Ping Identity

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 Ping Identity에서 SAML 애플리케이션을 생성하여 Security Cloud Sign On과(와) 통합하는 방법을 설명합니다.

시작하기

시작하기 전에

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

단계 **1** Ping ID 콘솔에서 다음을 수행합니다.

a) **Connections(**연결**)** > **Applications(**애플리케이션**)**로 이동합니다.

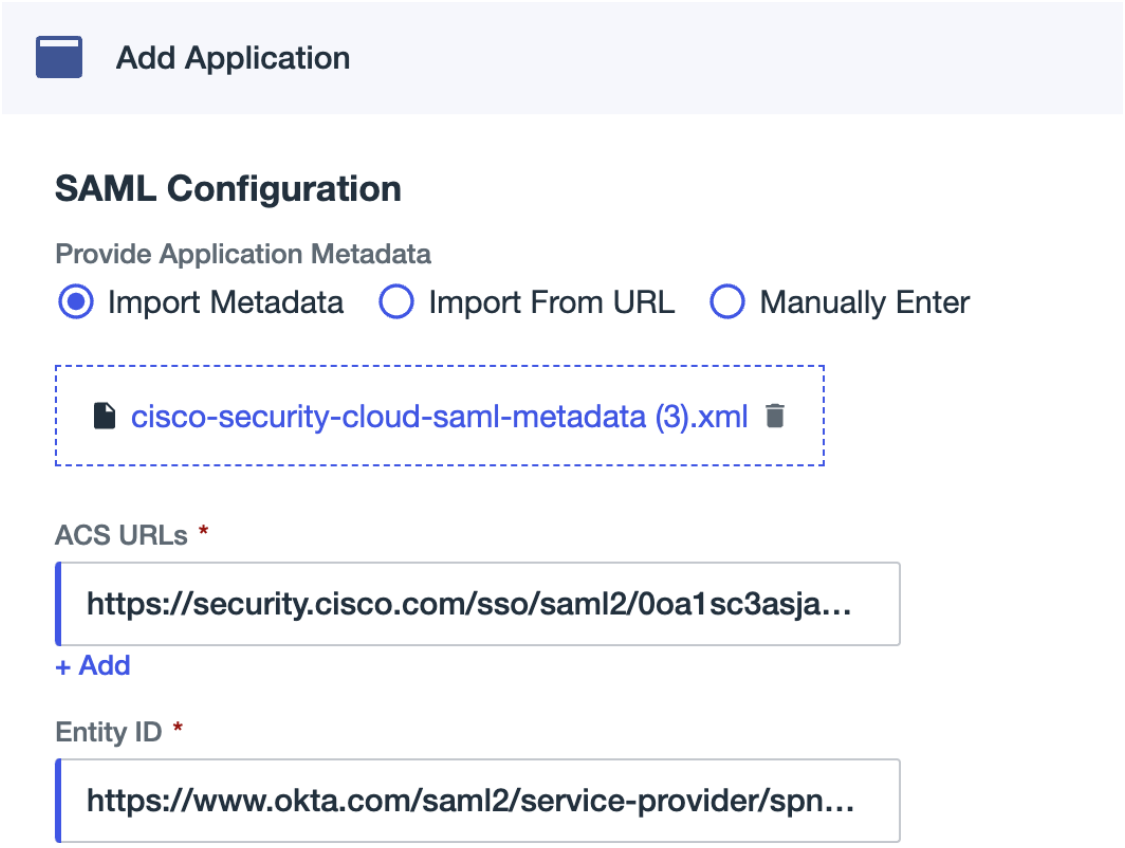
b) **+** 버튼을 클릭하여 **Add Application(**애플리케이션 추가**)** 대화 상자를 엽니다.

c) **Application Name(**애플리케이션 이름**)** 필드에 **`Secure Cloud Sign On`** 또는 다른 이름을 입력합니다.

d) 선택 사항으로 설명을 추가하고 아이콘을 업로드합니다.

e) **Application Type(**애플리케이션 유형**)**에 대해 **SAML** 애플리케이션을 선택한 다음 **Configure(**구성**)**를 클릭합니다.

