Microsoft Centera ID를 사용하여 SD-WAN에 대한 SSO 구성

목차

소개

이 문서에서는 Microsoft Entra ID를 사용하여 Cisco Catalyst SD-WAN(Software-Defined Wide-Area Network)에 대한 SSO(Single Sign-On)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

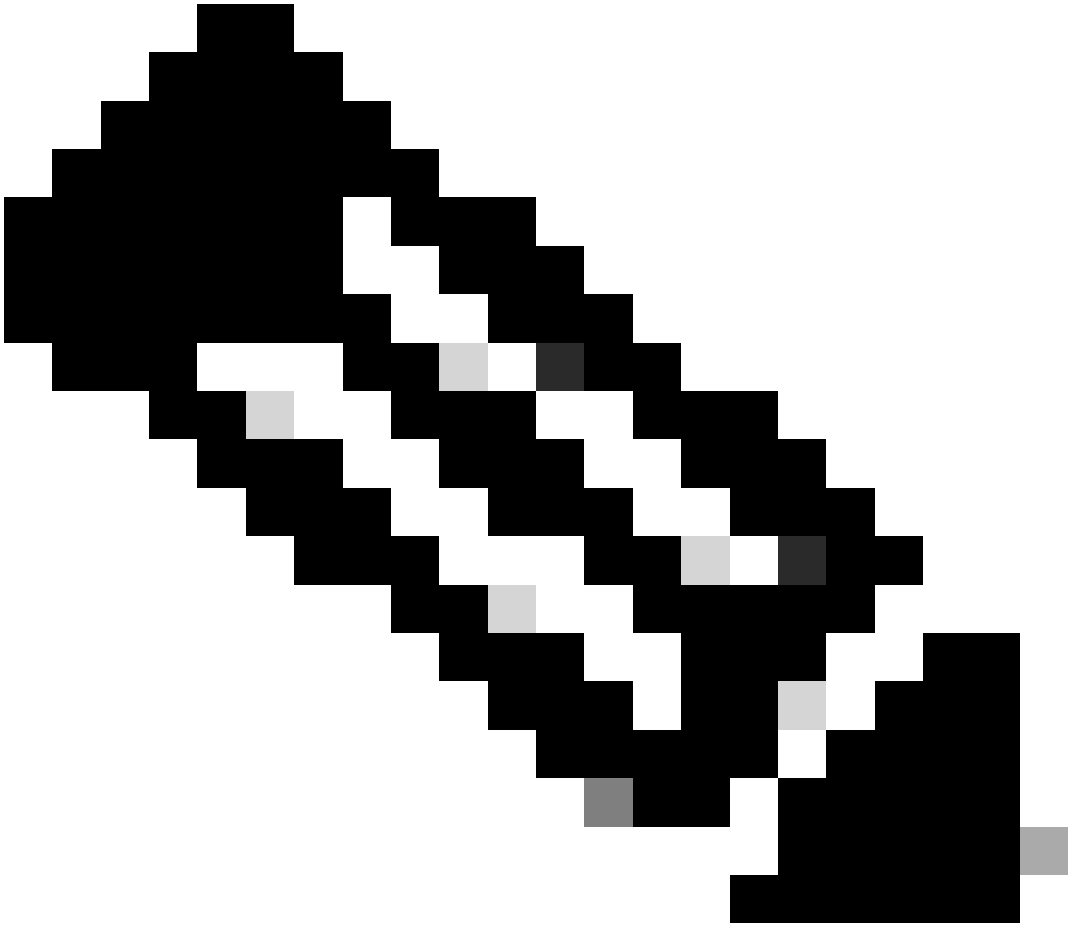
Cisco에서는 다음 항목에 대해 일반적으로 알고 있는 것이 좋습니다.

- 단일 로그인
- Cisco Catalyst SD-WAN 솔루션

사용되는 구성 요소

이 문서의 정보는 다음을 기반으로 합니다.

- Cisco Catalyst SD-WAN Manager 릴리스 20.15.3.1
- Microsoft Entra ID



참고: 이전에 Azure Active Directory(Azure AD)로 알려진 솔루션을 이제 Microsoft Entra ID라고 합니다.

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

Single Sign-On은 사용자가 단일 자격 증명 집합을 사용하여 여러 독립 애플리케이션이나 웹 사이트에 안전하게 액세스할 수 있는 인증 방법입니다. SSO를 사용하면 사용자는 더 이상 각 애플리케이션에 별도로 로그인할 필요가 없습니다. 인증된 후에는 허용된 모든 리소스에 원활하게 액세스할 수 있습니다.

SSO를 구현하는 일반적인 방법 중 하나는 SAML 2.0, WS-Federation 또는 OpenID Connect와 같은 프로토콜을 사용하여 IdP(ID 공급자)와 SP(서비스 공급자) 간에 신뢰를 설정하는 페더레이션을 사용하는 것입니다. 페더레이션은 인증을 중앙 집중화하여 보안, 신뢰성 및 사용자 환경을 개선합

니다.

Microsoft Entra ID는 이러한 페더레이션 프로토콜을 지원하는 널리 사용되는 클라우드 기반 ID 공급자입니다. Cisco Catalyst SD-WAN을 사용하는 SSO 설정에서 Microsoft Entra ID는 IdP 역할을 하고 Cisco SD-WAN Manager는 서비스 공급자 역할을 합니다.

통합은 다음과 같이 작동합니다.

1. 네트워크 관리자가 Cisco SD-WAN Manager에 로그인을 시도합니다.
2. Cisco SD-WAN Manager가 Microsoft Centera ID로 인증 요청을 보냅니다.
3. Microsoft Entra ID는 관리자에게 해당 Entra ID(Microsoft) 계정으로 인증하라는 프롬프트를 표시합니다.
4. 자격 증명이 검증되면 Microsoft Entra ID는 인증을 확인하는 보안 응답을 Cisco SD-WAN Manager로 다시 전송합니다.
5. Cisco SD-WAN Manager는 별도의 자격 증명 없이 액세스 권한을 부여합니다.

이 모델에서는

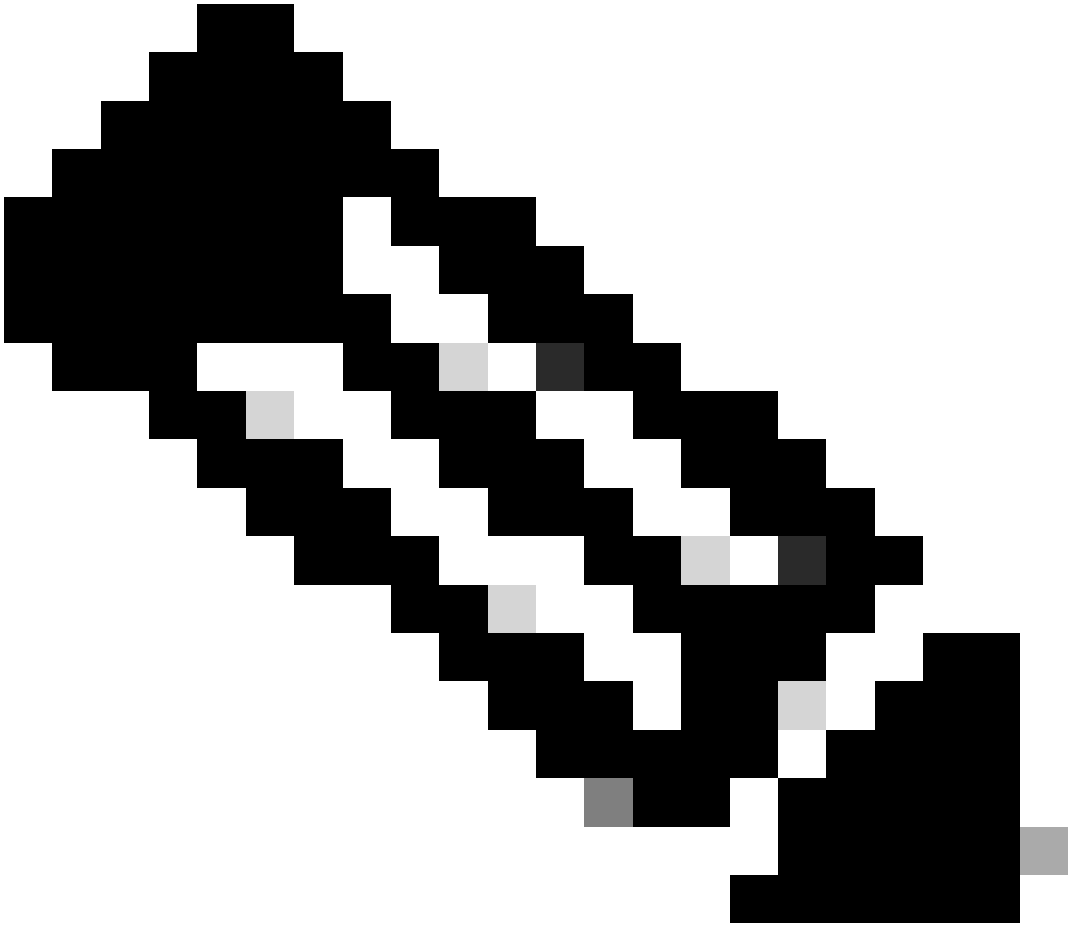
- IdP(ID 제공자) - 사용자 데이터를 저장하고 자격 증명을 검증합니다(예: Microsoft Entra ID, Okta, PingID, ADFS).
- 통신 사업자 - 액세스할 애플리케이션을 호스팅합니다(예: Cisco SD-WAN Manager).
- 사용자 - IdP 디렉터리에 계정이 있으며 서비스 공급자에 액세스할 권한이 있습니다.

Cisco Catalyst SD-WAN은 업계 표준에 따라 구성된 경우 모든 SAML 2.0 호환 IdP와 호환됩니다.

SSO(Single Sign-On) 사용의 이점

- ID 공급자를 통해 자격 증명 관리를 중앙 집중화합니다.
- 여러 개의 취약한 비밀번호를 제거하여 인증 보안을 강화합니다.
- 관리자의 보안 액세스를 간소화합니다.
- Cisco Catalyst SD-WAN Manager 및 기타 인증된 애플리케이션에 한 번의 클릭으로 액세스할 수 있습니다.

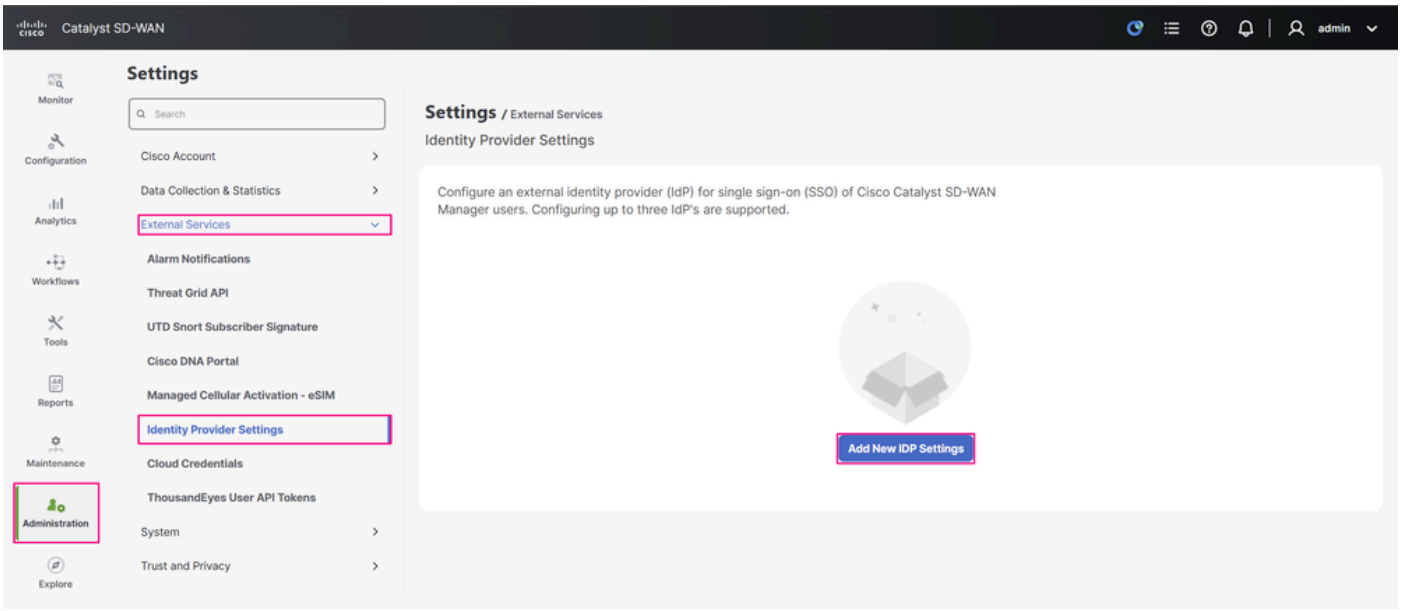
구성



참고: 지원되는 최소 릴리스: Cisco Catalyst SD-WAN Manager 릴리스 20.8.1.

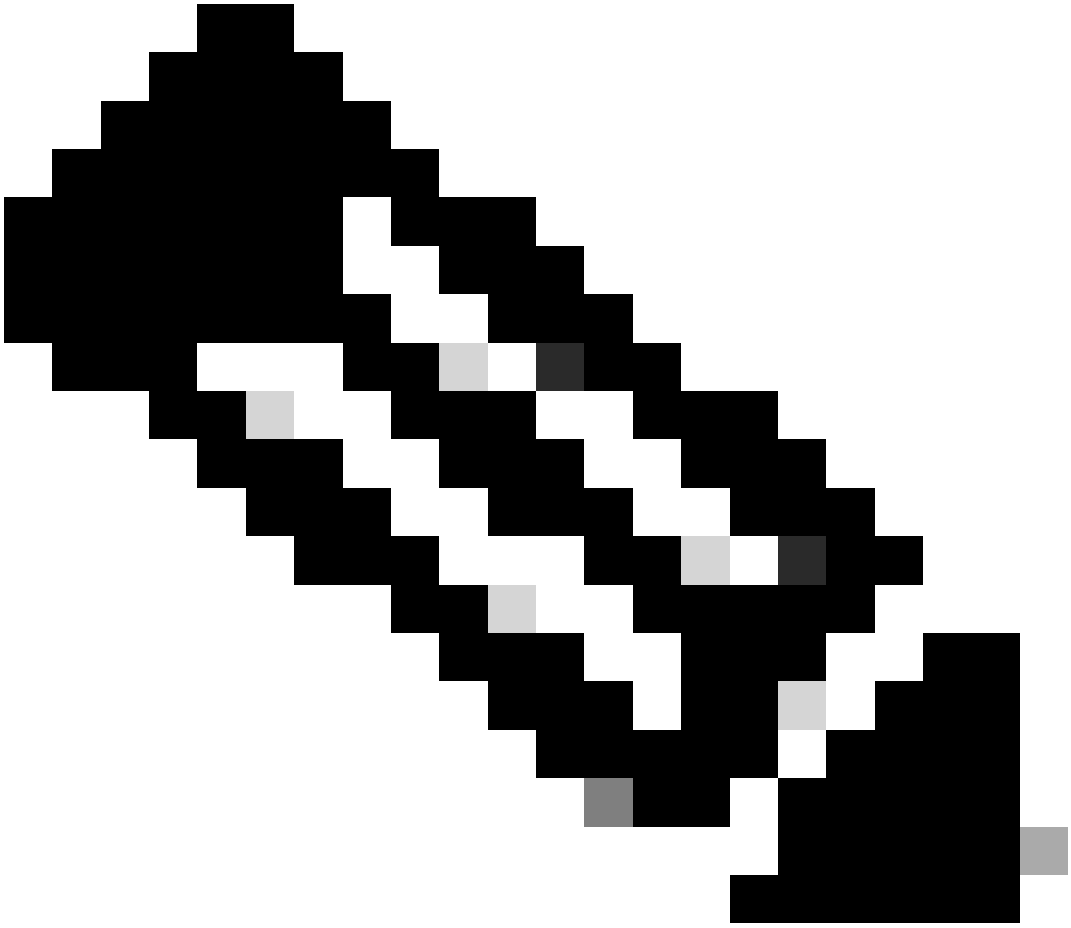
1단계. Cisco SD-WAN Manager SAML 메타데이터 가져오기

- Cisco SD-WAN Manager에서 Administration(관리) > Settings(설정) > External Services(외부 서비스) > Identity Provider Settings(ID 제공자 설정)로 이동하고 Add New IDP Settings(새 IDP 설정 추가)를 클릭합니다.



Cisco SD-WAN Manager UI

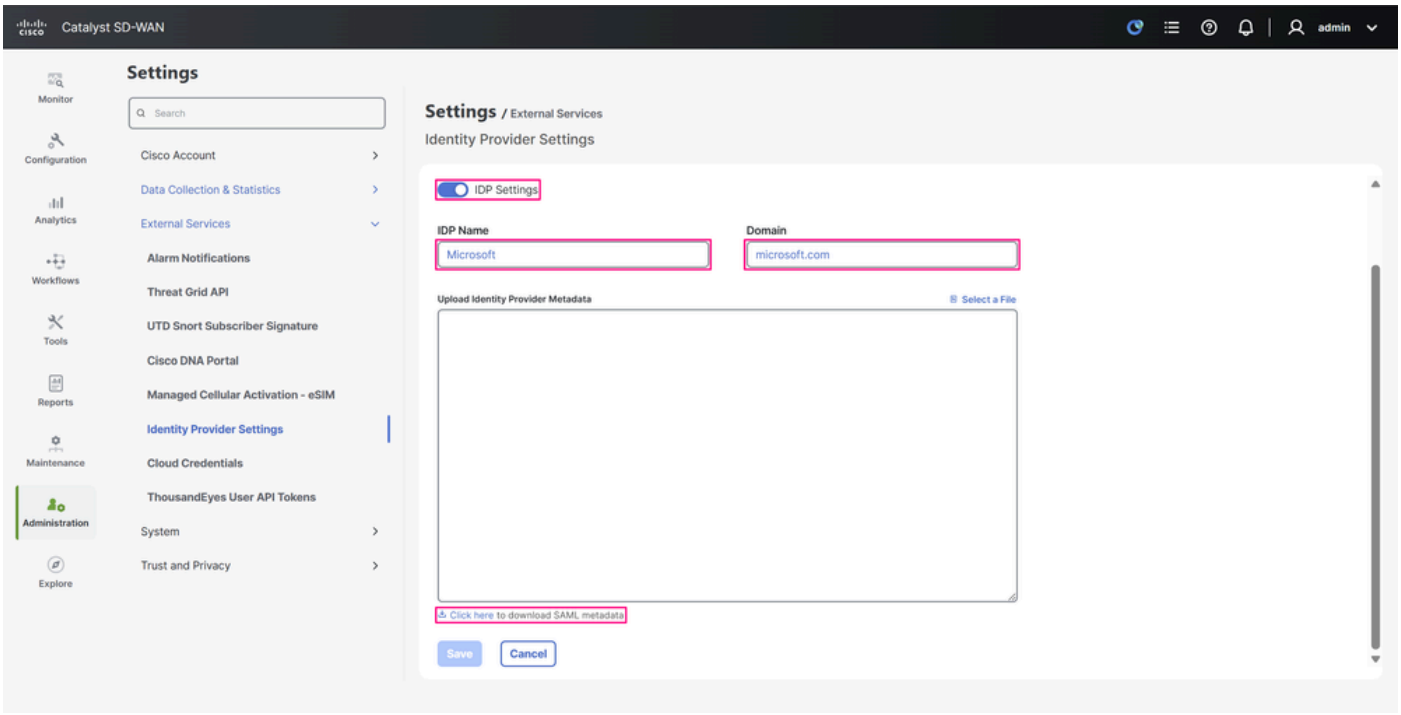
- ID 공급자 설정을 활성화하려면 IDP 설정을 토글합니다. IDP Name(IDP 이름) 필드에 사용 중인 IdP를 참조하는 이름을 입력하고 Domain(도메인) 필드에서 조직의 엔터프라이즈 응용 프로그램에서 사용자가 사용하는 도메인 이름과 일치하는 도메인을 입력합니다. SAML 메타데이터를 다운로드하고 메타데이터 XML 파일을 컴퓨터에 저장하려면 Click here를 클릭합니다. 이 파일은 다음 단계에서 Microsoft Entra ID에서 SSO를 구성하는 데 사용됩니다.



참고: 이 예에서 메타데이터 XML 파일은 Cisco SD-WAN Manager의 IP 주소를 직접 가리키지만, 많은 프로덕션 환경에서는 FQDN(Fully Qualified Domain Name)을 가리킵니다. 독립형 Cisco SD-WAN Manager의 경우, 메타데이터에 포함된 엔티티 ID는 다운로드할 때 Cisco SD-WAN Manager에 로그인하는 데 사용하는 URL과 일치합니다. 즉, 단일 노드 설정이므로 IP 주소 또는 FQDN에서 작동합니다.

Cisco SD-WAN Manager 클러스터의 경우 FQDN이 클러스터 노드 중 하나를 가리키고 메타데이터에 이 도메인이 엔티티 ID로 포함된다는 점에서 동일한 원칙이 적용됩니다. 클러스터의 FQDN과 함께 메타데이터를 사용하든 IP 주소를 사용하여 특정 노드에서 메타데이터를 사용하든, Microsoft Entra ID와 SSO 통합이 성공적으로 완료되면 다른 노드도 IdP 로그인 프롬프트로 리디렉션된다는 점이 다릅니다.

