CSM TACACS-integratie met ISE

Inhoud

Inleiding

Dit document beschrijft de procedure om Cisco Security Manager (CSM) te integreren met Identity Services Engine (ISE) voor beheergebruikers en verificatie met TACACS+ Protocol.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Security Manager (CSM).
- Identity Services Engine (ISE).
- TACACS-protocol.

Gebruikte componenten

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

- CSM Server versie 4.2.2
- ISE versie 3.0

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Standaard gebruikt Cisco Security Manager (CSM) een verificatiemodus die Cisco heet, werken om gebruikers lokaal te authentiseren en te autoriseren, om een gecentraliseerde verificatiemethode te kunnen gebruiken die u Cisco Identity Services Engine via het TACACS-protocol kunt gebruiken.

Configureren

Netwerkdiagram

Verificatieprocedure

Stap 1.Meld u aan bij de CSM-toepassing met de referenties van de beheerder.

Stap 2. Het verificatieproces start en ISE bevestigt de referenties lokaal of via de actieve map.

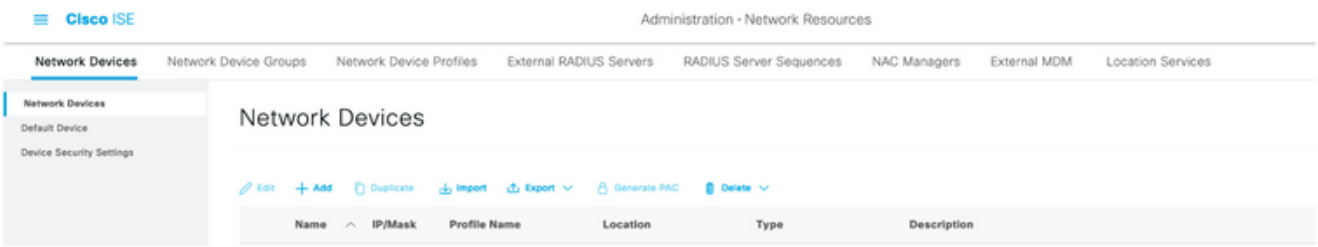
Stap 3. Zodra de authenticatie een succesvol ISE is, verstuurt u een vergunningspakket om de toegang tot CSM te verlenen.

Stap 4. CSM brengt de gebruikersnaam in kaart met de lokale gebruikersrol-toewijzing.

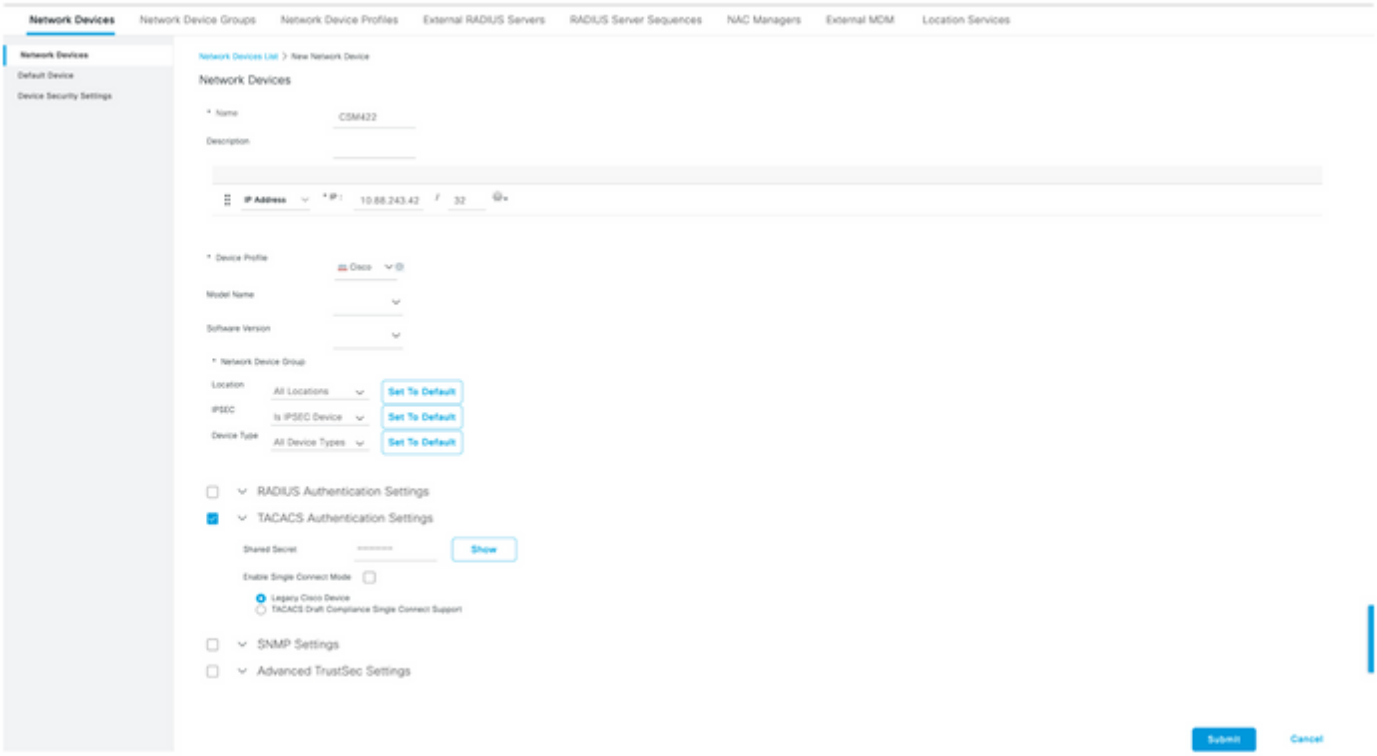
Stap 5. ISE toont een succesvol authentificatielevend logbestand.

ISE-configuratie

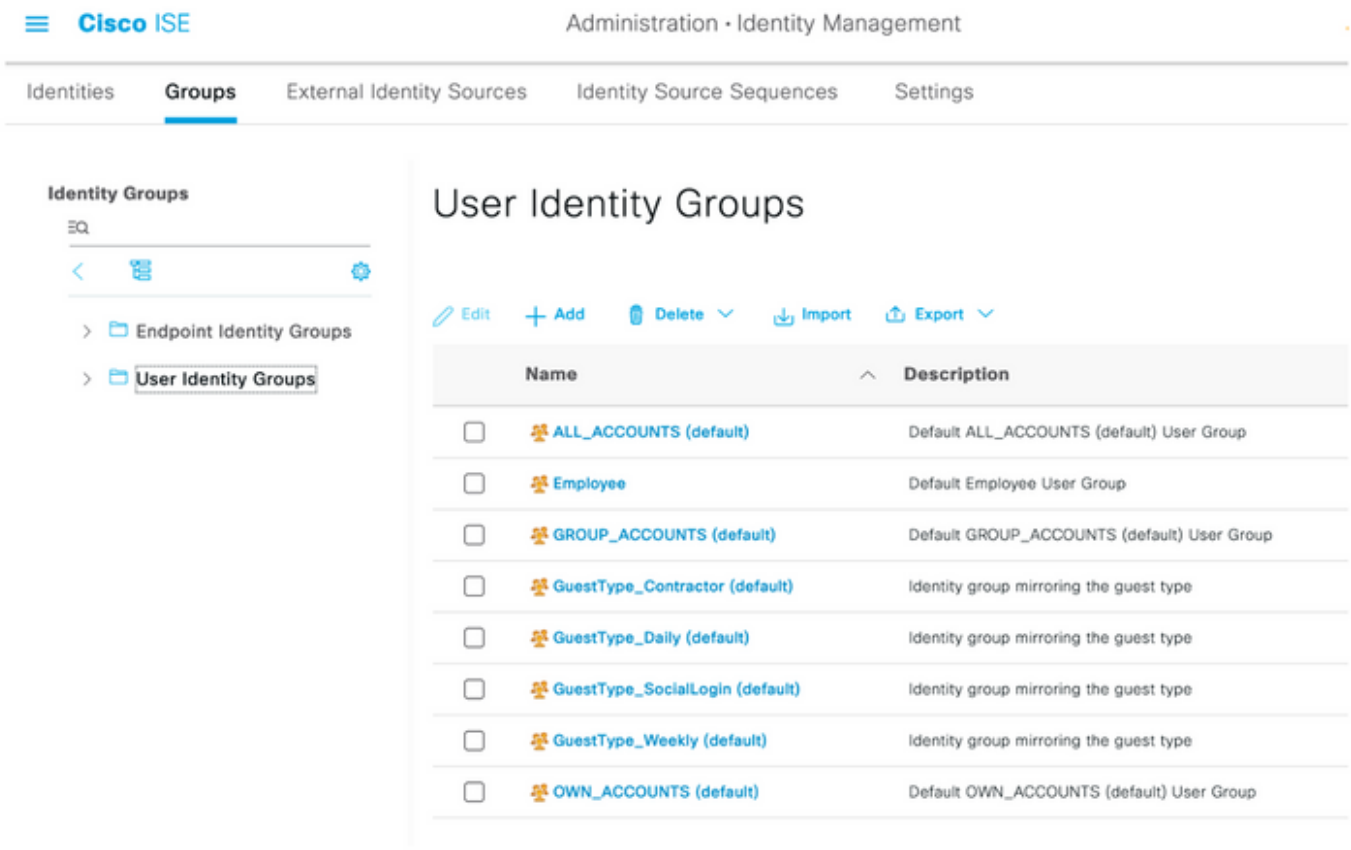
Stap 1. Selecteer het pictogram drie lijnen bevindt zich in de linker bovenhoek en navigeer naar **Beheer > Netwerkbronnen > Netwerkapparaten.**



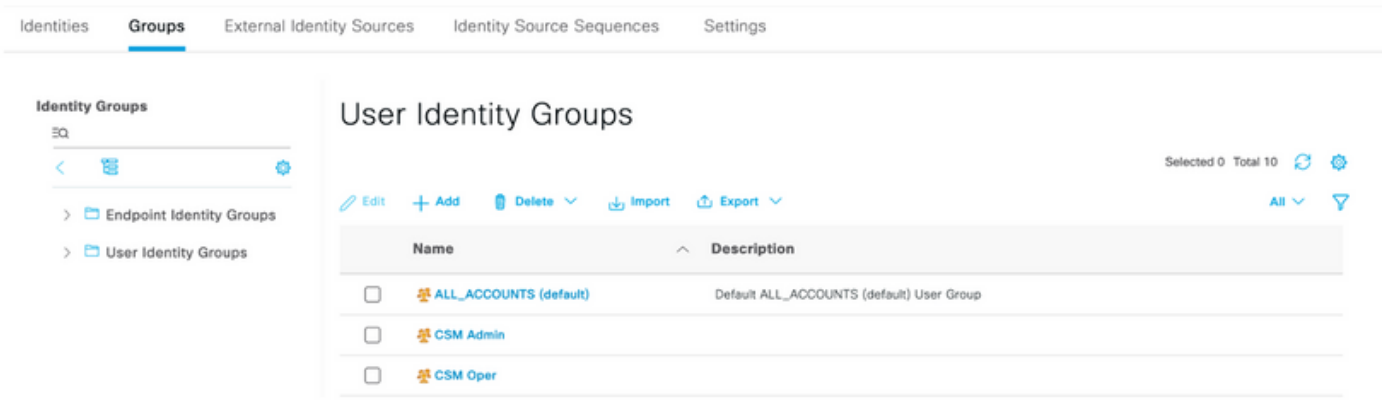
Stap 2. Selecteer de knop **+Add** en voer de juiste waarden voor de naam en het IP-adres van het netwerktoegangsapparaat in. Controleer vervolgens het selectieteken van de **TACACS-verificatie** en definieer een gedeeld geheim. Selecteer de knop **Indienen**.



