# ISE를 사용하여 Arista 스위치에서 TACACS+ 인증 구성

## 목차



## 소개

이 문서에서는 관리자 액세스의 중앙 집중식 AAA를 위해 Cisco ISE TACACS+를 Arista 스위치와 통합하는 방법에 대해 설명합니다.

## 사전 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ISE 및 TACACS+ 프로토콜.
- Arista 스위치

## 사용되는 구성 요소

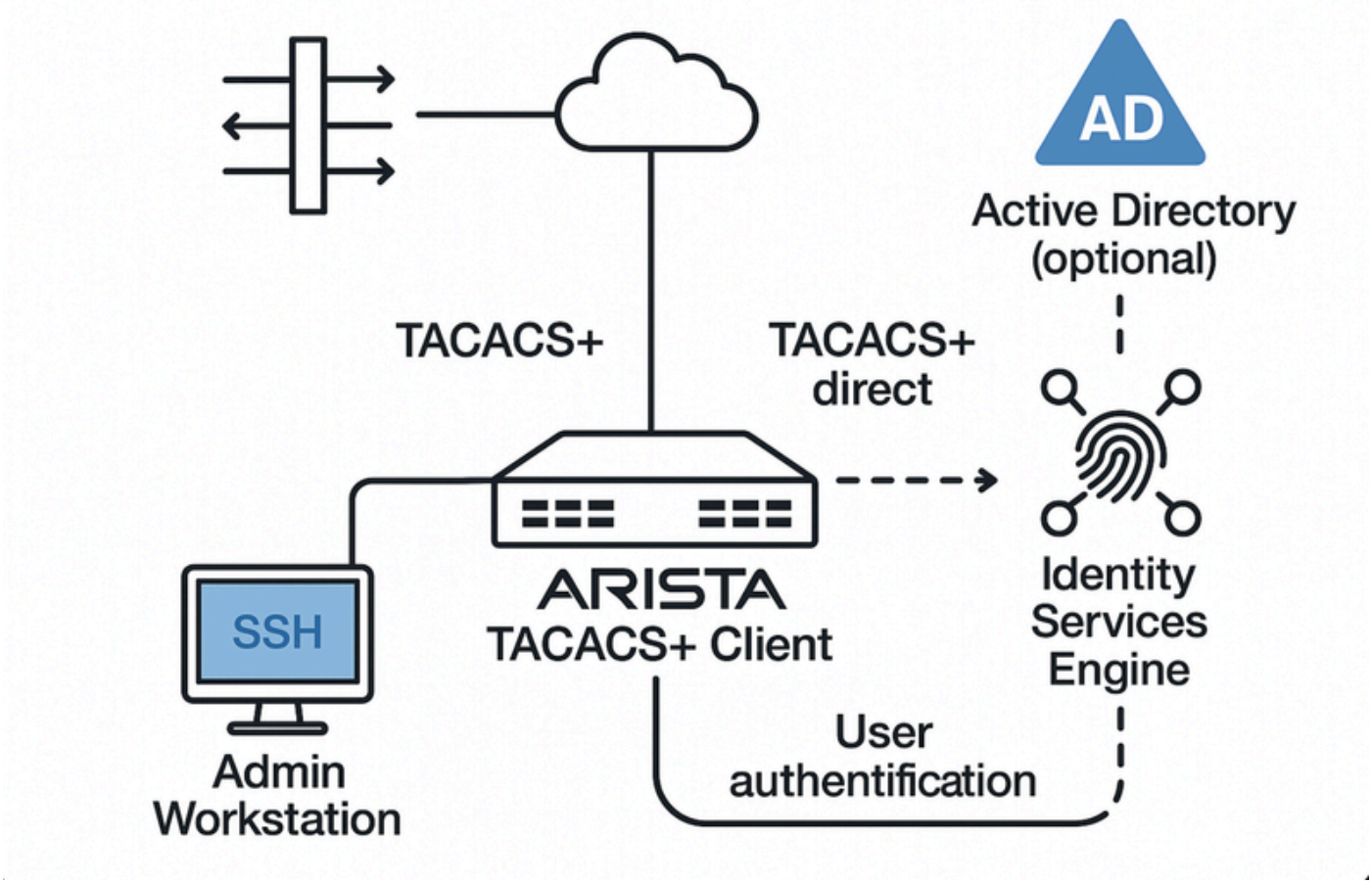
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 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 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다

