TACACS+-verificatie configureren op Arista-Switch met ISE

Inhoud

Inleiding

In dit document wordt beschreven hoe u Cisco ISE TACACS+ kunt integreren met een Arista-switch voor gecentraliseerde AAA van beheerderstoegang.

Voorwaarden

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco ISE en TACACS+ protocol.
- Arista switches

Gebruikte componenten

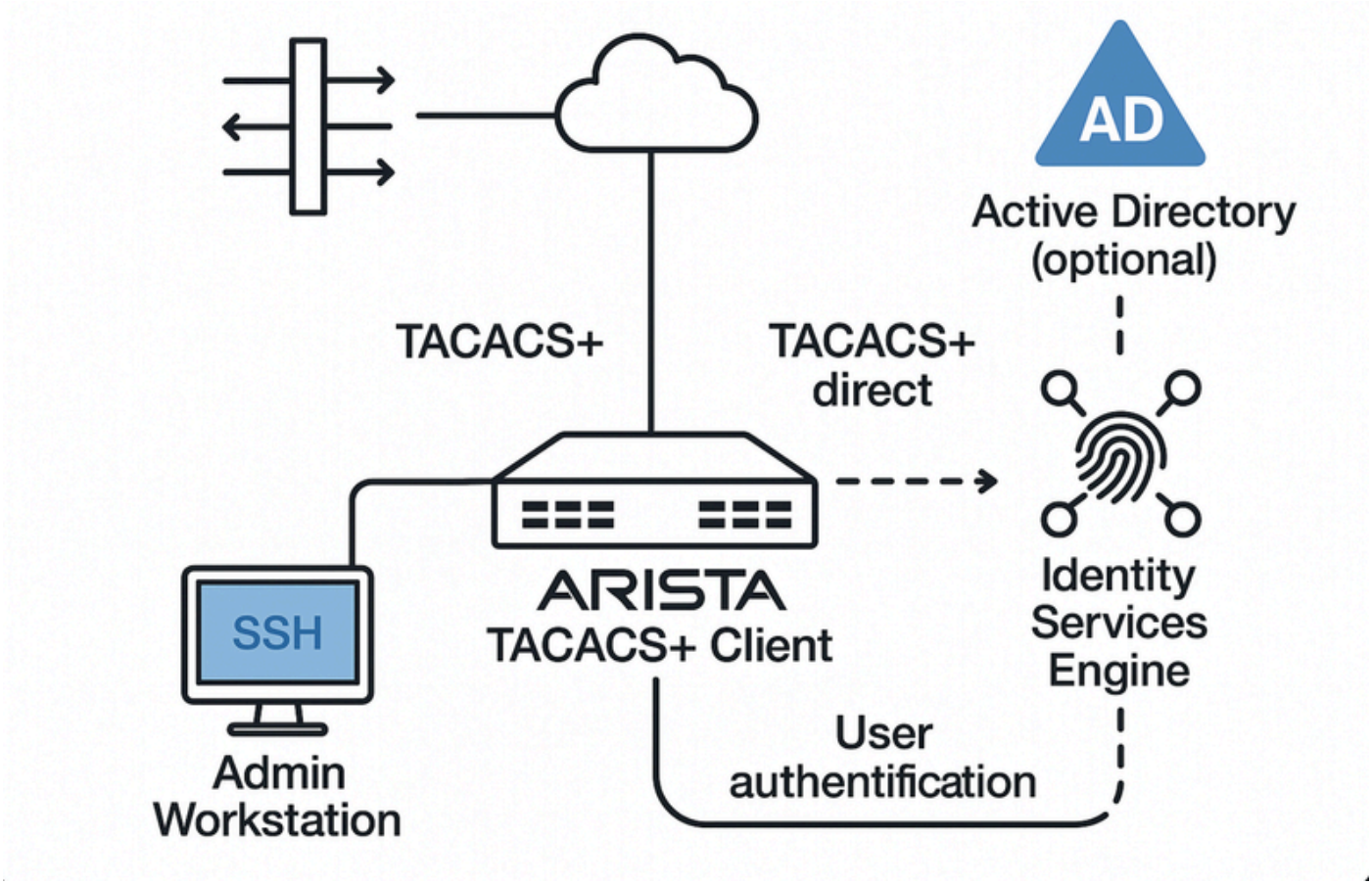
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Arista switch Software image versie: 4.33.2F
- 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

