ISE 기가비트 이더넷 1 인터페이스로 TACACS+ 구성

목차

소개

이 문서에서는 라우터 및 스위치가 네트워크 디바이스로 작동하는 기가비트 이더넷 1 인터페이스를 사용하는 ISE TACACS+ 컨피그레이션에 대해 설명합니다.

배경 정보

Cisco ISE는 최대 6개의 이더넷 인터페이스를 지원합니다. 본드 0, 본드 1, 본드 2의 세 가지 본드만 가질 수 있습니다. 본드의 일부인 인터페이스를 변경하거나 본드에서 인터페이스의 역할을 변경할

수 없습니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대해 알고 있는 것이 좋습니다.

- 기본 네트워킹 지식
- Cisco Identity Service Engine입니다.

사용되는 구성 요소

이 문서의 정보는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

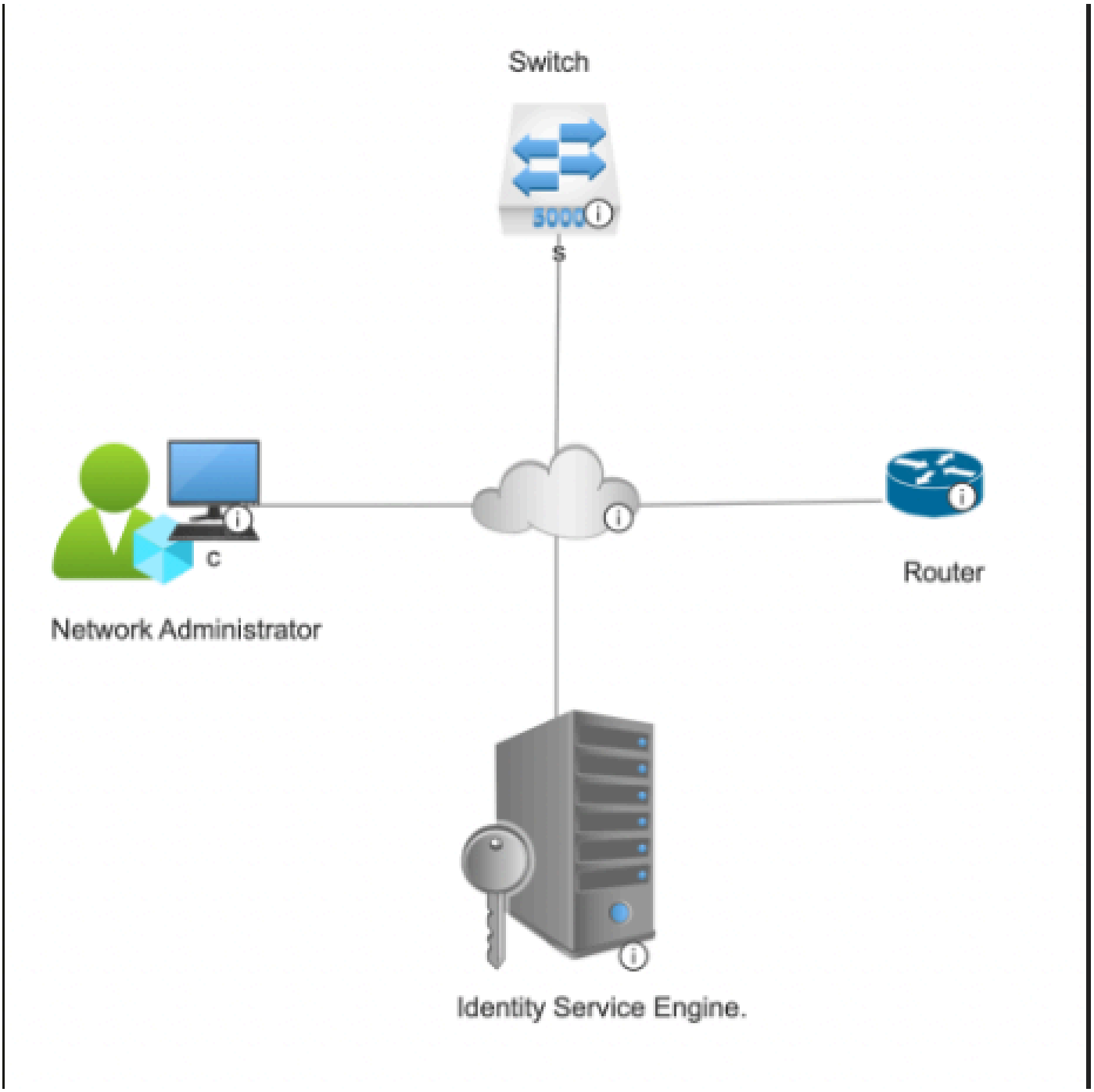
- Cisco Identity Service Engine v3.3
- Cisco IOS® Software 릴리스 17.x
- Cisco C9200 스위치.

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

이 컨피그레이션의 목적은 다음과 같습니다. TACACS+용 ISE의 기가비트 이더넷 1을 구성하고 ISE를 인증 서버로 사용하는 TACACS+로 스위치 및 라우터를 인증합니다.

네트워크 다이어그램

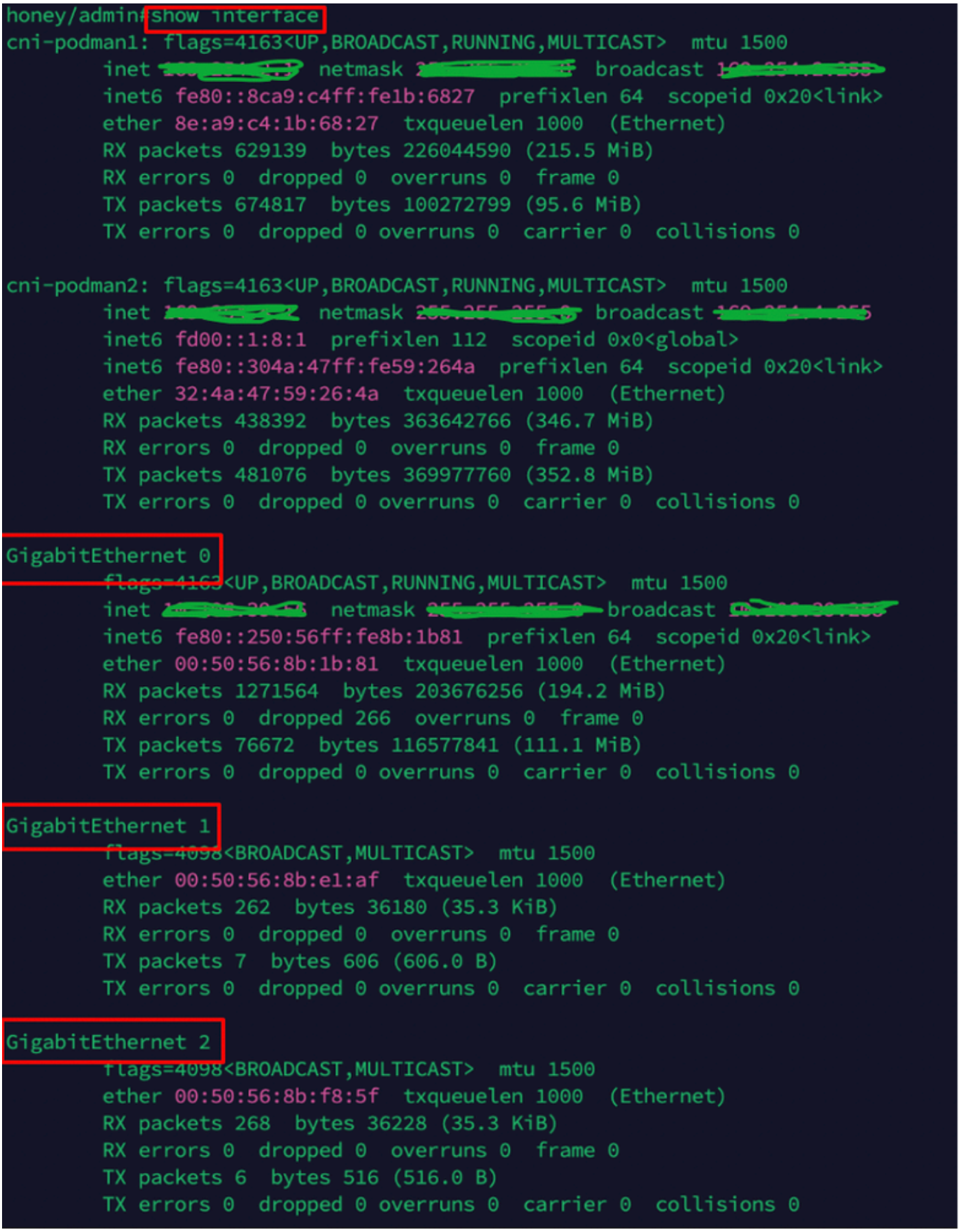


네트워크 토폴로지

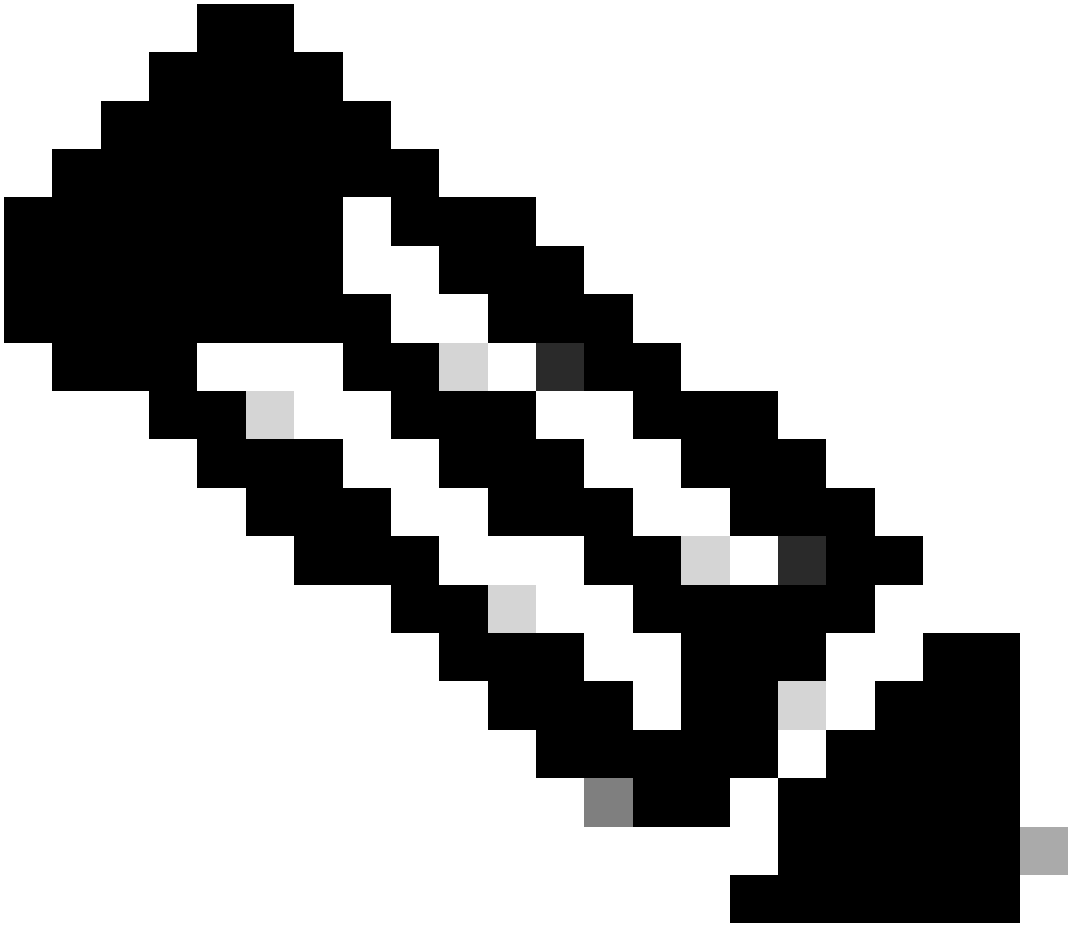
TACACS+용 ISE(Identity Services Engine) 구성

ISE의 기가비트 이더넷 1 인터페이스에 대한 IP 주소 구성

1. Device admin(디바이스 관리)이 활성화된 ISE PSN 노드의 CLI에 로그인하고 show interface 명령을 사용하여 사용 가능한 인터페이스를 확인합니다.



ISE에서 인터페이스 확인



참고: 이 컨피그레이션에서는 3개의 인터페이스만 ISE에 구성되며 기가비트 이더넷 1 인터페이스에 중점을 둡니다. 동일한 절차를 모든 인터페이스에 대한 IP 주소를 구성하는 데 적용할 수 있습니다. 기본적으로 ISE는 최대 6개의 기가비트 이더넷 인터페이스를 지원합니다.

---

2. 동일한 PSN 노드의 CLI에서 다음 명령을 사용하여 기가비트 이더넷 1 인터페이스에 IP 주소를 할당합니다.

hostnameofise#구성

hostnameofise/admin(config)#interface Gigabit Ethernet 1

hostnameofise/admin(config-GigabitEthernet-1)# <ip address> <subnet netmask> % IP 주소를 변경하면 ise 서비스가 다시 시작될 수 있습니다.

IP 주소 변경을 계속하시겠습니까?

