



Cisco Security Cloud Sign On ID 제공자 통합 가이드

초판: 2020년 9월 1일

최종 변경: 2022년 4월 19일

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



1 장

개요



중요 **Enterprise Manager**가 사용이 중지되었습니다. 이제 [보안 클라우드 제어](#) 를 사용하여 ID 공급자 통합을 관리할 수 있습니다. 자세한 내용은 [ID 공급자 통합 가이드](#)를 참조하십시오.

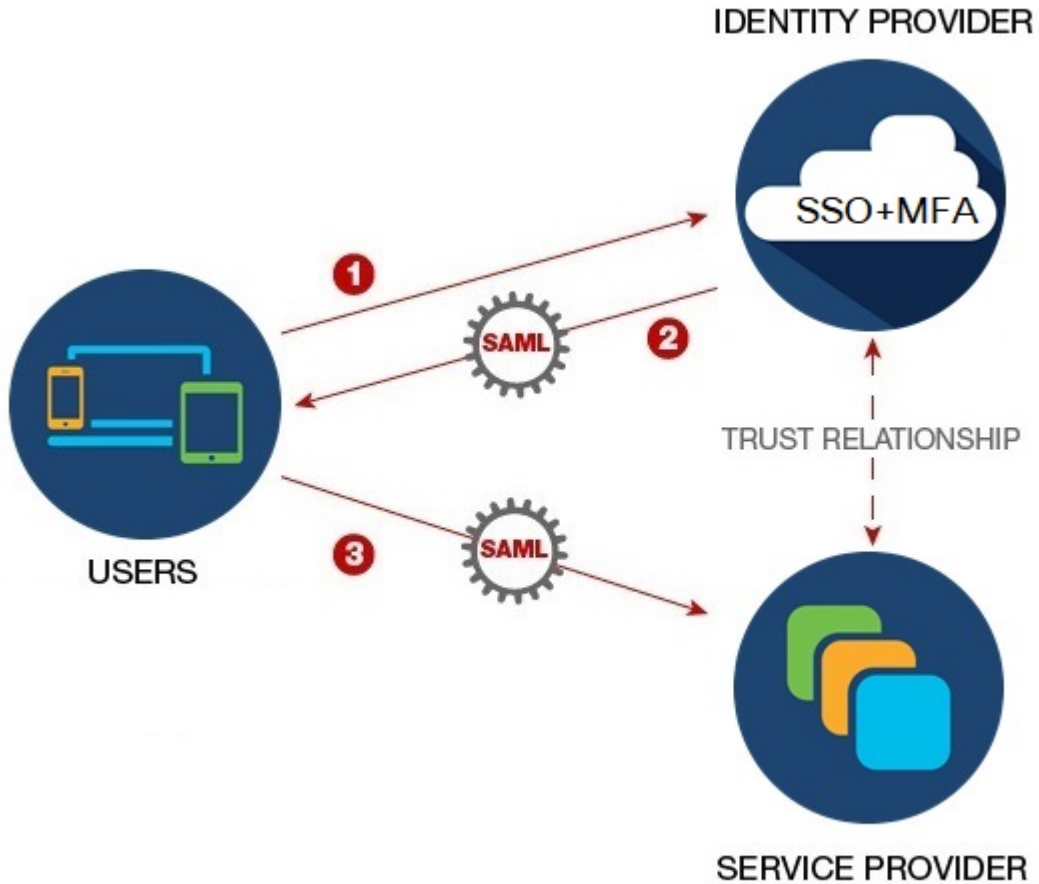
모든 기존 ID 공급자 통합 데이터는 보안 클라우드 컨트롤을 통해 사용할 수 있습니다.

- [개요, 1 페이지](#)
- [다단계 인증 요구 사항, 2 페이지](#)
- [기존 IdP 통합 고객, 3 페이지](#)

개요

SAML(Security Assertion Markup Language)을 사용하여 자체 또는 서드파티 IdP(ID 공급자)를 Cisco Security Cloud Sign On과(와) 통합할 수 있습니다. SAML은 ID 공급자(IdP)와 SP(통신 사업자) 간에 인증 및 권한 데이터를 교환하기 위한 XML 기반의 개방형 표준입니다. 이 경우 통신 사업자는 Security Cloud Sign On입니다. 통합되면 사용자는 SSO(Single Sign On) 자격 증명을 사용하여 Security Cloud

Sign On에 로그인할 수 있습니다



다단계 인증 요구 사항

Security Cloud Sign On에는 모든 계정에 대해 Duo 다단계 인증이 필요합니다. SAML(Security Assertion Markup Language)을 사용하여 ID 공급자 통합과 을 통합하는 고객은 Duo MFA를 옵트아웃할 수 있습니다.

Duo MFA에 등록된 사용자는 선택적으로 Google Authenticator에 등록할 수 있습니다. Google Authenticator에 등록된 후에는 후속 로그인에서는 Duo MFA 챌린지가 아닌 Google Authenticator 챌린지만 표시합니다.

Cisco 고객 ID 또는 Microsoft를 통해 페더레이션된 로그인을 사용하는 경우([Security Cloud Sign On](#) 페이지의 **Other login options**(기타 로그인 옵션) 아래) 동일한 정책이 적용됩니다.

기존 IdP 통합 고객

이 가이드에서 설명하는 [엔터프라이즈 설정 마법사](#)로 생성되지 않은 IdP 통합이 Security Cloud Sign On인 경우, 이 도구를 사용하여 기존 구성을 업데이트할 수 없습니다. 통합에 대해 다음 설정을 수정해야 하는 경우 [Cisco TAC를 사용하여 케이스를 열어야](#) 합니다.

- SAML SSO(Single Sign On) URL 또는 엔터티 ID URI
- X.509 서명 인증서
- MFA(다단계 인증) 설정



2 장

ID 제공자에 대한 SAML 요구 사항



중요 **Enterprise Manager**가 사용이 중지되었습니다. 이제 [보안 클라우드 제어](#) 를 사용하여 ID 공급자 통합을 관리할 수 있습니다. 자세한 내용은 [ID 공급자 통합 가이드](#)를 참조하십시오.

모든 기존 ID 공급자 통합 데이터는 보안 클라우드 컨트롤을 통해 사용할 수 있습니다.

- [개요, 5 페이지](#)
- [SAML 응답 요구 사항, 5 페이지](#)
- [SAML 메타데이터 요구 사항, 6 페이지](#)

개요

IdP에서 Security Cloud Sign On(으)로 보내는 SAML 응답은 [SAML 응답 요구 사항, 5 페이지](#)에 설명된 대로 몇 가지 규칙을 준수해야 합니다.

또한 IdP에서 [SAML 메타데이터 요구 사항](#)을 가져와야 합니다.

SAML 응답 요구 사항

SHA-256으로 서명된 SAML 응답

ID 공급자가 반환한 SAML 응답은 SHA-256 서명 알고리즘으로 서명되어야 합니다. Security Cloud Sign On은(는)서명되지 않았거나 다른 알고리즘으로 서명된 응답은 거부합니다.

SAML 응답 속성

IdP가 전송한 SAML 응답의 어설션에는 다음 속성 이름이 포함되어야 하며 IdP의 해당 속성에 매핑되어야 합니다.

SAML 어설션 속성 이름	IdP 사용자 속성
firstName	사용자의 이름입니다.
lastName	사용자의 성입니다.
email	사용자 이메일입니다. 이 값은 SAML 응답의 <NameID> 요소 값과 일치해야 합니다.

예를 들어, 다음 XML 스니펫은 Security Cloud Sign On ACL URL에 대한 SAML 응답에 포함된 <AttributeStatement> 요소의 예입니다.

```
<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">John
    </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">Doe
    </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">jdoe@example.com
    </saml2:AttributeValue>
  </saml2:Attribute>
</saml2:AttributeStatement>
```

NameID 요소

IdP에서 보낸 SAML 응답의 <NameID> 요소에는 유효한 이메일 주소가 값으로 있어야 하며, 이메일은 [SAML 응답 속성, 5 페이지](#)의 **email** 속성 값과 일치해야 합니다.

<NameID>의 **Format** 속성은 **urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified** 또는 **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**로 설정해야 합니다.

아래는 <NameID> 요소의 예입니다.

```
<saml2:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">jdoe@example.com</saml2:NameID>
```

SAML 메타데이터 요구 사항

Security Cloud Sign On과(와) 통합하려면 IdP의 SAML 애플리케이션에 있는 다음 메타데이터가 필요합니다.

- **SSO(Single Sign-On)** 서비스 초기 **URL** - "SSO URL" 또는 "로그인 URL"이라고도 합니다. 이 URL은 Security Cloud Sign On에 대한 IdP 시작 인증을 시작하는 데 사용할 수 있습니다.
- 엔터티 **ID URI** - IdP의 전역 고유 이름입니다. 이를 "발급자"라고도 합니다.
- **X.509** 서명 인증서 - IdP가 SAML 어설션 서명에 사용하는 공개/개인 키 쌍의 공개 키입니다.



