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.)

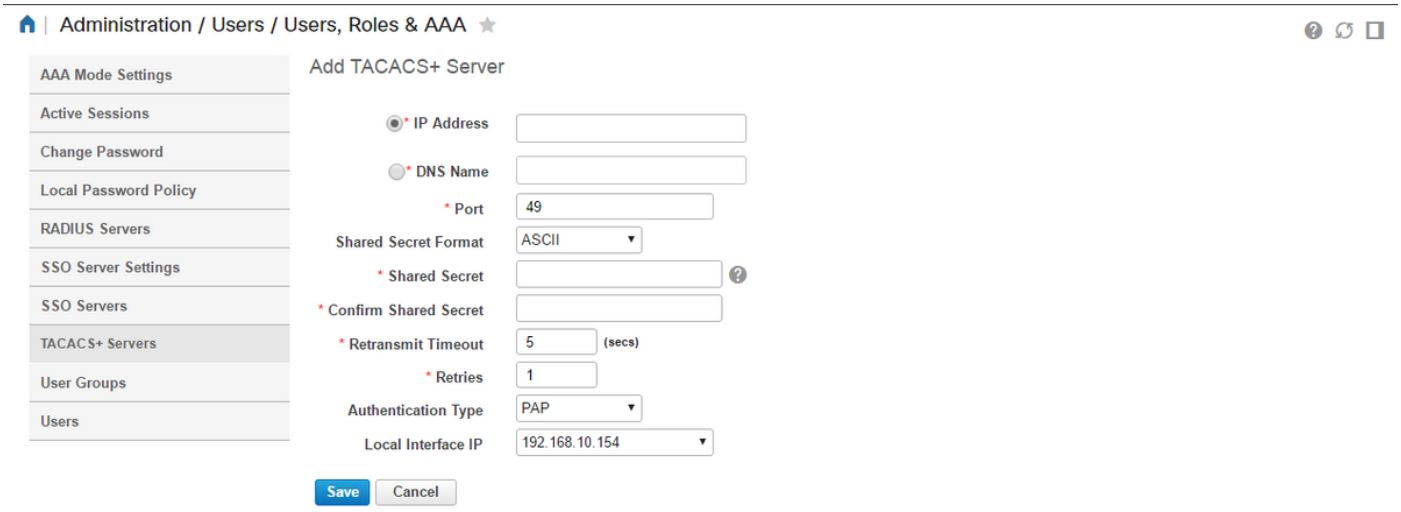
Prime-configuratie

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)



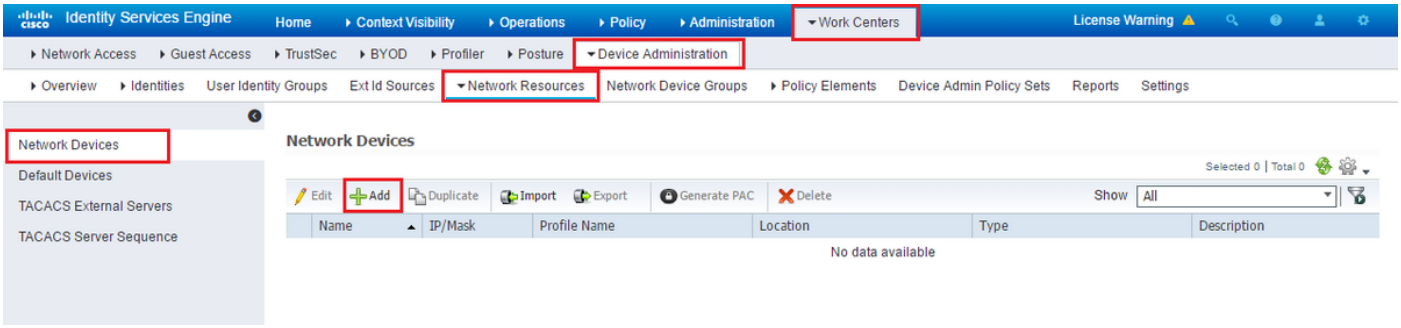
Hier moet u of IP-adres of DNS-adres van de server invoeren, evenals de gedeelde beveiligingstoets. Let ook op de IP-interface die u wilt gebruiken, aangezien hetzelfde IP-adres later moet worden gebruikt voor de AAA-client in ISE.

