

# Sistema operativo ampliable FirePOWER (FXOS) 2.2: Autenticación y autorización de chasis para administración remota con ACS mediante RADIUS

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuración del chasis FXOS](#)

[Configuración del servidor ACS](#)

[Verificación](#)

[Verificación del chasis FXOS](#)

[Verificación de ACS](#)

[Troubleshoot](#)

[Información Relacionada](#)

## Introducción

Este documento describe cómo configurar la autenticación y autorización RADIUS para el chasis del sistema operativo ampliable Firepower (FXOS) a través de Access Control Server (ACS).

El chasis FXOS incluye las siguientes funciones de usuario:

- Administrador: complete el acceso de lectura y escritura a todo el sistema. La cuenta de administrador predeterminada tiene asignada esta función de forma predeterminada y no se puede cambiar.
- Sólo lectura: acceso de sólo lectura a la configuración del sistema sin privilegios para modificar el estado del sistema.
- Operaciones: acceso de lectura y escritura a la configuración de NTP, configuración de Smart Call Home para Smart Licensing y registros del sistema, incluidos los servidores y fallos de syslog. Lea el acceso al resto del sistema.
- AAA: acceso de lectura y escritura a usuarios, funciones y configuración AAA. Lea el acceso al resto del sistema.

A través de CLI, esto puede verse de la siguiente manera:

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

Función:

Nombre de rol Priv

— —

aaa aaa

admin

operaciones

sólo lectura

Colaborado por Tony Ramirez, Jose Soto, Ingenieros del TAC de Cisco.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de Firepower eXtensible Operating System (FXOS)
- Conocimiento de la configuración ACS

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Firepower 4120 Security Appliance versión 2.2
- Cisco Access Control Server virtual versión 5.8.0.32

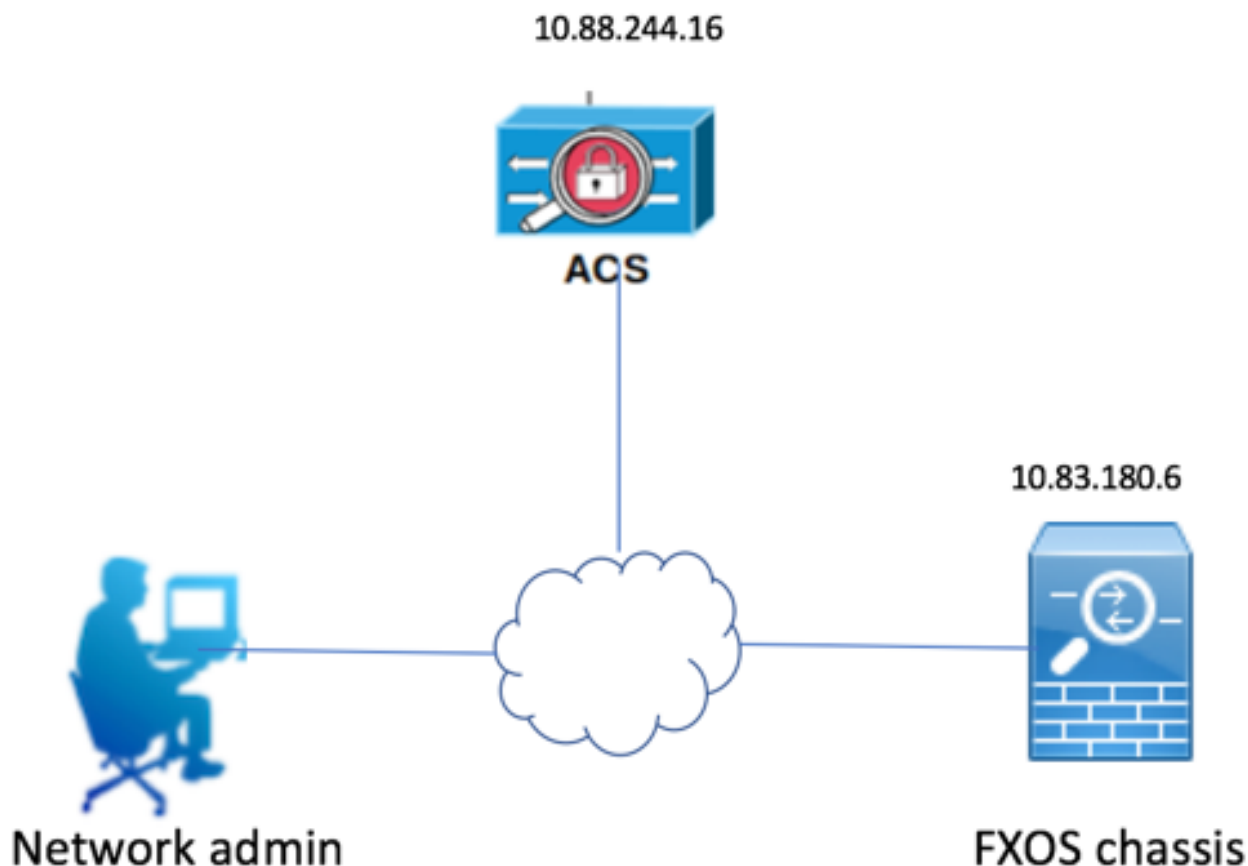
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Configurar

El objetivo de la configuración es:

- Autentique a los usuarios que inician sesión en la GUI basada en Web y SSH de FXOS mediante ACS.
- Autorice a los usuarios a iniciar sesión en la GUI basada en Web y SSH de FXOS según su respectivo rol de usuario mediante ACS.
- Verifique el correcto funcionamiento de la autenticación y autorización en el FXOS mediante ACS.

