ISE를 사용하는 IOS XR 디바이스에서 TLS 1.3을 통한 TACACS+ 구성

목차

소개

이 문서에서는 Cisco ISE(Identity Services Engine)를 서버로, Cisco IOS® XR 디바이스를 클라이언트로 사용하는 TACACS+ over TLS의 예를 설명합니다.

개요

TACACS+(Terminal Access Controller Access-Control System Plus) 프로토콜[RFC8907]은 하나 이상의 TACACS+ 서버를 통해 라우터, 네트워크 액세스 서버 및 기타 네트워크 디바이스에 대한 중앙 집중식 디바이스 관리를 가능하게 합니다. 특히 디바이스 관리 활용 사례에 맞게 맞춤화된 AAA(Authentication, Authorization, and Accounting) 서비스를 제공합니다.

TACACS+ over TLS 1.3 [RFC8446]은 보안 전송 계층을 도입하여 프로토콜을 개선하고 매우 중요한 데이터를 보호합니다. 이러한 통합으로 TACACS+ 클라이언트와 서버 간의 연결 및 네트워크 트래픽에 대한 기밀성, 무결성 및 인증이 보장됩니다.

설명서 사용

이 설명서에서는 작업을 두 부분으로 나누어 ISE가 Cisco IOS XR 기반 네트워크 디바이스에 대한 관리 액세스를 관리할 수 있도록 합니다.
· 1부 - 디바이스 관리를 위한 ISE 구성
· 2부 - TACACS+ over TLS용 Cisco IOS XR 구성

사전 요구 사항

요구 사항

TLS를 통해 TACACS+를 구성하기 위한 요구 사항:

- TACACS+에서 TLS를 통해 ISE 및 네트워크 디바이스의 인증서를 서명하는 데 사용되는 인증서를 서명하는 CA(Certificate Authority).
- CA(Certificate Authority)의 루트 인증서
- 네트워크 디바이스 및 ISE는 DNS 연결성을 가지며 호스트 이름을 확인할 수 있습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ISE VMware 가상 어플라이언스, 릴리스 3.4 패치 2
- Cisco 8201 Router, 릴리스 25.3.1

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.

라이센싱

Device Administration 라이센스를 사용하면 정책 서비스 노드에서 TACACS+ 서비스를 사용할 수 있습니다. 고가용성(HA) 독립형 구축에서 디바이스 관리 라이센스를 사용하면 HA 쌍의 단일 정책 서비스 노드에서 TACACS+ 서비스를 사용할 수 있습니다.

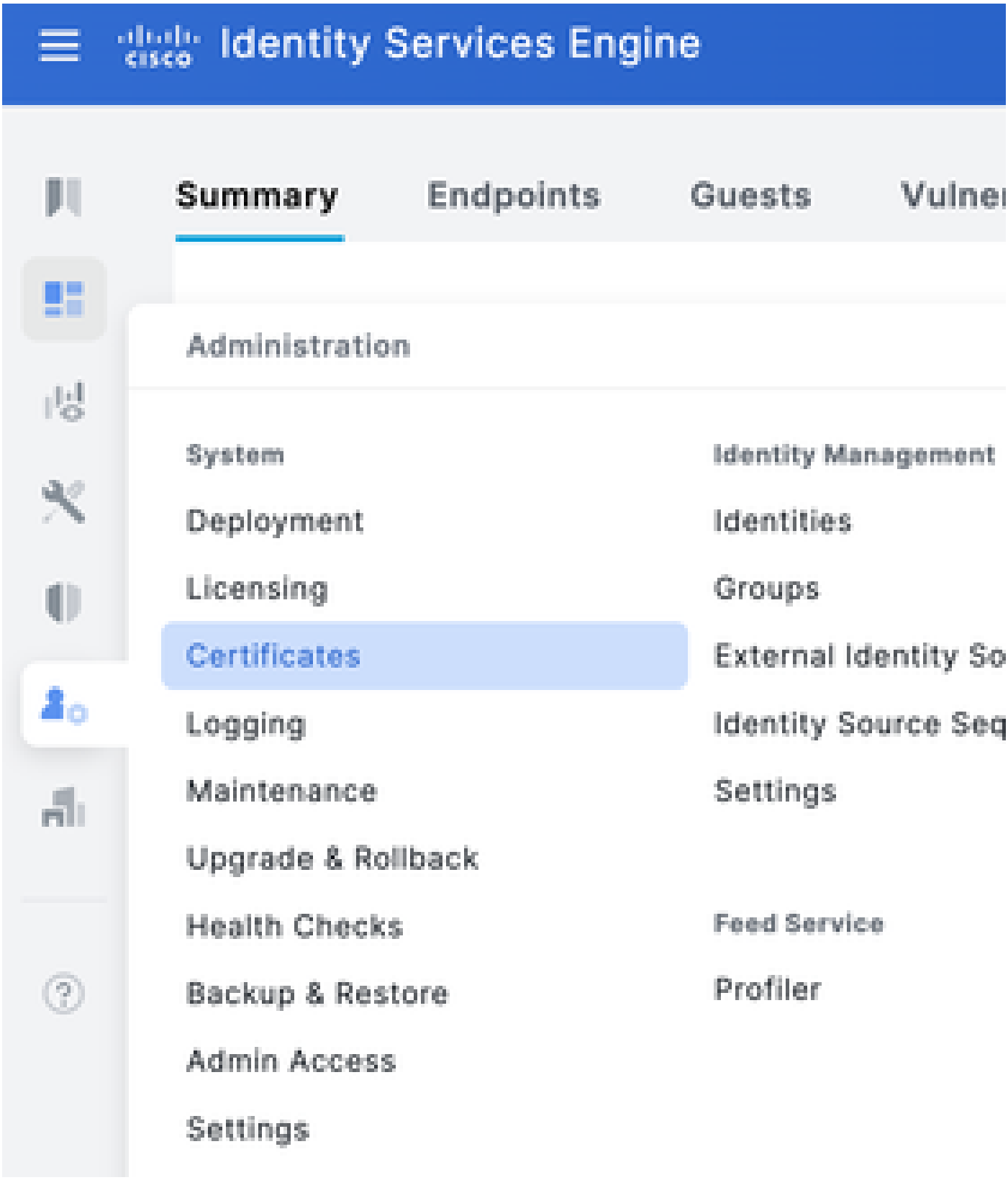
1부 - 디바이스 관리를 위한 ISE 컨피그레이션

TACACS+ 서버 인증을 위한 인증서 서명 요청 생성

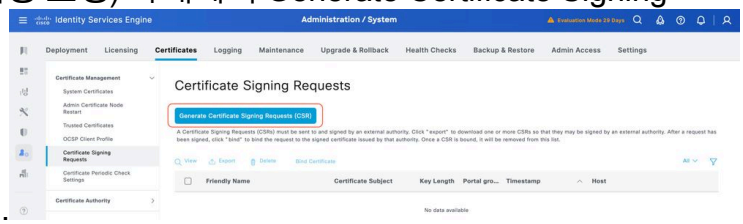
1단계. 지원되는 브라우저 중 하나를 사용하여 ISE 관리 웹 포털에 로그인합니다.

기본적으로 ISE는 모든 서비스에 자체 서명 인증서를 사용합니다. 첫 번째 단계는 CSR(Certificate Signing Request)을 생성하여 CA(Certificate Authority)에서 서명하도록 하는 것입니다.

2단계. Administration(관리) > System(시스템) > Certificates(인증서)로 이동합니다.

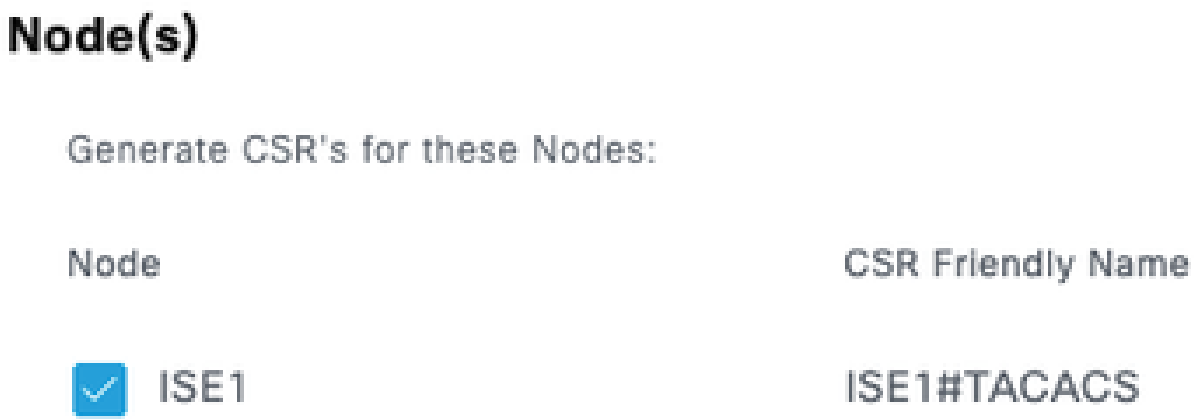


3단계. Certificate Signing Requests(인증서 서명 요청) 아래에서 Generate Certificate Signing Request(인증서 서명 요청 생성)를 클릭합니다.

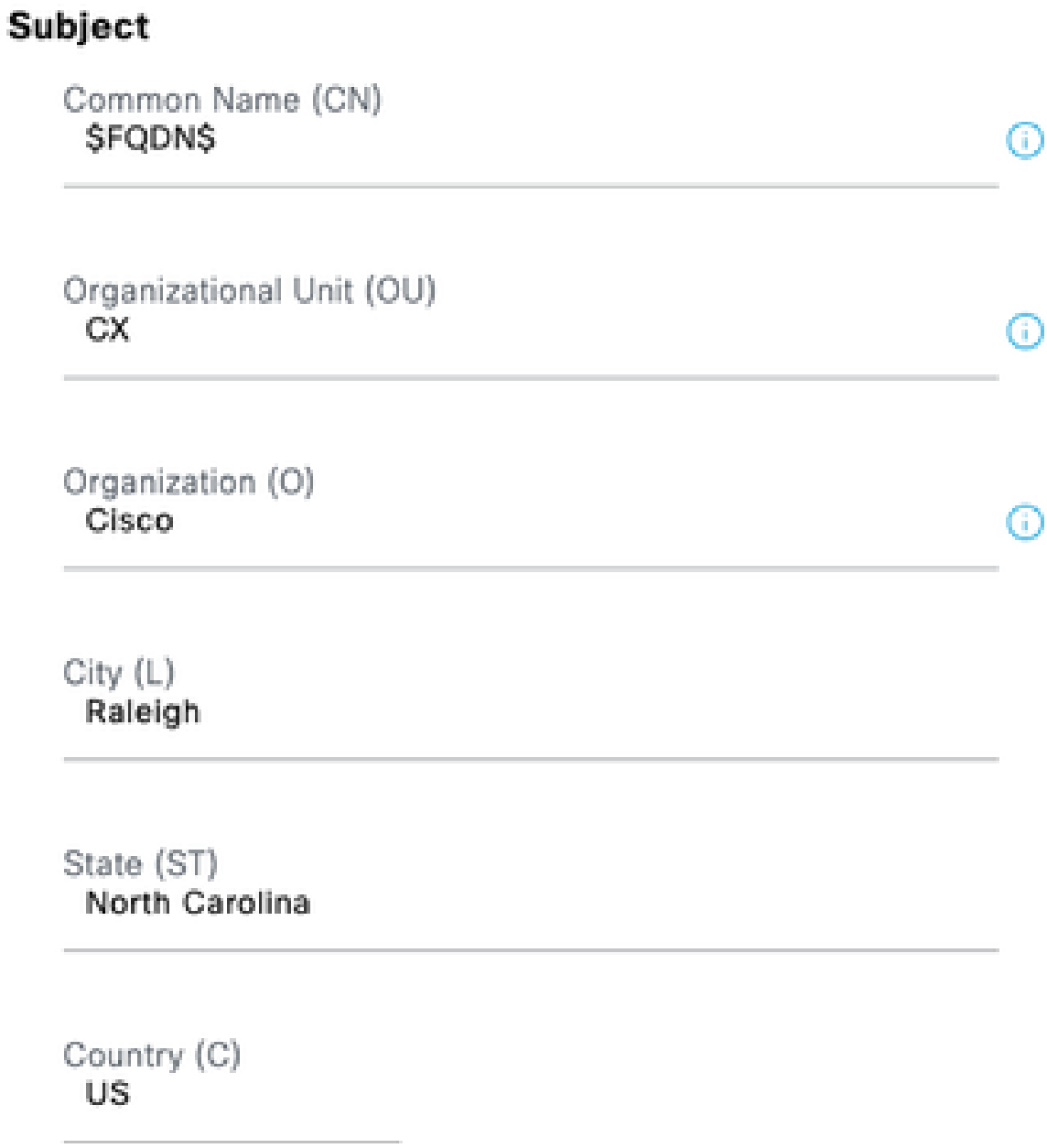


4단계. TACACS inUsage를 선택합니다.

5단계. TACACS+가 활성화된 PSN을 선택합니다.

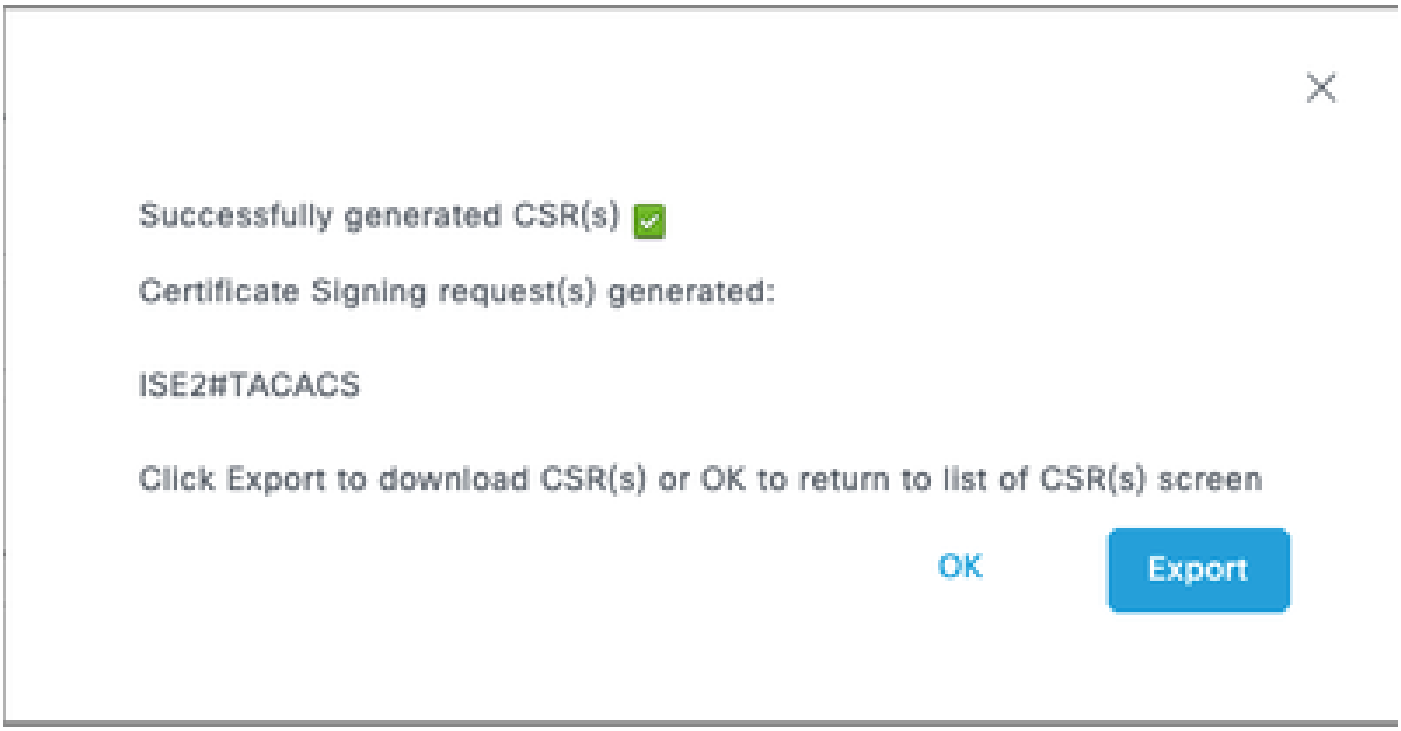


6단계. Subject(제목) 필드에 적절한 정보를 입력합니다.



7단계. SAN(Subject Alternative Name)에 DNS 이름 및 IP 주소를 추가합니다.

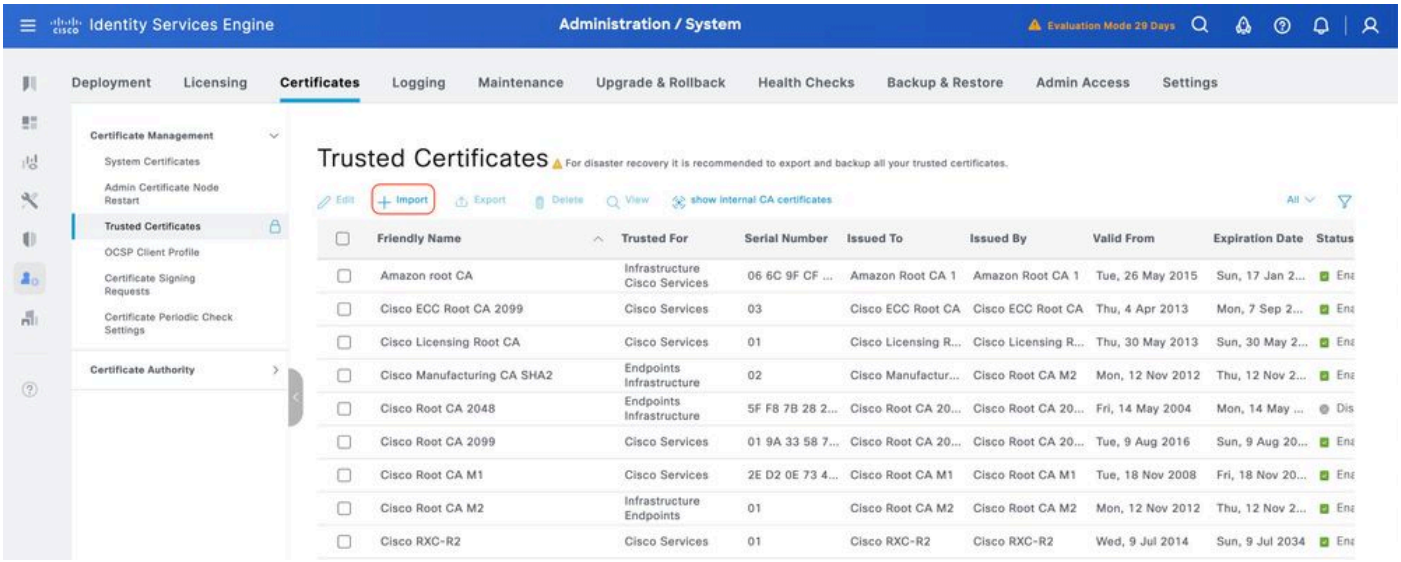
8단계. Generate(생성)를 클릭한 다음 Export(내보내기)를 클릭합니다.



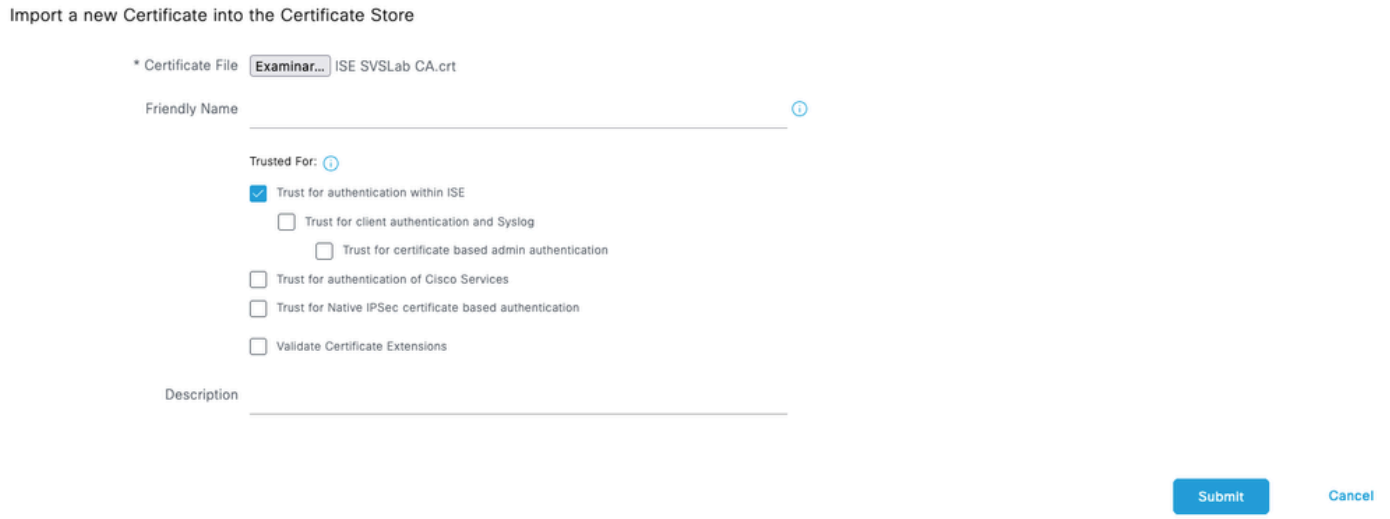
이제 CA(Certificate Authority)에서 서명한 인증서(CRT)를 가질 수 있습니다.

