

Configuración de la autenticación RADIUS de ISE para el administrador de chasis de firewall seguro (FCM)

Contenido

Introducción

Este documento describe el proceso de configuración del acceso de autorización/autenticación Radius para Secure Firewall Chassis Manager con ISE.

Prerequisites

Requirements

Cisco recomienda tener conocimiento de los siguientes temas:

- Administrador de chasis de firewall seguro (FCM)
- Cisco Identity Services Engine (ISE)
- Autenticación RADIUS

Componentes Utilizados

- Dispositivo de seguridad Cisco Firepower 4110 FXOS v2.12
- Cisco Identity Services Engine (ISE) v3.2, parche 4

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Configuraciones

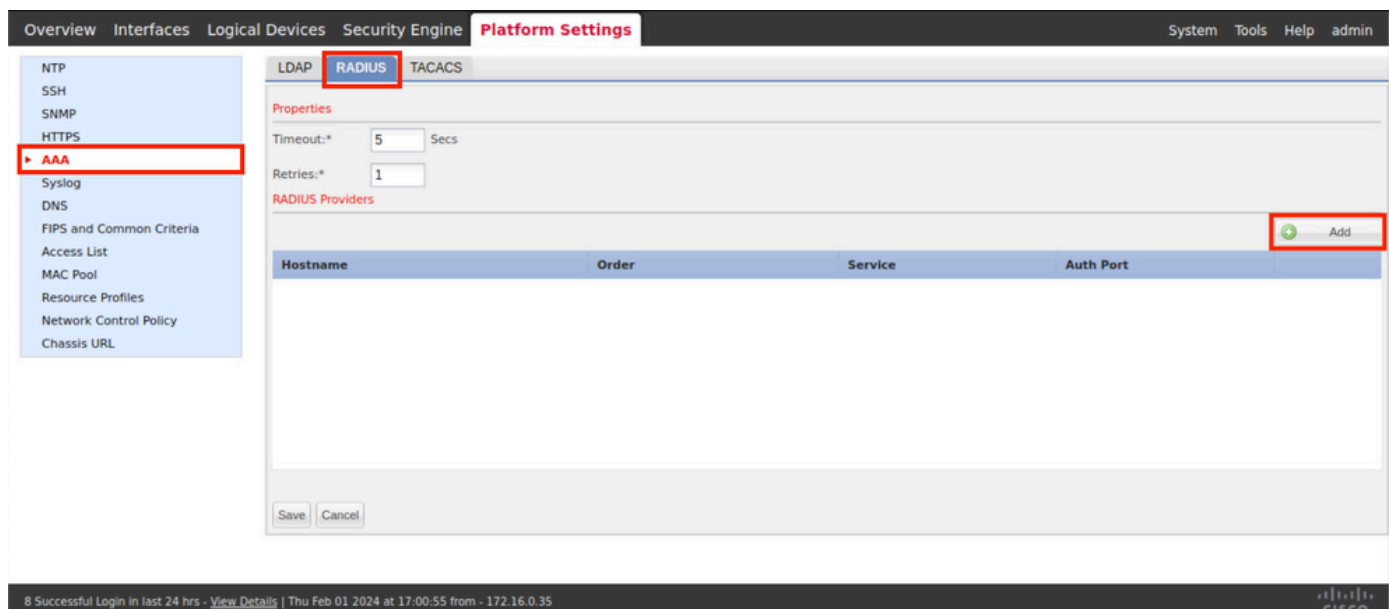
Administrador de chasis de firewall seguro

Paso 1. Inicie sesión en la GUI de Firepower Chassis Manager.

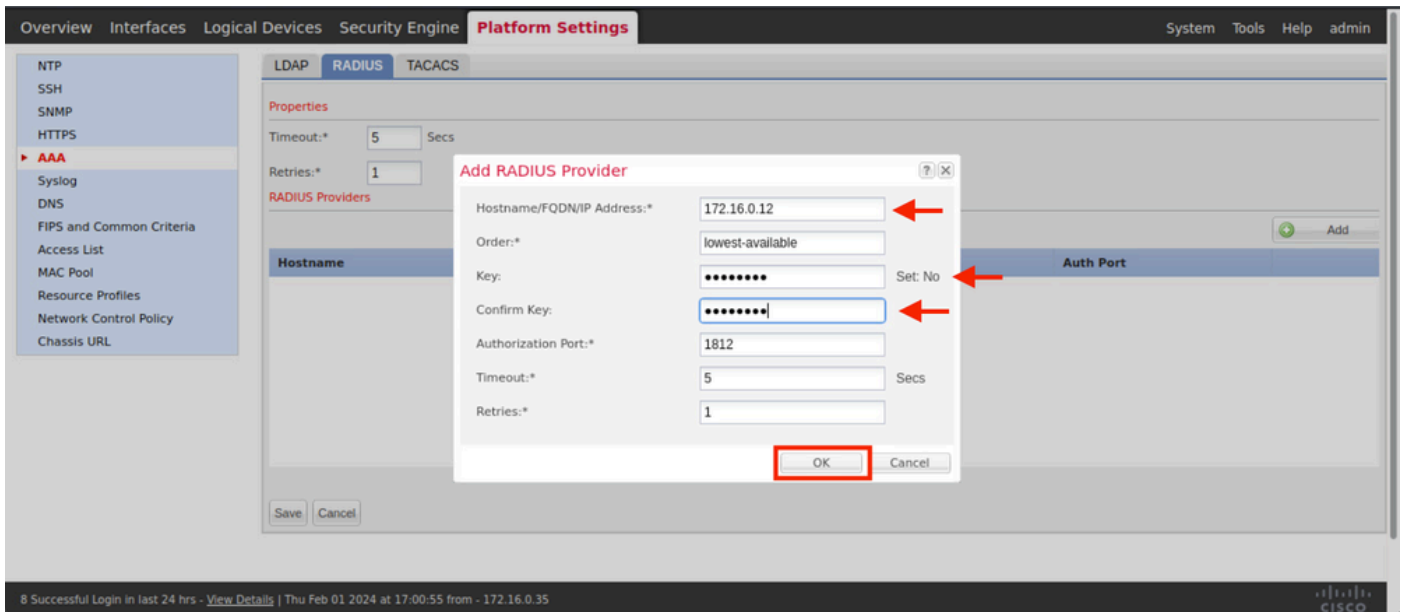
Paso 2. Vaya a Configuración de la plataforma



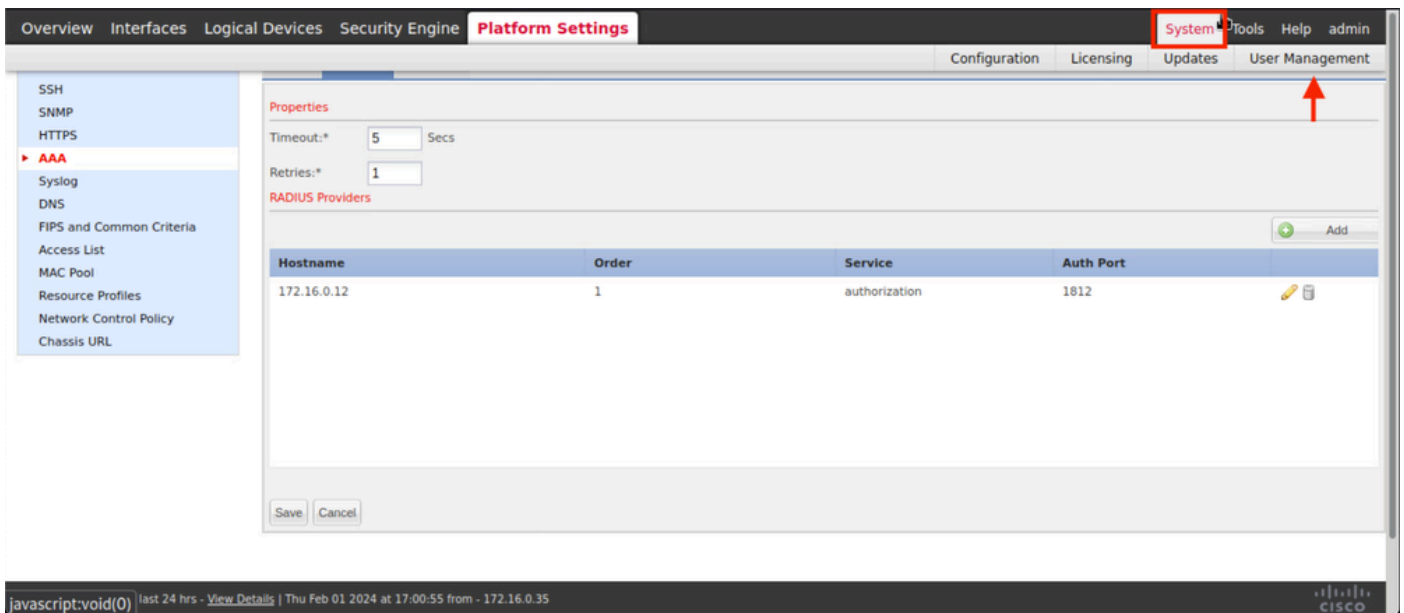
Paso 3. En el menú de la izquierda, haga clic sobre AAA. Seleccione Radius y Add a new RADIUS provider.



Paso 4. Rellene el menú de prompt con la información solicitada del proveedor de Radius. Click OK.



Paso 5. Vaya a System > User Management .



