

Firepower Système d'exploitation extensible (FXOS) 2.2 : Authentification et autorisation du châssis pour la gestion à distance avec ACS 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 ACS](#)

[Vérification](#)

[Vérification du châssis FXOS](#)

[Vérification ACS](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer l'authentification et l'autorisation TACACS+ pour le châssis Firepower eXtensible Operating System (FXOS) via Access Control Server (ACS).

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 panes. 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 ACS

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
- Serveur de contrôle d'accès Cisco virtuel version 5.8.0.32

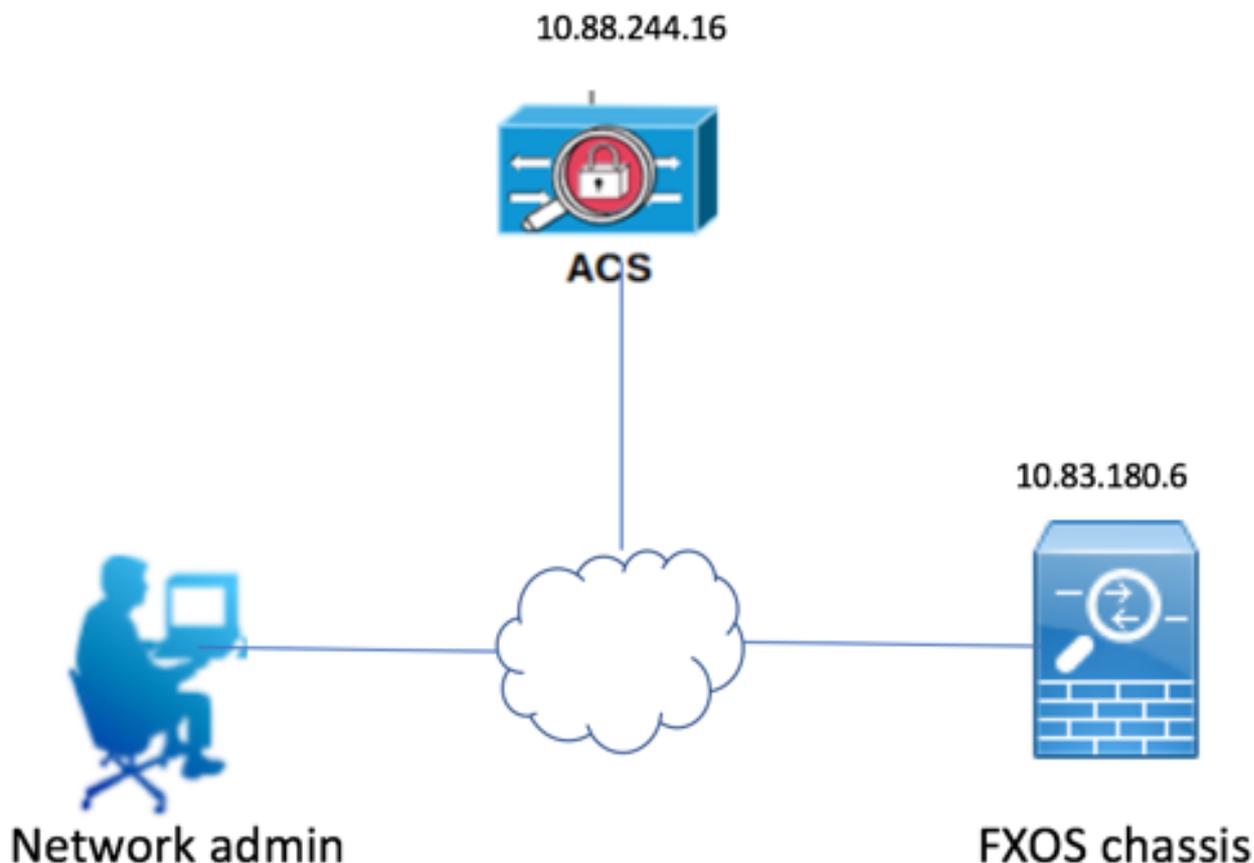
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

L'objectif de la configuration est de :

- Authentifiez les utilisateurs qui se connectent à l'interface utilisateur graphique Web et à SSH de FXOS à l'aide d'ACS.
- 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 d'ACS.
- Vérifiez le bon fonctionnement de l'authentification et de l'autorisation sur le FXOS au moyen d'ACS.