TACACS+ 서버 인증을 위한 루트 CA 인증서 업로드

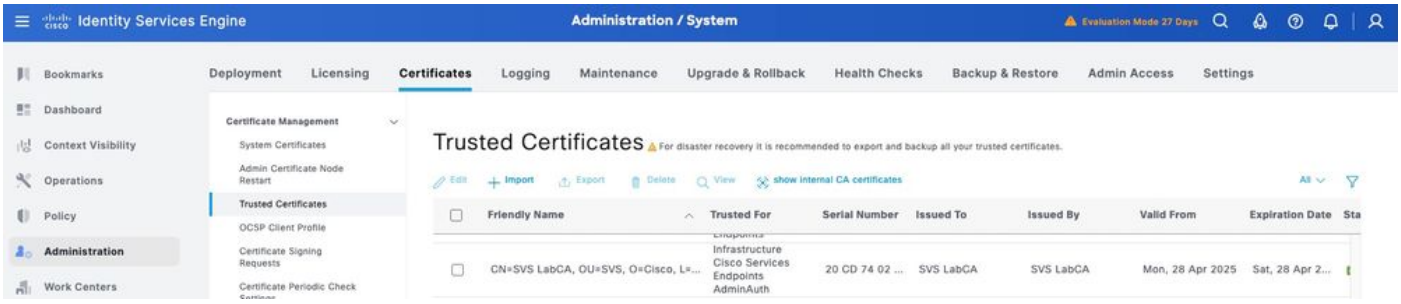
1단계.Administration(관리) > System(시스템) > Certificates(인증서)로 이동합니다. Trusted Certificates(신뢰할 수 있는 인증서) 아래에서 Import(가져오기)를 클릭합니다.



2단계. TACACS CSR(Certificate Signing Request)에 서명한 CA(Certificate Authority)에서 발급한 인증서를 선택합니다. 다음 사항을 확인하십시오. ISE 내 인증 신뢰 옵션을 사용할 수 있습니다.



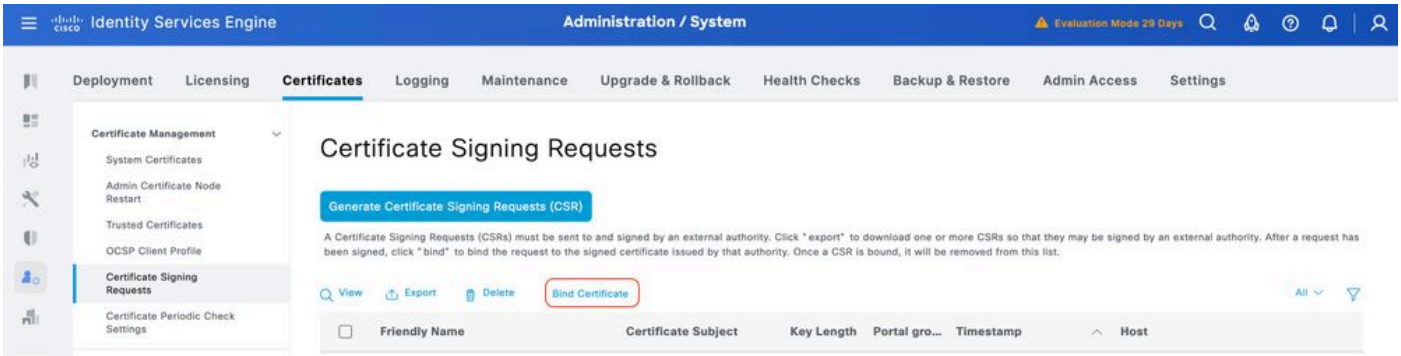
제출을 클릭합니다. 이제 인증서가 Trusted Certificates 아래에 나타나야 합니다.



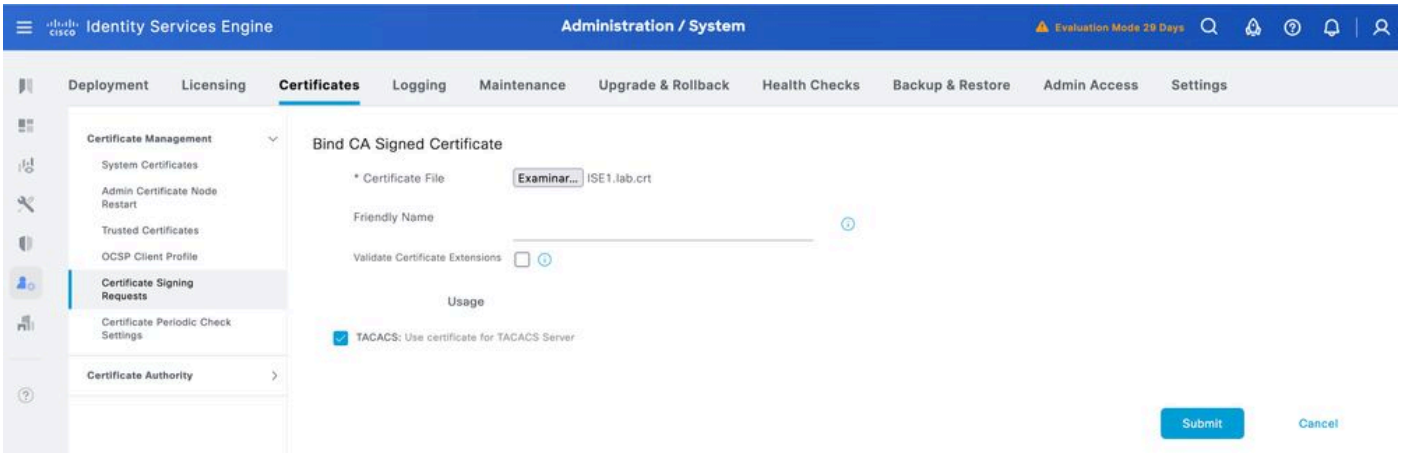
ISE에 서명된 CSR(Certificate Signing Request) 바인딩

CSR(Certificate Signing Request)에 서명하면 ISE에 서명된 인증서를 설치할 수 있습니다.

1단계. Administration(관리) > System(시스템) > Certificates(인증서)로 이동합니다. Certificate Signing Requests(인증서 서명 요청) 아래에서 이전 단계에서 생성된 TACACS CSR을 선택하고 Bind Certificate(인증서 바인딩)를 클릭합니다.

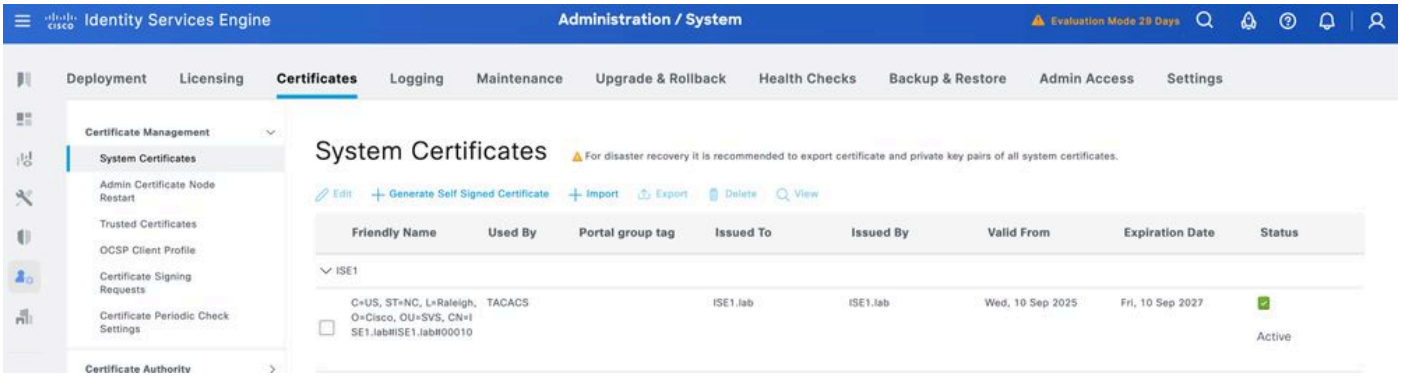


2단계. 서명된 인증서를 선택하고 Usage(사용) 아래의 TACACS(TACACS) 확인란이 선택된 상태로 유지되는지 확인합니다.



3단계. Submit(제출)을 클릭합니다. 기존 인증서 교체에 대한 경고가 표시되면 Yes(예)를 클릭하여 계속 진행합니다.

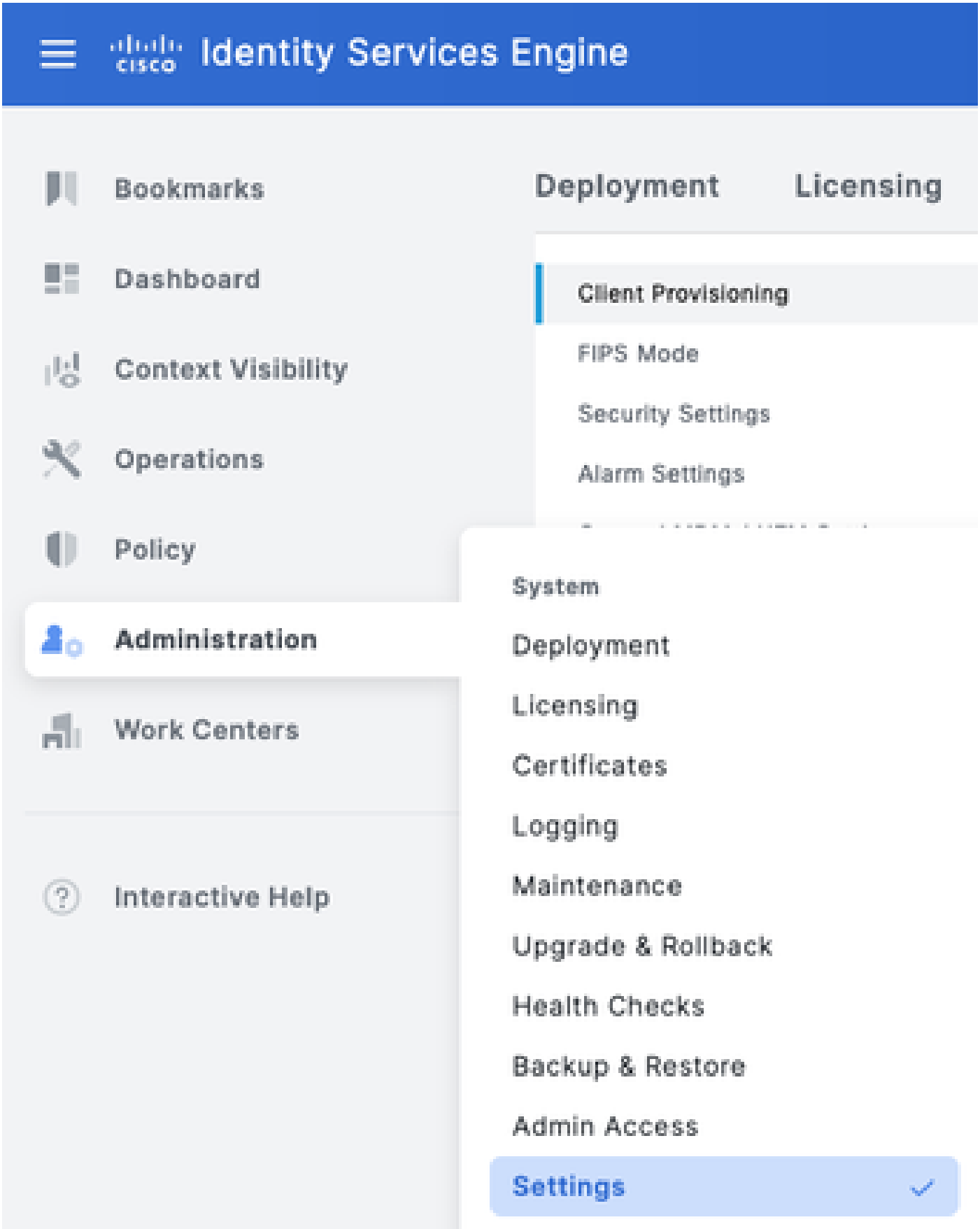
이제 인증서가 올바르게 설치되어야 합니다. System Certificates(시스템 인증서)에서 이를 확인할 수 있습니다.



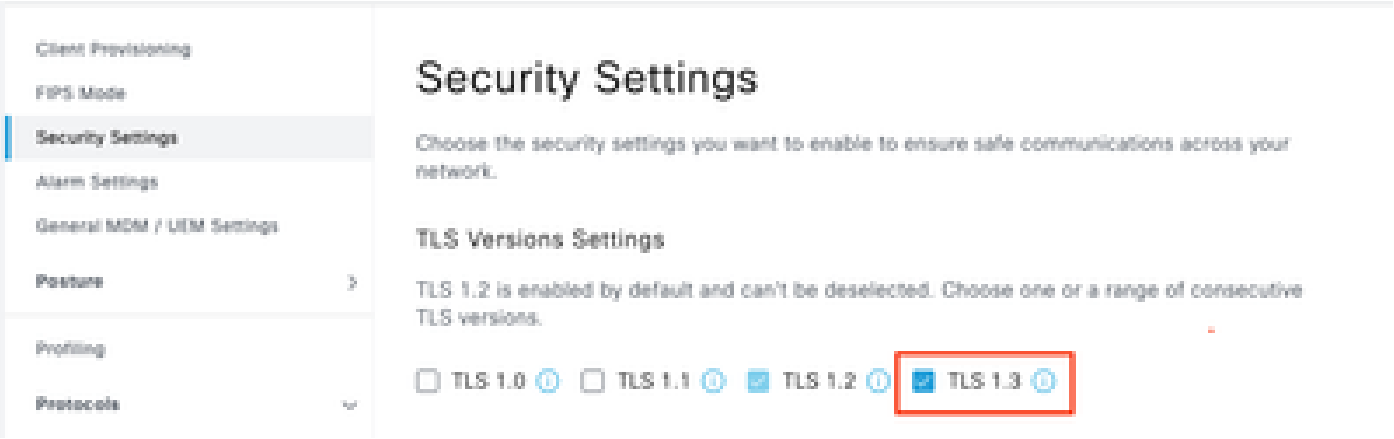
TLS 1.3 활성화

TLS 1.3은 ISE 3.4.x에서 기본적으로 활성화되지 않습니다. 수동으로 활성화해야 합니다.

1단계.Administration(관리) > System(시스템) > Settings(설정)로 이동합니다.



2단계. Security Settings(보안 설정)를 클릭하고 TLS Version Settings(TLS 버전 설정)에서 TLS1.3 옆의 확인란을 선택한 다음 Save(저장)를 클릭합니다.

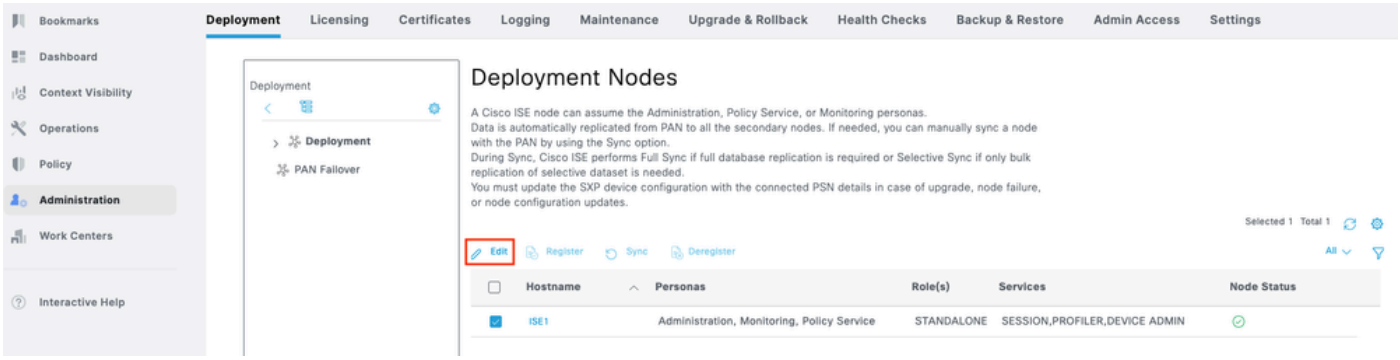


경고: TLS 버전을 변경하면 Cisco ISE 애플리케이션 서버가 모든 Cisco ISE 구축 시스템에서 다시 시작됩니다.

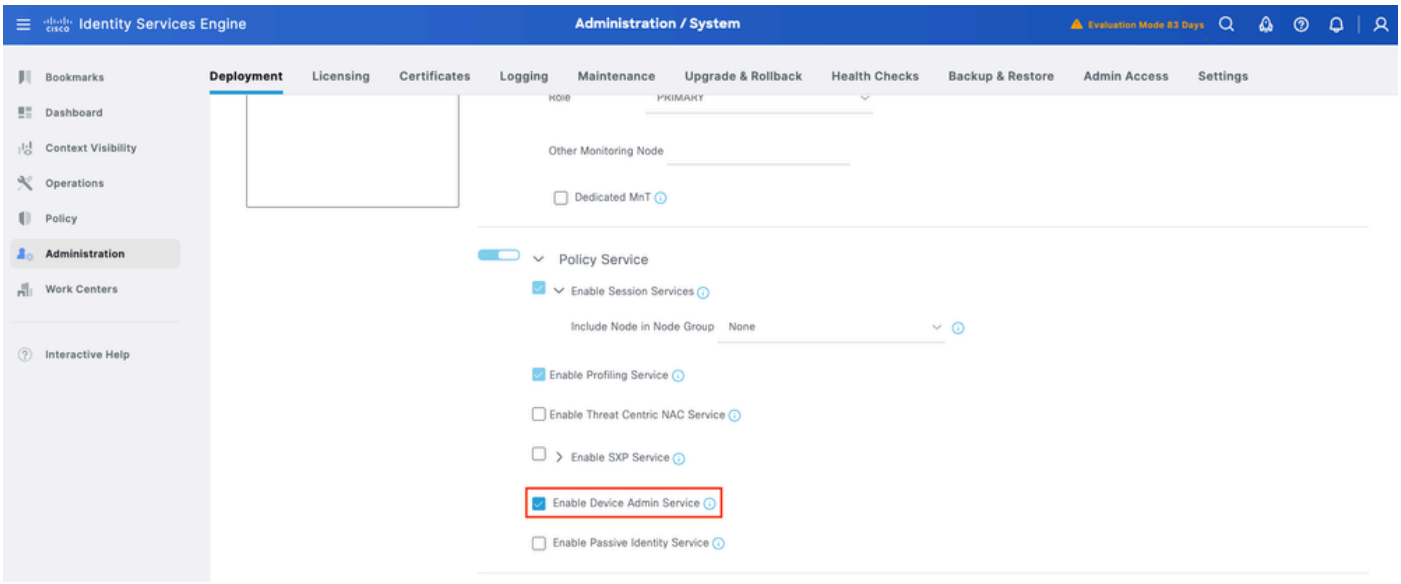
ISE에서 디바이스 관리 활성화

디바이스 관리 서비스(TACACS+)는 ISE 노드에서 기본적으로 활성화되지 않습니다. PSN 노드에서 TACACS+를 활성화하려면

1단계. Administration(관리) > System(시스템) > Deployment(구축)로 이동합니다. ISE 노드 옆의 확인란을 선택하고 Edit를 클릭합니다.



