Arista 스위치에서 RADIUS 기반 관리자 로그인 구성

목차

소개

이 문서에서는 RADIUS를 사용하여 Arista 스위치에서 관리자 로그인을 인증하도록 Cisco ISE(Identity Services Engine)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

계속하기 전에 다음을 확인하십시오.

- Cisco ISE(버전 3.x 권장)가 설치되어 작동 중입니다.
- RADIUS를 지원하는 EOS를 실행하는 Arista 스위치입니다.
- ISE에 구성된 AD(Active Directory) 또는 내부 사용자 데이터베이스

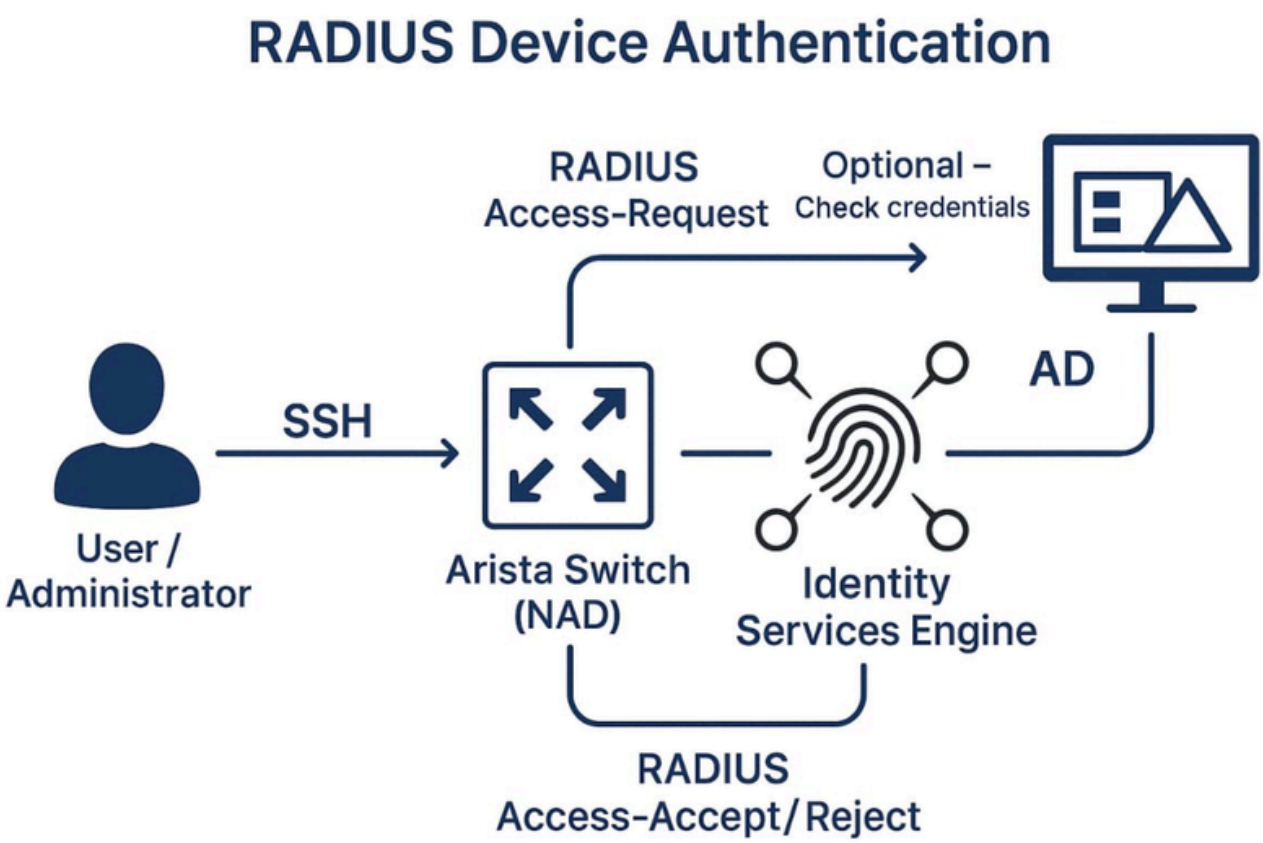
사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Arista 스위치 소프트웨어 이미지 버전: 4.33.2F
- Cisco ISE(Identity Services Engine) 버전 3.3 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.

네트워크 다이어그램



다음은 Active Directory(AD)를 선택 사항 인증 소스로 사용하는 Cisco ISE를 사용하는 Arista 스위치에 대한 RADIUS 기반 디바이스 인증을 설명하는 네트워크 다이어그램입니다.

다이어그램에는 다음이 포함됩니다.

- Arista Switch(네트워크 액세스 디바이스 및 NAD의 역할)
- Cisco ISE(RADIUS 서버로 작동)
- Active Directory (AD) [선택 사항] (ID 확인에 사용)
- 사용자/관리자(SSH를 통해 로그인)

구성

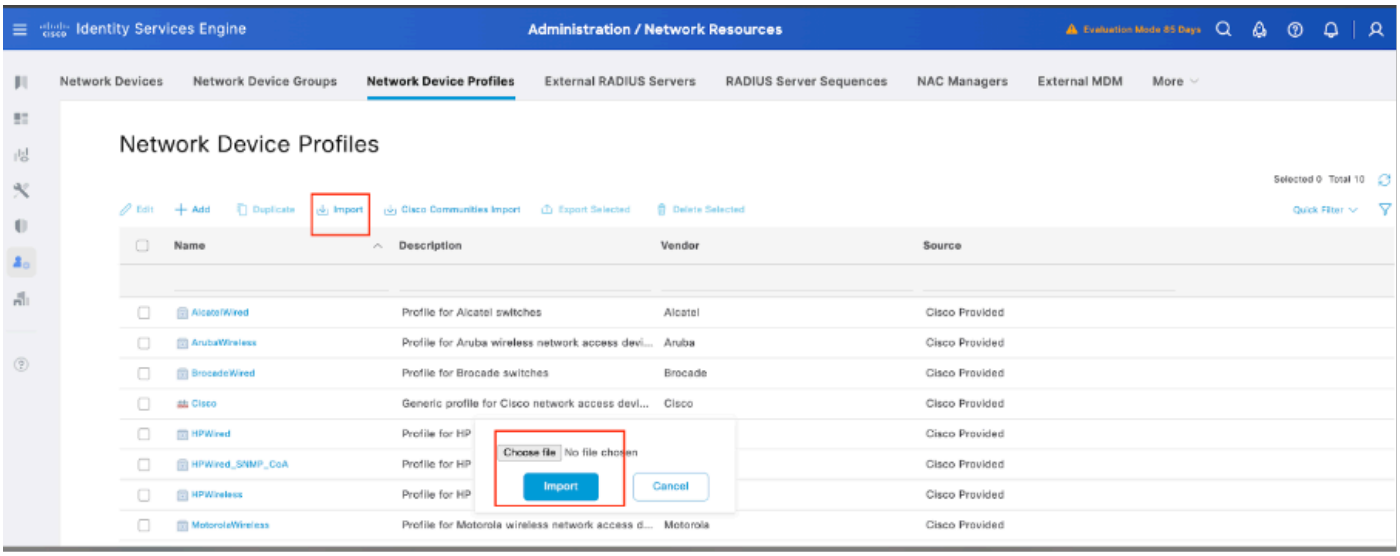
Cisco ISE 구성

1단계. Cisco ISE에 대한 Arista 네트워크 디바이스 프로파일 얻기

Cisco 커뮤니티는 Arista 디바이스에 대한 전용 NAD 프로필을 공유했습니다. 이 프로파일은 필요한 사전 파일과 함께 Arista CloudVision WiFi Dictionary and NAD Profile for ISE Integration(ISE 통합을 위한 Arista CloudVision WiFi 사전 및 NAD 프로파일) 문서에서 찾을 수 있습니다. 이 프로파일을 다운로드하고 ISE 설정으로 가져오면 더 원활한 통합이 가능합니다.

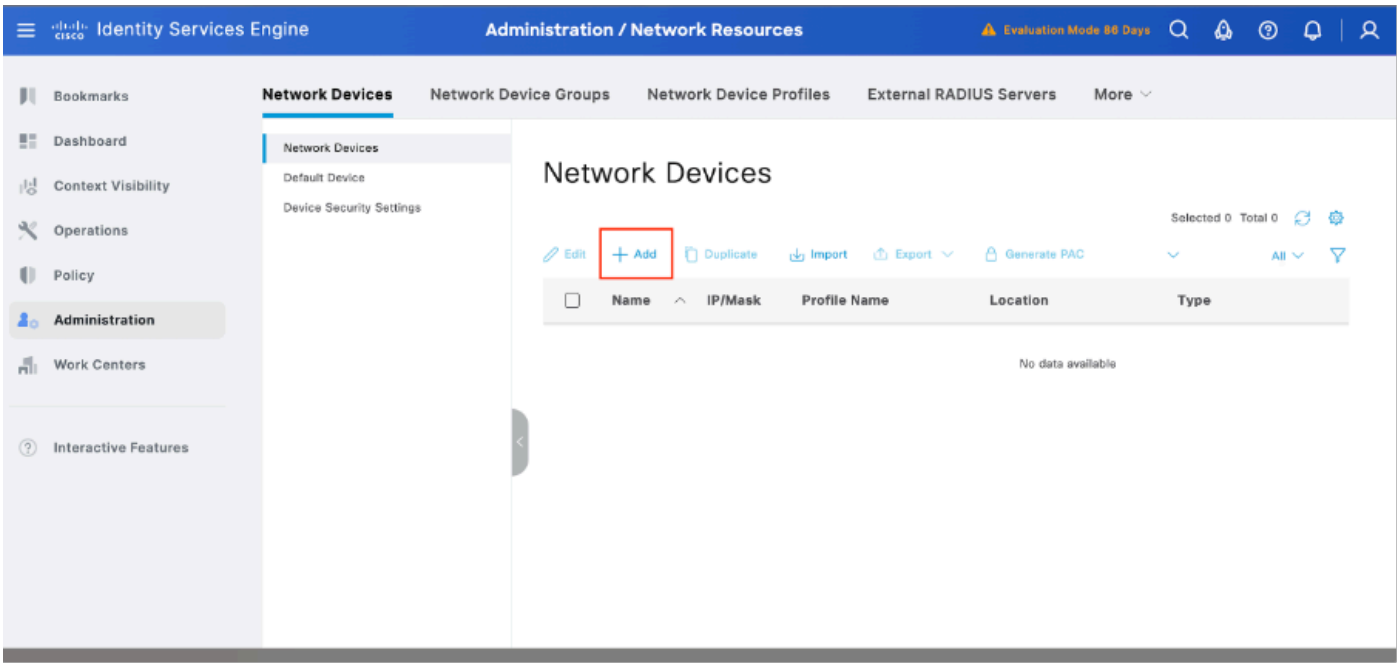
Cisco ISE로 Arista NAD 프로파일을 가져오는 단계는 다음과 같습니다.

