

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

Inhoud

[Inleiding](#)

[Overzicht](#)

[Gebruik van deze Guide](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[vergunning](#)

[ISE configureren voor Apparaatbeheer](#)

[Aanvraag voor certificaatondertekening genereren voor TACACS+-serververificatie](#)

[Root CA-certificaat uploaden voor TACACS+-serververificatie](#)

[Het ondertekende certificaatondertekeningsverzoek \(CSR\) binden aan ISE](#)

[TLS 1.3 inschakelen](#)

[Apparaatbeheer inschakelen op ISE](#)

[TACACS via TLS inschakelen](#)

[Groepen netwerkkapparaten en netwerkkapparaten](#)

[Identiteitswinkels configureren](#)

[TACACS+ Shell-profielen configureren](#)

[NX-OS-beheerder](#)

[NX-OS HelpDesk](#)

[Apparaatbeheerbeleidssets configureren](#)

[Cisco NX-OS configureren voor TACACS+ via TLS](#)

[TACACS+-serverconfiguratie](#)

[Trustpoint-configuratie](#)

[TACACS+ TLS-configuratie](#)

[AAA-configuratie](#)

[Gebruikerstoegang testen en oplossen voor NX-OS](#)

[Verificatie](#)

[Probleemoplossing](#)

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.



Administration

System

Deployment

Licensing

Certificates

Logging

Maintenance

Upgrade & Rollback

Health Checks

Backup & Restore

Admin Access

Settings

Identity Management

Identities

Groups

External Identity Sources

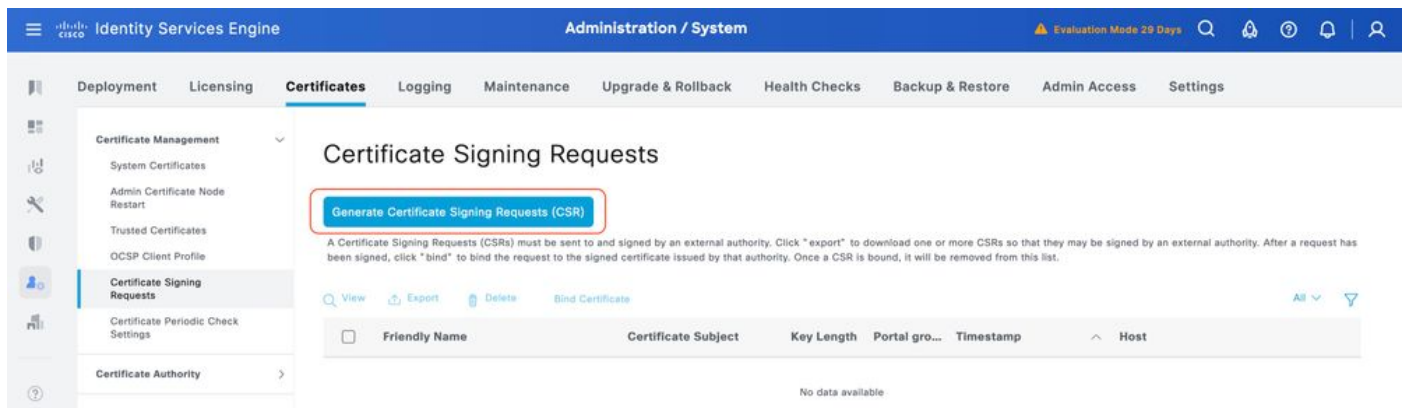
Identity Source Sequences

Settings

Feed Service

Profiler

Stap 3. Klik onder Certificaatondertekeningsverzoeken op Certificaatondertekeningsverzoek genereren.



Stap 4. Selecteer TACACS in Gebruik.

Usage

Certificate(s) will be used for **TACACS** ▼

Allow Wildcard Certificates ☐ ?

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

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☒ ISE1	ISE1#TACACS

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

Subject

Common Name (CN)
\$FQDN\$



Organizational Unit (OU)
CX



Organization (O)
Cisco



City (L)
Raleigh

State (ST)
North Carolina

Country (C)
US

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

Subject Alternative Name (SAN)

⋮	DNS Name	✓	ISE1.lab	−	+	
⋮	IP Address	✓	10.225.253.209	−	+	ⓘ

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.

Identity Services Engine Administration / System Evaluation Mode 29 Days

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Admin Certificate Node Restart
- Trusted Certificates**
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Settings

Certificate Authority

Trusted Certificates

For disaster recovery it is recommended to export and backup all your trusted certificates.

Edit Import Export Delete View show internal CA certificates

☐	Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Status
☐	Amazon root CA	Infrastructure Cisco Services	06 6C 9F CF ...	Amazon Root CA 1	Amazon Root CA 1	Tue, 26 May 2015	Sun, 17 Jan 2...	Ent
☐	Cisco ECC Root CA 2099	Cisco Services	03	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Mon, 7 Sep 2...	Ent
☐	Cisco Licensing Root CA	Cisco Services	01	Cisco Licensing R...	Cisco Licensing R...	Thu, 30 May 2013	Sun, 30 May 2...	Ent
☐	Cisco Manufacturing CA SHA2	Endpoints Infrastructure	02	Cisco Manufactur...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2...	Ent
☐	Cisco Root CA 2048	Endpoints Infrastructure	5F F8 7B 28 2...	Cisco Root CA 20...	Cisco Root CA 20...	Fri, 14 May 2004	Mon, 14 May ...	Dis
☐	Cisco Root CA 2099	Cisco Services	01 9A 33 58 7...	Cisco Root CA 20...	Cisco Root CA 20...	Tue, 9 Aug 2016	Sun, 9 Aug 20...	Ent
☐	Cisco Root CA M1	Cisco Services	2E D2 0E 73 4...	Cisco Root CA M1	Cisco Root CA M1	Tue, 18 Nov 2008	Fri, 18 Nov 20...	Ent
☐	Cisco Root CA M2	Infrastructure Endpoints	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2...	Ent
☐	Cisco RXC-R2	Cisco Services	01	Cisco RXC-R2	Cisco RXC-R2	Wed, 9 Jul 2014	Sun, 9 Jul 2034	Ent

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.

Import a new Certificate into the Certificate Store

* Certificate File **Examinar...** ISE SVSLab CA.crt

Friendly Name

Trusted For:

- ☒ Trust for authentication within ISE
- ☐ Trust for client authentication and Syslog
 - ☐ Trust for certificate based admin authentication
- ☐ Trust for authentication of Cisco Services
- ☐ Trust for Native IPSec certificate based authentication
- ☐ Validate Certificate Extensions

Description

Submit

Cancel

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

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System page. The left sidebar contains a menu with options like Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade & Rollback, Health Checks, Backup & Restore, Admin Access, and Settings. The main content area is titled "Trusted Certificates" and displays a table of certificates. The first row is highlighted with a red box, showing a certificate issued by SVS LabCA for the friendly name "CN=SVS LabCA, OU=SVS, O=Cisco, L=...".

Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Status
CN=SVS LabCA, OU=SVS, O=Cisco, L=...	Infrastructure Cisco Services Endpoints AdminAuth	20 CD 74 02 ...	SVS LabCA	SVS LabCA	Mon, 28 Apr 2025	Sat, 28 Apr 2...	Enz
Default self-signed server certificate	Endpoints Infrastructure	02 36 30 F4 6...	ISE2.tmo.svs.com	ISE2.tmo.svs.com	Fri, 11 Jul 2025	Sun, 11 Jul 2...	Enz
DigiCert Global Root CA	Cisco Services	08 3B E0 56 9...	DigiCert Global R...	DigiCert Global R...	Fri, 10 Nov 2006	Mon, 10 Nov ...	Enz
DigiCert Global Root G2 CA	Cisco Services	03 3A F1 E6 ...	DigiCert Global R...	DigiCert Global R...	Thu, 1 Aug 2013	Fri, 15 Jan 20...	Enz
DigiCert root CA	Endpoints Infrastructure	02 AC 5C 26 ...	DigiCert High Ass...	DigiCert High Ass...	Fri, 10 Nov 2006	Mon, 10 Nov ...	Enz
DigiCert SHA2 High Assurance Server ...	Endpoints Infrastructure	04 E1 E7 A4 ...	DigiCert SHA2 Hi...	DigiCert High Ass...	Tue, 22 Oct 2013	Sun, 22 Oct 2...	Enz

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.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System page. The left sidebar contains a menu with options like Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade & Rollback, Health Checks, Backup & Restore, Admin Access, and Settings. The main content area is titled "Certificate Signing Requests" and displays a button "Generate Certificate Signing Requests (CSR)". Below the button, there is a text box explaining that CSR requests must be sent to and signed by an external authority. At the bottom, there is a table with columns for Friendly Name, Certificate Subject, Key Length, Portal gro..., Timestamp, and Host. The "Bind Certificate" button is highlighted with a red box.

