ISE 및 TACACS+로 디바이스 관리를 위한 APIC 구성

목차

소개

이 문서에서는 TACACS+ 프로토콜을 사용한 관리자 사용자 인증을 위해 APIC을 ISE와 통합하는 절차에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- APIC(Application Policy Infrastructure Controller)
- Identity Services Engine(ISE)
- TACACS 프로토콜

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- APIC 버전 4.2(7u)
- ISE 버전 3.2 패치 1

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

네트워크 다이어그램

통합 다이어그램

인증 절차

1단계 관리자 사용자 자격 증명을 사용하여 APIC 애플리케이션에 로그인합니다.

2단계. 인증 프로세스가 트리거되고 ISE가 로컬 또는 Active Directory를 통해 자격 증명을 검증합니다.

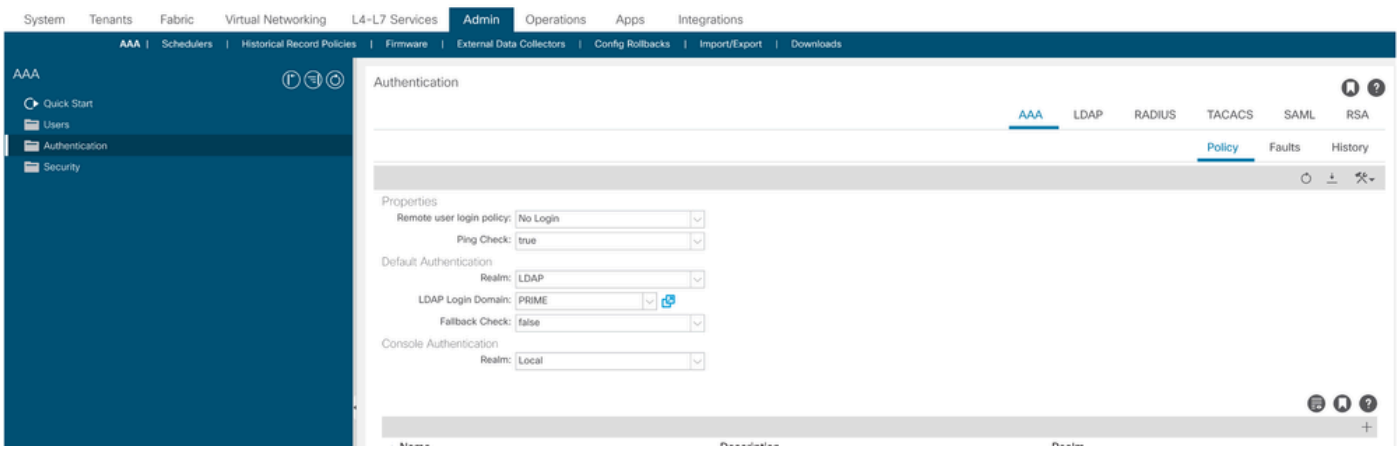
3단계. 인증에 성공하면 ISE는 APIC에 대한 액세스를 승인하기 위해 허용 패킷을 전송합니다.

4단계. ISE에서 성공적인 인증 라이브 로그를 표시합니다.

참고: APIC는 TACACS+ 컨피그레이션을 패브릭의 일부인 리프 스위치에 복제합니다.

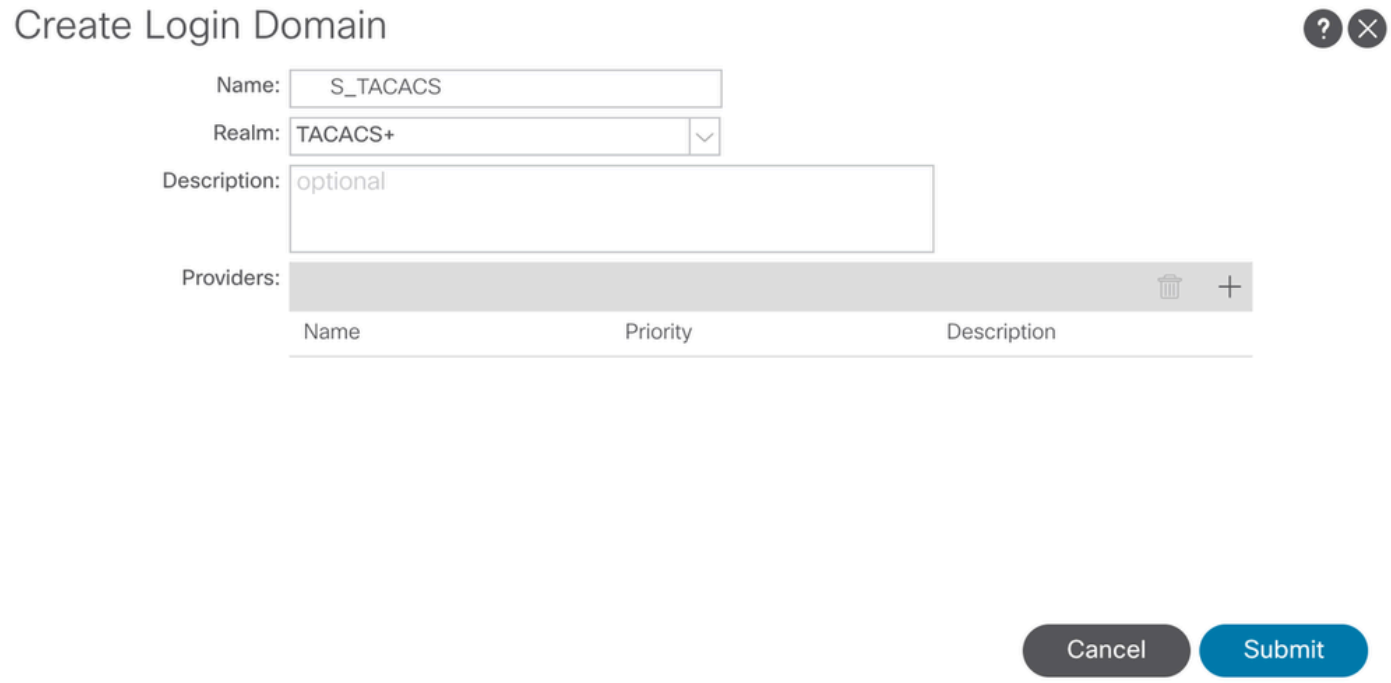
APIC 컨피그레이션

1단계. 새 로그인Admin > AAA > Authentication > AAA도메인을 생성하려면 아이콘으로+이동하여 선택합니다.

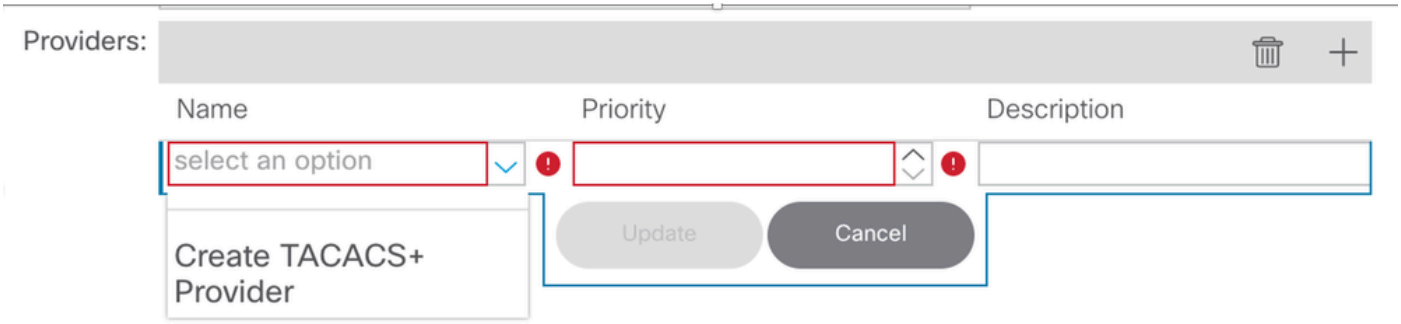


APIC 로그인 관리 컨피그레이션

2단계. 새 공급자를 생성하려면 새 로그인 도메인의 이름과 영역을 정의하고 Providers(공급자) 아래를+클릭합니다.