1. 프로파일 다운로드:
   - 위에 제공된 Cisco Community 링크에서 Arista NAD 프로파일을 가져옵니다.
2. Cisco ISE에 액세스:
   - Cisco ISE 관리 콘솔에 로그인합니다.
3. NAD 프로파일을 가져옵니다.
   - Administration(관리) > Network Resources(네트워크 리소스) > Network Device Profiles(네트워크 디바이스 프로파일)로 이동합니다.
   - Import(가져오기) 버튼을 클릭합니다.
   - 다운로드한 Arista NAD 프로파일 파일을 업로드합니다.



2단계. Arista 스위치를 네트워크 디바이스로 추가

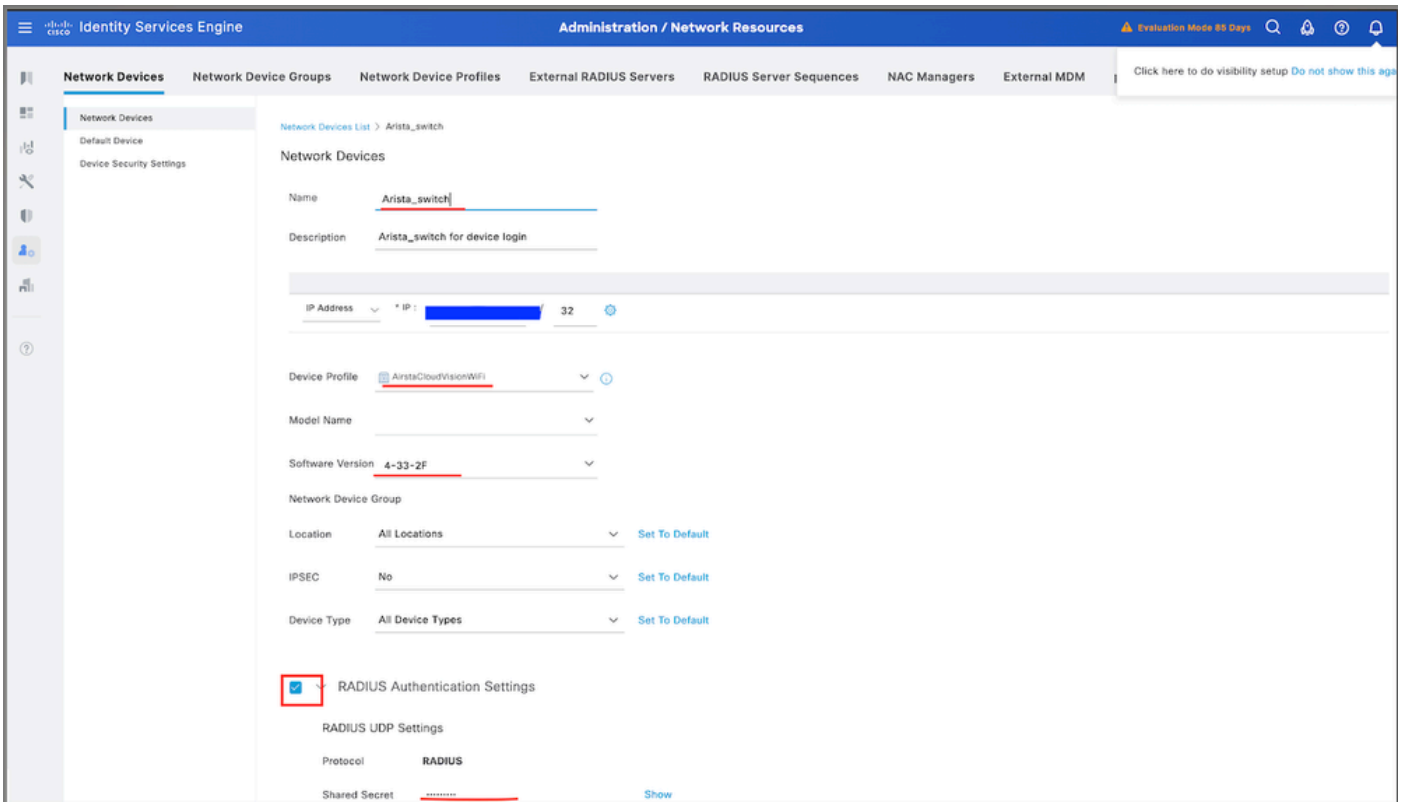
1. Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스) > +Add(추가)로 이동합니다.



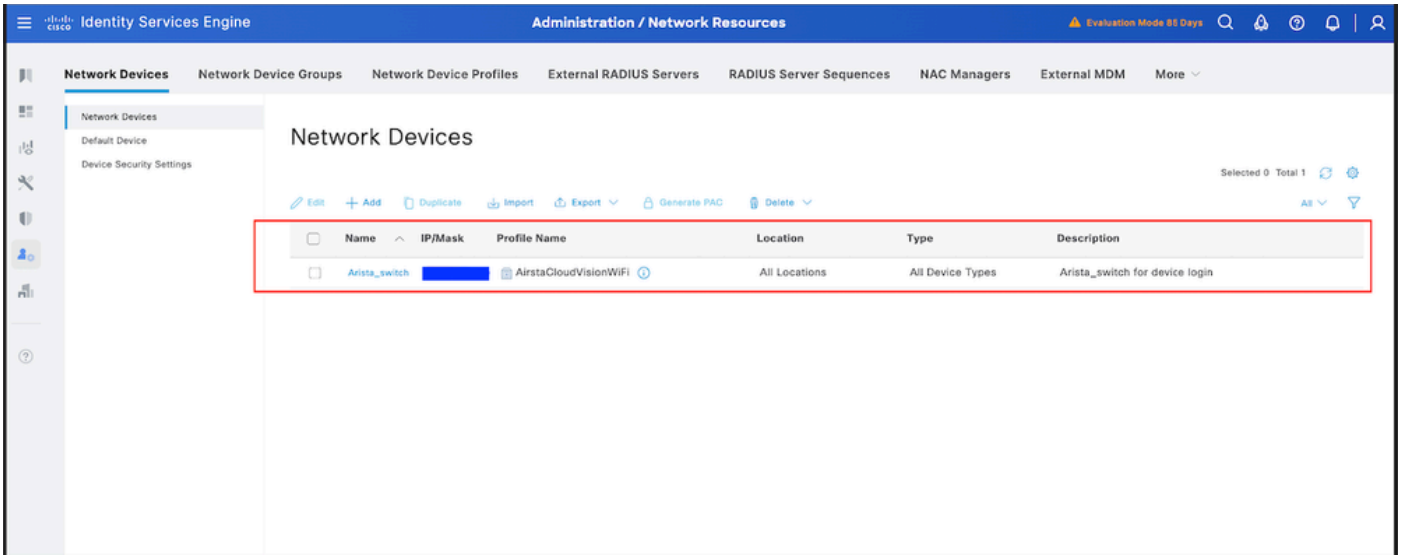
2. 추가를 누르고 다음 상세내역을 입력합니다.

1. 이름: 아리스타-스위치
2. IP 주소: <스위치 IP>
3. 장치 유형: 기타 유선 선택
4. 네트워크 장치 프로파일: airstaCloudVisionWiFi를 선택합니다.
5. RADIUS 인증 설정:
    1. RADIUS 인증 활성화
    2. 공유 암호를 입력합니다(스위치 컨피그레이션과 일치해야 함).

3. 저장을 클릭합니다.

