Entra ID로 RA VPNaaS에 대한 Cisco Secure Access 구성

목차

소개

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소

구성

- Azure 구성
- Cisco Secure Access 컨피그레이션

다음을 확인합니다.

문제 해결

- 아주레
- Cisco 보안 액세스

소개

이 문서에서는 Cisco Secure Access에서 RA VPN을 구성하여 Entra ID에 대해 인증하는 방법에 대해 단계별로 설명합니다.

사전 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Azure/Entra ID를 사용하는 지식
- Cisco Secure Access에 대한 지식

요구 사항

다음 요건을 충족해야 계속 진행할 수 있습니다.

- Cisco Secure Access Dashboard에 전체 관리자로 액세스합니다.
- Azure에 관리자로 액세스합니다.
- Cisco Secure Access에 대한 사용자 프로비저닝이 이미 완료되었습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Secure Access 대시보드
- Microsoft Azure 포털.

- Cisco Secure Client AnyConnect VPN 버전 5.1.8.105

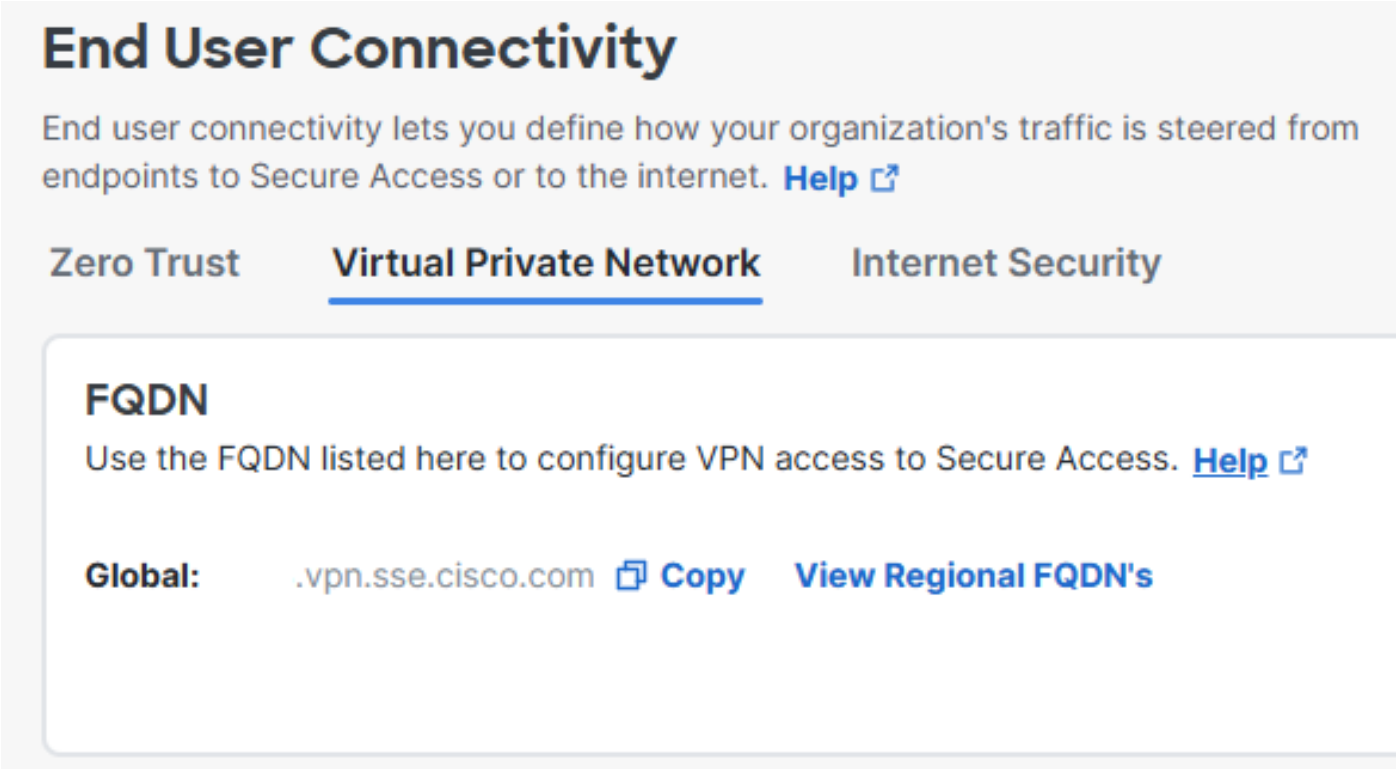
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

Azure 구성

1. Cisco Secure Access 대시보드에 로그인하고 VPN 전역 FQDN을 복사합니다. Azure 엔터프라이즈 응용 프로그램 구성에서 이 FQDN을 사용하고 있습니다.

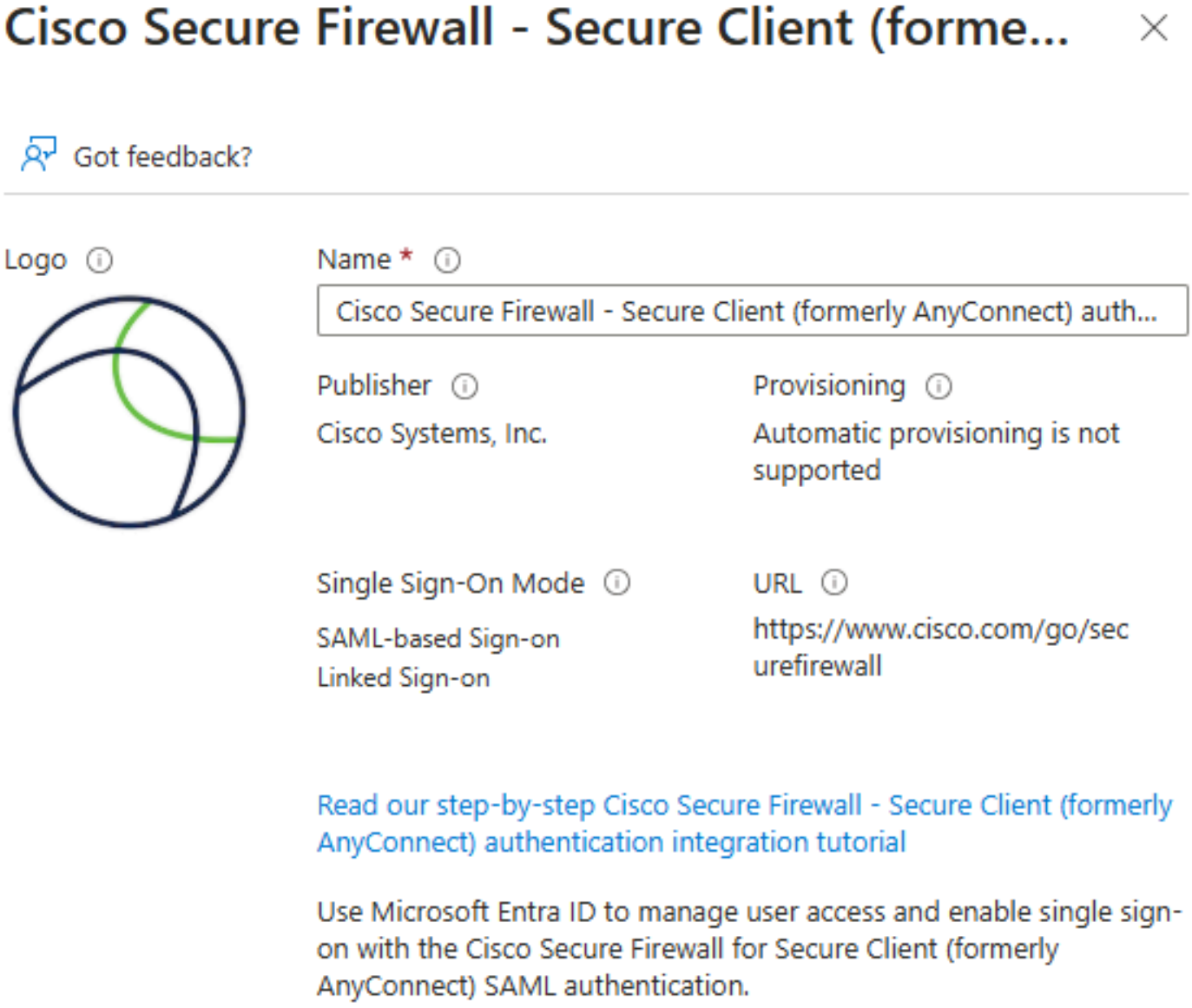
Connect(연결) > End User Connectivity(최종 사용자 연결) > Virtual Private Network(가상 사설망) > FQDN > Global(전역)



