Microsoft O365를 사용하여 이메일 암호화 추가 기능 구성

목차

소개

이 문서에서는 Microsoft Office 365를 통한 Cisco Email Encryption Service 추가 기능 중앙 집중식 구축을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco 보안 이메일 게이트웨이
- Cisco Secure Email Encryption Service(이전의 Cisco Registered Envelope Service)
- Microsoft O365 제품군(Exchange, Entra ID, Outlook)

사용되는 구성 요소

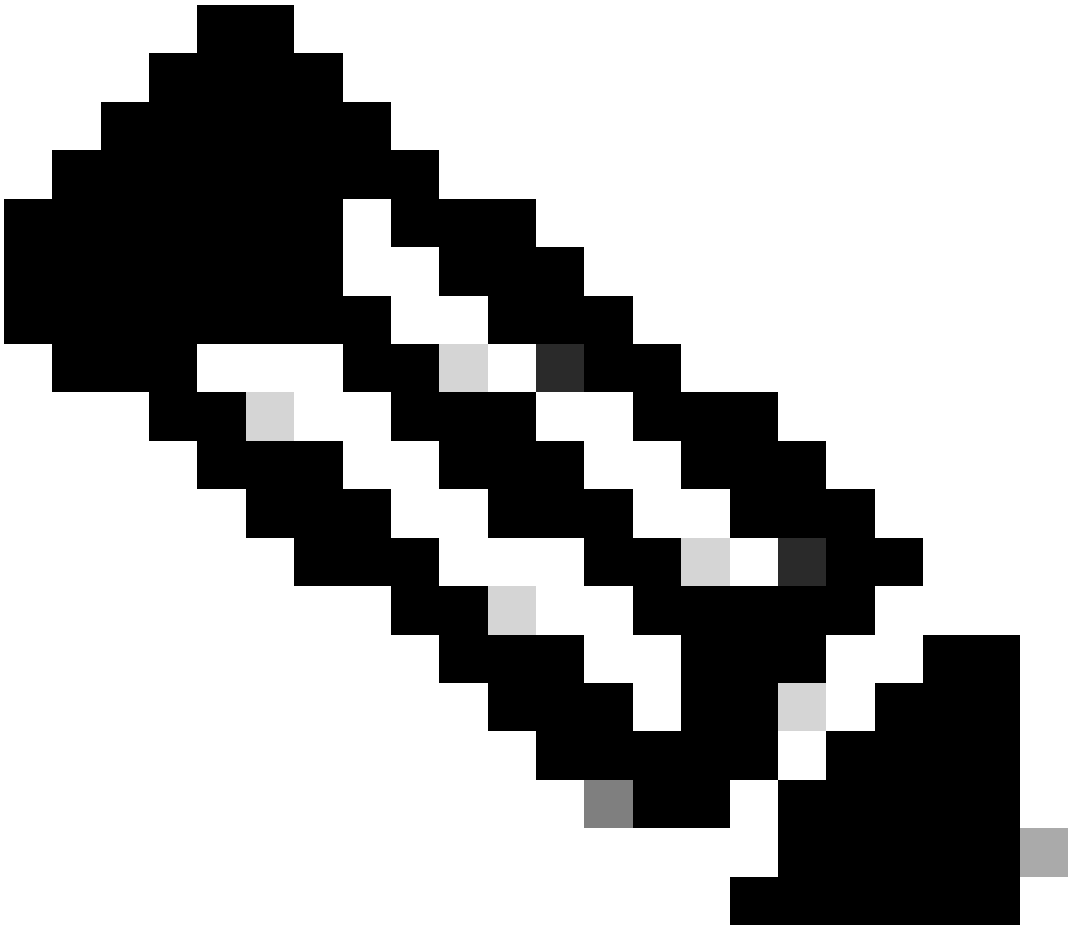
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Email Encryption 추가 기능 10.0.0
- Microsoft Exchange Online
- Microsoft Entra ID(이전의 Azure AD)
- O365용 Outlook(macOS, Windows)

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

Cisco Secure Email Encryption Service 추가 기능을 사용하면 최종 사용자가 클릭 한 번으로 Microsoft Outlook에서 직접 메시지를 암호화할 수 있습니다. 이 추가 기능은 Microsoft Outlook(Windows 및 macOS용) 및 Outlook Web App에 배포할 수 있습니다.



참고: 이 문서는 추가 기능을 사용하려는 모든 최종 사용자가 Office 365/Microsoft 365 구독을 사용하는 데 이상적이며 추가 기능을 사용하려는 모든 최종 사용자는 등록된 Cisco Secure Email Encryption Service 사용자입니다.

Cisco Secure Email Encryption Service 추가 기능 배포를 위한 모

범 사례

- 테스트 단계 - 부서 또는 기능 내의 소규모 최종 사용자 집합에 추가 기능을 배포합니다. 결과를 평가하고 성공하면 다음 단계로 이동합니다.
- 파일럿 단계 - 다양한 부서 및 기능의 더 많은 최종 사용자에게 추가 기능을 배포합니다. 결과를 평가하고 성공하면 다음 단계로 이동합니다.
- 프로덕션 단계 - 모든 사용자에게 추가 기능을 배포합니다.

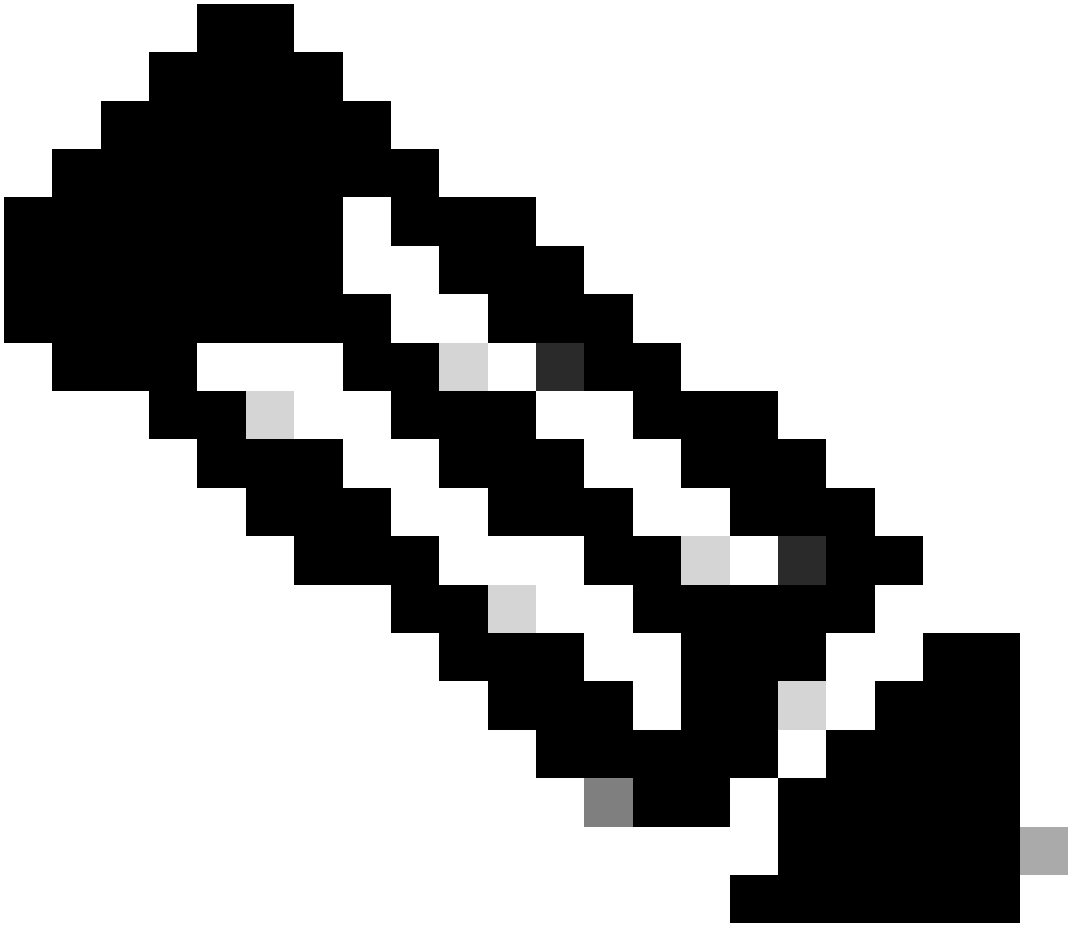
구성

Cisco Secure Email Encryption Service 추가 기능 애플리케이션 등록

1. Microsoft 365 Admin Center에 Cloud Application Administrator(Microsoft 365 Admin Center) 이상으로 로그인합니다.

2. 왼쪽 메뉴에서 를 확장하고 Admin Centers을 클릭합니다Identity.

