TACACS+ configureren via TLS 1.3 op een Nexus-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 NX-OS-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

In deze handleiding worden de activiteiten in twee delen verdeeld zodat ISE de beheerderstoegang voor netwerkapparaten met Cisco NX-OS kan beheren.
· Deel 1 – Configureer ISE voor Apparaatbeheer
· Deel 2 – Cisco NX-OS configureren voor TACACS+ via TLS

Voorwaarden

Vereisten

Voorwaarden 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 onderstaande software- en hardware-versies:

- ISE VMware virtual appliance, release 3.4 patch 2.
- Nexus 9000 switch model C9364D-GX2A, Cisco NX-OS versie 10.5(3t).

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.

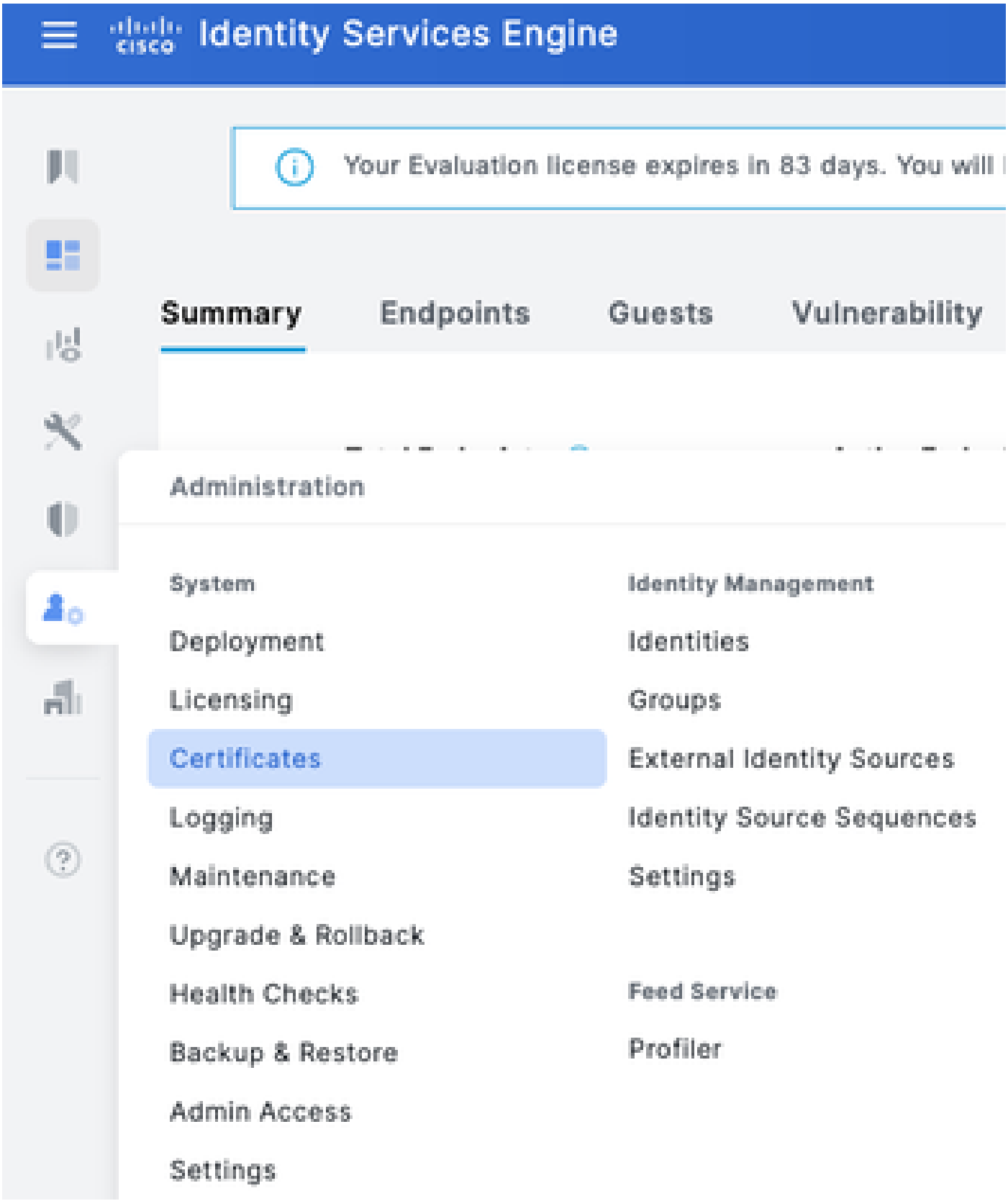
ISE configureren voor Apparaatbeheer

Aanvraag voor certificaatondertekening genereren voor TACACS+-serververificatie

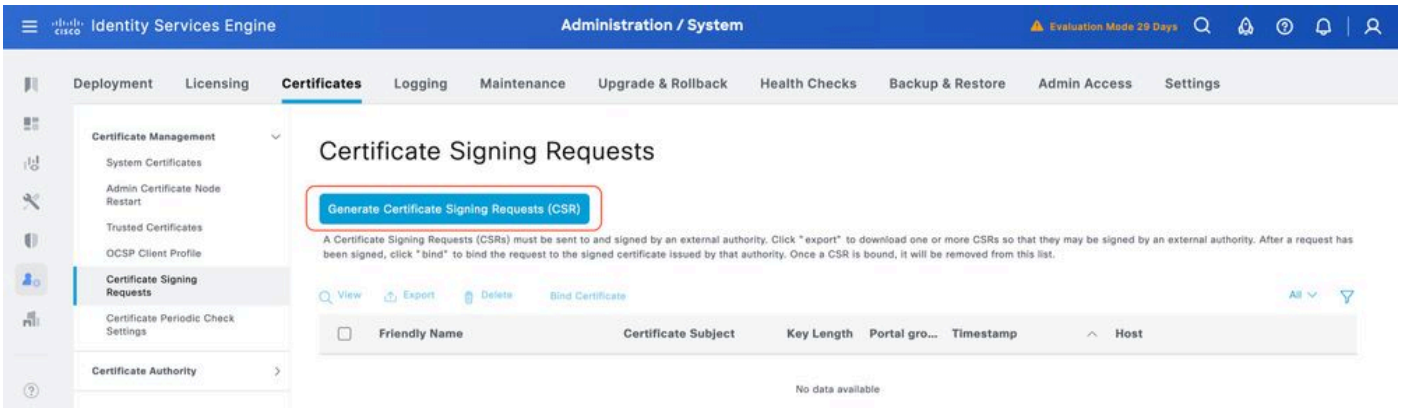
Stap 1. Meld u aan bij de ISE-beheerdersportal met een van de ondersteunde browsers.

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.

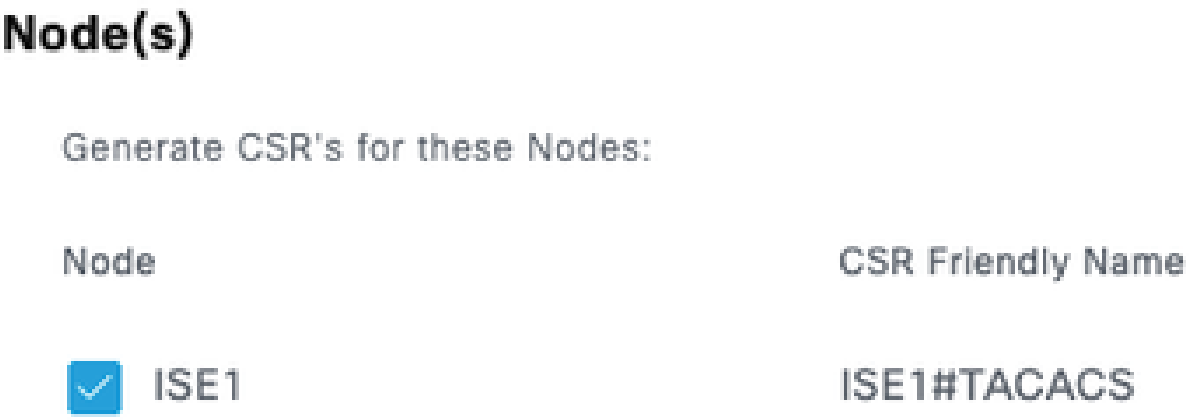


Stap 3. Klik onder Certificaatondertekeningsverzoeken op Certificaatondertekeningsverzoek genereren.

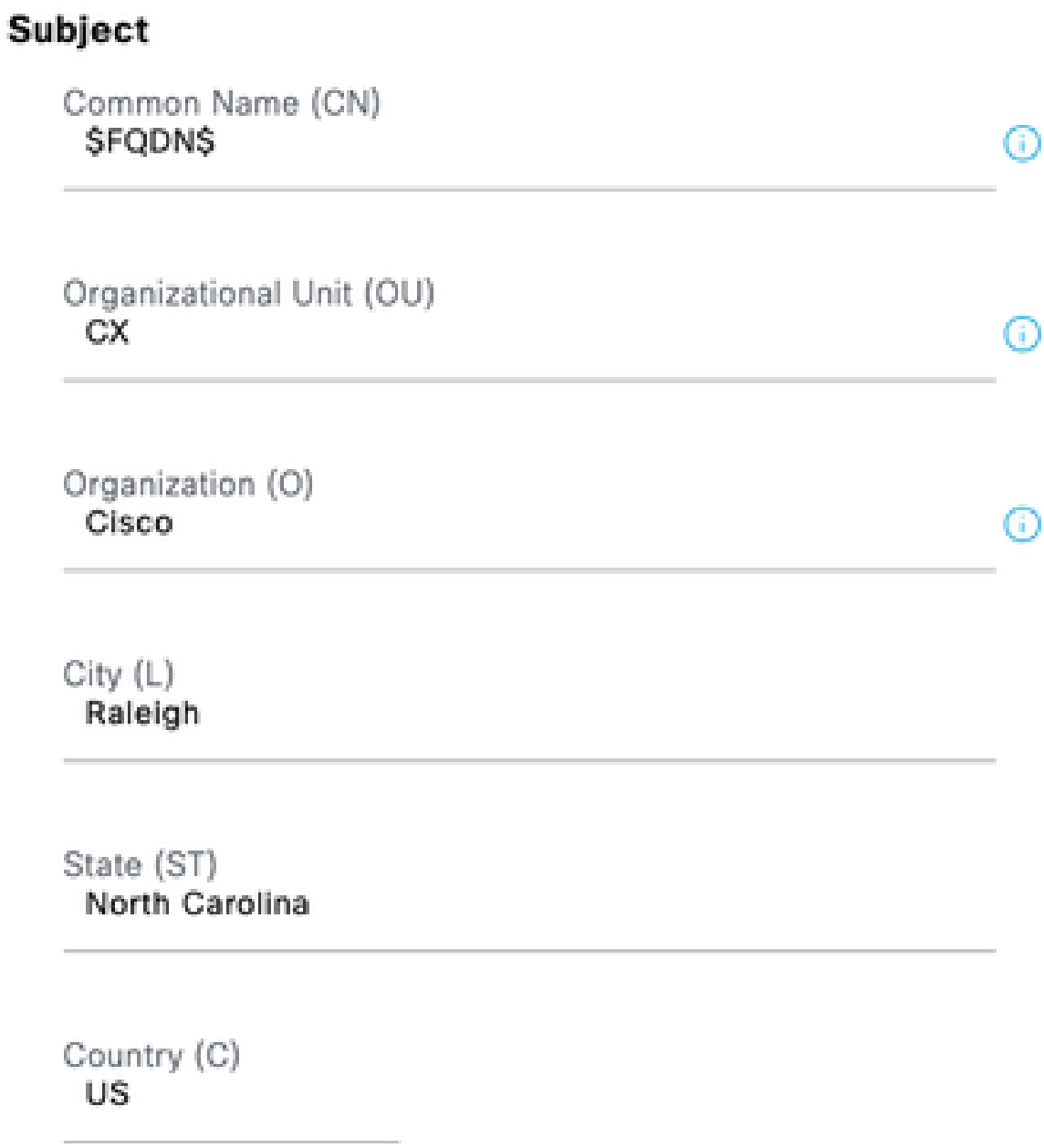


Stap 4. Selecteer TACACS in Gebruik.

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



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



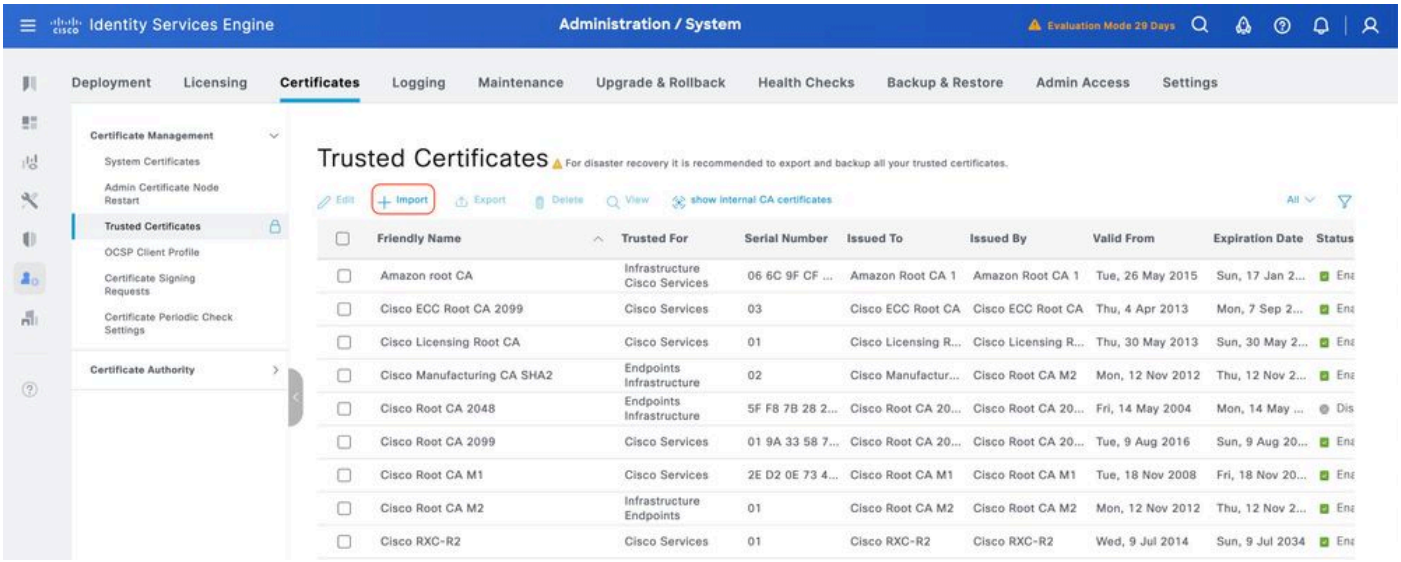
Stap 7. Voeg de DNS-naam en het IP-adres toe onder Alternatieve onderwerpnaam (SAN).

Stap 8. Klik op Genereren en vervolgens op Exporteren.

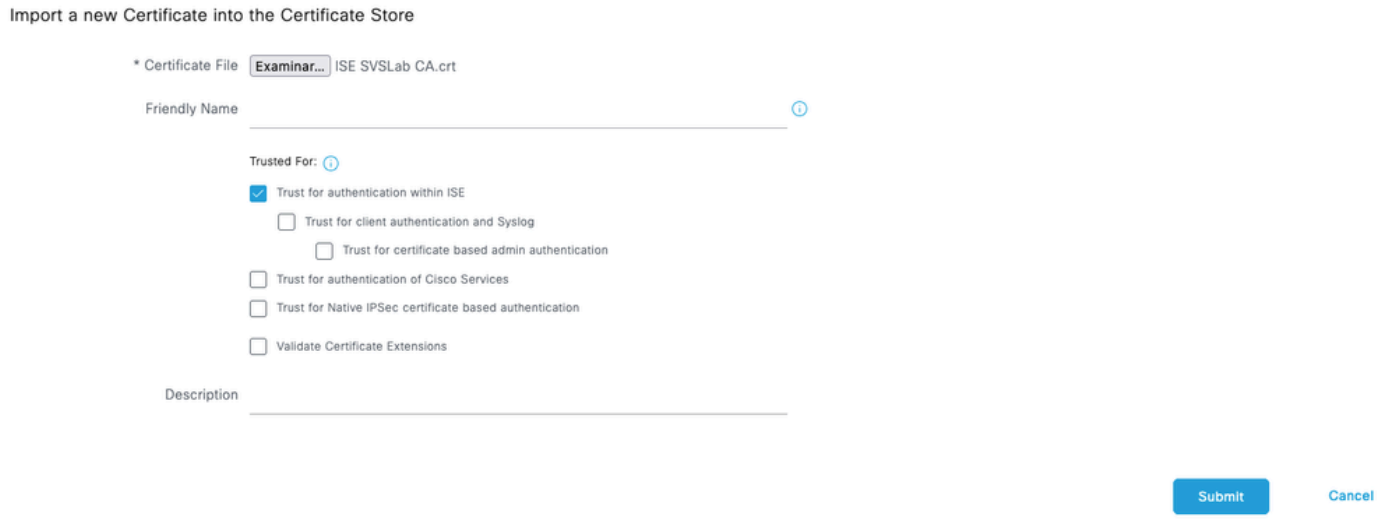
Nu kunt u het certificaat (CRT) laten ondertekenen door uw Certificate Authority (CA).

