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

Índice

Introdução

Este documento descreve como configurar a autenticação TACACS+ 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 Remirez, 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

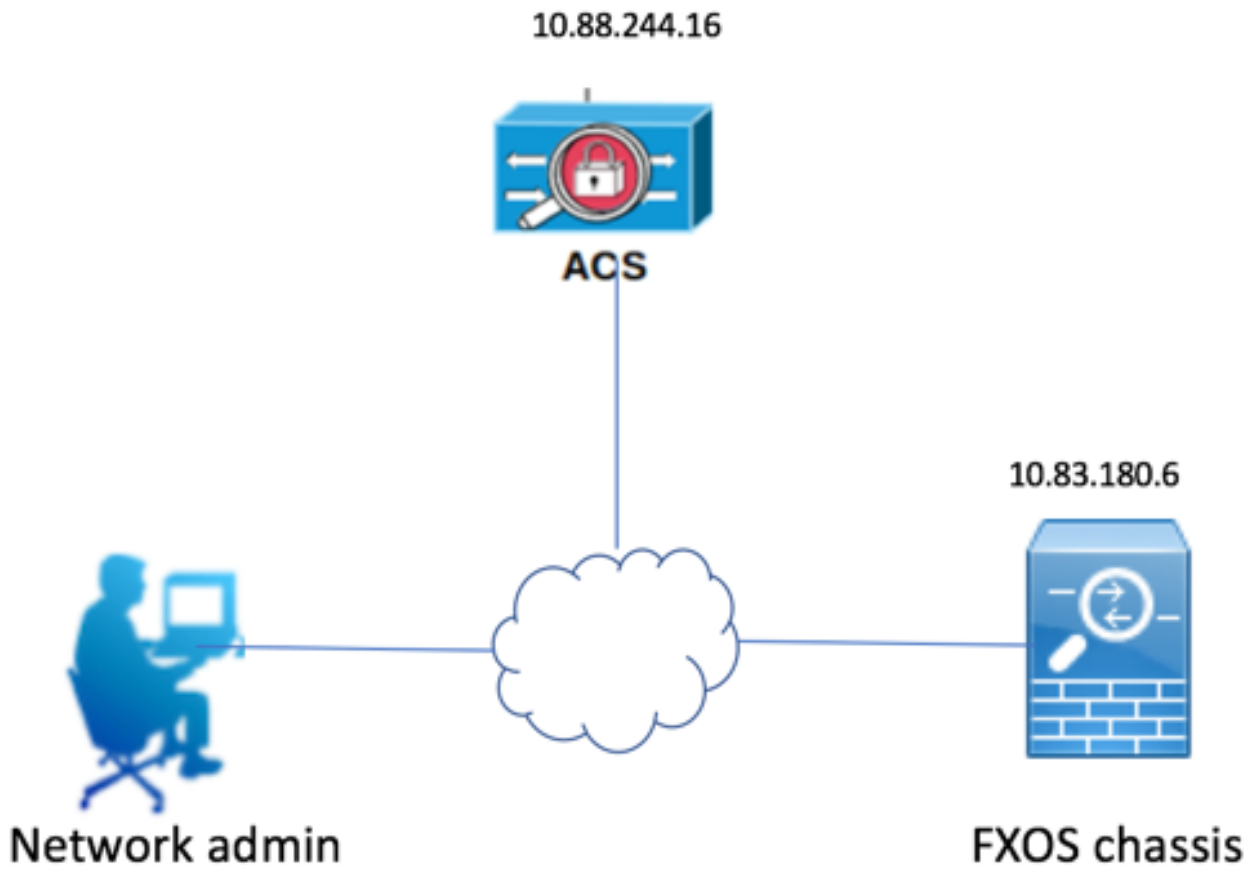
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer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



