Configuración de la autenticación y autorización externas de FDM con ISE mediante RADIUS

Contenido

Introducción

En este documento se describe el procedimiento para integrar Cisco Firepower Device Manager (FDM) con Identity Services Engine (ISE) para la autenticación de usuarios administradores con el protocolo RADIUS tanto para el acceso GUI como para el acceso CLI.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Administrador de dispositivos Firepower (FDM)
- Identity Services Engine (ISE)
- protocolo RADIUS

Componentes Utilizados

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

- Dispositivo Firepower Threat Defence (FTD), todas las plataformas Firepower Device Manager (FDM) versión 6.3.0+
- ISE versión 3.0

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.

Interoperabilidad

- Servidor RADIUS con usuarios configurados con funciones de usuario
- Los roles de usuario se deben configurar en el servidor RADIUS con cisco-av-pair
- Cisco-av-pair = fdm.userrole.authority.admin
- ISE se puede utilizar como servidor RADIUS

Licencias

Sin necesidad de licencia específica, la licencia básica es suficiente

Antecedentes

Esta función permite a los clientes configurar la autenticación externa con RADIUS y múltiples roles de usuario para esos usuarios.

Compatibilidad de RADIUS con Management Access con 3 funciones de usuario definidas por el sistema:

- READ_ONLY
- READ_WRITE (no puede realizar acciones críticas del sistema como actualizar, restaurar, etc.)
- ADMIN

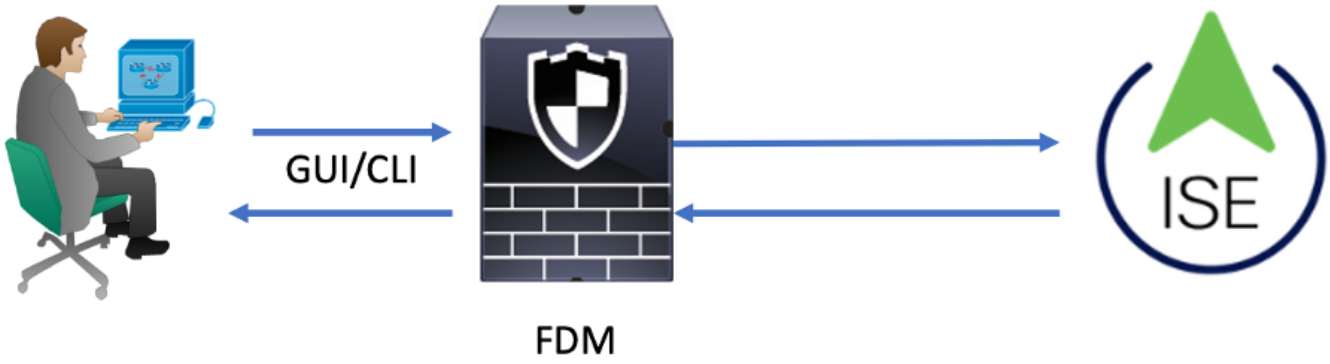
Existe la posibilidad de probar la configuración del servidor RADIUS y supervisar las sesiones de usuario activas y eliminar una sesión de usuario.

La función se implementó en FDM versión 6.3.0. Antes de la versión 6.3.0, FDM solo era compatible con un usuario (admin).

De forma predeterminada, Cisco Firepower Device Manager autentica y autoriza a los usuarios de forma local. Para disponer de un método de autenticación y autorización centralizado, puede utilizar Cisco Identity Service Engine a través del protocolo RADIUS.

Diagrama de la red

La siguiente imagen proporciona un ejemplo de una topología de red



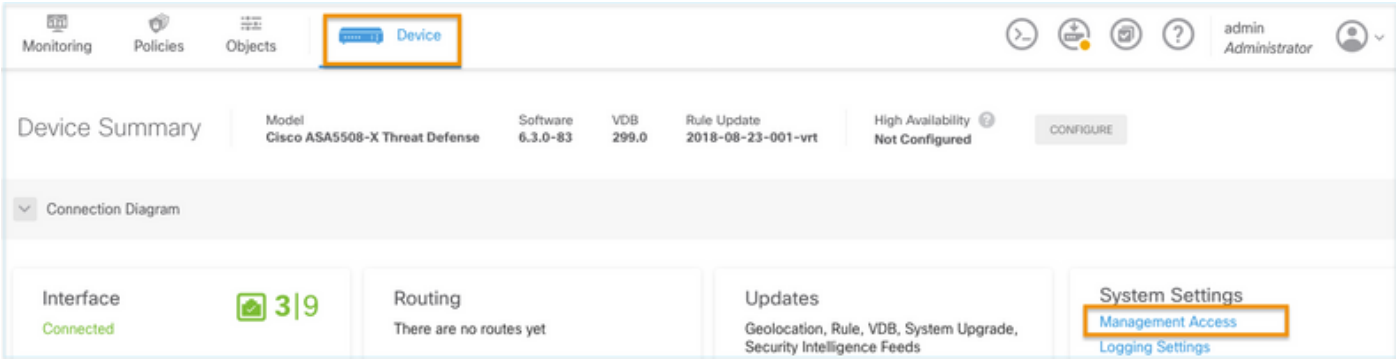
Proceso:

1. El usuario administrador introduce sus credenciales.
2. Se activa el proceso de autenticación e ISE valida las credenciales localmente o a través de Active Directory.
3. Una vez que la autenticación se realiza correctamente, ISE envía un paquete de permiso para la información de autenticación y autorización a FDM.
4. La cuenta funciona en ISE y se lleva a cabo un registro activo de autenticación correcto.

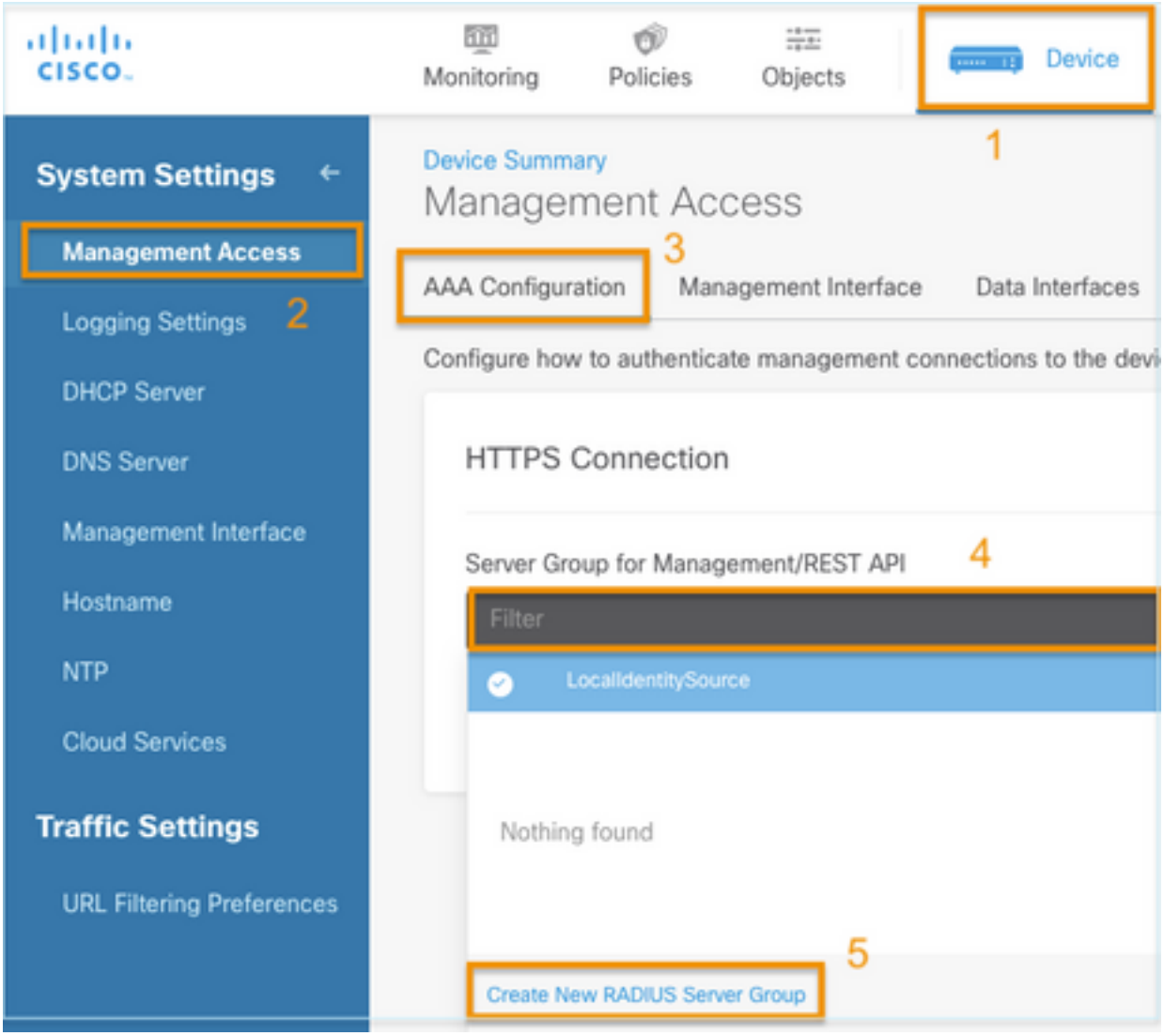
Configurar

Configuración del FDM

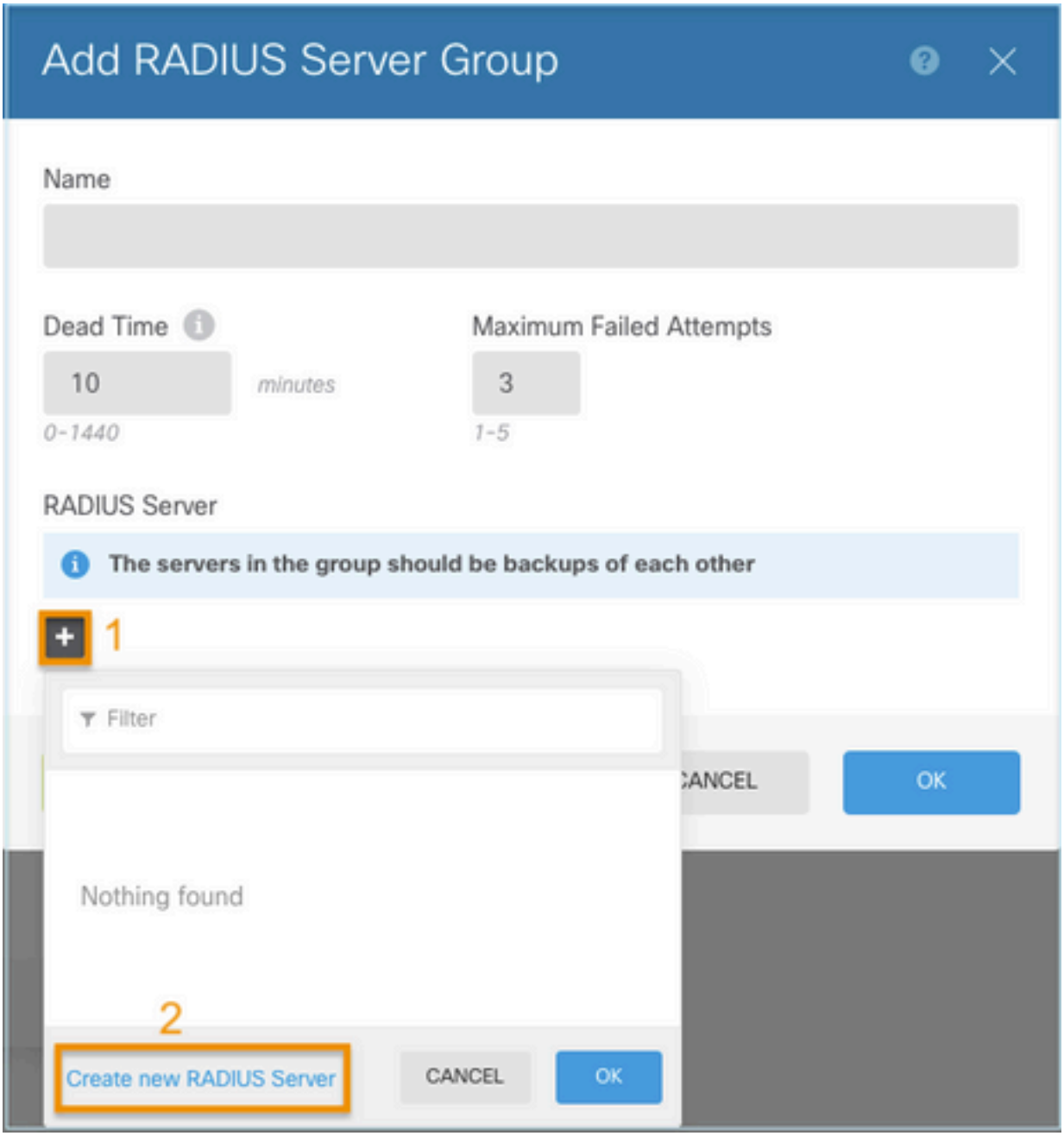
Paso 1. Inicie sesión en FDM y acceda a Device > System Settings > Management Access (Dispositivo > Configuración del sistema > Acceso a la gestión)