Root CA-certificaat uploaden voor TACACS+-serververificatie

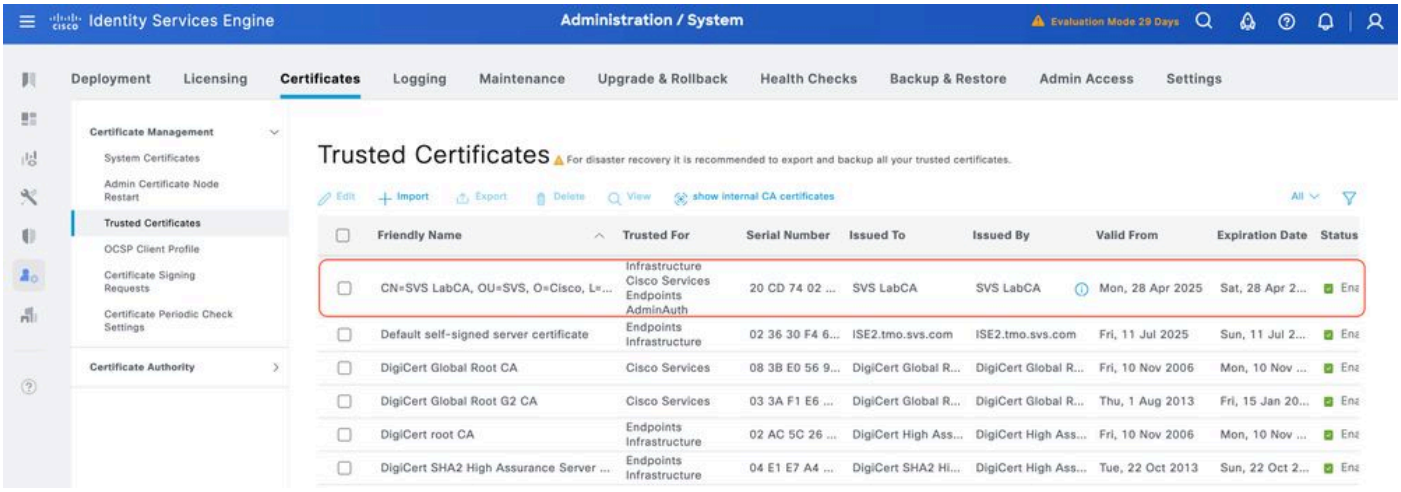
Stap 1. Ga naar Beheer > Systeem > Certificaten. Klik onder Vertrouwde certificaten op Importeren.



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



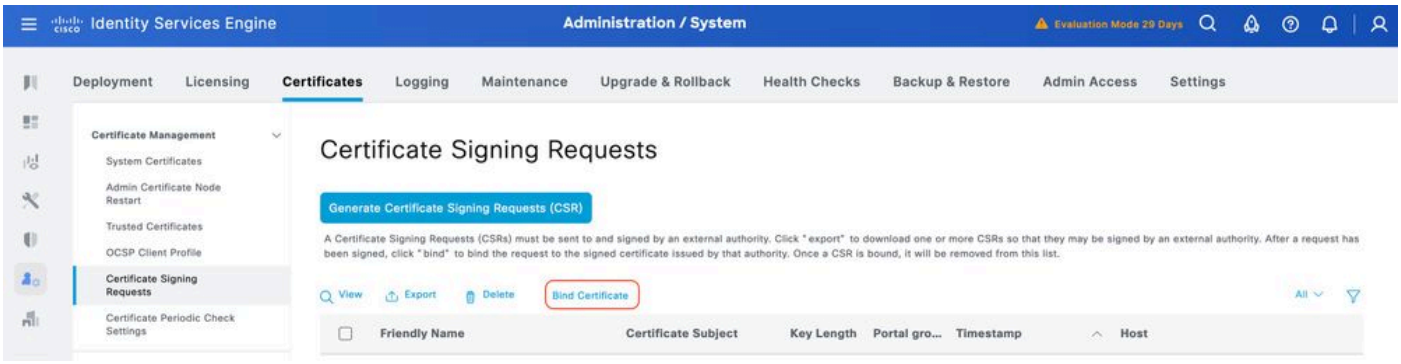
Klik op Indienen. Het certificaat moet nu worden weergegeven onder Vertrouwde certificaten.



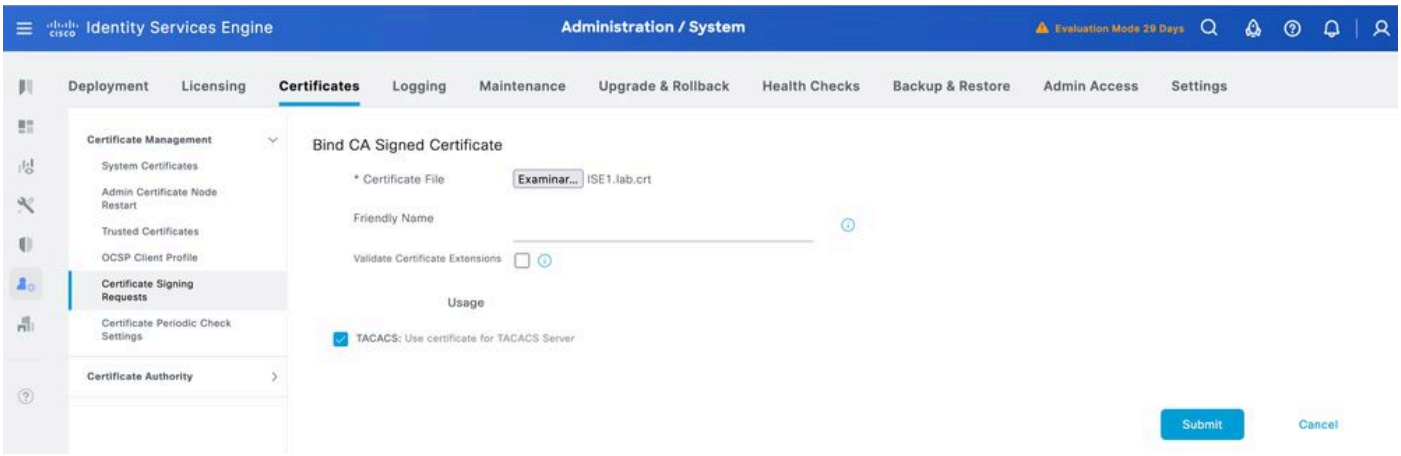
Het ondertekende certificaatondertekeningsverzoek (CSR) binden aan ISE

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

Stap 1. Ga naar Beheer > Systeem > Certificaten. Selecteer onder Certificaatondertekeningsverzoeken de TACACS-CSR die in de vorige stap is gegenereerd en klik op Certificaat binden.

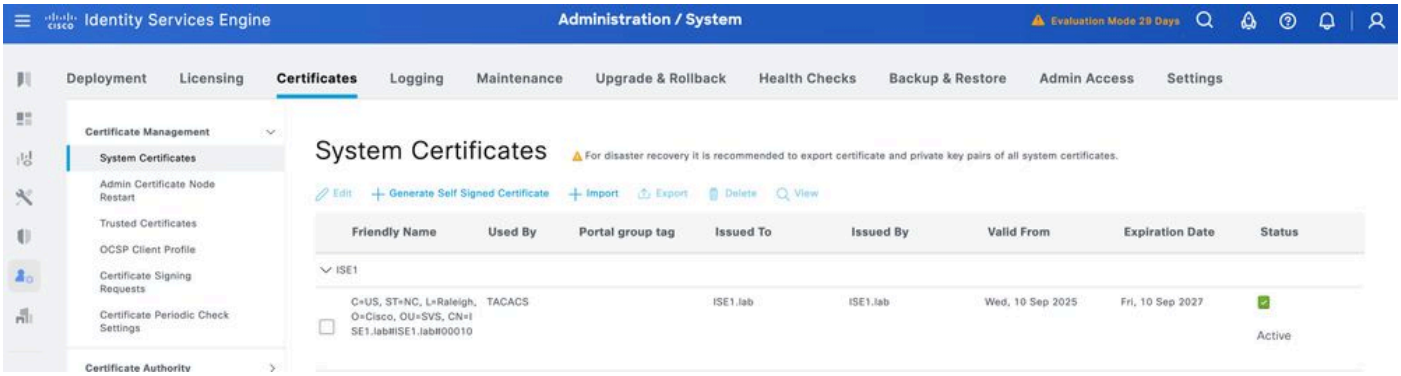


Stap 2. Selecteer het ondertekende certificaat en zorg ervoor dat het selectievakje TACACS onder Gebruik geselecteerd blijft.



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.

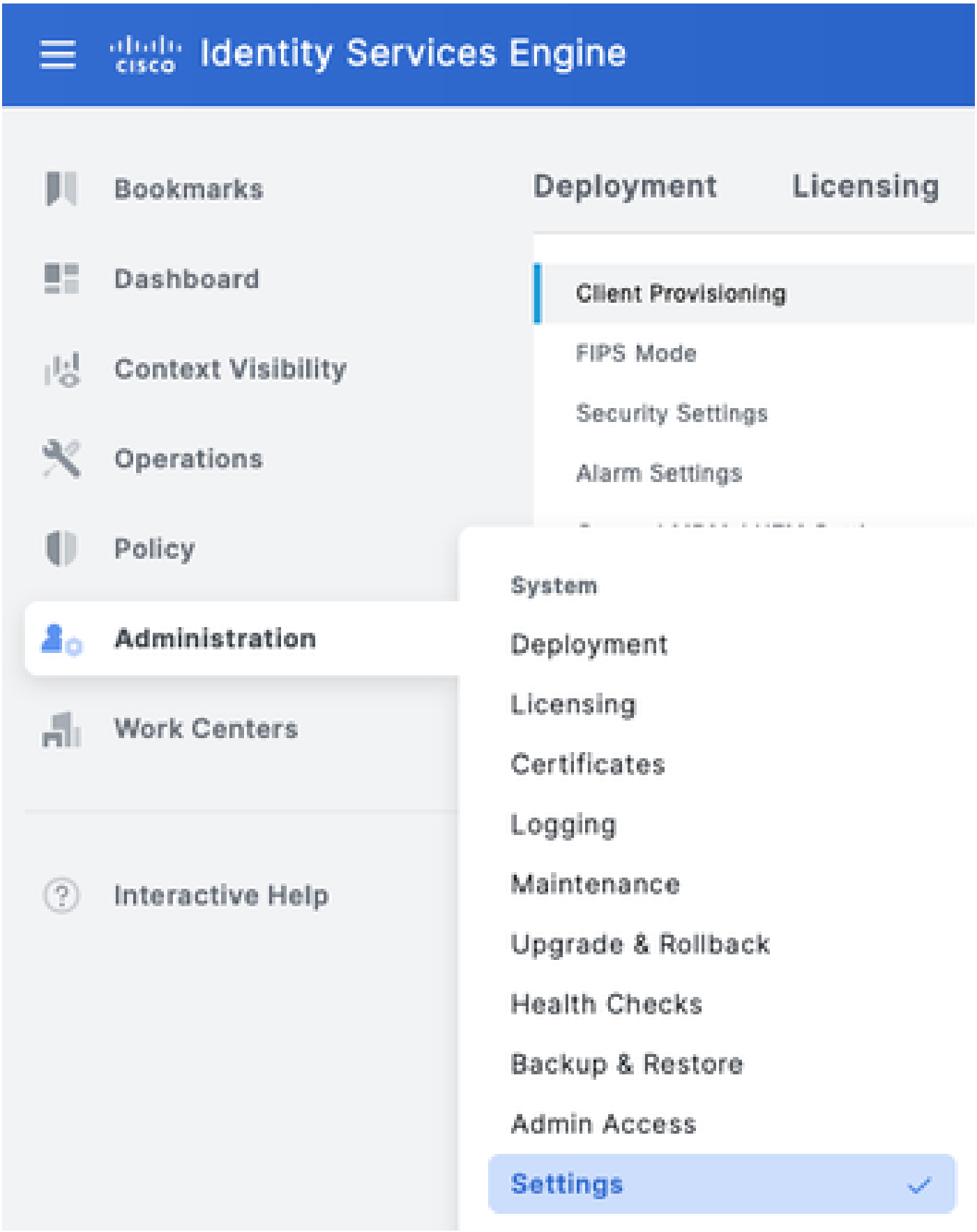
Het certificaat moet nu correct worden geïnstalleerd. U kunt dit controleren onder Systeemcertificaten.



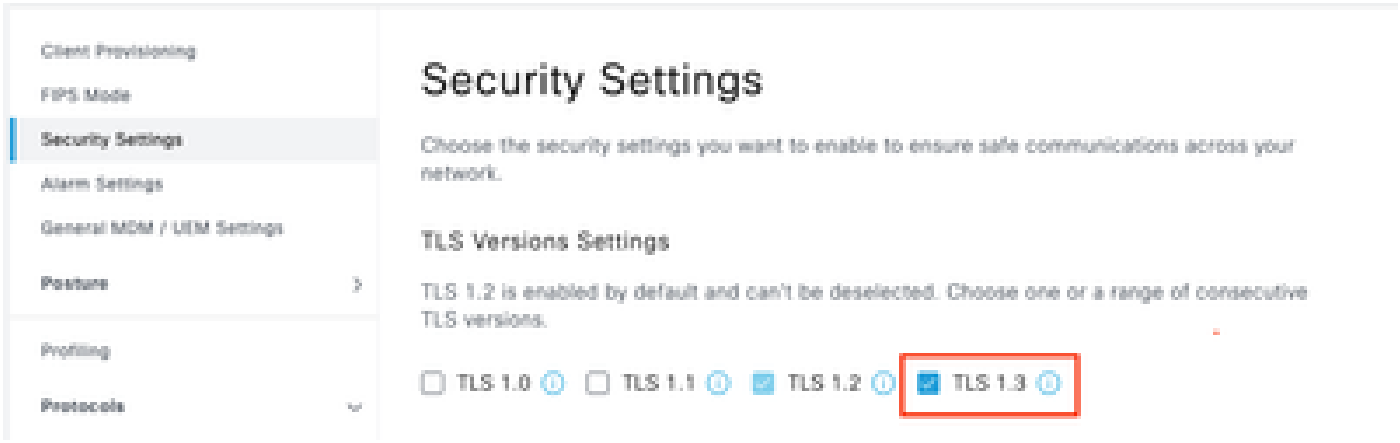
TLS 1.3 inschakelen

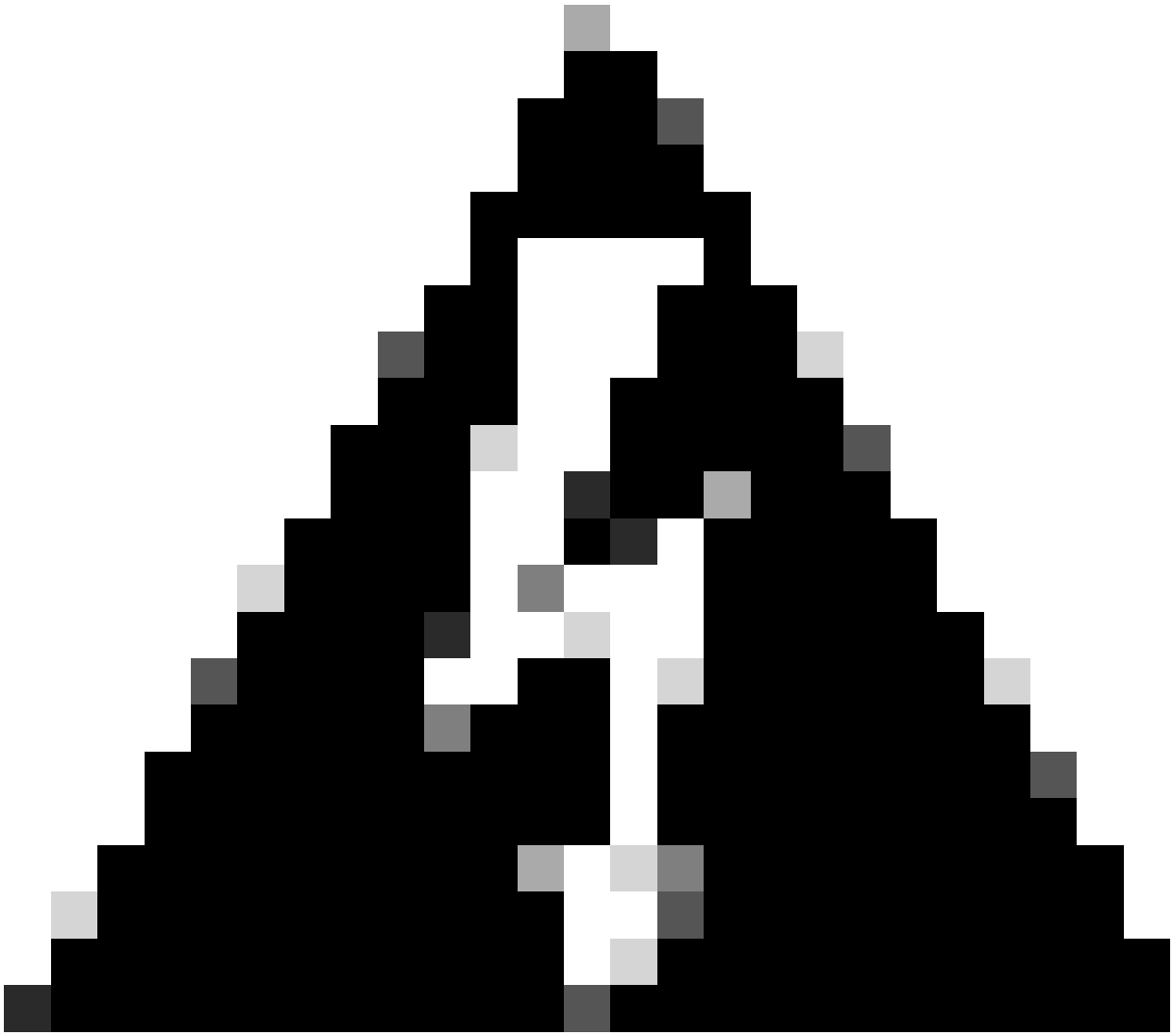
TLS 1.3 is standaard niet ingeschakeld in ISE 3.4.x. Het moet handmatig worden ingeschakeld.

