ISE configureren als externe verificatie voor DNAC GUI

Inhoud

Inleiding

Dit document beschrijft hoe u Cisco Identity Services Engine (ISE) kunt configureren als externe verificatie voor het beheer van Cisco DNA Center GUI.

Voorwaarden

Vereisten

Cisco raadt u aan deze onderwerpen te kennen:

- TACACS+- en RADIUS-protocollen.
- Cisco ISE-integratie met Cisco DNA Center
- Cisco ISE-beleidsevaluatie.

Gebruikte componenten

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

- Cisco Identity Services Engine (ISE) versie 3.4 patch1.
- Cisco DNA Center versie 2.3.5.5.1

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.

Voordat u begint

- Zorg ervoor dat er ten minste één RADIUS-verificatieserver is geconfigureerd op Systeem > Instellingen > Externe services > Verificatie- en beleidsservers.
- Alleen een gebruiker met SUPER-ADMIN-ROL permissies op DNAC kan deze procedure uitvoeren.
- Schakel externe verificatiefalback in.

⚠ Voorzichtig: In releases eerder dan 2.1.x, wanneer externe verificatie is ingeschakeld, valt Cisco DNA Center terug naar lokale gebruikers als de AAA-server onbereikbaar is of als de AAA-server een onbekende gebruikersnaam afwijst. In de huidige release valt Cisco DNA Center niet terug naar lokale gebruikers als de AAA-server onbereikbaar is of als de AAA-server een onbekende gebruikersnaam afwijst. Als de externe verificatie is ingeschakeld, kunnen externe gebruikers en lokale beheerders inloggen bij Cisco DNA Center.

Als u externe verificatiefalback wilt inschakelen, selecteert u SSH in de Cisco DNA Center-instantie en voert u de opdracht deze CLI in (magctl rbac external_auth_fallback).

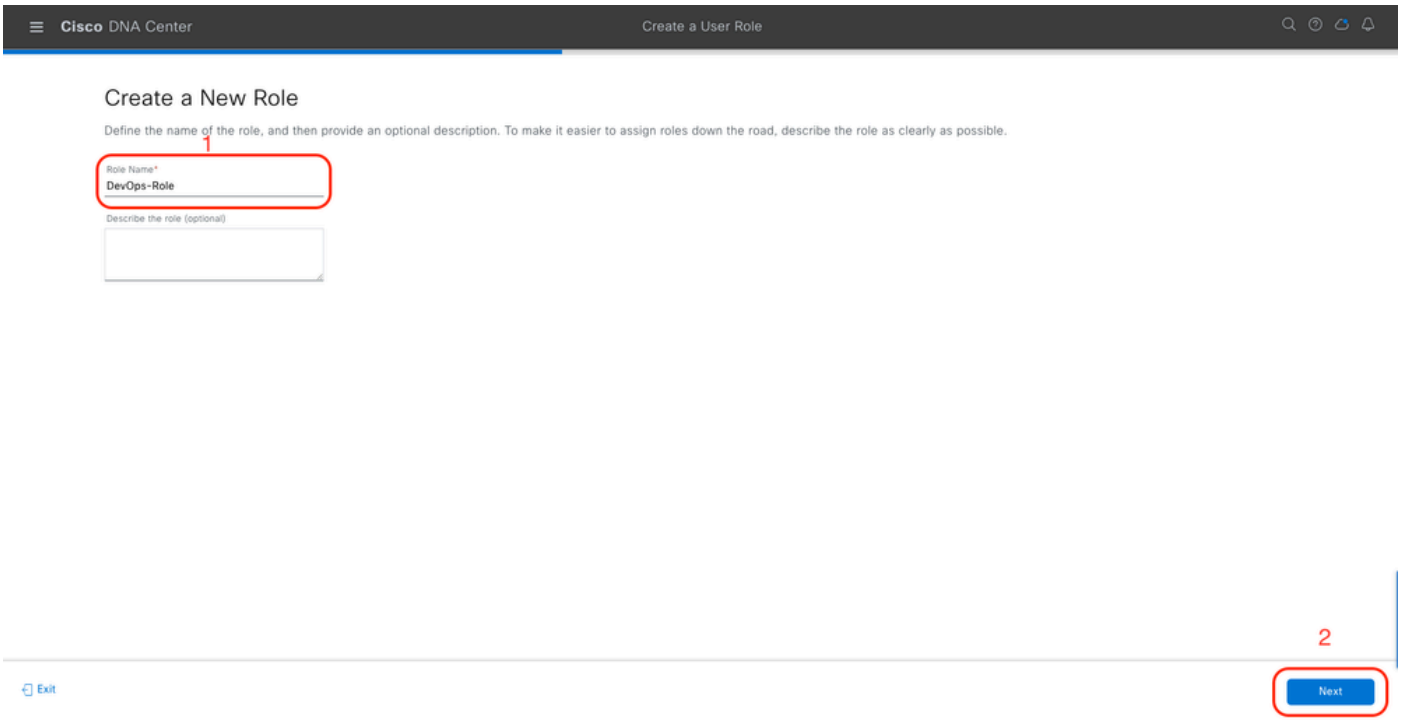
Configureren

(Option1) configureren van DNAC externe verificatie met behulp van RADIUS

Stap 1. (optioneel) Definieer een aangepaste rollen.
Configureer uw aangepaste rollen die aan uw eis voldoen, in plaats daarvan kunt u de standaard gebruikersrollen gebruiken. Dit kan worden gedaan via het tabblad Systeem > Gebruikers & rollen > Role Based Access Control.

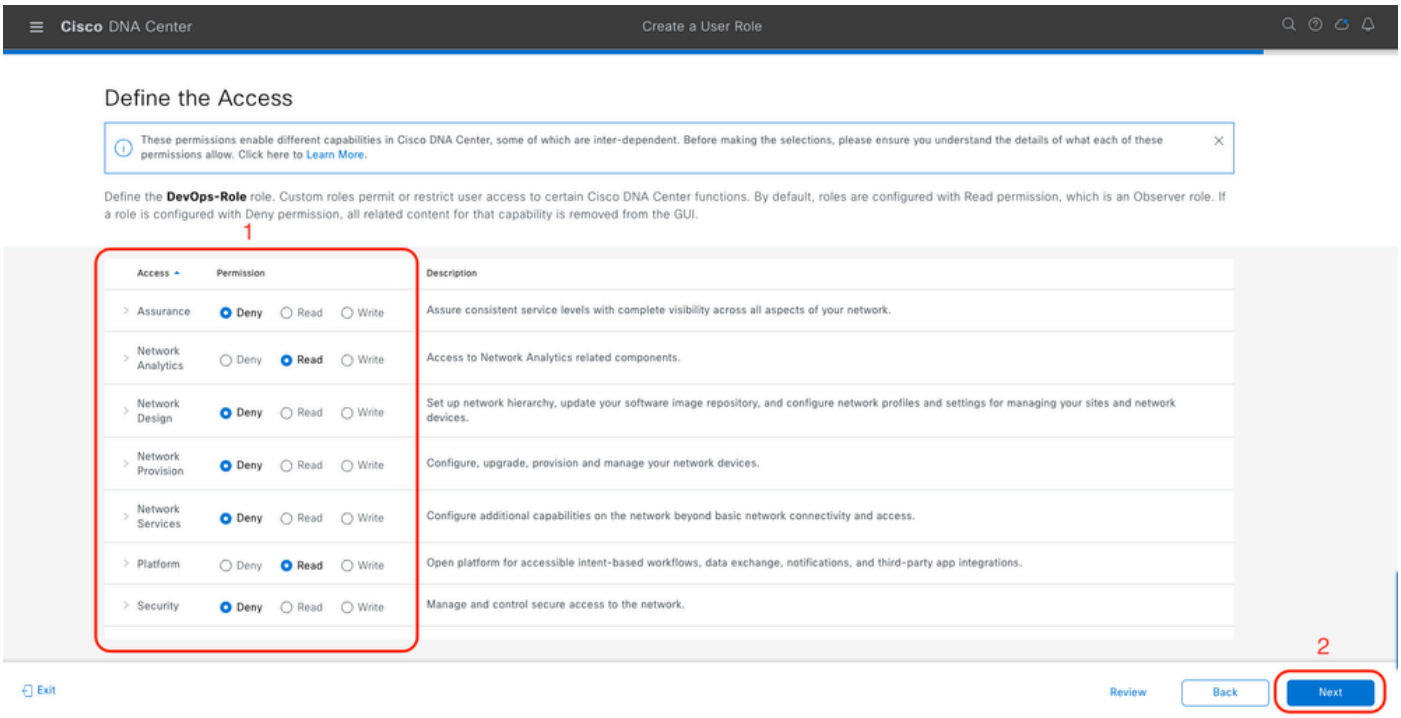
Procedure

a. Creëer een nieuwe rol.



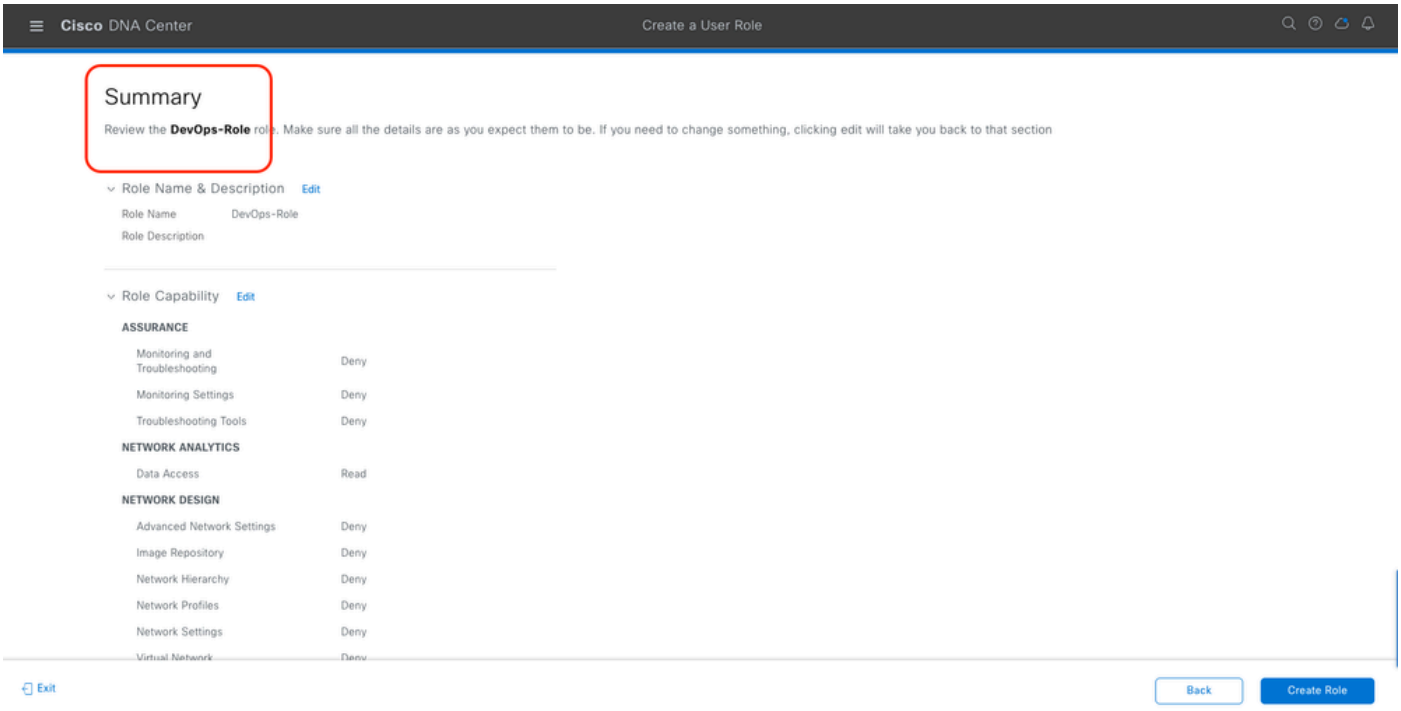
Functienaam DevOps

b. Definieer de toegang.

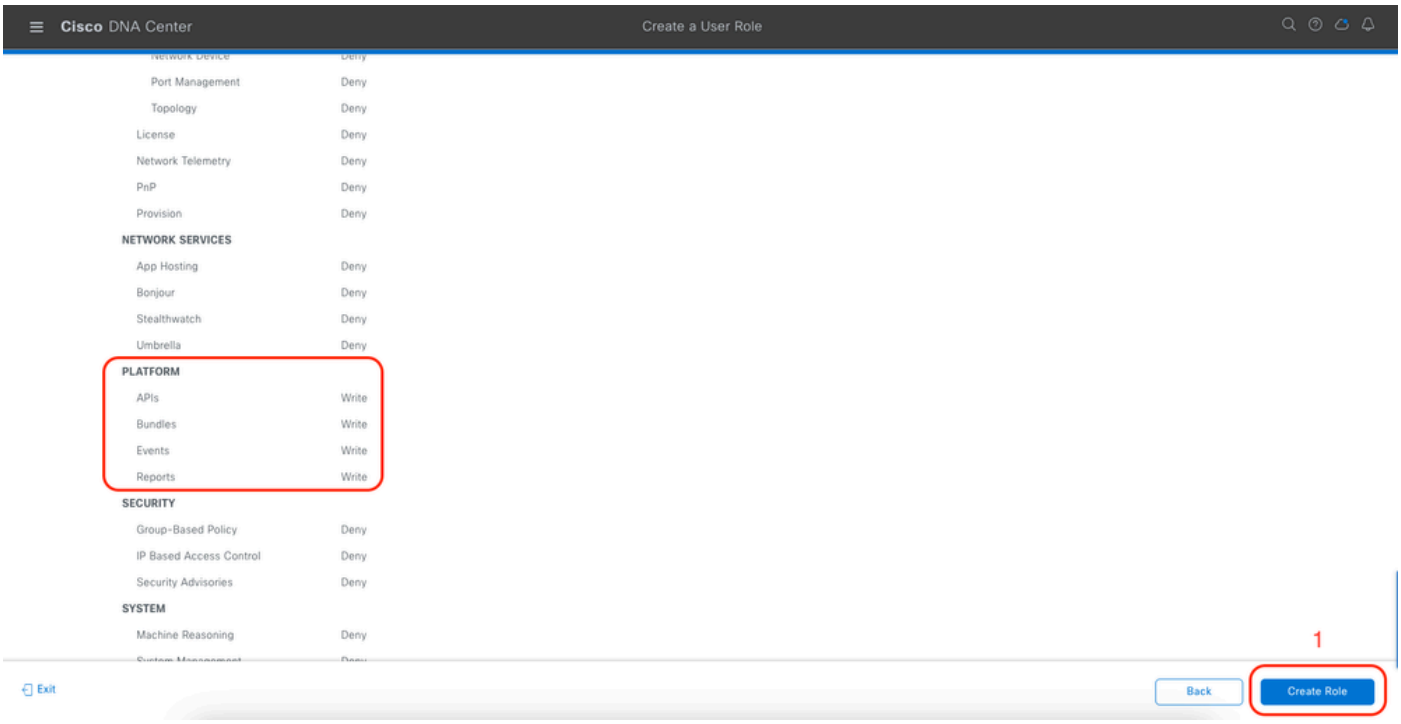


DTVops-roltoegang

c. Maak de nieuwe rol aan.



Samenvatting van DevOps-rol



Rol van devOps bekijken en maken

Stap 2. Configureer externe verificatie met RADIUS.
Dit kan worden gedaan via het tabblad Systeem > Gebruikers & rollen > Externe verificatie.