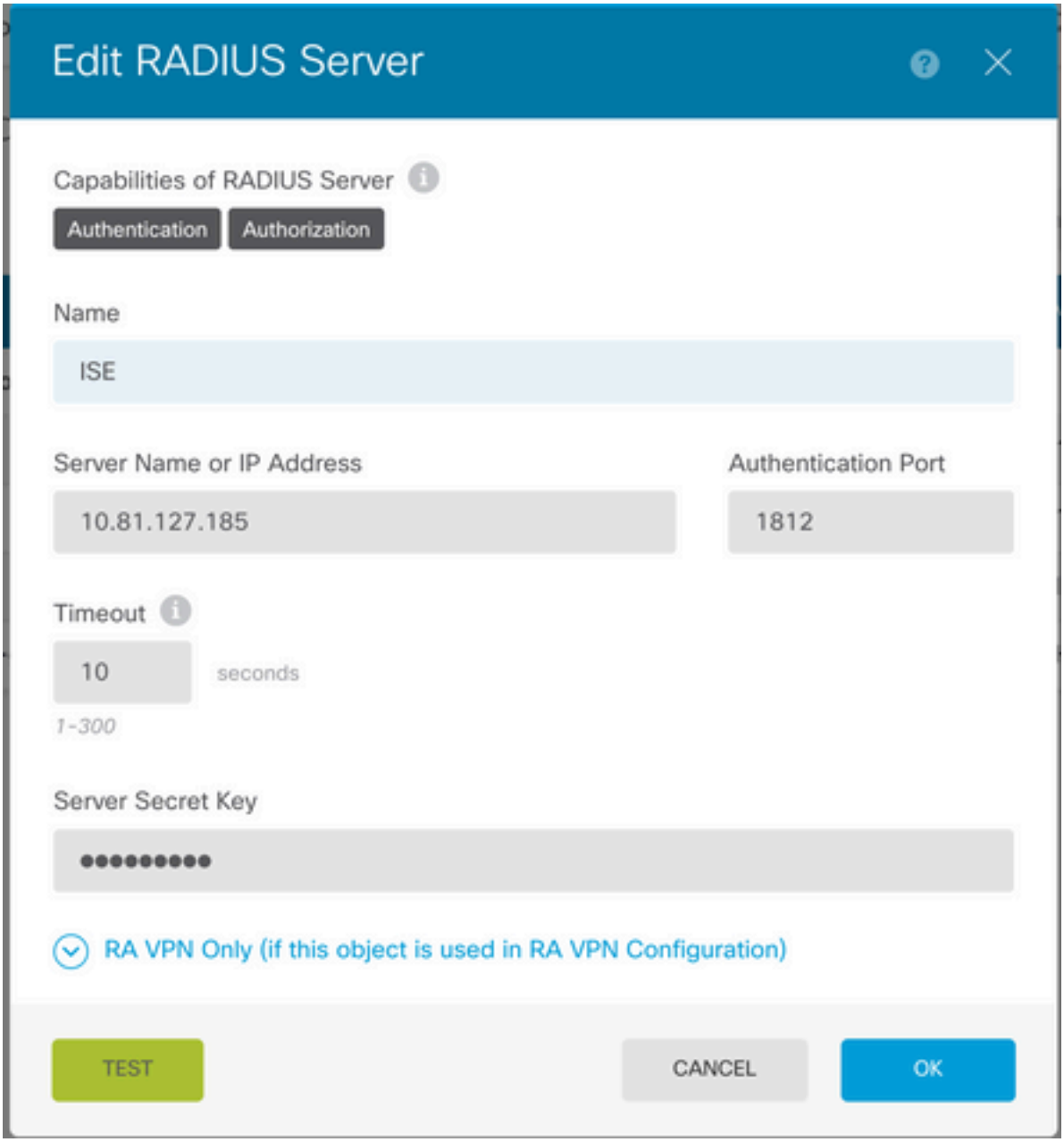


Paso 2. Crear nuevo grupo de servidores RADIUS

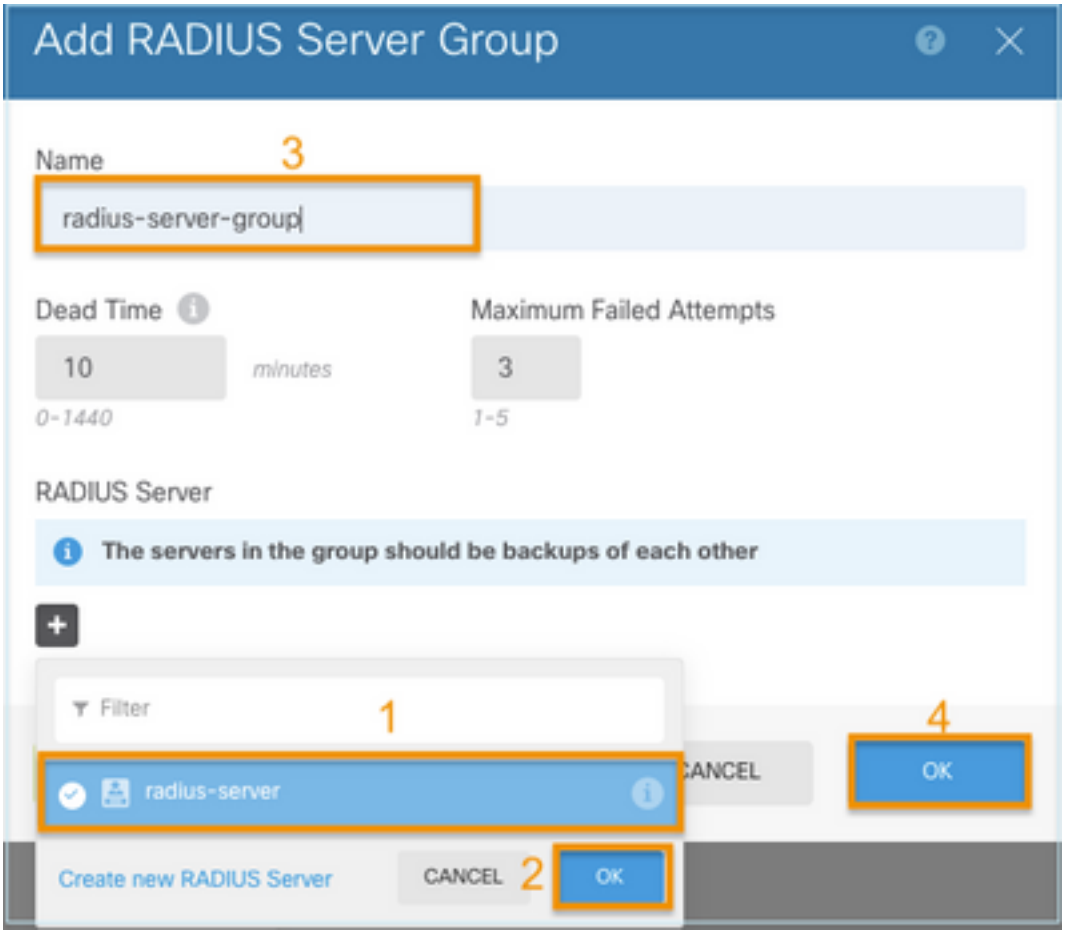


Paso 3. Crear nuevo servidor RADIUS

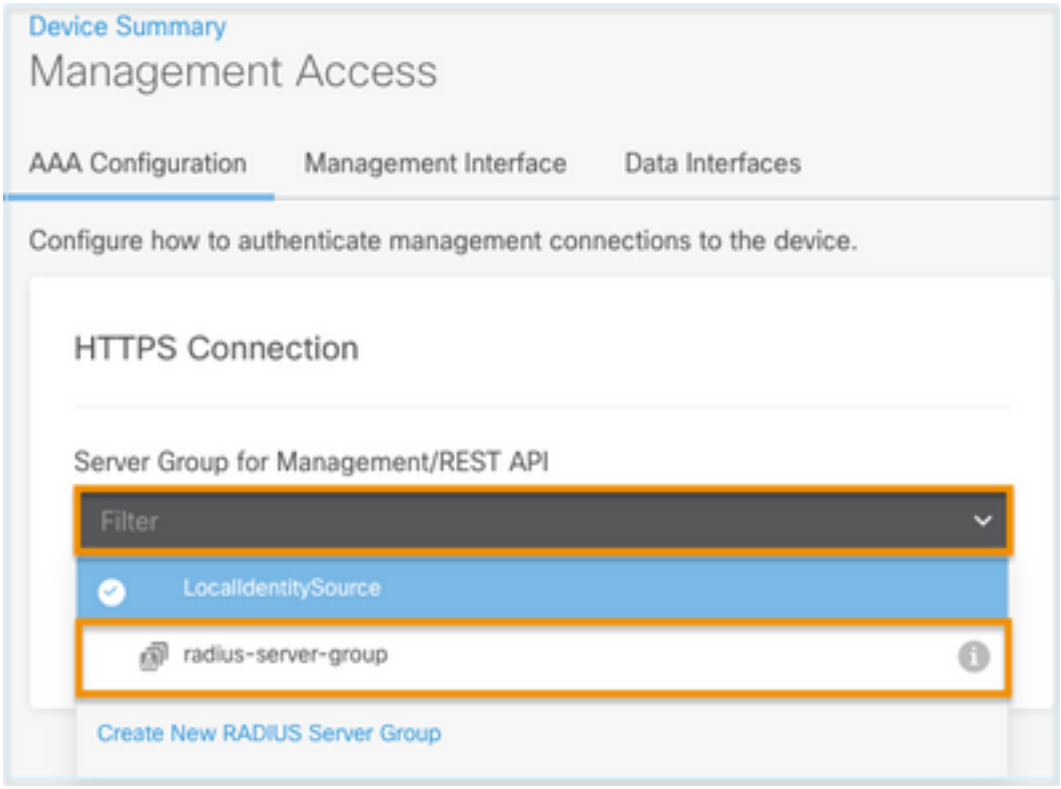

Add RADIUS Server Group
Name
Dead Time
10
minutes
0-1440
Maximum Failed Attempts
3
1-5
RADIUS Server
The servers in the group should be backups of each other
1
Filter
CANCEL
OK
Nothing found
2
Create new RADIUS Server
CANCEL
OK

