

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

Inhoud

[Inleiding](#)

[Overzicht](#)

[Gebruik van deze Guide](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[vergunning](#)

[Deel 1 - ISE-configuratie 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](#)

[Netwerkapparaat- en netwerkapparaatgroepen maken](#)

[Identiteitswinkels configureren](#)

[TACACS+-profielen configureren](#)

[IOS XR_RW - Beheerdersprofiel](#)

[IOS XR_RO - Gebruikersprofiel](#)

[TACACS+-opdrachtreksen configureren](#)

[CISCO IOS XR RW - Opdrachtset voor beheerders](#)

[CISCO IOS XR RO - Operator Command Set](#)

[Apparaatbeheerbeleidsets configureren](#)

[Deel 2 - Cisco IOS XR configureren voor TACACS+ ten opzichte van TLS 1.3](#)

[Initiële configuraties](#)

[Trustpoint configureren](#)

[TACACS & AAA configureren met TLS](#)

[Certificaatvernieuwing](#)

[Verificatie](#)

[Probleemoplossing](#)

Inleiding

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

Overzicht

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

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

Gebruik van deze Guide

Deze handleiding verdeelt de activiteiten in twee delen zodat ISE beheerderstoegang kan beheren voor Cisco IOS XR-gebaseerde netwerkapparaten.

- Deel 1 – Configureer ISE voor Apparaatbeheer
- Deel 2 - Cisco IOS XR configureren voor TACACS+ via TLS

Voorwaarden

Vereisten

Vereisten voor het configureren van TACACS+ via TLS:

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

Gebruikte componenten

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

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

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

vergunning

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

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

Deel 1 - ISE-configuratie voor apparaatbeheer

Aanvraag voor certificaatondertekening genereren voor TACACS+-serververificatie

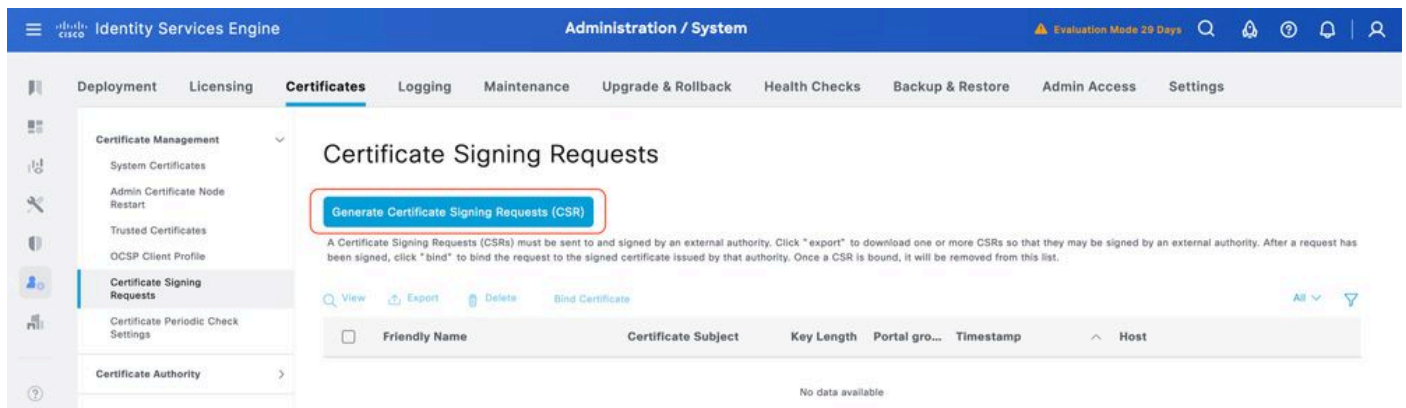
Stap 1. Meld u aan bij de ISE-beheerdersportal met een van de ondersteunde browsers.

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

Stap 2. Ga naar Beheer > Systeem > Certificaten.



Stap 3. Klik onder Certificaatondertekeningsverzoeken op Certificaatondertekeningsverzoek genereren.



Stap 4. Selecteer TACACS in gebruik.

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)

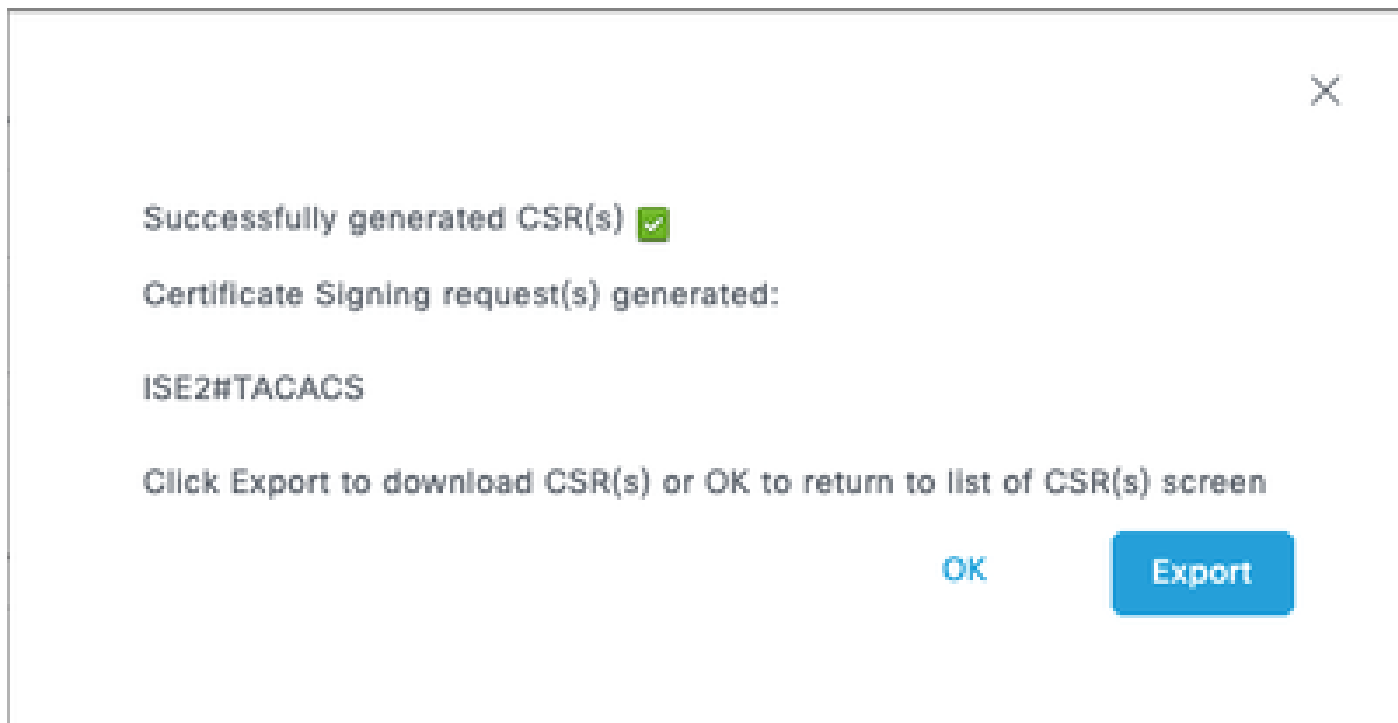
US

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	−	+	①

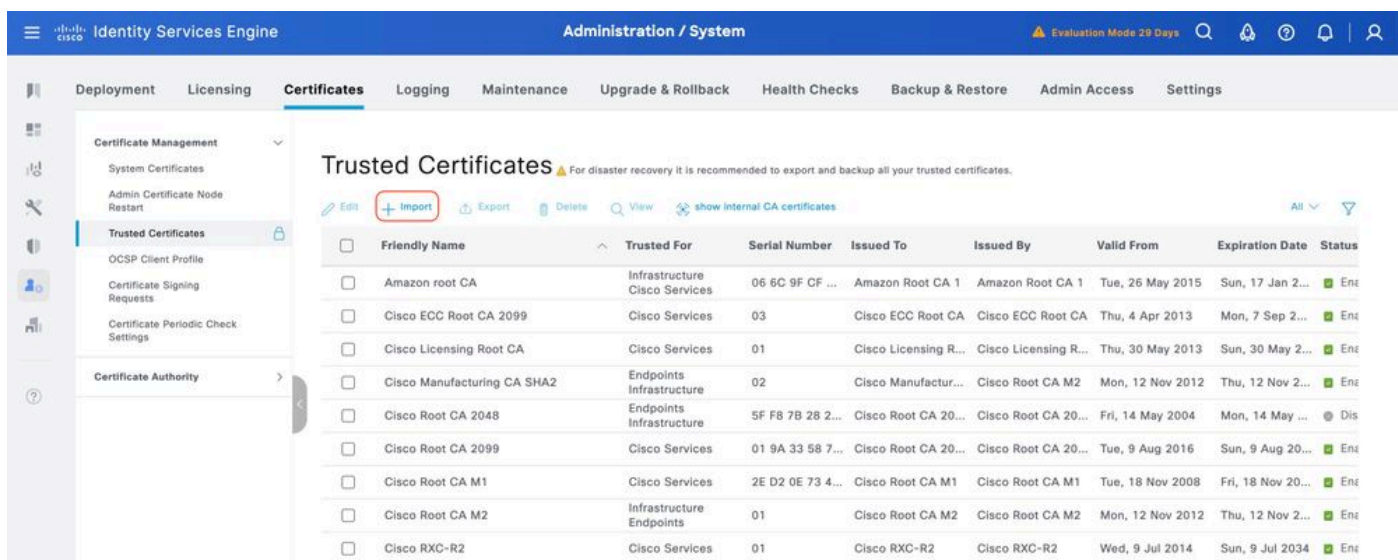
Stap 8. Klik op Genereren en vervolgens op Exporteren.



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

Root CA-certificaat uploaden voor TACACS+-serververificatie

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



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

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.

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...	

Het ondertekende certificaatondertekeningsverzoek (CSR) binden aan ISE

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

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

Generate Certificate Signing Requests (CSR)

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

View Export Delete Bind Certificate

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

Friendly Name

Validate Certificate Extensions ☐

Usage

☒ TACACS: Use certificate for TACACS Server

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?

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=I SE1.lab#ISE1.lab#000010	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. Navigeer naar Beheer > Systeem > Instellingen.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The left sidebar contains the following menu items: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (highlighted), Work Centers, and Interactive Help. The main content area shows the 'Deployment' tab selected, with a dropdown menu open. The dropdown menu lists the following options: Client Provisioning, FIPS Mode, Security Settings, Alarm Settings, System, Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade & Rollback, Health Checks, Backup & Restore, Admin Access, and Settings (highlighted with a checkmark).

Stap 2. Klik op Beveiligingsinstellingen, selecteer het selectievakje naast TLS1.3 onder Versie-instellingen 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

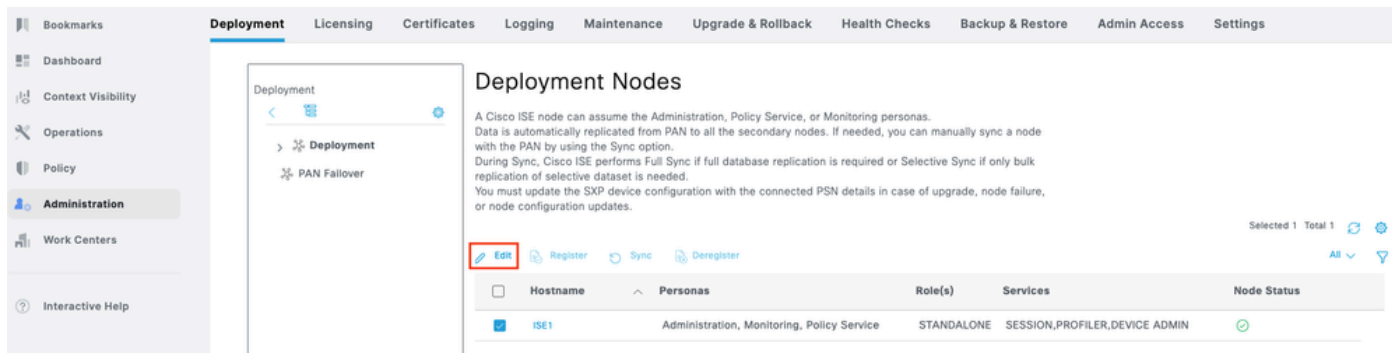


Waarschuwing: wanneer u de TLS-versie wijzigt, wordt de Cisco ISE-toepassingsserver opnieuw gestart op alle Cisco ISE-implementatiemachines.