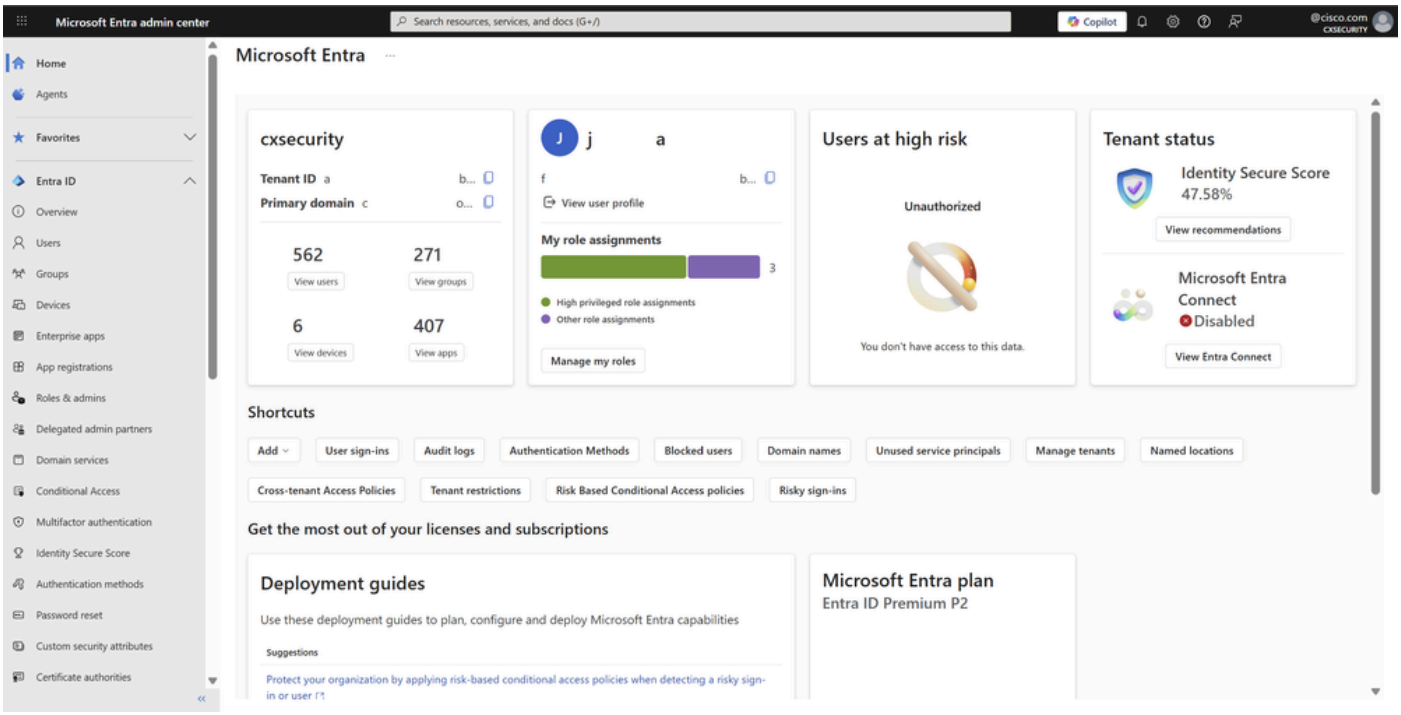
두 시나리오 모두의 주요 요구 사항은 Cisco SD-WAN Manager에서 사용하는 엔티티 ID(IP 주소 또는 FQDN)가 IdP 측에 구성된 식별자와 일치하는지 여부입니다.



IdP 설정 구성 페이지

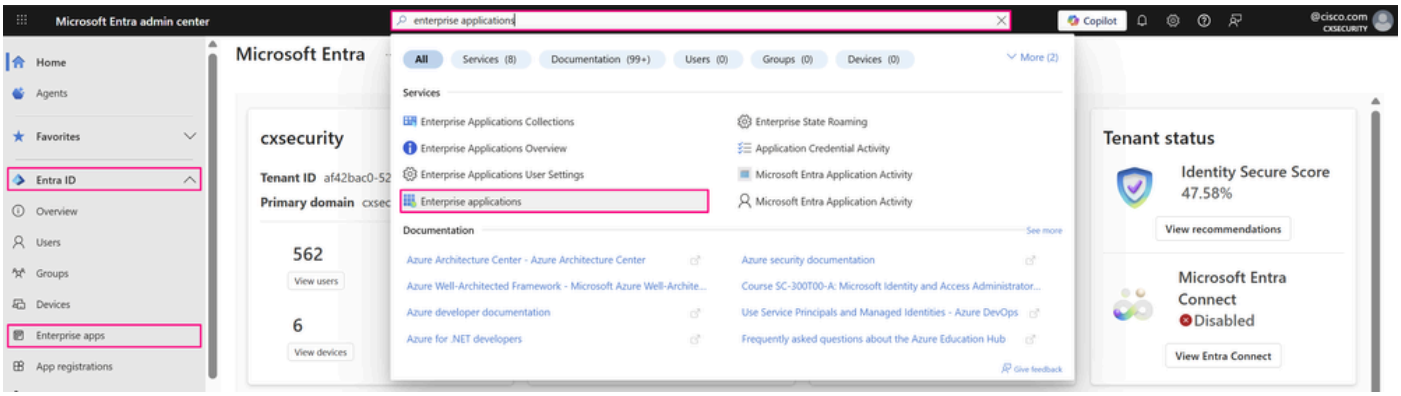
2단계. Microsoft Enterprise ID에서 SSO용 엔터프라이즈 애플리케이션 구성

- 다음 역할 중 하나를 사용하여 Microsoft Entra 관리 센터 포털에 로그인합니다. 클라우드 애플리케이션 관리자, 애플리케이션 관리자 또는 서비스 주체의 소유자입니다.



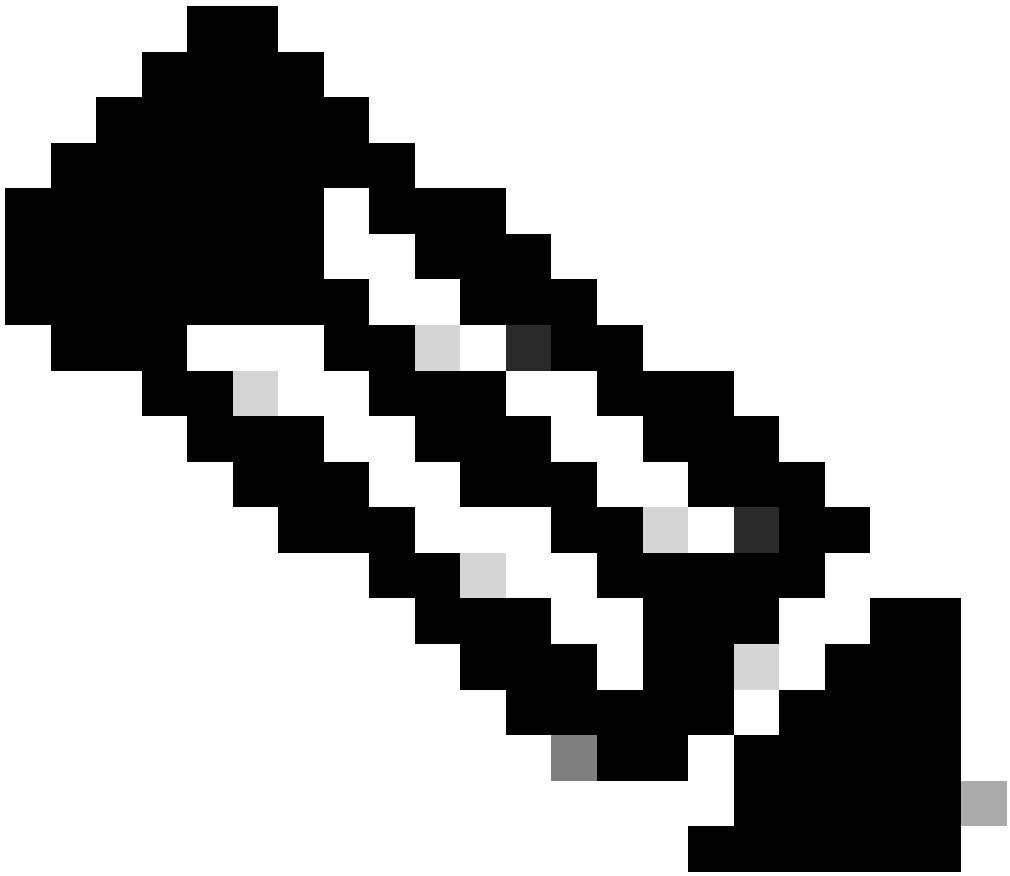
Microsoft Entra Admin Center 포털

- Enterprise ID > Enterprise apps로 이동하거나 포털 상단의 검색 표시줄에 엔터프라이즈 애플리케이션을 입력한 다음 Enterprise Applications를 선택하면 이 서비스에 액세스할 수도 있습니다.

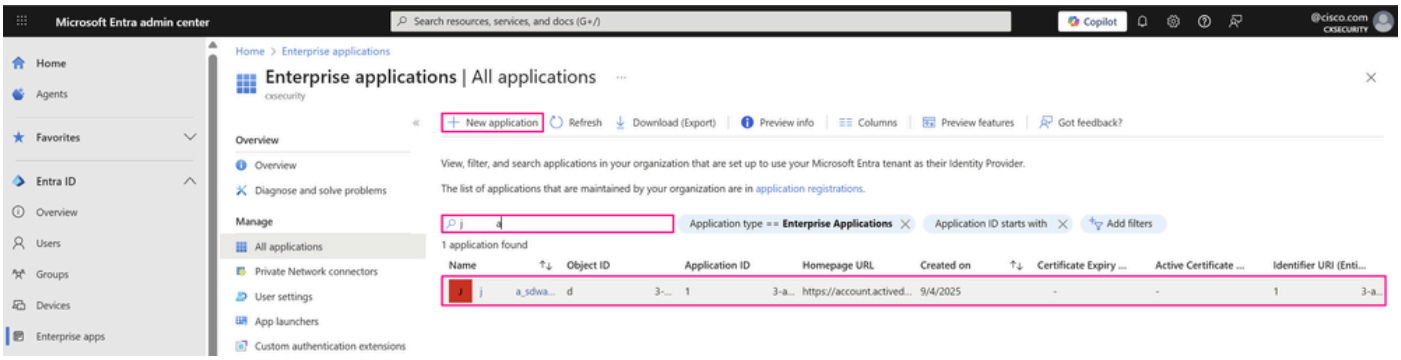


Microsoft Entra Admin Center 포털

- 모든 응용 프로그램 페이지가 열립니다. 검색 상자에 기존 애플리케이션의 이름을 입력한 다음 검색 결과에서 애플리케이션을 선택합니다.

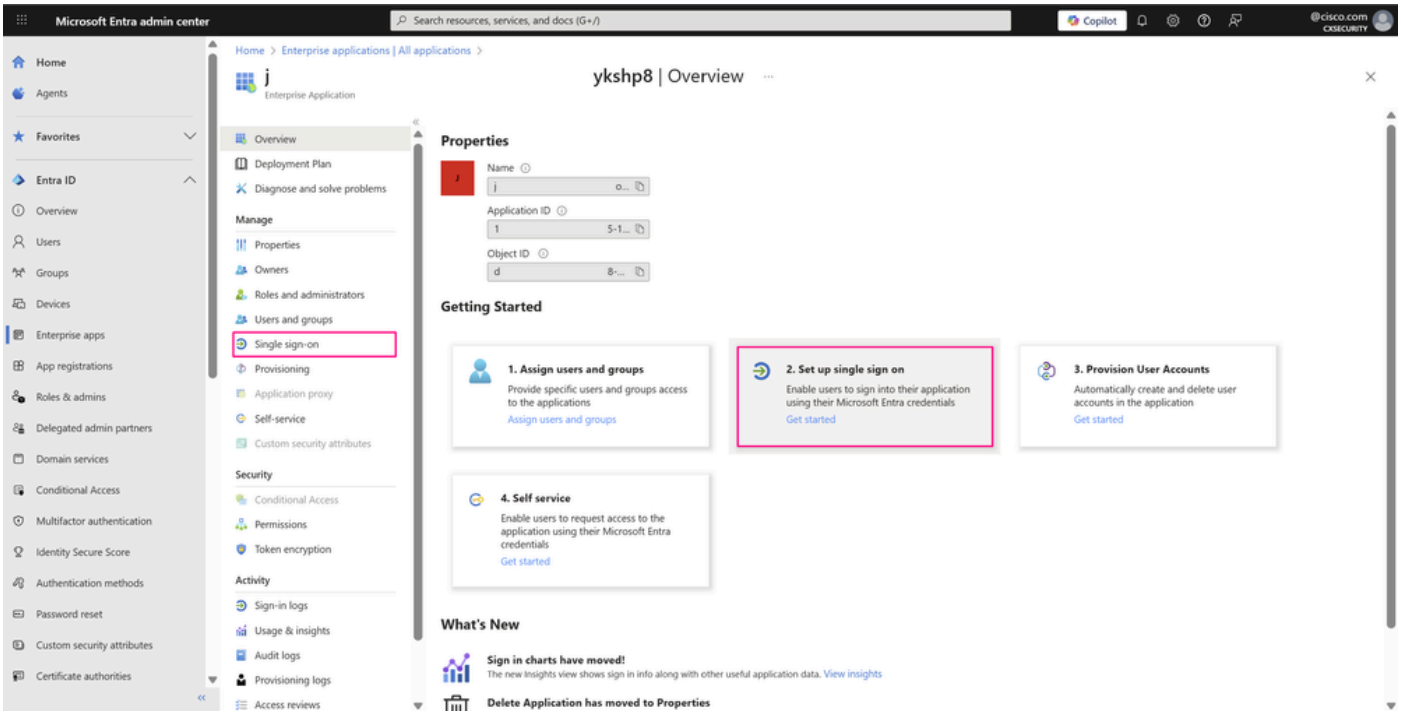


참고: 동일한 페이지에서 New application(새 애플리케이션)을 클릭할 때 조직의 요구 사항에 따라 맞춤형 엔터프라이즈 애플리케이션을 생성하고 아직 SSO 인증이 없는 경우 SSO 인증으로 구성할 수 있습니다.



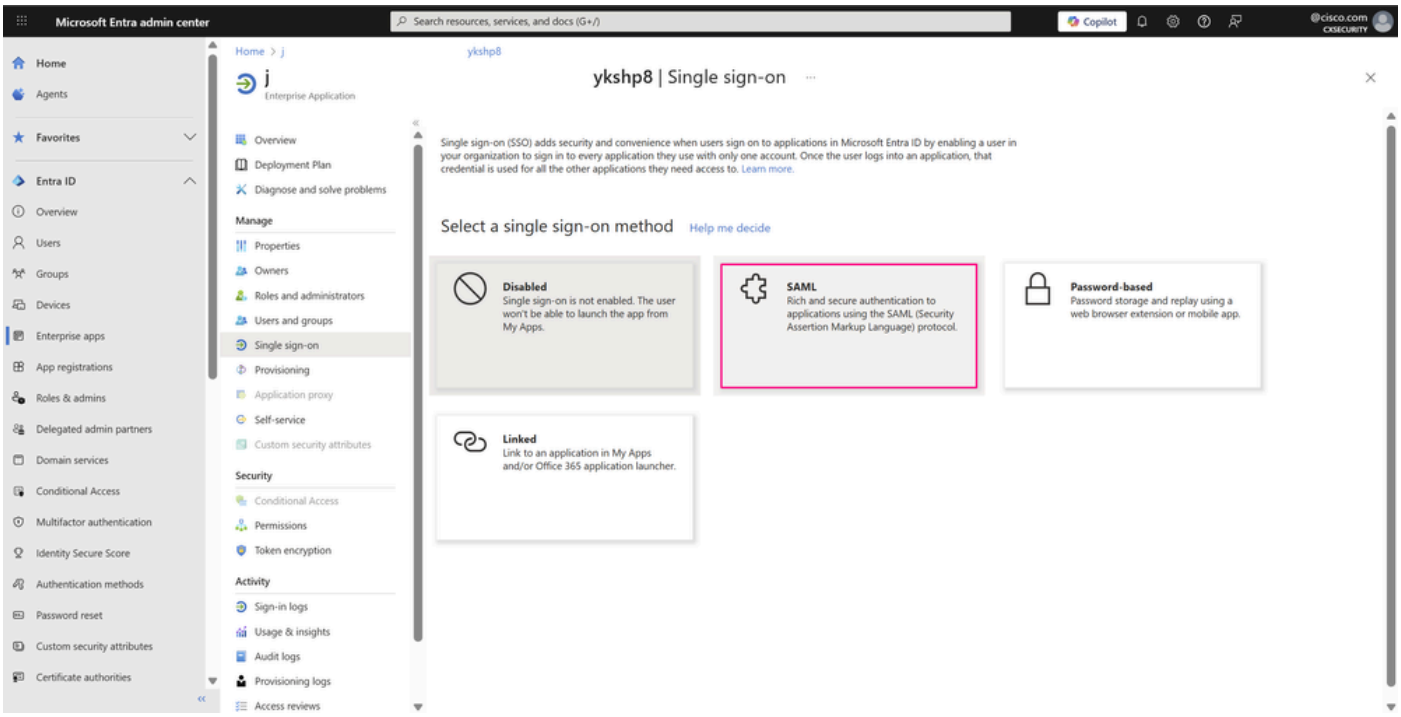
엔터프라이즈 애플리케이션 대시보드

- 왼쪽 메뉴의 [관리] 섹션에서 [단일 로그인]을 클릭하거나 개요 섹션 내의 [시작] 창에서 2. [단일 로그인]을 설정하여 편집을 위해 [단일 로그인] 창을 엽니다.



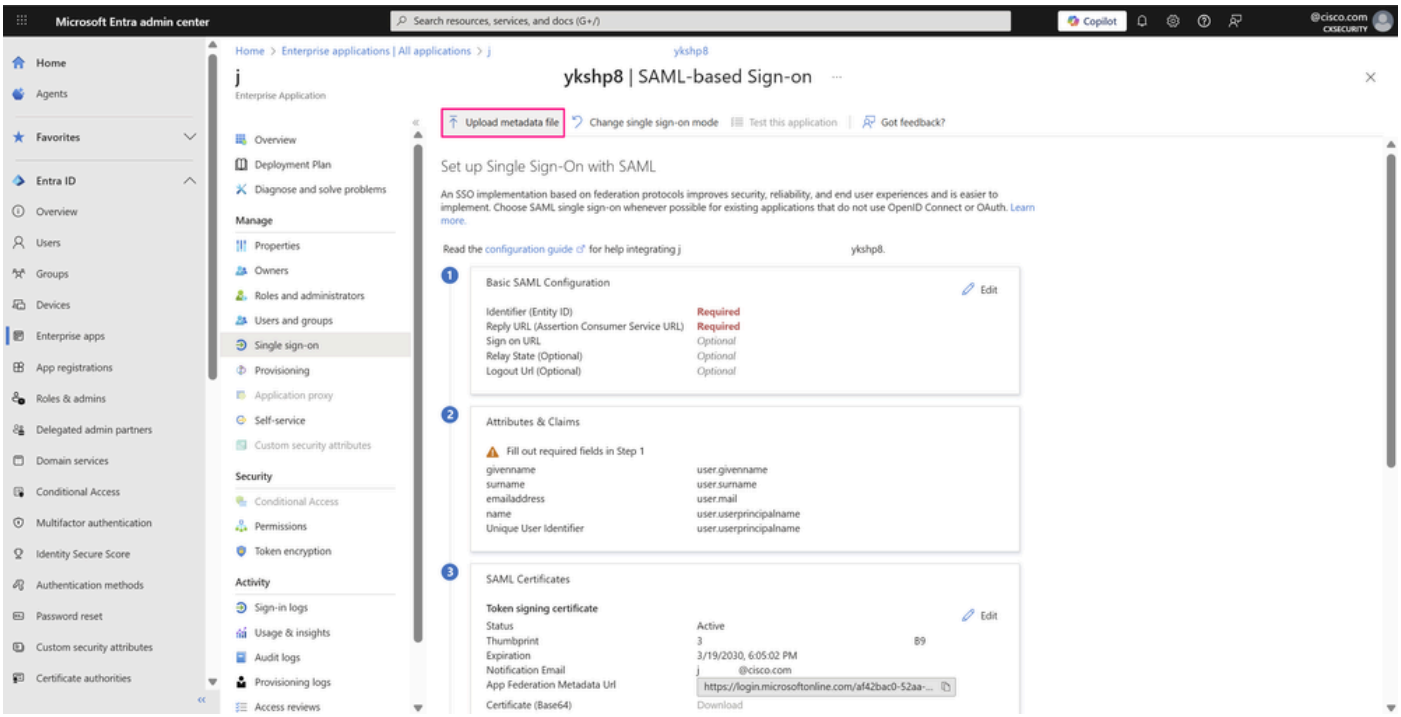
엔터프라이즈 애플리케이션 개요

- SAML을 선택하여 SSO 컨피그레이션 페이지를 엽니다.



