Firepower可扩展操作系统(FXO) 2.2 ：远程管理的机箱认证和授权与ACS使用RADIUS

目录

简介

本文描述如何通过访问控制服务器(ACS)配置RADIUS验证和授权Firepower可扩展操作系统的(FXO)机箱的。

FXO机箱包括以下用户角色：

- 管理员-对整个系统的完整读写访问。默认管理帐户分配此角色默认情况下，并且不可能更改。
- 只读-对系统配置的只读访问没有权限修改系统状态。
- 操作-对NTP配置、聪明的Call Home配置聪明许可授权的和系统日志的读写访问，包括系统日志服务器和故障。对系统的其余的读访问。
- AAA -对用户、角色和AAA配置的读写访问。对系统的其余的读访问。

通过CLI这能被看到如下：

fpr4120-TAC-A /security * #请**显示角色**

角色：

角色命名Priv

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

aaa aaa

admin admin

操作操作

只读只读

贡献用托尼雷米雷斯，何塞索托， Cisco TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题：

- 知识Firepower可扩展操作系统(FXO)
- ACS配置知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Firepower 4120安全工具版本2.2
- 虚拟Cisco访问控制服务器版本5.8.0.32

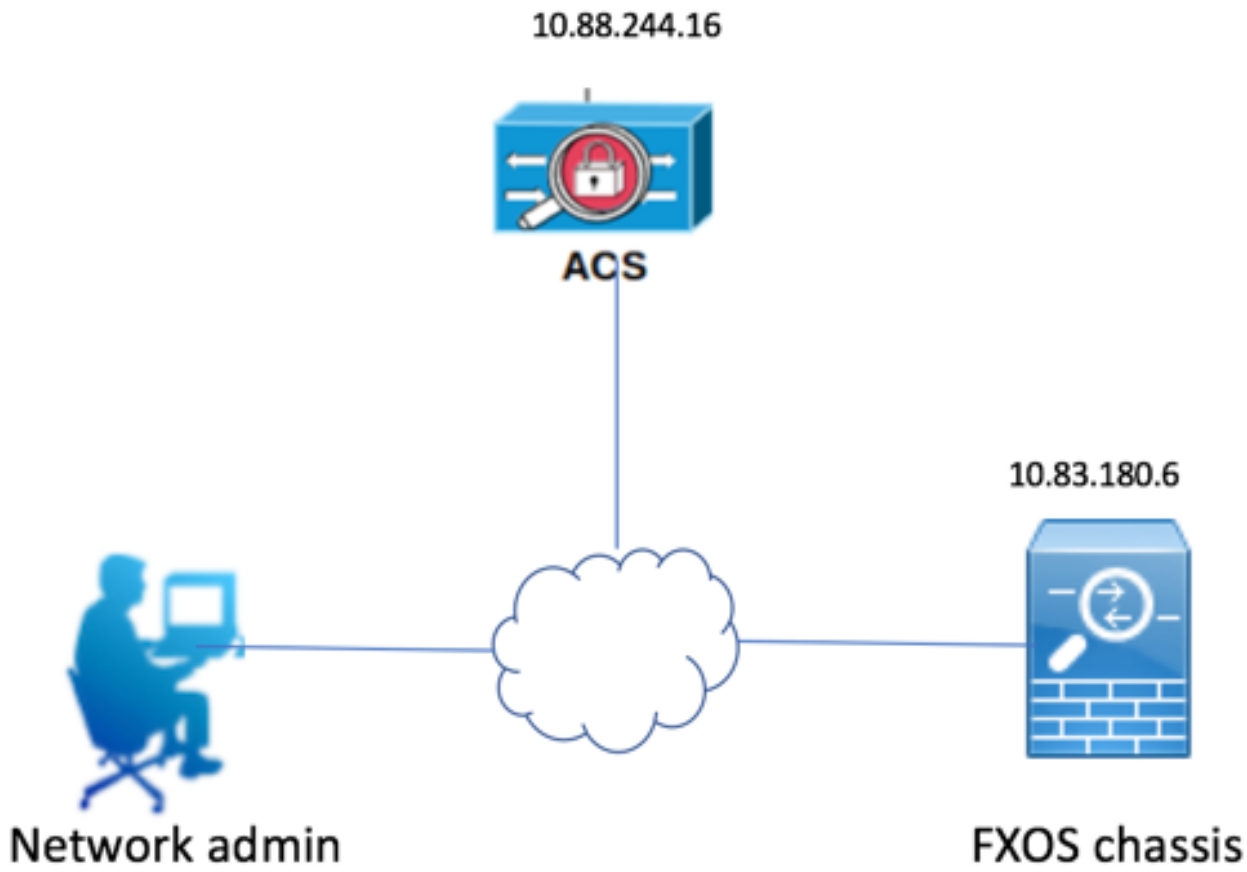
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