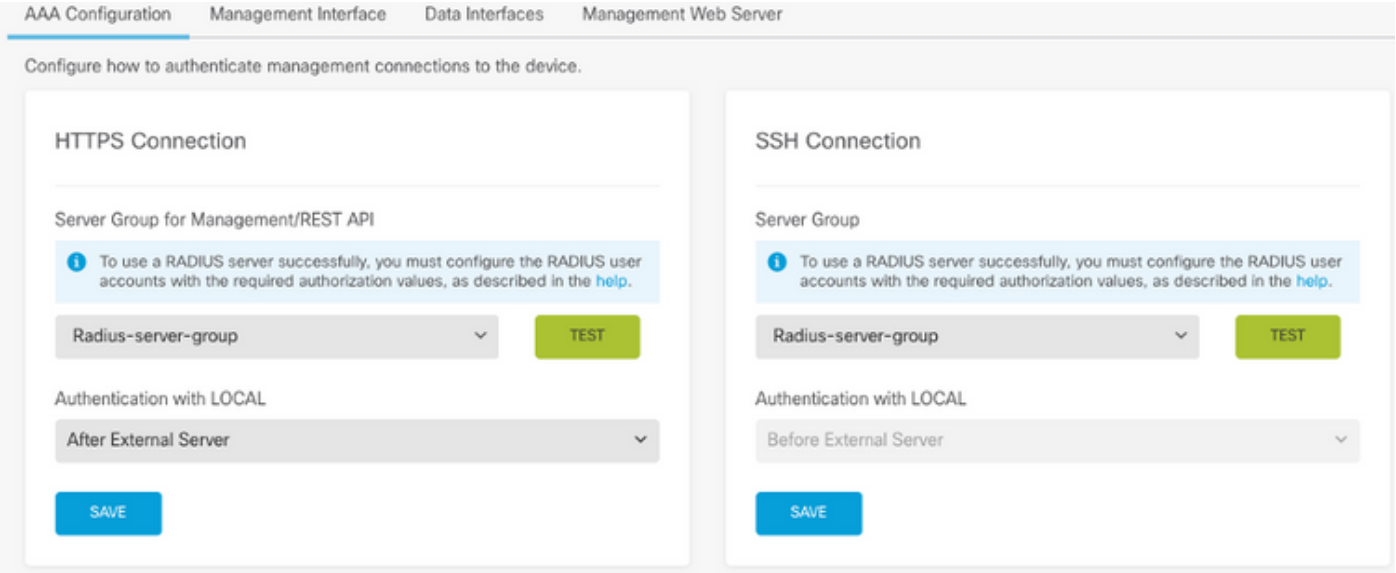


Paso 4. Agregar un servidor RADIUS al grupo de servidores RADIUS

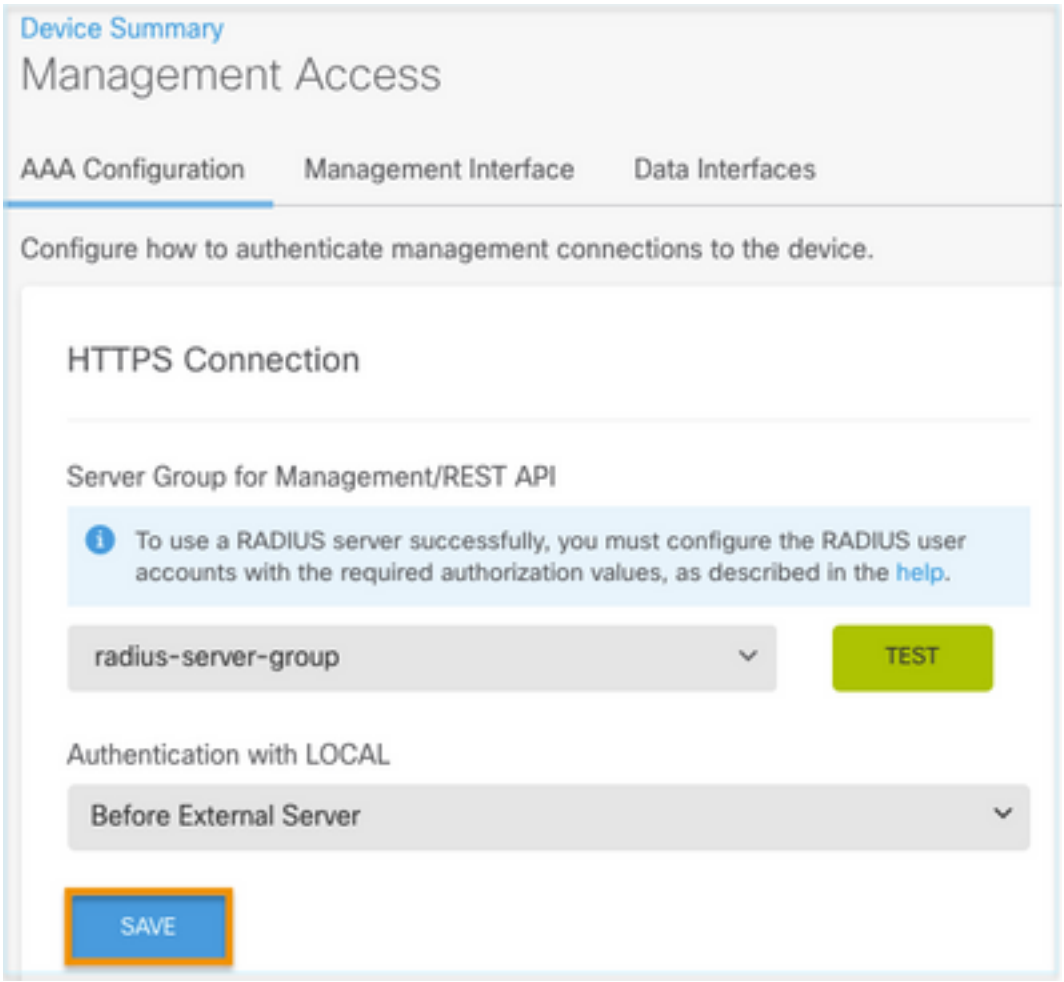


Paso 5. Seleccionar grupo creado como grupo de servidores para administración



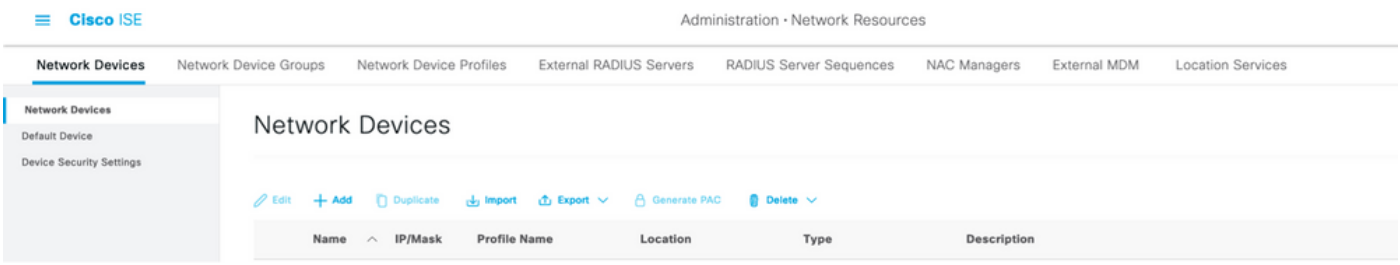


Paso 6. Guarde la configuración

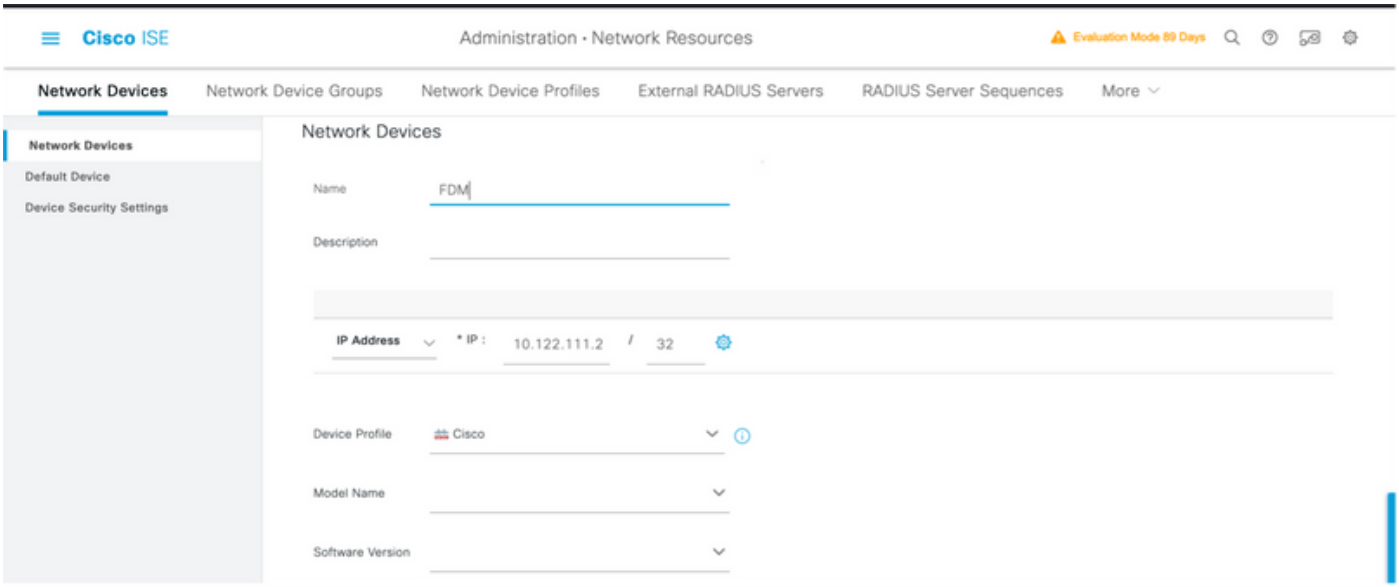


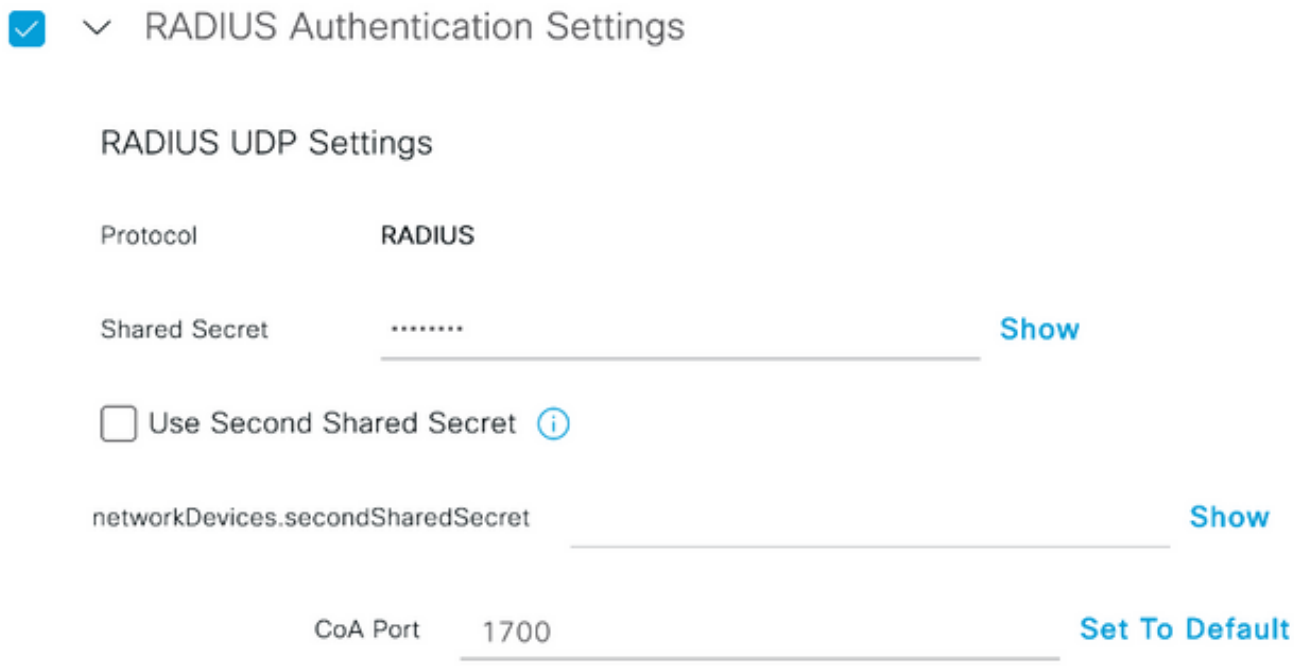
Configuración de ISE

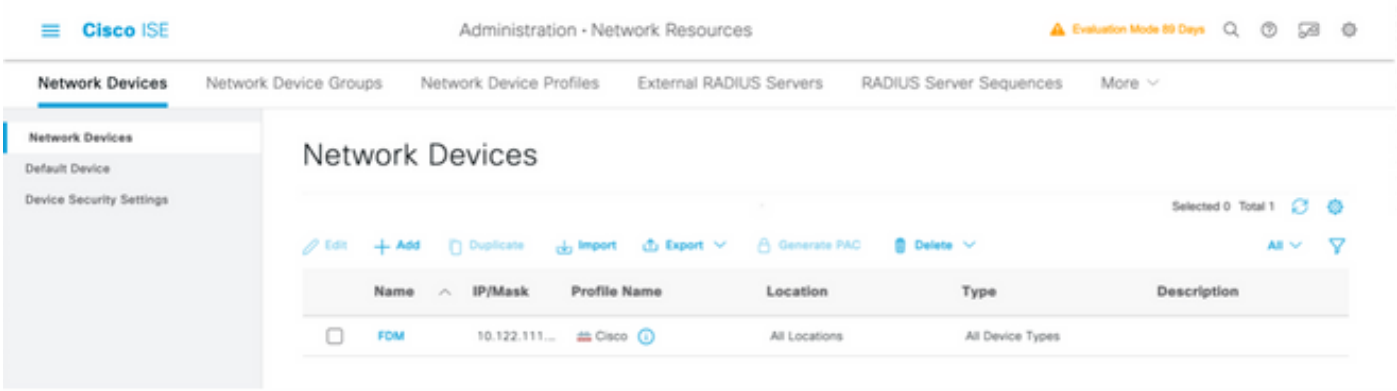
Paso 1. Icono de Navegar a tres líneas situado en la esquina superior izquierda y seleccione en **Administration > Network Resources > Network Devices**



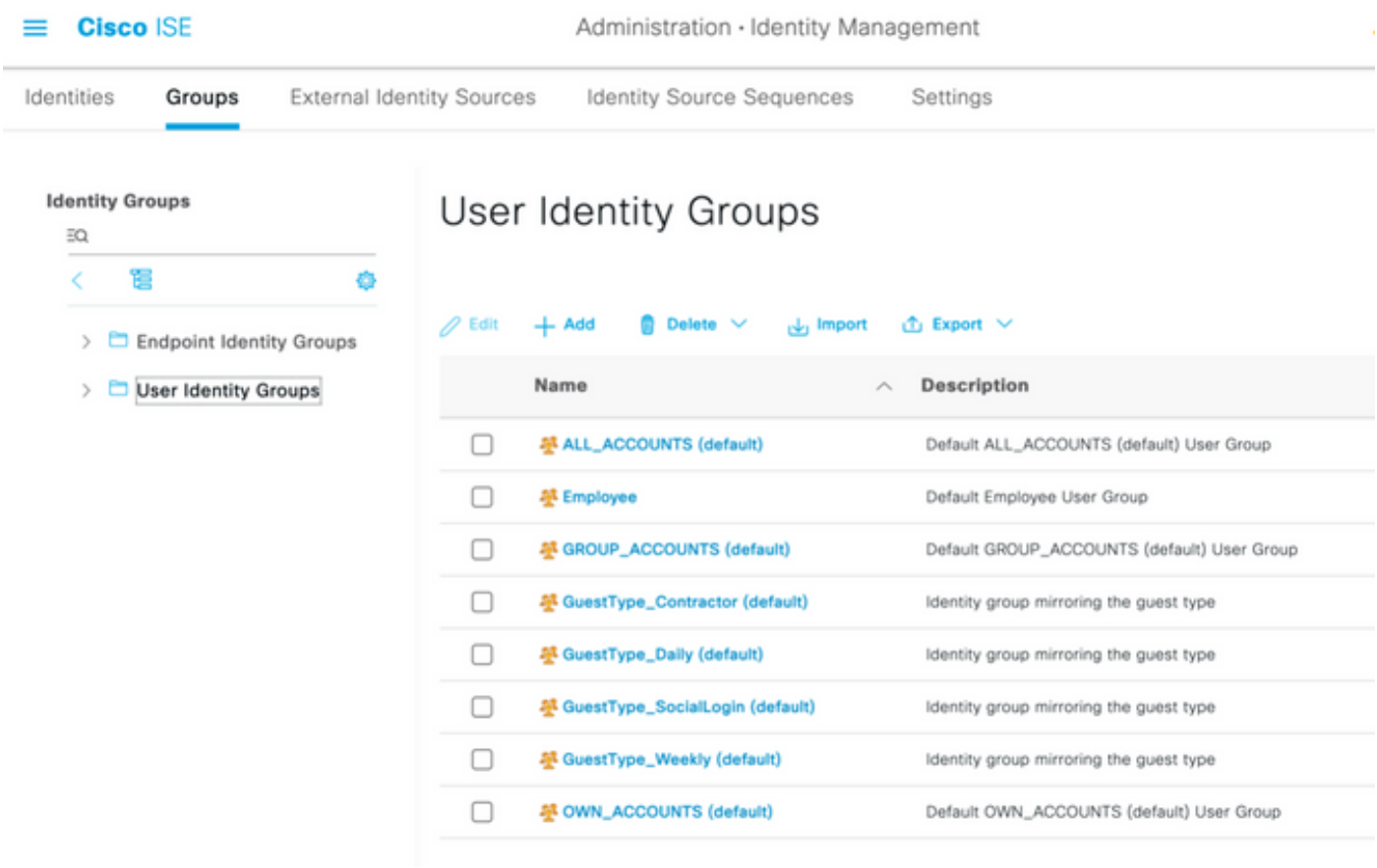
Paso 2. Seleccione el botón +Add y defina Network Access Device Name e IPAddress, luego marque la casilla de verificación RADIUS y defina un secreto compartido. Seleccionar al **enviar**



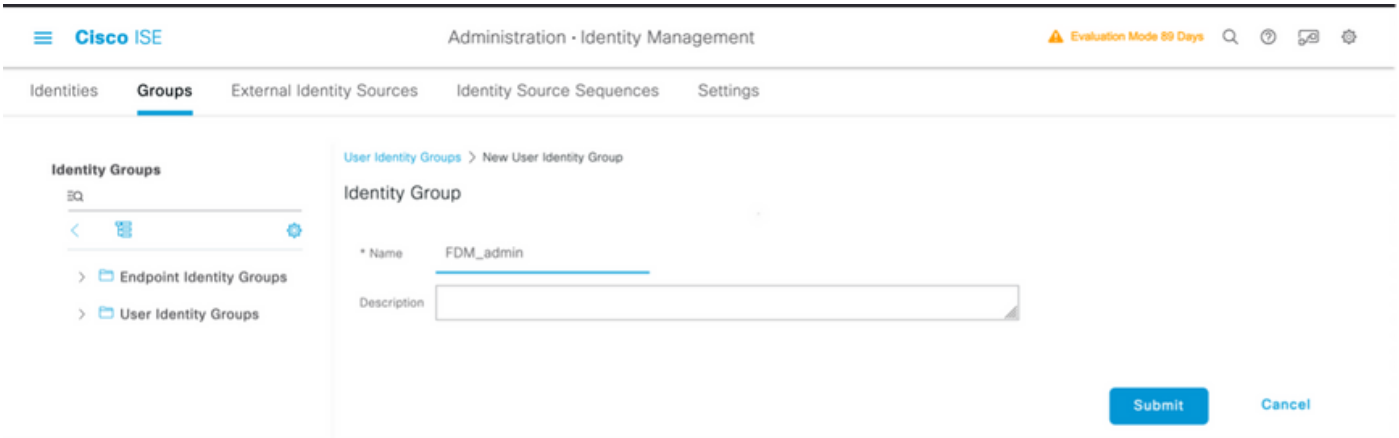


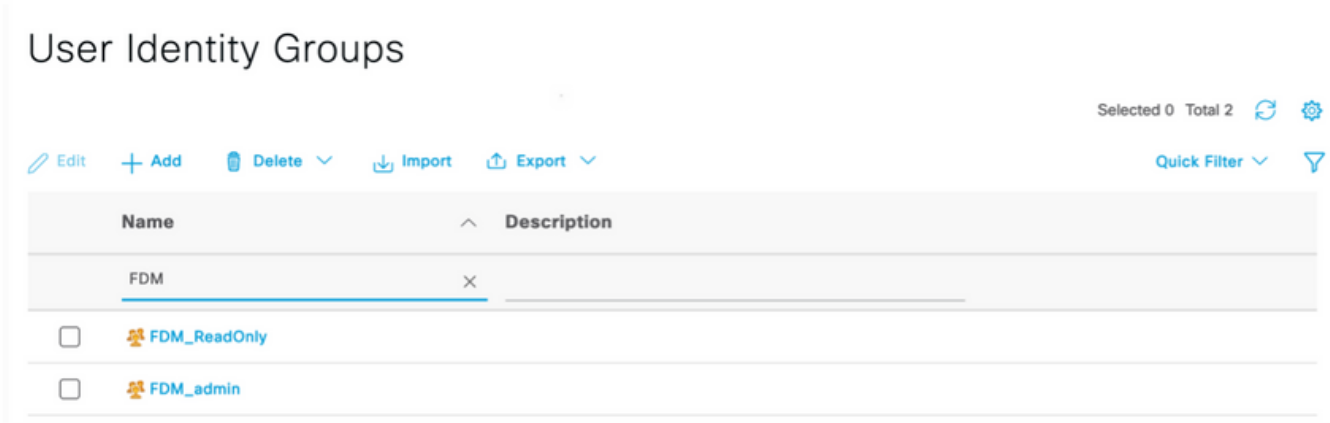


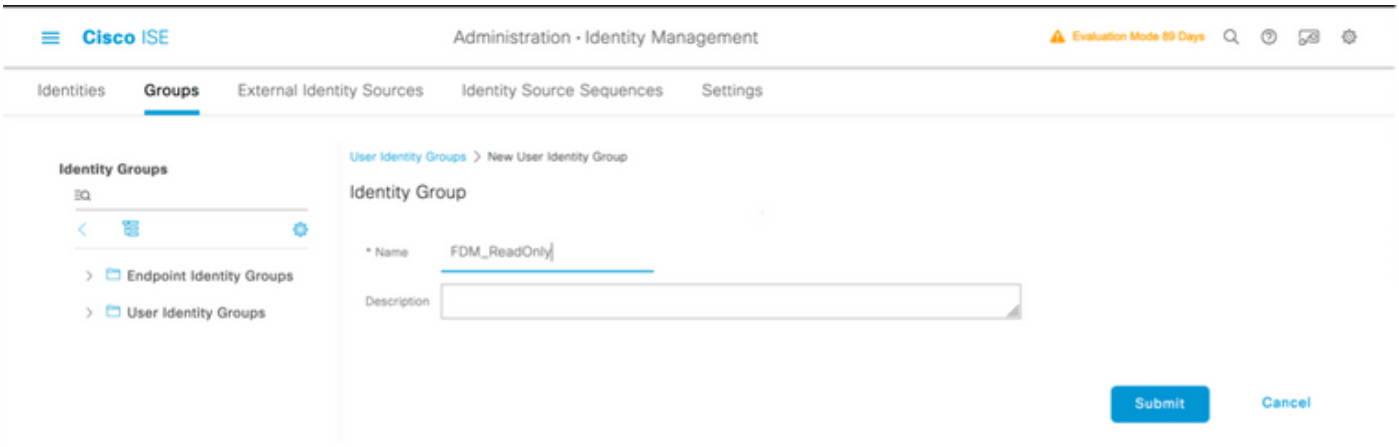
Paso 3. Icono de Navegar a tres líneas situado en la esquina superior izquierda y seleccione en **Administración > Gestión de identidades > Grupos**



