Toediening van TACACS+-apparaten configureren op Palo Alto met ISE

Inhoud

Inleiding

Voorwaarden

Gebruikte componenten

Netwerkdiagram

- verificatiestroom

Configureren

- Sectie 1: Palo Alto Firewall configureren voor TACACS+
- Sectie 2: TACACS+-configuratie op ISE

Verifiëren

- ISE-beoordeling

Probleemoplossing

- TACACS: ongeldig TACACS+-aanvraagpakket – mogelijk niet-overeenkomende gedeelde geheimen
  - Probleem
  - Mogelijke oorzaken
  - Oplossing

Inleiding

Dit document beschrijft de TACACS+ Configuratie op Palo Alto met Cisco ISE.

Voorwaarden

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco ISE en TACACS+ protocol.
- Firewall van Palo Alto.

Gebruikte componenten

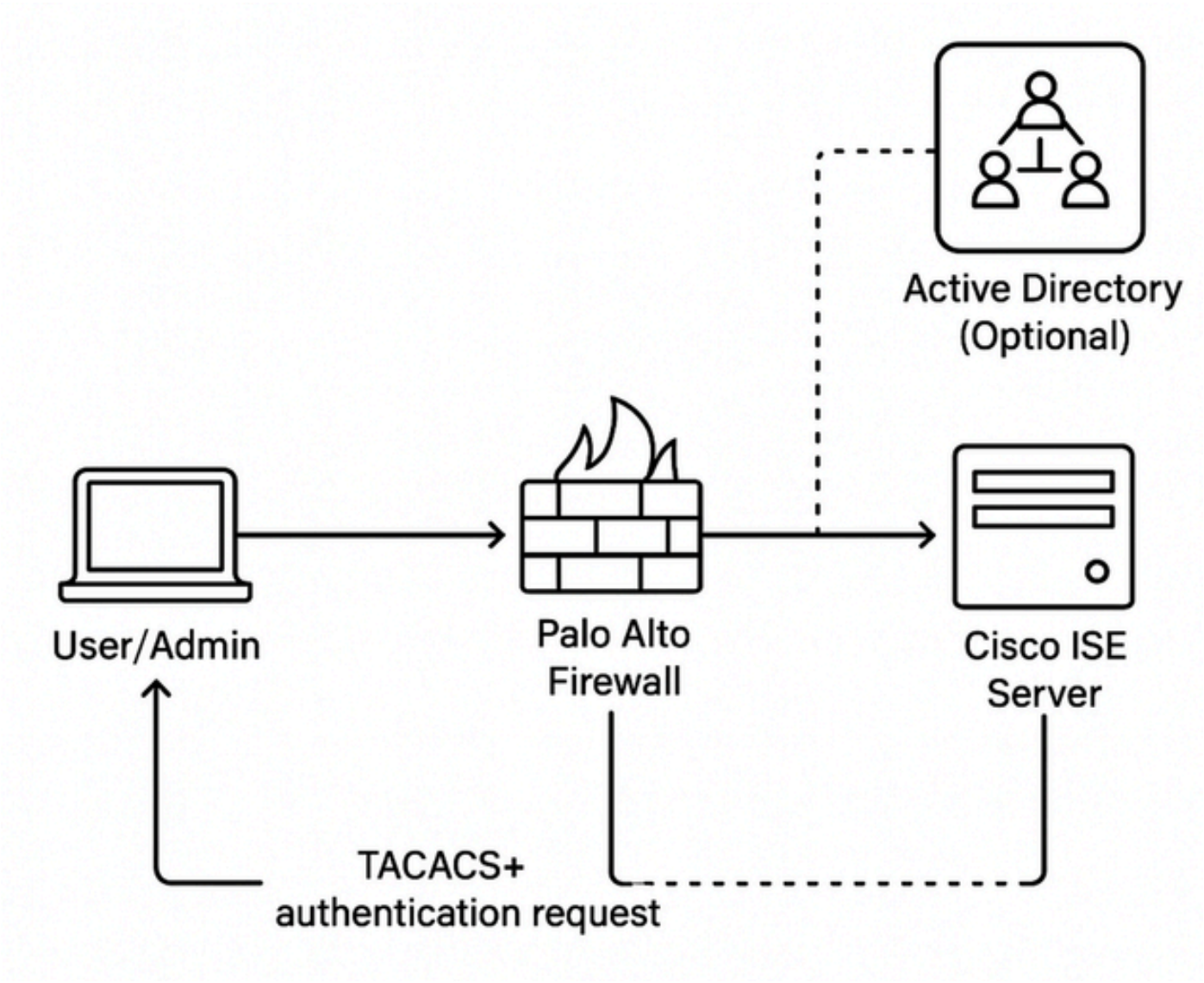
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Palo Alto Firewall versie 10.1.0
- Cisco Identity Services Engine (ISE) versie 3.3 Patch 4

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.

Netwerkdiagram



verificatiestroom

1. De beheerder meldt zich aan bij de Palo Alto-firewall.

2. Palo Alto stuurt een TACACS+-verificatieverzoek naar Cisco ISE.

3. Cisco ISE:

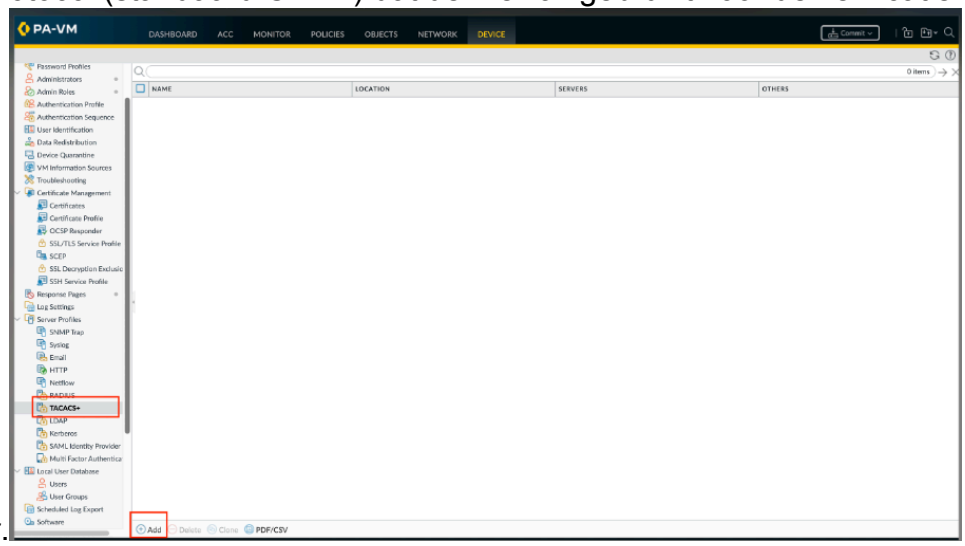
- Als AD is geïntegreerd, wordt door AD een query uitgevoerd voor verificatie en autorisatie.
- Als er geen AD is, wordt gebruik gemaakt van lokale identiteitswinkels of beleidsregels.
- Cisco ISE stuurt een autorisatiereactie naar Palo Alto op basis van het geconfigureerde beleid.
- De beheerder krijgt toegang met het juiste voorkeursniveau.

Configureren

Sectie 1: Palo Alto Firewall configureren voor TACACS+

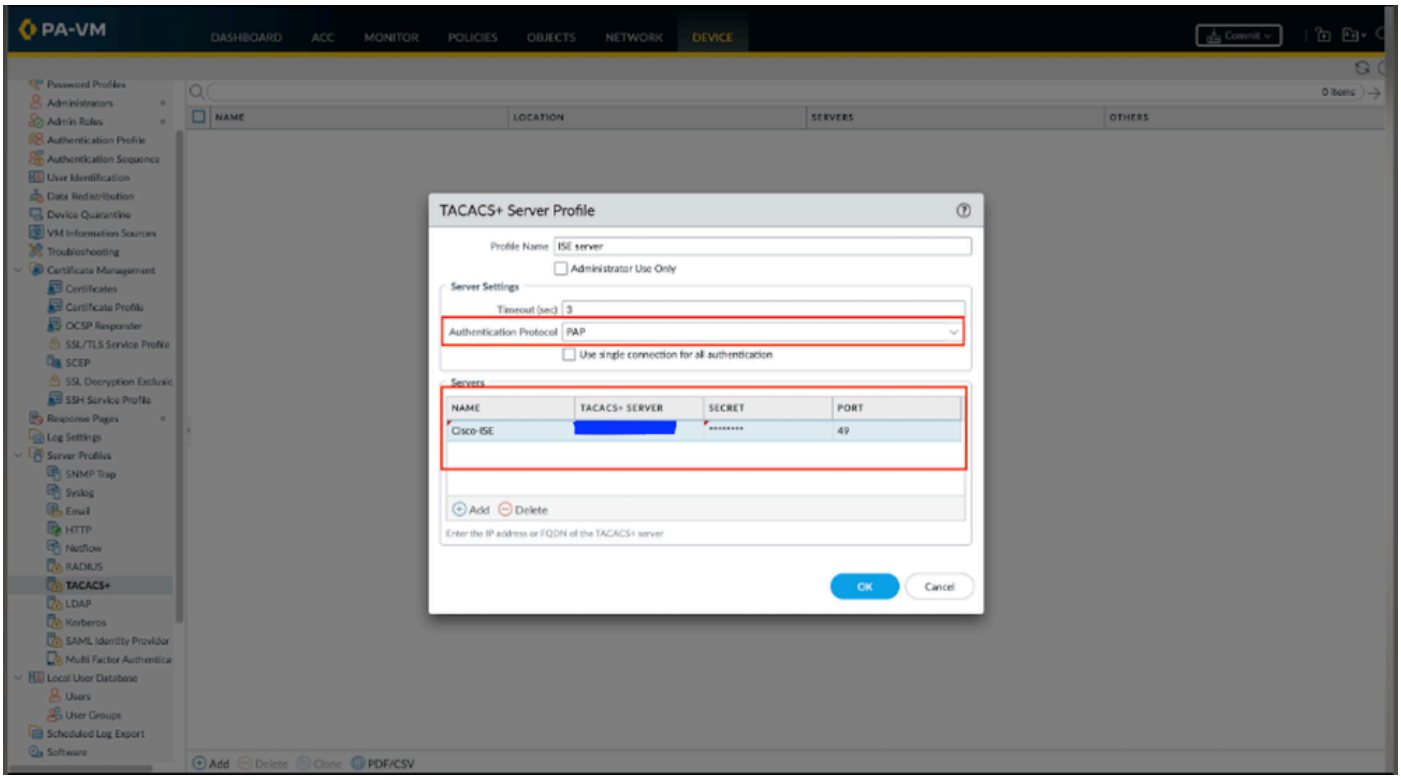
Stap 1. Voeg een TACACS+-serverprofiel toe.

In het profiel wordt gedefinieerd hoe de firewall verbinding maakt met de TACACS+-server.

1. Selecteer Apparaat > Serverprofielen > TACACS+ of Panorama > Serverprofielen > TACACS+ op Panorama en voeg een profiel toe.
2. Voer een profielnaam in om het serverprofiel te identificeren.
3. (Optioneel) Selecteer Alleen gebruiken door beheerder om de toegang tot beheerders te beperken.
4. Voer een time-outinterval in seconden in, waarna een verificatieverzoek een time-out krijgt (standaard 3; bereik 1-20).
5. Selecteer het verificatieprotocol (standaard CHAP) dat de firewall gebruikt voor de verificatie van de TACACS+-server. 

6. Voeg elke TACACS+-server toe en voer de volgende stappen uit:
    1. Een naam om de server te identificeren.
    2. Het IP-adres van de TACACS+-server of FQDN. Als u een FQDN-adresobject gebruikt om de server te identificeren en u vervolgens het adres wijzigt, moet u de wijziging vastleggen zodat het nieuwe serveradres van kracht wordt.
    3. Een geheim bevestigen en bevestigen om gebruikersnamen en wachtwoorden te versleutelen.
    4. De serverpoort voor verificatieverzoeken (standaard is 49). Klik op OK om het serverprofiel op te slaan.

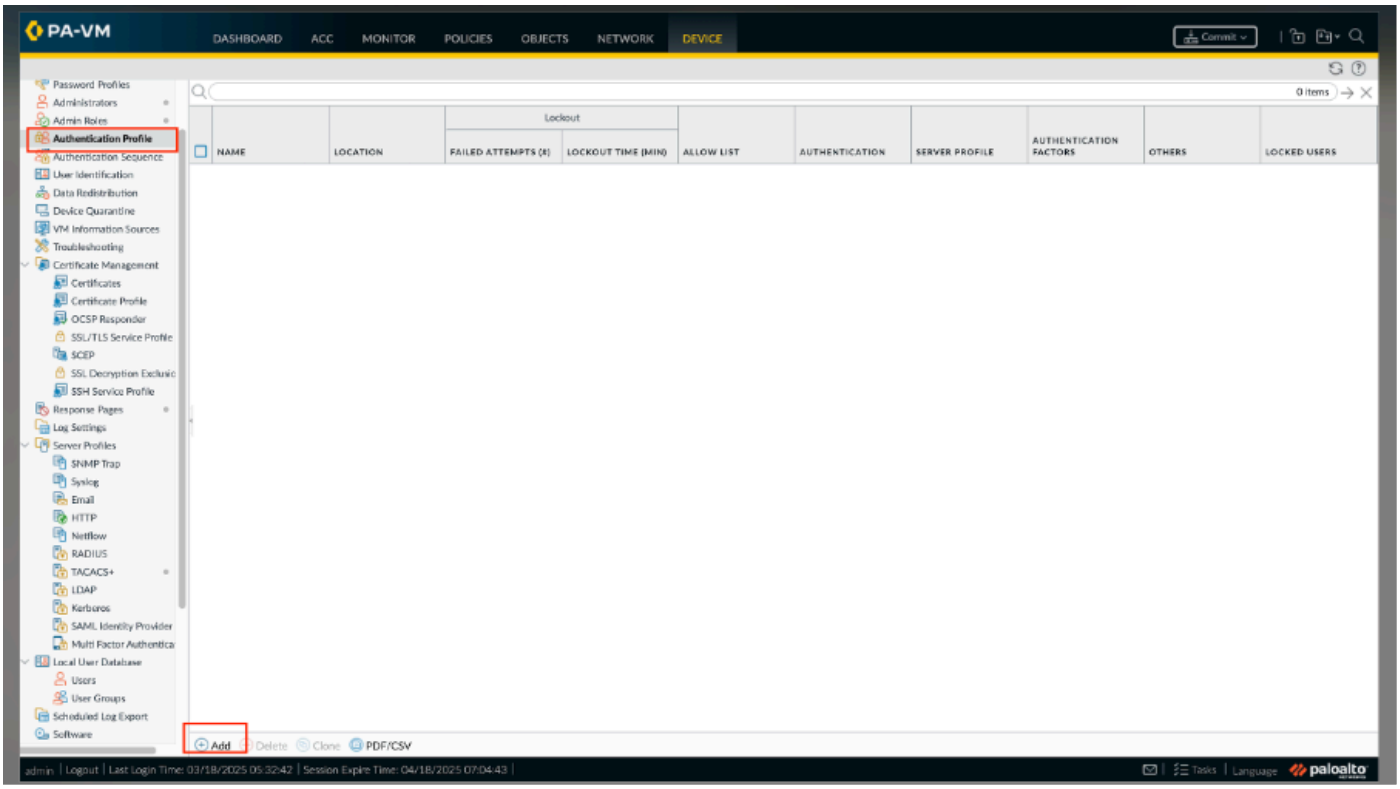
7. Klik op OK om het serverprofiel op te slaan.