Paso 6. Haga clic en la ficha Settings (Parámetros) y establezca Default Authentication (Autenticación predeterminada) en el menú desplegable Radius. A continuación, desplácese hacia abajo y guarde la configuración.


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

Configuration Licensing Updates **User Management**

Local Users **Settings**

Default Authentication

Local *Local is fallback authentication method

Local
RADIUS 
LDAP
TACACS
None
No-Login

Console Authentication

Remote User Settings

Remote User Role Policy

Local User Settings

Password Strength Check Enable

History Count (0-disabled,1-15)

Change Interval (1-730 hours)

Change Count (1-10)

No Change Interval (1-730 hours)

Days until Password Expiration (0-never,1-9999 days)

Password Expiration Warning Period (0-9999 days)

Expiration Grace Period (0-9999 days)

Password Reuse Interval (0-disabled,1-365 days)

Session Timeout(web UI,ssh,telnet) (0-never,3600 seconds)

8 Successful Login in last 24 hrs - [View Details](#) | Thu Feb 01 2024 at 17:00:55 from - 172.16.0.35

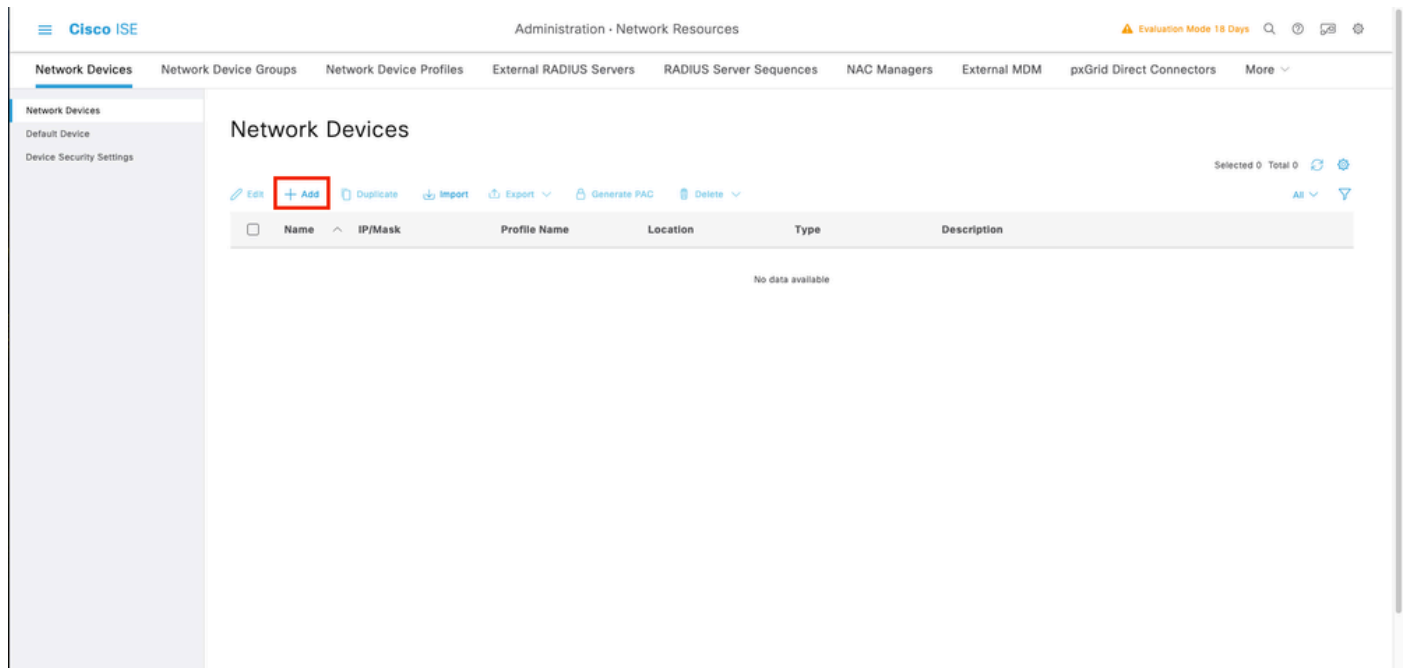
CISCO

Nota: la configuración de FCM ha finalizado en este punto.

Identity Service Engine

Paso 1. Agregue un nuevo dispositivo de red.

Navegue hasta el icono de hamburguesa ≡ ubicado en la esquina superior izquierda > Administración > Recursos de red > Dispositivos de red > +Agregar.

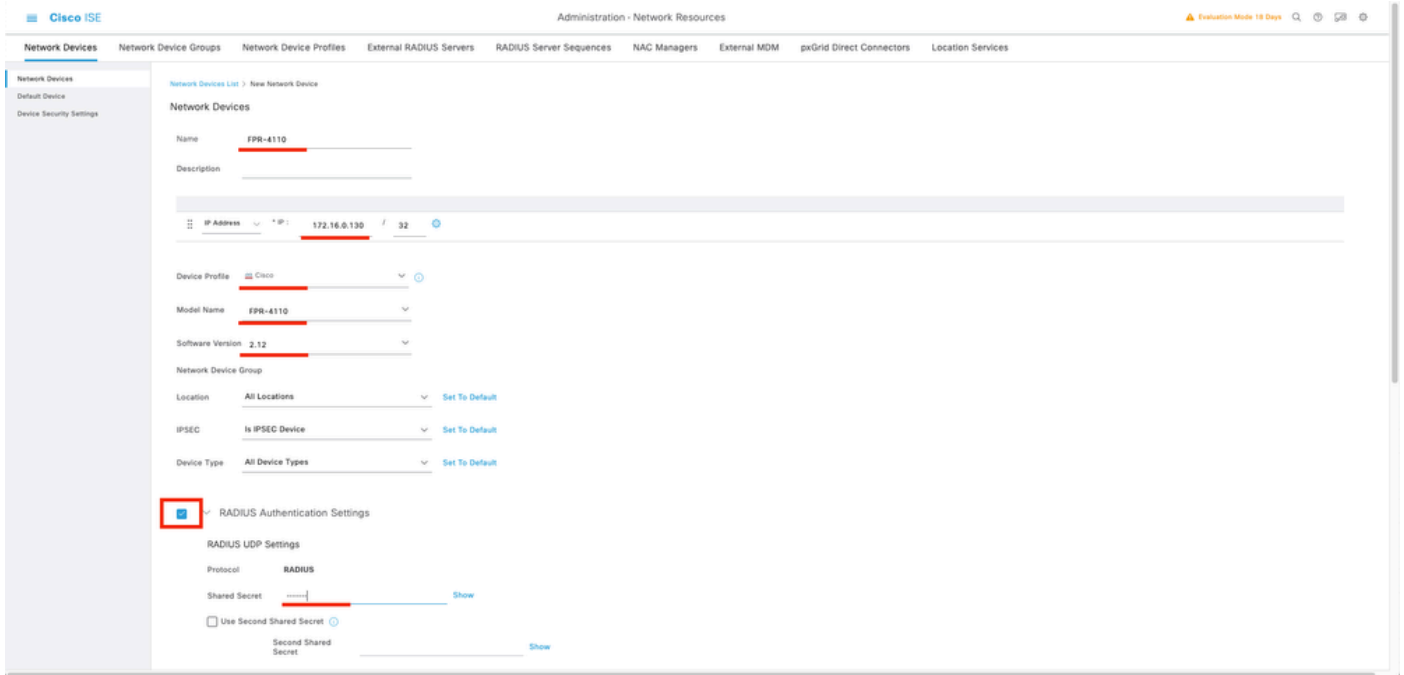


Paso 2. Rellene los parámetros solicitados para la información de los nuevos dispositivos de red.