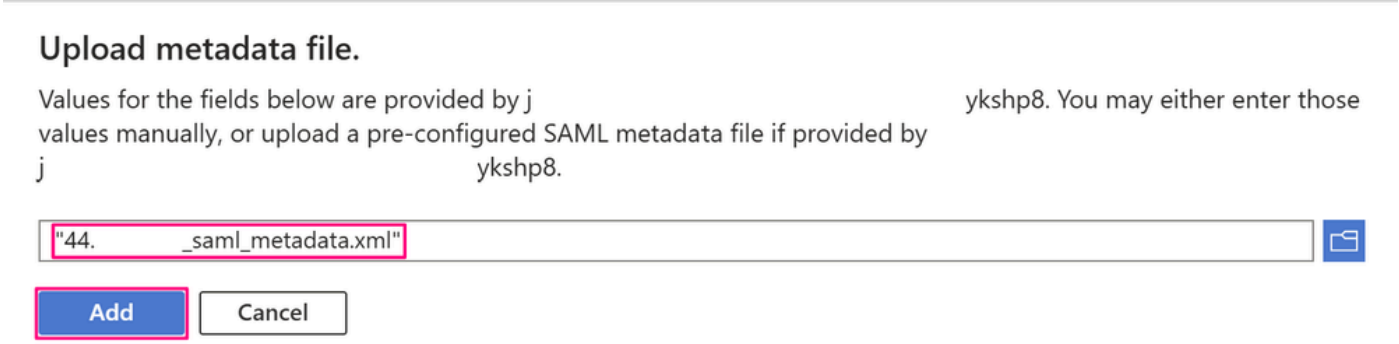
Single Sign-On 창

- Set up Single Sign-On with SAML(SAML을 사용하여 단일 로그인 설정) 페이지에서 Upload metadata file(메타데이터 파일 업로드)을 클릭합니다.



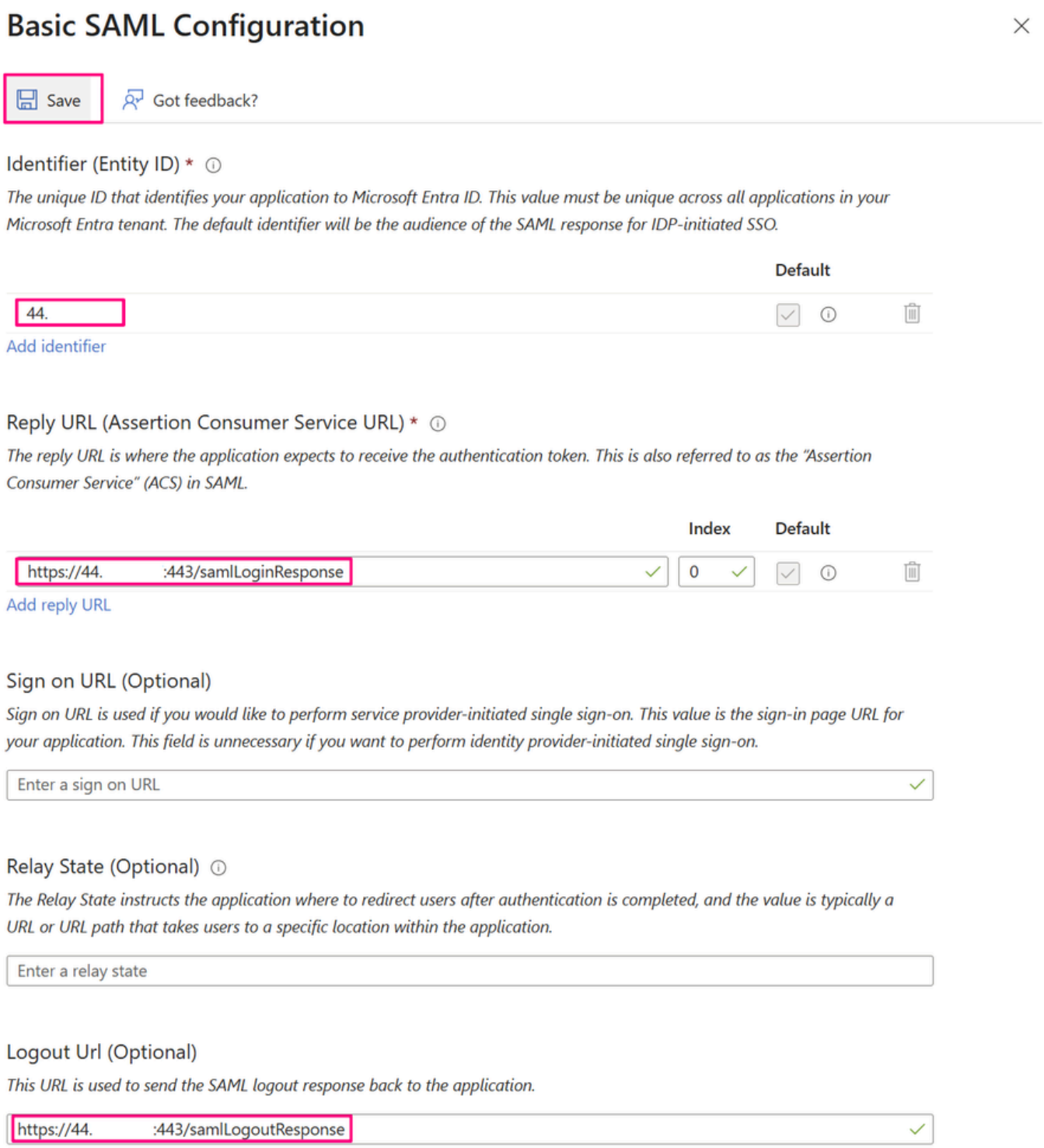
SAML을 사용하는 SSO 구성 페이지

- 메타데이터 파일 업로드 창에서 이전에 다운로드한 메타데이터 XML 파일을 찾아서 클릭한 다음 추가를 클릭합니다.



메타데이터 파일 업로드 창

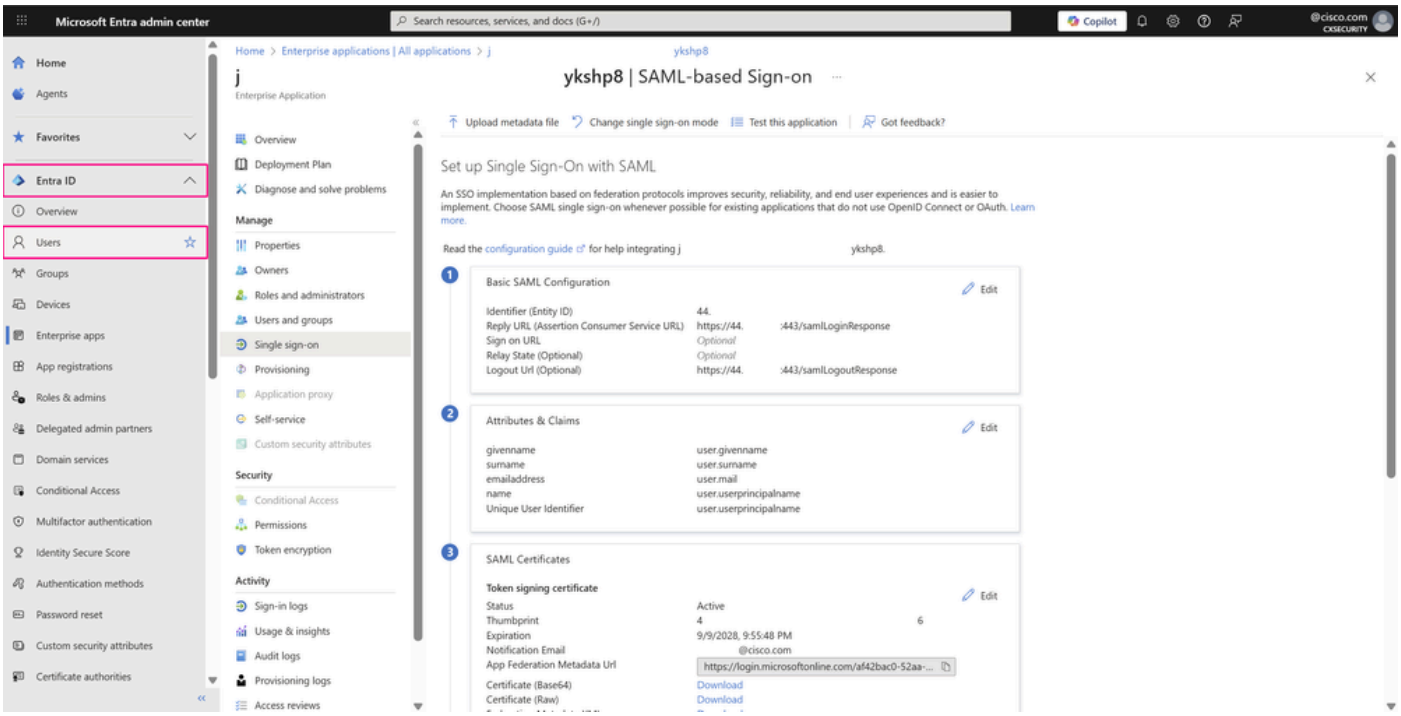
- Basic SAML Configuration(기본 SAML 컨피그레이션) 창에서 식별자(엔티티 ID)는 일반적으로 (이전 단계에서 설명한 대로) 통합하려는 애플리케이션(이 경우 Cisco SD-WAN Manager)에 해당하는 URL입니다. 파일이 성공적으로 업로드되면 Reply URL(회신 URL) 및 Logout URL(로그아웃 URL) 값이 자동으로 채워집니다. 계속하려면 저장을 클릭합니다.



기본 SAML 컨피그레이션 창

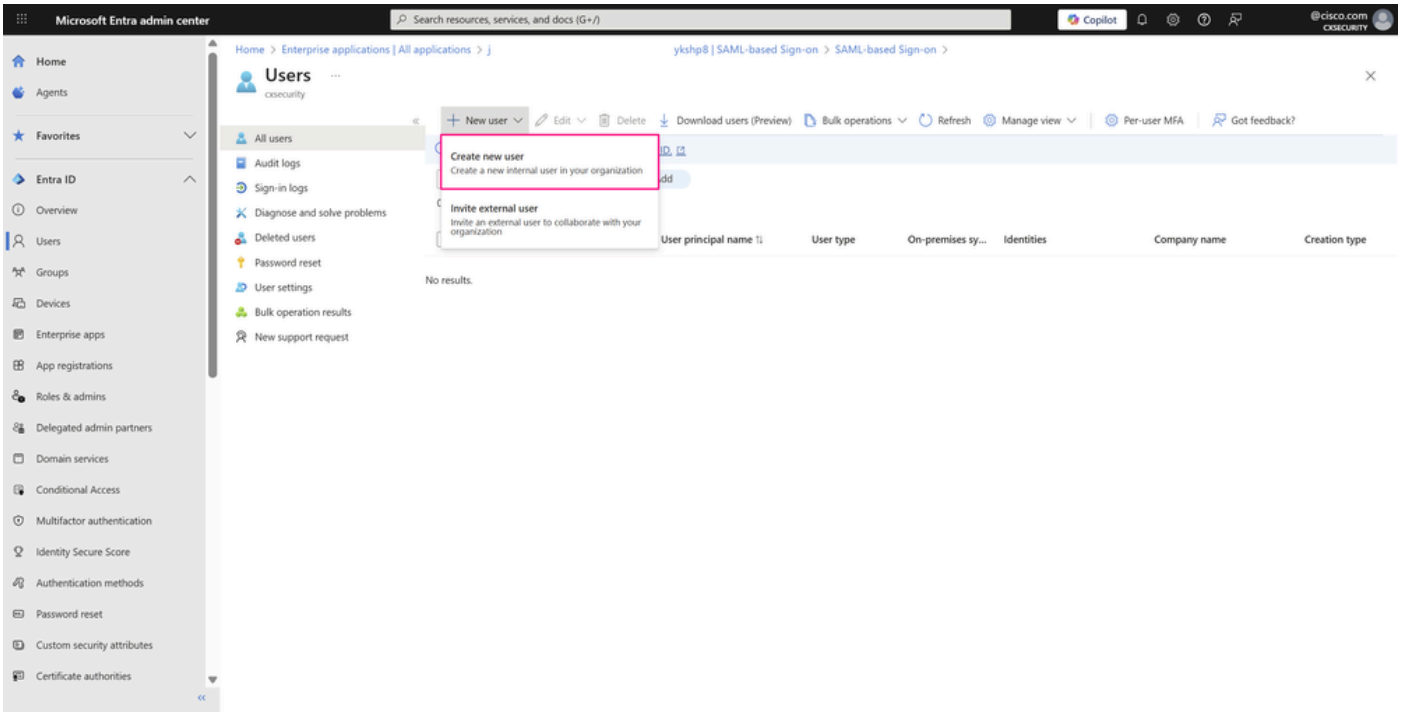
3단계. 엔터프라이즈 응용 프로그램에 사용자 또는 그룹 계정 추가

- 정의된 애플리케이션의 SAML 컨피그레이션 매개변수를 사용하여 엔터프라이즈 애플리케이션에서 애플리케이션에 로그인하는 사용자 또는 그룹을 추가합니다. 이렇게 하려면 먼저 Entra ID > Users(사용자)로 이동하거나, 이전 단계에 표시된 대로 포털 상단의 검색 표시줄에서 서비스 이름을 검색할 때 이 서비스에 액세스할 수도 있습니다.



SAML을 사용하는 SSO 구성 페이지

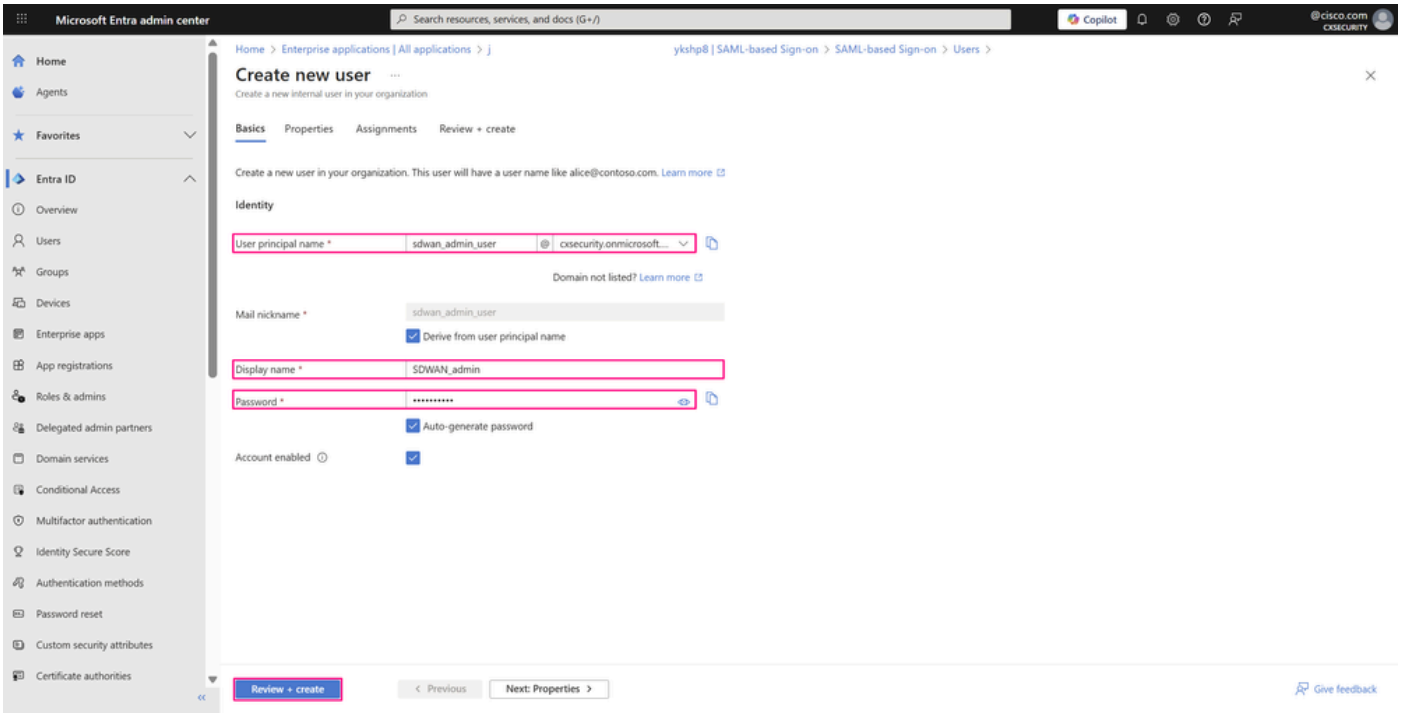
- Cisco SD-WAN Manager 및 프로덕션 환경에서 가장 일반적인 사용자 그룹 중 하나인 netadmin과의 SSO 인증을 설명하기 위해 그룹과 연결하는 사용자를 생성합니다. 이렇게 하려면 Entra ID > 사용자로 이동합니다. 그런 다음 새 사용자를 누르고 새 사용자 생성을 선택합니다.



사용자 대시보드

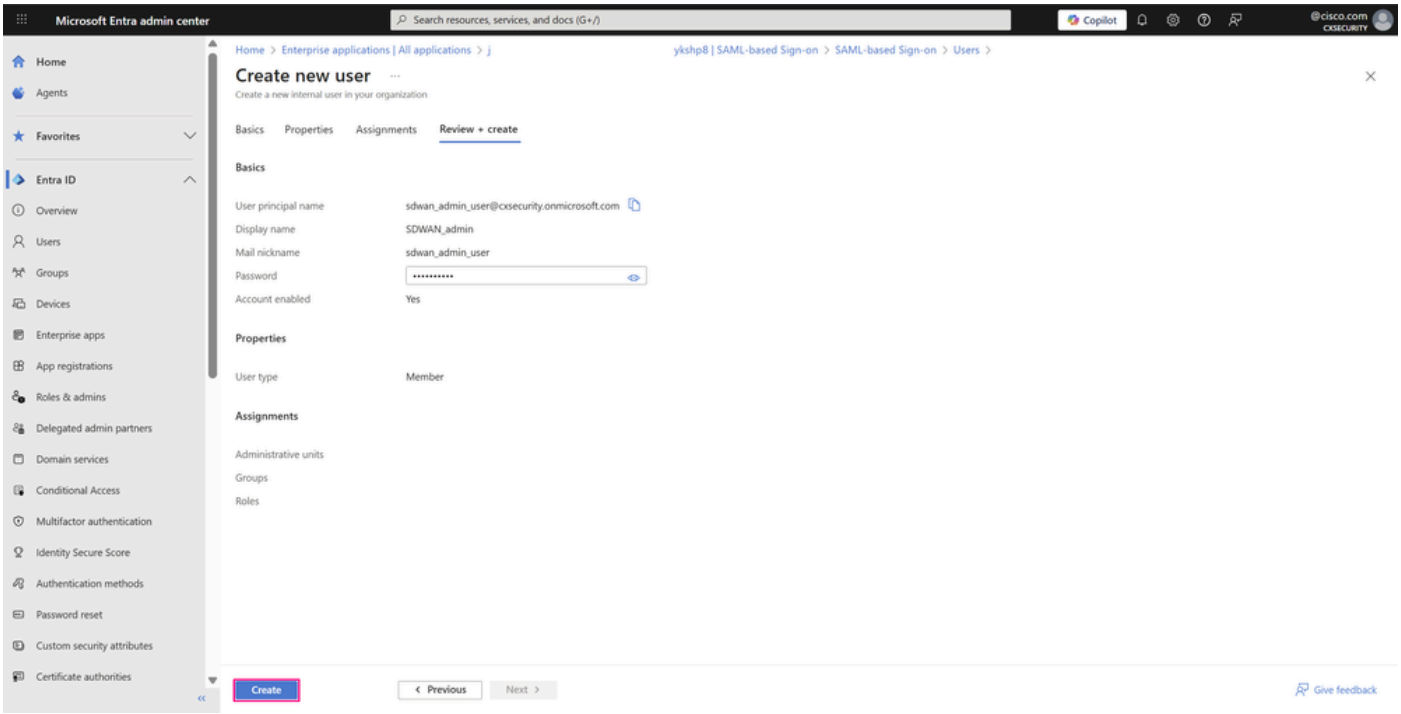
- Basics(기본) 탭에는 새 사용자를 생성하는 데 필요한 핵심 필드가 있습니다.
  - User principal name(사용자 계정 이름)에 고유한 사용자 이름을 입력하고 조직에서 사용할 수 있는 도메인 드롭다운 목록에서 도메인을 선택합니다.
  - 사용자의 표시 이름을 입력합니다.

- 사용자 지정 비밀번호를 입력하려면 Auto-generate password(비밀번호 자동 생성)를 선택 취소하거나 이 옵션을 선택한 상태로 유지하여 비밀번호를 자동으로 생성합니다.
- Assignments(할당) 탭에서 사용자를 그룹에 추가할 수 있지만 그룹 멤버십이 아직 생성되지 않았으므로 Review + create를 클릭합니다.



