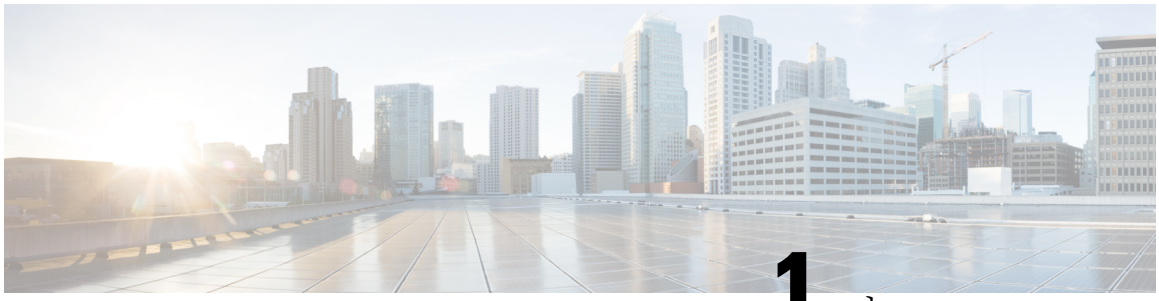
Cisco 보안 클라우드 제어 사용 설명서

초판: 2023년 4월 16일

최종 변경: 2023년 10월 6일

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

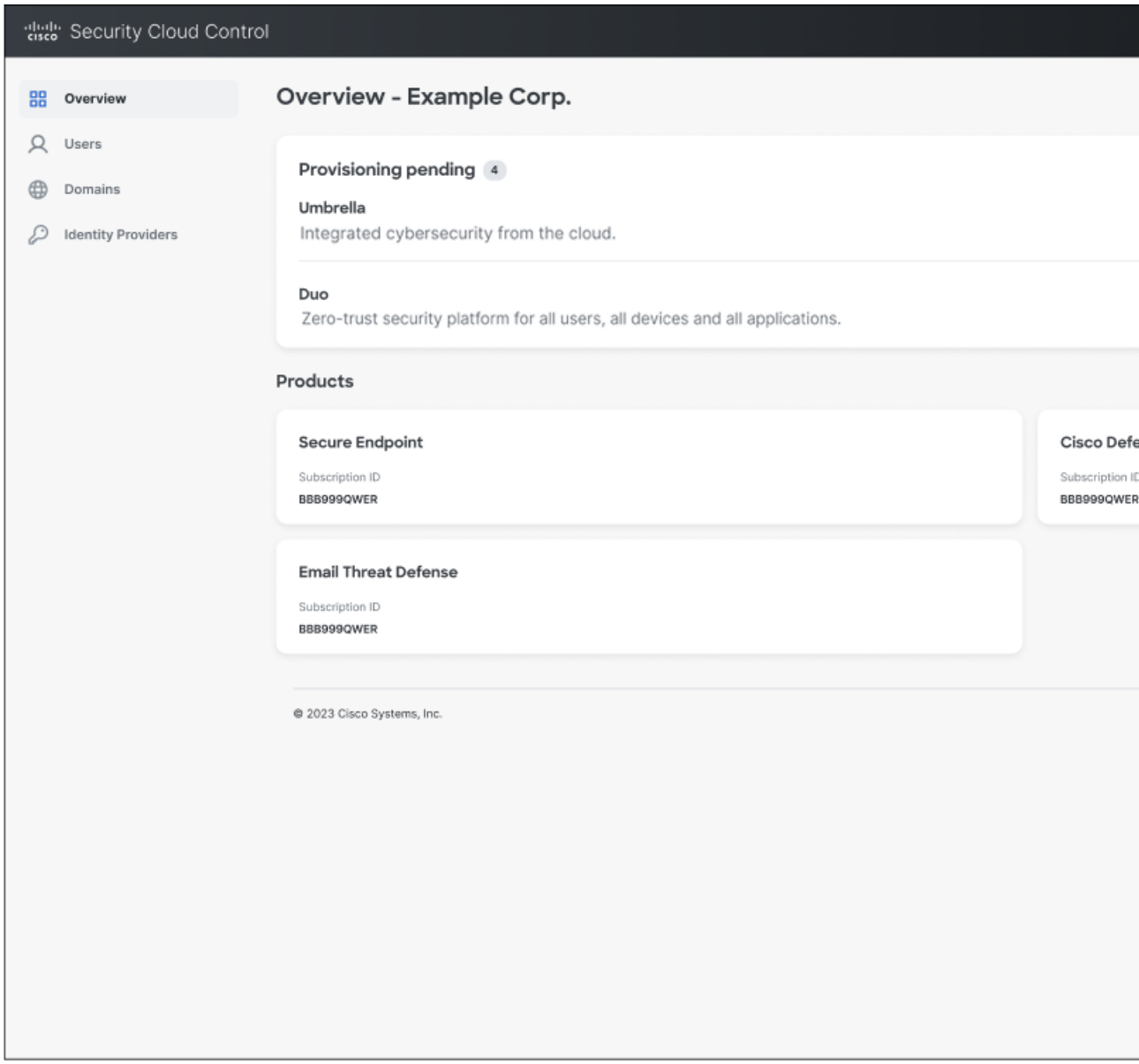
개요

Cisco Security Cloud 제어 개요

Security Cloud Control은 Cisco Security Cloud 전체에서 Cisco Secure 제품 프로비저닝, 사용자 ID 및 사용자 액세스 관리의 중앙 집중식 관리를 제공하는 웹 애플리케이션입니다. Security Cloud Control 관리자는 새로운 Security Cloud 엔터프라이즈를 생성하고, 엔터프라이즈의 사용자를 관리하고, 도메인을 클레임하고, 조직의 SSO ID 제공자를 통합하는 등의 작업을 수행할 수 있습니다.

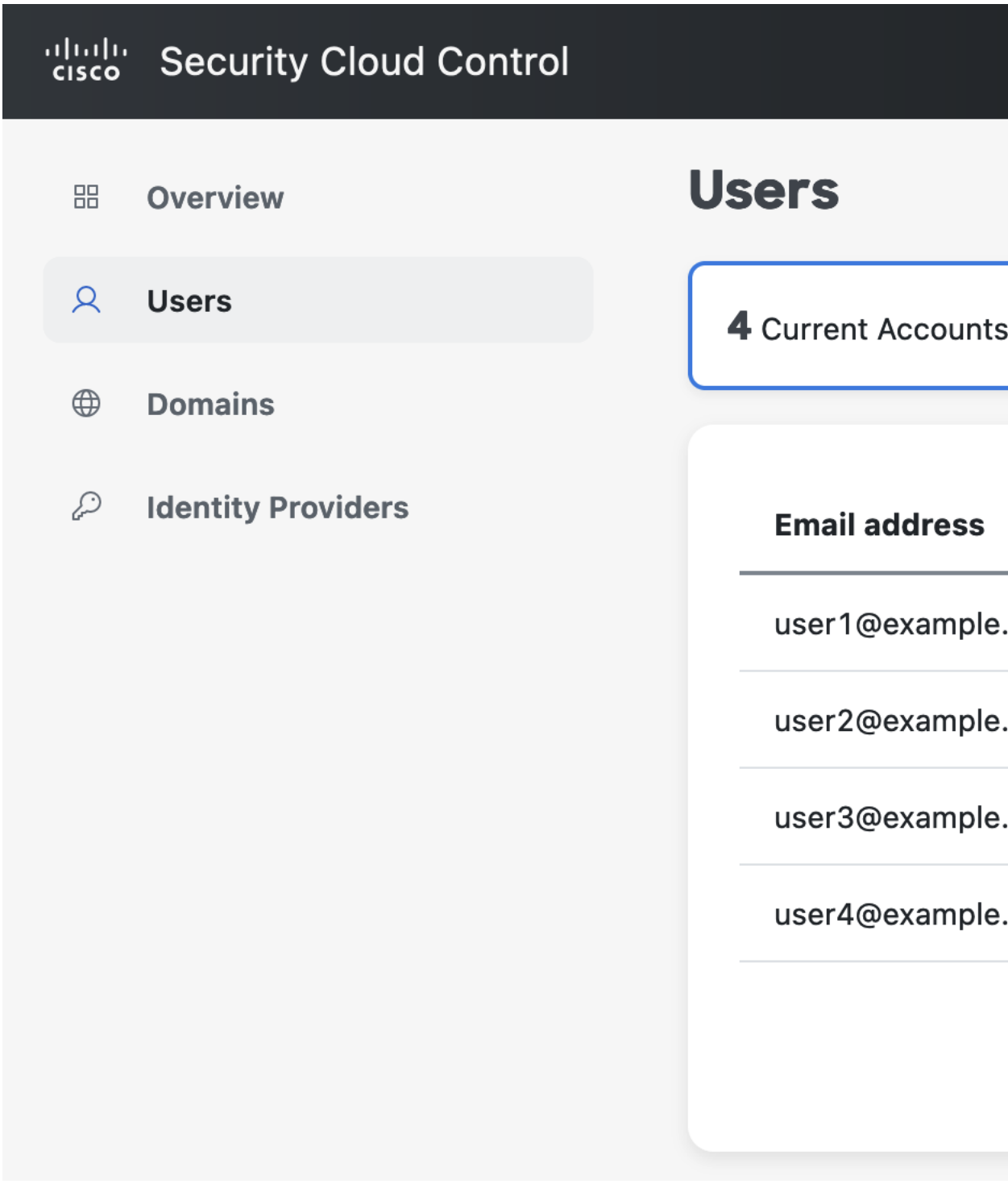
Overview(개요**)** 탭

Overview(개요**)** 탭에서는 Cisco Secure 제품 구독을 관리하고 새로운 제품 인스턴스를 제공합니다. 자세한 내용은 제품 및 구독 관리, 7 페이지 섹션을 참조해 주십시오.



Users(사용자**)** 탭

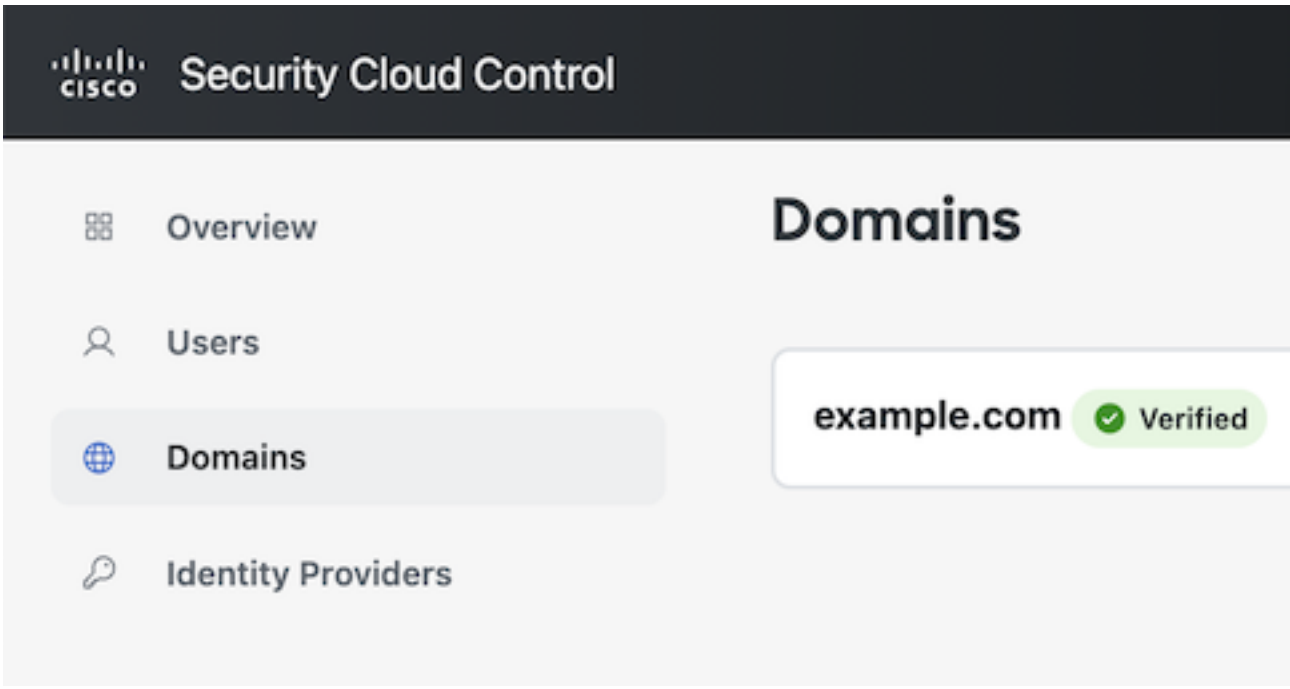
Users(사용자**)** 탭은 관리자가 엔터프라이즈에 사용자 초대 사용자를 나열합니다. 관리자는 사용자 비밀번호와 MFA 설정(도메인 클레임 및 확인의 사용자의 경우)을 재설정하고 사용자 계정을 비활성화할 수도 있습니다. 자세한 내용은 사용자 관리, 13 페이지를 참조하십시오.



