

# Firepower Système d'exploitation extensible (FXOS) 2.2 : Authentification/autorisation du châssis pour la gestion à distance avec ISE à l'aide de TACACS+

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configuration du châssis FXOS](#)

[Configuration du serveur ISE](#)

[Vérification](#)

[Vérification du châssis FXOS](#)

[Vérification ISE 2.0](#)

[Dépannage](#)

[Informations connexes](#)

## Introduction

Ce document décrit comment configurer l'authentification et l'autorisation TACACS+ pour le châssis Firepower eXtensible Operating System (FXOS) via Identity Services Engine (ISE).

Le châssis FXOS comprend les rôles d'utilisateur suivants :

- Administrateur : accès complet en lecture-écriture à l'ensemble du système. Ce rôle est attribué par défaut au compte d'administration par défaut et il ne peut pas être modifié.
- Lecture seule : accès en lecture seule à la configuration du système sans privilèges permettant de modifier l'état du système.
- Opérations : accès en lecture-écriture à la configuration NTP, à la configuration Smart Call Home pour Smart Licensing et aux journaux système, y compris les serveurs syslog et les pannes. Accès en lecture au reste du système.
- AAA : accès en lecture-écriture aux utilisateurs, aux rôles et à la configuration AAA. Accès en lecture au reste du système.

Par l'intermédiaire de l'interface de ligne de commande, ceci peut être vu comme suit :

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

Rôle :

Nom du rôle Priv.

—

aaa aaa

admin admin

opérations opérationnelles

lecture seule

Contribué par Tony Ramirez, Jose Soto, Ingénieurs TAC Cisco.

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de Firepower eXtensible Operating System (FXOS)
- Connaissance de la configuration ISE
- La licence TACACS+ Device Administration est requise dans ISE

### Components Used

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

- Appliance de sécurité Cisco Firepower 4120 version 2.2
- Cisco Identity Services Engine virtuel 2.2.0.470

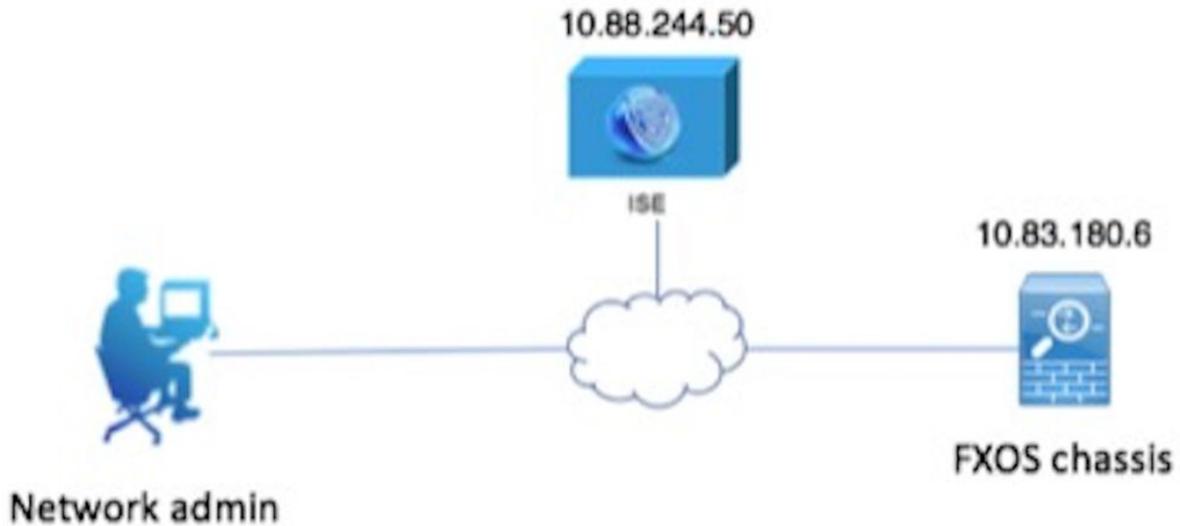
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Configuration

L'objectif de la configuration est de :

- Authentifier les utilisateurs qui se connectent à l'interface utilisateur graphique Web et à SSH de FXOS via ISE
- Autoriser les utilisateurs à se connecter à l'interface utilisateur graphique Web et à SSH de FXOS en fonction de leur rôle d'utilisateur respectif au moyen de ISE.
- Vérifier le bon fonctionnement de l'authentification et de l'autorisation sur FXOS par le biais de ISE

### Diagramme du réseau



## Configurations

### Configuration du châssis FXOS

#### Création d'un fournisseur TACACS+

Étape 1. Accédez à **Paramètres de la plate-forme > AAA**.

Étape 2. Cliquez sur l'onglet **TACACS**.

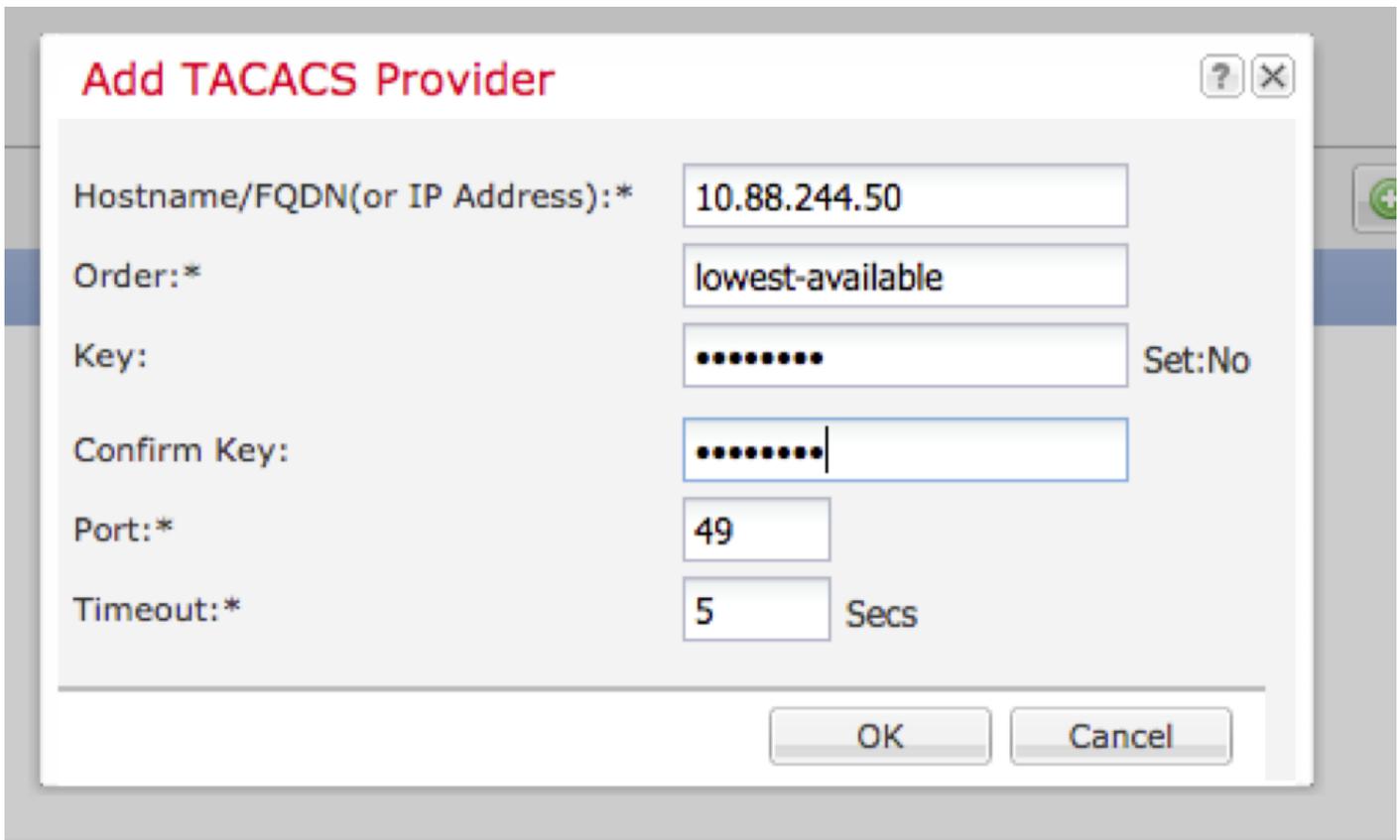


Étape 3. Pour chaque fournisseur TACACS+ à ajouter (jusqu'à 16 fournisseurs).

