

# Sistema operacional elástico de FirePOWER (FXO) 2.2: Autenticação/autorização do chassi para o Gerenciamento remoto com ISE usando o RADIUS

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configurando o chassi FXO](#)

[Configurando o server ISE](#)

[Verificar](#)

[Verificação FXO Chassis](#)

[Verificação ISE 2.0](#)

[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 Identity Services Engine (ISE).

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 ISE

### 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
- Cisco Identity Services Engine virtual 2.2.0.470

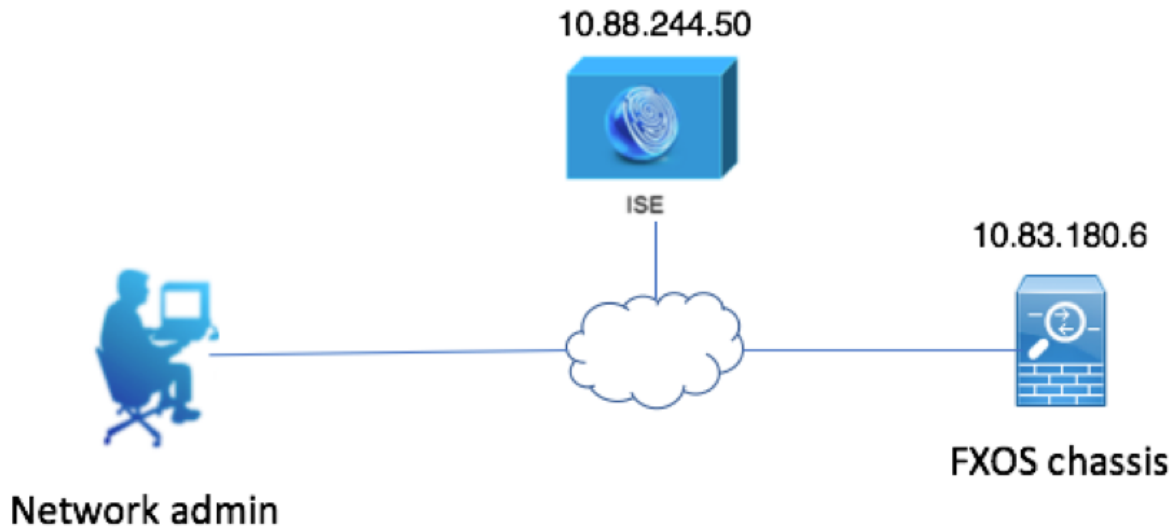
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer 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 ISE
- 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 ISE.
- Verifique a operação apropriada da authentication e autorização nos FXO por meio do ISE

### Diagrama de Rede



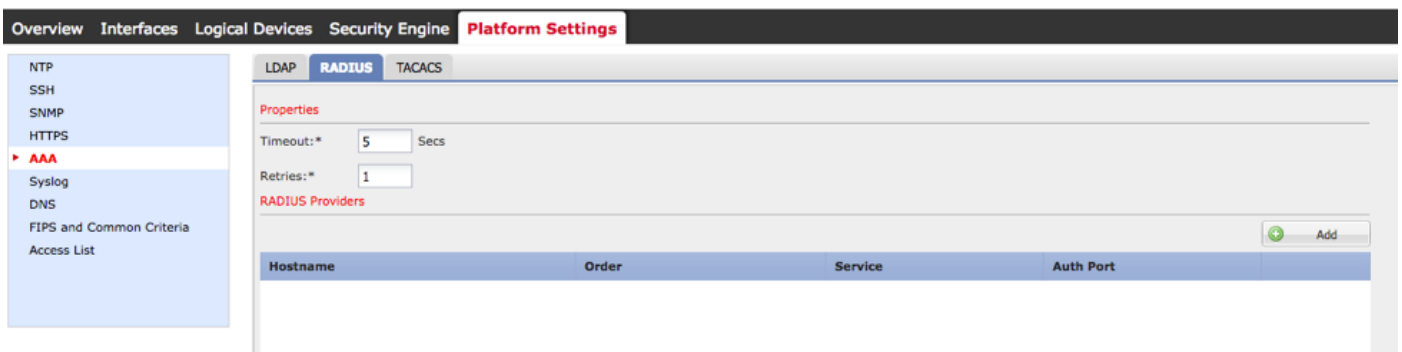
## Configurações

### 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**.

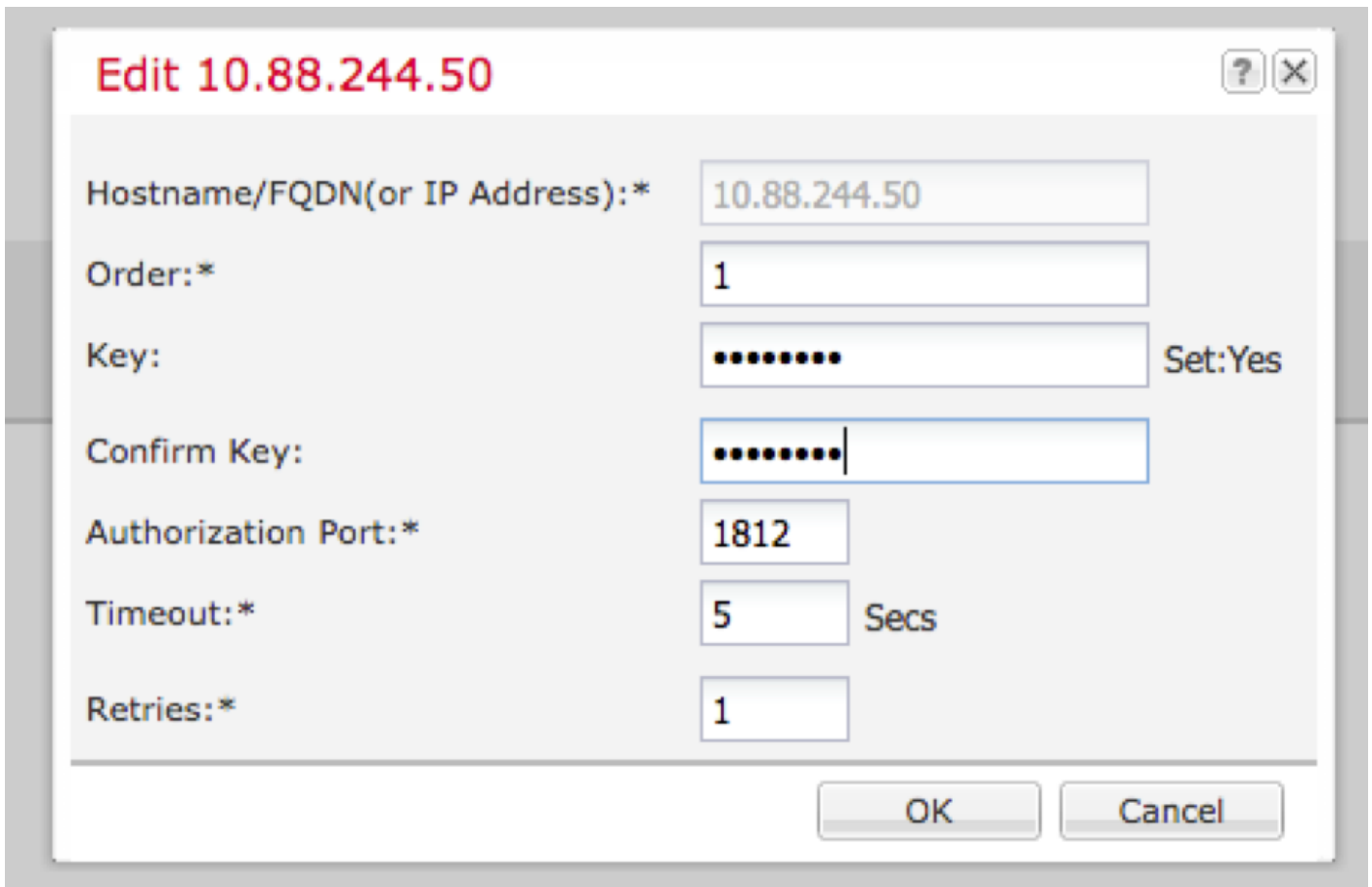


Etapa 3. Para cada fornecedor do RAIO que você quer adicionar (até 16 fornecedores).

