ISE configureren als externe verificatie voor Catalyst SD-WAN GUI

Inhoud

Inleiding

In dit document wordt beschreven hoe u de Cisco Identity Services Engine (ISE) configureert als een externe verificatie voor het beheer van de Cisco Catalyst SD-WAN GUI.

Voorwaarden

Vereisten

Cisco raadt u aan om kennis te hebben van deze onderwerpen:

- TACACS+-protocol
- Cisco ISE Device Administration
- Cisco Catalyst SD-WAN-beheer
- 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 Patch2
- Cisco Catalyst SD-WAN versie 20.15.3

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

Vanaf Cisco vManage Release 20.9.1 worden nieuwe tags gebruikt voor verificatie:

- Viptela-User-Group: voor gebruikersgroepdefinities in plaats van Viptela-Group-Name.
- Viptela-Resource-Group: voor definities van brongroepen.

Configureren - TACACS+ gebruiken

Catalyst SD-WAN configureren met behulp van TACACS+

Procedure

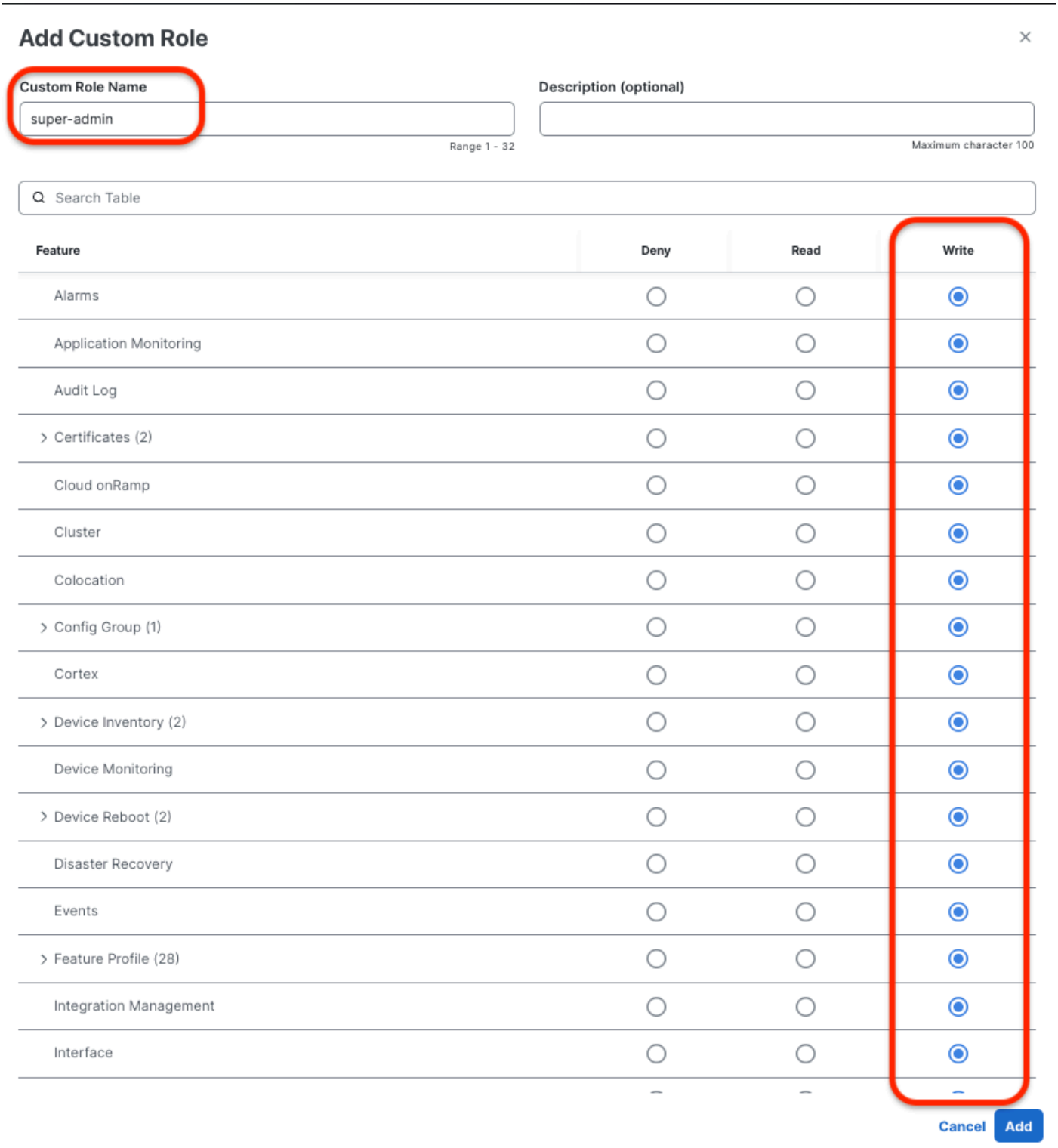
Stap 1. (Optioneel) Aangepaste rollen definiëren.

Configureer uw aangepaste rollen die aan uw vereisten voldoen, in plaats daarvan kunt u de standaardgebruikersrollen gebruiken. Dit kan worden gedaan vanuit het tabblad Catalyst SD-WAN: Beheer > Gebruikers en toegang > Rollen.