Diagramme du réseau



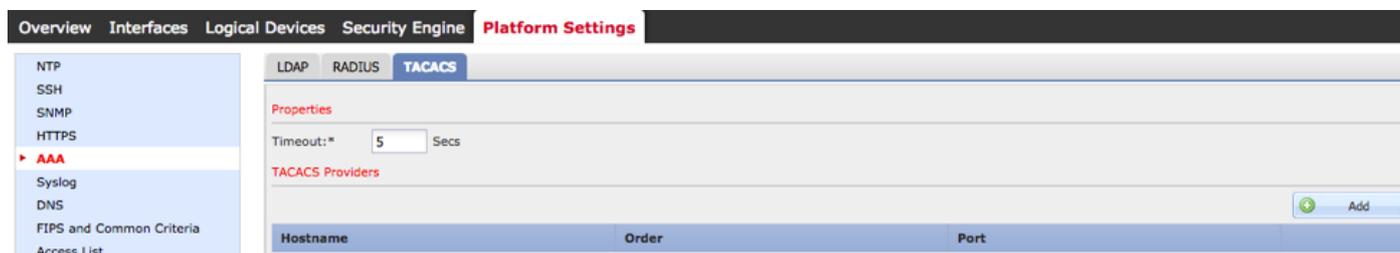
Configurations

Configuration du châssis FXOS

Création d'un fournisseur TACACS à l'aide du Gestionnaire de châssis

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. Dans la boîte de dialogue Ajouter un fournisseur TACACS, saisissez les valeurs requises.

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

Add TACACS Provider

Hostname/FQDN(or IP Address):*

Order:*

Key: Set: No

Confirm Key:

Port:*

Timeout:* Secs

Étape 4. Cliquez sur **Save**.

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

TACACS Providers

Hostname	Order	Port
10.88.244.16	1	49

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

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

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

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 afficher les résultats.

```
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 afficher les résultats.