Stap 3. Selecteer het pictogram drie regels bevindt zich in de linker bovenhoek en navigeer naar **Administratie > identiteitsbeheer > Groepen.**

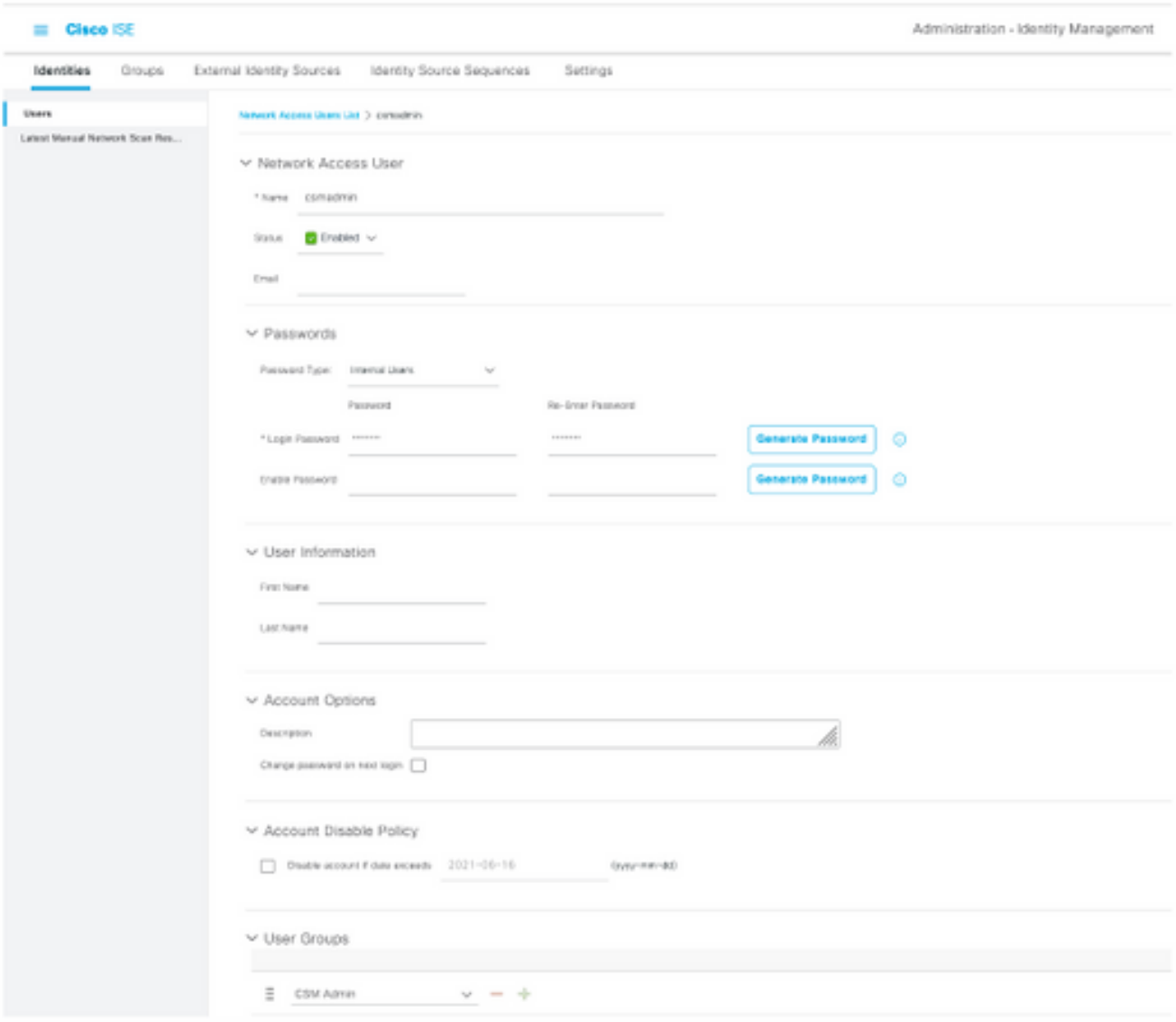


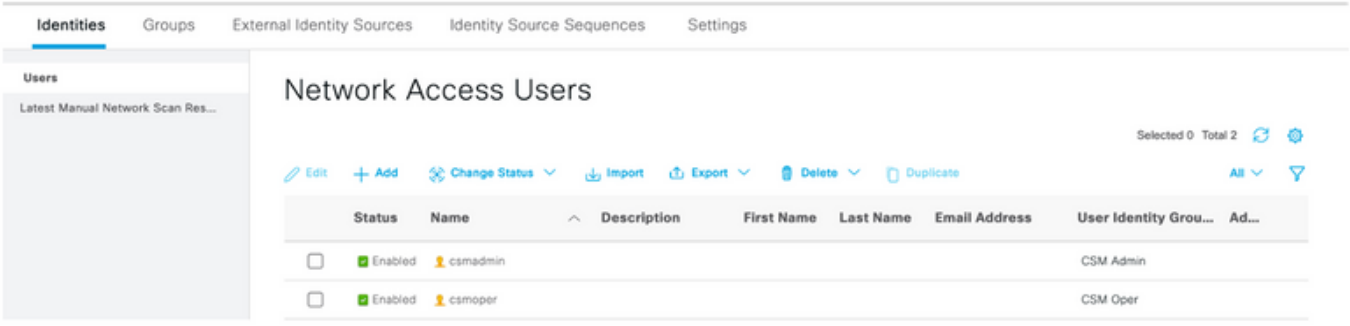
Stap 4. Navigeer naar **de** map **Gebruikersgroepen** en selecteer de knop **+Add**. Defineert een naam en selecteer de knop **Indienen**.



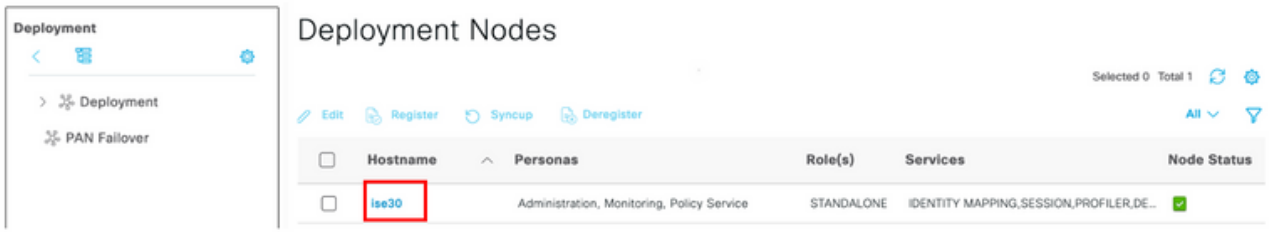
Opmerking: Dit voorbeeld maakt CSM Admin en CSM Oper Identity Services groepen. U kunt Stap 4 voor elk type Admin-gebruikers op CSM herhalen

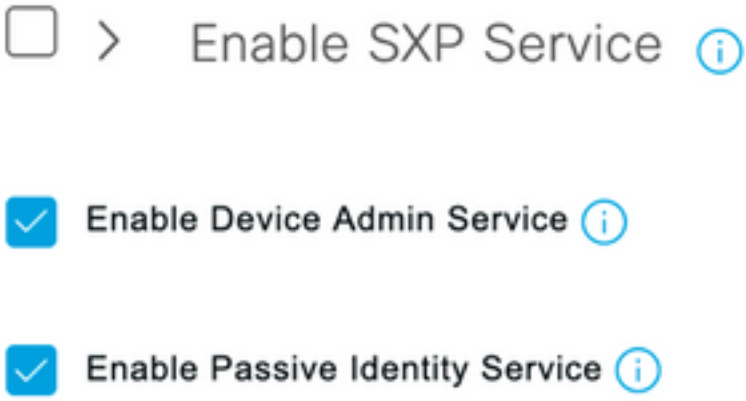
Stap 5. Selecteer het pictogram drie lijnen en navigeer naar **Administratie > Identity Management >Identificaties.** Selecteer de knop **+Add** en definieer de gebruikersnaam en het wachtwoord en selecteer vervolgens de groep waartoe de gebruiker behoort. In dit voorbeeld maakt u de **csmadmin-** en csmoper-gebruikers aan en toegewezen aan respectievelijk CSM Admin en CSM Oper groep.





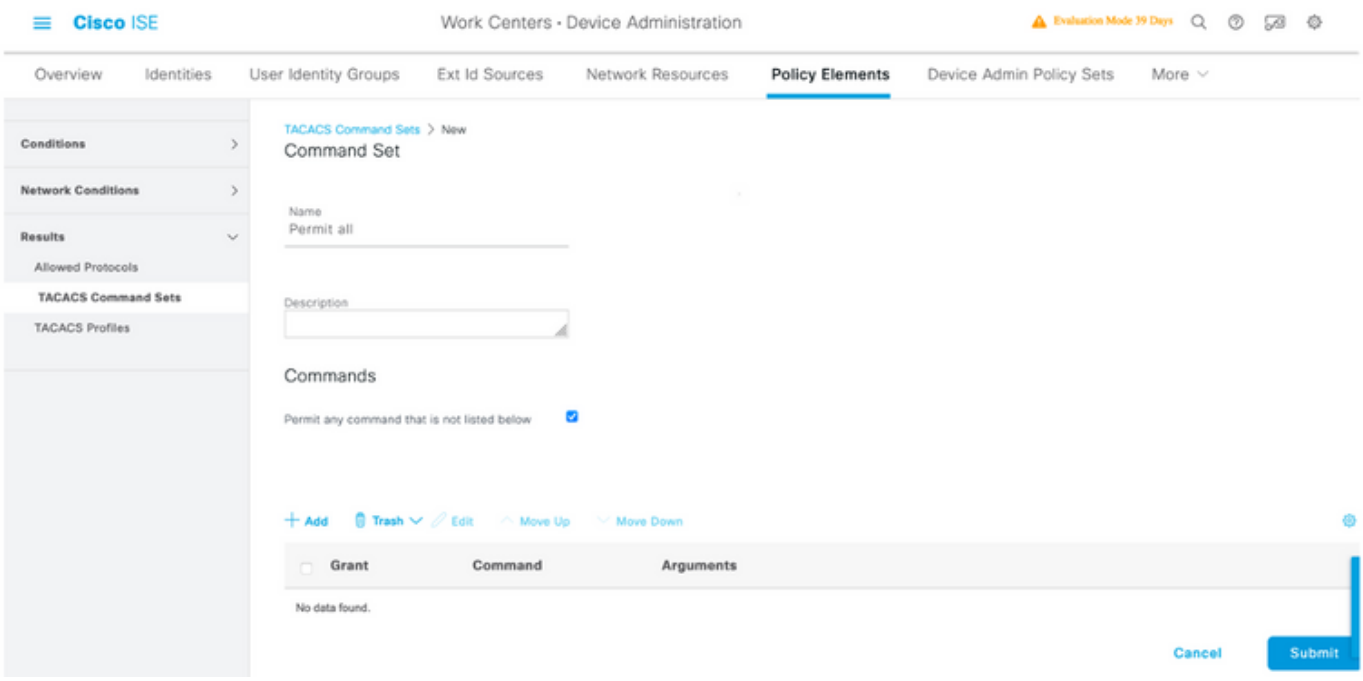
Stap 6. Selecteer en navigeer naar **Administratie > Systeem > Plaatsing.** Selecteer het hostname-knooppunt en stel **de apparaatbeheerservice** in