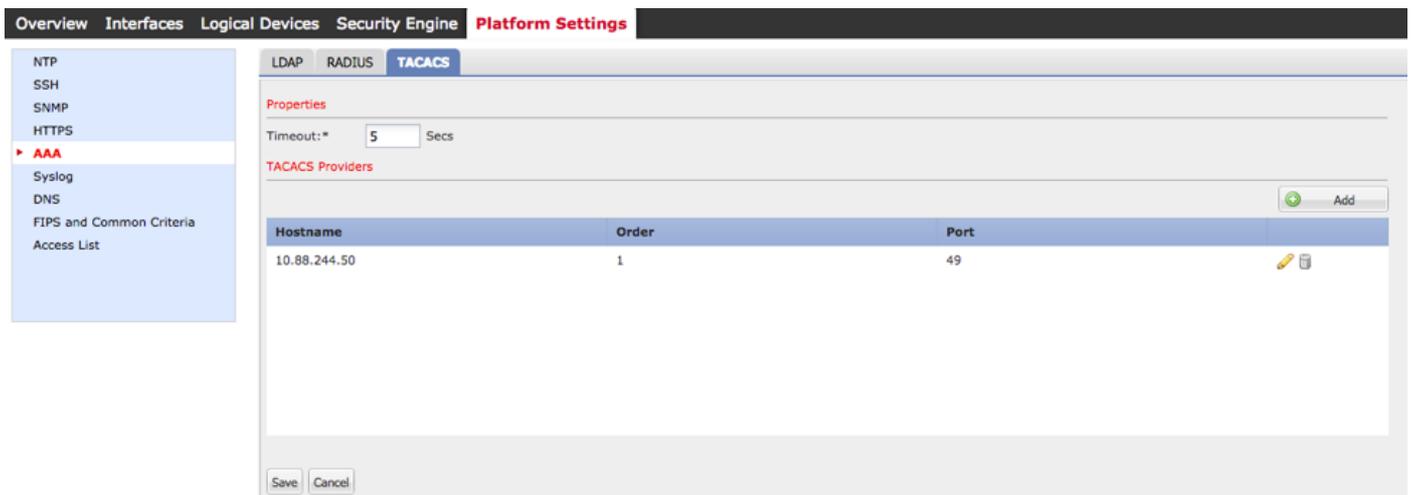
3.1. Dans la zone Fournisseurs TACACS, cliquez sur **Ajouter**.

3.2. Une fois la boîte de dialogue Ajouter un fournisseur TACACS ouverte, saisissez les valeurs requises.

3.3. Cliquez sur **OK** pour fermer la boîte de dialogue Ajouter un fournisseur TACACS.

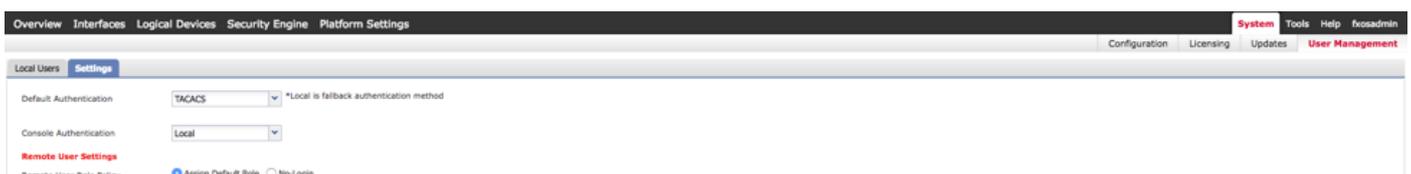


Étape 4. Cliquez sur **Save**.



Étape 5. Accédez à **System > User Management > Settings**.

Étape 6. Sous Authentication par défaut, sélectionnez **TACACS**.



**Création d'un fournisseur TACACS+ à l'aide de l'interface de ligne de commande**

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

```
fpr4120-TAC-A# scope security
```

```
fpr4120-TAC-A /security # scope default-auth
```

```
fpr4120-TAC-A /security/default-auth # set realm tacacs
```

Étape 2. Utilisez la commande **show detail** pour vérifier la configuration.

```
fpr4120-TAC-A /security/default-auth # show detail
```

Authentification par défaut :

Domaine d'administration : **Tacas**

Domaine opérationnel : **Tacas**

Période d'actualisation de la session Web (en secondes) : 600

Délai d'attente de session (en secondes) pour les sessions web, ssh, telnet : 600

Délai d'attente de session absolue (en secondes) pour les sessions Web, ssh et telnet : 3600

Délai d'expiration de la session de la console série (en secondes) : 600

Délai d'attente de session absolue de la console série (en secondes) : 3600

Groupe de serveurs Admin Authentication :

Groupe de serveurs d'authentification opérationnelle :

Utilisation du deuxième facteur : Non

Étape 3. Afin de configurer les paramètres du serveur TACACS, exécutez les commandes suivantes.

```
fpr4120-TAC-A# scope security
```

```
fpr4120-TAC-A /security # scope tacacs
```

```
fpr4120-TAC-A /security/tacacs # entrez server 10.88.244.50
```

```
fpr4120-TAC-A /security/tacacs/server # set descr « ACS Server »
```

```
fpr4120-TAC-A /security/tacacs/server* # set key
```

Saisissez la clé : **\*\*\*\*\***

Confirmez la clé : **\*\*\*\*\***

Étape 4. Utilisez la commande **show detail** pour vérifier la configuration.

```
fpr4120-TAC-A /security/tacacs/server* # show detail
```

Serveur TACACS+ :

Nom d'hôte, nom de domaine complet ou adresse IP : 10.88.244.50

Description :

Commande : 1

Port : 49

Clé : \*\*\*\*

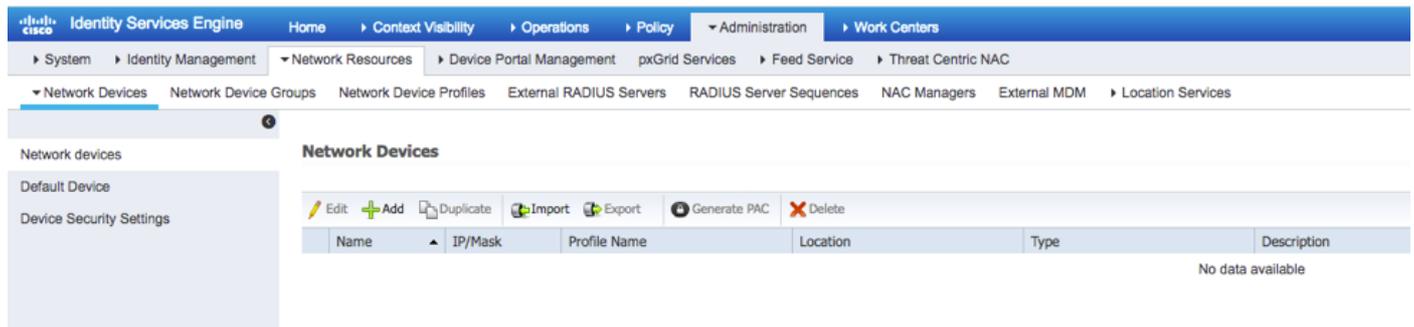
timeout : 5

## Configuration du serveur ISE

### Ajout du FXOS en tant que ressource réseau

Étape 1. Accédez à **Administration > Network Resources > Network Devices**.