Stap 1. Ga naar Beheer > Systeem > Instellingen.



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



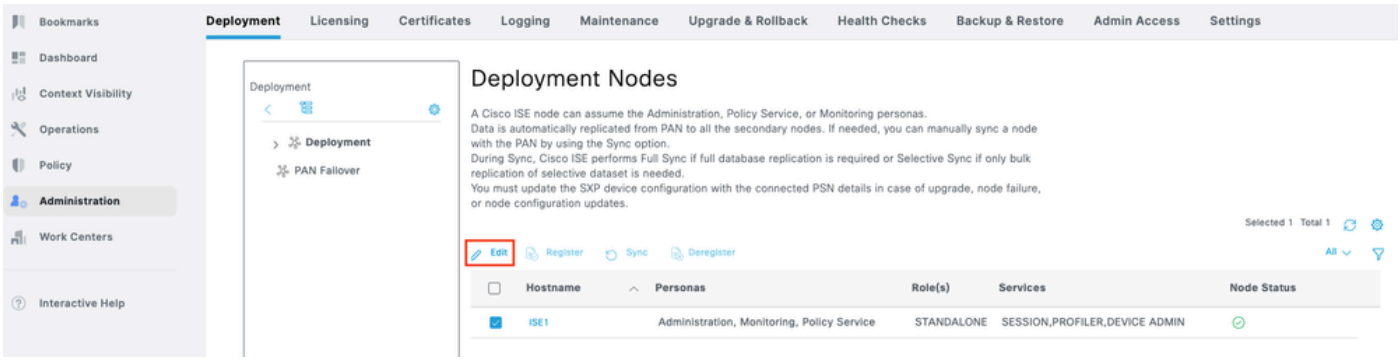


Waarschuwing: wanneer u de TLS-versie wijzigt, wordt de Cisco ISE-toepassingsserver opnieuw gestart op alle Cisco ISE-implementatiemachines.

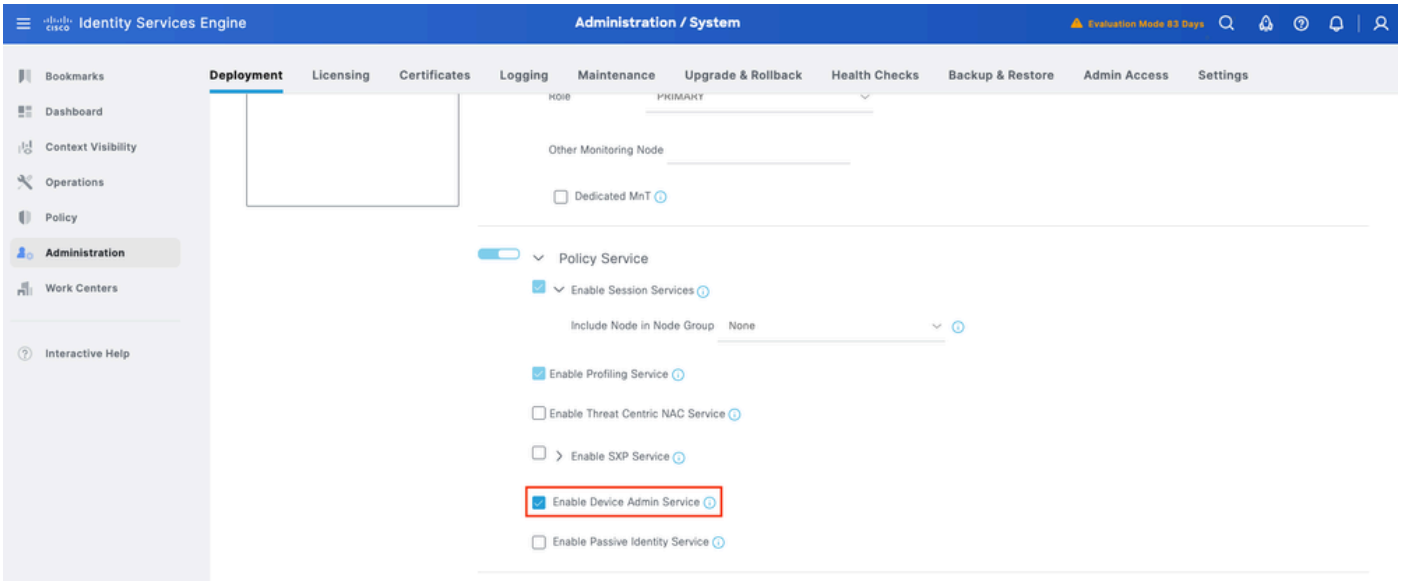
Apparaatbeheer inschakelen op ISE

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

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



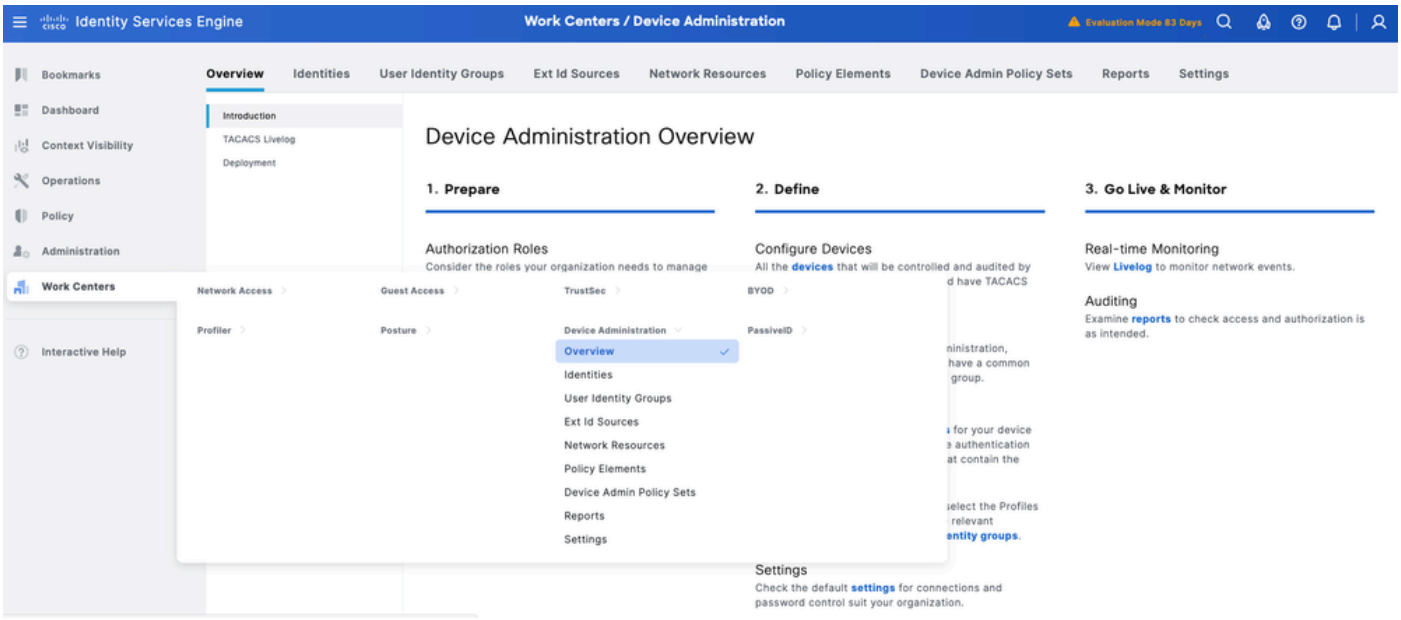
Stap 2. Blader onder Algemene instellingen omlaag en selecteer het selectievakje naast Apparaatbeheerservice inschakelen.



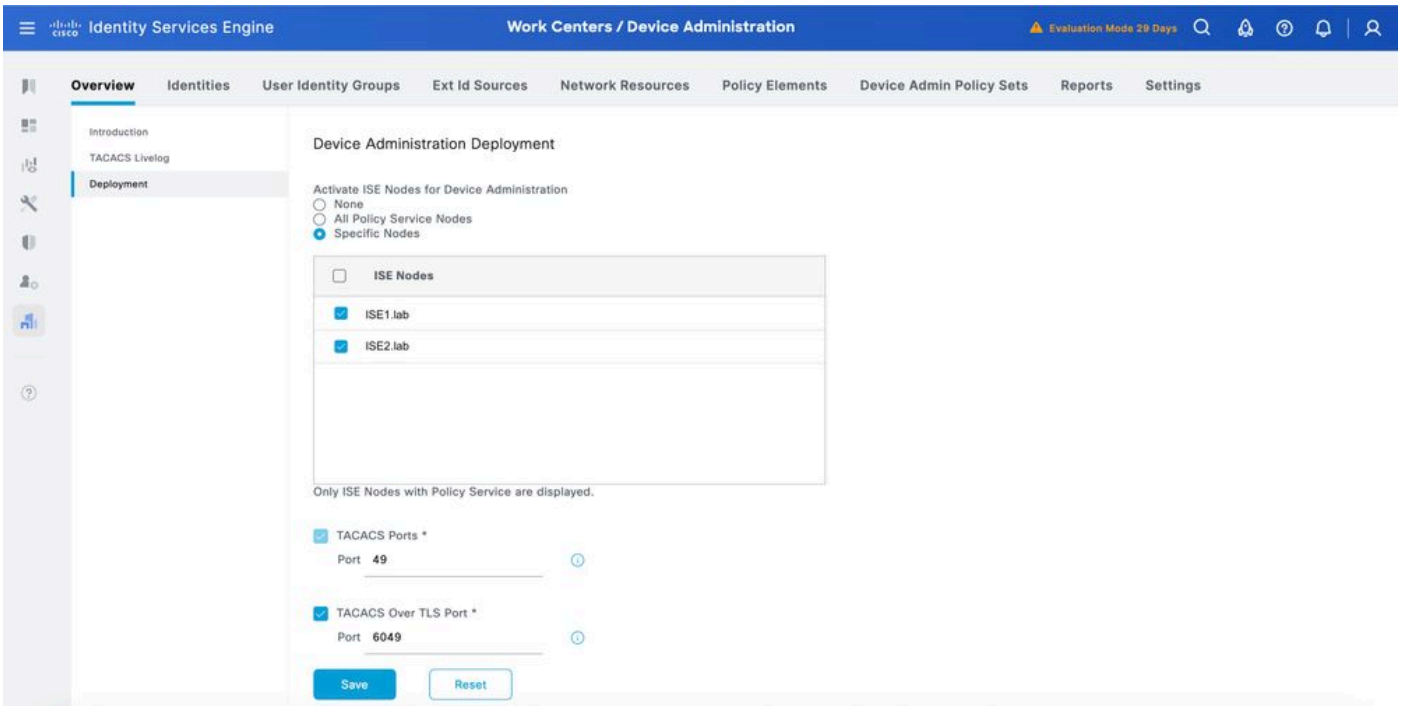
Stap 3. Sla de configuratie op. Device Admin Service is nu ingeschakeld op ISE.

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.

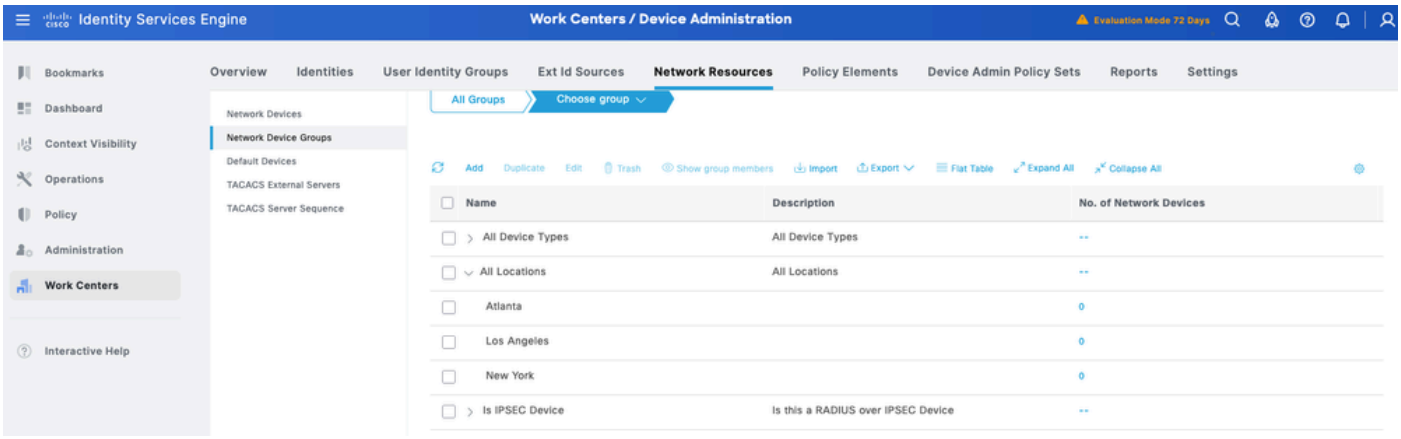


Stap 3. Behoud de standaardpoort 6049 of geef een andere TCP-poort op voor TACACS via TLS en klik vervolgens op Opslaan.

Groepen netwerkapparaten en netwerkapparaten

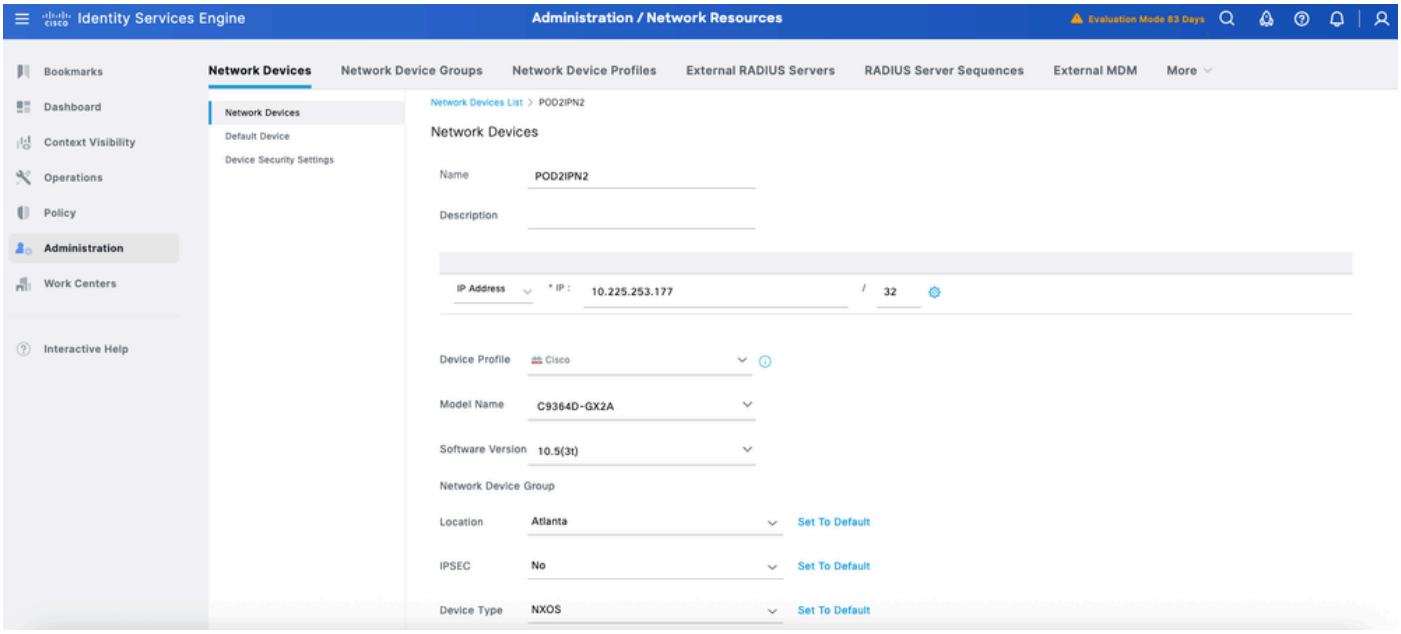
ISE biedt krachtige apparaatgroepering met meerdere apparaatgroephiërarchieën. Elke hiërarchie vertegenwoordigt een afzonderlijke en onafhankelijke classificatie van netwerkapparaten.

Stap 1. Navigeer naar Werkcentra > Apparaatbeheer > Netwerkbron. Klik op Netwerkapparaatgroepen.