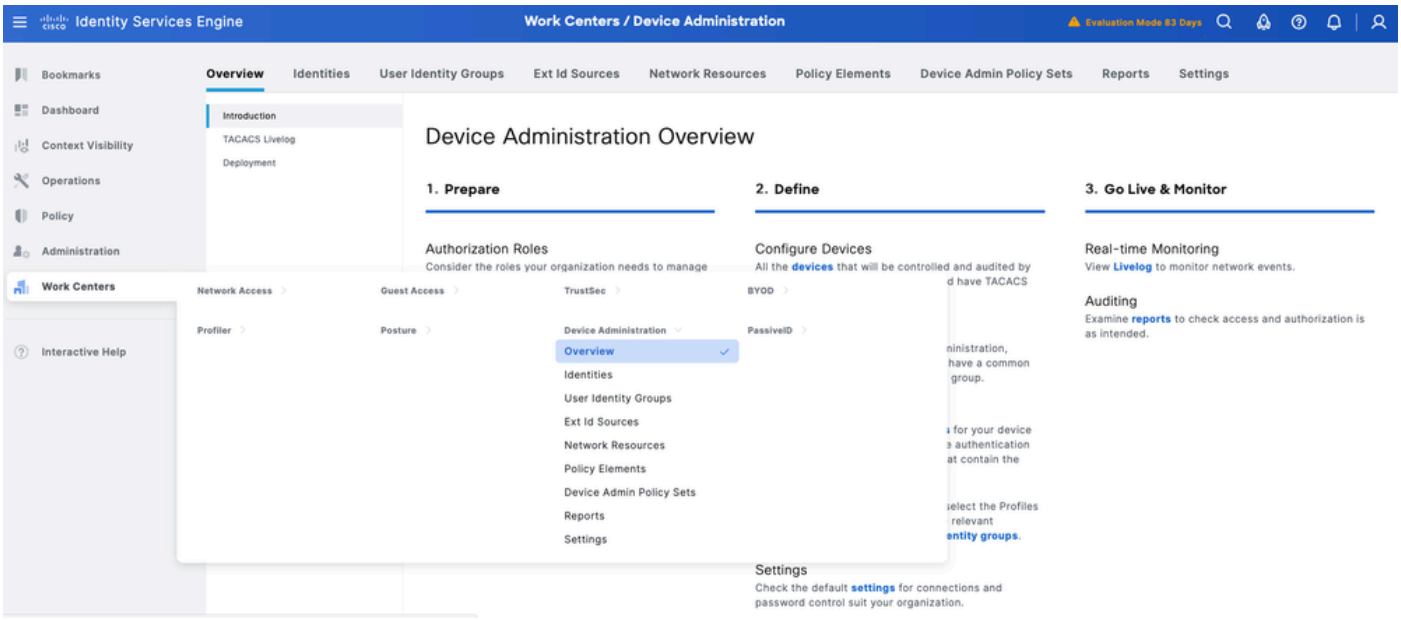
2단계. GeneralSettings(일반 설정)에서 아래로 스크롤하여 Enable Device Admin Service(디바이스 관리 서비스 활성화) 옆의 확인란을 선택합니다.



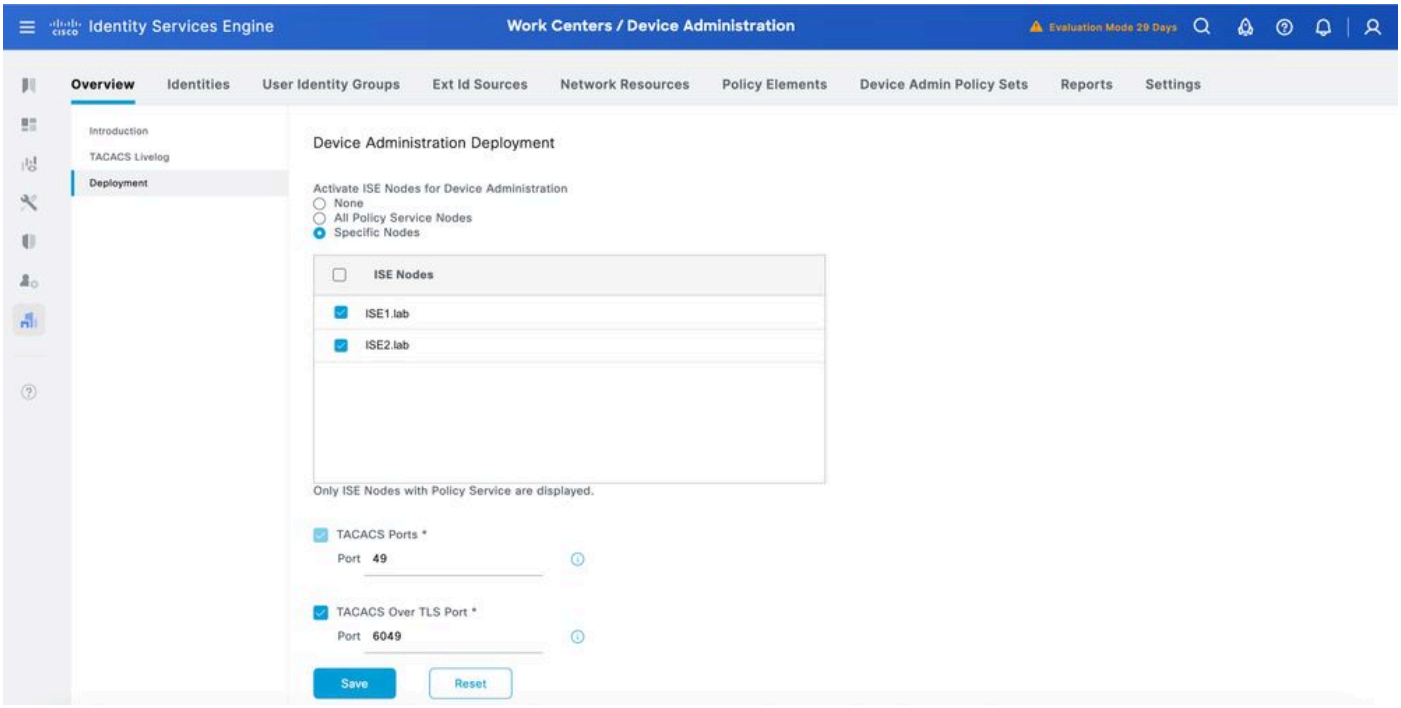
3단계. 구성을 저장합니다. 이제 ISE에서 디바이스 관리 서비스가 활성화됩니다.

TACACS Over TLS 활성화

1단계. Work Centers(작업 센터) > Device Administration(디바이스 관리) > Overview(개요)로 이동합니다.



2단계. Deployment(구축)를 클릭합니다. TACACS over TLS를 활성화할 PSN 노드를 선택합니다.

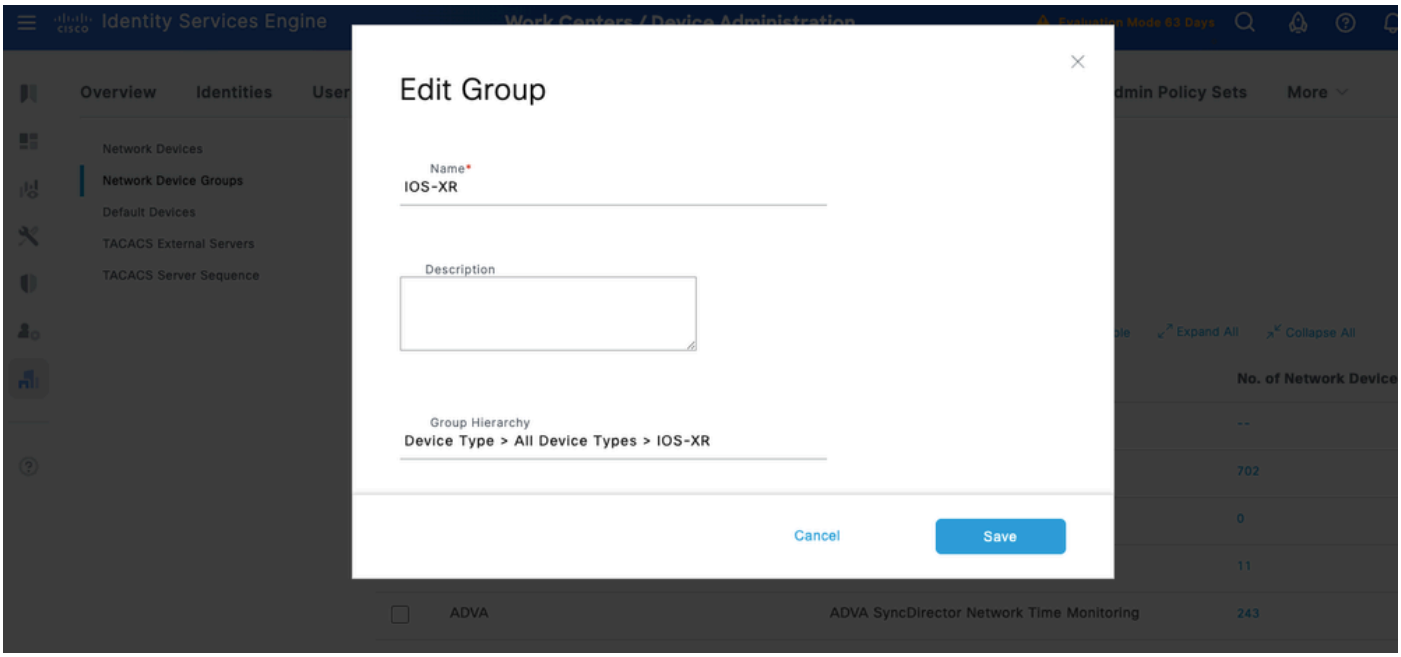


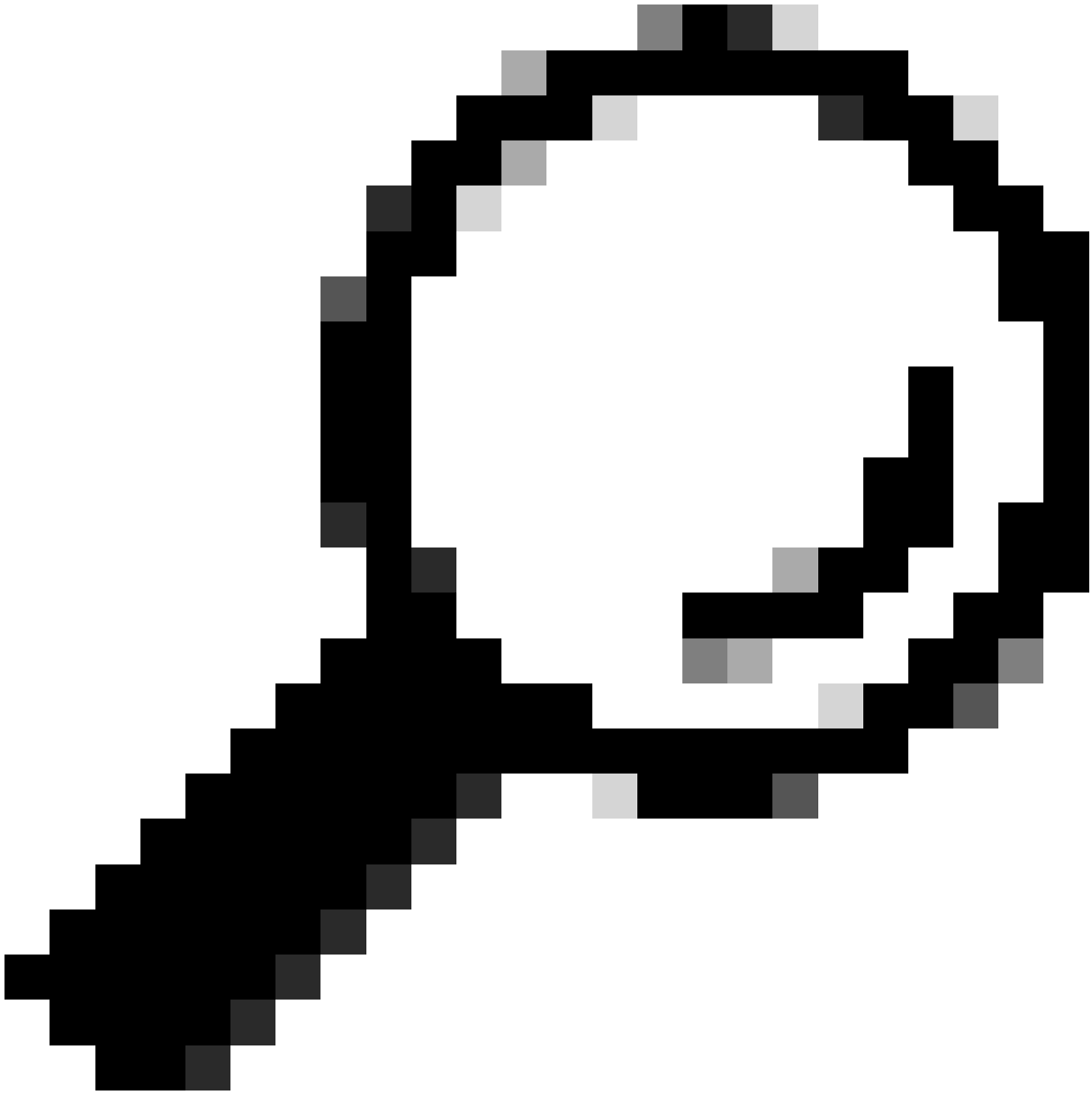
3단계. 기본 포트 6049를 유지하거나 TACACS over TLS에 대해 다른 TCP 포트를 지정한 다음 Save를 클릭합니다.

네트워크 디바이스 및 네트워크 디바이스 그룹 생성

ISE는 여러 디바이스 그룹 계층을 사용하여 강력한 디바이스 그룹화를 제공합니다. 각 계층 구조는 네트워크 장치의 개별적이고 독립적인 분류를 나타냅니다.

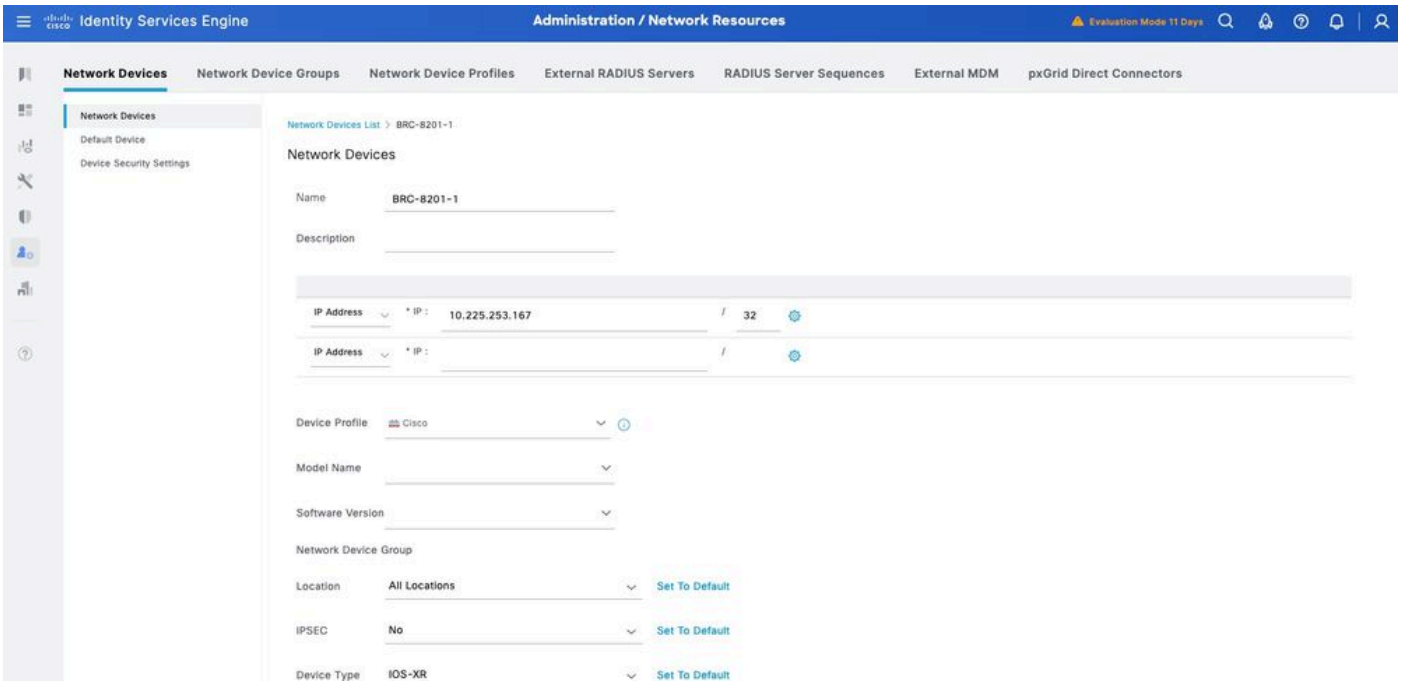
1단계. Work Centers(작업 센터) > Device Administration(디바이스 관리) > Network Resources(네트워크 리소스)로 이동합니다.Network Device Groups(네트워크 디바이스 그룹)를 클릭하고 이름이 IOS XR인 그룹을 생성합니다.


Identity Services Engine
Work Centers / Device Administration
Overview
Identities
User
Admin Policy Sets
More
Network Devices
Network Device Groups
Default Devices
TACACS External Servers
TACACS Server Sequence
Expand All
Collapse All
No. of Network Device
Edit Group
Name*
IOS-XR
Description
Group Hierarchy
Device Type > All Device Types > IOS-XR
Cancel
Save
ADVA
ADVA SyncDirector Network Time Monitoring
243

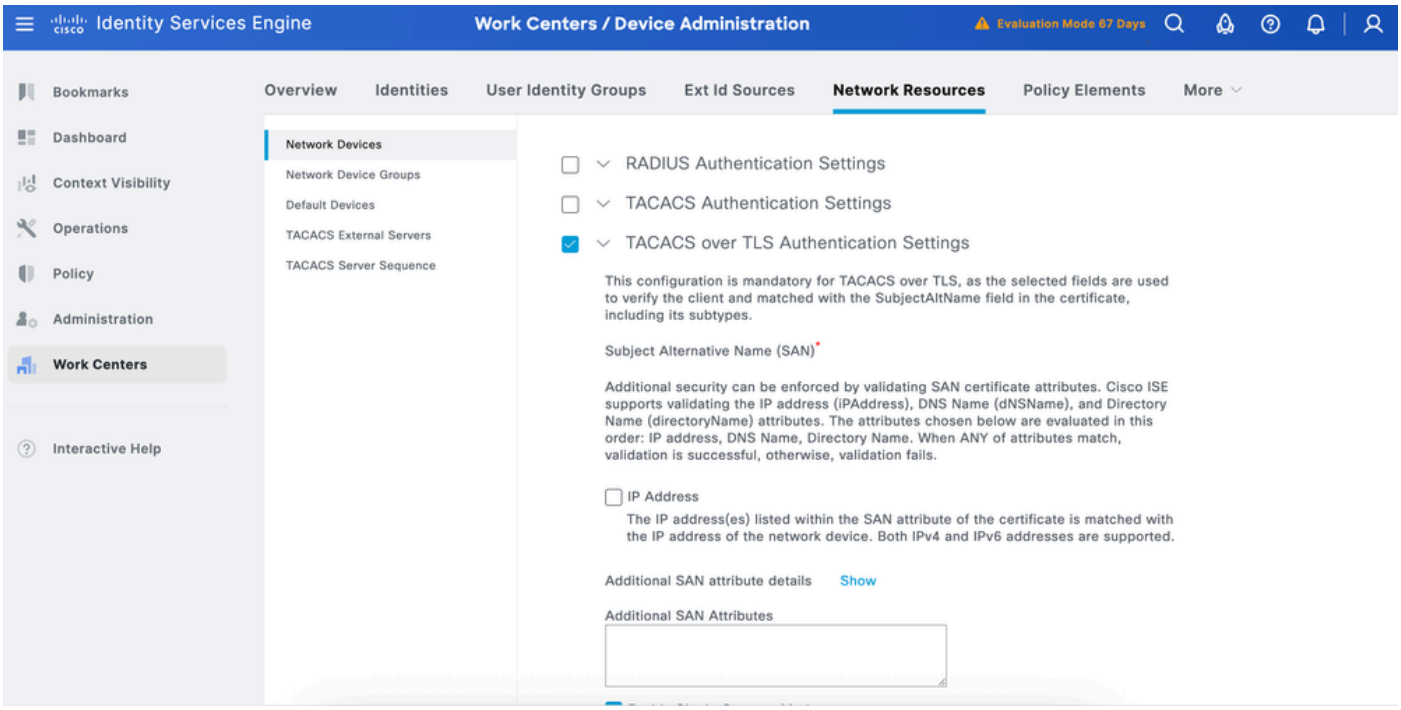


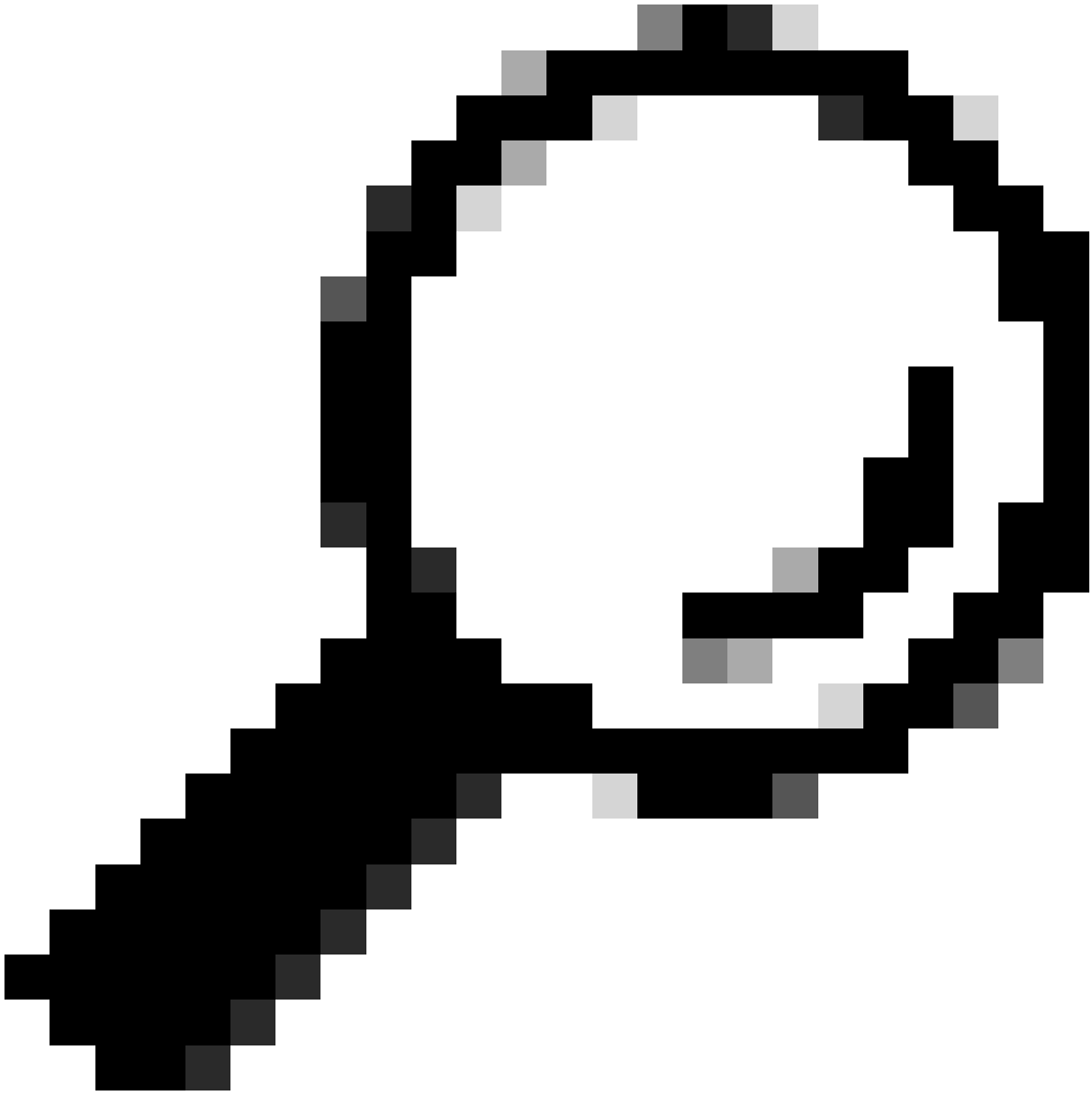
팁: 모든 디바이스 유형 및 모든 위치는 ISE에서 제공하는 기본 계층입니다. 사용자 자신의 계층을 추가 하고 정책 조건에서 나중에 사용 할 수 있는 네트워크 장치를 식별 하는 데 다양 한 구성 요소를 정의 할 수 있습니다

2단계. 이제 Cisco IOS XR 디바이스를 네트워크 디바이스로 추가합니다. Work Centers(작업 센터) > Device Administration(디바이스 관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동합니다. 새 네트워크 디바이스를 추가하려면 Add(추가)를 클릭합니다.