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

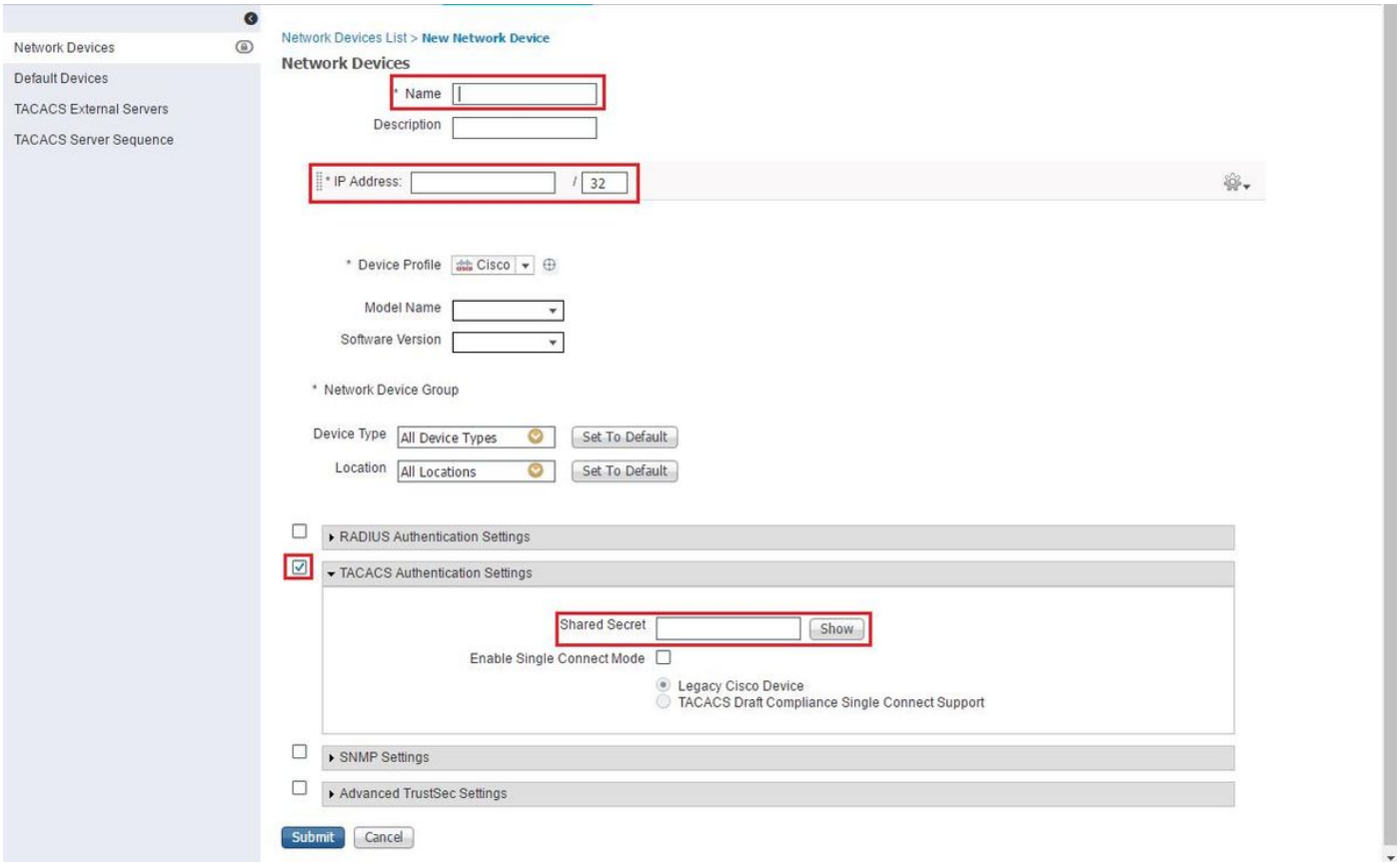
(Opmerking: Aanbevolen wordt om de back-up voor lokaal inschakelen te controleren, met ALLEEN een serverrespons of de optie On (geen respons of storing), in het bijzonder tijdens het testen van de configuratie

