

Systeme d'exploitation extensible de FirePOWER (FXOS) 2.2 : Authentification/autorisation de châssis pour la gestion à distance avec ISE utilisant RADIUS

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configurer le châssis FXOS](#)

[Configurer le serveur ISE](#)

[Vérifiez](#)

[Vérification FXOS Chasis](#)

[Vérification ISE 2.0](#)

[Dépannez](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer l'authentification et l'autorisation de RADIUS pour le châssis du système d'exploitation extensible de FirePOWER (FXOS) par l'intermédiaire du Cisco Identity Services Engine (ISE).

Le châssis FXOS inclut les rôles de l'utilisateur suivants :

- Administrateur - Complete lecture-et-écrivent l'accès au système entier. Le compte par défaut d'admin est assigné ce rôle par défaut et il ne peut pas être changé.
- En lecture seule - Accès en lecture seule à la configuration de système sans des privilèges de modifier l'état du système.
- Des exécutions - Lecture-et-écrivez l'accès à la configuration de NTP, à la configuration de Smart Call Home pour l'autorisation intelligente, et aux logs système, y compris des serveurs de Syslog et des défauts. Accès en lecture au reste du système.
- AAA - Lecture-et-écrivez l'accès aux utilisateurs, aux rôles, et à la configuration d'AAA. Accès en lecture au reste du système.

Par l'intermédiaire du CLI ceci peut être vu comme suit :

```
fpr4120-TAC-A /security * # show role
```

Rôle :

Role name Priv

----- ----

AAA d'AAA

admin d'admin

exécutions d'exécutions

en lecture seule en lecture seule

Contribué par Remirez élégant, Jose Soto, ingénieurs TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La connaissance du système d'exploitation extensible de FirePOWER (FXOS)
- La connaissance de la configuration ISE

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 2.2 d'appareils de Sécurité de Cisco FirePOWER 4120
- Logiciel Cisco Identity Services Engine virtuel 2.2.0.470

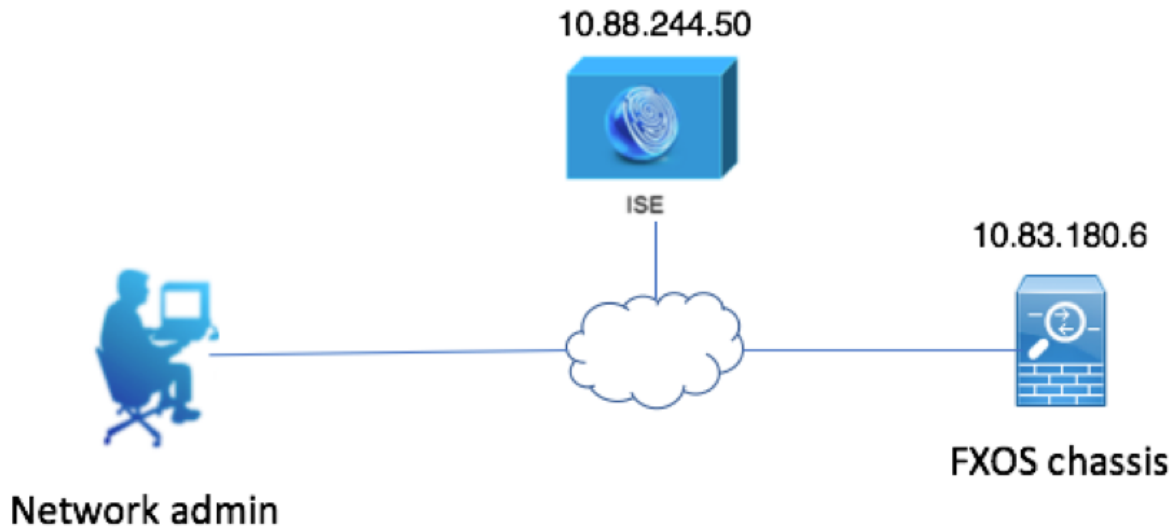
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Le but de la configuration est à :

- Authentifiez les utilisateurs se connectant dans le GUI du Web du FXOS et le SSH au moyen d'ISE
- Autorisez les utilisateurs se connectant dans le GUI du Web du FXOS et le SSH selon leur rôle de l'utilisateur respectif au moyen d'ISE.
- Vérifiez le bon fonctionnement de l'authentification et de l'autorisation sur le FXOS au moyen d'ISE

Diagramme du réseau



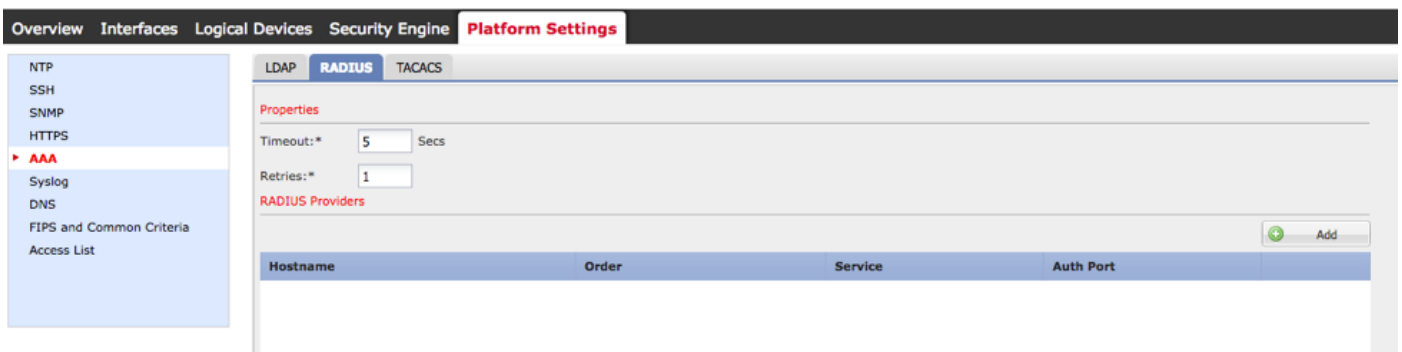
Configurations

Configurer le châssis FXOS

Création d'un fournisseur de RADIUS utilisant le gestionnaire de châssis

Étape 1. Naviguez vers des **configurations** > l'**AAA** de plate-forme.

Étape 2. Cliquez sur l'onglet de **RADIUS**.