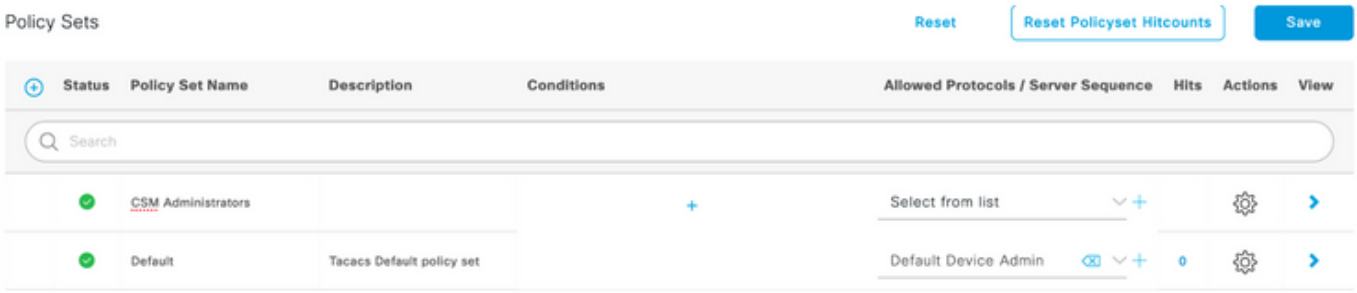
Opmerking: Selecteer in het geval van gedistribueerde implementatie het PSN-knooppunt dat TACACS-verzoeken behandelt

Stap 7. Selecteer het pictogram drie regels en navigeer naar **Administratie > Apparaatbeheer > Beleidselementen.** Navigeer naar **resultaten > TACACS Opdrachten.** Selecteer de knop **+Add,** definieer een naam voor de Opdrachtset en stel de **opdracht** in **die niet onder** het selectieteken **staat**. Selecteer **Indienen.**

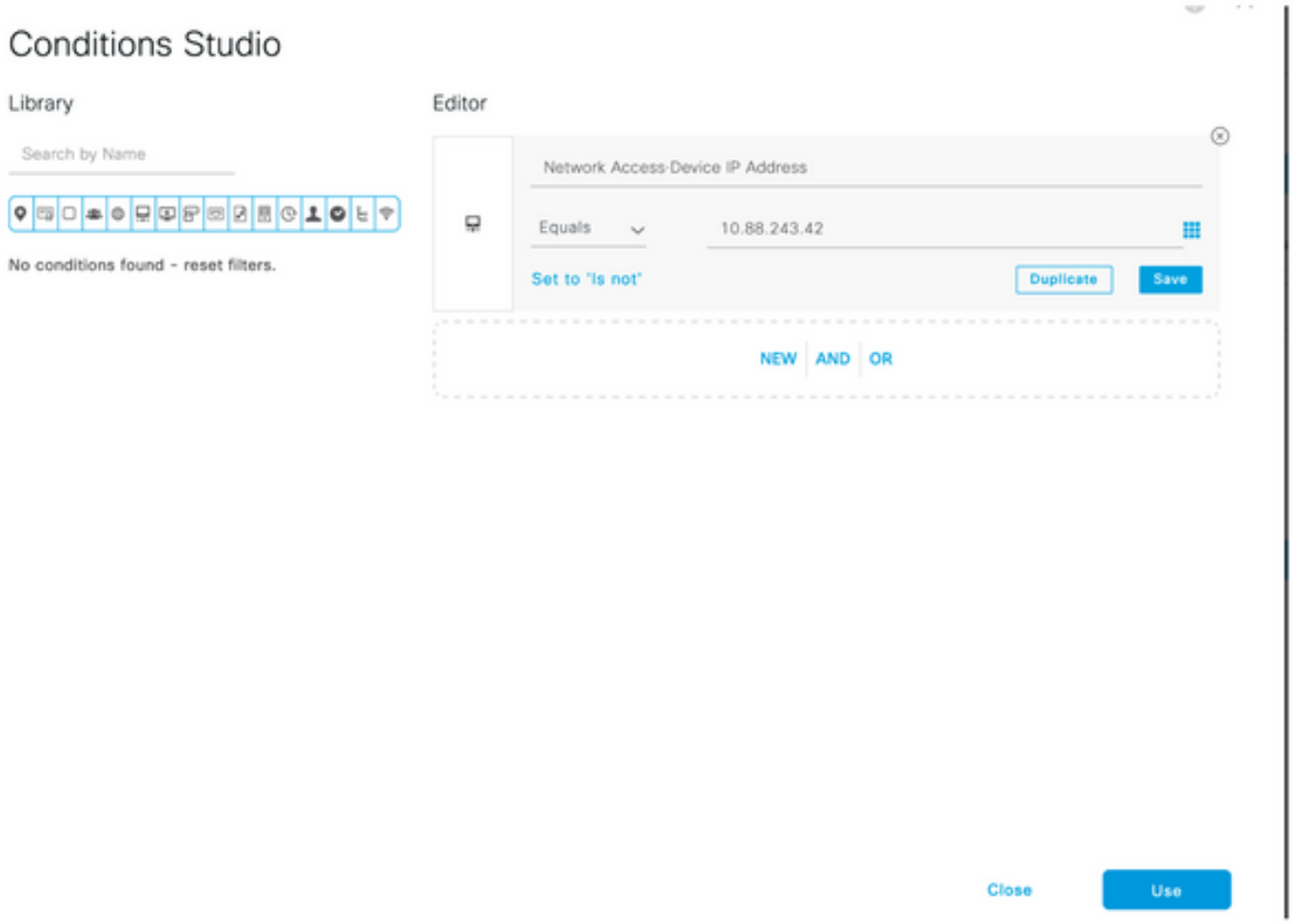


Stap 8. Selecteer het pictogram drie regels in de linker bovenhoek en navigeer naar **Administratie-**

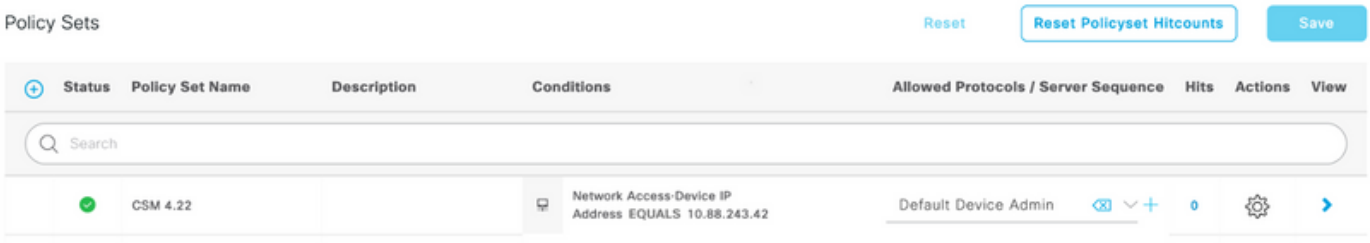
>Apparaatbeheer->Beleidssets voor apparaatbeheer. Selecteren  Hieronder staat de titel Policy Sets, definieer een naam en selecteer de knop **+** in het midden om een nieuwe voorwaarde toe te voegen.



Stap 9. Selecteer onder het venster conditionering een eigenschap toevoegen en selecteer vervolgens **het** pictogram **Netwerkapparaat**, gevolgd door het IP-adres van het netwerktoegangsapparaat. Selecteer **Waarde van** eigenschappen en voeg het CSM IP-adres toe. Selecteer **Gebruik** als u klaar bent.



Stap 10. Selecteer onder het gedeelte Protocollen toestaan de optie **Apparaatstandaardinstellingen**. Selecteer **Opslaan**



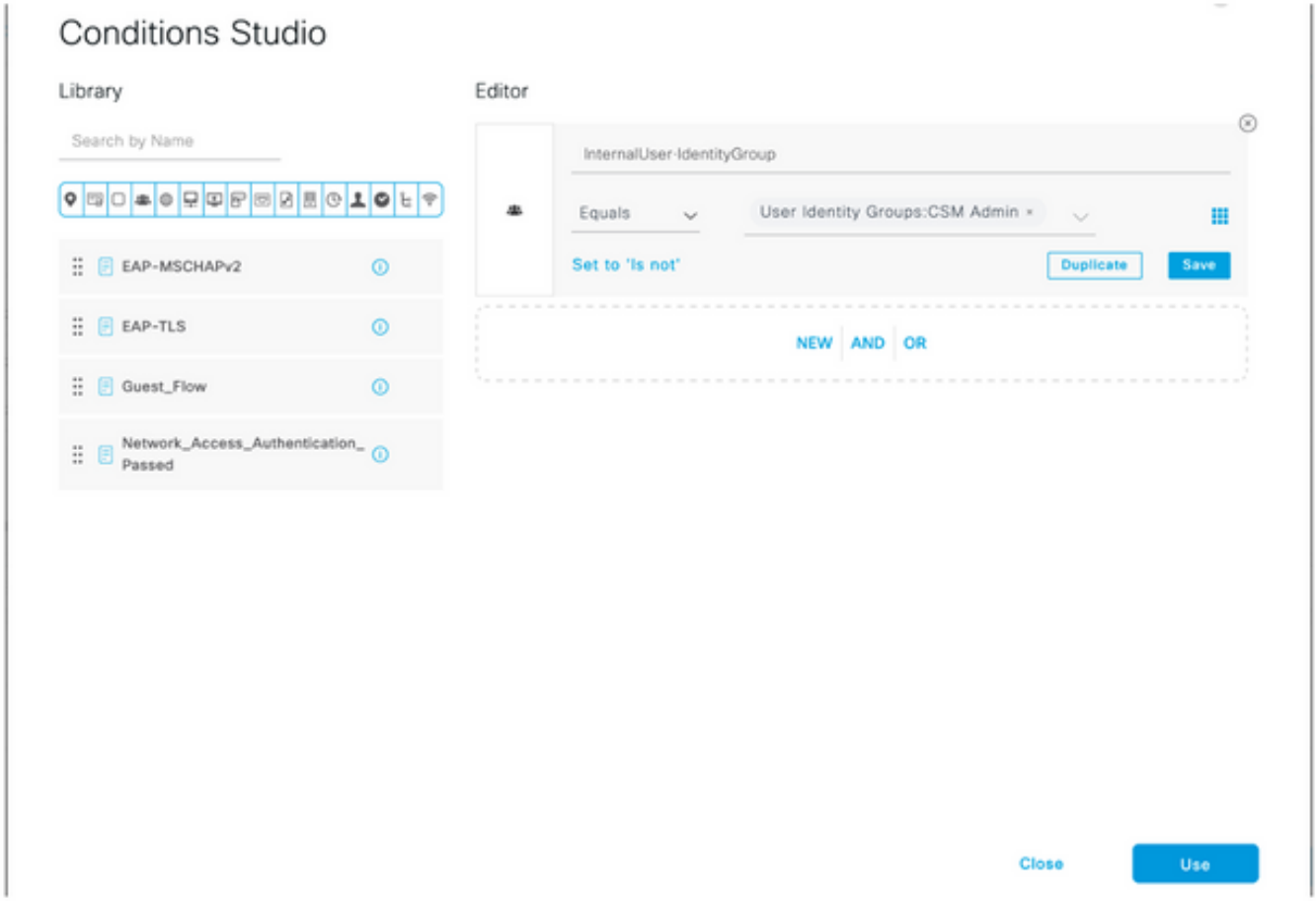
Stap 1. Selecteer de juiste pijl pictogram van het beleidskader dat is ingesteld om het echtheids- en autorisatiebeleid te definiëren