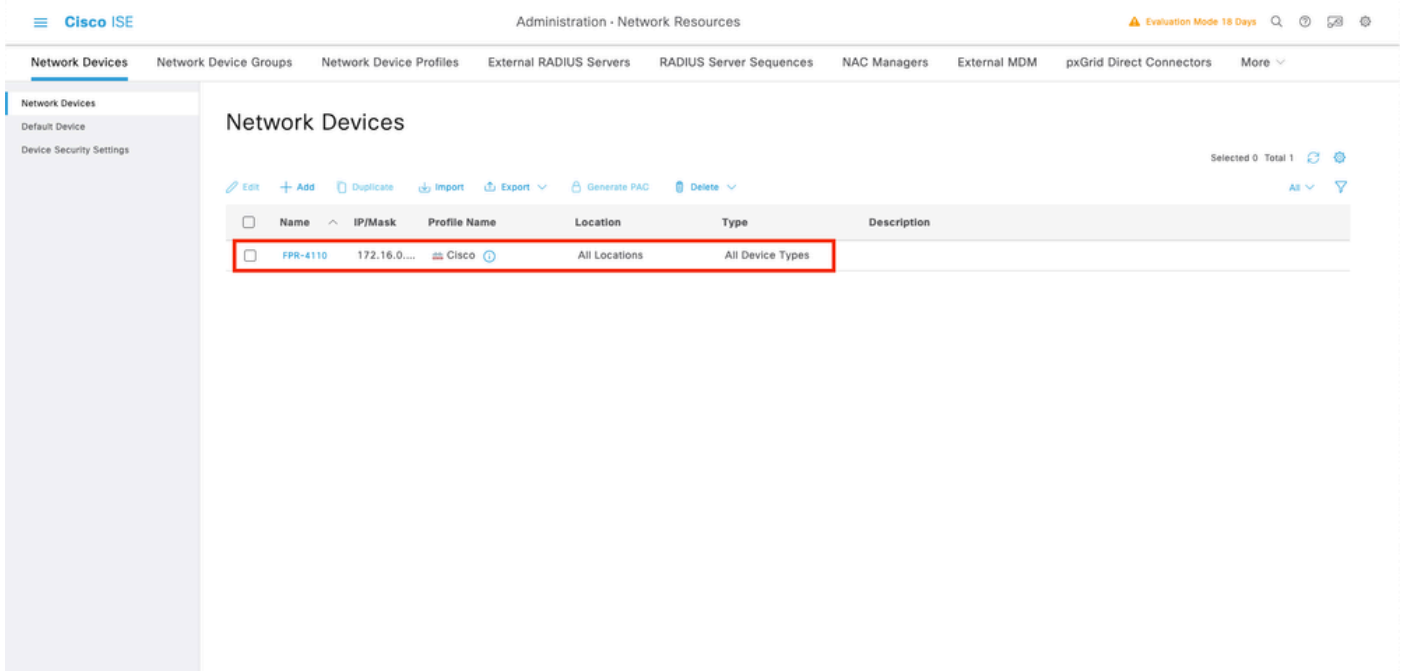
2.1 Marque la casilla RADIUS

2.2 Configure la misma clave secreta compartida que en la configuración Radius de FCM.

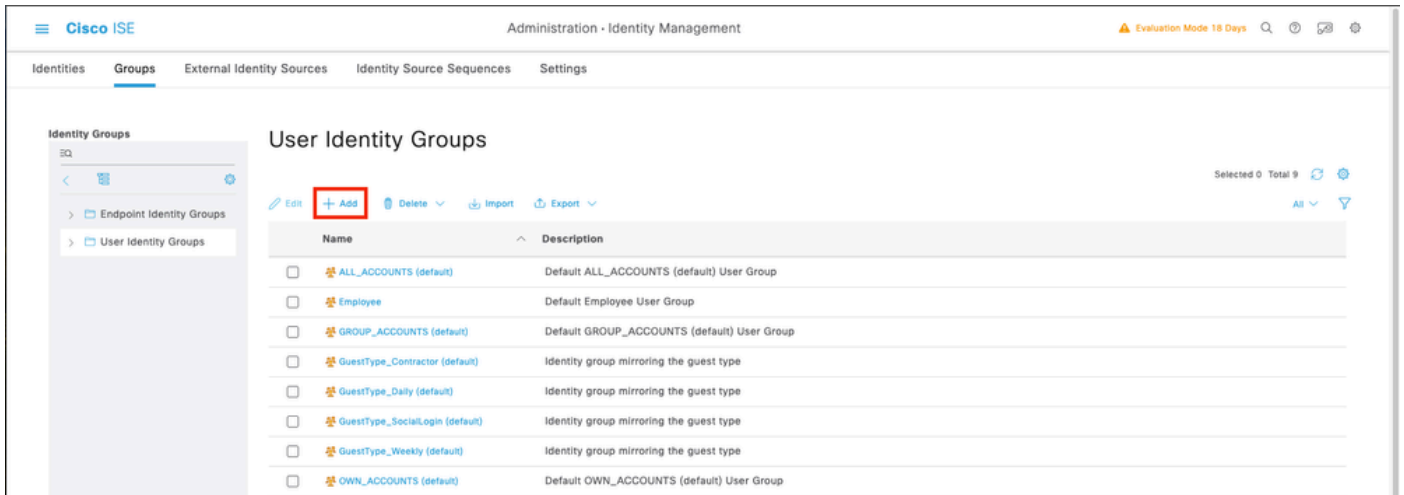
2.1 Desplácese hacia abajo y haga clic en Enviar.



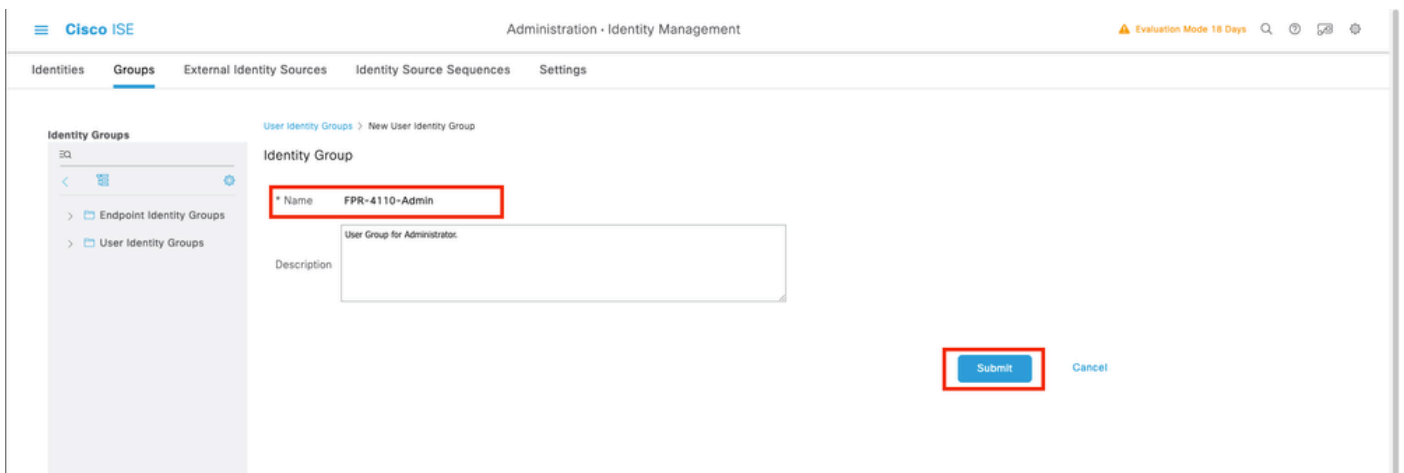
Paso 3. Validar que el nuevo dispositivo se muestra en Dispositivos de red.



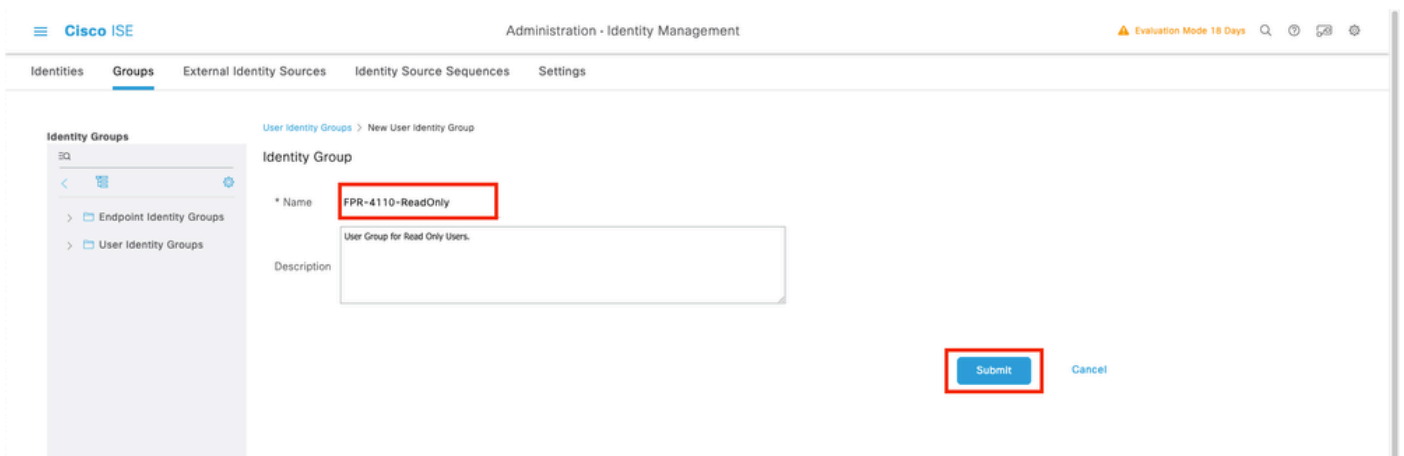
Paso 4. Cree los grupos de identidad de usuario necesarios. Navegue hasta el icono de hamburguesa ≡ ubicado en la esquina superior izquierda > Administración > Administración de identidad > Grupos > Grupos de identidad de usuario > + Agregar