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 > Network Resources > Network Devices. The left sidebar shows 'Network devices' with sub-items 'Default Device' and 'Device Security Settings'. The main content area is titled 'Network Devices' and contains a toolbar with 'Edit', 'Add', 'Duplicate', 'Import', 'Export', 'Generate PAC', and 'Delete' buttons. 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' centered below it.

Étape 3. Entrez les valeurs requises (Nom, Adresse IP, Type de périphérique et Activer TACACS+ et ajoutez la CLÉ), cliquez sur **Envoyer**.

Identity Services Engine 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 > FXOS

### Network Devices

\* Name

Description

\* IP Address:  /

\* Device Profile

Model Name

Software Version

\* Network Device Group

Device Type

IPSEC

Location

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret

Enable Single Connect Mode

Legacy Cisco Device  
 TACACS Draft Compliance Single Connect Support

SNMP Settings

Advanced TrustSec Settings

## Création des groupes d'identités et des utilisateurs

Étape 1. Accédez à Administration > Identity Management > Groups > User Identity Groups.

Étape 2. Cliquez sur Add.

Identity Services Engine 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

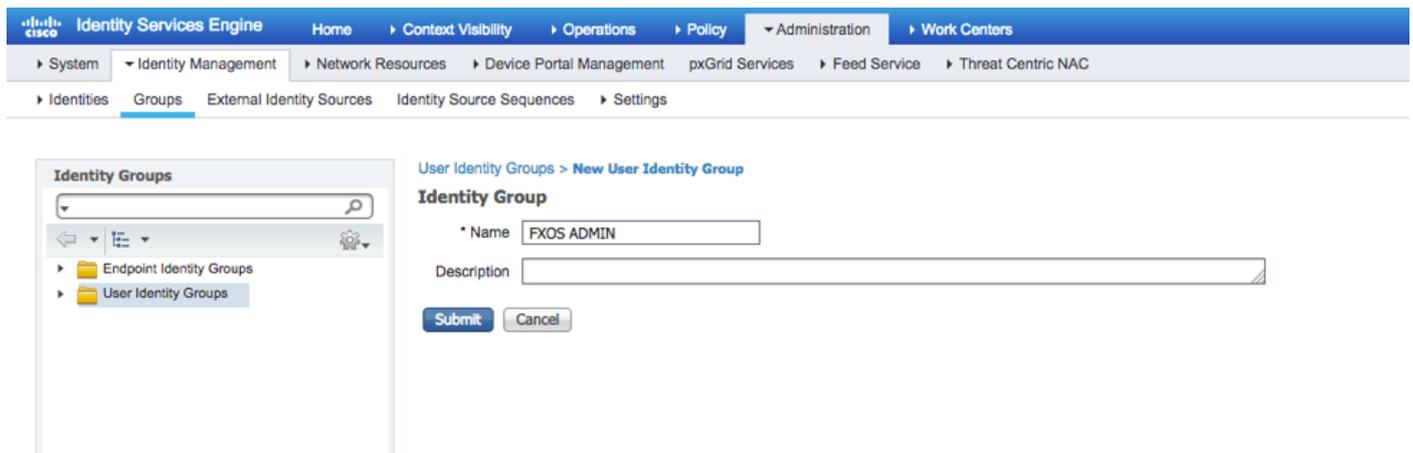
User Identity Groups

### User Identity Groups

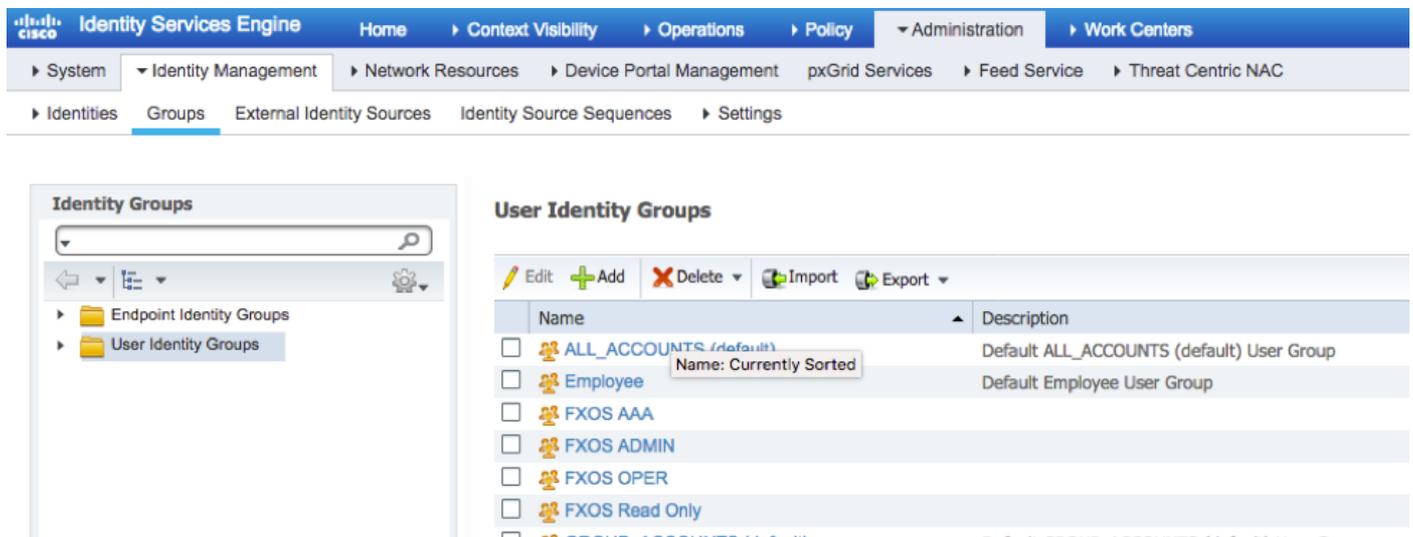
Edit Add Delete Import Export

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. Entrez la valeur de Name et cliquez sur **Submit**.

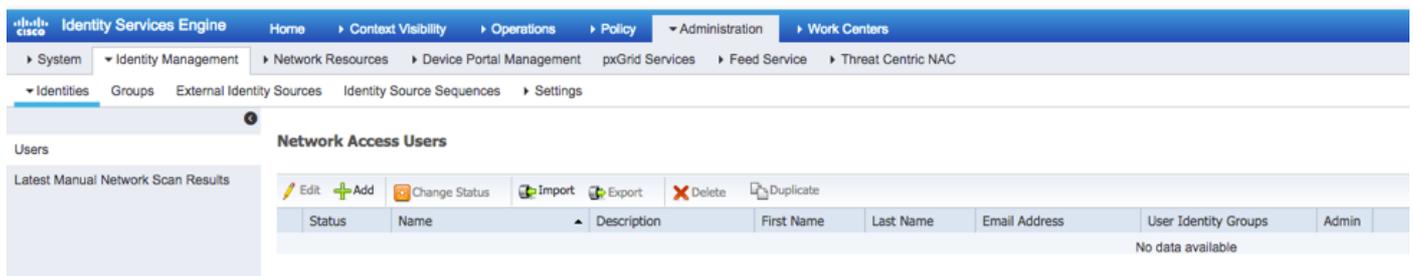


Étape 4. Répétez l'étape 3 pour tous les rôles utilisateur requis.