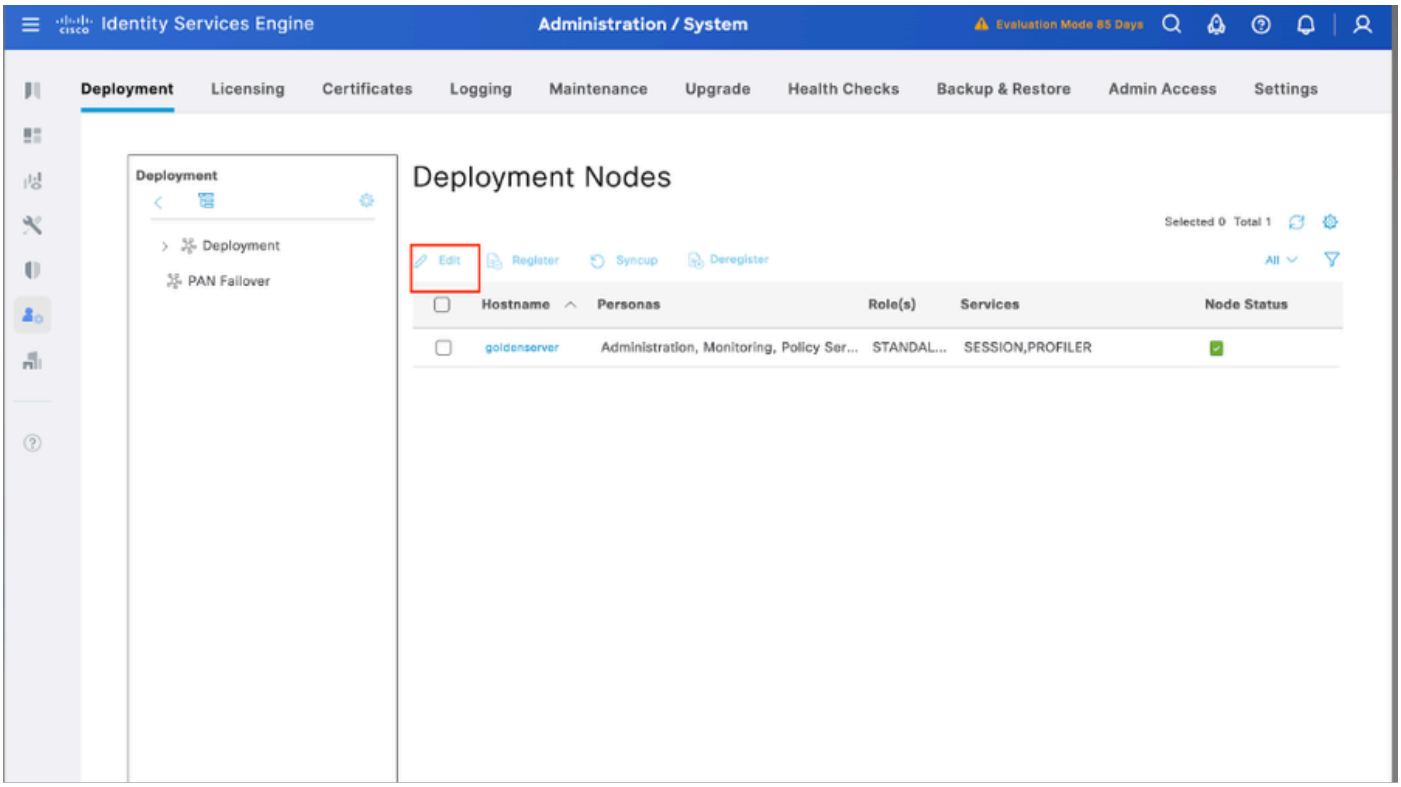


Configuraties

TACACS+-configuratie op ISE

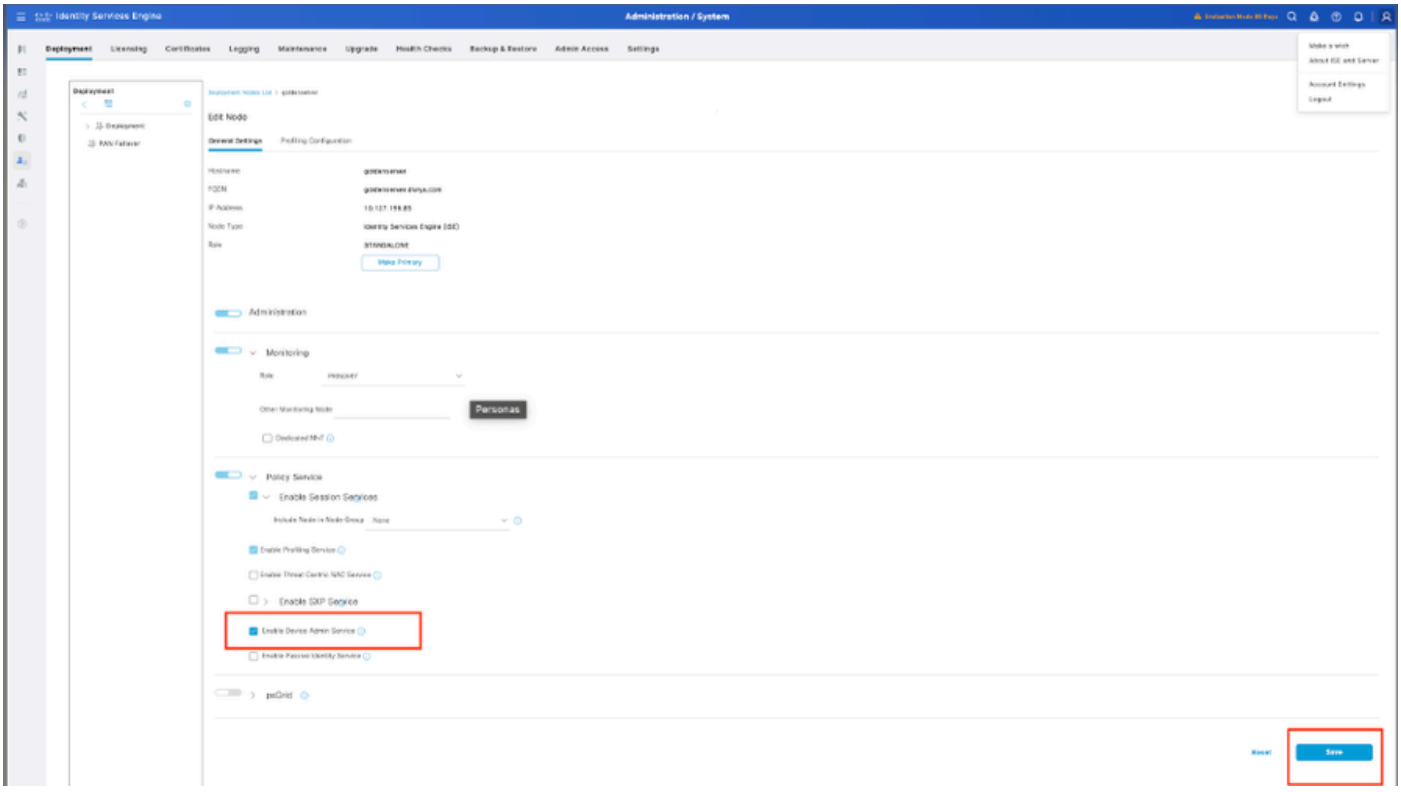
Stap 1. De eerste stap is om na te gaan of Cisco ISE over de nodige mogelijkheden beschikt om de TACACS+-verificatie af te handelen. Bevestig hiervoor dat de functie Apparaatbeheerservice is ingeschakeld in de gewenste beleidsserviceknooppunt (PSN).

Navigeer naar Beheer > Systeem > Implementatie, selecteer de juiste node 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.

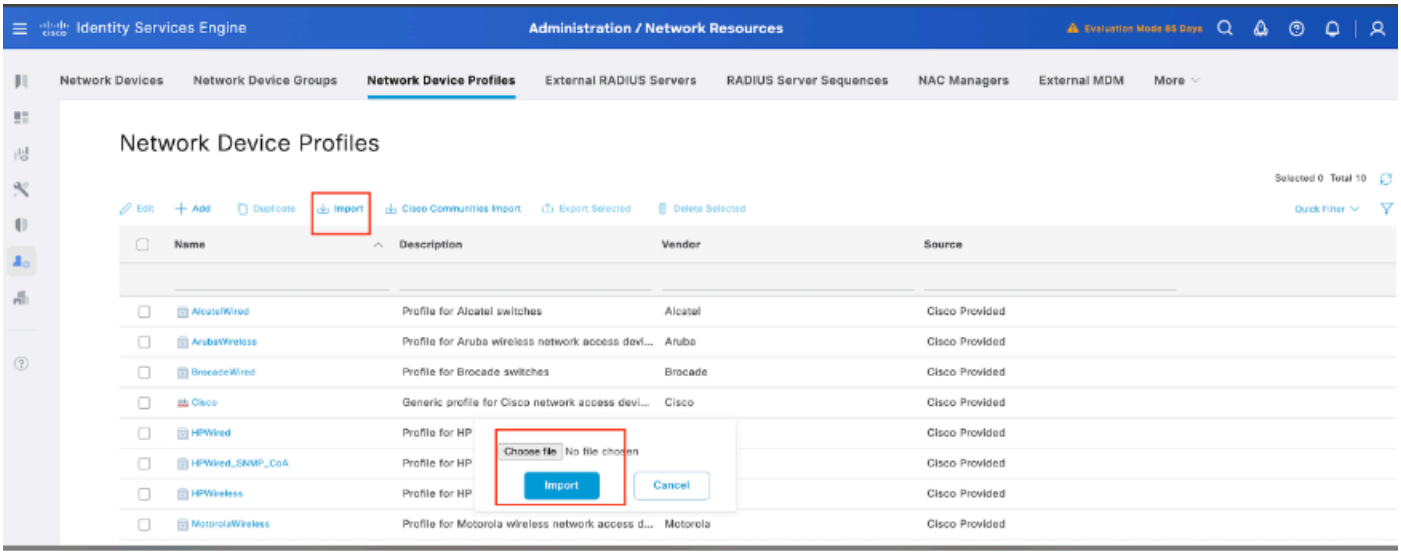


Stap 3. Het Arista Network Device Profile voor Cisco ISE verkrijgen.

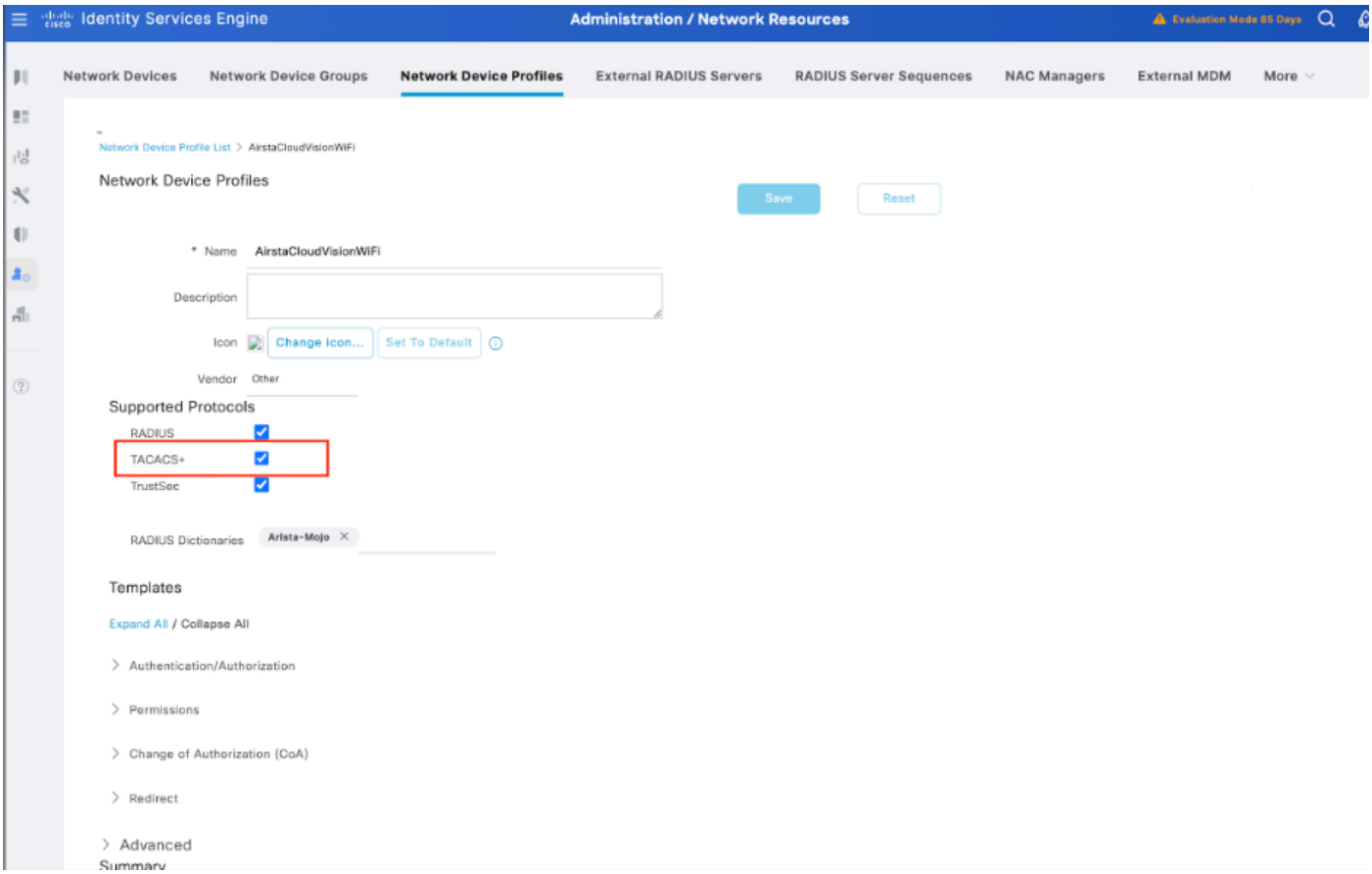
De Cisco Community heeft een speciaal NAD-profiel gedeeld voor Arista-apparaten. Dit profiel, samen met de benodigde woordenboekbestanden, is te vinden in het artikel Arista CloudVision WiFi Dictionary en NAD Profile for ISE Integration. Het downloaden en importeren van dit profiel in uw ISE-installatie vergemakkelijkt een soepelere integratie