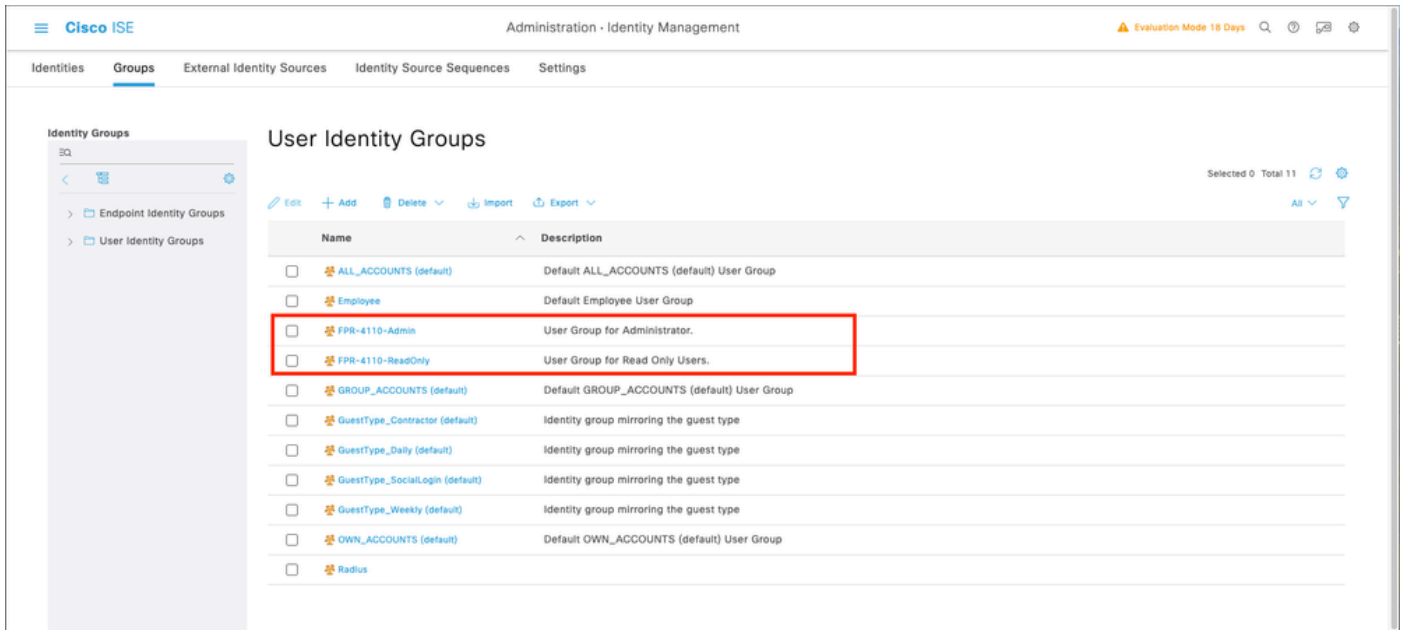
Paso 5. Establezca un nombre para el Admin User Identity Group y haga clic en Submit para guardar la configuración.



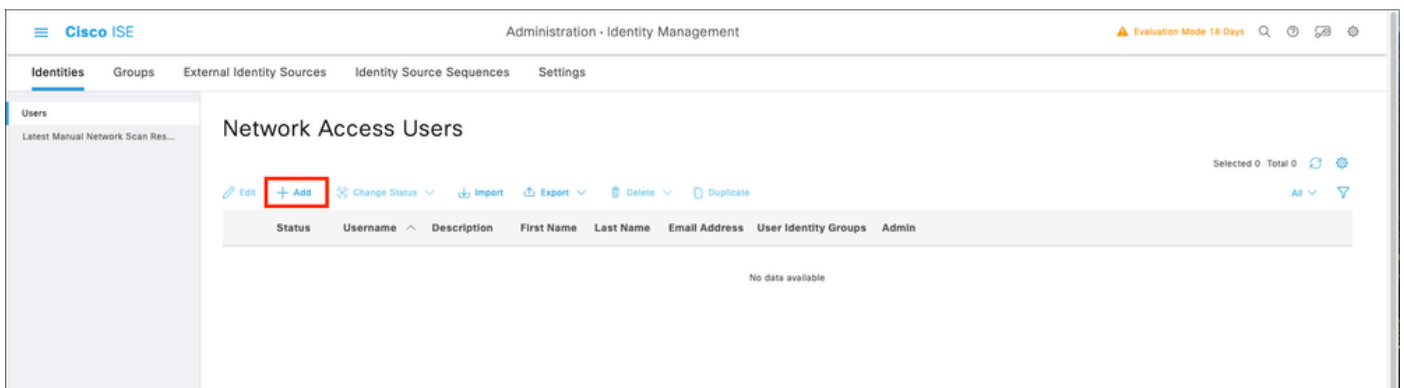
5.1 Repita el mismo proceso para los usuarios de ReadOnly.



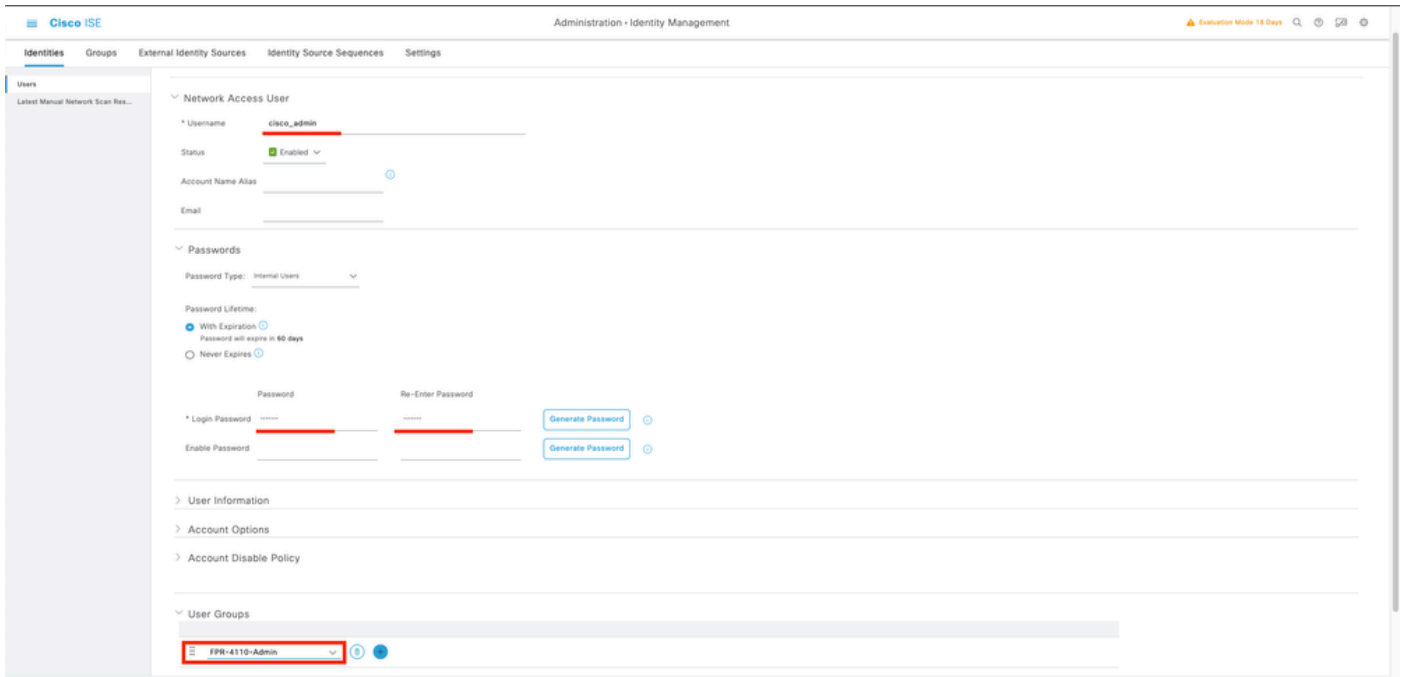
Paso 6. Valide que los nuevos grupos de usuarios aparezcan en Grupos de identidades de usuarios.



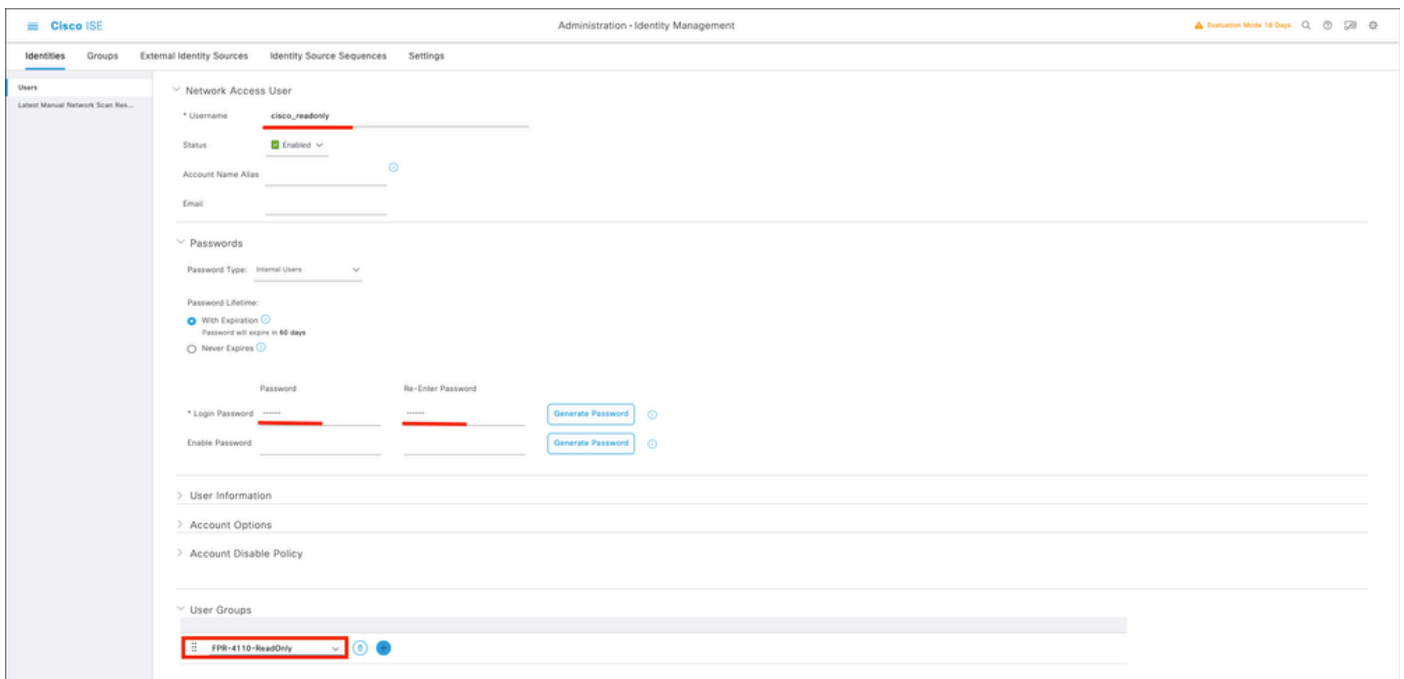
Paso 7. Cree los usuarios locales y agréguelos a su grupo correspondiente. Vaya al icono de hamburguesa ≡ > Administration > Identity Management > Identities > + Add.