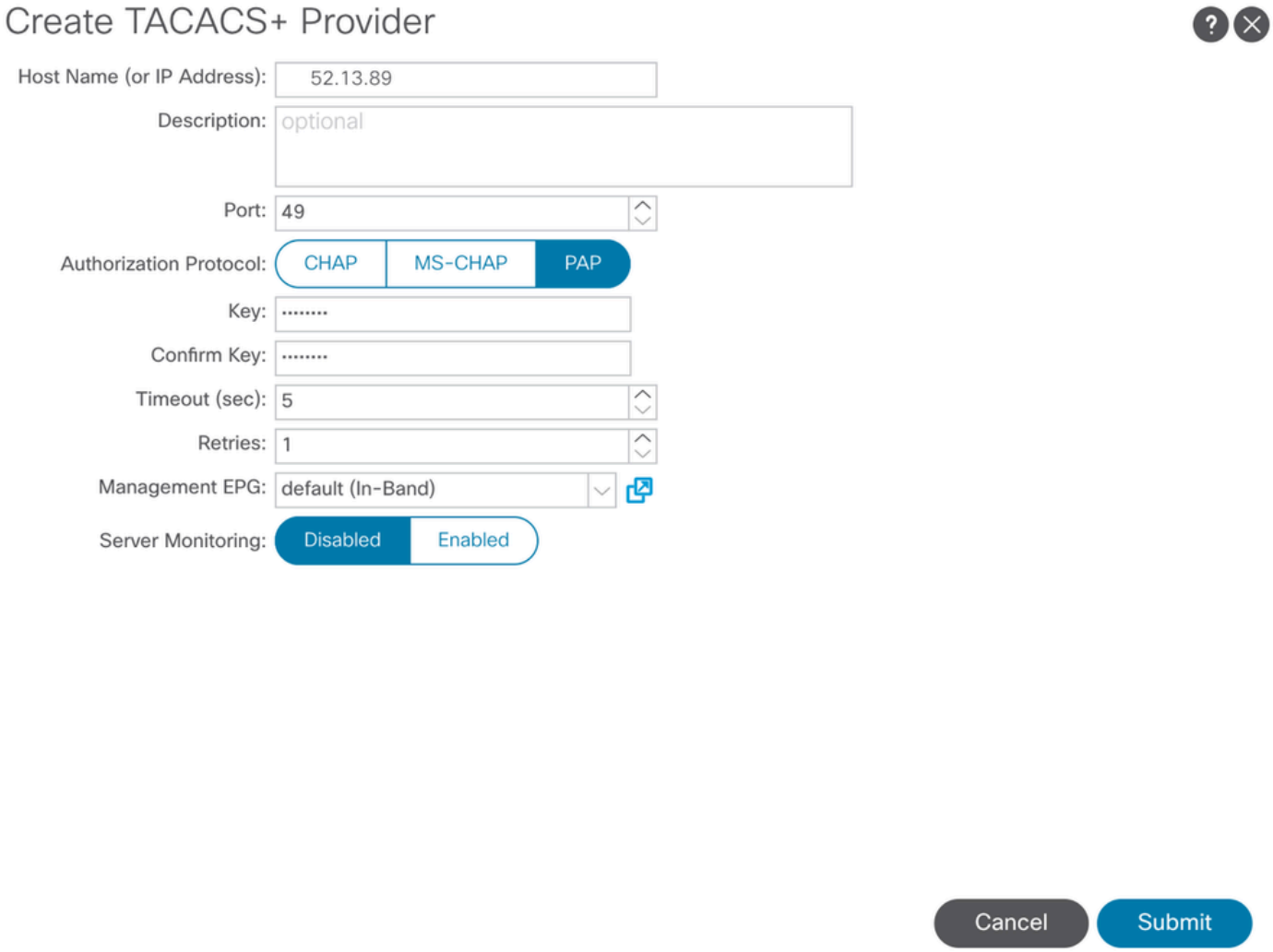


APIC 로그인 관리자

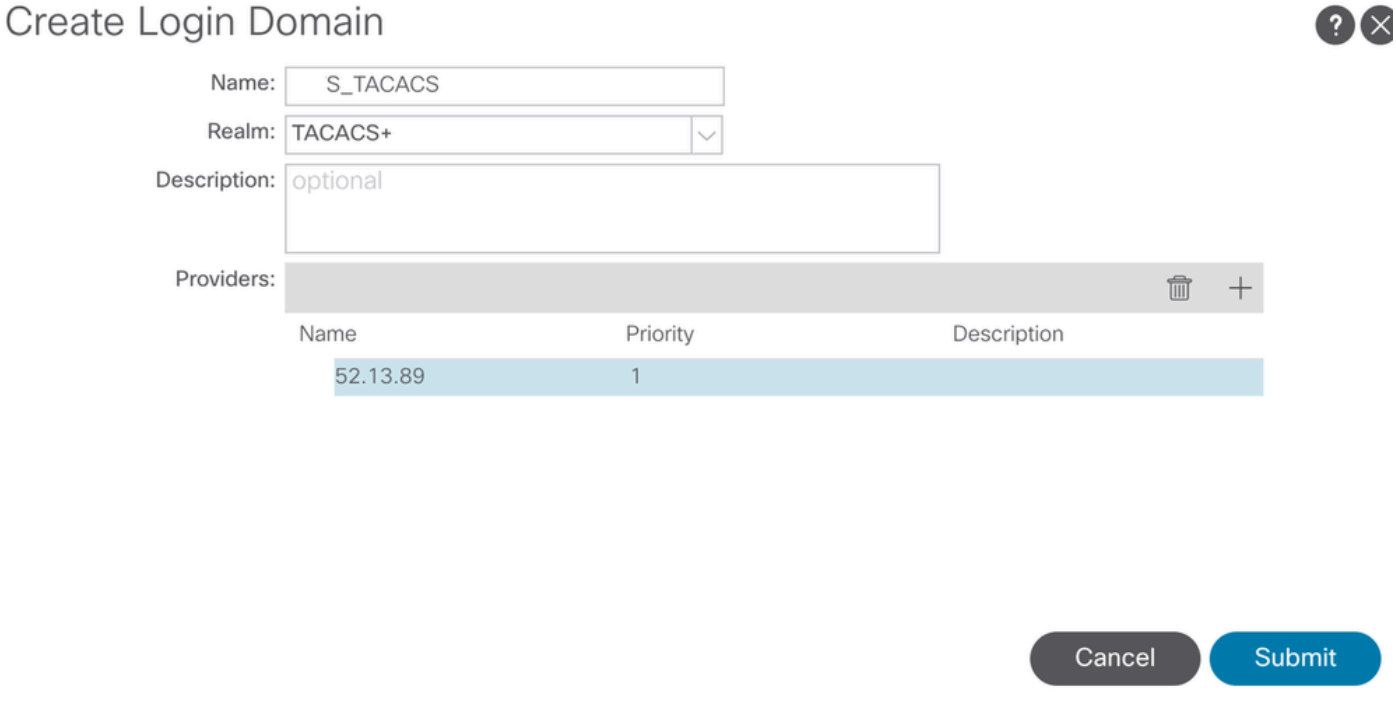


APIC TACACS 제공자

3단계. ISE IP 주소 또는 호스트 이름을 정의하고, 공유 암호를 정의하고, 관리 EPG(Endpoint Policy Group)를 선택합니다. 로그인 관리자Submit에 TACACS+ 제공자를 추가하려면 클릭합니다.