配置的目标对：

- 验证登录FXOS的基于Web的GUI和SSH的用户通过ACS。
- 认证登录FXOS的基于Web的GUI和SSH的用户根据他们的各自用户角色通过ACS。
- 通过ACS验证认证和授权正常操作在FXO的。

网络图



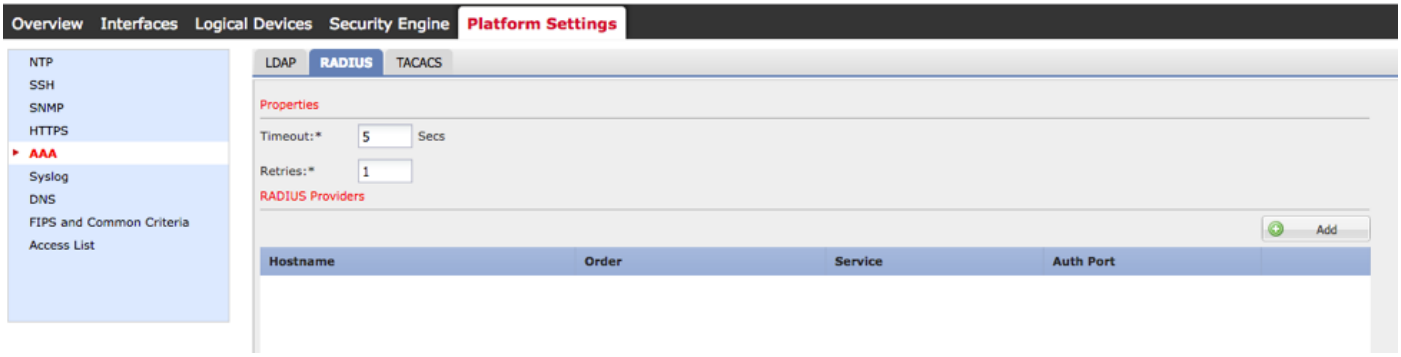
配置

配置FXO机箱

创建使用机箱管理器的RADIUS供应商

步骤1.导航对**平台设置>AAA。**

步骤2.点击**RADIUS选项。**

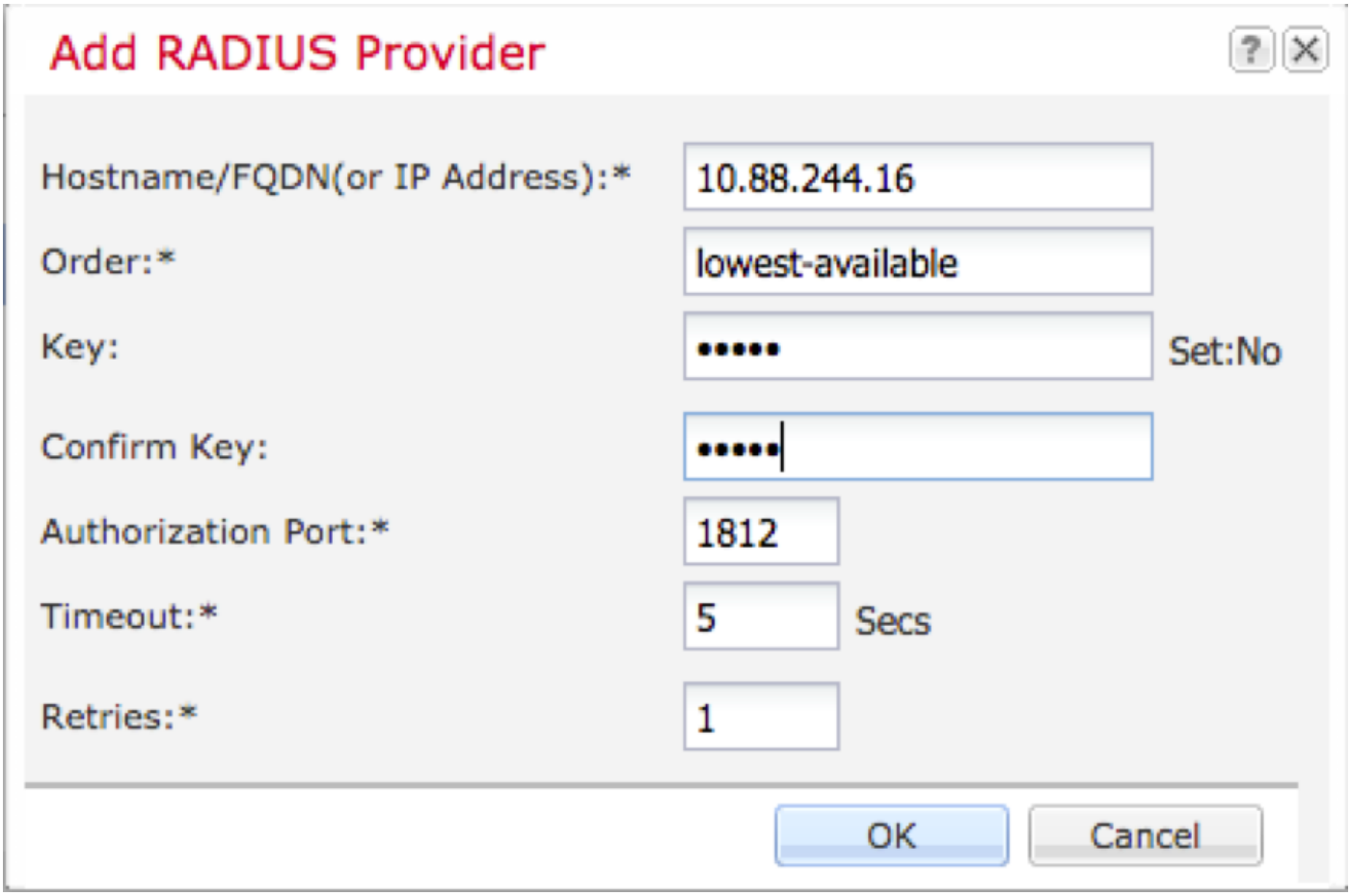


第三步：每个RADIUS供应商您想要添加(16个供应商)。

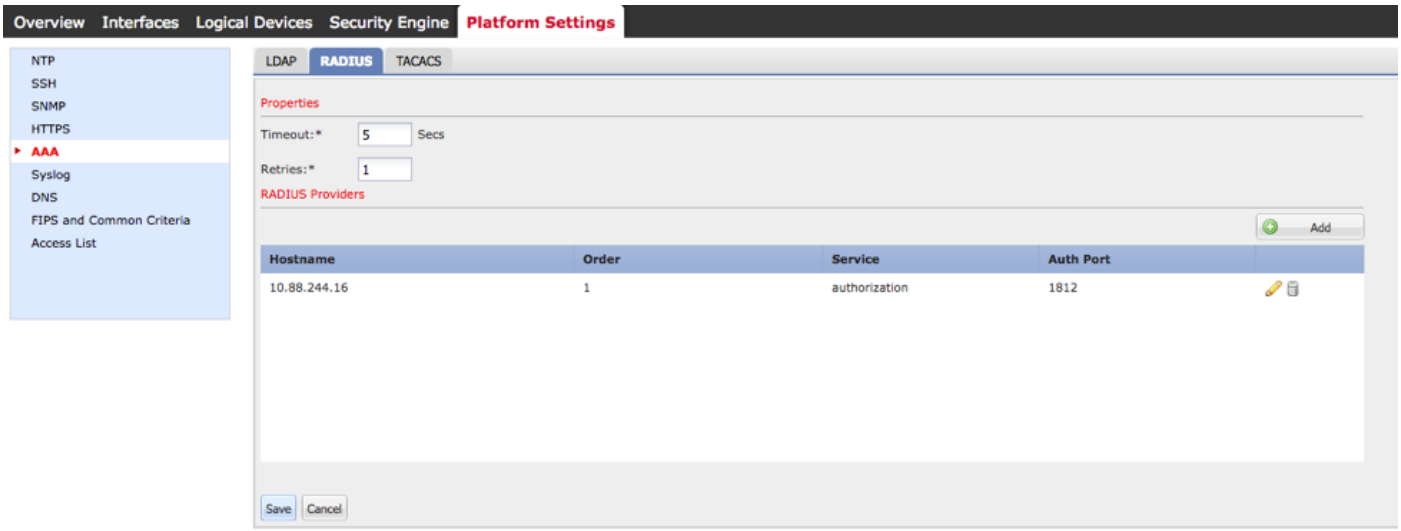
3.1. 在RADIUS供应商地区中，请单击**添加。**

3.2. 在添加RADIUS供应商对话框中，请输入需要的值。

3.3. 点击OK键关闭添加RADIUS供应商对话框。