Stappen voor het importeren van het Arista NAD-profiel in Cisco ISE:

1. Download het profiel:
    - Ontvang het Arista NAD profiel via de bovenstaande Cisco Community linkCisco Community
2. Toegang tot Cisco ISE:
    - Meld u aan bij uw Cisco ISE-beheerconsole
3. Het NAD-profiel importeren:
    - Navigeer naar Beheer > Netwerkbronnen > Netwerkapparaatprofielen
    - Klik op de knop Importeren
    - Upload het gedownloade Arista NAD profiel bestand.

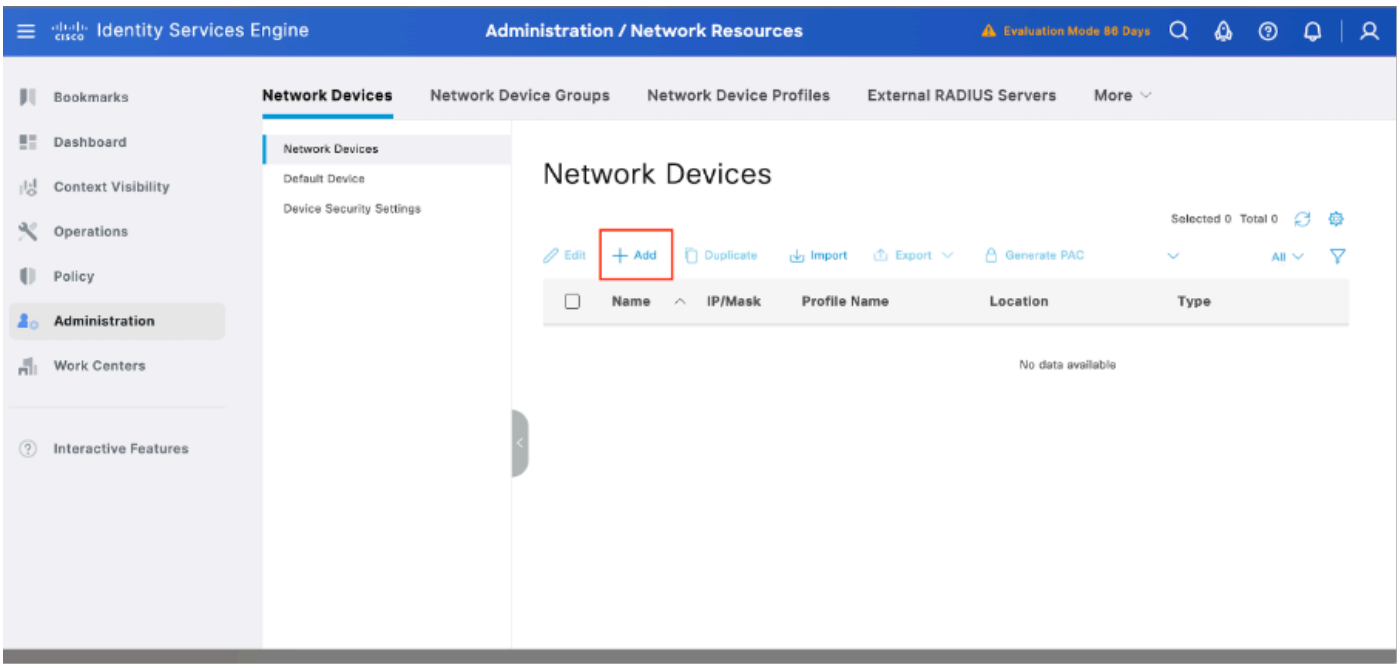


Nadat het uploaden is voltooid, navigeert u naar de optie Bewerken en schakelt u TACACS+ in als een ondersteund protocol.



Stap 2: Arista Switch toevoegen als netwerkapparaat.

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

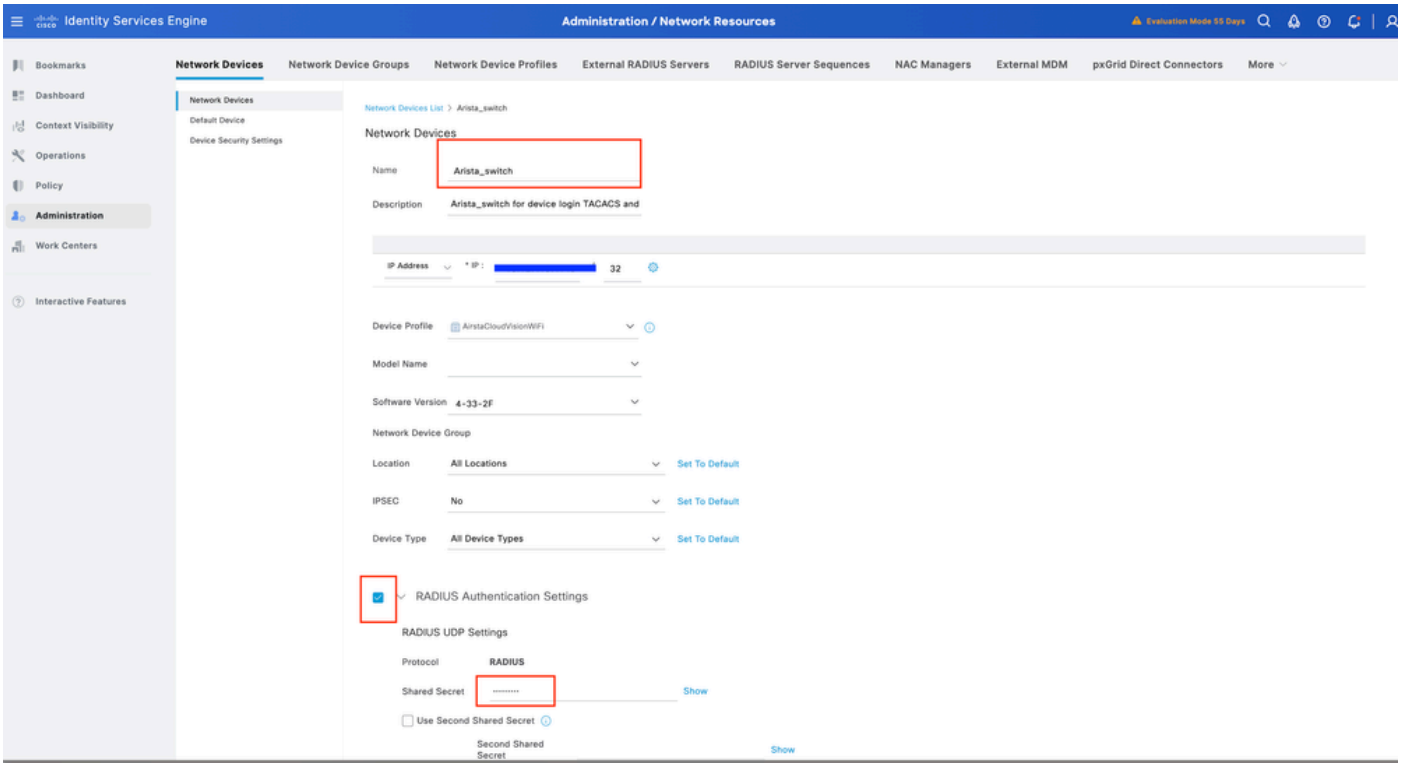


2. Klik op Toevoegen en voer deze gegevens in:

- IP-adres: <Switch-IP>
- Type apparaat: Andere bekabelde apparaten kiezen
- Netwerkapparaatprofiel: selecteer AirstaCloudVisionWiFi.

