CRES에 대한 Microsoft Entra ID SSO 외부 인증 구성

목차

소개

이 문서에서는 Cisco Secure Email Encryption Service에 인증하기 위해 Microsoft Entra ID Single Sign-on을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Secure Email Encryption Service(등록된 봉투)
- Microsoft Entra ID
- PEM 형식의 자체 서명 또는 CA 서명(선택 사항) X.509 SSL 인증서

사용되는 구성 요소

- Secure Email Encryption Service(Registered Envelope) 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.

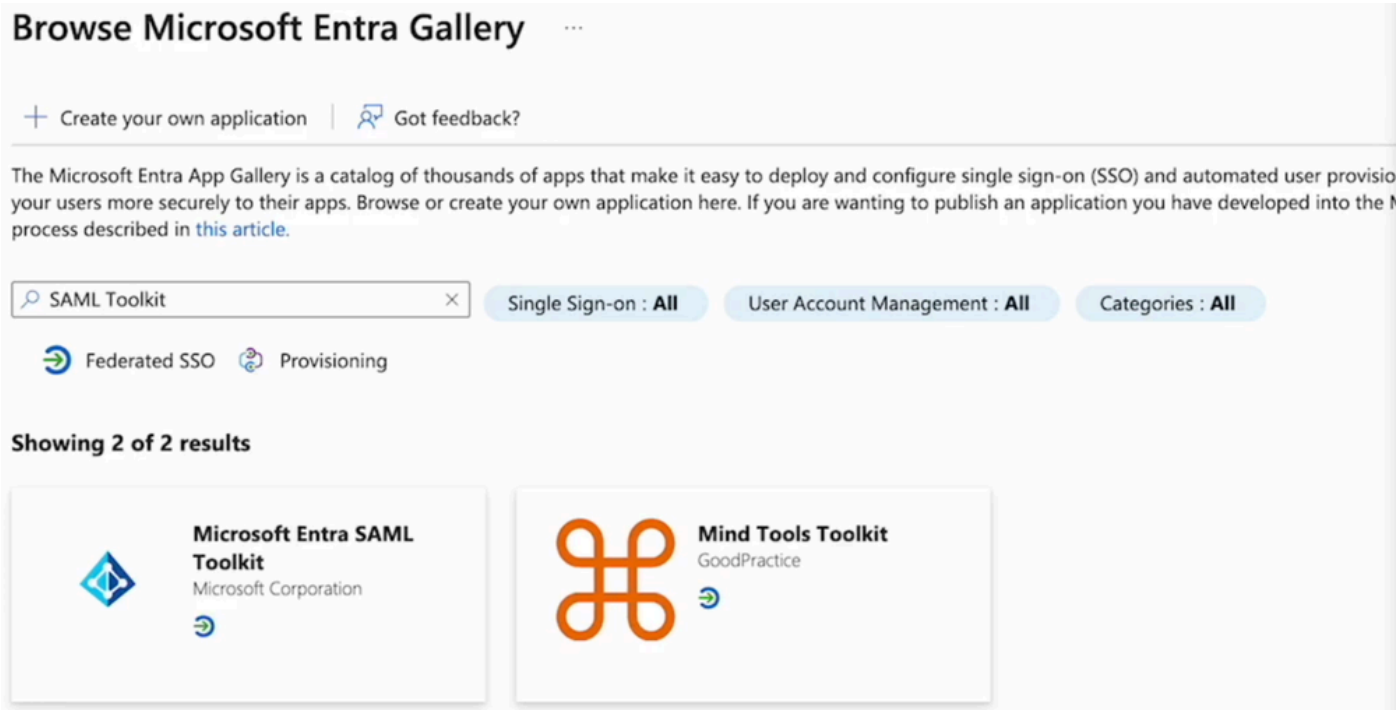
배경 정보

- Registered Envelope(등록된 봉투)은 SAML을 사용하는 최종 사용자에 대해 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.
- Registered Envelope(등록된 봉투)은 Microsoft Entra에 연결된 관리되는 ID 애플리케이션으로 설정할 수 있으며, 비밀번호 전용 인증이 안전하지 않거나 권장되지 않으므로 다단계 인증이 포함된 인증 방법이 있습니다.
- 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

