Auth0

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 Security Cloud Sign On과(와) 통합할 Auth0 SAML 애플리케이션을 생성하는 방법을 설명합니다.

시작하기

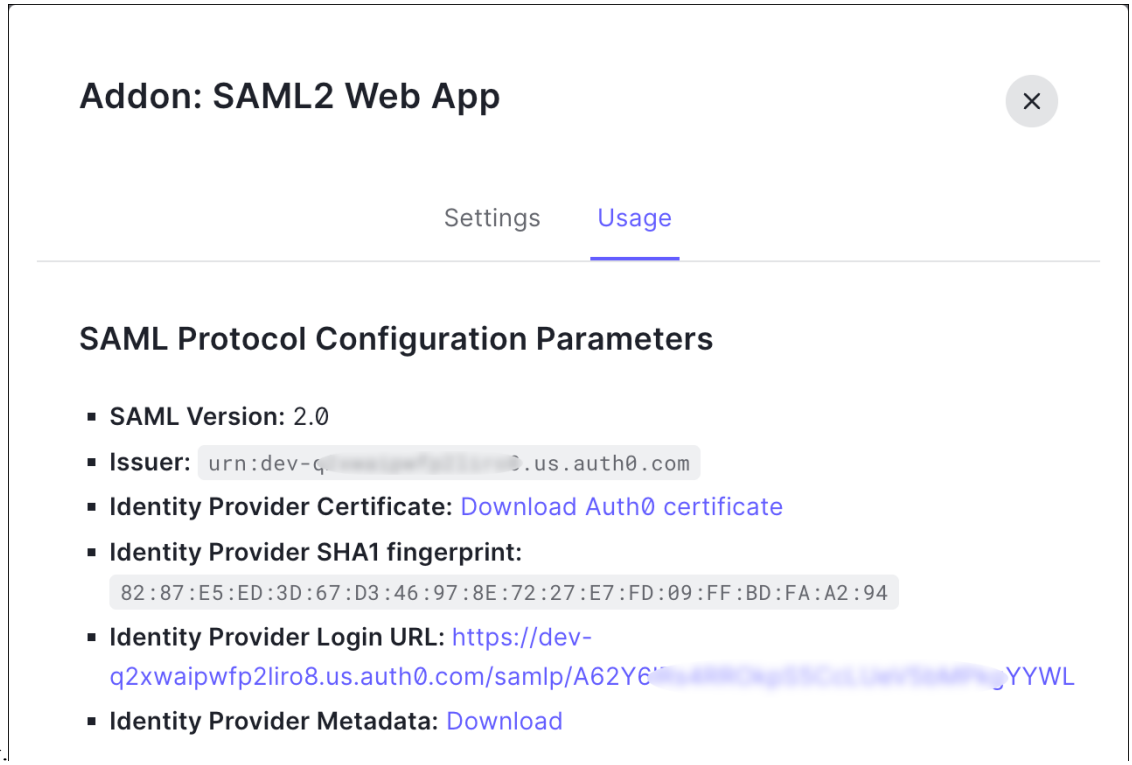
시작하기 전에

- 관리자 권한으로 Auth0 관리 콘솔에 로그인할 수 있어야 합니다.
- 1단계: 엔터프라이즈 생성 및 2단계: 이메일 도메인 클레임 및 확인를 완료해야 합니다.

단계 **1** Auth0 대시보드에 로그인하고 다음을 수행합니다.

a) **Applications(**애플리케이션**)** 메뉴에서 **Applications(**애플리케이션**)**을 선택합니다.
b) **Create Application(**애플리케이션 생성**)**을 클릭합니다.
c) **Name(**이름**)** 필드에 **`Secure Cloud Sign On`** 또는 다른 이름을 입력합니다.
d) 애플리케이션 유형으로 **Regular Web Applications(**일반 웹 애플리케이션**)**를 선택한 다음 **Create(**생성**)**를 클릭합니다.
e) **Addons(**애드온**)** 탭을 클릭합니다.

f) **SAML2 Web App(SAML2** 웹 애플리케이션**)** 토글을 클릭하여 애드온을 활성화합니다.
SAML2 Web App configuration(SAML2 웹 앱 구성) 대화 상자가 열립니



다.

g) **Issuer(**발급자**)** 및 **Identity Provider Login URL(ID** 공급자 로그인 **URL)** 필드의 값을 복사합니다.

h) **Download Auth0 certificate(Auth0** 인증서 다운로드**)**를 클릭하여 **Identity Provider Certificate(ID** 공급자 인증서**)**를 다운로드합니다.

