

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

Inhoud

[Inleiding](#)

[Overzicht](#)

[Gebruik van deze Guide](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[vergunning](#)

[Deel 1 - Configure ISE 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 XE RW - Beheerdersprofiel](#)

[IOS XE RO - Gebruikersprofiel](#)

[TACACS+-opdrachtreeksen configureren](#)

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

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

[Apparaatbeheerbeleidsets configureren](#)

[Deel 2 - Cisco IOS XE configureren voor TACACS+ via TLS 1.3](#)

[Configuratiemethode 1 - Sleutelpaar gegenereerd door apparaat](#)

[TACACS+-serverconfiguratie](#)

[Trustpoint-configuratie](#)

[TACACS & AAA met TLS-configuratie](#)

[Configuratiemethode 2 - CA-gegenereerd sleutelpaar](#)

[TACACS & AAA met TLS-configuratie](#)

[Verificatie](#)

Inleiding

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

Overzicht

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

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

Gebruik van deze Guide

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

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

Voorwaarden

Vereisten

Vereisten voor het configureren van TACACS+ via TLS:

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

Gebruikte componenten

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

- ISE VMware virtual appliance, release 3.4 patch 2
- Cisco IOS XE Software, versie 17.15+

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

vergunning

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

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

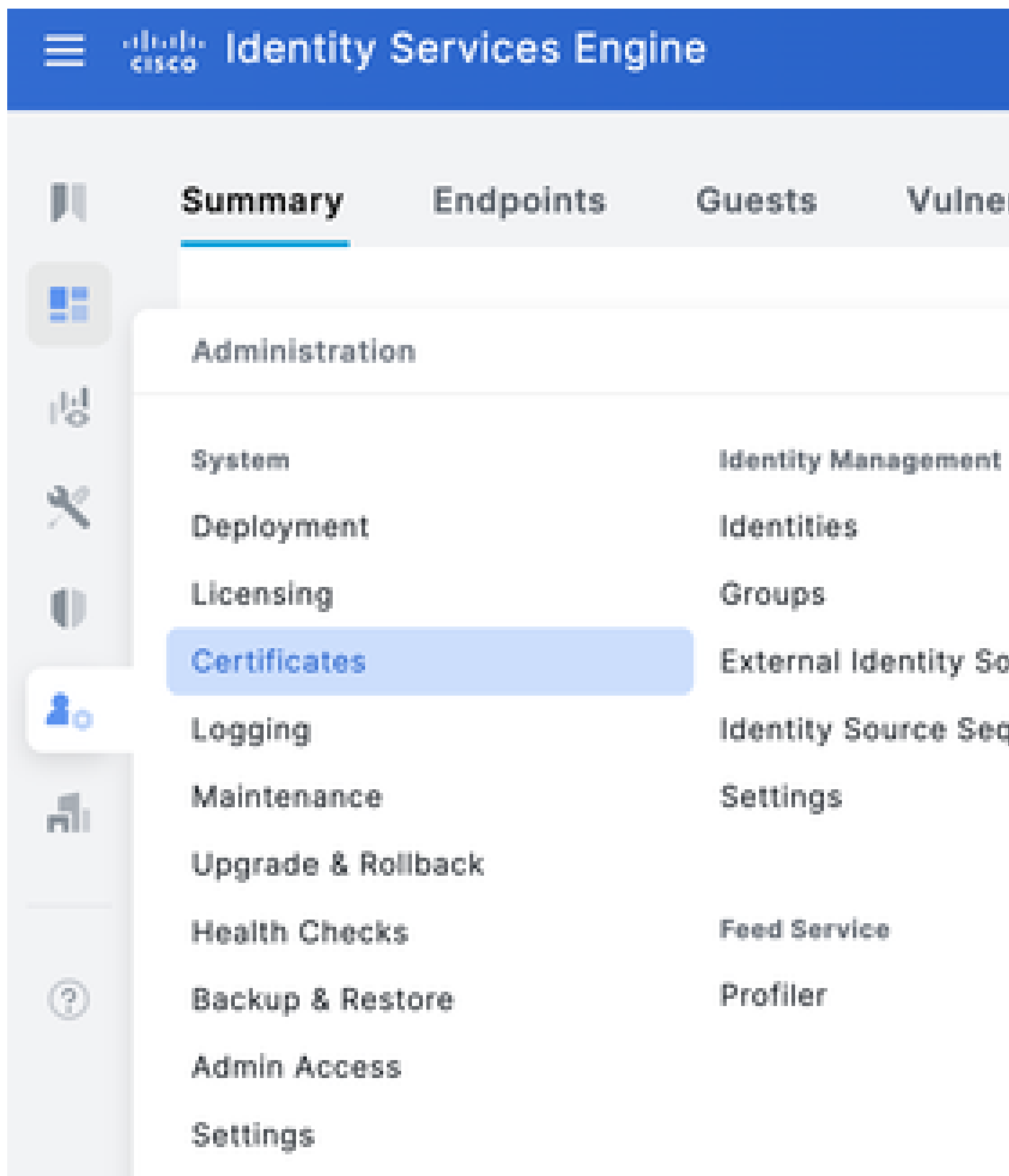
Deel 1 - Configureer ISE voor apparaatbeheer

Aanvraag voor certificaatondertekening genereren voor TACACS+-serververificatie

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

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

Stap 2. Navigeer naar Beheer > Systeem > Certificaten.



Stap 3. Klik onder Certificaatondertekeningsverzoeken op Certificaatondertekeningsverzoek genereren.



Stap 4. Selecteer TACACS in gebruik.

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

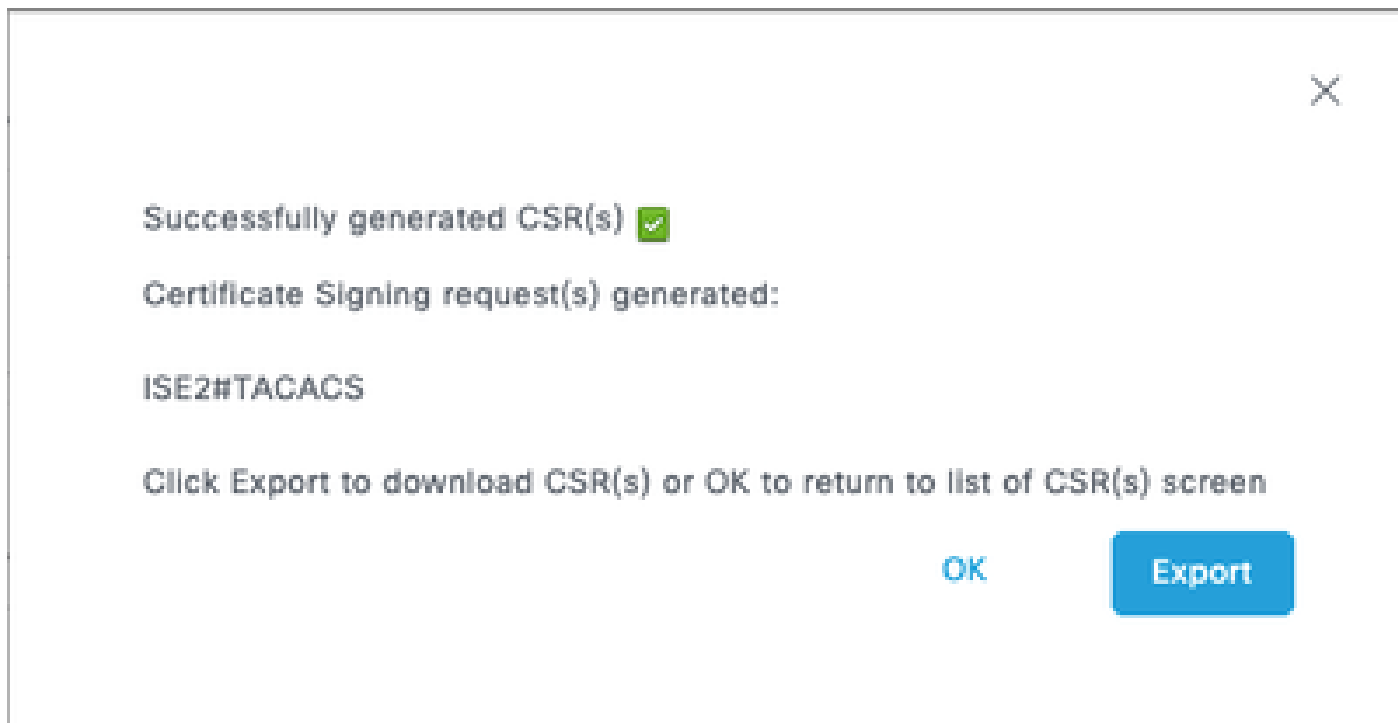
Country (C)
US

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 Certificate Authority (CA).

Root CA-certificaat uploaden voor TACACS+-serververificatie

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

☐	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 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

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

The screenshot shows the 'Trusted Certificates' section in the Cisco ISE Administration console. The left sidebar contains navigation links like 'Bookmarks', 'Dashboard', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The main content area shows a table of trusted certificates. The table has columns for 'Friendly Name', 'Trusted For', 'Serial Number', 'Issued To', 'Issued By', 'Valid From', and 'Expiration Date'. One certificate is listed with the friendly name 'CN=SVS LabCA, OU=SVS, O=Cisco, L=...' and a serial number '20 CD 74 02 ...'. The 'Valid From' date is 'Mon, 28 Apr 2025' and the 'Expiration Date' is 'Sat, 28 Apr 2025'.

Het ondertekende certificaatondertekeningverzoek (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 Certificaatondertekeningverzoeken de TACACS-CSR die in de vorige stap is gegenereerd en klik op Certificaat binden.

The screenshot shows the 'Certificate Signing Requests' section in the Cisco ISE Administration console. The left sidebar contains navigation links like 'Bookmarks', 'Dashboard', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The main content area shows a table of certificate signing requests. The table has columns for 'Friendly Name', 'Certificate Subject', 'Key Length', 'Portal gro...', 'Timestamp', and 'Host'. A 'Bind Certificate' button is highlighted in the table. Above the table, there is a 'Generate Certificate Signing Requests (CSR)' button and a note about the process of signing and binding CSRs.

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.