Stap 12. Selecteer Hieronder vindt u een naam voor verificatiebeleid. Selecteer vervolgens een naam en selecteer de optie + in het midden om een nieuwe voorwaarde toe te voegen. Selecteer onder het venster Condition een eigenschap toevoegen en selecteer vervolgens het pictogram **Netwerkapparaat**, gevolgd door het IP-adres van het netwerktoegangsapparaat. Selecteer **Waarde van** eigenschappen en voeg het CSM IP-adres toe. Selecteer **Gebruik** als u klaar bent

Stap 13. Selecteer **Interne** gebruikers als Identity Store en selecteer **Opslaan**

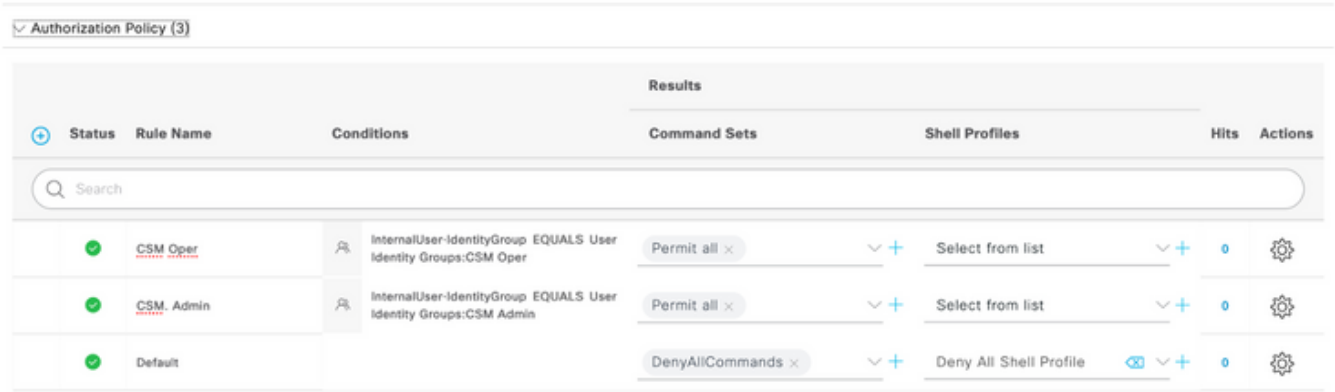
Opmerking: Identity Store kan worden gewijzigd in AD-winkel als ISE is aangesloten op een actieve map.

Stap 14. Selecteer Voer onder de titel Automation Policy een naam in en selecteer de knop **+** in het midden om een nieuwe voorwaarde toe te voegen. Selecteer onder het venster conditioner een eigenschap toevoegen en selecteer vervolgens **het** pictogram **Identity Group**, gevolgd door **Interne gebruiker: Identiteitsgroep.** Selecteer de CSM Admin Group en selecteer **Gebruik**.



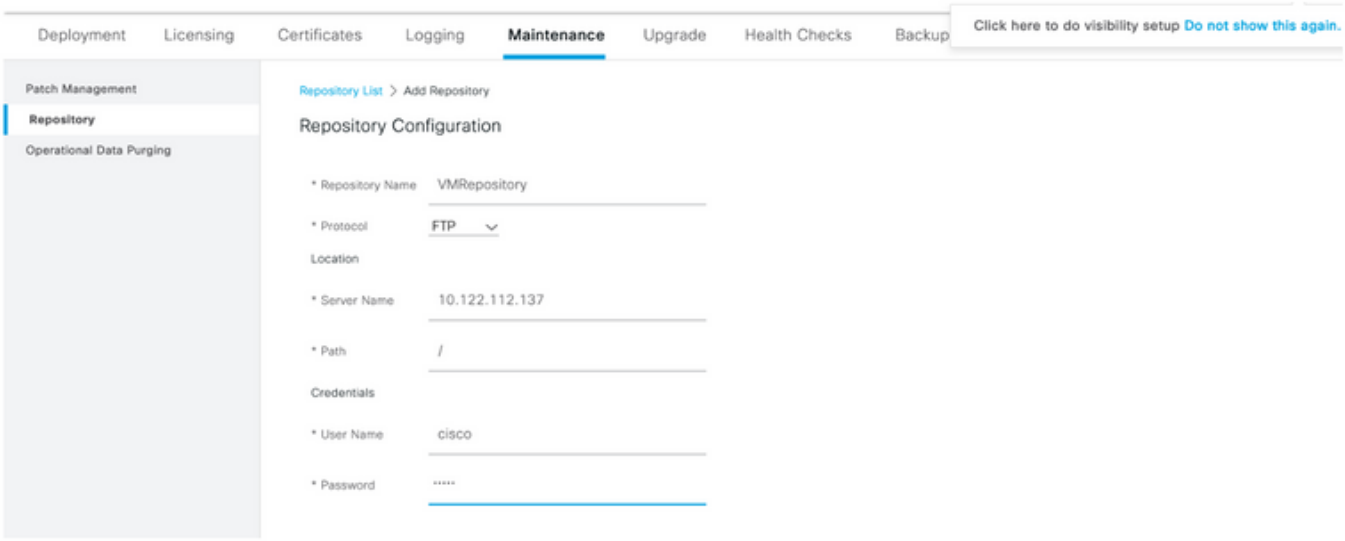
Stap 15. Selecteer onder Opdrachtset alle opdracht toestaan die in Stap 7 is gemaakt en selecteer **Opslaan**

Stap 14 en 15 herhalen voor de CSM-groep



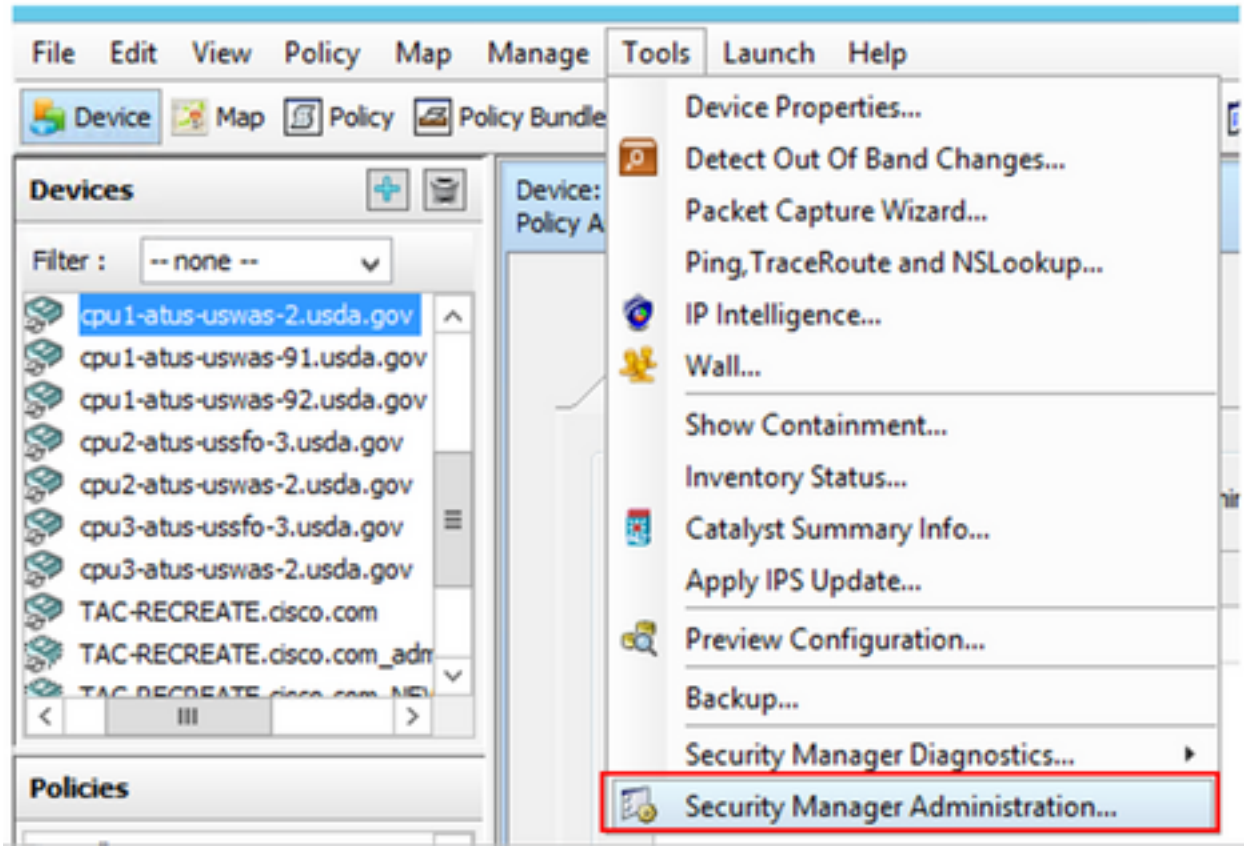
Stap 16 (optioneel). Selecteer het pictogram drie regels in de linker bovenhoek en selecteer **Beheer>Onderhoud>Bedieningsgebied**, selecteer **+Add** om een opslagplaats toe te voegen die wordt gebruikt om TCP-pompbestand op te slaan voor probleemoplossing.

Stap 17 (optioneel). Defineert een opslagnaam, protocol, servernaam, pad en Credentials. Selecteer **Indienen** als dit eenmaal is gedaan.