Friendly Name	Certificate Subject	Key Length	Portal gro...	Timestamp	Host
---------------	---------------------	------------	---------------	-----------	------

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

Identity Services Engine Administration / System Evaluation Mode 29 Days

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management System Certificates Admin Certificate Node Restart Trusted Certificates OCSP Client Profile **Certificate Signing Requests** Certificate Periodic Check Settings Certificate Authority

Bind CA Signed Certificate

* Certificate File Examine...

Friendly Name

Validate Certificate Extensions ☐

Usage

☒ TACACS: Use certificate for TACACS Server

Submit Cancel

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.

Warning

The certificate you are importing or generating matches an existing certificate. (Both certificates have the same subject.) If you proceed, the existing certificate will be replaced, and the new certificate will be given the same roles and Portal tag, if applicable, as the existing certificate.

Do you wish to replace the existing certificate?

No Yes

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

Identity Services Engine Administration / System Evaluation Mode 29 Days

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management System Certificates Admin Certificate Node Restart Trusted Certificates OCSP Client Profile Certificate Signing Requests Certificate Periodic Check Settings Certificate Authority

System Certificates For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

Edit + Generate Self Signed Certificate + Import Export Delete View

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
ISE1	C=US, ST=NC, L=Raleigh, O=Cisco, OU=SVS, CN=ISE1.lab#ISE1.lab#00010	TACACS	ISE1.lab	ISE1.lab	Wed, 10 Sep 2025	Fri, 10 Sep 2027	Active

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.



Identity Services Engine



Bookmarks



Dashboard



Context Visibility



Operations



Policy



Administration



Work Centers



?

Interactive Help

Deployment

Licensing

Client Provisioning

FIPS Mode

Security Settings

Alarm Settings

System

Deployment

Licensing

Certificates

Logging

Maintenance

Upgrade & Rollback

Health Checks

Backup & Restore

Admin Access

Settings ✓

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

Client Provisioning

FIPS Mode

Security Settings

Alarm Settings

General MDM / UEM Settings

Posture

Profiling

Protocols

Security Settings

Choose the security settings you want to enable to ensure safe communications across your network.

TLS Versions Settings

TLS 1.2 is enabled by default and can't be deselected. Choose one or a range of consecutive TLS versions.

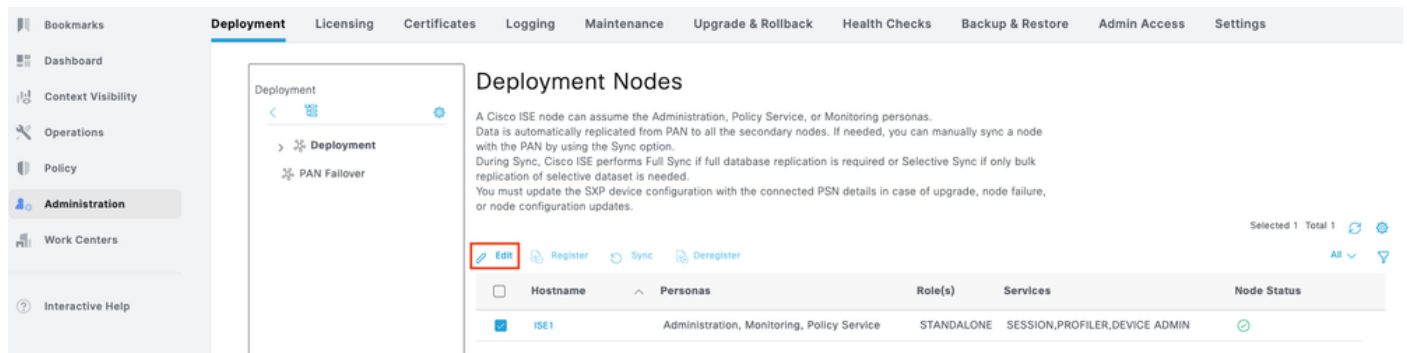
☐ TLS 1.0 ?☐ TLS 1.1 ?☒ TLS 1.2 ?☒ TLS 1.3 ?



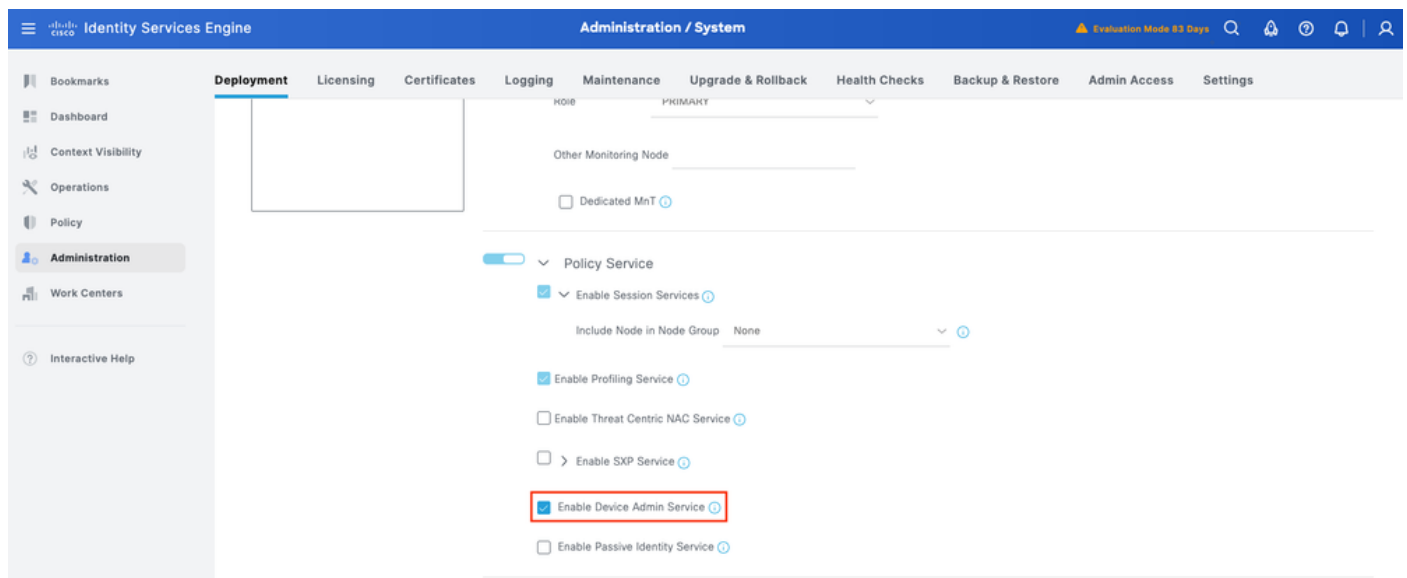
Waarschuwing: wanneer u de TLS-versie wijzigt, wordt de Cisco ISE-toepassingsserver opnieuw gestart op alle Cisco ISE-implementatiemachines.

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.



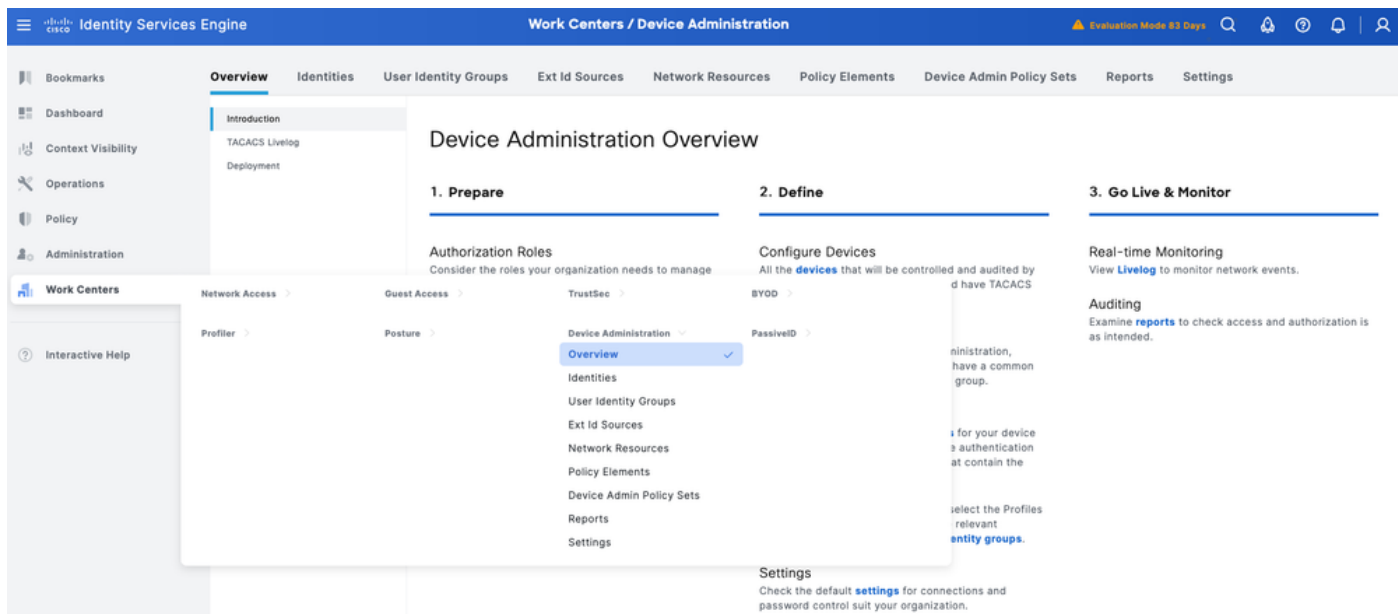
Stap 2. Blader onder Algemene instellingen omlaag en selecteer het selectievakje naast Apparaatbeheerservice inschakelen.



