

Sistema operativo ampliable FirePOWER (FXOS) 2.2: Autenticación/autorización de chasis para administración remota con ISE mediante TACACS+

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuración del chasis FXOS](#)

[Configuración del servidor ISE](#)

[Verificación](#)

[Verificación de FXOS Chasis](#)

[Verificación de ISE 2.0](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar la autenticación y autorización TACACS+ para el chasis Firepower eXtensible Operating System (FXOS) a través de Identity Services Engine (ISE).

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 de ISE
- La licencia de administración de dispositivos TACACS+ se requiere dentro de ISE

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 Identity Services Engine 2.2.0.470 virtual

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 ISE
- Autorice a los usuarios a iniciar sesión en la GUI basada en Web y SSH de FXOS según su función de usuario respectiva mediante ISE.
- Verifique el correcto funcionamiento de la autenticación y autorización en el FXOS mediante ISE

Diagrama de la red



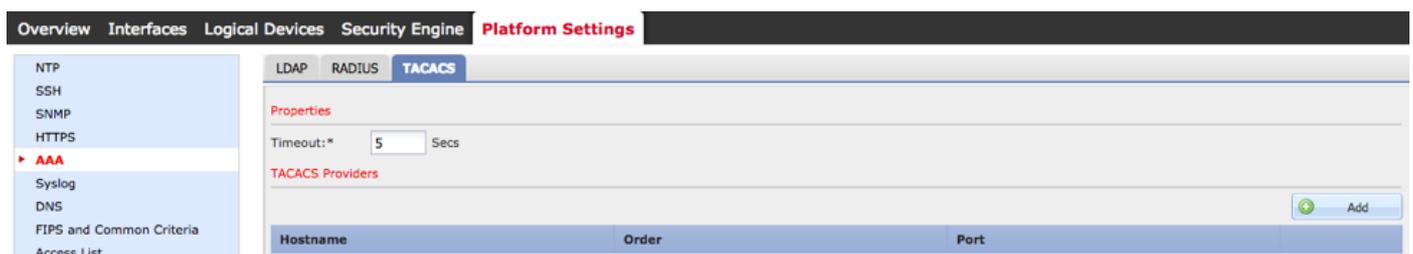
Configuraciones

Configuración del chasis FXOS

Creación de un proveedor TACACS+

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

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

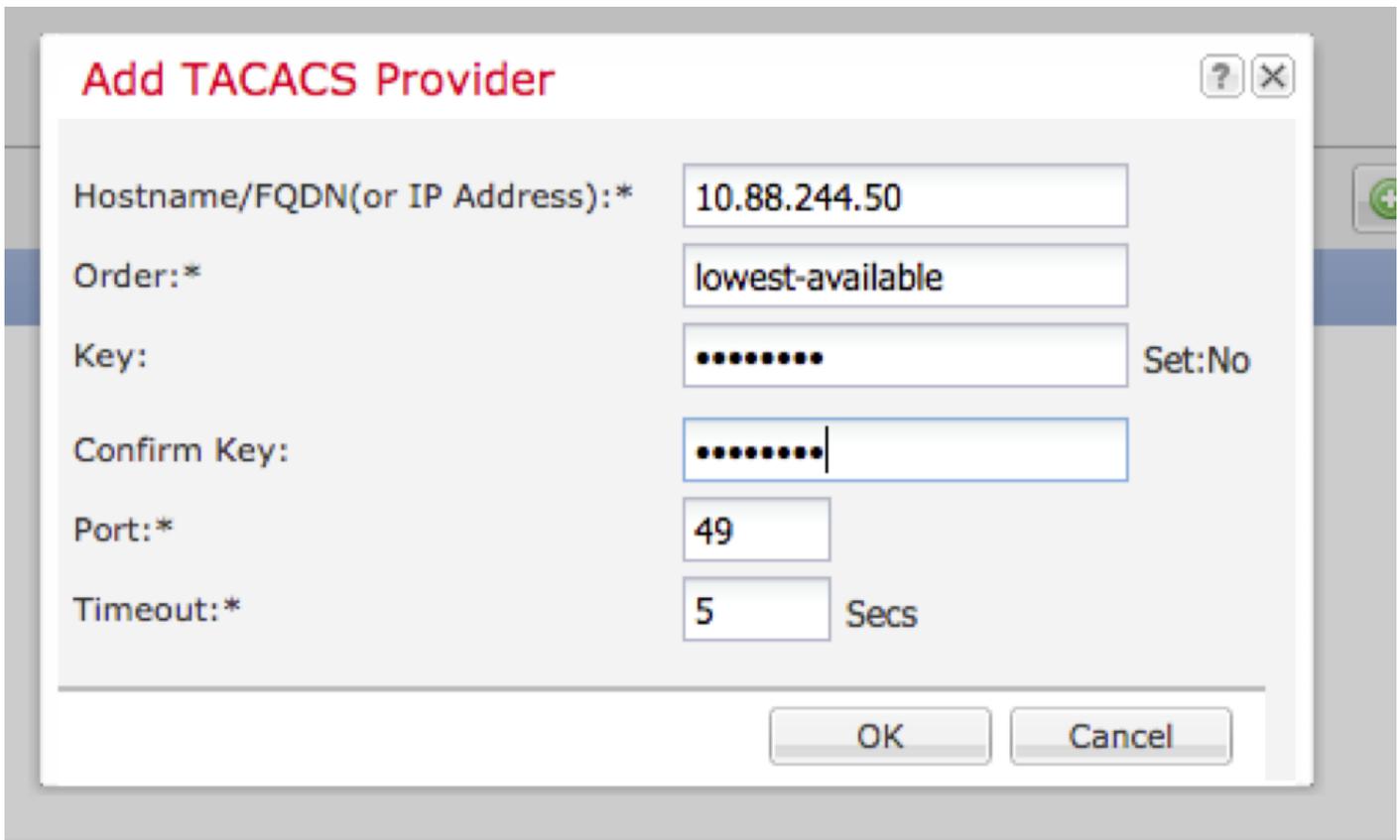


Paso 3. Para cada proveedor TACACS+ que desee agregar (hasta 16 proveedores).