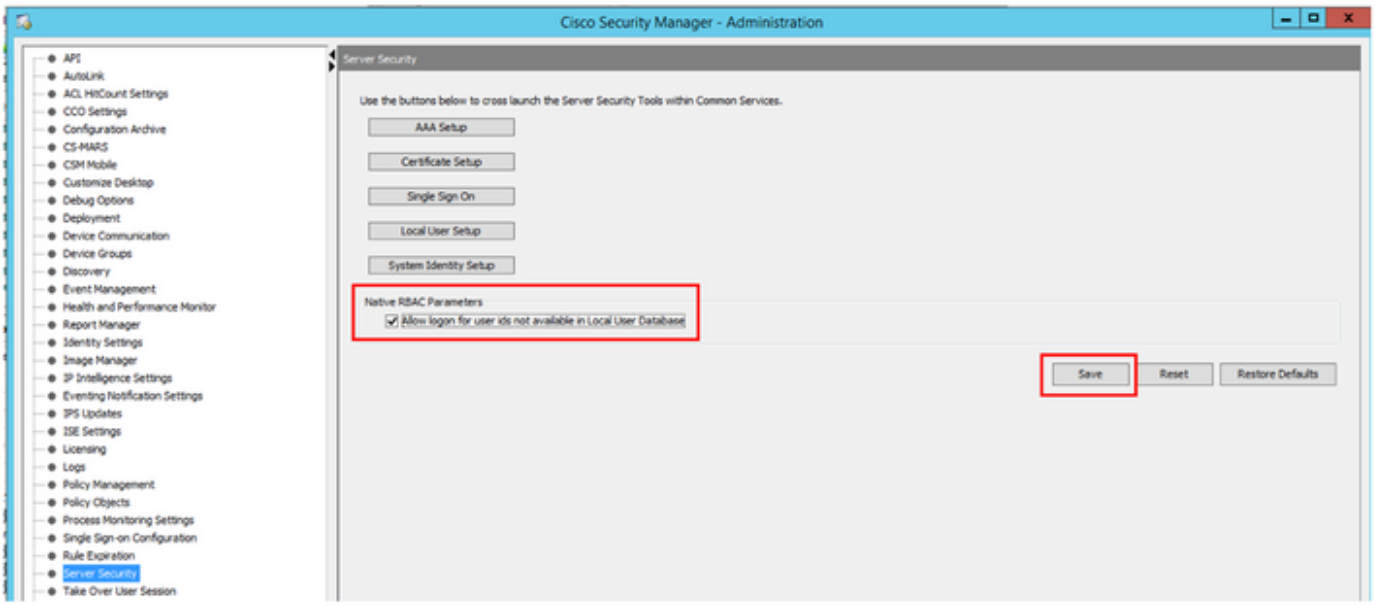


CSM-configuratie

Stap 1. Meld u aan bij de Cisco Security Manager-clienttoepassing met de lokale beheeraccount. In het menu navigeren naar **Gereedschappen > Beveiligingsbeheer**



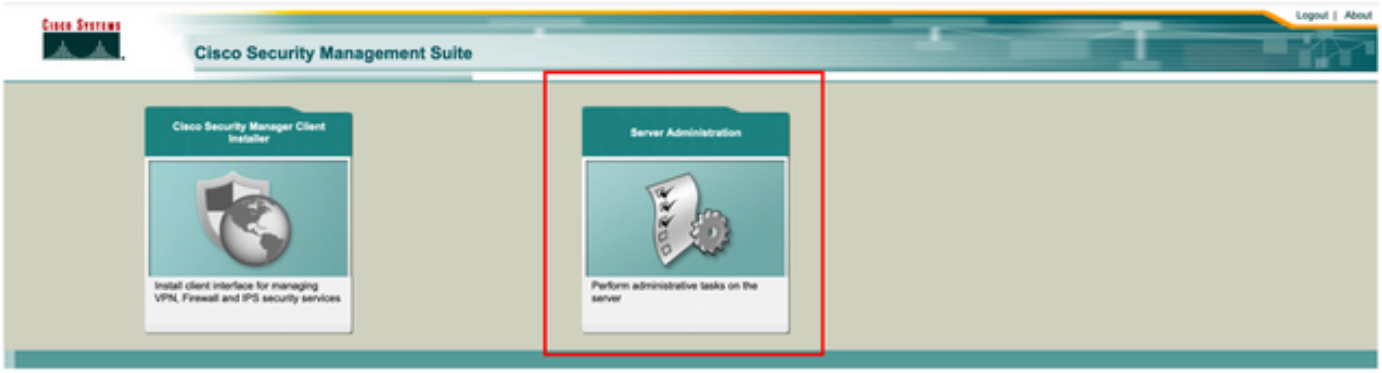
Stap 2. Controleer het vakje onder **Native RBAC-parameters.** Selecteer **Opslaan** en **Sluiten**



Stap 3. Selecteer in het menu **Bestand > Verzenden. Bestand > Indienen.**

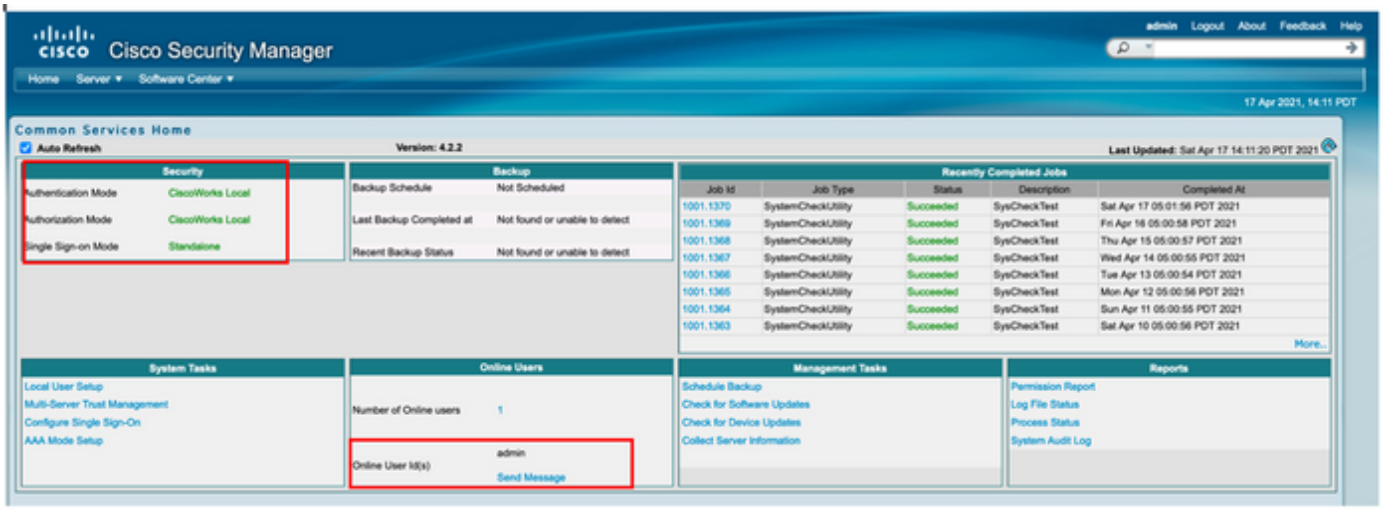
> **Opmerking:** Alle veranderingen moeten worden opgeslagen, in het geval van configuratieveranderingen die moeten worden voorgelegd en ingezet.

Stap 4. Navigeer naar CSM Management UI en type https://<enter_CSM_IP_Address en selecteer **Server Administration.**



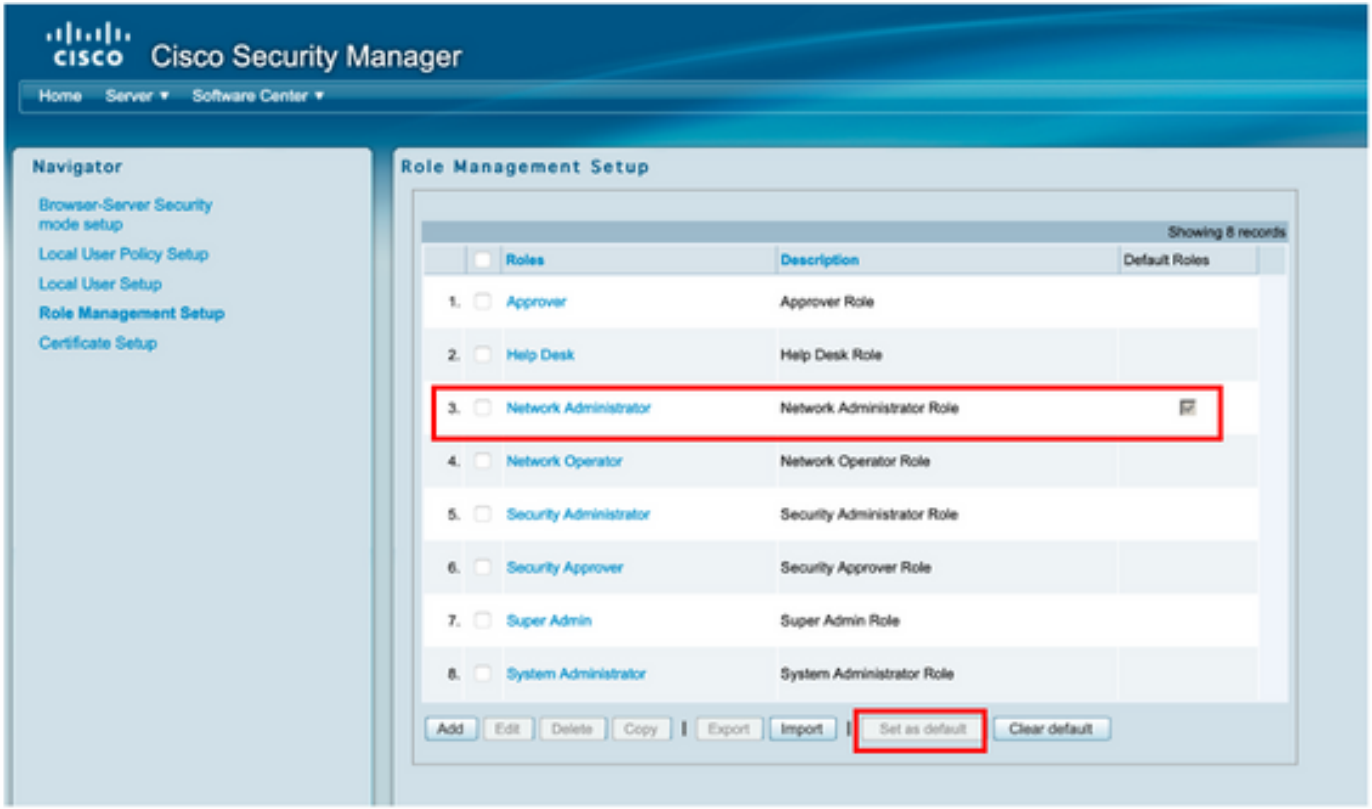
Opmerking: De stappen 4 tot 7 tonen de procedure om de standaardrol voor alle beheerders te definiëren die niet op ISE worden bepaald. Deze stappen zijn optioneel.

Stap 5. Verifieer de verificatiemodus op **CiscoWorks Local** en **Online** userID is de lokale admin-account die op CSM is gemaakt.



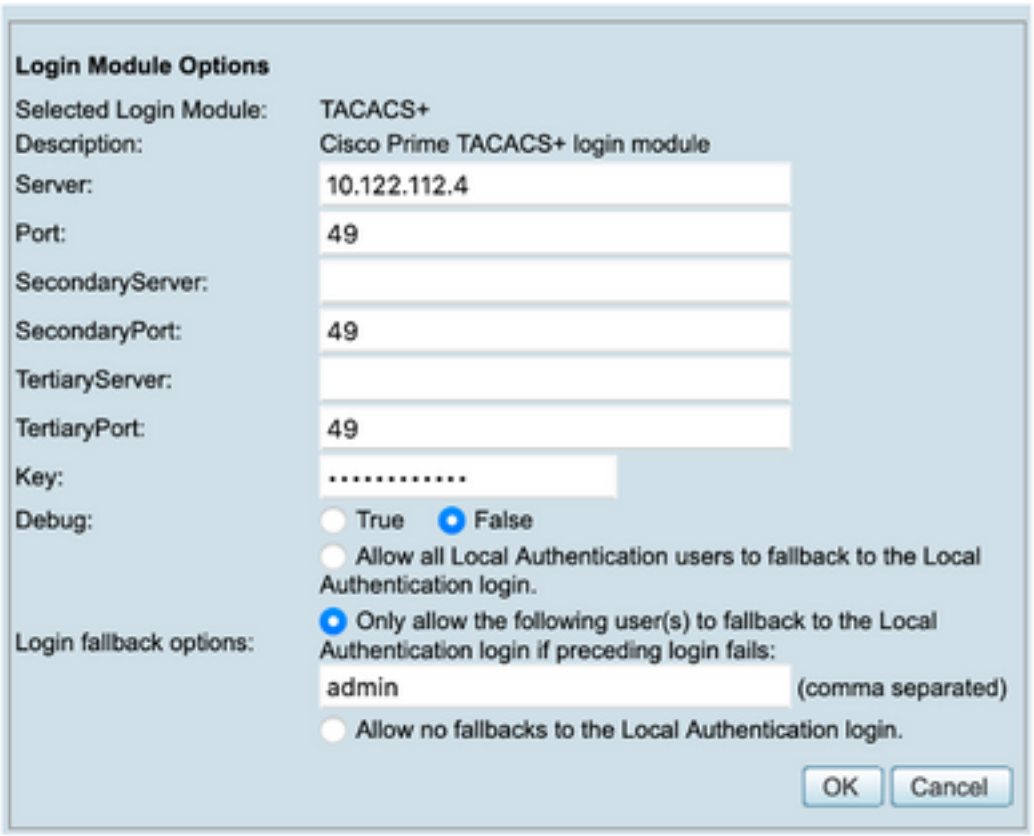
Stap 6. Navigeer naar **server** en selecteer **Beheer met één server**