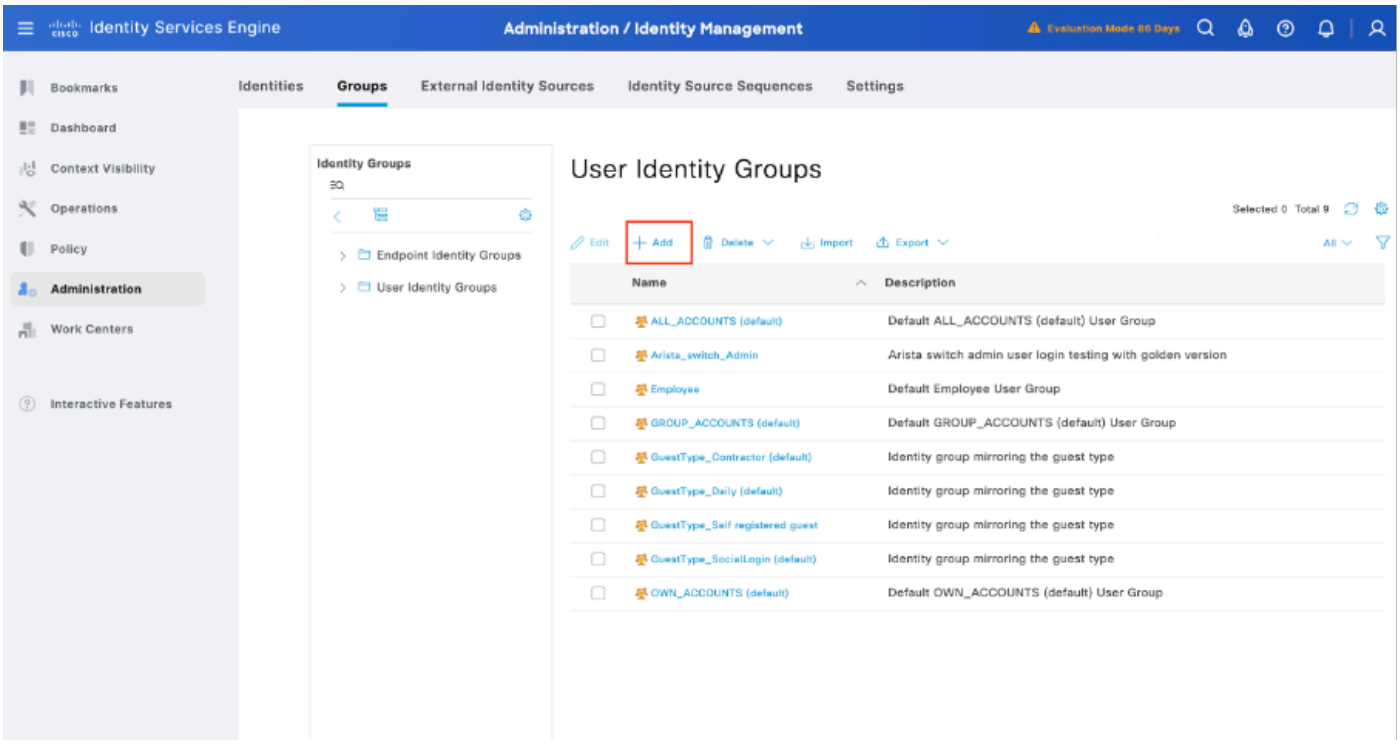


3단계. 새 디바이스가 네트워크 디바이스 아래에 표시되는지 확인



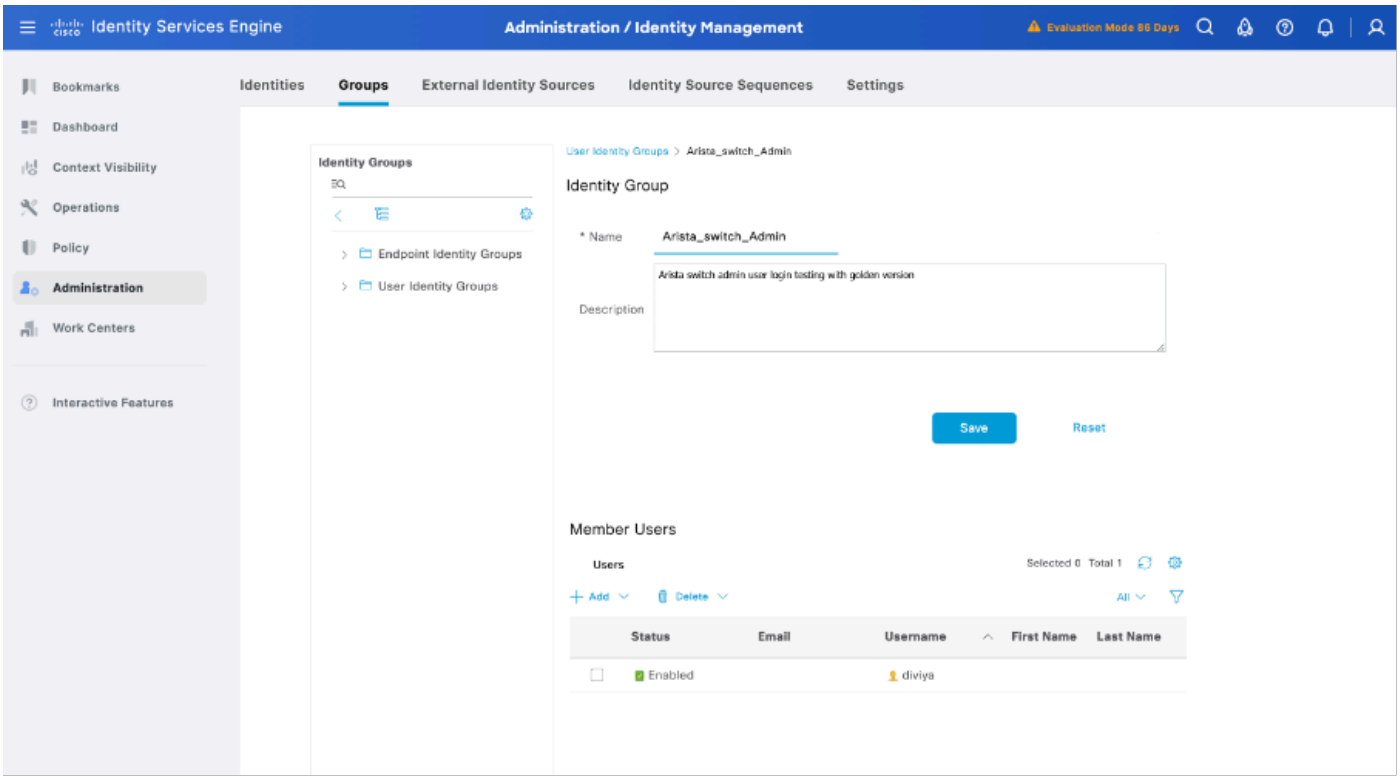
4단계. 필수 사용자 ID 그룹 생성

Administration(관리) > Identity Management(ID 관리) > Groups(그룹) > User Identity Groups(사용자 ID 그룹) > + Add(추가)로 이동합니다.



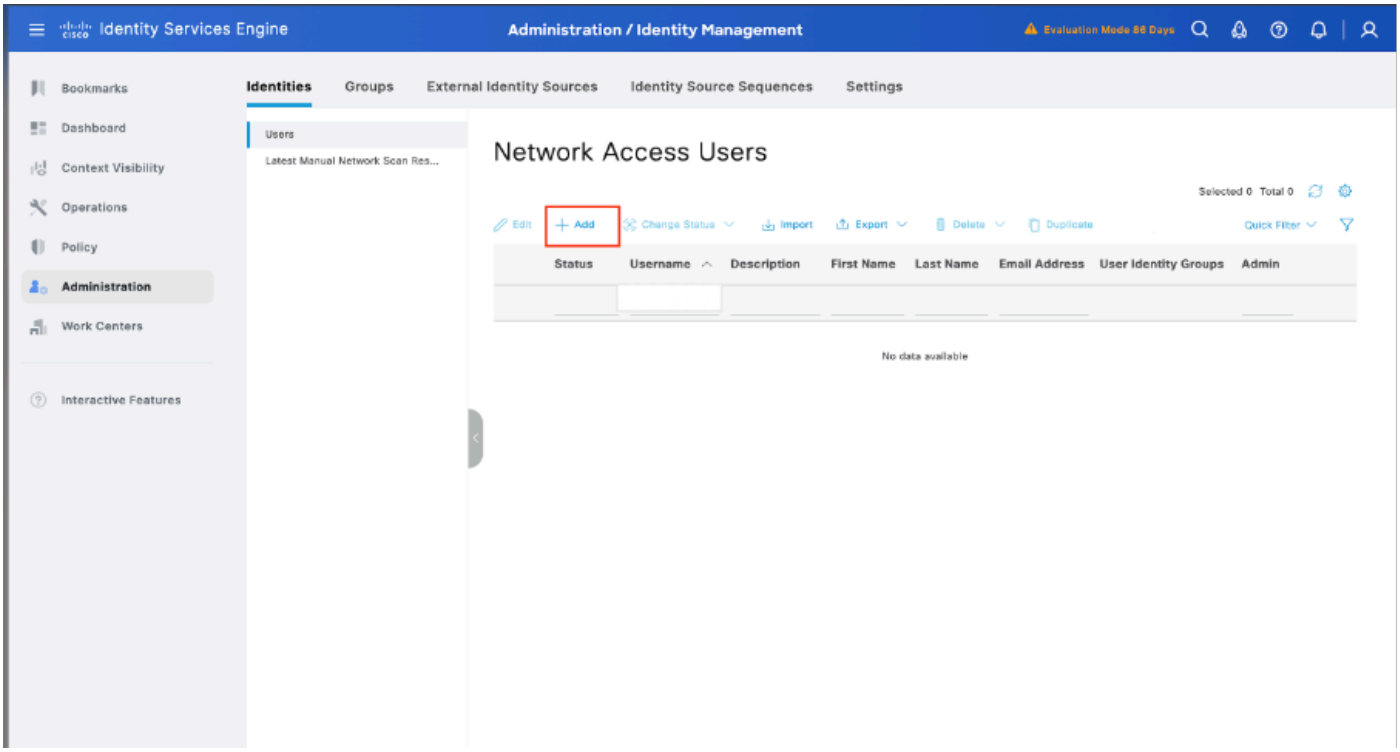
5단계. 관리자 사용자 ID 그룹의 이름 설정

컨피그레이션을 저장하려면 Submit(제출)을 클릭합니다.

