TACACS+ configureren via TLS 1.3 op een IOS XE-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® XE-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 XE-netwerkapparaten.
· Deel 1 – Configureer ISE voor Apparaatbeheer
· Deel 2 – Cisco IOS XE 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 IOS XE Software, versie 17.15+

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.

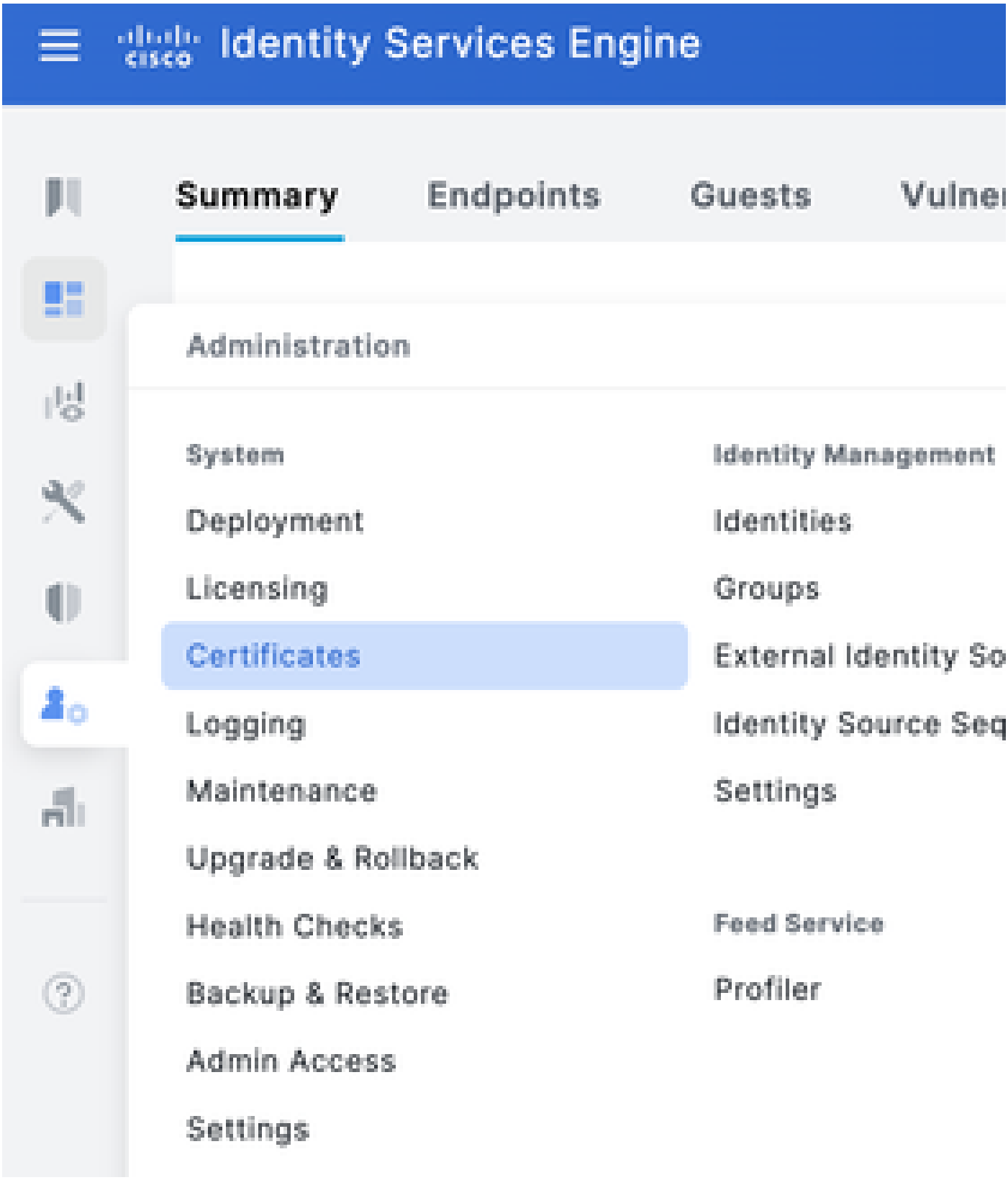
Deel 1 - Configureer ISE voor apparaatbeheer

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).

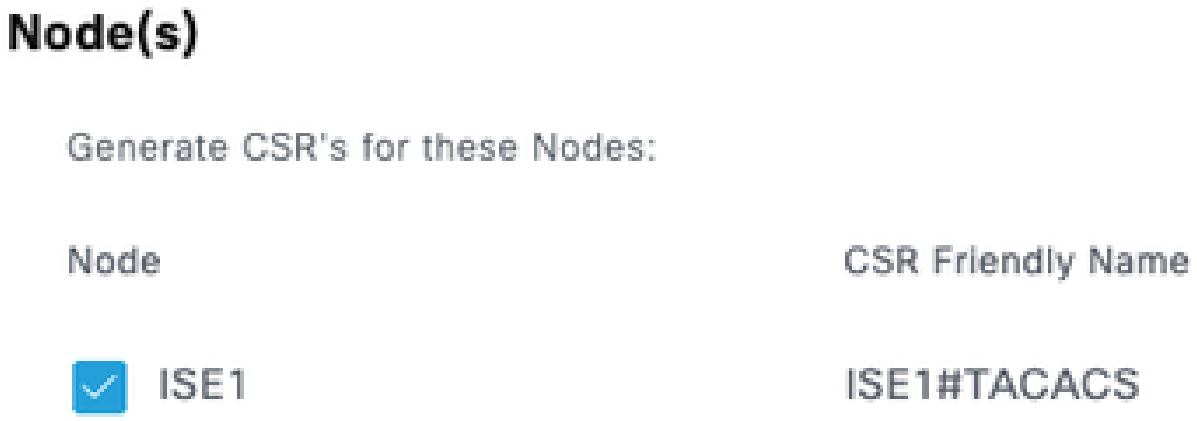
Stap 2.Navigeer naar Beheer **>** Systeem **>** Certificaten.



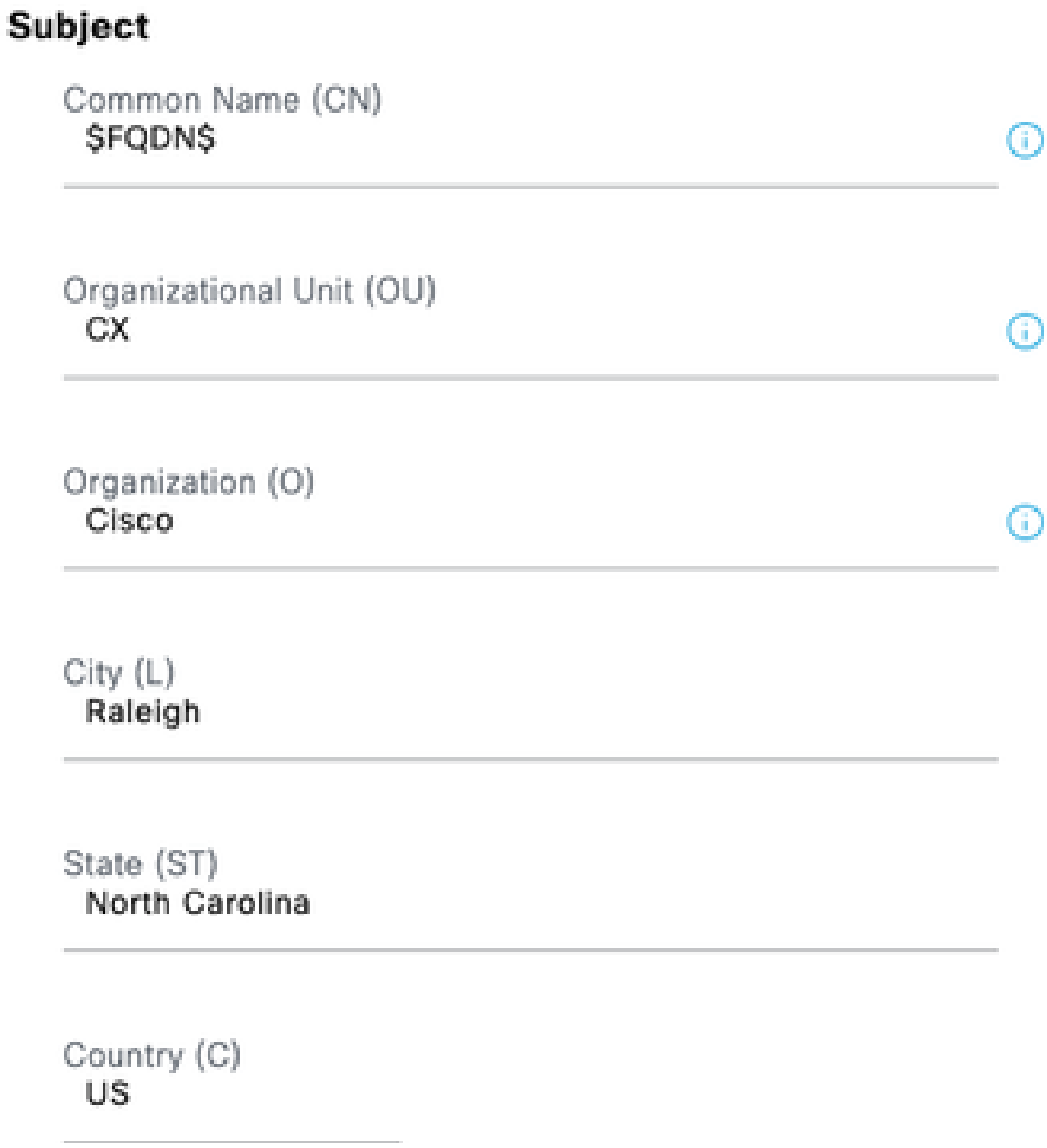
Stap 3. Klik onder Certificaatondertekeningsverzoeken op Certificaatondertekeningsverzoek genereren.

Stap 4. Selecteer TACACS in gebruik.

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

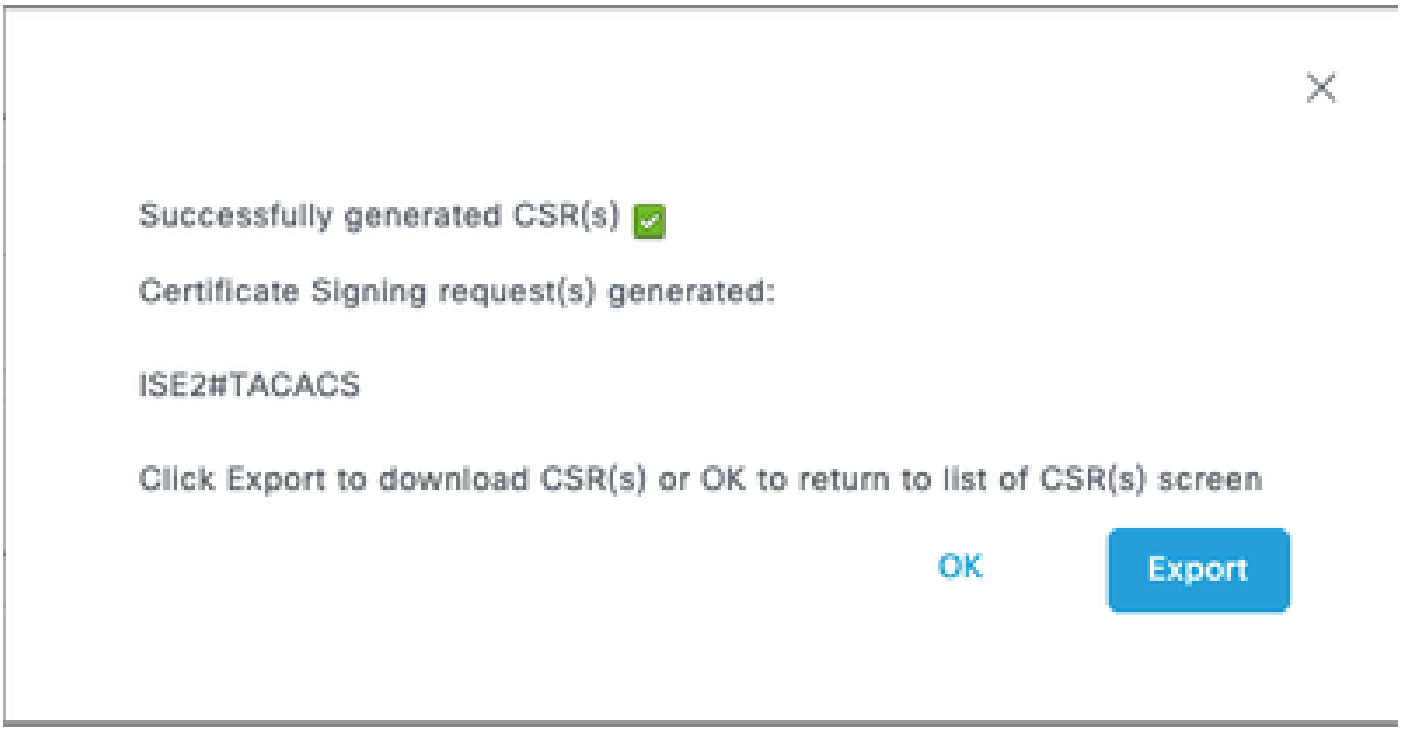


Stap 6. Vul de onderwerpvelden in met de juiste informatie.



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

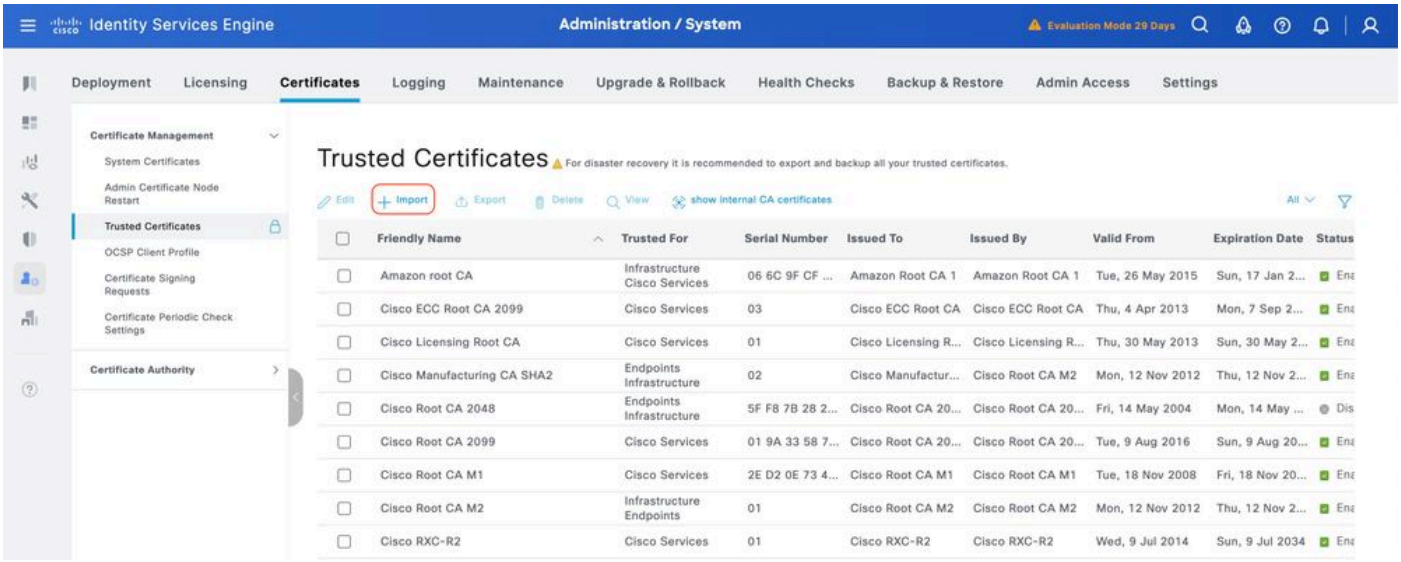
Stap 8. Klik op Genereren en vervolgens op Exporteren.