VPN 전역 FQDN

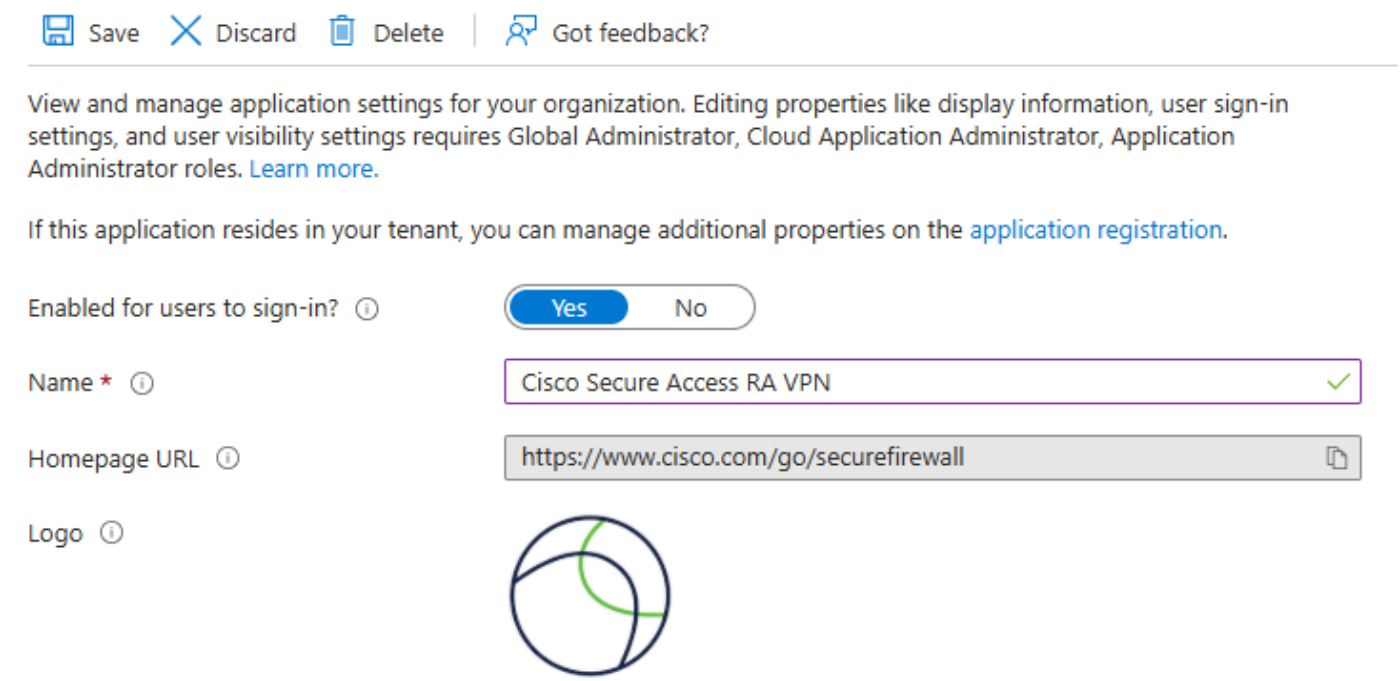
2. Azure에 로그인하여 RA VPN 인증을 위한 엔터프라이즈 응용 프로그램을 만듭니다. "Cisco Secure Firewall - Secure Client(이전의 AnyConnect) 인증"이라는 미리 정의된 응용 프로그램을 사용할 수 있습니다.

홈 > 엔터프라이즈 애플리케이션 > 새 애플리케이션 > Cisco Secure Firewall - Secure Client(이전의 AnyConnect) 인증 > 생성



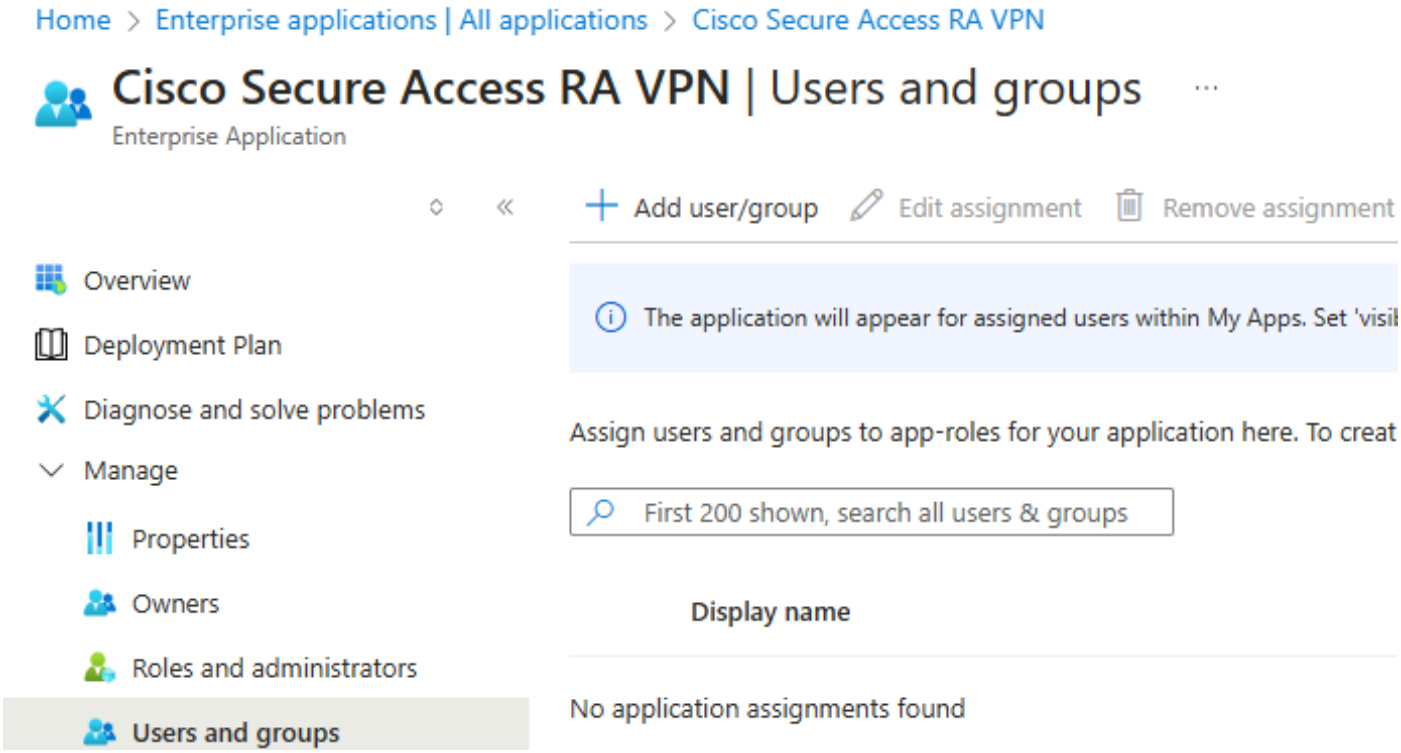
Azure에서 앱 만들기

3. 응용 프로그램의 이름을 바꿉니다.
   속성 > 이름



응용 프로그램 이름 바꾸기

4. 엔터프라이즈 애플리케이션 내에서 사용자가 AnyConnect VPN을 사용하여 인증할 수 있도록 할당합니다.
사용자 및 그룹 할당 > + 사용자/그룹 추가 > 할당

