DMP에 대한 Microsoft Entra ID SSO 외부 인증 구성

목차

소개

이 문서에서는 Cisco Domain Protection 포털을 인증하도록 Microsoft Entra ID Single Sign-On을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대해 알고 있는 것이 좋습니다.

- Cisco 도메인 보호
- Microsoft Entra ID
- PEM 형식의 자체 서명 또는 CA 서명(선택 사항) X.509 SSL 인증서

사용되는 구성 요소

- Cisco Domain Protection 관리자 액세스
- Microsoft Entra ID 관리 센터 관리자 액세스

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

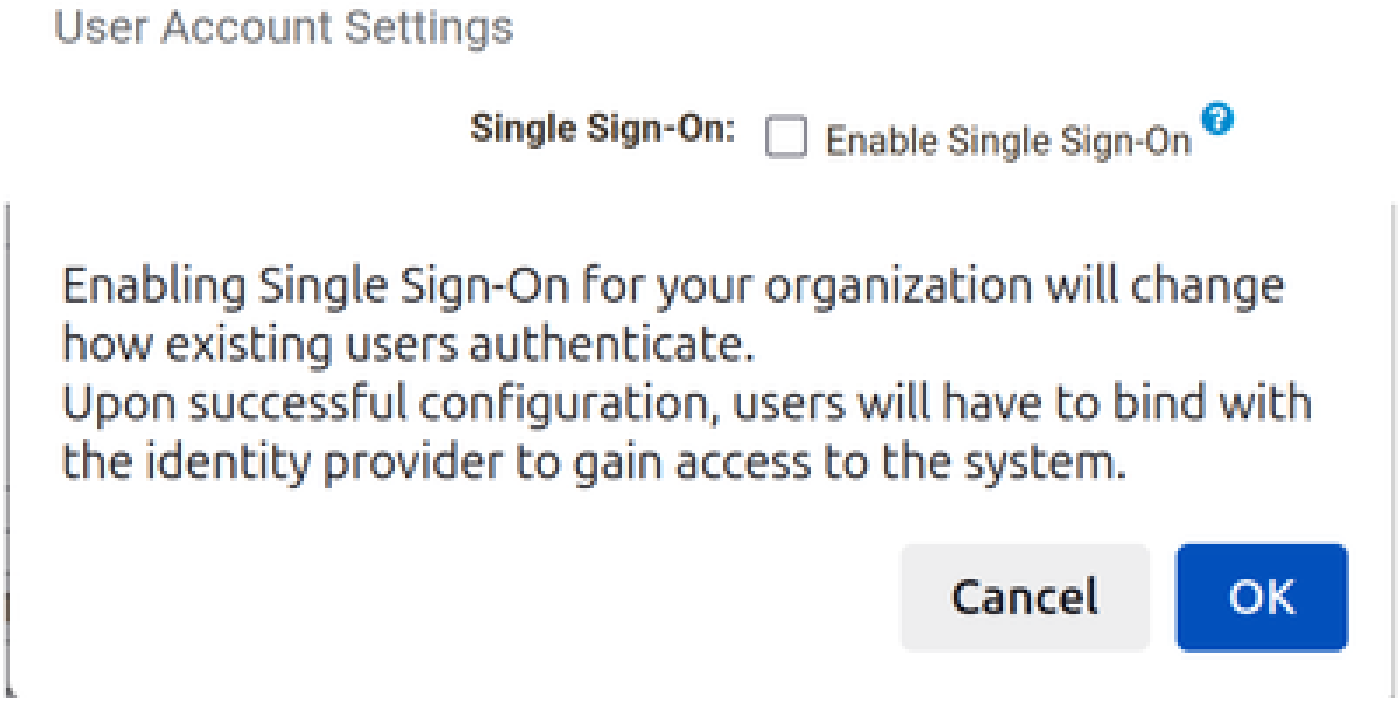
- Cisco Domain Protection은 SAML 2.0 프로토콜을 통해 최종 사용자를 위한 SSO 로그인을 활성화합니다.
- Microsoft Entra SSO는 SSO(Single Sign-On)를 통해 어디서나 SaaS(Software as a Service) 앱, 클라우드 앱 또는 온프레미스 앱에 대한 액세스를 허용하고 제어합니다.
- Cisco Domain Protection은 Microsoft Entra에 연결된 ID 관리 애플리케이션으로 설정할 수 있으며, 비밀번호 전용 인증은 안전하지 않으며 권장되지 않으므로 다단계 인증이 포함된 인증 방법을 사용합니다.
- SAML은 관리자가 정의된 애플리케이션 중 하나에 로그인한 후 해당 애플리케이션에 원활하게 액세스할 수 있도록 하는 XML 기반 개방형 표준 데이터 형식입니다.
- SAML에 대한 자세한 내용은 다음을 참조하십시오. SAML이란 무엇입니까?

