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

## Contenido



## 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 Identity Services Engine (ISE).

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 Remirez, 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 ISE

## 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
- Cisco Identity Services Engine virtual 2.2.0.470

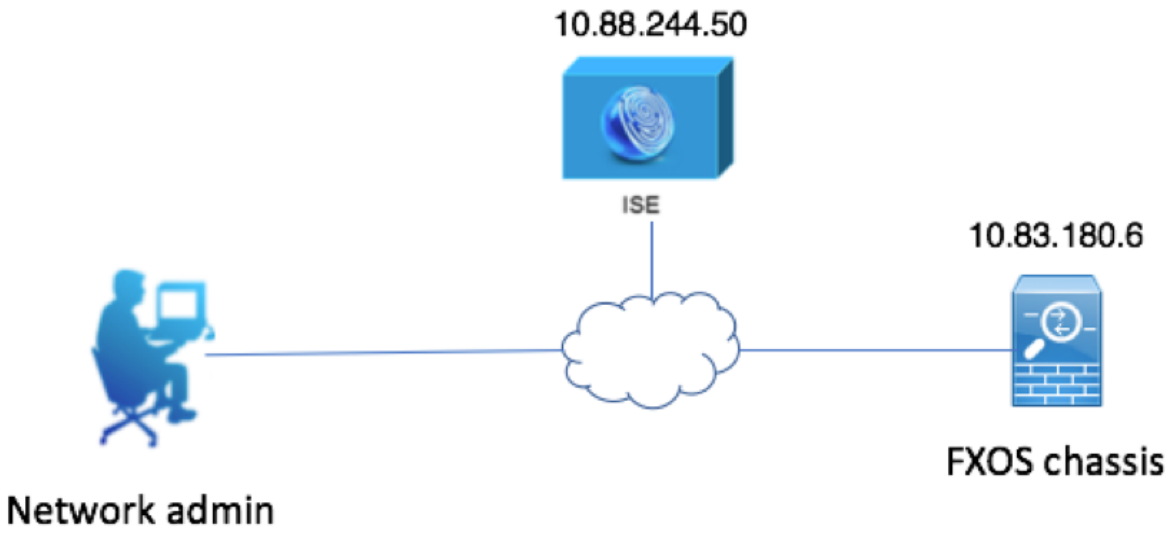
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de 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 ISE
- Autorice el registro de usuarios en el GUI basado en web y SSH FXOS según su rol del usuario respectivo mediante el ISE.
- Verifique la operación correcta de la autenticación y autorización en los FXO mediante el ISE

## Diagrama de la red



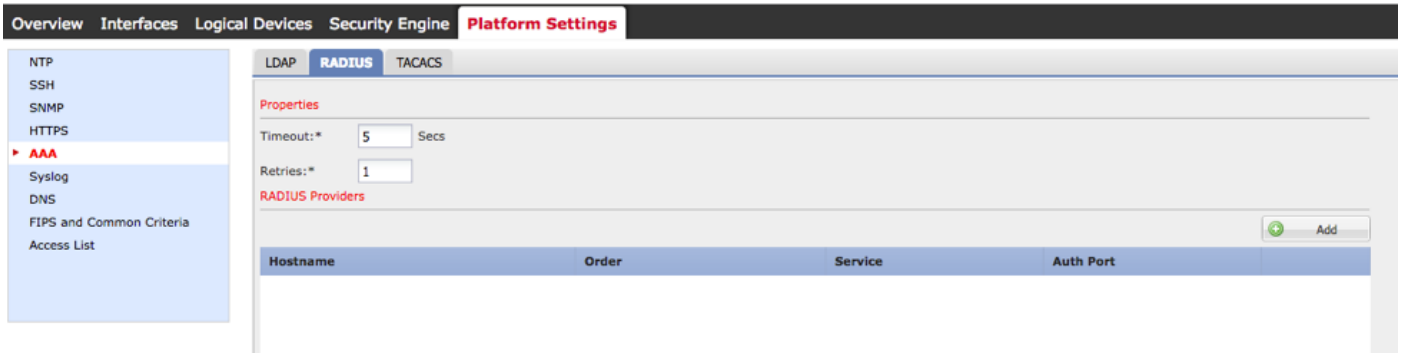

## Configuraciones

### 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 lengueta **RADIUS**.

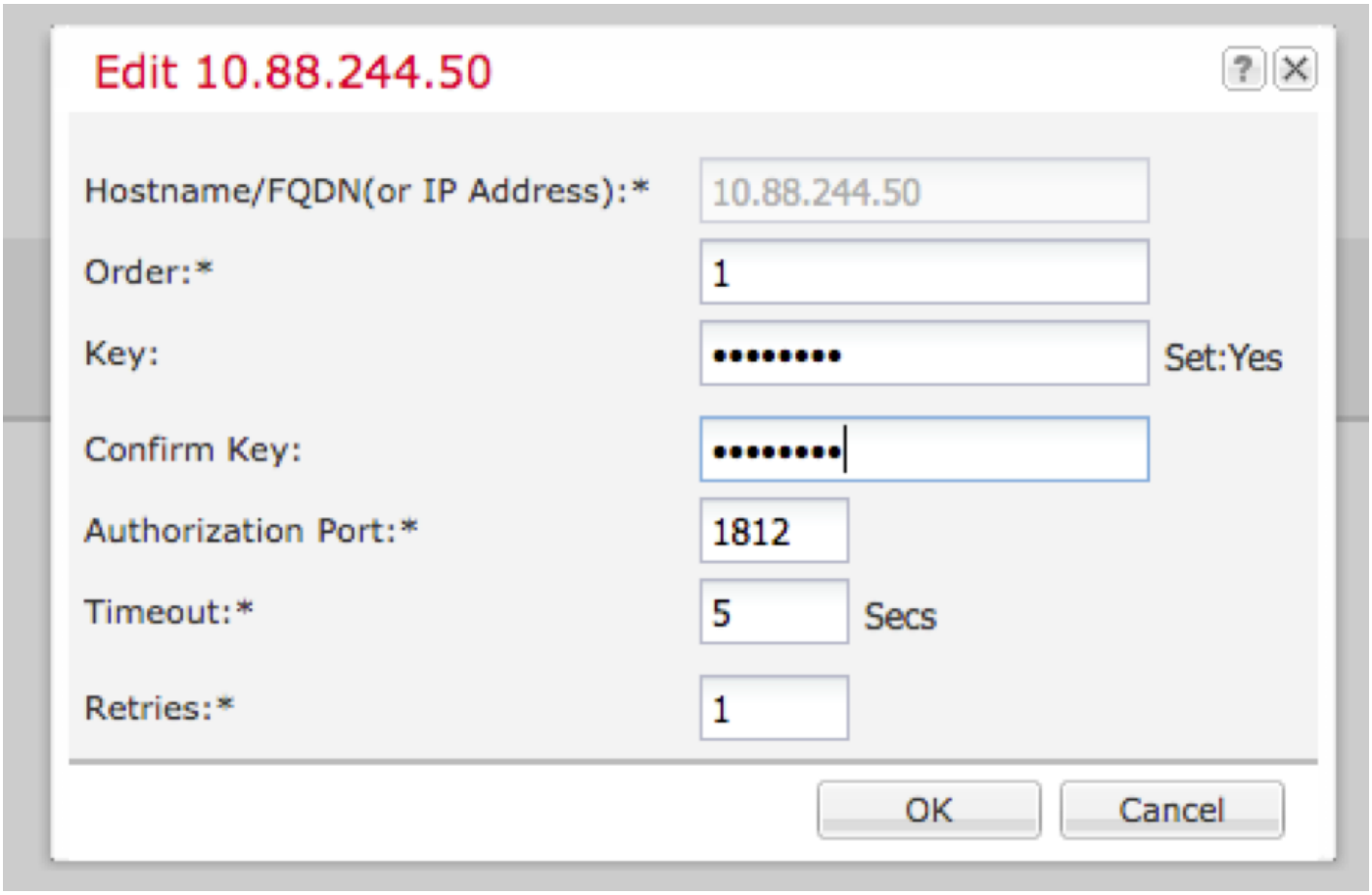



Paso 3. Para cada proveedor RADIUS que usted quiere agregar (hasta 16 proveedores).

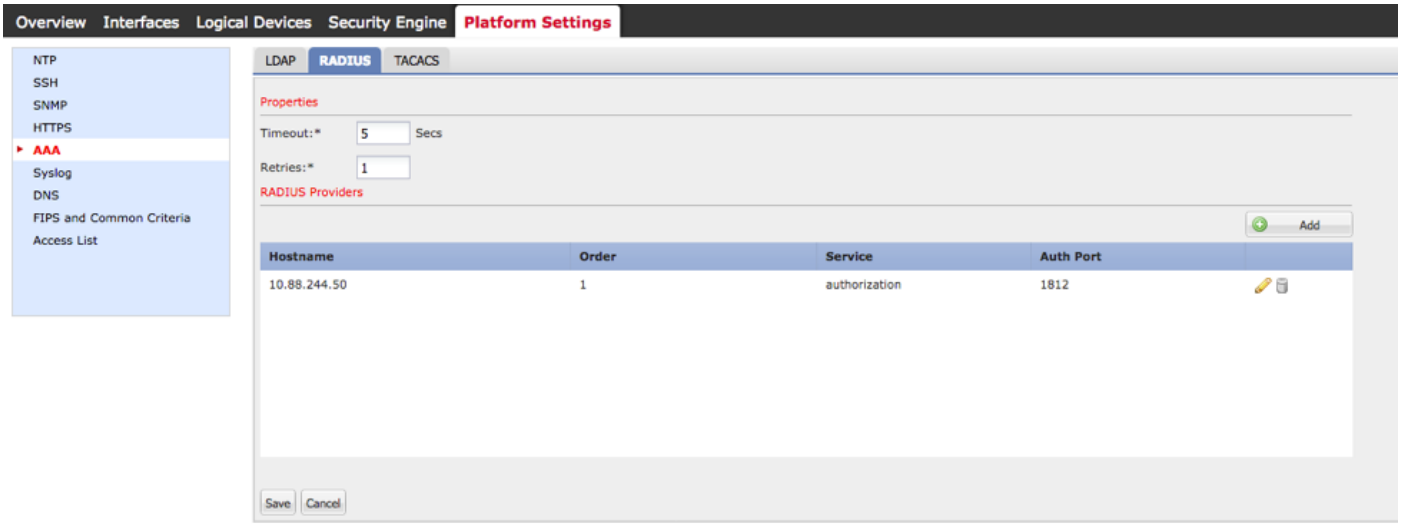
3.1. En el área de los proveedores RADIUS, haga click en Add