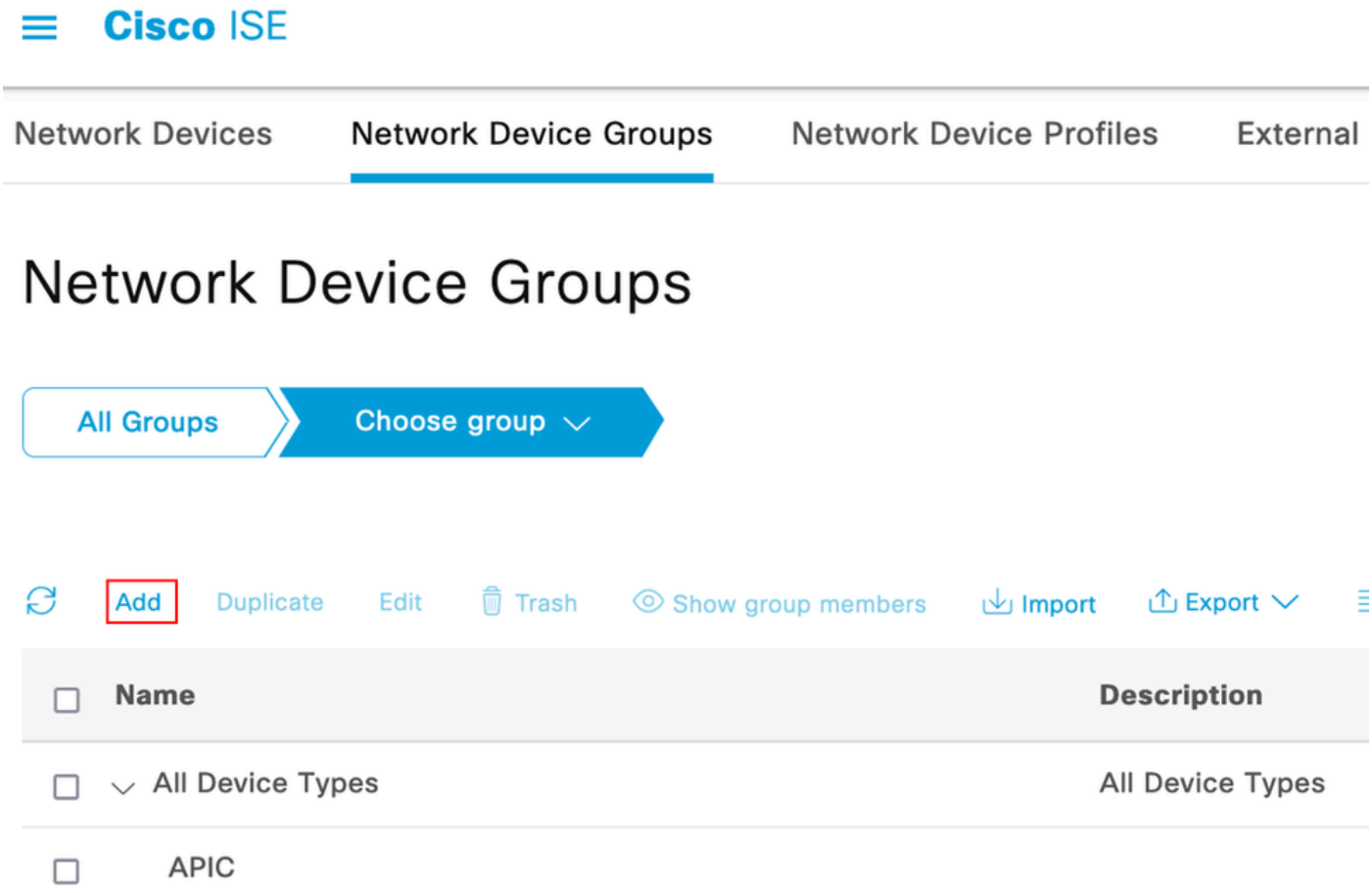
APIC TACACS 제공자 설정



TACACS 제공자 보기

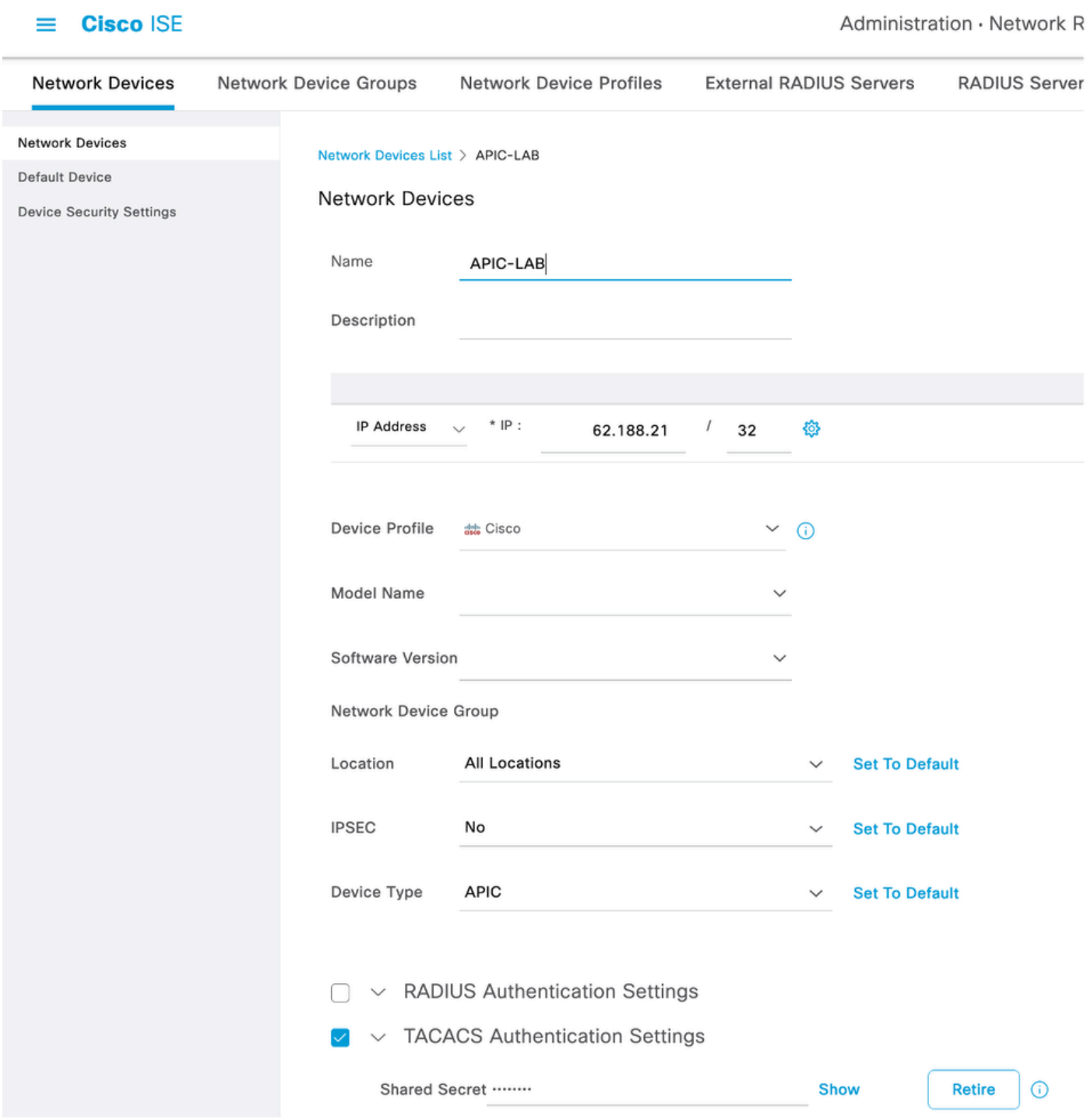
ISE 구성

>1단계. Administration(관리) > Network Resources(네트워크 리소스) > Network Device Groups(네트워크 디바이스 그룹)☰ 이동합니다. All Device Types(모든 디바이스 유형) 아래에 네트워크 디바이스 그룹을 생성합니다.



ISE 네트워크 디바이스 그룹

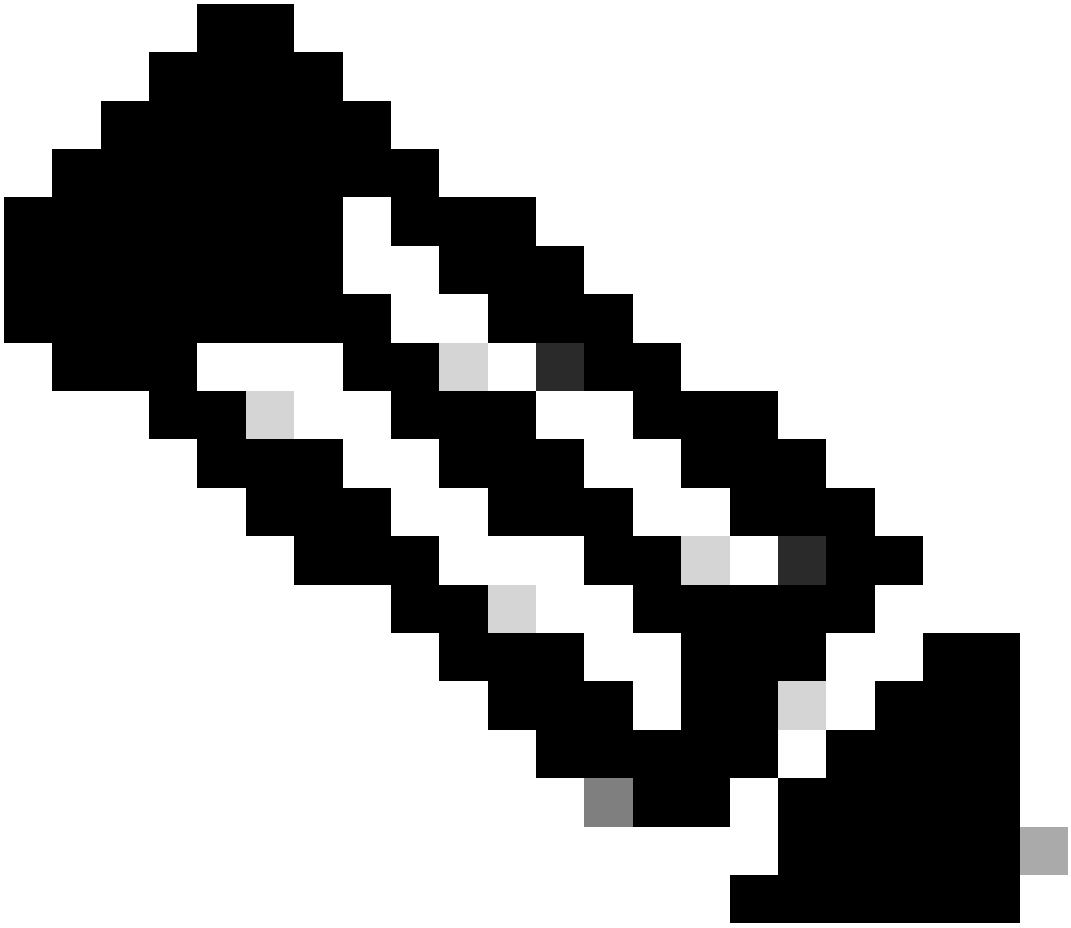
2단계. 로Administration > Network Resources > Network Devices이동합니다. Define APIC Name and IP address(APIC 이름 및 IP 주소 정의)를 선택하고Add, Device Type and TACACS+(디바이스 유형 및 TACACS+) 확인란에서 APIC를 선택하고, APIC TACACS+ Provider(APIC TACACS+ 제공자) 컨피그레이션에 사용되는 비밀번호를 정의합니다. 을 클릭합니다.Submit



리프 스위치에 대해 1단계와 2단계를 반복합니다.

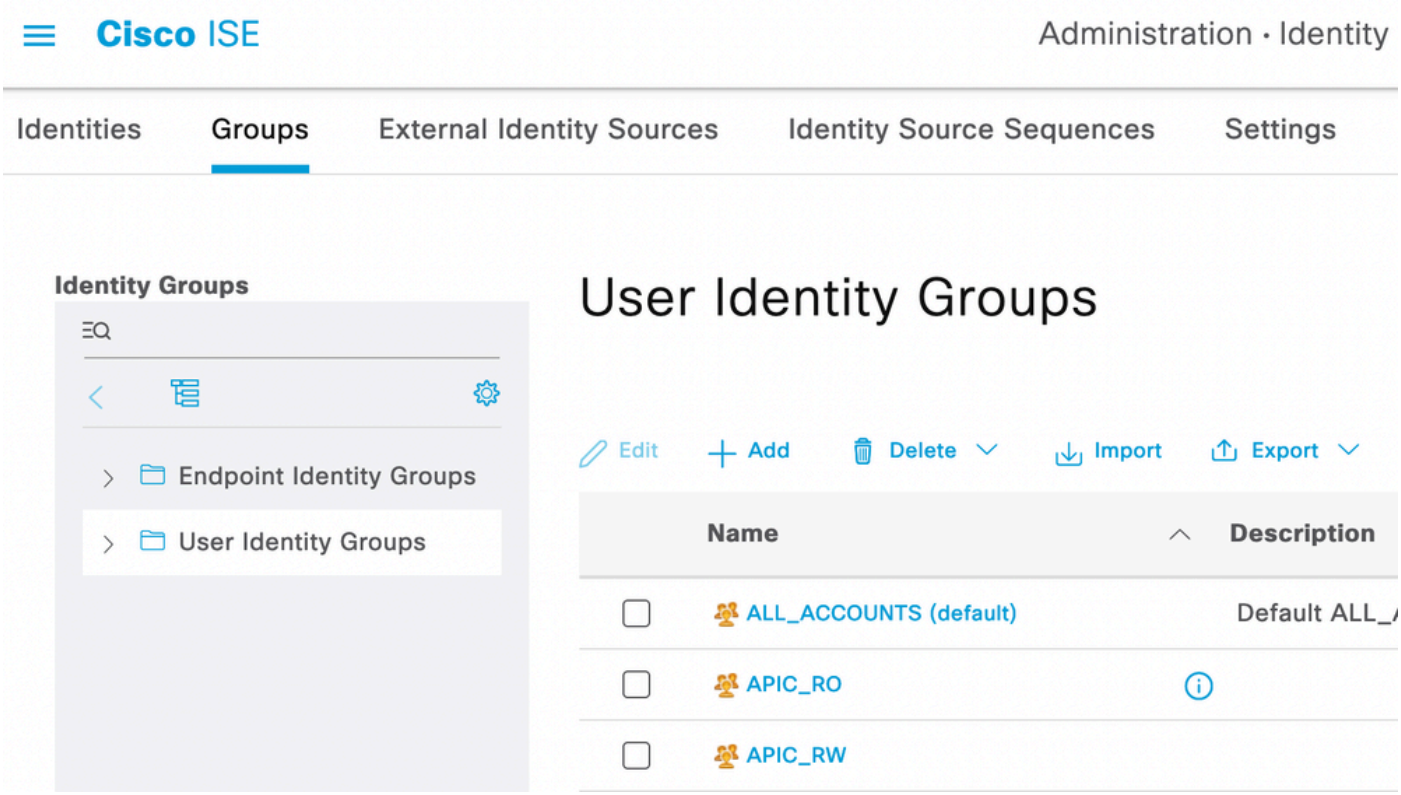
3단계. ISE를 Active Directory와 통합하려면 이 링크의 지침을 사용합니다.