ISE-configuratie

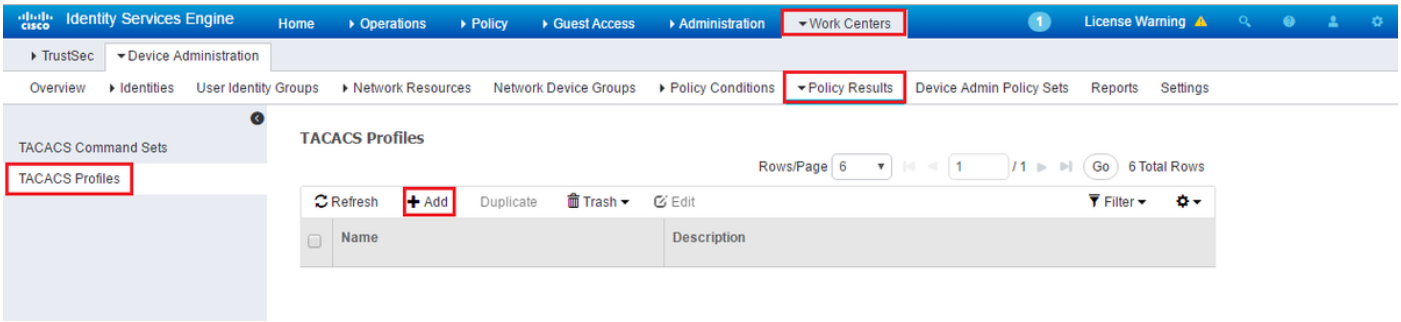
Prime als AAA-client op ISE configureren op werkcenters/apparaatbeheer/netwerkbronnen/netwerkapparaten/toevoegen



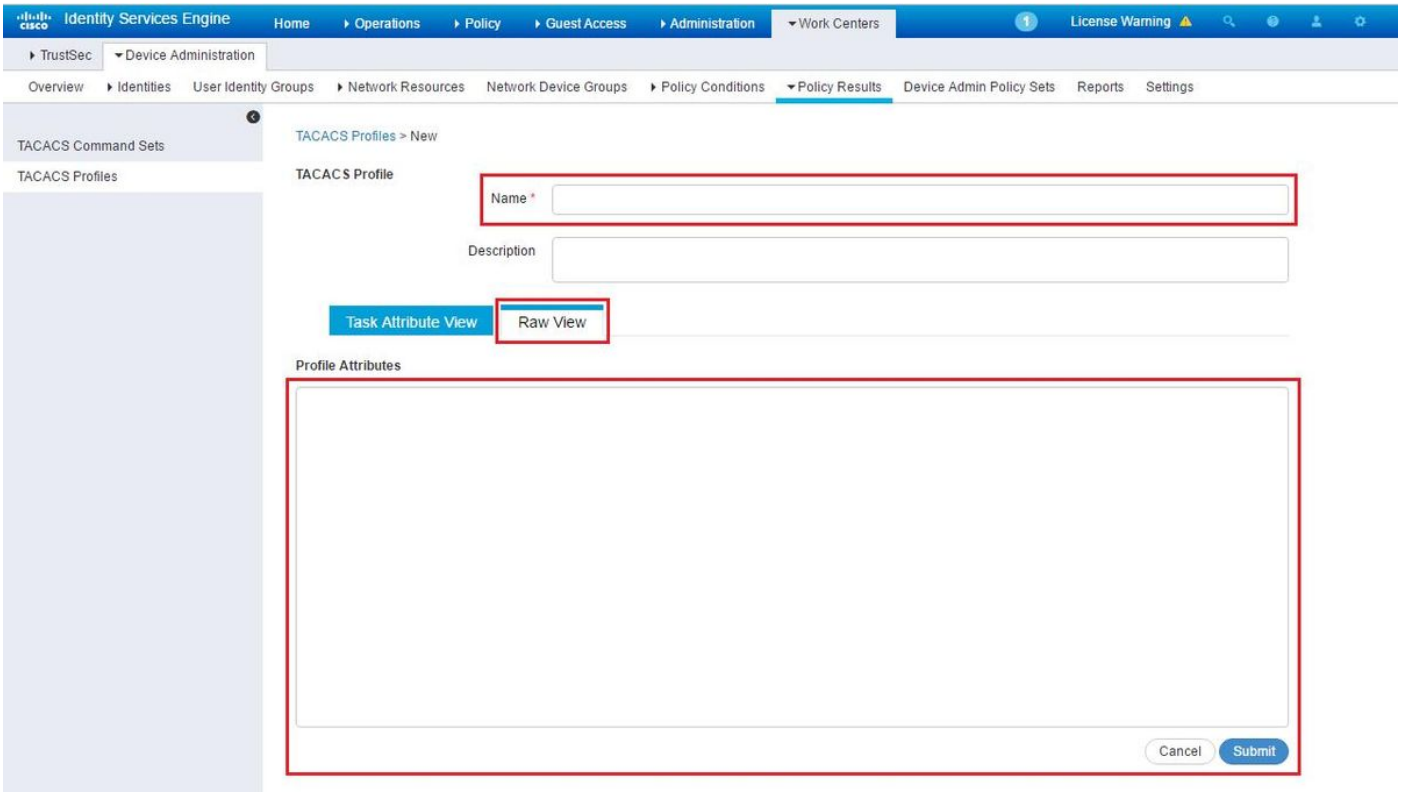
Voer de informatie in voor de Prime-server. De gewenste eigenschappen die u moet opnemen zijn Naam, IP-adres, selecteer de optie voor TACACS en het gedeelde geheim. Daarnaast kunt u een apparaattype toevoegen, specifiek voor Prime, om later als voorwaarde voor de vergunningsregel of andere informatie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



