

Firepower eXtensible Operating System (FXOS)

2.2: Chassis Authentication/Authoridering for Remote Management met ISE met behulp van RADIUS

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Het FXOS-chassis configureren](#)

[De ISE-server configureren](#)

[Verifiëren](#)

[Verificatie FXOS-chassis](#)

[ISE 2.0 Verificatie](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u RADIUS-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 systeemservern 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 Ramirez, 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

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

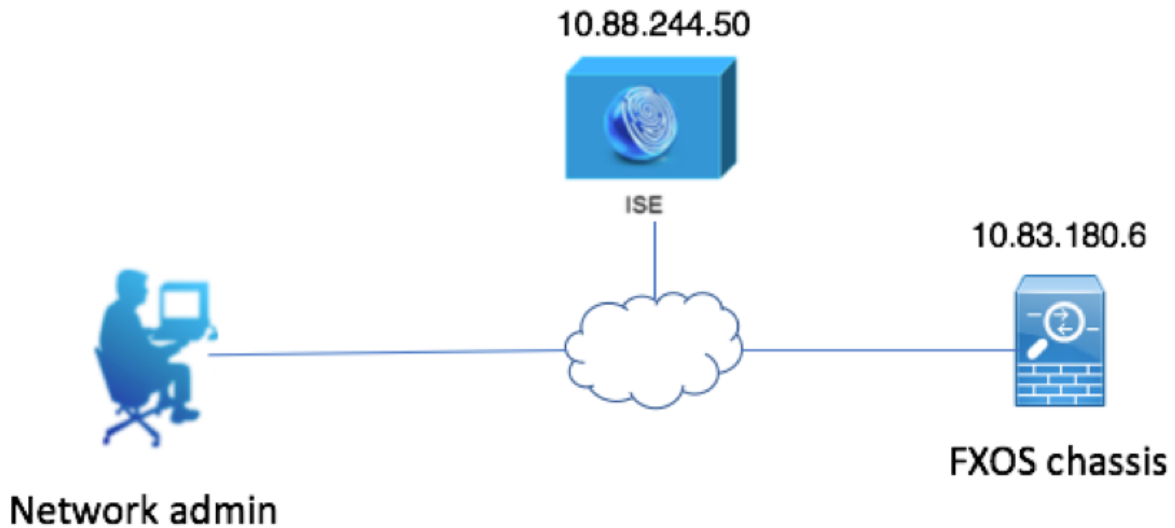
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

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

Netwerkdigram



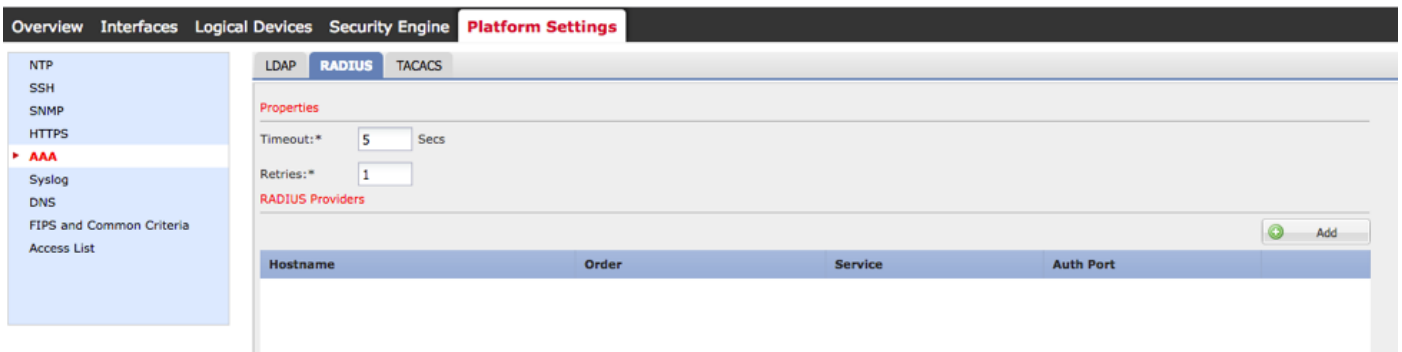
Configuraties

Het FXOS-chassis configureren

Een RADIUS-provider maken met Chassis Manager

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

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



Stap 3. Voor elke RADIUS-provider die u wilt toevoegen (maximaal 16 providers).

3.1. Klik in het gebied RADIUS-providers op **Add**.

3.2. Zodra het dialoogvenster RADIUS-providers toevoegen wordt geopend, specificeert u de gewenste waarden.

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

Edit 10.88.244.50

Hostname/FQDN(or IP Address):*

Order:*

Key: Set: Yes

Confirm Key:

Authorization Port:*

Timeout:* Secs

Retries:*

Stap 4. Klik op Opslaan.

Overview Interfaces Logical Devices Security Engine **Platform Settings**

NTP
SSH
SNMP
HTTPS
▶ **AAA**
Syslog
DNS
FIPS and Common Criteria
Access List

LDAP **RADIUS** TACACS

Properties

Timeout:* Secs

Retries:*

RADIUS Providers

Hostname	Order	Service	Auth Port
10.88.244.50	1	authorization	1812

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

Stap 6. Onder Standaard verificatie kiest u **RADIUS**.

Overview Interfaces Logical Devices Security Engine Platform Settings

System Tools Help frosadmin

Configuration Licensing Updates **User Management**

Local Users **Settings**

Default Authentication: *Local is fallback authentication method

Console Authentication:

Remote User Settings

Remote User Role Policy: Assign Default Role No-Login

Een RADIUS-provider maken met CLI

Stap 1. Om RADIUS-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-boogstraal**

Stap 2. Gebruik de opdracht **Details tonen** om de resultaten weer te geven.

