TACACS+ configureren via TLS 1.3 op een IOS XR-apparaat met ISE

Inhoud

Inleiding

Dit document beschrijft een voorbeeld voor TACACS+ over TLS met Cisco Identity Services Engine (ISE) als server en een Cisco IOS® XR-apparaat als client.

Overzicht

Het Terminal Access Controller Access-Control System Plus (TACACS+) Protocol [RFC8907] maakt gecentraliseerd apparaatbeheer mogelijk voor routers, netwerktoegangsservers en andere netwerkapparaten via een of meer TACACS+-servers. Het biedt authenticatie-, autorisatie- en boekhouddiensten (AAA), specifiek afgestemd op gebruikssituaties voor apparaatbeheer.

TACACS+ over TLS 1.3 [RFC8446] verbetert het protocol door een beveiligde transportlaag in te voeren, waardoor zeer gevoelige gegevens worden beschermd. Deze integratie waarborgt vertrouwelijkheid, integriteit en authenticatie voor de verbinding en het netwerkverkeer tussen TACACS+-clients en -servers.

Gebruik van deze Guide

Deze handleiding verdeelt de activiteiten in twee delen zodat ISE beheerderstoegang kan beheren voor Cisco IOS XR-gebaseerde netwerkapparaten.
· Deel 1 – Configureer ISE voor Apparaatbeheer
· Deel 2 - Cisco IOS XR configureren voor TACACS+ via TLS

Voorwaarden

Vereisten

Vereisten voor het configureren van TACACS+ via TLS:

- Een certificeringsinstantie (CA) om het certificaat te ondertekenen dat door TACACS+ over TLS wordt gebruikt om de certificaten van ISE en netwerkapparaten te ondertekenen.
- Het basiscertificaat van de certificeringsinstantie (CA).
- Netwerkapparaten en ISE hebben DNS-bereikbaarheid en kunnen hostnamen oplossen.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ISE VMware virtual appliance, release 3.4 patch 2
- Cisco 8201 Router, versie 25.3.1

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

vergunning

Met een Device Administration-licentie kunt u TACACS+-services gebruiken op een Policy

Service-node. Bij een standalone implementatie met hoge beschikbaarheid (HA) kunt u met een Device Administration-licentie TACACS+-services gebruiken op één Policy Service-node in het HA-paar.

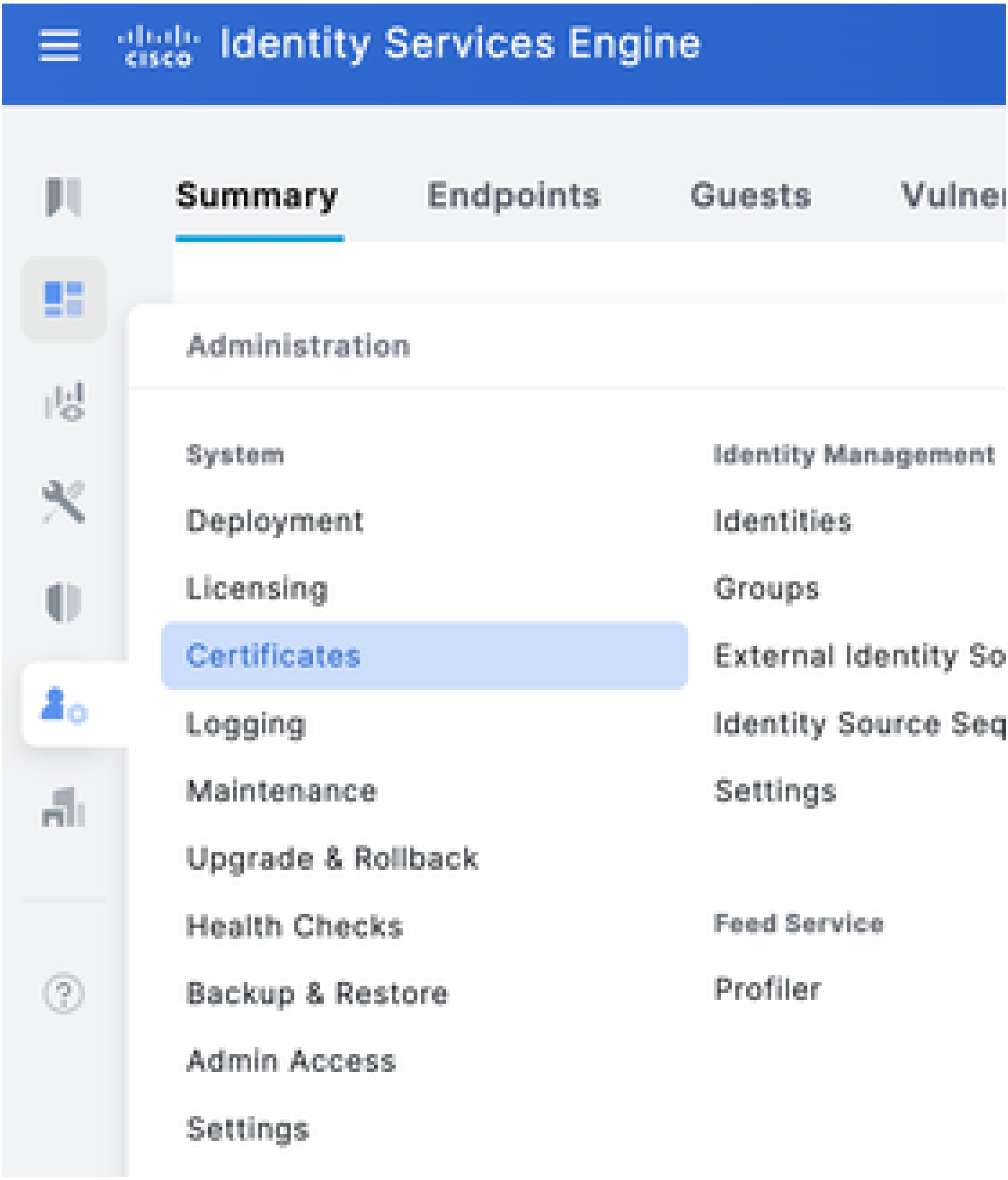
Deel 1 - ISE-configuratie voor apparaatbeheer

Aanvraag voor certificaatondertekening genereren voor TACACS+-serververificatie

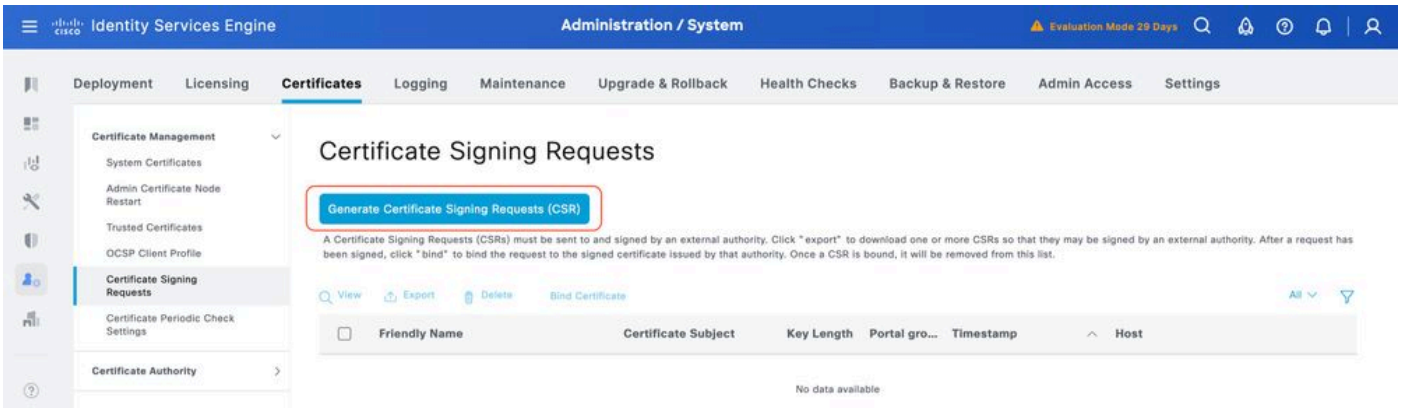
Stap 1. Meld u aan bij de ISE-beheerdersportal met een van de ondersteunde browsers.

Standaard gebruikt ISE een zelf ondertekend certificaat voor alle services. De eerste stap is het genereren van een Certificate Signing Request (CSR) om het te laten ondertekenen door onze Certificate Authority (CA).

Stap 2. Ga naar Beheer > Systeem > Certificaten.

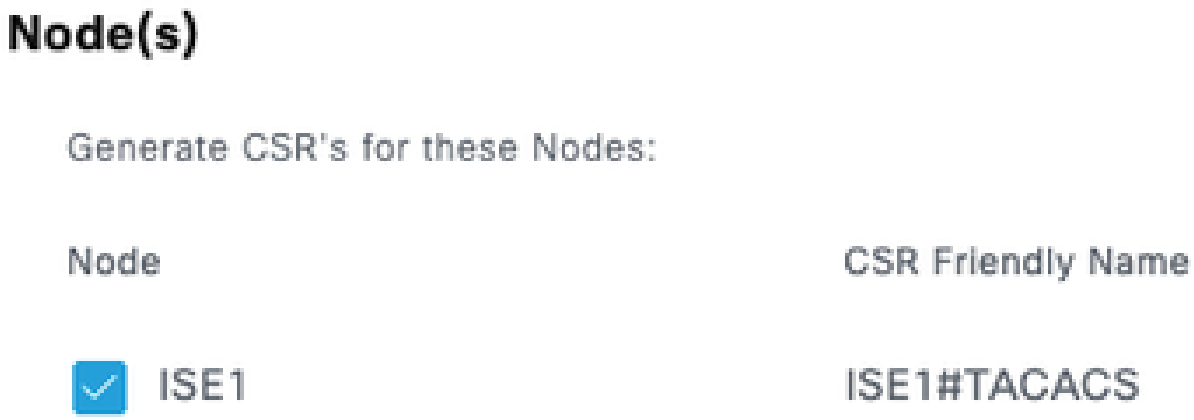


Stap 3. Klik onder Certificaatondertekeningsverzoeken op Certificaatondertekeningsverzoek genereren.

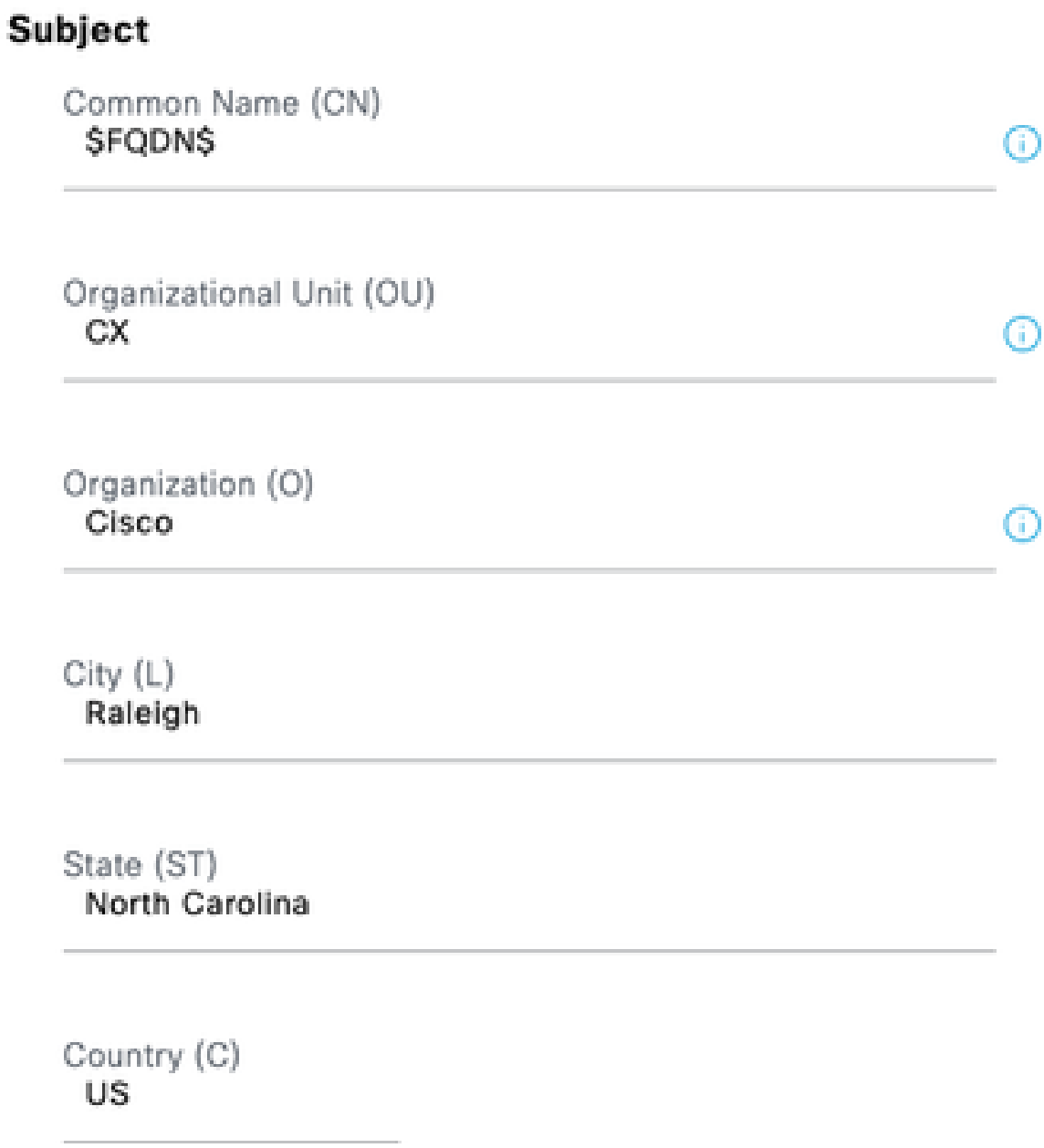


Stap 4. Selecteer TACACS in gebruik.

Stap 5. Selecteer de PSN's waarvoor TACACS+ is ingeschakeld.

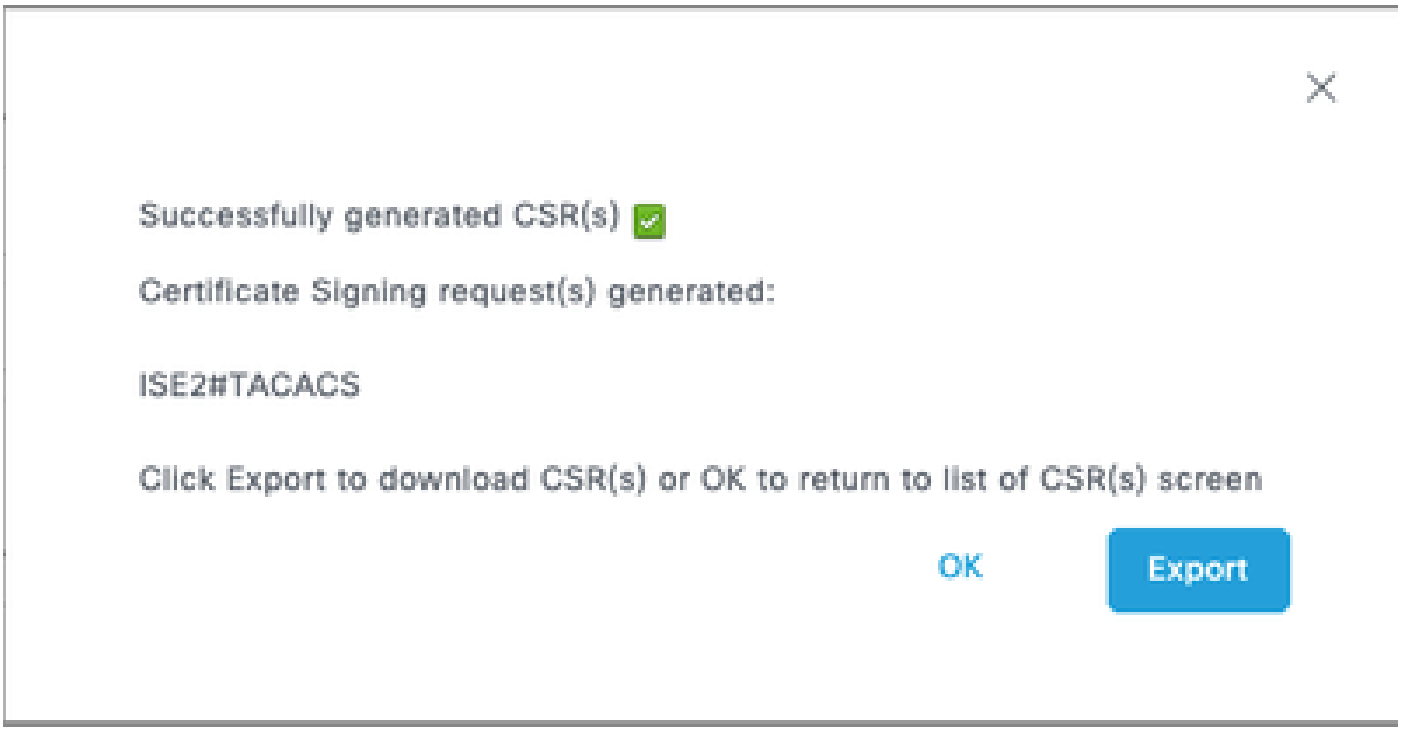


Stap 6. Vul de onderwerpvelden in met de juiste informatie.



Stap 7. Voeg de DNS-naam en het IP-adres toe onder Alternatieve onderwerpnaam (SAN).