사용자 생성 페이지

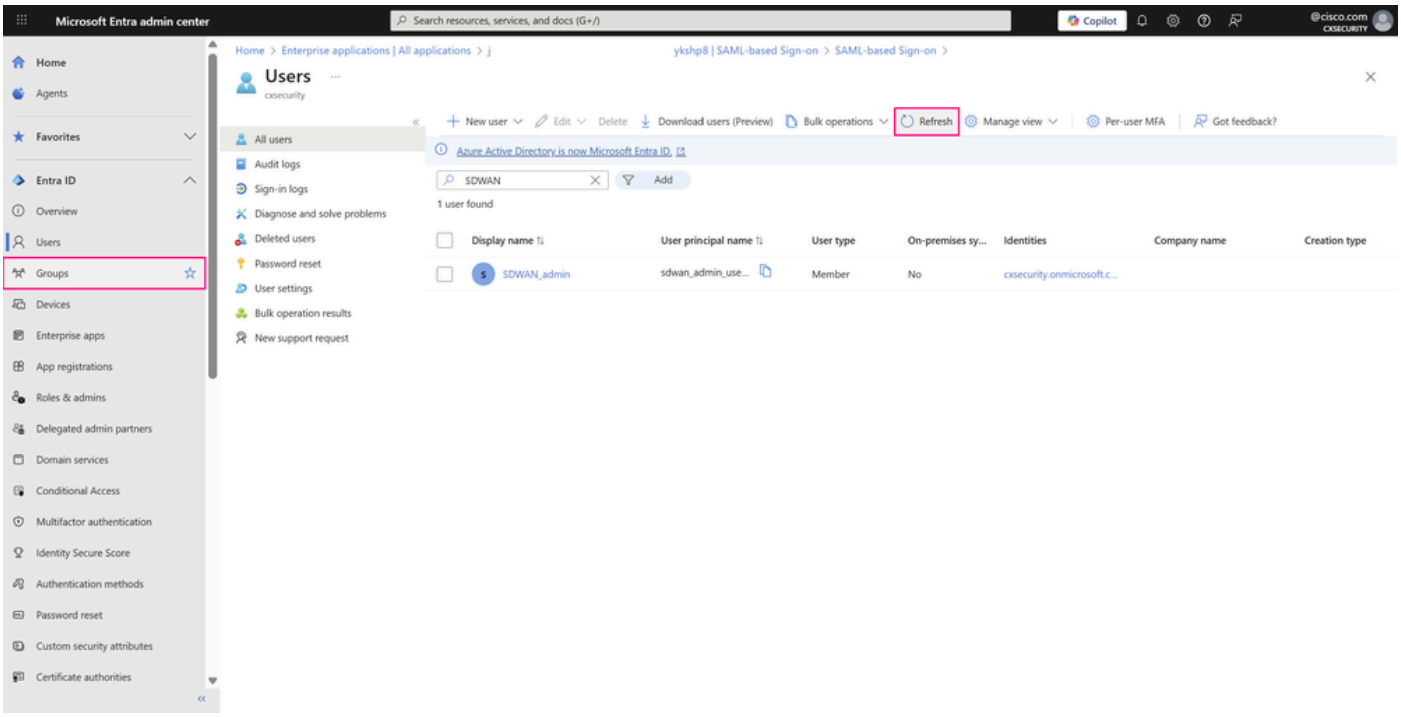
- 최종 탭에는 사용자 생성 워크플로의 주요 세부사항이 표시됩니다. 세부 정보를 검토하고 Create(생성)를 클릭하여 프로세스를 완료합니다.



사용자 생성 페이지

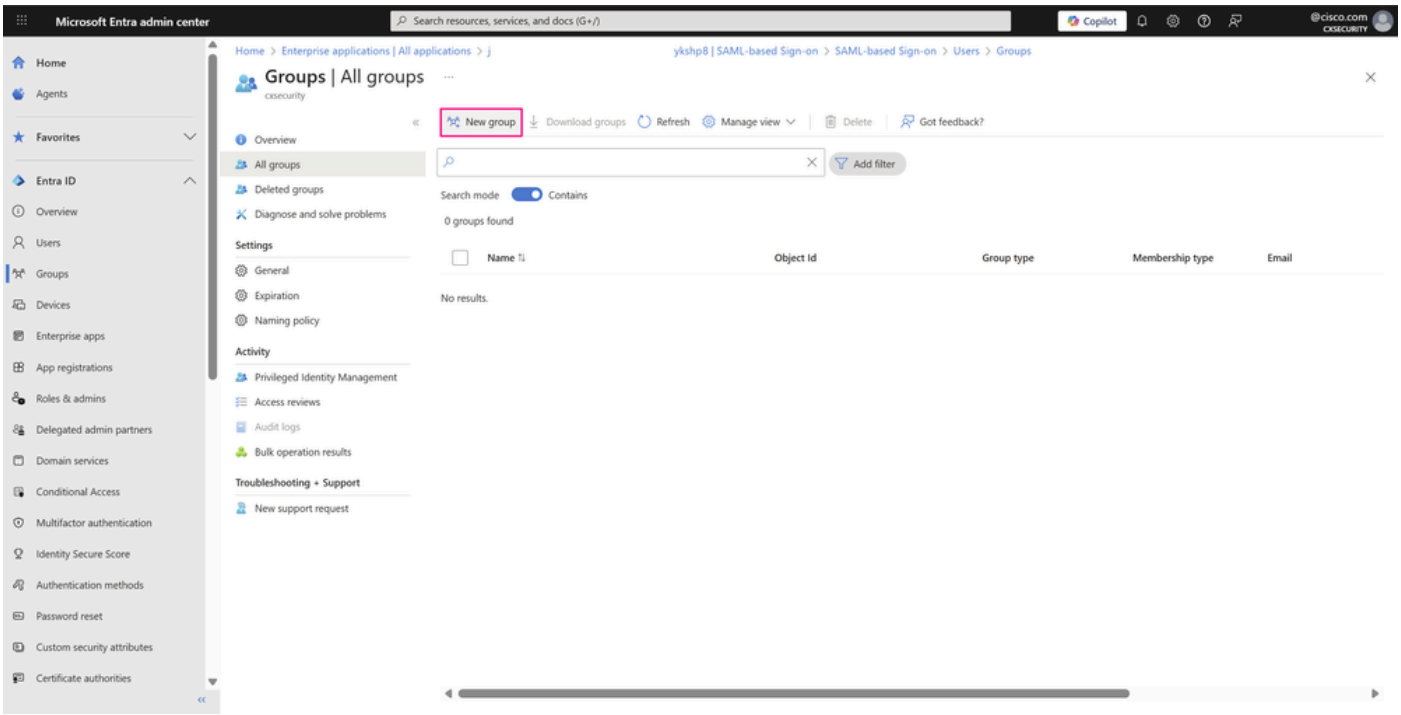
- 새 사용자가 잠시 후에 나타납니다. 그렇지 않은 경우 Refresh(새로 고침)를 클릭하고 서비스

내의 검색 막대를 사용하여 사용자를 검색합니다. 그런 다음 Entra ID > Groups > All groups로 이동하여 새 그룹을 생성합니다.



사용자 대시보드

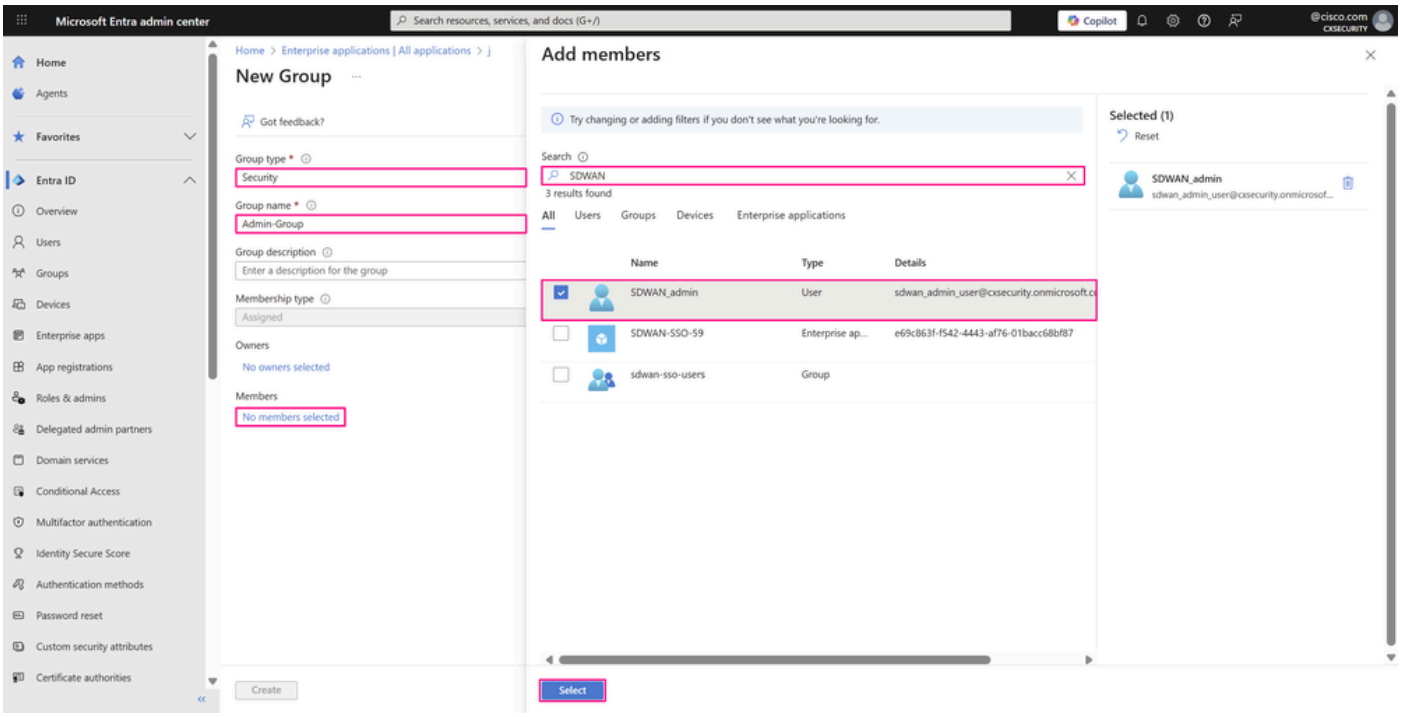
- 이 페이지에서 조직 내의 다른 그룹과 해당 권한을 관리합니다. 네트워크 관리자 권한이 있는 그룹을 생성하려면 새 그룹을 누릅니다.



모든 그룹 페이지

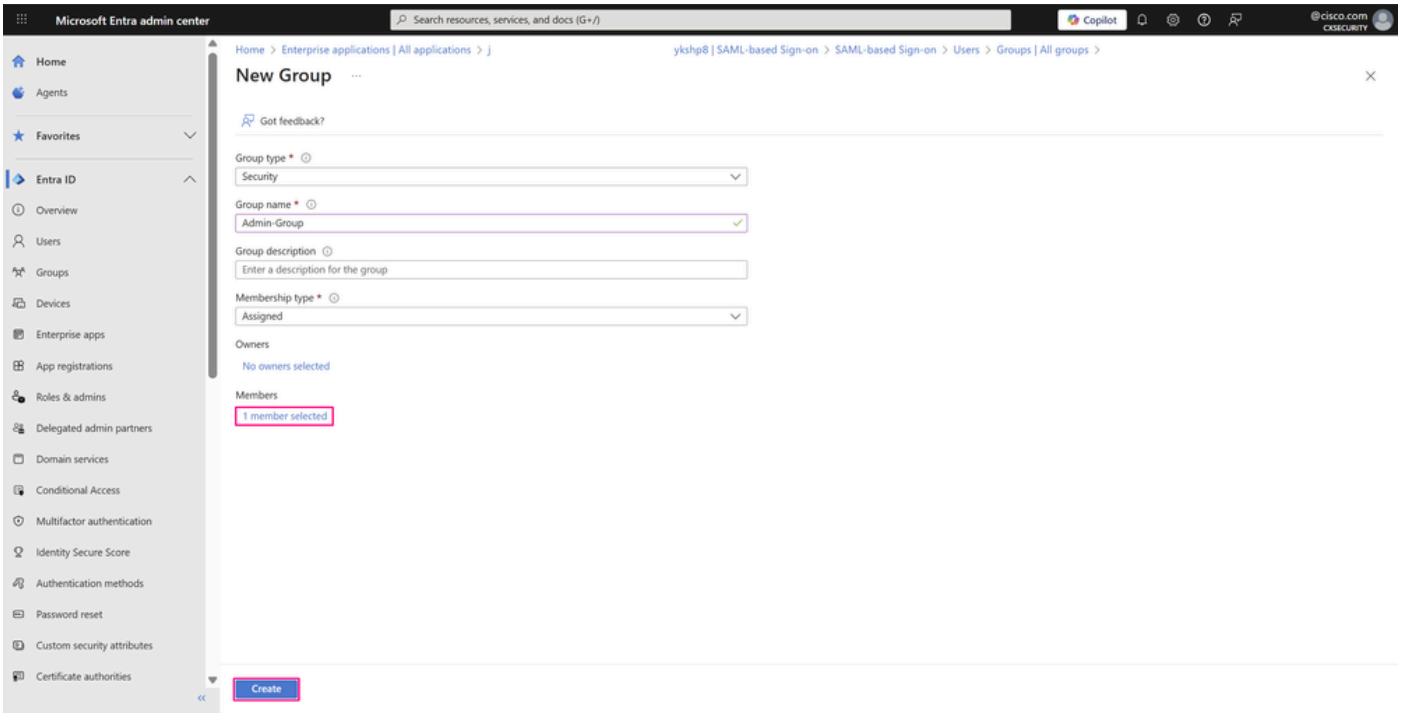
- 드롭다운 목록에서 그룹 유형을 선택합니다. 이 경우 보안을 선택합니다. 공유 리소스에 대한 액세스만 필요합니다. 그룹의 역할 또는 권한을 참조하는 그룹 이름을 입력합니다. 이때 Members(구성원) 필드에서 선택한 구성원을 클릭할 때 사용자를 그룹과 연결합니다.

◦ 멤버 추가 창에서 추가할 사용자(이 예에서는 방금 생성한 사용자)를 찾아서 선택한 다음 선택을 누릅니다.



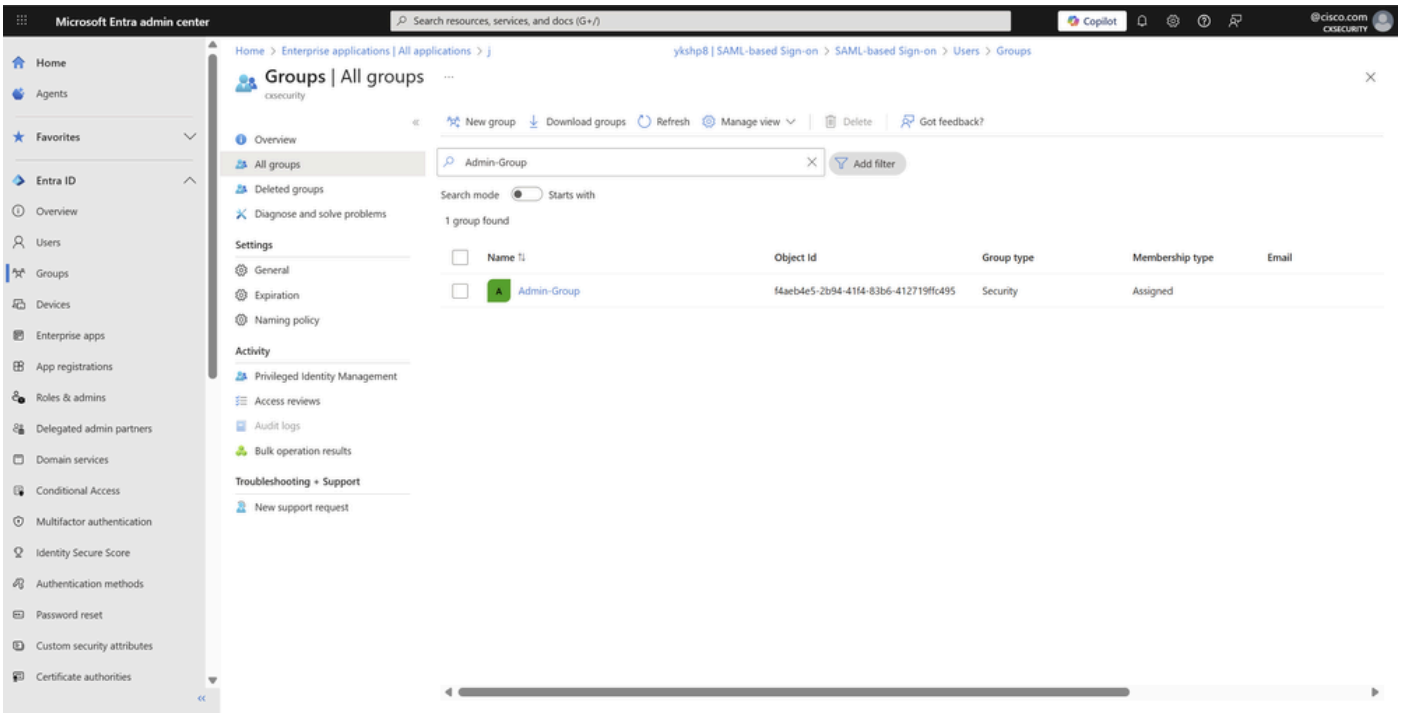
그룹 생성 페이지

- 그룹을 생성하려면 Create(생성)를 클릭합니다.



그룹 생성 페이지

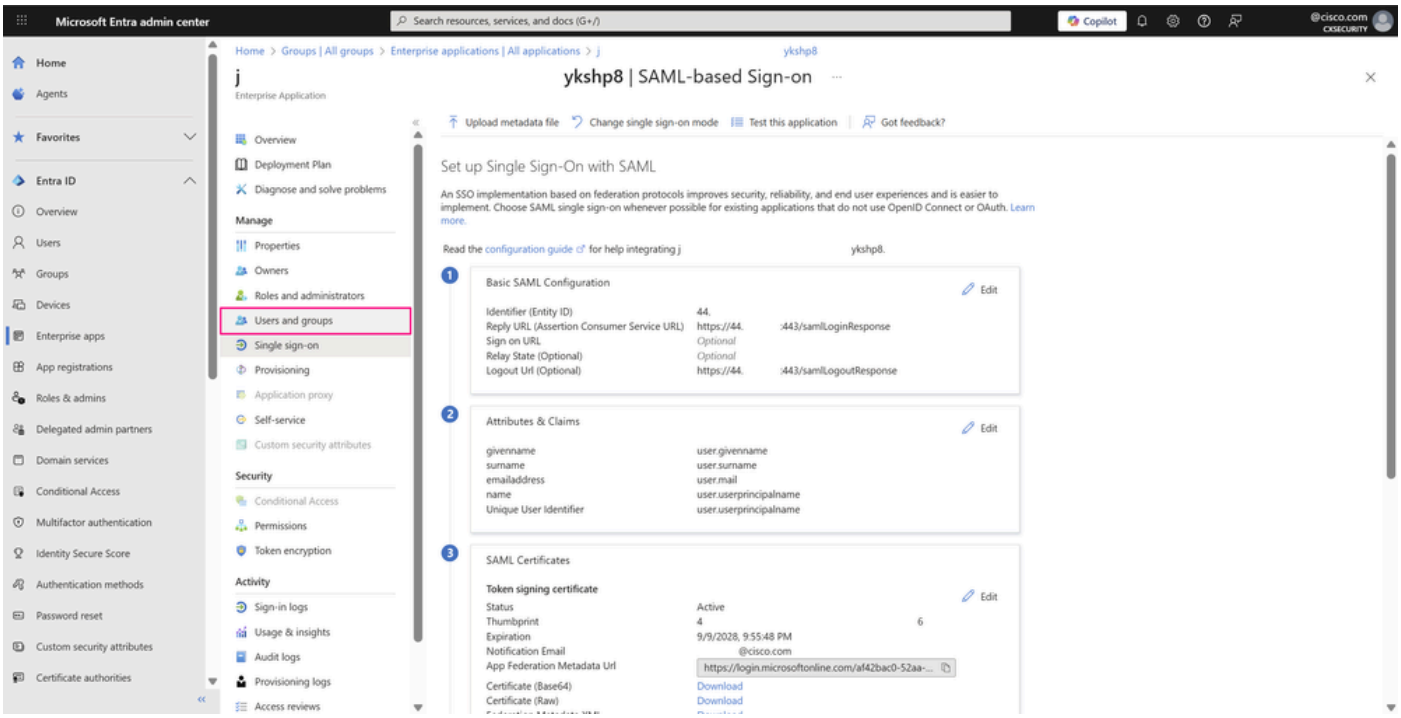
- 새 그룹이 잠시 후에 나타납니다. 그렇지 않은 경우 [새로 고침]을 클릭하고 서비스 내의 검색 표시줄을 사용하여 그룹 이름을 검색합니다. 이전 단계를 반복하여 다른 사용자를 만들고 다른 그룹 구성원에 추가하여 응용 프로그램 및 해당 응용 프로그램의 다른 사용자 그룹(예: 운영자)에 대한 SSO 로그인을 검증합니다.



모든 그룹 페이지

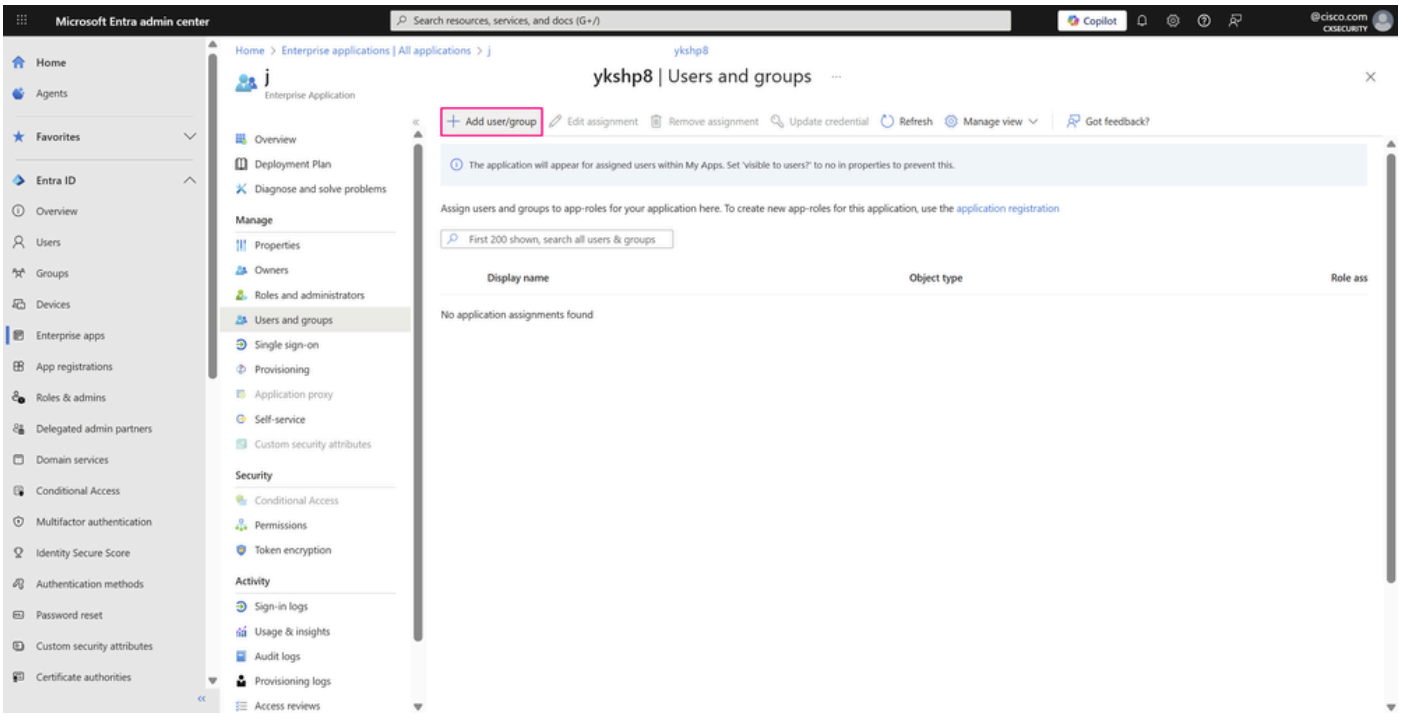
4단계. Microsoft Entra ID에 대한 SAML 그룹 프로비저닝 구성

- SAML 컨피그레이션에서 그룹 또는 그룹과 연결된 사용자를 프로비저닝하려면 엔터프라이즈 애플리케이션에 그룹 또는 사용자를 할당해야 합니다. 그러면 그룹 또는 사용자가 애플리케이션에 대한 로그인 권한(예: Cisco SD-WAN Manager)을 갖게 됩니다. Entra ID > Enterprise apps로 돌아가 엔터프라이즈 애플리케이션을 엽니다. 왼쪽 메뉴의 Manage(관리) 섹션에서 Users and groups(사용자 및 그룹)를 클릭합니다.