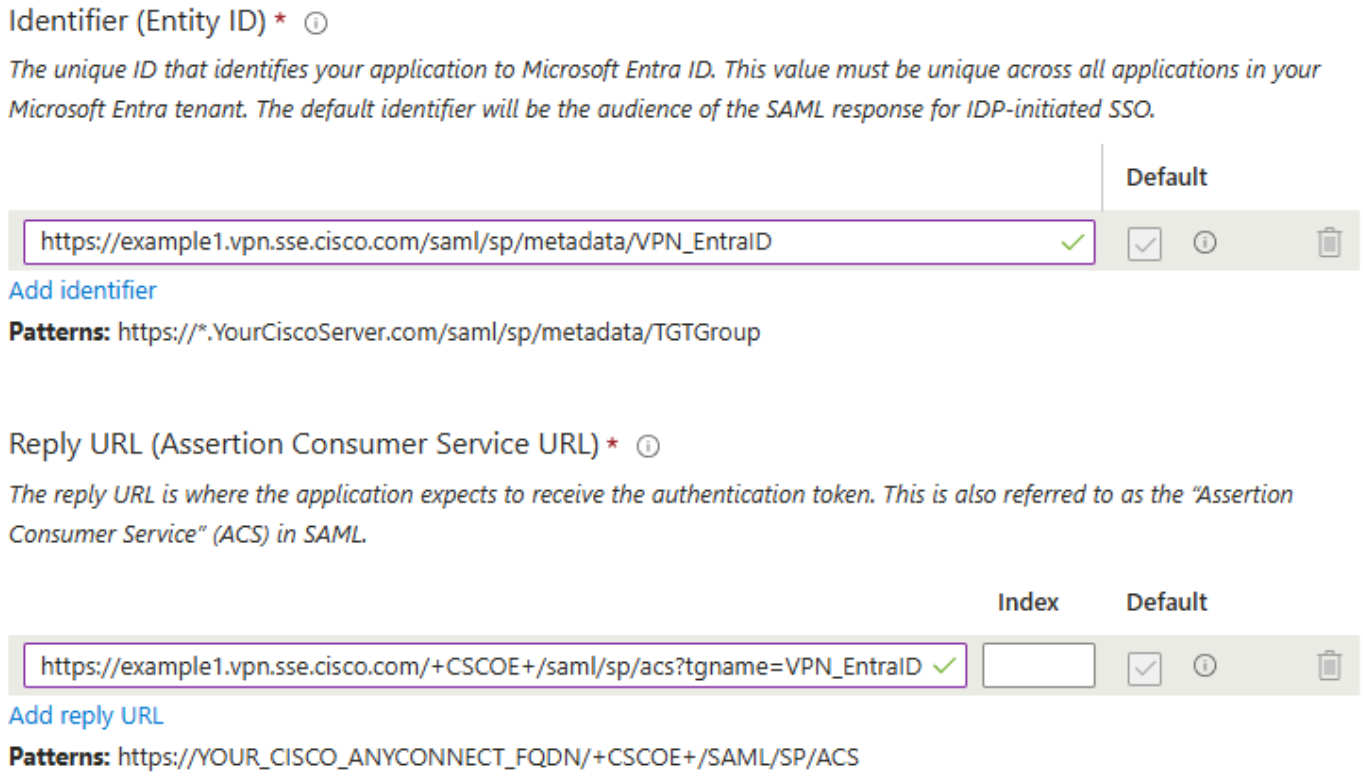


할당된 사용자/그룹

5. Single Sign-On을 클릭하고 SAML 매개변수를 구성합니다. 여기서는 1단계에서 복사한 FQDN과 2단계의 "Configuration Cisco Secure Access(Cisco 보안 액세스 구성)"에서 구성 중인 VPN 프로파일 이름을 사용합니다.

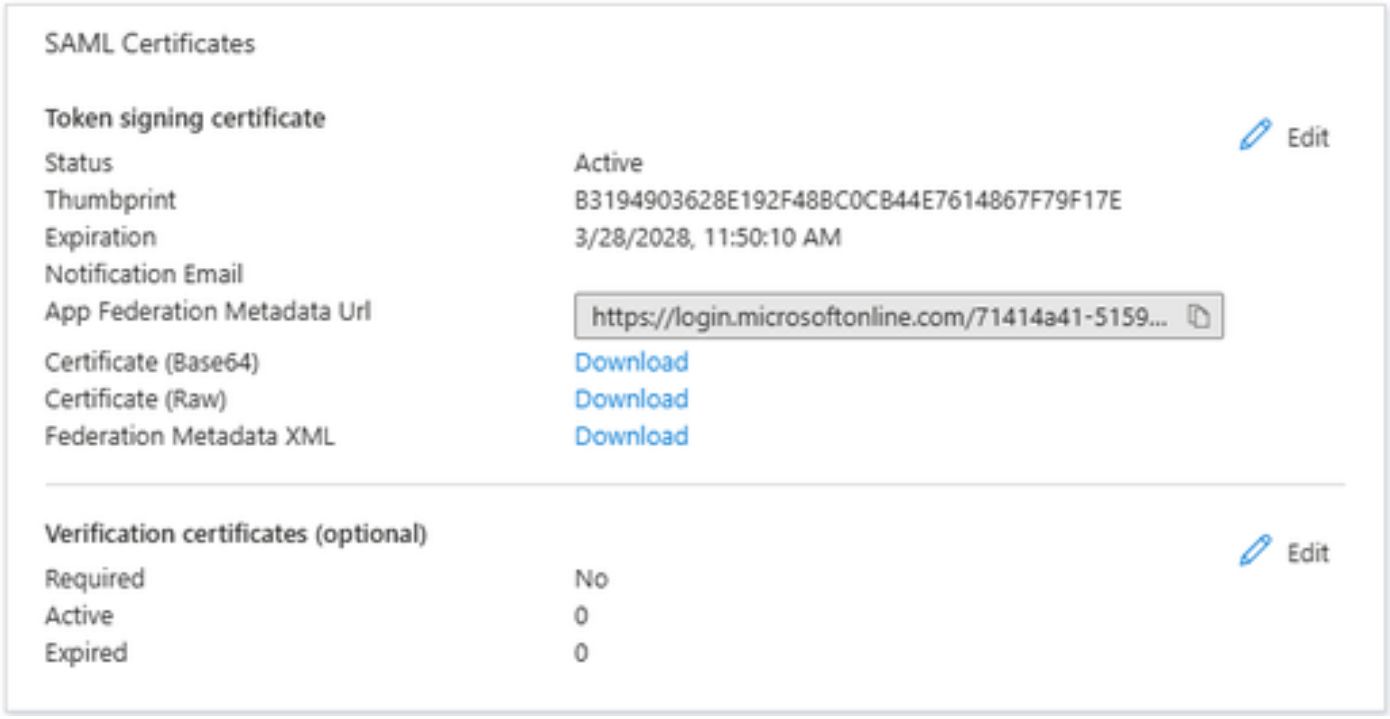
예를 들어 VPN 전역 FQDN이 example1.vpn.sse.cisco.com이고 Cisco Secure Access VPN 프로파일 이름이 VPN_EntraID인 경우 (Entity ID) 및 회신 URL(Assertion Consumer Service URL)의 값은 다음과 같습니다.

식별자(엔터티 ID): https://example1.vpn.sse.cisco.com/saml/sp/metadata/VPN_EntraID
회신 URL(Assertion Consumer Service URL): https://example1.vpn.sse.cisco.com/+CSCOE+/saml/sp/acs?tgname=VPN_EntraID



Azure의 SAML 매개 변수

6. 페더레이션 메타데이터 XML을 다운로드합니다.



Cisco Secure Access 컨피그레이션

1. Cisco Secure Access 대시보드에 로그인하고 IP 풀을 추가합니다.

Connect(연결) > End User Connectivity(최종 사용자 연결) > Virtual Private Network(가상 사설망) > Add IP Pool(IP 풀 추가)

지역: RA VPN을 구축할 지역을 선택합니다.
표시 이름: VPN IP 풀의 이름입니다.
DNS 서버: 연결된 후 DNS 확인에 사용할 DNS 서버 를 만들거나 할당합니다.
시스템 IP 풀: Secure Access에서 Radius 인증과 같은 기능을 사용할 때 인증 요청은 이 범위 내의 IP에 의해 소싱됩니다.
IP 풀: 새 IP 풀을 추가하고 사용자가 RA VPN에 연결되면 얻을 수 있는 IP를 지정합니다.

Setup VPN profiles

No VPN profiles added. To configure VPN profiles, you must first setup IP pools and then add profiles that map to users. Help

Add IP Pool

VPN 프로필 추가

Parameters

Edit this IP pool's parameters including its mapped region, DNS servers, and IP addresses

Region

Canada (Central)

Display name

RA VPN

DNS Server

DNS (208.67.222.222)