Procedure

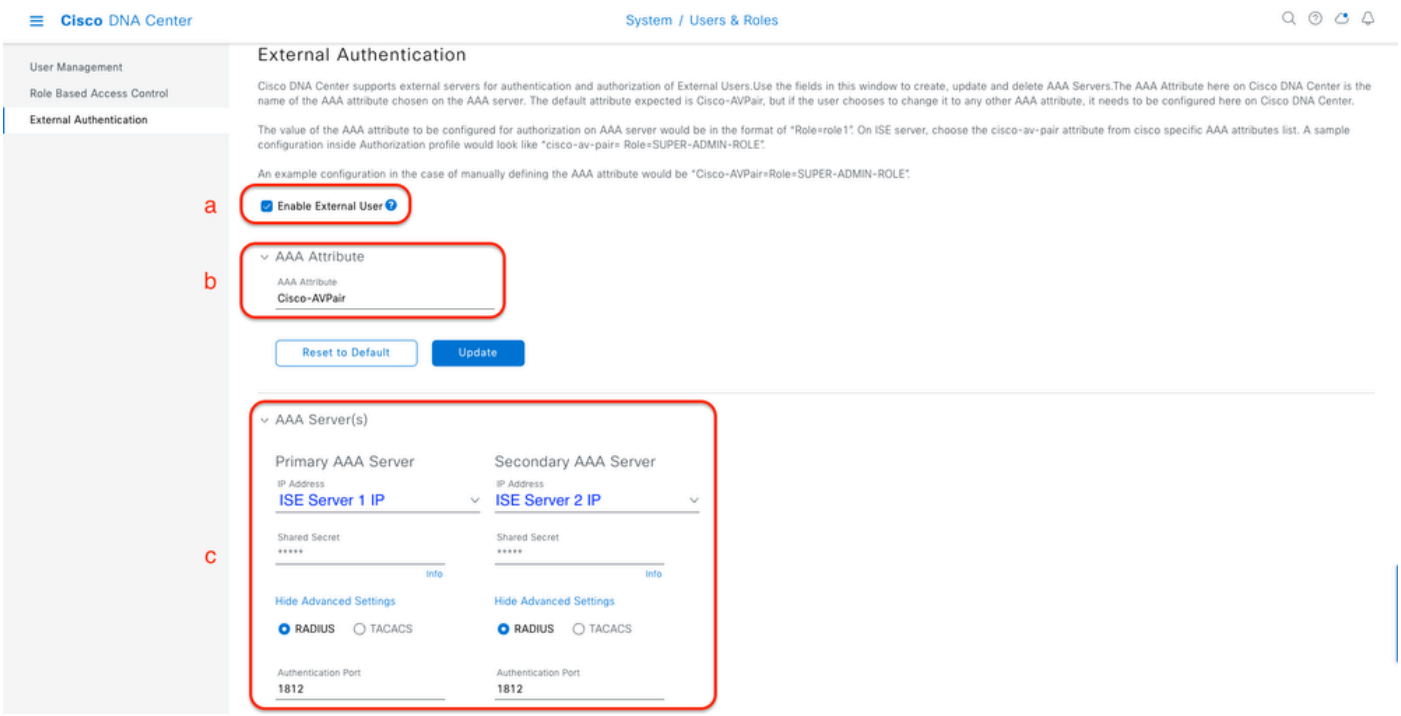
a. Als u externe verificatie in Cisco DNA Center wilt inschakelen, schakelt u het aanvinkvakje Externe gebruiker inschakelen in.

b. Stel de AAA-kenmerken in.

Voer Cisco AVPair in het veld AAA-kenmerken in.

c. (Optioneel) Configureer de primaire en secundaire AAA-server.

Zorg ervoor dat het RADIUS-protocol ten minste is ingeschakeld op de primaire AAA-server, of op zowel de primaire als de secundaire server.



(RADIUS) externe verificatiestappen

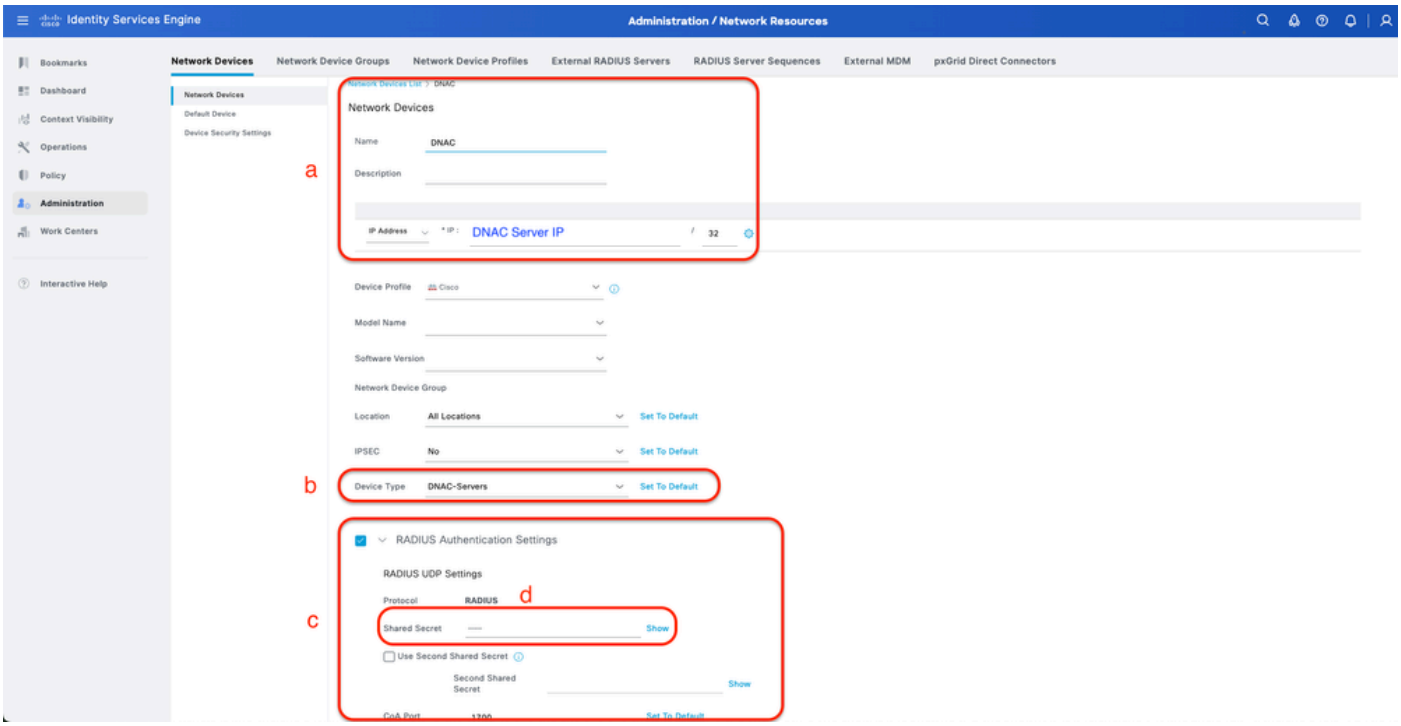
(Optie 1) ISE-instellingen voor RADIUS configureren

Stap 1. Voeg DNAC-server toe als netwerkapparaat op ISE.

Dit kan worden gedaan via het tabblad Beheer > Netwerkbronnen > Netwerkapparaten.

Procedure

a. Definieer (DNAC) naam en IP van netwerkapparaat.
b. (Optioneel) Apparaattype classificeren voor voorwaarde beleidsinstelling.
c. Schakel RADIUS-verificatie-instellingen in.
d. RADIUS gedeeld geheim instellen.



ISE Network Device (DNAC) voor RADIUS

Stap 2. Maak RADIUS-autorisatieprofielen.

Dit kan via het tabblad worden gedaan Beleid > Beleidselementen > Resultaten > autorisatie > Autorisatieprofielen.

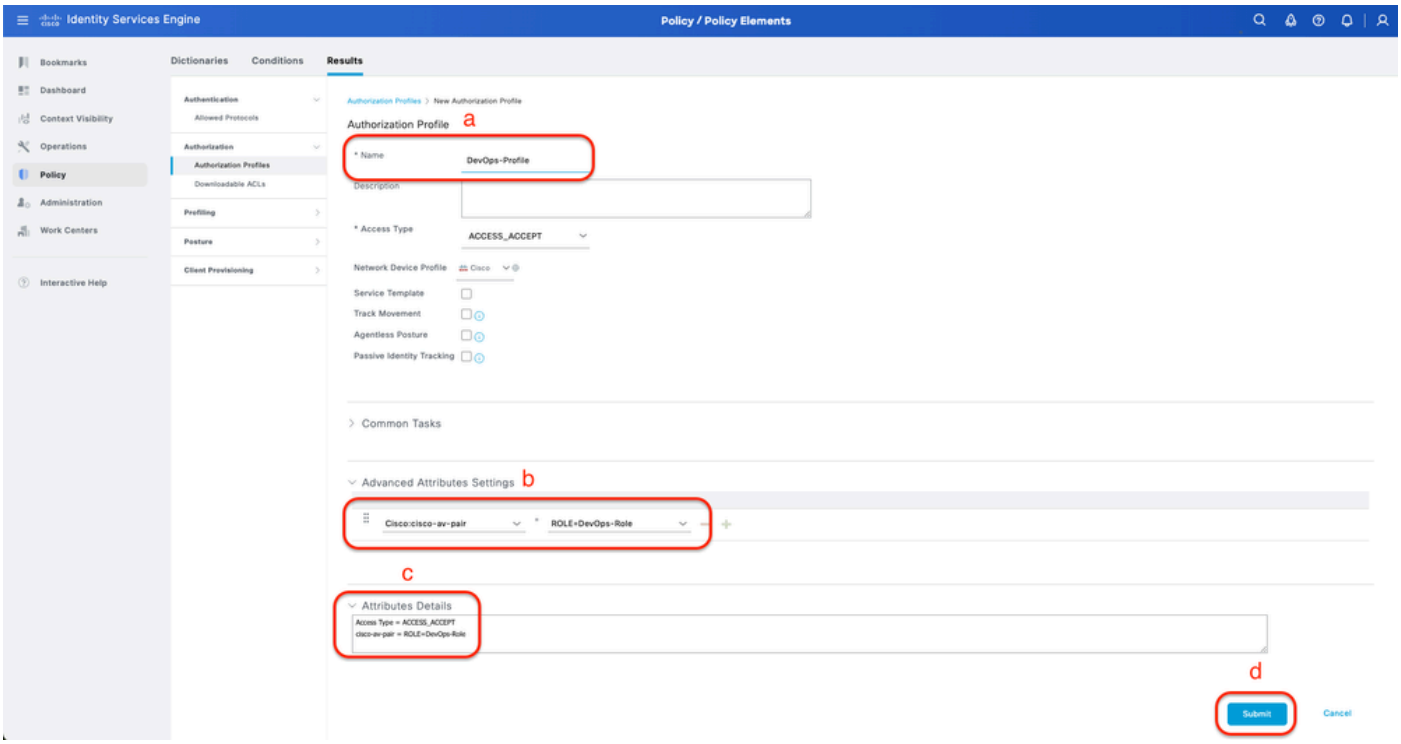
Opmerking: 3x RADIUS-autorisatieprofielen maken, één voor elke gebruikersrol.

Procedure
a. Klik op Add en definieer de naam van het RADIUS-autorisatieprofiel.

b. Voer het Cisco:cisco-av-paar in in de instellingen van geavanceerde kenmerken en vul de juiste gebruikersrol in.

- Voer voor de gebruikersrol (DecOps-Role) ROL=DevOps-Role in.
- Voor de gebruikersrol (NETWORK-ADMIN-ROL) voert u ROL=NETWORK-ADMIN-ROL in.
- Voer voor de gebruikersrol (SUPER-ADMIN-ROL) ROL=SUPER-ADMIN-ROL in.

c. Bekijk de details van de kenmerken.
d. Klik op Save (Opslaan).



Autorisatieprofiel maken

Stap 3. Gebruikersgroep maken.

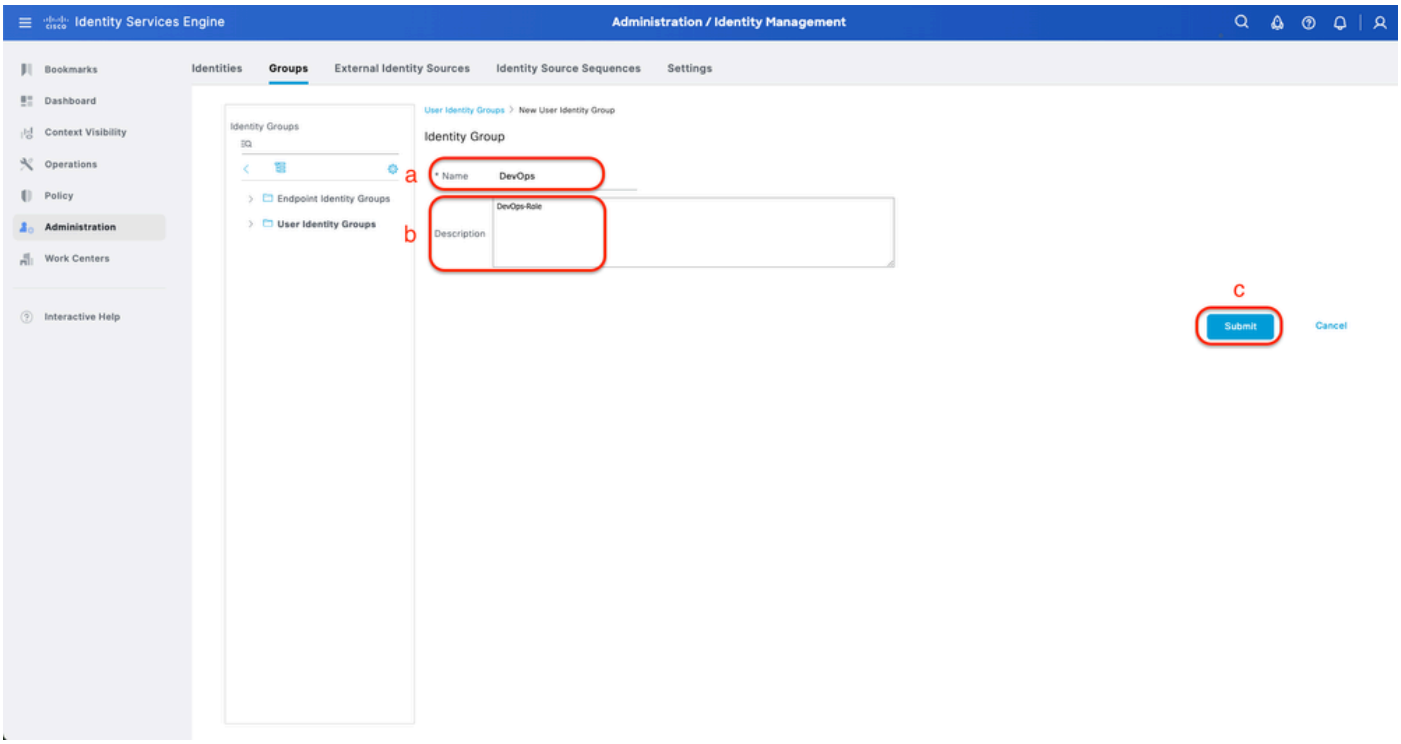
Dit kan worden gedaan via het tabblad Beheer > Identiteitsbeheer > Groepen > Gebruikersidentiteitsgroepen.

Procedure

a. Klik op Add en definieer de naam van de identiteitsgroep

b. (Optioneel) Definieer de beschrijving.

c. Klik op Verzenden.



Gebruikersidentiteitsgroep maken

Stap 4. Lokale gebruiker maken.

Dit kan worden gedaan via het tabblad Beheer > Identity Management > Identity > User.

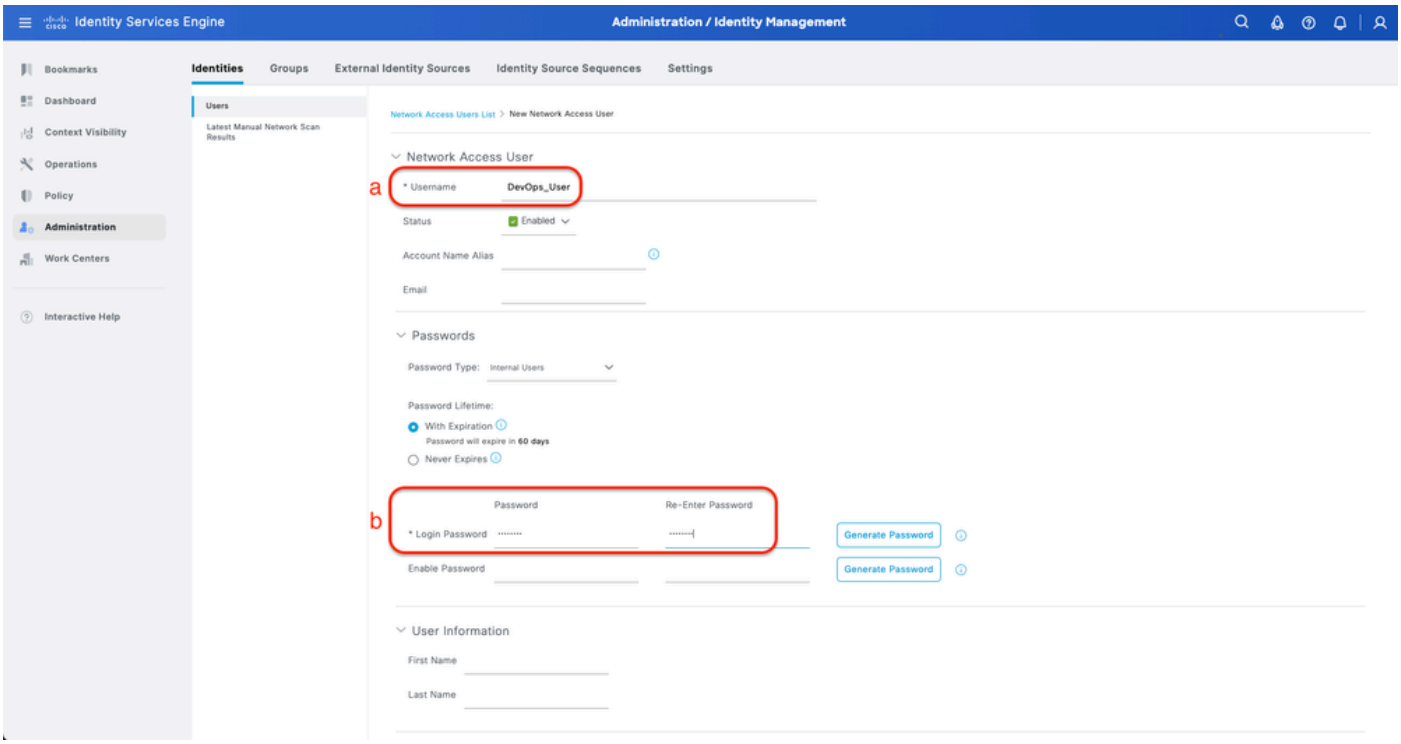
Procedure

a. Klik op Add en definieer de gebruikersnaam.