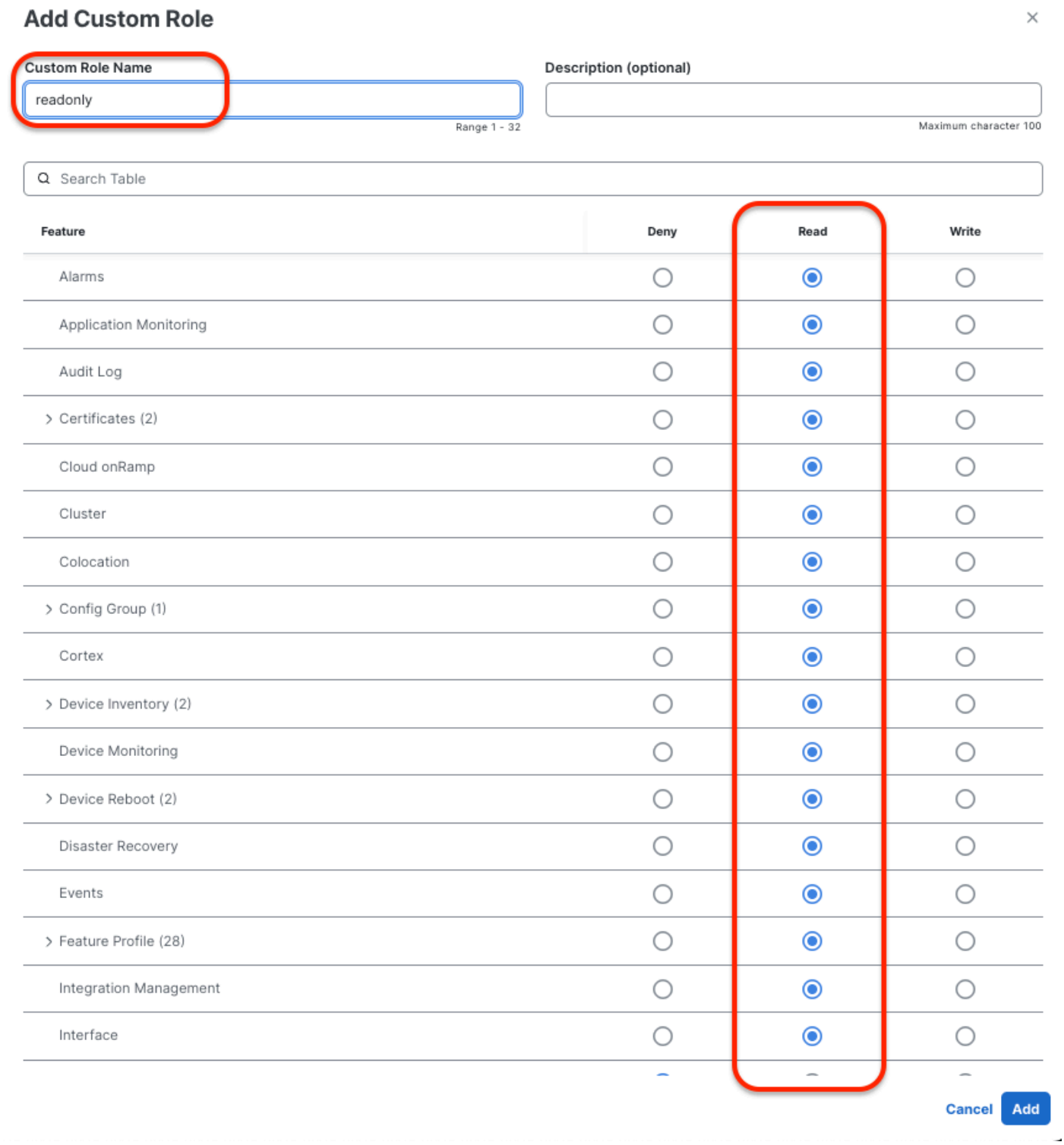
Twee aangepaste rollen maken:

1. Beheerdersrol: superbeheerder
2. Alleen-lezen rol: alleen-lezen

Dit kan worden gedaan vanuit het tabblad Catalyst SD-WAN: Beheer > Gebruikers en toegang > Rollen > Klik > Rol toevoegen.



Beheerdersrol (super-admin)



Alleen-lezen rol (alleen-lezen)

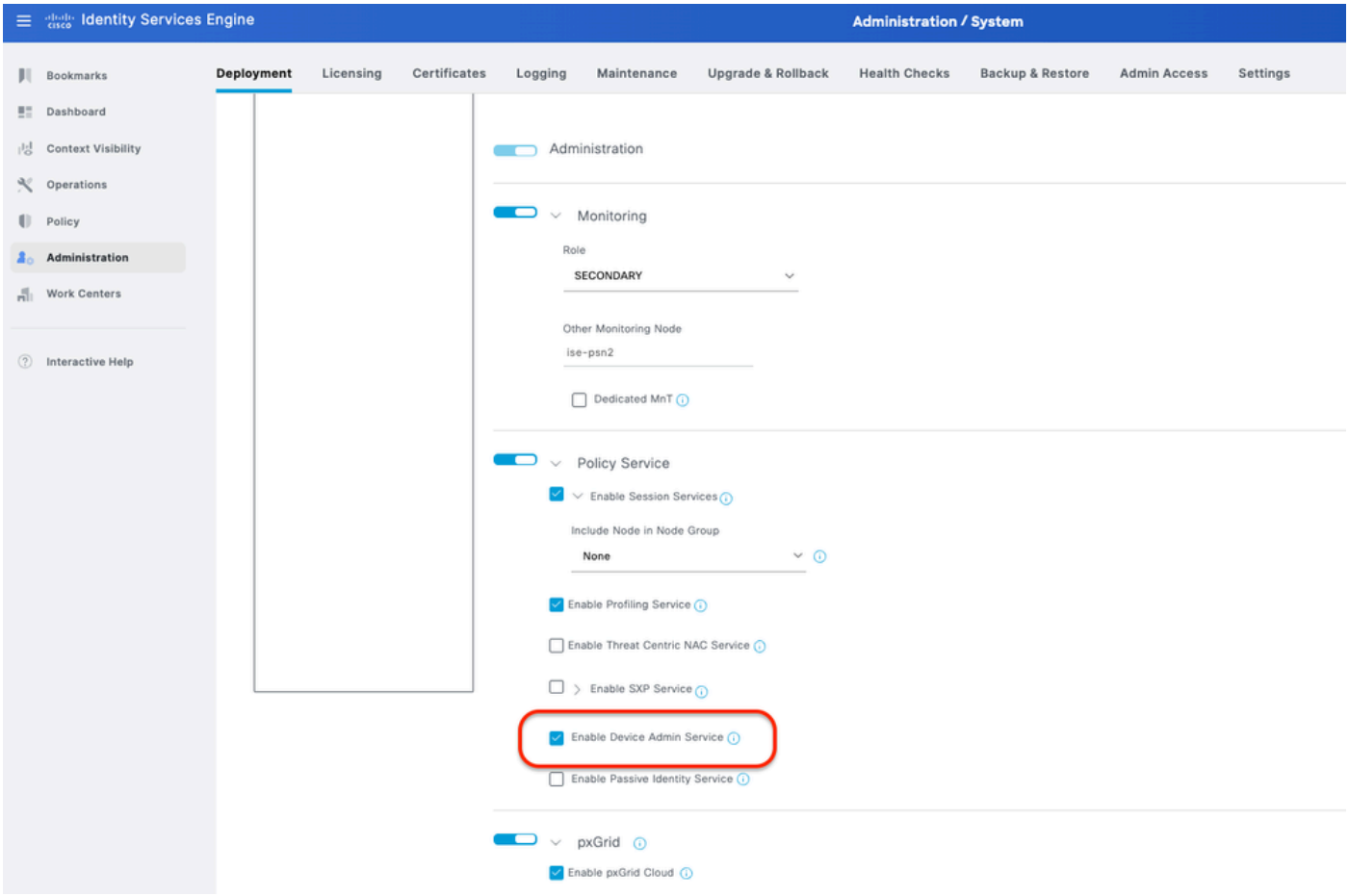
Stap 2. Configureer externe verificatie met behulp van TACACS+ (CLI).

```
Entering configuration mode terminal
vmanage(config)#
vmanage(config)#
vmanage(config)# system
vmanage(config-system)# aaa
vmanage(config-aaa)# auth-order tacacs radius local
vmanage(config-aaa)# auth-fallback
vmanage(config-aaa)# commit and-quit
Commit complete.
```

