Firepower eXtensible Operating System (FXOS) 2.2: Chassis verificatie/autorisatie voor extern beheer met ISE met behulp van TACACS+

Inhoud

Inleiding

Dit document beschrijft hoe u TACACS+ verificatie en autorisatie voor het FirePOWER Xtensible Operating System (FXOS) chassis via Identity Services Engine (ISE) kunt configureren.

Het FXOS-chassis bevat de volgende gebruikersrollen:

- Administrator - volledige toegang tot het volledige systeem voor lezen en schrijven. De standaard admin-account krijgt deze rol standaard toegewezen en kan niet worden gewijzigd.
- Alleen-lezen - alleen-lezen toegang tot de systeemconfiguratie zonder bevoegdheden om de systeemstatus te wijzigen.
- Operations - lees-en-schrijftoegang tot de NTP-configuratie, Smart Call Home-configuratie voor slimme licenties en systeemlogbestanden, inclusief systeemservers en fouten. Lees de toegang tot de rest van het systeem.
- AAA - lees-en-schrijf toegang tot gebruikers, rollen en AAA-configuratie. Lees de toegang tot de rest van het systeem.

Via CLI kan dit als volgt worden gezien:

fpr4120-TAC-A/security* # **rol**

Rol:

Functienaam Priv

— —

Aa aaa

beheerder

operaties

alleen-lezen

Bijgedragen door Tony Remirez, Jose Soto, Cisco TAC-engineers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van FirePOWER Xtensible Operating System (FXOS)
- Kennis van ISE-configuratie
- De licentie voor TACACS+ apparaatbeheer is vereist binnen ISE

Gebruikte componenten

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

- Cisco Firepower 4120 security applicatie versie 2.2
- Virtual Cisco Identity Services Engine 2.2.0.470

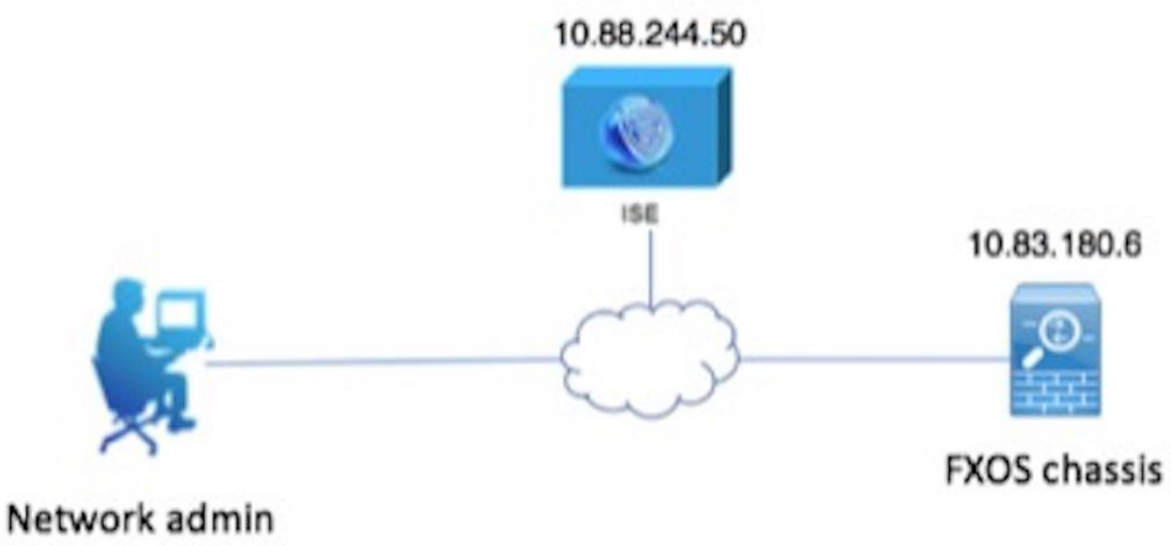
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Het doel van de configuratie is:

- Verifieer gebruikers die zich aanmelden in de op het web gebaseerde GUI en SSH van FXOS met behulp van ISE
- Geef gebruikers toestemming om te loggen in de op het web gebaseerde GUI en SSH van FXOS overeenkomstig hun respectieve gebruikersrol door middel van ISE.
- Controleer de goede werking van de echtheidscontrole en de vergunning op de FXOS door middel van ISE

Netwerkdiagram



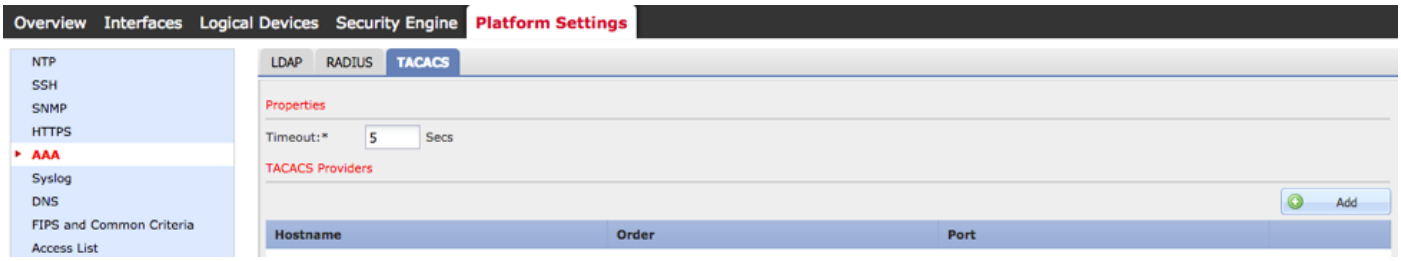
Configuraties

Het FXOS-chassis configureren

Een TACACS+ provider maken

Stap 1. Navigeer naar **platform instellingen > AAA.**

Stap 2. Klik op het tabblad **TACACS**.

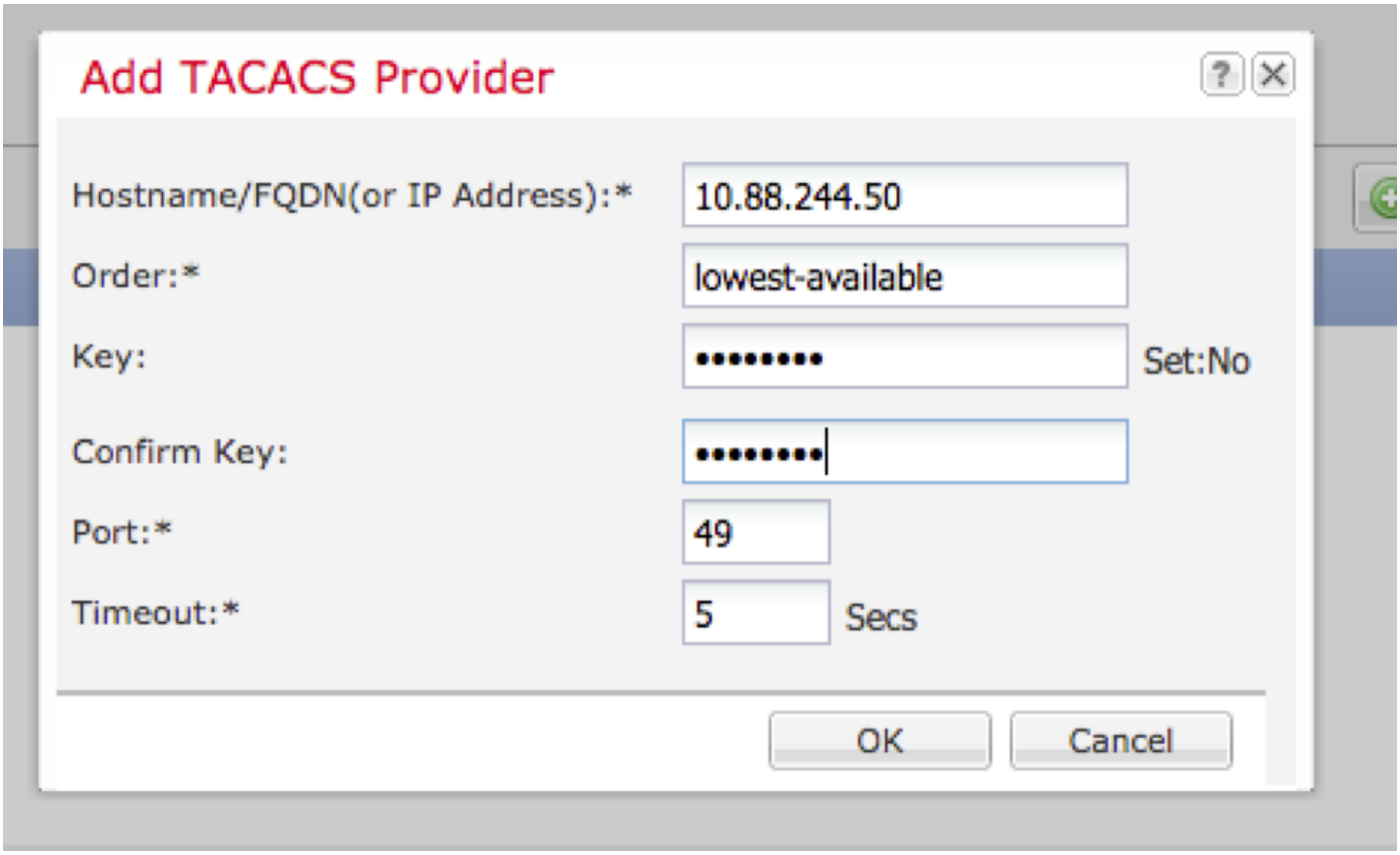


Stap 3. Voor elke TACACS+ provider die u wilt toevoegen (maximaal 16 providers).