Étape 5. Accédez à **Administration > Identity Management > Identity > Users**.

Étape 6. Cliquez sur **Add**.



Étape 7. Saisissez 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**

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	

## Création du profil Shell pour chaque rôle utilisateur

Étape 1. Accédez à **Centres de travail > Administration des périphériques > Eléments de stratégie > Résultats > Profils TACACS** et cliquez sur **+AJOUTER**.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings

**TACACS Profiles**

0 Selected Rows/Page 4 / 1 / 1 Go 4 Total Rows

Refresh Add Duplicate Trash Edit Filter

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	WLC ALL	WLC	WLC ALL
<input type="checkbox"/>	WLC MONITOR	WLC	WLC MONITOR
<input type="checkbox"/>	Deny All Shell Profile	Shell	Deny All Shell Profile
<input type="checkbox"/>	Default Shell Profile	Shell	Default Shell Profile

## Étape 2. Saisissez les valeurs requises pour le profil TACACS

### 2.1. Saisissez le nom.

TACACS Profiles > New

#### TACACS Profile

Name

Description

Task Attribute View

Raw View

### 2.2. Dans l'ONGLET Vue RAW, configurez CISCO-AV-PAIR suivant.

**cisco-av-pair=shell : rôles=« admin »**

### TACACS Profile

Name

Description

Task Attribute View

Raw View

### Profile Attributes

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

Cancel

Submit

2.3. Cliquez sur Submit.

### TACACS Profile

Name

Description

**Task Attribute View** Raw View

### Common Tasks

Common Task Type

<input type="checkbox"/> Default Privilege	<input type="text"/>	(Select 0 to 15)
<input type="checkbox"/> Maximum Privilege	<input type="text"/>	(Select 0 to 15)
<input type="checkbox"/> Access Control List	<input type="text"/>	
<input type="checkbox"/> Auto Command	<input type="text"/>	
<input type="checkbox"/> No Escape	<input type="text"/>	(Select true or false)
<input type="checkbox"/> Timeout	<input type="text"/>	Minutes (0-9999)
<input type="checkbox"/> Idle Time	<input type="text"/>	Minutes (0-9999)

### Custom Attributes

+ Add Trash Edit

Type	Name	Value	
<input type="checkbox"/> MANDATORY	cisco-av-pair	shell:roles="admin"	

Cancel Save

Étape 3. Répétez l'étape 2 pour les autres rôles d'utilisateur à l'aide des paires Cisco-AV suivantes.

**cisco-av-pair=shell : rôles=« aaa »**

**cisco-av-pair=shell : rôles=« opérations »**

**cisco-av-pair=shell : rôles=« lecture seule »**

### Custom Attributes

+ Add Trash Edit

Type	Name	Value	
<input type="checkbox"/> MANDATORY	cisco-av-pair	shell:roles="aaa"	

Cancel Save

## Custom Attributes

+ Add  Trash  Edit ⚙️

<input type="checkbox"/>	Type	Name	Value	
<input type="checkbox"/>	MANDATORY	cisco-av-pair	shell:roles="operations"	<input type="checkbox"/> <input type="checkbox"/>

## Custom Attributes

+ Add  Trash  Edit ⚙️

<input type="checkbox"/>	Type	Name	Value	
<input type="checkbox"/>	MANDATORY	cisco-av-pair	shell:roles="read-only"	<input type="checkbox"/> <input type="checkbox"/>

## TACACS Profiles

0 Selected

Rows/Page

/ 1

8 Total Rows

+ Add Duplicate  Trash  Edit Filter  ⚙️

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	WLC ALL	WLC	WLC ALL
<input type="checkbox"/>	WLC MONITOR	WLC	WLC MONITOR
<input type="checkbox"/>	Deny All Shell Profile	Shell	Deny All Shell Profile
<input type="checkbox"/>	Default Shell Profile	Shell	Default Shell Profile
<input type="checkbox"/>	FXOS_Admin_Profile	Shell	
<input type="checkbox"/>	FXOS_AAA_Shell	Shell	
<input type="checkbox"/>	FXOS_Operations_Shell	Shell	
<input type="checkbox"/>	FXOS_ReadOnly_Shell	Shell	

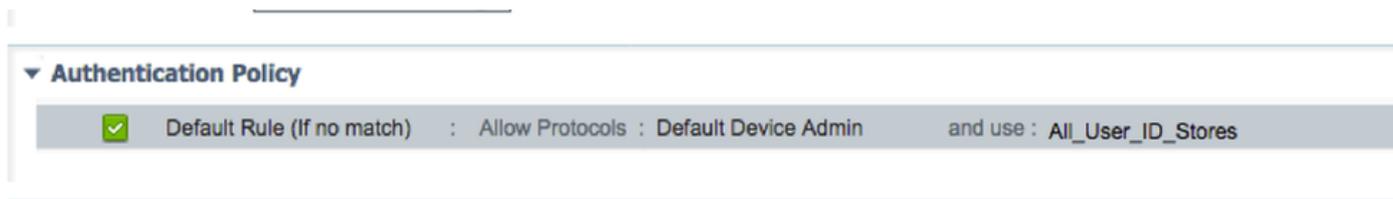
## Création de la stratégie d'autorisation TACACS

Étape 1. Accédez à **Centres de travail > Administration des périphériques > Jeux de stratégies d'administration des périphériques**.

The screenshot shows the Cisco ISE configuration interface for TACACS profiles. The left sidebar displays a list of profiles, including 'Tactics\_Default'. The main area shows the configuration for the selected profile, with sections for Proxy Server Sequence, Authentication Policy, and Authorization Policy. The Authorization Policy section includes a table with columns for Status, Rule Name, Conditions, Command Sets, and Shell Profiles. The 'Tactics\_Default' profile is selected, and its conditions are set to 'Deny All Shell Profile'.

Étape 2. Assurez-vous que la stratégie d'authentification pointe vers la base de données

Utilisateurs internes ou vers le magasin d'identités requis.



Étape 3. Cliquez sur la flèche à la fin de la stratégie d'autorisation par défaut et cliquez sur Insérer une règle ci-dessus.