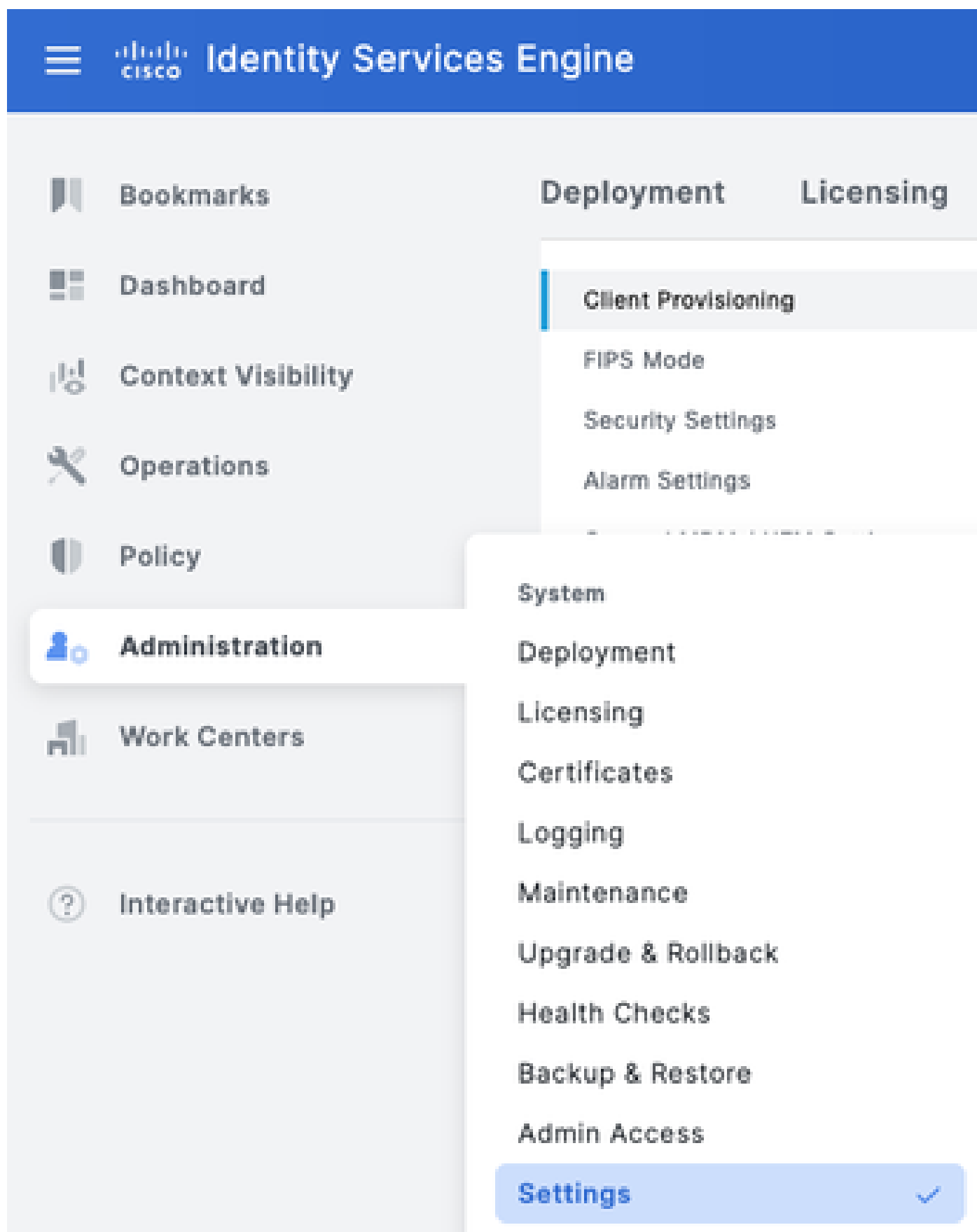
[Edit](#) [Generate Self Signed Certificate](#) [Import](#) [Export](#) [Delete](#) [View](#)

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
ISE1	C=US, ST=NC, L=Raleigh, TACACS O=Cisco, OU=SVS, CN=I SE1.lab#ISE1.lab#00010		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.



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

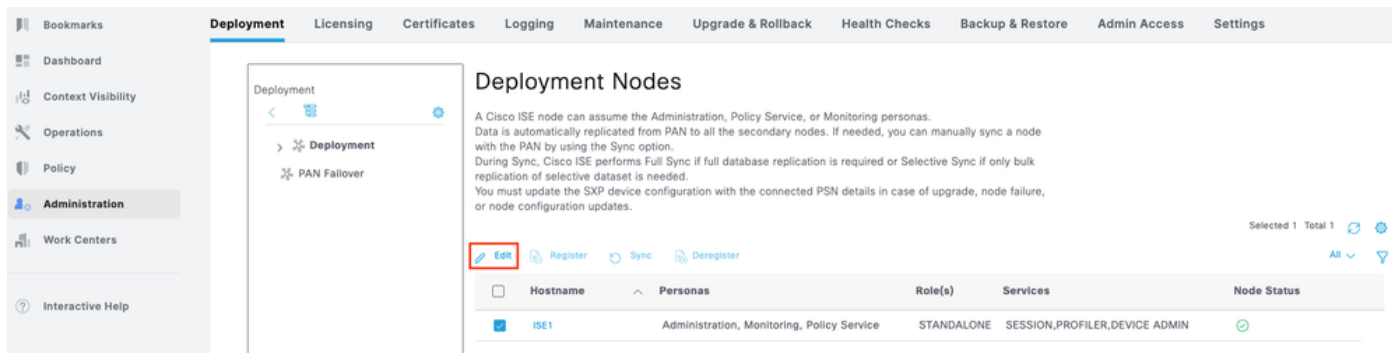


Waarschuwing: wanneer u de TLS-versie wijzigt, wordt de Cisco ISE-toepassingsserver opnieuw gestart op alle Cisco ISE-implementatiemachines.

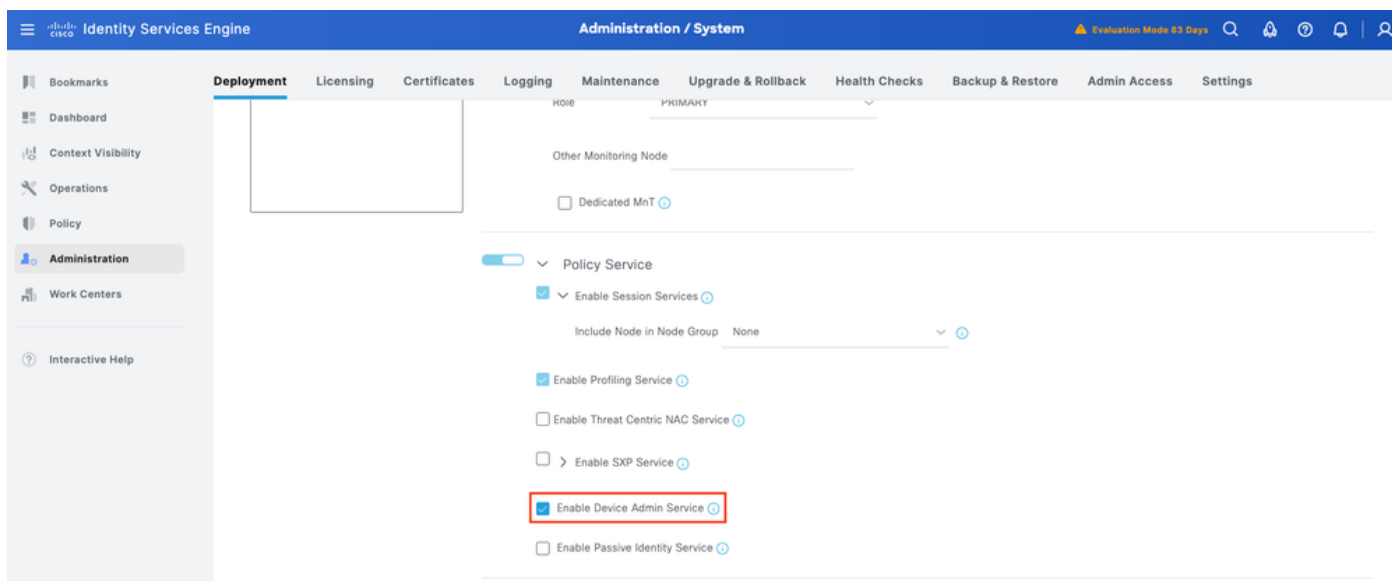
Apparaatbeheer inschakelen op ISE

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

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



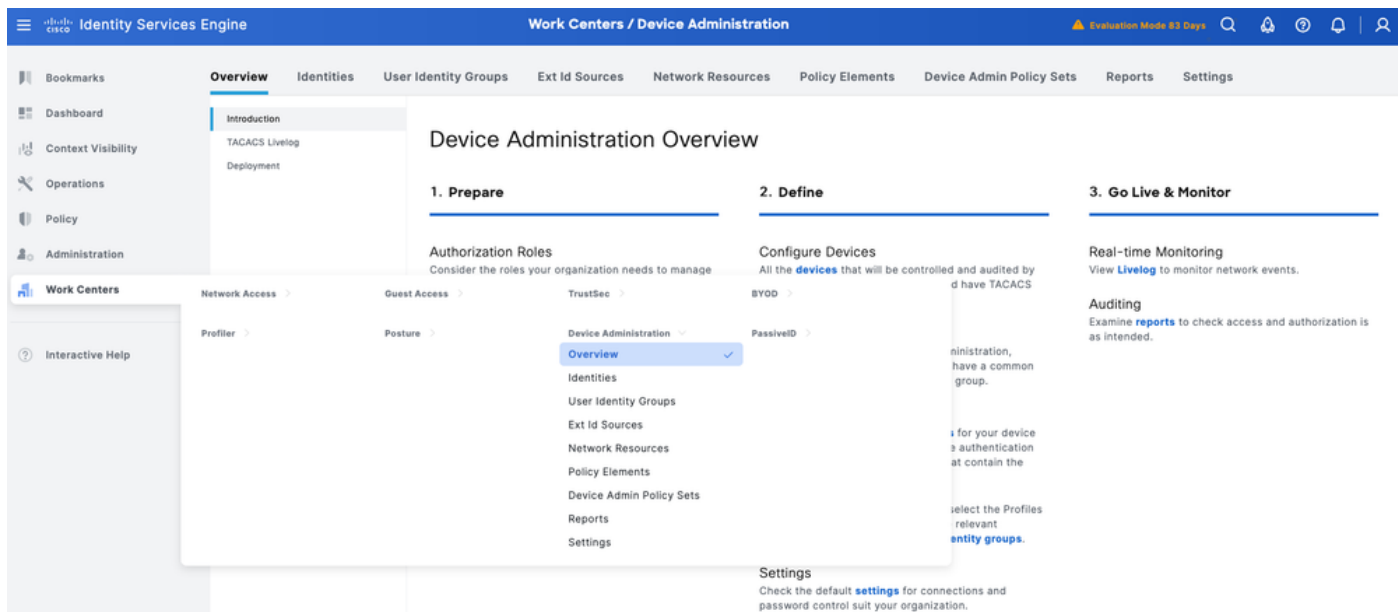
Stap 2. Blader onder Algemene instellingen omlaag en selecteer het selectievakje naast Apparaatbeheerservice inschakelen.