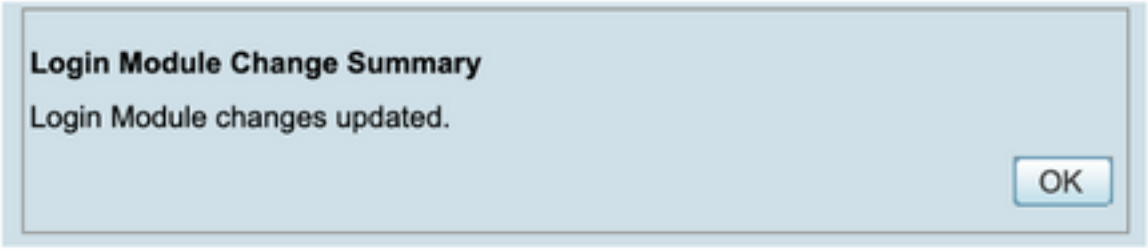
Stap 7. Selecteer de optie Rollend beheer instellen en selecteer het standaardrecht dat alle beheergebruikers bij verificatie ontvangen. U kunt bijvoorbeeld de netwerkbeheerder gebruiken. Nadat u deze optie hebt geselecteerd, selecteert u **deze standaard.**



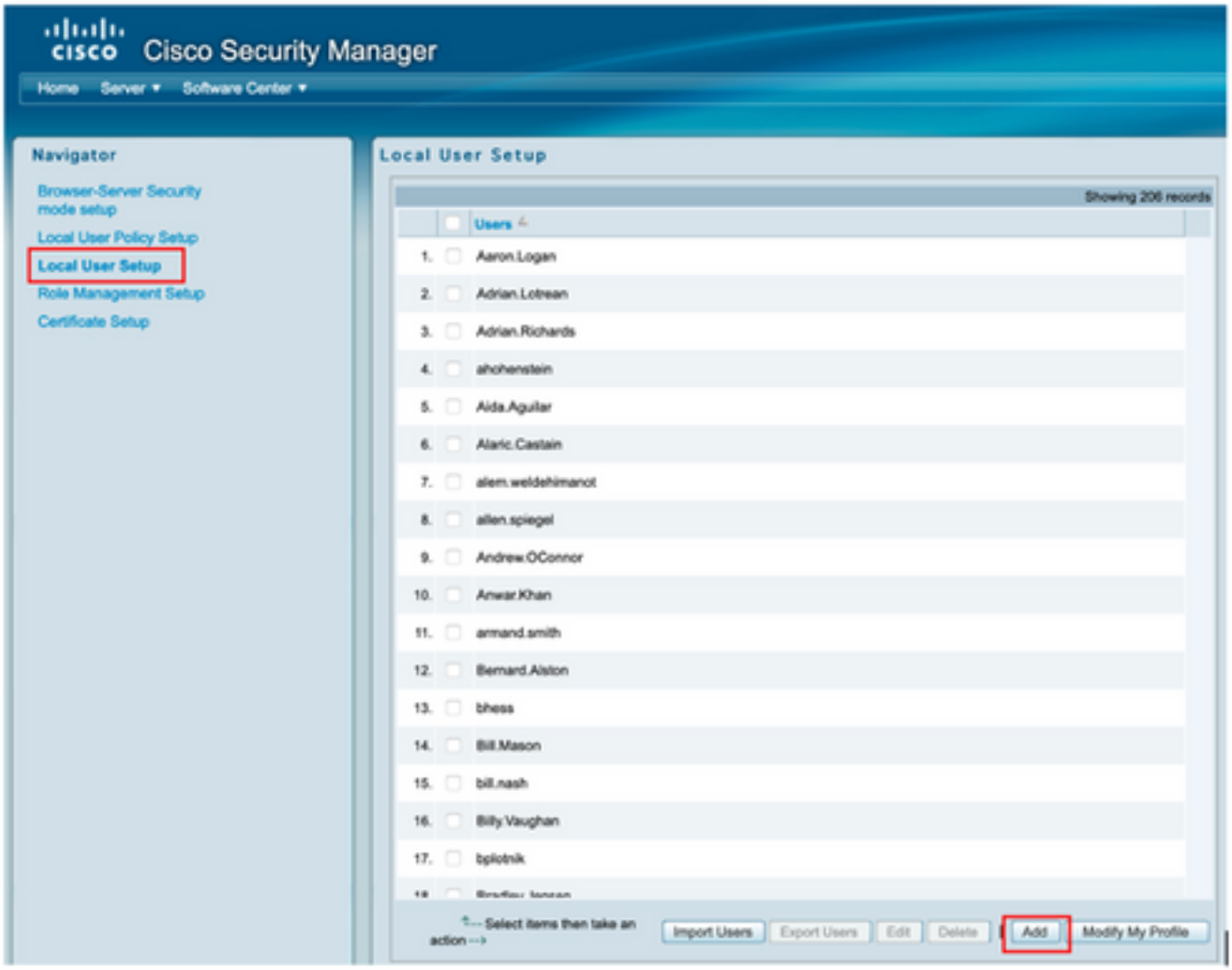
Stap 8. Selecteer **Server>Setup-rol AAA-modus** en selecteer vervolgens **TACACS+** optie **wijzigen en** ISE-informatie toevoegen.

Stap 9. Defineer ISE IP-adres en -toets, kunt u naar keuze de optie selecteren om alle lokale authenticatiegebruikers of slechts één gebruiker toe te staan als het inloggen mislukt**.** Bij dit voorbeeld is de enige beheerder toegestaan als back-upmethode. Selecteer **OK** om de wijzigingen op te slaan.

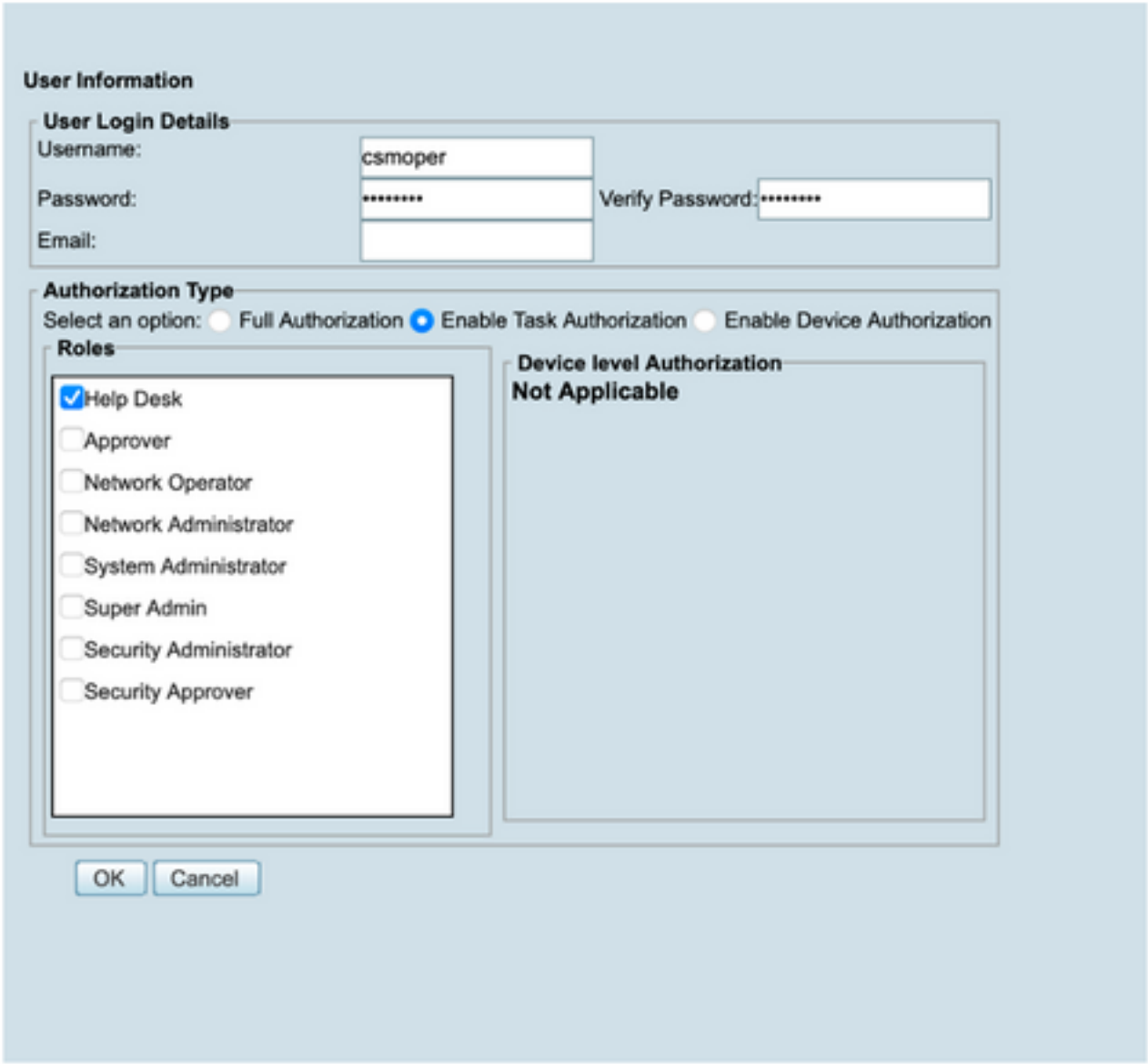




Stap 10. Selecteer **Server> Single Server Management** en selecteer vervolgens **Local User Setup** en selecteer **Add.**