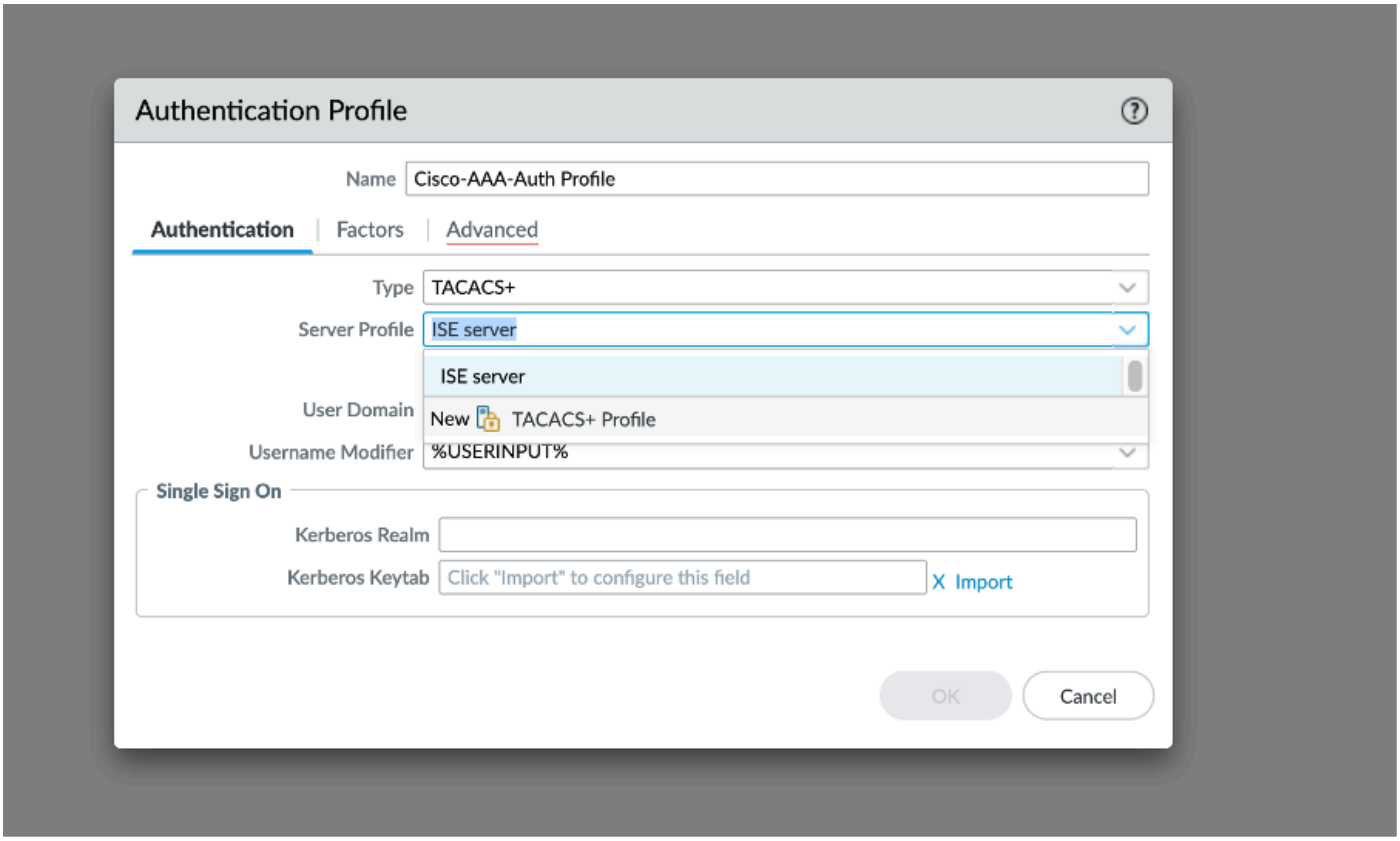


Stap 2. Wijs het TACACS+-serverprofiel toe aan een verificatieprofiel.

Het verificatieprofiel definieert de verificatie-instellingen die gemeenschappelijk zijn voor een set gebruikers.

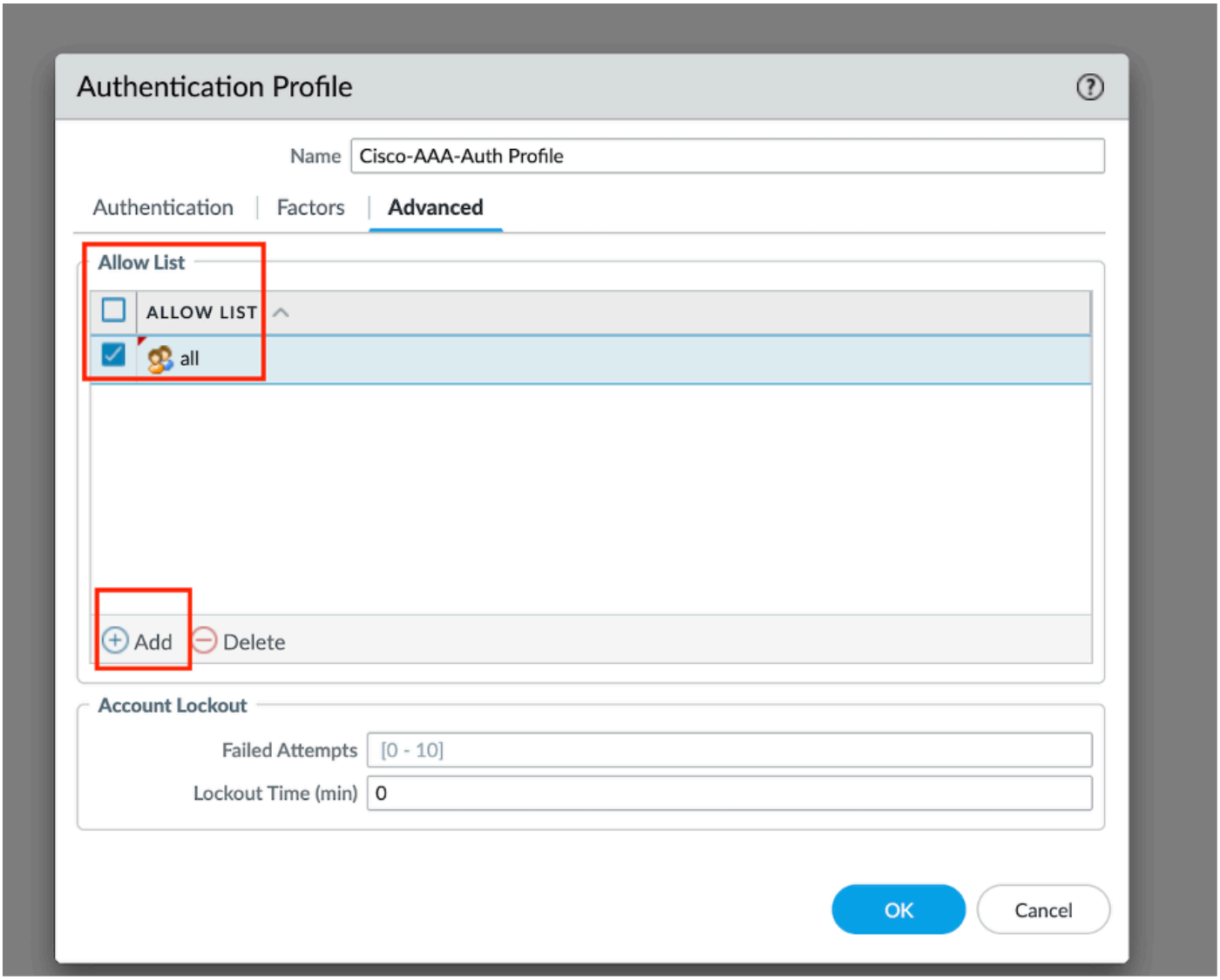
1. Selecteer Apparaat > Verificatieprofiel en voeg een profiel toe.
    1. Voer een naam in om het profiel te identificeren
    2. Stel het type in op TACACS+.
    3. Selecteer het serverprofiel dat u hebt ingesteld.
    4. Selecteer Gebruikersgroep ophalen van TACACS+ om gebruikersgroepinformatie te verzamelen van VSA's die zijn gedefinieerd op de TACACS+-server.





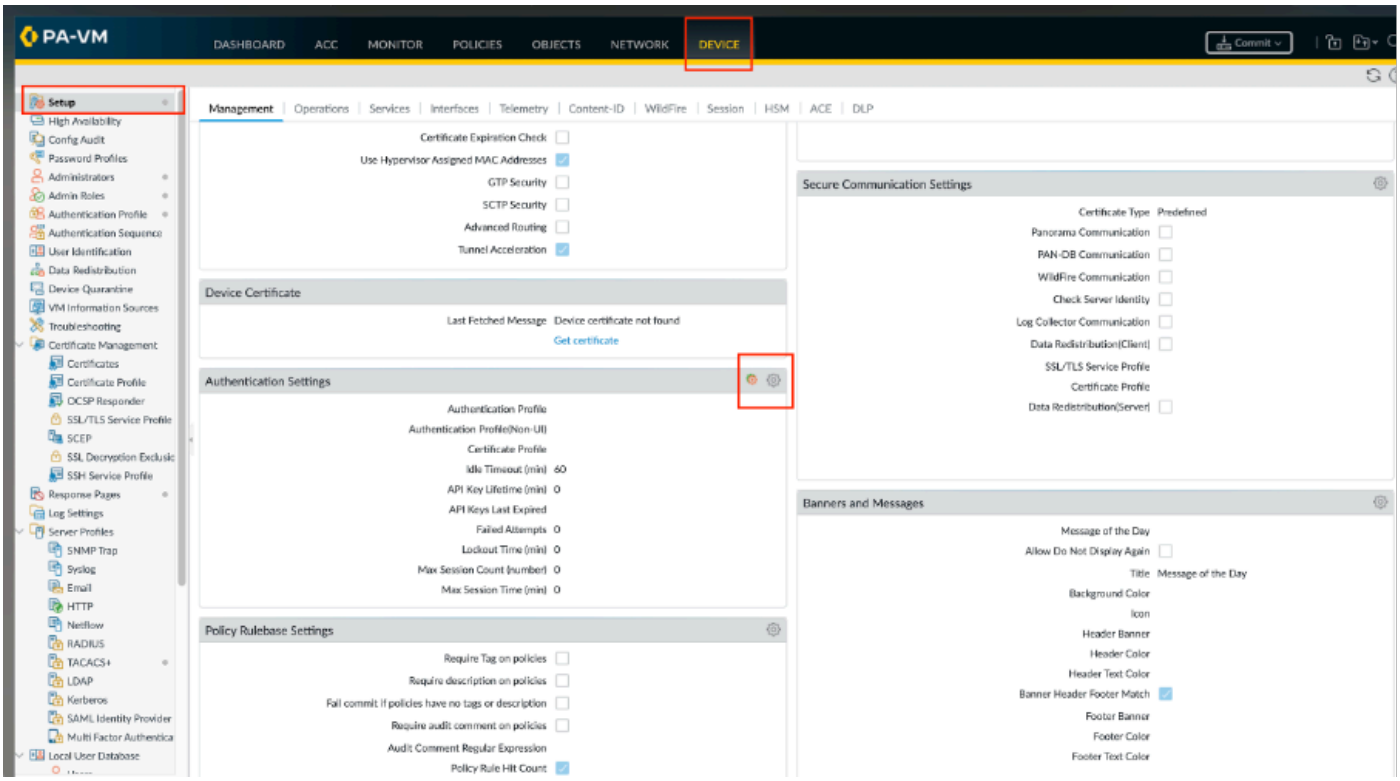
De firewall komt overeen met de groepsinformatie met de groepen die u opgeeft in de lijst Toestaan van het verificatieprofiel.