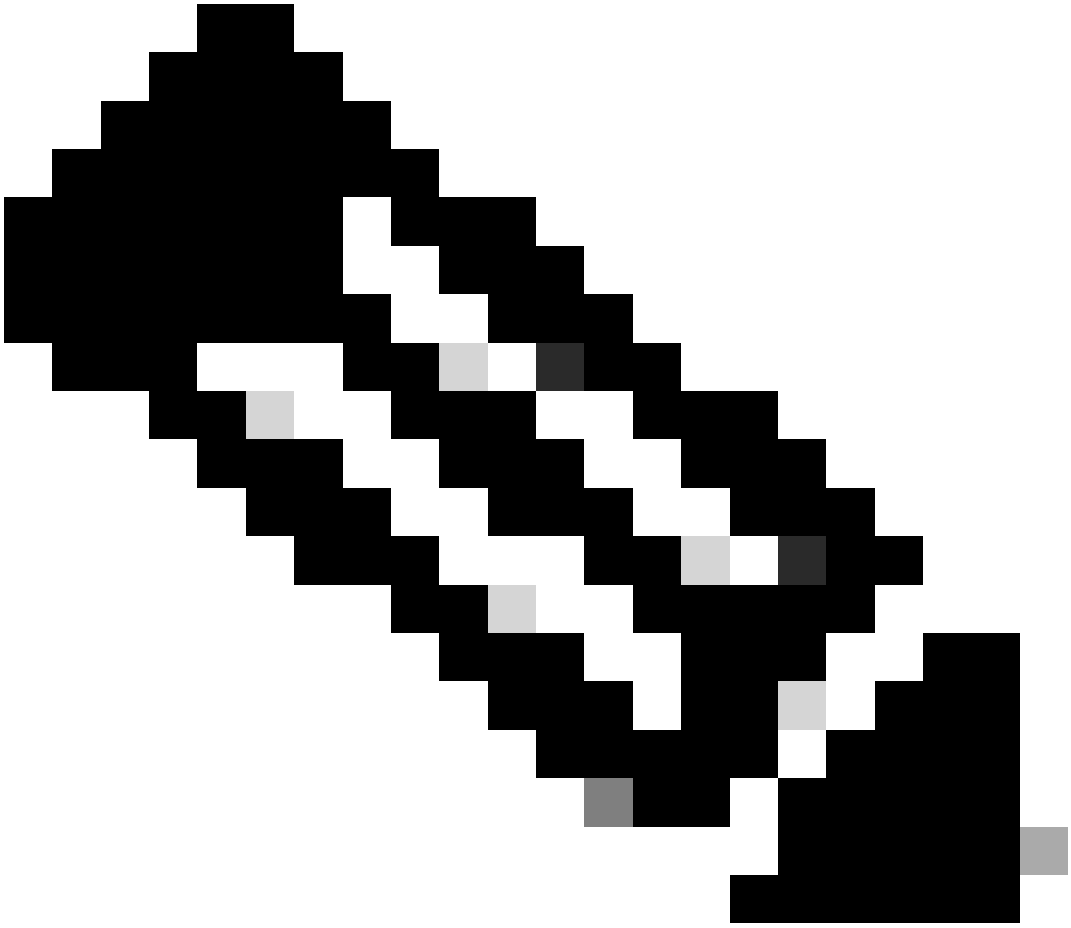
Microsoft Entra ID

1. Microsoft Entra ID 관리 센터로 이동하여 Add(추가) 버튼을 클릭합니다. 이미지에 표시된 대로 Enterprise Application(엔터프라이즈 애플리케이션)을 선택하고 Microsoft Entra SAML Toolkit을 검색합니다.