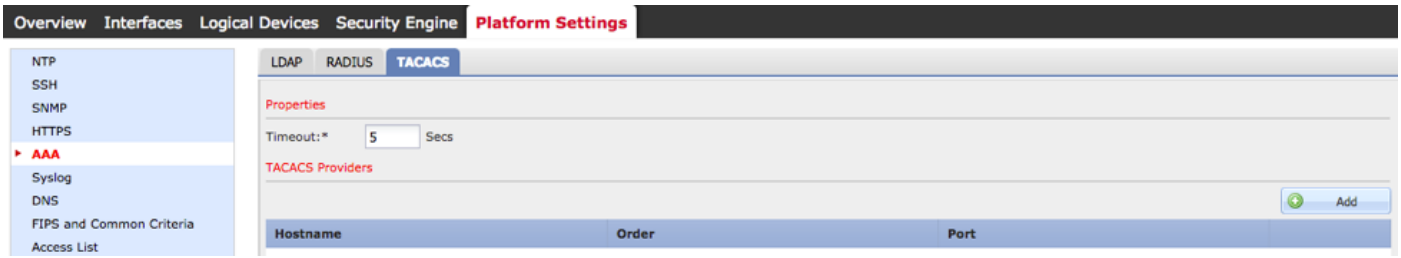
Configurações

Configurando o chassi FXO

Criando um fornecedor TACACS que usa o gerente do chassi

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

Etapa 2. Clique a aba **TACACS**.