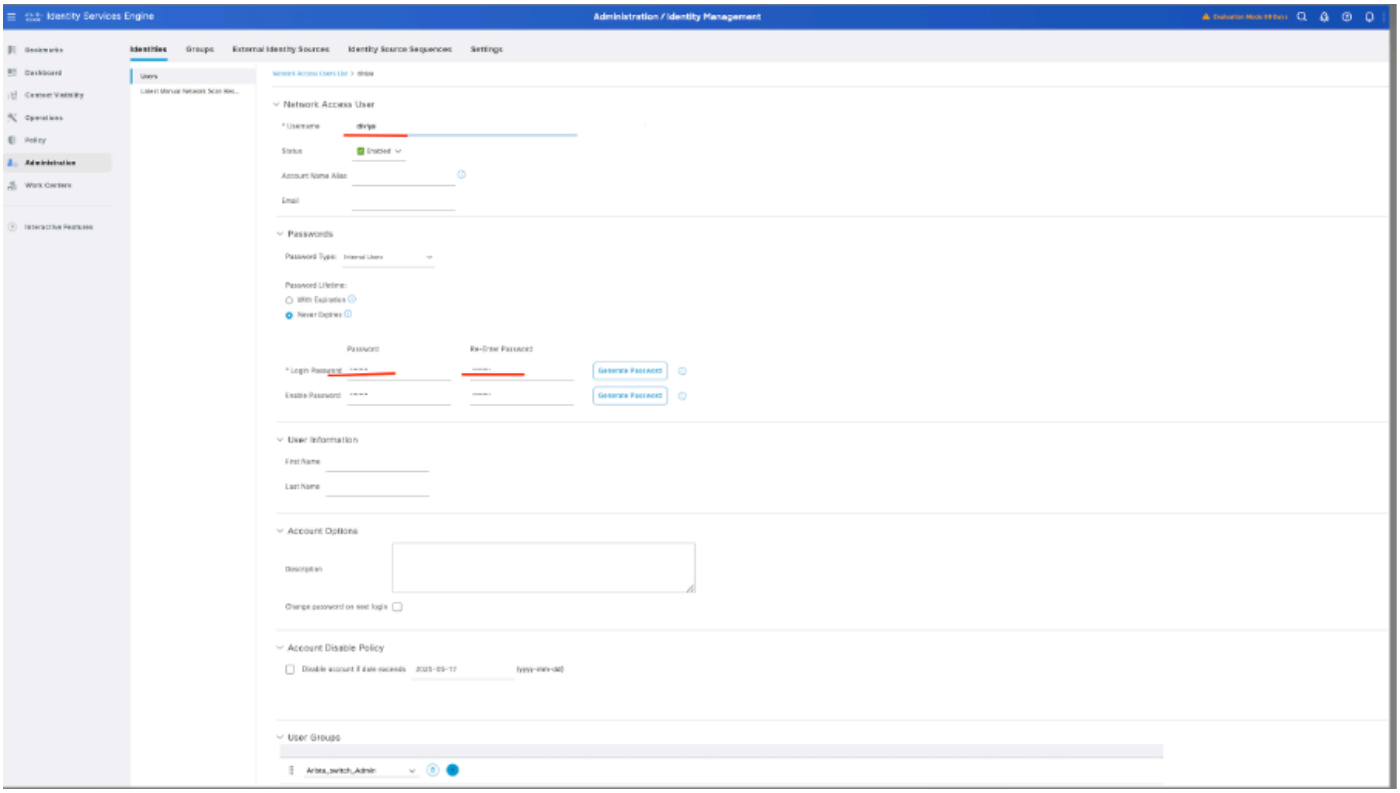


6단계. 로컬 사용자 생성 및 해당 Responder Group에 추가

Administration(관리) > Identity Management(ID 관리) > Identities(ID) > + Add(추가)로 이동합니다.



6.1. 관리자 권한이 있는 사용자를 추가합니다. 이름, 비밀번호를 설정하고 Arista_switch_Admin에 할당한 후 아래로 스크롤하고 Submit(제출)을 클릭하여 변경 사항을 저장합니다.

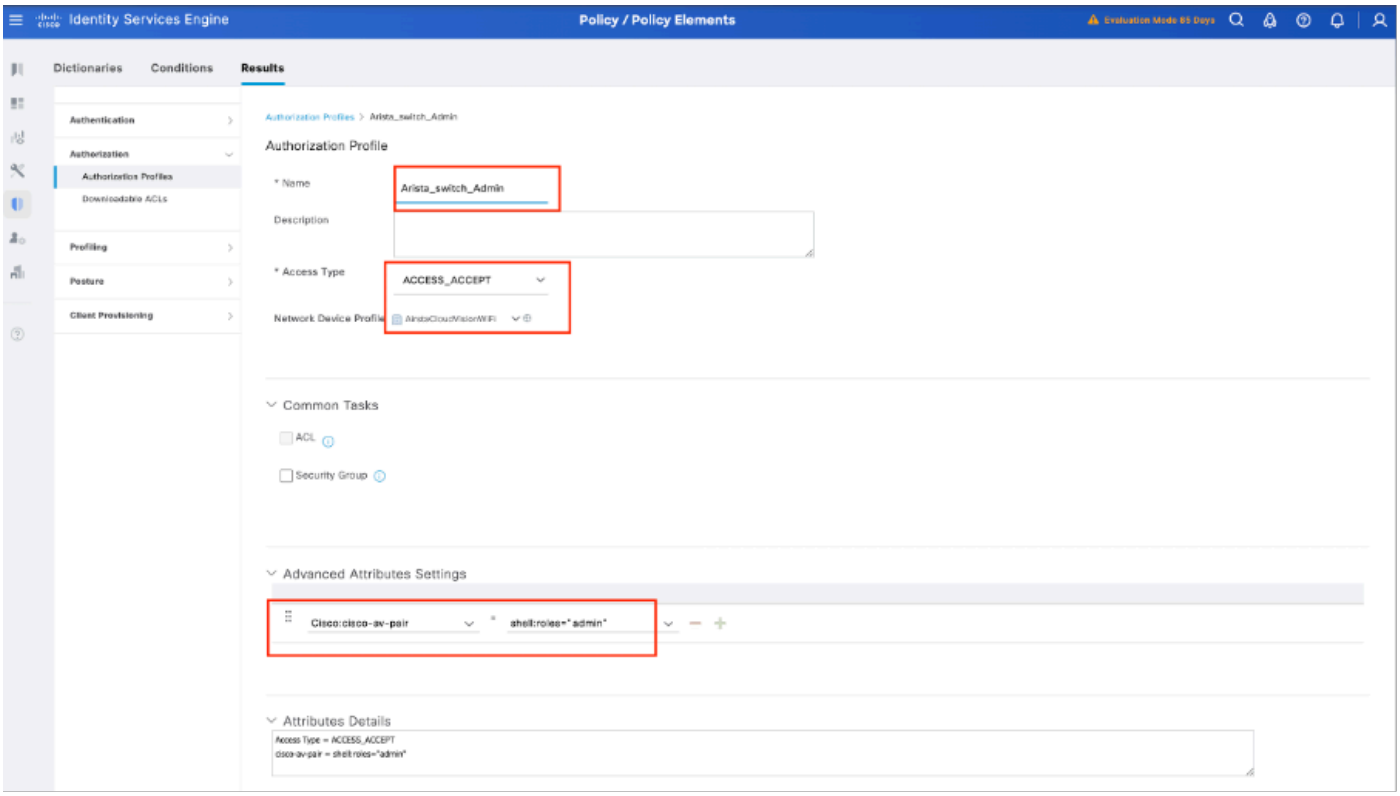


7단계. 관리자 사용자에 대한 권한 부여 프로파일 생성

Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Authorization(권한 부여) > Authorization Profiles(권한 부여 프로파일) > +Add(추가)로 이동합니다.

권한 부여 프로파일의 이름을 정의하고, Access Type(액세스 유형)을 ACCESS_ACCEPT로 남겨두

고 Advanced Attributes Settings(고급 특성 설정)에서 cisco-av-pair=shell:roles="admin"을 추가하고 Submit(제출)을 클릭합니다.



8단계. Arista 스위치 IP 주소와 일치하는 정책 집합 생성

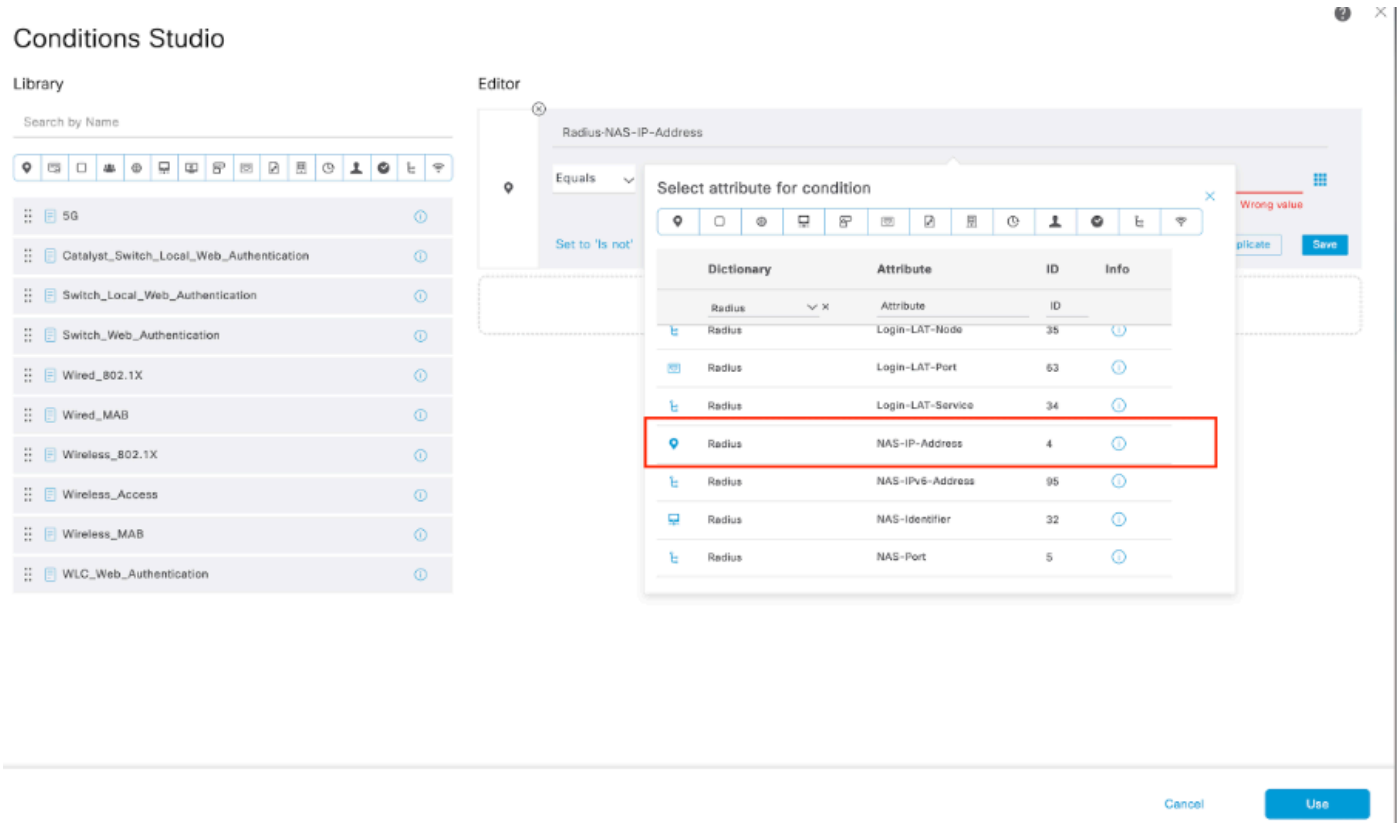
이는 다른 디바이스에서 사용자에게 액세스 권한을 부여하는 것을 방지하기 위한 것입니다.