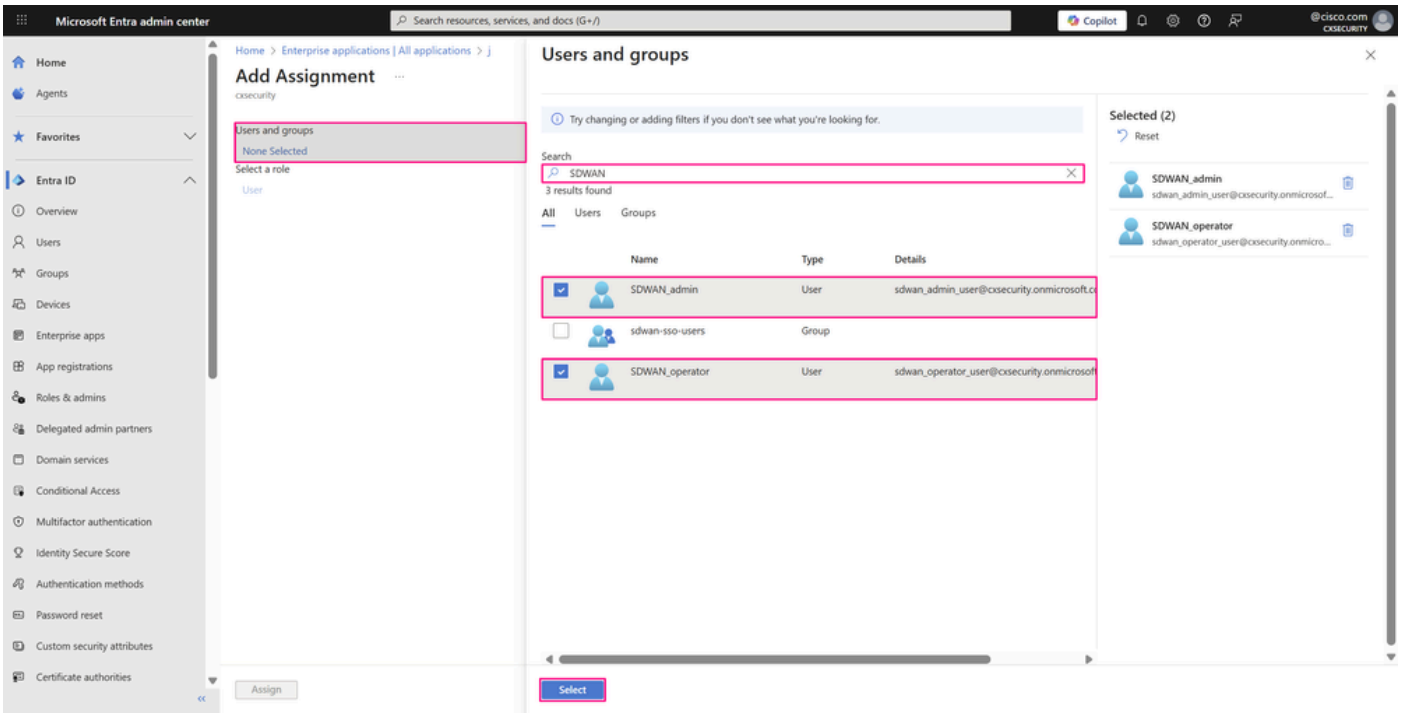
SAML을 사용하는 SSO 구성 페이지

- 그런 다음 사용자/그룹 추가를 클릭합니다.



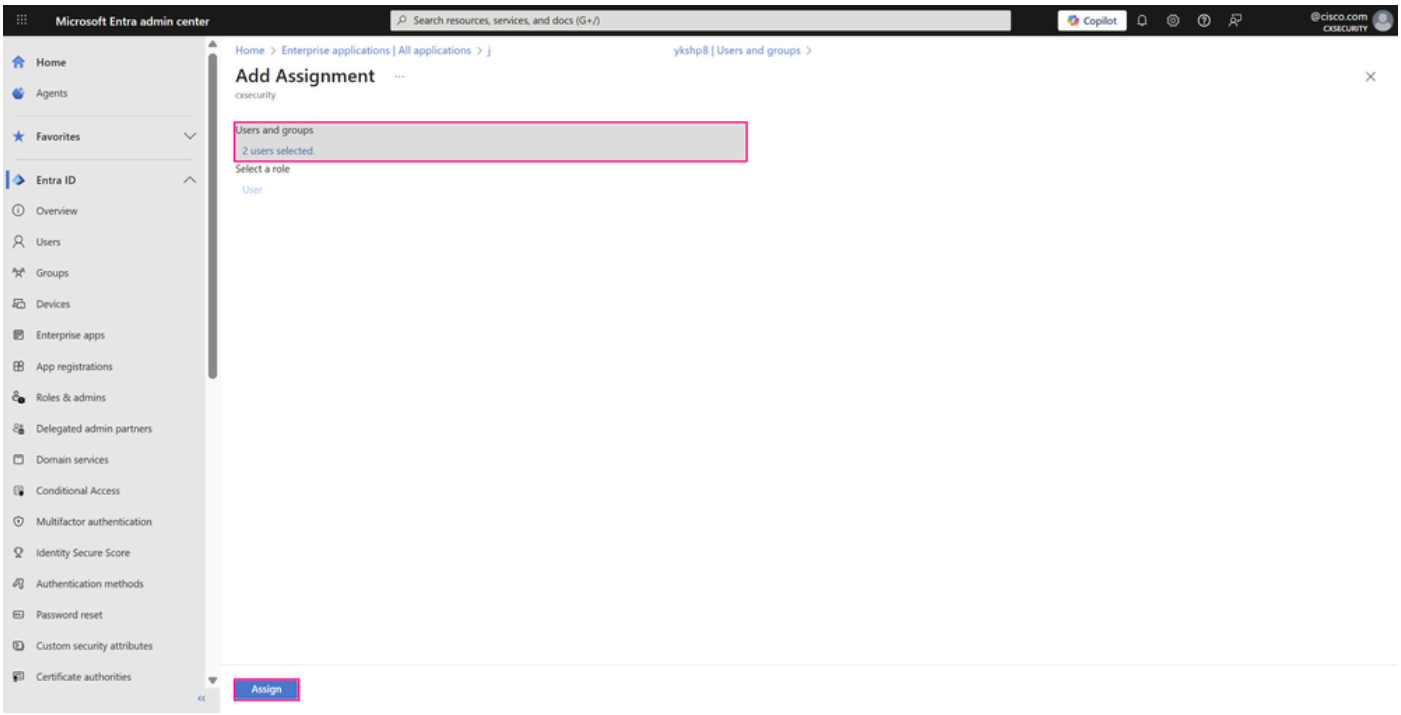
사용자 및 그룹 페이지

- Add Assignment(할당 추가) 창의 Users and groups(사용자 및 그룹) 필드에서 None Selected(선택 안 함)를 클릭합니다. 이전 단계에서 생성한 두 명의 사용자를 사용하여 응용 프로그램에 할당할 사용자 또는 그룹을 검색하고 선택한 다음 Select(선택)를 클릭합니다.



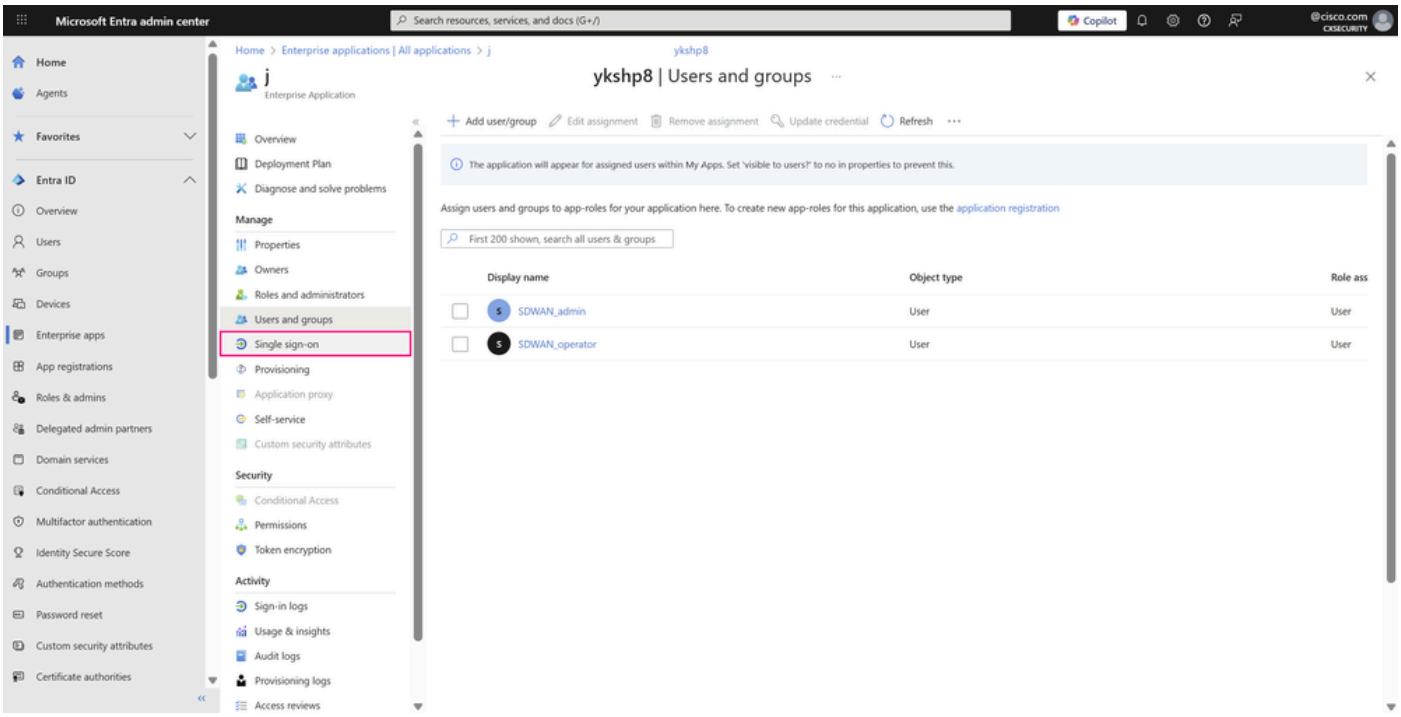
User/Group Assignment 창

- Assign(할당)을 클릭하여 사용자 또는 그룹을 애플리케이션에 할당합니다.



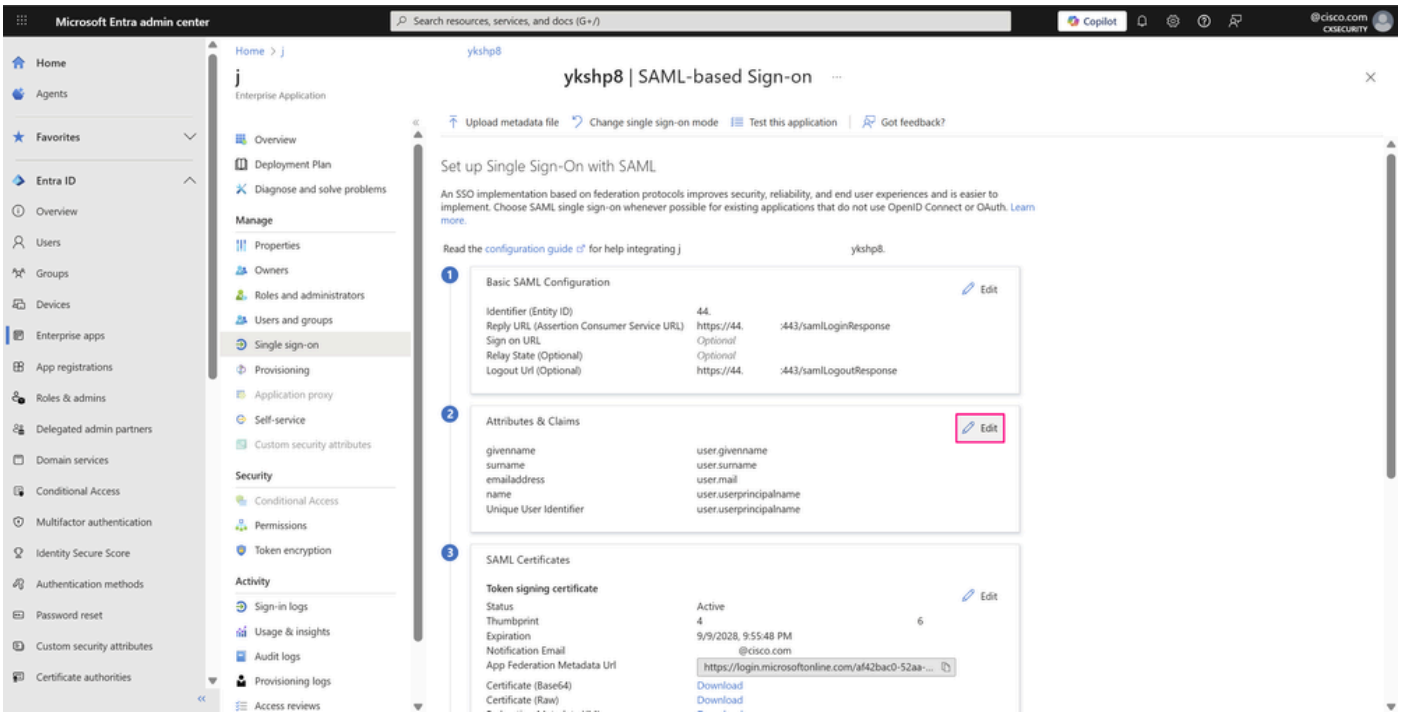
User/Group Assignment 창

- 엔터프라이즈 애플리케이션에 할당된 사용자는 할당 직후 나열됩니다. 왼쪽 메뉴의 Manage(관리) 섹션에서 Single sign-on을 클릭하여 애플리케이션의 SSO SAML 컨피그레이션에 액세스하고 나머지 필수 컨피그레이션을 완료합니다.



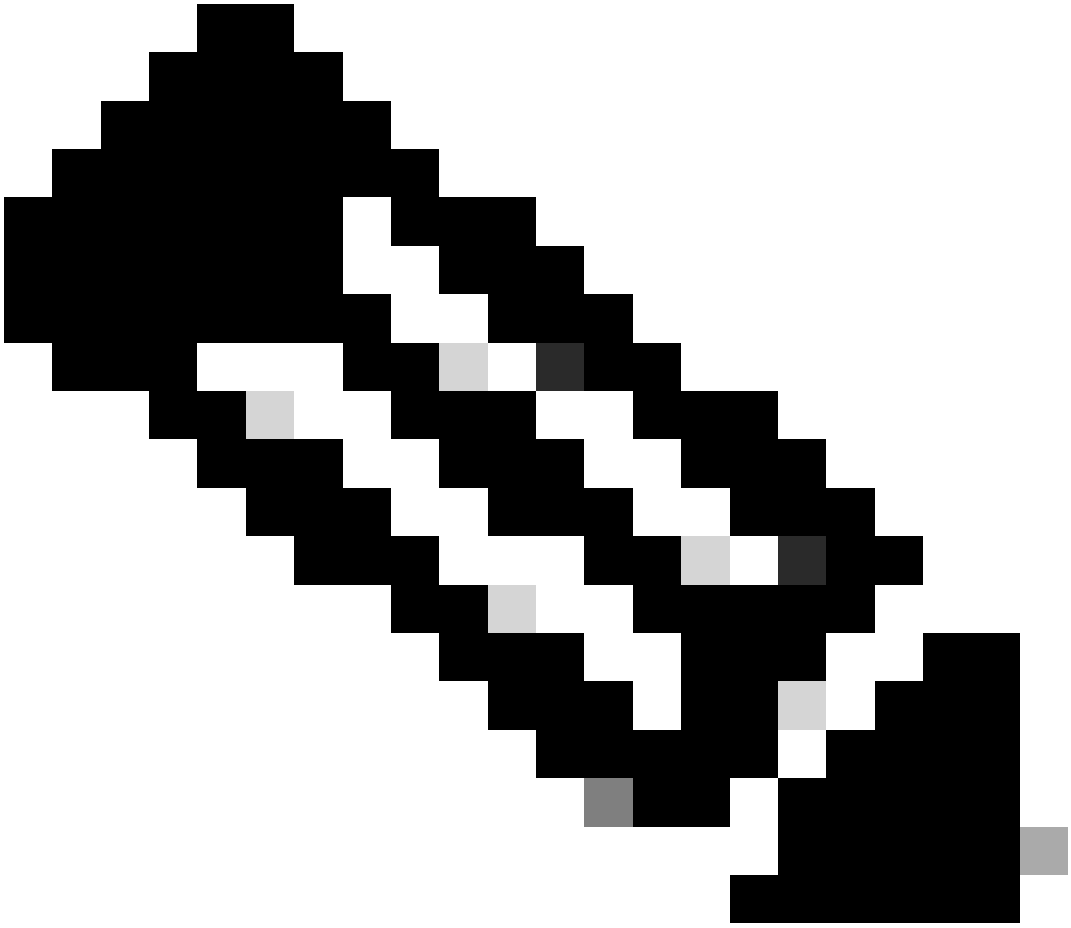
사용자 및 그룹 페이지

- SAML을 사용하여 단일 로그인 설정 페이지의 속성 및 클레임에서 편집을 클릭합니다.

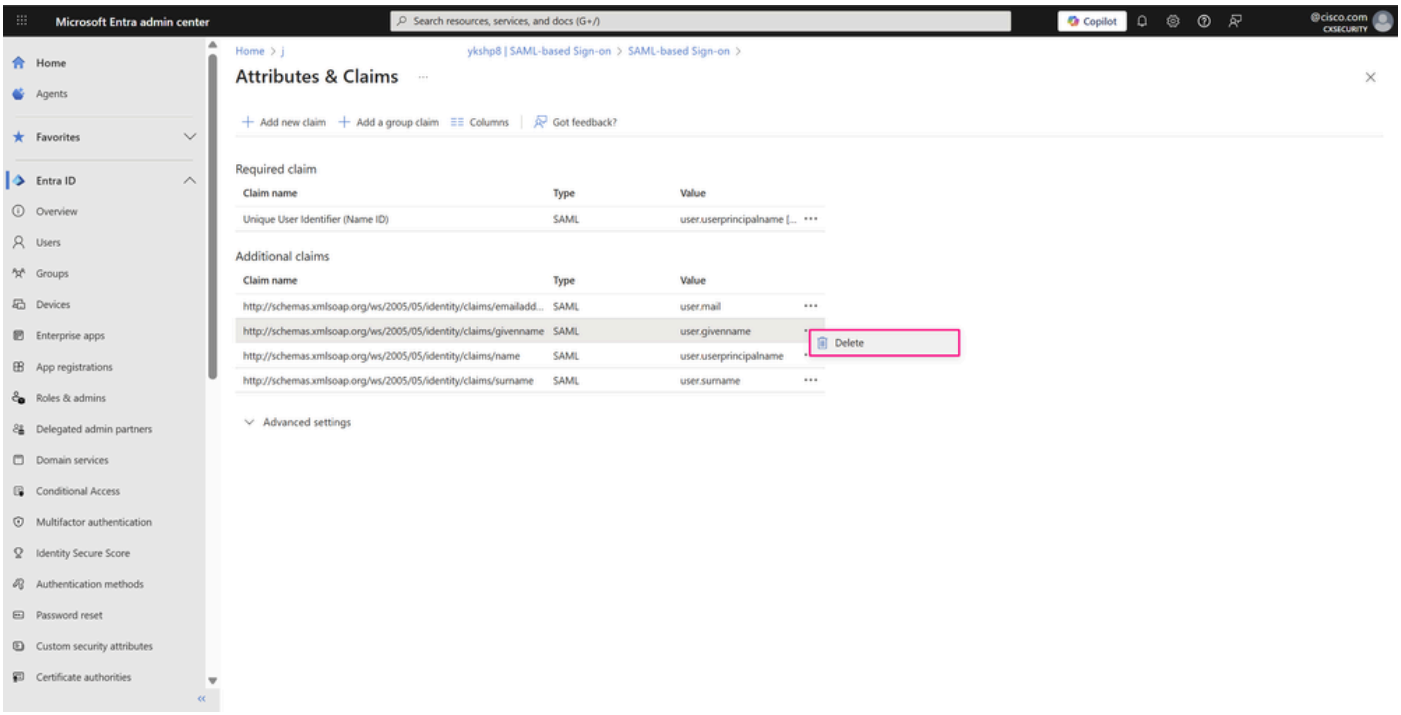


SAML을 사용하는 SSO 구성 페이지

- 속성 및 클레임 페이지에서 3점 아이콘을 클릭한 다음 삭제를 클릭하여 user.givenname 값의 클레임과 user.surname 값의 클레임을 제거합니다. 이 예제에는 클레임이 필요하지 않습니다 .¶응용 프로그램에 대한 기본 SSO 인증에는 다음 클레임만 필요합니다.
    - user-user.mail의 이메일 주소
    - user-user.userprincipalname의 UPN(User Principal Name)

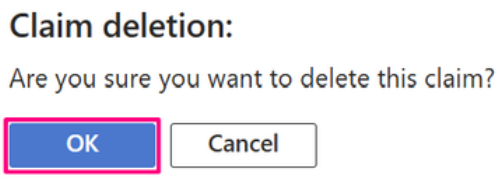


참고: 조직의 특정 요구에 따라 추가 청구가 필요할 수 있습니다.