계속할까요? [예, 아니요] 예

3. 2단계를 수행하면 ISE 노드 서비스가 다시 시작됩니다. ISE 서비스의 상태를 확인하려면 show application status ise 명령을 실행하고 이 스크린샷에 따라 서비스의 상태가 실행 중인지 확인합니다.

```
honey/admin#show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          1739169
Database Server                        running          102 PROCESSES
Application Server                     running          1755746
Profiler Database                      running          1746379
ISE Indexing Engine                    running          1757121
AD Connector                           running          1759148
M&T Session Database                   running          1752122
M&T Log Processor                      running          1755926
Certificate Authority Service          running          1759026
EST Service                            running          1786647
SXP Engine Service                     disabled
TC-NAC Service                         disabled
PassiveID WMI Service                  disabled
PassiveID Syslog Service               disabled
PassiveID API Service                  disabled
PassiveID Agent Service                disabled
PassiveID Endpoint Service             disabled
PassiveID SPAN Service                 disabled
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
ISE Messaging Service                  running          1743222
ISE API Gateway Database Service       running          1745409
ISE API Gateway Service                running          1750887
ISE pxGrid Direct Service              running          1874179
Segmentation Policy Service            disabled
REST Auth Service                      disabled
SSE Connector                          disabled
Hermes (pxGrid Cloud Agent)            disabled
McTrust (Meraki Sync Service)          disabled
ISE Node Exporter                      running          1760519
ISE Prometheus Service                 running          1762540
ISE Grafana Service                    running          1765779
ISE MNT LogAnalytics Elasticsearch     running          1768218
ISE Logstash Service                   running          1773207
ISE Kibana Service                     running          1774914
ISE Native IPSec Service               running          1779658
MFC Profiler                           running          1932013
```

ISE 서비스 상태 확인

4. show interface 명령을 사용하여 Gig1 인터페이스의 IP 주소를 확인합니다.

V

```
honey/admin#show interface
cni-podman1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::8ca9:c4ff:fe1b:6827  prefixlen 64  scopeid 0x20<link>
        ether 8e:a9:c4:1b:68:27  txqueuelen 1000  (Ethernet)
        RX packets 633876  bytes 228753800 (218.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 680052  bytes 102100762 (97.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

cni-podman2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fd00::1:8:1  prefixlen 112  scopeid 0x0<global>
        inet6 fe80::304a:47ff:fe59:264a  prefixlen 64  scopeid 0x20<link>
        ether 32:4a:47:59:26:4a  txqueuelen 1000  (Ethernet)
        RX packets 503576  bytes 516105026 (492.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 595701  bytes 383404526 (365.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 0
        flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::250:56ff:fe8b:1b81  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:8b:1b:81  txqueuelen 1000  (Ethernet)
        RX packets 1387052  bytes 213478717 (203.5 MiB)
        RX errors 0  dropped 266  overruns 0  frame 0
        TX packets 136494  bytes 261900250 (249.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 1
        flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::250:56ff:fe8b:e1af  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:8b:e1:af  txqueuelen 1000  (Ethernet)
        RX packets 5165  bytes 1072036 (1.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 2260 (2.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

CLI에서 ISE Gig2 인터페이스 IP 주소 확인

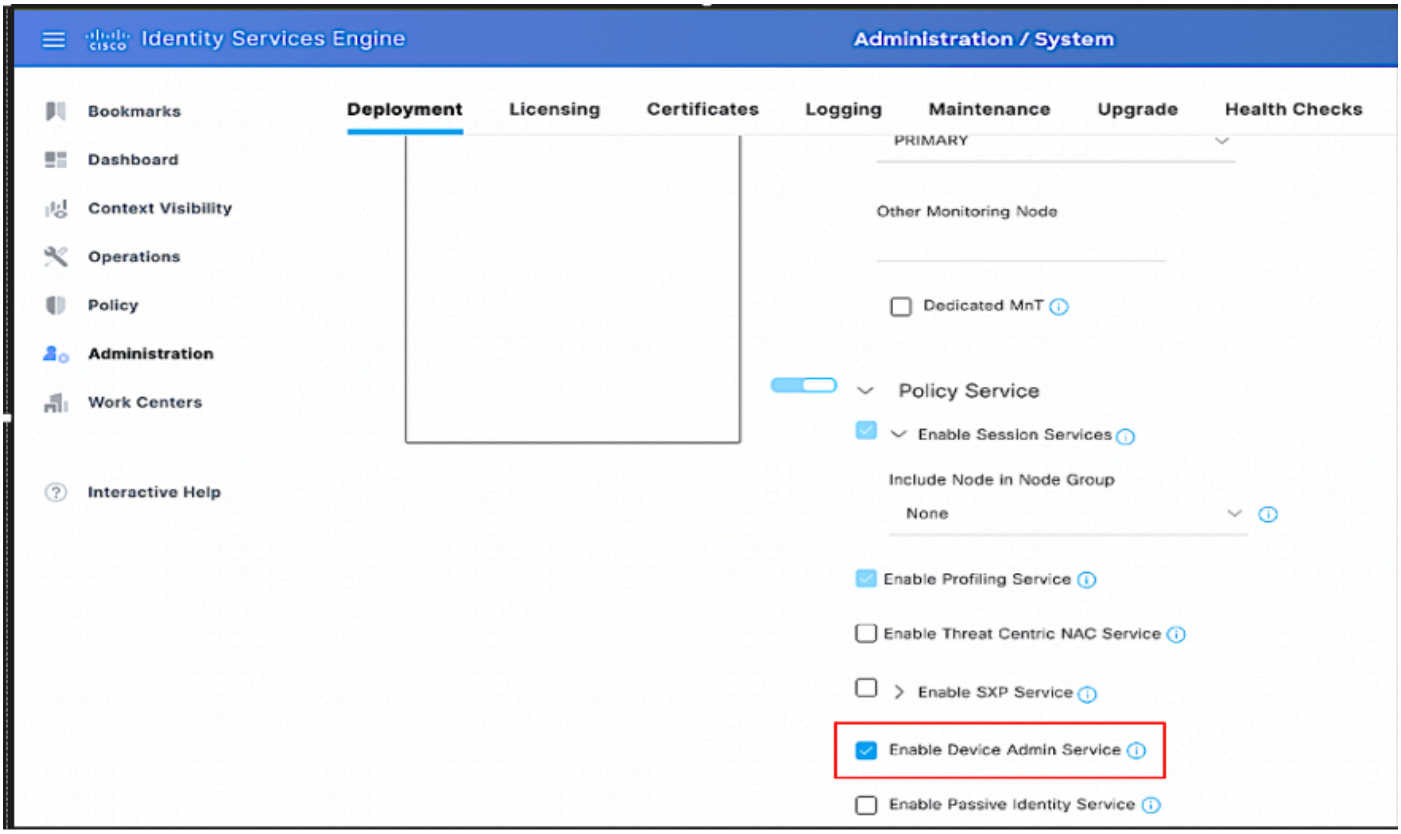
5. show ports를 사용하여 ISE 노드에서 포트 49의 허용치를 확인합니다 | inc 49 명령