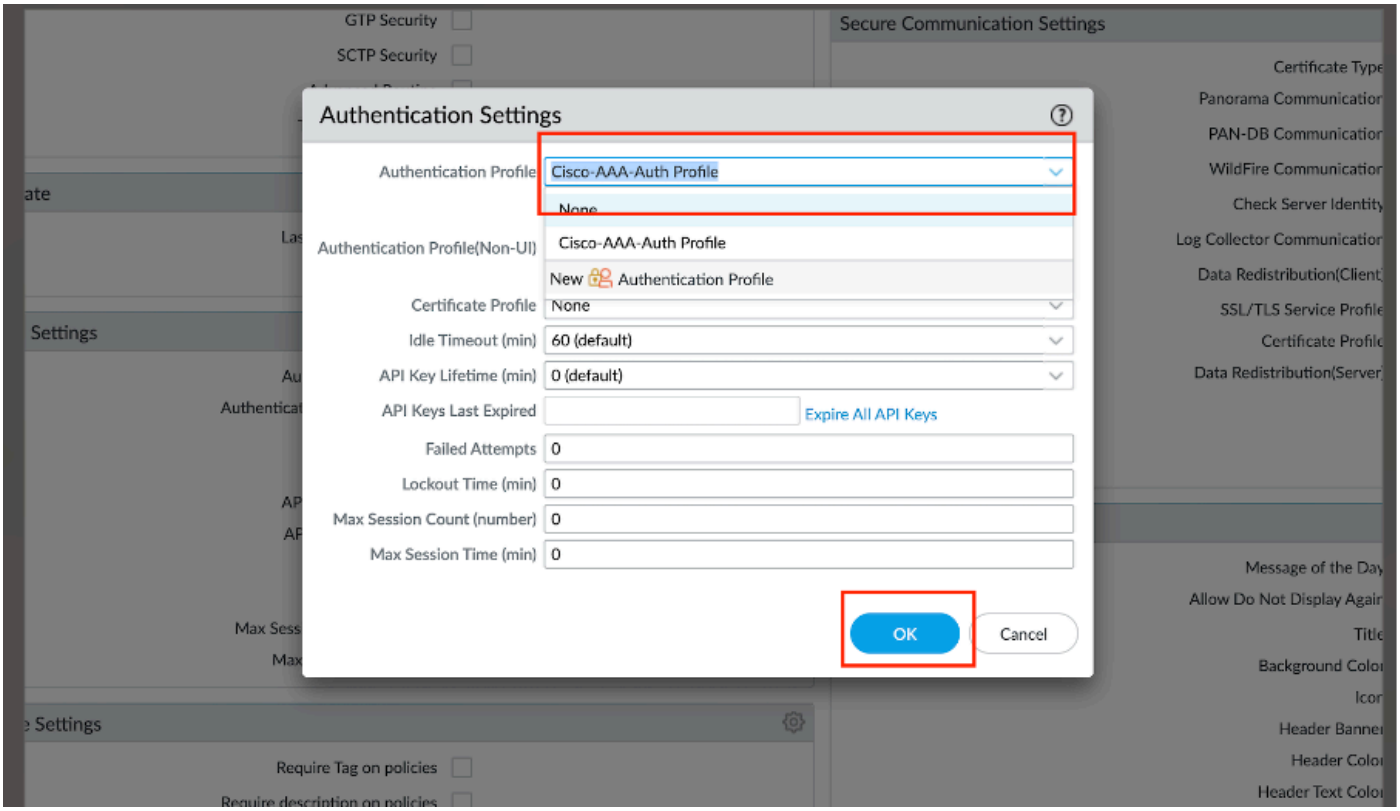
1. Selecteer Geavanceerd en voeg in de lijst Toestaan de gebruikers en groepen toe die met dit verificatieprofiel kunnen worden geverifieerd.
2. Klik op OK om het verificatieprofiel op te slaan.



Stap 3. Configureer de firewall om het verificatieprofiel voor alle beheerders te gebruiken.

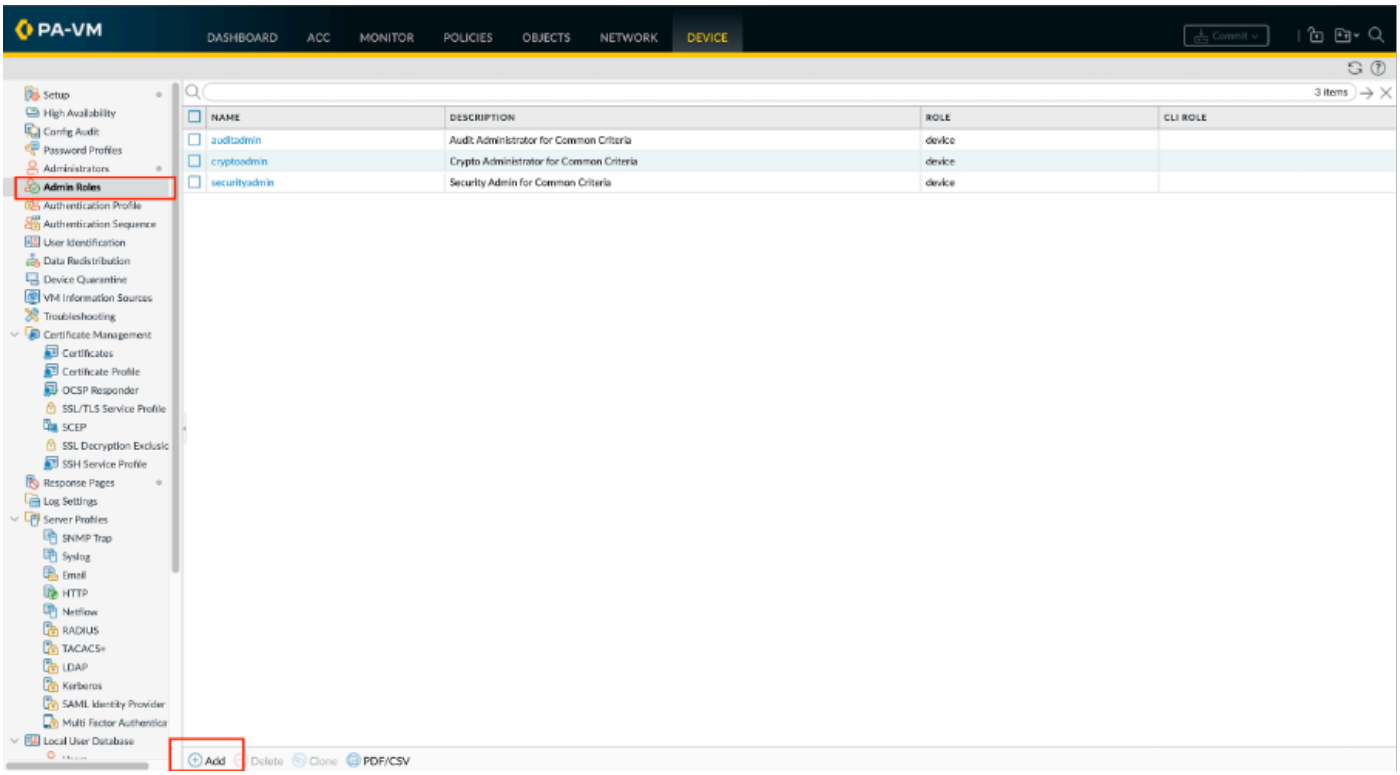
1. Selecteer Apparaat > Instellen > Beheer en bewerk de verificatieinstellingen.
2. Selecteer het verificatieprofiel dat u hebt geconfigureerd en klik op OK.



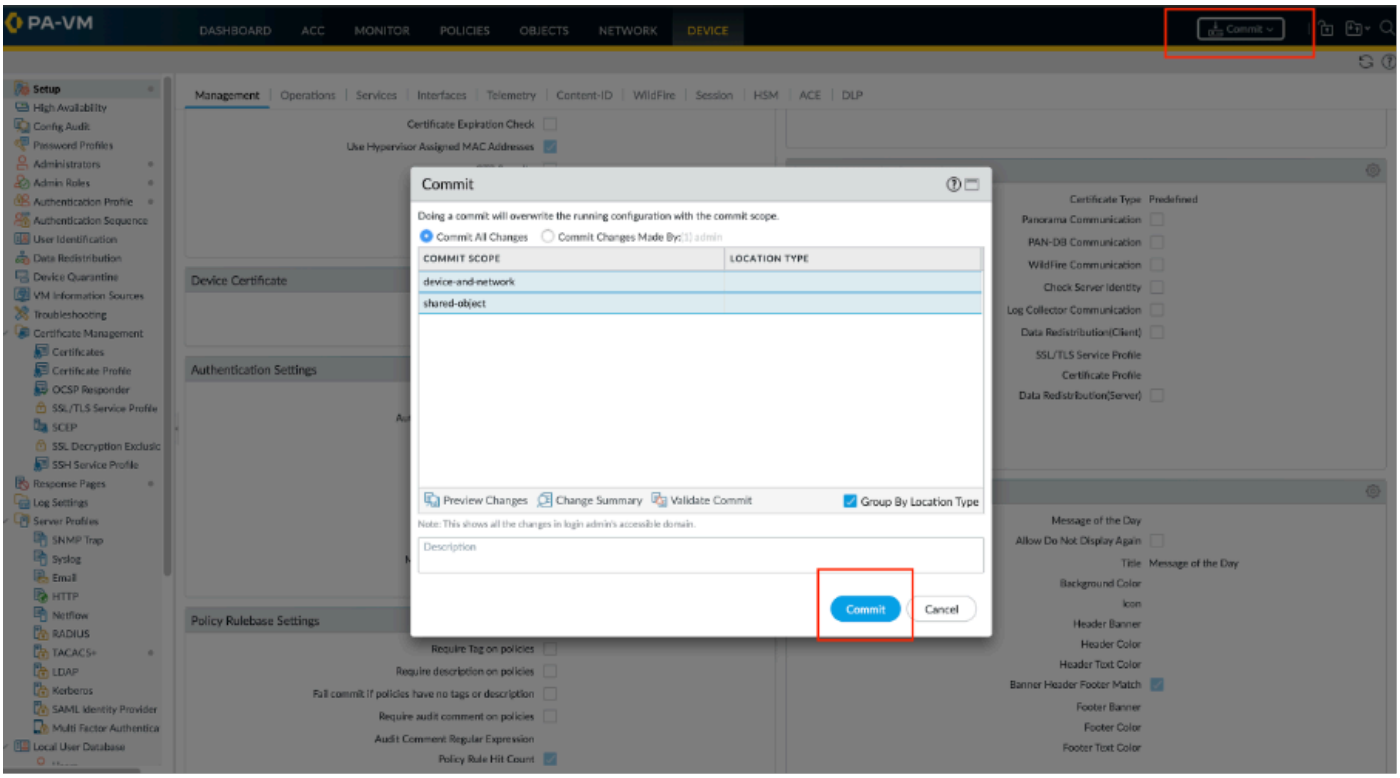


Stap 4. Een beheerdersrolprofiel configureren.

Selecteer Apparaat > Beheerrollen en klik op Toevoegen. Voer een naam in om de rol te identificeren.



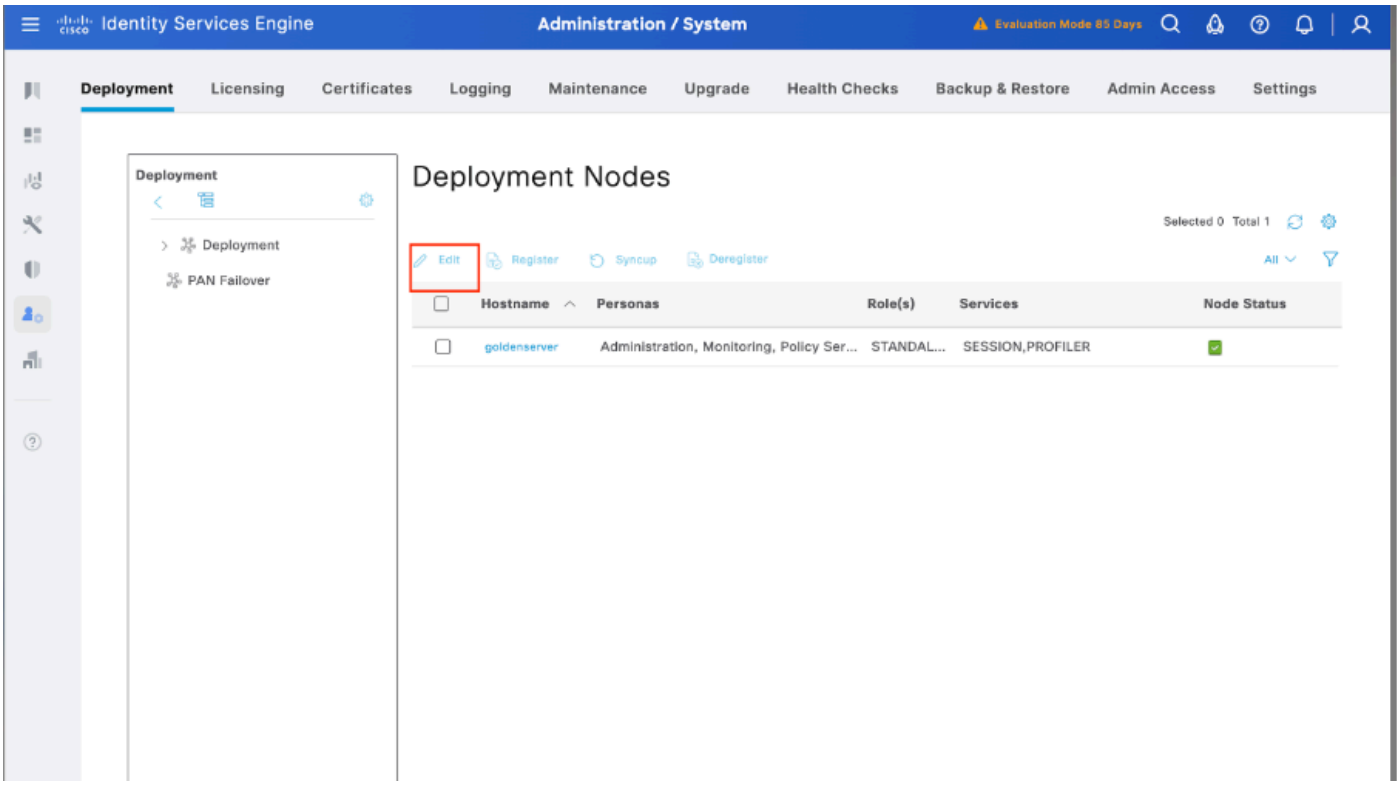
Stap 5. Wijzig de instellingen om deze te activeren in de firewall.