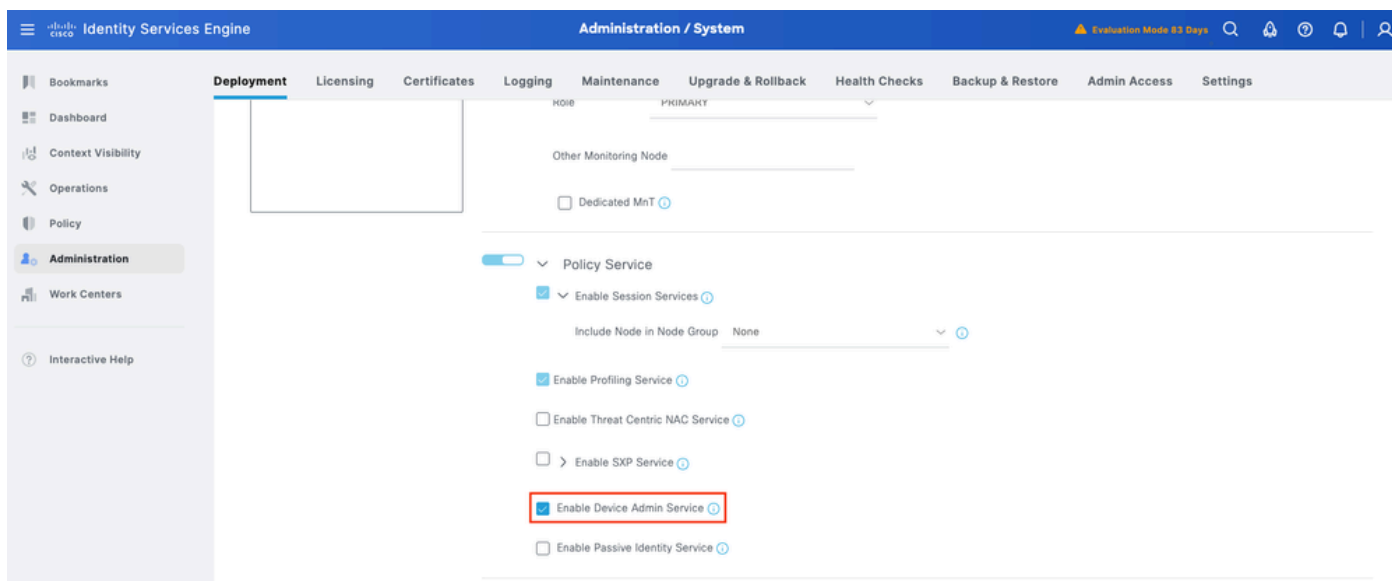
Apparaatbeheer inschakelen op ISE

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

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



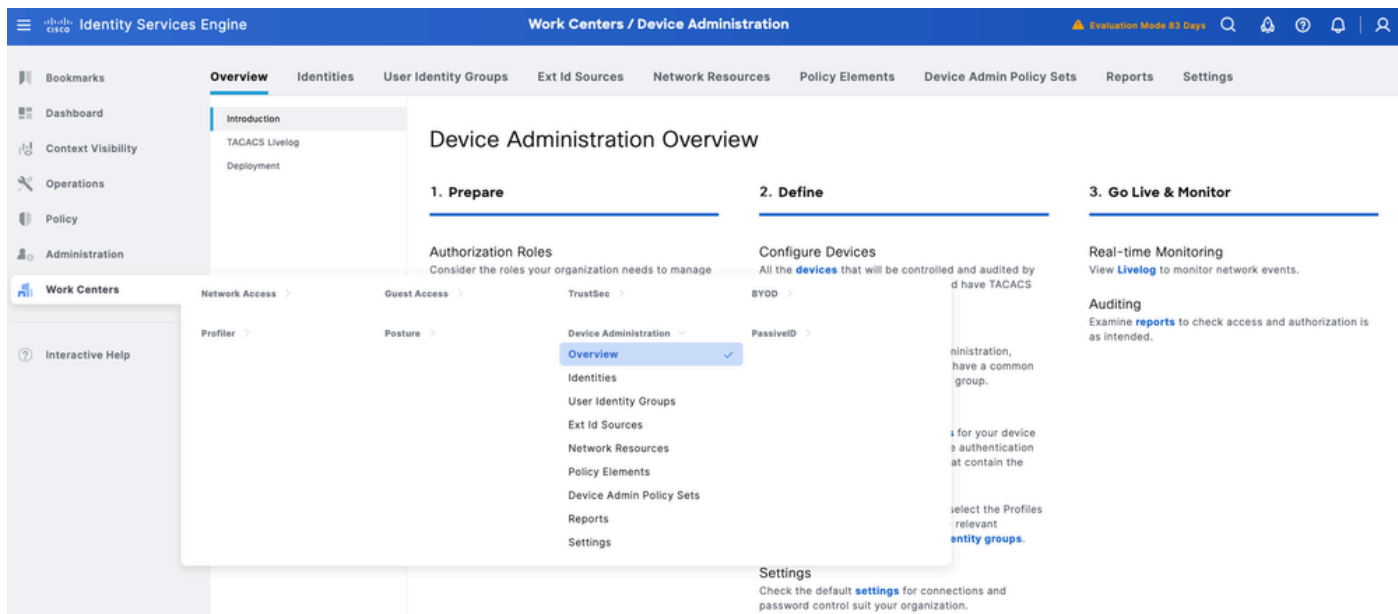
Stap 2. Blader onder Algemene instellingen omlaag en schakel het selectievakje naast Apparaatbeheerservice inschakelen in.



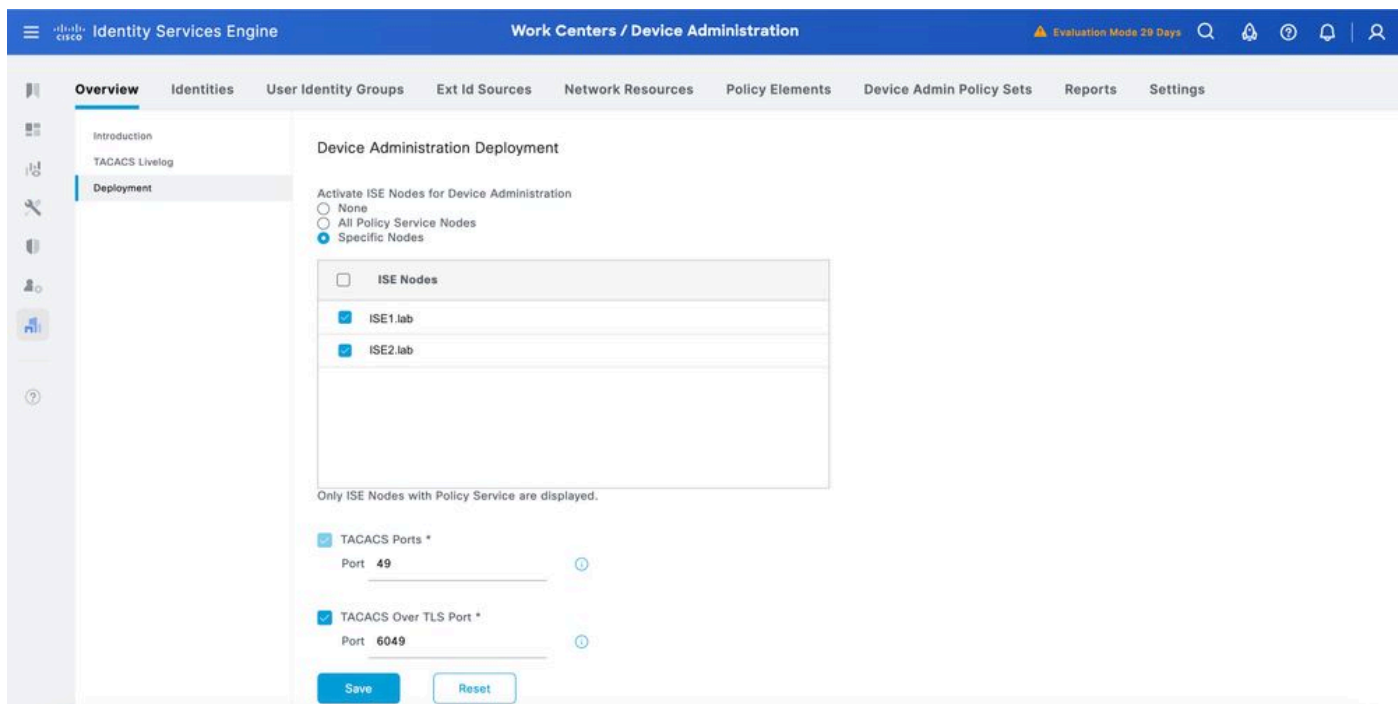
Stap 3. Sla de configuratie op. Device Admin Service is nu ingeschakeld op ISE.

TACACS via TLS inschakelen

Stap 1. Navigeer naar werkcentra > Apparaatbeheer > Overzicht.



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



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

Netwerkkapparaat- en netwerkkapparaatgroepen maken

ISE biedt krachtige apparaatgroepering met meerdere apparaatgroep hiërarchieën. Elke hiërarchie vertegenwoordigt een afzonderlijke en onafhankelijke classificatie van netwerkkapparaten.