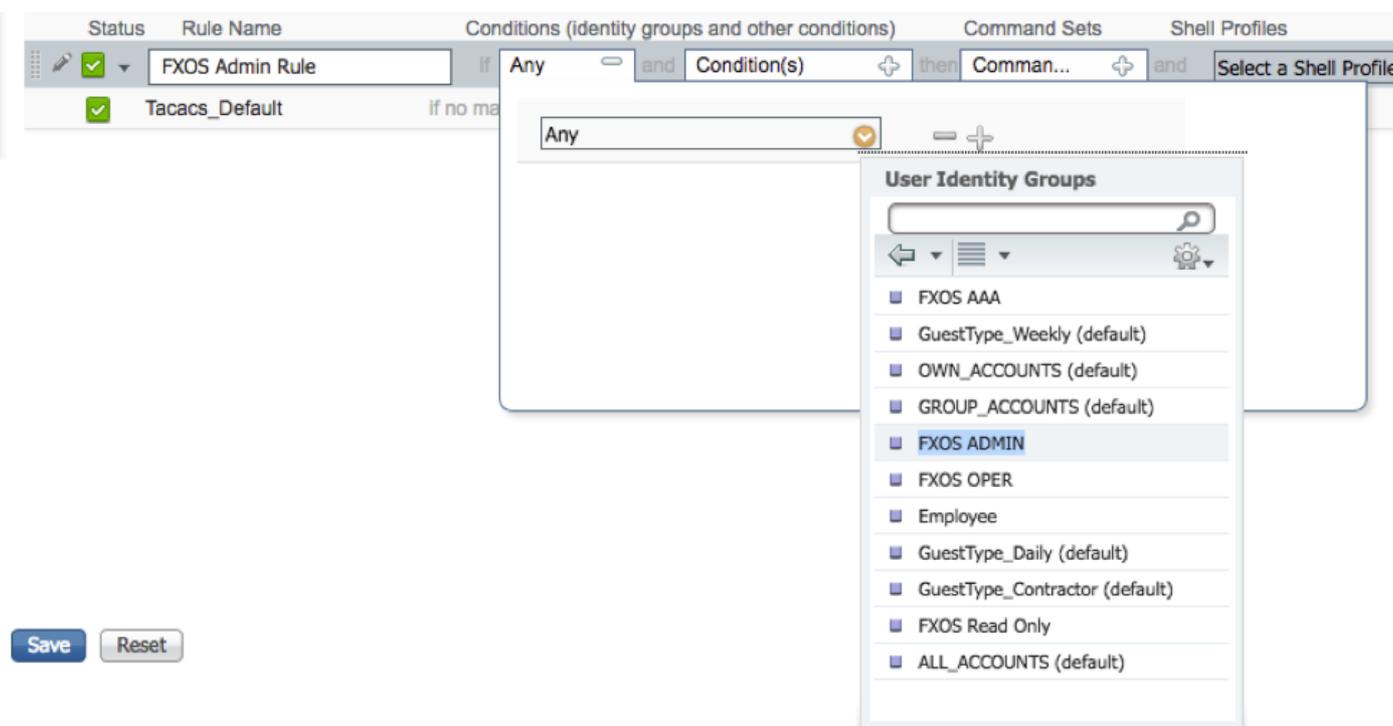


Étape 4. Entrez les valeurs de la règle avec les paramètres requis :

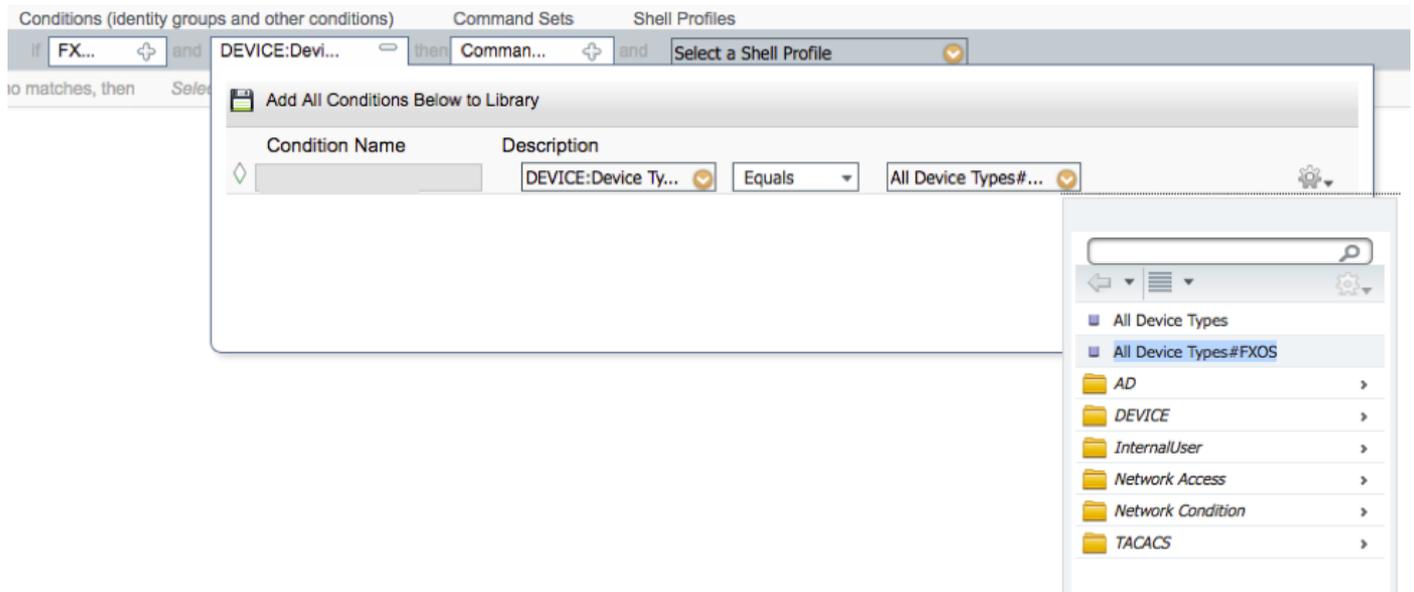
4.1. Nom de la règle : Règle d'administration FXOS.

4.2. Conditions.

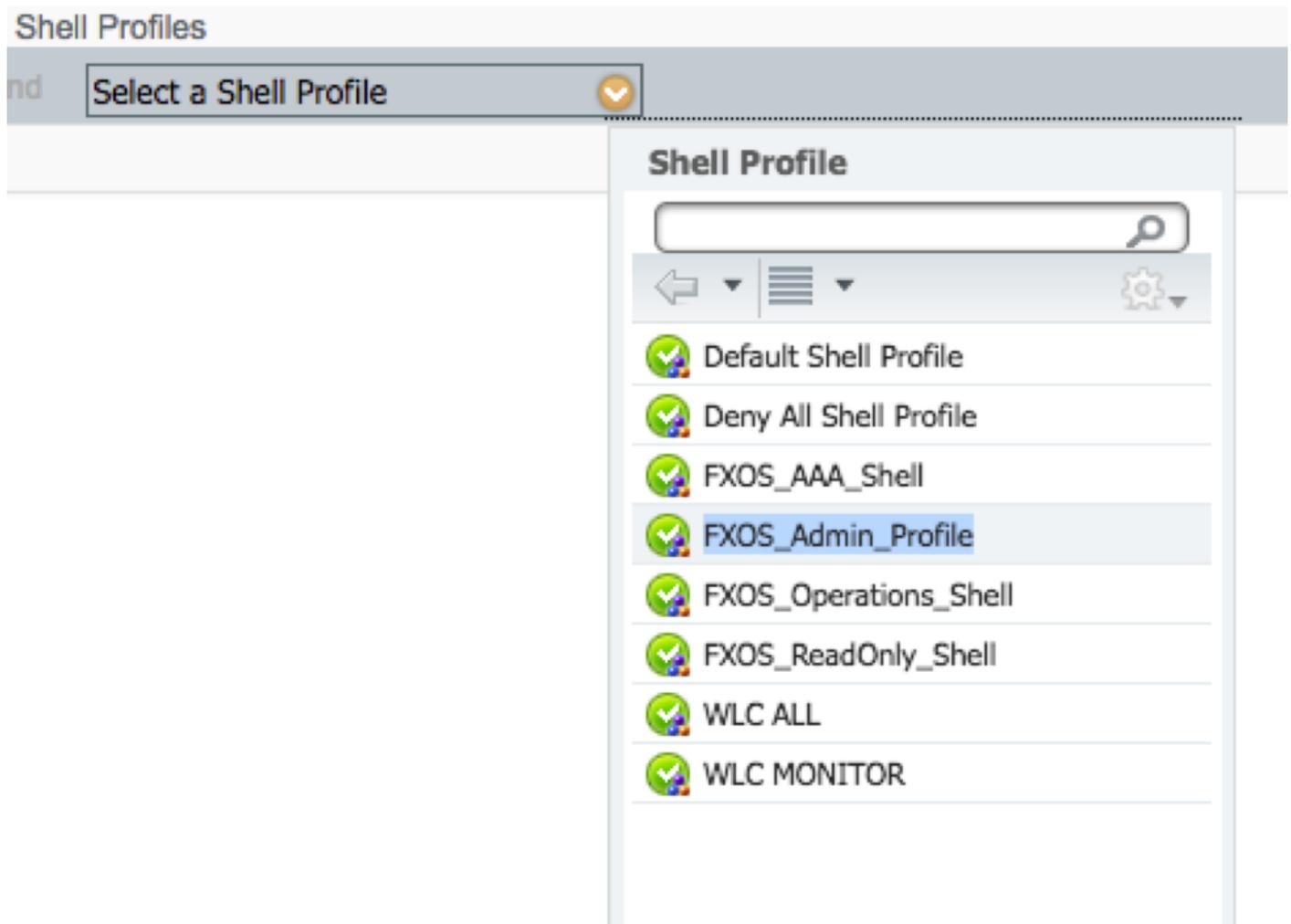
Si : Le groupe d'identités utilisateur est FXOS ADMIN



