ID 공급자 통합

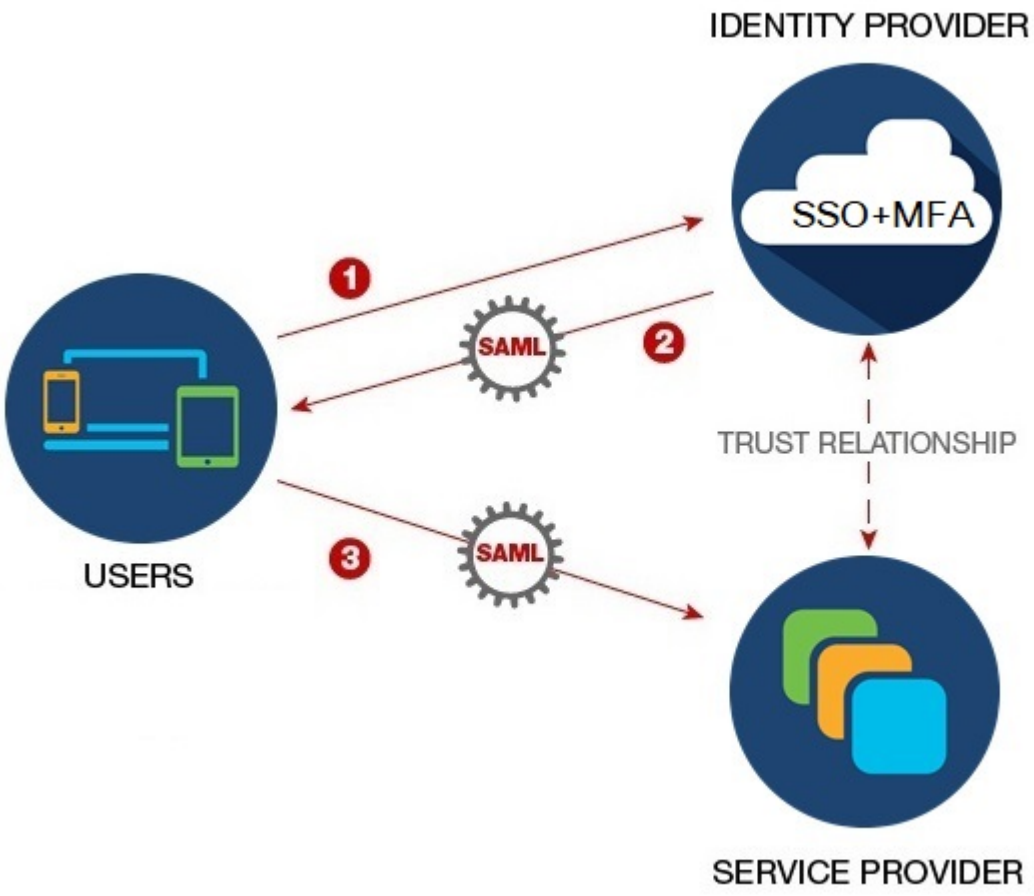
중요 **Enterprise Manager**가 사용이 중지되었습니다. 이제 보안 클라우드 제어 를 사용하여 ID 공급자 통합을 관리할 수 있습니다. 자세한 내용은 ID 공급자 통합 가이드를 참조하십시오.