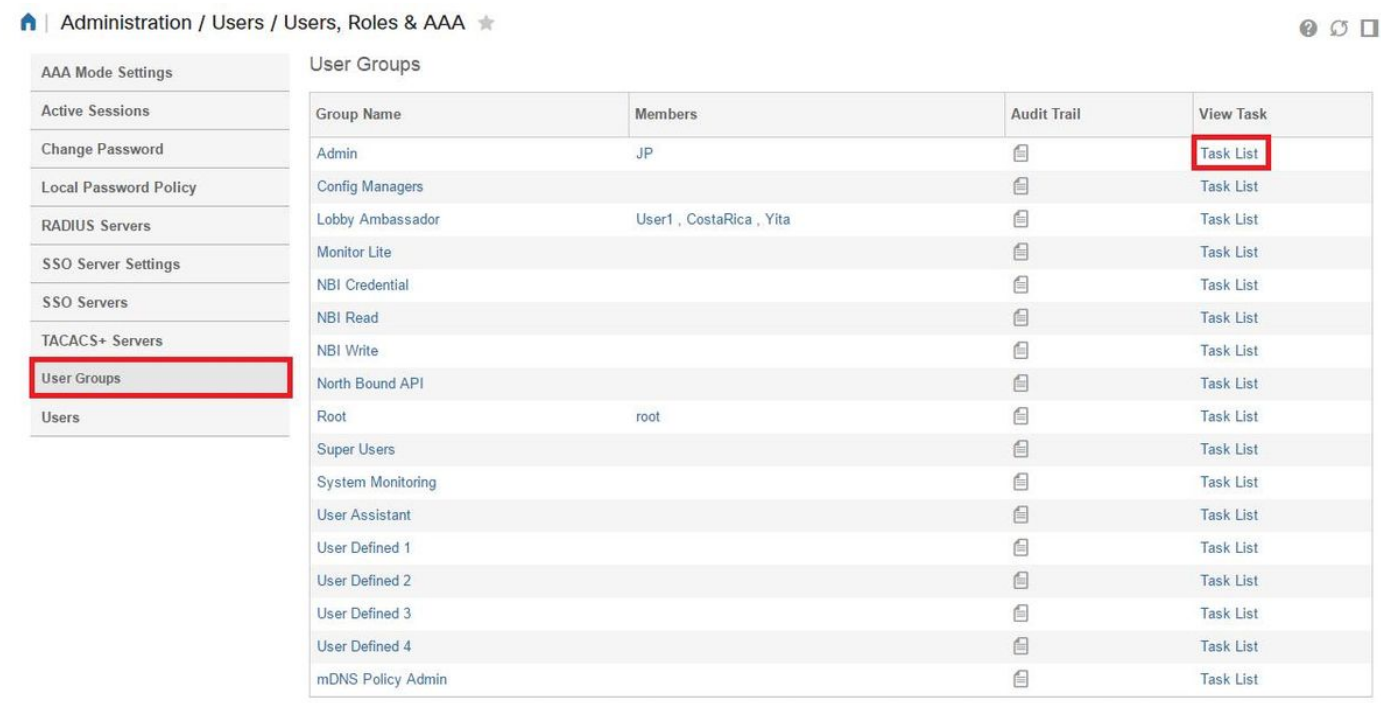
Maak vervolgens een TACACS-profielresultaat om de gewenste eigenschappen van ISE naar Prime te verzenden, om het juiste toegangsniveau te bieden. Blader naar werkcentra/beleidsresultaten/TACIS-profielen en selecteer de optie Toevoegen.