3단계. 디바이스의 IP 주소를 입력하고 디바이스의 위치 및 디바이스 유형(IOS XR)을 매핑하십시오. 마지막으로, TACACS+ over TLS 인증 설정을 활성화합니다.



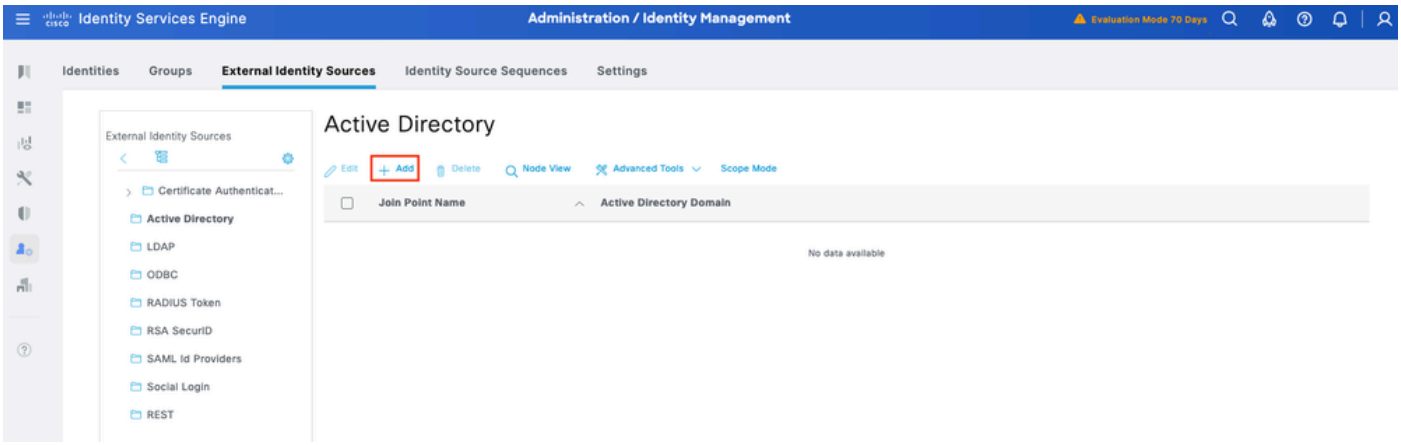


팁: 디바이스에 명령을 전송할 때마다 TCP 세션이 다시 시작되지 않도록 하려면 Enable Single Connect Mode(단일 연결 모드 활성화)를 사용하는 것이 좋습니다.

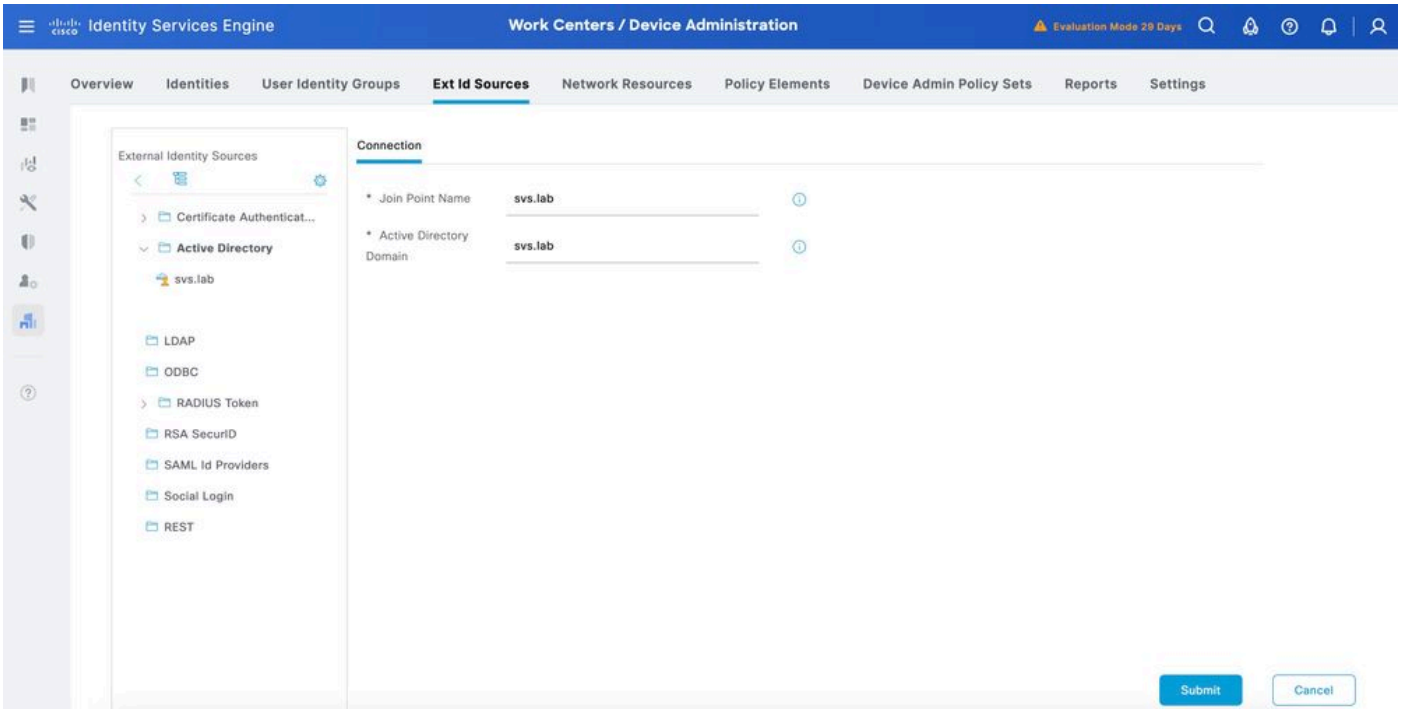
ID 저장소 구성

이 섹션에서는 디바이스 관리자를 위한 ID 저장소를 정의합니다. 이 저장소는 ISE 내부 사용자 및 지원되는 모든 외부 ID 소스가 될 수 있습니다. 여기서는 외부 ID 소스인 AD(Active Directory)를 사용합니다.

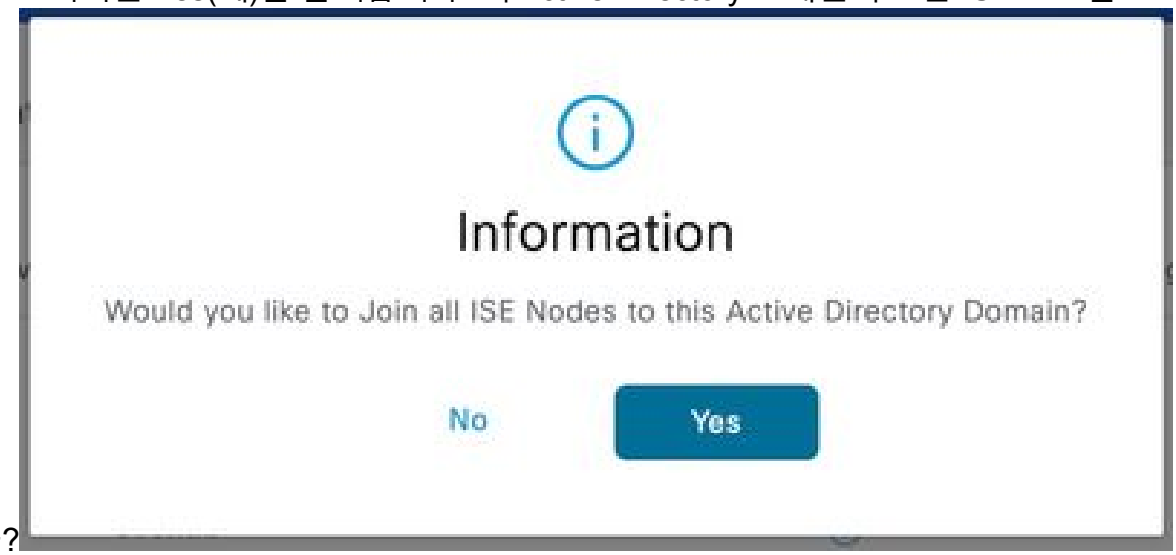
1단계. Administration(관리) > Identity Management(ID 관리) > External Identity Stores(외부 ID 저장소) > Active Directory로 이동합니다. 새 AD 조인트 포인트를 정의하려면 Add(추가)를 클릭합니다.



2단계. Join Point 이름과 AD 도메인 이름을 지정하고 Submit(제출)을 클릭합니다.



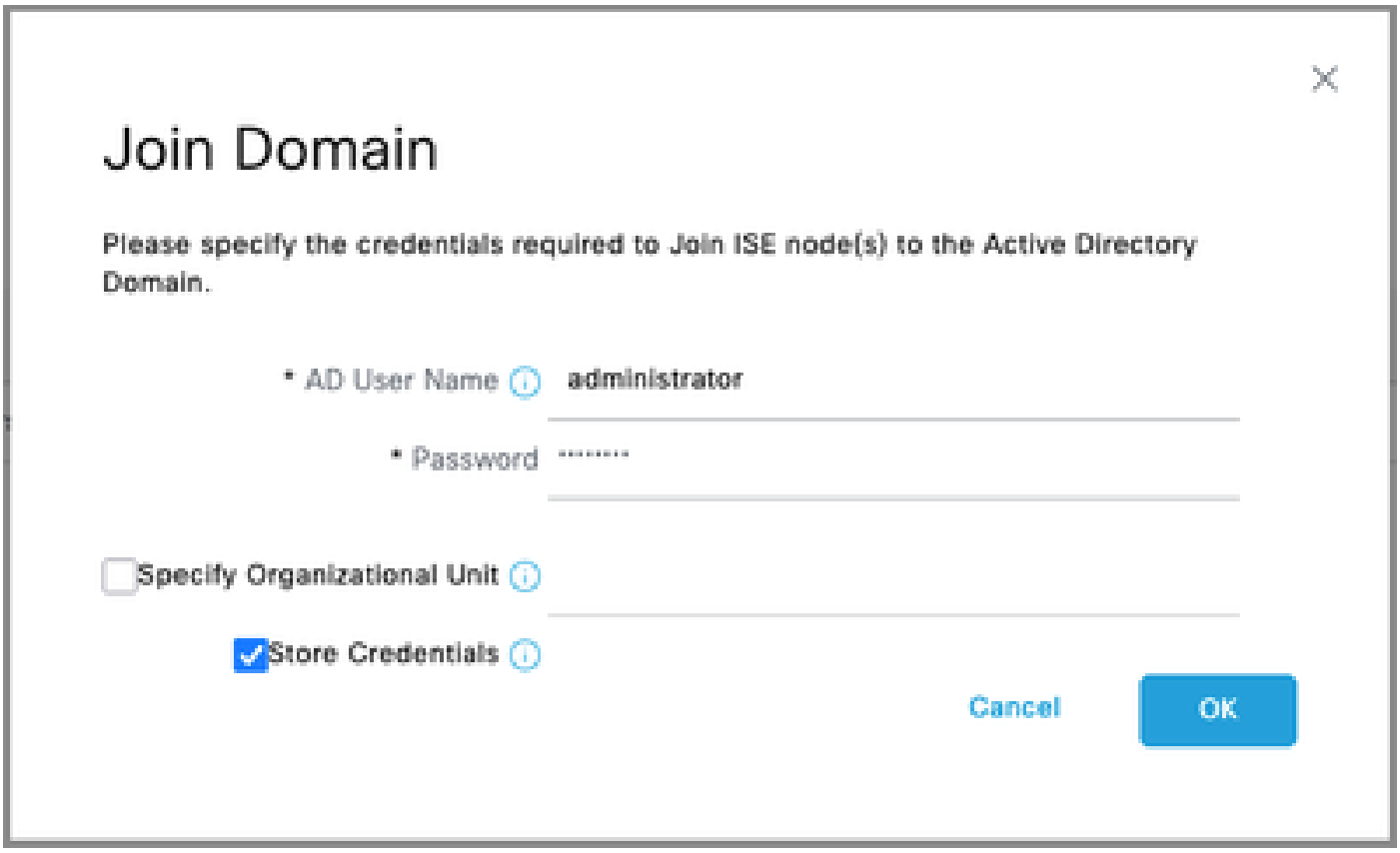
3단계. 메시지가 표시되면 Yes(예)를 클릭합니다. 이 Active Directory 도메인에 모든 ISE 노드를 조

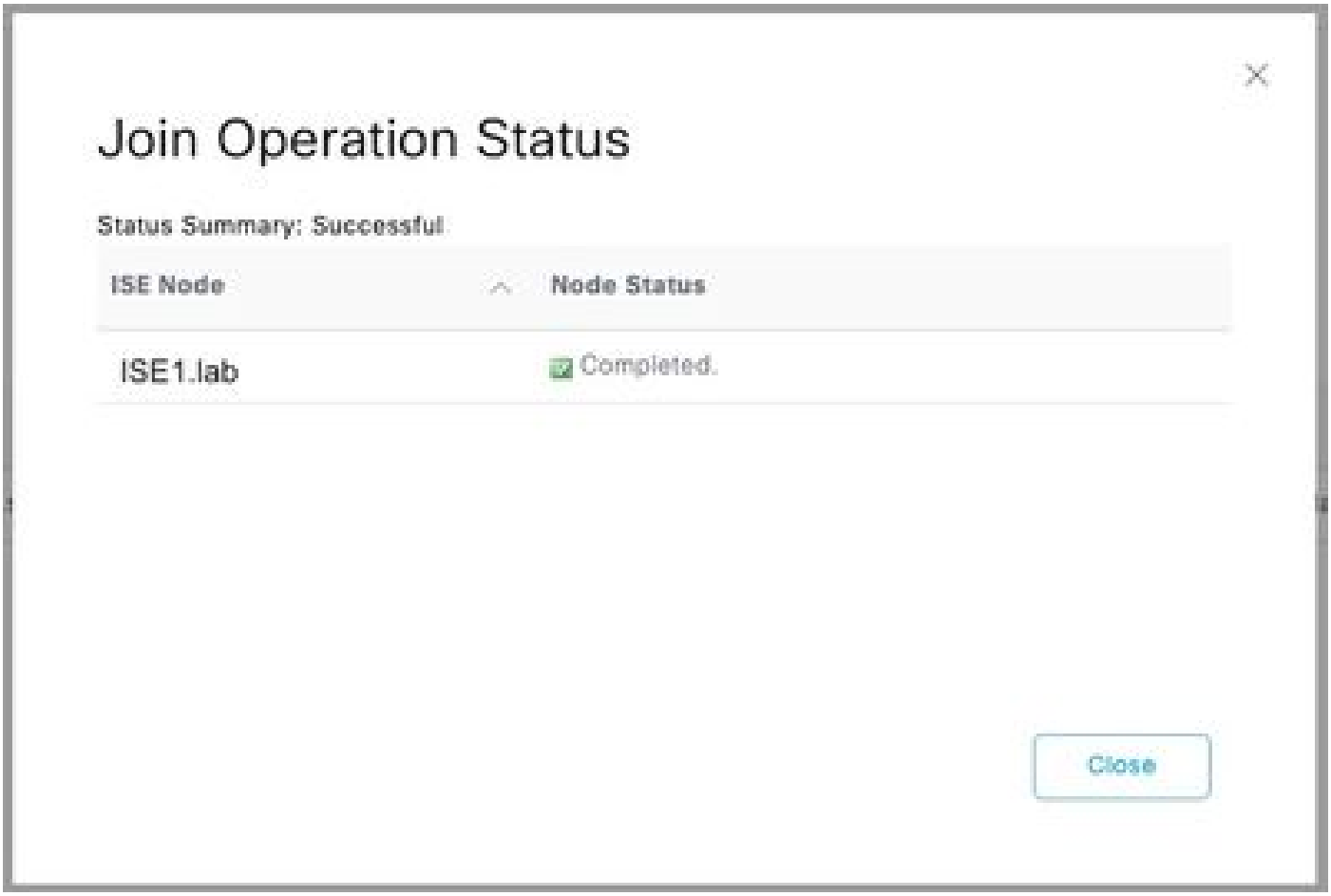


인하시겠습니까?

4단계. AD 조인 권한이 있는 자격 증명을 입력하고 ISE를 AD에 조인합니다. 작동 여부를 확인하려

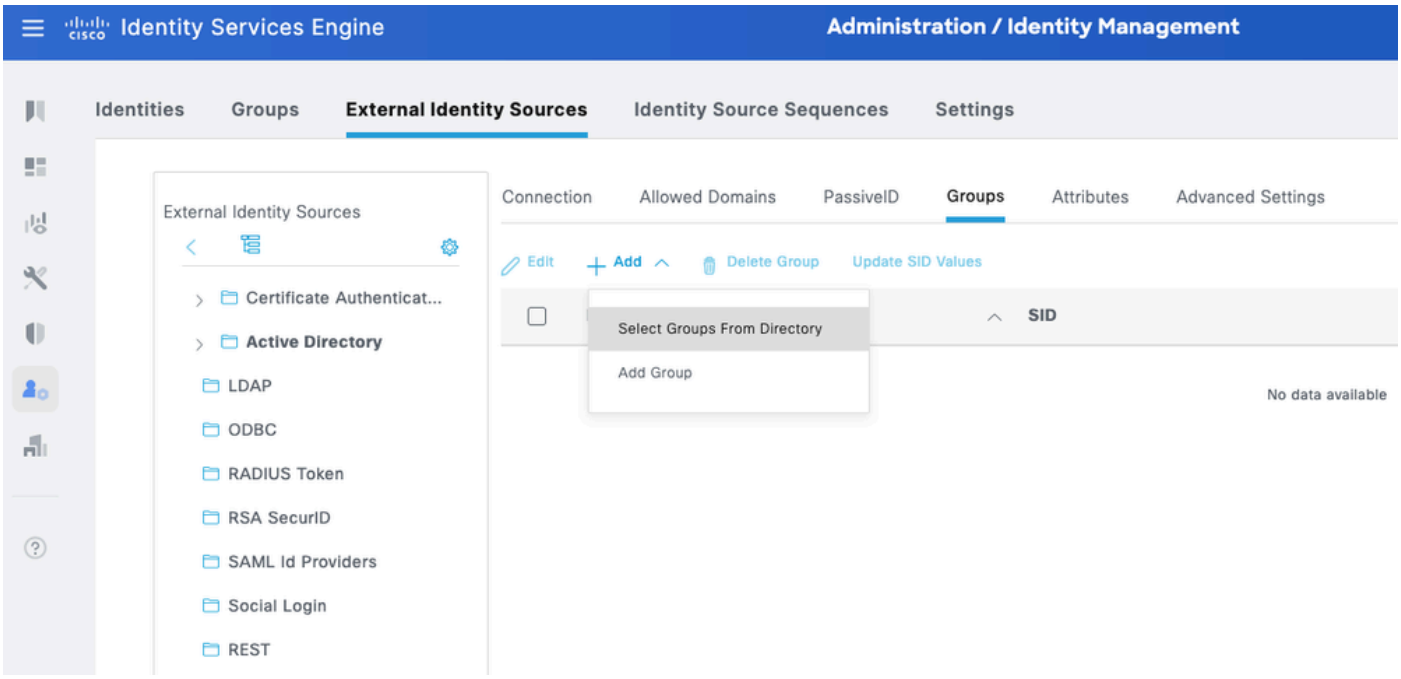
면 Status(상태)를 선택합니다.