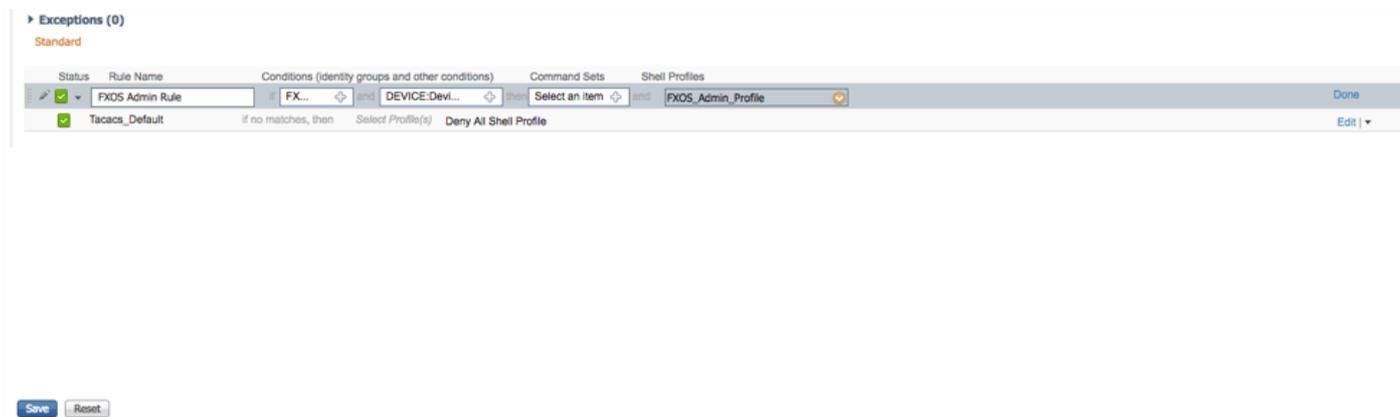
Et Périphérique : Type de périphérique égal à tous les types de périphériques #FXOS



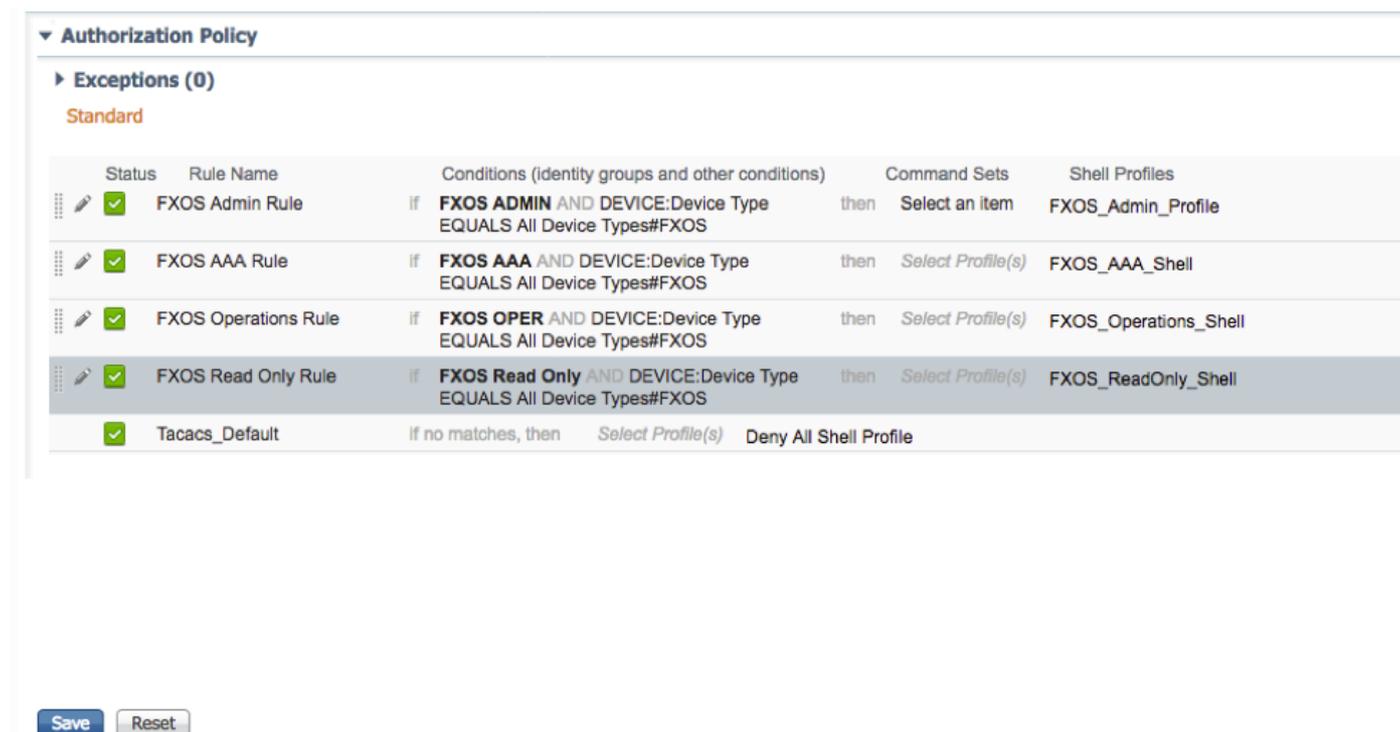
Profil Shell : Profil\_Admin\_FXOS



Étape 5. Cliquez sur **Done**.



Étape 6. Répétez les étapes 3 et 4 pour les autres rôles d'utilisateur et, lorsque vous avez terminé, cliquez sur **ENREGISTRER**.



## Vérification

Vous pouvez maintenant tester chaque utilisateur et vérifier le rôle d'utilisateur assigné.

### Vérification du châssis FXOS

1. Établissez une connexion Telnet ou SSH au châssis FXOS et connectez-vous à l'aide de l'un des utilisateurs créés sur l'ISE.

username (nom d'utilisateur) : fxosadmin

Mot de passe :

fxr4120-TAC-A# **sécurité de portée**

fxr4120-TAC-A /security # **show remote-user detail**

Utilisateur distant **fxosaaa** :

Description:

Rôles utilisateur :

Name : **aaa**

Name : **en lecture seule**

Utilisateur distant **fxosadmin** :

Description:

Rôles utilisateur :

Name : **admin**

Name : **en lecture seule**

Utilisateur distant **fxosoper** :

Description:

Rôles utilisateur :

Name : **opérations**

Name : **en lecture seule**

Utilisateur distant **fxosro** :

Description:

Rôles utilisateur :

Name : **en lecture seule**

En fonction du nom d'utilisateur saisi, l'interface de ligne de commande du châssis FXOS affiche uniquement les commandes autorisées pour le rôle d'utilisateur attribué.