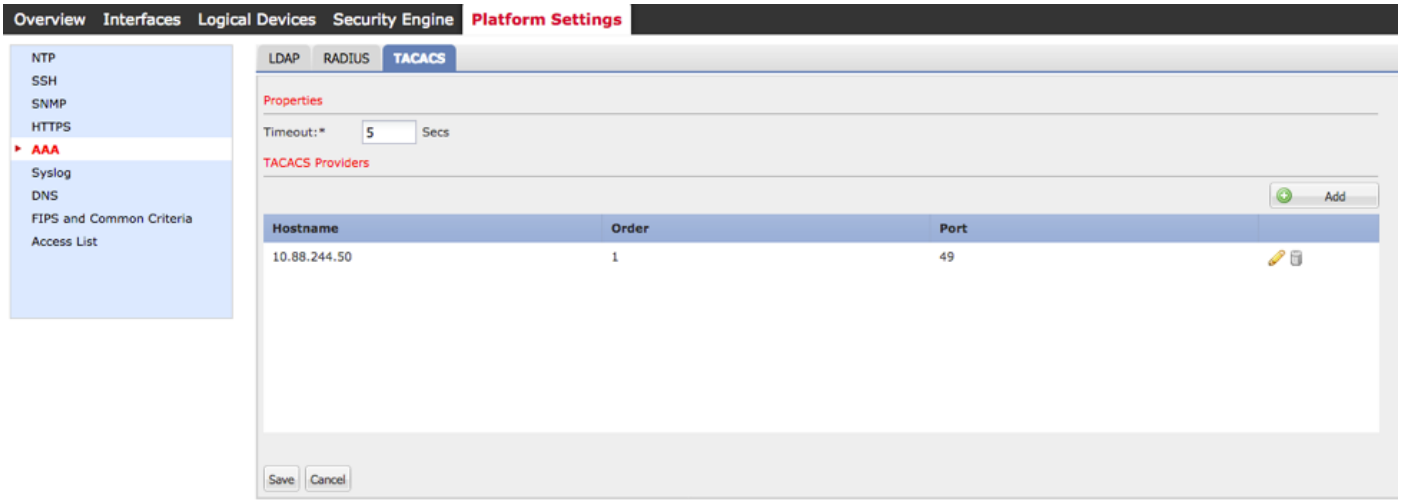
3.1. Klik in het gebied TACACS Providers op **Toevoegen.**

3.2. Zodra het dialoogvenster TACACS-providers wordt geopend, voert u de gewenste waarden in.

3.3. Klik op **OK** om het dialoogvenster Add TACACS Provider te sluiten.

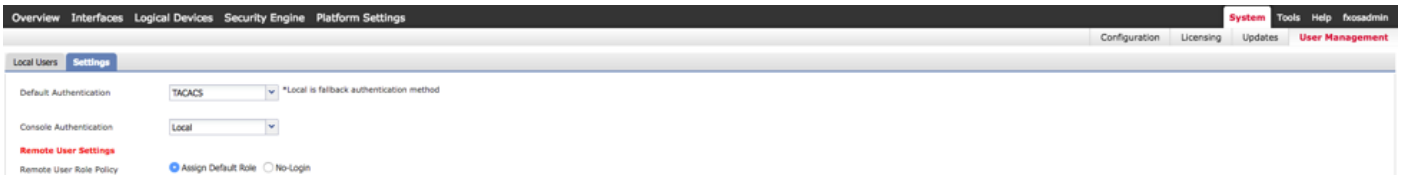


Stap 4. Klik op **Opslaan**.



Stap 5. Navigeer naar **Systeem > Gebruikersbeheer > Instellingen**.

Stap 6. Selecteer onder Standaardverificatie de optie **TACACS**.



Een TACACS+ provider maken met CLI

Stap 1. Om TACACS-verificatie mogelijk te maken, voert u de volgende opdrachten uit.

voor de **beveiliging** van 4120-TAC-A# **bereik**

fpr4120-TAC-A/security **#bereik: standaardinstelling**

fpr4120-TAC-A/security/default-auth **#set-realm-tac's**

Stap 2. Gebruik de opdracht **Details** tonen om de configuratie te controleren.

fpr4120-TAC-A/security/default-auth # **details laten zien**

Standaardverificatie:

Admin Realm: **Tacacs**

Operationeel antwoord: **Tacacs**

Web sessie verfrissing periode (in seconden): 600

Session timeout (in s) voor web-, ssh-, telnet-sessies: 600

Absolute sessietijd (in seconden) voor web-, ssh-, telnet-sessies: 3600

Seriële console-sessietijd (in seconden): 600

Seriële console absolute sessietijd (in seconden): 3600

Admin-servergroep:

Vak Operationele verificatieserver:

Gebruik van de tweede factor: Nee

Stap 3. Om de TACACS-serverparameters te configureren voert u de volgende opdrachten uit.

voor de **beveiliging** van 4120-TAC-A# **bereik**

fr4120-TAC-A/security # **tac-werkingssfeer**

fpr4120-TAC-A/security/tacacs # **server 10.8.244.50**

fpr4120-TAC-A/security/tacacs/server # **ingestelde "ACS-server"**

fpr4120-TAC-A/security/tacacs/server* # **ingestelde toets**

Geef de toets op: ******

Bevestig de toets: ******

Stap 4. Gebruik de opdracht **detail tonen** om de configuratie te controleren.

fpr4120-TAC-A/security/tacacs/server* # **details laten zien**

TACACS+ server:

Hostname, FQDN of IP-adres: 10.88.244.50

Descr:

Volgorde: 1

Port: 49

Sleutel: ****

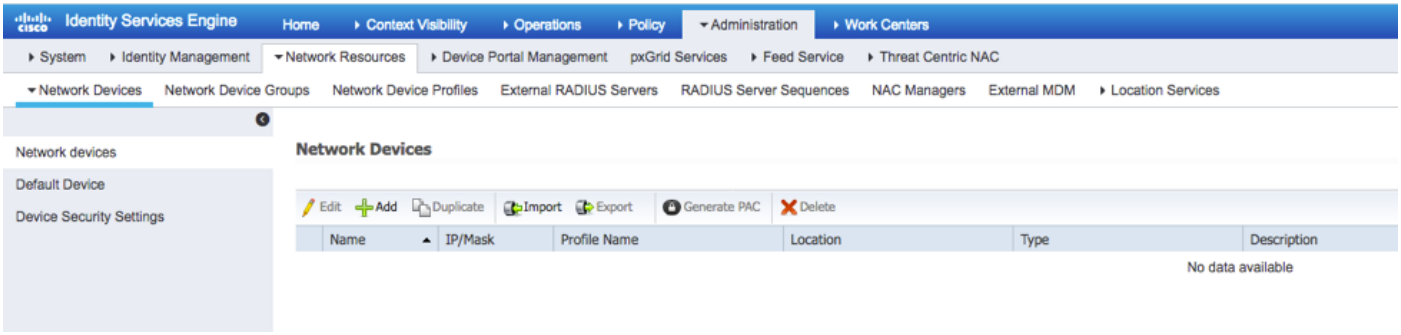
Time-out: 5

De ISE-server configureren

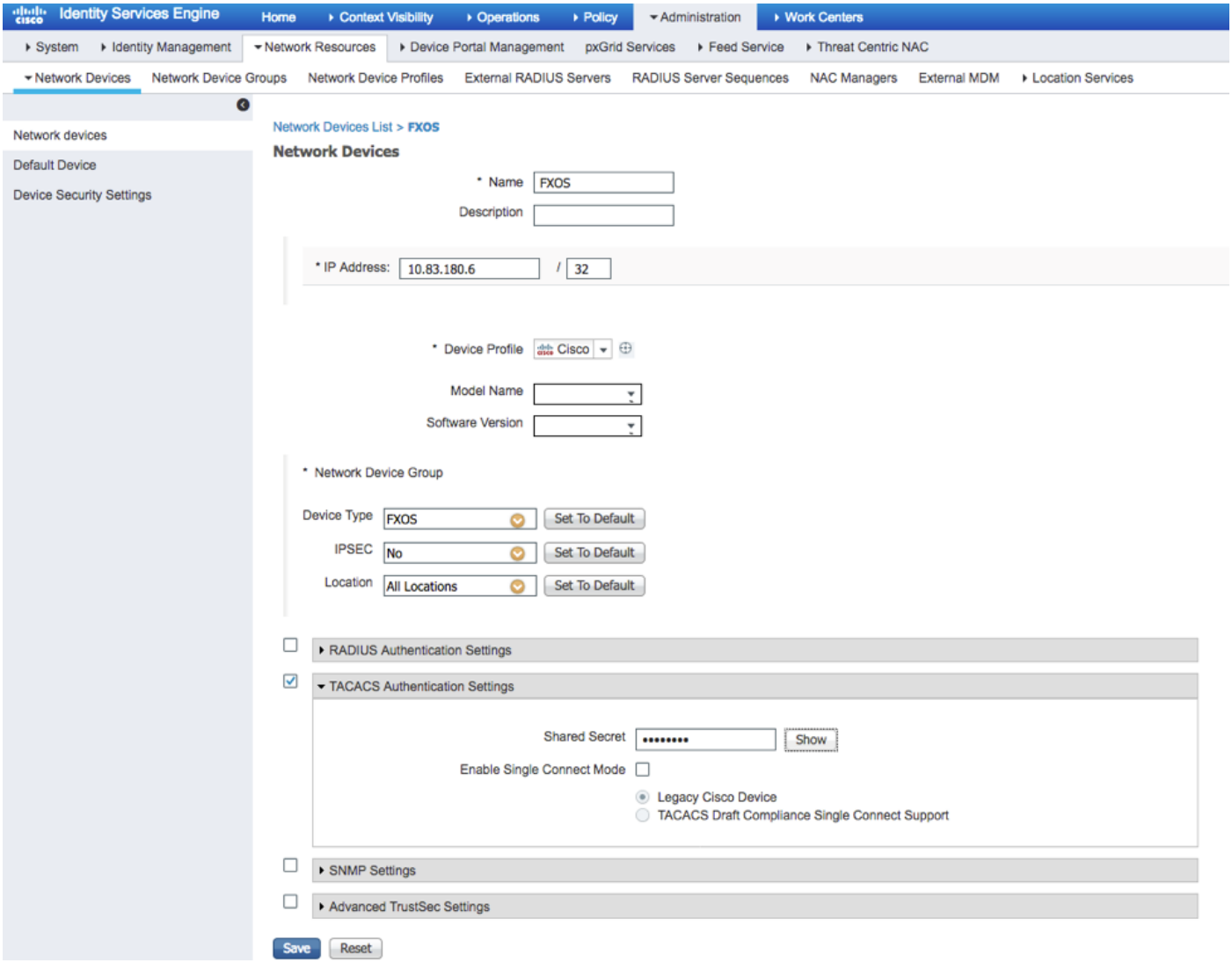
De FXOS als netwerkresource toevoegen

Stap 1. Navigeer naar **Beheer > Netwerkbronnen > Netwerkapparaten**.

Stap 2. Klik op **ADD.**



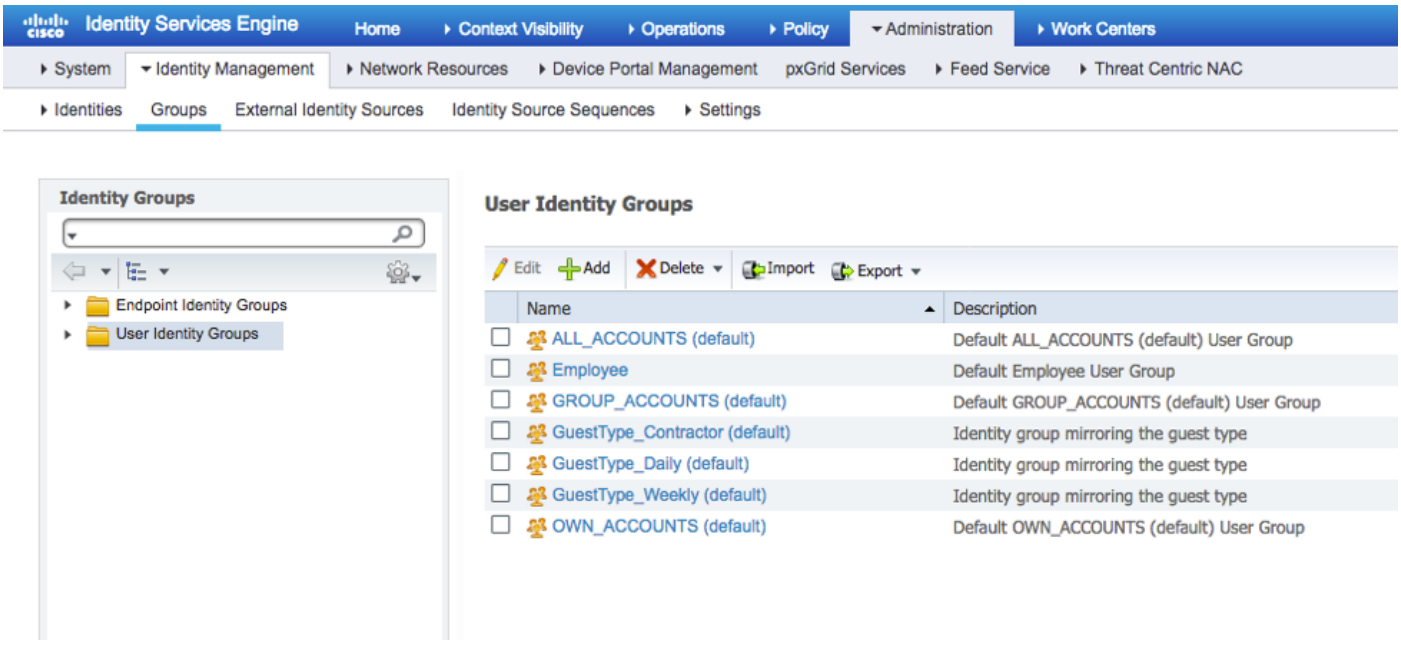
Stap 3. Voer de gewenste waarden in (Naam, IP-adres, Type apparaat en TACACS+ inschakelen en voeg de SLEUTEL toe) en klik op **Indienen.**