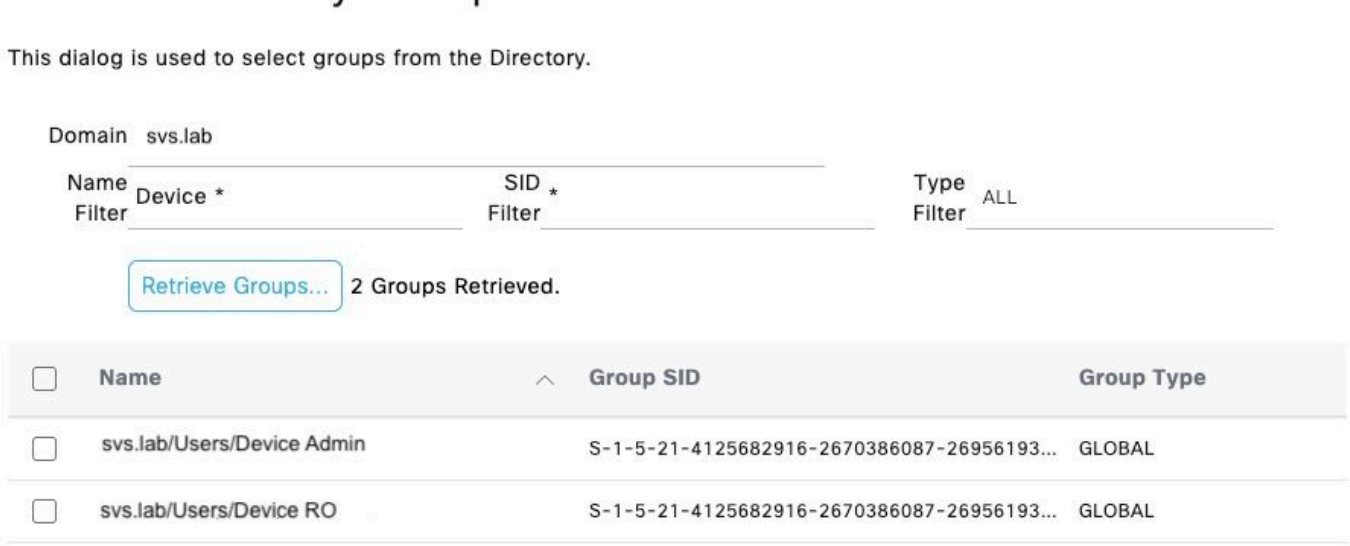


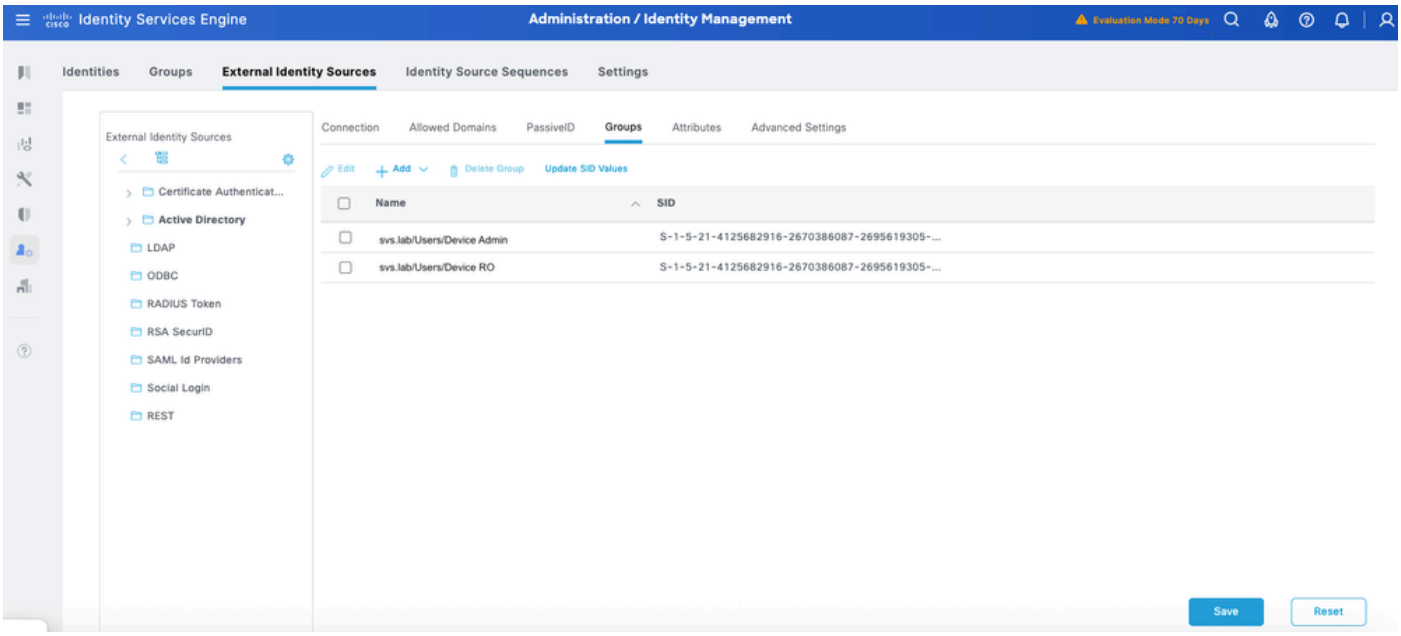


5단계. Groups(그룹) 탭으로 이동하고 Add(추가)를 클릭하여 디바이스 액세스 권한이 부여된 사용

자에 따라 필요한 모든 그룹을 가져옵니다. 이 예에서는 권한 부여 정책에서 사용되는 그룹을 보여 줍니다.







TACACS+ 프로파일 구성

TACACS+ 프로필을 Cisco IOS XR 디바이스의 사용자 역할에 매핑합니다. 이 예에서는 다음과 같이 정의됩니다.

- Root System Administrator(루트 시스템 관리자) - 디바이스에서 권한이 가장 높은 역할입니다. 루트 시스템 관리자 역할의 사용자는 모든 시스템 명령 및 컨피그레이션 기능에 대한 완전한 관리 액세스 권한을 갖습니다.
- 운영자 - 이 역할은 모니터링 및 문제 해결을 위해 시스템에 대한 읽기 전용 액세스가 필요한 사용자를 위한 것입니다.

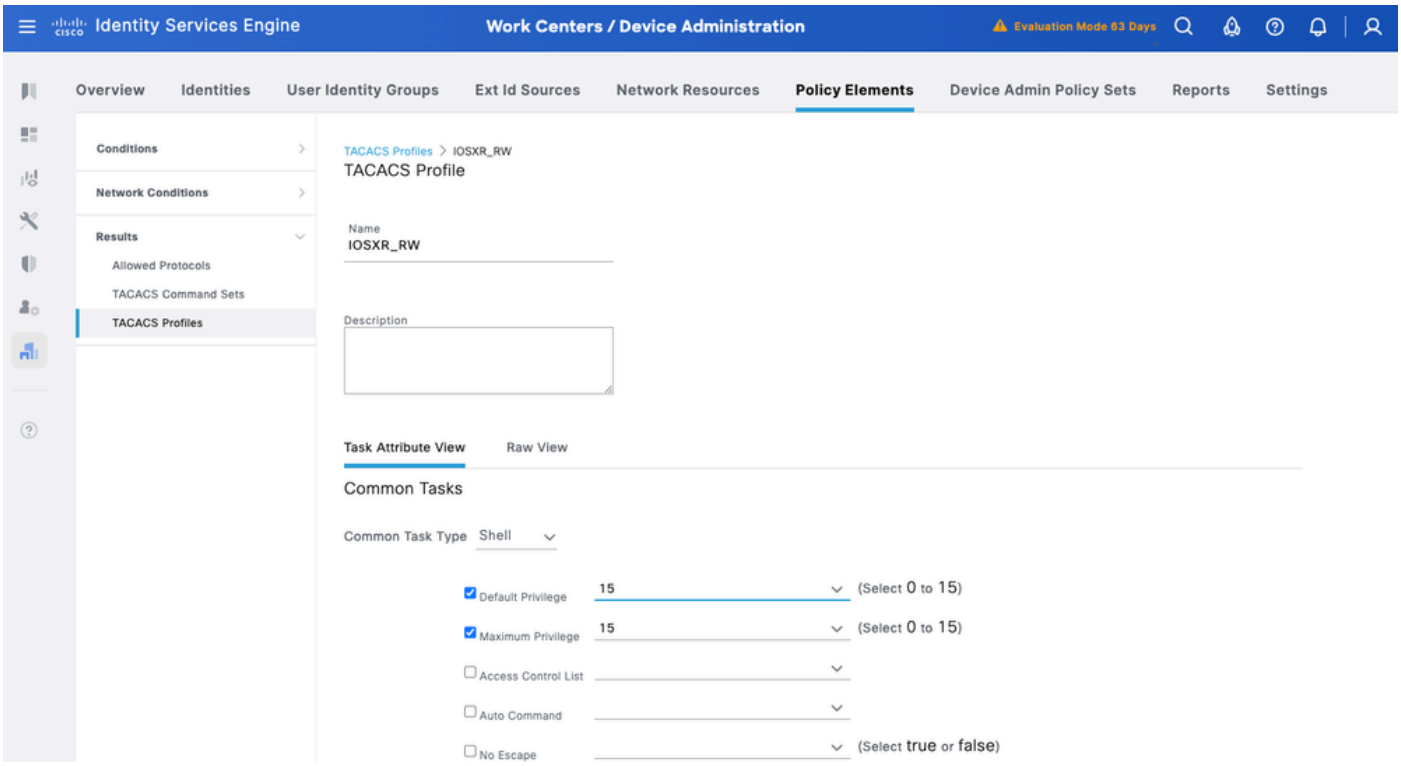
두 개의 TACACS+ 프로필을 정의합니다. IOSXR_RW 및 IOSXR_RO.

IOS XR_RW - 관리자 프로필

1단계. Work Centers(작업 센터) > Device Administration(디바이스 관리) > Policy Elements(정책 요소) > Results(결과) > TACACS Profiles(TACACS 프로필)로 이동합니다. 새 TACACS 프로필을 추가하고 이름을 IOSXR_RW로 지정합니다.

2단계. Default Privilege(기본 권한) 및 Maximum Privilege(최대 권한)를 선택하여 15로 설정합니다.

3단계. 컨피그레이션을 확인하고 저장합니다.

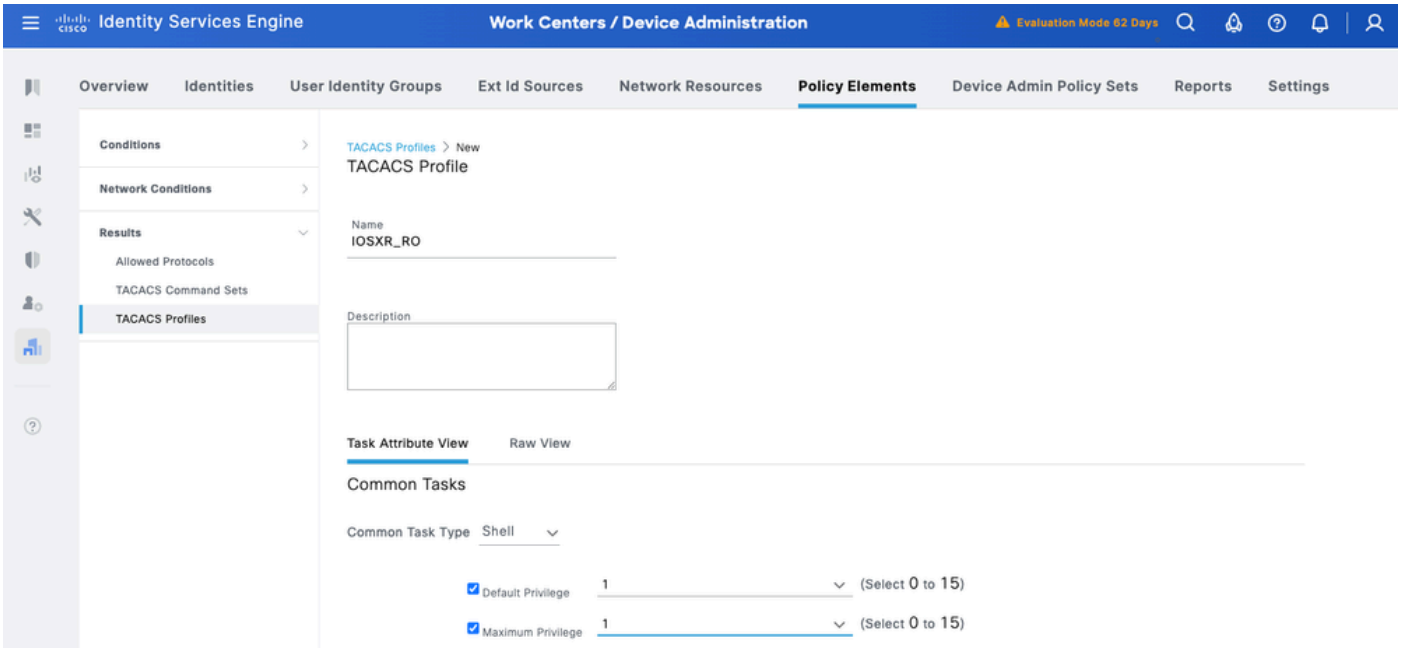


IOS XR_RO - 오퍼레이터 프로파일

1단계. Work Centers(작업 센터) > Device Administration(디바이스 관리) > Policy Elements(정책 요소) > Results(결과) > TACACS Profiles(TACACS 프로파일)로 이동합니다. 새 TACACS 프로파일을 추가하고 이름을 IOSXR_RO로 지정합니다.

2단계. Default Privilege(기본 권한) 및 Maximum Privilege(최대 권한)를 선택하여 1로 설정합니다.

3단계. 컨피그레이션을 확인하고 저장합니다.



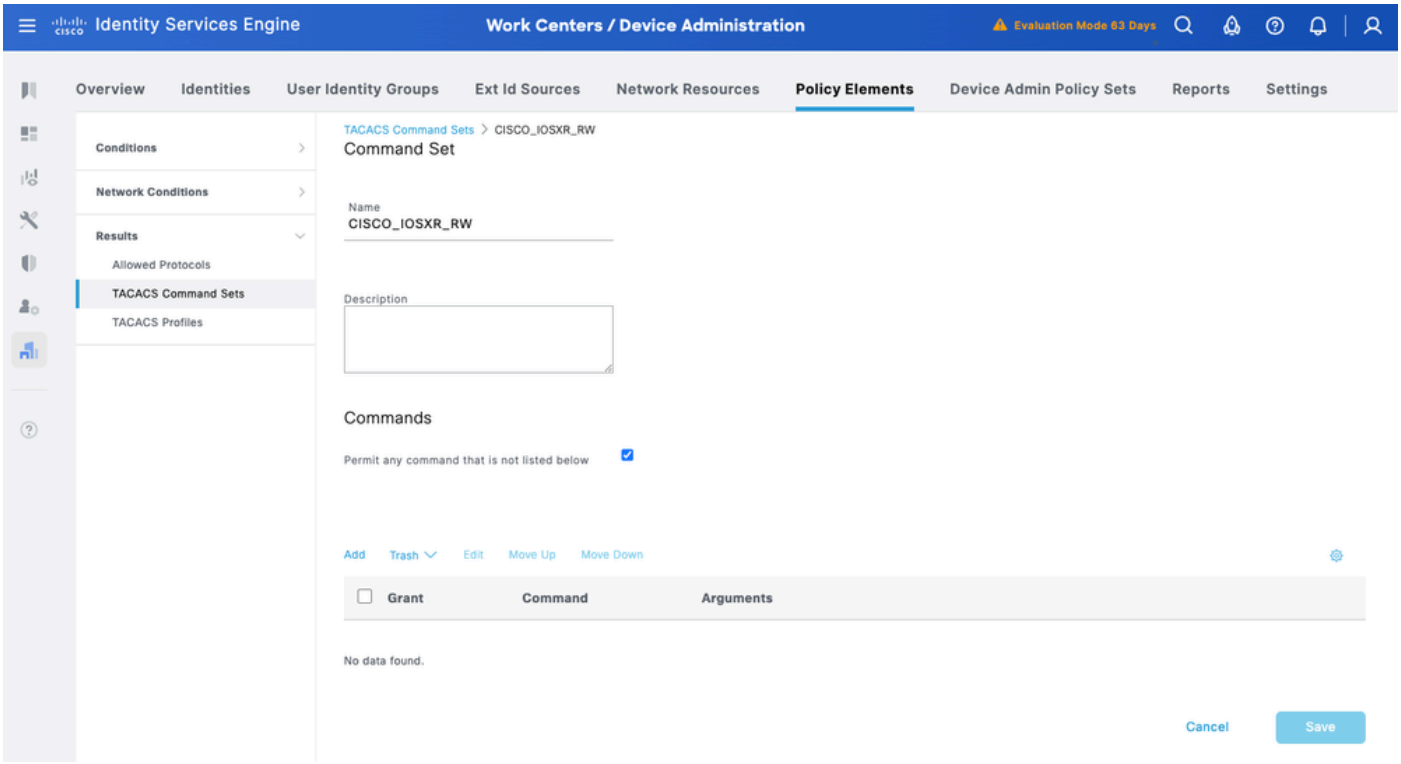
TACACS+ 명령 집합 구성

TACACS+ 명령 집합을 정의합니다. 이 예에서는 CISCO_IOSXR_RW 및 CISCO_IOSXR_RO로 정의됩니다.

CISCO IOS XR RW - 관리자 명령 집합

1단계. Work Centers(작업 센터) > Device Administration(디바이스 관리) > Policy Elements(정책 요소) > Results(결과) > TACACS Command Sets(TACACS 명령 집합)로 이동합니다. 새 TACACS 명령 집합을 추가하고 이름을 CISCO_IOSXR_RW로 지정합니다.

2단계. 아래에 나열되지 않은 모든 명령 허용 확인란을 선택하고(관리자 역할에 대한 모든 명령 허용) 저장을 클릭합니다.



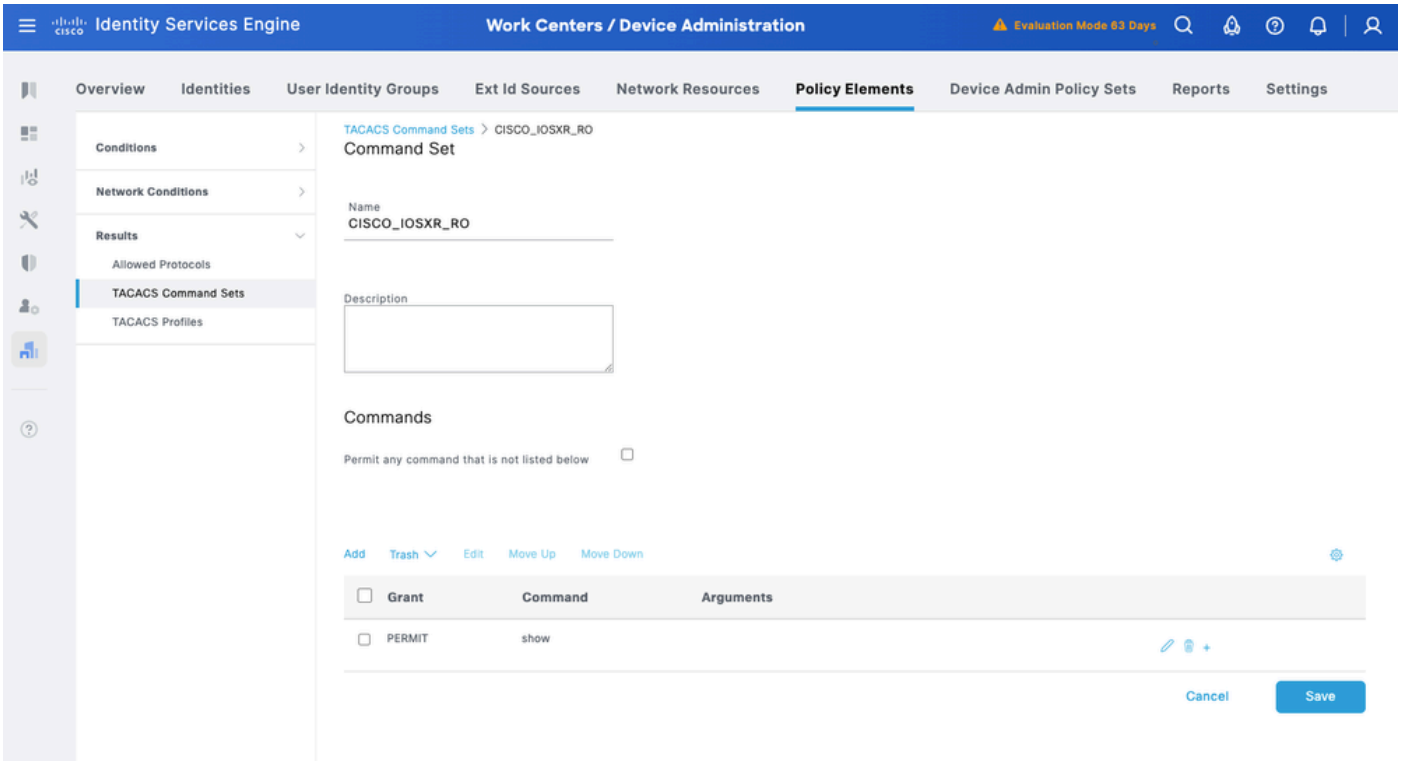
CISCO IOS XR RO - Operator 명령 집합

1단계. ISE UI에서 Work Centers(작업 센터) > Device Administration(디바이스 관리) > Policy Elements(정책 요소) > Results(결과) > TACACS Command Sets(TACACS 명령 집합)로 이동합니다. 새 TACACS 명령 집합을 추가하고 이름을 CISCO_IOSXR_RO로 지정합니다.