- RADIUS-verificatie-instellingen:
  - RADIUS-verificatie inschakelen.
  - Voer het gedeelde geheim in (dit moet overeenkomen met de configuratie van de switch).

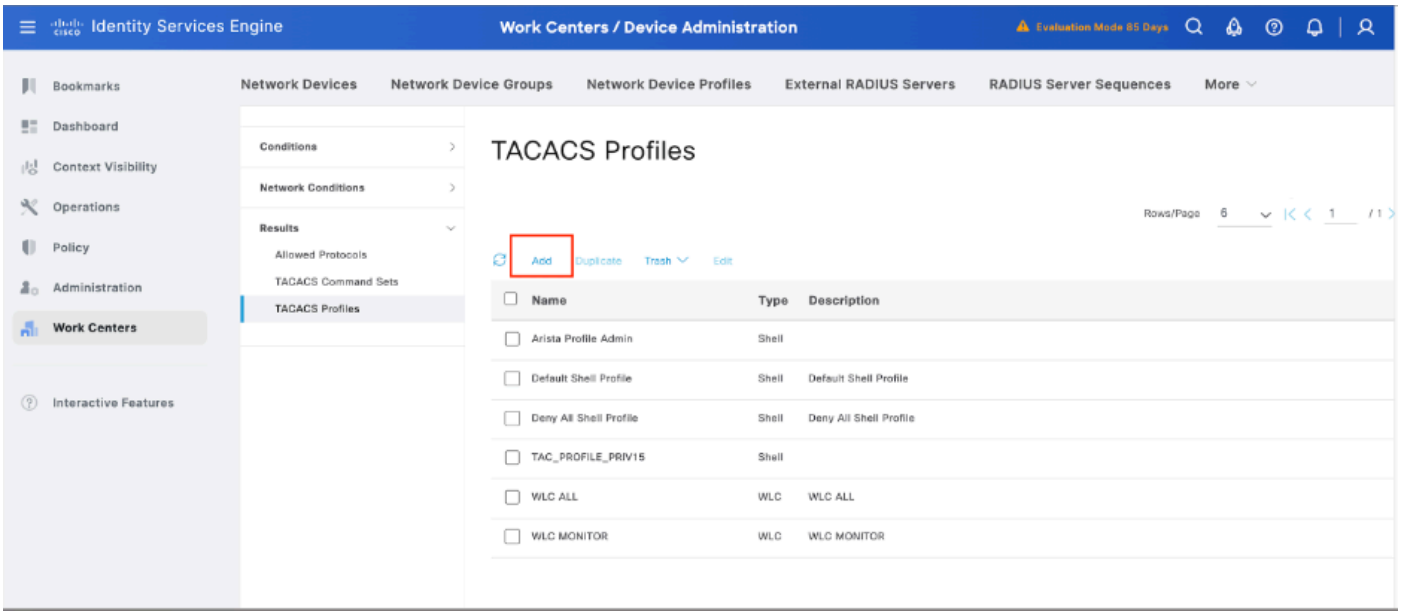
3. Klik op Opslaan:



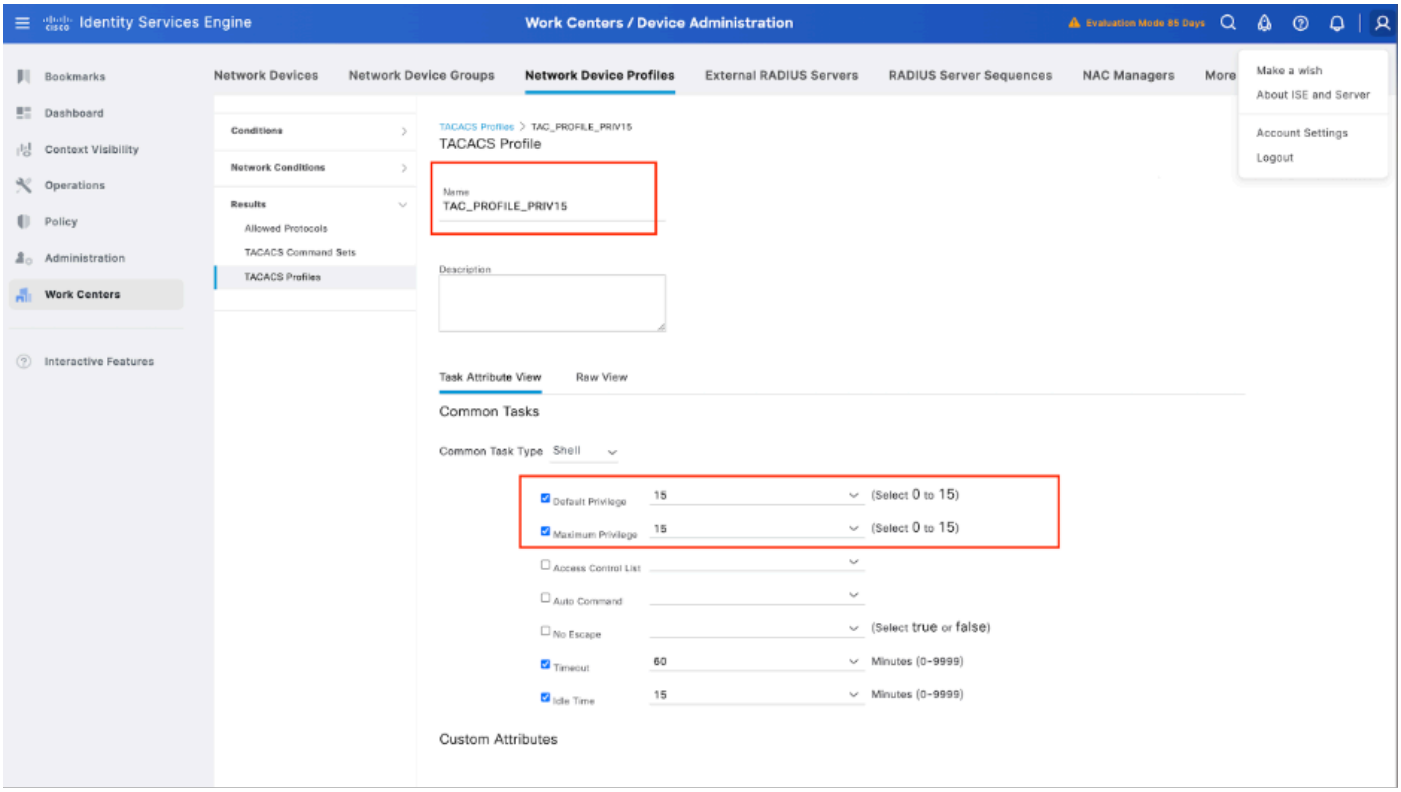
Stap 3. Het nieuwe apparaat valideren wordt weergegeven onder Netwerkapparaten:

Stap 4. Het TACACS-profiel configureren.

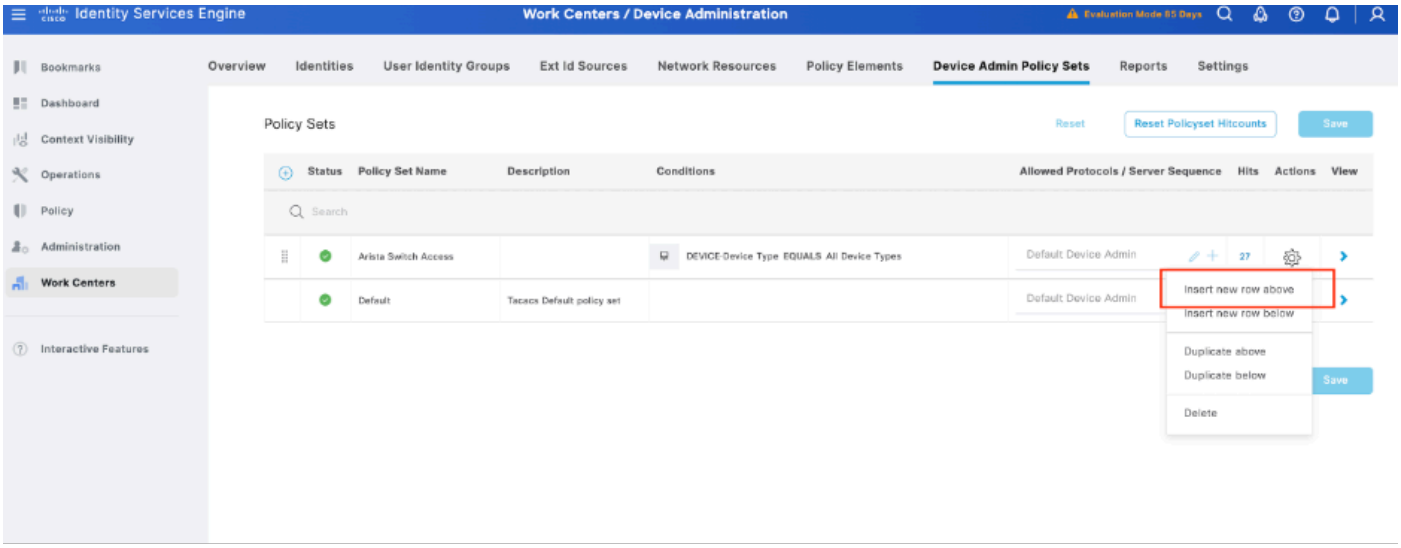
Maak een TACACS-profiel, navigeer naar het menu Werkcentra > Apparaatbeheer > Beleidselementen > Resultaten > TACACS-profielen en selecteer vervolgens Toevoegen:



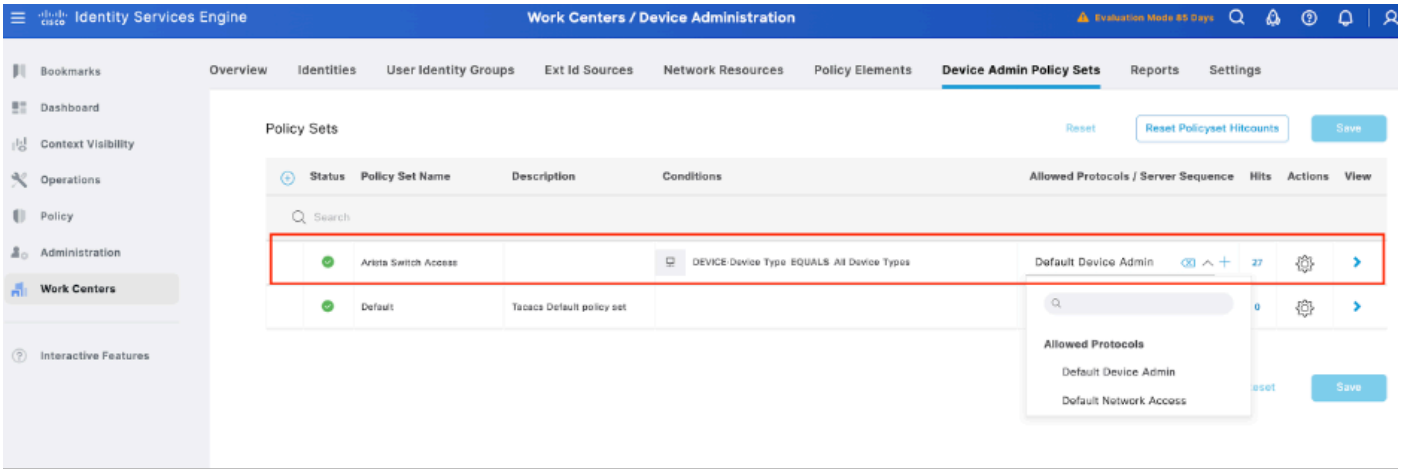
Voer een naam in, selecteer het selectievakje Standaardvoorrecht en stel de waarde in op 15. Selecteer bovendien Maximumvoorrecht, stel de waarde in op 15 en klik op Indienen:



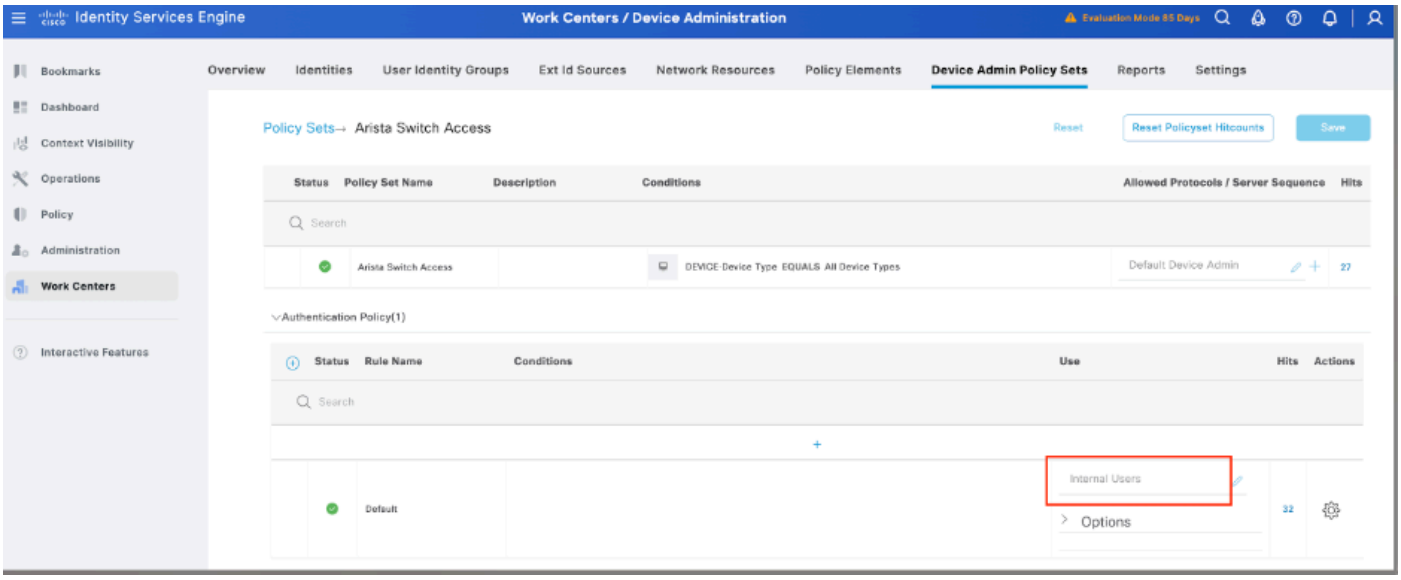
Stap 5. Maak een Device Admin Policy Set die voor uw Arista-Switch moet worden gebruikt, navigeer naar het menu Work Centers > Device Administration > Device Admin Policy Sets, selecteer vervolgens vanuit een bestaande beleidsset het tandwielpictogram en selecteer vervolgens een nieuwe rij hierboven invoegen.



Stap 6. Geef deze nieuwe beleidsset een naam, voeg voorwaarden toe afhankelijk van de eigenschappen van de TACACS+-verificaties die worden uitgevoerd vanuit de Arista-switch en selecteer als Toegestane protocollen > Standaardapparaatbeheer, sla uw configuratie op.