+ Add

DDNS Servers updates

System IP Pool ⓘ

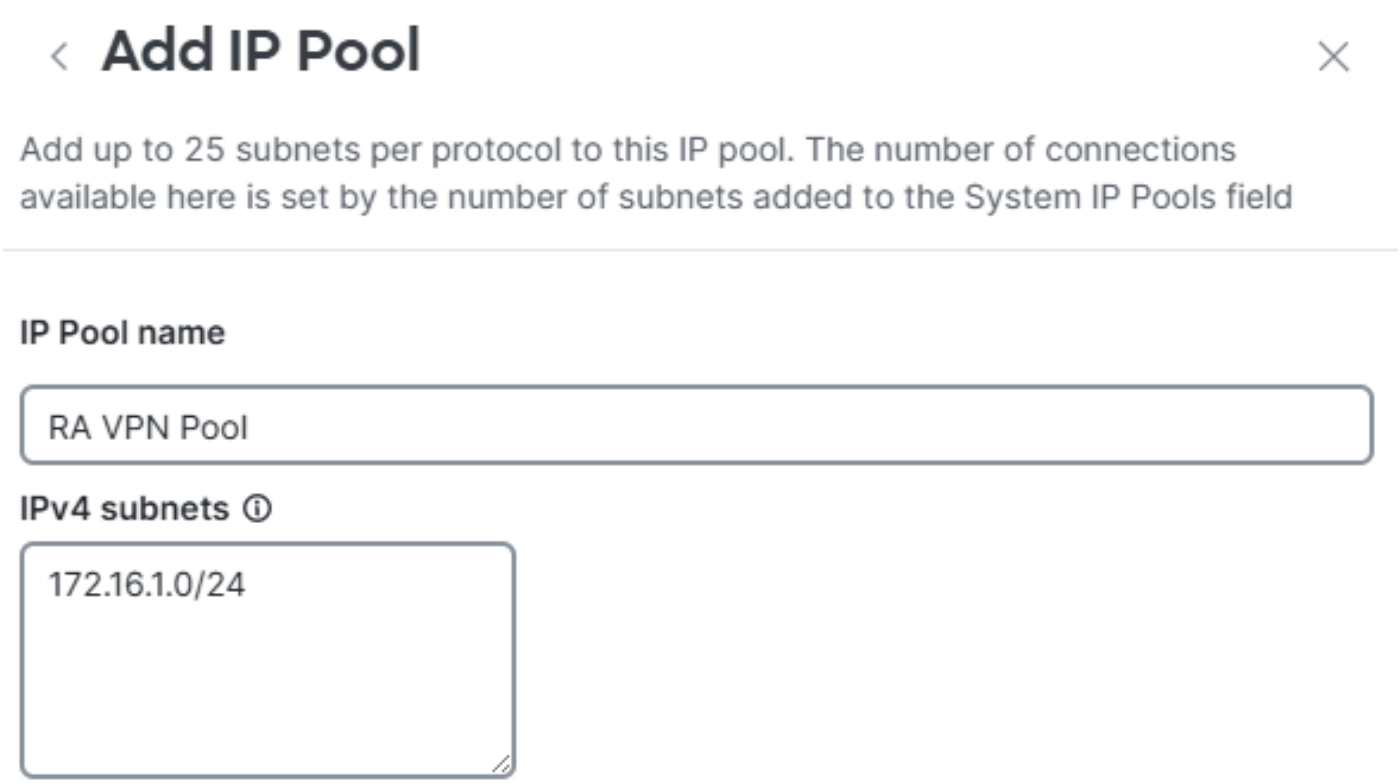
172.16.2.0/24

IP Pools

Add the IP pools this region will use. You can add a maximum of 25 IPV4 and 25 IPV6 subnets per IP pool. Help

+ Add

IP 풀 구성 - 1부

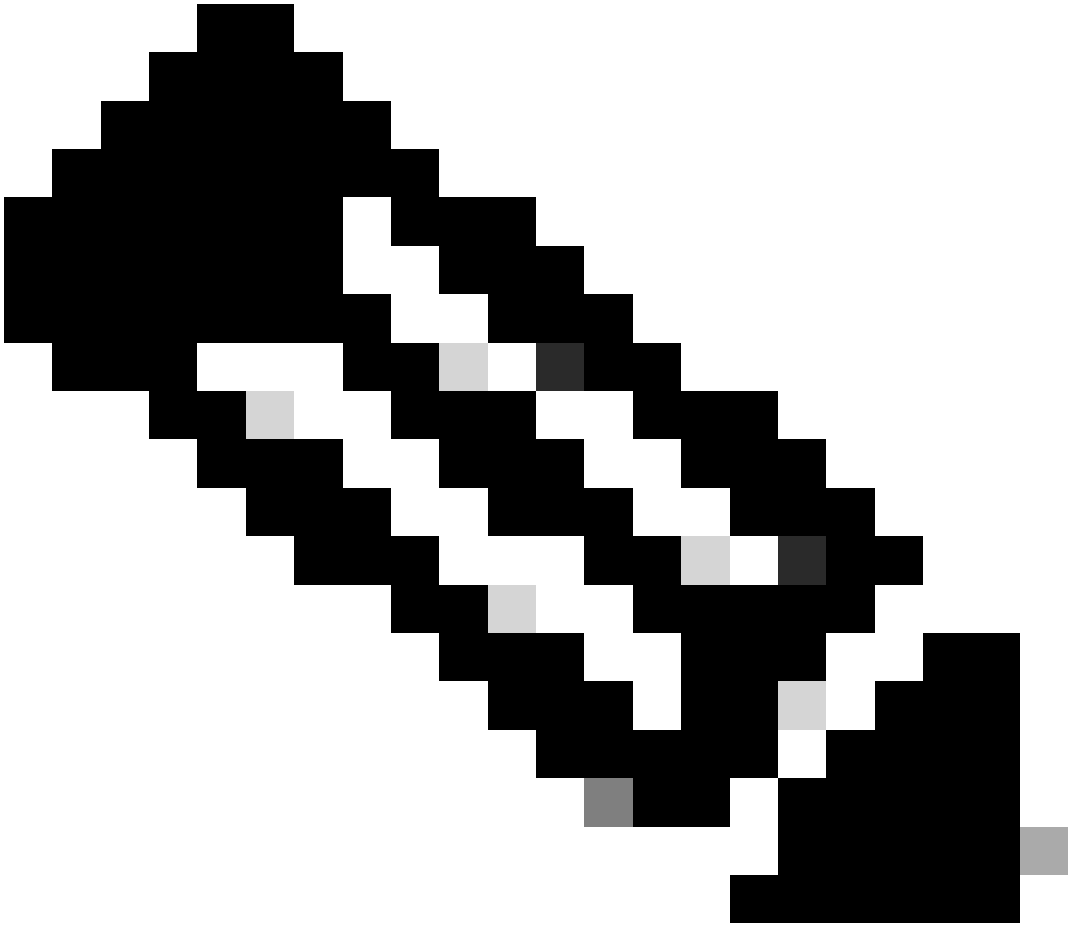


IP 풀 구성 - 2부

2. VPN 프로필을 추가합니다.

Connect(연결) > End User Connectivity(최종 사용자 연결) > Virtual Private Network(가상 사설망) > + VPN Profile(VPN 프로파일)