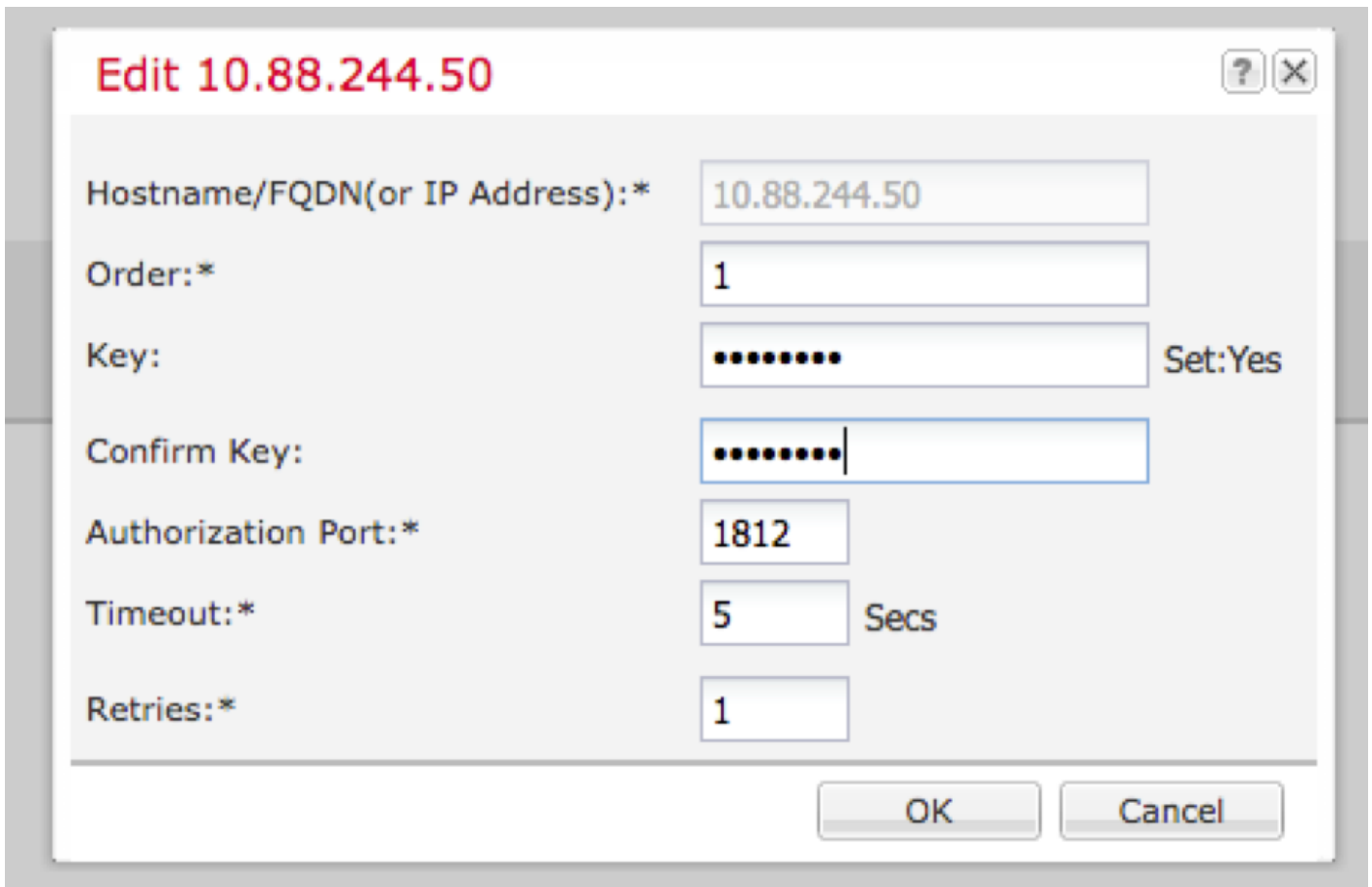


Étape 3. Pour chaque fournisseur de RADIUS que vous voulez ajouter (jusqu'à 16 fournisseurs).

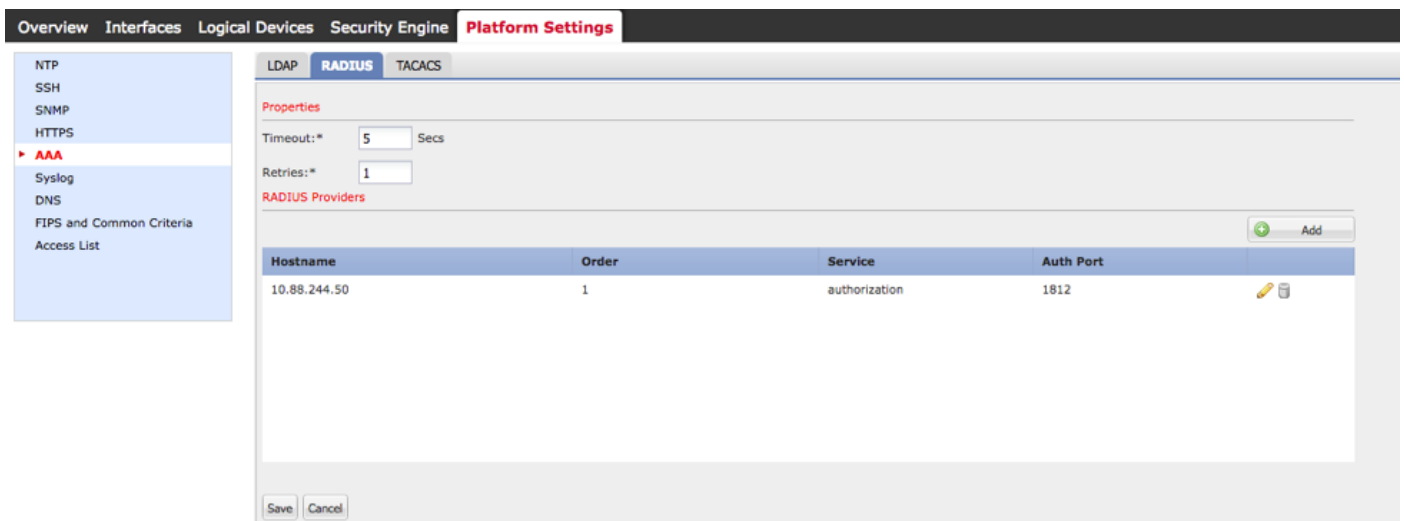
3.1. Dans la région de fournisseurs de RADIUS, cliquez sur Add.

3.2. Une fois la boîte de dialogue de fournisseur de RADIUS d'ajouter ouvre, écrit les valeurs exigées.

3.3. Cliquez sur OK pour fermer la boîte de dialogue de fournisseur de RADIUS d'ajouter.

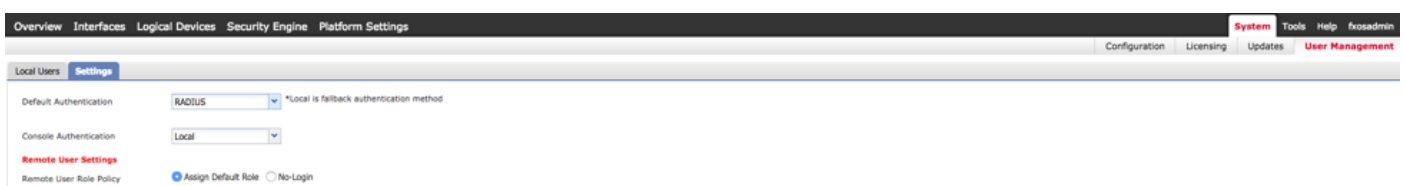


Étape 4. Sauvegarde de clic.



Étape 5. Naviguez vers le système > la gestion des utilisateurs > les configurations.

Étape 6. Sous l'authentification par défaut choisissez RADIUS.