2단계. Commands(명령) 섹션에서 새 명령을 추가합니다.

3단계. Grant(권한 부여) 열의 드롭다운 목록에서 Permit(허용)을 선택하고 Command(명령) 열에 show를 입력합니다. 확인 화살표를 클릭합니다.

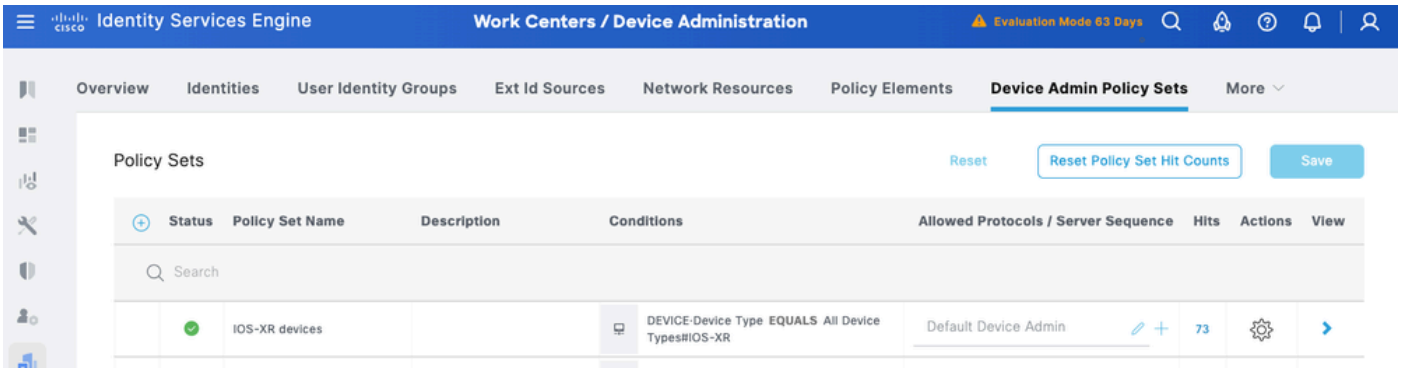
4단계. 데이터를 확인하고 저장을 클릭합니다.



디바이스 관리 정책 집합 구성

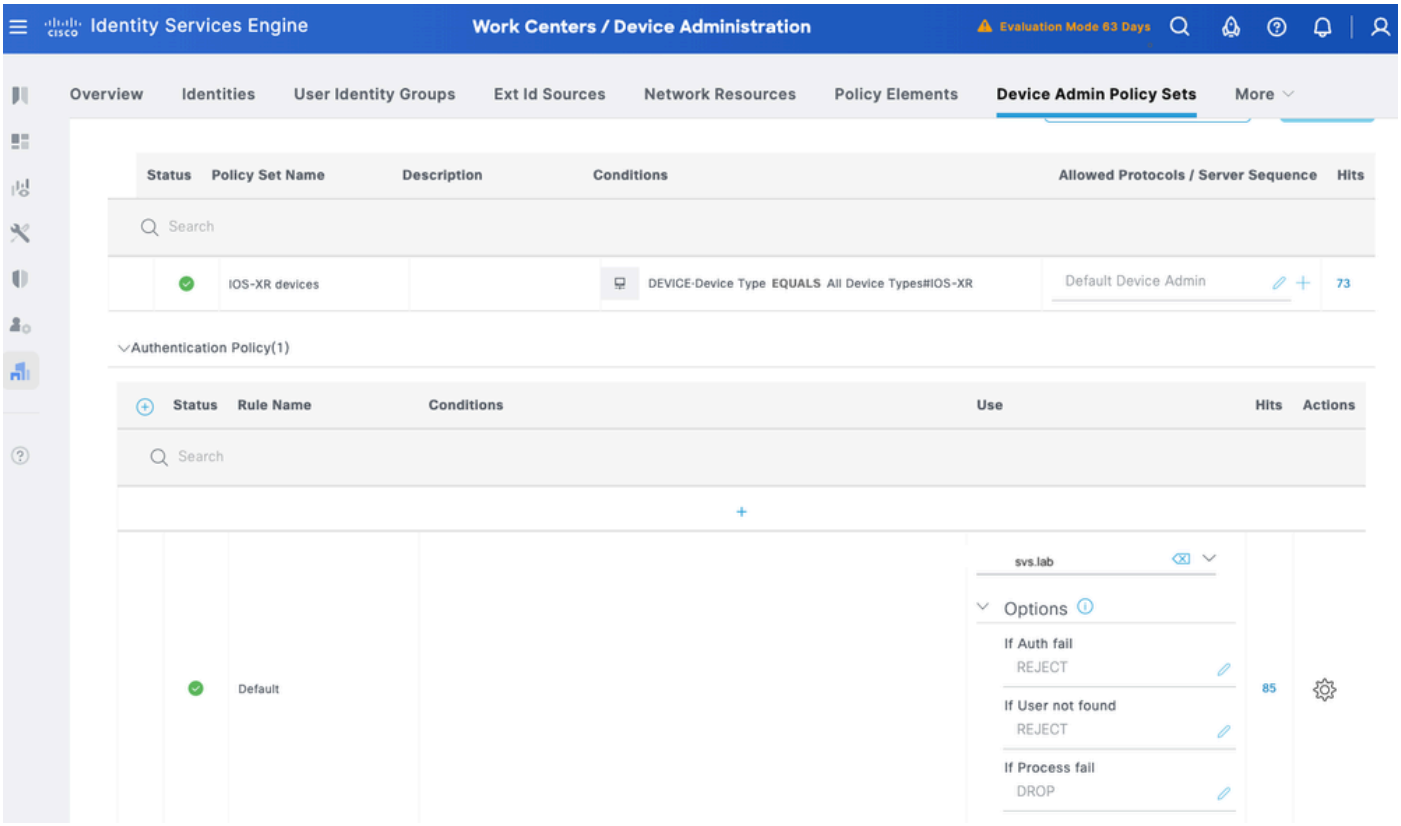
Policy Sets(정책 집합)는 Device Administration(디바이스 관리)에 대해 기본적으로 활성화되어 있습니다. 정책 집합은 TACACS 프로파일을 쉽게 적용할 수 있도록 디바이스 유형에 따라 정책을 구분할 수 있습니다.

1단계. Work Centers(작업 센터) > Device Administration(디바이스 관리) > Device Admin Policy Sets(디바이스 관리 정책 집합)로 이동합니다. 새 정책 집합 IOS XR 디바이스를 추가합니다. 조건에서 DEVICE:Device Type EQUALS All Device Types#IOS XR을 지정합니다. Allowed Protocols(허용된 프로토콜) 아래에서 Default Device Admin(기본 디바이스 관리)을 선택합니다.



2단계. Save(저장)를 클릭하고 오른쪽 화살표를 클릭하여 이 정책 집합을 구성합니다.

3단계. 인증 정책을 생성합니다. 인증에서는 AD를 ID 저장소로 사용합니다. If Auth fail(인증 실패 시), If User not found(사용자가 발견되지 않은 경우) 및 If Process fail(프로세스가 실패함)에 기본 옵션을 그대로 둡니다.

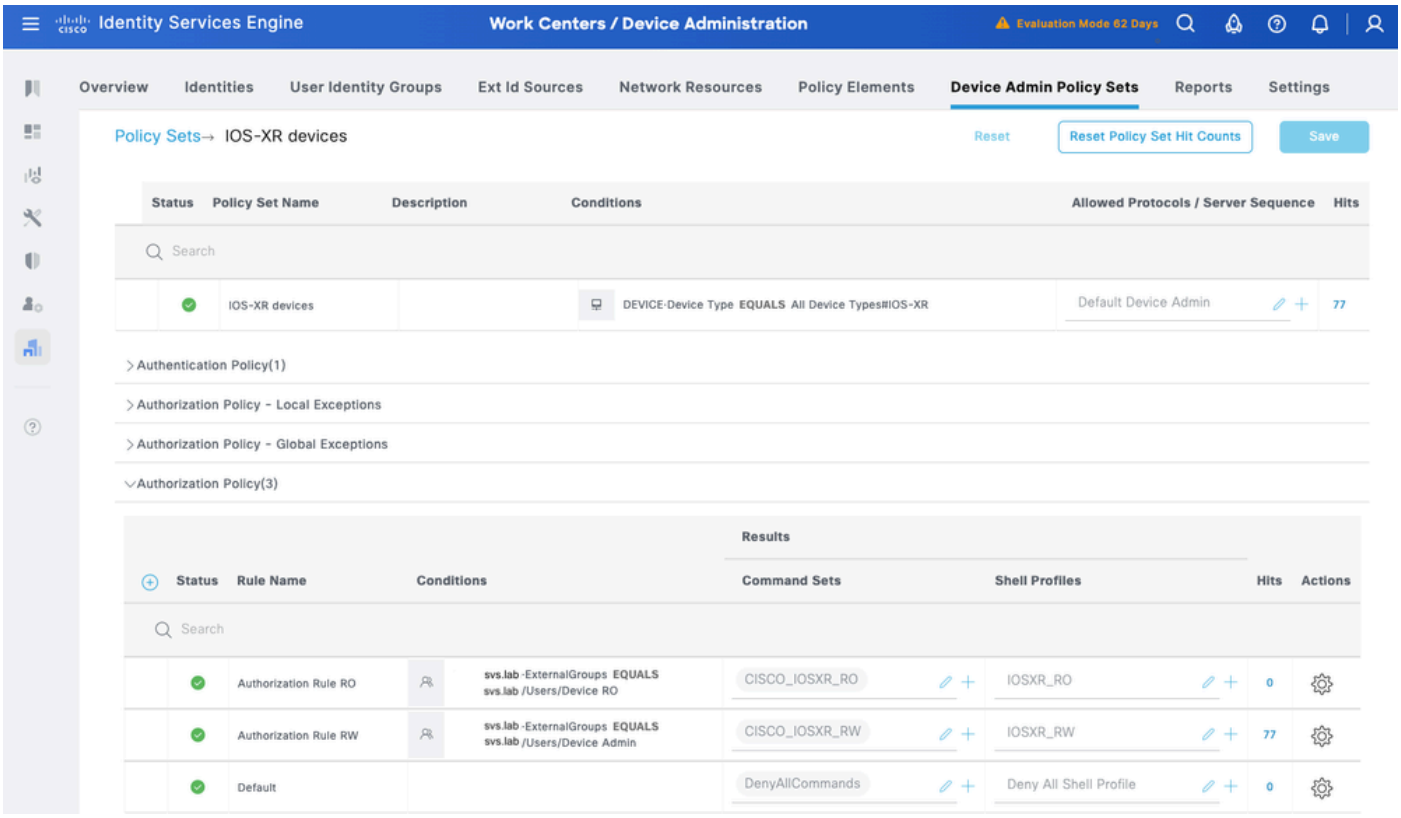


4단계. 권한 부여 정책을 정의합니다.

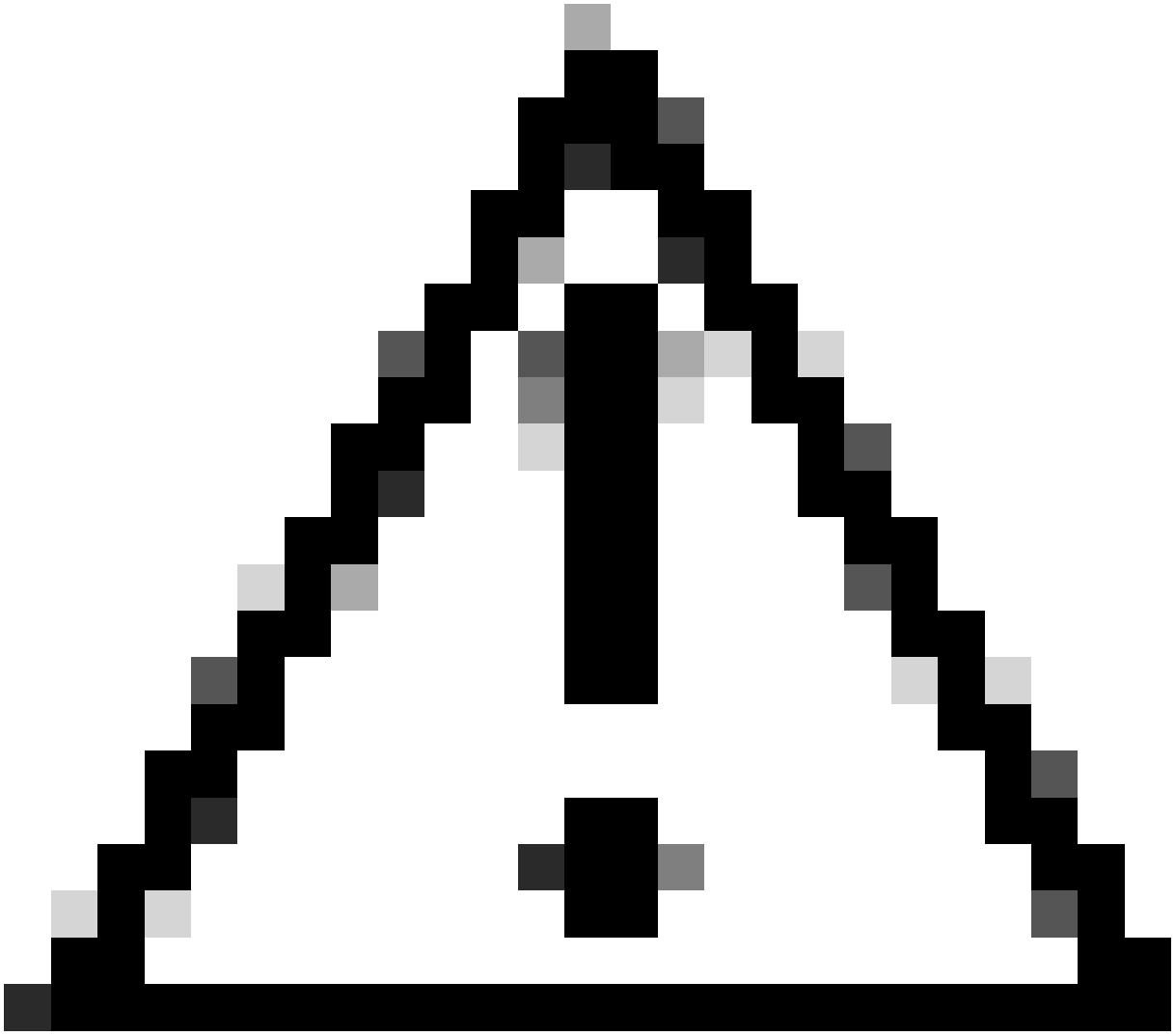
AD(Active Directory)의 사용자 그룹을 기반으로 권한 부여 정책을 생성합니다.

예를 들면 다음과 같습니다.

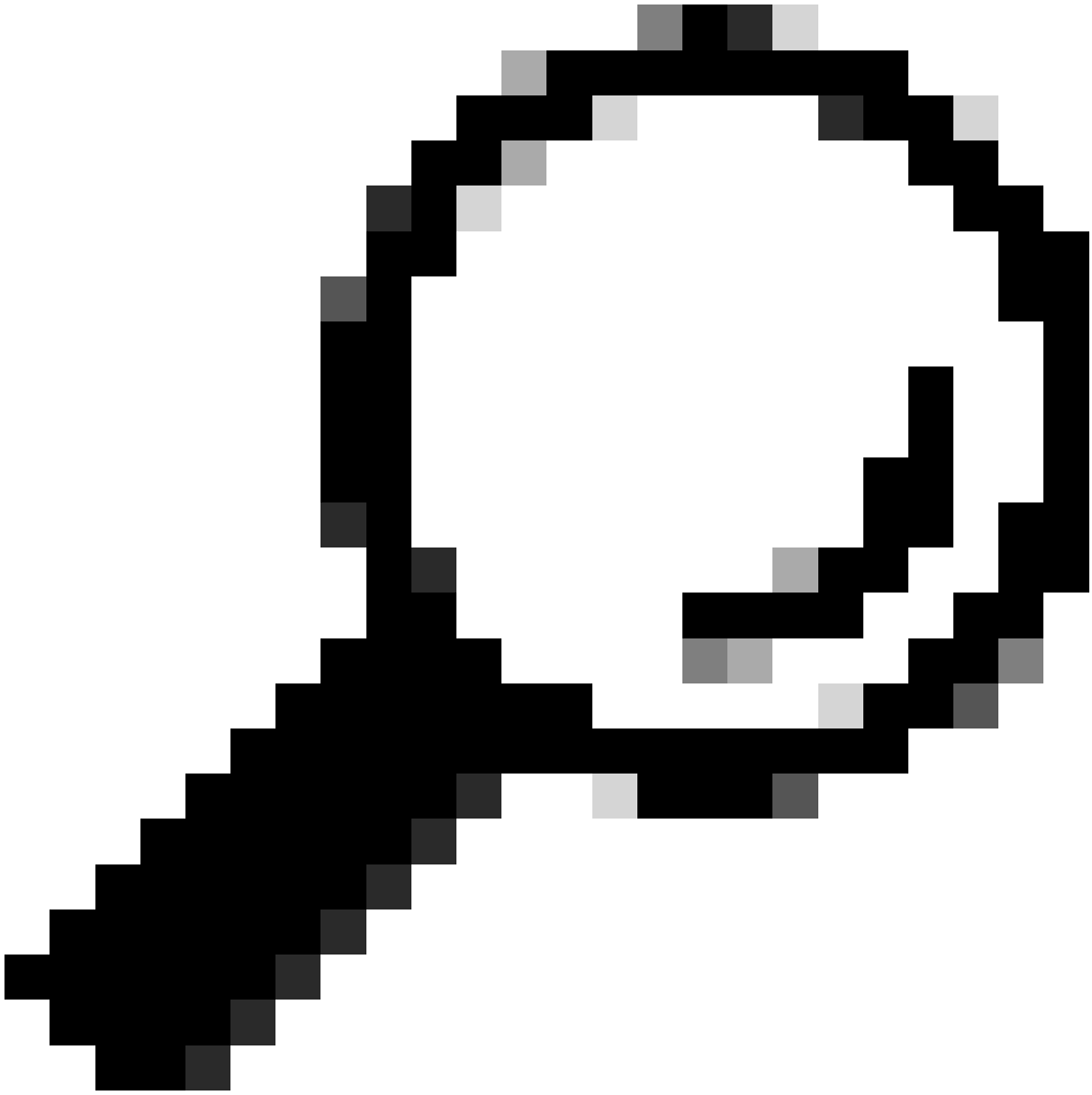
- AD 그룹 디바이스 RO의 사용자에게는 CISCO_IOSXR_RO 명령 집합 및 IOSXR_RO 셸 프로파일이 할당됩니다.
- AD 그룹 디바이스 관리자의 사용자는 CISCO_IOSXR_RW 명령 집합 및 IOSXR_RW 셸 프로필이 할당됩니다.



2부 - TLS 1.3을 통한 TACACS+용 Cisco IOS XR 구성



주의: 콘솔 연결에 연결할 수 있고 제대로 작동하는지 확인합니다.



팁: 디바이스에서 잠기지 않도록 컨피그레이션을 변경하는 동안 TACACS 대신 로컬 자격 증명을 사용하도록 임시 사용자를 구성하고 AAA 인증 및 권한 부여 방법을 변경하는 것이 좋습니다.

