

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](#)

[Configuración de FMC](#)

[Configuración de FTD](#)

[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 7.2.5
- vFTD 7.2.5.

- ISE 3.2

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.

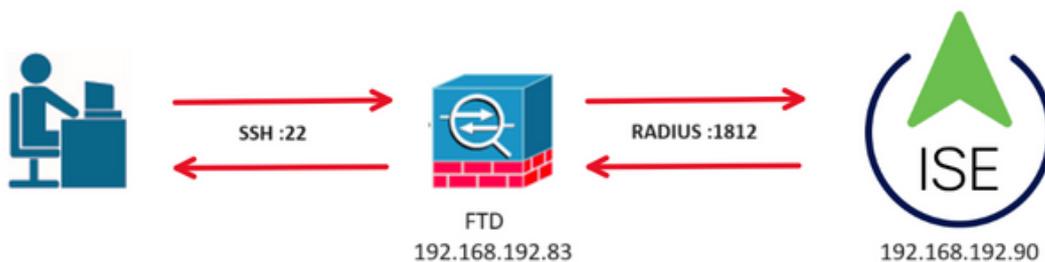
Autenticación externa para FMC

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

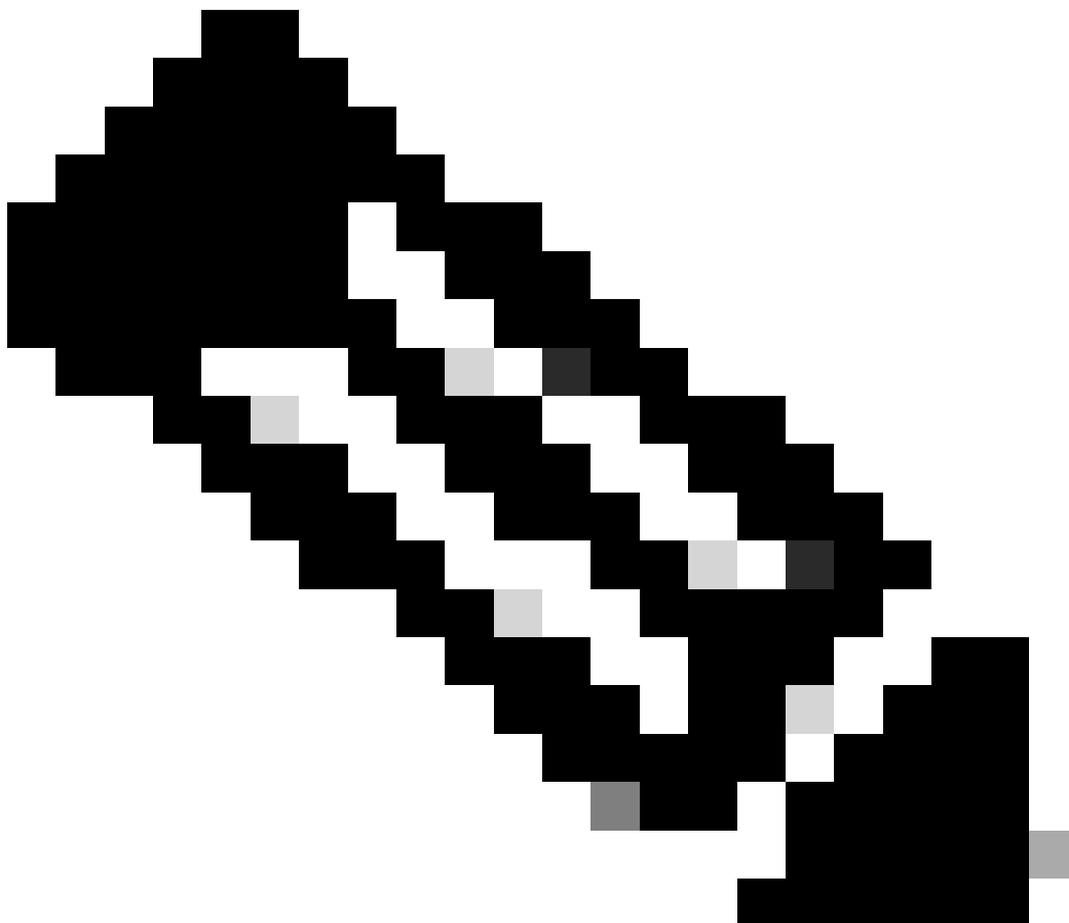
Para el FTD, sólo puede activar un objeto de autenticación externo.