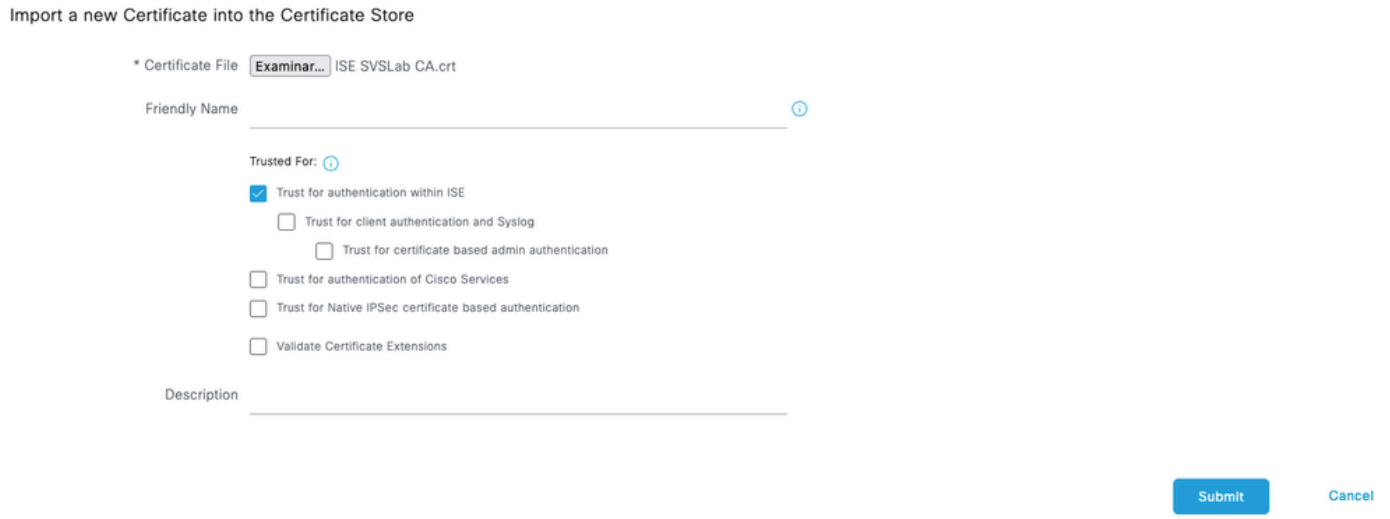
Nu kunt u het certificaat (CRT) laten ondertekenen door uw Certificate Authority (CA).

Root CA-certificaat uploaden voor TACACS+-serververificatie

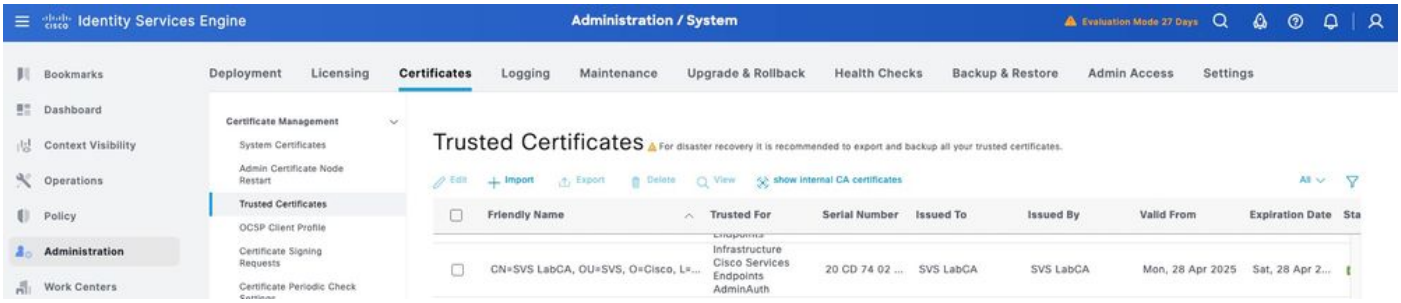
Stap 1. Ga naar Beheer > Systeem > Certificaten. Klik onder Vertrouwde certificaten op Importeren.



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



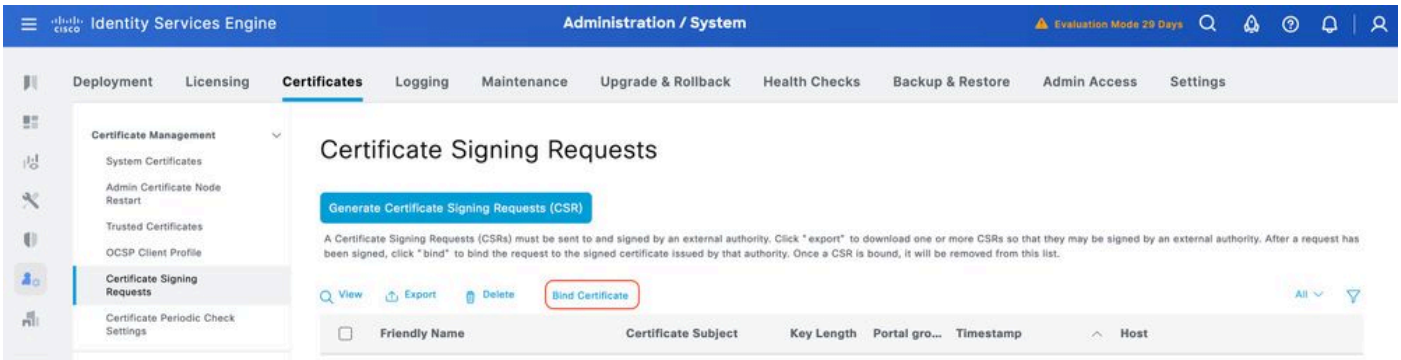
Stap 3. Klik op Indienen. Het certificaat moet nu worden weergegeven onder Vertrouwde certificaten.



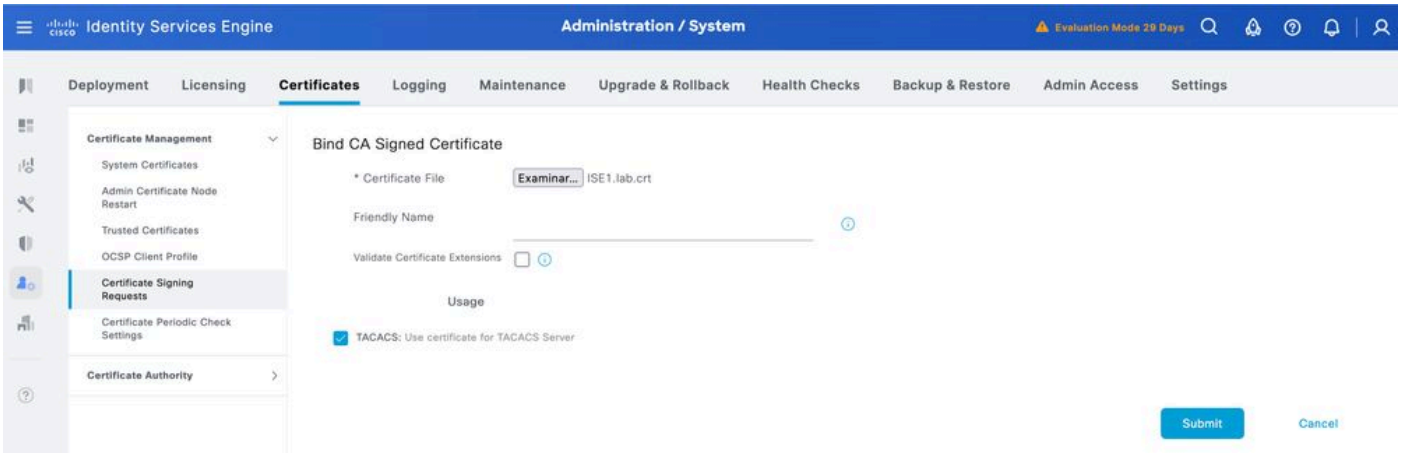
Het ondertekende certificaatondertekeningsverzoek (CSR) binden aan ISE

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 TACACS-CSR die in de vorige stap is gegenereerd en klik op Certificaat binden.

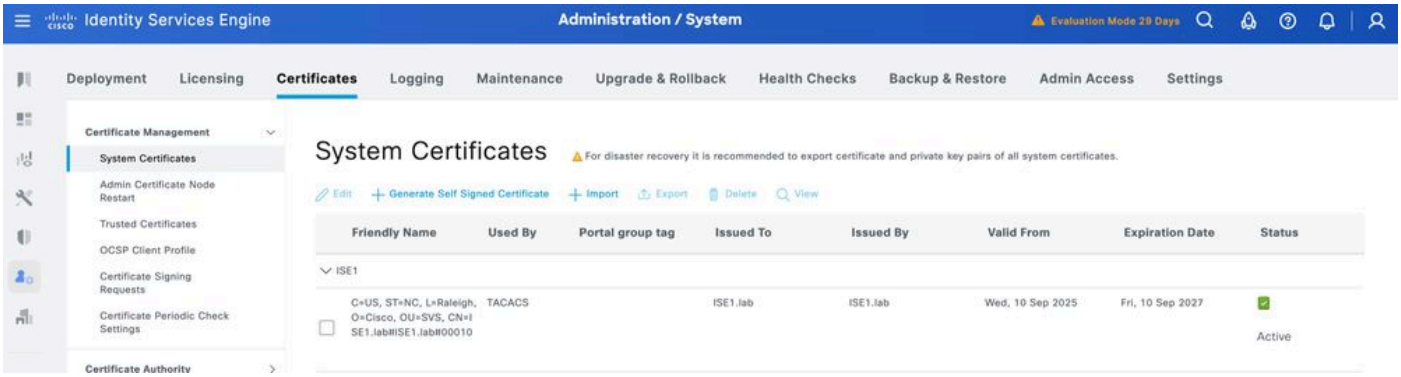


Stap 2.Selecteer het ondertekende certificaat en zorg ervoor dat het selectievakje TACACS onder Gebruik geselecteerd blijft.



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.

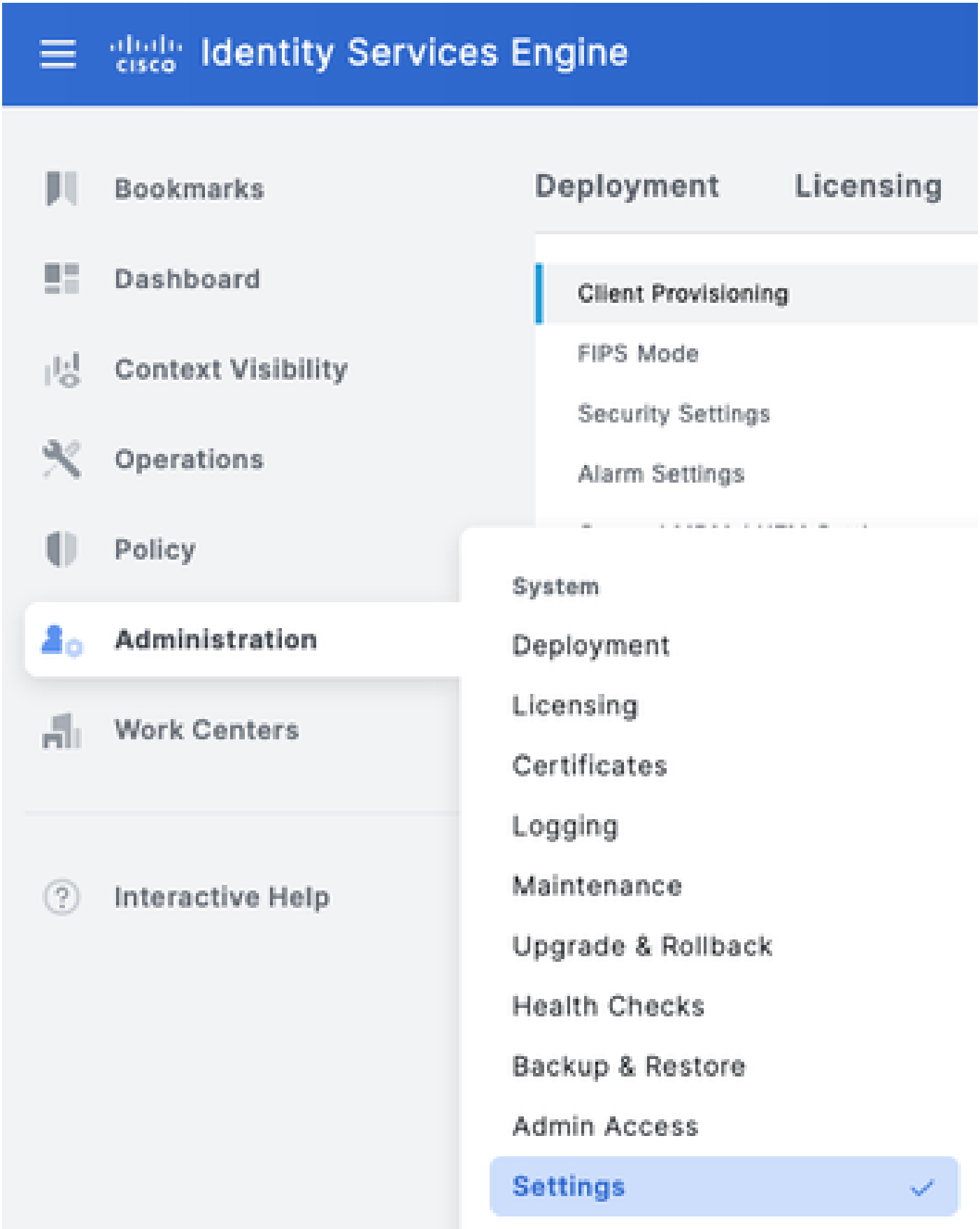
Het certificaat moet nu correct worden geïnstalleerd. U kunt dit controleren onder Systeemcertificaten.



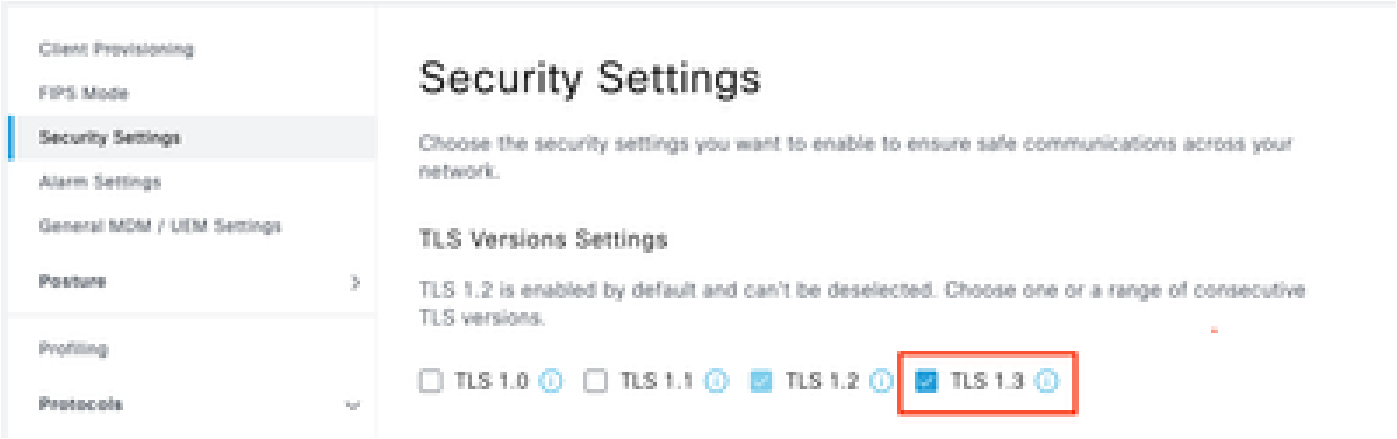
TLS 1.3 inschakelen

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 aanvinkvakje naast TLS1.3 onder Versie-instellingen en klik vervolgens op Opslaan.

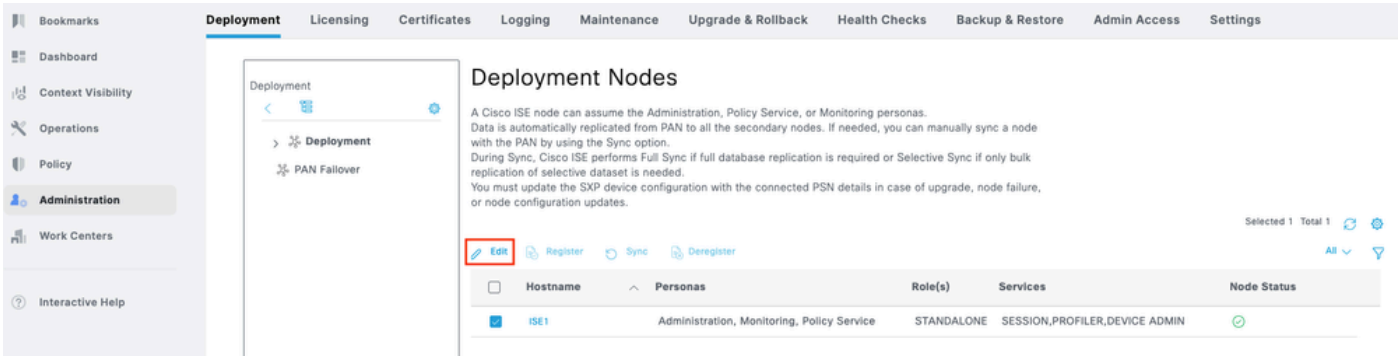


Waarschuwing: wanneer u de TLS-versie wijzigt, wordt de Cisco ISE-toepassingsserver opnieuw gestart op alle Cisco ISE-implementatiemachines.