vManger CLI - TACACS+-configuratie

ISE configureren voor TACACS+

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



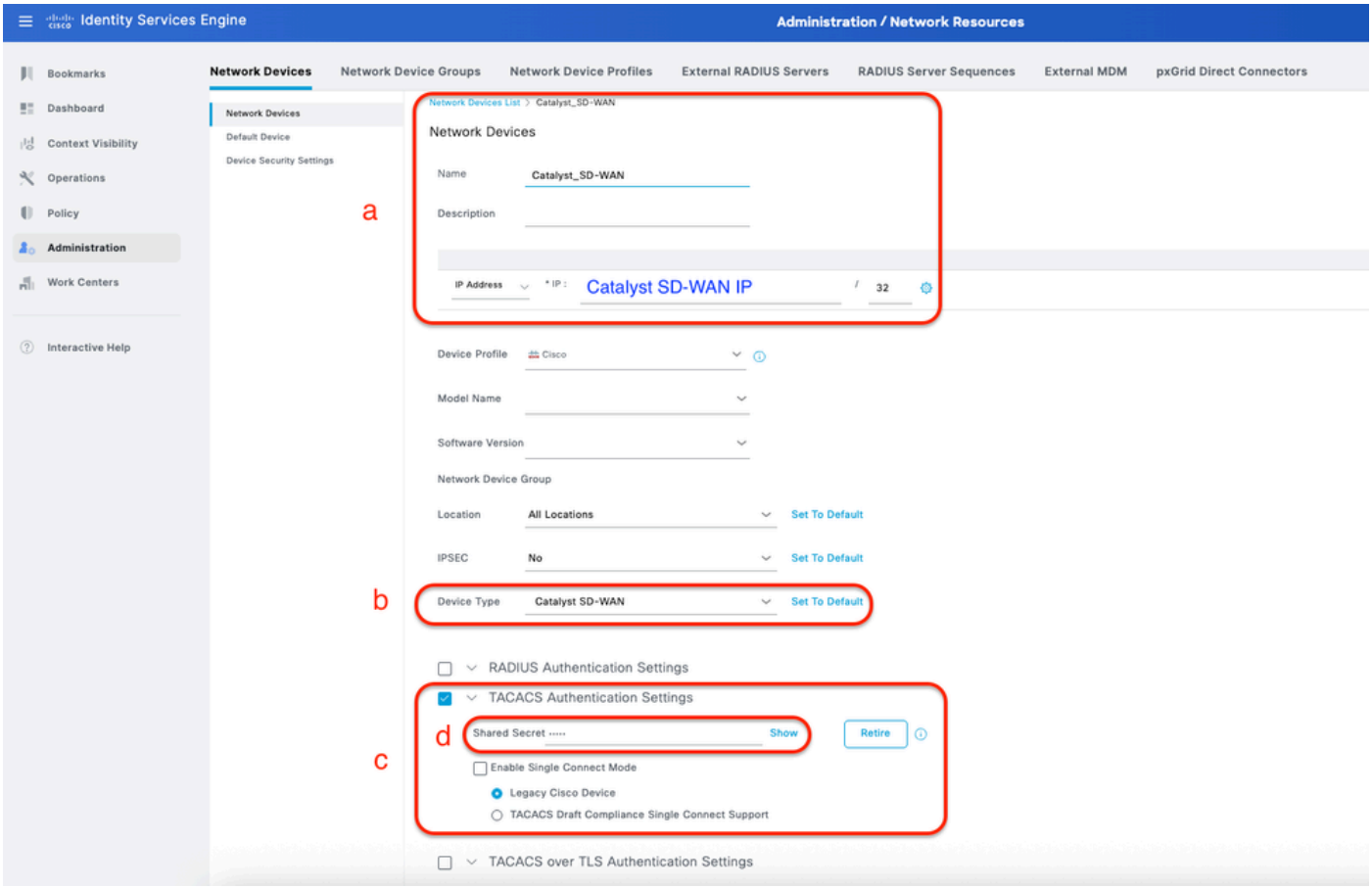
Apparaatbeheerservice inschakelen

Stap 2. Voeg Catalyst SD-WAN toe als netwerkapparaat op ISE.

U kunt dit doen via het tabblad Beheer > Netwerkbronnen > Netwerkapparaten.

Procedure

a. Definieer (Catalyst SD-WAN) de naam en het IP-adres van het netwerkapparaat.
b. (Optioneel) Type apparaat classificeren voor de voorwaarde Policy Set.
c. TACACS+-verificatie-instellingen inschakelen.
d. Gedeeld TACACS+-geheim instellen.