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

Standaardverificatie:

Admin Realm: **Straal**

Operationeel antwoord: **Straal**

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 RADIUS-serverparameters te configureren voert u de volgende opdrachten uit.

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

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

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

fpr4120-TAC-A/security/Straal/server # **ingestelde "ISE-server"**

fpr4120-TAC-A/security/Straal/server* # **insteltoets**

Geef de toets op: *********

Bevestig de toets: *********

Stap 4. Gebruik de opdracht **Details tonen** om de resultaten weer te geven.

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

RADIUS-server:

Hostname, FQDN of IP-adres: 10.88.244.50

Descr:

Volgorde: 1

Poorten: 1812

Sleutel: ****

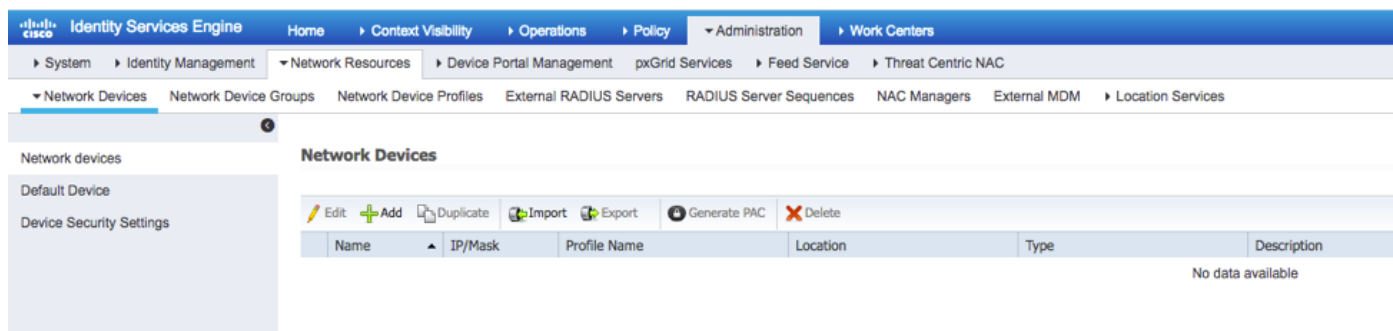
Time-out: 5

De ISE-server configureren

De FXOS als netwerkresource toevoegen

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

Stap 2. Klik op **ADD**



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Under Administration, the Network Resources section is expanded, showing Network Devices, Network Device Groups, Network Device Profiles, External RADIUS Servers, RADIUS Server Sequences, NAC Managers, External MDM, and Location Services. The Network Devices page is active, displaying a table with columns for Name, IP/Mask, Profile Name, Location, Type, and Description. The table is currently empty, with the text "No data available" displayed below it. The page also includes a sidebar with "Network devices", "Default Device", and "Device Security Settings" options, and a toolbar with actions like Edit, Add, Duplicate, Import, Export, Generate PAC, and Delete.

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

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network devices

Default Device

Device Security Settings

Network Devices List > New Network Device

Network Devices

* Name

Description

* IP Address: /

* Device Profile Cisco

Model Name

Software Version

* Network Device Group

Device Type

IPSEC

Location

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

CoA Port

RADIUS DTLS Settings ⓘ

DTLS Required ⓘ

Shared Secret ⓘ

CoA Port

Issuer CA of ISE Certificates for CoA ⓘ

Identiteitsgroepen en gebruikers maken

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

Stap 2. Klik op **ADD**.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities **Groups** External Identity Sources Identity Source Sequences Settings

Identity Groups

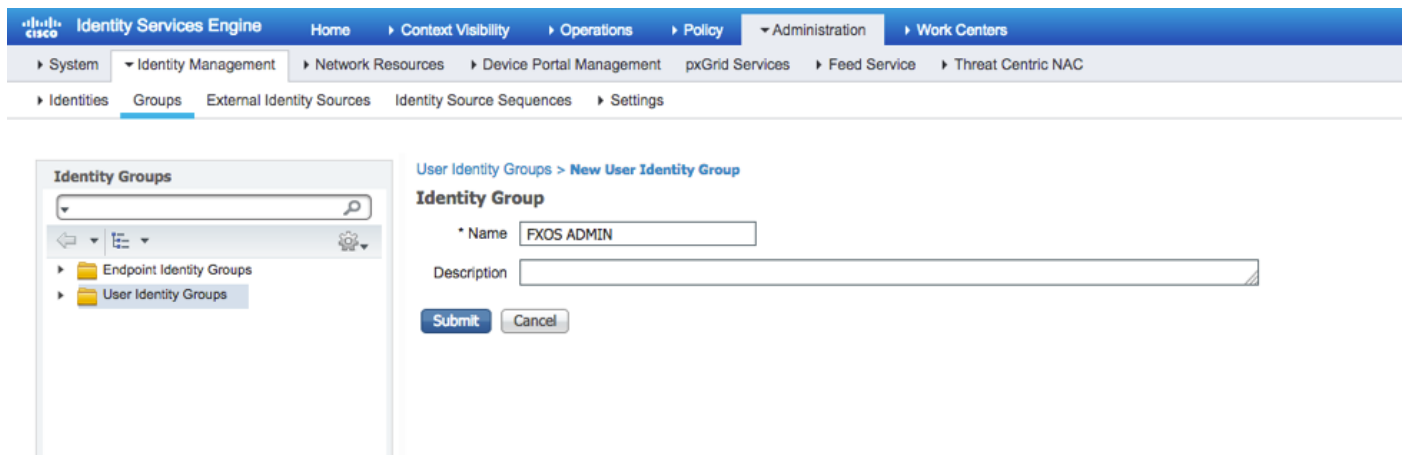
- Endpoint Identity Groups
- User Identity Groups**