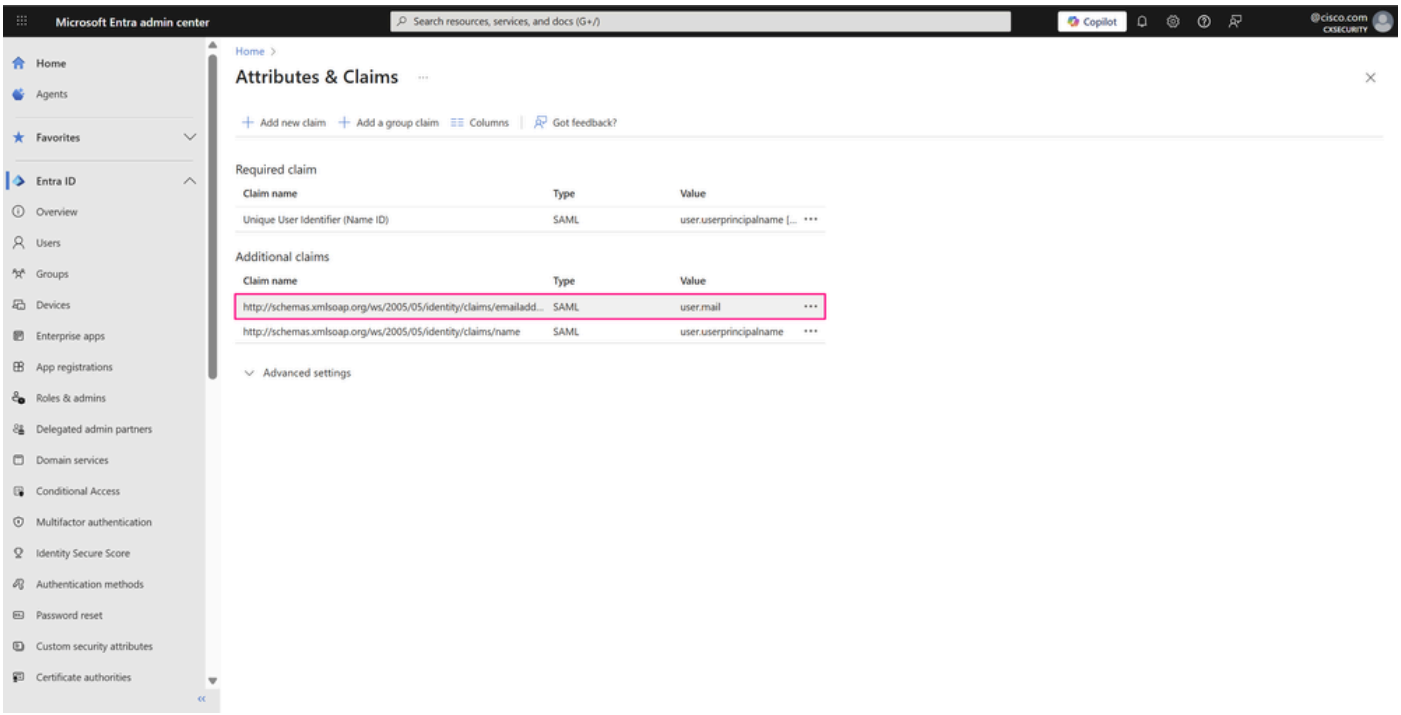
속성 및 클레임 페이지

- 청구 삭제 창에서 확인을 눌러 청구를 삭제합니다.



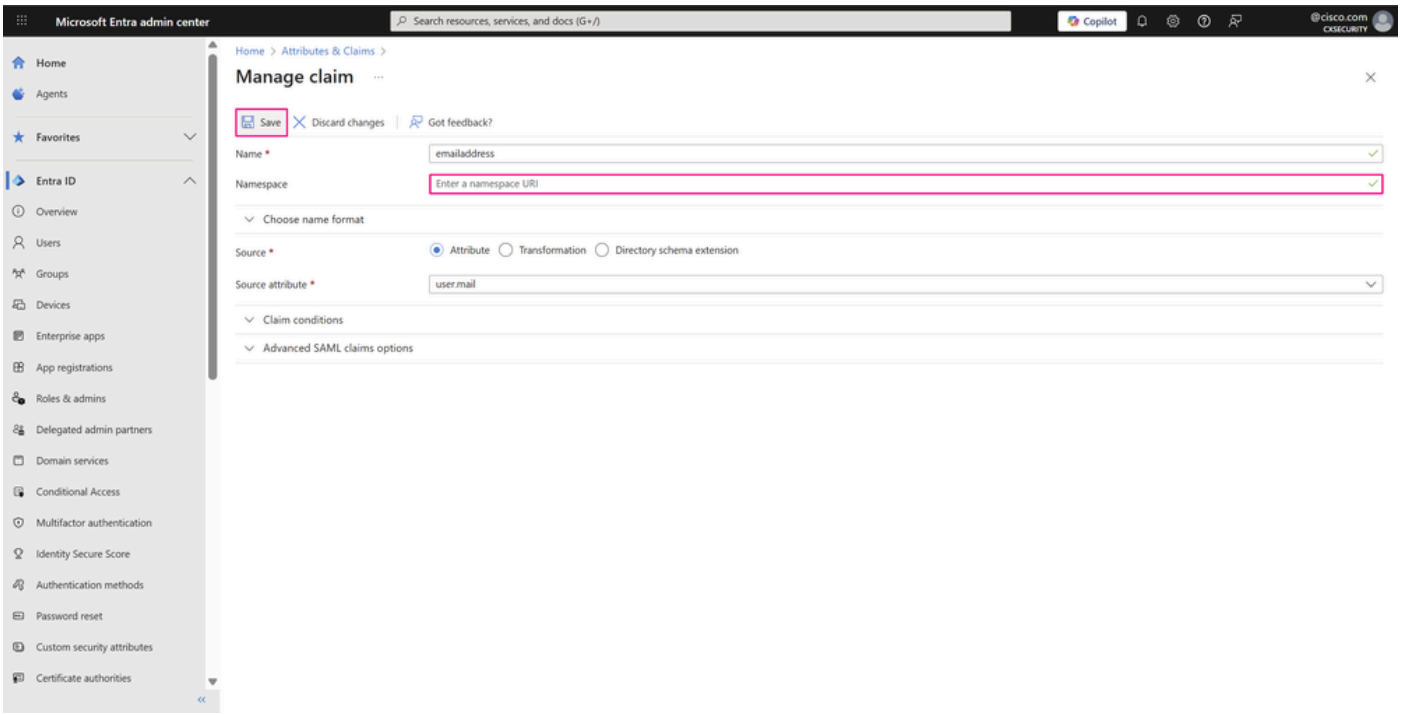
청구 삭제 창

- 다음으로, 이 필드는 선택 사항이므로 나머지 두 클레임의 클레임 이름에서 네임스페이스를 제거합니다. 이렇게 변경하면 더 쉽게 식별할 수 있도록 각 항목의 실제 이름이 이 페이지에 표시됩니다. 각 클레임 위에 마우스를 올려놓고 클릭하여 해당 설정에 액세스합니다.



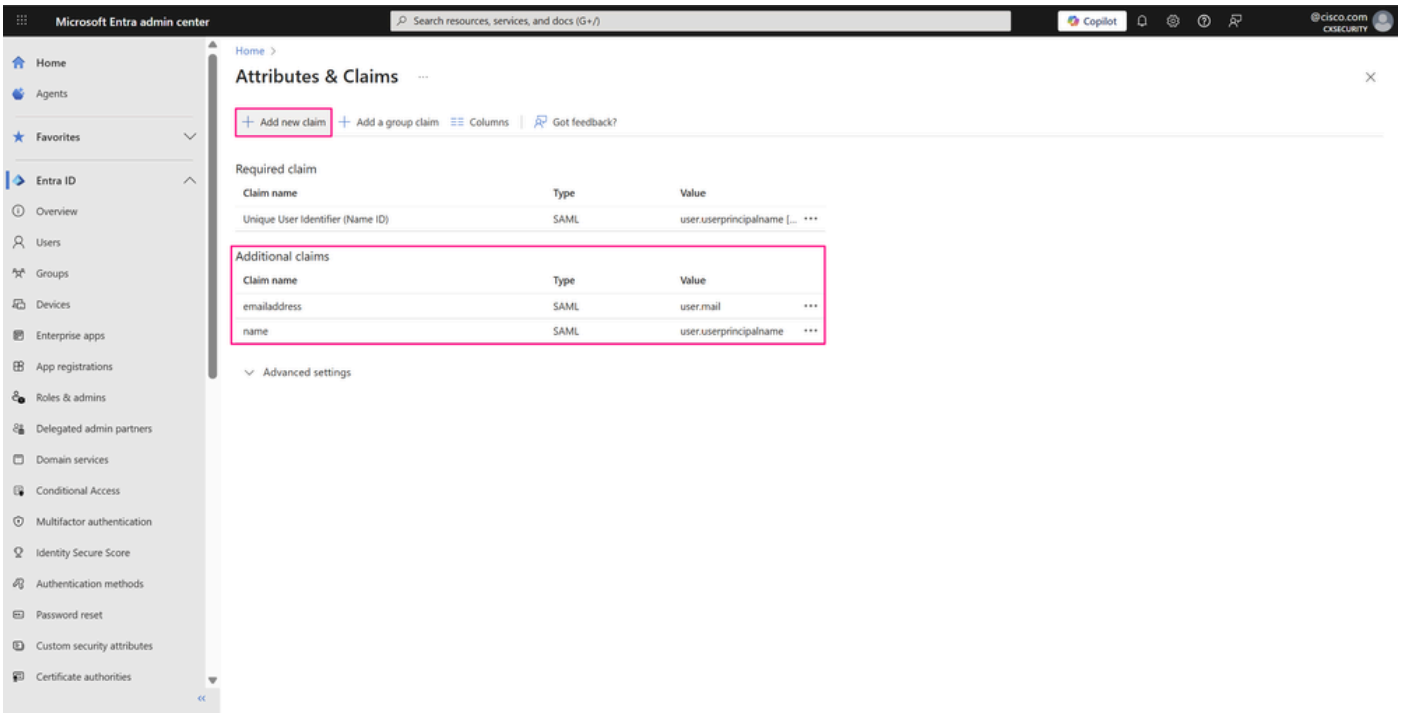
속성 및 클레임 페이지

- 클레임 관리 페이지에서 네임스페이스 필드를 삭제하고 저장을 클릭하여 변경 내용을 적용합니다.



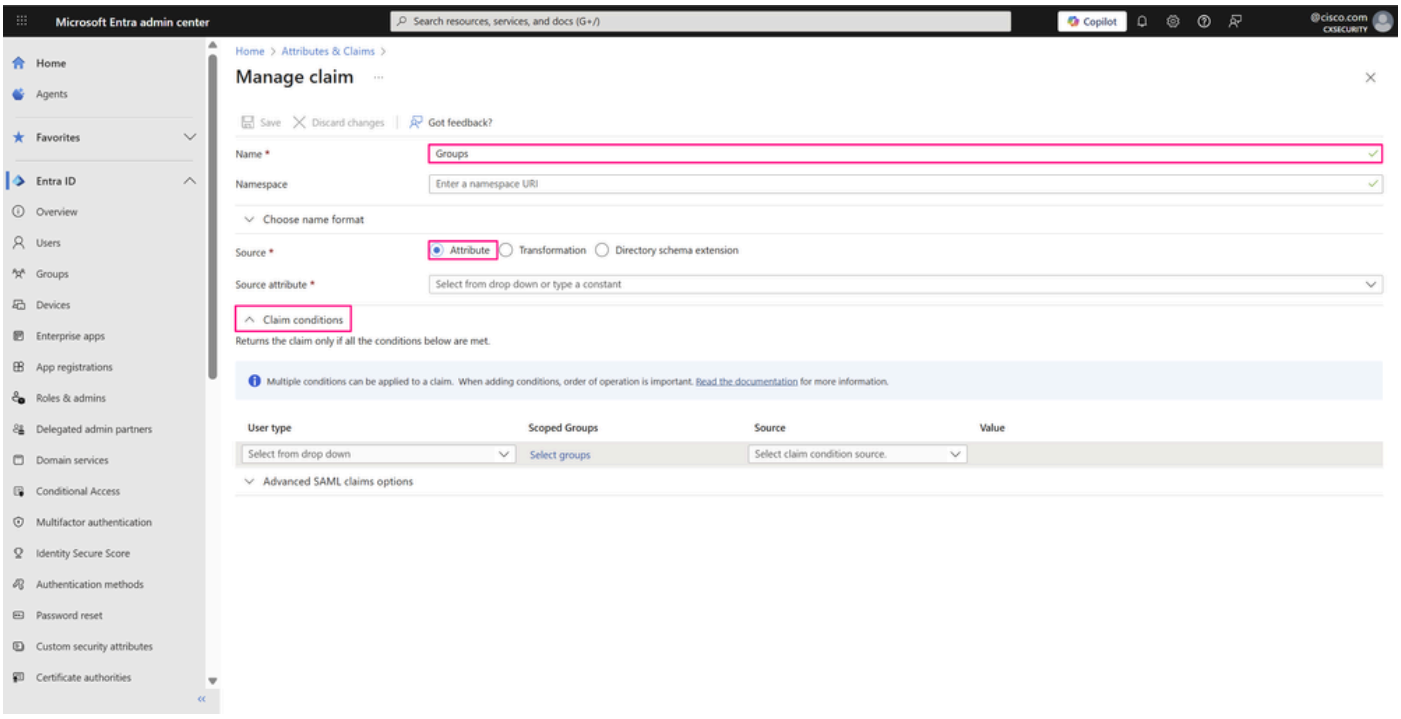
클레임 관리 페이지

- 이제 필요한 두 청구의 이름을 볼 수 있습니다. 그러나 사용자가 속하고 애플리케이션 리소스에 액세스할 권한이 있는 그룹을 정의하려면 추가 클레임이 여전히 하나 더 필요합니다. 이렇게 하려면 새 클레임 추가를 클릭합니다.



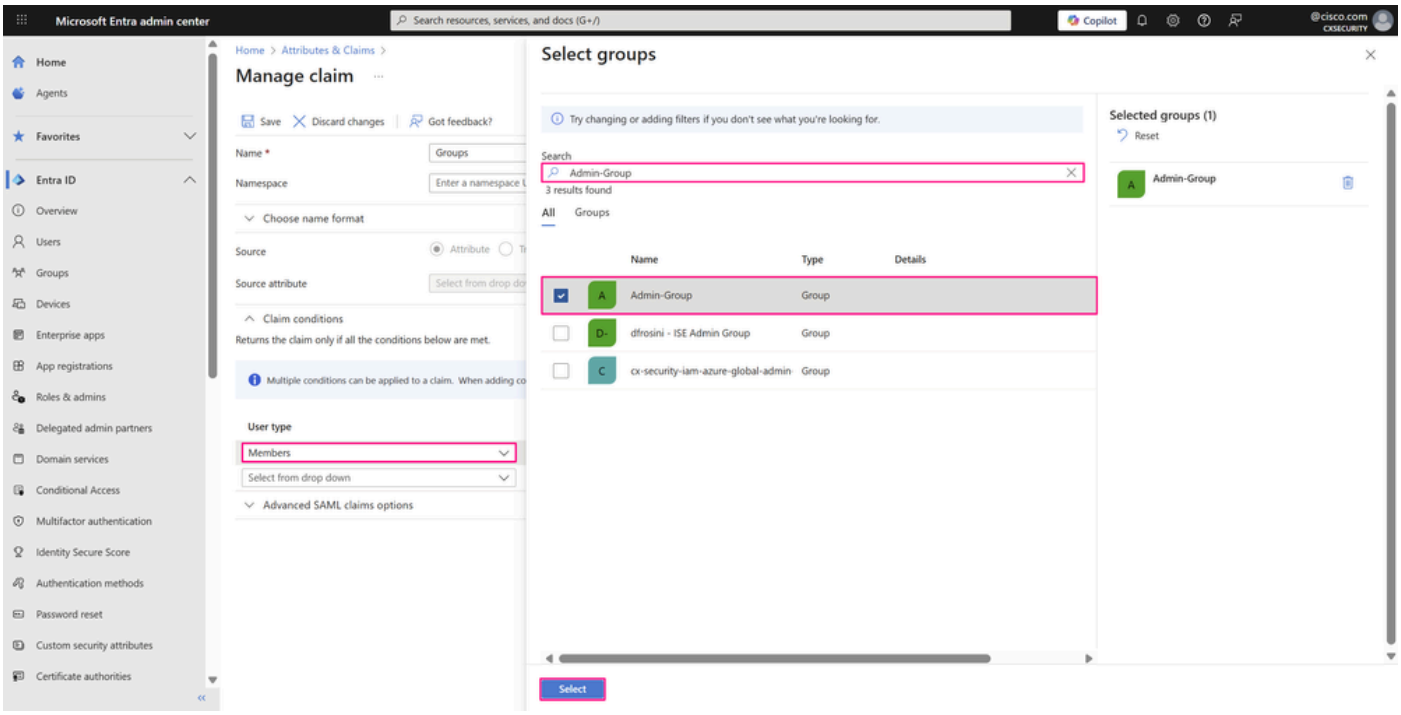
속성 및 클레임 페이지

- 이 클레임을 식별하는 이름을 입력하십시오. Source(소스) 옆에서 Attribute(특성)를 선택합니다. 그런 다음 Claim conditions(클레임 조건)를 클릭하여 옵션을 확장하고 여러 조건을 구성합니다.



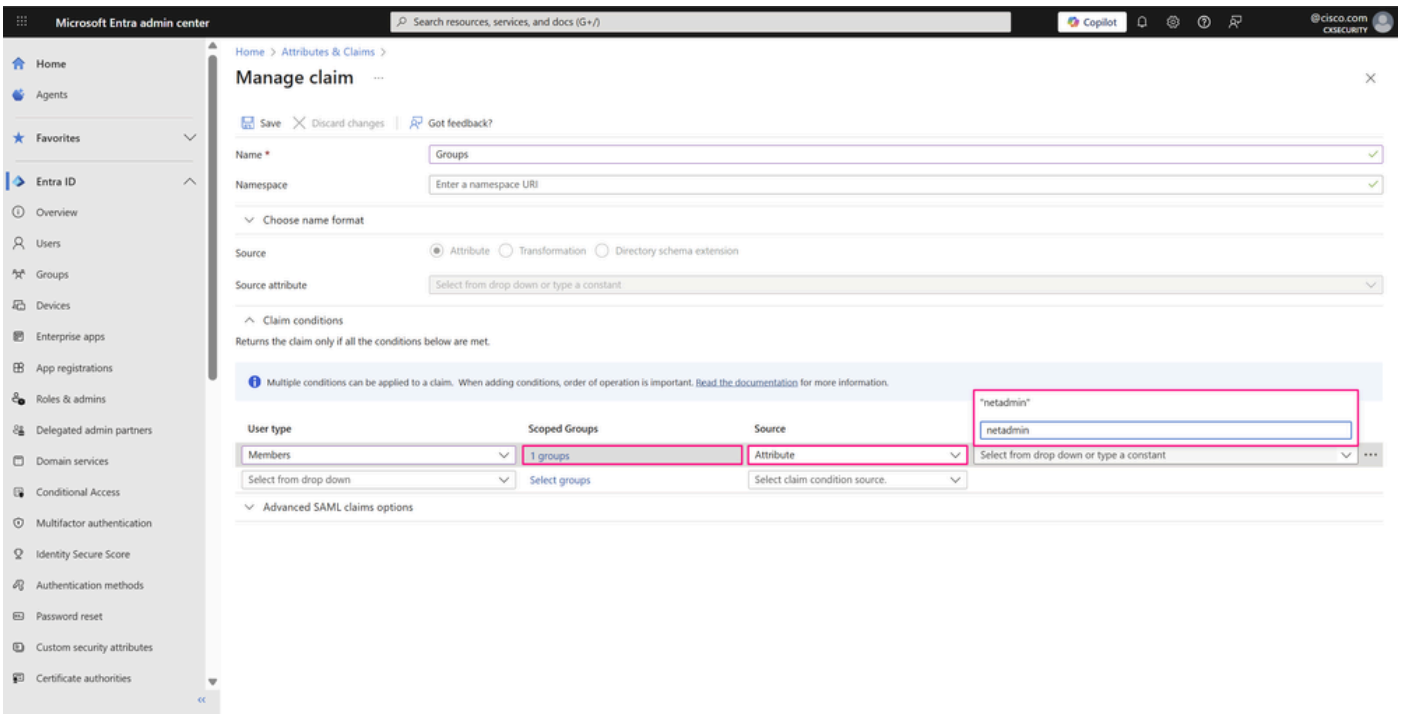
클레임 관리 페이지

- 클레임 조건의 사용자 유형 드롭다운 목록에서 구성원을 선택하고 그룹 선택을 클릭하여 사용자가 속해야 하는 그룹을 선택한 다음 선택을 클릭합니다.