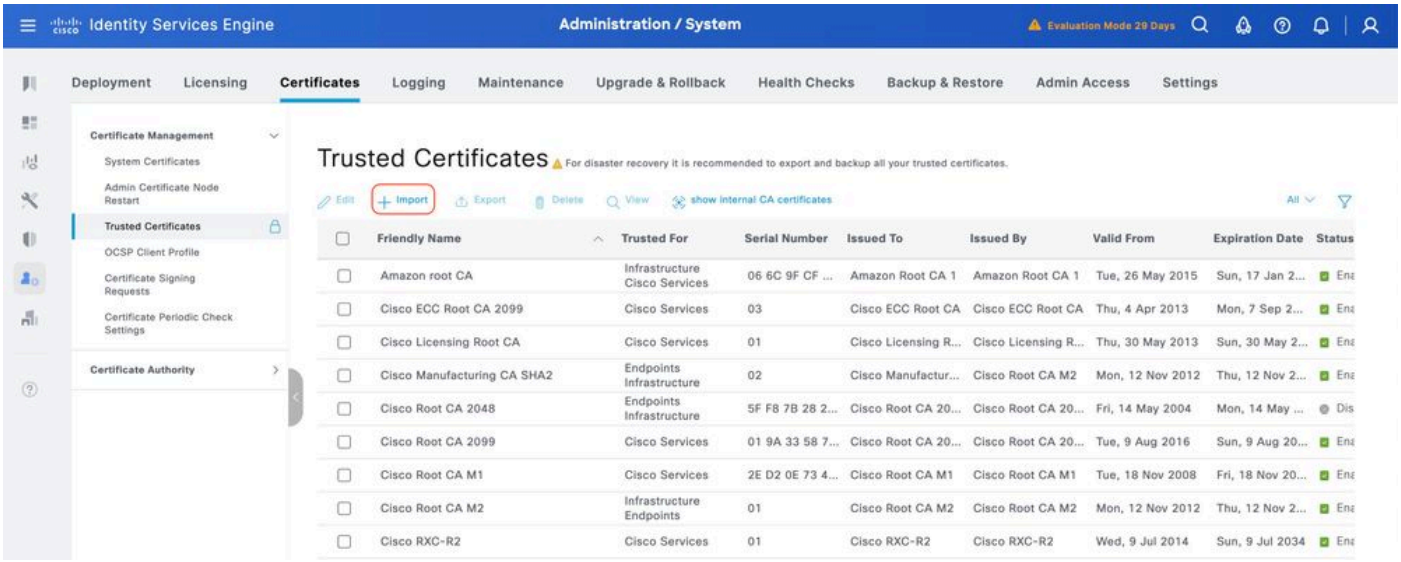
Stap 8. Klik op Genereren en vervolgens op Exporteren.



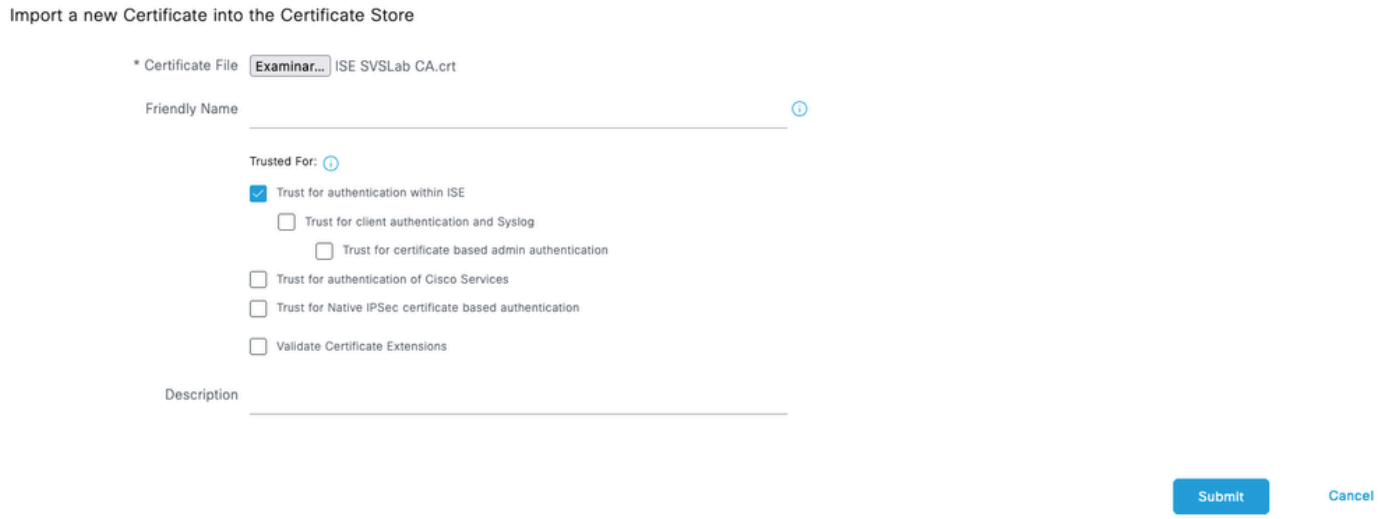
Nu kunt u het certificaat (CRT) laten ondertekenen door uw certificeringsinstantie (CA).

Root CA-certificaat uploaden voor TACACS+-serververificatie

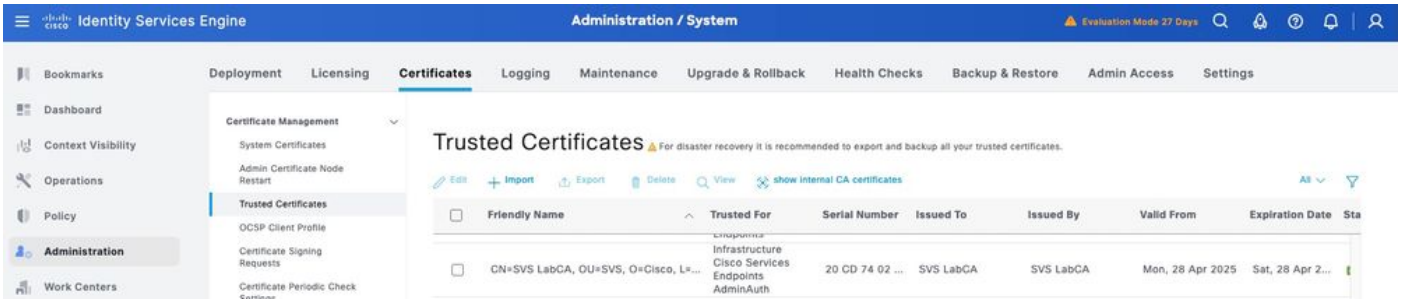
Stap 1.Navigeer naar Beheer > Systeem > Certificaten. Klik onder Vertrouwde certificaten op Importeren.



Stap 2. Selecteer het certificaat dat is afgegeven door de certificeringsinstantie (CA) die uw TACACS-certificaatondertekeningsverzoek heeft ondertekend. Zorg ervoor dat de Vertrouwen voor authenticatie binnen ISE optie is ingeschakeld.



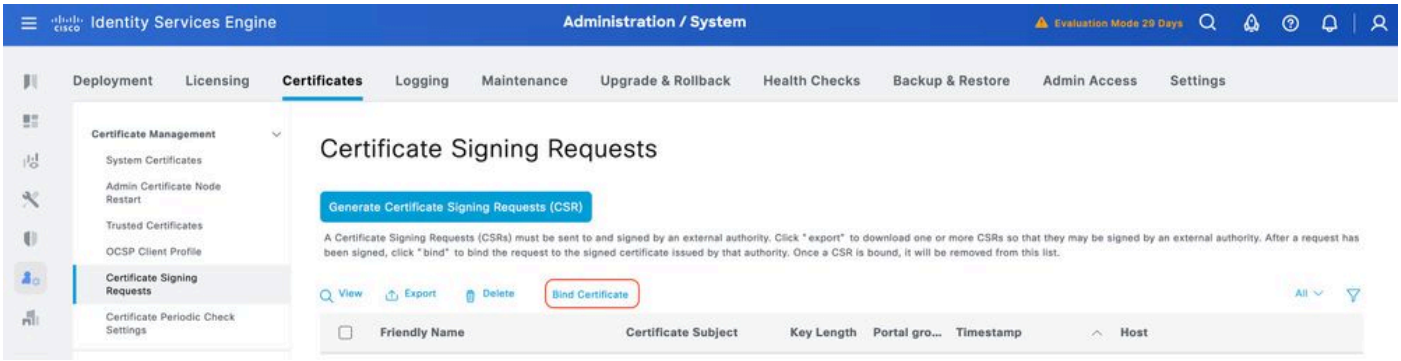
Klik op Indienen. Het certificaat moet nu worden weergegeven onder Vertrouwde certificaten.



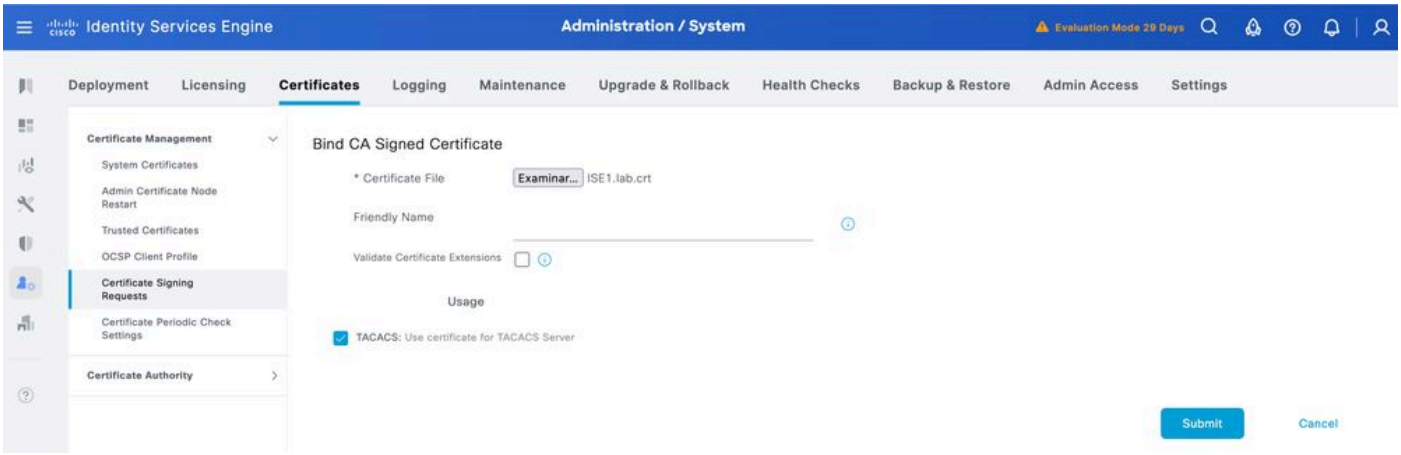
Het ondertekende certificaatondertekeningsverzoek (CSR) binden aan ISE

Zodra het Certificate Signing Request (CSR) is ondertekend, kunt u het ondertekende certificaat op ISE installeren.

Stap 1.Navigeer naar Beheer > Systeem > Certificaten. Selecteer onder Certificaatondertekeningsverzoeken de in de vorige stap gegenereerde TACACS-CSR en klik op Certificaat binden.

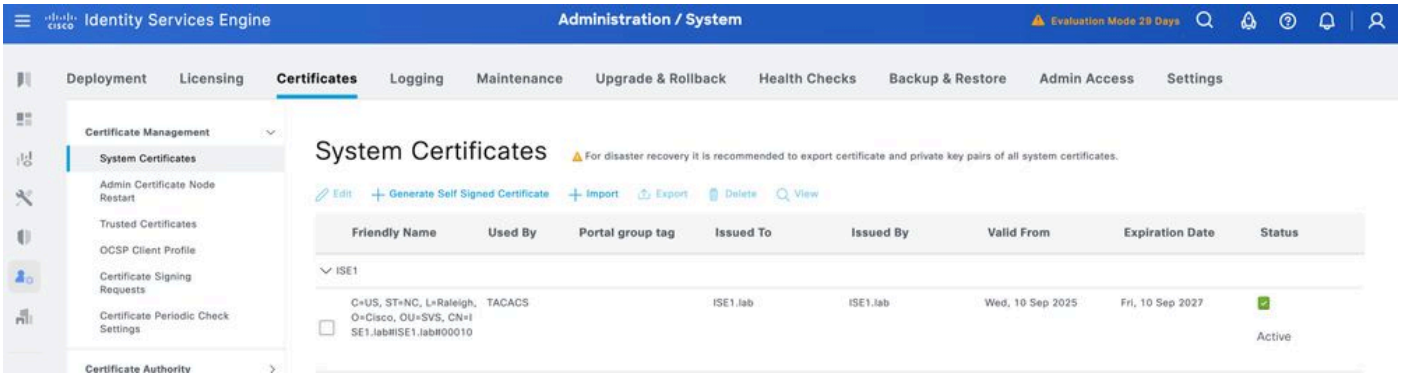


Stap 2.Selecteer het ondertekende certificaat en zorg ervoor dat het selectievakje TACACS onder Gebruik geselecteerd blijft.



Stap 3. Klik op Indienen. Als u een waarschuwing ontvangt over het vervangen van het bestaande certificaat, klikt u op Ja om door te gaan.

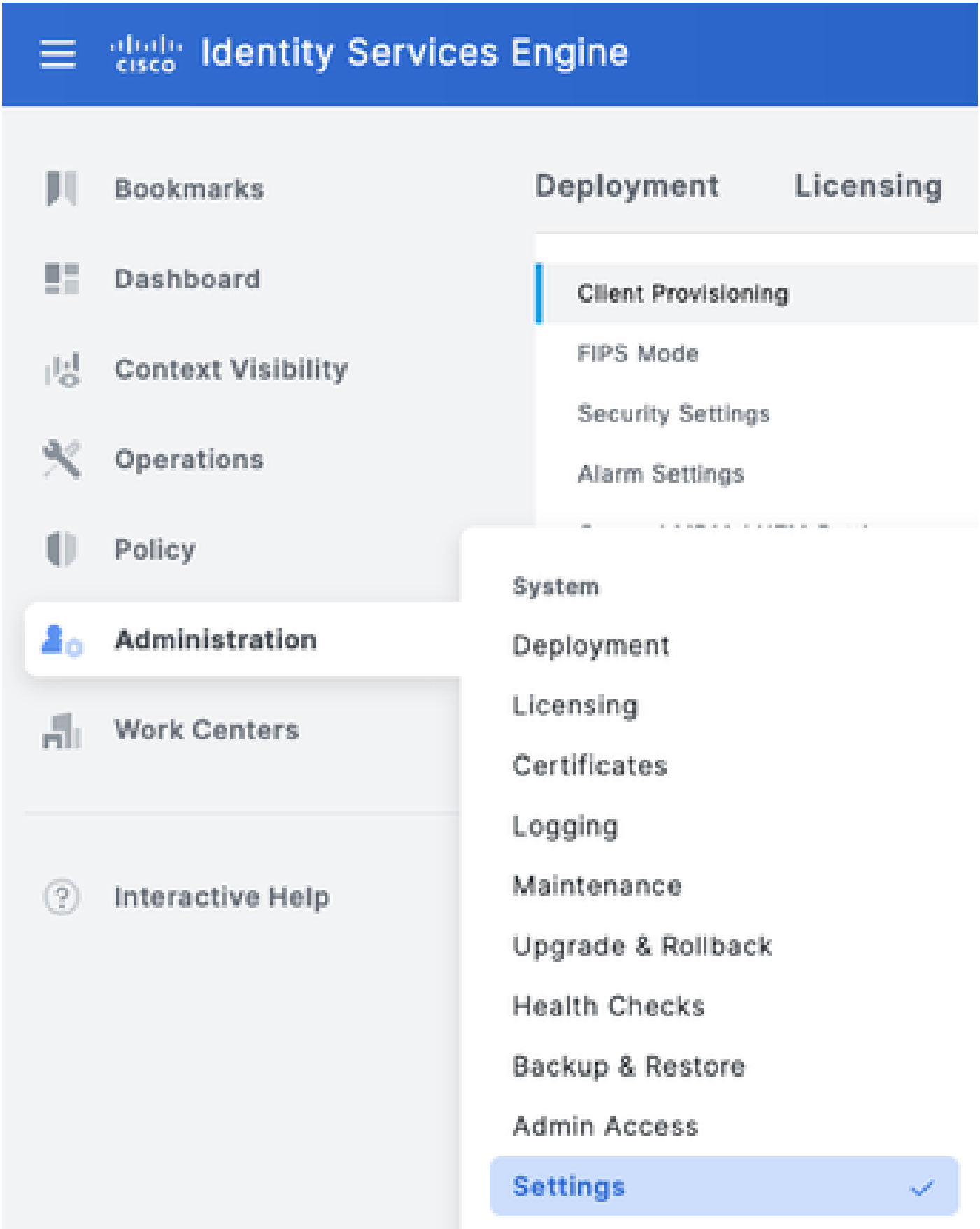
Het certificaat moet nu correct worden geïnstalleerd. U kunt dit controleren onder Systeemcertificaten.



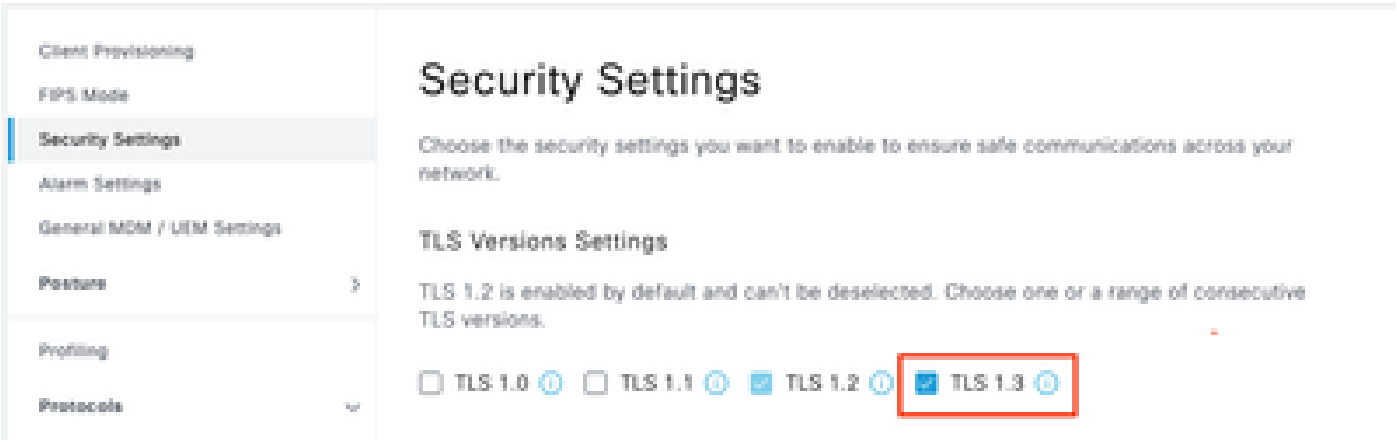
TLS 1.3 inschakelen

TLS 1.3 is standaard niet ingeschakeld in ISE 3.4.x. Het moet handmatig worden ingeschakeld.

Stap 1.Navigeer naar Beheer > Systeem > Instellingen.



Stap 2. Klik op Beveiligingsinstellingen, selecteer het selectievakje naast TLS1.3 onder Versie-instellingen TLS en klik vervolgens op Opslaan.

