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

## 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 RADIUS 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 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 Remirez, 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

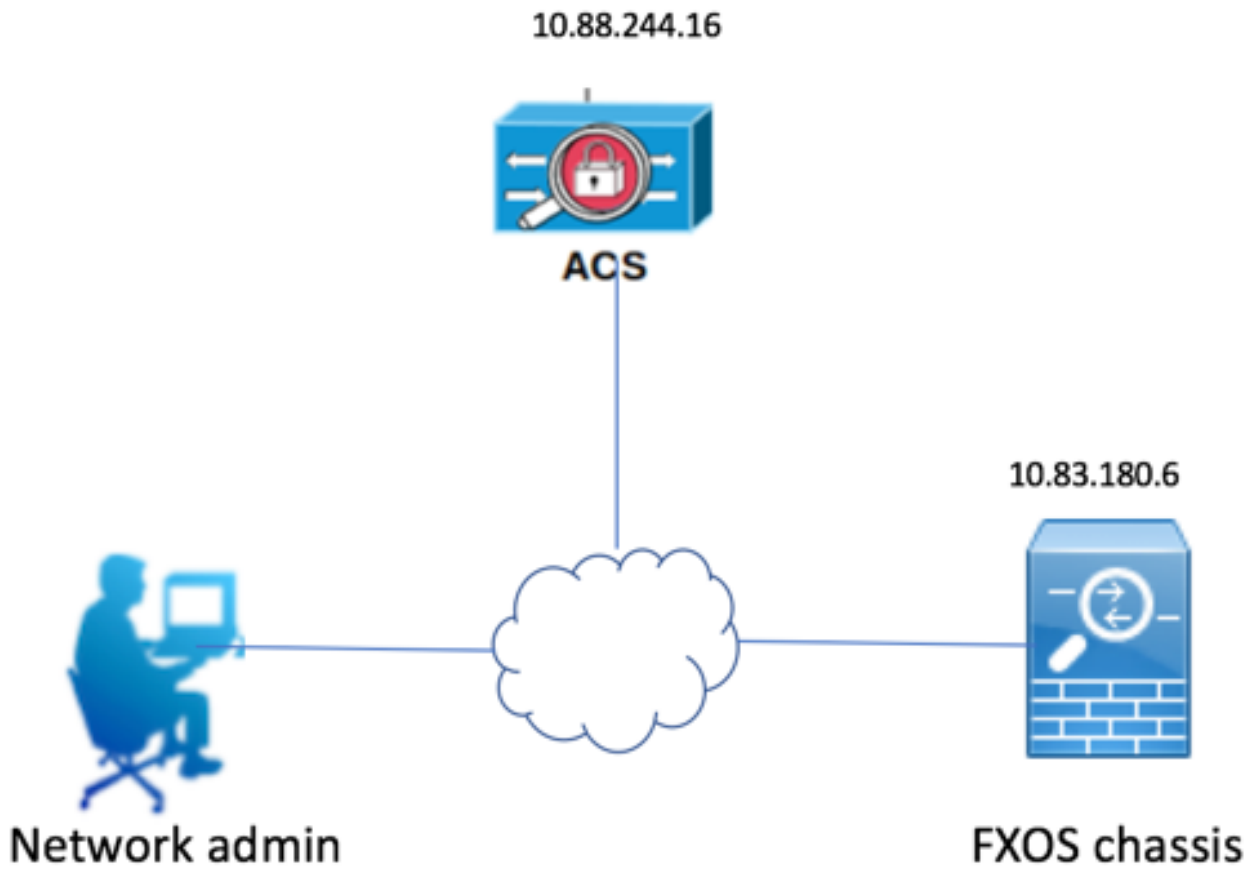
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