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/217351-ad-integration-for-cisco-ise-gui-and-cli.html



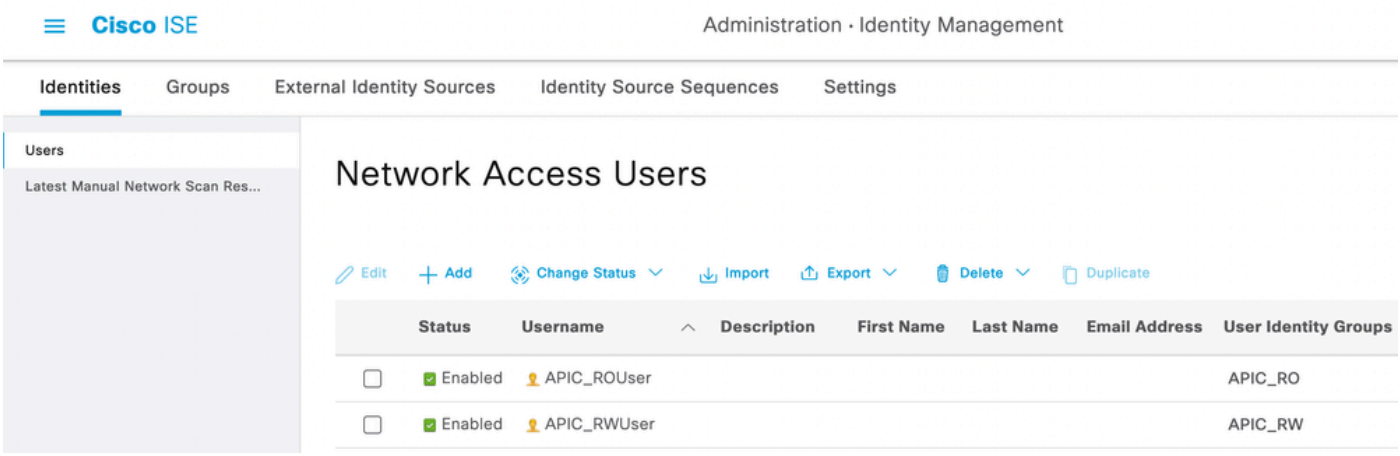
참고: 이 문서에는 ID 소스로 내부 사용자 및 AD 관리자 그룹이 모두 포함되어 있지만 내부 사용자의 ID 소스로 테스트가 수행됩니다. 결과는 AD 그룹에 대해 동일합니다.

4단계. (선택 사항) ☰로>Administration > Identity Management > Groups. 선택User Identity Groups 및 클릭 Add. 읽기 전용 Admin 사용자 및 Admin 사용자에 대해 하나의 그룹을 생성합니다.

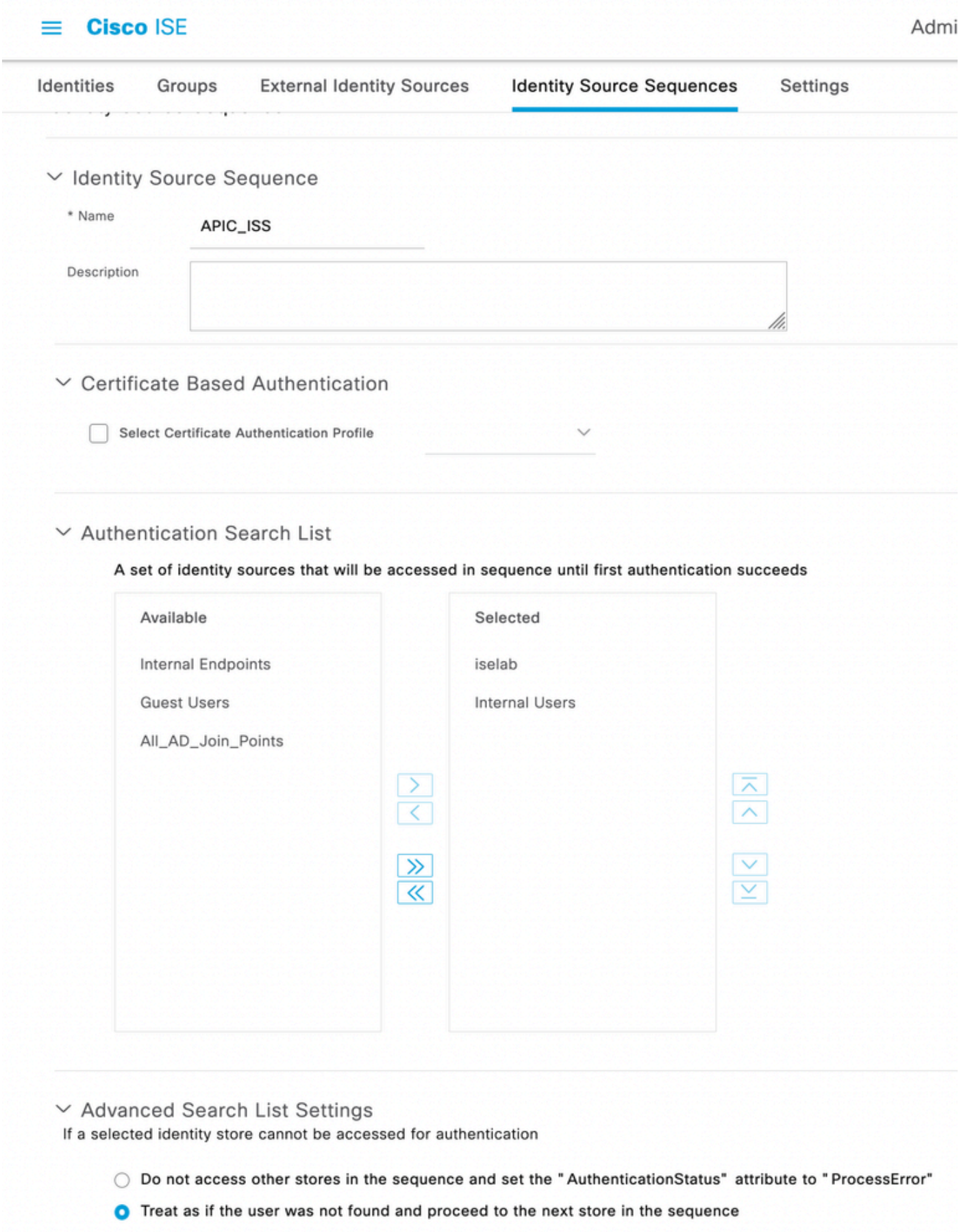


ID 그룹

5단계. (선택 사항) ☰로 >Administration > Identity Management > Identity.이동하여Add한 명의Read Only AdminAdmin사용자 및 사용자를 생성합니다. 각 사용자를 4단계에서 생성한 각 그룹에 할당합니다.