3.2. El cuadro de diálogo del proveedor del RADIO del agregar abre, ingresa una vez los valores requeridos.

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

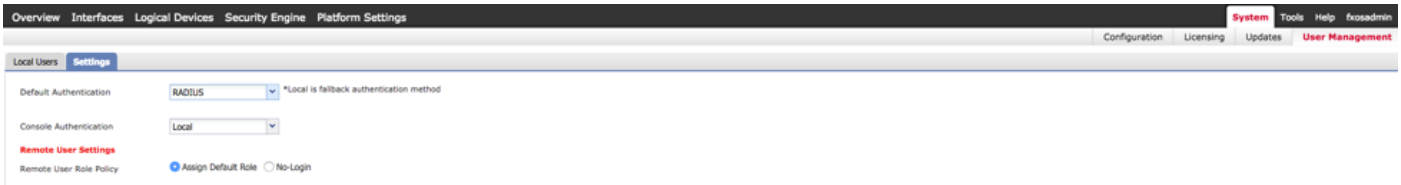



Paso 4. **Salvaguardia del** tecleo.




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 10.88.244.50**

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: 10.88.244.50

Descr:

Orden: 1

Puerto del auth: 1812

Clave: ****

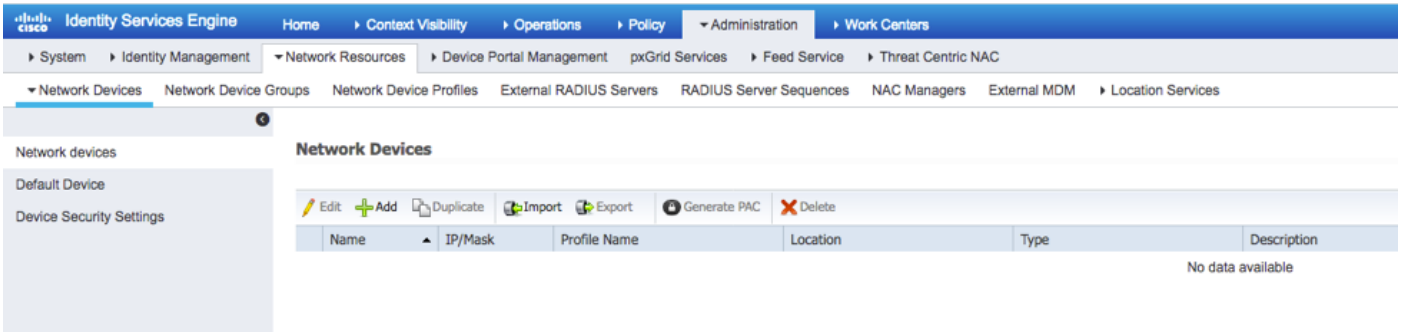
Descanso: 5

## Configurar el servidor ISE

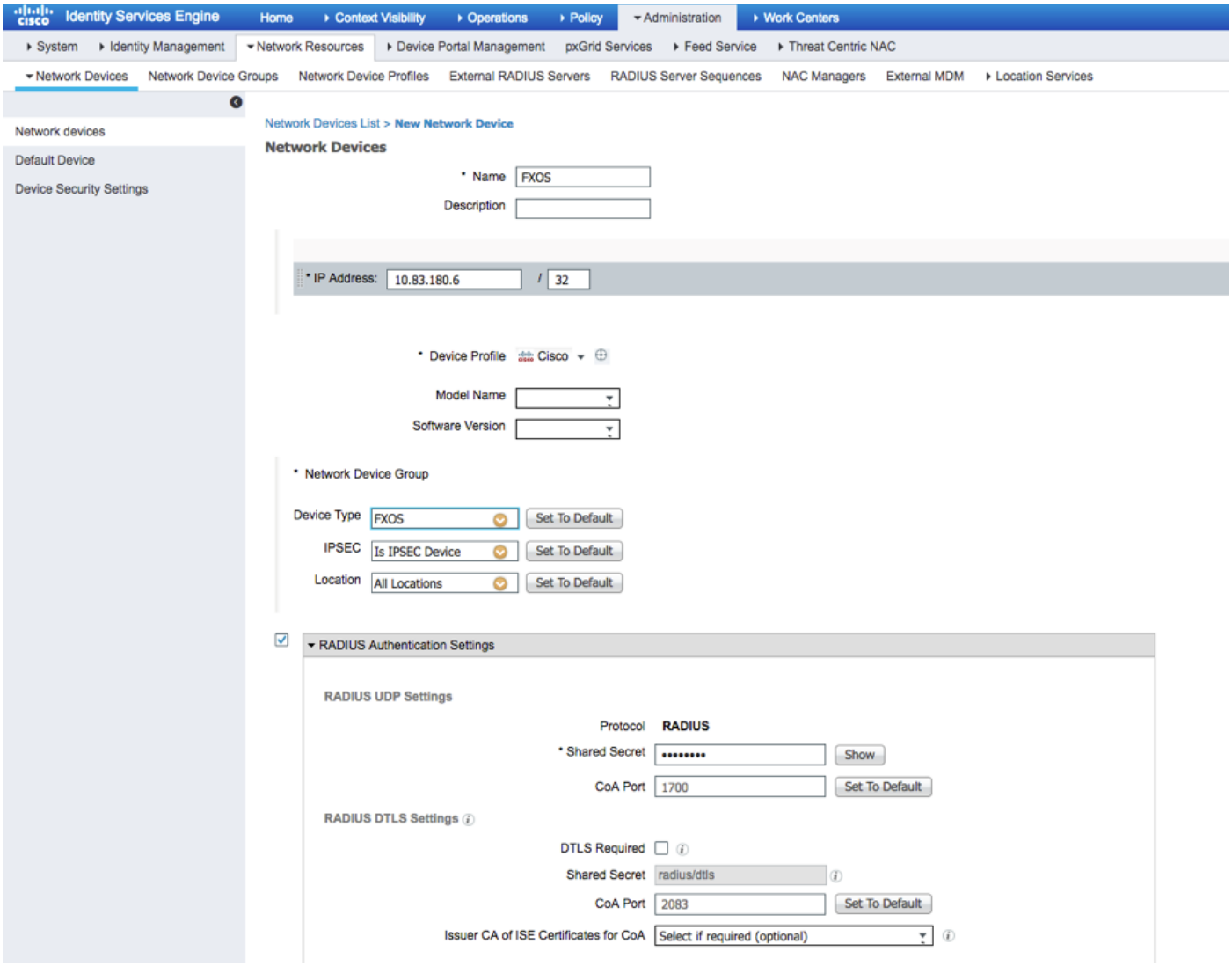
### Agregar los FXO como recurso de red

Paso 1. Navegue a la **administración > a los recursos de red > a los dispositivos de red**.

Paso 2. El tecleo **AGREGA**



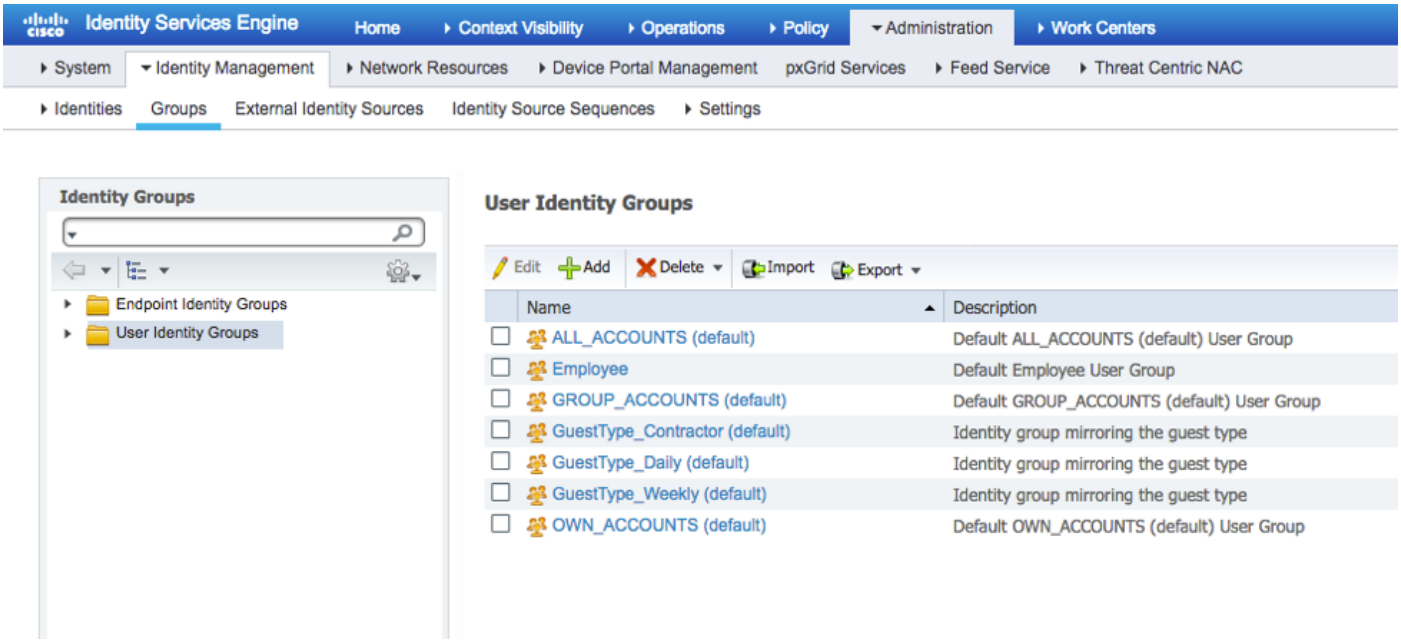

Paso 3. Ingrese los valores requeridos (el nombre, IP Address, tipo de dispositivo y habilita el RADIO y agrega la CLAVE), tecleo **someten.**