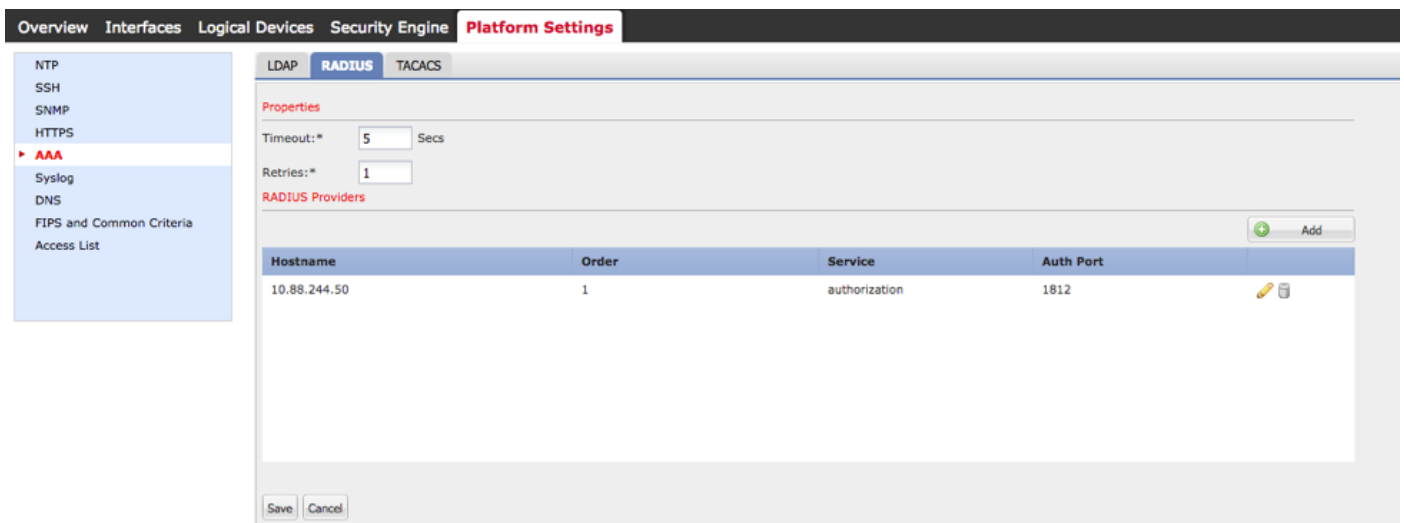
3.1. Na área dos fornecedores do RAIO, o clique **adiciona**.

3.2. Uma vez a caixa de diálogo do fornecedor do RAIO adicionar abre, incorpora os valores exigidos.

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

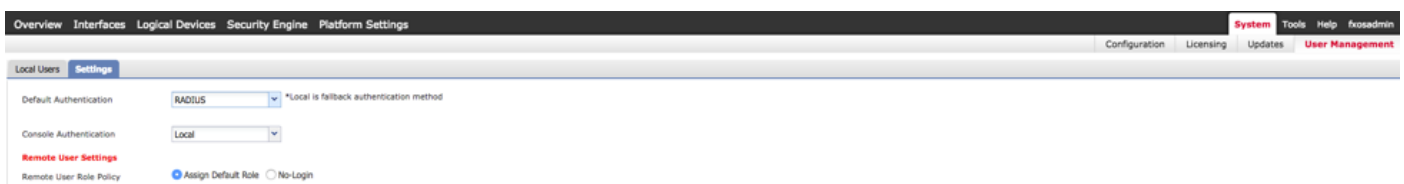


Etapa 4. Salvaguarda do clique.



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

Etapa 6. Sob a autenticação padrão escolha o RAIO.



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 ò 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 10.88.244.50**

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: 10.88.244.50

Descr:

Ordem: 1

Porta do AUTH: 1812

Chave: \*\*\*\*

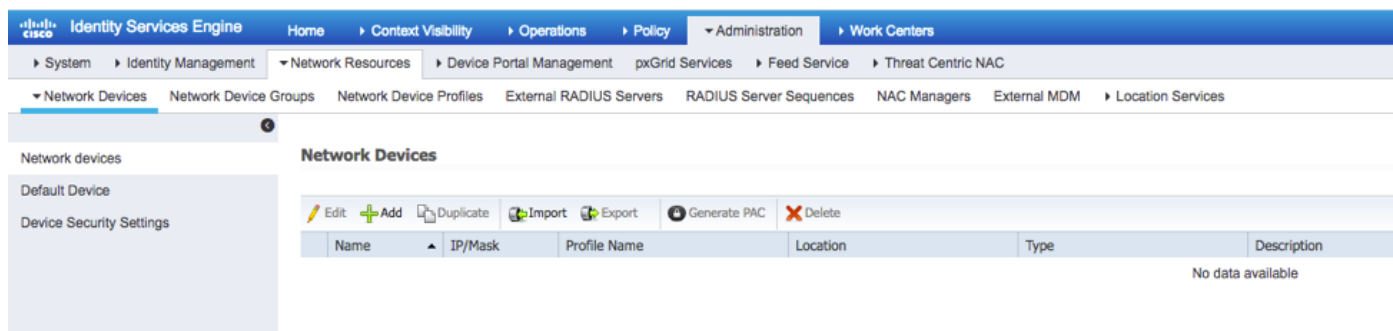
Intervalo: 5

## Configurando o server ISE

### Adicionando os FXO como uns recursos de rede

Etapa 1. Navegue à administração > aos recursos de rede > aos dispositivos de rede.

Etapa 2. O clique **ADICIONA**



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Under Administration, the Network Resources section is expanded, showing Network Devices, Network Device Groups, Network Device Profiles, External RADIUS Servers, RADIUS Server Sequences, NAC Managers, External MDM, and Location Services. The Network Devices page is active, displaying a table with columns for Name, IP/Mask, Profile Name, Location, Type, and Description. The table is currently empty, with the text "No data available" displayed below it. The toolbar above the table includes options for Edit, Add, Duplicate, Import, Export, Generate PAC, and Delete.

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), clique **submetem-se**.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network devices

Default Device

Device Security Settings

Network Devices List > New Network Device

**Network Devices**

\* Name

Description

---

\* IP Address:  /

\* Device Profile Cisco

Model Name

Software Version

\* Network Device Group

Device Type

IPSEC

Location

**RADIUS Authentication Settings**

**RADIUS UDP Settings**

Protocol **RADIUS**

\* Shared Secret

CoA Port

**RADIUS DTLS Settings** ⓘ

DTLS Required  ⓘ

Shared Secret  ⓘ

CoA Port

Issuer CA of ISE Certificates for CoA  ⓘ

## Criando os grupos e os usuários da identidade

Etapa 1. Navegue à administração > ao Gerenciamento de identidades > aos grupos > aos grupos da identidade do usuário.