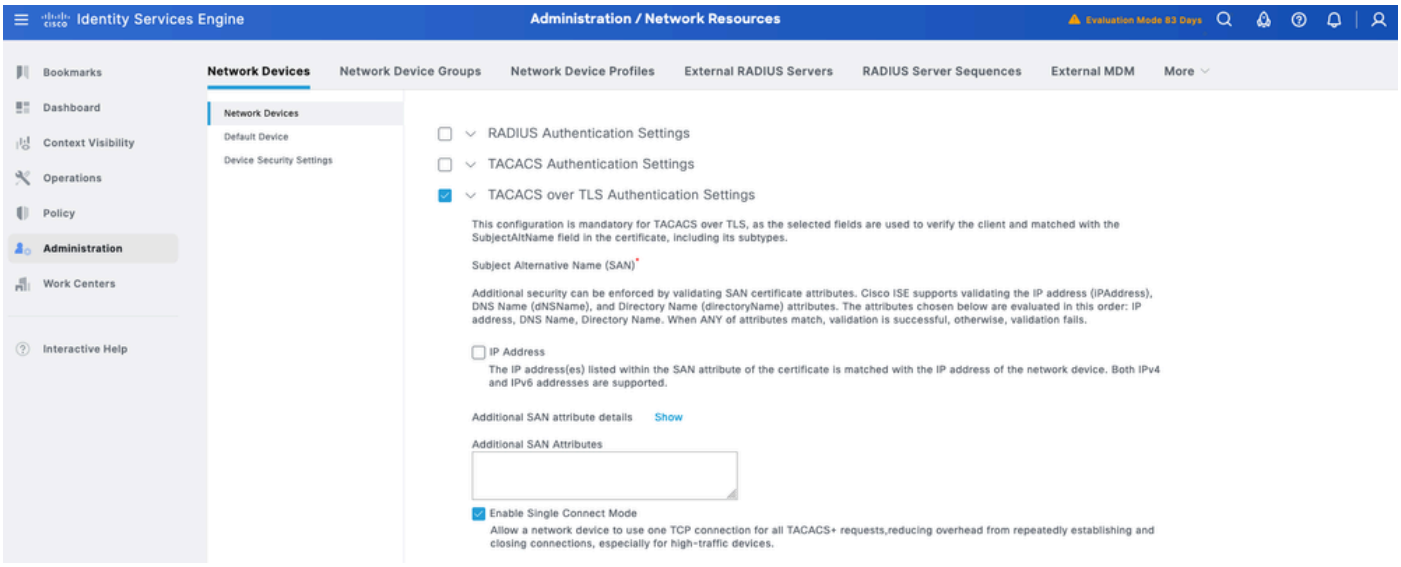


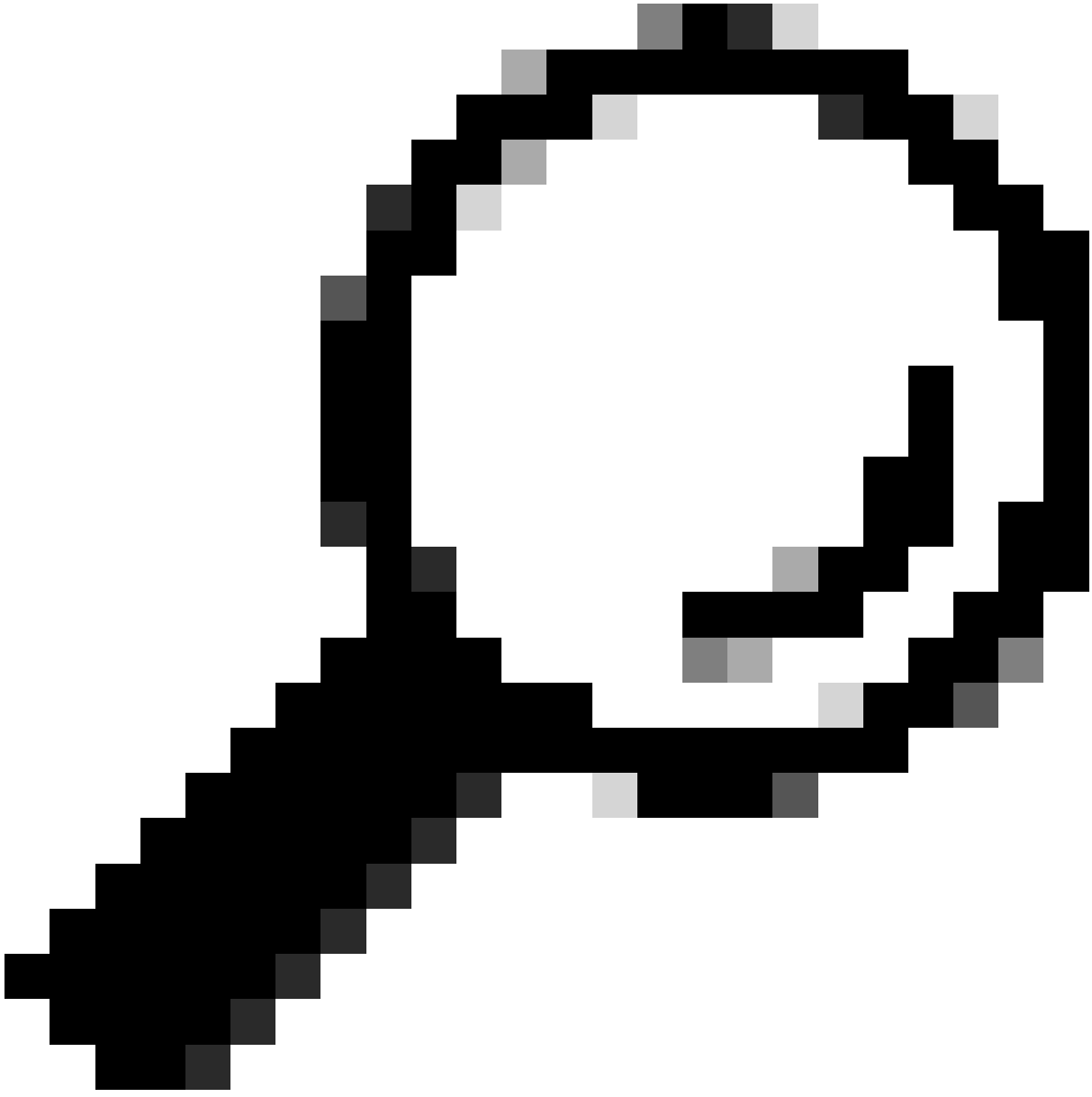
Alle apparaattypen en alle locaties zijn standaardhiërarchieën die door ISE worden aangeboden. U voegt uw eigen hiërarchieën toe en definieert de verschillende componenten bij het identificeren van een netwerkapparaat dat later in de beleidsvoorwaarde kan worden gebruikt.

Stap 2. Voeg nu een NS-OX-apparaat toe als netwerkapparaat. Navigeer naar Werkcentra > Apparaatbeheer > Netwerkbronnen. Klik op Toevoegen om een nieuw netwerkapparaat POD2IPN2 toe te voegen.



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


Identity Services Engine
Administration / Network Resources
Evaluation Mode 83 Days
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Help
Network Devices
Network Device Groups
Network Device Profiles
External RADIUS Servers
RADIUS Server Sequences
External MDM
More
Network Devices
Default Device
Device Security Settings
RADIUS Authentication Settings
TACACS Authentication Settings
TACACS over TLS Authentication Settings
This configuration is mandatory for TACACS over TLS, as the selected fields are used to verify the client and matched with the SubjectAltName field in the certificate, including its subtypes.
Subject Alternative Name (SAN)*
Additional security can be enforced by validating SAN certificate attributes. Cisco ISE supports validating the IP address (IPAddress), DNS Name (dNSName), and Directory Name (directoryName) attributes. The attributes chosen below are evaluated in this order: IP address, DNS Name, Directory Name. When ANY of attributes match, validation is successful, otherwise, validation fails.
IP Address
The IP address(es) listed within the SAN attribute of the certificate is matched with the IP address of the network device. Both IPv4 and IPv6 addresses are supported.
Additional SAN attribute details
Show
Additional SAN Attributes
Enable Single Connect Mode
Allow a network device to use one TCP connection for all TACACS+ requests,reducing overhead from repeatedly establishing and closing connections, especially for high-traffic devices.

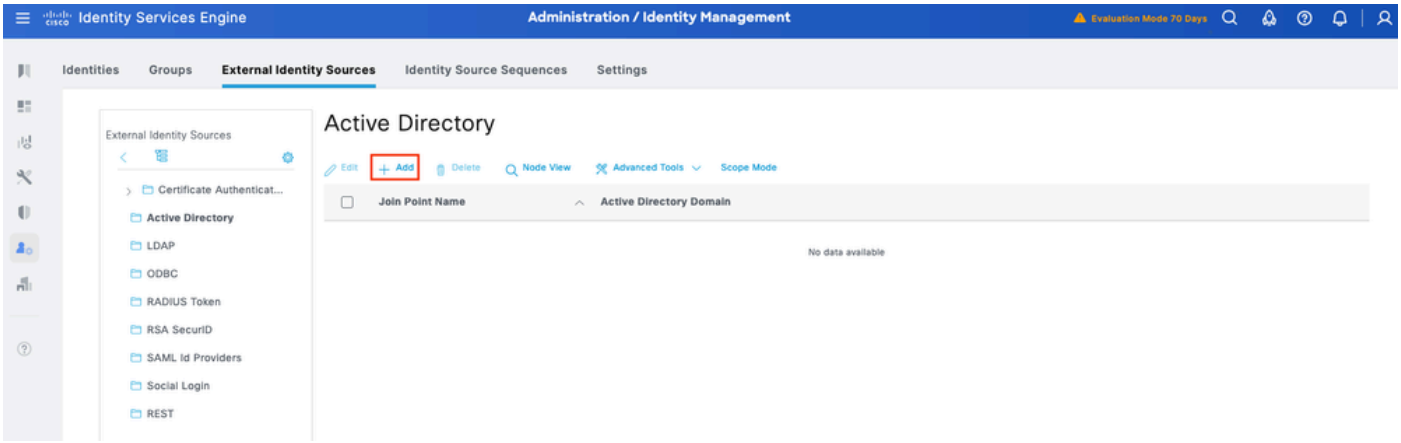


Tip: Het wordt aanbevolen om de modus Single Connect in te schakelen om te voorkomen dat de TCP-sessie opnieuw wordt gestart telkens wanneer een opdracht naar het apparaat wordt verzonden.

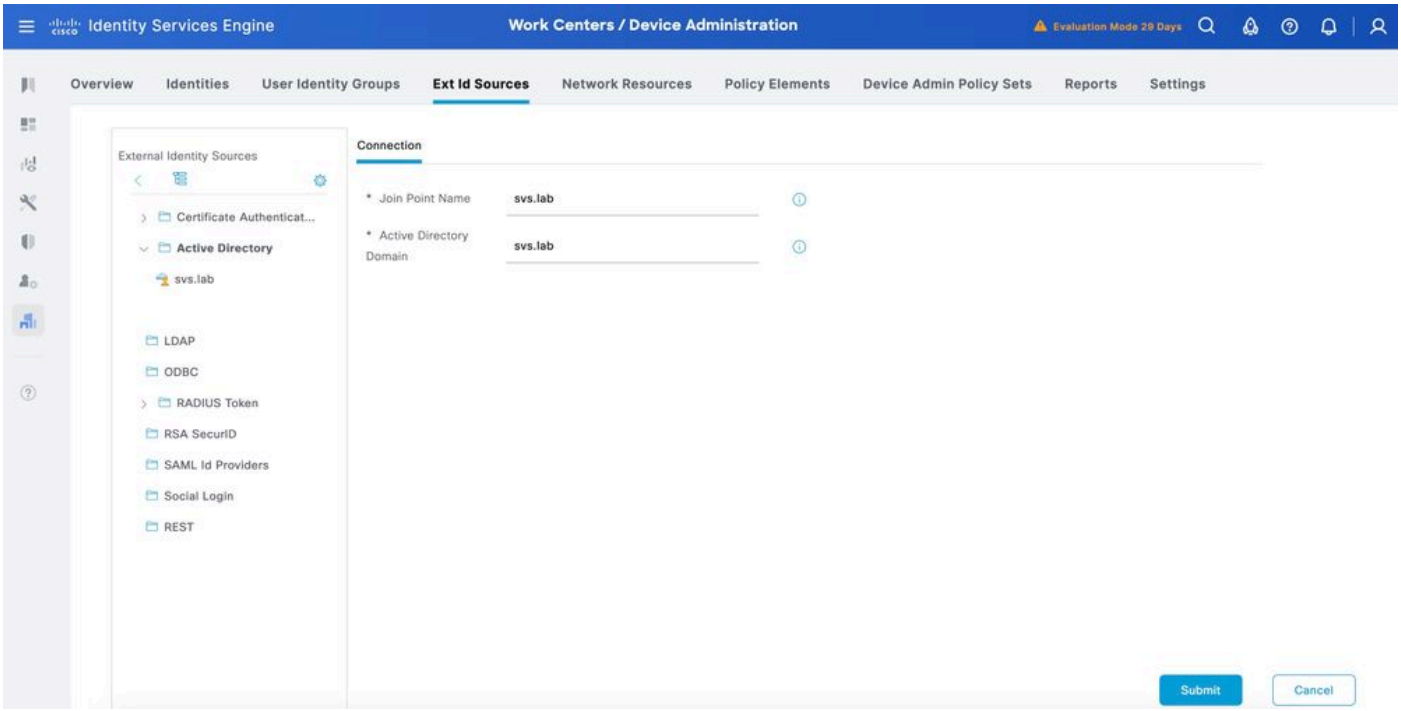
Identiteitswinkels configureren

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.

