

Sistema operacional Firepower eXtensible (FXOS) 2.2: Autenticação e autorização do chassi para gerenciamento remoto com ACS usando TACACS+.

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configurando o chassi FXOS](#)

[Configurando o servidor ACS](#)

[Verificar](#)

[Verificação do chassi FXOS](#)

[Verificação ACS](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como configurar a autenticação e a autorização TACACS+ para o chassi do Firepower eXtensible Operating System (FXOS) através do Access Control Server (ACS).

O chassi FXOS inclui as seguintes funções de usuário:

- Administrador - Acesso completo de leitura e gravação a todo o sistema. A conta admin padrão recebe essa função por padrão e não pode ser alterada.
- Somente leitura - Acesso somente leitura à configuração do sistema sem privilégios para modificar o estado do sistema.
- Operações - Acesso de leitura e gravação à configuração do NTP, configuração do Smart Call Home para Smart Licensing e registros do sistema, incluindo servidores de syslog e falhas. Leia o acesso ao restante do sistema.
- AAA - acesso de leitura e gravação a usuários, funções e configuração de AAA. Leia o acesso ao restante do sistema.

Através da CLI, isso pode ser visto da seguinte maneira:

```
fpr4120-TAC-A /security* # show role
```

Função:

Nome da função Priv

—

aaa aaa

admin admin

operações operacionais

somente leitura

Contribuído por Tony Ramirez, José Soto, engenheiros do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento do Firepower eXtensible Operating System (FXOS)
- Conhecimento da configuração do ACS

Componentes Utilizados

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

- Cisco Firepower 4120 Security Appliance versão 2.2
- Virtual Cisco Access Control Server versão 5.8.0.32

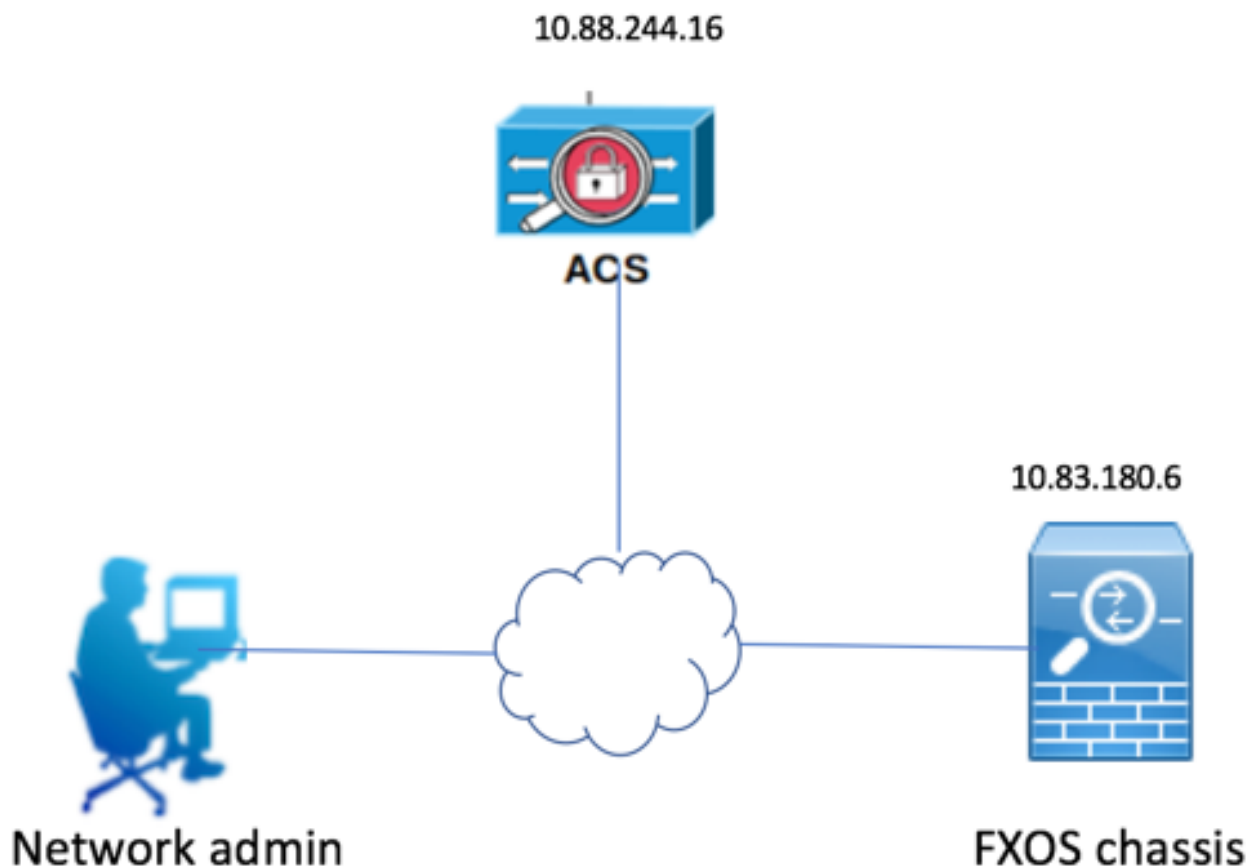
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

O objetivo da configuração é:

- Autentique os usuários que fazem login na GUI baseada na Web e no SSH do FXOS por meio do ACS.
- Autorize os usuários a fazer login na GUI baseada na Web e no SSH do FXOS de acordo com sua respectiva função de usuário por meio do ACS.
- Verifique o funcionamento correto da autenticação e autorização no FXOS por meio do ACS.