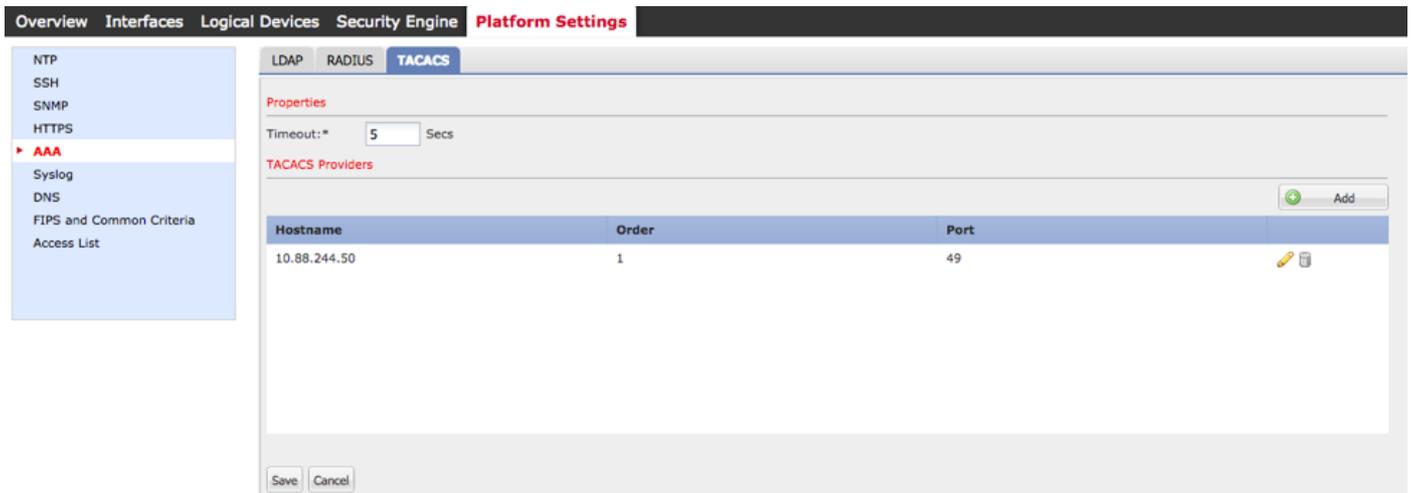
3.1. En el área Proveedores TACACS, haga clic en **Agregar**.

3.2. Cuando se abra el cuadro de diálogo Agregar proveedor TACACS, introduzca los valores necesarios.

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



Paso 4. Click **Save**.



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

Paso 6. En Default Authentication , elija **TACACS**.



Creación de un proveedor TACACS+ mediante CLI

Paso 1. Para habilitar la autenticación TACACS, 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 tacacs
```

Paso 2. Utilice el comando **show detail** para verificar la configuración.

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

Autenticación predeterminada:

Rango de administración: **TACACS**

Rango operativo: **TACACS**

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 TACACS, ejecute los siguientes comandos.

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

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