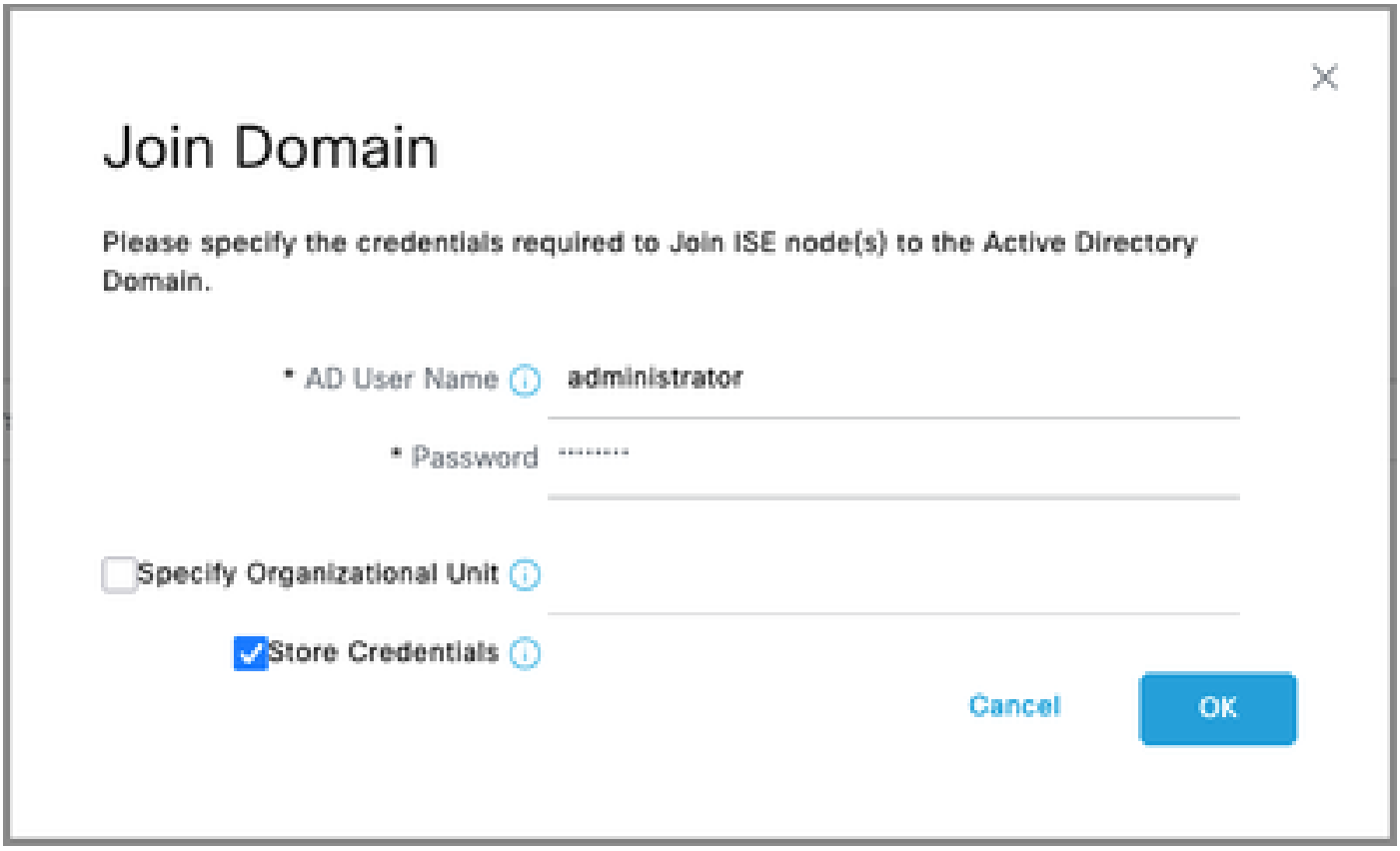


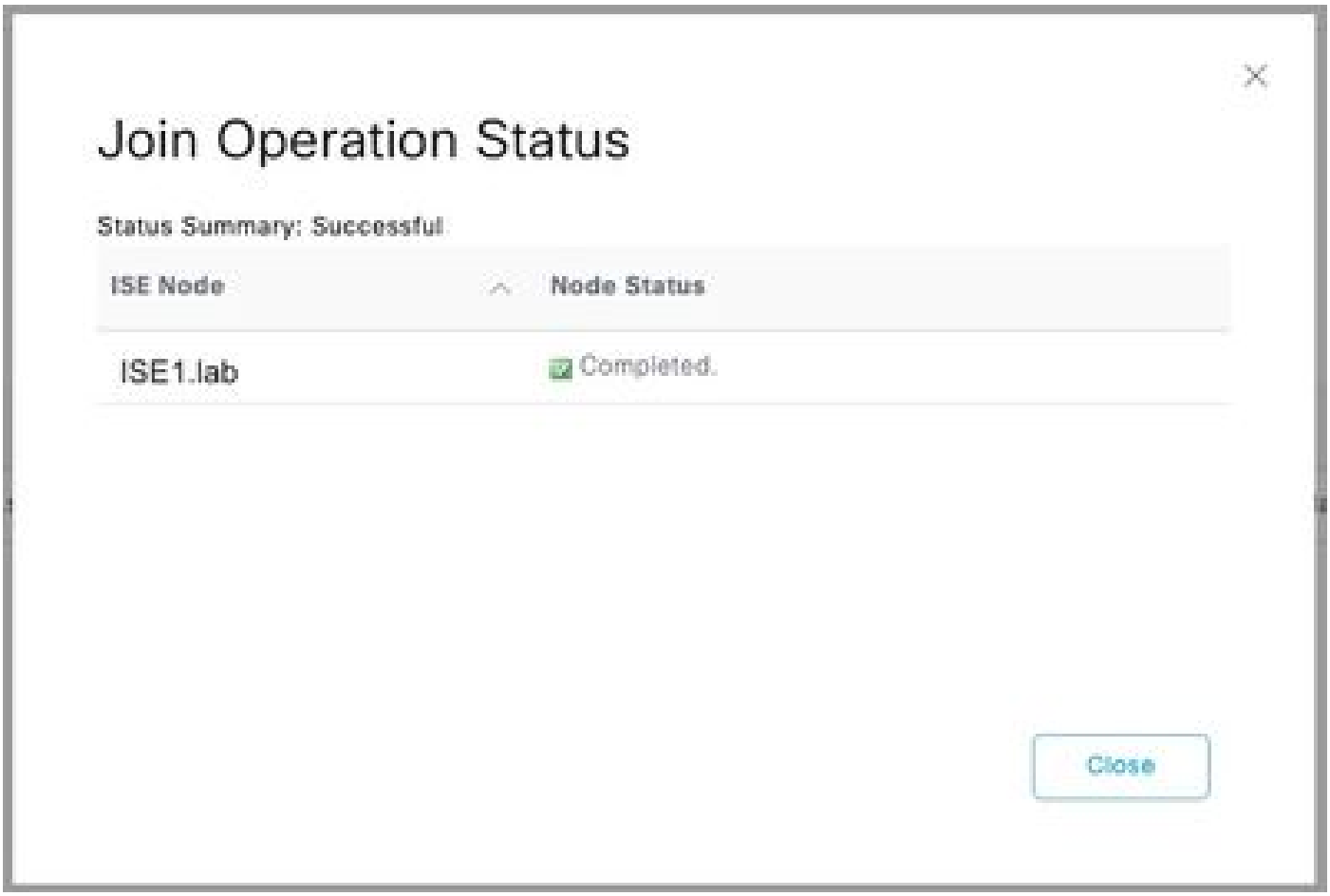
Stap 2. Geef de naam van het aanmeldpunt en de AD-domeinnaam op en klik op Indienen.



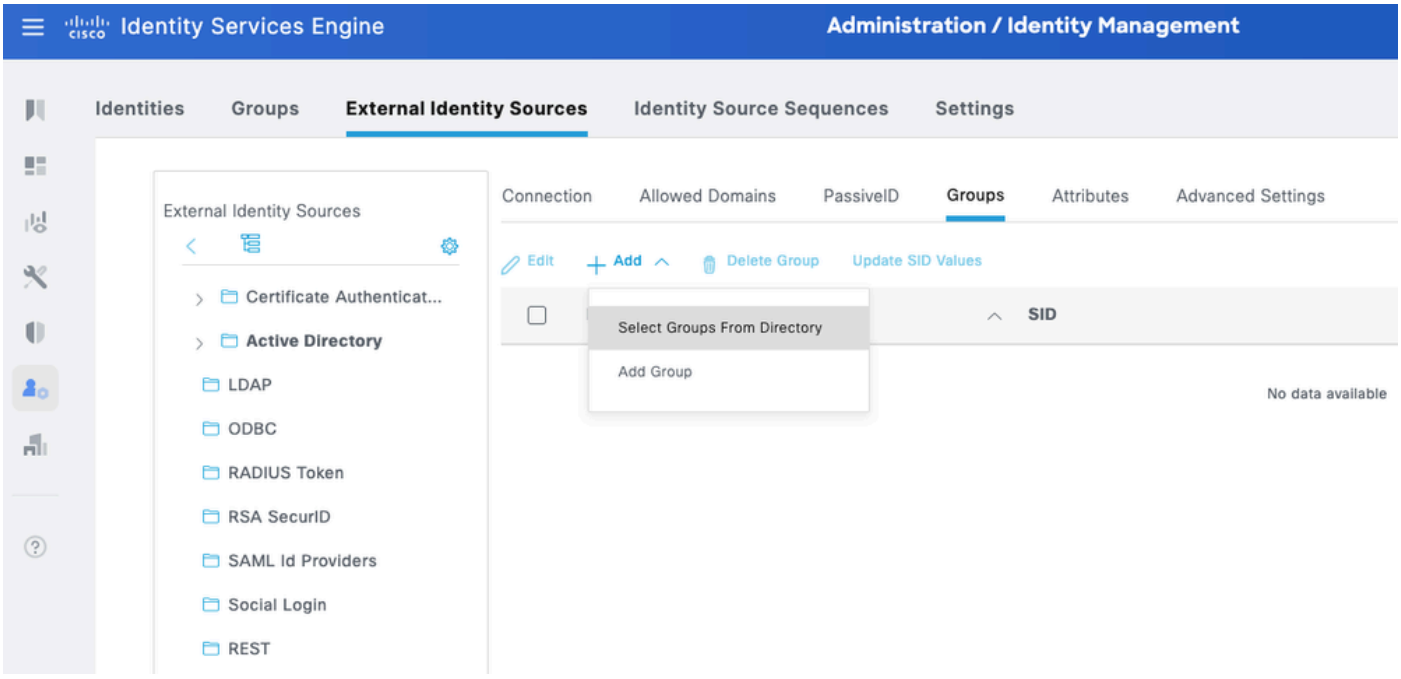
Stap 3. Klik op Ja wanneer u wordt gevraagd "Wilt u alle ISE-knooppunten aan dit Active Directory-domein toevoegen?"

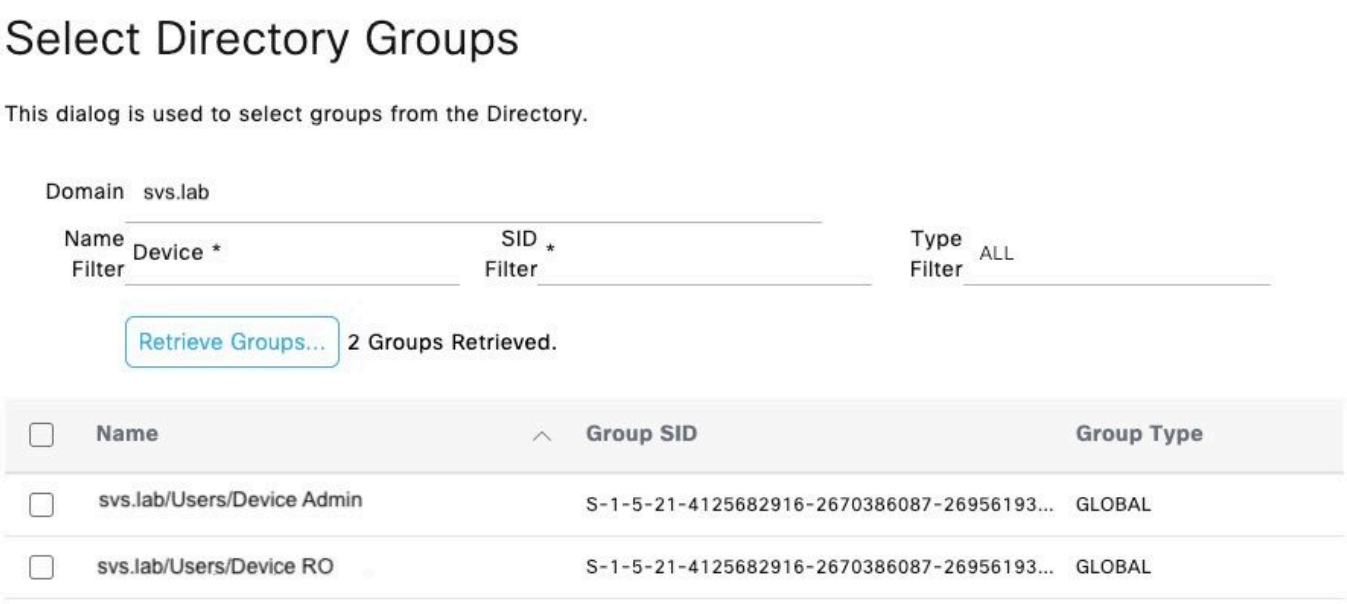
Stap 4. Voer de referenties in met AD join-bevoegdheden en voeg ISE toe aan AD. Controleer de status om te controleren of deze operationeel is.

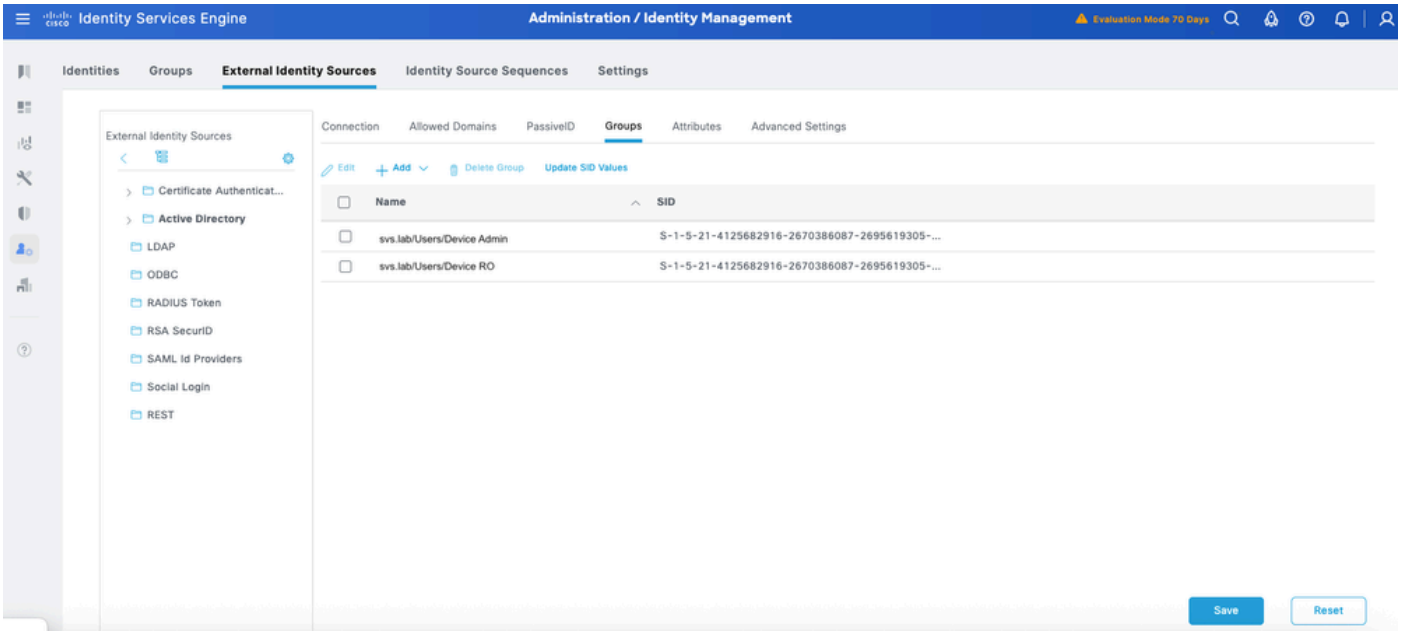




Stap 5. Navigeer naar het tabblad Groepen en klik op Toevoegen om alle benodigde groepen te krijgen op basis waarvan de gebruikers zijn geautoriseerd voor toegang tot het apparaat. In dit voorbeeld worden de groepen weergegeven die worden gebruikt in het machtigingsbeleid in deze handleiding.







TACACS+ Shell-profielen configureren

In tegenstelling tot Cisco IOS-apparaten, die gebruik maken van privilege levels voor autorisatie, Cisco NX-OS-apparaten implementeren role-based access control (RBAC). In ISE kunt u TACACS+-profielen toewijzen aan gebruikersrollen op Cisco NX-OS-apparaten met behulp van gemeenschappelijke taken van het Nexus-type.

De vooraf gedefinieerde rollen op NX-OS-apparaten verschillen tussen NX-OS-platforms. Twee gemeenschappelijke zijn:

- netwerkbeheerder – Vooraf gedefinieerde netwerkbeheerdersrol heeft volledige lees- en schrijftoegang tot alle opdrachten op de switch; alleen beschikbaar in de standaard Virtual Device Context (VDC) als de apparaten (bijvoorbeeld Nexus 7000) meerdere VDC's hebben. Gebruik de NX-OS CLI-opdracht cli-syntaxisrollen weergeven network-admin om de

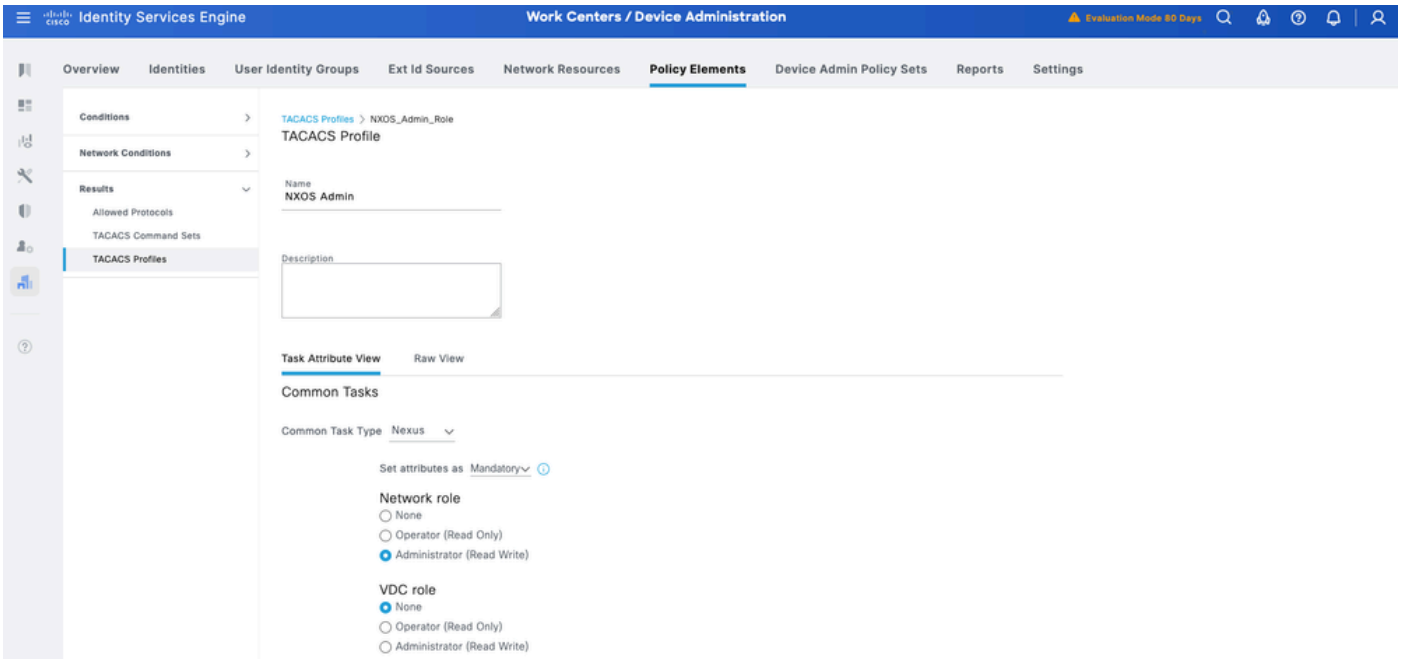
volledige lijst met opdrachten te zien die beschikbaar is voor deze rol.
- netwerkoperator – voorgedefinieerde netwerkbeheerdersrol heeft volledige leestoegang tot alle opdrachten op de switch; alleen beschikbaar in de standaard VDC als de toestellen (bijvoorbeeld Nexus 7000) meerdere VDC's hebben. Gebruik de NX-OS CLI-opdracht cli-syntaxisrollen weergeven netwerkoperator om de volledige lijst met opdrachten te zien die beschikbaar is voor deze rol.

Vervolgens worden twee TACACS-profielen gedefinieerd: NXOS Admin en NXOS HelpDesk.

