ISE를 사용하여 Palo Alto에서 TACACS+ 디바이스 관리 구성

목차

소개

이 문서에서는 Cisco ISE를 사용하는 Palo Alto의 TACACS+ 컨피그레이션에 대해 설명합니다.

사전 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ISE 및 TACACS+ 프로토콜.
- Palo Alto 방화벽

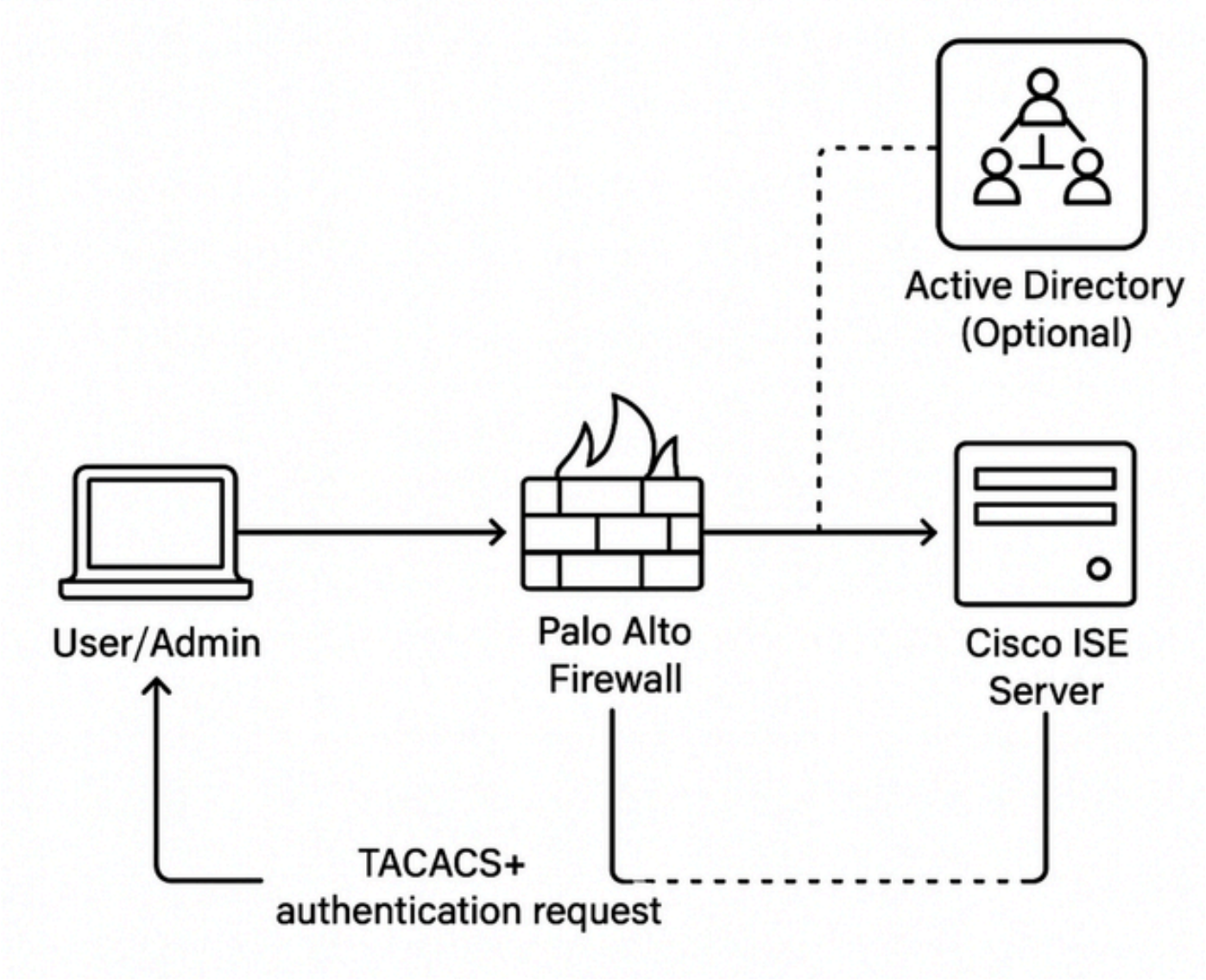
사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Palo Alto Firewall 버전 10.1.0
- 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



인증 흐름

1. 관리자가 Palo Alto 방화벽에 로그인합니다.

2. Palo Alto가 Cisco ISE에 TACACS+ 인증 요청을 보냅니다.

3. Cisco ISE:

- AD가 통합된 경우 AD에 인증 및 권한 부여를 쿼리합니다.
- AD가 없는 경우 로컬 ID 저장소 또는 정책을 사용합니다.
- Cisco ISE는 구성 된 정책을 기반으로 Palo Alto에 인증 응답을 전송 합니다.
- 관리자는 적절한 권한 레벨로 액세스 권한을 얻습니다.

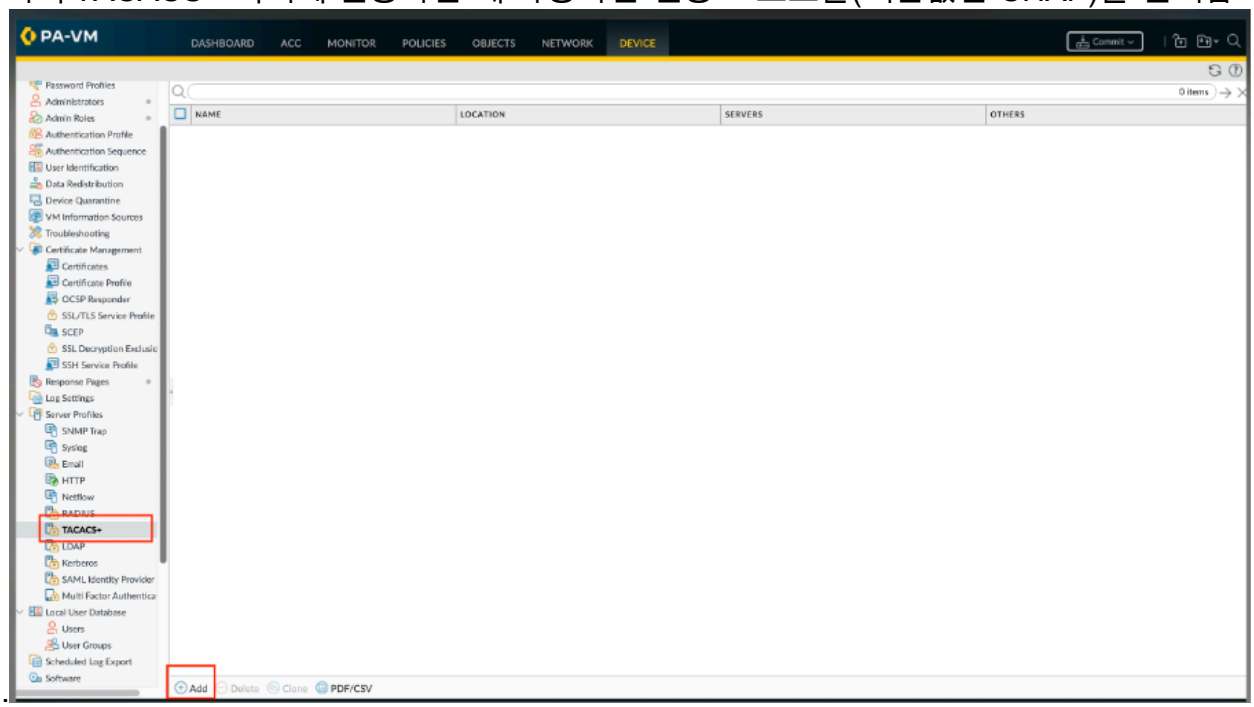
구성

섹션 1: TACACS+용 Palo Alto 방화벽 구성

1단계. TACACS+ 서버 프로파일을 추가합니다.

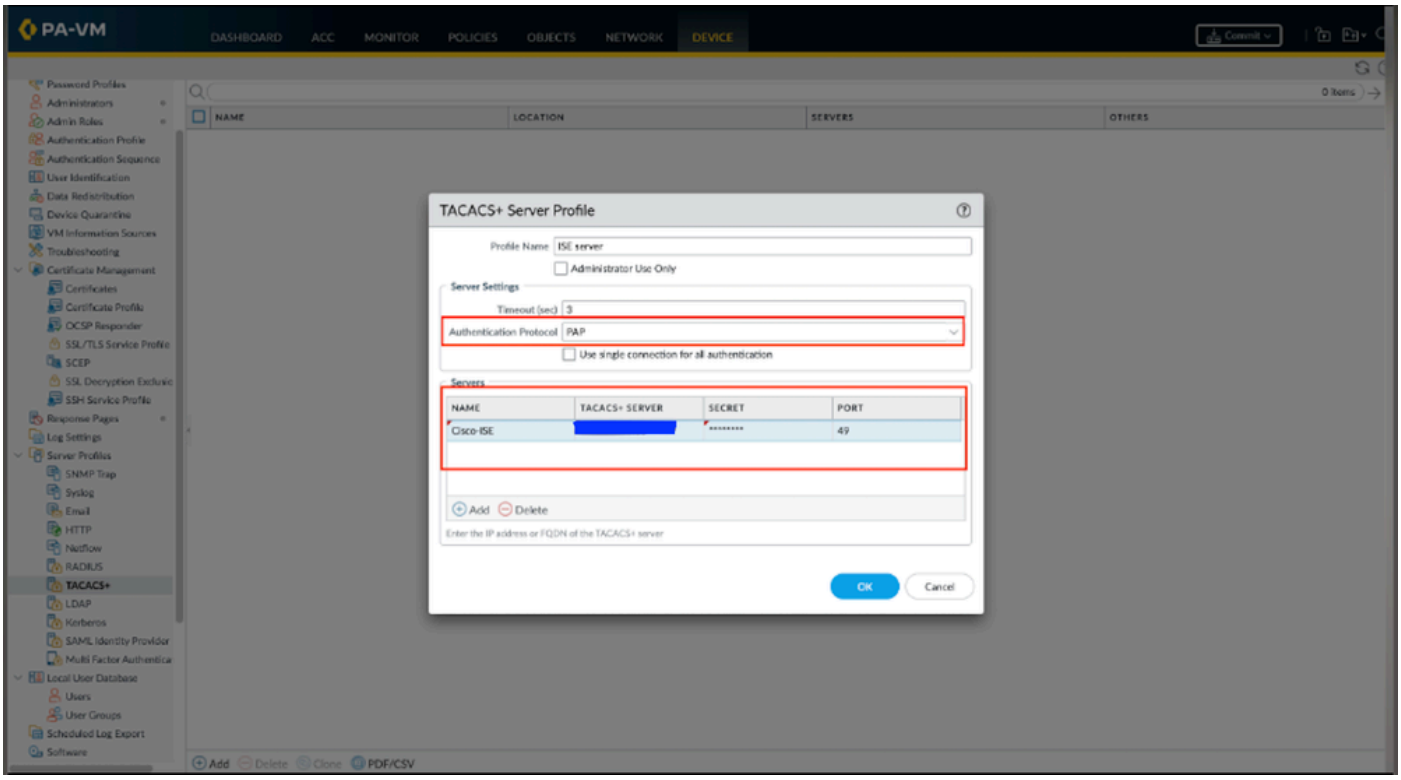
프로필은 방화벽이 TACACS+ 서버에 연결하는 방법을 정의합니다.

1. Device(디바이스) > Server Profiles(서버 프로필) > TACACS+ 또는 Panorama(파노라마) > Server Profiles(서버 프로필) > TACACS+ on Panorama(파노라마)를 선택하고 프로필을 추가합니다.
2. 서버 프로필을 식별하기 위한 프로필 이름을 입력합니다.
3. (선택 사항) 관리자 전용을 선택하여 관리자에 대한 액세스를 제한합니다.
4. 인증 요청이 시간 초과된 시간 초과 간격(초)을 입력합니다(기본값은 3; 범위는 1~20입니다.
5. 방화벽이 TACACS+ 서버에 인증하는 데 사용하는 인증 프로토콜(기본값은 CHAP)을 선택합니다.



6. 각 TACACS+ 서버를 추가하고 다음 단계를 수행합니다.
    1. 서버를 식별하기 위한 이름
    2. TACACS+ 서버 IP 주소 또는 FQDN입니다. FQDN 주소 객체를 사용하여 서버를 식별하고 그 후에 주소를 변경한 경우 새 서버 주소의 변경 사항을 커밋해야 적용됩니다.
    3. 사용자 이름 및 비밀번호를 암호화하기 위한 Secret 및 Confirm Secret
    4. 인증 요청을 위한 서버 포트(기본값은 49)입니다. OK(확인)를 클릭하여 서버 프로필을 저장합니다.

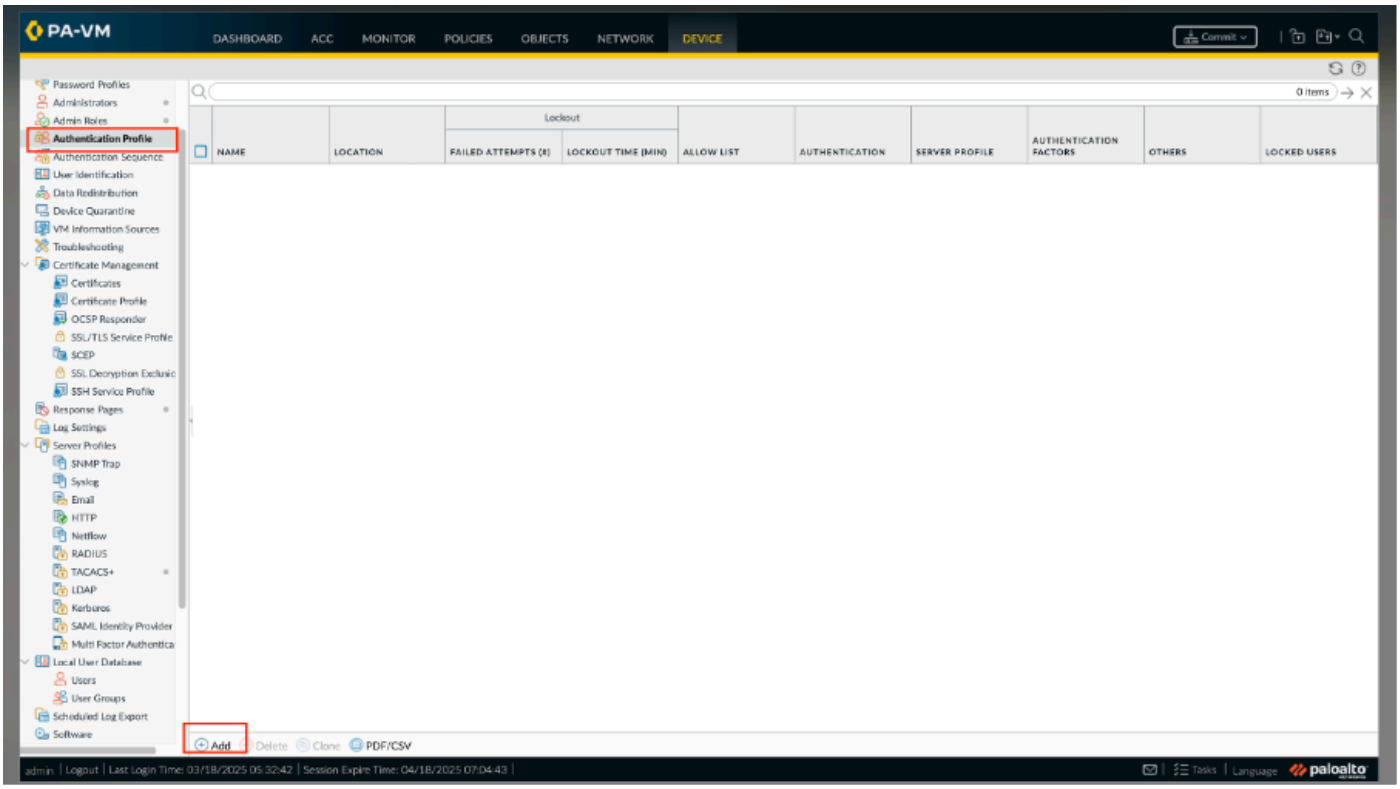
7. 서버 프로파일을 저장하려면 확인을 클릭합니다.