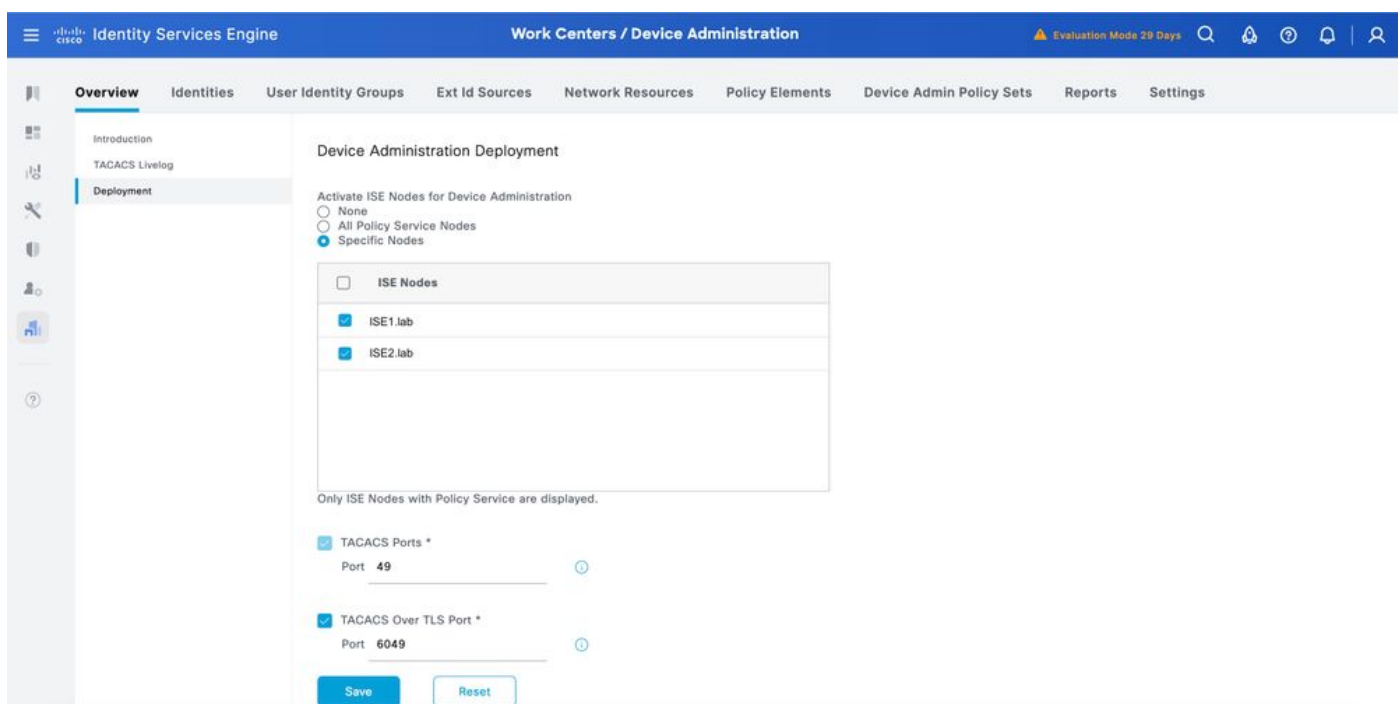
Stap 3. Sla de configuratie op. Device Admin Service is nu ingeschakeld op ISE.

TACACS via TLS inschakelen

Stap 1. Navigeer naar werkcentra > Apparaatbeheer > Overzicht.



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



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

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 XE.

Add Group

Name*

IOSXE



Description

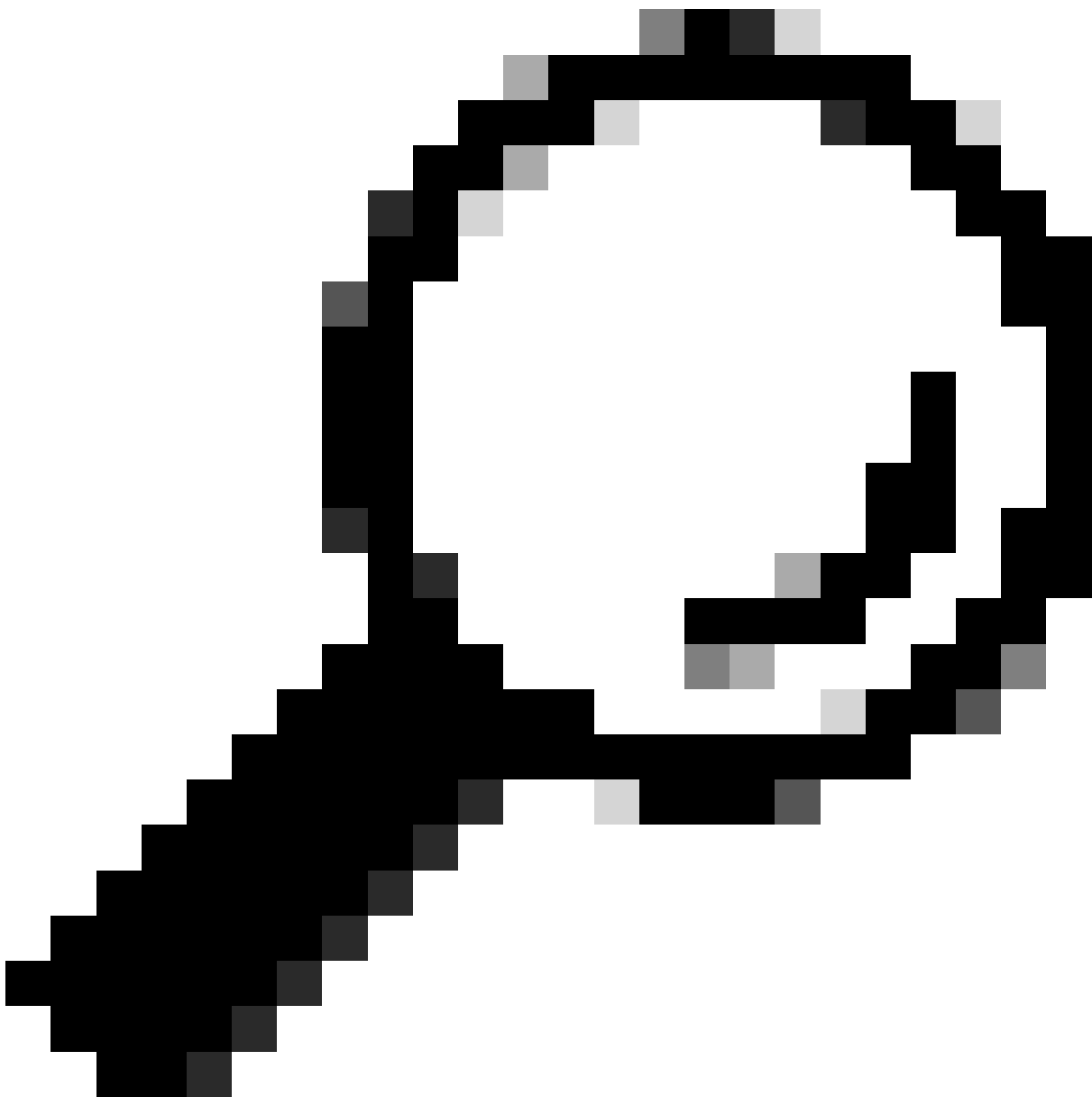
Parent Group*

Select Group or Add as root group



Cancel

Save



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

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

Identity Services Engine

Work Centers / Device Administration

Overview

Identities

User Identity Groups

Ext Id Sources

Network Resources

Policy Elements

Device Admin Policy Sets

More

Network Devices

Network Device Groups

Default Devices

TACACS External Servers

TACACS Server Sequence

Network Devices List > SVS_BRPASR1K

Network Devices

Name

SVS_BRPASR1K

Description

IP Address

* IP :

10.225.253.180

/

32

Device Profile

Cisco

Model Name

Software Version

Network Device Group

Location

All Locations

Set To Default

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

Identity Services Engine

Work Centers / Device Administration

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.