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

Identity Services Engine

Work Centers / Device Administration

Resolution Mode 93 Days

OverviewIdentitiesUsers

Network Devices

Network Device Groups

Default Devices

TACACS External Servers

TACACS Server Sequence

Admin Policy Sets

More

✕

Edit Group

Name*

IOS-XR

Description

Group Hierarchy

Device Type > All Device Types > IOS-XR

Cancel

Save

ADVA

ADVA SyncDirector Network Time Monitoring

No. of Network Device

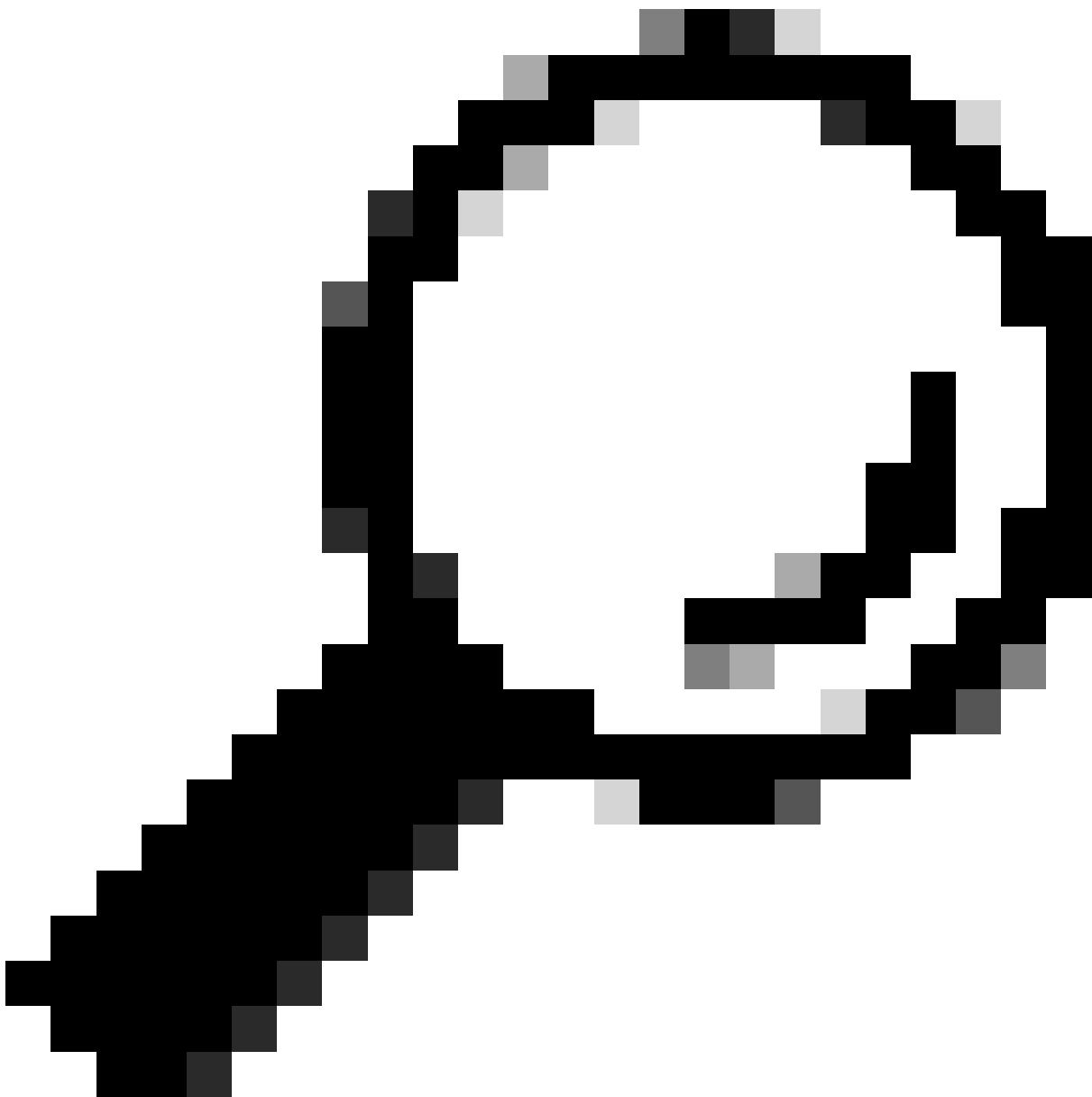
--

702

0

11

243



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

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

Identity Services Engine Administration / Network Resources Evaluation Mode 11 Days

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences External MDM pxGrid Direct Connectors

Network Devices List > BRC-8201-1

Network Devices

Name

Description

IP Address * IP: 32

IP Address * IP:

Device Profile

Model Name

Software Version

Network Device Group

Location [Set To Default](#)

IPSEC [Set To Default](#)

Device Type [Set To Default](#)

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

Identity Services Engine Work Centers / Device Administration Evaluation Mode 67 Days

Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Help

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements More

Network Devices

Network Device Groups

Default Devices

TACACS External Servers

TACACS Server Sequence

☐ 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)*

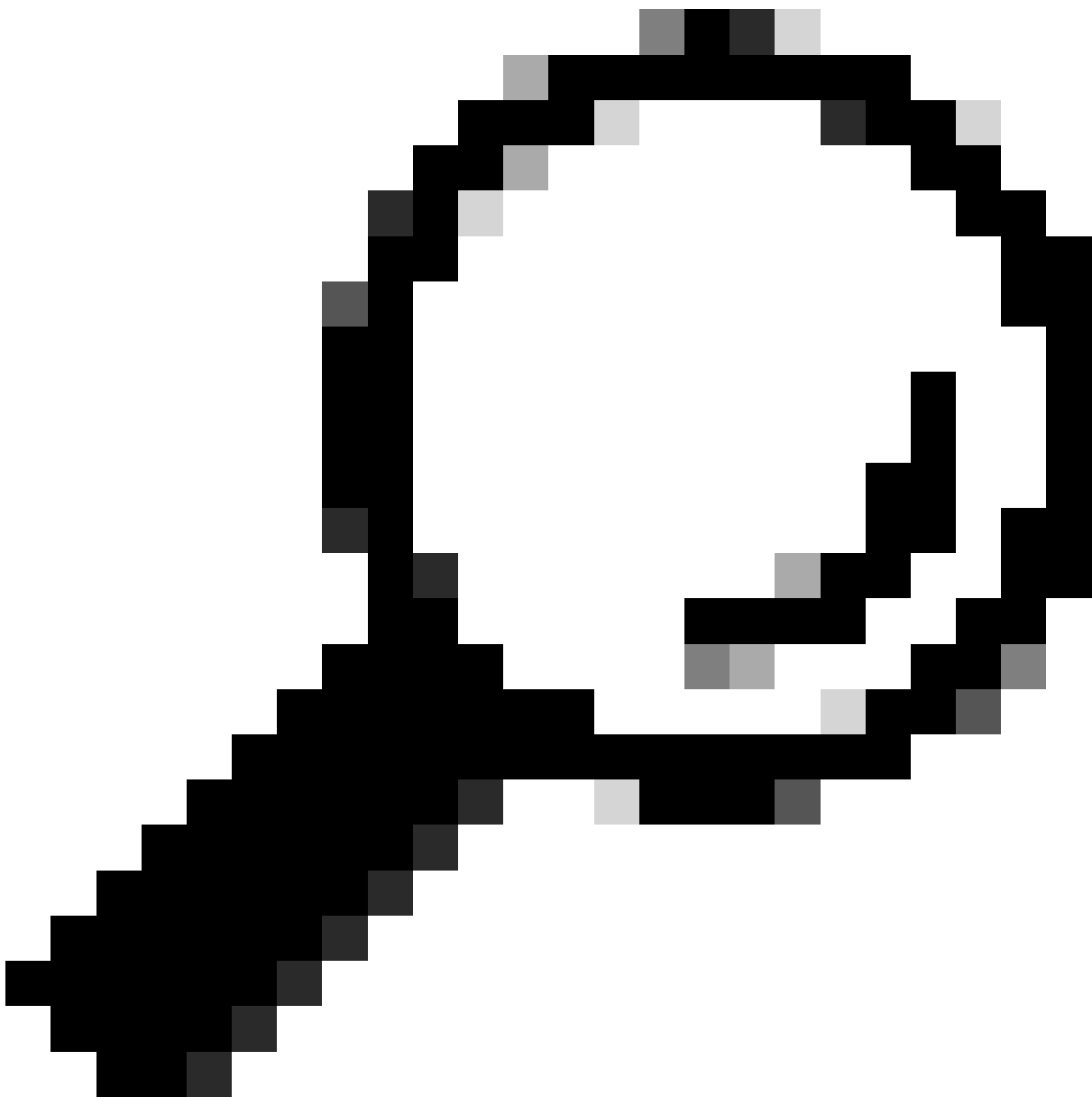
Additional security can be enforced by validating SAN certificate attributes. Cisco ISE supports validating the IP address (IPAddress), DNS Name (dNSName), and Directory Name (directoryName) attributes. The attributes chosen below are evaluated in this order: IP address, DNS Name, Directory Name. When 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

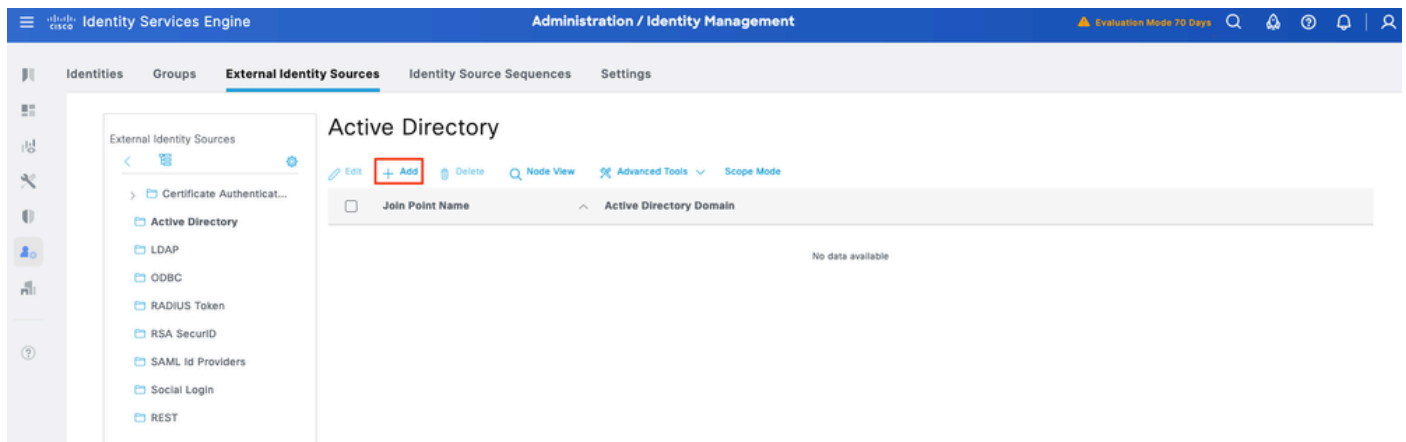


Tip: Het wordt aanbevolen om de modus Single Connect in te schakelen om te voorkomen dat de TCP-sessie opnieuw wordt gestart telkens wanneer een opdracht naar het apparaat wordt verzonden.