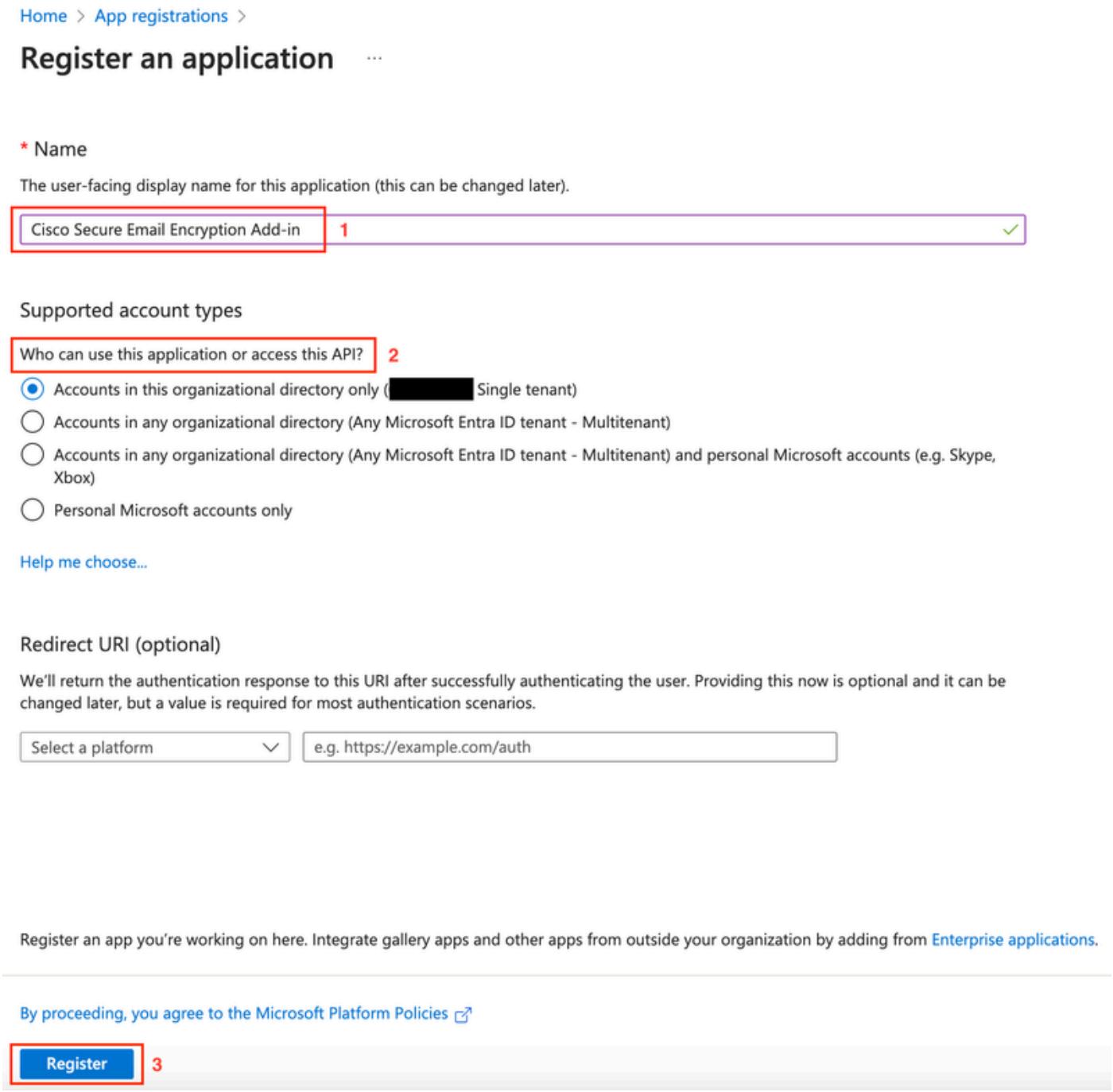
3. 탐색 Identity > Applications > App registrations및 선택 New registration.



참고: 여러 테넌트에 액세스할 수 있는 경우 오른쪽 상단 메뉴의 설정 아이콘을 사용하여 디렉터리 + 구독 메뉴에서 애플리케이션을 등록할 테넌트로 전환합니다.

