

# FCM(Secure Firewall Chassis Manager)에 대한 ISE Radius 인증 구성

## 목차

---

---

## 소개

이 문서에서는 ISE를 사용하는 Secure Firewall Chassis Manager에 대한 RADIUS 권한 부여/인증 액세스를 구성하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

Cisco에서는 다음 항목에 대해 숙지할 것을 권장합니다.

- FCM(보안 방화벽 새시 관리자)
- Cisco ISE(Identity Services Engine)
- Radius 인증

### 사용되는 구성 요소

- Cisco Firepower 4110 Security Appliance FXOS v2.12
- Cisco ISE(Identity Services Engine) v3.2 패치 4

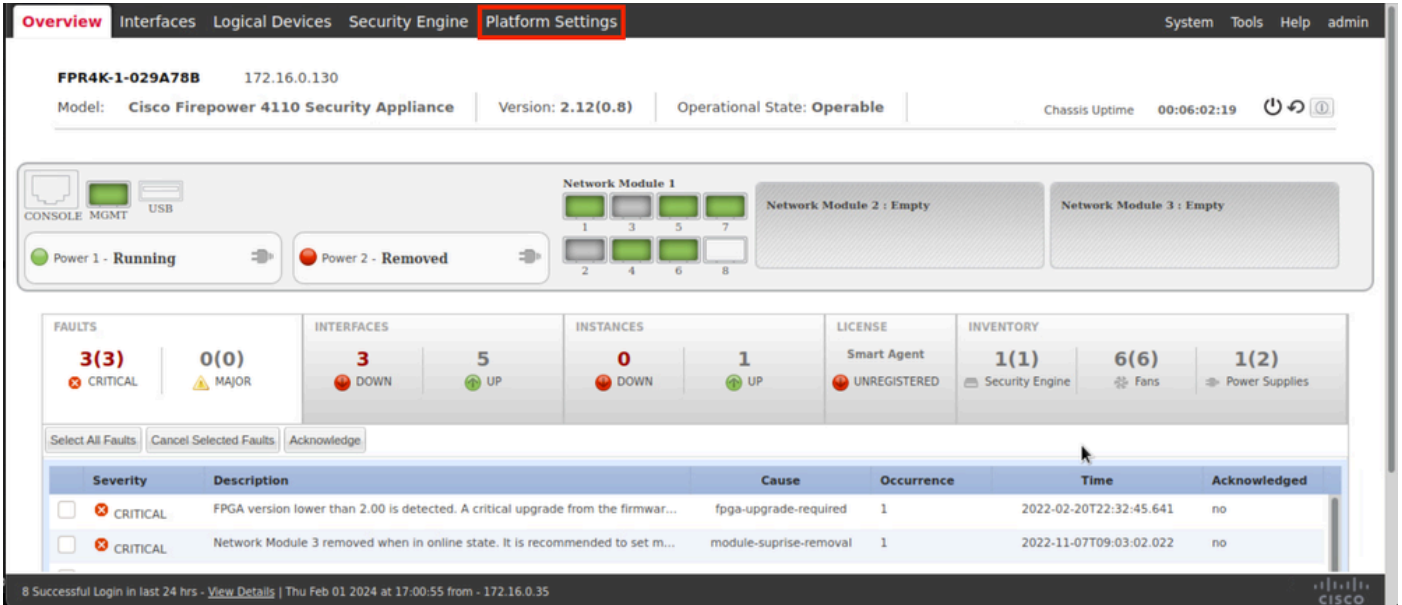
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 구성

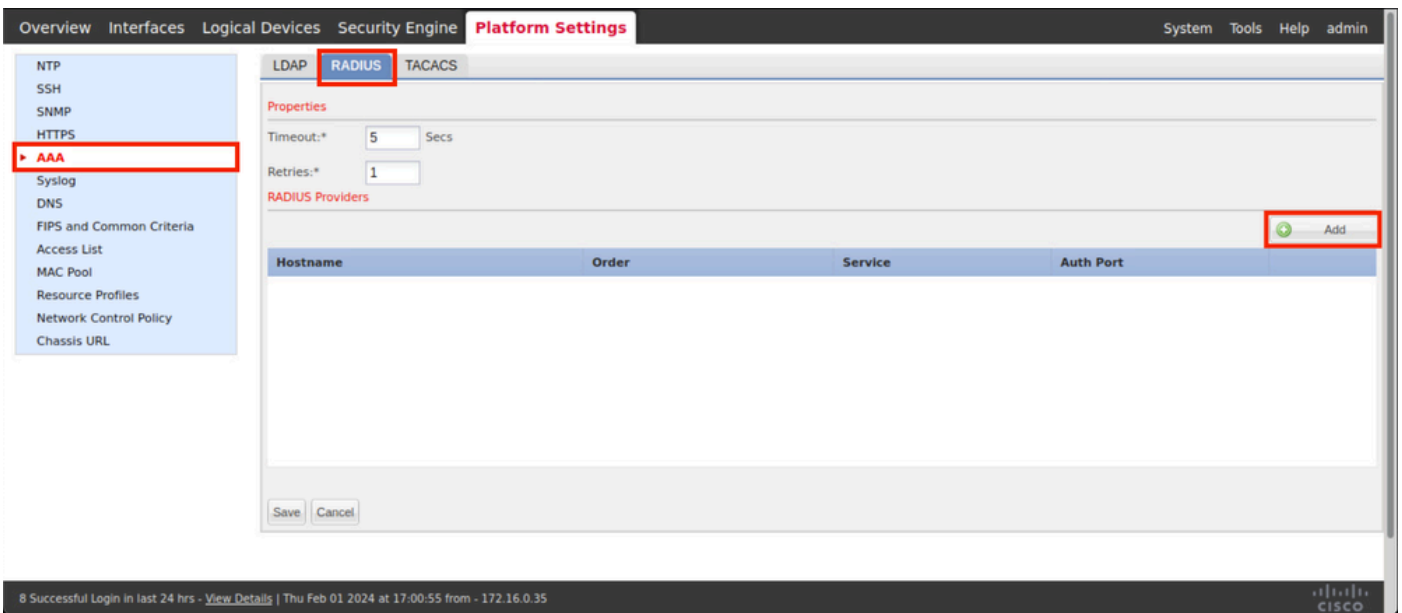
### 설정

#### 보안 방화벽 새시 관리자

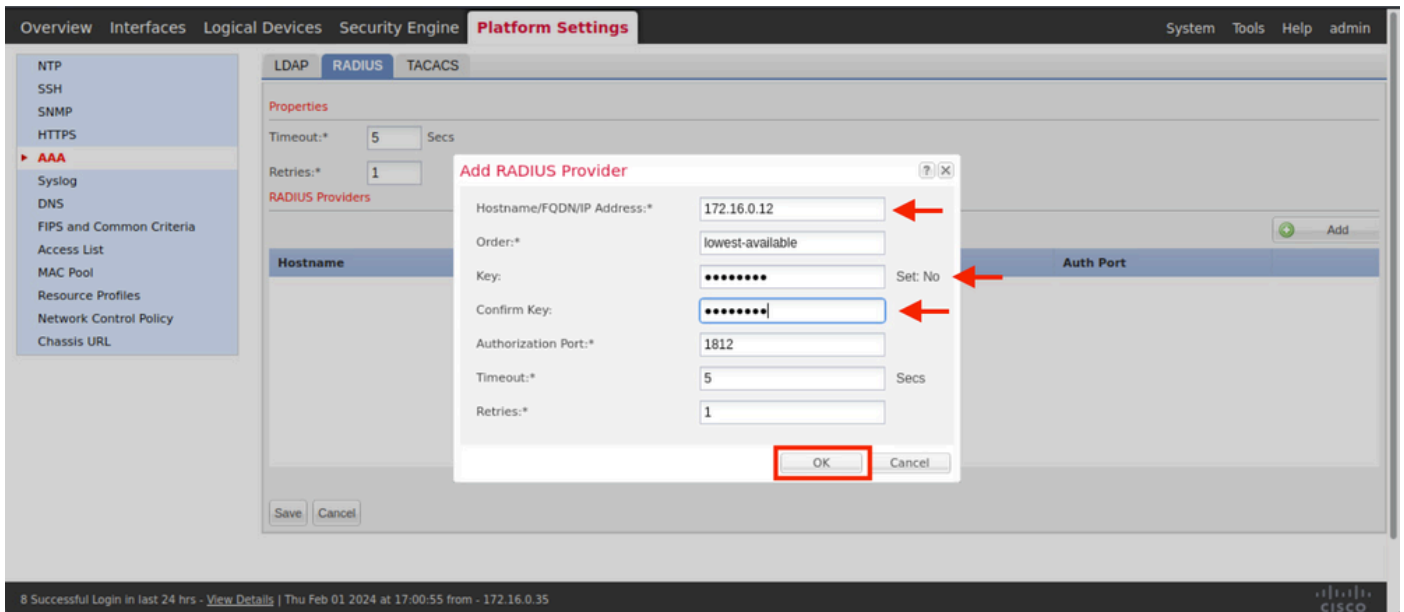
- 1단계. firepower Chassis Manager GUI에 로그인합니다.
- 2단계. 플랫폼 설정으로 이동합니다.



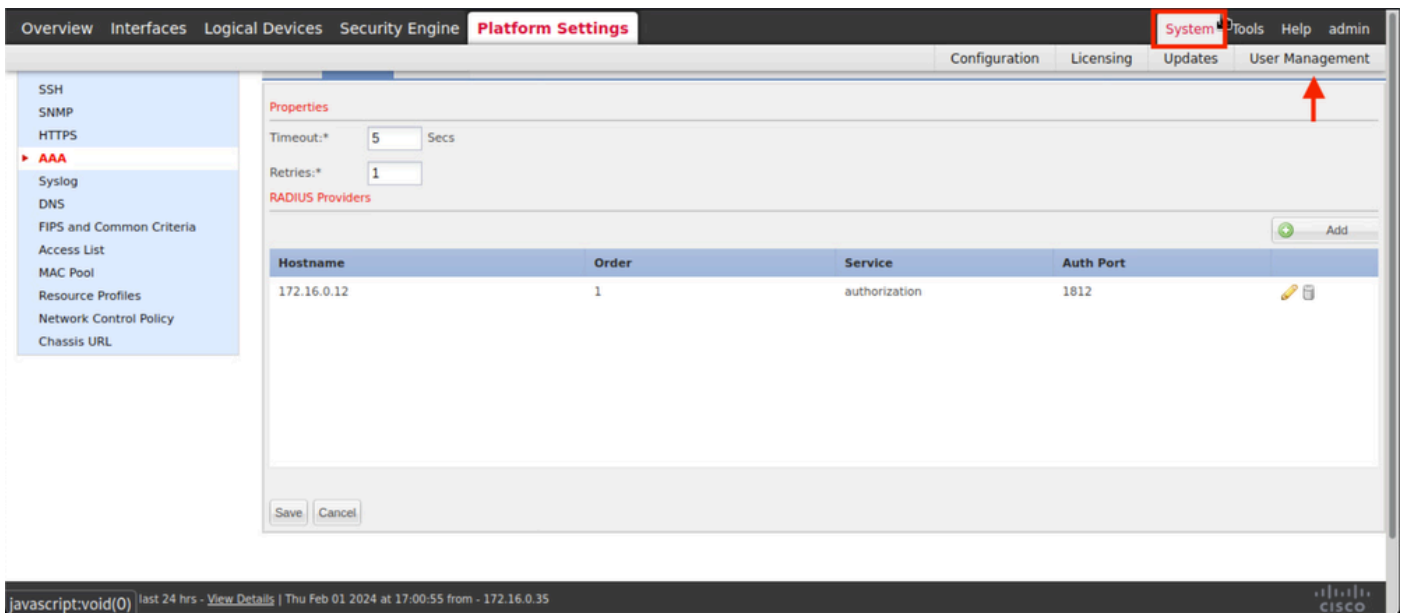
3단계. 왼쪽 메뉴에서 AAA 위를 클릭합니다. Radius를 선택하고 새 RADIUS 제공자를 추가합니다.