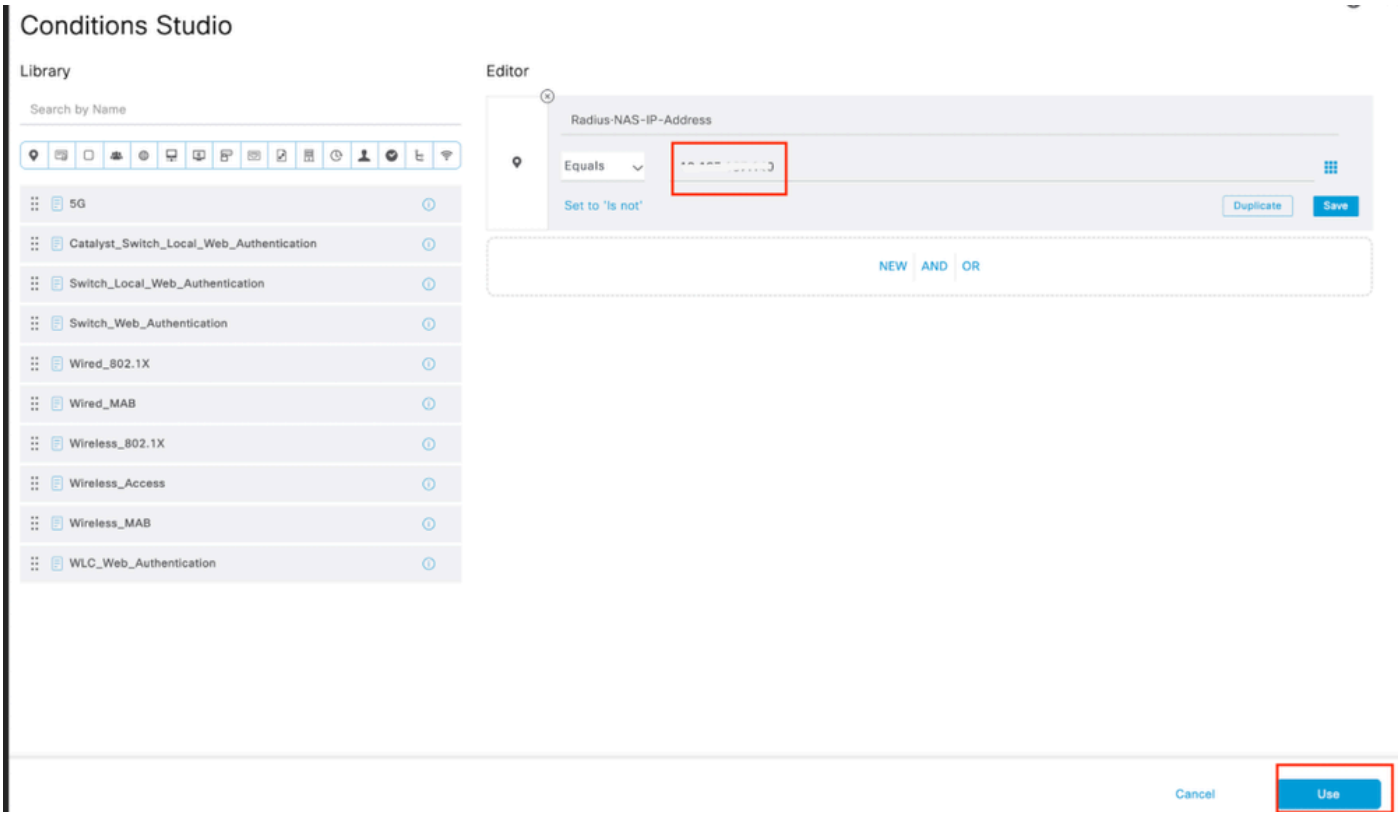
왼쪽 상단에서 Policy(정책) > Policy Sets(정책 집합) >Add(추가) 아이콘 기호로 이동합니다.

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

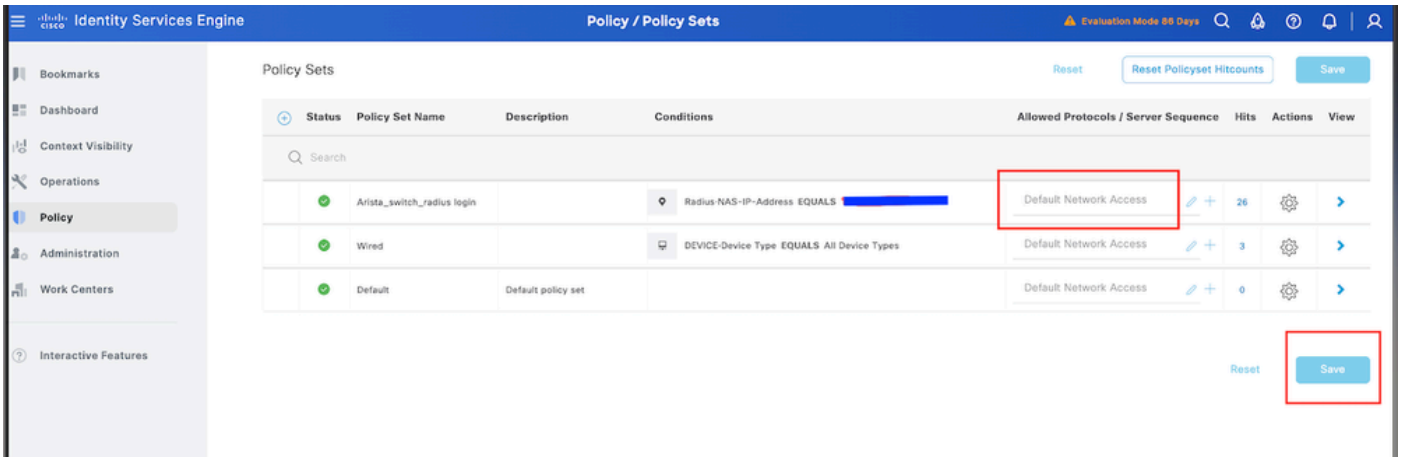
8.2 Arista 스위치 IP 주소와 일치하는 RADIUS NAS-IP-Address 특성에 대한 상위 조건을 추가한

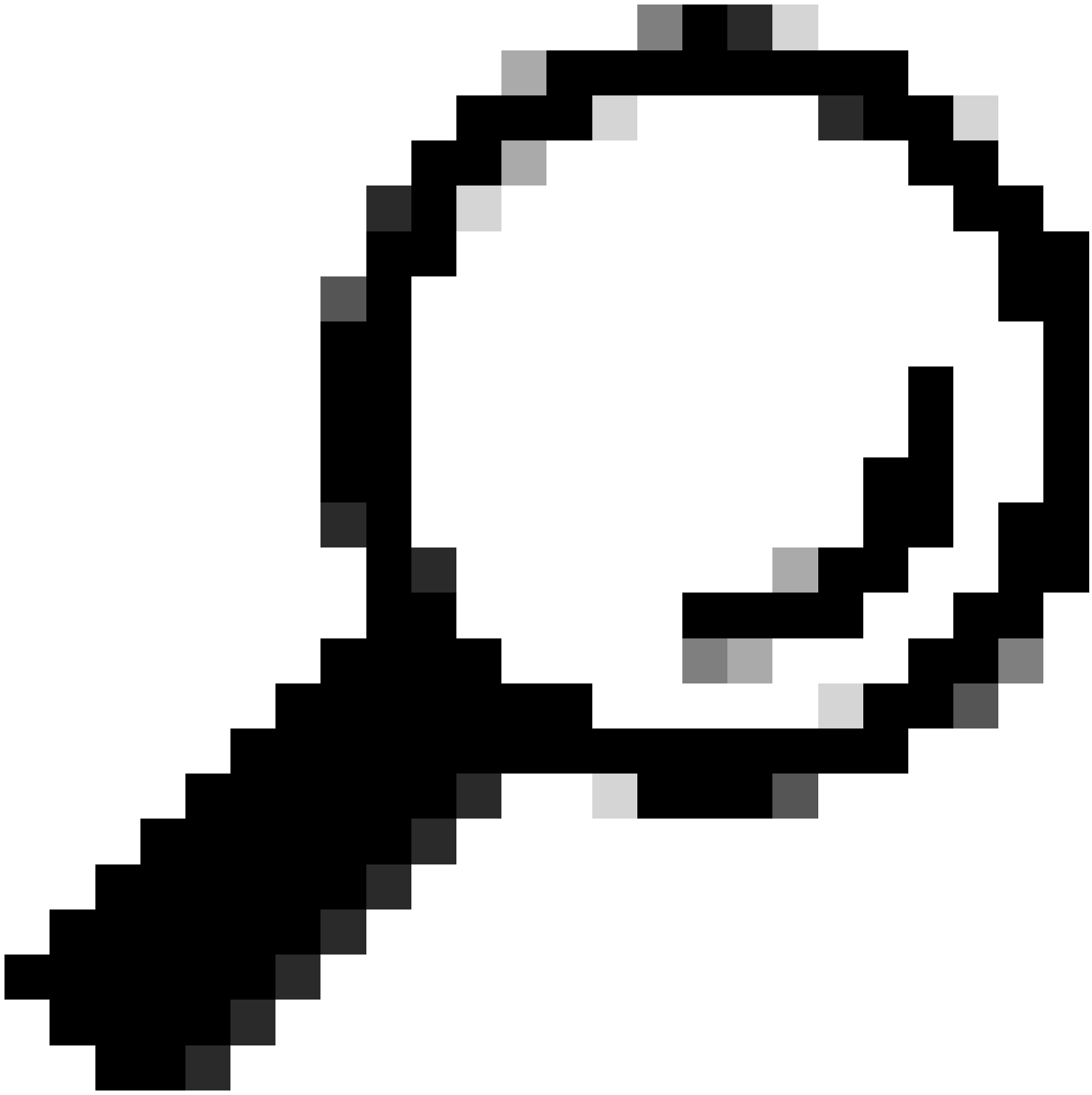
다음 Use(사용)를 클릭합니다.