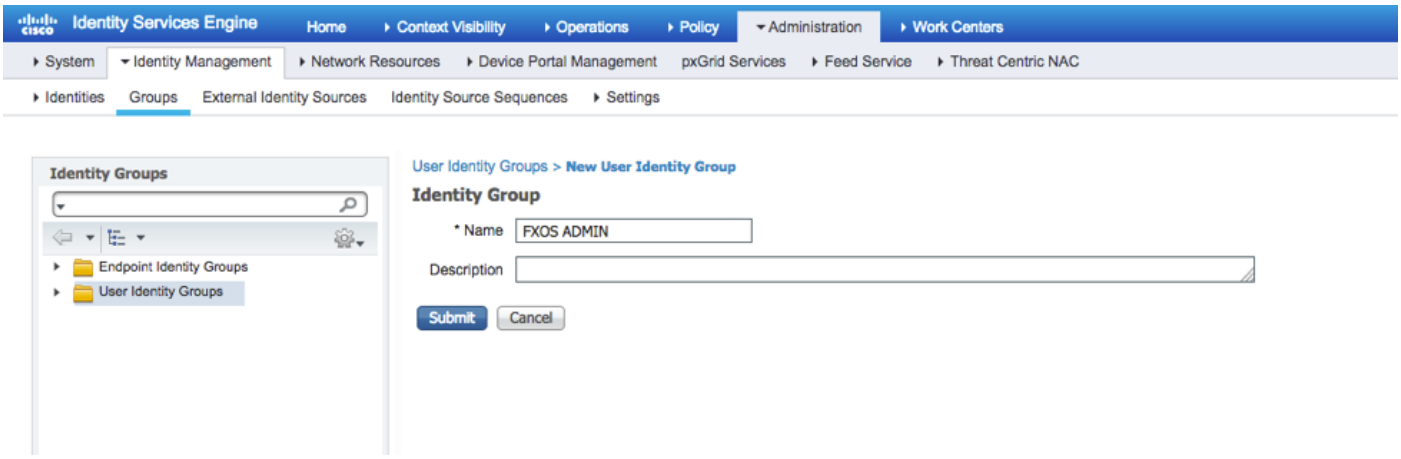
Identiteitsgroepen en gebruikers maken

Stap 1. Navigeer naar **Administratie > identiteitsbeheer > Groepen > Gebruikersidentiteitsgroepen.**

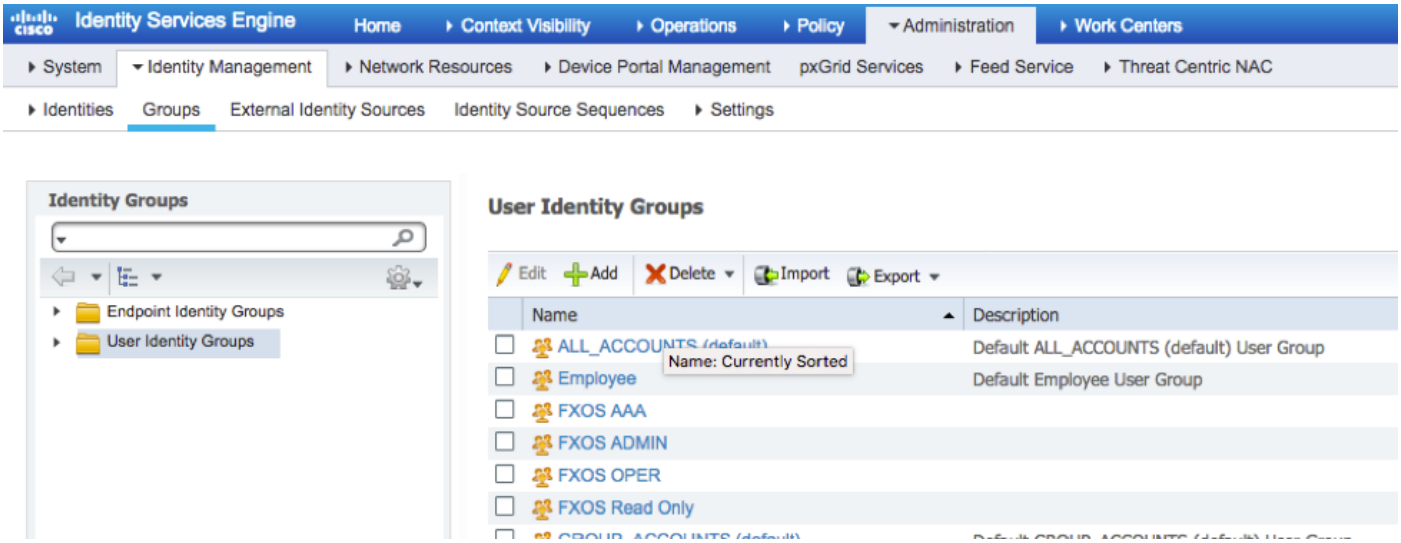
Stap 2. Klik op **ADD.**



Stap 3. Voer de waarde voor Naam in en klik op **Indienen.**

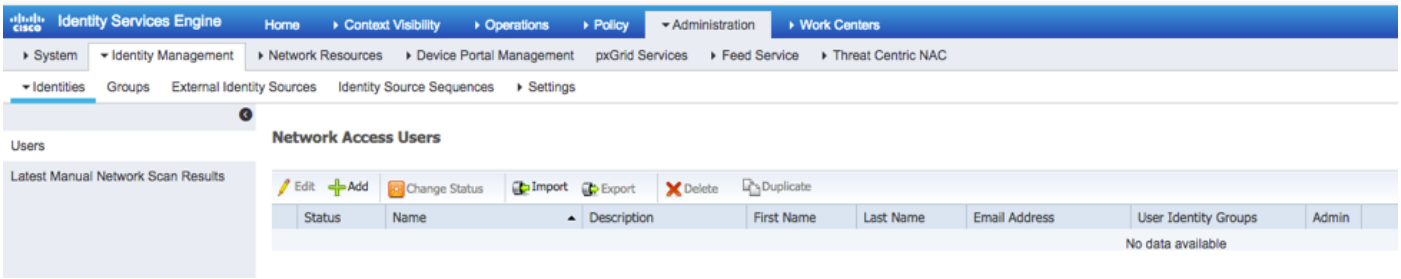


Stap 4. Herhaal stap 3 voor alle vereiste gebruikersrollen.

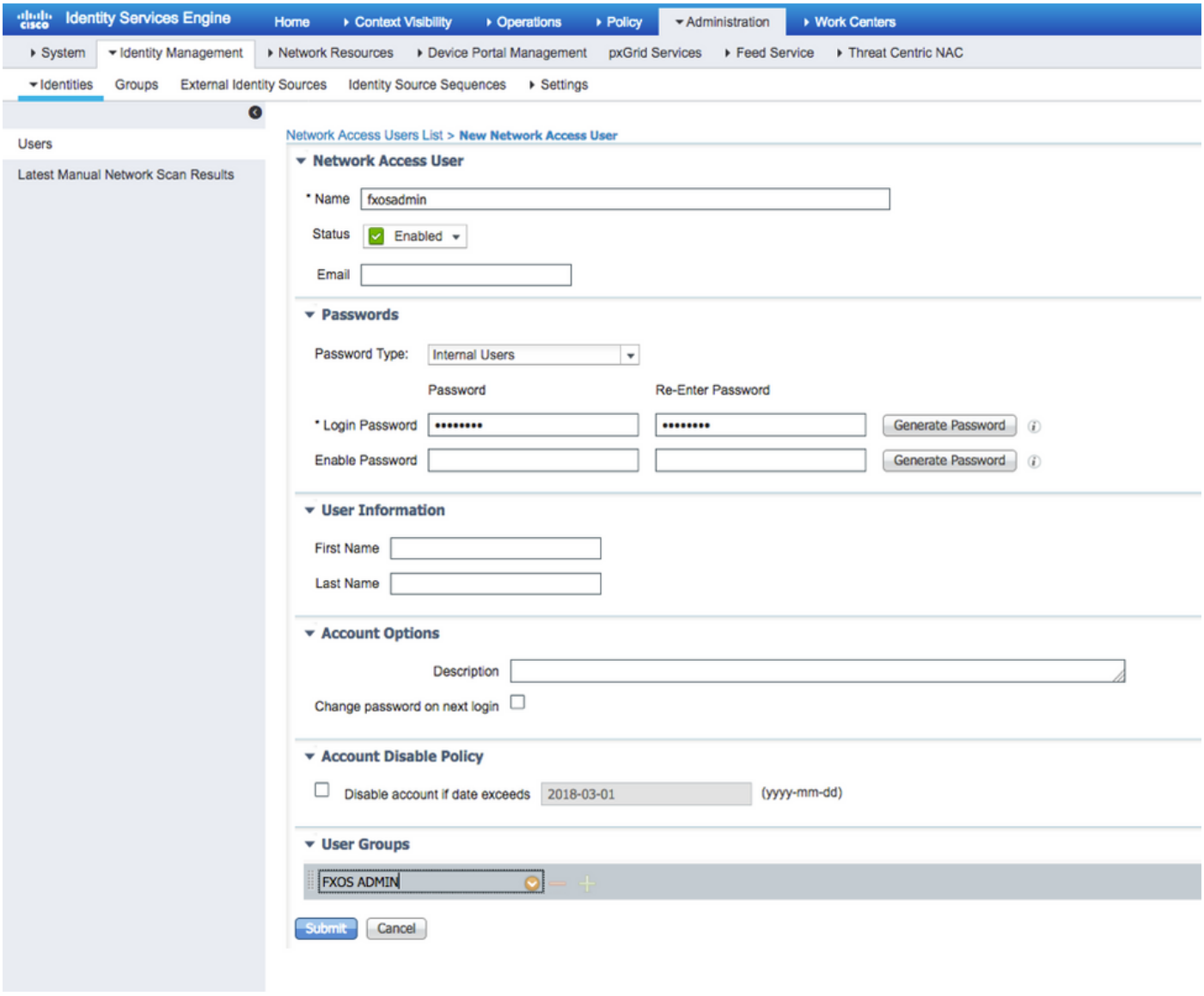


Stap 5. Navigeer naar **Administratie > Identity Management > Identity > Gebruikers.**