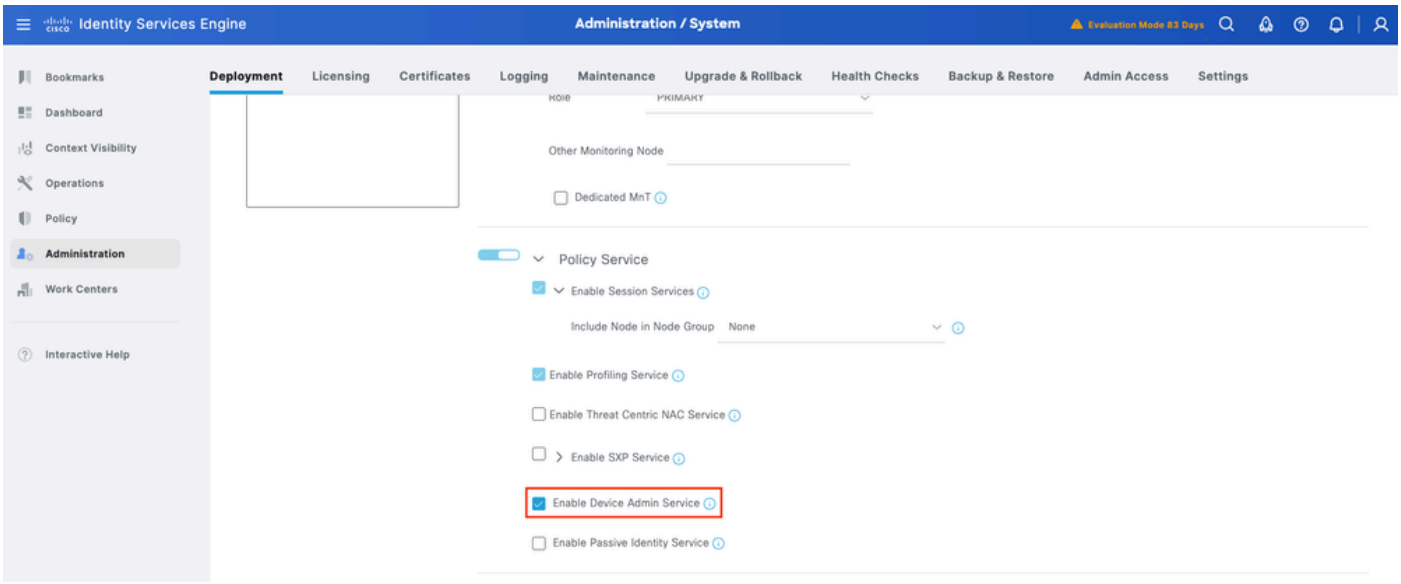
Apparaatbeheer inschakelen op ISE

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

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



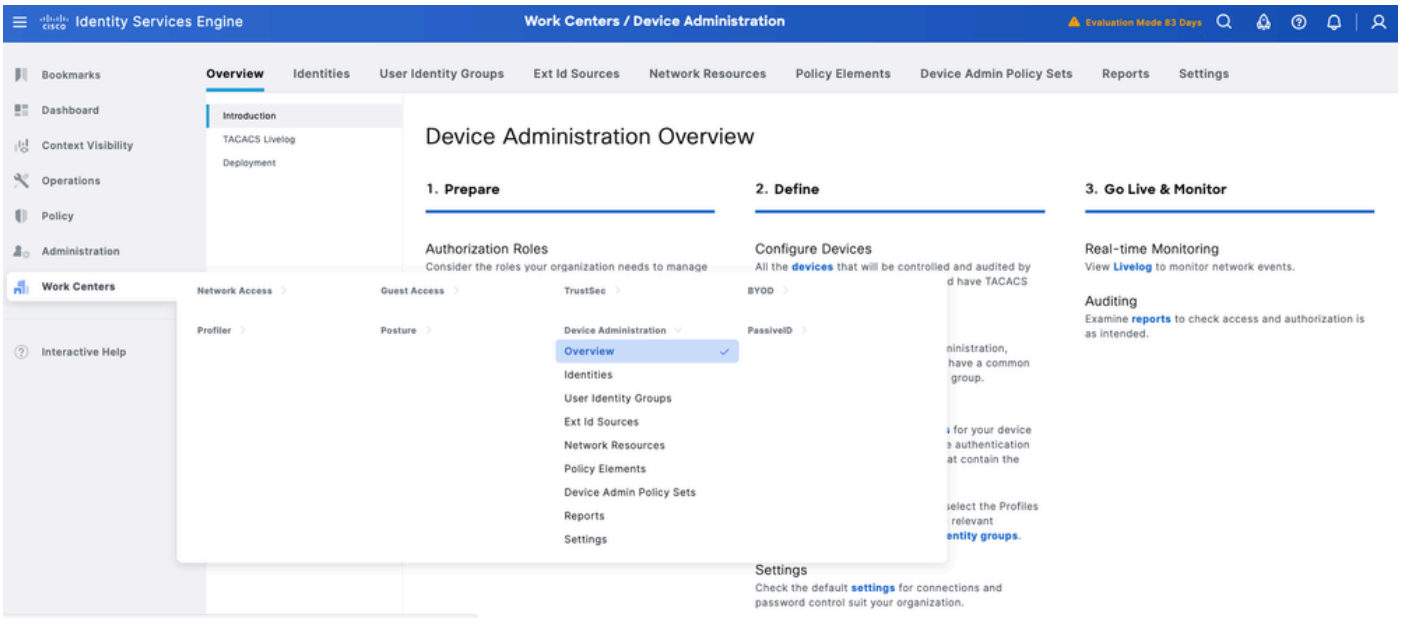
Stap 2. Blader onder Algemene instellingen omlaag en selecteer het selectievakje naast Apparaatbeheerservice inschakelen.



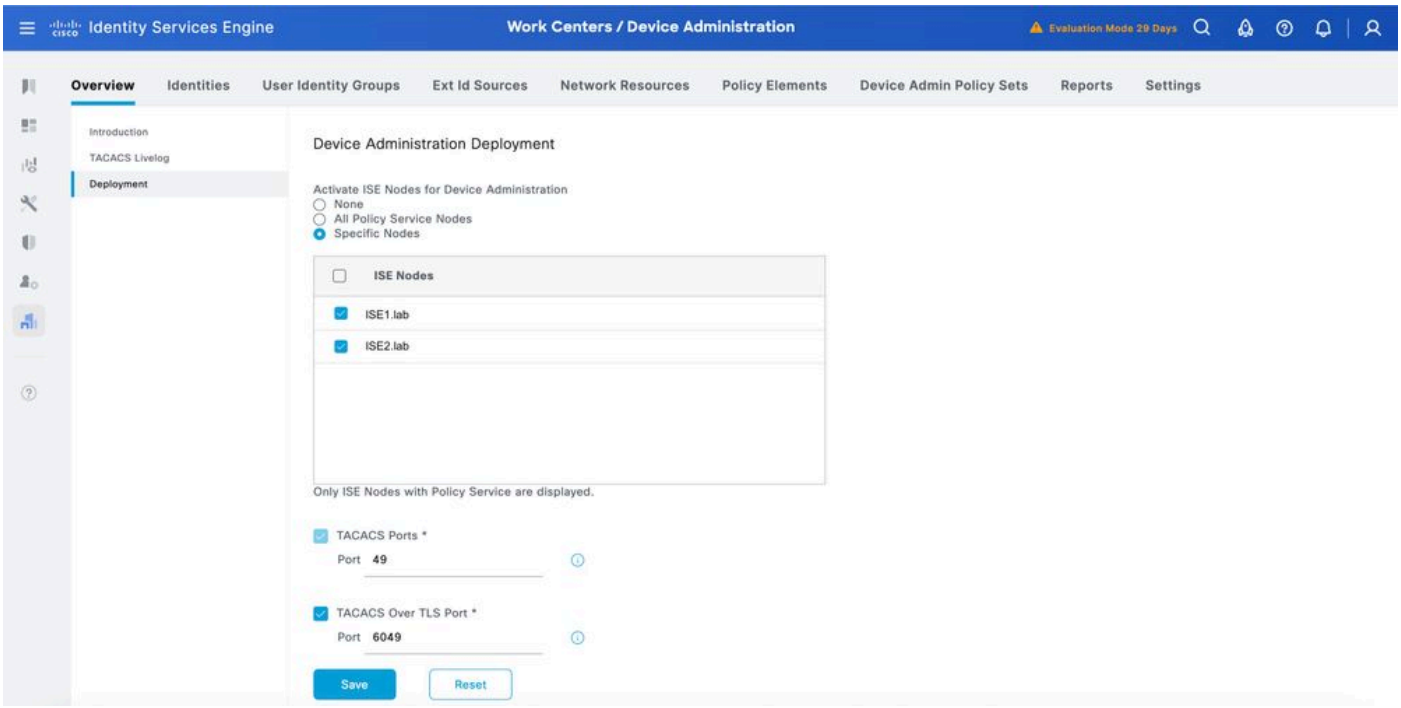
Stap 3. Sla de configuratie op. Device Admin Service is nu ingeschakeld op ISE.

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.

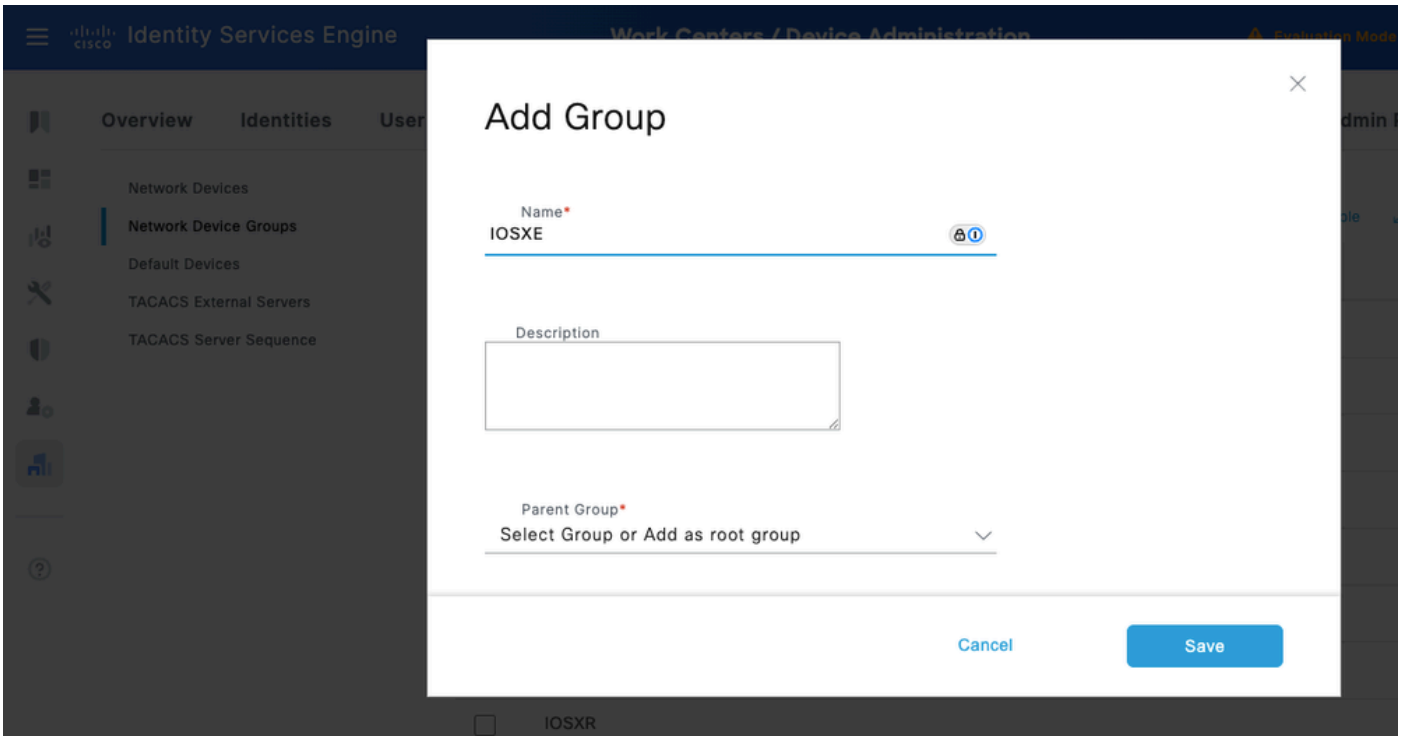


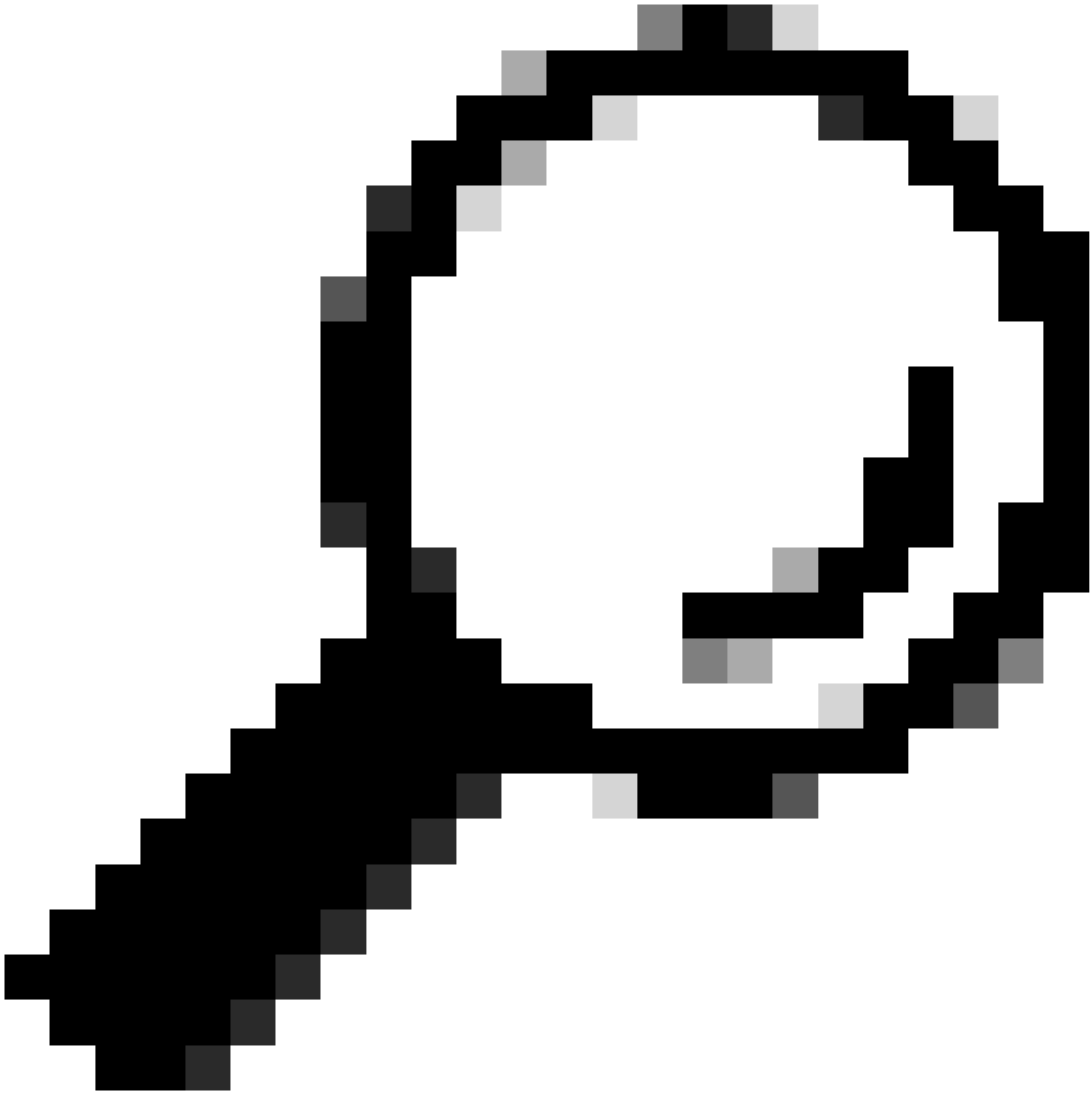
Stap 3.Behoud de standaardpoort 6049 of geef een andere TCP-poort op voor TACACS via TLS en klik vervolgens op Opslaan.

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 XE.