```
honey/admin#show ports | include 49
        tcp: 127.0.0.1:8888, 169.254.4.1:49, 169.254.2.1:49, [redacted]:49, [redacted]:49,
```

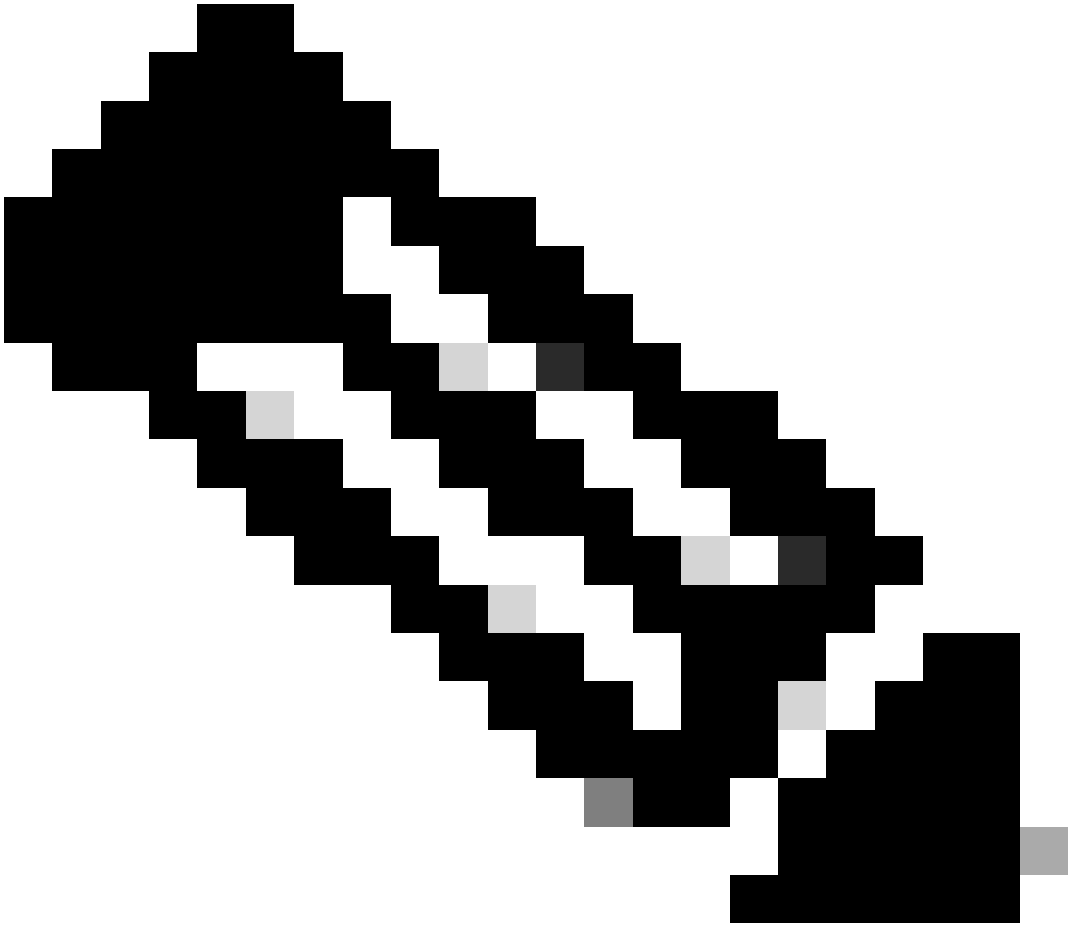
ISE에서 포트 49 허용 확인

ISE에서 디바이스 관리 활성화

ISE의 GUI > Administration(관리) > Deployment(구축) > Select the PSN node(PSN 노드 선택)로 이동한 다음 Enable Device admin service(디바이스 관리 서비스 활성화)를 선택합니다.



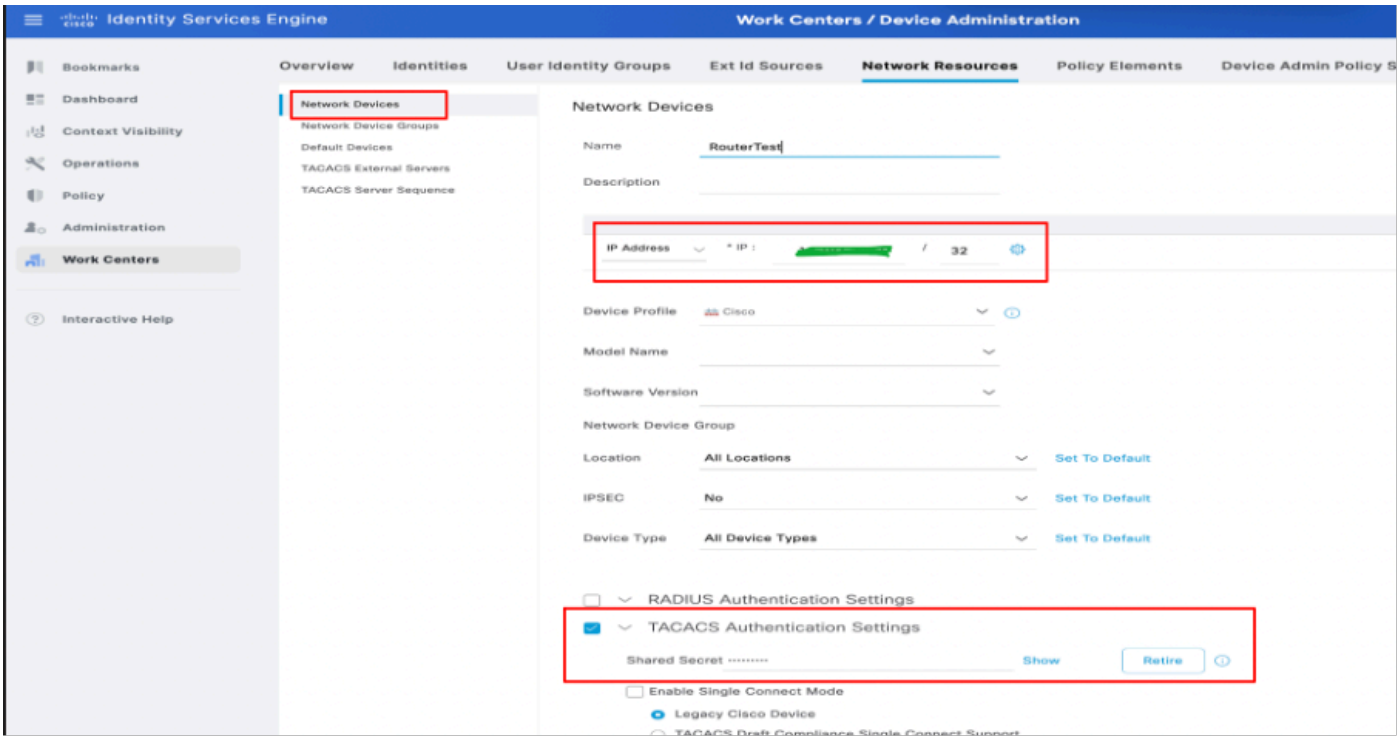
ISE에서 디바이스 관리 서비스 활성화



참고: 디바이스 관리 서비스를 활성화하려면 디바이스 관리 라이센스가 필요합니다.

ISE에서 네트워크 디바이스 추가

1. Work Centers(작업 센터) > Device Administration(디바이스 관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동합니다. Add(추가)를 클릭합니다. 이름, IP 주소를 입력합니다. TACACS+ 인증 설정 확인란을 선택하고 공유 암호 키를 제공합니다.



ISE의 네트워크 디바이스 컨피그레이션

2. 위의 절차에 따라 TACACS 인증에 필요한 모든 네트워크 디바이스를 추가합니다.

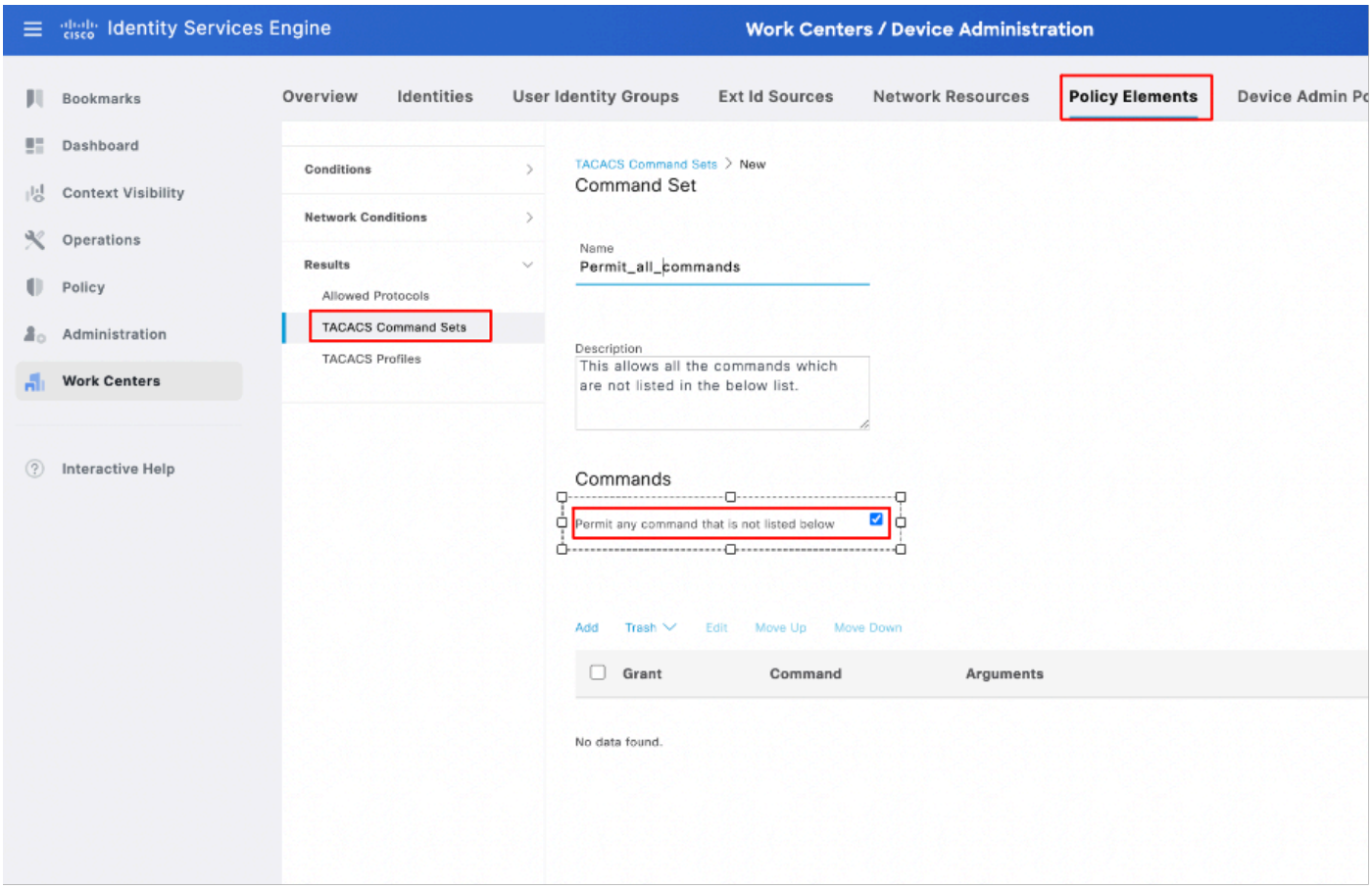
TACACS+ 명령 집합 구성

이 데모에는 두 개의 명령 집합이 구성되어 있습니다.

Permit_all_commands는 사용자 admin에 할당되며 디바이스의 모든 명령을 허용합니다.

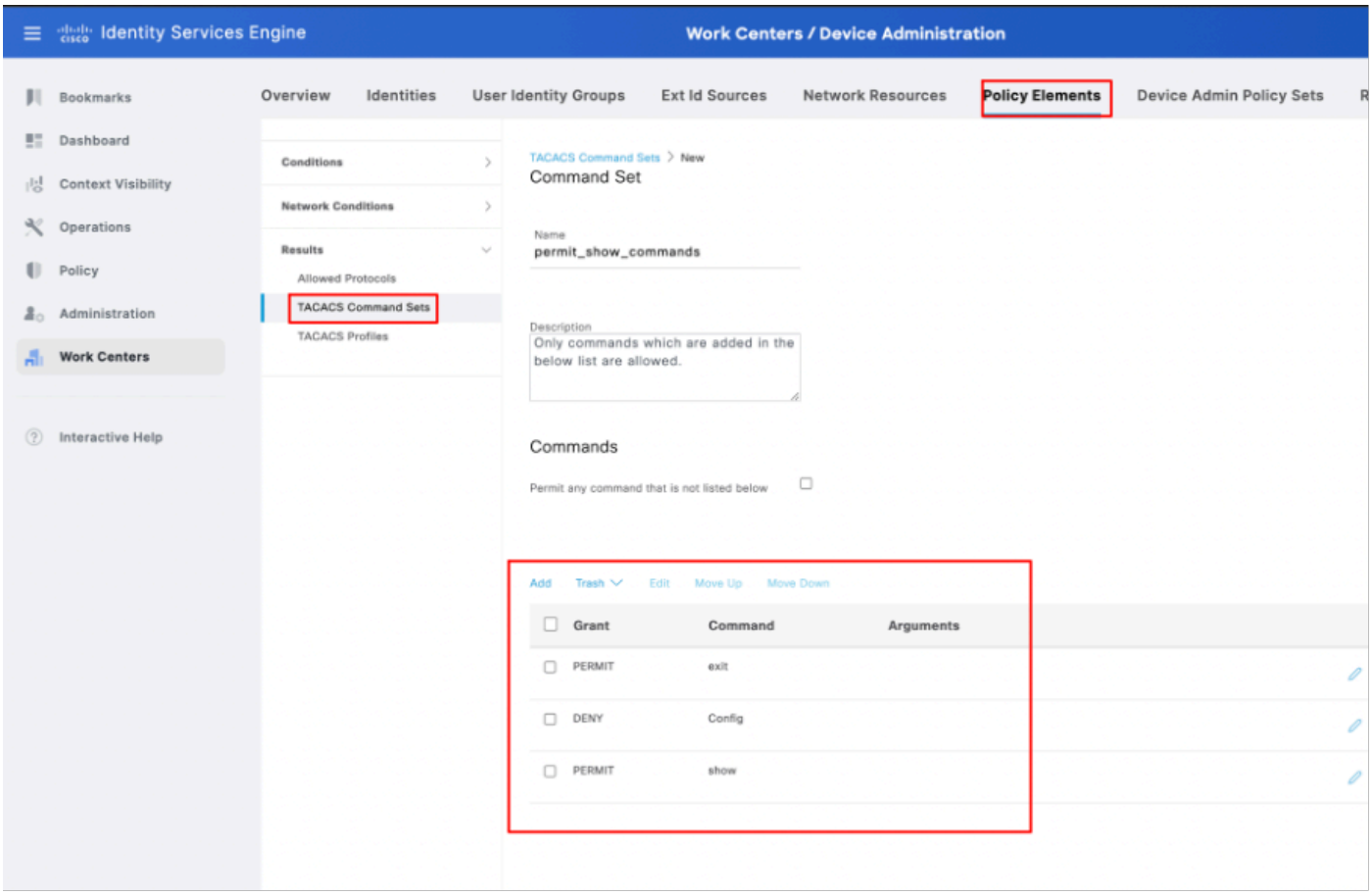
permit_show_commands는 사용자에게 할당되며 show 명령만 허용합니다

1. Work Centers(작업 센터) > Device Administration(디바이스 관리) > Policy Results(정책 결과) > TACACS Command Sets(TACACS 명령 집합)로 이동합니다. Add(추가)를 클릭합니다. Name PermitAllCommands(이름 PermitAllCommands)를 제공한 다음 Permit any command(모든 명령 허용) 확인란을 선택합니다. Submit(제출)을 클릭합니다.



ISE의 명령 집합 컨피그레이션

2. Work Centers(작업 센터) > Device Administration(디바이스 관리) > Policy Results(정책 결과) > TACACS Command Sets(TACACS 명령 집합)로 이동합니다. Add(추가)를 클릭합니다. Name(이름)PermitShowCommands를 제공하고 Add(추가)를 클릭한 다음 마지막으로 permit show and exit(show and exit) 명령을 입력합니다. 기본적으로 인수를 비워 둘 경우 모든 인수가 포함됩니다. Submit(제출)을 클릭합니다.

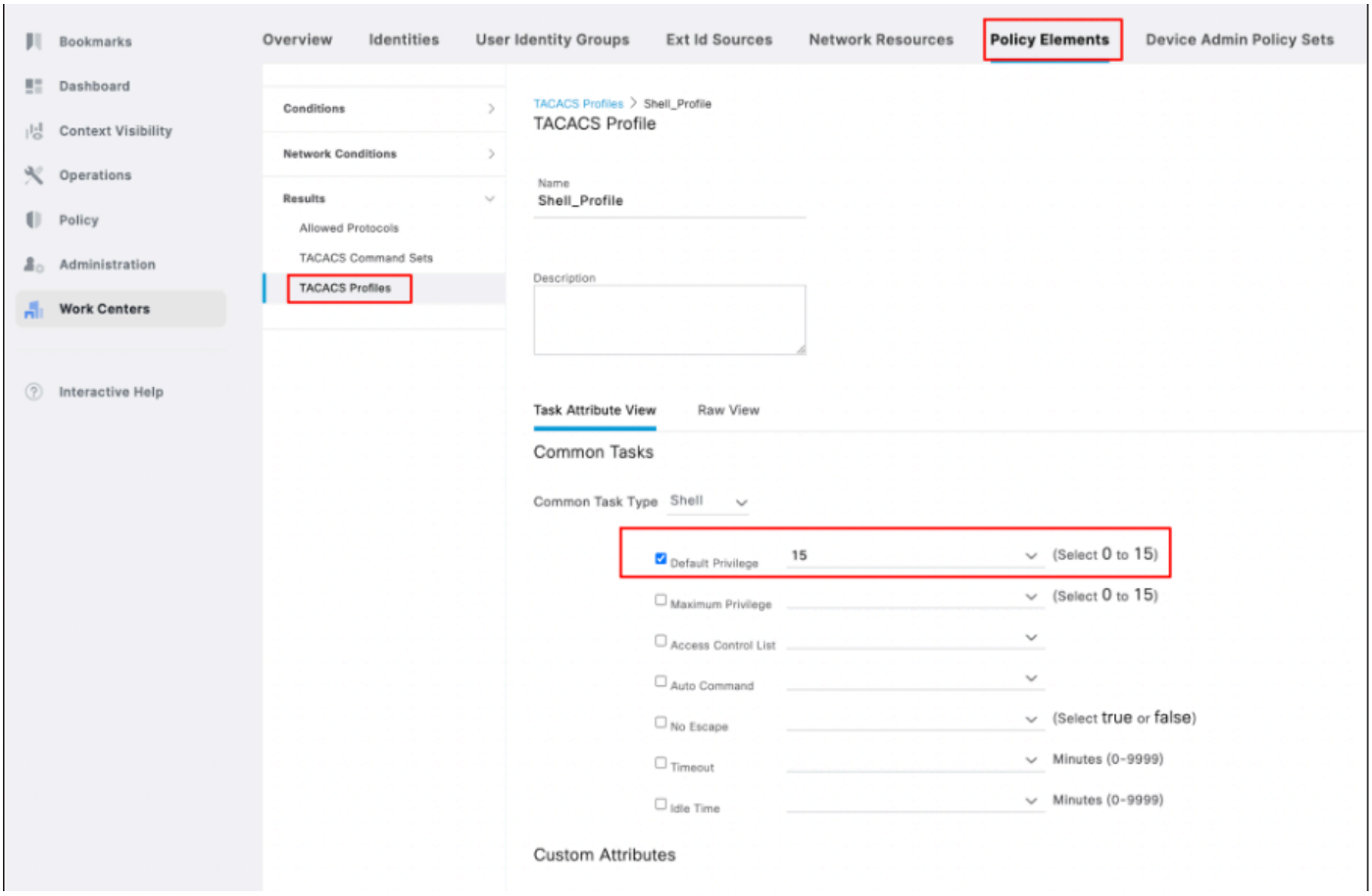


ISE의 permit_show_commands 구성

TACACS+ 프로파일 구성

단일 TACACS+ 프로파일이 구성되고 명령 권한 부여가 명령 집합을 통해 수행됩니다.