```
fpr4120-TAC-A /security/tacacs # ingrese server 10.88.244.50
```

```
fpr4120-TAC-A /security/tacacs/server # set descr "ACS Server"
```

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

Introduzca la clave: *****

Confirme la clave: *****

Paso 4. Utilice el comando **show detail** para verificar la configuración.

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

Servidor TACACS+:

Nombre de host, FQDN o dirección IP: 10.88.244.50

Descr:

Pedido: 1

Puerto: 49

Clave: ***

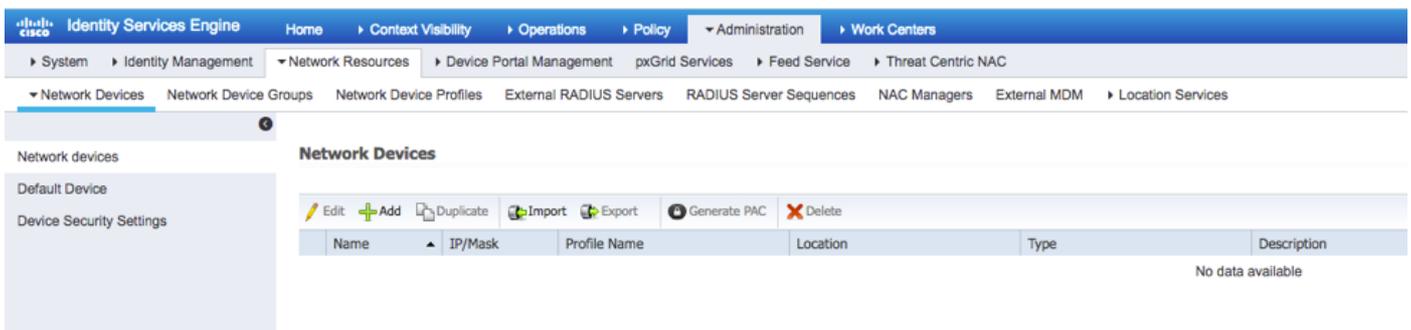
timeout (tiempo de espera): 5

Configuración del servidor ISE

Adición de FXOS como recurso de red

Paso 1. Vaya a **Administration > Network Resources > Network Devices**.

Paso 2. Haga clic en Add (Agregar).



Paso 3. Introduzca los valores necesarios (Nombre, Dirección IP, Tipo de dispositivo y Activar TACACS+ y agregue la CLAVE), haga clic en **Enviar**.

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 > FXOS

Network Devices

* Name

Description

* IP Address: /

* Device Profile

Model Name

Software Version

* Network Device Group

Device Type

IPSEC

Location

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret

Enable Single Connect Mode

Legacy Cisco Device
 TACACS Draft Compliance Single Connect Support

SNMP Settings

Advanced TrustSec Settings

Creación de grupos de identidad y usuarios

Paso 1. Vaya a **Administration > Identity Management > Groups > User Identity Groups**.

Paso 2. Haga clic en **Add (Agregar)**.

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

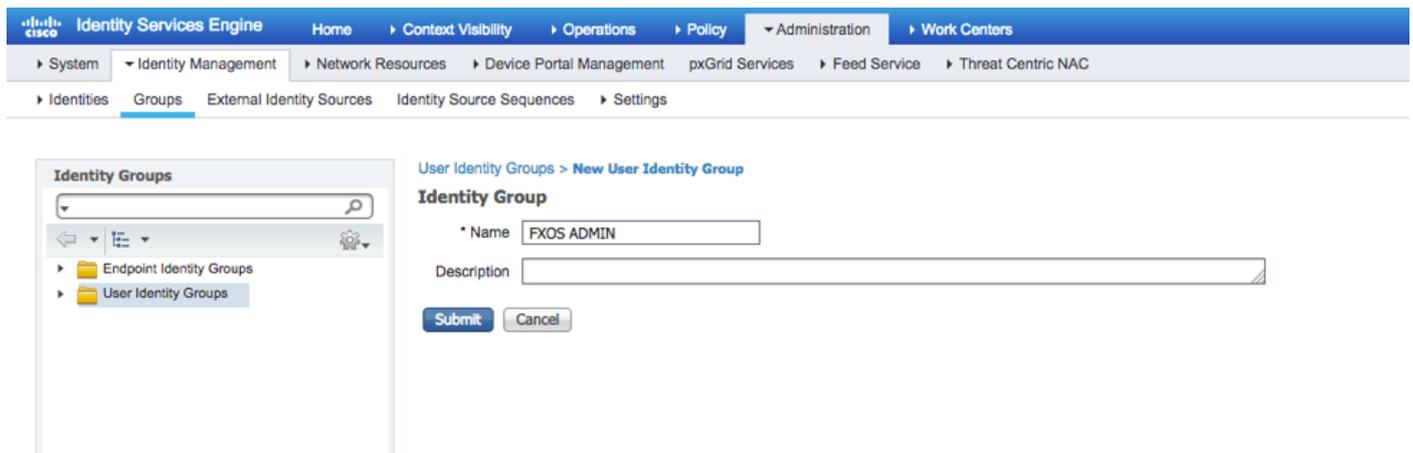
User Identity Groups

User Identity Groups

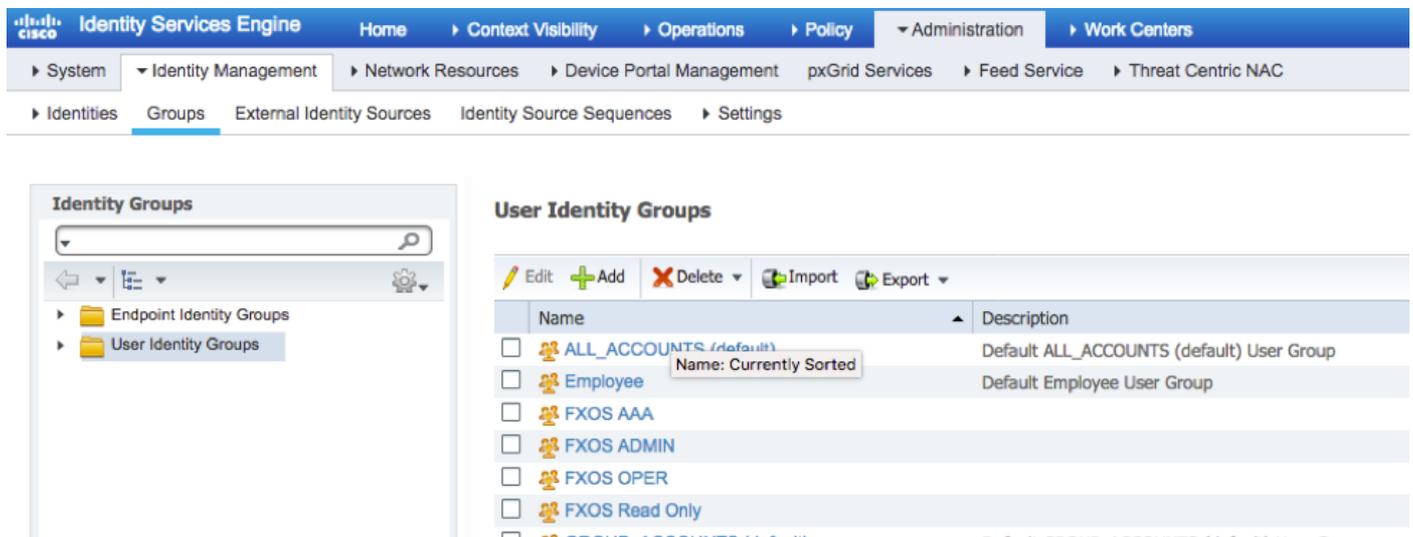
Edit Add Delete Import Export

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

Paso 3. Introduzca el valor para Name y haga clic en **Submit**.

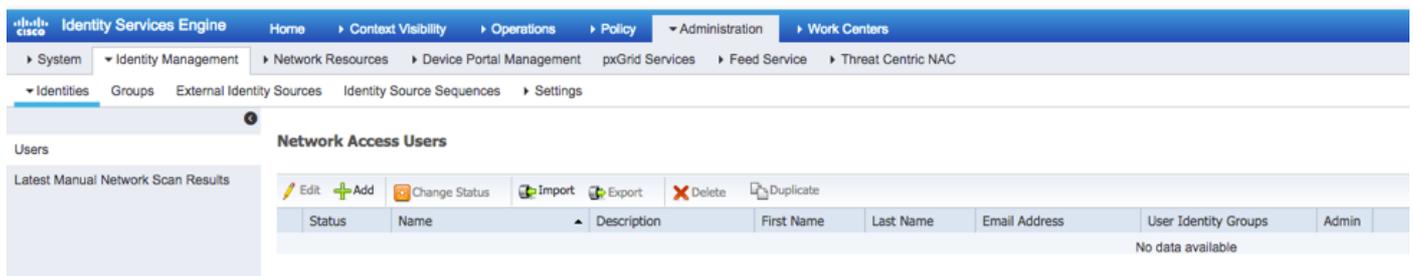


Paso 4. Repita el paso 3 para todas las funciones de usuario necesarias.



Paso 5. Vaya a **Administration > Identity Management > Identity > Users**.

Paso 6. Haga clic en **Add** (Agregar).