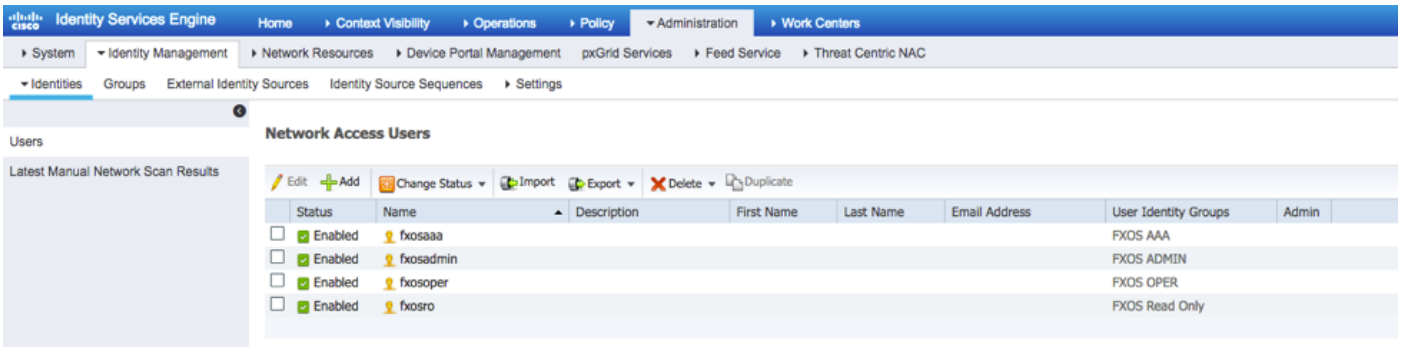
Stap 6. Klik op **ADD.**



Stap 7. Voer de gewenste waarden in (naam, gebruikersgroep, wachtwoord).

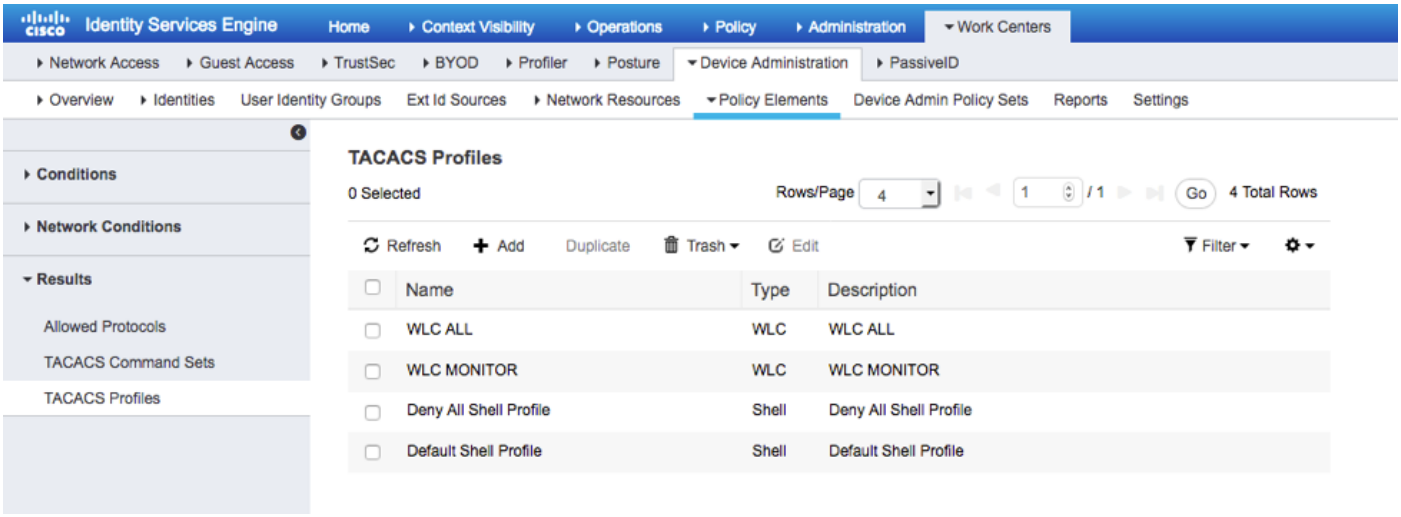


Stap 8. Herhaal stap 6 voor alle vereiste gebruikers.



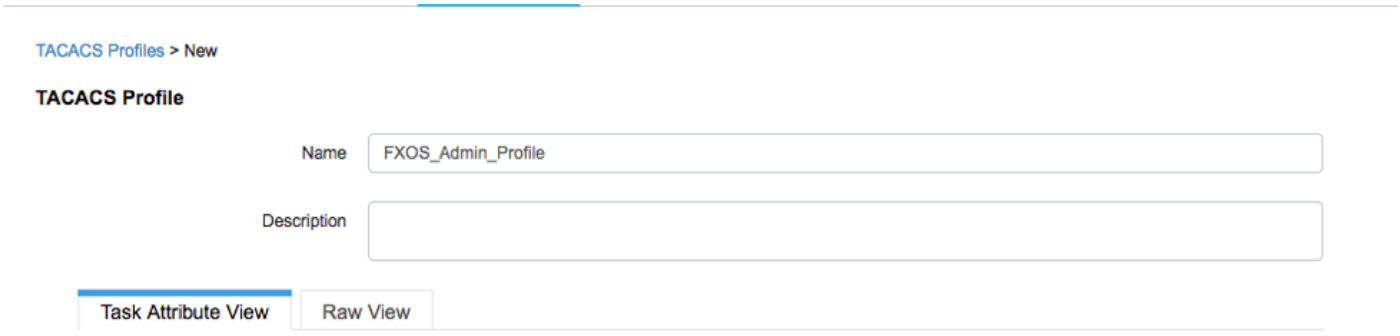
Het Shell-profiel maken voor elke gebruikersrol

Stap 1. Navigeer naar **werkcentra > Apparaatbeheer > Beleidselementen > Resultaten > TACACS-profielen** en klik op **+ADD.**



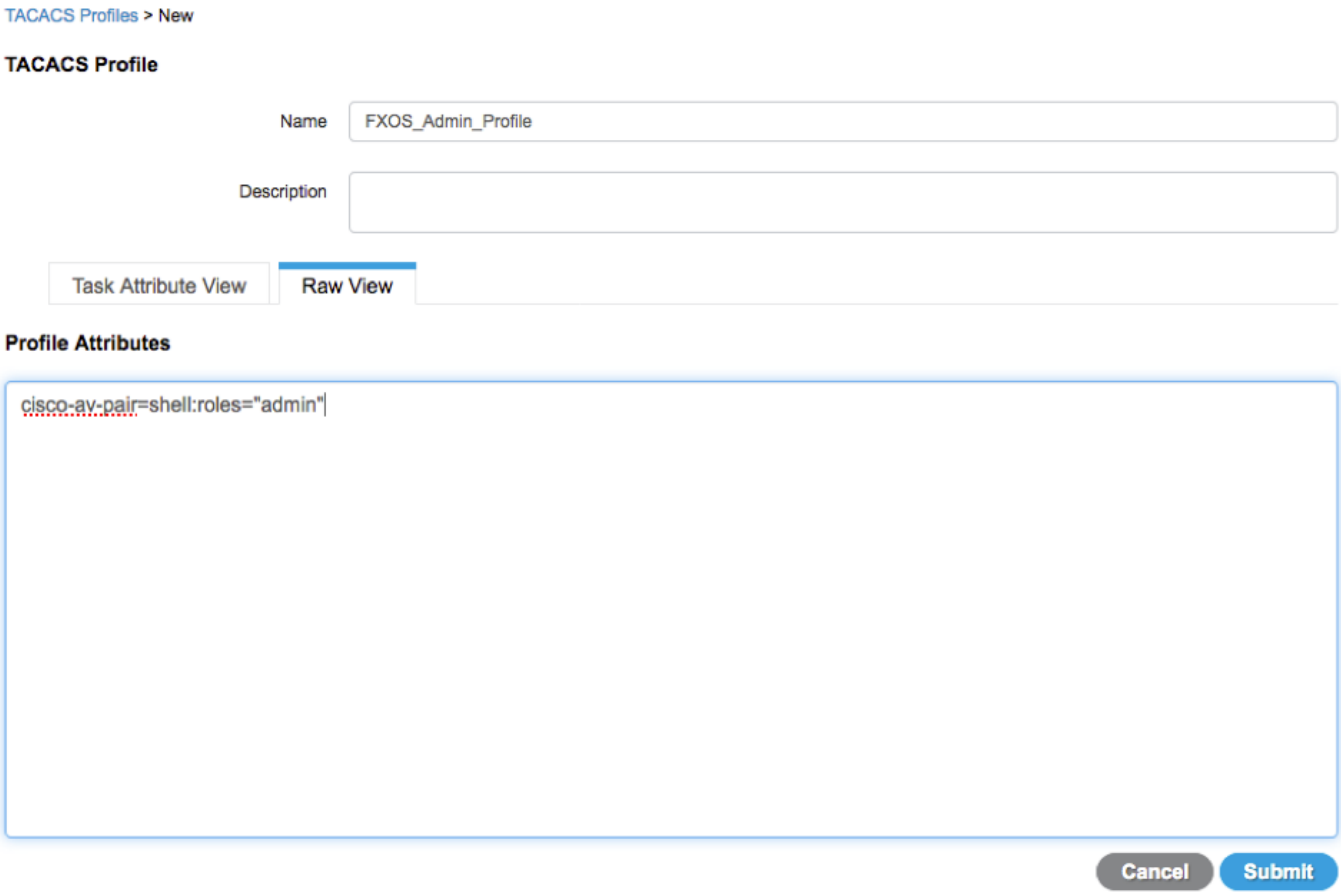
Stap 2. Voer de gewenste waarden in voor het TACACS-profiel