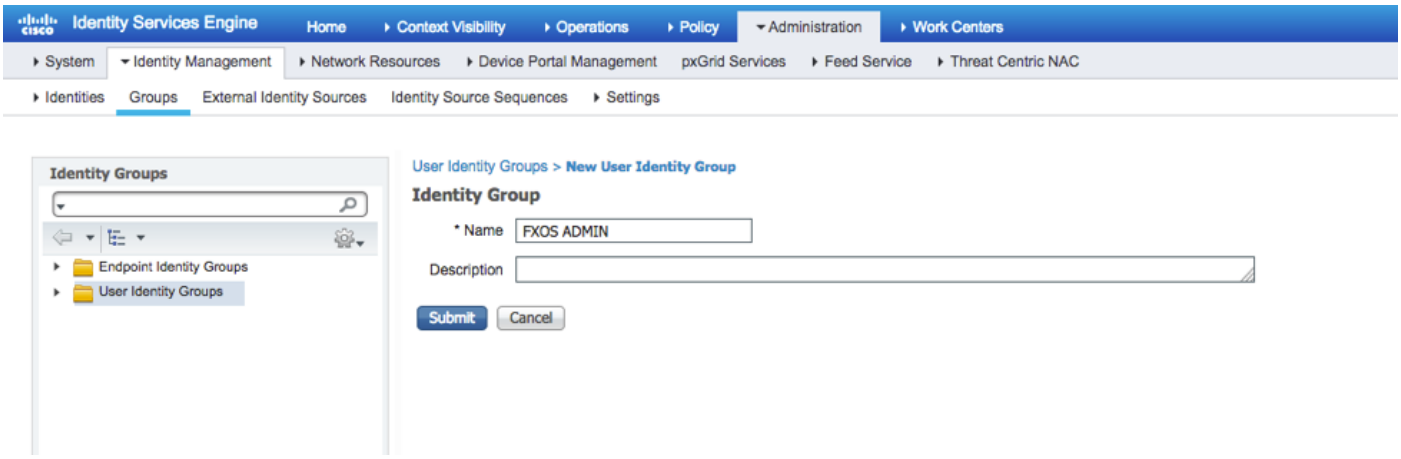

## Crear los grupos y a los usuarios de la identidad

Paso 1. Navegue a la **administración > a la Administración de la identidad > Groups > los grupos de la Identificación del usuario.**

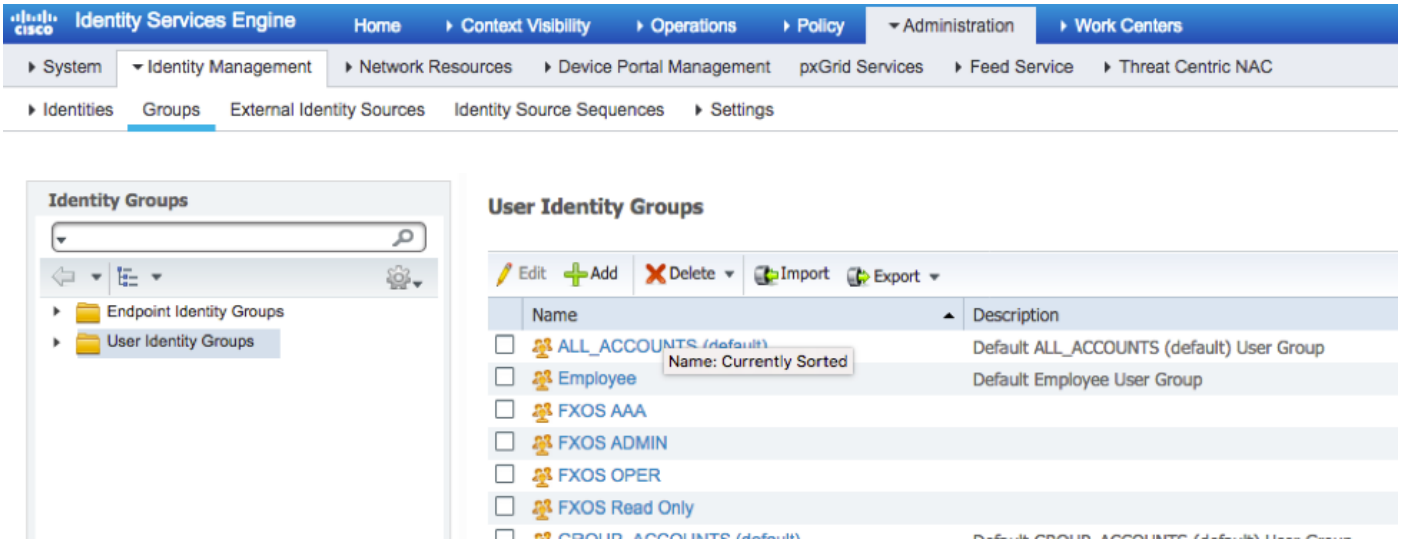
Paso 2. Haga click en Add



Paso 3. Ingrese el valor para el nombre y el tecleo **somete.**

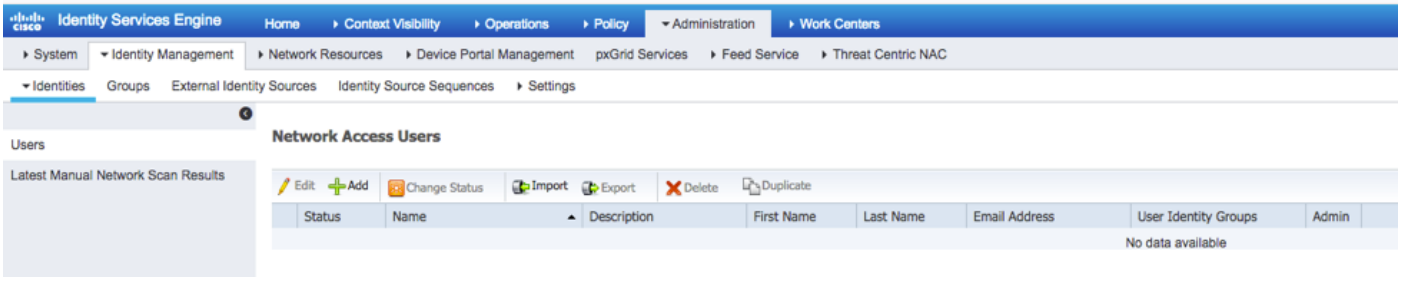



Paso 4. Relance el paso 3 para todos los rol del usuario requeridos.

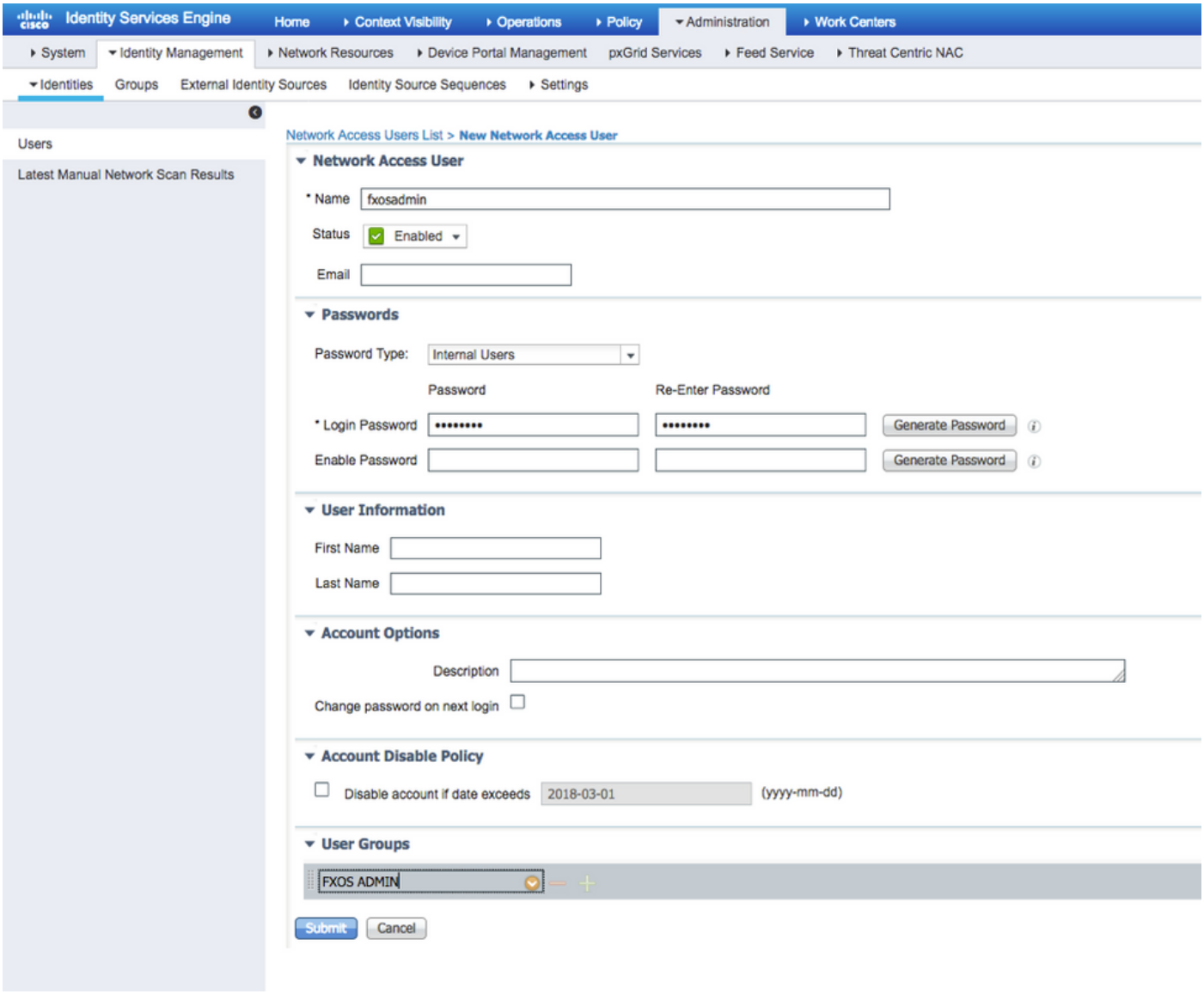



Paso 5. Navegue a la **administración > a la Administración de la identidad > a la identidad > Users.**