Paso 7. Introduzca los valores necesarios (Nombre, Grupo de usuarios, Contraseña).

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

Paso 8. Repita el paso 6 para todos los usuarios requeridos.

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

Edit Add Change Status Import Export Delete Duplicate

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	

Creación del perfil de shell para cada rol de usuario

Paso 1. Navegue hasta **Centros de trabajo > Administración de dispositivos > Elementos de políticas > Resultados > Perfiles TACACS** y haga clic **+AÑADIR**.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings

TACACS Profiles

0 Selected Rows/Page 4 / 1 / 1 Go 4 Total Rows

Refresh Add Duplicate Trash Edit Filter

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	WLC ALL	WLC	WLC ALL
<input type="checkbox"/>	WLC MONITOR	WLC	WLC MONITOR
<input type="checkbox"/>	Deny All Shell Profile	Shell	Deny All Shell Profile
<input type="checkbox"/>	Default Shell Profile	Shell	Default Shell Profile

Paso 2. Introduzca los valores necesarios para el perfil TACACS

2.1. Introduzca el nombre.

TACACS Profiles > New

TACACS Profile

Name

Description

Task Attribute View

Raw View

2.2. En la FICHA Vista en RAW, configure el siguiente CISCO-AV-PAIR.

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

TACACS Profile

Name

Description

Task Attribute View

Raw View

Profile Attributes

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

Cancel

Submit

2.3. Haga clic en Submit (Enviar).

TACACS Profile

Name

Description

Task Attribute View Raw View

Common Tasks

Common Task Type

<input type="checkbox"/> Default Privilege	<input type="text"/>	(Select 0 to 15)
<input type="checkbox"/> Maximum Privilege	<input type="text"/>	(Select 0 to 15)
<input type="checkbox"/> Access Control List	<input type="text"/>	
<input type="checkbox"/> Auto Command	<input type="text"/>	
<input type="checkbox"/> No Escape	<input type="text"/>	(Select true or false)
<input type="checkbox"/> Timeout	<input type="text"/>	Minutes (0-9999)
<input type="checkbox"/> Idle Time	<input type="text"/>	Minutes (0-9999)