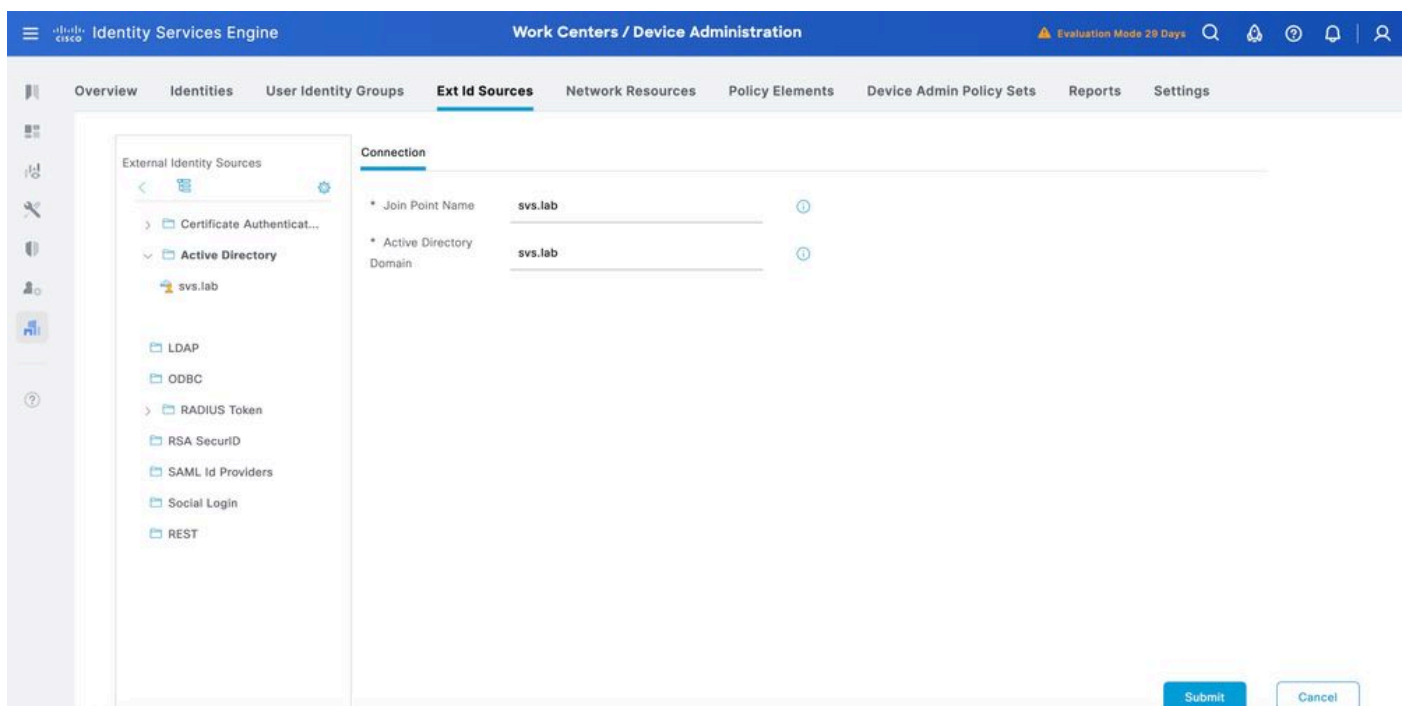
Identiteitswinkels configureren

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

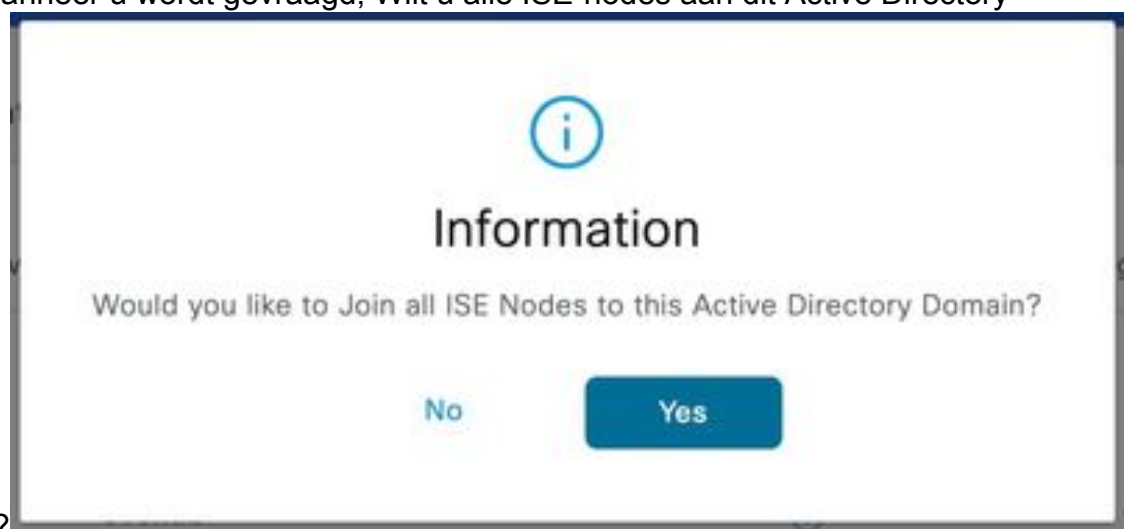
Stap 1. Navigeer naar Beheer > Identiteitsbeheer > Externe identiteitswinkels > Active Directory. Klik op Toevoegen om een nieuw AD-verbindingspunt te definiëren.



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



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



domein toevoegen?

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

×

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

×

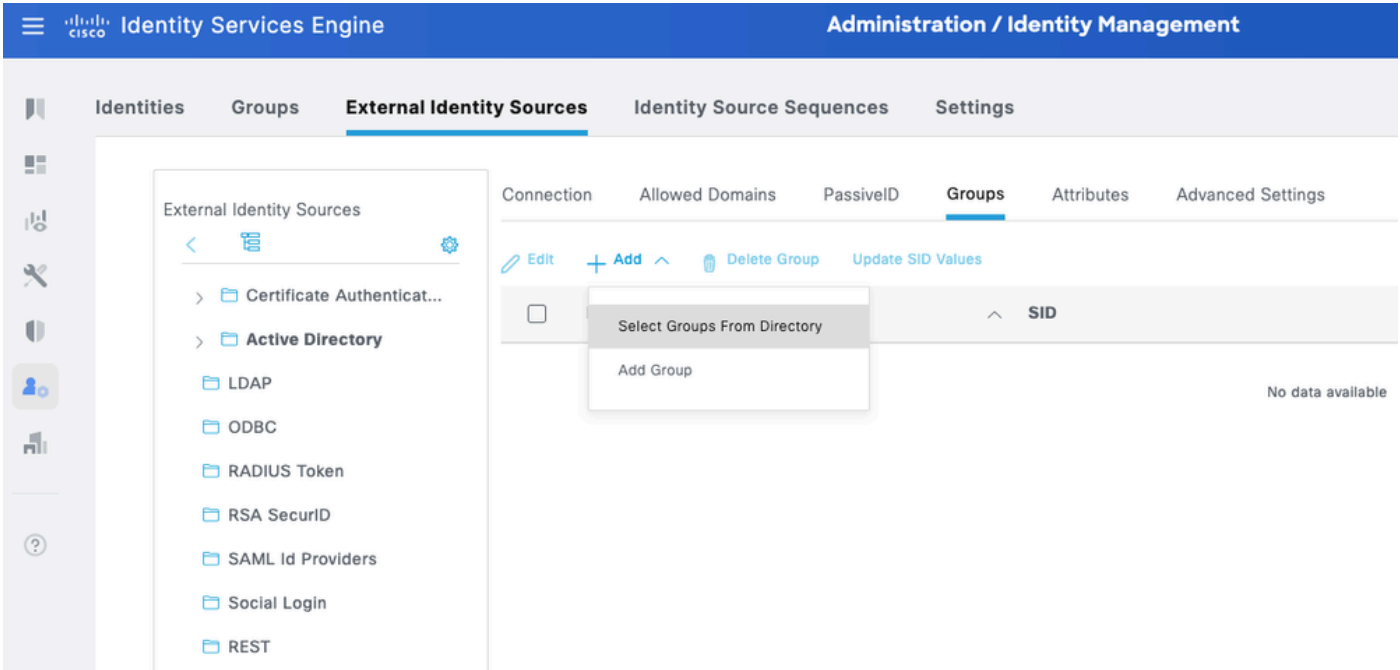
Join Operation Status

Status Summary: Successful.

ISE Node	Node Status
ISE1.lab	✔ Completed.

Close

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



Select Directory Groups

This dialog is used to select groups from the Directory.

Domain

svs.lab

Name

Device *

SID *

Type

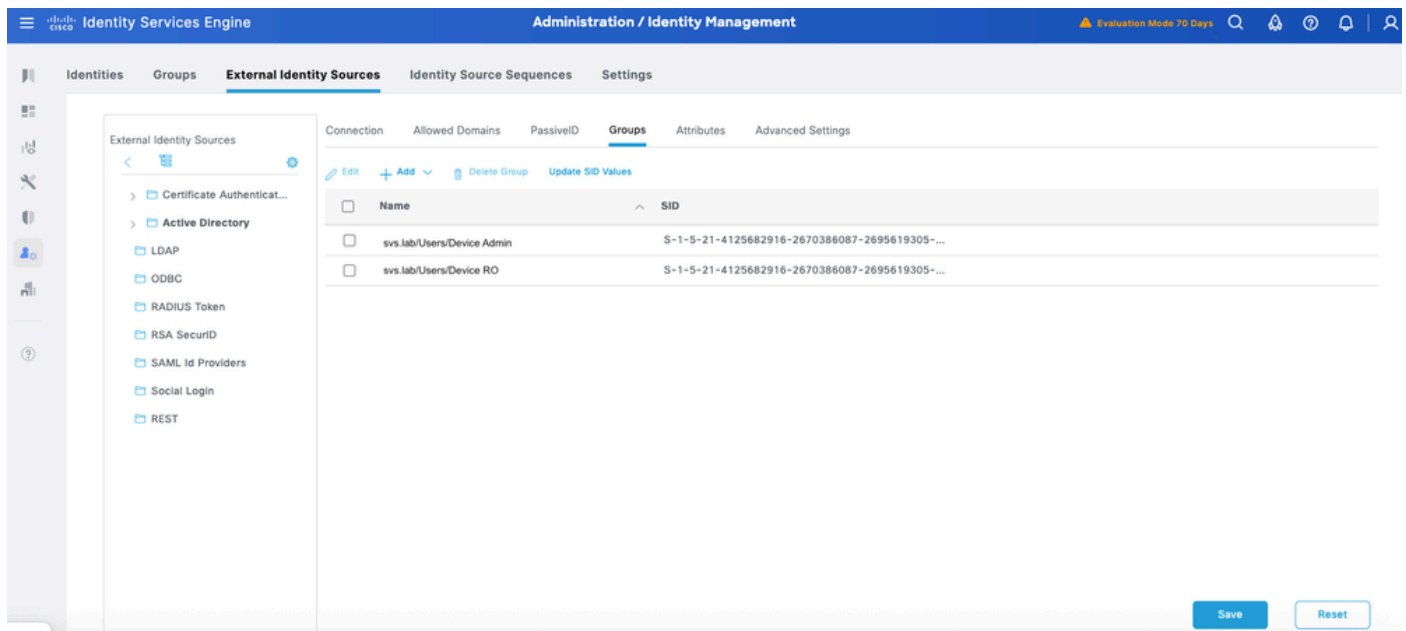
ALL

Filter

Retrieve Groups...

2 Groups Retrieved.

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



TACACS+-profielen configureren

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

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

Definieer twee TACACS+-profielen: IOSXR_RW en IOSXR_RO.

IOS XR_RW - Beheerdersprofiel

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

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

Stap 3. Bevestig de configuratie en sla op.

Identity Services Engine Work Centers / Device Administration Evaluation Mode 63 Days

Overview Identities User Identity Groups Ext Id Sources Network Resources **Policy Elements** Device Admin Policy Sets Reports Settings

TACACS Profiles > IOSXR_RW
TACACS Profile

Name: IOSXR_RW

Description:

Task Attribute View Raw View

Common Tasks

Common Task Type: Shell

☒ Default Privilege 15 (Select 0 to 15)

☒ Maximum Privilege 15 (Select 0 to 15)

☐ Access Control List

☐ Auto Command

☐ No Escape (Select true or false)

IOS XR_RO - Gebruikersprofiel

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

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

Stap 3. Bevestig de configuratie en bewaar.

Identity Services Engine Work Centers / Device Administration Evaluation Mode 62 Days

Overview Identities User Identity Groups Ext Id Sources Network Resources **Policy Elements** Device Admin Policy Sets Reports Settings

TACACS Profiles > New
TACACS Profile

Name: IOSXR_RO

Description:

Task Attribute View Raw View

Common Tasks

Common Task Type: Shell

☒ Default Privilege 1 (Select 0 to 15)

☒ Maximum Privilege 1 (Select 0 to 15)

TACACS+-opdrachtreksen configureren

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

CISCO_IOSXR_RW en CISCO_IOSXR_RO.

CISCO IOS XR RW - Opdrachtset voor beheerders

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

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

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes the Cisco logo, 'Identity Services Engine', and 'Work Centers / Device Administration'. A status indicator shows 'Evaluation Mode 63 Days'. The main navigation menu on the left includes Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements (selected), Device Admin Policy Sets, Reports, and Settings. The 'Policy Elements' section is active, showing a breadcrumb trail: TACACS Command Sets > CISCO_IOSXR_RW. The main content area is titled 'Command Set' and contains the following fields: 'Name' (CISCO_IOSXR_RW), 'Description' (empty text area), and 'Commands'. Under 'Commands', there is a checkbox labeled 'Permit any command that is not listed below' which is checked. Below this, there are links: Add, Trash, Edit, Move Up, and Move Down. A table with columns 'Grant', 'Command', and 'Arguments' is shown, but it is empty with the message 'No data found.' at the bottom. At the bottom right, there are 'Cancel' and 'Save' buttons.

CISCO IOS XR RO - Operator Command Set

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

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

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

Stap 4. Bevestig de gegevens en klik op Opslaan.

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 Command Sets > CISCO_IOSXR_RO Command Set'. It includes fields for 'Name' (CISCO_IOSXR_RO) and 'Description'. Below these is a 'Commands' section with a checkbox for 'Permit any command that is not listed below'. At the bottom, there is a table with columns 'Grant', 'Command', and 'Arguments'. The table contains one entry: 'PERMIT' for the command 'show'. Action buttons 'Add', 'Trash', 'Edit', 'Move Up', and 'Move Down' are located above the table. At the bottom right, there are 'Cancel' and 'Save' buttons.