3 장

ID 공급자 통합



중요 **Enterprise Manager**가 사용이 중지되었습니다. 이제 [보안 클라우드 제어](#) 를 사용하여 ID 공급자 통합을 관리할 수 있습니다. 자세한 내용은 [ID 공급자 통합 가이드](#)를 참조하십시오.

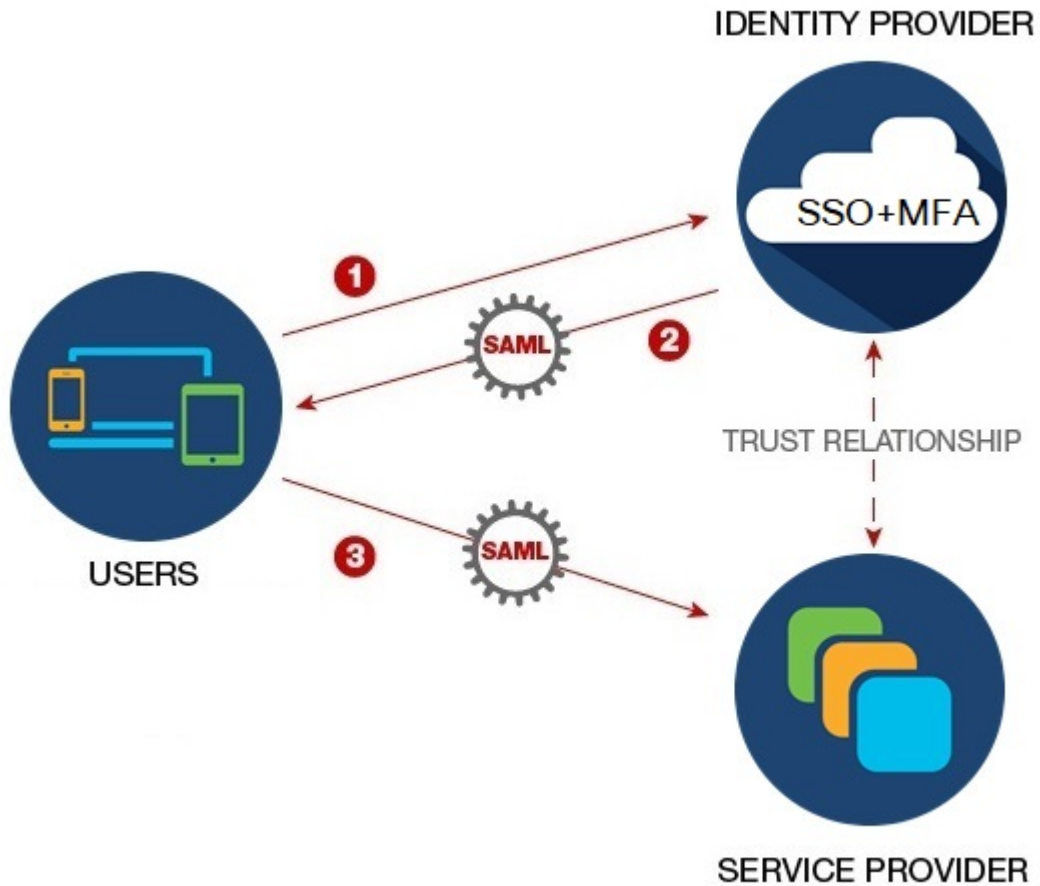
모든 기존 ID 공급자 통합 데이터는 보안 클라우드 컨트롤을 통해 사용할 수 있습니다.

- 개요, 9 페이지
- 엔터프라이즈 설정 마법사, 10 페이지
- 1단계: 엔터프라이즈 생성, 11 페이지
- 2단계: 이메일 도메인 클레임 및 확인, 12 페이지
- 3단계: SAML 메타데이터 교환, 13 페이지
- 4단계: SSO 통합 테스트, 15 페이지
- 5단계: IdP 통합 활성화, 16 페이지

개요

SAML(Security Assertion Markup Language)을 사용하여 자체 또는 서드파티 ID 공급자를 Security Cloud Sign On과(와) 통합할 수 있습니다. SAML은 ID 공급자(IdP)와 SP(통신 사업자), 이 경우 Security Cloud Sign On 간에 인증 및 권한 데이터를 교환하기 위한 XML 기반의 개방형 표준입니다. 통합되면 사용자는 일반적인 SSO(Single Sign On) 자격 증명을 사용하여 Security Cloud Sign On에 로그인할 수 있습

나

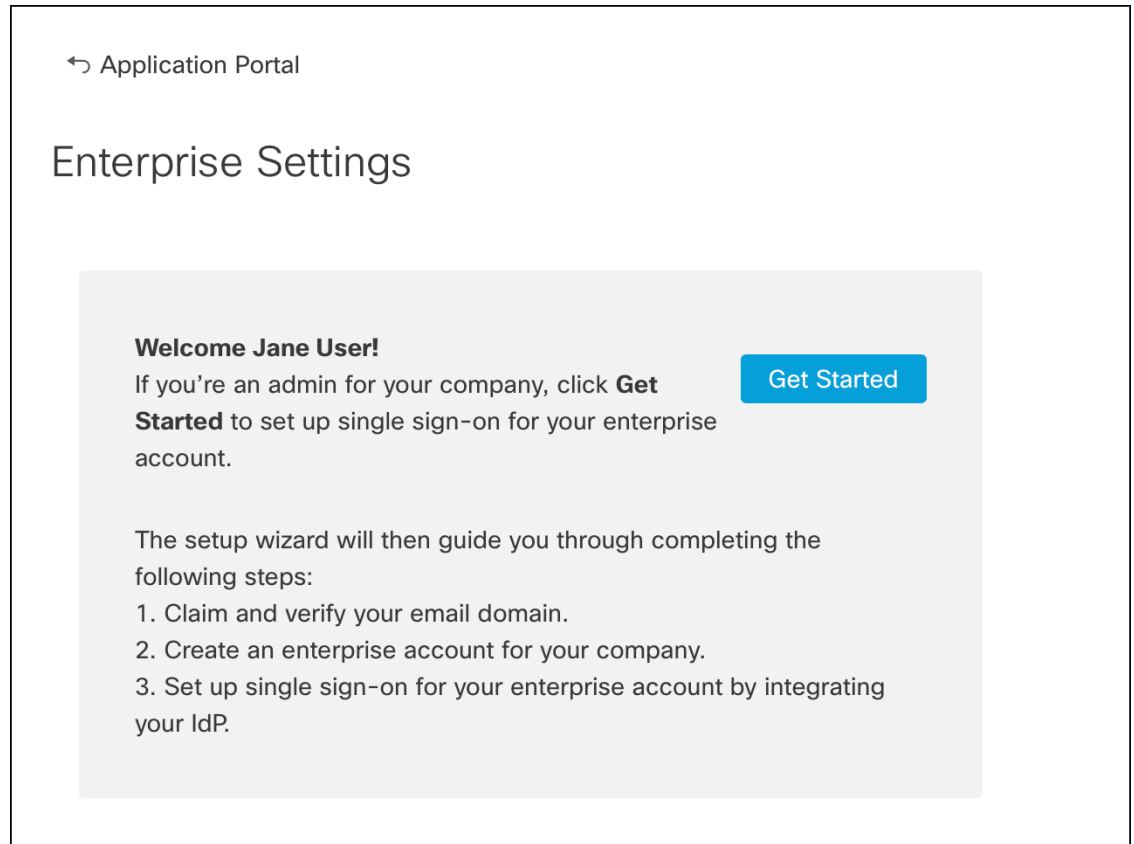


기본적으로 Security Cloud Sign On은(는) 모든 IdP의 사용자를 무료로 Duo 다단계 인증(MFA)에 등록합니다. 조직에서 이미 IdP와 MFA를 통합한 경우 통합 프로세스 중에 Duo 기반 MFA를 선택적으로 비활성화할 수 있습니다.

엔터프라이즈 설정 마법사

엔터프라이즈 설정 마법사가 자체 IdP를 Security Cloud Sign On과(와) 통합하는 여러 단계를 안내합니다. 마법사는 각 단계를 완료할 때마다 진행 상황을 저장하므로, 종료하고 나중에 돌아와서 프로세스를 완료할 수 있습니다.

엔터프라이즈 설정 마법사를 열려면 SecureX 애플리케이션 포털에서 프로필 아이콘을 클릭하고 **Enterprise Settings**(엔터프라이즈 설정)를 선택한 다음 **Get Started**(시작하기)를 클릭합니다.



설정 마법사를 사용하면 하나의 이메일 도메인을 클레임하고 하나의 ID 공급자를 구성할 수 있습니다. 다음과 같은 경우 [Cisco TAC에서 케이스를 열어야](#) 합니다.

- 둘 이상의 ID 공급자를 구성해야 합니다.
- 둘 이상의 이메일 도메인을 클레임해야 합니다.
- **2단계: 이메일 도메인 클레임 및 확인**한 후 조직 이름 또는 이메일 도메인을 변경합니다.



참고 엔터프라이즈 설정 마법사로 생성하지 않은 기존 IdP 통합이 있는 경우 마법사를 사용하여 통합을 수정할 수 없습니다. 자세한 내용은 [기존 IdP 통합 고객, 3 페이지](#)를 참조하십시오.

