ID 서비스 제공자 지침

이 가이드에서는 다양한 ID 서비스 제공자와 보안 클라우드 로그인을 통합하기 위한 지침을 제공합니다.

Auth0과 Security Cloud Sign On 통합

이 가이드에서는 Auth0 SAML 애드온을 보안 클라우드 로그인과 통합하는 방법을 설명합니다.

시작하기 전에

시작하기 전에 ID 제공자 통합 가이드의 내용을 읽고 전체 프로세스를 파악하십시오. 이 지침은 Auth0 SAML 통합 관련 세부 사항, 그중에서도 2단계: ID 제공자에 보안 클라우드 SAML 메타데이터 제공 및 3단계: IdP에서 보안 클라우드로 SAML 메타데이터 제공를 사용하여 해당 가이드를 보완합니다.

단계 **1** Auth0과 통합할 엔터프라이즈로 보안 클라우드 제어에 로그인합니다.

a) 1단계: 초기 설정의 설명에 따라 새 ID 제공자를 생성하고 Duo MFA의 옵트아웃 여부를 결정합니다.

b) 2단계: ID 제공자에 보안 클라우드 SAML 메타데이터 제공에서 공용 인증서를 다운로드하고, 다음 단계에서 사용할 엔터티 **ID** 및 **SSO(Single Sign-On)** 서비스 **URL**의 값을 복사합니다.

단계 **2** 새 브라우저 탭에서 Auth0 조직에 관리자로 로그인합니다. 곧 돌아올 것이므로 Security Cloud Control(보안 클라우드 제어) 브라우저 탭을 열어 둡니다.

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

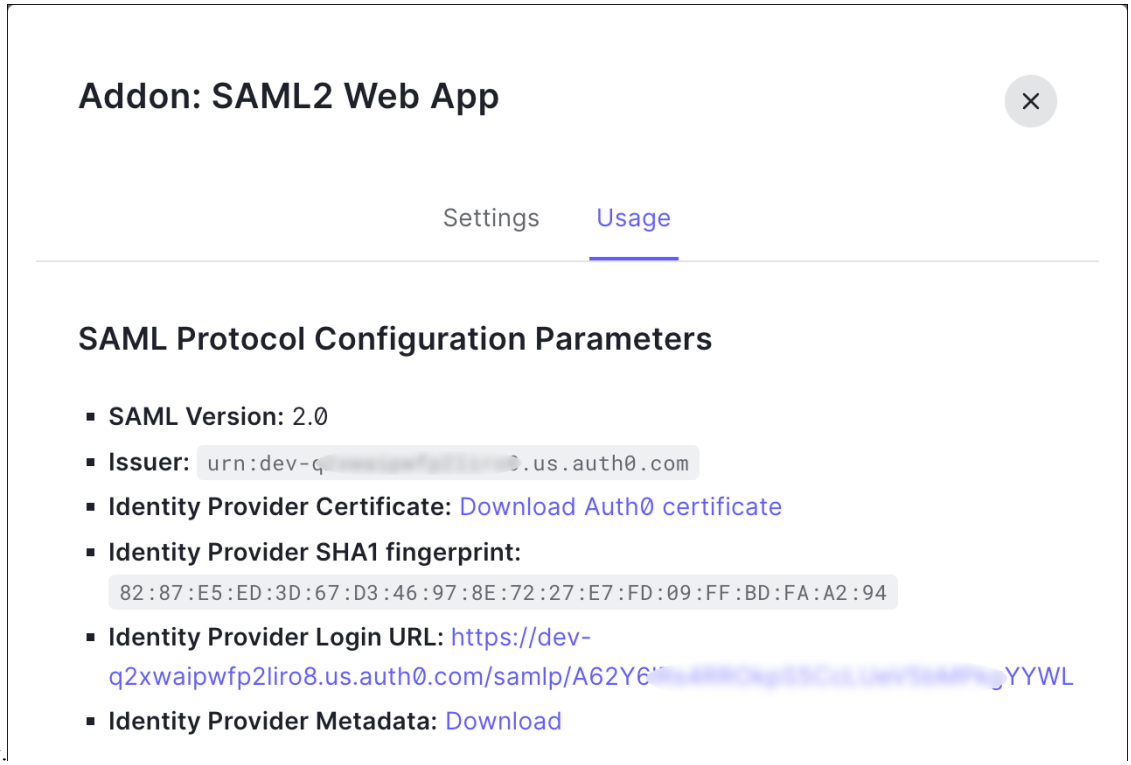
b) **Create Application(**애플리케이션 생성**)**을 클릭합니다.

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) **Usage(**사용**)** 탭에서 Auth0 **Identity Provider Certificate(ID** 제공자 인증서**)**와 **Identity Provider Metadata(ID** 제공자 메타데이터**)** 파일을 다운로드합니다.