Paso 4. Seleccione en Grupos de identidades de usuario y seleccione el botón **+Agregar**. Defina un nombre y seleccione en **Enviar**

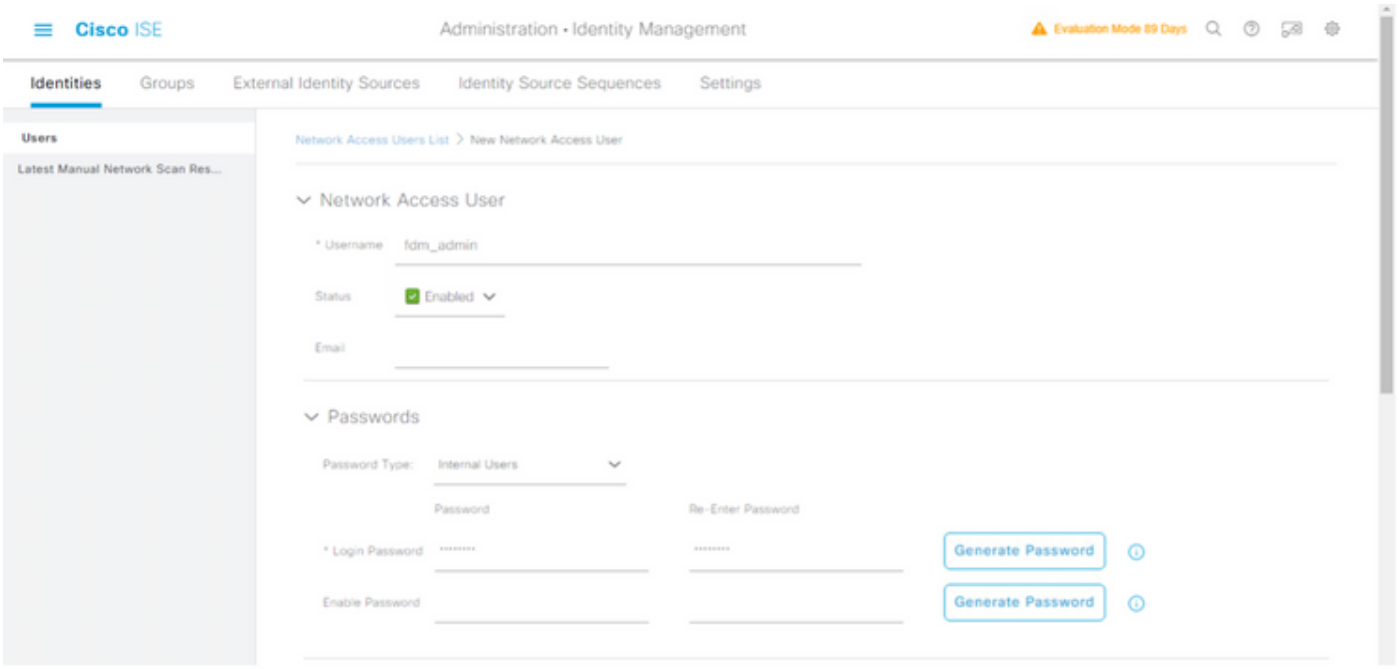


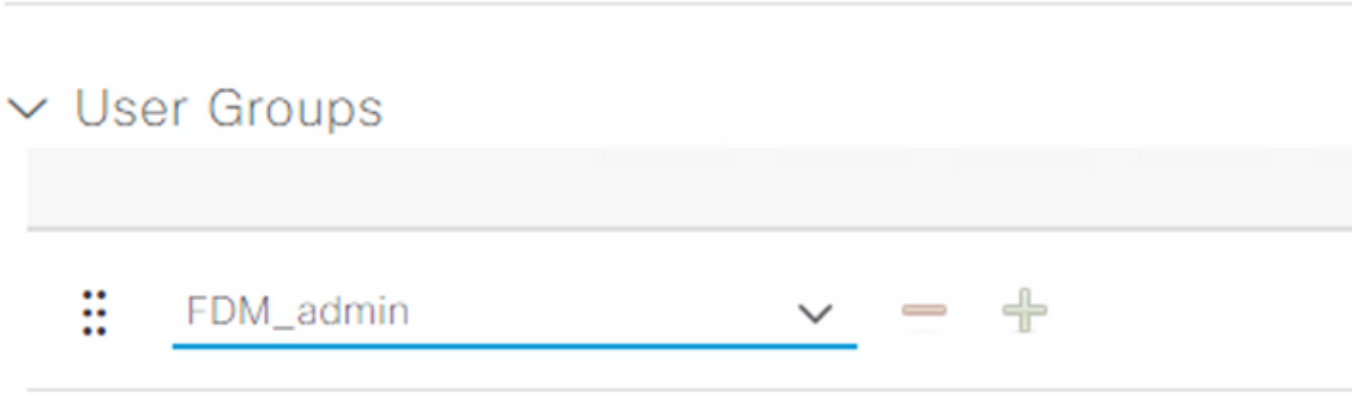


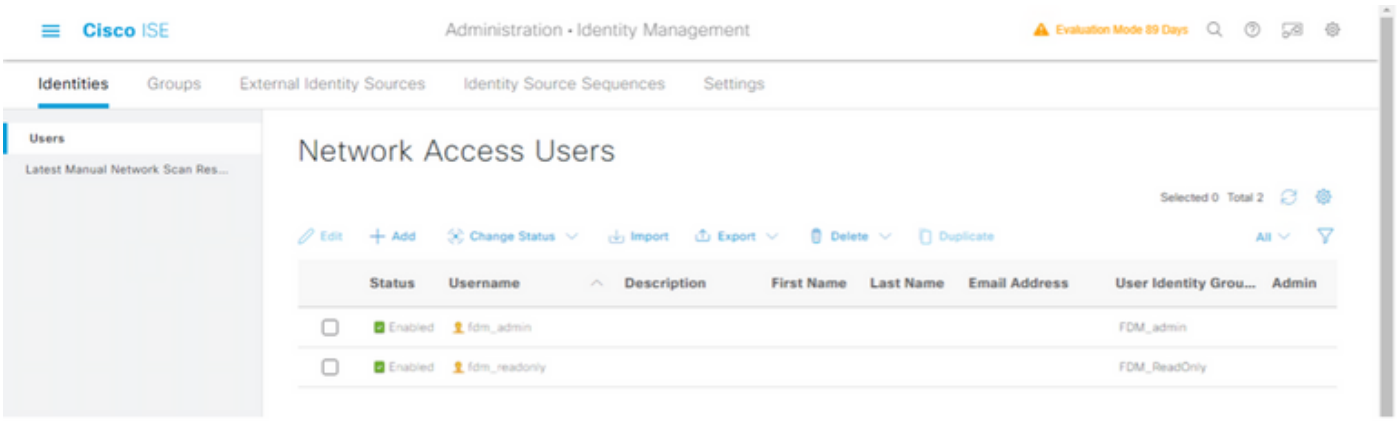


Nota: en este ejemplo, los grupos de identidad FDM_Admin y FDM_ReadOnly creados, puede repetir el paso 4 para cada tipo de usuarios administrativos utilizados en FDM.

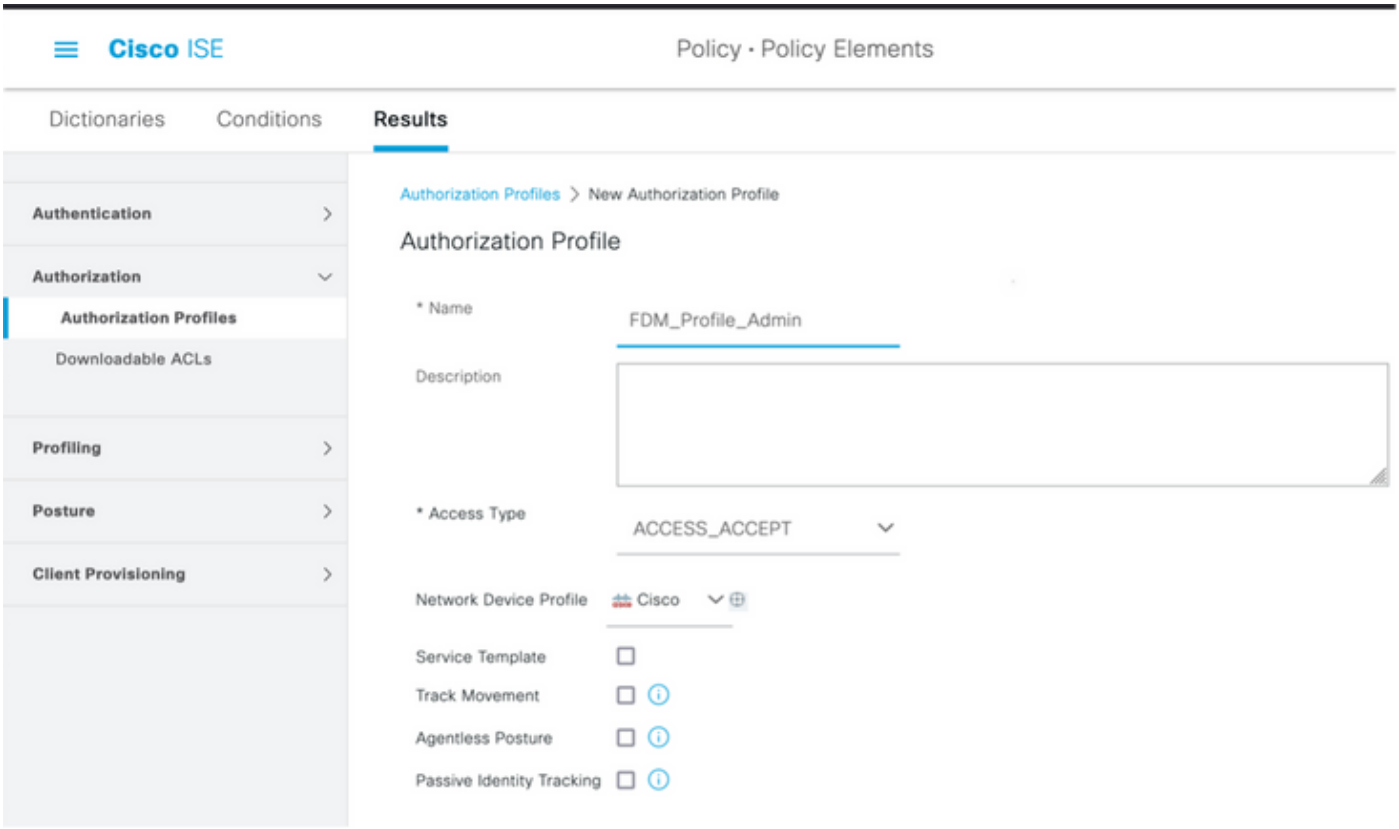
Paso 5. Navegue hasta el icono de tres líneas ubicado en la esquina superior izquierda y seleccione Administration > Identity Management > Identities. Seleccione on **+Add** y defina el nombre de usuario y la contraseña y, a continuación, seleccione el grupo al que pertenece el usuario. En este ejemplo, los usuarios fdm_admin y fdm_readonly se crearon y asignaron al grupo FDM_Admin y FDM_ReadOnly respectivamente.