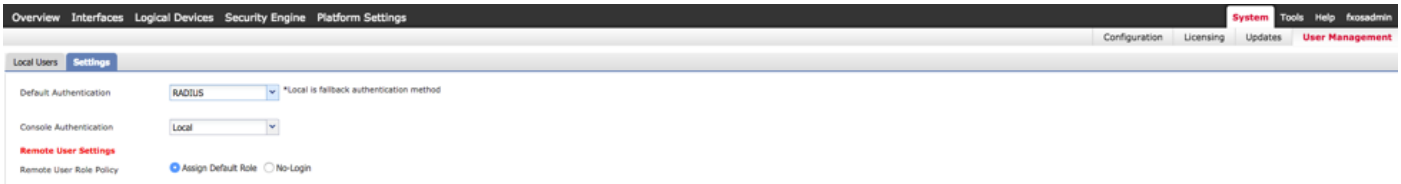


步骤4.点击**“Save”**。



步骤5.导航对**系统>用户管理>设置**。

第六步：在默认验证下请选择**RADIUS**。



创建使用CLI的RADIUS供应商

步骤1.为了启用RADIUS验证，请运行以下命令。

fpr4120-TAC-A#**范围安全**

fpr4120-TAC-A /security #**范围默认验证**

fpr4120-TAC-A /security/default-auth #**集领域radius**

第二步：请使用**detail命令的显示**显示结果。

fpr4120-TAC-A /security/default-auth #**显示详细信息**

默认验证：

Admin领域：**Radius**

可操作的领域：**Radius**

Web会话刷新期限(以秒) ：600

会话超时(以秒) Web的， SSH，远程登录会话：600