NX-OS-beheerder

Stap 1. Voeg een ander profiel toe en noem het NX-OS Admin.

Stap 2. Selecteer Verplicht in de vervolgkeuzelijst Attributen instellen. Selecteer Beheerder uit de optie Netwerkrol onder Algemene taken.



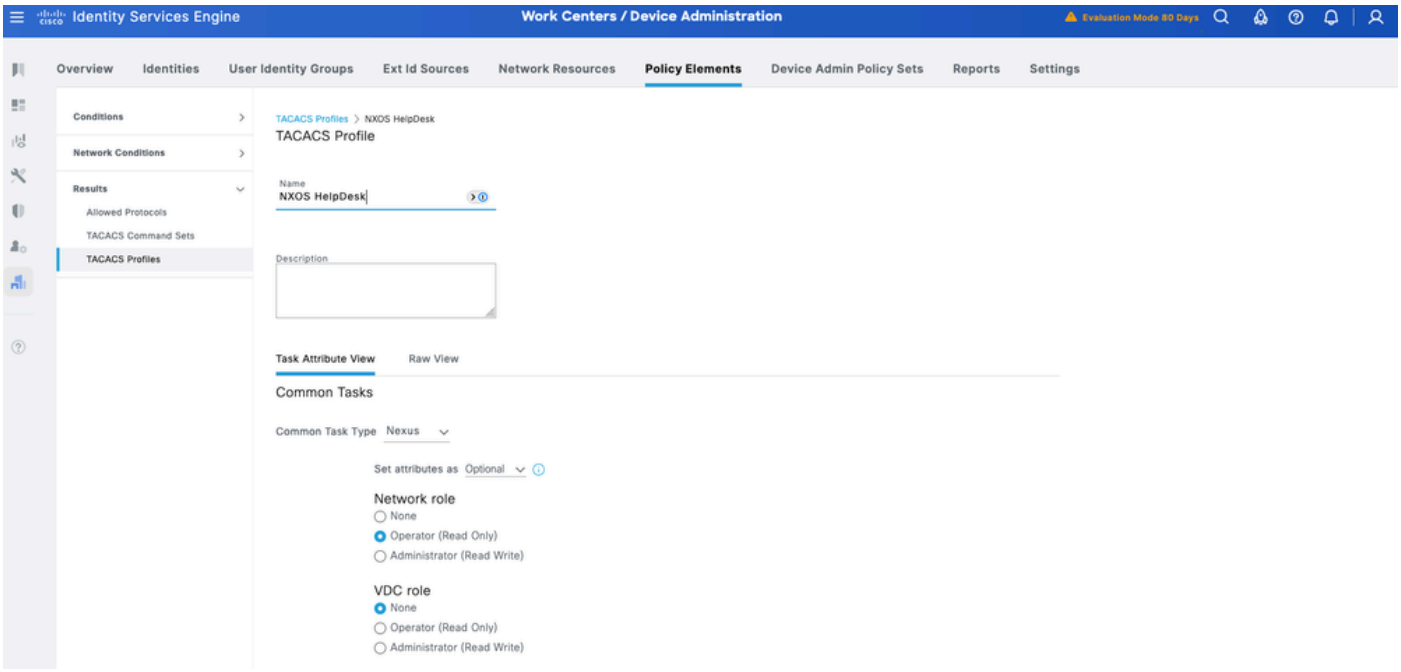
Stap 3. Klik op Indienen om het profiel op te slaan.

NX-OS HelpDesk

Stap 1. Navigeer vanuit ISE UI naar Werkcentra > Apparaatbeheer > Beleidselementen > Resultaten > TACACS-profielen. Voeg een nieuw TACACS-profiel toe en noem het NXOS HelpDesk. Ga naar de keuzelijst Gemeenschappelijk taaktype en kies Nexus.

U kunt de sjabloonwijzigingen zien die specifiek zijn voor de gebruikersrol. U kunt deze opties selecteren die overeenkomen met de gebruikersrol die u wilt configureren.

Stap 2. Selecteer Verplicht in de vervolgkeuzelijst Attributen instellen. Selecteer Operator uit de optie Netwerkrol onder Algemene taken.

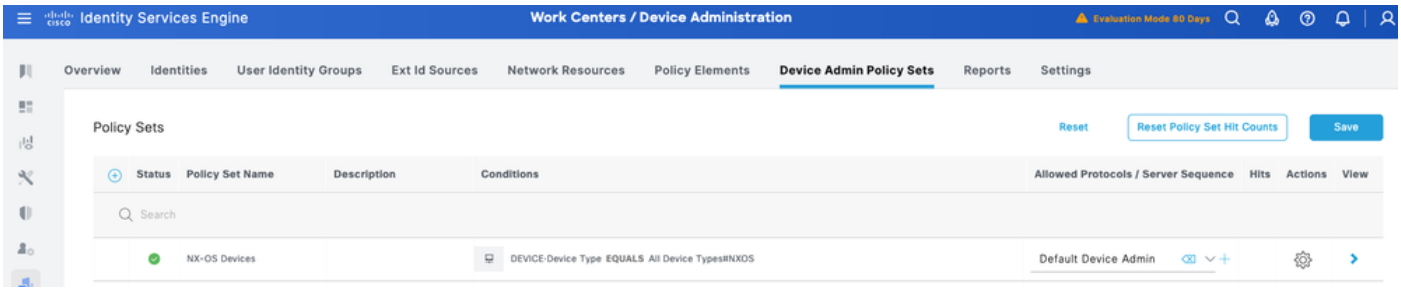


Stap 3. Klik op Opslaan om het profiel op te slaan.

Beleidssets voor apparaatbeheer configureren

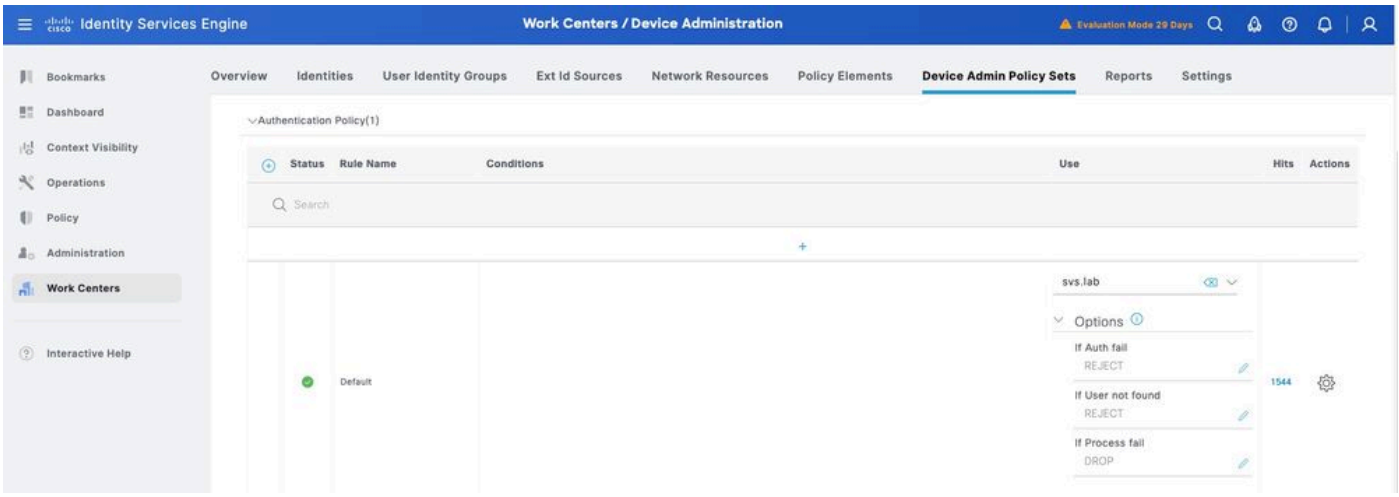
Beleidssets zijn standaard ingeschakeld voor Apparaatbeheer. Beleidsgroepen kunnen beleid verdelen op basis van de apparaattypen om de toepassing van TACACS-profielen te vergemakkelijken. Cisco IOS-apparaten gebruiken bijvoorbeeld Privilege Levels en/of Command Sets, terwijl Cisco NX-OS-apparaten aangepaste kenmerken gebruiken.

Stap 1. Navigeer naar Workcenters > Apparaatbeheer > Beleidssets apparaatbeheer. Voeg een nieuwe beleidsset NX-OS-apparaten toe. Onder voorwaarde specificeert u APPARAAT: Apparaattype IS GELIJK AAN Alle apparaattypen#NXOS. Selecteer onder Toegestane protocollen de optie Standaardapparaatbeheer.



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

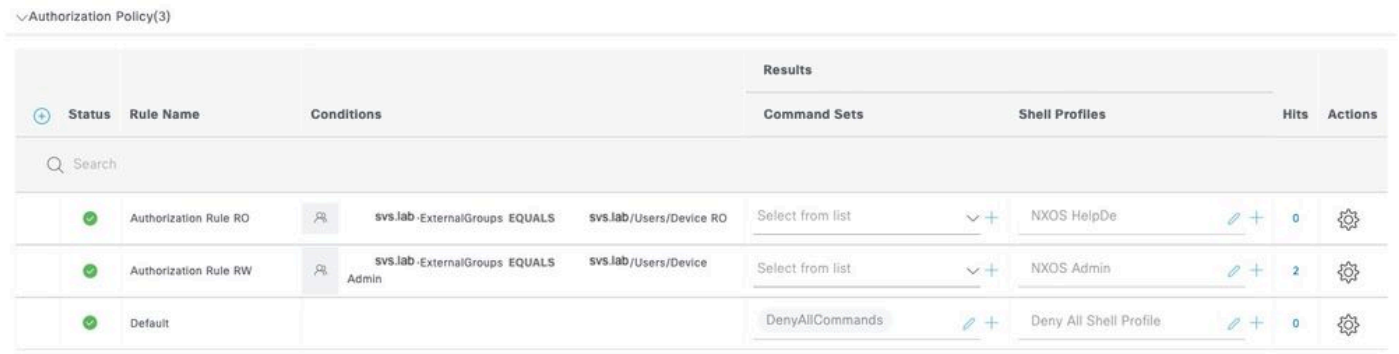
Stap 3. Maak het verificatiebeleid. Voor verificatie gebruikt u de advertentie als ID-winkel. Laat de standaardopties onder Als Auth mislukt, Als gebruiker niet gevonden en Als proces mislukt.



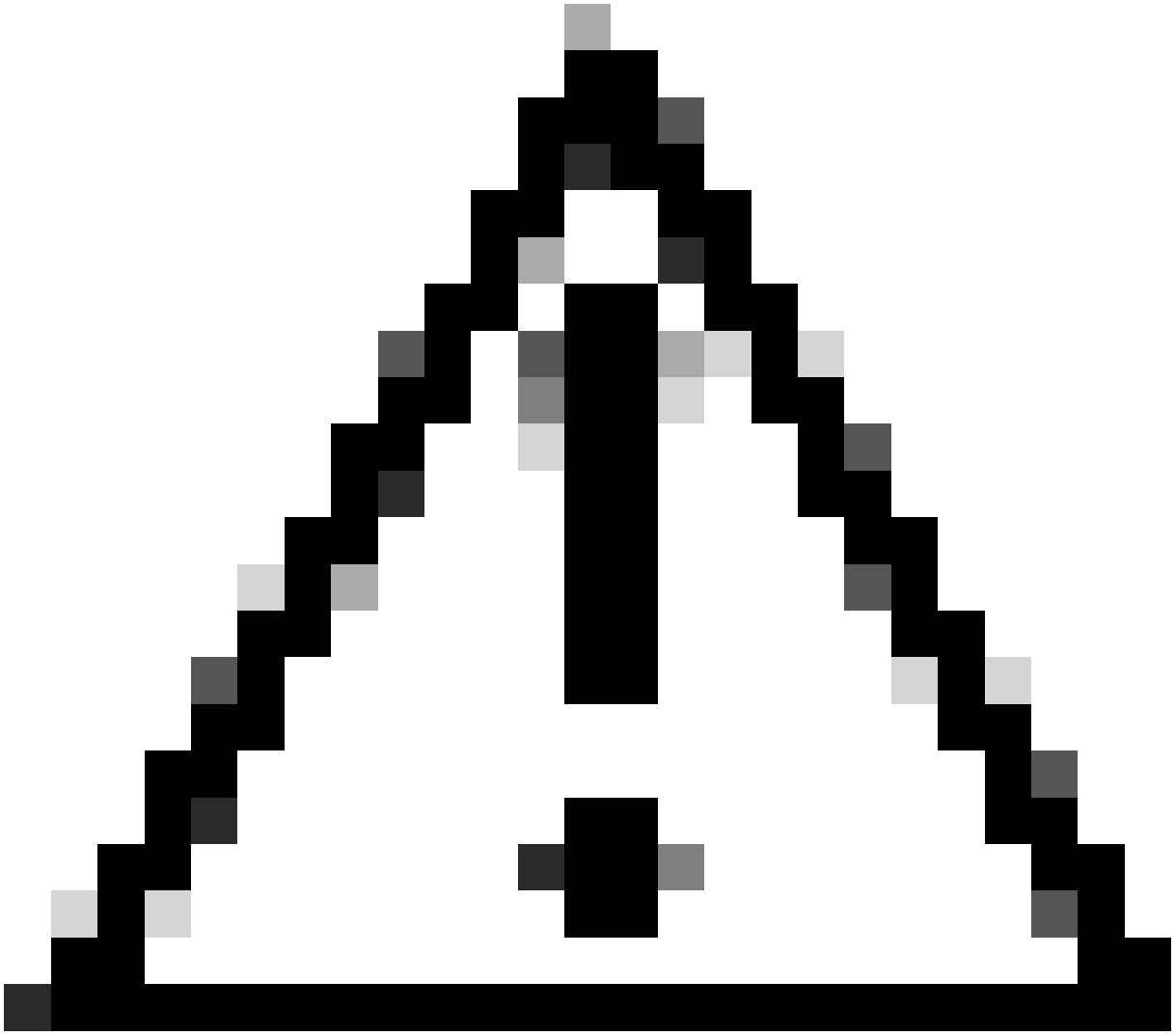
Stap 4. Definieer het autorisatiebeleid.

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

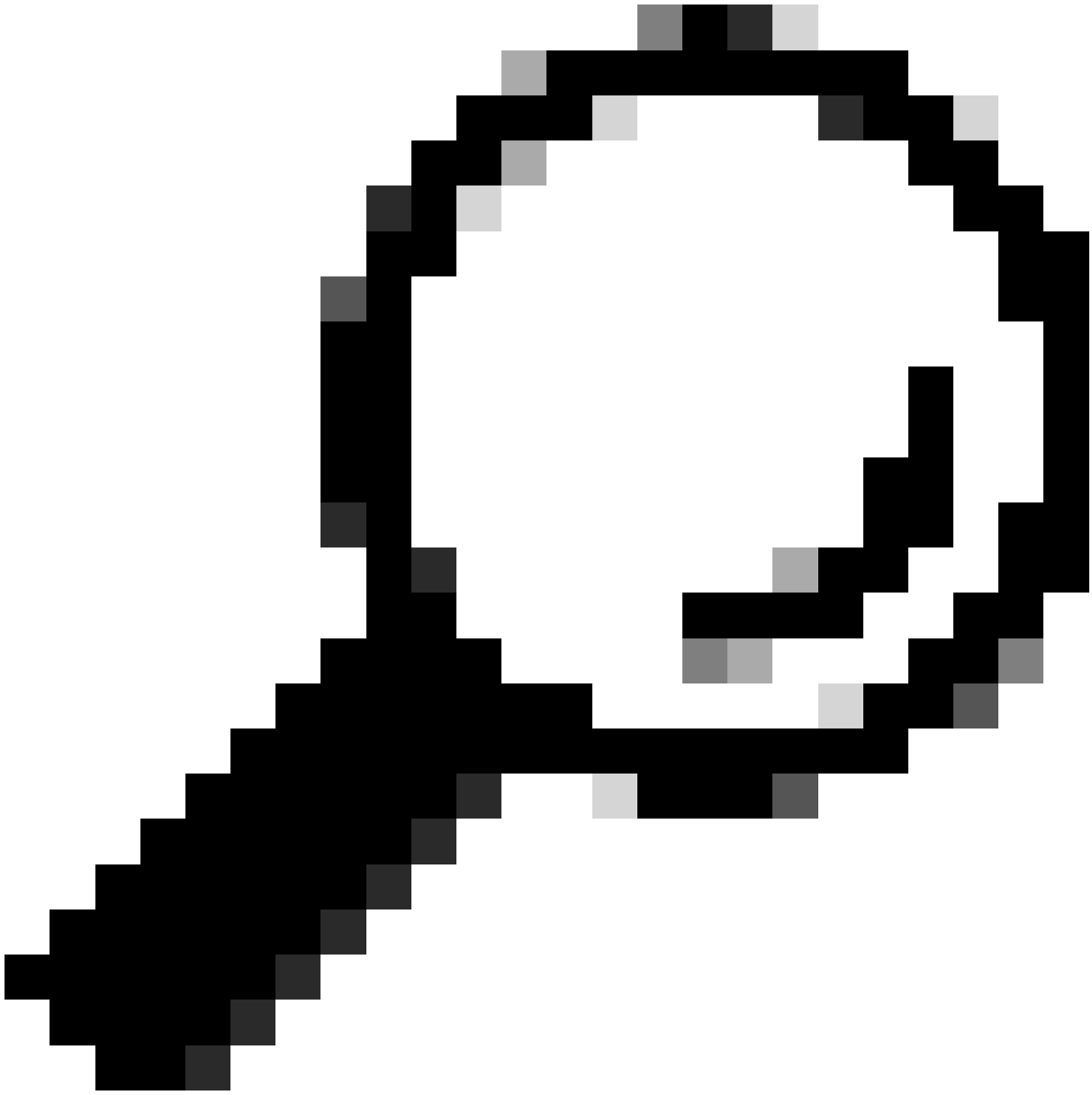
Voorbeeld:
· Gebruikers in de AD-groep Apparaatbeheer krijgen het TACACS-profiel van NXOS-beheerder toegewezen.
· Gebruikers in de AD-groep Device RO krijgen het NXOS HelpDesk TACACS-profiel toegewezen.