2.1. Voer de naam in.

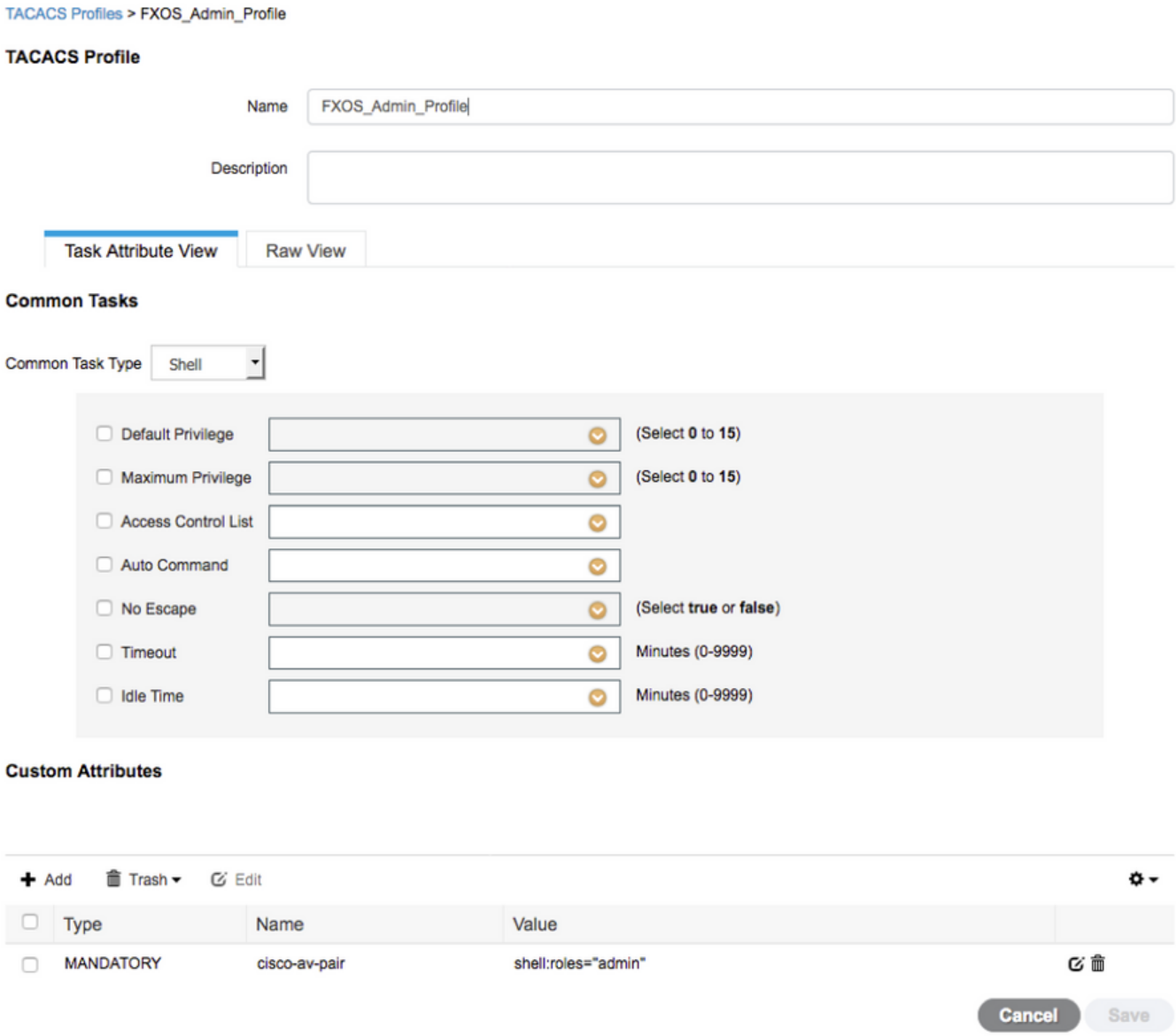


2.2. Configureer in het TAB **RAW View** het volgende CISCO-AV-PAIR.

cisco-av-pair=shell:rollen="admin"



2.3. Klik op **Indienen**.

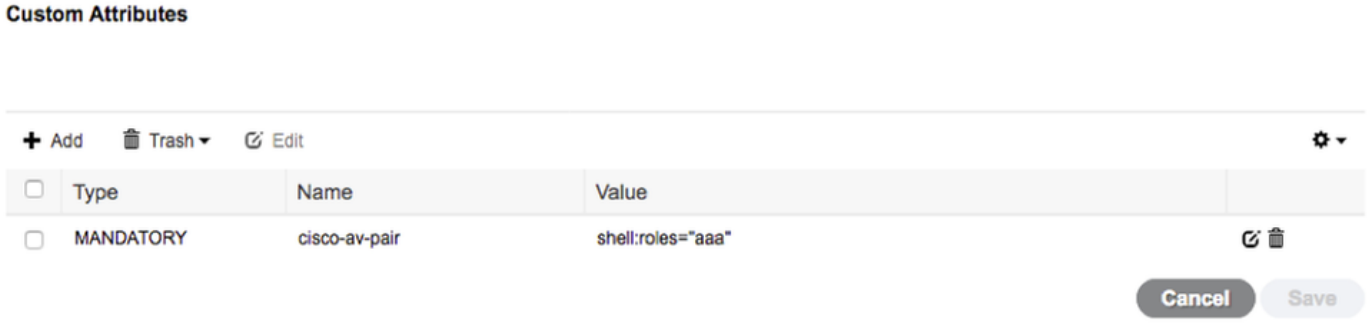


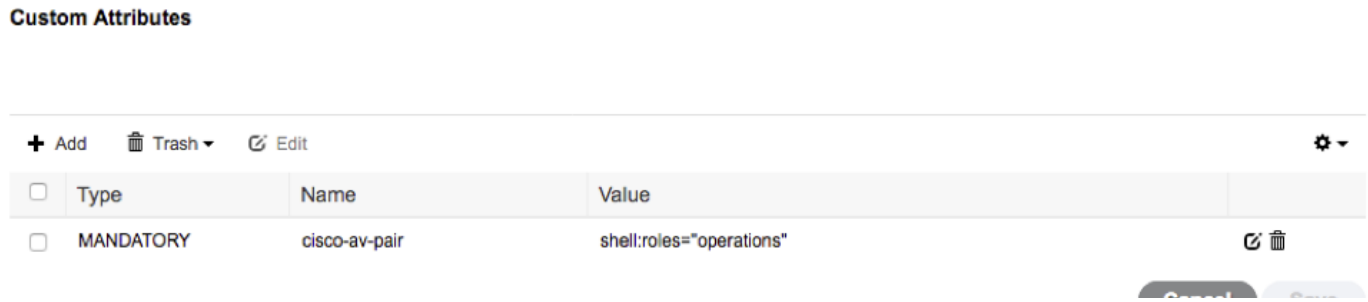
Stap 3. Herhaal stap 2 voor de overige gebruikershandleidingen met behulp van de volgende Cisco-AV-paren.

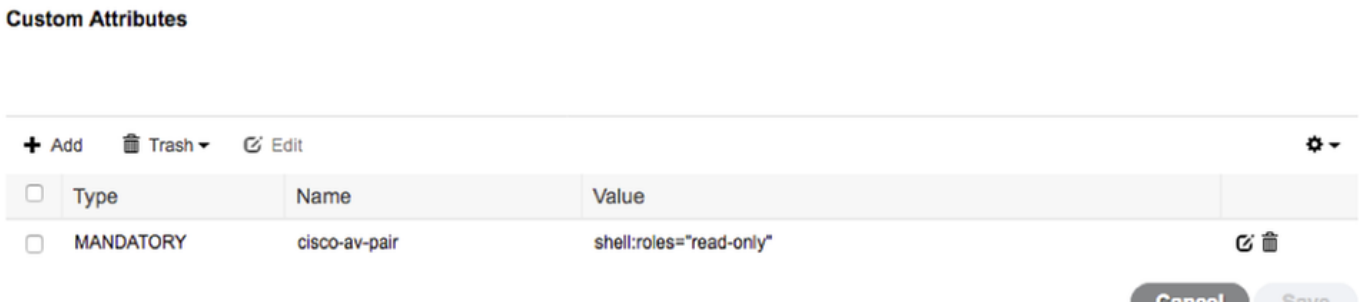
cisco-av-pair=shell:rollen="aaa"

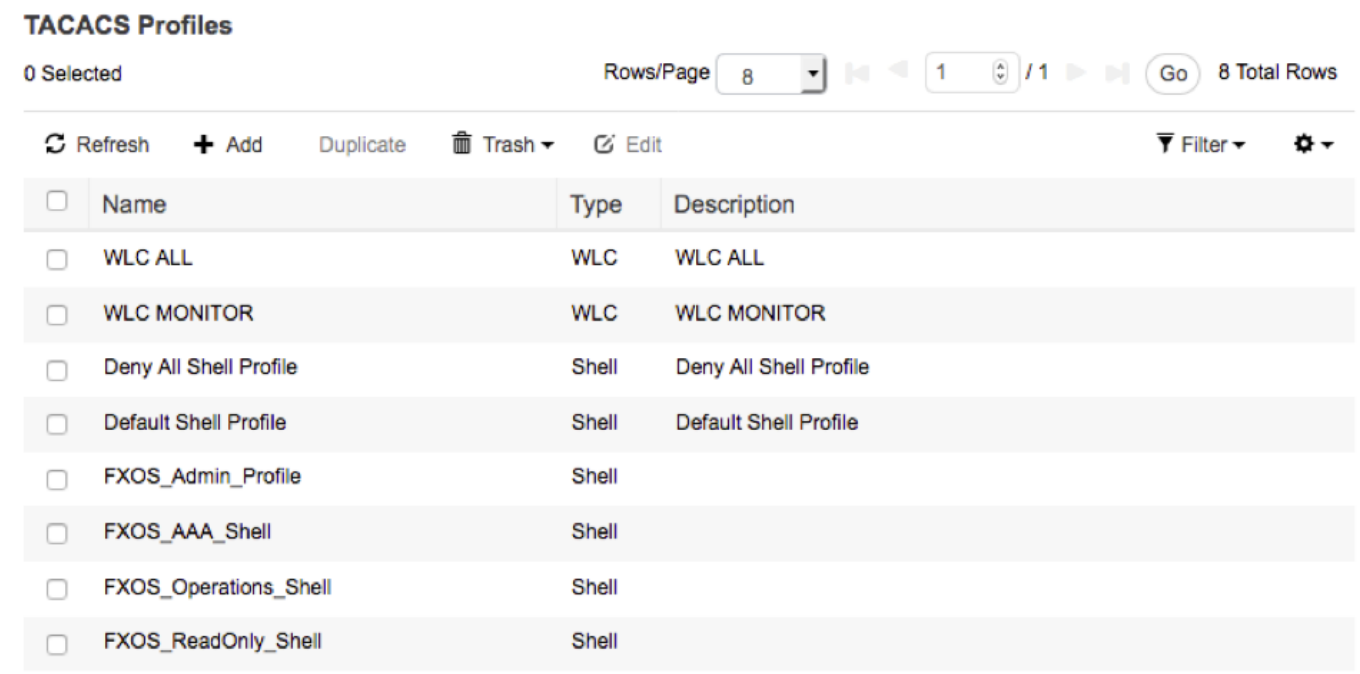
cisco-av-pair=shell:rollen="operaties"

cisco-av-pair=shell:rollen="alleen-lezen"