## 네트워크 다이어그램

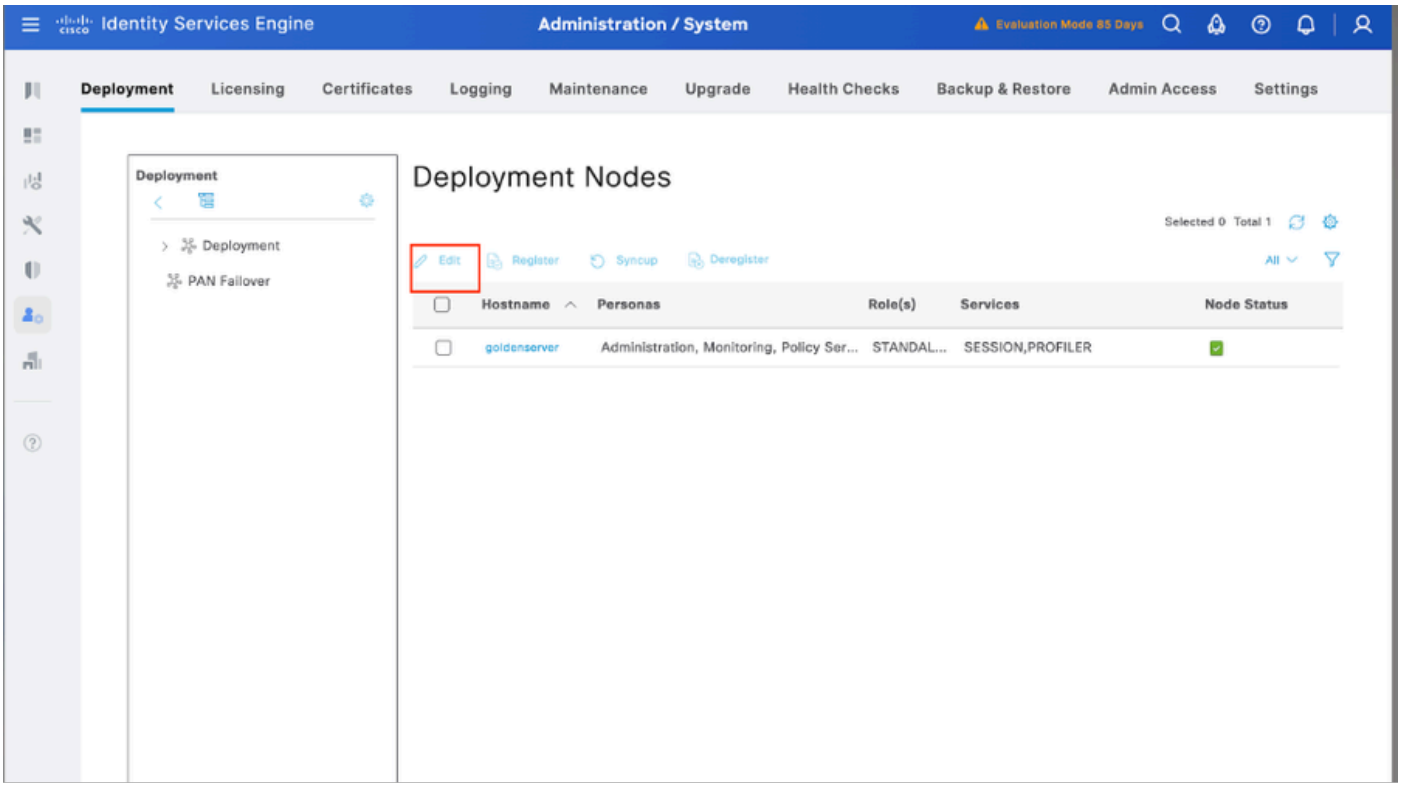



## 설정

### ISE의 TACACS+ 컨피그레이션

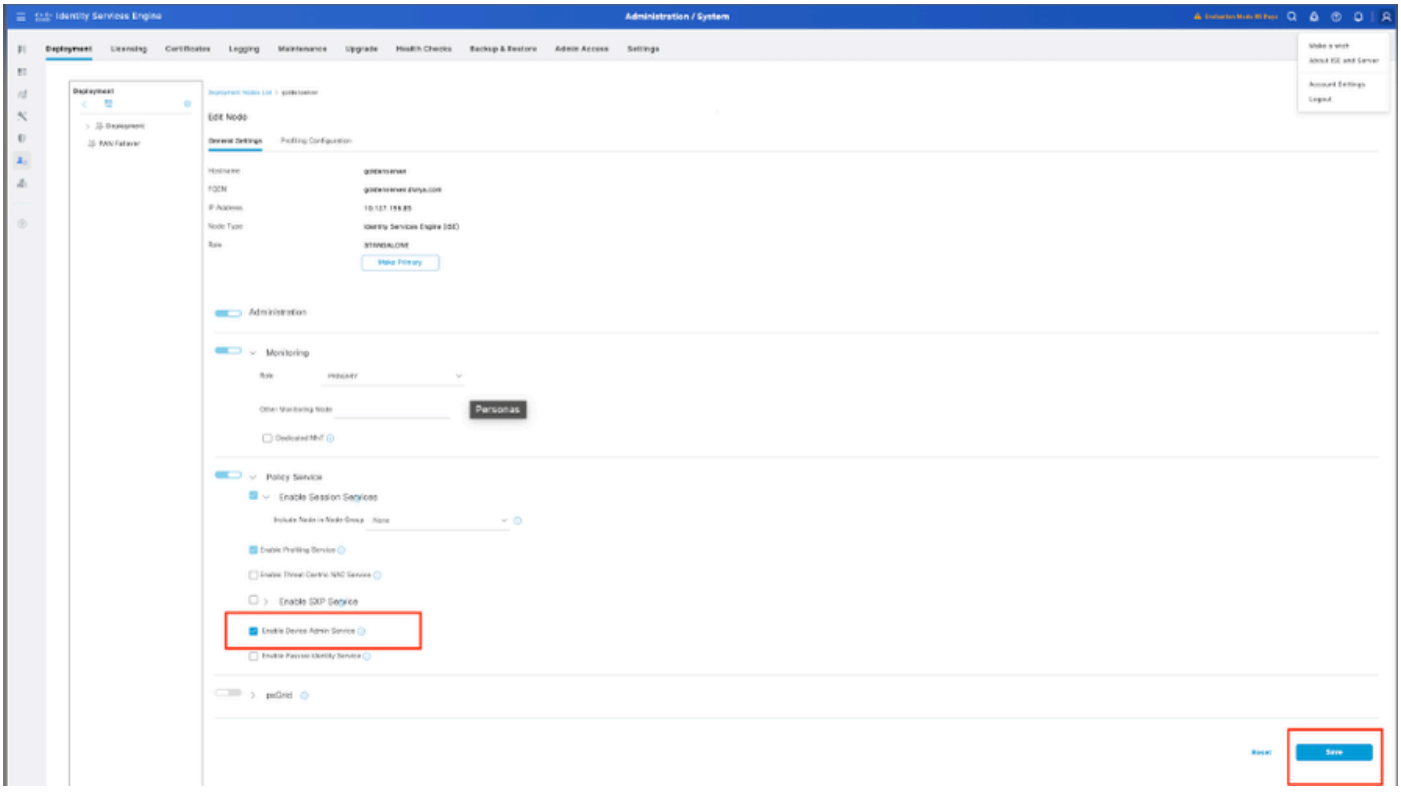
1단계. 첫 번째 단계는 Cisco ISE가 TACACS+ 인증을 처리하는 데 필요한 기능을 갖추고 있는지 확인하는 것입니다. 이렇게 하려면 원하는 PSN(Policy Service Node)에 디바이스 관리 서비스 기능이 활성화되어 있는지 확인합니다.

Administration > System > Deployment로 이동하여 ISE에서 TACACS+ 인증을 처리하는 해당 노드를 선택하고 Edit를 클릭하여 해당 컨피그레이션을 검토합니다.




2단계. 아래로 스크롤하여 Device Administration Service 기능을 찾습니다. 이 기능을 활성화하려면 구축에서 사용 가능한 TACACS+ 라이센스와 함께 정책 서비스 페르소나가 노드에서 활성화되어야 합니다.

확인란을 선택하여 기능을 활성화한 다음 컨피그레이션을 저장합니다.

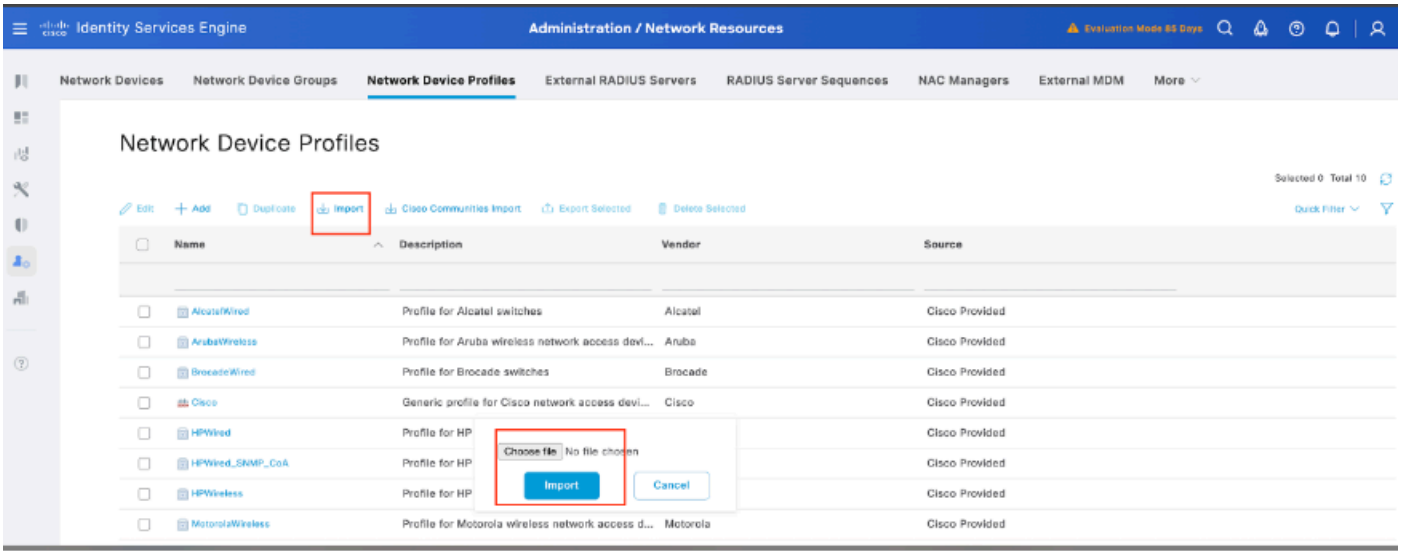



3단계. Cisco ISE용 Arista 네트워크 디바이스 프로파일 얻기

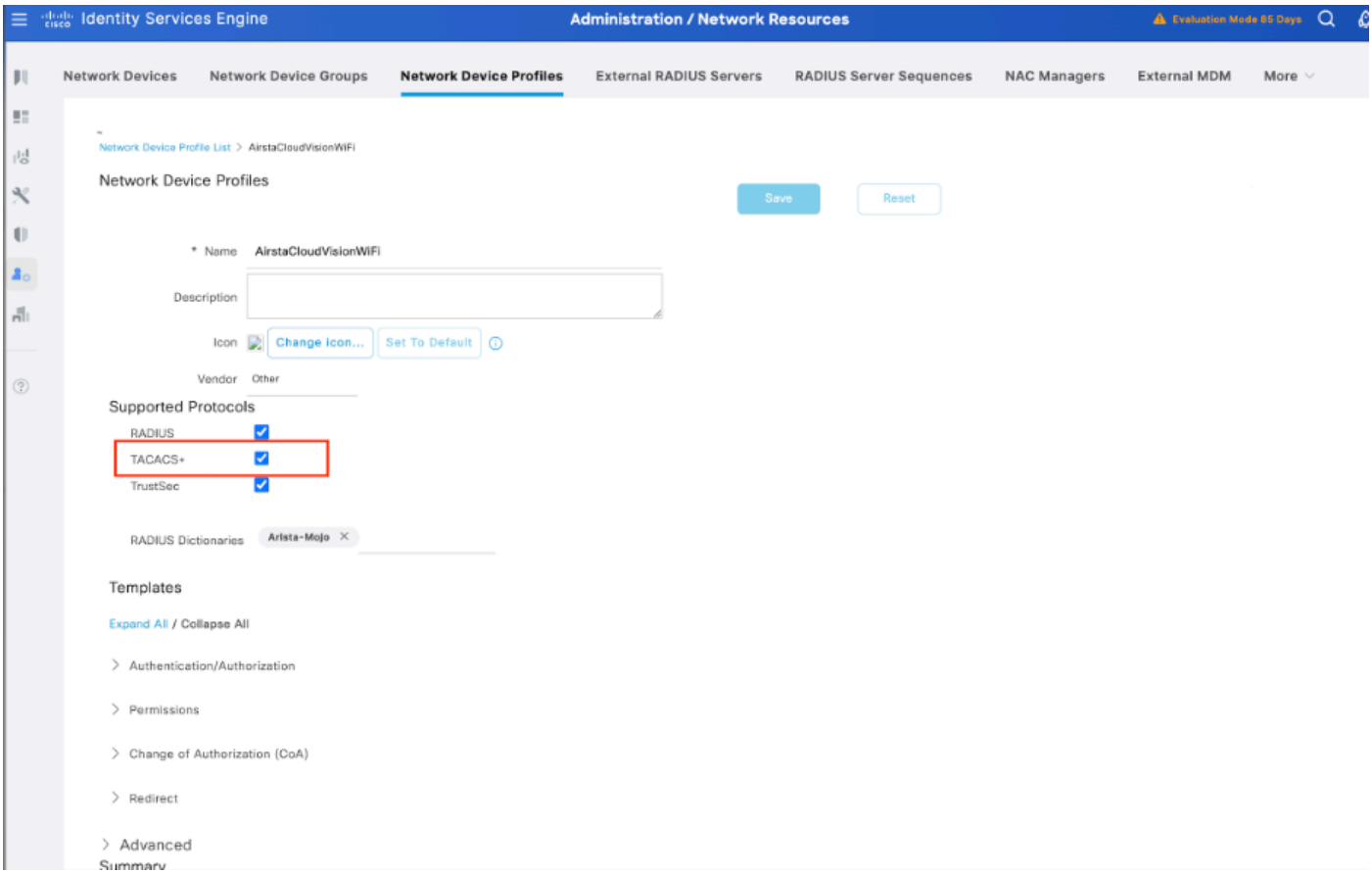
Cisco 커뮤니티는 Arista 디바이스에 대한 전용 NAD 프로필을 공유했습니다. 이 프로파일은 필요한 사전 파일과 함께 Arista CloudVision WiFi Dictionary and NAD Profile for ISE Integration(ISE 통합을 위한 Arista CloudVision WiFi 사전 및 NAD 프로파일) 문서에서 찾을 수 있습니다. 이 프로파일을 다운로드하고 ISE 설정으로 가져오면 더 원활한 통합이 가능합니다.