단계 **2** 엔터프라이즈 설정 마법사의 **Integrate Identity Provider(ID** 공급자 통합**)** 화면을 열고 다음을 수행합니다.

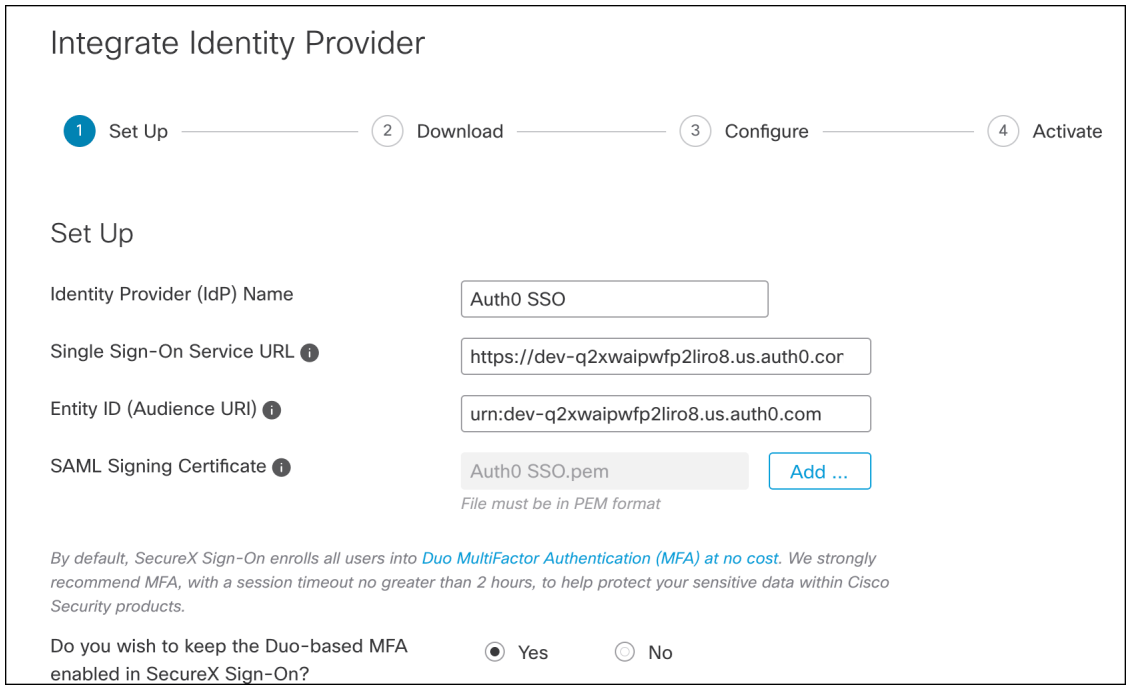
a) **Identity Provider Name(ID** 공급자 이름**)** 필드에 IdP의 이름(예:**`Auth0 SSO`**)을 입력합니다.

b) **Single Sign On Service URL(SSO** 서비스 **URL)** 필드에 SAML Addon(SAML 애드온) 대화 상자에서 복사한 **Identity Provider Login URL(ID** 공급자 로그인 **URL)**의 값을 입력합니다.

c) SAML Addon(SAML 애드온) 대화 상자에서 복사한 **Issuer(**발급자**)** 필드의 값을 **Entity ID(**엔터티 **ID)** 필드에 입력합니다.

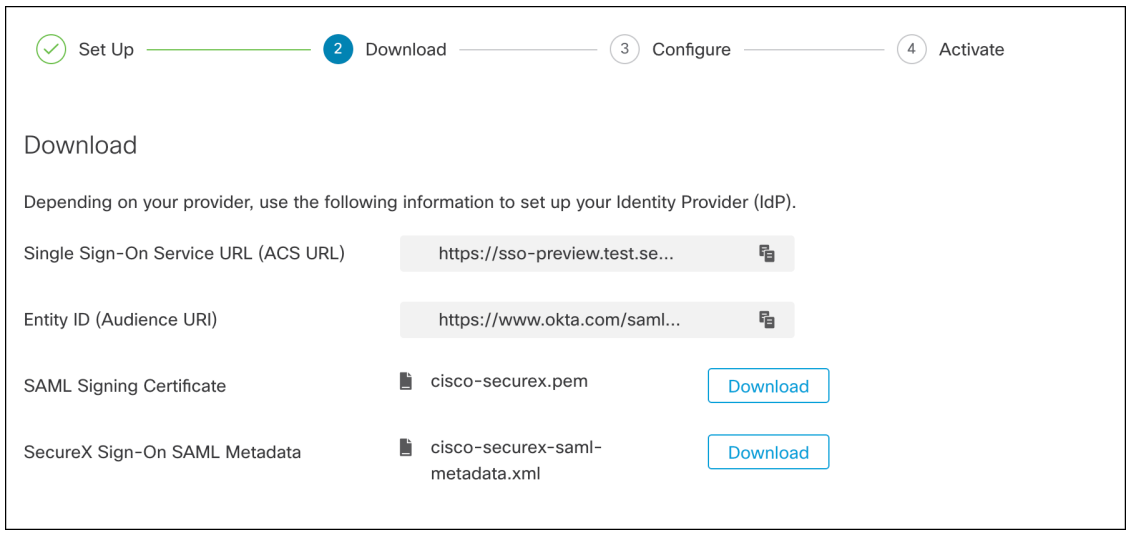
d) **Add File(**파일 추가**)**을 클릭하고 Auth0에서 다운로드한 SAML 서명 인증서를 선택합니다.