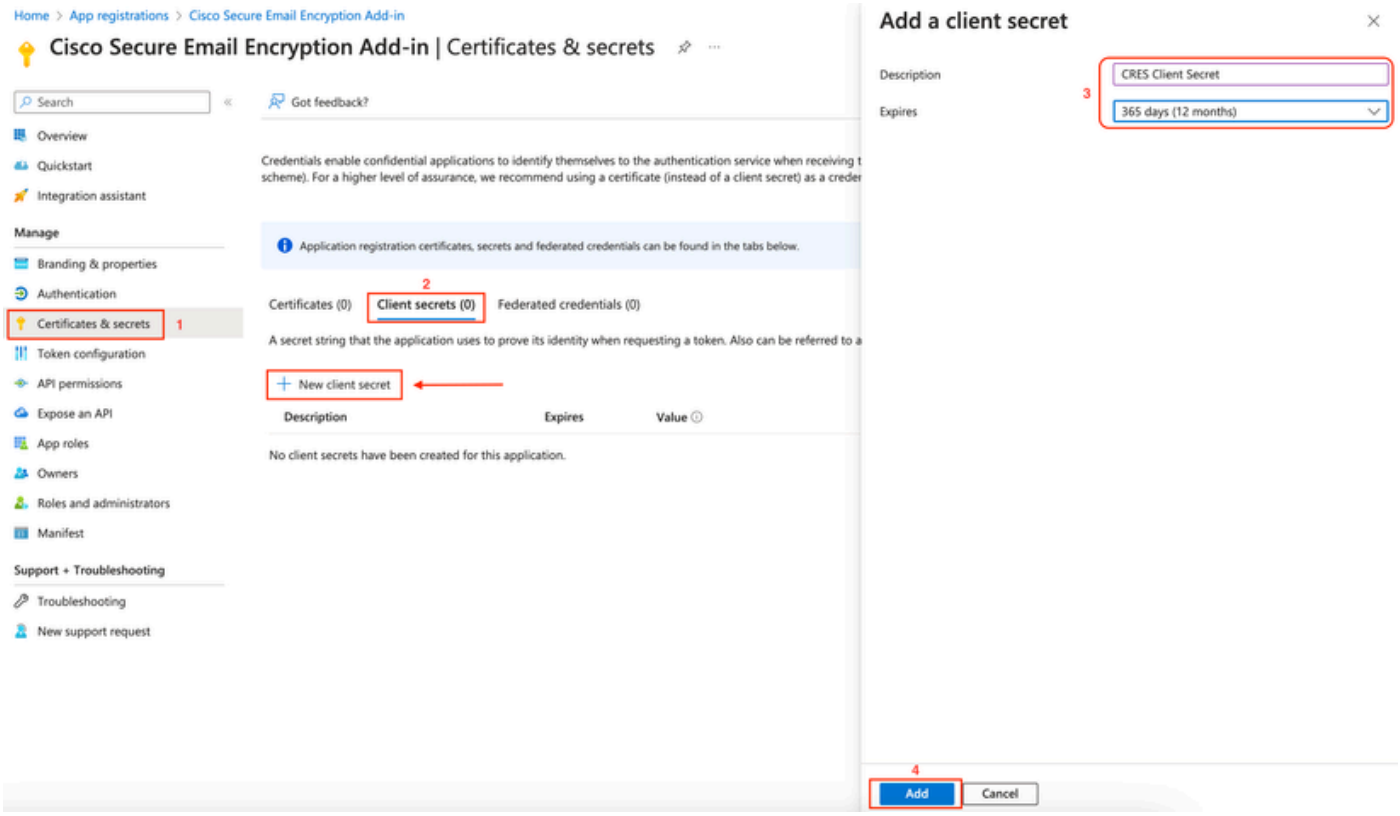
---

4. 애플리케이션에 대한 표시명을 입력하고 애플리케이션을 사용할 수 있는 계정을 선택한 후 누릅니다Register.



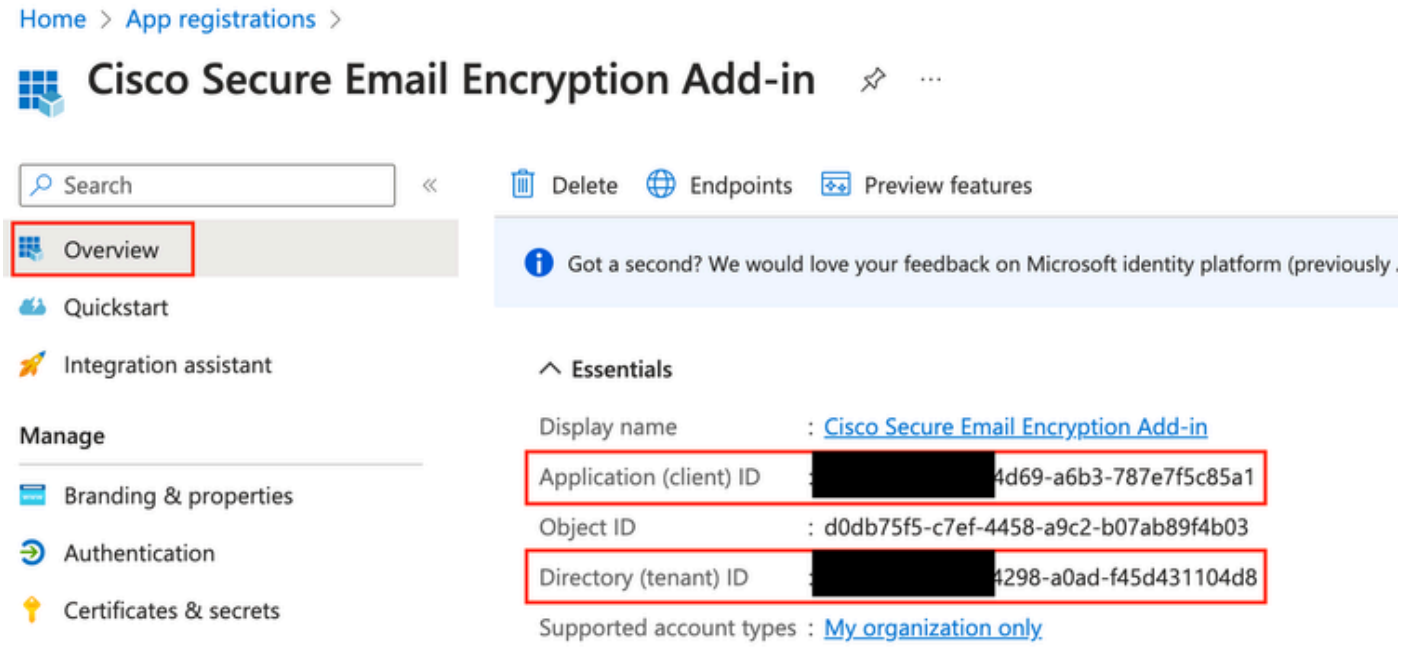
응용 프로그램 등록

5. 등록이 완료되면 애플리케이션으로 이동하여에서 클라이언트 암호를 Certificates & Secrets구성합니다. 조직 규정 준수에 따라 만료를 선택합니다.

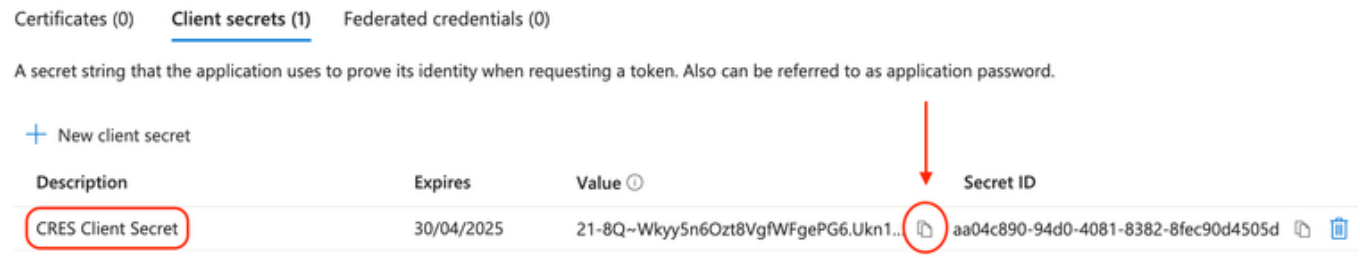


클라이언트 암호 구성

6. 등록된 애플리케이션의 개요 페이지에서 Application (client) ID 및 을 복사합니다Directory (tenant) ID. 이전 단계**Client Secret** 에서 생성된 인증서 및 비밀에서 를 복사합니다.



