

# O365로 Cloud Email Security 공유 사서함 구성

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[설정](#)

[1단계. EntraID에서 애플리케이션 생성](#)

[권한 할당](#)

[자격 증명 생성](#)

[2단계. Cisco Cloud Email Security 구성](#)

[테스트](#)

[추가 정보](#)

---

## 소개

이 문서에서는 Exchange Online(O365)의 공유 사서함에 대한 Cisco Secure Email Gateway 스팸 격리를 보기 위한 구성에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

컨피그레이션을 계속하려면 다음 요구 사항을 충족해야 합니다.

- 스팸 격리에 액세스하기 위한 SAML 인증 구현
- Exchange Online의 사용자 및 공유 사서함에 대한 정보입니다.
- 필요한 공유 사서함에 사용자를 할당합니다.
- EntraID 포털에 액세스하여 애플리케이션을 생성합니다.
- CES 보고 콘솔에 액세스하여 공유 사서함 서비스를 활성화합니다.

모든 요구 사항이 충족되면 아래의 컨피그레이션 단계를 따를 수 있습니다.

### 사용되는 구성 요소

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 배경 정보

이러한 이메일을 관리하기 위한 대체 구성도 사용할 수 있습니다. 여기에는 인증 없이 전자 메일을 릴리스할 수 있도록 스팸 알림을 사용하도록 설정하거나 플래그가 지정된 전자 메일을 Exchange Online의 해당 사서함의 정크 폴더로 리디렉션하는 사용자 지정 정책을 만드는 것이 포함됩니다.

## 설정

### 1단계. EntraID에서 애플리케이션 생성

Cisco Secure Email Gateway를 구성하기 전에 EntraID에서 필요한 액세스를 설정합니다.

1. EntraID에 액세스합니다.
2. App registrations(앱 등록)를 선택합니다.
3. New Registration(새 등록)을 클릭하고 이름으로 "Cisco CES Shared Mailbox"를 사용합니다.
4. 이 조직 디렉터리의 Accounts only(이메일SEC데모만 - 단일 테넌트)를 선택합니다.
5. Redirect URL(리디렉션 URL)에서 web(웹)을 선택하고 SPAM Quarantine(스팸 격리) 영역의 링크를 like <https://XXXXX-YYYY.ipmx.com/> 형식으로 [입력합니다](#).
6. Register(등록)를 클릭합니다.

### 권한 할당

1. 새로 만든 응용 프로그램을 엽니다.
2. API 권한으로 이동합니다.
3. 다음 Microsoft Graph 권한을 할당합니다.
  - Mail.Read.Shared: 위임, 사용자 및 공유 메일 읽기 허용
  - offline\_access: 위임, 부여된 데이터에 대한 액세스 유지 관리 허용
  - openid: 위임, 사용자가 로그인할 수 있음
  - 사용자 읽기: 위임, 사용자 프로필 로그인 및 읽기 허용
4. 마지막으로, Grant admin Consent for emailsecdemo를 클릭합니다.

Microsoft Azure Search resources, services, and docs (G+)

Home > emailsecdemo | App registrations > Cisco CES Shared mailbox

### Cisco CES Shared mailbox | API permissions

Search Refresh Got feedback?

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
  - Branding & properties
  - Authentication
  - Certificates & secrets
  - Token configuration
  - API permissions**
  - Expose an API
  - App roles
  - Owners
  - Roles and administrators
  - Manifest
- Support + Troubleshooting

#### Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for emailsecdemo

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (4)				
Mail.Read.Shared	Delegated	Read user and shared mail	No	Granted for emailsecde... <span>...</span>
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for emailsecde... <span>...</span>
openid	Delegated	Sign users in	No	Granted for emailsecde... <span>...</span>
User.Read	Delegated	Sign in and read user profile	No	Granted for emailsecde... <span>...</span>

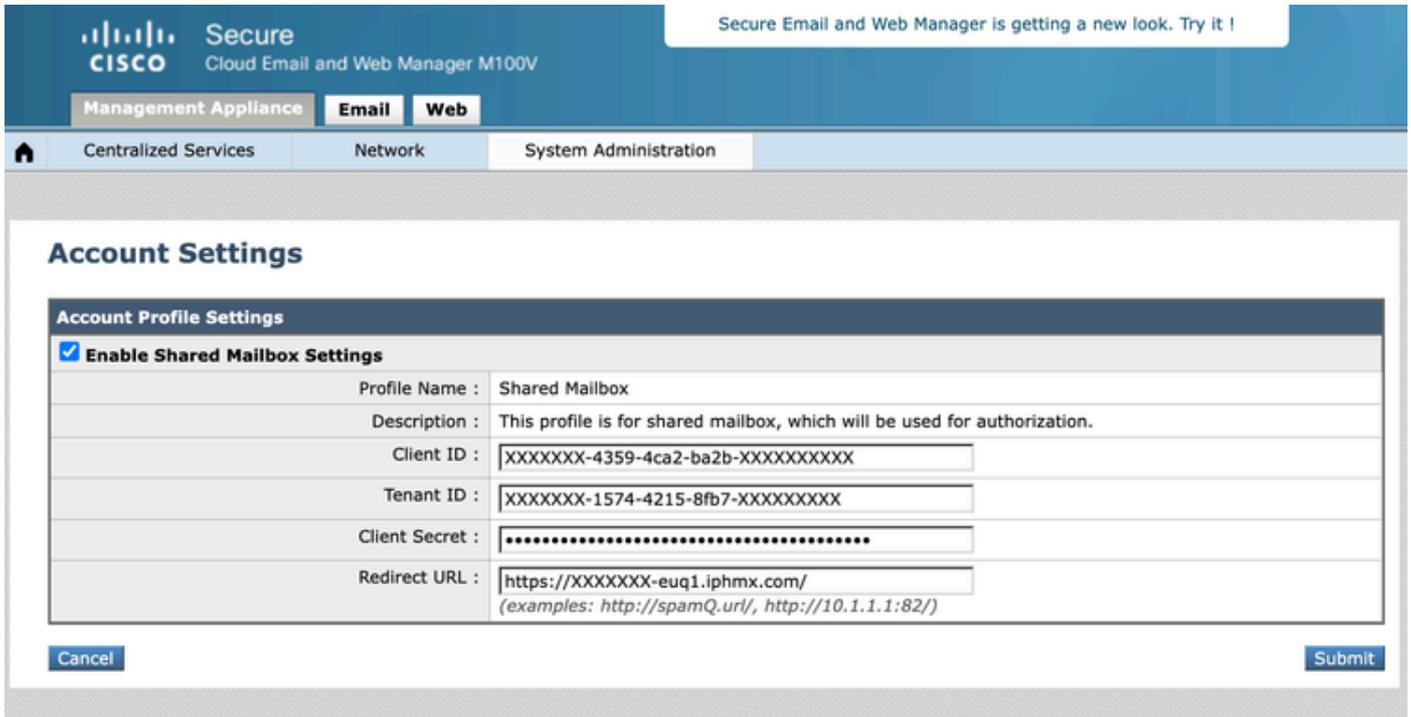
To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