☐

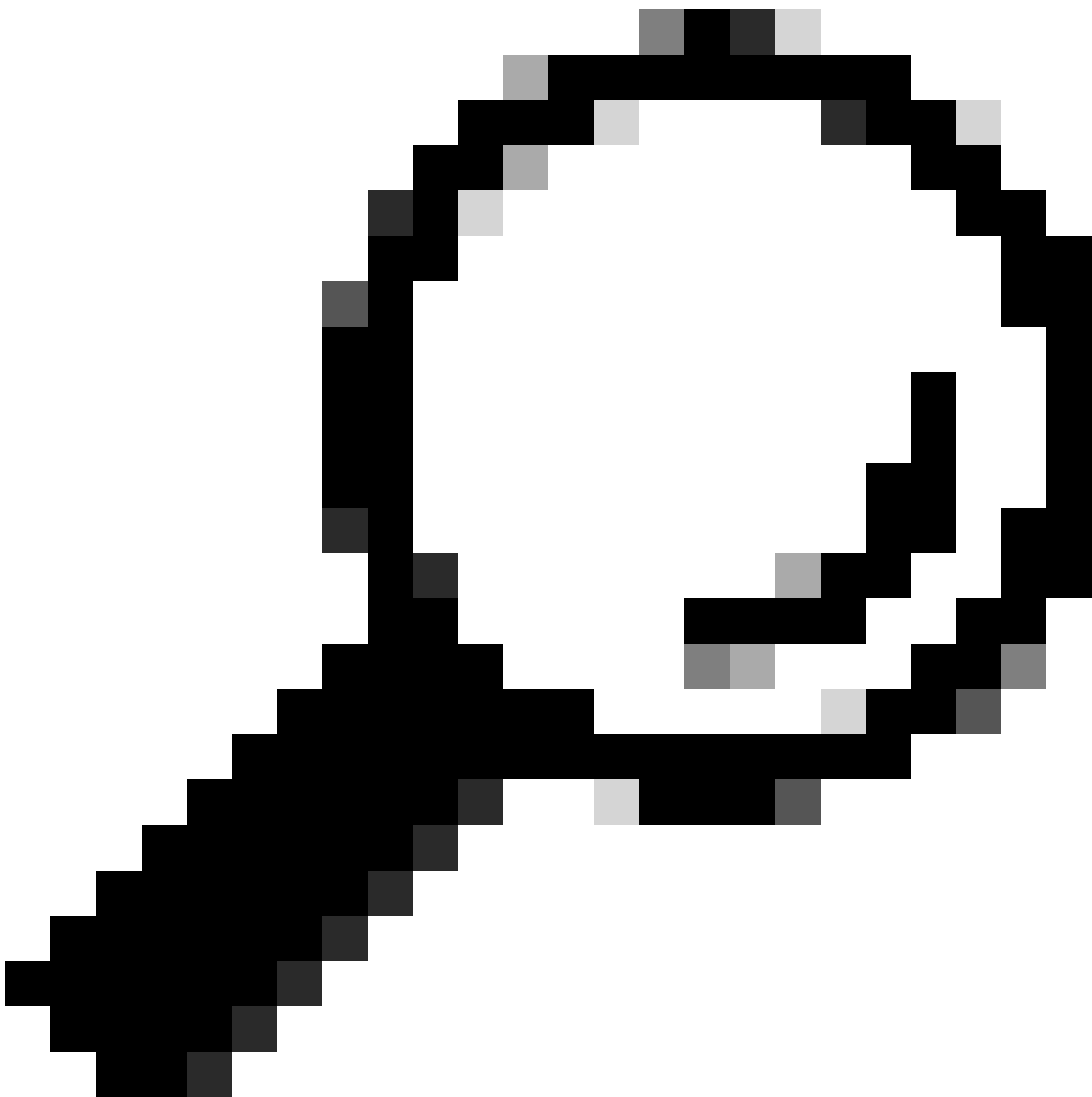
IP Address

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

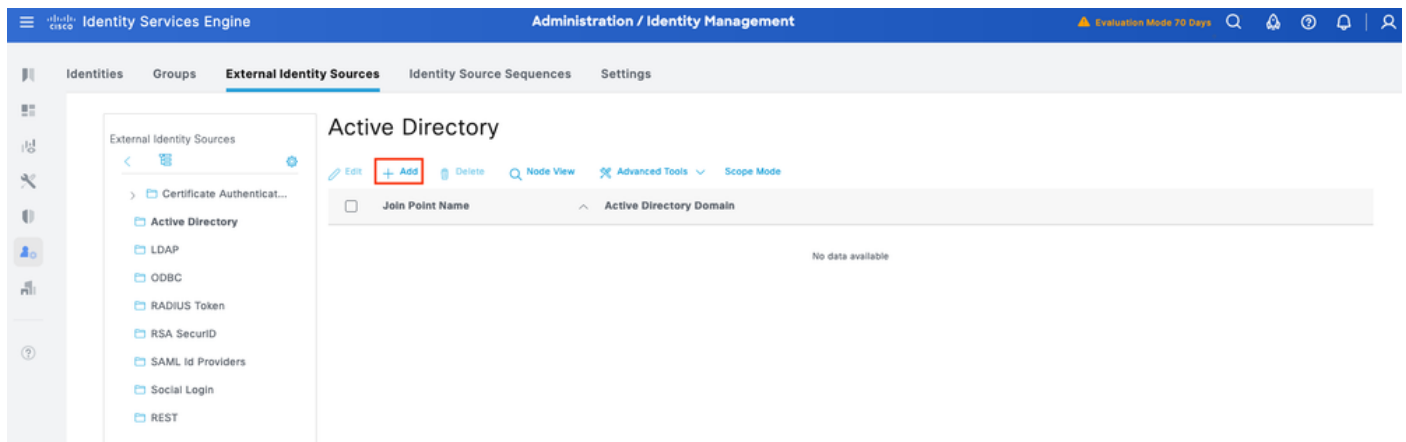


Tip: Het wordt aanbevolen om de modus Single Connect in te schakelen om te voorkomen dat de TCP-sessie opnieuw wordt gestart telkens wanneer een opdracht naar het apparaat wordt verzonden.

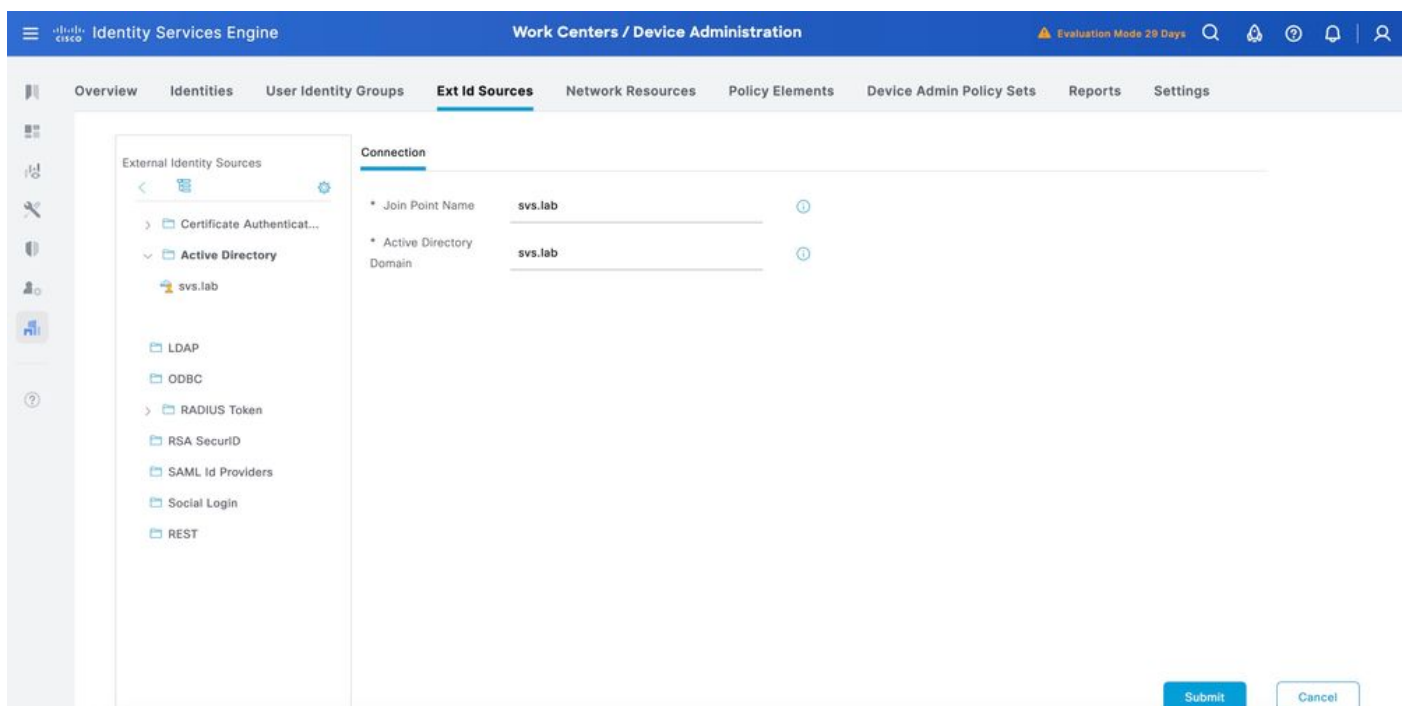
Identiteitswinkels configureren

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.

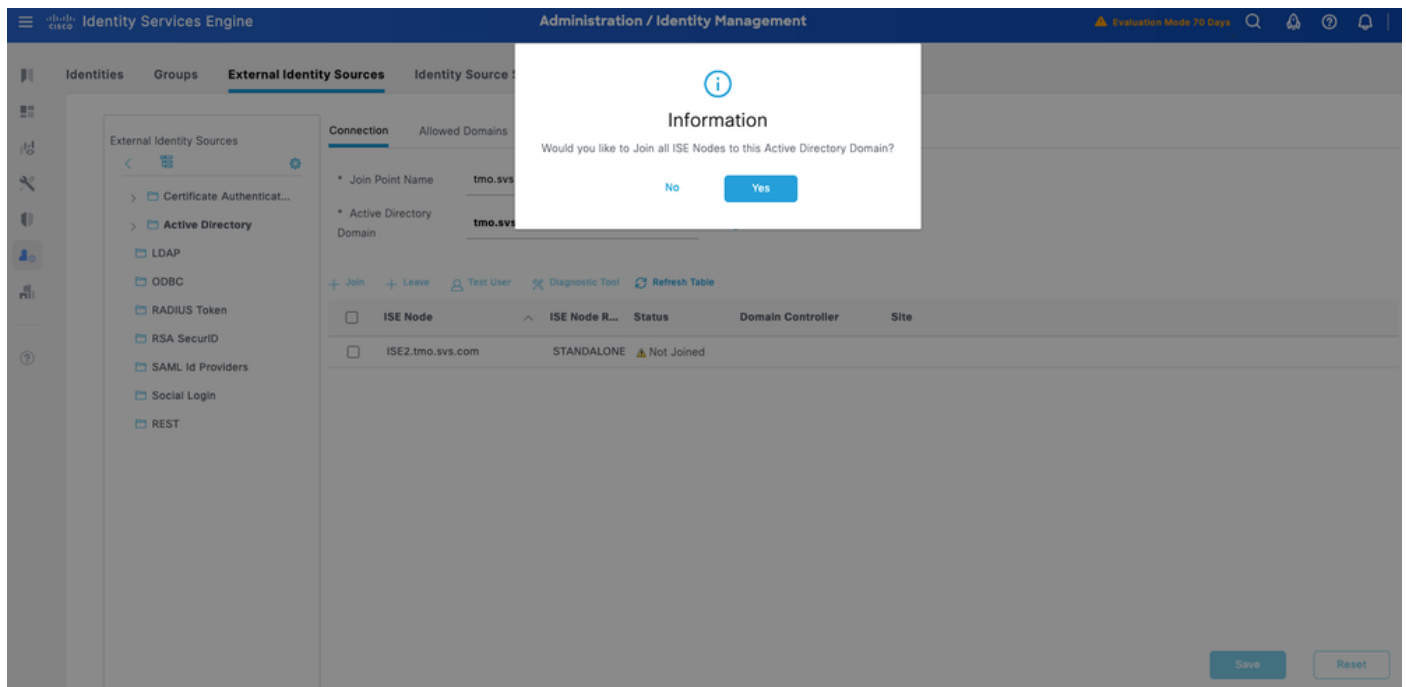
Stap 1. Navigeer naar Beheer > Identiteitsbeheer > Externe identiteitswinkels > Active Directory. Klik op Toevoegen om een nieuw AD-verbindingspunt te definiëren.



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-knooppunten aan dit Active Directory-domein toevoegen?



