Configuración de la autenticación externa FMC y FTD con ISE como servidor RADIUS

Contenido

- Introducción
- Prerequisites
  - Requirements
  - Componentes Utilizados
- Antecedentes
  - Autenticación externa para FMC
  - Autenticación externa para FTD
  - Topología de red
- Configurar
  - Configuración de ISE
    - Agregue sus dispositivos de red
    - Crear los grupos de identidad de usuarios locales y los usuarios
    - Crear los perfiles de autorización
    - Agregar un nuevo conjunto de políticas
  - Configuración de FMC
    - Agregue su servidor RADIUS de ISE para la autenticación FMC
  - Configuración de FTD
    - Agregue su servidor RADIUS de ISE para la autenticación FTD
    - Habilitar el servidor RADIUS
- Verificación

Introducción

Este documento describe un ejemplo de configuración de autenticación externa para Secure Firewall Management Center y Firewall Threat Defence.

Prerequisites

Requirements

Se recomienda tener conocimiento de estos temas:

- Configuración inicial de Cisco Secure Firewall Management Center a través de la GUI o el shell.
- Configuración de políticas de autenticación y autorización en ISE.
- Conocimiento básico de RADIUS.

Componentes Utilizados

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

- vFMC 7.4.2
- vFTD 7.4.2
- ISE 3.3

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.

Antecedentes

Cuando se habilita la autenticación externa para los usuarios administrativos y de gestión del sistema de firewall seguro, el dispositivo comprueba las credenciales del usuario con un protocolo ligero de acceso a directorios (LDAP) o un servidor RADIUS como se especifica en un objeto de autenticación externa.

Los objetos de autenticación externa pueden ser utilizados por los dispositivos FMC y FTD. Puede compartir el mismo objeto entre los distintos tipos de dispositivo o dispositivo, o bien crear objetos independientes.

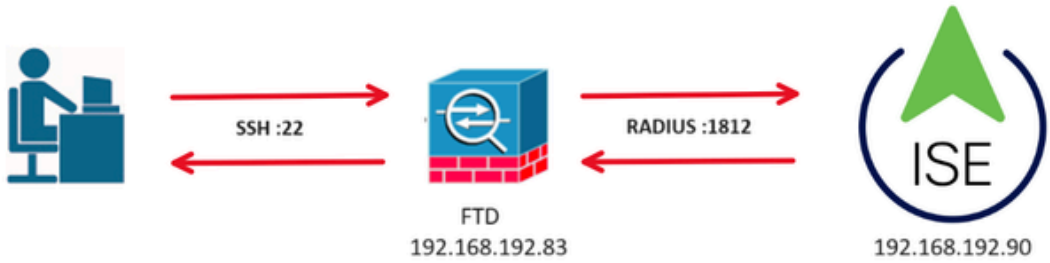
Autenticación externa para FMC

Puede configurar varios objetos de autenticación externos para el acceso a la interfaz web. Sólo se puede utilizar un objeto de autenticación externo para el acceso a CLI o shell.

Autenticación externa para FTD

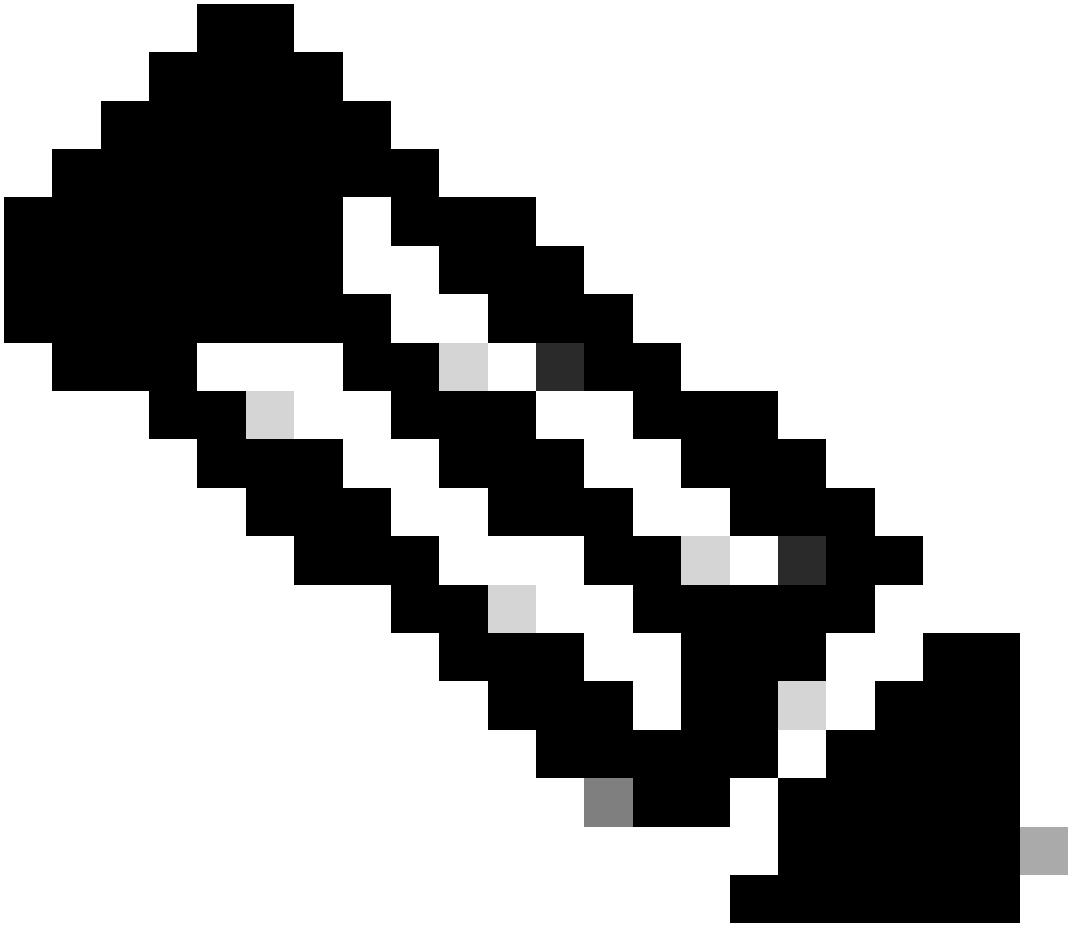
Para el FTD, sólo puede activar un objeto de autenticación externo.

Topología de red



Configurar

Configuración de ISE

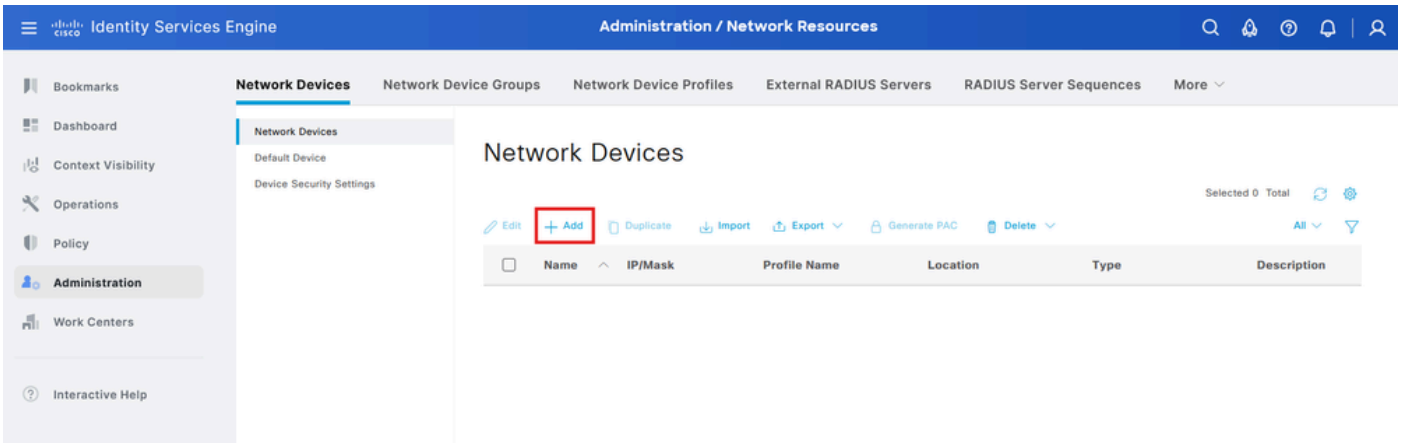


Nota: Hay varias formas de configurar las políticas de autenticación y autorización de ISE para los dispositivos de acceso a la red (NAD), como FMC. El ejemplo descrito en este documento es un punto de referencia en el que creamos dos perfiles (uno con derechos de administrador y el otro de solo lectura) y se puede adaptar para cumplir con las líneas de base para acceder a su red. Se pueden definir una o más políticas de autorización en ISE devolviendo los valores de atributo RADIUS al FMC que, a continuación, se asignan a un grupo de usuarios local definido en la configuración de políticas del sistema FMC.

Agregue sus dispositivos de red

Paso 1. Navegue hasta el icono de hamburguesa

situado en la esquina superior izquierda >Administración > Recursos de red > Dispositivos de red > +Agregar.

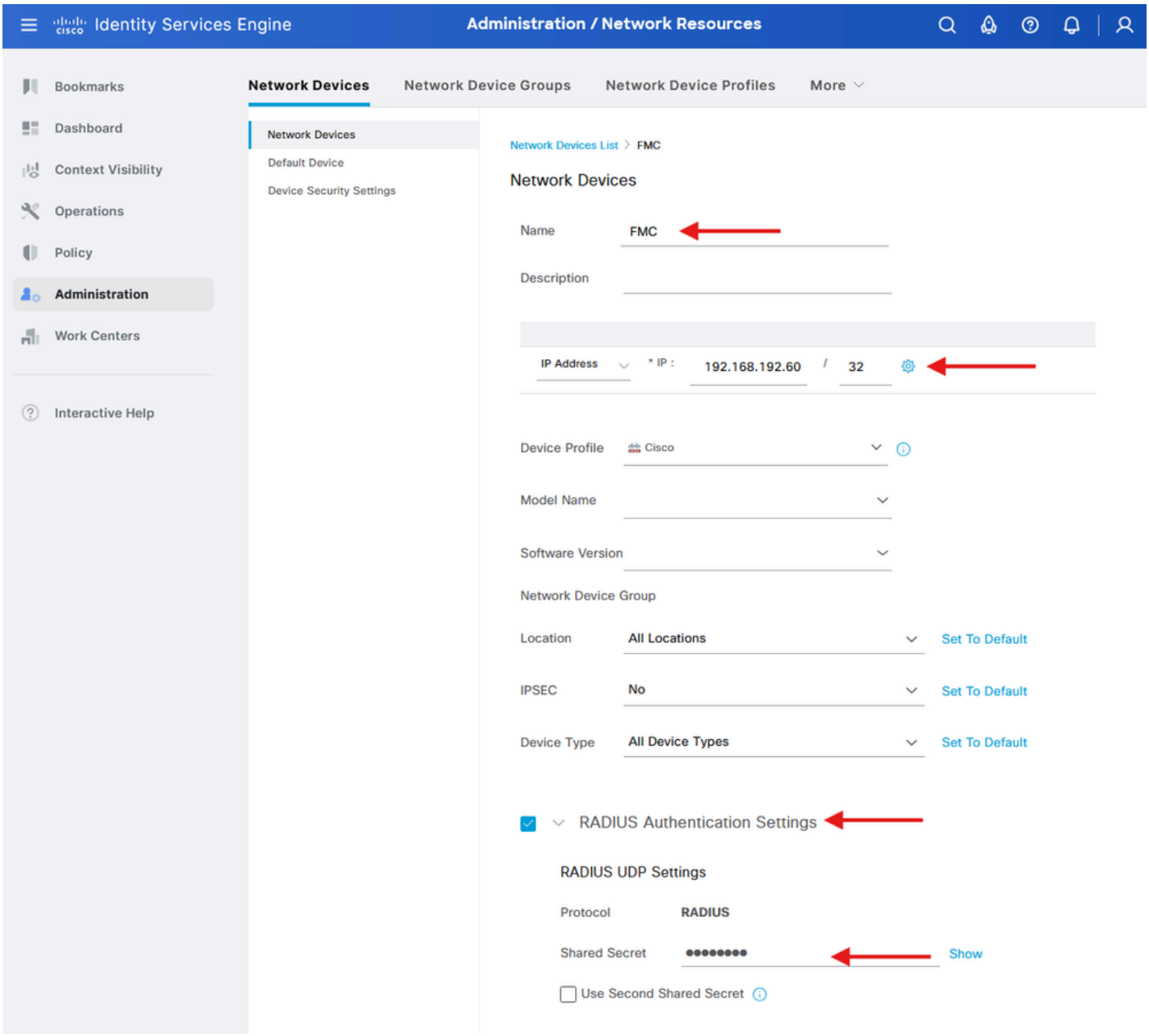


Paso 2. Asigne un nombre al objeto del dispositivo de red e inserte la dirección IP del CSP.

Marque la casilla de verificación RADIUS y defina un secreto compartido.

La misma clave debe utilizarse más adelante para configurar el FMC.

Una vez hecho esto, haga clic en Guardar.

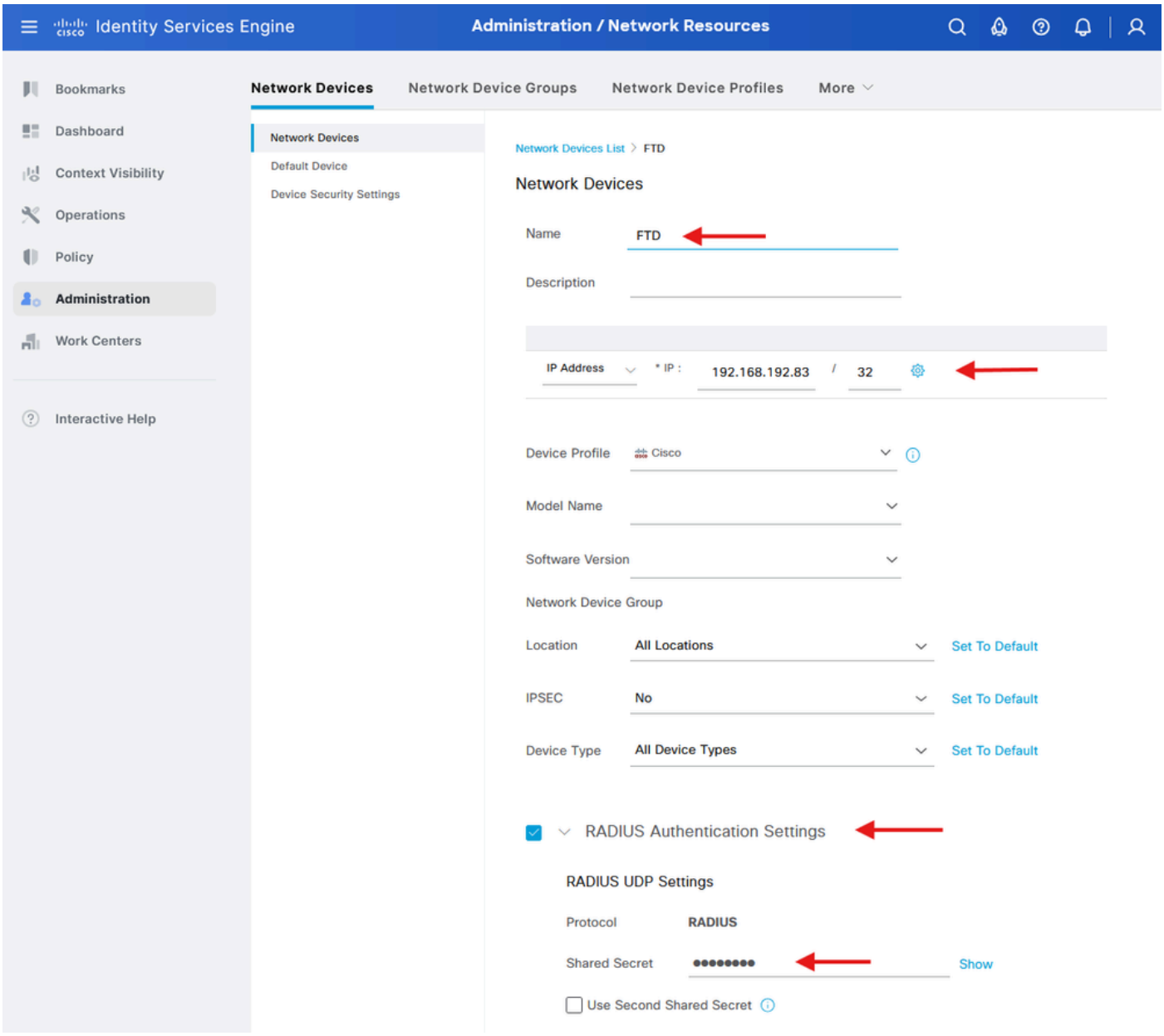


Paso 2.1. Repita el mismo procedimiento para añadir el FTD.

Asigne un nombre al objeto de dispositivo de red e inserte la dirección IP de FTD.

Marque la casilla de verificación RADIUS y defina un secreto compartido.

Una vez hecho esto, haga clic en Guardar.