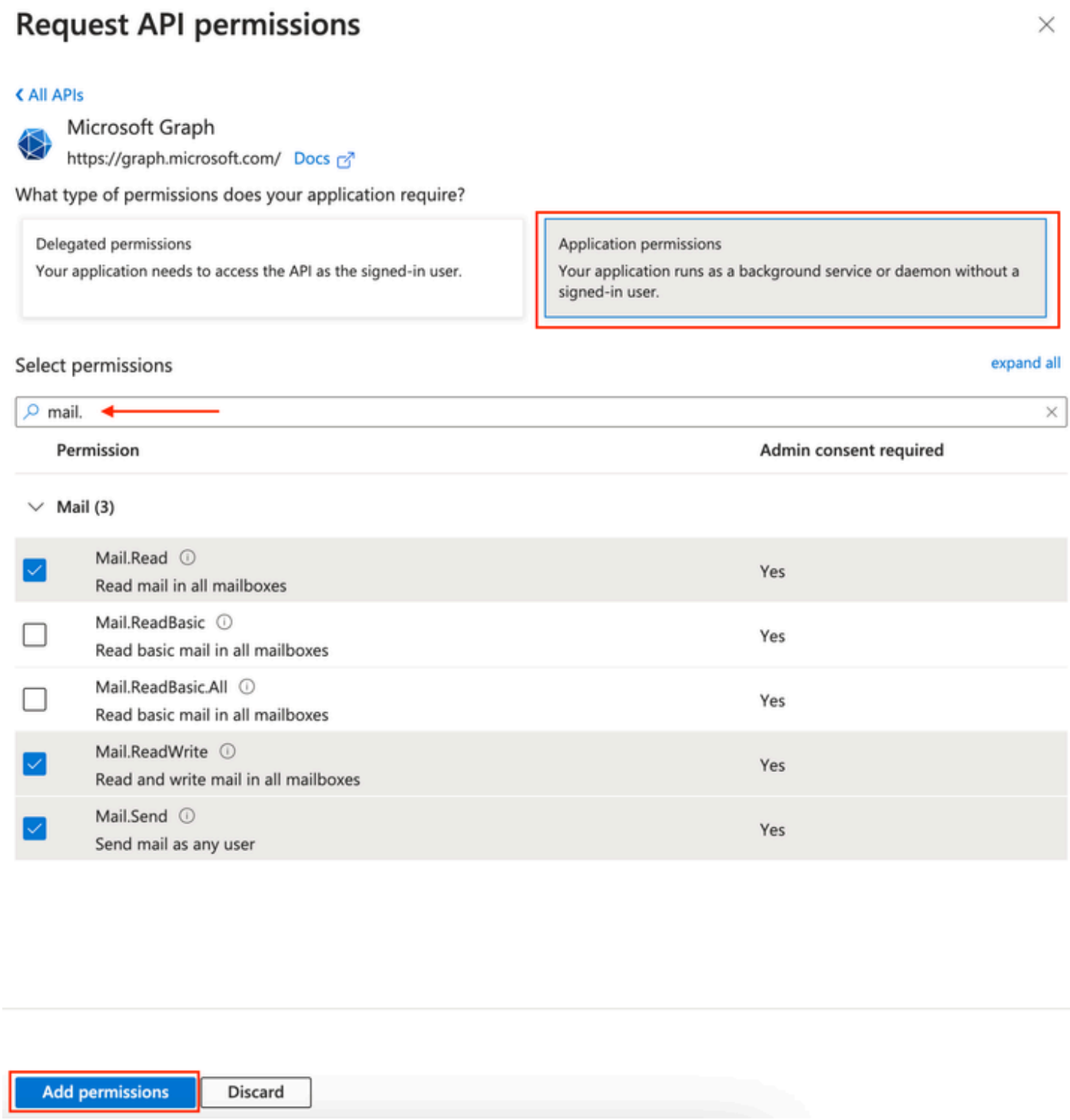
Entra ID 애플리케이션 개요



클라이언트 암호 복사

7. **등록된** 전자 **메일 암호화 애플리케이션**으로 이동한 다음 로 API permissions 이동합니다. Add a permission 를 클릭하고 필요한 Microsoft Graph Application Permissions(Microsoft Graph 애플리케이션 권한)를 선택합니다.

- Mail.읽기
- 메일 읽기/쓰기
- 메일.보내기
- 사용자 읽기.모두



Microsoft Graph 권한 컨피그레이션

7. 애플리케이션에 조직을 대신하여 권한에 대한 액세스 권한을 부여하려면 클릭합니다Grant Admin Consent for <tenant-name>.

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (4)				
Mail.Read	Application	Read mail in all mailboxes	Yes	Granted for [redacted]
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	Granted for [redacted]
Mail.Send	Application	Send mail as any user	Yes	Granted for [redacted]
User.Read.All	Application	Read all users' full profiles	Yes	Granted for [redacted]