User Identity Groups

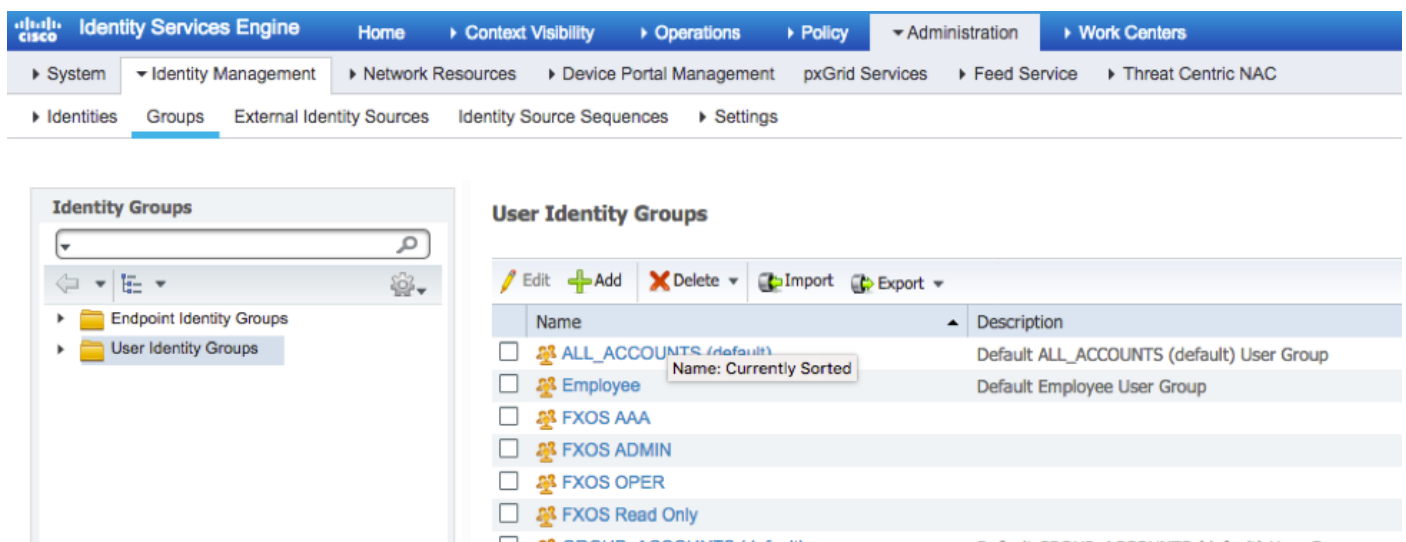
Edit Add Delete Import Export

Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/> Employee	Default Employee User Group
<input type="checkbox"/> GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
<input type="checkbox"/> GuestType_Contractor (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Daily (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Weekly (default)	Identity group mirroring the guest type
<input type="checkbox"/> OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

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

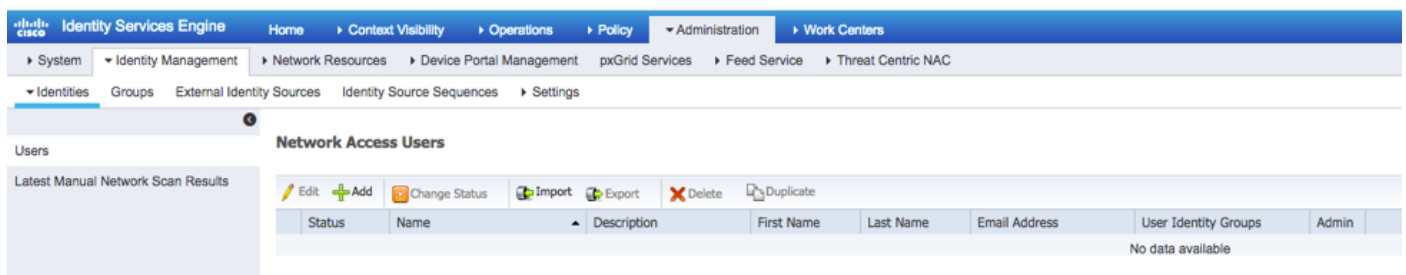


Stap 4. Herhaal stap 3 voor alle vereiste gebruikersrollen.



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

Stap 6. Klik op **ADD**.



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

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users List > New Network Access User

Network Access User

Name:

Status: Enabled

Email:

Passwords

Password Type: Internal Users

Password: Re-Enter Password: *i*

Enable Password: *i*

User Information

First Name:

Last Name:

Account Options

Description:

Change password on next login:

Account Disable Policy

Disable account if date exceeds: (yyyy-mm-dd)

User Groups

Stap 8. Herhaal stap 6 voor alle vereiste gebruikers.

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users

Edit Add Change Status Import Export Delete Duplicate

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input type="checkbox"/> Enabled	fxosaaa					FXOS AAA	
<input type="checkbox"/> Enabled	fxosadmin					FXOS ADMIN	
<input type="checkbox"/> Enabled	fxosoper					FXOS OPER	
<input type="checkbox"/> Enabled	fxosro					FXOS Read Only	

Het machtigingsprofiel maken voor elke gebruikersrol

Stap 1. Navigeer naar **Beleids-elementen > Resultaten > Vergunningsprofielen > Vergunningsprofielen.**

Standard Authorization Profiles
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Name	Profile	Description
<input type="checkbox"/> Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices. Ensu
<input type="checkbox"/> Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
<input type="checkbox"/> Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA port
<input type="checkbox"/> NSP_Onboard	Cisco	Onboard the device with Native Supplicant Provisionir
<input type="checkbox"/> Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
<input type="checkbox"/> DenyAccess		Default Profile with access type as Access-Reject
<input type="checkbox"/> PermitAccess		Default Profile with access type as Access-Accept

Stap 2. Vul alle eigenschappen in voor het machtigingsprofiel.