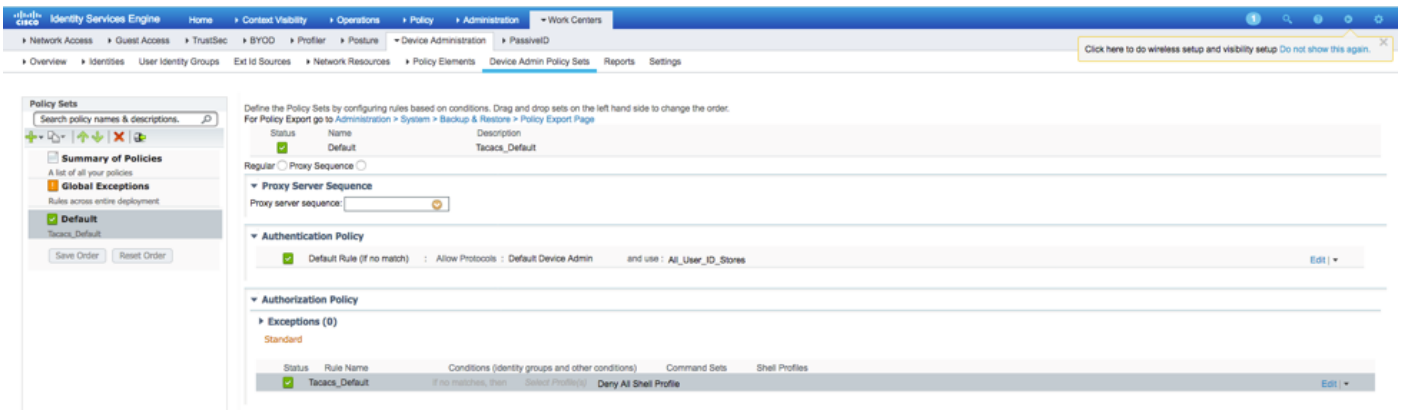




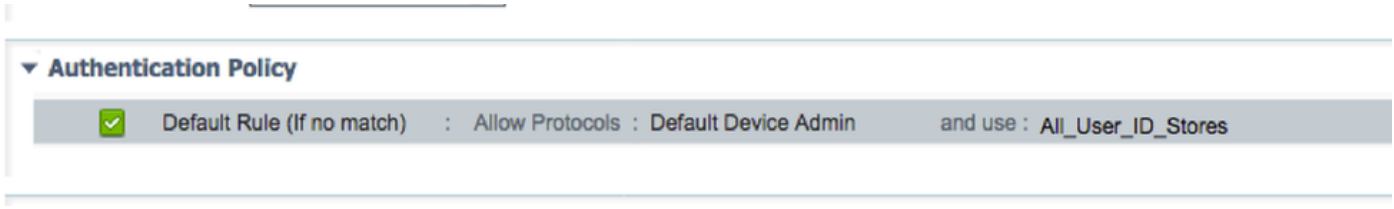


Het Tacacs-machtigingsbeleid creëren

Stap 1. navigeren naar **werkcentra > Apparaatbeheer > Apparaatbeheerset.**



Stap 2. Zorg ervoor dat het verificatiebeleid op de interne gebruikersdatabase of de vereiste identiteitswinkel wijst.



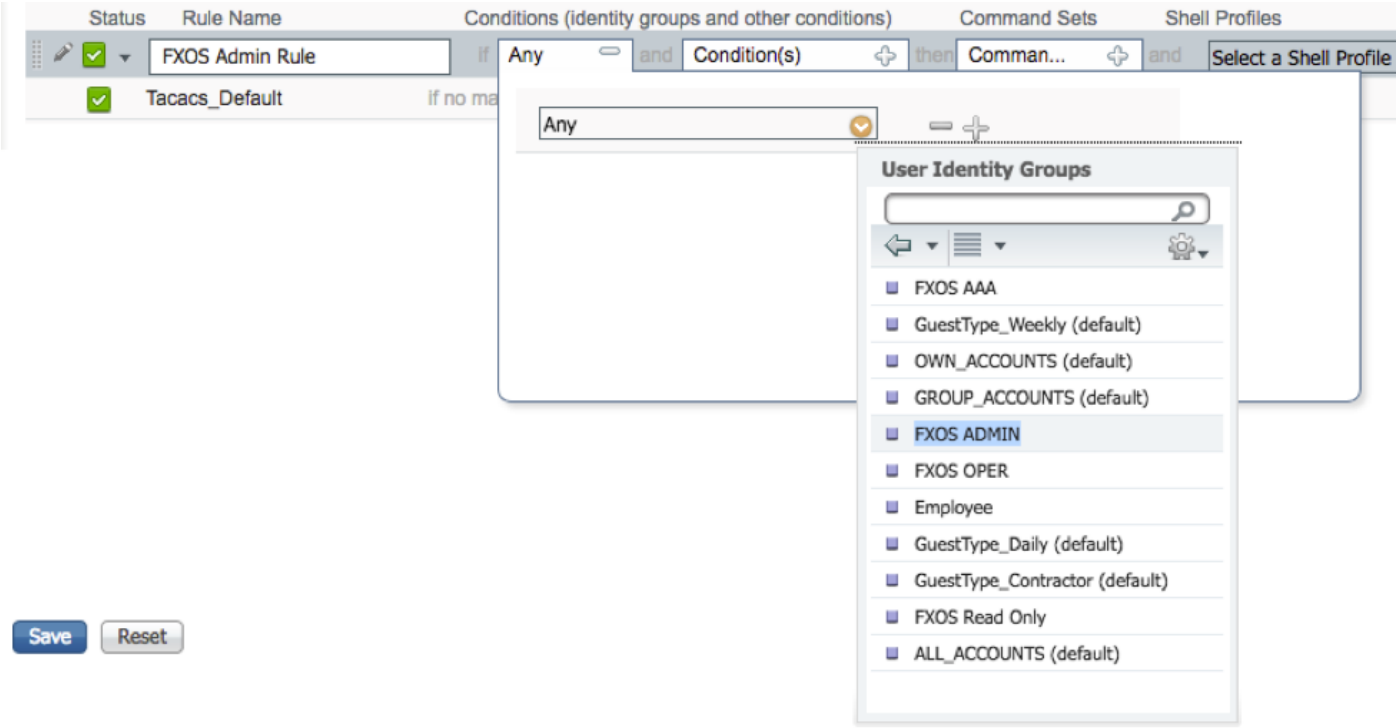
Stap 3. Klik op de pijl aan het einde van het standaardbeleid voor autorisatie en klik op boven regels invoegen.

Stap 4. Voer de waarden voor de regel in met de vereiste parameters:

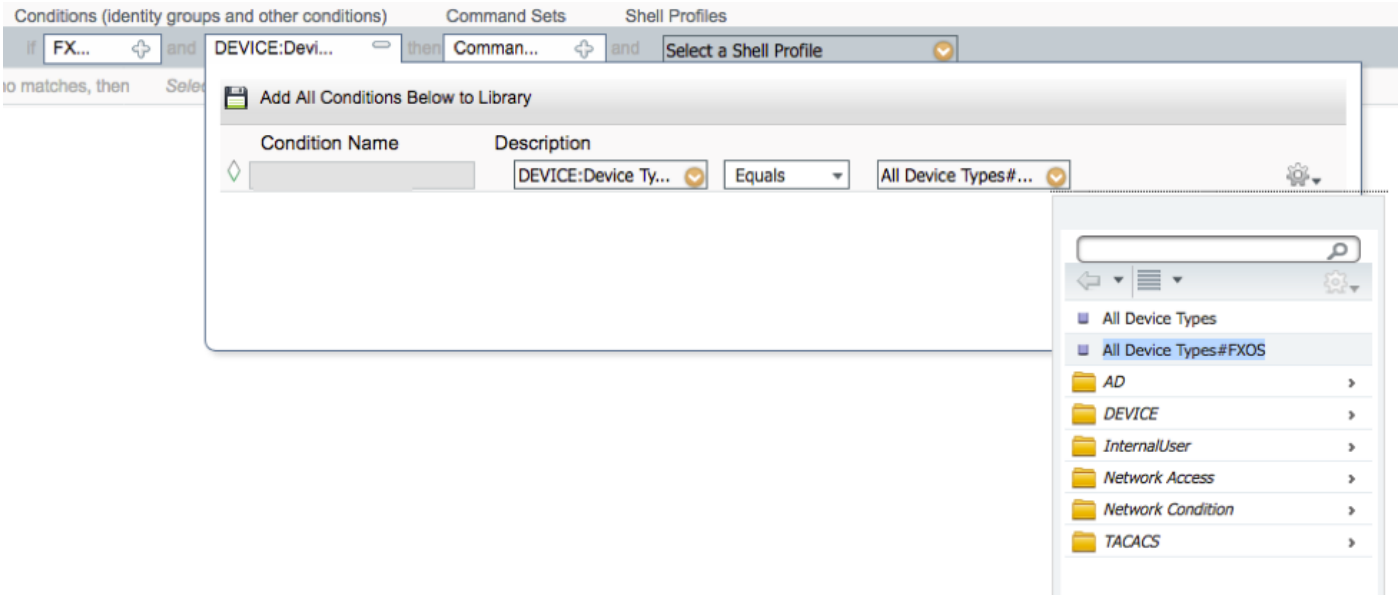
4.1. Naam van de regel: FXOS-beheerder.

4.2. Voorwaarden.

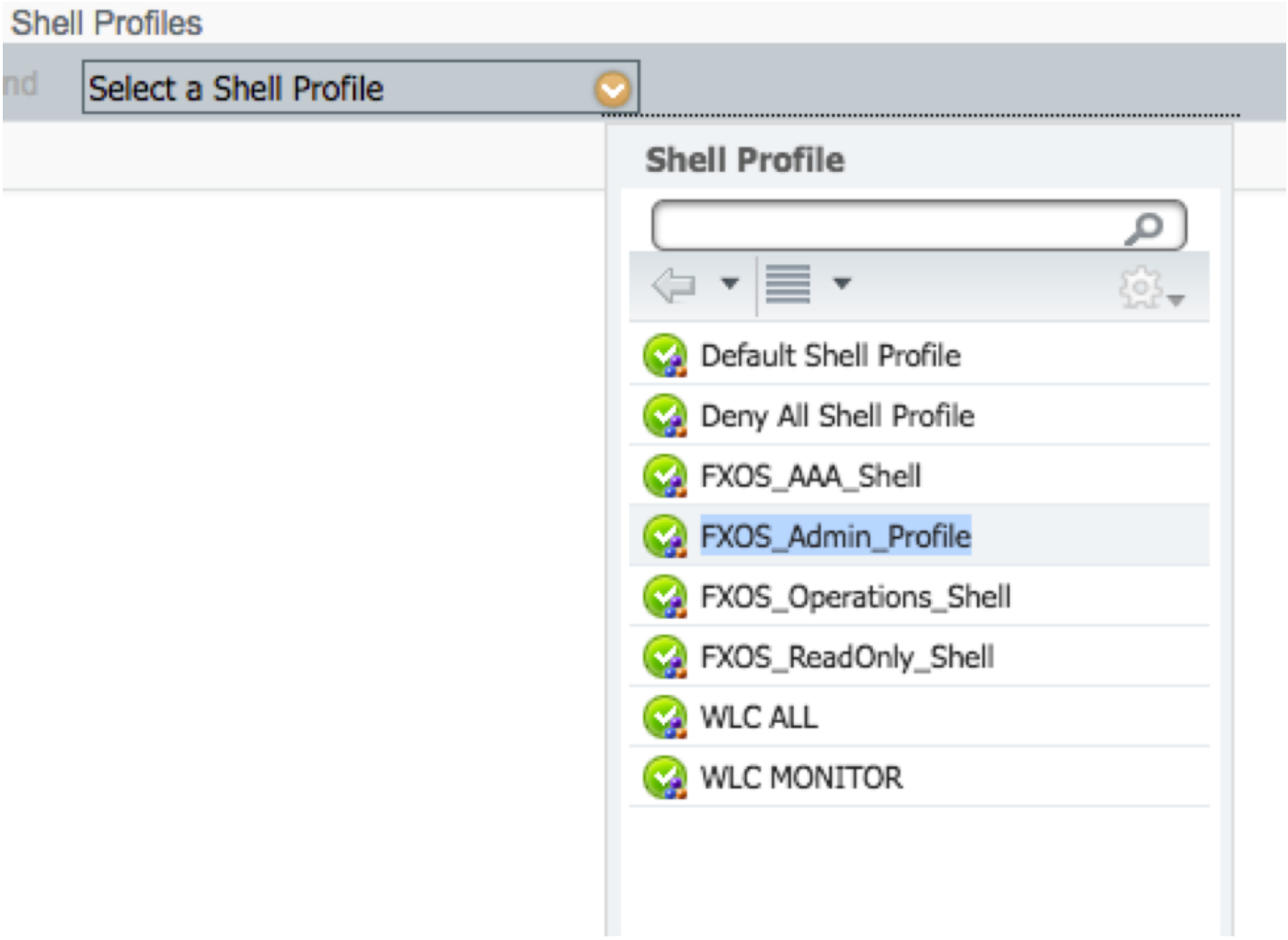
Indien : User Identity Group is FXOS ADMIN



