ID 제공자 통합 가이드

ID 제공자를 SAML(Security Assertion Markup Language)을 사용하는 Security Cloud Sign On과(와) 통합하여 엔터프라이즈 사용자에게 SSO를 제공할 수 있습니다. 기본적으로 Security Cloud Sign On은 모든 사용자를 추가 비용 없이 Duo Multi-Factor Authentication(MFA)에 등록합니다. 조직에서 이미 IdP와 MFA를 통합한 경우 통합 중에 Duo 기반 MFA를 선택적으로 비활성화할 수 있습니다.

특정 ID 서비스 제공자와 통합하는 방법은 다음 설명서를 참조하십시오.

- Auth0
- Azure AD
- Duo
- Google ID
- Okta
- Ping

참고 ID 제공자가 통합되면 도메인의 사용자는 예를 들어 Cisco 또는 Microsoft 소셜 로그인이 아닌 통합 ID 제공자를 통해 인증해야 합니다.

사전 요구 사항

ID 제공자를 Security Cloud Sign On와 통합하려면 다음이 필요합니다.

- 확인된 이메일 도메인
- ID 제공자의 관리 포털에서 SAML 애플리케이션을 생성하고 구성하는 기능

SAML 응답 요구 사항

보안 클라우드 로그인의 SAML 인증 요청에 대한 응답으로 ID 제공자가 SAML 응답을 전송합니다. 사용자가 정상적으로 인증되면 응답에는 `NameID` 속성 및 기타 사용자 속성을 포함하는 SAML 어설션이 포함됩니다. SAML 응답은 아래에 설명된 대로 특정 기준을 충족해야 합니다.

SHA-256 서명 응답

ID 제공자의 응답에 있는 SAML 어설션에는 다음 속성 이름이 포함되어야 합니다. 이러한 이름은 IdP 사용자 프로파일의 해당 속성에 매핑되어야 합니다. IdP 사용자 프로파일 속성 이름은 벤더에 따라 다릅니다.

SAML 어설션 속성

ID 제공자의 응답에 있는 SAML 어설션에는 다음 속성 이름이 포함되어야 합니다. 이러한 이름은 IdP 사용자 프로파일의 해당 속성에 매핑되어야 합니다. IdP 사용자 프로파일 속성 이름은 벤더에 따라 다릅니다.

SAML 어설션 속성 이름	**ID** 제공자 사용자 속성
firstName	사용자의 이름입니다.
lastName	사용자의 성입니다.
email	사용자 이메일입니다. 이 값은 SAML 응답의 **<NameID>** 요소 값과 일치해야 합니다(아래 참조).

<NameID> 요소 형식

SAML 응답의 `<NameID>` 요소의 값은 유효한 이메일 주소여야 하며 어설션의 `email` 속성 값과 일치해야 합니다. `<NameID>` 요소의 형식 속성은 다음 중 하나로 설정해야 합니다.

- `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
- `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`

SAML 어설션 예시

다음 XML은 ID 공급자가 보안 클라우드 로그인 ACL URL에 대한 SAML 응답의 예입니다. **jsmith@example.com**은 `<NameID>` 요소 및 `email` SAML 응답 속성에 따라 달라집니다.

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion ID="id95383894959750298492624 25" IssueInstant="2023-08-02T01:13:04.861Z"
Version="2.0"
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
    <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"/>
    <saml2:Subject>
        <saml2:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">jsmith@example.com</saml2:NameID>

        <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml2:SubjectConfirmationData NotOnOrAfter="2023-08-02T01:18:05.160Z"
Recipient="https://sso.security.cisco.com/sso/saml2/0oa1rs8y79aeweVg80h8"/>
        </saml2:SubjectConfirmation>
    </saml2:Subject>
    <saml2:Conditions NotBefore="2023-08-02T01:08:05.160Z"
NotOnOrAfter="2023-08-02T01:18:05.160Z">
        <saml2:AudienceRestriction>