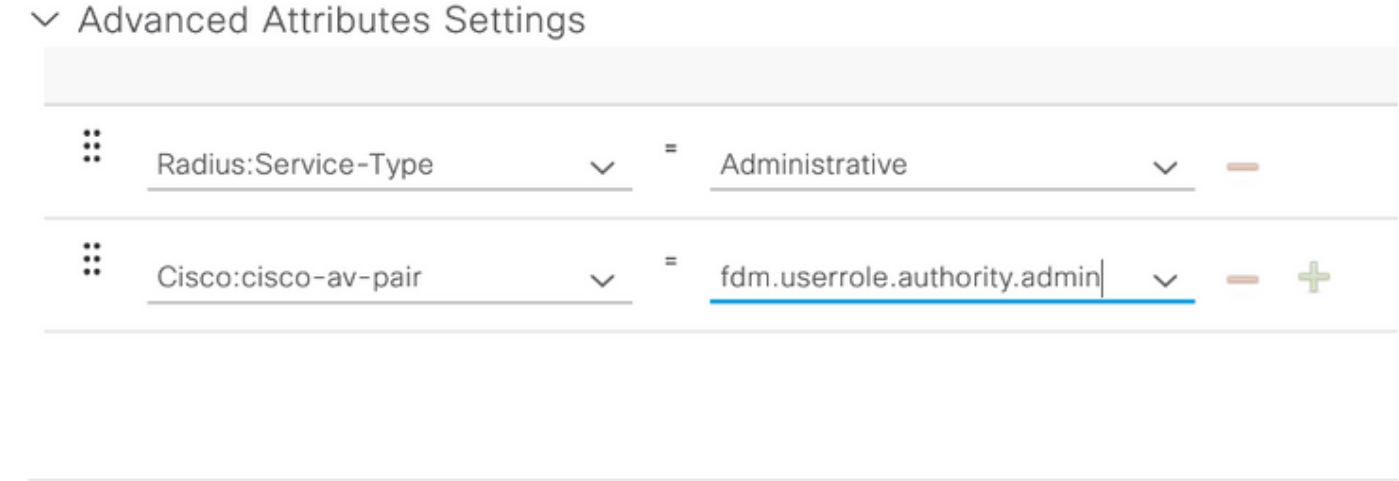


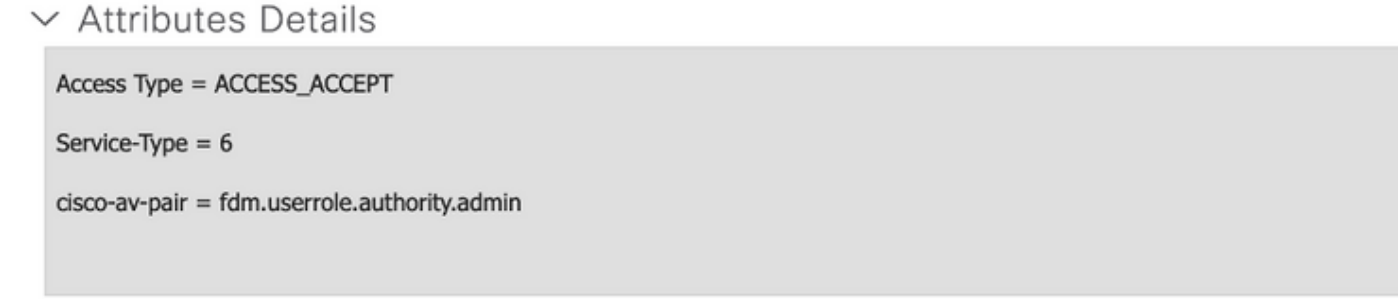


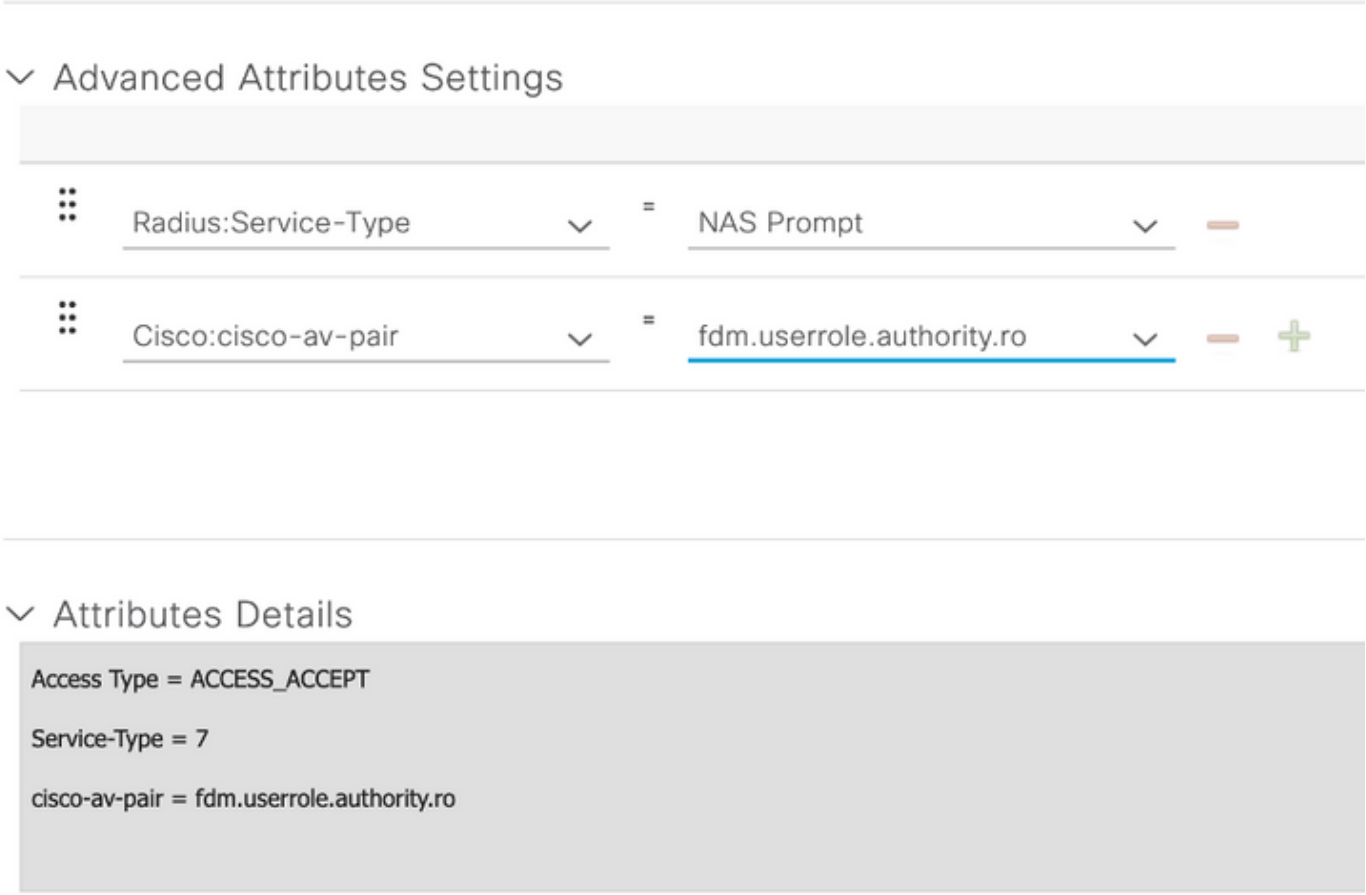


Paso 6. Seleccione el icono de tres líneas ubicado en la esquina superior izquierda y navegue hasta **Política > Elementos de política > Resultados > Autorización > Perfiles de autorización,** seleccione **+Agregar** y defina un nombre para el **Perfil de autorización**. Seleccione **Radius Service-type** y seleccione **Administrative**, luego seleccione **Cisco-av-pair** y pegue el rol que obtiene el usuario administrador, en este caso, el usuario recibe un privilegio de administración completo (fdm.userrole.authority.admin). Seleccione en **Enviar**. Repita este paso para cada rol, usuario de sólo lectura configurado como otro ejemplo en este documento.


Cisco ISE
Policy · Policy Elements
Dictionaries
Conditions
Results
Authentication
Authorization
Authorization Profiles
Downloadable ACLs
Profiling
Posture
Client Provisioning
Authorization Profiles > New Authorization Profile
Authorization Profile
* Name
FDM_Profile_Admin
Description
* Access Type
ACCESS_ACCEPT
Network Device Profile
Cisco
Service Template
Track Movement
Agentless Posture
Passive Identity Tracking


Advanced Attributes Settings
Radius:Service-Type
=
Administrative
Cisco:cisco-av-pair
=
fdm.userrole.authority.admin


Attributes Details
Access Type = ACCESS_ACCEPT
Service-Type = 6
cisco-av-pair = fdm.userrole.authority.admin

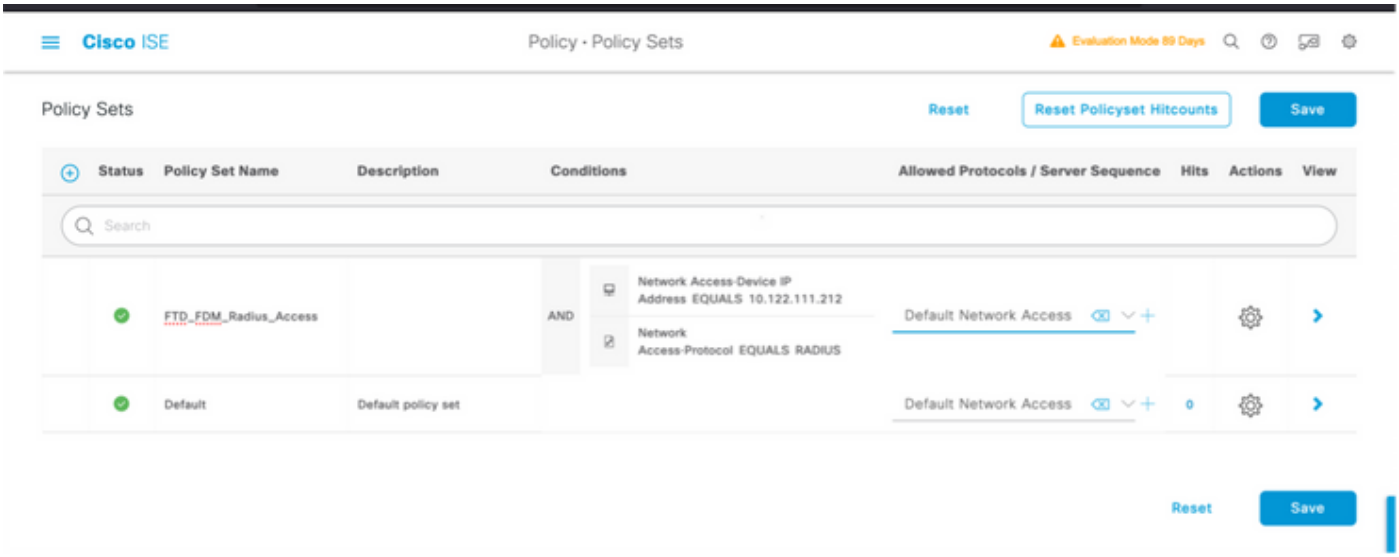


Nota: Asegúrese de que el orden de la sección de atributos avanzados sea el mismo que con el ejemplo de imágenes para evitar resultados inesperados al iniciar sesión con GUI y CLI.

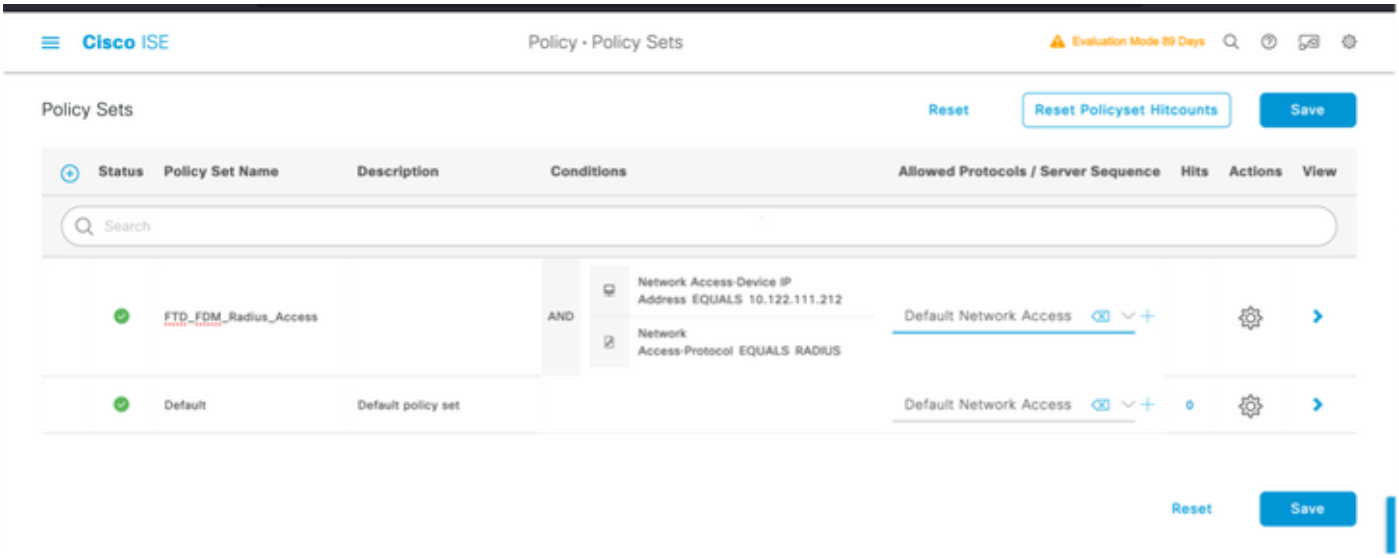
Paso 8. Seleccione el icono de tres líneas y desplácese hasta Directiva > Juegos de políticas.

Seleccionar en  **situado debajo del título de los conjuntos de políticas, defina un nombre y seleccione el botón + situado en el centro para agregar una nueva condición.**

Paso 9. En la ventana Condición, seleccione agregar un atributo y, a continuación, seleccione en el icono Dispositivo de red seguido de Dirección IP del dispositivo de acceso a la red. Seleccione **Attribute Value** y agregue la dirección IP de FDM. Agregue una nueva condición y seleccione en **Network Access** seguido de Protocol option, seleccione en **RADIUS** y seleccione en Use once done.



Paso 10. En la sección Permitir protocolos, seleccione **Device Default Admin**. Seleccionar al **guardar**



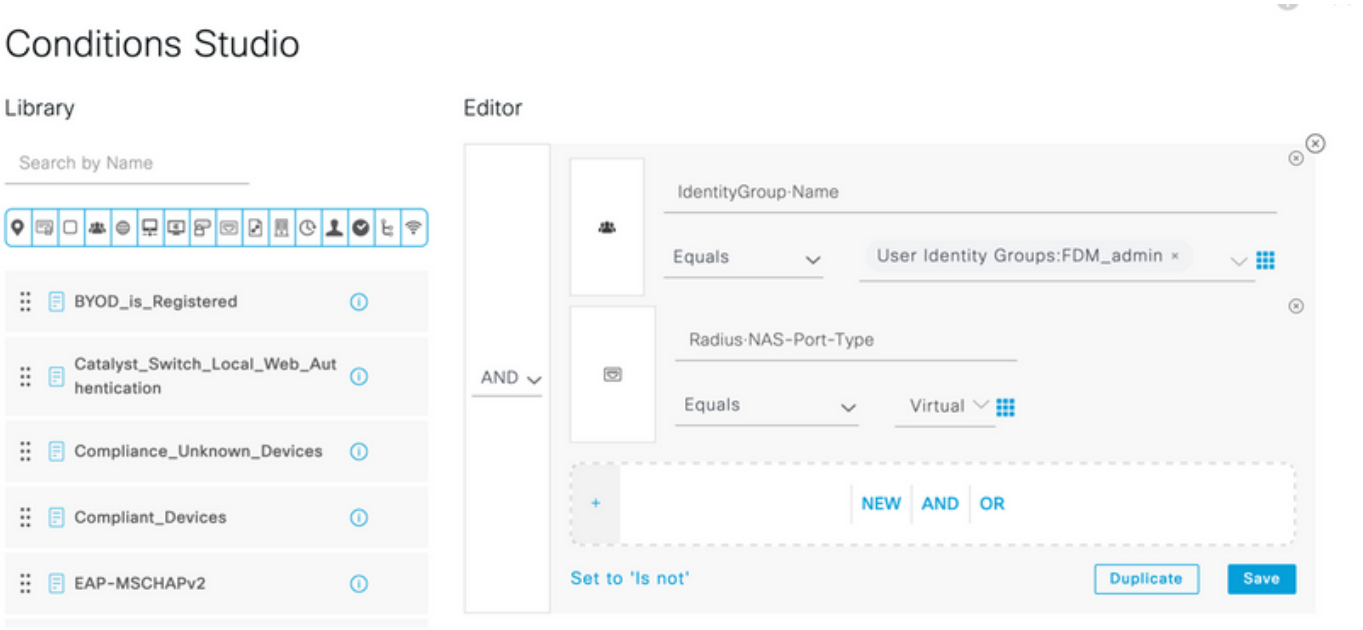
Paso 11. Seleccionar en la flecha derecha > del conjunto de directivas para definir directivas de autenticación y autorización

Paso 12. Seleccionar en ⊕ situado debajo del título de la directiva de autenticación, defina un nombre y seleccione en el signo + situado en el centro para agregar una nueva condición. En la ventana Condición, seleccione agregar un atributo y, a continuación, seleccione en el icono Dispositivo de red seguido de Dirección IP del dispositivo de acceso a la red. Seleccione en Valor de atributo y agregue la dirección IP de FDM. Seleccione en Usar una vez hecho