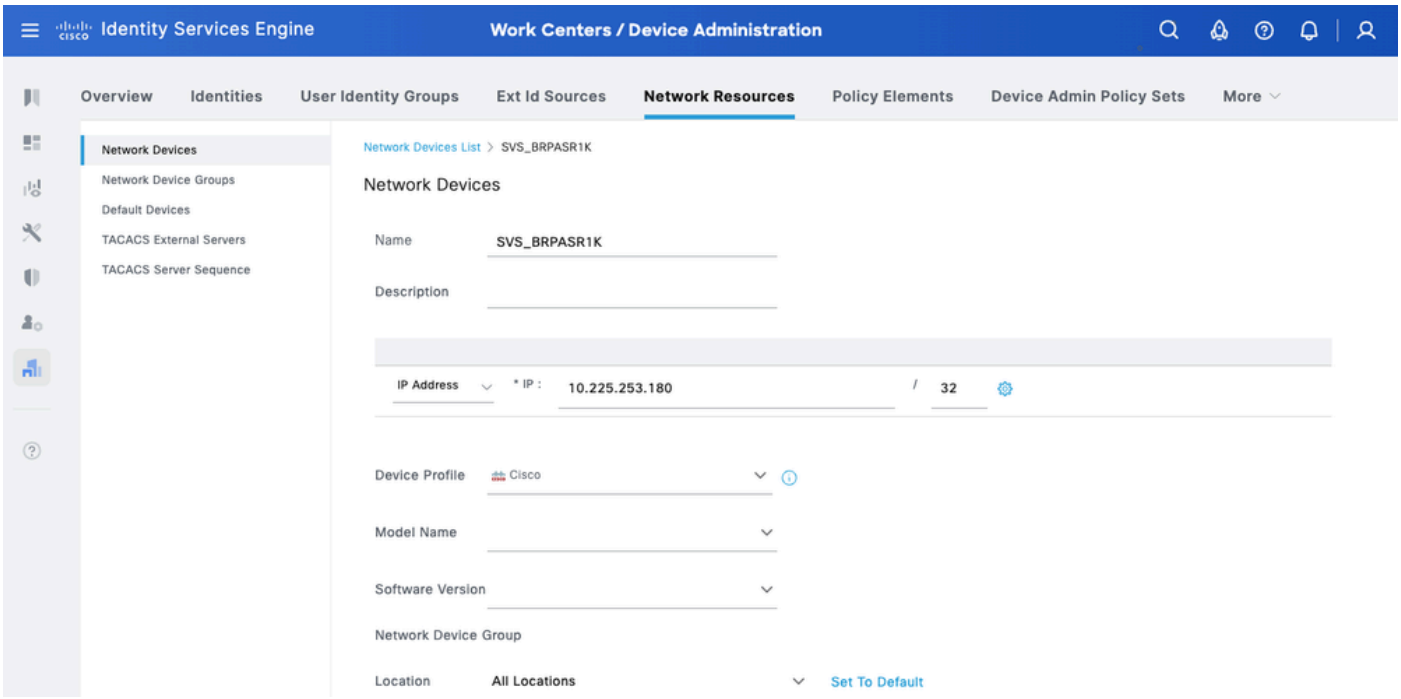

Identity Services Engine
Overview
Identities
Network Devices
Network Device Groups
Default Devices
TACACS External Servers
TACACS Server Sequence
Add Group
Name*
IOSXE
Description
Parent Group*
Select Group or Add as root group
Cancel
Save
IOSXR



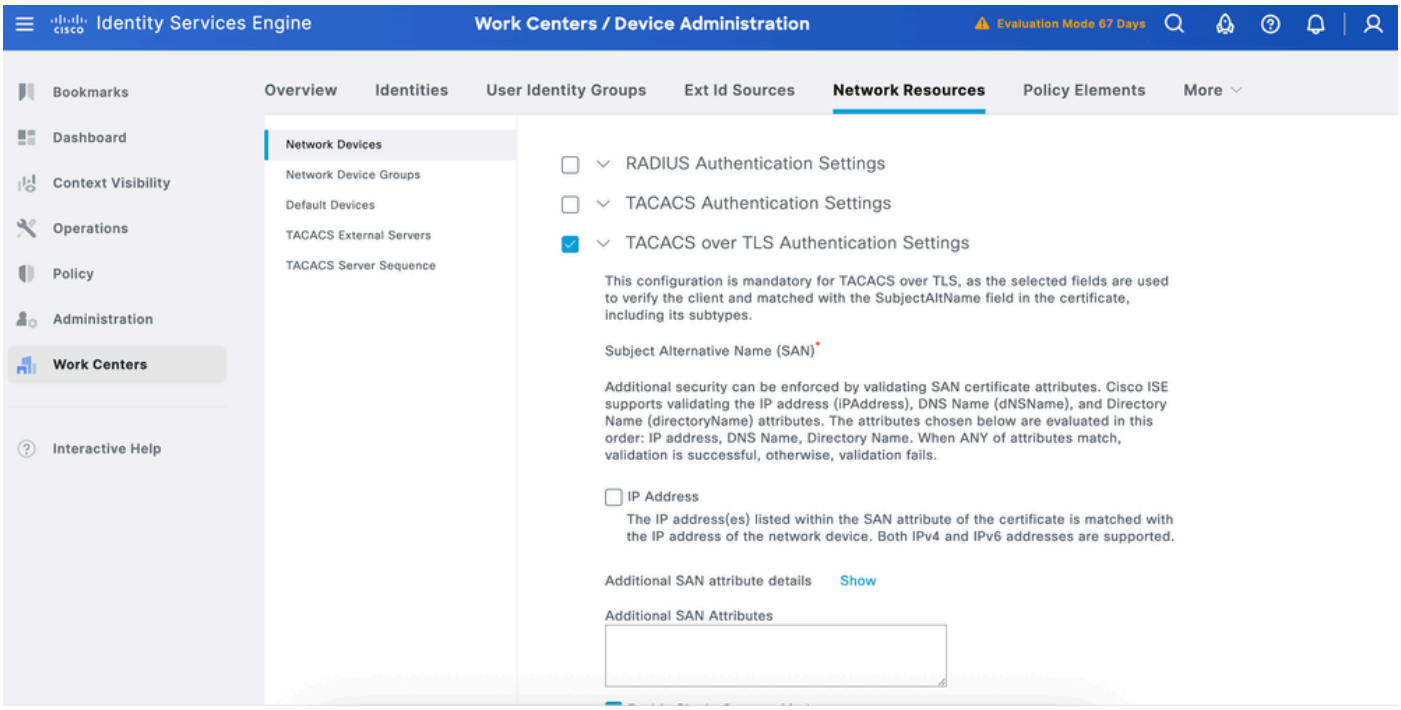
Tip: Alle apparaattypen en alle locaties zijn standaard hiërarchieën die door ISE worden verstrekt. U kunt uw eigen hiërarchieën toevoegen en de verschillende componenten definiëren bij het identificeren van een netwerkapparaat dat later in de beleidsvoorwaarde kan worden gebruikt

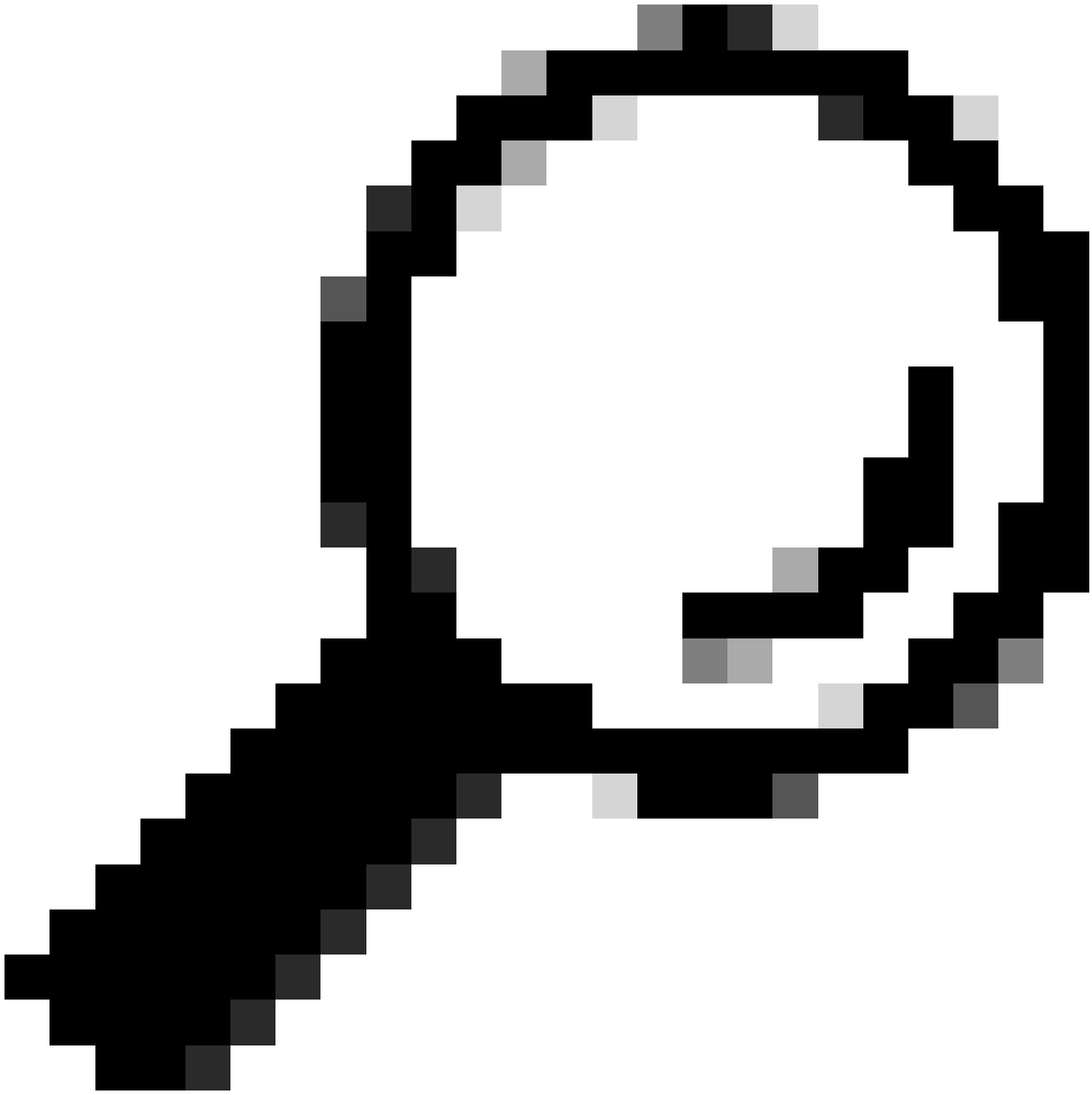
---

Stap 2.Voeg nu een Cisco IOS XE-apparaat toe als netwerkapparaat. Navigeer naar Werkcentra > Apparaatbeheer > Netwerkbronnen > Netwerkapparaten. Klik op Toevoegen om een nieuw netwerkapparaat toe te voegen. Voor deze test zou het SVS_BRPASR1K zijn.



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



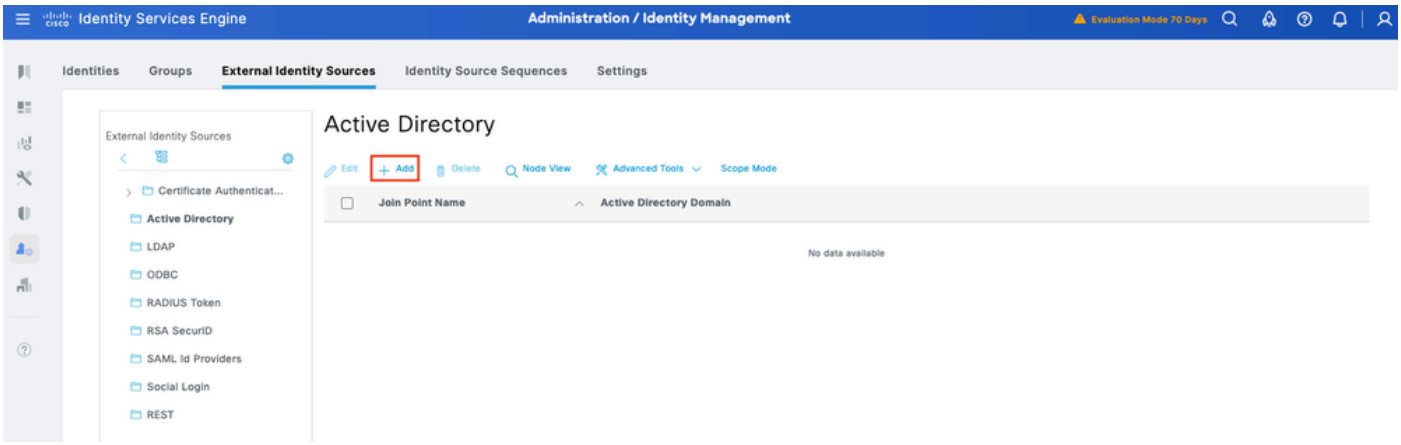


Tip: Het wordt aanbevolen om de modus Single Connect in te schakelen om te voorkomen dat de TCP-sessie opnieuw wordt gestart telkens wanneer een opdracht naar het apparaat wordt verzonden.

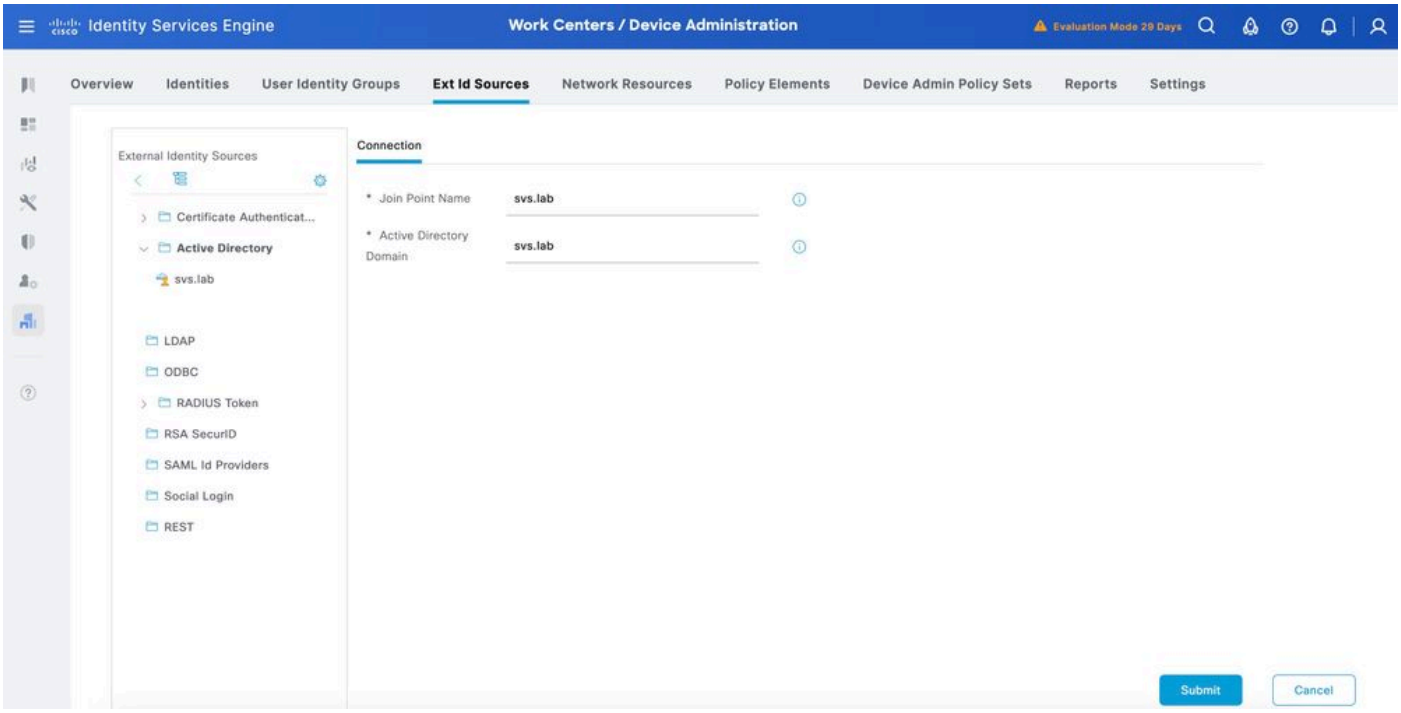
Identiteitswinkels configureren

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.

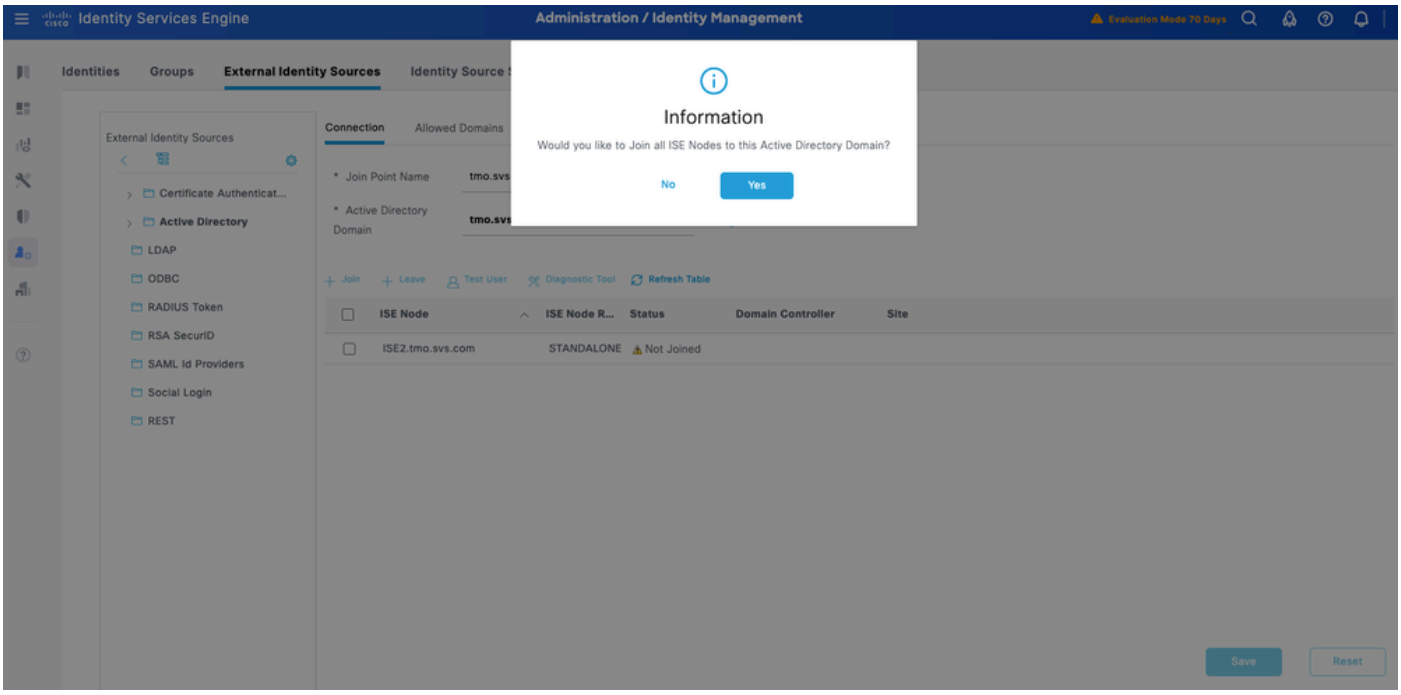
Stap 1. Navigeer naar Beheer > Identiteitsbeheer > Externe identiteitswinkels > Active Directory. Klik op Toevoegen om een nieuw AD-verbindingspunt te definiëren.



