Okta

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 Okta SAML 애플리케이션을 생성하고 Security Cloud Sign On과(와) 통합하는 방법을 설명합니다.

시작하기

시작하기 전에

- 관리자 권한으로 Okta 대시보드에 로그인할 수 있어야 합니다.
- 엔터프라이즈 설정 마법사의 1단계: 엔터프라이즈 생성 및 2단계: 이메일 도메인 클레임 및 확인를 완료해야 합니다.

단계 **1** Okta 관리 콘솔에 로그인하고 다음을 수행합니다.

a) **Applications(**애플리케이션**)** 메뉴에서 **Applications(**애플리케이션**)**를 선택합니다.

b) **Create App Integration(**앱 통합 생성**)**을 클릭합니다.

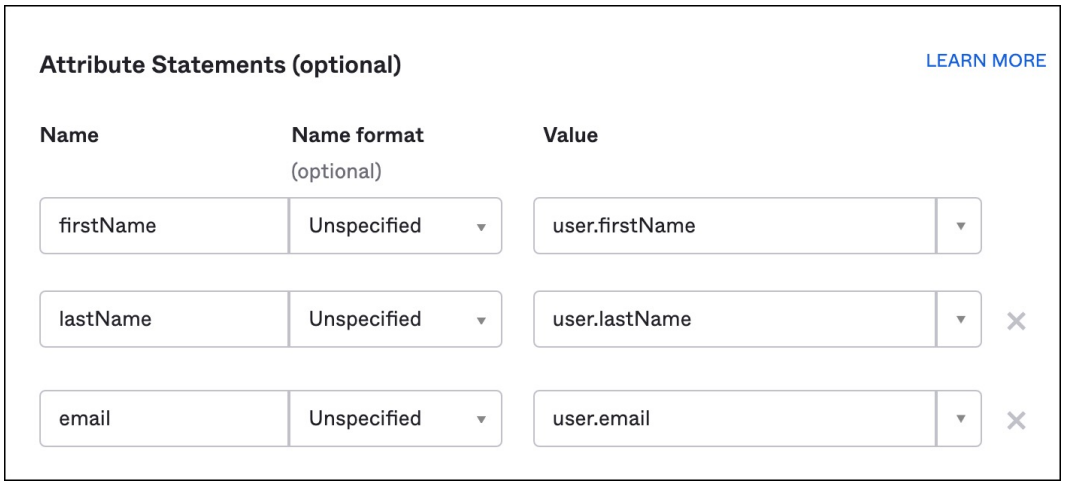
c) **SAML 2.0**을 선택하고 **Next(**다음**)**를 클릭합니다.

d) **General Settings(**일반 설정**)** 탭에서 통합의 이름(예: **Security Cloud Sign On**)을 입력하고 선택적으로 로고를 업로드합니다.

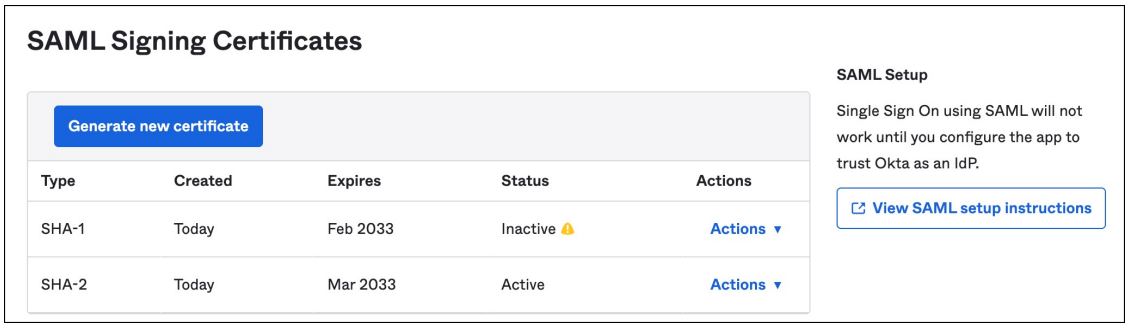
e) **Next(**다음**)**를 클릭합니다.
f) **Configure SAML(SAML** 구성**)** 탭에서.
g) **Single Sign on URL** 필드에서 임시 값(예: `https://example.com/sso`)을 입력합니다. 나중에 실제 Security Cloud Sign On ACS URL로 대체합니다.
h) **Audience URI(**대상 **URI)** 필드에 `https://example.com/audience`와 같은 임시 값을 입력합니다. 나중에 실제 Security Cloud Sign On 대상 ID URI로 대체합니다.
i) **Name ID format(**이름 **ID** 형식**)**에 대해 **Unspecified(**지정되지 않음**)** 또는 **EmailAddress**를 선택합니다.
j) **Application username(**애플리케이션 사용자 이름**)**에 대해 **Okta** 사용자 이름을 선택합니다.
k) **Attribute Statements(**속성 설명**)(**선택 사항**)** 섹션에서 다음 속성 매핑을 추가합니다.