Paso 13. Seleccione Usuarios internos como almacén de identidades y seleccione en Guardar

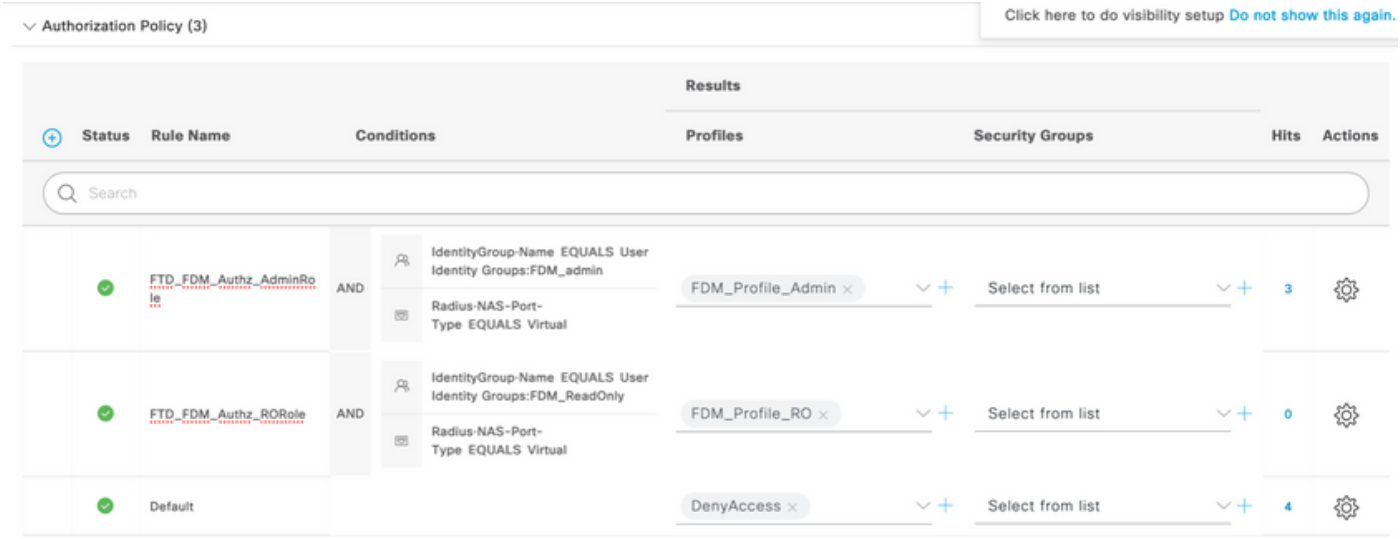
Nota: el almacén de identidades se puede cambiar a almacén de AD si ISE se une a Active Directory.

Paso 14. Seleccionar en  **situado debajo del título de la directiva de autorización, defina un nombre y seleccione en el signo + situado en el centro para agregar una nueva condición. En la ventana Condición, seleccione agregar un atributo y, a continuación, seleccione el icono Grupo de identidades seguido de Usuario interno:Grupo de identidades. Seleccione el grupo FDM_Admin, seleccione la opción AND junto con NEW para agregar una nueva condición, seleccione on port icon seguido de RADIUS NAS-Port-Type:Virtual y seleccione on Use.**



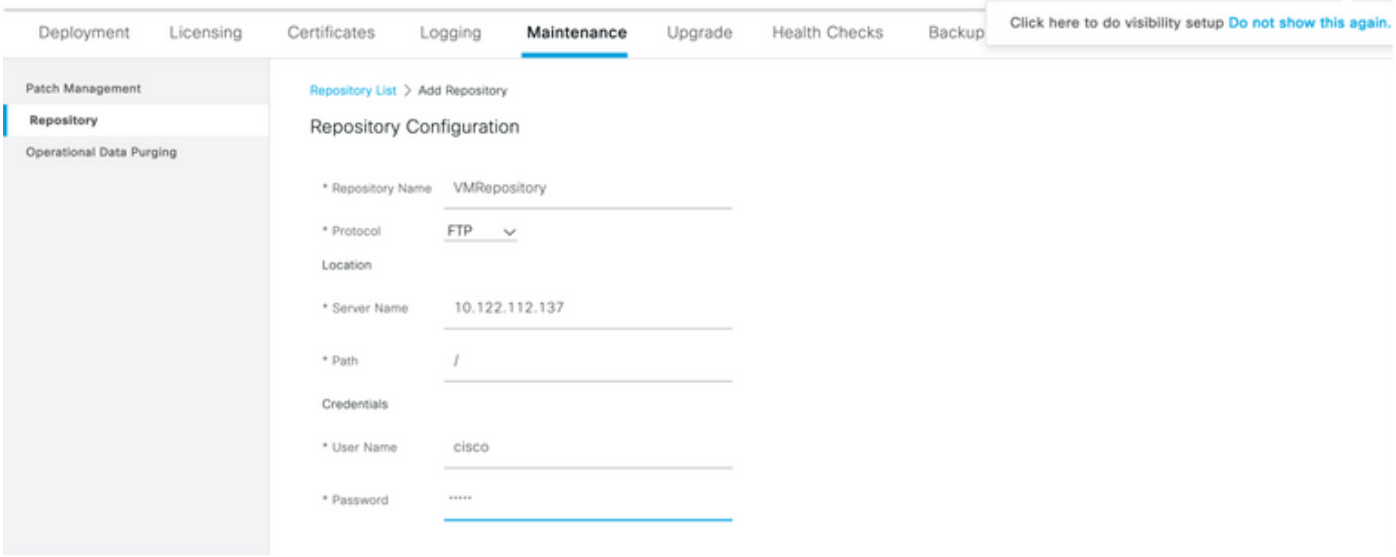
Paso 15. En Profiles (Perfiles), seleccione el perfil creado en el paso 6 y, a continuación, seleccione en Save (Guardar)

Repita los pasos 14 y 15 para el grupo FDM_ReadOnly



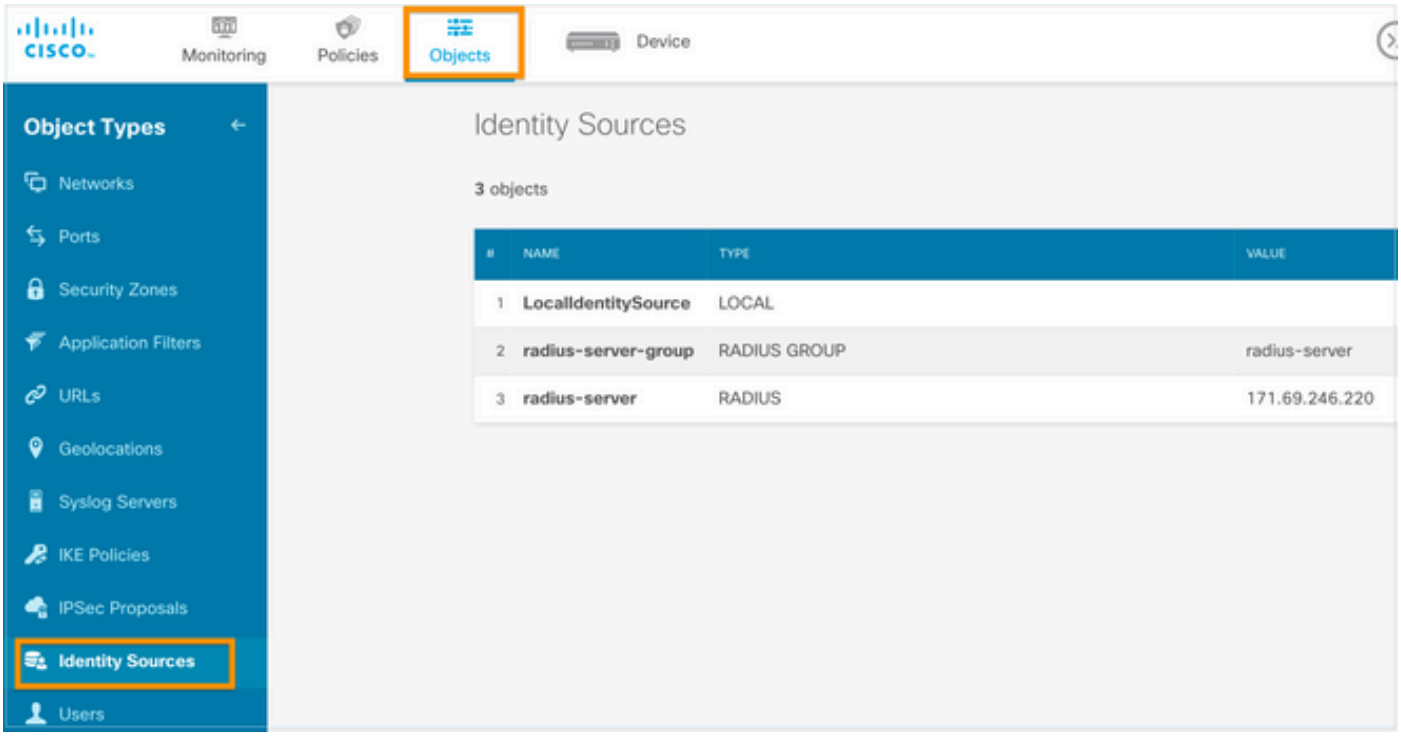
Paso 16 (opcional). Navegue hasta el icono de tres líneas ubicado en la esquina superior izquierda y seleccione en Administration > System > Maintenance > Repository y seleccione on +Add para agregar un repositorio utilizado para almacenar el archivo de volcado TCP para resolver problemas.

Paso 17 (opcional). Defina un nombre de repositorio, protocolo, nombre de servidor, ruta de acceso y credenciales. Seleccione en Enviar cuando haya terminado.

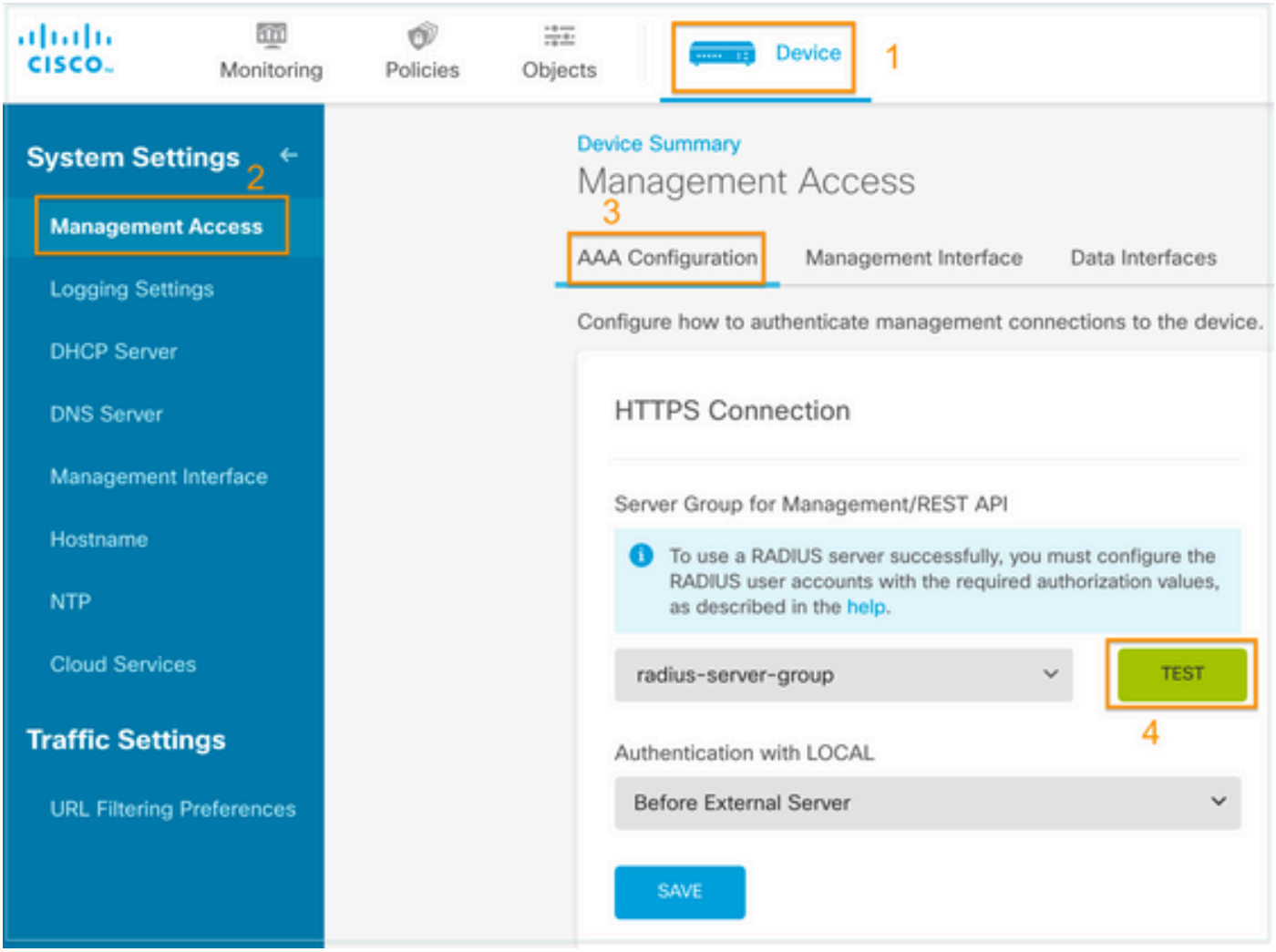


Verificación

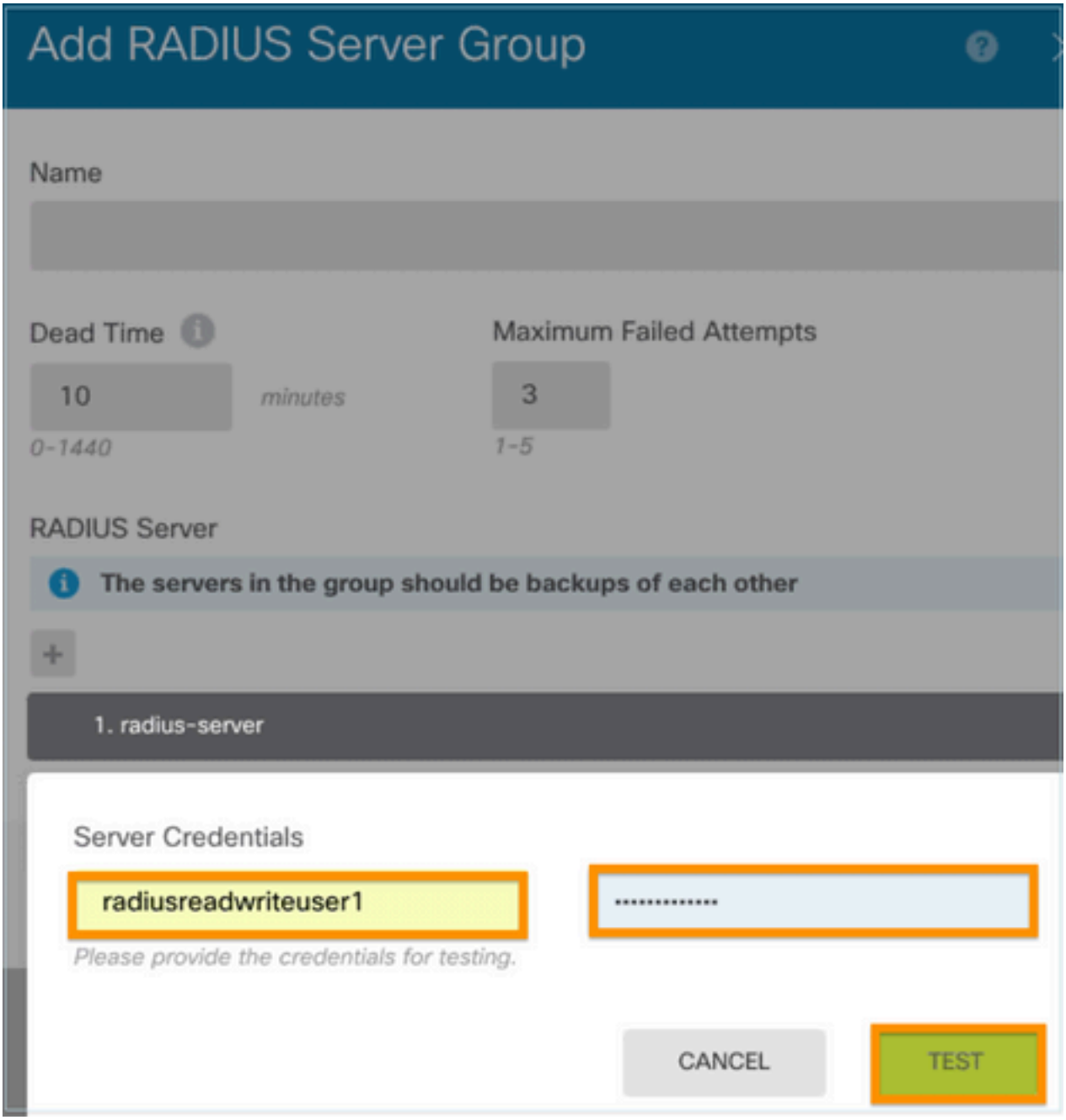
Paso 1.Navegue hasta Objetos > ficha Orígenes de identidad y verifique la configuración del Servidor RADIUS y del Servidor de grupo