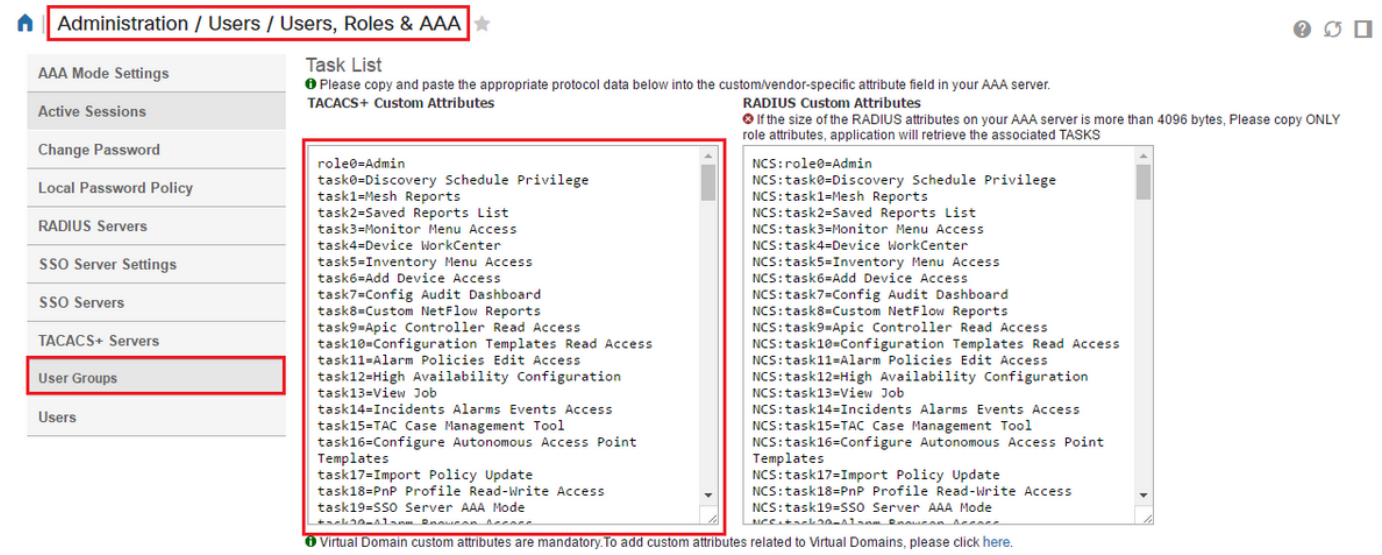
Configureer de naam en gebruik de optie Raw bekijken om de eigenschappen onder het vakje Profile attributes in te voeren. De eigenschappen zullen van de server zelf komen.