Topología de red



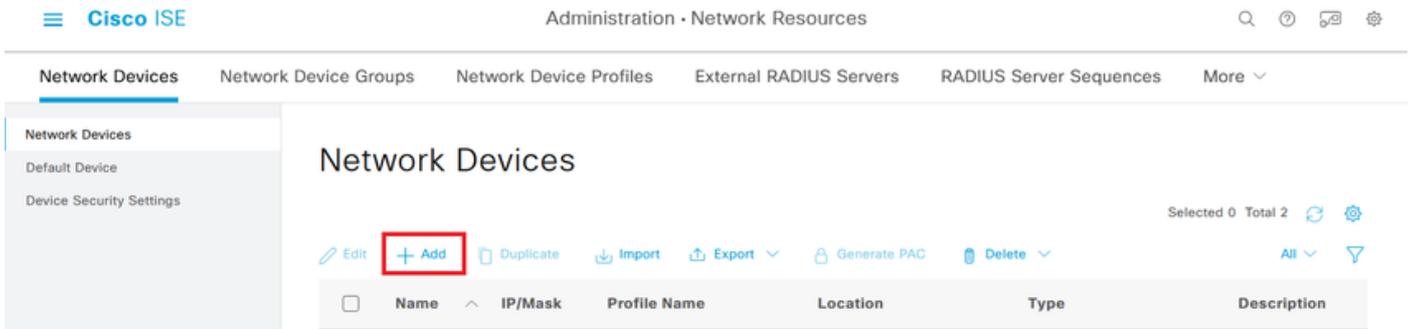
Configurar

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.

Paso 1. Agregue un nuevo dispositivo de red. Navegue hasta el icono de la hamburguesa  ubicado en la esquina superior izquierda >Administración > Recursos de red > Dispositivos de red > +Agregar.

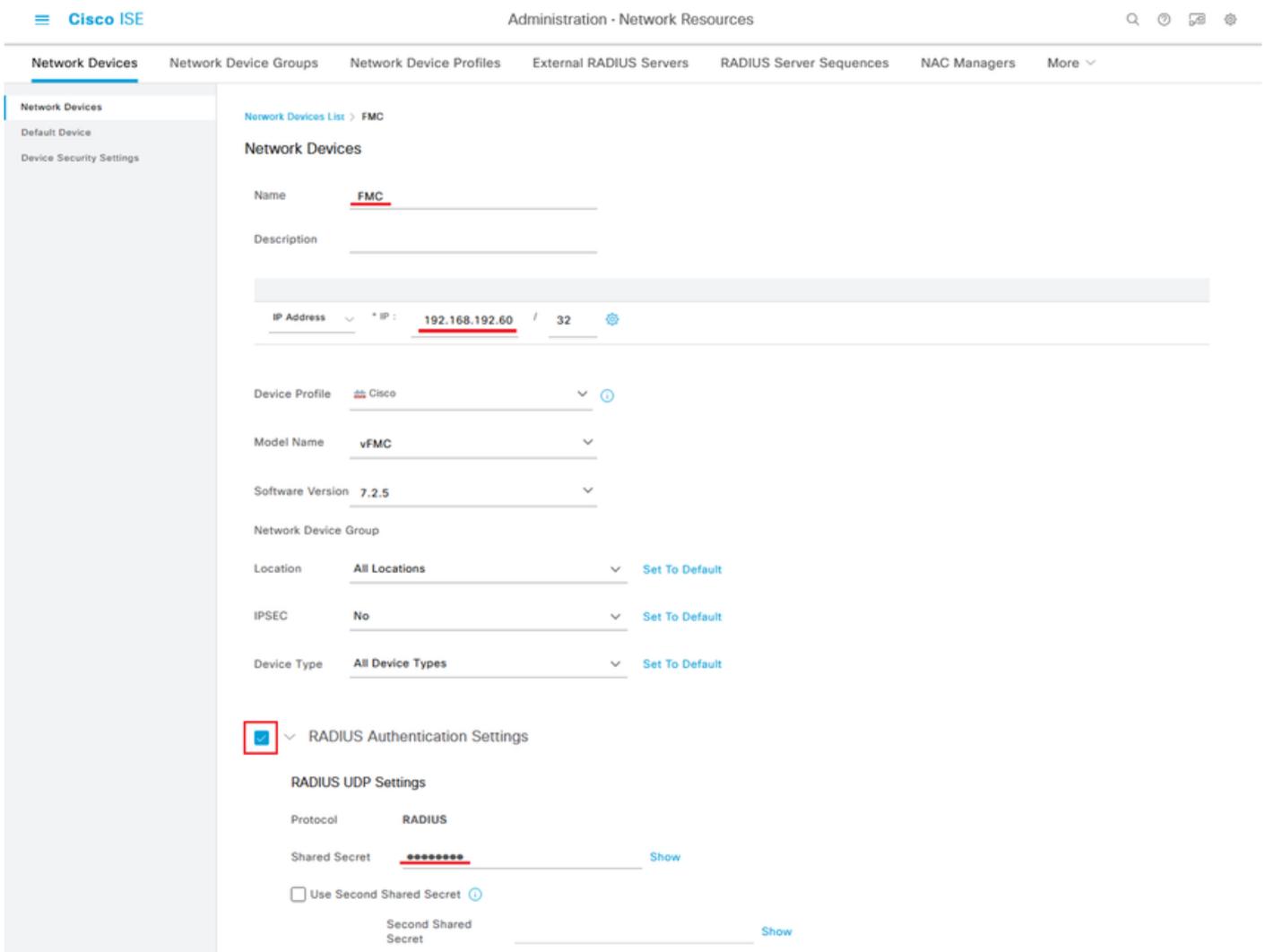


Paso 2. Asigne un nombre al objeto del dispositivo de red e inserte la dirección IP del CSP.