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

×

Join Domain

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

* AD User Name ⓘ

administrator

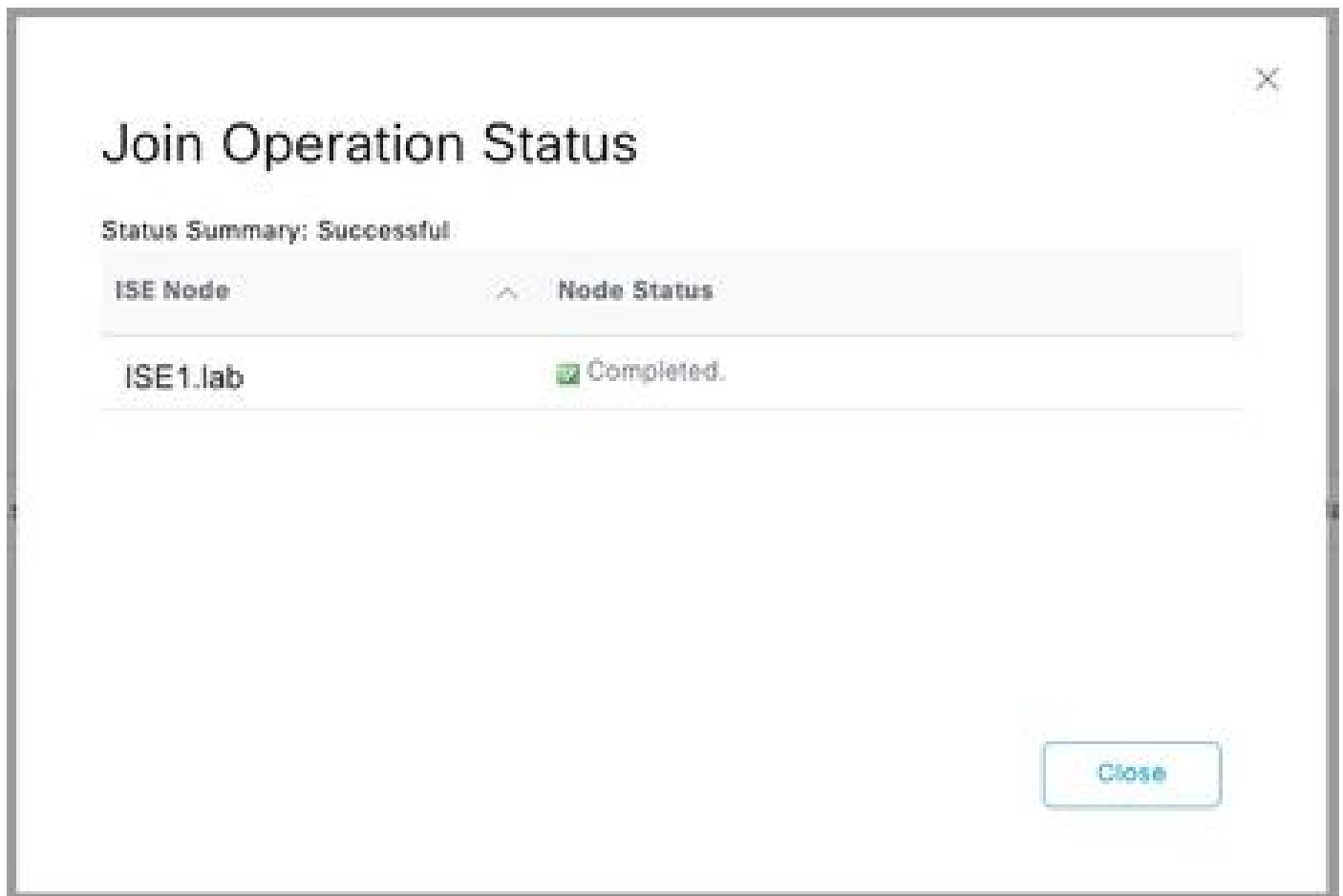
* Password ⓘ

☐ Specify Organizational Unit ⓘ

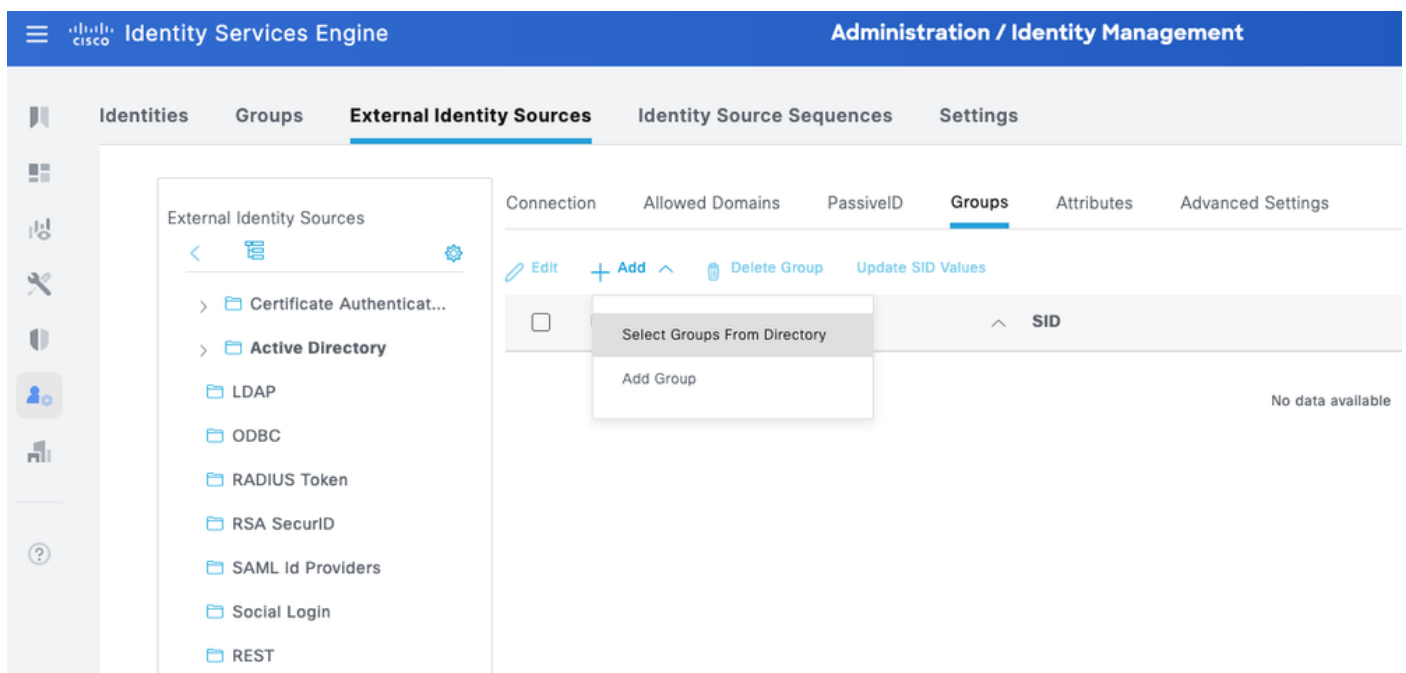
☒ Store Credentials ⓘ

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

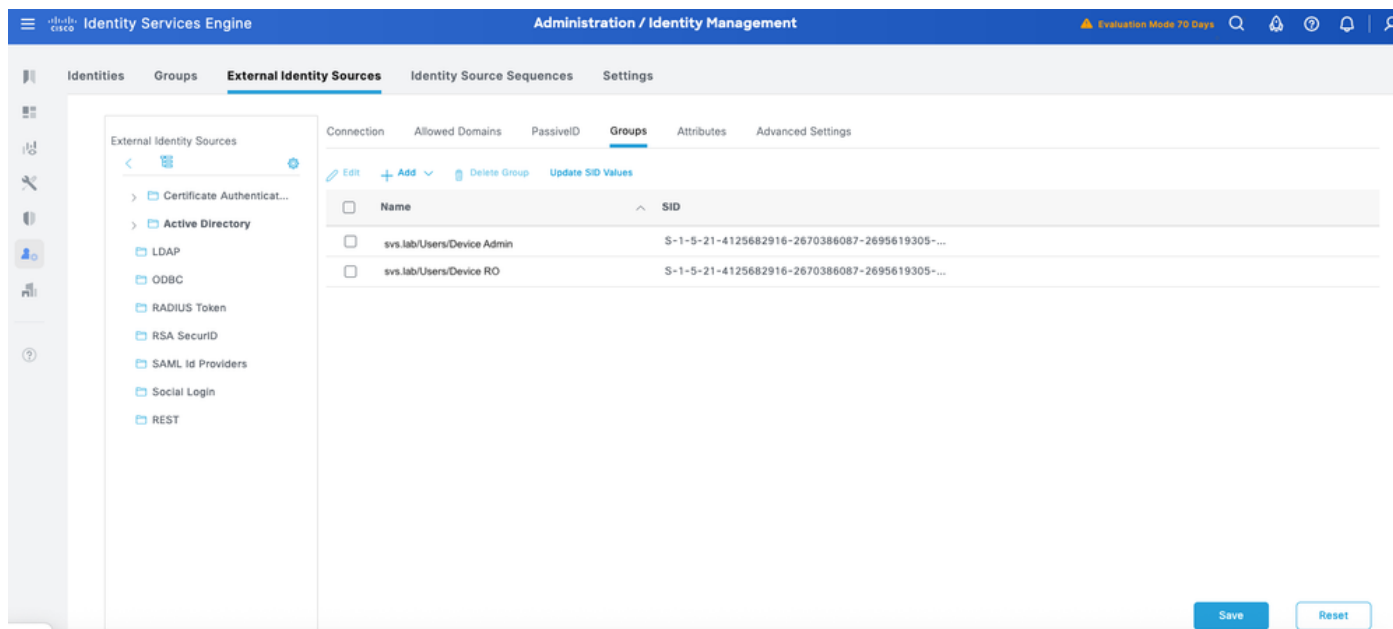
Name
Filter

SID *
Filter

Type
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

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

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

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

IOS XE_RW - Beheerdersprofiel

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

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

Stap 3. Bevestig de configuratie en bewaar.

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'. The main navigation menu on the left lists: Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements (selected), Device Admin Policy Sets, and More. The 'Policy Elements' section is active, showing a breadcrumb trail: TACACS Profiles > IOSXE_RW. The main content area is titled 'TACACS Profile' and contains the following fields:

- Name:** IOSXE_RW
- Description:** (Empty text box)
- Task Attribute View / Raw View:** (Tabs, with 'Task Attribute View' selected)
- Common Tasks:**
 - Common Task Type:** Shell
 - Default Privilege:** 15 (with a dropdown arrow and '(Select 0 to 15)')
 - Maximum Privilege:** 15 (with a dropdown arrow and '(Select 0 to 15)')

IOS XE_RO - Gebruikersprofiel

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

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

Stap 3. Bevestig de configuratie en bewaar.