## 자격 증명 생성

1. Application Overview(애플리케이션 개요) 화면에서 Client Credentials(클라이언트 자격 증명)로 이동합니다.
2. "클라이언트 암호"를 만들고 저장 후 사라지므로 안전한 위치에 값을 저장합니다.

## 2단계. Cisco Cloud Email Security 구성

1. 보고 콘솔을 열고 System Administration(시스템 관리) -> Account Settings(계정 설정)에 액세스합니다.
2. 공유 사서함 서비스를 활성화하고 구성합니다.
3. Edit Settings(설정 수정)를 클릭하고 서비스를 활성화하고 필수 필드를 추가합니다. EntraID 및 Client Secret에서 생성된 애플리케이션의 정보를 사용합니다.
4. EntraID 컨피그레이션으로 리디렉션 URL을 일관되게 구성합니다.
5. 공유 사서함에 액세스할 수 있는 사용자로 제출 및 테스트를 클릭합니다.



## 테스트

공유 사서함에 액세스할 수 있는 사용자로 테스트를 수행합니다.

SPAM 퀴런틴에는 액세스 권한이 있는 모든 공유 사서함을 추가할 수 있는 View Messages for mailbox 옵션이 새로 추가되었습니다.

1. Spam Quarantine(스팸 격리)을 열고 SAML을 사용하여 일반 사용자와 로그인합니다.
2. 사서함에 대한 메시지 보기를 클릭합니다.
3. 사용자가 액세스할 수 있는 공유 사서함 전자 메일 주소를 쓰고 Add Mailbox(사서함 추가)를 클릭합니다.
4. View Messages for Mailbox(사서함에 대한 메시지 보기)를 클릭하고 검토할 공유 사서함을 선택합니다.

## 추가 정보

스팸 격리 GUI 로그에서 사용자가 이메일을 릴리스하는 시기를 확인할 수 있습니다. 인증된 경우 릴리스한 사용자를 식별할 수 있습니다. 공유 사서함의 경우 로그 추적 ID를 분석하고 동일한 ID를 가진 사용자를 확인합니다.

```

Wed Jan 15 20:00:43 2025 Info: req:68.232.128.211 user:user1@domainabc.com id:5RwUAJcoaVYxN6nZ3xcW 200
Wed Jan 15 20:00:56 2025 Info: req:68.69.70.212 user:user1@domainabc.com id:5RwUAJcoaVYxN6nZ3xcW releas
Wed Jan 15 20:00:56 2025 Info: req:68.69.70.212 user:user1@domainabc.com id:5RwUAJcoaVYxN6nZ3xcW 303 PO
Wed Jan 15 20:00:56 2025 Info: req:68.69.70.212 user:user1@domainabc.com id:5RwUAJcoaVYxN6nZ3xcW 200 GE
Wed Jan 15 20:00:56 2025 Info: req:68.69.70.212 user:user1@domainabc.com id:5RwUAJcoaVYxN6nZ3xcW 200 GE
Wed Jan 15 20:01:15 2025 Info: login:68.69.70.212 user:shared1@domainabc.com session:5RwUAJcoaVYxN6nZ3xc
Wed Jan 15 20:01:15 2025 Info: req:68.69.70.212 user:user1@domainabc.com id:5RwUAJcoaVYxN6nZ3xcW 200 PO
Wed Jan 15 20:01:15 2025 Info: req:68.69.70.212 user:shared1@domainabc.com id:5RwUAJcoaVYxN6nZ3xcW 200

```

로그에서는 user1@domainabc.com과 shared1@domainabc.com 모두 동일한 세션 식별자 5RwUAJcoaVYxN6nZ3xcW를 사용하고 있음을 보여줍니다. 이는 두 사용자가 시스템에서 동일한 세션을 공유하거나 사용하고 있음을 의미합니다. 이는 shared1이 user1에 의해 처음 시작된 세션에서 작동하고 있음을 나타냅니다.

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.