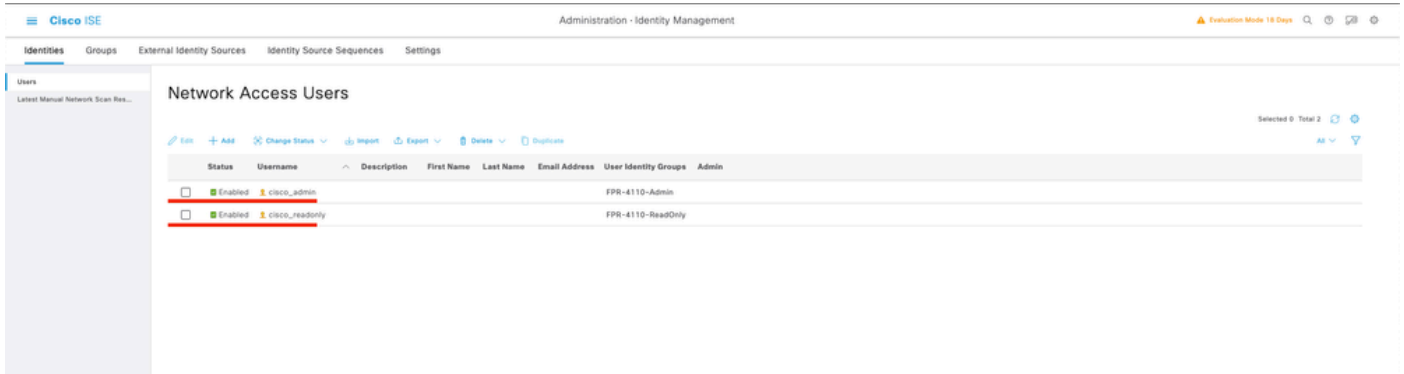
7.1 Agregue el usuario con derechos de administrador. Establezca un nombre, una contraseña y asígnelos a FPR-4110-Admin, desplácese hacia abajo y haga clic en Enviar para guardar los cambios.



7.2 Agregue el usuario con derechos de sólo lectura. Establezca un nombre y una contraseña y asígneselos a FPR-4110-ReadOnly, desplácese hacia abajo y haga clic en Submit para guardar los cambios.



7.3 Valide que los usuarios estén en Usuarios de acceso a la red.



Paso 8. Cree el perfil de autorización para el usuario administrador.

El chasis FXOS incluye las siguientes funciones de usuario:

- Administrador: acceso de lectura y escritura completo 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, la configuración de Smart Call Home para Smart Licensing y los registros del sistema, incluidos los servidores de registro del sistema y los fallos. Acceso de lectura al resto del sistema.
- AAA: acceso de lectura y escritura a usuarios, roles y configuración AAA. Acceso de lectura al resto del sistema

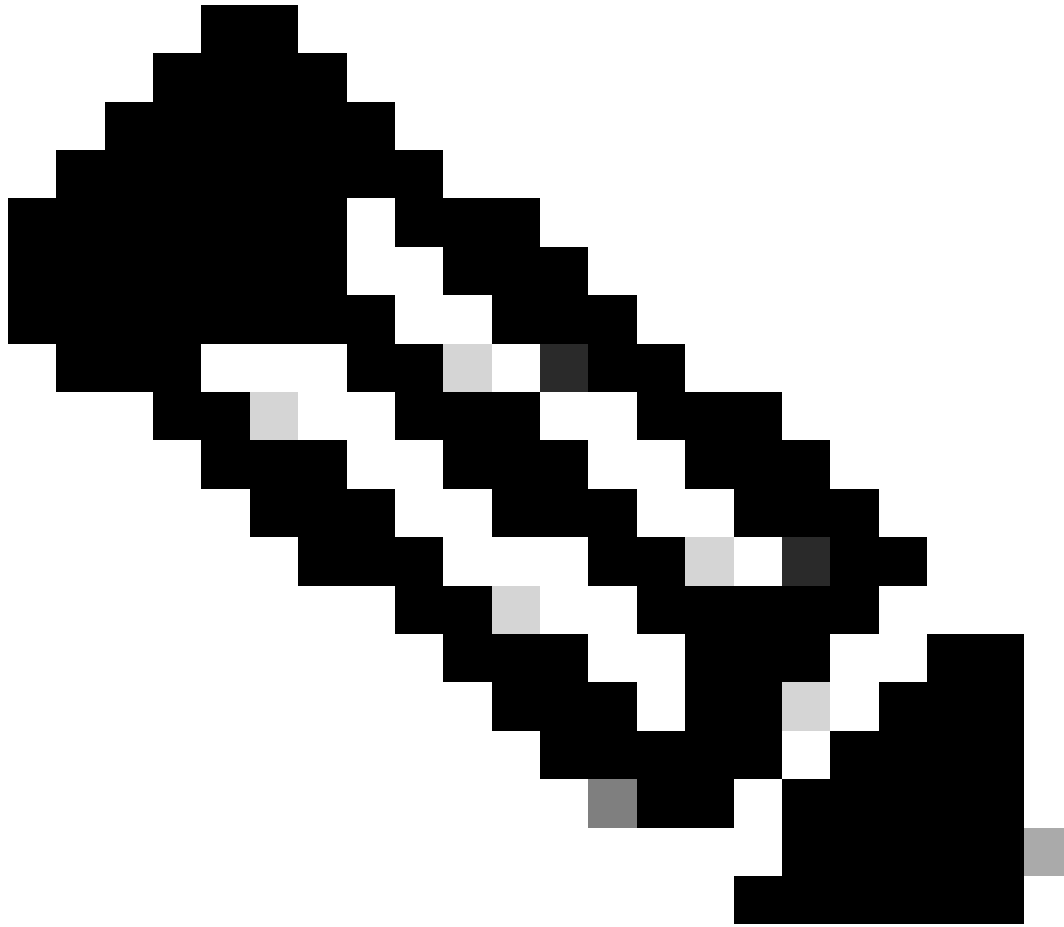
Atributos para cada función:

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

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

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

```
cisco-av-pair=shell:roles="read-only"
```



Nota: Esta documentación sólo define los atributos admin y read-only.

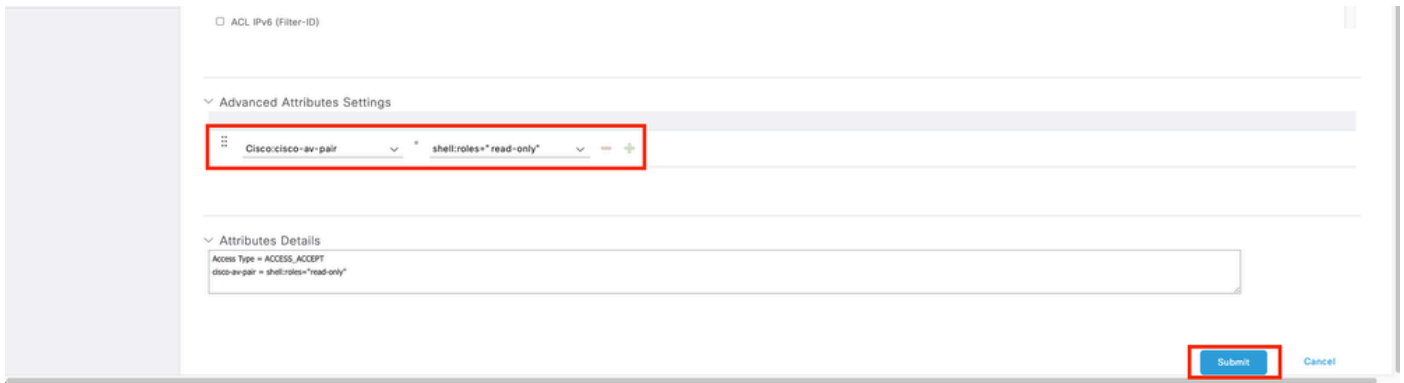
Vaya al icono de hamburguesa ≡ > Política > Elementos de política > Resultados > Autorización > Perfiles de autorización > +Agregar.

Defina un nombre para el perfil de autorización, deje el tipo de acceso como ACCESS_ACCEPT y en Advanced Attributes Settings agregue cisco-av-pair=shell:roles="admin" con y haga clic en Submit.

The screenshot shows the Cisco ISE interface for configuring an Authorization Profile. The breadcrumb trail is "Authorization Profiles > FPR-4110-Admins". The profile name is "FPR-4110-Admins" and the access type is "ACCESS_ACCEPT". Under "Advanced Attributes Settings", a rule is defined as "Cisco:cisco-av-pair" with the value "shell:roles=*admin*". The "Attributes Details" section shows the resulting configuration: "Access Type = ACCESS_ACCEPT" and "cisco-av-pair = shell:roles=*admin*". A "Submit" button is visible at the bottom right.