2.1. Het configureren van de profielnaam.

Authorization Profile

* Name:

Description:

* Access Type:

Network Device Profile: Cisco

2.2. Configureer in **geavanceerde** kenmerken de volgende CISCO-AV-PAIR:

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

Advanced Attributes Settings

Cisco:cisco-av-pair = shell:roles="admin"

2.3. Klik op **Opslaan**.

Save Reset

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"

▼ **Advanced Attributes Settings**

Cisco:cisco-av-pair = shell:roles="aaa" +

▼ **Advanced Attributes Settings**

Cisco:cisco-av-pair = shell:roles="operations" +

▼ **Advanced Attributes Settings**

Cisco:cisco-av-pair = shell:roles="read-only" +

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Standard Authorization Profiles

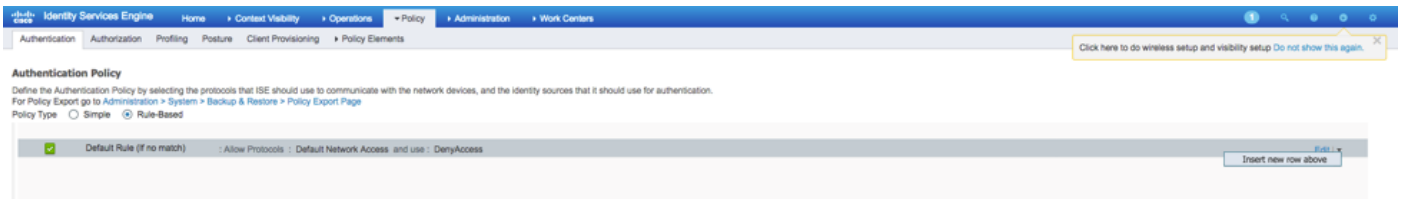
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Edit Add Duplicate Delete

<input type="checkbox"/>	Name	Profile
<input type="checkbox"/>	Blackhole_Wireless_Access	Cisco
<input type="checkbox"/>	Cisco_IP_Phones	Cisco
<input type="checkbox"/>	Cisco_WebAuth	Cisco
<input type="checkbox"/>	FXOS-AAA-PROFILE	Cisco
<input type="checkbox"/>	FXOS-ADMIN-PROFILE	Cisco
<input type="checkbox"/>	FXOS-OPER-PROFILE	Cisco
<input type="checkbox"/>	FXOS-ReadOnly-PROFILE	Cisco

Het verificatiebeleid maken

Stap 1. Navigeer naar **beleid > Verificatie >** en klik op het pijltje naast bewerken waar u de regel wilt maken.



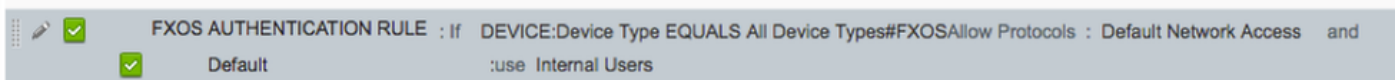
Stap 2. De instellingen zijn eenvoudig; het kan korter worden gemaakt , maar in dit voorbeeld gebruiken we het apparaattype :

Name: **FXOS-VERIFICATIEREGEL**

INDIEN nieuwe eigenschap/waarde selecteren: **Apparaat:Apparaattype is gelijk aan alle apparaattypen #FXOS**

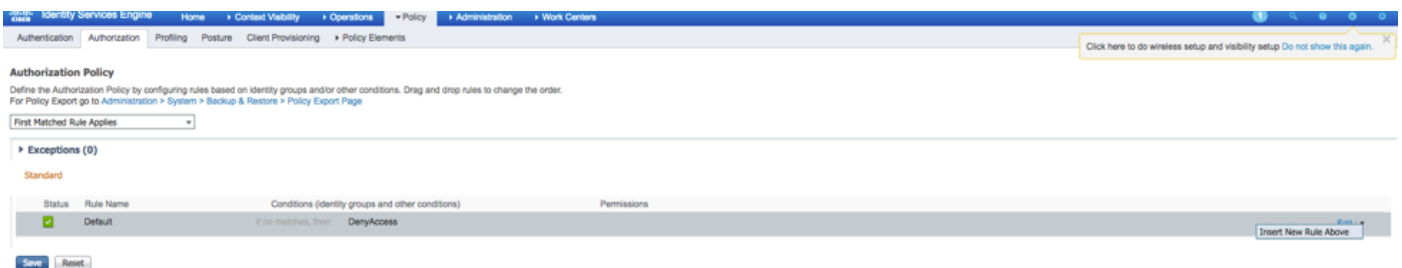
Protocollen toestaan: Standaard netwerktoegang

Gebruik: Interne gebruikers



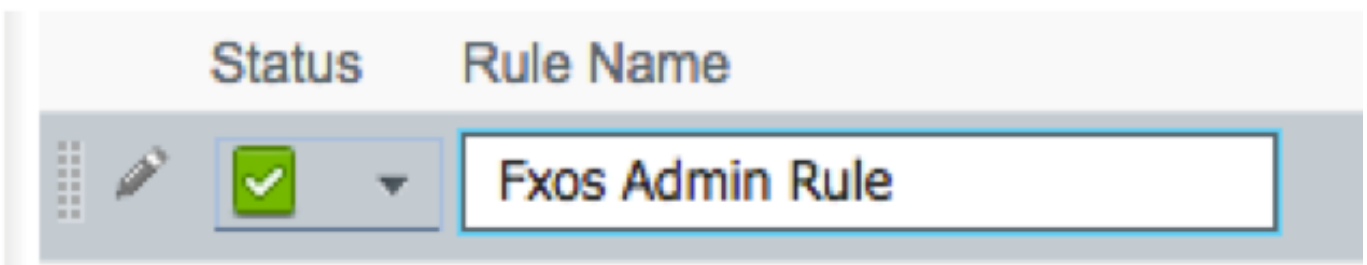
Het machtigingsbeleid maken

Stap 1. Navigeer naar **beleid > Vergunning >** en klik op het pijltje om te bewerken waar u de regel wilt maken.