4단계. 프롬프트 메뉴에 Radius 제공자의 요청 된 정보를 채웁니다. OK(확인)를 클릭합니다.



5단계. System(시스템) > User Management(사용자 관리)로 이동합니다.



6단계. Settings(설정) 탭을 클릭하고 드롭다운 메뉴에서 Default Authentication(기본 인증)을 Radius로 설정한 다음 아래로 스크롤하여 컨피그레이션을 저장합니다.


Overview Interfaces Logical Devices Security Engine Platform Settings **System** Tools Help admin

Configuration Licensing Updates **User Management**

Local Users **Settings**

**Default Authentication**

Local  \*Local is fallback authentication method

Local  
RADIUS   
LDAP  
TACACS  
None  
No-Login

Console Authentication

**Remote User Settings**

Remote User Role Policy

**Local User Settings**

Password Strength Check  Enable

History Count  (0-disabled,1-15)

Change Interval   (1-730 hours)

Change Count  (1-10)

No Change Interval   (1-730 hours)

Days until Password Expiration  (0-never,1-9999 days)

Password Expiration Warning Period  (0-9999 days)

Expiration Grace Period  (0-9999 days)

Password Reuse Interval  (0-disabled,1-365 days)

Session Timeout(web UI,ssh,telnet)  (0-never,3600 seconds)

8 Successful Login in last 24 hrs - [View Details](#) | Thu Feb 01 2024 at 17:00:55 from - 172.16.0.35

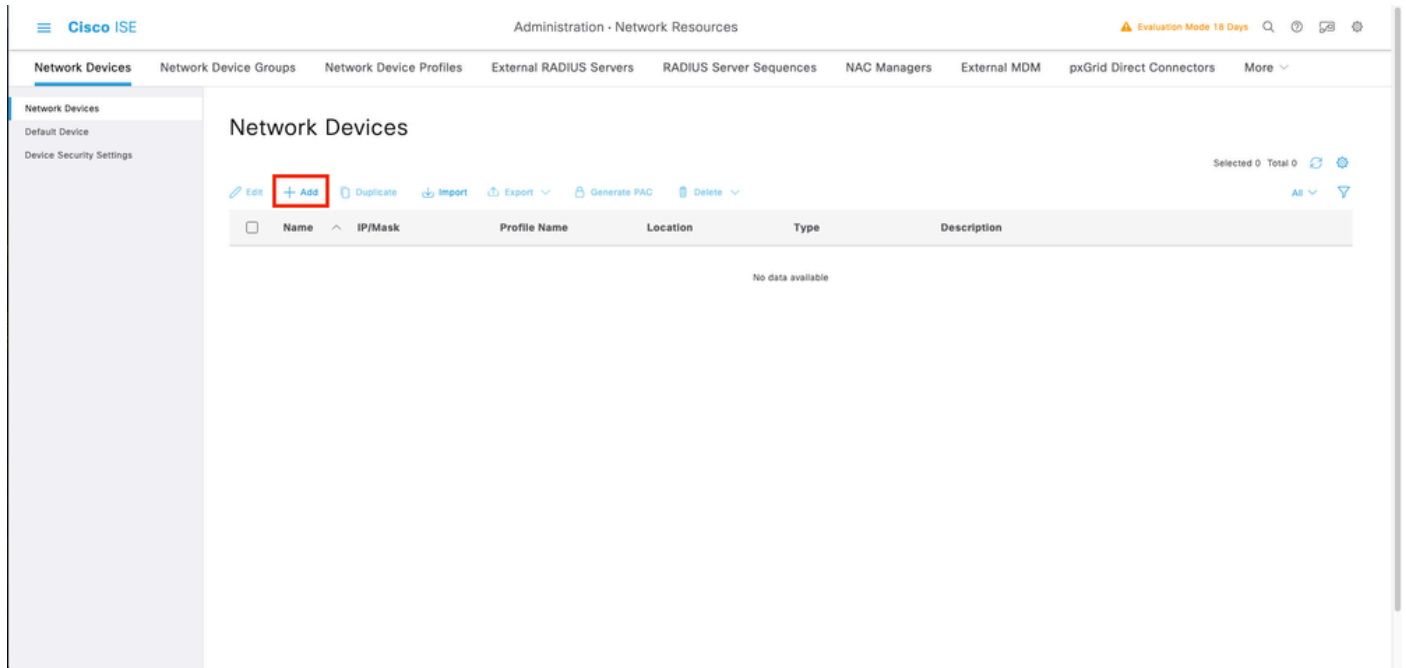
CISCO

참고: 이 시점에서 FCM 컨피그레이션이 완료되었습니다.

# ISE(Identity Service Engine)

1단계. 새 네트워크 디바이스를 추가합니다.

왼쪽 상단 모서리에 있는 버거 아이콘 ≡ > 관리 > 네트워크 리소스 > 네트워크 장치 > +Add로 이동합니다.

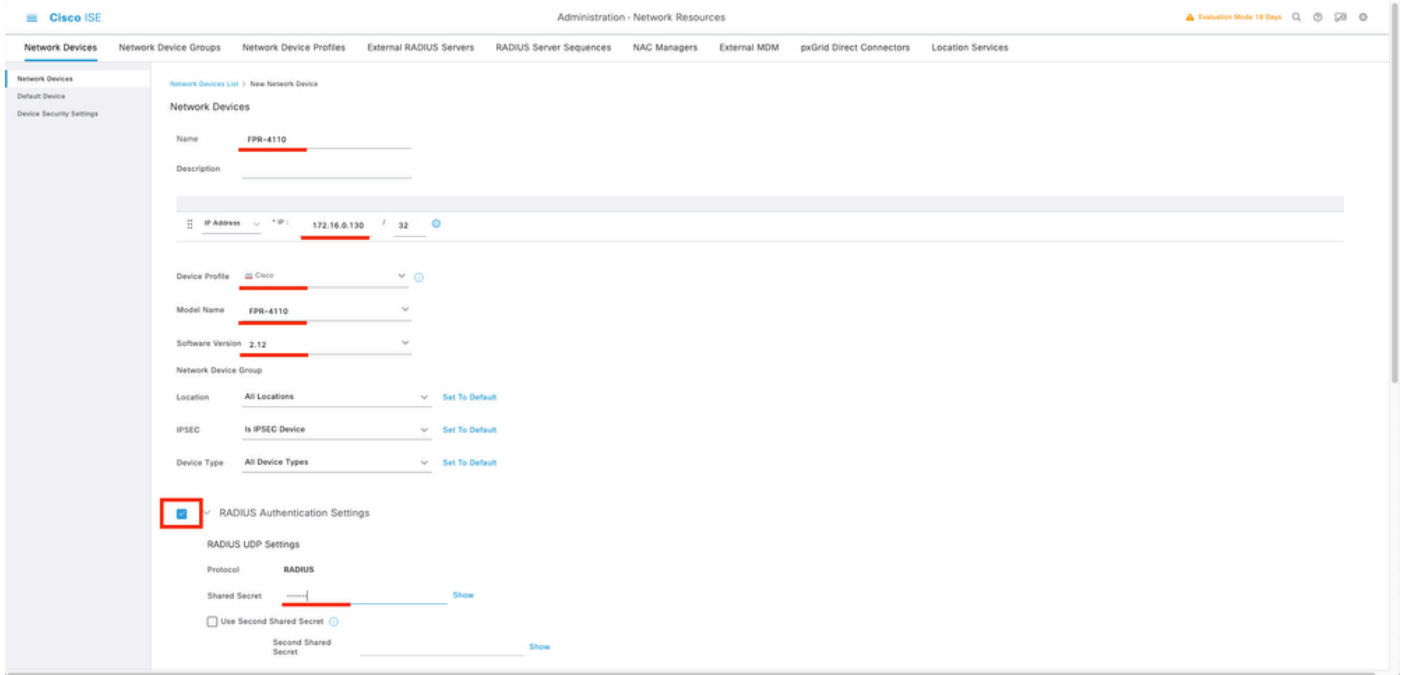


2단계. 새 네트워크 디바이스 정보에 대해 요청한 매개변수를 채웁니다.