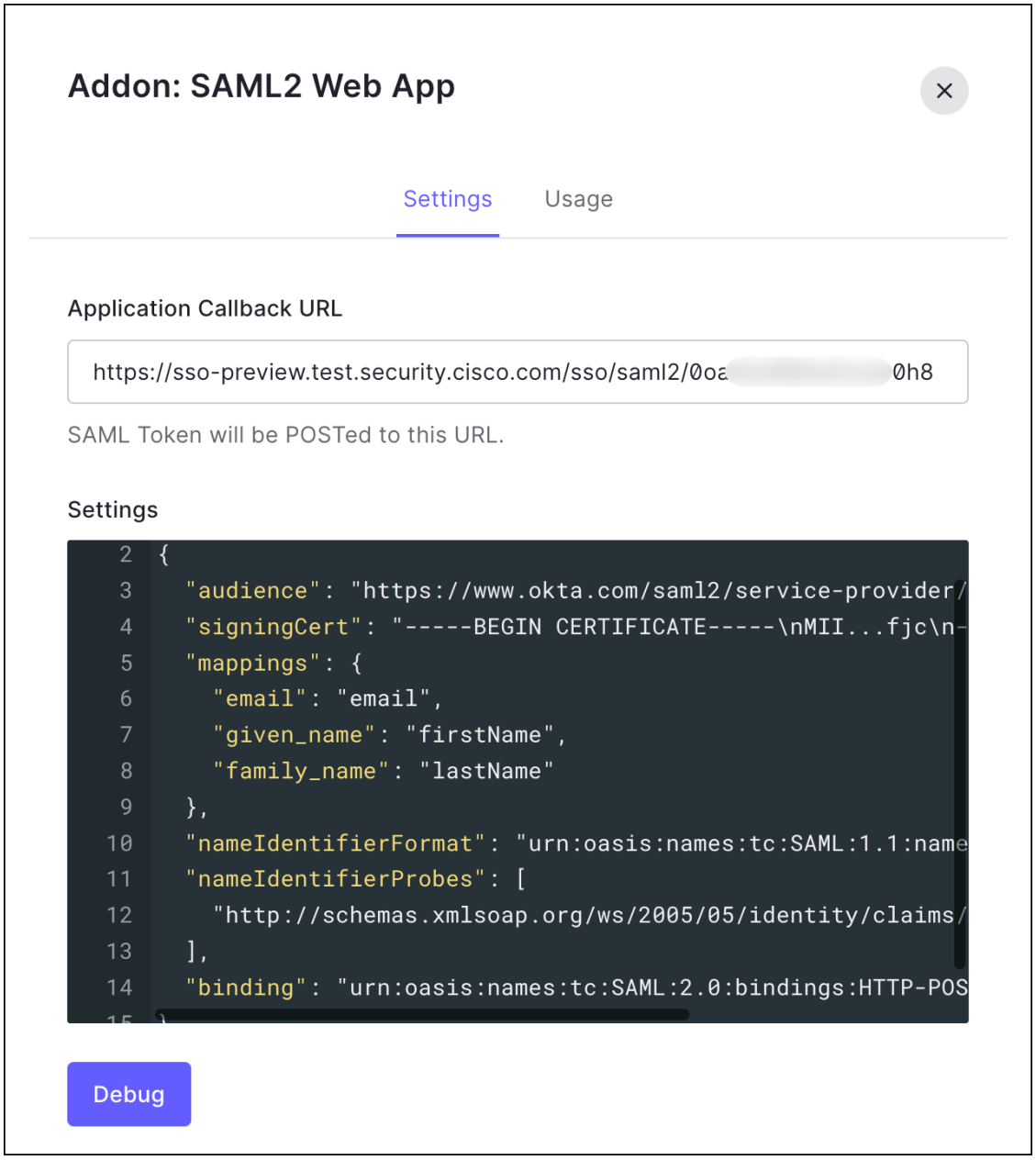
h) **Settings(**설정**)** 탭을 클릭합니다.

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

j) **Settings(**설정**)** 필드에서 다음 JSON 개체를 입력하여 `audience(대상)`의 값을 제공된 엔터티 **ID(**대상 **URI)**의 값으로 대체하고, `signingCert`를 한 줄의 텍스트로 변환된 보안 클라우드 제어에서 제공한 서명 인증서의 내용으로 대체합니다.

```
{
  "audience": "...",
  "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"
```

}



k) **Addon(**애드온**)** 대화 상자의 아래쪽에 있는 **Enable(**활성화**)**을 클릭하여 애플리케이션을 활성화합니다.

단계 **3** 보안 클라우드 제어로 돌아가서 **Next(**다음**)**를 클릭합니다. 사용자는 3단계: IdP에서 보안 클라우드로 SAML 메타데이터 제공에 있어야 합니다.

a) **XML file upload(XML** 파일 업로드**)** 옵션을 선택합니다.

b) Auth0에서 제공한 **ID** 제공자 메타데이터 파일을 업로드합니다.

다음에 수행할 작업

다음으로 4단계: SAML 통합 테스트 및 5단계: 통합 활성화의 지침에 따라 통합을 테스트하고 활성화합니다.