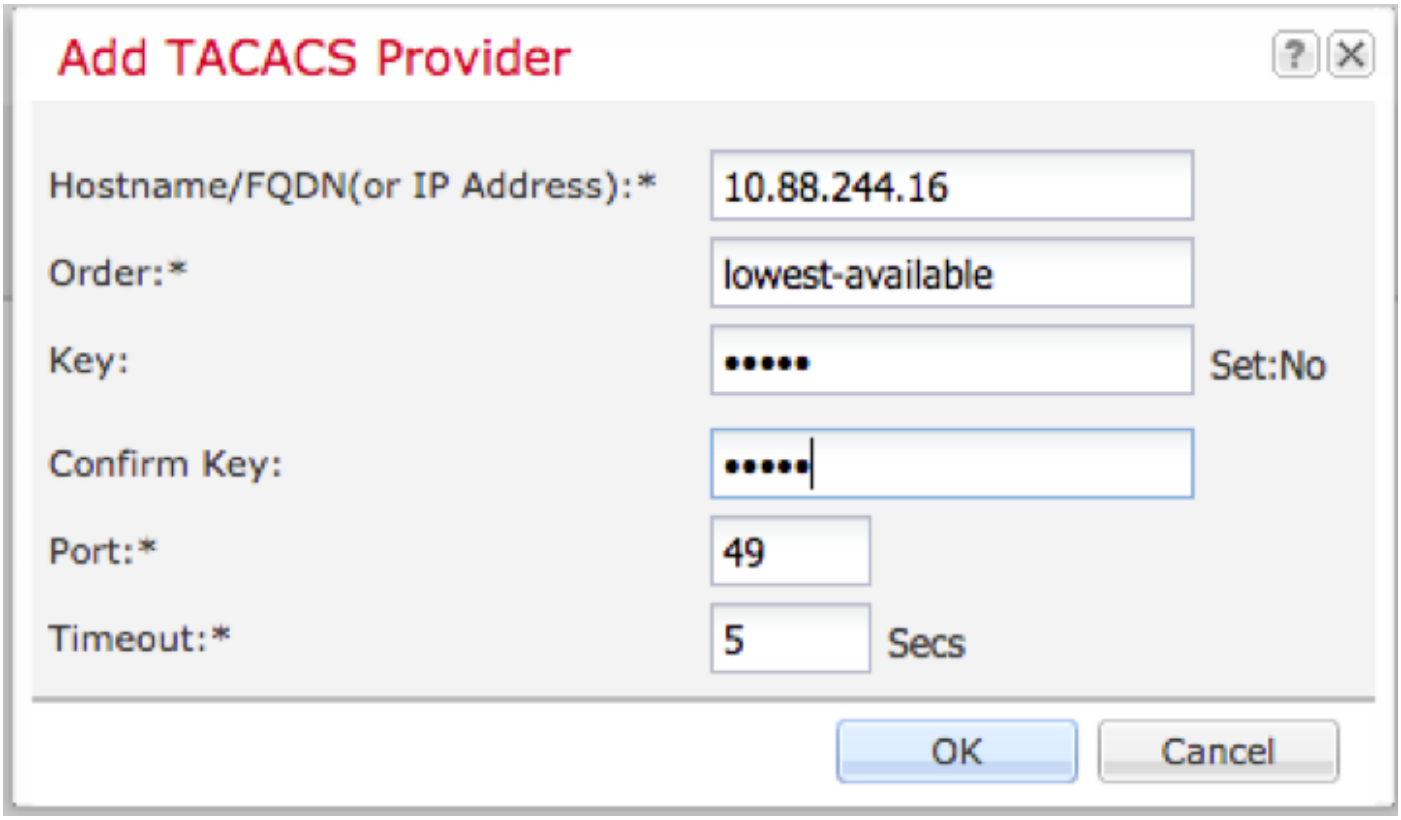


Etapa 3. Para cada fornecedor TACACS+ que você quer adicionar (até 16 fornecedores).

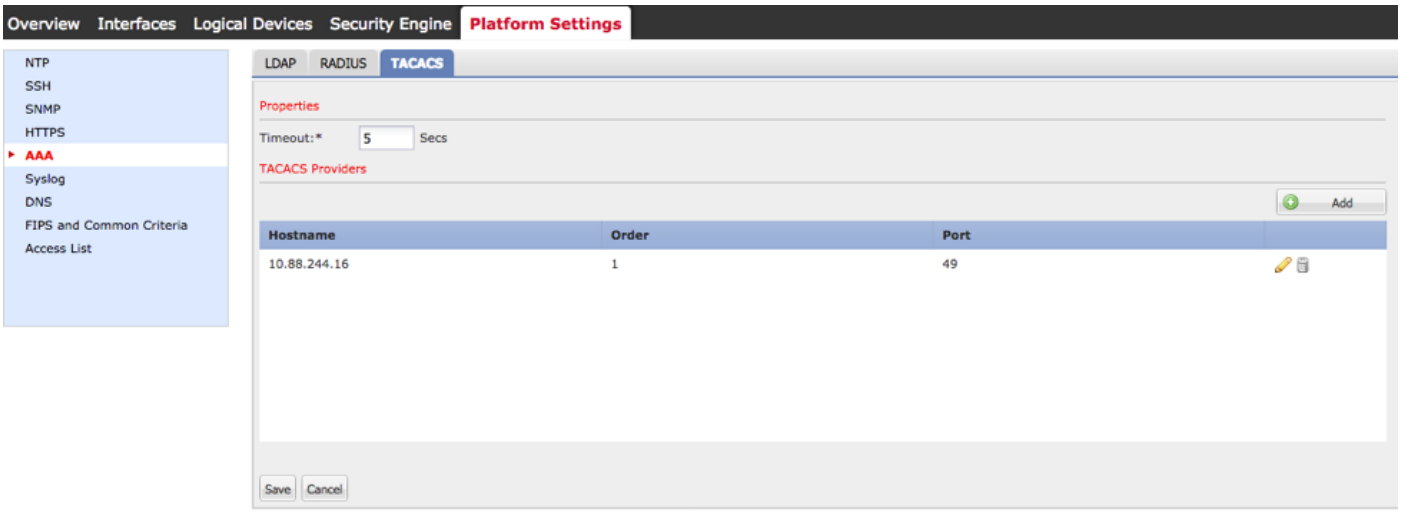
3.1. Na área dos fornecedores TACACS, o clique **adiciona.**