1단계: 엔터프라이즈 생성

첫 번째 단계는 Security Cloud Sign On에서 명명된 엔터프라이즈를 생성하는 것입니다. 이 엔터프라이즈는 클레임된 도메인 및 ID 공급자 설정과 연결됩니다.

단계 **1** Security Cloud Sign On 계정을 사용하여 [SecureX 애플리케이션 포털](#)에 로그인합니다.

2단계: 이메일 도메인 클레임 및 확인

단계 2 오른쪽 상단에 있는 프로필 아이콘을 클릭하고 **Enterprise Settings**(엔터프라이즈 설정)를 선택합니다.

단계 3 **Get Started**(시작하기)를 클릭합니다.

단계 4 엔터프라이즈 계정의 이름을 입력하고 **Save**(저장)를 클릭합니다.

↩ Enterprise Settings

Enterprise Account Name

1. Enter an account name for the enterprise, company, or organization associated with your domain. ⓘ
2. Click **Save**.

Example company Save

2단계: 이메일 도메인 클레임 및 확인

다음으로 엔터프라이즈의 이메일 도메인을 클레임하고 확인합니다. 이 단계를 완료하려면 도메인 이름 등록 기관 서비스 포털에서 DNS 레코드를 생성해야 합니다. 도메인을 확인했으면 DNS 레코드를 삭제할 수 있습니다.

단계 1 클레임할 도메인을 입력하고 **Submit**(제출)을 클릭합니다.

설정 마법사에 DNS TXT 레코드 이름 및 값이 표시됩니다.

6. Click **Verify**.

Record Name	_cisco-sxso-verification.www.example.com
Type	TXT
Value	69d5...:1d55

Verify

단계 2 도메인 이름 등록 기관 서비스에 로그인하여 지정된 레코드 이름과 값으로 TXT 레코드를 생성합니다.

단계 3 DNS 레코드가 전파될 때까지 기다린 다음 **Verify**(확인)를 클릭합니다.

단계 4 확인에 성공하면 **Integrate IdP**(IdP 통합)를 클릭하여 ID 공급자 통합을 시작합니다.

Success! You've claimed and verified your email domain and enterprise account name. Click Integrate IdP to sync up the single sign-on.

Integrate IdP

3단계: SAML 메타데이터 교환

이 단계에서는 IdP 및 Security Cloud Sign On간에 SAML 메타데이터와 서명 인증서를 교환합니다.

시작하기 전에

이 단계를 완료하려면 ID 공급자에서 생성한 [개요](#)에 대한 다음 정보가 필요합니다.

- **Single Sign-On Service URL** – HTTP POST를 통해 Security Cloud Sign On에서 SAML 인증 요청을 전송하는 URL입니다. URL의 도메인은 이전에 [2단계: 이메일 도메인 클레임 및 확인](#) 도메인과 일치해야 합니다.
- **Entity ID(엔터티 ID)** - 대상 URI라고도 하며 ID 공급자에게 Security Cloud Sign On을(를) 고유하게 식별합니다. IdP의 SAML 메타데이터에서 <EntityDescriptor> 요소를 비활성화합니다. 일부 IdP는 **ID** 공급자 발급자라고도 합니다.
- **SAML 서명 인증서** – IdP가 SAML 어설션에 서명하는 데 사용하는 x.509 서명 인증서입니다.



참고 인증서는 SHA-256 알고리즘으로 서명해야 합니다. 다른 알고리즘으로 서명된 어설션은 HTTP 400 오류로 인해 거부됩니다.

단계 1 **Set Up(설정)** 화면에서 **Identity Provider Name(ID 공급자 이름)** 필드에 IdP의 이름을 입력합니다.

단계 2 IdP의 SAML 통합에서 얻은 **Single Sign-On Service URL** 및 **Entity ID(엔터티 ID)**의 값을 입력합니다.

단계 3 **Add File(파일 추가)**을 클릭하고 이전에 IdP에서 다운로드한 SAML 서명 인증서를 선택합니다.

단계 4 사용자를 Duo MFA에 자동으로 등록하지 않으려면 **Do you wish to keep the Duo-based MFA enabled in Security Cloud Sign On?(Duo 기반 MFA를 계속 사용하시겠습니까?)**에 **No(아니요)**를 선택하면 됩니다.

Integrate Identity Provider

1 Set Up ————— 2 Download ————— 3 Configure

Set Up

Identity Provider (IdP) Name

Single Sign-On Service URL (Assertion Consumer Service URL) ⓘ

Entity ID (Audience URI) ⓘ

SAML Signing Certificate ⓘ
File must be in PEM format

By default, SecureX Sign-On enrolls all users into **Duo MultiFactor Authentication (MFA)** at no cost. We strongly recommend MFA, with a session timeout no greater than 2 hours, to help protect your sensitive data within Cisco Security products.

Do you wish to keep the Duo-based MFA enabled in SecureX Sign-On? Yes No
If your organization has integrated MFA at your IdP, you may wish to disable MFA at the SecureX Sign-On level.

단계 5 **Next(다음)**를 클릭하여 **Download** (다운로드) 화면으로 이동합니다.

단계 6 표시된 **Single Sign-On Service (ACS URL)**(단일 로그인 서비스(ACS URL)) 및 **Entity ID (Audience URL)**(엔터티 ID(대상 URL))를 복사하고 **SAML** 서명 인증서를 다운로드합니다.

Integrate Identity Provider

✓ Set Up ————— 2 Download ————— 3 Configure ————— 4 Activate

Download

Depending on your provider, use the following information to set up your Identity Provider (IdP).

Single Sign-On Service URL (ACS URL)

Entity ID (Audience URI)

SAML Signing Certificate

SecureX Sign-On SAML Metadata

단계 7 **7. Next(다음)**를 클릭하여 **Configure(구성)** 화면으로 이동합니다.

단계 8 IdP 관리 콘솔에서 SAML 애플리케이션 구성 페이지를 열고 다음을 변경합니다.

- ACS URL 및 Entity ID(엔터티 ID)에 할당된 임시 값을 이전 단계에서 얻은 값으로 업데이트합니다.

b) 설정 마법사에서 제공하는 SAML 서명 인증서를 업로드합니다.

참고 일부 IdP(예: 시작하기)는 인증서의 콘텐츠를 단일 라인 JSON 문자열(-----BEGIN CERTIFICATE-----\n...\n...\n- ----END CERTIFICATE-----\n)로 제공해야 합니다.

c) 구성 변경 사항을 SAML 앱 구성에 저장합니다.

다음에 수행할 작업

다음으로, 엔터프라이즈에서 IdP 통합을 테스트합니다.

4단계: SSO 통합 테스트

다음으로 엔터프라이즈 마법사에서 IdP로의 SSO 요청을 시작하여 IdP의 통합을 테스트합니다. SecureX 애플리케이션 대시보드로 돌아가면 테스트가 성공했음을 의미합니다.

- 비공개(시크릿) 창에서 URL을 테스트합니다.
- 로그인에 사용된 이메일 도메인은 이전에 클레임한 **2단계: 이메일 도메인 클레임 및 확인**과 일치해야 합니다.
- 신규 사용자(기존 Security Cloud Sign On 계정이 없는 사용자)와 기존 사용자를 모두 테스트합니다.

단계 1 엔터프라이즈 설정 마법사의 **Configure**(구성) 화면으로 돌아갑니다.

단계 2 2단계의 SSO URL을 클립보드에 복사하고 비공개(시크릿) 브라우저 창에서 엽니다.

Configure

1. Configure your IdP with the public certificate and SAML metadata you copied and downloaded from Cisco.
2. Test your IdP integration by opening this URL in a private (incognito) window.

<https://sso.security.cisco.com/sso/saml2/0oa...>

3. Once you sign in and land in the SecureX application portal, the configuration test is successful.

단계 3 ID 제공자로 로그인합니다.

- 로그인에 사용된 이메일 도메인은 이전에 클레임한 **2단계: 이메일 도메인 클레임 및 확인**과 일치해야 합니다.

- 보안 클라우드 로그인에 처음 등록할 때 사용한 계정이 아닌 계정으로 테스트합니다. 예를 들어 admin@example.com 계정을 사용하여 IdP 통합에 등록하고 생성한 경우 동일한 이메일을 사용하여 통합을 테스트하지 마십시오.