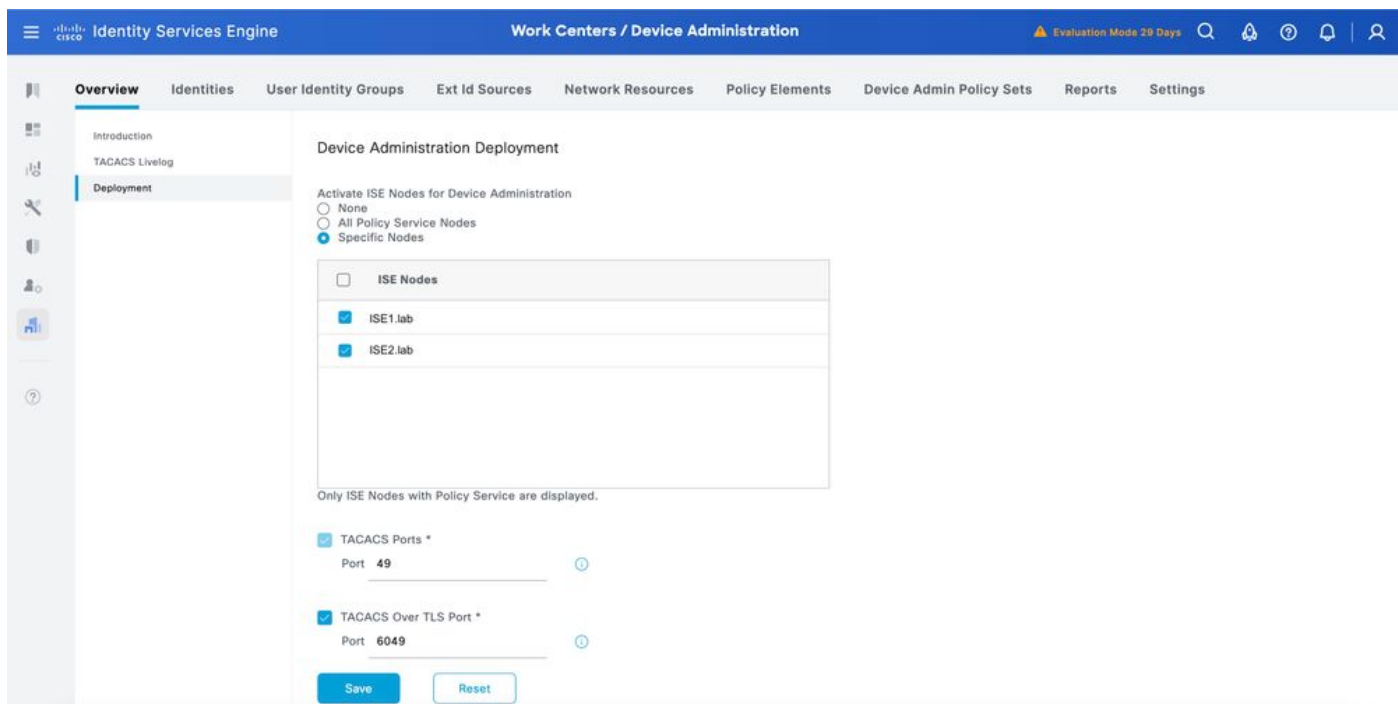
Stap 3. Sla de configuratie op. Device Admin Service is nu ingeschakeld op ISE.

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 apparaatgroefhiërarchieën. Elke hiërarchie vertegenwoordigt een afzonderlijke en onafhankelijke classificatie van netwerkapparaten.

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

The screenshot shows the 'Work Centers / Device Administration' page in Cisco ISE. The 'Network Resources' tab is selected, displaying a table of network devices. The table has three columns: 'Name', 'Description', and 'No. of Network Devices'. The rows include 'All Device Types', 'All Locations', and specific locations like Atlanta, Los Angeles, and New York. There are also options to add, duplicate, edit, or delete devices.

Name	Description	No. of Network Devices
> All Device Types	All Device Types	--
> All Locations	All Locations	--
Atlanta		0
Los Angeles		0
New York		0
> Is IPSEC Device	Is this a RADIUS over IPSEC Device	--

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 netwerkkapparaat dat later in de beleidsvoorwaarde kan worden gebruikt.

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

The screenshot shows the 'Administration / Network Resources' page in Cisco ISE. The 'Network Devices' tab is selected, displaying the configuration for a new network device named 'POD2IPN2'. The configuration includes fields for Name, Description, IP Address (10.225.253.177), Device Profile (Cisco), Model Name (C9364D-GX2A), Software Version (10.5(3t)), Location (Atlanta), IPSEC (No), and Device Type (NXOS).

Field	Value
Name	POD2IPN2
Description	
IP Address	10.225.253.177
Device Profile	Cisco
Model Name	C9364D-GX2A
Software Version	10.5(3t)
Location	Atlanta
IPSEC	No
Device Type	NXOS

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

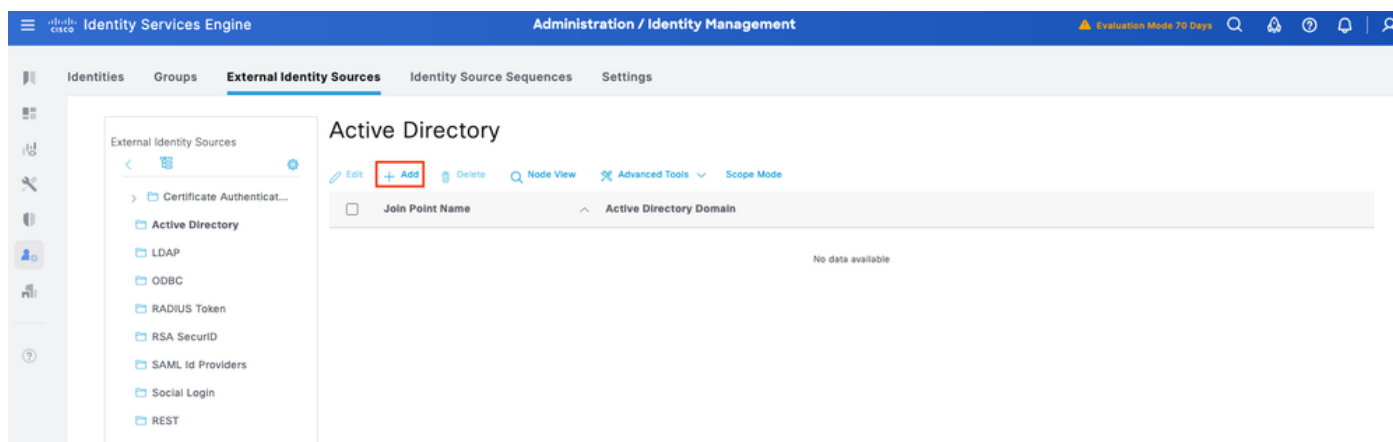
Allow a network device to use one TCP connection for all TACACS+ requests, reducing overhead from repeatedly establishing and closing connections, especially for high-traffic devices.

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.