Cisco NX-OS configureren voor TACACS+ via TLS



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.

TACACS+-serverconfiguratie

Stap 1. Eerste configuratie.

```
POD2IPN2# sho run tacacs

feature tacacs+

tacacs-server host 10.225.253.209 key 7 "F1whg.123"
```

```
aaa group server tacacs+ tacacs2
  server 10.225.253.209
  use-vrf management
```

Trustpoint-configuratie

Stap 1. Maak een sleutellabel, gebruik in uw geval het ecc-sleutelpaar.

<#root>

```
POD2IPN2(config)#
```

crypto key generate ecc label ec521-label exportable modulus 521

Stap 2. Vergelijk het met een trustpoint.

<#root>

```
POD2IPN2(config)#
```

crypto ca trustpoint ec521-tp

```
POD2IPN2(config-trustpoint)#
```

ecckeypair ec521-label

Stap 3. Installeer de openbare CA-sleutel.

<#root>

```
POD2IPN2(config)#
```

crypto ca authenticate ec521-tp

```
input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----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
83g9EMgKVOARIiVUa/qlAgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAYb4
QgEBBAQDAgAHMBkGCWCGSAGG+EIBDQQMFgpTVlMgTGFiIENBMAOGCSqGSIb3DQEB
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/qd2NRSBWffFOXE/AJHQG7STT
HaXLU9r2Ko6O3oecu8ysGTwLlIt/9T1/FOb0xZRugWcpJrVoTgDGuA==
-----END CERTIFICATE-----
```

END OF INPUT

```
Fingerprint(s): SHA1
Fingerprint=0E:B1:81:E9:5A:3E:D7:80:3B:C5:A8:05:9A:85:4A:95:C8:3A:C7:37

Do you accept this certificate? [yes/no]:yes
POD2IPN2(config)#
POD2IPN2(config)#
```

show crypto ca certificates ec521-tp

```
Trustpoint: ec521-tp
CA certificate 0:
subject=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
issuer=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
serial=20CD7402C4DA37F5
notBefore=Apr 28 17:05:00 2025 GMT
notAfter=Apr 28 17:05:00 2035 GMT
SHA1 Fingerprint=0E:B1:81:E9:5A:3E:D7:80:3B:C5:A8:05:9A:85:4A:95:C8:3A:C7:37
purposes: sslserver sslclient
POD2IPN2(config)#
```

Stap 4. Aanvraag voor identiteitscertificaat van switch genereren.

<#root>

```
POD2IPN2(config)#
```

crypto ca enroll ec521-tp

```
 Create the certificate request ..
 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:C1sco.123
 The subject name in the certificate will be the name of the switch.
```

```
 Include the switch serial number in the subject name? [yes/no]:
```

yes

```
 The serial number in the certificate will be: FDO2649OP4T
 Include an IP address in the subject name [yes/no]:
```

yes

```
ip address:10.225.253.177
 Include the Alternate Subject Name ? [yes/no]:
```

no

```
 The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIIBtjCCARcCAQAwKTERMA8GA1UEAwwIUE9EMklQTjIxFDASBgNVBAUTC0ZETzI2
NDkwUDRUMIGbMBAGByqGSM49AgEGBSuBBAAjA4GGAAQBGYT0iw7OvqIKQ/a22Lkg
Na9IhqWQvetjxKq485gqTSBEo6LzpkOhPAGE4jBveNHxYeIA7PfNWvJ7xTBWjDNX
/IYBm6E7Hd7q42OmCe8Mef+bqJBdJ9wzpyEjhI2lIIoXt4814nBxObkIWWyR5cZN
IiXTLk8P4IMZvPq8jRnELRxd8RGgSTAYBgkqhkiG9w0BCQcxCwwJQzFzY28uMTIz
MC0GCSqGSIb3DQEJDjEgMB4wHAYDVR0RAQH/BBIwEIIIUE9EMklQTjKHBArh/bEw
CgYIKoZIzj0EAwIDgYwAMIGIAkIAtzQ/knrW2ovCVoHAuq1v2cr0n3NenS/44lul
+3H1y52vn4Rm4CGU3wkzXU3qGO3YjhNjCXjhp3+uN2afFf1Wf3ECQgC4bumHVsfj
b5rwPIC5tvXS/A8upqIzqc0yt3OhpaDDOTWzzvZY7qFflCOl5p6pvUpHigqoZNg5
9xhNdM1CQSykOg==
-----END CERTIFICATE REQUEST-----
```

Stap 5. Importeer het identiteitsbewijs van de switch, ondertekend door CA.

```
<#root>
```

```
POD2IPN2(config)#
```

crypto ca import ec521-tp certificate

```
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIDzTCCAbWgAwIBAgIIC6zS76XYDm8wDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNTA3MTkxMDAwWhcNMjYwNTA3MTkxMDAwWjApMREwDwYDVQQDDAhQ
TOQySVBOMjEUMBIGA1UEBRMLRkRPMjYOOTBQNFQwgZswEAYHKoZIzj0CAQYFK4EE
ACMDgYYABAEZhPSLDs6+ogpD9rbYuSA1r0iGpZC962PEqrjzmCpNIESjovOmQ6E8
AYTiMG940fFh4gDs981a8nvFMFaMM1f8hgGboTsd3urjY6YJ7wx5/5uokFOn3DOn
ISOEjaUgihe3jzXicHE5uQhZbJHlxk0iJdMuTw/ggxm8+ryNGcQtHF3xEaNAMD4w
HgYJYIZIAYb4QgENBBEWD3hjYSBjZXJ0aWZpY2FOZTAcBgNVHREBAf8EEjAQgghQ
TOQySVBOMocECuH9sTANBgkqhkiG9w0BAQsFAAOCAgEANWGb6zm9TDPaM1yhPMx7
8uai/pF7VQC8NSCdOKqr4w4+695ZjJuzqFL3msodOQK0EdgxpQ4+pEa5msRtK0i8
mms2X/Px3/EShxoHrZO1PUXNTyZidXpGd/yTrdQAl5JzpW4pEudrbCJMZEEYtqoP
wD+4OE8vKoYEgyWlDrpRZOZG1usZczuUhLZ8orkjXMhWC26Q5aqiCKkyg10Nt6nb
liToeYy2Q0cTesSZCKvRBv6Ewj5JuSLemURyB4GHY+LT+A9UNmEUM2n+OSVEL329
3hS0qd/YVaEuxjjlg7jNiZb+UsW7IRx3Q8Rouo++ISACpH/PJ61LnlVxhXombiS6
INoa0GvQONrl+lFT8ADIdZ/Ukd5Ubhc9bh/sYzf4MWtkK1wVO16Hv7vGpSMYonD6
a271im+tJPyKnnezQ6OykzlGqsL/Ta6JOdip/fEYp8UmRq9InDh23gDjqrojWL7k
1R/bZpc+baMYXd/2pohHMSN0sKN3zNrJTlnuk5KCqFx//4P7mAoyZYiTIDp1pkYS
```

```
VK65fJKD+pYxIhSP9wN8rnwtzSCWbOZ78sgOO6Y6wIXyTPOUB3FWhD+GxtTkmEce
ZnAQbgxpgrg5lhpAEVabpC/zRU4UzTuBmv/WoY12zwXCr5WLXEOWtIe8CwFjSnch
lfKuuebdZkbwz72r7OyyX/U=
-----END CERTIFICATE-----
POD2IPN2(config)#
```

Controleer of het identiteitsbewijs van de switch is geregistreerd.

<#root>

```
POD2IPN2(config)#
```

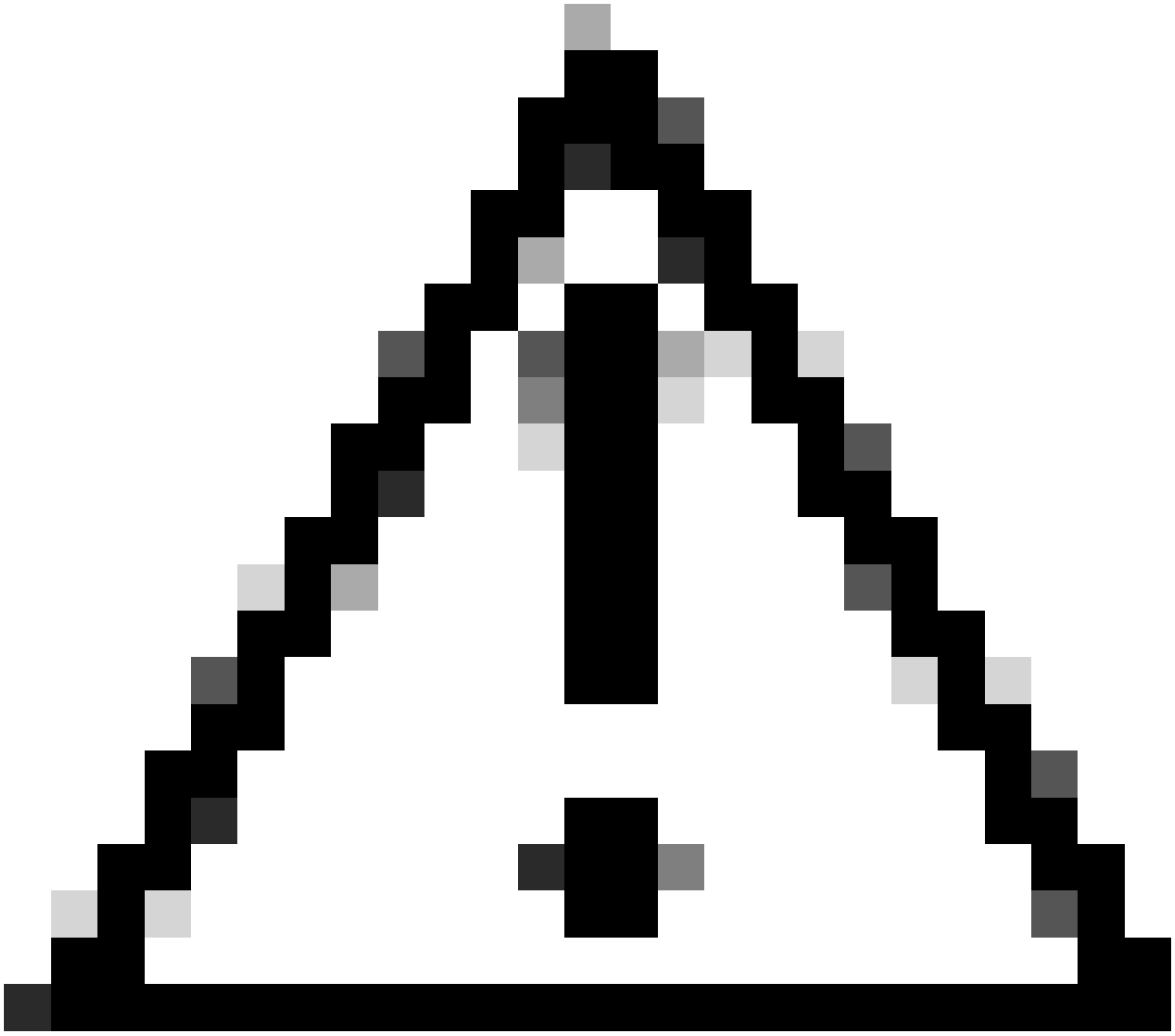
show crypto ca certificates ec521-tp

```
Trustpoint: ec521-tp
certificate:
subject=CN = POD2IPN2, serialNumber = FDO2649OP4T
issuer=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
serial=0BACD2EFA5D8OE6F
notBefore=May  7 19:10:00 2025 GMT
notAfter=May  7 19:10:00 2026 GMT
SHA1 Fingerprint=CA:B2:BF:3F:ED:2F:06:0B:C1:E4:DC:21:9F:9D:54:61:98:32:C5:13
purposes: sslserver sslclient

CA certificate 0:
subject=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
issuer=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
serial=2OCD74O2C4DA37F5
notBefore=Apr 28 17:05:00 2025 GMT
notAfter=Apr 28 17:05:00 2035 GMT
SHA1 Fingerprint=0E:B1:81:E9:5A:3E:D7:8O:3B:C5:A8:O5:9A:85:4A:95:C8:3A:C7:37
purposes: sslserver sslclient

POD2IPN2(config)#
```

TACACS+ TLS-configuratie



Let op: Voer deze configuratiewijzigingen uit via console met lokale referenties.

Stap 1. Configureer globale tacacs tls.

<#root>

```
POD2IPN2(config)#
tacacs-server secure tls
```

Stap 2. Wijzig de ISE-poort in de TLS-poort waarmee de ISE-server is geconfigureerd.

<#root>

```
POD2IPN2(config)#
tacacs-server host 10.225.253.209 port 6049 timeout 60 single-connection
```

Stap 3. Koppel de configuratie van de ISE-server op de switch aan het vertrouwenspunt voor de TLS-verbinding.

<#root>

POD2IPN2(config)#

tacacs-server host 10.225.253.209 tls client-trustpoint ec521-tp

Stap 4. Maak een tacacs-servergroep aan.

<#root>

POD2IPN2(config)#

aaa group server tacacs+ tacacs2

POD2IPN2(config-tacacs+)#

server 10.225.253.209

POD2IPN2(config-tacacs+)#

use-vrf management

Stap 5. De configuratie verifiëren.

<#root>

POD2IPN2#

sho run tacacs

```
feature tacacs+

tacacs-server secure tls
tacacs-server host 10.225.253.209 port 6049 timeout 60 single-connection
tacacs-server host 10.225.253.209 tls client-trustpoint ec521-tp
aaa group server tacacs+ tacacs2
    server 10.225.253.209
    use-vrf management
```

Stap 6. Test de externe gebruiker voordat u AAA-verificatie configureert.

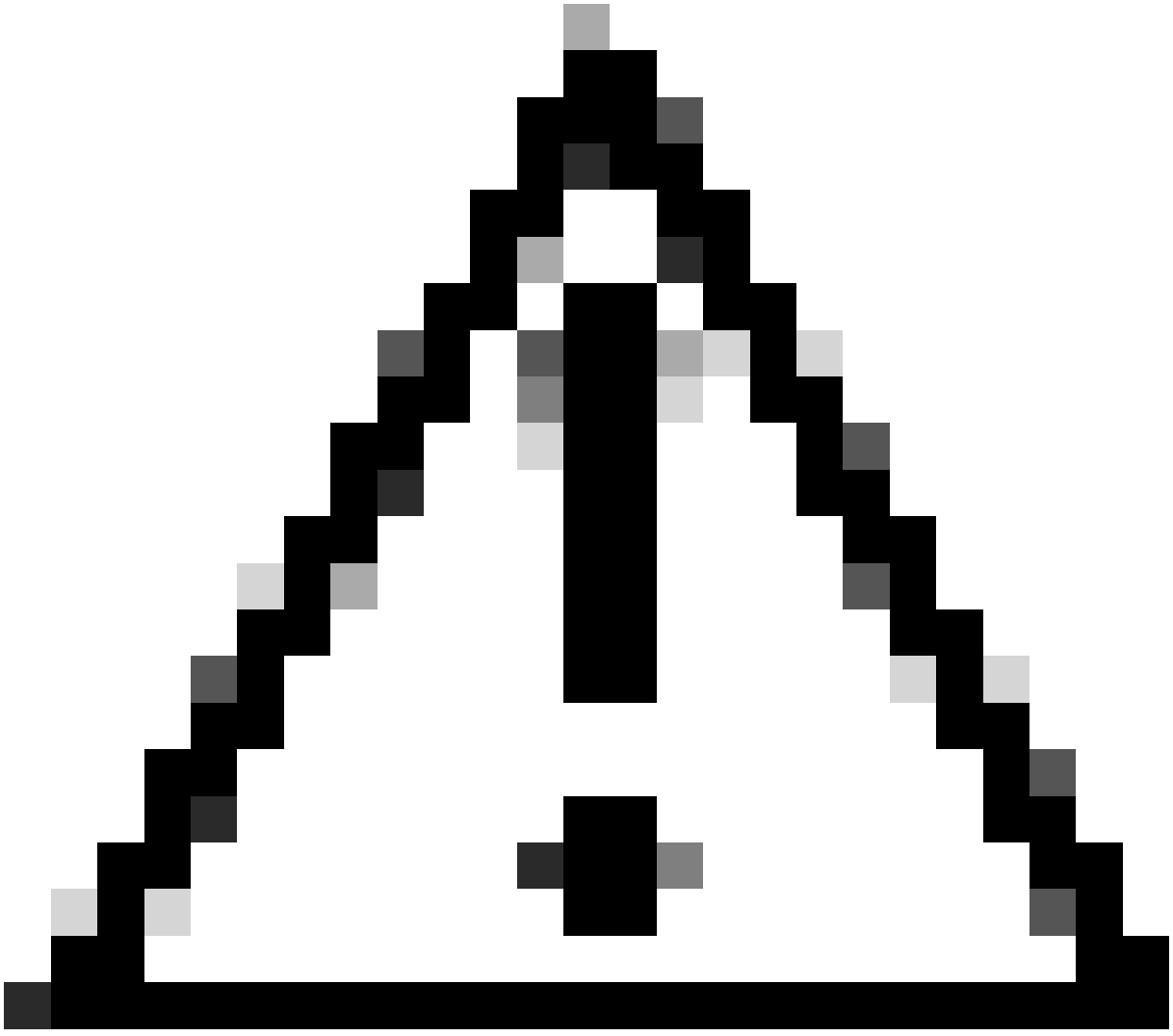
<#root>

```
POD2IPN2#
```

```
test aaa group tacacs2
```

```
user has been authenticated
POD2IPN2#
```