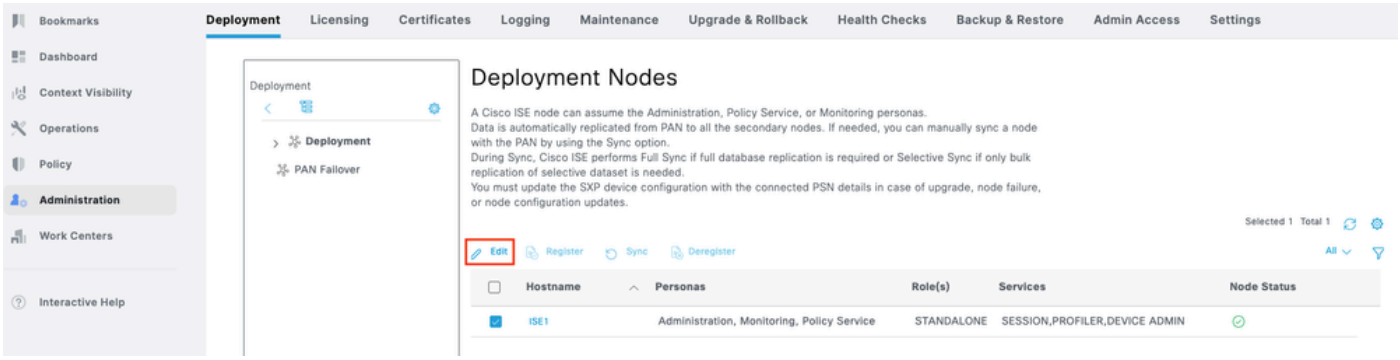


Waarschuwing: wanneer u de TLS-versie wijzigt, wordt de Cisco ISE-toepassingsserver opnieuw gestart op alle Cisco ISE-implementatiemachines.

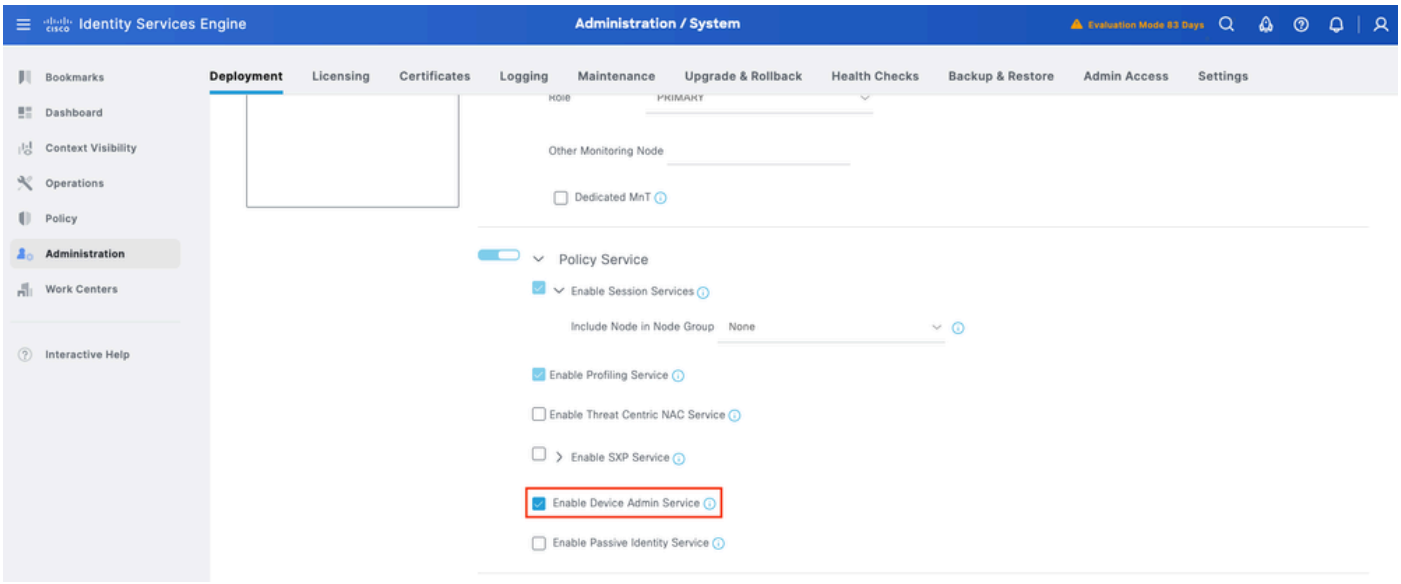
Apparaatbeheer inschakelen op ISE

De service Apparaatbeheer (TACACS+) is standaard niet ingeschakeld op een ISE-node. TACACS+ inschakelen op een PSN-node:

Stap 1. Ga naar Beheer > Systeem > Implementatie. Schakel het selectievakje naast de ISE-node in en klik op Bewerken.



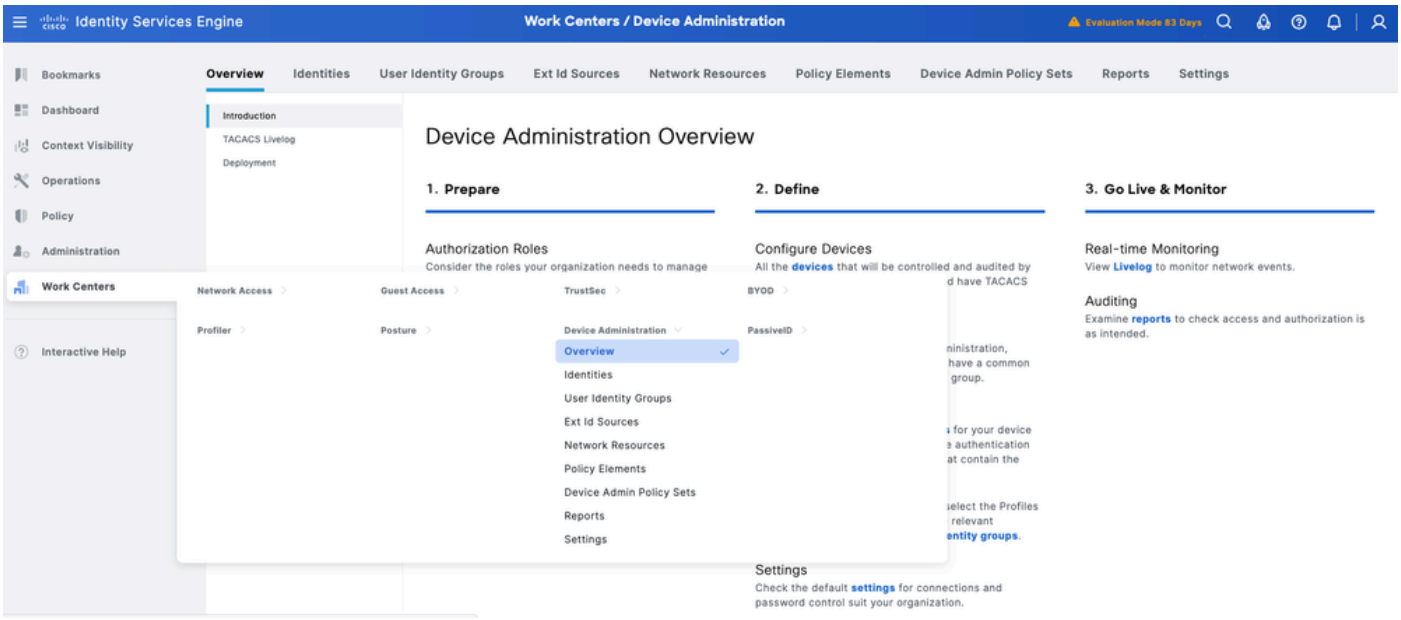
Stap 2. Blader onder Algemene instellingen omlaag en schakel het selectievakje naast Apparaatbeheerservice inschakelen in.



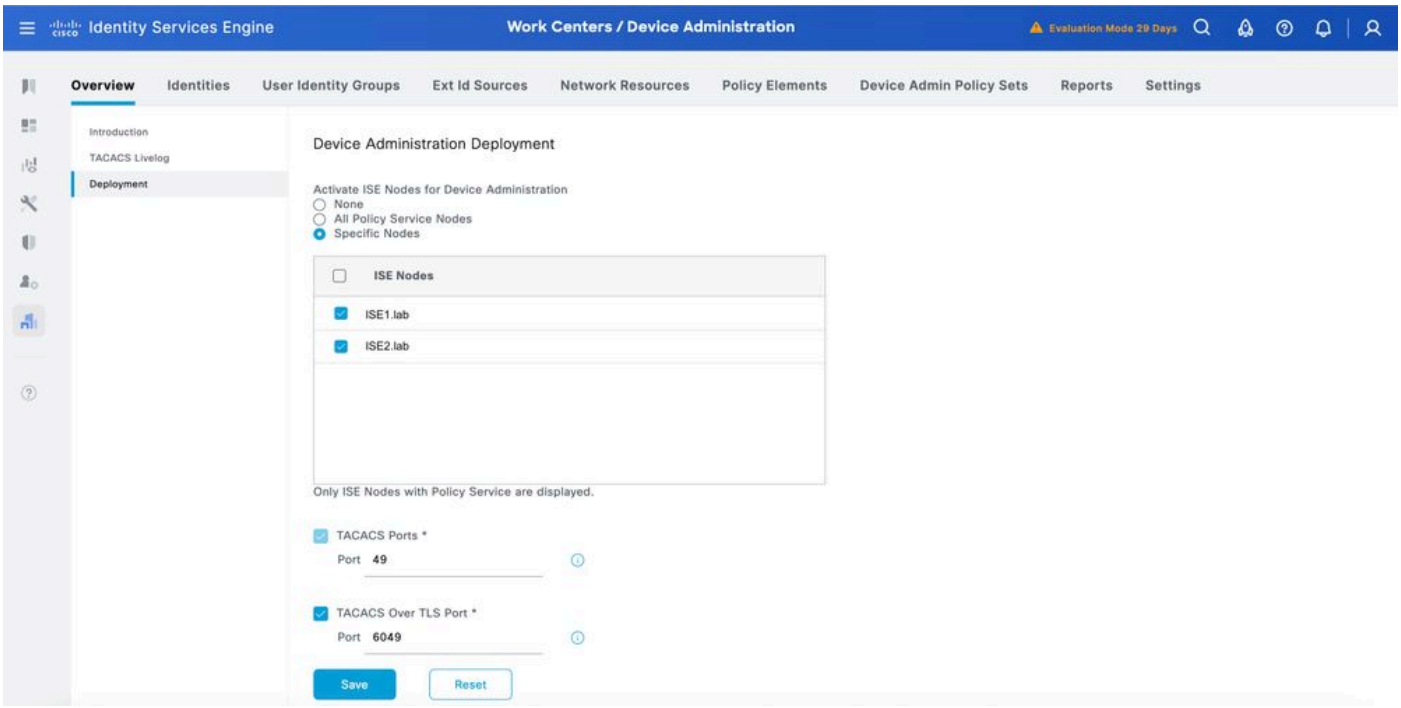
Stap 3. Sla de configuratie op. Device Admin Service is nu ingeschakeld op ISE.

TACACS via TLS inschakelen

Stap 1.Navigeer naar werkcentra > Apparaatbeheer > Overzicht.



Stap 2. Klik op Implementatie. Selecteer de PSN-knooppunten waar u TACACS via TLS wilt inschakelen.

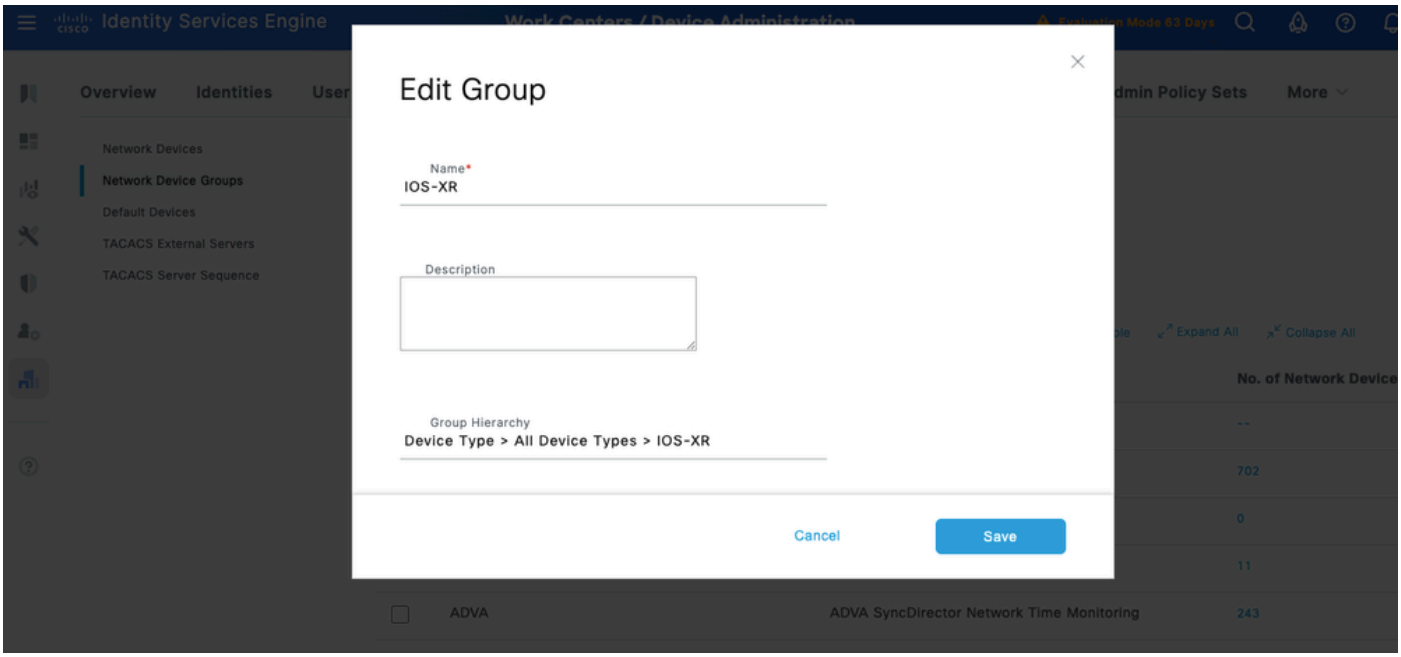


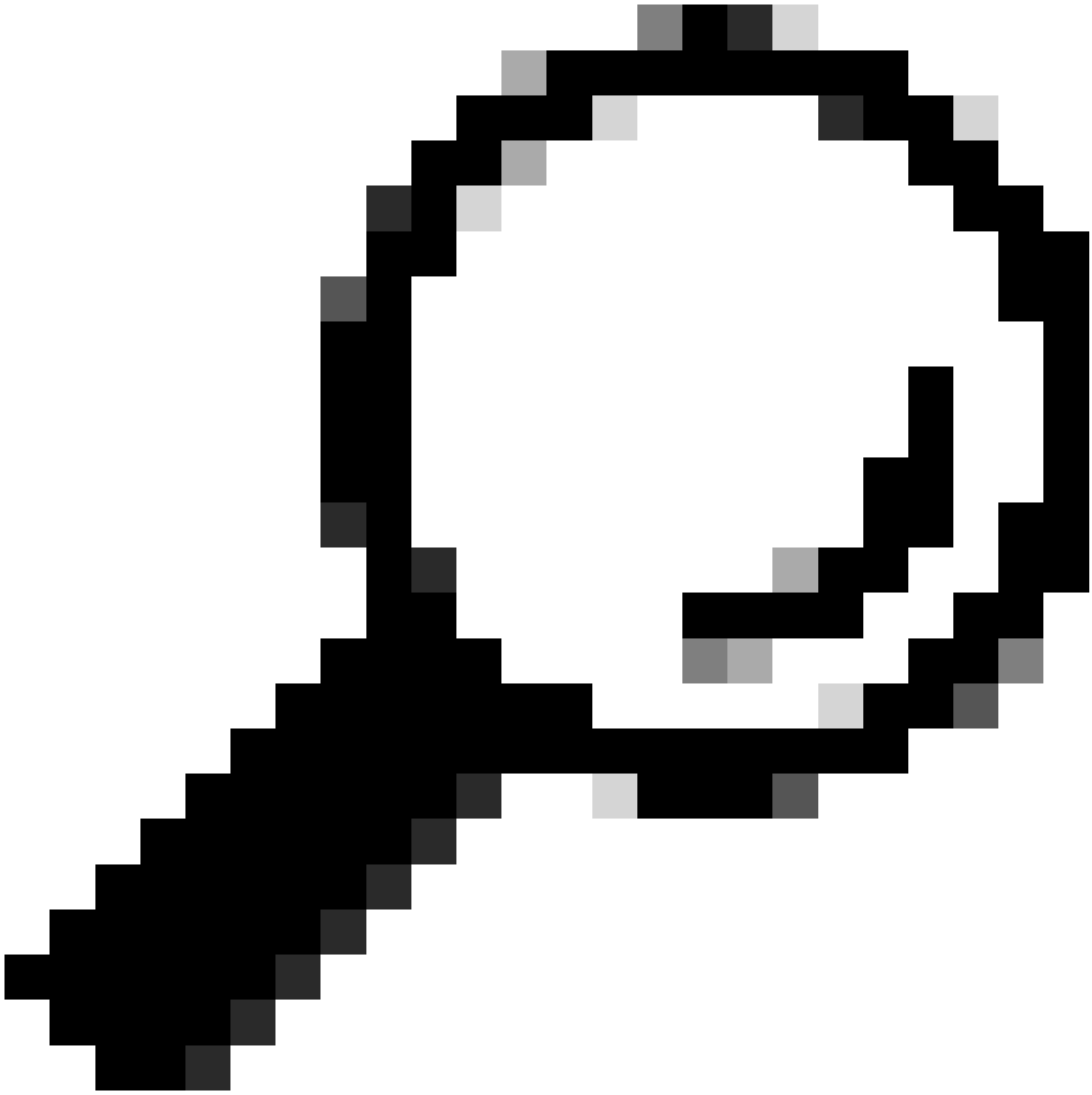
Stap 3.Behoud de standaardpoort 6049 of geef een andere TCP-poort op voor TACACS via TLS en klik vervolgens op Opslaan.

Netwerkapparaat- en netwerkapparaatgroepen maken

ISE biedt krachtige apparaatgroepering met meerdere apparaatgroephiërarchieën. Elke hiërarchie vertegenwoordigt een afzonderlijke en onafhankelijke classificatie van netwerkapparaten.

Stap 1.Navigeer naar Werkcentra > Apparaatbeheer > Netwerkbronnen.Klik op Netwerkapparaatgroepen en maak een groep met de naam IOS XR.