<saml2:Audience>https://www.okta.com/saml2/service-provider/12345678890</saml2:Audience>
        </saml2:AudienceRestriction>
    </saml2:Conditions>
    <saml2:AuthnStatement AuthnInstant="2023-08-02T01:13:04.861Z">
        <saml2:AuthnContext>

<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClassRef>

        </saml2:AuthnContext>
    </saml2:AuthnStatement>
    <saml2:AttributeStatement>
        <saml2:Attribute Name="firstName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
            <saml2:AttributeValue
                xmlns:xs="http://www.w3.org/2001/XMLSchema"
              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">Joe

            </saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute Name="lastName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
            <saml2:AttributeValue
                xmlns:xs="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Smith
            </saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
            <saml2:AttributeValue
                xmlns:xs="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">jsmith@example.com
            </saml2:AttributeValue>
        </saml2:Attribute>
    </saml2:AttributeStatement>
</saml2:Assertion>
```

1단계: 초기 설정

시작하기 전에

시작하려면 Secure 클라우드 엔터프라이즈의 이름을 제공하고, 사용자를 Duo Multi-Factor Authentication에 무료로 등록할지 아니면 자체 MFA 솔루션을 사용할지 결정해야 합니다.

모든 통합에서 Cisco Security 제품 내의 민감한 데이터를 보호하기 위해 세션 시간 제한이 2시간을 넘지 않는 MFA를 구현할 것을 강력하게 권장합니다.

단계 **1** 보안 클라우드 제어에 로그인합니다.

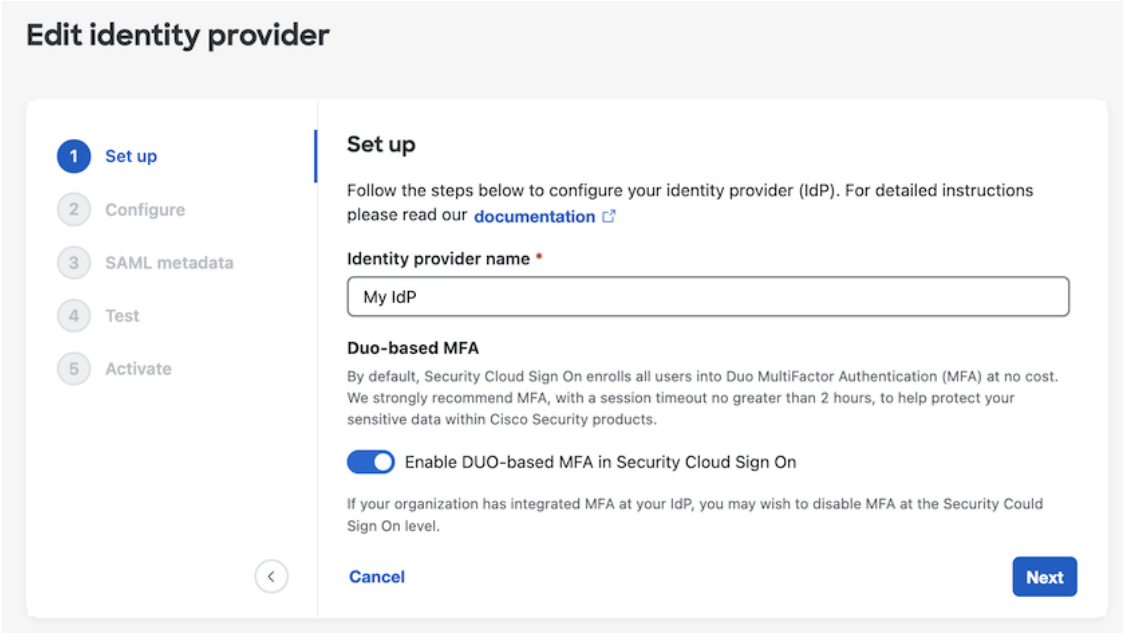
단계 **2** 왼쪽 탐색 메뉴에서 **Identity Providers(ID** 제공자**)**를 선택합니다.

단계 **3** **+Add Identity Provider(IdP** 제공자 추가**)**를 클릭합니다.

참고 아직 도메인을 클레임하지 않은 경우, **+ Add Domain(**도메인 추가**)** 버튼이 대신 표시됩니다. 도메인 클레임을 시작하려면 이 버튼을 클릭합니다.

단계 **4** **Set up(**설정**)** 화면에서 ID 제공자의 이름을 입력합니다.

단계 **5** 원하는 경우 클레임된 도메인의 사용자에 대해 Duo MFA를 옵트아웃합니다.



단계 **6** **Next(**다음**)**를 클릭하여 **Configure(**구성**)** 화면으로 이동합니다.

2단계: ID 제공자에 보안 클라우드 SAML 메타데이터 제공

이 단계에서는 보안 클라우드 제어에서 제공한 SAML 메타데이터 및 서명 인증서를 사용하여 ID 제공자의 SAML 애플리케이션을 구성합니다. 여기에는 다음이 포함됩니다.

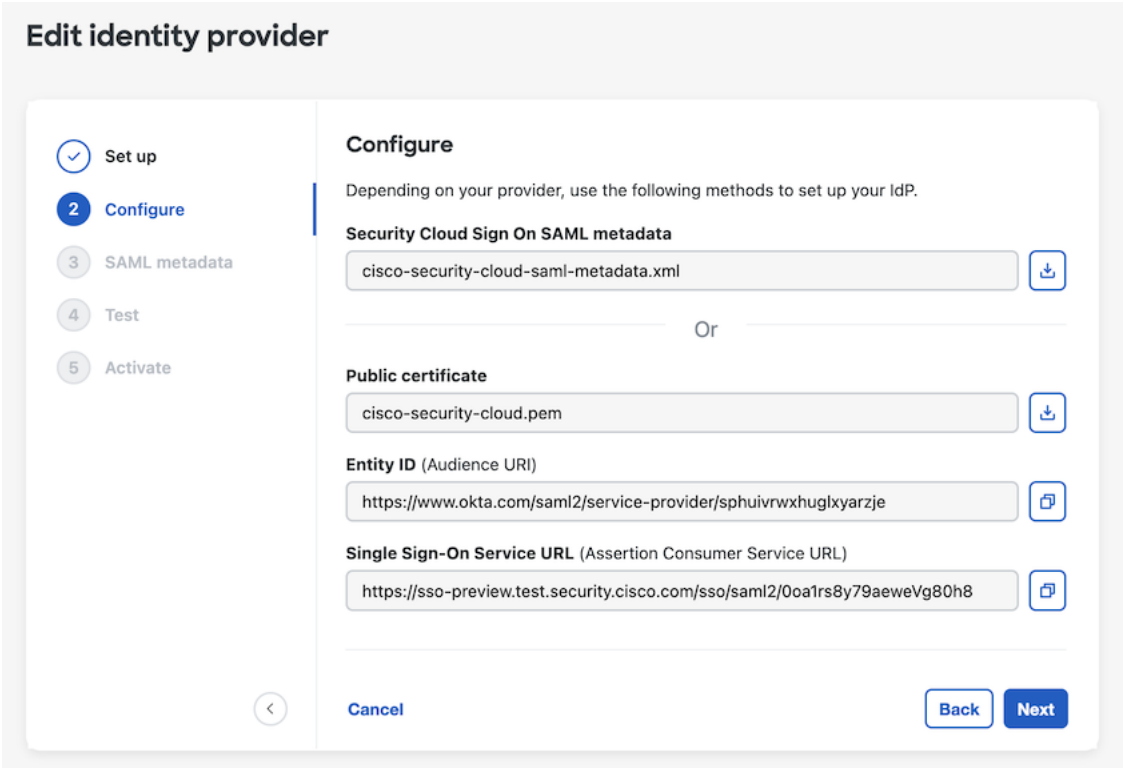