AAA-configuratie



Let op: zorg ervoor dat de externe gebruikersverificatie succesvol is voordat u doorgaat

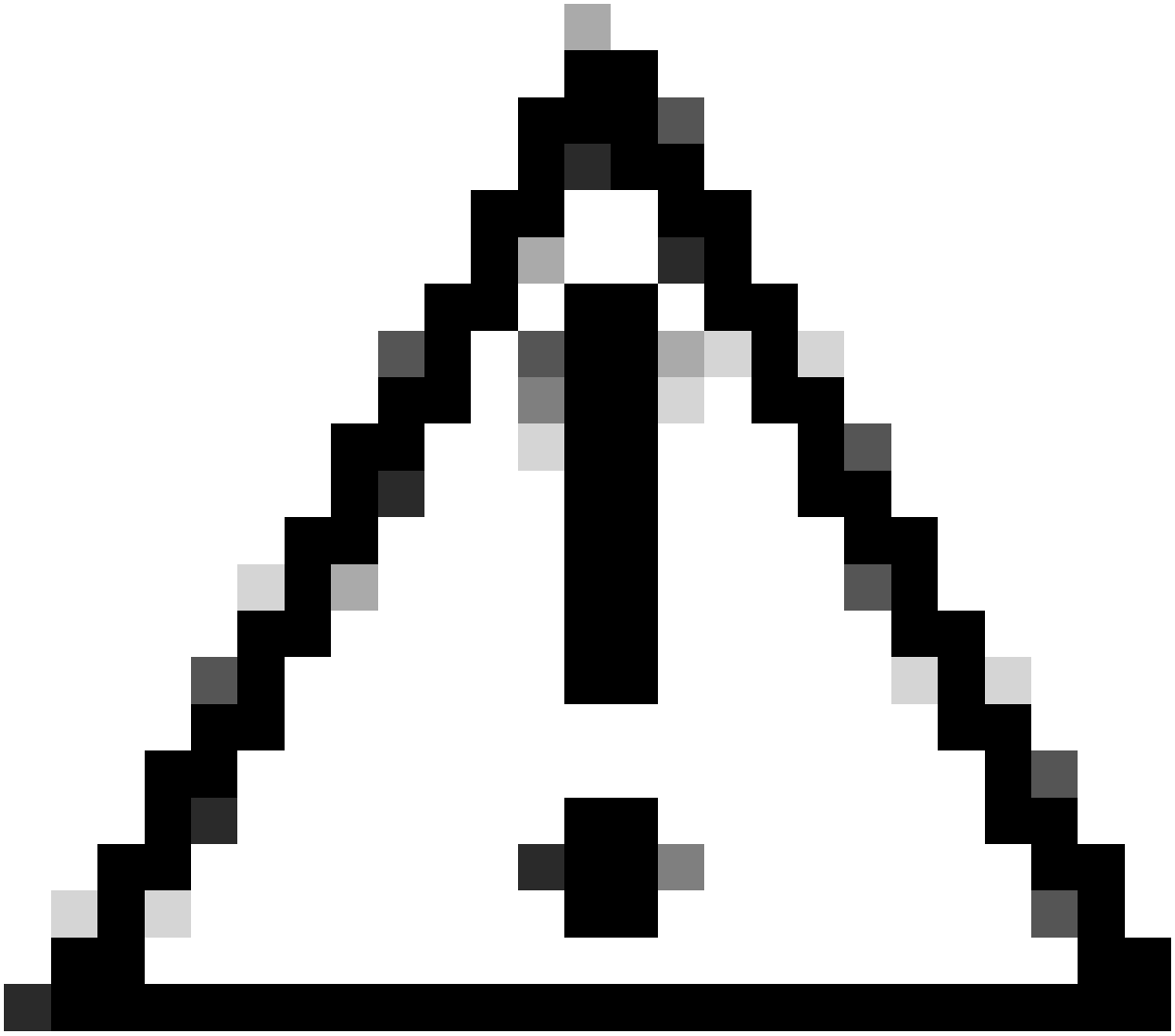
met AAA-configuraties.

Stap 1. Configureer AAA-verificatie op afstand.

<#root>

```
POD2IPN2(config)#
aaa authentication login default group tacacs2
```

Stap 2. Configureer AAA-autorisatie op afstand na het testen van de opdracht.



Let op: Zorg ervoor dat u de autorisatiestatus ziet als "AAA_AUTHOR_STATUS_PASS_ADD.

<#root>

```
POD2IPN2#
test aaa authorization command-type config-commands default user
        command "feature bgp"
sending authorization request for: user: pamemart, author-type:3, cmd "feature bgp"
user pamemart, author type 3, command: feature bgp, authorization-status:0x1(AAA_AUTHOR_STATUS_PASS_ADD)
```

Stap 3. Configureer de AAA-opdracht en de autorisatie van de configuratieopdracht.

```
<#root>
POD2IPN2(config)#
aaa authorization config-commands default group tacacs2 local
POD2IPN2(config)#
aaa authorization commands default group tacacs2 local
```

Gebruikerstoegang testen en oplossen voor NX-OS

Verificatie

Configuratie voor apparaatbeheer voor Cisco NX-OS is voltooid. U moet de configuratie valideren.

Stap 1. SSH en log in op de NX-OS-apparaten als verschillende rollen.

Stap 2. Controleer of de gebruiker toegang heeft tot de juiste opdrachten zodra deze zich op de opdrachtregelinterface (CLI) van het apparaat bevindt. Een helpdeskgebruiker moet bijvoorbeeld een gewoon IP-adres kunnen pingen (bijvoorbeeld 10.225.253.129), maar de actieve configuratie niet kunnen weergeven.

```
POD2IPN1# ping 10.225.253.129 vrf management
PING 10.225.253.129 (10.225.253.129): 56 data bytes
64 bytes from 10.225.253.129: icmp_seq=0 ttl=254 time=0.817 ms
64 bytes from 10.225.253.129: icmp_seq=1 ttl=254 time=0.638 ms
64 bytes from 10.225.253.129: icmp_seq=2 ttl=254 time=0.642 ms
64 bytes from 10.225.253.129: icmp_seq=3 ttl=254 time=0.651 ms
64 bytes from 10.225.253.129: icmp_seq=4 ttl=254 time=0.712 ms
```

```
--- 10.225.253.129 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.638/0.692/0.817 ms
POD2IPN1#
POD2IPN1# show running-config
% Permission denied for the role
```

Probleemoplossing

NX-OS-configuratievalidatie.

```
POD2IPN2# show crypto ca certificates
POD2IPN2# show crypto ca trustpoints
POD2IPN2# show tacacs-server statistics <server ip>
```

Gebruik deze opdrachten om de gebruikersverbindingen en rol(len) weer te geven.

```
show users
show user-account [<user-name>]
A sample output is shown below:
POD2IPN1# show users
NAME LINE TIME IDLE PID COMMENT
Admin-ro pts/5 May 15 23:49 . 16526 (10.189.1.151) session=ssh *
POD2IPN1# show user-account Admin-ro
user:Admin-ro
roles:network-operator
account created through REMOTE authentication
Credentials such as ssh server key will be cached temporarily only for this user account
Local login not possible...
```

Dit zijn nuttige fouten bij het oplossen van problemen met TACACS+:

```
debug TACACS+ aaa-request
2016 Jan 11 03:03:08.652514 TACACS[6288]:  process_aaa_tplus_request:Checking for state of mgmt0 port w
2016 Jan 11 03:03:08.652543 TACACS[6288]:  process_aaa_tplus_request: Group demoTG found. corresponding
2016 Jan 11 03:03:08.652552 TACACS[6288]:  process_aaa_tplus_request: checking for mgmt0 vrf:management
2016 Jan 11 03:03:08.652559 TACACS[6288]:  process_aaa_tplus_request:port_check will be done
2016 Jan 11 03:03:08.652568 TACACS[6288]:  state machine count 0
2016 Jan 11 03:03:08.652677 TACACS[6288]:  is_intf_up_with_valid_ip(1258):Proper IOD is found.
2016 Jan 11 03:03:08.652699 TACACS[6288]:  is_intf_up_with_valid_ip(1261):Port is up.
2016 Jan 11 03:03:08.653919 TACACS[6288]:  debug_av_list(797):Printing list
2016 Jan 11 03:03:08.653930 TACACS[6288]:  35 : 4 : ping
2016 Jan 11 03:03:08.653938 TACACS[6288]:  36 : 12 : 10.1.100.255
2016 Jan 11 03:03:08.653945 TACACS[6288]:  36 : 4 : <cr>
2016 Jan 11 03:03:08.653952 TACACS[6288]:  debug_av_list(807):Done printing list, exiting function
2016 Jan 11 03:03:08.654004 TACACS[6288]:  tplus_encrypt(659):key is configured for this aaa sessin.
2016 Jan 11 03:03:08.655054 TACACS[6288]:  num_inet_addrs: 1 first s_addr: -1268514550 10.100.1.10 s6_a
2016 Jan 11 03:03:08.655065 TACACS[6288]:  non_blocking_connect(259):interface ip_type: IPV4
```

```
2016 Jan 11 03:03:08.656023 TACACS[6288]:  non_blocking_connect(369): Proceeding with bind
2016 Jan 11 03:03:08.656216 TACACS[6288]:  non_blocking_connect(388): setsockopt success error:22
2016 Jan 11 03:03:08.656694 TACACS[6288]:  non_blocking_connect(489): connect() is in-progress for serv
2016 Jan 11 03:03:08.679815 TACACS[6288]:  tplus_decode_authen_response: copying hostname into context
```

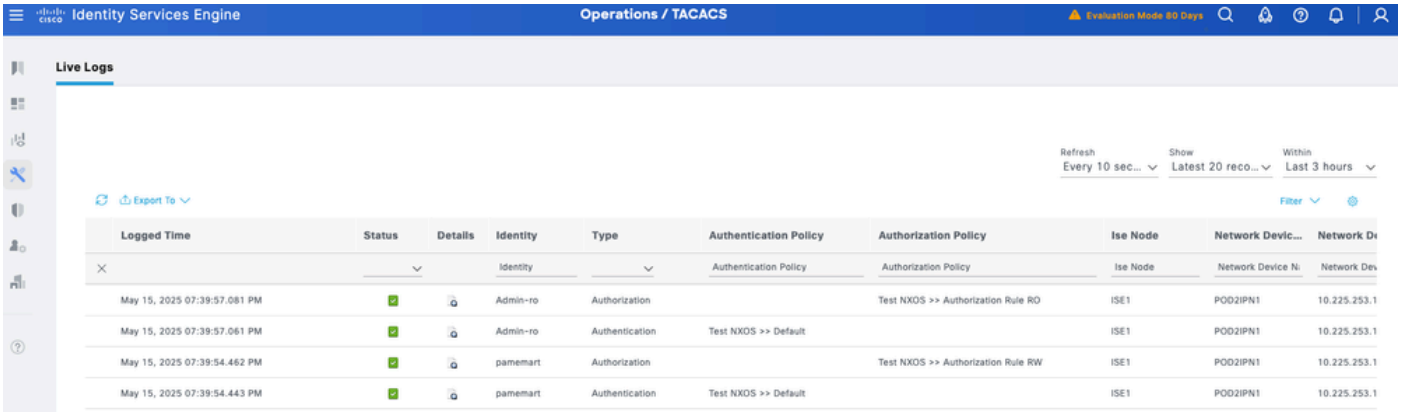
SSL-debug inschakelen.

```
touch '/bootflash/.enable_ssl_debugs'
```

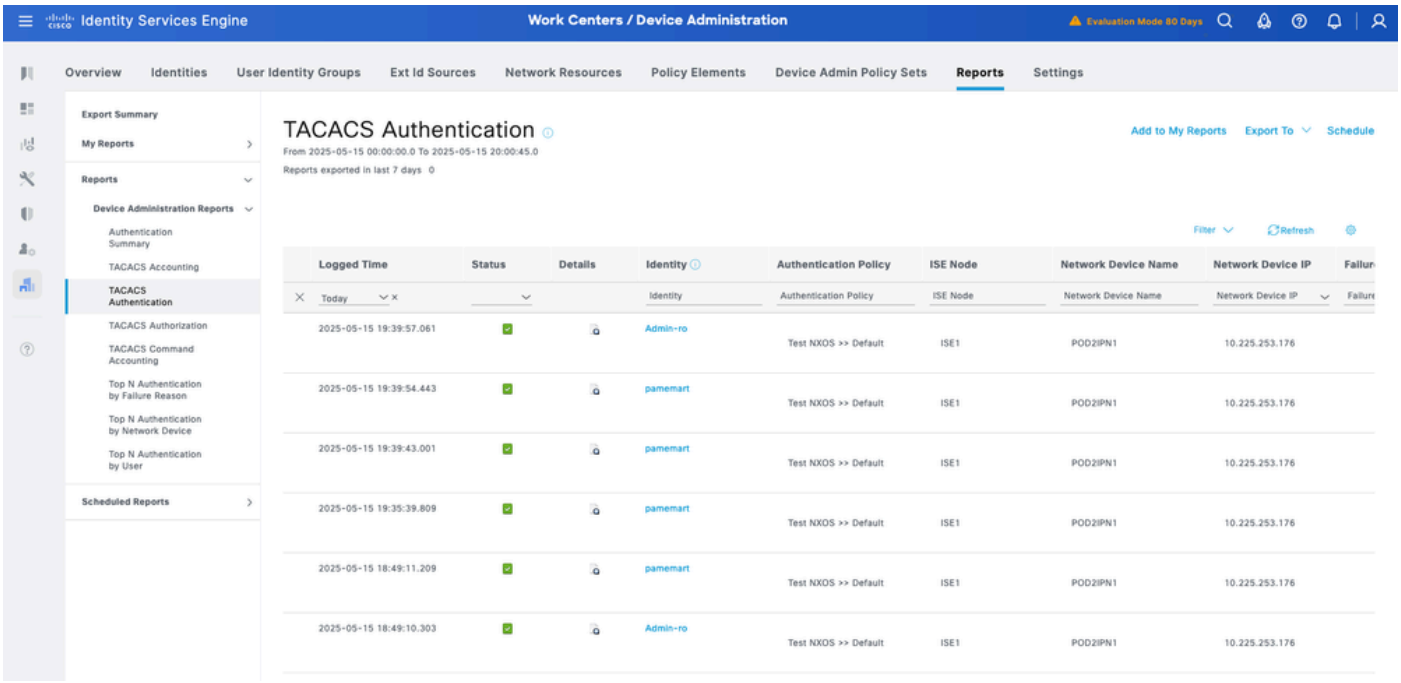
De inhoud van het debug-bestand weergeven.

```
cat /tmp/ssl_wrapper.log.*
```

Navigeer vanuit de ISE GUI naar Operations > TACACS Livelog. Alle TACACS-verificatie- en autorisatieverzoeken worden hier vastgelegd en de knop Details biedt gedetailleerde informatie over waarom een bepaalde transactie is geslaagd / mislukt.



Voor historische rapporten: ga naar Werkcentra > Apparaatbeheer > Rapporten > Apparaatbeheer om de verificatie-, autorisatie- en boekhoudrapporten te verkrijgen.


Identity Services Engine
Work Centers / Device Administration
Evaluation Mode 80 Days
Overview
Identities
User Identity Groups
Ext Id Sources
Network Resources
Policy Elements
Device Admin Policy Sets
Reports
Settings
Export Summary
My Reports
Reports
Device Administration Reports
Authentication Summary
TACACS Accounting
TACACS Authentication
TACACS Authorization
TACACS Command Accounting
Top N Authentication by Failure Reason
Top N Authentication by Network Device
Top N Authentication by User
Scheduled Reports
TACACS Authentication
From 2025-05-15 00:00:00.0 To 2025-05-15 20:00:45.0
Reports exported in last 7 days 0
Add to My Reports
Export To
Schedule
Filter
Refresh
Logged Time
Status
Details
Identity
Authentication Policy
ISE Node
Network Device Name
Network Device IP
Today
Identity
Authentication Policy
ISE Node
Network Device Name
Network Device IP
2025-05-15 19:39:57.061
Admin-ro
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176
2025-05-15 19:39:54.443
pamemart
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176
2025-05-15 19:39:43.001
pamemart
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176
2025-05-15 19:35:39.809
pamemart
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176
2025-05-15 18:49:11.209
pamemart
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176
2025-05-15 18:49:10.303
Admin-ro
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176

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.