8.3 완료되면 Save(저장)를 클릭합니다.

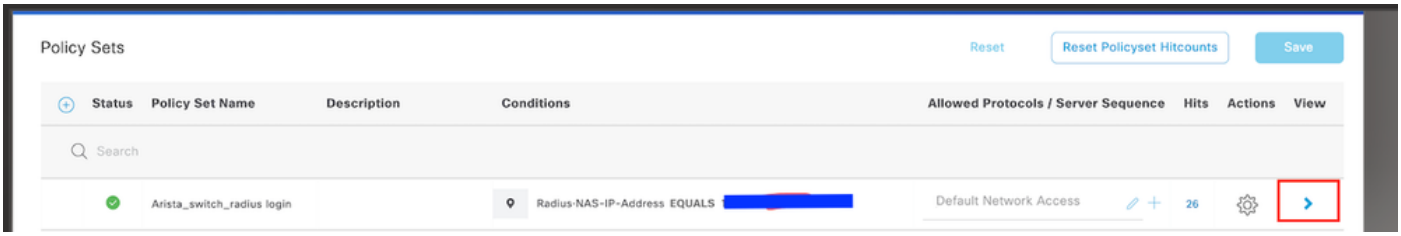




팁: 이 실습에서는 Default Network Access Protocols(기본 네트워크 액세스 프로토콜) 목록을 허용했습니다. 새 목록을 만들고 필요에 따라 목록을 좁힐 수 있습니다.

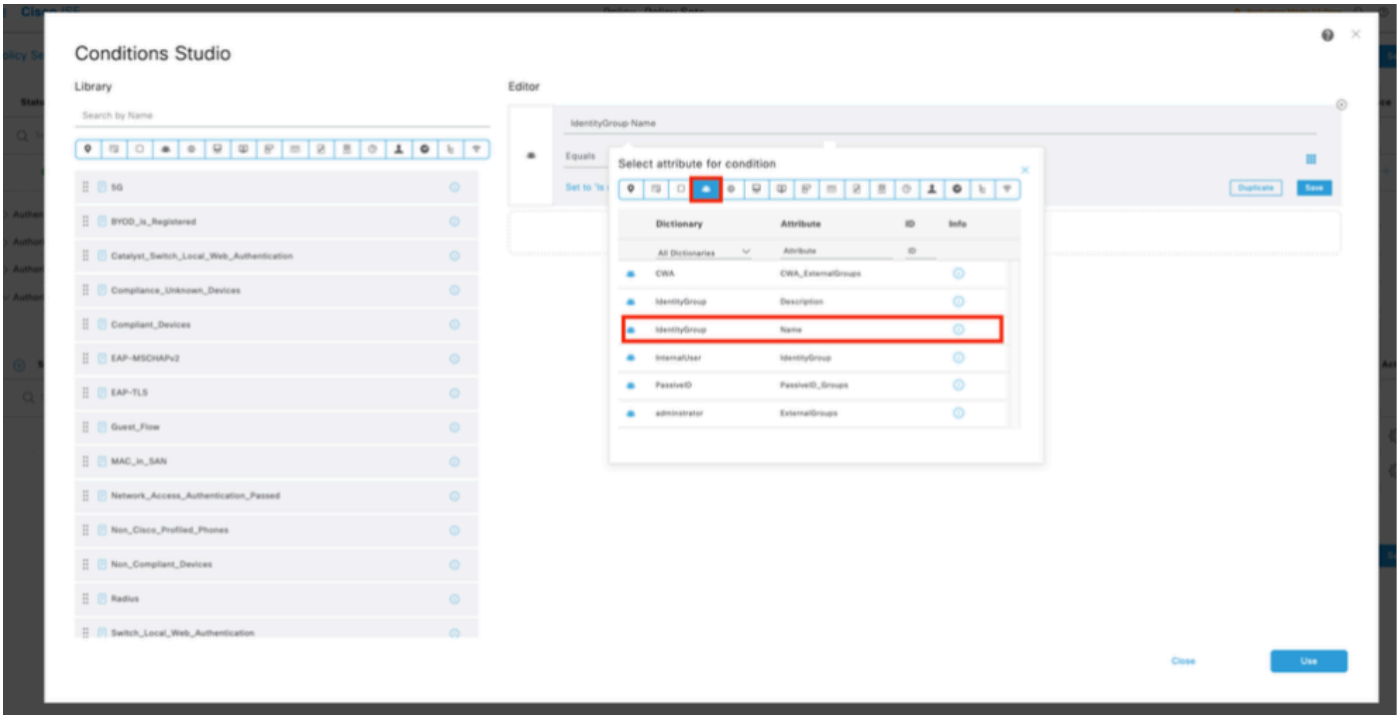
9단계. 새 정책 집합 보기

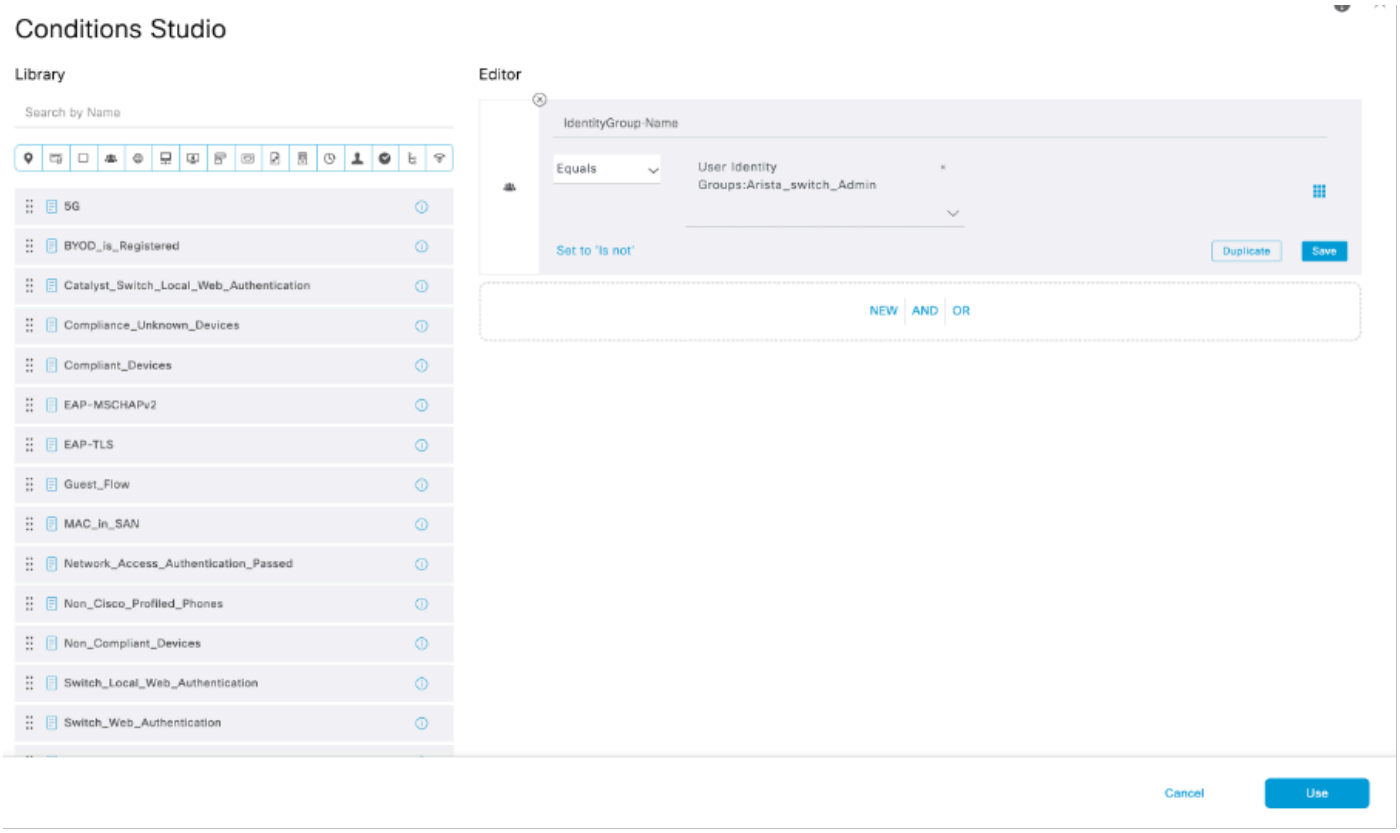
행의 끝에 있는 > 아이콘을 클릭합니다.