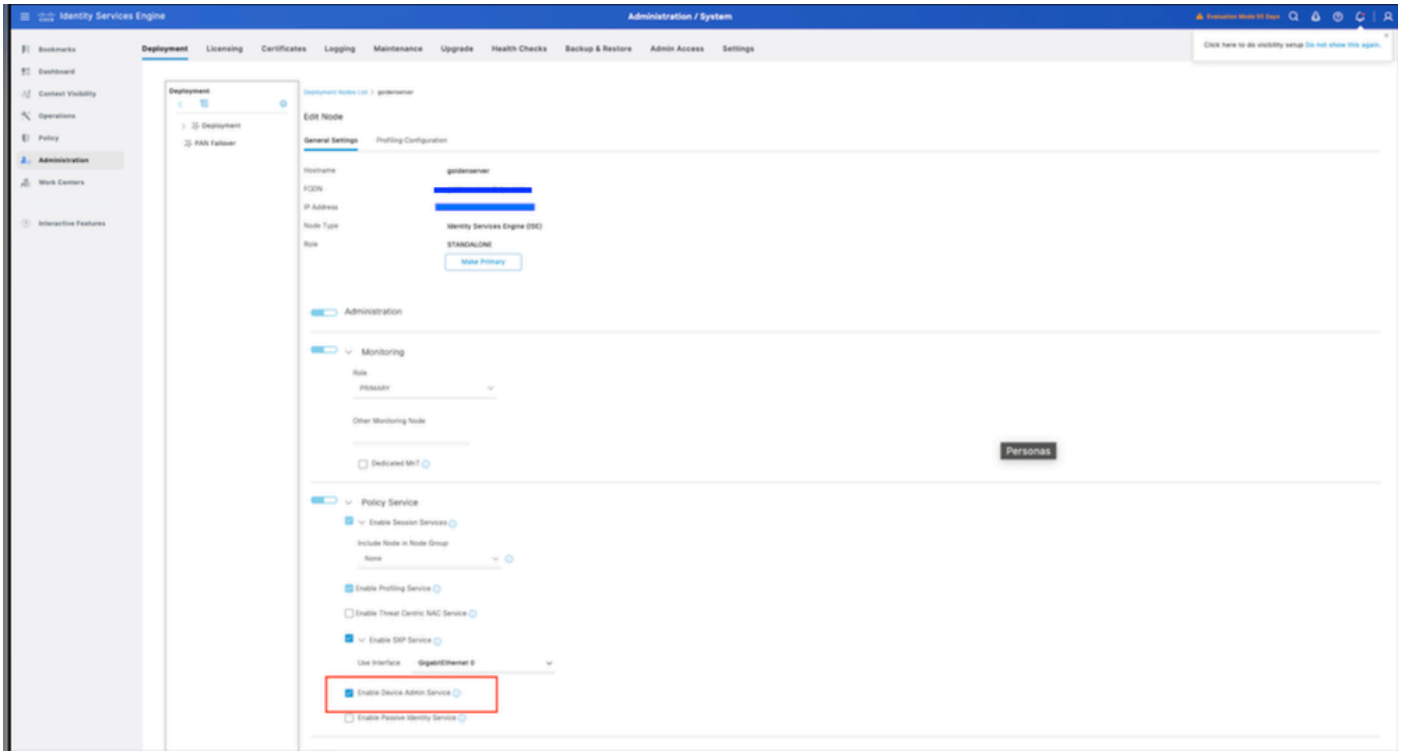
Sectie 2: TACACS+-configuratie op ISE

Stap 1. De eerste stap is om na te gaan of Cisco ISE over de nodige mogelijkheden beschikt om de TACACS+-verificatie af te handelen. Bevestig hiervoor dat de functie Apparaatbeheerservice is ingeschakeld in de gewenste beleidsserviceknooppunt (PSN). Navigeer naar Beheer > Systeem > Implementatie, selecteer het juiste knooppunt waar ISE TACACS+-verificatie verwerkt en klik op

Bewerken om de configuratie te bekijken.

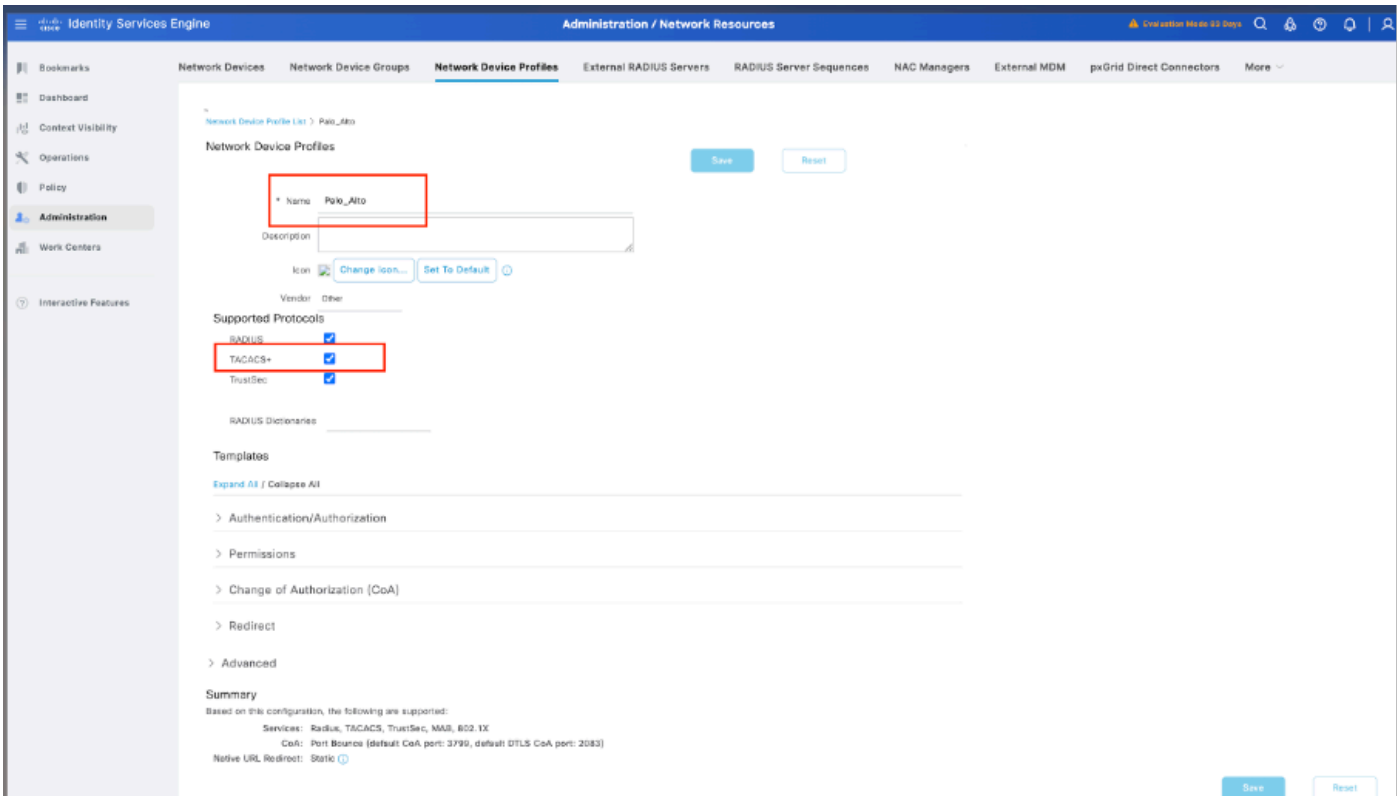


Stap 2. Blader omlaag om de functie Apparaatbeheerservice te vinden. Houd er rekening mee dat als u deze functie inschakelt, de persona van de Beleidsservice actief moet zijn op de node, samen met de beschikbare TACACS+-licenties in de implementatie. Schakel het selectievakje in om de functie in te schakelen en sla de configuratie vervolgens op.



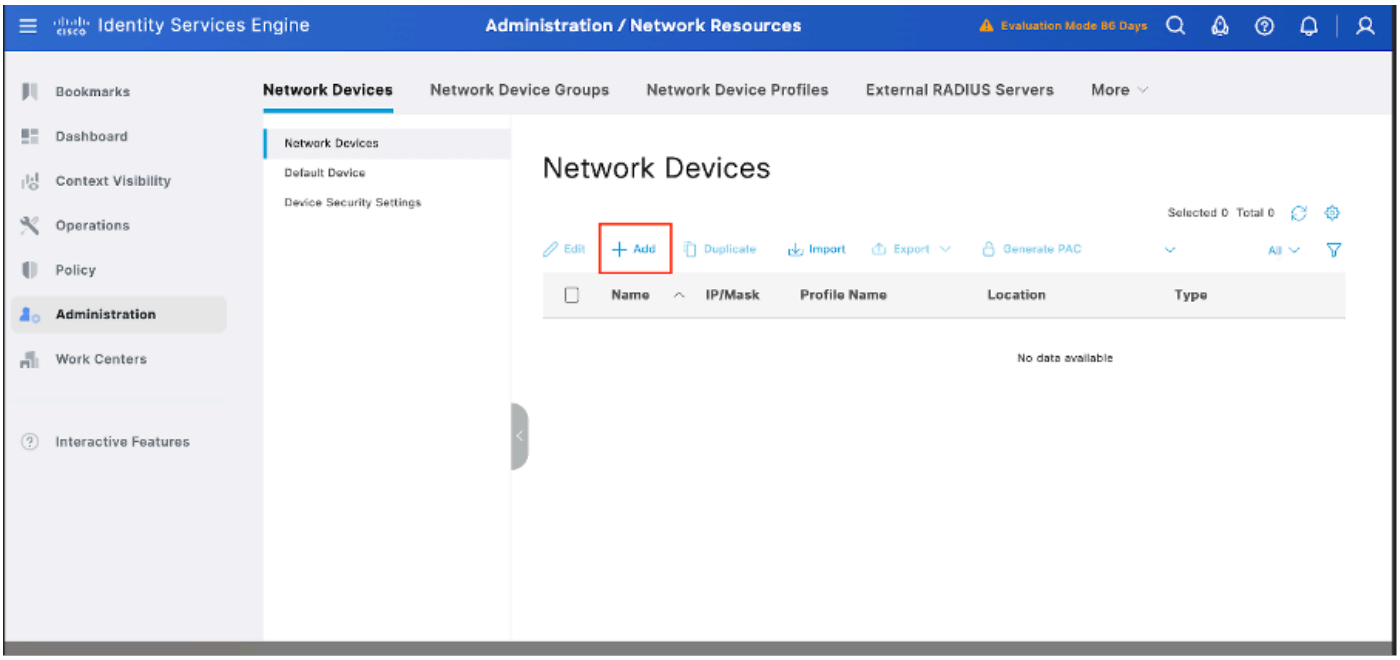
Stap 3. Configureer het Palo Alto Network Device Profile voor Cisco ISE.

Ga naar Beheer > Netwerkbronnen > Netwerkapparaatprofiel. Klik op Toevoegen en vermeld de naam (Palo Alto) en schakel TACACS+ in onder ondersteunde protocollen.



Stap 4. Palo Alto toevoegen als netwerkapparaat.

1. Navigeer naar Beheer > Netwerkbronnen > Netwerkapparaten > +Toevoegen.



2. Klik op Toevoegen en voer de volgende gegevens in:

Naam: Palo-Alto

IP-adres: <Palo-Alto IP>

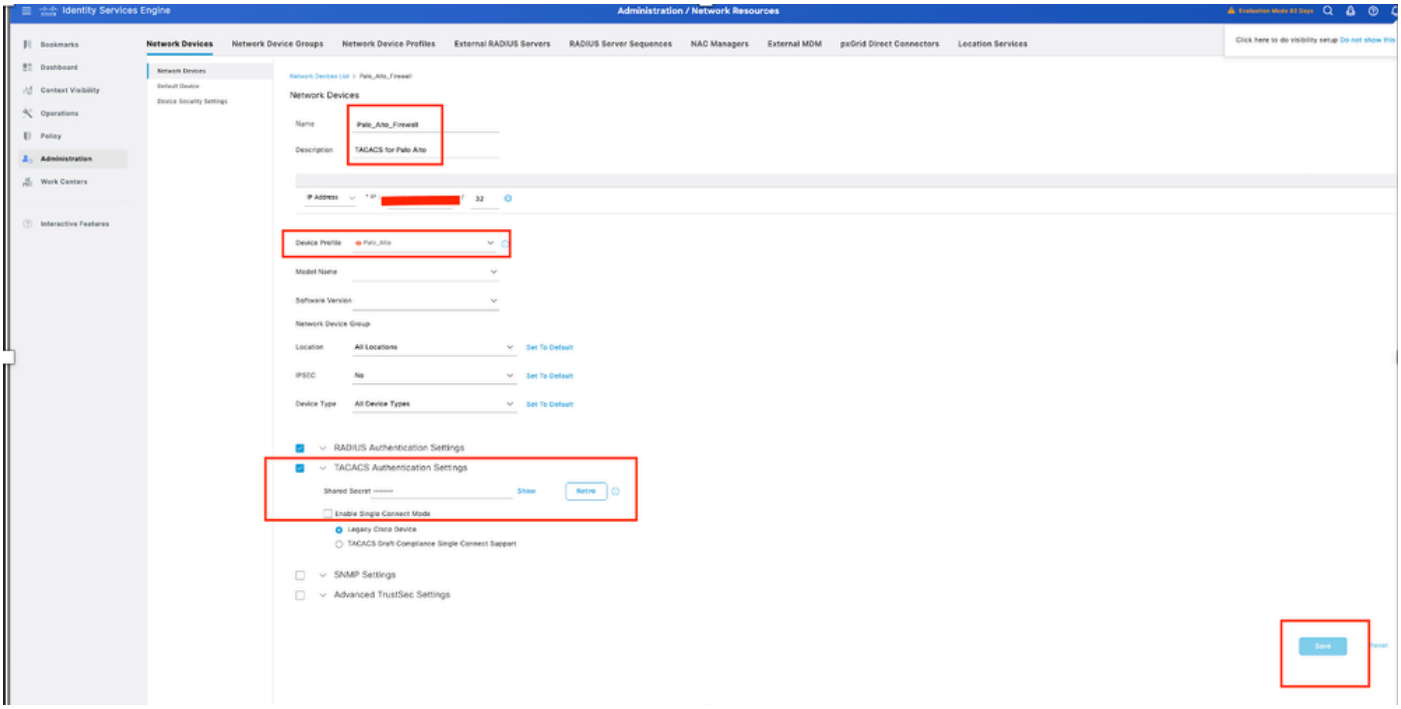
Network Device Profile: selecteer Palo Alto