# 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



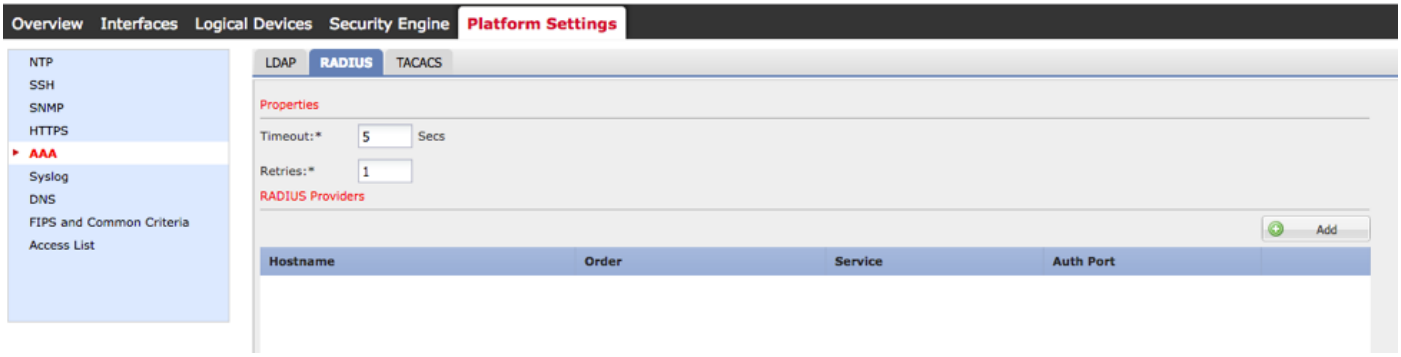

## Configurations

### Configuration du châssis FXOS

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

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

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

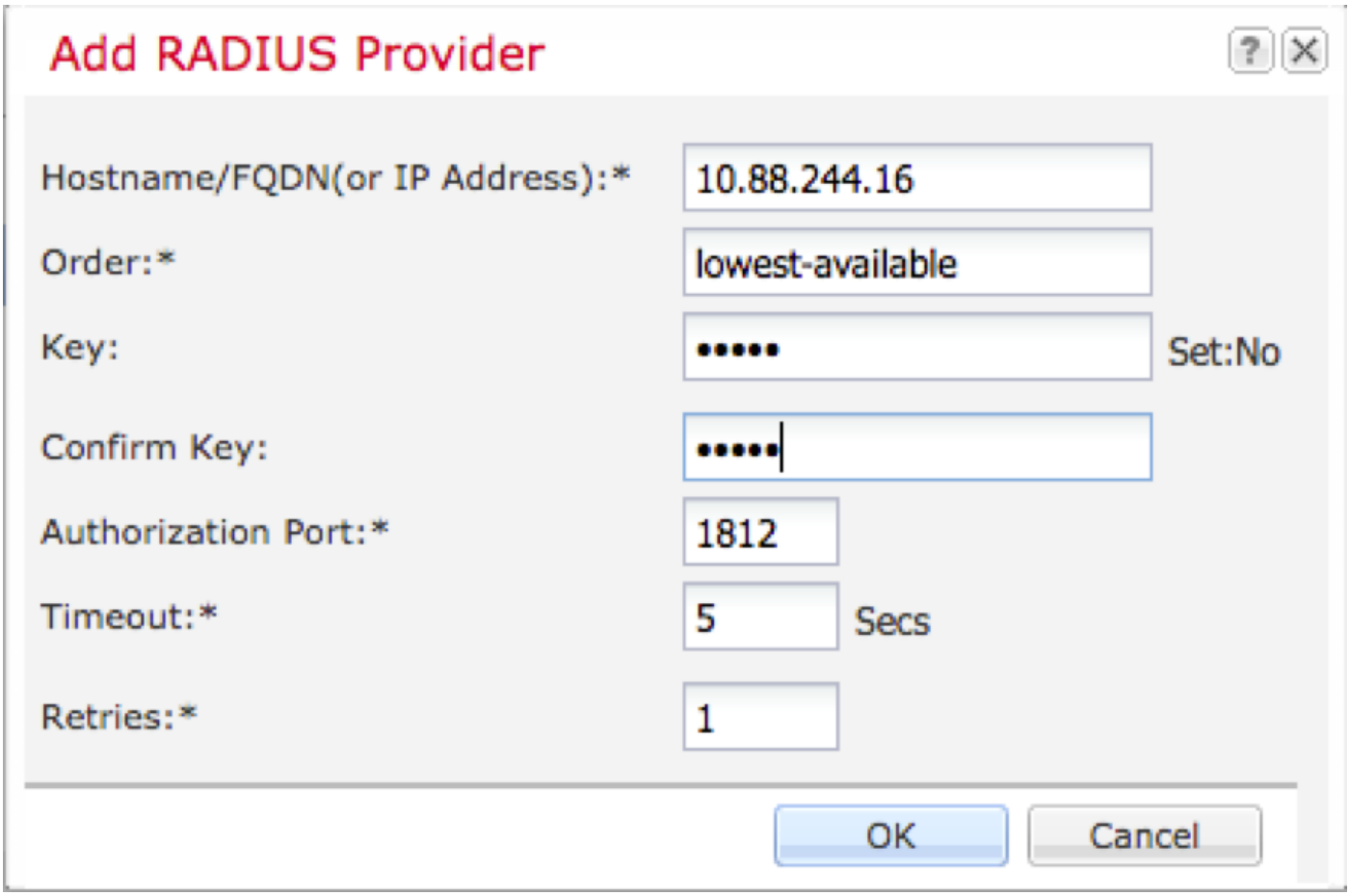



Étape 3. Pour chaque fournisseur RADIUS à ajouter (jusqu'à 16 fournisseurs).