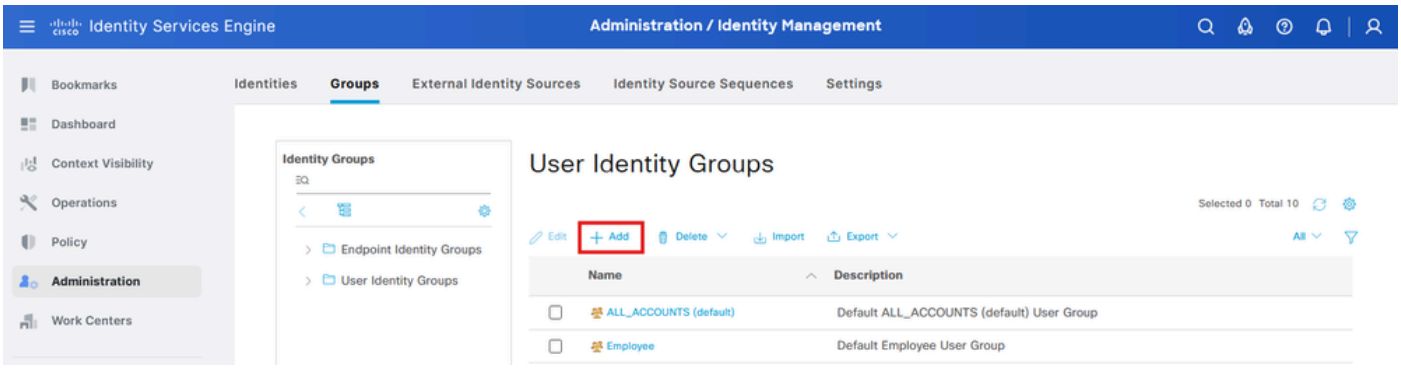


Paso 2.3. Validar que ambos dispositivos se muestren en Dispositivos de red.

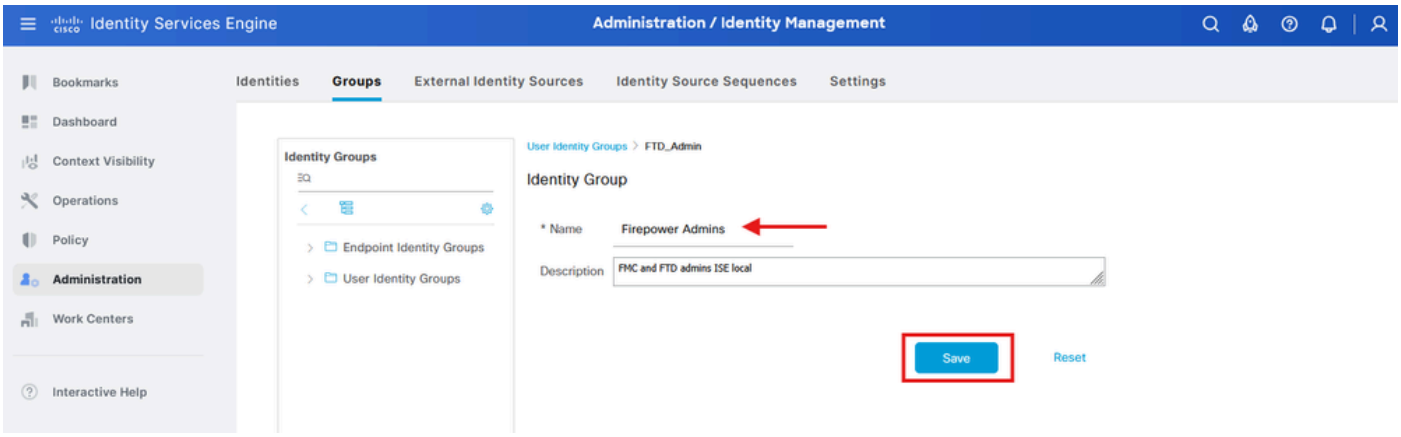
Crear los grupos de identidad de usuarios locales y los usuarios

Paso 3. Cree los grupos de identidad de usuario necesarios. Vaya al icono de hamburguesa

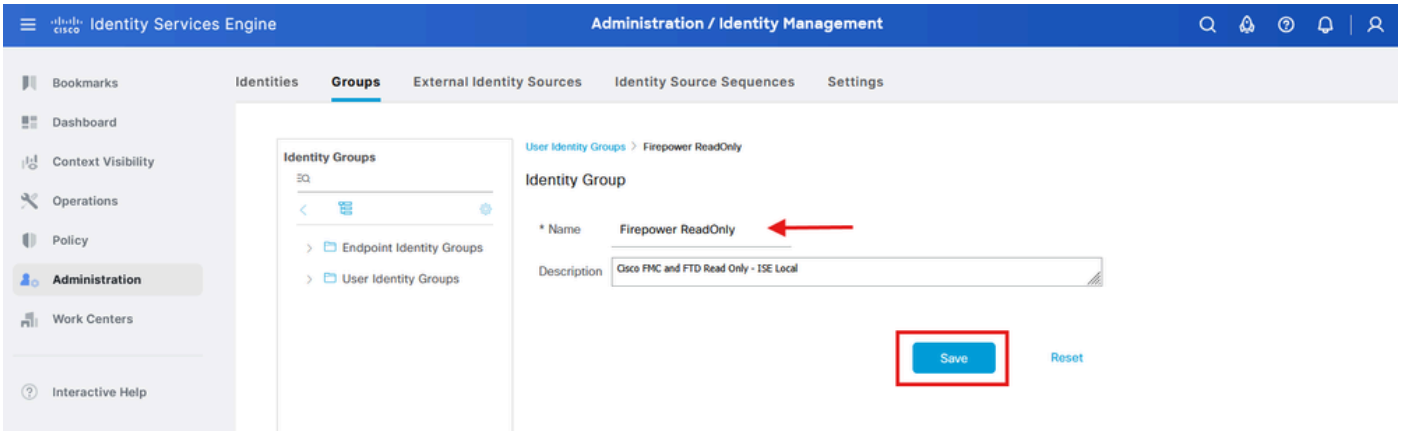
situado en la esquina superior izquierda > Administration > Identity Management > Groups > User Identity Groups > + Add



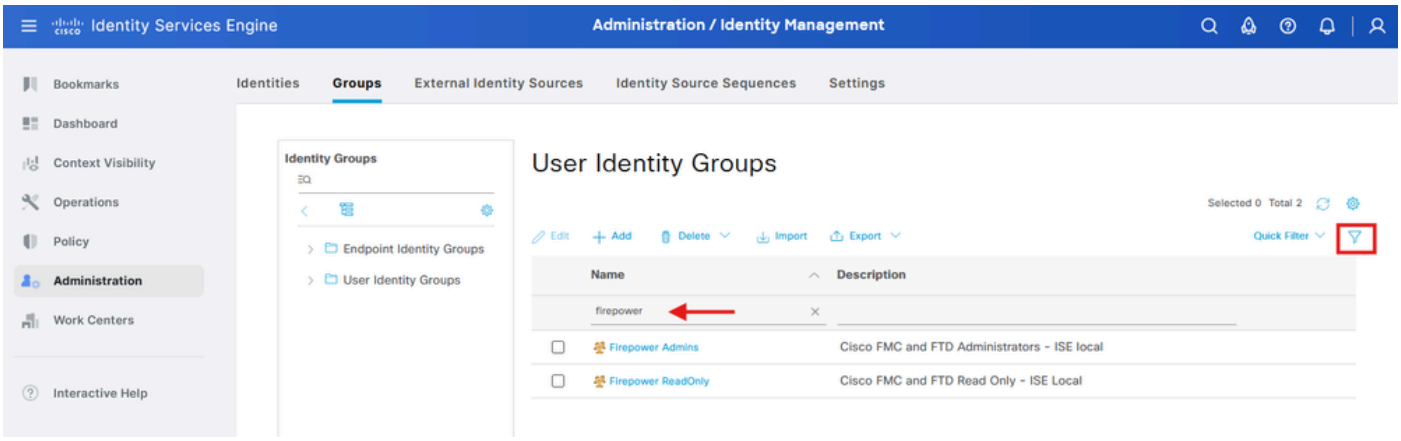
Paso 4. Asigne un nombre a cada grupo y haga clic en Guardar individualmente. En este ejemplo, estamos creando un grupo para usuarios administradores y otro para usuarios de sólo lectura. En primer lugar, cree el grupo para el usuario con derechos de administrador.



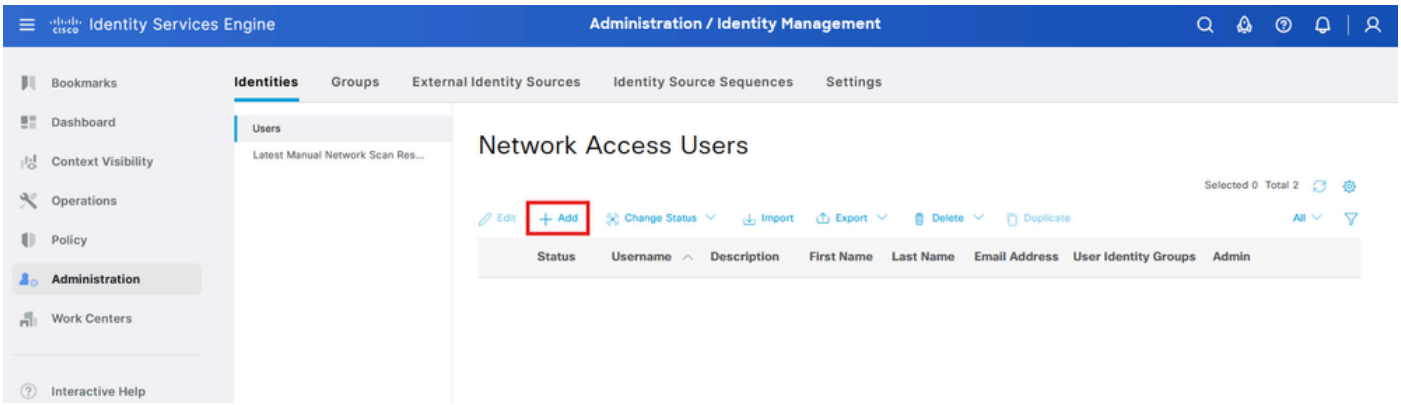
Paso 4.1. Crear el segundo grupo para el usuario de ReadOnly.



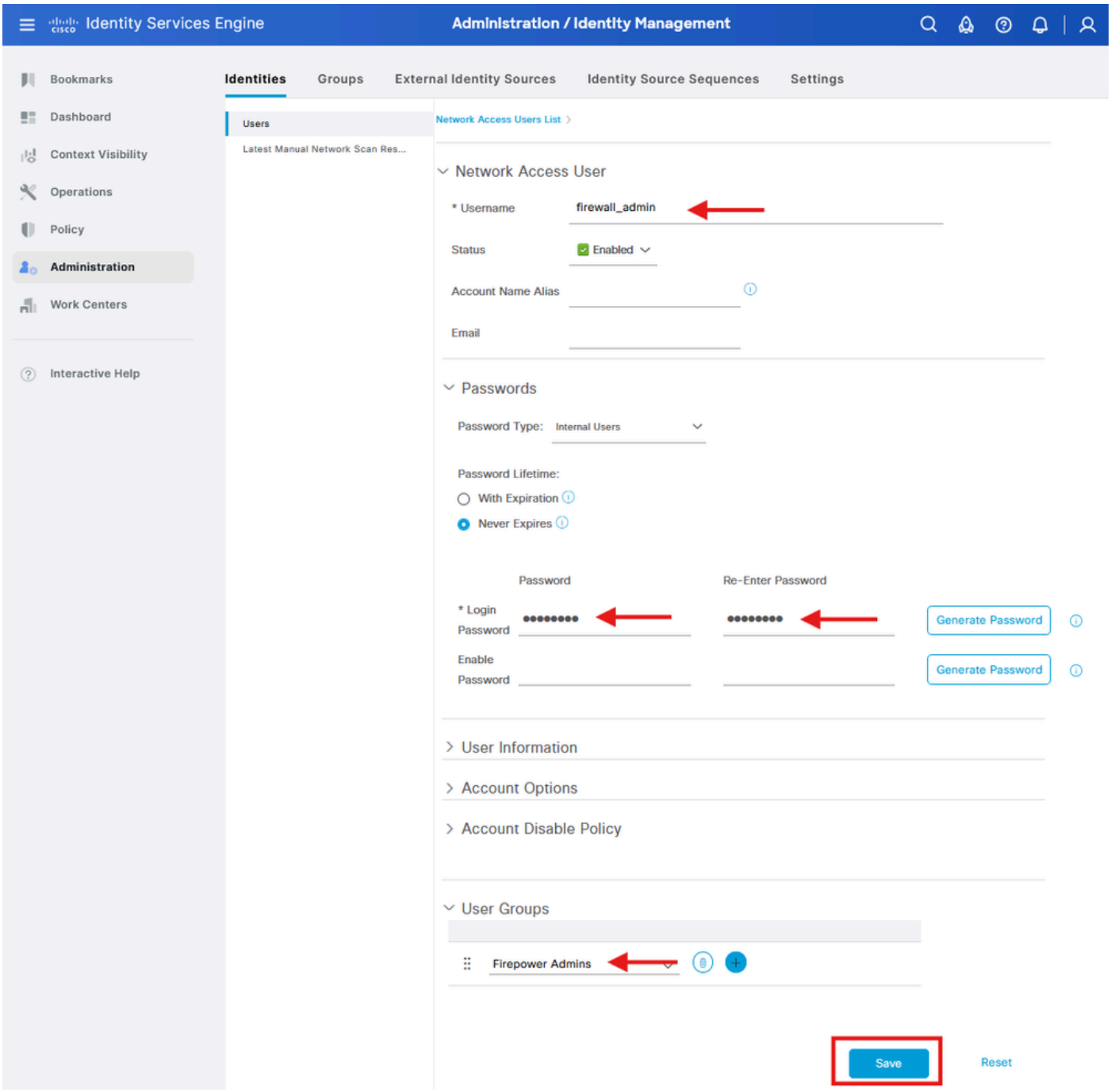
Paso 4.2. Validar ambos grupos se muestra en la Lista de grupos de identidad de usuarios. Utilice el filtro para encontrarlos fácilmente.



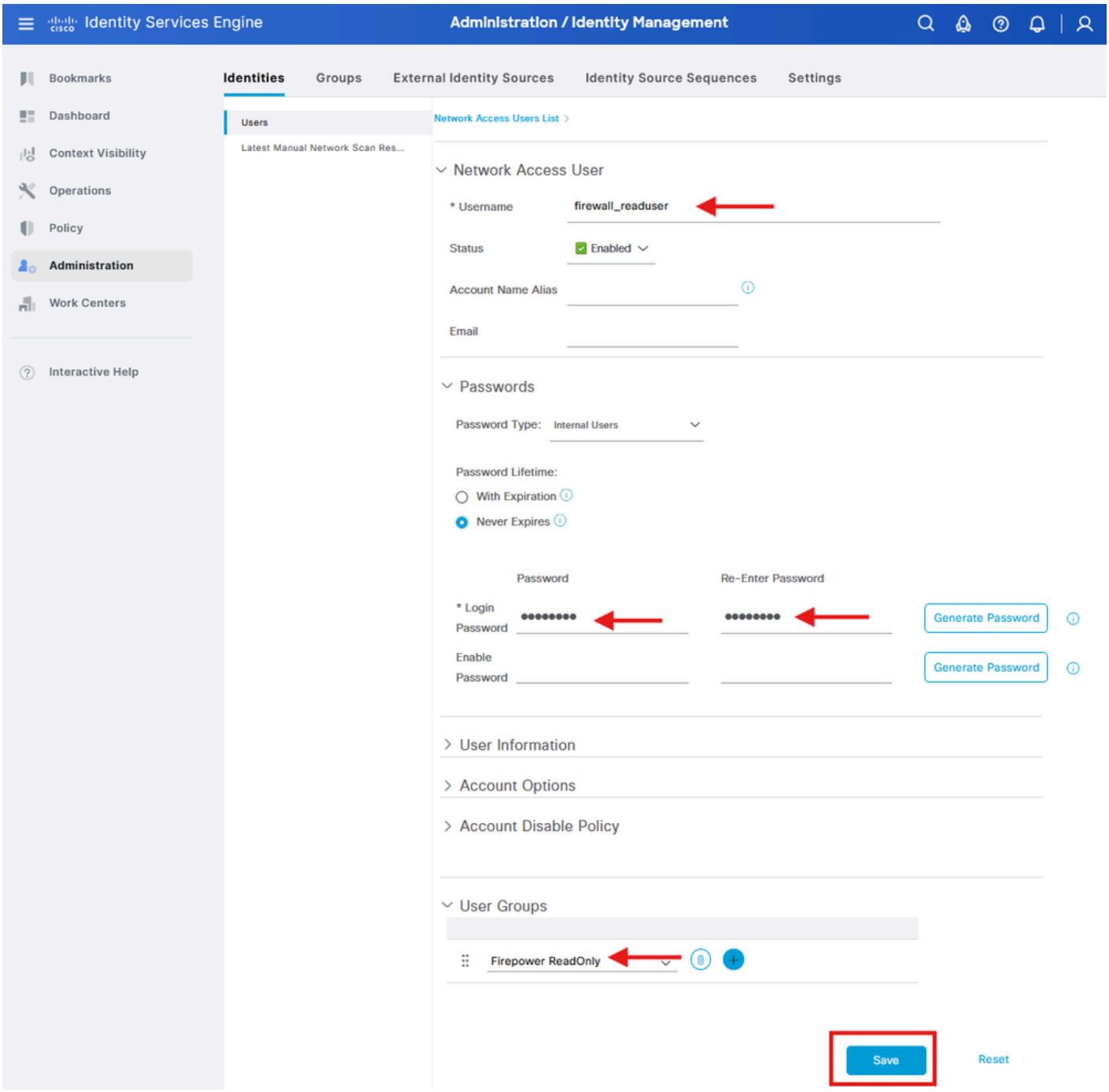
Paso 5. Cree los usuarios locales y agréguelos a su grupo correspondiente. Vaya a > Administration > Identity Management > Identities > + Add.