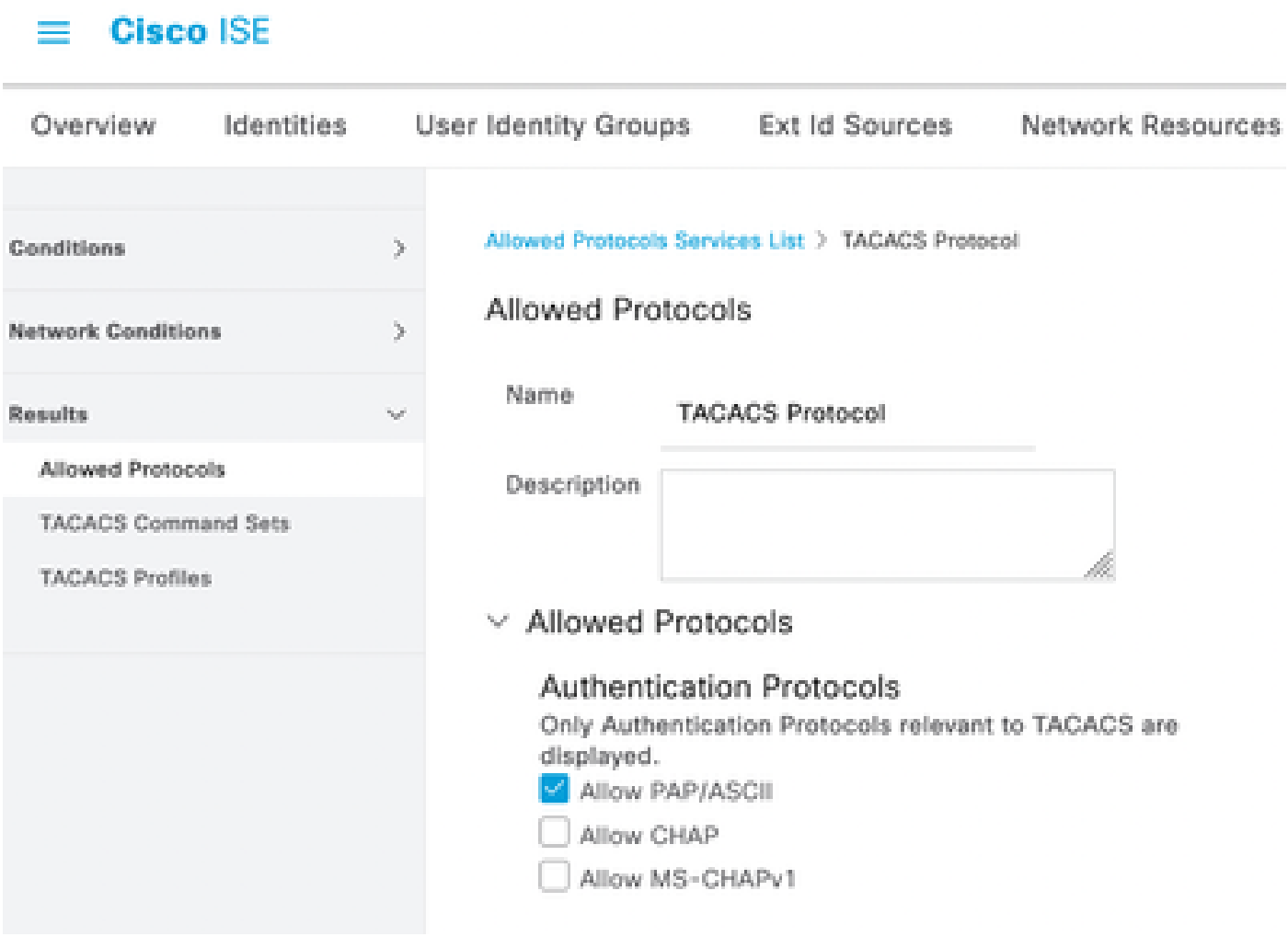
6단계. ☰로>Administration > Identity Management > Identity Source Sequence이동합니다. 목록Add에서 이름을 선택하고AD Join PointsInternal UsersID 소스를 정의합니다. 아래에서Treat as if the user was not found and proceed to the next store in the sequence를 선택하고 를Advanced Search List Settings클릭합니다Save.



ID 소스 시퀀스

7. Add(추가)☰>**Work Centers > Device Administration > Policy Elements > Results > Allowed Protocols.** Select(추가 선택

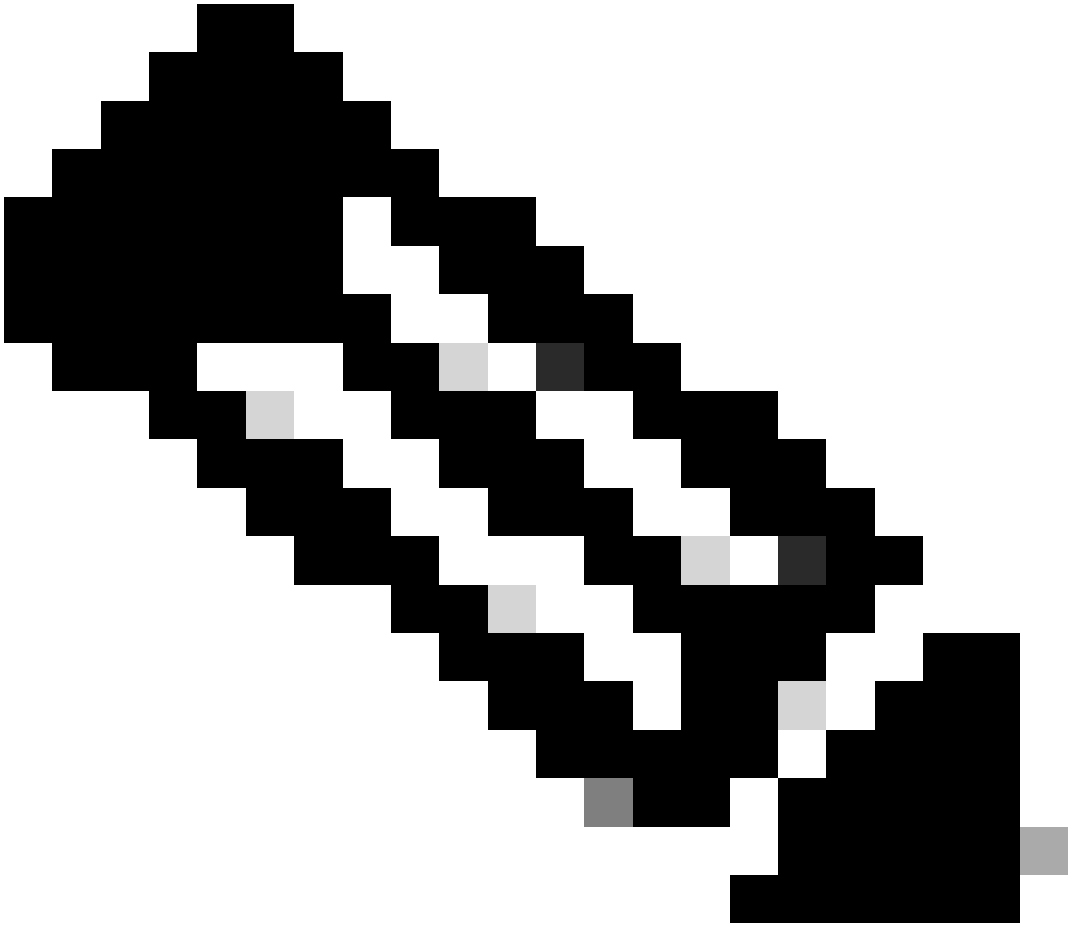
), Name(이름)으로 이동하고 Allow CHAP(CHAP 허용) 및 Allow MS-CHAPv1(인증 프로토콜 목록에서 MS-CHAPv1 허용)의 선택을 취소합니다. 저장을 선택합니다.



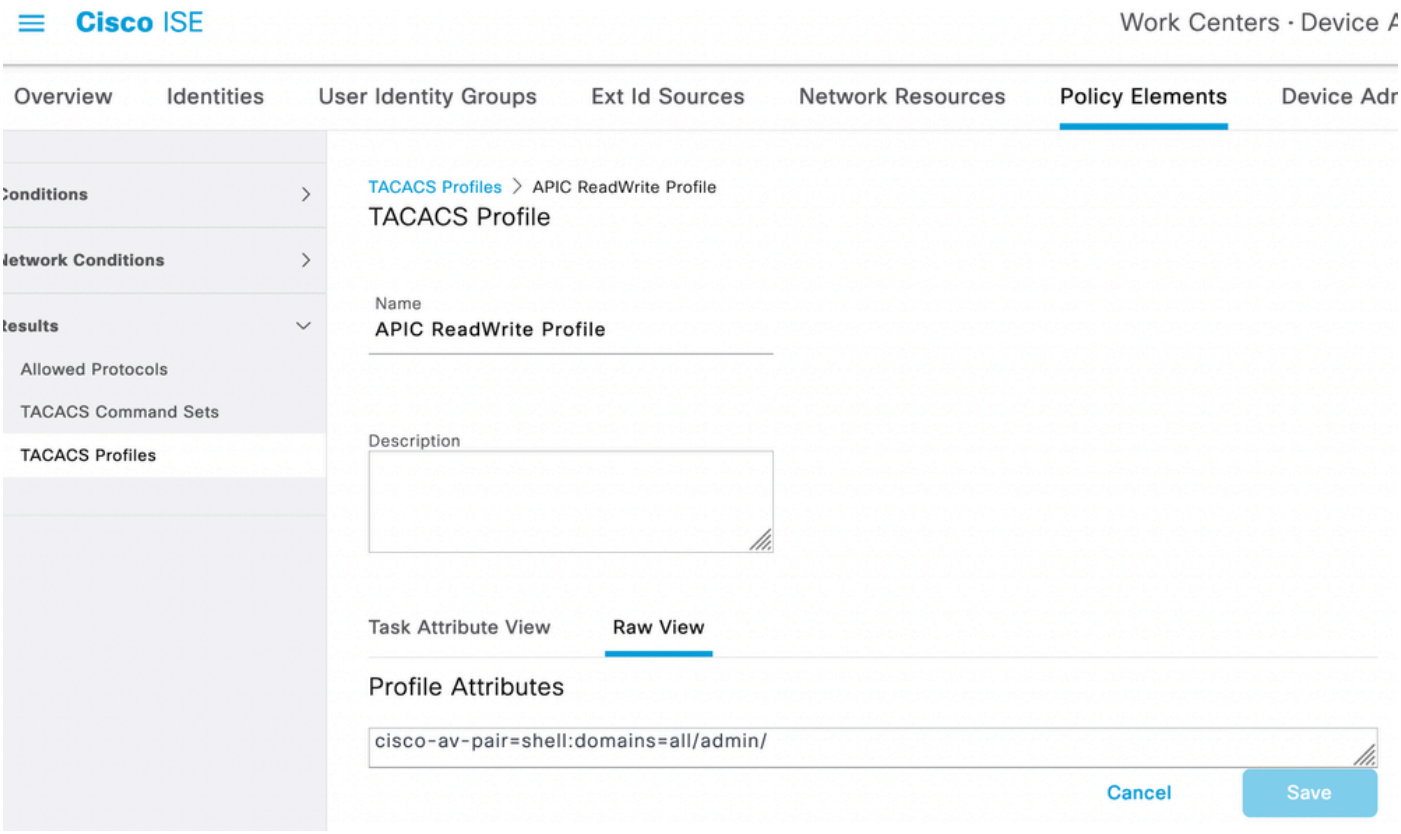
TACACS 허용 프로토콜

8. ☰로>Work Centers > Device Administration > Policy Elements > Results > TACACS Profile. 를 클릭하고add아래의 목록에 있는 특성을 기준으로 두 개의 프로파일을 생성합니다Raw View. 을 클릭합니다.Save

