

# Prime 3.1 TACACS-verificatie configureren tegen ISE 2.x

## Inhoud

[Inleiding](#)

[Vereisten](#)

[Configureren](#)

[Prime-configuratie](#)

[ISE-configuratie](#)

[Problemen oplossen](#)

## Inleiding

Dit document beschrijft hoe u de Prime-infrastructuur kunt configureren om via TACACS met ISE 2.x authentiek te verklaren.

## Vereisten

Cisco raadt u aan een basiskennis van deze onderwerpen te hebben:

- Identity Services Engine (ISE)
- Prime-infrastructuur

## Configureren

Cisco Prime Network Control System 3.1

Cisco Identity Services Engine 2.0 of hoger.

(Opmerking: ISE ondersteunt alleen TACACS vanaf versie 2.0, maar het is mogelijk om Prime te configureren om Radius te gebruiken. Prime bevat de lijst met RADIUS-kenmerken naast TACACS als u liever Radius wilt gebruiken, met een oudere versie van ISE of een oplossing van derden.)

## Prime-configuratie

Navigeren naar het volgende scherm: Administratie / Gebruikers/gebruikers, rollen en AA zoals hieronder te zien is.

Selecteer desgewenst het tabblad TACACS+ servers en selecteer de optie TACACS+ server toevoegen in de rechterbovenhoek en selecteer vervolgens Ga.

Op het volgende scherm is de configuratie van de TACACS-serveringang beschikbaar (dit moet

worden gedaan voor elke afzonderlijke TACACS-server)

Administration / Users / Users, Roles & AAA

AAA Mode Settings

Active Sessions

Change Password

Local Password Policy

RADIUS Servers

SSO Server Settings

SSO Servers

TACACS+ Servers

User Groups

Users

Add TACACS+ Server

IP Address

DNS Name

\* Port 49

Shared Secret Format ASCII

\* Shared Secret

\* Confirm Shared Secret

\* Retransmit Timeout 5 (secs)

\* Retries 1

Authentication Type PAP

Local Interface IP 192.168.10.154

Save Cancel

Hier moet u of IP-adres of DNS-adres van de server invoeren, evenals de gedeelde beveiligingstoets. Let ook op de IP-interface die u wilt gebruiken, aangezien hetzelfde IP-adres later moet worden gebruikt voor de AAA-client in ISE.

Om de configuratie op Prime te voltooien. U moet TACACS onder Beheer / Gebruikers / gebruikers, Roles & AAA inschakelen onder het tabblad Instellingen AAA-modus.

(Opmerking: Aanbevolen wordt om de back-up voor lokaal inschakelen te controleren, met ALLEEN een serverrespons of de optie On (geen respons of storing), in het bijzonder tijdens het testen van de configuratie