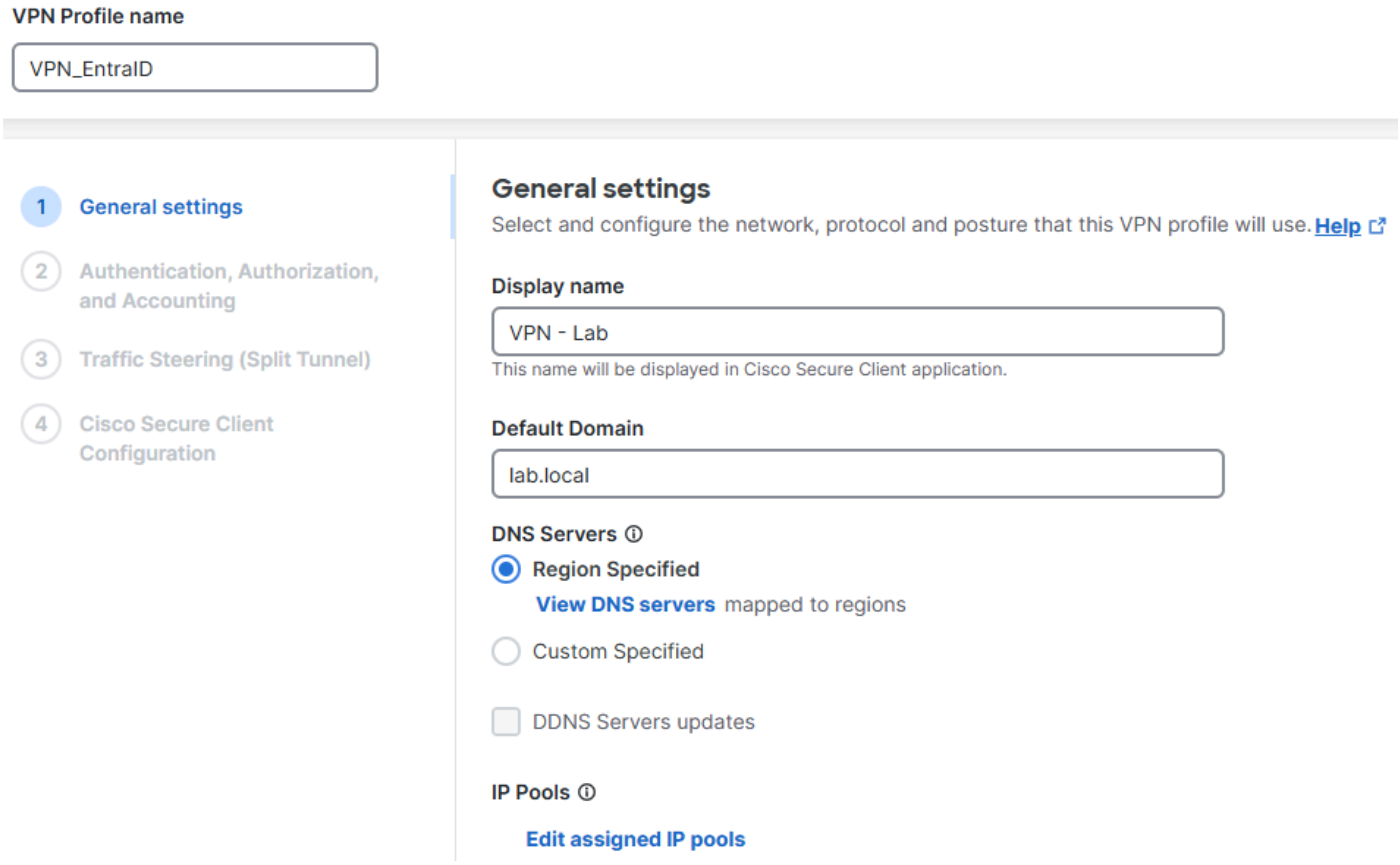
일반 설정



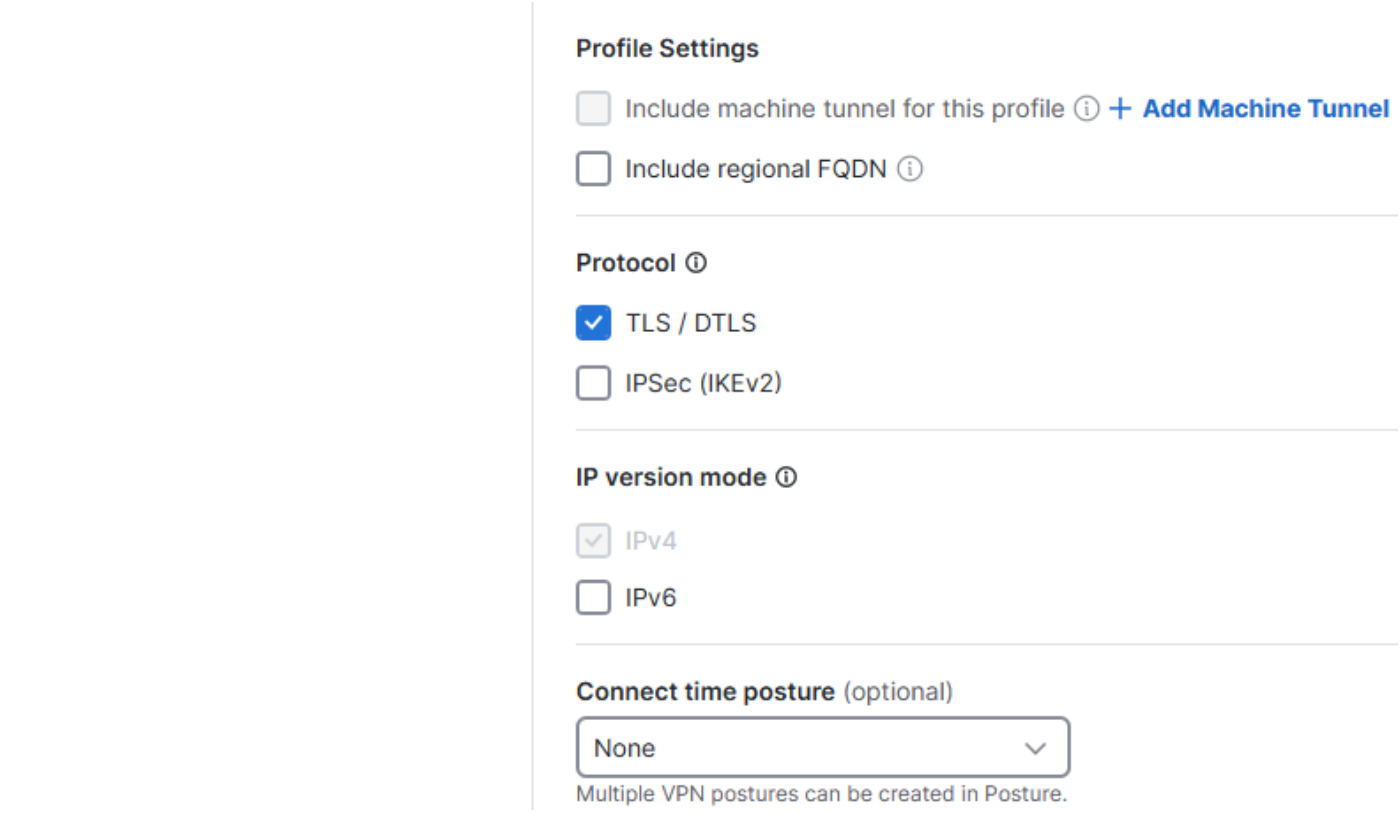
참고: 참고: VPN 프로필의 이름은 5단계에서 "Configuration Azure"에서 구성한 이름과 일치해야 합니다. 이 컨피그레이션 가이드에서는 VPN_EntraID를 사용했으므로 Cisco Secure Access에서 VPN 프로필 이름으로 동일하게 구성합니다.

VPN 프로필 이름: 이 VPN 프로필의 이름으로, 대시보드에만 표시됩니다.

표시 이름: 최종 사용자의 이름은 'Secure Client - Anyconnect' 드롭다운 메뉴에 표시되며, 이 RA VPN 프로파일에 연결할 때 표시됩니다.
기본 도메인: 도메인 사용자는 VPN에 연결되면 됩니다.
DNS 서버: DNS 서버 VPN 사용자가 VPN에 연결되면 받게 됩니다.
  지정된 지역: VPN IP 풀에 연결된 DNS 서버를 사용합니다.
  사용자 지정: 원하는 DNS를 수동으로 할당할 수 있습니다.
IP 풀: VPN에 연결되면 사용자에게 할당되는 IP.
프로필 설정: 머신 터널에 이 VPN 프로파일을 포함하거나 최종 사용자가 연결하려는 지역(구축된 IP 풀에 따라 다름)을 선택할 수 있도록 지역 FQDN을 포함합니다.
프로토콜: VPN 사용자가 트래픽 터널링에 사용할 프로토콜을 선택합니다.
연결 시간 상태(선택 사항): 연결 시간에 VPN Posture를 수행하는 데 필요한 경우 추가 정보



VPN 프로필 컨피그레이션 - 1부



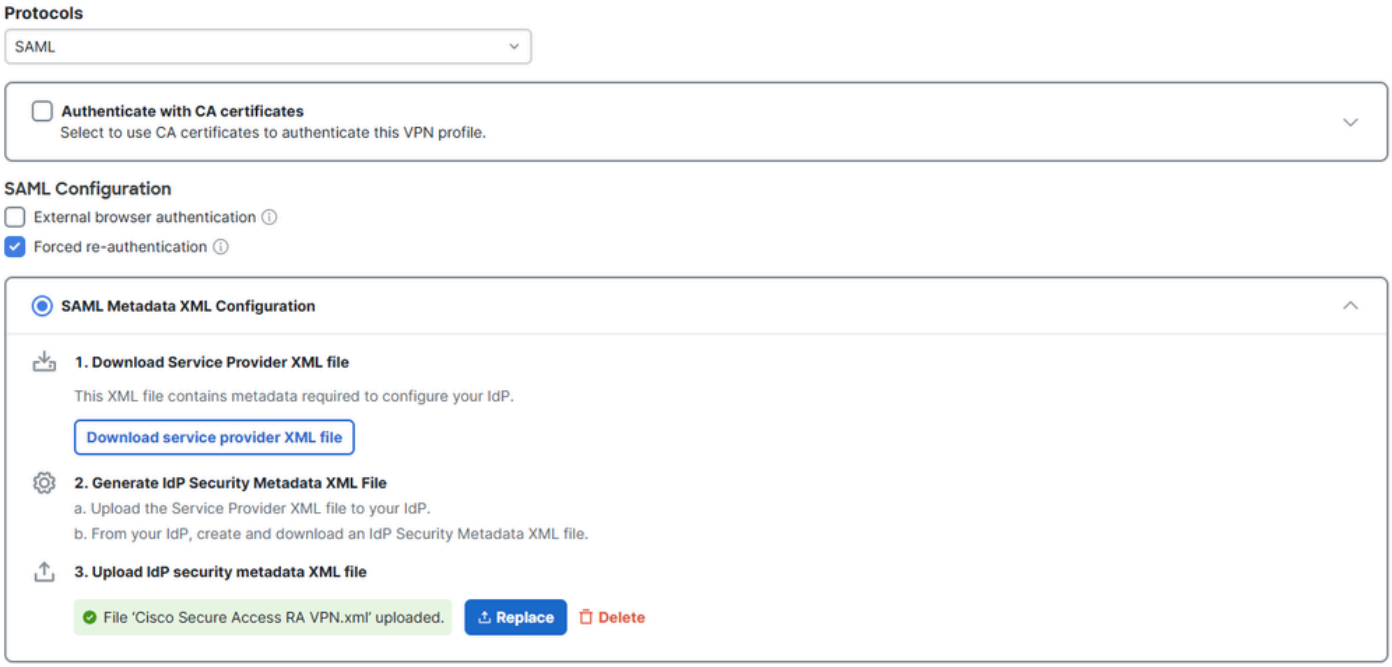
VPN 프로필 컨피그레이션 - 2부

인증, 권한 부여 및 계정 관리(AAA)

프로토콜: SAML을 선택합니다.

CA 인증서를 사용한 인증: SSL 인증서를 사용하여 인증하고 IdP SAML 제공자에 대해 권한을 부여하려는 경우
강제 재인증: VPN 연결이 설정될 때마다 강제로 다시 인증합니다. 강제 재인증은 세션 시간 초과를 기반으로 합니다. SAML IdP 설정(이 경우 Azure)이 적용될 수 있습니다.