Custom Attributes

+ Add Trash Edit

Type	Name	Value	
<input type="checkbox"/> MANDATORY	cisco-av-pair	shell:roles="admin"	

Cancel Save

Paso 3. Repita el paso 2 para las restantes funciones de usuario utilizando los siguientes pares AV-Cisco.

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

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

cisco-av-pair=shell:roles="sólo lectura"

Custom Attributes

+ Add Trash Edit

Type	Name	Value	
<input type="checkbox"/> MANDATORY	cisco-av-pair	shell:roles="aaa"	

Cancel Save

Custom Attributes

+ Add Trash Edit ⚙️

<input type="checkbox"/>	Type	Name	Value	
<input type="checkbox"/>	MANDATORY	cisco-av-pair	shell:roles="operations"	<input type="checkbox"/> <input type="checkbox"/>

Custom Attributes

+ Add Trash Edit ⚙️

<input type="checkbox"/>	Type	Name	Value	
<input type="checkbox"/>	MANDATORY	cisco-av-pair	shell:roles="read-only"	<input type="checkbox"/> <input type="checkbox"/>

TACACS Profiles

0 Selected

Rows/Page 1 / 1 8 Total Rows

+ Add Duplicate Trash Edit Filter ⚙️

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	WLC ALL	WLC	WLC ALL
<input type="checkbox"/>	WLC MONITOR	WLC	WLC MONITOR
<input type="checkbox"/>	Deny All Shell Profile	Shell	Deny All Shell Profile
<input type="checkbox"/>	Default Shell Profile	Shell	Default Shell Profile
<input type="checkbox"/>	FXOS_Admin_Profile	Shell	
<input type="checkbox"/>	FXOS_AAA_Shell	Shell	
<input type="checkbox"/>	FXOS_Operations_Shell	Shell	
<input type="checkbox"/>	FXOS_ReadOnly_Shell	Shell	

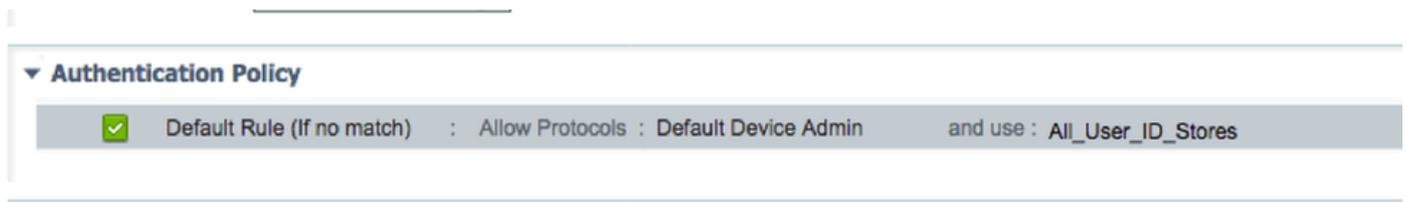
Creación de la Política de Autorización TACACS

Paso 1. Vaya a **Centros de trabajo > Administración de dispositivos > Conjuntos de políticas de administración de dispositivos**.

The screenshot shows the Cisco ISE configuration page for TACACS profiles. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main navigation bar includes: Network Access, Guest Access, TrustSec, BYOD, Profiler, Posture, Device Administration, and PassiveID. The sub-navigation bar includes: Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements, Device Admin Policy Sets, Reports, and Settings. A notification box says: "Click here to do wireless setup and visibility setup. Do not show this again." The "Policy Sets" section is active, showing a search bar and a "Summary of Policies" sidebar. The main content area is titled "Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order. For Policy Export go to Administration > System > Backup & Restores > Policy Export Page." The configuration for the "Tactics_Default" policy set is shown, including: Status: Default, Name: Tactics_Default, Regular: Proxy Sequence, Proxy server sequence: [dropdown], Authentication Policy: Default Rule (if no match): Allow Protocols: Default Device Admin and use: All_User_ID_Stores, Authorization Policy: Exceptions (0), Standard: Tactics_Default, Conditions (identity groups and other conditions): Deny All Shell Profile, Command Sets, and Shell Profiles.

Paso 2. Asegúrese de que la política de autenticación apunte a la base de datos de usuarios

internos o al almacén de identidades requerido.



Paso 3. Haga clic en la flecha situada al final de la política de autorización predeterminada y haga clic en insertar regla anterior.

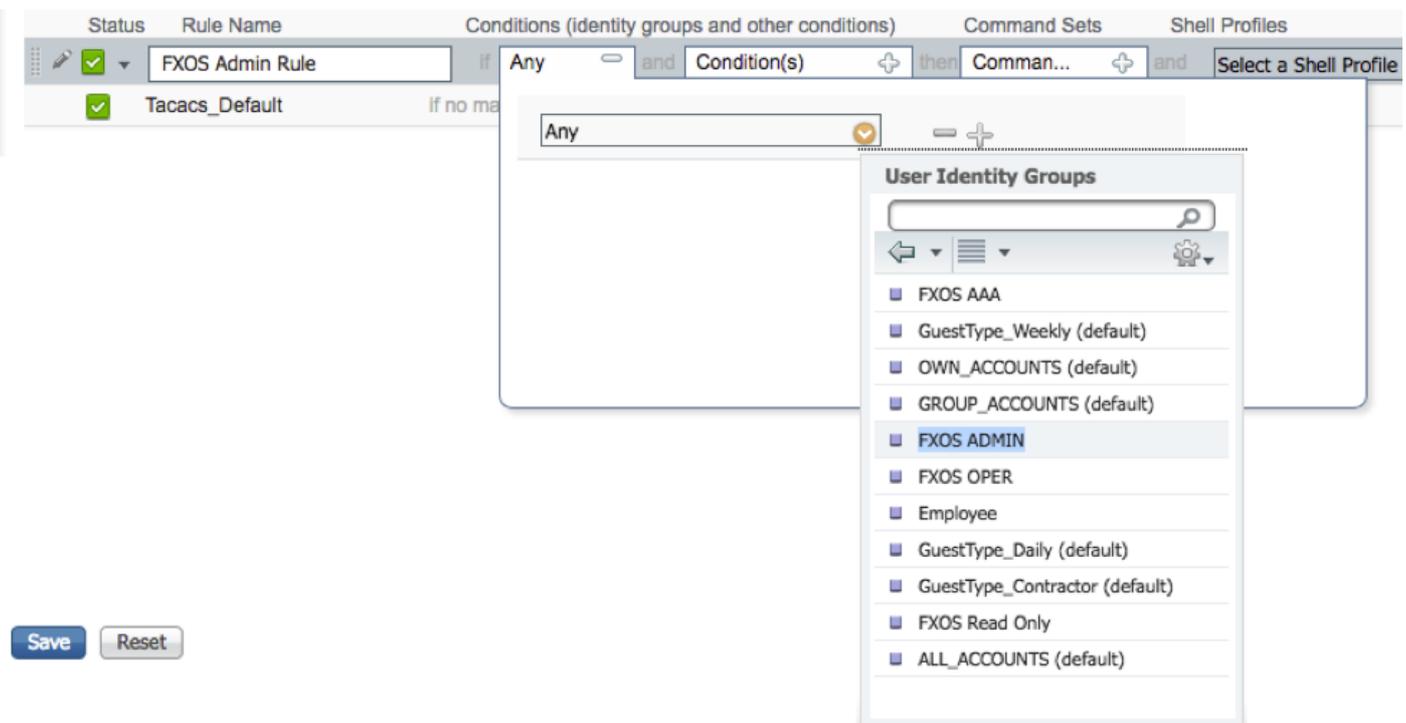


Paso 4. Introduzca los valores de la regla con los parámetros necesarios:

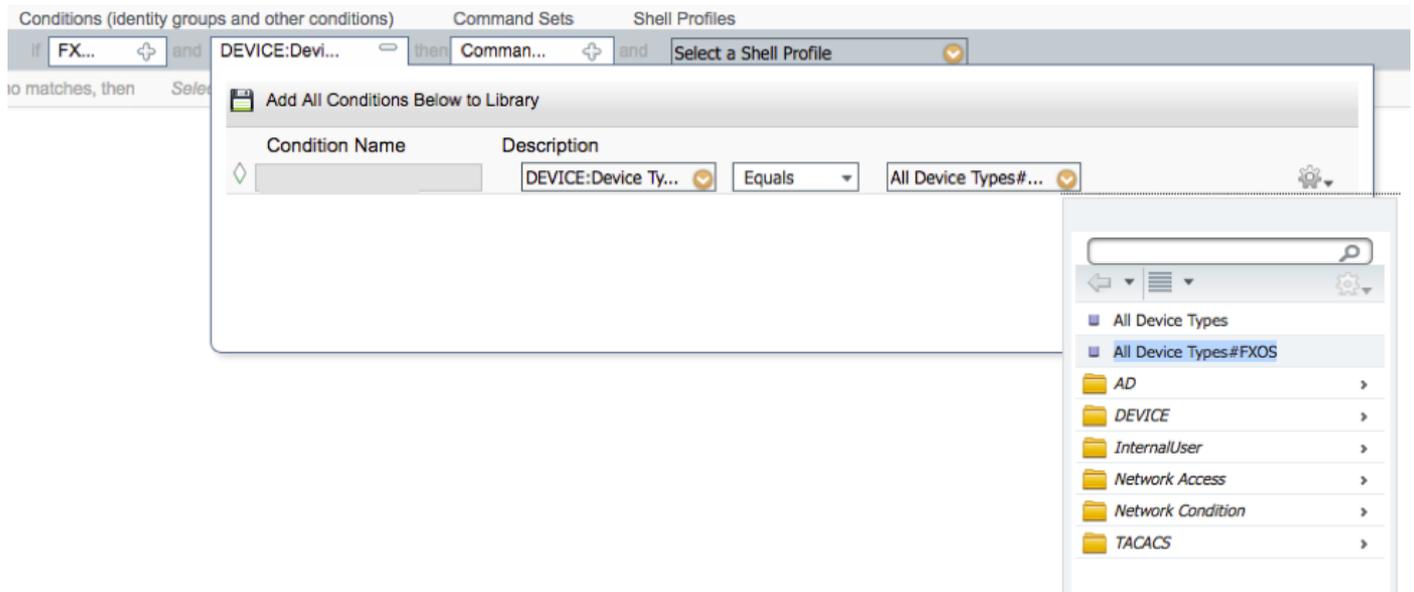
4.1. 'Nombre de la regla Regla de administración FXOS.

4.2. Condiciones.

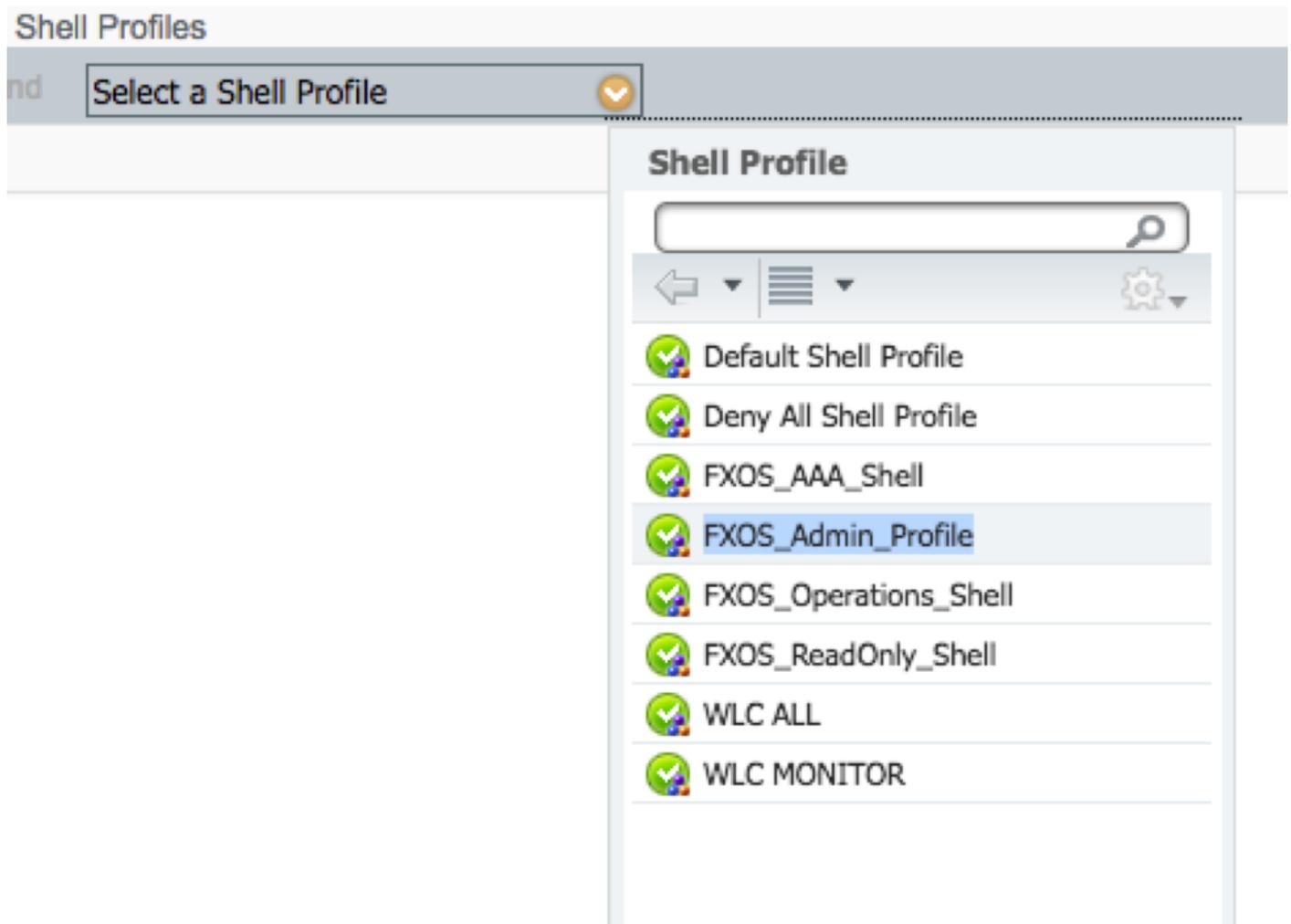
Si: El grupo de identidad de usuario es FXOS ADMIN



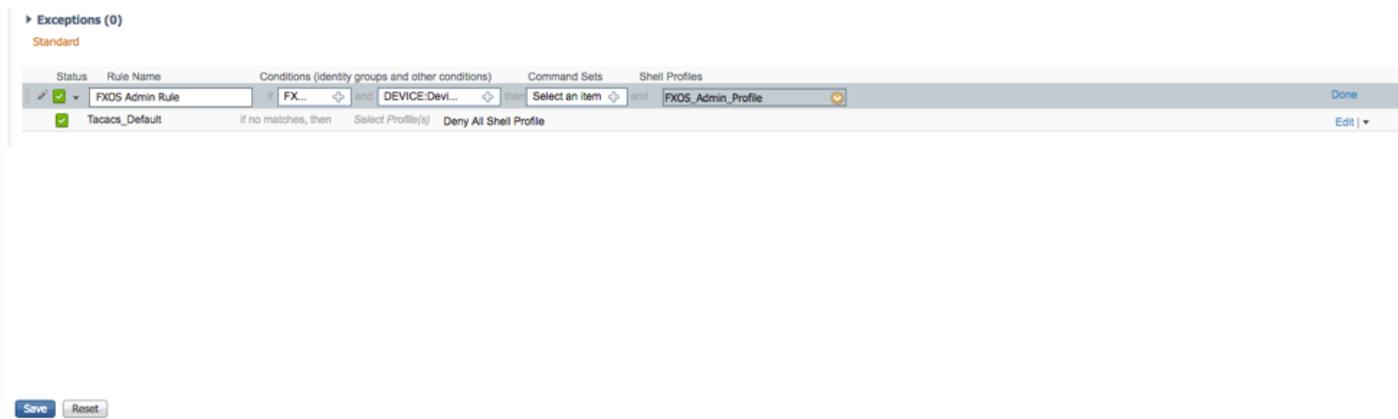
Y dispositivo: El tipo de dispositivo es igual a todos los tipos de dispositivo #FXOS



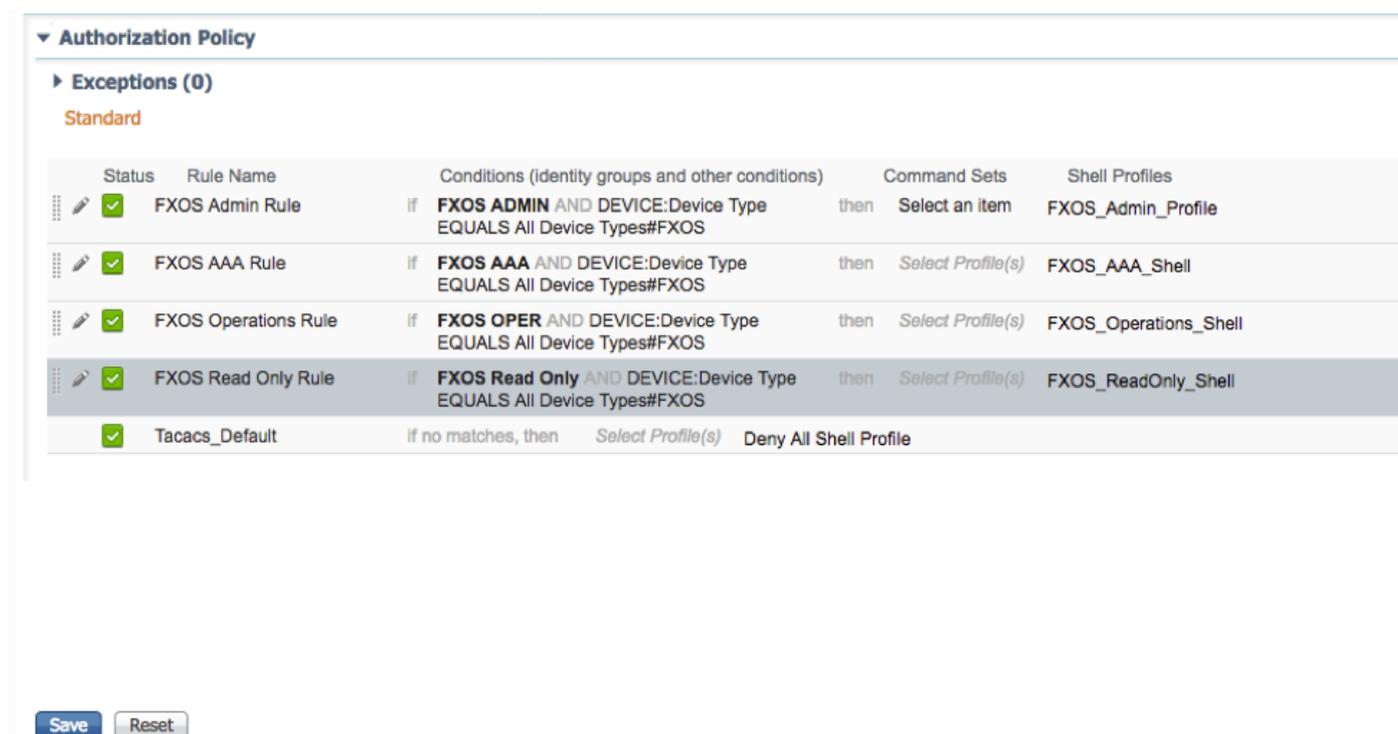
Perfil de shell: FXOS_Admin_Profile



Paso 5. Haga clic en Done (Listo).



Paso 6. Repita los pasos 3 y 4 para las funciones de usuario restantes y, cuando haya terminado, haga clic en **GUARDAR**.



Verificación

Ahora puede probar cada usuario y verificar la función de usuario asignada.

Verificación de FXOS Chasis

1. Telnet o SSH al chasis FXOS e inicie sesión con cualquiera de los usuarios creados en ISE.