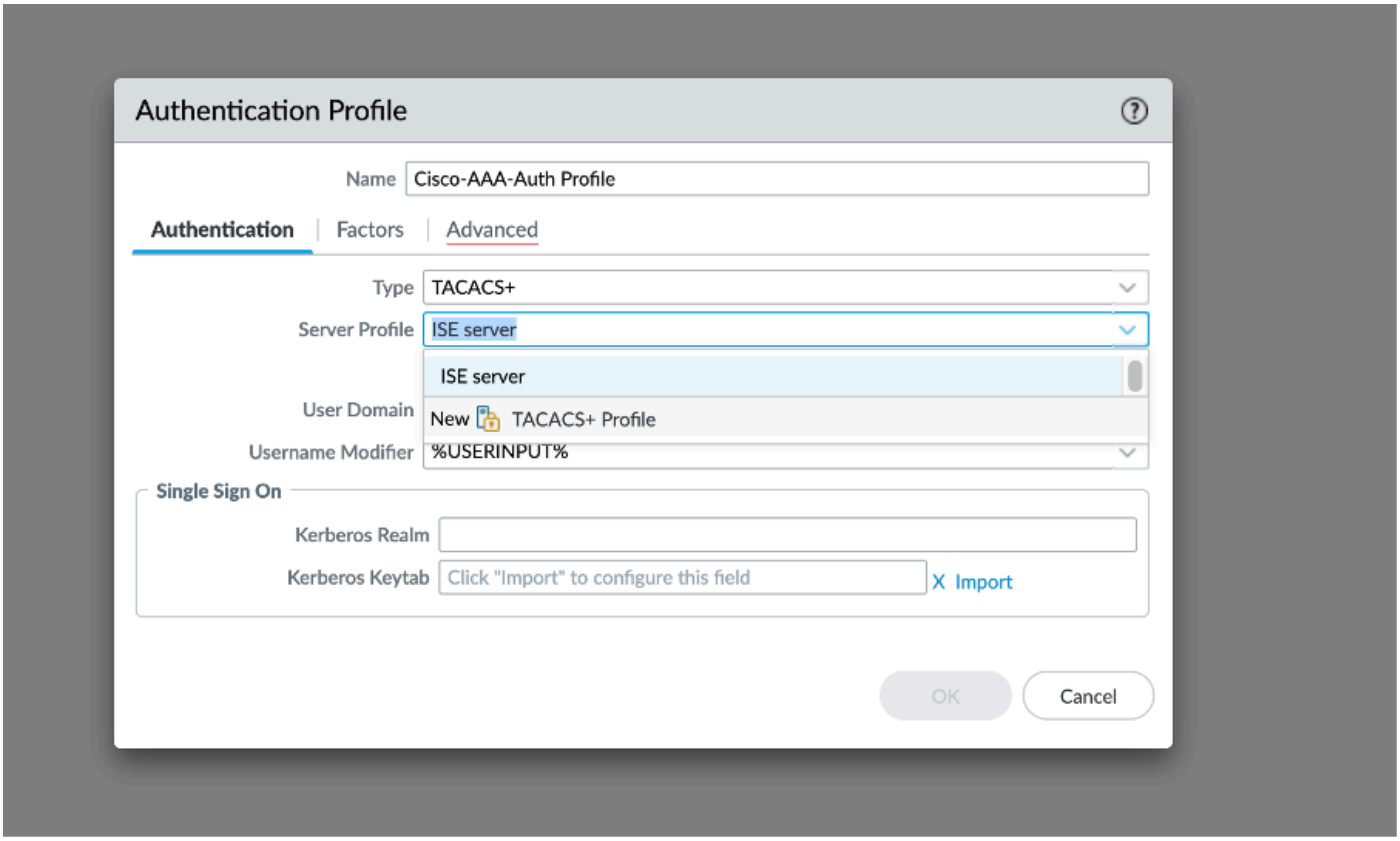


2단계. TACACS+ 서버 프로파일을 인증 프로파일에 할당합니다.

인증 프로파일은 사용자 집합에 공통된 인증 설정을 정의합니다.

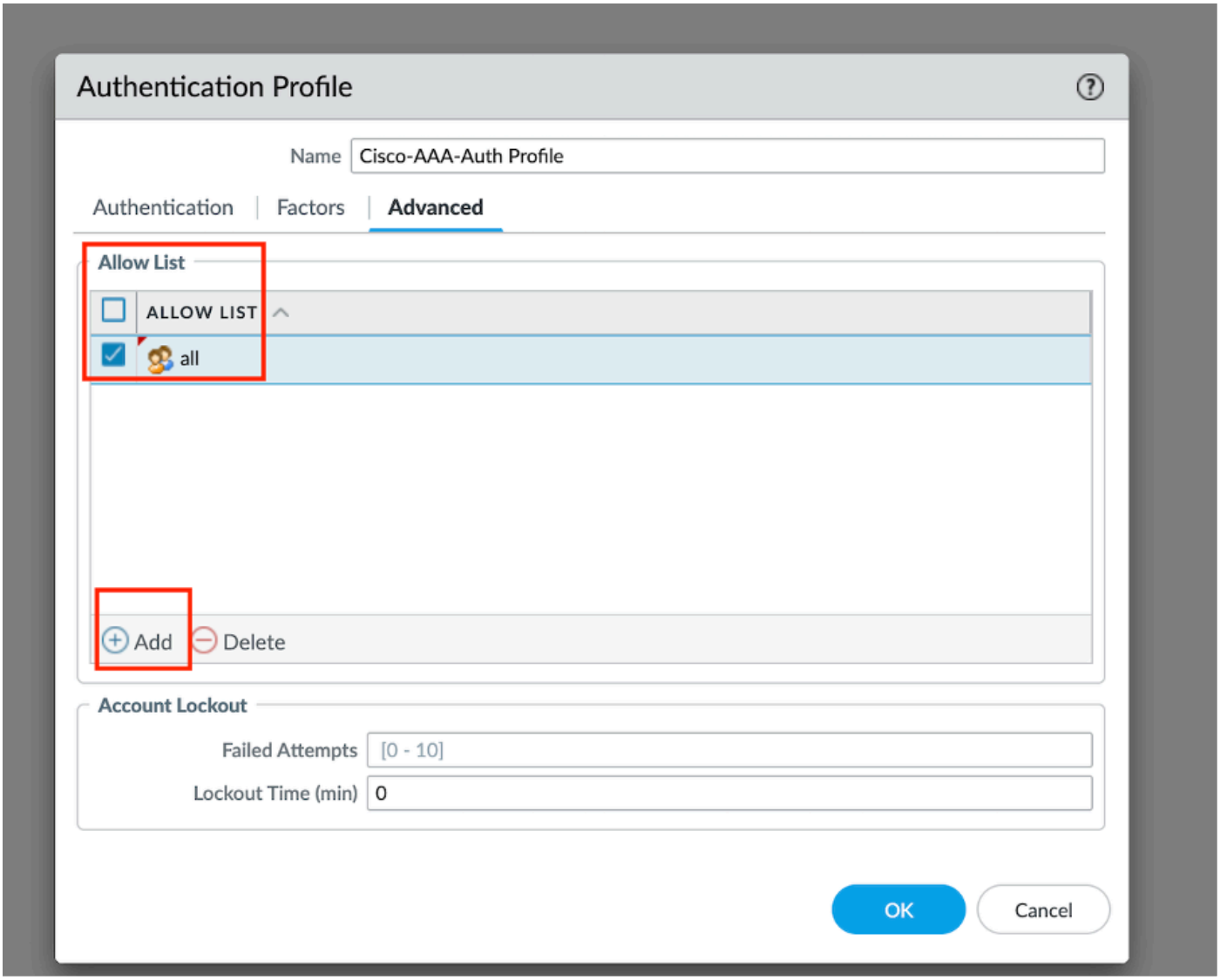
1. Device(디바이스) > Authentication Profile(인증 프로파일)을 선택하고 Add a profile(프로파일 추가)을 선택합니다.
    1. 프로필을 식별할 이름 입력
    2. Type(유형)을 TACACS+로 설정합니다.
    3. 구성한 서버 프로필을 선택합니다.
    4. Retrieve user group from TACACS+(TACACS+에서 사용자 그룹 검색)를 선택하여 TACACS+ 서버에 정의된 VSA에서 사용자 그룹 정보를 수집합니다.





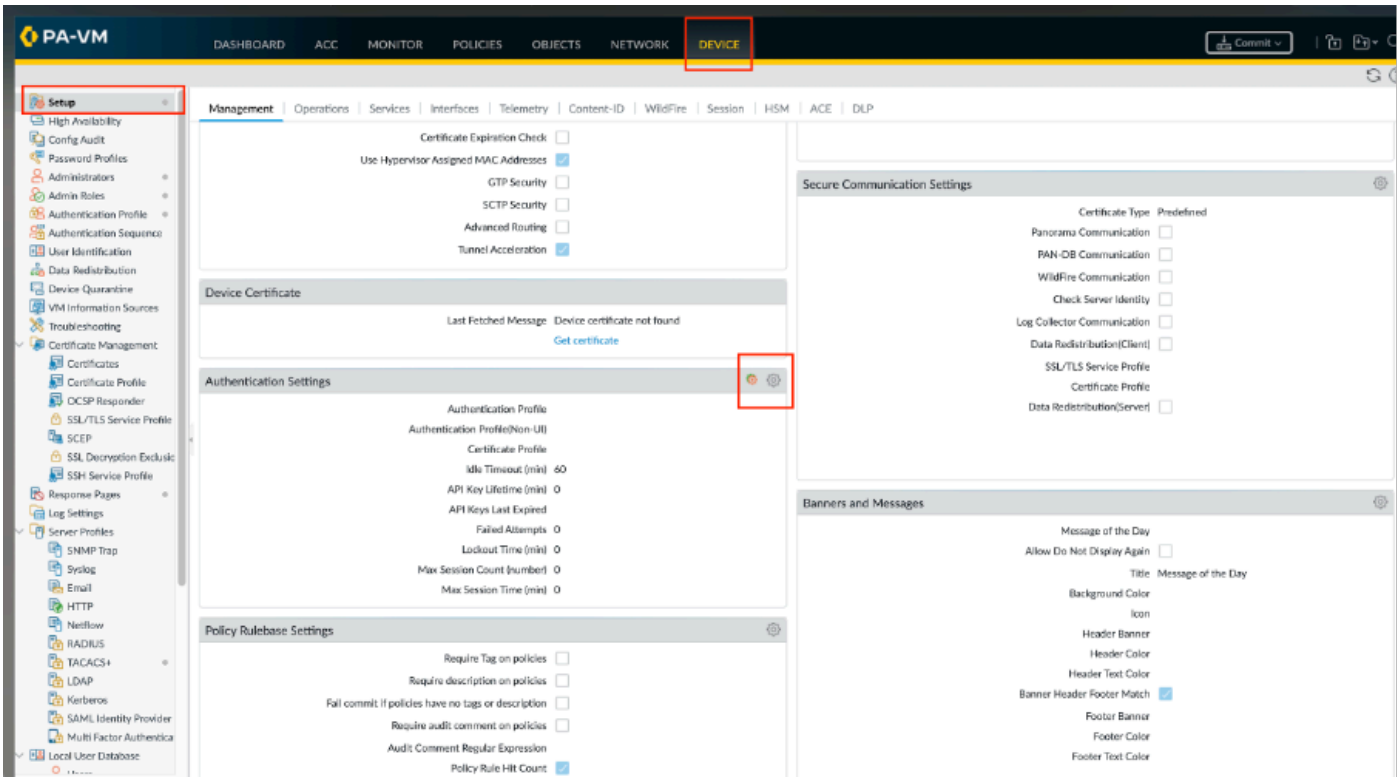
방화벽은 인증 프로필의 Allow List(허용 목록)에서 지정하는 그룹을 사용하여 그룹 정보를 확인합니다.