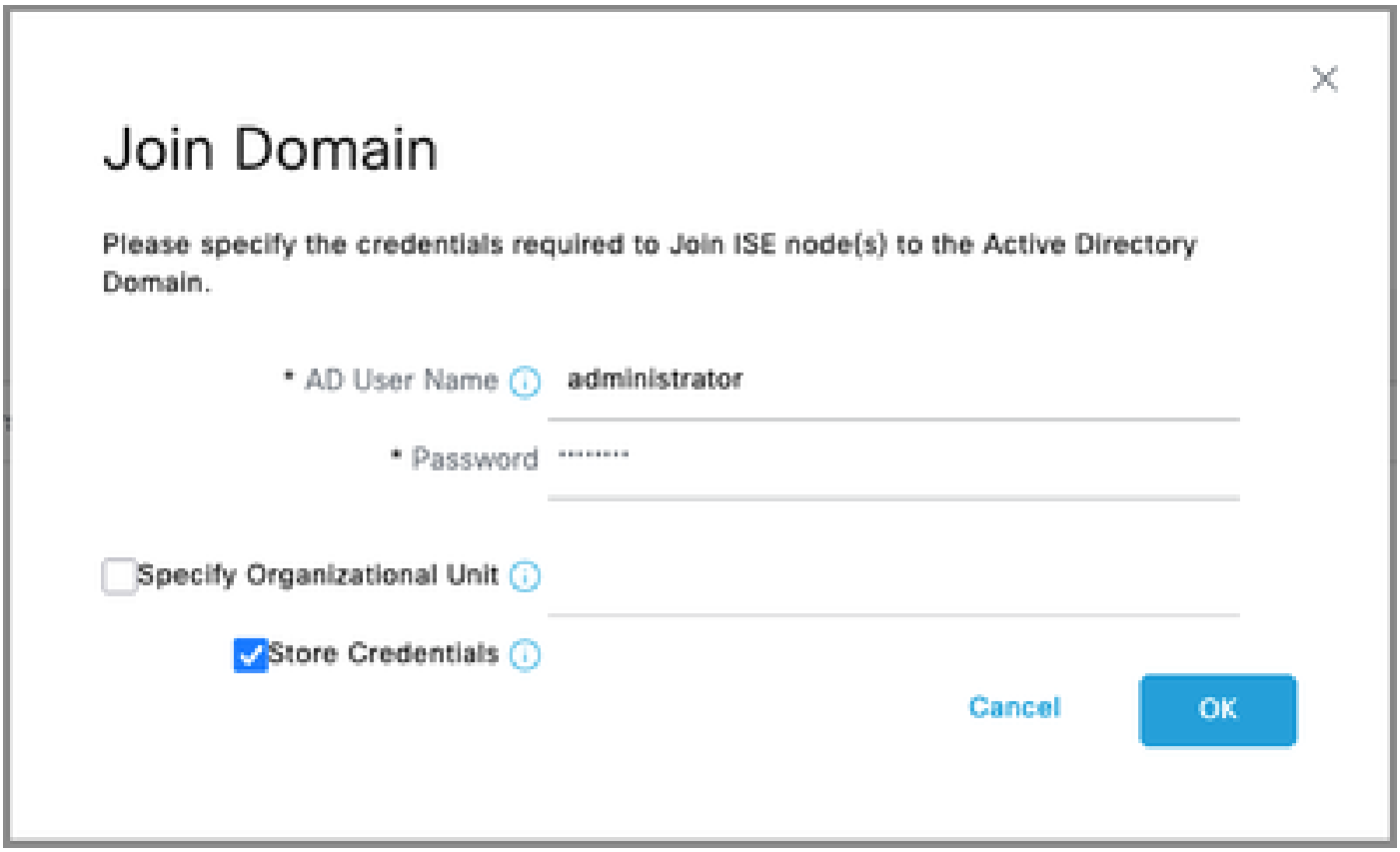
Stap 2. Geef de naam van het aanmeldpunt en de AD-domeinnaam op en klik op Indienen.

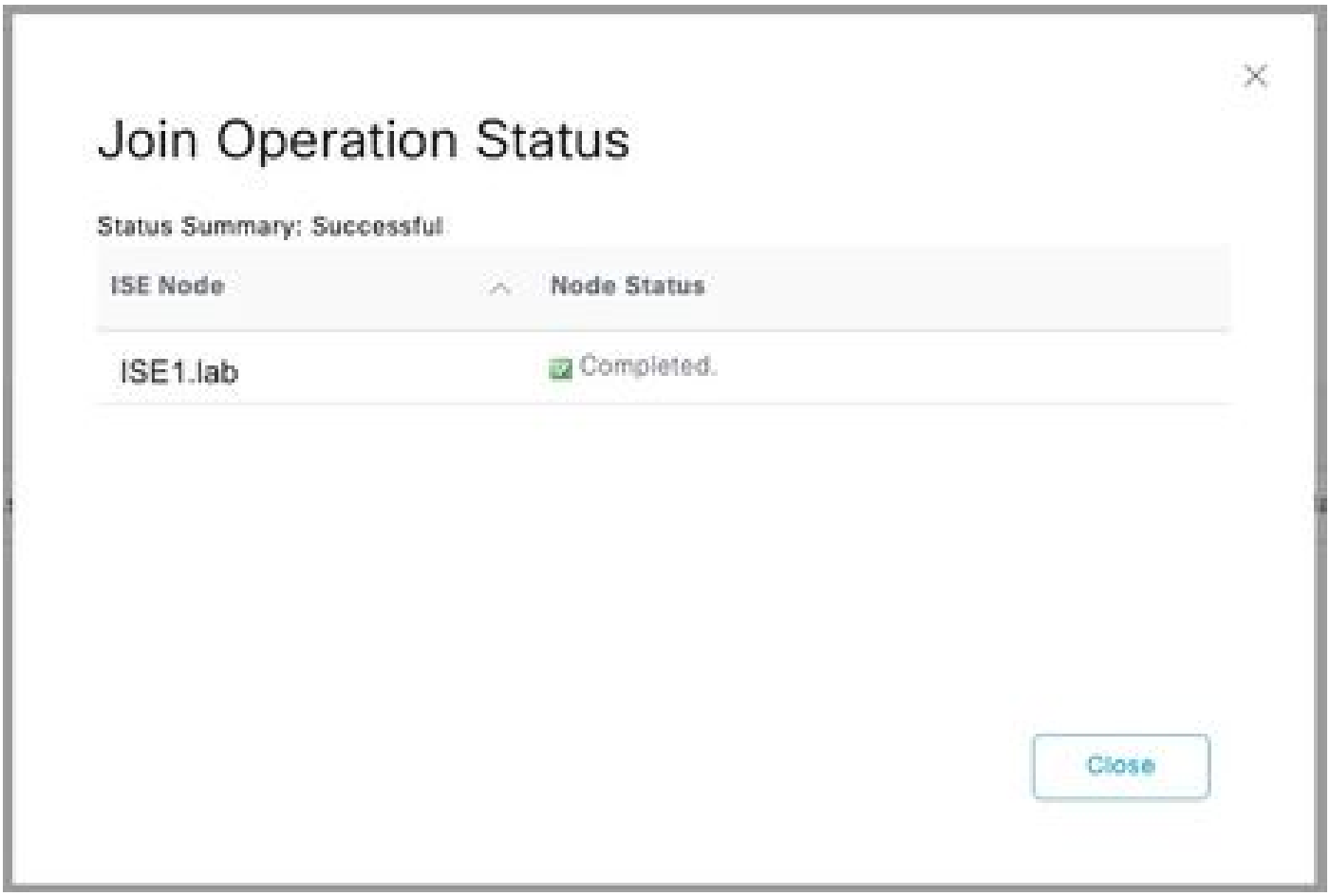


Stap 3. Klik op Ja wanneer u wordt gevraagd Wilt u alle ISE-knooppunten aan dit Active Directory-domein toevoegen?

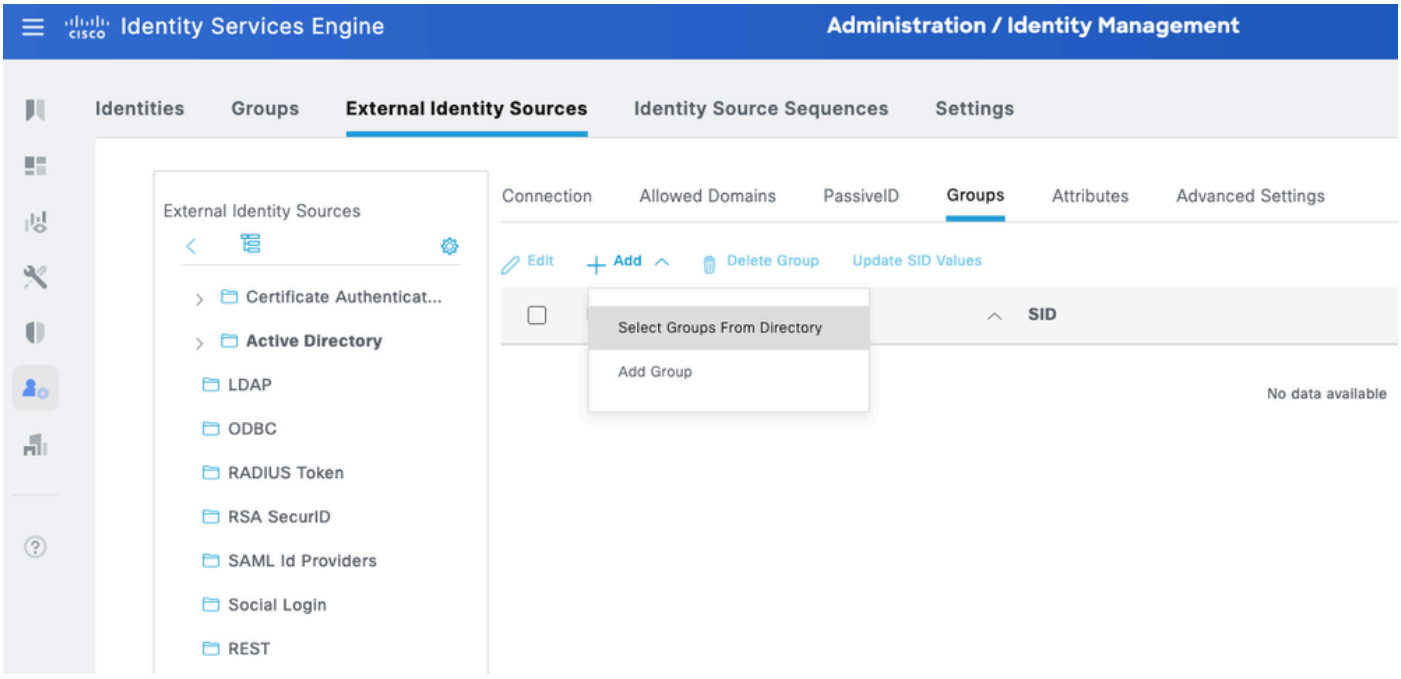


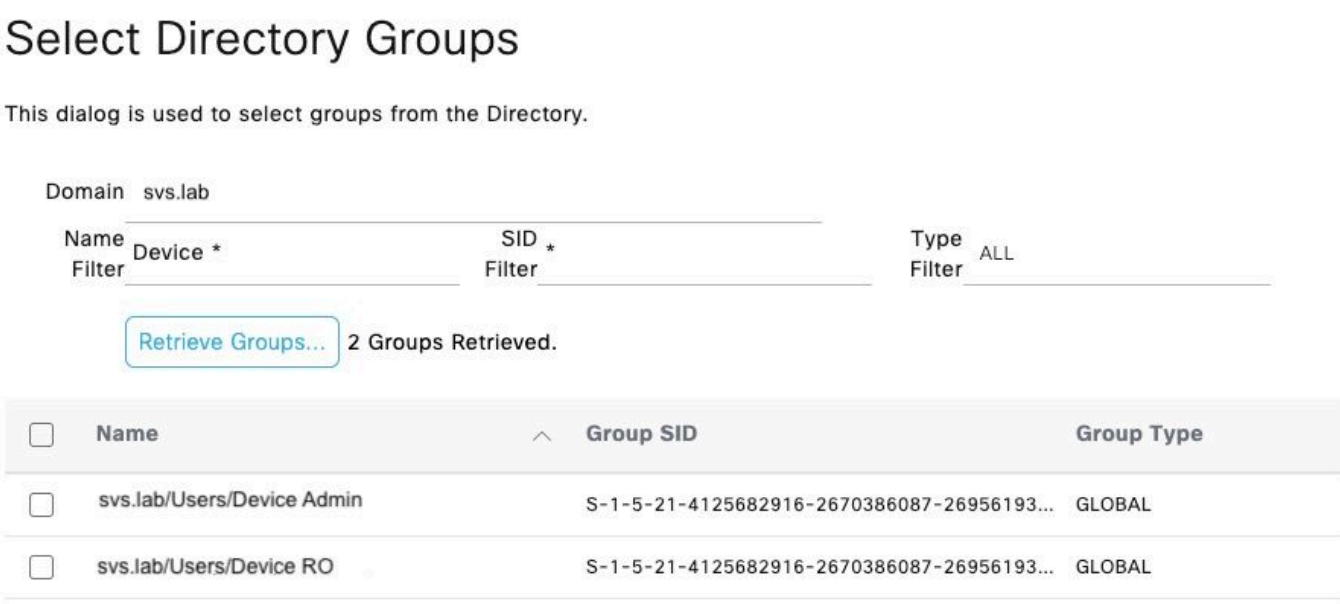
Stap 4. Voer de referenties in met AD join-bevoegdheden en voeg ISE toe aan AD. Controleer de status om te controleren of deze operationeel is.

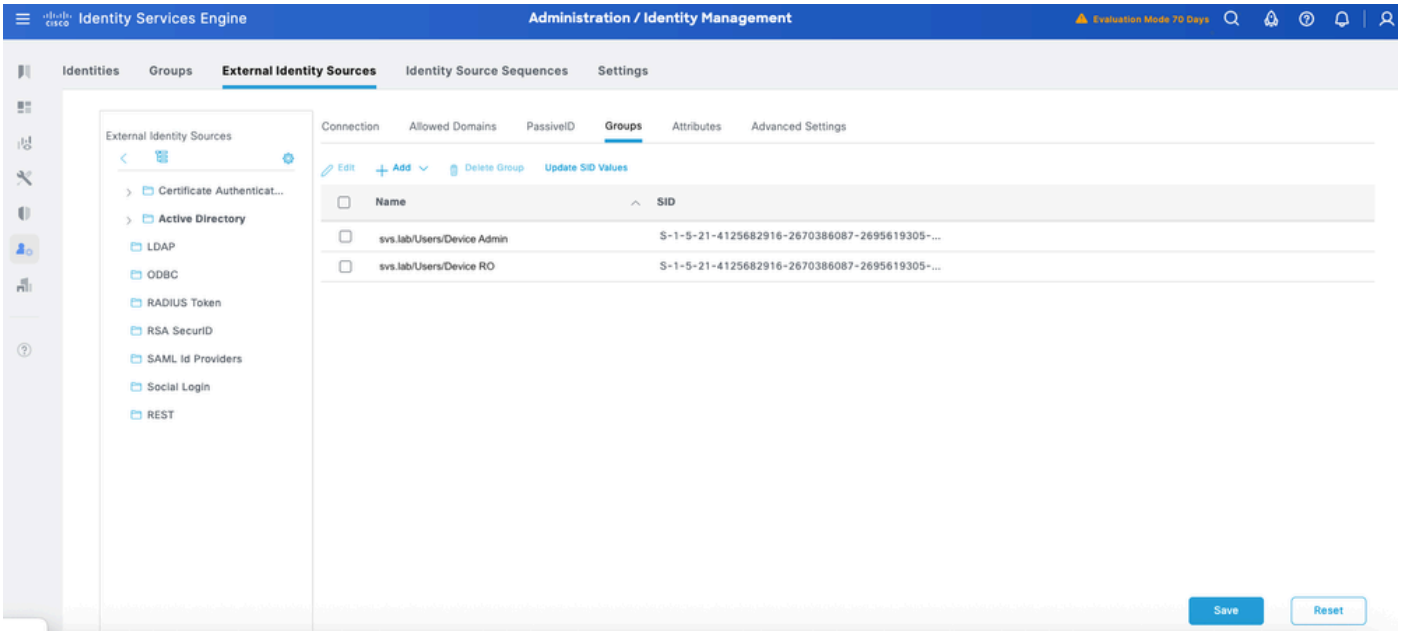




Stap 5. Navigeer naar het tabblad Groepen en klik op Toevoegen om alle benodigde groepen te krijgen op basis waarvan de gebruikers zijn geautoriseerd voor toegang tot het apparaat. In dit voorbeeld worden de groepen weergegeven die worden gebruikt in het machtigingsbeleid in deze handleiding







TACACS+-profielen configureren

U gaat de TACACS+-profielen toewijzen aan de twee belangrijkste gebruikersrollen op de Cisco IOS XE-apparaten:

- 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.

