Duo

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

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

개요

이 가이드에서는 Duo SAML 애플리케이션을 생성하고 Security Cloud Sign On과(와) 통합하는 방법을 설명합니다.

시작하기

시작하기 전에

- 사용자는 소유자 역할의 Duo 관리자여야 합니다.
- **Duo Admin(Duo 관리) - Single Sign-On - Configure Authentication Sources(**인증 소스 구성**)**에서 인증 소스를 하나 이상 이미 Duo에 구성해야 합니다.
- 엔터프라이즈 설정 마법사의 1단계: 엔터프라이즈 생성 및 2단계: 이메일 도메인 클레임 및 확인를 완료해야 합니다.

단계 **1** Duo Admin Panel에 로그인합니다.

a) 왼쪽 메뉴에서 **Applications(**애플리케이션**)**를 클릭한 다음 **Protect Application(**애플리케이션 보호**)**을 클릭합니다.

b) 일반 **SAML** 통신 사업자를 검색합니다.

c) **Duo**에서 호스팅하는 **SSO**를 사용하는 **2FA**의 보호 유형을 갖는 일반 서비스 제공자 애플리케이션 옆에 있는 **Protect(**보호**)**를 클릭합니다. Generic SAML Service Provider(일반 SAML 서비스 제공자) 구성 페이지가 열립니다.

d) **Metadata(**메타데이터**)** 섹션에서 다음을 수행합니다.

e) 엔터티 **ID**의 값을 복사하고 나중에 사용할 수 있도록 저장합니다.

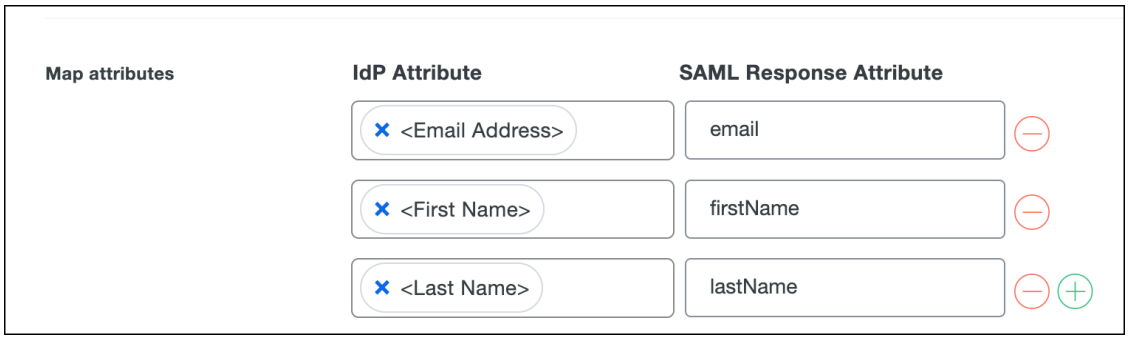
f) **SSO(Single Sign-On) URL**의 값을 복사하고 나중에 사용할 수 있도록 저장합니다.

g) Downloads(다운로드) 섹션에서 **Download certificate(**인증서 다운로드**)**를 클릭합니다.

h) SAML Response(SAML 응답) 섹션에서 다음을 수행합니다.

- **NameID** 형식에 대해 **urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified** 또는 **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress** 중 하나를 선택합니다.
- **NameID** 속성에 대해 **<Email Address>**를 선택합니다.
- **Map Attributes(**맵 속성**)** 섹션에서 Duo IdP 사용자 속성에 대한 SAML 응답 속성의 다음 매핑을 입력합니다.

IdP 속성	**SAML** 응답 속성
<Email Address>	**email**
<First Name>	**firstName**
<Last Name>	**lastName**



i) **Settings(**설정**)** 섹션의 **Name(**이름**)** 필드에 보안 클라우드 로그인 또는 다른 값을 입력합니다.

Duo SAML 설정 브라우저 창을 열어 둡니다.

단계 **2** 새 브라우저 탭에서 엔터프라이즈 설정 마법사를 엽니다. 현재 **Integrate Identity Provider(ID** 공급자 통합**)** 화면(3 단계: SAML 메타데이터 교환 참조)의 **Set Up(**설정**)** 단계에 있어야 합니다.

a) **Identity Provider Name(ID** 공급자 이름**)** 필드에 IdP의 이름(예:`Duo SSO`)을 입력합니다.

b) Duo에서 복사한 **SSO(Single Sign-On) URL**의 값을 **SSO(Single Sign On)** 서비스 **URL** 필드에 입력합니다.

c) **Entity ID(**엔터티 **ID)** 필드에 Duo에서 복사한 **Entity ID(**엔터티 **ID)** 필드의 값을 입력합니다.