Etapa 2. O clique **ADICIONA**.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities **Groups** External Identity Sources Identity Source Sequences Settings

**Identity Groups**

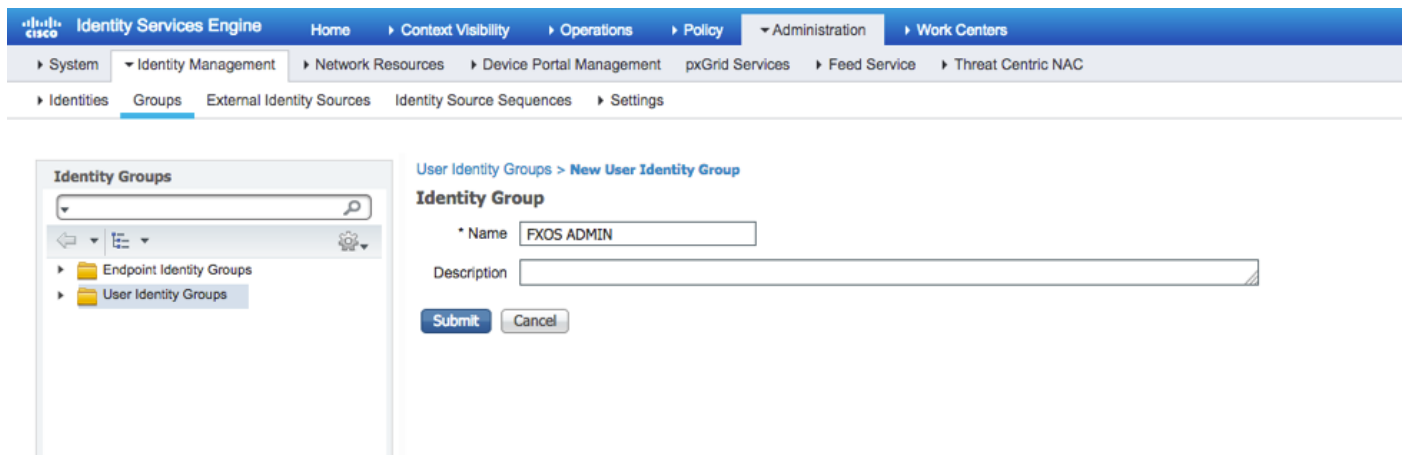
- Endpoint Identity Groups
- User Identity Groups**

**User Identity Groups**

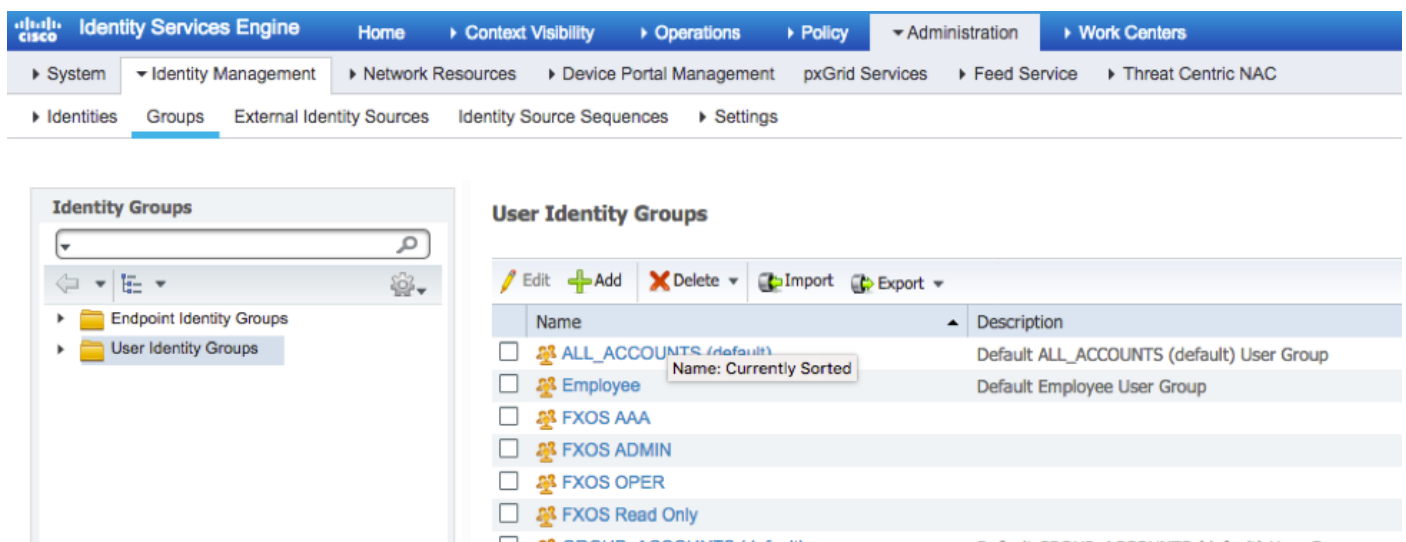
Edit  Add  Delete  Import  Export

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/>	Employee	Default Employee User Group
<input type="checkbox"/>	GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
<input type="checkbox"/>	GuestType_Contractor (default)	Identity group mirroring the guest type
<input type="checkbox"/>	GuestType_Daily (default)	Identity group mirroring the guest type
<input type="checkbox"/>	GuestType_Weekly (default)	Identity group mirroring the guest type
<input type="checkbox"/>	OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

Etapa 3. Incorpore o valor para o nome e o clique **submete-se**.

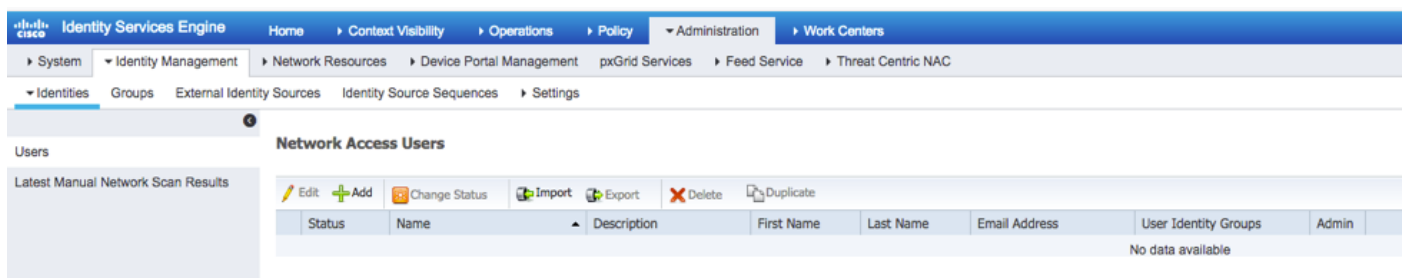


Etapa 4. Repita etapa 3 para todos os papéis de usuário exigidos.



Etapa 5. Navegue à **administração** > ao **Gerenciamento de identidades** > à **identidade** > aos **usuários**.

Etapa 6. O clique **ADICIONA**.



Etapa 7. Incorpore os valores exigidos (nome, grupo de usuário, senha).



Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users List > New Network Access User

**Network Access User**

Name:

Status:  Enabled

Email:

**Passwords**

Password Type:

Password:  Re-Enter Password:

Enable Password:

**User Information**

First Name:

Last Name:

**Account Options**

Description:

Change password on next login:

**Account Disable Policy**

Disable account if date exceeds  (yyyy-mm-dd)

**User Groups**

Etapa 8. Repita a etapa 6 para todos os usuários exigidos.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

**Network Access Users**

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input type="checkbox"/> Enabled	fxosaaa					FXOS AAA	
<input type="checkbox"/> Enabled	fxosadmin					FXOS ADMIN	
<input type="checkbox"/> Enabled	fxosoper					FXOS OPER	
<input type="checkbox"/> Enabled	fxosro					FXOS Read Only	

Criando o perfil da autorização para cada papel de usuário

Etapa 1. Navegue à política > aos elementos da política > aos resultados > à autorização > aos perfis da autorização.

**Standard Authorization Profiles**  
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Name	Profile	Description
Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices. Ensu
Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA port
NSP_Onboard	Cisco	Onboard the device with Native Supplicant Provisionir
Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
DenyAccess		Default Profile with access type as Access-Reject
PermitAccess		Default Profile with access type as Access-Accept

Etapa 2. Encha todos os atributos para o perfil da autorização.

### 2.1. Configurar o nome de perfil.

**Authorization Profile**

\* Name:

Description:

\* Access Type:

Network Device Profile:

### 2.2. Em ajustes avançados dos atributos configurar o seguinte CISCO-AV-PAIR

`cisco-av-pair=shell: roles= " admin"`

**Advanced Attributes Settings**

Cisco:cisco-av-pair = shell:roles="admin"

### 2.3. Click Save.

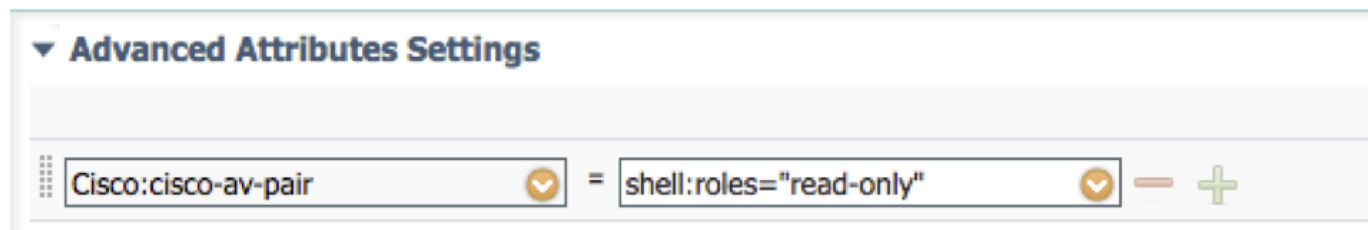
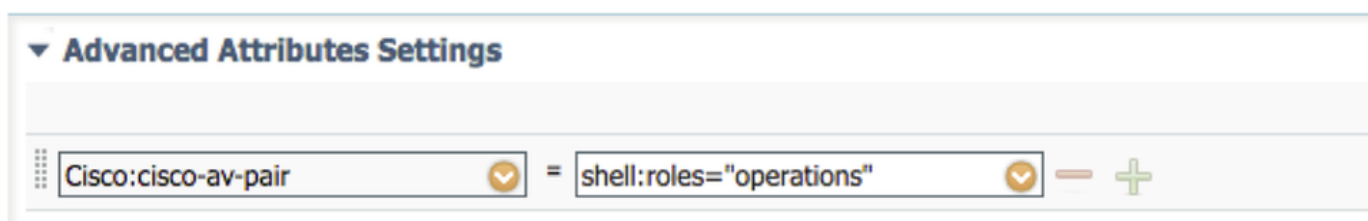
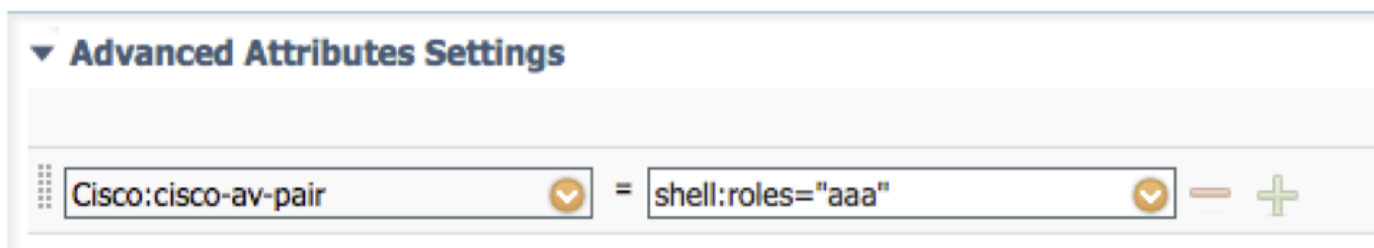
**Save** **Reset**

Etapa 3. Repita etapa 2 para os papéis de usuário restantes usando os seguintes pares Cisco AV

cisco-av-pair=shell: roles= " aaa"

cisco-av-pair=shell: roles= " operações"

cisco-av-pair=shell: roles= " de leitura apenas"



Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Authentication Authorization Profiling Posture Client Provisioning > Policy Elements

Dictionarys > Conditions > Results

### Standard Authorization Profiles

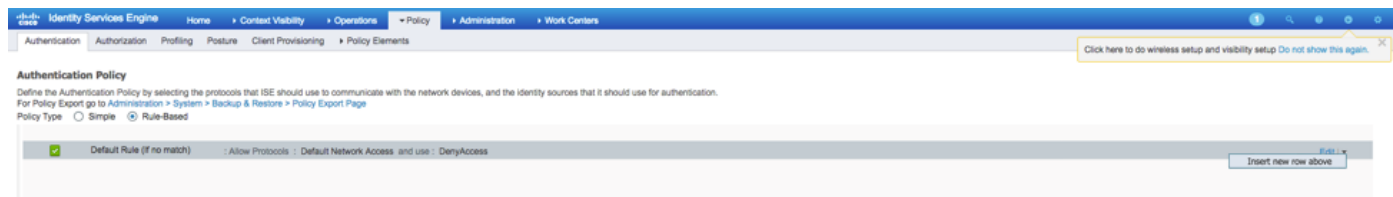
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Edit + Add Duplicate Delete

<input type="checkbox"/>	Name	Profile
<input type="checkbox"/>	Blackhole_Wireless_Access	Cisco ⊕
<input type="checkbox"/>	Cisco_IP_Phones	Cisco ⊕
<input type="checkbox"/>	Cisco_WebAuth	Cisco ⊕
<input type="checkbox"/>	FXOS-AAA-PROFILE	Cisco ⊕
<input type="checkbox"/>	FXOS-ADMIN-PROFILE	Cisco ⊕
<input type="checkbox"/>	FXOS-OPER-PROFILE	Cisco ⊕
<input type="checkbox"/>	FXOS-ReadOnly-PROFILE	Cisco ⊕

Criando a política de autenticação

Etapa 1. Navegue à **política > à autenticação >** e clique a seta ao lado de editam onde você quer criar a regra.