Paso 5.1. Cree primero el usuario con derechos de administrador. Asigne un nombre, una contraseña y el grupo Firepower Admins.



Paso 5.2. Agregue el usuario con derechos de sólo lectura. Asigne un nombre, una contraseña y el grupo Firepower ReadOnly.



Crear los perfiles de autorización

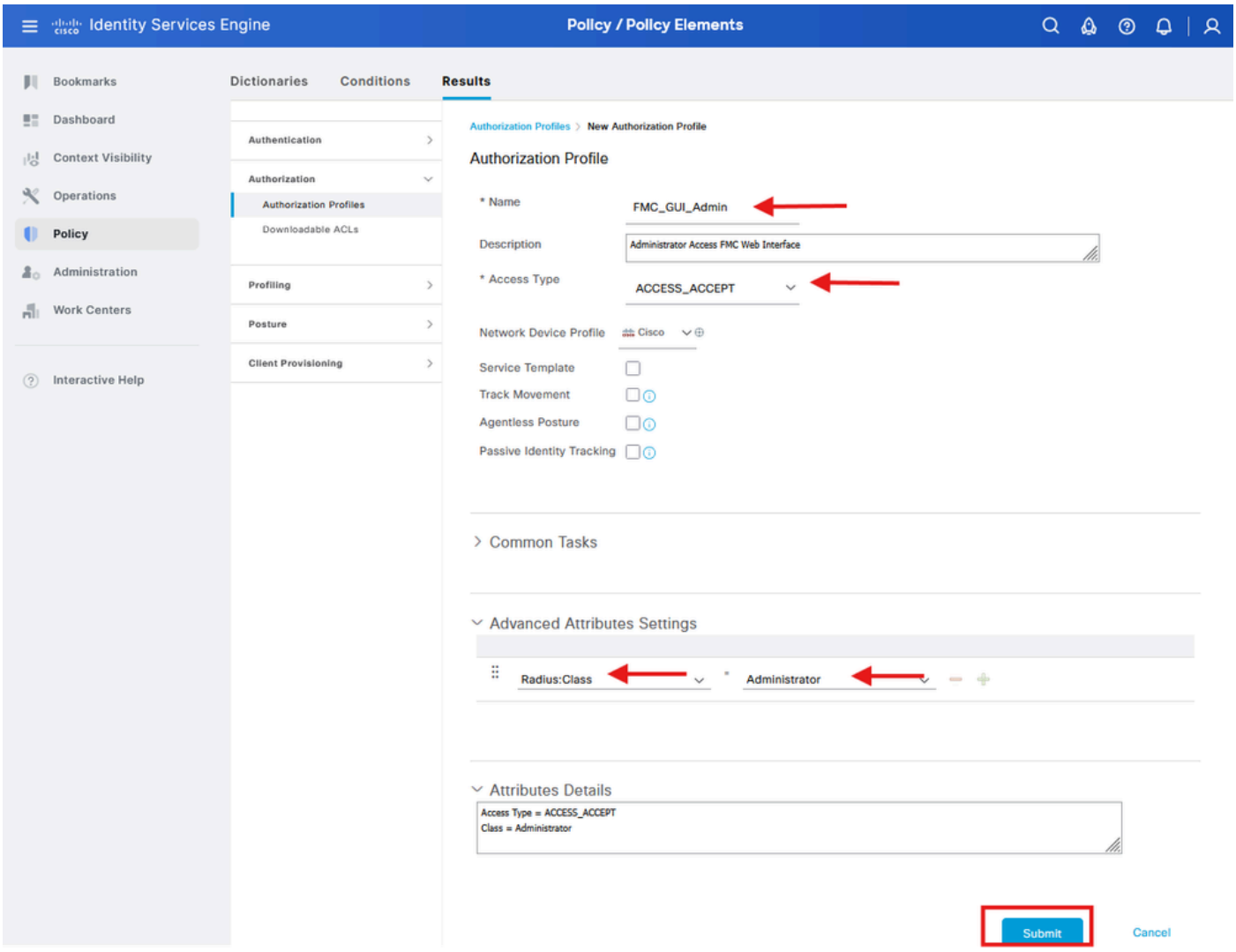
Paso 6. Cree el perfil de autorización para el usuario administrador de la interfaz web de FMC.

Vaya a

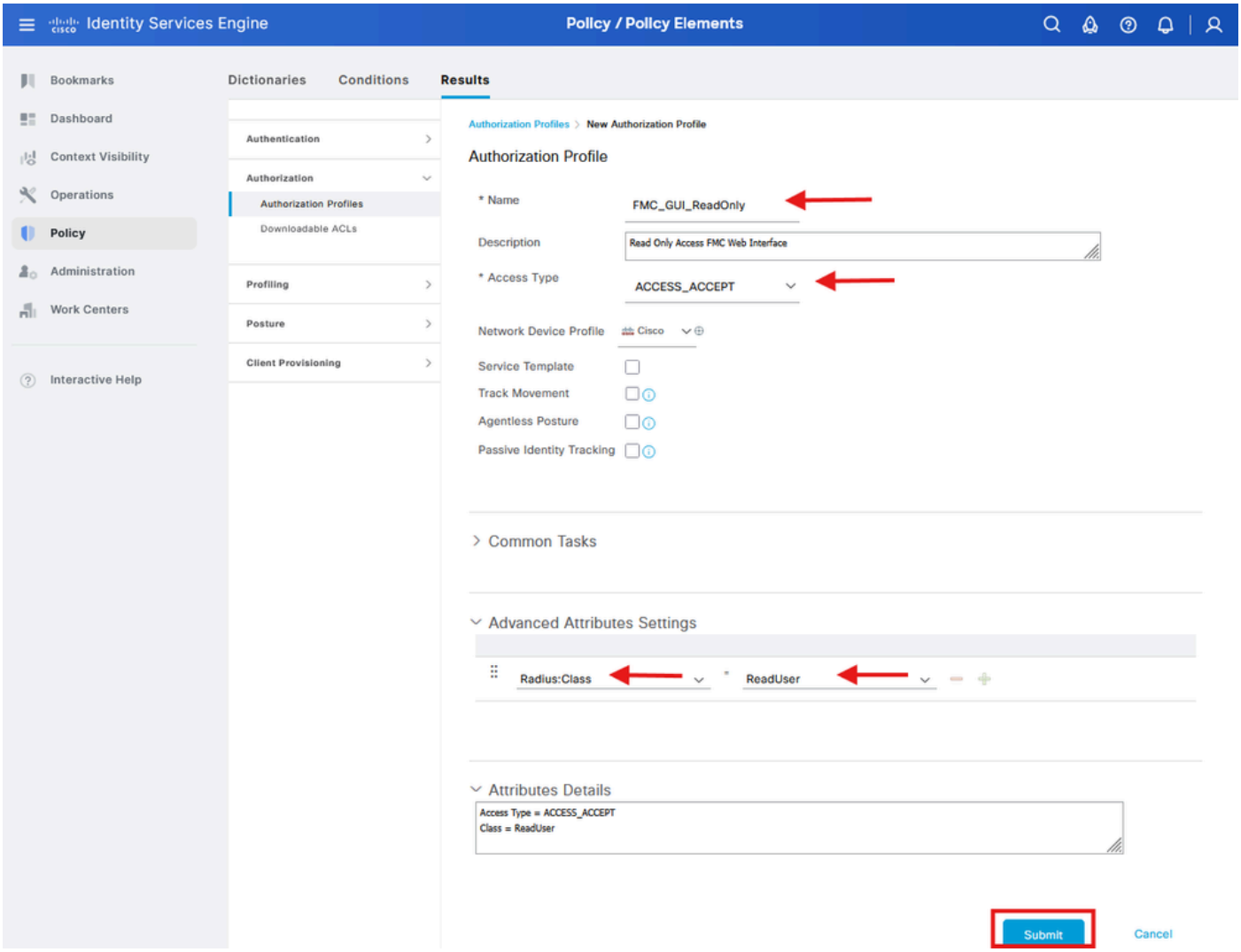
> Directiva > Elementos de directiva > Resultados > Autorización > Perfiles de autorización > +Agregar.

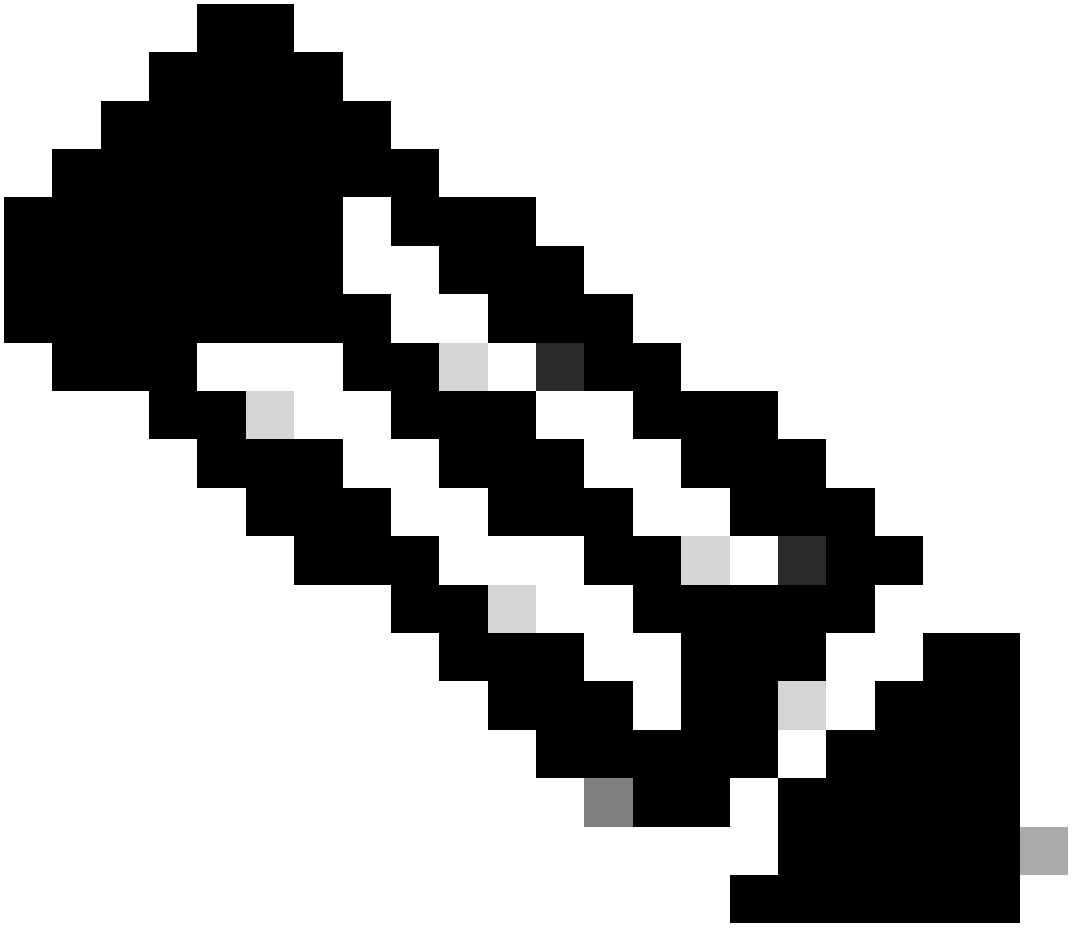
Defina un nombre para el perfil de autorización, deje el tipo de acceso como ACCESS_ACCEPT.

En Advanced Attributes Settings (Parámetros de atributos avanzados), agregue un Radius > Class—[25] con el valor Administrator y haga clic en Submit.



Paso 6.1. Repita el paso anterior para crear el perfil de autorización para el usuario de sólo lectura de la interfaz web de FMC. Cree la clase Radius con el valor ReadUser en su lugar Administrator esta vez.


Identity Services Engine
Policy / Policy Elements
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Help
Dictionaries
Conditions
Results
Authentication
Authorization
Authorization Profiles
Downloadable ACLs
Profiling
Posture
Client Provisioning
Authorization Profiles > New Authorization Profile
Authorization Profile
* Name
FMC_GUI_ReadOnly
Description
Read Only Access FMC Web Interface
* Access Type
ACCESS_ACCEPT
Network Device Profile
Cisco
Service Template
Track Movement
Agentless Posture
Passive Identity Tracking
Common Tasks
Advanced Attributes Settings
Radius:Class
ReadUser
Attributes Details
Access Type = ACCESS_ACCEPT
Class = ReadUser
Submit
Cancel



Nota: Para FMC (todas las versiones) y FTD (6.2.3 y 6.3), debe definir los usuarios para el acceso de la interfaz de línea de comandos (CLI) en el objeto de autenticación externa de FMC, que se muestra en el paso 4 del procedimiento de configuración de FMC. Para FTD 6.4 y versiones posteriores, recomendamos definir usuarios en el servidor RADIUS como se muestra en el siguiente paso.

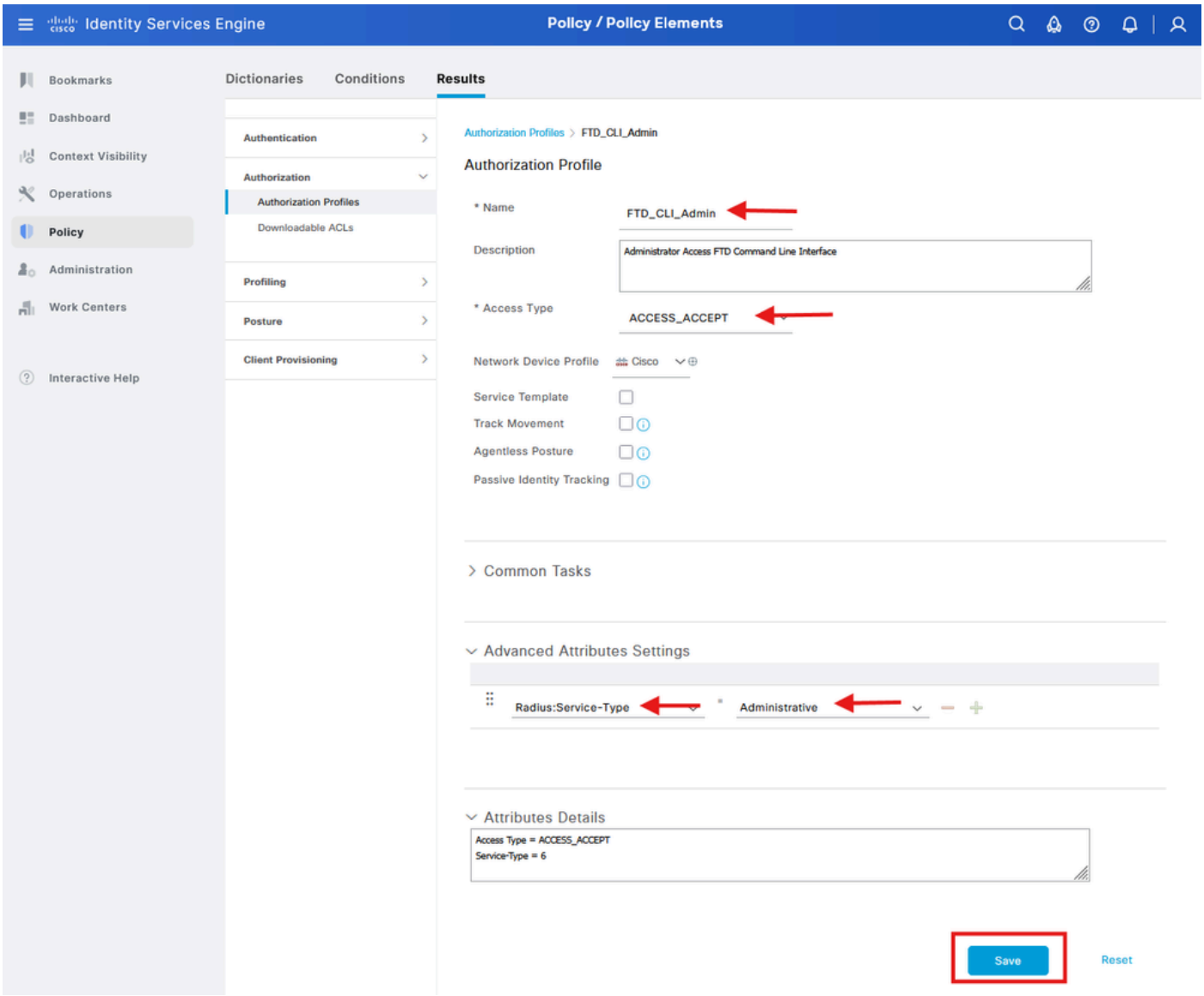
Paso 7. Crear el perfil de autorización para el usuario CLI de FTD con derechos de administrador.