Administration / Users / Users, Roles & AAA

AAA Mode Settings

Active Sessions

Change Password

Local Password Policy

RADIUS Servers

SSO Server Settings

SSO Servers

TACACS+ Servers

User Groups

Users

AAA Mode Settings

AAA Mode

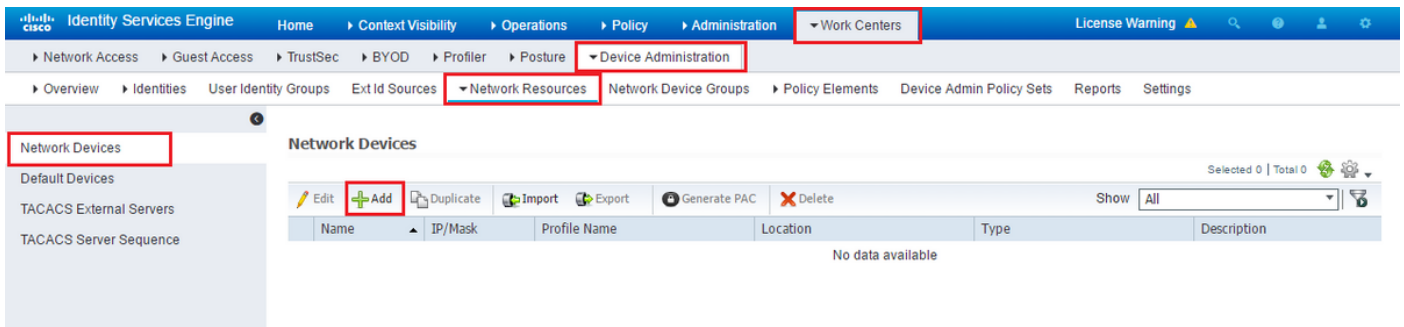
Local  RADIUS  TACACS+  SSO

Enable fallback to Local ONLY on no server respons:

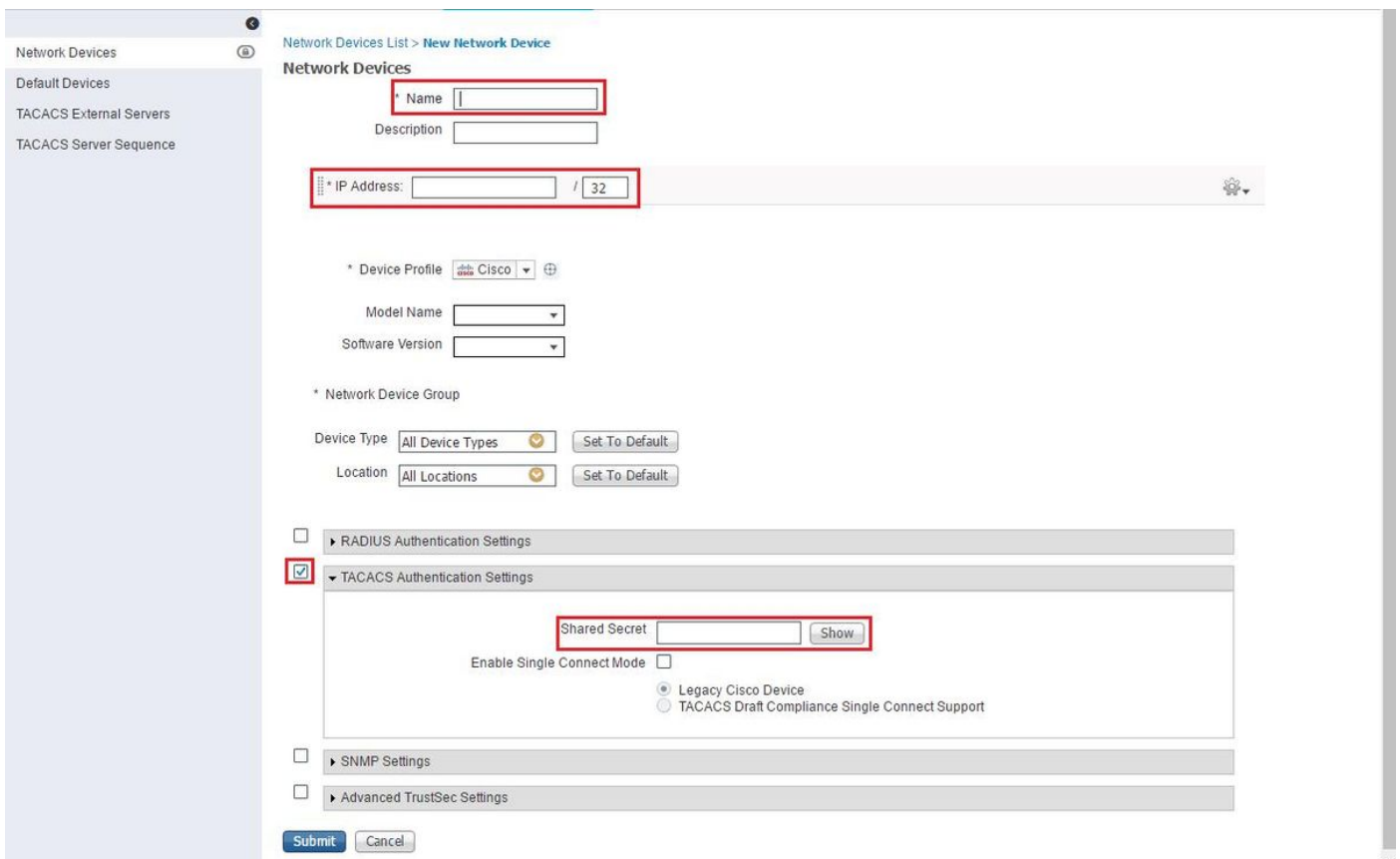
Save

## ISE-configuratie

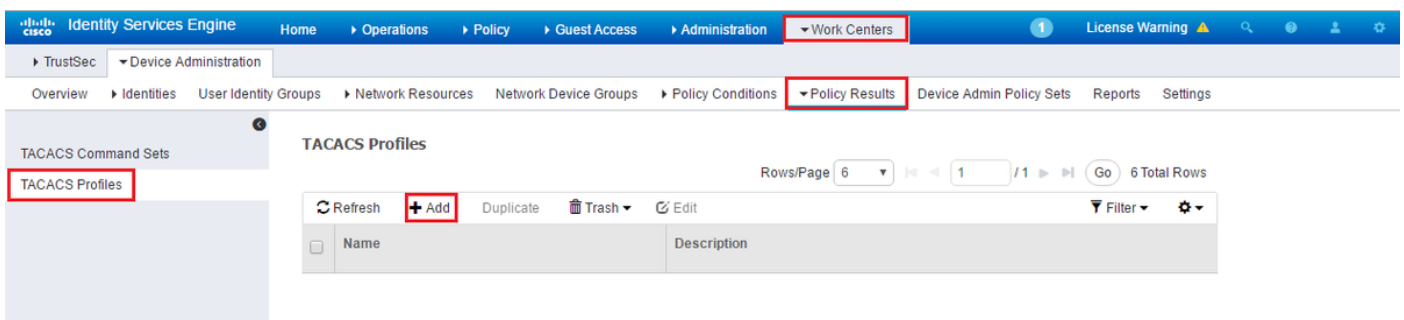
Prime als AAA-client op ISE configureren op  
werkcenters/apparaatbeheer/netwerkbronnen/netwerkapparaten/toevoegen