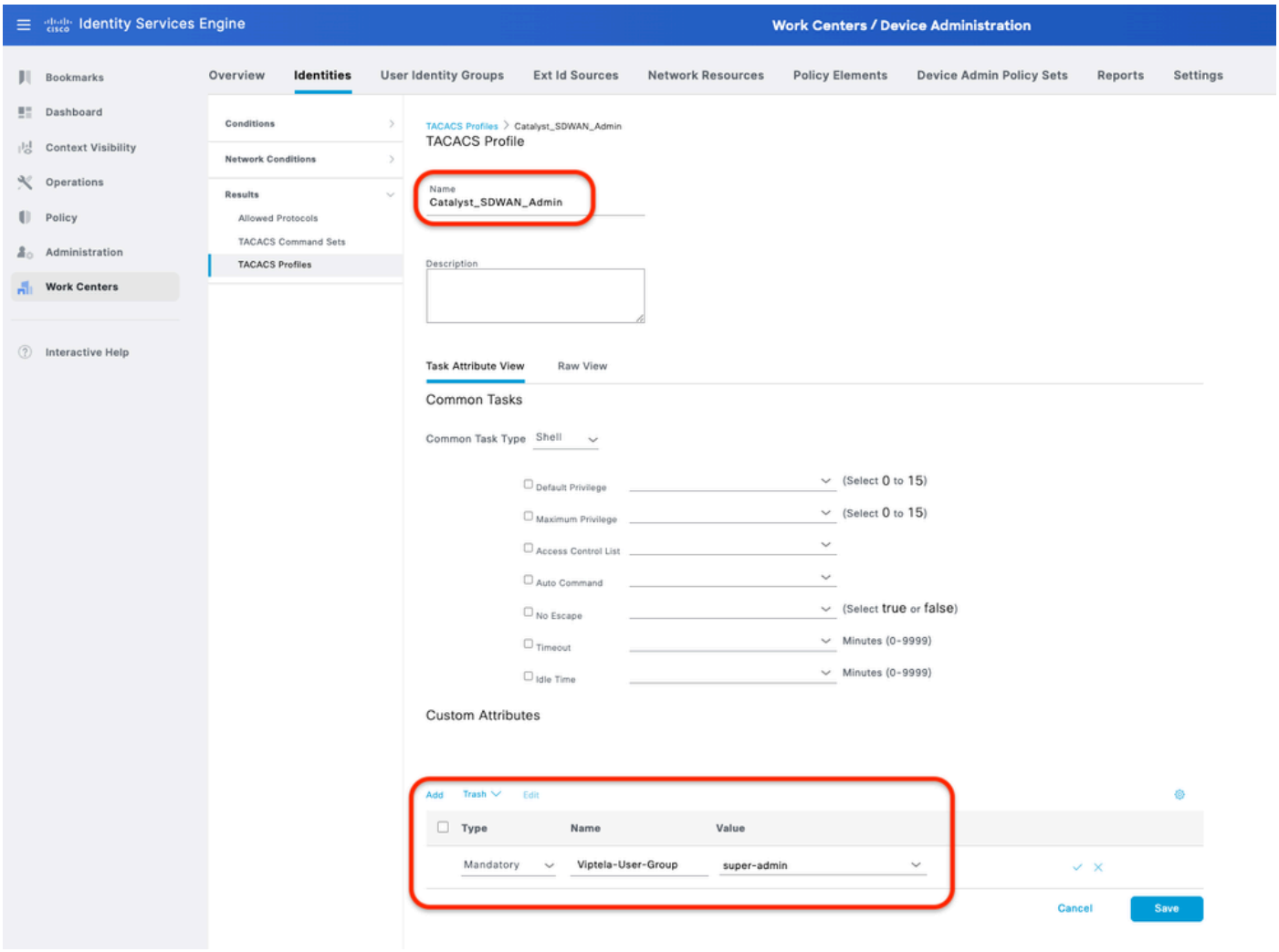
ISE Network Device Catalyst (SD-WAN) voor TACACS+

Stap 3. Maak een TACACS+-profiel voor elke Catalyst SD-WAN-rol.

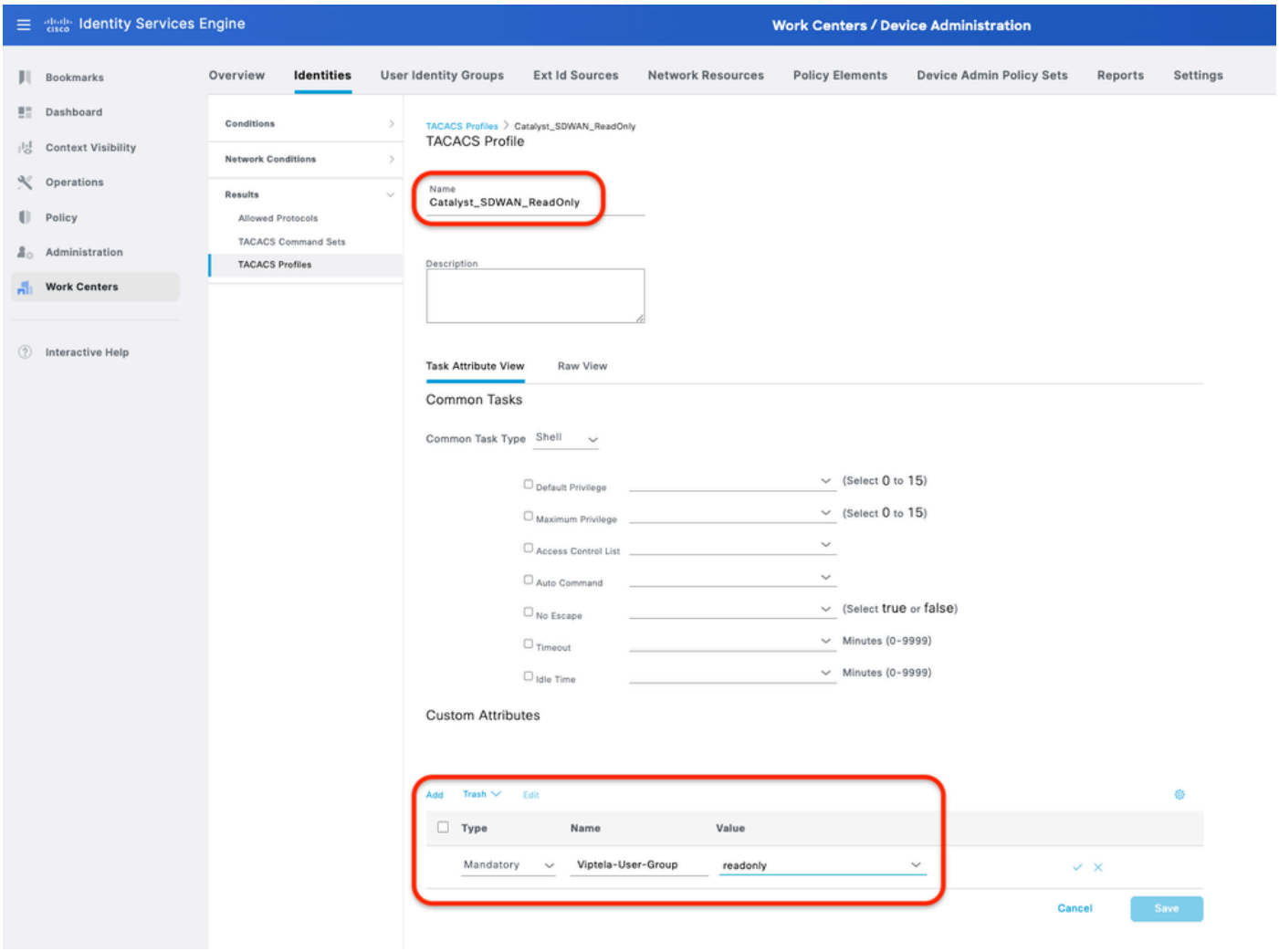
TACACS+-profielen maken:

1. Catalyst_SDWAN_Admin: voor Super Admin-gebruikers.
2. Catalyst_SDWAN_ReadOnly: voor alleen-lezen gebruikers.

U kunt dit doen via het tabblad Werkcentra > Apparaatbeheer > Beleidselementen > Resultaten > TACACS-profielen > Toevoegen.



