Firepower 拡張可能なオペレーティング システム（FXOS） 2.2: RADIUS を使用して ACS の遠隔管理のためのシャーシ認証 および 権限

目次

概要

この資料に Access Control Server （ ACS ）によって Firepower 拡張可能なオペレーティング システム（ FXOS ）シャーシのための RADIUS認証および許可を設定する方法を記述されています。

FXOS シャーシは次のユーザの役割が含まれています:

- 管理者-システム全体に読み書きアクセスを完了して下さい。 デフォルト管理者アカウントこのロールはデフォルトで割り当てられ、変更することができません。
- 読み取り専用-システム 状態を変更する特権無しのシステム構成への読み取り専用アクセス。
- オペレーション-スマートな認可のための NTP 設定、Smart Call Home 設定、および syslog サーバおよびエラーを含むシステムログへの読み書きアクセス。 システムの他への読み取りアクセス。
- AAA： ユーザ、ロールおよび AAA設定への読み書きアクセス。 システムの他への読み取りアクセス。

CLI によってこれは次の通り見られる場合があります:

fpr4120-TAC-A /security * **#ロールを示して下さい**

ロール:

ロール名 Priv

---------- ----

AAA AAA

admin admin

オペレーション オペレーション

読み取り専用読み取り専用

、ホセ Soto トニー Remirez によって貢献される、Cisco TAC エンジニア。

前提条件

要件

次の項目に関する知識が推奨されます。

- Firepower 拡張可能なオペレーティング システム（FXOS）のナレッジ
- ACS 設定のナレッジ

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Firepower 4120 セキュリティ アプライアンス バージョン 2.2
- バーチャル Cisco Access Control Server バージョン 5.8.0.32

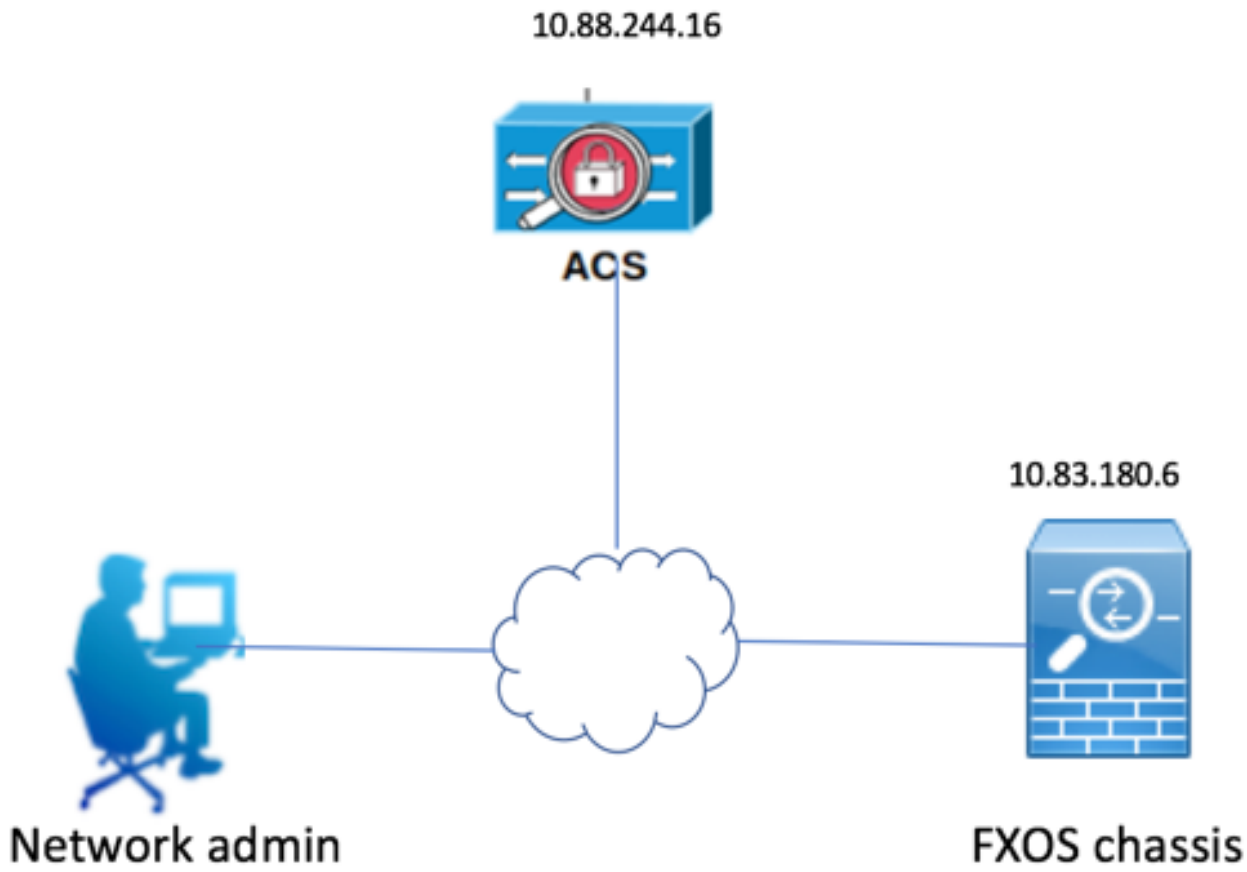
本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