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

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

니

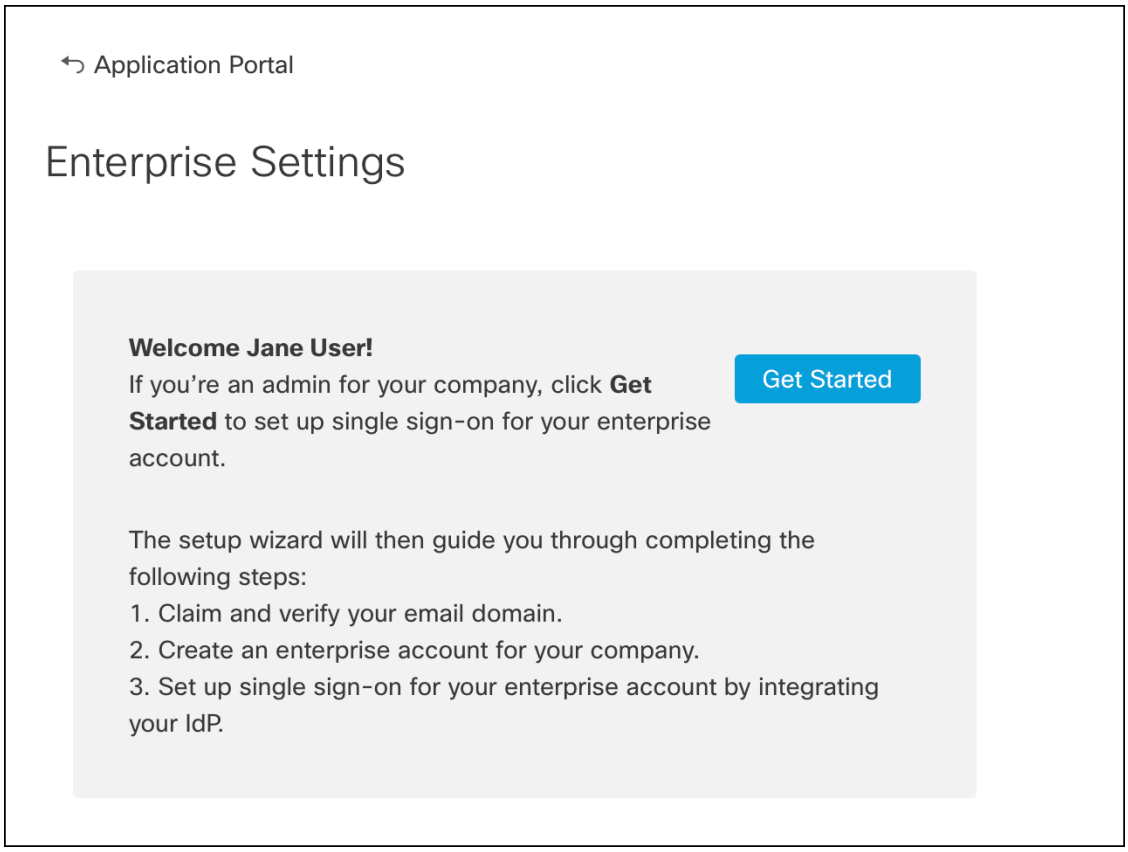


기본적으로 Security Cloud Sign On은(는) 모든 IdP의 사용자를 무료로 Duo 다단계 인증(MFA)에 등록합니다. 조직에서 이미 IdP와 MFA를 통합한 경우 통합 프로세스 중에 Duo 기반 MFA를 선택적으로 비활성화할 수 있습니다.

엔터프라이즈 설정 마법사

엔터프라이즈 설정 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 확인한 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 고객를 참조하십시오.

1단계: 엔터프라이즈 생성

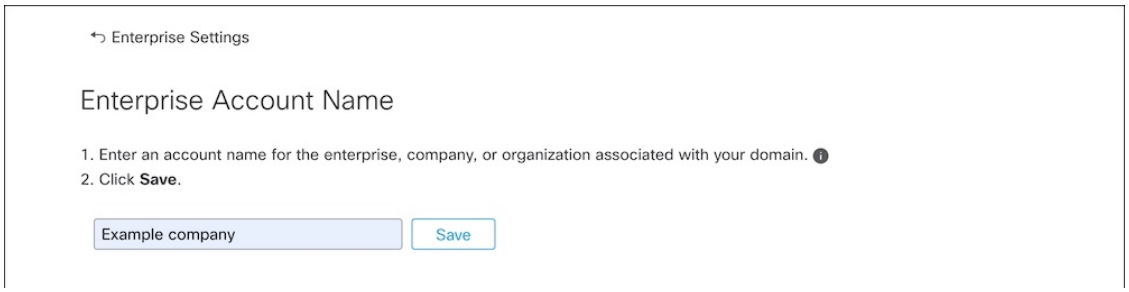
첫 번째 단계는 Security Cloud Sign On에서 명명된 엔터프라이즈를 생성하는 것입니다. 이 엔터프라이즈는 클레임된 도메인 및 ID 공급자 설정과 연결됩니다.

단계 **1** Security Cloud Sign On 계정을 사용하여 SecureX 애플리케이션 포털 에 로그인합니다.

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.