TACACS+ profiel - (Catalyst_SDWAN_Admin)



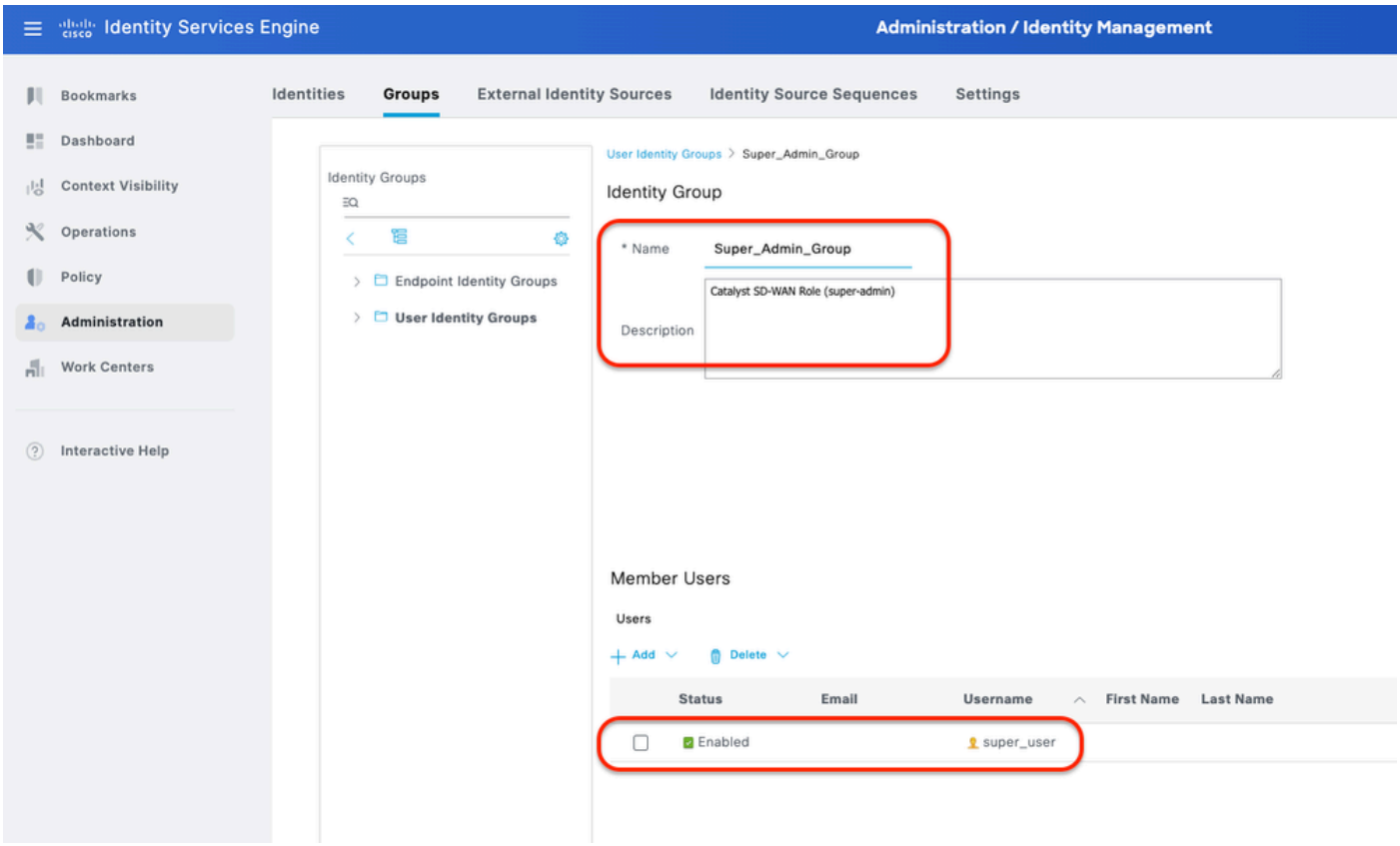
TACACS+-profiel - (Catalyst_SDWAN_ReadOnly)

Stap 4. Maak een gebruikersgroep en voeg lokale gebruikers toe als lid.

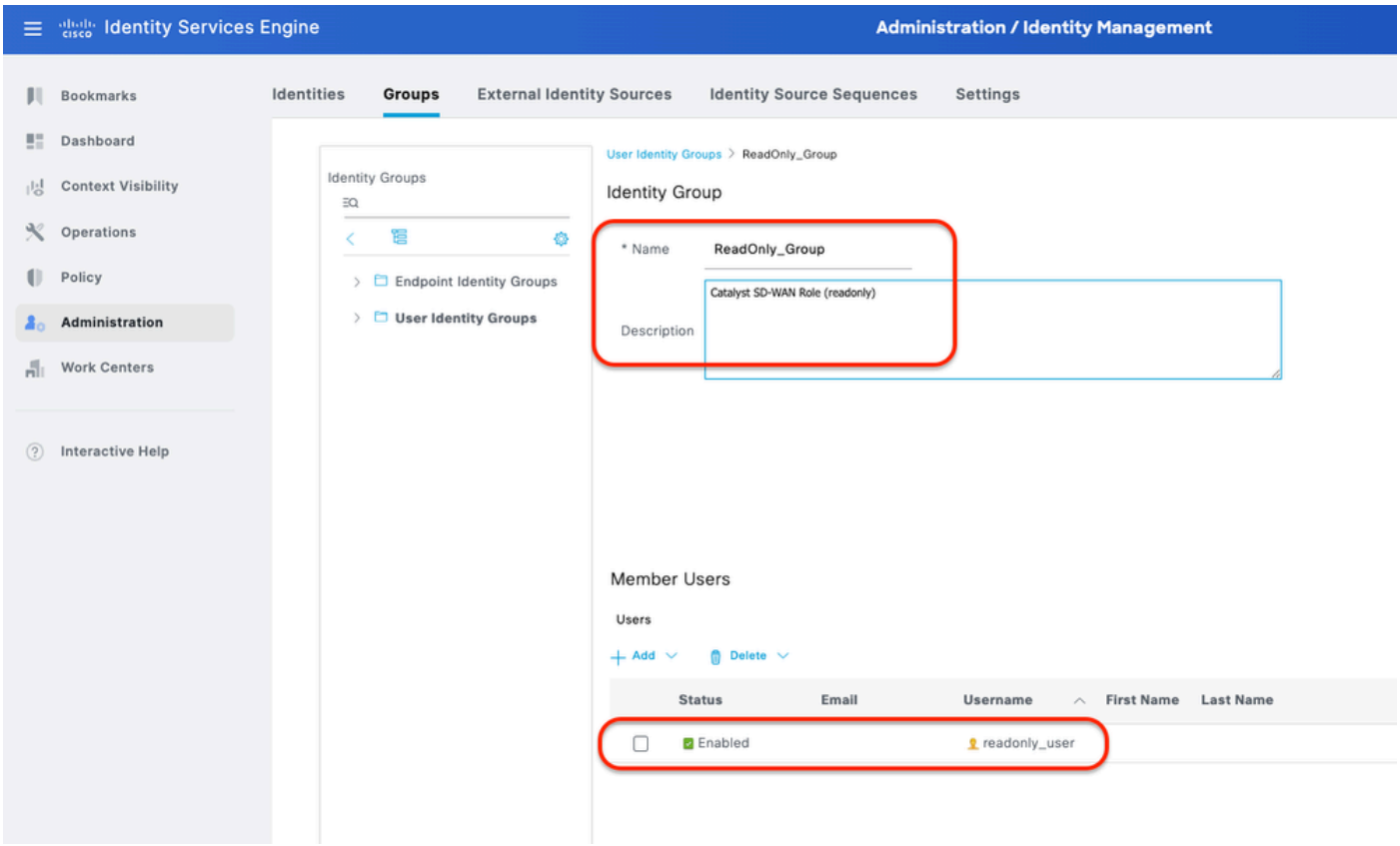
Dit kan worden gedaan via het tabblad Werkcentra > Apparaatbeheer > Gebruikersidentiteitsgroepen.

