

# Sistema operacional elástico de FirePOWER (FXO) 2.2: Authentication e autorização do chassi para o Gerenciamento remoto com ACS usando o RAIO

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configurando o chassi FXO](#)

[Configurando o servidor ACS](#)

[Verificar](#)

[Verificação do chassi FXO](#)

[Verificação ACS](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

## Introdução

Este documento descreve como configurar a autenticação RADIUS e a autorização para o chassi elástico do sistema operacional de FirePOWER (FXO) através do Access Control Server (ACS).

O chassi FXO inclui os seguintes papéis de usuário:

- Administrador - Termine o acesso de leitura e gravação ao sistema inteiro. A conta admin do padrão é atribuída este papel à revelia e não pode ser mudada.
- Read-Only - Acesso somente leitura à configuração de sistema sem privilégios alterar o estado de sistema.
- Operações - Acesso de leitura e gravação à configuração de NTP, à configuração esperta do Call Home para Smart que licencia, e aos log de sistema, incluindo servidores de SYSLOG e falhas. Acesso de leitura ao resto do sistema.
- AAA - Acesso de leitura e gravação aos usuários, aos papéis, e à configuração de AAA. Acesso de leitura ao resto do sistema.

Através do CLI isto pode ser visto como segue:

```
fpr4120-TAC-A /security * # papel da mostra
```

Papel:

Priv do nome do papel

----- ----

aaa aaa

admin admin

operações das operações

de leitura apenas de leitura apenas

Contribuído por Tony Ramirez, Jose Soto, engenheiros de TAC da Cisco.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento do sistema operacional elástico de FirePOWER (FXO)
- Conhecimento da configuração ACS

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão 2.2 da ferramenta de segurança de Cisco FirePOWER 4120
- Versão 5.8.0.32 virtual do Access Control Server de Cisco

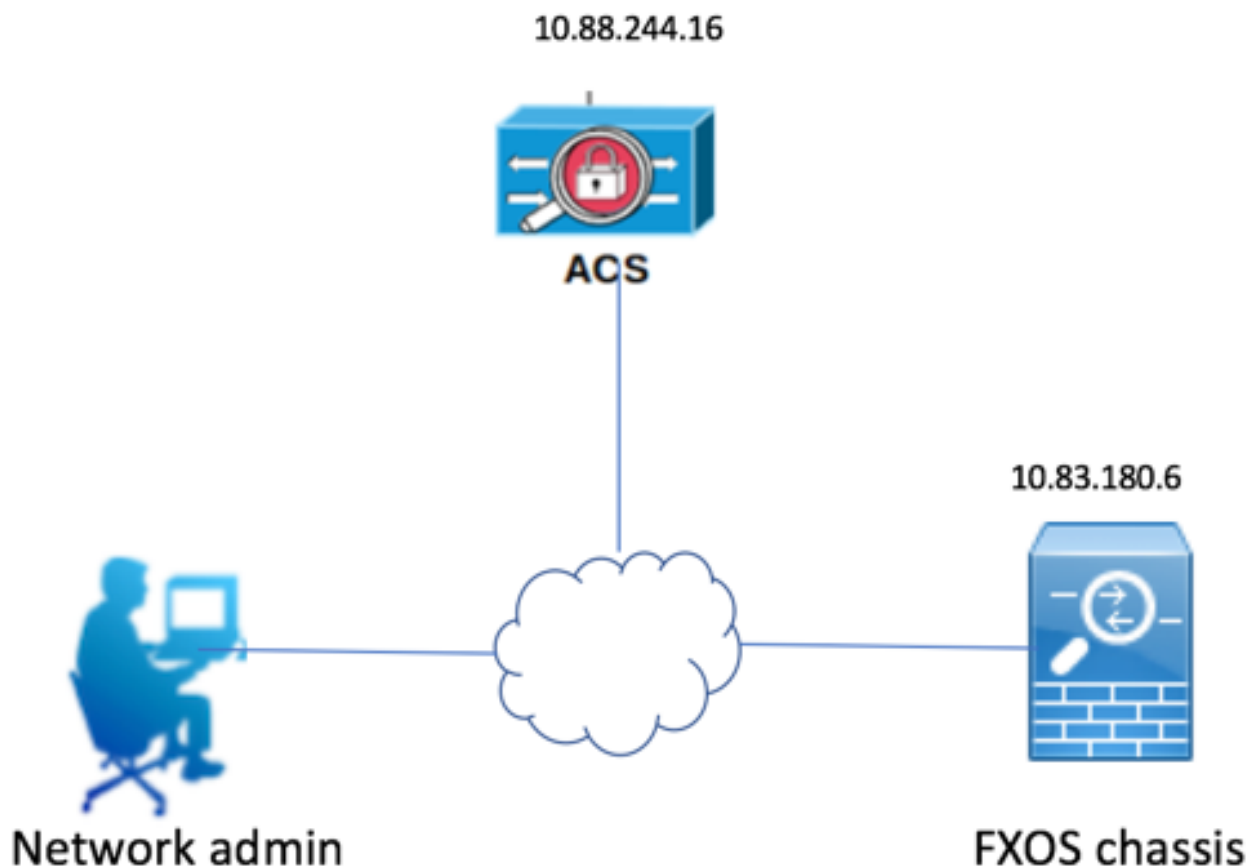
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Configurar

O objetivo da configuração está a:

- Autentique os usuários que registram no GUI com base na Web e no SSH do FXOS por meio do ACS.
- Autorize os usuários que registram no GUI com base na Web e no SSH do FXOS de acordo com seu papel de usuário respectivo por meio do ACS.
- Verifique a operação apropriada da authentication e autorização nos FXO por meio do ACS.