Cisco ISE로 Arista NAD 프로파일을 가져오는 단계:

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.

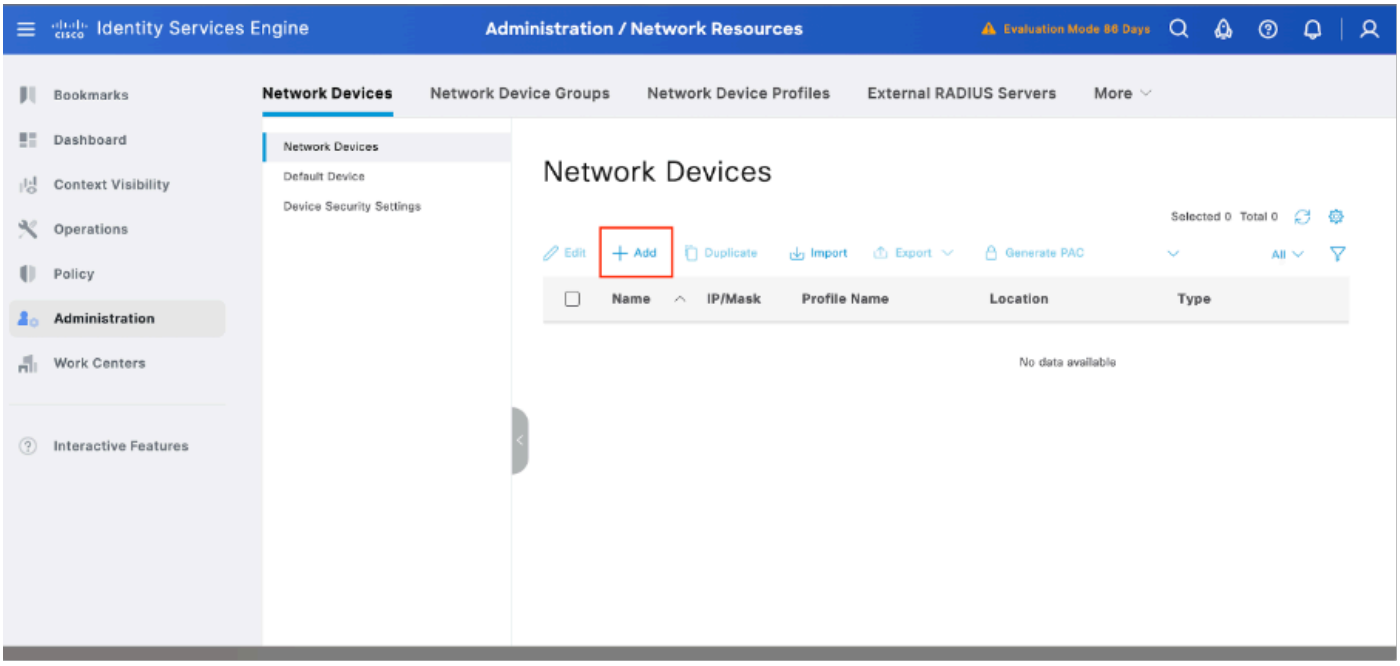



업로드가 완료되면 Edit(수정) 옵션으로 이동하여 지원되는 프로토콜로 TACACS+를 활성화합니다.




2단계: Arista 스위치를 네트워크 디바이스로 추가합니다.

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

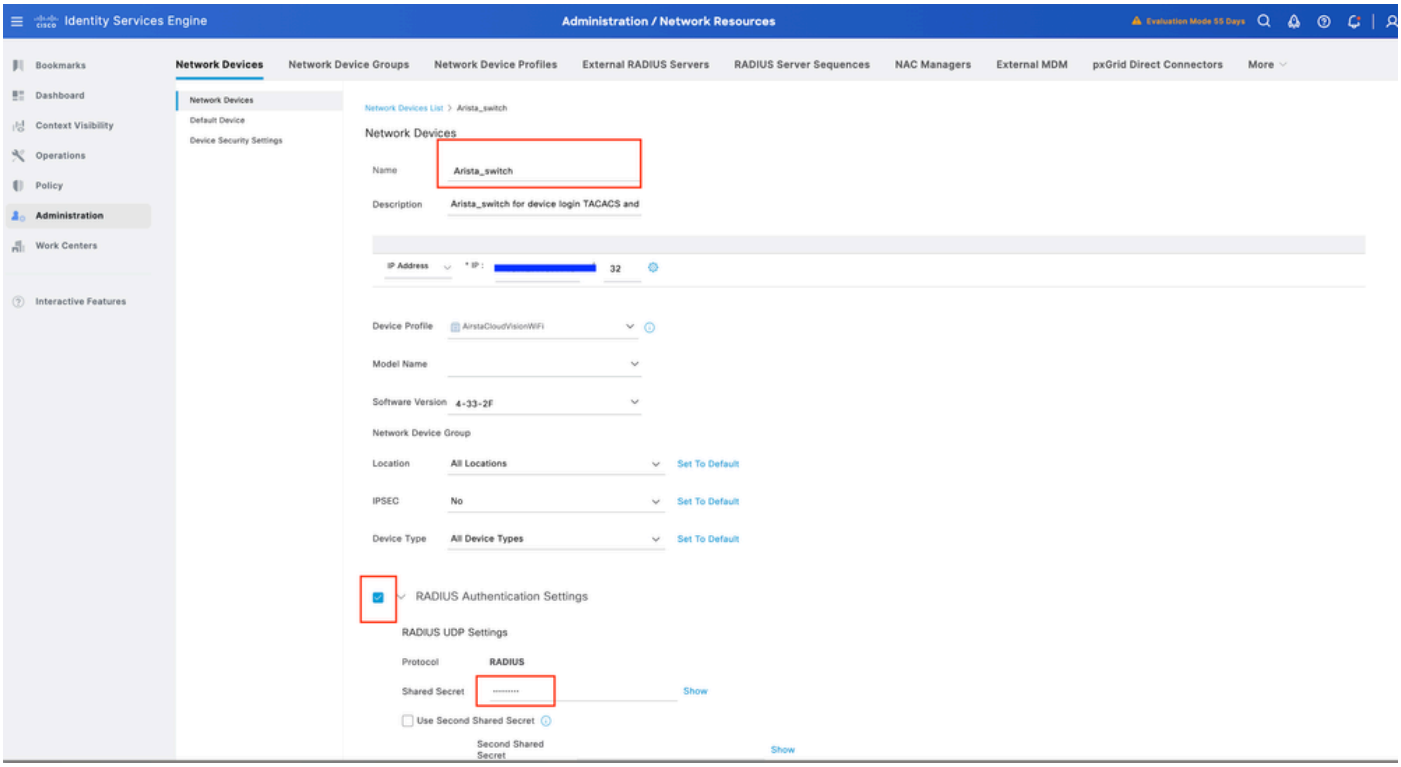



2.Add(추가)를 클릭하고 다음 세부 정보를 입력합니다.

- IP 주소: <스위치 IP>
- 장치 유형: 기타 유선 선택

- 네트워크 장치 프로파일: airstaCloudVisionWiFi를 선택합니다.
- RADIUS 인증 설정:
  - RADIUS 인증을 활성화합니다.
  - 공유 암호를 입력합니다(스위치 컨피그레이션과 일치해야 함).