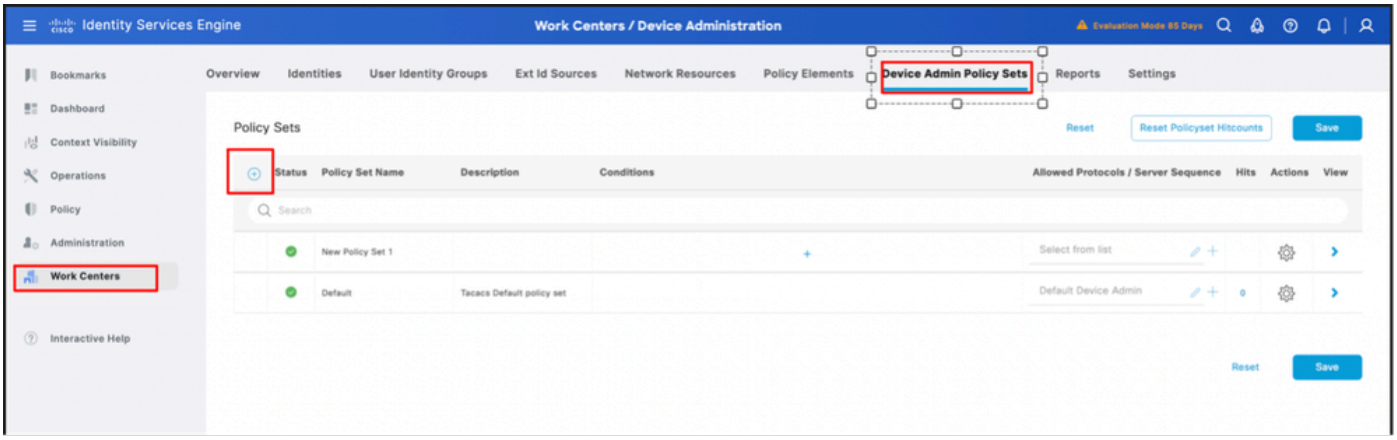
TACACS+ 프로필을 구성하려면 Work Centers(작업 센터) > Device Administration(디바이스 관리) > Policy Results(정책 결과) > TACACS Profiles(TACACS 프로필)로 이동합니다. 추가를 누르고 셸 프로파일의 이름을 입력하고 기본 권한 확인란을 선택한 다음 값 15를 입력합니다. 마지막으로 제출을 누릅니다.



ISE에서 TACACS 프로파일 컨피그레이션

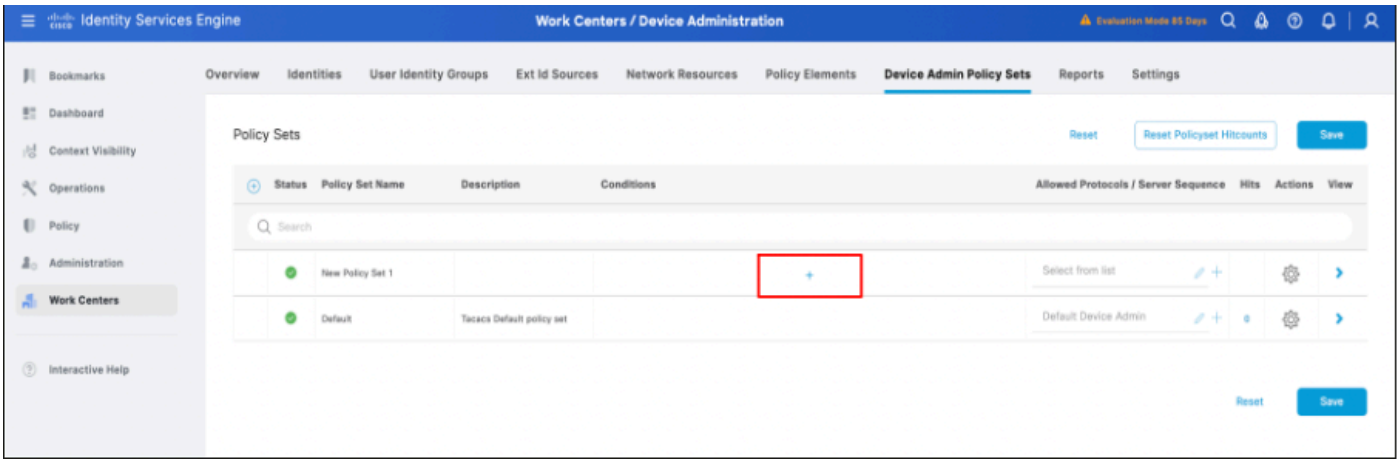
TACACS+ 인증 및 권한 부여 프로파일 구성

1. ISE PAN GUI -> Administration -> Work Centers -> Device administration -> Device admin policy sets에 로그인합니다. 새 정책을 만들려면 +(더하기) 아이콘을 클릭합니다. 이 경우 정책 집합의 이름은 New Policy set 1로 지정됩니다.



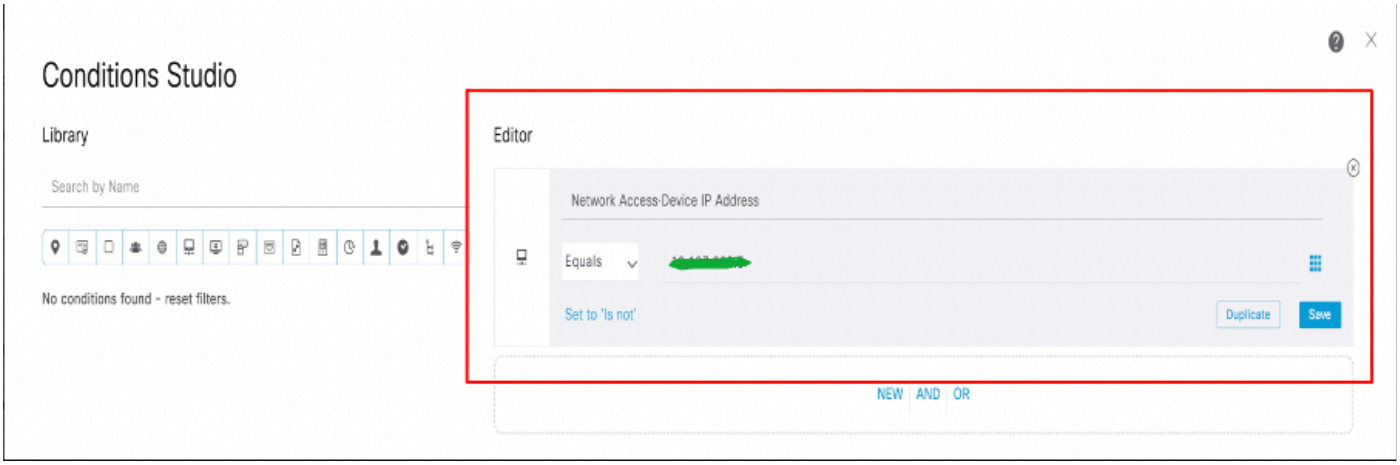
ISE에 설정된 정책 컨피그레이션

2. 정책 집합을 저장하기 전에 이 스크린샷과 같이 조건을 구성해야 합니다. 정책 집합에 대한 조건을 구성하려면 +(더하기) 아이콘을 클릭합니다.

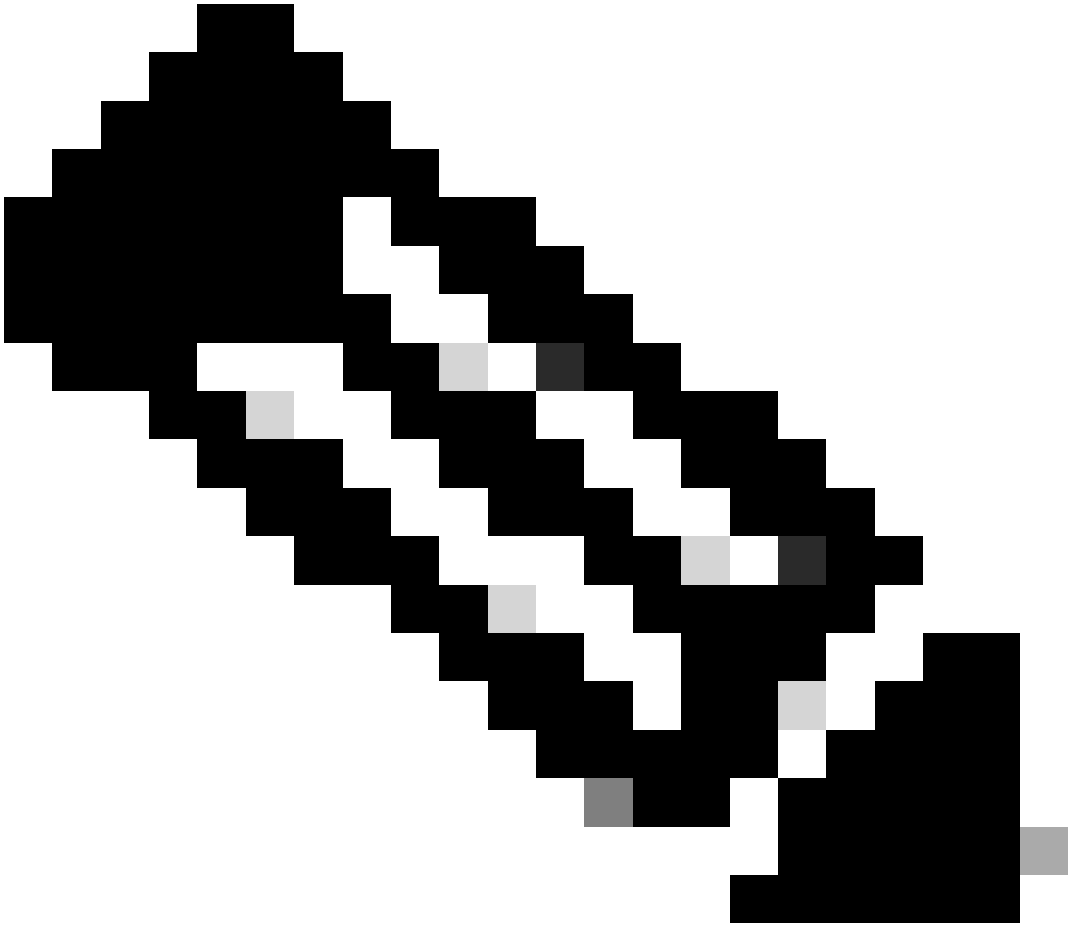


ISE의 정책 설정 조건 컨피그레이션

3. 2단계에서 설명한 +(더하기) 아이콘을 클릭하면 조건 스튜디오 대화상자가 열립니다. 필요한 조건을 구성합니다. 새 조건 또는 기존 조건과 함께 조건을 저장하고 스크롤합니다. Use를 클릭합니다.



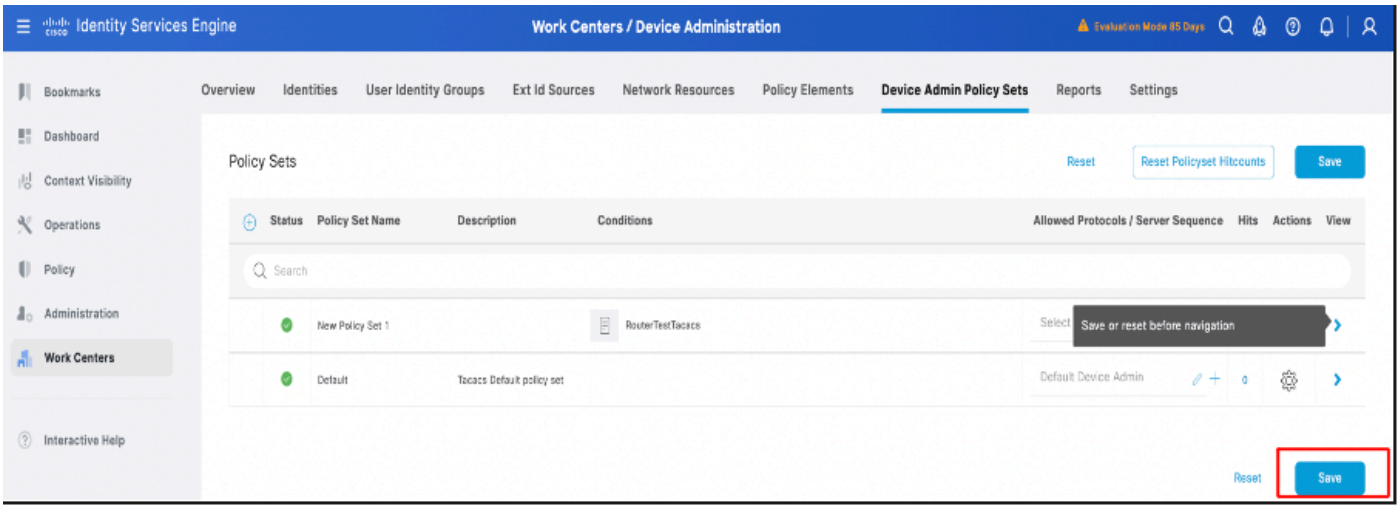
ISE의 정책 설정 조건 컨피그레이션



참고: 이 문서의 경우 조건은 네트워크 디바이스 IP와 일치합니다. 그러나 구축 요구 사항에 따라 조건을 변경할 수 있습니다.

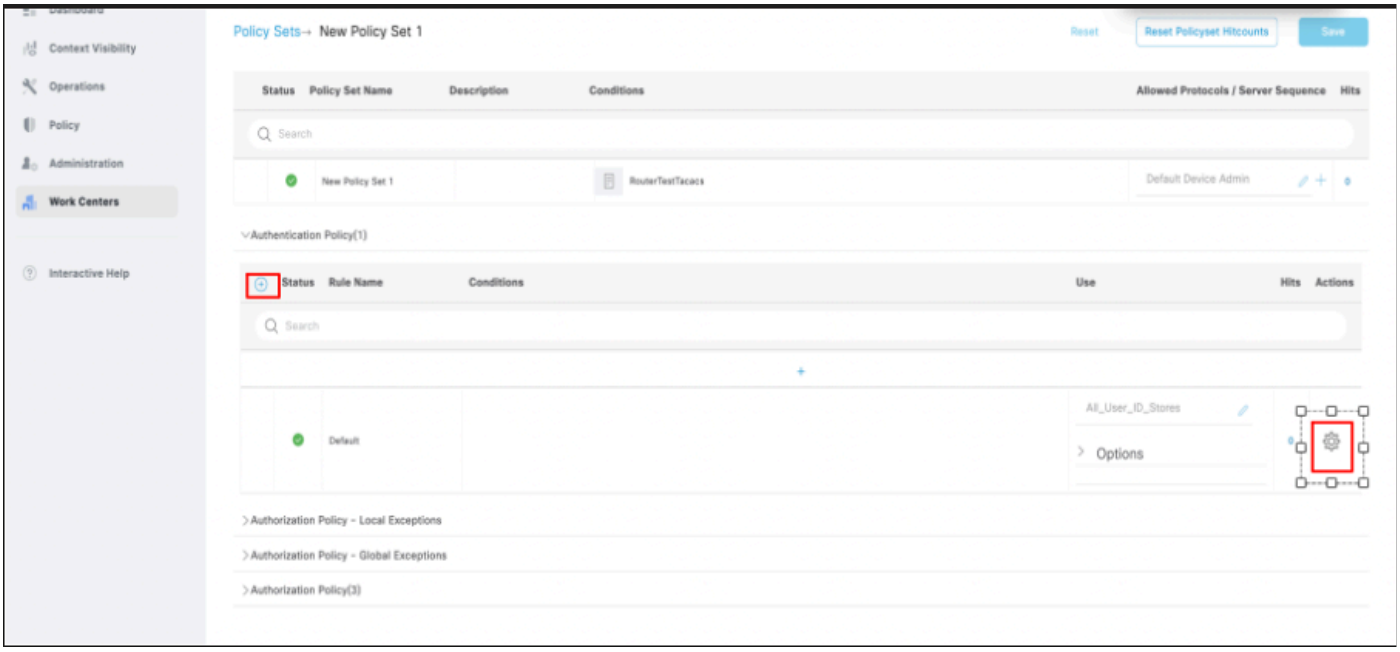
---

4. 조건을 구성하고 저장한 후 허용되는 프로토콜을 Default device admin으로 구성합니다. Save 옵션을 클릭하여 생성한 정책 집합을 저장합니다.

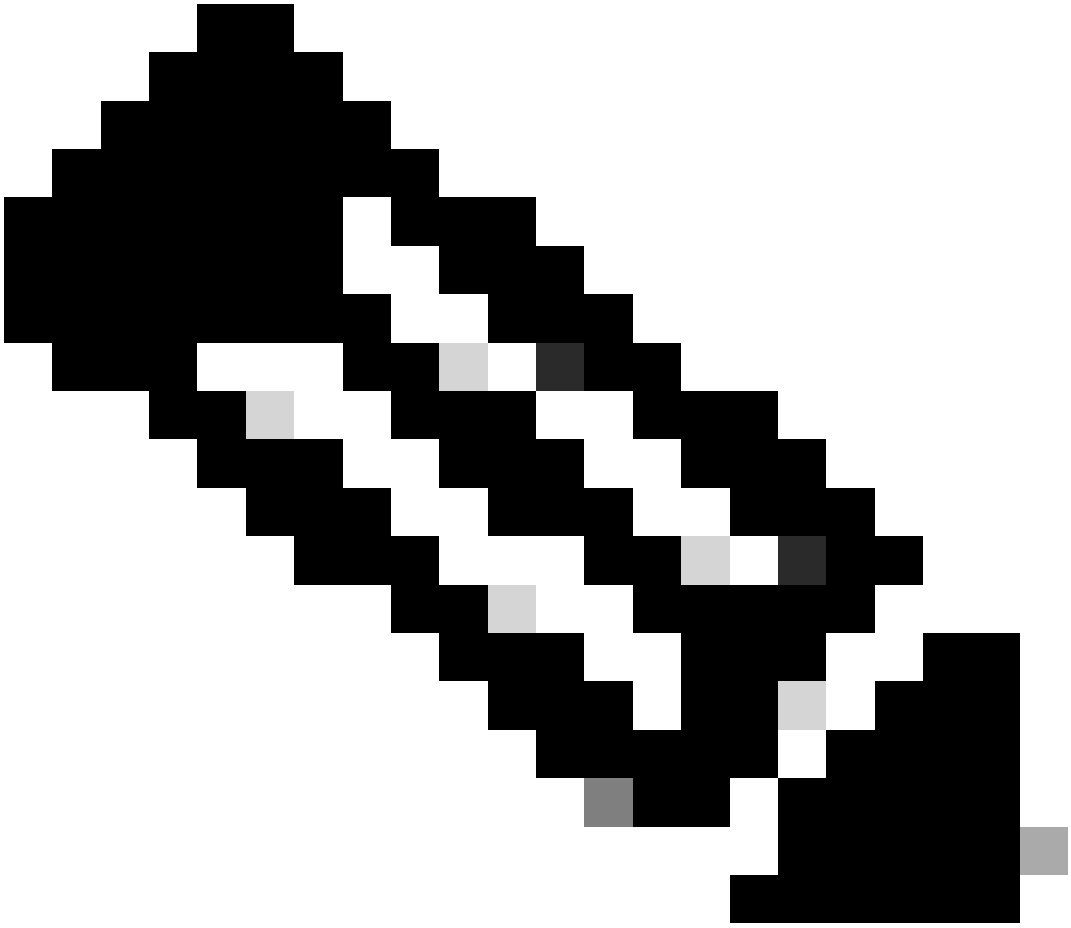


정책 설정 컨피그레이션 확인

5. 새 정책 집합 -> 인증 정책 (1) -> +(더하기) 아이콘을 누르거나 기어 아이콘을 눌러 새 인증 정책을 생성한 다음 위에 새 행을 삽입합니다.



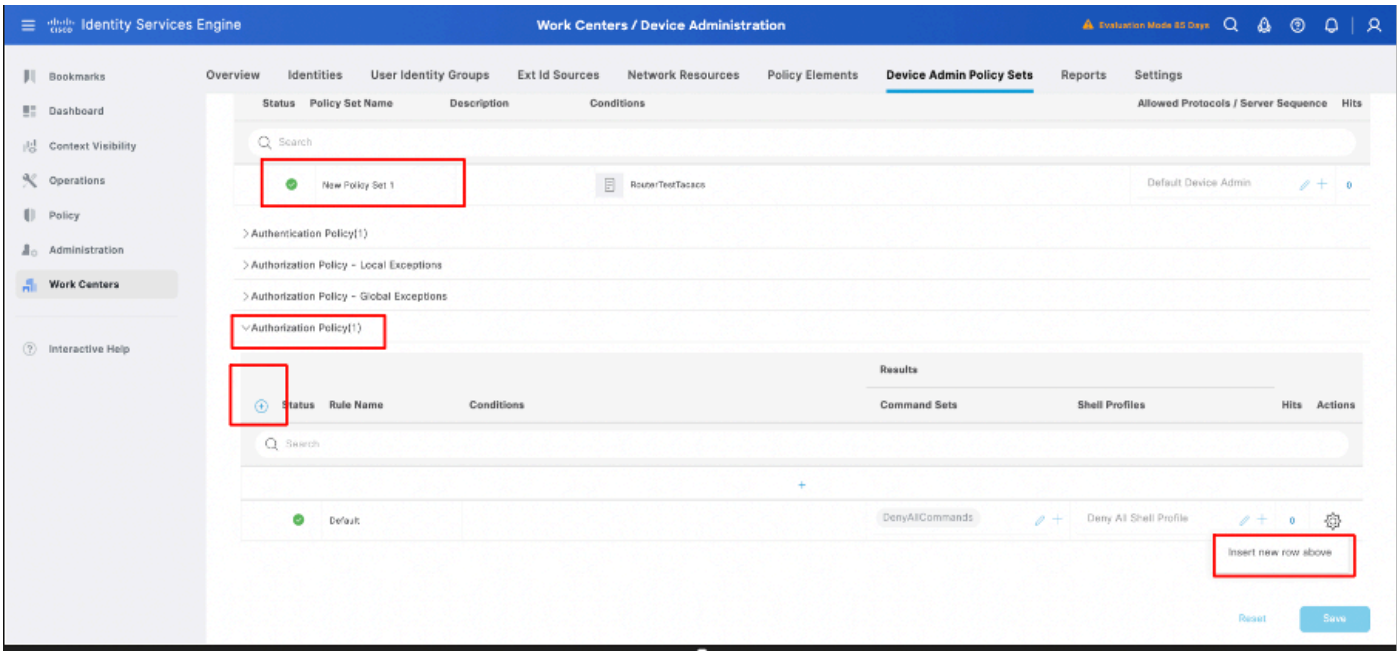
정책 집합의 인증 정책 구성.



참고: 이 데모에서는 All_User_ID_Stores와 함께 설정된 기본 인증 정책이 사용됩니다. 그러나 ID 저장소의 사용은 구축 요구 사항에 따라 사용자 정의할 수 있습니다.

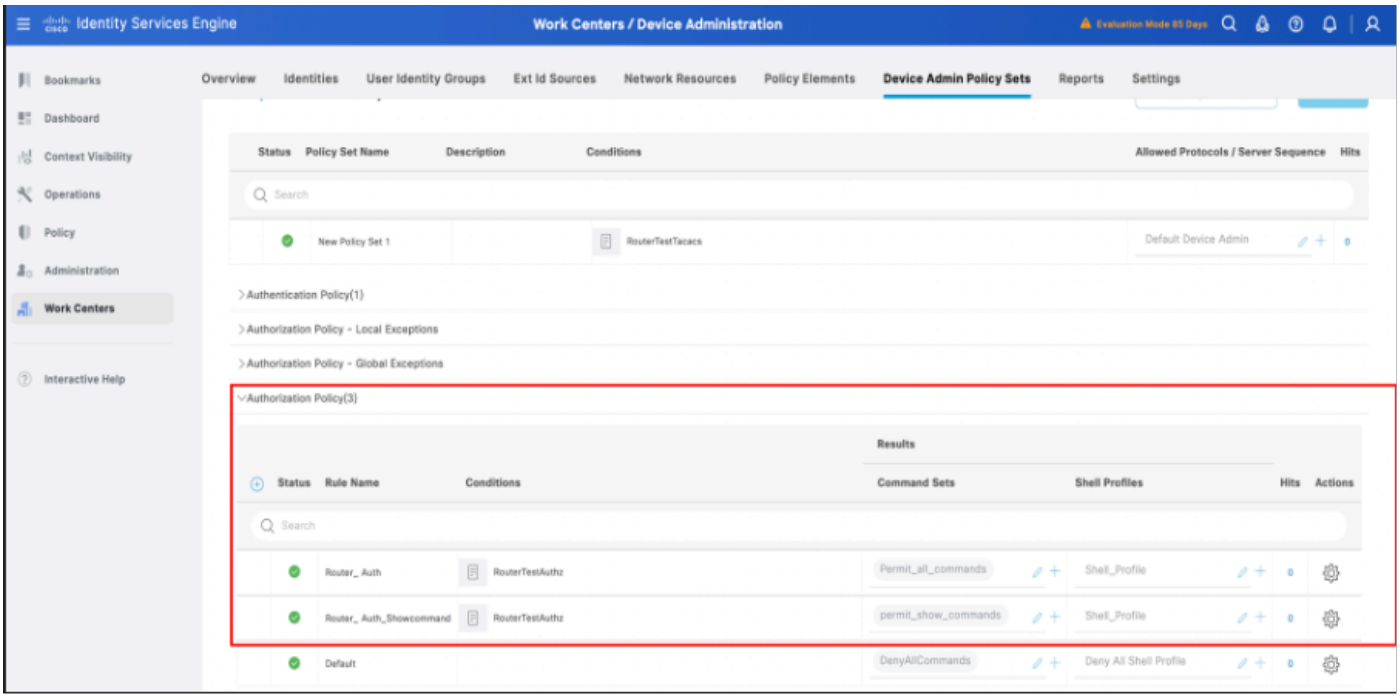
---

6. 새 정책 집합 -> 권한 부여 정책 (1)을 확장합니다. +(더하기) 아이콘 을 클릭하거나 기어 아이콘 을 클릭합니다. 그런 다음 권한 부여 정책을 생성하기 위해 위에 새 행을 삽입합니다.

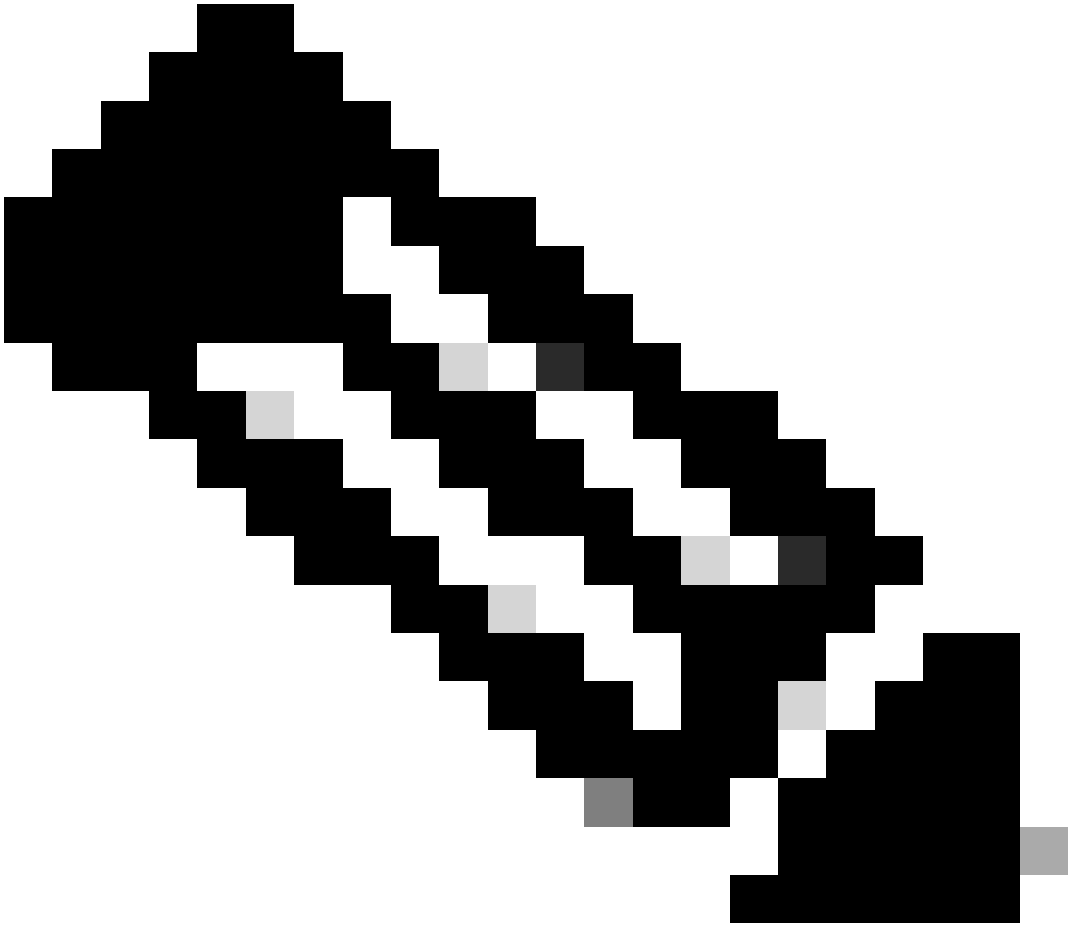


권한 부여 정책 구성

7. 권한 부여 정책에 매핑된 조건, 명령 집합 및 셸 프로필을 사용하여 권한 부여 정책을 구성합니다.