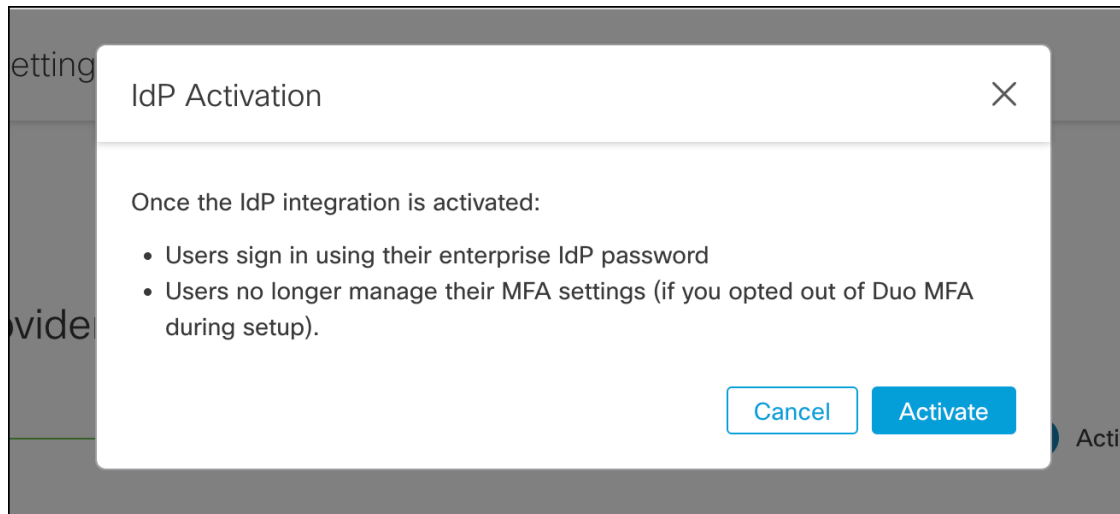
SecureX 애플리케이션 포털이 표시되면 설정 테스트가 성공한 것입니다. SSO 프로세스 중에 오류가 발생하면 [문제 해결, 17 페이지](#)의 내용을 참조하십시오.

단계 4 통합을 테스트한 후에는 **Next**(다음)를 클릭하여 **Activate**(활성화) 페이지로 이동합니다.

5단계: IdP 통합 활성화

4단계: [SSO 통합 테스트](#)하고 조직에서 활성화할 준비가 되면 이를 활성화할 수 있습니다. 활성화되면 사용자는 엔터프라이즈(IdP) 이메일 주소와 암호를 사용하여 로그인합니다. 무료 Duo MFA 등록을 옵트아웃하면 사용자가 더 이상 MFA 설정을 관리하지 않습니다.

IdP 및 Security Cloud Sign On과(와)의 통합을 활성화하려면 **Activate my IdP**(내 IdP 활성화)를 클릭한 다음 확인 대화 상자에서 **Activate**(활성화)를 클릭합니다.





4 장

문제 해결



중요 **Enterprise Manager**가 사용이 중지되었습니다. 이제 **보안 클라우드 제어**를 사용하여 ID 공급자 통합을 관리할 수 있습니다. 자세한 내용은 **ID 공급자 통합 가이드**를 참조하십시오.

모든 기존 ID 공급자 통합 데이터는 보안 클라우드 컨트롤을 통해 사용할 수 있습니다.

- [SSO\(Single Sign-On\)/SAML 오류, 17 페이지](#)
- [엔터프라이즈 마법사 오류, 18 페이지](#)
- [Cisco 보안 제품과의 통합, 18 페이지](#)

SSO(Single Sign-On)/SAML 오류

통합 테스트 시 **HTTP 400** 오류

엔터프라이즈 설정 마법사에서 **4단계: SSO 통합 테스트**할 때 HTTP 400 오류가 발생하는 경우 다음 문제 해결 단계를 시도해 보십시오.

사용자의 로그인 이메일 도메인이 클레임된 도메인과 일치하는지 확인합니다.

테스트에 사용하는 사용자 계정의 이메일 도메인이 **2단계: 이메일 도메인 클레임 및 확인**과 일치하는지 확인합니다.

예를 들어 최상위 도메인(예: example.com)을 클레임한 경우 사용자는

<username>@signon.example.com이 아닌 <username>@example.com으로 로그인해야 합니다.

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 속성, 5 페이지](#)를 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, 5 페이지](#)를 참조하십시오.

IdP의 SAML 응답이 SHA-256으로 서명되었는지 확인합니다.

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

엔터프라이즈 마법사 오류

도메인을 확인하는 동안 오류 발생

2단계: 이메일 도메인 클레임 및 확인할 때 오류가 발생하는 경우 다음 문제 해결 단계를 시도해 보십시오.

잠시 기다렸다가 다시 시도하십시오.

잠시 기다렸다가 **Verify(확인)**를 다시 클릭합니다. DNS 레코드 업데이트가 DNS 서버로 전파되는 데 걸리는 시간은 통신 사업자에 따라 다릅니다.

TXT DNS 레코드 이름 및 값 확인

도메인 등록 기관에서 생성한 TXT DNS 레코드의 이름과 값이 엔터프라이즈 설정 마법사에 표시된 것과 일치하는지 확인합니다.

SSO(Single Sign-On) 테스트 오류

4단계: SSO 통합 테스트할 때 오류가 발생하는 경우 SAML 구성 문제 또는 사용자 계정 문제일 가능성이 높습니다. 문제 해결 단계는 **SSO(Single Sign-On)/SAML 오류, 17 페이지**의 내용을 참조하십시오.

Cisco 보안 제품과의 통합

Cisco 보안 제품 로그인 오류

Security Cloud Sign On에는 로그인할 수 있지만 하나 이상의 Cisco 보안 제품에는 로그인할 수 없는 경우 다음을 확인하십시오.

제품이 **Security Cloud Sign On**에 옵트인을 요구하는지 확인합니다.

Cisco Umbrella와 같은 일부 Cisco 보안 제품은 기본적으로 Security Cloud Sign On을(를) 지원하지 않지만 옵트인이 필요한 제품도 있습니다. **지원되는 보안 제품** 목록에는 옵트인이 필요한 Cisco 보안 제품이 나와 있습니다.

Security Cloud Sign On ID가 제품 ID와 일치하는지 확인합니다.

각 사용자의 Security Cloud Sign On ID(이메일)가 제품 ID와 일치해야 합니다. 예를 들어 사용자 이름이 **user@example.com**인 Security Cloud Sign On 계정이 있다고 가정해 보겠습니다. Security Cloud Sign On 계정을 사용하여 Umbrella로 인증하려면 동일한 이메일을 사용하는 기존 Umbrella 계정이 있어야 합니다.



I 부

ID 공급자 통합 가이드

- [Auth0, 21 페이지](#)
- [Azure AD, 27 페이지](#)
- [Duo, 31 페이지](#)
- [Google, 35 페이지](#)
- [Okta, 39 페이지](#)
- [Ping Identity, 43 페이지](#)
- [일반 IdP 지침, 49 페이지](#)



5 장

Auth0



중요 **Enterprise Manager**가 사용이 중지되었습니다. 이제 **보안 클라우드 제어**를 사용하여 ID 공급자 통합을 관리할 수 있습니다. 자세한 내용은 **ID 공급자 통합 가이드**를 참조하십시오.

모든 기존 ID 공급자 통합 데이터는 보안 클라우드 컨트롤을 통해 사용할 수 있습니다.

- [개요, 21 페이지](#)
- [시작하기, 21 페이지](#)

개요

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

시작하기

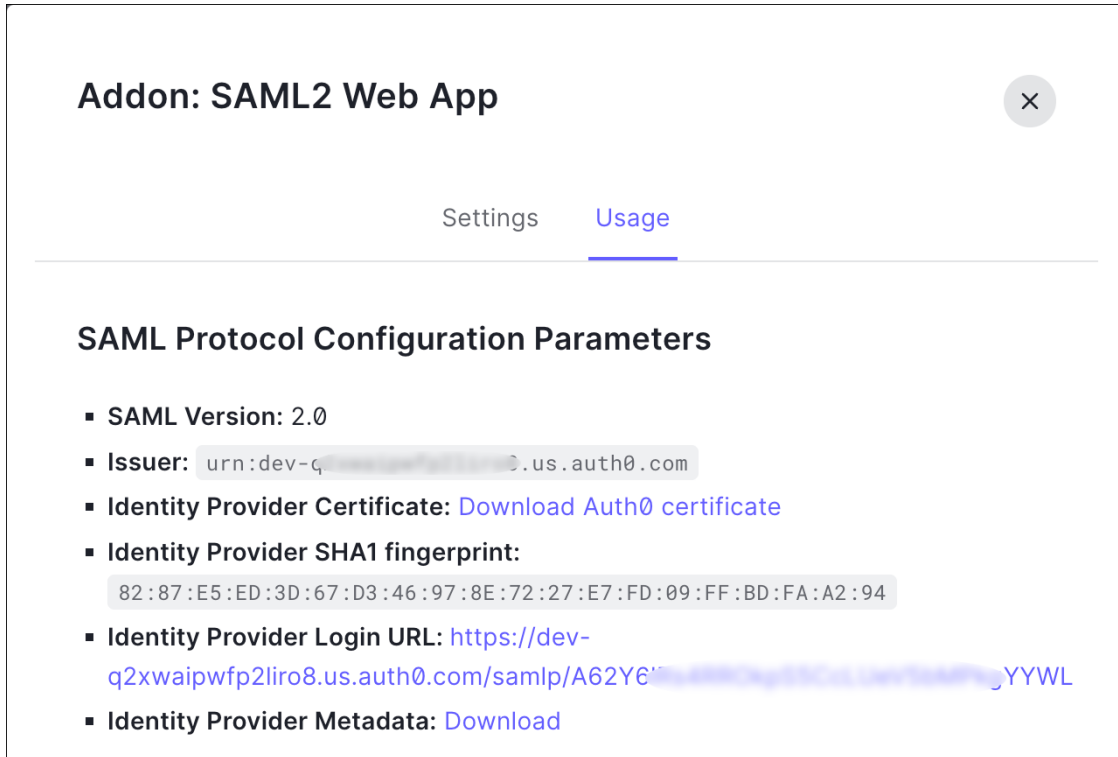
시작하기 전에

- 관리자 권한으로 Auth0 관리 콘솔에 로그인할 수 있어야 합니다.
- **1단계: 엔터프라이즈 생성, 11 페이지** 및 **2단계: 이메일 도메인 클레임 및 확인, 12 페이지**를 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 열립니다.