Vaya a

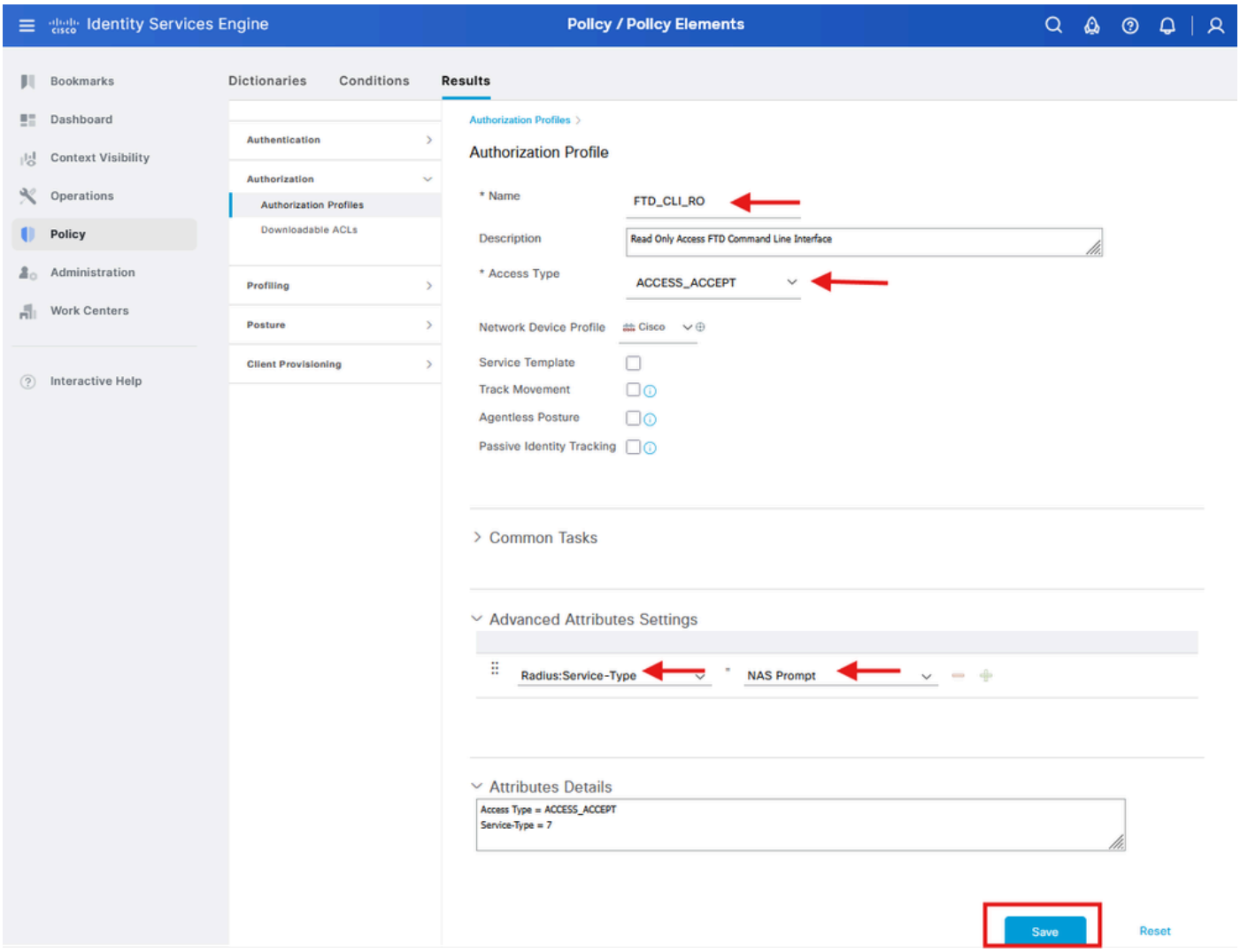
> Directiva > Elementos de directiva > Resultados > Autorización > Perfiles de autorización > +Agregar.

Defina un nombre para el perfil de autorización, deje el tipo de acceso como ACCESS_ACCEPT.

En Advanced Attributes Settings (Parámetros de atributos avanzados), agregue Radius > Service-Type—[6] con el valor Administrative y haga clic en Submit.



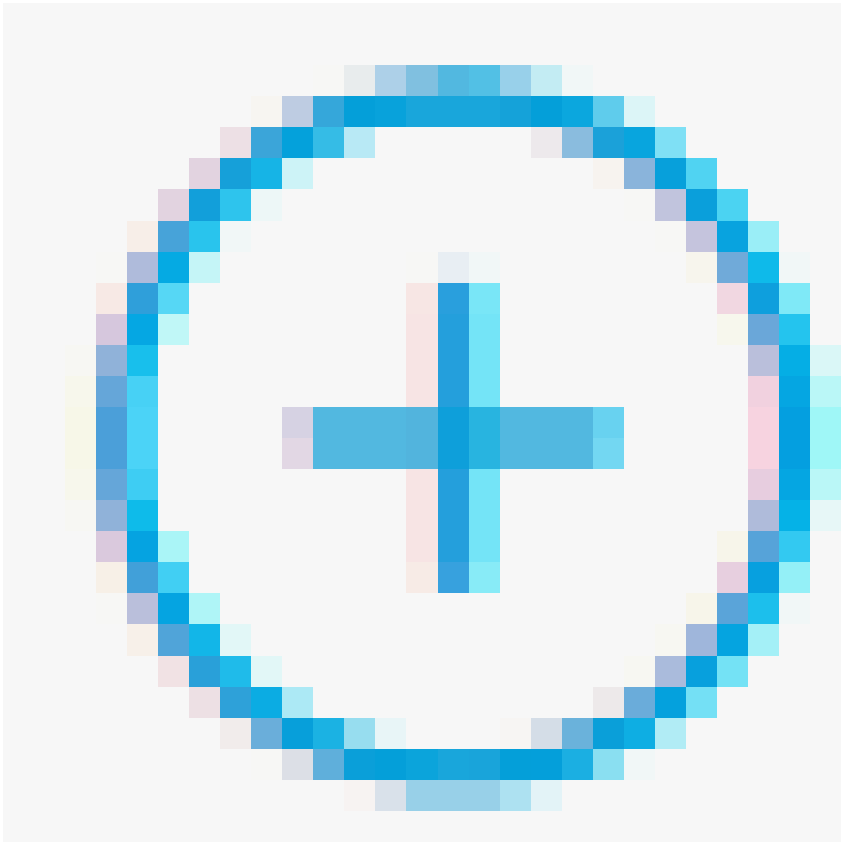
Paso 7.1. Repita el paso anterior para crear el perfil de autorización para el usuario de sólo lectura de CLI de FTD. Esta vez cree Radius > Service-Type—[6] con el valor NAS Prompt en su lugar.



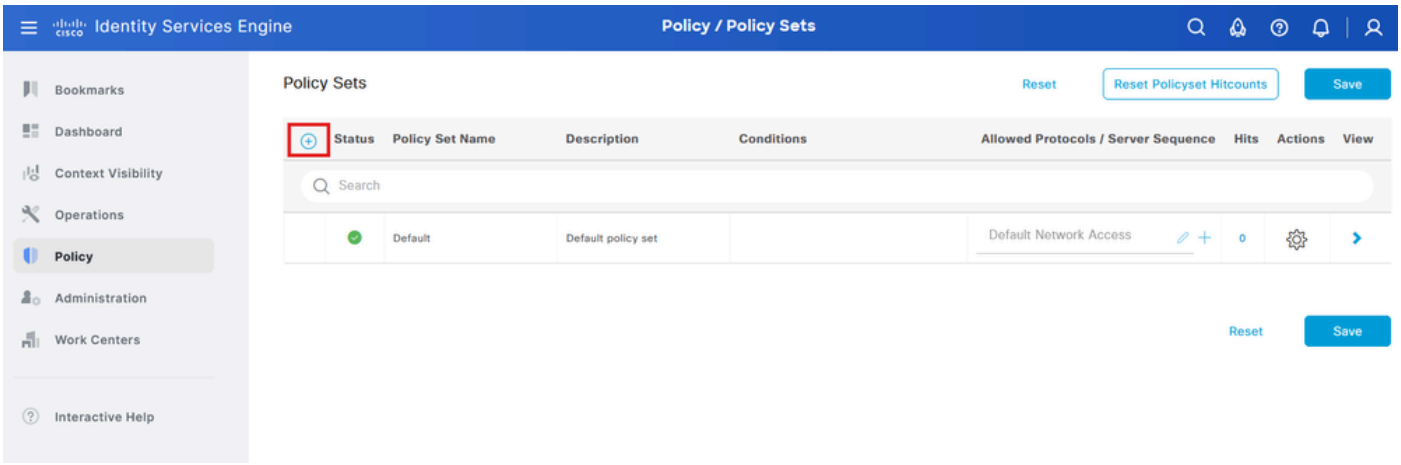
Agregar un nuevo conjunto de políticas

Paso 8. Cree un conjunto de políticas que coincida con la dirección IP del CSP. Esto es para evitar que otros dispositivos concedan acceso a los usuarios.

Vaya a



> Directiva > Conjuntos de directivas > situado en la esquina superior izquierda.

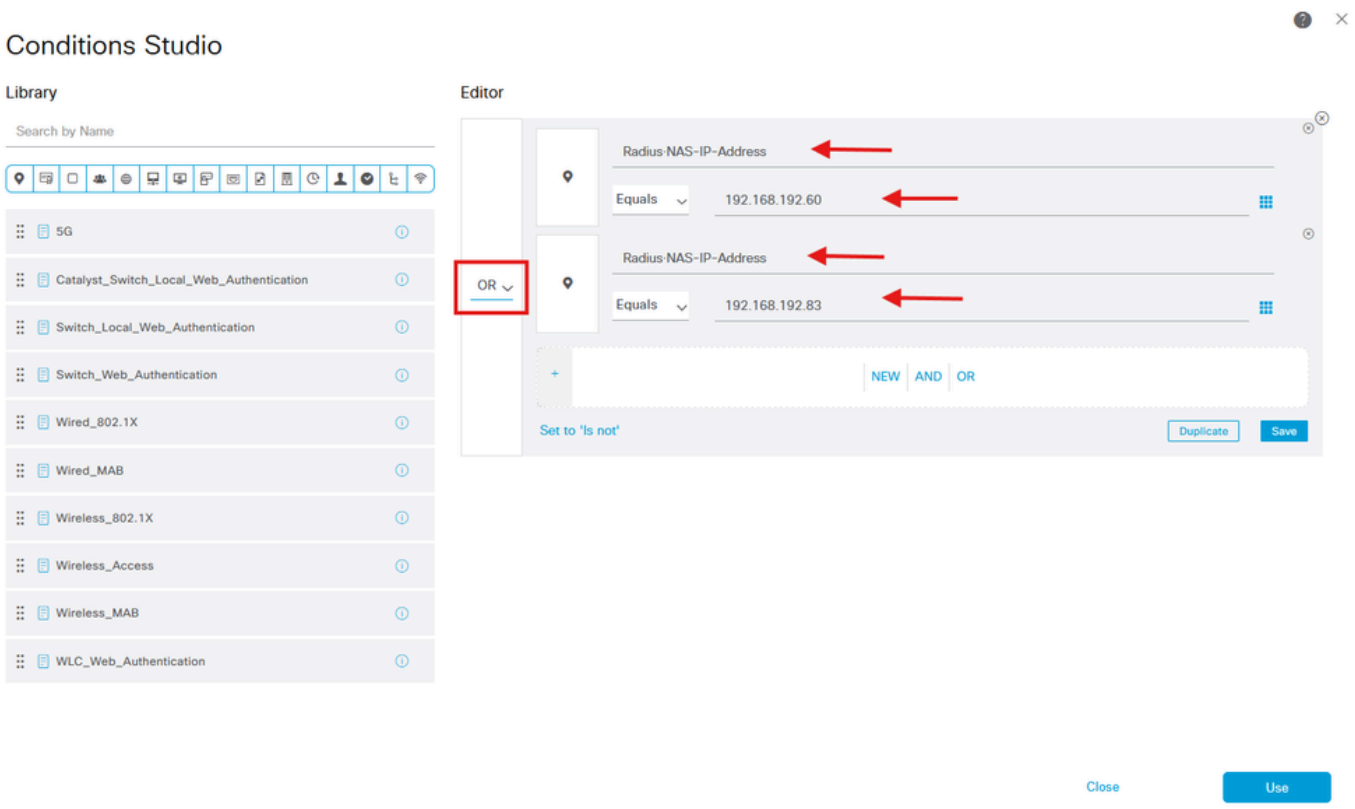


Paso 8.1. Se coloca una nueva línea en la parte superior de los conjuntos de políticas.

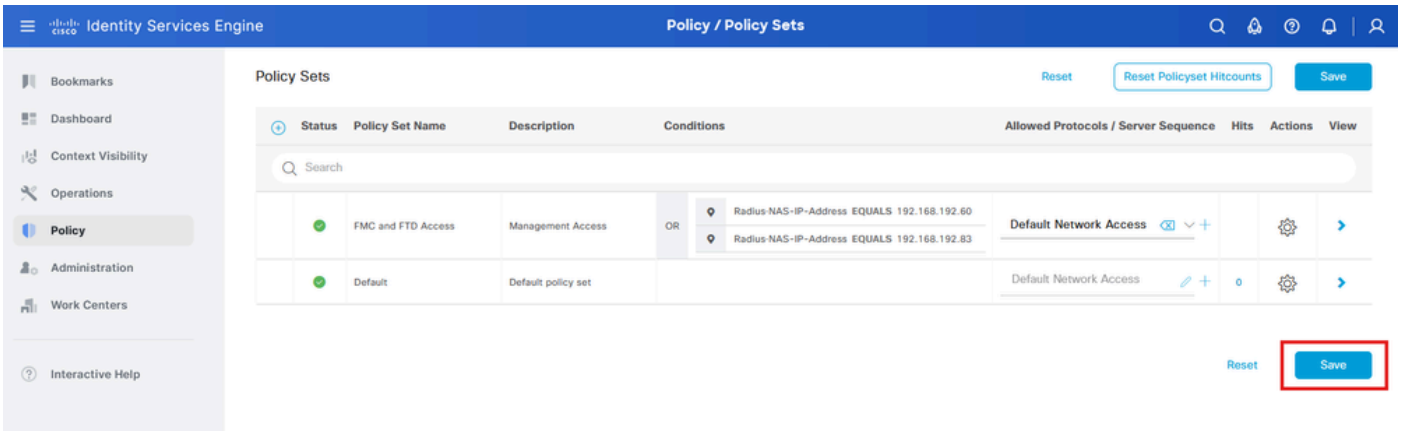
Asigne un nombre a la nueva política y agregue una condición superior para el atributo RADIUS NAS-IP-Address que coincida con la dirección IP de FMC.

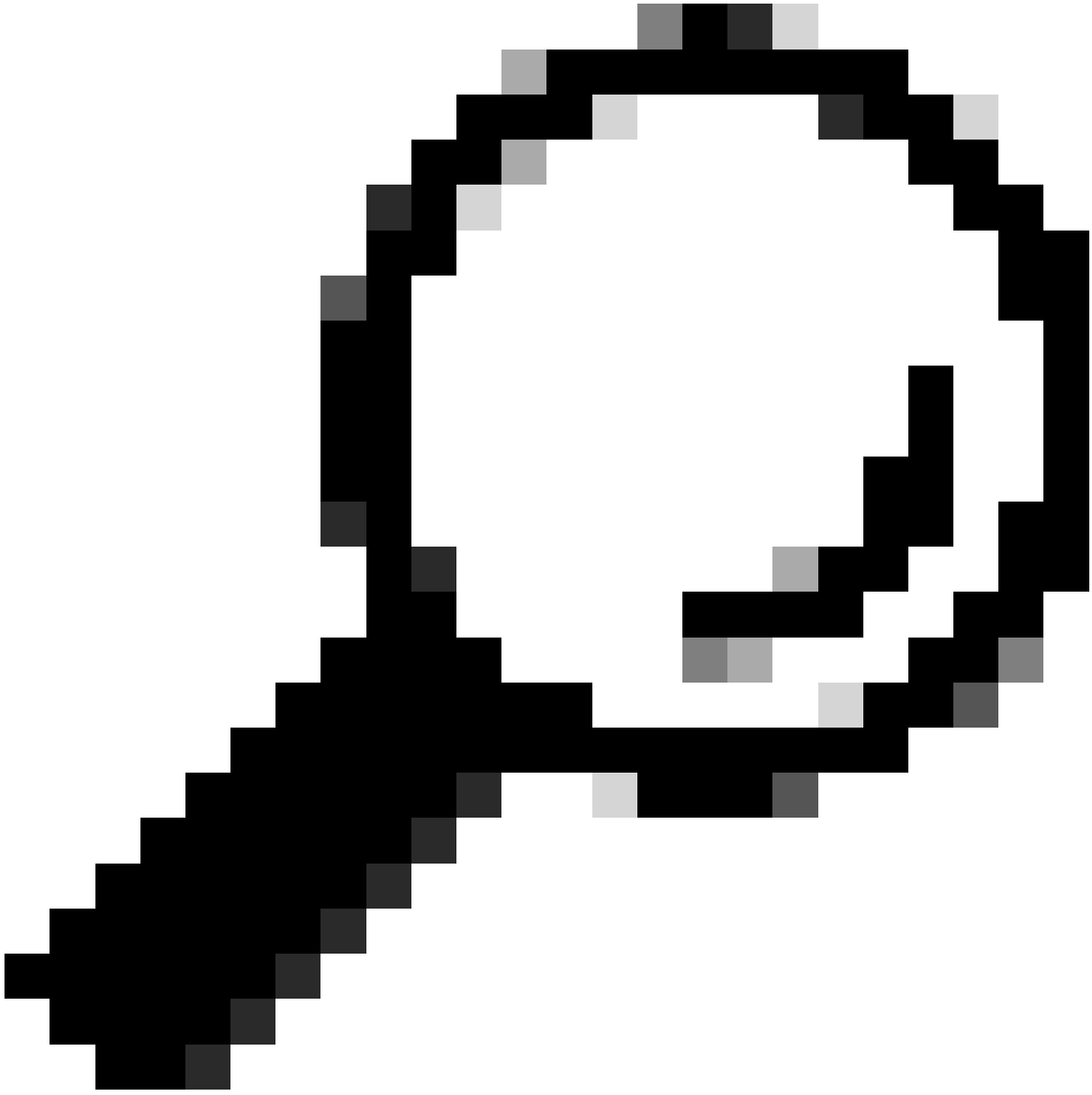
Agregue una segunda condición con OR para incluir la dirección IP del FTD.