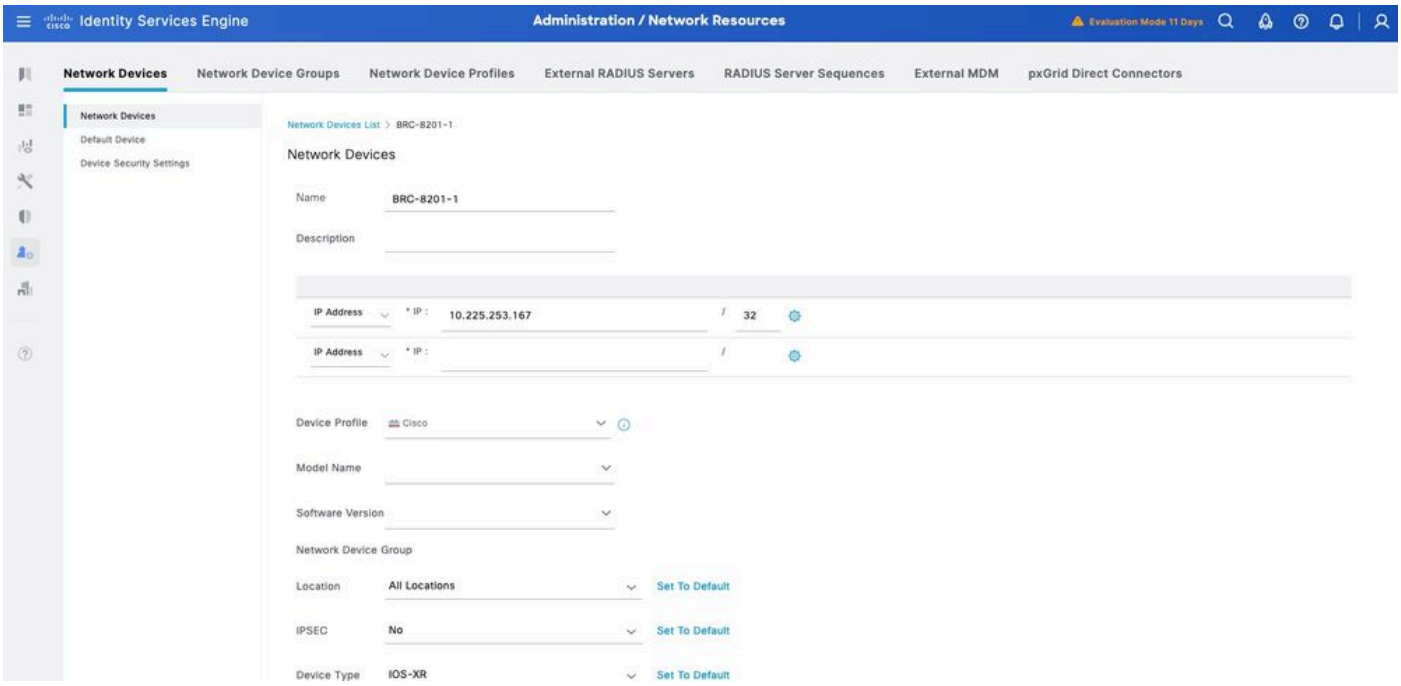

Identity Services Engine
Work Centers / Device Administration
Overview
Identities
User
Admin Policy Sets
More
Network Devices
Network Device Groups
Default Devices
TACACS External Servers
TACACS Server Sequence
Expand All
Collapse All
No. of Network Device
Edit Group
Name*
IOS-XR
Description
Group Hierarchy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



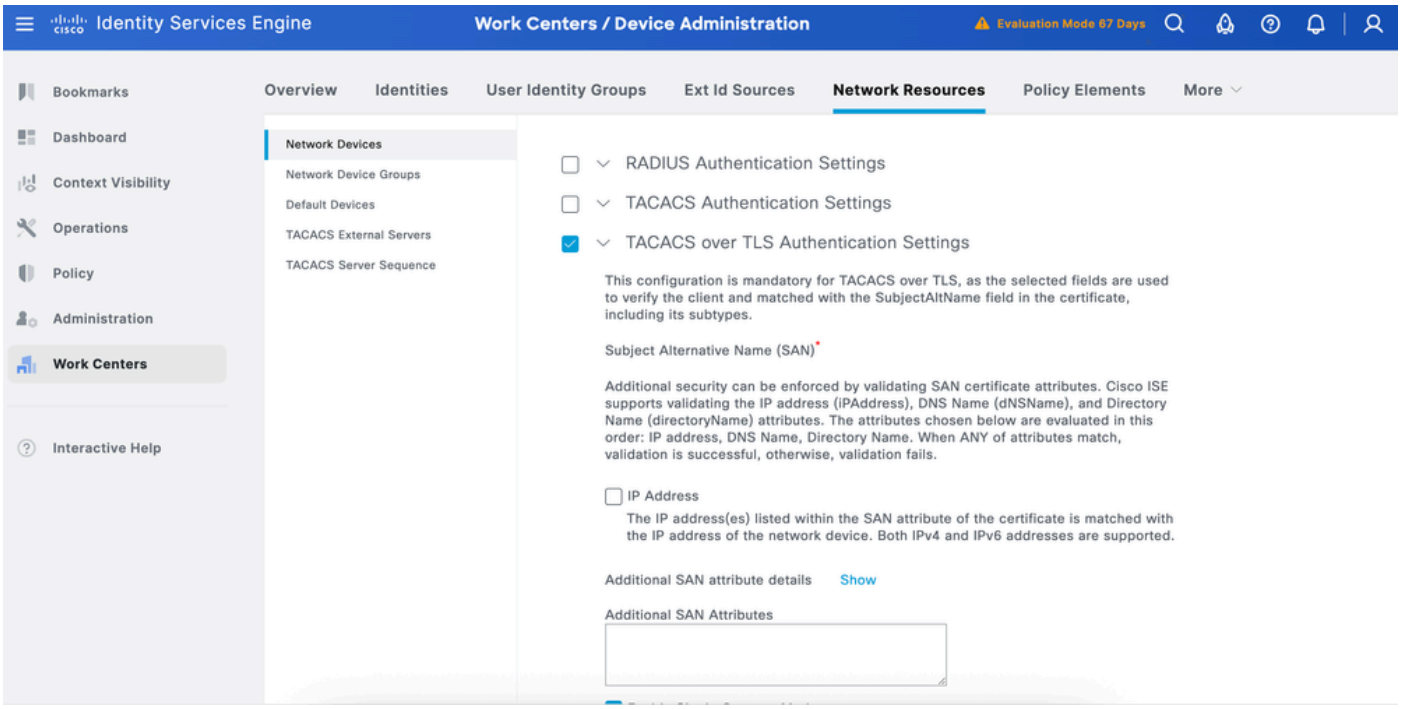
Tip: Alle apparaattypen en alle locaties zijn standaard hiërarchieën die door ISE worden verstrekt. U kunt uw eigen hiërarchieën toevoegen en de verschillende componenten definiëren bij het identificeren van een netwerkapparaat dat later in de beleidsvoorwaarde kan worden gebruikt

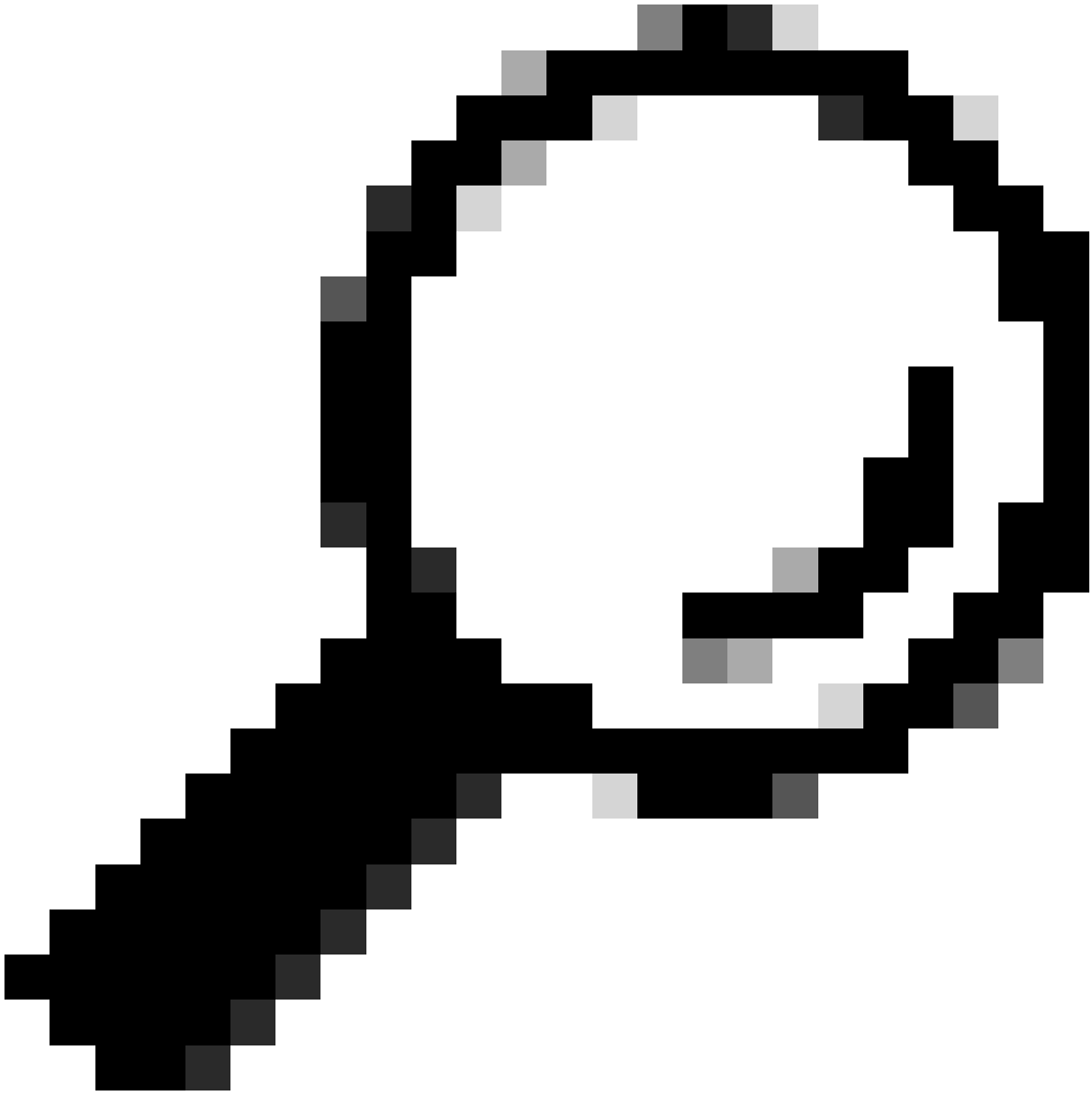
---

Stap 2. Voeg nu een Cisco IOS XR-apparaat toe als netwerkapparaat. Navigeer naar Werkcentra **>** Apparaatbeheer **>** Netwerkbronnen **>** Netwerkapparaten. Klik op Toevoegen om een nieuw netwerkapparaat toe te voegen.



Stap 3.Voer het IP-adres van het apparaat in en zorg ervoor dat u de locatie en het apparaattype (IOS XR) voor het apparaat in kaart brengt. Schakel ten slotte de TACACS+ over TLS-verificatie-instellingen in.



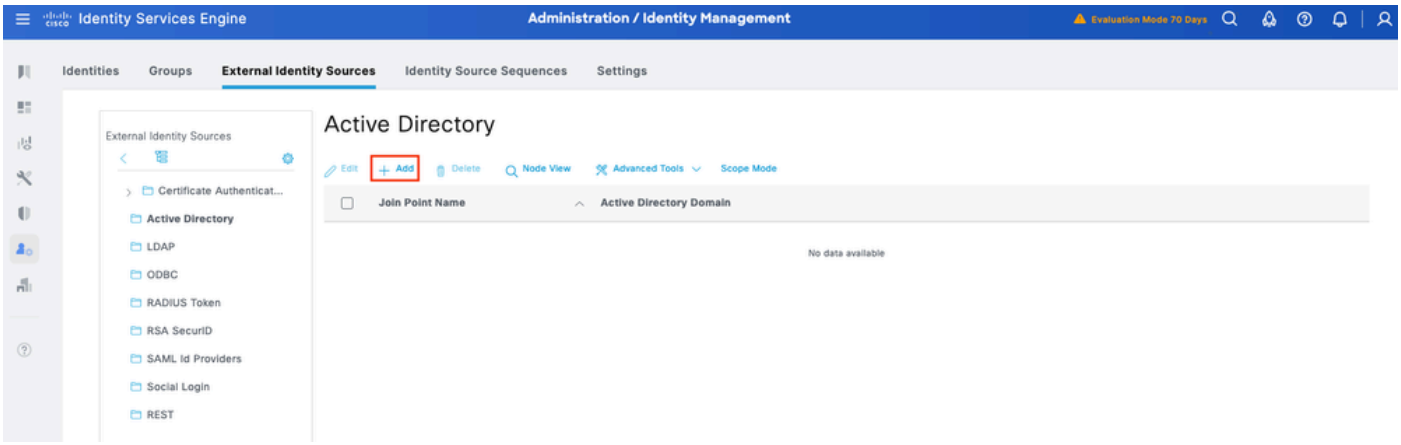


Tip: Het wordt aanbevolen om de modus Single Connect in te schakelen om te voorkomen dat de TCP-sessie opnieuw wordt gestart telkens wanneer een opdracht naar het apparaat wordt verzonden.

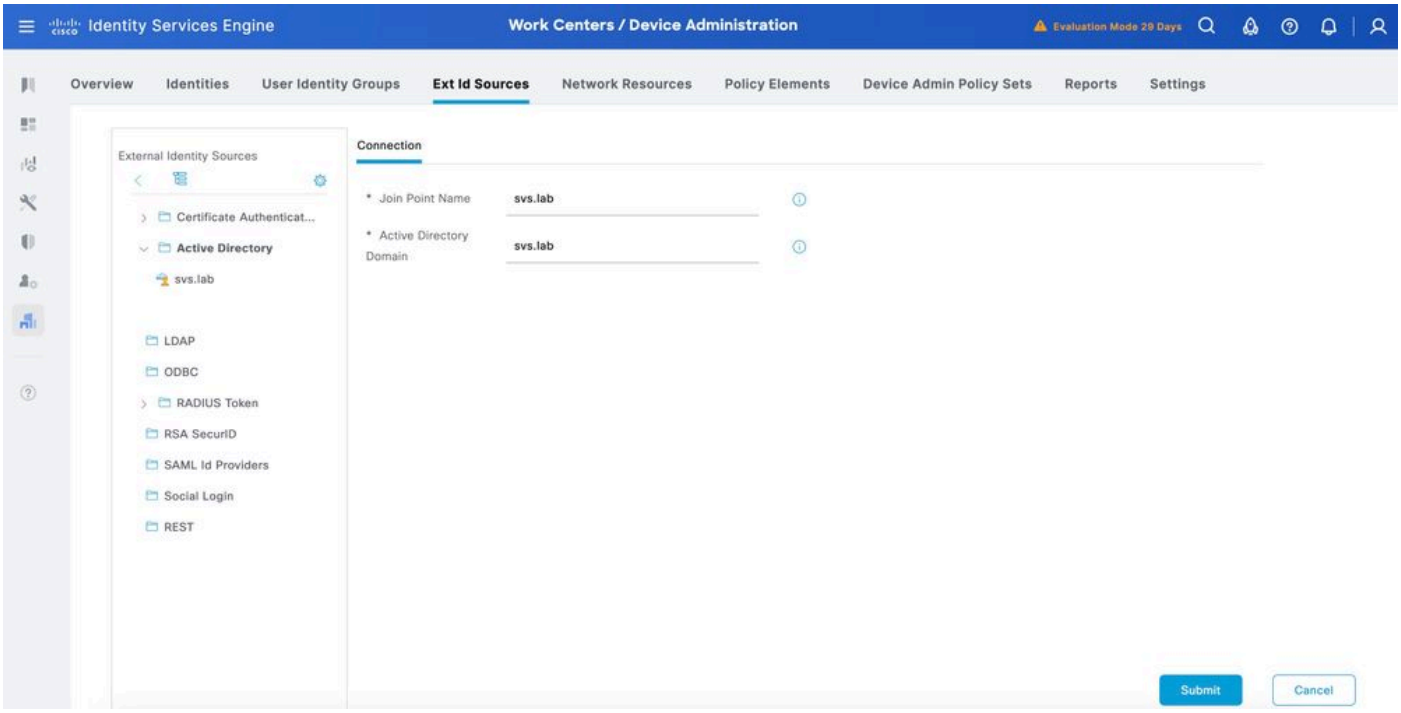
Identiteitswinkels configureren

In dit gedeelte wordt een Identity Store gedefinieerd voor de apparaatbeheerders, die de ISE Internal Users en alle ondersteunde externe identiteitsbronnen kunnen zijn. Hierbij wordt Active Directory (AD) gebruikt, een externe identiteitsbron.

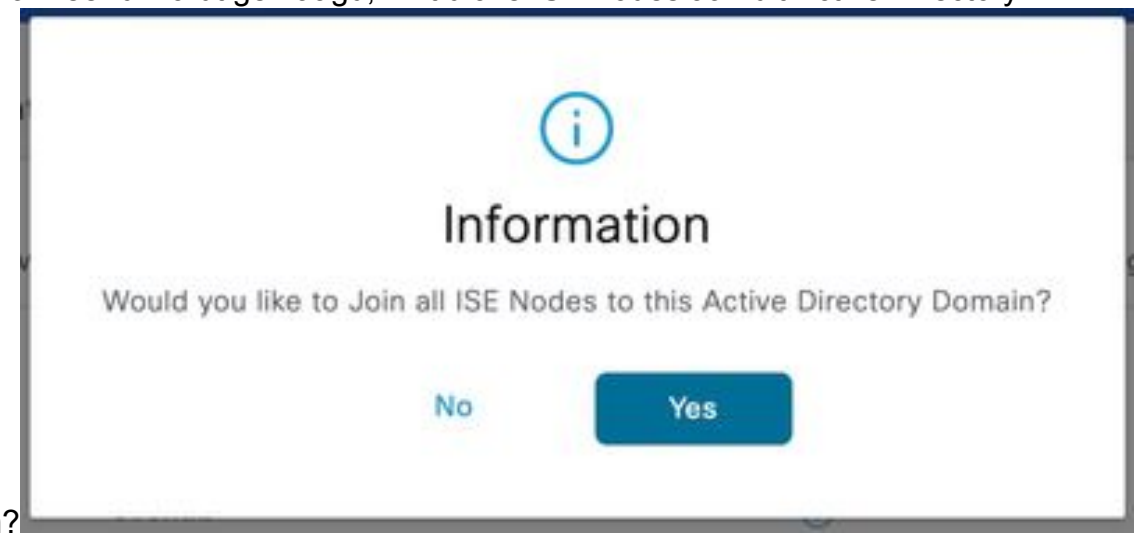
Stap 1. Navigeer naar Beheer > Identiteitsbeheer > Externe identiteitswinkels > Active Directory. Klik op Toevoegen om een nieuw AD-verbindingspunt te definiëren.