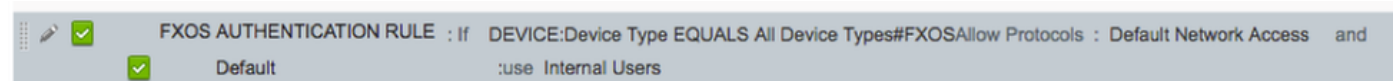
Etapa 2. A instalação é simples; pode ser mais granulada feito mas para este exemplo nós usaremos o tipo de dispositivo:

Nome: **REGRA DA AUTENTICAÇÃO FXO**

SE atributo/valor novos seletos: **Dispositivo: O tipo de dispositivo iguala todos os tipos de dispositivos #FXOS**

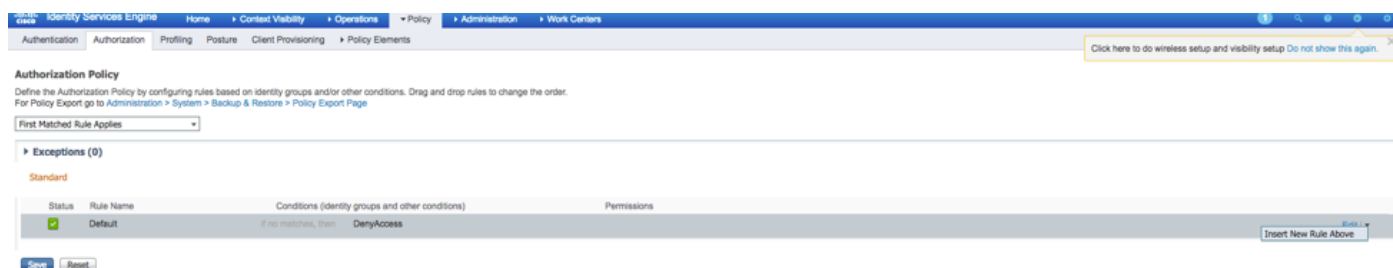
Permita protocolos: **Acesso de rede padrão**

Uso: **Usuários internos**



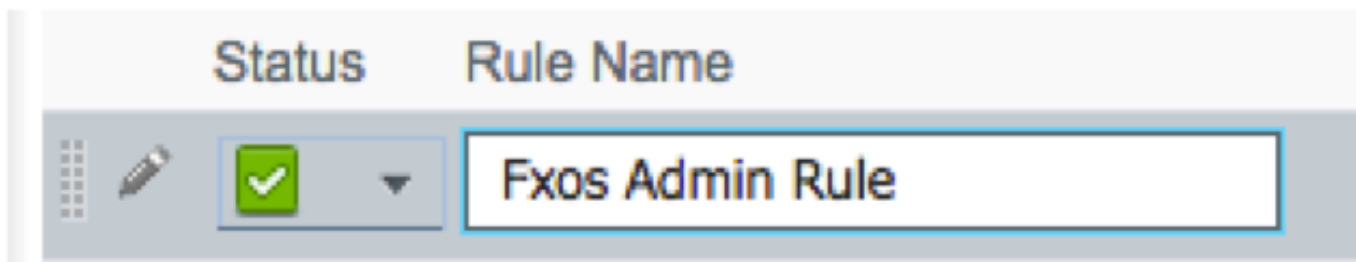
## Criando a política da autorização

Etapa 1. Navegue à **política > à autorização >** e clique a rede da seta para editar onde você quer criar a regra.

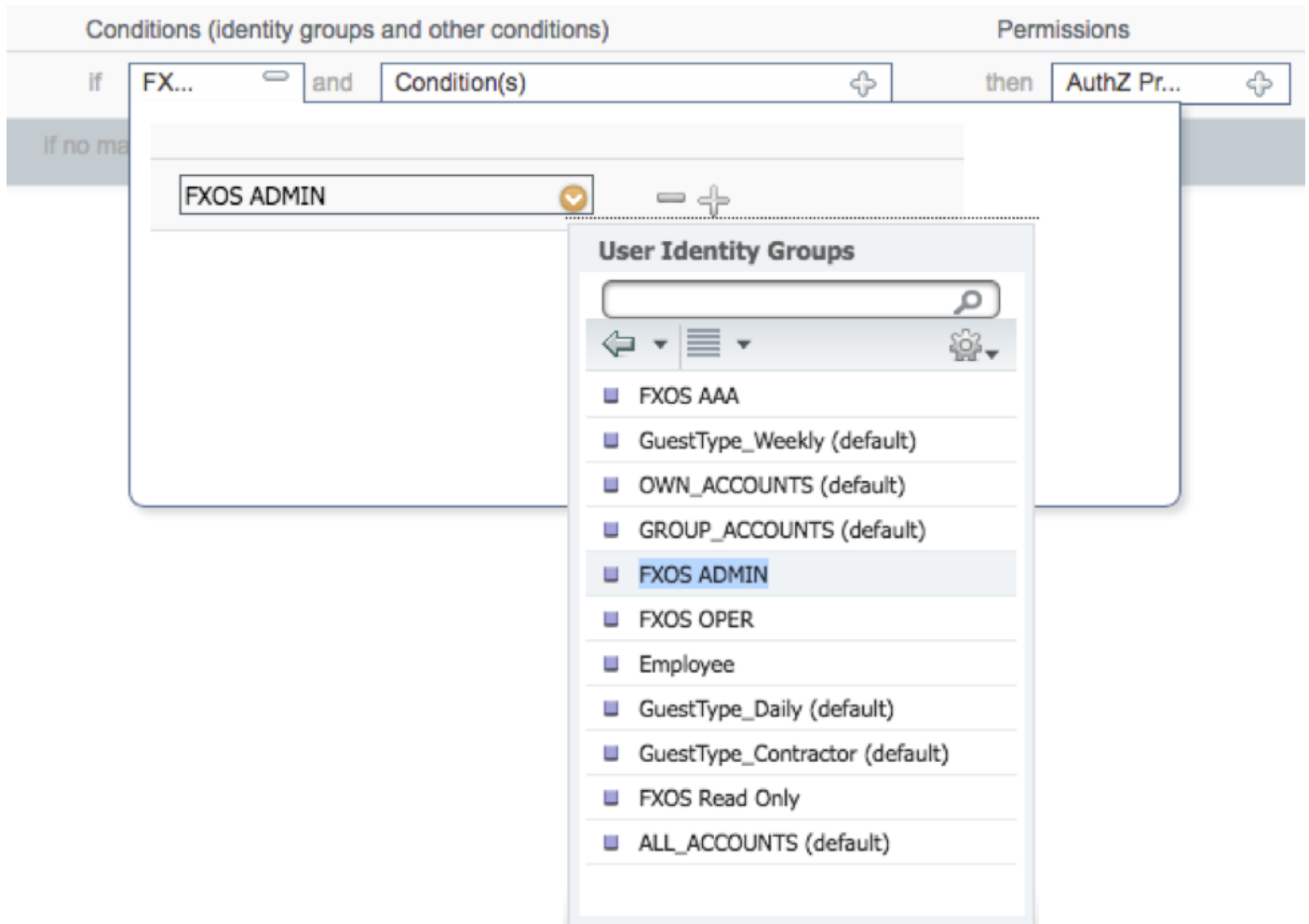


Etapa 2. Incorpore os valores para a regra da autorização com os parâmetros requerido.