- **SSO(Single Sign-On)** 서비스 **URL** – ACS(Assertion Consumer Service) URL이라고도 하는 이 URL은 ID 제공자가 사용자를 인증한 후 SAML 응답을 전송하는 위치입니다.
- **Entity ID(**엔터티 **ID)**- 대상 URI라고도 하며 ID 제공자에게 Security Cloud Sign On를 고유하게 식별합니다.
- **Signing certificate(**서명 인증서**)** – 인증 요청에서 Security Cloud Sign On가 전송한 서명을 확인하기 위해 ID 제공자가 사용하는 X.509 서명 인증서입니다.

보안 클라우드는 ID 제공자(지원되는 경우)에 업로드할 수 있는 단일 SAML 메타데이터 파일로 이 정보를 제공하며, 개별 값은 복사하여 붙여넣을 수 있습니다. 상업적으로 사용 가능한 여러 ID 서비스 제공자 관련 단계는 ID 서비스 제공자 지침의 내용을 참조하십시오.

단계 **1** ID 제공자가 지원하는 경우 **Configure(**구성**)** 페이지에서 SAML 메타데이터 파일을 다운로드합니다. 그렇지 않으면 단일 로그인 서비스 및 엔터티 **ID** 값을 복사하고 공용 인증서를 다운로드합니다.

단계 **2** ID 제공자에서 보안 클라우드 로그인과 통합할 SAML 애플리케이션을 엽니다.

단계 **3** 공급자가 지원하는 경우, SAML 메타데이터 파일을 업로드합니다. 그렇지 않을 경우, 필요한 보안 클라우드 로그인 SAML URI를 복사하여 SAML 애플리케이션의 해당 구성 필드에 붙여넣고 보안 클라우드 로그인 공개 서명 인증서를 업로드합니다.



단계 **4** Security Cloud Sign On XML 메타데이터 파일을 가져오거나 SSO 서비스 URL 및 엔터티 ID 값을 수동으로 입력하고 공개 서명 인증서를 업로드하여 이전 단계에서 얻은 SAML 메타데이터로 SAML 애플리케이션을 구성합니다.

단계 **5** 보안 클라우드 제어로 돌아가 **Next(**다음**)**를 클릭합니다.

다음에 수행할 작업

다음으로 ID 제공자의 SAML 애플리케이션에 해당하는 메타데이터를 보안 클라우드 제어에 제공합니다.