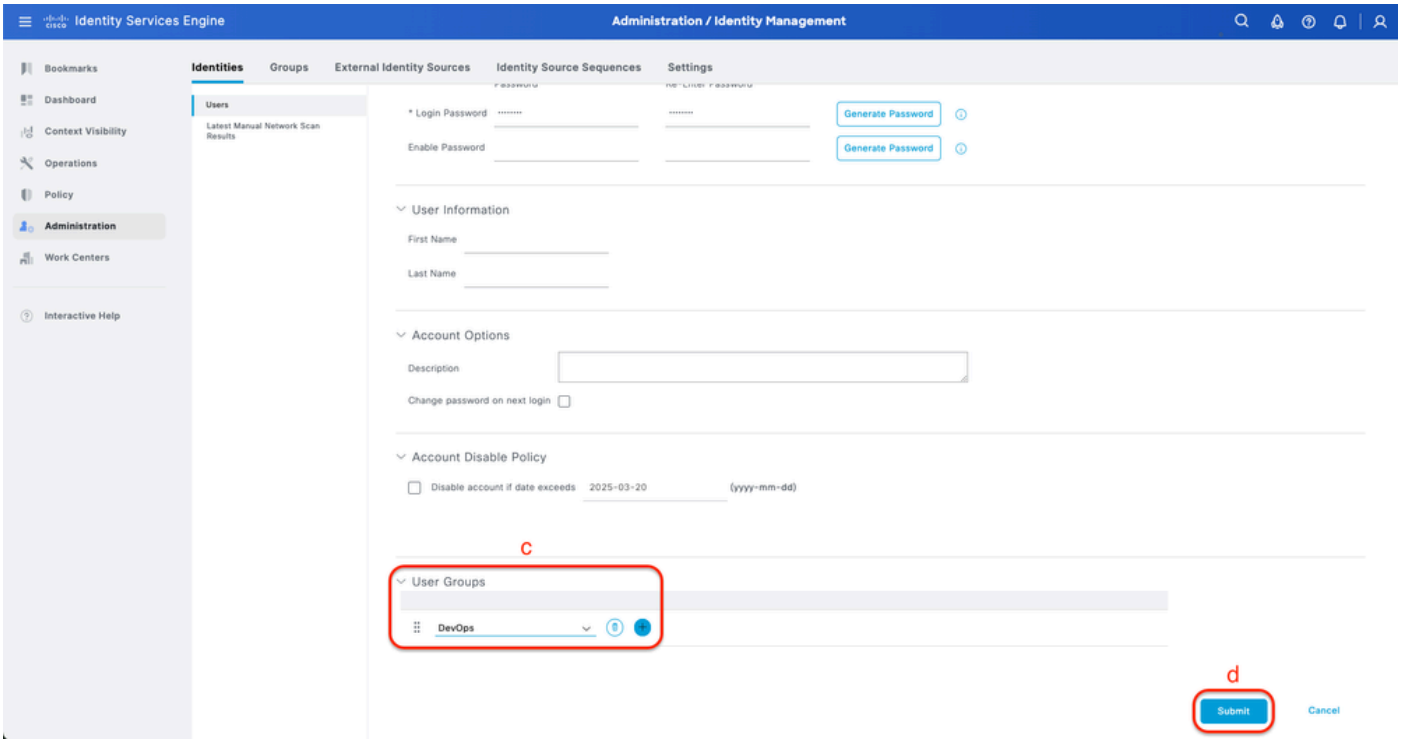
b. Stel het inlogwachtwoord in.

c. Voeg de gebruiker toe aan de verwante gebruikersgroep.

d. Klik op Verzenden.



Lokale gebruiker maken 1-2



Lokale gebruiker maken 2-2

Stap 5. (optioneel) Voeg RADIUS-beleidsset toe.

Dit kan worden gedaan via het tabblad Policy > Policy Sets.

Procedure

a. Klik op Acties en kies (Nieuwe rij hierboven invoegen).

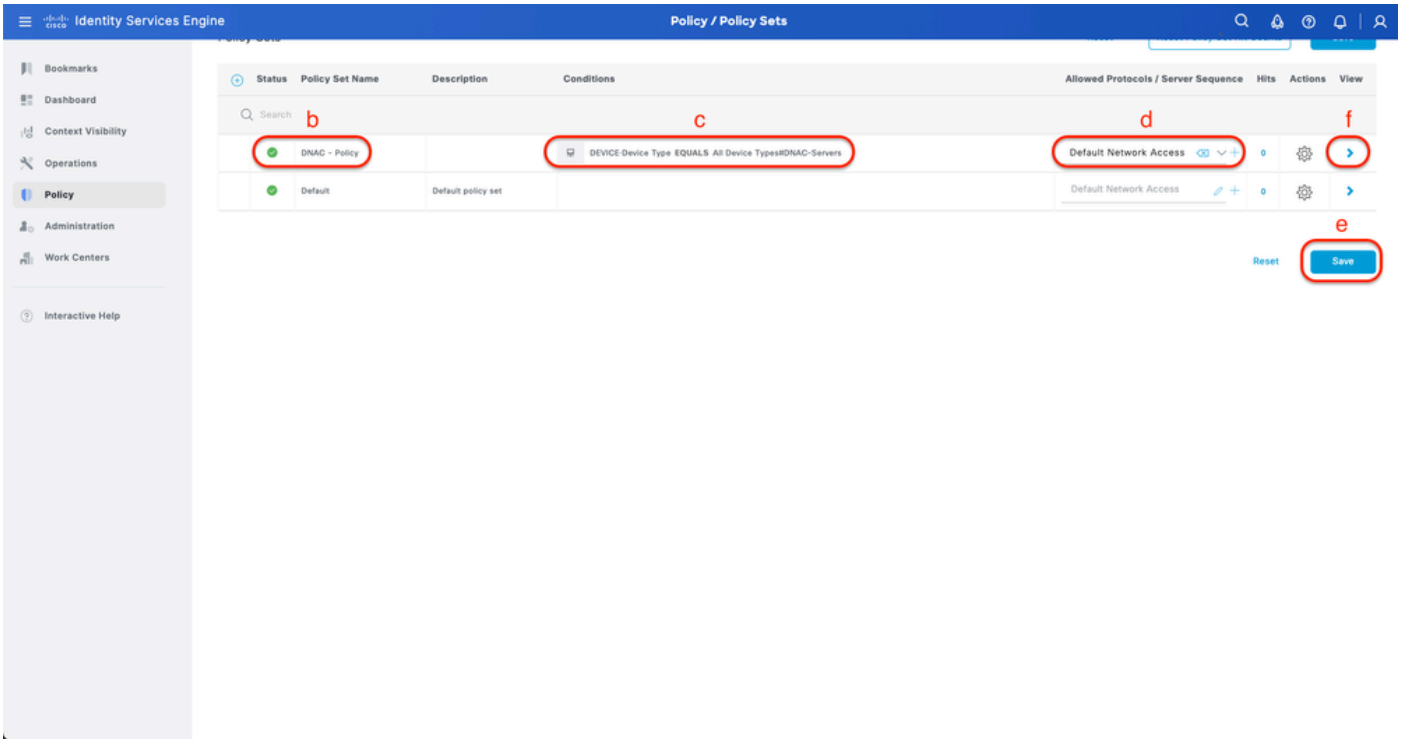
b. Bepaal de naam van de beleidsset.

c. Stel de voorwaarde voor de beleidsset in om het apparaattype te selecteren dat u eerder hebt gemaakt op (Stap 1 > b).

d. Stel de toegestane protocollen in.

e. Klik op Save (Opslaan).

f. Klik op (>) Beleidsweergave om verificatie- en autorisatieregels te configureren.



RADIUS-beleidsset toevoegen

Stap 6. Configureer het RADIUS-verificatiebeleid.

Dit kan worden gedaan via het tabblad Beleid > Beleidssets > Klik (>).

Procedure

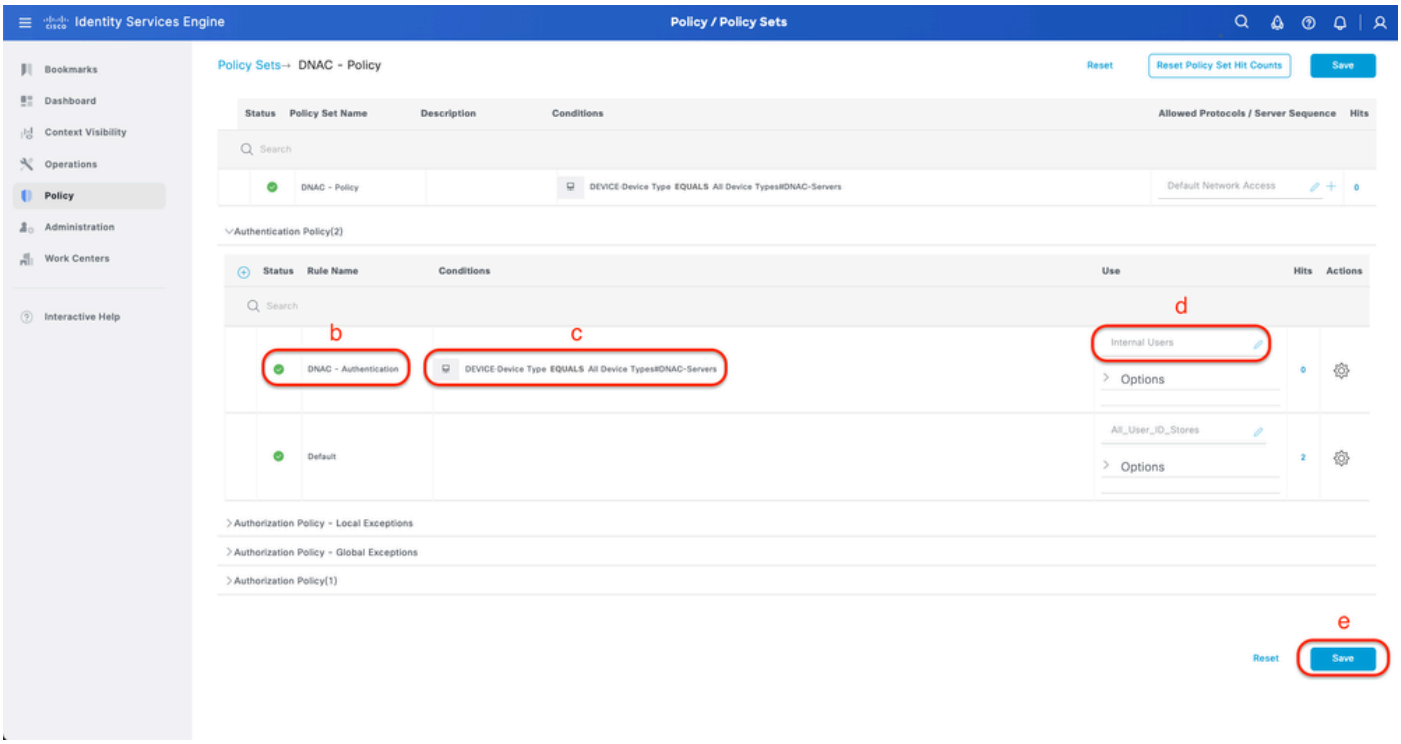
a. Klik op Acties en kies (Nieuwe rij hierboven invoegen).

b. Definieer de naam van het verificatiebeleid.

c. Stel de voorwaarde voor het verificatiebeleid in en selecteer het apparaattype dat u eerder hebt gemaakt (Stap 1 > b).

d. Stel het gebruik van het verificatiebeleid voor de identiteitsbron in.

e. Klik op Save (Opslaan).



RADIUS-verificatiebeleid toevoegen

Stap 7. Configureer het RADIUS-autorisatiebeleid.

Dit kan worden gedaan via het tabblad Beleid > Beleidssets> Klik op (>).

Deze stap om een autorisatiebeleid te maken voor elke gebruikersrol:

- SUPER-ADMIN-ROL
- NETWERKBEHEERROL
- DevOps-Role

Procedure

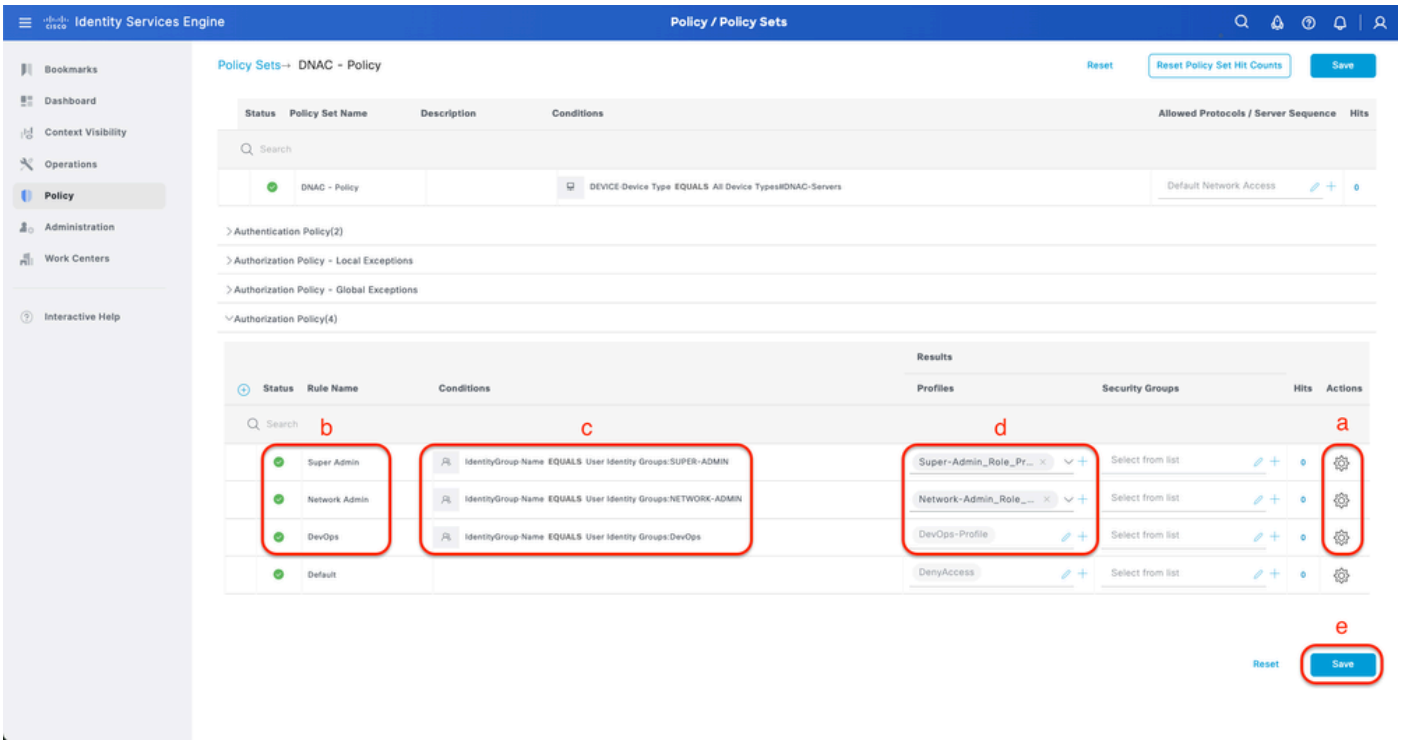
a. Klik op Acties en kies (Nieuwe rij hierboven invoegen).

b. Definieer de naam van het autorisatiebeleid.

c. Stel de voorwaarde voor het autorisatiebeleid in en selecteer de gebruikersgroep die u in hebt gemaakt (Stap 3).

d. Stel de resultaten/profielen van het autorisatiebeleid in en selecteer het autorisatieprofiel dat u hebt gemaakt in (Stap 2).

e. Klik op Save (Opslaan).