구성

Cisco 도메인 보호(1부)

1. Cisco Domain Protection 관리 포털에 로그인하고 Admin(관리) > Organization(조직)으로 이동합니다. 이미지에 표시된 대로 Edit Organization Details(조직 세부 정보 수정) 버튼을 클릭합니다.

2. 사용자 계정 설정 섹션으로 이동하여 단일 로그인 사용 확인란을 클릭합니다. 이미지에 표시된 것처럼 메시지가 나타납니다.

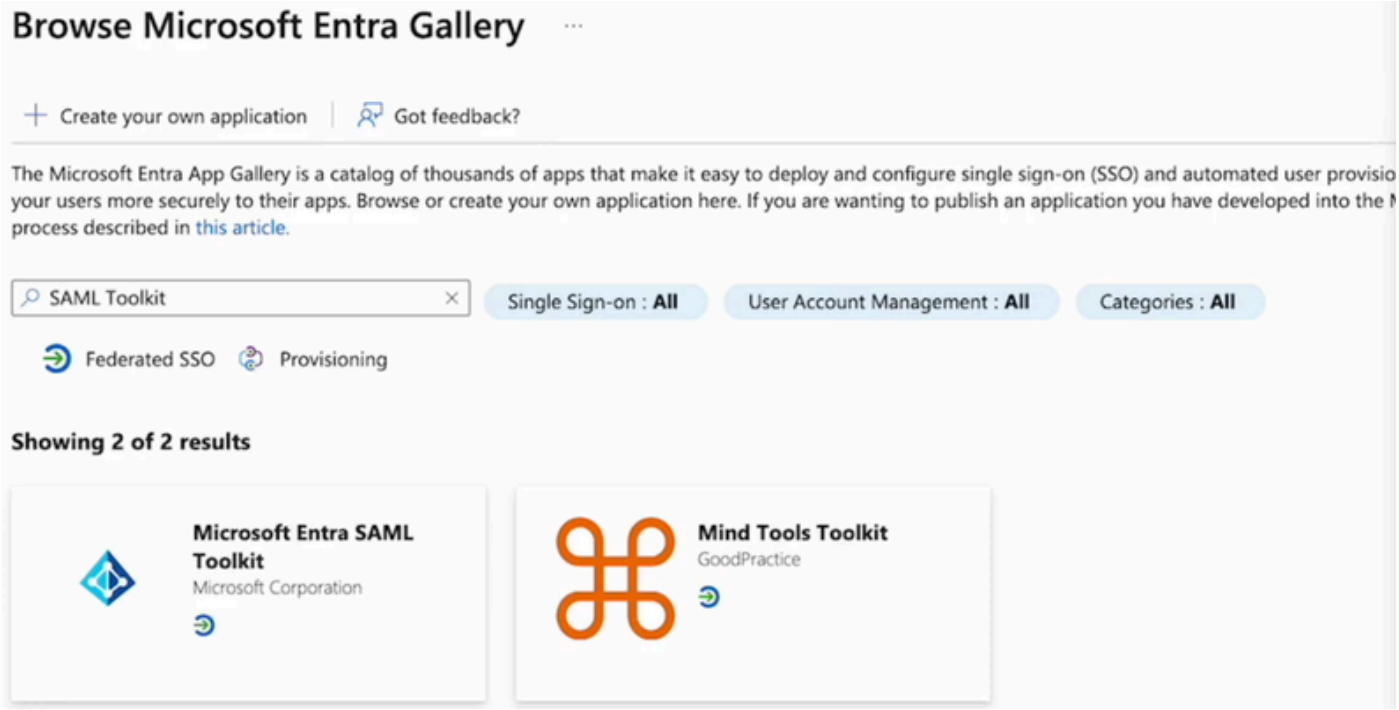


3. 확인 버튼을 클릭하고 엔티티 ID 및 Assertion Consumer Service(ACS) URL 매개변수를 복사합니다. 이러한 매개변수는 Microsoft Entra ID Basic SAML 인증에 사용해야 합니다. 나중에 Name Identifier Format(이름 식별자 형식), SAML 2.0 Endpoint(SAML 2.0 엔드포인트) 및 Public Certificate(퍼블릭 인증서) 매개변수를 설정하기 위해 돌아갑니다.