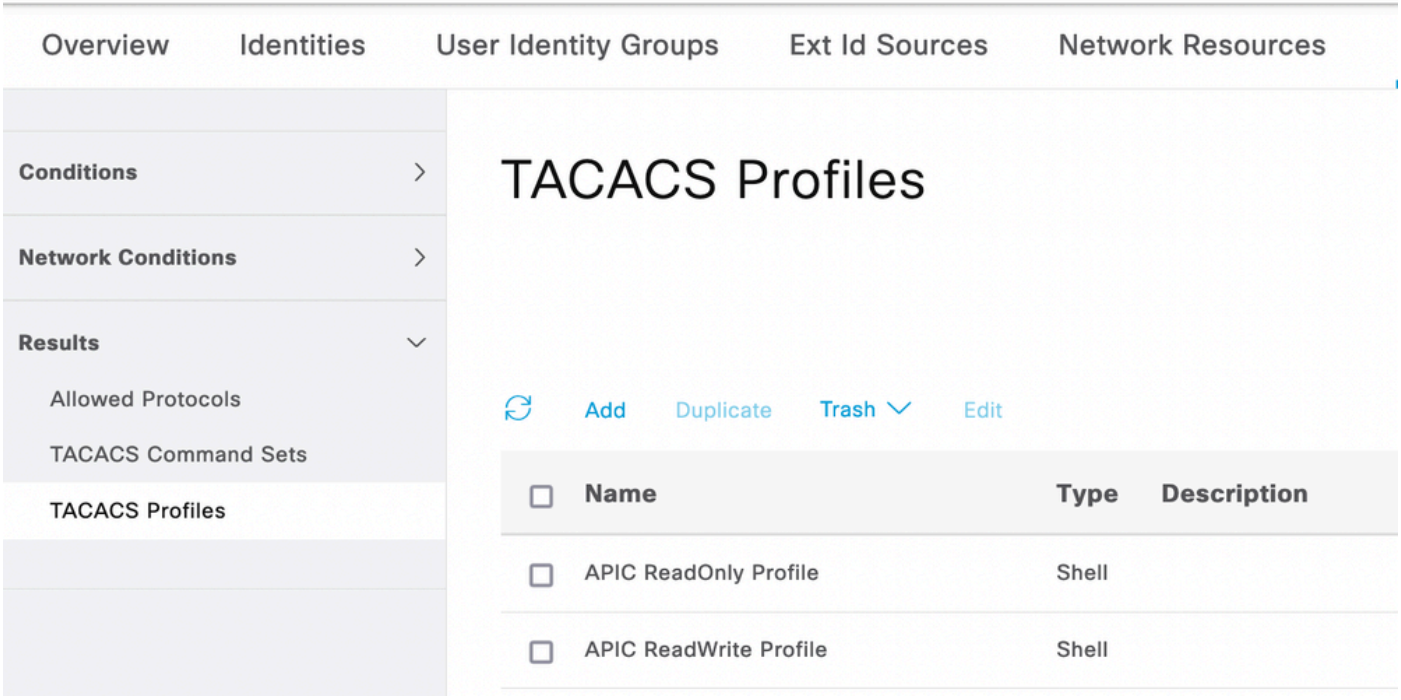
- 관리자 사용자: cisco-av-pair=shell:domains=all/admin/
- 읽기 전용 관리자 사용자: cisco-av-pair=shell:domains=all//read-all



참고: 공백 또는 추가 문자의 경우 권한 부여 단계가 실패합니다.

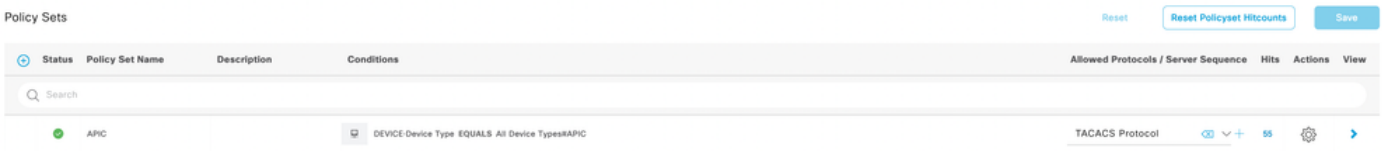


TACACS 프로파일



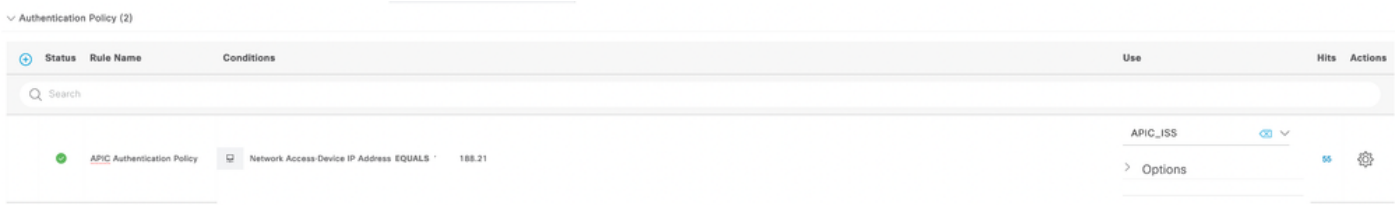
TACACS 관리자 및 읽기 전용 관리자 프로파일

9단계. ☰ 로>Work Centers > Device Administration > Device Admin Policy Set이동합니다. APICNew Policy Set(새 정책 집합)를 생성하고 이름을 정의한 다음 1단계에서 생성한 디바이스 유형을 선택합니다. 7단계에서 TACACS Protocol생성한 프로토콜을 허용되는 프로토콜로 선택하고 을 클릭합니다Save.

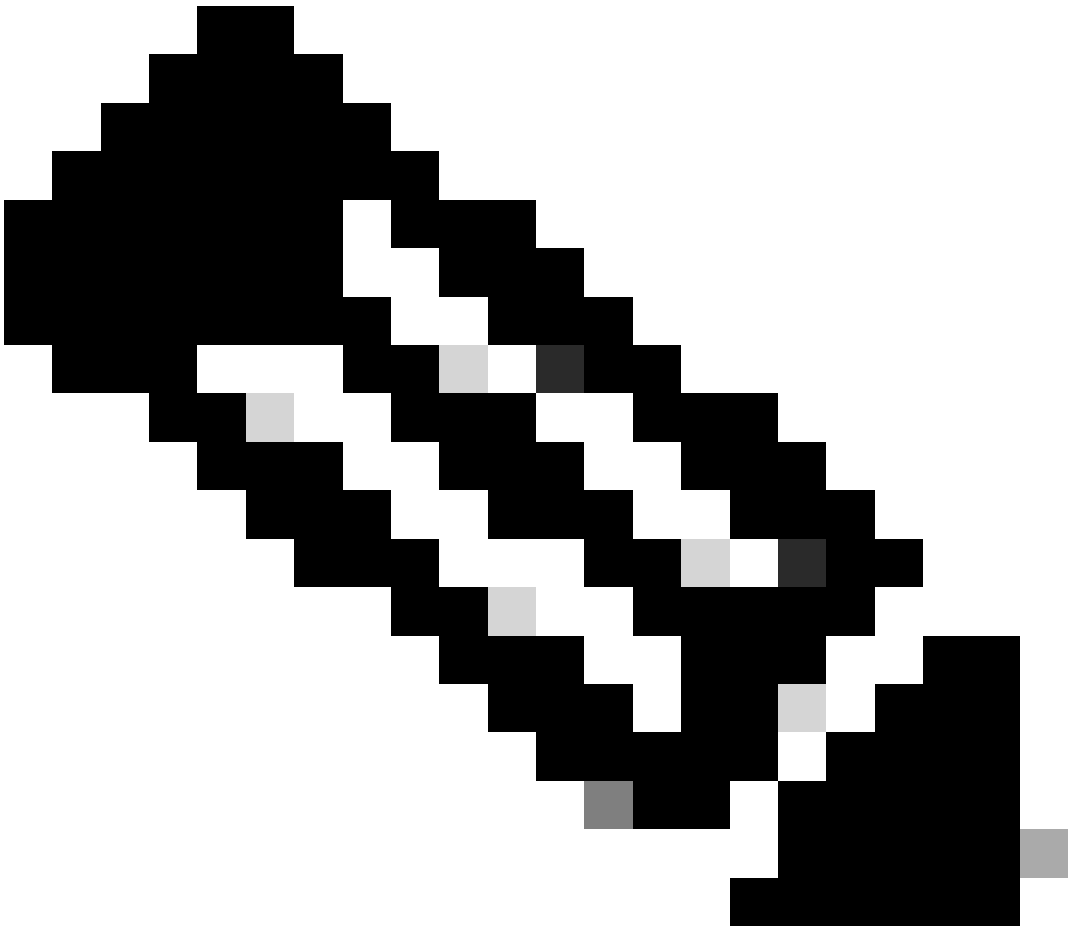


TACACS 정책 집합

10단계. New(새로 만들기)에서 오른쪽 화살표를Policy Set클릭하고>인증 정책을 생성합니다. 이름을 정의하고 조건으로 디바이스 IP 주소를 선택합니다. 그런 다음 6단계에서 생성한 ID 소스 시퀀스를 선택합니다.