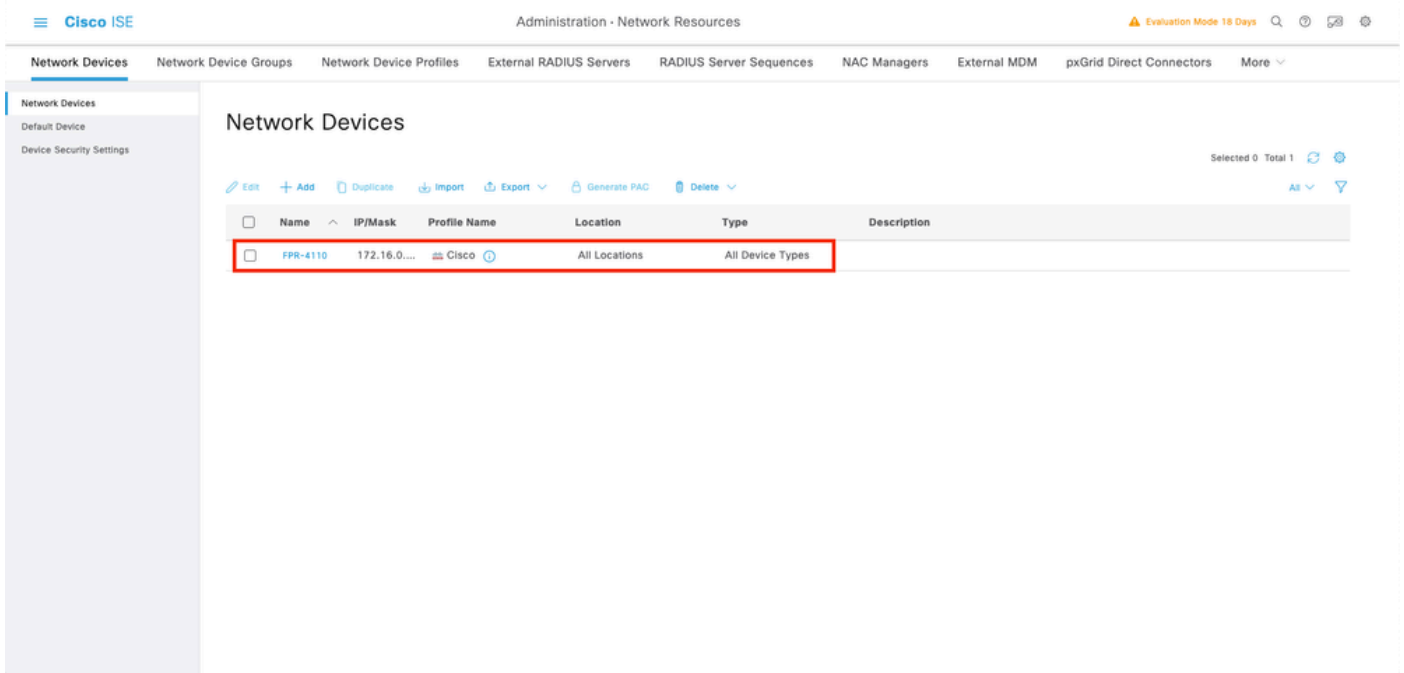
2.1 RADIUS 확인란을 선택합니다

2.2 FCM Radius 컨피그레이션과 동일한 공유 암호 키를 구성합니다.

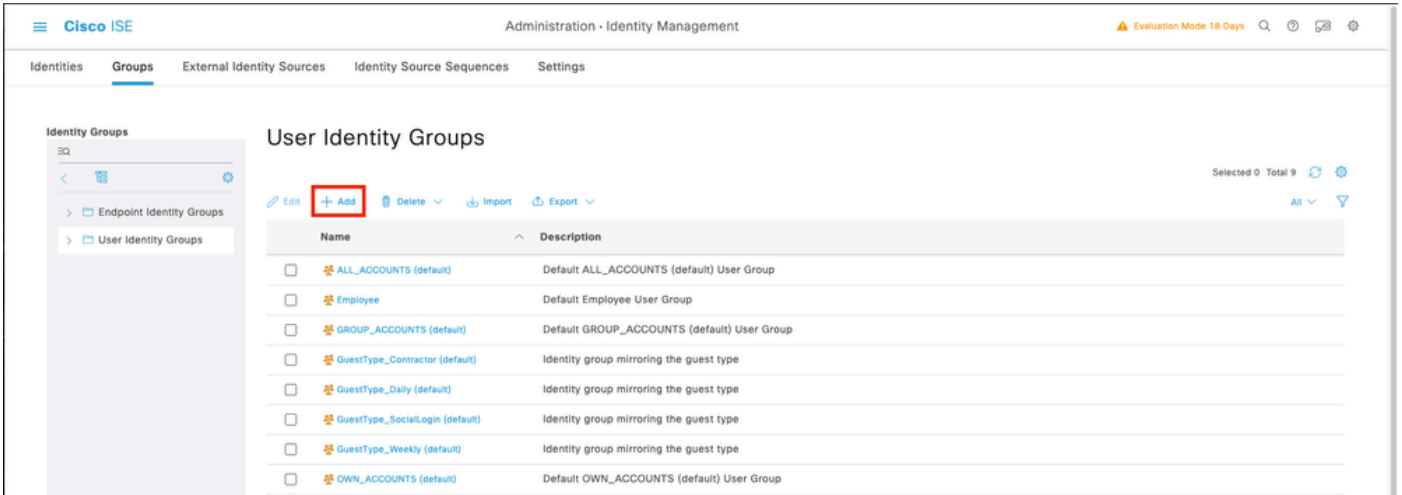
2.1 아래로 스크롤하여 Submit(제출)을 클릭합니다.



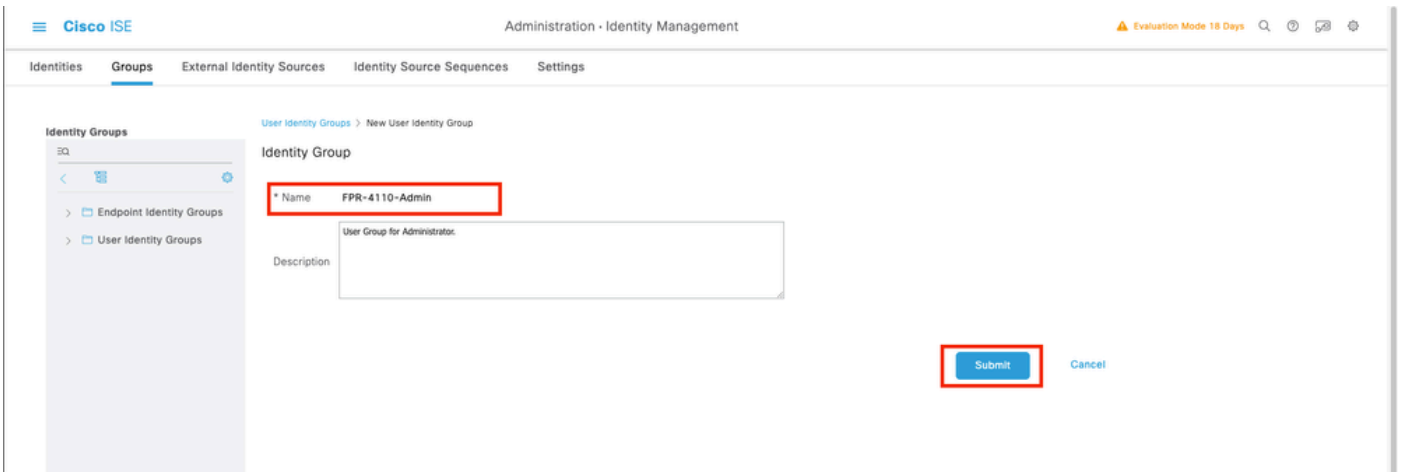
3단계. 새 디바이스가 Network Devices(네트워크 디바이스)에 표시되는지 확인합니다.



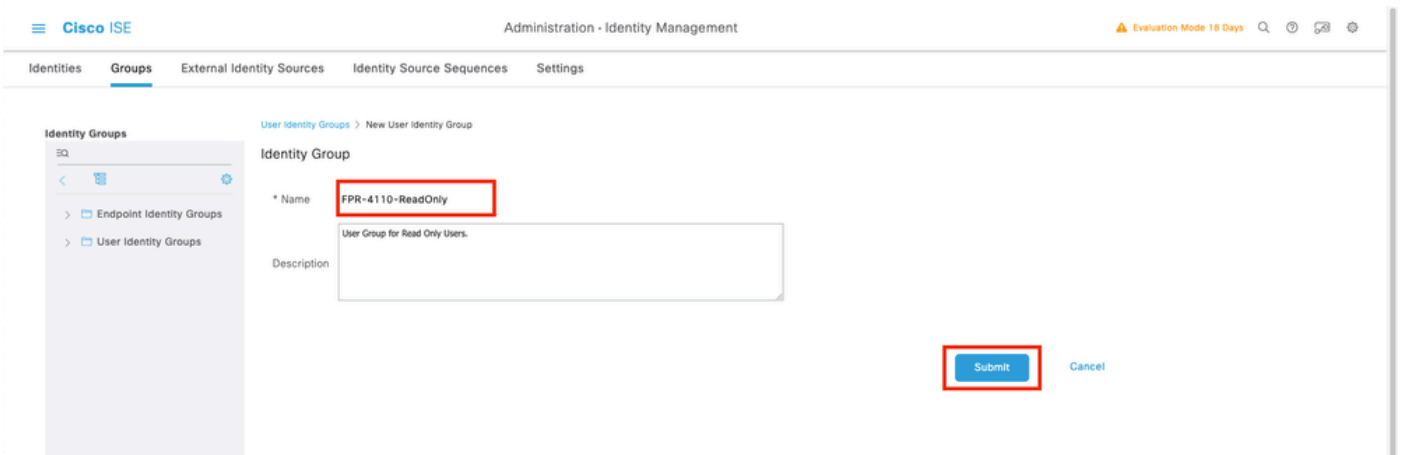
4단계. 필요한 사용자 ID 그룹을 생성합니다. 왼쪽 상단 구석에 있는 버거 아이콘 ≡ > 관리 > 신원 관리 > 그룹 > 사용자 ID 그룹 > + 추가



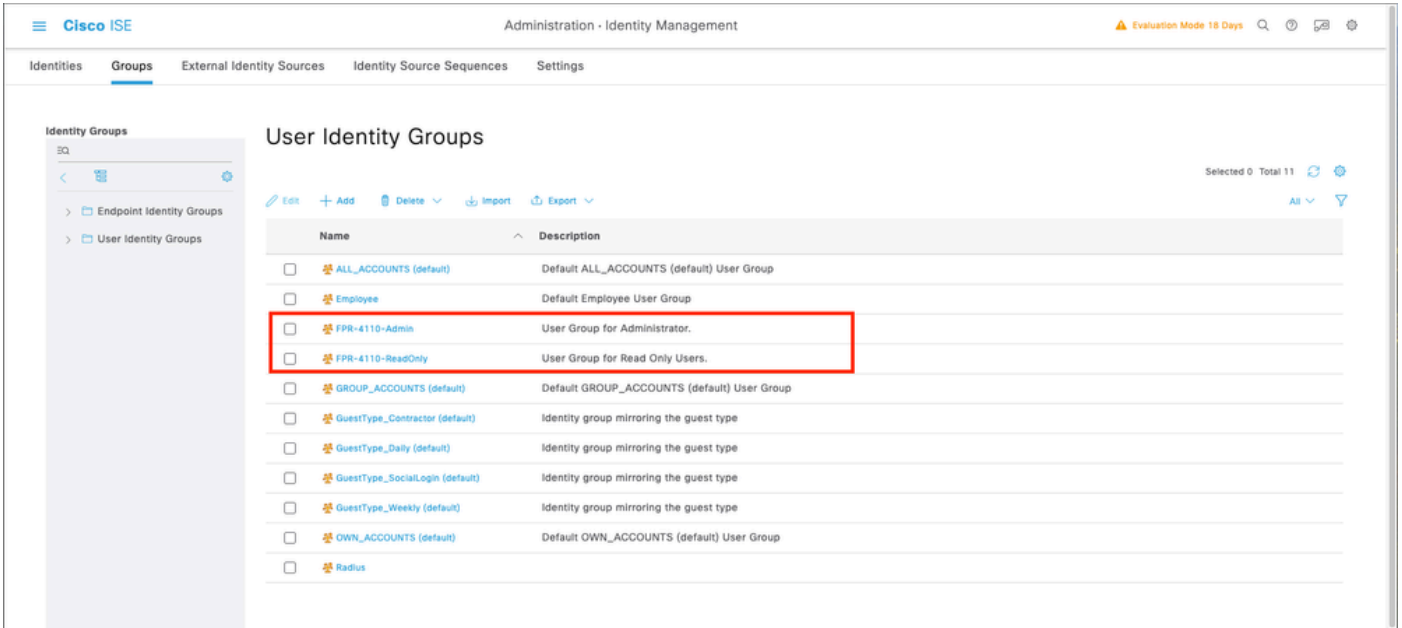
5단계. 컨피그레이션을 저장하려면 Admin User Identity Group(관리자 사용자 ID 그룹)의 이름을 설정하고 Submit(제출)을 클릭합니다.



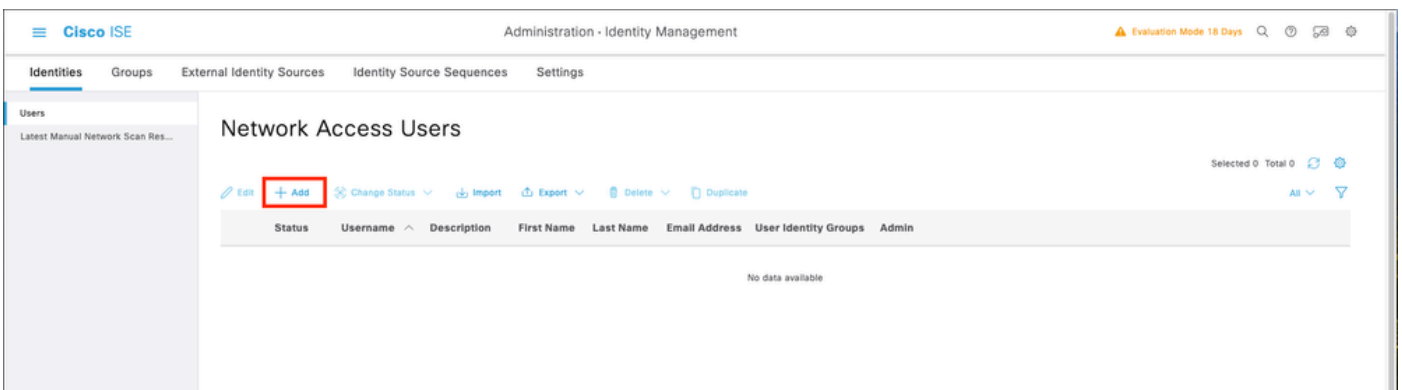
5.1 ReadOnly 사용자에게 대해 동일한 프로세스를 반복합니다.