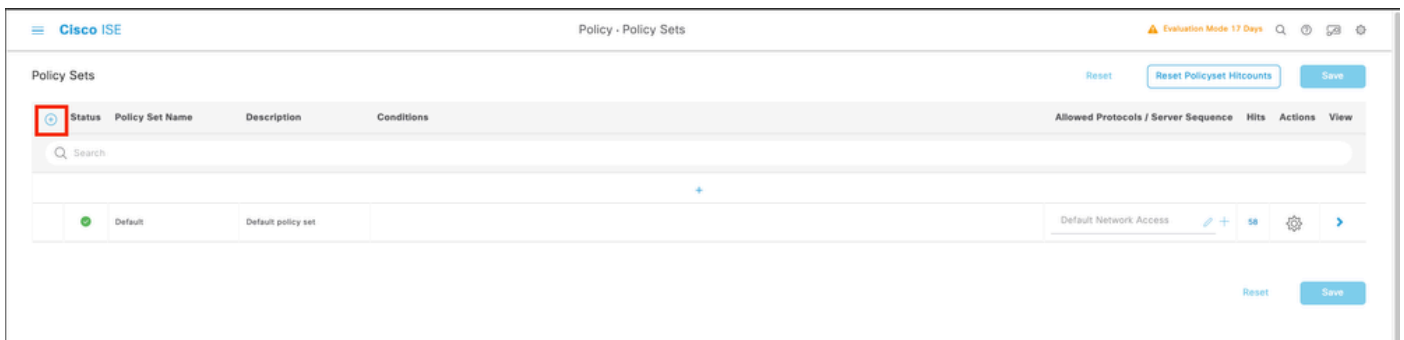
8.1 Repita el paso anterior para crear el perfil de autorización para el usuario de sólo lectura. Cree la clase Radius con el valor read-only en su lugar Administrator esta vez.

The screenshot shows the Cisco ISE interface for creating a new Authorization Profile. The breadcrumb trail is "Authorization Profiles > New Authorization Profile". The profile name is "FPR-4110-ReadOnly" and the access type is "ACCESS_ACCEPT". The configuration options for Network Device Profile, Service Template, Track Movement, Agentless Posture, and Passive Identity Tracking are all set to their default or disabled states.

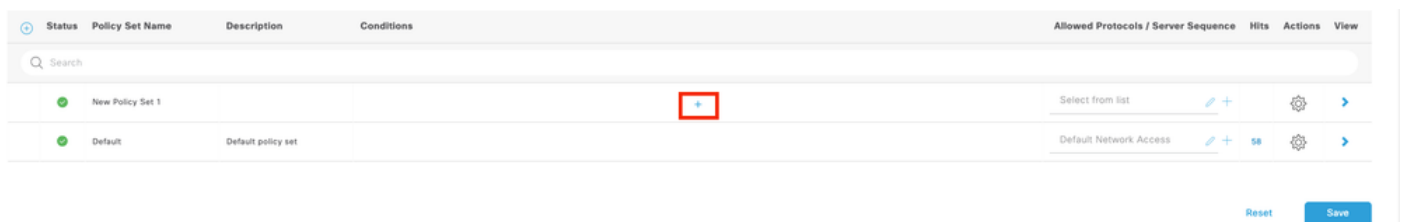


Paso 9. Cree un conjunto de políticas que coincida con la dirección IP de FMC. Esto es para evitar que otros dispositivos concedan acceso a los usuarios.

Navegue hasta ≡ Policy > Policy Sets > Agregar icono de signo en la esquina superior izquierda.



9.1 Se coloca una nueva línea en la parte superior de los conjuntos de políticas. Haga clic en el icono Add para configurar una nueva condición.



9.2 Agregue una condición superior para el atributo RADIUS NAS-IP-Address que coincida con la dirección IP de FCM y, a continuación, haga clic en Usar.

Library

Search by Name

5G
Catalyst_Switch_Local_Web_Authentication
Radius
Switch_Local_Web_Authentication
Switch_Web_Authentication
Wired_802.1X
Wired_MAB
Wireless_802.1X
Wireless_Access
Wireless_MAB
WLC_Web_Authentication

Editor

Radius-NAS-IP-Address

Equals

Set to 'is not'

Wrong value

Duplicate Save

Select attribute for condition

Dictionary	Attribute	ID	Info
All Dictionaries	Attribute	ID	
Microsoft	MS-User-IPv4-Address	61	
Network Access	ISE Host Name		
Radius	DNS-Server-IPv6-Address	169	
Radius	Framed-IP-Address	8	
Radius	Framed-IPv6-Address	168	
Radius	NAS-IP-Address	4	
Radius	Stateful-IPv6-Address-Pool	172	

Library

Search by Name

5G
Catalyst_Switch_Local_Web_Authentication
Radius
Switch_Local_Web_Authentication
Switch_Web_Authentication
Wired_802.1X
Wired_MAB
Wireless_802.1X
Wireless_Access
Wireless_MAB
WLC_Web_Authentication

Editor

Radius-NAS-IP-Address

Equals

172.16.0.130

Set to 'is not'

Duplicate Save

NEW AND OR

Close Use

9.3 Una vez completado, haga clic en Guardar.

Clisco ISE

Policy - Policy Sets

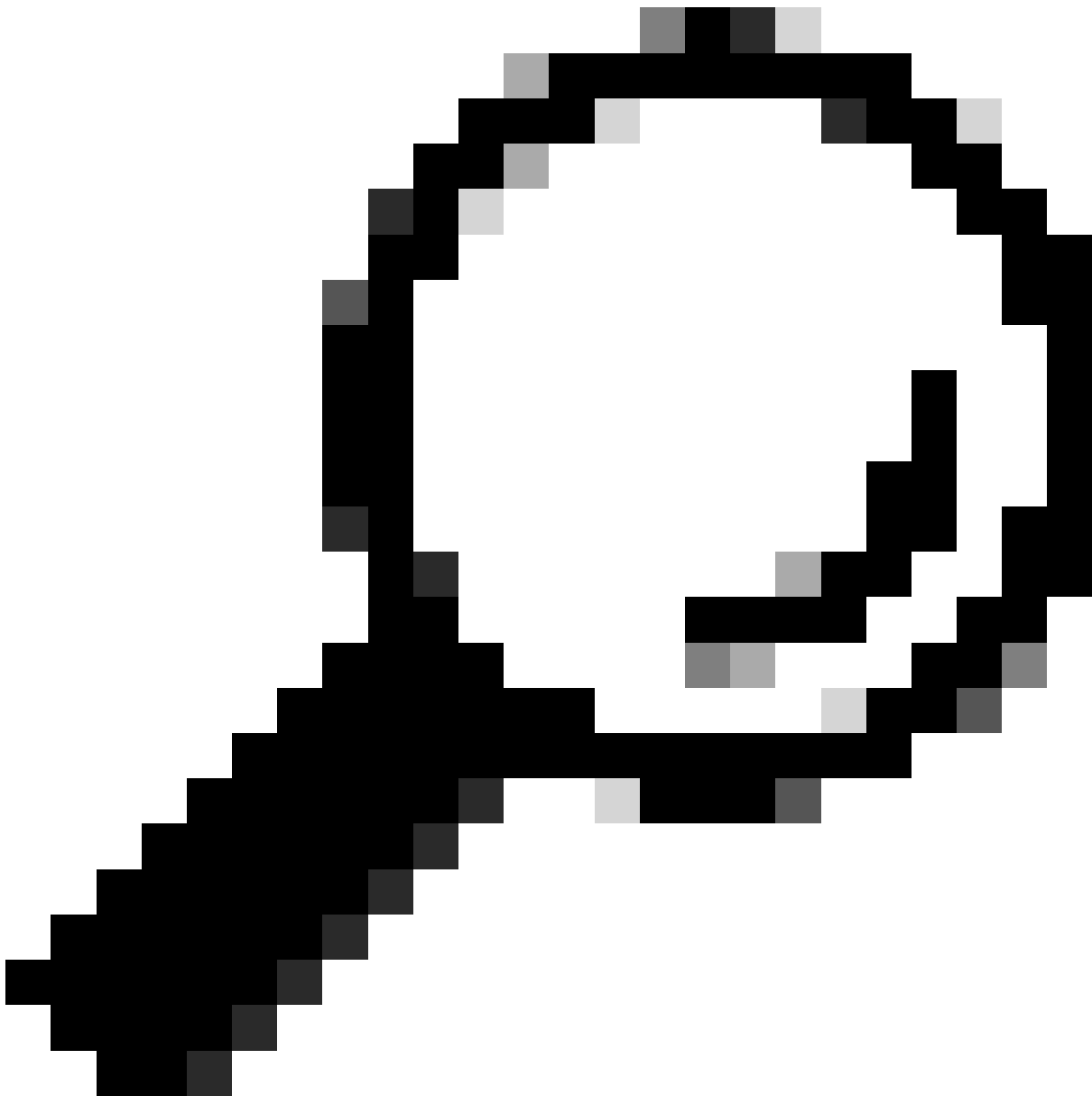
Evaluation Mode 17 Days

Policy Sets

Reset Reset Policyset Hitcounts Save

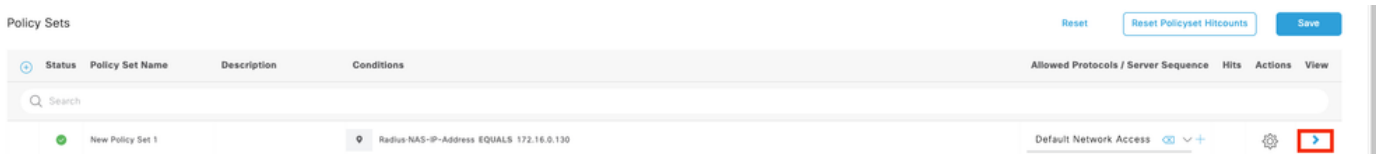
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	New Policy Set 1		Radius-NAS-IP-Address EQUALS 172.16.0.130	Default Network Access			
●	Default	Default policy set		Default Network Access	58		