Création d'un fournisseur de RADIUS utilisant le CLI

Étape 1. Afin d'activer l'authentification de RADIUS, exécutez les commandes suivantes.

Sécurité de portée fpr4120-TAC-A#

fpr4120-TAC-A /security # **par défaut-auth de portée**

fpr4120-TAC-A /security/default-auth # **a placé le rayon de royaume**

Étape 2. Utilisez la commande de **détail d'exposition** d'afficher les résultats.

fpr4120-TAC-A /security/default-auth # **détail d'exposition**

Authentification par défaut :

Royaume d'admin : **Radius**

Royaume opérationnel : **Radius**

La session Web régénèrent la période (en quelques sec) : 600

Délai d'attente de session (en quelques sec) pour le Web, ssh, sessions de telnet : 600

Délai d'attente de session absolu (en quelques sec) pour le Web, ssh, sessions de telnet : 3600

Délai d'attente de session de console série (en quelques sec) : 600

Délai d'attente de session absolu de console série (en quelques sec) : 3600

Groupe de serveurs d'authentification d'admin :

Groupe de serveurs opérationnel d'authentification :

Utilisation de 2ème facteur : Non

Étape 3. Afin de configurer des paramètres de serveur de RADIUS exécutez les commandes suivantes.

Sécurité de portée fpr4120-TAC-A#

fpr4120-TAC-A /security # **rayon de portée**

fpr4120-TAC-A /security/radius # **présentent le serveur 10.88.244.50**

fpr4120-TAC-A /security/radius/server # **a placé le descr « serveur ISE »**

fpr4120-TAC-A /security/radius/server * # **placez la clé**

Introduisez la clé : *********

Confirmez la clé : *********

Étape 4. Utilisez la commande de **détail d'exposition** d'afficher les résultats.

fpr4120-TAC-A /security/radius/server * # détail d'exposition

Serveur de RADIUS :

Adresse Internet, FQDN ou adresse IP : 10.88.244.50

Descr :

Commande : 1

Port authentique : 1812

Clé : ****

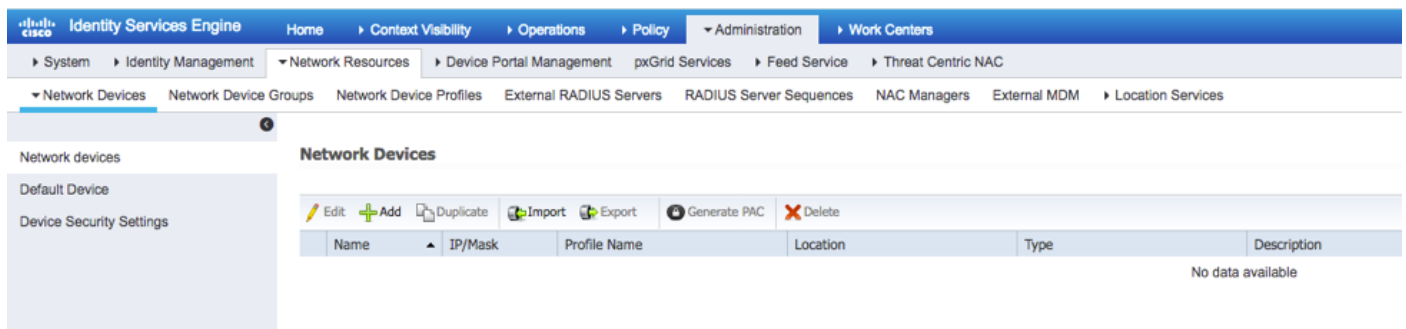
Délai d'attente : 5

Configurer le serveur ISE

Ajouter le FXOS comme ressource de réseau

Étape 1. Naviguez vers la **gestion > les ressources de réseau > les périphériques de réseau.**

Étape 2. Cliquez sur Add



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The left sidebar shows the navigation menu with 'Network Devices' selected. The main content area is titled 'Network Devices' and contains a toolbar with icons for Edit, Add, Duplicate, Import, Export, Generate PAC, and Delete. Below the toolbar is a table with columns: Name, IP/Mask, Profile Name, Location, Type, and Description. The table is currently empty, with the text 'No data available' displayed at the bottom right.

Étape 3. Écrivez les valeurs requises (le nom, l'adresse IP, le type de périphérique et l'enable RADIUS et ajoutent la CLÉ), cliquez sur Submit.

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

Création des groupes et des utilisateurs d'identité

Étape 1. Naviguez vers la gestion > la Gestion de l'identité > les groupes > les groupes d'identité de l'utilisateur.

Étape 2. Cliquez sur 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

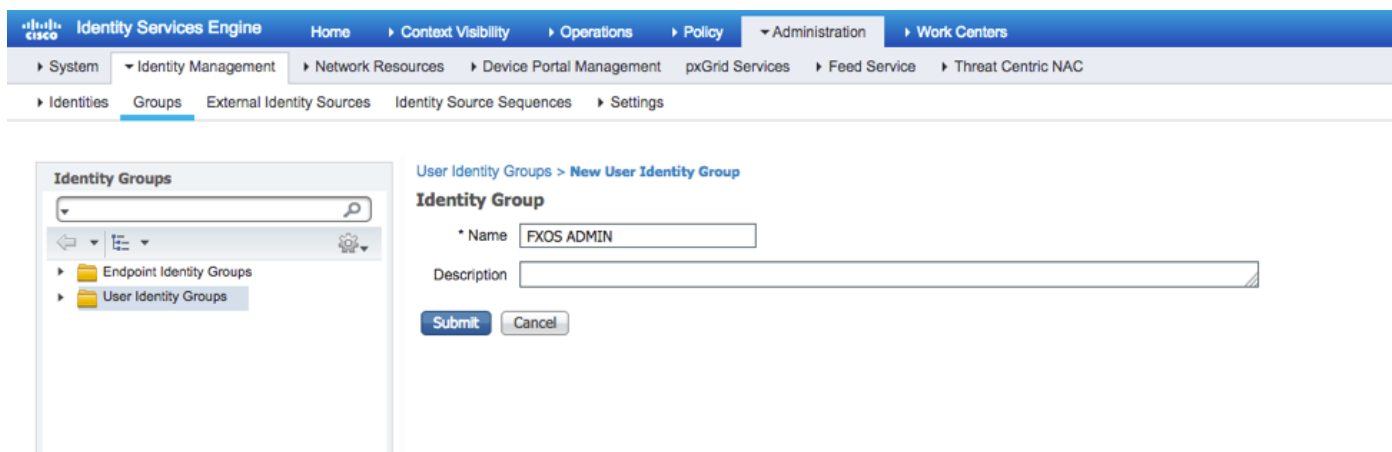
- Endpoint Identity Groups
- User Identity Groups