6단계. User Identity Groups(사용자 ID 그룹) 아래에 새 사용자 그룹이 표시되는지 확인합니다.

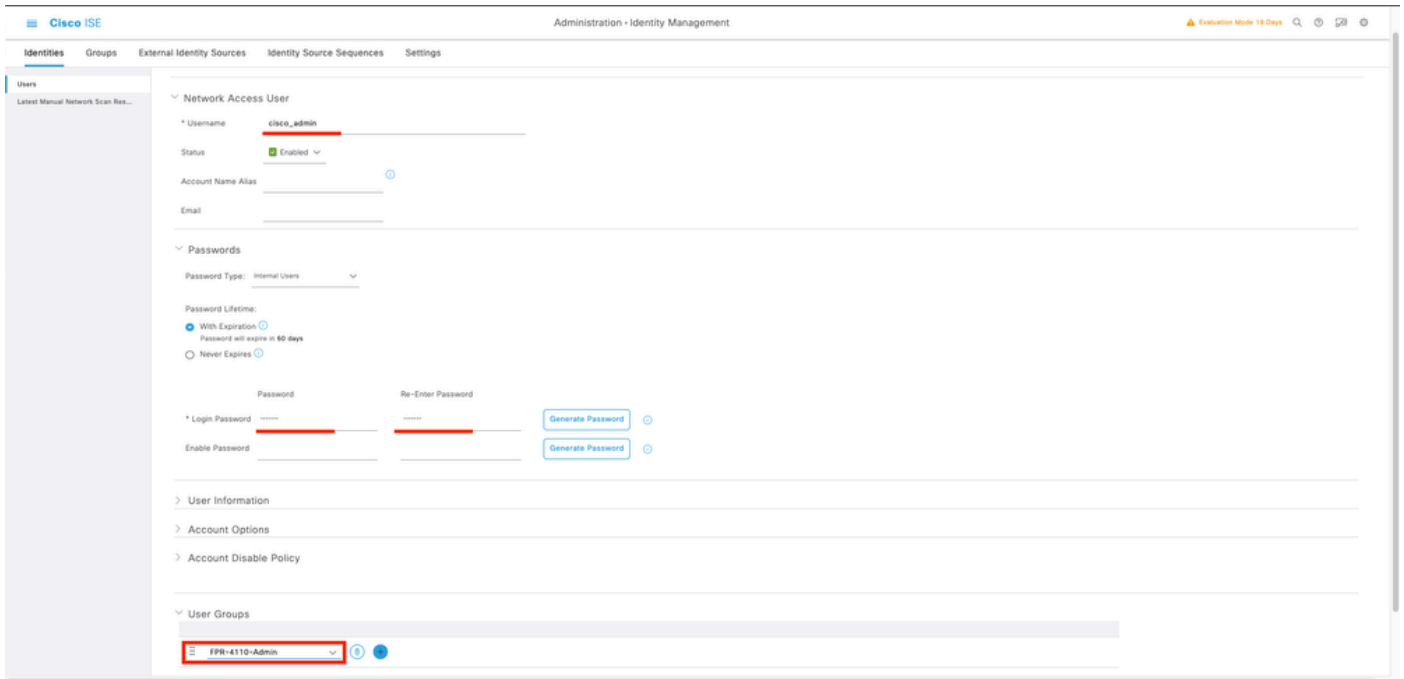


7단계. 로컬 사용자를 생성하고 해당 Responder 그룹에 추가합니다. 버거 아이콘으로 이동 ≡ > 관리 > 신원 관리 > ID > + 추가.

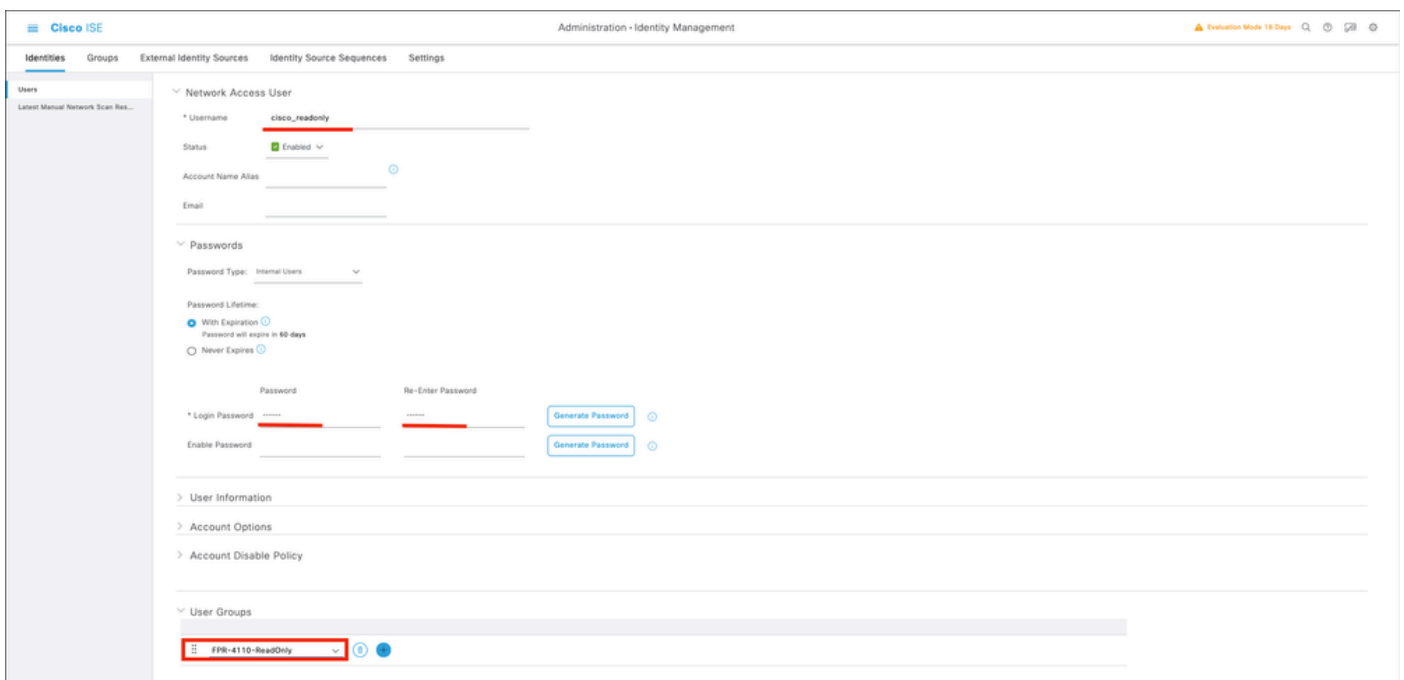


7.1 관리자 권한이 있는 사용자를 추가합니다. 이름, 비밀번호를 설정하고 FPR-4110-Admin에 할당한 후 아래로 스크롤하고 Submit(제출)을 클릭하여 변경 사항을 저장합니다.

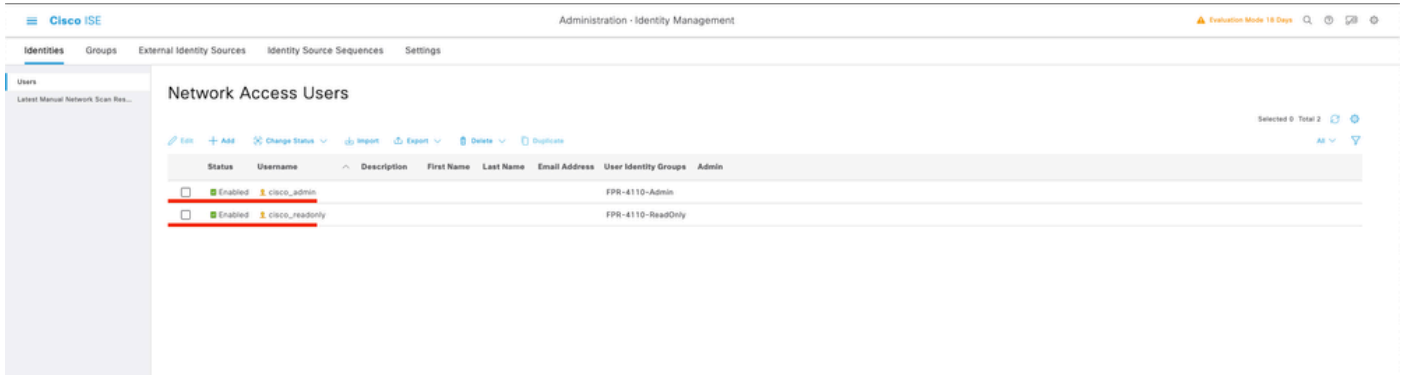




7.2 읽기 전용 권한이 있는 사용자를 추가합니다. 이름, 비밀번호를 설정하고 FPR-4110-ReadOnly에 할당한 후 아래로 스크롤하고 Submit(제출)을 클릭하여 변경 사항을 저장합니다.



7.3 사용자가 Network Access Users(네트워크 액세스 사용자)에 있는지 확인합니다.



8단계.관리자 사용자에게 권한 부여 프로파일을 생성합니다.

FXOS 새시에는 다음과 같은 사용자 역할이 포함됩니다.

- 관리자 - 전체 시스템에 대한 완전한 읽기 및 쓰기 액세스. 기본 관리자 계정은 기본적으로 이 역할에 할당되며 변경할 수 없습니다.
- 읽기 전용 - 시스템 상태를 수정할 권한이 없는 시스템 컨피그레이션에 대한 읽기 전용 액세스.
- 운영 - NTP 컨피그레이션, Smart Licensing용 Smart Call Home 컨피그레이션, 시스템 로그 (syslog 서버 및 결함 포함)에 대한 읽기 및 쓰기 액세스 시스템의 나머지 부분에 대한 읽기 액세스.
- AAA - 사용자, 역할 및 AAA 구성에 대한 읽기 및 쓰기 액세스. 시스템의 나머지 부분에 대한 읽기 액세스

각 역할의 특성:

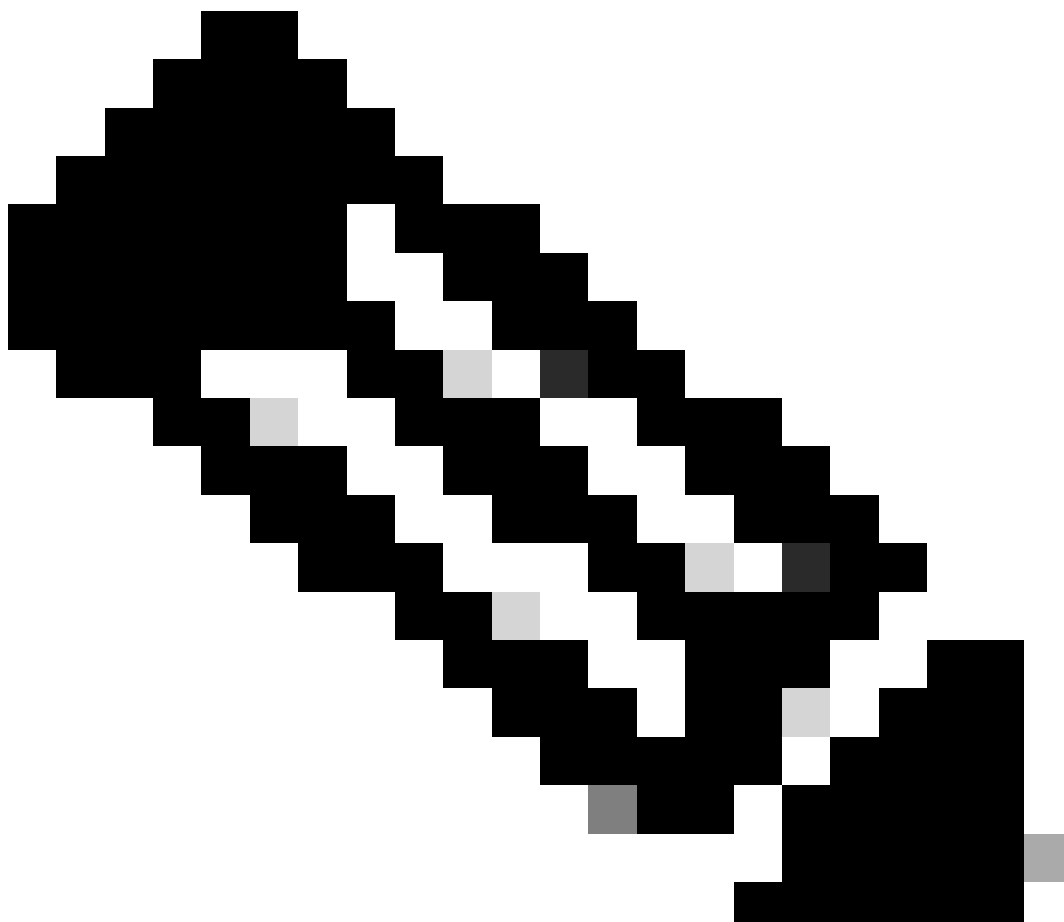
cisco-av-pair=shell:roles="admin"

cisco-av-pair=shell:roles="aaa"

cisco-av-pair=shell:roles="operations"

cisco-av-pair=shell:roles="읽기 전용"

---

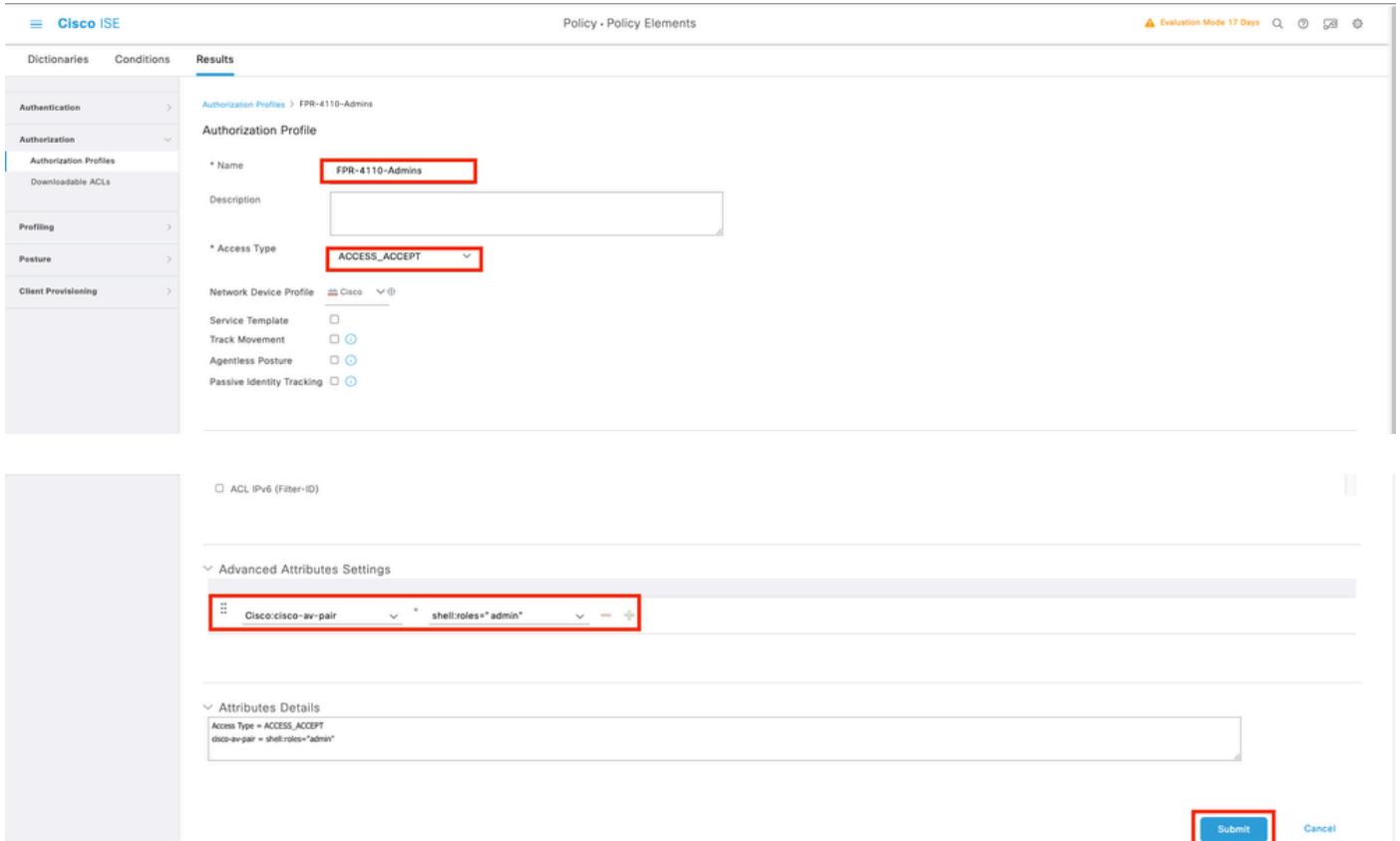


참고: 이 설명서는 admin 및 read-only 특성만 정의합니다.

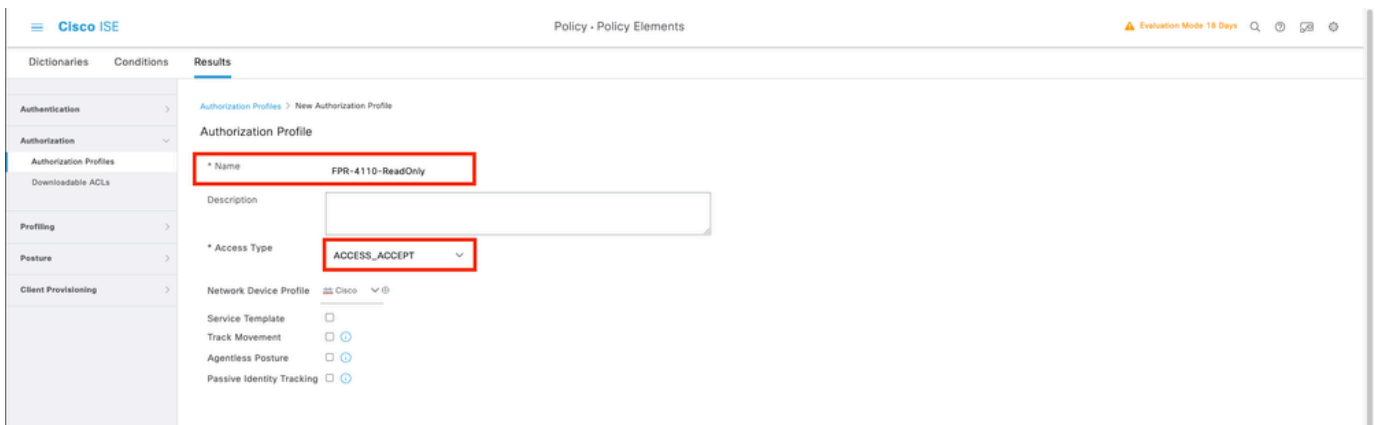
---

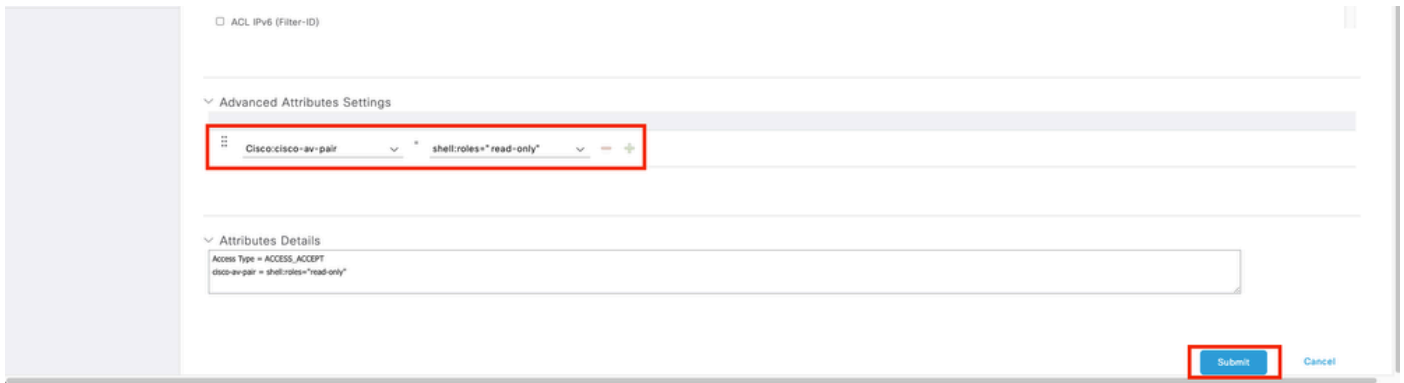
버거 아이콘으로 이동 ≡ > 정책 > 정책 구성 요소 > 결과 > 인증 > 인증 프로파일 > +추가.

권한 부여 프로파일의 이름을 정의하고, Access Type(액세스 유형)을 ACCESS\_ACCEPT로 남겨두고 Advanced Attributes Settings(고급 특성 설정)에서 cisco-av-pair=shell:roles="admin"을 추가하고 Submit(제출)을 클릭합니다.



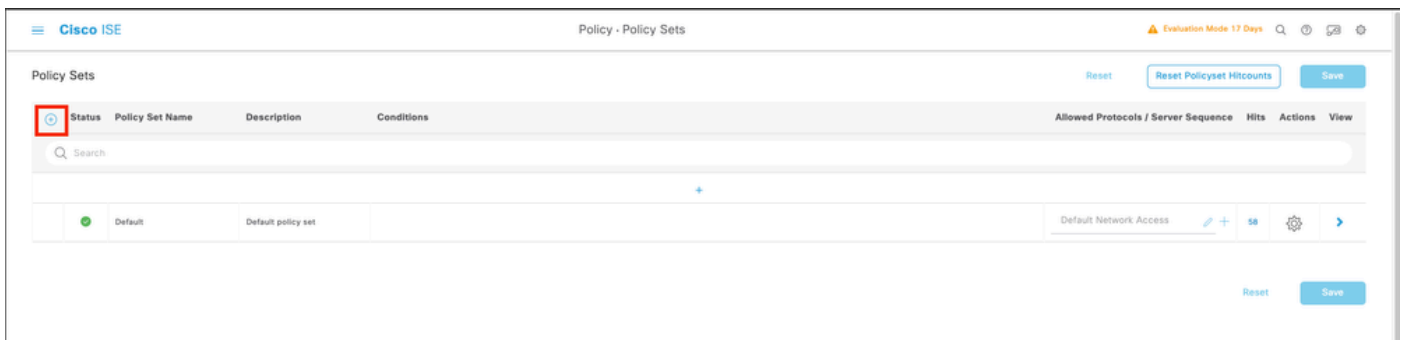
8.1 이전 단계를 반복하여 읽기 전용 사용자에 대한 권한 부여 프로파일을 생성합니다. 이번에는 Administrator 대신 읽기 전용 값으로 Radius 클래스를 만듭니다.