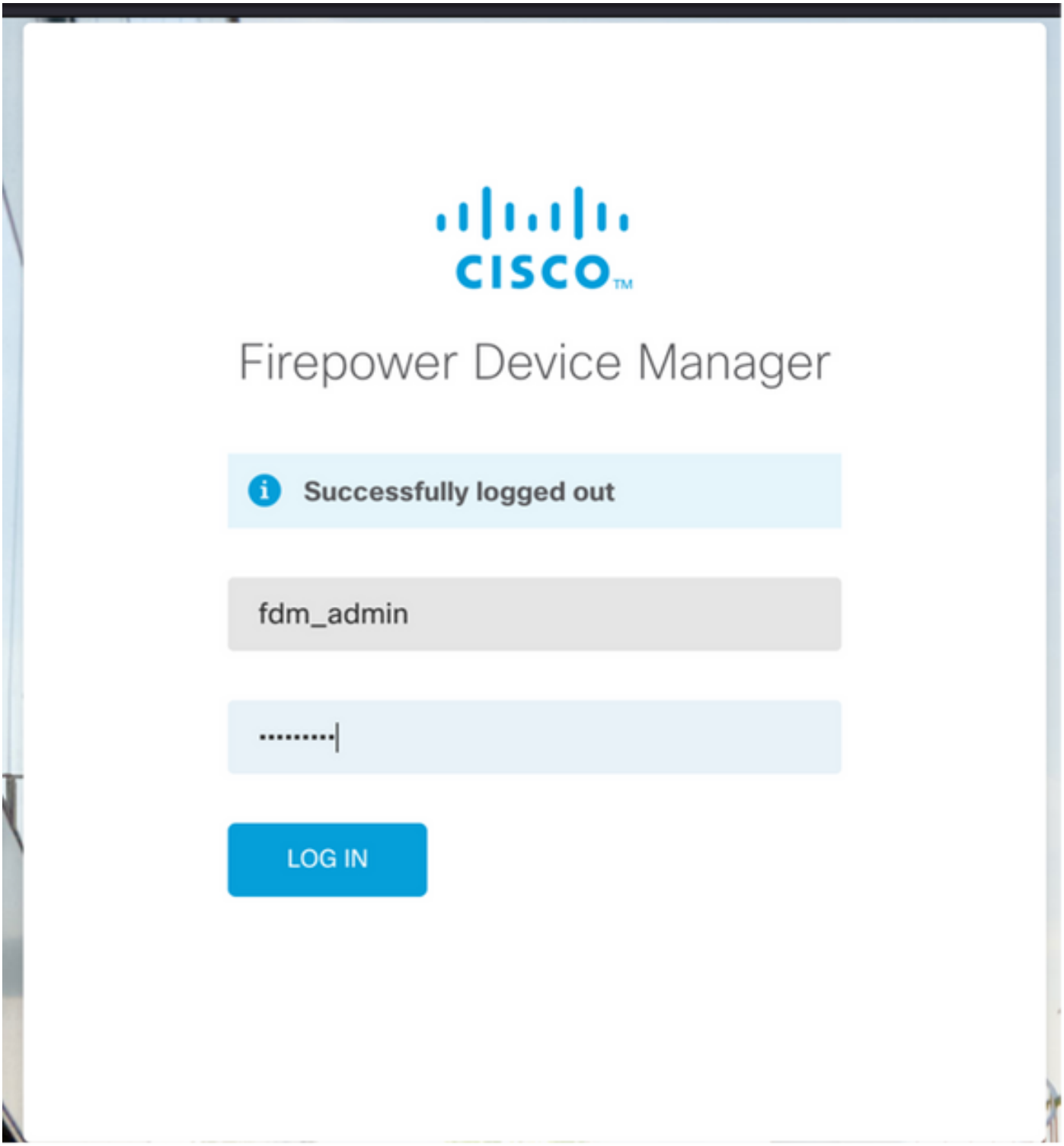
Paso 2. Vaya a Device > System Settings > Management Access tab y seleccione el botón TEST



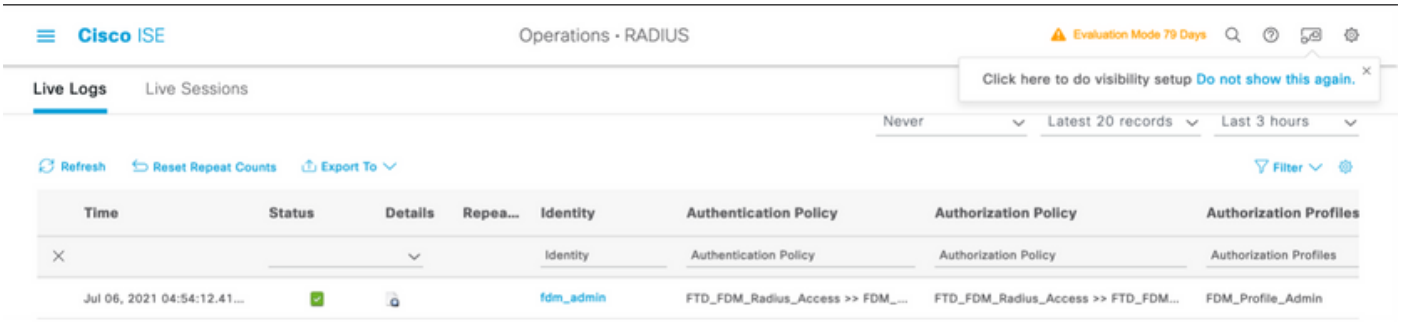
Paso 3.Inserte las credenciales del usuario y seleccione el botón TEST.



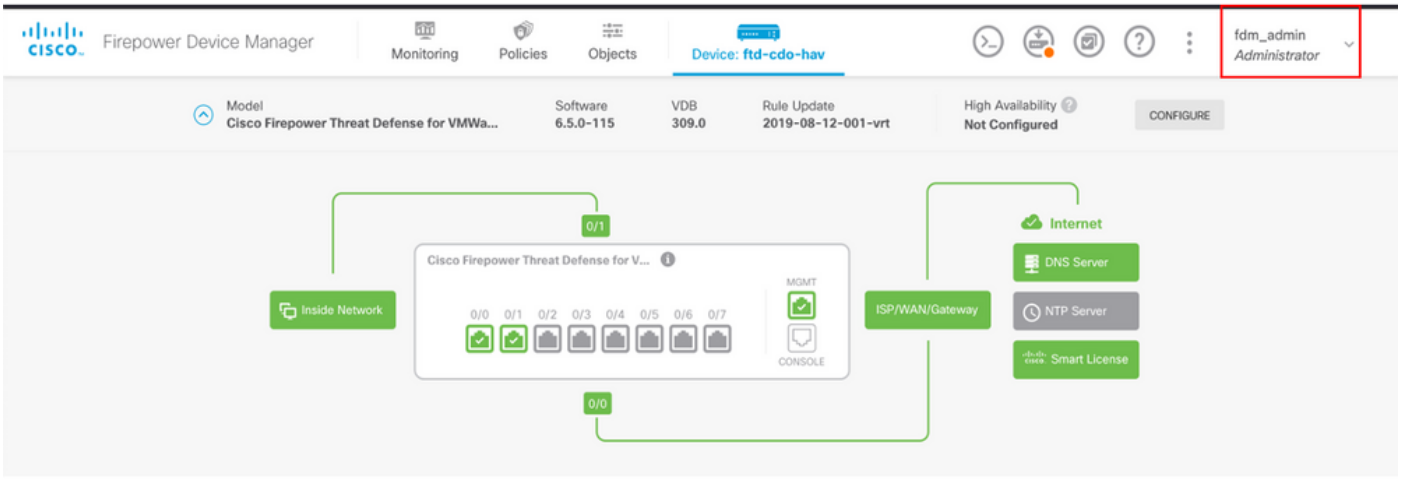
Paso 4. Abra un nuevo explorador de ventanas y escriba https://FDM_ip_Address, utilice el nombre de usuario y la contraseña de fdm_admin creados en el paso 5 de la sección de configuración de ISE.



El intento de inicio de sesión correcto se puede verificar en los registros en directo de RADIUS de ISE



El usuario administrador también se puede revisar en FDM, en la esquina superior derecha



CLI del administrador de dispositivos de Cisco Firepower (usuario administrador)

```
ECANOGUT-M-D4N7:~ ecanogut$ ssh fdm_admin@10.122.111.212
The authenticity of host '10.122.111.212 (10.122.111.212)' can't be established.
ECDSA key fingerprint is SHA256:sqpyFmCcGBslEjjDMdHnrkqdw40qvc7ne1I+Pjw6fJs.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.122.111.212' (ECDSA) to the list of known hosts.
Password:
!!! New external username identified. Please log in again to start a session. !!
!

Copyright 2004-2019, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.5.0 (build 4)
Cisco Firepower Threat Defense for VMWare v6.5.0 (build 115)

Connection to 10.122.111.212 closed.
```

```
ECANOGUT-M-D4N7:~ ecanogut$ ssh fdm_admin@10.122.111.212
Password:
Last login: Tue Jul  6 17:01:20 UTC 2021 from 10.24.242.133 on pts/0

Copyright 2004-2019, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.5.0 (build 4)
Cisco Firepower Threat Defense for VMWare v6.5.0 (build 115)

>
```

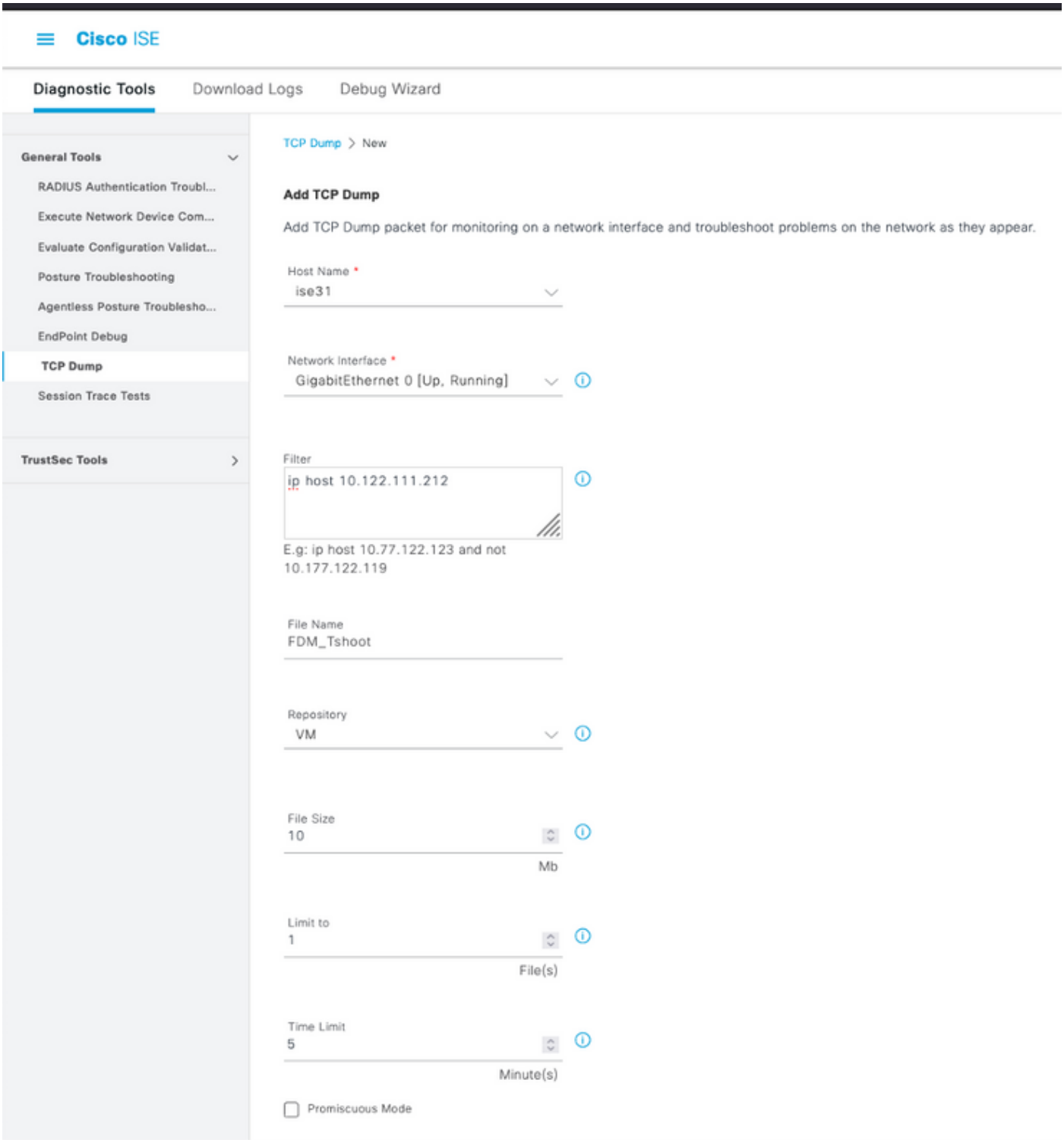
Troubleshoot

Esta sección proporciona la información que puede utilizar para resolver problemas de su configuración.