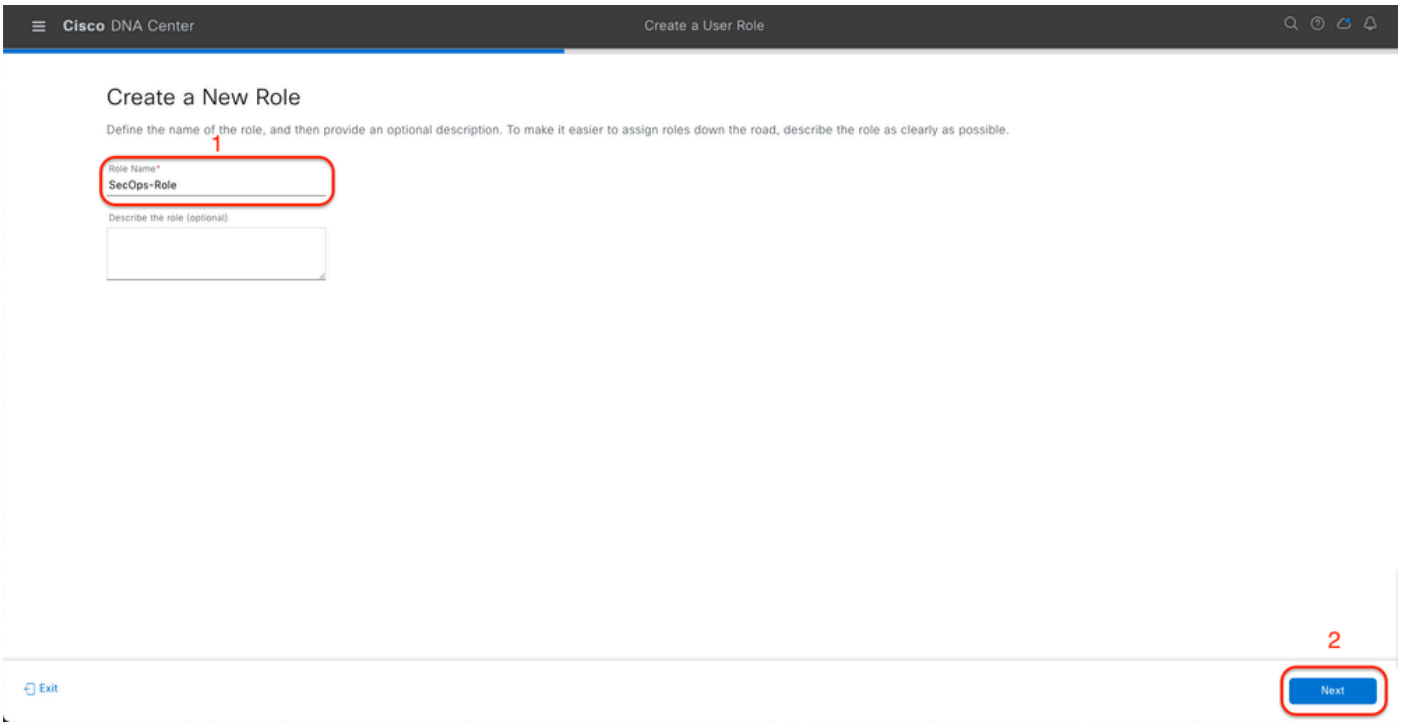
Toepassingsbeleid toevoegen

(Optie2) DNAC externe verificatie configureren met behulp van TACACS+

Stap 1. (optioneel) Definieer een aangepaste rollen.
Configureer uw aangepaste rollen die aan uw eis voldoen, in plaats daarvan kunt u de standaard gebruikersrollen gebruiken. Dit kan worden gedaan via het tabblad Systeem > Gebruikers & rollen > Role Based Access Control.

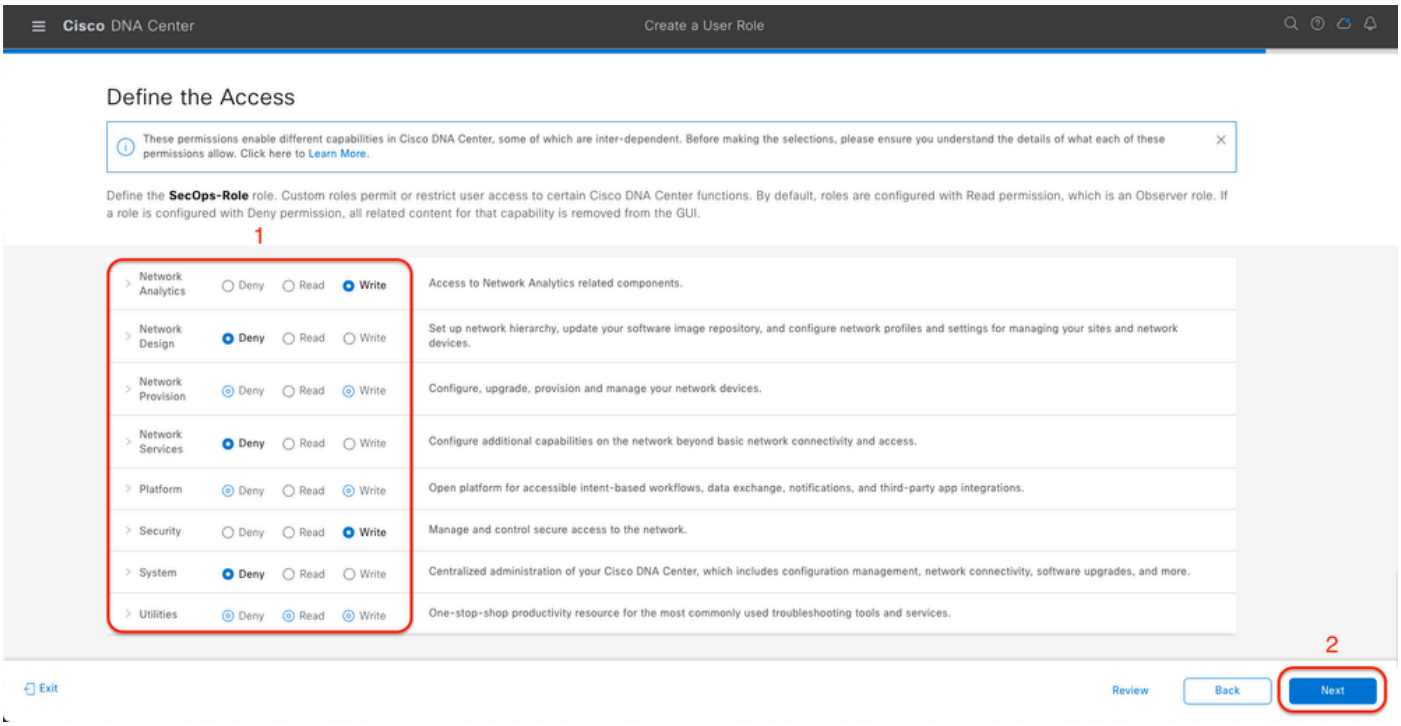
Procedure

a. Creëer een nieuwe rol.



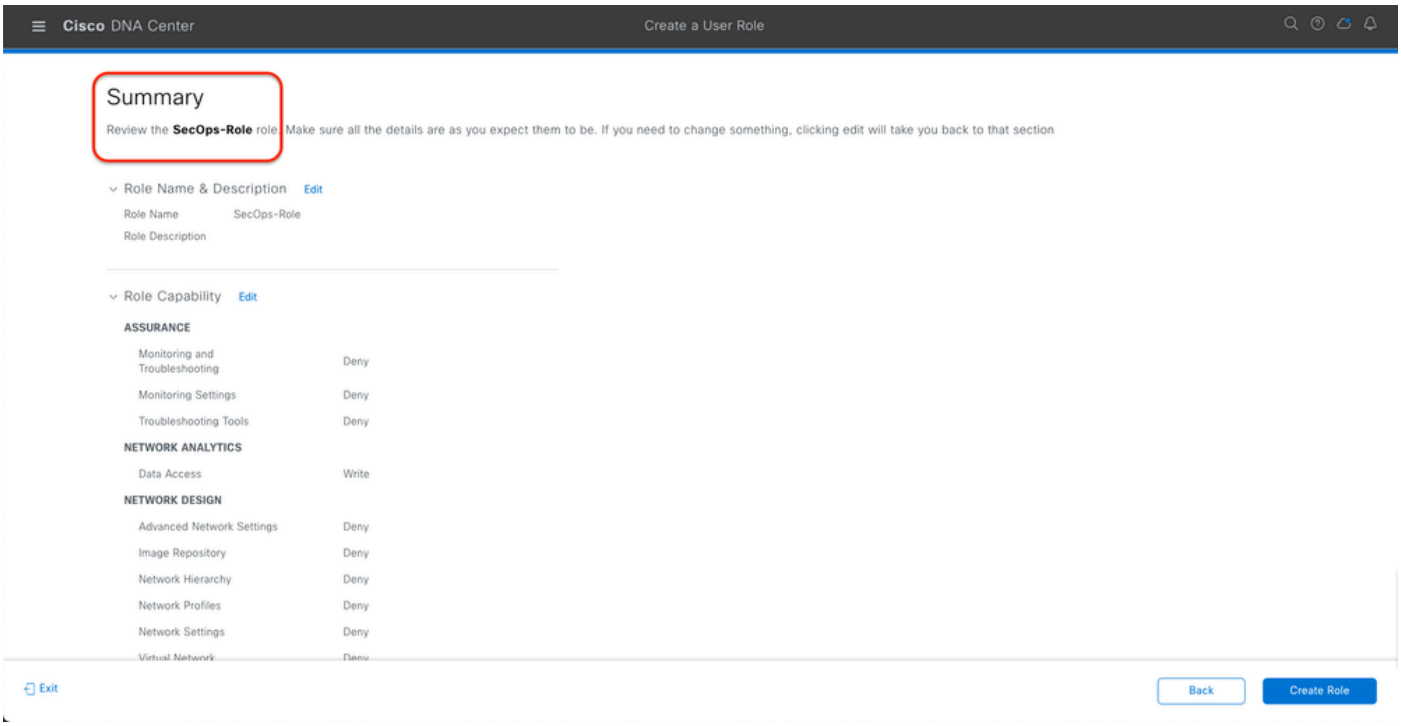
SecOPS Rol Naam

b. Definieer de toegang.

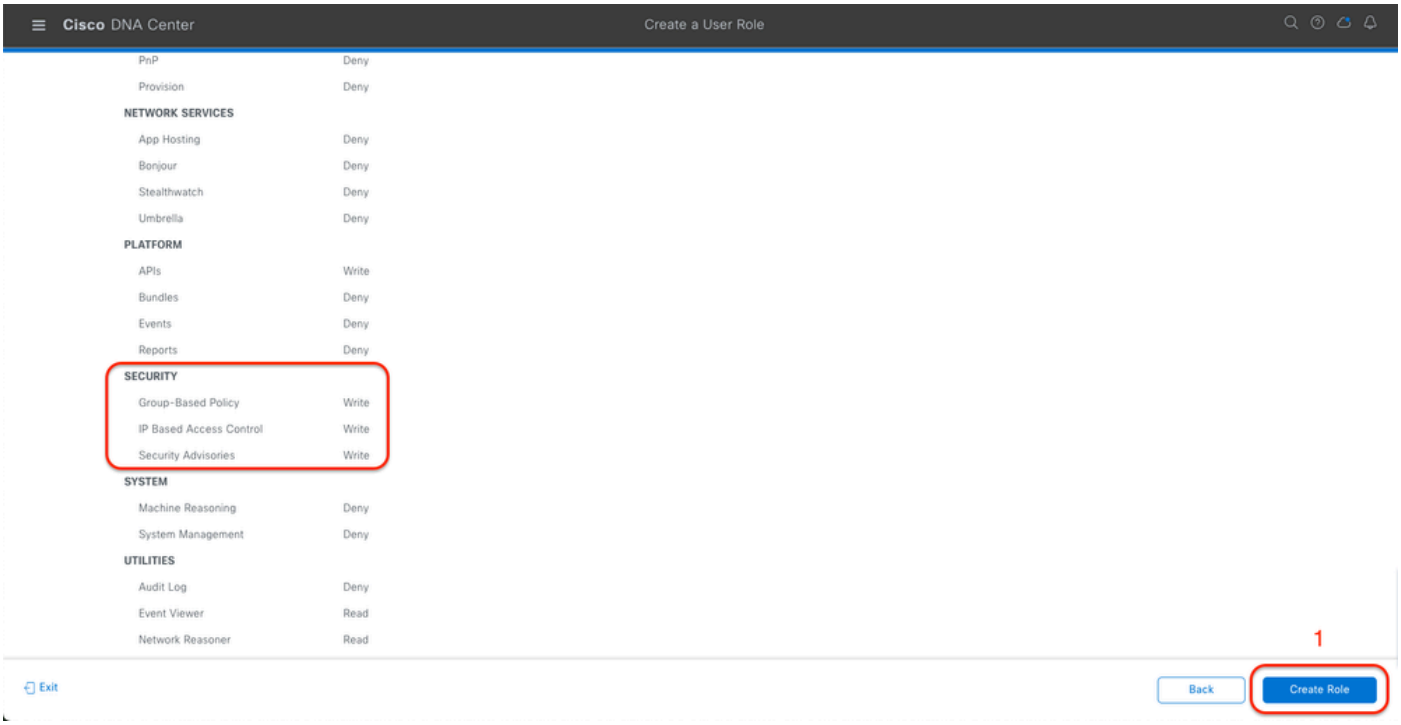


SecOPS roltoegang

c. Maak de nieuwe rol aan.



Samenvatting van SecOps-rol



Rol van selecties bekijken en maken

Stap 2. Configureer externe verificatie met TACACS+.
Dit kan worden gedaan via het tabblad Systeem > Gebruikers & rollen > Externe verificatie.

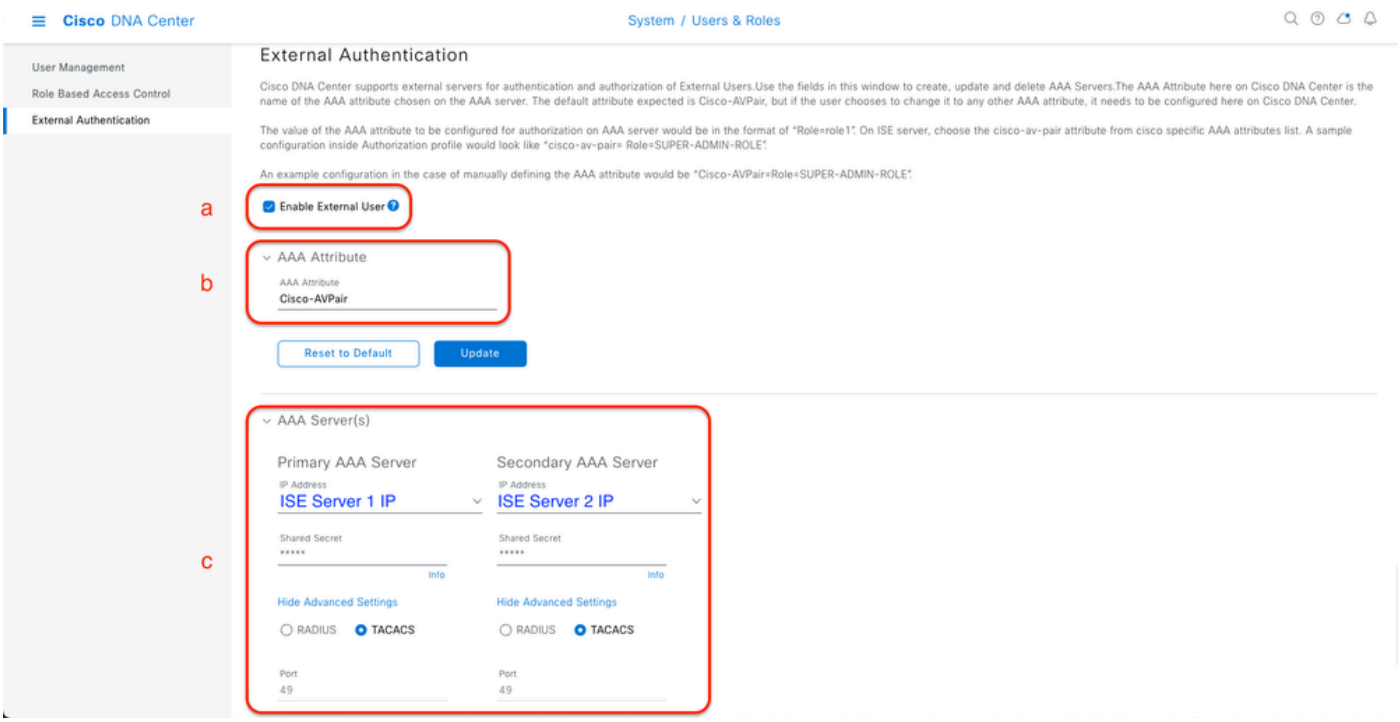
a. Als u externe verificatie in Cisco DNA Center wilt inschakelen, schakelt u het aanvinkvakje Externe gebruiker inschakelen in.

b. Stel de AAA-kenmerken in.

Voer Cisco AVPair in het veld AAA-kenmerken in.

c. (Optioneel) Configureer de primaire en secundaire AAA-server.

