

Sistema operativo extensible de FirePOWER (FXO) 2.2: Autenticación y autorización del chasis para la administración remota con el ACS usando el RADIUS

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configurar el chasis FXO](#)

[Configurar al servidor ACS](#)

[Verificación](#)

[Verificación del chasis FXO](#)

[Verificación ACS](#)

[Troubleshooting](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar la autenticación de RADIUS y la autorización para el chasis extensible del sistema operativo de FirePOWER (FXO) vía el Access Control Server (ACS).

El chasis FXO incluye los rol del usuario siguientes:

- Administrador - Acceso de lectura y escritura completo al sistema entero. La cuenta de administración predeterminada se asigna este papel por abandono y no puede ser cambiada.
- Solo lectura - Acceso de sólo lectura a la configuración del sistema sin los privilegios de modificar al Estado del sistema.
- Operaciones - Acceso de lectura y escritura a la configuración del NTP, a la configuración elegante del Call Home para Smart que autoriza, y a los registros del sistema, incluyendo los servidores de Syslog y los incidentes. Acceso de lectura al resto del sistema.
- AAA - Acceso de lectura y escritura a los usuarios, a los papeles, y a la configuración AAA. Acceso de lectura al resto del sistema.

Vía el CLI esto puede ser vista como sigue:

```
fpr4120-TAC-A /security * # papel de la demostración
```

Papel:

Priv del nombre de la función

----- ----

aaa aaa

admin admin

operaciones de las operaciones

solo lectura solo lectura

Contribuido por Tony Ramirez, Jose Soto, ingenieros de Cisco TAC.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento del sistema operativo extensible de FirePOWER (FXO)
- Conocimiento de la configuración de ACS

Componentes Utilizados

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

- Versión 2.2 del dispositivo de seguridad de Cisco FirePOWER 4120
- Versión 5.8.0.32 virtual del Access Control Server de Cisco

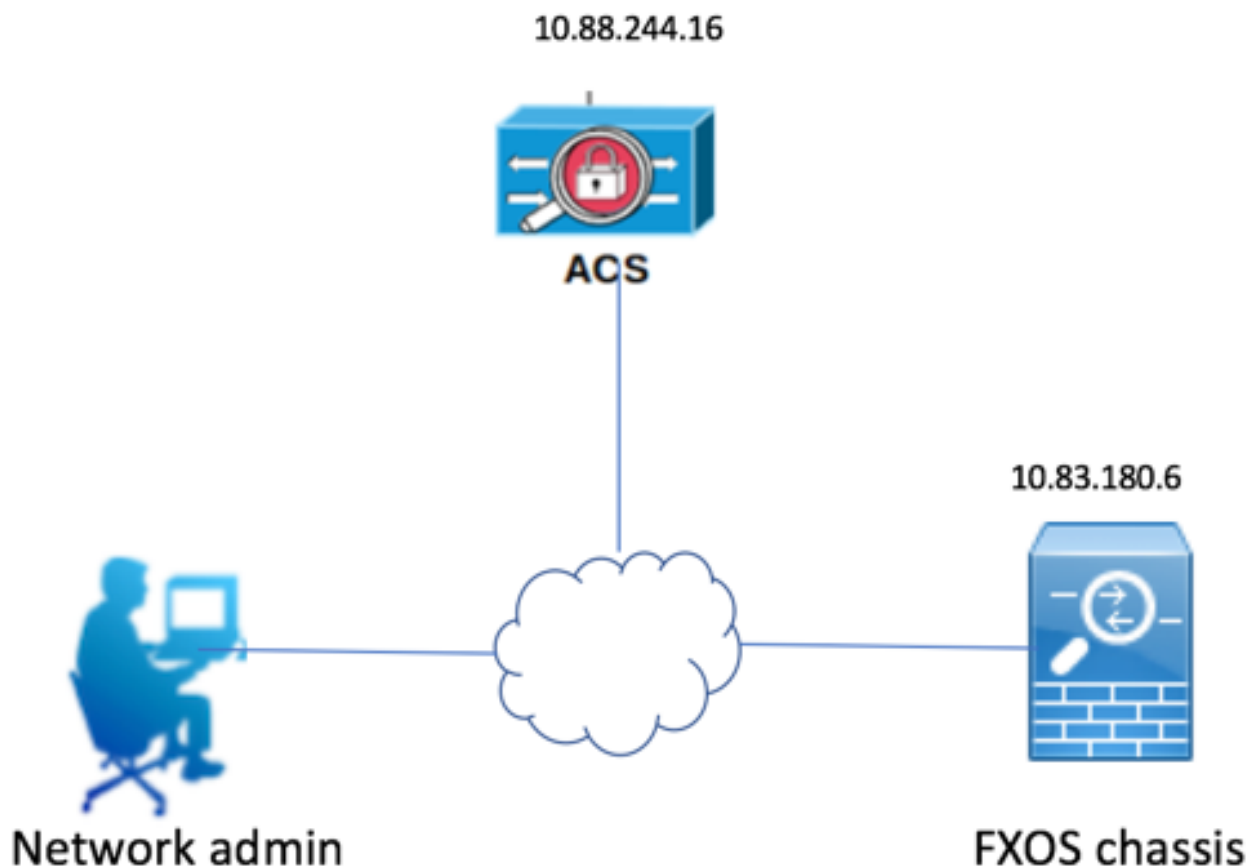
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