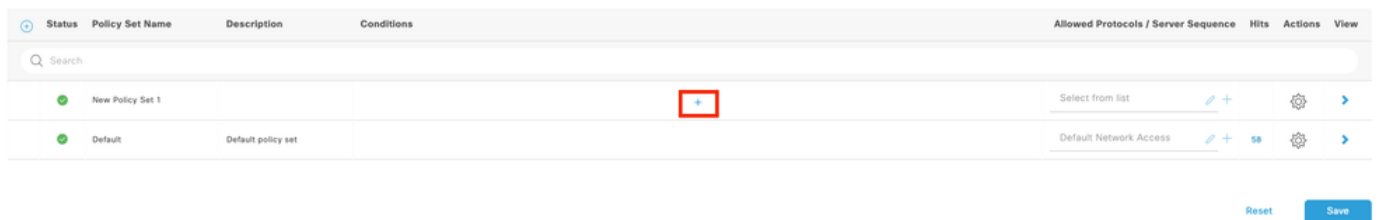


9단계.FMC IP 주소와 일치하는 정책 집합을 생성합니다. 이는 다른 디바이스에서 사용자에게 액세스 권한을 부여하는 것을 방지하기 위한 것입니다.

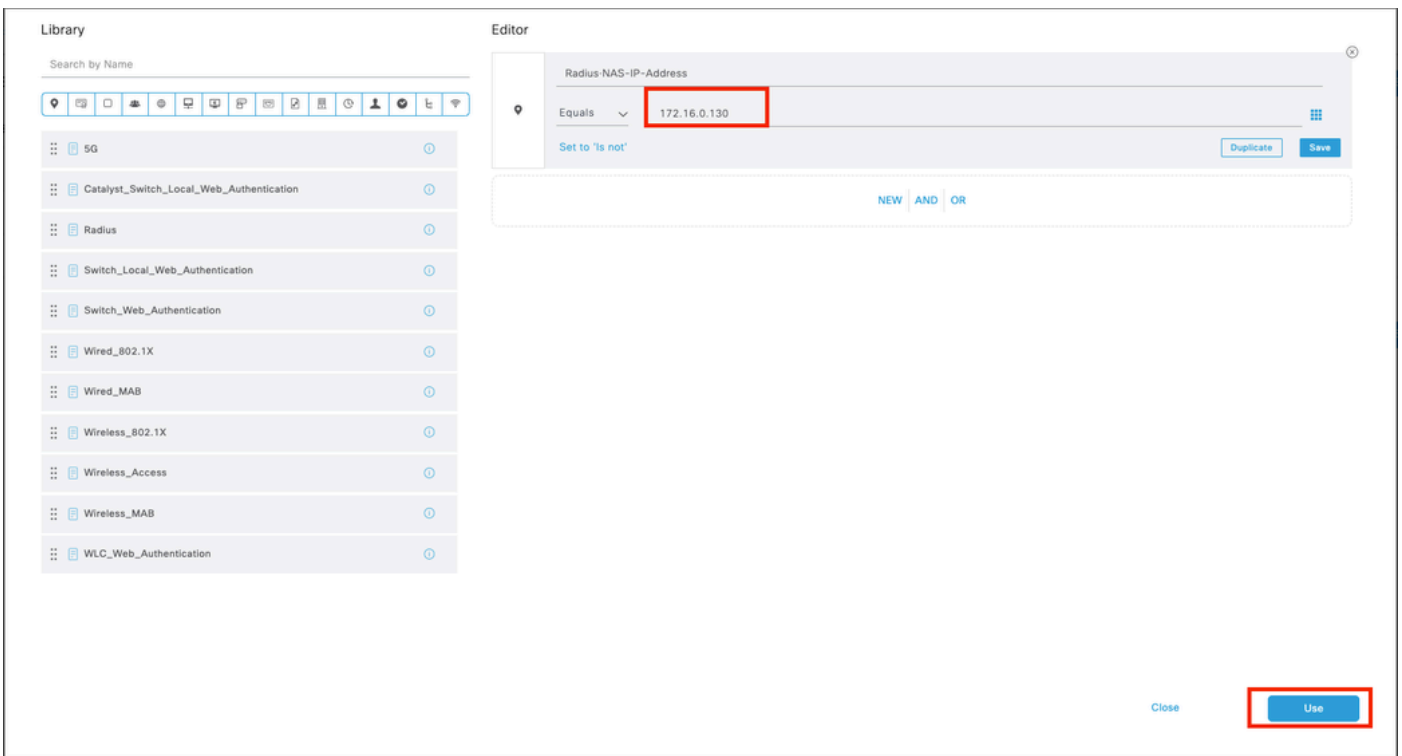
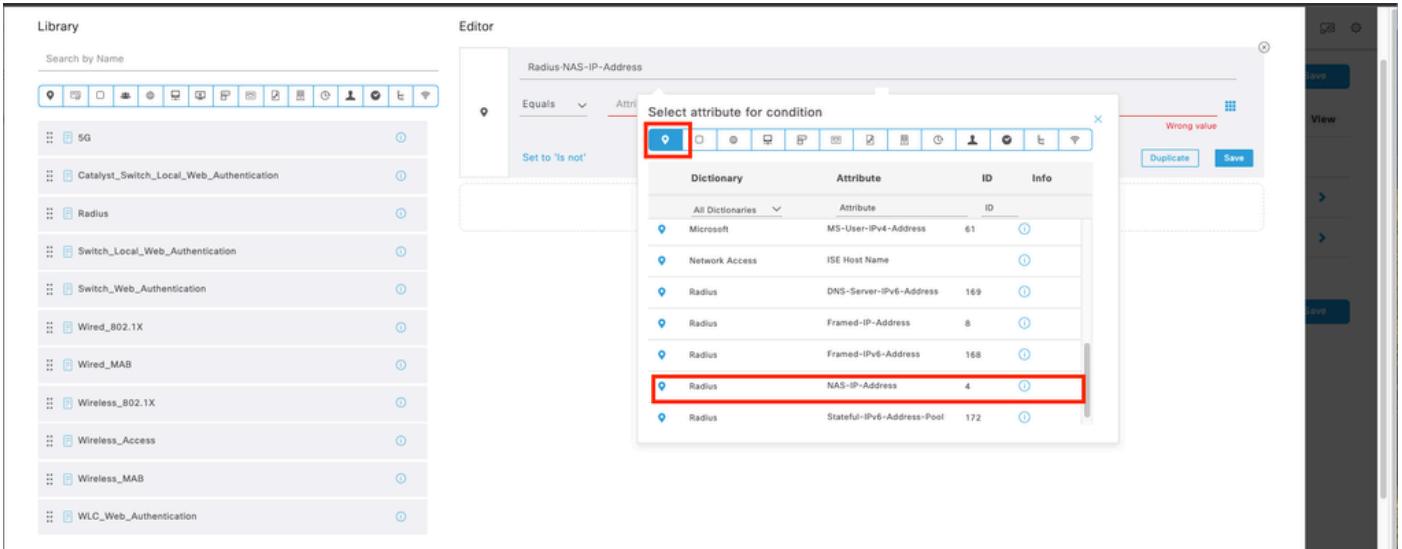
좌측 상단 모서리에 ≡ > Policy > Policy Sets > Add 아이콘 기호로 이동합니다.



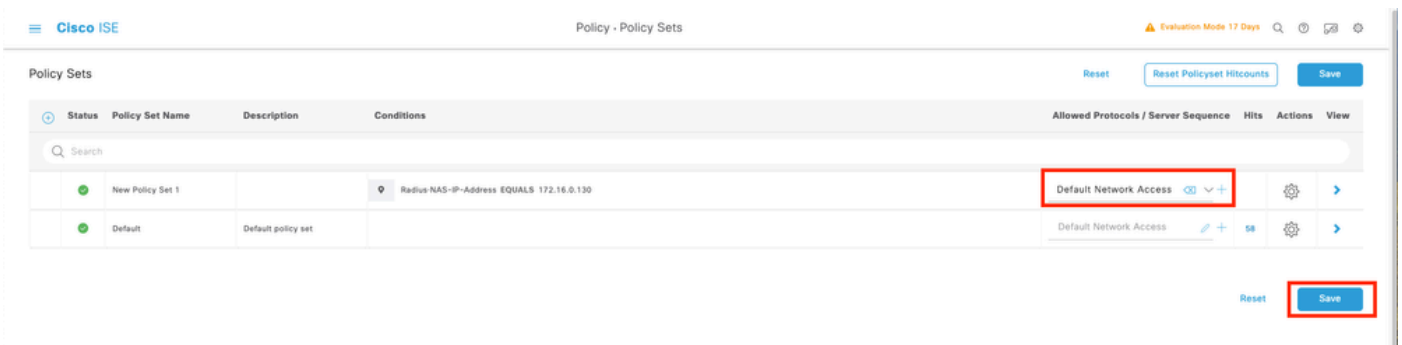
9.1 정책 세트의 맨 위에 새 라인이 배치됩니다. 새 조건을 구성하려면 Add(추가) 아이콘을 클릭합니다.

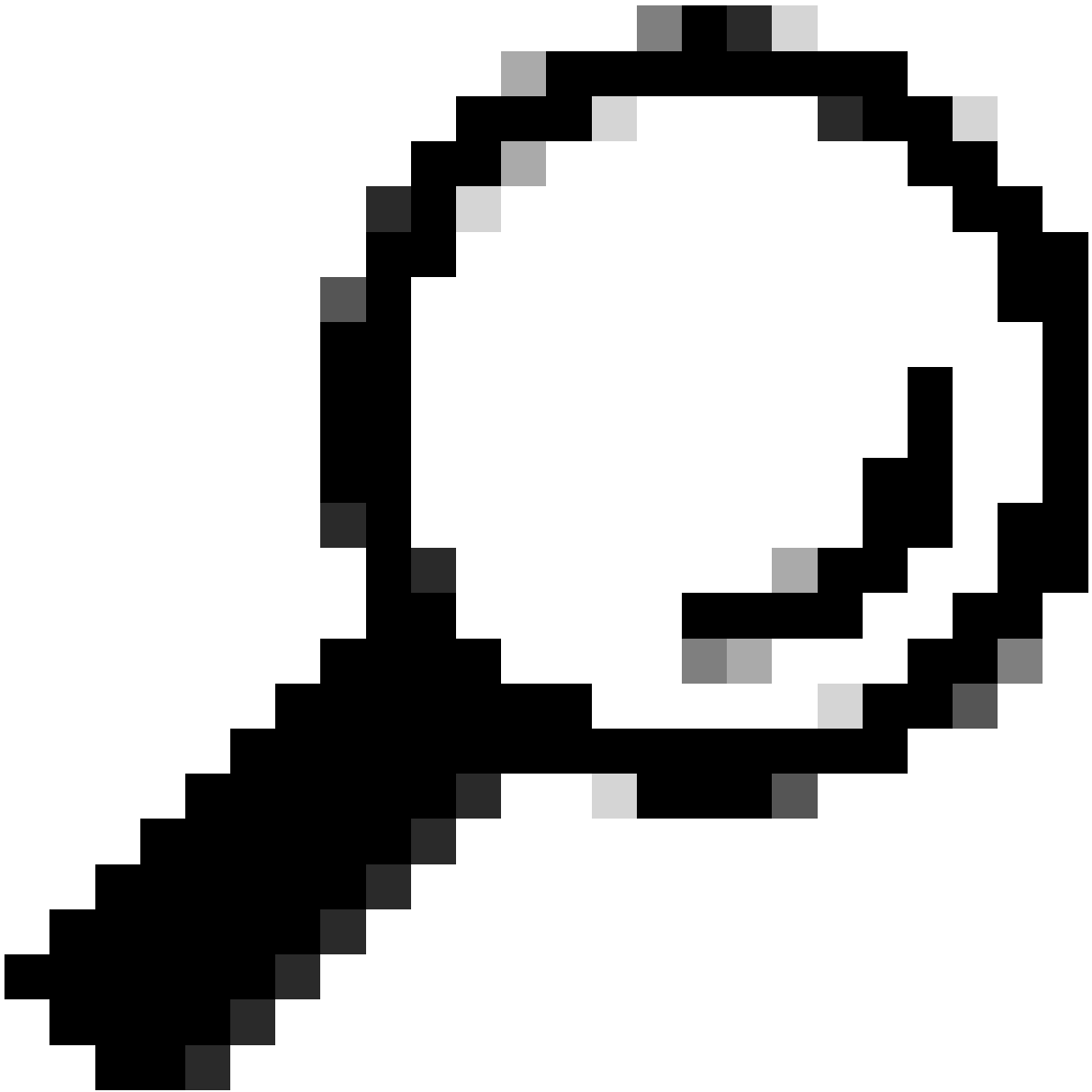


9.2 FCM IP 주소와 일치하는 RADIUS NAS-IP-Addressattribute에 대한 상위 조건을 추가한 다음 Use(사용)를 클릭합니다.



9.3 완료되면 저장을 클릭합니다.