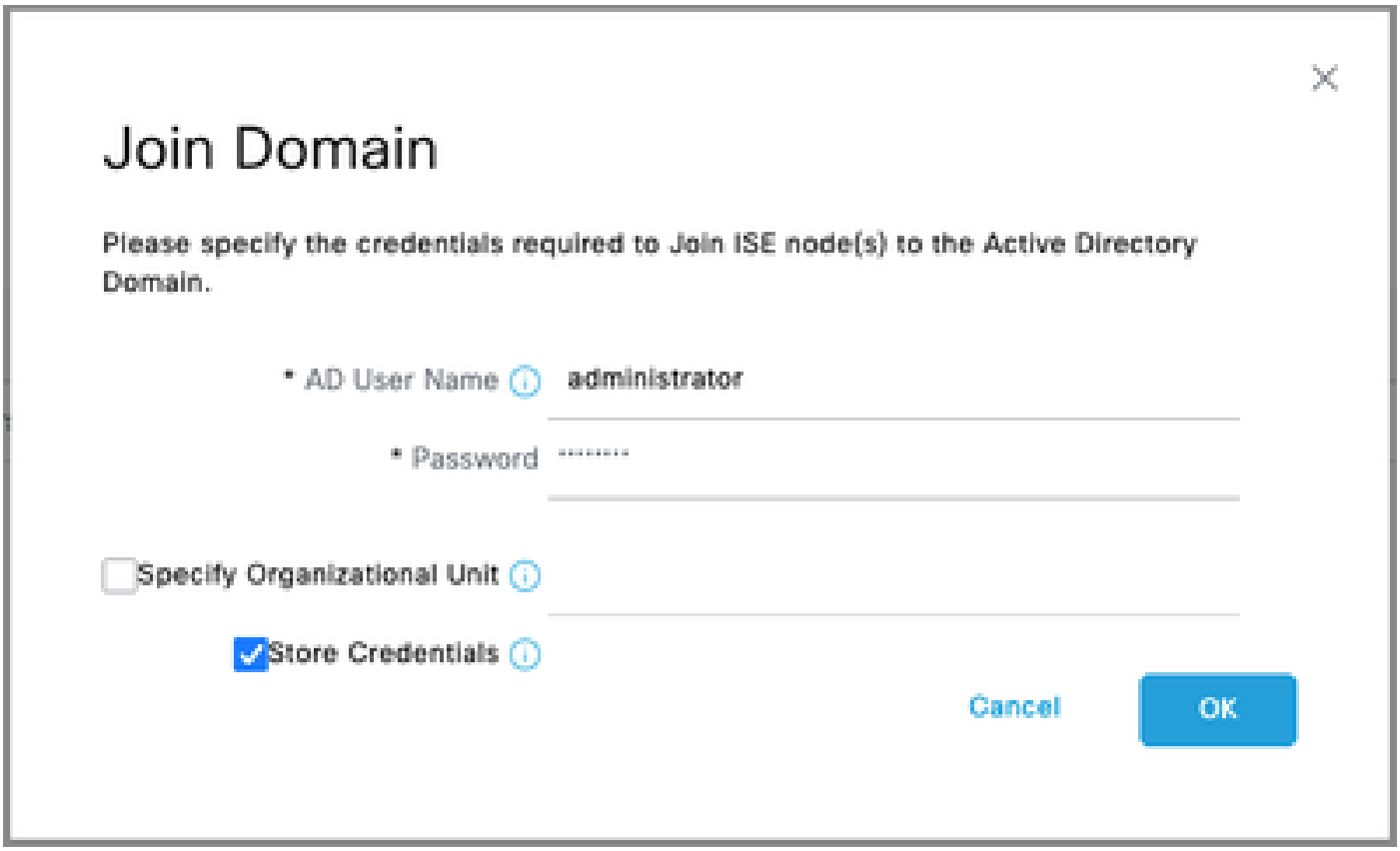
Stap 2. Geef de naam van het aanmeldpunt en de AD-domeinnaam op en klik op Indienen.

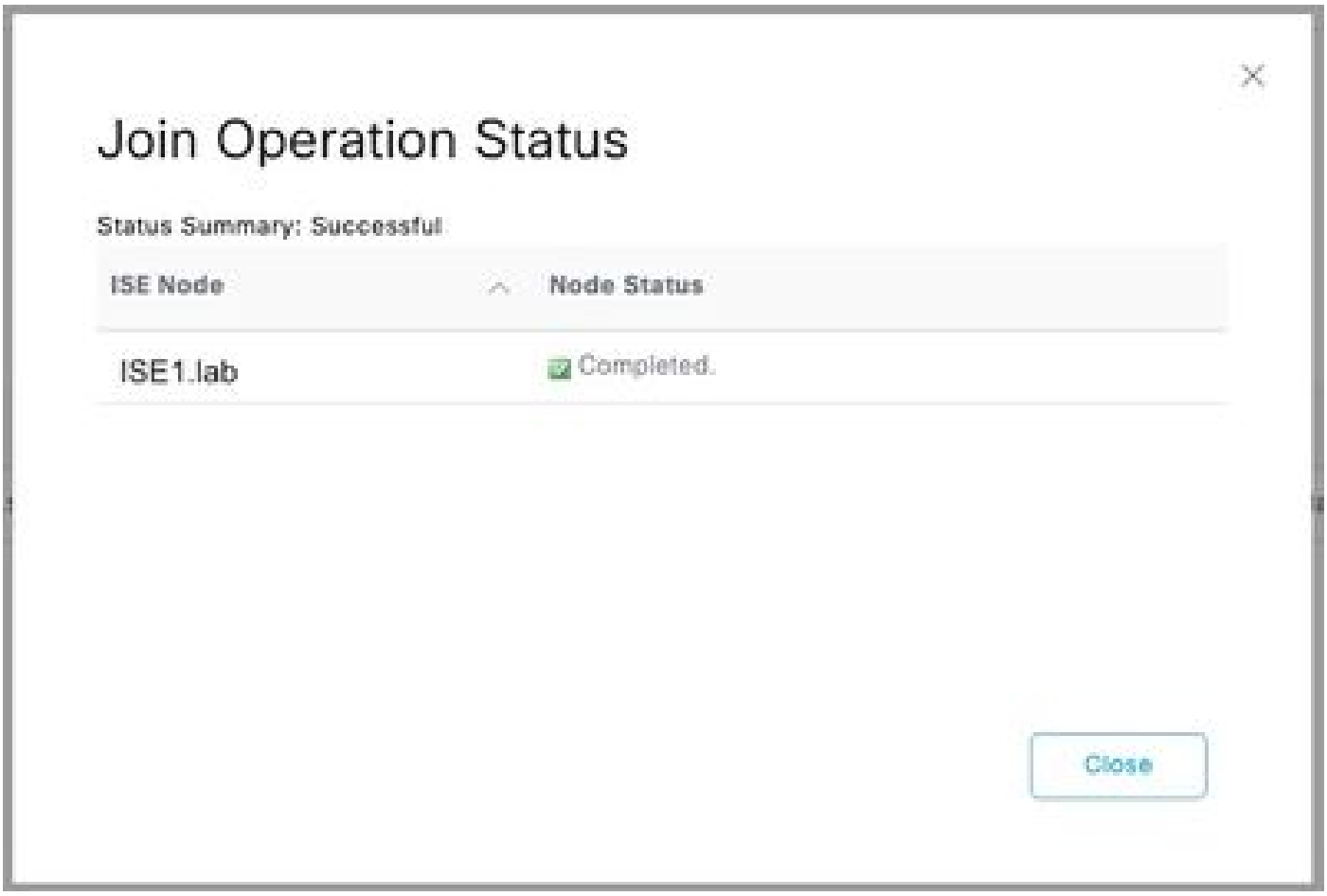


Stap 3.Klik op Ja wanneer u wordt gevraagd, Wilt u alle ISE-nodes aan dit Active Directory-domein toevoegen?

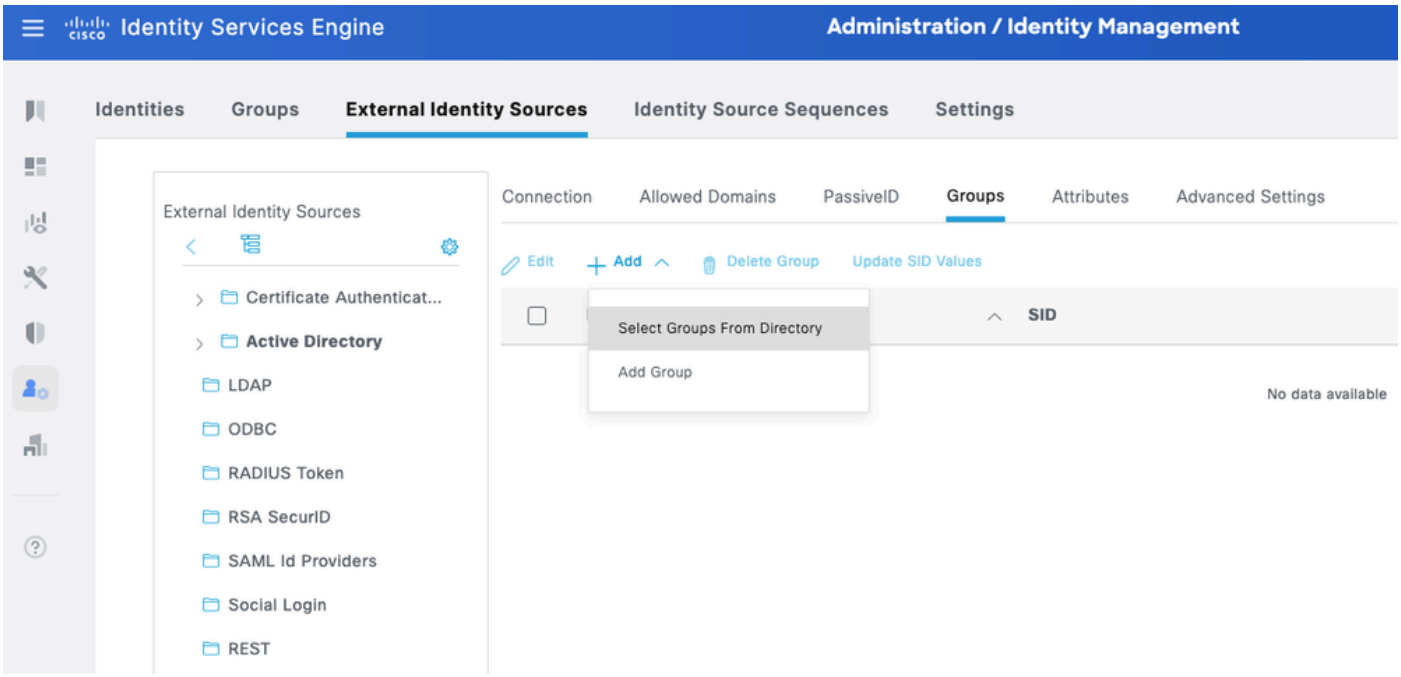


Stap 4.Voer de referenties in met AD join-bevoegdheden en voeg ISE toe aan AD. Controleer de status om te controleren of deze operationeel is.





Stap 5.Navigeer naar het tabblad Groepen en klik op Toevoegen om alle benodigde groepen te krijgen op basis waarvan de gebruikers zijn geautoriseerd voor toegang tot het apparaat. In dit voorbeeld worden de groepen weergegeven die in het machtigingsbeleid worden gebruikt.



Select Directory Groups

This dialog is used to select groups from the Directory.

Domain svs.lab

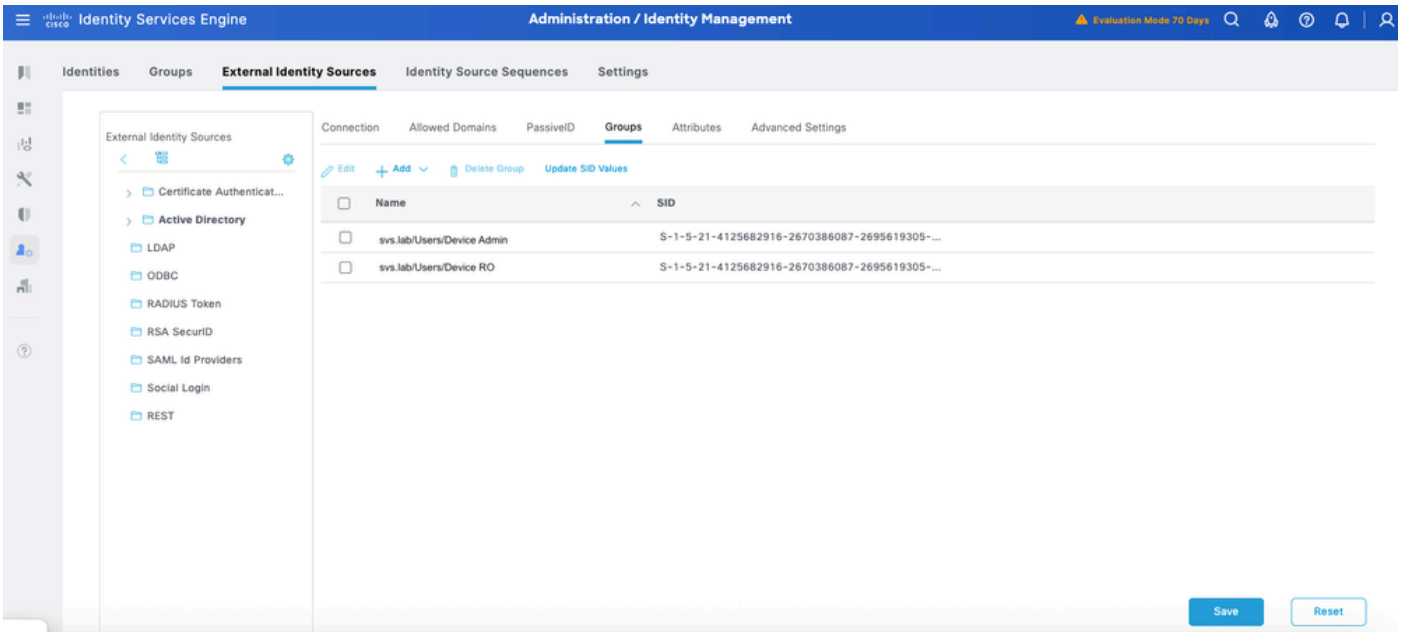
Name Filter Device *

SID Filter *

Type Filter ALL

Retrieve Groups... 2 Groups Retrieved.

Name	Group SID	Group Type
svs.lab/Users/Device Admin	S-1-5-21-4125682916-2670386087-26956193...	GLOBAL
svs.lab/Users/Device RO	S-1-5-21-4125682916-2670386087-26956193...	GLOBAL



TACACS+-profielen configureren

De TACACS+-profielen toewijzen aan gebruikersrollen op de Cisco IOS XR-apparaten. In dit voorbeeld worden deze gedefinieerd:

- Root System Administrator – Dit is de meest geprivilegieerde rol in het apparaat. De gebruiker met de rol van hoofdsysteembeheerder heeft volledige beheerderstoegang tot alle systeemopdrachten en configuratiemogelijkheden.
- Operator – Deze rol is bedoeld voor gebruikers die alleen-lezen toegang tot het systeem nodig hebben voor monitoring en probleemoplossing.

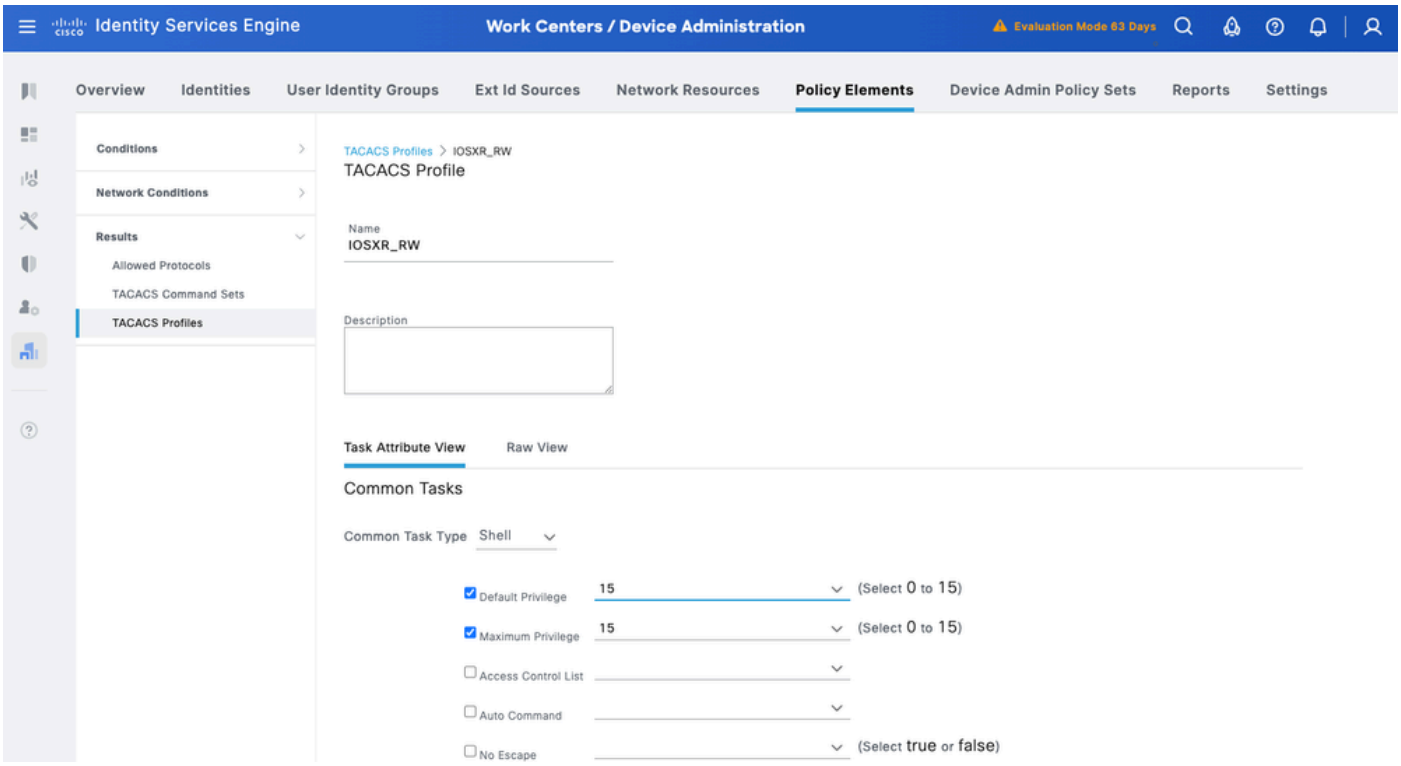
Definieer twee TACACS+-profielen: IOSXR_RW en IOSXR_RO.