User Identity Groups

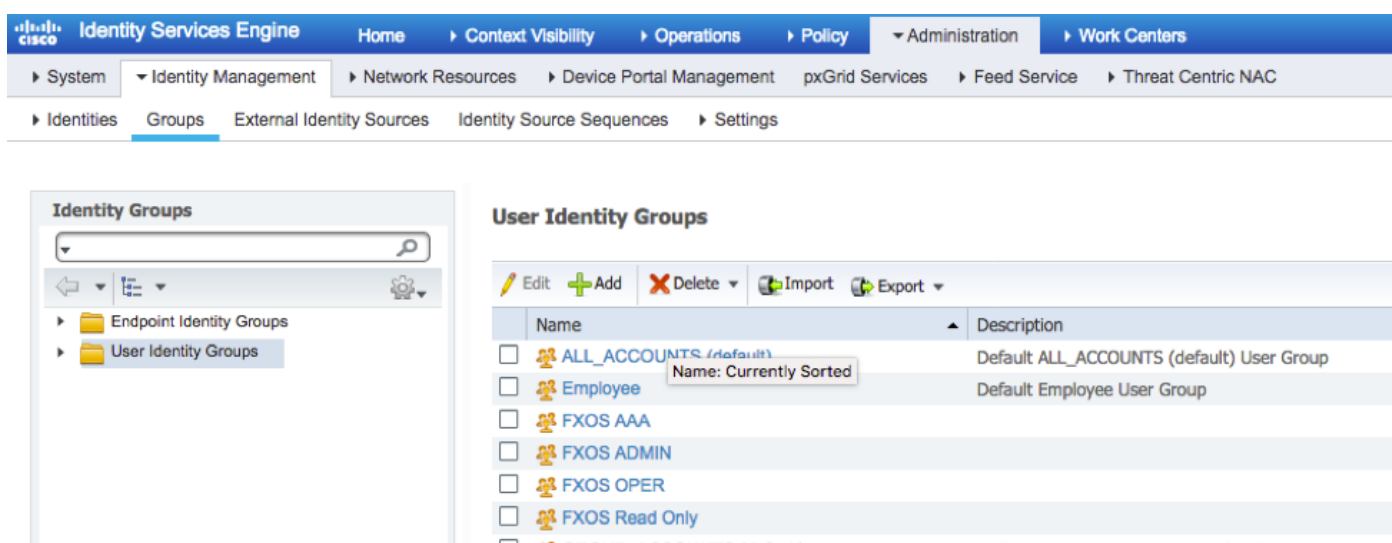
Edit Add Delete Import Export

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

Étape 3. Écrivez la valeur pour le nom et cliquez sur Submit.

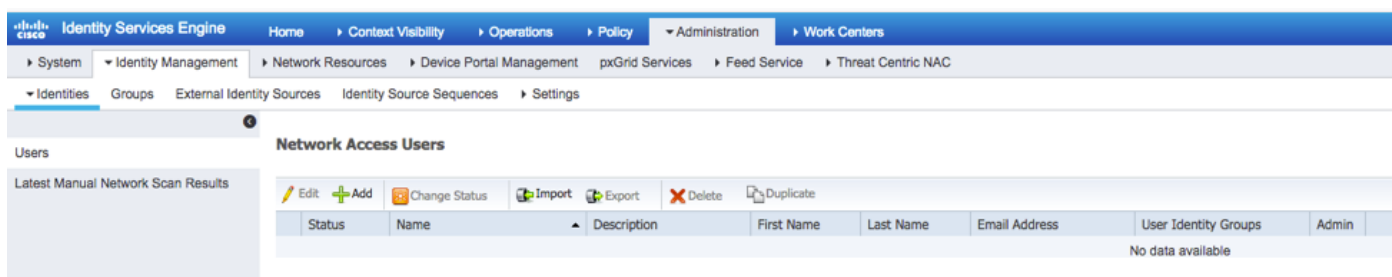


Étape 4. Répétez l'étape 3 pour tous les rôles de l'utilisateur requis.



Étape 5. Naviguez vers la gestion > la Gestion de l'identité > l'identité > les utilisateurs.

Étape 6. Cliquez sur Add.



Étape 7. Écrivez les valeurs requises (nom, groupe d'utilisateurs, mot de passe).

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:

Password: Re-Enter Password:

Enable Password:

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

Étape 8. Répétez l'étape 6 pour tous les utilisateurs requis.

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

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	

Création du profil d'autorisation pour chaque rôle de l'utilisateur

Étape 1. Naviguez vers la **stratégie > les éléments de stratégie > les résultats > l'autorisation > les profils d'autorisation**.

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

Étape 2. Remplissez tous les attributs pour le profil d'autorisation.

2.1. Configurez le nom de profil.

Authorization Profile

* Name:

Description:

* Access Type:

Network Device Profile:

2.2. Dans des **attributs avancés** les configurations configurent le CISCO-AV-PAIR suivant **cisco-av-pair=shell : roles= " admin »**

Advanced Attributes Settings

=

2.3. Cliquez sur **Save**.

Save **Reset**

Étape 3. Répétez l'étape 2 pour les rôles de l'utilisateur restants utilisant les Cisco-POIDs du

commerce-paires suivantes

cisco-av-pair=shell : roles= " AAA »

cisco-av-pair=shell : roles= " exécutions »

cisco-av-pair=shell : roles= " en lecture seule »

▼ **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

Dictionary Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Standard Authorization Profiles

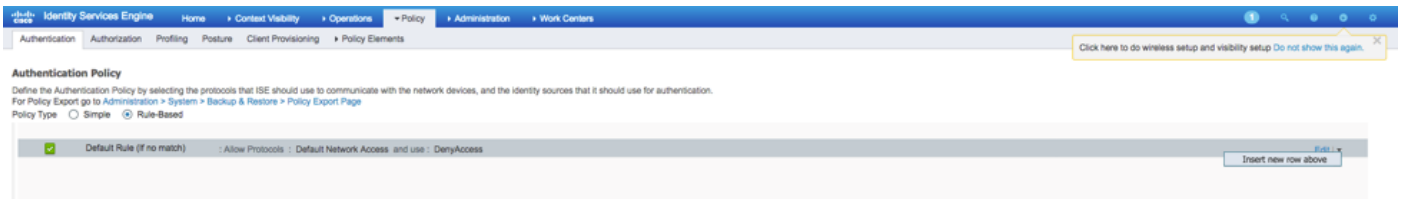
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

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

Création de la stratégie d'authentification

Étape 1. Naviguez vers la **stratégie > l'authentification >** et cliquez sur la flèche à côté de éditent où vous voulez créer la règle.