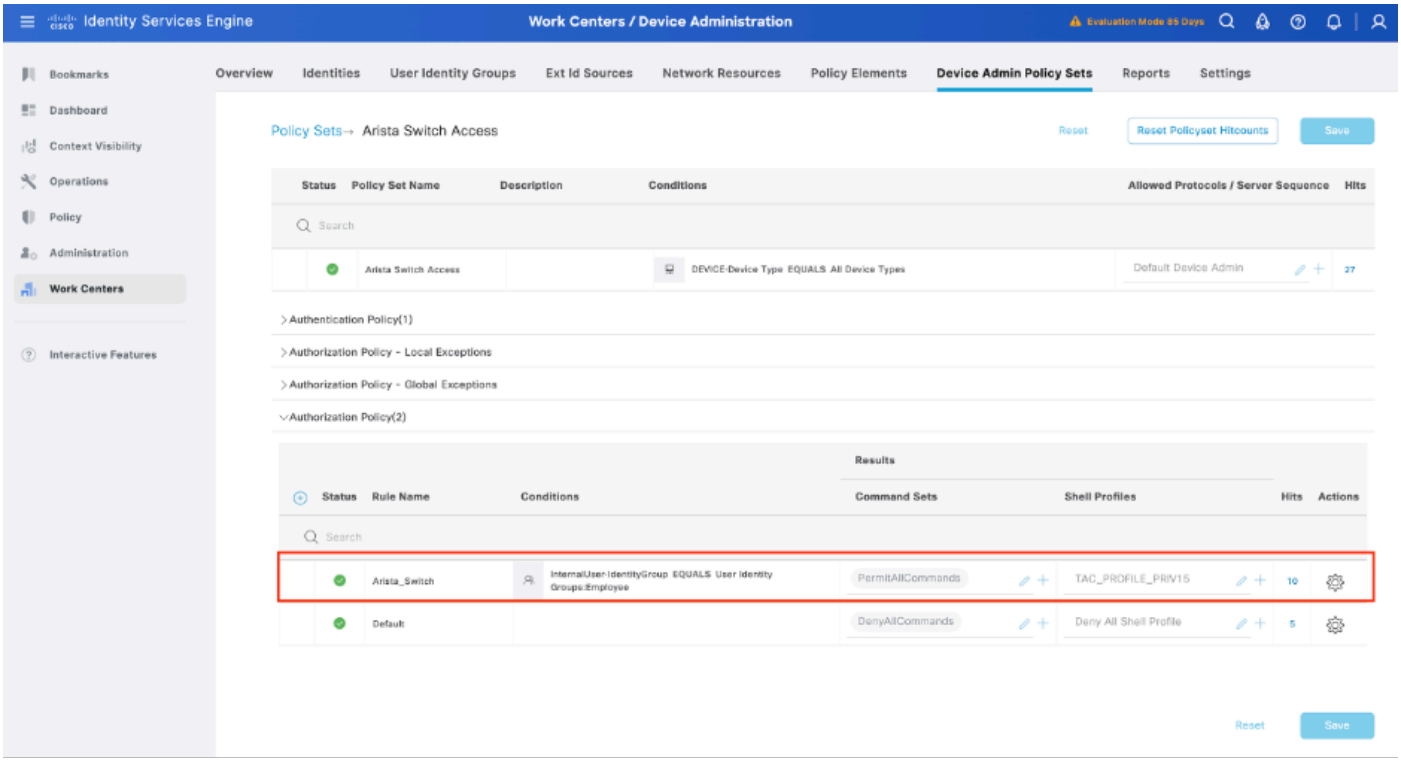


Stap 7. Selecteer in de optie > bekijken en selecteer vervolgens in het gedeelte Authenticatiebeleid de externe identiteitsbron die Cisco ISE gebruikt om de gebruikersnaam en referenties voor verificatie op de Arista-switch op te vragen. In dit voorbeeld komen de referenties overeen met interne gebruikers die zijn opgeslagen in ISE.



Stap 8. Scroll naar beneden tot de sectie Autorisatiebeleid naar standaardbeleid, selecteer het tandwielpictogram en plaats een regel hierboven.

Stap 9. Geef de nieuwe autorisatieregel een naam, voeg voorwaarden toe met betrekking tot de gebruiker die al is geverifieerd als groepslidmaatschap en voeg in de sectie Shell-profielen het TACACS-profiel toe dat u eerder hebt geconfigureerd, sla de configuratie op.



Arista-Switch configureren

Stap 1. TACACS+-verificatie inschakelen

Meld u aan bij de Arista switch en ga naar de configuratiemodus:

configureren

Ja!

tacacs-server host <ISE-IP> key <TACACS-SECRET>

Ja!

aaa-groepsserver tacacs+ ISE_TACACS

  server <ISE-IP>

Ja!

standaard aanmeldingsgroep voor aaa-verificatie ISE_TACACS lokaal

aaa authorisatie exec default groep ISE_TACACS lokaal

aaa accounting commando's 15 standaard start-stop groep ISE_TACACS

Ja!

einde

Stap 2. Sla de configuratie op

Om de configuratie tijdens het opnieuw opstarten te behouden:

Schrijfgeheugen

OF

Opstartconfiguratie voor kopiëren-uitvoeren

Verifiëren

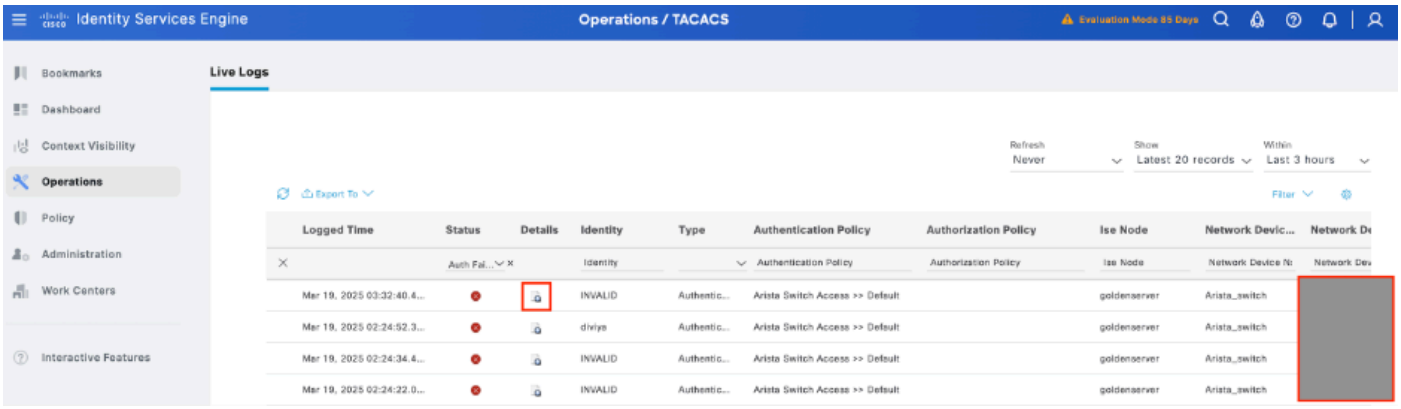
ISE-beoordeling

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

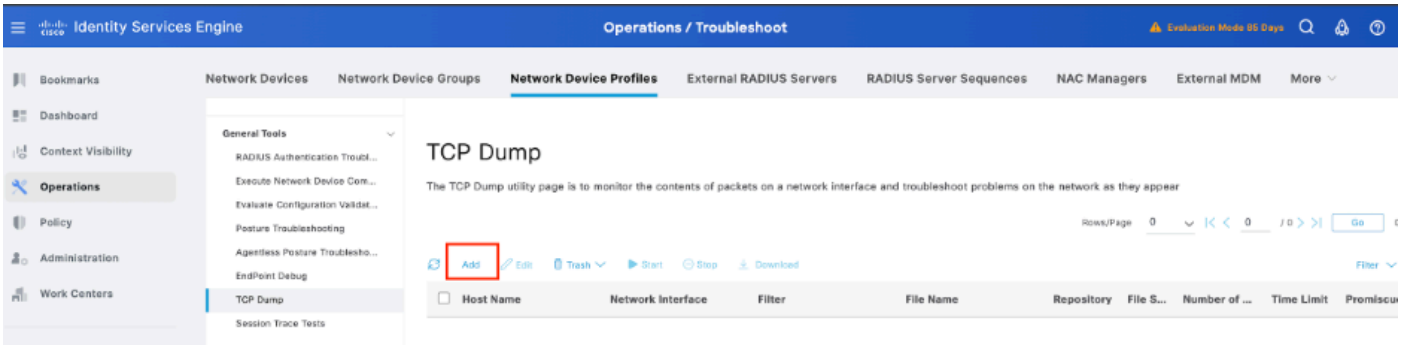
- GUI: controleer of de node is vermeld bij de service DEVICE ADMIN in > Systeem > Implementatie.
- CLI: Voer de opdracht show ports uit | neem 49 op om te bevestigen dat er verbindingen in de TCP-poort zijn die behoren tot TACACS+

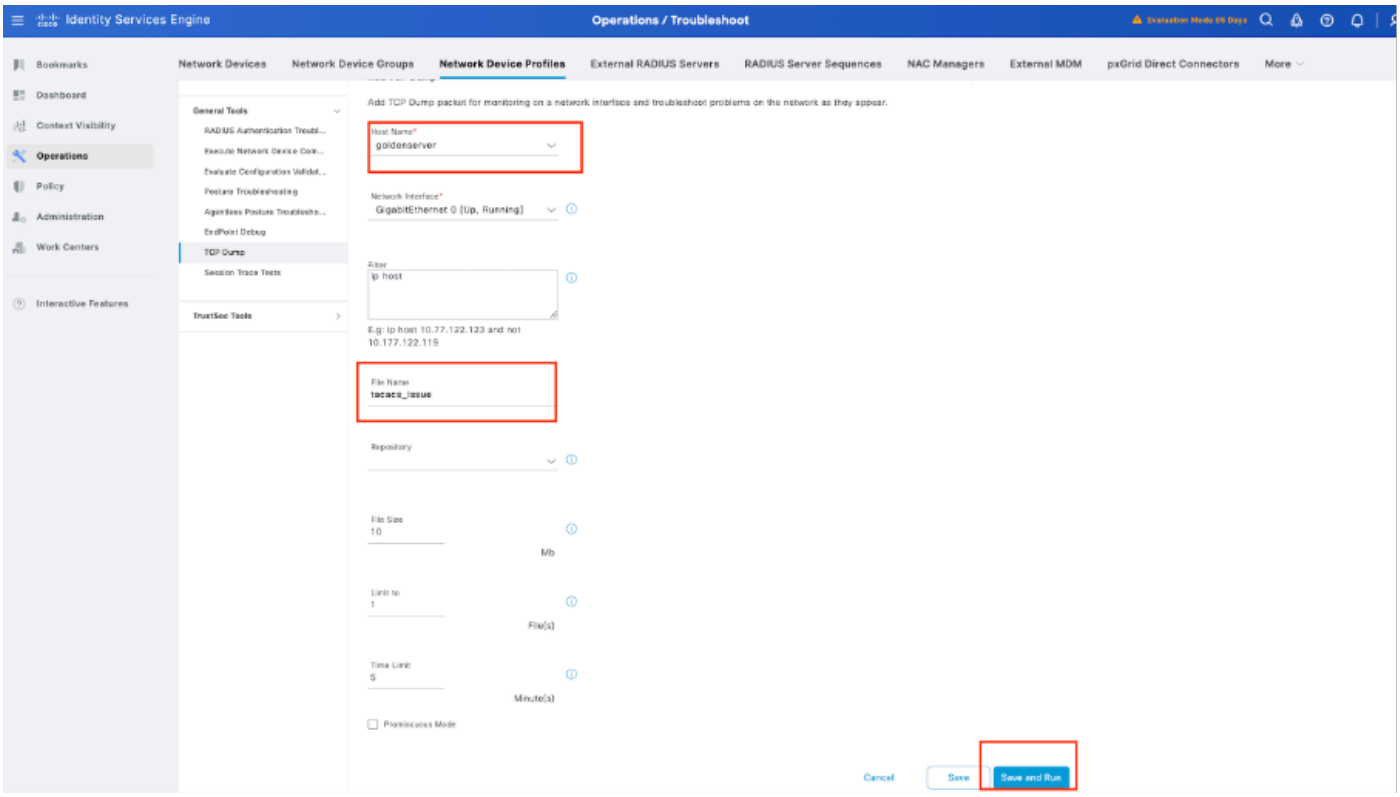
Stap 2. Bevestig of er livelogs zijn met betrekking tot TACACS+-verificatiepogingen: dit kan worden gecontroleerd in het menu Bewerkingen > TACACS > Live-logs,