設定

設定の目標はにあります:

- ACS によって FXOS の Webベース GUI および SSH にログイン して いるユーザを認証して下さい。
- ACS によってそれぞれユーザの役割に従って FXOS の Webベース GUI および SSH にログイン して いるユーザを許可して下さい。
- ACS によって FXOS の認証 および 権限の正しい動作を確認して下さい。

ネットワーク図



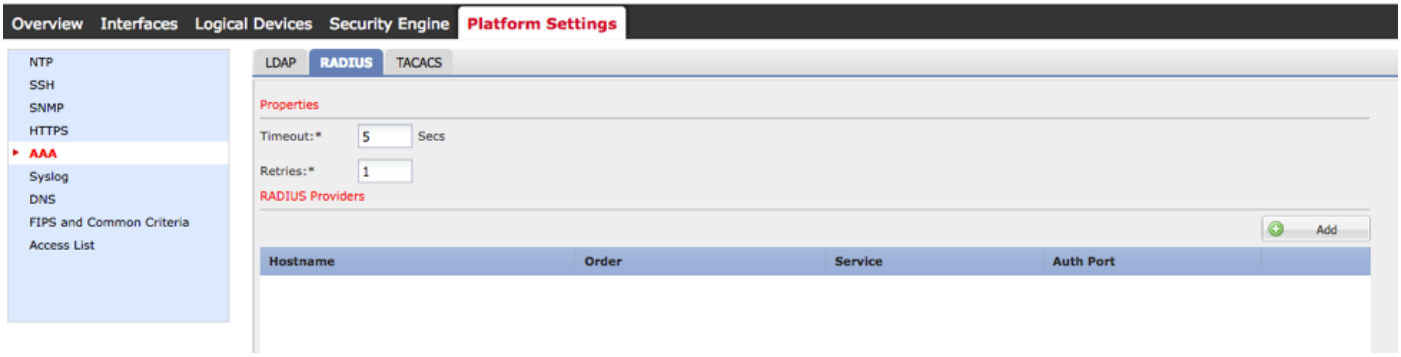