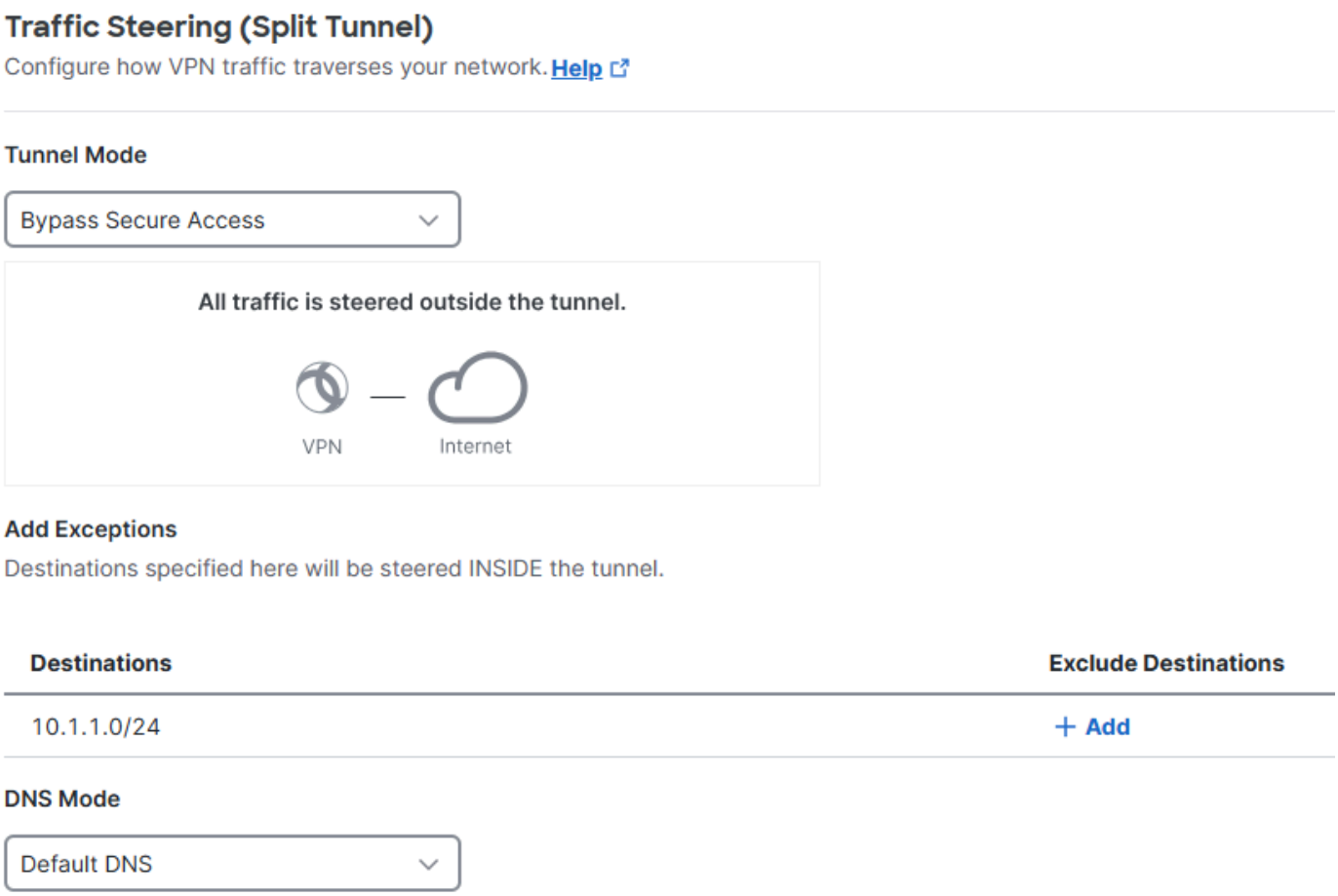
6단계에서 "Azure 구성"에서 다운로드한 XML 파일 페더레이션 메타데이터 XML 파일을 업로드합니다.



SAML 구성

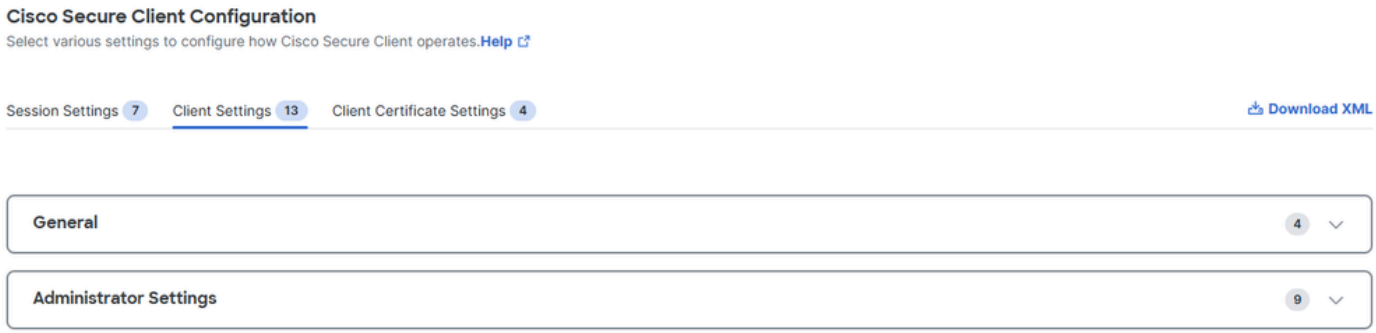
트래픽 스티어링(스플릿 터널)

터널 모드:
  보안 액세스에 연결: 모든 트래픽은 터널(Tunnel All)로 간주하여 전송됩니다.
  보안 액세스 우회: Exceptions(예외) 섹션에서 정의한 특정 트래픽만 터널링됩니다(스플릿 터널).
DNS 모드:
  기본 DNS: 모든 DNS 쿼리는 VPN 프로필에 의해 정의된 DNS 서버를 통해 이동합니다. 부정적인 응답의 경우 DNS 쿼리는 물리적 어댑터에 구성된 DNS 서버로 이동할 수도 있습니다.
  모든 DNS 터널: VPN을 통해 모든 DNS 쿼리를 터널링합니다.
  스플릿 DNS: 아래에 지정된 도메인에 따라 특정 DNS 쿼리만 VPN 프로필을 통해 이동합니다.



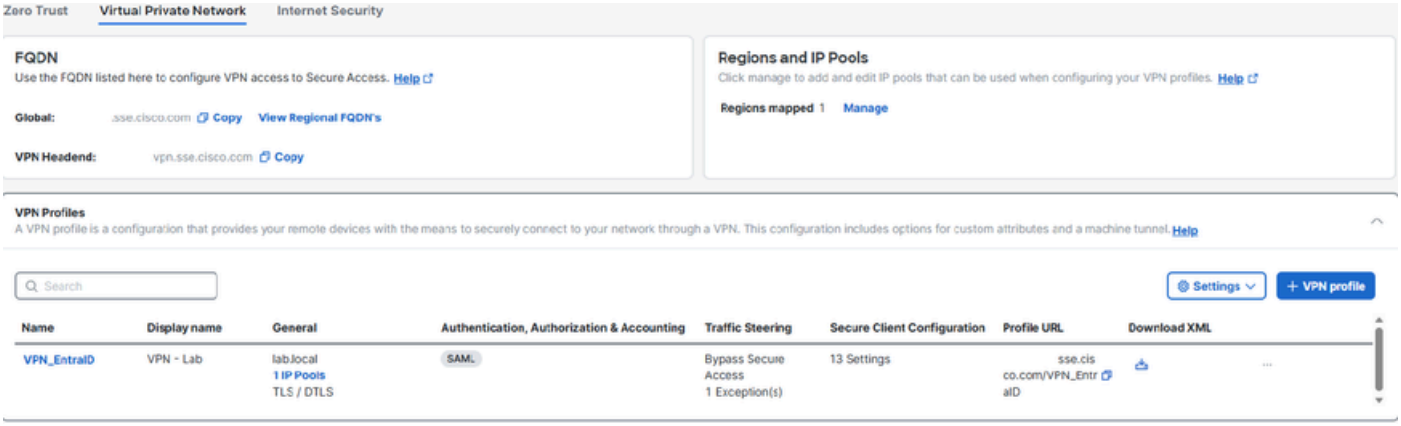
트래픽 조정 컨피그레이션

Cisco Secure Client 컨피그레이션
이 설명서에서는 이러한 고급 설정을 구성하지 않습니다. 다음과 같이 고급 기능을 구성할 수 있습니다. TND, Always-On, Certificate Matching, Local Lan Access 등. 여기에 설정을 저장합니다.



고급 설정

3. VPN 프로필은 다음과 같아야 합니다. VPN 사용을 시작하려면 최종 사용자에게 xml 프로파일을 다운로드하고 사전 배포하거나("C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile" 아래) Cisco Secure Client - AnyConnect VPN UI에 입력할 프로파일 URL을 제공할 수 있습니다.