### Diagrama de la red



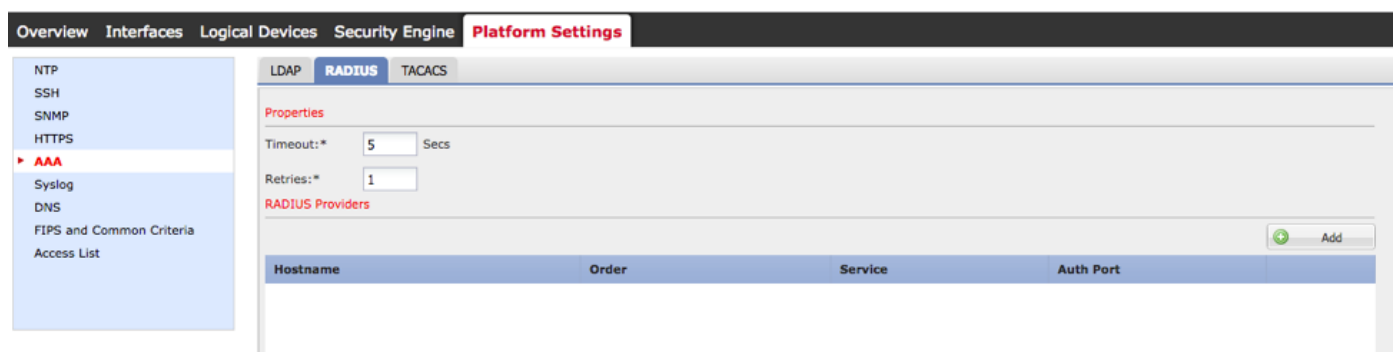
## Configuraciones

### Configuración del chasis FXOS

#### Creación de un Proveedor RADIUS con el Administrador de Chasis

Paso 1. Vaya a **Configuración de plataforma > AAA**.

Paso 2. Haga clic en la pestaña **RADIUS**.



Paso 3. Para cada proveedor RADIUS que desee agregar (hasta 16 proveedores).

3.1. En el área Proveedores RADIUS, haga clic en **Agregar**.

3.2. En el cuadro de diálogo Agregar proveedor RADIUS, introduzca los valores necesarios.

3.3. Haga clic en **Aceptar** para cerrar el cuadro de diálogo Agregar proveedor RADIUS.

**Add RADIUS Provider**

Hostname/FQDN(or IP Address):\* 10.88.244.16

Order:\* lowest-available

Key: ..... Set:No

Confirm Key: .....

Authorization Port:\* 1812

Timeout:\* 5 Secs

Retries:\* 1

OK Cancel

Paso 4. Click **Save**.

Overview Interfaces Logical Devices Security Engine **Platform Settings**

LDAP **RADIUS** TACACS

Properties

Timeout:\* 5 Secs

Retries:\* 1

RADIUS Providers

Hostname	Order	Service	Auth Port
10.88.244.16	1	authorization	1812

Save Cancel

Paso 5. Vaya a **System > User Management > Settings**.

Paso 6. En Default Authentication (Autenticación predeterminada), elija **RADIUS**.

Overview Interfaces Logical Devices Security Engine Platform Settings

Configuration Licensing Updates **User Management**

Local Users **Settings**

Default Authentication: RADIUS \*Local is fallback authentication method

Console Authentication: Local

Remote User Settings

Remote User Role Policy:  Assign Default Role  No-Login

## Creación de un Proveedor RADIUS con CLI

Paso 1. Para habilitar la autenticación RADIUS, ejecute los siguientes comandos.

```
seguridad de alcance fpr4120-TAC-A#
```

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

```
fpr4120-TAC-A /security/default-auth # set realm radius
```

Paso 2. Utilice el comando **show detail** para mostrar los resultados.

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

Autenticación predeterminada:

Rango de administración: **Radius**

Rango operativo: **Radius**

Período de actualización de la sesión web(en segundos): 600

Tiempo de espera de sesión(en segundos) para sesiones web, ssh, telnet: 600

Tiempo de espera de sesión absoluto(en segundos) para sesiones web, ssh, telnet: 3600

Tiempo de espera de la sesión de la consola serie(en segundos): 600

Tiempo de espera de la sesión absoluta de la consola serie(en segundos): 3600

Grupo de servidores de autenticación de administrador:

Grupo de servidores de autenticación operativa:

Uso del segundo factor: No

Paso 3. Para configurar los parámetros del servidor RADIUS, ejecute los siguientes comandos.

```
seguridad de alcance fpr4120-TAC-A#
```

```
fpr4120-TAC-A /security # scope radius
```

```
fpr4120-TAC-A /security/radius # ingrese servidor 10.88.244.16
```

```
fpr4120-TAC-A /security/radius/server # set descr "ISE Server"
```

```
fpr4120-TAC-A /security/radius/server* # set key
```

Introduzca la clave: \*\*\*\*\*

Confirme la clave: \*\*\*\*\*

Paso 4. Utilice el comando **show detail** para mostrar los resultados.

fpr4120-TAC-A /security/radius/server\* # **show detail**

Servidor RADIUS:

Nombre de host, FQDN o dirección IP: 10.88.244.16

Descr:

Pedido: 1

Puerto de autenticación: 1812

Clave: \*\*\*

timeout (tiempo de espera): 5

### **Configuración del servidor ACS**

#### **Adición de FXOS como recurso de red**

Paso 1. Navegue hasta **Recursos de Red > Dispositivos de Red y Clientes AAA**.

Paso 2. Haga clic en **Crear**.

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:  Go

<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

Create Duplicate Edit Delete | File Operations Export

Paso 3. Introduzca los valores necesarios (Nombre, Dirección IP, Tipo de dispositivo y Activar RADIUS y agregue la CLAVE).

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

Paso 4. Haga clic en Submit (Enviar).





## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).