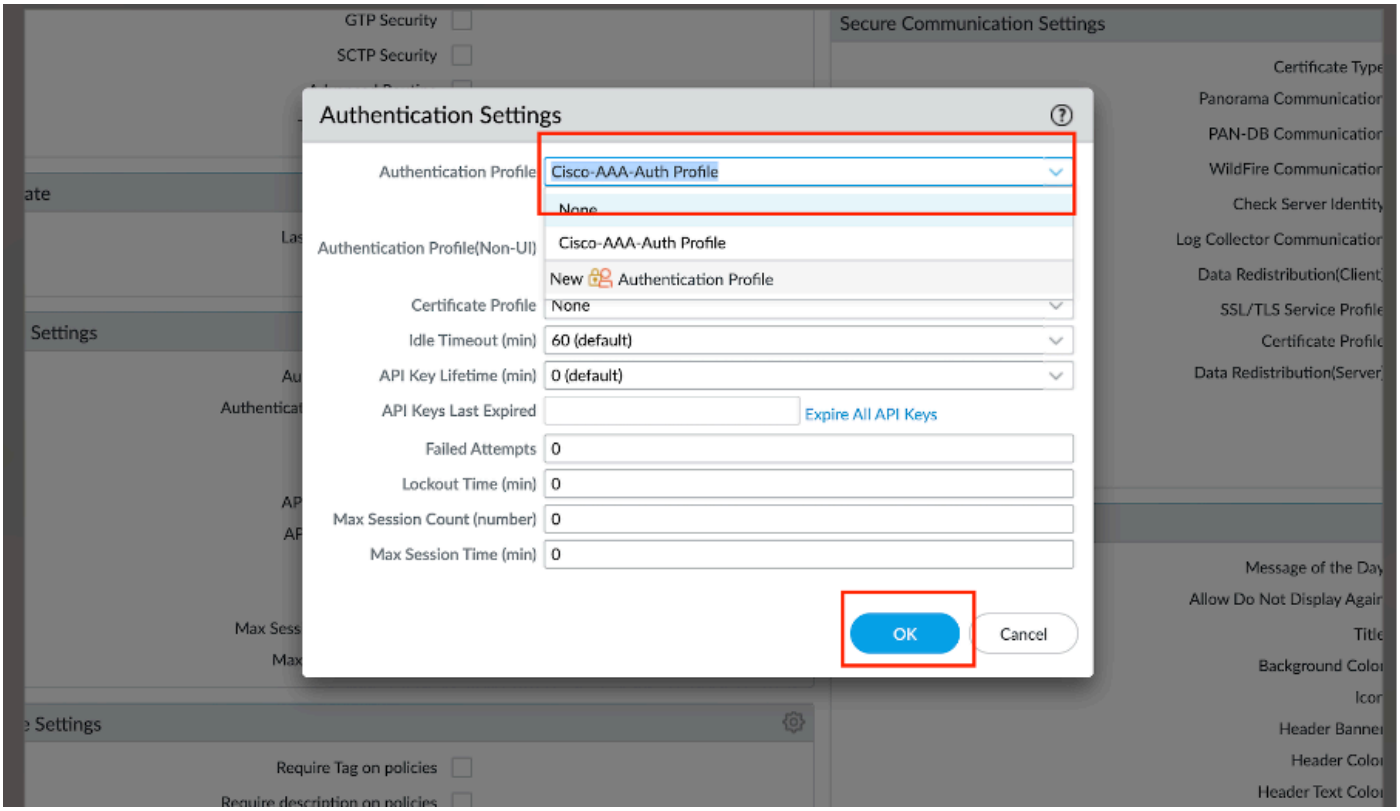
1. Advanced(고급)를 선택하고 Allow List(허용 목록)에서 이 인증 프로필로 인증할 수 있는 사용자 및 그룹을 추가합니다.
2. OK(확인)를 클릭하여 인증 프로필을 저장합니다.



3단계. 모든 관리자에 대해 인증 프로필을 사용하도록 방화벽을 구성합니다.

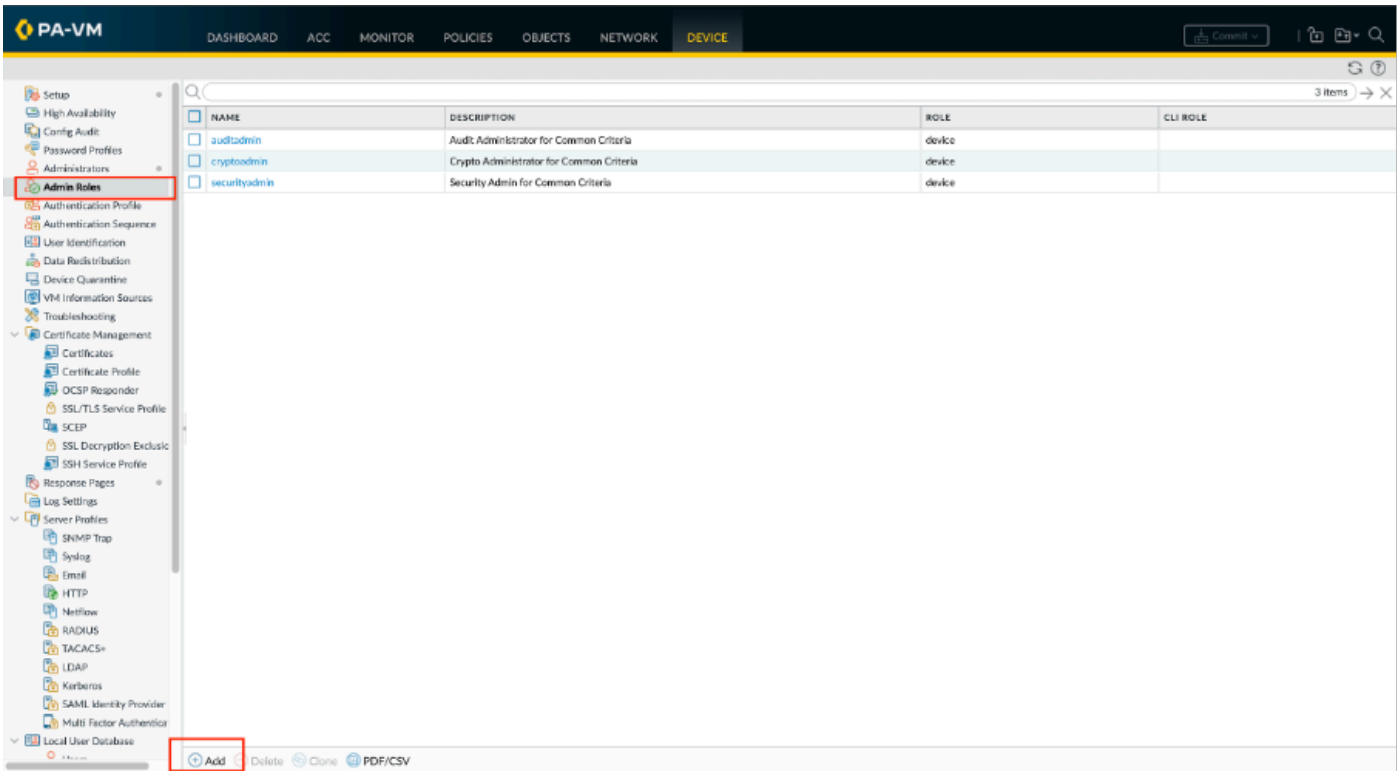
1. Device(디바이스) > Setup(설정) > Management(관리)를 선택하고 Authentication Settings(인증 설정)를 편집합니다.
2. 구성한 인증 프로파일을 선택하고 확인을 클릭합니다.



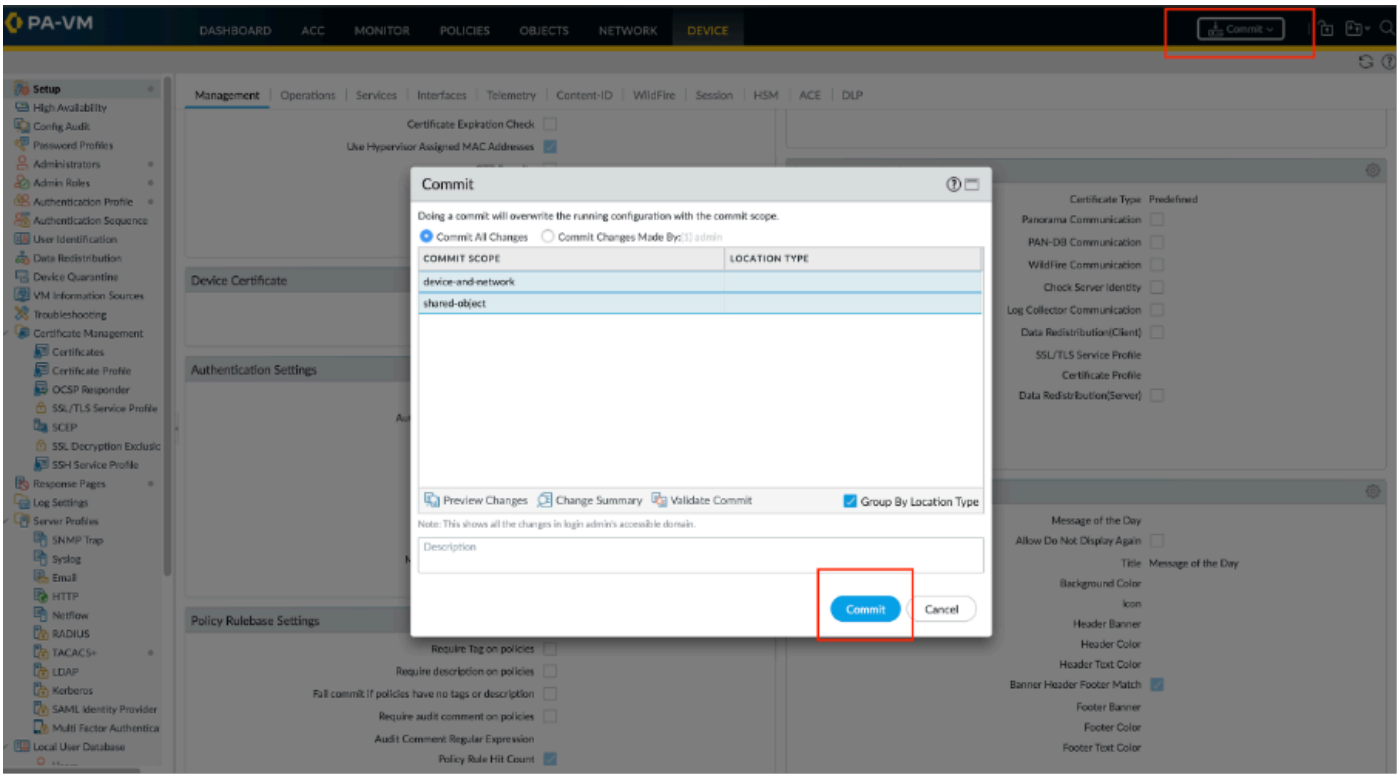


4단계. 관리자 역할 프로필을 구성합니다.

Device(디바이스) > Admin Roles(관리자 역할)를 선택하고 Add(추가)를 클릭합니다. 역할을 식별하는 이름을 입력합니다.



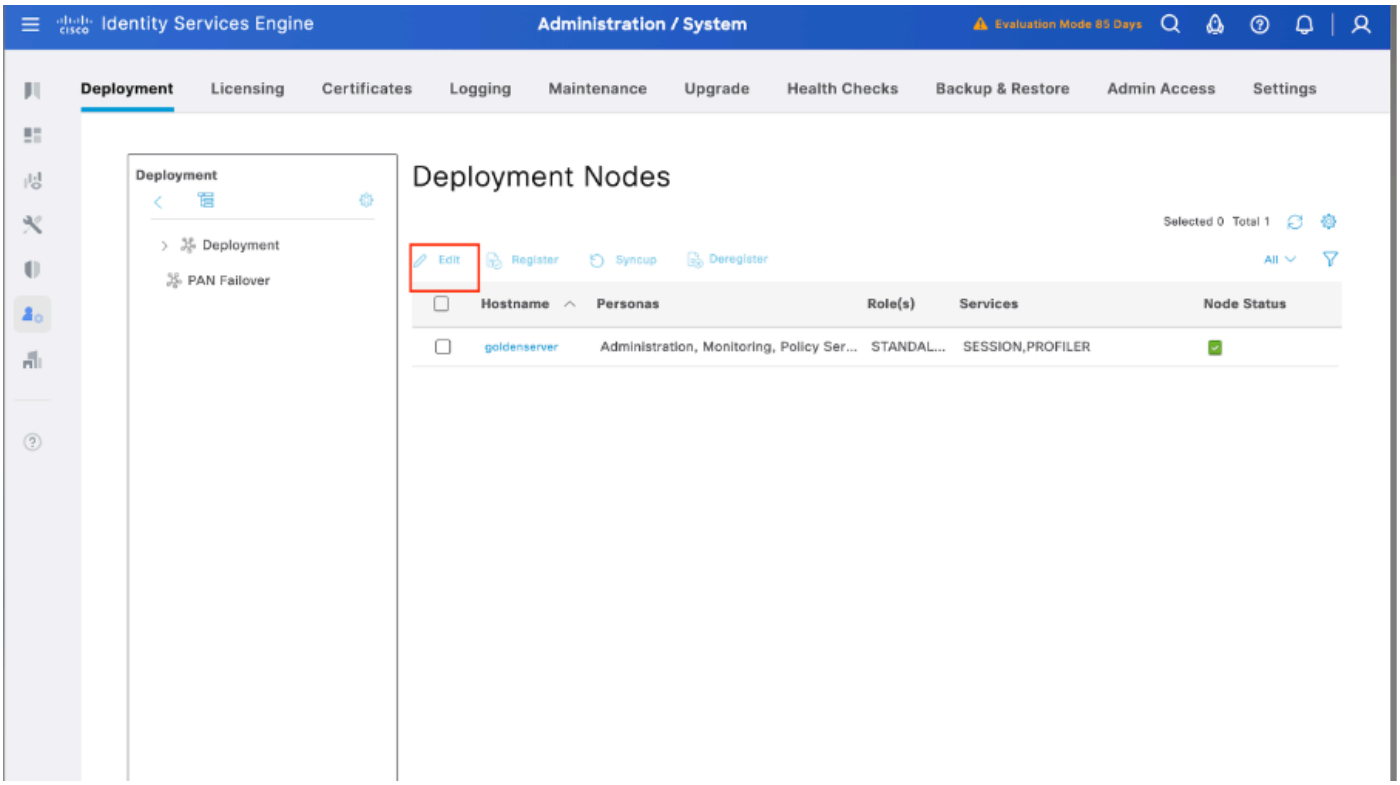
5단계. 변경 사항을 커밋하여 방화벽에서 활성화합니다.