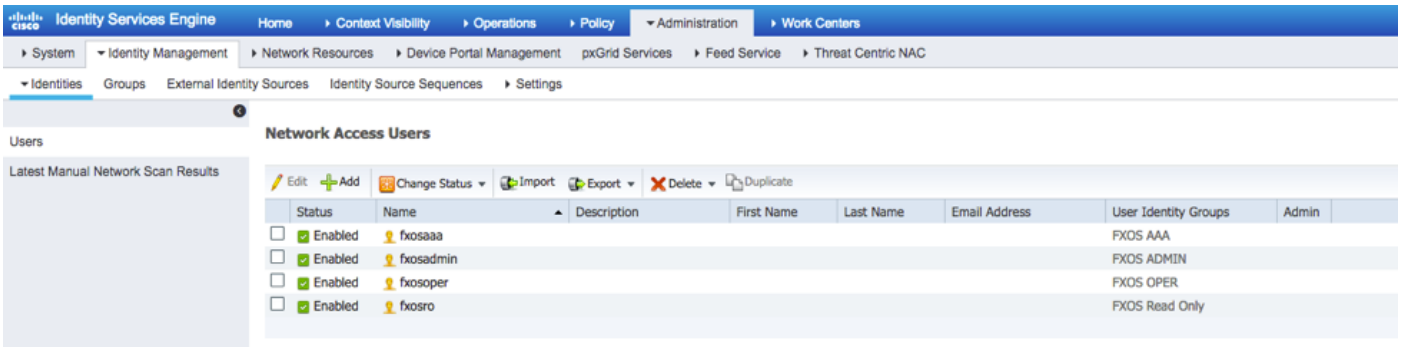
Paso 6. Haga click en Add




Paso 7. Ingrese los valores requeridos (nombre, grupo de usuarios, contraseña).

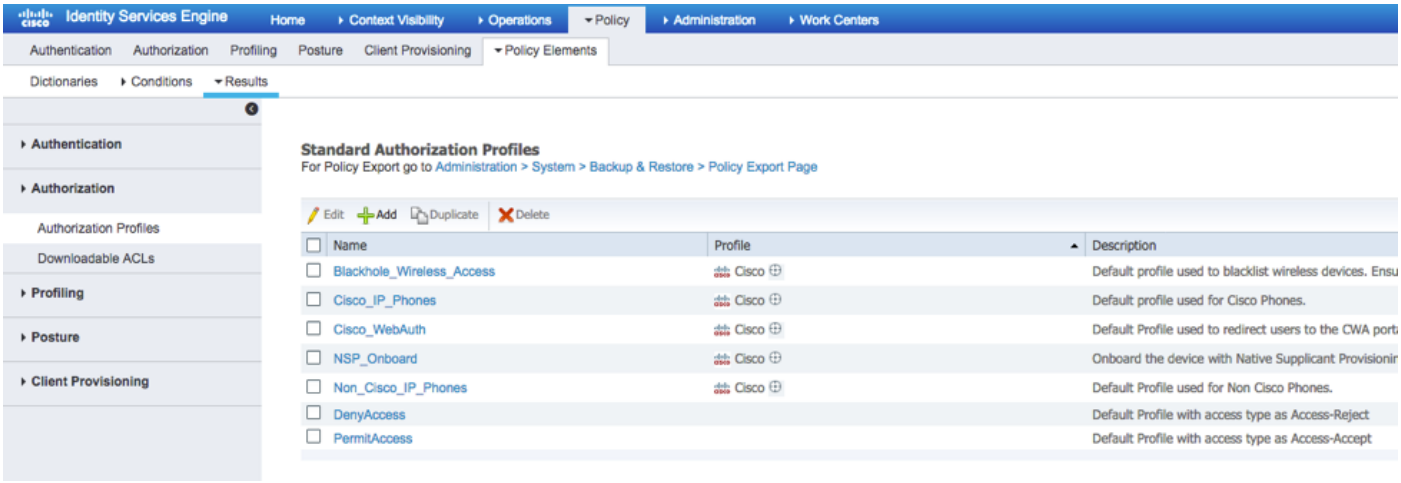



Paso 8. Relance el paso 6 para todos los usuarios requeridos.



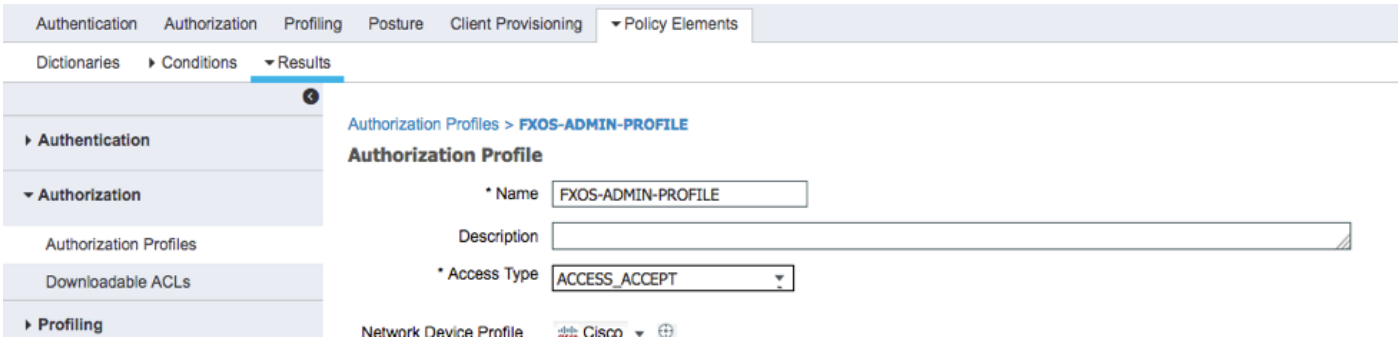

## Crear el perfil de la autorización para cada rol del usuario

Paso 1. Navegue a la **directiva > a los elementos de la directiva > a los resultados > a la autorización > a los perfiles de la autorización.**



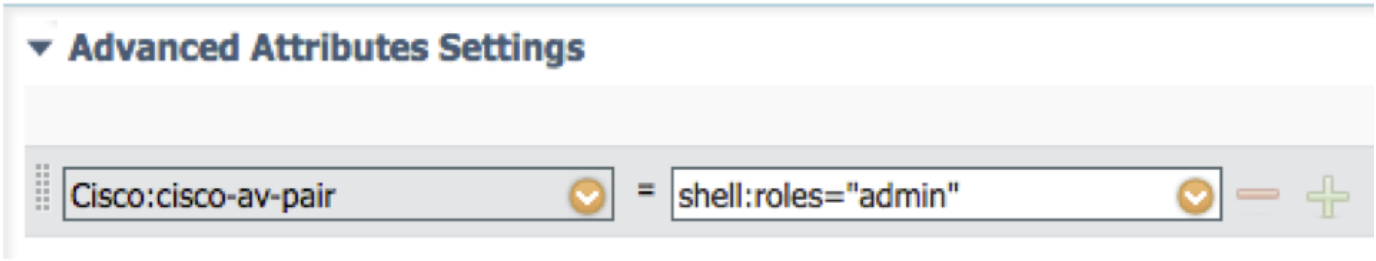

Paso 2. Llene todos los atributos para el perfil de la autorización.

2.1. Configure el nombre del perfil.

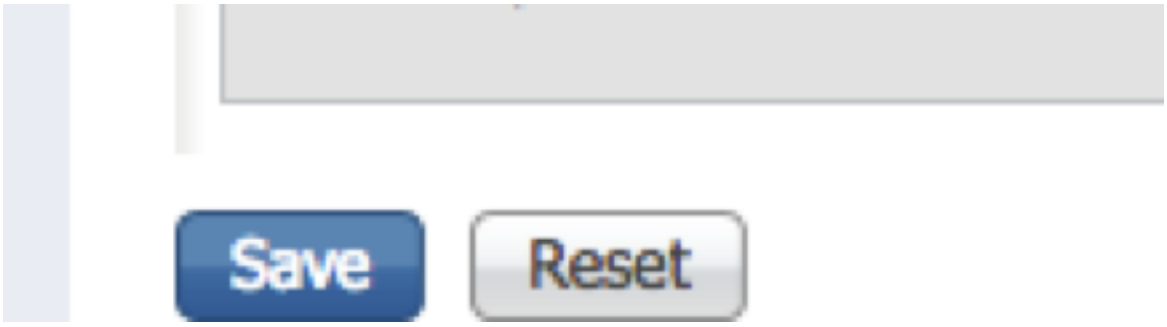



2.2. En las **configuraciones avanzadas de los atributos** configure el CISCO-AV-PAIR siguiente

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




2.3. Click **Save**.

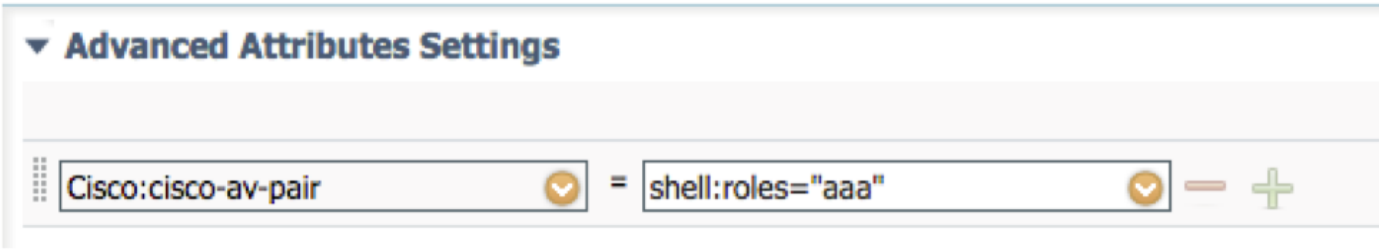


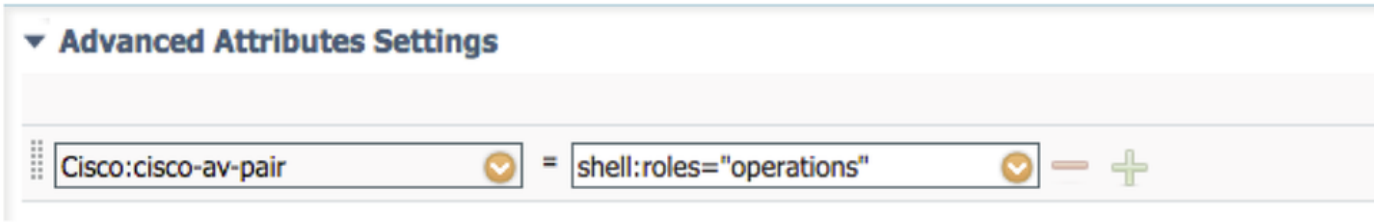
Paso 3. Relance el paso 2 para los rol del usuario restantes usando los cisco av-pair siguientes