이름**(SAML** 어설션에 있음**)**	값**(Okta** 프로파일에 있음**)**
email	user.email
firstName	user.firstName
lastName	user.email

그림 ***1:*** 속성 추가의 예



l) **Next(**다음**)**를 클릭합니다.
m) Okta에 피드백을 제공한 다음 **Finish(**완료**)**를 클릭합니다.
n) 사용자 그룹에 애플리케이션을 할당합니다.
o) **Sign On(**로그인**)** 탭에서.
p) 아래로 스크롤하여 **View SAML Setup Instructions(SAML** 설정 지침 보기**)**를 클릭합니다.



q) 열리는 페이지에서 **ID** 공급자 **Single Sign-On URL** 및 **ID** 공급자 발급자를 복사하고 **X.509** 인증서를 다운로드합니다.
다음으로 SAML 애플리케이션을 엔터프라이즈 설정 마법사의 Security Cloud Sign On과(와) 통합하기 시작합니다.

단계 **2** 새 브라우저 탭에서 엔터프라이즈 설정 마법사를 엽니다. 현재 3단계: SAML 메타데이터 교환에 있어야 합니다.

a) **Identity Provider Name(ID** 공급자 이름**)** 필드에 IdP의 이름(예:`Okta SSO`)을 입력합니다.
b) Okta에서 복사한 **ID** 공급자 **SSO(Single Sign-On) URL**의 값을 **Single Sign On Service URL** 필드에 입력합니다.
c) **Entity ID(**엔터티 **ID)** 필드에 Okta에서 복사한 **Identity Provider Issuer(ID** 공급자 발급자**)** 필드의 값을 입력합니다.
d) **Add File(**파일 추가**)**을 클릭하고 Okta에서 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) 다음 단계에서 사용할 수 있도록 **Single Sign-On Service URL (ACS URL)** 및 **Entity ID (Audience URI)** 필드의 값을 복사하고 저장합니다.
h) 다음 단계에서 사용할 **SAML** 서명 인증서(cisco-securex.pem)를 다운로드합니다.

단계 **3** Okta에서 SAML 애플리케이션 설정으로 돌아갑니다.

a) **General(**일반**)** 탭을 클릭합니다.
b) **SAML Settings(SAML** 설정**)** 섹션에서 **Edit(**편집**)**를 클릭합니다.
c) **Next(**다음**)**를 클릭합니다.
d) **Single sign-on URL**의 값을 엔터프라이즈 설정 마법사가 제공한 "Single Sign-On Service URL (ACS URL)" 필드의 값으로 교체합니다.
e) **Audience URI (SP Entity ID)(**대상 **URI (SP** 엔터티 **ID))**의 값을 엔터프라이즈 설정 마법사가 제공한 "Entity ID (Audience URI)(엔터티 ID(대상 URI))" 필드의 값으로 교체합니다.
f) **Show Advanced Settings(**고급 설정 표시**)**를 클릭하고 **Signature Certificate(**서명 인증서**)** 필드를 찾습니다.
g) **Browse files...(**파일 찾아보기**...)**를 클릭하고 이전에 다운로드한 Cisco SAML 서명 인증서를 찾습니다.
h) **Next(**다음**)**를 클릭합니다.
i) 변경 사항을 저장하려면 **Finish(**마침**)**를 클릭합니다.

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

a) 표시된 URL을 복사하여 비공개(시크릿) 브라우저 창에서 엽니다.
브라우저가 Okta 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.