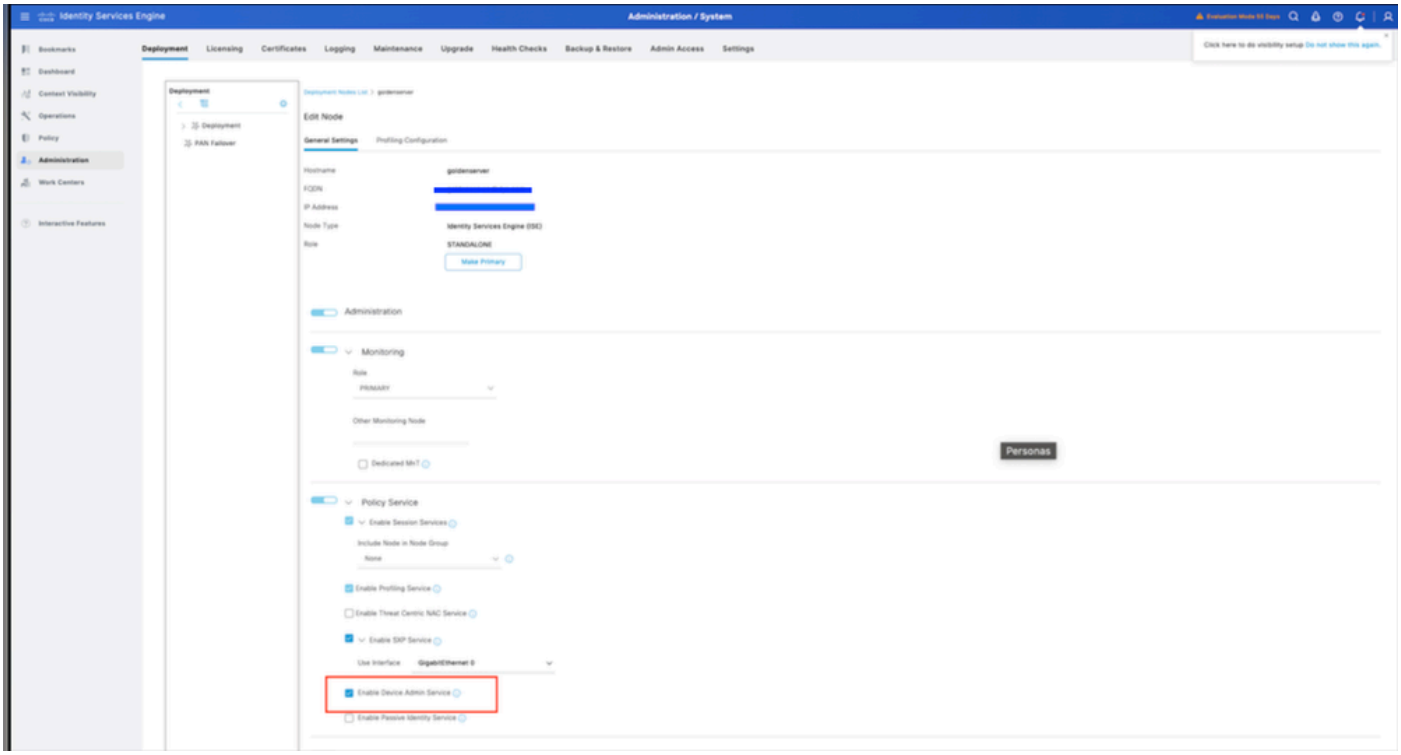
섹션 2: ISE의 TACACS+ 컨피그레이션

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(관리) > System(시스템) > Deployment(구축)로 이동하여 ISE가 TACACS+ 인증을 처리하는 해당 노드를 선택하고 Edit(편집)를 클릭하여 해당 컨피

그레이션을 검토합니다.



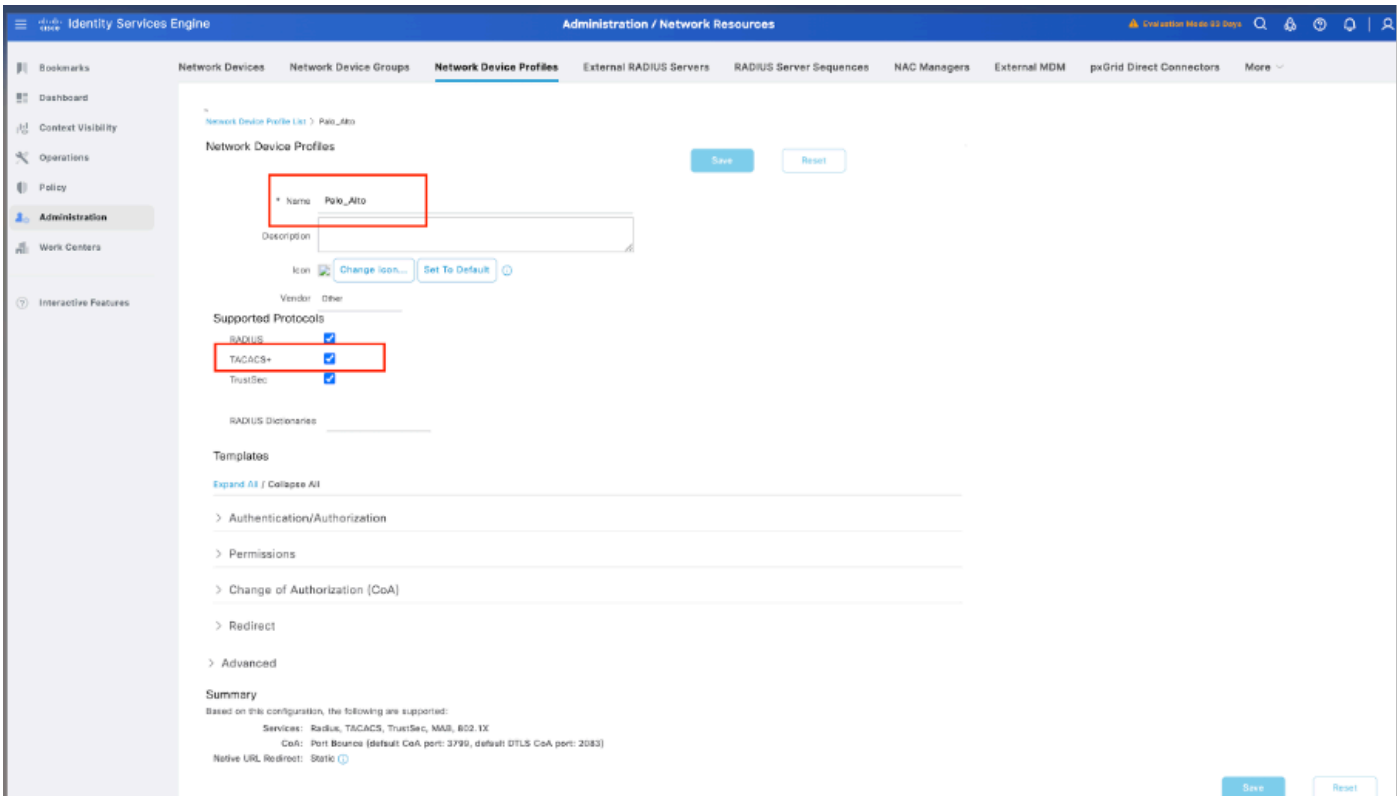
2단계. 아래로 스크롤하여 Device Administration Service 기능을 찾습니다. 이 기능을 활성화하려면 구축에서 사용 가능한 TACACS+ 라이센스와 함께 정책 서비스 페르소나가 노드에서 활성화되어야 합니다. 확인란을 선택하여 기능을 활성화한 다음 컨피그레이션을 저장합니다.



3단계. Cisco ISE용 Palo Alto 네트워크 디바이스 프로필을 구성합니다.

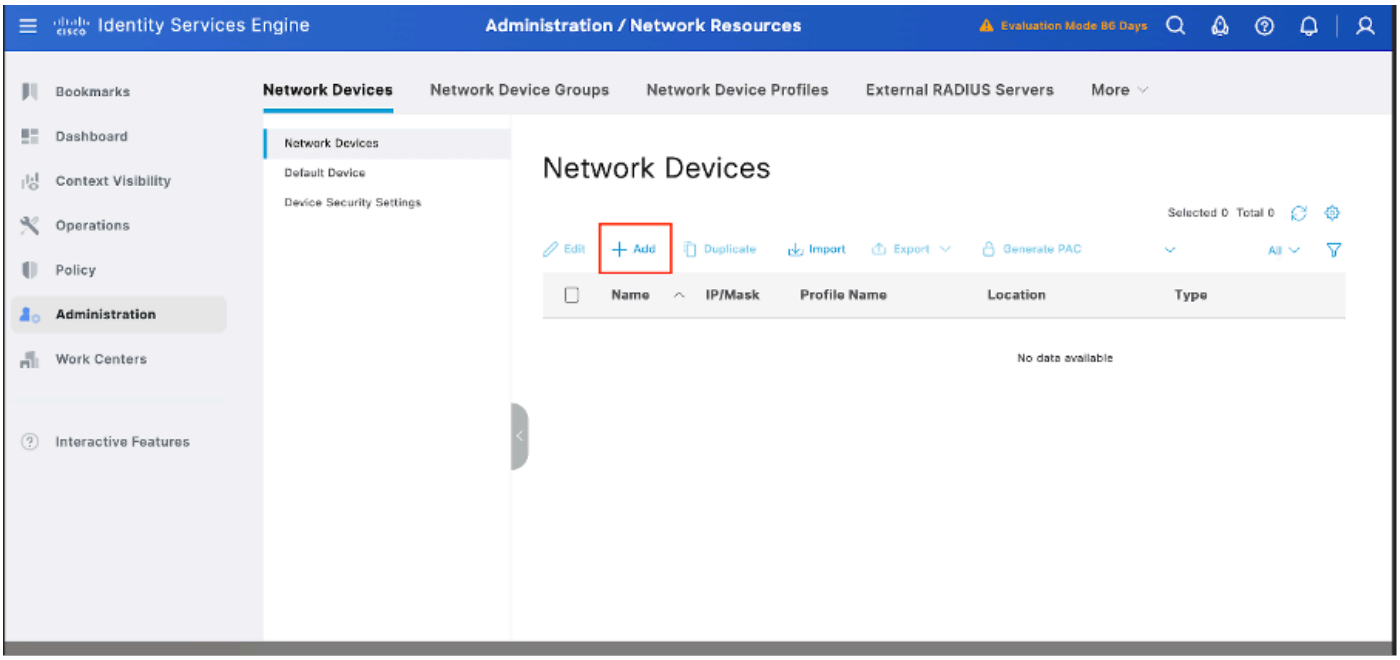
Administration(관리) > Network Resources(네트워크 리소스) > Network device profile(네트워크 디

바이스 프로파일)로 이동합니다. Add(추가)를 클릭하고 이름을 언급하며(Palo Alto) 지원되는 프로토콜에서 TACACS+를 활성화합니다.



4단계. Palo Alto를 네트워크 디바이스로 추가합니다.

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



2. 추가를 누르고 다음 상세내역을 입력합니다.

이름: 팔로알토

IP 주소: <Palo-Alto IP>

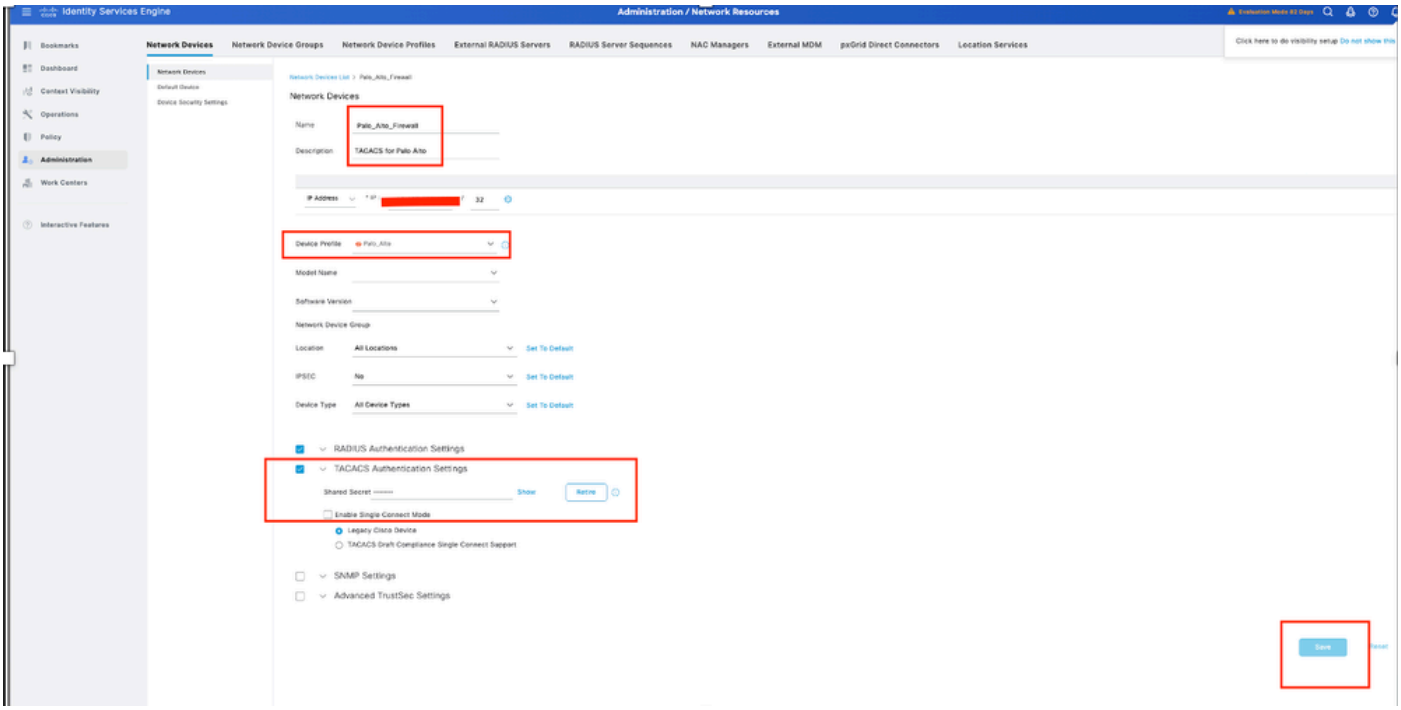
네트워크 장치 프로파일: Palo Alto 선택

TACACS 인증 설정:

TACACS+ 인증 활성화

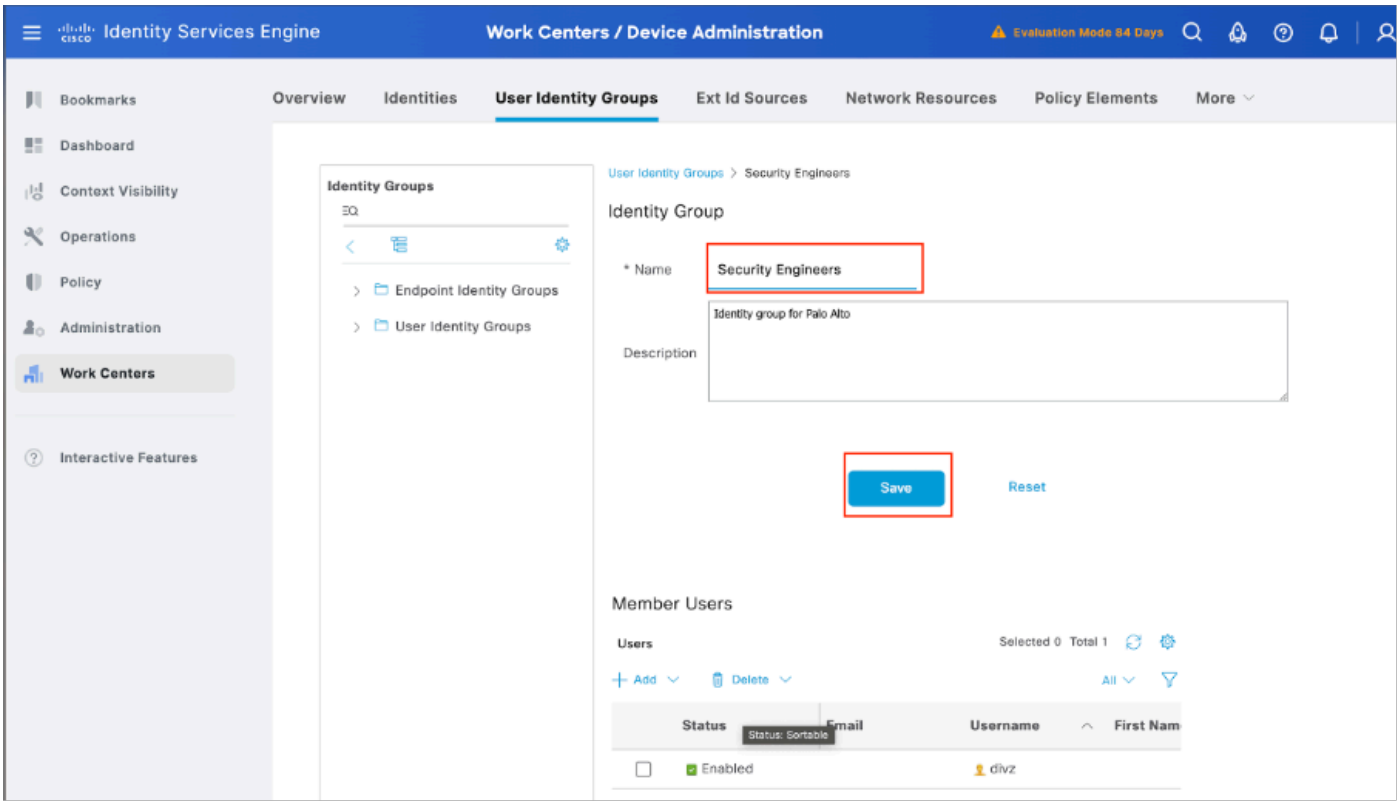
공유 암호 입력(Palo Alto 컨피그레이션과 일치해야 함)

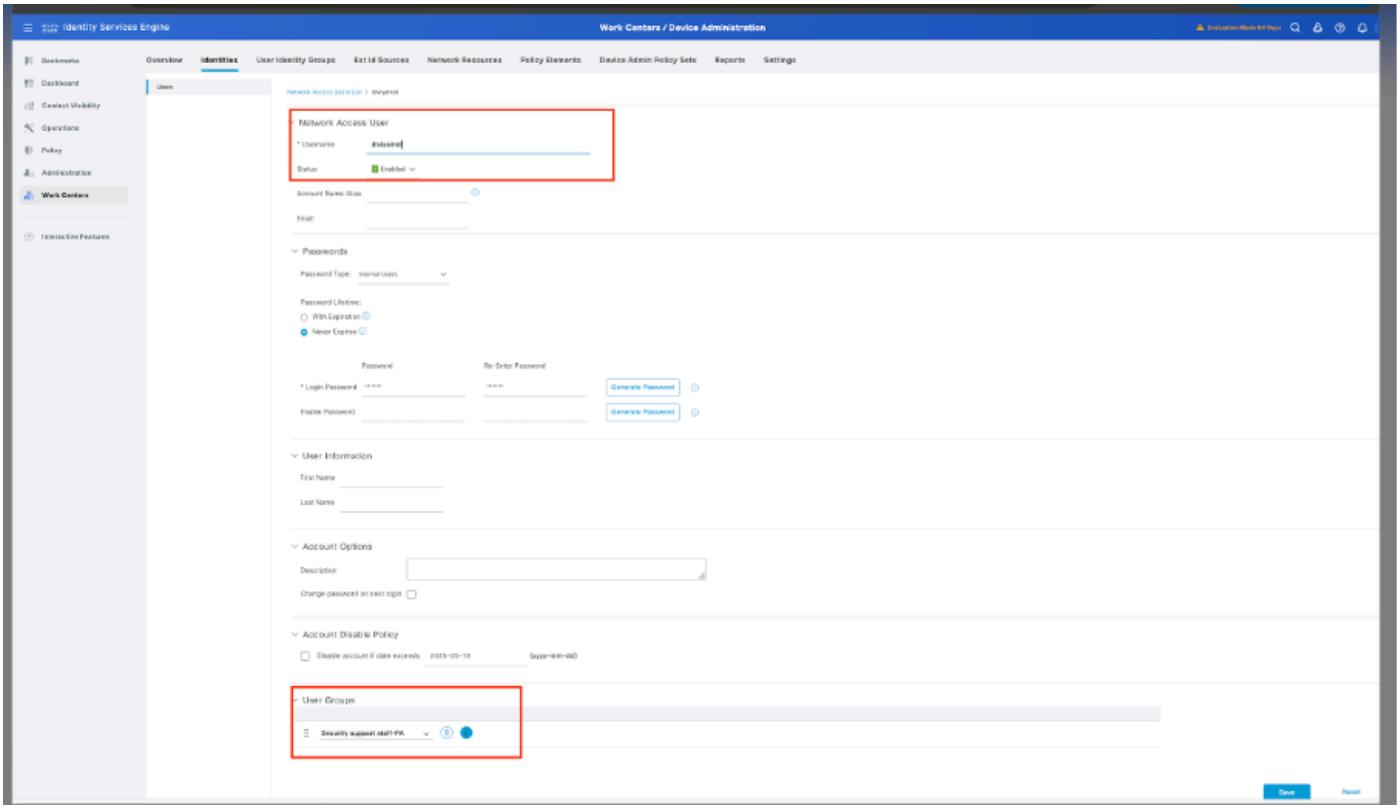
저장을 클릭합니다.

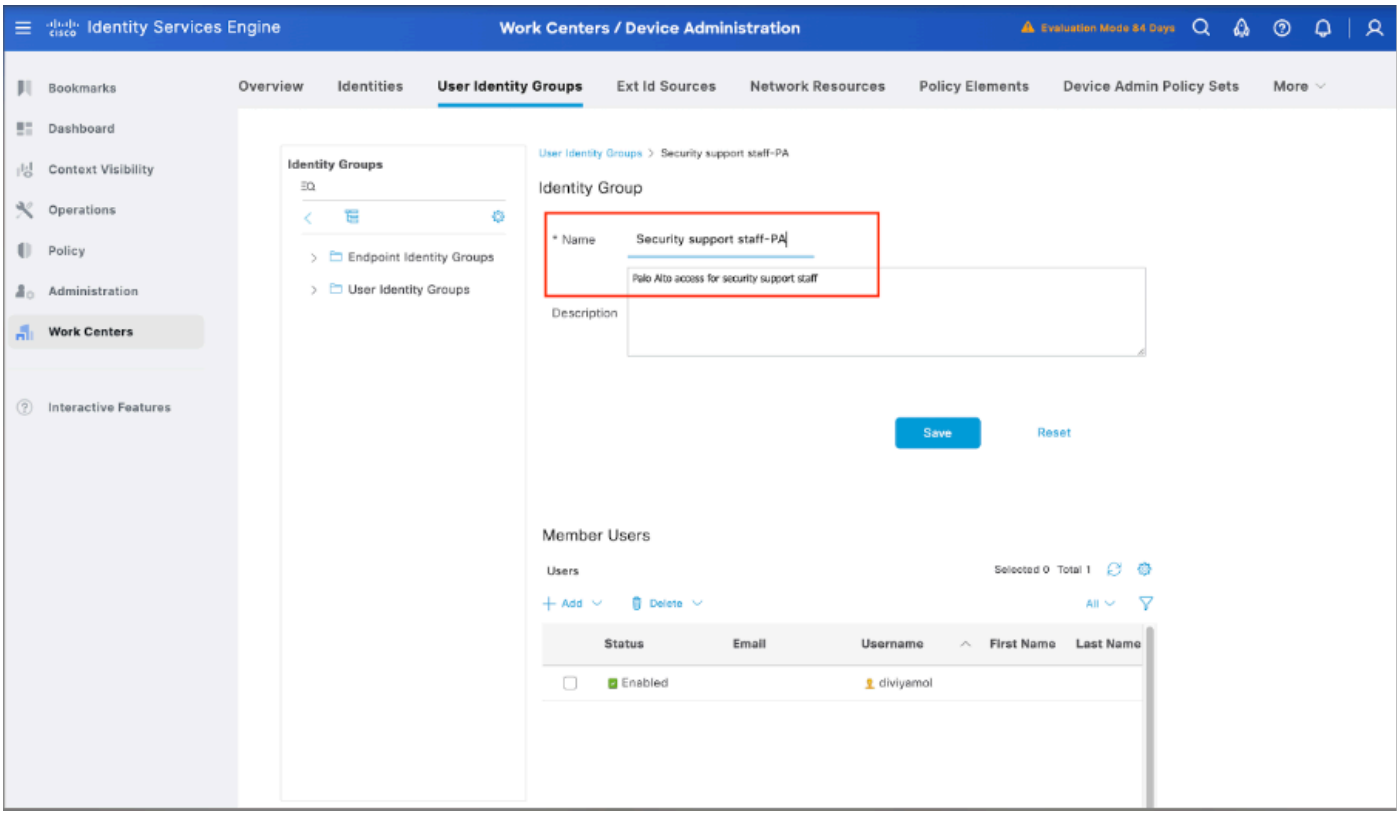


5단계. 사용자 ID 그룹을 생성합니다.

Work Centers(작업 센터) > Device Administration(디바이스 관리) > User Identity Groups(사용자 ID 그룹)로 이동한 다음 Add(추가)를 클릭하고 사용자 그룹의 이름을 지정합니다.


Identity Services Engine
Work Centers / Device Administration
Evaluation Mode 84 Days
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Features
Overview
Identities
User Identity Groups
Ext Id Sources
Network Resources
Policy Elements
More
Identity Groups
Endpoint Identity Groups
User Identity Groups
User Identity Groups > Security Engineers
Identity Group
* Name
Security Engineers
Description
Identity group for Palo Alto
Save
Reset
Member Users
Users
Selected 0 Total 1
Add
Delete
All
Status
Email
Username
First Nam
Status: Sortable
Enabled
divz

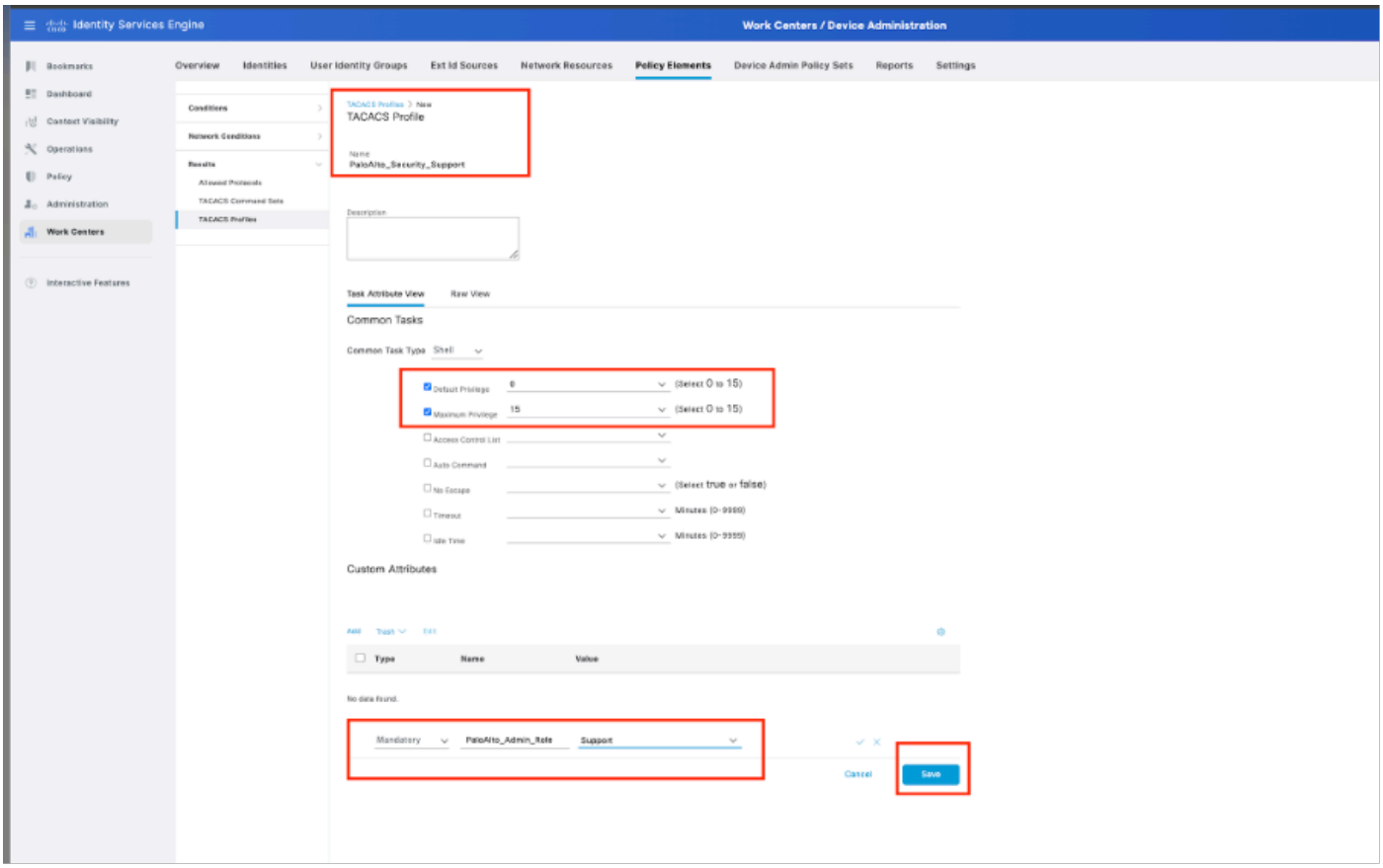

Identity Services Engine
Work Centers / Device Administration
Network Access User
Passwords
User Information
Account Options
Account Disable Policy
User Groups