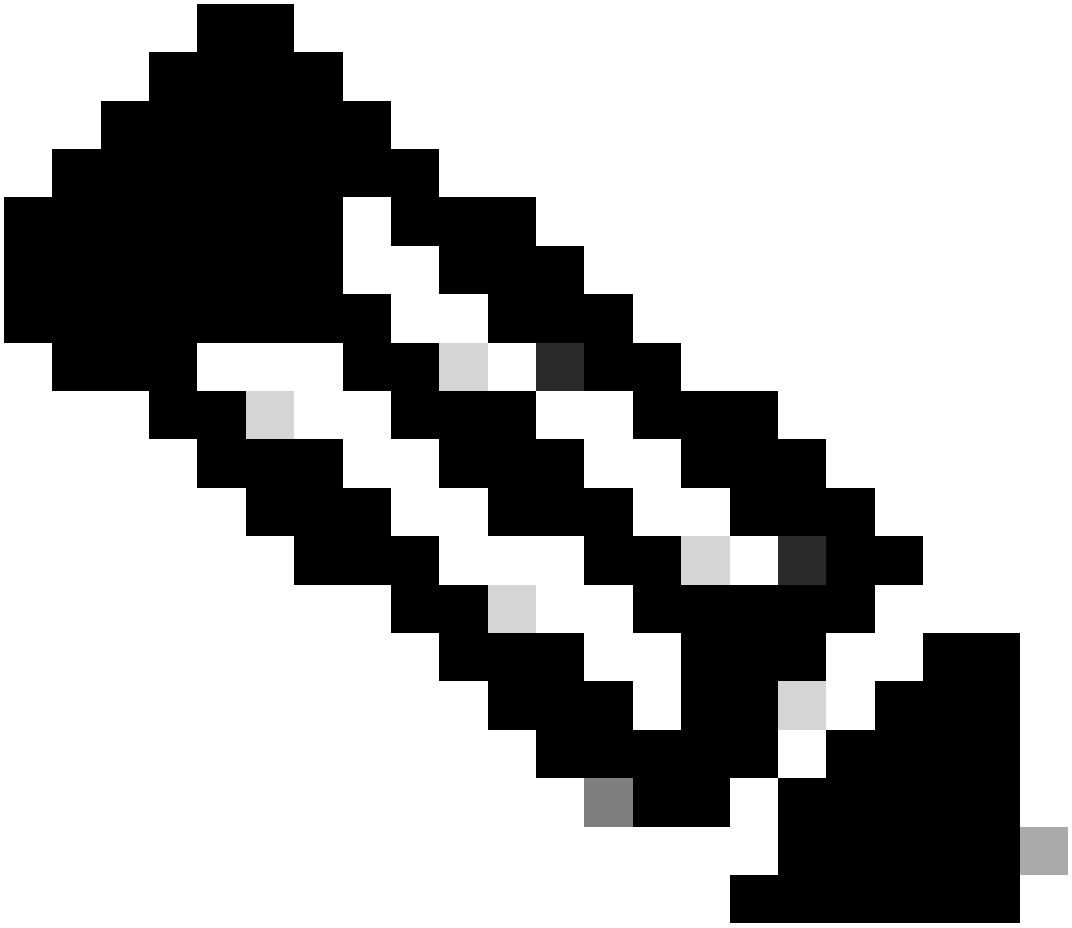
클레임 관리 페이지

- 클레임이 값을 검색하는 Source 드롭다운 목록에서 Attribute를 선택합니다. 응용 프로그램에 정의된 사용자 그룹을 참조하는 사용자의 사용자 지정 특성을 값 필드에 입력합니다. 이 예에서 netadmin은 Cisco SD-WAN Manager의 표준 사용자 그룹 중 하나입니다. 특성 값을 따옴표 없이 입력하고 Enter 키를 누릅니다.

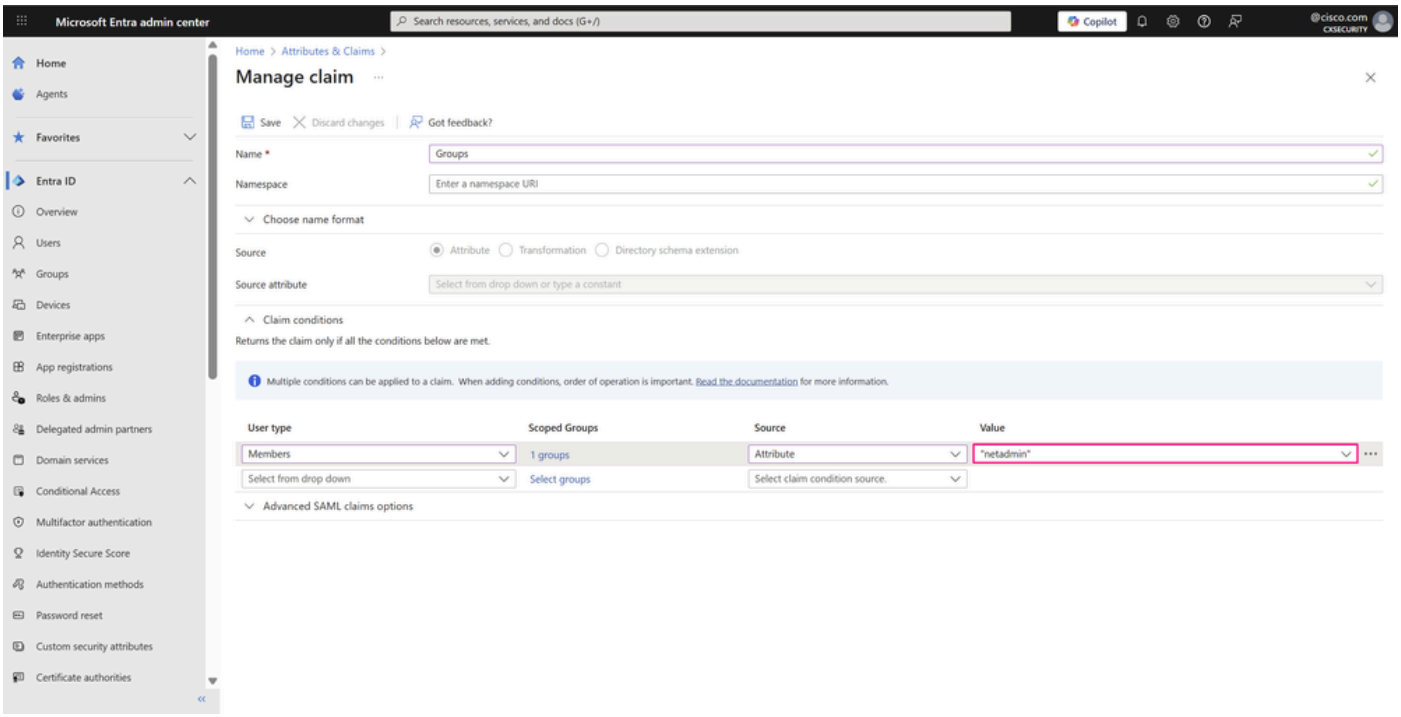


클레임 관리 페이지

- 바로 뒤에 Microsoft Centera ID가 이 값을 문자열로 처리하기 때문에 특성 값이 따옴표와 함께 나타납니다.

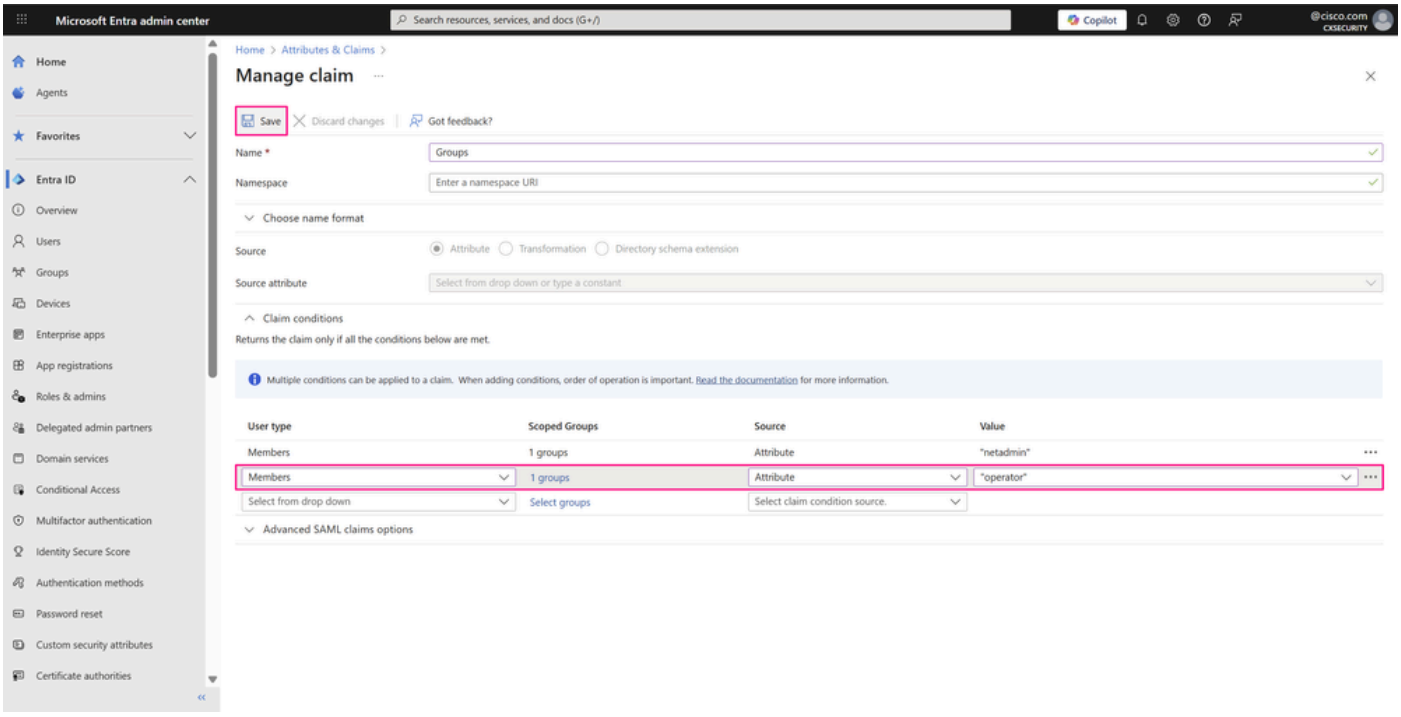


참고: 클레임 조건 내의 이러한 매개변수는 Cisco SD-WAN Manager에 정의된 사용자 그룹과 항상 일치해야 하므로 엔터프라이즈 애플리케이션의 SSO SAML 컨피그레이션에서 매우 관련성이 높습니다. 이 일치는 Microsoft Entra ID에서 사용자가 속한 그룹을 기반으로 사용자에게 부여되는 권한 또는 권한을 결정합니다.



클레임 관리 페이지

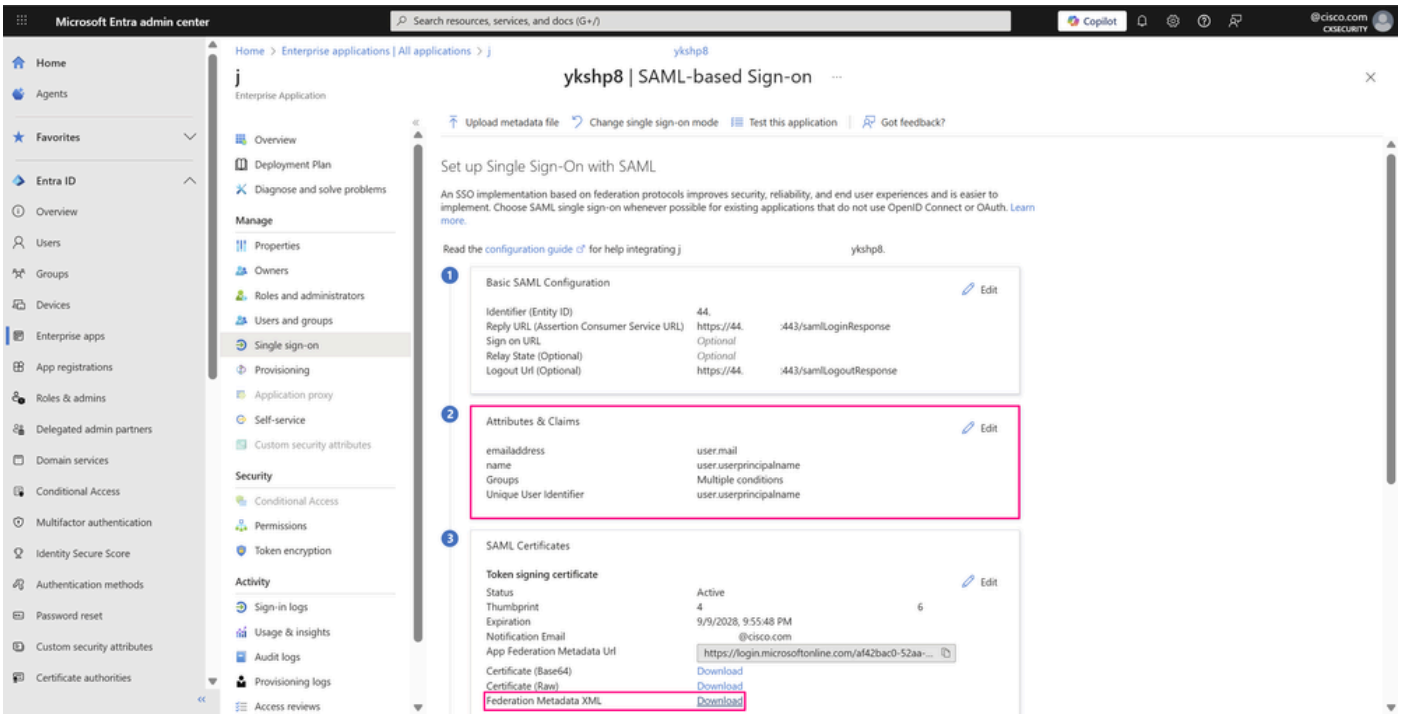
- Cisco SD-WAN Manager의 운영자 사용자 그룹에 매핑되는, 생성된 두 번째 그룹에 대한 두 번째 클레임 조건에 대해 동일한 단계를 반복합니다. 이 프로세스는 응용 프로그램에 로그인하려는 특정 권한이 있는 서로 다른 각 그룹에 필요합니다. 단일 조건 내에 여러 그룹을 추가할 수도 있습니다. Save(저장)를 클릭하여 변경 사항을 저장합니다.



클레임 관리 페이지

- SAML을 사용하여 Single Sign-On 설정 페이지에서 속성 및 클레임 섹션에 변경된 사항이 표시됩니다. Microsoft Entra ID의 컨피그레이션을 완료하려면 SAML Certificates(SAML 인증서)에서 Federation Metadata XML(페더레이션 메타데이터 XML) 옆의 Download(다운로드)를

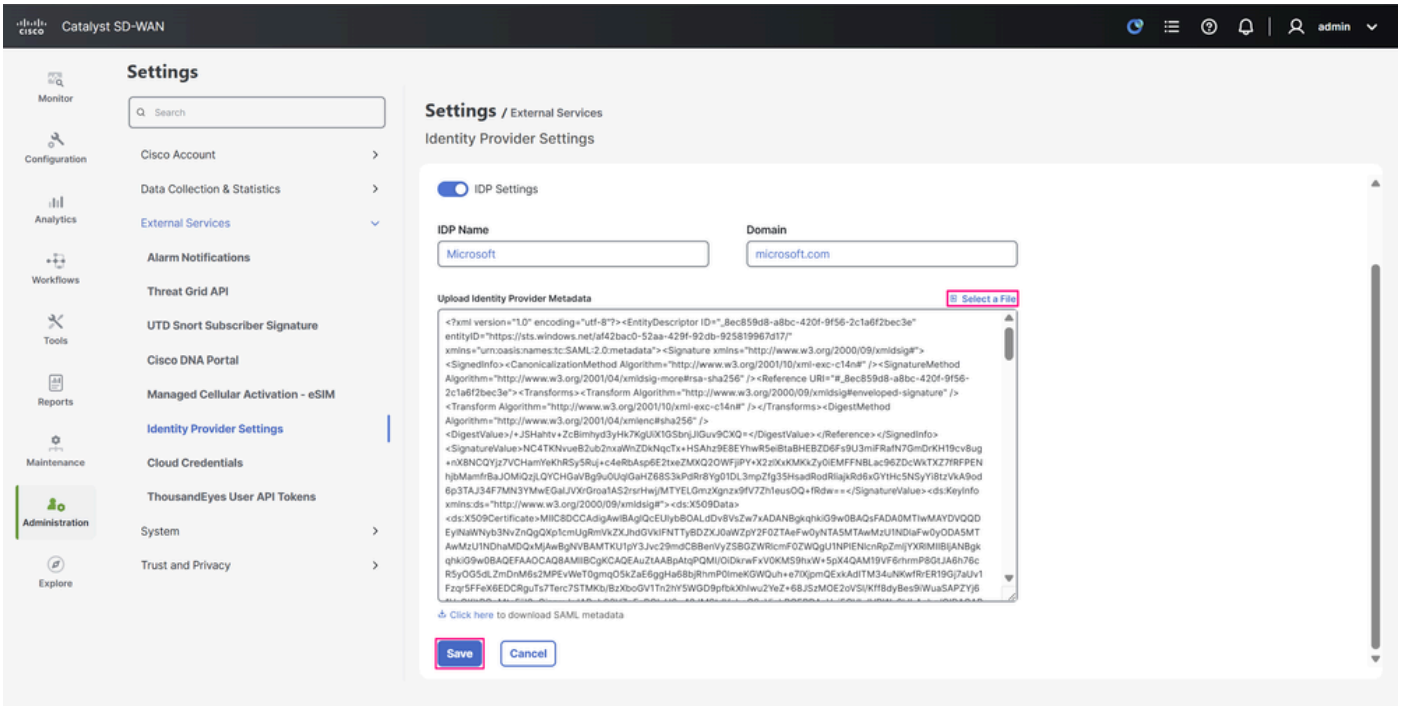
클릭하여 애플리케이션에 ID 서비스를 제공하는 XML 파일을 다운로드합니다.



SAML을 사용하는 SSO 구성 페이지

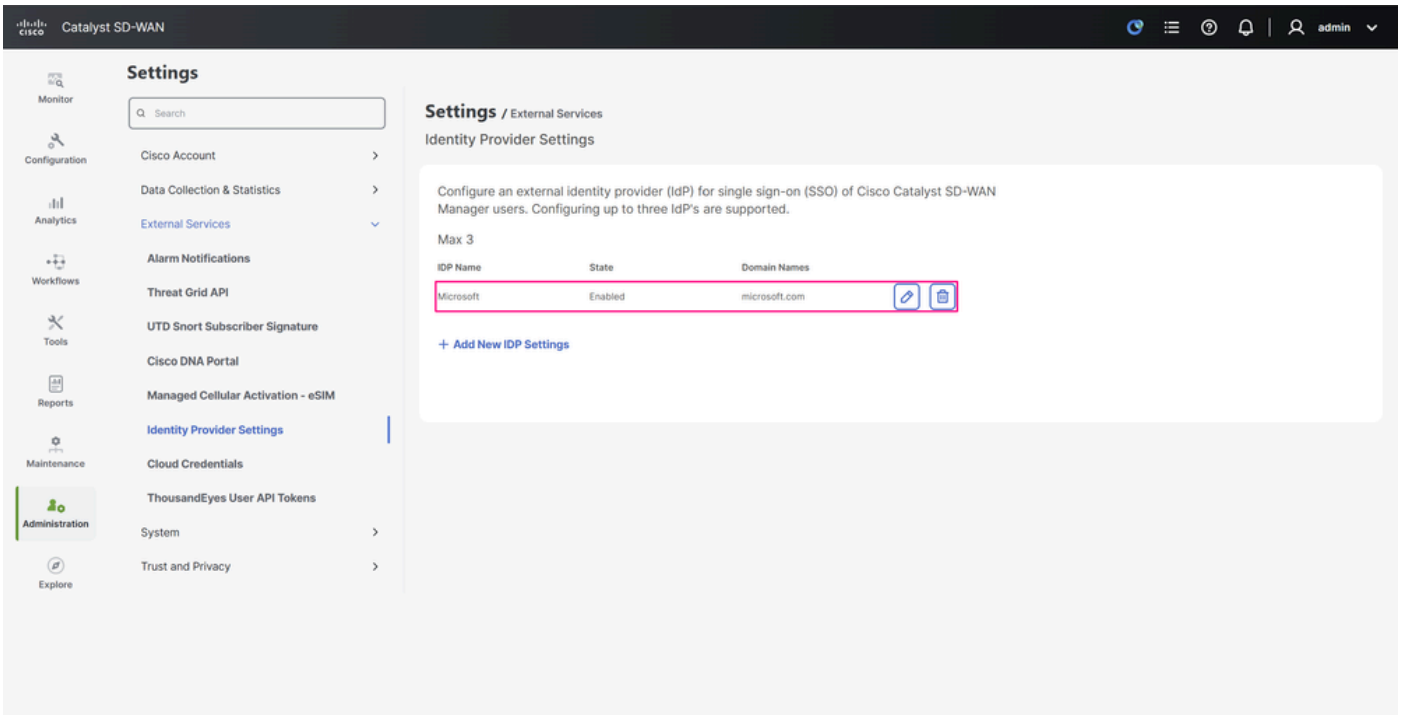
5단계. Microsoft Entra ID SAML 메타데이터 파일을 Cisco SD-WAN Manager로 가져옵니다.