Apparaatbeheerbeleidsets configureren

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

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

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), and More. The main content area is titled 'Policy Sets'. It includes a 'Reset' button, a 'Reset Policy Set Hit Counts' button, and a 'Save' button. Below these is a table with columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, Hits, Actions, and View. The table contains one entry: 'IOS-XR devices' with a status of 'On'. The 'Conditions' column shows 'DEVICE-Device Type EQUALS All Device Types#IOS-XR'. The 'Allowed Protocols / Server Sequence' column shows 'Default Device Admin'. The 'Hits' column shows '73'. Action buttons 'Edit', 'Add', and 'View' are located to the right of the table entry. At the bottom right, there are 'Cancel' and 'Save' buttons.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
On	IOS-XR devices		DEVICE-Device Type EQUALS All Device Types#IOS-XR	Default Device Admin	73	Edit Add	View

Stap 2. Klik op Opslaan en klik op de rechtermuis 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.

Identity Services Engine Work Centers / Device Administration Evaluation Mode 63 Days

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements **Device Admin Policy Sets** More

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
	IOS-XR devices		DEVICE-Device Type EQUALS All Device Types#IOS-XR	Default Device Admin	73

Authentication Policy(1)

Status	Rule Name	Conditions	Use	Hits	Actions
	Default				

svs.lab

Options ⓘ

If Auth fail
REJECT

If User not found
REJECT

If Process fail
DROP

85

Stap 4. Definieer het autorisatiebeleid.

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

Voorbeeld:

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

Identity Services Engine **Work Centers / Device Administration** ⚠️ Evaluation Mode 62 Days

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements **Device Admin Policy Sets** Reports Settings

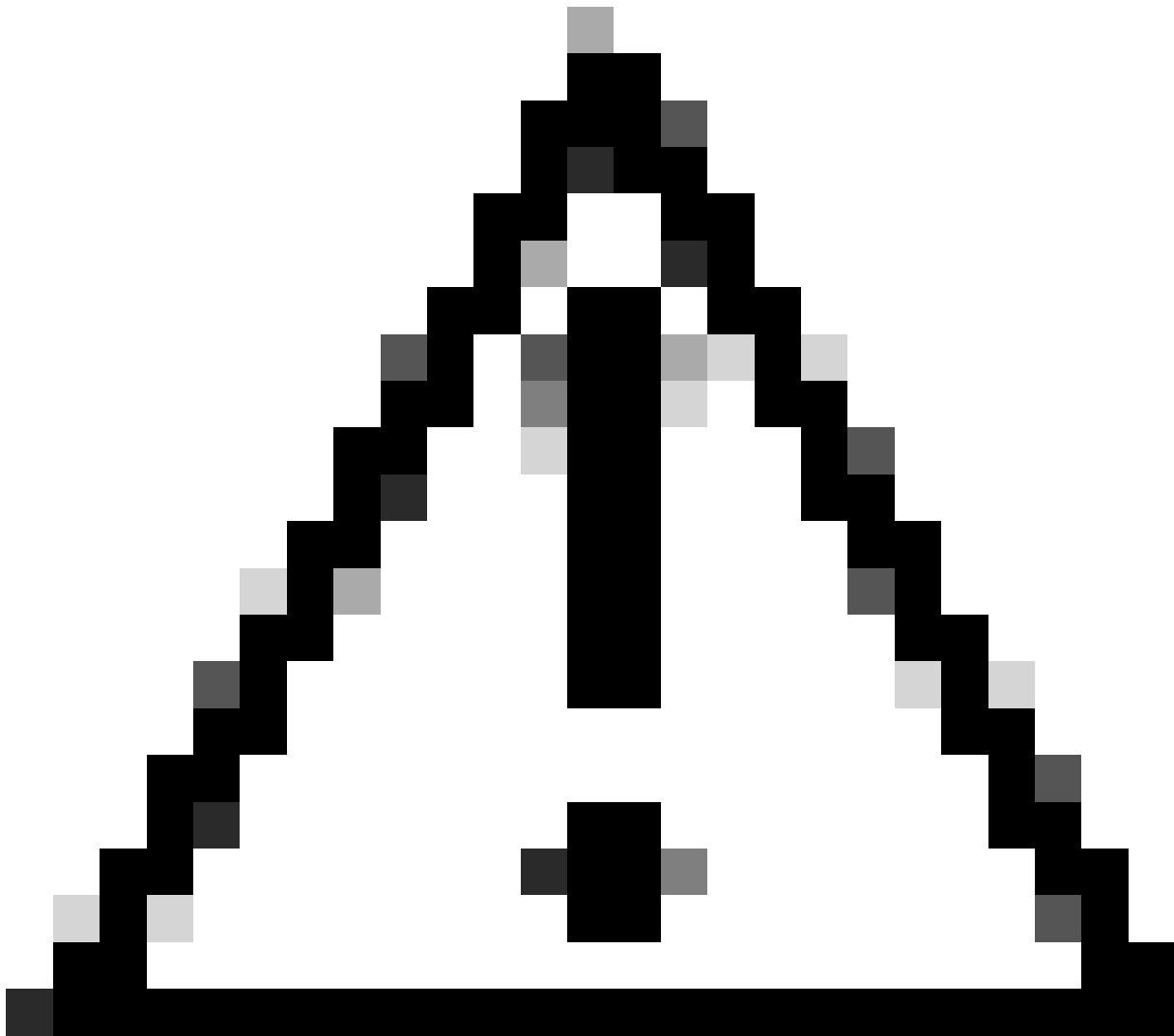
Policy Sets → IOS-XR devices [Reset](#) [Reset Policy Set Hit Counts](#) [Save](#)

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
Search					
✓	IOS-XR devices		DEVICE=Device Type EQUALS All Device Types#IOS-XR	Default Device Admin ✎ +	77

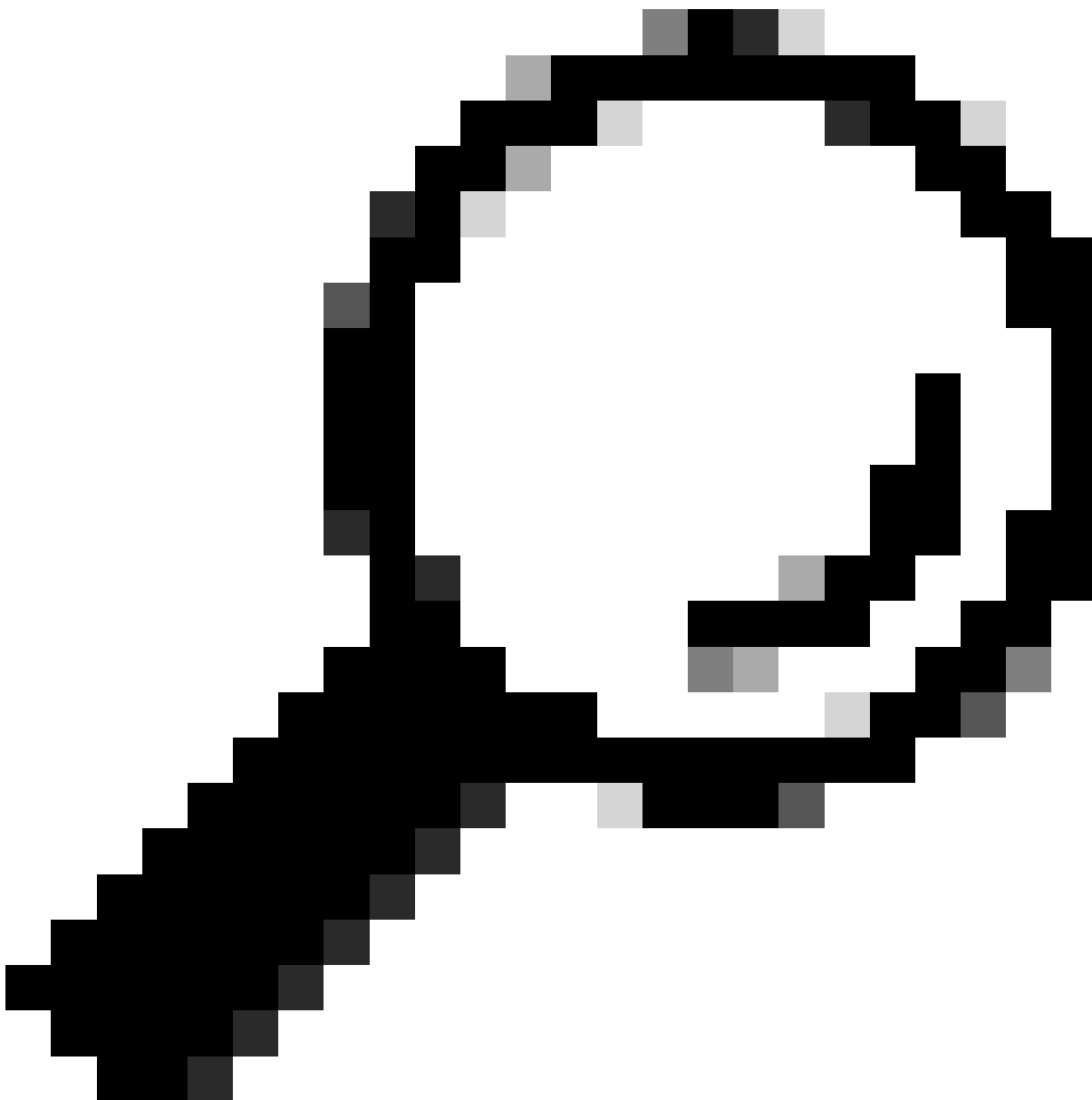
- > Authentication Policy(1)
- > Authorization Policy - Local Exceptions
- > Authorization Policy - Global Exceptions
- ∨ Authorization Policy(3)

				Results			
+ Status	Rule Name	Conditions		Command Sets	Shell Profiles	Hits	Actions
Search							
✓	Authorization Rule RO	⊞ svcs.lab - ExternalGroups EQUALS svcs.lab /Users/Device RO		CISCO_IOSXR_RO ✎ +	IOSXR_RO ✎ +	0	⚙️
✓	Authorization Rule RW	⊞ svcs.lab - ExternalGroups EQUALS svcs.lab /Users/Device Admin		CISCO_IOSXR_RW ✎ +	IOSXR_RW ✎ +	77	⚙️
✓	Default			DenyAllCommands ✎ +	Deny All Shell Profile ✎ +	0	⚙️

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



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



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

Initiële configuraties

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

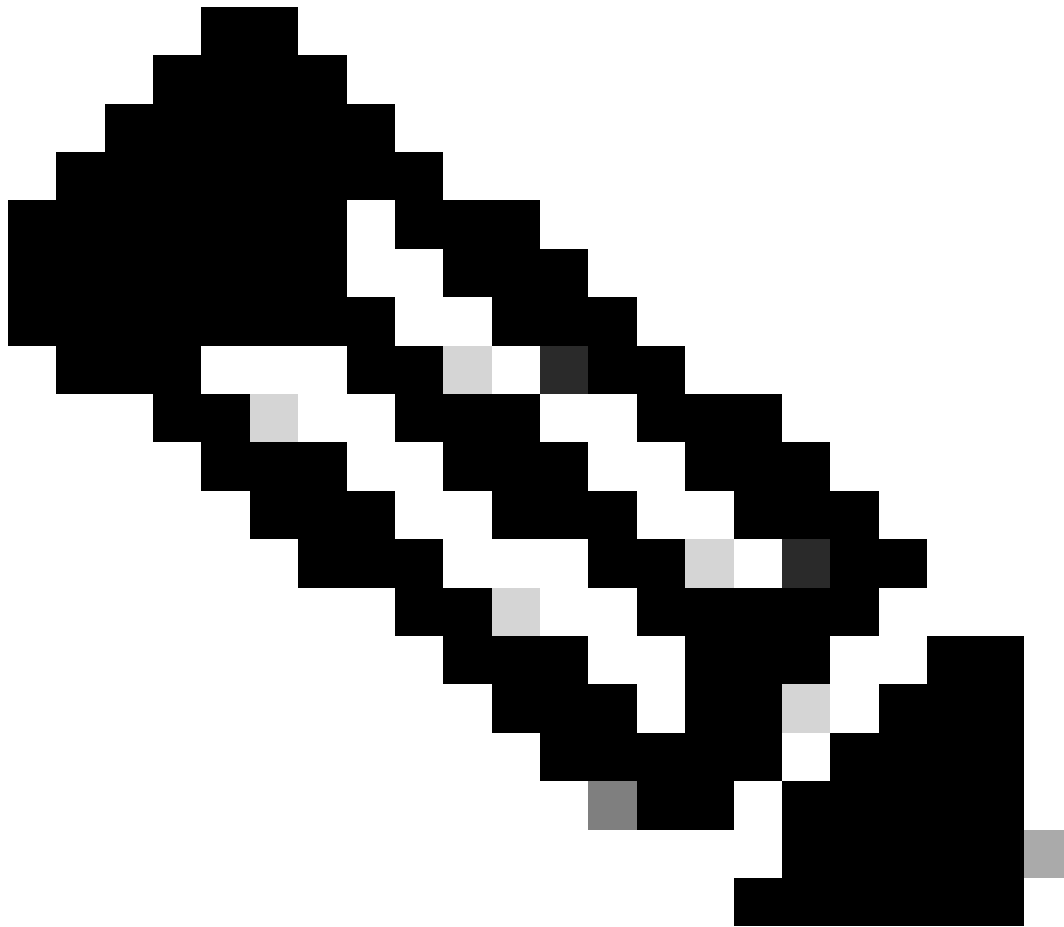
```
domain vrf mgmt name svcs.lab
domain vrf mgmt name-server 10.225.253.247
no domain vrf mgmt lookup disable
```

```
RP/0/RP0/CPU0:BRC-8201-1#ping vrf mgmt ise1.svs.lab
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.225.253.209 timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

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

```
show crypto ca trustpoint
show crypto ca certificates
```

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



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

Trustpoint configureren

Stap 1. Keypair-configuratie (optioneel).