Rôle utilisateur Admin.

fxr4120-TAC-A /security # ?

reconnaître

clear-user-sessions Clear User Sessions

créer des objets gérés

supprimer les objets managés

désactiver les services Désactive

activer les services

Entrez un objet managé

étendue Modifie le mode actuel

définir les valeurs de propriété

show show system information

terminer les sessions cimc actives

fpr4120-TAC-A# **connect fxos**

fpr4120-TAC-A (fxos)# **debug aaa aaa-request**

fpr4120-TAC-A (fxos)#

Rôle utilisateur en lecture seule.

fpr4120-TAC-A /security # ?

étendue Modifie le mode actuel

définir les valeurs de propriété

show show system information

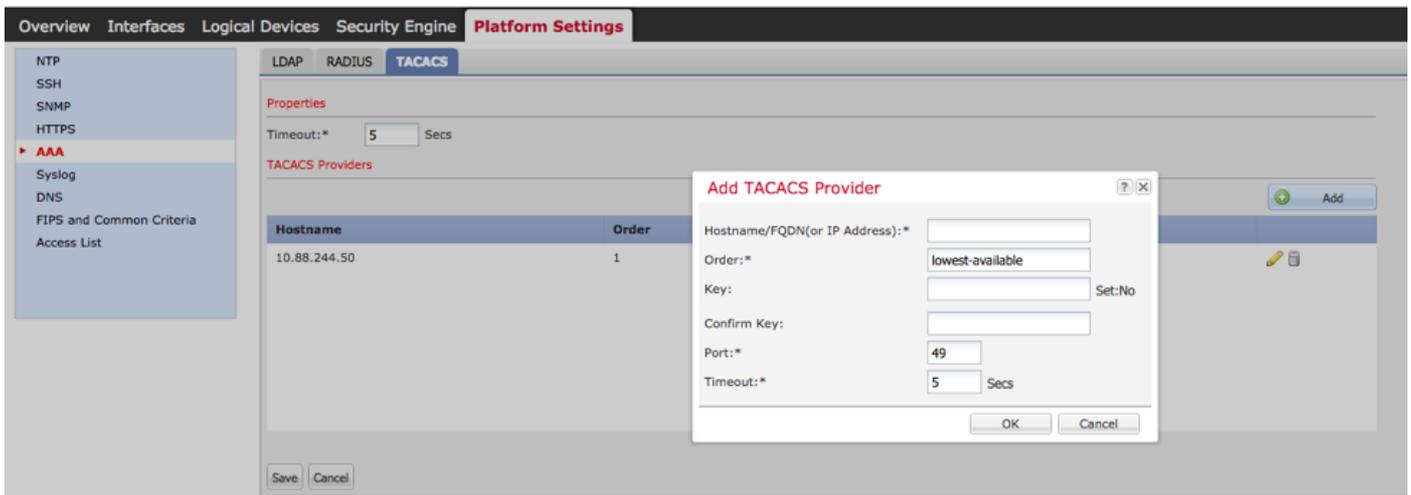
fpr4120-TAC-A# **connect fxos**

fpr4120-TAC-A (fxos)# **debug aaa aaa-request**

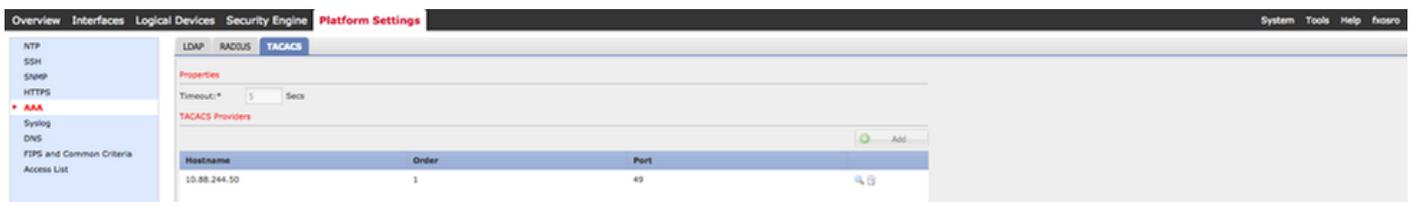
% Autorisation refusée pour le rôle

2. Accédez à l'adresse IP du châssis FXOS et connectez-vous à l'aide de l'un des utilisateurs créés sur l'ISE.

Rôle utilisateur Admin.



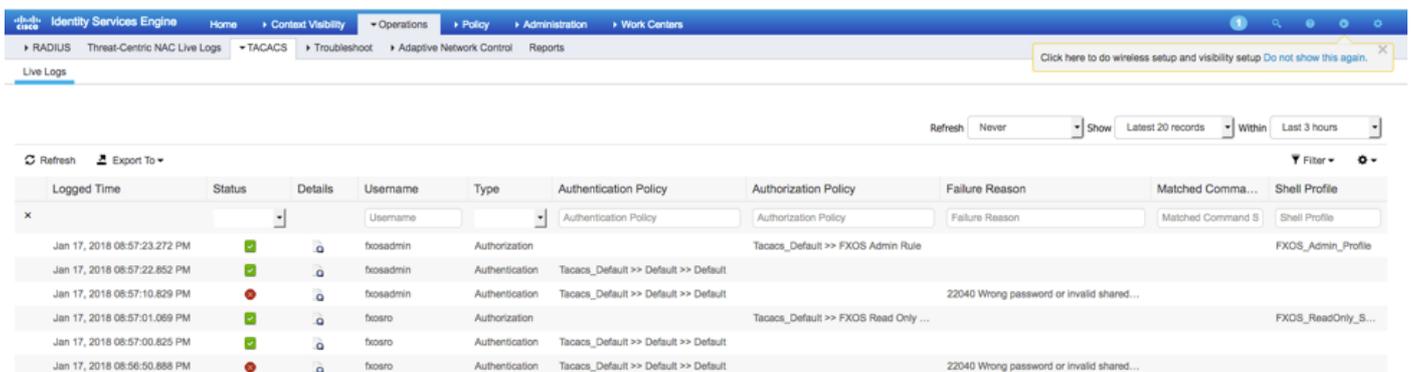
Rôle utilisateur en lecture seule.



**Note:** Notez que le bouton **ADD** est grisé.

## Vérification ISE 2.0

1. Accédez à **Opérations > TACACS Livelog**. Vous devriez être en mesure de voir des tentatives réussies et échouées.



## Dépannage

Pour déboguer l'authentification et l'autorisation AAA, exécutez les commandes suivantes dans l'interface de ligne de commande FXOS.

```
fpr4120-TAC-A# connect fxos
```

```
fpr4120-TAC-A (fxos)# debug aaa aaa-request
```

```
fpr4120-TAC-A (fxos)# debug aaa event
```

```
fpr4120-TAC-A (fxos)# debug aaa errors
```

fpr4120-TAC-A (fxos)# term mon

Après une tentative d'authentification réussie, le résultat suivant s'affiche.