Domains(도메인**)** 탭

Domains(도메인**)** 탭에는 엔터프라이즈에 대해 클레임되고 확인된 이메일 도메인이 나열되어 있습니다. ID 제공자를 Security Cloud Sign On과 통합하려면 도메인을 확인해야 합니다. 또한 이를 통해 관

리자는 클레임된 도메인에 있는 사용자의 비밀번호 또는 MFA 설정을 재설정할 수 있습니다. 자세한 내용은 도메인 관리, 17 페이지를 참조하십시오.



Identity Providers(ID 제공자) 탭

Identity Providers(ID 제공자) 탭에는 현재 엔터프라이즈에 대해 SAML(Secure Assertion Markup Language)을 사용하여 Security Cloud Sign On과 통합되는 모든 ID 제공자가 나열됩니다. 이를 통해 엔터프라이즈 사용자는 ID 제공자의 SSO 인증서를 사용해 Cisco Secure 제품에 액세스할 수 있습니다. 자세한 내용은 ID 제공자 통합 가이드, 19 페이지의 내용을 참조하십시오.

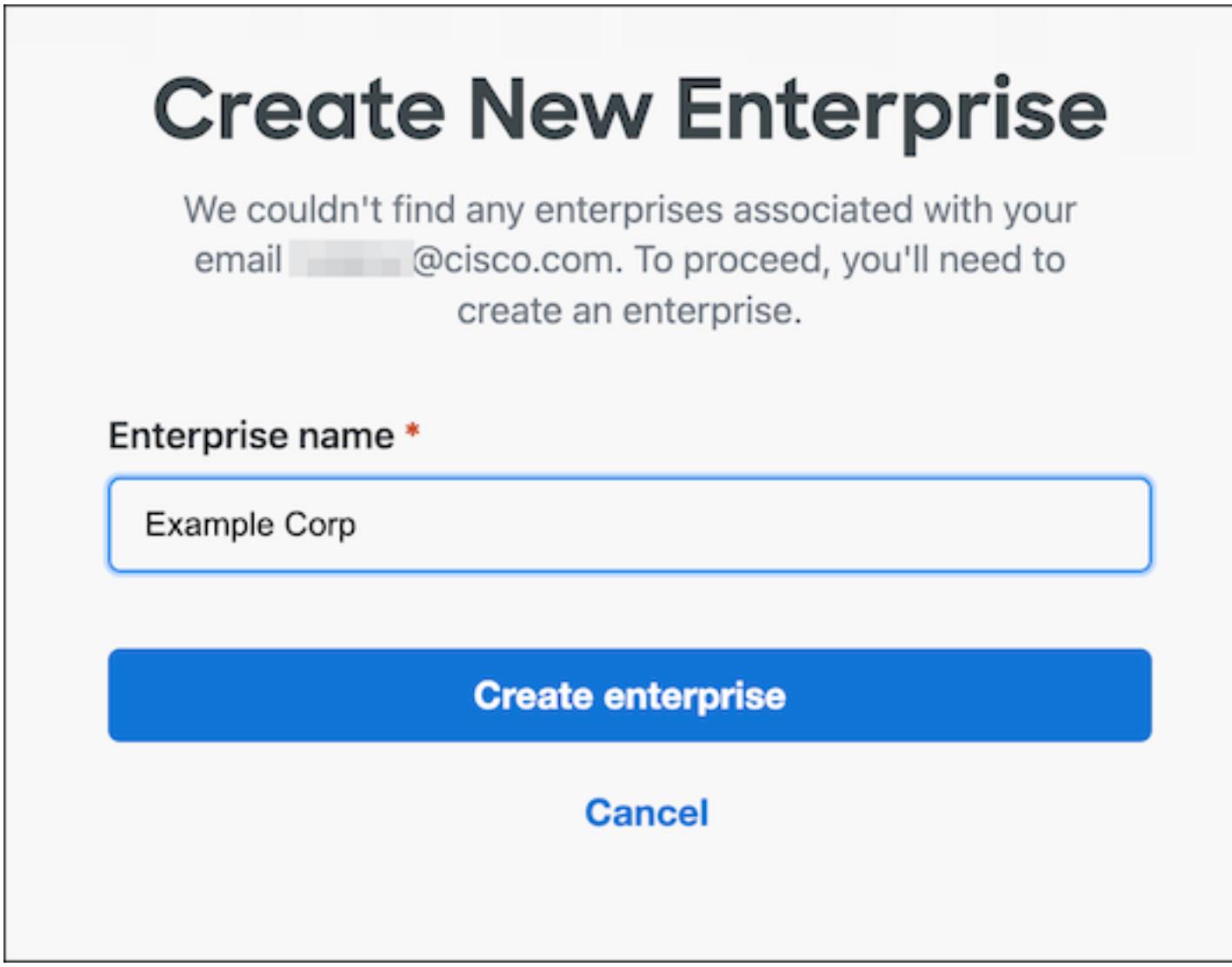
Security Cloud Control 로그인

보안 클라우드 제어에 로그인하려면 Cisco Security Cloud Sign On 계정이 필요합니다. 계정이 없는 경우에는 새로 생성할 수 있습니다. 보안 클라우드 로그인으로 인증하면 보안 클라우드 엔터프라이즈도 선택해야 합니다. 엔터프라이즈는 조직의 사용자, 제품 구독, 클레임된 도메인 및 기타 정보로 구성됩니다.

단계 **1** Security Cloud Control(보안 클라우드 제어)에 로그인합니다.

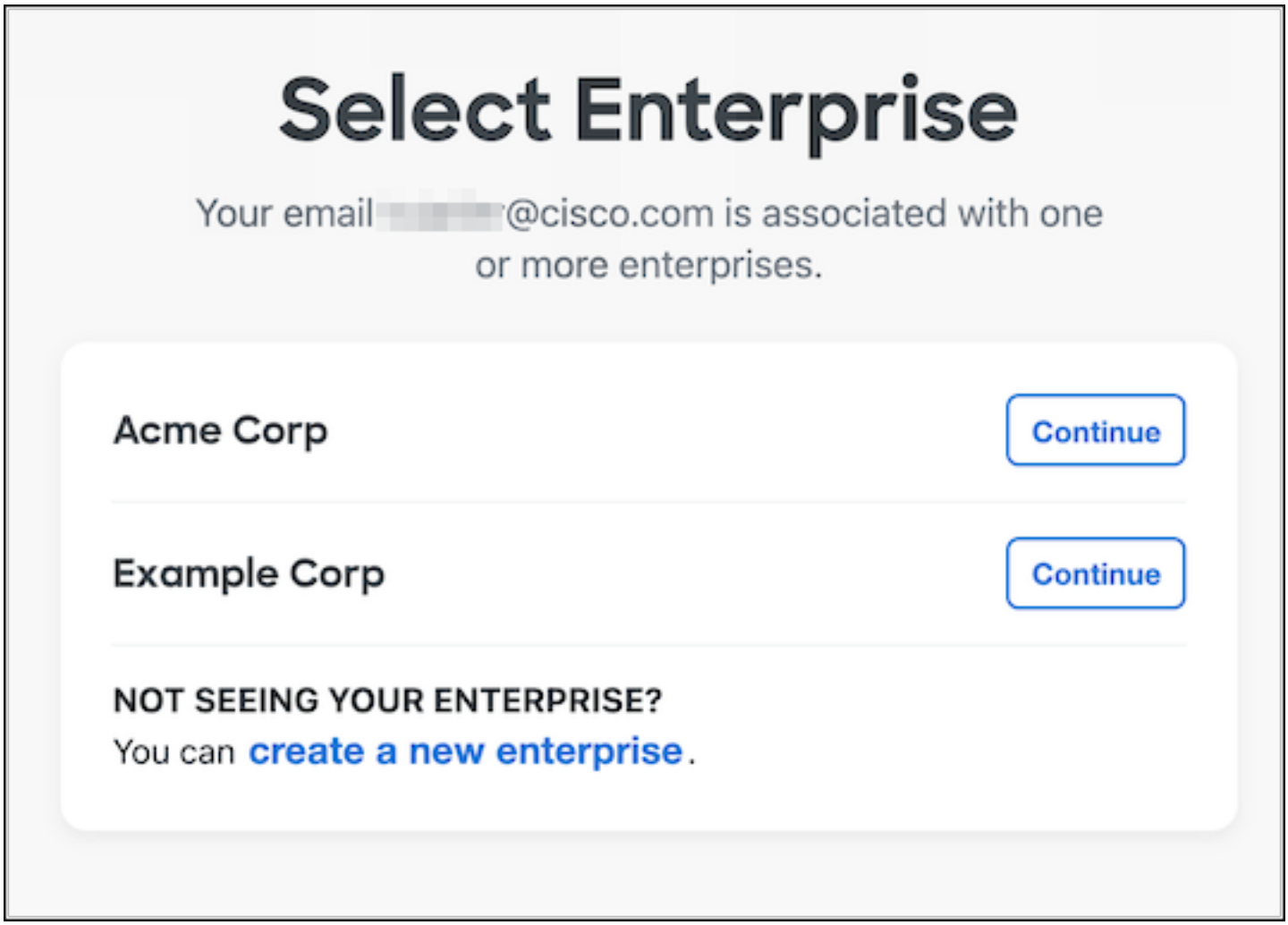
계정이 보안 클라우드 엔터프라이즈와 연결되지 않은 경우 계속하려면 계정을 생성해야 합니다. 또는 기존 엔터프라이즈에 로그인하려면 **3**단계로 건너뜁니다.

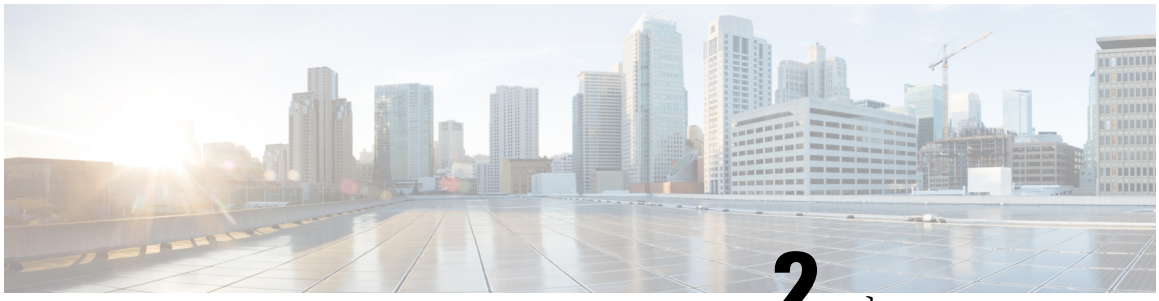
단계 **2** 엔터프라이즈 이름을 입력하고 **Create enterprise(**엔터프라이즈 생성**)**를 클릭합니다.