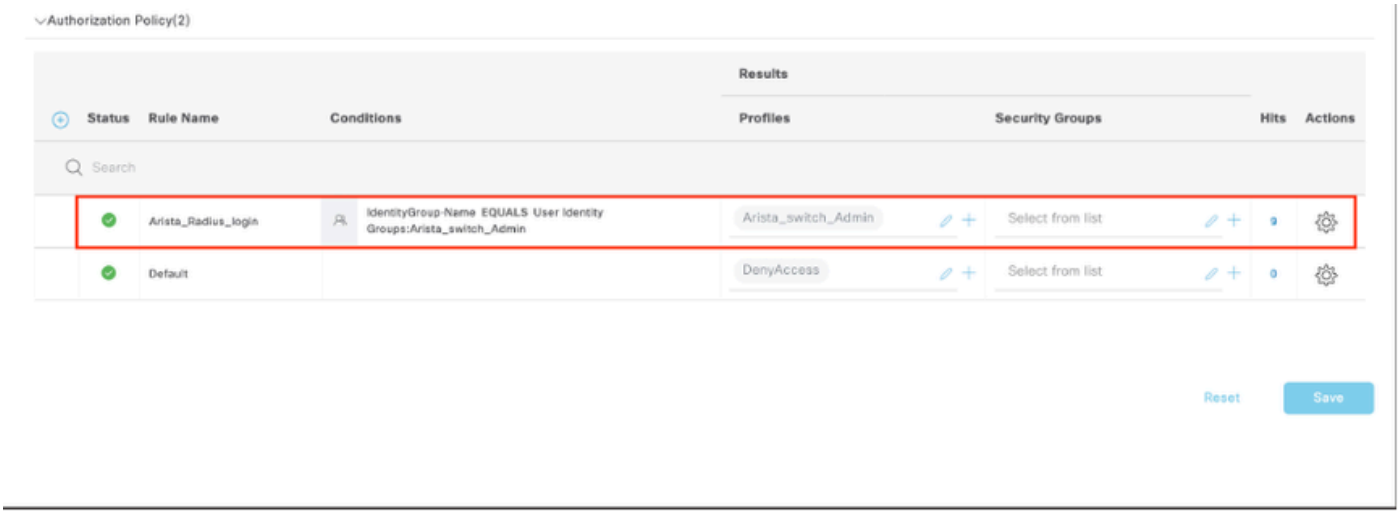
9.1 Authorization Policy(권한 부여 정책) 메뉴를 확장하고 (+)를 클릭하여 새 조건을 추가합니다.

9.2 Attribute Name Equals User Identity Groups(사용자 ID 그룹과 특성 이름이 동일한 사전 ID 그룹)과 일치하는 조건을 설정합니다. Arista_switch_Admin(7단계에서 생성된 그룹 이름)을 입력하고 Use(사용)를 클릭합니다.





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



Arista 스위치 구성

1단계. RADIUS 인증 활성화

Arista 스위치에 로그인하고 컨피그레이션 모드로 들어갑니다.

구성

!

radius-server host <ISE-IP> key <RADIUS-SECRET>

radius-server 시간 초과 5

radius-server 재전송 3

radius-server deadtime 30

!

aaa 그룹 서버 radius ISE

  서버 <ISE-IP>

!

aaa 인증 로그인 기본 그룹 ISE 로컬

aaa authorization exec 기본 그룹 ISE 로컬

aaa accounting exec 기본 시작-중지 그룹 ISE

aaa accounting 명령 15 default start-stop group ISE

aaa 회계 시스템 기본 시작 중지 그룹 ISE

!

끝

2단계. 구성 저장

재부팅 시 설정을 유지하려면

write memory

또는

running-config startup-config 복사

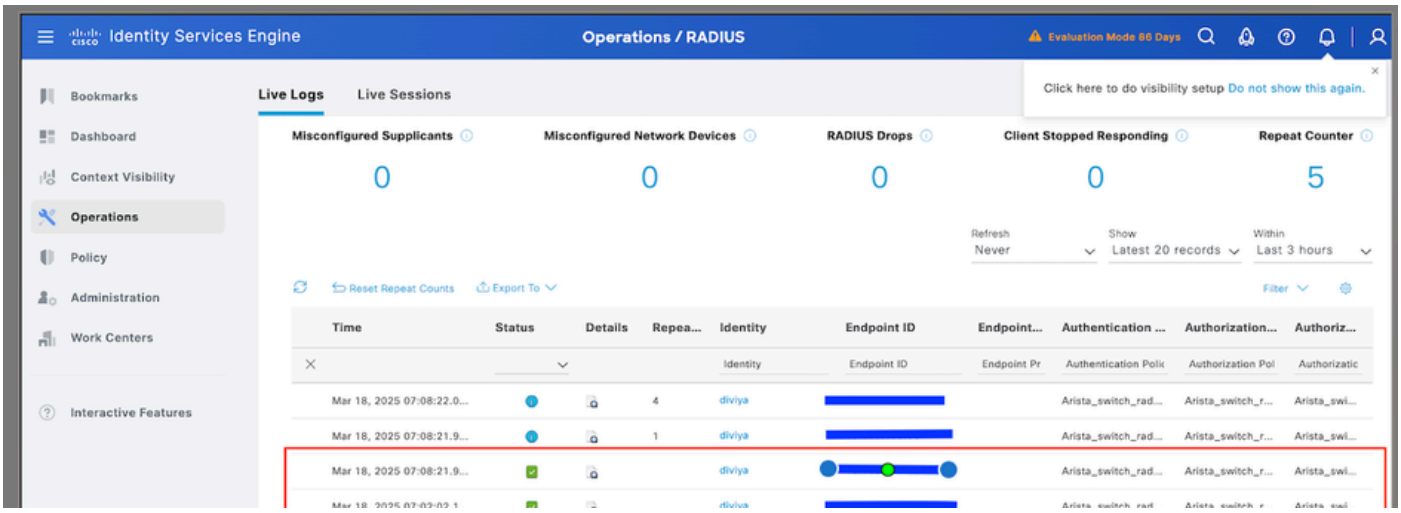
다음을 확인합니다.

ISE 검토

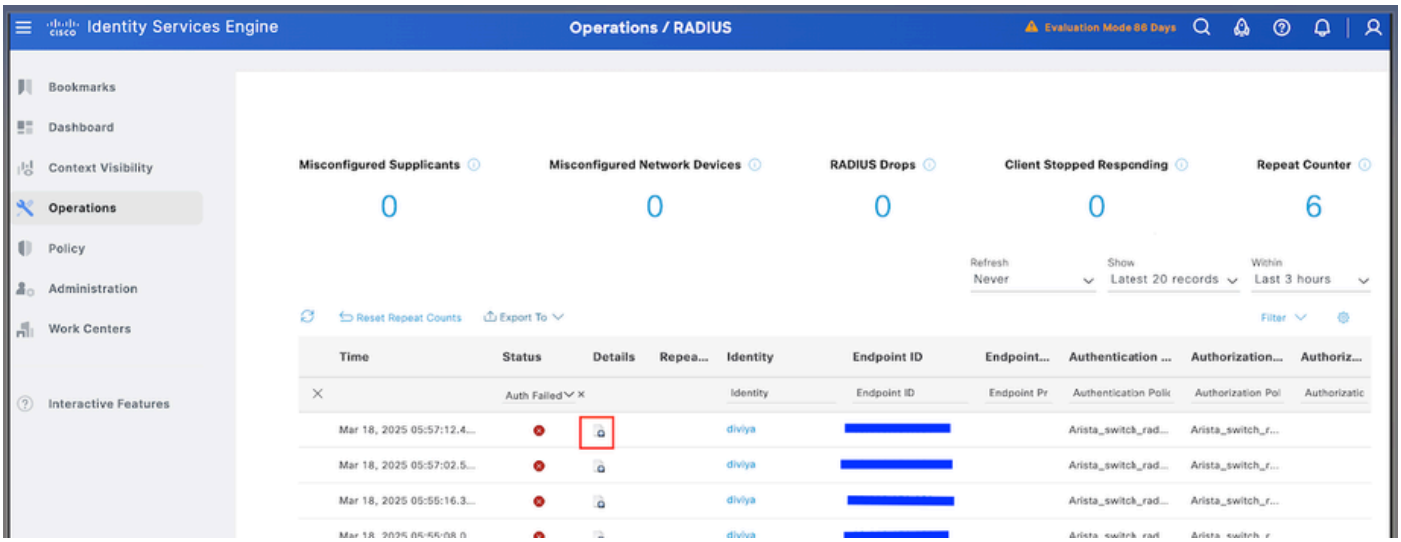
1. 새 Radius 자격 증명을 사용하여 Arista 스위치에 로그인합니다.

    1.1 Operations(운영) > Radius > Live logs(라이브 로그)로 이동합니다.

    1.2 표시되는 정보는 사용자가 성공적으로 로그인했는지 여부를 보여줍니다.



2. 실패 상태의 경우 세션 상세내역을 검토합니다.