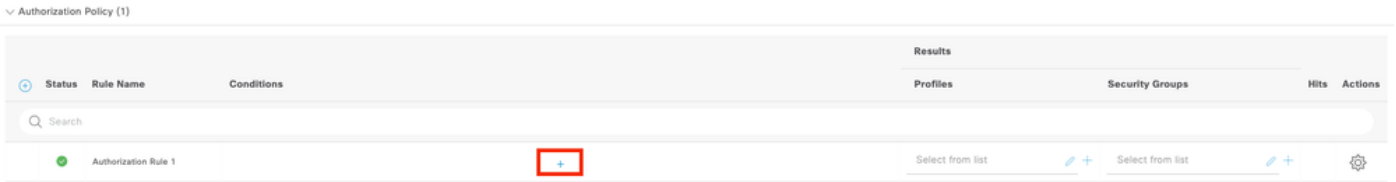


팁: 이 연습에서는 Default Network Access Protocols(기본 네트워크 액세스 프로토콜) 목록을 허용했습니다. 새 목록을 만들고 필요에 따라 목록을 좁힐 수 있습니다.

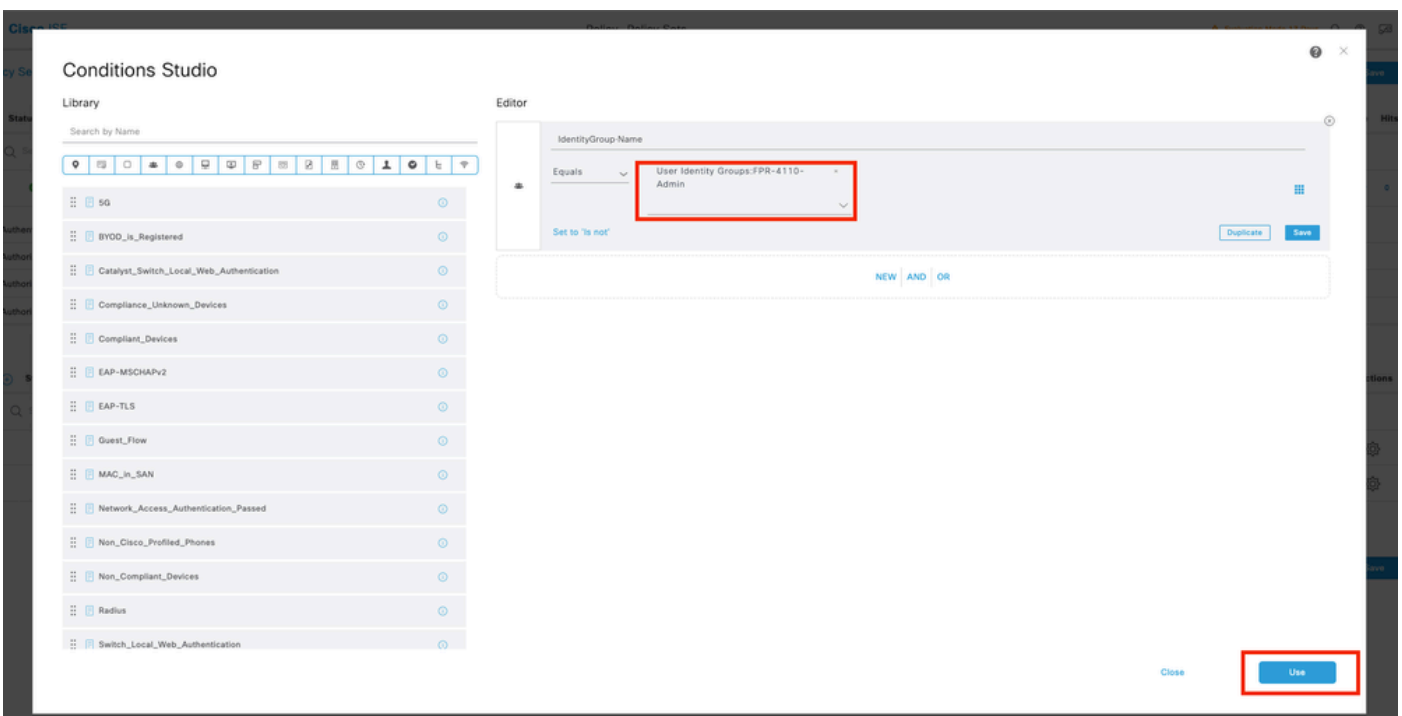
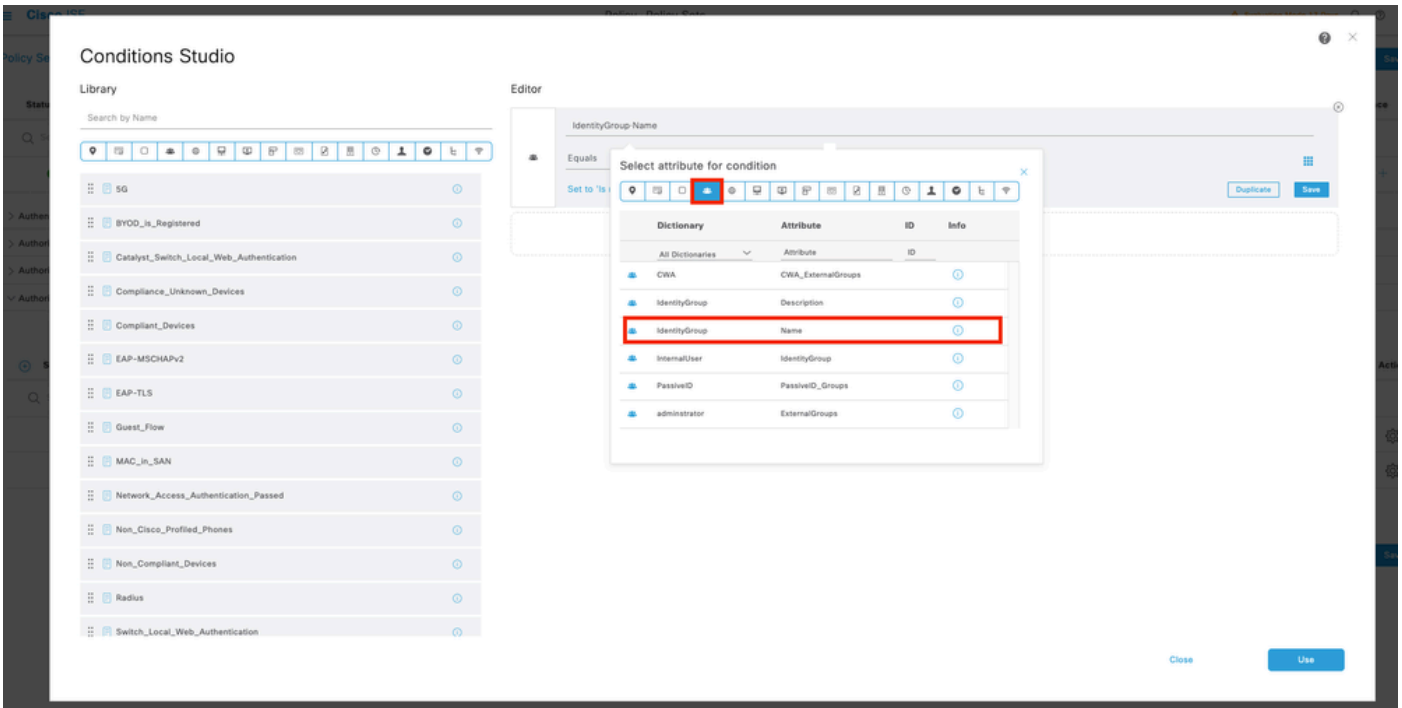
10단계. 행의 끝에 있는 > 아이콘을 눌러 새 정책 집합을 확인합니다.



10.1 Authorization Policy(권한 부여 정책) 메뉴를 확장하고 (+)를 클릭하여 새 조건을 추가합니다.

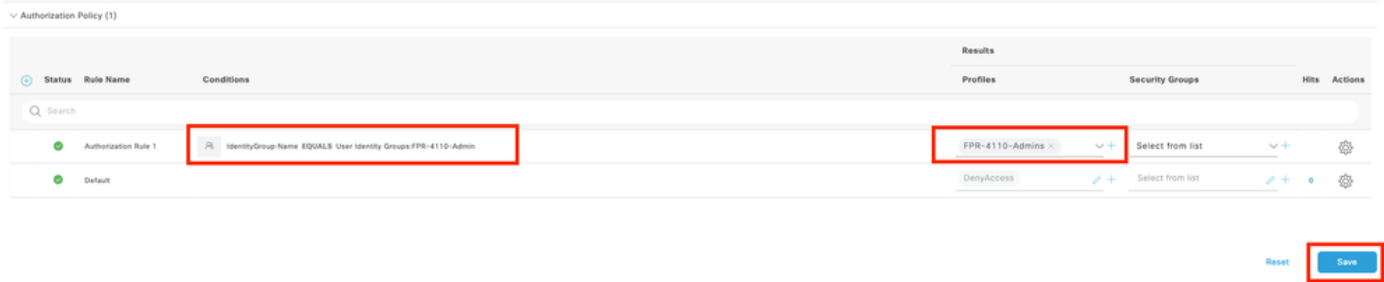


10.2 AttributeName Equals User Identity Groups(AttributeName Equals User Identity Groups: FPR-4110-Admins)(7단계에서 만든 그룹 이름)와 일치하는 조건을 설정하고 Use를 클릭합니다.