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 사용자에게 대해 무료 Duo 기반 MFA 서비스를 옵트아웃할 수 있습니다.

Integrate Identity Provider

1 Set Up — 2 Download — 3 Configure — 4 Activate

Set Up

Identity Provider (IdP) Name

Single Sign-On Service URL ⓘ

Entity ID (Audience URI) ⓘ

SAML Signing Certificate ⓘ
File must be in PEM format

By default, SecureX Sign-On enrolls all users into **Duo MultiFactor Authentication (MFA) at no cost**. We strongly recommend MFA, with a session timeout no greater than 2 hours, to help protect your sensitive data within Cisco Security products.

Do you wish to keep the Duo-based MFA enabled in SecureX Sign-On? Yes No

- 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.

✓ Set Up — 2 Download — 3 Configure — 4 Activate

Download

Depending on your provider, use the following information to set up your Identity Provider (IdP).

Single Sign-On Service URL (ACS URL)

Entity ID (Audience URI)

SAML Signing Certificate

SecureX Sign-On SAML Metadata

- 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)**(엔티티 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"
}
```

Addon: SAML2 Web App ✕

Settings
Usage

Application Callback URL

https://sso-preview.test.security.cisco.com/sso/saml2/0oa[redacted]0h8

SAML Token will be POSTed to this URL.

Settings