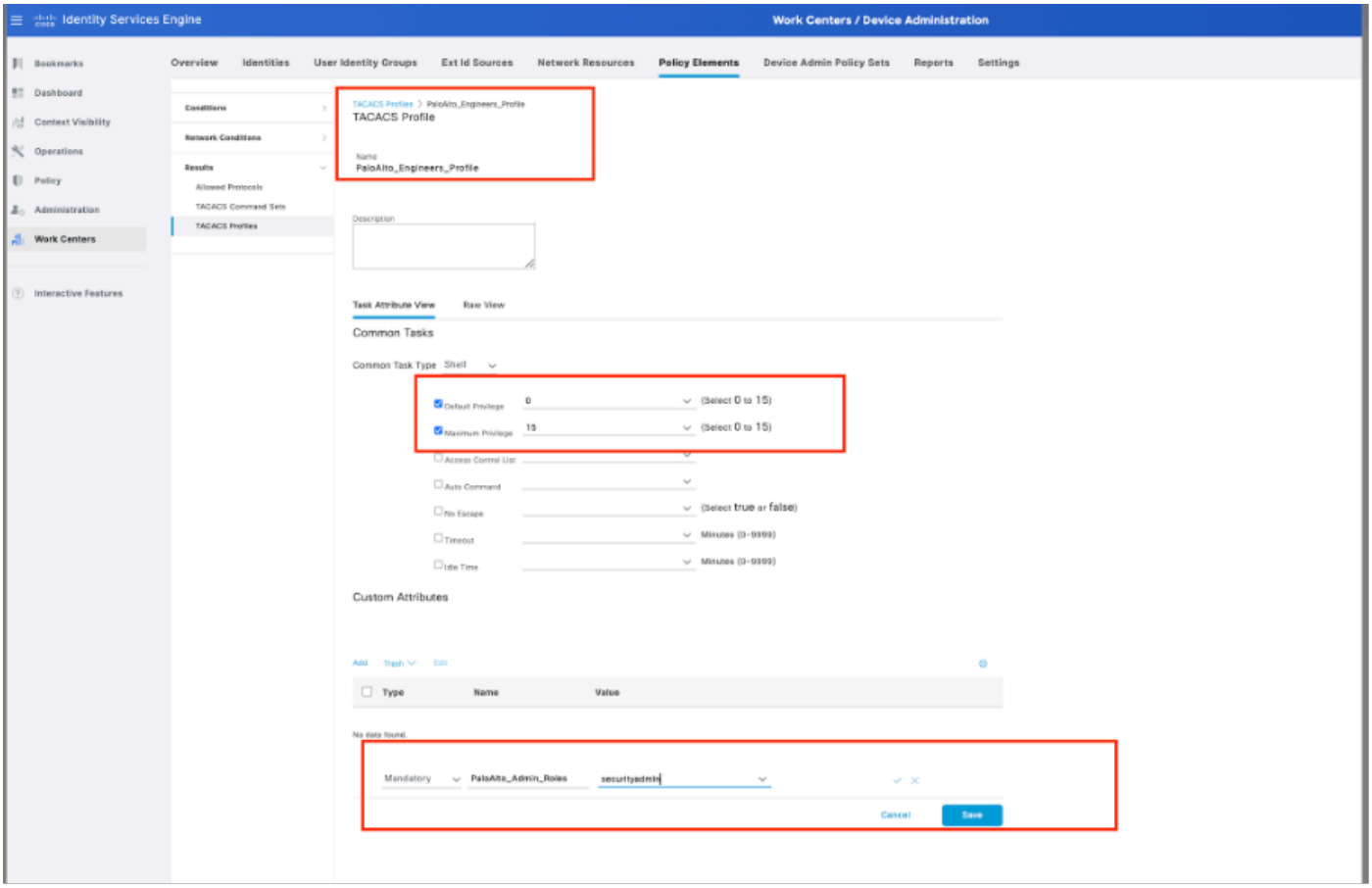


6단계. TACACS 프로파일을 구성합니다.

다음으로 TACACS 프로파일을 구성합니다. 여기서 Privilege Level(권한 레벨) 및 Timeout(시간 제한) 설정과 같은 설정을 구성할 수 있습니다. Work Centers(작업 센터) > Device Administration(디바이스 관리) -> Policy Elements(정책 요소) -> Results(결과) -> TACACS Profiles(TACACS 프로필)로 이동합니다.

Add(추가)를 클릭하여 새 TACACS 프로필을 생성합니다. 프로필에 올바른 이름을 지정하십시오.





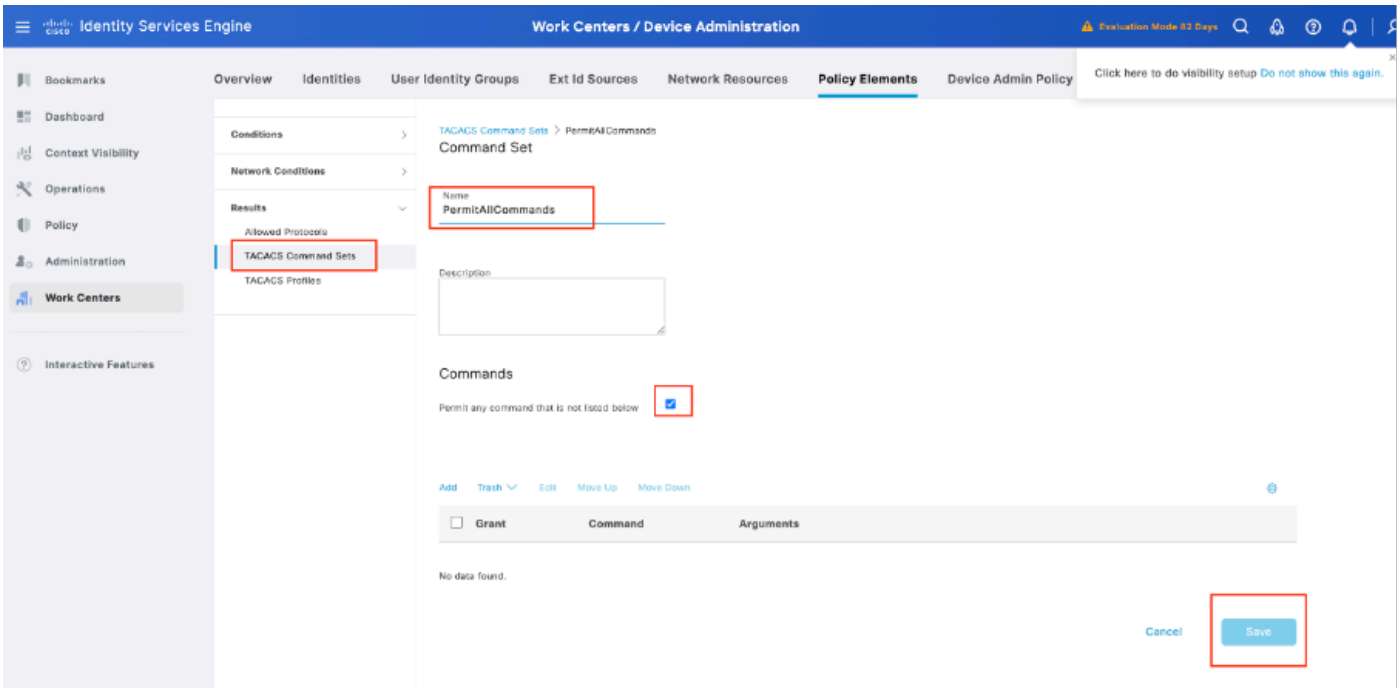
6단계. TACACS 명령 집합을 구성합니다.

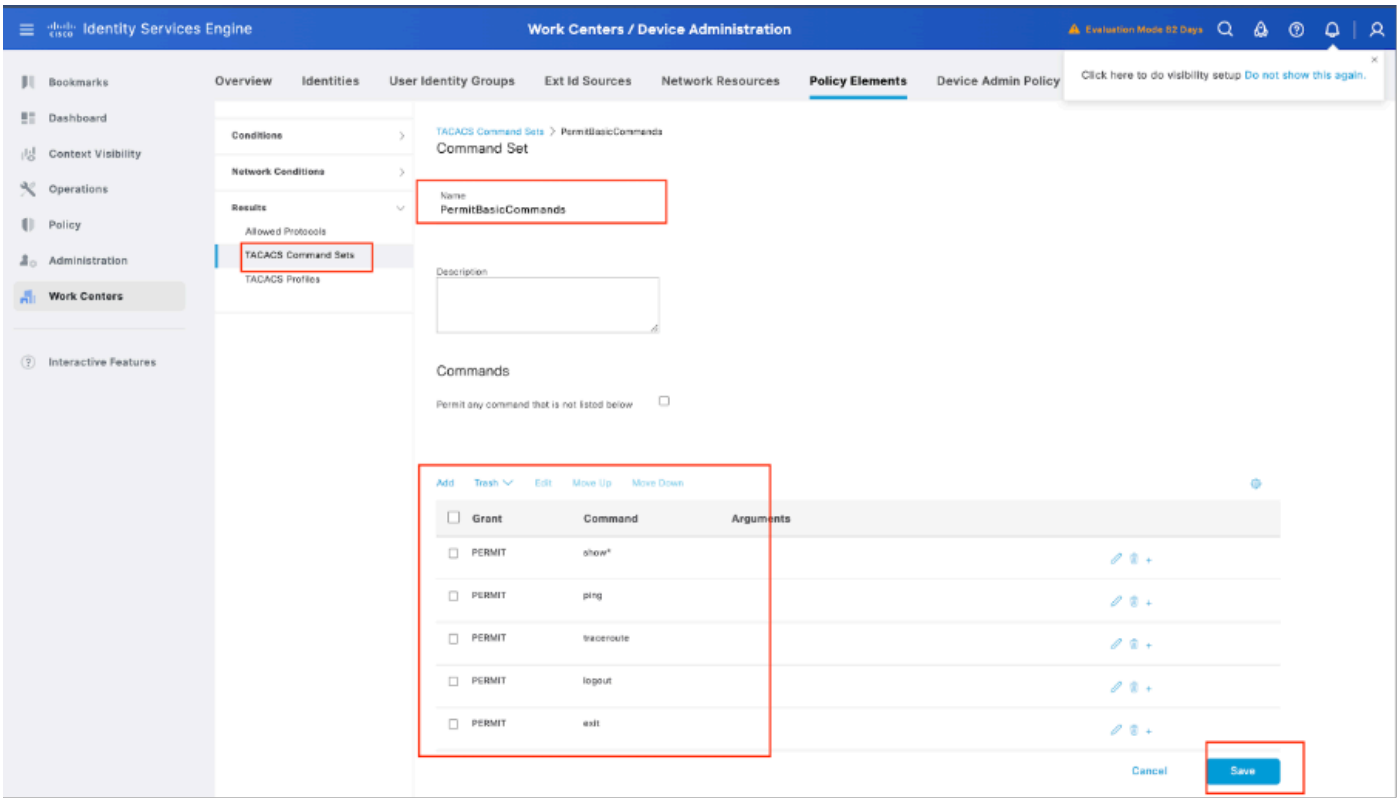
이제 어떤 명령을 사용자가 사용할 수 있는지 구성해야 합니다. 사용 가능한 모든 명령에 대한 액세

스 권한을 제공하는 권한 레벨 15를 이 두 가지 사용 사례에 모두 부여할 수 있으므로 TACACS 명령 집합을 사용하여 사용 가능한 명령을 제한합니다.

Work Centers(작업 센터) > Device Administration(디바이스 관리) > Policy Elements(정책 요소) >Results(결과) -> TACACS Command Sets(TACACS 명령 집합)로 이동합니다. Add(추가)를 클릭하여 새 TACACS 명령 집합을 생성하고 이름을 PermitAllCommands로 지정합니다. 보안 지원을 위해 이 TACACS 명령 집합을 적용합니다.

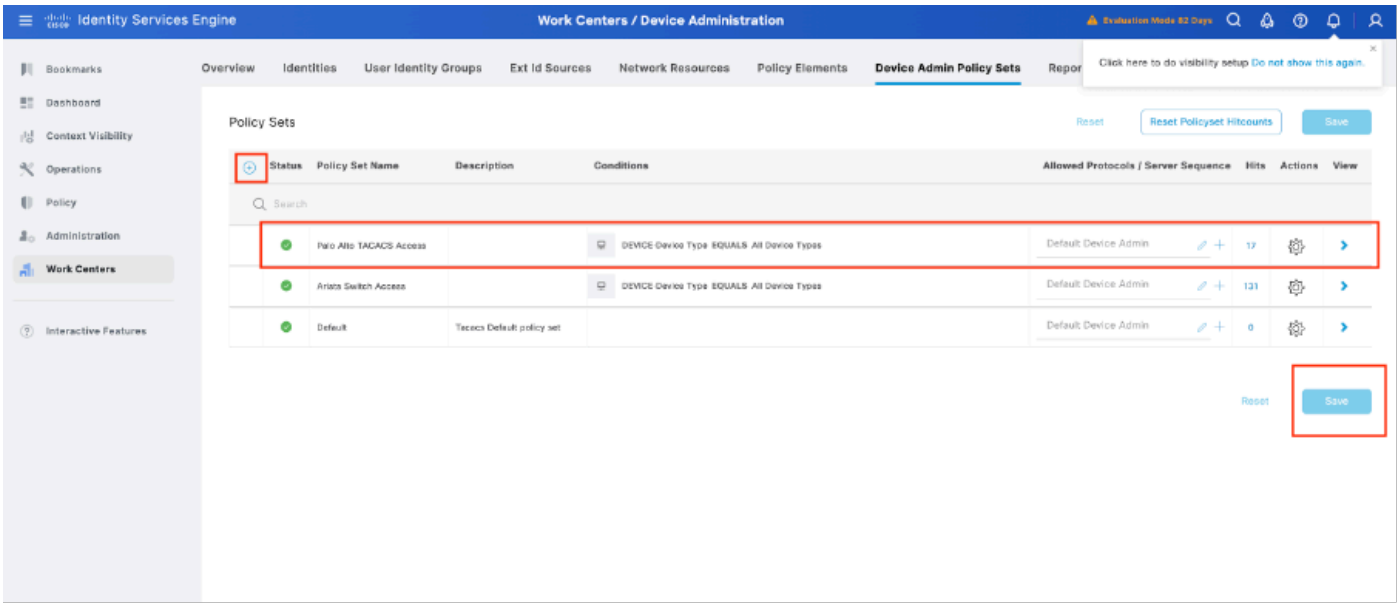
이 TACACS 명령 집합에서 구성해야 할 유일한 사항은 아래에 나열되지 않은 모든 명령을 허용하는 확인란을 선택하는 것입니다.