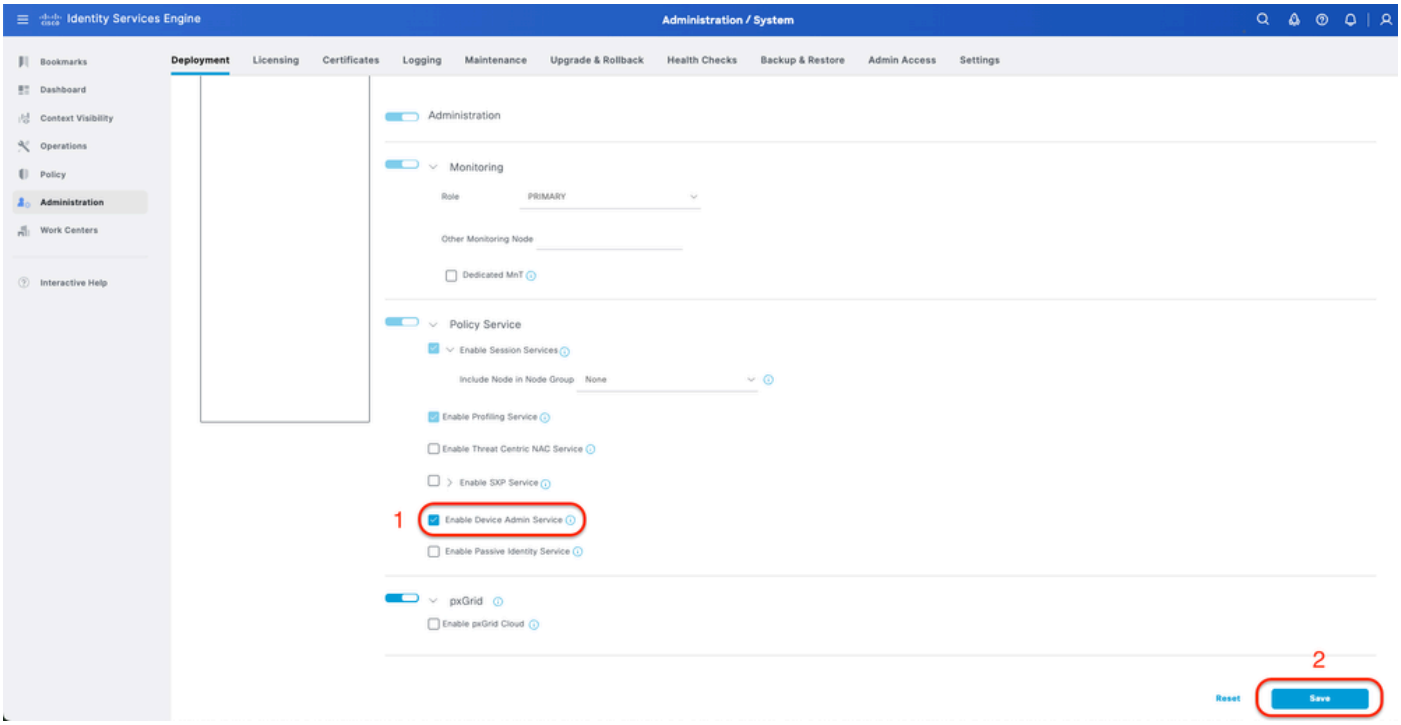
Zorg ervoor dat het TACACS+-protocol ten minste is ingeschakeld op de primaire AAA-server, of op zowel de primaire als de secundaire server.



Configuratiestappen (TACACS+) externe verificatie

(Optie 2) ISE-configuratie voor TACACS+

Stap 1. Schakel de Apparaatbeheerservice in.
Dit kan worden gedaan via het tabblad Beheer > Systeem > Implementatie > Bewerken (ISE-PSN-knooppunt) > Controleren of Apparaatbeheerservice is ingeschakeld.



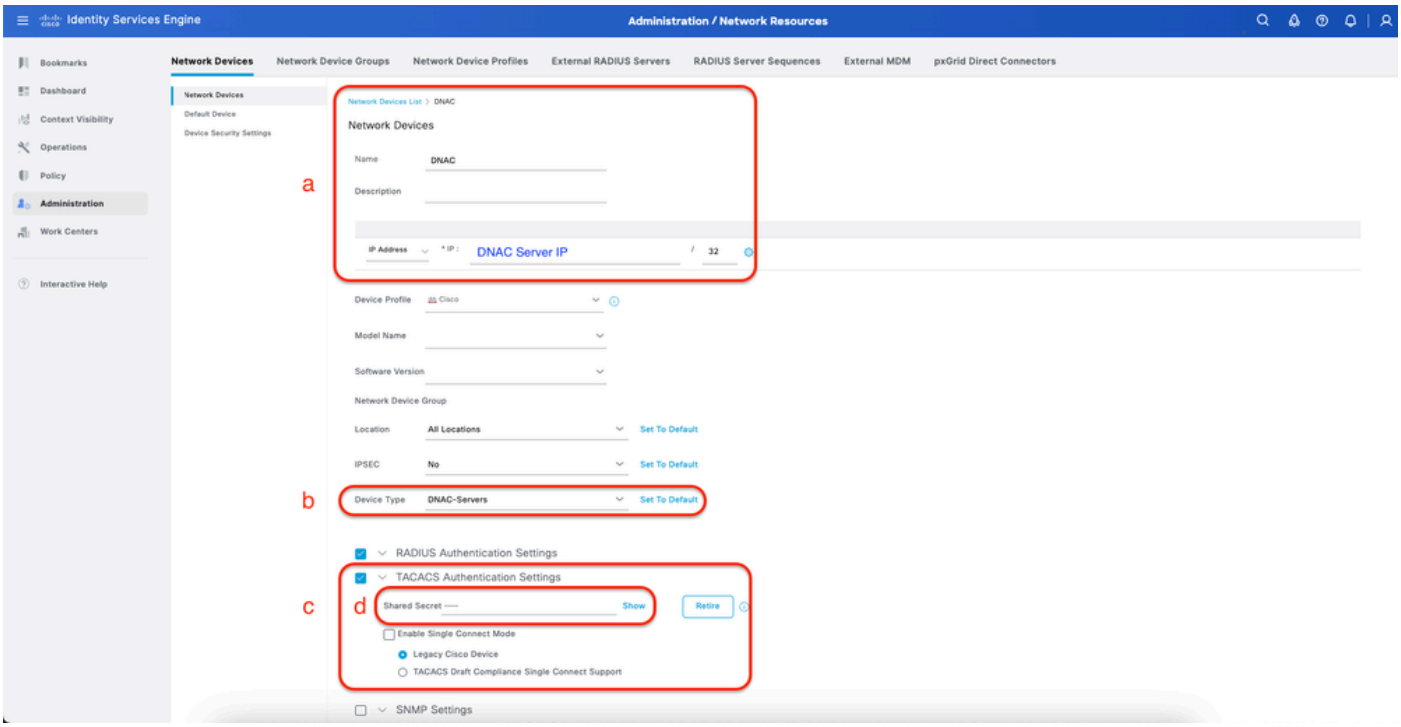
Service voor apparaatbeheer inschakelen

Stap 2. Voeg DNAC-server toe als netwerkapparaat op ISE.

Dit kan worden gedaan via het tabblad Beheer > Netwerkbronnen > Netwerkapparaten.

Procedure

a. Definieer (DNAC) naam en IP van netwerkapparaat.
b. (Optioneel) Apparaattype classificeren voor voorwaarde beleidsinstelling.
c. Schakel TACACS+ verificatie-instellingen in.
d. Stel TACACS+ gedeeld geheim in.



ISE-netwerkapparaat (NAC) voor TACACS+

Stap 3. Maak TACACS+ profielen voor elke DNAC rol.

Dit kan worden gedaan via het tabblad Werkcentra > Apparaatbeheer > Beleidselementen > Resultaten > TACACS-profielen.

Opmerking: 3x TACACS+ profielen maken, één voor elke gebruikersrol.

Procedure

a. Klik op Add en definieer de naam van het TACACS-profiel.

b. Klik op het tabblad Raw View.

c. Voer de Cisco-AVPair=ROL= in en vul de juiste gebruikersrol in.

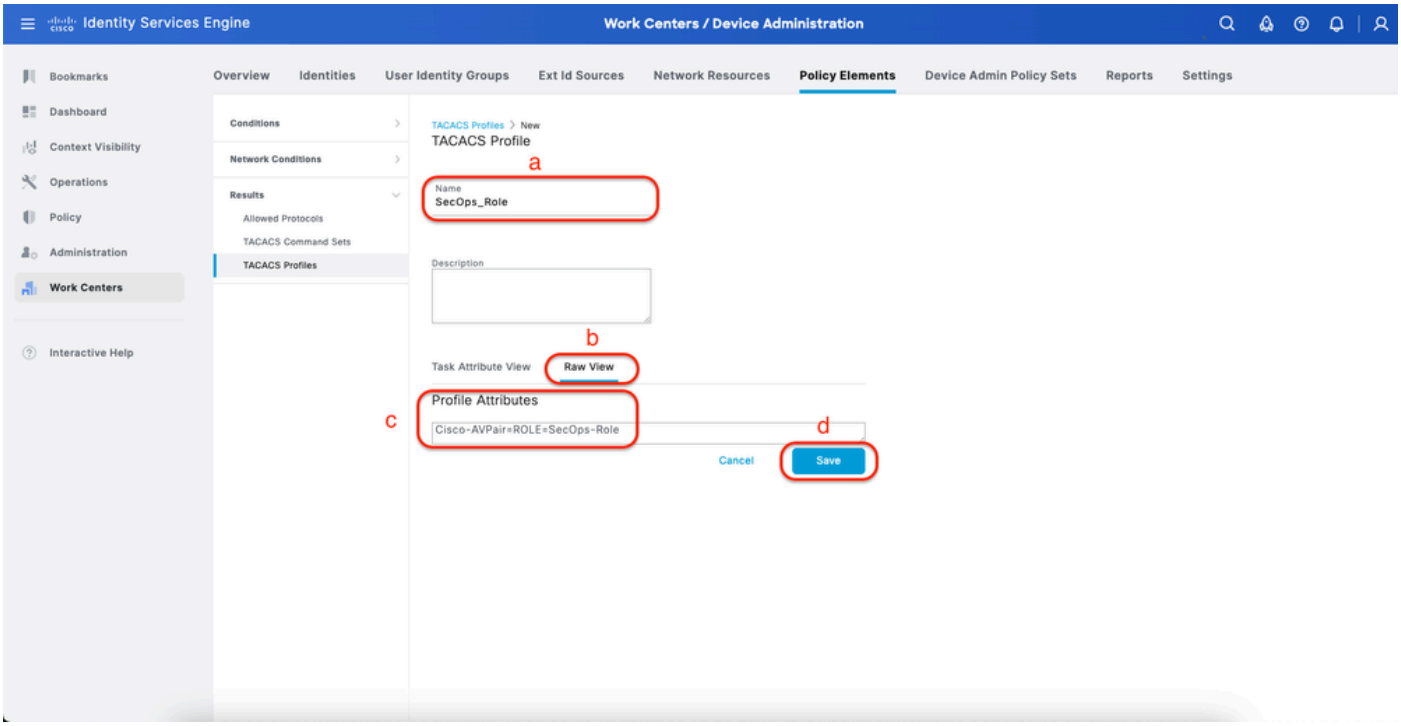
- Voer voor de gebruikersrol (SecOps-Role) Cisco-AVPair=ROLE=SecOps-Role in.

- Voer voor de gebruikersrol (NETWORK-ADMIN-ROL) Cisco-AVPair=ROLE=NETWORK-ADMIN-ROL in.
- Voer voor de gebruikersrol (SUPER-ADMIN-ROL) Cisco-AVPair=ROLE=SUPER-ADMIN-ROL in.

Opmerking: Vergeet niet dat AVPair value (Cisco-AVPair=ROLE=) een hoofdlettergevoeligheid is en ervoor zorgt dat deze overeenkomt met de DNAC User Role.

---

d. Klik op Save (Opslaan).



TACACS-profiel maken (secOps_Role)

Stap 4. Gebruikersgroep maken.

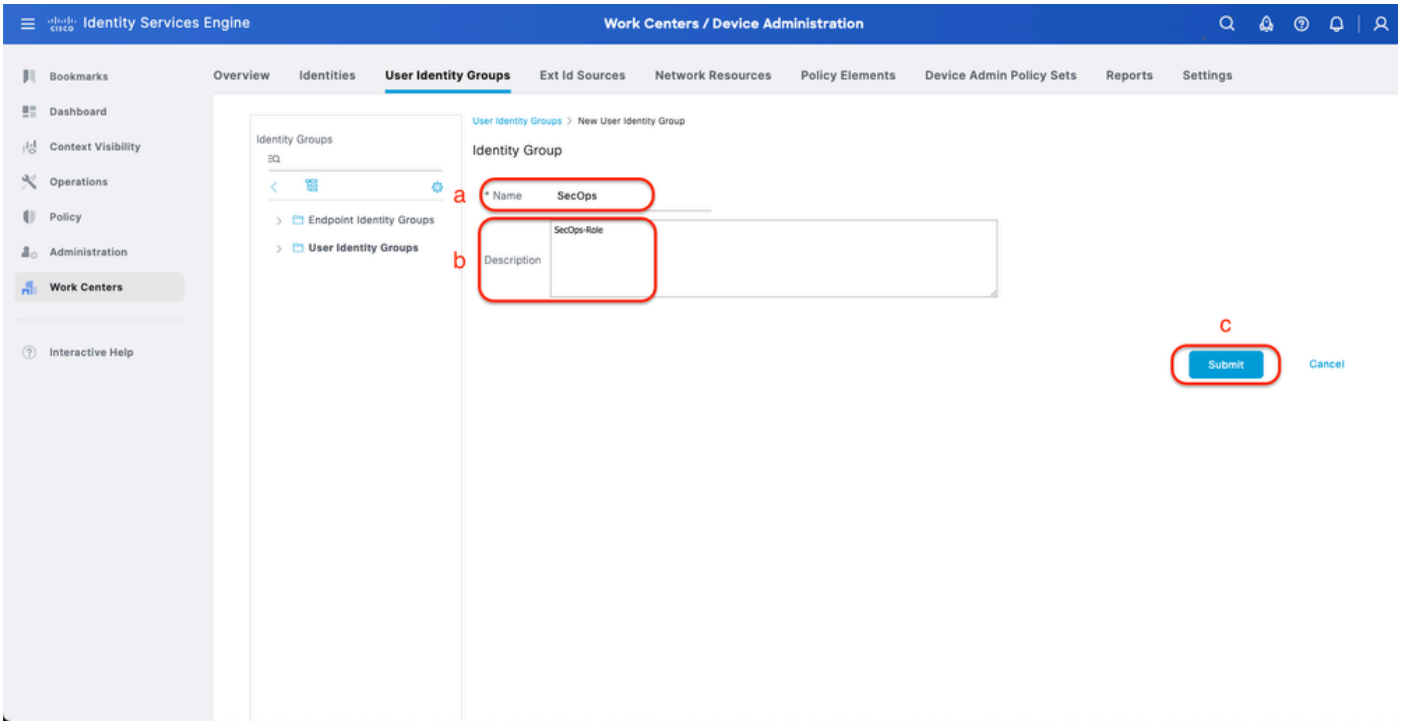
Dit kan worden gedaan via het tabblad Workcenters > Apparaatbeheer > Gebruikersidentiteitsgroepen.

Procedure

a. Klik op Add en definieer de naam van de identiteitsgroep.

b. (Optioneel) Definieer de beschrijving.

c. Klik op Verzenden.



Gebruikersidentiteitsgroep maken

Stap 5. Lokale gebruiker maken.

Dit kan worden gedaan via het tabblad Work Centers > Apparaatbeheer > Identiteiten > Gebruikers.

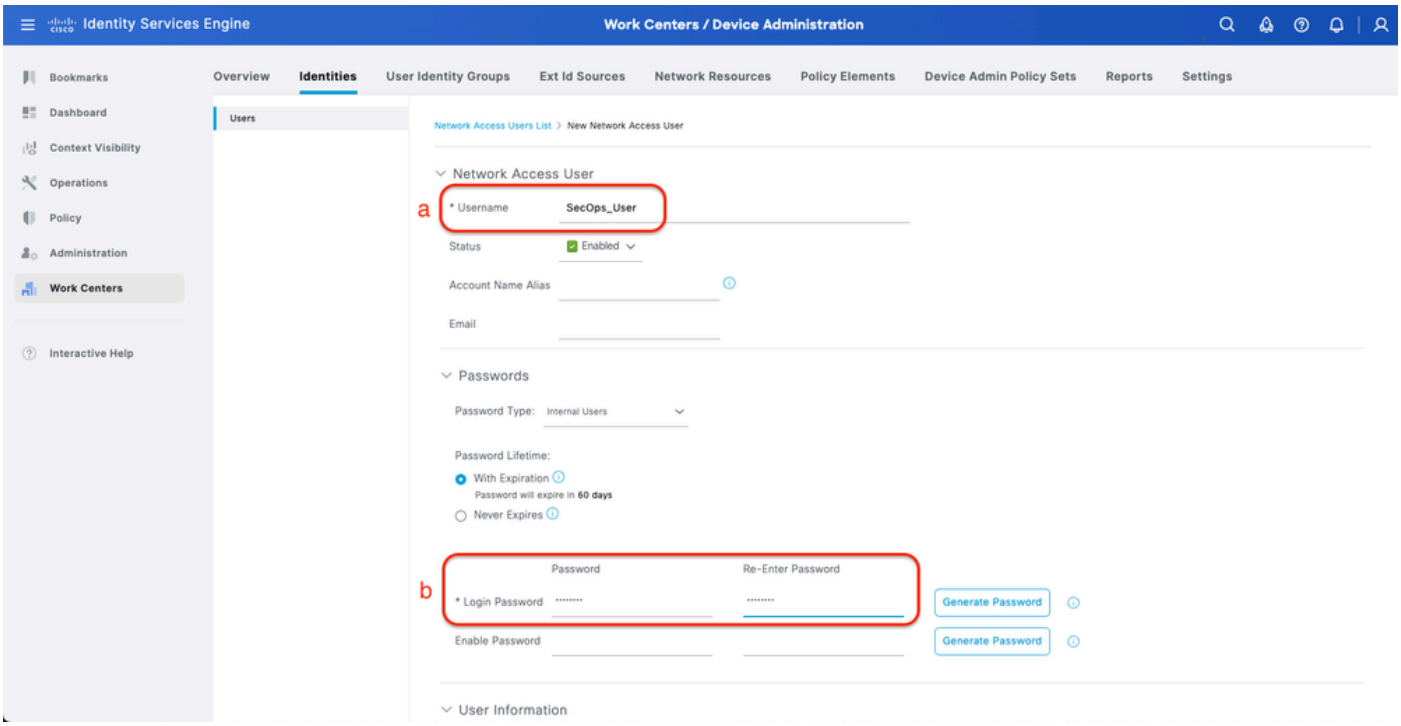
Procedure

a. Klik op Add en definieer de gebruikersnaam.