TACACS-verificatie-instellingen:

TACACS+-verificatie inschakelen

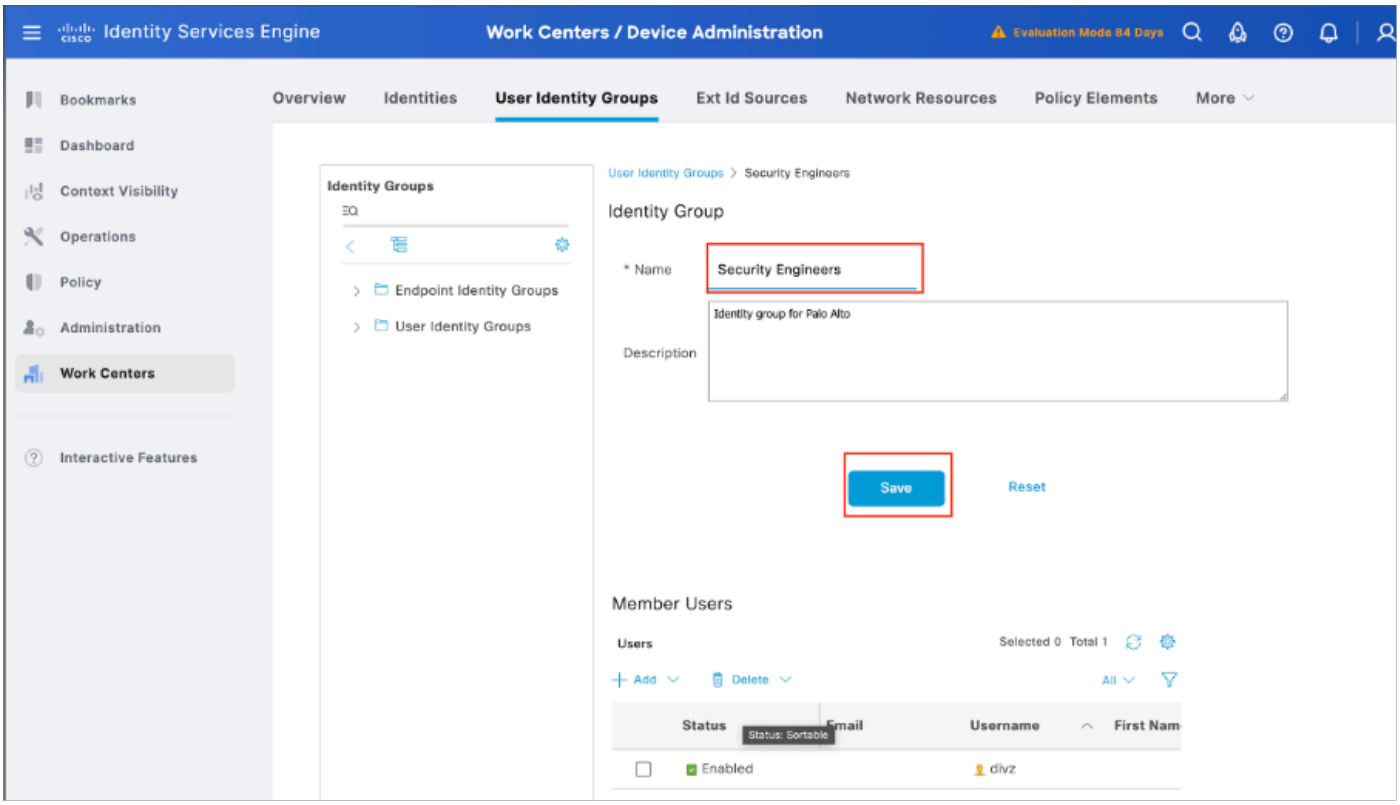
Voer het gedeelde geheim in (moet overeenkomen met de Palo Alto-configuratie)

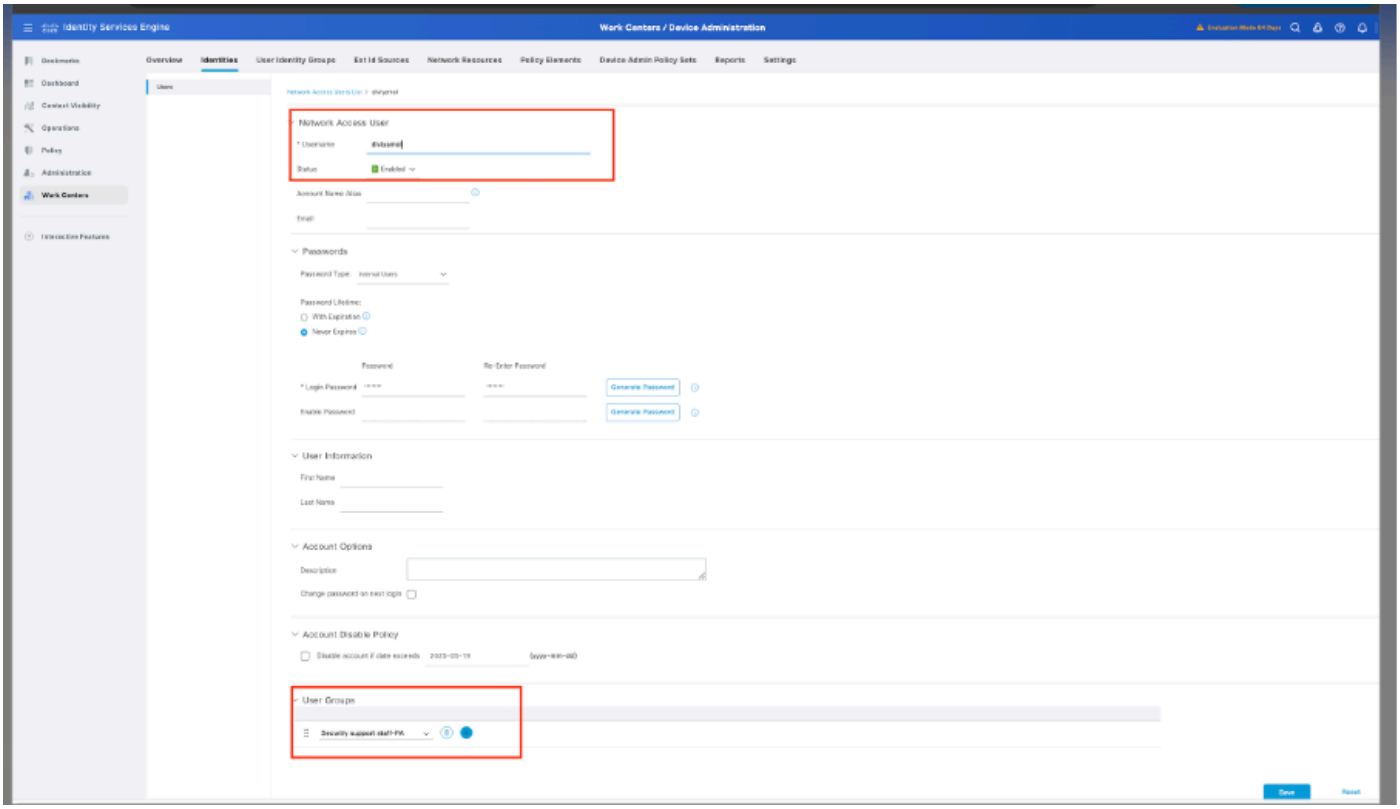
Klik op Save (Opslaan).

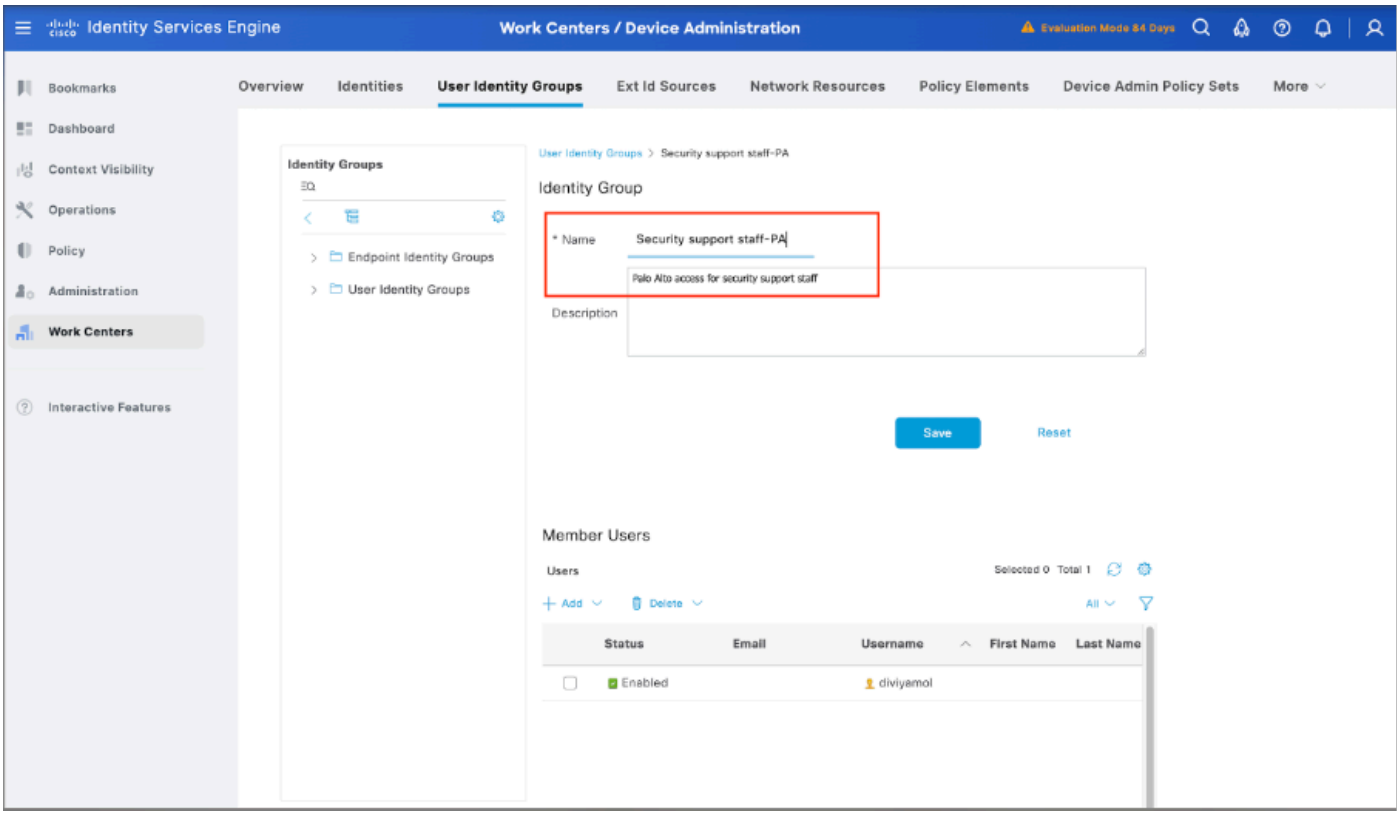


Stap 5. Gebruikersidentiteitsgroepen maken.

Navigeer naar Werkcentra > Apparaatbeheer > Gebruikersidentiteitsgroepen en klik vervolgens op Toevoegen en geef de naam voor de gebruikersgroep op.


Identity Services Engine
Work Centers / Device Administration
Evaluation Mode 84 Days
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Features
Overview
Identities
User Identity Groups
Ext Id Sources
Network Resources
Policy Elements
More
Identity Groups
Endpoint Identity Groups
User Identity Groups
User Identity Groups > Security Engineers
Identity Group
* Name
Security Engineers
Description
Identity group for Palo Alto
Save
Reset
Member Users
Users
Selected 0 Total 1
Add
Delete
All
Status
Email
Username
First Nam
Status: Sortable
Enabled
divz

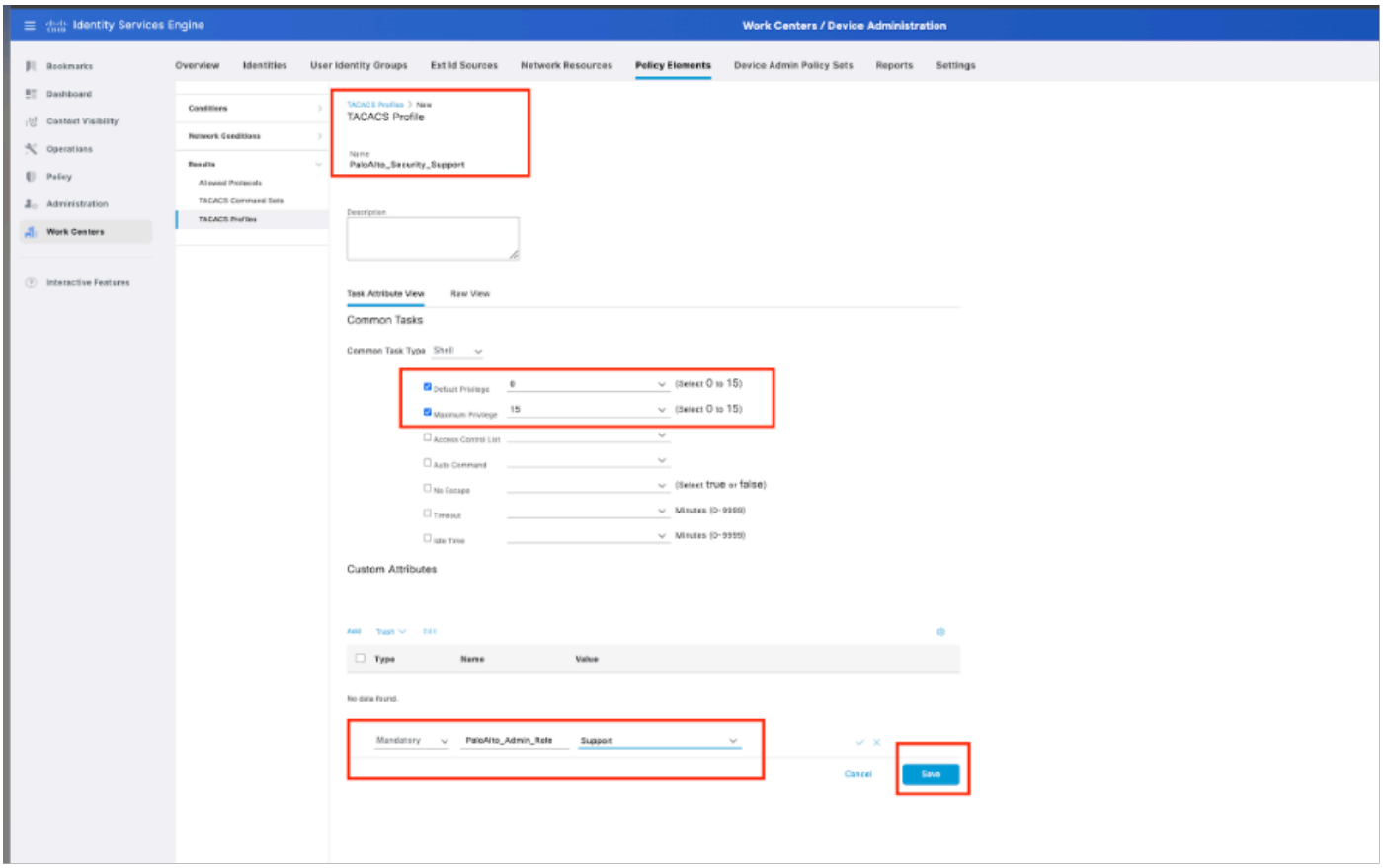

Identity Services Engine
Work Centers / Device Administration
Network Access User
Passwords
User Information
Account Options
Account Disable Policy
User Groups