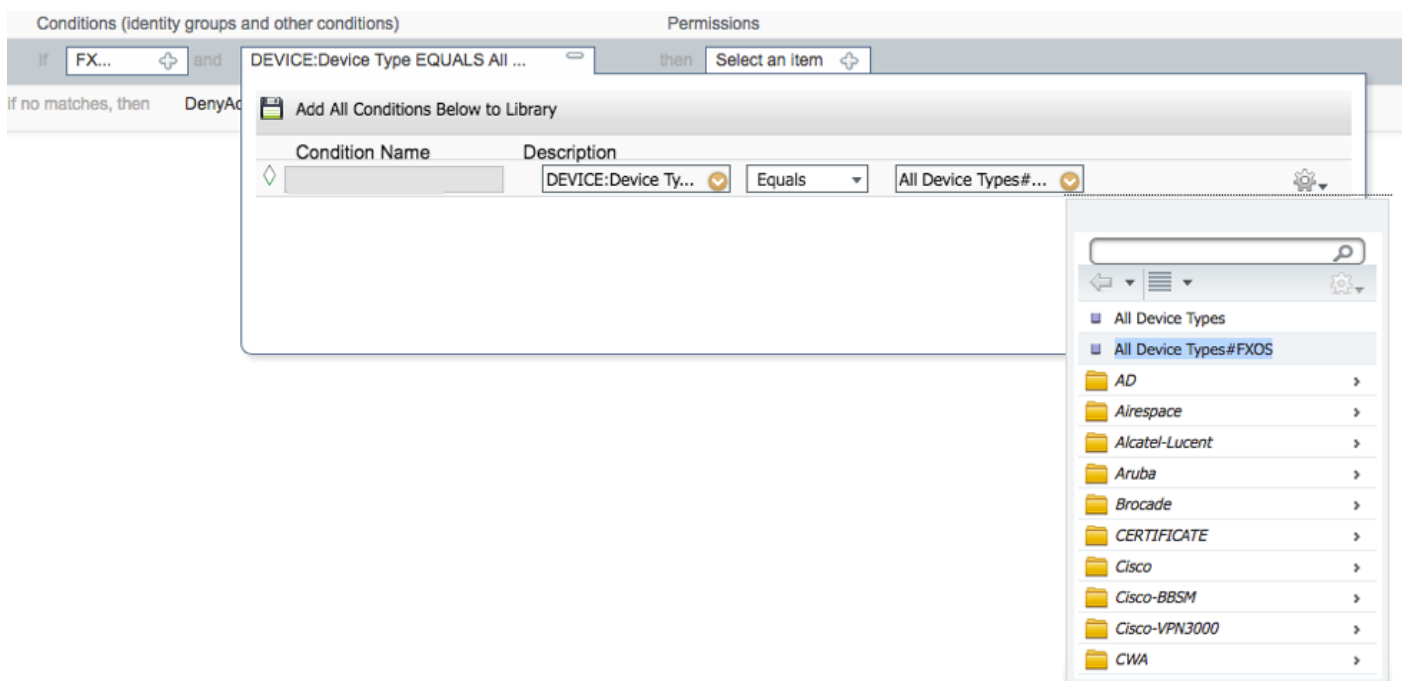
2.1. Nome da regra: **Regra de Fxos <USER ROLE>**.



2.2. Se: **Grupos da identidade do usuário > <USER seletor ROLE>**.



2.3. E: Crie a condição nova > o dispositivo: O tipo de dispositivo iguala todos os tipos de dispositivos #FXOS.



2.4. Permissões: O padrão > escolhe o papel de usuário do perfil

Permissions

then FXOS-A...

FXOS-ADMIN-PROFILE

**Standard**

- Blackhole\_Wireless\_Access
- Cisco\_IP\_Phones
- Cisco\_WebAuth
- DenyAccess
- FXOS-AAA-PROFILE
- FXOS-ADMIN-PROFILE**
- FXOS-OPER-PROFILE
- FXOS-ReadOnly-PROFILE
- NSP\_Onboard
- Non\_Cisco\_IP\_Phones
- PermitAccess

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Fxos Admin Rule	if <b>FXOS ADMIN</b> AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-ADMIN-PROFILE

Etapa 3. Repita etapa 2 para todos os papéis de usuário.

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Fxos Admin Rule	if <b>FXOS ADMIN</b> AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-ADMIN-PROFILE
<input checked="" type="checkbox"/>	Fxos AAA Rule	if <b>FXOS AAA</b> AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-AAA-PROFILE
<input checked="" type="checkbox"/>	Fxos Oper Rule	if <b>FXOS OPER</b> AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-OPER-PROFILE
<input checked="" type="checkbox"/>	Fxos Read only Rule	if <b>FXOS Read Only</b> AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-ReadOnly-PROFILE
<input checked="" type="checkbox"/>	Default	if no matches, then DenyAccess	

Etapa 4. **Salv guarda** do clique na parte inferior da página.

 Save Reset

## Verificar

Você pode agora testar cada usuário e verificar o papel de usuário atribuído.

### Verificação FXO Chasis

1. Telnet ou SSH ao chassi e ao início de uma sessão FXO usando alguns dos usuários criados no ISE.

Nome de usuário: fxosadmin

Senha:

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

fpr4120-TAC-A /security # **detalhe do usuário remoto da mostra**

**Fxosaaa do usuário remoto:**

Descrição:

Papéis de usuário:

Nome: **aaa**

Nome: **somente leitura**

**Fxosadmin do usuário remoto:**

Descrição:

Papéis de usuário:

Nome: **admin**

Nome: **somente leitura**

**Fxosoper do usuário remoto:**

Descrição:

Papéis de usuário:

Nome: **operações**

Nome: **somente leitura**

**Fxosro** do usuário remoto:

Descrição:

Papéis de usuário:

Nome: **somente leitura**

Segundo o username incorporado o chassi FXO o CLI indicará somente os comandos autorizados para o papel de usuário atribuído.

Papel de usuário admin.

fpr4120-TAC-A /security #?

reconheça reconhecem

as claro-USER-sessões cancelam sessões do usuário

crie criam objetos gerenciado

suprima de objetos gerenciado da supressão

serviços das inutilizações do desabilitação

permita permite serviços

entre incorpora um objeto gerenciado

o espaço muda o modo atual

ajuste valores do proprietário ajustados

mostre a informação de sistema da mostra

termine sessões do Active cimc

fpr4120-TAC-A# **conectam fxos**

fpr4120-TAC-A (fxos) # **debugam AAA-pedidos aaa**

fpr4120-TAC-A (fxos) #

Papel de usuário de leitura apenas.

fpr4120-TAC-A /security #?