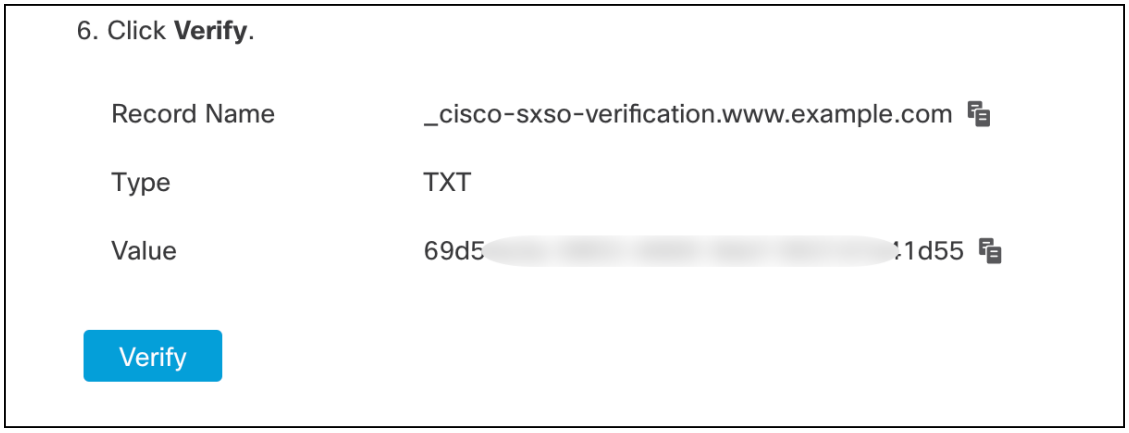


2단계: 이메일 도메인 클레임 및 확인

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.

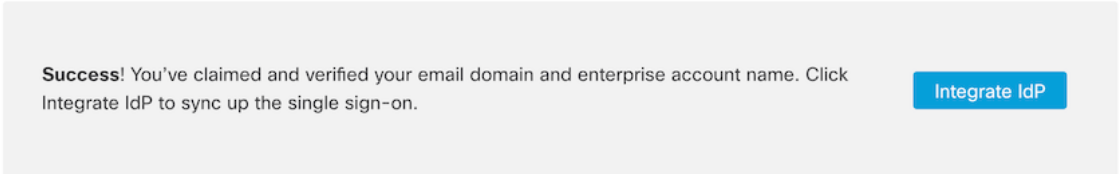
설정 마법사에 DNS TXT 레코드 이름 및 값이 표시됩니다.



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.



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 SAML 통합에 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. `IdP` 의 SAML 메타데이터에서 `<EntityDescriptor>` 요소를 비활성화합니다. 일부 IdP는 **ID** 공급자 발급자라고도 합니다.
- **SAML** 서명 인증서 – IdP가 SAML 어설션에 서명하는 데 사용하는 x.509 서명 인증서입니다.

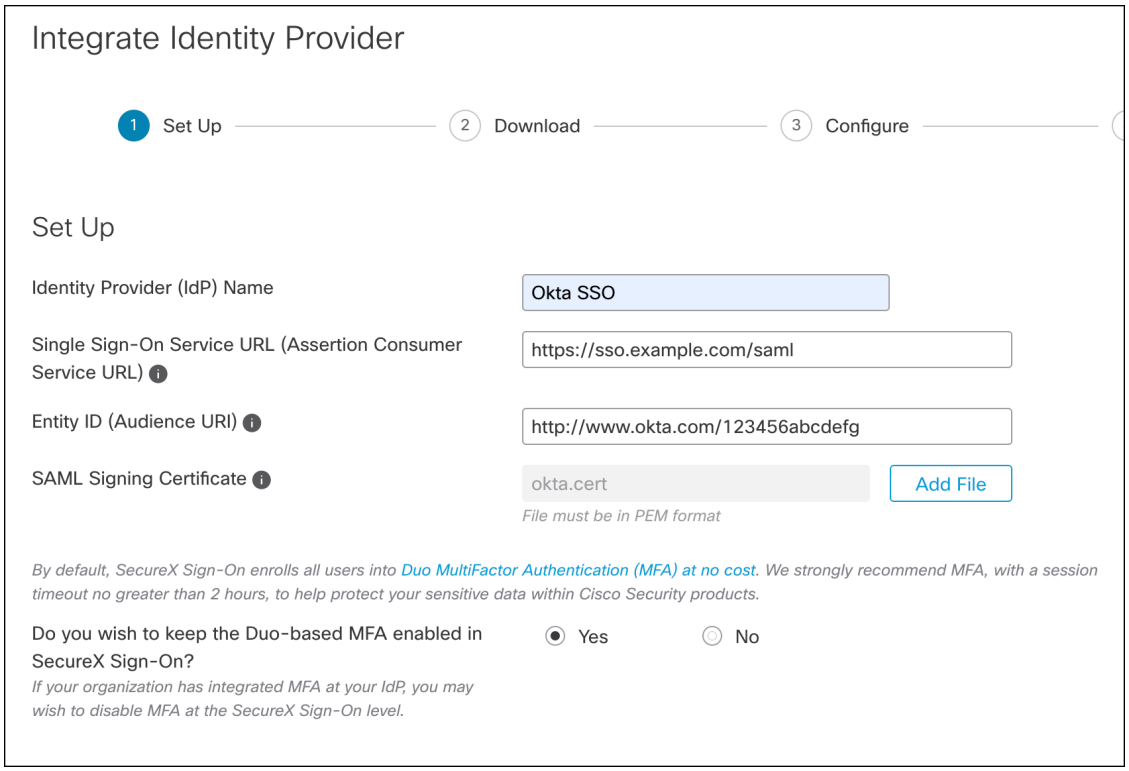
참고 인증서는 SHA-256 알고리즘으로 서명해야 합니다. 다른 알고리즘으로 서명된 어설션은 HTTP 400 오류로 인해 거부됩니다.