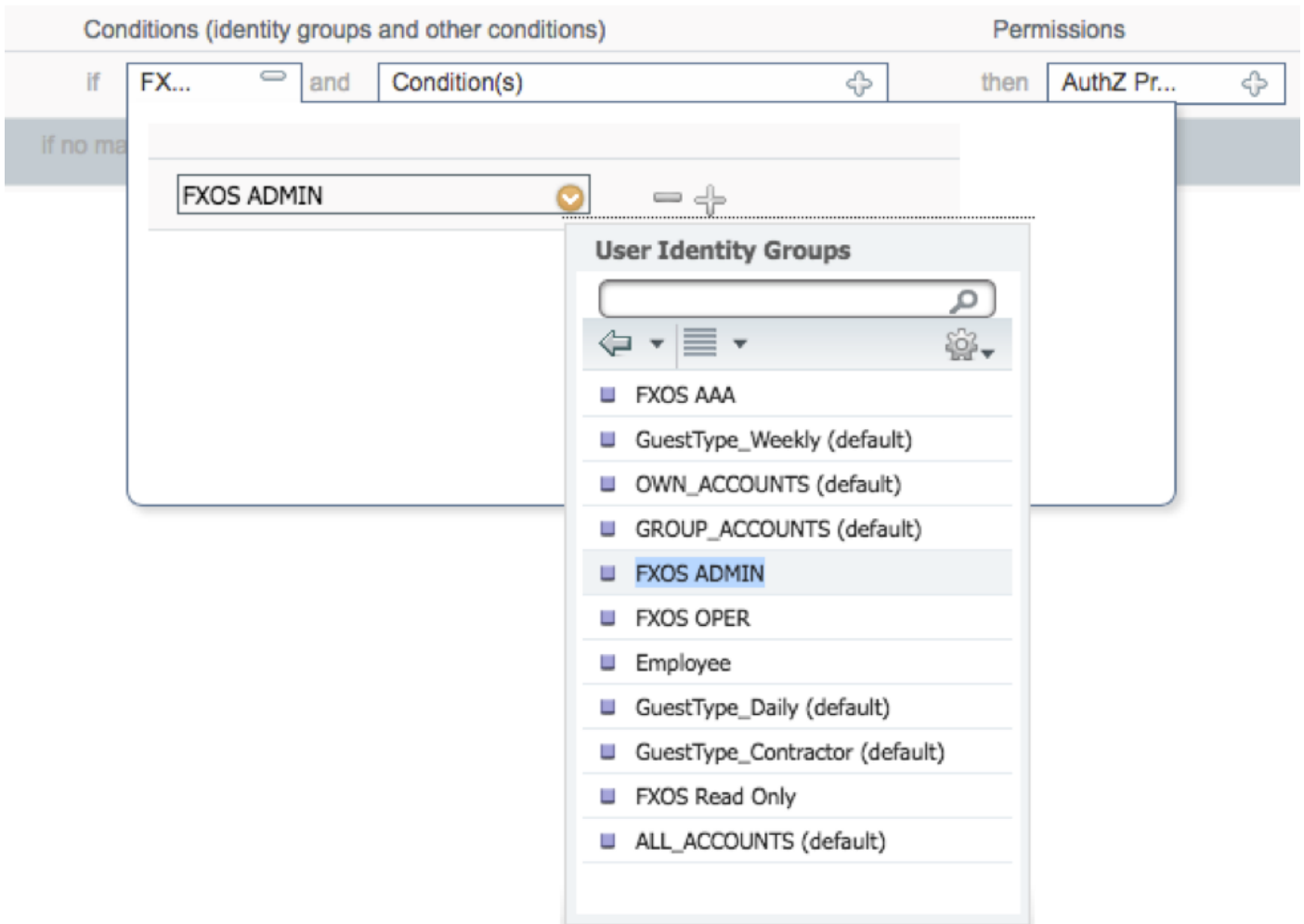


Stap 2. Voer de waarden voor de machtigingsregel in met de vereiste parameters.