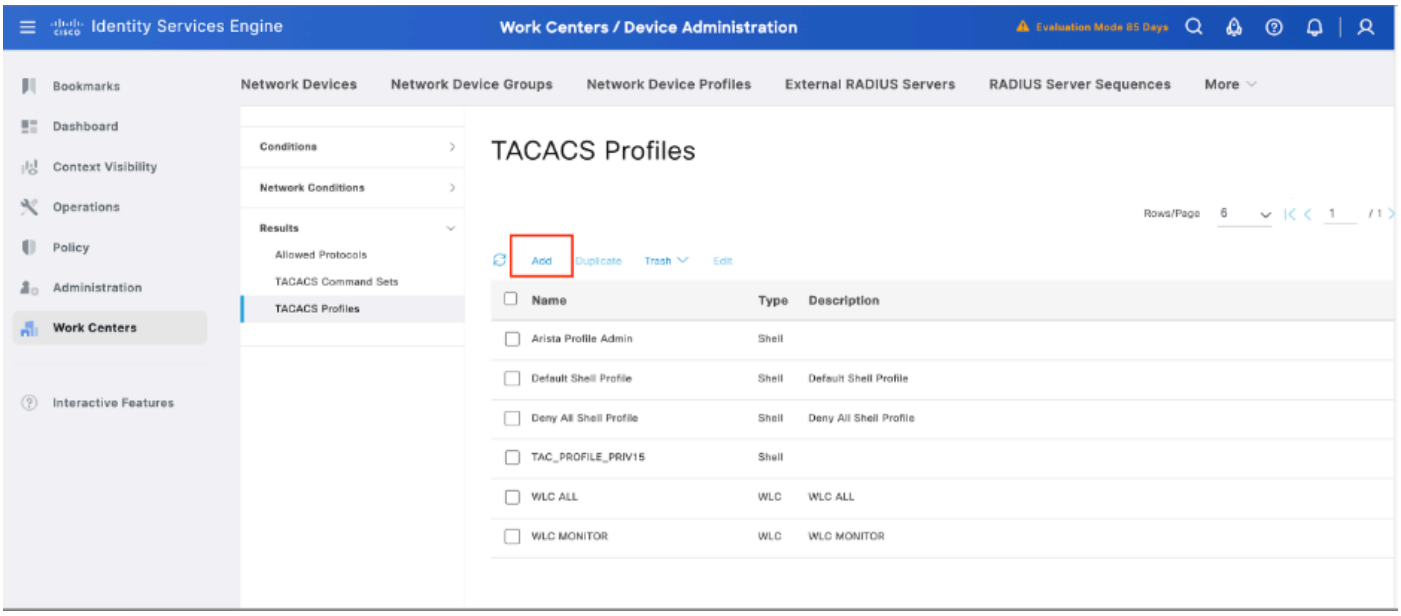
3. 저장을 클릭합니다.



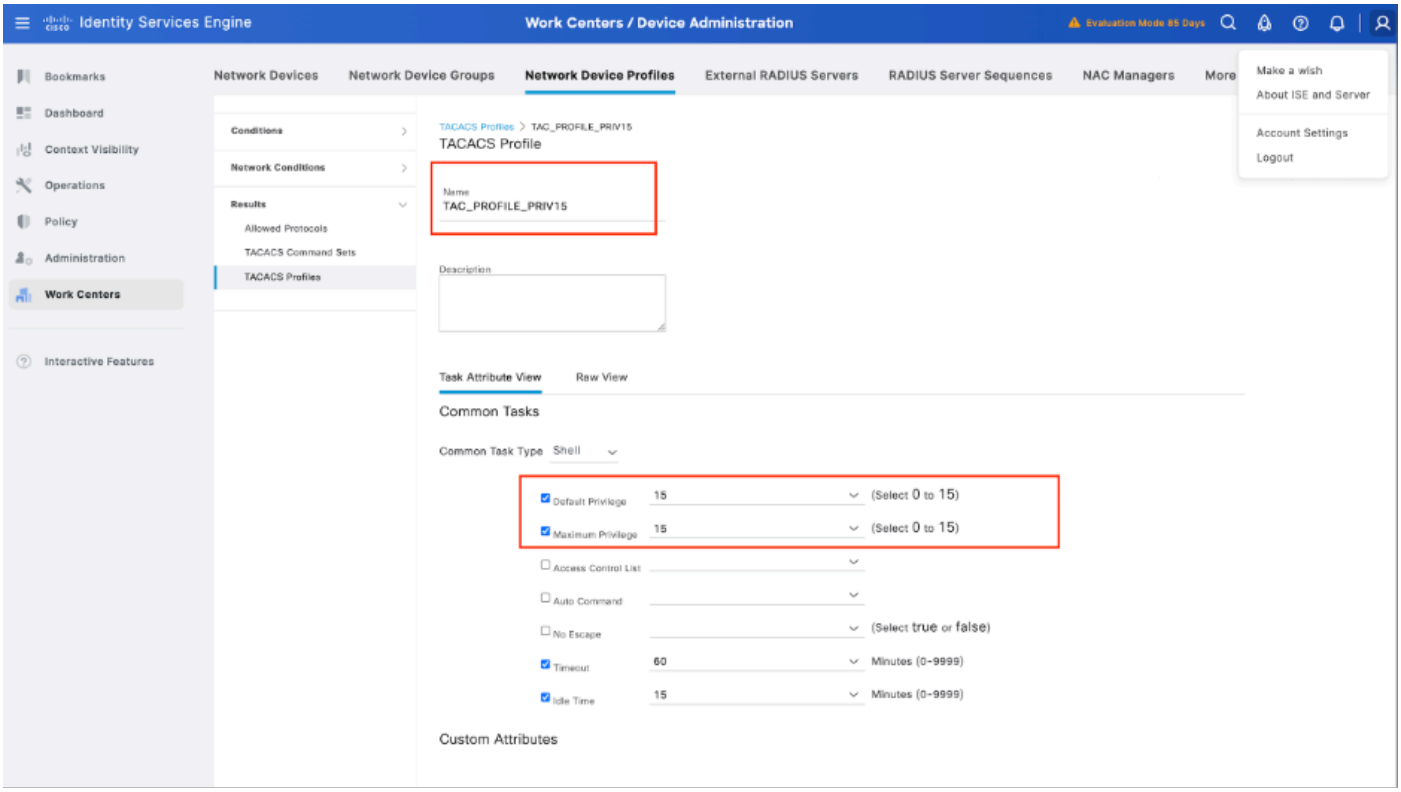

3단계. Network Devices(네트워크 디바이스)에 새 디바이스가 표시되는지 확인합니다.


4단계. TACACS 프로파일을 구성합니다.

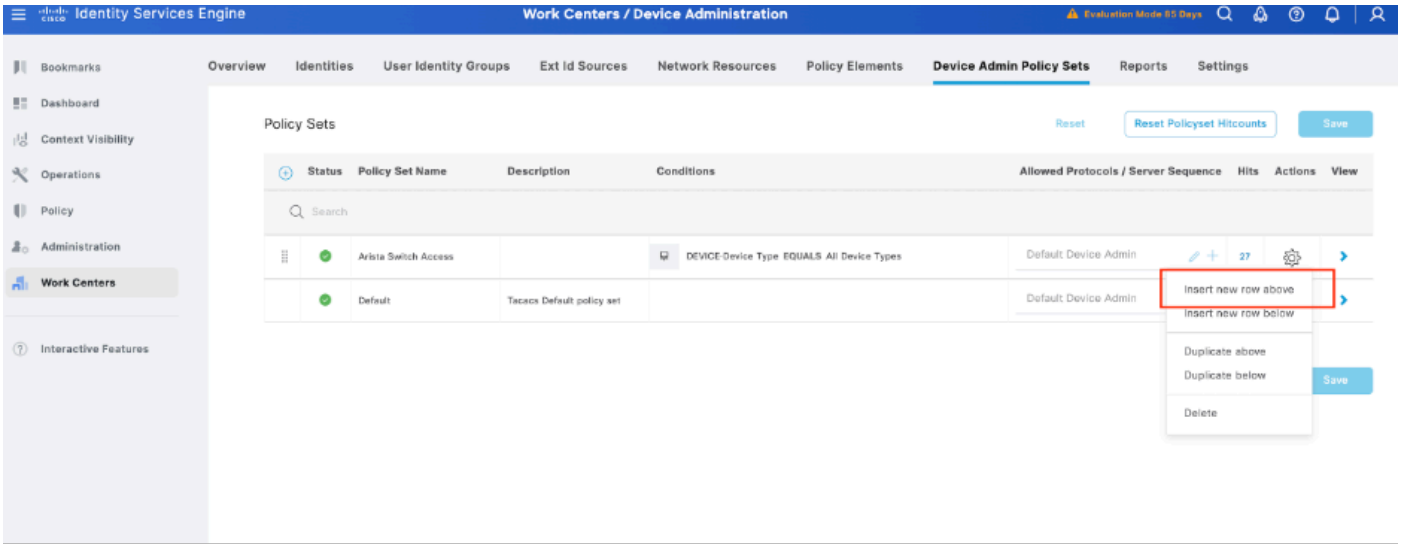
TACACS 프로필을 생성하고 Work Centers(작업 센터) > Device Administration(디바이스 관리) > Policy Elements(정책 요소) > Results(결과) > TACACS Profiles(TACACS 프로필) 메뉴로 이동한 다음 Add(추가)를 선택합니다.