Azure AD와 Security Cloud Sign On 통합

이 가이드에서는 Azure AD를 보안 클라우드 제어와 통합하는 방법을 설명합니다.

시작하기 전에

시작하기 전에 ID 제공자 통합 가이드의 내용을 읽고 전체 프로세스를 파악하십시오. 이 지침은 Azure AD SAML 통합 관련 세부 사항, 그중에서도 2단계: ID 제공자에 보안 클라우드 SAML 메타데이터 제공 및 3단계: IdP에서 보안 클라우드로 SAML 메타데이터 제공를 사용하여 해당 가이드를 보완합니다.

단계 **1** Azure AD와 통합할 엔터프라이즈로 보안 클라우드 제어에 로그인합니다.

a) 1단계: 초기 설정의 설명에 따라 새 ID 제공자를 생성하고 Duo MFA의 옵트아웃 여부를 결정합니다.

b) 2단계: ID 제공자에 보안 클라우드 SAML 메타데이터 제공에서 공용 인증서를 다운로드하고, 다음 단계에서 사용할 엔터티 **ID** 및 **SSO(Single Sign-On)** 서비스 **URL**의 값을 복사합니다.

단계 **2** 새 브라우저 탭에서 https://portal.azure.com에 관리자로 로그인합니다. 곧 돌아올 것이므로 Security Cloud Control(보안 클라우드 제어) 탭을 열어 둡니다.

계정에서 둘 이상의 테넌트에 액세스할 수 있는 경우 오른쪽 상단에서 계정을 선택합니다. 포털 세션을 원하는 Azure AD 테넌트로 설정합니다.

a) **Azure Active Directory**를 클릭합니다.

b) 왼쪽 사이드바에서 **Enterprise Applications(**엔터프라이즈 애플리케이션**)**을 클릭합니다.

c) **+ New Application(+** 새 애플리케이션**)**을 클릭하고 **`Azure AD SAML`** 툴킷을 검색합니다.

d) **Azure AD SAML Toolkit(Azure AD SAML** 툴킷**)**을 클릭합니다.

e) **Name(**이름**)** 필드에 **`Security Cloud Sign On`** 또는 다른 값을 입력하고 **Create(**생성**)**를 클릭합니다.

f) Overview(개요) 페이지의 왼쪽 사이드바에서 **Manage(**관리**)** 아래 **Single Sign On(**단일 인증**)**을 클릭합니다.

g) SSO(Single Sign-On, 단일 인증) 방법 선택 시 **SAML**을 선택합니다.

h) **Basic SAML Configuration(**기본 **SAML** 구성**)** 패널에서 **Edit(**편집**)**를 클릭하고 다음을 수행합니다.

- **Identifier (Entity ID)(**식별자**(**엔터티 **ID))**에서 **Add Identifier(**식별자 추가**)**를 클릭하고 보안 클라우드 제어에서 제공된 엔터티 **ID** URL을 입력합니다.
- **Reply URL (Assertion Consumer Service URL)(**회신 **URL (**어설션 소비자 서비스 **URL))**에서 **Add reply URL(**회신 **URL** 추가**)**를 클릭하고 보안 클라우드 제어의 **SSO(Single Sign-On)** 서비스 **URL**을 입력합니다.
- **Sign-on URL(**로그인 **URL)** 필드에 **`https://sign-on.security.cisco.com/`**을 입력합니다.
- **Save(**저장**)**를 클릭하고 **Basic SAML Configuration(**기본 **SAML** 구성**)** 패널을 닫습니다.

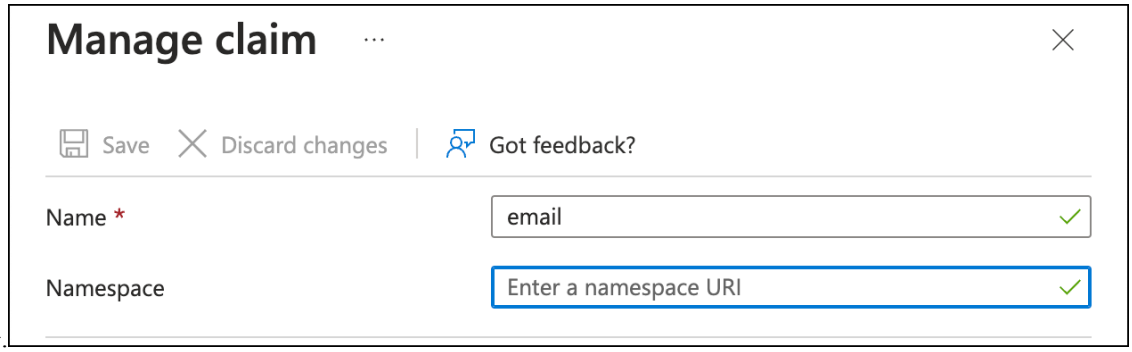
i) **Attributes and Claims(**속성 및 클레임**)** 패널에서 **Edit(**편집**)**를 클릭합니다.