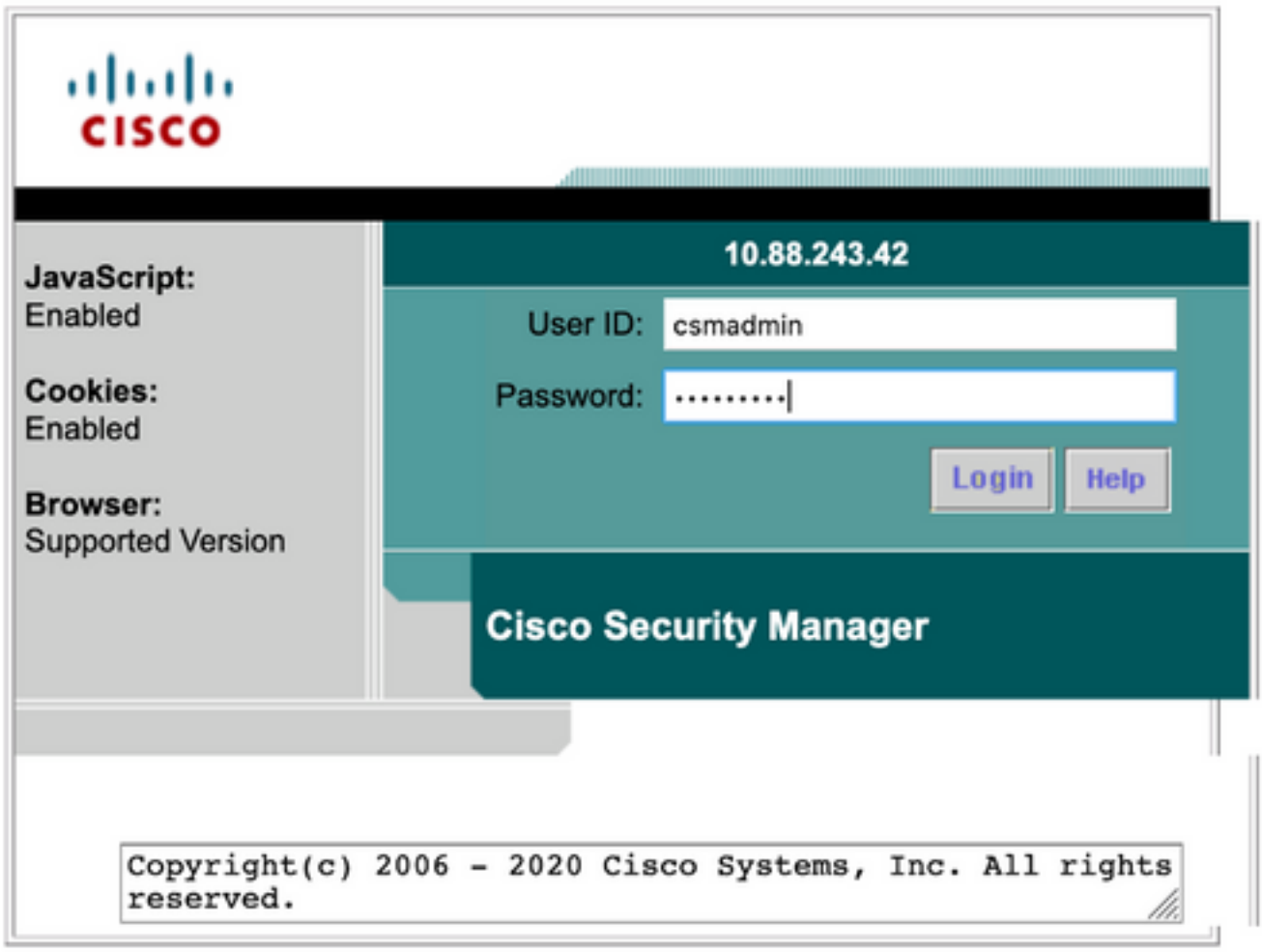
Stap 1. Defineer de zelfde gebruikersnaam en het wachtwoord die op ISE op stap 5 zijn gemaakt onder de ISE configuratie sectie, de rol van de **taakautorisatie van de Help-Desktop** worden gebruikt in dit voorbeeld. Selecteer **OK** om de beheerder op te slaan.



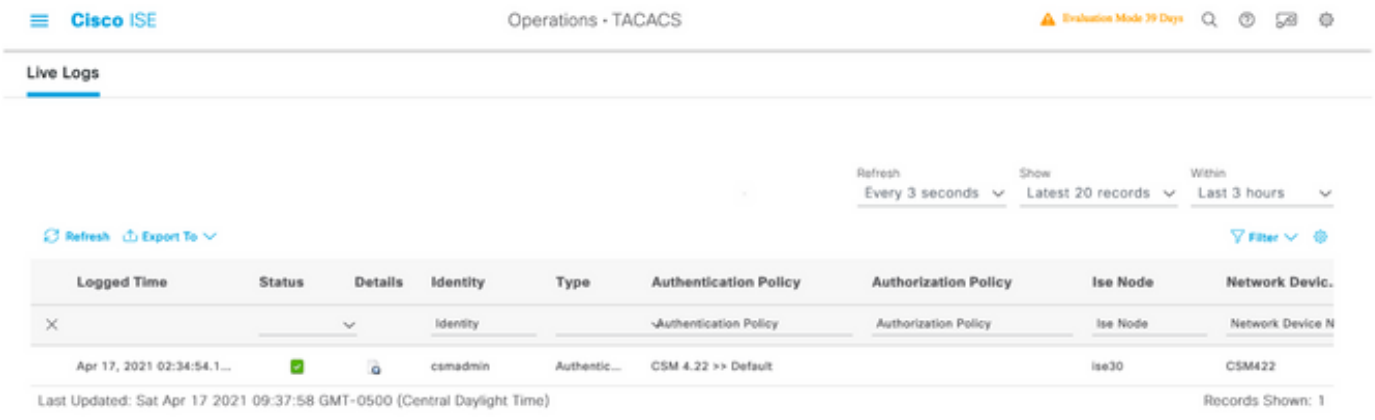
Verifiëren

Cisco Security Manager-client voor UI

Stap 1. Open een nieuwe browser van het venster en type https://<enter_CSM_IP_Address, gebruik csmadmin gebruikersnaam en wachtwoord die zijn gemaakt op stap 5 onder het configuratiescherm van ISE.



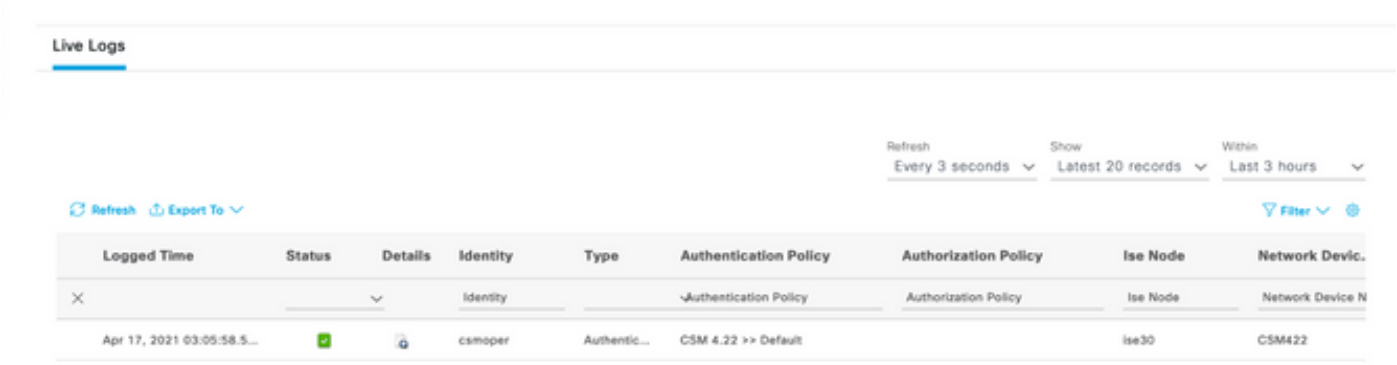
Succesvolle loggen in de poging kunnen worden geverifieerd op ISE TACACS-levende stammen



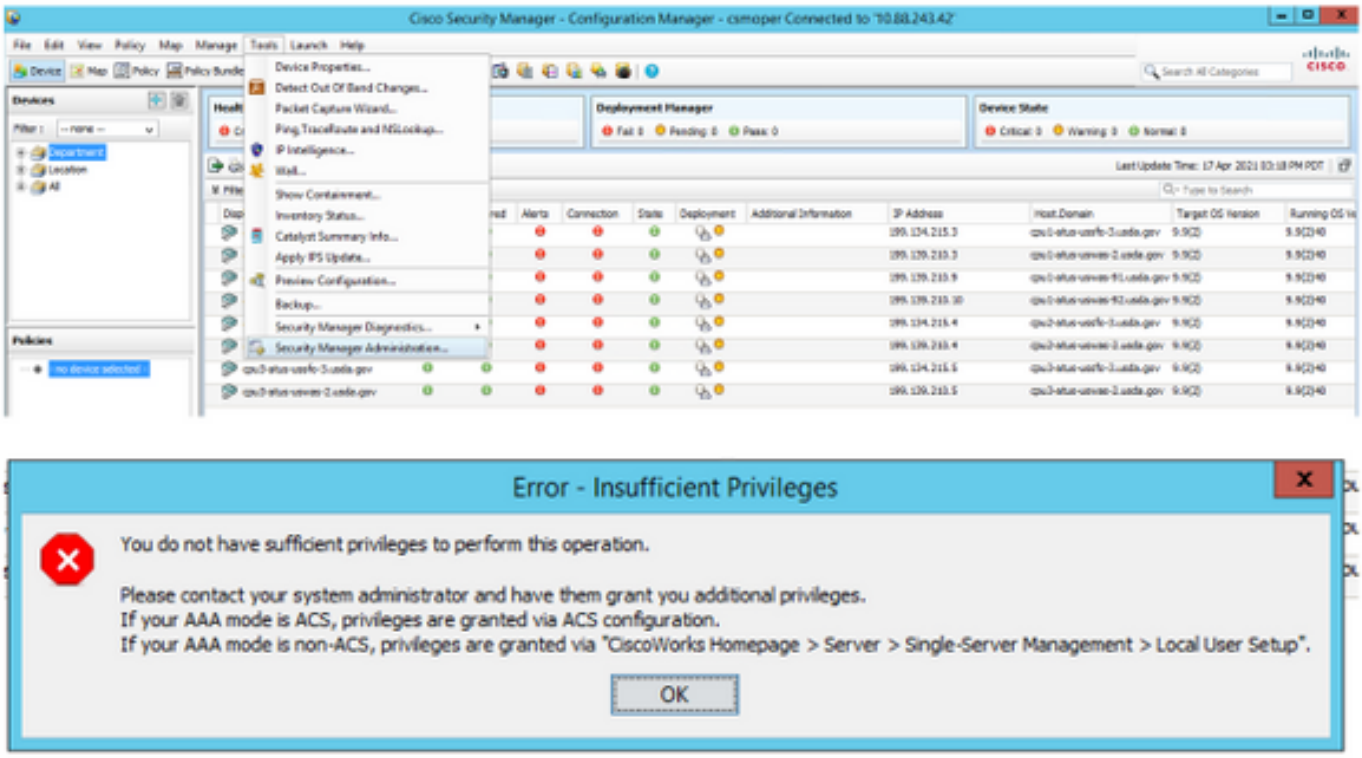
Cisco Security Manager-clienttoepassing

Stap 1. Meld u aan bij de Cisco Security Manager-clienttoepassing met de helpdesk Admin-account.

Succesvolle loggen in de poging kunnen worden geverifieerd op ISE TACACS-levende stammen



Stap 2. Selecteer **Gereedschappen > Security Manager-beheerprogramma** van de CSM-client en er verschijnt een foutbericht dat er geen rechten zijn.



Stap 3. Herhaal stappen 1 tot en met 3 met **csmadmin-**account om de juiste rechten te valideren, is aan deze gebruiker geleverd.