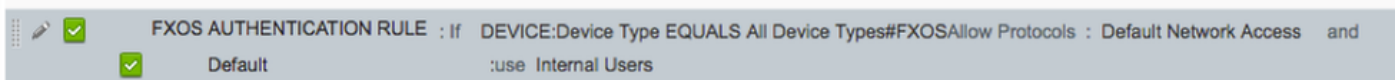
Étape 2. L'installation est simple ; il peut être plus granulaire fait mais pour cet exemple nous utiliserons le type de périphérique :

Nom : **RÈGLE D'AUTHEMIFICATION FXOS**

SI nouveaux attribut/valeur choisis : **Périphérique : Le type de périphérique égale tous les types de périphériques #FXOS**

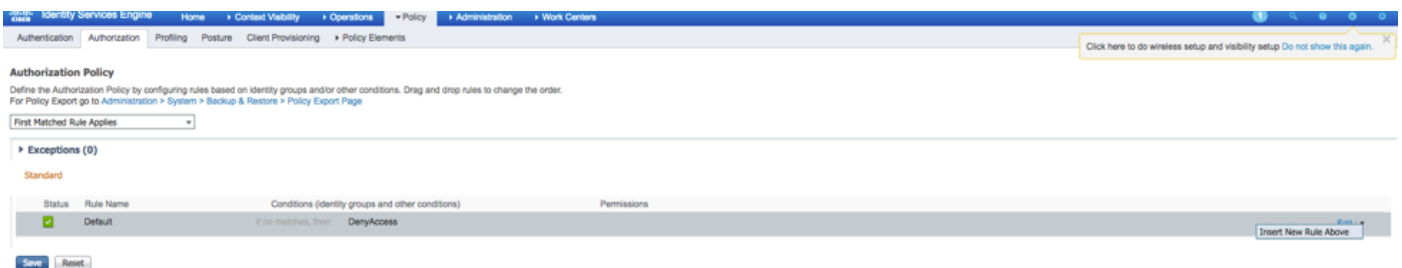
Permettez les protocoles : **Accès au réseau par défaut**

Utilisation : **Utilisateurs internes**



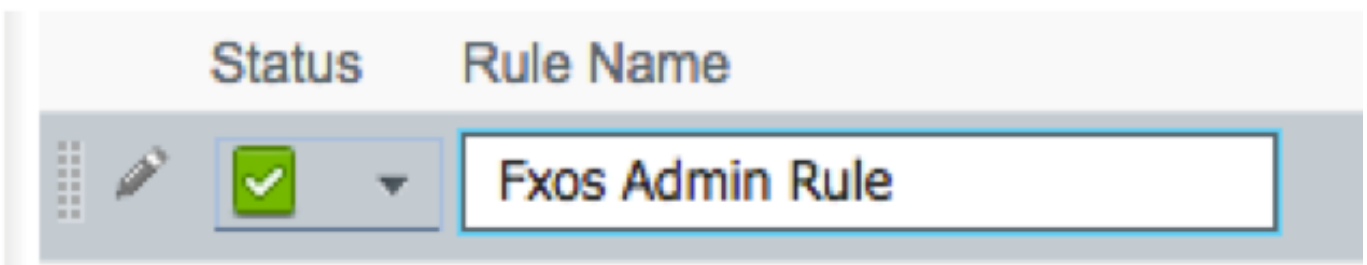
Création de la stratégie d'autorisation

Étape 1. Naviguez vers la **stratégie > l'autorisation >** et cliquez sur le net de flèche pour éditer où vous voulez créer la règle.

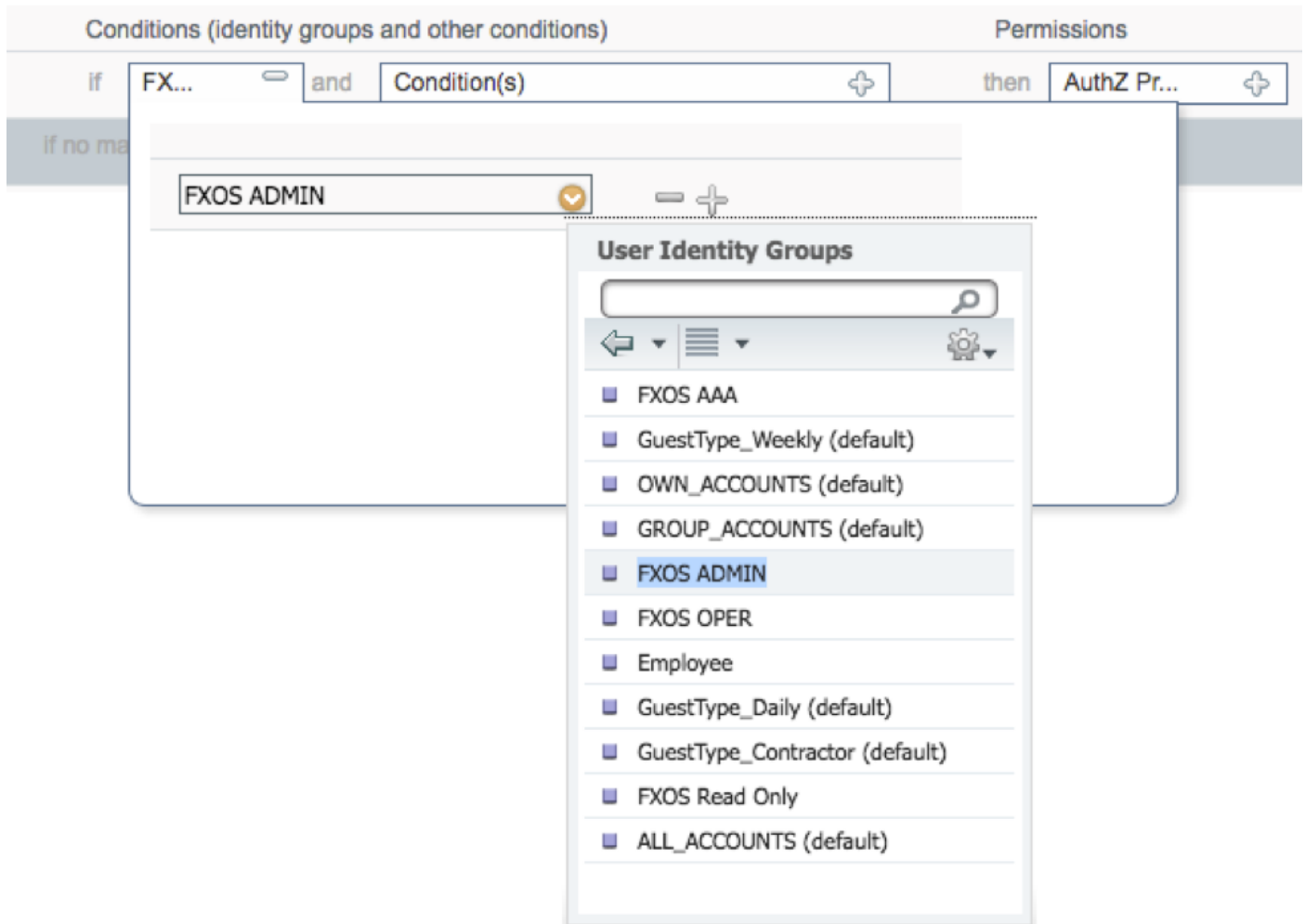


Étape 2. Écrivez les valeurs pour la règle d'autorisation avec les paramètres requis.