엔터프라이즈를 생성하고 나면 **Select Enterprise(**엔터프라이즈 선택**)** 페이지로 다시 이동합니다.

단계 **3** **Continue(**계속**)**를 클릭하여 로그인할 엔터프라이즈를 선택합니다.


Select Enterprise
Your email @cisco.com is associated with one or more enterprises.
Acme Corp
Continue
Example Corp
Continue
NOT SEEING YOUR ENTERPRISE?
You can create a new enterprise.



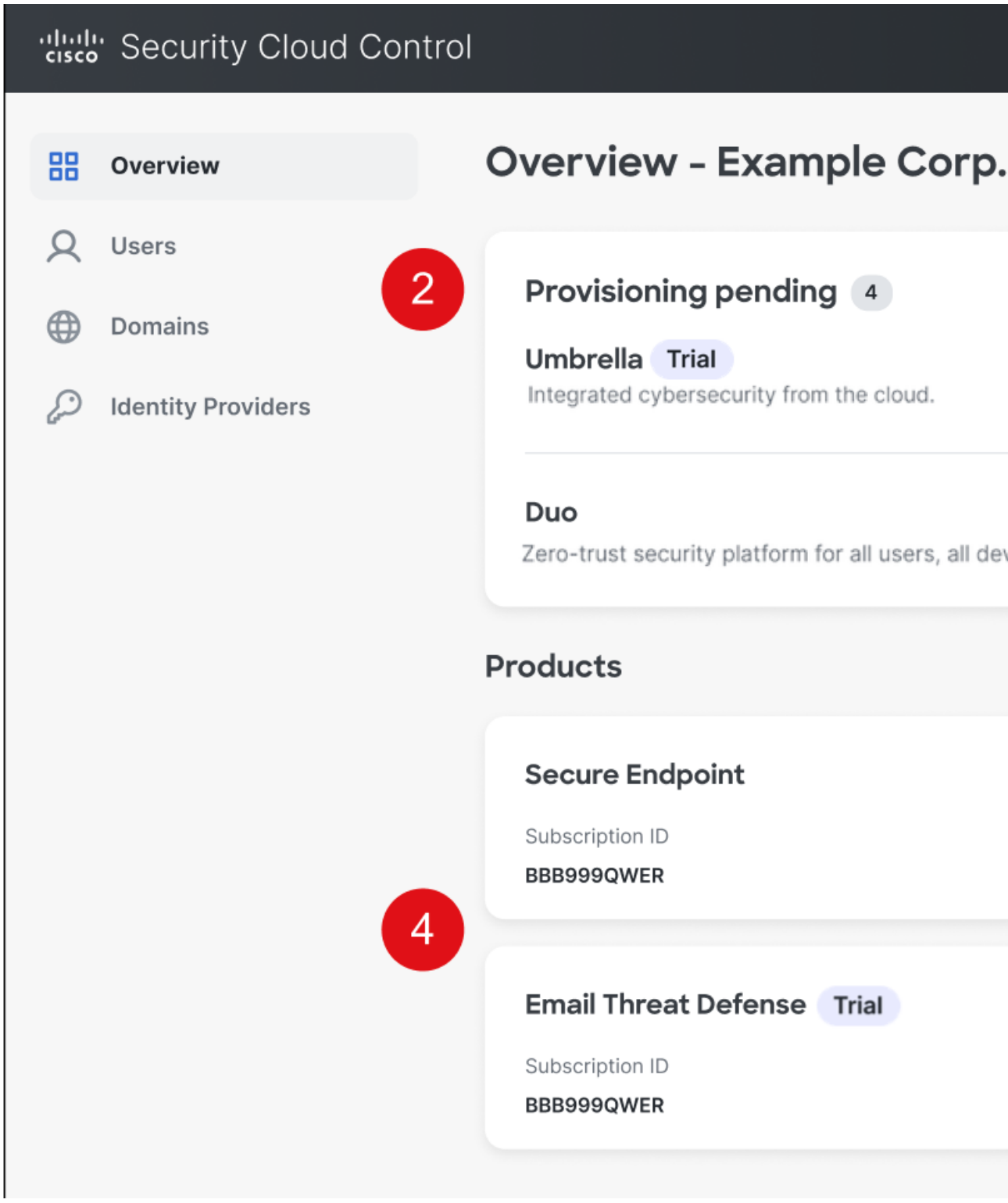
2 장

제품 및 구독 관리

개요

Cisco에서 새 구독을 구매하면, 구매 프로세스 중에 지정한 초기 프로비저닝 연락처로 구독 클레임 코드가 이메일로 전송됩니다. 보안 클라우드 엔터프라이즈 관리자가 클레임 코드를 받으면 **Claim subscription(**구독 클레임**)(1)**을 클릭하여 현재 엔터프라이즈를 위한 구독을 신청합니다.

구독이 클레임되면 해당 제품은 **Provisioning pending(**프로비저닝 보류**)** 아래에 해당 시작 날짜**(2)**와 함께 나열됩니다. 제품 구독의 시작 날짜에 도달하면 **Start provisioning(**프로비저닝 시작 버튼**)(3)**이 활성화되어 엔터프라이즈 관리자가 제품을 프로비저닝할 수 있습니다. 프로비저닝된 제품 및 진행 중인 제품이 **Products(**제품**)** 섹션**(4)**에 나열됩니다. Trial 레이블은 평가판 구독을 나타냅니다.


Security Cloud Control
Overview
Users
Domains
Identity Providers
2
Overview - Example Corp.
Provisioning pending 4
Umbrella Trial
Integrated cybersecurity from the cloud.
Duo
Zero-trust security platform for all users, all dev
Products
Secure Endpoint
Subscription ID
BBB999QWER
4
Email Threat Defense Trial
Subscription ID
BBB999QWER

구독 클레임

Cisco Secure 제품 구독을 구매하면 초기 프로비저닝 연락처로 지정된 사용자에게 구독 클레임 번호가 이메일로 전송됩니다. 이 연락처는 구독을 관리할 Security Cloud Control 관리자일 수도 있고 아닐 수도 있습니다. Security Cloud Control 관리자는 클레임 번호를 사용하여 엔터프라이즈를 위한 구독을 클레임합니다. 클레임되면 구독의 제품이 **Provision pending(**프로비저닝 보류 중**)** 목록에 추가되고 구독의 시작 날짜에 도달하면 구독을 프로비저닝할 수 있습니다(제품 인스턴스 프로비저닝, 10 페이지 참조).

시작하기 전에

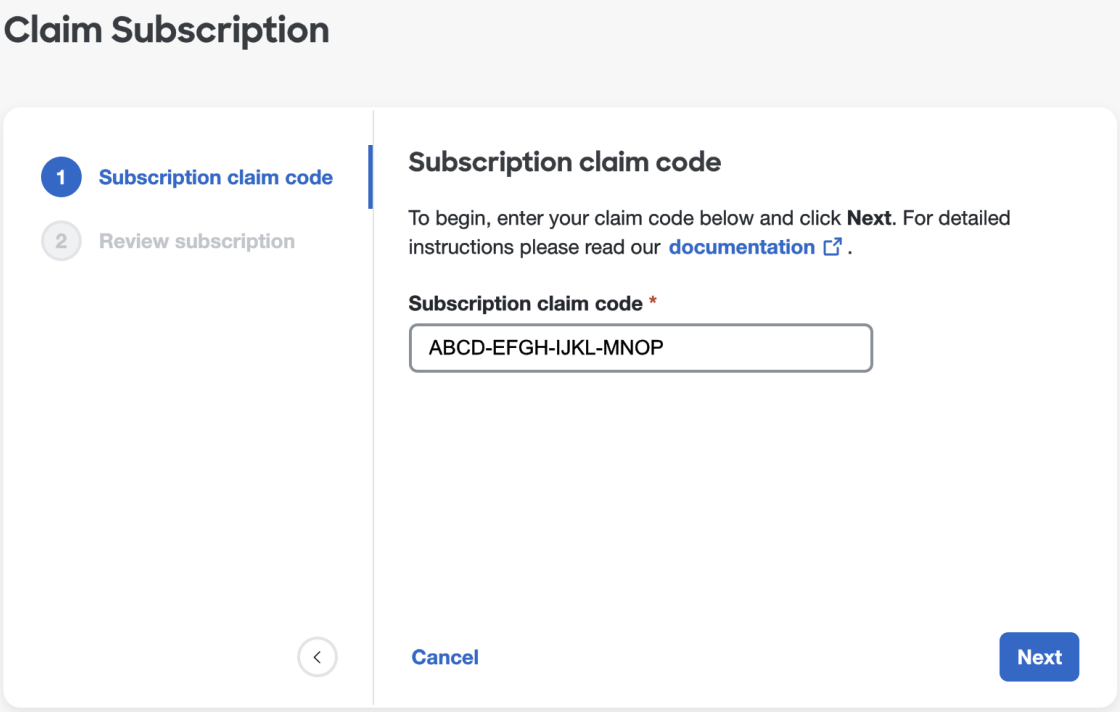
이 단계를 완료하려면 구독 클레임 코드가 필요합니다.

단계 **1** 보안 클라우드 제어에 로그인합니다.

단계 **2** 메시지가 표시되면 구독의 제품을 클레임 및 프로비저닝할 엔터프라이즈를 선택하거나 새 엔터프라이즈를 생성합니다.

단계 **3** 오른쪽 상단에서 **Claim subscription(**구독 클레임**)**을 클릭합니다.

단계 **4** 클레임 번호를 입력하고 **Next(**다음**)**를 클릭합니다.



단계 **5** 구독의 제품 목록을 검토한 다음 **Claim subscription(**구독 클레임**)**을 클릭합니다.

구독의 제품이 **Overview(**개요**)** 탭의 **Provisioning pending(**프로비저닝 보류 중**)** 목록에 추가됩니다.

다음에 수행할 작업

구독 시작 날짜에 도달한 제품 인스턴스 프로비저닝을 시작할 수 있습니다.

제품 인스턴스 프로비저닝

구독이 구독 클레임 시작일에 도달하면 새 제품 인스턴스를 프로비저닝하거나 기존 제품 인스턴스에 구독을 적용할 수 있습니다(사용 가능한 경우). 새 인스턴스를 프로비저닝할 때 인스턴스를 프로비저닝할 지리적 지역과 초기 관리자의 이메일을 제공해야 합니다.