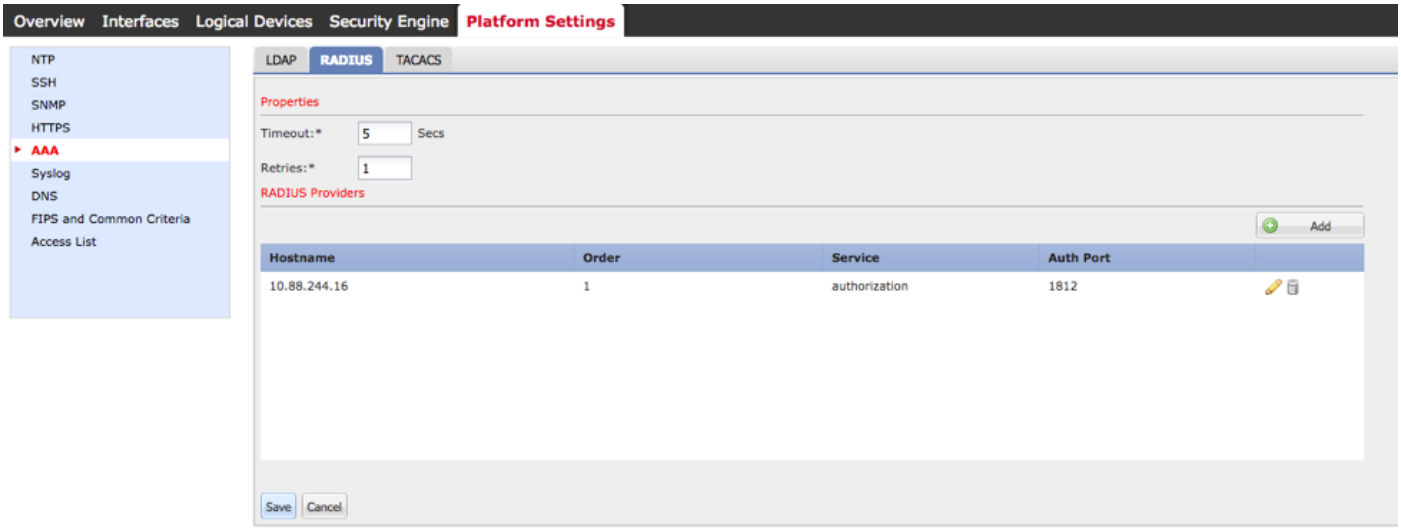
3.1. Dans la zone Fournisseurs RADIUS, cliquez sur **Ajouter.**

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

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

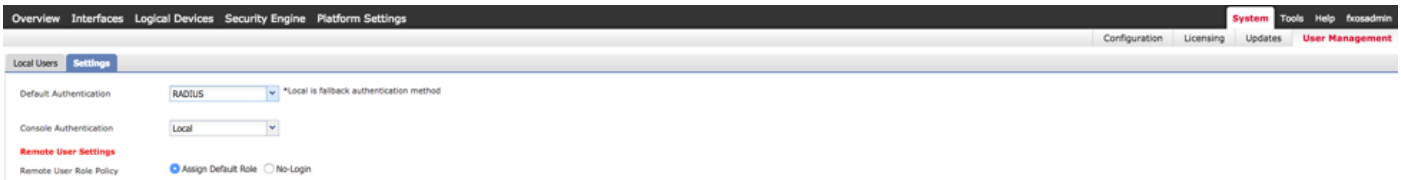



Étape 4. Click **Save**.




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

Étape 6. Sous Default Authentication, sélectionnez **RADIUS**.