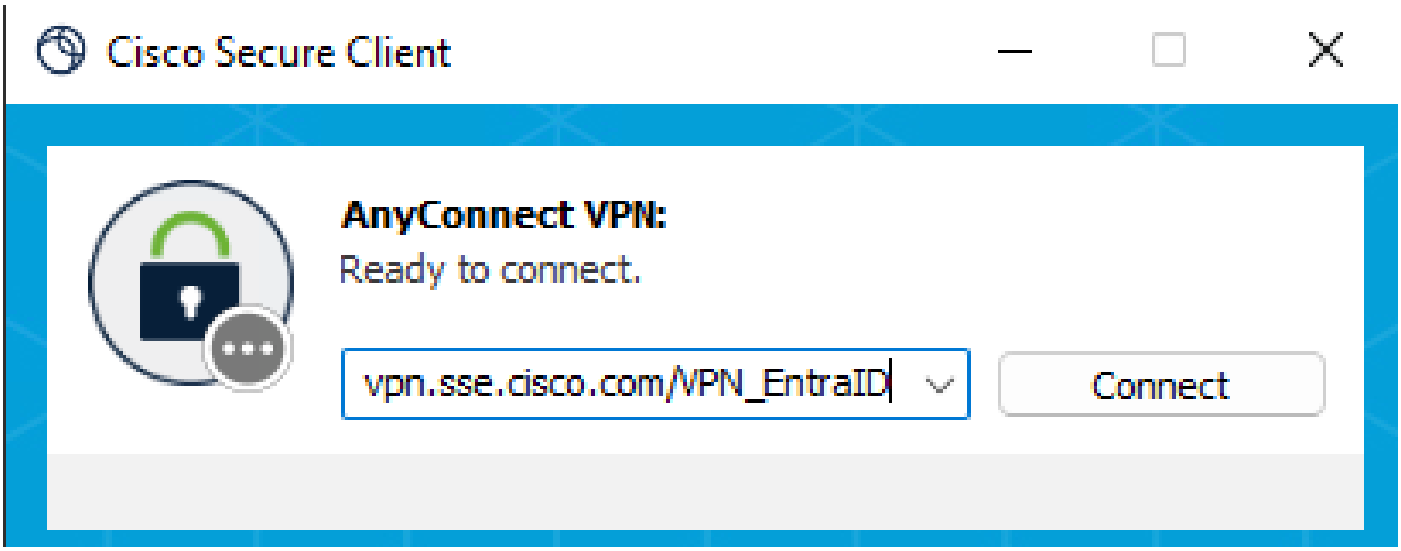
전역 FQDN 및 프로필 URL

다음을 확인합니다.

이때 RA VPN 컨피그레이션을 테스트할 준비가 되어 있어야 합니다.
사용자가 처음 연결할 때 PC의 "C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile" 아래에 프로필 URL 주소를 지정하거나 XML 프로필을 사전 배포해야 합니다. VPN 서비스를 다시 시작하고 드롭다운 메뉴에 이 VPN 프로필에 연결하는 옵션이 표시되어야 합니다.

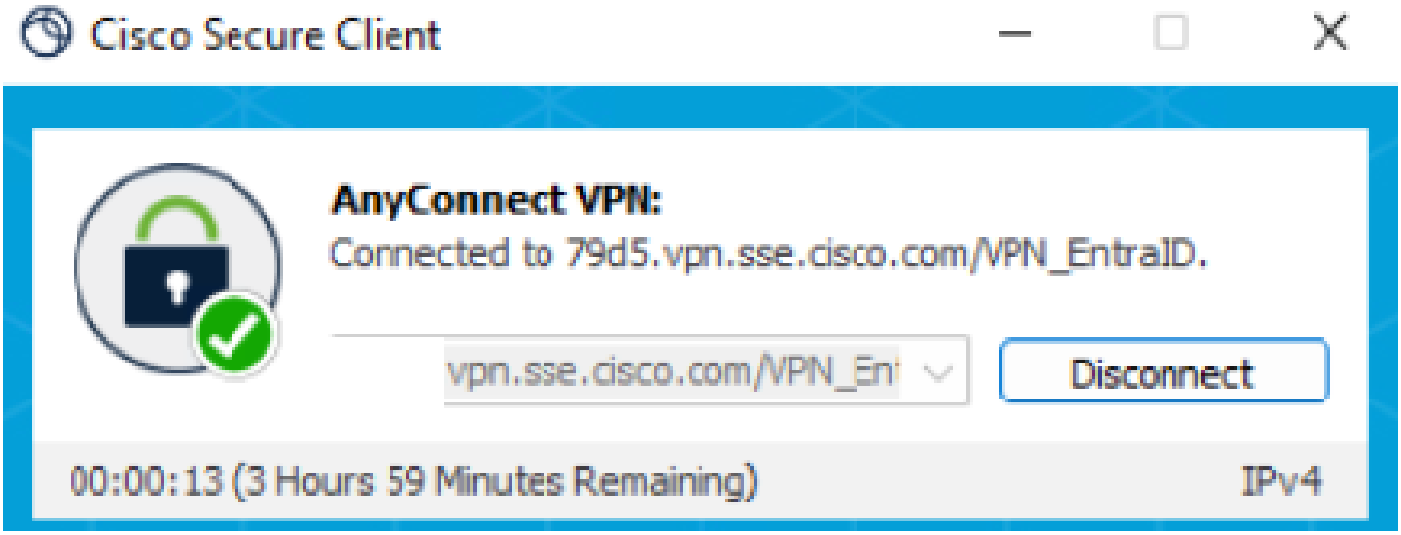
이 예에서는 첫 번째 연결 시도에 대해 사용자에게 프로필 URL 주소를 제공합니다.

첫 번째 연결 이전:



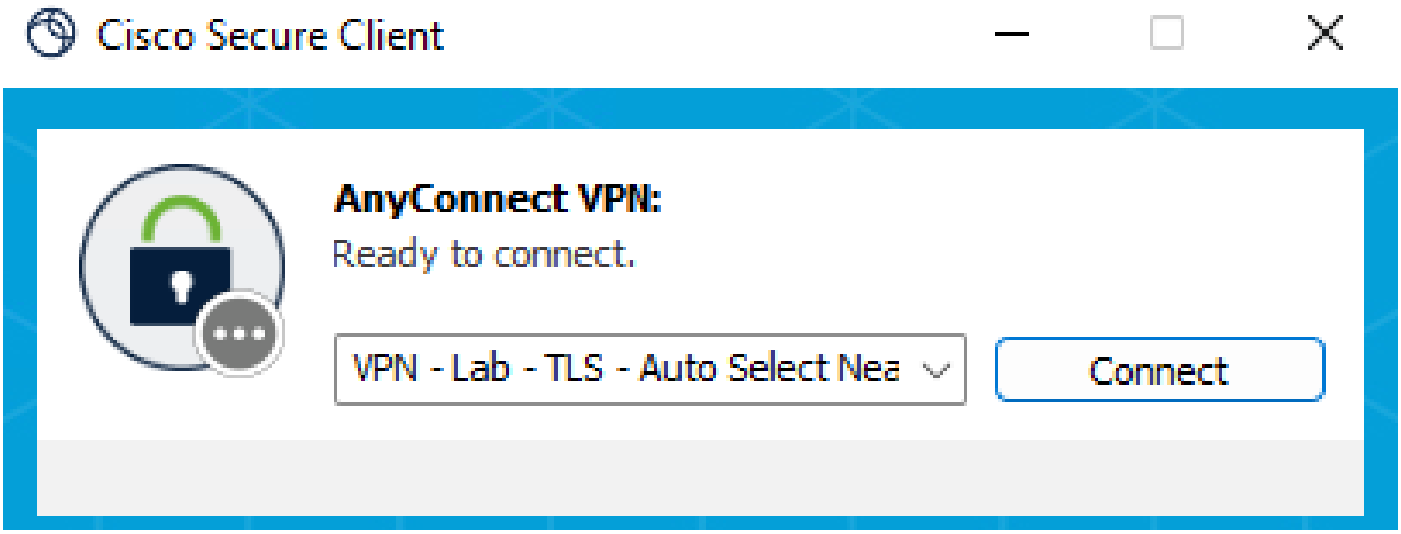
이전 VPN 연결

자격 증명을 입력하고 VPN에 연결합니다.



VPN에 연결됨

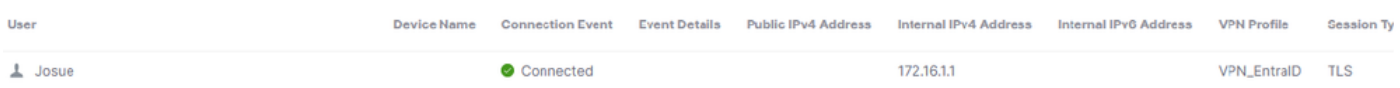
처음 연결한 후 드롭다운 메뉴에서 이제 "VPN - Lab" VPN 프로파일에 연결하는 옵션을 볼 수 있어야 합니다.