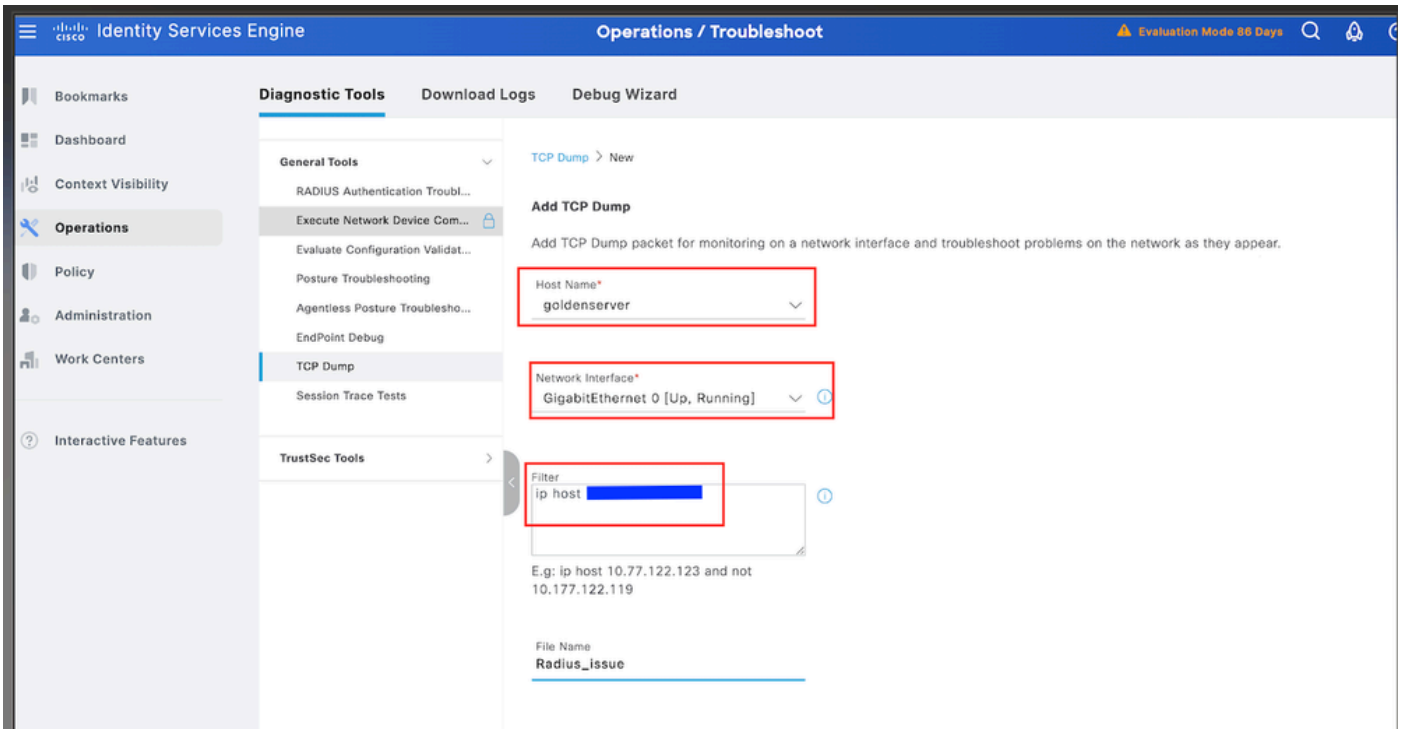


3. Radius Live 로그에 표시되지 않는 요청의 경우 UDP 요청이 패킷 캡처를 통해 ISE 노드에 도달하는지 검토합니다.

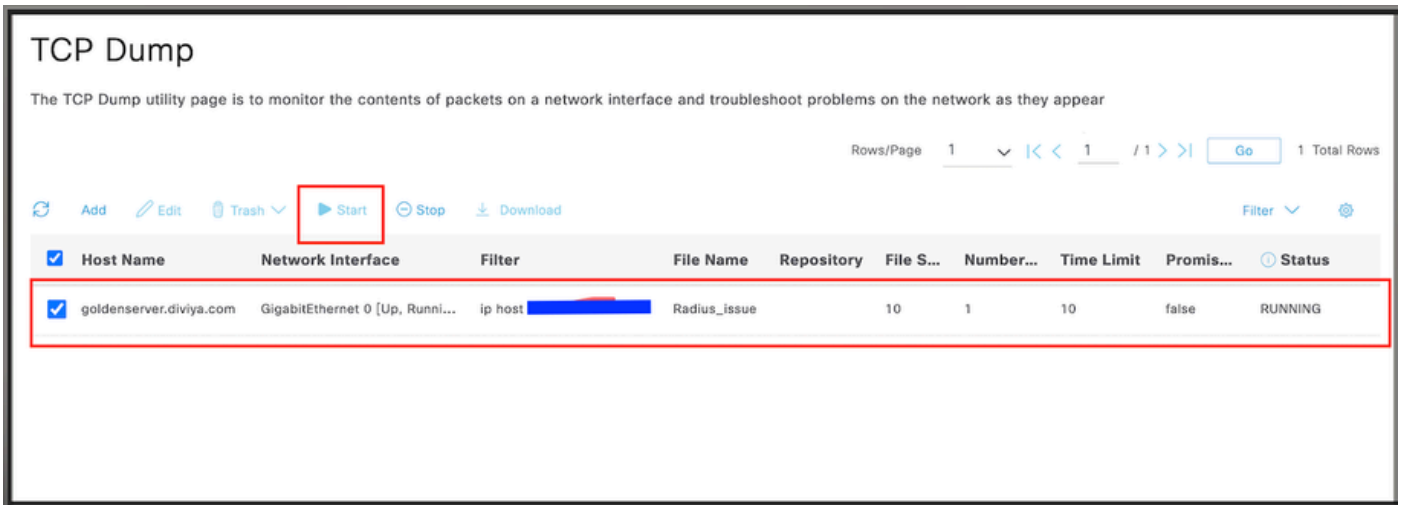
3.1. Operations(운영) > Troubleshoot(문제 해결) > Diagnostic Tools(진단 도구) > TCP dump(TCP 덤프)로 이동합니다.

3.2. UDP 패킷이 ISE 노드에 도착하는지 검토하기 위해 새 캡처를 추가하고 파일을 로컬 시스템에 다운로드합니다.

3.3. 요청한 정보를 입력하고 아래로 스크롤한 후 저장을 클릭합니다.



3.4. 캡처를 선택하고 시작합니다.



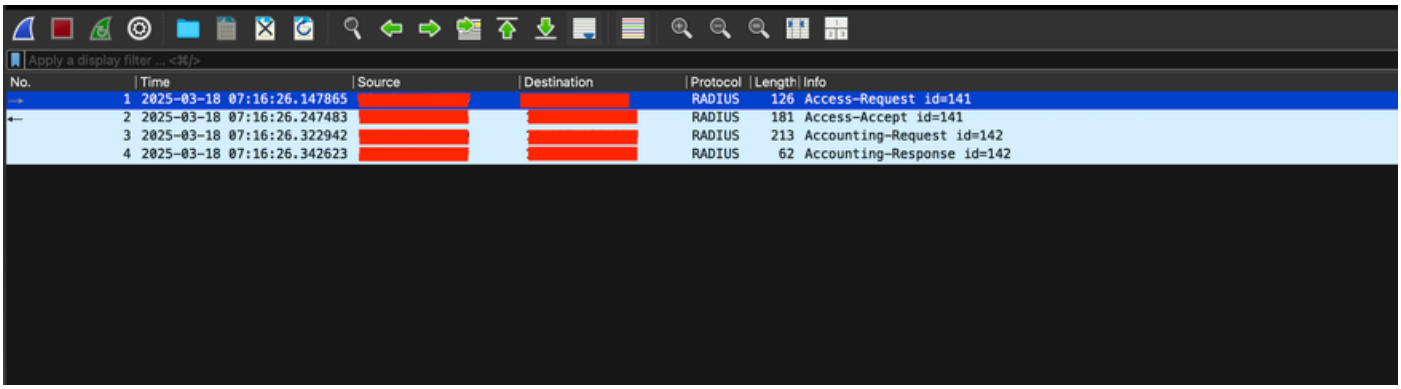
3.5. ISE 캡처가 실행되는 동안 Arista 스위치에 로그인을 시도합니다.

3.6. ISE에서 TCP 덤프를 중지하고 파일을 로컬 시스템에 다운로드합니다.

3.7. 트래픽 출력을 검토합니다.

예상 출력:

패킷 No1. 포트 1812(RADIUS)를 통해 Arista 스위치에서 ISE 서버로 요청합니다.
패킷 No2. ISE 서버 응답이 초기 요청을 수락합니다.



문제 해결

시나리오 1. "5405 RADIUS 요청 삭제됨"

문제

이 시나리오에서는 네트워크 디바이스(예: Arista 스위치)가 인증을 시도할 때 Cisco ISE에서 "11007 Could not locate Network Device or AAA Client(네트워크 디바이스 또는 AAA 클라이언트를 찾을 수 없음)"라는 이유로 "5405 RADIUS Request dropped(5405 RADIUS 요청 삭제됨)" 오류를 해결하는 것이 포함됩니다.

가능한 원인

- Cisco ISE(Identity Services Engine)는 IP 주소가 알려진 네트워크 디바이스 간에 나열되지 않으므로 Arista 스위치를 식별할 수 없습니다.
- RADIUS 요청은 ISE가 유효한 네트워크 디바이스 또는 AAA 클라이언트로 인식하지 않는 IP 주소에서 옵니다.
- 스위치와 ISE 간의 컨피그레이션이 일치하지 않을 수 있습니다(예: 잘못된 IP 또는 공유 암호).

솔루션

- 올바른 IP 주소로 네트워크 장치의 Cisco ISE 목록에 스위치를 추가 합니다.
- ISE에 구성된 IP 주소 및 공유 암호가 스위치에 설정된 것과 정확히 일치하는지 확인합니다.
- 수정한 후에는 RADIUS 요청을 제대로 인식하고 처리해야 합니다.

시나리오 2: Arista 스위치가 백업 ISE PSN으로 장애 조치에 실패함

문제

Arista 스위치는 RADIUS 인증에 Cisco ISE를 사용하도록 구성됩니다. 기본 ISE PSN(Policy Service Node)을 사용할 수 없게 되면 스위치가 백업 PSN으로 자동으로 장애 조치되지 않습니다.

따라서 인증 로그는 기본 ISE PSN에서만 나타나며, 기본 ISE가 다운된 경우 보조/백업 PSN에서 로그가 없습니다.

가능한 원인

- Arista 스위치의 RADIUS 서버 컨피그레이션은 기본 ISE 노드만 가리키므로 백업 서버는 사용되지 않습니다.
- RADIUS 서버 우선순위가 제대로 설정되지 않았거나 백업 ISE IP가 컨피그레이션에 없습니다.
- 스위치의 시간 초과 및 재전송 설정이 너무 낮게 설정되어 백업 PSN으로 제대로 대체되지 않습니다.
- 스위치는 PSN에 대해 FQDN을 사용하지만 DNS 확인에서 모든 A 레코드를 반환하지 않으므로 기본 서버에만 접속됩니다.

솔루션

- 스위치의 RADIUS 서버 그룹 컨피그레이션에 여러 ISE PSN IP가 입력되었는지 확인합니다. 이렇게 하면 기본 서버에 연결할 수 없는 경우 스위치가 백업 ISE PSN을 사용할 수 있습니다.

  컨피그레이션 예:

  ```
  radius-server host <ISE1-IP> key <secret>

  radius-server host <ISE2-IP> key <secret>
  ```

- RADIUS 서버 우선순위, 시간 초과 및 재전송 값이 안정적인 장애 조치를 위해 올바르게 구성되었는지 확인합니다.
- FQDN을 사용하는 경우 DNS 설정 및 확인을 검사하여 모든 PSN IP 주소가 반환되어 스위치에 의해 사용되는지 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.