IOS XR_RW - Beheerdersprofiel

Stap 1. Navigeer naar Werkcentra > Apparaatbeheer > Beleidselementen > Resultaten > TACACS-profielen. Voeg een nieuw TACACS-profiel toe en noem het IOSXR_RW.

Stap 2. Controleer en stel het standaardvoorrecht en het maximumvoorrecht in op 15.

Stap 3. Bevestig de configuratie en sla op.

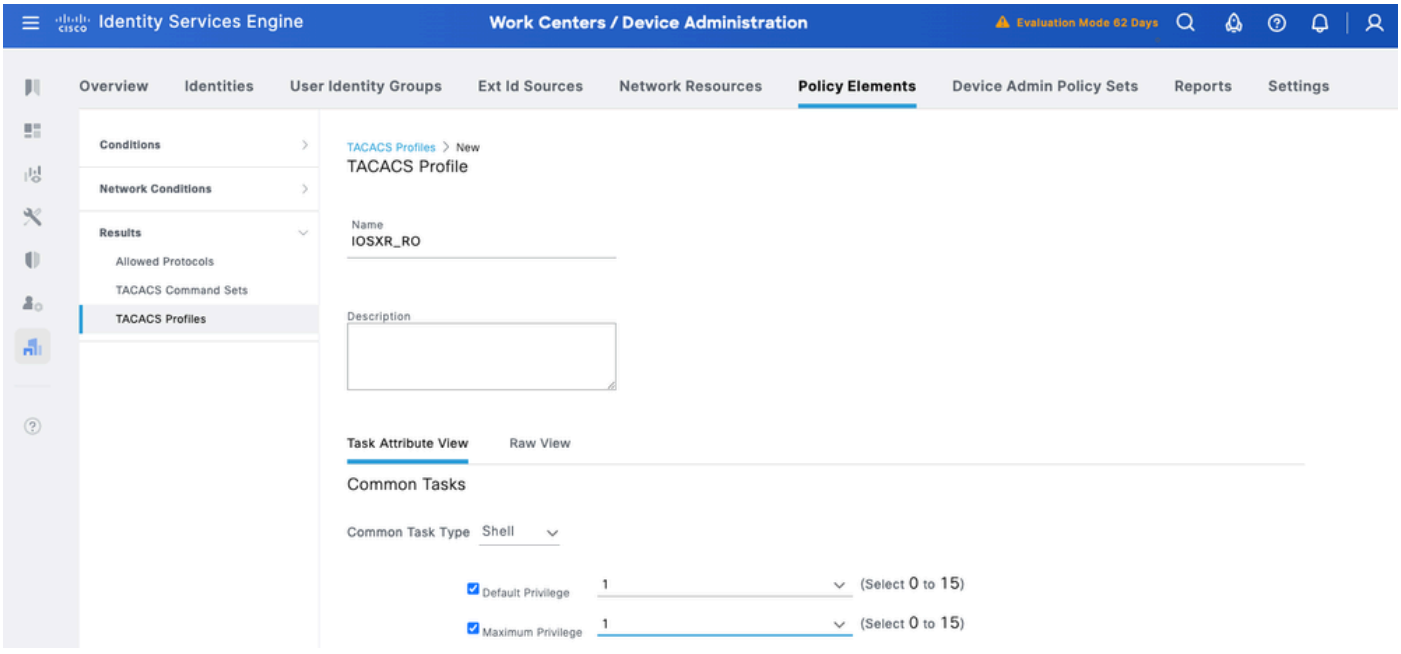


IOS XR_RO - Gebruikersprofiel

Stap 1. Navigeer naar Werkcentra > Apparaatbeheer > Beleidselementen > Resultaten > TACACS-profielen. Voeg een nieuw TACACS-profiel toe en noem het IOSXR_RO.

Stap 2. Controleer en stel het standaardvoorrecht en het maximumvoorrecht in op 1.

Stap 3. Bevestig de configuratie en bewaar.



TACACS+-opdrachtreeksen configureren

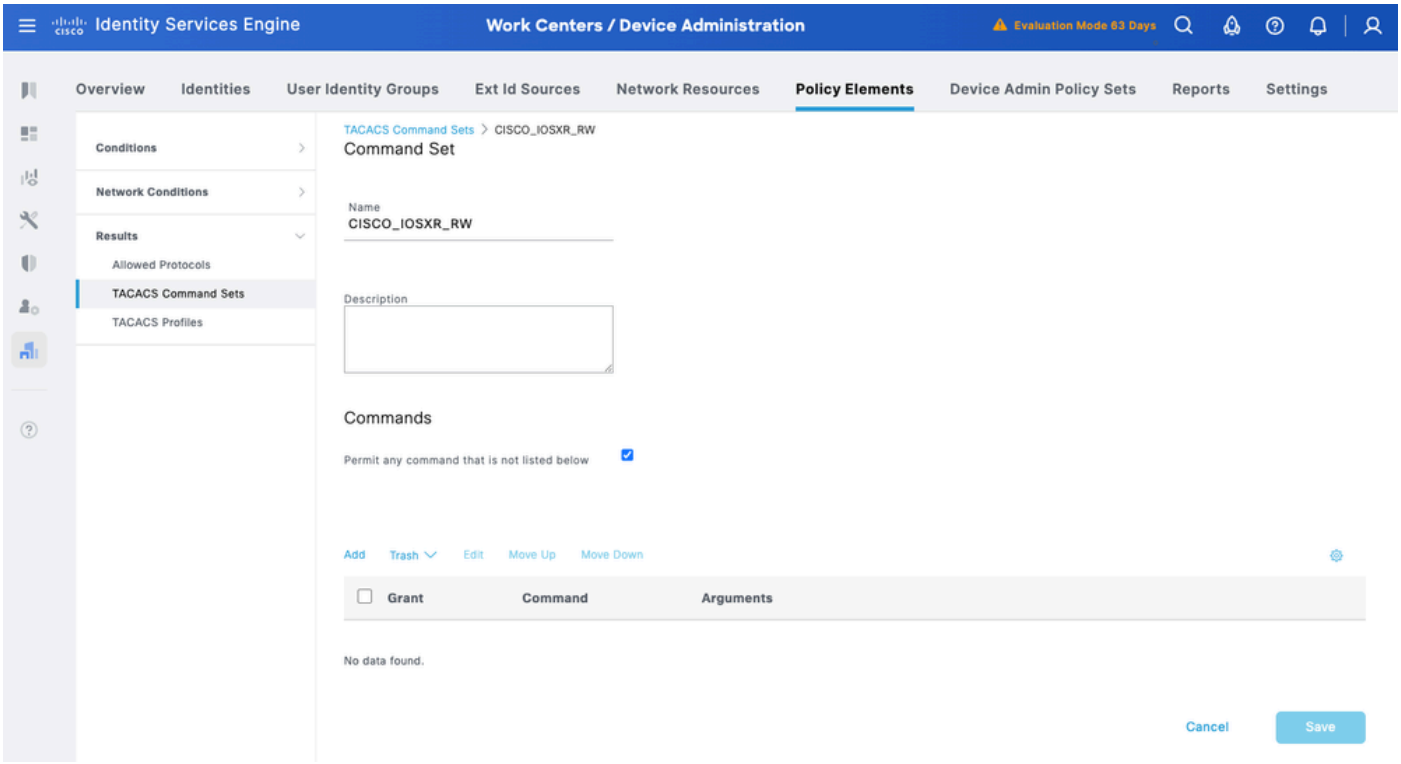
De TACACS+-opdrachtsets definiëren: in dit voorbeeld worden deze gedefinieerd als

CISCO_IOSXR_RW en CISCO_IOSXR_RO.

CISCO IOS XR RW - Opdrachtset voor beheerders

Stap 1. Navigeer naar Werkcentra > Apparaatbeheer > Beleidselementen > Resultaten > TACACS-opdrachtsets. Voeg een nieuwe TACACS-opdrachtset toe en noem deze CISCO_IOSXR_RW.

Stap 2. Schakel het selectievakje Toestaan in voor opdrachten die niet hieronder worden vermeld (hiermee kunt u een opdracht voor de beheerdersrol toestaan) en klik op Opslaan.



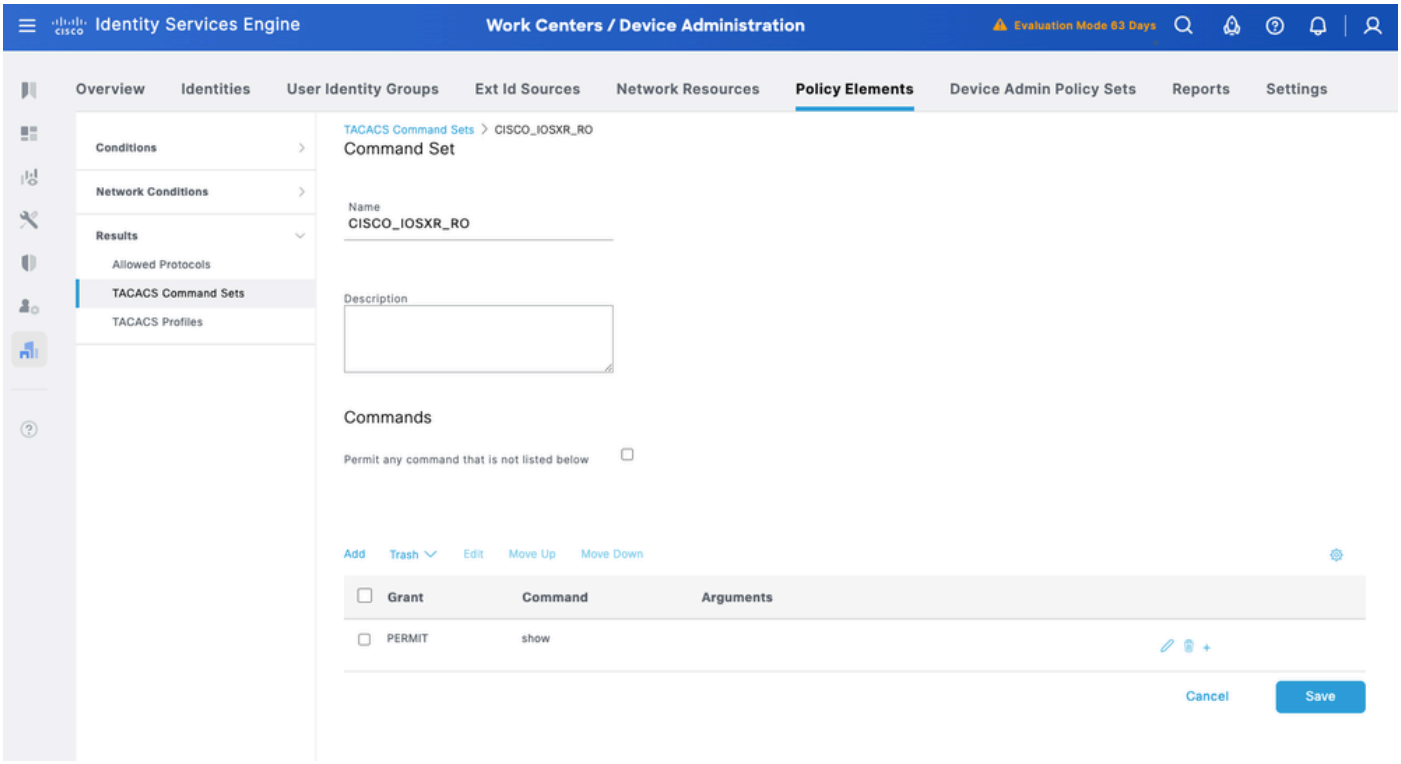
CISCO IOS XR RO - Operator Command Set

Stap 1. Navigeer vanuit ISE UI naar Werkcentra > Apparaatbeheer > Beleidselementen > Resultaten > TACACS-opdrachtsets. Voeg een nieuwe TACACS-opdrachtset toe en noem deze CISCO_IOSXR_RO.

Stap 2. Voeg in het gedeelte Opdrachten een nieuwe opdracht toe.

Stap 3. Selecteer Toestaan in de vervolgkeuzelijst voor de kolom Grant en voer show in op de kolom Command; en klik op de pijl controleren pijl.

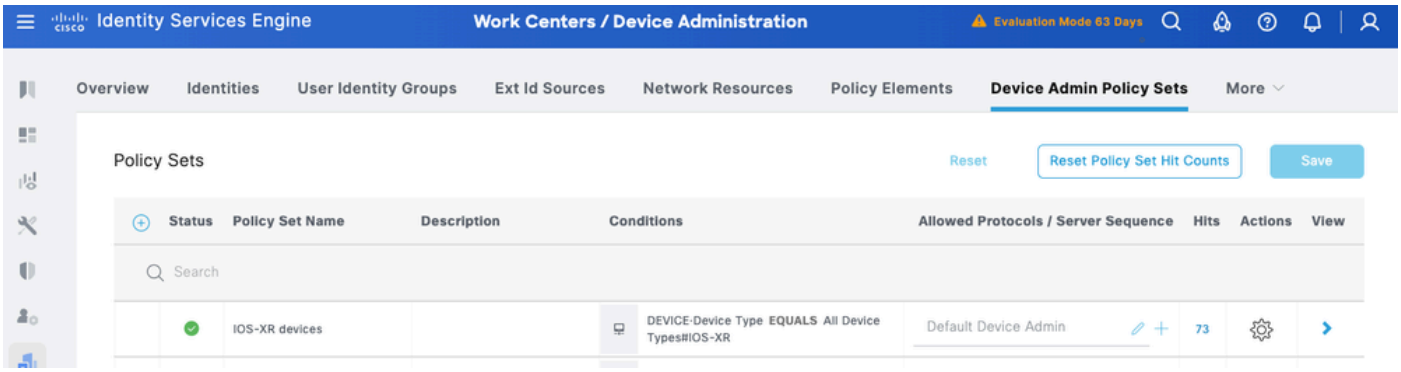
Stap 4. Bevestig de gegevens en klik op Opslaan.



Apparaatbeheerbeleidssets configureren

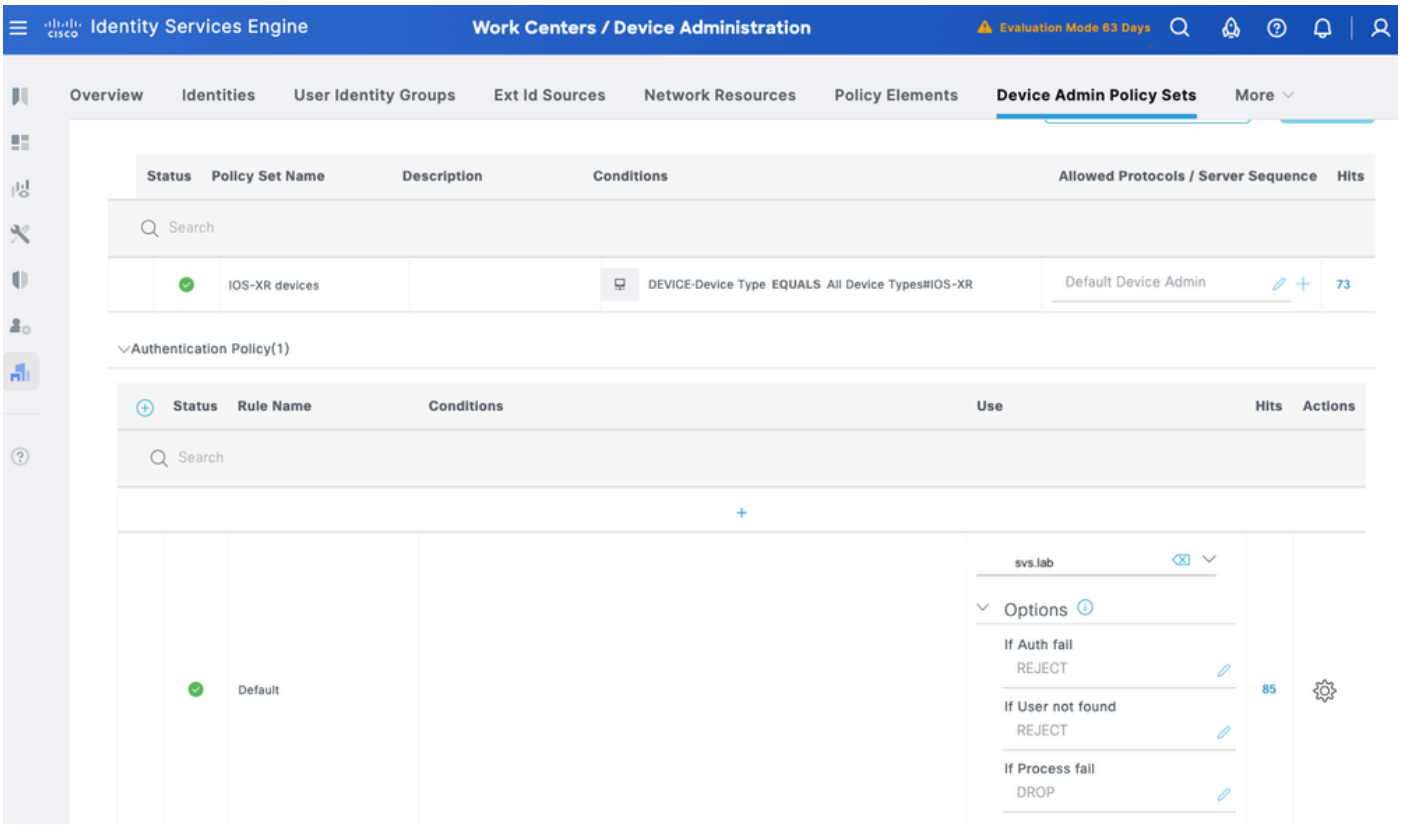
Beleidssets zijn standaard ingeschakeld voor Apparaatbeheer. Beleidsgroepen kunnen beleid verdelen op basis van de apparaattypen om de toepassing van TACACS-profielen te vergemakkelijken.