```

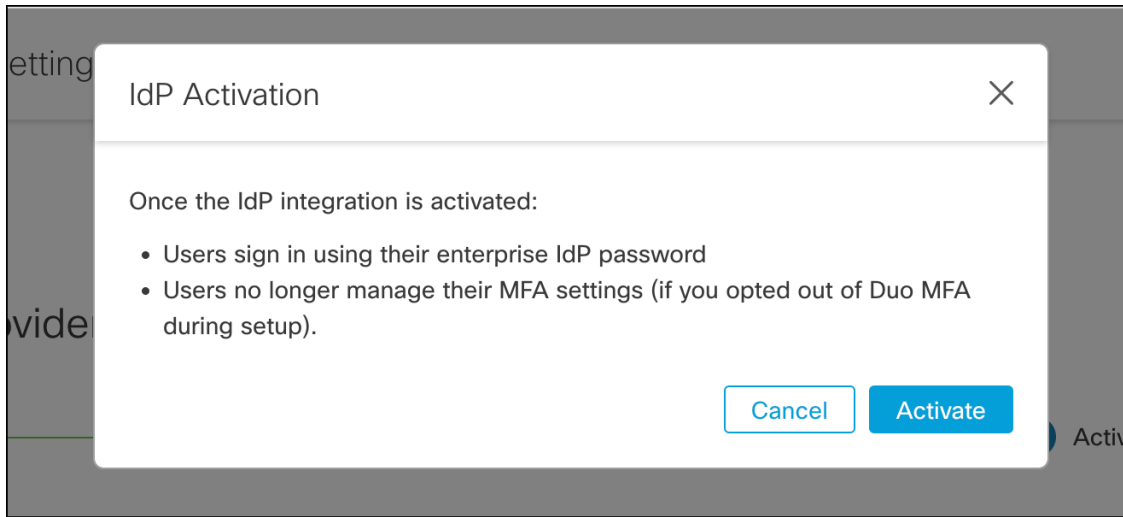
2 {
3   "audience": "https://www.okta.com/saml2/service-provider/
4   "signingCert": "-----BEGIN CERTIFICATE-----\nMII...fjc\n
5   "mappings": {
6     "email": "email",
7     "given_name": "firstName",
8     "family_name": "lastName"
9   },
10  "nameIdentifierFormat": "urn:oasis:names:tc:SAML:1.1:name
11  "nameIdentifierProbes": [
12    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/
13  ],
14  "binding": "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POS
15  }
```

Debug

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) **2단계: 이메일 도메인 클레임 및 확인**과 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.





6 장

Azure AD



중요 **Enterprise Manager**가 사용이 중지되었습니다. 이제 **보안 클라우드 제어**를 사용하여 ID 공급자 통합을 관리할 수 있습니다. 자세한 내용은 **ID 공급자 통합 가이드**를 참조하십시오.

모든 기존 ID 공급자 통합 데이터는 보안 클라우드 컨트롤을 통해 사용할 수 있습니다.

- [개요, 27 페이지](#)
- [시작하기, 27 페이지](#)

개요

이 가이드에서는 Azure AD SAML 애플리케이션을 생성하고 Security Cloud Sign On과(와) 통합하는 방법을 설명합니다.



- 참고**
- Azure AD 사용자의 UPN(사용자 계정 이름)은 해당 사용자의 이메일 주소와 항상 같지는 않습니다.
 - <NameID> 요소 및 SAML 응답의 email 사용자 속성은 사용자의 이메일 주소를 포함해야 합니다. 자세한 내용은 [SAML 응답 요구 사항, 5 페이지](#)를 참조하십시오.
 - 지정된 이메일 주소는 기존 제품 액세스 제어에 사용된 주소와 일치해야 합니다. 일치하지 않으면 제품 액세스 제어를 업데이트해야 합니다.

시작하기

시작하기 전에

- 관리자 권한으로 [Azure 포털](#)에 로그인할 수 있어야 합니다.

- 엔터프라이즈 설정 마법사의 **1단계: 엔터프라이즈 생성, 11 페이지** 및 **2단계: 이메일 도메인 클레임 및 확인, 12 페이지**를 완료해야 합니다.

단계 1 <https://portal.azure.com>에 로그인합니다.

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

- Azure Active Directory**를 클릭합니다.
- 왼쪽 사이드바에서 **Enterprise Applications**(엔터프라이즈 애플리케이션)을 클릭합니다.
- + New Application**(+ 새 애플리케이션)을 클릭하고 **Azure AD SAML** 툴킷을 검색합니다.
- Azure AD SAML Toolkit**(Azure AD SAML 툴킷)을 클릭합니다.
- Name**(이름) 필드에 **SecureX Sign On** 또는 다른 값을 입력하고 **Create**(생성)를 클릭합니다.
- Overview(개요) 페이지의 왼쪽 사이드바에서 **Manage**(관리) 아래 **Single Sign On**(단일 인증)을 클릭합니다.
- SSO(Single Sign-On, 단일 인증) 방법 선택 시 **SAML**을 선택합니다.
- Basic SAML Configuration**(기본 SAML 구성) 패널에서 **Edit**(편집)를 클릭합니다.
 - **Identifier (Entity ID)**(식별자(엔터티 ID))에서 **Add Identifier**(식별자 추가)를 클릭하고 임시 값 **https://example.com** 또는 기타 유효한 URL을 입력합니다. 나중에 이 임시 값을 대체합니다.
 - **Reply URL (Assertion Consumer Service URL)**(회신 URL(어설션 소비자 서비스 URL))에서 **Add reply URL**(회신 URL 추가)를 클릭하고 임시 값 **https://example.com** 또는 기타 유효한 URL을 입력합니다. 나중에 이 임시 값을 대체합니다.
 - **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.
- 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)가 `user.primaryauthoritativeemail`을 사용하도록 설정합니다.

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

이 섹션에서는 `user.userprincipalname`의 값이 유효한 이메일 주소를 나타내는 것으로 가정합니다. 그렇지 않은 경우 **email** 클레임의 **Source attribute**(소스 속성)이 `user.primaryauthoritativeemail`을 사용하도록 설정합니다.

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

각 클레임에 대한 **Namespace**(네임스페이스) 필드의 선택을 취소해야 합니다.

다.

- l) **SAML Certificates**(SAML 인증서) 패널에서 인증서(Base64) 인증서에 대해 **Download**(다운로드)를 클릭합니다.
- m) **Set up Single Sign-On with SAML**(SAML을 이용한 SSO 설정) 섹션에서 로그인 URL 및 Azure AD 식별자의 값을 복사하여 이 절차의 뒷부분에서 사용할 수 있습니다.

단계 2 새 브라우저 탭에서 Enterprise 설정 마법사를 엽니다. 현재 **Integrate Identity Provider**(ID 공급자 통합) > **Set Up**(설정) 화면(3단계: **SAML 메타데이터 교환**, 13 페이지)에 있어야 합니다.

- a) **Identity Provider (IdP) Name**(ID 공급자(IdP) 이름) 필드에 **Azure SSO** 또는 통합에 대한 다른 이름을 입력합니다.
- b) Azure에서 복사한 **Login URL**(로그인 URL) 필드의 값을 **Single Sign-On Service URL** 필드에 입력합니다.
- c) **Entity ID (Audience URI)**(엔터티 ID(대상 URI)) 필드에 Azure에서 복사한 **Azure AD** 식별자 값을 입력합니다.
- d) **Add File**(파일 추가)을 클릭하고 Azure 포털에서 다운로드한 SAML 서명 인증서를 업로드합니다.
- e) 필요한 경우 사용자에 대해 무료 Duo MFA를 옵트아웃합니다.
- f) **Download**(다운로드) 화면에서 **Next**(다음)를 클릭합니다.
- g) 이 절차에서 나중에 사용할 수 있도록 **Single Sign-On Service URL (ACS URL)** 및 **Entity ID (Audience URI)** 필드의 값을 복사합니다.
- h) **Next**(다음)를 클릭합니다.

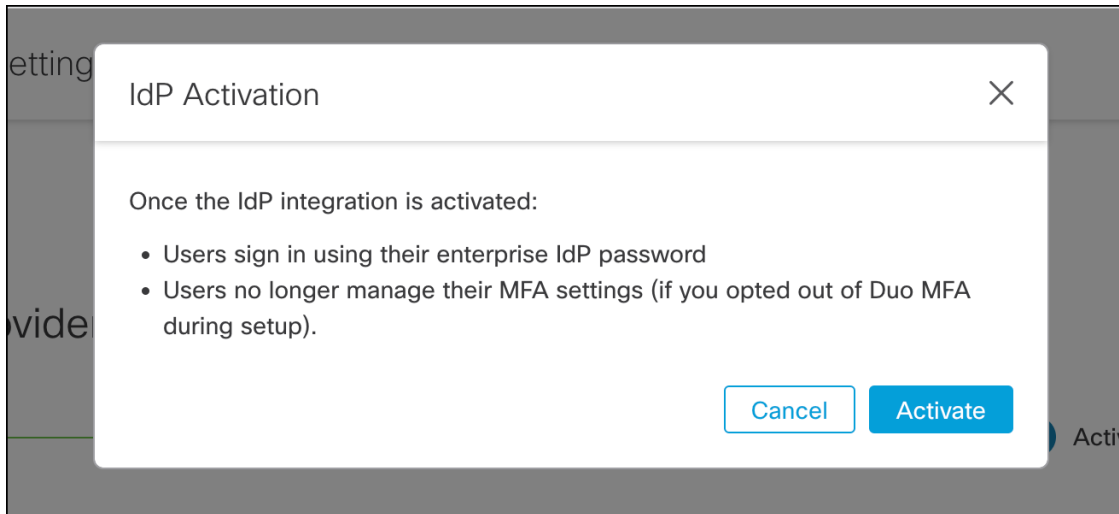
단계 3 Azure 콘솔 브라우저 탭으로 돌아갑니다.

- a) **Basic SAML Configuration**(기본 SAML 구성) 섹션에서 **Edit**(편집)를 클릭합니다.
- b) **Identifier (Entity ID)**(식별자(엔터티 ID)) 필드에서 입력한 임시 ID 공급자를 엔터프라이즈 설정 마법사에서 복사한 **Entity ID (Audience URI)**(엔터티 ID(대상 URI)) 필드의 값으로 대체합니다.
- c) **Reply URL (Assertion Consumer Service URL)**(회신 URL(어설션 소비자 서비스 URL)) 필드에서 입력한 임시 ID 공급자를 엔터프라이즈 설정 마법사에서 복사한 **ACS URL(Single Sign-On Service URL)** 필드의 값으로 대체합니다.
- d) **Save**(저장)를 클릭하고 **Basic SAML Configuration**(기본 SAML 구성) 패널을 닫습니다.

단계 4 엔터프라이즈 설정 마법사로 돌아가 통합을 테스트합니다. **Configure**(구성) 화면(4단계: **SSO 통합 테스트**, 15 페이지)에 있어야 하며 다음을 수행해야 합니다.

- a) 제공된 URL을 복사하여 개인(시크릿) 창을 엽니다.
- b) SAML 애플리케이션과 연결된 Azure AD 계정으로 로그인합니다.
SecureX 애플리케이션 포털로 돌아가면 테스트가 성공한 것입니다. 오류가 발생하면 **문제 해결**, 17 페이지의 내용을 참조하십시오.
- c) **Next**(다음)를 클릭하여 활성화 화면으로 진행합니다.

d) 준비가 되면 **Activate my IdP**(내 IdP 활성화)를 클릭한 다음 대화 상자에서 선택을 확인합니다.





7 장

Duo



중요 **Enterprise Manager**가 사용이 중지되었습니다. 이제 **보안 클라우드 제어**를 사용하여 ID 공급자 통합을 관리할 수 있습니다. 자세한 내용은 **ID 공급자 통합 가이드**를 참조하십시오.

모든 기존 ID 공급자 통합 데이터는 보안 클라우드 컨트롤을 통해 사용할 수 있습니다.

- [개요, 31 페이지](#)
- [시작하기, 31 페이지](#)

개요

이 가이드에서는 Duo SAML 애플리케이션을 생성하고 Security Cloud Sign On과(와) 통합하는 방법을 설명합니다.

시작하기

시작하기 전에

- 사용자는 소유자 역할의 Duo 관리자여야 합니다.
- **Duo Admin(Duo 관리) - Single Sign-On - Configure Authentication Sources**(인증 소스 구성)에서 인증 소스를 하나 이상 이미 Duo에 구성해야 합니다.
- 엔터프라이즈 설정 마법사의 **1단계: 엔터프라이즈 생성, 11 페이지** 및 **2단계: 이메일 도메인 클레임 및 확인, 12 페이지**를 완료해야 합니다.

단계 1 Duo Admin Panel에 로그인합니다.

- a) 왼쪽 메뉴에서 **Applications**(애플리케이션)를 클릭한 다음 **Protect Application**(애플리케이션 보호)을 클릭합니다.
- b) 일반 **SAML** 통신 사업자를 검색합니다.

- c) Duo에서 호스팅하는 SSO를 사용하는 2FA의 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 ID의 값을 복사하고 나중에 사용할 수 있도록 저장합니다.
- f) **SSO(Single Sign-On) URL**의 값을 복사하고 나중에 사용할 수 있도록 저장합니다.
- g) 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
<Last Name>	lastName

Map attributes	IdP Attribute	SAML Response Attribute
	<Email Address>	email
	<First Name>	firstName
	<Last Name>	lastName

- i) **Settings**(설정) 섹션의 **Name**(이름) 필드에 보안 클라우드 로그인 또는 다른 값을 입력합니다.
Duo SAML 설정 브라우저 창을 열어 둡니다.

단계 2 새 브라우저 탭에서 엔터프라이즈 설정 마법사를 엽니다. 현재 **Integrate Identity Provider**(ID 공급자 통합) 화면(**3 단계: SAML 메타데이터 교환, 13 페이지 참조**)의 **Set Up**(설정) 단계에 있어야 합니다.

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

Set Up — 2 Download — 3 Configure — 4 Activate

Download

Depending on your provider, use the following information to set up your Identity Provider (IdP).

Single Sign-On Service URL (ACS URL)	https://sso-preview.test.se...	
Entity ID (Audience URI)	https://www.okta.com/saml...	
SAML Signing Certificate	cisco-securex.pem	Download
SecureX Sign-On SAML Metadata	cisco-securex-saml-metadata.xml	Download

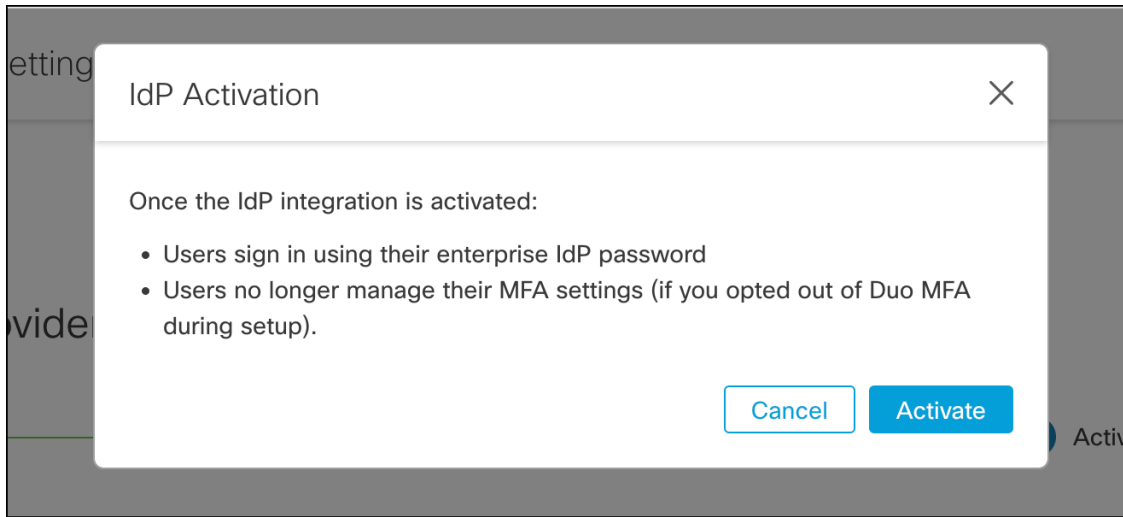
- i) **Next(다음)**를 클릭하여 **Configure(구성)** 화면으로 이동합니다.

단계 3 Duo SAML 애플리케이션 구성으로 돌아가 다음을 수행합니다.

- a) **Service Provider(통신 사업자)** 섹션의 **Entity ID(엔터티 ID)** 필드에 이전 단계에서 설정 마법사가 제공한 **Entity ID (Audience URI)** 필드의 값을 입력합니다.
- b) **Assertion Consumer Service (ACS) URL**에 이전 단계에서 설정 마법사가 제공한 **Single Sign-On Service URL (ACS URL)** 필드의 값을 입력합니다.
- c) 구성 페이지의 하단에서 **Save(저장)**를 클릭합니다.

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

- a) 표시된 URL을 복사하여 비공개(시크릿) 브라우저 창에서 엽니다. 브라우저가 Duo SSO URL로 리디렉션됩니다.
- b) **2단계: 이메일 도메인 클레임 및 확인**과 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) 사용자에게 통합을 활성화하려면 **Activate my IdP(내 IdP 활성화)**를 클릭합니다.
- e) 대화 상자에서 결정을 확인합니다.





8 장

Google



중요 **Enterprise Manager**가 사용이 중지되었습니다. 이제 **보안 클라우드 제어**를 사용하여 ID 공급자 통합을 관리할 수 있습니다. 자세한 내용은 **ID 공급자 통합 가이드**를 참조하십시오.

모든 기존 ID 공급자 통합 데이터는 보안 클라우드 컨트롤을 통해 사용할 수 있습니다.

- [개요, 35 페이지](#)
- [시작하기, 35 페이지](#)

개요