f) **SAML Configuration(SAML** 구성**)** 대화 상자에서 SAML 메타데이터를 수동 입력하는 옵션을 선택하고 **ACS URL** 및 엔터티 **ID**에 대한 임시 URL을 입력합니다. 나중에 실제 URL로 대체합니다.



g) **Save(**저장**)**를 클릭합니다.

h) **Configuration(**구성**)** 탭을 클릭합니다.

i) **Download Signing Certificate(**서명 인증서 다운로드**)**를 클릭합니다.

j) 다음 단계에서 사용할 발급자 **ID** 및 **SSO(Single Sign-On)** 서비스 속성의 값을 복사합니다.

k) **Attribute Mappings(**속성 매핑**)** 탭을 클릭합니다.

l) 편집(연필) 아이콘을 클릭합니다.

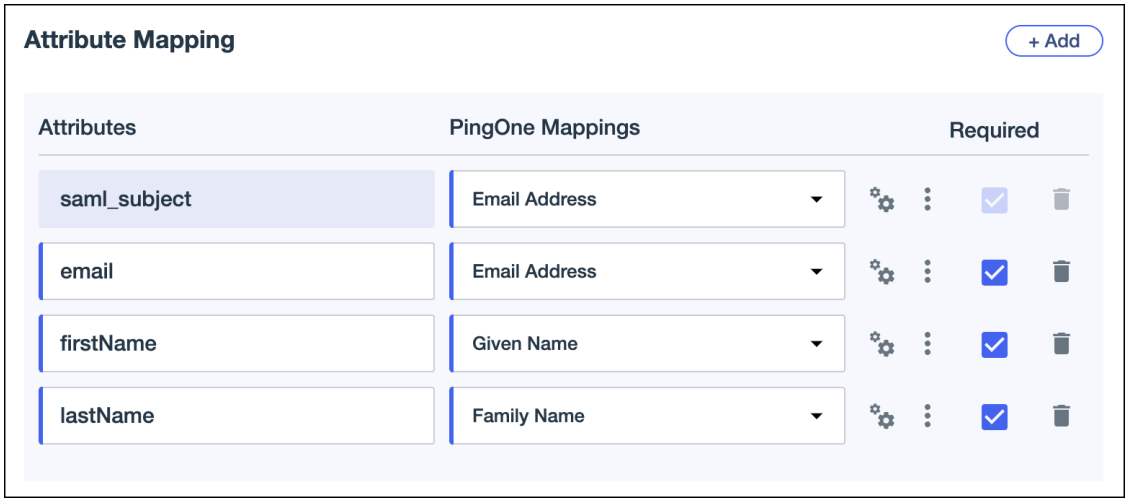
m) 필수 **saml_subject** 속성의 경우 **Email Address(**이메일 주소**)**를 선택합니다.

n) **+Add(**추가**)**를 클릭하고 다음 SAML 속성 매핑을 PingOne 사용자 ID 속성에 추가하여 각 매핑에 대해 **Required(**필수**)** 옵션을 활성화합니다.

특성	**PingOne** 매핑
firstName	이메일 주소
lastName	이름

특성	**PingOne** 매핑
email	제품군 이름

Attribute Mapping(속성 매핑) 패널은 다음과 같이 표시됩니다.



o) **Save(**저장**)**를 클릭하여 매핑을 저장합니다.