- **Required claim(**필수 클레임**)**에서 고유 사용자 식별자**(**이름 **ID)** 클레임을 클릭하여 편집합니다.
- **Source(**소스**)** 속성 필드를 `user.userprincipalname`으로 설정합니다. 이 섹션에서는 **user.userprincipalname**의 값이 유효한 이메일 주소를 나타내는 것으로 가정합니다. 그렇지 않은 경우 **Source(**소스**)**를 **user.primaryauthoritativeemail**로 설정합니다.

j) **Additional Claims(**추가 클레임**)** 패널에서 **Edit(**편집**)**를 클릭하고 Azure AD 사용자 속성과 SAML 특성 간에 다음 매핑을 생성합니다.

이름	네임스페이스	소스 속성
`email`	값 없음	`user.userprincipalname`
`firstName`	값 없음	`user.givenname`
`lastName`	값 없음	`user.surname`

아래에 나와 있는 것처럼 각 클레임에 대한 **Namespace(**네임스페이스**)** 필드의 선택을 취소해야 합니다.



k) **SAML Certificates(SAML** 인증서**)** 패널에서 인증서**(Base64)** 인증서에 대해 **Download(**다운로드**)**를 클릭합니다.

l) **Set up Single Sign-On with SAML(SAML**을 이용한 **SSO** 설정**)** 섹션에서 로그인 **URL** 및 **Azure AD** 식별자의 값을 복사하여 이 절차의 뒷부분에서 사용할 수 있습니다.

단계 **3** 보안 클라우드 제어로 돌아가서 **Next(**다음**)**를 클릭합니다. 사용자는 3단계: IdP에서 보안 클라우드로 SAML 메타데이터 제공에 있어야 합니다.

a) **Manual Configuration(**수동 구성**)** 옵션을 선택합니다.

b) **SSO(Single Sign-On)** 서비스 **URL(**어설션 소비자 서비스 **URL)** 필드에 Azure에서 제공하는 로그인 **URL** 값을 입력합니다.

c) **Entity ID (Audience URI)(**엔터티 **ID(**대상 **URI))** 필드에 Azure AD에서 제공한 **Azure AD** 식별자 값을 입력합니다.

d) Azure에서 제공하는 서명 인증서를 업로드합니다.

단계 **4** **Security Cloud Control(**보안 클라우드 제어**)**에서 **Next(**다음**)**를 클릭합니다.

다음에 수행할 작업

4단계: SAML 통합 테스트 및 5단계: 통합 활성화에 따라 통합을 테스트하고 활성화합니다.

Duo와 Security Cloud Sign On 통합

이 가이드에서는 Duo SAML 애플리케이션을 보안 클라우드 로그인과 통합하는 방법을 설명합니다.

시작하기 전에

시작하기 전에 ID 제공자 통합 가이드의 내용을 읽고 전체 프로세스를 파악하십시오. 이 지침은 Duo SAML 통합 관련 세부 사항, 그중에서도 2단계: ID 제공자에 보안 클라우드 SAML 메타데이터 제공 및 3단계: IdP에서 보안 클라우드로 SAML 메타데이터 제공를 사용하여 해당 가이드를 보완합니다.

단계 **1** Duo와 통합할 엔터프라이즈로 보안 클라우드 제어에 로그인합니다.

a) 1단계: 초기 설정의 설명에 따라 새 ID 제공자를 생성하고 Duo MFA의 옵트아웃 여부를 결정합니다.

b) 2단계: ID 제공자에 보안 클라우드 SAML 메타데이터 제공에서 공용 인증서를 다운로드하고, 다음 단계에서 사용할 엔터티 **ID** 및 **SSO(Single Sign-On)** 서비스 **URL**의 값을 복사합니다.

단계 **2** 새 브라우저 탭에서 관리자로 Duo 조직에 로그인합니다. 곧 돌아올 것이므로 Security Cloud Control(보안 클라우드 제어) 탭을 열어 둡니다.

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.

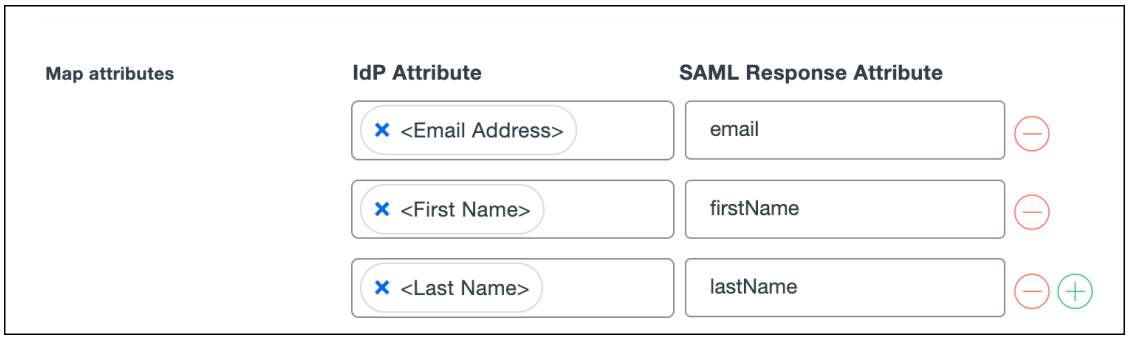
g) 나중에 사용할 수 있도록 Downloads(다운로드) 섹션에서 **Download certificate(**인증서 다운로드**)**를 클릭합니다.