The screenshot shows the Cisco ISE 'Policy Elements' configuration page. The left sidebar contains a navigation menu with 'TACACS Profiles' selected. The main content area is titled 'Name IOSXE_RO'. Below this is a 'Description' field. Further down, there are tabs for 'Task Attribute View' (selected) and 'Raw View'. Under 'Task Attribute View', there is a section for 'Common Tasks' with a 'Common Task Type' dropdown set to 'Shell'. Below this, there are four task configuration rows:

Task Name	Privilege	Access Control List	Auto Command
☒ Default Privilege	1 (Select 0 to 15)	☐	☐
☒ Maximum Privilege	1 (Select 0 to 15)	☐	☐
☐ Access Control List		☐	☐
☐ Auto Command		☐	☐

TACACS+-opdrachtreeksen configureren

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

CISCO_IOS XE_RW - Opdrachtset voor beheerders

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

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

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring a TACACS Command Set. The breadcrumb trail is: TACACS Command Sets > CISCO_IOSXE_RW Command Set. The Name field is filled with 'CISCO_IOSXE_RW'. The Description field is empty. Under the Commands section, the checkbox 'Permit any command that is not listed below' is checked. At the bottom, there is a table with columns: Grant, Command, and Arguments.

Grant	Command	Arguments
☐		

CISCO_IOS XE_RO - Operator Command Set

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

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

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

Stap 4. Bevestig de gegevens en klik op Opslaan.

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring a TACACS Command Set. The breadcrumb trail is: TACACS Command Sets > CISCO_IOSXE_RO Command Set. The Name field is filled with 'CISCO_IOSXE_RO'. The Description field is empty. Under the Commands section, the checkbox 'Permit any command that is not listed below' is unchecked. At the bottom, there is a table with columns: Grant, Command, and Arguments.

Grant	Command	Arguments
☐	PERMIT	show

Apparaatbeheerbeleidssets configureren

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

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

The screenshot shows the 'Device Admin Policy Sets' configuration page in the Cisco ISE console. The page has a blue header with the Cisco Identity Services Engine logo and the title 'Work Centers / Device Administration'. Below the header is a navigation bar with tabs: Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements, and Device Admin Policy Sets (selected). The main content area shows a table of Policy Sets. There is one policy set named 'IOS-XE devices' with a status of 'On'. The conditions are 'DEVICE-Device Type EQUALS All Device Types#IOS-XE'. The allowed protocols are 'Default Device Admin'. The page includes buttons for 'Reset', 'Reset Policy Set Hit Counts', and 'Save'.

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.

The screenshot shows the 'Authentication Policy' configuration page in the Cisco ISE console. The page has a blue header with the Cisco Identity Services Engine logo and the title 'Work Centers / Device Administration'. Below the header is a navigation bar with tabs: Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements, Device Admin Policy Sets, Reports, and Settings. The main content area shows a table of Authentication Policies. There is one policy set named 'Default' with a status of 'On'. The conditions are 'Default'. The page includes buttons for 'Reset', 'Reset Policy Set Hit Counts', and 'Save'. A dropdown menu is open showing options for 'If Auth fail', 'If User not found', and 'If Process fail'.

Stap 4. Definieer het autorisatiebeleid.

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

Voorbeeld:

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

Identity Services Engine Work Centers / Device Administration

Policy Sets → IOS-XE devices

Reset Reset Policy Set Hit Counts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	IOS-XE devices		DEVICE-Device Type EQUALS All Device Types#IOS-XE	Default Device Admin	0

> Authentication Policy(1)

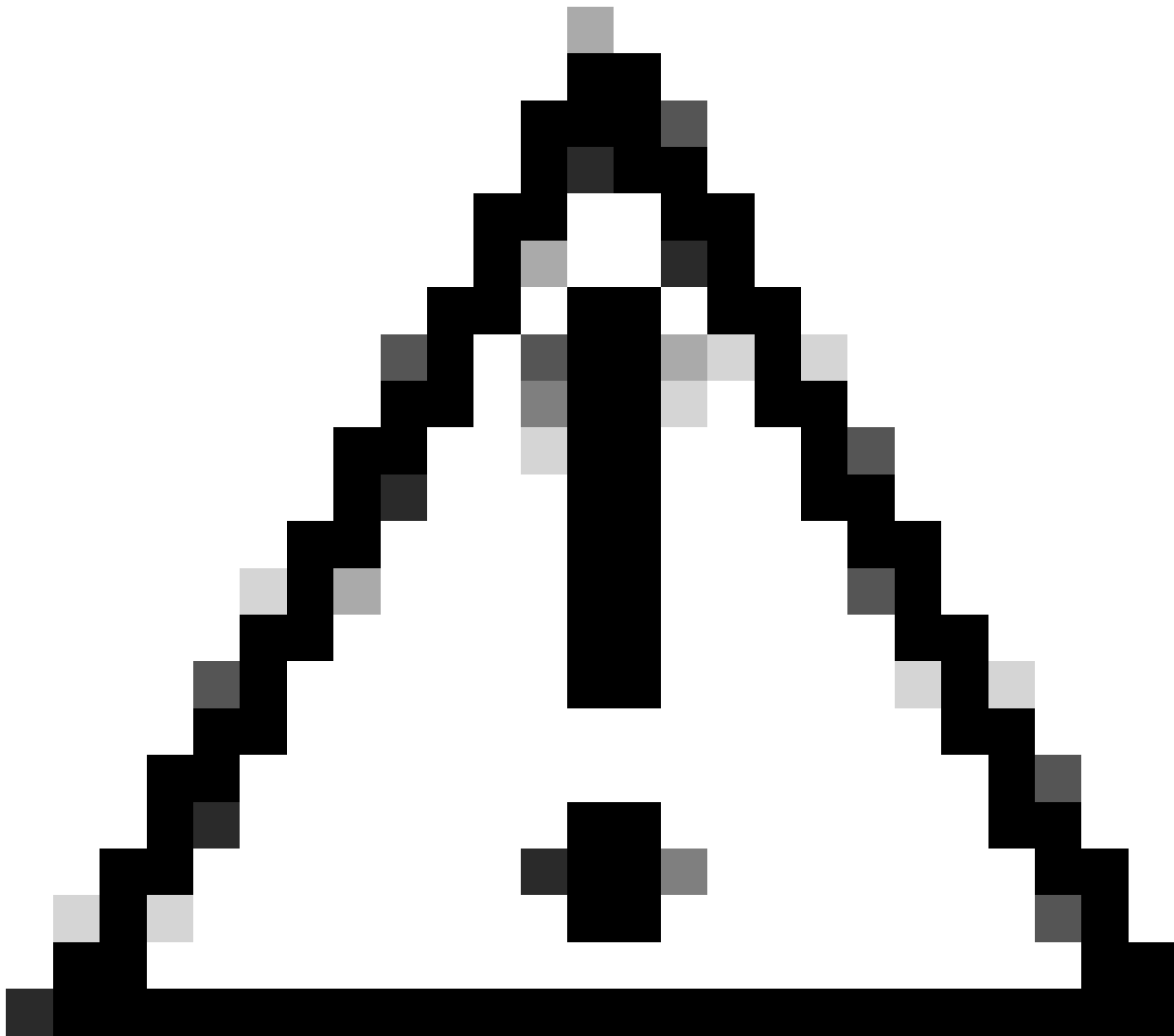
> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

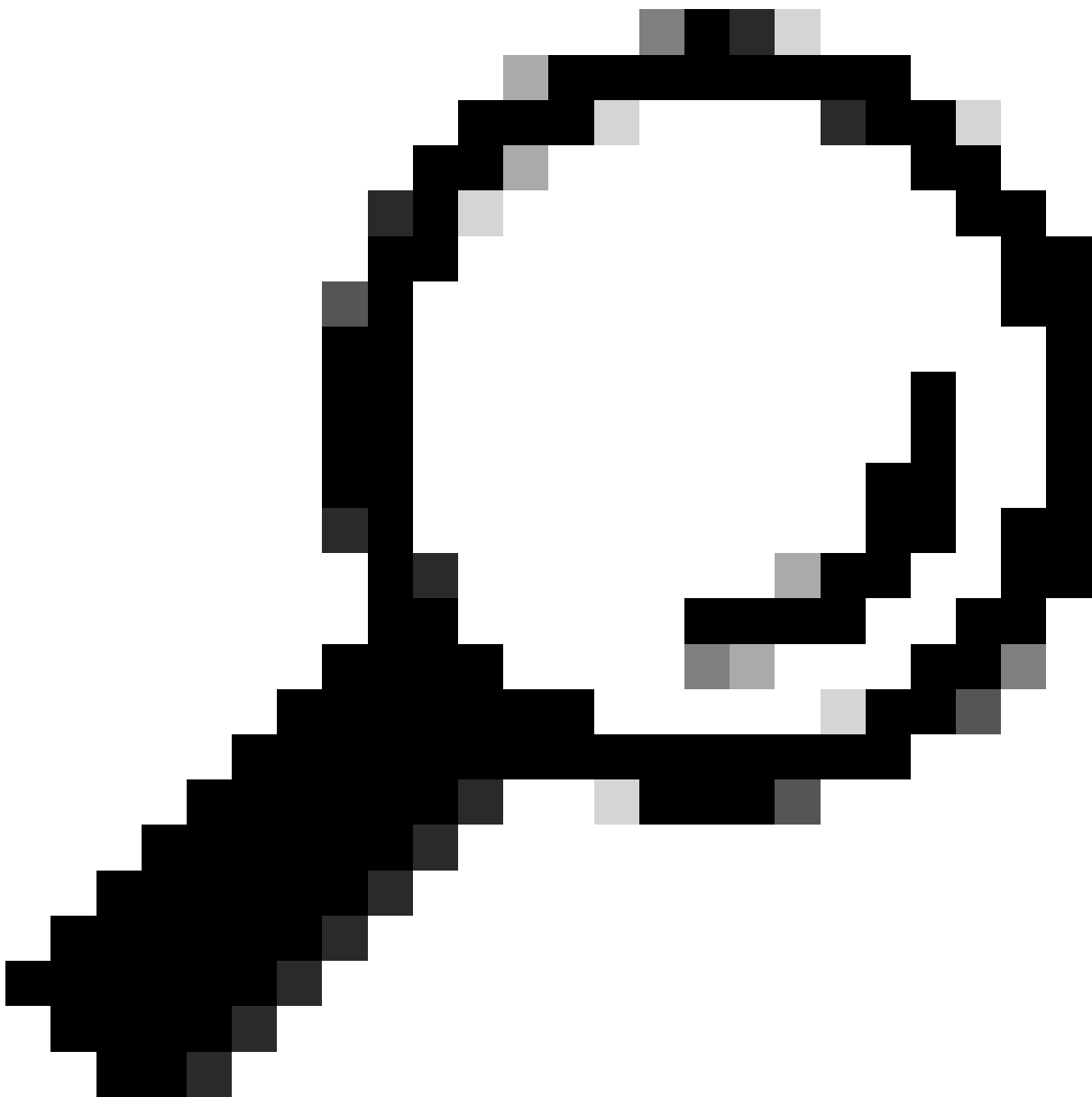
✓ Authorization Policy(3)