ISE에서 권한 부여 정책의 완전한 컨피그레이션



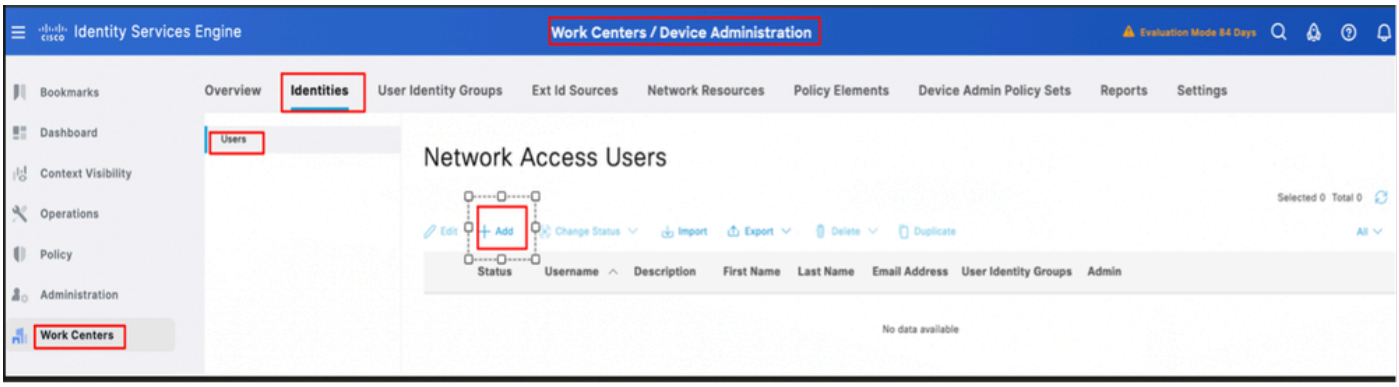
참고: 구성된 조건은 랩 환경에 따라 다르며 구축 요구 사항에 따라 구성할 수 있습니다.

---

8. TACACS+에 사용되는 스위치 또는 기타 네트워크 디바이스에 대한 정책 세트를 구성하려면 처음 6단계를 수행합니다.

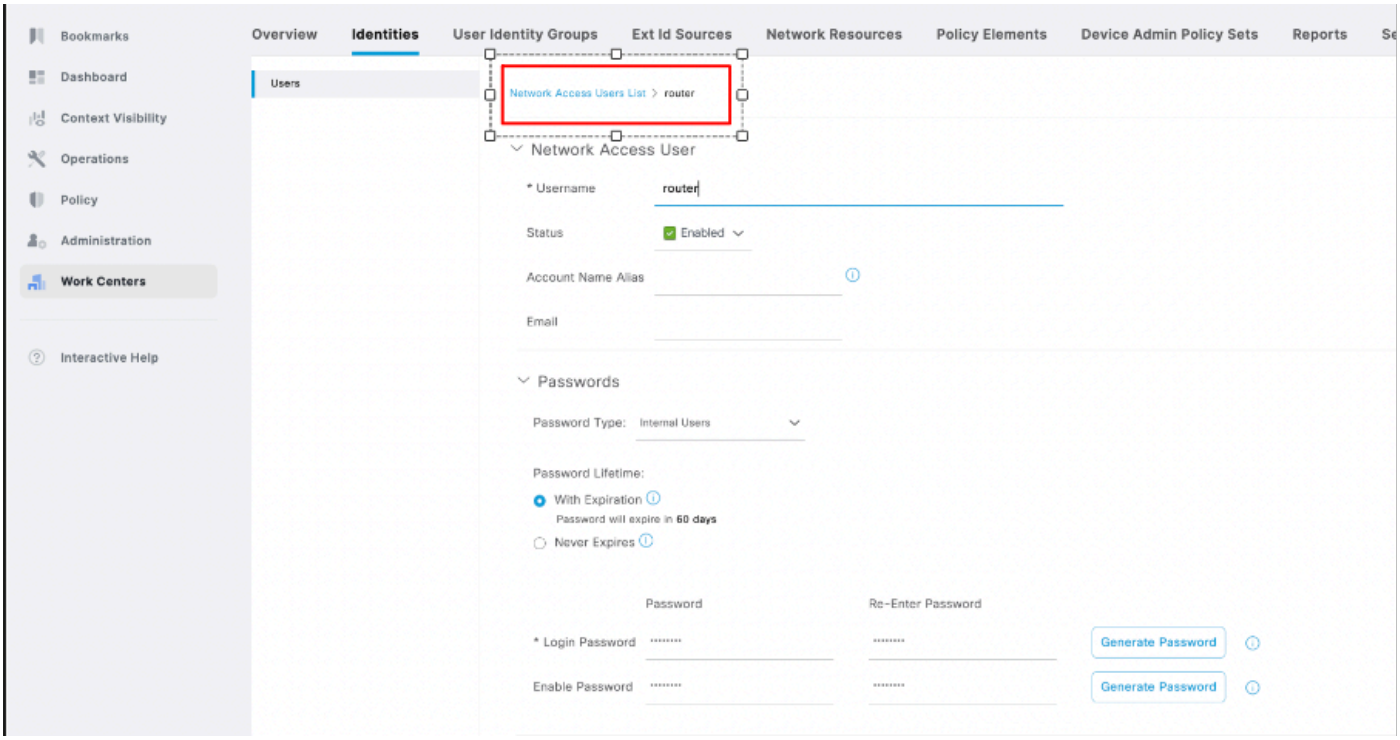
ISE에서 NAD의 TACACS 인증을 위한 네트워크 액세스 사용자 구성

1. Workcenters(작업 센터) -> Device Administration(디바이스 관리) -> Identities(ID) -> Users(사용자)로 이동합니다. 새 사용자를 만들려면 +(더하기) 아이콘을 클릭합니다.



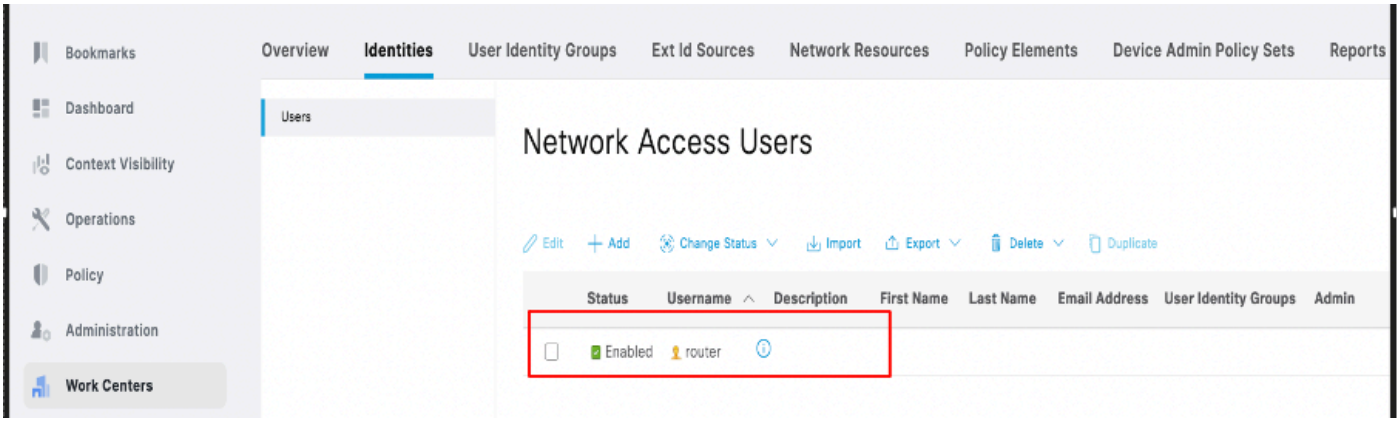
ISE에서 네트워크 액세스 사용자 구성

2. 사용자 이름과 비밀번호 세부 정보를 확장하고 사용자를 사용자 ID 그룹에 매핑합니다(선택 사항). 그런 다음 제출을 누릅니다.



네트워크 액세스 사용자 구성 - 계속

3. Work Centers(작업 센터) -> Identities(ID) -> Users(사용자) -> Network Access users(네트워크 액세스 사용자)에서 사용자 이름 구성을 제출한 후 사용자가 시각적으로 구성 및 활성화됩니다.



TACACS+용 라우터 구성

TACACS+ 인증 및 권한 부여를 위한 Cisco IOS 라우터 구성

1. 라우터의 CLI에 로그인하고 라우터에서 TACACS를 구성하기 위해 다음 명령을 실행합니다.

ASR1001-X(config)#aaa new-model — NAD에서 aaa를 활성화하는 데 필요한 명령

ASR1001-X(config)#aaa session-id common. —NAD에서 aaa를 활성화하는 데 필요한 명령입니다 .

ASR1001-X(config)#aaa 인증 로그인 기본 그룹 tacacs+ 로컬

ASR1001-X(config)#aaa authorization exec default group tacacs+

ASR1001-X(config)#aaa authorization network list1 group tacacs+

ASR1001-X(config)#tacacs 서버 ise1

ASR1001-X(config-server-tacacs)#address ipv4 <TACACS 서버의 IP 주소 > . - ISE 인터페이스 G1 IP 주소.

ASR1001-X(config-server-tacacs)# 키 XXXXX

ASR1001-X(config)# aaa group server tacacs+ isegroup

ASR1001-X(config-sg-tacacs+)#server 이름 ise1

ASR1001-X(config-sg-tacacs+)#ip vrf forwarding Mgmt-intf

ASR1001-X(config-sg-tacacs+)#ip tacacs 소스-인터페이스 GigabitEthernet0

ASR1001-X(config-sg-tacacs+)#ip tacacs 소스-인터페이스 GigabitEthernet1

ASR1001-X(구성)#exit

2. 라우터 TACACS+ 컨피그레이션을 저장한 후 show run aaa 명령을 사용하여 TACACS+ 컨피그레이션을 확인합니다.

ASR1001-X#show run aaa

!