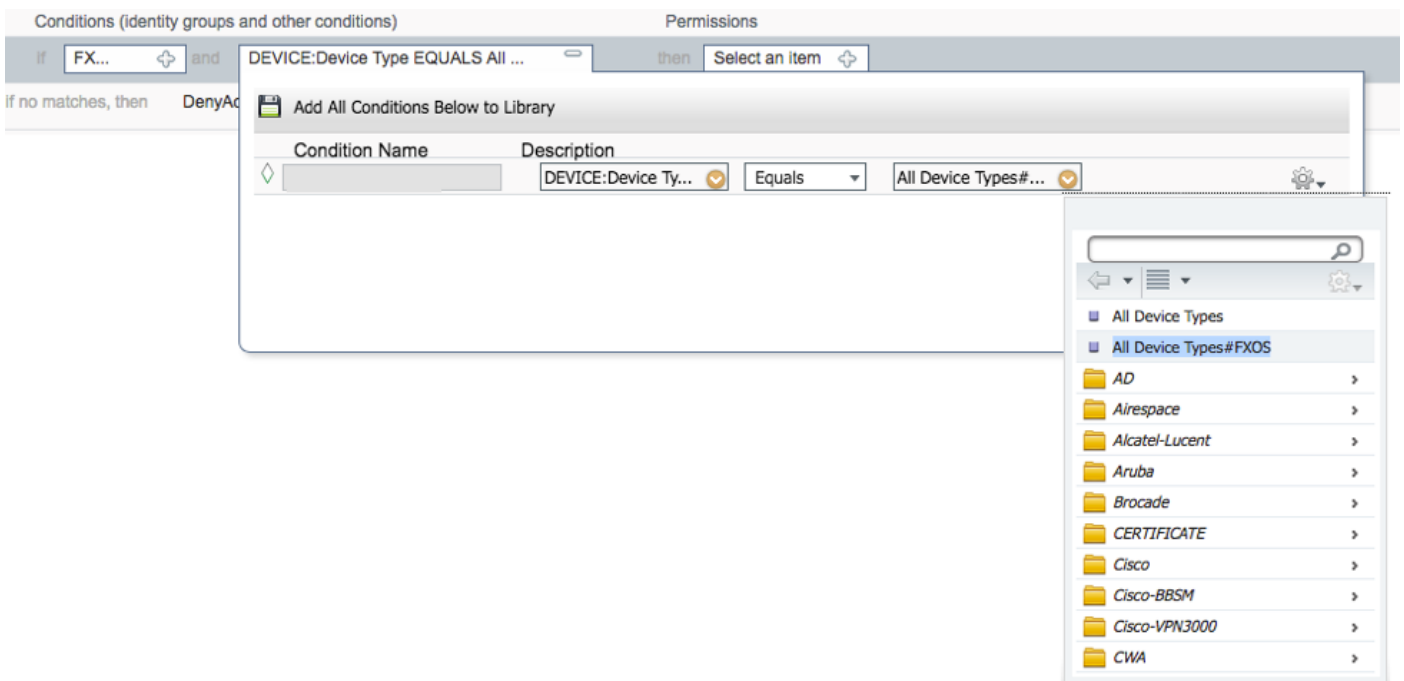
2.1. Naam van de regel: **De regel van <USER ROLE>**.



2.2. Indien: Gebruikersidentiteitsgroepen > Selecteer **<USER ROLE>**.



2.3. EN: Maak nieuwe conditionering > Apparaat:Het type apparaat is gelijk aan **alle apparaten types #FXOS**.



2.4. Toestemmingen: Standaard > Kies het **profiel** van **gebruikersrol**

Permissions

then FXOS-A...

FXOS-ADMIN-PROFILE

Standard

- Blackhole_Wireless_Access
- Cisco_IP_Phones
- Cisco_WebAuth
- DenyAccess
- FXOS-AAA-PROFILE
- FXOS-ADMIN-PROFILE**
- FXOS-OPER-PROFILE
- FXOS-ReadOnly-PROFILE
- NSP_Onboard
- Non_Cisco_IP_Phones
- PermitAccess

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Fxos Admin Rule	if FXOS ADMIN AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-ADMIN-PROFILE

Stap 3. Herhaal stap 2 voor alle gebruikersrollen.

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Fxos Admin Rule	if FXOS ADMIN AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-ADMIN-PROFILE
<input checked="" type="checkbox"/>	Fxos AAA Rule	if FXOS AAA AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-AAA-PROFILE
<input checked="" type="checkbox"/>	Fxos Oper Rule	if FXOS OPER AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-OPER-PROFILE
<input checked="" type="checkbox"/>	Fxos Read only Rule	if FXOS Read Only AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-ReadOnly-PROFILE
<input checked="" type="checkbox"/>	Default	if no matches, then DenyAccess	

Stap 4. Klik op **Opslaan** onder op de pagina.

Save

Reset

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 **FPR4120-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

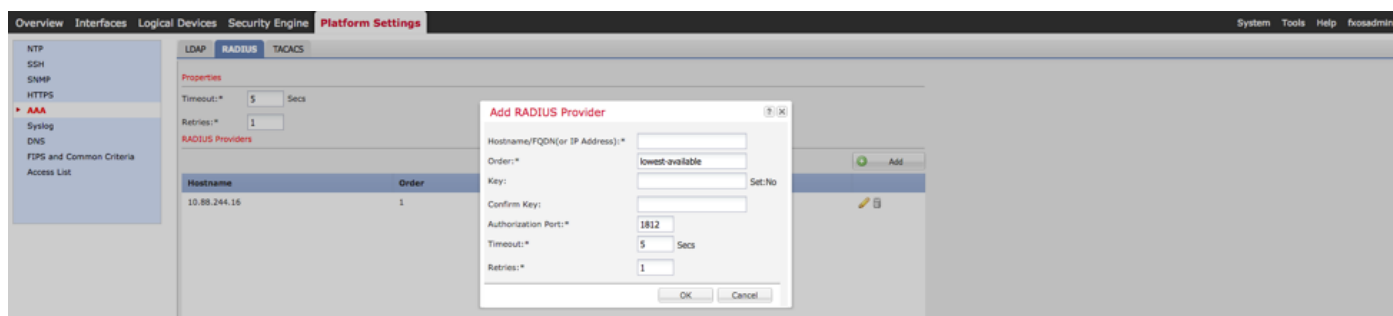
FPR4120-TAC-A#connect fxos

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

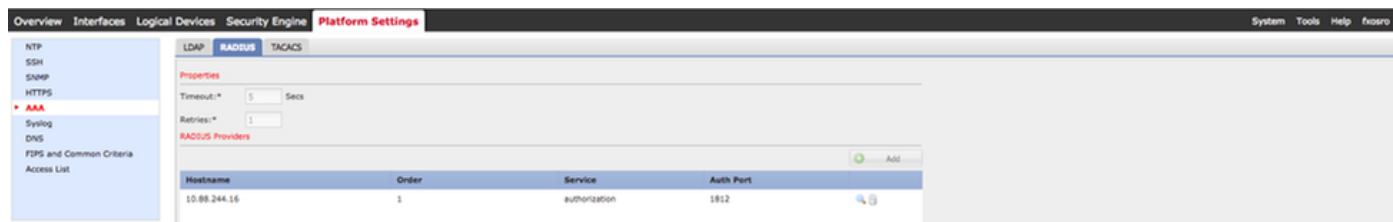
% Toestemming geweigerd voor de rol

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

Gebruiker beheren.



