Microsoft 수신 허용 - 발신자 메시지를 스팸 또는 그레이메일 판정으로 치료하지 않음)** 확인란을 선택합니다. 수신 허용 - 발신자 플래그는 스팸 및 그레이메일 판정에는 적용되지만 악성 및 피싱 판정에는 적용되지 않습니다. 즉, 스팸 또는 그레이메일 판정이 있는 수신 허용 - 발신자 메시지는 치료되지 않습니다.

## Secure Email Threat Defense 이 ( 가 ) 사용자가 Outlook 의 정크 메일에 대해 수행하는 작업을 준수합니까?

사용자는 **Never Block Sender( 발신자 차단 안 함 )** 또는 **Add to Safe Senders( 수신 허용 - 발신자에 추가 )** 와 같은 Outlook 정크 옵션을 사용하여 이메일을 표시할 수 있습니다. Secure Email Threat Defense 에서 이러한 설정을 준수하도록 하려면 Policy( 정책 ) 페이지에서 **Do not remediate Microsoft Safe Sender messages with Spam or Graymail verdicts(Microsoft 수신 허용 - 발신자 메시지를 스팸 또는 그레이메일 판정으로 치료하지 않음)** 확인란을 선택합니다. 수신 허용 - 발신자 플래그는 스팸 및 그레이메일 판정에는 적용되지만 악성 및 피싱 판정에는 적용되지 않습니다. 즉, 스팸 또는 그레이메일 판정이 있는 수신 허용 - 발신자 메시지는 치료되지 않습니다.

## 저널링 크기 제한은 얼마입니까?

150MB 를 초과하는 메시지는 Microsoft 365 에서 저널링되지 않습니다.

## 일부 도메인이 Secure Email Threat Defense 에 표시되지 않는 이유는 무엇입니까?

Secure Email Threat Defense 테넌트와 연결된 이메일 기능이 있는 도메인을 가져옵니다. 도메인에 이메일 기능이 없으면 Secure Email Threat Defense 에 표시되지 않습니다.

## Microsoft 365 의 저널링에 대한 자세한 내용은 어디에서 확인할 수 있습니까?

Microsoft 설명서를 참조하십시오. <https://docs.microsoft.com/en-us/exchange/security-and-compliance/journaling/journaling>





# 메시지 및 검색

## 메시지가 잘못 분류되었음을 Cisco 에 알려려면 어떻게 해야 하나요 ?

메시지가 올바르게 분류되지 않았다고 생각되는 경우 (오탐 또는 미탐) 메시지를 **재분류**할 수 있습니다. 메시지가 **Cisco Talos**의 검토를 위해 대기열에 추가됩니다. **Talos**는 피드백을 사용하여 향후 분류에 영향을 줄 수 있습니다.

## 이미 재분류한 발신자로부터 이메일이 계속 수신되는 이유는 무엇입니까 ?

재분류는 선택한 메시지의 관정에만 영향을 미칩니다. 선택한 발신자가 보낸 향후 메시지에 대한 변경 사항이나 메시지 내용을 기반으로 한 변경 사항은 표시되지 않습니다. 메시지가 **Cisco Talos**의 검토를 위해 대기열에 추가됩니다. **Talos**는 피드백을 사용하여 향후 분류에 영향을 줄 수 있습니다.

**SEG(Secure Email Gateway)**가 있는 경우 **Settings( 설정)**( 톱니바퀴 아이콘 ) > **Policy( 정책)** 페이지에서 이를 표시해야 합니다. 이 정보는 오탐을 줄이는 데 도움이 됩니다.

오탐 스캔 또는 그레이메일 메시지의 경우 **관정 재정의**의 메시지 규칙을 추가하는 것이 좋습니다.

이 문제가 계속되면 **지원, 13 페이지**에 문의하십시오.

## 혼합 이메일이란 무엇입니까 ?

혼합으로 분류된 이메일은 내부 주소에서 내부 및 외부 수신자 모두에게 전송되는 이메일입니다.

## 일부 메시지가 혼합으로 분류된 내부 메일 목록으로 전송되는 이유는 무엇입니까 ?

**Microsoft 365**에서 여러 가지 방법으로 메일 목록을 만들 수 있습니다. 메일 그룹이 **Microsoft 365** 그룹 또는 외부 메일 그룹으로 생성된 경우 내부 및 외부 수신자를 모두 목록에 포함할 수 있습니다. **Microsoft**는 이러한 메시지를 혼합으로 보고합니다. 이는 **Secure Email Threat Defense**의 치료에 영향을 주지 않습니다.

## 일부 메시지가 내 메시지 페이지에 두 번 표시되는 이유는 무엇입니까 ?

중복 항목은 **Microsoft**가 단일 이메일에 대해 여러 저널을 생성한 결과입니다. 이 문제는 여러 가지 이유로 발생할 수 있습니다. 예를 들어 **Exchange** 관리자가 설정한 메일 규칙 또는 도메인이 아닌 사용자가 있는 그룹에 전송된 메일이 해당됩니다.

## 비공개 수신자란 무엇을 의미합니까 ?

비공개 수신자는 이메일에 나열되지 않은 수신자를 의미합니다. 예를 들어 **BCC( 숨은 참조)**가 수신자에게 전송되는 경우를 예로 들 수 있습니다. **Secure Email Threat Defense BCC** 수신자를 추적하지 않지만 탐지 및 치료는 영향을 받지 않습니다.





## 지원

### Secure Email Threat Defense 문서에 액세스하려면 어떻게 해야 하나요 ?

도움말 메뉴를 사용하거나 다음 링크를 통해 **Secure Email Threat Defense** 에서 직접 **Secure Email Threat Defense** 문서에 액세스할 수 있습니다.

- [Cisco Secure Email Threat Defense 사용 설명서](#)
- [Cisco Secure Email Threat Defense 릴리스 노트](#)

### 고객 지원에 문의하려면 어떻게 하나요 ?

**Secure Email Threat Defense PoV(Proof of Value)** 평가 고객인 경우 [cmd-support@cisco.com](mailto:cmd-support@cisco.com) 으로 이메일을 보내십시오.

전체 라이선스가 있는 **Secure Email Threat Defense** 고객인 경우 :

- 온라인 지원 케이스를 엽니다 : <https://www.cisco.com/c/en/us/support/index.html>
- 이메일 [TAC@cisco.com](mailto:TAC@cisco.com)
- 여기에 있는 전 세계 전화 번호로 **Cisco TAC** 에 문의하십시오 .  
<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

**참고 :** 케이스를 열려면 **Secure Email Threat Defense** 계약을 **cisco.com** 어카운트에 연결해야 합니다 . **cisco.com** 어카운트가 아직 없는 경우 [여기](#)로 이동하여 어카운트를 생성하십시오 .

### 새로운 기능에 대한 질문이 있는 경우 어떻게 해야 하나요 ?

새로운 기능에 대한 질문이 있거나 새로운 기능에 대한 아이디어가 있는 경우 [cmd-bu@cisco.com](mailto:cmd-bu@cisco.com) 으로 이메일을 보낼 수 있습니다.





## 번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.