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**

IdP 속성	SAML 응답 속성
<Last Name>	**lastName**



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

단계 **3** 보안 클라우드 제어로 돌아가서 **Next(**다음**)**를 클릭합니다. 사용자는 3단계: IdP에서 보안 클라우드로 SAML 메타데이터 제공에 있어야 합니다.

a) **Manual Configuration(**수동 구성**)** 옵션을 선택합니다.
b) **SSO(Single Sign-On)** 서비스 **URL(**어설션 소비자 서비스 **URL)** 필드에 Duo에서 제공한 **SSO(Single Sign-On) URL** 값을 입력합니다.
c) **Entity ID (Audience URI)(**엔터티 **ID(**대상 **URI))** 필드에 Duo에서 제공한 엔터티 **ID** 값을 입력합니다.
d) Duo에서 다운로드한 서명 인증서를 업로드합니다.

다음에 수행할 작업

다음으로 4단계: SAML 통합 테스트 및 5단계: 통합 활성화의 지침에 따라 통합을 테스트하고 활성화합니다.

Google Identity와 Security Cloud Sign On 통합

이 가이드에서는 Google ID SAML 애플리케이션을 Security Cloud Sign On과 통합하는 방법을 설명합니다.

시작하기 전에

시작하기 전에 ID 제공자 통합 가이드의 내용을 읽고 전체 프로세스를 파악하십시오. 이 지침은 Google Identity 통합 관련 세부 사항, 그중에서도 2단계: ID 제공자에 보안 클라우드 SAML 메타데이터 제공 및 3단계: IdP에서 보안 클라우드로 SAML 메타데이터 제공를 사용하여 해당 가이드를 보완합니다.

단계 **1** Google과 통합할 엔터프라이즈로 보안 클라우드 제어에 로그인합니다.

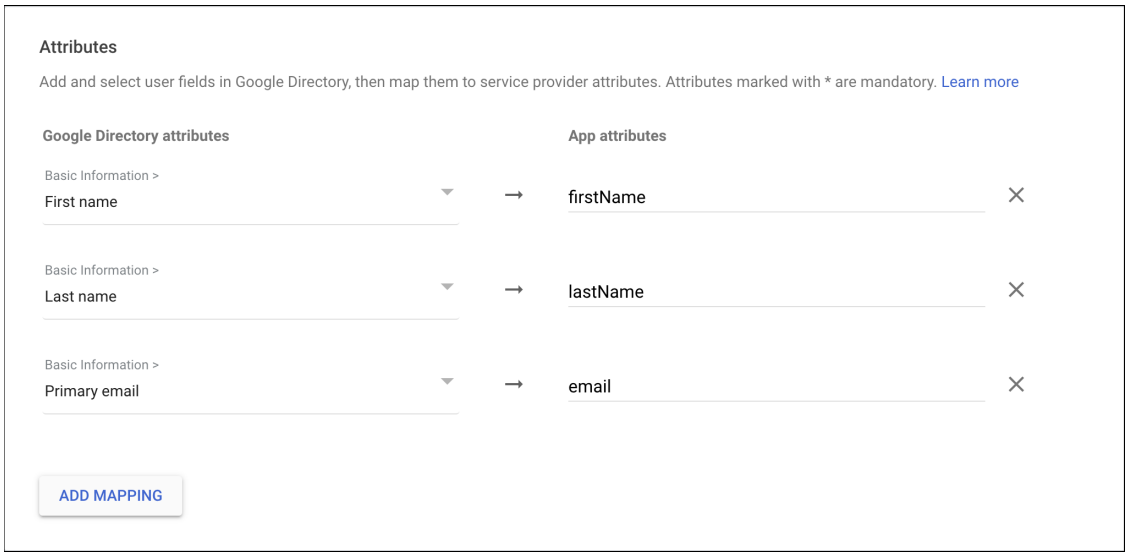
a) 1단계: 초기 설정의 설명에 따라 새 ID 제공자를 생성하고 Duo MFA의 옵트아웃 여부를 결정합니다.

b) 2단계: ID 제공자에 보안 클라우드 SAML 메타데이터 제공에서 공용 인증서를 다운로드하고, 다음 단계에서 사용할 엔터티 **ID** 및 **SSO(Single Sign-On)** 서비스 **URL**의 값을 복사합니다.