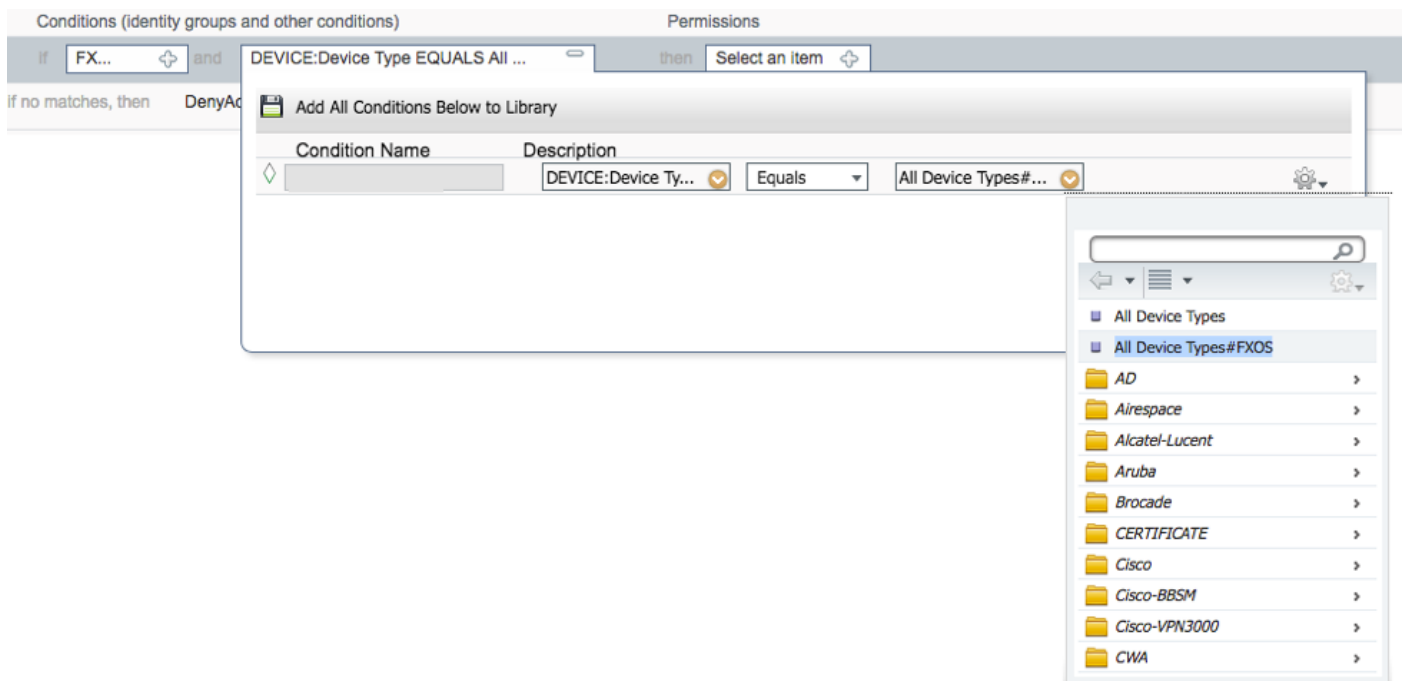
2.1. Nom de règle : **Règle de Fxos <USER ROLE>**.



2.2. Si : **Groupes d'identité de l'utilisateur > <USER choisi ROLE>**.



2.3. ET : Créez le nouveaux état > périphérique : Le type de périphérique égale tous les types de périphériques #FXOS.



2.4. Autorisations : La norme > choisissent le rôle de l'utilisateur de profil

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

Étape 3. Répétez l'étape 2 pour tous les rôles de l'utilisateur.

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	

Étape 4. **Sauvegarde de clic** au bas de page.

Save

Reset

Vérifiez

Vous pouvez maintenant examiner chaque utilisateur et vérifier le rôle de l'utilisateur assigné.

Vérification FXOS Chassis

1. Telnet ou SSH au châssis FXOS et procédure de connexion utilisant les utilisateurs créés l'uns des sur l'ISE.

Nom d'utilisateur : fxosadmin

Mot de passe :

Sécurité de portée fpr4120-TAC-A#

fpr4120-TAC-A /security # **petit groupe d'utilisateur distant d'exposition**

Fxosaaa d'utilisateur distant :

Description :

Rôles de l'utilisateur :

Nom : **AAA**

Nom : **en lecture seule**

Fxosadmin d'utilisateur distant :

Description :

Rôles de l'utilisateur :

Nom : **admin**

Nom : **en lecture seule**

Fxosoper d'utilisateur distant :

Description :

Rôles de l'utilisateur :

Nom : **exécutions**

Nom : **en lecture seule**

Fxosro d'utilisateur distant :

Description :

Rôles de l'utilisateur :

Nom : **en lecture seule**

Selon le nom d'utilisateur écrit le châssis FXOS le cli affichera seulement les commandes autorisées pour le rôle de l'utilisateur assigné.

Rôle de l'utilisateur d'admin.

fpr4120-TAC-A /security # ?

reconnaissez reconnaissent

sessions de clear user de clair-utilisateur-sessions

créez les objets gérés Create

objets gérés par effacement d'effacement

le débranchement désactive des services

l'enable active des services

entrez écrit un objet géré

la portée change le mode courant

placez les valeurs d'une propriété réglées

affichez les informations de show system

terminez les sessions de l'Active cimc

fpr4120-TAC-A# **connectent des fxos**

fpr4120-TAC-A (fxos) # **AAA-demandes de debug aaa**

fpr4120-TAC-A (fxos) #

Rôle de l'utilisateur en lecture seule.

fpr4120-TAC-A /security # ?