- 엔터티 ID: dmp.cisco.com
- 어설션 소비자 서비스 URL: https://<dmp_id>.dmp.cisco.com/auth/saml/callback

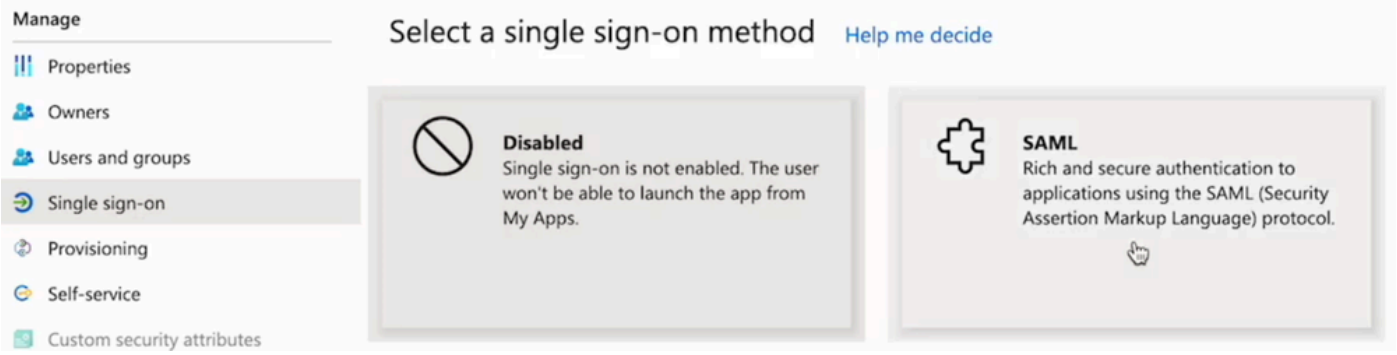
Microsoft Entra ID

1. Microsoft Entra ID 관리 센터로 이동하고 추가 버튼을 클릭합니다. Enterprise Application을 선택하고 이미지와 같이 Microsoft Entra SAML 툴킷을 검색합니다.



2. 의미 있는 값으로 이름을 지정하고 생성을 클릭합니다. 예: Domain Protection Sign On.

3. 왼쪽 패널의 관리 섹션으로 이동합니다. Single sign-on을 클릭하고 SAML을 선택합니다.



4. Basic SAML Configuration(기본 SAML 컨피그레이션) 패널에서 Edit(편집)를 클릭하고 매개변수를 입력합니다.

- 식별자(엔터티 ID): dmp.cisco.com

- 회신 URL(Assertion Consumer Service URL): https://<dmp_id>.dmp.cisco.com/auth/saml/callback
- 로그온 URL: https://<dmp_id>.dmp.cisco.com/auth/saml/callback
- 저장을 클릭합니다.

5. [속성 및 클레임] 패널에서 [편집]을 클릭합니다.

Required claim(필수 클레임)에서 Unique User Identifier(Name ID) 클레임을 클릭하여 수정합니다.

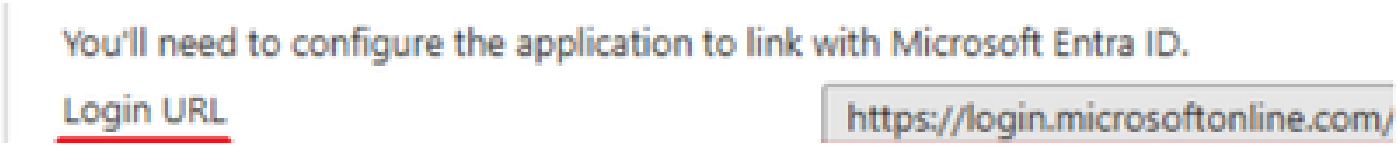
- Source 특성 필드를 user.userprincipalname으로 설정합니다. user.userprincipalname 값이 유효한 이메일 주소를 나타낸다고 가정합니다. 그렇지 않은 경우 Source를 user.primaryauthoritativeemail로 설정합니다.
- Additional Claims(추가 클레임) 패널에서 Edit(편집)를 클릭하고 Microsoft Entra ID 사용자 속성과 SAML 특성 간의 매핑을 생성합니다.

이름	네임스페이스	소스 특성
이메일 주소	값 없음	user.userprincipalname
이름	값 없음	user.givenname
성	값 없음	user.surname

아래 그림과 같이 각 클레임에 대한 네임스페이스 필드를 지워야 합니다.