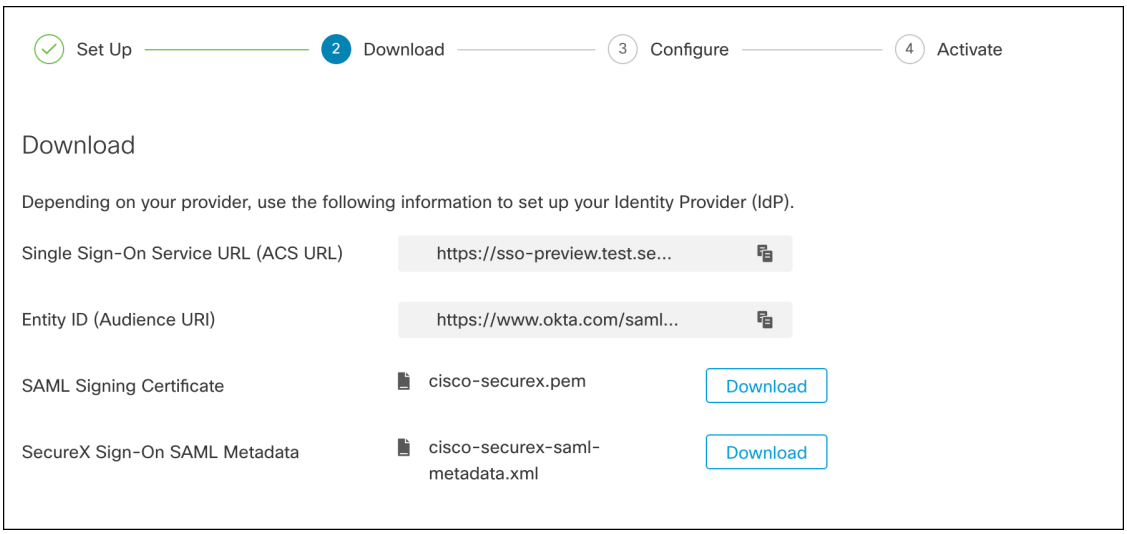
d) **Add File(**파일 추가**)**을 클릭하고 Duo에서 다운로드한 SAML 서명 인증서를 선택합니다.

e) 원하는 경우 사용자에 대해 무료 Duo 기반 MFA 서비스를 옵트아웃할 수 있습니다.

f) **Next(**다음**)**를 클릭하여 **Download (**다운로드**)** 화면으로 이동합니다.

g) 나중에 사용할 수 있도록 **Single Sign-On Service URL (ACS URL)** 및 **Entity ID (Audience URI)** 필드의 값을 복사하고 저장합니다.

h) **SAML** 서명 인증서(cisco-securex.pem)를 다운로드합니다.



i) **Next(**다음**)**를 클릭하여 **Configure(**구성**)** 화면으로 이동합니다.

단계 **3** Duo SAML 애플리케이션 구성으로 돌아가 다음을 수행합니다.

a) **Service Provider(**통신 사업자**)** 섹션의 **Entity ID(**엔터티 **ID)** 필드에 이전 단계에서 설정 마법사가 제공한 **Entity ID (Audience URI)** 필드의 값을 입력합니다.

b) **Assertion Consumer Service (ACS) URL**에 이전 단계에서 설정 마법사가 제공한 **Single Sign-On Service URL (ACS URL)** 필드의 값을 입력합니다.

c) 구성 페이지의 하단에서 **Save(**저장**)**를 클릭합니다.

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

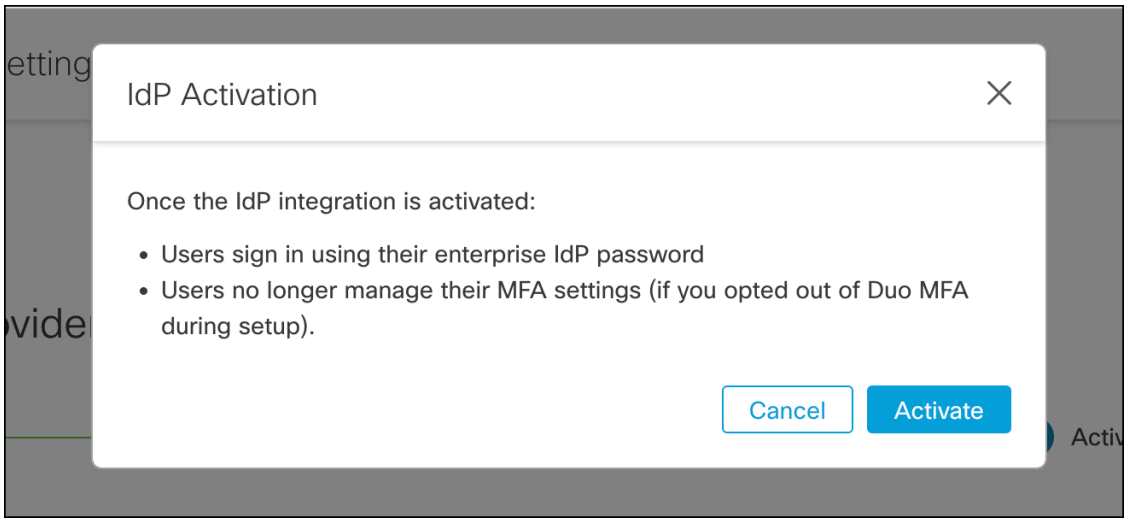
a) 표시된 URL을 복사하여 비공개(시크릿) 브라우저 창에서 엽니다.
브라우저가 Duo SSO URL로 리디렉션됩니다.

b) 클레임된 도메인과 일치하는 이메일 주소로 Duo에 로그인합니다.
SecureX 애플리케이션 포털로 다시 연결되면 테스트에 성공한 것입니다.

c) 설정 마법사에서 **Next(**다음**)**를 클릭하여 **Activate(**활성화**)** 화면으로 이동합니다.

d) 사용자에 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