Stap 1.Navigeer naar werkcentra > Apparaatbeheer > Beleidssets apparaatbeheer. Voeg een nieuwe beleidsset IOS XR-apparaten toe. Geef onder de voorwaarde APPARAAT op: Apparaattype IS GELIJK AAN Alle apparaattypen#IOS XR. Selecteer onder Toegestane protocollen de optie Standaardapparaatbeheer.



Stap 2. Klik op Opslaan en klik op de rechterpijl om deze beleidsset te configureren.

Stap 3. Maak het verificatiebeleid. Voor verificatie gebruikt u de advertentie als ID-winkel. Laat de standaardopties onder Als Auth mislukt, Als gebruiker niet gevonden en Als proces mislukt.

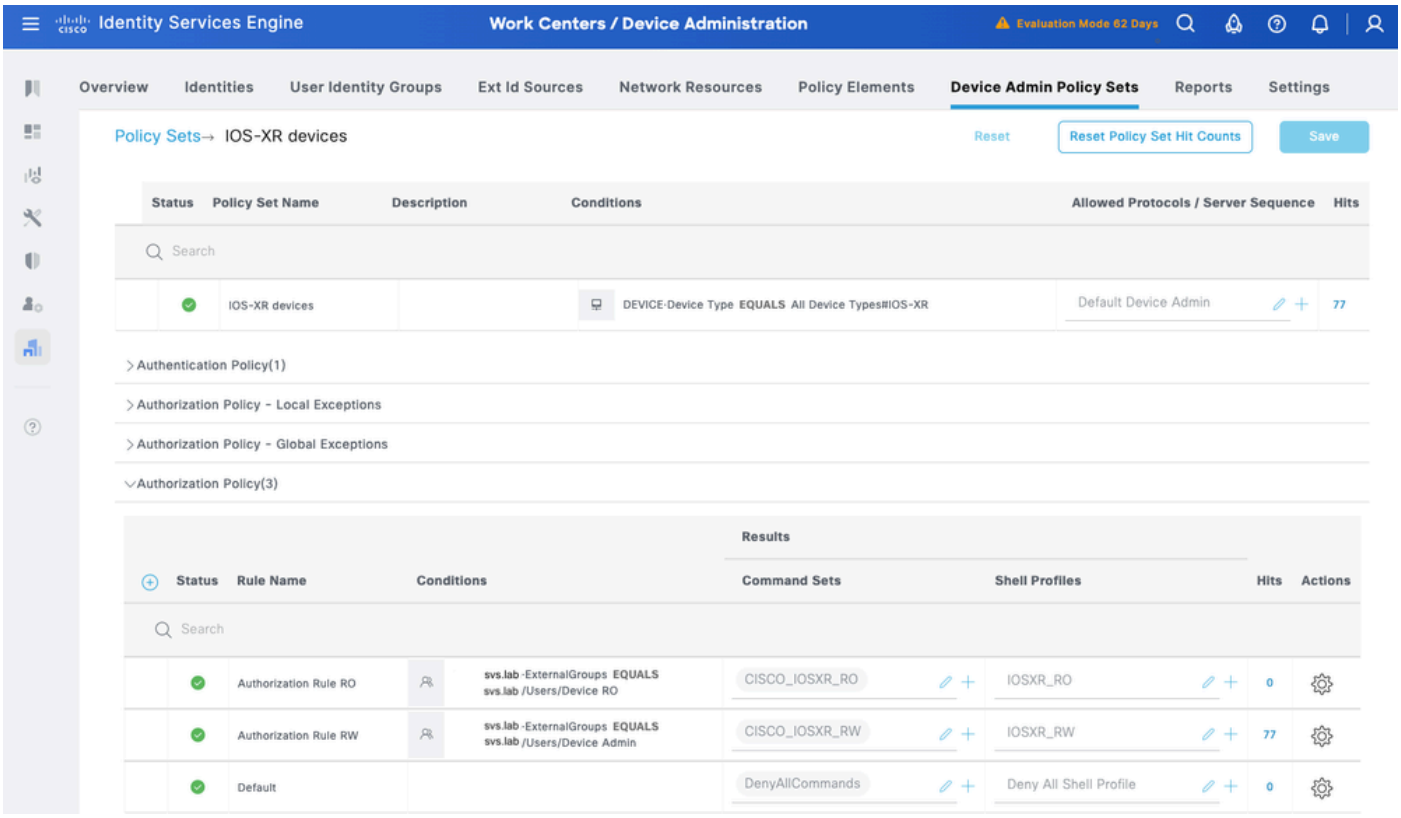


Stap 4. Definieer het autorisatiebeleid.

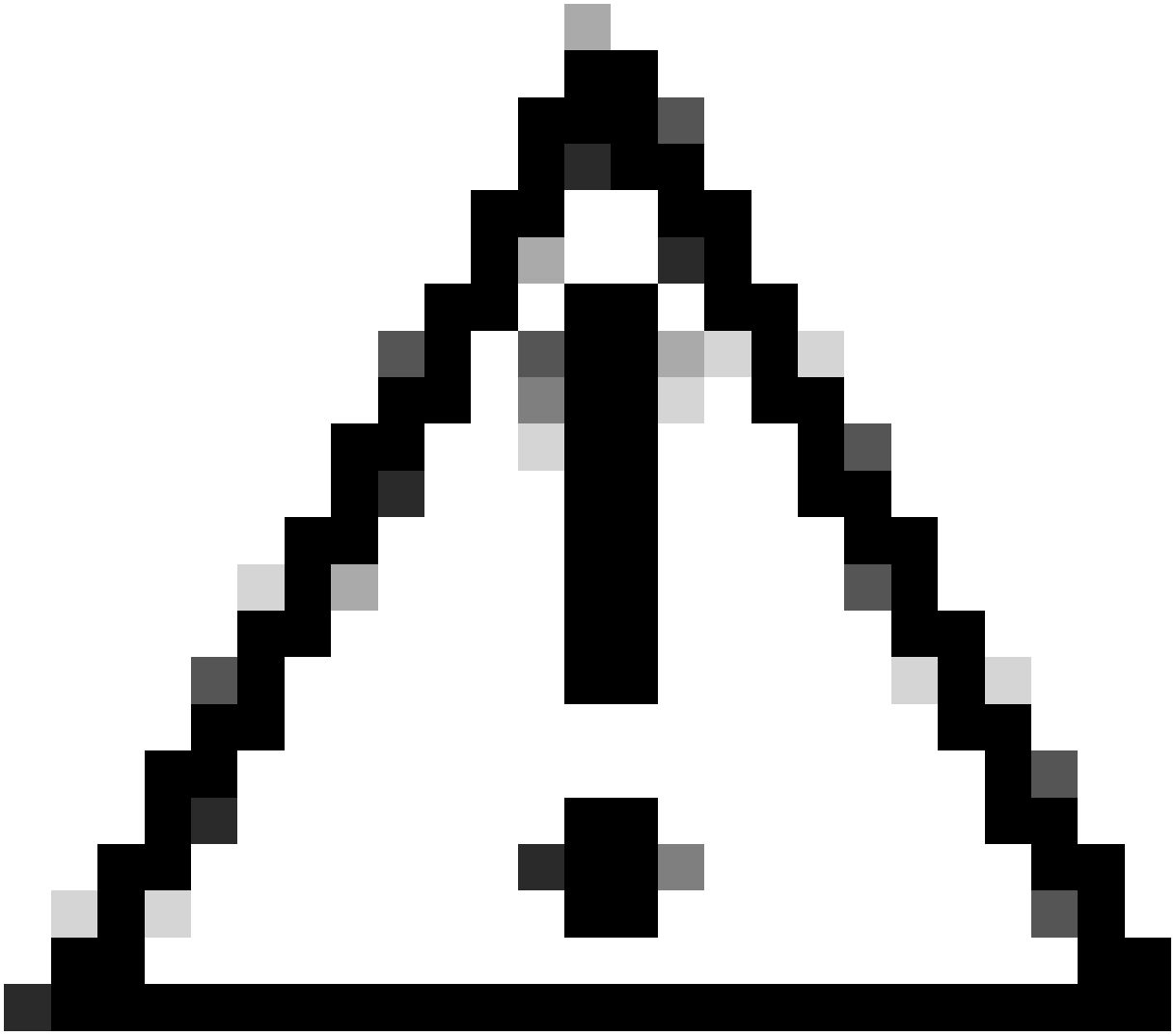
Maak het autorisatiebeleid op basis van gebruikersgroepen in Active Directory (AD).

Voorbeeld:

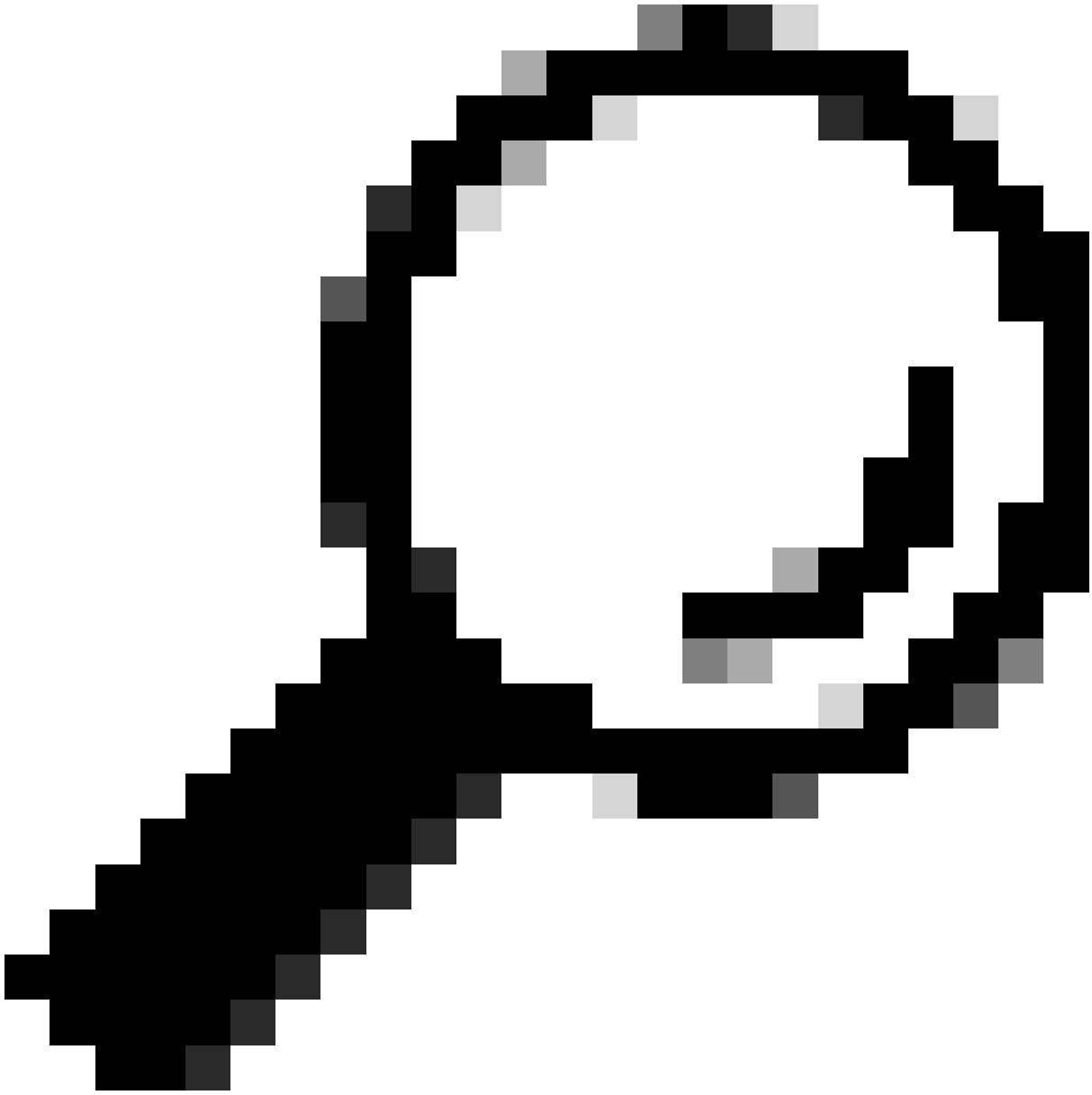
- Gebruikers in de AD-groep Apparaat RO krijgen de CISCO_IOSXR_RO-opdrachtset en het IOSXR_RO-shell-profiel toegewezen.
- Gebruikers in de AD-groep Apparaatbeheer krijgen de CISCO_IOSXR_RW-opdrachtset en het IOSXR_RW-shell-profiel toegewezen.



Deel 2 - Cisco IOS XR configureren voor TACACS+ ten opzichte van TLS 1.3



Let op: Zorg ervoor dat de consoleverbinding bereikbaar is en goed functioneert.



Tip: Het wordt aanbevolen om een tijdelijke gebruiker te configureren en de AAA-verificatie- en autorisatiemethoden te wijzigen om lokale referenties te gebruiken in plaats van TACACS tijdens het aanbrengen van configuratiewijzigingen, om te voorkomen dat het apparaat wordt vergrendeld.

Initiële configuraties

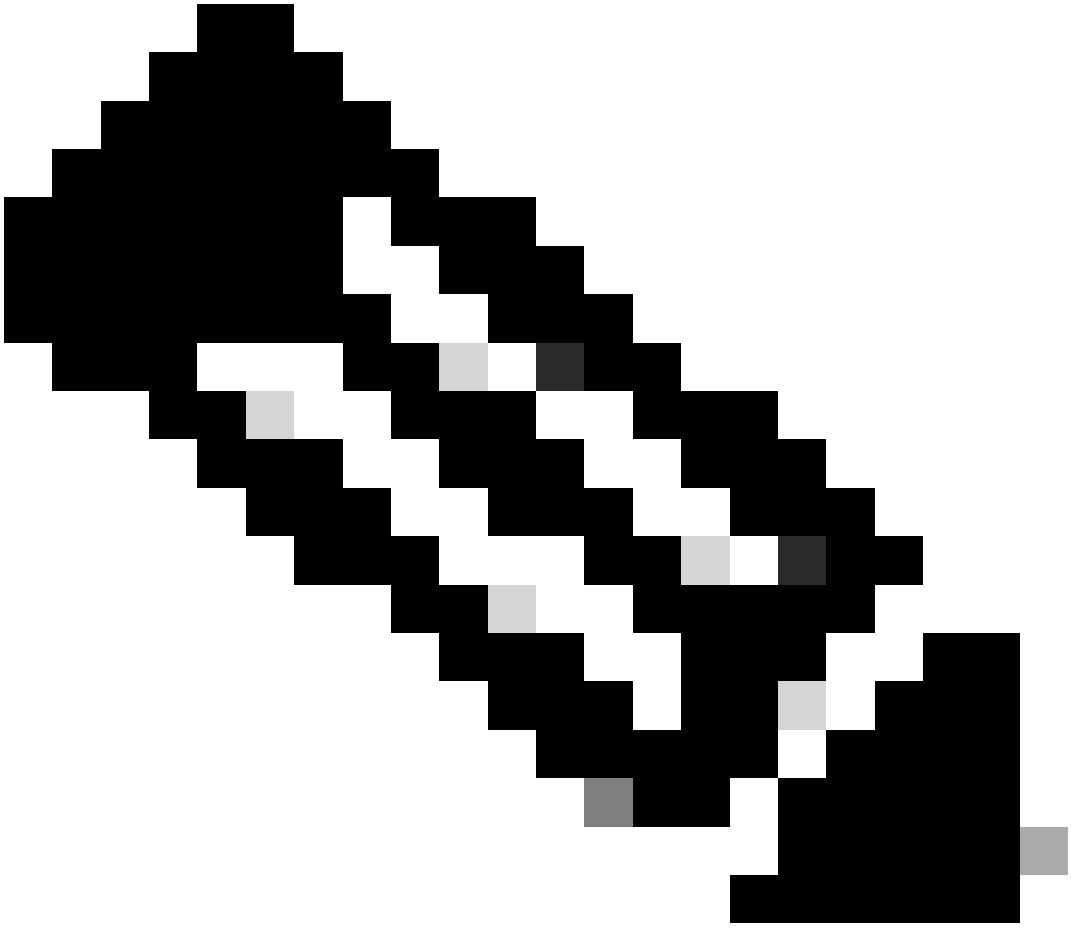
Stap 1. Zorg ervoor dat name-server (DNS) is geconfigureerd en dat de router met succes Frequently Qualified Domain Names (FQDN's) kan oplossen, met name de ISE-server FQDN.

```
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
```

Stap 2. Verwijder alle oude/ongebruikte trustpoints en certificaten. Zorg ervoor dat er geen oude vertrouwenspunten en certificaten aanwezig zijn. Als u oude vermeldingen ziet, verwijdert/verwijdert u deze.

```
show crypto ca trustpoint
show crypto ca certificates

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



Opmerking: U kunt handmatig een nieuw RSA-sleutelpaar maken en dit koppelen onder trustpoint. Als u er geen maakt, wordt het standaardsleutelpaar gebruikt. Het definiëren van een ECC-sleutelpaar onder Trustpoint wordt momenteel niet ondersteund.

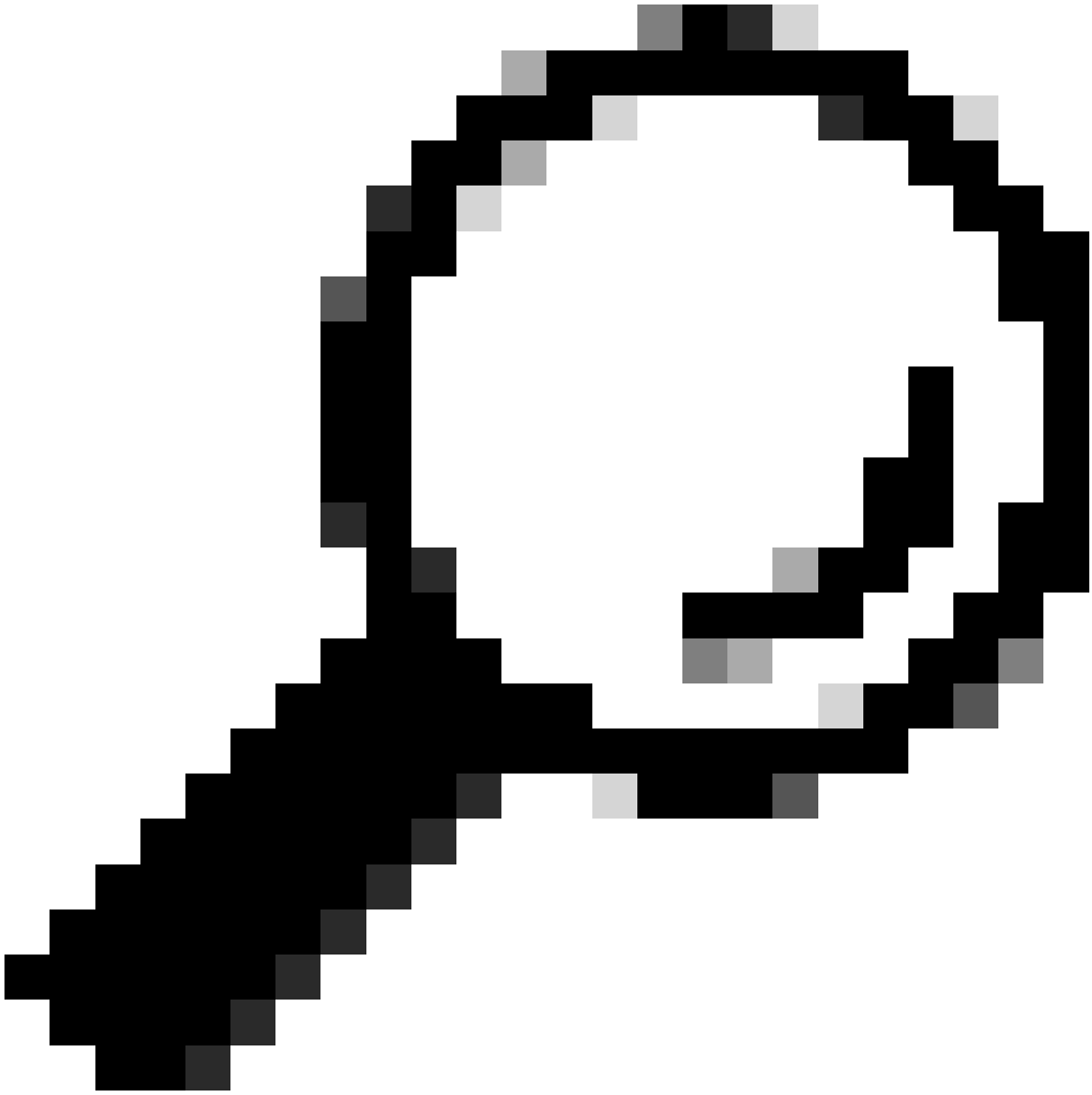
Trustpoint configureren

Stap 1. Keypair-configuratie (optioneel).