### Diagrama de Rede



## Configurações

### Configurando o chassi FXO

Criando um fornecedor do RAIO que usa o gerente do chassi

Etapa 1. Navegue aos ajustes da plataforma > ao AAA.

Etapa 2. Clique a aba do RAIO.

The screenshot shows the "Platform Settings" page in a network management interface. The left sidebar contains a menu with options: NTP, SSH, SNMP, HTTPS, AAA (highlighted), Syslog, DNS, FIPS and Common Criteria, and Access List. The main content area is titled "RADIUS" and includes "Properties" and "RADIUS Providers" sections. The "Properties" section has input fields for "Timeout:\*" (set to 5) and "Retries:\*" (set to 1). The "RADIUS Providers" section features a table with columns for "Hostname", "Order", "Service", and "Auth Port", and an "Add" button.

Etapa 3. Para cada fornecedor do RAIO que você quer adicionar (até 16 fornecedores).

3.1. Na área dos fornecedores do RAIO, o clique **adiciona**.

3.2. Na caixa de diálogo do fornecedor do RAIO adicionar, incorpore os valores exigidos.

3.3. **APROVAÇÃO** do clique para fechar a caixa de diálogo do fornecedor do RAIO

adicionar.

### Add RADIUS Provider

Hostname/FQDN(or IP Address):\*

Order:\*

Key:  Set:No

Confirm Key:

Authorization Port:\*

Timeout:\*  Secs

Retries:\*

Etapa 4. Salvar do clique.

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

Retries:\*

RADIUS Providers

Hostname	Order	Service	Auth Port	
10.88.244.16	1	authorization	1812	

Etapa 5. Navegue ao sistema > ao gerenciamento de usuário > aos ajustes.

Etapa 6. Sob a autenticação padrão escolha o RAIO.

Overview Interfaces Logical Devices Security Engine Platform Settings

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

## Criando um fornecedor do RAIO que usa o CLI

Etapa 1. A fim permitir a autenticação RADIUS, execute os comandos seguintes.

**Segurança do espaço** fpr4120-TAC-A#

fpr4120-TAC-A /security # padrão-AUTH do espaço

fpr4120-TAC-A /security/default-auth # ajustou o raio do reino

Etapa 2. Use o **comando detail da mostra** indicar os resultados.

fpr4120-TAC-A /security/default-auth # **detalhe da mostra**

Autenticação padrão:

Reino Admin: **Radius**

Reino operacional: **Radius**

A sessão da web refresca o período (nos segundos): 600

Timeout de sessão (nos segundos) para a Web, ssh, sessões de Telnet: 600

Timeout de sessão absoluto (nos segundos) para a Web, ssh, sessões de Telnet: 3600

Timeout de sessão do console serial (nos segundos): 600

Timeout de sessão absoluto do console serial (nos segundos): 3600

Grupo de servidor da Autenticação de admin:

Grupo de Authentication Server operacional:

Uso do ó fator: No

Etapa 3. A fim configurar parâmetros do servidor Radius execute os comandos seguintes.

**Segurança do espaço** fpr4120-TAC-A#

fpr4120-TAC-A /security # **raio do espaço**

fpr4120-TAC-A /security/radius # **entram no server 10.88.244.16**

fpr4120-TAC-A /security/radius/server # **ajustou o descr "server ISE"**

fpr4120-TAC-A /security/radius/server \* # **ajuste a chave**

Incorpore a chave: **\*\*\*\*\***

Confirme a chave: **\*\*\*\*\***

Etapa 4. Use o **comando detail da mostra** indicar os resultados.

fpr4120-TAC-A /security/radius/server \* # **detalhe da mostra**

Servidor Radius:

Hostname, FQDN ou endereço IP de Um ou Mais Servidores Cisco ICM NT: 10.88.244.16

Descr:

Ordem: 1

Porta do AUTH: 1812

Chave: \*\*\*\*

Intervalo: 5

### **Configurando o servidor ACS**

#### **Adicionando os FXO como uns recursos de rede**

Etapa 1. Navegue aos **recursos de rede > aos dispositivos de rede e aos clientes de AAA.**

Etapa 2. O clique **cria.**

My Workspace

**Network Resources**

- Network Device Groups
  - Location
  - Device Type
  - Network Devices and AAA Clients**
  - Default Network Device
  - External Proxy Servers
  - OCSP Services
- Users and Identity Stores
- Policy Elements
- Access Policies
- Monitoring and Reports
- System Administration

Network Resources > Network Devices and AAA Clients

**Network Devices**

Filter:  Match if:

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

|

Etapa 3. Incorpore os valores exigidos (o nome, endereço IP de Um ou Mais Servidores Cisco ICM NT, tipo de dispositivo e permite o RAIO e adiciona a CHAVE).

Name:

Description:

**Network Device Groups**

Location

Device Type

**IP Address**

- Single IP Address    IP Subnets    IP Range(s)

IP:

**Authentication Options**

- ▼ TACACS+

Shared Secret:

- Single Connect Device
- Legacy TACACS+ Single Connect Support
- TACACS+ Draft Compliant Single Connect Support

- ▼ RADIUS

Shared Secret:

CoA port:

- Enable KeyWrap

Key Encryption Key:

Message Authenticator Code Key:

- Key Input Format  ASCII  HEXADECIMAL

 = Required fields

Etapa 4. O clique **submete-se**.