Maak twee groepen voor gebruikersidentiteit:

1. Super_Admin_Group
2. ReadOnly_Group



Gebruikersidentiteitsgroep - (Super_Admin_Group)



Gebruikersidentiteitsgroep - (ReadOnly_Group)

Stap 5. (Optioneel) TACACS+-beleidsset toevoegen.

Dit kan worden gedaan via het tabblad Werkcentra > Apparaatbeheer > Beleidssets apparaatbeheer.

Procedure

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

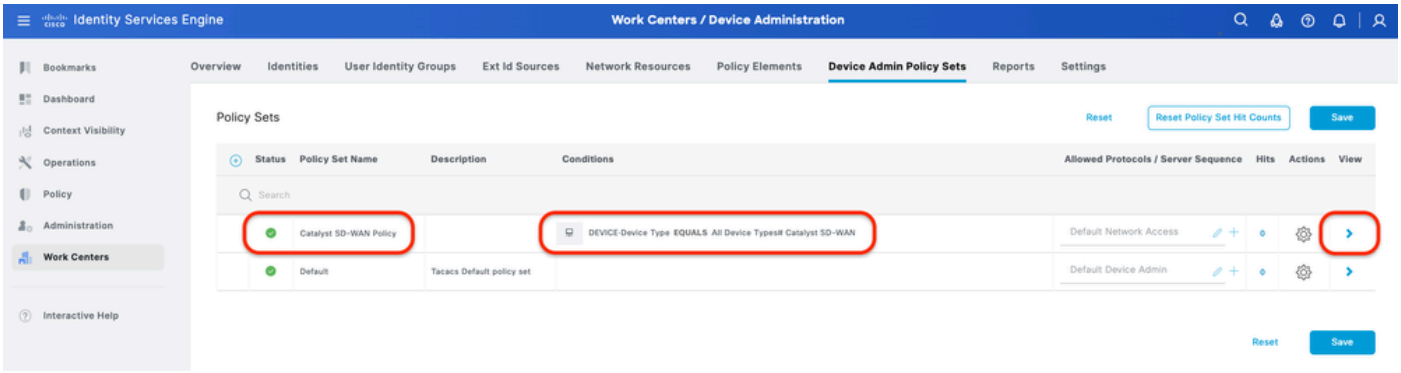
b. Definieer de naam van de beleidsset.

c. Stel de voorwaarde voor beleidssets in op Selecteer apparaattype dat u eerder hebt gemaakt op (Stap 2 > b).

d. Stel de toegestane protocollen in.

e. Klik op Opslaan.

f. Klik op (>) Weergave beleidsset om de verificatie- en autorisatieregels te configureren.



ISE-beleidsset

Stap 6. Configureer het TACACS+-verificatiebeleid.

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

Procedure

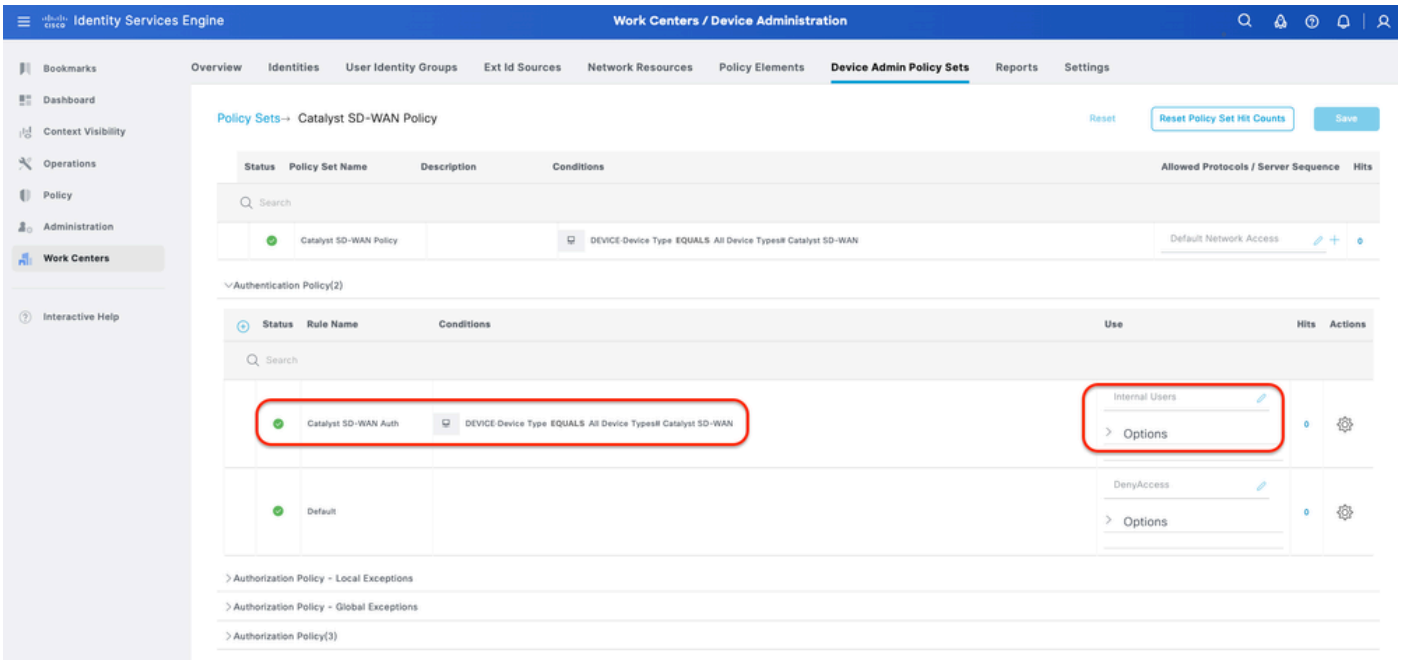
a. Klik op Acties en kies (Nieuwe rij hierboven invoegen).