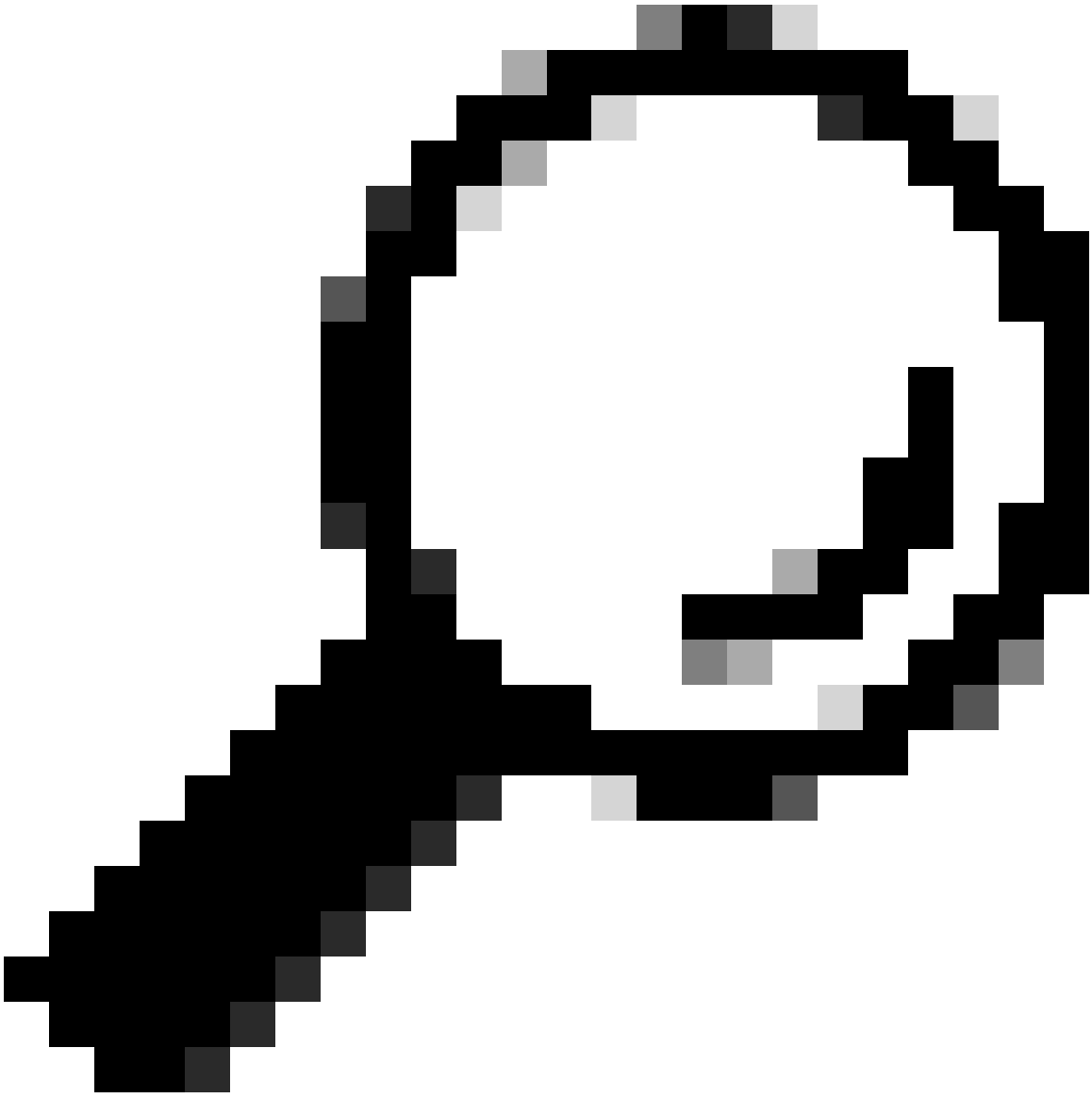
Microsoft Graph API 권한

CRES(Cisco Secure Email Encryption) 관리 포털에서 도메인 및 추가 기능 설정 구성

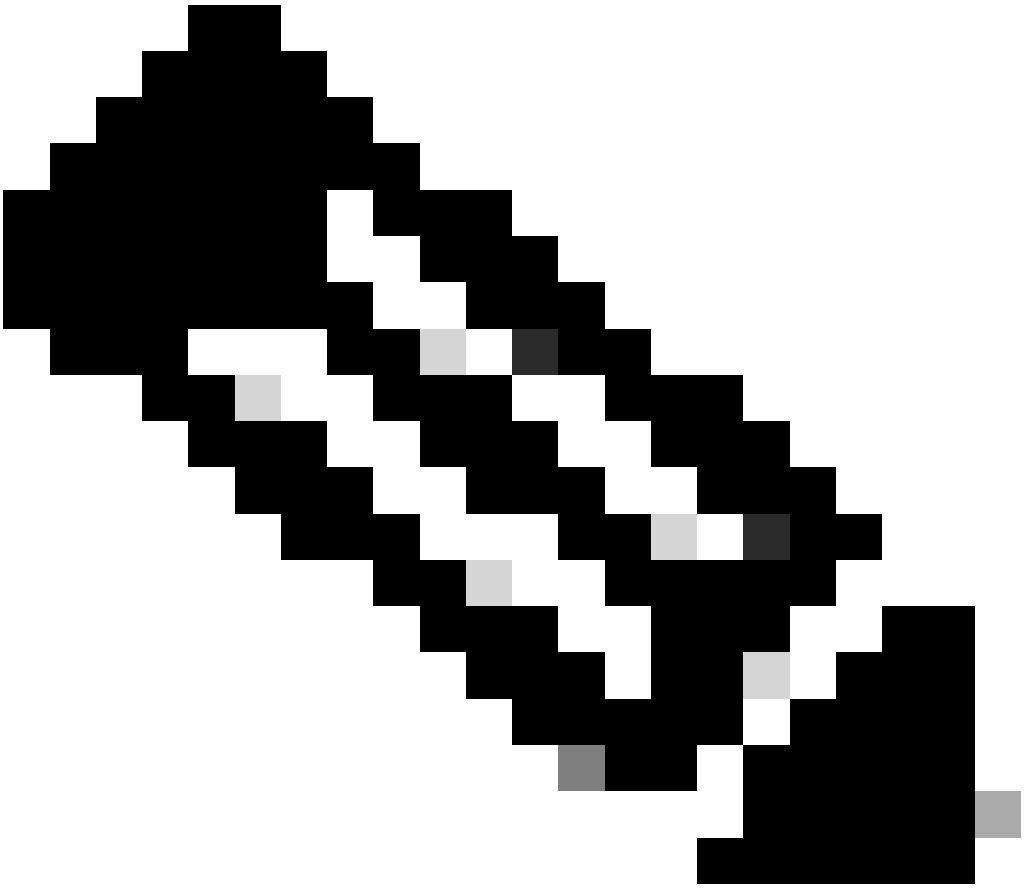
1. Cisco CRES(Secure Email Encryption Service) 관리 포털에 계정 관리자로 로그인합니다. (보안 이메일 암호화 서비스)

2. 로 Accounts > Manage Accounts 이동합니다. 조직에 할당된 계정 번호 또는 이메일 암호화 추가 기능을 구성하려는 계정을 클릭합니다.

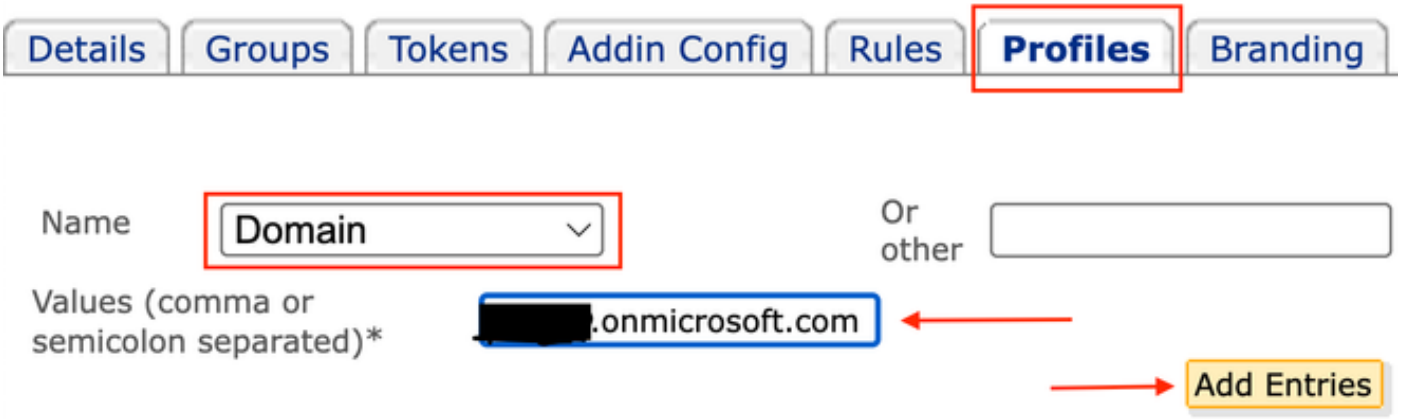
3. 탐색하여 Profiles 이름 유형을 **도메인**으로 선택하고 값 아래에 **전자 메일 도메인** 이름을 입력합니다. 클릭 **Add Entries** 을 하고 5~10초 동안 기다립니다. (브라우저 페이지를 새로 고치거나 다른 페이지가 성공적으로 추가될 때까지 해당 페이지로 이동하지 마십시오.)



팁: 동일한 단계를 반복하여 조직에서 이메일 암호화 서비스를 사용할 다른 이메일 도메인을 추가합니다.



참고: CRES 관리 포털에 추가된 이메일 도메인을 받으려면 Cisco Technical Assistance Center에 문의하십시오.