Validación de la comunicación con la herramienta TCP Dump en ISE

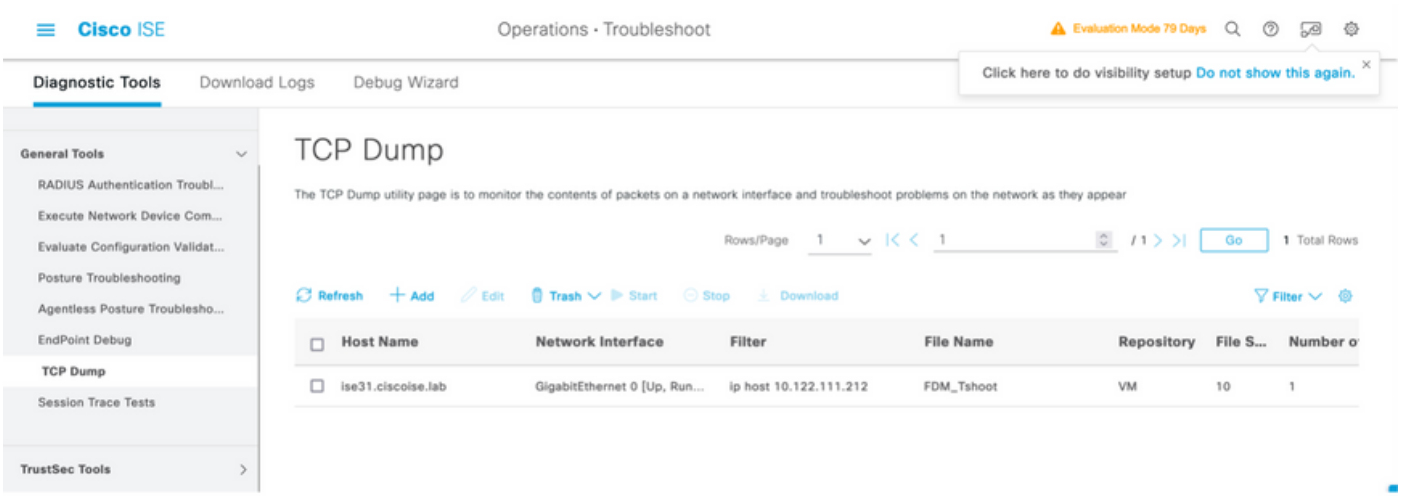
Paso 1. Inicie sesión en ISE, seleccione el icono de tres líneas situado en la esquina superior izquierda y vaya a **Operaciones > Solución de problemas > Herramientas de diagnóstico.**

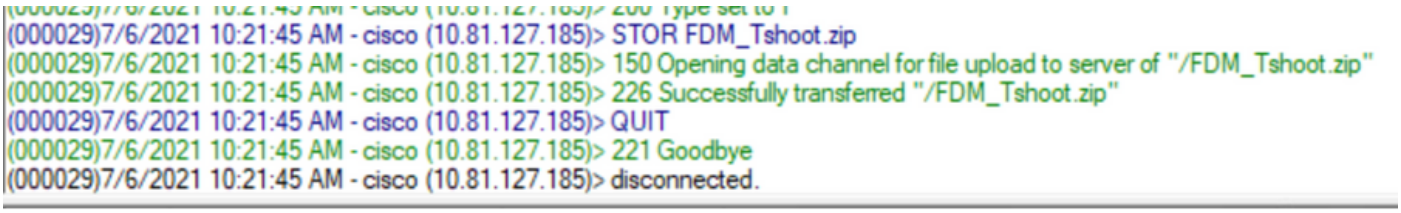
Paso 2. En Herramientas generales, seleccione en Volcados TCP y, a continuación, seleccione en **Agregar+**. Seleccione Nombre de host, Nombre de archivo de interfaz de red, Repositorio y, opcionalmente, un filtro para recopilar sólo el flujo de comunicación de la dirección IP de FDM. Seleccionar al **guardar y ejecutar**

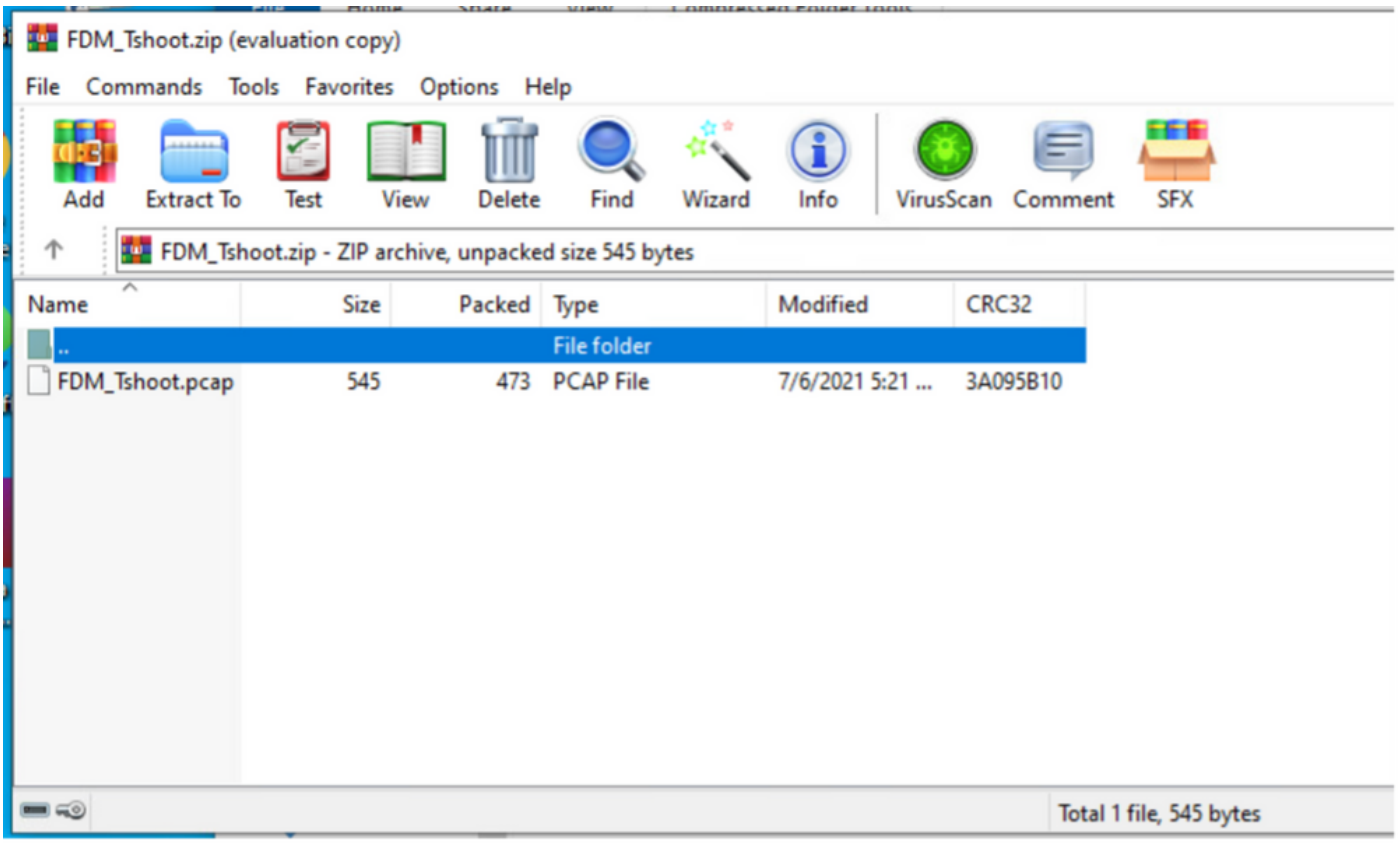


Paso 3. Inicie sesión en la interfaz de usuario de FDM y escriba las credenciales de administrador.

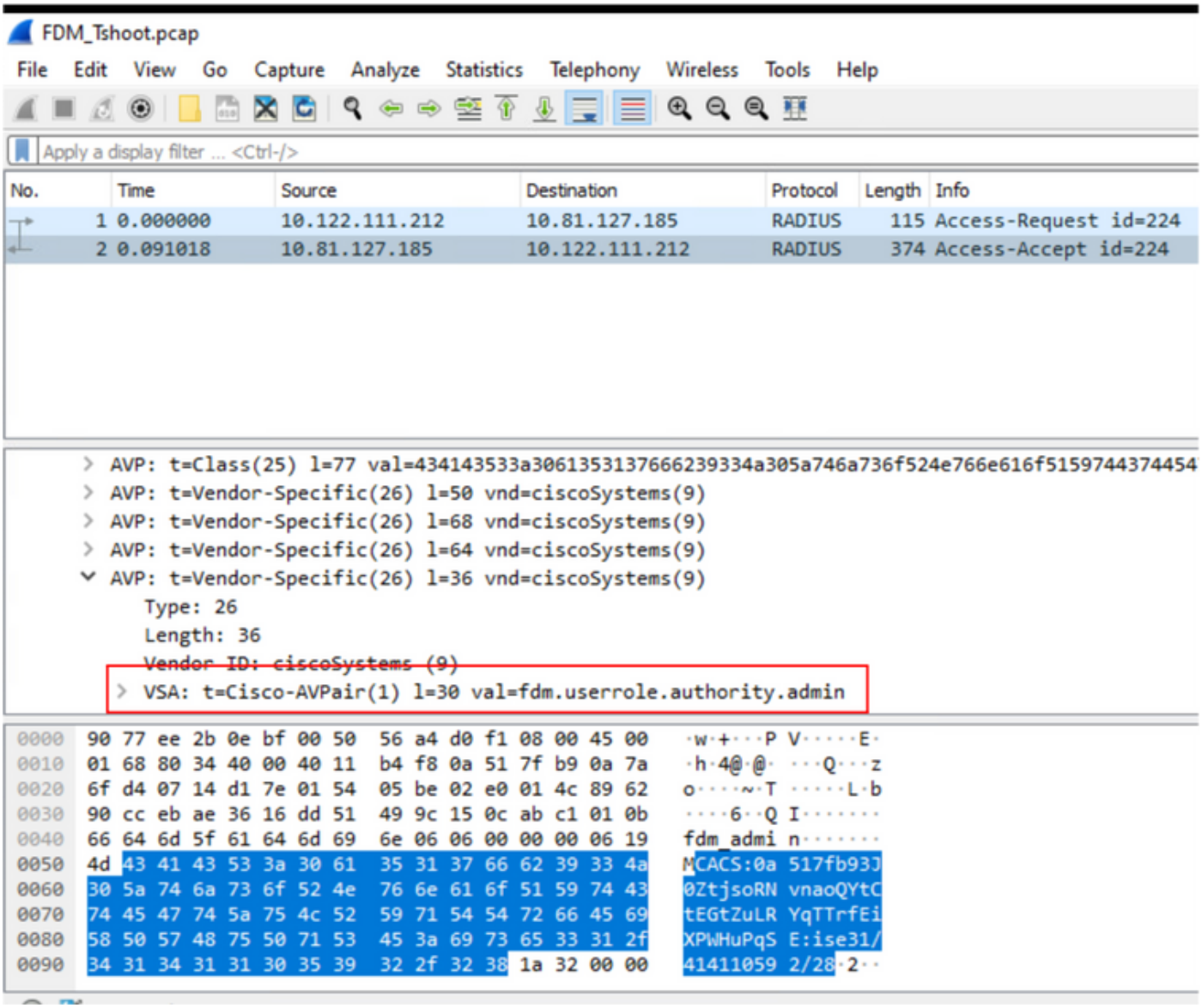
Paso 4. En ISE, seleccione el botón **Stop** y verifique que el archivo pcap se ha enviado al repositorio definido.







Paso 5. Abra el archivo pcap para validar la comunicación correcta entre FDM e ISE.



Si no se muestra ninguna entrada en el archivo pcap, valide las siguientes opciones:

1. Se ha agregado la dirección IP de ISE correcta en la configuración de FDM
2. En caso de que haya un firewall en el medio, verifique que el puerto 1812-1813 esté permitido.
3. Comprobar la comunicación entre ISE y FDM

Validación de la comunicación con el archivo generado por FDM.

En la página de solución de problemas de archivos generados a partir de dispositivos FDM, busque palabras clave:

- FdmPasswordLoginHelper
- NGFWDefaultUserMgmt
- AAAIdentitySourceStatusManager
- RadiusIdentitySourceManager

Todos los registros relacionados con esta función se pueden encontrar en /var/log/cisco/ngfw-onbox.log

Referencias:

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd-

fdm-mgmt.html#id_73793

Problemas comunes

Caso 1: la autenticación externa no funciona

- Compruebe la clave secreta, el puerto o el nombre de host
- Configuración incorrecta de AVP en RADIUS
- El servidor puede estar en "tiempo muerto"

Caso 2: falla la prueba IdentitySource

- Asegúrese de que se guardan los cambios realizados en el objeto
- Asegúrese de que las credenciales son correctas

Limitaciones

- FDM permite un máximo de 5 sesiones de FDM activas.
- Creación de la 6a sesión resulta en la 1a sesión revocada
- El nombre de RadiusIdentitySourceGroup no puede ser "LocalIdentitySource"
- Máximo de 16 RadiusIdentitySources para un RadiusIdentitySourceGroup
- La configuración incorrecta de AVP en RADIUS resulta en la denegación de acceso a FDM

Preguntas y respuestas

P: ¿Funciona esta función en el modo de evaluación?

R: Sí

P: Si dos usuarios de solo lectura inician sesión, donde tienen acceso al usuario de solo lectura 1 y inician sesión desde dos exploradores diferentes. ¿Cómo se mostrará? ¿Qué pasará?

R.: Ambas sesiones de usuario se muestran en la página de sesiones de usuario activas con el mismo nombre. Cada entrada muestra un valor individual para la marca de tiempo.

P: ¿Cuál es el comportamiento? El servidor RADIUS externo proporciona un rechazo de acceso frente a "no response" si tiene la autenticación local configurada en 2nd?

R.: Puede probar la autenticación LOCAL aunque obtenga rechazo de acceso o sin respuesta si tiene la autenticación local configurada en 2º lugar.

P.: Cómo diferencia ISE una solicitud RADIUS de inicio de sesión de administrador frente a una solicitud RADIUS para autenticar un usuario VPN de RA

R: ISE no diferencia una solicitud RADIUS para los usuarios de administración frente a los de RAVPN. FDM examina el atributo cisco-avpair para averiguar la autorización para el acceso de administrador. ISE envía todos los atributos configurados para el usuario en ambos casos.

P.: Esto significa que los registros de ISE no pueden diferenciar entre un inicio de sesión de administrador de FDM y el mismo usuario que accede a la VPN de acceso remoto en el mismo

dispositivo. ¿Se ha pasado algún atributo RADIUS a ISE en la solicitud de acceso en la que ISE pueda introducir la clave?

R: A continuación se muestran los atributos RADIUS ascendentes que se envían desde el FTD a ISE durante la autenticación RADIUS para RAVPN. Estos no se envían como parte de la Solicitud de acceso a la administración de autenticación externa y se pueden utilizar para diferenciar un registro de administración de FDM en comparación con el inicio de sesión de usuario de RAVPN.

146 - Nombre del grupo de túnel o Nombre del perfil de conexión.

150 - Tipo de cliente (valores aplicables: 2 = AnyConnect Client SSL VPN, 6 = AnyConnect Client IPsec VPN (IKEv2).

151 - Tipo de sesión (valores aplicables: 1 = VPN SSL de cliente AnyConnect, 2 = VPN IPSec de cliente AnyConnect (IKEv2)).

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).