단계 **2** 새 브라우저 탭에서 슈퍼 관리자 권한이 있는 계정을 사용하여 Google 관리 콘솔에 로그인합니다. Security Cloud Control 탭을 열어 둡니다.

a) 관리 콘솔에서 Menu(메뉴) > **Apps(앱)** > **Web and mobile apps(웹 및 모바일 앱)**로 이동합니다.
b) **Add App(앱 추가)** > **Add custom SAML app(사용자 지정 SAML 앱 추가)**을 클릭합니다.
c) **App Details(앱 세부 정보)** 페이지에서:
   - 애플리케이션 이름으로 `Secure Cloud Sign On` 또는 다른 값을 입력합니다.
   - 아이콘을 업로드하여 애플리케이션과 연결할 수도 있습니다.
d) **Continue(계속)**를 클릭하여 **Google ID** 제공자 세부정보 페이지로 이동합니다.
e) **Download Metadata(메타데이터 다운로드)**를 클릭하여 나중에 사용할 수 있도록 Google SAML 메타데이터 파일을 다운로드합니다.
f) **Continue(계속)**를 클릭하여 **Service provider details(서비스 제공자 세부 정보)** 페이지로 이동합니다.
g) **ACS URL** 필드에 Security Cloud Control에서 제공하는 **Single Sign-On** 서비스 **URL**을 입력합니다.
h) Security Cloud Control에서 제공한 **Entity ID(엔터티 ID)** URL을 **Entity ID(엔터티 ID)** 필드에 입력합니다.
i) **Signed Response(서명한 응답)** 옵션을 선택합니다.
j) **Name ID Format(이름 ID 형식)**에 대해 `UNSPECIFIED` 또는 `EMAIL`을 선택합니다.
k) **Name ID(이름 ID)**에 대해 **Basic Information(기본 정보) - Primary Email(기본 이메일)**을 선택합니다.
l) **Continue(계속)**를 클릭하여 **Attribute mapping(속성 매핑)** 페이지로 이동합니다.
m) 다음 Google Directory 속성 매핑을 앱 속성에 추가합니다.

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



n) 마침을 클릭합니다.

단계 **3** 보안 클라우드 제어로 돌아가서 **Next(**다음**)**를 클릭합니다. 사용자는 3단계: IdP에서 보안 클라우드로 SAML 메타데이터 제공에 있어야 합니다.

a) **XML file upload(XML** 파일 업로드**)** 옵션을 선택합니다.
b) Google에서 이전에 다운로드한 SAML 메타데이터 파일을 업로드합니다.
c) **Next(**다음**)**를 클릭하여 테스트 페이지로 이동합니다.

다음에 수행할 작업

다음으로 4단계: SAML 통합 테스트 및 5단계: 통합 활성화의 지침에 따라 통합을 테스트하고 활성화합니다.

Okta와 Security Cloud Sign On 통합

이 가이드에서는 Okta SAML 애플리케이션을 Security Cloud Control과 통합하는 방법을 설명합니다.

시작하기 전에

시작하기 전에 ID 제공자 통합 가이드의 내용을 읽고 전체 프로세스를 파악하십시오. 이 지침은 Okta SAML 통합 관련 세부 사항, 그중에서도 2단계: ID 제공자에 보안 클라우드 SAML 메타데이터 제공 및 3단계: IdP에서 보안 클라우드로 SAML 메타데이터 제공를 사용하여 해당 가이드를 보완합니다.

단계 **1** Okta와 통합할 엔터프라이즈로 보안 클라우드 제어에 로그인합니다.

a) 1단계: 초기 설정의 설명에 따라 새 ID 제공자를 생성하고 Duo MFA의 옵트아웃 여부를 결정합니다.
b) 2단계: ID 제공자에 보안 클라우드 SAML 메타데이터 제공에서 공용 인증서를 다운로드하고, 다음 단계에서 사용할 엔터티 **ID** 및 **SSO(Single Sign-On)** 서비스 **URL**의 값을 복사합니다.

단계 2 새 브라우저 탭에서 Okta 조직에 관리자로 로그인합니다. 곧 돌아올 것이므로 Security Cloud Control(보안 클라우드 제어) 탭을 열어 둡니다.

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 클릭하여 **Configure SAML(SAML** 구성**)** 화면으로 이동합니다.
f) **Single Sign-On URL** 필드에 Security Cloud Control에서 제공하는 **Single Sign-On** 서비스 **URL**을 입력합니다.
g) Security Cloud Control에서 제공한 **Entity ID(**엔터티 **ID)**를 **Audience URI(**대상 **URI)** 필드에 입력합니다.
h) **Name ID format(**이름 **ID** 형식**)**에 대해 **Unspecified(**지정되지 않음**)** 또는 **EmailAddress**를 선택합니다.
i) **Application username(**애플리케이션 사용자 이름**)**에 대해 **Okta** 사용자 이름을 선택합니다.
j) **Attribute Descriptions(**속성 설명**)(**선택 사항**)** 섹션에서 다음 이름 SAML 속성 매핑을 Okta 사용자 프로파일 값에 추가합니다.