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

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

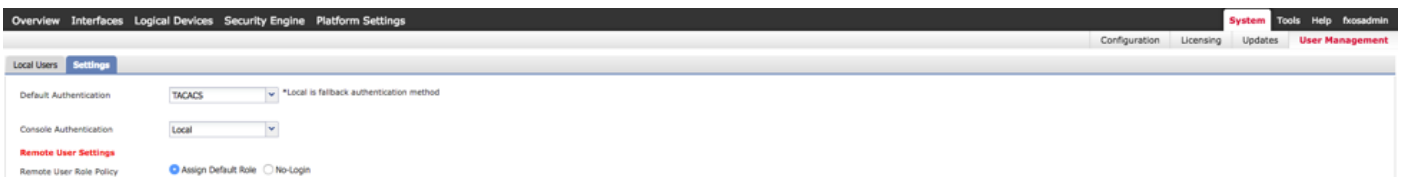


Etapa 4. **Salvaguarda do** clique.



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

Etapa 6. Sob a autenticação padrão escolha o **TACACS**.



Criando um fornecedor TACACS+ que usa o CLI

Etapa 1. A fim permitir a autenticação TACACS 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 tacacs 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: **Tacacs**

Reino operacional: **Tacacs**

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 de TACACS execute os comandos seguintes.

Segurança do espaço fpr4120-TAC-A#

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

fpr4120-TAC-A /security/tacacs # **entram no server 10.88.244.50**

fpr4120-TAC-A /security/tacacs/server # **ajustou o descr "servidor ACS"**

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

Server TACACS+:

Hostname, FQDN ou endereço IP de Um ou Mais Servidores Cisco ICM NT: 10.88.244.50

Descr:

Ordem: 1

Porta: 49

Chave: ****

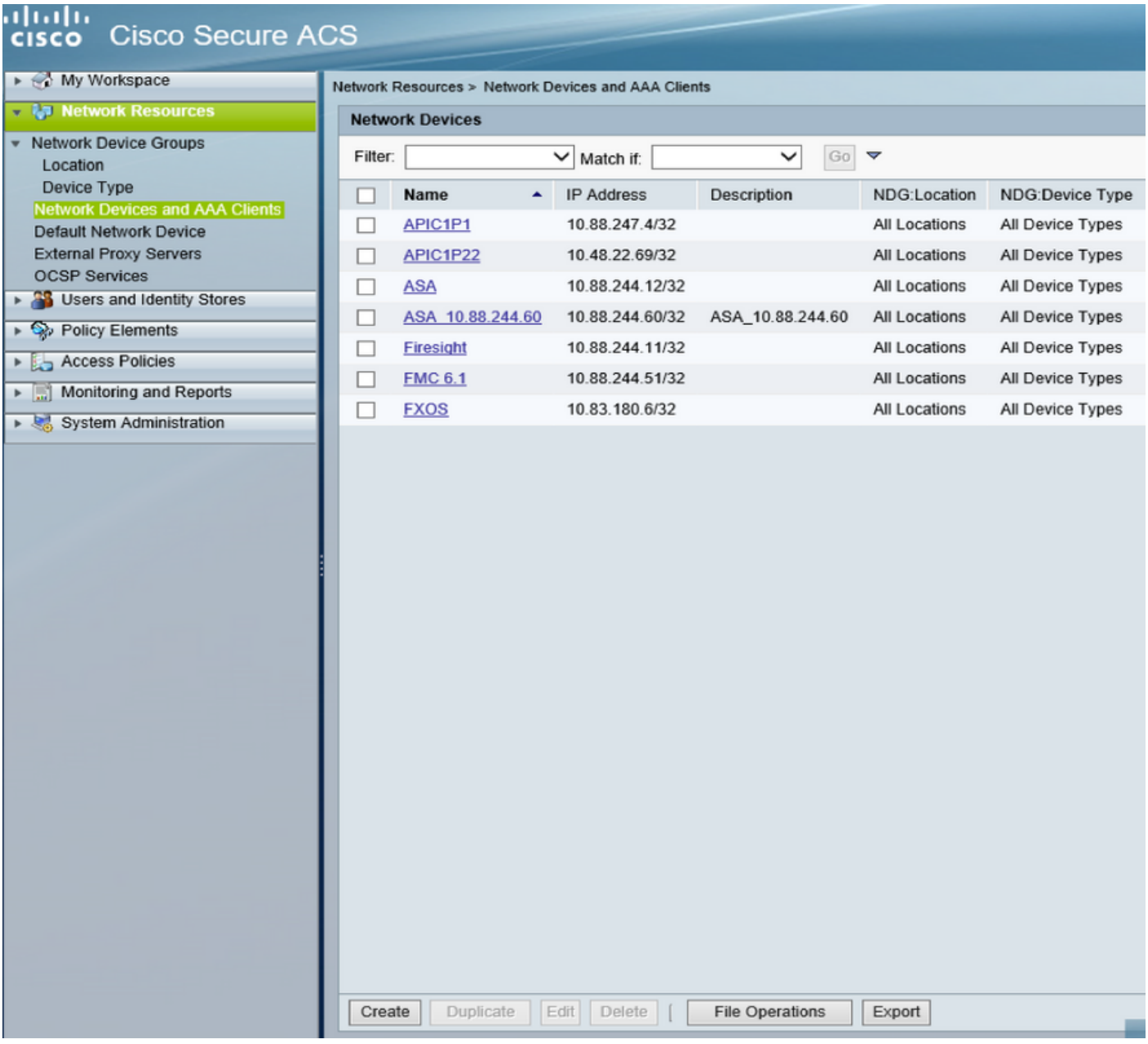
Intervalo: 5

Configurando o servidor ACS

Adicionando os FXO como uns recursos de rede

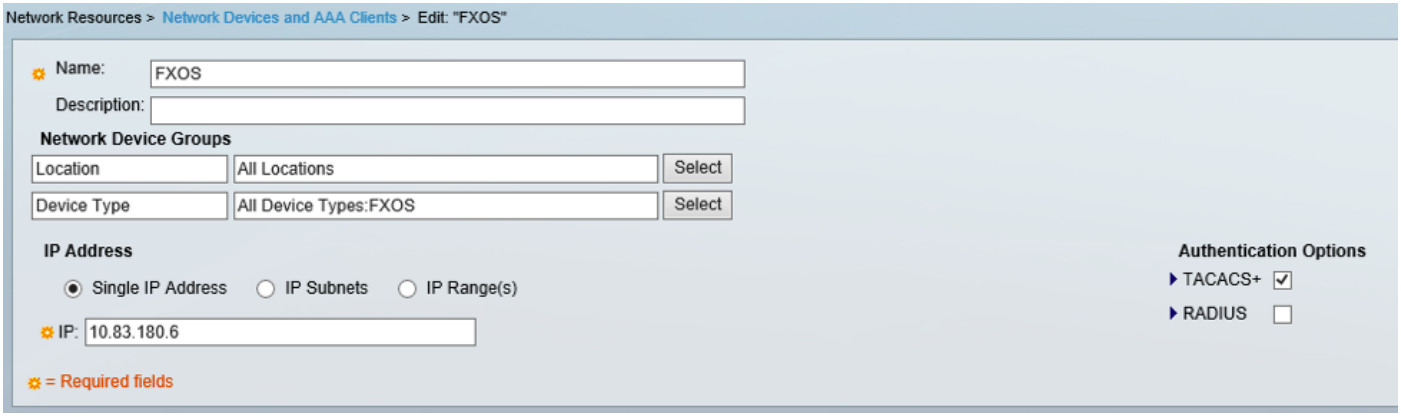
Etapa 1. Navegue aos **recursos de rede > aos dispositivos de rede e aos clientes de AAA**.

Etapa 2. O clique **cria.**



Etapa 3. Incorpore os valores exigidos (o nome, endereço IP de Um ou Mais Servidores Cisco

ICM NT, tipo de dispositivo e permite o TACACS+ e adiciona a CHAVE).



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