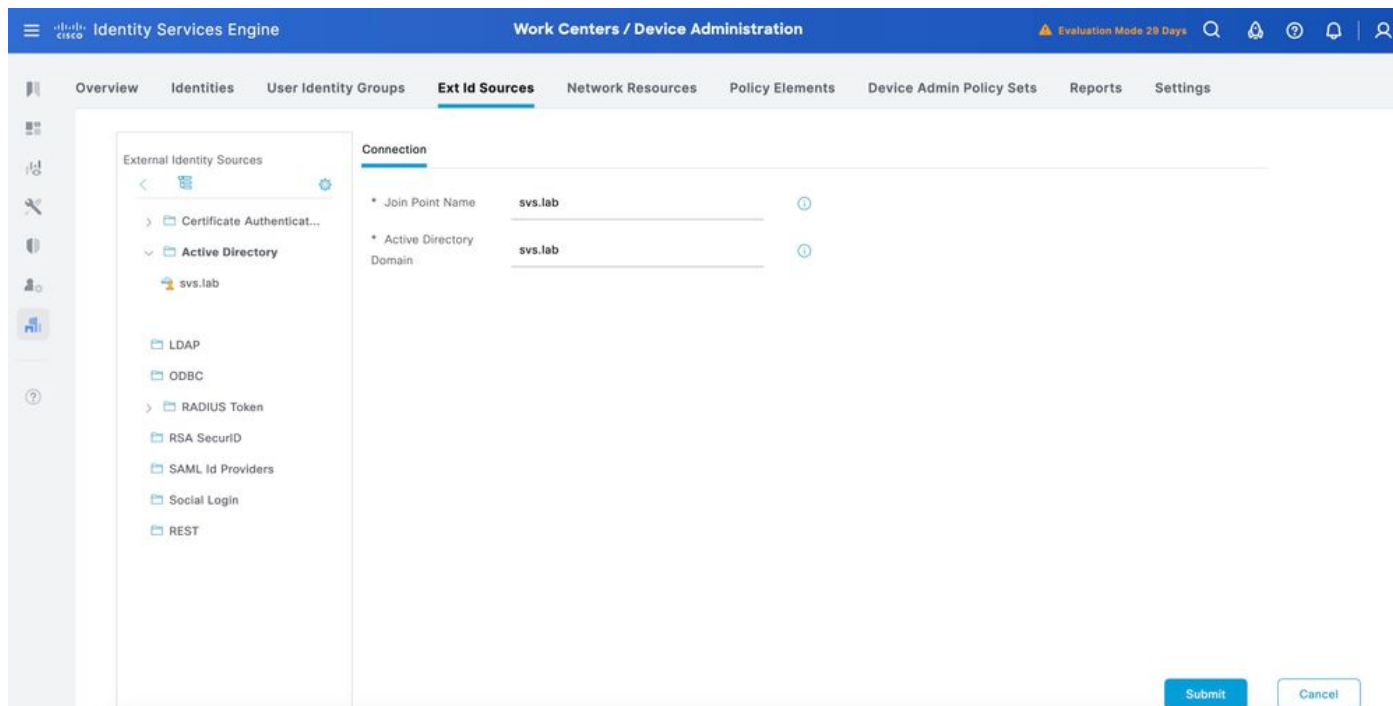
Identiteitswinkels configureren

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?"



Information

Would you like to Join all ISE Nodes to this Active Directory Domain?

No

Yes

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.