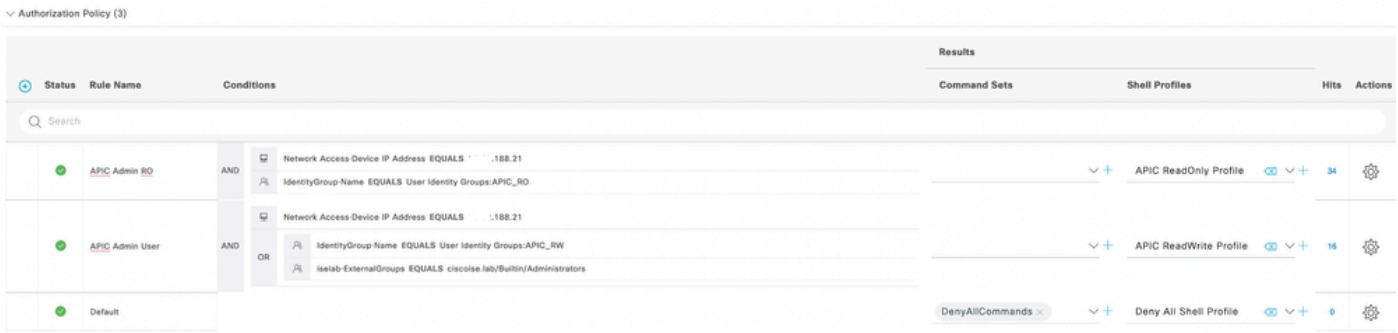


인증 정책



참고: 위치 또는 기타 특성을 인증 조건으로 사용할 수 있습니다.

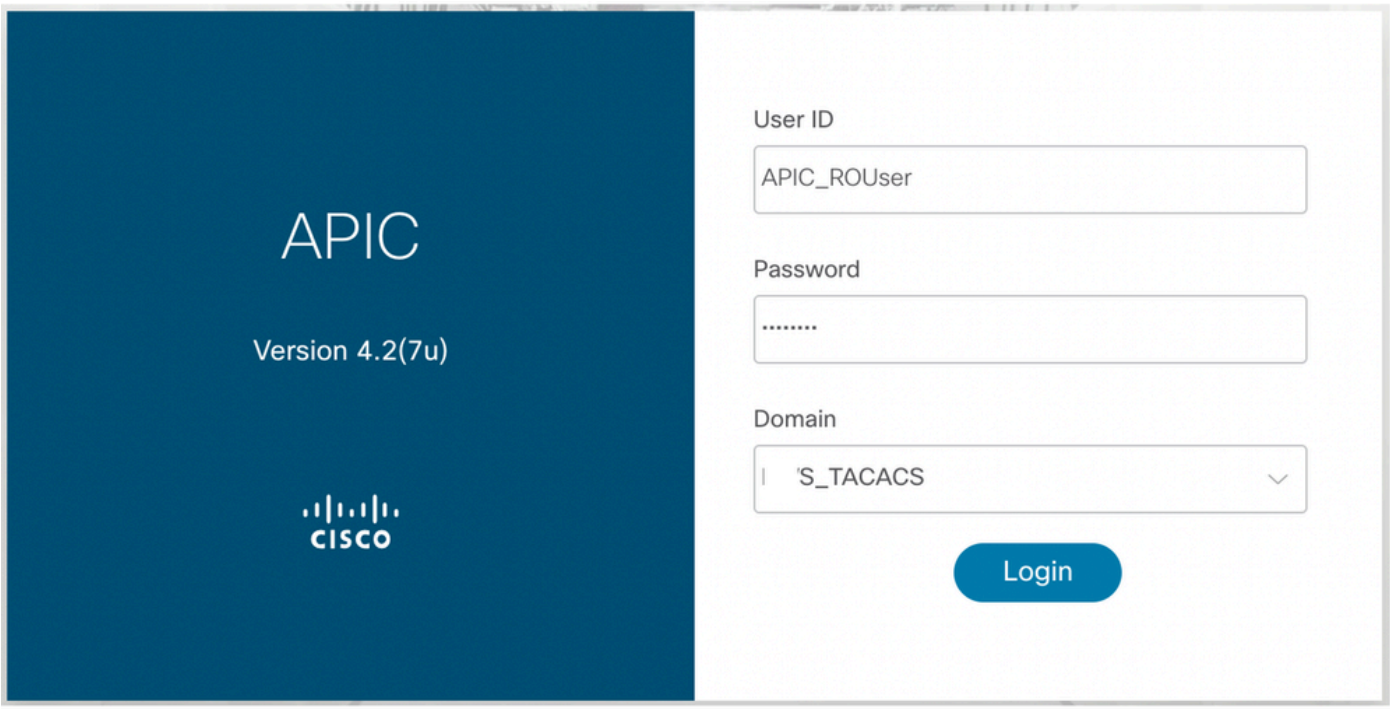
11단계. 각 관리자 사용자 유형에 대한 권한 부여 프로파일을 생성하고, 이름을 정의하고, 내부 사용자 및/또는 AD 사용자 그룹을 조건으로 선택합니다. APIC와 같은 추가 조건을 사용할 수 있습니다. 각 권한 부여 정책에서 적절한 셸 프로필을 선택하고 를Save클릭합니다.



TACACS 권한 부여 프로파일

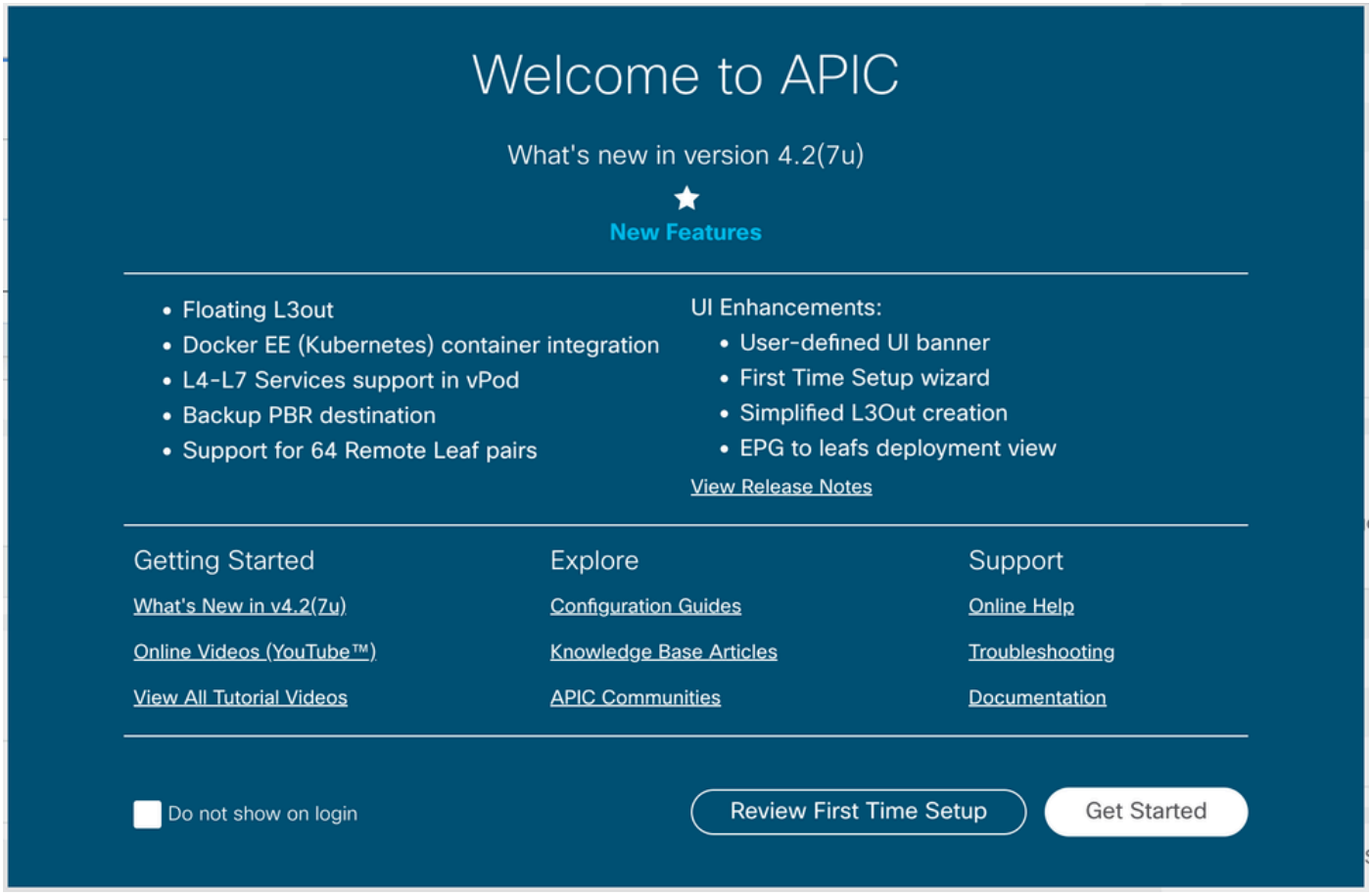
다음을 확인합니다.

1단계. 사용자 관리자 자격 증명을 사용하여 APIC UI에 로그인합니다. 목록에서 TACACS 옵션을 선택합니다.