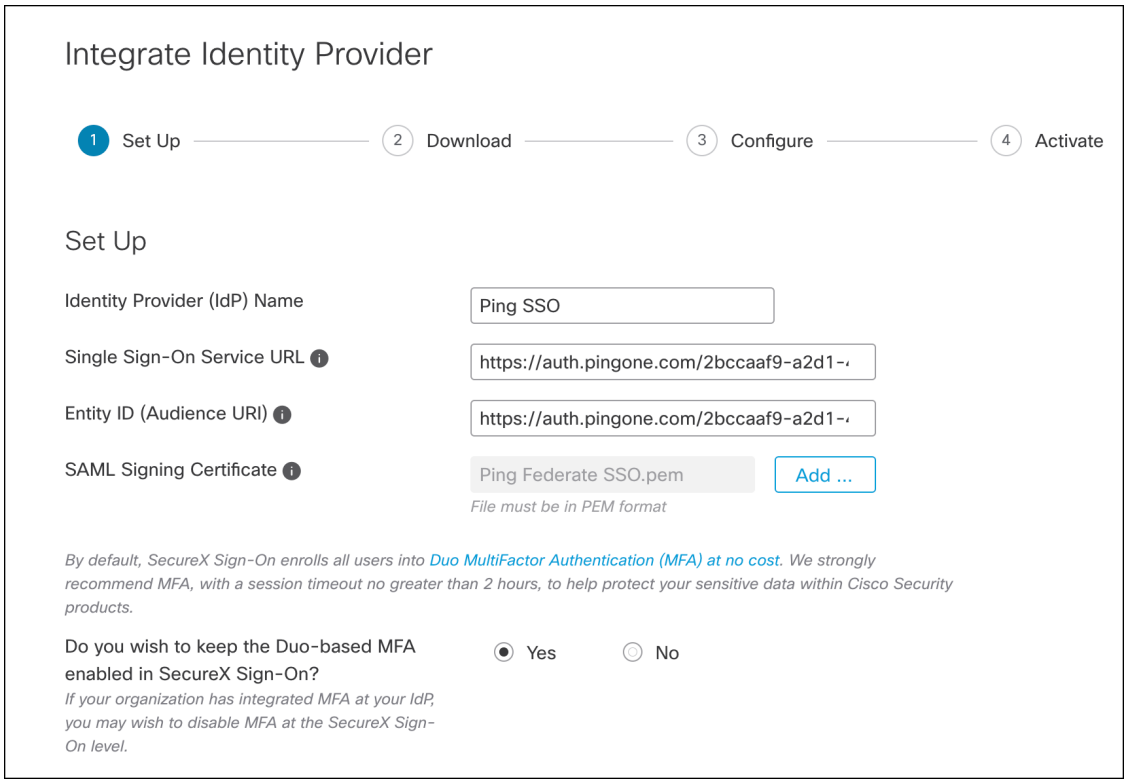
단계 **2** 새 브라우저 탭에서 Enterprise 설정 마법사를엽니다. 현재 **Integrate Identity Provider(ID** 공급자 통합**)** 화면(3단계: SAML 메타데이터 교환)의 **Set Up(**설정**)** 단계에 있어야 합니다.

a) **Identity Provider (IdP) Name(ID** 공급자**(IdP)** 이름**)** 필드에 통합의 이름(예: `Ping SSO`)을 입력합니다.

b) Ping SAML 애플리케이션에서 복사한 **Issuer ID(**발급자 **ID)** 필드의 값을 **Single Sign-On Service URL** 필드에 입력합니다.

c) **Add...(**추가**...)**를 클릭하고 이전에 다운로드한 Ping 서명 인증서를 선택합니다.

d) 원하는 경우 사용자에 대해 무료로 Duo 다단계 인증을 옵트아웃할 수 있습니다.



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

f) **Download(**다운로드**)** 화면에서 **Single Sign-On Service URL (ACS URL)(SSO** 서비스 **URL(ACS URL))** 및 **Entity ID (Audience URI)(**엔터티 **ID(**대상 **URI))** 속성의 값을 복사하고 **Download(**다운로드**)**를 클릭하여 서명 인증서를 다운로드합니다.

단계 **3** Ping ID 콘솔로 돌아가 다음 작업을 수행합니다.

a) **Configuration(**구성**)** 탭에서 편집(연필) 아이콘을 클릭합니다.

b) **ACS URL** 필드의 임시 URL을 이전 단계에서 복사한 "Single Sign-On Service URL(ACS URL)"로 바꿉니다.

c) **Entity ID(**엔터티 **ID)** 필드의 임시 URL을 이전 단계에서 복사한 "엔터티 ID (대상 URI)"로 대체합니다.

d) **Verification Certificate(**확인 인증서**)** 필드에 대해 **Import(**가져오기**)** 옵션을 선택하고 **Choose File(**파일 선택**)**을 클릭합니다.

e) 이전 단계에서 다운로드한 Security Cloud Sign On 서명 인증서를 선택합니다.

f) **Save(**저장**)**를 클릭합니다.

g) 애플리케이션 구성 패널 상단의 토글을 클릭하여 애플리케이션에 대한 사용자 액세스를 활성화합니다.

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

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

b) 클레임된 도메인과 일치하는 이메일 주소로 Ping ID에 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.