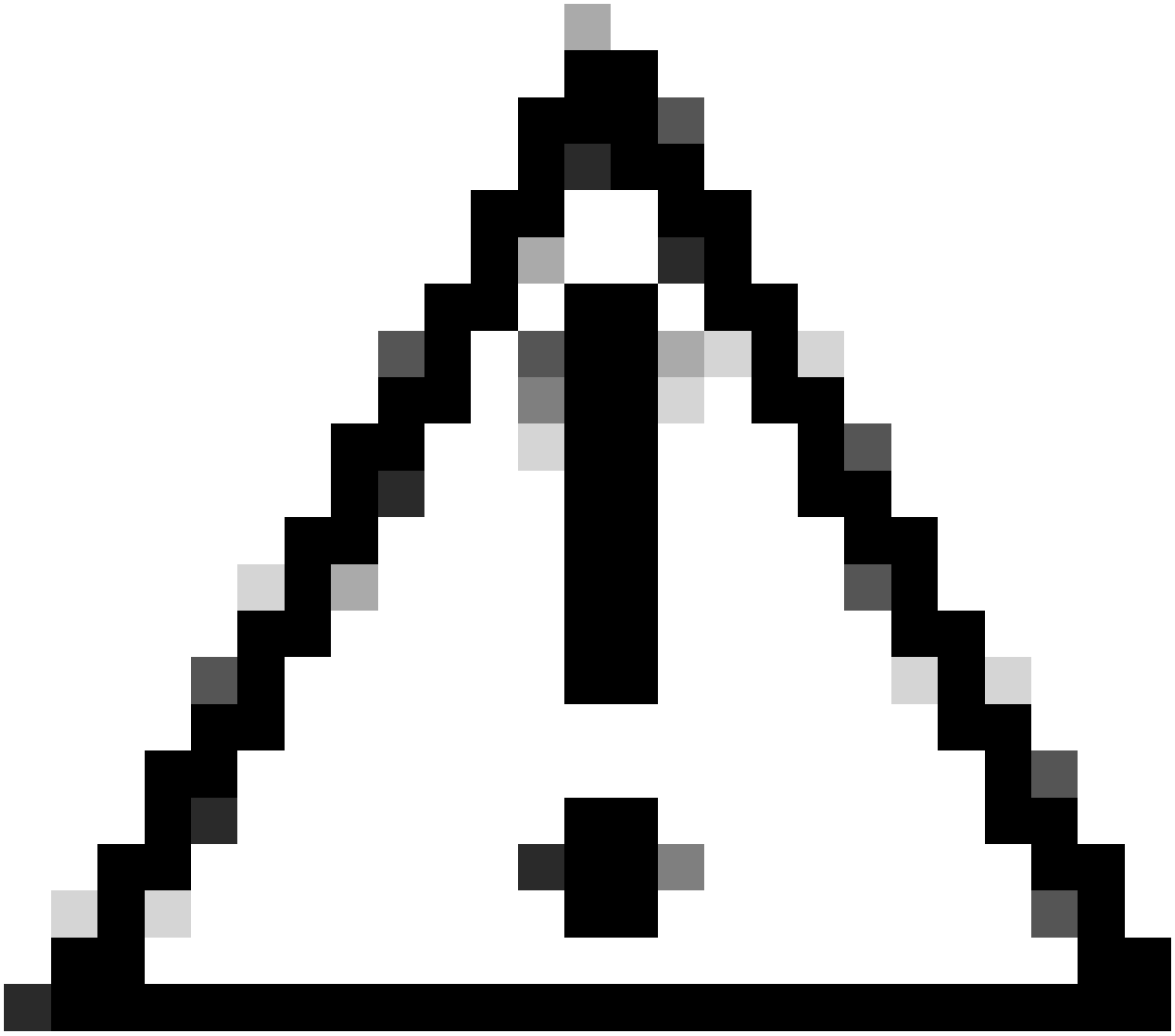


CRES 관리 포털 프로필

4. 탭으로 Add-in Config 이동합니다.

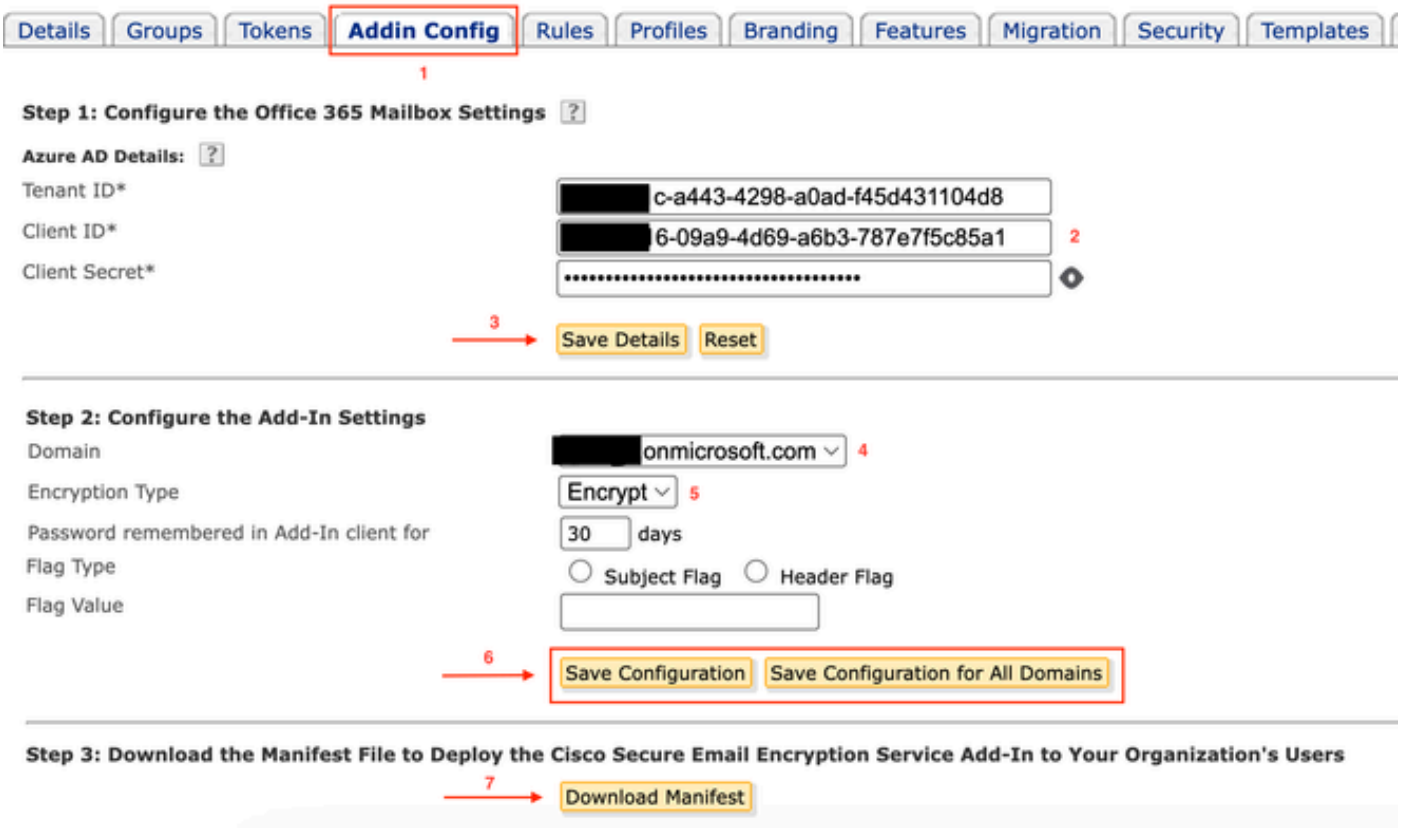
1단계: Azure AD Details(Azure AD 세부사항) 아래에 Entra ID에서 가져온 테넌트, 클라이언트 ID 및 암호를 입력합니다. 를 Save Details 클릭합니다.

2단계: 도메인, Encryption Type(암호화 유형)을 선택하고 을 클릭합니다Save Configuration. 추가된 모든 도메인에 동일한 설정을 적용하려면 All Domains(모든 도메인)에 Save Configuration사용합니다.



주의: 1단계와 2단계를 함께 완료하지 않고 다른 페이지로 이동하지 마십시오. 2단계가 동시에 완료되지 않으면 Azure AD 세부 정보가 저장되지 않습니다.

3단계: 을 Download Manifest 클릭합니다.