Reset Save

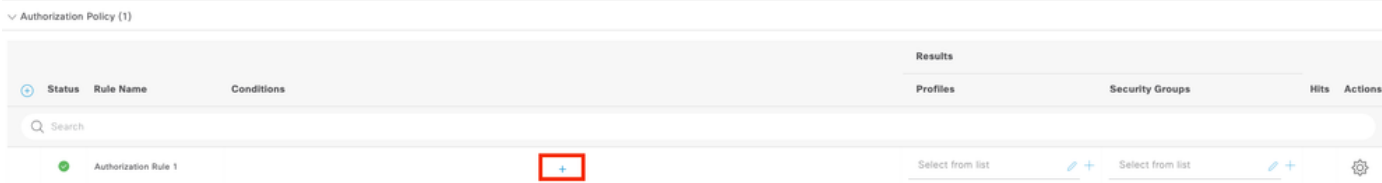


Sugerencia: para este ejercicio hemos permitido la lista Protocolos de acceso a la red predeterminados. Puede crear una lista nueva y reducirla según sea necesario.

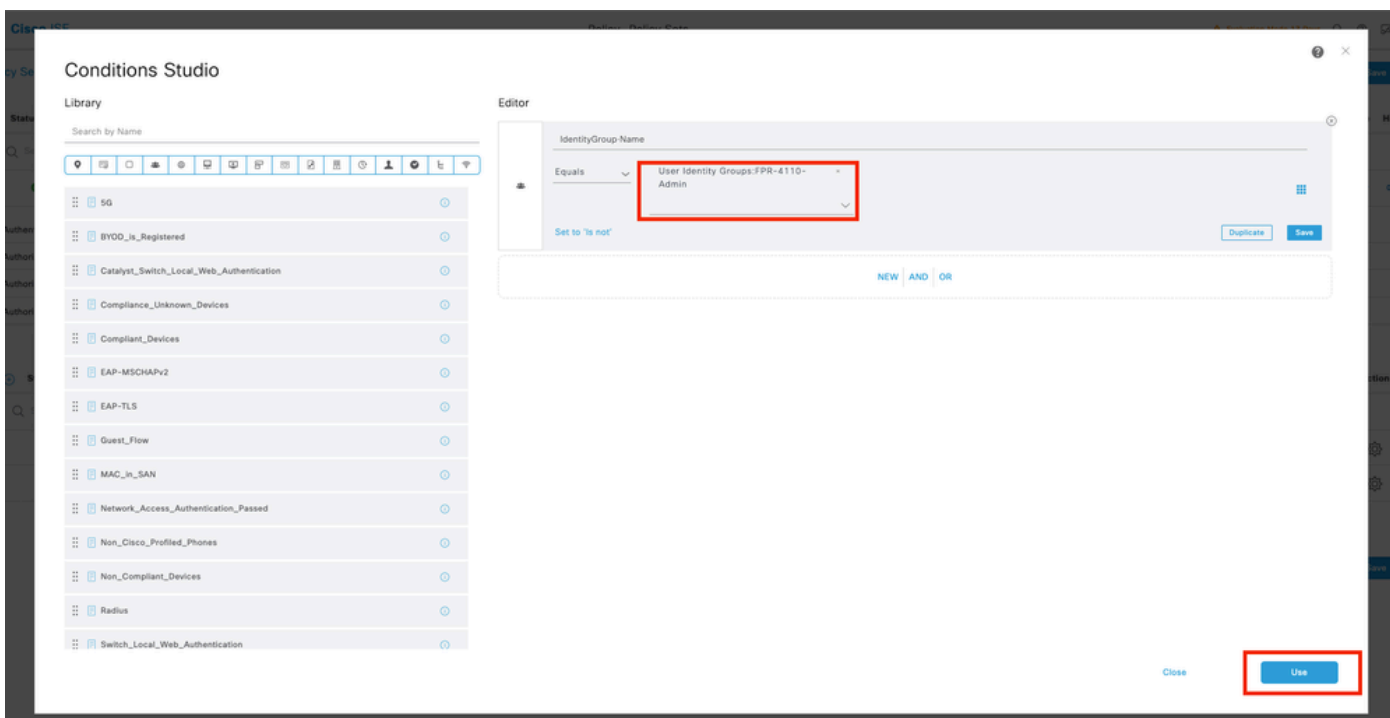
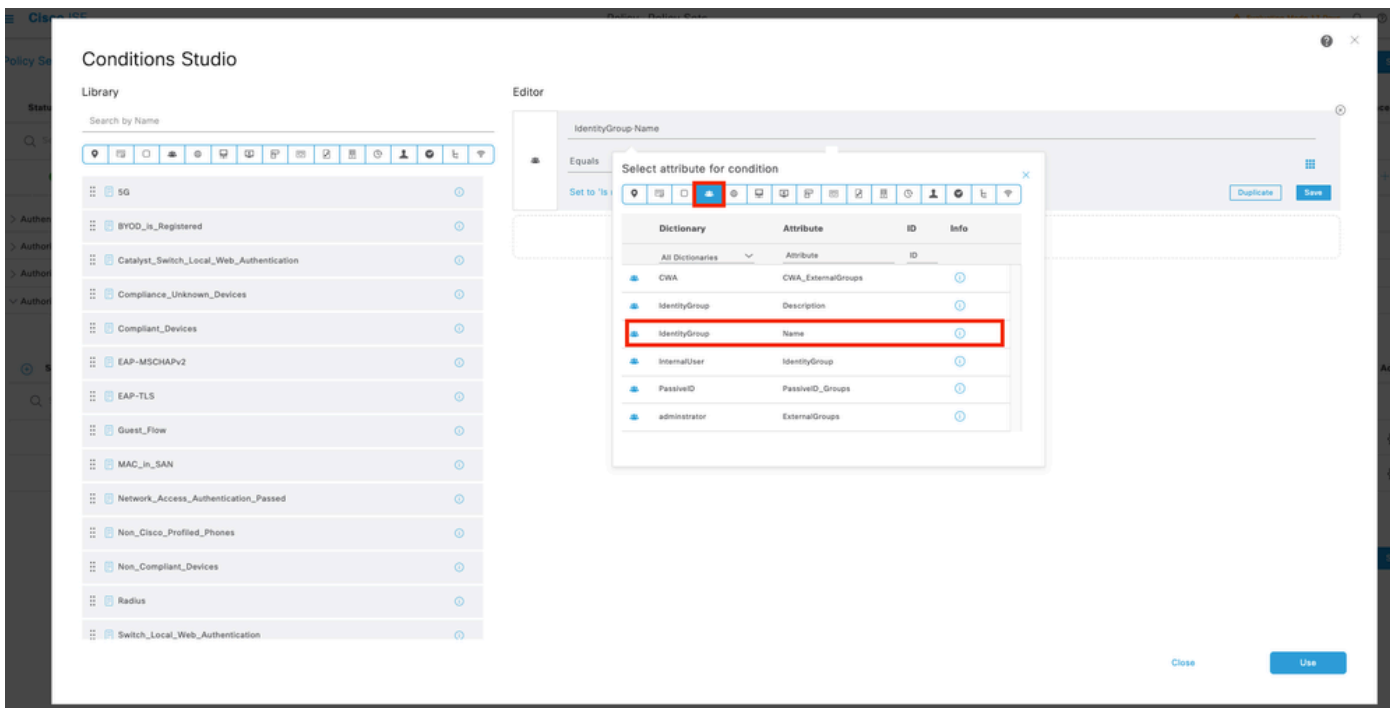
Paso 10. Para ver el nuevo conjunto de políticas, pulse el icono > situado al final de la fila.



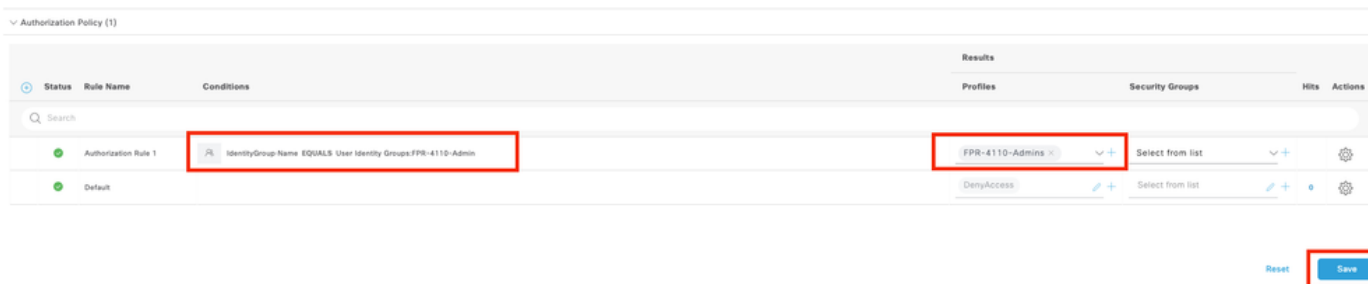
10.1 Expanda el menú Authorization Policy y haga clic en (+) para agregar una nueva condición.