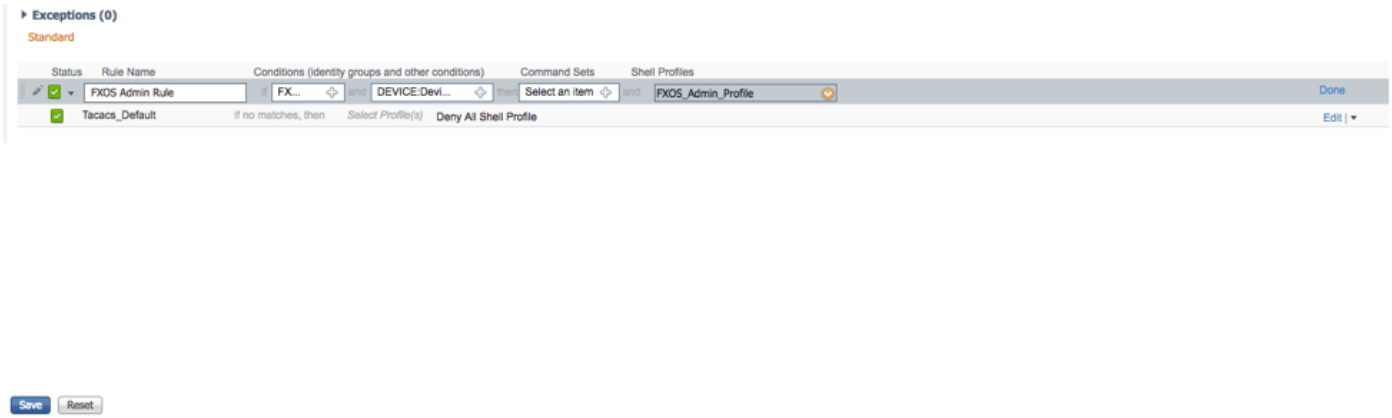
En apparaat: Apparaattype is gelijk aan alle apparaattypen #FXOS



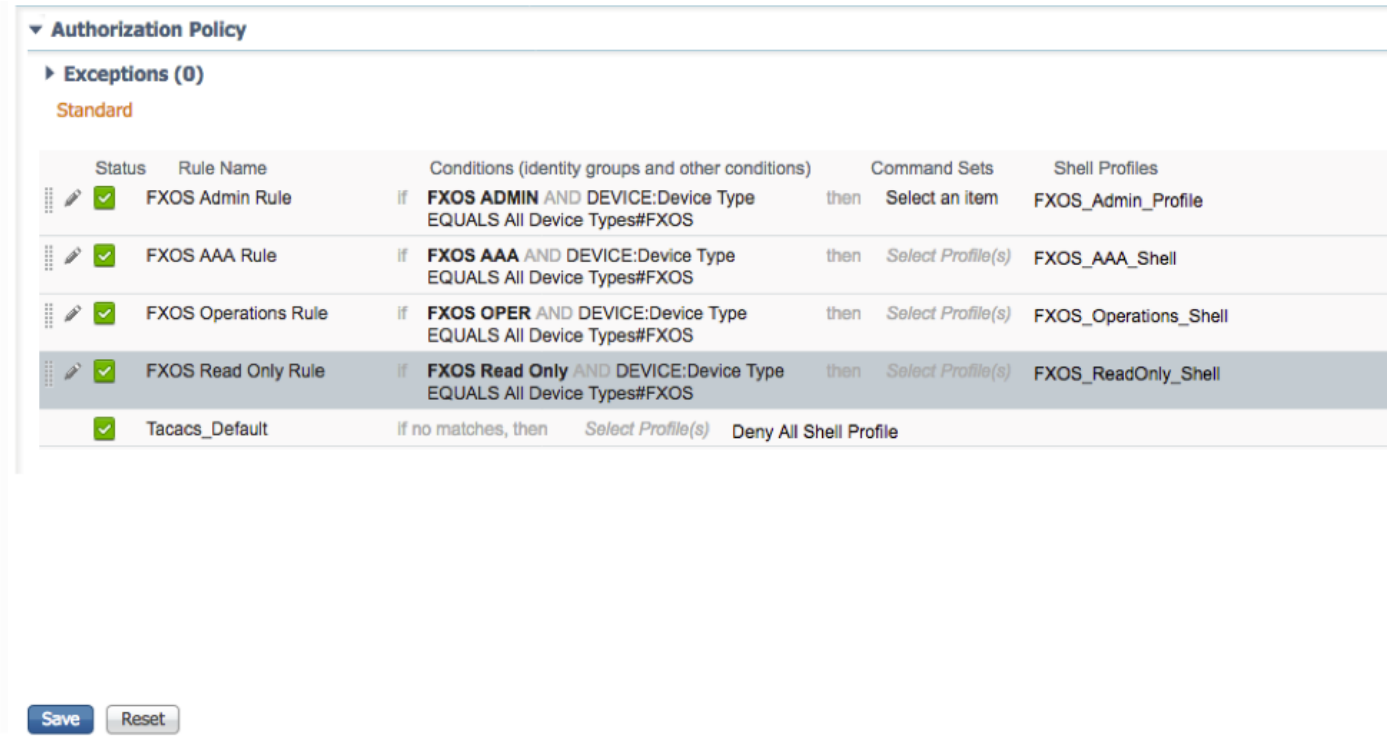
Shell Profile : FXOS_Admin_Profiel



Stap 5. Klik op **Gereedschap**.



Stap 6. Herhaal stap 3 en 4 voor de resterende gebruikersrollen en na het klaar zijn klikt u op **OPSLAAN**.



Verifiëren

U kunt nu elke gebruiker testen en de toegewezen gebruikersrol controleren.

Verificatie FXOS-chassis

1. Telnet of SSH aan het FXOS-chassis en inloggen met behulp van een van de gemaakte gebruikers op ISE.

Username: fxosadmin

Wachtwoord:

Voor de **beveiliging** van de **FPR**4120-TAC-A**#scope**

fpr4120-TAC-A/security **# geeft details voor externe gebruikers weer**

Afstandsbediening door gebruiker:

Beschrijving:

Rol gebruiker:

Name: Aa

Name: alleen-lezen

Afstandsbediening door gebruiker fxosadmin:

Beschrijving:

Rol gebruiker:

Name: besturen

Name: alleen-lezen

Afstandsbediening door gebruiker:

Beschrijving:

Rol gebruiker:

Name: verrichting

Name: alleen-lezen

Afstandsbediening door gebruiker:

Beschrijving:

Rol gebruiker:

Name: alleen-lezen

Afhankelijk van de gebruikersnaam die in de FXOS-chassiscli is ingevoerd, worden alleen de opdrachten weergegeven die zijn geautoriseerd voor de gebruikersrol die is toegewezen.

Gebruiker beheren.

fpr4120-TAC-A/security # ?

erkennen

duidelijke gebruikerssessies Wis gebruikerssessies

Maken beheerde objecten

Verwijdert beheerde objecten verwijderen

schakelt uitgeschakeld services uit

diensten mogelijk maken

Voer een beheerd object in

scope wijzigt de huidige modus

Vastgestelde waarden

Systeeminformatie weergeven

actieve cimc-sessies beëindigen

FPR4120-TAC-A#**connect fxos**

fpr4120-TAC-A (fxos)# **debug Aa-verzoeken**

fpr4120-TAC-A (FXS)#

Alleen-lezen gebruikersrol.

fpr4120-TAC-A/security # **?**

scope wijzigt de huidige modus

Vastgestelde waarden

Systeeminformatie weergeven

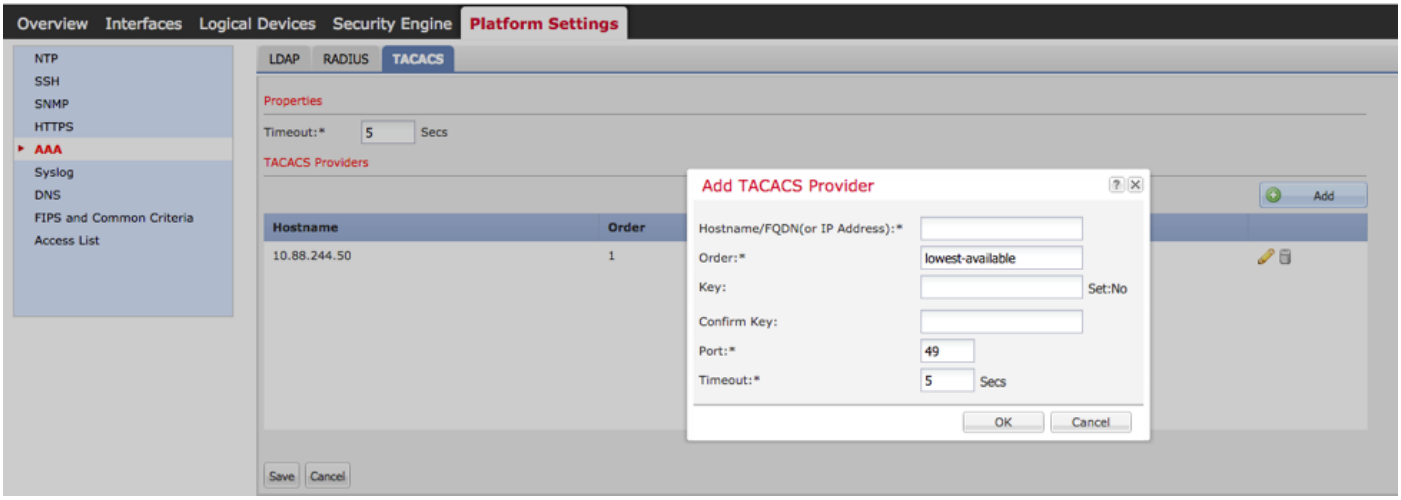
FPR4120-TAC-A#**connect fxos**

fpr4120-TAC-A (fxos)# **debug Aa-verzoeken**

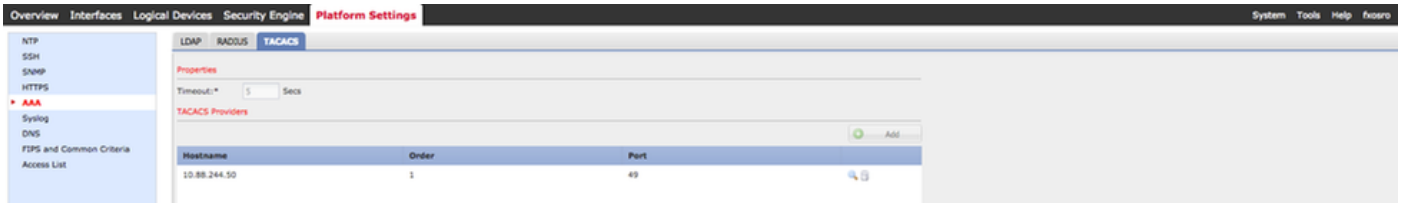
% Toestemming geweigerd voor de rol

2. Bladeren naar het FXOS-chassis IP-adres en inloggen met behulp van een van de gemaakte gebruikers in ISE.

Gebruiker beheren.