```
<#root>
```

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

```
crypto key generate rsa
```

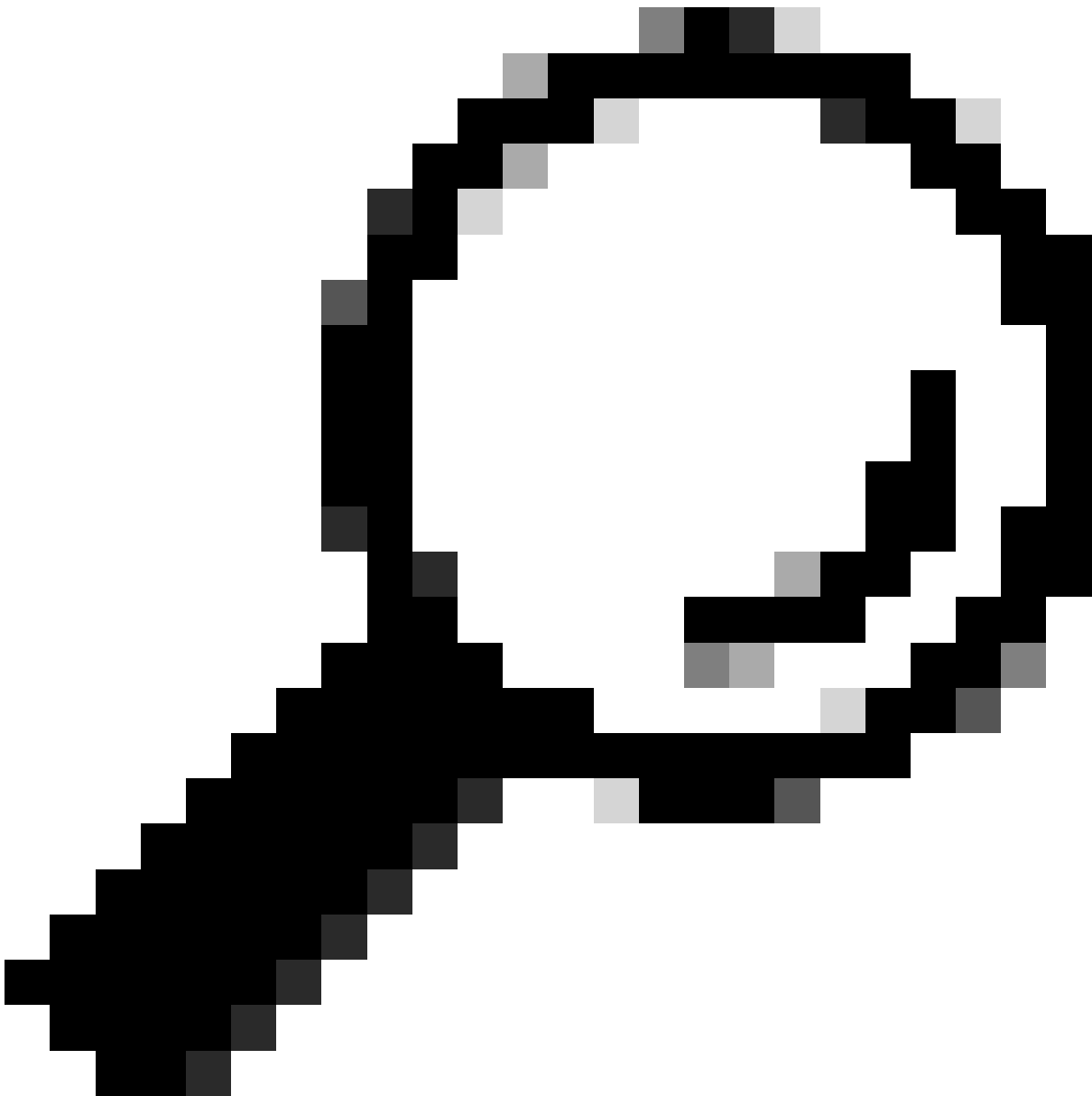
```
RP/0/RP0/CPU0:BRC-8201-1(config)#
```

```
crypto ca trustpoint
```

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

```
rsakeypair
```

Stap 2. Creëer TrustPoint.



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

```
<#root>
```

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

```
crypto ca trustpoint sv
```

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

```
vrf mgmt
```

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

```
crl optional
```



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

```
subject-name C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=brc-8201-1.svs.lab
```

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

```
subject-alternative-name IP:10.225.253.167,DNS:brc-8201-1.svs.lab
```

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

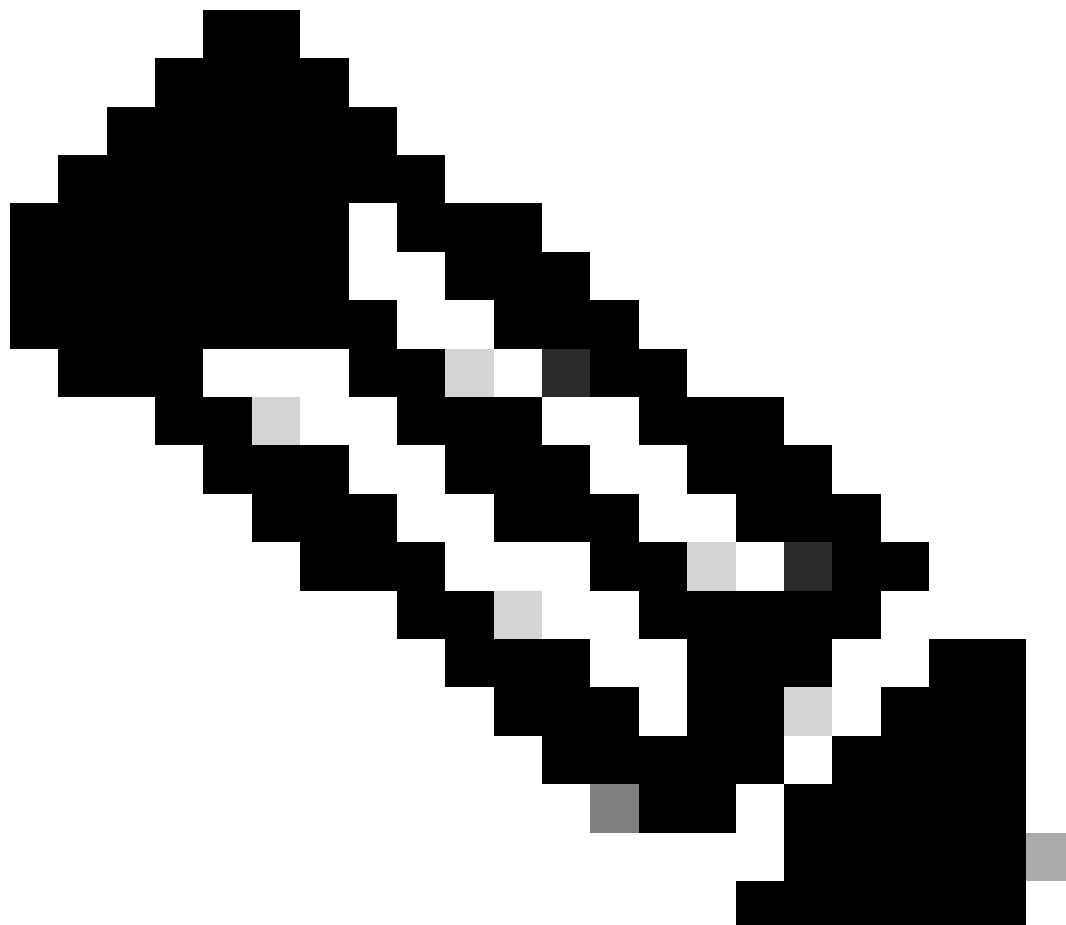
```
enrollment url terminal
```

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

```
rsakeypair svs-4096
```

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

```
commit
```



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

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

<#root>

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

crypto ca authenticate svcs

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

-----BEGIN CERTIFICATE-----