Join Domain

Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

* AD User Name ⓘ administrator

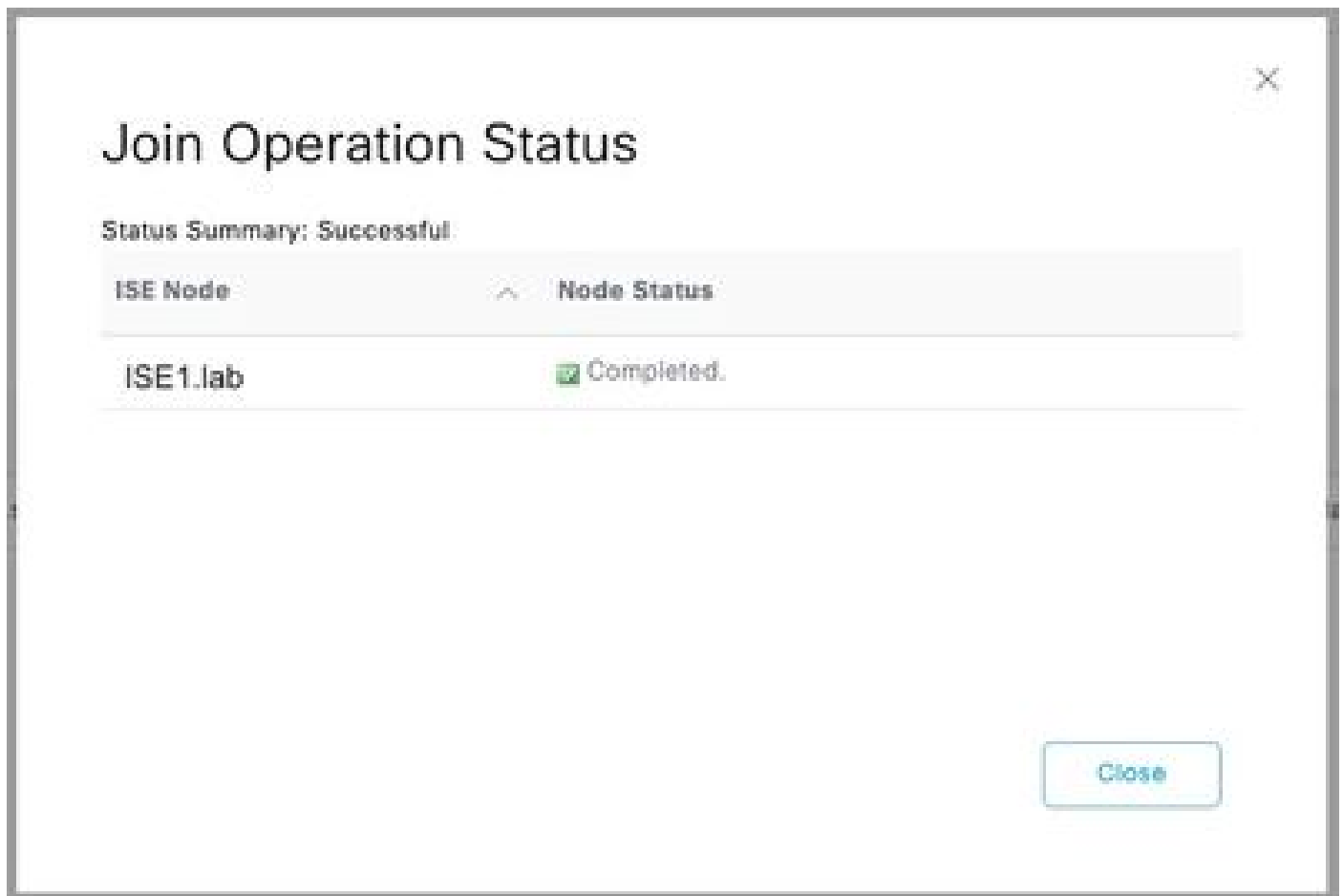
* Password

☐ Specify Organizational Unit ⓘ

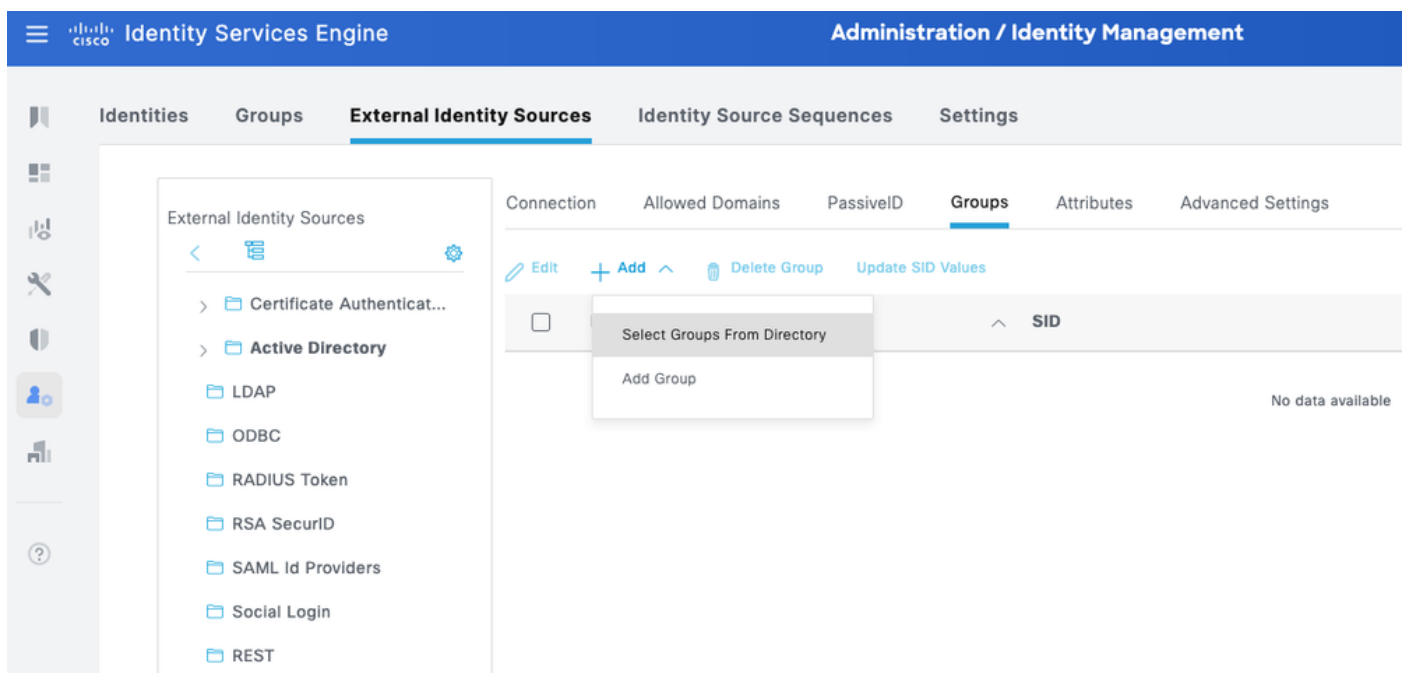
☒ Store Credentials ⓘ

Cancel

OK



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.



Select Directory Groups

This dialog is used to select groups from the Directory.

Domain svs.lab

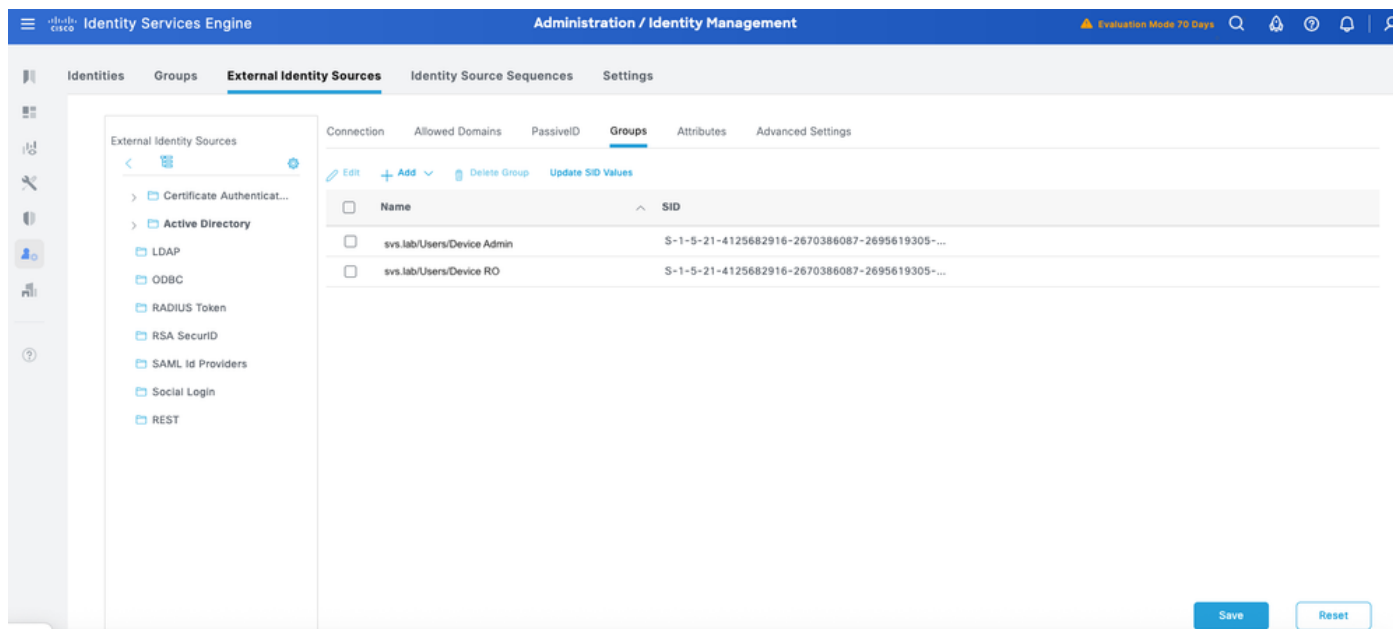
Name
Filter Device *

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+ 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 Netwerkkrol onder Algemene taken.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine' and 'Work Centers / Device Administration'. The left sidebar shows a tree view with 'Policy Elements' selected. The main content area is titled 'TACACS Profiles > NXOS_Admin_Role' and 'TACACS Profile'. It contains a form with the following fields:

- Name:** NXOS Admin
- Description:** (Empty text box)
- Task Attribute View / Raw View:** (Tabs)
- Common Tasks:**
 - Common Task Type:** Nexus (dropdown)
 - Set attributes as:** Mandatory (dropdown)
 - Network role:**
 - ☐ None
 - ☐ Operator (Read Only)
 - ☒ Administrator (Read Write)
 - VDC role:**
 - ☒ None
 - ☐ Operator (Read Only)
 - ☐ Administrator (Read Write)

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

NX-OS HelpDesk

Stap 1. Navigeer vanuit ISE UI naar Werkcentra > Apparaatbeheer > Beleids-elementen > 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 Netwerkkrol onder Algemene taken.

The screenshot shows the 'Policy Elements' configuration page in the Cisco ISE 'Work Centers / Device Administration' section. The left sidebar contains navigation links: Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements (selected), Device Admin Policy Sets, Reports, and Settings. The main content area is titled 'TACACS Profile' and shows the configuration for a TACACS Profile. The 'Name' field is set to 'NXOS HelpDesk'. The 'Description' field is empty. Below the description, there are tabs for 'Task Attribute View' and 'Raw View'. Under 'Common Tasks', the 'Common Task Type' is set to 'Nexus'. The 'Set attributes as' dropdown is set to 'Optional'. The 'Network role' is set to 'Operator (Read Only)'. The 'VDC role' is set to 'None'.

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.

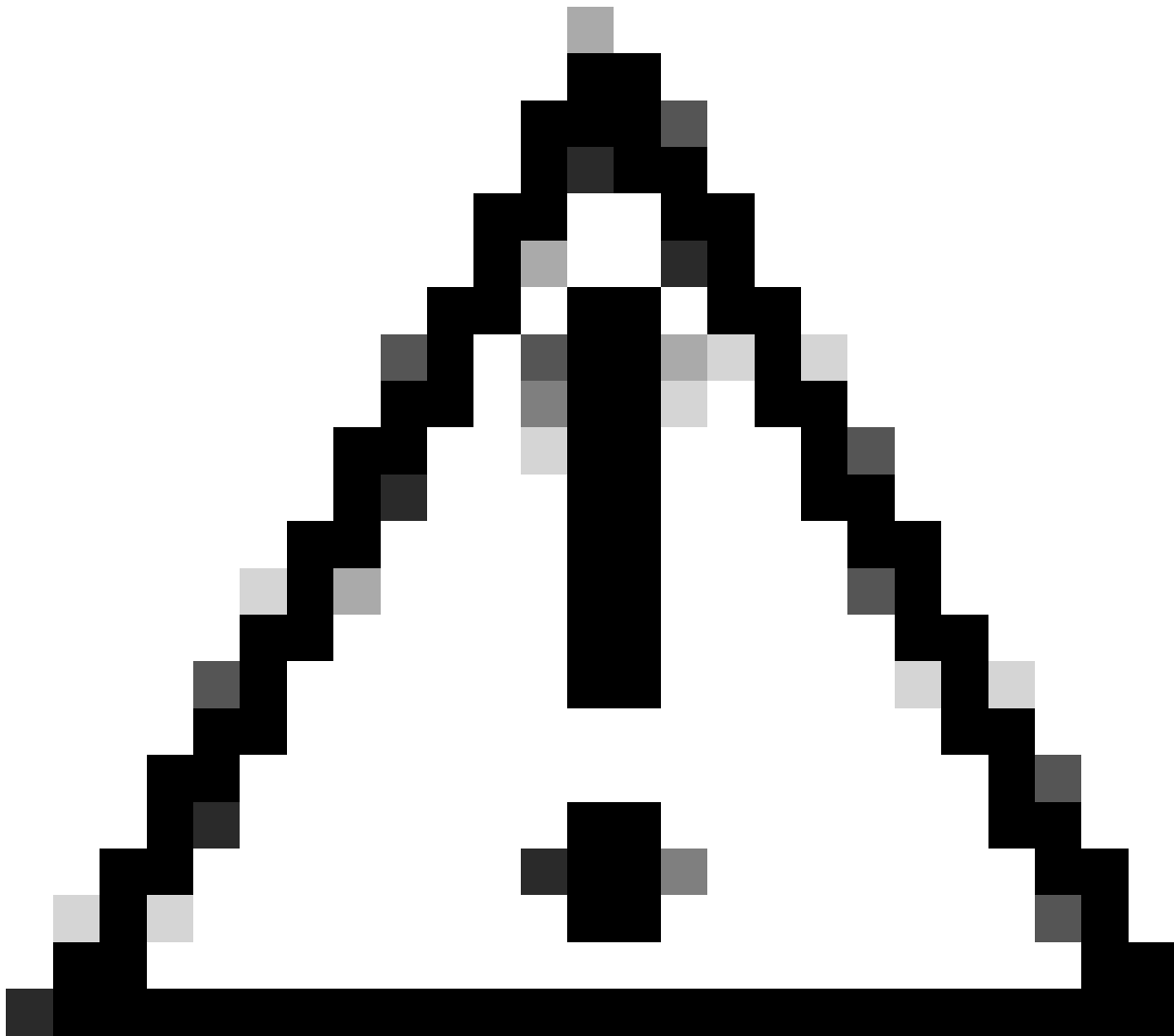
The screenshot shows the 'Device Admin Policy Sets' configuration page in the Cisco ISE 'Work Centers / Device Administration' section. The left sidebar contains navigation links: Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements, Device Admin Policy Sets (selected), Reports, and Settings. The main content area is titled 'Policy Sets' and shows a table of policy sets. The table has columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, Hits, Actions, and View. There is a search bar and a 'Reset' button. The table contains one row with the following data:

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
On	NX-OS Devices		DEVICE-Device Type EQUALS All Device Types#NXOS	Default Device Admin	0		

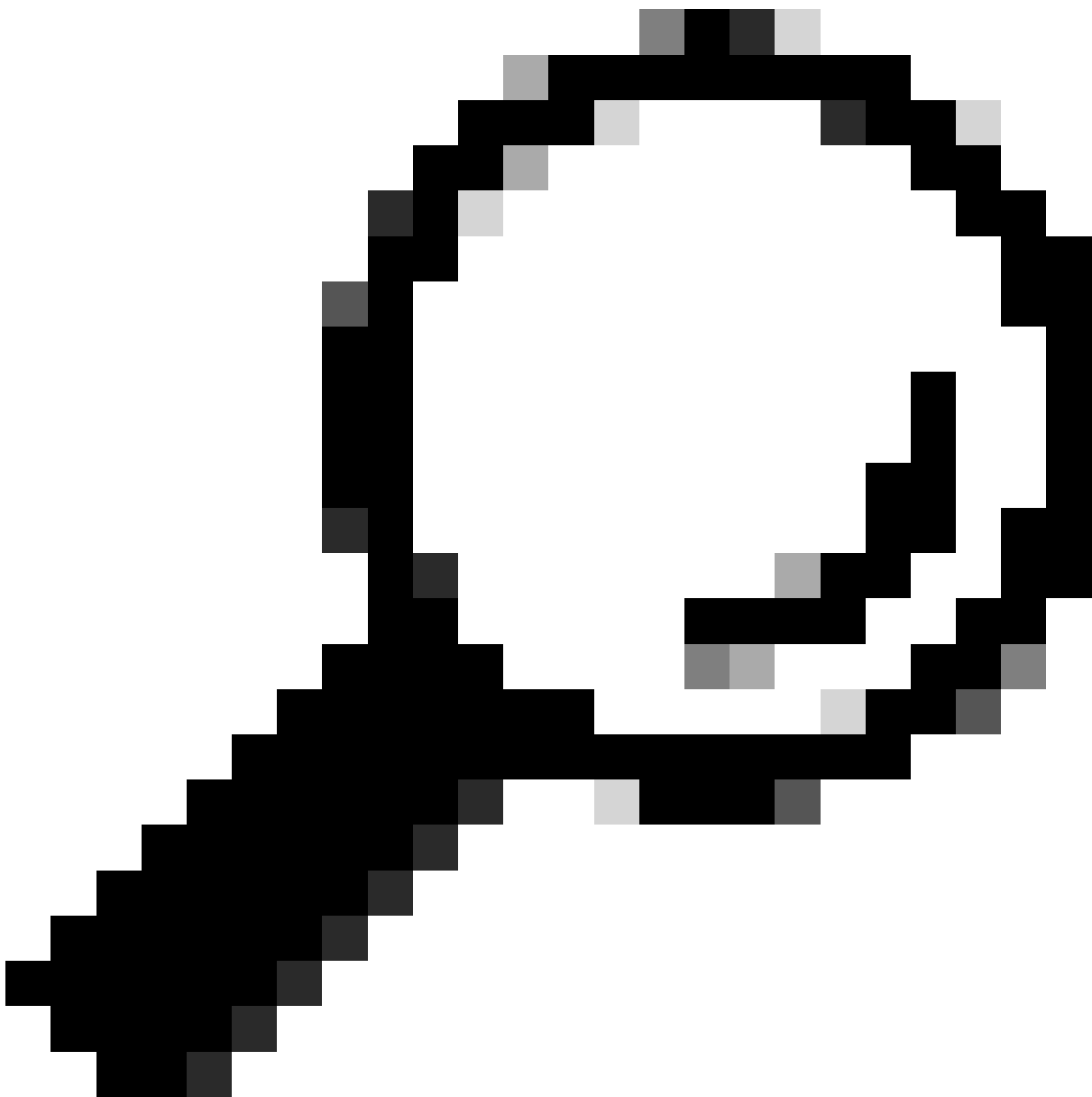
Stap 2. Klik op Opslaan en klik op de rechterpijl om deze beleidsset te configureren.

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.

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-----
MIIFlDCCA3ygAwIBAgIIIM10AsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZzAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECjMDU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNDI4MTcwNTAwWhcNMjUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUUA1UECBM0Tm9ydGggQ2Fyb2xpbmExEDAOBgNVBACTB1JhbGVpZ2gxDjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTV1MxEjAQBgNVBAMTCVNWUyBMWJJDQTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZU0yn2vIn6gKbx3M7vaRq
2YjwZ1zSH6EkEvxnJT+y+kksiFD33GyHQepk7vfp4NFU50tQ4HC7t/A0v9grDa3QW
VvwV4MBbJhFM3s0J/ejgDYcMZhIAaPy0Zo5WLboOkXEiKjPLatkXojB8FVrhLF3O
jMBSqwa4/Wlniy5S+7s4FFxsCf20COWfBAsnrs0tatIIhmcnx+VLJP7MRm8f0w4m
mutNo7IhbJSrgAFXmj1bBjMmgspObULO/wxMHdTbtPBf11HRHTkNIo3qy04UADL2
WpoGhgT/FaxxBo2UBCnYVaP+jjREONYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
```

```
+qh23SL43uW5A3iSw/BuU1E9p7B0e8oDNKU6gX1ojKyLP/gC7j8AeP03ir+KZui8
b8X4iYn/67SbZfFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVpL334rTIxy9hpKZIKB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTA01xh60I4QnK+MNQKpTjt/E4
ydH10rrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVL1783nTc9wYptQEPi5sw
83g9EMgKV0ARIiVUa/q1AgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAyb4
QgEBBAAQDAgAHMBkGCWCGSAGG+EIBDQQMFGpTVlMgTGFIEENBMAOGCSqGSIb3DQEB
CwUAA4ICAQAIT308oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oK0dGayi
iSEkSSX9qyfLFINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
O+ja6zTQqj06lqJhmrSkyFbYf/ZTpe4d10zJsZjNsN0r8bF9nOA/7qNZLp3Z3cpU
PU0KdbiSvRqnPw3e8TFITVmAzcX8COI2SrYFMSUazo1VBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7a1uJapXkmnj5qPeGhN0pB
Q9r14reov4so2EspkXS7CrH9yGfpIyTprokz1UvZBZ8v1oI7YZmjFmem+5rT6Gnk
eU/1X7nV61SYG5W5K+I8uaKuyBHOMn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggz1POdsS/i6Lo7ypYX0eB9HgVDckzQsLXQuHGj/2WsgPgDRcjkvnyURk4Jx+Ib
xDrmo7e0XPpSW4172a6K18CR3U2Cr4wsuvndPEq/qd2NRSBWffFOX/AJHQG7STT
HaXLU9r2Ko603oecu8ysGTWl1It/9T1/F0b0xZRugWcpJrVoTgDGuA==
-----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:Cisco.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: FD026490P4T