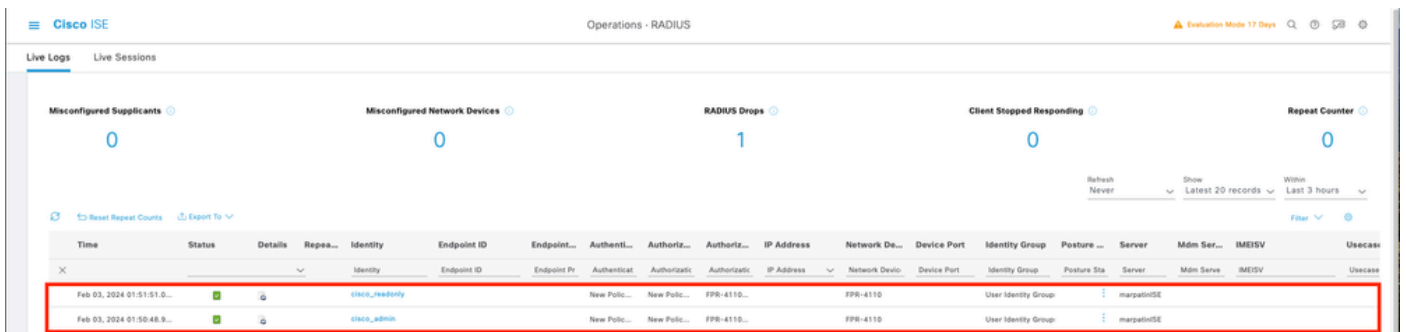
10.3단계 Authorization(권한 부여) 정책에 새 조건이 구성되었는지 확인한 다음 Profiles(프로필) 아래에 사용자 프로필을 추가합니다.



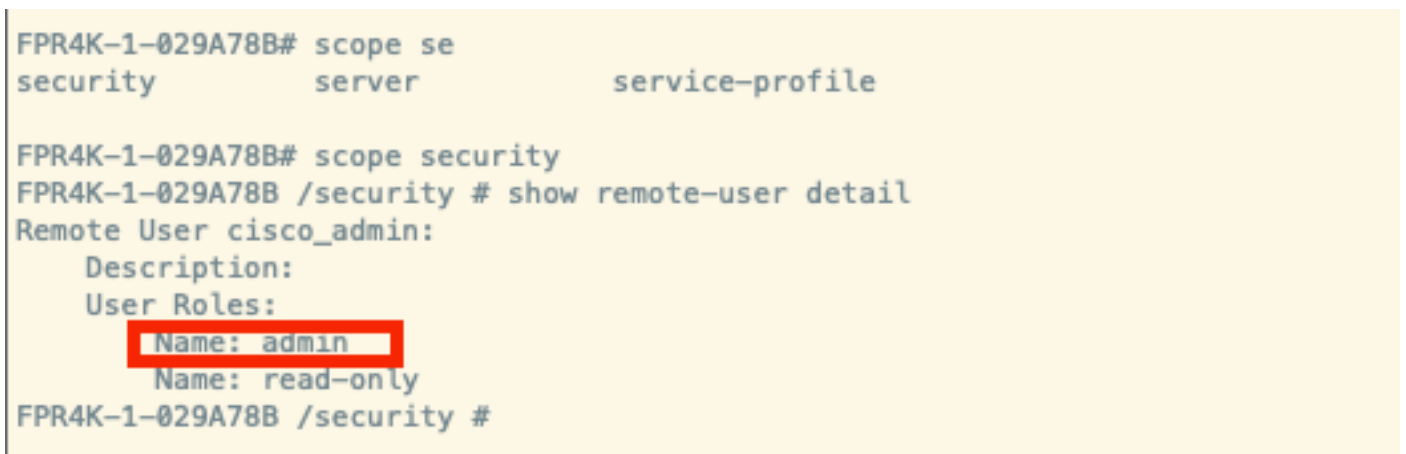
11단계. 읽기 전용 사용자에게 대해 9단계에서 동일한 프로세스를 반복하고 Save(저장)를 클릭합니다.

다음을 확인합니다.

1. 새 Radius 자격 증명을 사용하여 FCM GUI에 로그인합니다.
2. 버거 아이콘 ≡ > Operations(운영) > Radius > Live logs(라이브 로그)로 이동합니다.
3. 표시되는 정보는 사용자가 성공적으로 로그인했는지 보여줍니다.



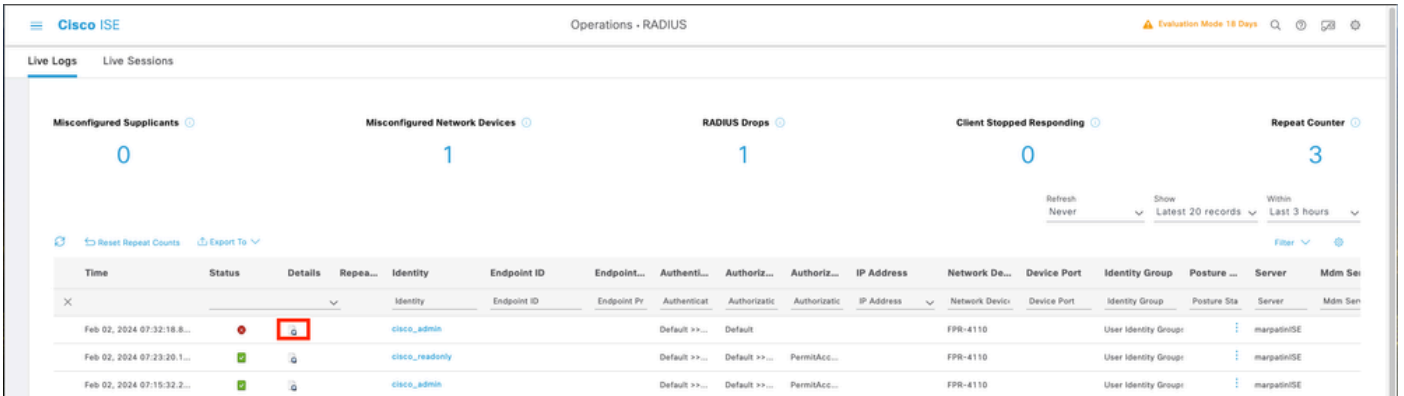
4. Secure Firewall 새시 CLI에서 로깅된 사용자 역할을 확인합니다.



# 문제 해결

1. ISE GUI에서 버거 아이콘 ≡ > Operations(운영) > Radius > Live logs(라이브 로그)로 이동합니다

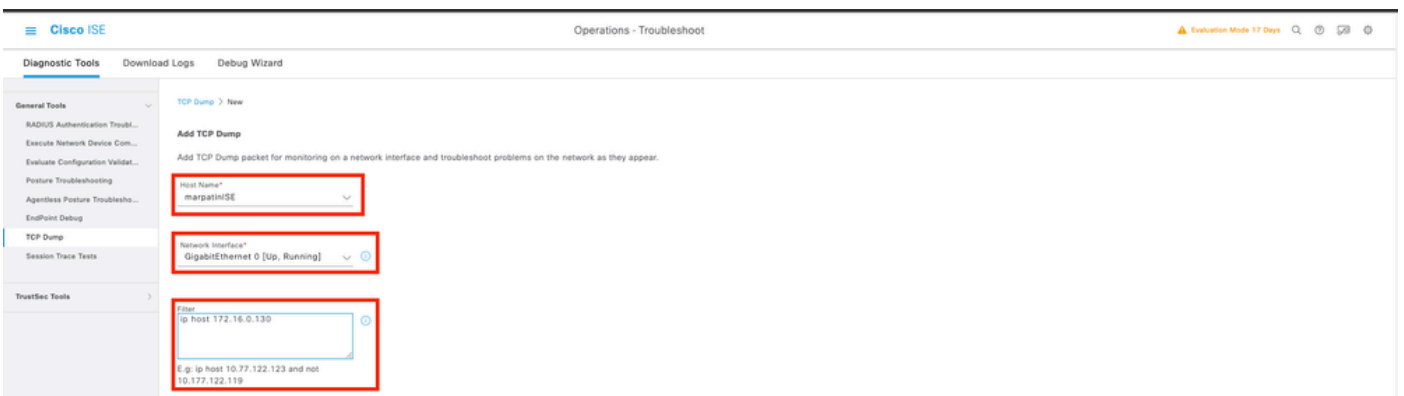
- 1.1 로그 세션 요청이 ISE 노드에 도달하는지 확인합니다.
- 1.2 실패한 상태의 경우 세션의 세부 정보를 검토합니다.



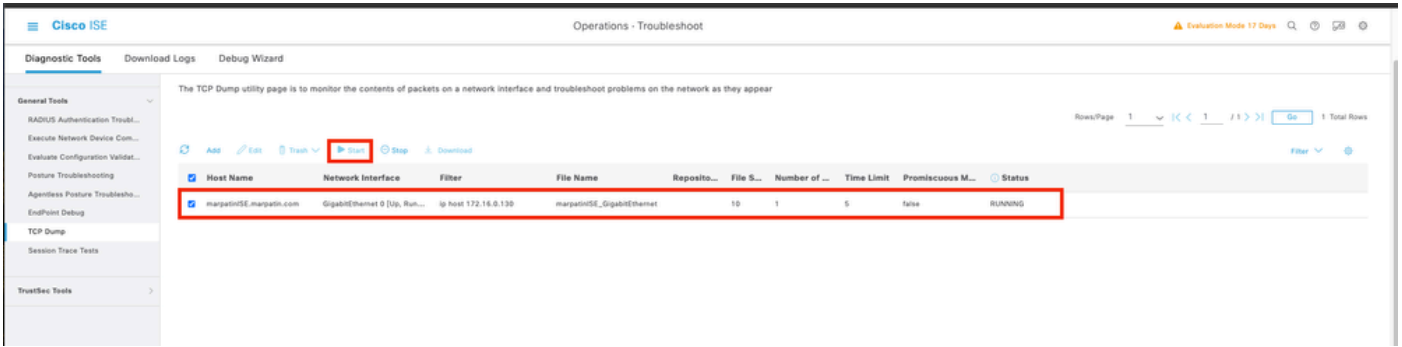
2. Radius Live 로그에 표시되지 않는 요청의 경우 UDP 요청이 패킷 캡처를 통해 ISE 노드에 도달하는지 검토합니다.

버거 아이콘 ≡ > Operations(운영) > Troubleshoot(문제 해결) > Diagnostic Tools(진단 도구) > TCP dump(TCP 덤프)로 이동합니다. UDP 패킷이 ISE 노드에 도착하는지 검토하기 위해 새 캡처를 추가하고 파일을 로컬 시스템에 다운로드합니다.

2.1 요청한 정보를 입력하고 아래로 스크롤한 다음 Save(저장)를 클릭합니다.



2.2 캡처를 선택하고 시작합니다.



2.3 ISE 캡처가 실행되는 동안 Secure Firewall Chassis에 로그인을 시도합니다

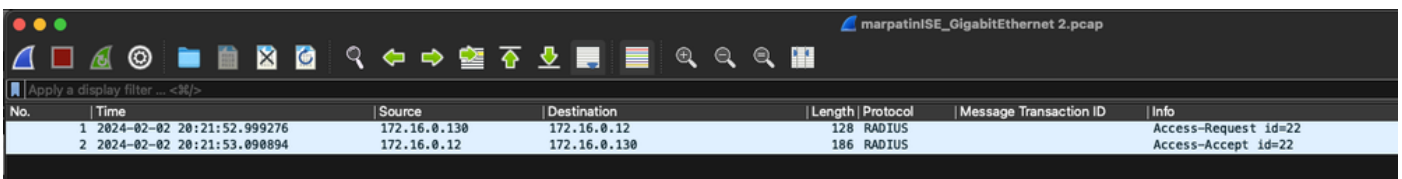
2.4 ISE에서 TCP 덤프를 중지하고 파일을 로컬 시스템에 다운로드합니다.

2.5 트래픽 출력을 검토합니다.

예상 출력:

패킷 No1. 포트 1812(RADIUS)를 통해 보안 방화벽에서 ISE 서버로 요청

패킷 No2. 초기 요청을 수락하는 ISE 서버 응답입니다.



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.