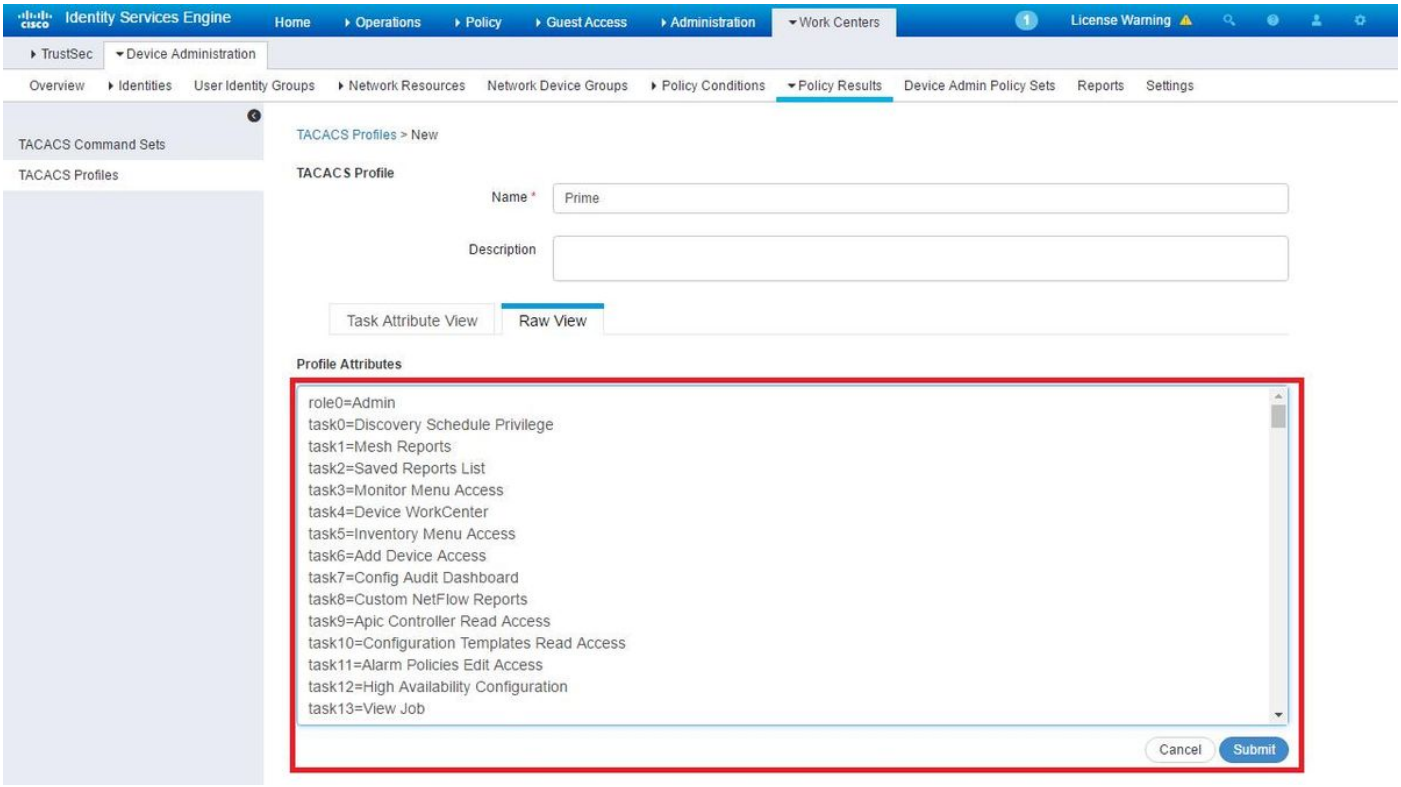
Verkrijg de eigenschappen onder het scherm van Beheer / Gebruikers/gebruikers, Roles & AAA en selecteer het tabblad Gebruikersgroepen. Hier selecteert u het groepstoegangsniveau dat u wilt bieden. In dit voorbeeld wordt de toegang tot de beheerder verleend door de juiste lijst van de taak aan de linkerkant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