```
<#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
```

Stap 2. Creëer TrustPoint.

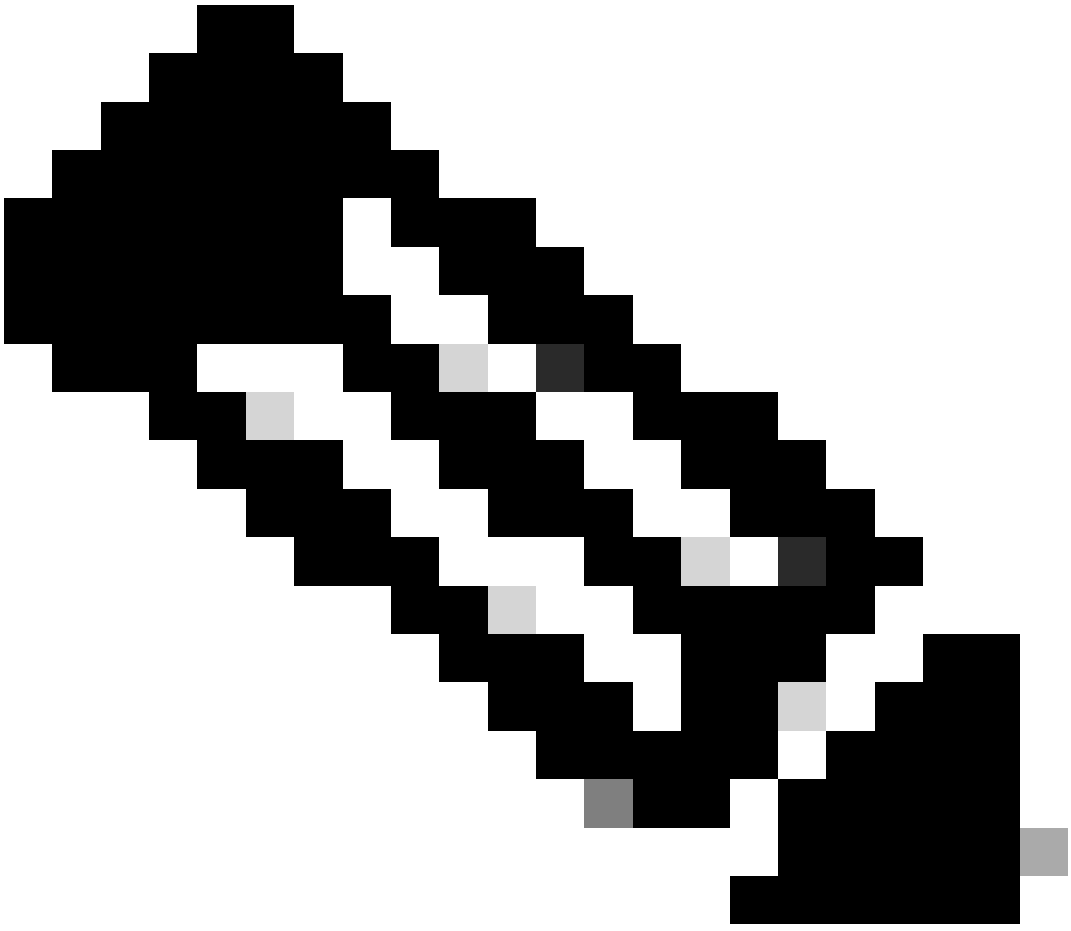


Tip: DNS-configuratie voor alternatieve onderwerpnaam is optioneel (indien ingeschakeld op ISE), maar wordt aanbevolen.

<#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
```



Opmerking: Als u een komma in O of OU moet gebruiken, kunt u een backslash (\) gebruiken vóór de komma. Bijvoorbeeld: O=Cisco Systems\, Inc.

Stap 3. Verifieer Trustpoint door CA-certificaat te installeren.

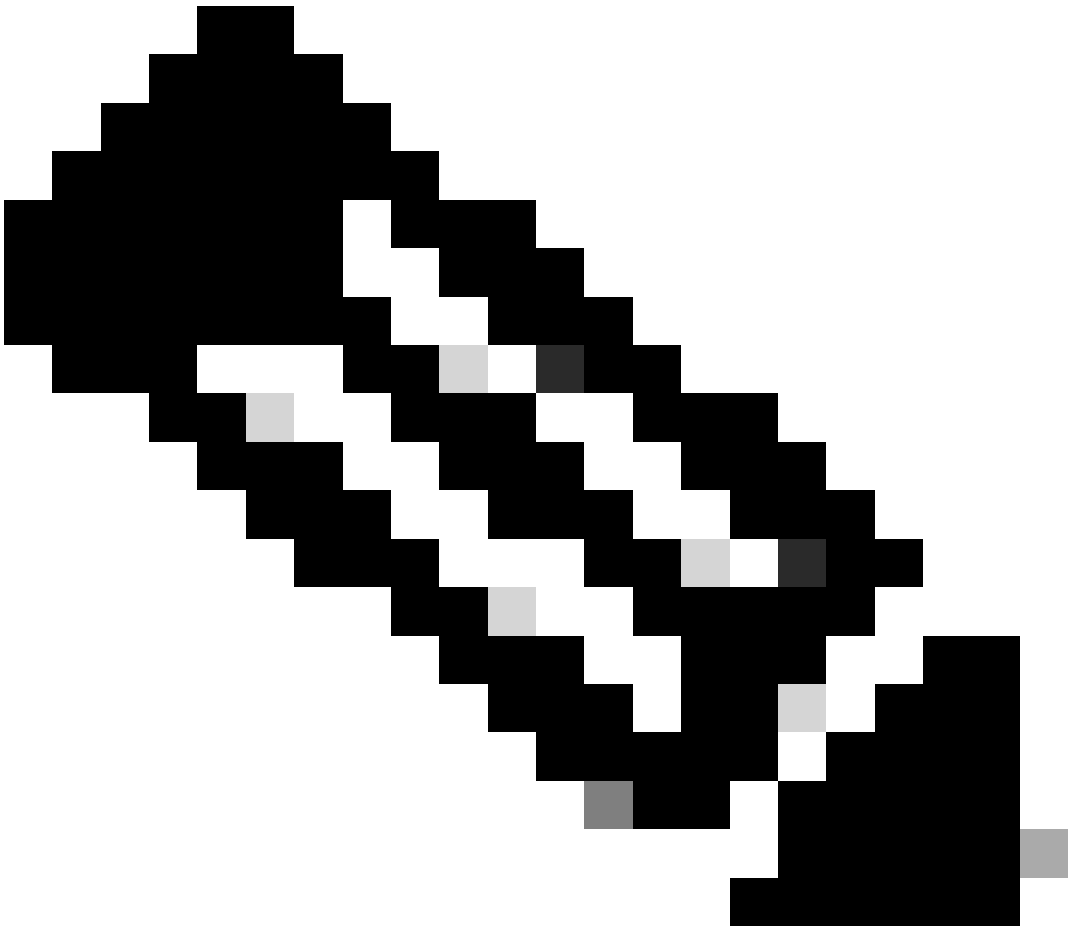
<#root>

```
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
```



Opmerking: als u een ondergeschikt CA-systeem hebt, moet u zowel Root CA- als Sub CA-certificaten importeren. Gebruik dezelfde opdracht met Sub CA bovenaan en Root CA onderaan.

Stap 4. Genereer een aanvraag voor certificaatondertekening (CSR).

<#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

Stap 5. CA-ondertekend certificaat importeren.

<#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
7DFVxBt6PwIDAQABo4GAMH4wHgYJYIZIAYb4QgENBBEWD3hjYSBjZXJOaWZpY2F0
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
```

Controleer of het identiteitscertificaat van de router is geregistreerd.

<#root>

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

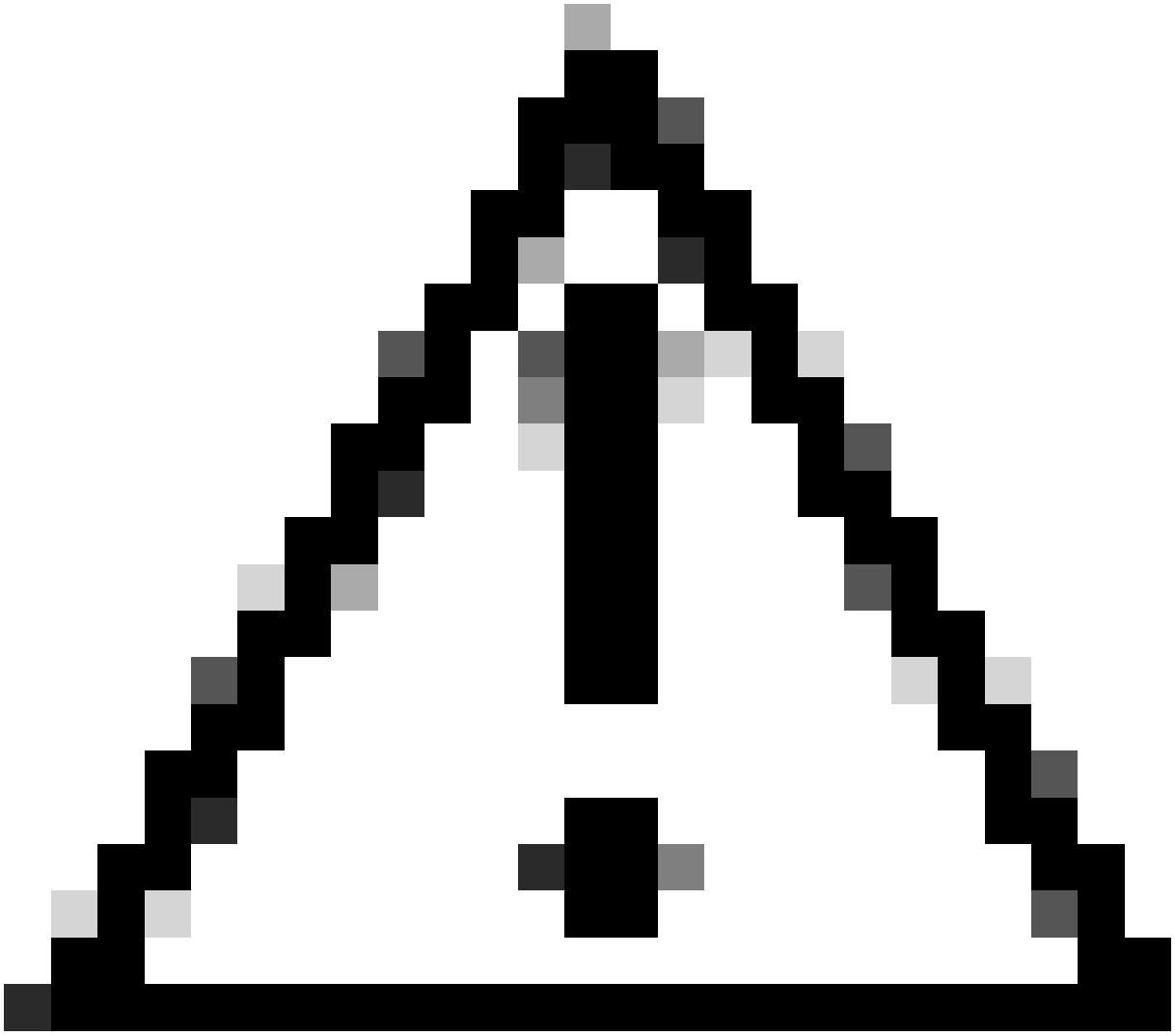
show crypto ca trustpoint svs detail

```
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
```

TACACS & AAA configureren met TLS



Let op: voer de configuratiewijzigingen uit via console met lokale referenties.

Stap 1. De TACACS+-server configureren.

```
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
```

Stap 2. Configureer de AAA-groep.

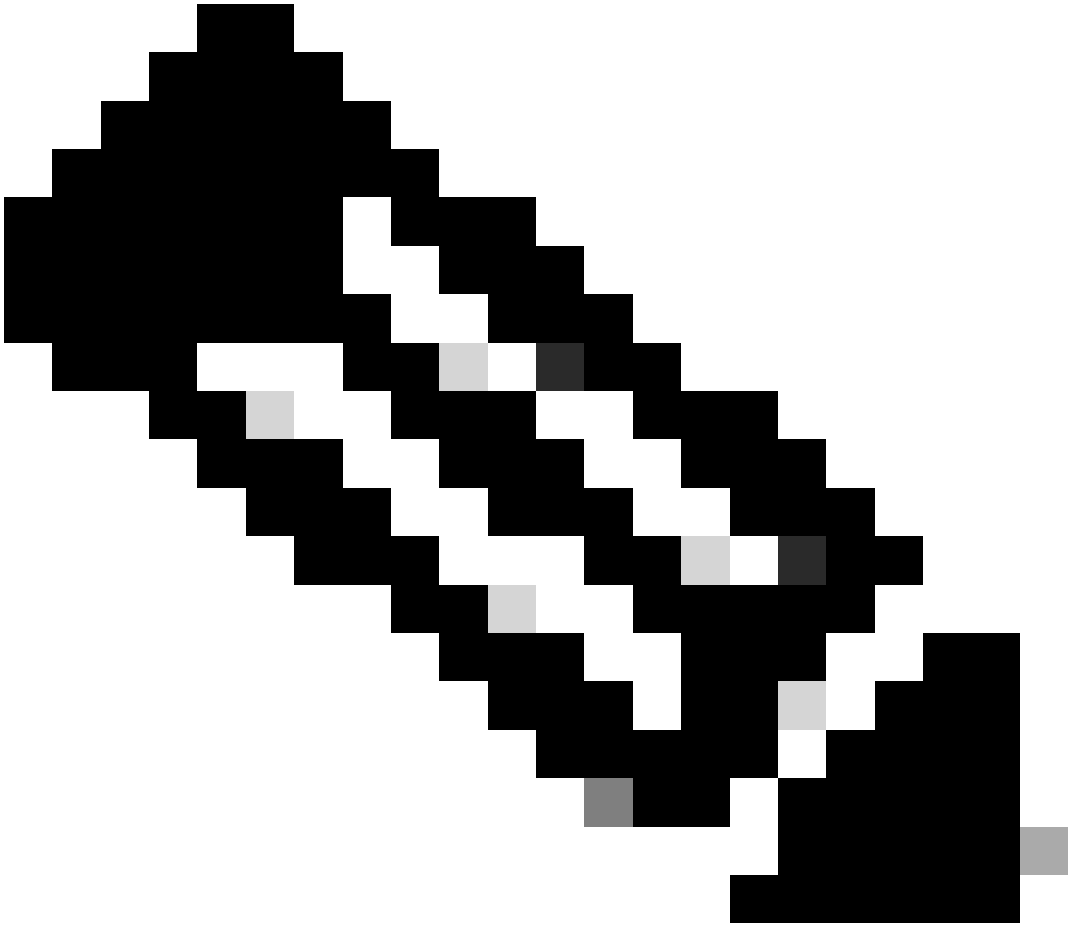
```
aaa group server tacacs+ tac_tls_sc
```

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

Stap 2. Configureer AAA.

```
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
```

Certificaatvernieuwing



Opmerking: Vertrouwenspunt hoeft niet te worden verwijderd uit de TACACS+-configuratie tijdens de verlenging.

Stap 1. Controleer de huidige geldigheidsdatums van het certificaat.

```
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
```

Stap 2. Bestaande Trustpoint-certificaat verwijderen.

```
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#
```

Stap 3. Vertrouwenspunt opnieuw verifiëren en inschrijven zoals beschreven in de stappen onder Configuratie van Trustpoint.

Stap 4. Controleer of de geldigheidsdatums van het certificaat zijn bijgewerkt.

```
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=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 : 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
```

Verificatie

De configuratie verifiëren.

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

Foutopsporing voor TACACS+

```
debug tacacs tls
```

Foutopsporing TLS

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

Test de externe gebruiker voordat u AAA-verificatie configureert.

<#root>

test aaa group tacacs2

```
user has been authenticated
```

Probleemoplossing

De certificaten wissen (hiermee worden alle certificaten verwijderd die aan een vertrouwenspunt zijn gekoppeld).

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

Herstart TACACS-proces (indien nodig)

```
process restart tacacsd
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.