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-----

```
MIIBtjCCARcCAQAwKTERMA8GA1UEAwIUE9EMk1QTjIxFDASBgNVBAUTC0ZETzI2
NDkwUDRUMIGbMBAGByqGSM49AgEGBSuBBAAjA4GGAAQBGYT0iw7OvqIKQ/a22Lkg
Na9IhqWQvetjxKq485gqTSBEo6Lzpk0hPAGE4jBveNHxYeIA7PfNWvJ7xTBWjDNX
/IYBm6E7Hd7q420mCe8Mef+bqJBdJ9wzpyEjhI21IIoXt4814nBx0bkIWWyR5cZN
IiXtLk8P4IMZvPq8jRnELRxd8RGgSTAYBgkqhkiG9w0BCQcxCwwJQzFzY28uMTIz
MCOGCSqGSIb3DQEJDDjEgMB4wHAYDVR0RAQH/BBIwEIIIIUE9EMk1QTjKHBArh/bEw
CgYIKoZIZj0EAWIDgYwAMIGIAkIAtzQ/knrW2ovCvoHAuq1v2cr0n3NenS/441u1
+3H1y52vn4Rm4CGU3wkzXU3qG03YjhNjCXjhp3+uN2afFf1Wf3ECQgC4bumHVsfj
b5rwPIC5tvXS/A8upqIzqc0yt30hpaDDOTWzzvZY7qFf1C015p6pvUpHiqqoZNg5
9xhNdM1CQSyk0g==
```

-----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
BhMCVVMxZmFzAVBgNVBAGTDk5vbnR0IENhcm9saW5hMRAwDgYDVQQHEwdSYWx1aWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECXMdu1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNTA3MTkxMDAwWhcNMjUwNTA3MTkxMDAwWjApMREwDwYDVQQDDAhQ
TOQySVBOMjEUMBIGA1UEBRMLRkRPMjY0OTBQNFQwgZswEAYHKoZIzj0CAQYFK4EE
ACMDgYYABAEZhpSLDs6+ogpD9rbYuSA1r0iGpZC962PEqrjzmCpNIESjovOmQ6E8
AYTiMG940fFh4gDs981a8nvFMFAmM1f8hgGboTsd3urjY6YJ7wx5/5uokF0n3DOn
ISOEjaUgihe3jzXiCHE5uQhZbJH1xk0iJdMuTw/ggxm8+ryNGCQtHF3xEaNAMD4w
HgYJYIZIAyb4QgENBBEWD3hjYSBjZXJ0aWZpY2F0ZTAwBgNVHREBAf8EEjAQgghQ
TOQySVBOMocECuH9sTANBgkqhkiG9w0BAQsFAAOCAgEANWGb6zm9TDPaM1yhPMx7
8uai/pF7VQC8NSCdOKqr4w4+695ZjJuzqFL3msodOQK0EdgxpQ4+pEa5msRtK0i8
mms2X/Px3/EShxoHrZ01PUXNTyZidXpGd/yTrdQA15JzpW4pEudrbCJMZEYtqoP
wD+40E8vKoYEgyWlDrpRZ0ZG1usZczUUhLZ8orkjXMhWC26Q5aqiCKkyg10Nt6nb
1iToeYy2Q0cTesSZCKvRBv6Ewj5JuSLeMURyB4GHY+LT+A9UNmEUM2n+OSVEL329
3hS0qd/YVaEuxjjlg7jNiZb+UsW7IRx3Q8Rouo++ISACpH/PJ61Ln1VxhXombiS6
INoaOGvQONr1+lFT8ADIdZ/Ukd5Ubhc9bh/sYzf4MwtKk1wV016Hv7vGpSMYonD6
a271im+tJPyKneezQ60yKz1GqsL/Ta6J0dip/fEYp8UmRq9InDh23gDjqrojl7k
1R/bZpc+baMYXd/2pohHMSN0sKN3zNrJT1nuk5KCqFx//4P7mAoyZYiTIDp1pkYS
```

```
VK65fJKD+pYxIhSP9wN8rnwtzSCWb0Z78sg006Y6wIXyTP0UB3FWhD+GxtTkmEce
ZnAQbgxpgrg5lhpAEVabpC/zRU4UzTuBmv/WoY12zwXCr5WLXEOWtIe8CwFjSnch
1fKuuebdZkbwz72r70yyX/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 = FD026490P4T
```

```
issuer=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
```

```
serial=0BACD2EFA5D80E6F
```

```
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=20CD7402C4DA37F5
```

```
notBefore=Apr 28 17:05:00 2025 GMT
```

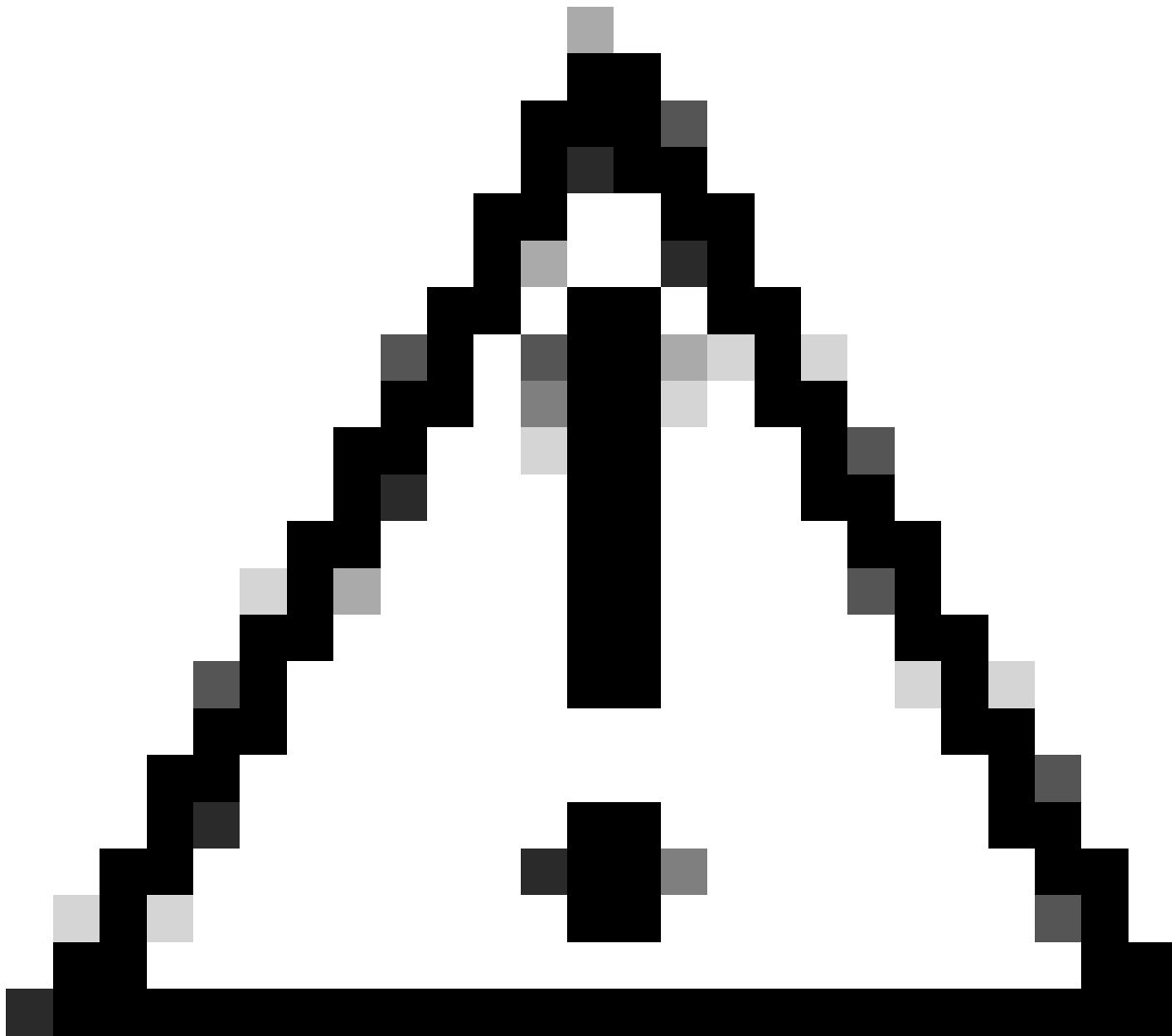
```
notAfter=Apr 28 17:05:00 2035 GMT
```