3단계: IdP에서 보안 클라우드로 SAML 메타데이터 제공

Security Cloud Control(보안 클라우드 제어)에서 SAML 메타데이터를 사용하여 2단계: ID 제공자에 보안 클라우드 SAML 메타데이터 제공했다면, 다음 단계는 SAML 애플리케이션의 해당 메타데이터를 Security Cloud Control(보안 클라우드 제어)에 제공하는 것입니다. 상업적으로 사용 가능한 여러 ID 서비스 제공자 관련 단계는 ID 서비스 제공자 지침의 내용을 참조하십시오.

시작하기 전에

이 단계를 완료하려면 ID 공급자의 SAML 애플리케이션에 대한 다음 메타데이터가 필요합니다.

- SSO(Single Sign-On) 서비스 URL

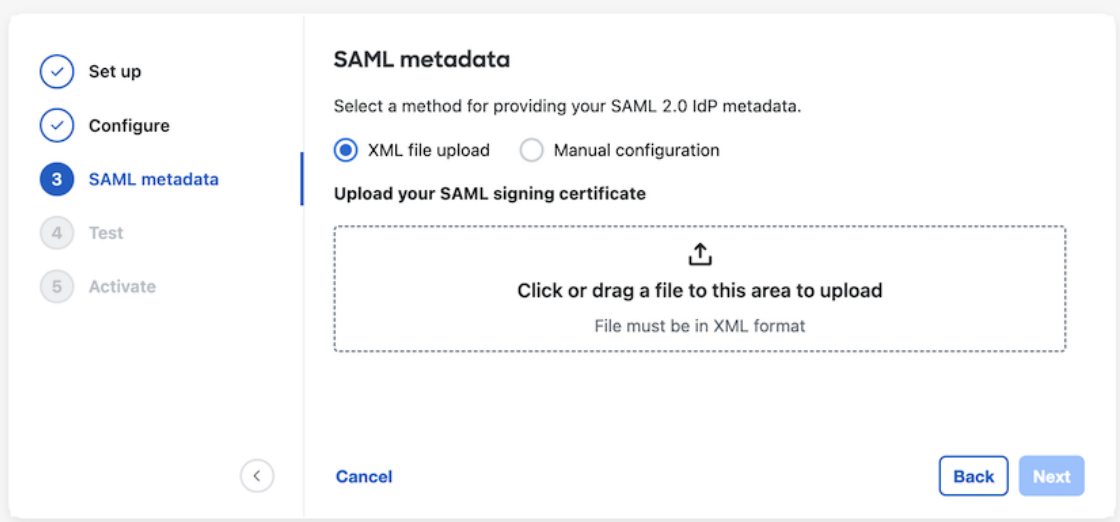
- 엔터티 ID(대상 URI)
- PEM 형식의 서명 인증서

ID 제공자 방식에 따라 모든 정보가 포함된 메타데이터 XML 파일을 업로드하거나 개별 SAML URI를 수동으로 입력(복사/붙여넣기)하고 서명 인증서를 업로드할 수 있습니다. 상업적으로 사용 가능한 여러 ID 서비스 제공자 관련 단계는 ID 서비스 제공자 지침의 내용을 참조하십시오.

단계 **1** Security Cloud Control(보안 클라우드 제어)을 사용하여 브라우저 탭을 엽니다.

단계 **2** **SAML** 메타데이터 단계에서 다음 중 하나를 수행합니다.

- ID 제공자의 XML 메타데이터 파일이 있는 경우 **XML file Upload(XML** 파일 업로드**)**를 선택하고 XML 파일을 업로드합니다.
- 그렇지 않으면 **Manual configuration(**수동 구성**)**을 클릭하고 SSO(Single Sign-On) 서비스 URL, 엔터티 ID, ID 제공자가 제공한 공개 서명 인증서를 업로드합니다.



단계 **3** **Next(**다음**)**를 클릭합니다.

다음에 수행할 작업

다음으로 SSO를 Security Cloud Control(보안 클라우드 제어)에서 ID 제공자로 시작하여 4단계: SAML 통합 테스트합니다.

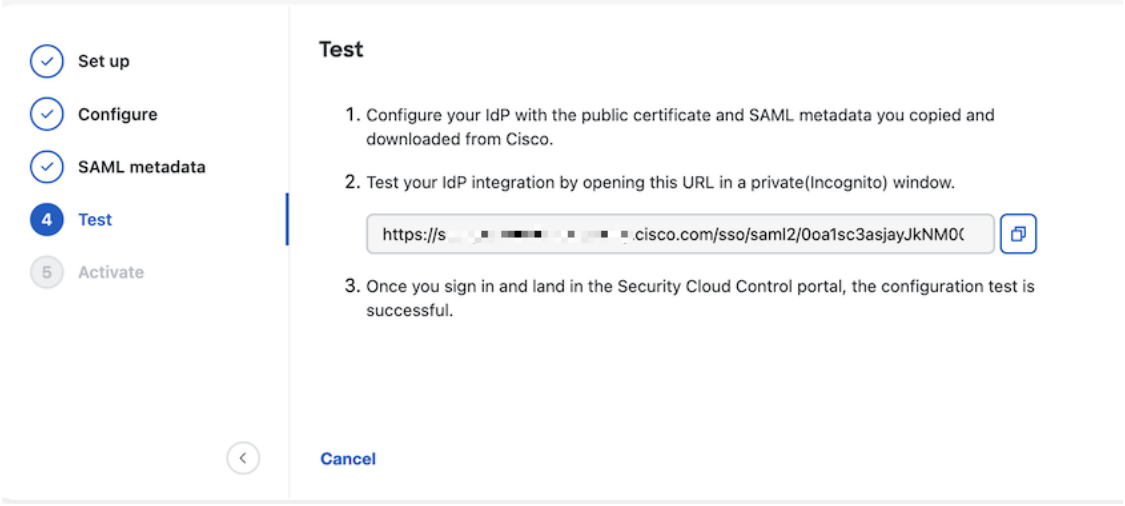