設定

FXOS シャーシの設定

シャーシ マネージャを使用する RADIUS プロバイダの作成

ステップ 1.**プラットフォーム設定 > AAA** へのナビゲート。

ステップ 2. **RADIUS タブを**クリックして下さい。



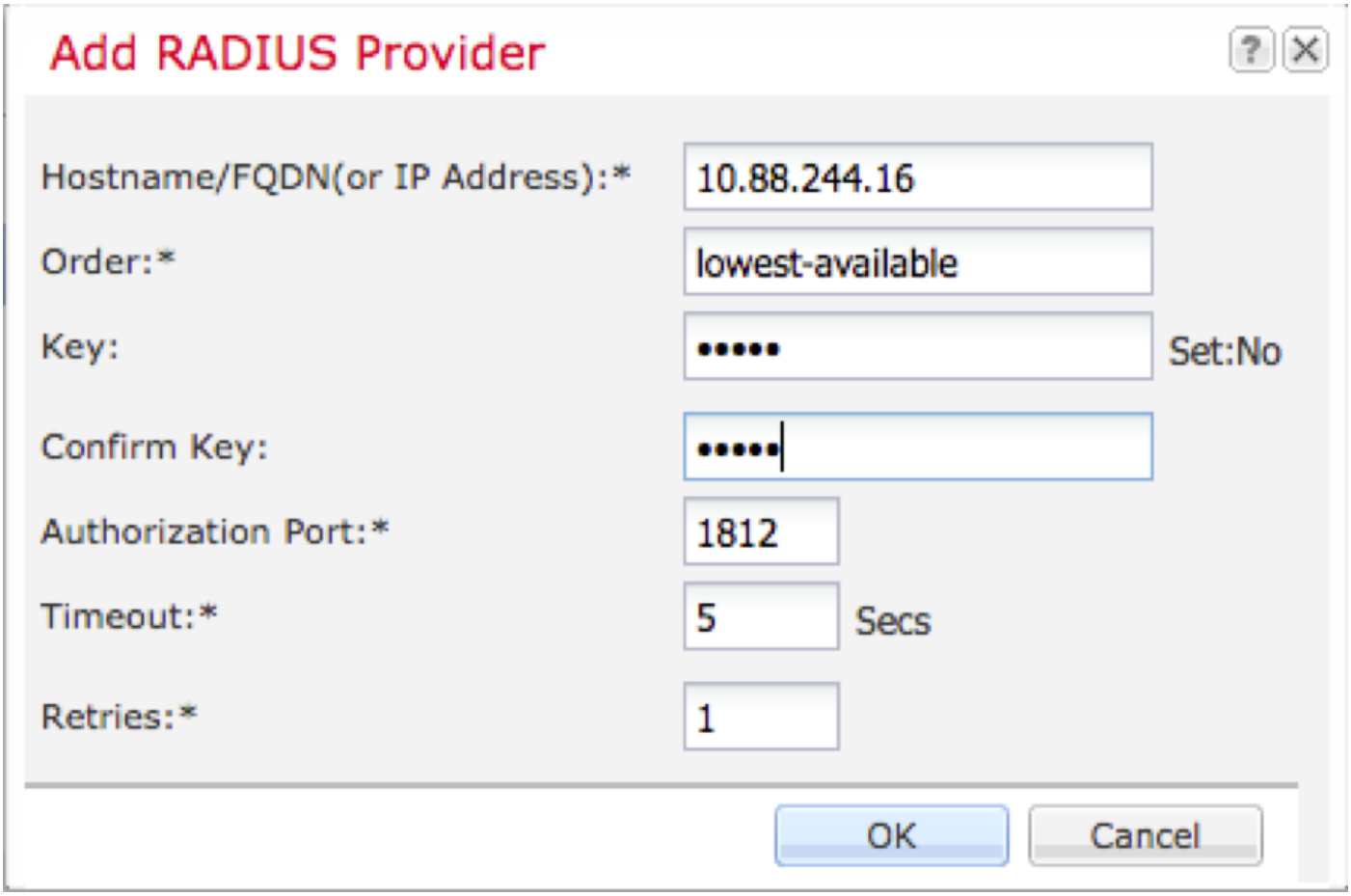
ステップ 3 追加したいと思う各 RADIUS プロバイダに関しては（16 人までのプロバイダ）。