이 가이드에서는 Google Workplace SAML 애플리케이션을 생성하여 Security Cloud Sign On과(와) 통합하는 방법을 설명합니다.

시작하기

시작하기 전에

- 슈퍼 관리자 권한이 있는 Google Workspace 계정이 있어야 합니다.
- 엔터프라이즈 설정 마법사의 **1단계: 엔터프라이즈 생성, 11 페이지** 및 **2단계: 이메일 도메인 클레임 및 확인, 12 페이지**를 완료해야 합니다.

단계 1 슈퍼 관리자 권한이 있는 계정을 사용하여 [Google 관리 콘솔](#)에 로그인합니다.

- 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.

- Continue**(계속)를 클릭합니다.
- SSO URL** 및 엔터티 **ID**를 복사하고 인증서를 다운로드합니다.

단계 2 새 브라우저 탭에서 Enterprise 설정 마법사를 엽니다. 사용자는 3단계: [SAML 메타데이터 교환](#), 13 페이지에 있어야 합니다.

- ID 공급자(IdP)** 이름에 **Google SSO** 또는 다른 값을 입력합니다.
- Single Sign-On Service URL** 필드에 Google Admin Console에서 복사한 "SSO URL"을 입력합니다.
- Entity ID (Audience URI)**(엔터티 **ID**(대상 **URI**)) 필드에 Google Admin Console에서 복사한 "엔터티 ID"를 입력합니다.
- Add File...**(파일 추가...)을 클릭하고 Google Admin Console에서 다운로드한 인증서를 선택합니다.
- 원하는 경우 사용자에게 대해 무료 **Duo 다단계 인증**을 옵트아웃합니다.
- Next**(다음)를 클릭합니다.
- Single Sign-On Service URL(ACS URL)** 및 엔터티 **ID**(대상 **URI**)를 복사하고 **SAML 서명 인증서**를 다운로드합니다.

단계 3 Google Admin Console로 돌아갑니다.

- Add custom SAML app**((맞춤형 **SAML** 앱 추가)) 페이지에서 **Continue**(계속)를 클릭합니다.
- 이전에 엔터프라이즈 설정 마법사에서 복사한 "Single Sign-On Service URL(ACS URL)을 **ACS URL** 필드에 입력합니다.
- Name ID**(이름 **ID**) 형식에 대해 **UNSPECIFIED** 또는 **EMAIL**을 선택합니다.
- Name ID(이름 ID)에 대해 **Basic Information**(기본 정보) > **Primary Email**(기본 이메일)을 선택합니다.
- Continue**(계속)를 클릭합니다.
- Attributes mapping**(속성 매핑) 페이지에서 다음 속성 매핑을 추가합니다.

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

Attributes

Add and select user fields in Google Directory, then map them to service provider attributes. Attributes marked with * are mandatory. [Learn more](#)

Google Directory attributes	App attributes
Basic Information > First name	firstName
Basic Information > Last name	lastName
Basic Information > Primary email	email

[ADD MAPPING](#)

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

- 표시된 URL을 복사하여 비공개(시크릿) 브라우저 창에서 엽니다. 브라우저가 Google SSO URL로 리디렉션됩니다.
- 2단계: 이메일 도메인 클레임 및 확인**과 일치하는 이메일 주소로 Google에 로그인합니다. SecureX 애플리케이션 포털로 다시 연결되면 테스트에 성공한 것입니다.
- 설정 마법사에서 **Next**(다음)를 클릭하여 **Activate**(활성화) 화면으로 이동합니다.
- 사용자에 대한 통합을 활성화하려면 **Activate my IdP**(내 IdP 활성화)를 클릭합니다.
- 대화 상자에서 결정을 확인합니다.

IdP Activation [X]

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](#)



9 장

Okta



중요 **Enterprise Manager**가 사용이 중지되었습니다. 이제 **보안 클라우드 제어**를 사용하여 ID 공급자 통합을 관리할 수 있습니다. 자세한 내용은 **ID 공급자 통합 가이드**를 참조하십시오.

모든 기존 ID 공급자 통합 데이터는 보안 클라우드 컨트롤을 통해 사용할 수 있습니다.

- [개요, 39 페이지](#)
- [시작하기, 39 페이지](#)

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, 11 페이지** 및 **2단계: 이메일 도메인 클레임 및 확인, 12 페이지**를 완료해야 합니다.

단계 1 Okta 관리 콘솔에 로그인하고 다음을 수행합니다.

- Applications**(애플리케이션) 메뉴에서 **Applications**(애플리케이션)를 선택합니다.
- Create App Integration**(앱 통합 생성)을 클릭합니다.
- SAML 2.0**을 선택하고 **Next**(다음)를 클릭합니다.
- 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

Attribute Statements (optional) [LEARN MORE](#)

Name	Name format (optional)	Value
firstName	Unspecified ▼	user.firstName ▼
lastName	Unspecified ▼	user.lastName ▼ ×
email	Unspecified ▼	user.email ▼ ×

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

SAML Signing Certificates

[Generate new certificate](#)

Type	Created	Expires	Status	Actions
SHA-1	Today	Feb 2033	Inactive ⚠	Actions ▼
SHA-2	Today	Mar 2033	Active	Actions ▼

SAML Setup

Single Sign On using SAML will not work until you configure the app to trust Okta as an IdP.

[View SAML setup instructions](#)

- q) 열리는 페이지에서 **ID 공급자 Single Sign-On URL** 및 **ID 공급자 발급자**를 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 교환, 13 페이지**에 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.

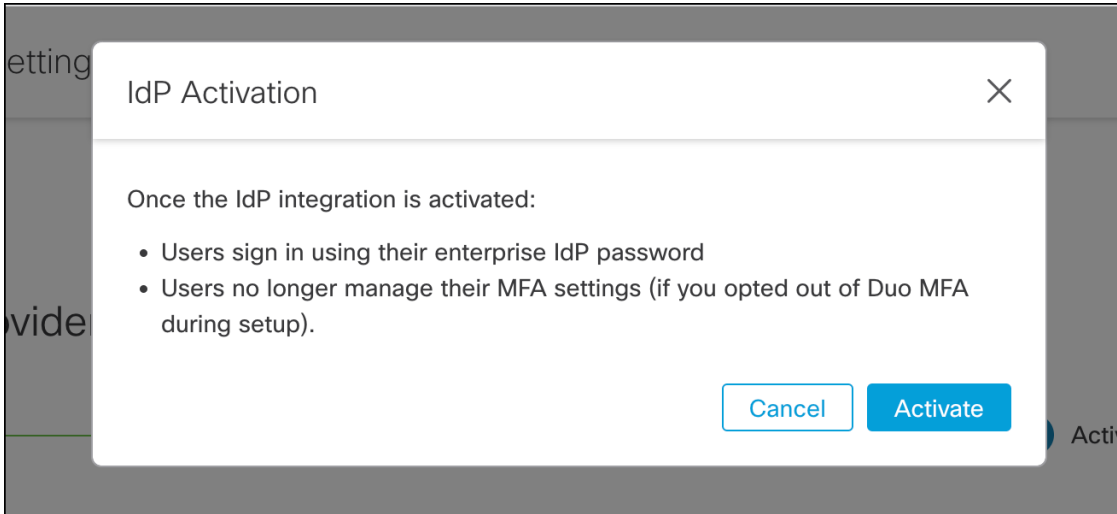
- a) **General**(일반) 탭을 클릭합니다.
- b) **SAML Settings**(SAML 설정) 섹션에서 **Edit**(편집)를 클릭합니다.
- c) **Next**(다음)를 클릭합니다.
- d) **Single sign-on URL**의 값을 엔터프라이즈 설정 마법사가 제공한 "Single Sign-On Service URL (ACS URL)" 필드의 값으로 교체합니다.
- e) **Audience URI (SP Entity ID)**(대상 URI (SP 엔터티 ID))의 값을 엔터프라이즈 설정 마법사가 제공한 "Entity 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) **2단계: 이메일 도메인 클레임 및 확인**과 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) 사용자에게 통합을 활성화하려면 **Activate my IdP**(내 IdP 활성화)를 클릭합니다.
- e) 대화 상자에서 결정을 확인합니다.





10 장

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 가이드**를 참조하십시오.

모든 기존 ID 공급자 통합 데이터는 보안 클라우드 컨트롤을 통해 사용할 수 있습니다.

- [개요, 43 페이지](#)
- [시작하기, 43 페이지](#)

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, 11 페이지** 및 **2단계: 이메일 도메인 클레임 및 확인, 12 페이지**를 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.

Add Application

SAML Configuration

Provide Application Metadata

Import Metadata Import From URL Manually Enter

 cisco-security-cloud-saml-metadata (3).xml 

ACS URLs *

https://security.cisco.com/sso/saml2/0oa1sc3asja...

+ Add

Entity ID *

https://www.okta.com/saml2/service-provider/spn...

- 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.

Attributes	PingOne Mappings	Required
saml_subject	Email Address	<input checked="" type="checkbox"/>
email	Email Address	<input checked="" type="checkbox"/>
firstName	Given Name	<input checked="" type="checkbox"/>
lastName	Family Name	<input checked="" type="checkbox"/>

o) **Save**(저장)를 클릭하여 매핑을 저장합니다.

단계 2 새 브라우저 탭에서 [엔터프라이즈 설정 마법사](#)입니다. 현재 **Integrate Identity Provider(ID 공급자 통합)** 화면(3단계: [SAML 메타데이터 교환, 13 페이지](#))의 **Set Up**(설정) 단계에 있어야 합니다.

- Identity Provider (IdP) Name**(ID 공급자(IdP) 이름) 필드에 통합의 이름(예: **Ping SSO**)을 입력합니다.
- Ping SAML 애플리케이션에서 복사한 **Issuer ID**(발급자 ID) 필드의 값을 **Single Sign-On Service URL** 필드에 입력합니다.
- Add...**(추가...)를 클릭하고 이전에 다운로드한 Ping 서명 인증서를 선택합니다.
- 원하는 경우 사용자에게 대해 무료로 Duo 다단계 인증을 옵트아웃할 수 있습니다.

Integrate Identity Provider

1 Set Up
2 Download
3 Configure
4 Activate

Set Up

Identity Provider (IdP) Name

Single Sign-On Service URL ⓘ

Entity ID (Audience URI) ⓘ

SAML Signing Certificate ⓘ

File must be in PEM format

By default, SecureX Sign-On enrolls all users into [Duo MultiFactor Authentication \(MFA\)](#) at no cost. We strongly recommend MFA, with a session timeout no greater than 2 hours, to help protect your sensitive data within Cisco Security products.

Do you wish to keep the Duo-based MFA enabled in SecureX Sign-On? Yes No

If your organization has integrated MFA at your IdP, you may wish to disable MFA at the SecureX Sign-On level.

- 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.

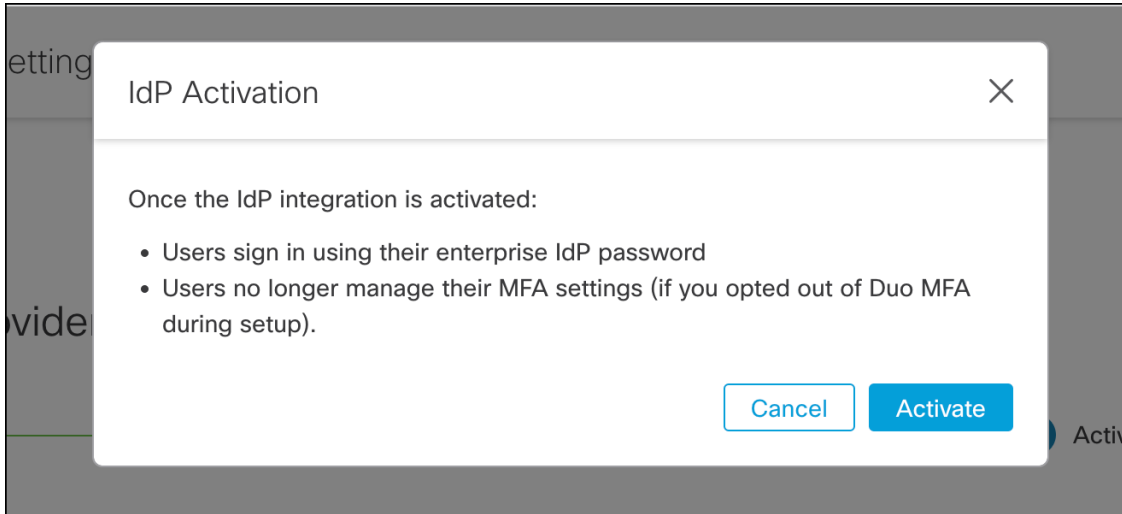
단계 3 Ping ID 콘솔로 돌아가 다음 작업을 수행합니다.

- 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) **2단계: 이메일 도메인 클레임 및 확인**과 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.





11 장

일반 IdP 지침



중요 **Enterprise Manager**가 사용이 중지되었습니다. 이제 **보안 클라우드 제어**를 사용하여 ID 공급자 통합을 관리할 수 있습니다. 자세한 내용은 **ID 공급자 통합 가이드**를 참조하십시오.

모든 기존 ID 공급자 통합 데이터는 보안 클라우드 컨트롤을 통해 사용할 수 있습니다.

- 일반 IdP 지침, 49 페이지
- SAML 응답 요구 사항, 49 페이지
- SAML 메타데이터 요구 사항, 50 페이지

일반 IdP 지침

특정 ID 공급자용 SAML 애플리케이션 생성에 대한 지침이 여기에 없는 경우 IdP가 제공하는 지침을 따르십시오. SAML 응답은 적절한 <NameID> 값과 속성 이름 매핑을 사용하여 구성해야 합니다. 또한 Security Cloud Sign On에 SAML 앱의 SSO(Single Sign On) URL 및 엔터티 ID를 제공해야 합니다.

SAML 응답 요구 사항

SHA-256으로 서명된 SAML 응답

ID 공급자가 반환한 SAML 응답은 SHA-256 서명 알고리즘으로 서명되어야 합니다. Security Cloud Sign On은(는)서명되지 않았거나 다른 알고리즘으로 서명된 응답은 거부합니다.

SAML 응답 속성

IdP가 전송한 SAML 응답의 어설션에는 다음 속성 이름이 포함되어야 하며 IdP의 해당 속성에 매핑되어야 합니다.

SAML 어설션 속성 이름	IdP 사용자 속성
firstName	사용자의 이름입니다.

SAML 어설션 속성 이름	IdP 사용자 속성
lastName	사용자의 성입니다.
email	사용자 이메일입니다. 이 값은 SAML 응답의 <NameID> 요소 값과 일치해야 합니다.

예를 들어, 다음 XML 스니펫은 Security Cloud Sign On ACL URL에 대한 SAML 응답에 포함된 <AttributeStatement> 요소의 예입니다.