b. De naam van het verificatiebeleid definiëren.

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

d. Stel het verificatiebeleid Gebruik voor identiteitsbron in.

e. Klik op Opslaan.



Authenticatiebeleid

Stap 7. Het machtigingsbeleid van TACACS+ configureren.

U kunt dit doen via het tabblad Werkcentra > Apparaatbeheer > Apparaatbeheerbeleidssets > Klik op (>).

Deze stap om het machtigingsbeleid voor elke SD-WAN-rol van de katalysator te maken:

- Catalyst SD-WAN Authz (super-admin): super-admin
- Catalyst SD-WAN Authz (alleen-lezen): alleen-lezen

Procedure

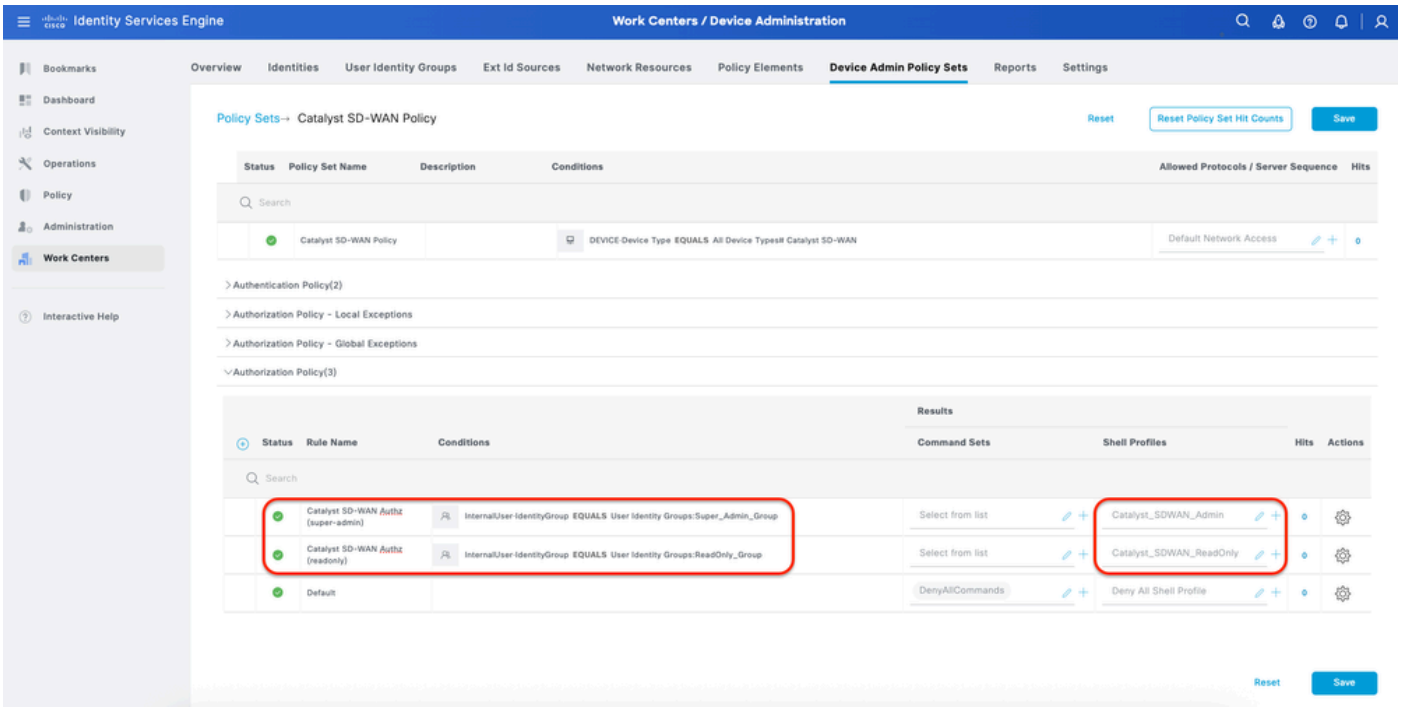
a. Klik op Acties en kies (Nieuwe rij hierboven invoegen).

b. Definieer de naam van het autorisatiebeleid.

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

d. Stel de Shell-profielen voor het machtigingsbeleid in en selecteer het TACACS-profiel dat u in hebt gemaakt (stap 3).

e. Klik op Opslaan.