```
MIIFDCCA3ygAwIBAgIIIM10AsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZzAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECjMDU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUGA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBACTB1JhbGVpZ2gxZjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLLEwNTV1MxEjAQBgNVBAMTCVNWUyBYWJJDQTC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZUOyn2vIn6gKbx3M7vaRq
2YjwZ1zSH6EkEvxnJTty+kksiFD33GyHQepk7vfp4NFU50tQ4HC7t/A0v9grDa3QW
VwvV4MBbJhFM3s0J/ejgDYcMZhIAAPy0Zo5WLboOkXEiKjPLatKXojB8FVrhLF30
jMBSqwa4/Wlniy5S+7s4FFxsCf20COWfBAsnrs0tatIIhmcnx+VLJP7MRm8f0w4m
mutNo7IhbJSrgAFXmj1bBjMmgspObULo/wxMHdTbtPBf11HRHTkNIto3qy04UADL2
WpoGhgT/FaxxBo2UBcnYVaP+jjREONYT973MCbVAAxtNVU6bEBROz+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7B0e8oDNKU6gX1ojKyLP/gC7j8AeP03ir+KZui8
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVpl334rTixy9hpKZIkB86t2ZA3JX8CLsbCa13sA
z1XC0NX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTA01xh60I4QnK+MNQKpTjt/E4
ydH10rrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVL1783nTc9wYptQEPi5sw
83g9EMgKV0ARIiVUa/q1AgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAyb4
QgEBBAQDAgAHMBkGCWCSAGG+EIBDQQMFGpTV1MgTGFiIENBMAOGCSqGSIb3DQEB
CwUAA4ICAQAIT308oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oK0dGayi
iSEkSSX9qyflFINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXR67X+v
0+ja6zTQqj06lqJhmrSkyFbYf/ZTpe4d10zJsZjNsN0r8bF9n0A/7qNZLp3Z3cpU
PU0KdbiSvRqnPw3e8TfITVmAzcx8COI2SrYFMSUazo1VBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7a1uJapXkmnj5qPeGhN0pB
Q9r14reov4so2EspkXS7CrH9yGfpiYtprokz1UvZBZ8v1oI7YZmjFmem+5rT6Gnk
eU/1X7nV61SYG5W5K+I8uaKuyBHOMn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggz1P0dsS/i6Lo7ypYX0eB9HgVDCkzQsLXQuHGj/2WsgPgDRcjkvnyURk4Jx+Ib
xDrmo7e0XPPSW4172a6K18CR3U2Cr4wsuvndPEq/qd2NRSBWffFOXE/AJHQG7STT
HaXLU9r2Ko603oecu8ysGTWl1It/9T1/F0b0xZRugWcpJrVoTgDGUA==
```

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

quit

Serial Number : AB:CD:87:FD:41:12:C3:FE:FD:87:D5

Subject:

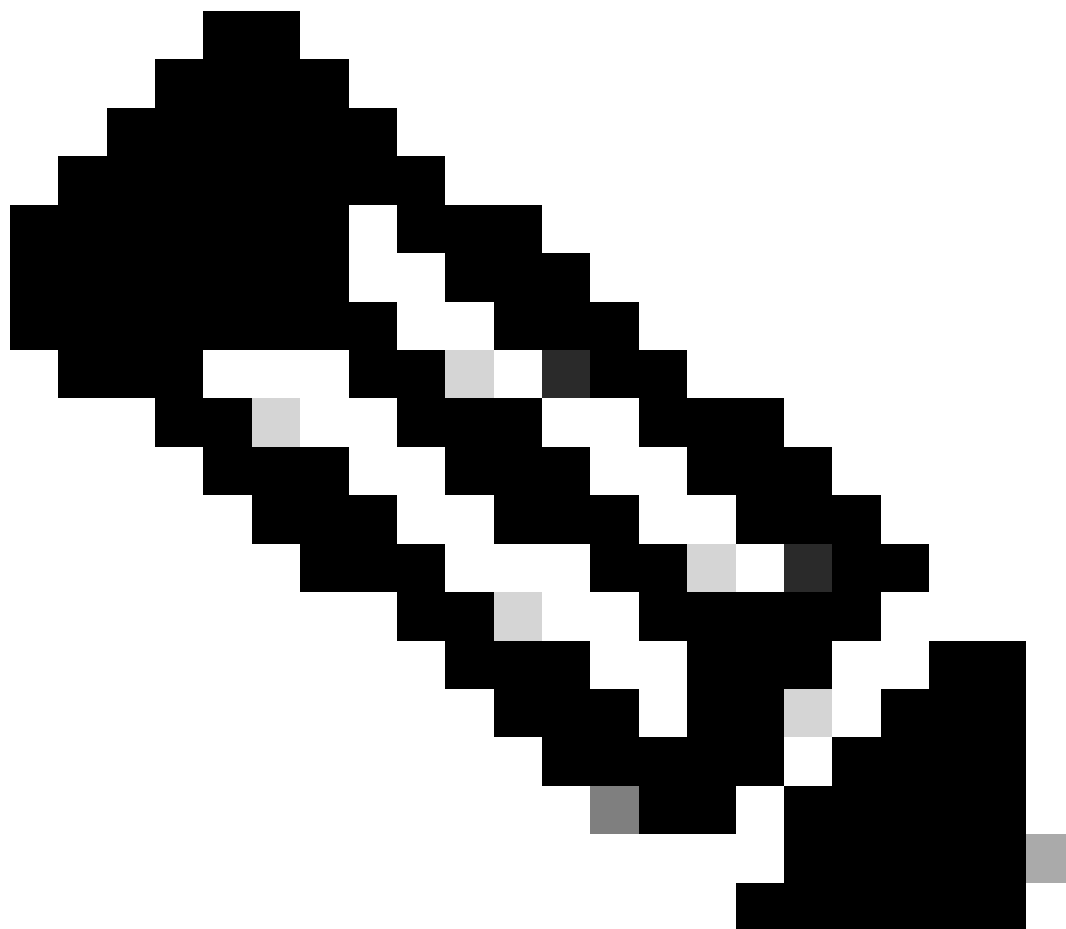
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US

Issued By :

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

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

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



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

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

<#root>

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

crypto ca enroll svcs

Fri May 9 14:52:44.030 UTC

% Start certificate enrollment ...

% Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate.

% For security reasons your password will not be saved in the configuration.

% Please make a note of it.

Password:

Re-enter Password:

% The subject name in the certificate will include: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=10.225.253.167

% The subject name in the certificate will include: BRC-8201-1.svs.lab

% Include the router serial number in the subject name? [yes/no]:

yes

% The serial number in the certificate will be: 4090843b

% Include an IP address in the subject name? [yes/no]:

yes

Enter IP Address[]

10.225.253.167

Fingerprint: 36354532 38324335 43434136 42333545

Display Certificate Request to terminal? [yes/no]:

yes

Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----

MIIDQTCCAikCAQAwcjELMAkGA1UEBhMCVVMxCzAJBgNVBAGMAk5DMQwwCgYDVQQQH
DANSVFAXDjAMBGNVBAoMBUNpc2NmMQwwCgYDVQQQLDANTVlMxZzAVBgNVBAMMDjEw
LjIyNS4yNTMuMTY3MREwDwYDVQQFEwg0MDkwODQzYjCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBALwx9w4DnTtr1oDH9iOZxPvEDARwN0t4WrPEjaQc1ZUA
6ax6Cxq/0JlQiUf2+eQv+4rKZqAZ1xDhiaIMGqETn00LKpwmtx10IqXL7UYMHwF
9vRII52zomkWA8a63Wx66UkExaXoeXaf5HkLoqDu68X83U7LPvMe1sMwvmq7Rmy2
DAu30HB/JfYlQCHmTVFz3M5fBt86xx4t1nxTFU/4lRwMC73UdL5YdKJLjMpBT2tN
E3piZ+kL4p1c9U4RIBkU8/G4drzFbGvHCIkKwI0cb1X2HgtbVQdCXTAwJDmr209
zd2ZCa5enTbOKHbNXuHjpy0k8MewKOV2muwxVcQbej8CAwEAAACBiTAYBgqhkiG
9w0BCQcxCMJQzFzY28uMTIzMG0GCSqGSIb3DQEJJDJFgMF4wDgYDVROPAQH/BAQD
AgWgMCAGA1UdJQEB/wQwMBQGCSqGSIb3DQEJJDJFgMF4wDgYDVROPAQH/BAQD
MB8GA1UdEQQYMBaCDjEwLjIyNS4yNTMuMTY3hwQK4f2nMA0GCSqGSIb3DQEBBQUA
A4IBAQBbX0eWF5ZUz701GFjuQHBBdgYb+3lhF0xbYm9psIWfv1uwjKkOL297tGHv
Iux7nMyrDVkSJ81i5BSTdd9FE6AbSFswj1YpO+IxxUM971Ejwg2rj+jABDR7I8SU
06Y06mS9x2ZJYqImeq8xwIr19Hi+7tyaLe6apfTI1jdgVxB+Xyz0FJMckI05US3j
T/3aw/115RcXerdrh360MUHEepUjIx/15u9s1c7e1mxACoQE6f90A+fdg2zYt0ME
Z6VAw64cY+YF6iLbYv7c4l1z05Zj2NJBkUpeqijkFAKY/1rIXTHypzH/p2ma4zuS
46a+kLXsVHZ716ZMB3WrUzB2ZN00

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

Stap 5. CA-ondertekend certificaat importeren.

<#root>

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

crypto ca import svcs certificate

Fri May 9 15:00:35.426 UTC

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