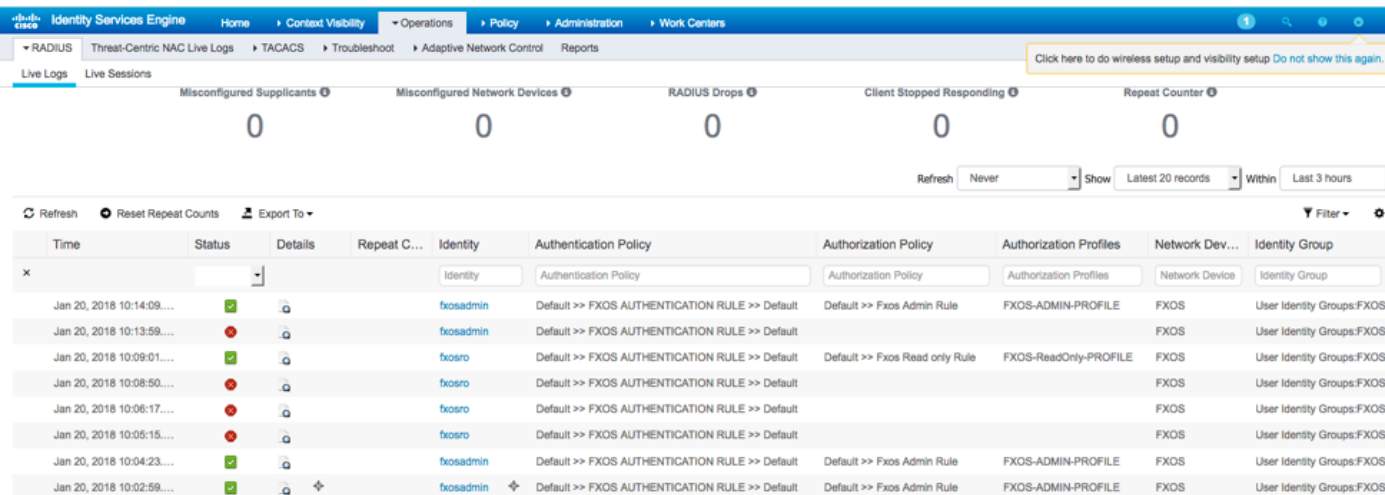
Alleen-lezen gebruikersrol.



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

ISE 2.0 Verificatie

1. Navigeer naar **Operations > RADIUS > Live logs**. 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 20 17:18:02:410275 aaa: aaa_req_process voor authenticatie. zitting nr. 0

2018 jan 20 17:18:02:410297 aaa: aaa_req_process: Algemeen AAA-verzoek van toepassing: aanmelding appln_subtype: standaard

2018 jan 20 17:18:02:410310 aaa: probeer_next_aaa_methode

2018 jan. 20 17:18:02.410330 aaa: in totaal zijn de methoden 1 , de huidige te beproeven index is 0

2018 jan. 20 17:18:02.41034 aaa: handle_req_gebruikt_methode

2018 jan 20 17:18:02:410356 aaa: AAA_METHOD_SERVER_GROUP

2018 jan. 20 17:18:02.410367 aaa: aaa_sg_methode_handler groep = straal

2018 jan 20 17:18:02:410379 aaa: Het gebruik van sg_protocol dat naar deze functie wordt doorgegeven

2018 jan 20 17:18:02:410393 aaa: Aanvraag naar RADIUS-service verzenden

2018 jan. 20 17:18:02.412944 aaa: mts_send_msg_to_prot_daemon: Loodlengte = 374

2018 jan 20 17:18:02.412973 aaa: zitting : 0x8df68c toegevoegd aan de sessietabel 1

2018 jan. 20 17:18:02.412987 aaa: Configureer methodegroep succesvol

2018 jan. 20 17:18:02.656425 aaa: aaa_proces_fd_set

2018 jan. 20 17:18:02.65647 aaa: aaa_process_fd_set: Back-uplijn

2018 jan. 20 17:18:02.656470 aaa: mts_message_response_handler: reactie op mts

2018 jan 20 17:18:02.656483 aaa: prot_daemon_reponse_handler

2018 jan 20 17:18:02.656497 aaa: zitting : 0x8df68c verwijderd uit de sessietabel 0

2018 jan 20 17:18:02.656512 aaa: is_a_rep_status_successtatus = 1

2018 jan 20 17:18:02.656525 aaa: is_a_rep_status_successie is TRUE

2018 jan. 20 17:18:02.656538 aaa: aaa_send_client_response voor authenticatie. sessie->flags=21.aaa_resp->flags=0.

2018 jan. 20 17:18:02.656550 aaa: AAA_REQ_FLAG_NORMAAL

2018 jan 20 17:18:02.65657 aaa: mts_send_response Succesvol

2018 jan 20 17:18:02:700520 aaa: aaa_process_fd_set: Back-uplijn op aaa_accounting_q

2018 jan 20 17:18:02:70068 aaa: OUDE OPCODE: accounting_interim_update

2018 jan 20 17:18:02:700702 aaa: aaa_aangemaakt_local_acct_req: gebruiker=, sessie_id=, log=added files

2018 jan 20 17:18:02:700725 aaa: aaa_req_process voor accounting. zitting nr. 0

2018 jan 20 17:18:02.700738 aaa: MTS aanvraag referentie is NULL. LOKALE AANVRAAG

2018 jan 20 17:18:02.700749 aaa: AAA_REQ_RESPONSE_NOT_NOED instellen

2018 jan 20 17:18:02.700762 aaa: aaa_req_process: Algemeen AAA-verzoek van toepassing: standaard appln_subtype: standaard

2018 jan 20 17:18:02.700774 aaa: probeer_next_aaa_methode

2018 jan 20 17:18:02:700798 aaa: geen standaardinstellingen voor methoden

2018 jan 20 17:18:02.700-810 aaa: geen configuratie beschikbaar voor dit verzoek

2018 jan 20 17:18:02:700997 aaa: aaa_send_client_response voor accounting. sessie->flags=254.aaa_rep->flags=0.