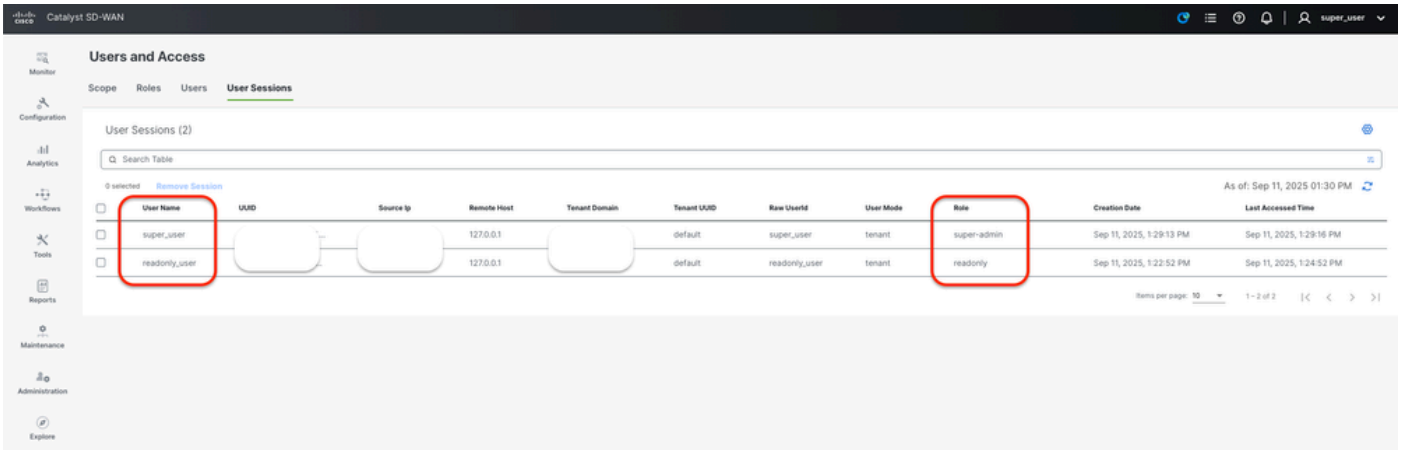


machtigingsbeleid

Controleer de configuratie van TACACS+

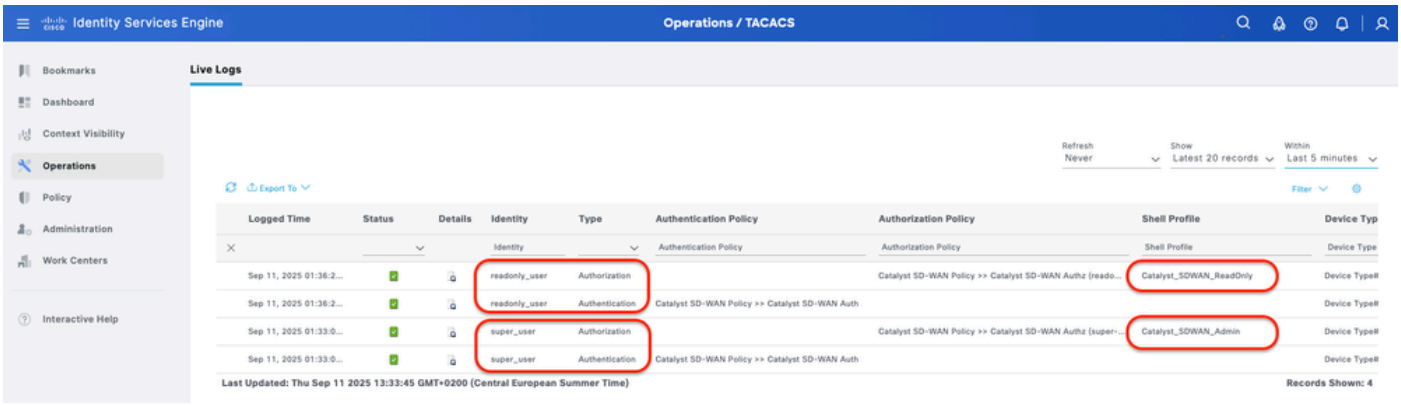
1- Display Catalyst SD-WAS User Sessions Catalyst SD-WAN: Beheer > Gebruikers en toegang > Gebruikersessies.

U kunt de lijst bekijken van externe gebruikers die voor het eerst zijn ingelogd via RADIUS. De informatie die wordt weergegeven, bevat hun gebruikersnamen en rollen.



Catalyst SD-WAS-gebruikerssessies

2- ISE - TACACS Live-Logs Operations > TACACS > Live-Logs.


Identity Services Engine
Operations / TACACS
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Help
Live Logs
Refresh
Never
Show
Latest 20 records
Within
Last 5 minutes
Export To
Filter
Logged Time
Status
Details
Identity
Type
Authentication Policy
Authorization Policy
Shell Profile
Device Typ
Sep 11, 2025 01:36:2...
readonly_user
Authorization
Catalyst SD-WAN Policy >> Catalyst SD-WAN Authz (reado...
Catalyst_SDWAN_ReadOnly
Device Type#
Sep 11, 2025 01:36:2...
readonly_user
Authentication
Catalyst SD-WAN Policy >> Catalyst SD-WAN Auth
Device Type#
Sep 11, 2025 01:33:0...
super_user
Authorization
Catalyst SD-WAN Policy >> Catalyst SD-WAN Authz (super-...
Catalyst_SDWAN_Admin
Device Type#
Sep 11, 2025 01:33:0...
super_user
Authentication
Catalyst SD-WAN Policy >> Catalyst SD-WAN Auth
Device Type#
Last Updated: Thu Sep 11 2025 13:33:45 GMT+0200 (Central European Summer Time)
Records Shown: 4

Live-logs

Protocol	Tacacs
Type	Authorization
Service-Argument	ppp
Protocol-Argument	ip
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	Lookup
SelectedAccessService	Default Network Access
RequestLatency	27
IdentityGroup	User Identity Groups:ReadOnly_Group
SelectedAuthenticationIdentityStores	Internal Users
AuthenticationStatus	AuthenticationPassed
UserType	User
CPMSessionID	316584755210.127.198.7438561Authorization3165847552
IdentitySelectionMatchedRule	Catalyst SD-WAN Auth
StepLatency	1=0;2=0;3=4;4=3;5=4;6=0;7=2;8=1;9=0;10=8;11=2;12=3;13=0;14=0;15=0
TotalAuthenLatency	27
ClientLatency	0
TacacsPlusTLS	false
Network Device Profile	Cisco
IPSEC	IPSEC#Is IPSEC Device#No
EnableFlag	Enabled
Response	{Author-Reply-Status=PassAdd; AVPair=Viptela-User-Group=readonly; }

Gedetailleerde live-logs - (alleen-lezen)

Protocol	Tacacs
Type	Authorization
Service-Argument	ppp
Protocol-Argument	ip
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	Lookup
SelectedAccessService	Default Network Access
RequestLatency	30
IdentityGroup	User Identity Groups:Super_Admin_Group
SelectedAuthenticationIdentityStores	Internal Users
AuthenticationStatus	AuthenticationPassed
UserType	User
CPMSessionID	354536652810.127.198.7460535Authorization3545366528
IdentitySelectionMatchedRule	Catalyst SD-WAN Auth
StepLatency	1=1;2=0;3=3;4=3;5=3;6=0;7=2;8=0;9=0;10=10;11=4;12=4;13=0;14=1;15=0
TotalAuthenLatency	30
ClientLatency	0
TacacsPlusTLS	false
Network Device Profile	Cisco
IPSEC	IPSEC#Is IPSEC Device#No
EnableFlag	Enabled
Response	{Author-Reply-Status=PassAdd; AVPair=Viptela-User-Group=super-admin; }

Problemen oplossen

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

Referenties

- Beheerdershandleiding voor de Cisco Identity Services-engine, release 3.4
- Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x

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.