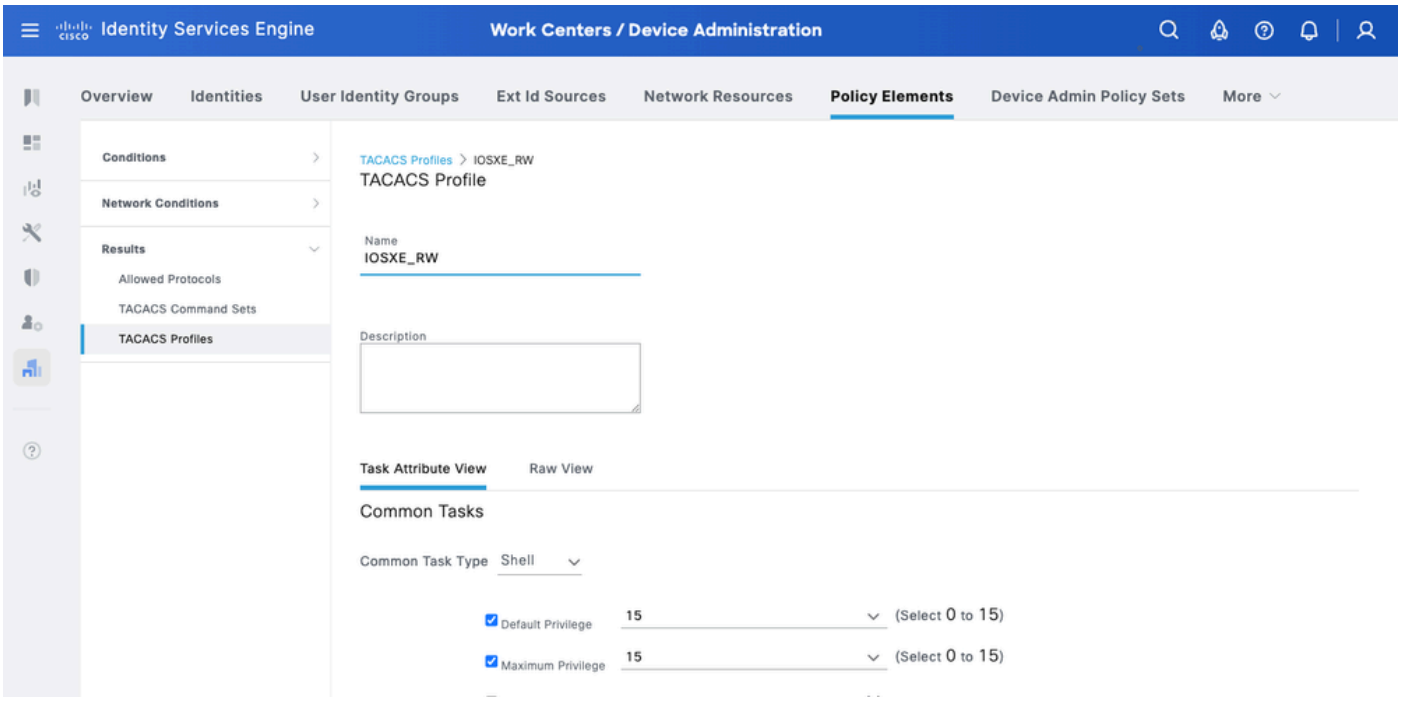
Deze worden gedefinieerd als twee TACACS+-profielen: IOS XE_RW en IOSXR_RO.

IOS XE_RW - Beheerdersprofiel

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

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

Stap 3. Bevestig de configuratie en bewaar.

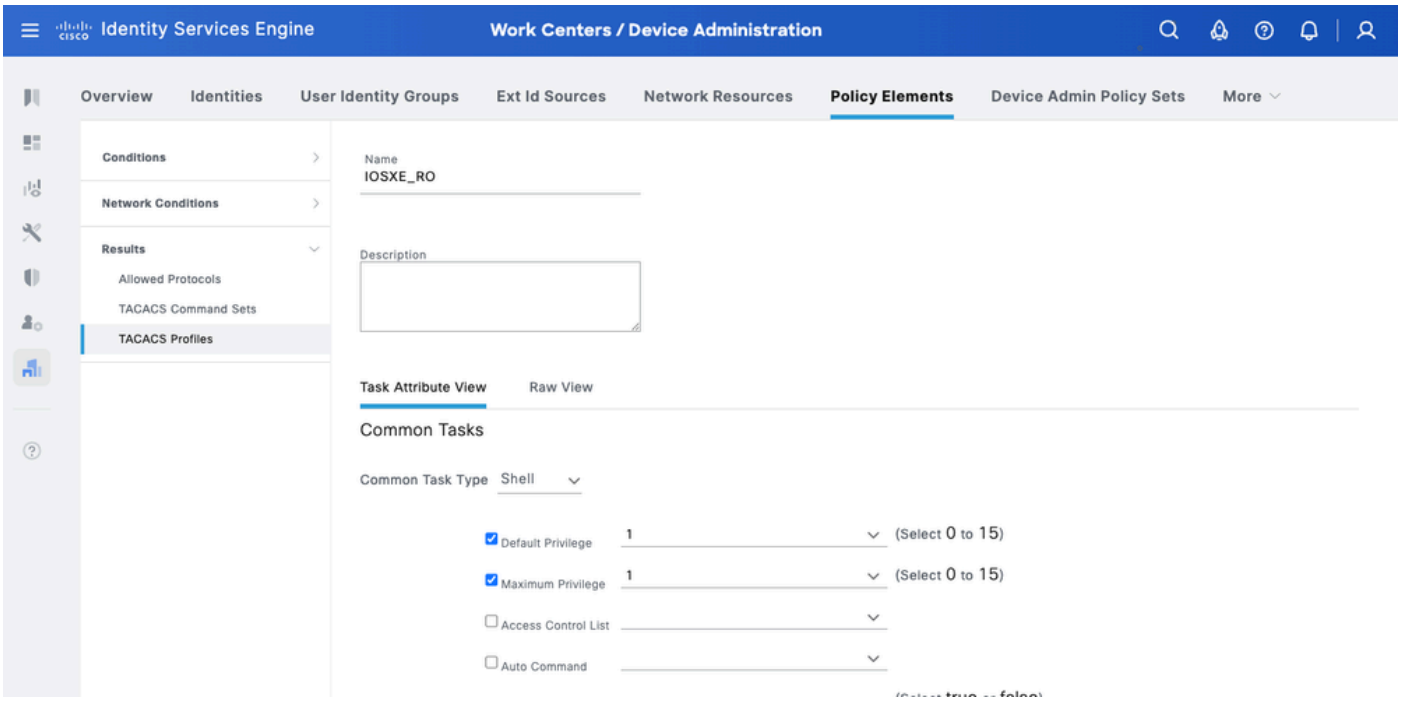


IOS XE_RO - Gebruikersprofiel

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

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

Stap 3. Bevestig de configuratie en bewaar.



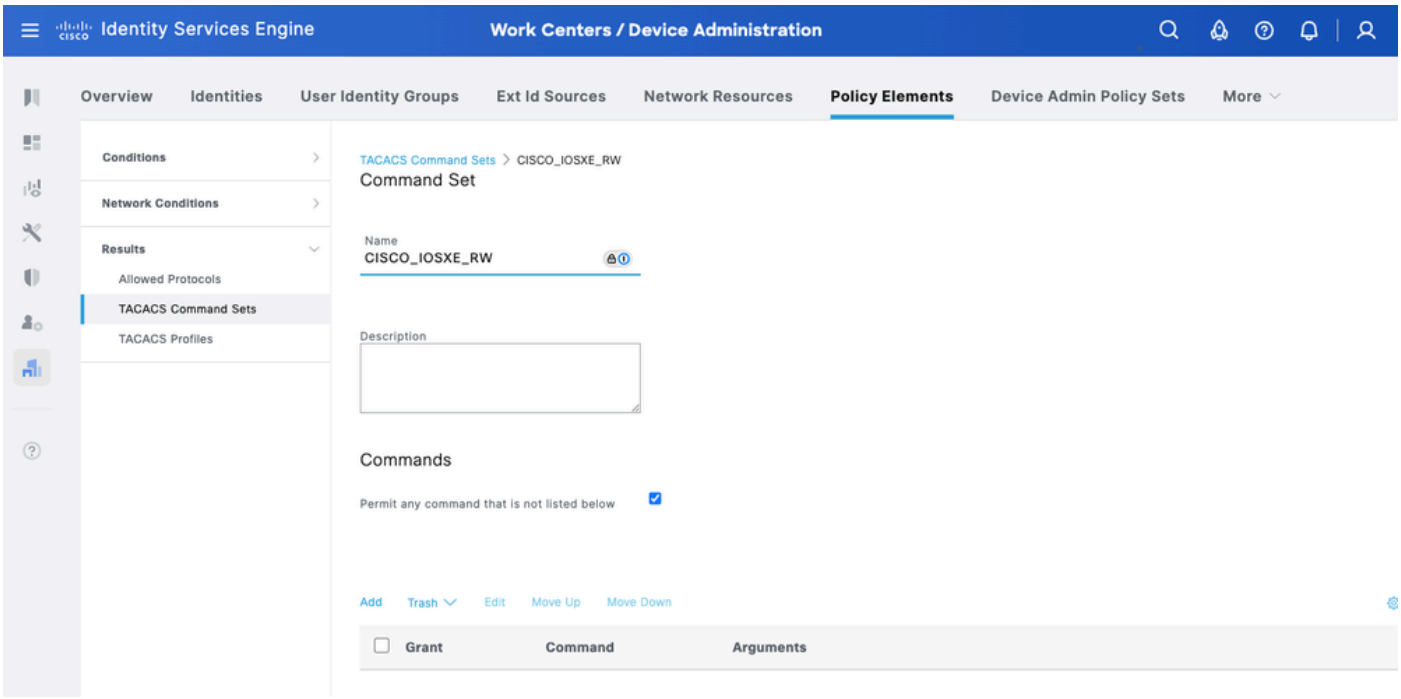
TACACS+-opdrachtreeksen configureren

Deze worden gedefinieerd als twee TACACS+-opdrachtsets: CISCO_IOS XE_RW en CISCO_IOS XE_RO.

CISCO_IOS XE_RW - Opdrachtset voor beheerders

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

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



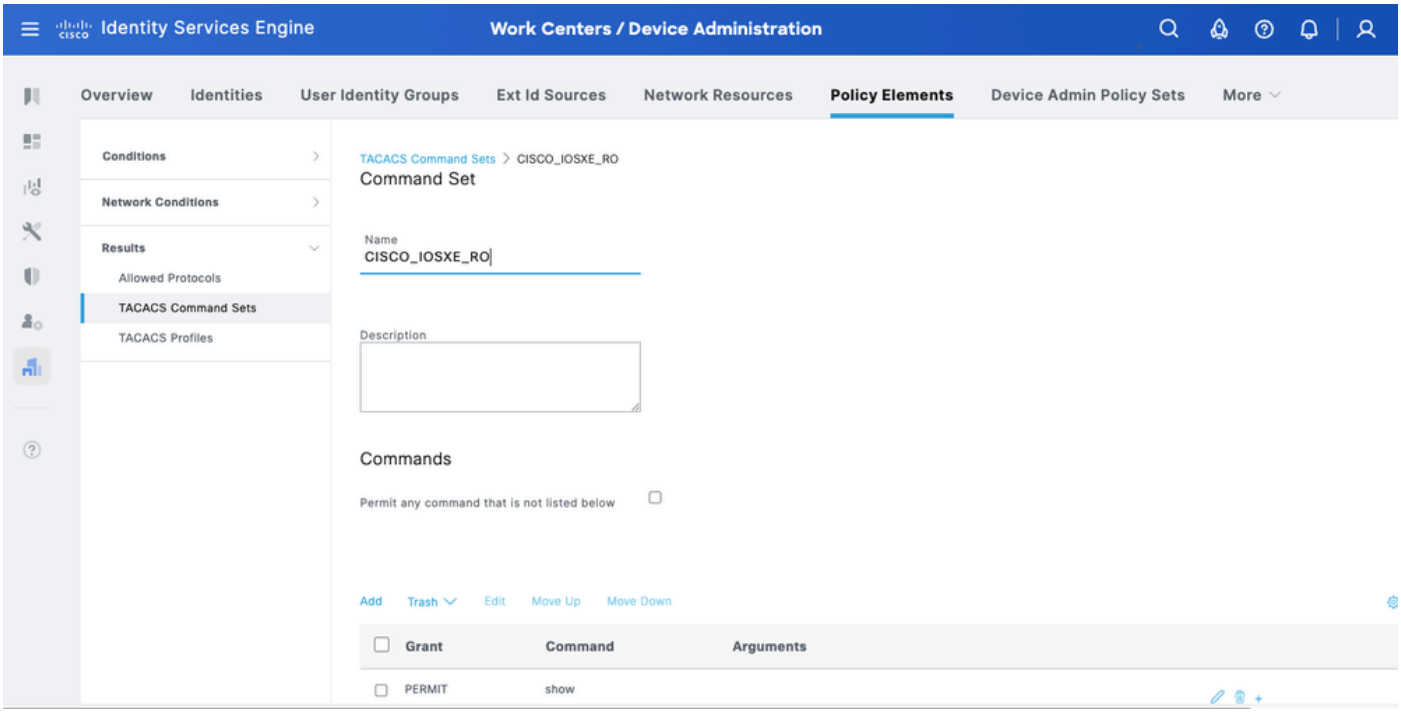
CISCO_IOS XE_RO - Operator Command Set

Stap 1 Van ISE UI, navigeert u naar Werkcentra > Apparaatbeheer > Beleidselementen > Resultaten > TACACS-opdrachtsets. Voeg een nieuwe TACACS-opdrachtset toe en noem deze CISCO_IOS XE_RO.

Stap 2. In het gedeelte Opdrachten voegt u een nieuwe opdracht toe.

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

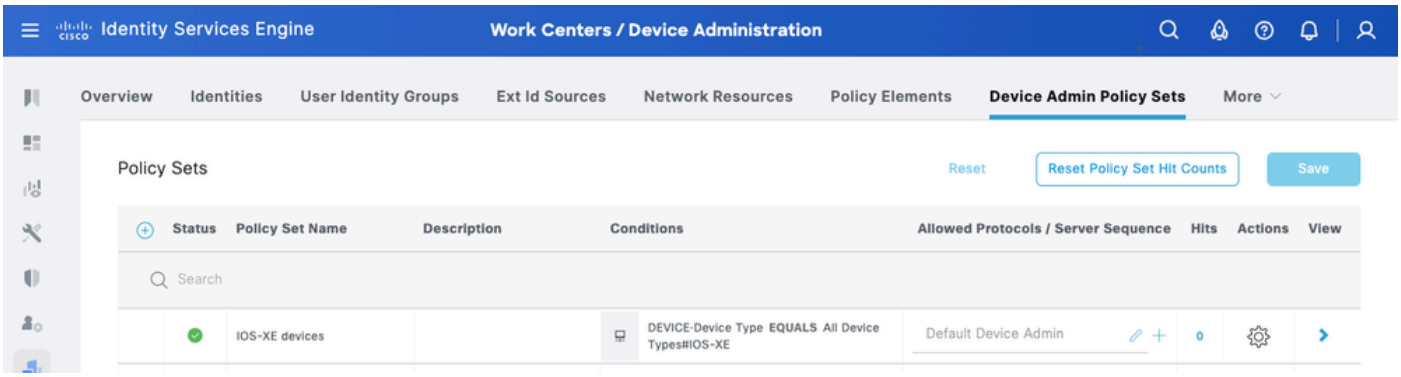
Stap 4. Bevestig de gegevens en klik op Opslaan.