Nombre de usuario: fxosadmin

Contraseña

fpr4120-TAC-A# **scope security**

fpr4120-TAC-A /security # **show remote-user detail**

Usuario remoto **fxosaaa**:

Descripción:

Funciones de usuario:

Nombre: **aaa**

Nombre: **sólo lectura**

Usuario remoto **fxosadmin**:

Descripción:

Funciones de usuario:

Nombre: **admin**

Nombre: **sólo lectura**

Fxosoper Usuario remoto:

Descripción:

Funciones de usuario:

Nombre: **operaciones**

Nombre: **sólo lectura**

Usuario remoto **fxosro**:

Descripción:

Funciones de usuario:

Nombre: **sólo lectura**

Según el nombre de usuario introducido, la cli del chasis FXOS sólo mostrará los comandos autorizados para el rol de usuario asignado.

Admin User Role (Función de usuario de administrador).

fpr4120-TAC-A /security # ?

Reconocimiento

clear-user-sessions Clear User Sessions

Crear objetos administrados

eliminar objetos administrados

inhabilitar servicios

enable Habilita servicios

introducir un objeto administrado

scope Cambia el modo actual

establecer valores de propiedad

show Show system information

finalizar sesiones cimc activas

fpr4120-TAC-A# **connect fxos**

fpr4120-TAC-A (fxos)# **debug aaa-requests**

fpr4120-TAC-A (fxos)#

Función de usuario de sólo lectura.

fpr4120-TAC-A /security # ?

scope Cambia el modo actual

establecer valores de propiedad

show Show system information

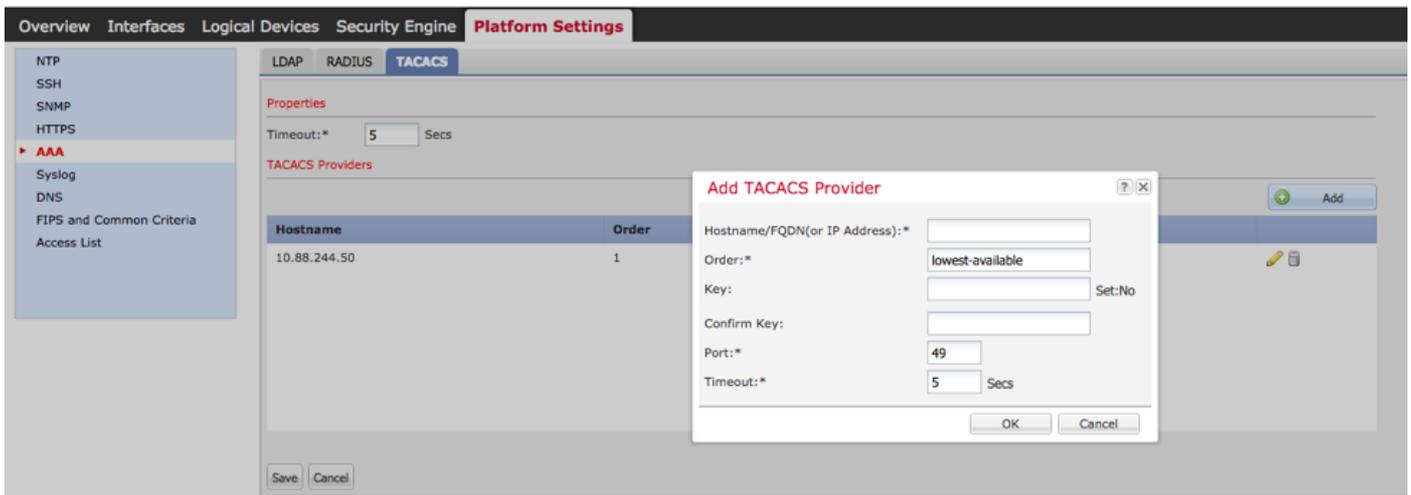
fpr4120-TAC-A# **connect fxos**

fpr4120-TAC-A (fxos)# **debug aaa-requests**

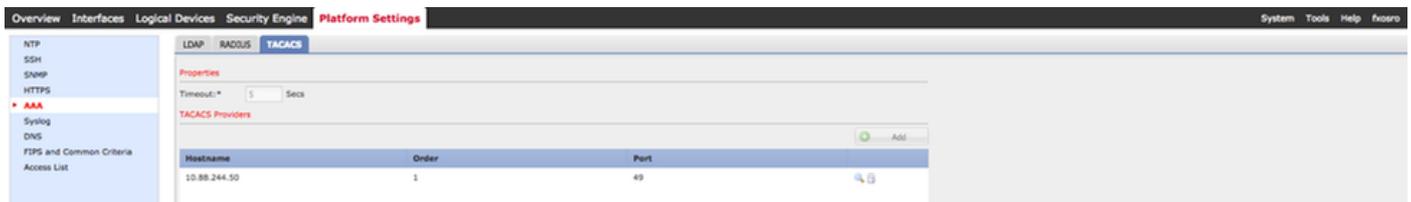
% Permiso denegado para la función

2. Busque la dirección IP del chasis FXOS e inicie sesión con cualquiera de los usuarios creados en ISE.

Admin User Role (Función de usuario de administrador).



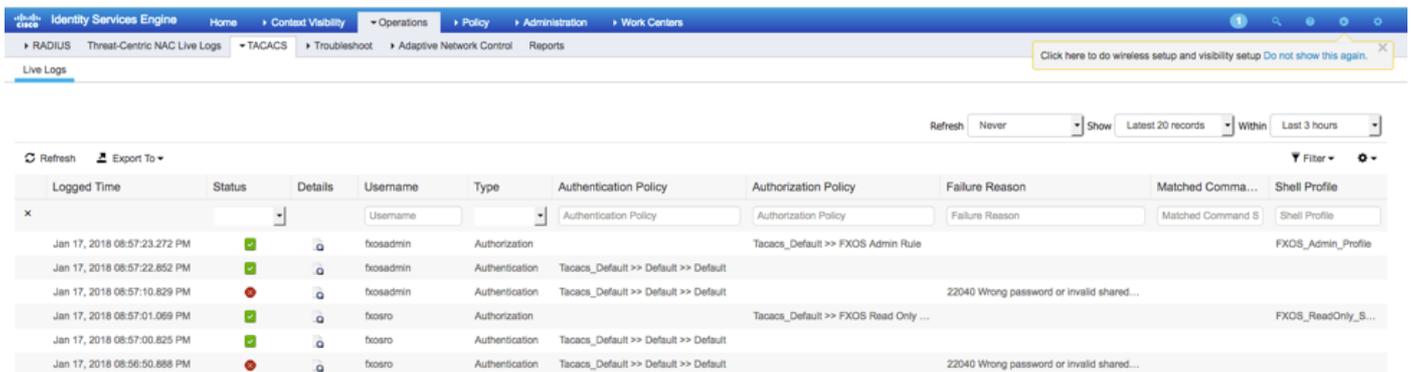
Función de usuario de sólo lectura.



Nota: Observe que el botón **ADD** está atenuado.

Verificación de ISE 2.0

1. Navegue hasta **Operaciones > Enlace TACACS**. Debería poder ver intentos exitosos y fallidos.



Troubleshoot

Para depurar la autenticación y autorización AAA, ejecute los siguientes comandos en el cli FXOS.