Haga clic en Utilizar para mantener los cambios y salir del editor.

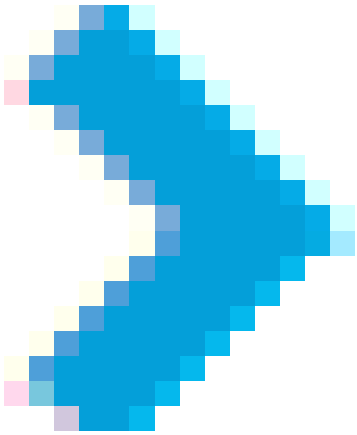


Paso 8.2. Una vez completado, presione Guardar.

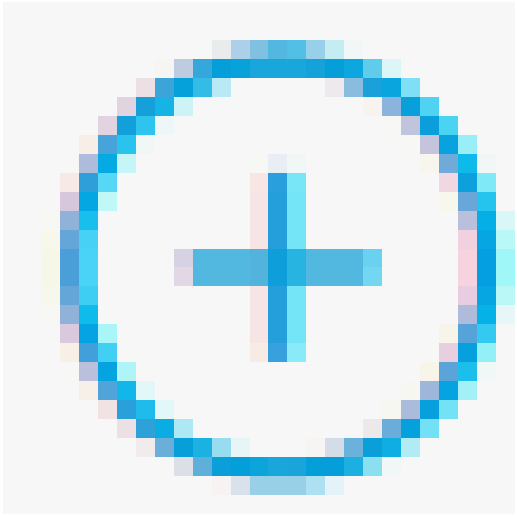




Consejo: Para este ejercicio hemos permitido la lista Default Network Access Protocols . Puede crear una lista nueva y reducirla según sea necesario.



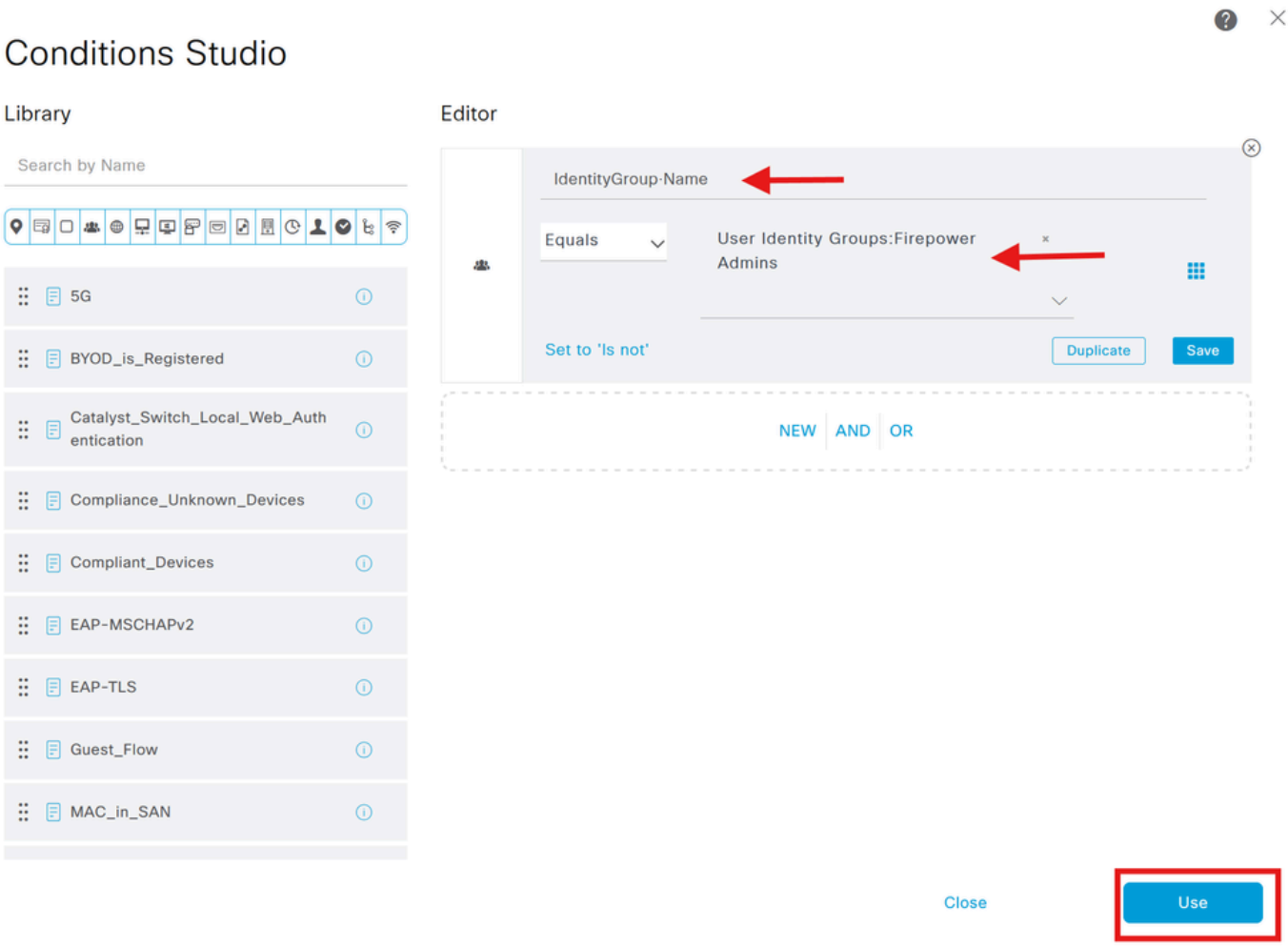
Paso 9. Consulte el nuevo conjunto de políticas pulsando el botón situado al final de la fila.



Expanda el menú Directiva de autorización y presione la tecla icono para agregar una nueva regla que permita el acceso al usuario con derechos de administrador.

Dale un nombre.

Establezca las condiciones para que el Grupo de Identidad de Diccionario coincida con el Nombre de Atributo Igual y elija Grupos de Identidad de Usuario: Firepower Admins (el nombre del grupo creado en el paso 4) y haga clic en Usar.

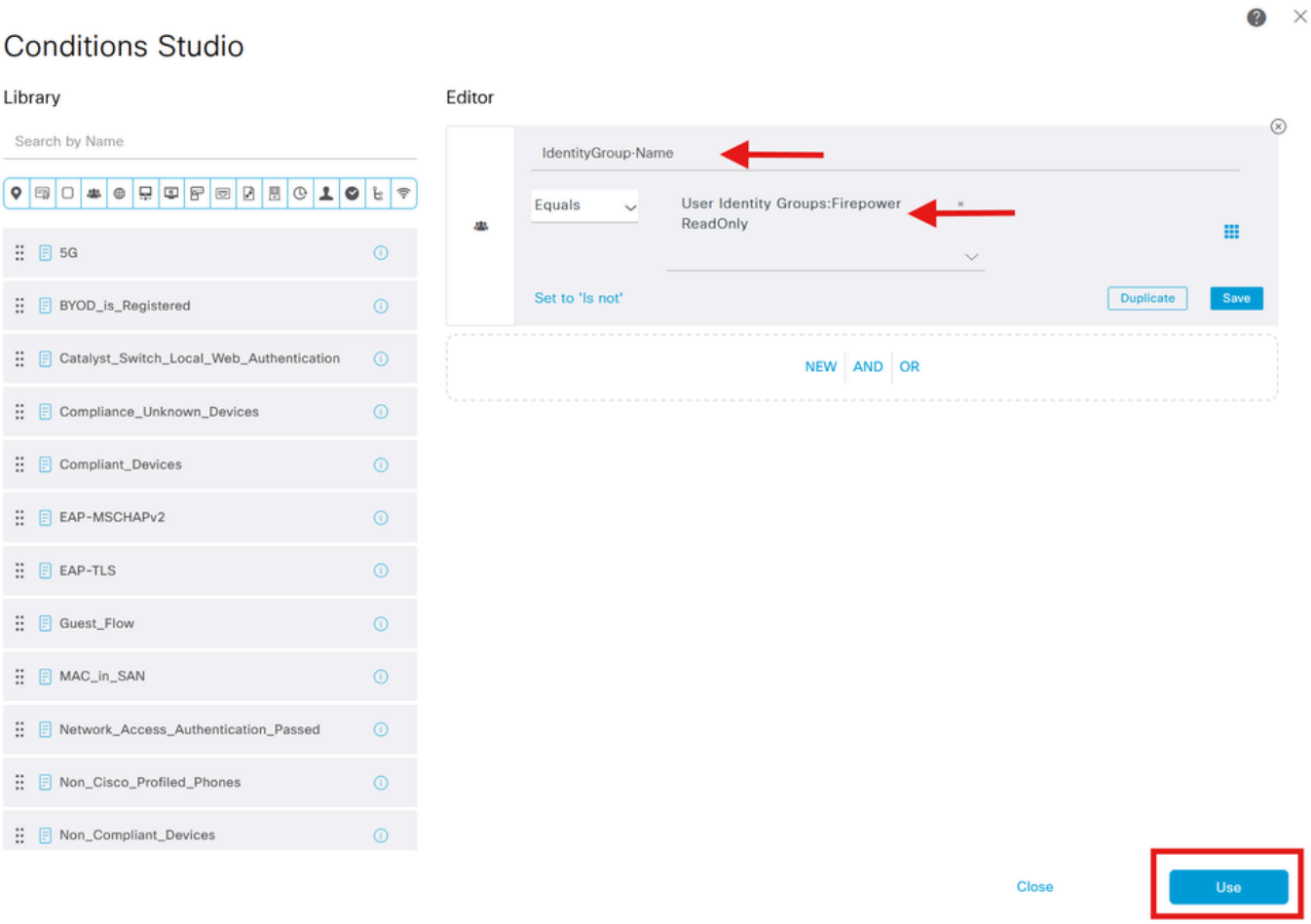


Paso 10. Haga clic en el botón

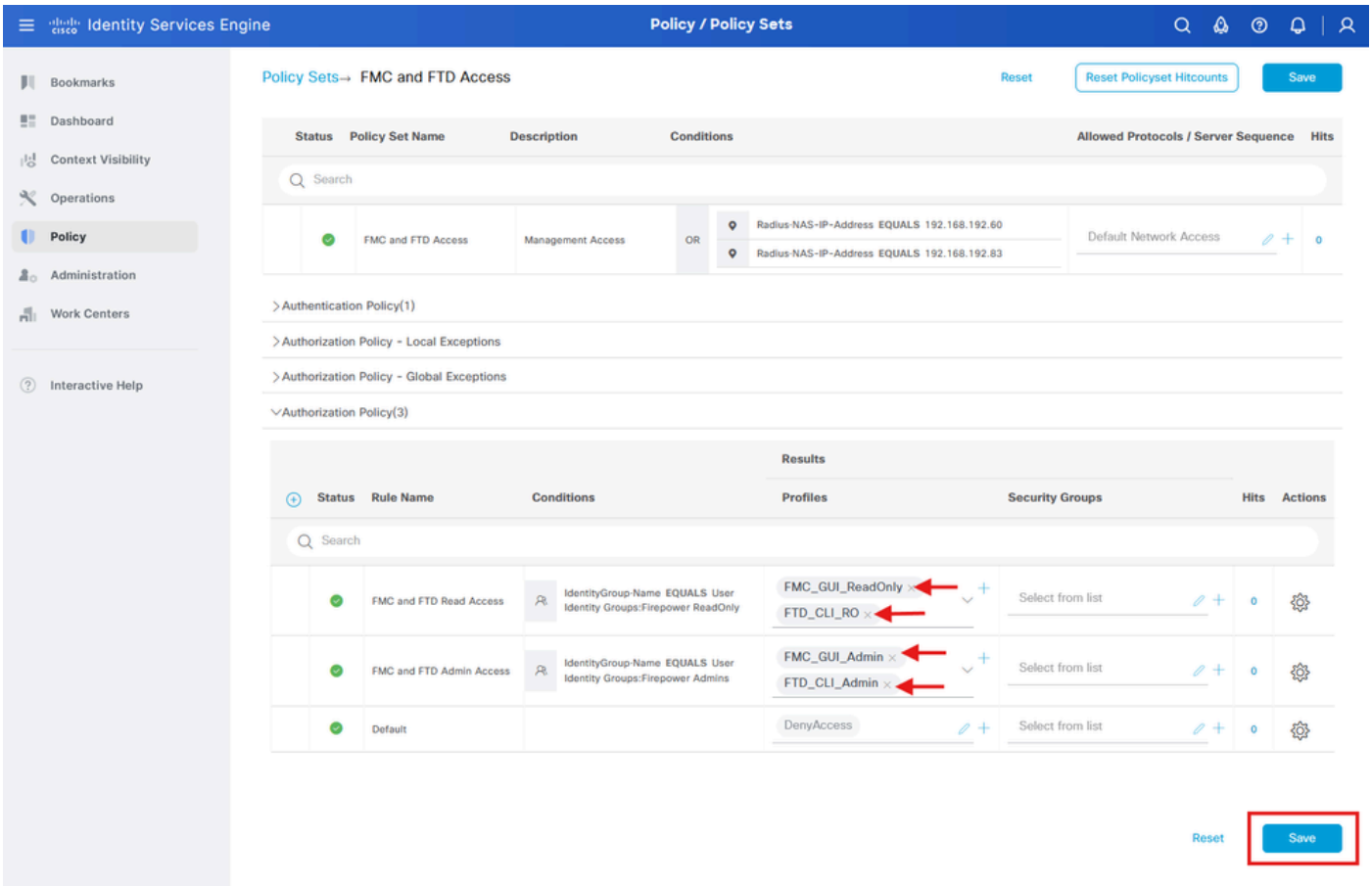
icono para agregar una segunda regla que permita el acceso al usuario con derechos de sólo lectura.

Dale un nombre.

Establezca las condiciones para que coincidan con el Grupo de Identidad de Diccionario con Nombre de Atributo Igual a Grupos de Identidad de Usuario: Firepower ReadOnly (el nombre de grupo creado en el paso 4.1) y haga clic en Use (Utilizar).



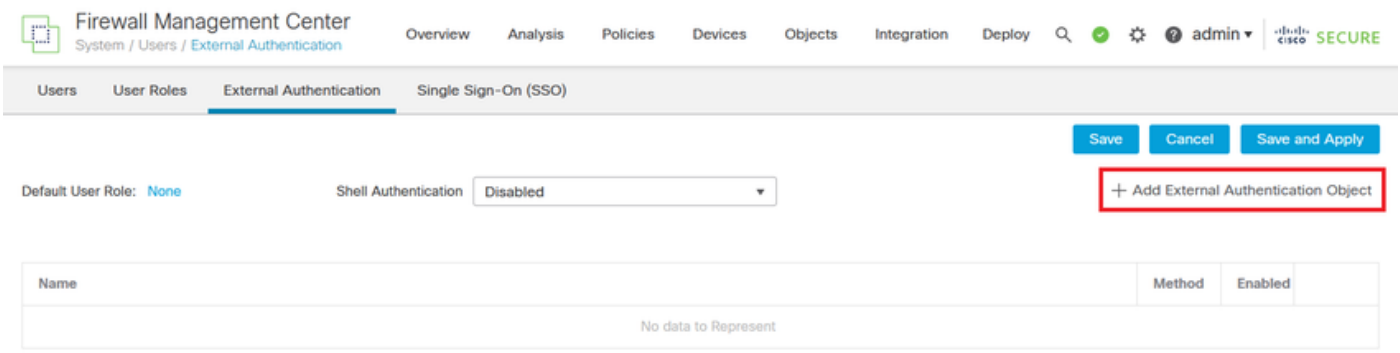
Paso 11. Establezca los perfiles de autorización para cada regla y haga clic en Guardar.