绝对会话超时(以秒) Web的， SSH，远程登录会话：3600

串行控制台会话超时(以秒) ：600

串行控制台绝对会话超时(以秒) ：3600

Admin认证服务器组：

可操作的认证服务器组：

使用第2个要素：无

步骤3.为了配置RADIUS服务器参数请运行以下命令。

fpr4120-TAC-A#**范围安全**

fpr4120-TAC-A /security #**范围radius**

fpr4120-TAC-A /security/radius #**回车服务器10.88.244.16**

fpr4120-TAC-A /security/radius/server #**集descr “ISE服务器”**

fpr4120-TAC-A /security/radius/server * #**集密钥**

输入密钥：******

确认密钥：******

第四步：请使用**detail命令的显示**显示结果。

fpr4120-TAC-A /security/radius/server * #请**显示详细信息**

RADIUS服务器：

主机名、FQDN或者IP地址：10.88.244.16

Descr ：

命令：1

验证波尔特：1812

密钥：****

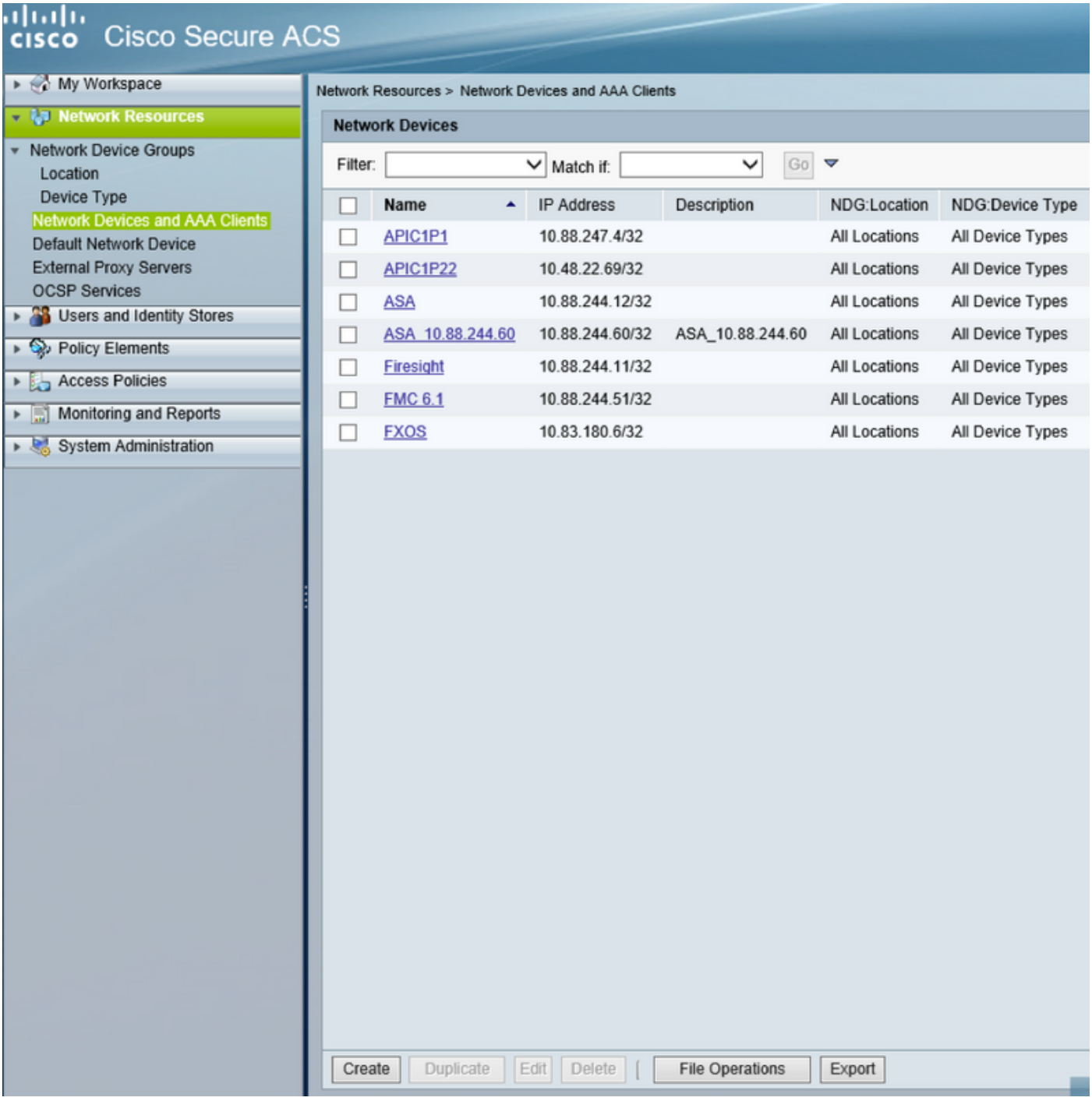
超时：5

配置ACS服务器

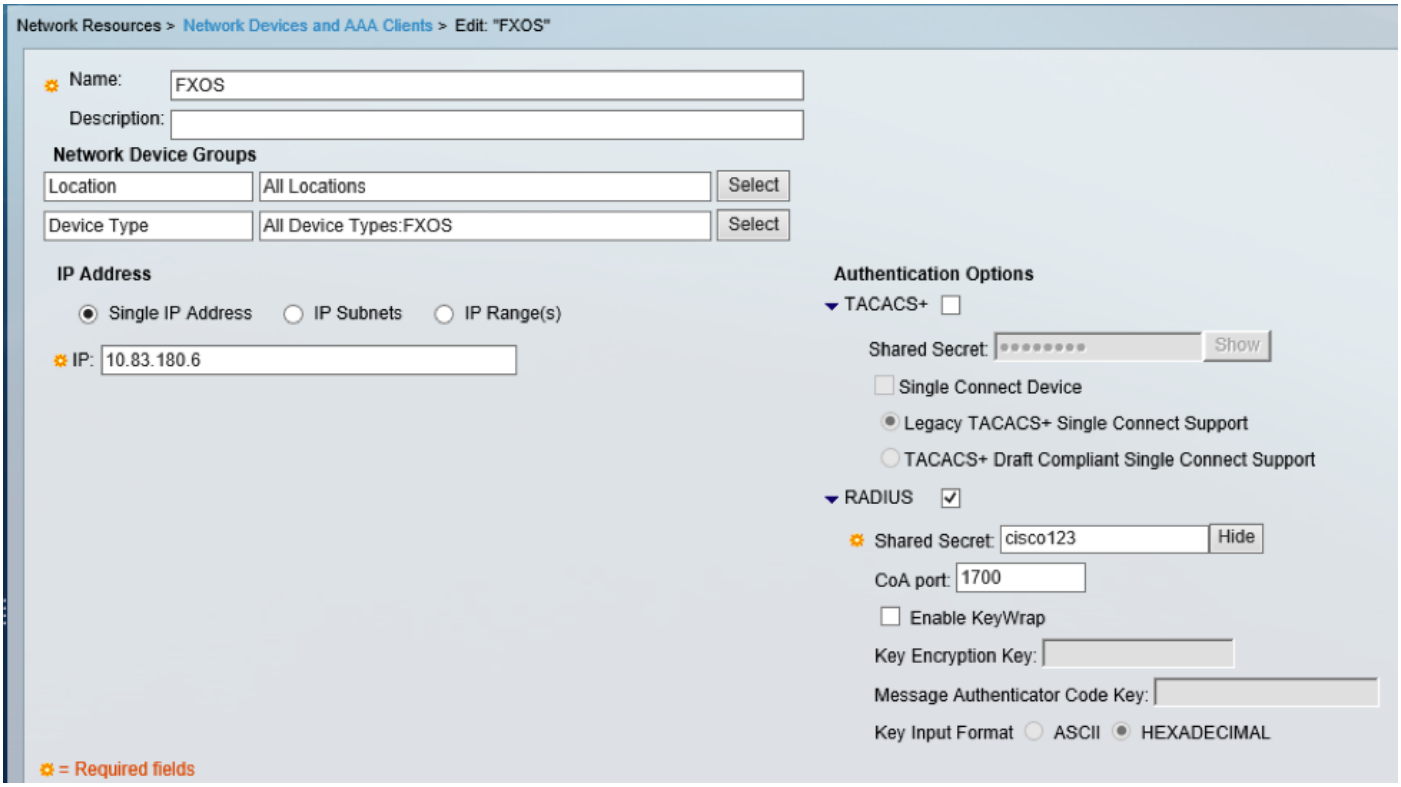
添加FXO作为网络资源

步骤1.导航给**网络资源>网络设备和AAA客户端**。

步骤2.单击**创建**。



步骤3.输入需要的值(名称、IP地址、设备类型和Enable (event) RADIUS和添加KEY)。


Network Resources > Network Devices and AAA Clients > Edit: "FXOS"
Name: FXOS
Description:
Network Device Groups
Location
All Locations
Select
Device Type
All Device Types:FXOS
Select
IP Address
Single IP Address
IP Subnets
IP Range(s)
IP: 10.83.180.6
Authentication Options
TACACS+
Shared Secret:
Show
Single Connect Device
Legacy TACACS+ Single Connect Support
TACACS+ Draft Compliant Single Connect Support
RADIUS
Shared Secret: cisco123
Hide
CoA port: 1700
Enable KeyWrap
Key Encryption Key:
Message Authenticator Code Key:
Key Input Format
ASCII
HEXADECIMAL
= Required fields

步骤4.单击**提交**。