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

k) **Show Advanced Settings(**고급 설정 표시**)**를 클릭합니다.
l) **Next(**다음**)**를 클릭합니다.
m) **Signature Certificate(**서명 인증서**)**의 경우 **Browse files...(**파일 찾아보기**...)**를 클릭하고 Security Cloud Control에서 이전에 다운로드한 공개 서명 인증서를 업로드합니다.

참고 응답 및 어설션은 RSA-SHA256 알고리즘으로 서명되어야 합니다.

n) **Sign On(**로그인**)** → **Settings(**설정**)** → **Sign on method(**로그인 방법**)**에서 **Show details(**세부 정보 표시**)**를 클릭합니다.
o) **Next(**다음**)**를 클릭하고 Okta에 피드백을 제공한 다음 **Finish(**완료**)**를 클릭합니다.
p) **Sign on URL(**로그인 **URL)** 및 **Issuer(**발급자**)**의 값을 복사하고 서명 인증서를 다운로드하여 Security Cloud Control에 제공합니다.

단계 3 보안 클라우드 제어로 돌아가서 **Next(**다음**)**를 클릭합니다. 사용자는 3단계: IdP에서 보안 클라우드로 SAML 메타데이터 제공에 있어야 합니다.

a) **Manual Configuration(**수동 구성**)** 옵션을 선택합니다.
b) **SSO(Single Sign-On)** 서비스 **URL(**어설션 소비자 서비스 **URL)** 필드에 Okta에서 제공한 로그인 **URL** 값을 입력합니다.
c) **Entity ID (Audience URI)(**엔터티 **ID(**대상 **URI))** 필드에 Okta에서 제공한 **Issuer(**발급자**)** 값을 입력합니다.
d) Okta에서 제공하는 서명 인증서를 업로드합니다.

다음에 수행할 작업

다음으로 4단계: SAML 통합 테스트 및 5단계: 통합 활성화의 지침에 따라 통합을 테스트하고 활성화합니다.

Ping Identity와 Security Cloud Sign On 통합

이 가이드에서는 Ping 애플리케이션을 보안 클라우드 로그인과 통합하는 방법을 설명합니다.

시작하기 전에

시작하기 전에 ID 제공자 통합 가이드의 내용을 읽고 전체 프로세스를 파악하십시오. 이 지침은 Ping 통합 관련 세부 사항, 그중에서도 2단계: ID 제공자에 보안 클라우드 SAML 메타데이터 제공 및 3단계: IdP에서 보안 클라우드로 SAML 메타데이터 제공를 사용하여 해당 가이드를 보완합니다.

단계 **1** Ping과 통합할 엔터프라이즈로 보안 클라우드 제어에 로그인합니다.

a) 1단계: 초기 설정의 설명에 따라 새 ID 제공자를 생성하고 Duo MFA의 옵트아웃 여부를 결정합니다.

b) 2단계: ID 제공자에 보안 클라우드 SAML 메타데이터 제공에서 나중에 사용할 수 있도록 **Security Cloud Sign On SAML** 메타데이터 파일을 다운로드합니다.

단계 **2** 새 브라우저 탭에서 Ping 관리 콘솔에 로그인합니다. Security Cloud Control 브라우저 탭을 열어 둡니다.

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

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

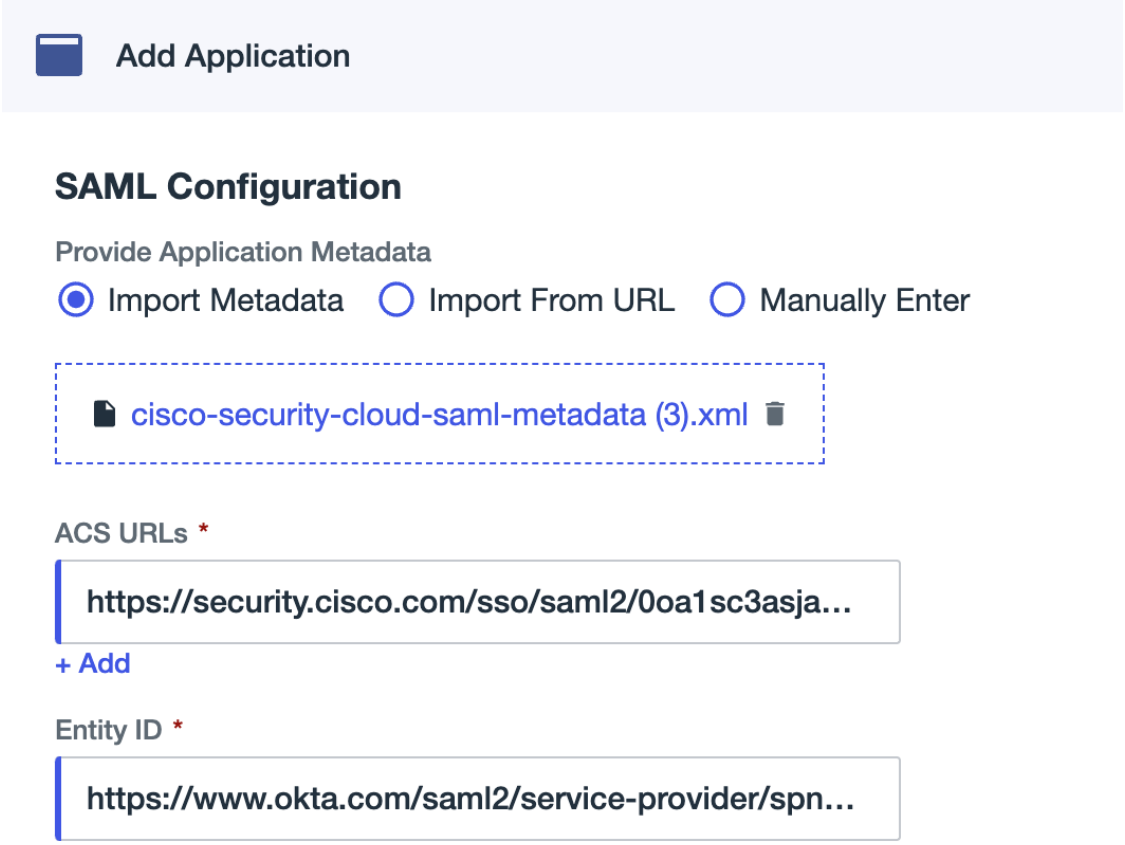
c) **Application Name(**애플리케이션 이름**)** 필드에 **`Secure Cloud Sign On`** 또는 다른 이름을 입력합니다.