Status	Rule Name	Conditions	Results			Hits	Actions
			Command Sets	Shell Profiles			
✓	Authorization Rule RO	svs.lab-ExternalGroups EQUALS svs.lab/Users/Device RO	CISCO_IOSXE_RO	IOSXE_RO	0		
✓	Authorization Rule RW	svs.lab-ExternalGroups EQUALS svs.lab/Users/Device Admin	CISCO_IOSXE_RW	IOSXE_RW	0		
✓	Default		DenyAllCommands	Deny All Shell Profile	0		

Deel 2 - Cisco IOS XE configureren voor TACACS+ via TLS 1.3



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



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

Configuratiemethode 1 - Sleutelpaar gegenereerd door apparaat

TACACS+-serverconfiguratie

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

```
ip domain name sv.s.lab
```

```
crypto key generate ec keysiz 256 label sv-256ec-key
```

Trustpoint-configuratie

Stap 1 Maak een routervertrouwenspunt en koppel het sleutelpaar.

```
crypto pki trustpoint sv_cat9k
  enrollment terminal pem
  subject-name C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=cat9k.sv.s.lab
  serial-number none
  ip-address none
  revocation-check none
  eckeypair sv-256ec-key
```

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

```
<#root>
```

```
cat9k(config)#
```

```
crypto pki authenticate sv_cat9k
```

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
```

```
MIIF1DCCA3ygAwIBAgIIIM10AsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZzAVBgNVBAGTDk5vbnRoIENhcnR5aW5hMRwwDgYDVQQHEwdSYWx1aWdo
MQ4wDAYDVQQKEwVkaXNjbzEMMAoGA1UECXMdU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNDI4MTcwNTAwWhcNMjUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUgA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBACTB1JhbGVpZ2gxDjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTV1MxEjAQBgNVBAMTCVNWUyBMWJJDQTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZU0yn2vIn6gKbx3M7vaRq
2YjwZ1zSH6EkEvxnJT+y+kksFD33GyHQepk7vfp4NFU50tQ4HC7t/A0v9grDa3QW
VwvV4MBBjHFM3s0J/ejgDYCMZhIAaPy0Zo5WLboOkXEiKjPLatKXojB8FVrhLF3O
jMBSqwa4/Wlniy5S+7s4FFxsCf20COWfBAsnrs0tatIIhmcnx+VLJP7MRm8f0w4m
mutNo7IhbJSrgAFXmj1bBjMmgsp0bULo/wxMHdTbtPBf11HRHTkNIo3qy04UADL2
WpoGhgT/FaxxBo2UBcnYVaP+jjREONYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7B0e8oDNKU6gX1ojKyLP/gC7j8AeP03ir+KZui8
b8X4iYn/67SbzZFhwn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
```

```
gJ+kQXe7QtT/u6m1MrtjE3gAEVpL334rTIxy9hpKZIkB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTA01xh60I4QnK+MNQKpTjt/E4
ydHl0rrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVL1783nTc9wYptQEPi5sw
83g9EMgKV0ARIiVUa/q7AgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAyb4
QgEBBAQDAgAHMBkGCWCGSAGG+EIBDQMFgptV1MgTGF1IENBMAOGCSqGSIb3DQEB
CwUAA4ICAQAIAIT308oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oK0dGayi
iSEkSSX9qyfLFINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
O+ja6zTQqj06lqJhmrSkyFbYf/ZTpe4d10zJsZjNsN0r8bF9nOA/7qNZLp3Z3cpU
PU0KdbiSvRqnPw3e8TfITVmAzcx8COI2SrYFMSUazo1VBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7a1uJapXkmnj5qPeGhN0pB
Q9r14reov4so2EspkXS7CrH9yGfPiYtprokz1UvZBZ8v1oI7YZmjFmem+5rT6Gnk
eU/1X7nV61SYG5W5K+I8uaKuyBHOMn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggz1P0dsS/i6Lo7ypYX0eB9HgVDCkzQsLXQuHGj/2WsgPgDRcjkvnyURk4Jx+Ib
xDrmo7e0XPpSW4l72a6K18CR3U2Cr4wsuvndPEq/qd2NRSBWffFOXe/AJHQG7STT
HaXLU9r2Ko603oecu8ysGTWl1It/9T1/F0b0xZRugWcpJrVoTgDGuA==
```

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

Certificate has the following attributes:

Fingerprint MD5: D9C404B2 EC08A260 EC3539E7 F54ED17D

Fingerprint SHA1: 0EB181E9 5A3ED780 3BC5A805 9A854A95 C83AC737

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

yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

cat9k(config)#

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

<#root>

cat9k(config)#

crypto pki enroll svcs_cat9k

% Start certificate enrollment ..

% The subject name in the certificate will include: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=cat9k.svs.lab

% The subject name in the certificate will include: cat9k.svs.lab

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

yes

Certificate Request follows:

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

```
MIIBfDCCASMAQAwgYQxGjAYBgNVBAMTEWdhD1rLnRtby5zdnMuY29tMQwwCgYD
VQQLewNTV1MxDjAMBgNVBAoTBUNpc2NvMQwwCgYDVQQHEwNSVFAXCzAJBgNVBAGT
Ak5DMQswCQYDVQQGEwJVUzEgMB4GCSqGSIb3DQEJAhYRY2F0OWsudG1vLnN2cy5j
b20wWTATBgqhkJOPQIBBggqhkJOPQMBBwNCAATpYE7atscrt14ddevCh3UgxjYi
4N4oBGWrpJBctKy4so8V5i6RXDt7kHgPzp14Qnf20bcXVODE1wtTAHHBrIXqoDww
OgYJKoZIhvcNAQkOMS0wKzAcBgNVHREETFATghFjYXQ5ay50bW8uc3ZzLmNvbTAL
```

```
BgNVHQ8EBAMCB4AwCgYIKoZIzj0EAwQDRwAwRAIgZqP2QTWm3ZZrmIphJ7+jSTER
40kTx2DiVs1c1Xf+vR4CIBcSb18DIYz84DmgMHUaf778/cmpe9cWakvdaxMWseBH
-----END CERTIFICATE REQUEST-----
```

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

Redisplay enrollment request? [yes/no]:

no

cat9k(config)#

Stap 4. CA-ondertekend certificaat importeren.

<#root>

cat9k(config)#

crypto pki import svcs_cat9k certificate

Enter the base 64 encoded certificate.

End with a blank line or the word "quit" on a line by itself

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

```
MIID8zCCAdugAwIBAgIIKfdYWg5WpskwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZzFzAVBgNVBAGTDk5vbnRoIENhcm9saW5hMRwwDgYDVQQHEwdSYWx1aWdo
MQ4wDAYDVQQKEwVDAxNjBzEMMAoGA1UECXMUDU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNTE0MTUxMjAwWhcNMjUwNTE0MTUxMjAwWjCBhDEaMBgGA1UEAxMR
Y2F0OWsudG1vLnN2cy5jb20xDDAKBgNVBAsTA1NWUzE0MAwGA1UEChMFQ21zY28x
DDAKBgNVBAcTA1JUUELMMAkGA1UECBMCTkMxCzAJBgNVBAYTA1VTMSAwHgYJKoZI
hvcNAQkCFhFjYXQ5ay50bW8uc3ZzLmNvbTBZMBMGByqGSM49AgEGCCqGSM49AwEH
A0IAB01gtTq2xyu2Xh1168KHdSDGNiLg3igEZaukkFy0rLiYjXmLpFc03uQeA/O
nXhCd/bRtxdU4MTXC1MAccGsheqjTTBLMB4GCWCGSAGG+EIBDQRRFg94Y2EgY2Vy
dG1maWNhdGUwHAYDVRORBBUwE4IRY2F0OWsudG1vLnN2cy5jb20wCwYDVR0PBAQD
AgeAMAOGCSqGSIb3DQEBGwUAA4ICAQB0bgKVykeyVC9Usvuu0AUsGaZHGwy2H9Yd
m5vIau6PjczkCzIoAIghHPGQhIgpEcRqtGyXPZ2r8TCJP11WXNN/G73sFyWAHzY
RtmIM5KIojiDHLtiFpayxv9juDu0ZRx+wYR2PIQ5eLv1bafg7K8E82sq0Cf0tcPr
Oc0NU8UCxq0bd0gu4XsdBN1+wcWFqeQSDLP7nxvh00m/LXwCWUhwgVio0AuU2Fe
k5NthtvdXNAhRAImQdTyq6u/yB7vwTwJHcRiJc5USsyZCsTBb6RvL+HsXqBgXGc5
1xCS0LtY0dUxFipJyK2MOZBY2zq2cNSc8Xbso5/OEQmnHtpWPvj4rSPUHQSY+4m
Qq2Sn3iqf4mGh/A08T4iXfWDwfNezh7ZxMsCSCK/ZR1ELZ2hj60fzwX1H27Uf8XU
ecr0Wx+WzRn7LVRCaGQzFkukfi8S4DLLNtxNHFSLBVX5yHXCLEL+CQ7n8Z/pxcB
VVRpitwN3Zb09poZyWiRLTnBsb42xNaWiL9bjQznA0iTDfmfFFourBsaAioz7ouY
2r1Mh+OpE83Uu+41OTMawDgGiEv7iaiJ6xWc95EC+Adm0x3FvBXMtIM9qr7WwHW6
3C2hVYHJH254e1V5+H8iiz7rovEPm8ZDsnvYpJn4Km3iDvBNqp/vvAHOFcyXrvG6
3i/1b9erGQ==
```

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

% Router Certificate successfully imported

cat9k(config)#

TACACS & AAA met TLS-configuratie

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

```
tacacs server sv_s_tacacs
  address ipv4 10.225.253.209
  single-connection
  tls port 6049
  tls idle-timeout 60
  tls connection-timeout 60
  tls trustpoint client sv_s_cat9k
  tls ip tacacs source-interface GigabitEthernet0/0
  tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ sv_s_tls
  server name sv_s_tacacs
  ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

Stap 2. AAA-methoden configureren.