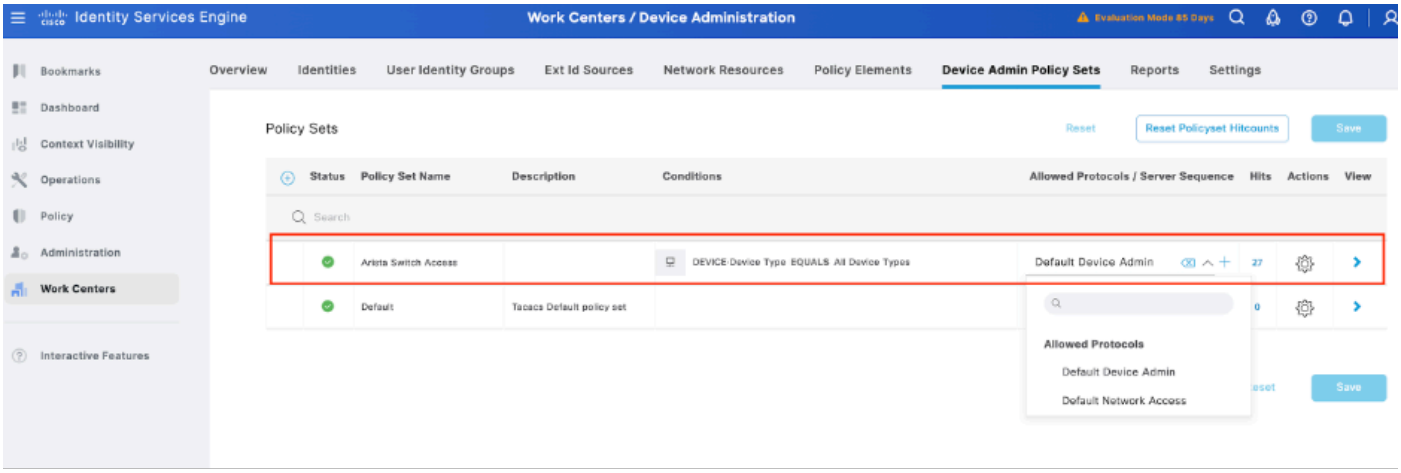

이름을 입력하고 기본 권한 확인란을 선택한 다음 값을 15로 설정합니다. 또한 최대 권한을 선택하고 값을 15로 설정한 다음 제출을 누릅니다.



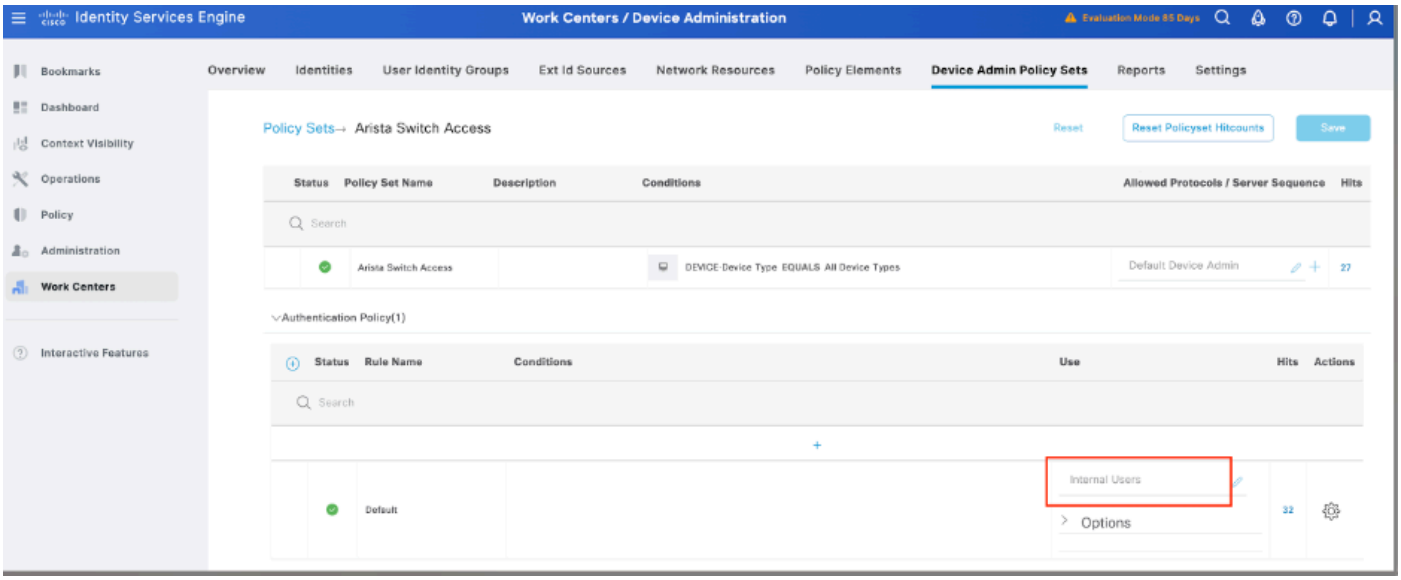

5단계. Arista 스위치에 사용할 Device Admin Policy Set(디바이스 관리 정책 집합)를 생성하고, Work Centers(작업 센터) > Device Administration(디바이스 관리) > Device Admin Policy Sets(디바이스 관리 정책 집합) 메뉴로 이동한 다음, 기존 정책 집합에서 기어 아이콘을 선택하여 Insert new row above(위에 새 행 삽입)를 선택합니다.




6단계. 이 새 정책 세트의 이름을 지정하고, Arista 스위치에서 진행 중인 TACACS+ 인증의 특성에 따라 조건을 추가하고, Allowed Protocols(허용되는 프로토콜) > Default Device Admin(기본 디바이스 관리)으로 선택하고, 컨피그레이션을 저장합니다.

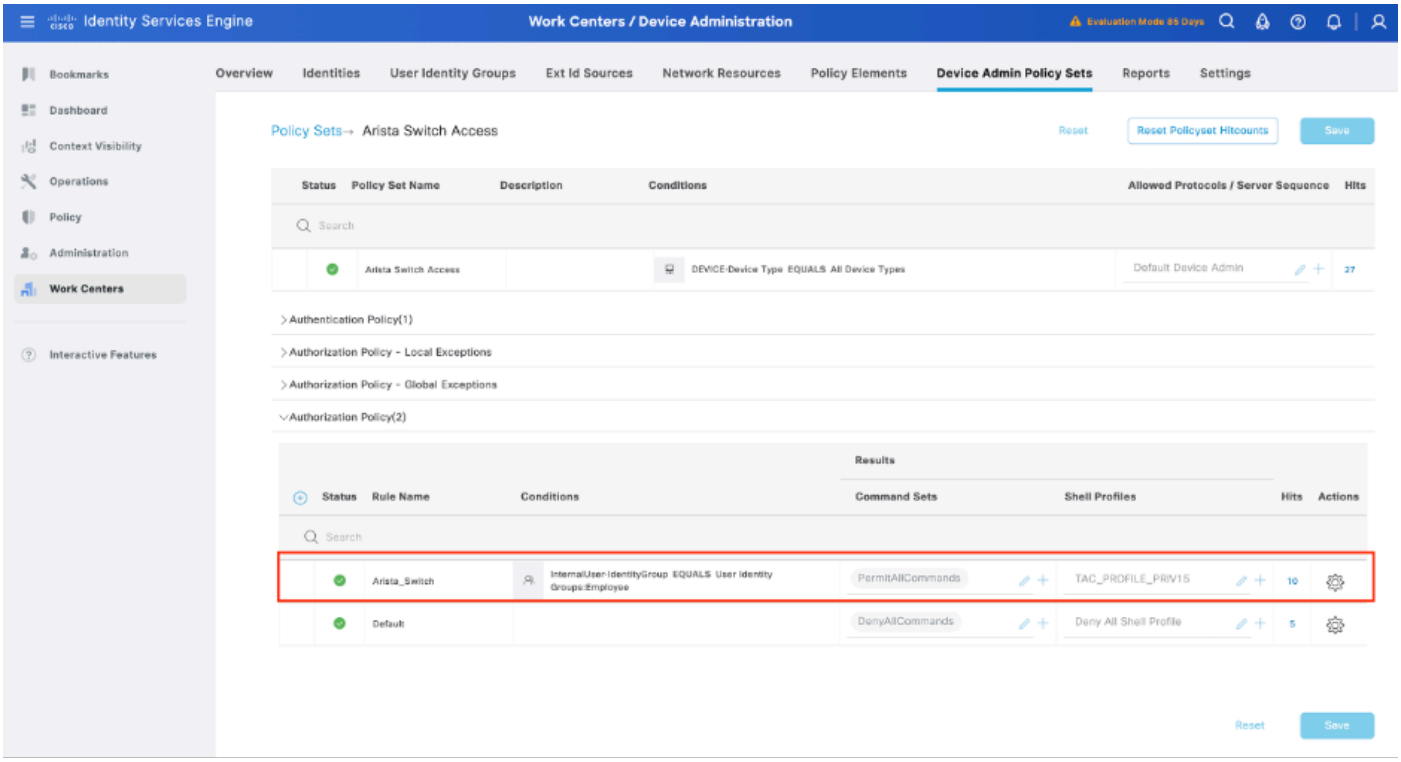



7단계. > view 옵션에서 선택한 다음 Authentication Policy(인증 정책) 섹션에서 Cisco ISE가 Arista 스위치에서 인증을 위해 사용자 이름 및 자격 증명을 쿼리하는 데 사용하는 외부 ID 소스를 선택합니다. 이 예에서 자격 증명은 ISE에 저장된 내부 사용자에 해당합니다.