3.1. RADIUS プロバイダ エリアで、『Add』 をクリック して下さい。

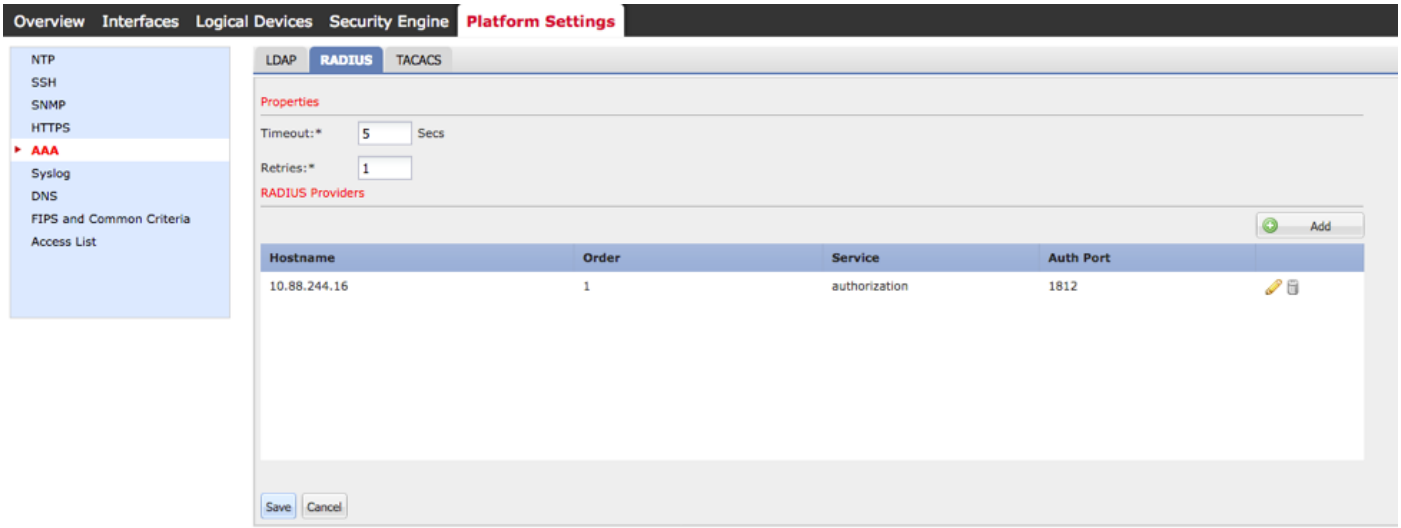
3.2. 追加 RADIUS プロバイダ ダイアログボックスでは、必要な値を入力して下さい。

3.3. 追加 RADIUS プロバイダ ダイアログボックスを閉じるために『OK』 をクリック し

て下さい。

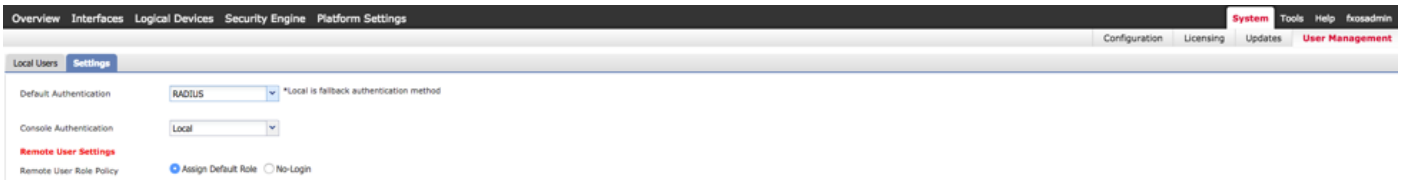


ステップ 4. 『SAVE』 をクリック して下さい。



ステップ 5.**システム > ユーザマネージメント > 設定**へのナビゲート。

ステップ 6 デフォルトの認証の下で『RADIUS』 を選択 して下さい。



CLI を使用する RADIUS プロバイダの作成

ステップ 1. RADIUS認証を有効に するために、次のコマンドを実行して下さい。

fpr4120-TAC-A# **スコープ セキュリティ**

fpr4120-TAC-A /security #**スコープ デフォルトauth**

fpr4120-TAC-A /security/default-auth は#**レルム半径を設定しました**

呼び出します。 結果を表示する**提示 detail コマンドを**使用して下さい。

fpr4120-TAC-A /security/default-auth は#**詳細を示します**

デフォルトの認証:

Admin レルム: **Radius**

操作上レルム: **Radius**

Web セッション リフレッシュ期間（秒で）: 600

Web のためのセッション タイムアウト（秒で）、ssh、Telnetセッション: 600

Web のための絶対セッション タイムアウト（秒で）、ssh、Telnetセッション: 3600

シリアルコンソール セッション タイムアウト（秒で）: 600

シリアルコンソール絶対セッション タイムアウト（秒で）: 3600

Admin 認証サーバ グループ:

操作上認証サーバ グループ:

第 2 ファクタの使用: なし

ステップ 3. RADIUSサーバ パラメータを設定するために次のコマンドを実行して下さい。

fpr4120-TAC-A# **スコープ セキュリティ**

fpr4120-TAC-A /security #**スコープ半径**

fpr4120-TAC-A /security/radius は#**サーバ 10.88.244.16 を入力します**

fpr4120-TAC-A /security/radius/server は#**設定しました descr 「ISE サーバ」を**

fpr4120-TAC-A /security/radius/server * # **Set 鍵**

キーを入力して下さい: ******

キーを確認して下さい: ******

ステップ 4 結果を表示する**提示 detail コマンドを**使用して下さい。

fpr4120-TAC-A /security/radius/server * **#詳細を示して下さい**

RADIUSサーバ:

ホスト名、FQDN または IP アドレス: 10.88.244.16

descr :

発注： 1

Auth ポート: 1812

凡例： ****

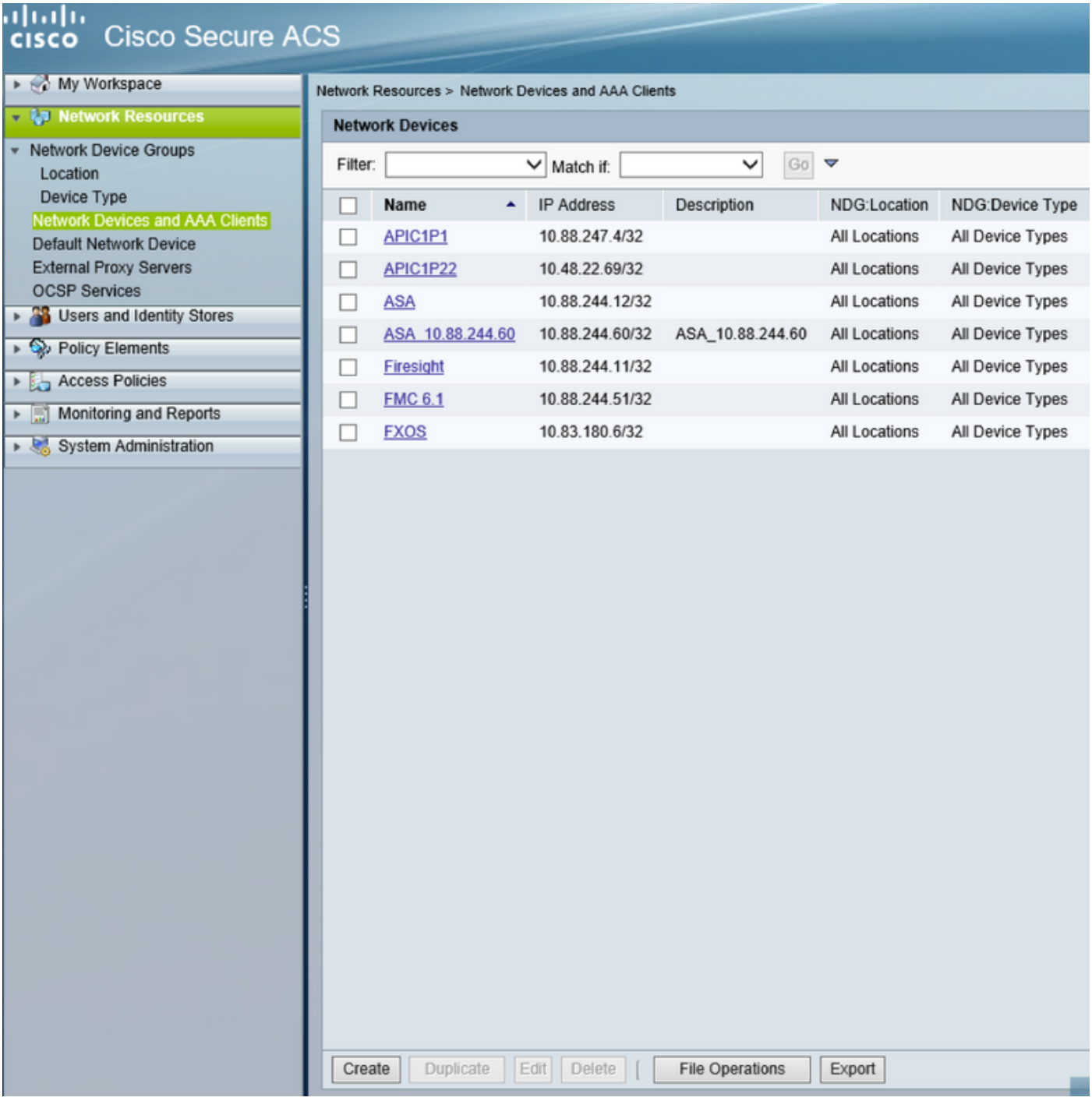
タイムアウト： 5

ACS サーバの設定

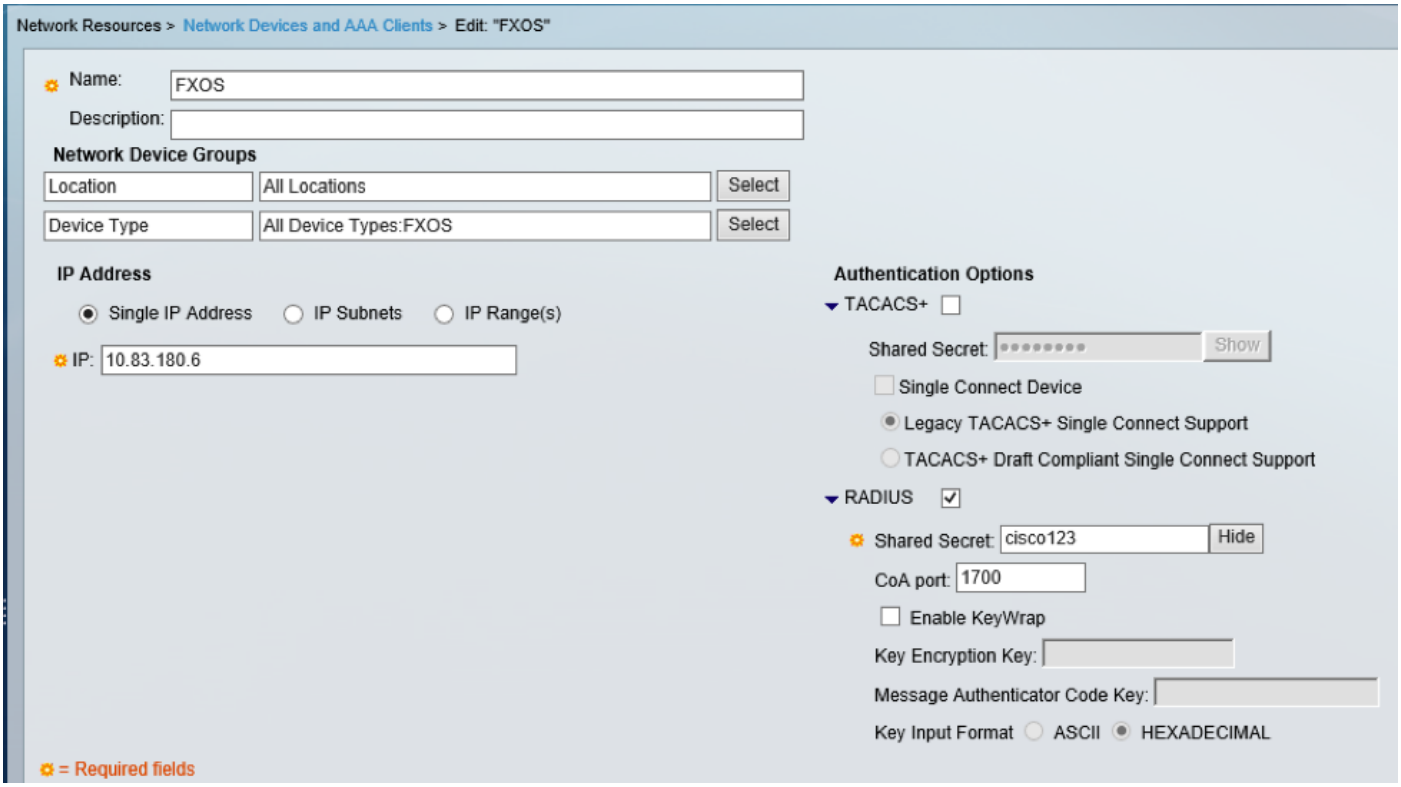
ネットワークリソースとして FXOS の追加

ステップ 1.**ネットワークリソース > ネットワークデバイスおよび AAA クライアント**へのナビゲート。

ステップ 2. 『Create』 をクリック して下さい。



ステップ 3.必要な値を入力して下さい (名前、IP アドレス、デバイスの種類およびイネーブル RADIUS はおよび KEY を追加します) 。



ステップ 4. 『SUBMIT』 をクリック して下さい。