aaa 인증 로그인 기본 그룹 isegroup local

aaa authorization exec 기본 그룹 isegroup

aaa authorization network list1 group isegroup

사용자 이름 admin 비밀번호 0 XXXXXXX

!

tacacs 서버 ise1

주소 ipv4 <TACACS 서버의 IP 주소>

키 XXXXX

!

!

aaa 그룹 서버 tacacs+ isegroup

서버 이름 ise1

ip vrf 전달 관리-intf

ip tacacs 소스 인터페이스 GigabitEthernet1

!

!

!

aaa 새 모델

aaa session-id common

!

!

TACACS+용 스위치 구성

TACACS+ 인증 및 권한 부여를 위한 스위치 구성

1. 스위치의 CLI에 로그인하고 스위치에서 TACACS를 구성하기 위해 다음 명령을 실행합니다.

C9200L-48P-4X#구성 t

한 줄에 하나씩 컨피그레이션 명령을 입력합니다. CNTL/Z로 종료합니다.

C9200L-48P-4X(config)#aaa 새 모델. — NAD에서 aaa를 활성화하는 데 필요한 명령

C9200L-48P-4X(config)#aaa session-id common. —NAD에서 aaa를 활성화하는 데 필요한 명령입니다.

C9200L-48P-4X(config)#aaa 인증 로그인 기본 그룹 isegroup local

C9200L-48P-4X(config)#aaa authorization exec default group isegroup

C9200L-48P-4X(config)#aaa authorization network list1 group isegroup

C9200L-48P-4X(config)#tacacs 서버 ise1

C9200L-48P-4X(config-server-tacacs)#address ipv4 <TACACS 서버의 IP 주소> — ISE 인터페이스 G1 IP 주소.

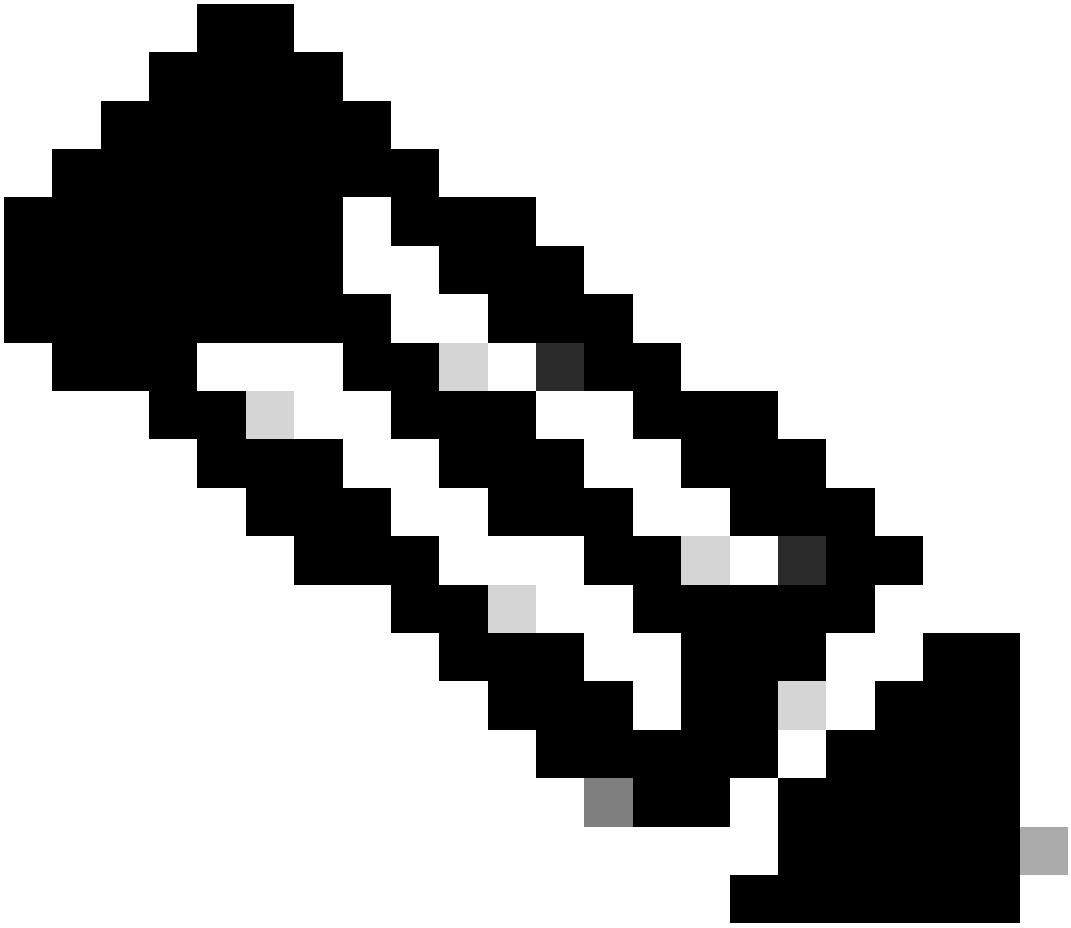
C9200L-48P-4X(config-server-tacacs)#key XXXXX

C9200L-48P(config)#aaa group server tacacs+ isegroup

C9200L-48P(config-sg-tacacs+)#server 이름 ise1

C9200L-48P-4X(config)#exit

C9200L-48P-4X#wr 메모리



참고: NAD TACACS+ 컨피그레이션에서 tacacs+는 구축 요구 사항에 따라 맞춤화할 수 있는 그룹입니다.

---

2. 스위치 TACACS+ 컨피그레이션을 저장한 후 show run aaa 명령을 사용하여 TACACS+ 컨피그레이션을 확인합니다.

C9200L-48P#show run aaa

!

aaa 인증 로그인 기본 그룹 isegroup local

aaa authorization exec 기본 그룹 isegroup

aaa authorization network list1 group isegroup

사용자 이름 admin 비밀번호 0 XXXXX

!

!

tacacs 서버 ise1

주소 ipv4 <TACACS 서버의 IP 주소>

키 XXXXX

!

!

aaa 그룹 서버 tacacs+ isegroup

서버 이름 ise1

!

!

!

aaa 새 모델

aaa session-id common

!

!

확인

라우터에서 확인