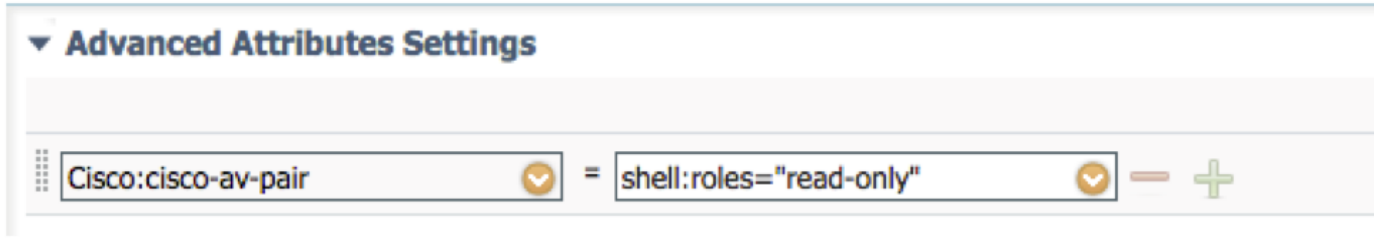
**cisco-av-pair=shell: roles= " aaa”**

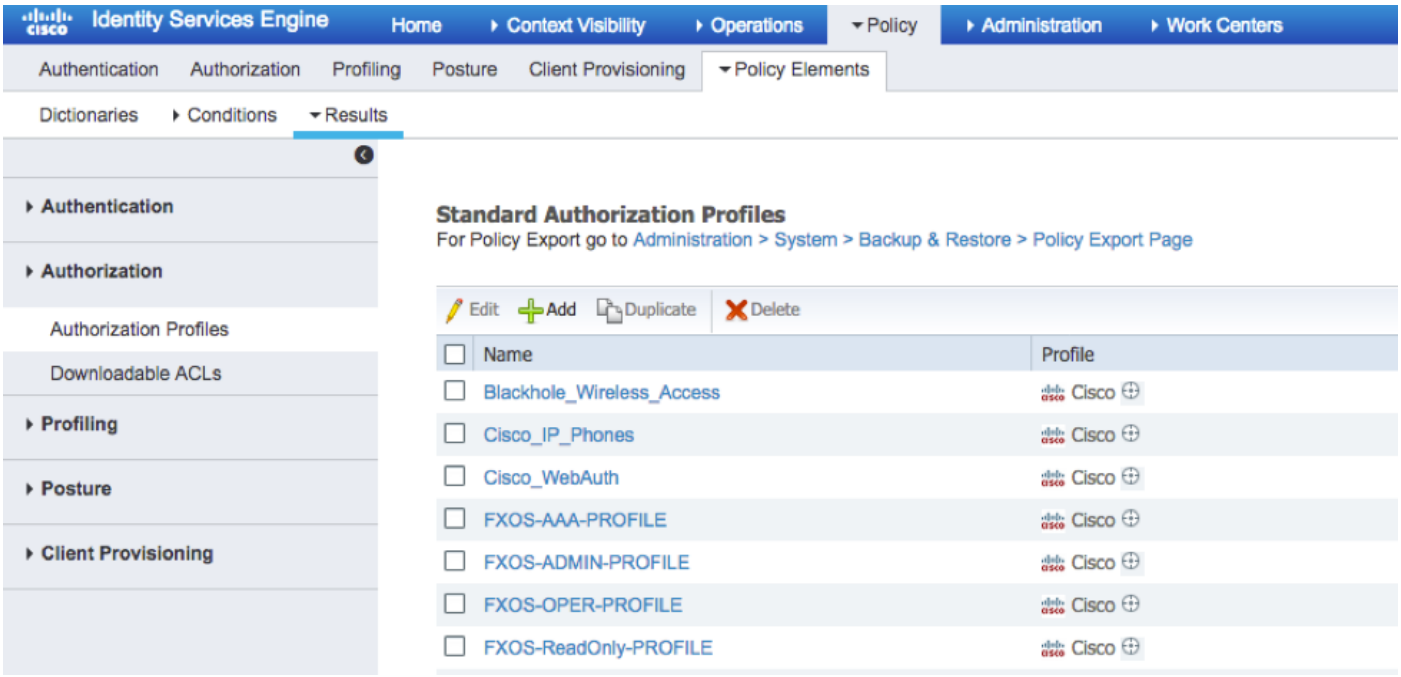
**cisco-av-pair=shell: roles= " operaciones”**

**cisco-av-pair=shell: roles= " solo lectura”**



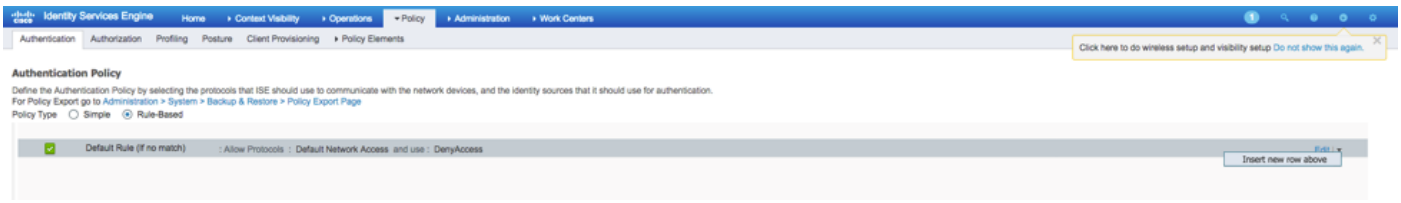



## Crear la política de autenticación

Paso 1. Navegue a la **directiva > a la autenticación >** y haga clic la flecha al lado de editan donde usted quiere crear la regla.



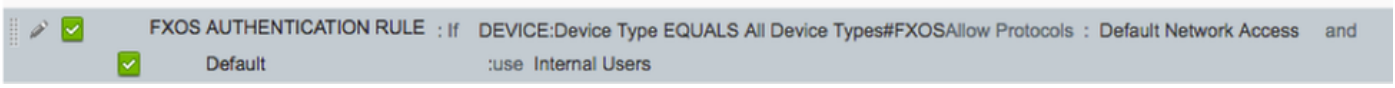

Paso 2. La configuración es simple; puede ser más granular hecho pero por este ejemplo utilizaremos el tipo de dispositivo:

Nombre: **REGLA DE LA AUTENTICACIÓN FXO**

SI nuevos atributo/valor selectos: **Dispositivo: El tipo de dispositivo iguala todos los tipos de dispositivos #FXOS**

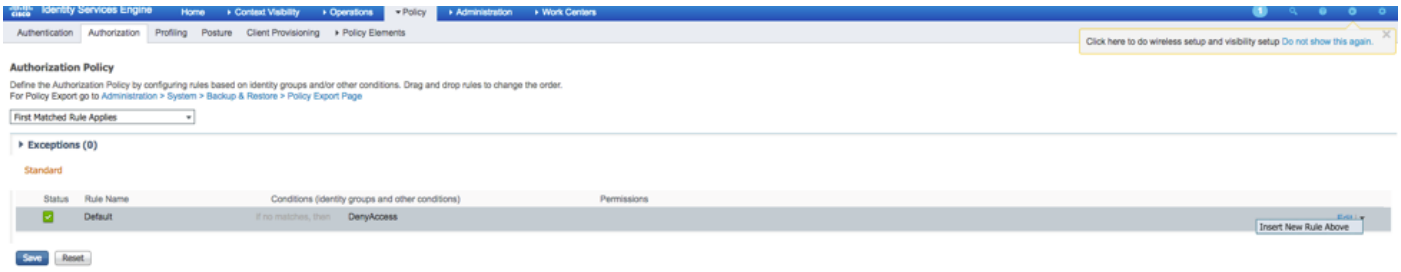
Permita los protocolos: Acceso de red predeterminada

Uso: Usuarios internos



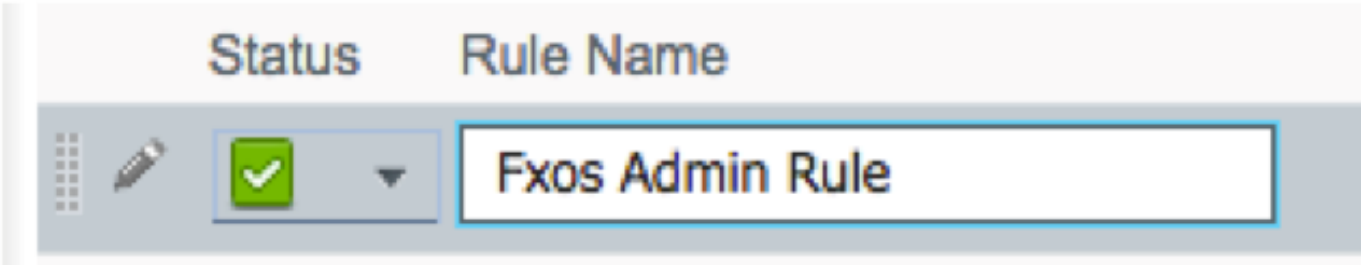

## Crear la directiva de la autorización

Paso 1. Navegue a la **directiva > a la autorización >** y haga clic la red de la flecha para editar donde usted quiere crear la regla.