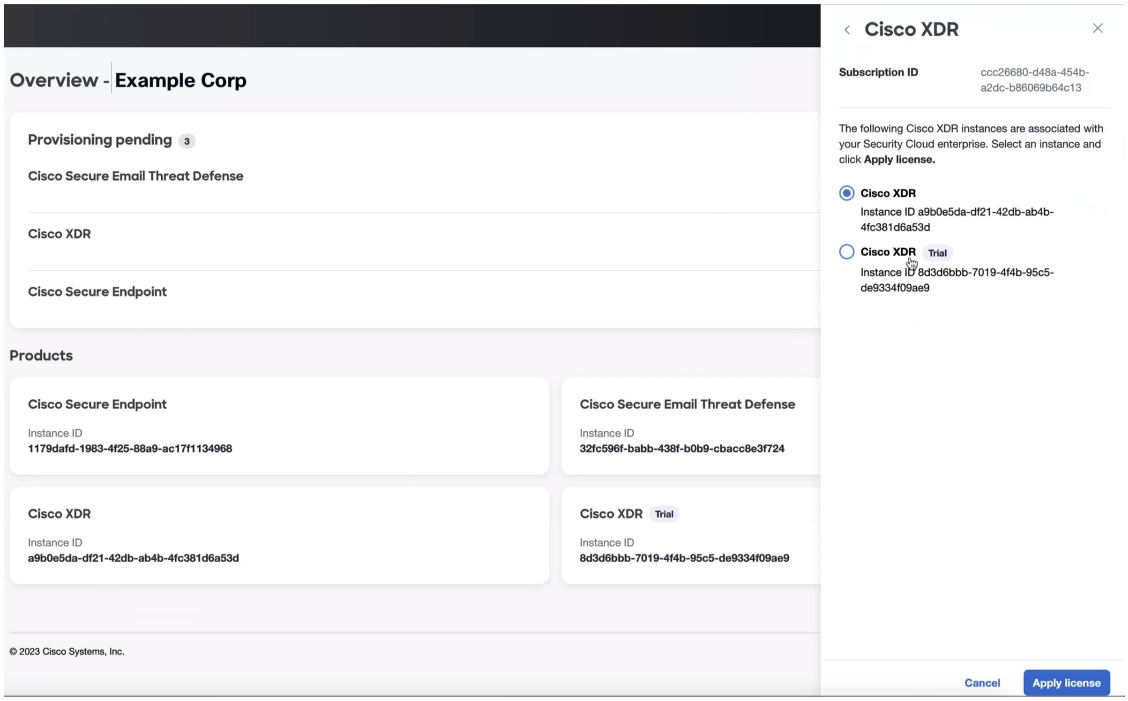
기존 인스턴스에 구독을 적용하면 기존 인스턴스의 라이선스를 이용해 새 인스턴스를 프로비저닝하거나 기존 인스턴스에 라이선스를 적용할 수 있습니다.

단계 **1** 보안 클라우드 제어에 로그인합니다.

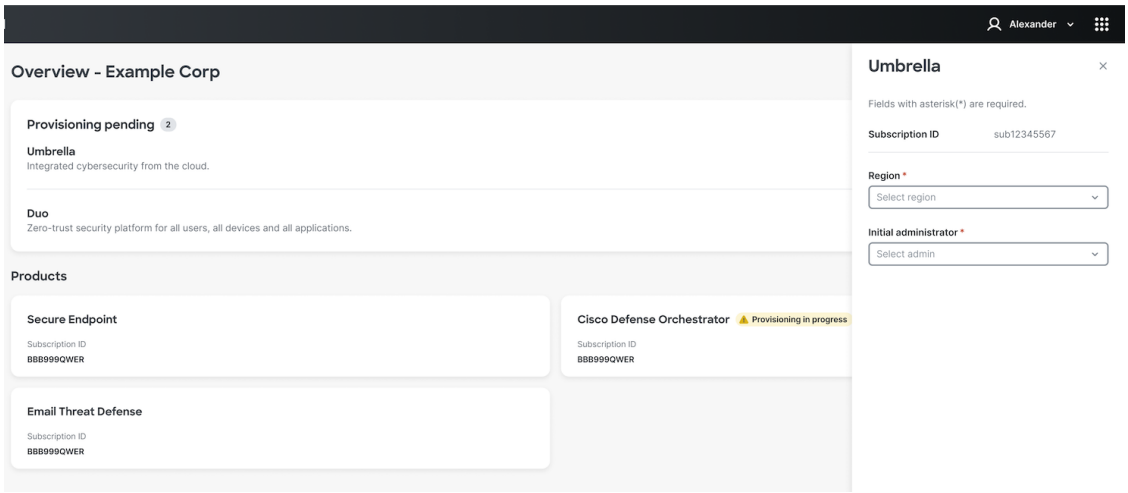
단계 **2** 엔터프라이즈를 선택하라는 메시지가 표시되면 관련 제품 구독을 구독 클레임하는 데 사용한 것과 같은 엔터프라이즈를 선택합니다.

단계 **3** **Overview(**개요**)** 탭의 **Pending provisioning(**프로비저닝 보류**)** 아래에서 프로비저닝할 제품을 찾고 **Start provisioning(**프로비저닝 시작**)**을 클릭합니다.

Products(제품)에 나열된 기존 제품 인스턴스가 있는 경우, 새 인스턴스를 프로비저닝할 것인지 아니면 기존 제품 인스턴스에 라이선스를 적용할 것인지 묻는 메시지가 표시됩니다. 예를 들어 다음 스크린샷에서는 사용자가 전체 라이선스가 있는 기존 XDR 인스턴스에 Cisco XDR 구독을 적용하기로 선택했습니다.



새 인스턴스를 생성하도록 선택하거나 라이선스를 적용할 기존 인스턴스가 없는 경우, 인스턴스를 프로비저닝할 지역과 초기 관리자의 이메일을 제공하라는 메시지가 표시됩니다.



단계 **4**

단계 **5** **Provision(**프로비저닝**)**을 클릭하여 프로비저닝 프로세스를 시작합니다.

제품이 **Overview(**개요**)** 탭의 **Products(**제품**)** 테이블에 추가됩니다.

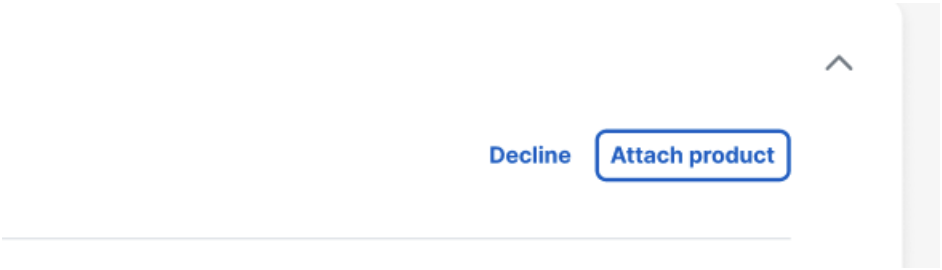
외부에서 관리되는 제품 인스턴스 첨부

Security Cloud Control 외부에서 관리되는 Cisco 제품 인스턴스가 있는 경우 선택적으로 이를 Security Cloud 엔터프라이즈에 연결할 수 있습니다. Cisco는 먼저 Security Cloud Control 관리자 목록에 이메일을 전송하여 인스턴스를 Security Cloud에 연결하라는 초대를 받습니다. 관리자는 로그인하여 Security Cloud에 외부 인스턴스를 연결할 수 있습니다. Security Cloud에 연결된 제품 인스턴스에는 제품 이름 옆에 외부에서 관리되는 레이블이 있습니다.

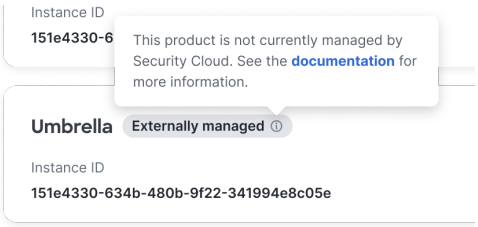
단계 **1** 보안 클라우드 제어에 로그인합니다.

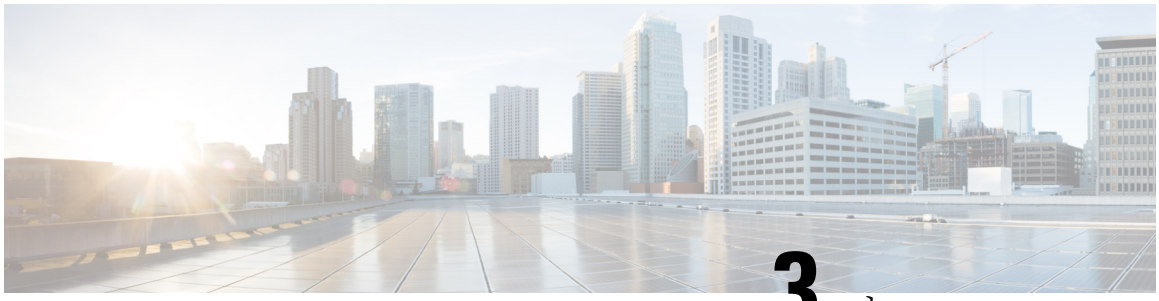
단계 **2** 엔터프라이즈를 선택하라는 프롬프트가 표시되면 외부에서 관리되는 제품 인스턴스를 첨부할 엔터프라이즈를 선택합니다.

단계 **3** 첨부할 제품 옆에 있는 **Attach Product(**제품 첨부**)**를 클릭합니다.



첨부된 제품은 외부 관리 레이블과 함께 제품 목록에 표시됩니다.





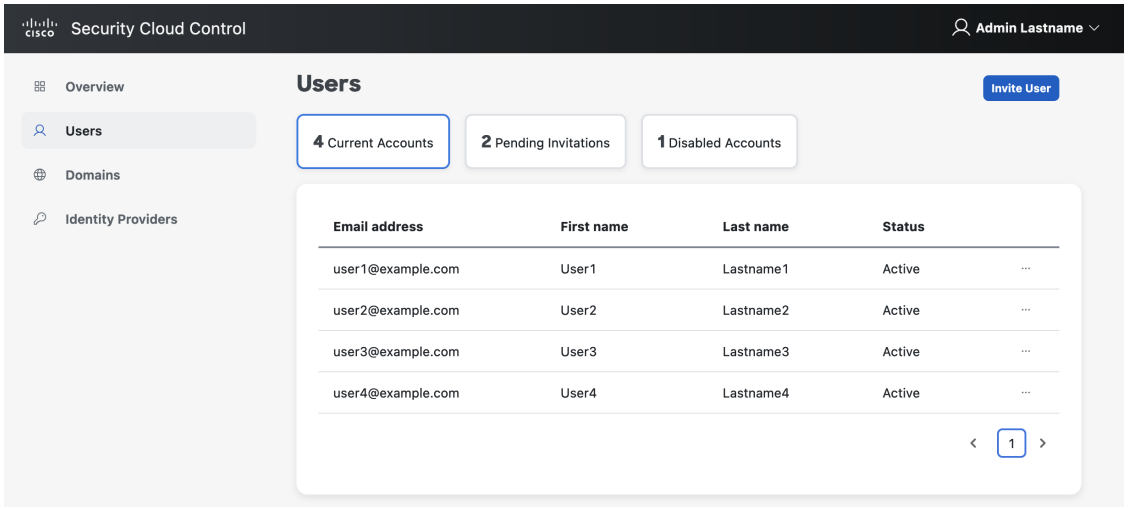
3 장

사용자 관리

사용자 나열

Users(사용자**)** 페이지는 사용자 계정에 대한 다음 보기를 제공합니다.

- **Current Accounts(**현재 계정**)**에는 엔터프라이즈에 사용자 초대 엔터프라이즈 내의 사용자가 나열됩니다.
- **Pending Invitations(**보류 중인 초대**)**에는 엔터프라이즈에 사용자 초대되었지만 아직 계정을 활성화하지 않은 사용자가 나열됩니다.
- **Disabled Accounts(**비활성화된 계정**)**에는 계정이 사용자 계정 제거 또는 비활성화 사용자의 목록이 나열됩니다.



사용자 초대

엔터프라이즈 관리자는 사용자를 엔터프라이즈에 가입하도록 초대할 수 있습니다.