라우터의 CLI에서 test aaa group tacacsgroupname username password new 명령을 사용하여 기가비트 이더넷 1 인터페이스를 사용하는 ISE에 대한 TACACS+의 실제 인증을 수행합니다.

다음은 라우터 및 ISE의 샘플 출력입니다.

라우터에서 포트 49 확인:

ASR1001-X#telnet ISE Gig 1 인터페이스 IP 49

ISE GIg 1 인터페이스 IP, 49 시도 중... 열기

ASR1001-X#test aaa group isegroup router XXXX 신규

암호 전송 중

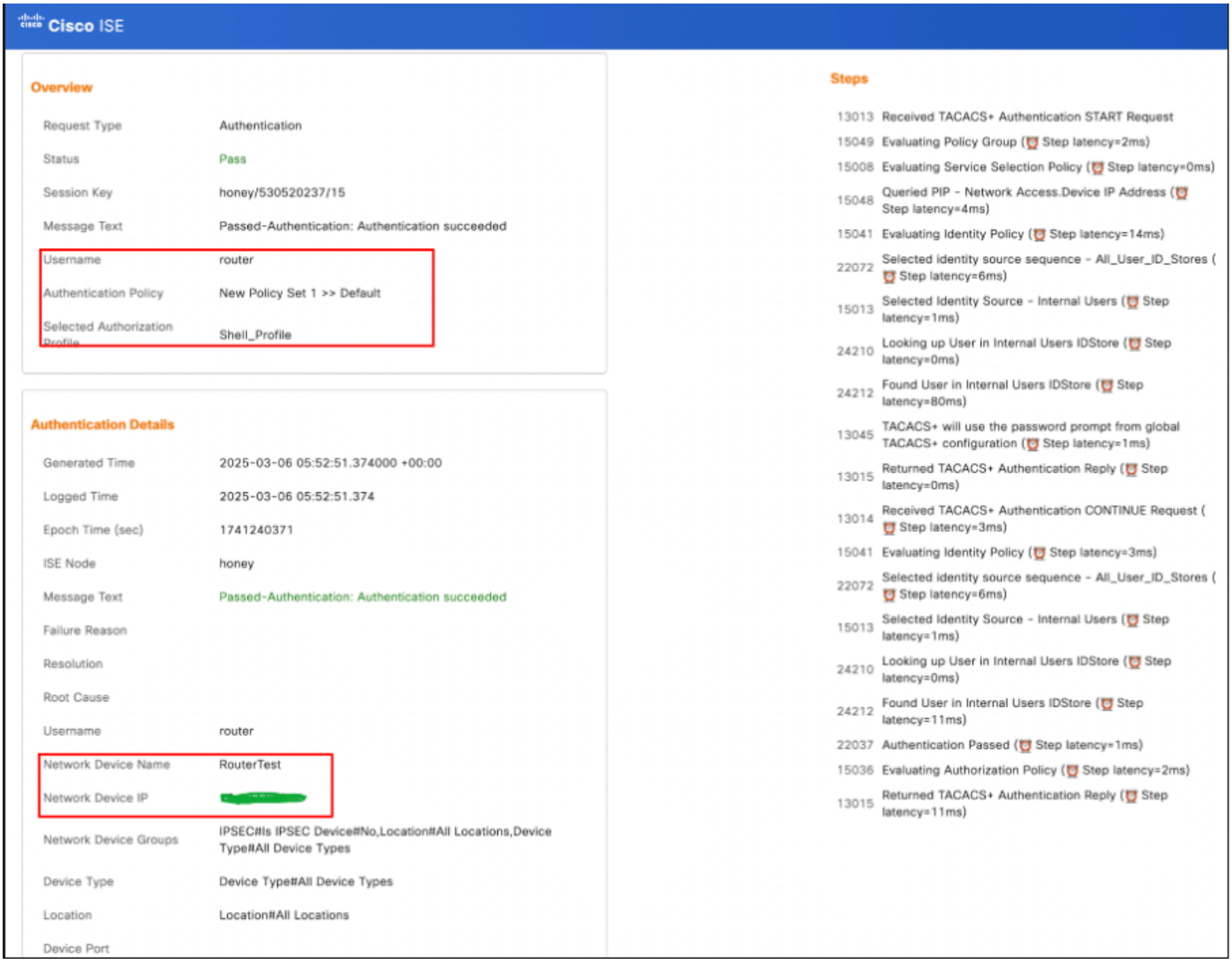
사용자를 인증했습니다.

사용자 특성

사용자 이름 0 "라우터"

reply-message 0 "암호:"

ISE에서 확인하려면 GUI -> Operations(작업) -> TACACS live logs(TACACS 라이브 로그)에 로그인한 다음, Network Device Details(네트워크 디바이스 세부사항) 필드에서 라우터 IP로 필터링합니다.



ISE의 TACACS 라이브 로그 - 라우터 확인

스위치 확인

스위치의 CLI에서 test aaa group tacacsgroupname username password newn 명령을 사용하여 기가비트 이더넷 1 인터페이스를 사용하는 ISE에 대한 TACACS+의 인증을 확인합니다.

다음은 switch & ISE의 샘플 출력입니다.

스위치에서 포트 49 확인:

C9200L-48P# 텔넷 ISE Gig1 인터페이스 IP 49

ISE Gig1 인터페이스 IP, 49 시도 중... 열기

C9200L-48P#test aaa group isegroup switch XXXX new

암호 전송 중

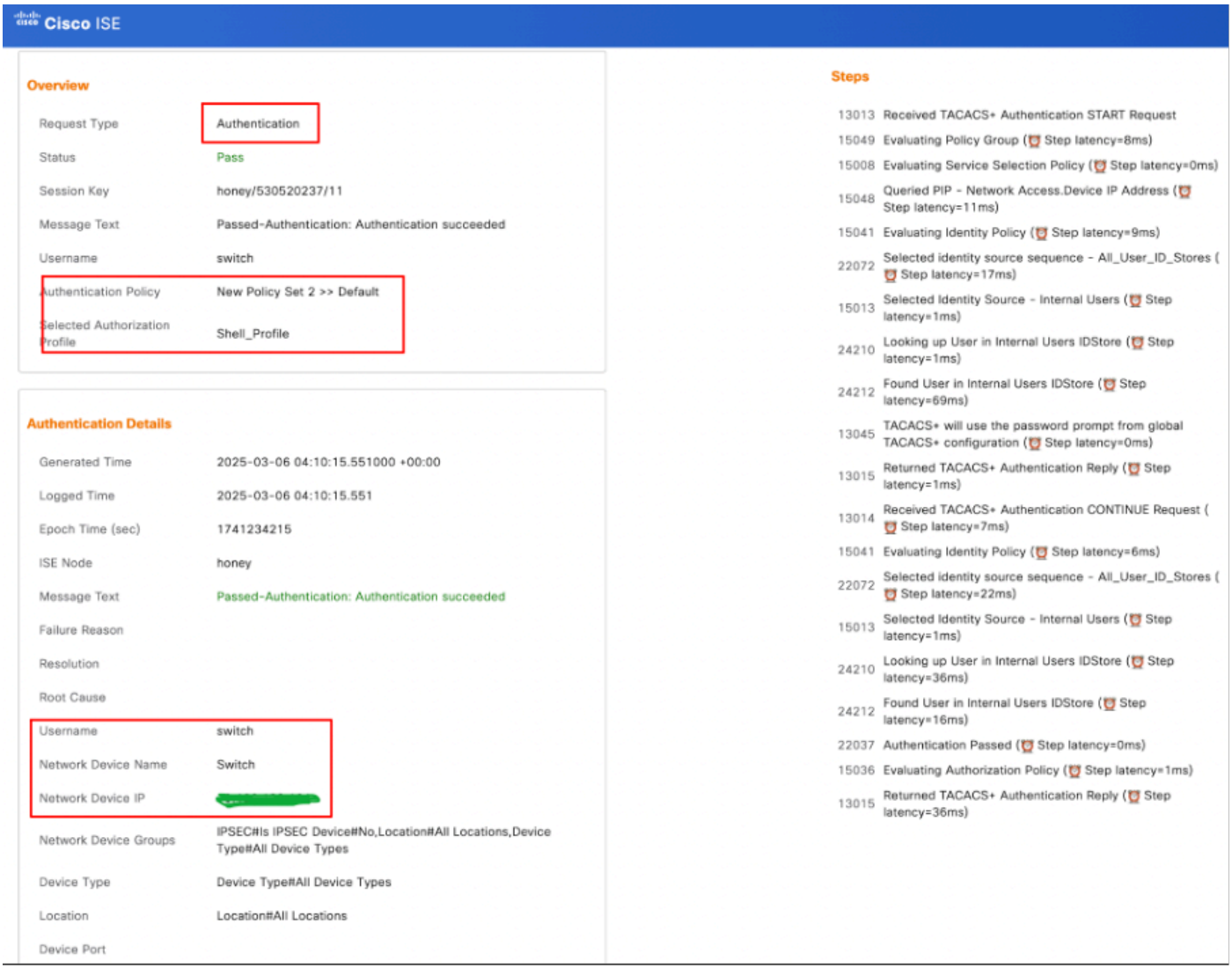
사용자를 인증했습니다.

사용자 특성

사용자 이름 0 "switch"

reply-message 0 "암호:"

ISE에서 확인하려면 GUI -> Operations(작업) -> TACACS live logs(TACACS 라이브 로그)에 로그인한 다음, Network Device Details(네트워크 디바이스 세부 정보) 필드에서 스위치 IP로 필터링합니다.



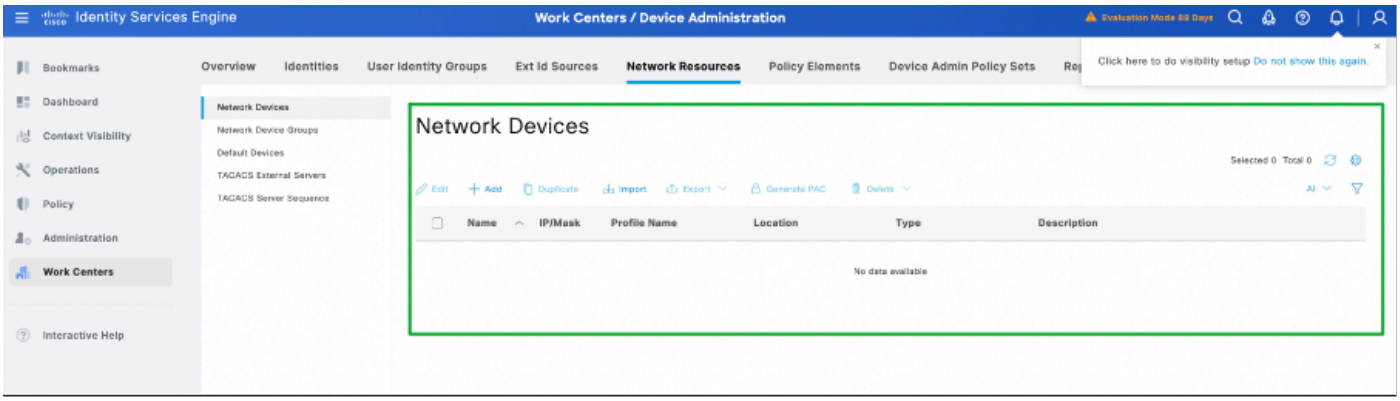
ISE의 TACACS 라이브 로그 - 스위치 확인.

문제 해결

이 섹션에서는 TACACS+ 인증과 관련하여 발견되는 몇 가지 일반적인 문제에 대해 설명합니다.

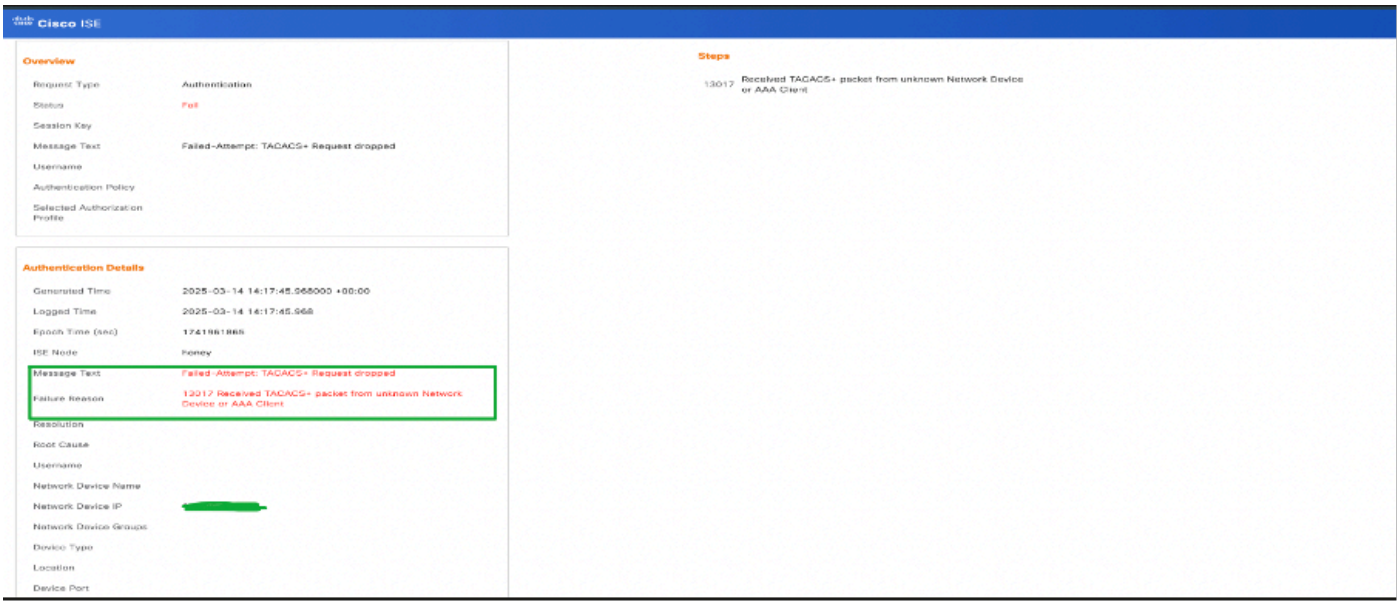
시나리오 1: TACACS+ 인증이 "오류: 13017 Network Device or AAA Client에서 TACACS+ 패킷을 받았습니다."

이 시나리오는 네트워크 디바이스가 ISE에서 네트워크 리소스로 추가되지 않을 때 발생합니다. 이 스크린샷에서 볼 수 있듯이 스위치는 ISE의 네트워크 리소스에 추가되지 않습니다.



문제 해결 시나리오 - 네트워크 디바이스가 ISE에 추가되지 않았습니다.

이제 스위치/네트워크 디바이스에서 인증을 테스트하면 패킷이 예상대로 ISE에 도달합니다. 그러나 "오류: 13017 스크린샷과 같이 " Received TACACS+ packet from unknown Network Device or AAA Client(알 수 없는 네트워크 디바이스 또는 AAA 클라이언트에서 TACACS+ 패킷 수신)"를 선택합니다.