### Création d'un fournisseur RADIUS à l'aide de l'interface de ligne de commande

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

fpr4120-TAC-A# **scope security**

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

fpr4120-TAC-A /security/default-auth # **set realm radius**

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 : **RADIUS**

Domaine opérationnel : **RADIUS**

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 RADIUS, exécutez les commandes suivantes.

fpr4120-TAC-A# **scope security**

fpr4120-TAC-A /security # **scope radius**

fpr4120-TAC-A /security/radius # **entrez server 10.88.244.16**

fpr4120-TAC-A /security/radius/server # **set descr « ISE Server »**

fpr4120-TAC-A /security/radius/server* # **set key**

Saisissez la clé : ******

Confirmez la clé : ******

Étape 4. Utilisez la commande **show detail** pour afficher les résultats.

fpr4120-TAC-A /security/radius/server* # **show detail**

Serveur RADIUS :

Nom d'hôte, nom de domaine complet ou adresse IP : 10.88.244.16

Description :

Commande : 1

Port d'authentification : 1812

Clé : ****

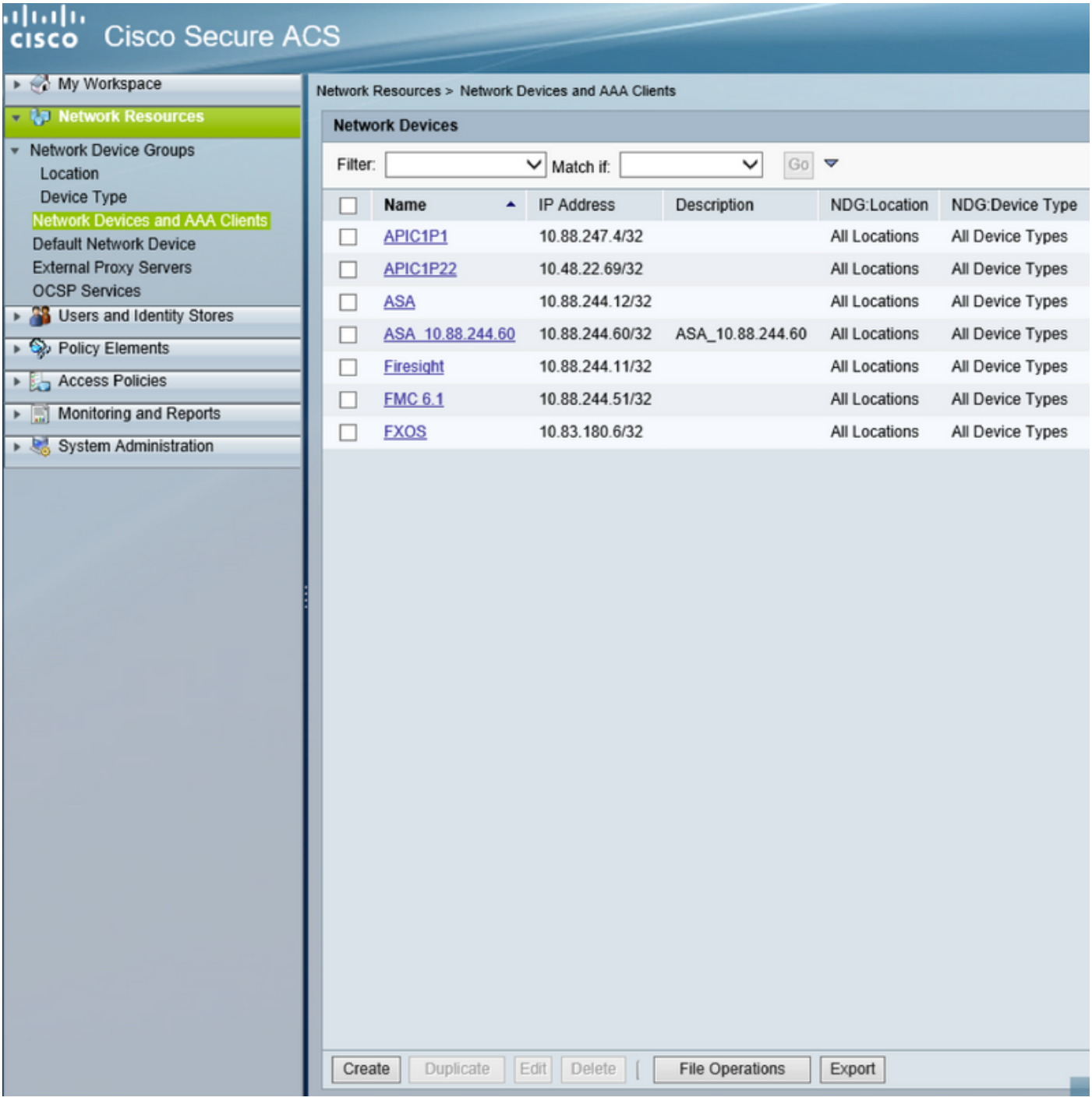
timeout : 5

## Configuration du serveur ACS

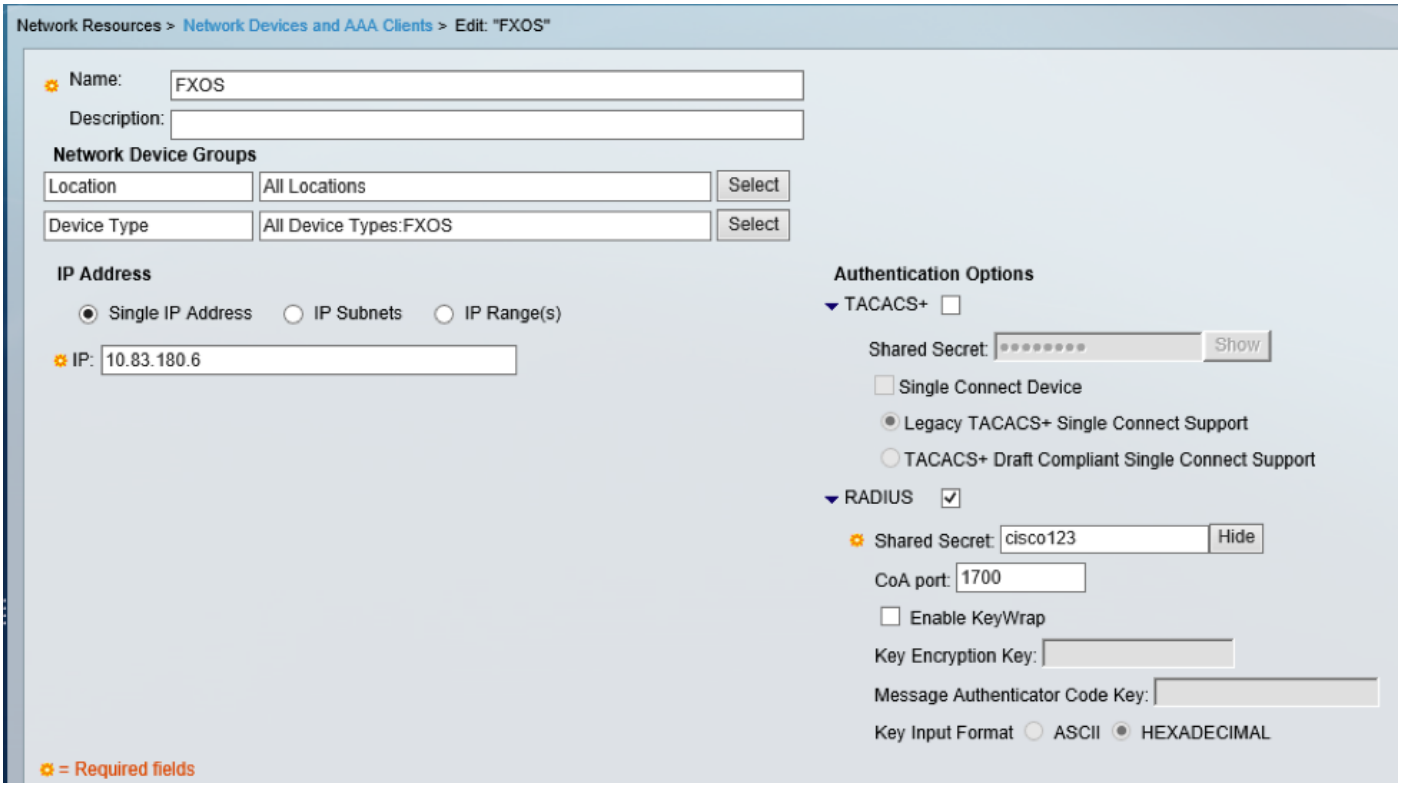
### Ajout du FXOS en tant que ressource réseau

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

Étape 2. Click **Create.**




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




Étape 4. Cliquez sur Submit.