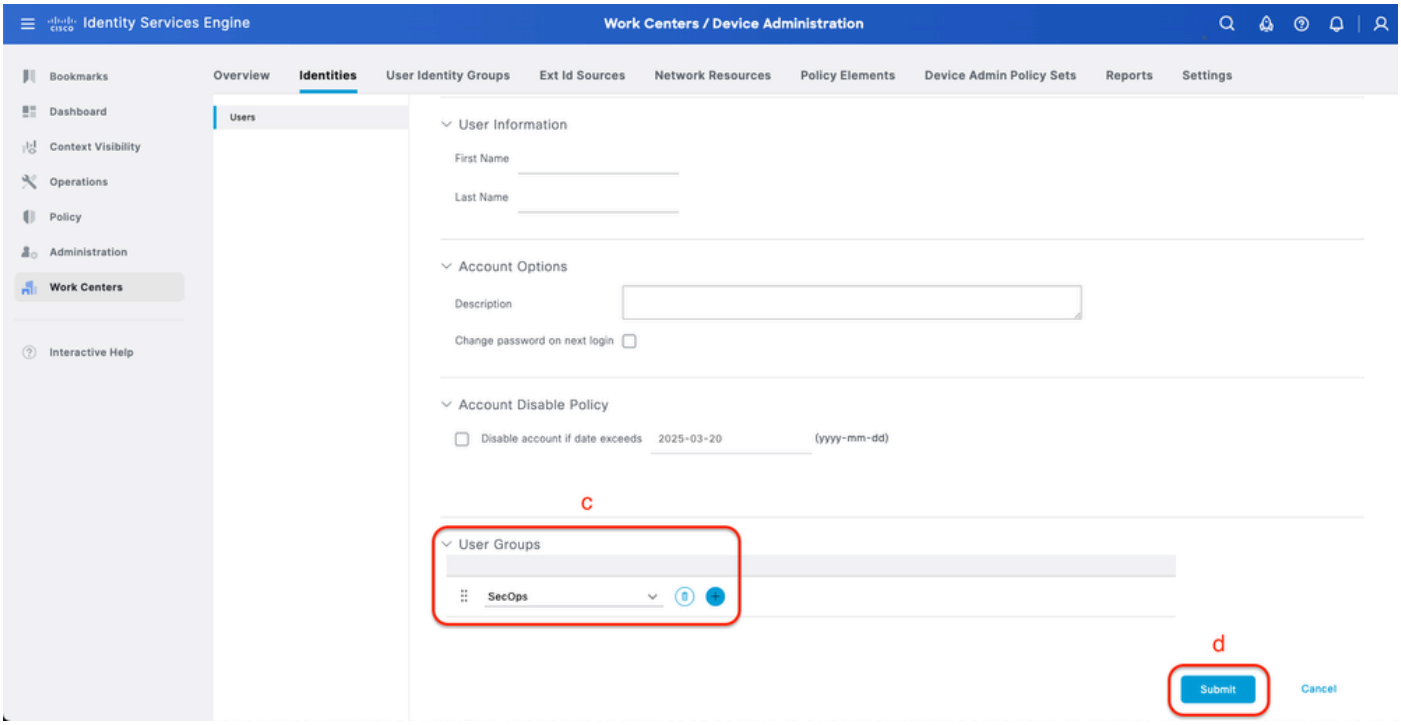
b. Stel het inlogwachtwoord in.

c. Voeg de gebruiker toe aan de verwante gebruikersgroep.

d. Klik op Verzenden.



Lokale gebruiker maken 1-2



Lokale gebruiker maken 2-2

Stap 6. (optioneel) Voeg een TACACS+ beleidsset toe.

Dit kan worden gedaan via het tabblad Werkcentra > Apparaatbeheer > Apparaatbeheerbeleidssets.

Procedure

a. Klik op Acties en kies (Nieuwe rij hierboven invoegen).

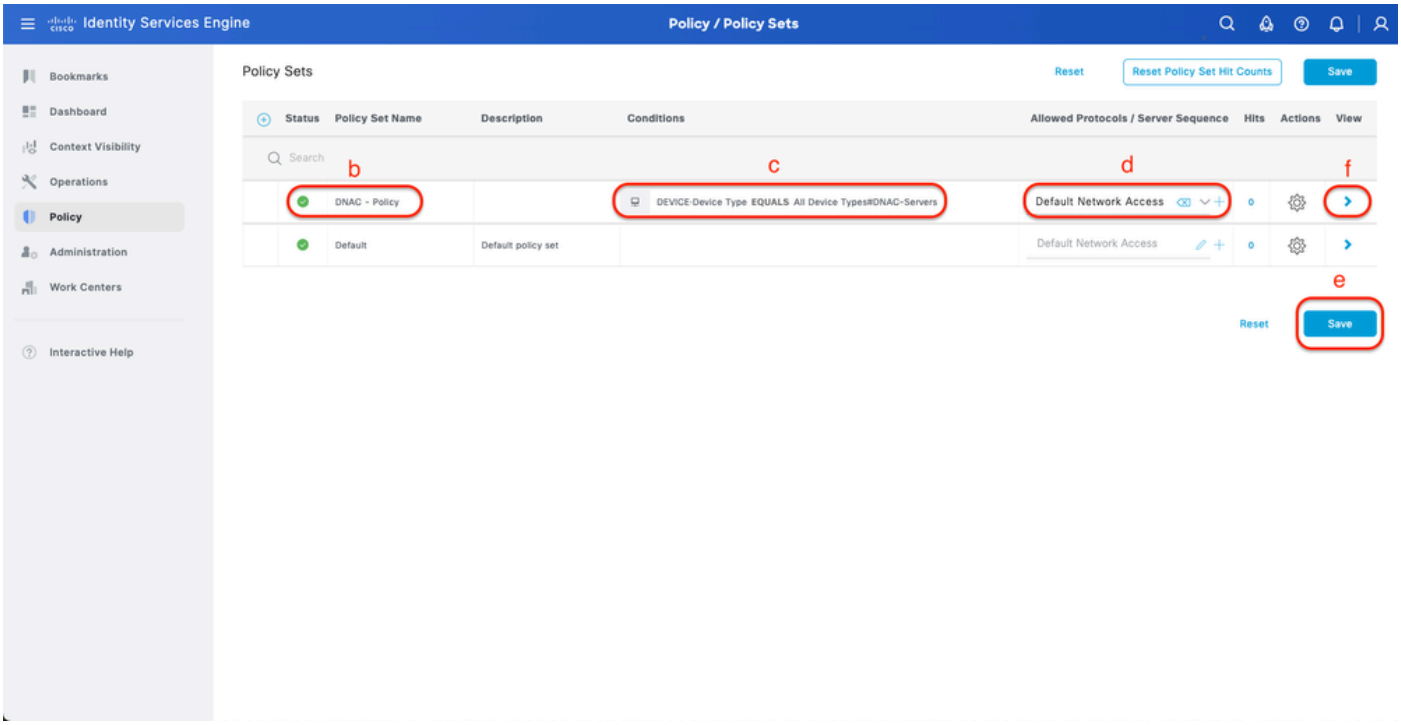
b. Bepaal de naam van de beleidsset.

c. Stel de Policy Set Condition in op Selecteer Apparaattype dat u eerder hebt gemaakt op (Stap 2 > b).

d. Stel de toegestane protocollen in.

e. Klik op Save (Opslaan).

f. Klik op (>) Beleidsweergave om verificatie- en autorisatieregels te configureren.



Reeks TACACS+ beleid toevoegen

Stap 7. Configuratie van het TACACS+-verificatiebeleid.

Dit kan worden gedaan via het tabblad Werkcentra > Apparaatbeheer > Beleidssets voor Apparaatbeheer > Klik op (>).

Procedure

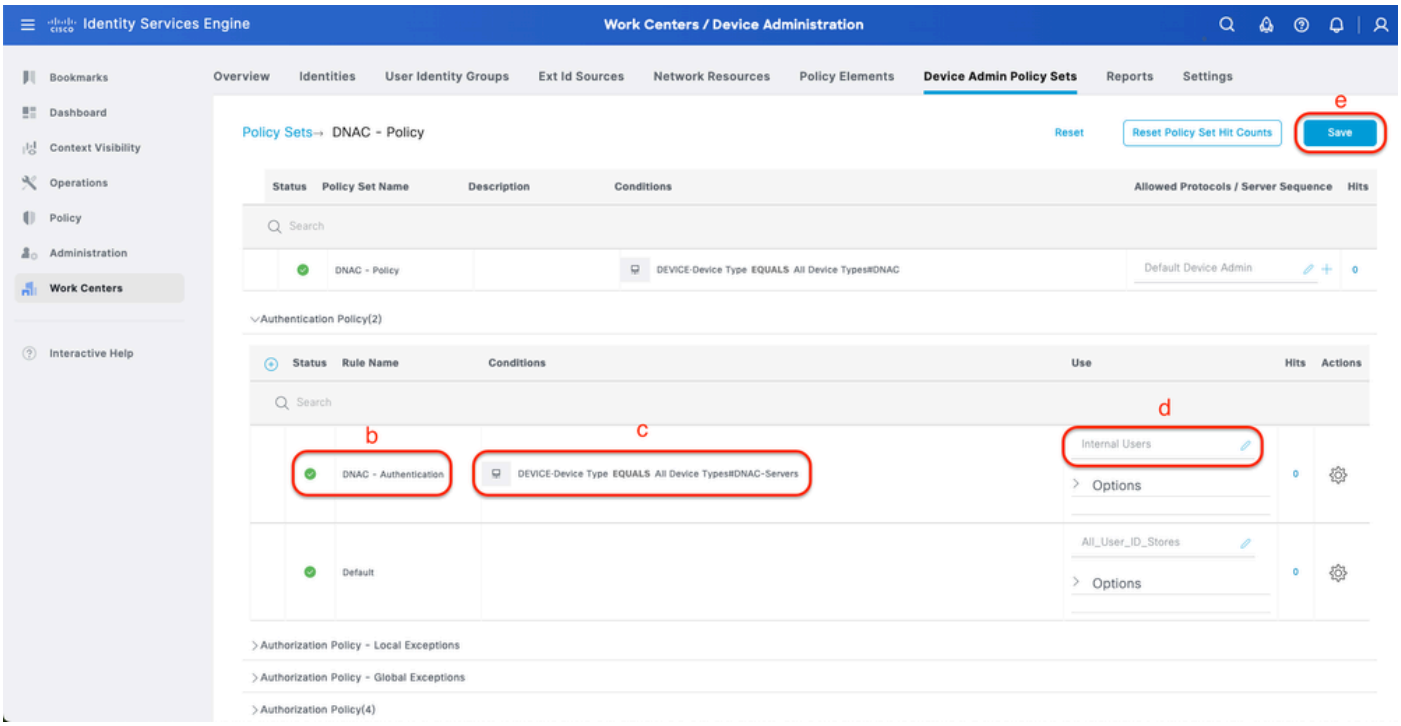
a. Klik op Acties en kies (Nieuwe rij hierboven invoegen).

b. Definieer de naam van het verificatiebeleid.

c. Stel de voorwaarde voor het verificatiebeleid in en selecteer het apparaattype dat u eerder hebt gemaakt (Stap 2 > b).

d. Stel het gebruik van het verificatiebeleid voor de identiteitsbron in.

e. Klik op Save (Opslaan).



Tacacs+-verificatiebeleid toevoegen

Stap 8. Configureer het beleid voor TACACS+ autorisatie.

Dit kan worden gedaan via het tabblad Workcenters > Apparaatbeheer > Apparaatbeheerbeleidssets > Klik op (>).

Deze stap om een autorisatiebeleid te maken voor elke gebruikersrol:

- SUPER-ADMIN-ROL
- NETWERKBEHEERROL
- Tweede rol

Procedure

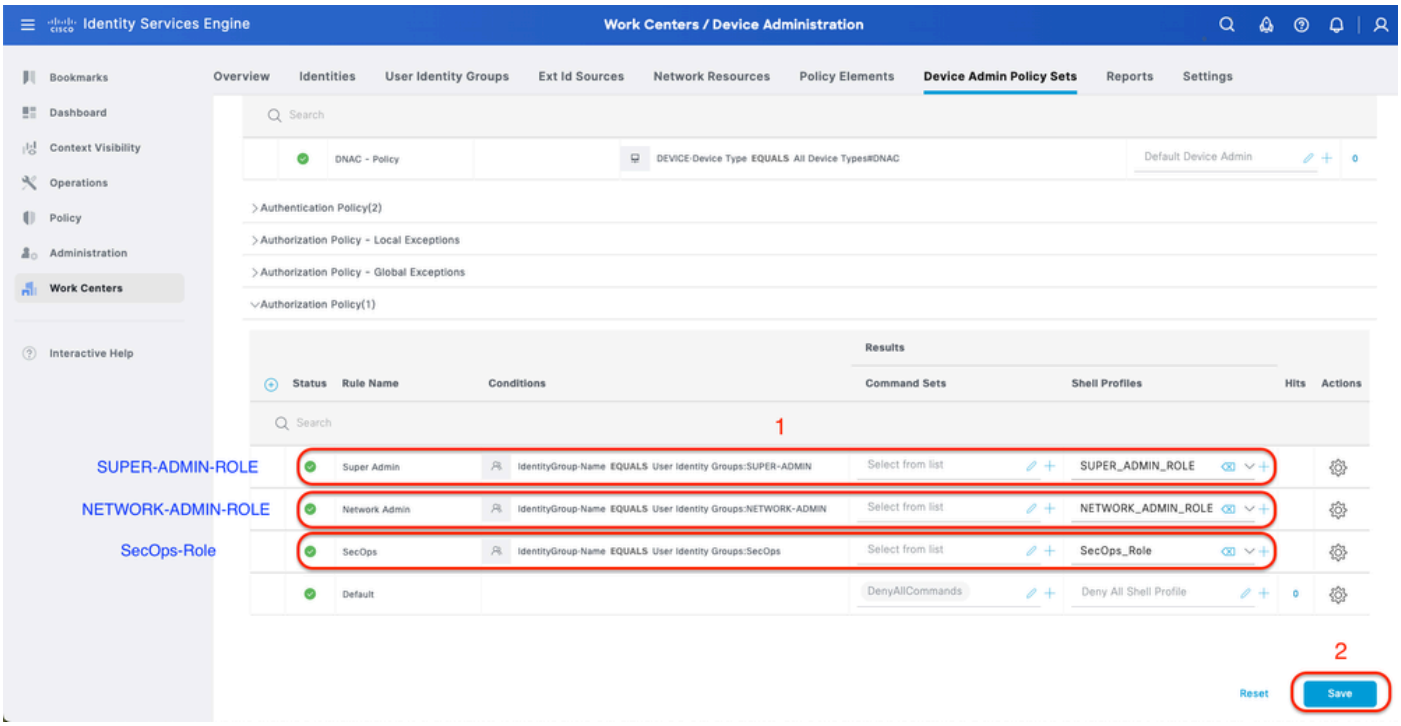
a. Klik op Acties en kies (Nieuwe rij hierboven invoegen).

b. Definieer de naam van het autorisatiebeleid.

c. Stel de voorwaarde voor het autorisatiebeleid in en selecteer de gebruikersgroep die u in hebt gemaakt (Stap 4).

d. Stel het Shell-profiel van het autorisatiebeleid in en selecteer TACACS-profiel dat u in (Stap 3) hebt gemaakt.

e. Klik op Save (Opslaan).