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

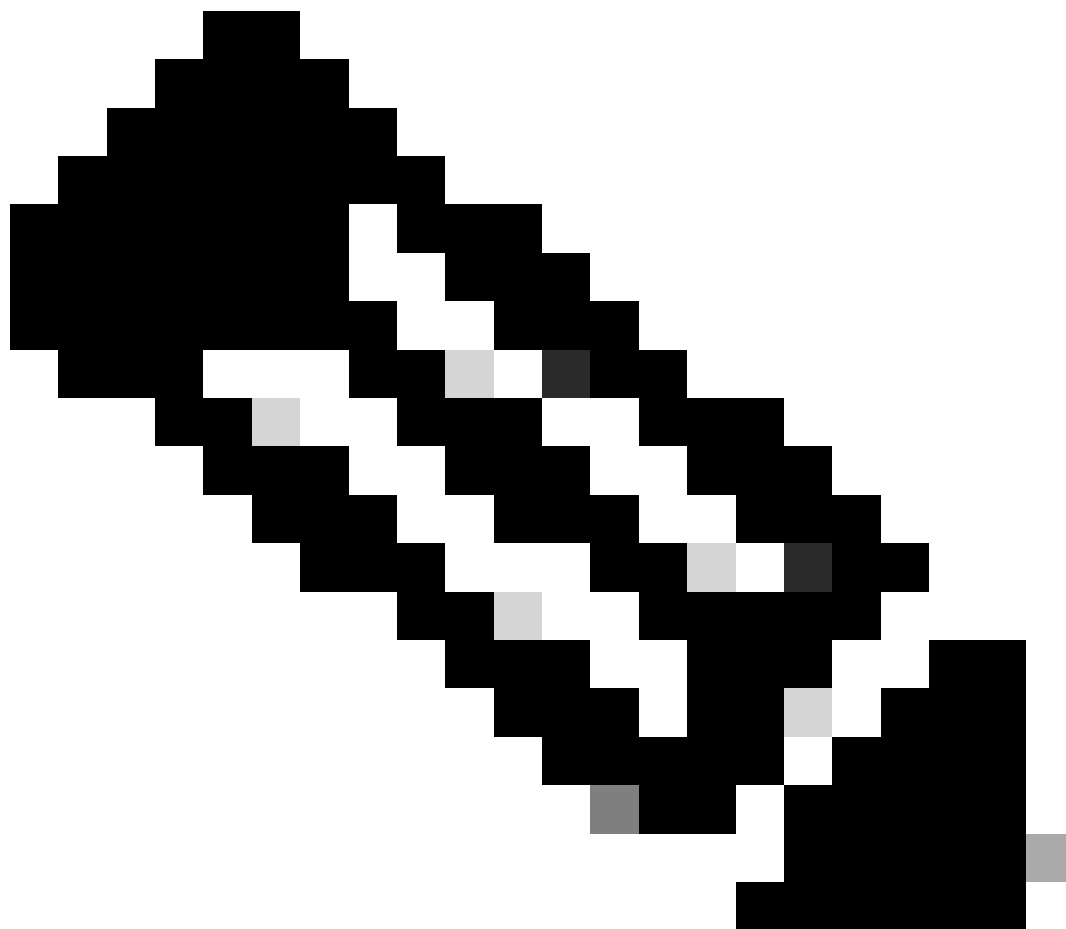
Configuratiemethode 2 - CA-gegenereerd sleutelpaar

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

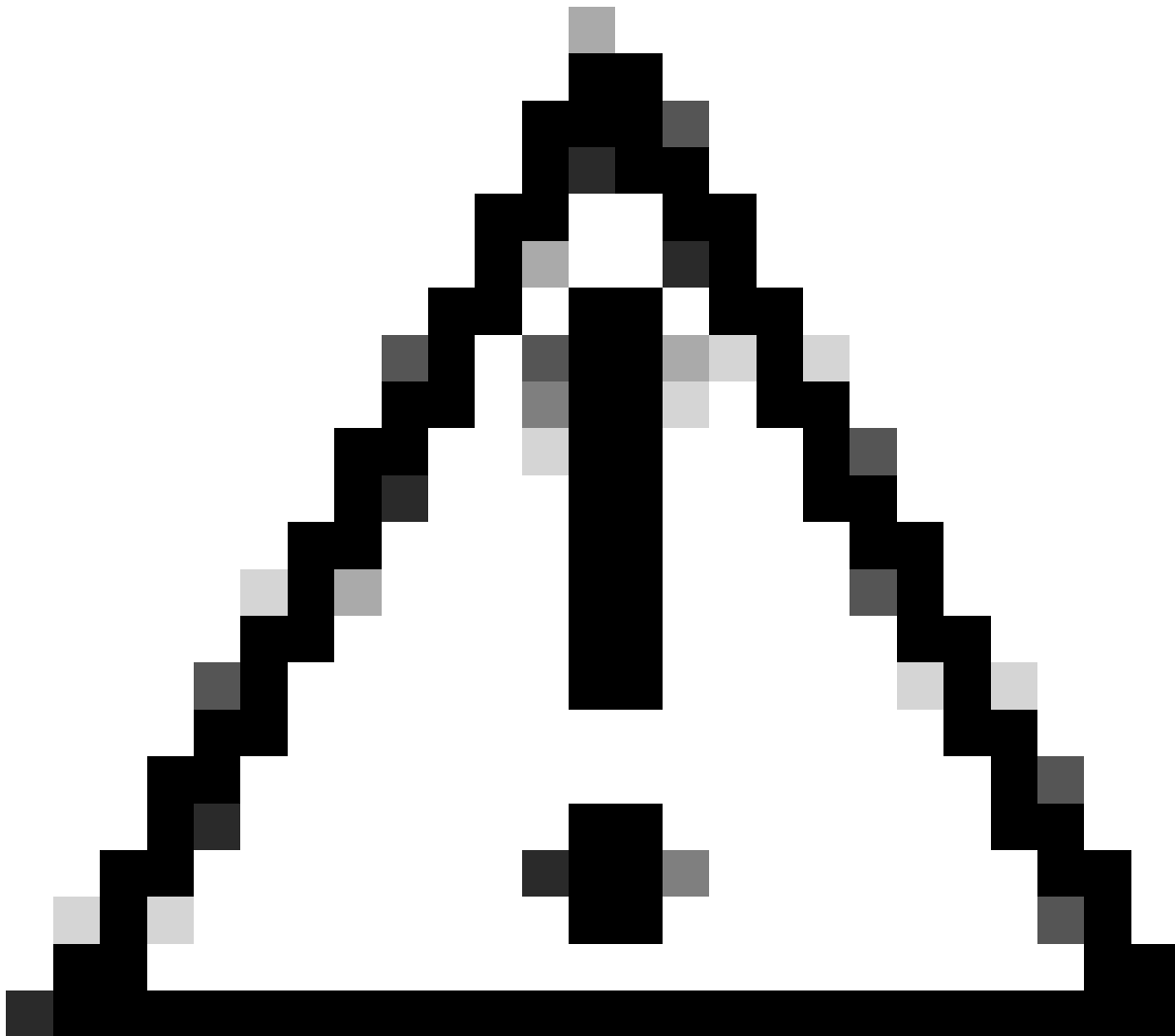
Stap 1. Maak een client trustpoint aan.

```
cat9k(config)#crypto pki trustpoint sv_s_cat9k_25jun17
cat9k(ca-trustpoint)#revocation-check none
```

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



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



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

```
<#root>
```

```
cat9k#
```

```
copy sftp bootflash: vrf Mgmt-vrf
```

```
Address or name of remote host [10.225.253.247]?
```

```
Source username [svs-user]?
```

```
Source filename [cat9k.svs.lab.pfx]? /home/svs-user/upload/cat9k-25jun17.pfx
```

```
Destination filename [cat9k-25jun17.pfx]?
```

```
Password:
```

```
!
```

```
2960 bytes copied in 3.022 secs (979 bytes/sec)
```

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

<#root>

cat9k#

crypto pki import svc_cat9k_25jun17 pkcs12 bootflash:cat9k-25jun17.pfx

password C1sco.123

% Importing pkcs12...Reading file from bootflash:cat9k-25jun17.pfx

CRYPTO_PKI: Imported PKCS12 file successfully.

cat9k#

cat9k#

show crypto pki certificates svc_cat9k_25jun17

Certificate

Status: Available

Certificate Serial Number (hex): 5860BF33A2033365

Certificate Usage: General Purpose

Issuer:

cn=SVS LabCA

ou=SVS

o=Cisco

l=Raleigh

st=North Carolina

c=US

Subject:

Name: cat9k.svs.lab

e=pkalkur@cisco.com

cn=cat9k.svs.lab

ou=svs

o=cisco

l=rtg

st=nc

c=us

Validity Date:

start date: 17:56:00 UTC Jun 17 2025

end date: 17:56:00 UTC Jun 17 2026

Associated Trustpoints: svc_cat9k_25jun17

CA Certificate

Status: Available

Certificate Serial Number (hex): 20CD7402C4DA37F5

Certificate Usage: General Purpose

Issuer:

cn=SVS LabCA

ou=SVS

o=Cisco

l=Raleigh

st=North Carolina

c=US

Subject:

cn=SVS LabCA

ou=SVS

o=Cisco

l=Raleigh

st=North Carolina

c=US

Validity Date:

start date: 17:05:00 UTC Apr 28 2025

end date: 17:05:00 UTC Apr 28 2035

Associated Trustpoints: svc_cat9k_25jun17 svc_cat9k

Storage: nvram:SVSLabCA#37F5CA.cer

TACACS & AAA met TLS-configuratie

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

```
tacacs server svb_tacacs
  address ipv4 10.225.253.209
  single-connection
  tls port 6049
  tls idle-timeout 60
  tls connection-timeout 60
  tls trustpoint client svb_cat9k
  tls ip tacacs source-interface GigabitEthernet0/0
  tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ svb_tls
  server name svb_tacacs
  ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

Stap 2. AAA-methoden configureren.

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

Verificatie

De configuratie verifiëren.

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

Debug voor AAA en TACACS+.

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

! Below debugs will be needed only if there is any issue with SSL Handshake

```
debug ip tcp transactions
debug ip tcp packet
debug crypto pki transactions
debug crypto pki API
debug crypto pki messages
debug crypto pki server
debug ssl openssl errors
debug ssl openssl msg
debug ssl openssl states
clear logging
```

Over deze vertaling

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