Microsoft Entra 갤러리 찾아보기

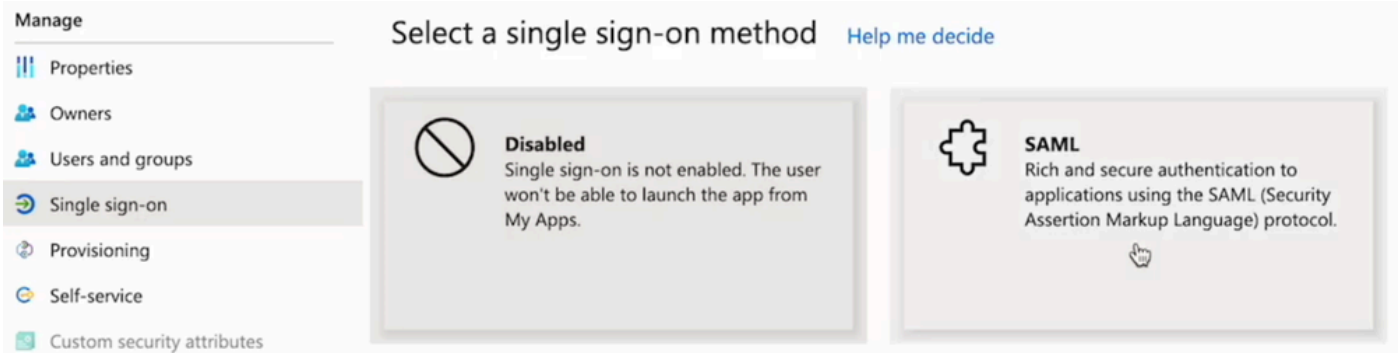
2. 의미 있는 값으로 이름을 지정하고 생성을 클릭합니다. 예: CRES Single Sign On.



참고: 모든 사용자가 CRES 포털에 로그인할 수 있도록 하려면 CRES Sign On(SAML 툴킷) 등록 정보에서 필수 할당을 수동으로 비활성화해야 하며, Assignment Required(할당 필수)에서 No(아니요)를 선택합니다.

---

3. 왼쪽 패널로 이동하여 관리 섹션 아래에서 Single Sign-On을 클릭하고 SAML을 선택합니다.



4. Basic SAML Configuration(기본 SAML 컨피그레이션) 패널에서 Edit(편집)를 클릭하고 다음과 같이 속성을 입력합니다.

- 식별자(엔티티 ID): https://res.cisco.com/
- 회신 URL(어설션 소비자 서비스 URL): https://res.cisco.com/websafe/ssourl
- 로그온 URL: https://res.cisco.com/websafe/ssourl
- 저장을 클릭합니다.

5. [속성 및 클레임] 패널에서 [편집]을 클릭합니다.

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

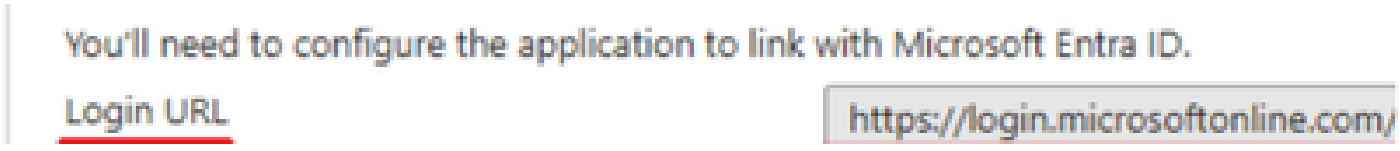
- 소스 특성 필드를 user.userprincipalname으로 설정합니다. user.userprincipalname 값이 유효한 이메일 주소를 나타낸다고 가정합니다. 그렇지 않은 경우 Source를 user.primaryauthoritativeemail로 설정합니다.
- Additional Claims(추가 클레임) 패널에서 Edit(편집)를 클릭하고 Microsoft Entra ID 사용자 속성과 SAML 특성 간의 매핑을 생성합니다.