첫 번째 VPN 연결 후

사용자가 연결할 수 있었던 원격 액세스 로그를 확인하십시오.

Monitor(모니터링) > Remote Access Log(원격 액세스 로그)



Cisco Secure Access 로그인

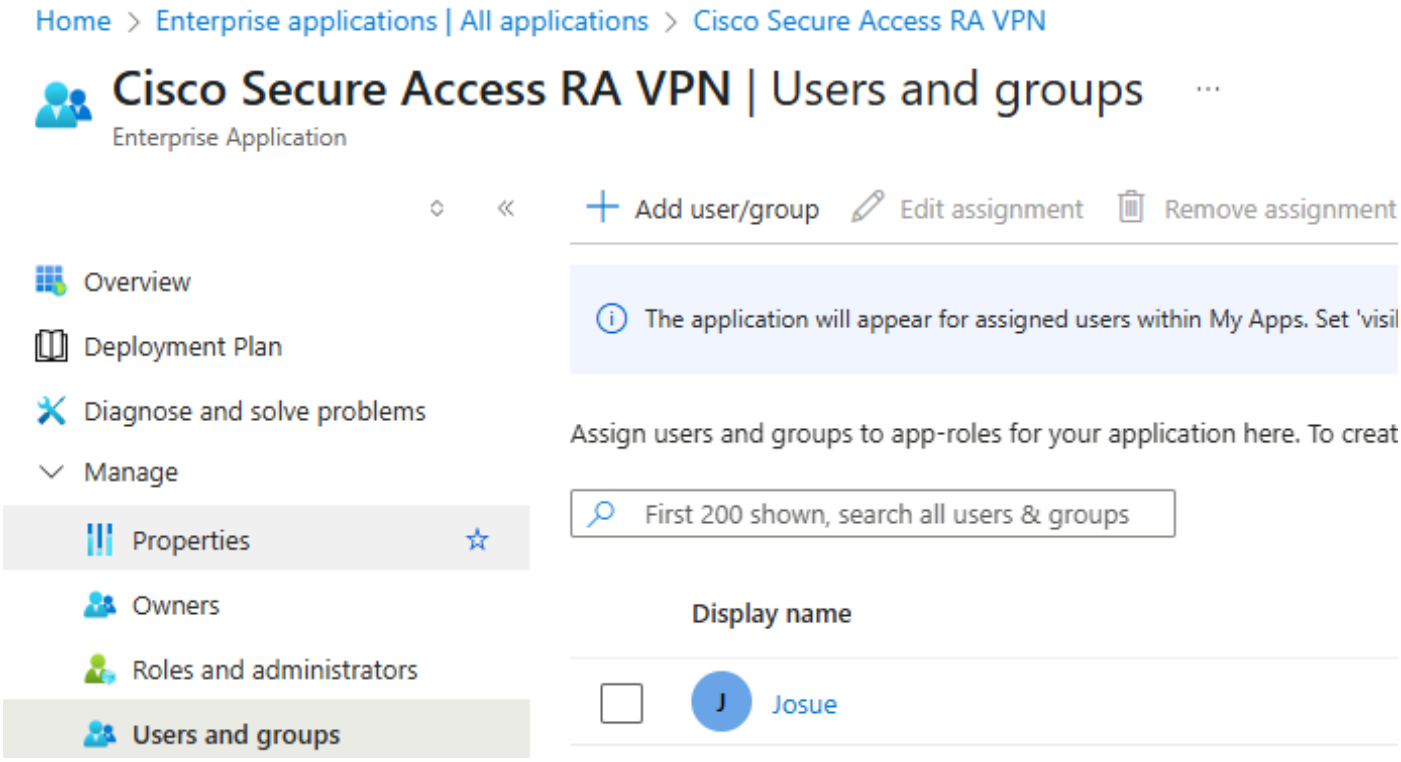
문제 해결

다음은 몇 가지 일반적인 문제에 대해 수행할 수 있는 기본 트러블슈팅에 대해 설명합니다.

아주레

Azure에서 사용자가 Cisco Secure Access에 대한 인증을 위해 만든 엔터프라이즈 응용 프로그램에 할당되었는지 확인합니다.

홈 > Enterprise Applications > Cisco Secure Access RA VPN > Manage > Users and Groups

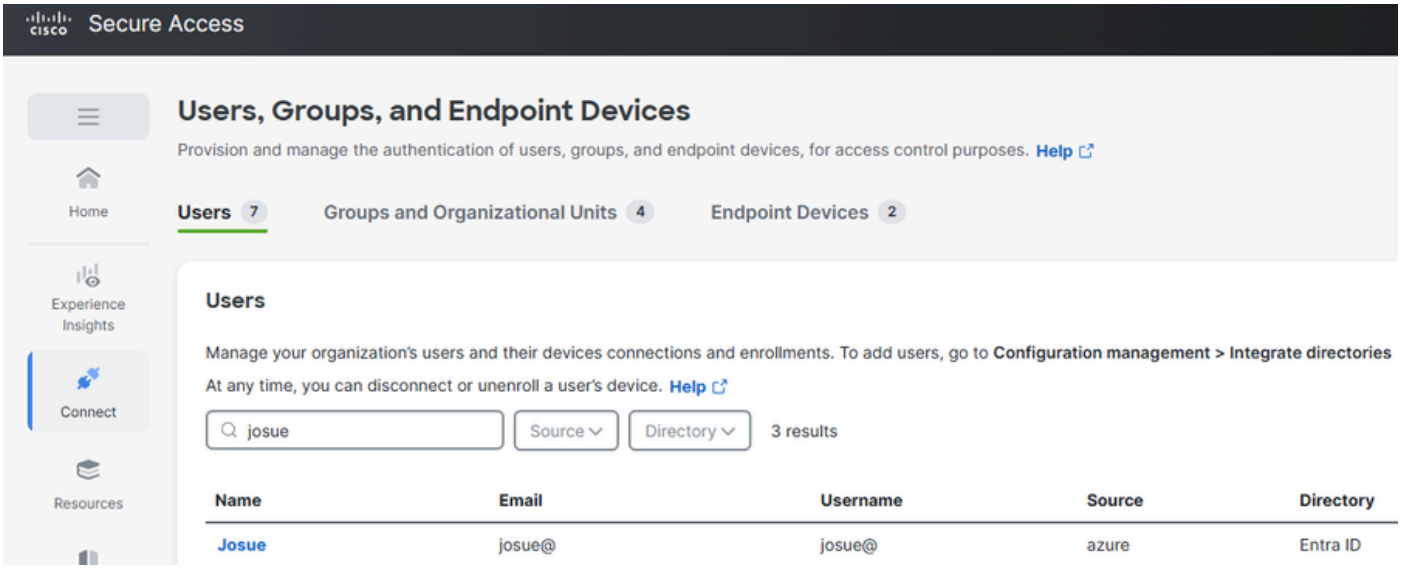


사용자 할당 확인

Cisco 보안 액세스

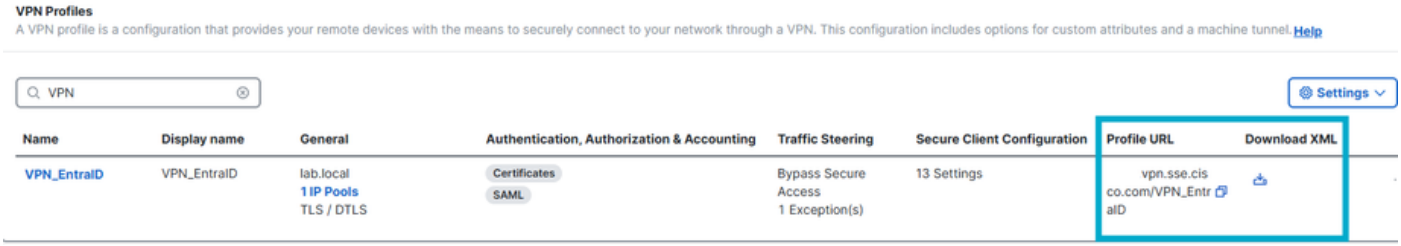
Cisco Secure Access에서 RA VPN을 통해 연결할 수 있는 사용자를 프로비저닝했는지, 또한 Cisco Secure Access에서 프로비저닝된 사용자(사용자, 그룹 및 엔드포인트 장치 아래)가 Azure의 사용자(엔터프라이즈 응용 프로그램에서 할당된 사용자)와 일치하는지 확인합니다.

Connect(연결) > Users, Groups, and Endpoint Devices(사용자, 그룹 및 엔드포인트 디바이스)



"확인" 단계에 설명된 대로 사용자에게 PC에 올바른 XML 파일이 프로비저닝되었는지 또는 사용자에게 프로필 URL이 제공되었는지 확인합니다.

Connect(연결) > End User Connectivity(최종 사용자 연결) > Virtual Private Network(가상 사설망)



프로필 URL 및 .xml 프로필

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.