단계 **1** **Users(**사용자**)** 탭을 선택합니다.

단계 **2** **Invite User(**사용자 초대**)**를 클릭합니다.

단계 **3** 사용자의 이름, 성 및 이메일을 입력합니다.

단계 **4** **Invite(**초대**)**를 클릭합니다.

초대된 사용자에게는 1시간 후에 만료되는 활성화 링크가 포함된 이메일이 전송됩니다. 아직 활성화되지 않은 초대는 **Pending Invitations(**보류 중인 초대**)**에서 볼 수 있습니다(사용자 나열, 13 페이지 참조).

참고 Security Cloud Sign On과 ID 제공자 통합 가이드한 기업의 사용자에게는 계정 활성화 이메일이 전송되지 않습니다.

사용자 편집

엔터프라이즈 관리자는 사용자의 이름과 성을 편집할 수 있습니다. 사용자의 이메일 주소는 변경할 수 없습니다.

단계 **1** 왼쪽 탐색 메뉴에서 **Users(**사용자**)**를 클릭한 다음 **Current Users(**현재 사용자**)**를 클릭합니다.

단계 **2** 메뉴 아이콘 ...을 클릭하고 **Edit(**편집**)**를 선택합니다.

단계 **3** 사용자의 이름 또는 성을 편집합니다.

단계 **4** **Update(**업데이트**)**를 클릭합니다.

사용자 비밀번호 또는 **MFA** 설정 재설정

엔터프라이즈 관리자는 도메인 클레임 및 확인에 속하는 사용자의 비밀번호 및 MFA 자격 증명을 재설정할 수 있습니다.

단계 **1** **Users(**사용자**)** 탭을 선택합니다.

단계 **2** **Current Accounts(**현재 계정**)**에서 비밀번호 또는 MFA 설정을 재설정할 사용자를 찾은 다음 아이콘 메뉴 ...를 클릭합니다.

a) 사용자 비밀번호를 재설정하려면 **Reset password(**비밀번호 재설정**)**를 선택합니다.

b) 사용자의 MFA 설정을 재설정하려면 **Reset MFA(MFA** 재설정**)**를 선택합니다.

사용자가 다음에 로그인할 때 비밀번호를 재설정하거나 Duo MFA 자격 증명을 설정하라는 메시지가 표시됩니다.

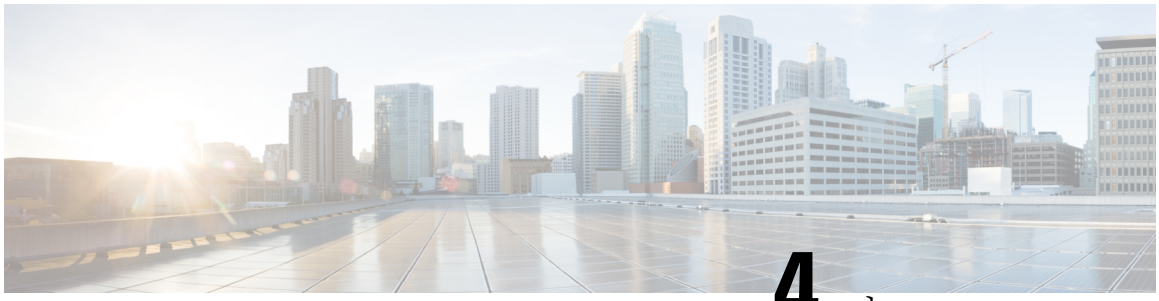
사용자 계정 제거 또는 비활성화

단계 **1** **Users(**사용자**)** 탭을 선택합니다.

단계 **2** **Current Accounts(**현재 계정**)**에서 제거하거나 비활성화할 사용자 계정을 찾은 다음 아이콘 메뉴  를 클릭합니다.

a) 엔터프라이즈에서 사용자를 제거하려면 **Remove(**제거**)**를 선택합니다.

b) 사용자 계정을 비활성화하려면 **Disable(**비활성화**)**을 선택합니다.



4 장

도메인 관리

보안 클라우드 제어에서 엔터프라이즈의 도메인 클레임 및 확인할 수 있습니다. 이는 보안 클라우드 로그인과 ID 제공자 통합 가이드하기 위한 사전 요건입니다. 또한 엔터프라이즈 관리자가 클레임된 도메인에서 사용자 비밀번호 또는 MFA 설정을 재설정할 수 있도록 하는 데 필요합니다.

도메인 클레임 및 확인

- 생성하는 DNS 레코드는 보안 클라우드 제어에서 도메인을 확인하면 삭제할 수 있습니다.
- 현재는 보안 클라우드 제어를 사용하여 단일 도메인을 확인할 수 있습니다. 여러 도메인을 확인해야 하는 경우 Cisco Technical Assistance Center(TAC)에서 케이스를 엽니다.

시작하기 전에

이 작업을 완료하려면 도메인의 등록 기관 서비스에서 DNS 레코드를 생성할 수 있어야 합니다.

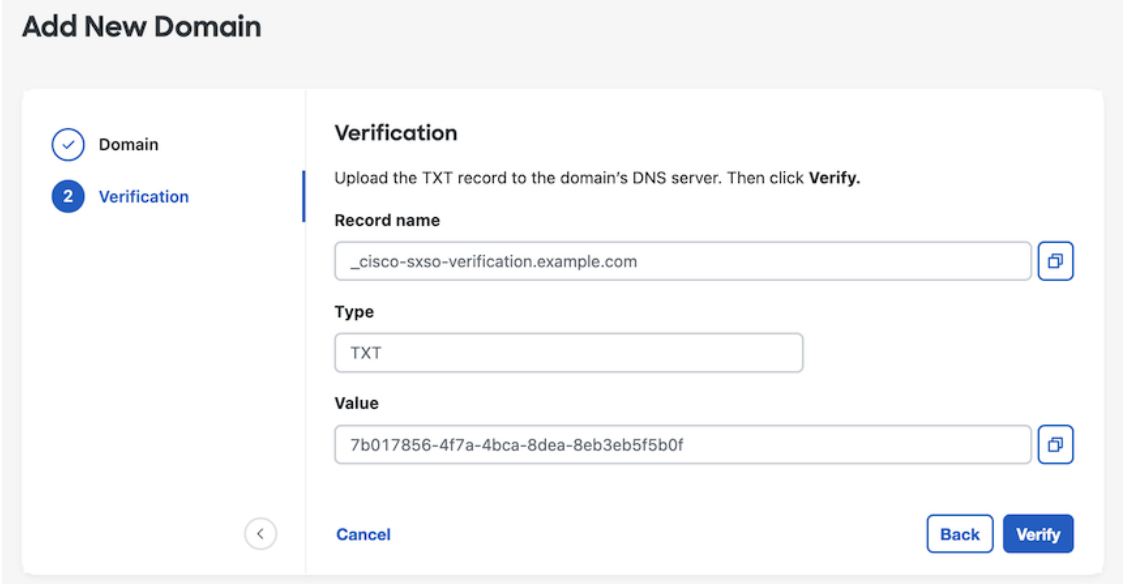
Domains(도메인**)** 탭에는 사용자가 도메인 클레임 및 확인했거나 확인 중인 도메인이 나열됩니다. 도메인을 클레임하지 않은 경우 **+ Add Domain(+** 도메인 추가**)** 버튼이 대신 표시됩니다.

단계 **1** **Domains(**도메인**)** 탭을 선택합니다.

단계 **2** **+ Add Domain(+** 도메인 추가**)**을 클릭합니다.

단계 **3** **Add New Domain(**새 도메인 추가**)** 화면에서 클레임할 도메인 이름을 입력하고 **Next(**다음**)**를 클릭합니다.

Verification(확인) 페이지에 도메인 등록 기관에서 생성해야 하는 TXT 레코드의 레코드 이름과 값이 표시됩니다.



단계 **4** 새 브라우저 탭에서 도메인 이름 등록 기관 서비스에 로그인합니다.

단계 **5** 보안 클라우드 제어에서 제공한 지정된 레코드 이름 및 값으로 새 TXT 레코드를 생성합니다.

단계 **6** 변경 사항을 저장하고 DNS 레코드가 전파될 때까지 기다립니다.

단계 **7** **Add New Domain(**새 도메인 추가**)**로 돌아가 **Verify(**확인**)**를 클릭합니다.

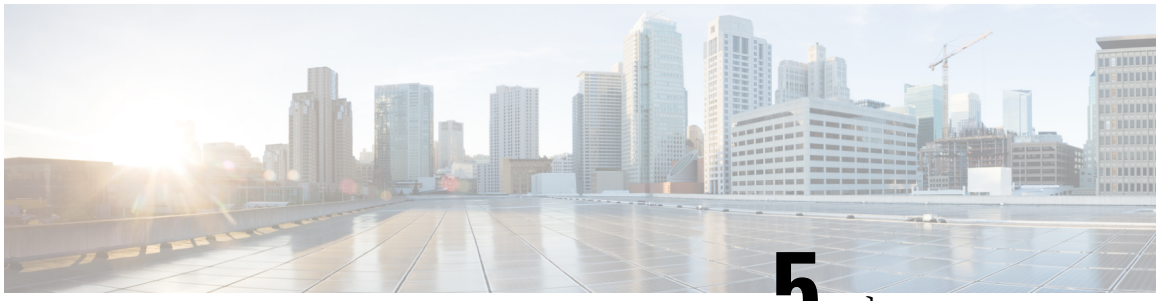
확인에 실패했음을 알리는 메시지가 나타납니다. 확인에 실패한 경우 다음을 시도해 보십시오.

- DNS 레코드가 전파될 때까지 더 기다립니다.
- 도메인 등록 기관에서 생성한 DNS 레코드의 유형, 이름, 값이 보안 클라우드 제어에서 생성한 값과 일치하는지 확인합니다.

다음에 수행할 작업

이메일 도메인을 확인했으면 다음을 수행할 수 있습니다.

- Security Cloud Sign On와 ID 제공자 통합 가이드.
- 클레임된 도메인의 사용자에 대한 사용자 비밀번호 또는 MFA 설정 재설정.



5 장

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.

- 도메인 클레임 및 확인
- 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.

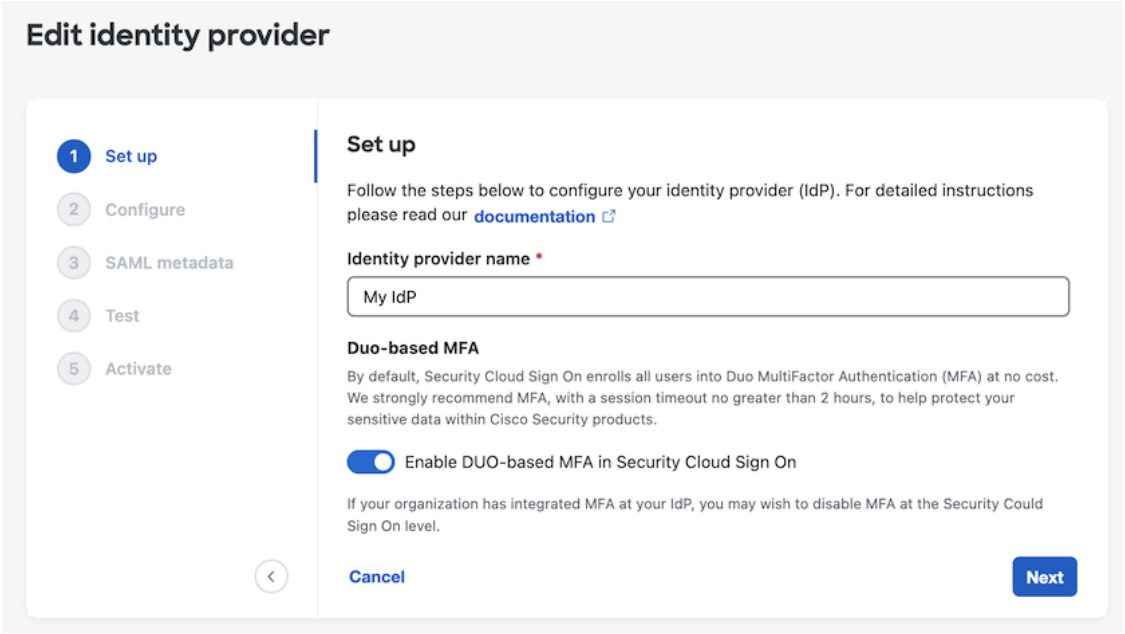
단계 **2** 왼쪽 탐색 메뉴에서 **Identity Providers(ID 제공자)**를 선택합니다.