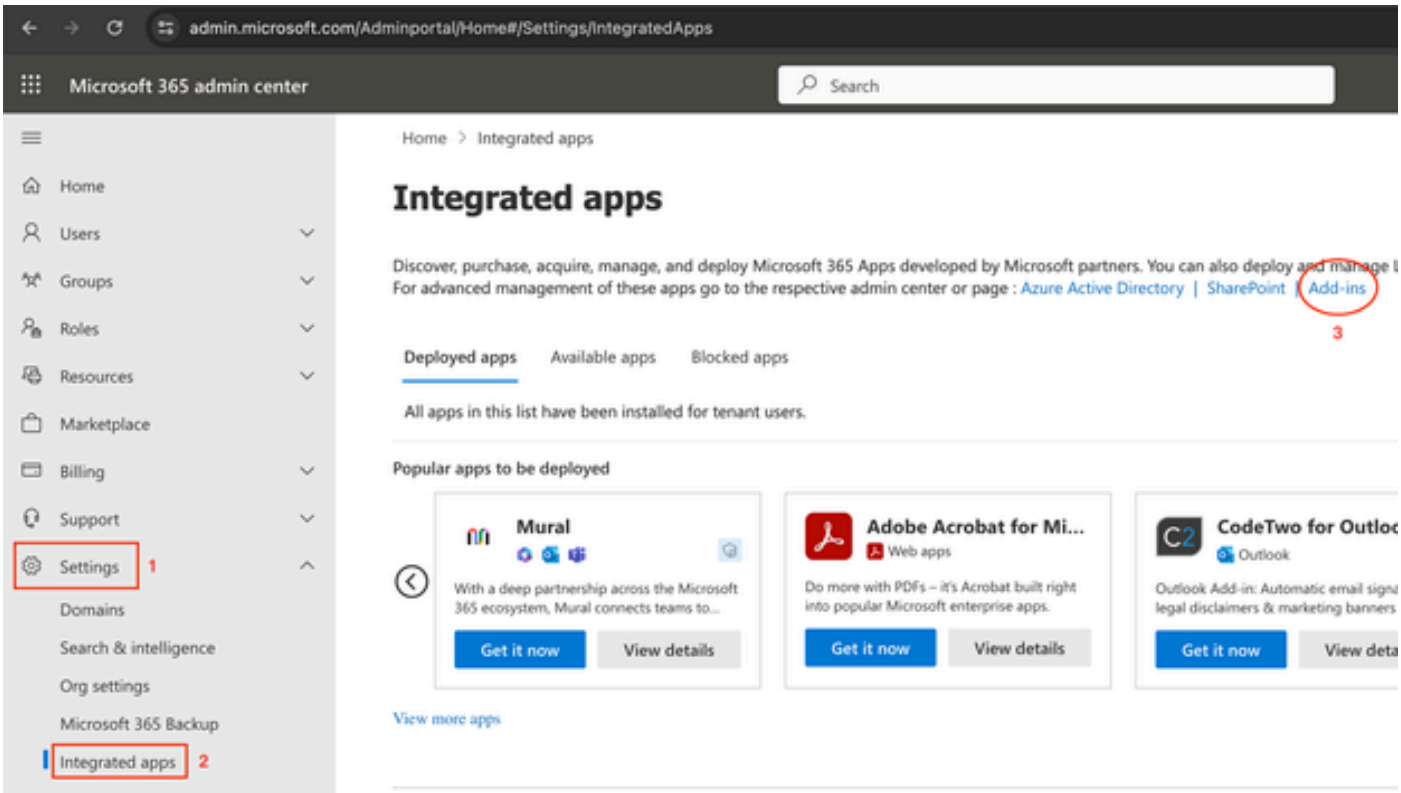


CRES 관리 포털 추가 기능 구성

Microsoft 365에 매니페스트 파일을 업로드하여 Email Encryption Service 추가 기능 배포

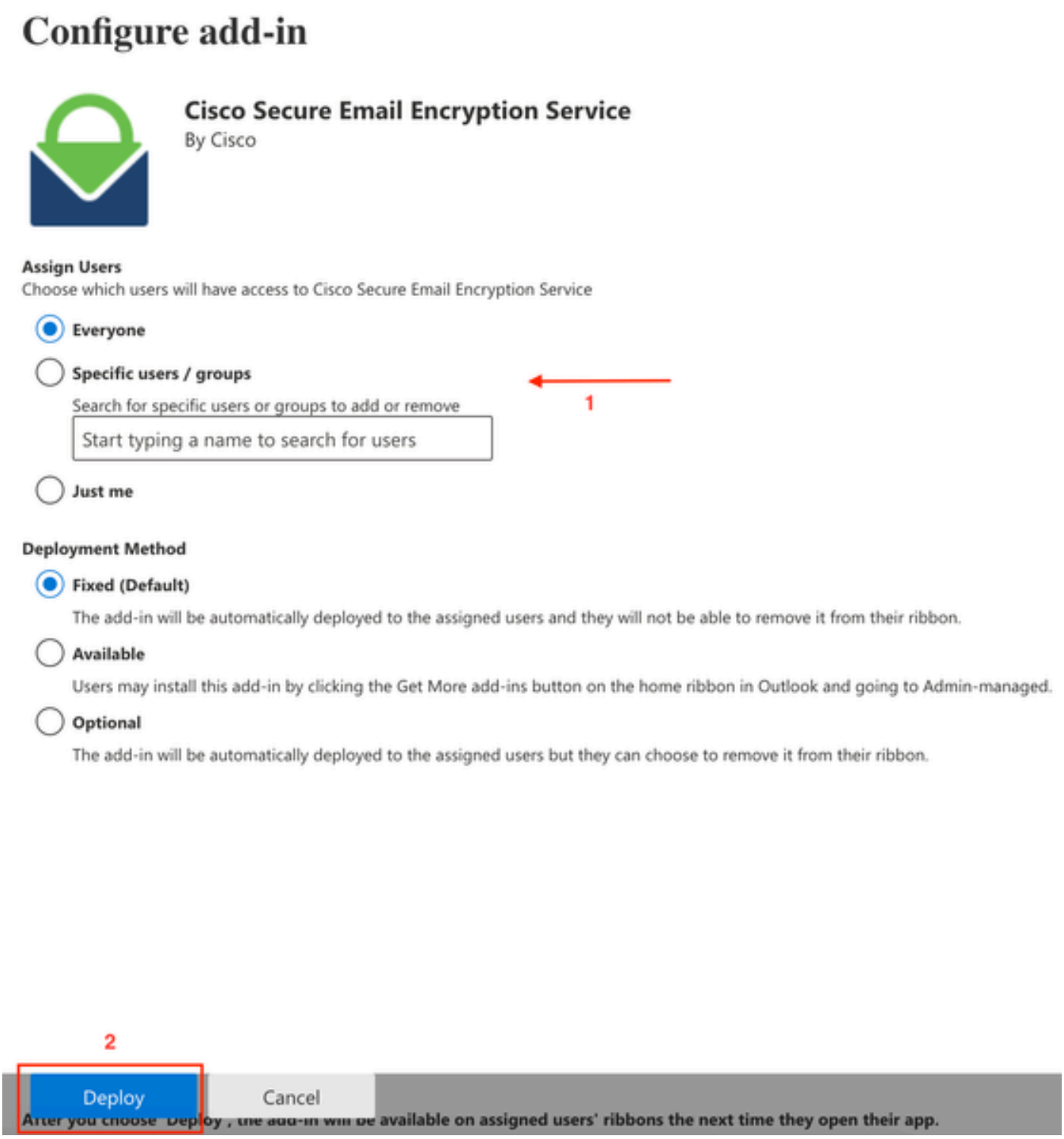
1. Microsoft 365 관리 센터에 관리자로 로그인합니다. (Microsoft 365 관리 센터).

2. 추가 기능Settings > Integrated apps 으로 **이동하여 클릭합니다**.



3. 클릭Deploy Add-in을 하고 선택합니다Upload Custom Apps. 이전 I have the manifest file (.xml) on this device단계에서 Cisco Email Encryption Service 관리 포털에서 다운로드한 파일을 선택하고 업로드합니다. 를 Upload 클릭합니다.

4. 다음 단계에서 Cisco Secure Email Encryption Service에 액세스해야 하는 사용자를 할당합니다. 단계별 방식 구축의 경우 를 선택하고 Specifc Users/groups를 클릭합니다Deploy.