8단계. Authorization Policy to Default policy(권한 부여 정책에서 기본 정책으로) 섹션이 표시될 때까지 아래로 스크롤하여 기어 아이콘을 선택한 다음 위에 하나의 규칙을 삽입합니다.

9단계. 새 Authorization Rule(권한 부여 규칙)의 이름을 지정하고, 그룹 멤버십으로 이미 인증된 사용자에 대한 조건을 추가하고, Shell Profiles(셸 프로파일) 섹션에서 이전에 구성한 TACACS 프로파일을 추가하고 컨피그레이션을 저장합니다.




## Arista 스위치 구성

1단계. TACACS+ 인증 활성화

Arista 스위치에 로그인하고 컨피그레이션 모드로 들어갑니다.

구성

!

tacacs-server host <ISE-IP> key <TACACS-SECRET>

!

aaa 그룹 서버 tacacs+ ISE_TACACS

  서버 <ISE-IP>

!

aaa 인증 로그인 기본 그룹 ISE_TACACS 로컬

aaa authorization exec 기본 그룹 ISE_TACACS 로컬

aaa accounting 명령 15 default start-stop group ISE_TACACS

!

끝

2단계. 구성을 저장합니다.

재부팅 시에도 컨피그레이션을 유지하려면

쓰기 메모리 #

또는

# running-config startup-config 복사

# 다음을 확인합니다.

## ISE 검토

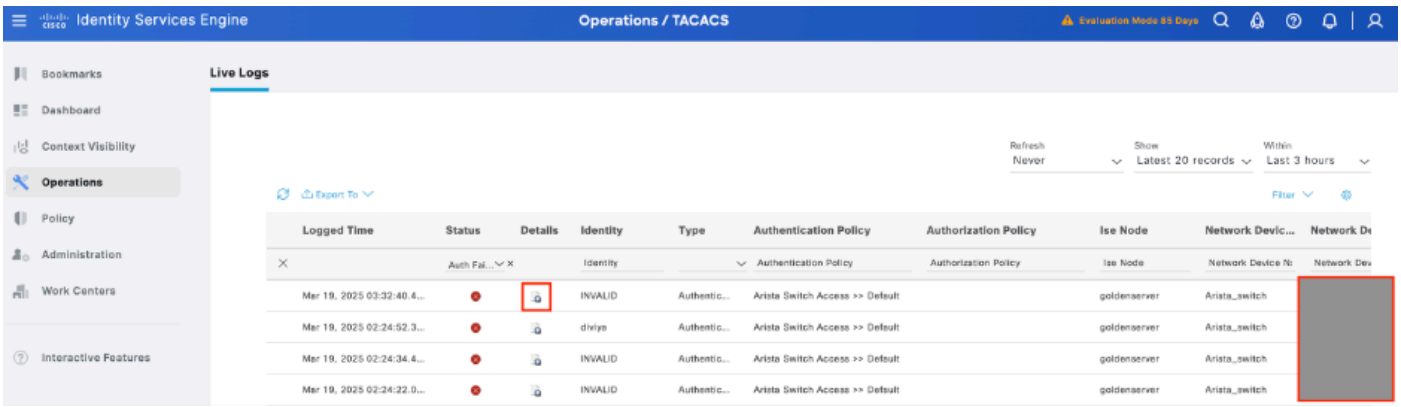
1단계. TACACS+ 서비스 가용성이 실행 중인지 검토합니다. 다음을 체크인할 수 있습니다.

- GUI: 서비스 DEVICE ADMIN(디바이스 관리)에 노드가 나열되어 있는지 System(시스템) > Deployment(구축)에서 검토합니다.
- CLI: show ports 명령을 실행합니다 | TACACS+에 속하는 TCP 포트에 연결이 있는지 확인하려면 49를 포함합니다.

```
goldenserver/admin#show ports | include 49
tcp: [redacted]
```

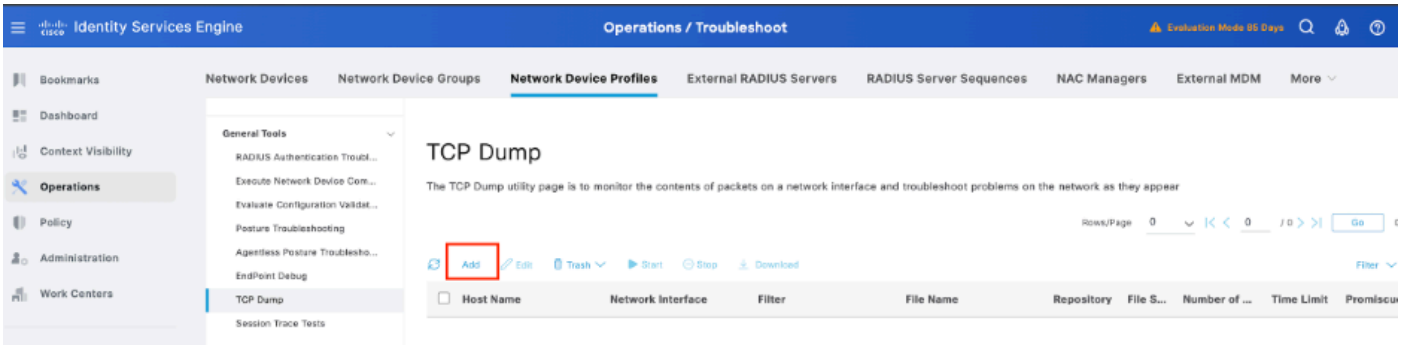
2단계. TACACS+ 인증 시도와 관련된 livelogs가 있는지 확인합니다. 이는 Operations(작업) > TACACS > Live logs(라이브 로그) 메뉴에서 확인할 수 있습니다.

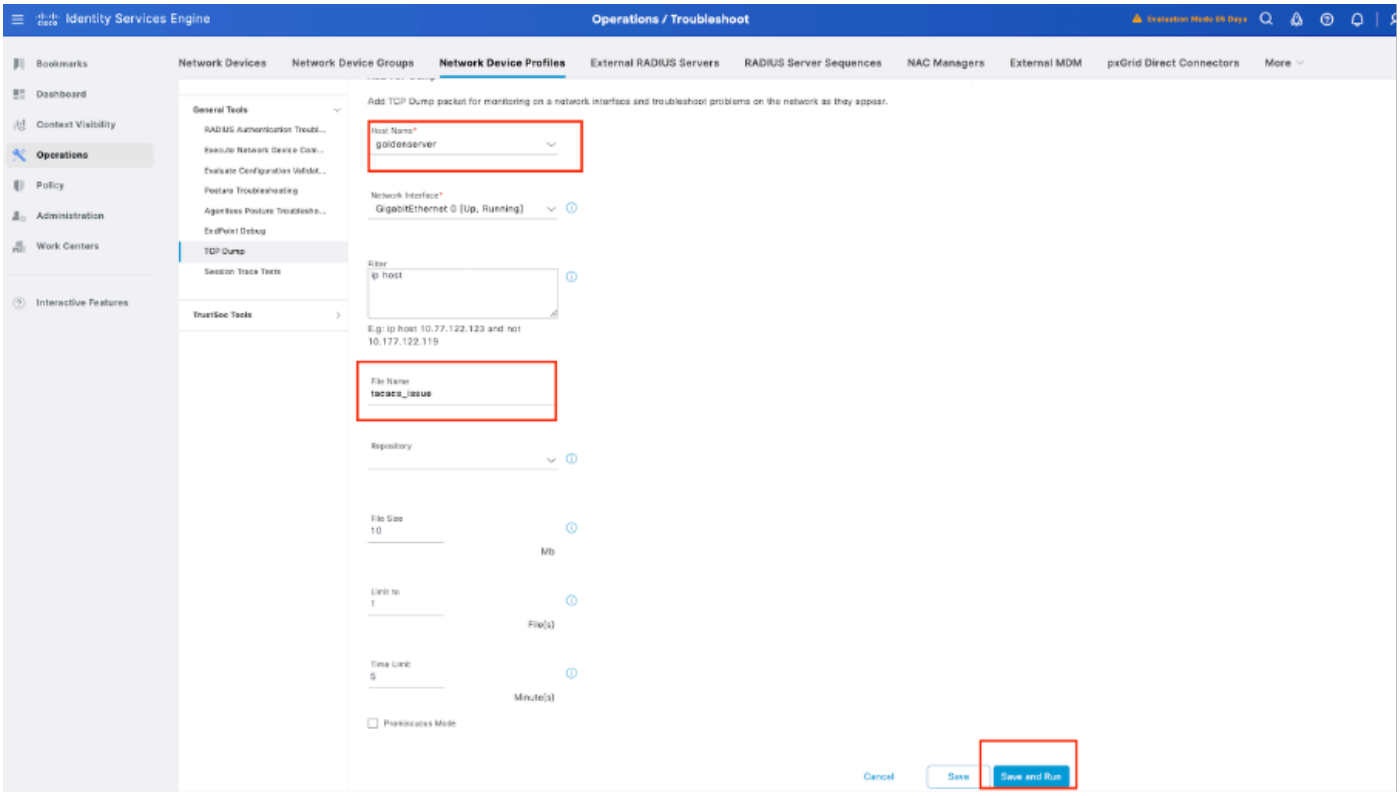
실패 사유에 따라 컨피그레이션을 조정하거나 실패 원인을 해결할 수 있습니다.