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

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

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

단계 **5** 원하는 경우 도메인 클레임 및 확인의 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.

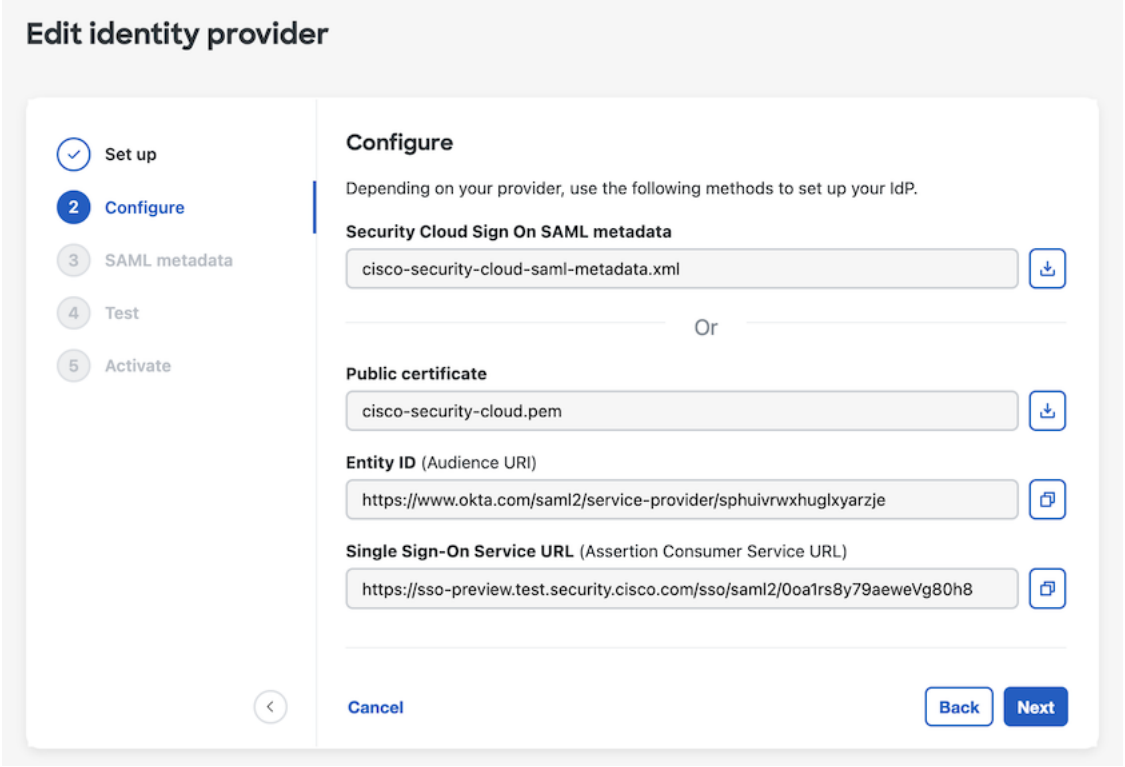
- **SSO(Single Sign-On)** 서비스 **URL** – ACS(Assertion Consumer Service) URL이라고도 하는 이 URL은 ID 제공자가 사용자를 인증한 후 SAML 응답을 전송하는 위치입니다.
- **Entity ID(**엔터티 **ID)**- 대상 URI라고도 하며 ID 제공자에게 Security Cloud Sign On를 고유하게 식별합니다.
- **Signing certificate(**서명 인증서**)** – 인증 요청에서 Security Cloud Sign On가 전송한 서명을 확인하기 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 지침, 29 페이지의 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 지침, 29 페이지의 내용을 참조하십시오.

시작하기 전에

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

- SSO(Single Sign-On) 서비스 URL

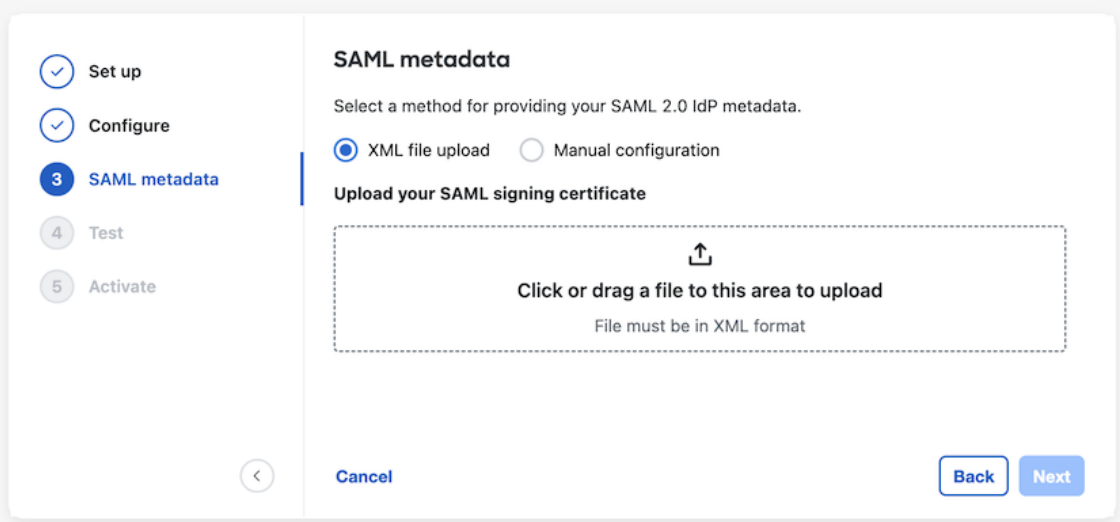
- 엔터티 ID(대상 URI)
- PEM 형식의 서명 인증서

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 지침, 29 페이지의 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.

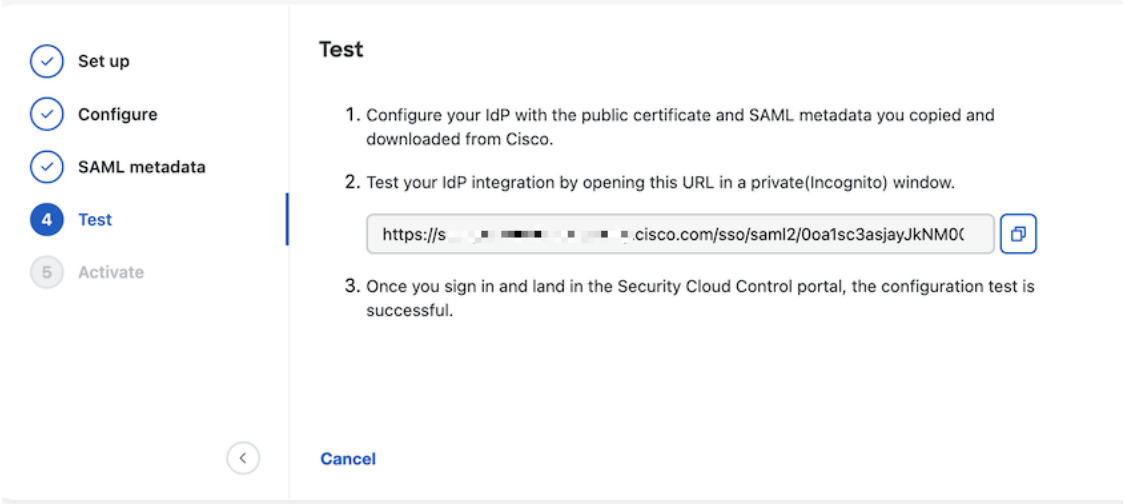
4단계: SAML 통합 테스트

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, 27 페이지의 내용을 참조하십시오.

Next(다음**)**를 클릭하여 활성화 단계로 진행합니다.

5단계: 통합 활성화

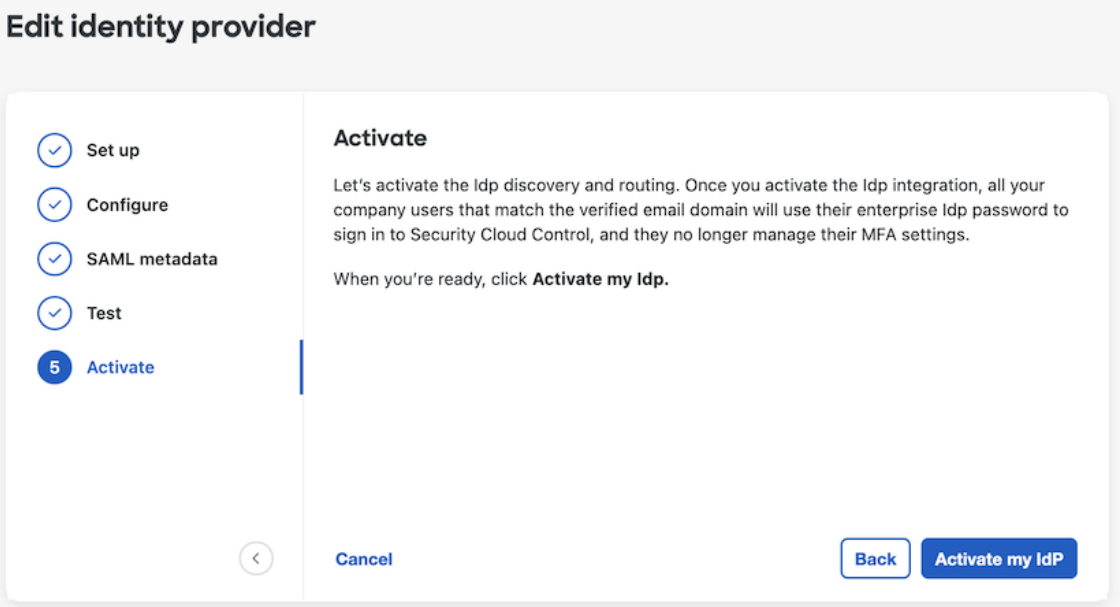
4단계: SAML 통합 테스트 후에는 활성화할 수 있습니다. 통합을 활성화하면 다음과 같은 효과가 있습니다.