Apparaatbeheerbeleidssets configureren

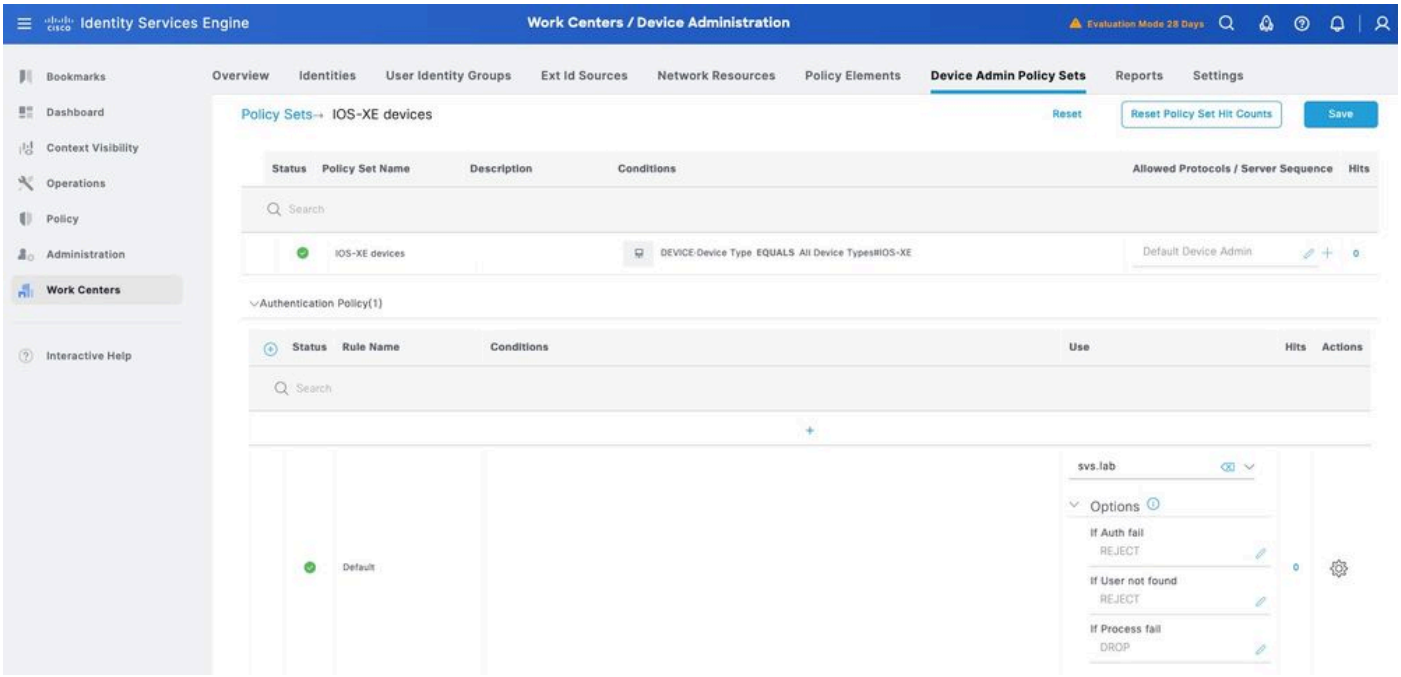
Beleidssets zijn standaard ingeschakeld voor Apparaatbeheer. Beleidsgroepen kunnen beleid verdelen op basis van de apparaattypen om de toepassing van TACACS-profielen te vergemakkelijken.

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



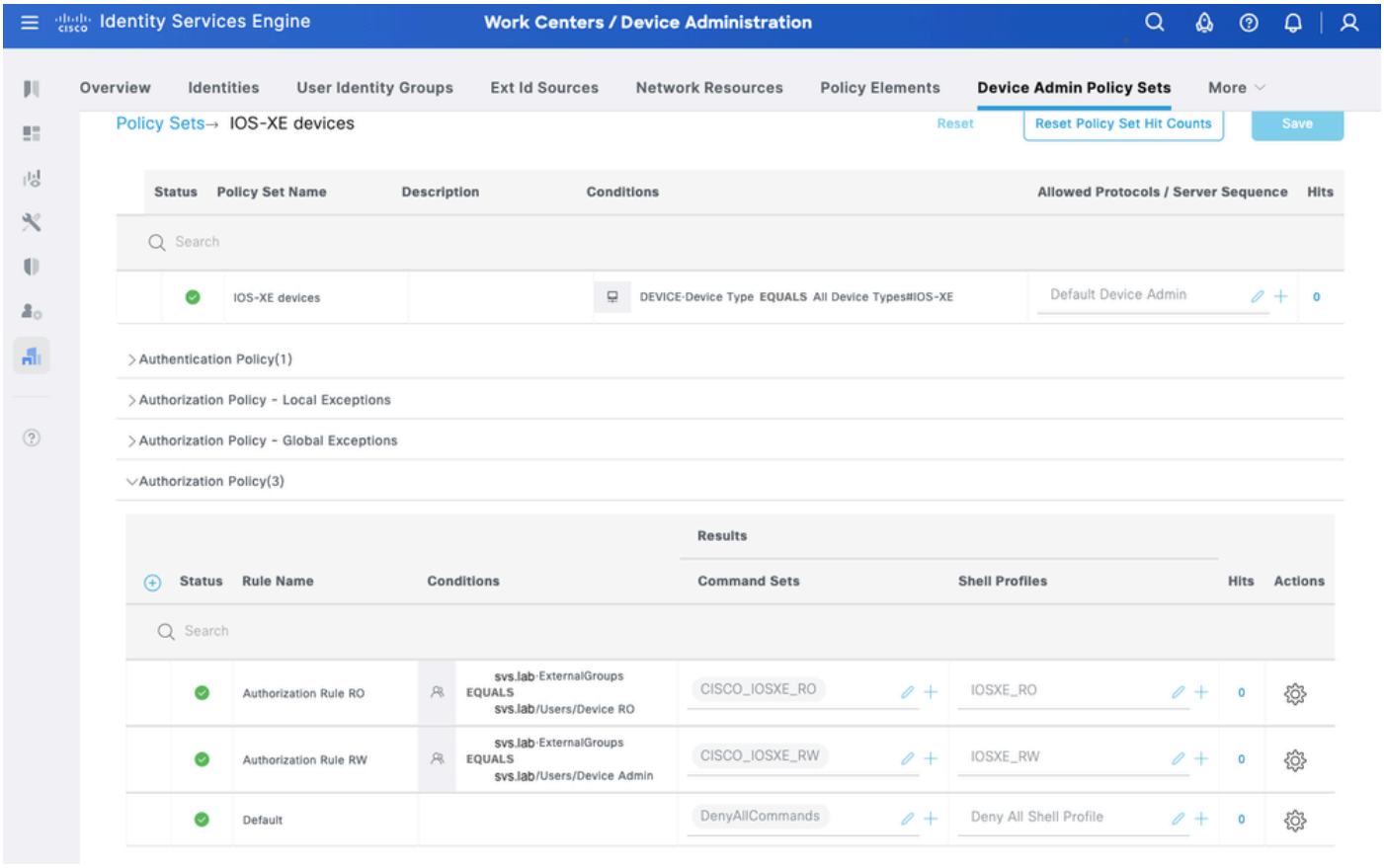
Stap 4. Definieer het autorisatiebeleid.

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

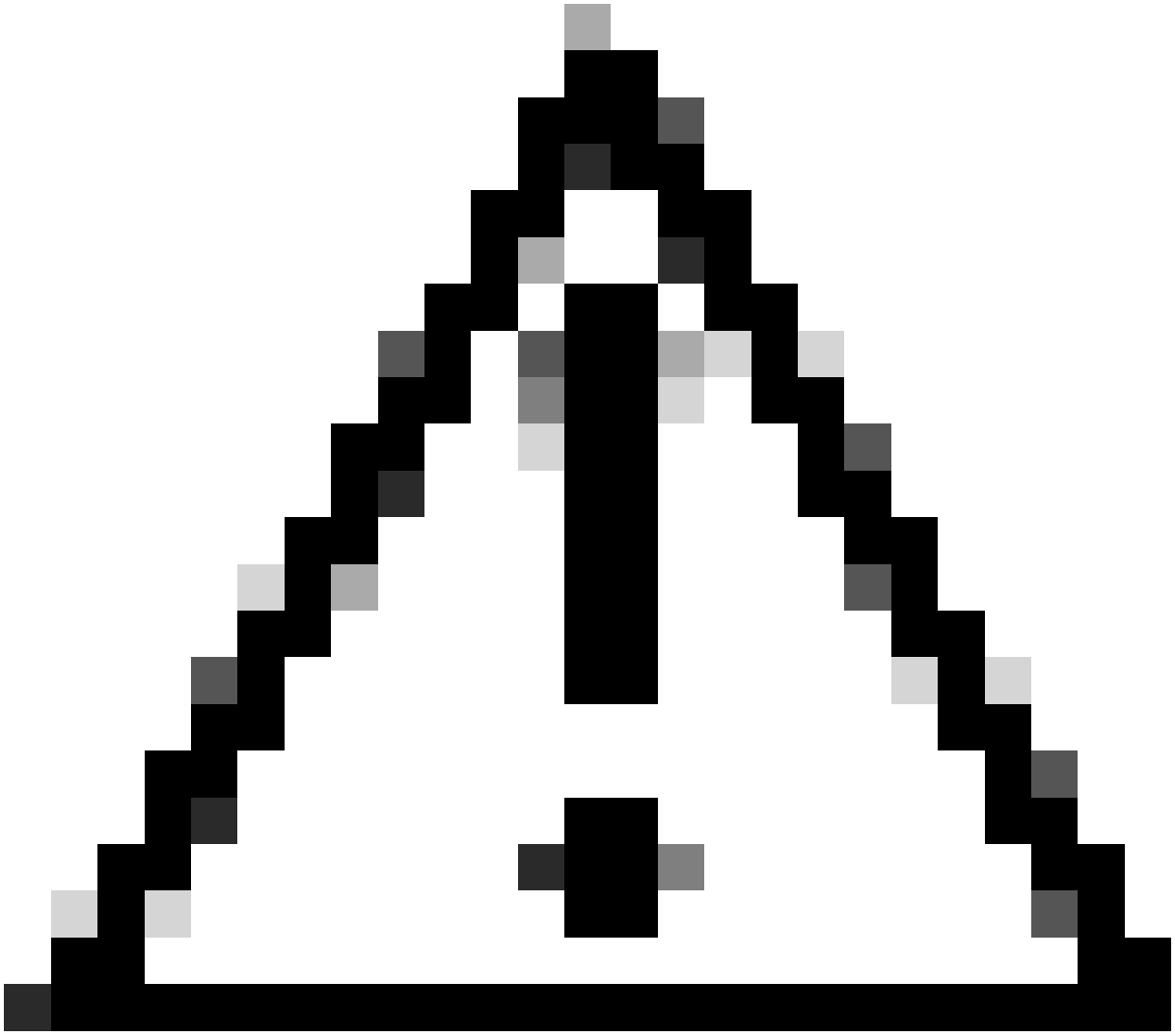
Voorbeeld:

· Gebruikers in de AD-groep Device RO krijgen de CISCO_IOSXR_RO-opdrachtset en het IOSXR_RO-shell-profiel toegewezen.

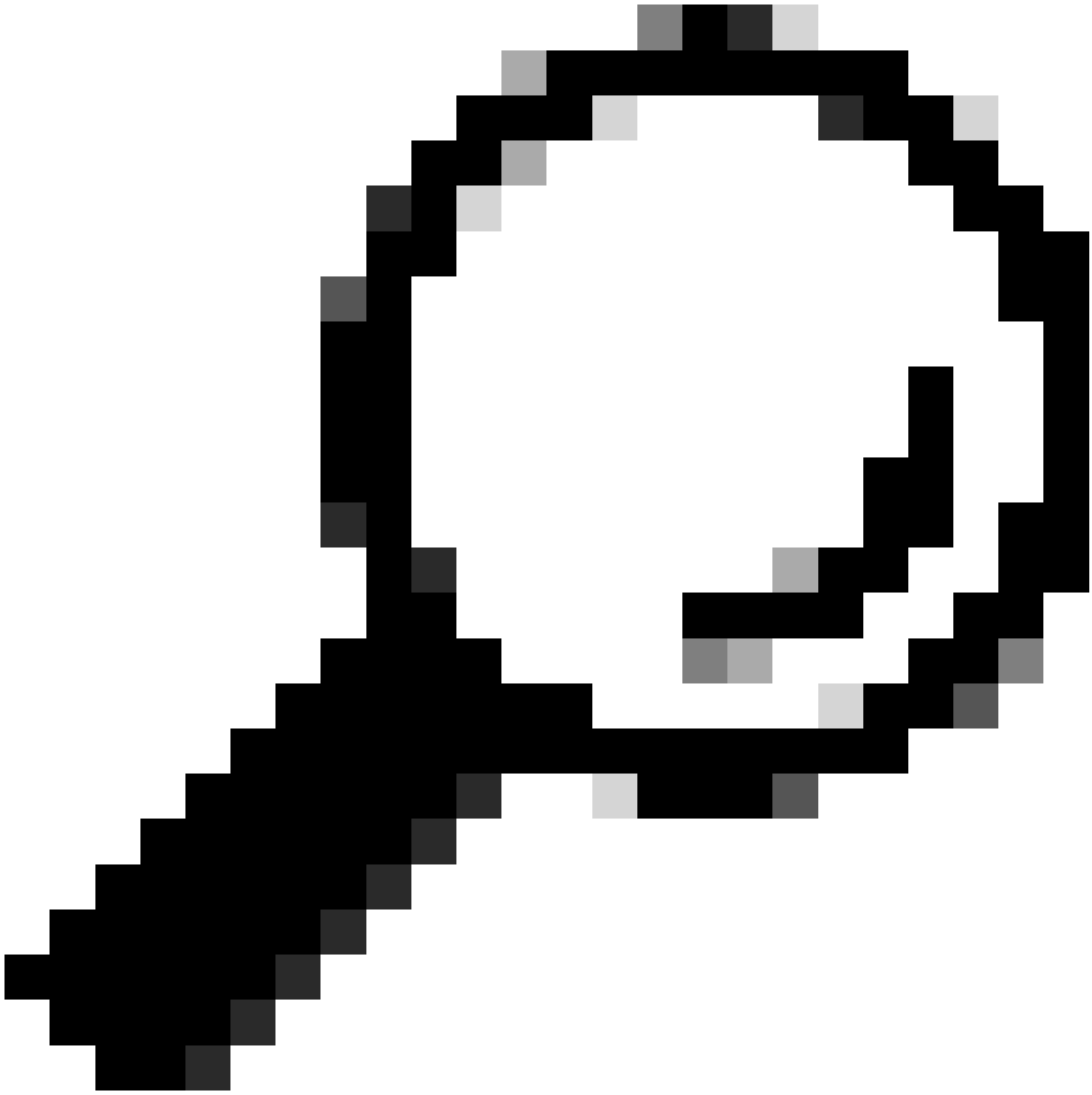
· Gebruikers in de AD-groep Apparaatbeheer krijgen de CISCO_IOSXR_RW-opdrachtset en het IOSXR_RW-shell-profiel toegewezen.



Deel 2 - Cisco IOS XE configureren voor TACACS+ via 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.

Configuratiemethode 1 - Sleutelpaar gegenereerd door apparaat

TACACS+-serverconfiguratie

Stap 1Configureer de domeinnaam en genereer een sleutelpaar dat wordt gebruikt voor routertrustpoint.

```
ip domain name svs.lab

crypto key generate ec keysize 256 label svs-256ec-key
```

Trustpoint-configuratie

Stap 1 Maak een routervertrouwenspunt en koppel het sleutelpaar.

```
crypto pki trustpoint svs_cat9k
  enrollment terminal pem
  subject-name C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=cat9k.svs.lab
  serial-number none
  ip-address none
  revocation-check none
  eckeypair svs-256ec-key
```

Stap 2. Verifieer Trustpoint door CA-certificaat te installeren.

<#root>

cat9k(config)#

crypto pki authenticate svs_cat9k

```
Enter the base 64 encoded CA certificate.

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+t3c1sNbN2AtFi4cJovTA01xh6OI4QnK+MNQKpTjt/E4
ydHl0rrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVLl783nTc9wYptQEPi5sw
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
xDrmo7eOXPpSW4l72a6Kl8CR3U2Cr4wsuvndPEq/qd2NRSBWffF0XE/AJHQG7STT
HaXLU9r2Ko6O3oecu8ysGTwLlIt/9T1/FOb0xZRugWcpJrVoTgDGuA==

-----END CERTIFICATE-----

Certificate has the following attributes:
   Fingerprint MD5: D9C4O4B2 ECO8A26O EC3539E7 F54ED17D
   Fingerprint SHA1: OEB181E9 5A3ED78O 3BC5A8O5 9A854A95 C83AC737

% Do you accept this certificate? [yes/no]:

yes


Trustpoint CA certificate accepted.
% Certificate successfully imported

cat9k(config)#
```

Stap 3. Genereer een aanvraag voor certificaatondertekening (CSR).

```
<#root>

cat9k(config)#

crypto pki enroll svs_cat9k


% Start certificate enrollment ..

% The subject name in the certificate will include: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=cat9k.svs.lab
% The subject name in the certificate will include: cat9k.svs.lab
Display Certificate Request to terminal? [yes/no]:

yes


Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
MIIBfDCCASMCAQAwgYQxGjAYBgNVBAMTEWNhdDlrLnRtby5zdnMuY29tMQwwCgYD
VQQLEwNTVlMxDjAMBgNVBAoTBUNpc2NvMQwwCgYDVQQHEwNSVFAxCzAJBgNVBAgT
Ak5DMQswCQYDVQQGEwJVUzEgMB4GCSqGSIb3DQEJAhYRY2FOOWsudG1vLnN2cy5j
b20wWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATpYE7atscrtl4ddevCh3UgxjYi
4N4oBGWrpJBctKy4so8V5i6RXDt7kHgPzp14Qnf20bcXVODE1wtTAHHBrIXqoDww
OgYJKoZIhvcNAQkOMSOwKzAcBgNVHREEFTATghFjYXQ5ay5ObW8uc3ZzLmNvbTAL
```

```
BgNVHQ8EBAMCB4AwCgYIKoZIzj0EAwQDRwAwRAIgZqP2QTwM3ZZrmIphJ7+jSTER
40kTx2DiVs1c1Xf+vR4CIBcSb18DIYz84DmgMHUaf778/cmpe9cWakvdaxMWseBH
-----END CERTIFICATE REQUEST-----

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]:
```

no

```
cat9k(config)#
```

Stap 4. CA-ondertekend certificaat importeren.