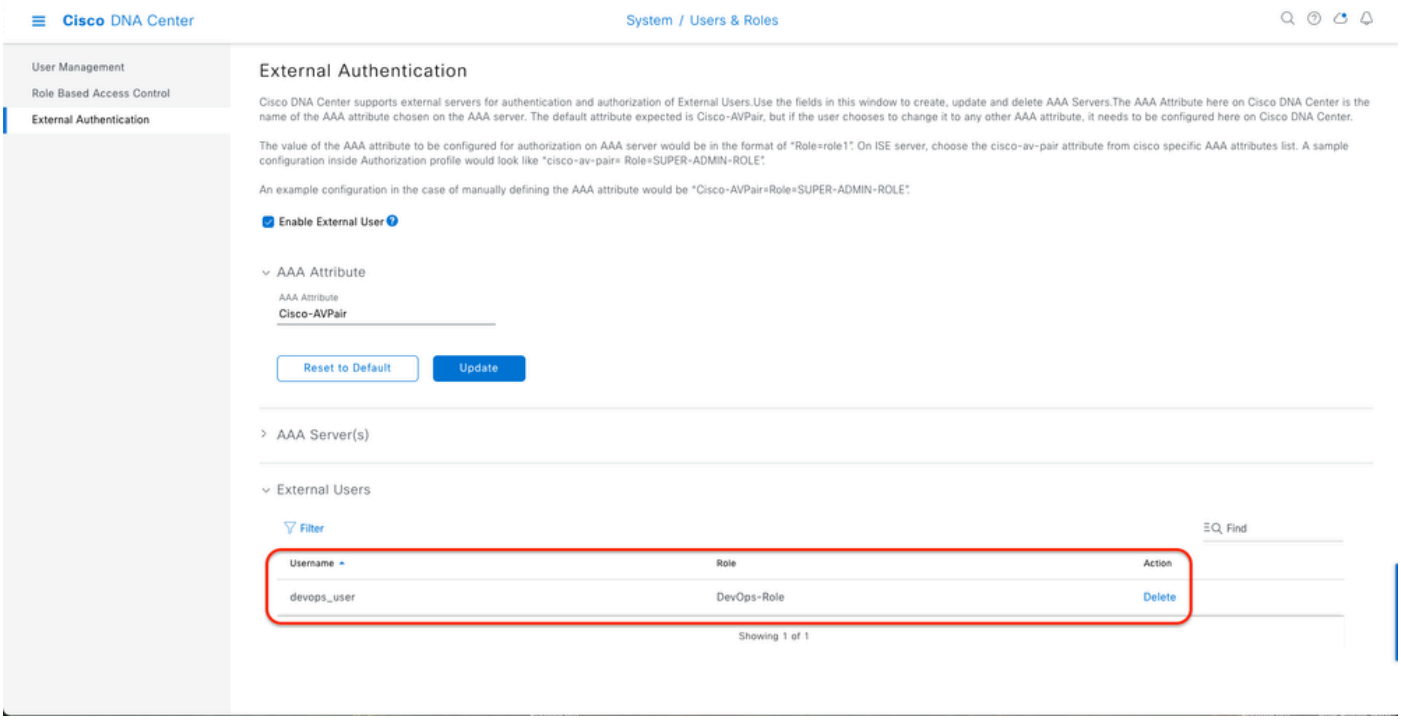


Toepassingsbeleid toevoegen

Verifiëren

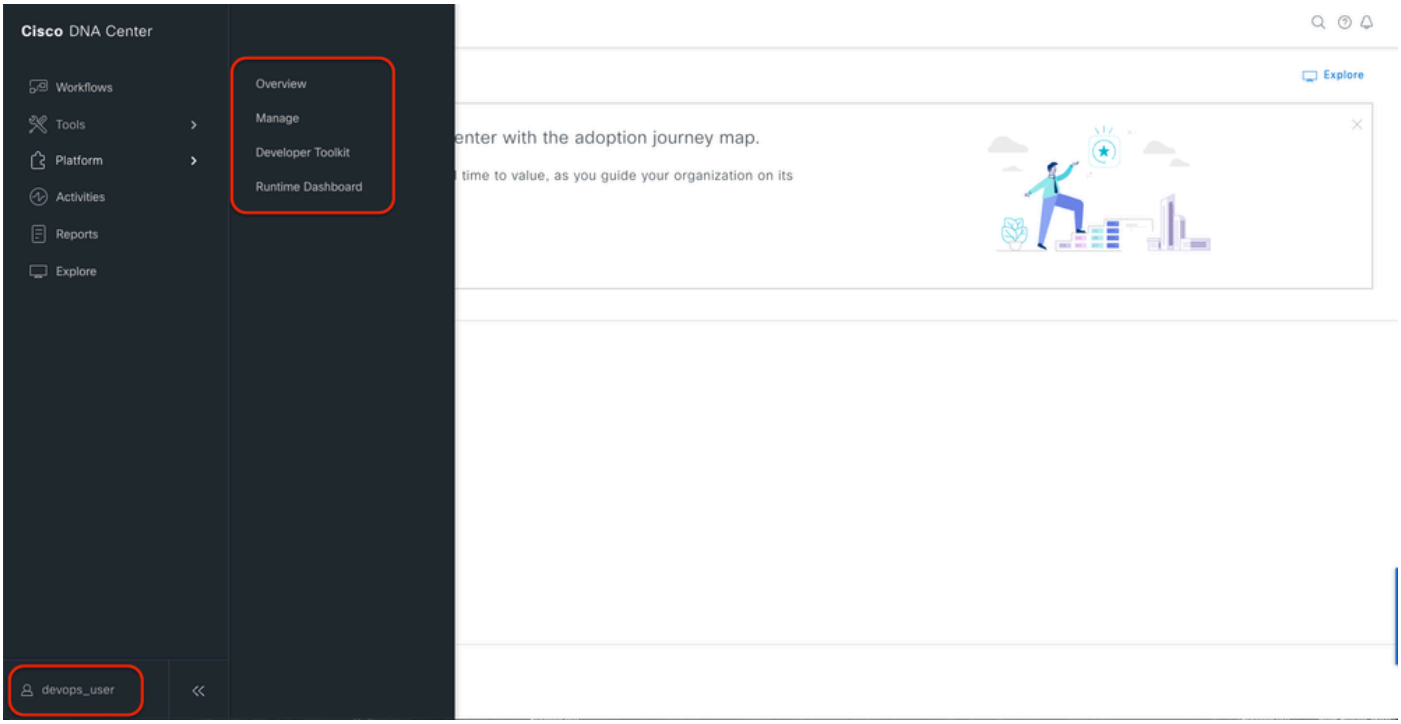
Controleer de RADIUS-configuratie

1- DNAC - Display Externe Gebruikers Systeem > Gebruikers & Rollen > Externe Verificatie > Externe Gebruikers.
U kunt de lijst bekijken van externe gebruikers die voor het eerst via RADIUS zijn aangemeld. De informatie die wordt weergegeven omvat hun gebruikersnamen en rollen.



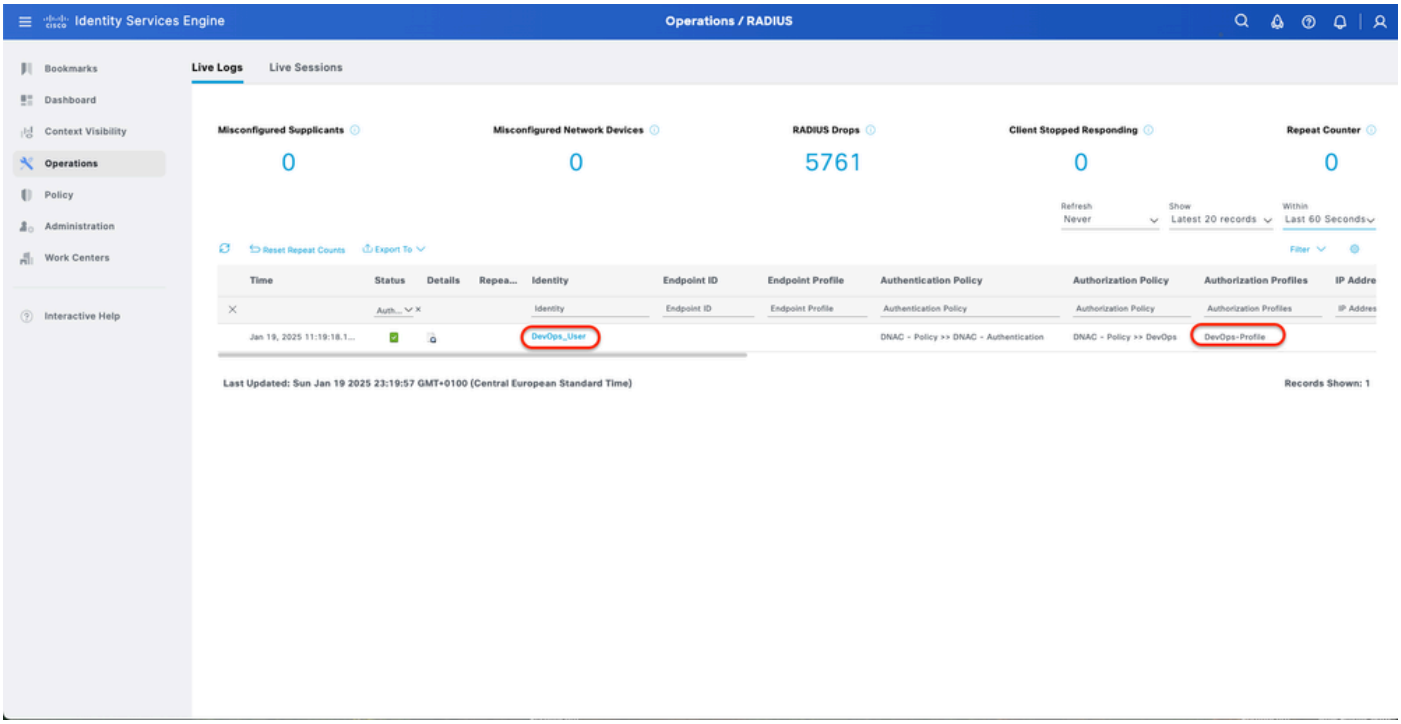
Externe gebruikers

2. DNAC - Bevestig de toegang van gebruikers.



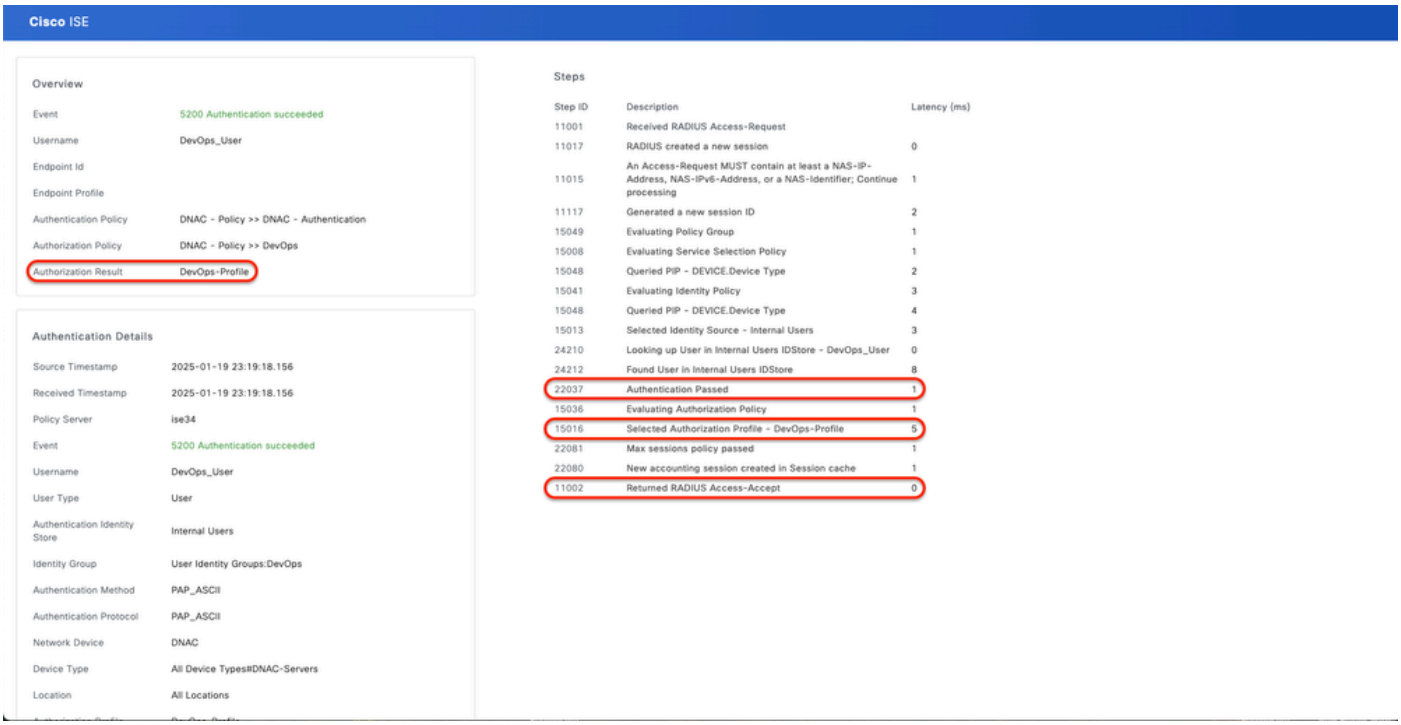
Beperkte gebruikerstoegang

3.a ISE - RADIUS Live-logs Operations > RADIUS > Live-logs.

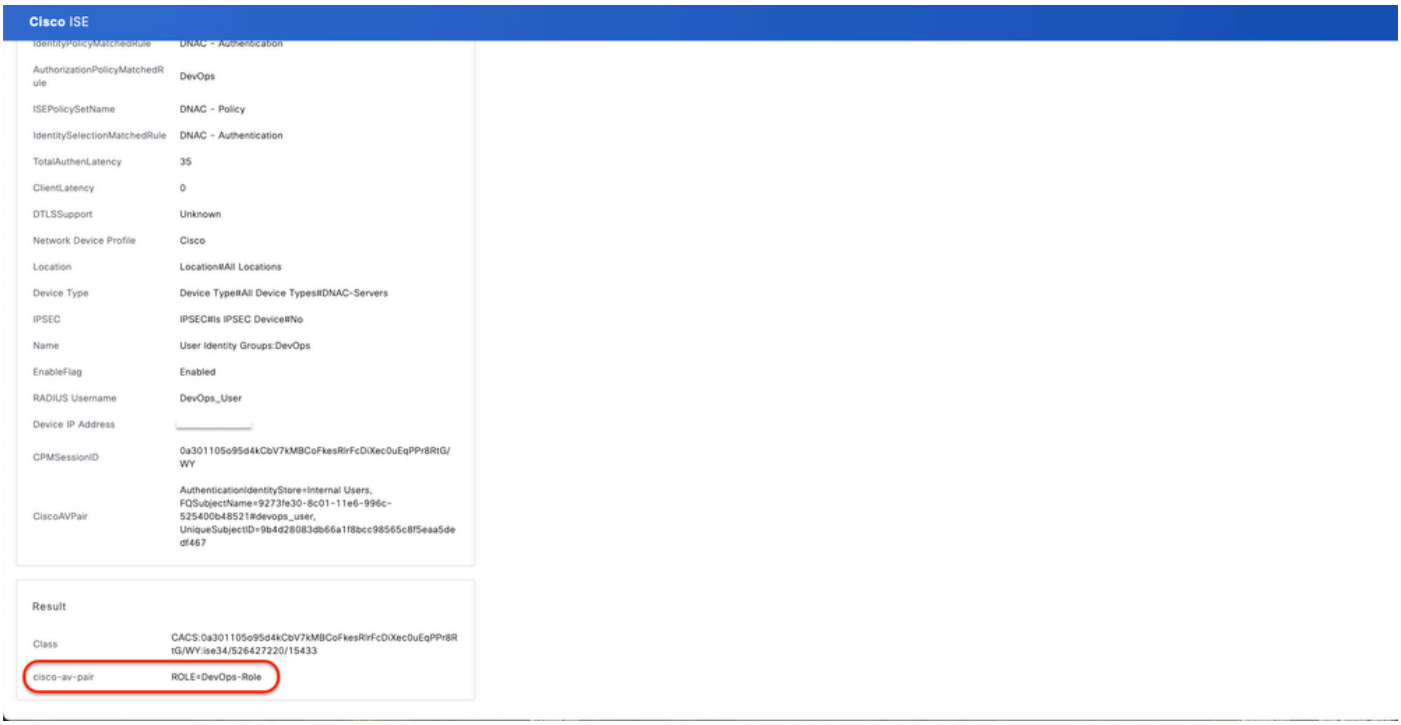


RADIUS live-logs

3.b ISE - RADIUS Live-logs Operations > RADIUS > Live-logs > Klik (Details) voor autorisatielogboek.