Configuración de FMC

Agregue su servidor RADIUS de ISE para la autenticación FMC

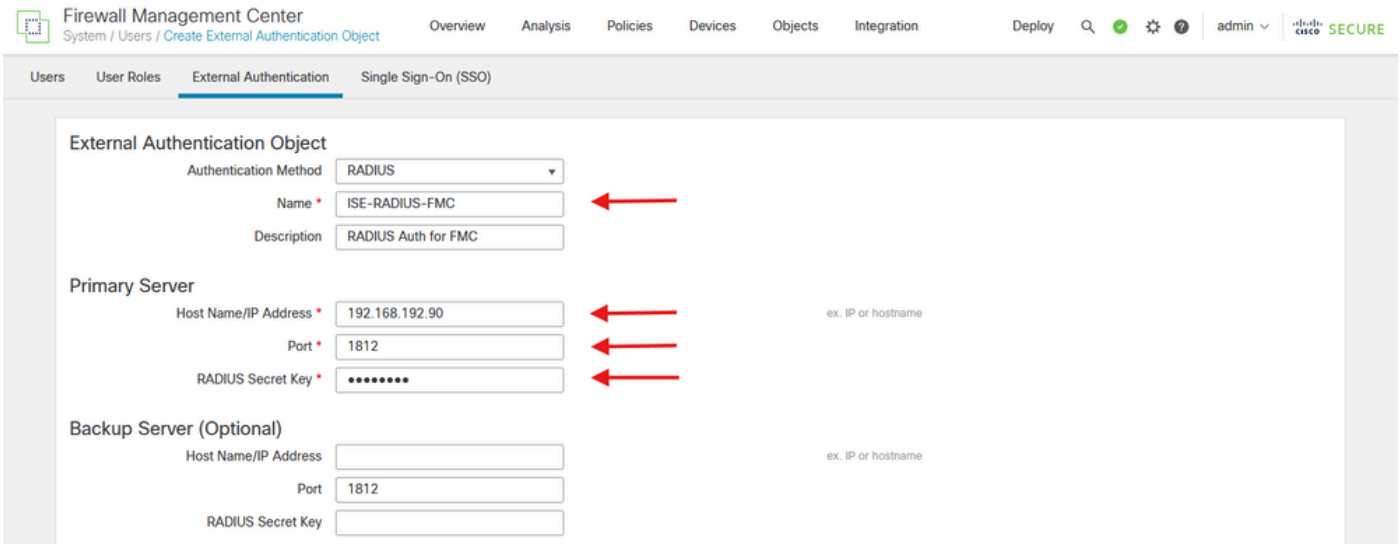
Paso 1. Cree el Objeto de Autenticación Externa en Sistema > Usuarios > Autenticación Externa > + Agregar Objeto de Autenticación Externa.



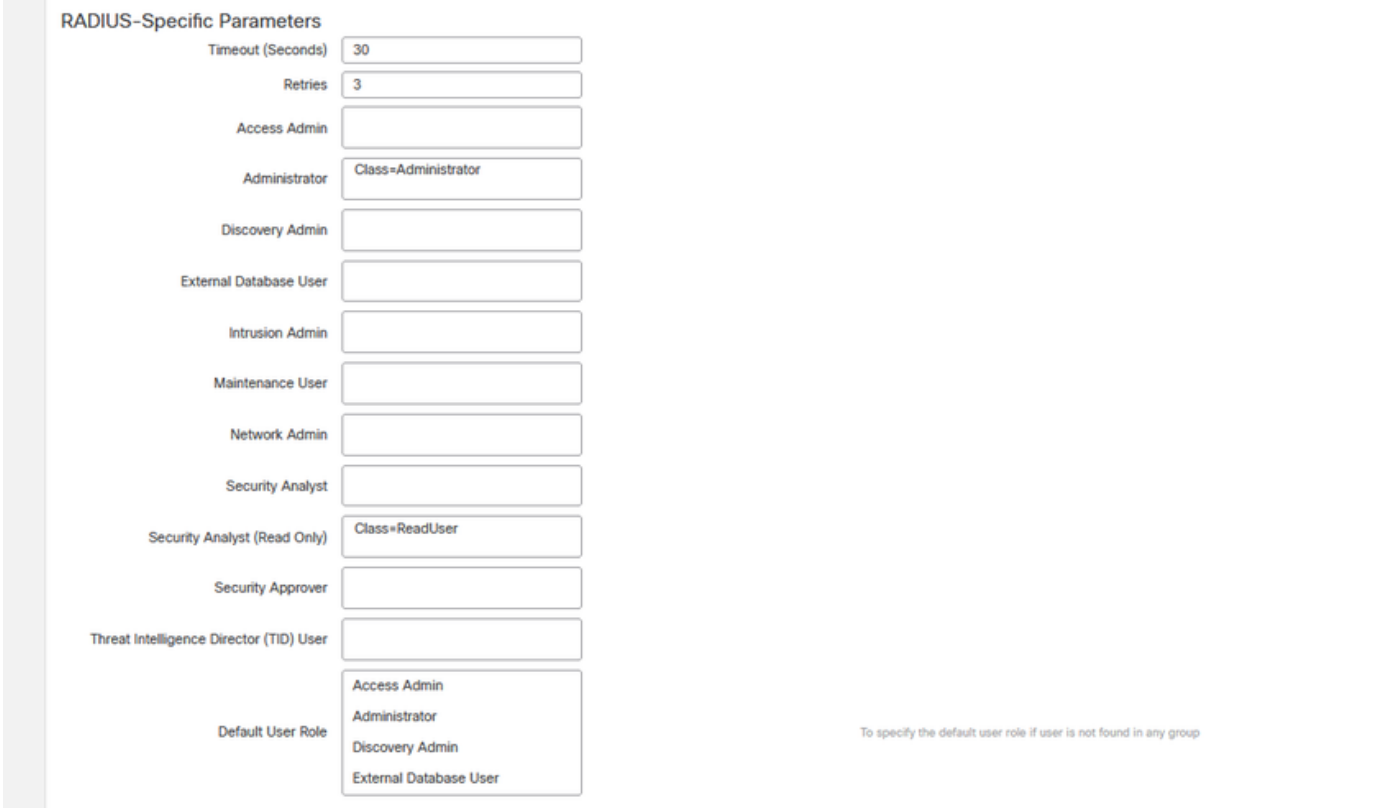
Paso 2. Seleccione RADIUS como método de autenticación.

En Objeto de autenticación externa, asigne un Nombre al nuevo objeto.

A continuación, en el parámetro Primary Server, inserte la dirección IP de ISE y la misma clave secreta RADIUS que utilizó en el paso 2 de la configuración de ISE.

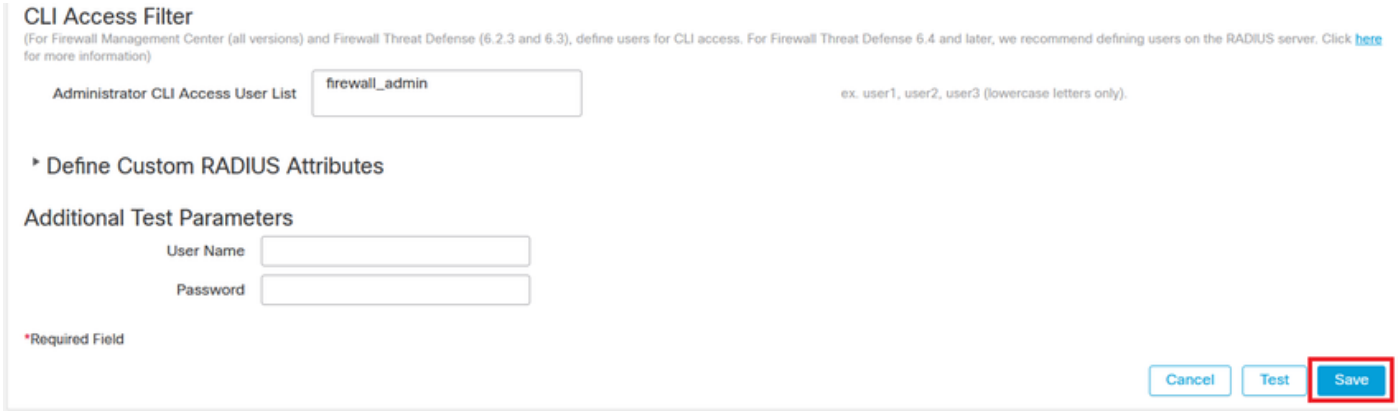


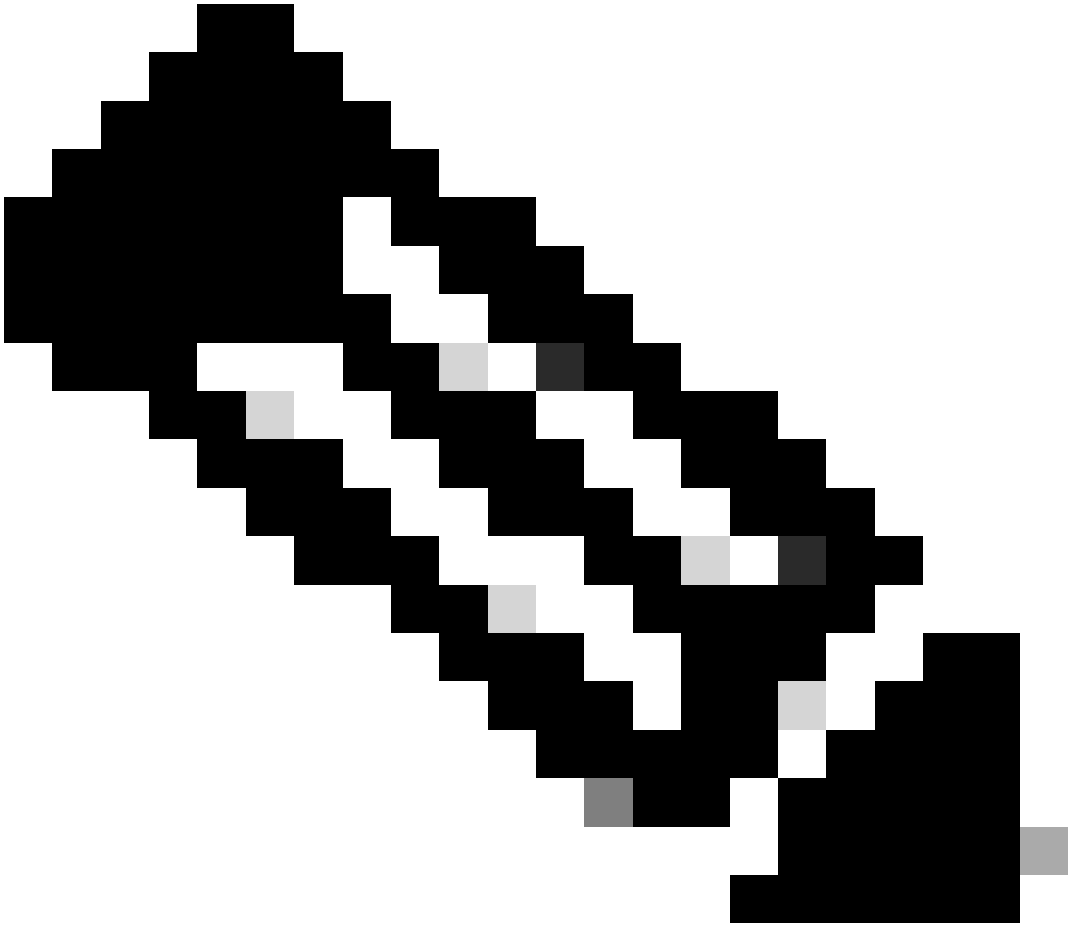
Paso 3. Inserte los valores de atributos de clase RADIUS que se configuraron en los pasos 6 y 7 de la configuración de ISE: Administrator y ReadUser para firewall_admin y firewall_readuser respectivamente.



Paso 4. Rellene la Lista de usuarios de acceso CLI del administrador en Filtro de acceso CLI con el nombre de usuario que debe tener acceso CLI al FMC.

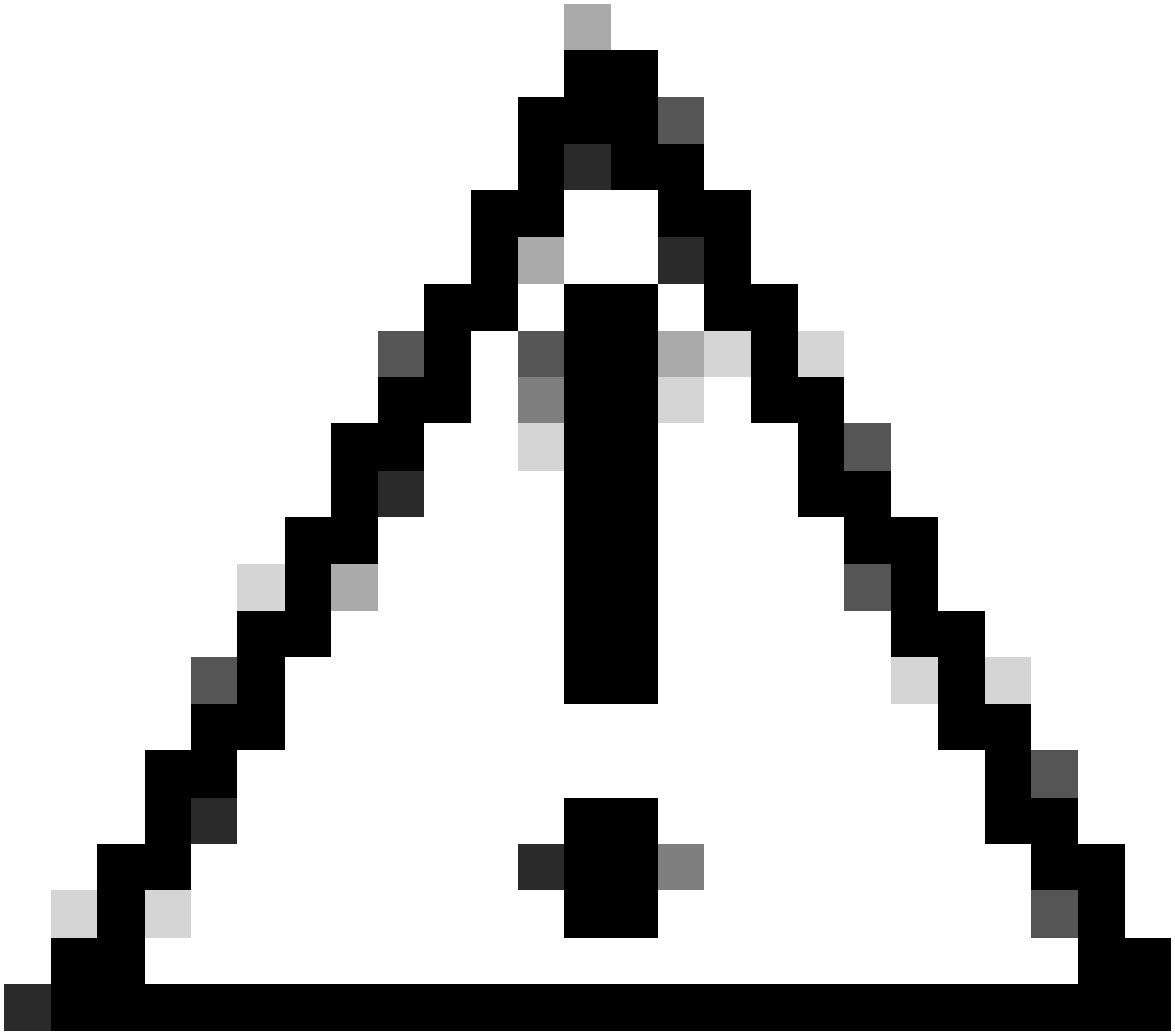
Haga clic en Guardar una vez hecho.





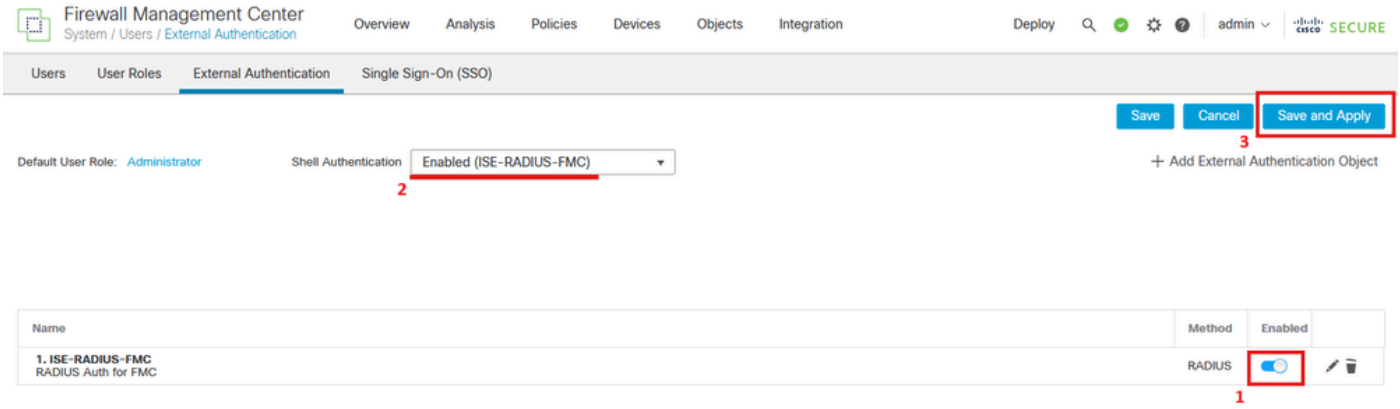
Nota: En este procedimiento, definimos los usuarios en el servidor RADIUS mediante el atributo Service-Type para evitar que los usuarios de ReadOnly obtengan acceso CLI al FTD con derechos de experto.

Para acceder a la CLI de FMC debe utilizar esta lista de usuarios.