10.2 Establezca las condiciones para que coincidan con el grupo DictionaryIdentity con AttributeName es igual a User Identity Groups: FPR-4110-Admins (el nombre de grupo creado en el paso 7) y haga clic en Use.



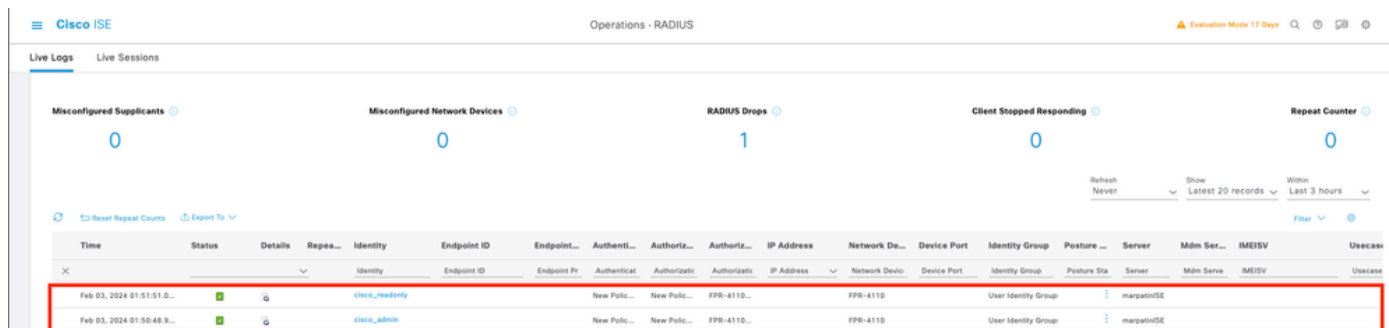
Paso 10.3 Valide que la nueva condición esté configurada en la política de autorización, luego agregue un perfil de usuario bajo Perfiles.



Paso 11. Repita el mismo proceso en el paso 9 para los usuarios de sólo lectura y haga clic en Guardar.

Verificación

1. Intente iniciar sesión en la GUI de FCM con las nuevas credenciales de Radius
2. Navegue hasta el icono de hamburguesa ≡ > Operaciones > Radio > Registros en vivo.
3. La información mostrada indica si un usuario ha iniciado sesión correctamente.



4. Valide el rol de usuarios registrados desde la CLI del chasis de firewall seguro.

```

FPR4K-1-029A78B# scope se
security          server          service-profile

FPR4K-1-029A78B# scope security
FPR4K-1-029A78B /security # show remote-user detail
Remote User cisco_admin:
  Description:
  User Roles:
    Name: admin
    Name: read-only
FPR4K-1-029A78B /security #

```

Troubleshoot

1. En la GUI de ISE , vaya al icono de hamburguesa ≡ > Operaciones > Radio > Registros en directo.

1.1 Valide si la solicitud de sesión de registro está llegando al nodo ISE.

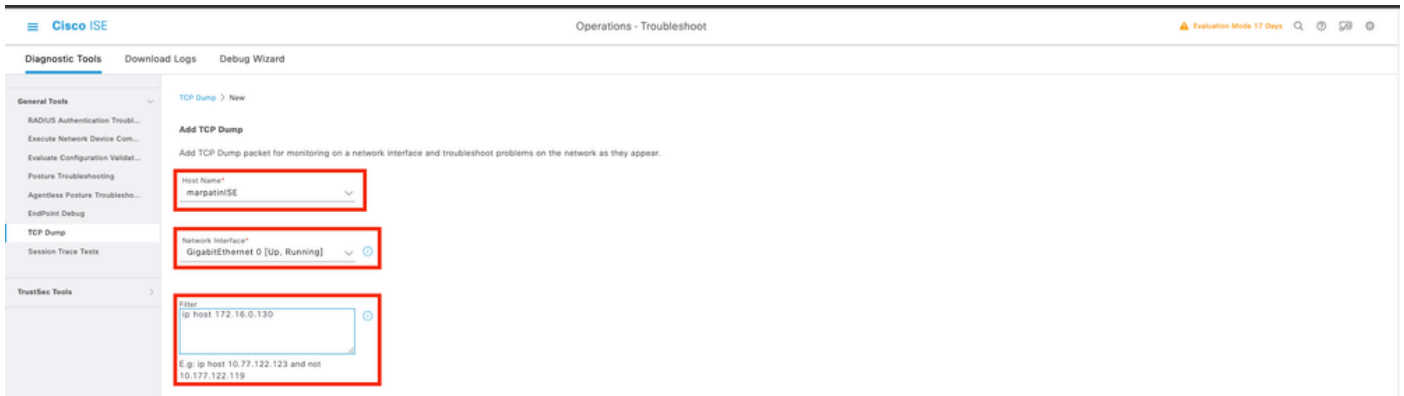
1.2 Para ver el estado de error, revise los detalles de la sesión.

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authent...	Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture ...	Server	Mdm Se
Feb 02, 2024 07:32:18.8...	❌	🔍		cisco_admin	Endpoint ID	Endpoint Pr	Default >>...	Default	Default	IP Address	Network Device	Device Port	User Identity Group	Posture Sta	Server	Mdm Sen
Feb 02, 2024 07:23:20.1...	✅	🔍		cisco_readonly			Default >>...	Default >>...	PermitAcc...		FPR-4110		User Identity Group		marpat@ISE	
Feb 02, 2024 07:15:32.2...	✅	🔍		cisco_admin			Default >>...	Default >>...	PermitAcc...		FPR-4110		User Identity Group		marpat@ISE	

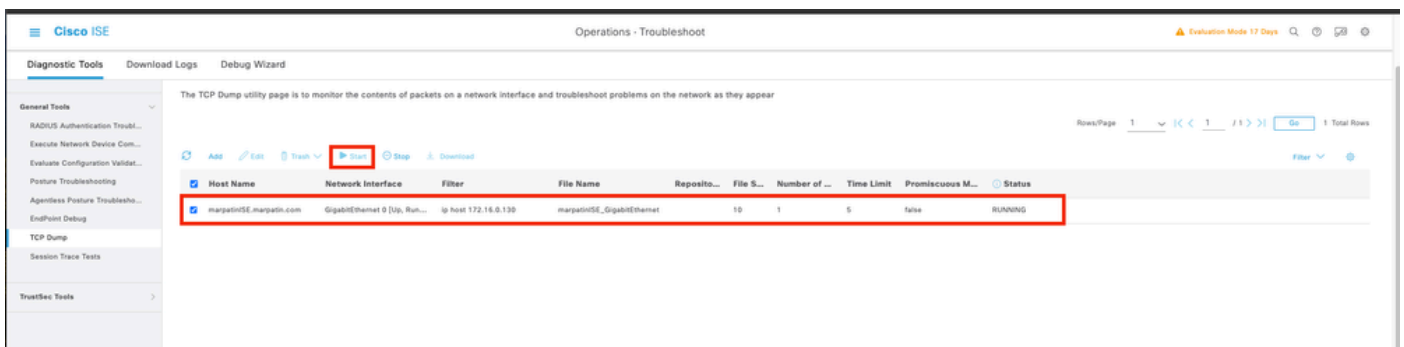
2. Para las solicitudes que no se muestran en los registros de Radius Live , revise si la solicitud UDP está llegando al nodo ISE a través de una captura de paquetes.

Vaya al icono de hamburguesa ≡ > Operaciones > Solución de problemas > Herramientas de diagnóstico > Volcado de TCP. Agregue una nueva captura y descargue el archivo en su máquina local para revisar si los paquetes UDP llegan al nodo ISE.

2.1 Rellene la información solicitada, desplácese hacia abajo y haga clic en Guardar.



2.2 Seleccione e inicie la captura.



2.3 Intento de registro en el chasis de firewall seguro mientras se ejecuta la captura de ISE

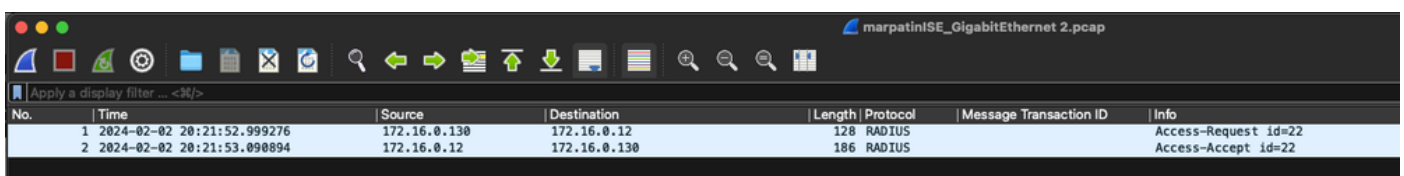
2.4 Detenga el volcado de TCP en ISE y descargue el archivo en un equipo local.

2.5 Revise la salida del tráfico.

Resultado esperado:

Paquete nº 1. Solicitud del firewall seguro al servidor ISE a través del puerto 1812 (RADIUS)

Paquete nº 2. Respuesta del servidor ISE que acepta la solicitud inicial.



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).