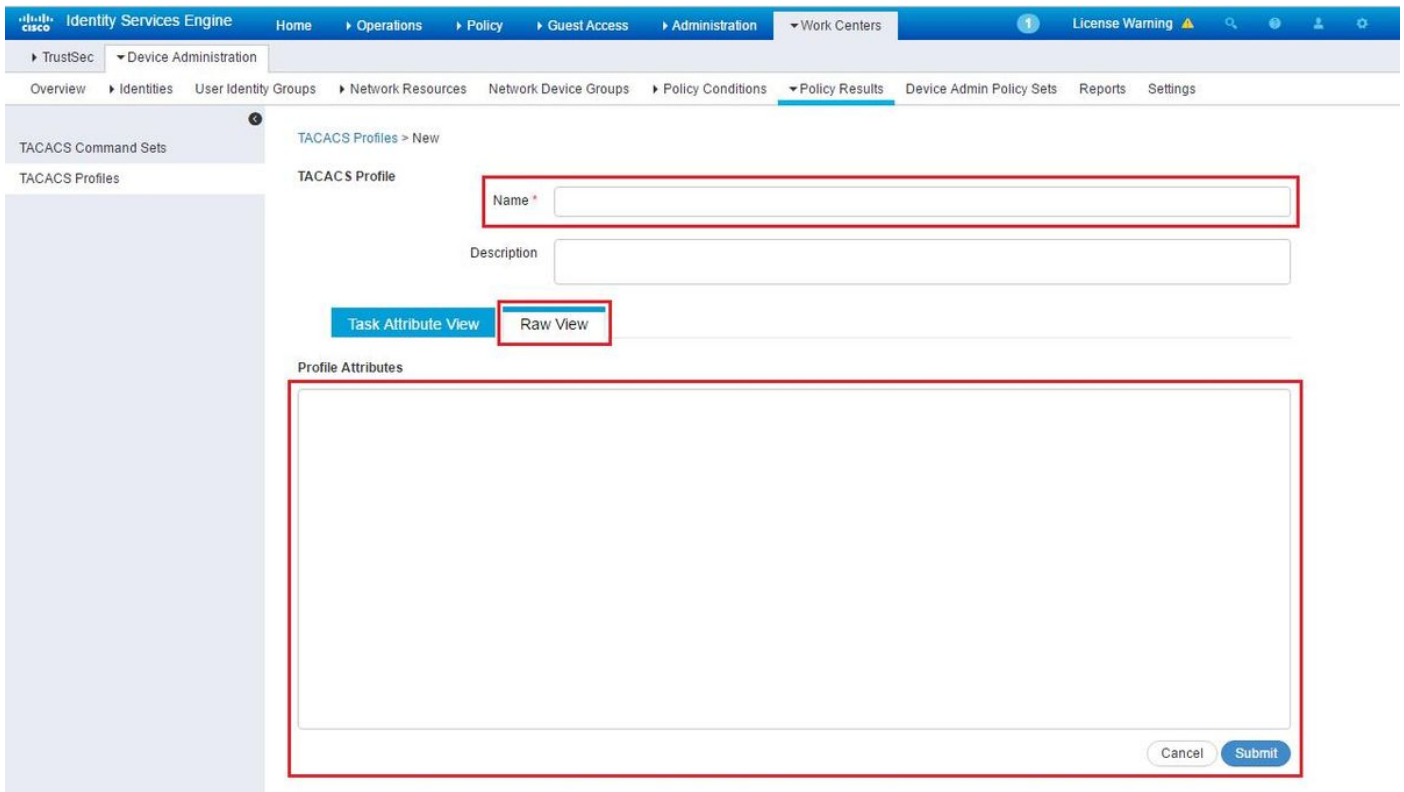
Voer de informatie in voor de Prime-server. De gewenste eigenschappen die u moet opnemen zijn Naam, IP-adres, selecteer de optie voor TACACS en het gedeelde geheim. Daarnaast kunt u een apparaattype toevoegen, specifiek voor Prime, om later als voorwaarde voor de vergunningsregel of andere informatie te gebruiken. Dit is echter optioneel.



Maak vervolgens een TACACS-profielresultaat om de gewenste eigenschappen van ISE naar Prime te verzenden, om het juiste toegangsniveau te bieden. Blader naar werkcentra/beleidsresultaten/TACIS-profielen en selecteer de optie Toevoegen.



Configureer de naam en gebruik de optie Raw bekijken om de eigenschappen onder het vakje Profile attributes in te voeren. De eigenschappen zullen van de server zelf komen.



Verkrijg de eigenschappen onder het scherm van Beheer / Gebruikers/gebruikers, Roles & AAA en selecteer het tabblad Gebruikersgroepen. Hier selecteert u het groepstoegangs niveau dat u wilt bieden. In dit voorbeeld wordt de toegang tot de beheerder verleend door de juiste lijst van de taak aan de linkerkant te selecteren.