```
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)#
```

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.

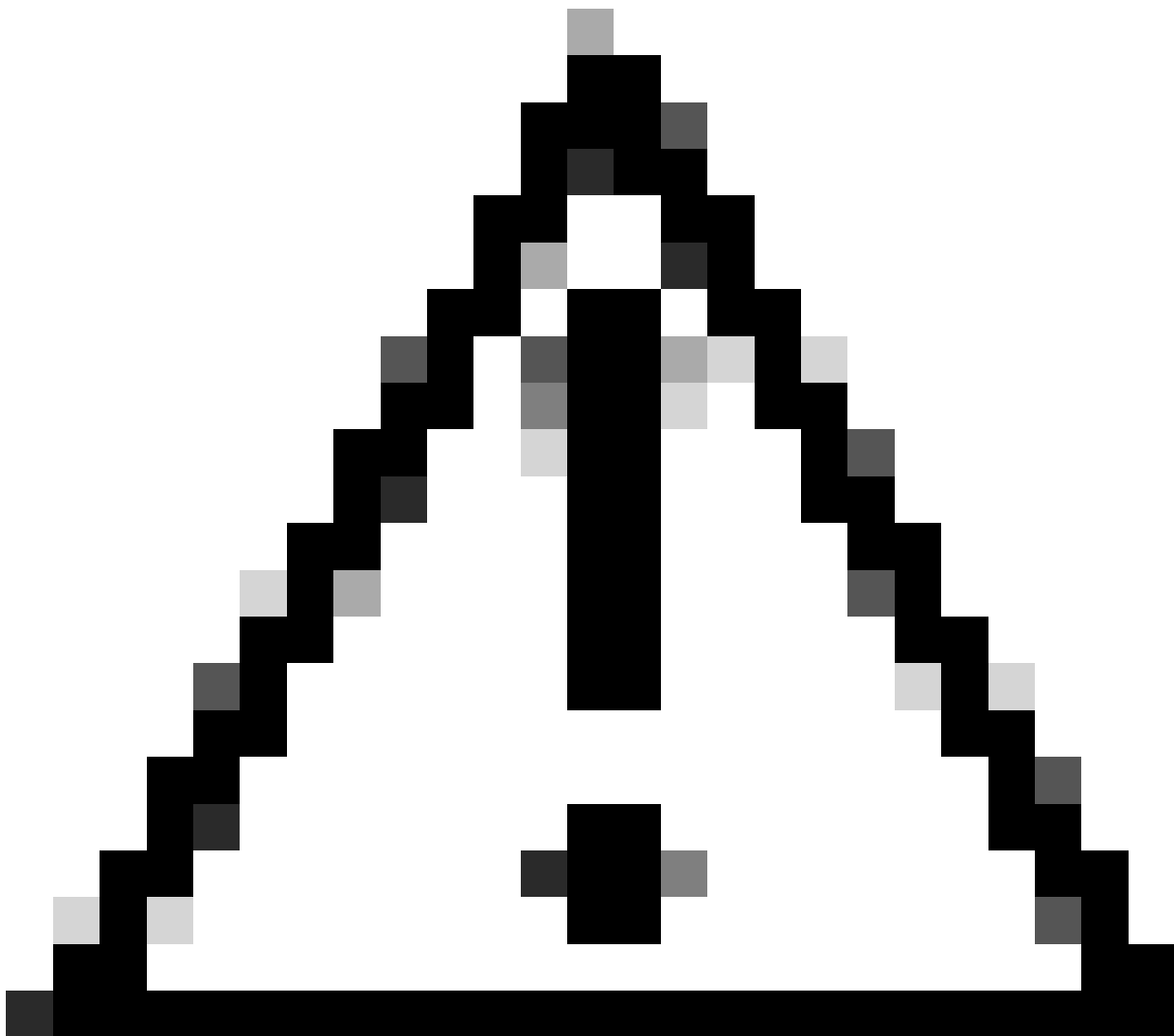
```
<#root>
```

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.

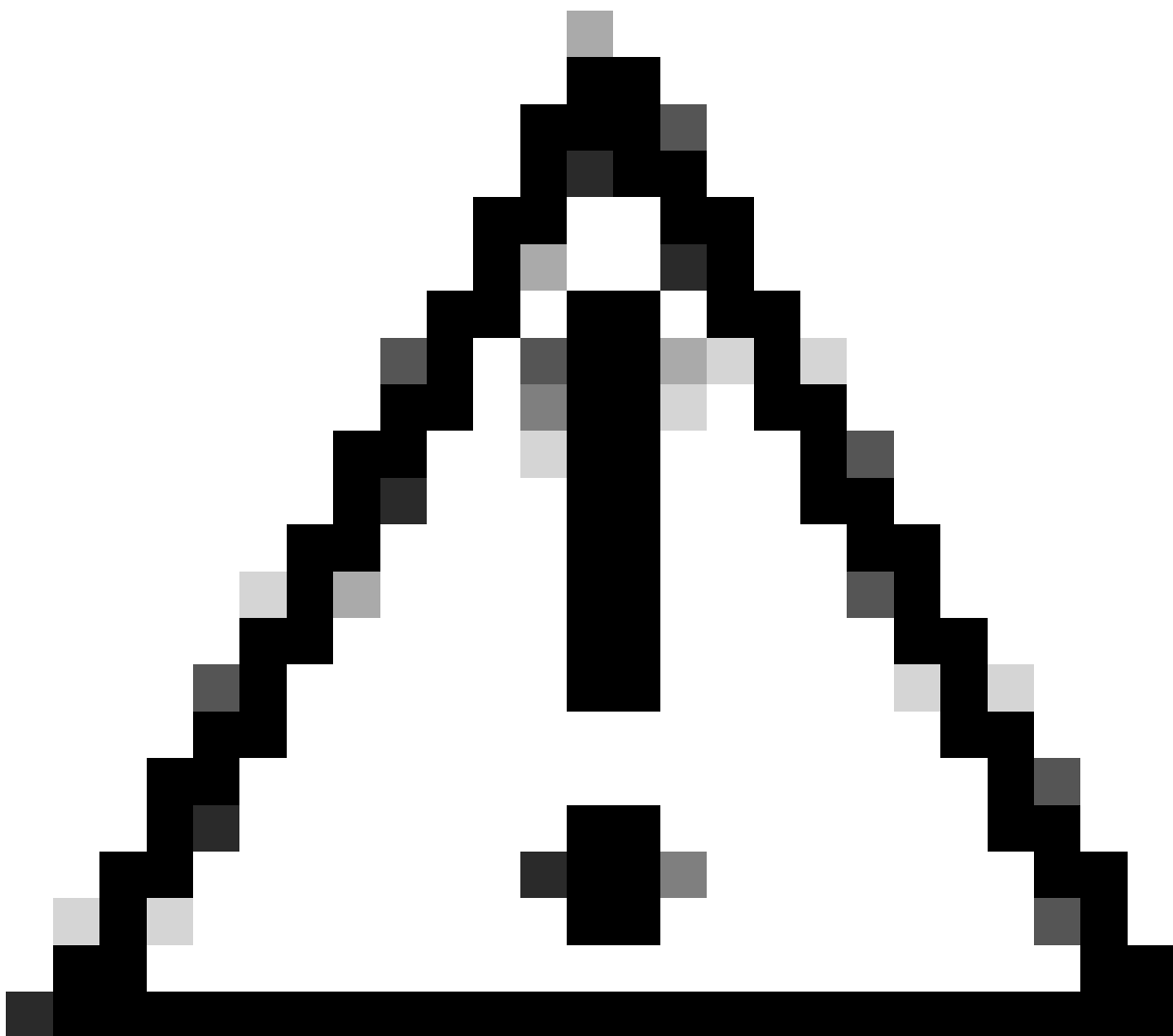
Stap 1. Configureer AAA-verificatie op afstand.

```
<#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.

Identity Services Engine

Operations / TACACS

Evaluation Mode 80 Days

Live Logs

Refresh

Every 10 sec...

Show

Latest 20 reco...

Within

Last 3 hours

Export To

Filter

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Devic...	Network Dr
			Identity		Authentication Policy	Authorization Policy	Ise Node	Network Device Ni	Network Dev
May 15, 2025 07:39:57.081 PM			Admin-ro	Authorization		Test NXOS >> Authorization Rule RO	ISE1	POD2IPN1	10.225.253.1
May 15, 2025 07:39:57.061 PM			Admin-ro	Authentication	Test NXOS >> Default		ISE1	POD2IPN1	10.225.253.1
May 15, 2025 07:39:54.462 PM			pamemart	Authorization		Test NXOS >> Authorization Rule RW	ISE1	POD2IPN1	10.225.253.1
May 15, 2025 07:39:54.443 PM			pamemart	Authentication	Test NXOS >> Default		ISE1	POD2IPN1	10.225.253.1

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

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

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	Failure
X Today X			Identity	Authentication Policy	ISE Node	Network Device Name	Network Device IP	Failure
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.