La meta de la configuración está a:

- Autentique el registro de usuarios en el GUI basado en web y SSH FXOS mediante el ACS.
- Autorice el registro de usuarios en el GUI basado en web y SSH FXOS según su rol del usuario respectivo mediante el ACS.
- Verifique la operación correcta de la autenticación y autorización en los FXO mediante el ACS.

Diagrama de la red



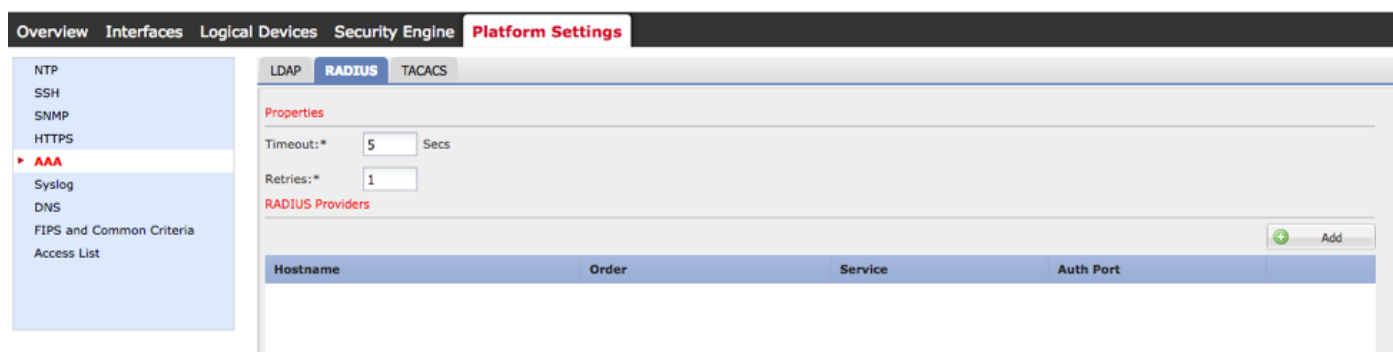
Configuraciones

Configurar el chasis FXO

Crear un proveedor RADIUS que usa al administrador del chasis

Paso 1. Navegue a las configuraciones de la plataforma >AAA.

Paso 2. Haga clic la lengüeta RADIUS.