TACACS 라이브 로그 - 네트워크 디바이스가 ISE에 추가되지 않은 경우 실패.

네트워크 디바이스(스위치)에서 확인

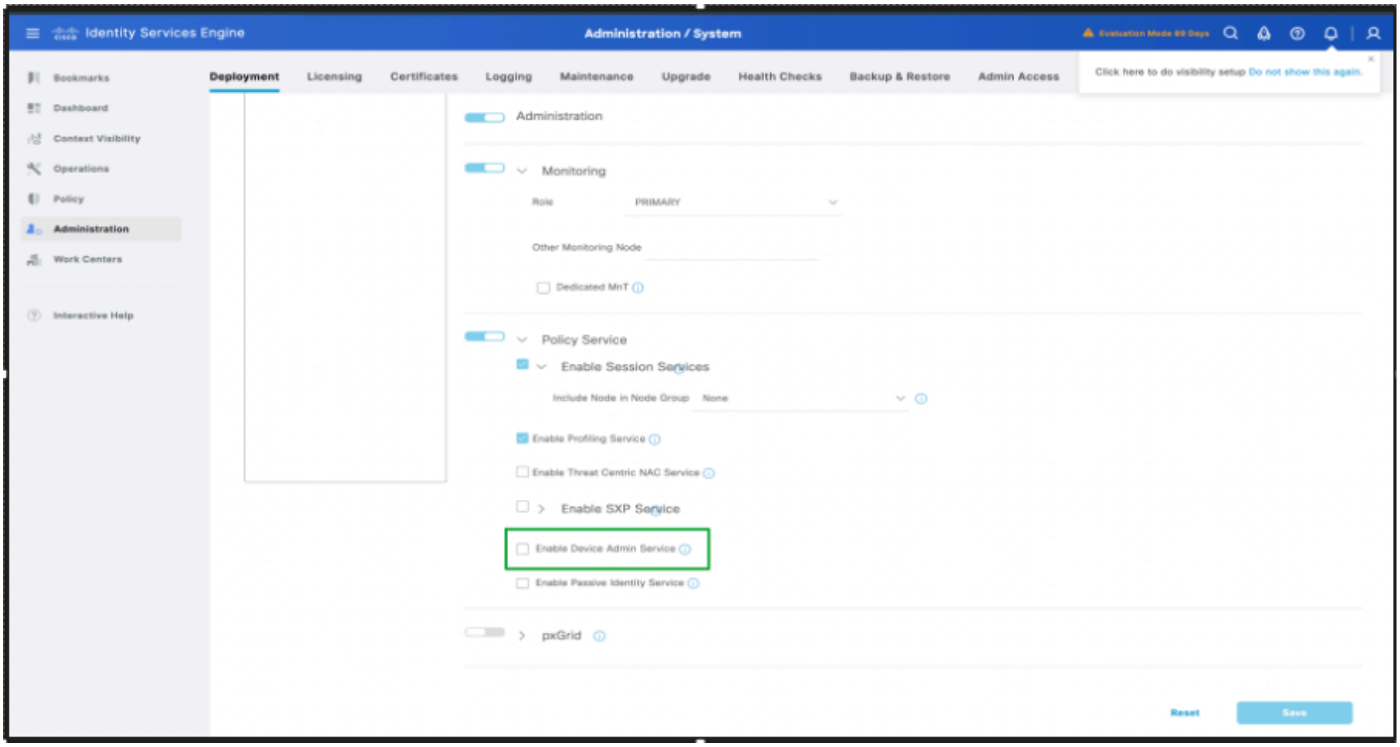
Switch#test aaa group isegroup switch XXXXXX new(스위치#테스트 aaa 그룹 isegroup 스위치 XXXXXX 신규)
사용자 거부됨

해결책: 스위치/라우터/네트워크 디바이스가 ISE의 네트워크 디바이스로 추가되었는지 확인합니다. 디바이스가 추가되지 않은 경우 ISE의 네트워크 디바이스 목록에 네트워크 디바이스를 추가합니다.

시나리오 2: ISE는 아무 정보 없이 TACACS+ 패킷을 자동으로 삭제합니다.

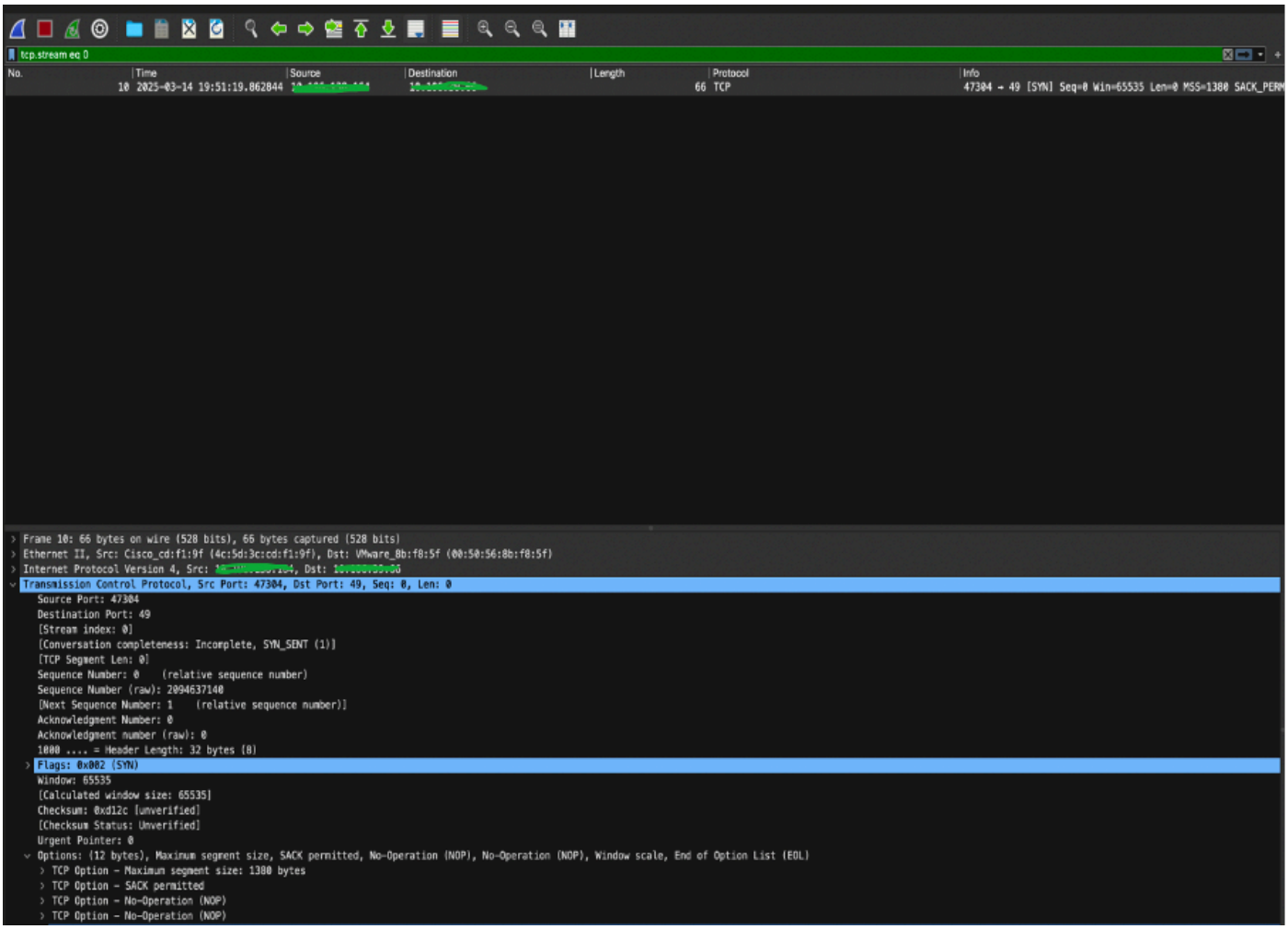
이 시나리오는 ISE에서 Device Administration Service가 비활성화될 때 발생합니다. 이 시나리오에서 ISE는 패킷을 삭제하고 ISE의 네트워크 리소스에 추가된 네트워크 디바이스에서 인증이 시작되더라도 라이브 로그가 표시되지 않습니다.

이 스크린샷에서 보여주는 것처럼, ISE에서 Device Administration(디바이스 관리)이 비활성화됩니다.



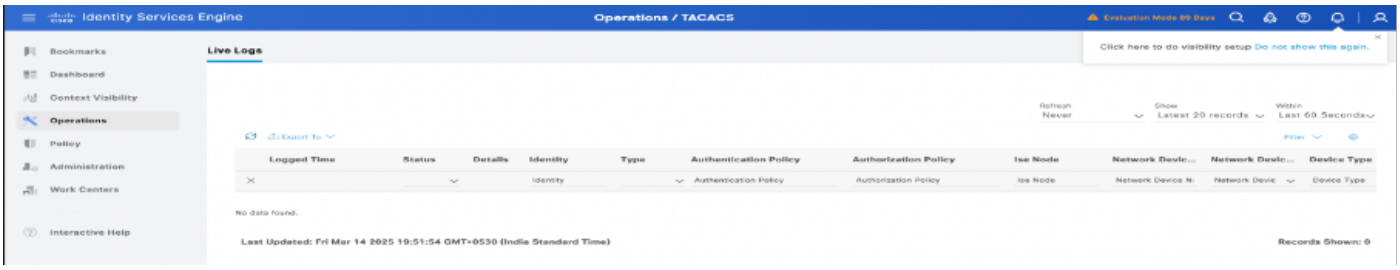
시나리오: 디바이스 관리가 ISE에서 활성화되지 않습니다.

사용자가 네트워크 디바이스에서 인증을 시작하면 ISE는 라이브 로그에 정보 없이 패킷을 자동으로 삭제하고 ISE는 TACACS 인증 프로세스를 완료하기 위해 네트워크 디바이스에서 보낸 Syn 패킷에 응답하지 않습니다. 다음 스크린샷을 참조하십시오.



TACACS 중에 ISE가 패킷을 자동으로 삭제

ISE는 인증 동안 라이브 로그를 표시하지 않습니다.



TACACS 라이브 로그 없음 - ISE에서 확인

네트워크 디바이스(스위치)에서 확인

스위치 번호
Switch#test aaa group isegroup switch XXXX new(스위치#테스트 aaa 그룹 isegroup 스위치 XXXX 신규)
사용자 거부됨
스위치 번호
*3월 14일 13:54:28.144: T+: 버전 192(0xC0), 유형 1, 시퀀스 1, 암호화 1, SC 0
*3월 14일 13:54:28.144: T+: session_id 10158877(0x9B031D), dlen 14(0xE)
*3월 14일 13:54:28.144: T+: type:AUTHEN/START, priv_lvl:15 action:LOGIN ascii
*3월 14일 13:54:28.144: T+: svc:LOGIN user_len:6 port_len:0 (0x0) raaddr_len:0 (0x0) data_len:0
*3월 14일 13:54:28.144: T+: 사용자: 스위치
*3월 14일 13:54:28.144: T+: 포트:
*3월 14일 13:54:28.144: T+: rem_addr:
*3월 14일 13:54:28.144: T+: 데이터:
*3월 14일 13:54:28.144: T+: 패킷 종료

해결책: ISE에서 디바이스 관리를 활성화합니다.

참조

- TACACS 인증 문제 해결
- Cisco Identity Services Engine 관리자 가이드, 릴리스 3.3
- TACACS 서버용 VRF

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.