- 페더레이션 메타데이터를 Cisco SD-WAN Manager에 업로드하려면 Administration(관리) > Settings(설정) > External Services(외부 서비스) > Identity Provider Settings(ID 제공자 설정)로 이동하고 Select a file(파일 선택)을 클릭합니다. Microsoft Entra ID에서 방금 다운로드한 파일을 선택한 다음 저장을 클릭합니다.



IdP 설정 구성 페이지

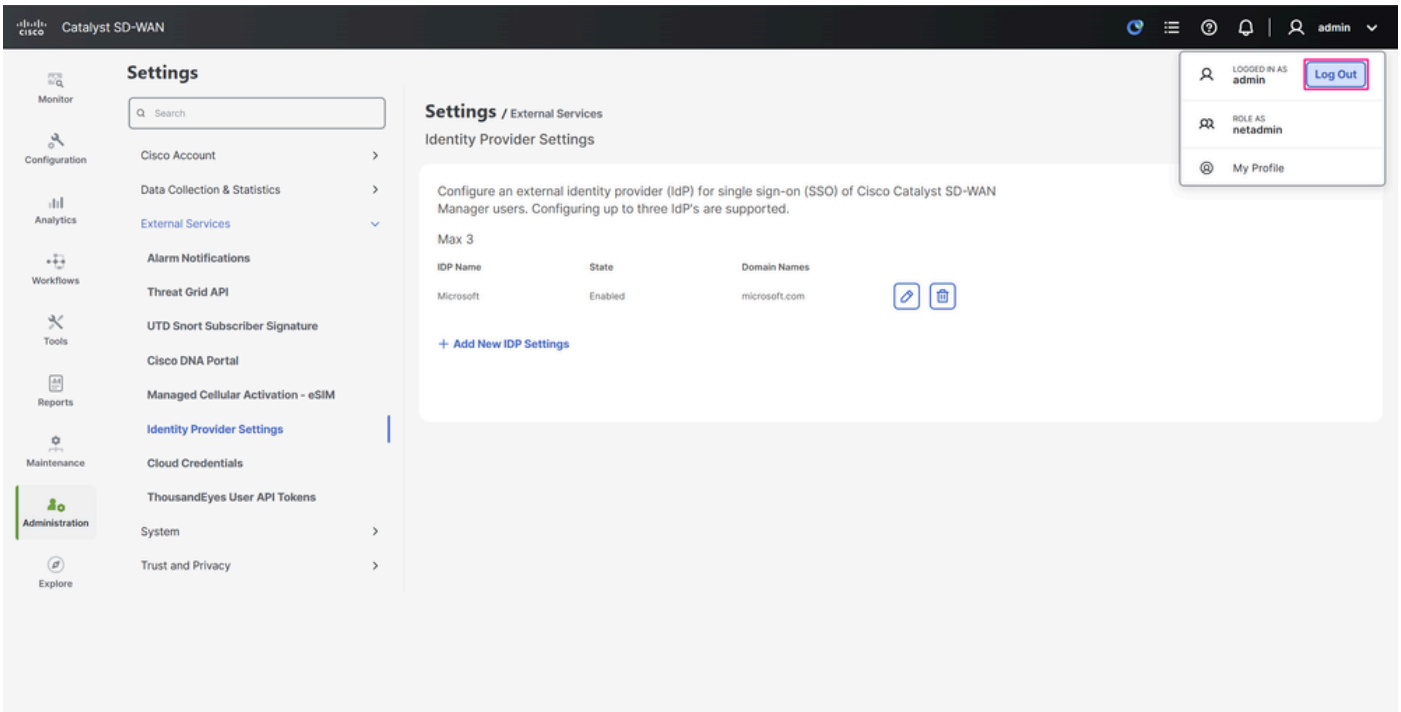
- 이제 IdP 설정 및 메타데이터가 저장됩니다.



IdP 설정 구성 페이지

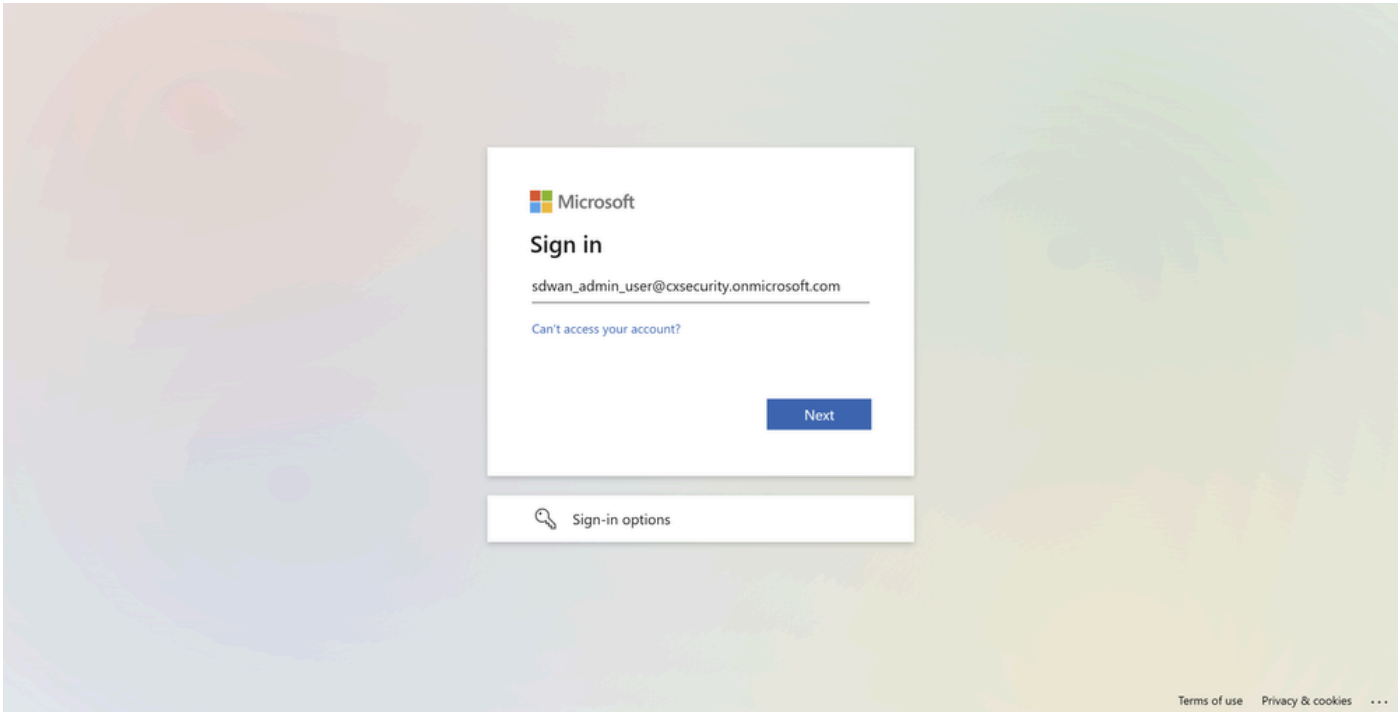
다음을 확인합니다.

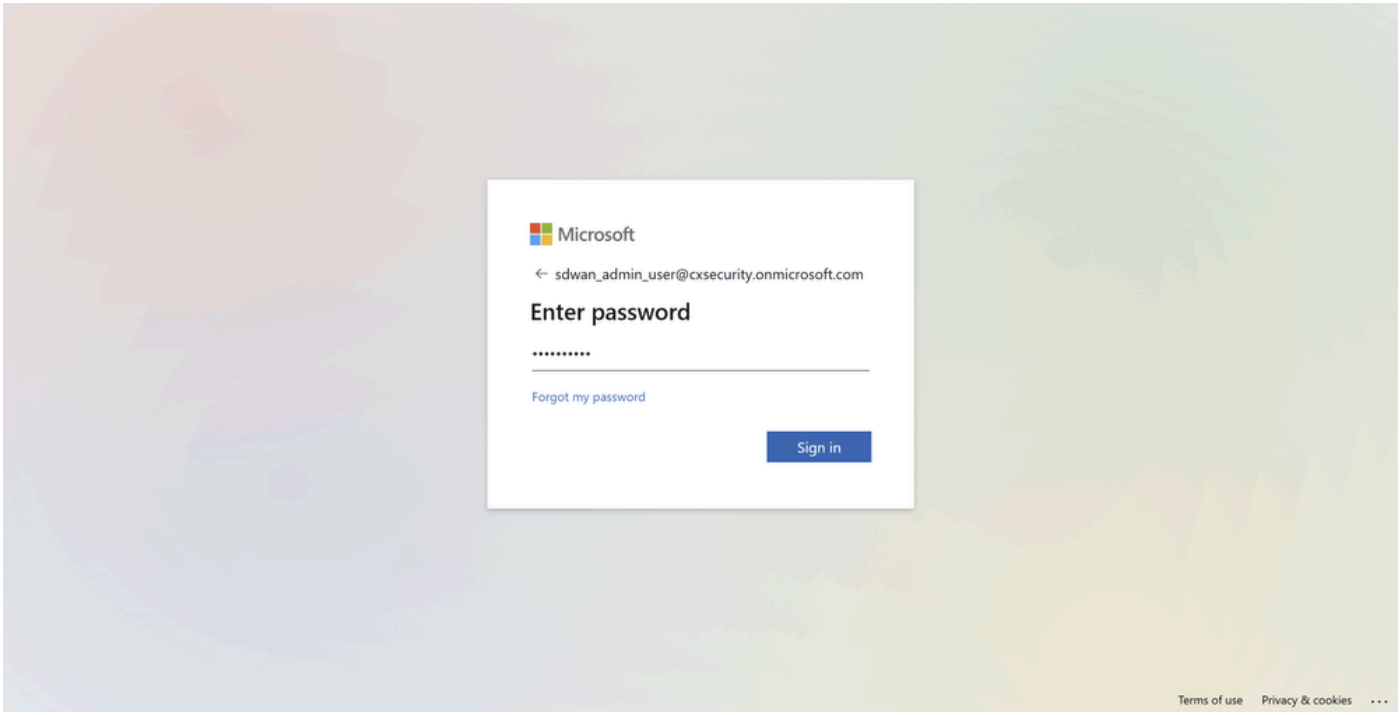
- UI의 오른쪽 상단 모서리에서 프로필 이름을 클릭하여 옵션을 확장한 다음 Log Out(로그아웃)을 클릭하여 포털에서 로그아웃합니다.



프로필 메뉴

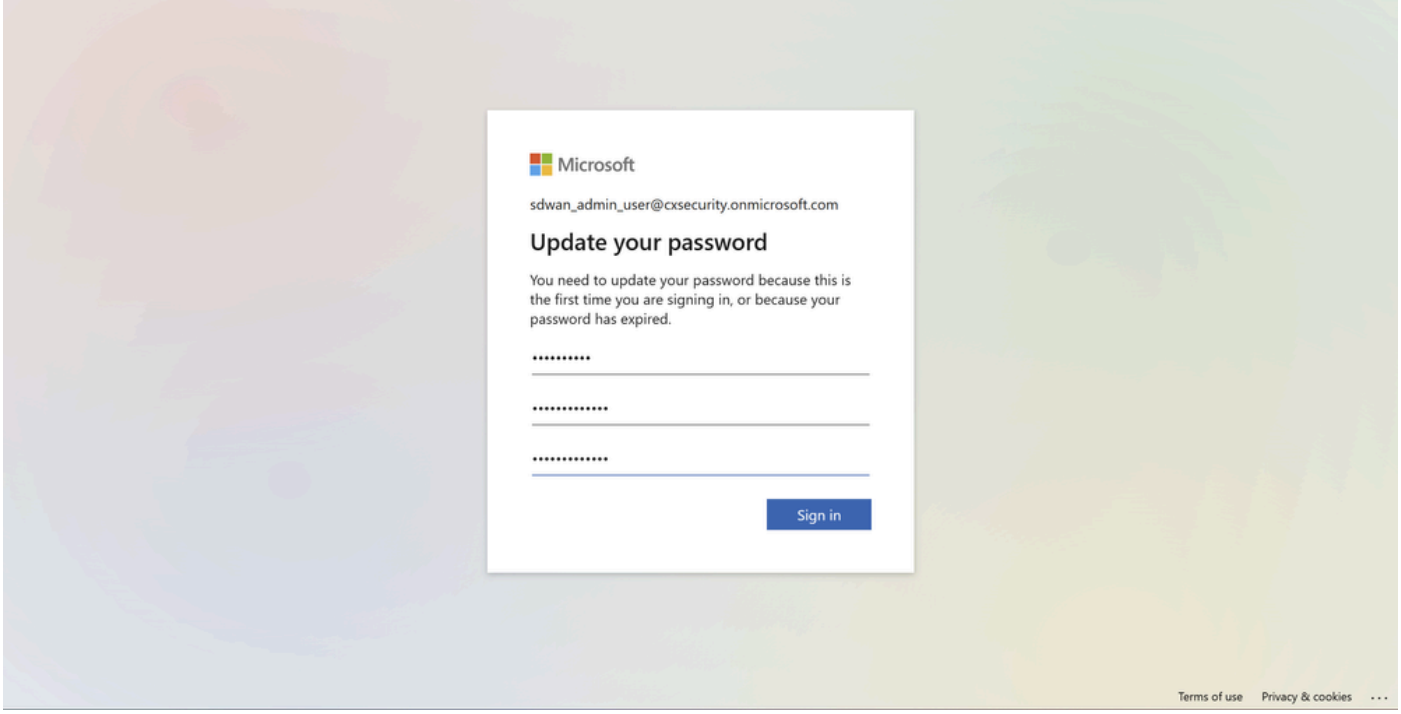
- Microsoft 인증 화면으로 즉시 리디렉션되며, 여기서 Microsoft Entra ID SSO 사용자의 자격 증명으로 로그인합니다.





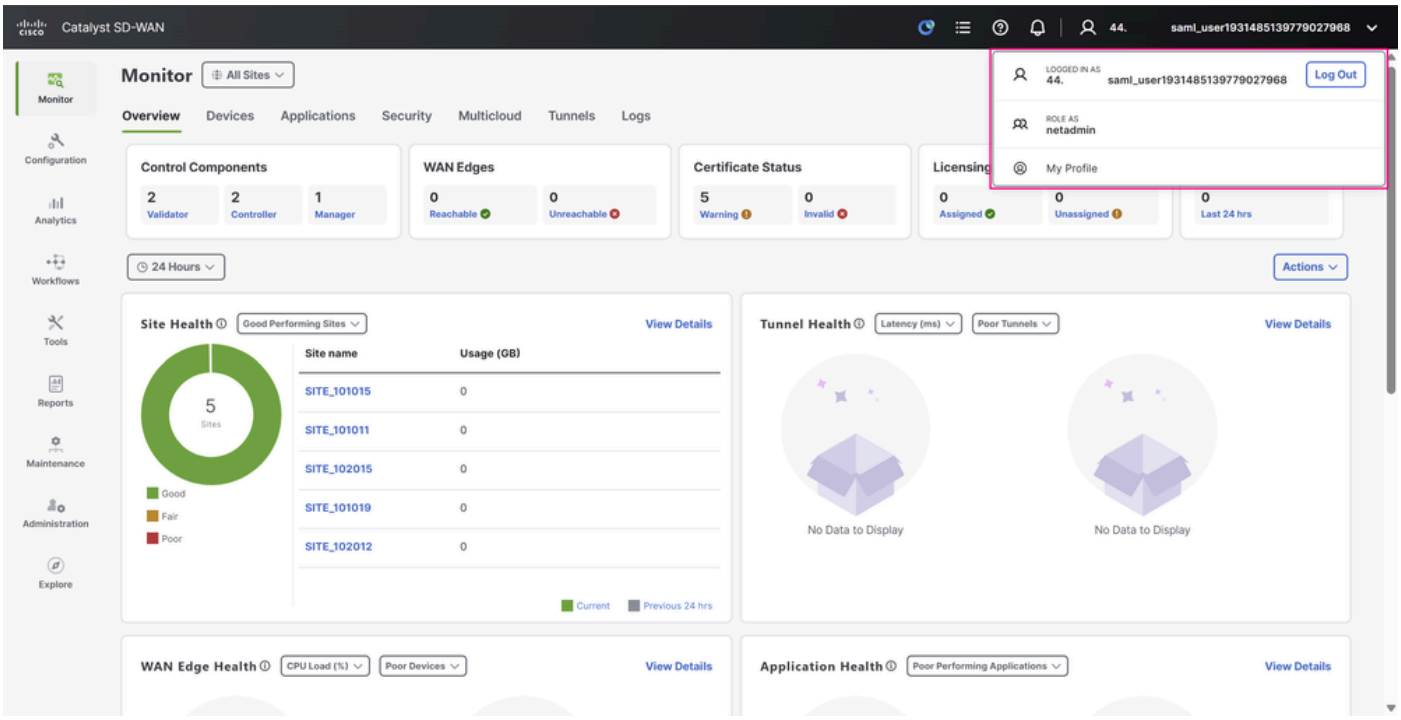
Microsoft 로그인 화면

- SSO 사용자가 처음으로 로그인하는 것이므로 프롬프트에서 비밀번호 변경을 요청합니다.



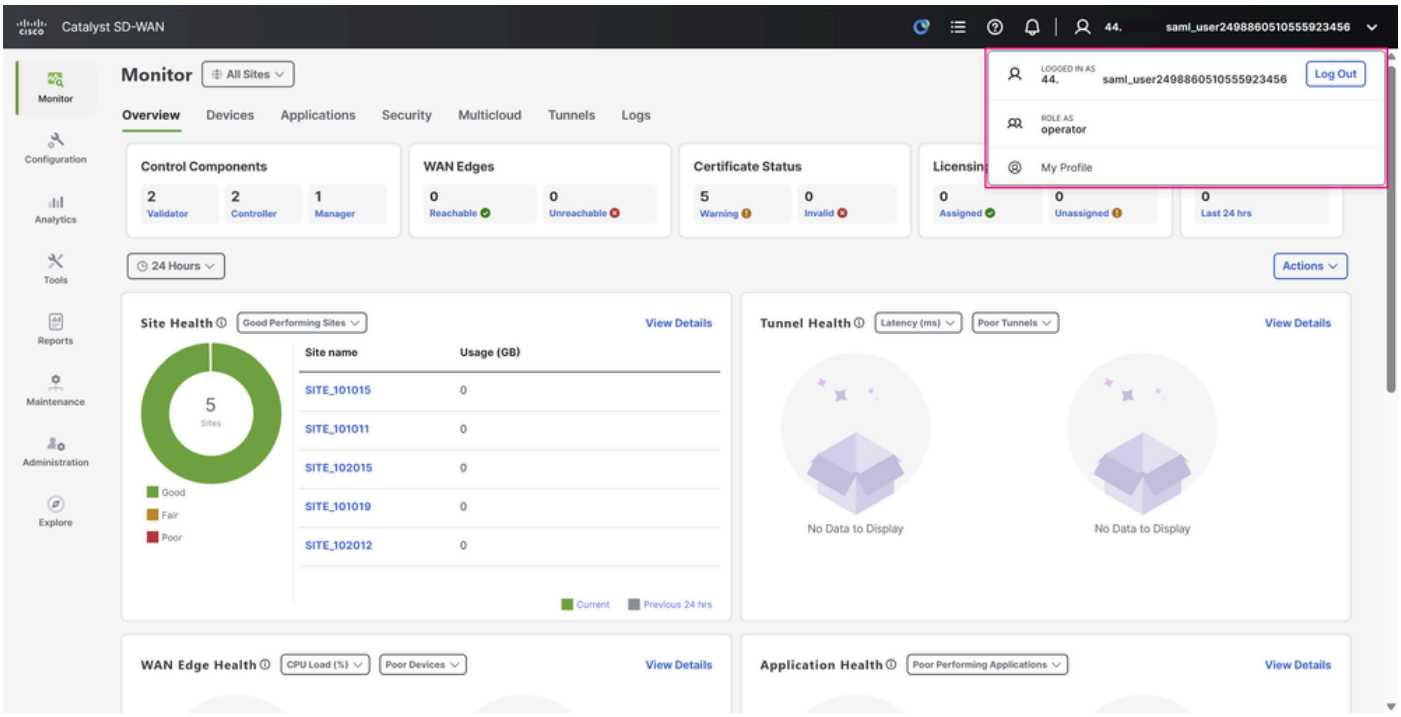
Microsoft 로그인 화면

- 로그인에 성공하면 대시보드의 오른쪽 상단 모서리에서 프로필 세부 정보를 다시 확장하고 Microsoft Entra ID에 구성된 것처럼 netadmin 역할로 사용자가 감지되었음을 확인할 수 있습니다.



Cisco SD-WAN Manager UI

- 마지막으로 다른 사용자와 동일한 로그인 테스트를 수행합니다. 동일한 동작이 표시됩니다. 이제 사용자가 운영자 역할로 식별됩니다.



Cisco SD-WAN Manager UI

관련 정보

- [Cisco IOS XE Catalyst SD-WAN에서 Single Sign-On 구성]

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.