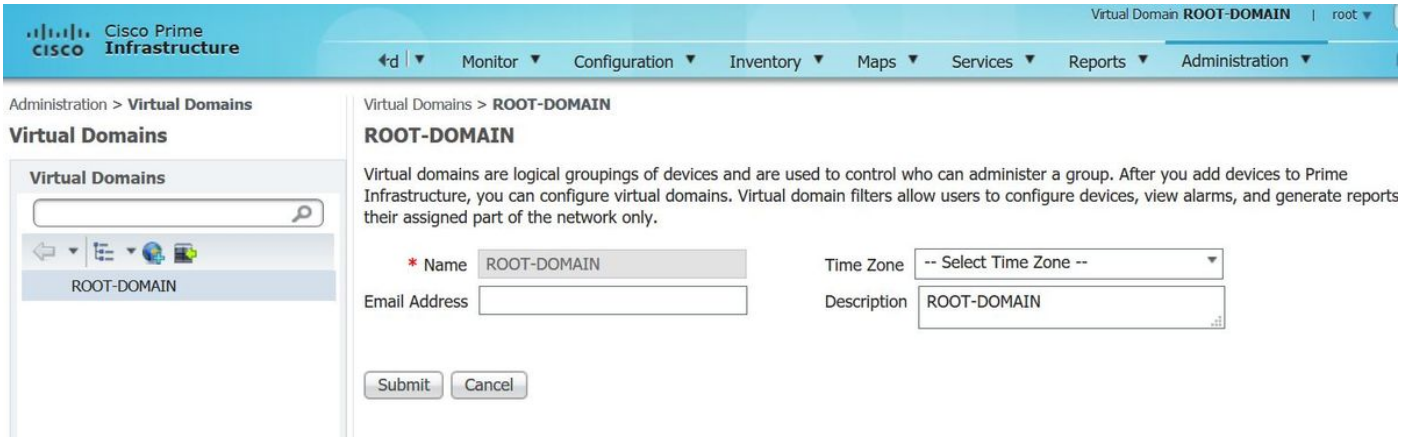
Kopieer alle TACACS-aangepaste eigenschappen.



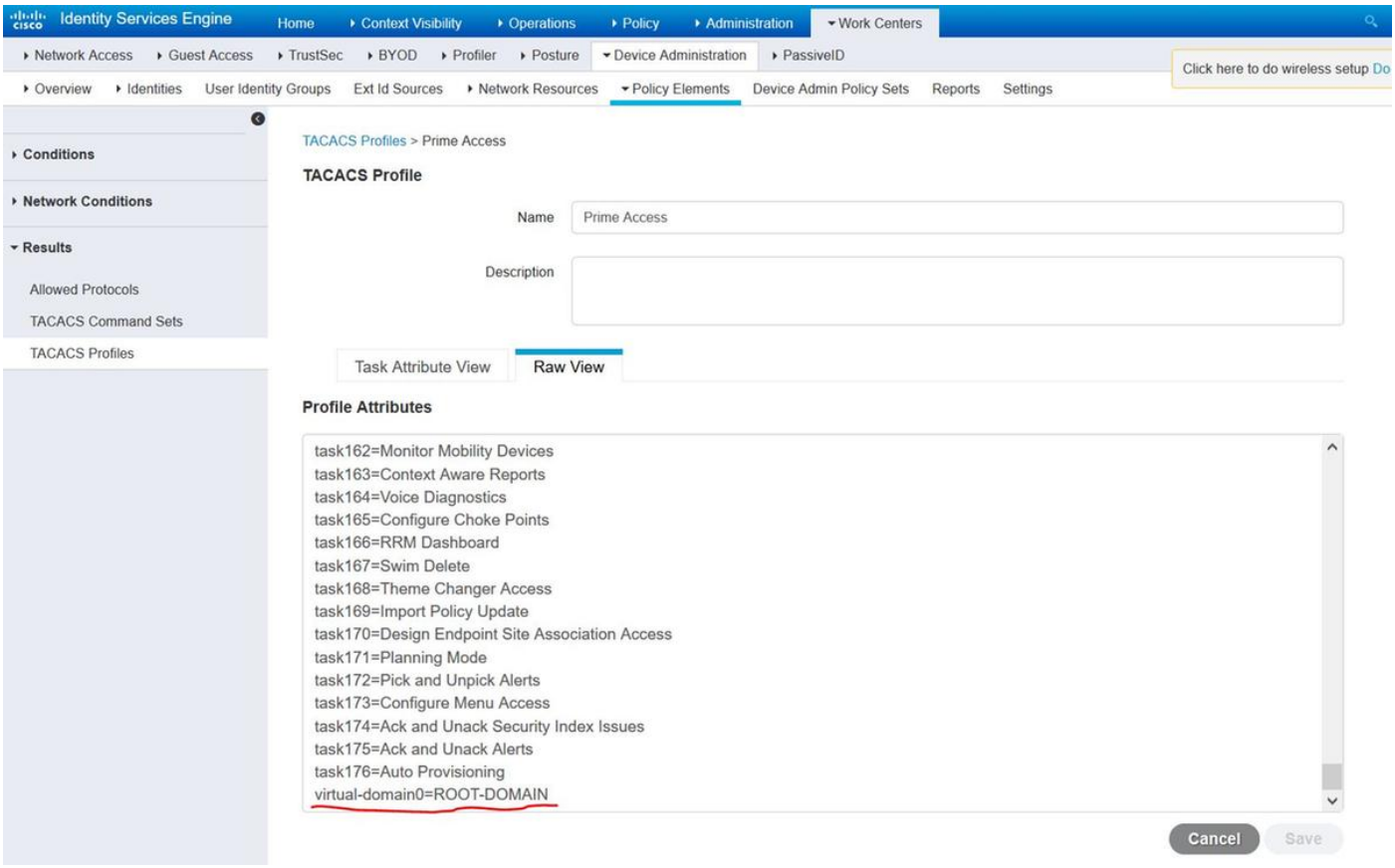
Plakt ze vervolgens in het gedeelte Raw View van het profiel op ISE.