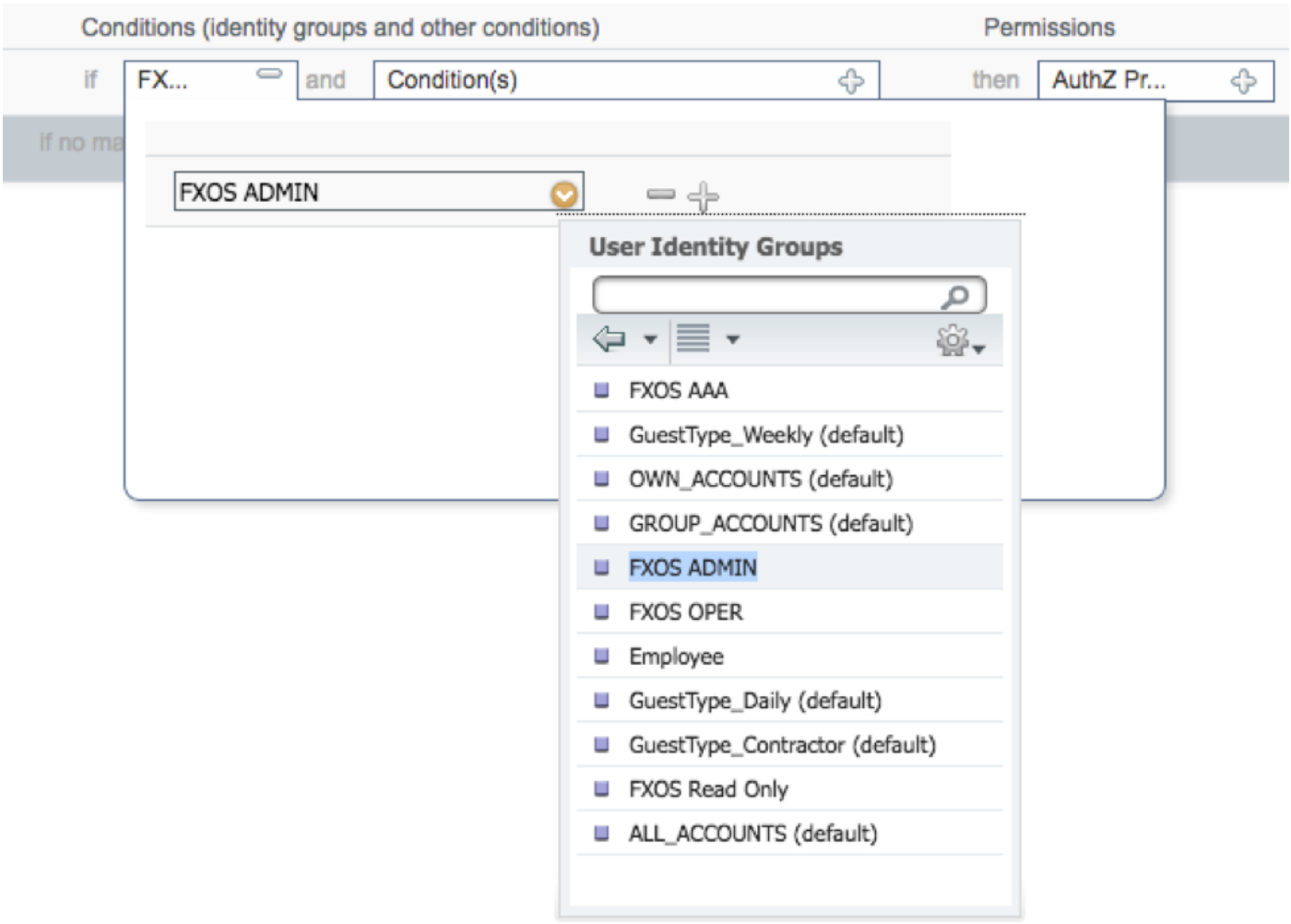



Paso 2. Ingrese los valores para la regla de la autorización con los parámetros obligatorios.

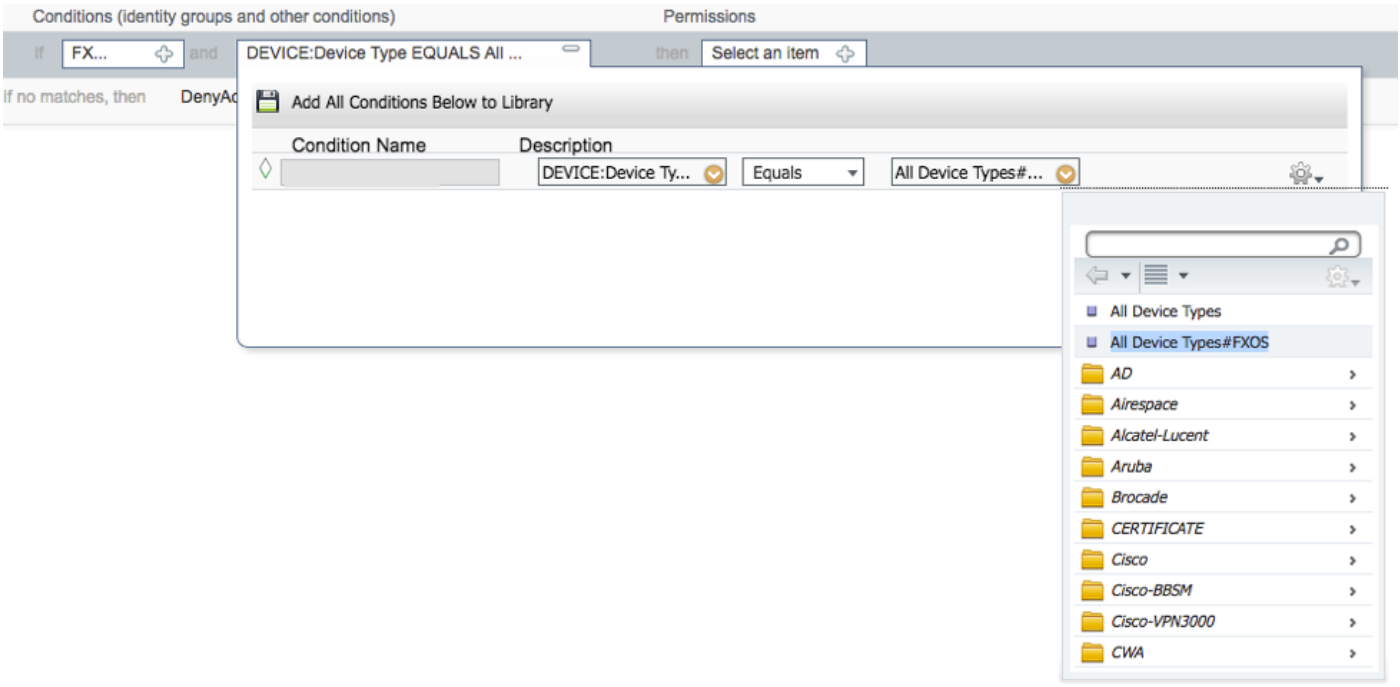
2.1. 'Nombre de la regla **Regla de Fxos <USER ROLE>.**