4단계: SAML 통합 테스트

SAML 애플리케이션과 보안 클라우드 로그인 간에 SAML 메타데이터를 교환한 후에 통합을 테스트할 수 있습니다. 보안 클라우드 로그인에서 ID 제공자의 SSO URL로 SAML 요청을 보냅니다. ID 제

공자가 사용자를 정상적으로 인증하면 사용자는 SecureX 애플리케이션 포털로 리디렉션되고 자동으로 로그인됩니다.

중요: 보안 클라우드 제어에서 SAML 통합을 생성하는 데 사용한 계정이 아닌 SSO 사용자 계정으로 테스트해야 합니다. 예를 들어 admin@example.com을 사용하여 통합을 생성한 다음 다른 SSO 사용자(예: jsmith@example.com)로 테스트한 경우입니다.

단계 **1** 보안 클라우드 제어에서 테스트 페이지에 표시된 로그인 URL을 클립보드에 복사하고 비공개(시크릿) 브라우저 창에서 엽니다.



단계 **2** ID 제공자로 로그인합니다.

IdP를 통해 인증한 후 SecureX 애플리케이션 포털에 로그인한 경우 테스트가 성공한 것입니다. 오류가 표시되는 경우 SAML 오류 문제 해결, 9 페이지의 내용을 참조하십시오.

Next(다음**)**를 클릭하여 활성화 단계로 진행합니다.

5단계: 통합 활성화

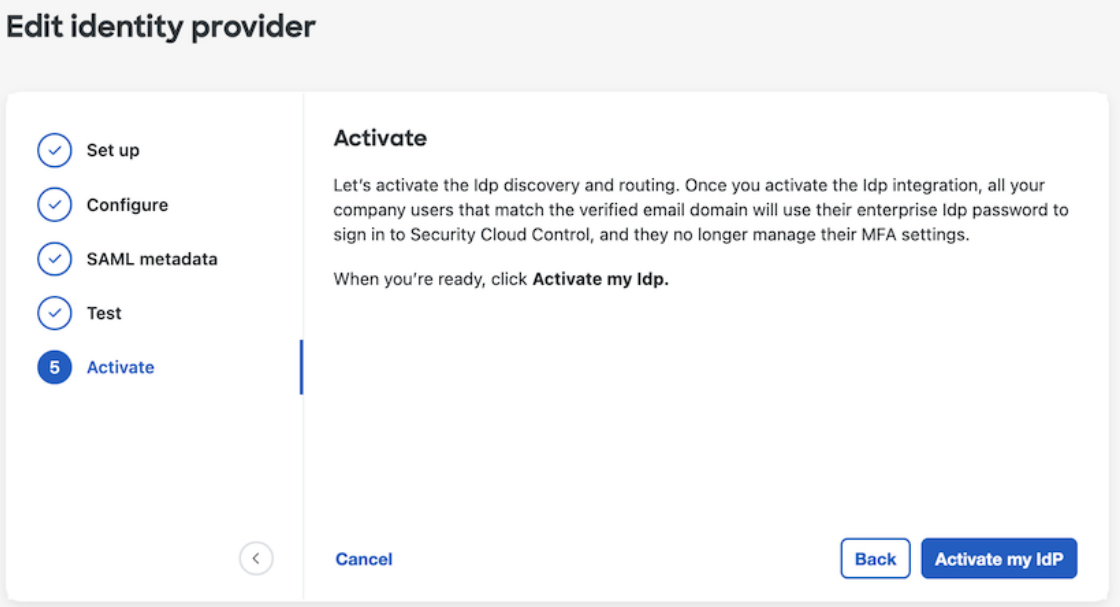
4단계: SAML 통합 테스트 후에는 활성화할 수 있습니다. 통합을 활성화하면 다음과 같은 효과가 있습니다.

- 확인된 도메인의 사용자는 반드시 통합 ID 제공자를 사용하여 인증해야 합니다. 사용자가 Cisco 또는 Microsoft 소셜 로그인 옵션을 사용하여 로그인하려고 하면 400 오류가 발생합니다.
- 클레임된 도메인과 일치하는 이메일 도메인으로 Security Cloud Sign On에 로그인하는 사용자는 인증을 위해 ID 제공자로 리디렉션됩니다.
- Duo MFA를 선택한 경우 클레임된 도메인의 사용자는 더 이상 MFA 설정을 관리하지 않습니다.

주의 통합을 활성화하기 전에 4단계: SAML 통합 테스트해야 합니다.

통합을 활성화하면 다음과 같은 효과가 있습니다.

