



Google



중요 **Enterprise Manager**가 사용이 중지되었습니다. 이제 **보안 클라우드 제어**를 사용하여 ID 공급자 통합을 관리할 수 있습니다. 자세한 내용은 **ID 공급자 통합 가이드**를 참조하십시오.

모든 기존 ID 공급자 통합 데이터는 보안 클라우드 컨트롤을 통해 사용할 수 있습니다.

- [개요, 1 페이지](#)
- [시작하기, 1 페이지](#)

개요


이 가이드에서는 Google Workplace SAML 애플리케이션을 생성하여 Security Cloud Sign On과(와) 통합하는 방법을 설명합니다.

시작하기

시작하기 전에

- 슈퍼 관리자 권한이 있는 Google Workspace 계정이 있어야 합니다.
- 엔터프라이즈 설정 마법사의 **1단계: 엔터프라이즈 생성** 및 **2단계: 이메일 도메인 클레임 및 확인**을 완료해야 합니다.

단계 1 슈퍼 관리자 권한이 있는 계정을 사용하여 [Google 관리 콘솔](#)에 로그인합니다.

- 관리 콘솔에서 Menu(메뉴)  > **Apps(앱)** > **Web and mobile apps(웹 및 모바일 앱)**로 이동합니다.
- Add App(앱 추가)** > **Add custom SAML app(사용자 지정 SAML 앱 추가)**을 클릭합니다.
- App Details(앱 세부 정보)** 페이지에서:
 - 애플리케이션 이름으로 **Secure Cloud Sign On** 또는 다른 값을 입력합니다.

- 아이콘을 업로드하여 애플리케이션과 연결할 수도 있습니다.

- Continue**(계속)를 클릭합니다.
- SSO URL** 및 엔터티 **ID**를 복사하고 인증서를 다운로드합니다.

단계 2 새 브라우저 탭에서 Enterprise 설정 마법사를 엽니다. 사용자는 3단계: **SAML 메타데이터 교환**에 있어야 합니다.

- ID 공급자(IdP)** 이름에 **Google SSO** 또는 다른 값을 입력합니다.
- Single Sign-On Service URL** 필드에 Google Admin Console에서 복사한 "SSO URL"을 입력합니다.
- Entity ID (Audience URI)**(엔터티 ID(대상 URI)) 필드에 Google Admin Console에서 복사한 "엔터티 ID"를 입력합니다.
- Add File...**(파일 추가...)을 클릭하고 Google Admin Console에서 다운로드한 인증서를 선택합니다.
- 원하는 경우 사용자에 대해 무료 **Duo 다단계 인증**을 옵트아웃합니다.
- Next**(다음)를 클릭합니다.
- Single Sign-On Service URL(ACS URL)** 및 엔터티 ID(대상 URI)를 복사하고 **SAML 서명 인증서**를 다운로드합니다.

단계 3 Google Admin Console로 돌아갑니다.

- Add custom SAML app**((맞춤형 SAML 앱 추가)) 페이지에서 **Continue**(계속)를 클릭합니다.
- 이전에 엔터프라이즈 설정 마법사에서 복사한 "Single Sign-On Service URL(ACS URL)을 **ACS URL** 필드에 입력합니다.
- Name ID**(이름 ID) 형식에 대해 **UNSPECIFIED** 또는 **EMAIL**을 선택합니다.
- Name ID(이름 ID)에 대해 **Basic Information**(기본 정보) > **Primary Email**(기본 이메일)을 선택합니다.
- Continue**(계속)를 클릭합니다.
- Attributes mapping**(속성 매핑) 페이지에서 다음 속성 매핑을 추가합니다.

Google 디렉토리 속성	앱 속성
이름	firstName
성	lastName
기본 이메일	email

Attributes

Add and select user fields in Google Directory, then map them to service provider attributes. Attributes marked with * are mandatory. [Learn more](#)

Google Directory attributes	→	App attributes	
Basic Information > First name	→	firstName	×
Basic Information > Last name	→	lastName	×
Basic Information > Primary email	→	email	×

[ADD MAPPING](#)

단계 4 엔터프라이즈 설정 마법사의 **Configure**(구성) 화면으로 돌아갑니다.

- a) 표시된 URL을 복사하여 비공개(시크릿) 브라우저 창에서 엽니다.
브라우저가 Google SSO URL로 리디렉션됩니다.
- b) **클레임된 도메인**과 일치하는 이메일 주소로 Google에 로그인합니다.
SecureX 애플리케이션 포털로 다시 연결되면 테스트에 성공한 것입니다.
- c) 설정 마법사에서 **Next**(다음)를 클릭하여 **Activate**(활성화) 화면으로 이동합니다.
- d) 사용자에게 대한 통합을 활성화하려면 **Activate my IdP**(내 IdP 활성화)를 클릭합니다.
- e) 대화 상자에서 결정을 확인합니다.

IdP Activation ×

Once the IdP integration is activated:

- Users sign in using their enterprise IdP password
- Users no longer manage their MFA settings (if you opted out of Duo MFA during setup).

Cancel
Activate

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.