- 확인된 도메인의 사용자는 반드시 통합 ID 제공자를 사용하여 인증해야 합니다. 사용자가 Cisco 또는 Microsoft 소셜 로그인 옵션을 사용하여 로그인하려고 하면 400 오류가 발생합니다.
- 도메인 클레임 및 확인과 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 도메인 클레임 및 확인과 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**.**

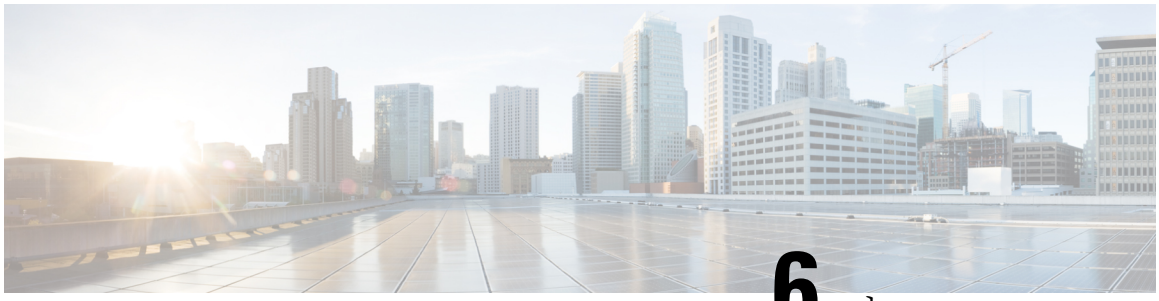
SAML 응답에 포함된 `<NameId>` 요소의 값은 이메일 주소여야 합니다. 이메일 주소는 사용자의 SAML 속성에 지정된 이메일과 일치해야 합니다. 자세한 내용은 SAML 응답 요구 사항, 20 페이지를 참조하십시오.

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, 20 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.



6 장

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 가이드, 19 페이지의 내용을 읽고 전체 프로세스를 파악하십시오. 이 지침은 Auth0 SAML 통합 관련 세부 사항, 그중에서도 2단계: ID 제공자에 보안 클라우드 SAML 메타데이터 제공, 23 페이지 및 3단계: IdP에서 보안 클라우드로 SAML 메타데이터 제공, 24 페이지를 사용하여 해당 가이드를 보완합니다.

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

a) 1단계: 초기 설정, 22 페이지의 설명에 따라 새 ID 제공자를 생성하고 Duo MFA의 옵트아웃 여부를 결정합니다.

b) 2단계: ID 제공자에 보안 클라우드 SAML 메타데이터 제공, 23 페이지에서 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.

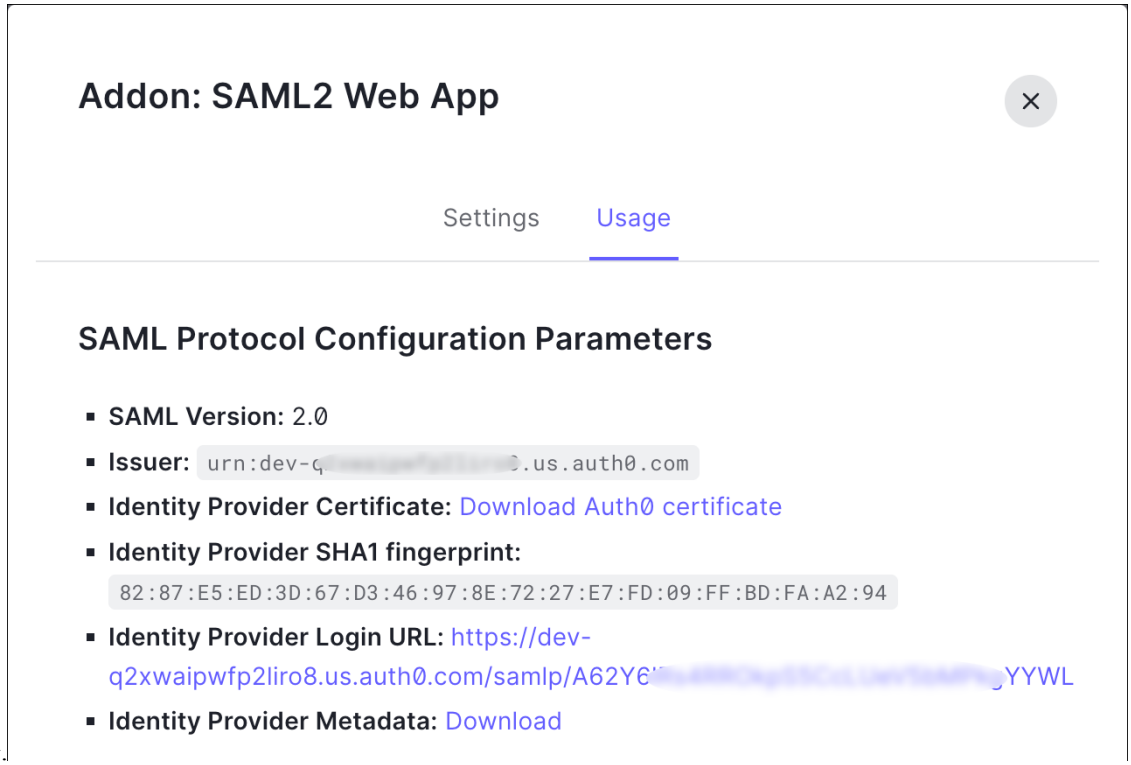
b) **Create Application(**애플리케이션 생성**)**을 클릭합니다.

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.

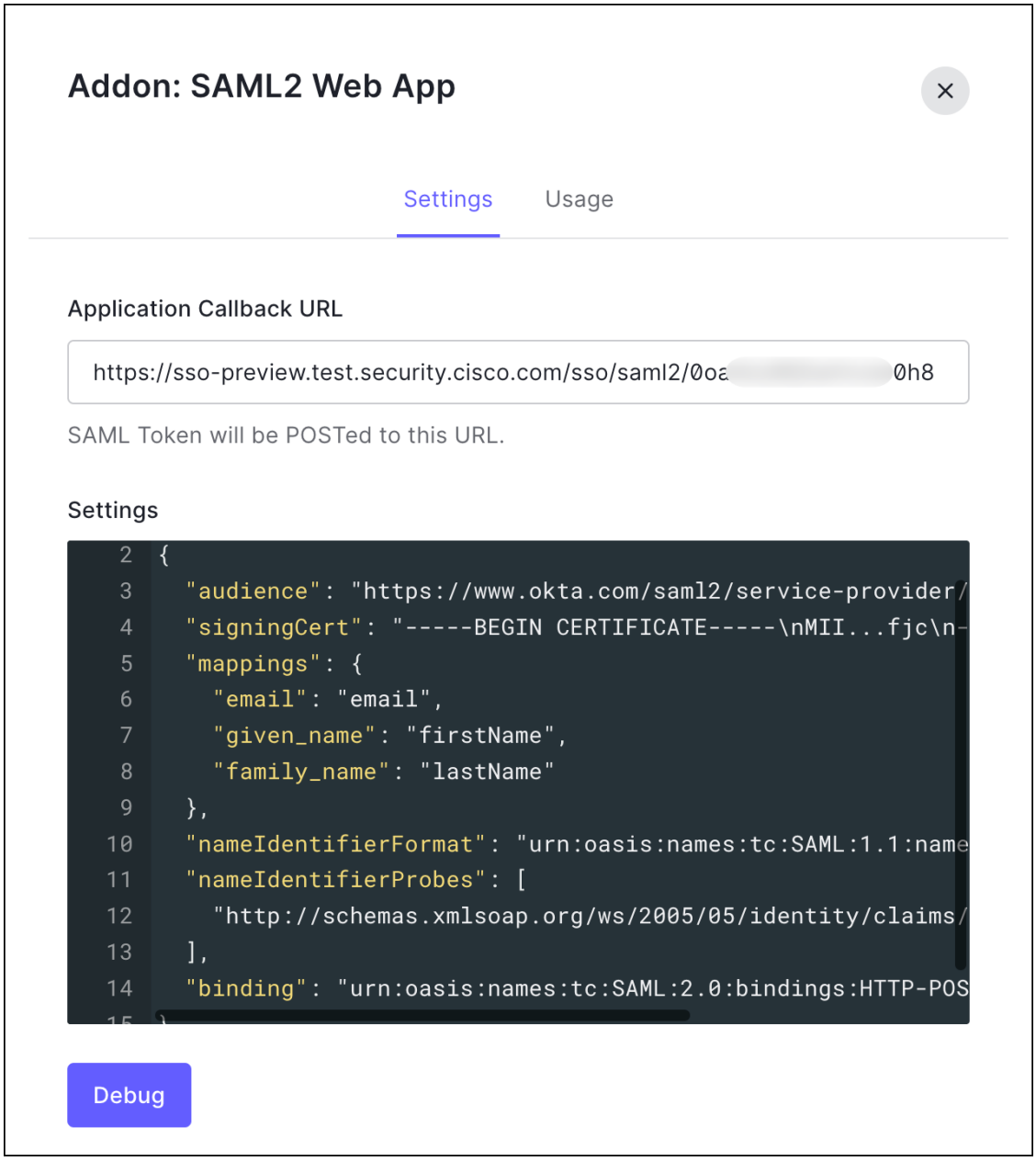
h) **Settings(**설정**)** 탭을 클릭합니다.

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 제공, 24 페이지에 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, 25 페이지 및 5단계: 통합 활성화, 26 페이지의 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 가이드, 19 페이지의 내용을 읽고 전체 프로세스를 파악하십시오. 이 지침은 Azure AD SAML 통합 관련 세부 사항, 그중에서도 2단계: ID 제공자에 보안 클라우드 SAML 메타데이터 제공, 23 페이지 및 3단계: IdP에서 보안 클라우드로 SAML 메타데이터 제공, 24 페이지를 사용하여 해당 가이드를 보완합니다.

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

a) 1단계: 초기 설정, 22 페이지의 설명에 따라 새 ID 제공자를 생성하고 Duo MFA의 옵트아웃 여부를 결정합니다.
b) 2단계: ID 제공자에 보안 클라우드 SAML 메타데이터 제공, 23 페이지에서 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.

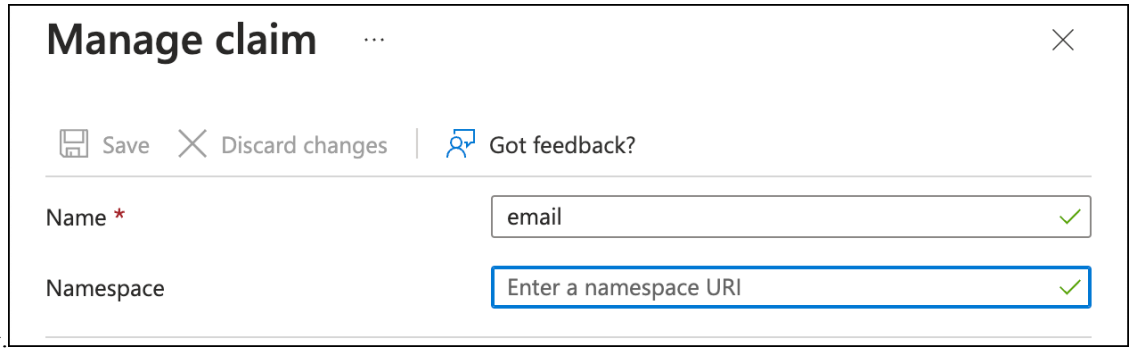
i) **Attributes and Claims(**속성 및 클레임**)** 패널에서 **Edit(**편집**)**를 클릭합니다.

- **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 제공, 24 페이지에 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, 25 페이지 및 5단계: 통합 활성화, 26 페이지에 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 가이드, 19 페이지의 내용을 읽고 전체 프로세스를 파악하십시오. 이 지침은 Duo SAML 통합 관련 세부 사항, 그중에서도 2단계: ID 제공자에 보안 클라우드 SAML 메타데이터 제공, 23 페이지 및 3단계: IdP에서 보안 클라우드로 SAML 메타데이터 제공, 24 페이지를 사용하여 해당 가이드를 보완합니다.

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

a) 1단계: 초기 설정, 22 페이지의 설명에 따라 새 ID 제공자를 생성하고 Duo MFA의 옵트아웃 여부를 결정합니다.

b) 2단계: ID 제공자에 보안 클라우드 SAML 메타데이터 제공, 23 페이지에서 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.