o espaço muda o modo atual



ajuste valores do proprietário ajustados

mostre a informação de sistema da mostra

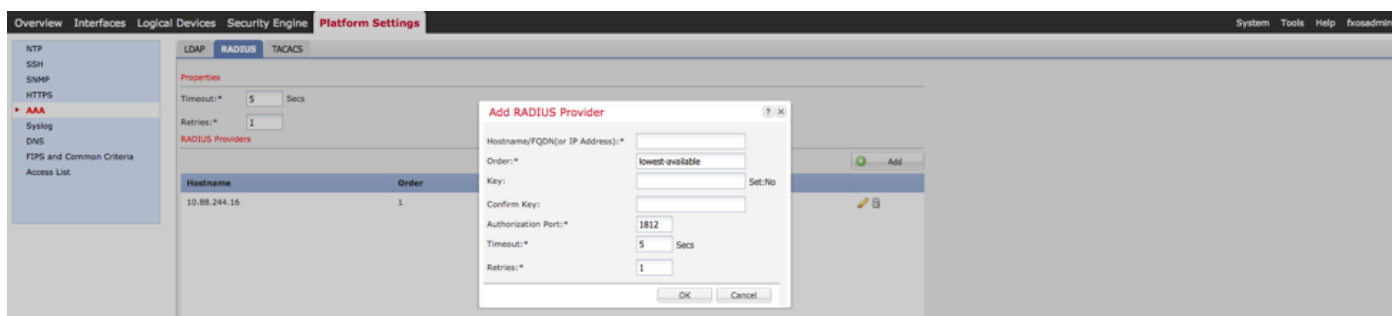
fpr4120-TAC-A# conectam fxos

fpr4120-TAC-A (fxos) # debugam AAA-pedidos aaa

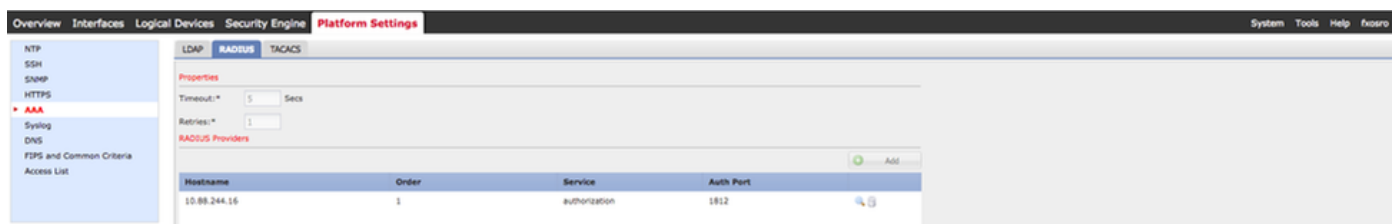
% da permissão negada para o papel

2. Consulte ao endereço IP de Um ou Mais Servidores Cisco ICM NT e ao início de uma sessão do chassi FXO usando alguns dos usuários criados no ISE.

Papel de usuário admin.



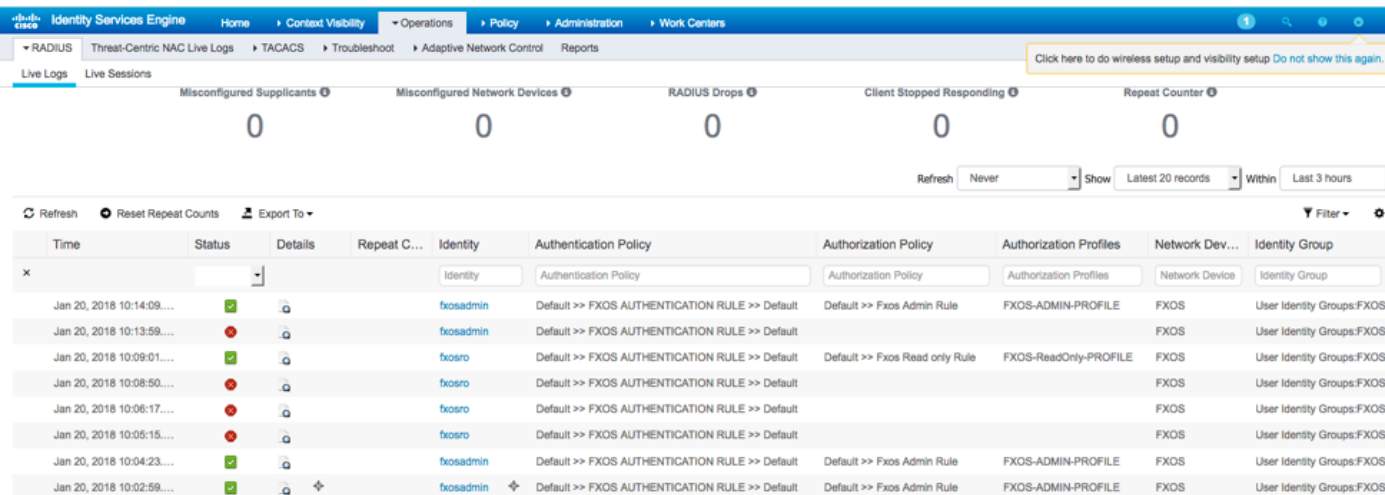
Papel de usuário de leitura apenas.



**Note:** Observe que o botão Add é desabilitada para fora.

## Verificação ISE 2.0

1. Navegue às operações > ao RAIIO > logs vivos. Você deve poder ver bem sucedido e falhas de tentativa.



# Troubleshooting

A fim debugar a autenticação de AAA e a autorização execute os comandos seguintes nos FXO CLI.

```
fpr4120-TAC-A# conectam fxos
```

```
fpr4120-TAC-A (fxos) # debugam AAA-pedidos aaa
```

```
fpr4120-TAC-A (fxos) # debugam o evento aaa
```

```
fpr4120-TAC-A (fxos) # debugam erros aaa
```

```
fpr4120-TAC-A (fxos) # termo segunda-feira
```

Depois que uma tentativa da autenticação bem sucedida, você considerará a seguinte saída.

```
2018 o 20 de janeiro 17:18:02.410275 aaa: aaa_req_process para a autenticação. sessão nenhum 0
```

```
2018 o 20 de janeiro 17:18:02.410297 aaa: aaa_req_process: Pedido geral AAA do appln: appln_subtype do início de uma sessão: padrão
```

```
2018 o 20 de janeiro 17:18:02.410310 aaa: try_next_aaa_method
```

```
2018 o 20 de janeiro 17:18:02.410330 aaa: os métodos totais configurados são 1, deslocamento predeterminado atual a ser tentado são 0
```

```
2018 o 20 de janeiro 17:18:02.410344 aaa: handle_req_using_method
```

```
2018 o 20 de janeiro 17:18:02.410356 aaa: AAA_METHOD_SERVER_GROUP
```

```
2018 o 20 de janeiro 17:18:02.410367 aaa: grupo = raio do aaa_sg_method_handler
```

```
2018 o 20 de janeiro 17:18:02.410379 aaa: Usando o sg_protocol que é passado a esta função
```

```
2018 o 20 de janeiro 17:18:02.410393 aaa: Enviando o pedido ao serviço de raio
```

```
2018 o 20 de janeiro 17:18:02.412944 aaa: mts_send_msg_to_prot_daemon: Comprimento de carga útil = 374
```

```
2018 o 20 de janeiro 17:18:02.412973 aaa: sessão: 0x8dfd68c adicionado à tabela 1 da sessão
```

```
2018 o 20 de janeiro 17:18:02.412987 aaa: Grupo configurado do método sucedido
```

```
2018 o 20 de janeiro 17:18:02.656425 aaa: aaa_process_fd_set
```

```
2018 o 20 de janeiro 17:18:02.656447 aaa: aaa_process_fd_set: mtscallback no aaa_q
```

```
2018 o 20 de janeiro 17:18:02.656470 aaa: mts_message_response_handler: uma resposta dos mts
```

2018 o 20 de janeiro 17:18:02.656483 aaa: prot\_daemon\_reponse\_handler

2018 o 20 de janeiro 17:18:02.656497 aaa: sessão: 0x8dfd68c removido da tabela 0 da sessão

2018 o 20 de janeiro 17:18:02.656512 aaa: estado dos is\_aaa\_resp\_status\_success = 1

2018 o 20 de janeiro 17:18:02.656525 aaa: os is\_aaa\_resp\_status\_success são VERDADEIROS

2018 o 20 de janeiro 17:18:02.656538 aaa: aaa\_send\_client\_response para a autenticação. session->flags=21. aaa\_resp->flags=0.