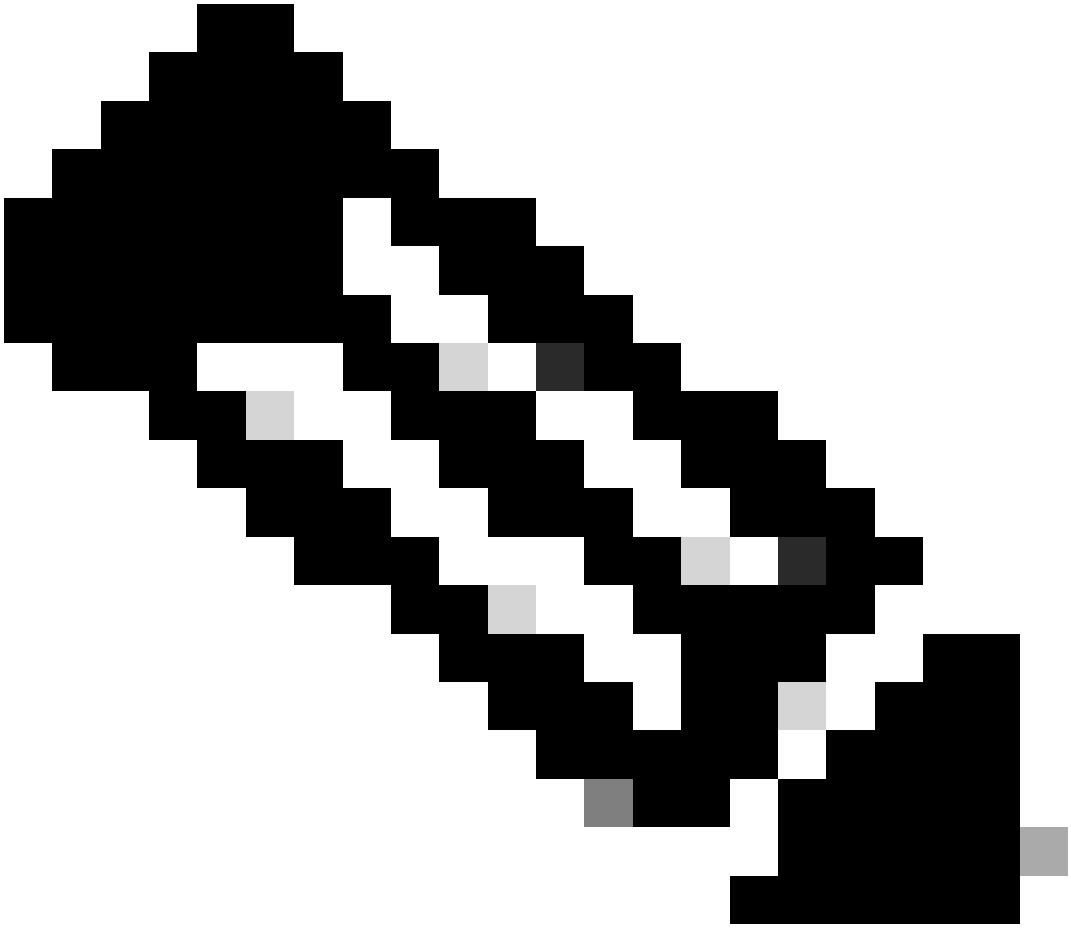
Precaución: Cualquier usuario con acceso CLI al FMC puede obtener acceso al shell de Linux con el comando expert. Los usuarios del shell de Linux pueden obtener privilegios de root, lo que puede representar un riesgo para la seguridad. Asegúrese de restringir la lista de usuarios con acceso al shell de CLI o Linux.

Paso 5. Habilite el nuevo objeto. Establézcalo como el método de autenticación de shell para FMC y haga clic en Guardar y aplicar.



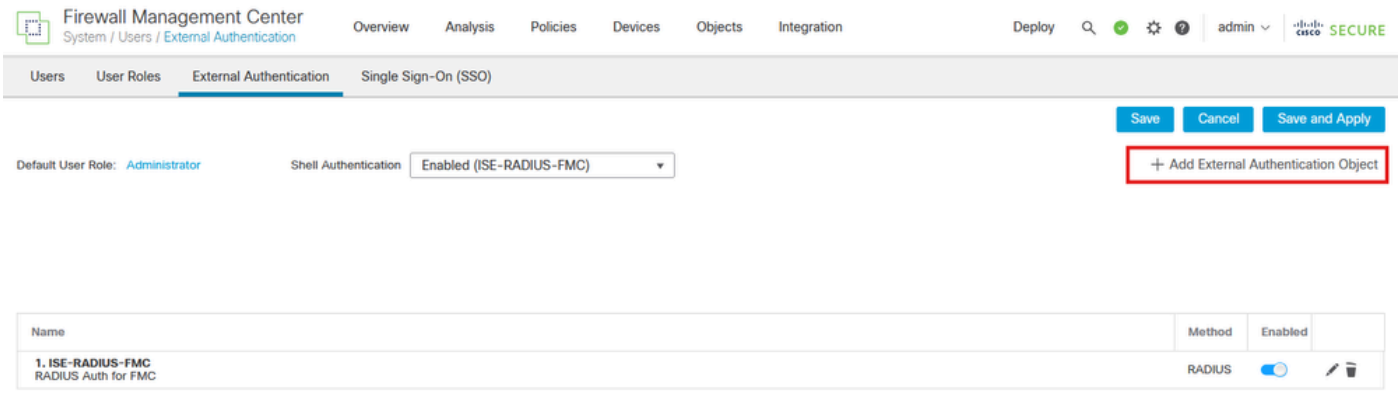
Configuración de FTD

Agregue su servidor RADIUS de ISE para la autenticación FTD



Nota: Puede compartir el mismo objeto entre el centro de gestión y los dispositivos o crear objetos independientes en función de dónde desee definir los usuarios y el nivel de autorización que deben tener. En esta situación, estamos definiendo a nuestros usuarios en el servidor RADIUS, por lo que necesitamos crear objetos independientes para la defensa frente a amenazas y el centro de gestión.

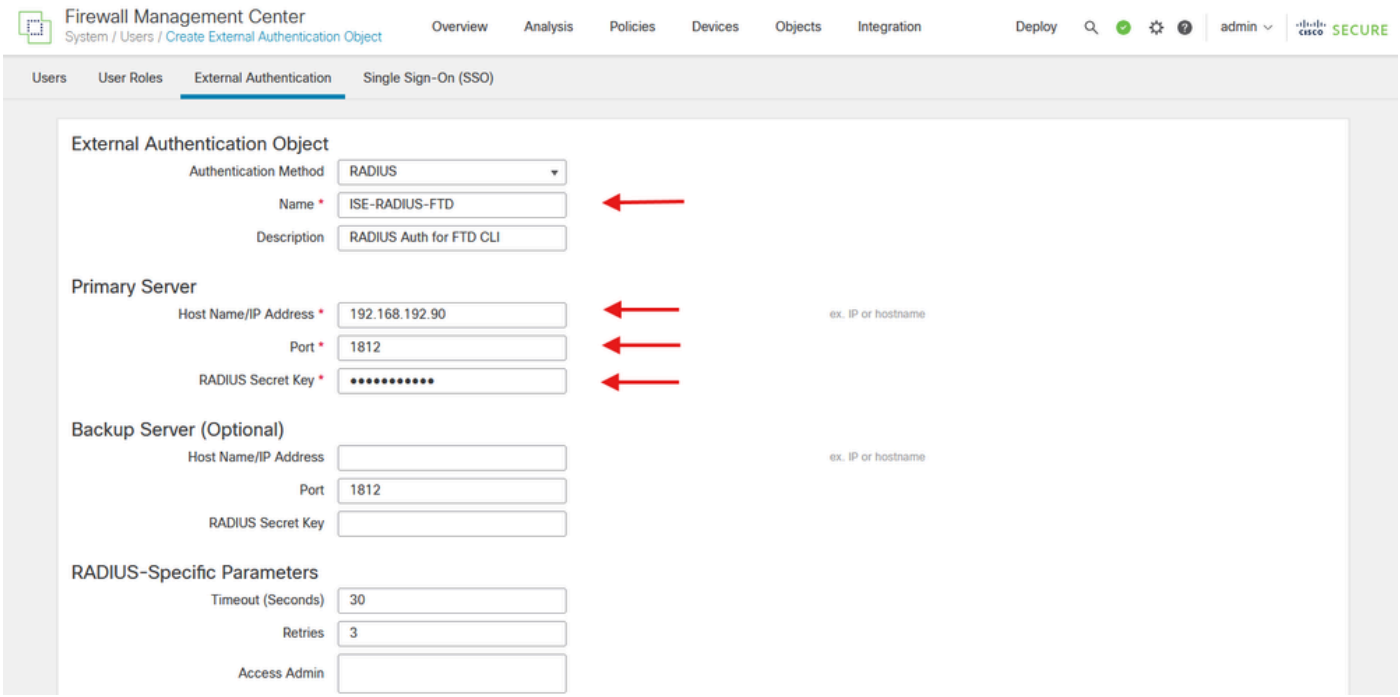
Paso 1. Igual que hizo para el FMC, cree el objeto de autenticación externa en Sistema > Usuarios > Autenticación externa > + Agregar objeto de autenticación externa.

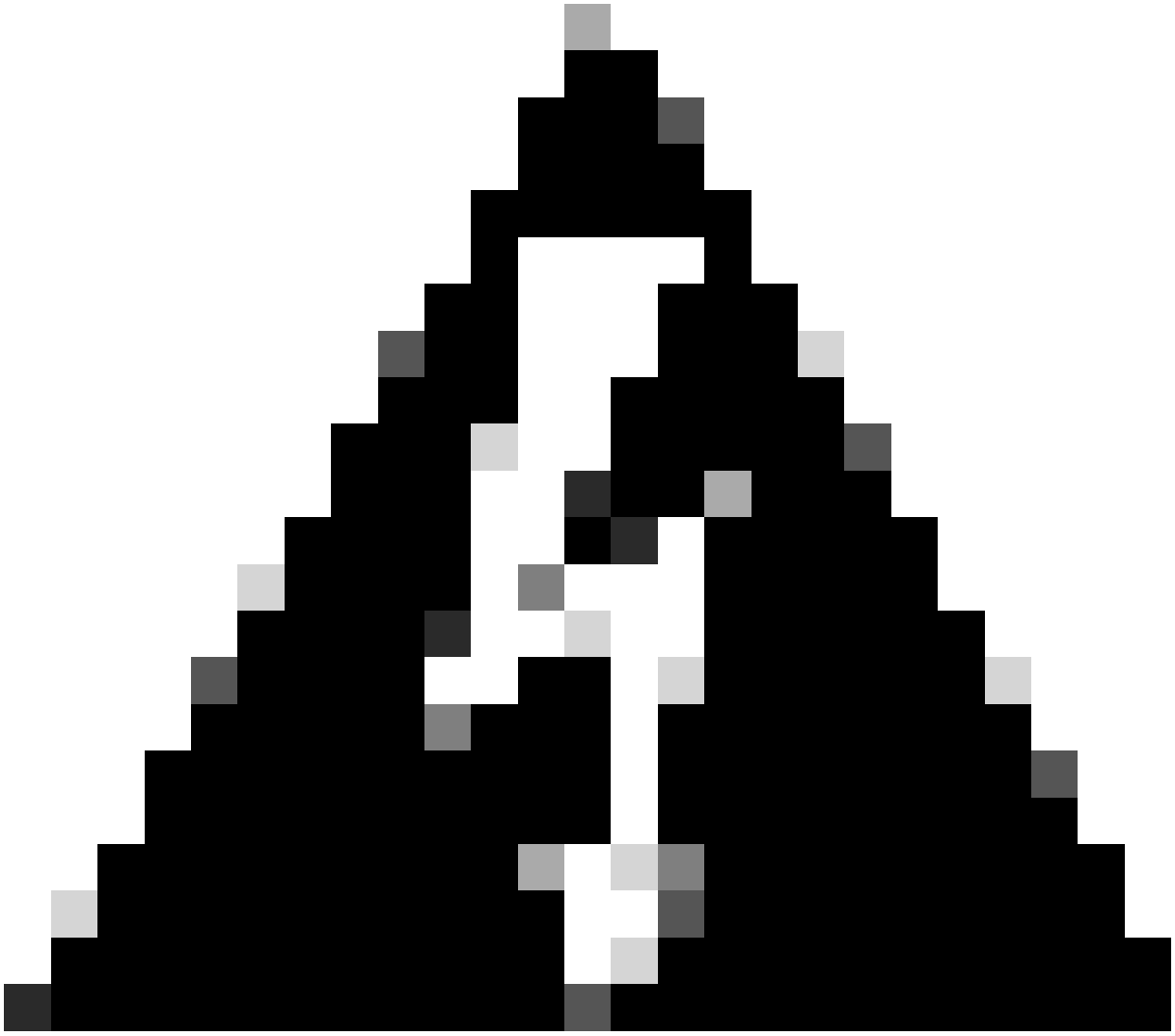


Paso 2. Seleccione RADIUS como método de autenticación.

En Objeto de autenticación externa, asigne un Nombre al nuevo objeto.

A continuación, en el parámetro Primary Server, inserte la dirección IP de ISE y la misma clave secreta RADIUS que utilizó en el paso 2.1 de la configuración de ISE. Haga clic en Save (Guardar).

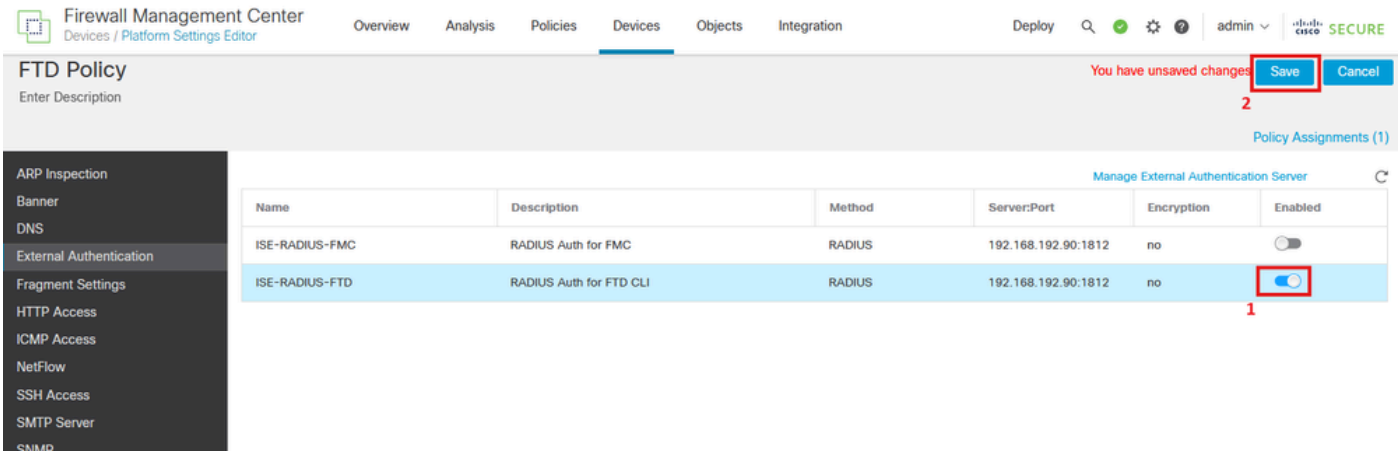




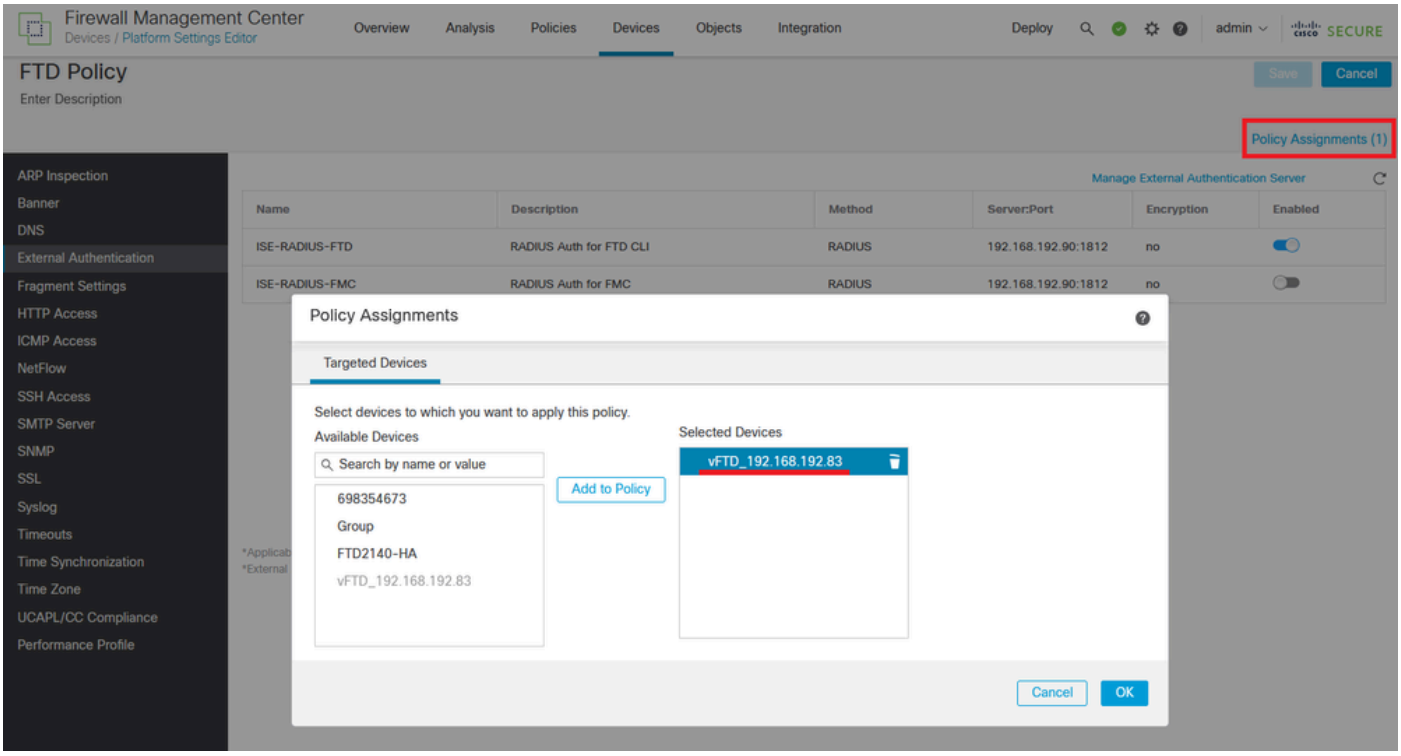
Advertencia: El intervalo de tiempo de espera es diferente para el FTD y el FMC, por lo que si comparte un objeto y cambia el valor predeterminado de 30 segundos, asegúrese de no exceder un intervalo de tiempo de espera menor (1-300 segundos) para los dispositivos FTD. Si establece el tiempo de espera en un valor más alto, la configuración RADIUS de defensa contra amenazas no funciona.