2018 jan. 20 17:18:02.701010 aaa: antwoord op een verzoek om boekhouding van de oude bibliotheek zal als SUCCESS worden verstuurd

2018 jan 20 17:18:02:701021 aaa: antwoord niet nodig voor dit verzoek

2018 jan 20 17:18:02:701033 aaa: AAA_REQ_FLAG_LOCAL_RESP

2018 jan. 20 17:18:02.701044 aaa: aaa_schoonmaak_sessie

2018 jan 20 17:18:02:701055 aaa: Aa_req moet worden vrijgelaten.

2018 jan. 20 17:18:02.701067 aaa: Terugvalmethode plaatselijk

2018 jan 20 17:18:02:706922 aaa: aaa_proces_fd_set

2018 jan 20 17:18:02:706937 aaa: aaa_process_fd_set: Back-uplijn op aaa_accounting_q

2018 jan 20 17:18:02:706959 aaa: OUDE OPCODE: accounting_interim_update

2018 jan 20 17:18:02:706972 aaa: aaa_aangemaakt_local_acct_req: gebruiker=, sessie_id=, log=added gebruiker:fxosro aan de rol:alleen-lezen

Na een mislukte verificatiepoging ziet u de volgende uitvoer.

2018 jan 20 17:15:18:102130 aaa: aaa_proces_fd_set

2018 jan 20 17:15:18:102149 aaa: aaa_process_fd_set: Back-uplijn

2018 jan 20 17:15:18:102267 aaa: aaa_proces_fd_set

2018 jan 20 17:15:18:102281 aaa: aaa_process_fd_set: Back-uplijn

2018 jan 20 17:15:18:102363 aaa: aaa_proces_fd_set

2018 jan 20 17:15:18:102377 aaa: aaa_process_fd_set: Back-uplijn

2018 jan 20 17:15:18:102456 aaa: aaa_proces_fd_set

2018 jan 20 17:15:18:102468 aaa: aaa_process_fd_set: Back-uplijn

2018 jan 20 17:15:18:102489 aaa: mts_aaa_req_proces

2018 jan 20 17:15:18:102503 aaa: aaa_req_process voor authenticatie. zitting nr. 0

2018 jan 20 17:15:18:102526 aaa: aaa_req_process: Algemeen AAA-verzoek van toepassing: aanmelding appln_subtype: standaard

2018 jan 20 17:15:18:102540 aaa: probeer_next_aaa_methode

2018 jan 20 17:15:18:102562 aaa: in totaal zijn de methoden 1 , de huidige te beproeven index is 0

2018 jan 20 17:15:18:102575 aaa: handle_req_gebruikt_methode

2018 jan 20 17:15:18:102586 aaa: AAA_METHOD_SERVER_GROUP

2018 jan 20 17:15:18:102598 aaa: aaa_sg_methode_handler groep = straal

2018 jan 20 17:15:18:102610 aaa: Het gebruik van sg_protocol dat naar deze functie wordt doorgegeven

2018 jan 20 17:15:18:102625 aaa: Aanvraag naar RADIUS-service verzenden

2018 jan 20 17:15:18:102658 aaa: mts_send_msg_to_prot_daemon: Loodlengte = 371

2018 jan 20 17:15:18:102684 aaa: zitting : 0x8df68c toegevoegd aan de sessietabel 1

2018 jan 20 17:15:18:102698 aaa: Configureer methodegroep succesvol

2018 jan 20 17:15:18:273682 aaa: aaa_proces_fd_set

2018 jan 20 17:15:18:273724 aaa: aaa_process_fd_set: Back-uplijn

2018 jan 20 17:15:18:273753 aaa: mts_message_response_handler: reactie op mts

2018 jan 20 17:15:18:273768 aaa: prot_daemon_reponse_handler

2018 jan 20 17:15:18:273783 aaa: zitting : 0x8df68c verwijderd uit de sessietabel 0

2018 jan 20 17:15:18:273801 aaa: is_a_rep_status_successtatus = 2

2018 jan 20 17:15:18:273815 aaa: is_a_rep_status_successie is TRUE

2018 jan 20 17:15:18:273829 aaa: aaa_send_client_response voor authenticatie. sessie->flags=21.aaa_resp->flags=0.

2018 jan 20 17:15:18:273843 aaa: AAA_REQ_FLAG_NORMAAL

2018 jan 20 17:15:18:27387 aaa: mts_send_response Succesvol

2018 jan 20 17:15:18:273902 aaa: aaa_schoonmaak_sessie

2018 jan 20 17:15:18:273916 aaa: mts_drop-applicatie voor msg

2018 jan 20 17:15:18:273935 aaa: Aa_req moet worden vrijgelaten.

2018 jan 20 17:15:18:280416 aaa: aaa_proces_fd_set

2018 jan 20 17:15:18:280443 aaa: aaa_process_fd_set: Back-uplijn

2018 jan 20 17:15:18:280454 aaa: aaa_wellicht_info_fig: GET_REQ voor ABBYY inlogfoutmelding

2018 jan 20 17:15:18:280460 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.

Plug-in: [CSCvg87518](#)