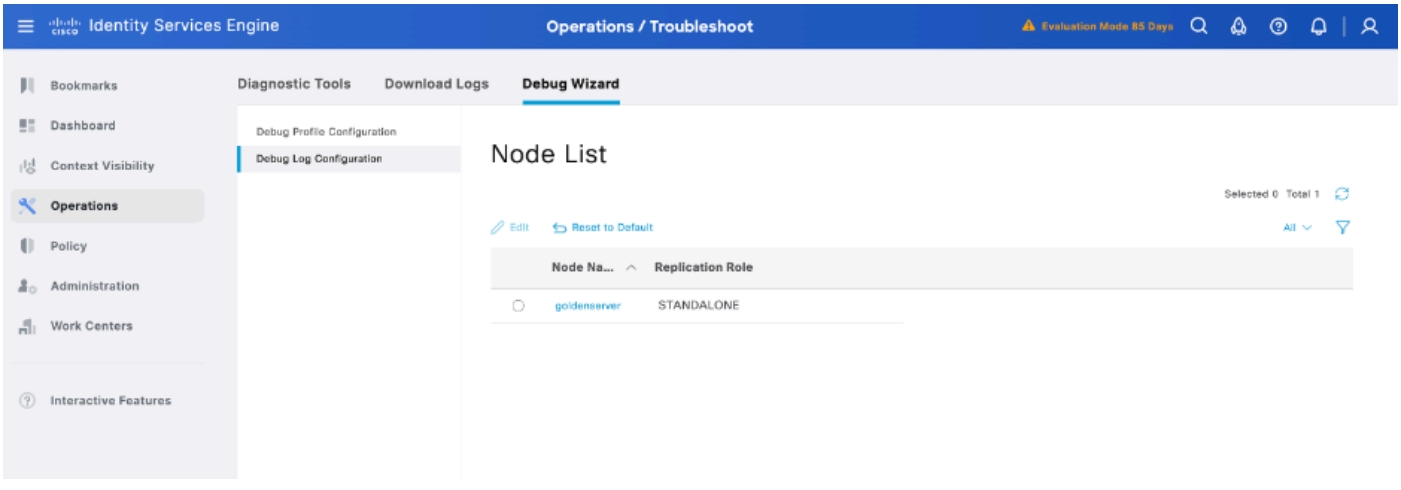

3단계. Livelog가 표시되지 않는 경우 패킷 캡처를 수행합니다. Operations(운영) > Troubleshoot(문제 해결) > Diagnostic Tools(진단 도구) > General Tools(일반 도구) > TCP Dump(TCP 덤프) 메뉴

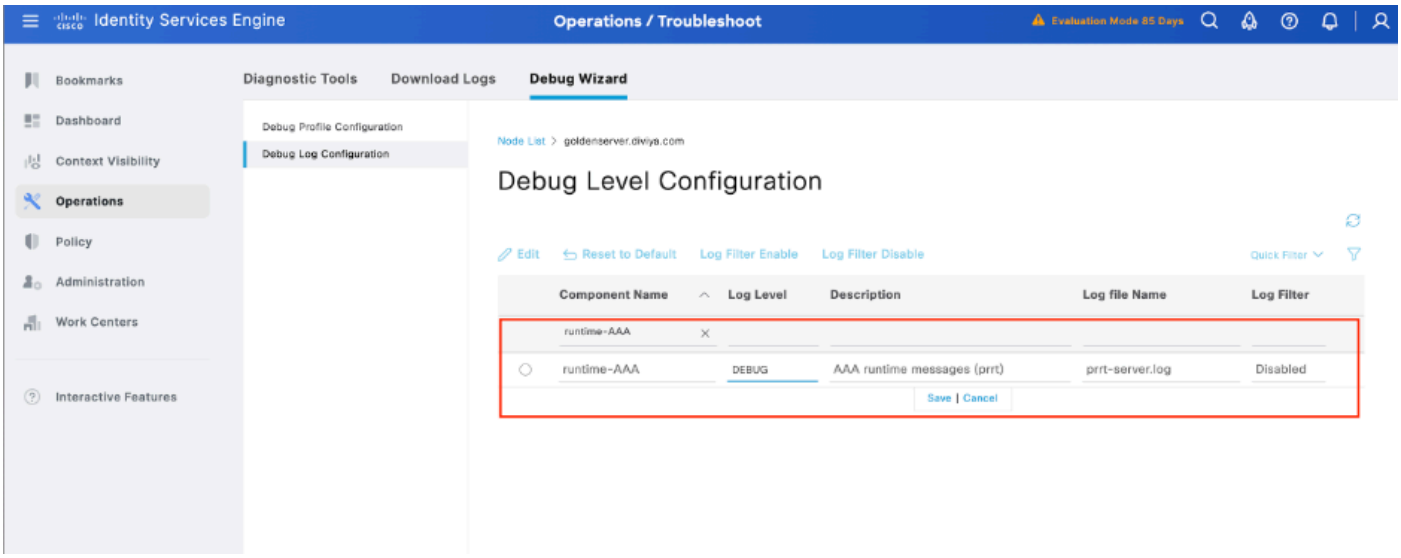
로 이동하여 Add(추가)를 선택합니다.




4단계. Operations(운영) > Troubleshoot(문제 해결) > Debug Wizard(디버그 마법사) > Debug log configuration(디버그 로그 컨피그레이션)에서 인증이 수행되는 PSN 내의 디버그에서 구성 요소 런타임-AAA를 활성화하고, PSN 노드를 선택한 다음 Edit(편집) 버튼을 선택합니다.





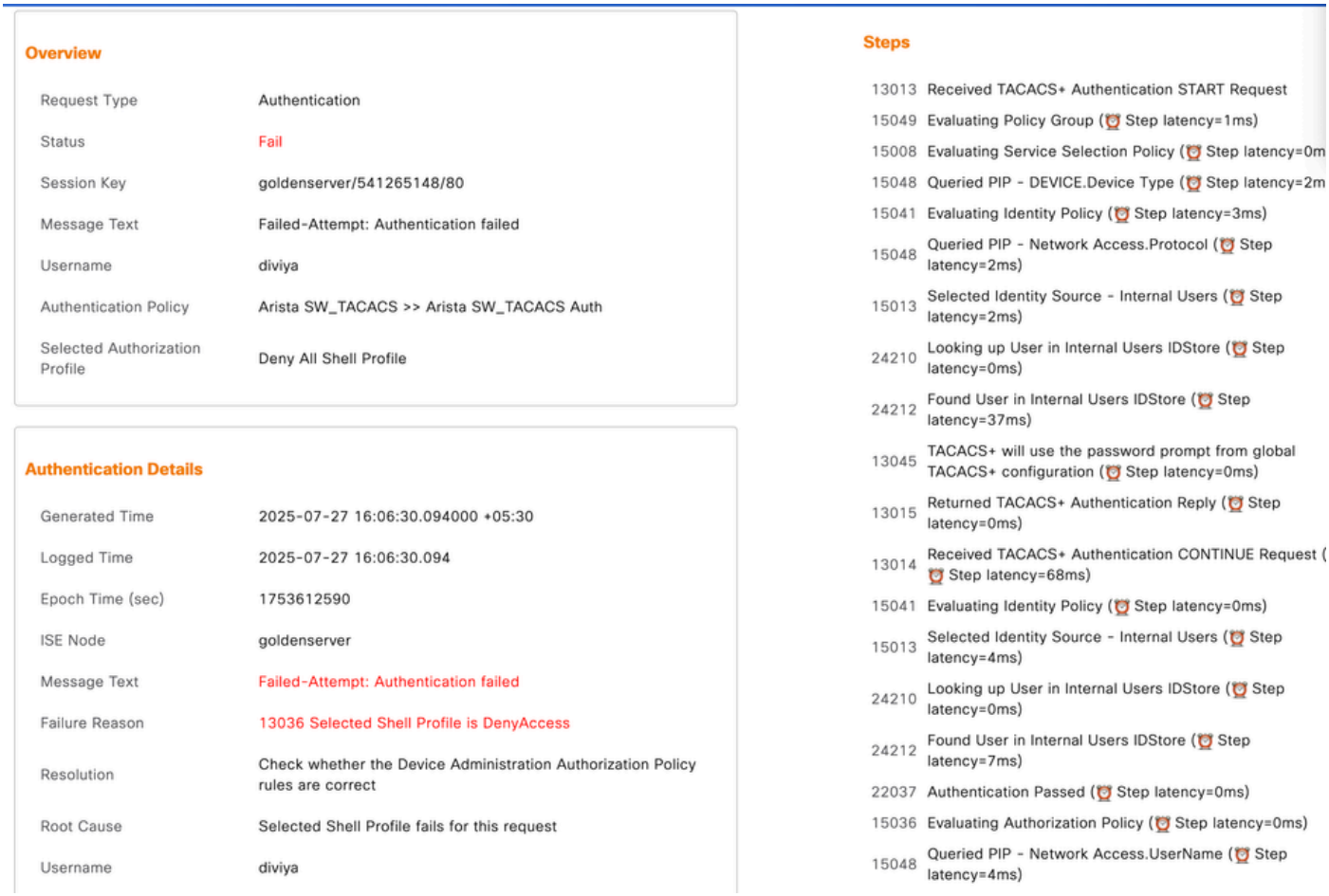

런타임 AAA 구성 요소를 식별하고, 로깅 수준을 디버그로 설정하고, 문제를 재현하고, 추가 조사를 위해 로그를 분석합니다.