6. Attributes & Claims 섹션이 채워지면 마지막 섹션인 SAML Signing Certificate가 채워집니다.

- 로그인 URL을 저장합니다.



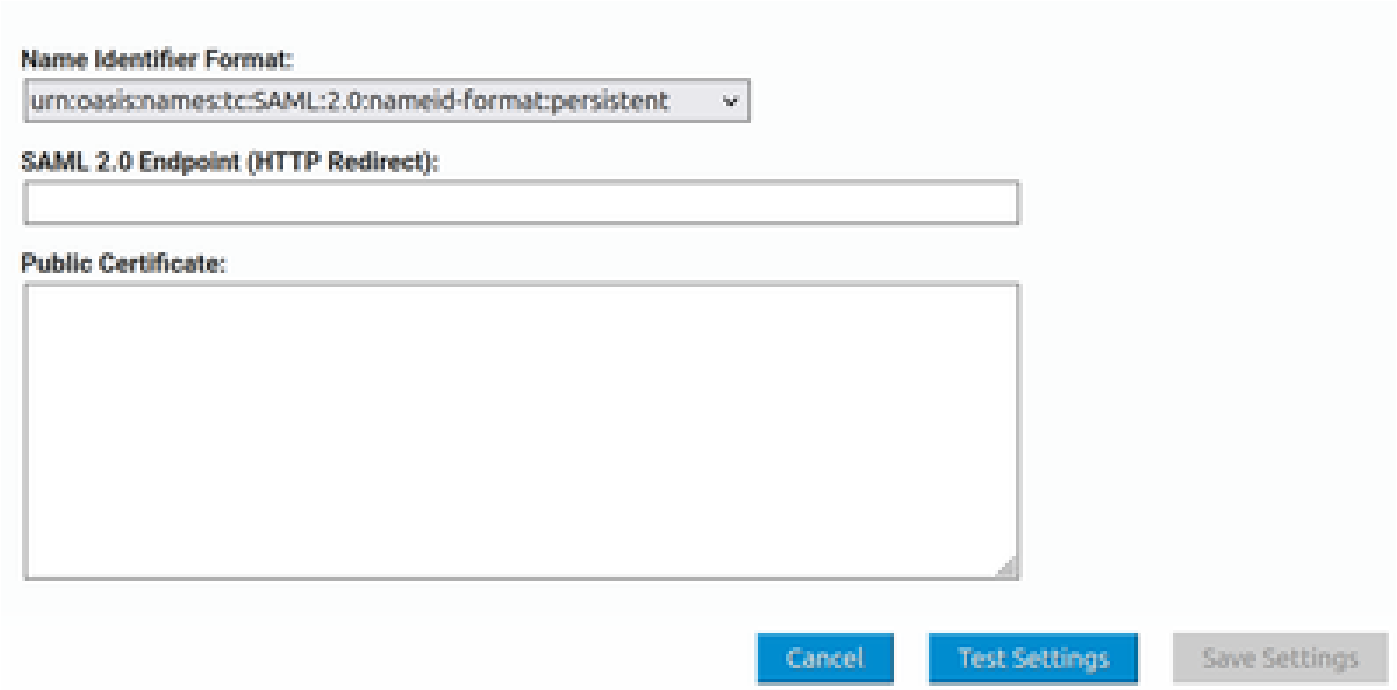
- 인증서를 저장합니다(Base64).

Cisco 도메인 보호(2부)

Cisco Domain Protection(Cisco 도메인 보호) > Enable Single Sign-On(단일 로그인 활성화) 섹션으로 돌아갑니다.

- 이름 식별자 형식: urn:oasis:names:tc:SAML:2.0:nameid-format:persistent

- SAML 2.0 엔드포인트(HTTP 리디렉션): Microsoft Entra ID에서 제공하는 로그인 URL
- 공용 인증서: Microsoft Entra ID에서 제공하는 인증서(Base64)



다음을 확인합니다.

테스트 설정을 누릅니다. 그러면 ID 공급자의 로그인 페이지로 리디렉션됩니다. SSO 자격 증명을 사용하여 로그인합니다.

로그인에 성공하면 창을 닫을 수 있습니다. Save Settings(설정 저장)를 클릭합니다.

문제 해결

```
Error - Error parsing X509 certificate
```

- 인증서가 Base64에 있는지 확인합니다.

```
Error - Please enter a valid URL
```

- Microsoft Entra ID에서 제공한 로그인 URL이 올바른지 확인합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.