la portée change le mode courant

placez les valeurs d'une propriété réglées

affichez les informations de show system

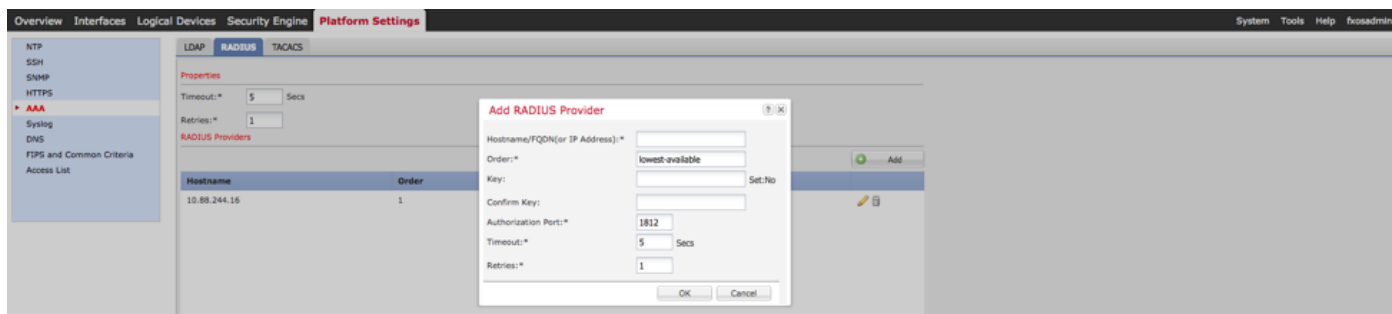
fpr4120-TAC-A# connectent des fxos

fpr4120-TAC-A (fxos) # AAA-demandes de debug aaa

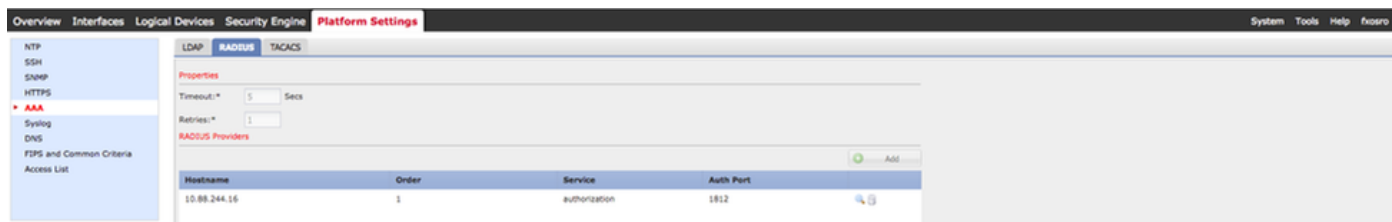
% d'autorisation refusée pour le rôle

2. Parcourez à l'adresse IP et à la procédure de connexion de châssis FXOS utilisant les utilisateurs créés l'uns des sur l'ISE.

Rôle de l'utilisateur d'admin.



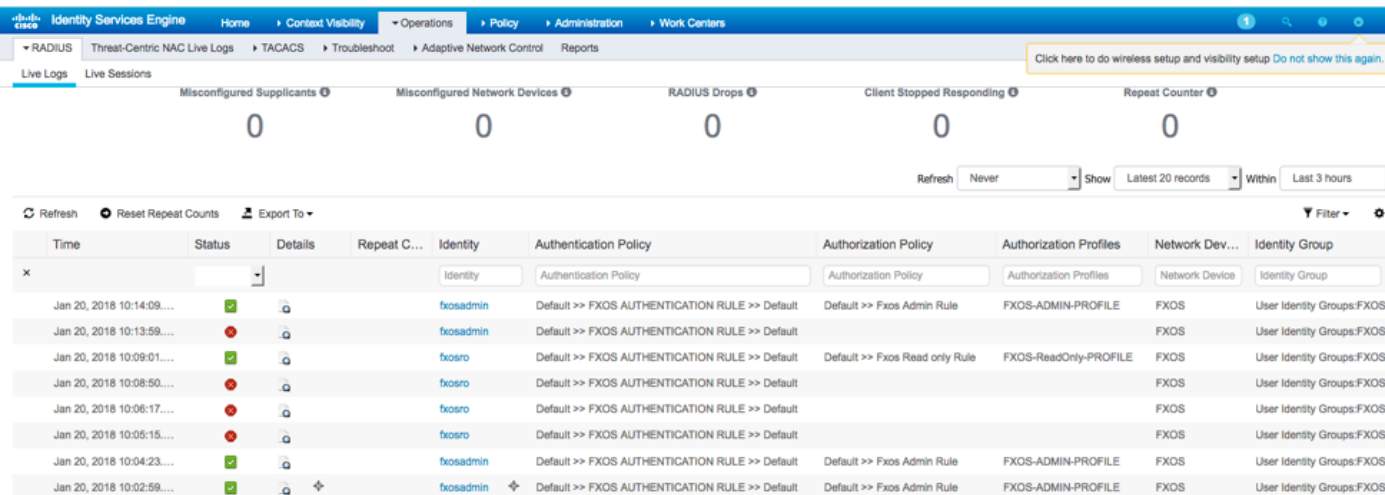
Rôle de l'utilisateur en lecture seule.



Note: Notez que le bouton d'AJOUTER est greyed.

Vérification ISE 2.0

1. Naviguez vers des exécutions > RADIUS > vivent des logs. Vous devriez pouvoir voir réussi et des essais ratés.



Dépannez

Le debug aaa authentication et l'autorisation exécutent les commandes suivantes dans le FXOS cli.

```
fpr4120-TAC-A# connectent des fxos
```

```
fpr4120-TAC-A (fxos) # AAA-demandes de debug aaa
```

```
fpr4120-TAC-A (fxos) # événement de debug aaa
```

```
fpr4120-TAC-A (fxos) # erreurs de debug aaa
```

```
fpr4120-TAC-A (fxos) # terme lundi
```

Après qu'une tentative réussie d'authentification, vous voie la sortie suivante.

```
2018 AAAs du 20 janvier 17:18:02.410275 : aaa_req_process pour l'authentification. session No. 0
```

```
2018 AAAs du 20 janvier 17:18:02.410297 : aaa_req_process : Demande de général AAA d'appln  
: appln_subtype de procédure de connexion : par défaut
```

```
2018 AAAs du 20 janvier 17:18:02.410310 : try_next_aaa_method
```

```
2018 AAAs du 20 janvier 17:18:02.410330 : les méthodes totales configurées est 1, index en  
cours à essayer est 0
```

```
2018 AAAs du 20 janvier 17:18:02.410344 : handle_req_using_method
```

```
2018 AAAs du 20 janvier 17:18:02.410356 : AAA_METHOD_SERVER_GROUP
```

```
2018 AAAs du 20 janvier 17:18:02.410367 : groupe = rayon d'aaa_sg_method_handler
```

```
2018 AAAs du 20 janvier 17:18:02.410379 : Utilisant le sg_protocol qui est passé à cette fonction
```

```
2018 AAAs du 20 janvier 17:18:02.410393 : Envoi de la demande au service RADIUS
```

```
2018 AAAs du 20 janvier 17:18:02.412944 : mts_send_msg_to_prot_daemon : Longueur de  
charge utile = 374
```

```
2018 AAAs du 20 janvier 17:18:02.412973 : session : 0x8dfd68c ajouté au tableau 1 de session
```

```
2018 AAAs du 20 janvier 17:18:02.412987 : Groupe configuré de méthode réussi
```

```
2018 AAAs du 20 janvier 17:18:02.656425 : aaa_process_fd_set
```

```
2018 AAAs du 20 janvier 17:18:02.656447 : aaa_process_fd_set : mtscallback sur l'aaa_q
```

```
2018 AAAs du 20 janvier 17:18:02.656470 : mts_message_response_handler : une réponse de  
mts
```

```
2018 AAAs du 20 janvier 17:18:02.656483 : prot_daemon_reponse_handler
```

2018 AAAs du 20 janvier 17:18:02.656497 : session : 0x8dfd68c retiré du tableau 0 de session

2018 AAAs du 20 janvier 17:18:02.656512 : état d'is_aaa_resp_status_success = 1

2018 AAAs du 20 janvier 17:18:02.656525 : les is_aaa_resp_status_success est VRAI

2018 AAAs du 20 janvier 17:18:02.656538 : aaa_send_client_response pour l'authentification. session->flags=21. aaa_resp->flags=0.