초기 컨피그레이션

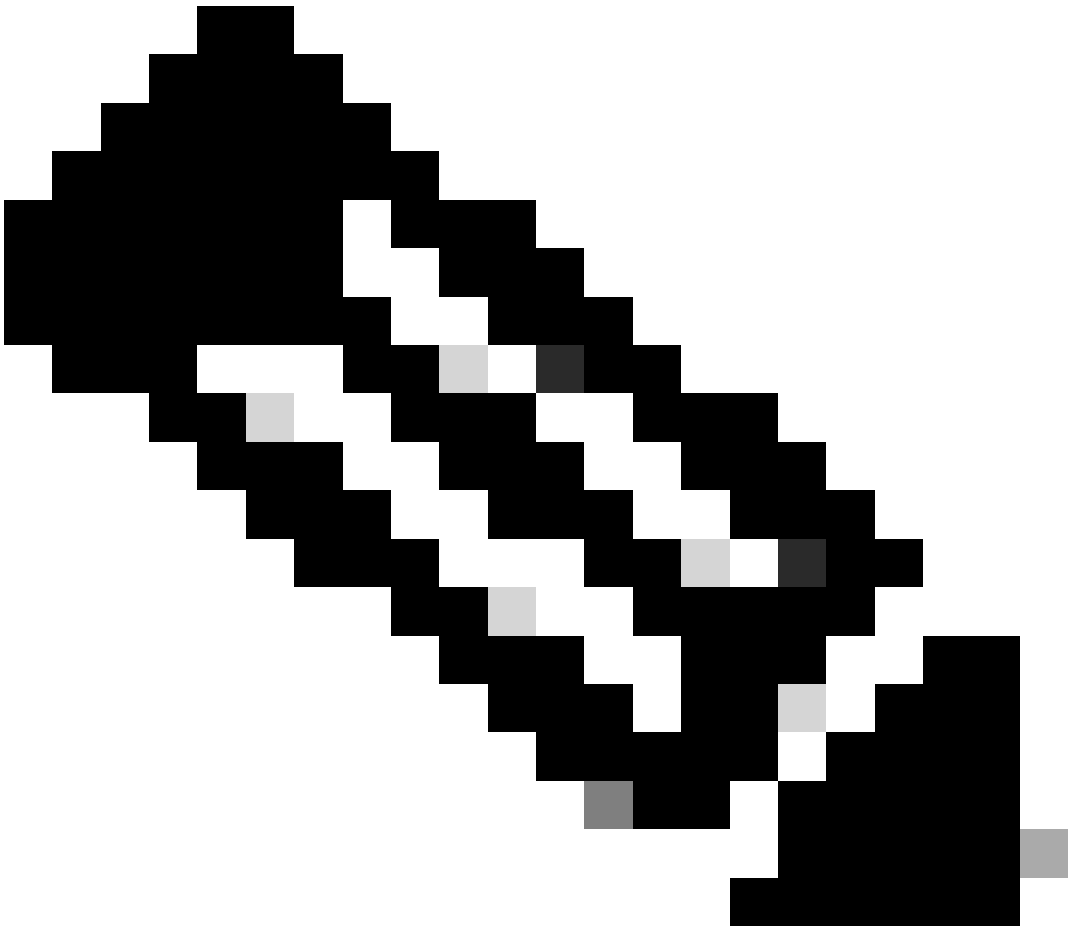
1단계. DNS(Name-server)가 구성되어 있고 라우터가 FQDN(Frequently Qualified Domain Names), 특히 ISE 서버 FQDN을 성공적으로 확인할 수 있는지 확인합니다.

```
domain vrf mgmt name svs.lab
domain vrf mgmt name-server 10.225.253.247
no domain vrf mgmt lookup disable

RP/0/RP0/CPU0:BRC-8201-1#ping vrf mgmt ise1.svs.lab
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.225.253.209 timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

2단계. 이전/사용하지 않은 신뢰 지점 및 인증서를 지웁니다. 이전 신뢰 지점 및 인증서가 없는지 확인합니다. 이전 항목이 표시되면 해당 항목을 제거/지웁니다.

```
show crypto ca trustpoint
show crypto ca certificates

(config)# no crypto ca trustpoint <tp-name>
# clear crypto ca certificates <tp-name>
```



참고: 수동으로 새 RSA 키 쌍을 생성하여 신뢰 지점 아래에 연결할 수 있습니다. 하나를 생

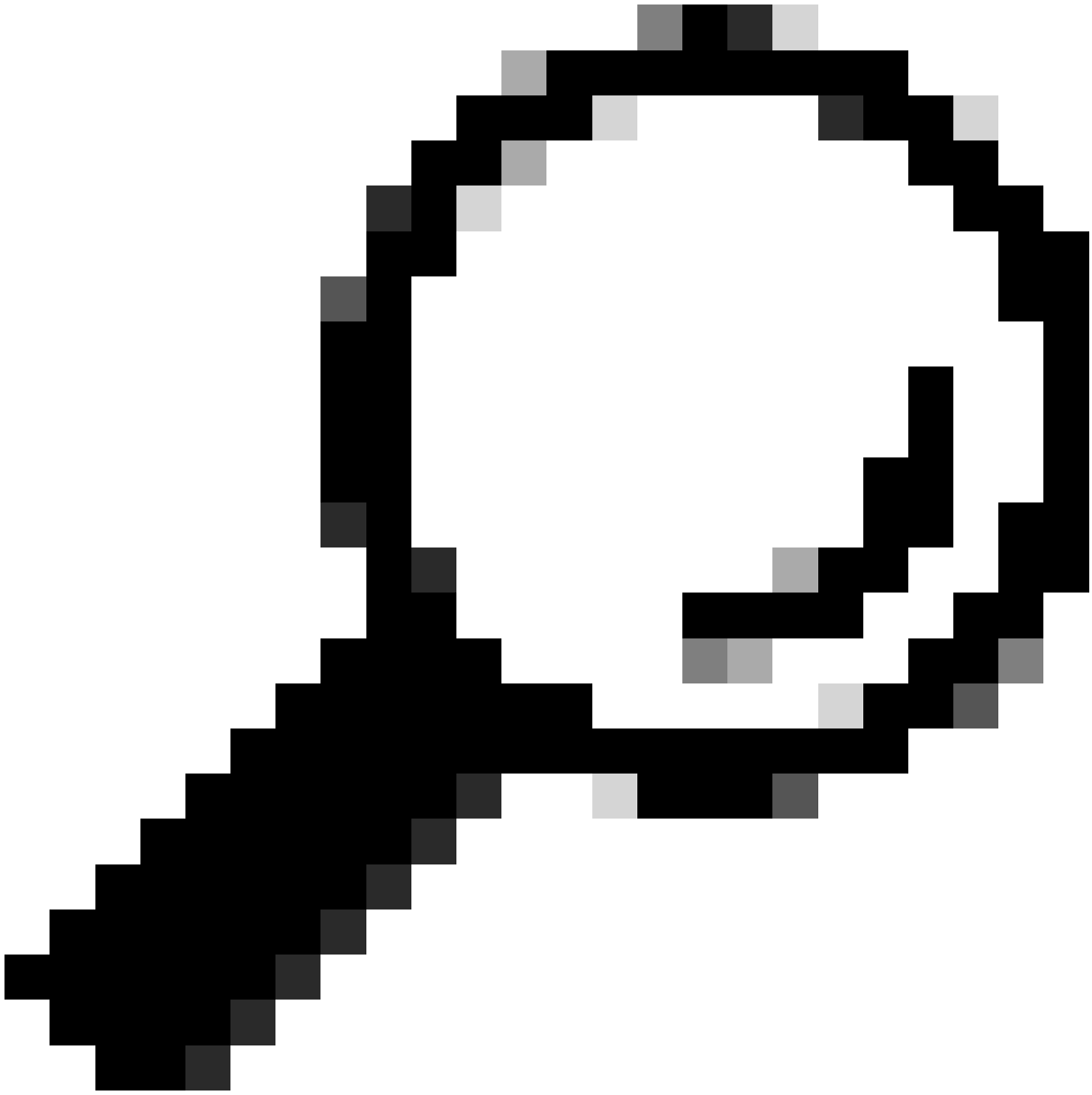
성하지 않으면 기본 키 쌍이 사용됩니다. 신뢰 지점에서 ECC 키 쌍을 정의하는 것은 현재 지원되지 않습니다.

신뢰 지점 구성

1단계. 키 쌍 컨피그레이션(선택 사항).

```
<#root>
RP/0/RP0/CPU0:BRC-8201-1(config)#
crypto key generate rsa

          4096

RP/0/RP0/CPU0:BRC-8201-1(config)#
crypto ca trustpoint

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
rsakeypair
```

2단계. 신뢰 지점을 생성합니다.



팁: 주체 대체 이름에 대한 DNS 컨피그레이션은 선택 사항이지만(ISE에서 활성화된 경우) 권장됩니다.

<#root>

RP/0/RP0/CPU0:BRC-8201-1(config)#

crypto ca trustpoint svs

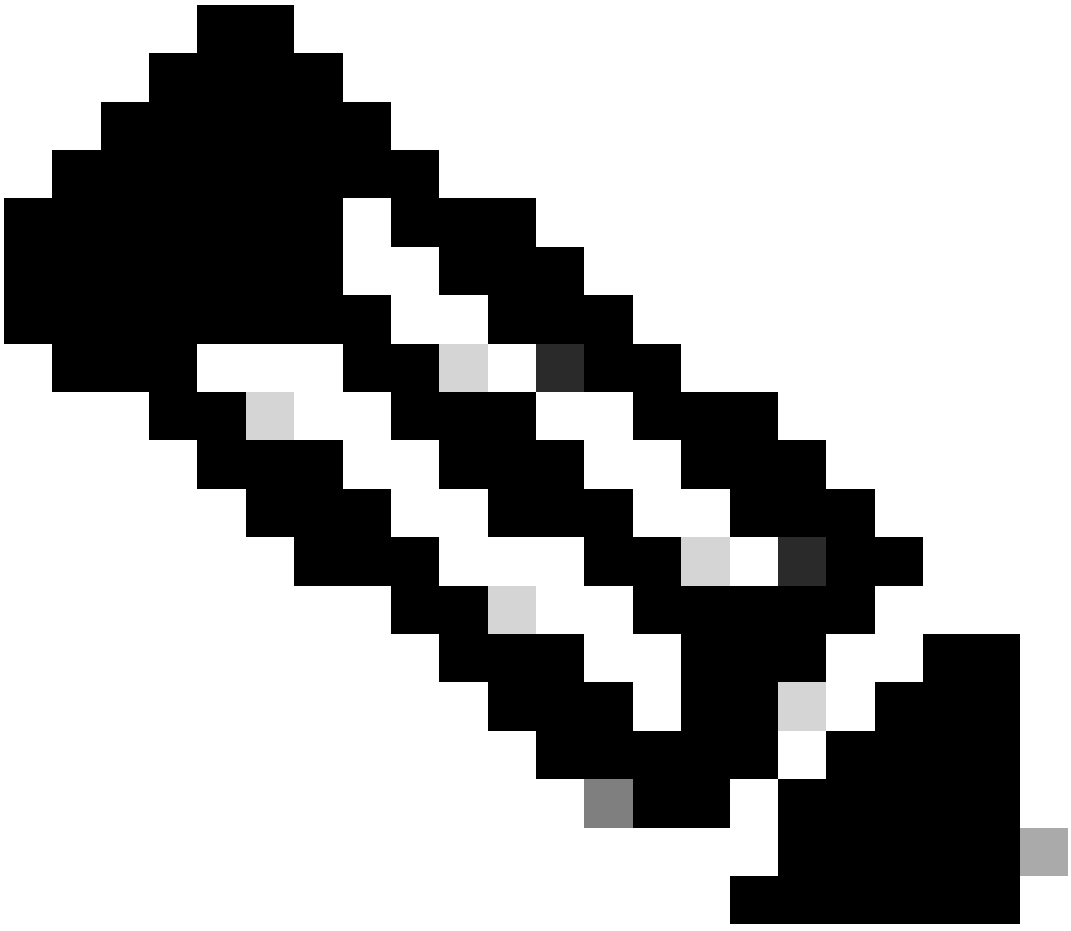
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#

vrf mgmt

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#

crl optional

```
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
subject-name C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=brc-8201-1.svs.lab

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
subject-alternative-name IP:10.225.253.167,DNS:brc-8201-1.svs.lab

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
enrollment url terminal
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
rsakeypair svs-4096

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
commit
```



참고: O 또는 OU에서 쉼표를 사용해야 하는 경우 쉼표 앞에 백슬래시(\)를 사용할 수 있습니다. 예를 들면 다음과 같습니다. O=Cisco Systems\, Inc.

3단계. CA 인증서를 설치하여 신뢰 지점을 인증합니다.

<#root>

RP/0/RP0/CPU0:BRC-8201-1#

crypto ca authenticate svs

```
Enter the base64/PEM encoded certificate/certificates.
Please note: for multiple certificates use only PEM.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIFlDCCA3ygAwIBAgIIIM1OAsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUGA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBAcTB1JhbGVpZ2gxDjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTVlMxEjAQBgNVBAMTCVNWUyBMYWJDQTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZUOyn2vIn6gKbx3M7vaRq
2YjwZlzSH6EkEvxnJTy+kksiFD33GyHQepk7vfp4NFU5OtQ4HC7t/AOv9grDa3QW
VwvV4MBbJhFM3s0J/ejgDYcMZhIAaPyOZo5WLboOkXEiKjPLatkXojB8FVrhLF3O
jMBSqwa4/Wlniy5S+7s4FFxsCf2OCOWfBAsnrs0tatIIhmcnx+VLJP7MRm8fOw4m
mutNo7IhbJSrgAFXmjlbBjMmgspObULo/wxMHdTbtPBf11HRHTkNIo3qyO4UADL2
WpoGhgT/FaxxBo2UBcnYVaP+jjRE0NYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7BOe8oDNKU6gXlojKyLP/gC7j8AePO3ir+KZui8
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVpL334rTIxy9hpKZIkB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTAO1xh6OI4QnK+MNQKpTjt/E4
ydHlOrrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVLl783nTc9wYptQEPi5sw
83g9EMgKV0ARIiVUa/qlAgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAYb4
QgEBBAQDAgAHMBkGCWCGSAGG+EIBDQQMFgpTVlMgTGFiIENBMA0GCSqGSIb3DQEB
CwUAA4ICAQAIT3O8oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oKOdGayi
iSEkSSX9qyfLfINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
O+ja6zTQqjO6lqJhmrSkyFbYf/ZTpe4d1OzJsZjNsNOr8bF9nOA/7qNZLp3Z3cpU
PUOKdbiSvRqnPw3e8TfITVmAzcx8COI2SrYFMSUazolVBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7aluJapXkmnj5qPeGhNOpB
Q9r14reov4so2EspkXS7CrH9yGfpIyTprokz1UvZBZ8vloI7YZmjFmem+5rT6Gnk
eU/lX7nV61SYG5W5K+I8uaKuyBHOMn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggzlPOdsS/i6Lo7ypYXOeB9HgVDCkzQsLXQuHGj/2WsgPgdRcjkvnyURk4Jx+Ib
xDrmo7e0XPpSW4l72a6Kl8CR3U2Cr4wsuvndPEq/qd2NRSBWffF0XE/AJHQG7STT
HaXLU9r2Ko6O3oecu8ysGTwLlIt/9T1/FOb0xZRugWcpJrVoTgDGuA==
-----END CERTIFICATE-----
```

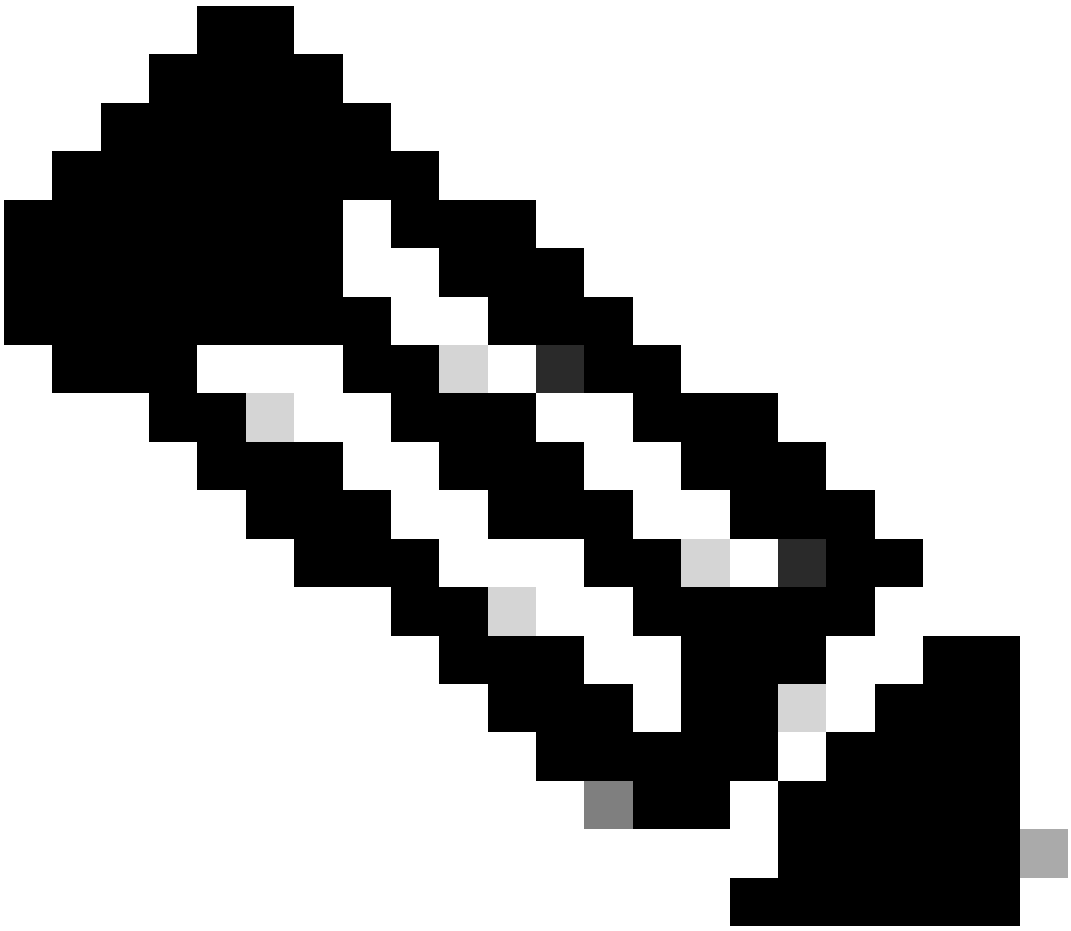
quit

```
   Serial Number : AB:CD:87:FD:41:12:C3:FE:FD:87:D5
   Subject:
      CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
   Issued By :
      CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
```

```
   Validity Start : 17:05:00 UTC Mon Apr 28 2025
   Validity End : 17:05:00 UTC Sat Apr 28 2035
RP/0/RP0/CPU0:May 9 14:52:20.961 UTC: pki_cmd[66362]: %SECURITY-PKI-6-LOG_INFO_DETAIL : Fingerprint: 2A
   SHA1 Fingerprint:
      0EB181E95A3ED7803BC5A8059A854A95C83AC737
Do you accept this certificate? [yes/no]:
```

yes

```
RP/0/RP0/CPU0:May 9 14:52:23.437 UTC: cepki[153]: %SECURITY-CEPKI-6-INFO : certificate database updated
```



참고: 하위 CA 시스템이 있는 경우 루트 CA 및 하위 CA 인증서를 모두 가져와야 합니다. 위의 하위 CA와 아래의 루트 CA에서도 동일한 명령을 사용합니다.

4단계. CSR(Certificate Signing Request)을 생성합니다.

<#root>

```
RP/0/RP0/CPU0:BRC-8201-1#
```

crypto ca enroll svs

```
Fri May 9 14:52:44.030 UTC
% Start certificate enrollment ...
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
% For security reasons your password will not be saved in the configuration.
% Please make a note of it.
```

Password:

Re-enter Password:

```
% The subject name in the certificate will include: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=10.225.253.167
% The subject name in the certificate will include: BRC-8201-1.svs.lab
% Include the router serial number in the subject name? [yes/no]:
```

yes

```
% The serial number in the certificate will be: 4090843b
% Include an IP address in the subject name? [yes/no]:
```

yes

```
Enter IP Address[]
```

10.225.253.167

```
Fingerprint: 36354532 38324335 43434136 42333545
Display Certificate Request to terminal? [yes/no]:
```

yes