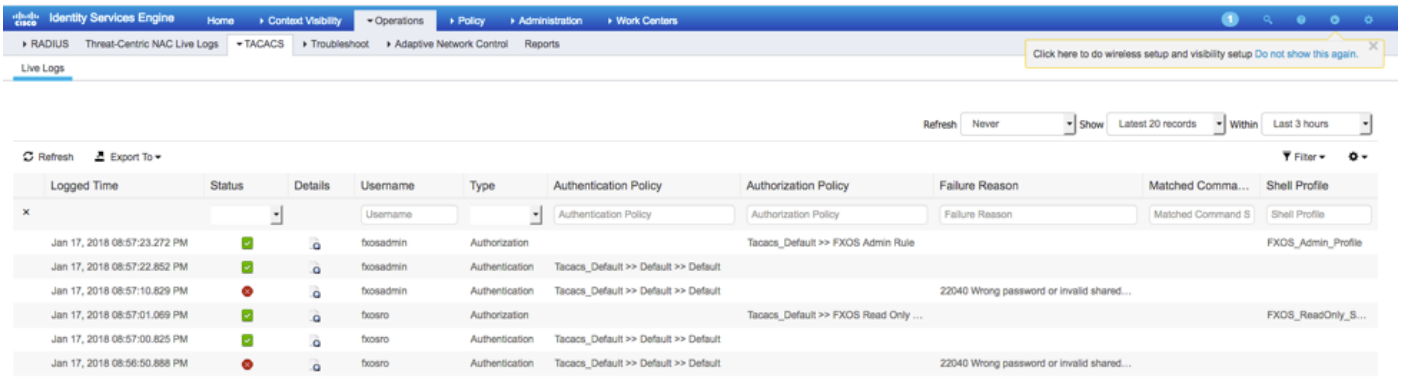
Alleen-lezen gebruikersrol.



Opmerking: Merk op dat de knop **ADD** gegraveerd is.

ISE 2.0 Verificatie

1. Navigeer naar **bewerkingen > TACACS-loggen.** Je zou succesvolle en mislukte pogingen moeten kunnen zien.



Problemen oplossen

Om AAA-verificatie en -autorisatie te reinigen voert u de volgende opdrachten in de FXOS-cloud uit.

FPR4120-TAC-A#**connect fxos**

fpr4120-TAC-A (fxos)# **debug Aa-verzoeken**

fpr4120-TAC-A (fxos)# **debug van gebeurtenis**

fpr4120-TAC-A (FXS)# **bug van fouten in de verwerking**

fpr4120-TAC-A (FXS)# **termijnmon**

Na een succesvolle authenticatie poging, zult u de volgende output zien.

2018 jan 17 15:46:40.305247 aaa: aaa_req_process voor authenticatie. zitting nr. 0

2018 jan 17 15:46:40.305262 aaa: aaa_req_process: Algemeen AAA-verzoek van toepassing: aanmelding appln_subtype: standaard

2018 jan 17 15:46:40.305271 aaa: probeer_next_aaa_methode

2018 jan 17 15:46:40.305285 aaa: in totaal zijn de methoden 1 , de huidige te beproeven index is 0

2018 jan 17 15:46:40.305294 aaa: handle_req_gebruikt_methode

2018 jan 17 15:46:40.305301 aaa: AAA_METHOD_SERVER_GROUP

2018 jan 17 15:46:40.305308 aaa: aaa_sg_handler groep = tacacs

2018 jan 17 15:46:40.305315 aaa: Het gebruik van sg_protocol dat naar deze functie wordt doorgegeven

2018 jan 17 15:46:40.305324 aaa: Aanvraag naar TACACS-service verzenden

2018 jan 17 15:46:40.305384 aaa: Configureer methodegroep succesvol

2018 jan 17 15:46:40,554631 aaa: aaa_proces_fd_set

2018 jan 17 15:46:40,555229 aaa: aaa_process_fd_set: Back-uplijn

2018 jan 17 15:46:40,555817 aaa: mts_message_response_handler: reactie op mts

2018 jan 17 15:46:40,556387 aaa: prot_daemon_reponse_handler

2018 jan 17 15:46:40,557042 aaa: zitting : 0x8df68c verwijderd uit de sessietabel 0

2018 jan 17 15:46:40,557059 aaa: is_a_rep_status_successtatus = 1

2018 jan 17 15:46:40,557066 aaa: is_a_rep_status_successie is TRUE

2018 jan 17 15:46:40,557075 aaa: aaa_send_client_response voor authenticatie. sessie->flags=21.aaa_resp->flags=0.

2018 jan 17 15:46:40,557083 aaa: AAA_REQ_FLAG_NORMAAL

2018 jan 17 15:46:40,557106 aaa: mts_send_response Succesvol

2018 jan 17 15:46:40,557364 aaa: aaa_req_process voor autorisatie. zitting nr. 0

2018 jan 17 15:46:40,557378 aaa: aaa_req_process aangeroepen met context vanaf appln: aanmelding appln_subtype: default authen_type:2, authen_ethode: 0

2018 jan 17 15:46:40,557386 aaa: aaa_send_req_use_context

2018 jan 17 15:46:40,557394 aaa: aaa_sg_handler groep = (nul)

2018 jan 17 15:46:40,557401 aaa: Het gebruik van sg_protocol dat naar deze functie wordt doorgegeven

2018 jan 17 15:46:40,557408 aaa: op context gebaseerde of gerichte AAA-req (behalve: geen relaisverzoek). Kan geen kopie van een verzoek aannemen

2018 jan 17 15:46:40,557415 aaa: Aanvraag naar TACACS-service verzenden

2018 jan 17 15:46:40.801732 aaa: aaa_send_client_response voor autorisatie. sessie->flags=9. aaa_rep->flags=0.

2018 jan 17 15:46:40.801740 aaa: AAA_REQ_FLAG_NORMAAL

2018 jan 17 15:46:40.801761 aaa: mts_send_response Succesvol

2018 jan 17 15:46:40,848932 aaa: OUDE OPCODE: accounting_interim_update

2018 jan 17 15:46:40,848943 aaa: aaa_aangemaakt_local_acct_req: gebruiker=, sessie_id=, log=added gebruiker:fxosadmin aan de rol:admin

2018 jan 17 15:46:40,848963 aaa: aaa_req_process voor accounting. zitting nr. 0

2018 jan 17 15:46:40,848972 aaa: MTS aanvraag referentie is NULL. LOKALE AANVRAAG

2018 jan 17 15:46:40,848982 aaa: AAA_REQ_RESPONSE_NOT_NOED instellen

2018 jan 17 15:46:40,848992 aaa: aaa_req_process: Algemeen AAA-verzoek van toepassing: standaard appln_subtype: standaard

2018 jan 17 15:46:40,849002 aaa: probeer_next_aaa_methode

2018 jan 17 15:46:40,849022 aaa: geen standaardinstellingen voor methoden

2018 jan 17 15:46:40,849032 aaa: geen configuratie beschikbaar voor dit verzoek

2018 jan 17 15:46:40,849043 aaa: probeert_fallback_ethode

2018 jan 17 15:46:40,849053 aaa: handle_req_gebruikt_methode

2018 jan 17 15:46:40,849063 aaa: local_methode_handler

2018 jan 17 15:46:40,849073 aaa: aaa_local_accounting_msg

2018 jan 17 15:46:40,849085 aaa: update::toegevoegde gebruiker:fxosadmin aan de rol:admin

Na een mislukte verificatiepoging ziet u de volgende uitvoer.

2018 jan 17 15:46:17,836271 aaa: aaa_req_process voor authenticatie. zitting nr. 0

2018 jan 17 15:46:17,836616 aaa: aaa_req_process: Algemeen AAA-verzoek van toepassing: aanmelding appln_subtype: standaard

2018 jan 17 15:46:17,837063 aaa: probeer_next_aaa_methode

2018 jan 17 15:46:17,837416 aaa: in totaal zijn de methoden 1 , de huidige te beproeven index is 0

2018 jan 17 15:46:17,83776 aaa: handle_req_gebruikt_methode

2018 jan 17 15:46:17.838103 aaa: AAA_METHOD_SERVER_GROUP

2018 jan 17 15:46:17,83847 aaa: aaa_sg_handler groep = tacacs

2018 jan 17 15:46:17.83826 aaa: Het gebruik van sg_protocol dat naar deze functie wordt doorgegeven

2018 jan 17 15:46:17.839-167 aaa: Aanvraag naar TACACS-service verzenden

2018 jan 17 15:46:17.840-225 aaa: Configureer methodegroep succesvol

2018 jan 17 15:46:18:043710 aaa: is_a_rep_status_successtatus = 2

2018 jan 17 15:46:18.044048 aaa: is_a_rep_status_successie is TRUE

2018 jan 17 15:46:18.044395 aaa: aaa_send_client_response voor authenticatie. sessie->flags=21.aaa_resp->flags=0.

2018 jan 17 15:46:18.044733 aaa: AAA_REQ_FLAG_NORMAAL

2018 jan 17 15:46:18:045096 aaa: mts_send_response Succesvol

2018 jan 17 15:46:18.04567 aaa: aaa_schoonmaak_sessie

2018 jan 17 15:46:18.045689 aaa: mts_drop-applicatie voor msg

2018 jan 17 15:46:18:045699 aaa: Aa_req moet worden vrijgelaten.

2018 jan 17 15:46:18.045715 aaa: aaa_proces_fd_set

2018 jan 17 15:46:18:045722 aaa: aaa_process_fd_set: Back-uplijn

2018 jan 17 15:46:18.045732 aaa: aaa_wellicht_info_fig: GET_REQ voor ABBYY inlogfoutmelding

2018 jan 17 15:46:18.045738 aaa: terugkrijgen de retourwaarde van de configuratie:onbekend beveiligingsitem

Gerelateerde informatie

De opdracht van de Ethanalyzer op FX-OS CLI zal om een wachtwoord vragen wanneer TACACS/RADIUS-verificatie is ingeschakeld. Dit gedrag wordt veroorzaakt door een bug.

Eenmalig id: CSCvg875-18