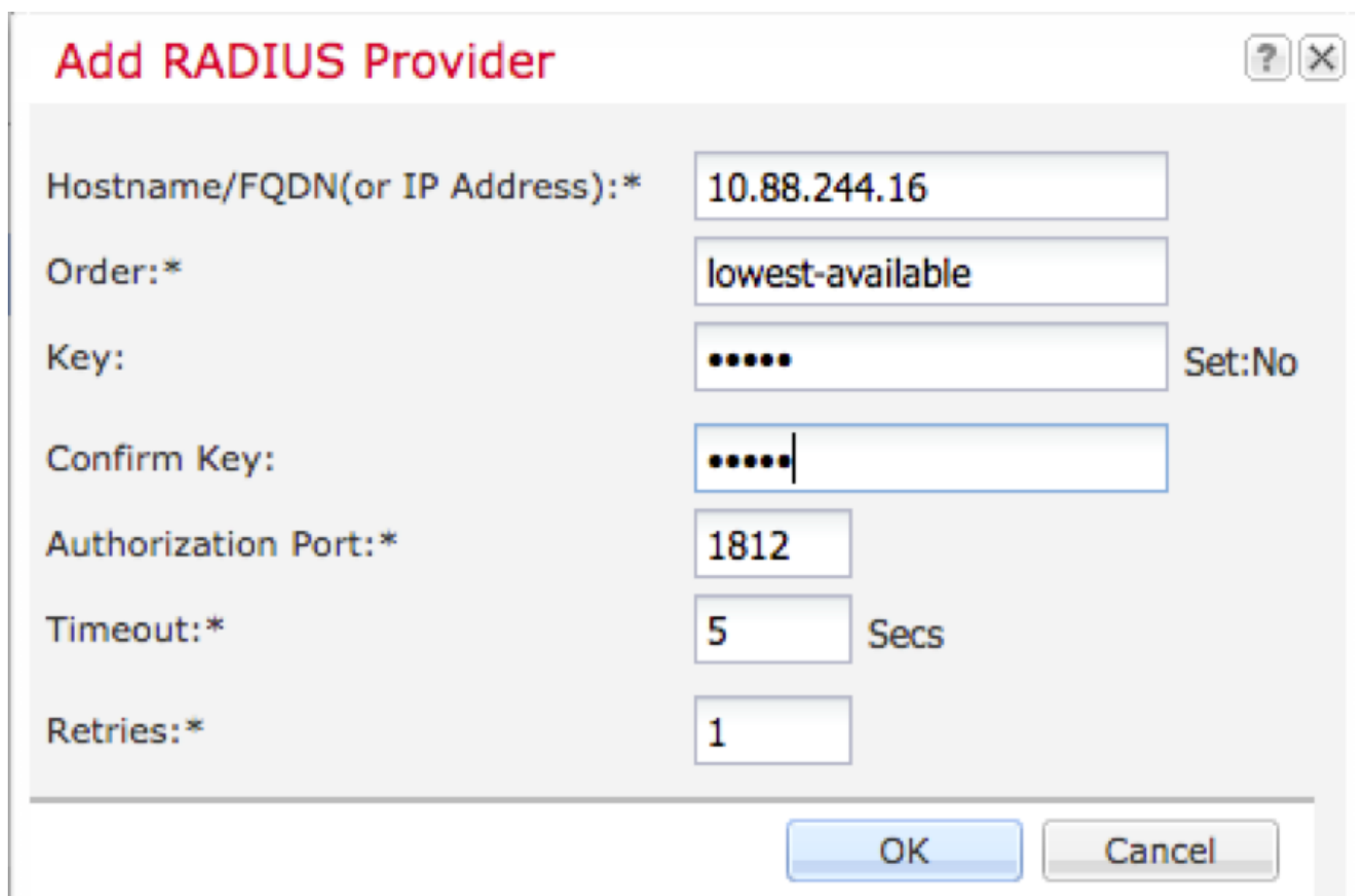


Paso 3. Para cada proveedor RADIUS que usted quiere agregar (hasta 16 proveedores).

3.1. En el área de los proveedores RADIUS, haga click en Add

3.2. En el cuadro de diálogo del proveedor del RADIO del agregar, ingrese los valores requeridos.

3.3. Haga Click en OK para cerrar el cuadro de diálogo del proveedor del agregar RADIUS.

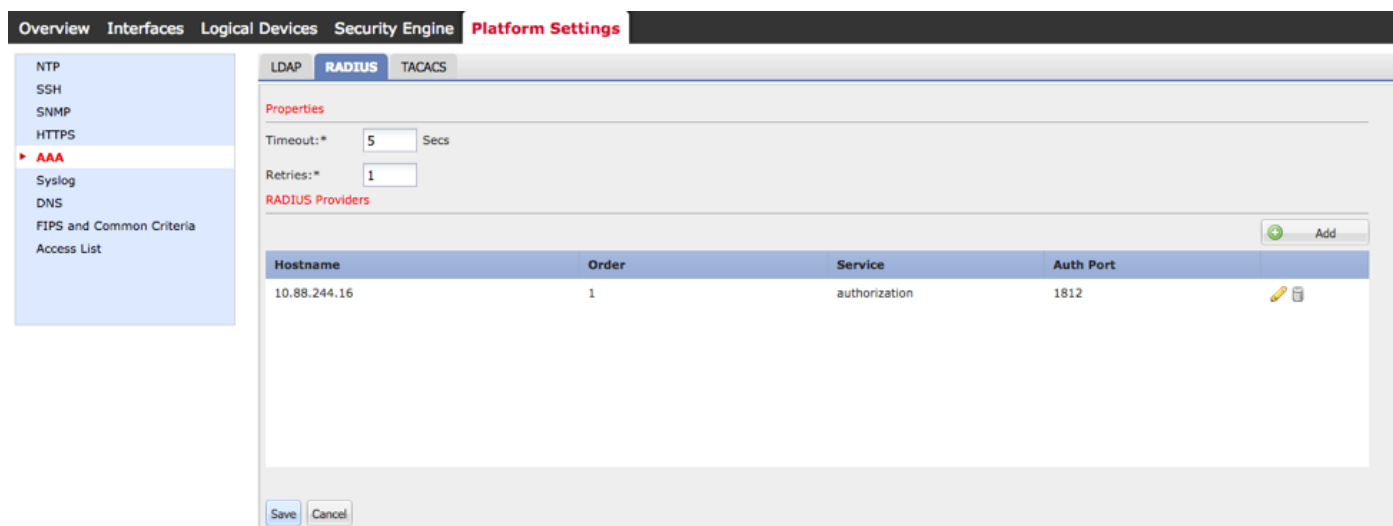


The image shows a dialog box titled "Add RADIUS Provider" with a question mark and close button in the top right corner. The dialog contains several input fields and buttons:

- Hostname/FQDN(or IP Address):*
- Order:*
- Key: Set:No
- Confirm Key:
- Authorization Port:*
- Timeout:* Secs
- Retries:*

At the bottom right, there are two buttons: "OK" and "Cancel".