```
Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
MIIDQTCCAikCAQAwcjELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAk5DMQwwCgYDVQQH
DANSVFAxDjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQLDANTVlMxFzAVBgNVBAMMDjEw
LjIyNS4yNTMuMTY3MREwDwYDVQQFEwg0MDkwODQzYjCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBALwx9w4DnTtrloDH9iOZxPvEDARwN0t4WrPEjaQclZUA
6ax6Cxq/0JlQiUf2+eQv+4rKZqAZ1xDhiaiMGqETnO0LKpwmtx10IqXL7UYMHHwF
9vRII52zomkWA8a63Wx66UkExaXoeXaf5HkLoqDu68X83U7LPvMe1sMwvmq7Rmy2
DAu30HB/JfYlQCHmTVFz3M5fBt86xx4t1nxTFU/4lRWMC73UdL5YdKJLjMpBT2tN
E3piZ+kL4p1c9U4RIBkU8/G4drzFbGvHCIkWkwI0cb1X2HgtbVQdCXTAwJDmr2O9
zd2ZCa5enTbOKHbNXuHjpy0k8MewKOV2muwxVcQbej8CAwEAAaCBiTAYBgkqhkiG
9w0BCQcxCxMJQzFzY28uMTIzMG0GCSqGSIb3DQEJDjFgMF4wDgYDVR0PAQH/BAQD
AgWgMCAGA1UdJQEB/wQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAJBgNVHRMEAjAA
MB8GA1UdEQQYMBaCDjEwLjIyNS4yNTMuMTY3hwQK4f2nMA0GCSqGSIb3DQEBBQUA
A4IBAQBBXOeWF5ZUz7O1GFjuQHBBDgYb+3lhFOxbYm9psIWfv1uwjkKoL297tGHv
Iux7nMyrDVkSJ81i5BSTdd9FE6AbSFswjlYpO+IxkUM971Ejwg2rj+jABDR7I8SU
O6YO6mS9x2ZJYqImeq8xwIr19Hi+7tyaLe6apfTIljdgVxB+XyzOFJMckIO5US3j
T/3aw/115RcXerdrh36oMUHEepUjIx/15u9s1c7e1mxACoQE6f9OA+fdg2zYtOME
Z6VAw64cY+YF6iLbYv7c4lizO5Zj2NJbUKpeqijkFAkY/1rIxTHypzH/p2ma4zuS
46a+kLXsVHZ716ZMB3WrUzB2ZNOO
```

```
-----END CERTIFICATE REQUEST-----
---End - This line not part of the certificate request---
Redisplay enrollment request? [yes/no]:
```

no

5단계. CA 서명 인증서를 가져옵니다.

<#root>

```
RP/0/RP0/CPU0:BRC-8201-1#
```

crypto ca import svs certificate

```
Fri May 9 15:00:35.426 UTC


Enter the base64/PEM encoded certificate/certificates.
Please note: for multiple certificates use only PEM.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIE3zCCAsegAwIBAgIINL1NAUzx14UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNTA5MTQ1NzAwWhcNMjYwNTA5MTQ1NzAwWjByMQswCQYDVQQGEwJV
UzELMAkGA1UECAwCTkMxDDAKBgNVBAcMA1JUUDEOMAwGA1UECgwFQ2lzY28xDDAK
BgNVBAsMA1NWUzEXMBUGA1UEAwwOMTAuMjI1LjI1My4xNjcxETAPBgNVBAUTCDQw
OTA4NDNiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvDH3DgOdO2uW
gMf2I5nE+8QMBHA3S3has8SNpByVlQDprHoLGr/QmVCJR/b55C/7ispmoBnXEOGJ
qIwaoROc7QsqnCa3HXQipcvtRgwcfAX29EgjnbOiaRYDxrrdbHrpSQTFpeh5dp/k
eQuioO7rxfzdTss+8x7WwzC+artGbLYMC7fQcH8l9iVAIeZNUXPczl8G3zrHHi3W
fFMVT/iVFYwLvdROvlhOokuMykFPaOOTemJn6QvinVz1ThEgGRTz8bh2vMVsa8cI
iRaTAjRxvVfYeC1tVBOJdMDAkOavY73N3ZkJrl6dNs4ods1e4eOnLSTwx7Ao5Xaa
7DFVxBt6PwIDAQABo4GAMH4wHgYJYIZIAYb4QgENBBEWD3hjYSBjZXJOaWZpY2FO
ZTAOBgNVHQ8BAf8EBAMCBaAwIAYDVR0lAQH/BBYwFAYIKwYBBQUHAwEGCCsGAQUF
BwMCMAkGA1UdEwQCMAAwHwYDVR0RBBgwFoIOMTAuMjI1LjI1My4xNjeHBArh/acw
DQYJKoZIhvcNAQELBQADggIBAARpS5bEck+ojO121O6WxedDQ8VduObBtrnOH+Nt
94EA1co7HEe4USf1FiASAX7rNveLpY3ICmLh+tQZYTZrQ93tb9mMTZg7exqN89ZU
VlXoB2UOTri5Kl0/+izEGgyNq42/ytAP8YOO7HR/2jf7gfhoRvwcR5QNOEHv4o6l
Zma5Xio1sBbkA7JB2mpzzZg4ZjsyV8lRGXxxgyt1mwNmb7EiAc8lodRcgyp7FNh3
F/k9cMMMr5lM4Ysvoltx1k9AeLjzb2syv5/fG6QuOZdWwTaaQhOY2h/cVDiV97wg
ODlmEfdSv6QrxQSujZr22RzVyKKHltuiV2B74pthUuGRBtfHS5XFy7uTTbfGX8M6
ZJw8rX1SADr8tDplrf1ZIrPmv3ZPP7woTB22yWzydOuse+5IalbOw7OtwN4t/IIw
8CJu6HfnDXLDPZOjsC8steffrSlopwGccp3j6aZKPFz+I/Purb44a9WxEWa2TA7H
+rloynBcGMetOHxVLnptlsC7Q4mN/MDXeGyW+OTNCirNEG/gqcu+dn9EnNKkE2WV
oF537Ow+uNHoK8Bdt8mqadUT4OoUSqY8ArVOBomO5tzbemreVPmQAZ/IahZ7TqKo
3dGNonTAfFTESM1iujQ81iRKsikDHySnwcCM2nilCKZrhVq5IB8NK6jKRJZOeQAX
vMt1
-----END CERTIFICATE-----
```

quit

```
Serial Number : C2:F4:AB:34:02:D2:76:74:65:34:FE:D5
Subject:
serialNumber=4090843b,CN=10.225.253.167,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
Issued By :
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
```

```
Validity Start : 14:57:00 UTC Fri May 09 2025
Validity End : 14:57:00 UTC Sat May 09 2026
SHA1 Fingerprint:
21E4DA0B02181D08B6E51F0CC754BCE5B815C792
```

라우터 ID 인증서가 등록되었는지 확인합니다.

<#root>

```
RP/0/RP0/CPU0:BRC-8201-1#
```

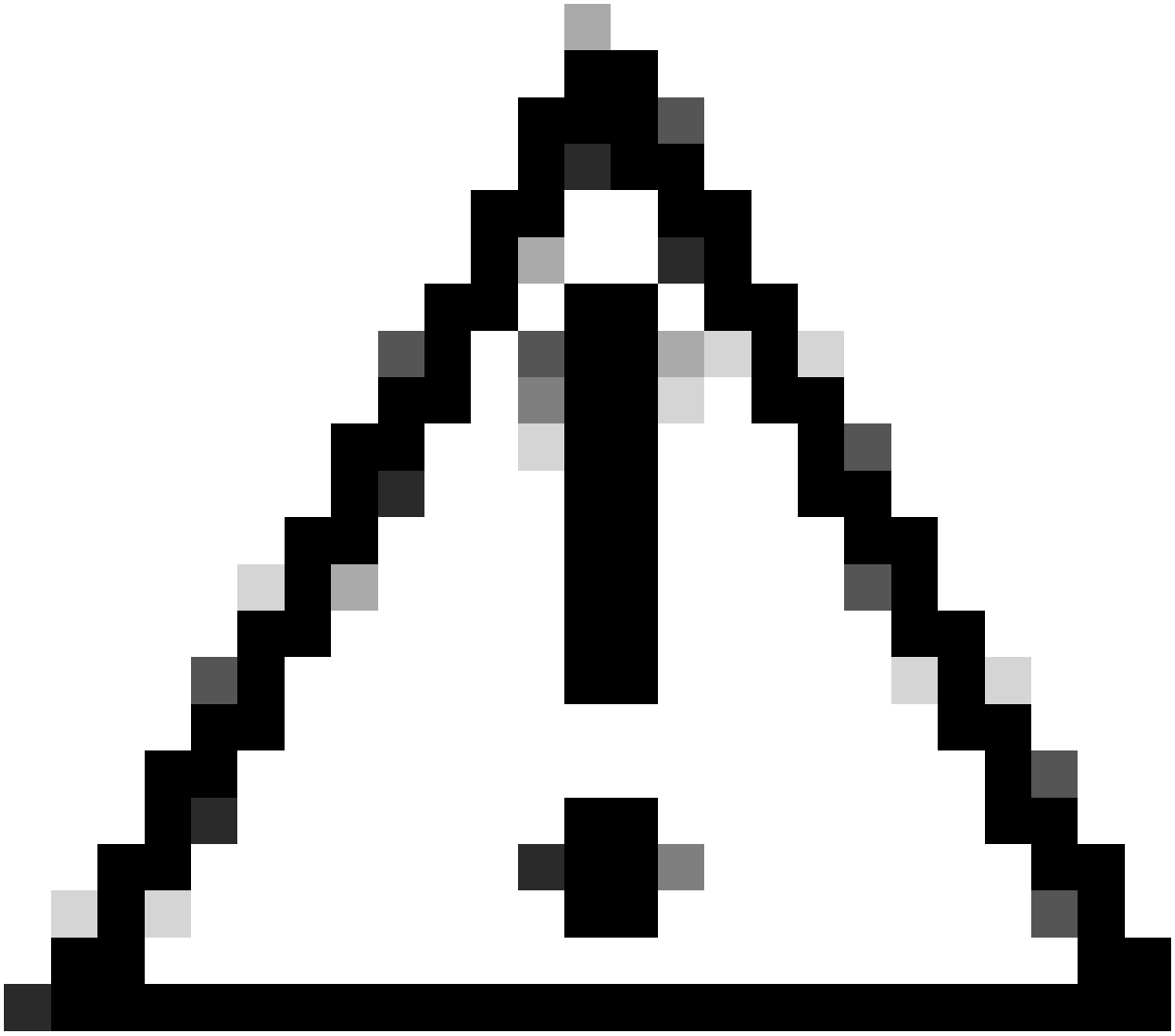
show crypto ca trustpoint svs detail

```
Trustpoint        :svs-new
================================================================
KeyPair Label: the_default
CRL:optional
enrollment: terminal
subject name: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=brc-8201-1.svs.lab

RP/0/RP0/CPU0:BRC-8201-1#
```

show crypto ca certificates svs

```
Wed May 14 14:55:58.173 UTC

Trustpoint       : svs-new
================================================
CA certificate
  Serial Number  : 20:01:20:1F:B6:9D:C3:FE:43:78:FF:64
  Subject:
        CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
  Issued By      :
        CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
  Validity Start : 17:05:00 UTC Mon Apr 28 2025
  Validity End   : 17:05:00 UTC Sat Apr 28 2035
  SHA1 Fingerprint:
         0EB181E95A3ED7803BC5A8059A854A95C83AC737
Router certificate
  Key usage      : General Purpose
  Status         : Available
  Serial Number  : FD:AC:20:1F:B6:9D:C3:FE:98:43:ED
  Subject:
        serialNumber=4090843b,CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
  Issued By      :
        CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
  Validity Start : 19:59:00 UTC Fri May 09 2025
  Validity End   : 19:59:00 UTC Sat May 09 2026
  SHA1 Fingerprint:
         AC17E4772D909470F753BDBFA463F2DF522CC2A6
Associated Trustpoint: svs
```

TLS를 사용하여 TACACS 및 AAA 구성



주의: 로컬 자격 증명을 사용하여 콘솔을 통해 컨피그레이션 변경을 수행합니다.

1단계. TACACS+ 서버를 구성합니다.

```
tacacs source-interface MgmtEth0/RP0/CPU0/0 vrf mgmt
tacacs-server host 10.225.253.209 port 49
  key 7 072C705F4D0648574453

aaa group server tacacs+ tacacs2
 server 10.225.253.209
 vrf mgmt
```

2단계. AAA 그룹을 구성합니다.

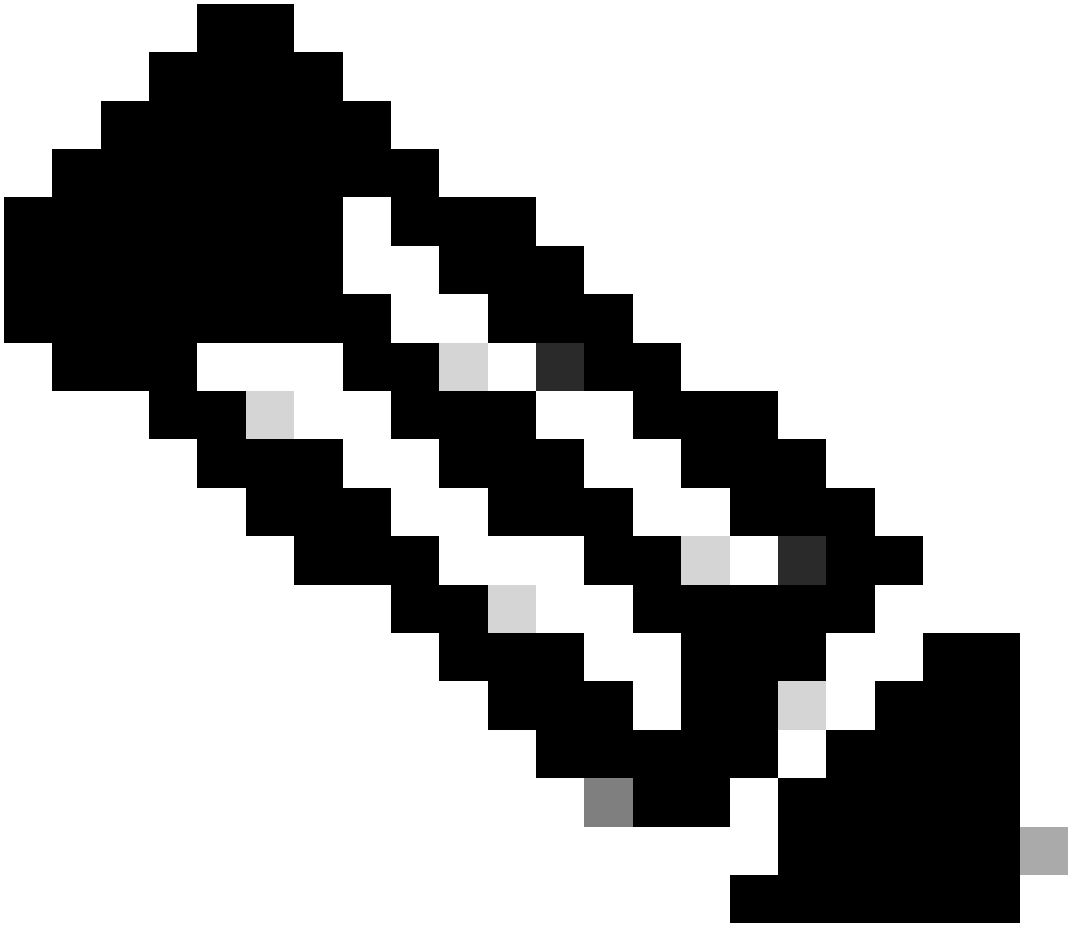
```
aaa group server tacacs+ tac_tls_sc
```

```
 vrf mgmt
 server-private 10.225.253.209 port 6049
  timeout 10
  tls
   trustpoint svs
  !
  single-connection
```

2단계. AAA를 구성합니다.

```
aaa accounting exec default start-stop group tac_tls_sc
aaa accounting system default start-stop group tac_tls_sc
aaa accounting network default start-stop group tac_tls_sc
aaa accounting commands default stop-only group tac_tls_sc
aaa authorization exec default group tac_tls_sc local
aaa authorization commands default group tac_tls_sc none
aaa authentication login default group tac_tls_sc local
```

인증서 갱신



참고: 신뢰 지점은 갱신 중에 TACACS+ 컨피그레이션에서 제거할 필요가 없습니다.

1단계. 현재 인증서 유효 날짜를 확인합니다.

```
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates svs-new
Thu Aug 14 15:13:37.465 UTC

Trustpoint : svs-new
================================================
CA certificate
  Serial Number : 30:A2:10:14:C9:5E:B0:E0:07:CE:0A:24:16:69:90:ED:D1:34:B5:9B
  Subject:
        CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Issued By :
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 22:13:17 UTC Thu Jun 26 2025
  Validity End : 22:13:16 UTC Tue Jun 25 2030

  CRL Distribution Point
```

```
http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=m9uBlQsZDYy6wxomiFWB5GvOAZM

  SHA1 Fingerprint:
        EA8FB276563B927FCAF0174D9FD1C58F3E8B5FF2
Trusted Certificate Chain
  Serial Number : 1F:A6:6E:2E:F8:AB:CE:B4:9C:B8:07:5A:9F:2B:32:02:B4:56:5C:96
  Subject:
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Issued By :
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 22:13:17 UTC Thu Jun 26 2025
  Validity End : 22:13:16 UTC Sun Jun 24 2035
  SHA1 Fingerprint:
        E225647FF9BDA176D2998D5A3A9770270F37D2A7
Router certificate
  Key usage : General Purpose
  Status : Available
  Serial Number : 7A:13:EB:C0:6A:8D:66:68:09:0B:32:C7:0C:D8:05:BD:81:72:9B:4E
  Subject:
        CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
  Issued By :
        CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 16:38:36 UTC Wed Jul 30 2025
  Validity End : 16:38:35 UTC Thu Jul 30 2026
  CRL Distribution Point

http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=X4as2q+6I9Bd4QglQa8g1xoH8GY
  SHA1 Fingerprint:
        B562F3CF507CE7F97893F28BC896794CFF6995C1
Associated Trustpoint: svs-new
```

2단계. 기존 신뢰 지점 인증서를 삭제합니다.

```
RP/0/RP0/CPU0:BRC-8201-1#clear crypto ca certificates KF_TP
Thu Aug 14 15:25:26.286 UTC
certificates cleared for trustpoint KF_TP
RP/0/RP0/CPU0:Aug 14 15:25:26.577 UTC: cepki[382]: %SECURITY-CEPKI-6-INFO : certificate database update
RP/0/RP0/CPU0:BRC-8201-1#
RP/0/RP0/CPU0:BRC-8201-1#
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates KF_TP
Thu Aug 14 15:25:37.270 UTC
RP/0/RP0/CPU0:BRC-8201-1#
```

3단계. Trustpoint Configuration(신뢰 지점 컨피그레이션)의 단계에 설명된 대로 신뢰 지점을 재인증하고 등록합니다.

4단계. 인증서 유효 날짜가 업데이트되었는지 확인합니다.

```
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates KF_TP
Thu Aug 14 15:31:28.309 UTC

Trustpoint : KF_TP
==================================================
```

```
CA certificate
  Serial Number : 30:A2:10:14:C9:5E:B0:E0:07:CE:0A:24:16:69:90:ED:D1:34:B5:9B
  Subject:
CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Issued By :
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 22:13:17 UTC Thu Jun 26 2025
  Validity End : 22:13:16 UTC Tue Jun 25 2030

  CRL Distribution Point

http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=m9uBlQsZDYy6wxomiFWB5Gv0AZM
  SHA1 Fingerprint:
        EA8FB276563B927FCAF0174D9FD1C58F3E8B5FF2
Trusted Certificate Chain
  Serial Number : 1F:A6:6E:2E:F8:AB:CE:B4:9C:B8:07:5A:9F:2B:32:02:B4:56:5C:96
  Subject:
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Issued By :
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 22:13:17 UTC Thu Jun 26 2025
  Validity End : 22:13:16 UTC Sun Jun 24 2035
  SHA1 Fingerprint:
        E225647FF9BDA176D2998D5A3A9770270F37D2A7
Router certificate
  Key usage : General Purpose
  Status : Available
  Serial Number : 1F:B0:AE:44:CF:8E:24:62:83:42:2F:34:BF:D0:82:07:DF:E4:49:0B
  Subject:
        CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
  Issued By :
        CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 15:17:29 UTC Thu Aug 14 2025
  Validity End : 15:17:28 UTC Fri Aug 14 2026

  CRL Distribution Point

http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=X4as2q+6I9Bd4QglQa8g1xoH8GY
  SHA1 Fingerprint:
        D3CE0AEB51C5E8009F626A1A9FD633FB9AFA96DE
Associated Trustpoint: KF_TP
```

확인

구성 확인.

```
show crypto ca certificates [detail]
show crypto ca trustpoint detail
show tacacs details
```

TACACS+에 대한 디버그

```
debug tacacs tls
```

TLS 디버그

```
debug ssl error
debug ssl events
```

AAA 인증을 구성하기 전에 원격 사용자를 테스트합니다.

<#root>

test aaa group tacacs2

```
user has been authenticated
```

문제 해결

인증서 지우기(신뢰 지점과 연결된 모든 인증서가 삭제됩니다).

```
clear crypto ca certificate <trustpoint name>
```

TACACS 프로세스 재시작(필요한 경우)

```
process restart tacacsd
```

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.