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

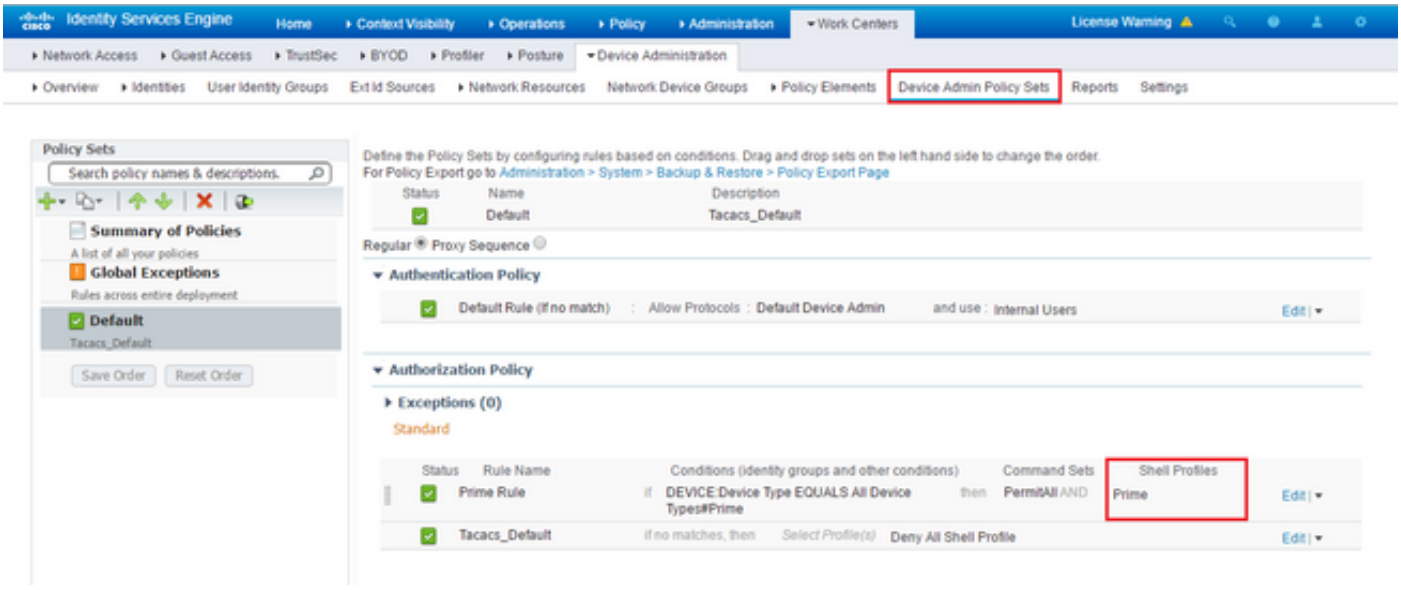


Naam Prime Virtual Domain moet worden toegevoegd als eigenschap **virtuele-domein0=**"virtuele domeinnaam"



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)



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.