Paso 4. Salvaguardia del teclado.





The image shows a screenshot of a web interface for "Platform Settings". The navigation menu on the left includes: Overview, Interfaces, Logical Devices, Security Engine, Platform Settings (selected), NTP, SSH, SNMP, HTTPS, AAA (selected), Syslog, DNS, FIPS and Common Criteria, and Access List. The main content area is titled "RADIUS" and has tabs for "LDAP", "RADIUS", and "TACACS".

Under "Properties", there are two fields:

- Timeout:* Secs
- Retries:*

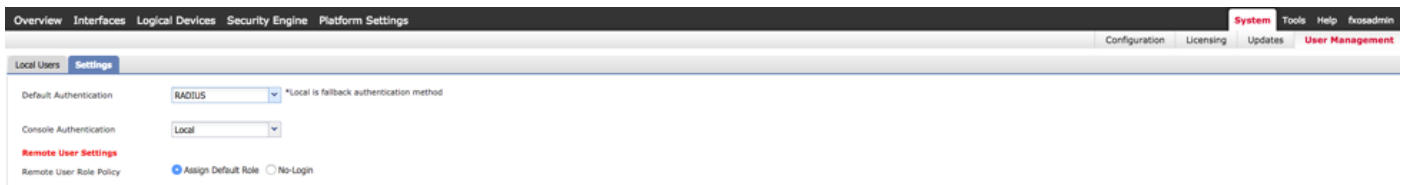
Below this is a section for "RADIUS Providers" with an "Add" button (green plus icon). A table lists the configured providers:

Hostname	Order	Service	Auth Port	
10.88.244.16	1	authorization	1812	 

At the bottom left of the main content area, there are "Save" and "Cancel" buttons.

Paso 5. Navegue al sistema > User Management (Administración de usuario) > las configuraciones.

Paso 6. Bajo autenticación predeterminada elija el RADIUS.



Crear un proveedor RADIUS que usa el CLI

Paso 1. Para habilitar la autenticación de RADIUS, funcione con los siguientes comandos.

Seguridad del alcance fpr4120-TAC-A#

fpr4120-TAC-A /security # valor por defecto-auth del alcance

fpr4120-TAC-A /security/default-auth # fijó el radio del reino

Paso 2. Utilice el **comando detail de la demostración** de visualizar los resultados.

fpr4120-TAC-A /security/default-auth # **detalle de la demostración**

Autenticación predeterminada:

Reino Admin: **Radius**

Reino operativo: **Radius**

La sesión web restaura el período (en los secs): 600

Tiempo de espera de la sesión (en los secs) para la red, ssh, sesiones telnets: 600

Tiempo de espera de la sesión absoluto (en los secs) para la red, ssh, sesiones telnets: 3600

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

Tiempo de espera de la sesión absoluto de la consola en serie (en los secs): 3600

Grupo de servidores del Admin authentication (autenticación de administrador):

Grupo de servidor de autenticación operativo:

Uso del 2do factor: No

Paso 3. Para configurar los parámetros del servidor de RADIUS funcione con los siguientes comandos.

Seguridad del alcance fpr4120-TAC-A#

fpr4120-TAC-A /security # **radio del alcance**

fpr4120-TAC-A /security/radius # **ingresan el servidor 10.88.244.16**

fpr4120-TAC-A /security/radius/server # **fijó el descr "servidor ISE"**

fpr4120-TAC-A /security/radius/server * # **fije la clave**

Ingrese la clave: *****

Confirme la clave: *****

Paso 4. Utilice el **comando detail de la demostración** de visualizar los resultados.

fpr4120-TAC-A /security/radius/server * # **detalle de la demostración**

Servidor de RADIUS:

Nombre de host, FQDN o dirección IP: 10.88.244.16

Descr:

Orden: 1

Puerto del auth: 1812

Clave: ****

Descanso: 5

Configurar al servidor ACS

Agregar los FXO como recurso de red

Paso 1. Navegue a los **recursos de red > a los dispositivos de red y a los clientes AAA.**

Paso 2. El tecleo **crea.**

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"/>	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"/>	FXQS	10.83.180.6/32		All Locations	All Device Types

Create Duplicate Edit Delete | File Operations Export

Paso 3. Ingrese los valores requeridos (el nombre, IP Address, tipo de dispositivo y habilita el RADIO y agrega 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. El tecleo **somete**.