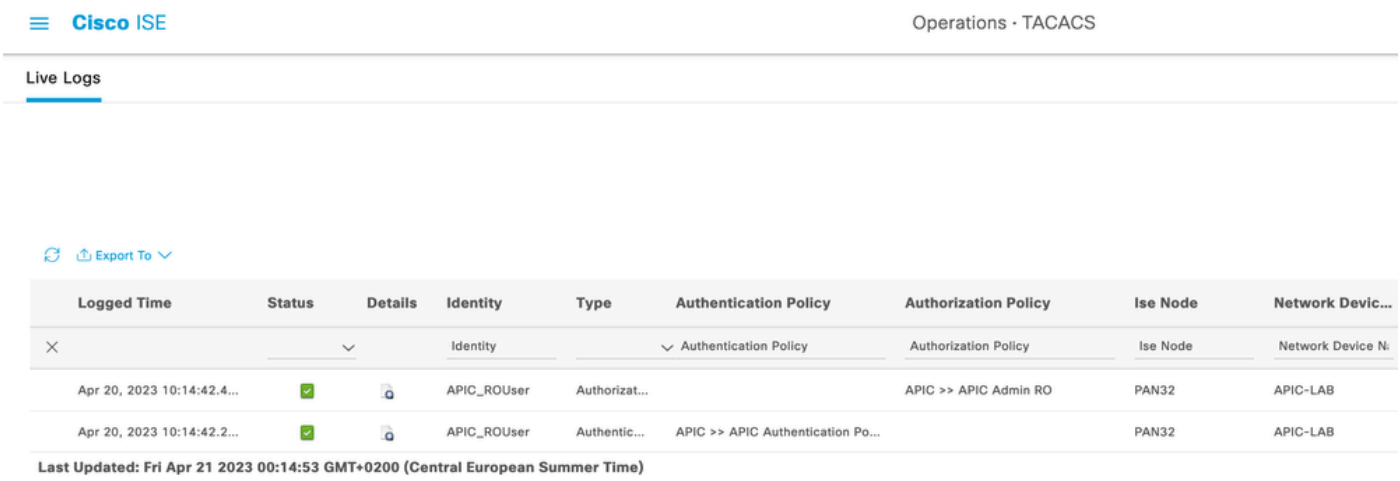
APIC 로그인

2단계. APIC UI에 대한 액세스를 확인하고 TACACS 라이브 로그에 적절한 정책이 적용되었는지 확인합니다.



APIC 환영 메시지

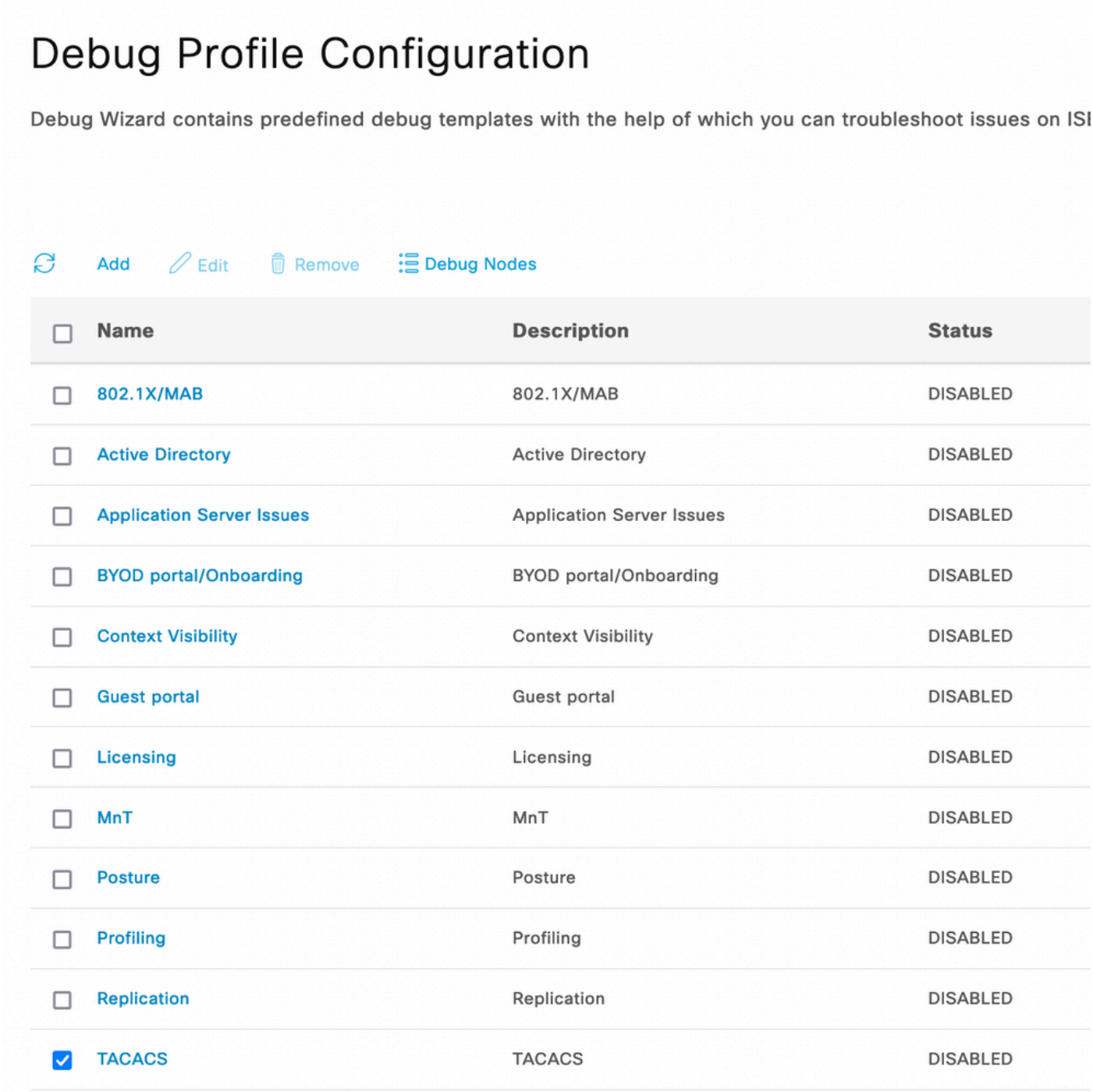
읽기 전용 관리자 사용자에 대해 1단계와 2단계를 반복합니다.



TACACS+ 라이브 로그

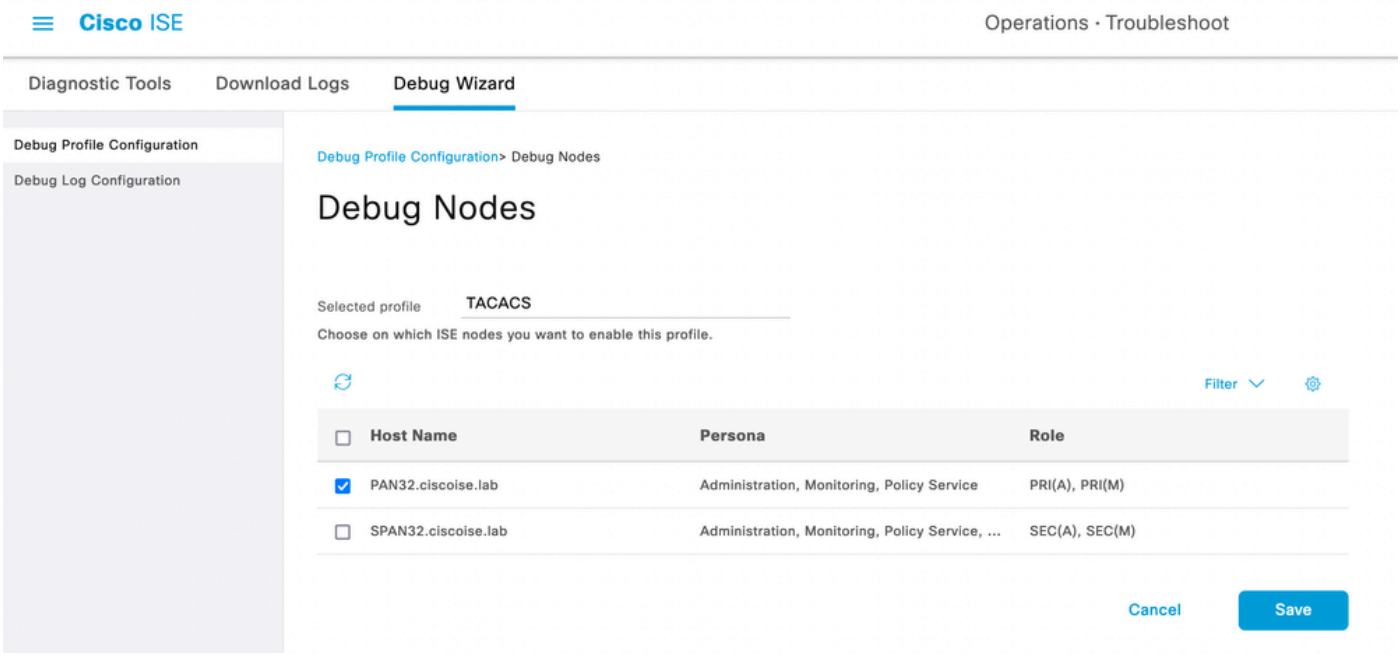
문제 해결

1단계. ☰로>Operations > Troubleshoot > Debug Wizard이동합니다. 을 선택하고TACACS을 클릭합니다 Debug Nodes.



디버그 프로필 컨피그레이션

2단계. 트래픽을 수신하는 노드를 선택하고 을 클릭합니다Save.



디버그 노드 선택

3단계. 새 테스트를 수행하고 아래와Operations > Troubleshoot > Download logs 같이 아래에 있는 로그를 다운로드합니다.

```
AcsLogs,2023-04-20 22:17:16,866,DEBUG,0x7f93cabc7700,cntx=0004699242,sesn=PAN32/469596415/70,CPMSession
```

디버깅에 인증 및 권한 부여 정보가 표시되지 않는 경우 다음을 검증합니다.

1. Devices Administration(디바이스 관리) 서비스는 ISE 노드에서 활성화됩니다.
2. 올바른 ISE IP 주소가 APIC 컨피그레이션에 추가되었습니다.
3. 방화벽이 중간에 있는 경우 포트 49(TACACS)가 허용되는지 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.