```
-----BEGIN CERTIFICATE-----  
MIIE3zCCAsegAwIBAgIINL1NAUzx14UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE  
BhMCVVMxZmZAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWx1aWdo  
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECXMdU1ZTMRIwEAYDVQQDEw1TV1MgTGFi  
Q0EwHhcNMjUwNTA5MTQ1NzAwWWhcNMjUwNTA5MTQ1NzAwWjByMQswCQYDVQQGEwJV  
UzELMAkGA1UECAwCTMxMDDAKBgNVBACMA1JUUEDEOMAwGA1UECgwFQ21zY28xDDAK  
BgNVBAsMA1NWUzEXMBUGA1UEAwwOMTAumjI1LjI1My4xNjcxETAPBgNVBAUTCDQw  
OTA4NDNiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvDH3DgOd02uW  
gMf2I5nE+8QMBHA3S3has8SNpByV1QDprHoLGr/QmVCJR/b55C/7ispmoBnXEOGJ  
qIwaoR0c7QsqnCa3HXQipcvrtRgwcFAX29Egjnboi aRYDxrdbHrpSQTfpeh5dp/k  
eQuio07rxfdzTss+8x7WwzC+artGbLYMC7fQcH819iVAIeZNUXPcz18G3zrHHI3W  
fFMVT/iVFYwLvdR0v1h0okuMykFPa00TemJn6QvinVz1ThEgGRTz8bh2vMVsa8cI  
iRaTajRxxvFyEC1tVB0JdMDAK0avY73N3Zkjr16dNs4ods1e4eOnLSTwx7Ao5Xaa  
7DFVxBt6PwIDAQBo4GAMH4wHgYJYIZIAyb4QgENBBEWD3hjYSBjZXJ0aWZpY2F0  
ZTA0BgNVHQ8BAf8EBAMCBaAwIAyDVR01AQH/BBYwFAYIKwYBBQUHAWEGCCsGAQUF  
BwMCMAMkGA1UdEwQCMAAwHwYDVR0RBBGwFoIOMTAumjI1LjI1My4xNjcxETAPBgNV  
DQYJKoZIhvcNAQELBQADggIBAARpS5bEck+oj012106WxedDQ8Vdu0bBtrn0H+Nt  
94EA1co7HEe4USf1FiASAX7rNveLpY3ICmLh+tQZYTzRQ93tb9mMTZg7exqN89ZU  
V1XoB2U0Tri5K10/+izEGgyNq42/ytAP8Y007HR/2jf7gfhovwvR5QN0EHv4o61  
Zma5Xio1sBbkA7JB2mpzzZg4ZjsyV81RGXxxgyt1mwNmb7EiAc81odRcgyp7FNh3  
F/k9cMMMr51M4Ysvo1tx1k9AeLjb2syv5/fG6Qu0ZdWwTaaQh0Y2h/cVDiV97wg  
0D1mEfDsv6QrxQSujZr22RzVykKH1tuiV2B74pthUuGRBtFHS5Xfy7uTTbfGX8M6  
ZJw8rX1SADr8tDp1rf1ZIrPmv3ZPP7woTB22yWzyd0use+5Ia1b0w70twN4t/IiW  
8CJu6HfnDXLDPZ0jsC8steffrS1opwGccp3j6aZKPFz+I/Purb44a9WxEwa2TA7H  
+r1oynBcGMet0HxVLnptlsC7Q4mN/MDXeGyW+OTNCirNEG/gqcu+dn9EnNKkE2WV  
oF5370w+uNHok8Bdt8mqadUT40oUSqY8ArV0Bom05tzbemreVPmQAZ/IahZ7TqKo  
3dGNontAFTTESM1iujQ81iRKsikdHysnwcCM2ni1CKZrhVq5IB8NK6jKRJZ0eQAX  
vMt1  
-----END CERTIFICATE-----
```

quit

Serial Number : C2:F4:AB:34:02:D2:76:74:65:34:FE:D5

Subject:

serialNumber=4090843b,CN=10.225.253.167,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US

Issued By :

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

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

Controleer of het identiteitscertificaat van de router is geregistreerd.

<#root>

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

show crypto ca trustpoint svcs detail

Trustpoint :svs-new
=====

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

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

show crypto ca certificates svcs

Wed May 14 14:55:58.173 UTC

Trustpoint : svcs-new
=====

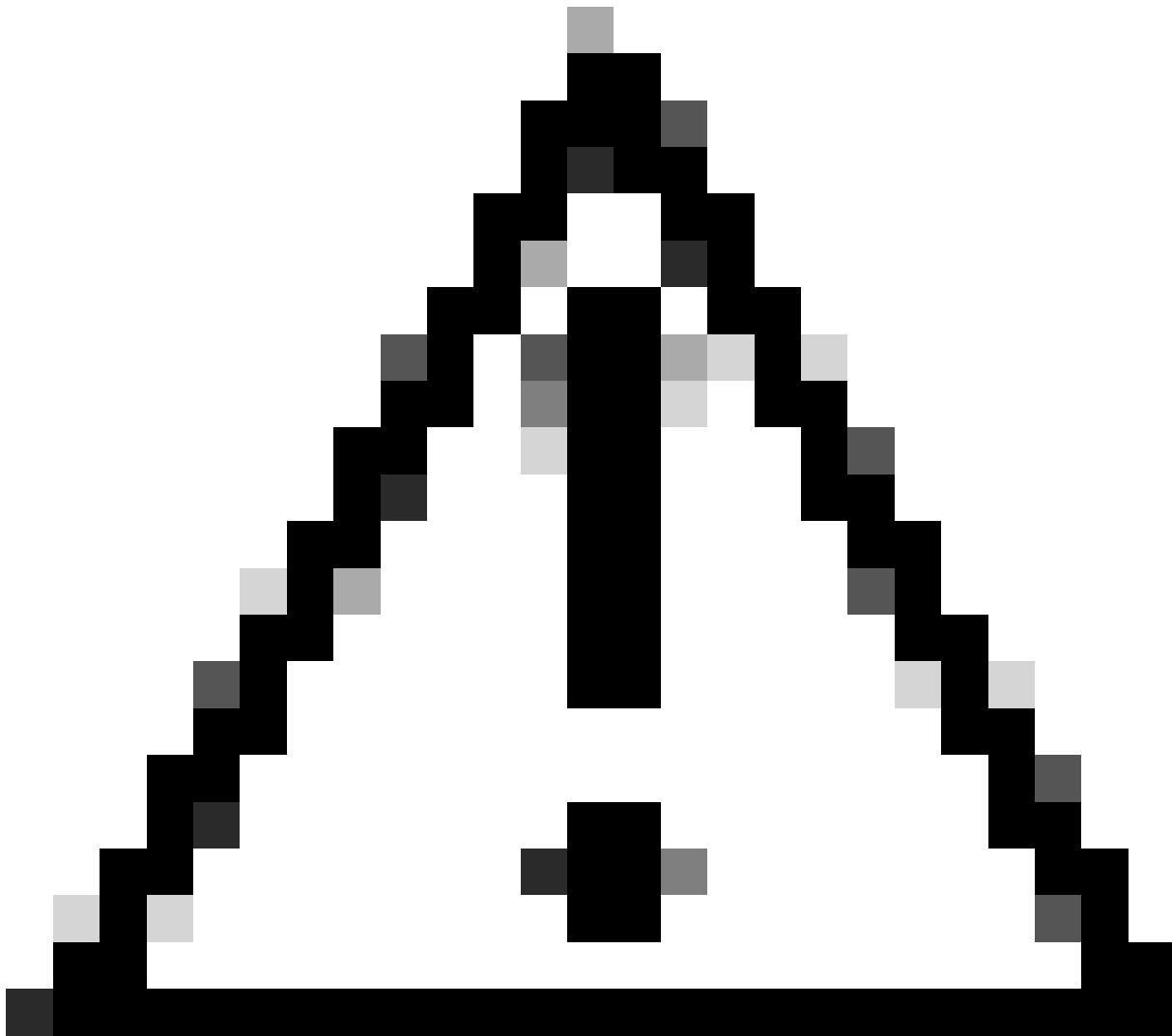
CA certificate
Serial Number : 20:01:20:1F:B6:9D:C3:FE:43:78:FF:64
Subject:
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
Issued By :
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
Validity Start : 17:05:00 UTC Mon Apr 28 2025
Validity End : 17:05:00 UTC Sat Apr 28 2035
SHA1 Fingerprint:
0EB181E95A3ED7803BC5A8059A854A95C83AC737

Router certificate

Key usage	: General Purpose
Status	: Available
Serial Number	: FD:AC:20:1F:B6:9D:C3:FE:98:43:ED
Subject:	
serialNumber=4090843b,CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US	
Issued By :	
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US	
Validity Start : 19:59:00 UTC Fri May 09 2025	
Validity End : 19:59:00 UTC Sat May 09 2026	
SHA1 Fingerprint:	
AC17E4772D909470F753BDBFA463F2DF522CC2A6	

Associated Trustpoint: svcs

TACACS & AAA configureren met TLS



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

Stap 1. De TACACS+-server configureren.

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

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

Stap 2. Configureer de AAA-groep.

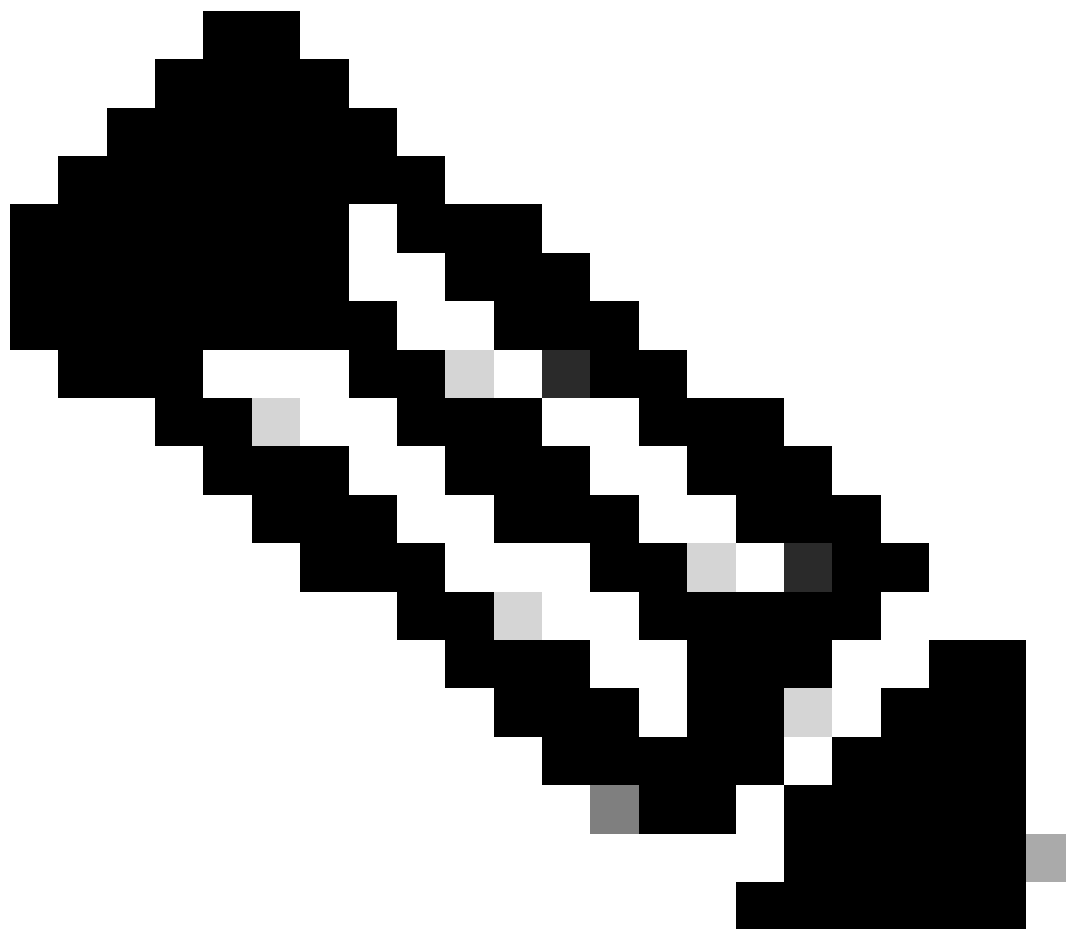
```
aaa group server tacacs+ tac_tls_sc
```

```
vrf mgmt
server-private 10.225.253.209 port 6049
timeout 10
tls
  trustpoint sv5
!
single-connection
```

Stap 2. Configureer AAA.

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

Certificaatvernieuwing



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

Stap 1. Controleer de huidige geldigheidsdatums van het certificaat.

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

```
Trustpoint : svcs-new
```

```
=====
```

```
CA certificate
```

```
Serial Number : 30:A2:10:14:C9:5E:B0:E0:07:CE:0A:24:16:69:90:ED:D1:34:B5:9B
```

```
Subject:
```

```
CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
```

```
Issued By :
```

```
CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
```

```
Validity Start : 22:13:17 UTC Thu Jun 26 2025
```

```
Validity End : 22:13:16 UTC Tue Jun 25 2030
```

CRL Distribution Point

<http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=m9uB1QsZDYy6wxomiFWB5Gv0AZM>

SHA1 Fingerprint:

EA8FB276563B927FCAF0174D9FD1C58F3E8B5FF2

Trusted Certificate Chain

Serial Number : 1F:A6:6E:2E:F8:AB:CE:B4:9C:B8:07:5A:9F:2B:32:02:B4:56:5C:96

Subject:

CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US

Issued By :

CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US

Validity Start : 22:13:17 UTC Thu Jun 26 2025

Validity End : 22:13:16 UTC Sun Jun 24 2035

SHA1 Fingerprint:

E225647FF9BDA176D2998D5A3A9770270F37D2A7

Router certificate

Key usage : General Purpose

Status : Available

Serial Number : 7A:13:EB:C0:6A:8D:66:68:09:0B:32:C7:0C:D8:05:BD:81:72:9B:4E

Subject:

CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US

Issued By :

CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US

Validity Start : 16:38:36 UTC Wed Jul 30 2025

Validity End : 16:38:35 UTC Thu Jul 30 2026

CRL Distribution Point

<http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=X4as2q+6I9Bd4Qg1Qa8g1xoH8GY>

SHA1 Fingerprint:

B562F3CF507CE7F97893F28BC896794CFF6995C1

Associated Trustpoint: svb-new

Stap 2. Bestaande Trustpoint-certificaat verwijderen.

```
RP/0/RP0/CPU0:BRC-8201-1#clear crypto ca certificates KF_TP
```

```
Thu Aug 14 15:25:26.286 UTC
```

```
certificates cleared for trustpoint KF_TP
```

```
RP/0/RP0/CPU0:Aug 14 15:25:26.577 UTC: cepki[382]: %SECURITY-CEPKI-6-INFO : certificate database updated
```

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

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

```
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates KF_TP
```

```
Thu Aug 14 15:25:37.270 UTC
```

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

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

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

```
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates KF_TP
```

```
Thu Aug 14 15:31:28.309 UTC
```

Trustpoint : KF_TP

=====

CA certificate

Serial Number : 30:A2:10:14:C9:5E:B0:E0:07:CE:0A:24:16:69:90:ED:D1:34:B5:9B

Subject:

CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US

Issued By :

CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US

Validity Start : 22:13:17 UTC Thu Jun 26 2025

Validity End : 22:13:16 UTC Tue Jun 25 2030

CRL Distribution Point

<http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=m9uB1QsZDYy6wxomiFWB5Gv0AZM>

SHA1 Fingerprint:

EA8FB276563B927FCAF0174D9FD1C58F3E8B5FF2

Trusted Certificate Chain

Serial Number : 1F:A6:6E:2E:F8:AB:CE:B4:9C:B8:07:5A:9F:2B:32:02:B4:56:5C:96

Subject:

CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US

Issued By :

CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US

Validity Start : 22:13:17 UTC Thu Jun 26 2025

Validity End : 22:13:16 UTC Sun Jun 24 2035

SHA1 Fingerprint:

E225647FF9BDA176D2998D5A3A9770270F37D2A7

Router certificate

Key usage : General Purpose

Status : Available

Serial Number : 1F:B0:AE:44:CF:8E:24:62:83:42:2F:34:BF:D0:82:07:DF:E4:49:0B

Subject:

CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US

Issued By :

CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US

Validity Start : 15:17:29 UTC Thu Aug 14 2025

Validity End : 15:17:28 UTC Fri Aug 14 2026

CRL Distribution Point

<http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=X4as2q+6I9Bd4Qg1Qa8g1xoH8GY>

SHA1 Fingerprint:

D3CE0AEB51C5E8009F626A1A9FD633FB9AFA96DE

Associated Trustpoint: KF_TP

Verificatie

De configuratie verifiëren.

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

Foutopsporing voor TACACS+

```
debug tacacs tls
```

Foutopsporing TLS

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

Test de externe gebruiker voordat u AAA-verificatie configureert.

```
<#root>
```

```
test aaa group tacacs2
```

```
user has been authenticated
```

Probleemoplossing

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

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

Herstart TACACS-proces (indien nodig)

```
process restart tacacsd
```

Over deze vertaling

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