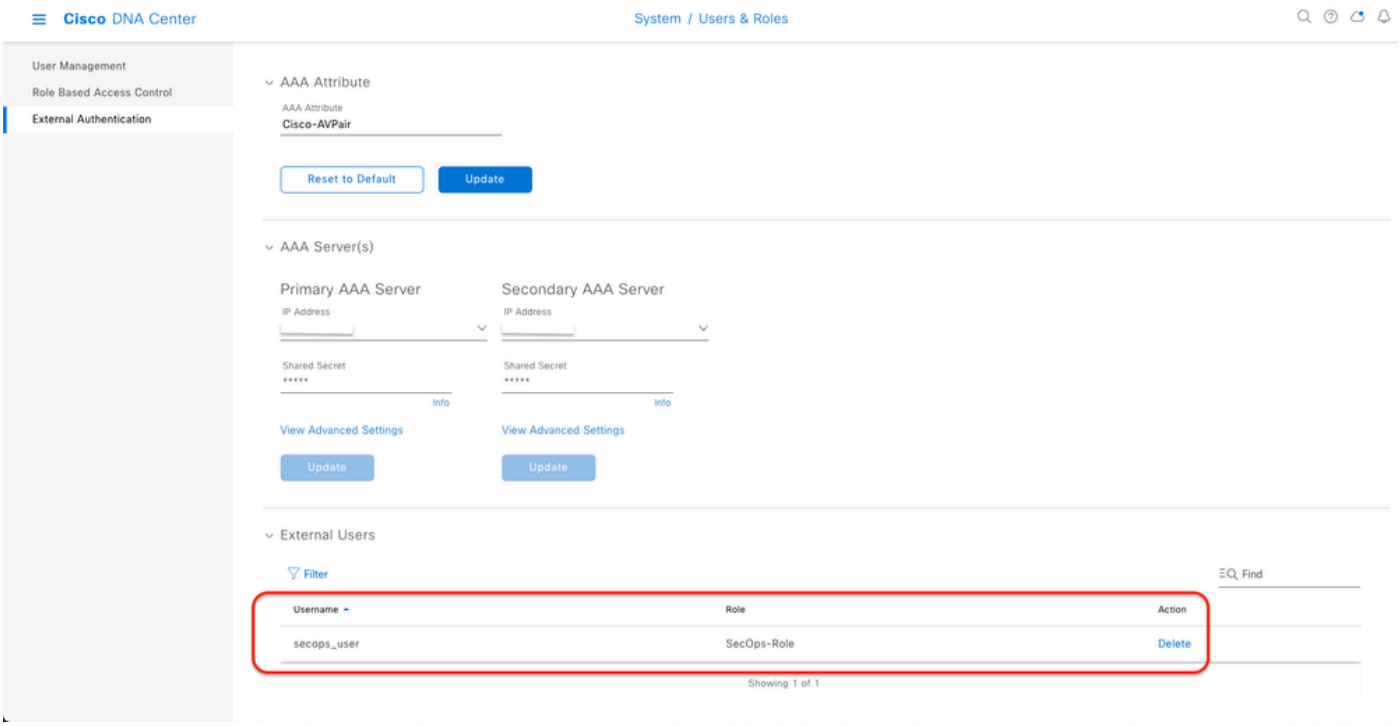
RADIUS gedetailleerde Live-logs 1-2



RADIUS gedetailleerde Live-logs 2-2

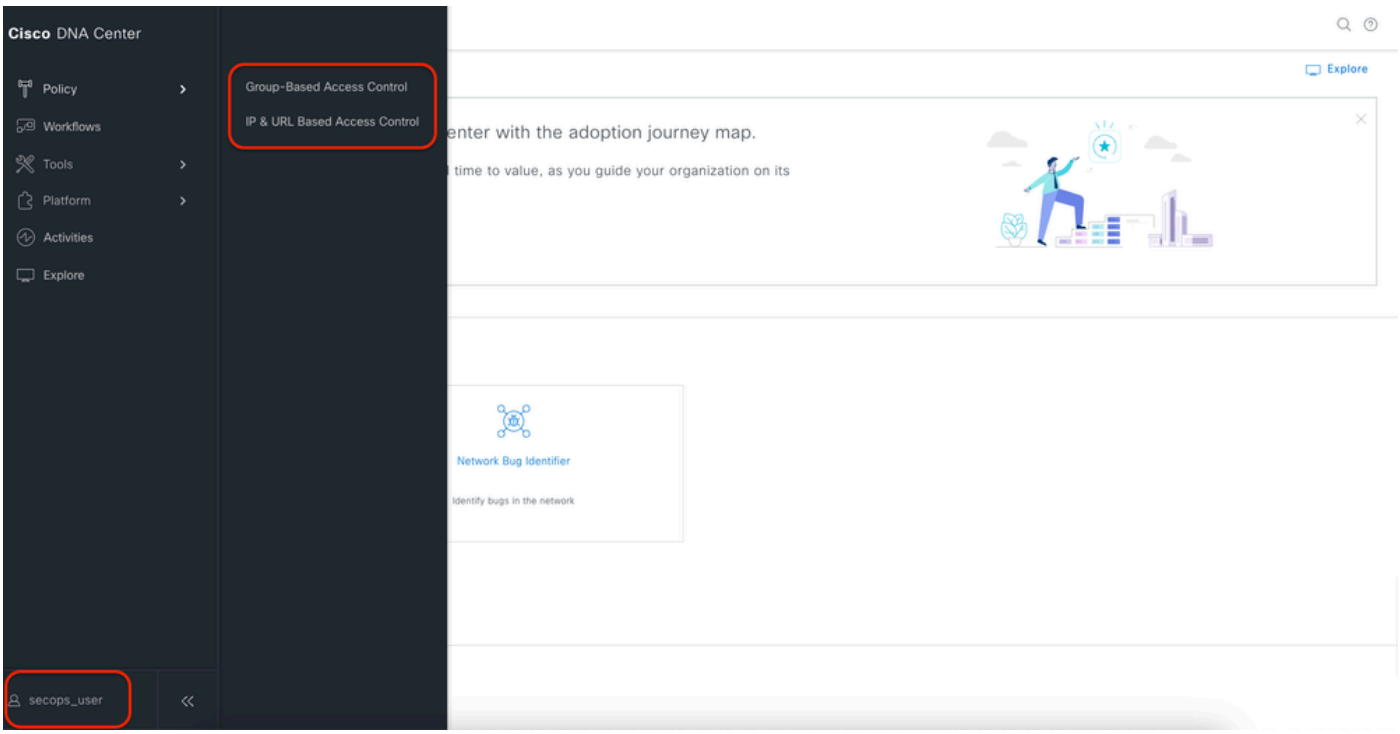
Controleer de TACACS+ configuratie

1- DNAC - Display Externe Gebruikers Systeem > Gebruikers & Rollen > Externe Verificatie > Externe Gebruikers.
U kunt de lijst bekijken van externe gebruikers die voor het eerst via TACACS+ zijn ingelogd. De informatie die wordt weergegeven omvat hun gebruikersnamen en rollen.



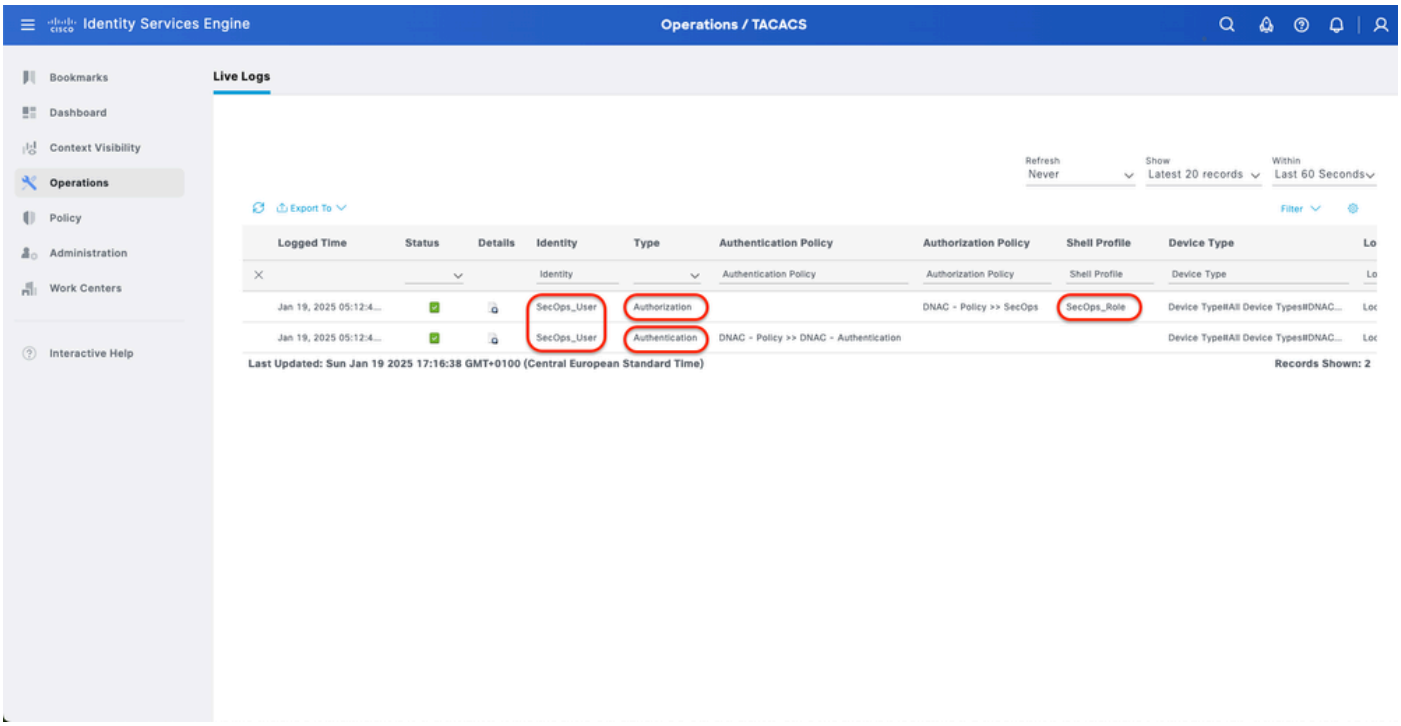
Externe gebruikers

2. DNAC - Bevestig de toegang van gebruikers.



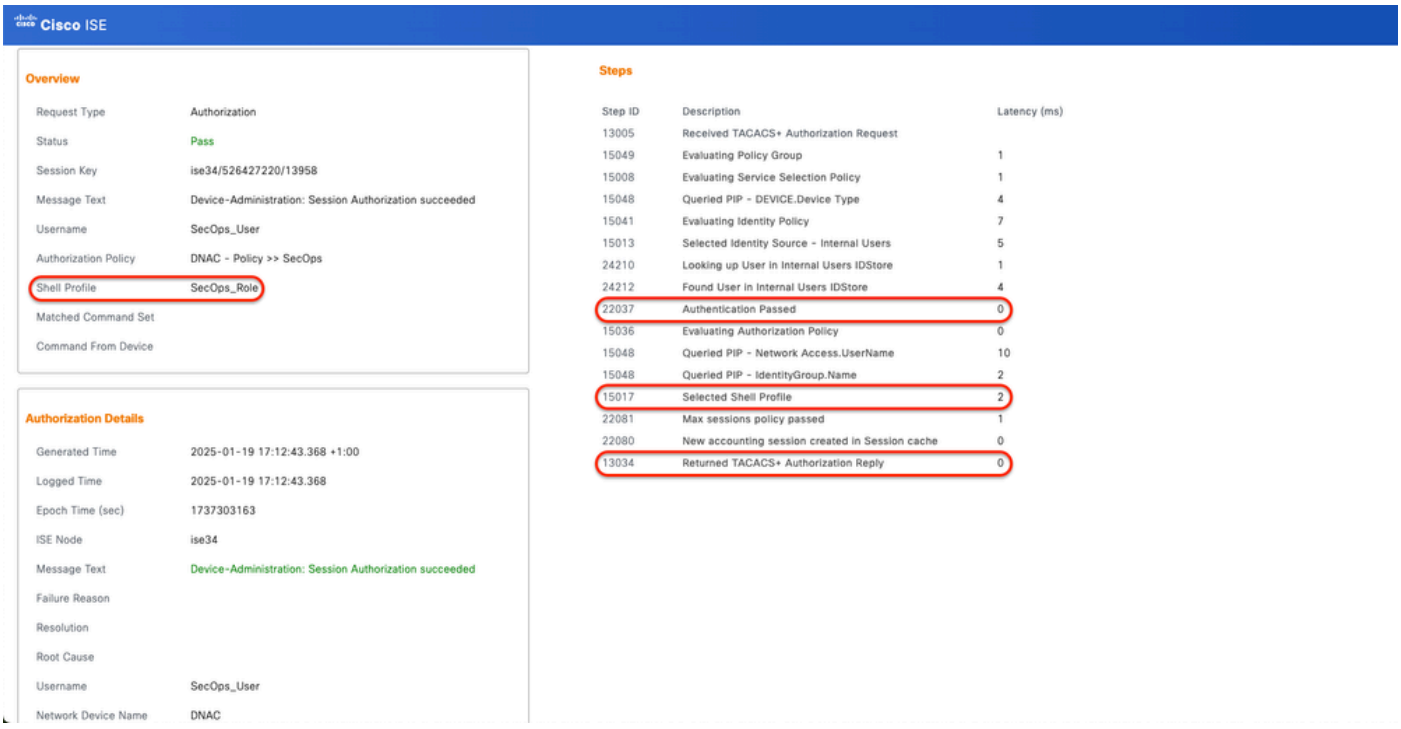
Beperkte gebruikerstoegang

3.a ISE - TACACS+ Live-Logs Work Centers > Apparaatbeheer > Overzicht > TACACS Livelog.

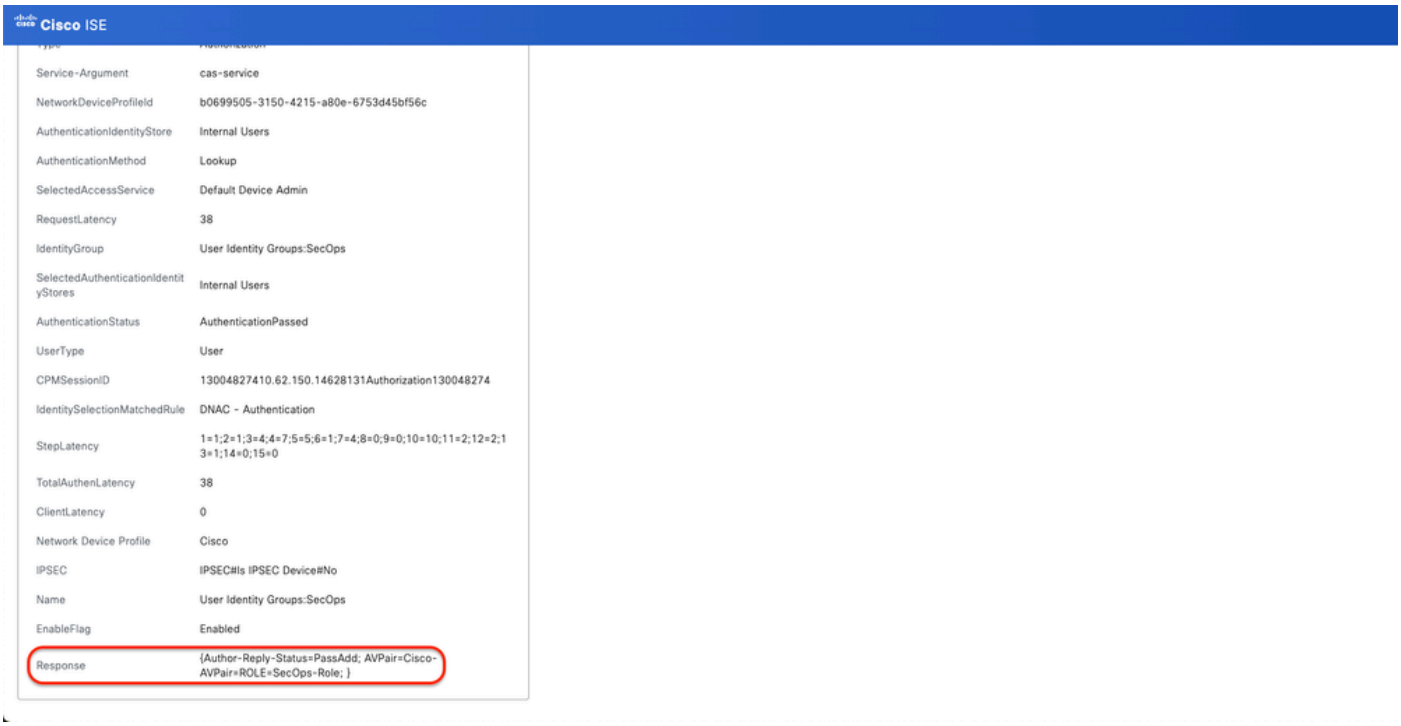


Live logs voor TACACS

3.b ISE - gedetailleerde TACACS+ Live-Logs Work Centers > Apparaatbeheer > Overzicht > TACACS Livelog > Klik (Details) voor autorisatielogboek.



Gedetailleerde live-logs 1-2 voor TACACS+



Gedetailleerde live-logs 2-2 voor TACACS+

Problemen oplossen

Er is momenteel geen specifieke diagnostische informatie beschikbaar voor deze configuratie.

Referenties

- Beheerdershandleiding voor Cisco Identity Services Engine, release 3.4 > Apparaatbeheer
- Beheerdershandleiding Cisco DNA Center, release 2.3.5

- Cisco DNA Center: Rol-gebaseerde toegangscontrole met externe verificatie

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.