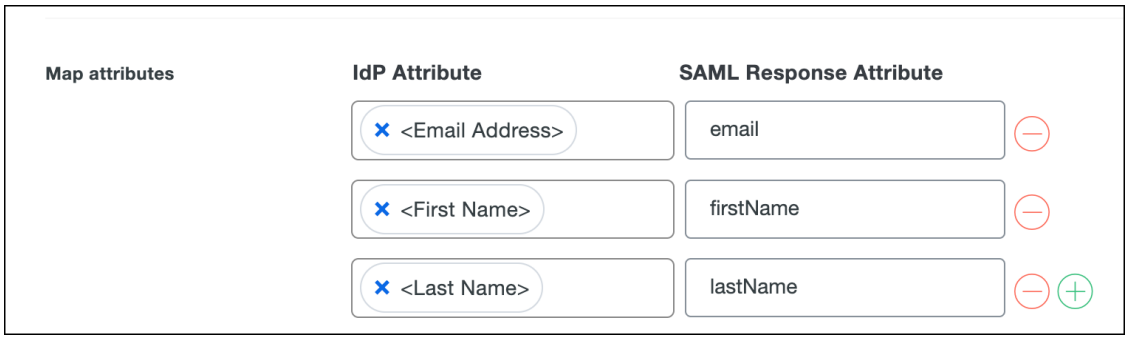
f) **SSO(Single Sign-On) URL**의 값을 복사하고 나중에 사용할 수 있도록 저장합니다.

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**
<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 제공, 24 페이지에 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, 25 페이지 및 5단계: 통합 활성화, 26 페이지의 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 가이드, 19 페이지의 내용을 읽고 전체 프로세스를 파악하십시오. 이 지침은 Google Identity 통합 관련 세부 사항, 그중에서도 2단계: ID 제공자에 보안 클라우드 SAML 메타데이터 제공, 23 페이지 및 3단계: IdP에서 보안 클라우드로 SAML 메타데이터 제공, 24 페이지를 사용하여 해당 가이드를 보완합니다.

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

a) 1단계: 초기 설정, 22 페이지의 설명에 따라 새 ID 제공자를 생성하고 Duo MFA의 옵트아웃 여부를 결정합니다.

b) 2단계: ID 제공자에 보안 클라우드 SAML 메타데이터 제공, 23 페이지에서 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.

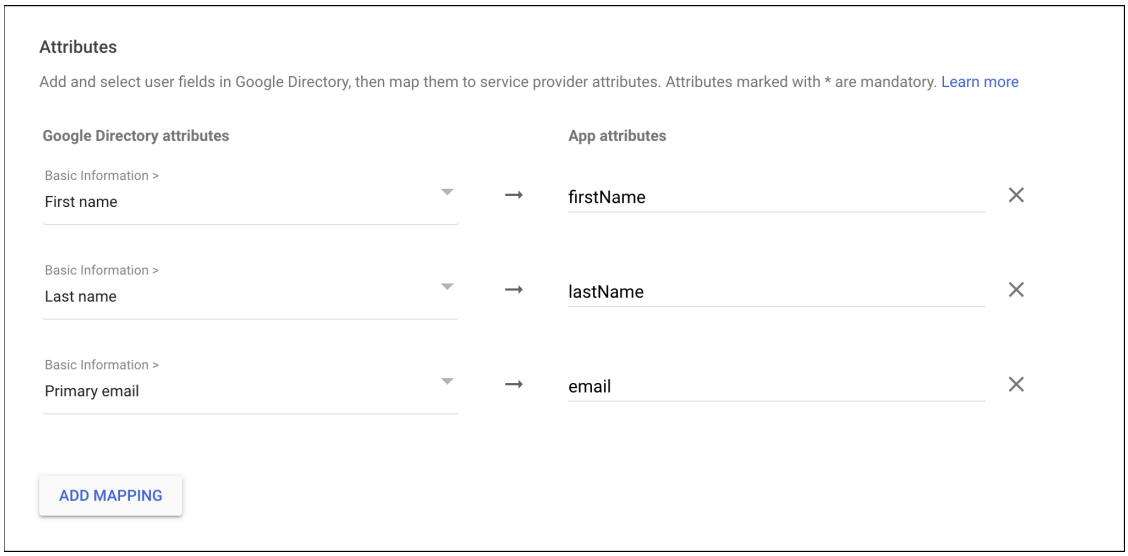
j) **Name ID Format(이름 ID 형식)**에 대해 `UNSPECIFIED` 또는 `EMAIL`을 선택합니다.

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 제공, 24 페이지에 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, 25 페이지 및 5단계: 통합 활성화, 26 페이지의 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 가이드, 19 페이지의 내용을 읽고 전체 프로세스를 파악하십시오. 이 지침은 Okta SAML 통합 관련 세부 사항, 그중에서도 2단계: ID 제공자에 보안 클라우드 SAML 메타데이터 제공, 23 페이지 및 3단계: IdP에서 보안 클라우드로 SAML 메타데이터 제공, 24 페이지를 사용하여 해당 가이드를 보완합니다.

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

a) 1단계: 초기 설정, 22 페이지의 설명에 따라 새 ID 제공자를 생성하고 Duo MFA의 옵트아웃 여부를 결정합니다.

b) 2단계: ID 제공자에 보안 클라우드 SAML 메타데이터 제공, 23 페이지에서 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.email

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 제공, 24 페이지에 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, 25 페이지 및 5단계: 통합 활성화, 26 페이지의 지침에 따라 통합을 테스트하고 활성화합니다.

Ping 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 가이드, 19 페이지의 내용을 읽고 전체 프로세스를 파악하십시오. 이 지침은 Google Identity 통합 관련 세부 사항, 그중에서도 2단계: ID 제공자에 보안 클라우드 SAML 메타데이터 제공, 23 페이지 및 3단계: IdP에서 보안 클라우드로 SAML 메타데이터 제공, 24 페이지를 사용하여 해당 가이드를 보완합니다.

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

a) 1단계: 초기 설정, 22 페이지의 설명에 따라 새 ID 제공자를 생성하고 Duo MFA의 옵트아웃 여부를 결정합니다.

b) 2단계: ID 제공자에 보안 클라우드 SAML 메타데이터 제공, 23 페이지에서 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.

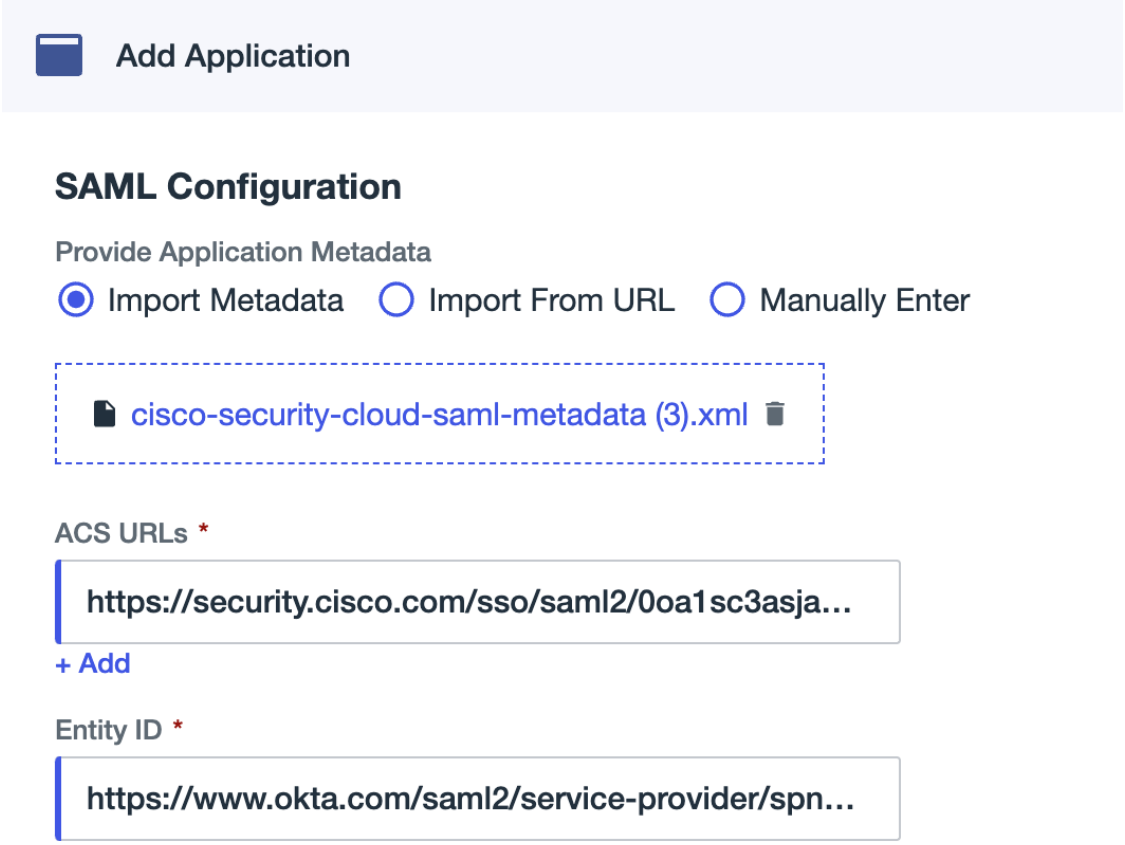
c) **Application Name(**애플리케이션 이름**)** 필드에 **`Secure Cloud Sign On`** 또는 다른 이름을 입력합니다.

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.

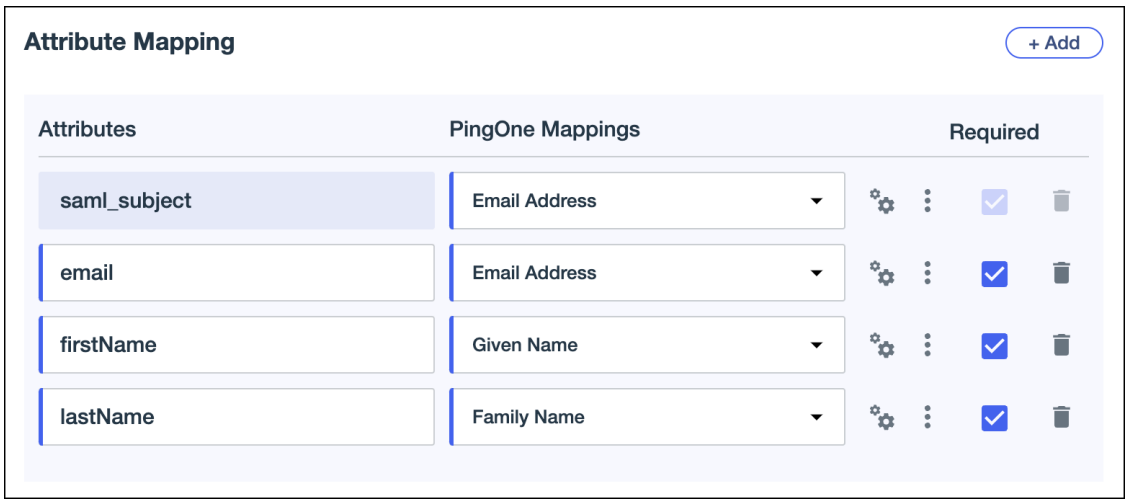
l) 편집(연필) 아이콘을 클릭합니다.

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 제공, 24 페이지에 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, 25 페이지 및 5단계: 통합 활성화, 26 페이지의 지침에 따라 통합을 테스트하고 활성화합니다.