# 문제 해결

## 문제 1

Cisco ISE와 Arista 스위치(또는 모든 네트워크 디바이스) 간의 TACACS+ 인증은 다음 오류 메시지와 함께 실패합니다.

"13036 셸 프로필이 DenyAccess인 경우"



**Overview**

| | |
|---|---|
| Request Type | Authentication |
| Status | Fail |
| Session Key | goldenserver/541265148/80 |
| Message Text | Failed-Attempt: Authentication failed |
| Username | diviya |
| Authentication Policy | Arista SW_TACACS >> Arista SW_TACACS Auth |
| Selected Authorization Profile | Deny All Shell Profile |

**Authentication Details**

| | |
|---|---|
| Generated Time | 2025-07-27 16:06:30.094000 +05:30 |
| Logged Time | 2025-07-27 16:06:30.094 |
| Epoch Time (sec) | 1753612590 |
| ISE Node | goldenserver |
| Message Text | Failed-Attempt: Authentication failed |
| Failure Reason | 13036 Selected Shell Profile is DenyAccess |
| Resolution | Check whether the Device Administration Authorization Policy rules are correct |
| Root Cause | Selected Shell Profile fails for this request |
| Username | diviya |

**Steps**

| | |
|---|---|
| 13013 | Received TACACS+ Authentication START Request |
| 15049 | Evaluating Policy Group (Step latency=1ms) |
| 15008 | Evaluating Service Selection Policy (Step latency=0m |
| 15048 | Queried PIP - DEVICE.Device Type (Step latency=2m |
| 15041 | Evaluating Identity Policy (Step latency=3ms) |
| 15048 | Queried PIP - Network Access.Protocol (Step latency=2ms) |
| 15013 | Selected Identity Source - Internal Users (Step latency=2ms) |
| 24210 | Looking up User in Internal Users IDStore (Step latency=0ms) |
| 24212 | Found User in Internal Users IDStore (Step latency=37ms) |
| 13045 | TACACS+ will use the password prompt from global TACACS+ configuration (Step latency=0ms) |
| 13015 | Returned TACACS+ Authentication Reply (Step latency=0ms) |
| 13014 | Received TACACS+ Authentication CONTINUE Request ( Step latency=68ms) |
| 15041 | Evaluating Identity Policy (Step latency=0ms) |
| 15013 | Selected Identity Source - Internal Users (Step latency=4ms) |
| 24210 | Looking up User in Internal Users IDStore (Step latency=0ms) |
| 24212 | Found User in Internal Users IDStore (Step latency=7ms) |
| 22037 | Authentication Passed (Step latency=0ms) |
| 15036 | Evaluating Authorization Policy (Step latency=0ms) |
| 15048 | Queried PIP - Network Access.UserName (Step latency=4ms) |

Cisco ISE의 "13036 Selected Shell Profile is DenyAccess" 오류는 일반적으로 TACACS+ 디바이스 관리 시도 중에 권한 부여 정책이 DenyAccess로 설정된 셸 프로파일과 일치했음을 의미합니다.이는 일반적으로 잘못 구성된 셸 프로파일 자체의 결과가 아니라, 구성된 권한 부여 규칙 중 어떤 것도 들어오는 사용자 특성(예: 그룹 멤버십, 디바이스 유형 또는 위치)과 일치하지 않음을 나타냅니다. 그 결과 ISE는 기본 규칙 또는 명시적 거부 규칙으로 폴백하여 액세스가 거부됩니다.

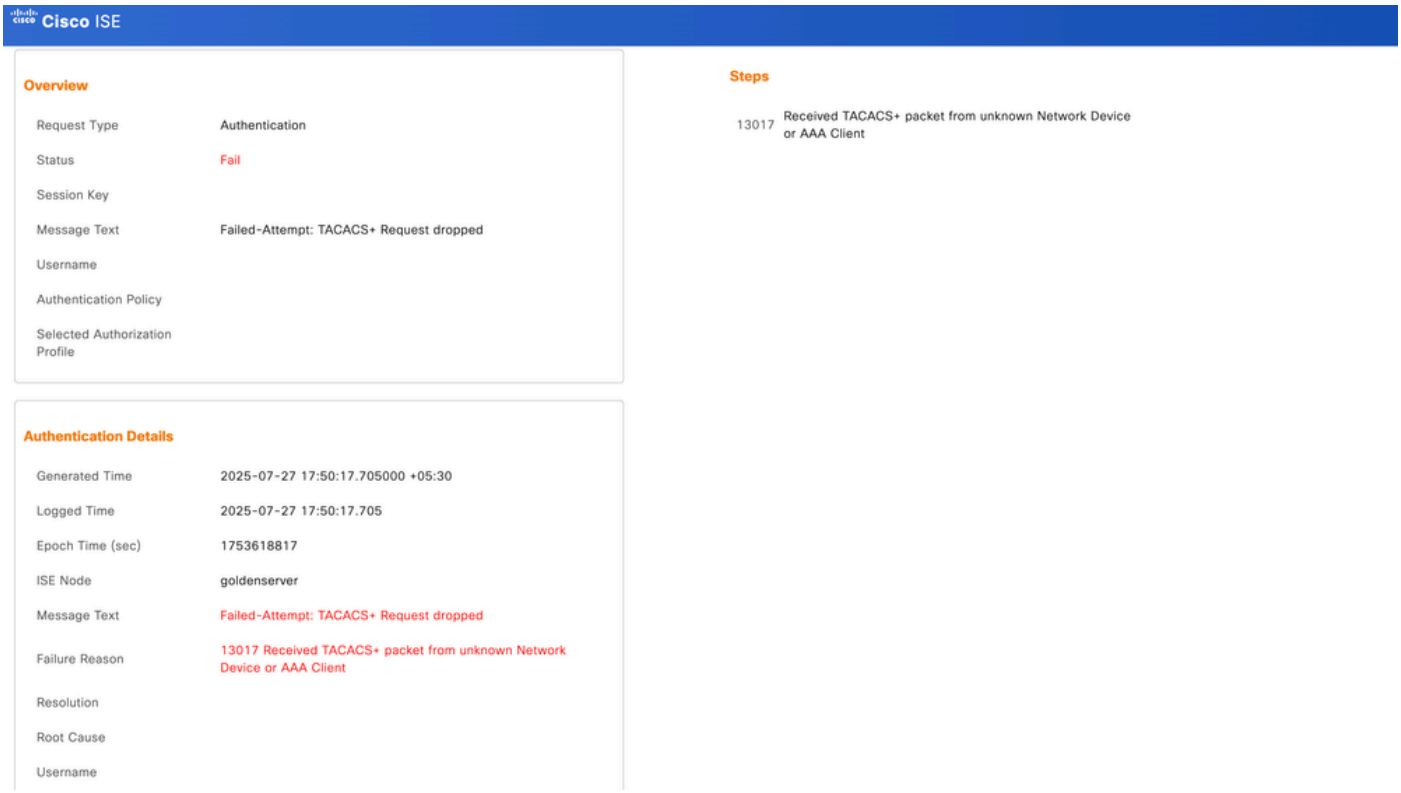
가능한 원인

- ISE의 권한 부여 정책 규칙을 검토합니다. 사용자 또는 디바이스가 적절한 액세스를 허용하는 것과 같이 원하는 셸 프로파일을 할당하는 올바른 규칙과 일치하는지 확인합니다.
- AD 또는 내부 사용자 그룹 매핑이 올바르고 사용자 그룹 구성원 자격, 장치 유형 및 프로토콜과 같은 정책 조건이 정확하게 지정되었는지 확인합니다.
- ISE 라이브 로그 및 실패한 시도의 세부 정보를 사용하여 정확히 일치하는 규칙과 그 이유를 확인합니다.

## 문제 2

Cisco ISE와 Arista 스위치(또는 모든 네트워크 디바이스) 간의 TACACS+ 인증은 다음 오류 메시지와 함께 실패합니다.

"13017 네트워크 디바이스 또는 AAA 클라이언트에서 수신된 TACACS+ 패킷"




가능한 원인

- 가장 일반적인 이유는 스위치의 IP 주소가 ISE에서 네트워크 디바이스로 추가되지 않기 때문입니다(Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스) 아래).
- IP 주소 또는 범위가 TACACS+ 패킷을 전송하기 위해 Arista 스위치에서 사용 중인 소스 IP와 정확히 일치하는지 확인합니다.
- 스위치에서 관리 인터페이스를 사용하는 경우 정확한 IP(서브넷/범위가 아님)가 ISE에 추가되었는지 확인합니다.

솔루션

- ISE GUI에서 Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동합니다.
- Arista 스위치의 정확한 소스 IP 주소가 TACACS+ 통신에 사용되는지 확인합니다(대부분의 경우 관리 인터페이스 IP).
- 공유 암호를 지정합니다(Arista 스위치에 설정된 것과 일치해야 함).

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.