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.

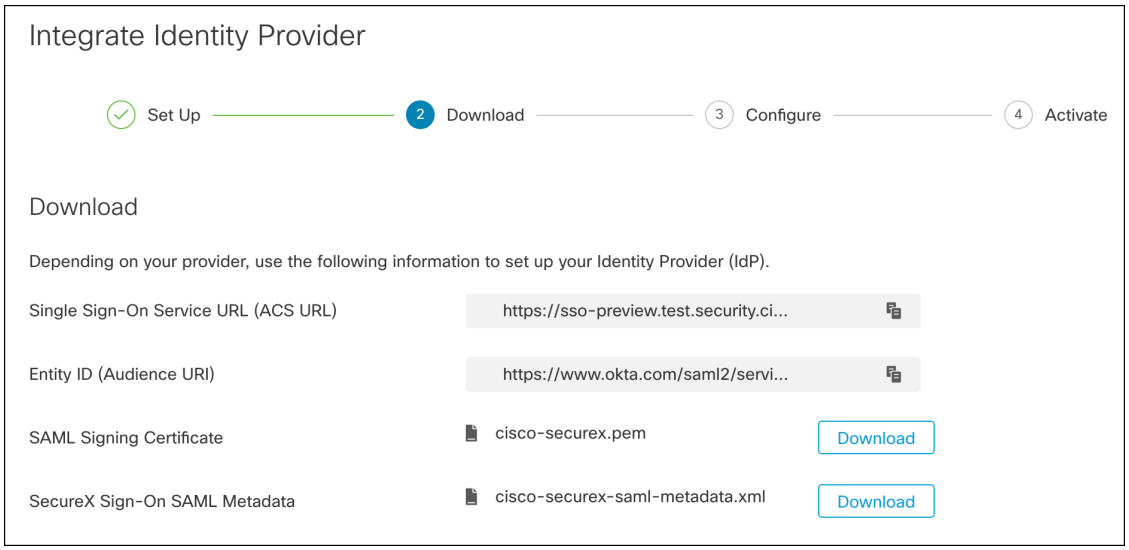
단계 **3** **Add File(파일 추가)**을 클릭하고 이전에 IdP에서 다운로드한 SAML 서명 인증서를 선택합니다.

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 **MFA**를 계속 사용하시겠습니까**?)**에 **No(**아니요**)**를 선택하면 됩니다.



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.



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

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

a) **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:Auth0)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.

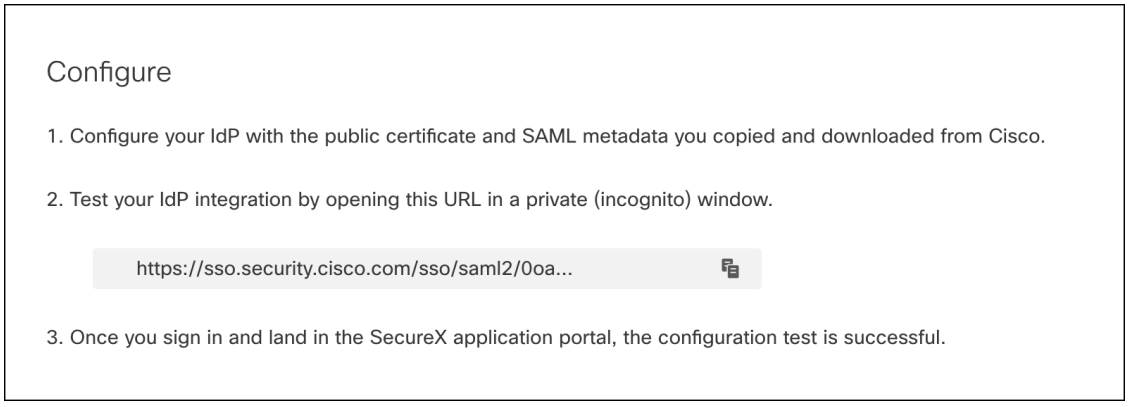
4단계: SSO 통합 테스트

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 확인과 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.



단계 **3** ID 제공자로 로그인합니다.

- 로그인에 사용된 이메일 도메인은 이전에 클레임한 2단계: 이메일 도메인 클레임 및 확인과 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 해결의 내용을 참조하십시오.

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

5단계: IdP 통합 활성화

4단계: SSO 통합 테스트하고 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.