2018 AAAs du 20 janvier 17:18:02.656550 : AAA_REQ_FLAG_NORMAL

2018 AAAs du 20 janvier 17:18:02.656577 : mts_send_response réussi

2018 AAAs du 20 janvier 17:18:02.700520 : aaa_process_fd_set : mtscallback sur l'aaa_accounting_q

2018 AAAs du 20 janvier 17:18:02.700688 : VIEIL OP CODE : accounting_interim_update

2018 AAAs du 20 janvier 17:18:02.700702 : aaa_create_local_acct_req : user=, session_id=, fxsro log=added d'utilisateur

2018 AAAs du 20 janvier 17:18:02.700725 : aaa_req_process pour la comptabilité. session No. 0

2018 AAAs du 20 janvier 17:18:02.700738 : La référence de demande MTS est NULLE. Demande LOCALE

2018 AAAs du 20 janvier 17:18:02.700749 : Établissement d'AAA_REQ_RESPONSE_NOT_NEEDED

2018 AAAs du 20 janvier 17:18:02.700762 : aaa_req_process : Demande de général AAA d'appln : appln_subtype par défaut : par défaut

2018 AAAs du 20 janvier 17:18:02.700774 : try_next_aaa_method

2018 AAAs du 20 janvier 17:18:02.700798 : aucune méthodes configurées pour le par défaut de par défaut

2018 AAAs du 20 janvier 17:18:02.700810 : aucune configuration disponible pour ceci demande

2018 AAAs du 20 janvier 17:18:02.700997 : aaa_send_client_response pour la comptabilité. session->flags=254. aaa_resp->flags=0.

2018 AAAs du 20 janvier 17:18:02.701010 : la réponse pour la demande de comptabilité de la vieille bibliothèque sera envoyée comme SUCCÈS

2018 AAAs du 20 janvier 17:18:02.701021 : réponse non requise pour cette demande

2018 AAAs du 20 janvier 17:18:02.701033 : AAA_REQ_FLAG_LOCAL_RESP

2018 AAAs du 20 janvier 17:18:02.701044 : aaa_cleanup_session

2018 AAAs du 20 janvier 17:18:02.701055 : l'aaa_req devrait être libéré.

2018 AAAs du 20 janvier 17:18:02.701067 : Tombent de retour les gens du pays de méthode réussis

2018 AAAs du 20 janvier 17:18:02.706922 : aaa_process_fd_set

2018 AAAs du 20 janvier 17:18:02.706937 : aaa_process_fd_set : mtscallback sur l'aaa_accounting_q

2018 AAAs du 20 janvier 17:18:02.706959 : VIEIL OPCODE : accounting_interim_update

2018 AAAs du 20 janvier 17:18:02.706972 : aaa_create_local_acct_req : user=, session_id=, utilisateur log=added : fxosro au rôle : en lecture seule

Après qu'une tentative d'authentification défailante, vous voie la sortie suivante.

2018 AAAs du 20 janvier 17:15:18.102130 : aaa_process_fd_set

2018 AAAs du 20 janvier 17:15:18.102149 : aaa_process_fd_set : mtscallback sur l'aaa_q

2018 AAAs du 20 janvier 17:15:18.102267 : aaa_process_fd_set

2018 AAAs du 20 janvier 17:15:18.102281 : aaa_process_fd_set : mtscallback sur l'aaa_q

2018 AAAs du 20 janvier 17:15:18.102363 : aaa_process_fd_set

2018 AAAs du 20 janvier 17:15:18.102377 : aaa_process_fd_set : mtscallback sur l'aaa_q

2018 AAAs du 20 janvier 17:15:18.102456 : aaa_process_fd_set

2018 AAAs du 20 janvier 17:15:18.102468 : aaa_process_fd_set : mtscallback sur l'aaa_q

2018 AAAs du 20 janvier 17:15:18.102489 : mts_aaa_req_process

2018 AAAs du 20 janvier 17:15:18.102503 : aaa_req_process pour l'authentification. session No. 0

2018 AAAs du 20 janvier 17:15:18.102526 : aaa_req_process : Demande de général AAA d'appln : appln_subtype de procédure de connexion : par défaut

2018 AAAs du 20 janvier 17:15:18.102540 : try_next_aaa_method

2018 AAAs du 20 janvier 17:15:18.102562 : les méthodes totales configurées est 1, index en cours à essayer est 0

2018 AAAs du 20 janvier 17:15:18.102575 : handle_req_using_method

2018 AAAs du 20 janvier 17:15:18.102586 : AAA_METHOD_SERVER_GROUP

2018 AAAs du 20 janvier 17:15:18.102598 : groupe = rayon d'aaa_sg_method_handler

2018 AAAs du 20 janvier 17:15:18.102610 : Utilisant le sg_protocol qui est passé à cette fonction

2018 AAAs du 20 janvier 17:15:18.102625 : Envoi de la demande au service RADIUS

2018 AAAs du 20 janvier 17:15:18.102658 : mts_send_msg_to_prot_daemon : Longueur de charge utile = 371

2018 AAAs du 20 janvier 17:15:18.102684 : session : 0x8dfd68c ajouté au tableau 1 de session

2018 AAAs du 20 janvier 17:15:18.102698 : Groupe configuré de méthode réussi

2018 AAAs du 20 janvier 17:15:18.273682 : aaa_process_fd_set

2018 AAAs du 20 janvier 17:15:18.273724 : aaa_process_fd_set : mtscallback sur l'aaa_q

2018 AAAs du 20 janvier 17:15:18.273753 : mts_message_response_handler : une réponse de mts

2018 AAAs du 20 janvier 17:15:18.273768 : prot_daemon_reponse_handler

2018 AAAs du 20 janvier 17:15:18.273783 : session : 0x8dfd68c retiré du tableau 0 de session

2018 AAAs du 20 janvier 17:15:18.273801 : état d'is_aaa_resp_status_success = 2

2018 AAAs du 20 janvier 17:15:18.273815 : les is_aaa_resp_status_success est VRAI

2018 AAAs du 20 janvier 17:15:18.273829 : aaa_send_client_response pour l'authentification. session->flags=21. aaa_resp->flags=0.

2018 AAAs du 20 janvier 17:15:18.273843 : AAA_REQ_FLAG_NORMAL

2018 AAAs du 20 janvier 17:15:18.273877 : mts_send_response réussi

2018 AAAs du 20 janvier 17:15:18.273902 : aaa_cleanup_session

2018 AAAs du 20 janvier 17:15:18.273916 : mts_drop des msg de demande

2018 AAAs du 20 janvier 17:15:18.273935 : l'aaa_req devrait être libéré.

2018 AAAs du 20 janvier 17:15:18.280416 : aaa_process_fd_set

2018 AAAs du 20 janvier 17:15:18.280443 : aaa_process_fd_set : mtscallback sur l'aaa_q

2018 AAAs du 20 janvier 17:15:18.280454 : aaa_enable_info_config : GET_REQ pour le message d'erreur de procédure de connexion d'AAA

2018 AAAs du 20 janvier 17:15:18.280460 : obtenu de retour la valeur de retour de l'exécution de configuration : élément inconnu de Sécurité

[Informations connexes](#)

La commande d'Ethanalyzer sur FX-OS cli incitera pour le mot de passe pour un mot de passe quand l'authentification TACACS/RADIUS est activée. Ce comportement est provoqué par par une bogue.

Id de bogue : [CSCvg87518](#)