```
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 : ****

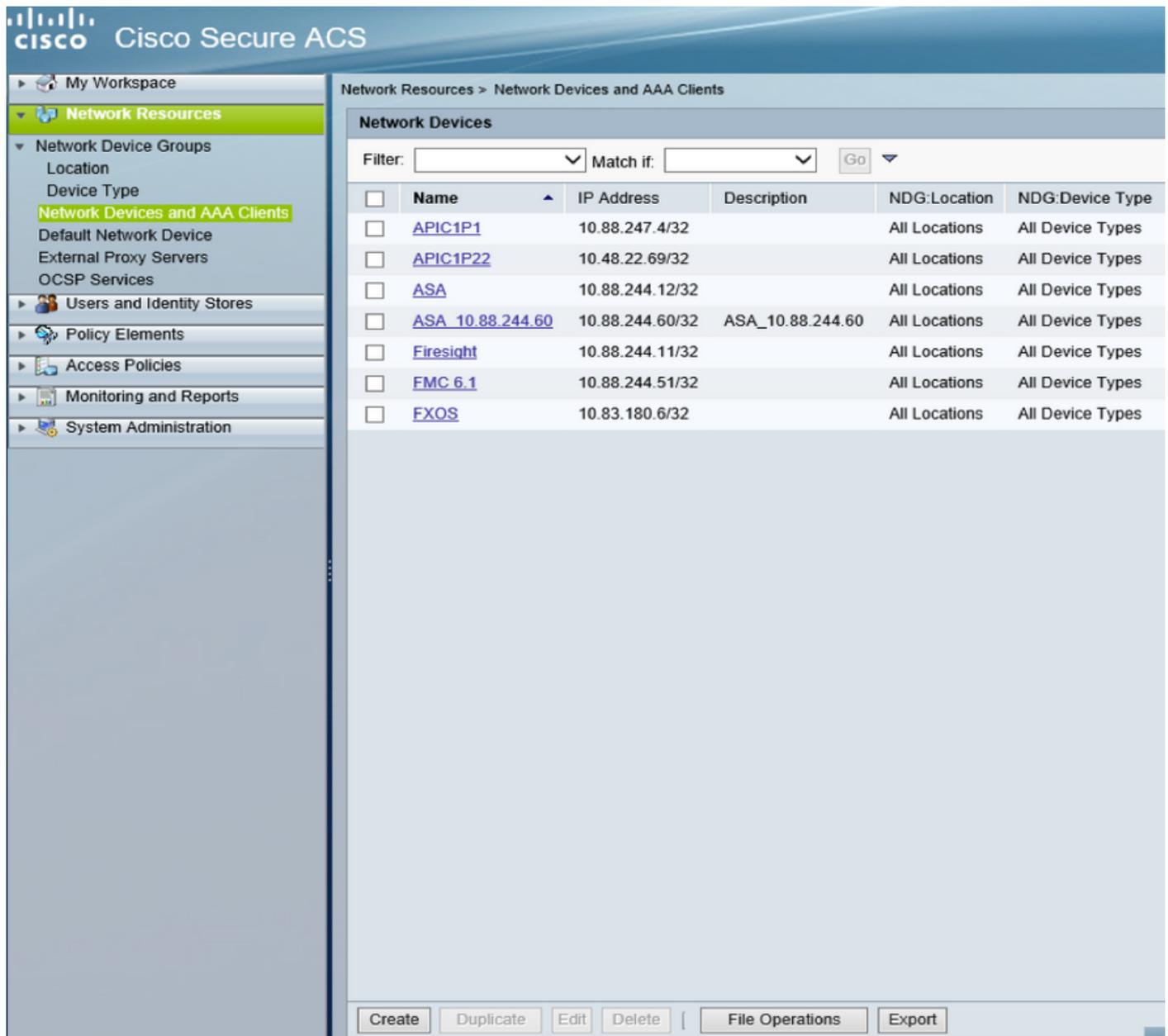
timeout : 5

Configuration du serveur ACS

Ajout du FXOS en tant que ressource réseau

Étape 1. Accédez à **Network Resources > Network Devices and AAA Clients**.

Étape 2. Cliquez sur **Create**.



The screenshot shows the Cisco Secure ACS web interface. The left sidebar contains a navigation menu with 'Network Resources' expanded. The main content area is titled 'Network Resources > Network Devices and AAA Clients' and displays a table of network devices. The table has columns for Name, IP Address, Description, NDG:Location, and NDG:Device Type. The 'FXOS' device is highlighted in blue. Below the table are buttons for 'Create', 'Duplicate', 'Edit', 'Delete', 'File Operations', and 'Export'.

<input type="checkbox"/>	Name	IP Address	Description	NDG:Location	NDG:Device Type
<input type="checkbox"/>	APIC1P1	10.88.247.4/32		All Locations	All Device Types
<input type="checkbox"/>	APIC1P22	10.48.22.69/32		All Locations	All Device Types
<input type="checkbox"/>	ASA	10.88.244.12/32		All Locations	All Device Types
<input type="checkbox"/>	ASA_10.88.244.60	10.88.244.60/32	ASA_10.88.244.60	All Locations	All Device Types
<input type="checkbox"/>	Firesight	10.88.244.11/32		All Locations	All Device Types
<input type="checkbox"/>	FMC 6.1	10.88.244.51/32		All Locations	All Device Types
<input type="checkbox"/>	FXOS	10.83.180.6/32		All Locations	All Device Types

Étape 3. Saisissez les valeurs requises (Nom, Adresse IP, Type de périphérique et Activer TACACS+ et ajoutez la CLÉ).

Network Resources > Network Devices and AAA Clients > Edit: "FXOS"

Name:

Description:

Network Device Groups

Location

Device Type

IP Address

Single IP Address IP Subnets IP Range(s)

IP:

Authentication Options

▶ TACACS+

▶ RADIUS

= Required fields

Étape 4. Cliquez sur Submit.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.