Habilitar el servidor RADIUS

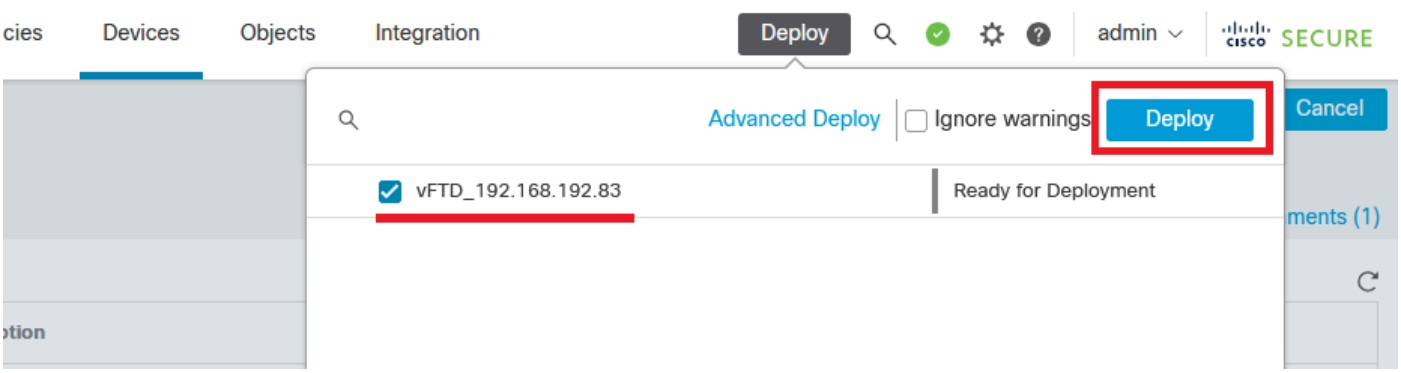
Paso 1. En la GUI de FMC, navegue hasta Dispositivos > Configuración de plataforma. Edite su política actual o cree una nueva si no tiene ninguna asignada al FTD al que necesita acceder. Habilite el servidor RADIUS bajo Autenticación Externa y haga clic en Guardar.

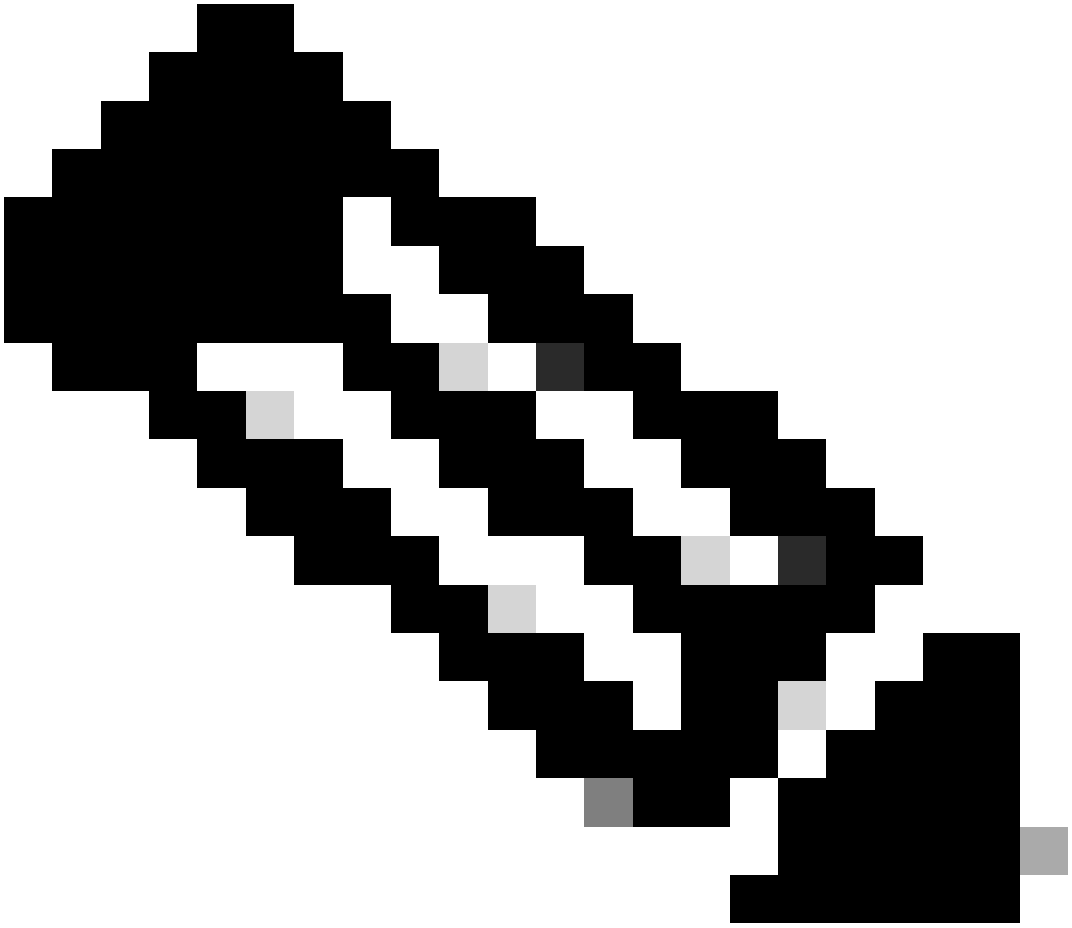


Paso 2. Asegúrese de que el FTD al que necesita acceder aparezca en Asignaciones de políticas como dispositivo seleccionado.



Paso 3. Implemente los cambios.

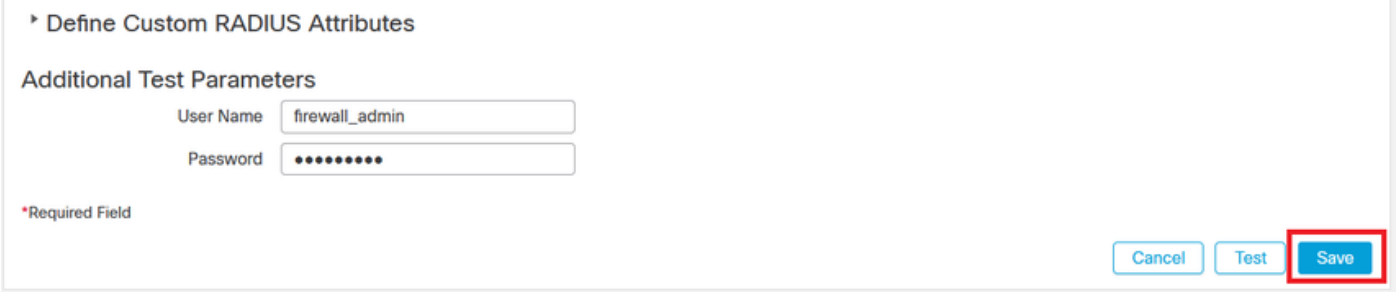




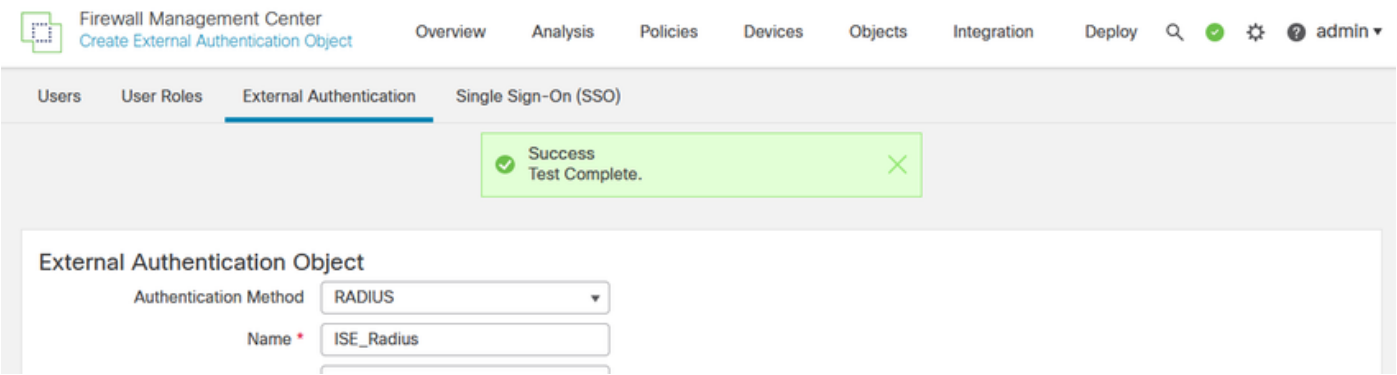
Nota: Si previamente configuró un nombre de usuario externo existente como usuario interno mediante el comando configure user add, threat defense primero verifica la contraseña contra el usuario interno y, si esto falla, verifica el servidor RADIUS. Tenga en cuenta que no puede agregar más adelante un usuario interno con el mismo nombre que un usuario externo, ya que la implementación fallará; solo se admiten usuarios internos preexistentes.

Verificación

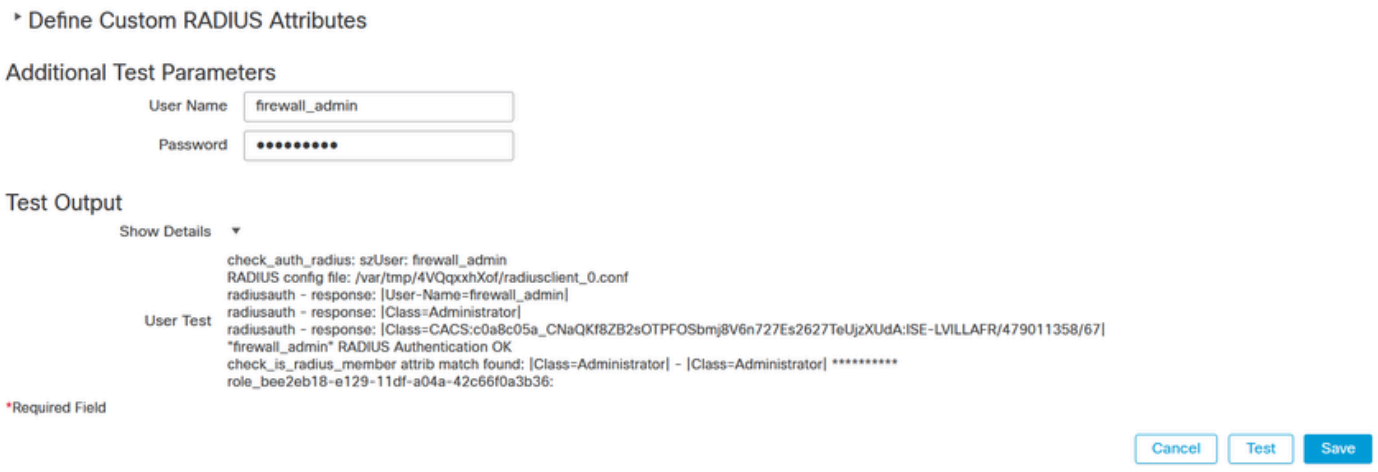
- Compruebe que la nueva implementación funciona correctamente.
- En la GUI de FMC, navegue hasta los parámetros del servidor RADIUS y desplácese hacia abajo hasta la sección Parámetros de prueba adicionales.
- Introduzca un nombre de usuario y una contraseña para el usuario de ISE y haga clic en Probar.



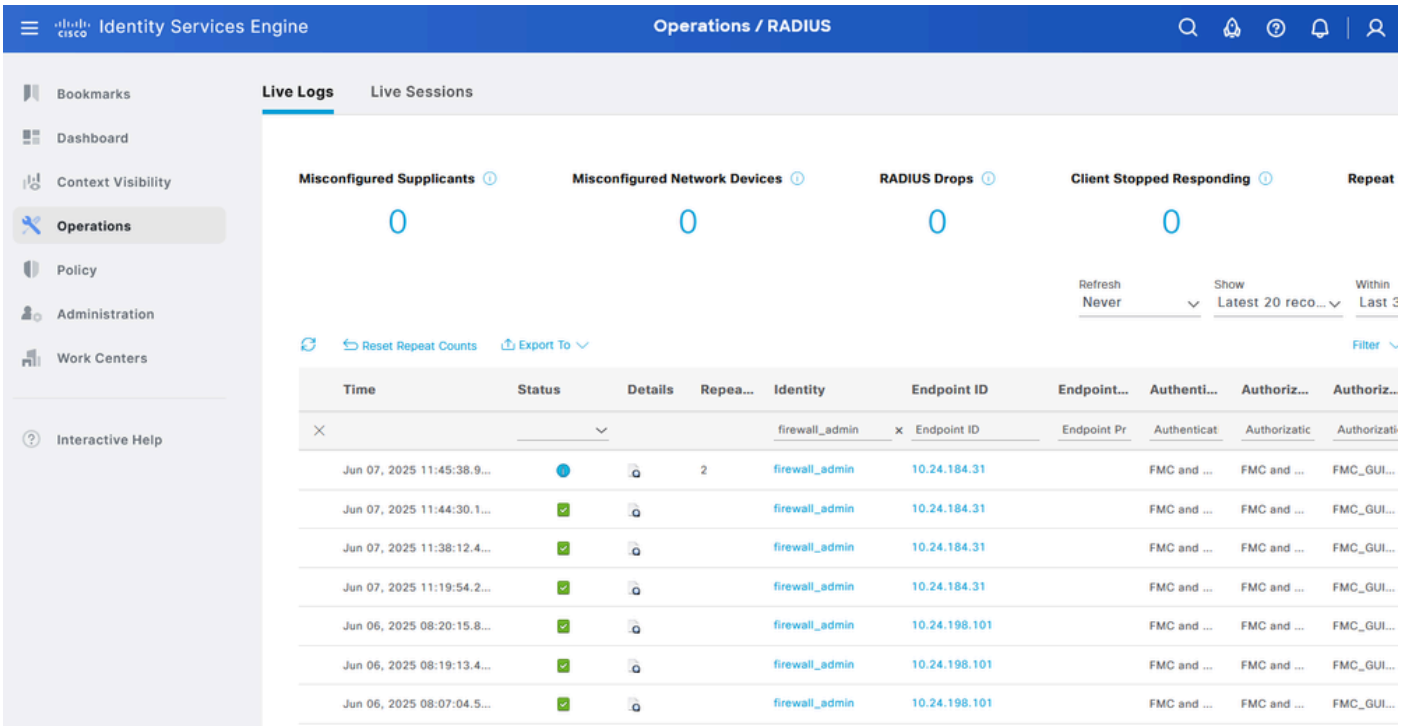
- Una prueba correcta muestra un mensaje verde Prueba de éxito completada en la parte superior de la ventana del navegador.



- Para obtener más información, puede expandir Detalles en Resultado de la prueba.



- Verifique la solicitud de autenticación y la respuesta en su ISE RADIUS en Operaciones > RADIUS > Registros en vivo.


Identity Services Engine
Operations / RADIUS
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Help
Live Logs
Live Sessions
Misconfigured Supplicants
0
Misconfigured Network Devices
0
RADIUS Drops
0
Client Stopped Responding
0
Repeat
Refresh
Never
Show
Latest 20 reco...
Within
Last 3
Reset Repeat Counts
Export To
Filter
Time
Status
Details
Repea...
Identity
Endpoint ID
Endpoint...
Authenti...
Authoriz...
Authoriz...
firewall_admin
Endpoint ID
Endpoint Pr
Authenticat
Authorizatic
Jun 07, 2025 11:45:38.9... 2 firewall_admin 10.24.184.31 FMC and ... FMC and ... FMC_GUI...
Jun 07, 2025 11:44:30.1... firewall_admin 10.24.184.31 FMC and ... FMC and ... FMC_GUI...
Jun 07, 2025 11:38:12.4... firewall_admin 10.24.184.31 FMC and ... FMC and ... FMC_GUI...
Jun 07, 2025 11:19:54.2... firewall_admin 10.24.184.31 FMC and ... FMC and ... FMC_GUI...
Jun 06, 2025 08:20:15.8... firewall_admin 10.24.198.101 FMC and ... FMC and ... FMC_GUI...
Jun 06, 2025 08:19:13.4... firewall_admin 10.24.198.101 FMC and ... FMC and ... FMC_GUI...
Jun 06, 2025 08:07:04.5... firewall_admin 10.24.198.101 FMC and ... FMC and ... FMC_GUI...

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).