Administration / Users / Users, Roles & AAA

AAA Mode Settings	User Groups			
Active Sessions	Group Name	Members	Audit Trail	View Task
Change Password	Admin	JP		<b>Task List</b>
Local Password Policy	Config Managers			Task List
RADIUS Servers	Lobby Ambassador	User1 , CostaRica , Yita		Task List
SSO Server Settings	Monitor Lite			Task List
SSO Servers	NBI Credential			Task List
TACACS+ Servers	NBI Read			Task List
<b>User Groups</b>	NBI Write			Task List
Users	North Bound API			Task List
	Root	root		Task List
	Super Users			Task List
	System Monitoring			Task List
	User Assistant			Task List
	User Defined 1			Task List
	User Defined 2			Task List
	User Defined 3			Task List
	User Defined 4			Task List
	mDNS Policy Admin			Task List

Kopieer alle TACACS-aangepaste eigenschappen.

- AAA Mode Settings
- Active Sessions
- Change Password
- Local Password Policy
- RADIUS Servers
- SSO Server Settings
- SSO Servers
- TACACS+ Servers
- User Groups**
- Users

**Task List**

Please copy and paste the appropriate protocol data below into the custom/vendor-specific attribute field in your AAA server.

**TACACS+ Custom Attributes**

```
role0=Admin
task0=Discovery Schedule Privilege
task1=Mesh Reports
task2=Saved Reports List
task3=Monitor Menu Access
task4=Device WorkCenter
task5=Inventory Menu Access
task6=Add Device Access
task7=Config Audit Dashboard
task8=Custom NetFlow Reports
task9=Apic Controller Read Access
task10=Configuration Templates Read Access
task11=Alarm Policies Edit Access
task12=High Availability Configuration
task13=View Job
task14=Incidents Alarms Events Access
task15=TAC Case Management Tool
task16=Configure Autonomous Access Point
Templates
task17=Import Policy Update
task18=PnP Profile Read-Write Access
task19=SSO Server AAA Mode
task20=Alarm Resource Access
```

**RADIUS Custom Attributes**

If the size of the RADIUS attributes on your AAA server is more than 4096 bytes, Please copy ONLY role attributes, application will retrieve the associated TASKS

```
NCS:role0=Admin
NCS:task0=Discovery Schedule Privilege
NCS:task1=Mesh Reports
NCS:task2=Saved Reports List
NCS:task3=Monitor Menu Access
NCS:task4=Device WorkCenter
NCS:task5=Inventory Menu Access
NCS:task6=Add Device Access
NCS:task7=Config Audit Dashboard
NCS:task8=Custom NetFlow Reports
NCS:task9=Apic Controller Read Access
NCS:task10=Configuration Templates Read Access
NCS:task11=Alarm Policies Edit Access
NCS:task12=High Availability Configuration
NCS:task13=View Job
NCS:task14=Incidents Alarms Events Access
NCS:task15=TAC Case Management Tool
NCS:task16=Configure Autonomous Access Point
Templates
NCS:task17=Import Policy Update
NCS:task18=PnP Profile Read-Write Access
NCS:task19=SSO Server AAA Mode
NCS:task20=Alarm Resource Access
```

Virtual Domain custom attributes are mandatory. To add custom attributes related to Virtual Domains, please click here.

Plakt ze vervolgens in het gedeelte Raw View van het profiel op ISE.

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is: Home > Operations > Policy > Guest Access > Administration > Work Centers. The left sidebar shows 'TrustSec' > 'Device Administration' > 'TACACS Profiles'. The main content area is titled 'TACACS Profile' and shows a form for 'Prime'. The 'Raw View' tab is selected, displaying a list of task attributes:

```
role0=Admin
task0=Discovery Schedule Privilege
task1=Mesh Reports
task2=Saved Reports List
task3=Monitor Menu Access
task4=Device WorkCenter
task5=Inventory Menu Access
task6=Add Device Access
task7=Config Audit Dashboard
task8=Custom NetFlow Reports
task9=Apic Controller Read Access
task10=Configuration Templates Read Access
task11=Alarm Policies Edit Access
task12=High Availability Configuration
task13=View Job
```

Buttons for 'Task Attribute View' and 'Raw View' are visible. At the bottom of the raw view area are 'Cancel' and 'Submit' buttons.