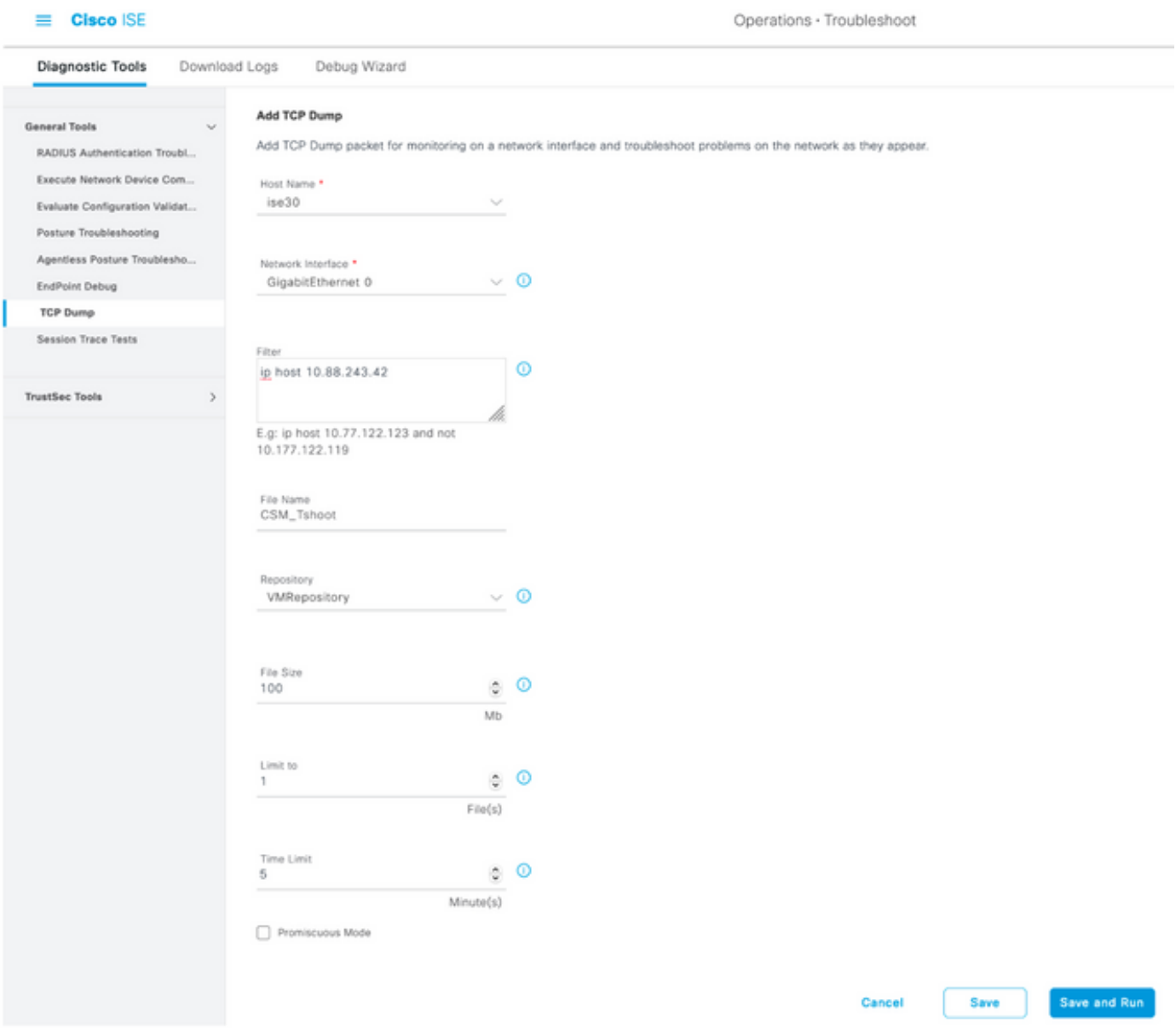
Problemen oplossen

Deze sectie verschaft de informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Communicatievalidatie met TCP-pomp op ISE

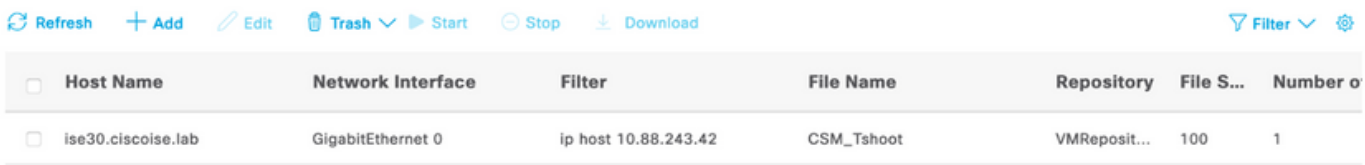
Stap 1. Meld u aan bij ISE en navigeer naar het pictogram drie regels in de linker bovenhoek en selecteer **Operations>Troubleshooter>Diagnostische tools.**

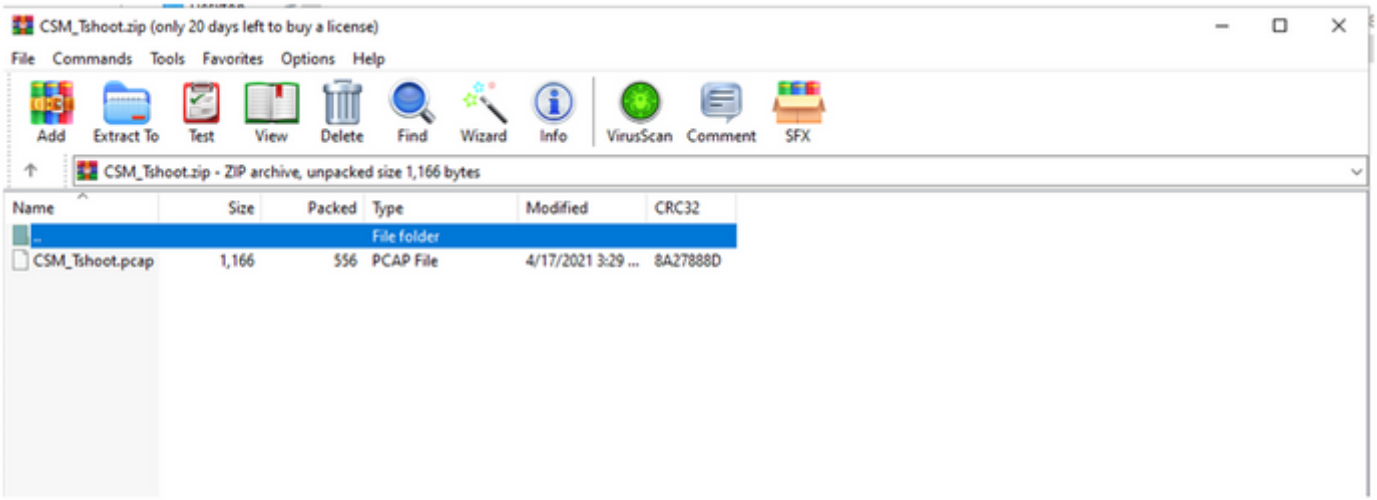
Stap 2. Selecteer onder **Algemene gereedschappen** de optie **TCP-pompen** en selecteer vervolgens **Add+.** Selecteer Hostname, de naam van het Netwerkinterfacebestand, de bestandsnaam en naar keuze een filter om alleen CSM IP-adrescommunicatiestroom te verzamelen. Selecteer **Opslaan en uitvoeren**



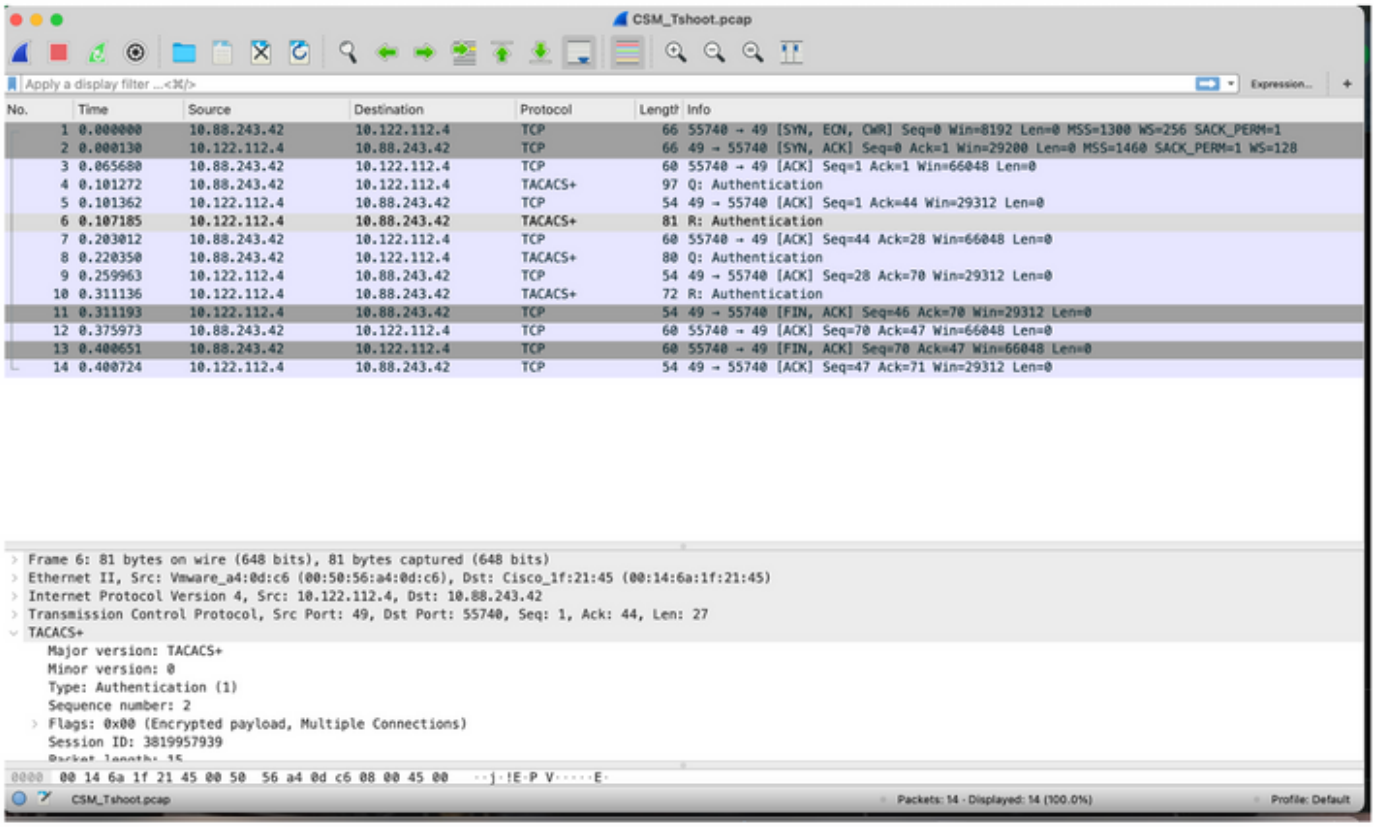
Stap 3. Meld u aan bij CSM-clienttoepassing of client-UI en typt u de admin-referenties.

Stap 4. Selecteer op ISE **de** knop **Stop** en controleer of het PDF-bestand naar de gedefinieerde opslaglocatie is verzonden.





Stap 5. Open het PDF-bestand om de succesvolle communicatie tussen CSM en ISE te valideren.



Als er geen items worden weergegeven in een cap-bestand, valideer dan het volgende:

1. Apparaatbeheerservice is ingeschakeld voor ISE-knooppunt
2. Rechts ISE IP-adres is toegevoegd aan de CSM-configuratie
3. Als er een firewall in het midden is, is poort 49 (TACACS) toegestaan.