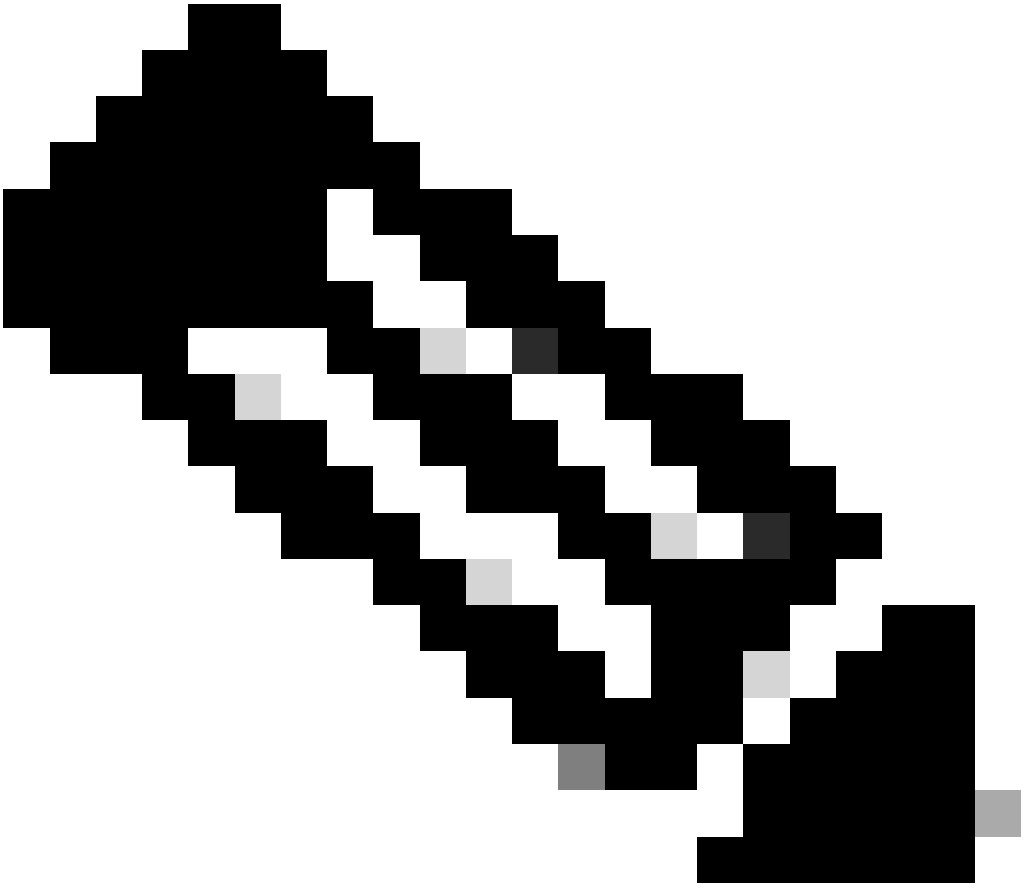


5. 추가 기능이 배포되면 최종 사용자의 리본(Outlook 클라이언트)에 표시되는 데 최대 12시간이 걸릴 수 있습니다.

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

1. Office 365/Microsoft 365 또는 Outlook Web App용 Outlook을 시작하고 암호화할 메시지를 작성하고 유효한 받는 사람을 하나 이상 추가합니다.



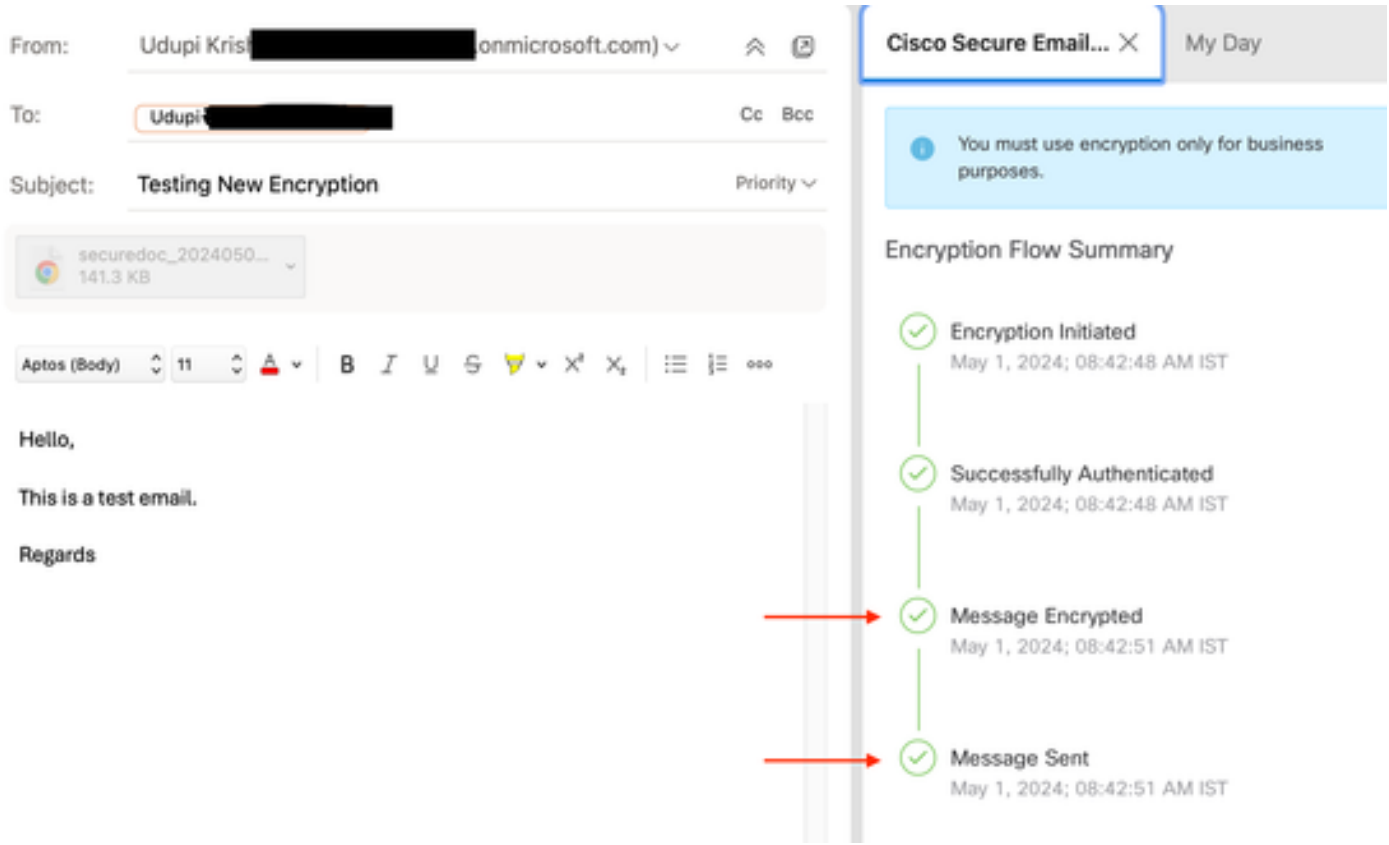
참고: 암호화 유형(관리자가 설정)이 암호화인 경우 다음 단계로 진행하기 전에 메시지를 완료하고 유효한 수신자를 추가했는지 확인하십시오. 3단계 이후에는 메시지가 암호화되어 즉시 전송됩니다.

---

2. Cisco Secure Email Encryption Service 추가 기능을 열거나 클릭합니다.

- Outlook Web App에서 Send(보내기) 및 Discard(버리기) 버튼 근처에 있는 줄임표 아이콘을 클릭하고 을 Cisco Secure Email Encryption Service 클릭합니다.
- Windows 또는 MacOS용 Outlook의 리본 또는 도구 모음에서 암호화를 클릭합니다.
- MacOS용 Outlook 버전 16.42 이상에서 새 Outlook 인터페이스를 사용하는 경우 도구 모음에서 을 클릭합니다Cisco Secure Email Encryption Service.

3. 자격 증명을 입력하고 를 Sign in 클릭합니다. (Encryption Type(암호화 유형)이 Flag(플래그)인 경우에만 클릭합니다Send.)



Microsoft Outlook 암호화 상태

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- Cisco Secure Email Encryption Service 계정 관리자 사용 설명서
- Cisco Secure Email Encryption Service 추가 기능 사용 설명서
- Microsoft Entra 애플리케이션 등록 가이드
- Cisco 기술 지원 및 다운로드

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.