```
<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">John
    </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">Doe
    </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">jdoe@example.com
    </saml2:AttributeValue>
  </saml2:Attribute>
</saml2:AttributeStatement>
```

NameID 요소

IdP에서 보낸 SAML 응답의 <NameID> 요소에는 유효한 이메일 주소가 값으로 있어야 하며, 이메일은 [SAML 응답 속성, 49 페이지](#)의 **email** 속성 값과 일치해야 합니다.

<NameID>의 **Format** 속성은 **urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified** 또는 **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**로 설정해야 합니다.

아래는 <NameID> 요소의 예입니다.

```
<saml2:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">jdoe@example.com</saml2:NameID>
```

SAML 메타데이터 요구 사항

Security Cloud Sign On과(와) 통합하려면 IdP의 SAML 애플리케이션에 있는 다음 메타데이터가 필요합니다.

- **SSO(Single Sign-On)** 서비스 초기 **URL** - "SSO URL" 또는 "로그인 URL"이라고도 합니다. 이 URL은 Security Cloud Sign On에 대한 IdP 시작 인증을 시작하는 데 사용할 수 있습니다.
- 엔터티 **ID URI** - IdP의 전역 고유 이름입니다. 이를 "발급자"라고도 합니다.
- **X.509** 서명 인증서 - IdP가 SAML 어설션 서명에 사용하는 공개/개인 키 쌍의 공개 키입니다.

번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.