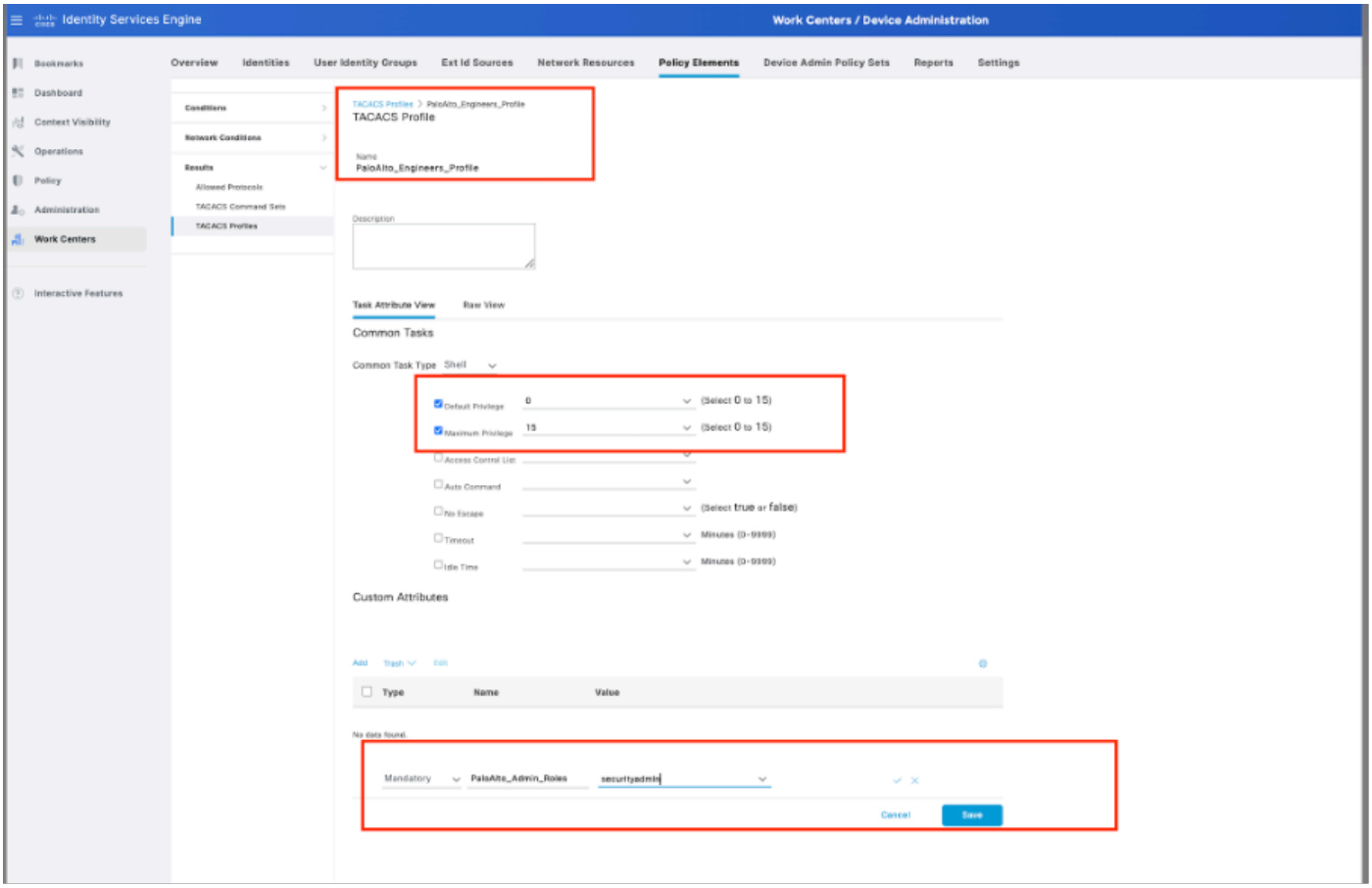


Stap 6. Een TACACS-profiel configureren.

Vervolgens configureert u een TACACS-profiel, waarin u instellingen zoals Privilege Level en time-outinstellingen kunt configureren. Navigeer naar Werkcentra > Apparaatbeheer -> Beleidselementen -> Resultaten -> TACACS-profielen.

Klik op Toevoegen om een nieuw TACACS-profiel te maken. Geef het profiel een goede naam.





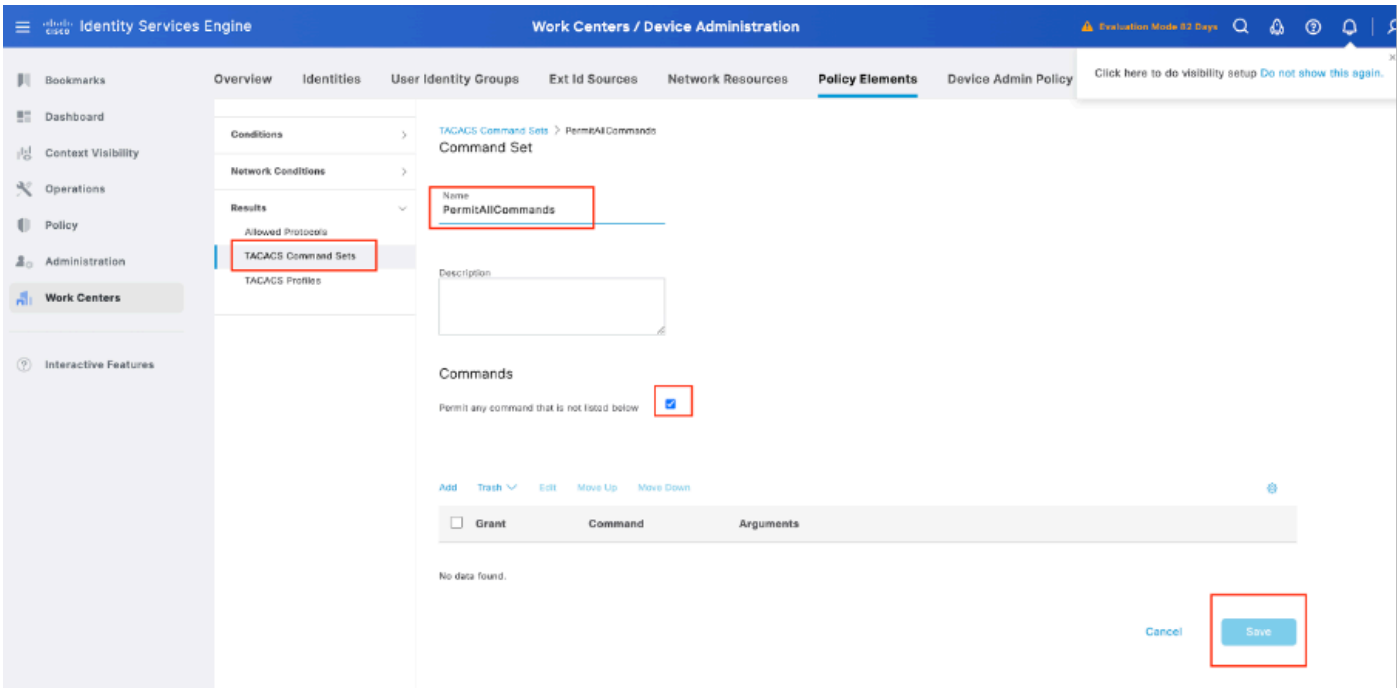
Stap 6. TACACS-opdrachtsets configureren.

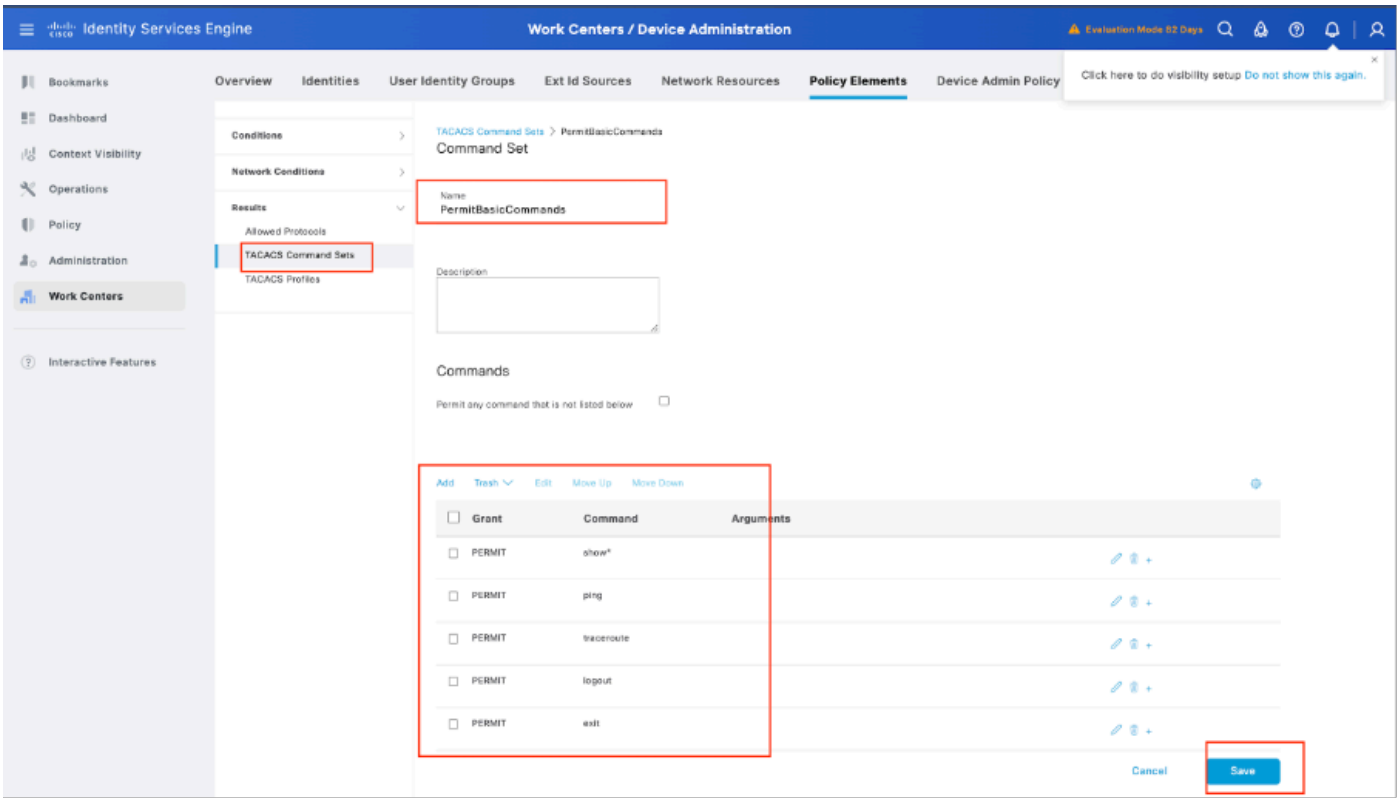
Nu is het tijd om te configureren welke commando's gebruikers mogen gebruiken. Aangezien u

beide use cases het Privilege Level 15 kunt toekennen, dat toegang geeft tot elke beschikbare opdracht, kunt u TACACS-opdrachtsets gebruiken om te beperken welke opdrachten kunnen worden gebruikt.

Navigeer naar Werkcentra > Apparaatbeheer > Beleidselementen > Resultaten -> TACACS-opdrachtsets. Klik op Toevoegen om een nieuwe TACACS-opdrachtset te maken en geef deze de naam PermitAllCommands. Pas deze TACACS-opdrachtset voor beveiligingsondersteuning toe.