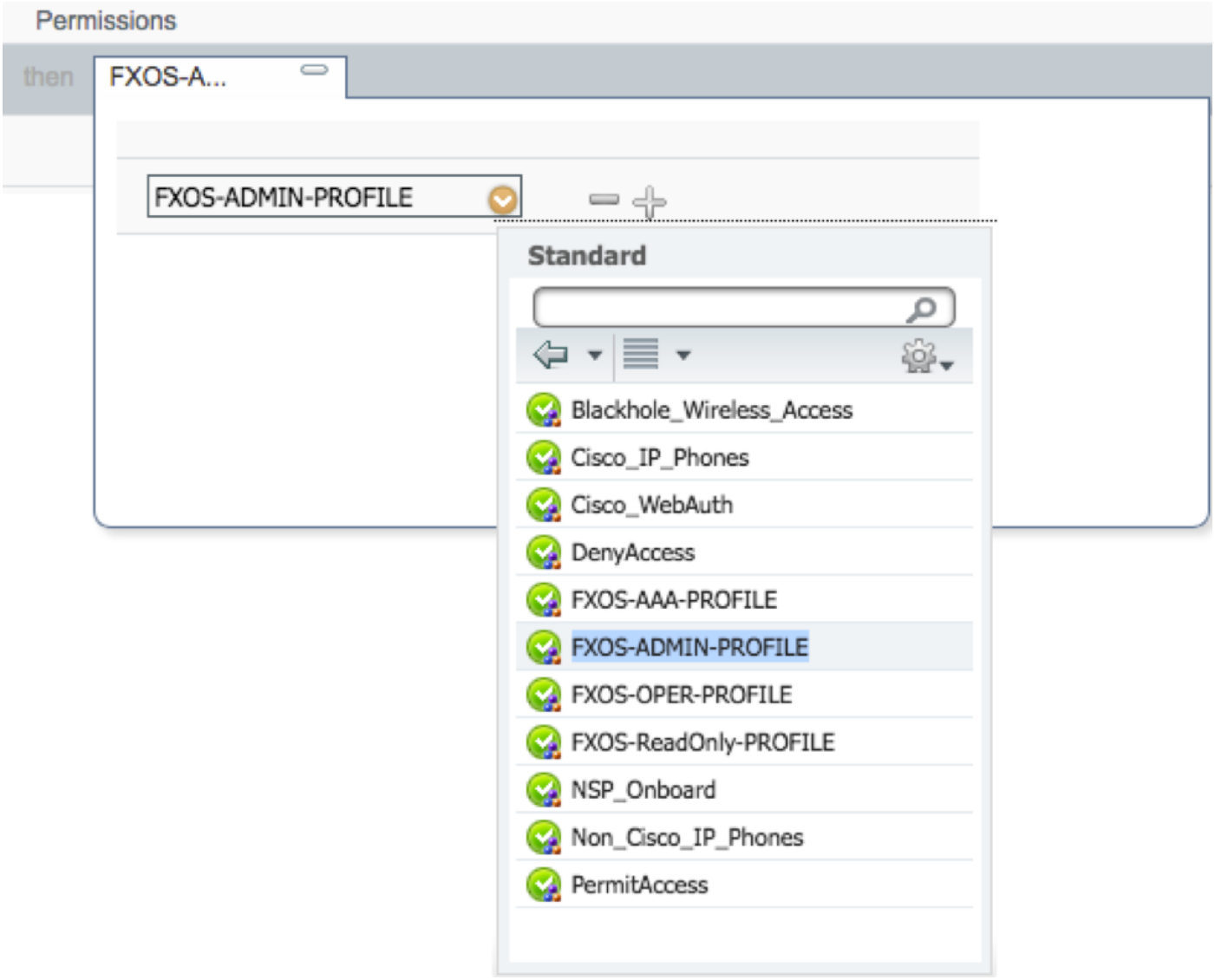

2.2. Si: Grupos de la Identificación del usuario > <USER selecto **ROLE>**.




2.3. Y: Cree la nuevos condición > dispositivo: El tipo de dispositivo iguala **todos los tipos de dispositivos #FXOS**.




2.4. Permisos: El estándar > elige el **rol del usuario del perfil**

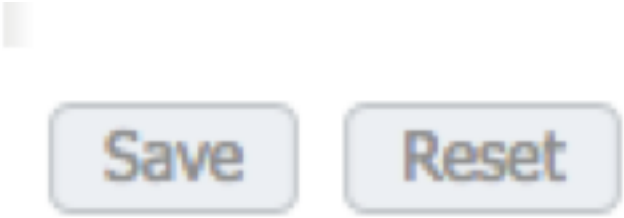



| Status | Rule Name | Conditions (identity groups and other conditions) | Permissions |
|---|---|---|---|
| ✓ | Fxos Admin Rule | if **FXOS ADMIN** AND DEVICE:Device Type EQUALS All Device Types#FXOS | then FXOS-ADMIN-PROFILE |

Paso 3. Relance el paso 2 para todos los rol del usuario.

| Status | Rule Name | Conditions (identity groups and other conditions) | Permissions |
|---|---|---|---|
| ✓ | Fxos Admin Rule | if **FXOS ADMIN** AND DEVICE:Device Type EQUALS All Device Types#FXOS | then FXOS-ADMIN-PROFILE |
| ✓ | Fxos AAA Rule | if **FXOS AAA** AND DEVICE:Device Type EQUALS All Device Types#FXOS | then FXOS-AAA-PROFILE |
| ✓ | Fxos Oper Rule | if **FXOS OPER** AND DEVICE:Device Type EQUALS All Device Types#FXOS | then FXOS-OPER-PROFILE |
| ✓ | Fxos Read only Rule | if **FXOS Read Only** AND DEVICE:Device Type EQUALS All Device Types#FXOS | then FXOS-ReadOnly-PROFILE |
| ✓ | Default | if no matches, then DenyAccess | |

Paso 4. **Salvaguardia del** tecleo en la parte inferior de la página.




# Verificación

Usted puede ahora probar a cada usuario y verificar el rol del usuario asignado.

### Verificación FXO Chasis

1. Telnet o SSH al chasis FXO y login usando los usuarios creados uces de los en el ISE.

Nombre de usuario: fxosadmin

Contraseña

**Seguridad del alcance** fpr4120-TAC-A#

fpr4120-TAC-A /security # **detalle del usuario remoto de la demostración**

**Fxosaaa del** usuario remoto:

Descripción:

Rol del usuario:

Nombre: **aaa**

Nombre: **sólo lectura**

**Fxosadmin del** usuario remoto:

Descripción:

Rol del usuario:

Nombre: **admin**

Nombre: **sólo lectura**

**Fxosoper del** usuario remoto:

Descripción:

Rol del usuario:

Nombre: **operaciones**

Nombre: **sólo lectura**

**Fxosro del** usuario remoto:

Descripción:

Rol del usuario:

Nombre: **sólo lectura**

Dependiendo del nombre de usuario ingresado el chasis FXO el cli visualizará solamente los comandos autorizados para el rol del usuario asignado.

Papel de Usuario administrador.

¿fpr4120-TAC-A /security **#?**

reconozca reconocen

las claro-usuario-sesiones borran a las sesiones del usuario

cree crean los objetos administrados

borre los objetos administrados de la cancelación

la neutralización inhabilita los servicios

el permiso habilita los servicios

ingrese ingresa un objeto administrado

el alcance cambia al modo actual

fije los valores de propiedad determinados

muestre la información del sistema de la demostración

termine las sesiones del Active cimc

fpr4120-TAC-A**# conectan los fxos**

fpr4120-TAC-A (fxos) # AAA-**peticiones aaa del debug**

fpr4120-TAC-A (fxos) #

Rol del usuario solo lectura.

¿fpr4120-TAC-A /security **#?**

el alcance cambia al modo actual

fije los valores de propiedad determinados

muestre la información del sistema de la demostración

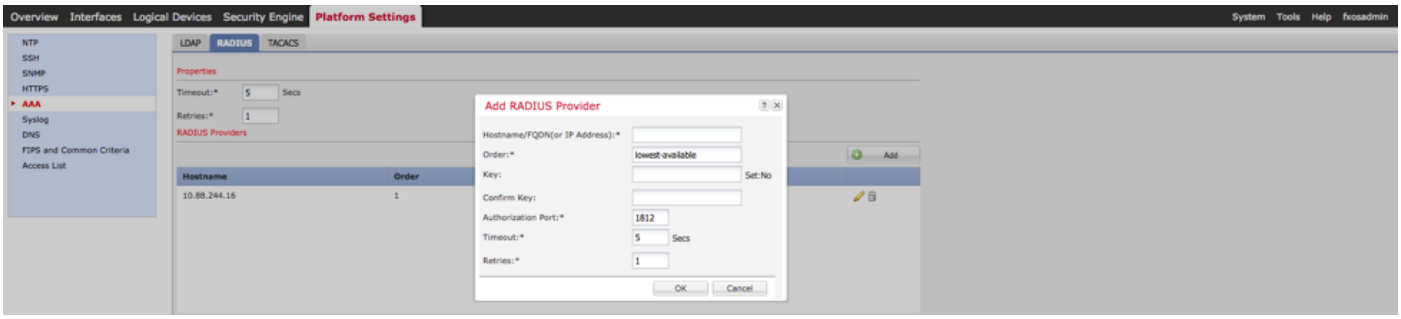
fpr4120-TAC-A# **conectan los fxos**

fpr4120-TAC-A (fxos) # AAA-**peticiones aaa del debug**

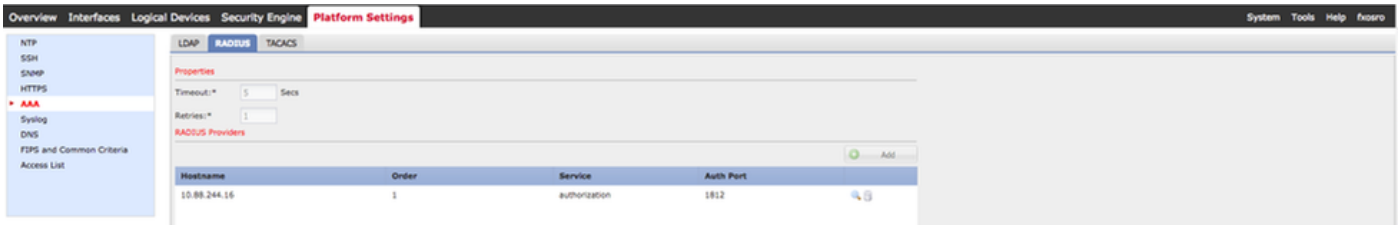
% del permiso negado para el papel

2. Hojee a la dirección IP y al login del chasis FXO usando los usuarios creados uces de los en el ISE.

Papel de Usuario administrador.



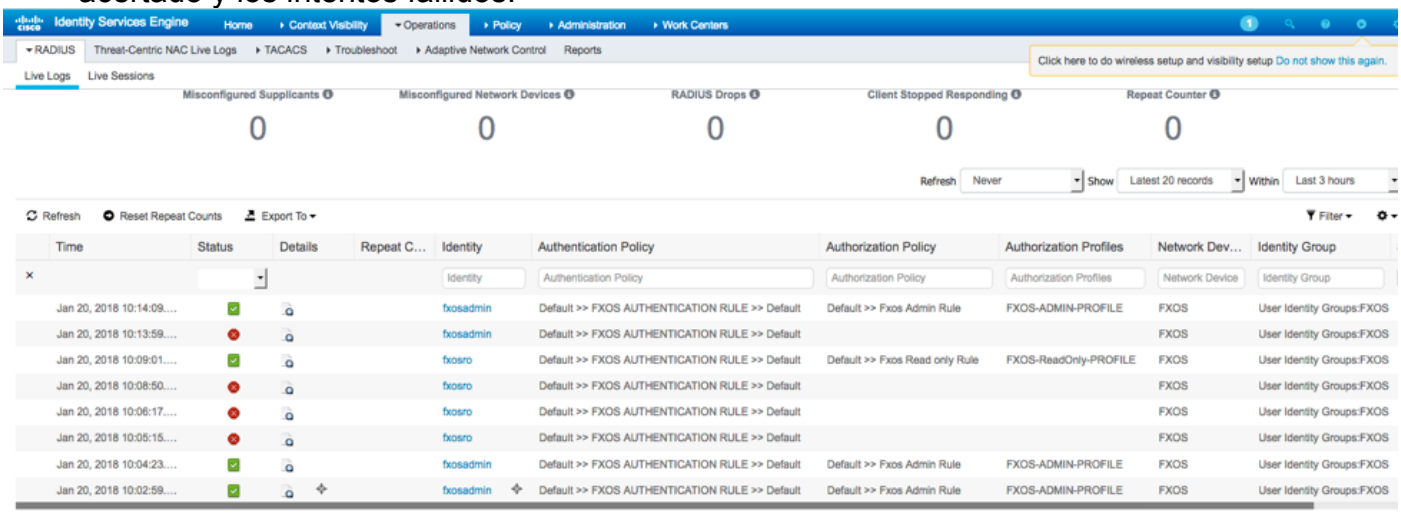

Rol del usuario solo lectura.