Diagrama de Rede



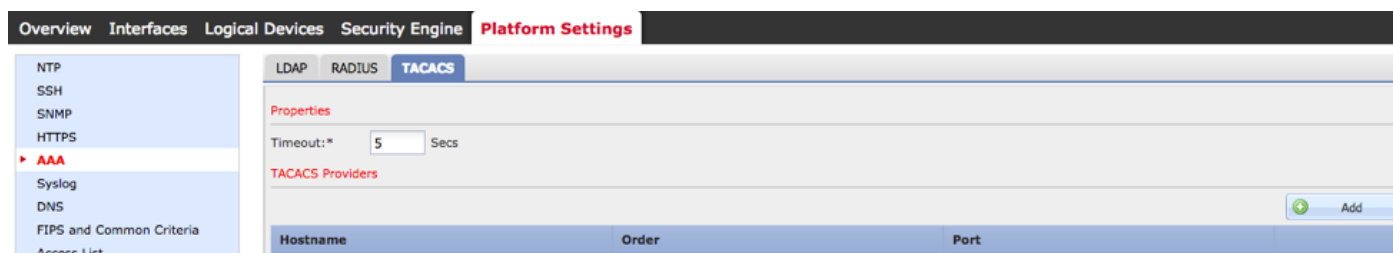
Configurações

Configurando o chassi FXOS

Criando um provedor TACACS usando o chassi Manager

Etapa 1. Navegue até Configurações da plataforma > AAA.

Etapa 2. Clique na guia TACACS.



Etapa 3. Para cada provedor TACACS+ que você deseja adicionar (até 16 provedores).

- 3.1. Na área TACACS Providers (Provedores de TACACS), clique em **Add (Adicionar)**.
- 3.2. Na caixa de diálogo Adicionar provedor TACACS, insira os valores necessários.
- 3.3. Clique em **OK** para fechar a caixa de diálogo Adicionar Provedor TACACS.

Add TACACS Provider

Hostname/FQDN(or IP Address):*

Order:*

Key: Set: No

Confirm Key:

Port:*

Timeout:* Secs

Etapa 4. Click **Save**.

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

TACACS Providers

Hostname	Order	Port
10.88.244.16	1	49

Etapa 5. Navegue até **System > User Management > Settings**.

Etapa 6. Em Autenticação padrão, escolha **TACACS**.

Overview Interfaces Logical Devices Security Engine Platform Settings **System** Tools Help frosadmin

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 provedor TACACS+ usando CLI

Etapa 1. Para habilitar a autenticação TACACS, execute os seguintes comandos.

segurança de escopo fpr4120-TAC-A#

fpr4120-TAC-A /security # **scope default-auth**

fpr4120-TAC-A /security/default-auth # **set realm tacacs**

Etapa 2. Use o comando **show detail** para exibir os resultados.

fpr4120-TAC-A /security/default-auth # **show detail**

Autenticação padrão:

Domínio administrativo: **TACACS**

Domínio operacional: **TACACS**

Período de atualização da sessão da Web (em segundos): 600

Tempo limite da sessão (em segundos) para sessões web, ssh, telnet: 600

Tempo limite da sessão absoluta (em segundos) para sessões web, ssh, telnet: 3600

Tempo limite da sessão do console serial (em segundos): 600

Tempo limite da sessão absoluta do console serial (em segundos): 3600

Grupo de servidores de Autenticação do Administrador:

Grupo de servidores de Autenticação Operacional:

Uso do segundo fator: No

Etapa 3. Para configurar os parâmetros do servidor TACACS, execute os seguintes comandos.

segurança de escopo fpr4120-TAC-A#

fpr4120-TAC-A /segurança # **táticas de escopo**

fpr4120-TAC-A /security/tacacs # **entre no servidor 10.88.244.50**

fpr4120-TAC-A /security/tacacs/server # **set descr "Servidor ACS"**

fpr4120-TAC-A /security/tacacs/server* # **set key**

Digite a chave: *********

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

Etapa 4. Use o comando **show detail** para exibir os resultados.

fpr4120-TAC-A /security/tacacs/server* # **show detail**

Servidor TACACS+:

Nome do host, FQDN ou endereço IP: 10.88.244.50

Descr:

Pedido: 1

Porta: 49

Chave: ****

tempo limite: 5

Configurando o servidor ACS

Adicionando o FXOS como um recurso de rede

Etapa 1. Navegue até **Network Resources > Network Devices and AAA Clients**.

Etapa 2. Clique em **Criar**.

The screenshot shows the Cisco Secure ACS web interface. The left sidebar contains a navigation menu with the following items: My Workspace, Network Resources (expanded), Network Device Groups, Location, Device Type, Network Devices and AAA Clients (highlighted), Default Network Device, External Proxy Servers, OSCP Services, Users and Identity Stores, Policy Elements, Access Policies, Monitoring and Reports, and System Administration. The main content area is titled 'Network Resources > Network Devices and AAA Clients' and displays a table of 'Network Devices'. The table has the following columns: Name, IP Address, Description, NDG:Location, and NDG:Device Type. The table contains the following data:

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

At the bottom of the interface, there are buttons for 'Create', 'Duplicate', 'Edit', 'Delete', 'File Operations', and 'Export'.

Etapa 3. Insira os valores necessários (Nome, Endereço IP, Tipo de dispositivo e Habilitar

TACACS+ e adicione a CHAVE).

Network Resources > Network Devices and AAA Clients > Edit: "FXOS"

Description:

Network Device Groups

Location

Device Type

IP Address

Single IP Address IP Subnets IP Range(s)

Authentication Options

TACACS+ RADIUS

= Required fields

Etapa 4. Clique em Submit.