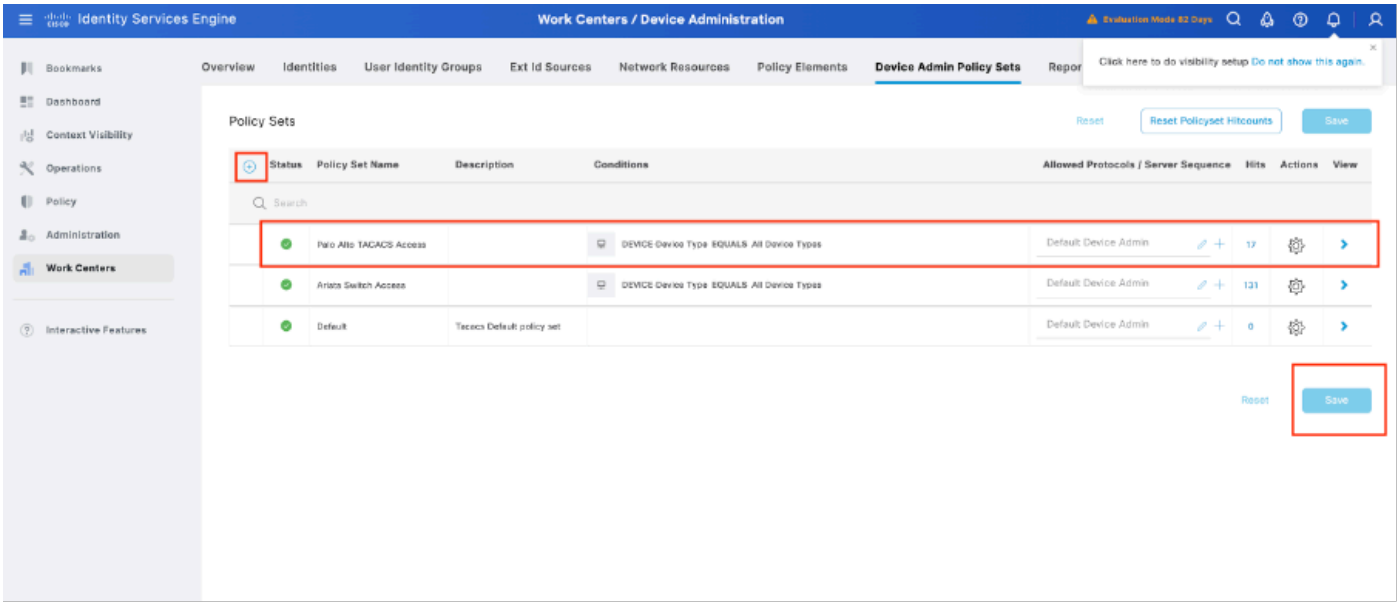
Het enige dat u in deze TACACS-opdrachtset hoeft te configureren, is het selectievakje voor Toestemming aanvinken voor opdrachten die hieronder niet worden vermeld.



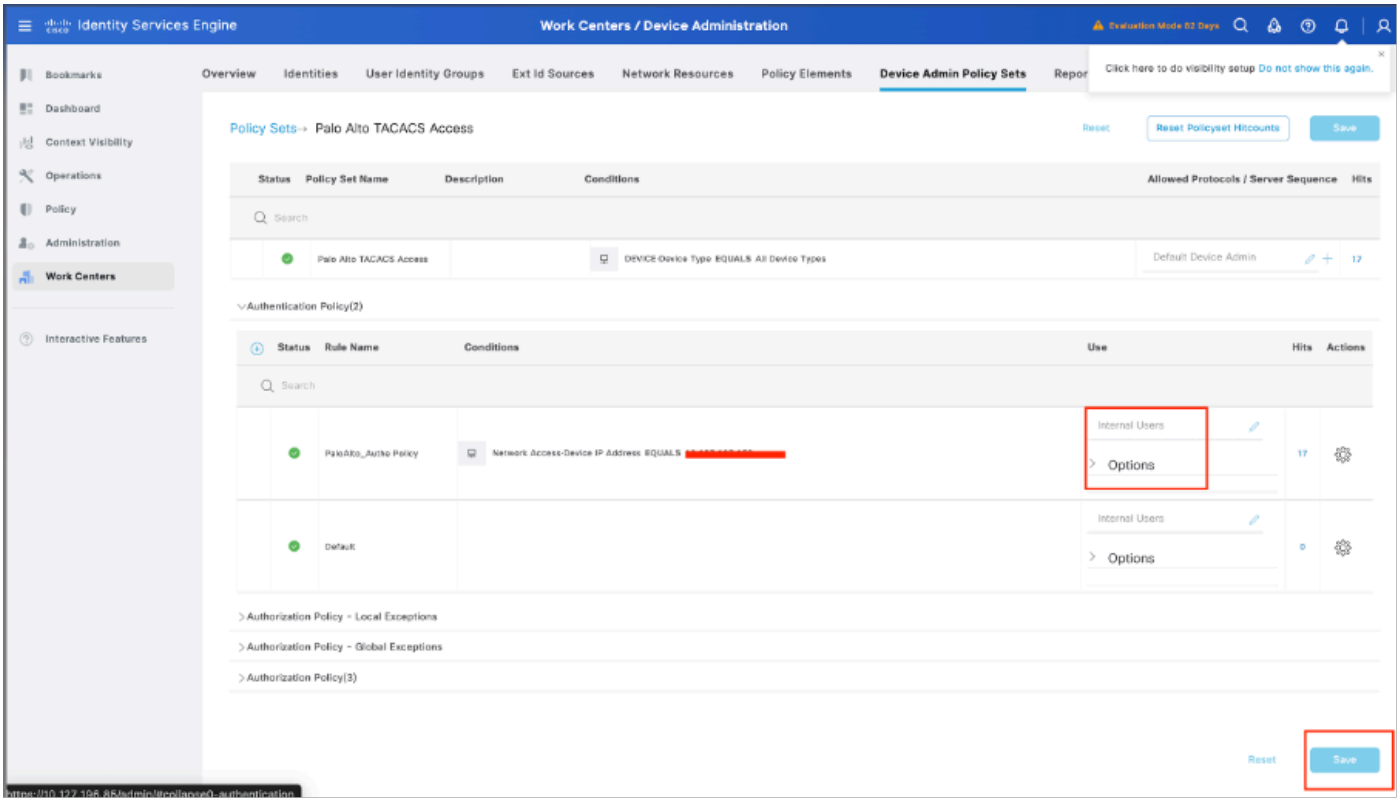


Stap 7. Maak een Device Admin Policy Set voor uw Palo Alto, navigeer in het menu Work Centers > Device Administration > Device Admin Policy Sets, klik op het Add + pictogram.

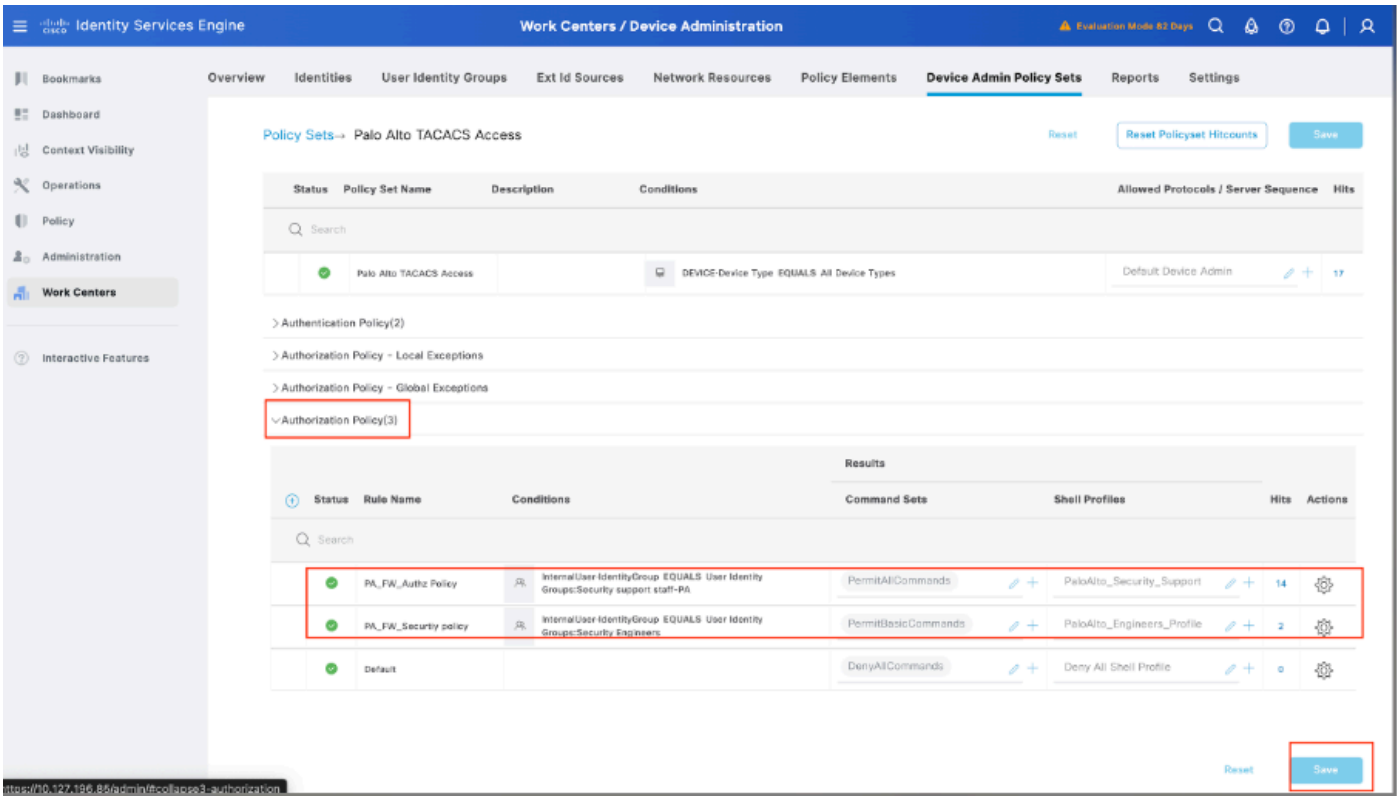
Stap 8. Geef deze nieuwe beleidsset een naam, voeg voorwaarden toe afhankelijk van de kenmerken van de TACACS+-verificaties die worden uitgevoerd vanuit de Palo Alto Firewall en selecteer als Toegestane protocollen > Standaardapparaatbeheer. Sla uw configuratie op.



Stap 9. Selecteer in de optie > bekijken en selecteer vervolgens in het gedeelte Authenticatiebeleid de externe identiteitsbron die Cisco ISE gebruikt om de gebruikersnaam en referenties voor verificatie op te vragen in de Palo Alto Firewall. In dit voorbeeld komen de referenties overeen met interne gebruikers die zijn opgeslagen in ISE.



Stap 10. Blader omlaag tot de sectie Autorisatiebeleid tot het standaardbeleid, selecteer het tandwielpictogram en plaats een regel hierboven.



Stap 11. Geef de nieuwe autorisatieregel een naam, voeg voorwaarden toe met betrekking tot de gebruiker die al is geverifieerd als groepslidmaatschap en voeg in het gedeelte Shell-profielen het eerder geconfigureerde TACACS-profiel toe en sla de configuratie op.

Verifiëren

ISE-beoordeling

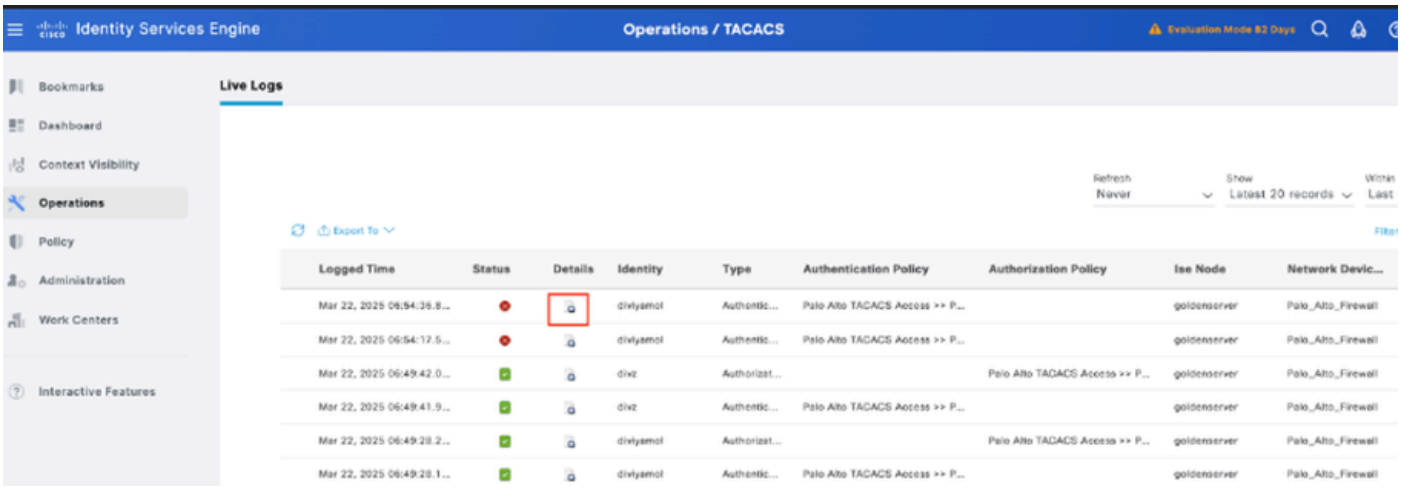
Stap 1. Controleer of de TACACS+-service actief is. Dit kan worden ingecheckt:

- GUI: Controleer of de node is vermeld bij de service DEVICE ADMIN in Beheer -> Systeem -> Implementatie.
- CLI: Voer de opdracht show ports uit | neem 49 op om te bevestigen dat er verbindingen in de TCP-poort zijn die behoren tot TACACS+