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



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

g) 나중에 사용할 수 있도록 **Single Sign-On Service URL** 및 엔터티 **ID**의 값을 복사하고 **SAML** 서명 인증서(cisco-securex.pem)를 다운로드합니다.



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

단계 **3** Auth0 콘솔의 Addon configuration(애드온 구성) 대화 상자로 돌아갑니다.

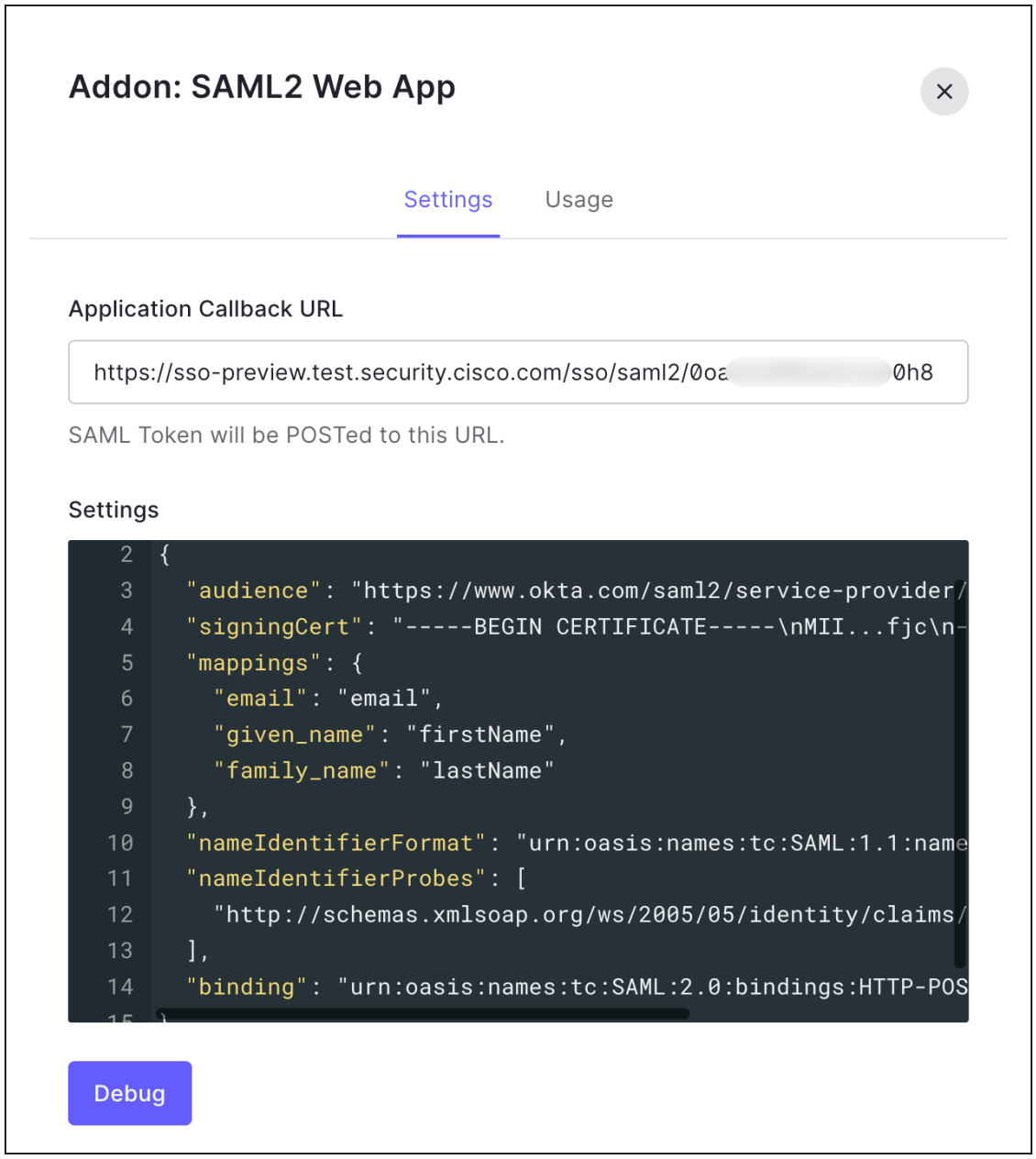
a) **Settings(**설정**)** 탭을 클릭합니다.