2018 o 20 de janeiro 17:18:02.656550 aaa: AAA\_REQ\_FLAG\_NORMAL

2018 o 20 de janeiro 17:18:02.656577 aaa: mts\_send\_response bem sucedido

2018 o 20 de janeiro 17:18:02.700520 aaa: aaa\_process\_fd\_set: mtscallback no aaa\_accounting\_q

2018 o 20 de janeiro 17:18:02.700688 aaa: OPCODE VELHO: accounting\_interim\_update

2018 o 20 de janeiro 17:18:02.700702 aaa: aaa\_create\_local\_acct\_req: user=, session\_id=, fxosro log=added do usuário

2018 o 20 de janeiro 17:18:02.700725 aaa: aaa\_req\_process para explicar. sessão nenhum 0

2018 o 20 de janeiro 17:18:02.700738 aaa: A referência do pedido MTS é NULA. Pedido LOCAL

2018 o 20 de janeiro 17:18:02.700749 aaa: Ajustando AAA\_REQ\_RESPONSE\_NOT\_NEEDED

2018 o 20 de janeiro 17:18:02.700762 aaa: aaa\_req\_process: Pedido geral AAA do appln: appln\_subtype do padrão: padrão

2018 o 20 de janeiro 17:18:02.700774 aaa: try\_next\_aaa\_method

2018 o 20 de janeiro 17:18:02.700798 aaa: nenhuns métodos configurados para o padrão do padrão

2018 o 20 de janeiro 17:18:02.700810 aaa: nenhuma configuração disponível para esta pedido

2018 o 20 de janeiro 17:18:02.700997 aaa: aaa\_send\_client\_response para explicar. session->flags=254. aaa\_resp->flags=0.

2018 o 20 de janeiro 17:18:02.701010 aaa: a resposta para o pedido explicando da biblioteca velha será enviada como o SUCESSO

2018 o 20 de janeiro 17:18:02.701021 aaa: resposta não necessária para este pedido

2018 o 20 de janeiro 17:18:02.701033 aaa: AAA\_REQ\_FLAG\_LOCAL\_RESP

2018 o 20 de janeiro 17:18:02.701044 aaa: aaa\_cleanup\_session

2018 o 20 de janeiro 17:18:02.701055 aaa: o aaa\_req deve ser livrado.

2018 o 20 de janeiro 17:18:02.701067 aaa: Recuar o local do método sucedido

2018 o 20 de janeiro 17:18:02.706922 aaa: aaa\_process\_fd\_set

2018 o 20 de janeiro 17:18:02.706937 aaa: aaa\_process\_fd\_set: mtscallback no  
aaa\_accounting\_q

2018 o 20 de janeiro 17:18:02.706959 aaa: OPPOSITE VELHO: accounting\_interim\_update

2018 o 20 de janeiro 17:18:02.706972 aaa: aaa\_create\_local\_acct\_req: user=, session\_id=,  
usuário log=added: fxosro ao papel: somente leitura

Depois que uma tentativa da autenticação falha, você considerará a seguinte saída.

2018 o 20 de janeiro 17:15:18.102130 aaa: aaa\_process\_fd\_set

2018 o 20 de janeiro 17:15:18.102149 aaa: aaa\_process\_fd\_set: mtscallback no aaa\_q

2018 o 20 de janeiro 17:15:18.102267 aaa: aaa\_process\_fd\_set

2018 o 20 de janeiro 17:15:18.102281 aaa: aaa\_process\_fd\_set: mtscallback no aaa\_q

2018 o 20 de janeiro 17:15:18.102363 aaa: aaa\_process\_fd\_set

2018 o 20 de janeiro 17:15:18.102377 aaa: aaa\_process\_fd\_set: mtscallback no aaa\_q

2018 o 20 de janeiro 17:15:18.102456 aaa: aaa\_process\_fd\_set

2018 o 20 de janeiro 17:15:18.102468 aaa: aaa\_process\_fd\_set: mtscallback no aaa\_q

2018 o 20 de janeiro 17:15:18.102489 aaa: mts\_aaa\_req\_process

2018 o 20 de janeiro 17:15:18.102503 aaa: aaa\_req\_process para a autenticação. sessão  
nenhum 0

2018 o 20 de janeiro 17:15:18.102526 aaa: aaa\_req\_process: Pedido geral AAA do appln:  
appln\_subtype do início de uma sessão: padrão

2018 o 20 de janeiro 17:15:18.102540 aaa: try\_next\_aaa\_method

2018 o 20 de janeiro 17:15:18.102562 aaa: os métodos totais configurados são 1, deslocamento  
predeterminado atual a ser tentado são 0

2018 o 20 de janeiro 17:15:18.102575 aaa: handle\_req\_using\_method

2018 o 20 de janeiro 17:15:18.102586 aaa: AAA\_METHOD\_SERVER\_GROUP

2018 o 20 de janeiro 17:15:18.102598 aaa: grupo = raio do aaa\_sg\_method\_handler

2018 o 20 de janeiro 17:15:18.102610 aaa: Usando o sg\_protocol que é passado a esta função

2018 o 20 de janeiro 17:15:18.102625 aaa: Enviando o pedido ao serviço de raio

2018 o 20 de janeiro 17:15:18.102658 aaa: mts\_send\_msg\_to\_prot\_daemon: Comprimento de carga útil = 371

2018 o 20 de janeiro 17:15:18.102684 aaa: sessão: 0x8dfd68c adicionado à tabela 1 da sessão

2018 o 20 de janeiro 17:15:18.102698 aaa: Grupo configurado do método sucedido

2018 o 20 de janeiro 17:15:18.273682 aaa: aaa\_process\_fd\_set

2018 o 20 de janeiro 17:15:18.273724 aaa: aaa\_process\_fd\_set: mtscallback no aaa\_q

2018 o 20 de janeiro 17:15:18.273753 aaa: mts\_message\_response\_handler: uma resposta dos mts

2018 o 20 de janeiro 17:15:18.273768 aaa: prot\_daemon\_reponse\_handler

2018 o 20 de janeiro 17:15:18.273783 aaa: sessão: 0x8dfd68c removido da tabela 0 da sessão

2018 o 20 de janeiro 17:15:18.273801 aaa: estado dos is\_aaa\_resp\_status\_success = 2

2018 o 20 de janeiro 17:15:18.273815 aaa: os is\_aaa\_resp\_status\_success são VERDADEIROS

2018 o 20 de janeiro 17:15:18.273829 aaa: aaa\_send\_client\_response para a autenticação. session->flags=21. aaa\_resp->flags=0.

2018 o 20 de janeiro 17:15:18.273843 aaa: AAA\_REQ\_FLAG\_NORMAL

2018 o 20 de janeiro 17:15:18.273877 aaa: mts\_send\_response bem sucedido

2018 o 20 de janeiro 17:15:18.273902 aaa: aaa\_cleanup\_session

2018 o 20 de janeiro 17:15:18.273916 aaa: mts\_drop de msg do pedido

2018 o 20 de janeiro 17:15:18.273935 aaa: o aaa\_req deve ser livrado.

2018 o 20 de janeiro 17:15:18.280416 aaa: aaa\_process\_fd\_set

2018 o 20 de janeiro 17:15:18.280443 aaa: aaa\_process\_fd\_set: mtscallback no aaa\_q

2018 o 20 de janeiro 17:15:18.280454 aaa: aaa\_enable\_info\_config: GET\_REQ para o Mensagem de Erro do início de uma sessão aaa

2018 o 20 de janeiro 17:15:18.280460 aaa: recebido de volta o valor do retorno da operação da configuração: artigo desconhecido da Segurança

## Informações Relacionadas

O comando de Ethanalyzer em FX-OS CLI alertará para a senha para uma senha quando a autenticação TACACS/RADIUS é permitida. Este comportamento é causado por um erro.

Bug ID: [CSCvg87518](#)