Virtuele eigenschappen van het Domein zijn verplicht. U vindt informatie over het Root-Domain onder Prime-beheer -> Virtuele domeinen.

The screenshot shows the Cisco Prime Infrastructure console. The breadcrumb navigation is: Administration > Virtual Domains. The main content area is titled 'Virtual Domains > ROOT-DOMAIN'. Below the title is a description: 'Virtual domains are logical groupings of devices and are used to control who can administer a group. After you add devices to Prime Infrastructure, you can configure virtual domains. Virtual domain filters allow users to configure devices, view alarms, and generate reports their assigned part of the network only.'

The configuration form includes the following fields:

- Name:** ROOT-DOMAIN
- Time Zone:** -- Select Time Zone --
- Email Address:** (empty field)
- Description:** ROOT-DOMAIN

'Submit' and 'Cancel' buttons are located at the bottom of the form.

Naam Prime Virtual Domain moet worden toegevoegd als eigenschap `virtuele-domein0="virtuele domeinnaam"`

The screenshot shows the Cisco ISE configuration interface for a TACACS Profile. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Policy Elements. The profile name is 'Prime Access'. The 'Raw View' tab is selected, showing the following profile attributes:

```
task162=Monitor Mobility Devices
task163=Context Aware Reports
task164=Voice Diagnostics
task165=Configure Choke Points
task166=RRM Dashboard
task167=Swim Delete
task168=Theme Changer Access
task169=Import Policy Update
task170=Design Endpoint Site Association Access
task171=Planning Mode
task172=Pick and Unpick Alerts
task173=Configure Menu Access
task174=Ack and Unack Security Index Issues
task175=Ack and Unack Alerts
task176=Auto Provisioning
virtual-domain0=ROOT-DOMAIN
```

Buttons for 'Cancel' and 'Save' are visible at the bottom right.

Zodra dat wordt gedaan moet u een regel maken om het Shell-profiel toe te wijzen dat in de vorige stap is gemaakt, onder Workcenters/Apparaatbeheer/Apparaatbeheerset

(Opmerking: De "Voorwaarden" zullen afhankelijk van de plaatsing verschillen, maar u kunt "Type apparaat" specifiek gebruiken voor Prime of een ander type filter, zoals het IP-adres van de premier, als een van de "Voorwaarden" zodat deze regel naar behoren filtert)

The screenshot shows the Cisco ISE configuration interface for Device Admin Policy Sets. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Device Admin Policy Sets. The 'Default' policy set is selected, showing the following configuration:

Status	Name	Description
<input checked="" type="checkbox"/>	Default	Tacacs_Default

Below this, the 'Authentication Policy' and 'Authorization Policy' sections are visible. The 'Authorization Policy' section shows a rule named 'Prime Rule' with the following conditions and command sets:

Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles
<input checked="" type="checkbox"/>	Prime Rule	if DEVICE-Device Type EQUALS All Device Types#Prime	then PermitAll AND	Prime
<input checked="" type="checkbox"/>	Tacacs_Default	if no matches, then	Select Profile(s) Deny All Shell Profile	

Op dit punt moet de configuratie zijn voltooid.

## Problemen oplossen



Als deze configuratie niet geslaagd is en als de lokale fall-back optie ingeschakeld is op Prime, kunt u een failover van ISE forceren door het IP-adres van Prime te verwijderen. Dit zal ervoor zorgen dat ISE niet reageert en het gebruik van lokale geloofsbrieven forceert. Als de lokale back-up ingesteld is om op basis van een nee te worden uitgevoerd, werken de lokale accounts nog steeds en krijgen ze toegang tot de klant.

Als ISE een succesvolle authenticatie laat zien en de juiste regel aanpast echter is Prime het verzoek nog steeds afwijzen, kunt u controleren of de eigenschappen in het profiel correct zijn ingesteld en er worden geen extra eigenschappen verzonden.