```
fr4120-TAC-A# connect fxos
```

```
fr4120-TAC-A (fxos)# debug aaa-requests
```

```
fr4120-TAC-A (fxos)# debug aaa event
```

```
fr4120-TAC-A (fxos)# debug aaa errors
```

fpr4120-TAC-A (fxos)# **plazo mon**

Después de un intento de autenticación exitoso, verá el siguiente resultado.

2018 17 ene 15:46:40.305247 aaa: aaa_req_process para autenticación. session no 0

2018 17 ene 15:46:40.305262 aaa: aaa_req_process: Solicitud AAA general de appln: login
appln_subtype: predeterminado

2018 17 ene 15:46:40.305271 aaa: try_next_aaa_method

2018 17 ene 15:46:40.305285 aaa: total de métodos configurados es 1, el índice actual que se
probará es 0

2018 17 ene 15:46:40.305294 aaa: handle_req_using_method

2018 17 ene 15:46:40.305301 aaa: AAA_METHOD_SERVER_GROUP

2018 17 ene 15:46:40.305308 aaa: aaa_sg_method_handler group = tacacs

2018 17 ene 15:46:40.305315 aaa: Uso de sg_protocol que se pasa a esta función

2018 17 ene 15:46:40.305324 aaa: Envío de una solicitud al servicio TACACS

2018 17 ene 15:46:40.305384 aaa: Grupo de métodos configurado correctamente

2018 17 ene 15:46:40.554631 aaa: aaa_process_fd_set

2018 17 ene 15:46:40.555229 aaa: aaa_process_fd_set: mtscallback en aaa_q

2018 17 ene 15:46:40.555817 aaa: mts_message_response_handler: una respuesta mts

2018 17 ene 15:46:40.556387 aaa: prot_daemon_reponse_handler

2018 17 ene 15:46:40.557042 aaa: sesión: 0x8dfd68c eliminado de la tabla de sesiones 0

2018 17 ene 15:46:40.557059 aaa: is_aaa_resp_status_éxito status = 1

2018 17 ene 15:46:40.557066 aaa: is_aaa_resp_status_éxito es VERDADERO

2018 17 ene 15:46:40.557075 aaa: aaa_send_client_response para autenticación. session-
>indicadores=21. aaa_resp->indicadores=0.

2018 17 ene 15:46:40.557083 aaa: AAA_REQ_FLAG_NORMAL

2018 17 ene 15:46:40.557106 aaa: mts_send_response satisfactoria

2018 17 ene 15:46:40.557364 aaa: aaa_req_process para autorización. session no 0

2018 17 ene 15:46:40.557378 aaa: aaa_req_process llamado con contexto desde appln: login
appln_subtype: default authen_type:2, authen_method: 0

2018 17 ene 15:46:40.557386 aaa: aaa_send_req_using_context

2018 17 ene 15:46:40.557394 aaa: aaa_sg_method_handler group = (nulo)

2018 17 ene 15:46:40.557401 aaa: Uso de sg_protocol que se pasa a esta función

2018 17 ene 15:46:40.557408 aaa: solicitud AAA dirigida o basada en el contexto(excepción: no es una solicitud de relay). No aceptará copia de una solicitud

2018 17 ene 15:46:40.557415 aaa: Envío de una solicitud al servicio TACACS

2018 17 ene 15:46:40.801732 aaa: aaa_send_client_response para autorización. session->indicadores=9. aaa_resp->indicadores=0.

2018 17 ene 15:46:40.801740 aaa: AAA_REQ_FLAG_NORMAL

2018 17 ene 15:46:40.801761 aaa: mts_send_response satisfactoria

2018 17 ene 15:46:40.848932 aaa: ANTIGUO OPCODE: accounting_interina_update

2018 17 ene 15:46:40.848943 aaa: aaa_create_local_acct_req: user=, session_id=, log=usuario agregado:fxosadmin a la función:admin

2018 17 ene 15:46:40.848963 aaa: aaa_req_process para contabilidad. session no 0

2018 17 ene 15:46:40.848972 aaa: La referencia de solicitud MTS es NULL. solicitud LOCAL

2018 17 ene 15:46:40.848982 aaa: Configuración de AAA_REQ_RESPONSE_NOT_NEEDED

2018 17 ene 15:46:40.848992 aaa: aaa_req_process: Solicitud AAA general de appln: appln_subtype predeterminado: predeterminado

2018 17 ene 15:46:40.849002 aaa: try_next_aaa_method

2018 17 ene 15:46:40.849022 aaa: no hay métodos configurados para el valor predeterminado

2018 17 ene 15:46:40.849032 aaa: no hay configuración disponible para esta solicitud

2018 17 ene 15:46:40.849043 aaa: try_fallback_method

2018 17 ene 15:46:40.849053 aaa: handle_req_using_method

2018 17 ene 15:46:40.849063 aaa: local_method_handler

2018 17 ene 15:46:40.849073 aaa: aaa_local_accounting_msg

2018 17 ene 15:46:40.849085 aaa: actualización::usuario agregado:fxosadmin a la función:admin

Después de un intento fallido de autenticación, verá el siguiente resultado.

2018 17 ene 15:46:17.836271 aaa: aaa_req_process para autenticación. session no 0

2018 17 ene 15:46:17.836616 aaa: aaa_req_process: Solicitud AAA general de appln: login appln_subtype: predeterminado

2018 17 ene 15:46:17.837063 aaa: try_next_aaa_method

2018 17 ene 15:46:17.837416 aaa: total de métodos configurados es 1, el índice actual que se probará es 0

2018 17 ene 15:46:17.837766 aaa: handle_req_using_method

2018 17 ene 15:46:17.838103 aaa: AAA_METHOD_SERVER_GROUP

2018 17 ene 15:46:17.838477 aaa: aaa_sg_method_handler group = tacacs

2018 17 ene 15:46:17.838826 aaa: Uso de sg_protocol que se pasa a esta función

2018 17 ene 15:46:17.839167 aaa: Envío de una solicitud al servicio TACACS

2018 17 ene 15:46:17.840225 aaa: Grupo de métodos configurado correctamente

2018 17 ene 15:46:18.043710 aaa: is_aaa_resp_status_éxito status = 2

2018 17 ene 15:46:18.044048 aaa: is_aaa_resp_status_éxito es VERDADERO

2018 17 ene 15:46:18.044395 aaa: aaa_send_client_response para autenticación. session->indicadores=21. aaa_resp->indicadores=0.

2018 17 ene 15:46:18.044733 aaa: AAA_REQ_FLAG_NORMAL

2018 17 ene 15:46:18.045096 aaa: mts_send_response satisfactoria

2018 17 ene 15:46:18.045677 aaa: aaa_cleanup_session

2018 17 ene 15:46:18.045689 aaa: mts_drop of request msg

2018 17 ene 15:46:18.045699 aaa: aaa_req debe ser liberado.

2018 17 ene 15:46:18.045715 aaa: aaa_process_fd_set

2018 17 ene 15:46:18.045722 aaa: aaa_process_fd_set: mtscallback en aaa_q

2018 17 ene 15:46:18.045732 aaa: aaa_enable_info_config: mensaje de error GET_REQ for aaa login

2018 17 ene 15:46:18.045738 aaa: devuelve el valor devuelto de la operación de configuración:elemento de seguridad desconocido

Información Relacionada

El comando Ethalyzer en FX-OS cli solicitará una contraseña cuando la autenticación TACACS/RADIUS esté habilitada. Este comportamiento es causado por un error.

ID de la falla: [CSCvg87518](#)