단계 1 Activate(활성화) 단계에서 **Activate my IdP(내 IdP 활성화)**를 클릭합니다.



단계 2 대화 상자에서 **Activate(활성화)**를 클릭하여 작업을 확인합니다.

SAML 오류 문제 해결

4단계: SAML 통합 테스트할 때 HTTP 400 오류가 발생하는 경우 다음 문제 해결 단계를 시도해 보십시오.

사용자의 로그인 이메일 도메인이 클레임된 도메인과 일치하는지 확인합니다.

테스트에 사용하는 사용자 어카운트의 이메일 도메인이 클레임한 도메인과 일치하는지 확인합니다.
예를 들어 최상위 도메인(예: `example.com`)을 클레임한 경우 사용자는 `<username>@signon.example.com`이 아닌 `<username>@example.com`으로 로그인해야 합니다.

사용자가 **ID** 제공자를 통해 로그인하는지 확인합니다.

사용자는 통합 ID 제공자를 통해 인증해야 합니다. 사용자가 Cisco 또는 Microsoft 소셜 로그인 옵션을 사용하여 로그인하거나 Okta를 통해 직접 로그인을 시도할 경우 HTTP 400 오류가 반환됩니다.

SAML 응답의 **<NameID>** 요소가 이메일 주소인지 확인합니다**.**

SAML 응답에 포함된 `<NameId>` 요소의 값은 이메일 주소여야 합니다. 이메일 주소는 사용자의 SAML 속성에 지정된 이메일과 일치해야 합니다. 자세한 내용은 SAML 응답 요구 사항, 2 페이지를 참조하십시오.

SAML 응답에 올바른 속성 클레임이 포함되어 있는지 확인합니다**.**

IdP가 Security Cloud Sign On에 대한 SAML 응답에 필수 사용자 속성인 **firstName**, **lastName**, **email**이 포함되어 있습니다. 자세한 내용은 SAML 응답 요구 사항, 2 페이지를 참조하십시오.

IdP의 **SAML** 응답이 **SHA-256**으로 서명되었는지 확인합니다**.**

ID 공급자의 SAML 응답은 SHA-256 서명 알고리즘으로 서명해야 합니다. Security Cloud Sign On은(는) 서명되지 않았거나 다른 알고리즘으로 서명된 어설션은 거부합니다.