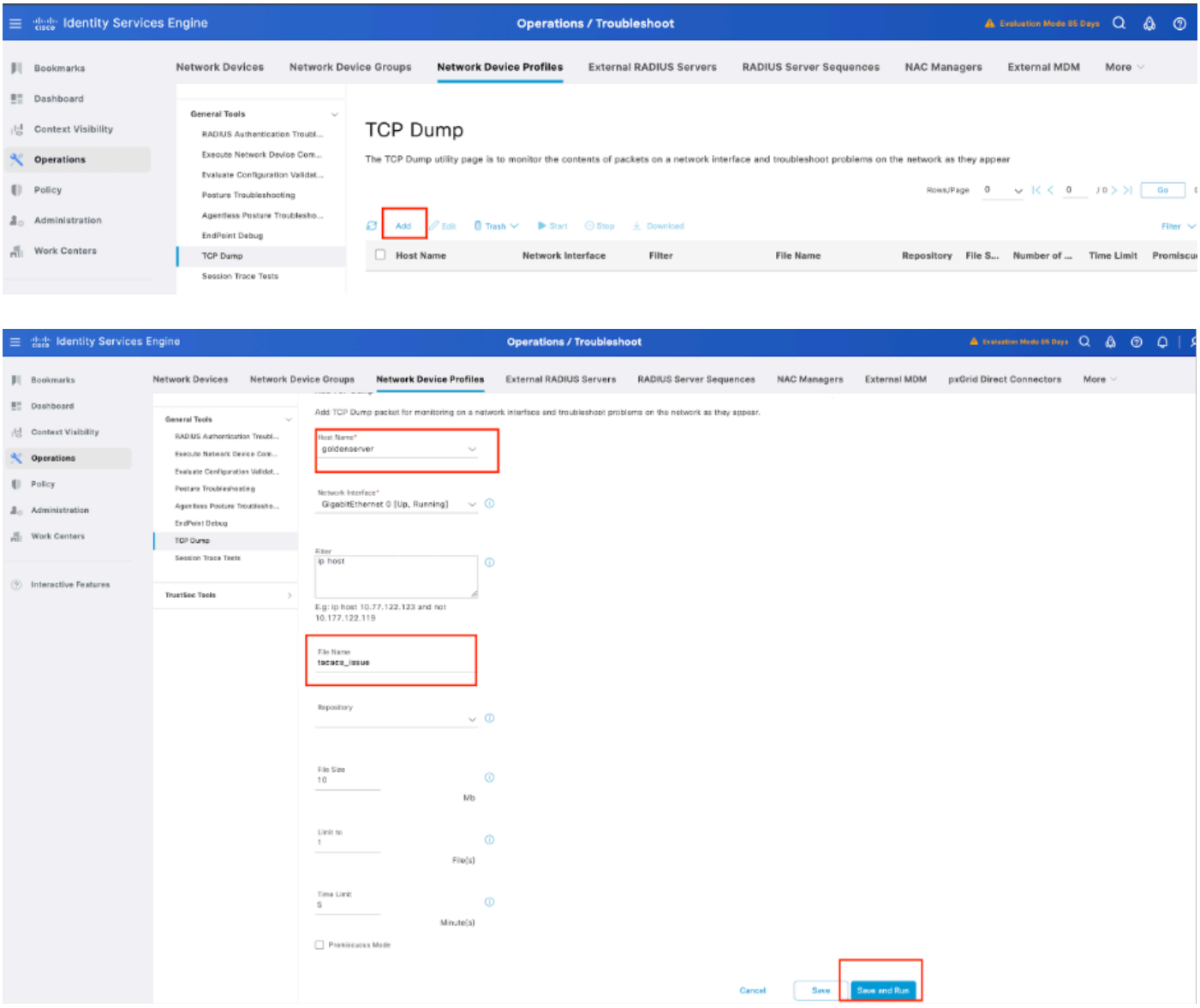
```
goldenserver/admin#show ports | include 49
tcp: [redacted]
```

Stap 2. Bevestig of er live logs zijn met betrekking tot TACACS+ authenticatie pogingen: dit kan worden gecontroleerd in het menu Operations -> TACACS -> Live logs.

Afhankelijk van de reden van de storing kunt u uw configuratie aanpassen of de oorzaak van de storing aanpakken.

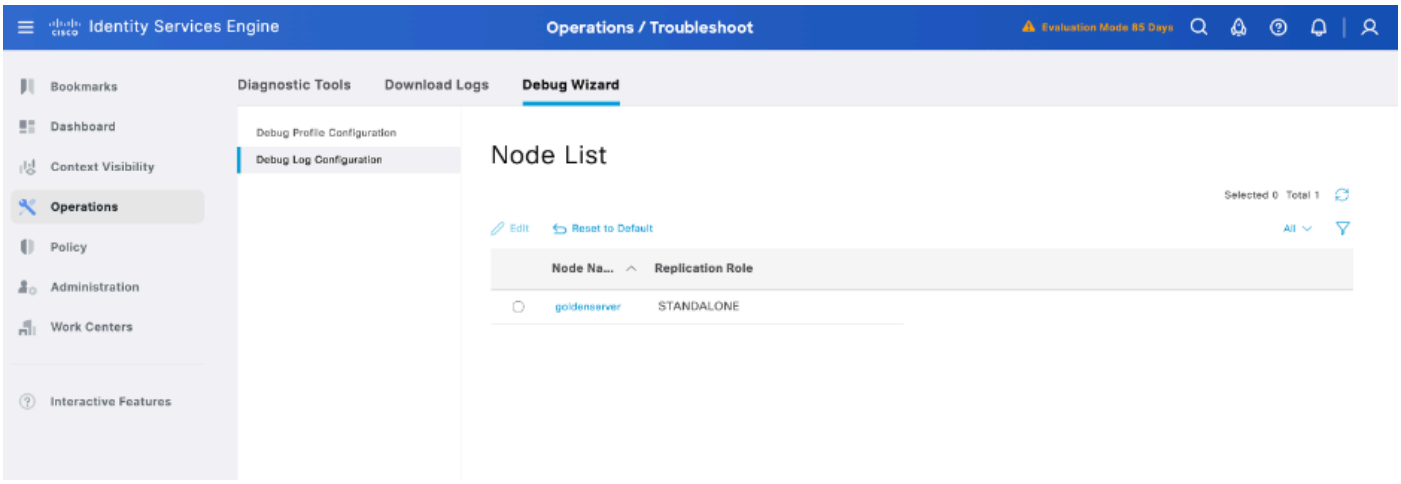


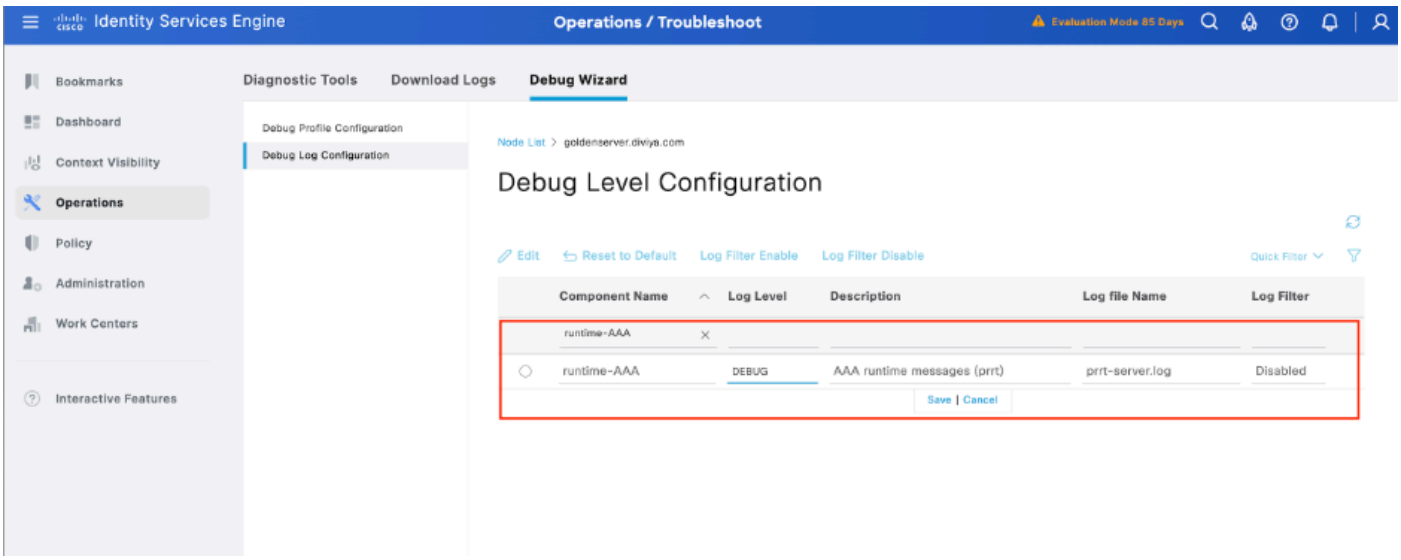
Stap 3. Als u geen live logboek ziet, gaat u verder met het vastleggen van pakketten en navigeert u naar het menu Bewerkingen > Problemen oplossen > Diagnostische hulpmiddelen > Algemene hulpmiddelen > TCP-dump, selecteer Toevoegen.



Stap 4. Schakel de component runtime-AAA in voor foutopsporing binnen de PSN van waaruit de verificatie wordt uitgevoerd in Operations > Troubleshoot > Debug Wizard > Debug log

configuratie, selecteer PSN node, selecteer vervolgens volgende in bewerken knop.





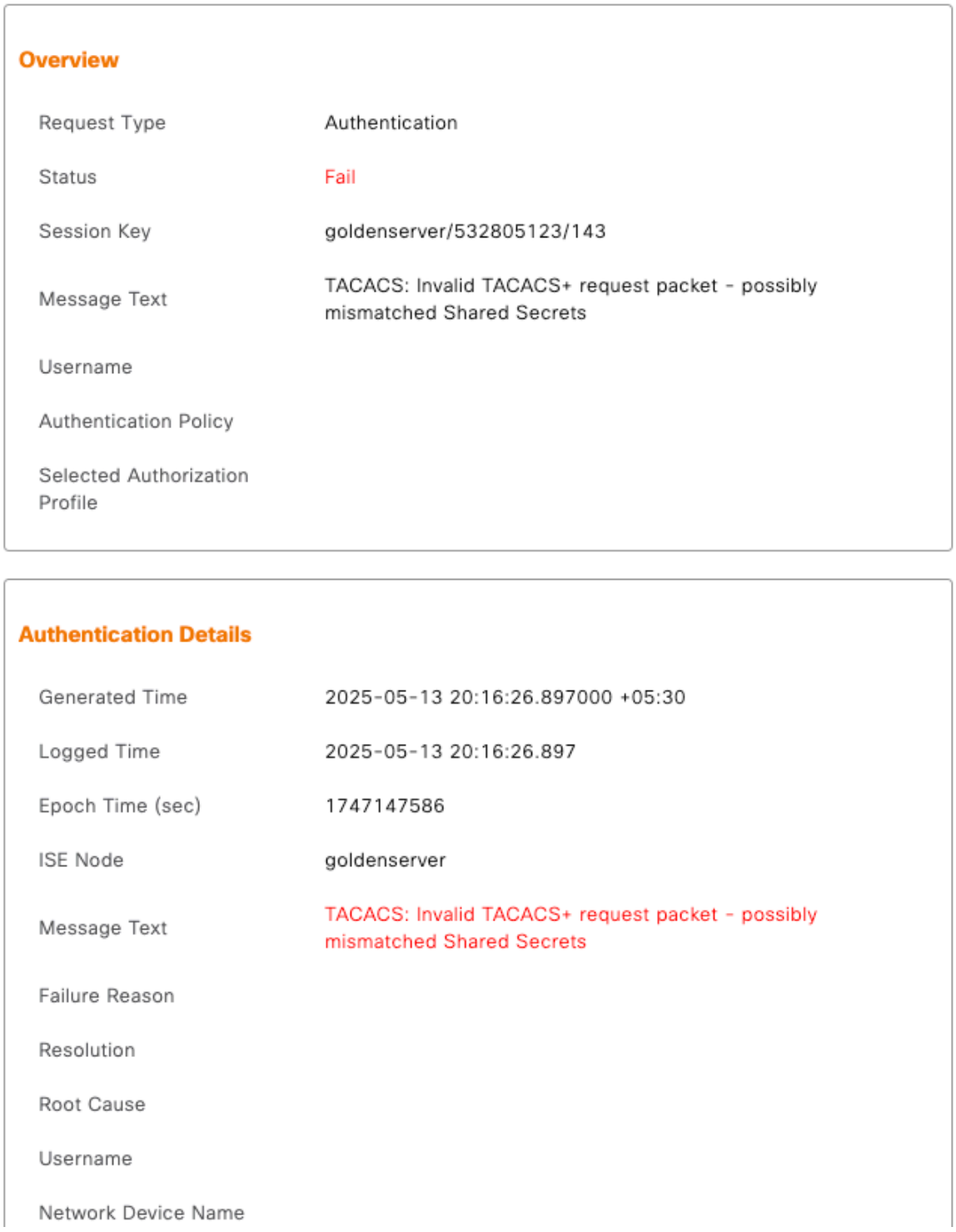
Identificeer de runtime-AAA-component, stel het logboekniveau in op debuggen, reproduceer het probleem en analyseer de logs voor verder onderzoek.

Probleemoplossing

TACACS: ongeldig TACACS+-aanvraagpakket – mogelijk niet-overeenkomende gedeelde geheimen

Probleem

De TACACS+-verificatie tussen de Cisco ISE en de Palo Alto-firewall (of een ander netwerkapparaat) mislukt met de foutmelding:
"Ongeldig TACACS+-aanvraagpakket - mogelijk niet-overeenkomende gedeelde geheimen"



Dit voorkomt succesvolle administratieve aanmeldingspogingen en kan invloed hebben op de toegangscontrole van het apparaat door middel van gecentraliseerde verificatie.

Mogelijke oorzaken

- Een mismatch in het gedeelde geheim dat is geconfigureerd op Cisco ISE en de Palo Alto-firewall of het netwerkapparaat.
- Onjuiste TACACS+-serverconfiguratie op het apparaat (zoals verkeerd IP-adres, poort of protocol).

Oplossing

Er zijn verschillende mogelijke oplossingen voor dit probleem:

1. Controleer het gedeelde geheim:

- Over Cisco ISE:
  Navigeer naar Beheer > Netwerkbronnen > Netwerkapparaten, selecteer het betreffende apparaat en bevestig het gedeelde geheim.
- Op de Palo Alto firewall:
  Ga naar Apparaat > Serverprofielen > TACACS+ en zorg ervoor dat het gedeelde geheim exact overeenkomt, inclusief hoofdletters en speciale tekens.

2. Controleer de instellingen van de TACACS+-server:

- Controleer of het juiste IP-adres en de juiste poort (standaard is 49) van Cisco ISE zijn geconfigureerd in het TACACS+-profiel van de firewall.
- Controleer of het protocoltype TACACS+ is (niet RADIUS).

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.