b) 엔터프라이즈 설정 마법사에서 복사한 **SSO(Single Sign-On)** 서비스 **URL**의 값을 **Application Callback URL(**애플리케이션 콜백 **URL)** 필드에 입력합니다.

c) 선택적으로, **Debug(**디버그**)**를 클릭하여 샘플 SAML 응답의 구조와 콘텐츠를 확인합니다(응답을 디버깅하려면 Auth0 사용자가 SAML 애플리케이션에 할당되어야 합니다).

d) **Settings(**설정**)** 필드에 다음 JSON 개체를 입력합니다. <ENTITY_ID_URI>를 이전에 복사한 **Entity ID (Audience URI)(**엔터티 **ID(**대상 **URI))** 필드의 값으로 대체하고 <SIGNING_CERT>를 한 줄 문자열로 변환하여 다운로드한 SecureX 로그인 서명 인증서(PEM 파일)의 콘텐츠로 바꿉니다.

```
{
  "audience": "https://www.okta.com/saml2/...",
  "signingCert": "-----BEGIN CERTIFICATE-----\n...-----END CERTIFICATE-----\n",
  "mappings": {
    "email": "email",
    "given_name": "firstName",
    "family_name": "lastName"
  },
  "nameIdentifierFormat": "urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified",
  "nameIdentifierProbes": [
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
  ],
  "binding": "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
}
```



e) 대화 상자의 아래쪽에 있는 **Enable(**활성화**)**을 클릭하여 SAML 애플리케이션을 활성화합니다.

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

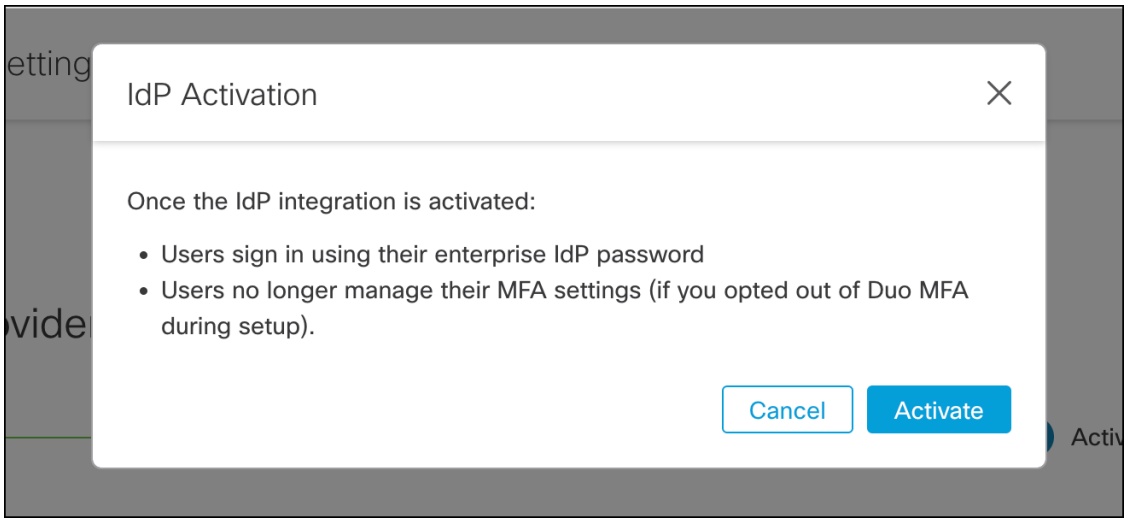
a) 표시된 URL을 복사하여 비공개(시크릿) 브라우저 창에서 엽니다.
브라우저는 Auth0 SSO 페이지로 리디렉션됩니다.

b) 클레임된 도메인과 일치하는 이메일 주소로 Auth0에 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