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. 다음 값을 CRES 포털에 필요한 대로 저장합니다.

- 로그인 URL을 저장합니다.



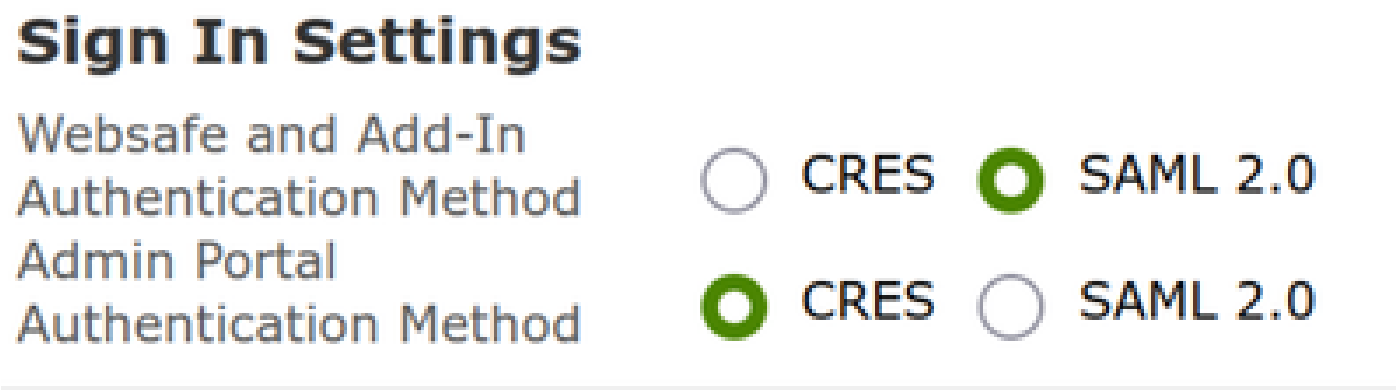
- Certificate (Base64) Download(인증서(Base64) 다운로드) 링크를 선택합니다.

Cisco Email Encryption 서비스

1. Secure Email Encryption Service 조직 포털에 관리자로 로그인합니다.

2. 계정 탭에서 계정 관리 탭을 선택하고 계정 번호를 클릭합니다.

3. 상세내역 탭에서 인증 방법으로 스크롤하고 SAML 2.0을 선택합니다.



4.- 다음과 같이 속성을 입력 합니다.

- SSO 대체 전자 메일 특성 이름: 이메일 주소
- SSO 서비스 공급자 엔티티 ID*: https://res.cisco.com/
- SSO 고객 서비스 URL*: 이 링크는 Entra ID에서 제공합니다.
- SSO 로그아웃 URL: 비워두십시오.

5.- SAML 활성화를 클릭합니다.

다음을 확인합니다.

로그인에 성공한 후 SAML 인증이 활성화되었음을 확인하는 새 창이 나타납니다. 다음을 누릅니다. 그러면 ID 공급자의 로그인 페이지로 리디렉션됩니다. SSO 자격 증명을 사용하여 로그인합니다. 성공적으로 로그인하면 창을 닫을 수 있습니다. 저장을 클릭합니다.

문제 해결

창이 ID 공급자의 로그인 페이지로 리디렉션하지 않은 경우 오류를 제공하면 추적이 반환됩니다. 특성 및 클레임을 검토하고, CRES 인증 방법 섹션에 있는 것과 동일한 이름으로 구성되었는지 확인하십시오. SAML 로그인에 사용되는 사용자 전자 메일 주소는 CRES의 전자 메일 주소와 일치해야 합니다. 별칭은 사용하지 마십시오.

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.