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 **Import Metadata(**메타데이터 가져오기**)** 옵션을 선택하고 **Select a file(**파일 선택**)**을 클릭합니다.

g) Security Cloud Control에서 다운로드한 **Security Cloud Sign On SAML** 메타데이터 파일을 찾습니다.



h) **Save(**저장**)**를 클릭합니다.

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

j) **Download Metadata(**메타데이터 다운로드**)**를 클릭하여 Security Cloud Control에 제공할 SAML 메타데이터 파일을 다운로드합니다.

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

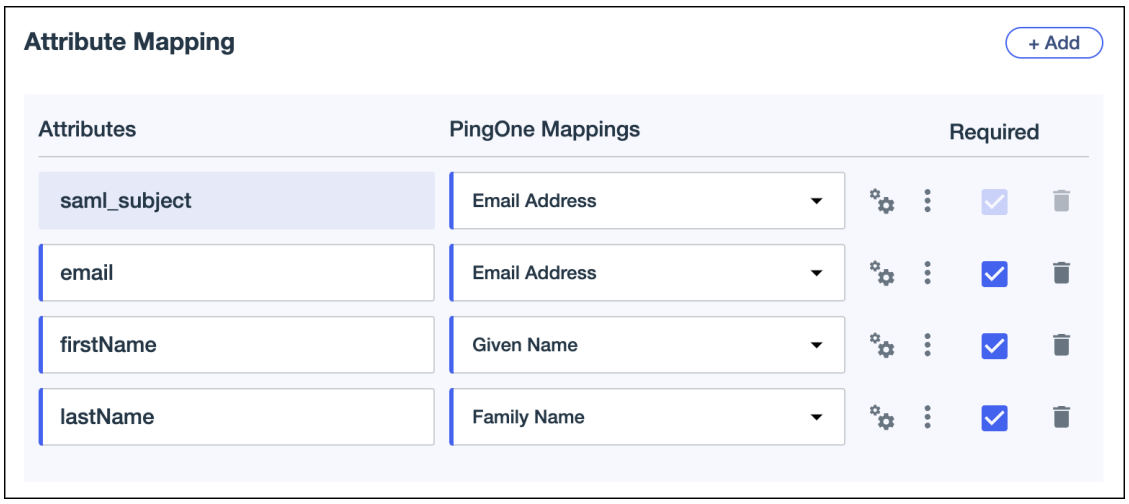
l) 편집(연필) 아이콘을 클릭합니다.

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
email	제품군 이름

Attribute Mapping(속성 매핑) 패널은 다음과 같이 표시됩니다.



o) **Save(**저장**)**를 클릭하여 매핑을 저장합니다.

단계 **3** 보안 클라우드 제어로 돌아가서 **Next(**다음**)**를 클릭합니다. 사용자는 3단계: IdP에서 보안 클라우드로 SAML 메타데이터 제공에 있어야 합니다.

a) **XML file upload(XML** 파일 업로드**)** 옵션을 선택합니다.
b) Ping에서 이전에 다운로드한 SAML 메타데이터 파일을 업로드합니다.
c) **Next(**다음**)**를 클릭하여 테스트 페이지로 이동합니다.

다음에 수행할 작업

다음으로 4단계: SAML 통합 테스트 및 5단계: 통합 활성화의 지침에 따라 통합을 테스트하고 활성화합니다.