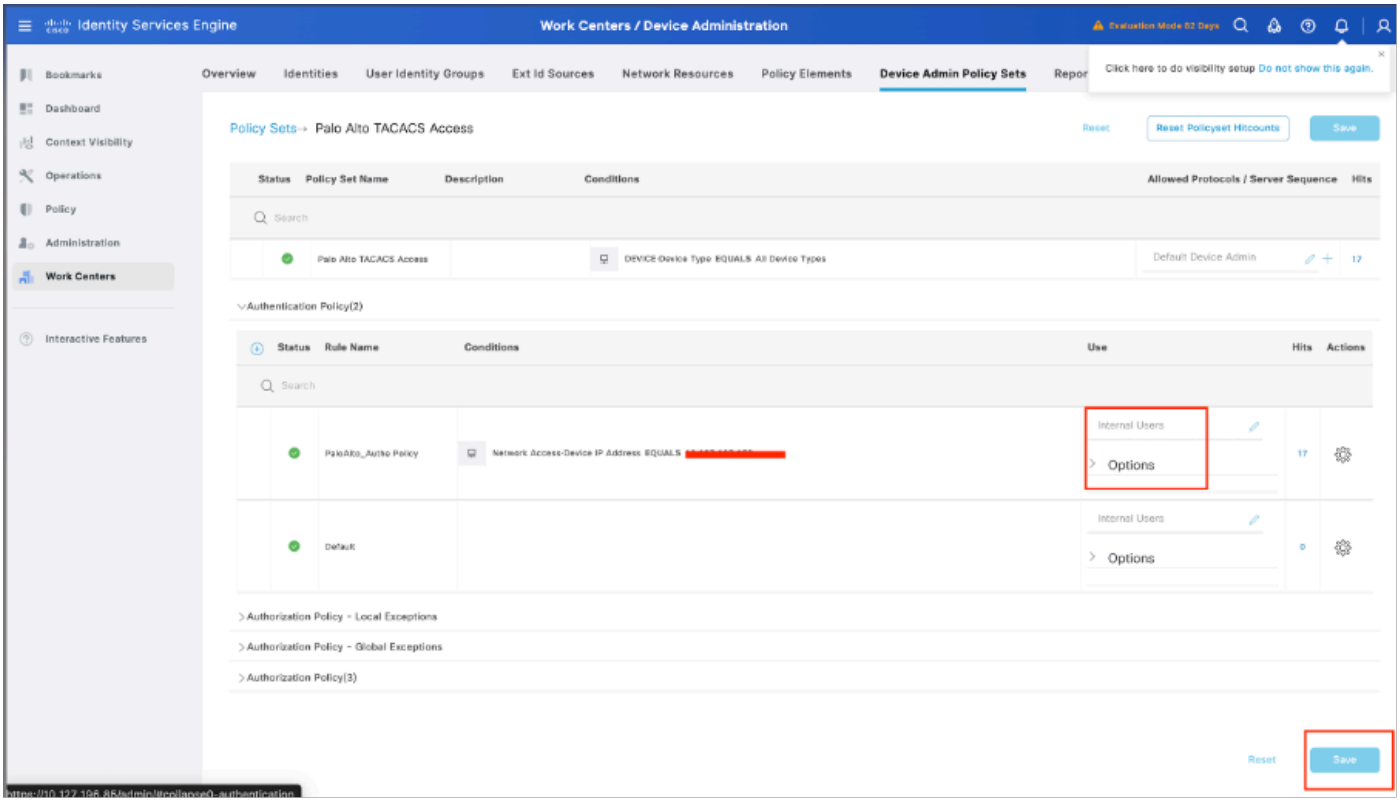


7단계. Palo Alto에 사용할 Device Admin Policy Set(디바이스 관리 정책 집합)를 생성하고 Work Centers(작업 센터) > Device Administration(디바이스 관리) > Device Admin Policy Sets(디바이스 관리 정책 집합) 메뉴를 탐색한 다음 Add(추가) + 아이콘을 클릭합니다.

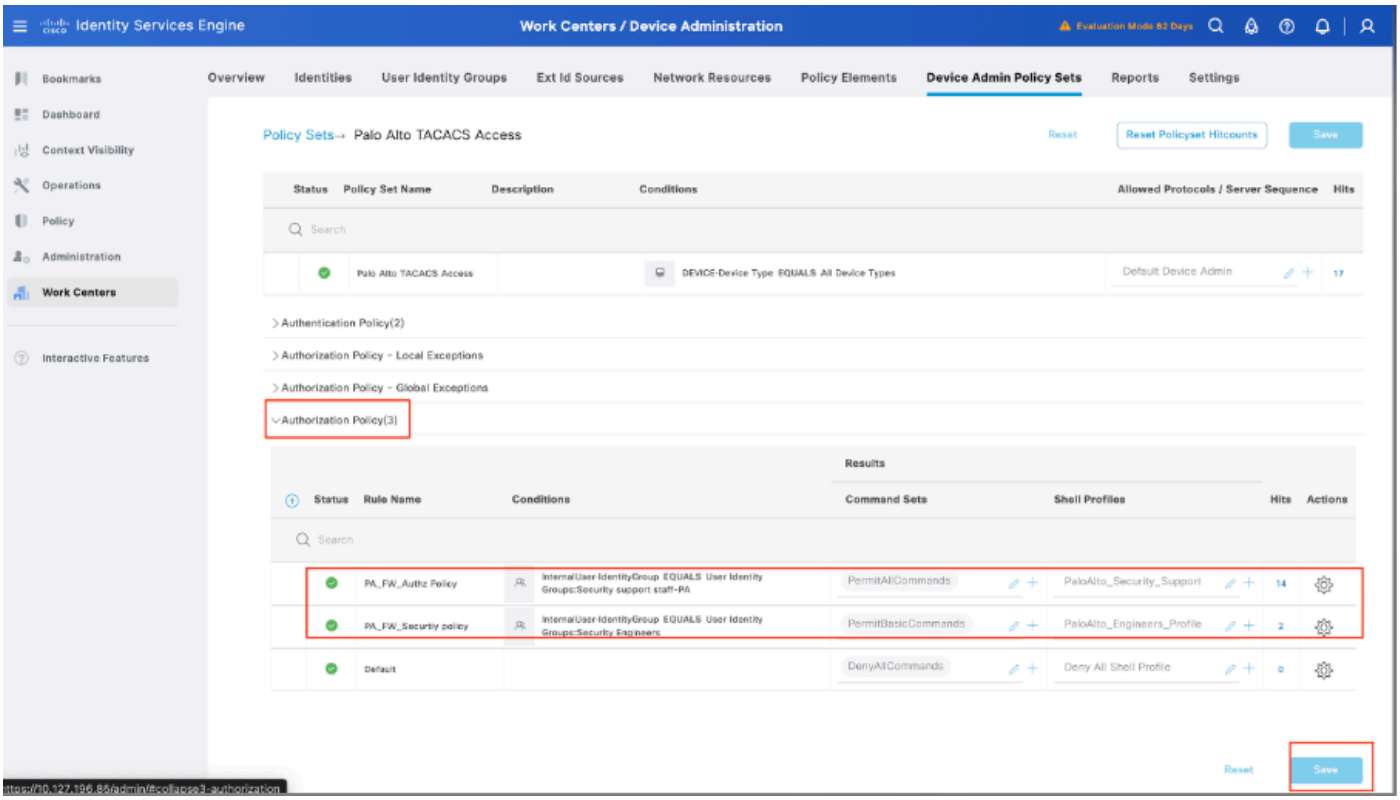
8단계. 이 새 정책 집합의 이름을 지정하고, Palo Alto Firewall에서 진행 중인 TACACS+ 인증의 특성에 따라 조건을 추가하고, Allowed Protocols(허용되는 프로토콜) > Default Device Admin(기본 디바이스 관리)으로 선택합니다. 구성을 저장합니다.



9단계. > view 옵션에서 선택한 다음 Authentication Policy(인증 정책) 섹션에서 Cisco ISE가 Palo Alto Firewall에서 인증을 위해 사용자 이름 및 자격 증명을 쿼리하는 데 사용하는 외부 ID 소스를 선택합니다. 이 예에서 자격 증명은 ISE에 저장된 내부 사용자에 해당합니다.



10단계. Authorization Policy(권한 부여 정책)라는 섹션이 기본 정책으로 설정될 때까지 아래로 스크롤하여 기어 아이콘을 선택한 다음 위에 하나의 규칙을 삽입합니다.



11단계. 새 Authorization Rule(권한 부여 규칙)의 이름을 지정하고 이미 그룹 멤버십으로 인증된 사용자에 대한 조건을 추가하고 Shell Profiles(셸 프로파일) 섹션에서 이전에 구성한 TACACS 프로파일을 추가하고 컨피그레이션을 저장합니다.

다음을 확인합니다.

ISE 검토

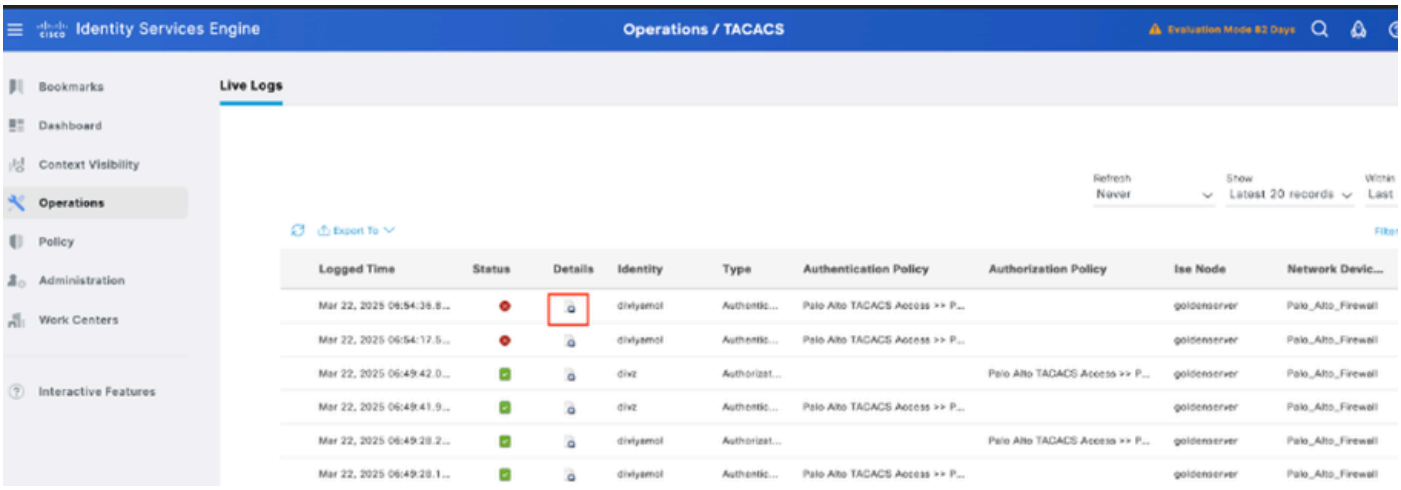
1단계. TACACS+ 서비스 가용성이 실행 중인지 검토합니다. 다음을 체크인할 수 있습니다.

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

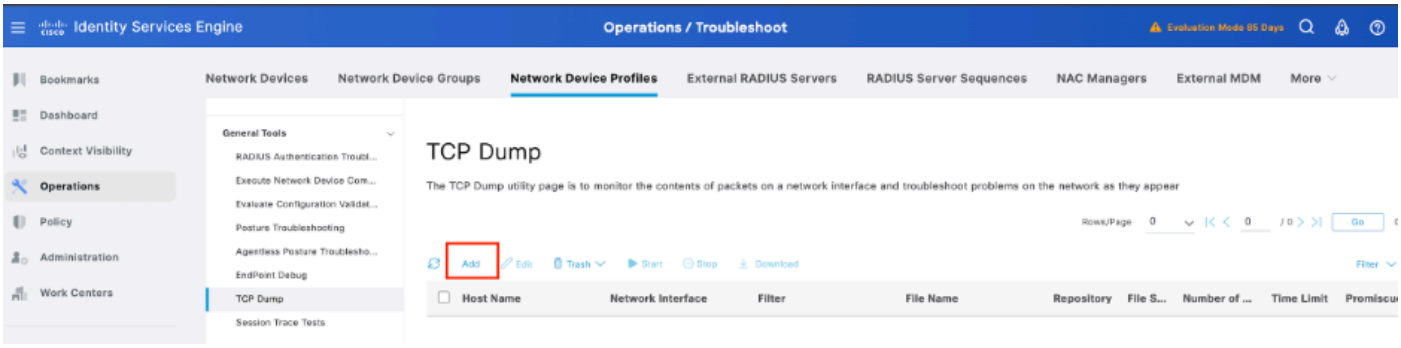
```
goldenserver/admin#show ports | include 49
tcp: [redacted]
```