<#root>

```
cat9k(config)#
```

crypto pki import svs_cat9k certificate

```
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIID8zCCAdugAwIBAgIIKfdYWg5WpskwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNTE0MTUxMjAwWhcNMjYwNTE0MTUxMjAwWjCBhDEaMBgGA1UEAxMR
Y2F0OWsudG1vLnN2cy5jb20xDDAKBgNVBAsTA1NWUzEOMAwGA1UEChMFQ2lzY28x
DDAKBgNVBAcTA1JUUDELMAkGA1UECBMCTkMxCzAJBgNVBAYTAlVTMSAwHgYJKoZI
hvcNAQkCFhFjYXQ5ay5ObW8uc3ZzLmNvbTBZMBMGByqGSM49AgEGCCqGSM49AwEH
A0IABOlgTtq2xyu2Xh1168KHdSDGNiLg3igEZaukkFyOrLiyjxXmLpFcO3uQeA/O
nXhCd/bRtxdU4MTXC1MAccGsheqjTTBLMB4GCWCGSAGG+EIBDQQRFg94Y2EgY2Vy
dGlmaWNhdGUwHAYDVR0RBBUwE4IRY2F0OWsudG1vLnN2cy5jb20wCwYDVR0PBAQD
AgeAMA0GCSqGSIb3DQEBCwUAA4ICAQBObgKVykeyVC9UsvuuOAUsGaZHGwy2H9Yd
m5vIaui6PJczkCzIoAIghHPGQhIgpEcRqtGyXPZ2r8TCJP11WXNN/G73sFyWAhzY
RtmIM5KIojiDHLtifPayxv9juDuOZRx+wYR2PIQ5eLv1bafg7K8E82sqOCfOtcPr
Oc0NU8UCxqObdOgu4XsdBN1+wcWFqeQSDLmP7nxvhOOm/LXwCWUHwgVioOAuU2Fe
k5NthtvdxNAhRAImQdTyq6u/yB7vwTwJHcRiJc5USsyzCsTBb6RvL+HsXqBgXGc5
lxCSoLtYOdUxFIpJyK2MOZBY2zq2cNSc8Xbso5/OEQmnHtpWPvij4rSPUhQSY+4m
Qq2Sn3iqf4mGh/AO8T4iXfWDWfNezh7ZxMsCSCK/ZRlELZ2hj6OfzwX1H27Uf8XU
ecr0Wx+WzRn7LVRCaGQzFkukfi8S4DLLNtxnNHfsLBVX5yHXCLEL+CQ7n8Z/pxcB
VVrPitwN3ZbO9poZyWiRLTnBsb42xNaWiL9bjQznAOiTDfmfFFourBsaAioz7ouY
2r1Mh+OpE83Uu+4lOTMawDgGiEv7iaiJ6xWc95EC+AdmOx3FvBXMtIM9qr7WwHW6
3C2hVYHJH254elV5+H8iiz7rovEPm8ZDsnvYpJn4Km3iDvBNqp/vvAHOFcyXrvG6
3i/1b9erGQ==
-----END CERTIFICATE-----

% Router Certificate successfully imported

cat9k(config)#
```

TACACS & AAA met TLS-configuratie

Stap 1. Maak TACACS-server- en AAA-groepen, koppel het vertrouwenspunt van de client (router).

```
tacacs server svs_tacacs
 address ipv4 10.225.253.209
 single-connection
 tls port 6049
 tls idle-timeout 60
 tls connection-timeout 60
 tls trustpoint client svs_cat9k
 tls ip tacacs source-interface GigabitEthernet0/0
 tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ svs_tls
 server name svs_tacacs
 ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

Stap 2. AAA-methoden configureren.

```
aaa authentication login default group svs_tls local enable
aaa authentication login console local enable
aaa authentication enable default group svs_tls enable
aaa authorization config-commands
aaa authorization exec default group svs_tls local if-authenticated
aaa authorization commands 1 default group svs_tls local if-authenticated
aaa authorization commands 15 default group svs_tls
aaa accounting exec default start-stop group svs_tls
aaa accounting commands 1 default start-stop group svs_tls
aaa accounting commands 15 default start-stop group svs_tls
aaa session-id common
```

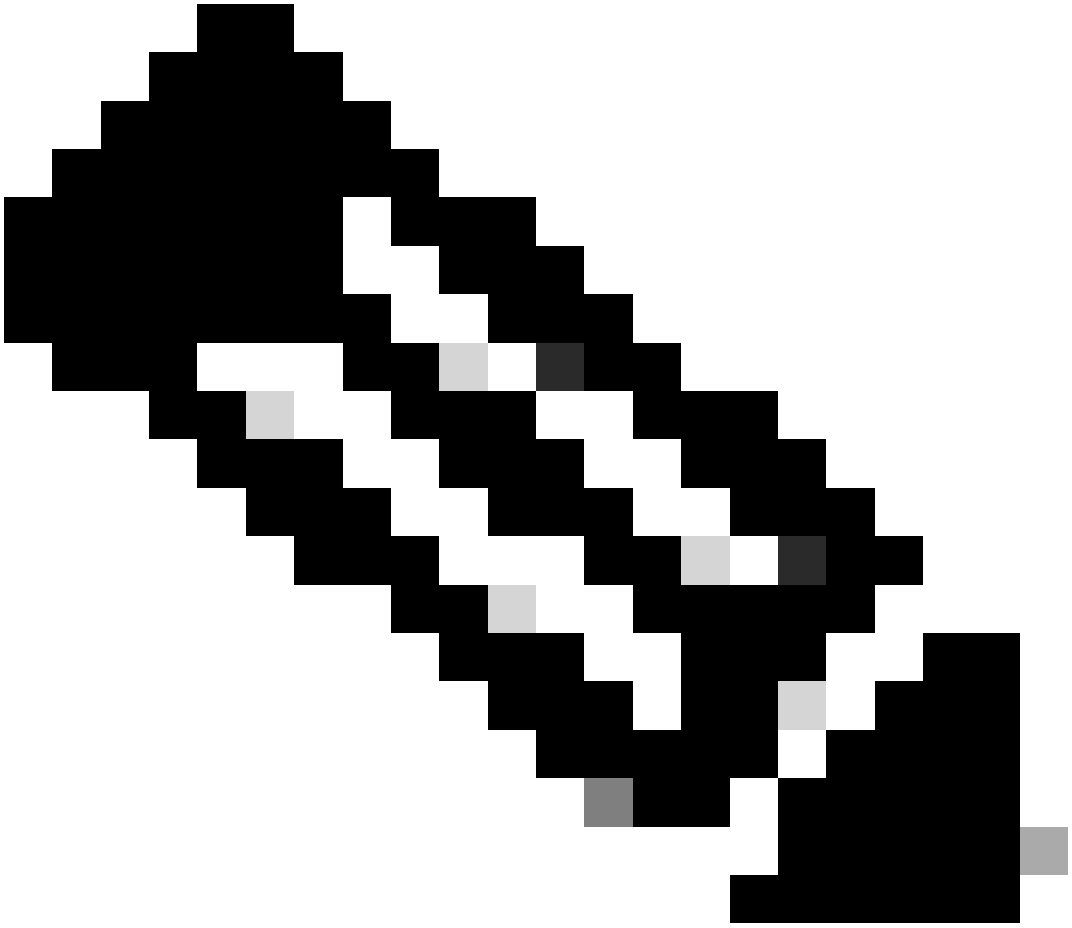
Configuratiemethode 2 - CA-gegenereerd sleutelpaar

Als u de sleutels, apparaten en CA-certificaten rechtstreeks importeert in een PKCS#12-indeling in plaats van de CSR-methode, kunt u deze methode gebruiken.

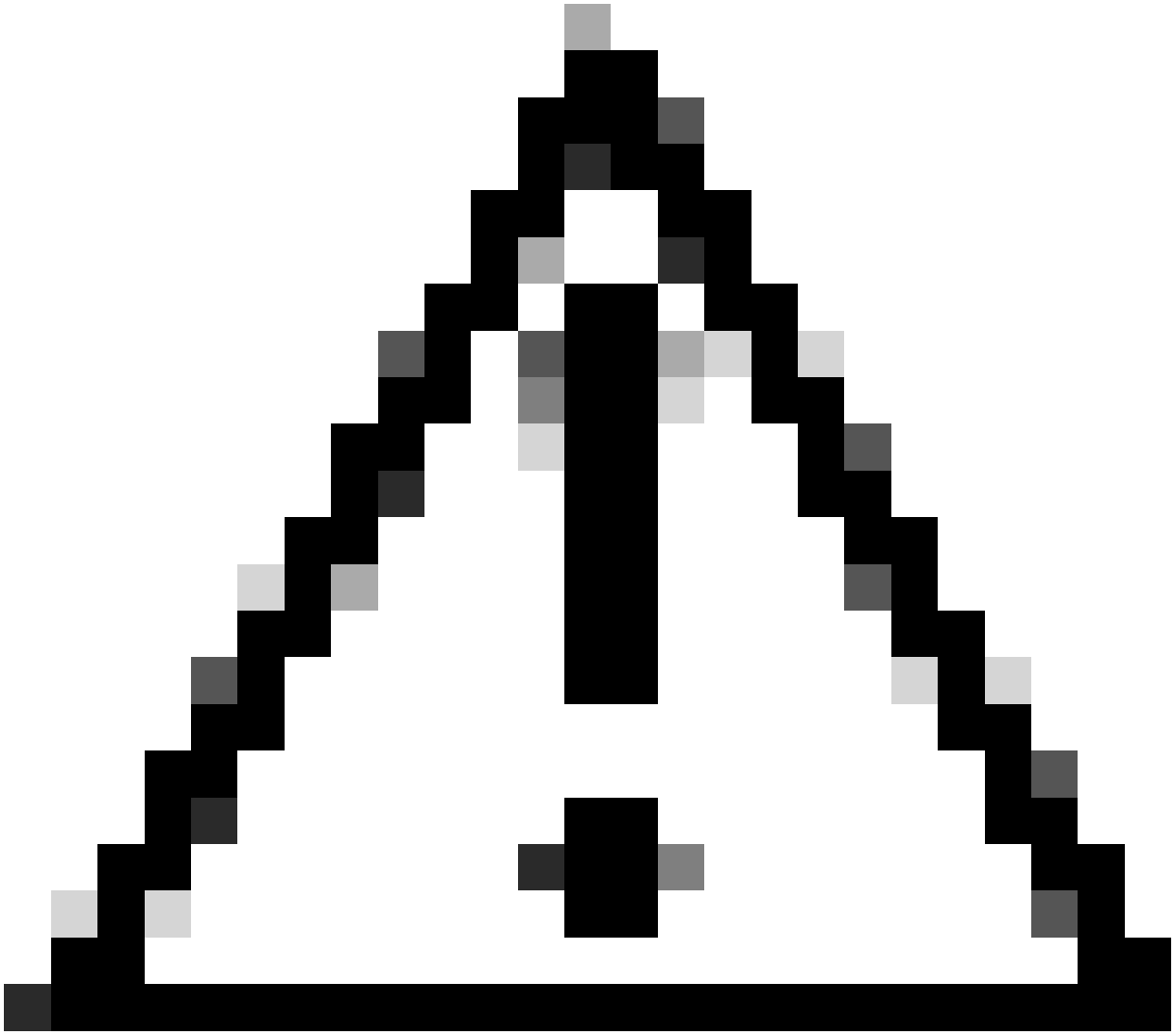
Stap 1. Maak een client trustpoint aan.

```
cat9k(config)#crypto pki trustpoint svs_cat9k_25jun17
cat9k(ca-trustpoint)#revocation-check none
```

Stap 2. Kopieer het PKCS#12-bestand naar bootflash.



Opmerking: Zorg ervoor dat het PKCS#12-bestand de volledige certificaatketen en de privésleutel als gecodeerd bestand bevat.



Let op: sleutels in de geïmporteerde PKCS#12 moeten van het RSA-type zijn (bijv.: RSA 2048), niet ECC.

<#root>

cat9k#

copy sftp bootflash: vrf Mgmt-vrf

```
Address or name of remote host [10.225.253.247]?
Source username [svs-user]?
Source filename [cat9k.svs.lab.pfx]? /home/svs-user/upload/cat9k-25jun17.pfx
Destination filename [cat9k-25jun17.pfx]?
Password:
!
2960 bytes copied in 3.022 secs (979 bytes/sec)
```

Stap 3. Importeer het PKCS#12-bestand met de opdracht importeren.

<#root>

```
cat9k#

crypto pki import svs_cat9k_25jun17 pkcs12 bootflash:cat9k-25jun17.pfx

 password C1sco.123
% Importing pkcs12...Reading file from bootflash:cat9k-25jun17.pfx
CRYPTO_PKI: Imported PKCS12 file successfully.
cat9k#

cat9k#

show crypto pki certificates svs_cat9k_25jun17


Certificate
  Status: Available
  Certificate Serial Number (hex): 586OBF33A2O33365
  Certificate Usage: General Purpose
  Issuer:
    cn=SVS LabCA
    ou=SVS
    o=Cisco
    l=Raleigh
    st=North Carolina
    c=US
  Subject:
    Name: cat9k.svs.lab
    e=pkalkur@cisco.com
    cn=cat9k.svs.lab
    ou=svs
    o=cisco
    l=rtp
    st=nc
    c=us
  Validity Date:
    start date: 17:56:00 UTC Jun 17 2025
    end   date: 17:56:00 UTC Jun 17 2026
  Associated Trustpoints: svs_cat9k_25jun17

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 2OCD74O2C4DA37F5
  Certificate Usage: General Purpose
  Issuer:
    cn=SVS LabCA
    ou=SVS
    o=Cisco
    l=Raleigh
    st=North Carolina
    c=US
  Subject:
    cn=SVS LabCA
    ou=SVS
    o=Cisco
    l=Raleigh
    st=North Carolina
    c=US
  Validity Date:
    start date: 17:05:00 UTC Apr 28 2025
    end   date: 17:05:00 UTC Apr 28 2035
  Associated Trustpoints: svs_cat9k_25jun17 svs_cat9k
```

```
  Storage: nvram:SVSLabCA#37F5CA.cer
```

TACACS & AAA met TLS-configuratie

Stap 1. Maak TACACS-server- en AAA-groepen, koppel het vertrouwenspunt van de client (router).

```
tacacs server svs_tacacs
 address ipv4 10.225.253.209
 single-connection
 tls port 6049
 tls idle-timeout 60
 tls connection-timeout 60
 tls trustpoint client svs_cat9k
 tls ip tacacs source-interface GigabitEthernet0/0
 tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ svs_tls
 server name svs_tacacs
 ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

Stap 2. AAA-methoden configureren.

```
aaa authentication login default group svs_tls local enable
aaa authentication login console local enable
aaa authentication enable default group svs_tls enable
aaa authorization config-commands
aaa authorization exec default group svs_tls local if-authenticated
aaa authorization commands 1 default group svs_tls local if-authenticated
aaa authorization commands 15 default group svs_tls
aaa accounting exec default start-stop group svs_tls
aaa accounting commands 1 default start-stop group svs_tls
aaa accounting commands 15 default start-stop group svs_tls
aaa session-id common
```

Verificatie

De configuratie verifiëren.

```
show tacacs
show crypto pki certificates <>
show crypto pki trustpoints <>
```

Debug voor AAA en TACACS+.

```
debug aaa authentication
debug aaa authorization
debug aaa accounting
debug aaa subsys
debug aaa protocol local
debug tacacs authentication
debug tacacs authorization
debug tacacs accounting
debug tacacs events
debug tacacs packet
debug tacacs
debug tacacs secure

! Below debugs will be needed only if there is any issue with SSL Handshake
debug ip tcp transactions
debug ip tcp packet
debug crypto pki transactions
debug crypto pki API
debug crypto pki messages
debug crypto pki server
debug ssl openssl errors
debug ssl openssl msg
debug ssl openssl states
clear logging
```

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.