**Note**: Note que el **botón Add** es greyed hacia fuera.

## Verificación ISE 2.0

1. Navegue a las **operaciones > al RADIUS > los registros vivos.** Usted debe poder ver acertado y los intentos fallidos.



# Troubleshooting

Para hacer el debug de la autenticación AAA y la autorización funcione con los siguientes comandos en los FXO cli.

fpr4120-TAC-A# **conectan los fxos**

fpr4120-TAC-A (fxos) # AAA-**peticiones aaa del debug**

fpr4120-TAC-A (fxos) # **evento aaa del debug**

fpr4120-TAC-A (fxos) # **errores aaa del debug**

fpr4120-TAC-A (fxos) # **término lunes**

Después de que una tentativa de la autenticación satisfactoria, usted considere el producto siguiente.

2018 20 de enero 17:18:02.410275 aaa: aaa_req_process para la autenticación. sesión ningún 0

2018 20 de enero 17:18:02.410297 aaa: aaa_req_process: Petición general AAA del appln: appln_subtype del login: predeterminado

2018 20 de enero 17:18:02.410310 aaa: try_next_aaa_method

2018 20 de enero 17:18:02.410330 aaa: los métodos totales configurados son 1, índice actual que se intentará son 0

2018 20 de enero 17:18:02.410344 aaa: handle_req_using_method

2018 20 de enero 17:18:02.410356 aaa: AAA_METHOD_SERVER_GROUP

2018 20 de enero 17:18:02.410367 aaa: grupo = radio del aaa_sg_method_handler

2018 20 de enero 17:18:02.410379 aaa: Usando el sg_protocol que se pasa a esta función

2018 20 de enero 17:18:02.410393 aaa: Envío de la petición al servicio RADIUS

2018 20 de enero 17:18:02.412944 aaa: mts_send_msg_to_prot_daemon: Magnitud de carga útil = 374

2018 20 de enero 17:18:02.412973 aaa: sesión: 0x8dfd68c agregado al cuadro 1 de la sesión

2018 20 de enero 17:18:02.412987 aaa: Grupo configurado del método tenido éxito

2018 20 de enero 17:18:02.656425 aaa: aaa_process_fd_set

2018 20 de enero 17:18:02.656447 aaa: aaa_process_fd_set: mtscallback en el aaa_q

2018 20 de enero 17:18:02.656470 aaa: mts_message_response_handler: una respuesta de los mts

2018 20 de enero 17:18:02.656483 aaa: prot_daemon_reponse_handler

2018 20 de enero 17:18:02.656497 aaa: sesión: 0x8dfd68c quitado del cuadro 0 de la sesión

2018 20 de enero 17:18:02.656512 aaa: estatus de los is_aaa_resp_status_success = 1

2018 20 de enero 17:18:02.656525 aaa: los is_aaa_resp_status_success son VERDADES

2018 20 de enero 17:18:02.656538 aaa: aaa_send_client_response para la autenticación. session->flags=21. aaa_resp->flags=0.

2018 20 de enero 17:18:02.656550 aaa: AAA_REQ_FLAG_NORMAL

2018 20 de enero 17:18:02.656577 aaa: mts_send_response acertado

2018 20 de enero 17:18:02.700520 aaa: aaa_process_fd_set: mtscallback en el aaa_accounting_q

2018 20 de enero 17:18:02.700688 aaa: OPCODE VIEJO: accounting_interim_update

2018 20 de enero 17:18:02.700702 aaa: aaa_create_local_acct_req: user=, session_id=, fxosro log=added del usuario

2018 20 de enero 17:18:02.700725 aaa: aaa_req_process para considerar. sesión ningún 0

2018 20 de enero 17:18:02.700738 aaa: La referencia de la petición MTS es NULA. Petición LOCAL

2018 20 de enero 17:18:02.700749 aaa: Determinación de AAA_REQ_RESPONSE_NOT_NEEDED

2018 20 de enero 17:18:02.700762 aaa: aaa_req_process: Petición general AAA del appln: appln_subtype predeterminado: predeterminado

2018 20 de enero 17:18:02.700774 aaa: try_next_aaa_method

2018 20 de enero 17:18:02.700798 aaa: ningunos métodos configurados para el valor por defecto del valor por defecto

2018 20 de enero 17:18:02.700810 aaa: ninguna configuración disponible para esto petición

2018 20 de enero 17:18:02.700997 aaa: aaa_send_client_response para considerar. session->flags=254. aaa_resp->flags=0.

2018 20 de enero 17:18:02.701010 aaa: la respuesta para la petición que considera de la biblioteca vieja será enviada como ÉXITO

2018 20 de enero 17:18:02.701021 aaa: respuesta no necesaria para esta petición

2018 20 de enero 17:18:02.701033 aaa: AAA_REQ_FLAG_LOCAL_RESP

2018 20 de enero 17:18:02.701044 aaa: aaa_cleanup_session

2018 20 de enero 17:18:02.701055 aaa: el aaa_req debe ser liberado.

2018 20 de enero 17:18:02.701067 aaa: Cae detrás el local del método tenido éxito

2018 20 de enero 17:18:02.706922 aaa: aaa_process_fd_set

2018 20 de enero 17:18:02.706937 aaa: aaa_process_fd_set: mtscallback en el aaa_accounting_q

2018 20 de enero 17:18:02.706959 aaa: OPCODE VIEJO: accounting_interim_update

2018 20 de enero 17:18:02.706972 aaa: aaa_create_local_acct_req: user=, session_id=, usuario log=added: fxosro al papel: sólo lectura

Después de que una tentativa de la autenticación fallida, usted considere el producto siguiente.

2018 20 de enero 17:15:18.102130 aaa: aaa_process_fd_set

2018 20 de enero 17:15:18.102149 aaa: aaa_process_fd_set: mtscallback en el aaa_q

2018 20 de enero 17:15:18.102267 aaa: aaa_process_fd_set

2018 20 de enero 17:15:18.102281 aaa: aaa_process_fd_set: mtscallback en el aaa_q

2018 20 de enero 17:15:18.102363 aaa: aaa_process_fd_set

2018 20 de enero 17:15:18.102377 aaa: aaa_process_fd_set: mtscallback en el aaa_q

2018 20 de enero 17:15:18.102456 aaa: aaa_process_fd_set

2018 20 de enero 17:15:18.102468 aaa: aaa_process_fd_set: mtscallback en el aaa_q

2018 20 de enero 17:15:18.102489 aaa: mts_aaa_req_process

2018 20 de enero 17:15:18.102503 aaa: aaa_req_process para la autenticación. sesión ningún 0

2018 20 de enero 17:15:18.102526 aaa: aaa_req_process: Petición general AAA del appln: appln_subtype del login: predeterminado

2018 20 de enero 17:15:18.102540 aaa: try_next_aaa_method

2018 20 de enero 17:15:18.102562 aaa: los métodos totales configurados son 1, índice actual que se intentará son 0

2018 20 de enero 17:15:18.102575 aaa: handle_req_using_method

2018 20 de enero 17:15:18.102586 aaa: AAA_METHOD_SERVER_GROUP

2018 20 de enero 17:15:18.102598 aaa: grupo = radio del aaa_sg_method_handler

2018 20 de enero 17:15:18.102610 aaa: Usando el sg_protocol que se pasa a esta función

2018 20 de enero 17:15:18.102625 aaa: Envío de la petición al servicio RADIUS

2018 20 de enero 17:15:18.102658 aaa: mts_send_msg_to_prot_daemon: Magnitud de carga útil = 371

2018 20 de enero 17:15:18.102684 aaa: sesión: 0x8dfd68c agregado al cuadro 1 de la sesión

2018 20 de enero 17:15:18.102698 aaa: Grupo configurado del método tenido éxito

2018 20 de enero 17:15:18.273682 aaa: aaa_process_fd_set

2018 20 de enero 17:15:18.273724 aaa: aaa_process_fd_set: mtscallback en el aaa_q

2018 20 de enero 17:15:18.273753 aaa: mts_message_response_handler: una respuesta de los mts

2018 20 de enero 17:15:18.273768 aaa: prot_daemon_reponse_handler

2018 20 de enero 17:15:18.273783 aaa: sesión: 0x8dfd68c quitado del cuadro 0 de la sesión

2018 20 de enero 17:15:18.273801 aaa: estatus de los is_aaa_resp_status_success = 2

2018 20 de enero 17:15:18.273815 aaa: los is_aaa_resp_status_success son VERDADES

2018 20 de enero 17:15:18.273829 aaa: aaa_send_client_response para la autenticación. session->flags=21. aaa_resp->flags=0.

2018 20 de enero 17:15:18.273843 aaa: AAA_REQ_FLAG_NORMAL

2018 20 de enero 17:15:18.273877 aaa: mts_send_response acertado

2018 20 de enero 17:15:18.273902 aaa: aaa_cleanup_session

2018 20 de enero 17:15:18.273916 aaa: mts_drop de los msg de la petición

2018 20 de enero 17:15:18.273935 aaa: el aaa_req debe ser liberado.

2018 20 de enero 17:15:18.280416 aaa: aaa_process_fd_set

2018 20 de enero 17:15:18.280443 aaa: aaa_process_fd_set: mtscallback en el aaa_q

2018 20 de enero 17:15:18.280454 aaa: aaa_enable_info_config: GET_REQ para el mensaje de error del login aaa

2018 20 de enero 17:15:18.280460 aaa: conseguido detrás el valor devuelto de la operación de la configuración: elemento desconocido de la Seguridad

# Información Relacionada

El comando de Ethanalyzer en FX-OS cli indicará para la contraseña para una contraseña cuando se habilita la autenticación TACACS/RADIUS. Este comportamiento es causado por un bug.

ID de bug: CSCvg87518