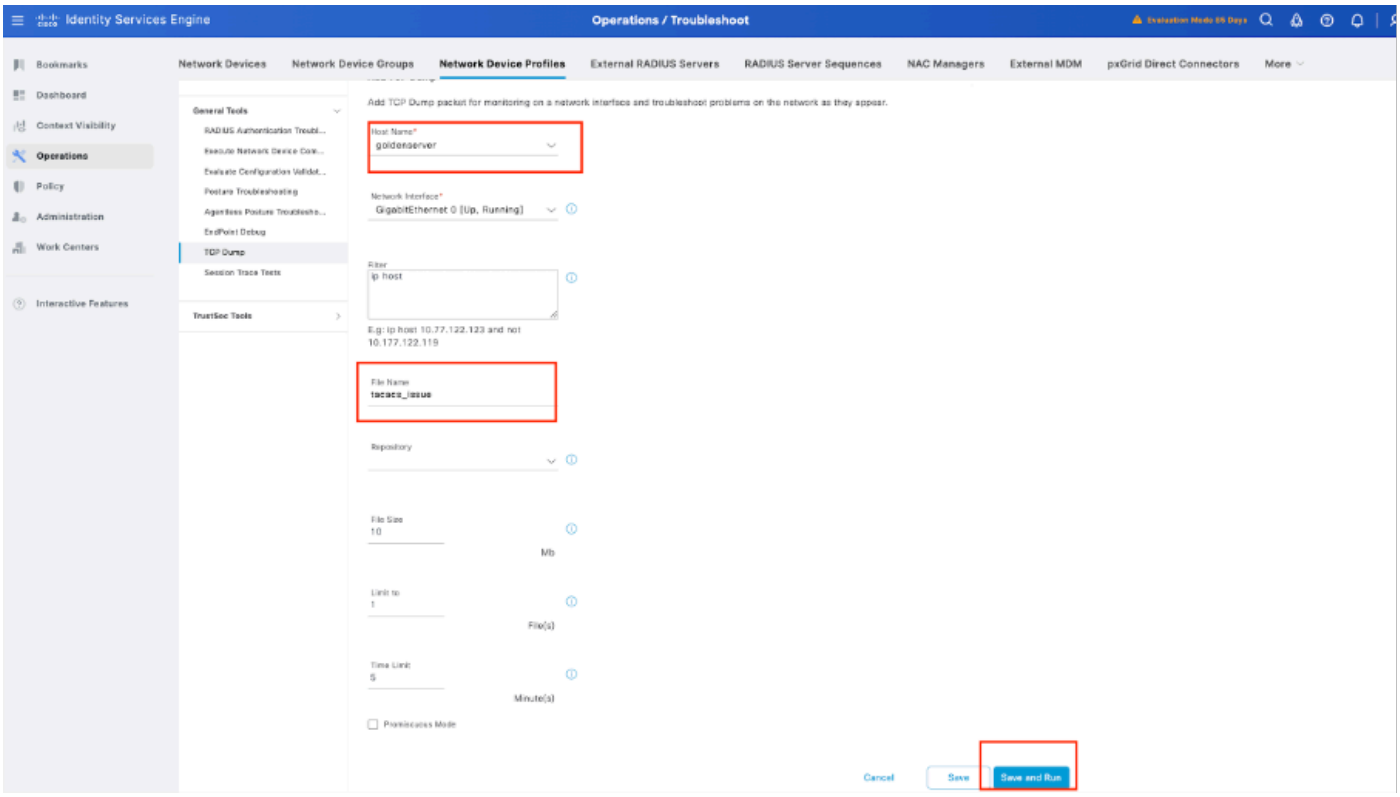
2단계. TACACS+ 인증 시도와 관련된 라이브 로그가 있는지 확인합니다. 이는 Operations(작업) -> TACACS -> Live logs(라이브 로그) 메뉴에서 선택할 수 있습니다.

실패 사유에 따라 컨피그레이션을 조정하거나 실패 원인을 해결할 수 있습니다.



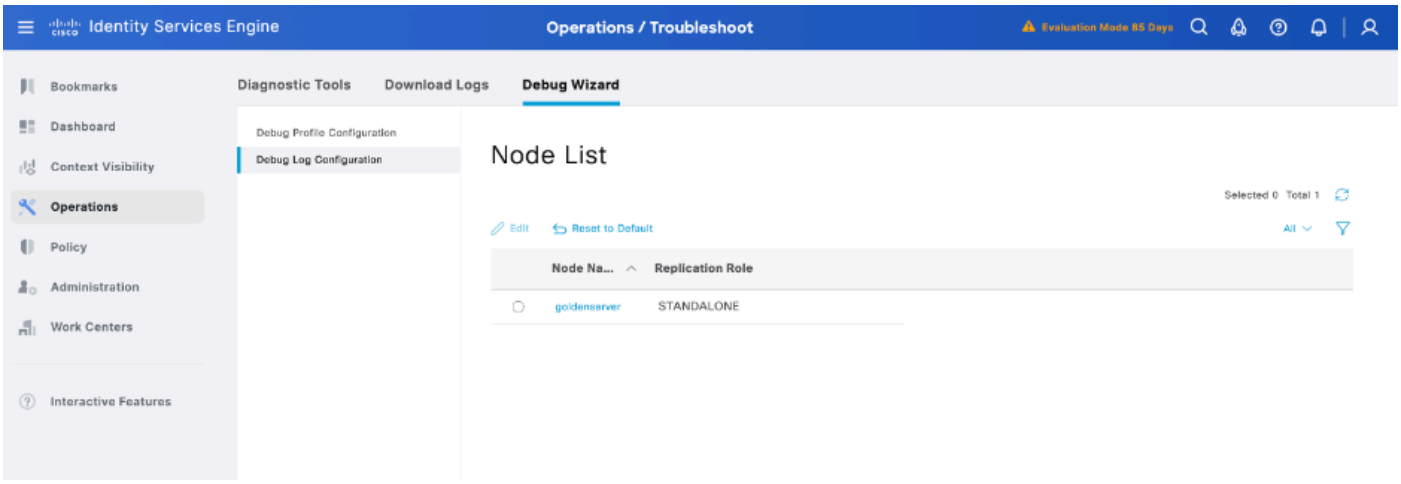
3단계. 라이브 로그가 표시되지 않는 경우 패킷 캡처를 진행하려면 Operations(운영) > Troubleshoot(문제 해결) > Diagnostic Tools(진단 도구) > General Tools(일반 도구) > TCP Dump(TCP 덤프) 메뉴로 이동한 후 Add(추가)를 선택합니다.

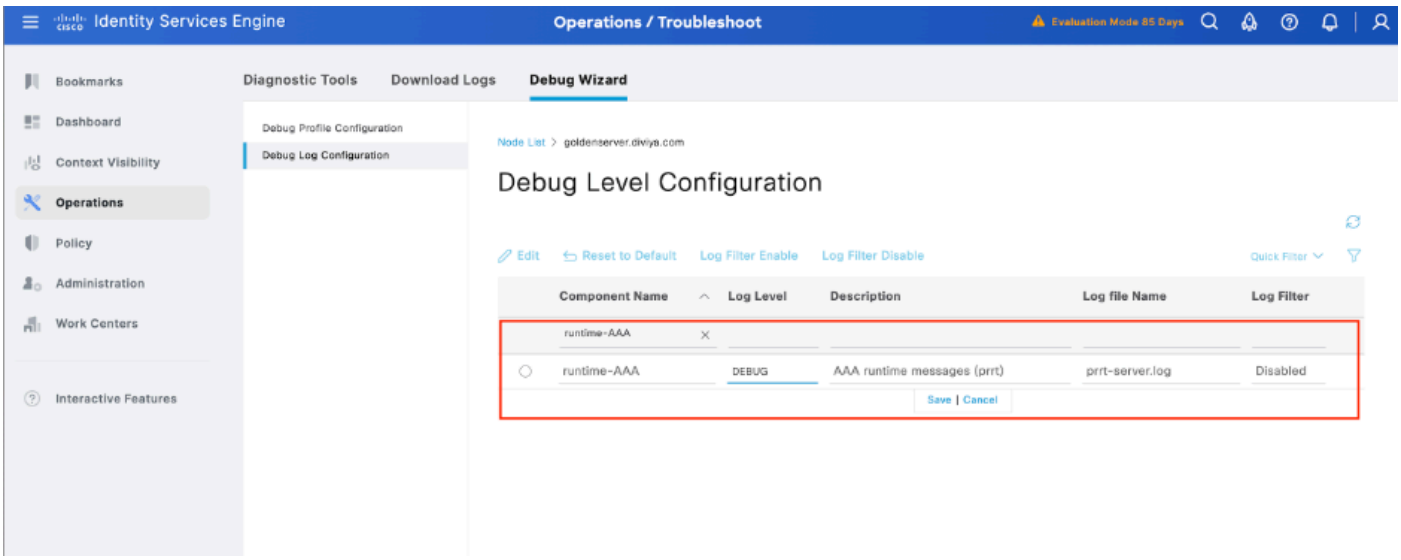




4단계. Operations(운영) > Troubleshoot(문제 해결) > Debug Wizard(디버그 마법사) > Debug log configuration(디버그 로그 컨피그레이션)에서 인증이 수행되는 PSN 내의 디버그에서 구성 요소

runtime-AAA를 활성화하고, PSN 노드를 선택한 후 edit(편집) 버튼에서 next(다음)를 선택합니다.





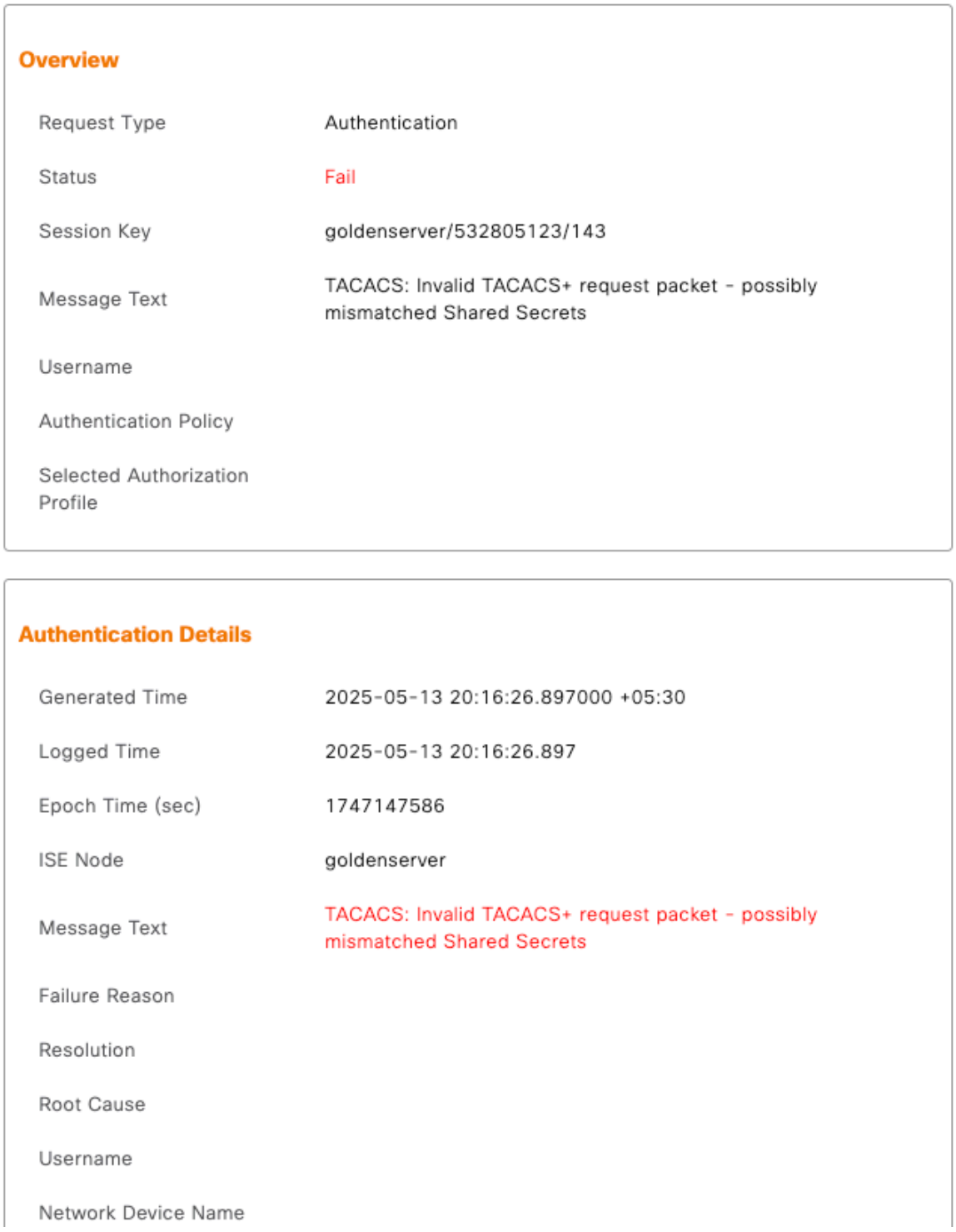
런타임 AAA 구성 요소를 식별하고, 로깅 수준을 디버그로 설정하고, 문제를 재현하고, 추가 조사를 위해 로그를 분석합니다.

문제 해결

TACACS: 잘못된 TACACS+ 요청 패킷 - 공유 암호가 일치하지 않을 수 있습니다.

문제

Cisco ISE와 Palo Alto 방화벽(또는 모든 네트워크 디바이스) 간의 TACACS+ 인증은 다음 오류 메시지와 함께 실패합니다.
"잘못된 TACACS+ 요청 패킷 - 공유 암호가 일치하지 않을 수 있습니다."



Overview

Request Type	Authentication
Status	Fail
Session Key	goldenserver/532805123/143
Message Text	TACACS: Invalid TACACS+ request packet - possibly mismatched Shared Secrets
Username	
Authentication Policy	
Selected Authorization Profile	

Authentication Details

Generated Time	2025-05-13 20:16:26.897000 +05:30
Logged Time	2025-05-13 20:16:26.897
Epoch Time (sec)	1747147586
ISE Node	goldenserver
Message Text	TACACS: Invalid TACACS+ request packet - possibly mismatched Shared Secrets
Failure Reason	
Resolution	
Root Cause	
Username	
Network Device Name	

이렇게 하면 성공적인 관리 로그인 시도를 방지할 수 있으며 중앙 집중식 인증을 통해 디바이스 액세스 제어에 영향을 줄 수 있습니다.

가능한 원인

- Cisco ISE에 구성된 공유 비밀과 Palo Alto 방화벽 또는 네트워크 디바이스가 일치하지 않습니다.
- 디바이스에서 잘못된 TACACS+ 서버 컨피그레이션(예: 잘못된 IP 주소, 포트 또는 프로토콜)입니다.

솔루션

이 문제에 대한 몇 가지 해결 방법이 있습니다.

1. 공유 암호를 확인합니다.

- Cisco ISE의 경우:
  Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동하여 영향을 받는 디바이스를 선택하고 공유 암호를 확인합니다.

- Palo Alto 방화벽:
  Device(디바이스) > Server Profiles(서버 프로필) > TACACS+로 이동하여 공유 암호가 대/소문자 및 특수 문자를 포함하여 정확히 일치하는지 확인합니다.

2. TACACS+ 서버 설정 확인:

- 방화벽의 TACACS+ 프로필에 Cisco ISE의 올바른 IP 주소 및 포트(기본값은 49)가 구성되어 있는지 확인합니다.

- 프로토콜 유형이 TACACS+(RADIUS가 아님)인지 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.