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



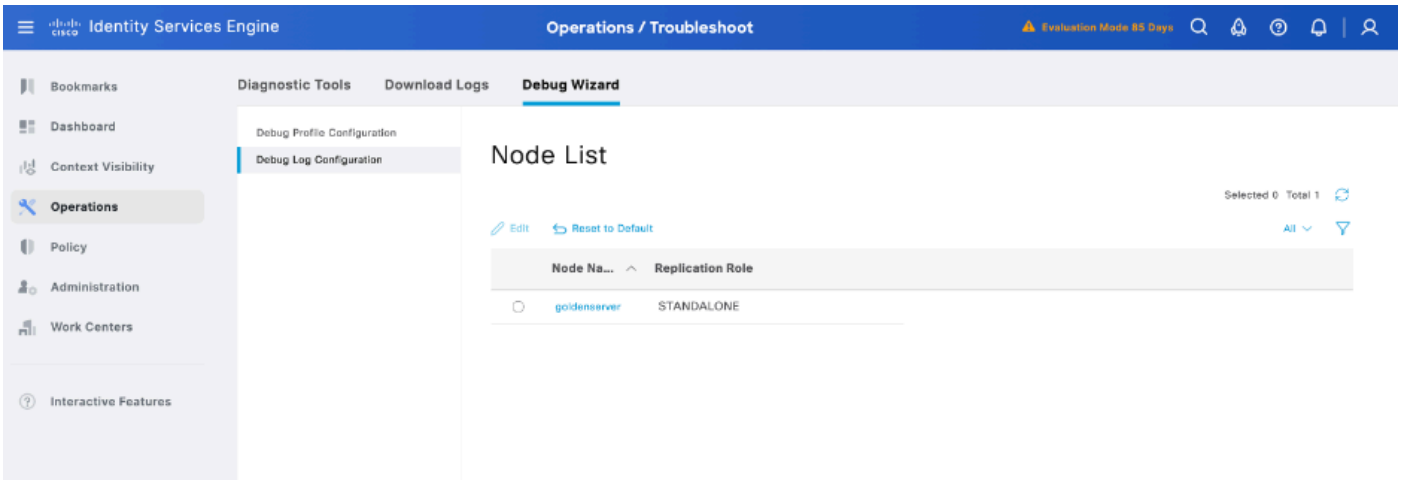
Stap 3. Als u geen livelog ziet, gaat u verder met het vastleggen van pakketten. Navigeer naar het menu Bewerkingen > Problemen oplossen > Diagnostische hulpprogramma's > Algemene hulpprogramma's > TCP-dumping, selecteer Toevoegen:

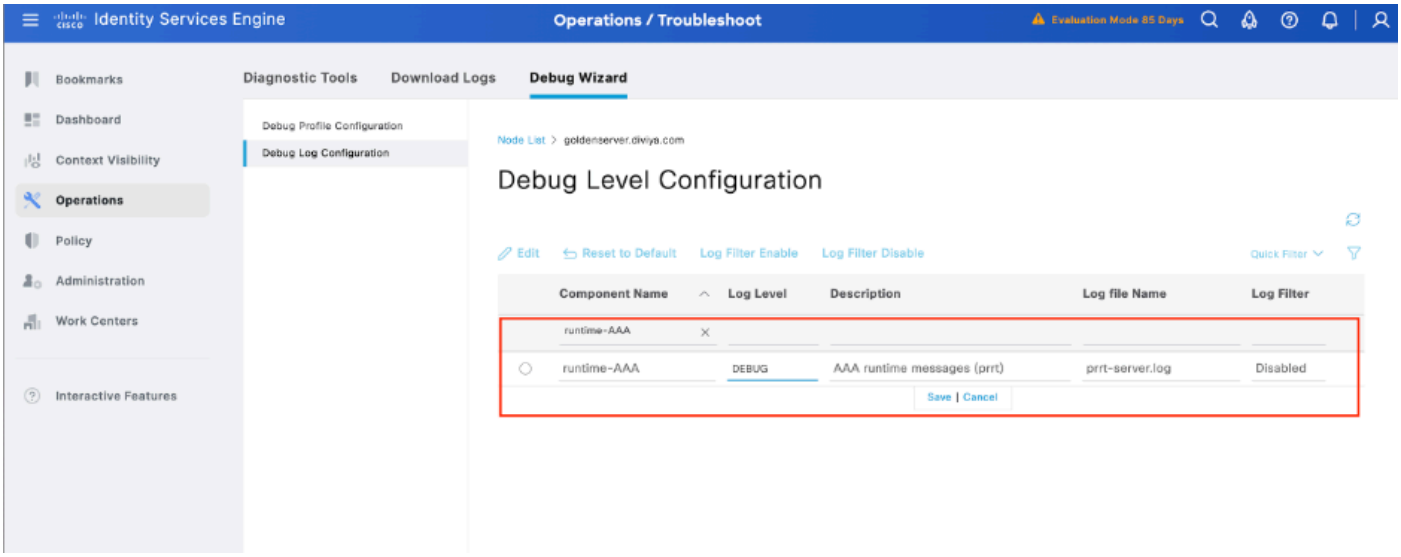




Stap 4. Schakel de component runtime-AAA in voor foutopsporing binnen de PSN van waaruit de

verificatie wordt uitgevoerd in Operations > Troubleshoot > Debug Wizard > Debug log configuratie, selecteer PSN node, en selecteer de knop Bewerken:





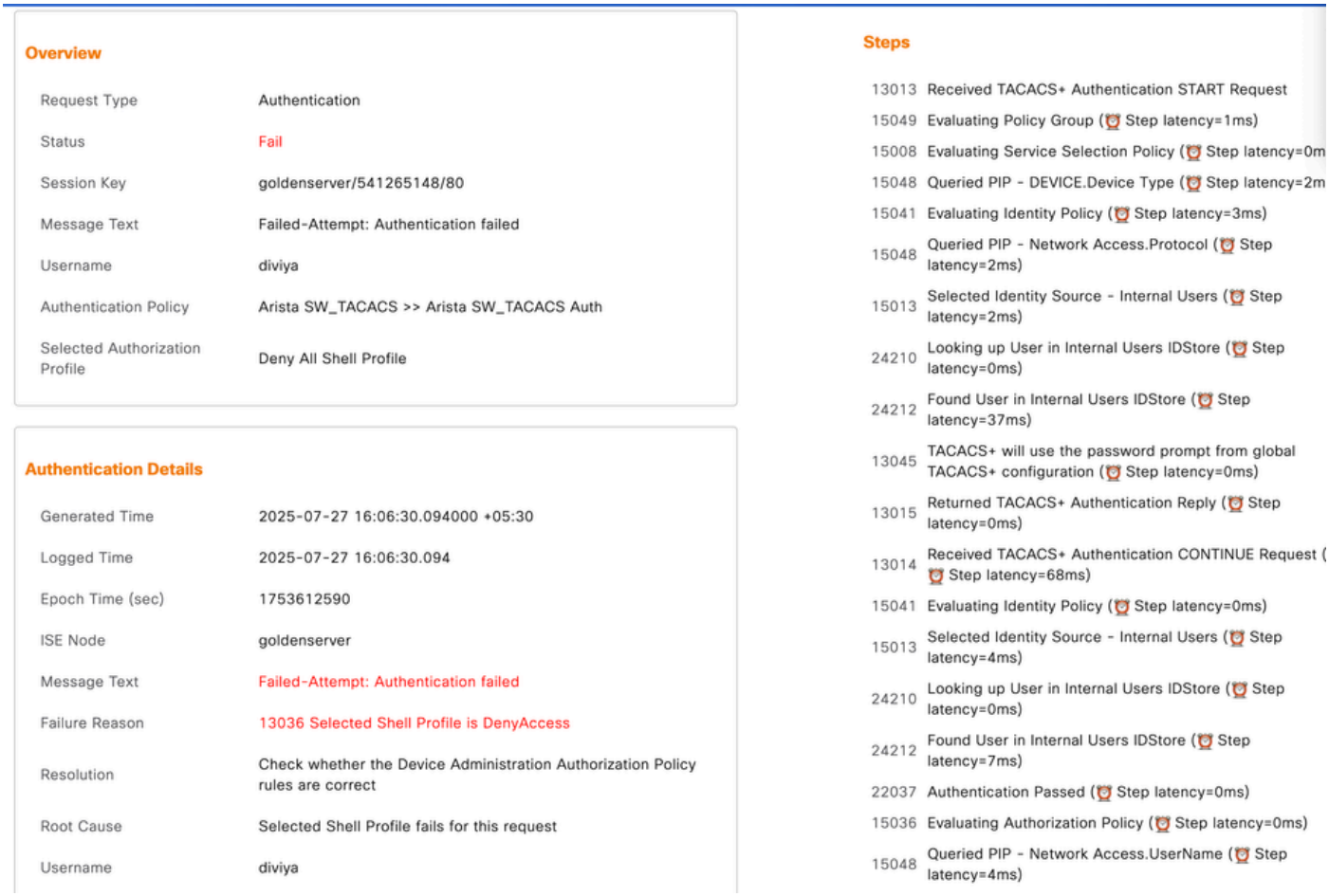
Identificeer de runtime-AAA-component, stel het logboekniveau in op debuggen, reproduceer het probleem en analyseer de logs voor verder onderzoek.

Probleemoplossing

Probleem 1

De TACACS+-verificatie tussen de Cisco ISE en de Arista-switch (of een ander netwerkapparaat) mislukt met de foutmelding:

"13036 Selected Shell Profile is DenyAccess"



De fout "13036 Selected Shell Profile is DenyAccess" in Cisco ISE betekent meestal dat tijdens een TACACS+-apparaatbeheerpoging het autorisatiebeleid overeenkomt met een shell-profiel dat is ingesteld op DenyAccess.Dit is meestal niet het gevolg van een verkeerd geconfigureerd shell-profiel zelf, maar geeft eerder aan dat geen van de geconfigureerde autorisatieregels overeenkwam met de attributen van de inkomende gebruiker (zoals groepslidmaatschap, apparaattype of locatie). Als gevolg hiervan valt ISE terug naar een standaardregel of een expliciete weigeringsregel, waardoor de toegang wordt geweigerd.

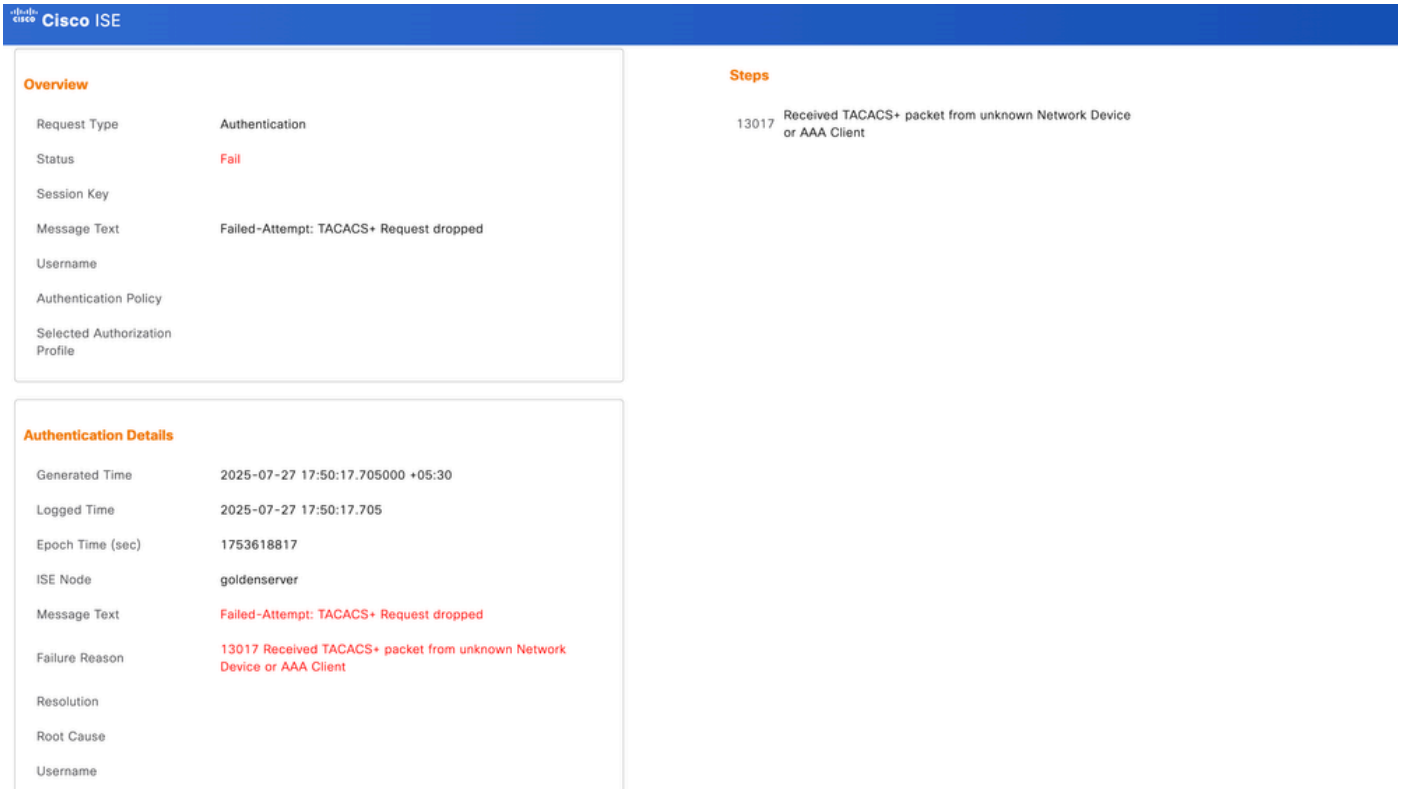
Mogelijke oorzaken

- Herziening van de regels voor het vergunningenbeleid in ISE. Bevestig dat de gebruiker of het apparaat voldoet aan de juiste regel die het beoogde shell-profiel toewijst, zoals een regel die passende toegang mogelijk maakt.
- Zorg ervoor dat de toewijzing van de AD of interne gebruikersgroep correct is en dat de beleidsvoorwaarden, zoals lidmaatschap van de gebruikersgroep, apparaattype en protocol, nauwkeurig worden gespecificeerd.
- Gebruik ISE live logs en details van de mislukte poging om precies te zien welke regel is gekoppeld en waarom.

Probleem 2

De TACACS+-verificatie tussen de Cisco ISE en de Arista-Switch (of een ander netwerkapparaat) mislukt met de foutmelding:

"13017 Ontvangen TACACS+-pakket van onbekend netwerkapparaat of AAA-client"



Mogelijke oorzaken

- De meest voorkomende reden is dat het IP-adres van de switch niet wordt toegevoegd als netwerkapparaat in ISE (onder Beheer > Netwerkbronnen > Netwerkapparaten).
- Zorg ervoor dat het IP-adres of bereik exact overeenkomt met het bron-IP dat door de Arista-switch wordt gebruikt om TACACS+-pakketten te verzenden.
- Als uw switch een beheerinterface gebruikt, controleert u of het exacte IP-adres (niet alleen een subnet/bereik) is toegevoegd in ISE.

Oplossing

- Ga naar Beheer > Netwerkbronnen > Netwerkapparaten in de ISE GUI.
- Controleer of het exacte bron-IP-adres op de Arista-switch wordt gebruikt voor TACACS+-communicatie (meestal de beheerinterface IP).
- Geef het gedeelde geheim op (het moet overeenkomen met wat is ingesteld op de Arista-switch).

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.