17 janvier 2018 15:46:40.305247 aaa : aaa\_req\_process pour l'authentification. session no 0

17 janvier 2018 15:46:40.305262 aaa : aaa\_req\_process : Demande AAA générale de l'application : login appln\_subtype : par défaut

17 janvier 2018 15:46:40.305271 aaa : try\_next\_aaa\_méthode

17 janvier 2018 15:46:40.305285 aaa : total des méthodes configurées est 1, l'index actuel à essayer est 0

17 janvier 2018 15:46:40.305294 aaa : handle\_req\_using\_méthode

17 janvier 2018 15:46:40.305301 aaa : GROUPE\_SERVEURS\_MÉTHODE\_AAA

17 janvier 2018 15:46:40.305308 aaa : aaa\_sg\_method\_handler groupe = tacacs

17 janvier 2018 15:46:40.305315 aaa : Utilisation de sg\_protocol passé à cette fonction

17 janvier 2018 15:46:40.305324 aaa : Envoi de la demande au service TACACS

17 janvier 2018 15:46:40.305384 aaa : Groupe de méthodes configuré Réussite

17 janvier 2018 15:46:40.554631 aaa : aaa\_process\_fd\_set

17 janvier 2018 15:46:40.555229 aaa : aaa\_process\_fd\_set : mtscallback sur aaa\_q

17 janvier 2018 15:46:40.555817 aaa : mts\_message\_response\_handler : réponse mts

17 janvier 2018 15:46:40.556387 aaa : prot\_daemon\_reponse\_handler

17 janvier 2018 15:46:40.557042 aaa : session : 0x8dfd68c supprimé de la table de session 0

17 janvier 2018 15:46:40.557059 aaa : is\_aaa\_resp\_status\_success status = 1

17 janvier 2018 15:46:40.557066 aaa : is\_aaa\_resp\_status\_success est TRUE

17 janvier 2018 15:46:40.557075 aaa : aaa\_send\_client\_response pour l'authentification. session->flags=21. aaa\_resp->flags=0.

17 janvier 2018 15:46:40.557083 aaa : AAA\_REQ\_FLAG\_NORMAL

17 janvier 2018 15:46:40.557106 aaa : mts\_send\_response Réussite

17 janvier 2018 15:46:40.557364 aaa : aaa\_req\_process pour autorisation. session no 0

17 janvier 2018 15:46:40.557378 aaa : aaa\_req\_process appelé avec contexte à partir de appln : login appln\_subtype : type\_auteur par défaut : 2, méthode\_auteur : 0

17 janvier 2018 15:46:40.557386 aaa : aaa\_send\_req\_using\_contexte

17 janvier 2018 15:46:40.557394 aaa : groupe aaa\_sg\_method\_handler = (null)

17 janvier 2018 15:46:40.557401 aaa : Utilisation de sg\_protocol passé à cette fonction

17 janvier 2018 15:46:40.557408 aaa : demande AAA basée sur le contexte ou dirigée(exception : pas une requête de relais). Ne prendra pas copie de la demande aaa

17 janvier 2018 15:46:40.557415 aaa : Envoi de la demande au service TACACS

17 janvier 2018 15:46:40.801732 aaa : aaa\_send\_client\_response pour autorisation. session->flags=9. aaa\_resp->flags=0.

17 janvier 2018 15:46:40.801740 aaa : AAA\_REQ\_FLAG\_NORMAL

17 janvier 2018 15:46:40.801761 aaa : mts\_send\_response Réussite

17 janvier 2018 15:46:40.848932 aaa : ANCIEN OPICODE : mise à jour\_intermédiaire\_comptable

17 janvier 2018 15:46:40.848943 aaa : aaa\_create\_local\_acct\_req : user=, session\_id=, log=ajouté utilisateur:fxosadmin au rôle:admin

17 janvier 2018 15:46:40.848963 aaa : aaa\_req\_process pour la comptabilité. session no 0

17 janvier 2018 15:46:40.848972 aaa : La référence de la demande MTS est NULL. Demande LOCALE

17 janvier 2018 15:46:40.848982 aaa : Définition de AAA\_REQ\_RESPONSE\_NOT\_NEEDED

17 janvier 2018 15:46:40.848992 aaa : aaa\_req\_process : Demande AAA générale de l'application : appln\_subtype par défaut : par défaut

17 janvier 2018 15:46:40.849002 aaa : try\_next\_aaa\_méthode

17 janvier 2018 15:46:40.849022 aaa : Aucune méthode configurée pour la valeur par défaut

17 janvier 2018 15:46:40.849032 aaa : aucune configuration disponible pour cette demande

17 janvier 2018 15:46:40.849043 aaa : try\_fallback\_méthode

17 janvier 2018 15:46:40.849053 aaa : handle\_req\_using\_méthode

17 janvier 2018 15:46:40.849063 aaa : gestionnaire\_méthode\_locale

17 janvier 2018 15:46:40.849073 aaa : aaa\_local\_accounting\_msg

17 janvier 2018 15:46:40.849085 aaa : mettre à jour::utilisateur ajouté:fxosadmin au rôle:admin

Après une tentative d'authentification échouée, le résultat suivant s'affiche.

17 janvier 2018 15:46:17.836271 aaa : aaa\_req\_process pour l'authentification. session no 0

17 janvier 2018 15:46:17.836616 aaa : aaa\_req\_process : Demande AAA générale de l'application : login appln\_subtype : par défaut

17 janvier 2018 15:46:17.837063 aaa : try\_next\_aaa\_méthode

17 janvier 2018 15:46:17.837416 aaa : total des méthodes configurées est 1, l'index actuel à essayer est 0

17 janvier 2018 15:46:17.837766 aaa : handle\_req\_using\_méthode

17 janvier 2018 15:46:17.838103 aaa : GROUPE\_SERVEURS\_MÉTHODE\_AAA

17 janvier 2018 15:46:17.838477 aaa : aaa\_sg\_method\_handler groupe = tacacs

17 janvier 2018 15:46:17.838826 aaa : Utilisation de sg\_protocol passé à cette fonction

17 janvier 2018 15:46:17.839167 aaa : Envoi de la demande au service TACACS

17 janvier 2018 15:46:17.840225 aaa : Groupe de méthodes configuré Réussite

17 janvier 2018 15:46:18.043710 aaa : is\_aaa\_resp\_status\_success status = 2

17 janvier 2018 15:46:18.044048 aaa : is\_aaa\_resp\_status\_success est TRUE

17 janvier 2018 15:46:18.044395 aaa : aaa\_send\_client\_response pour l'authentification. session->flags=21. aaa\_resp->flags=0.

17 janvier 2018 15:46:18.044733 aaa : AAA\_REQ\_FLAG\_NORMAL

17 janvier 2018 15:46:18.045096 aaa : mts\_send\_response Réussite

17 janvier 2018 15:46:18.045677 aaa : aaa\_cleanup\_session

17 janvier 2018 15:46:18.045689 aaa : mts\_drop de la requête msg

17 janvier 2018 15:46:18.045699 aaa : aaa\_req doit être libéré.

17 janvier 2018 15:46:18.045715 aaa : aaa\_process\_fd\_set

17 janvier 2018 15:46:18.045722 aaa : aaa\_process\_fd\_set : mtscallback sur aaa\_q

17 janvier 2018 15:46:18.045732 aaa : aaa\_enable\_info\_config : GET\_REQ pour un message d'erreur de connexion aaa

17 janvier 2018 15:46:18.045738 aaa : récupération de la valeur de retour de l'opération de configuration:élément de sécurité inconnu

## Informations connexes

La commande Ethanalyzer sur le cli FX-OS vous invite à saisir un mot de passe lorsque l'authentification TACACS/RADIUS est activée. Ce comportement est causé par un bogue.

ID de bogue: [CSCvg87518](#)