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.

The screenshot shows the configuration page for a Network Device in Cisco ISE. The device name is 'FTD' and its IP address is '192.168.192.83/32'. The device profile is 'Cisco', model name is 'vFTD', and software version is '7.2.5'. The RADIUS Authentication Settings section is expanded, and the 'RADIUS' checkbox is checked. The 'Shared Secret' is masked with asterisks. The 'Use Second Shared Secret' checkbox is unchecked.

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

The screenshot shows the 'Network Devices' list in Cisco ISE. The table displays two devices: FMC and FTD. The FTD device is highlighted in blue.

Name	IP/Mask	Profile Name	Location	Type	Description
FMC	192.168.192.60/32	Cisco	All Locations	All Device Types	
FTD	192.168.192.83/32	Cisco	All Locations	All Device Types	

Paso 3. Cree los grupos de identidad de usuario necesarios. Vaya al icono de la hamburguesa  situado en la esquina superior izquierda > Administración > Gestión de identidades > Grupos > Grupos de identidades de usuario > + Agregar

The screenshot shows the Cisco ISE Administration interface for Identity Management. The breadcrumb trail is Administration > Identity Management > User Identity Groups. On the left, there is a sidebar for 'Identity Groups' with a search bar and a tree view containing 'Endpoint Identity Groups' and 'User Identity Groups'. The main area displays a table with columns for 'Name' and 'Description'. Above the table, there are action buttons: 'Edit', '+ Add' (highlighted with a red box), 'Delete', 'Import', and 'Export'. The table currently shows no data, with 'Selected 0' and 'Total 11' indicated.

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.

The screenshot shows the configuration form for a new 'Identity Group'. The breadcrumb trail is Administration > Identity Management > User Identity Groups > FMC and FTD admins. The form has two fields: '* Name' with the value 'FMC and FTD admins' and 'Description' with the value 'FMC and FTD admins ISE local.'. At the bottom of the form, there are two buttons: 'Save' (highlighted with a red box) and 'Reset'.

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

The screenshot shows the configuration form for a second 'Identity Group'. The breadcrumb trail is Administration > Identity Management > User Identity Groups > FMC and FTD ReadOnly. The form has two fields: '* Name' with the value 'FMC and FTD ReadOnly' and 'Description' with the value 'FMC and FTD ReadOnly.'. At the bottom of the form, there are two buttons: 'Save' (highlighted with a red box) and 'Reset'.

Paso 4.2. Validar que ambos grupos se muestran en la Lista de grupos de identidades de usuario. Utilice el filtro para encontrarlos fácilmente.

The screenshot shows the Cisco ISE Administration interface for Identity Management. The main heading is "User Identity Groups". On the left, a sidebar shows a tree view with "User Identity Groups" selected. The main content area has a toolbar with "Edit", "+ Add", "Delete", "Import", and "Export" buttons. Below the toolbar is a table with columns "Name" and "Description". The table contains two entries: "fmc" and "FMC and FTD admins ISE local". A "Quick Filter" dropdown is visible on the right, highlighted with a red box.

Name	Description
fmc	
<input type="checkbox"/> FMC and FTD ReadOnly	FMC and FTD ReadOnly
<input type="checkbox"/> FMC and FTD admins	FMC and FTD admins ISE local.

Paso 5. Cree los usuarios locales y agréguelos a su grupo correspondiente. Vaya a > Administración > Gestión de identidad > Identidades > + Agregar.

The screenshot shows the Cisco ISE Administration interface for Identity Management, specifically the "Network Access Users" section. The main heading is "Network Access Users". On the left, a sidebar shows a tree view with "Users" selected. The main content area has a toolbar with "Edit", "+ Add", "Change Status", "Import", "Export", and "Delete" buttons. Below the toolbar is a table with columns: "Status", "Username", "Description", "First Name", "Last Name", "Email Address", "User Identity Groups", and "Adn". The table is currently empty, displaying "No data available".

Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Adn
No data available							

Paso 5.1. En primer lugar, cree el usuario con derechos de administrador. Asignarle un nombre, una contraseña y los administradores de FMC y FTD del grupo.

Users
Latest Manual Network Scan Res...

Network Access Users List > New Network Access User

Network Access User

* Username firewall_admin

Status Enabled

Account Name Alias

Email

Passwords

Password Type: Internal Users

Password Lifetime:

With Expiration

Never Expires

Password Re-Enter Password

* Login Password ●●●●●●●● ●●●●●●●● [Generate Password](#)

Enable Password _____ _____ [Generate Password](#)

Users
Latest Manual Network Scan Res...

User Groups

FMC and FTD admins [+](#)

[Submit](#) [Cancel](#)

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

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Res...

Network Access Users List > New Network Access User

Network Access User

* Username firewall_readuser

Status Enabled ▾

Account Name Alias ⓘ

Email

Passwords

Password Type: Internal Users ▾

Password Lifetime:

- With Expiration ⓘ
- Never Expires ⓘ

Password Re-Enter Password

* Login Password ⓘ

Enable Password ⓘ

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Res...

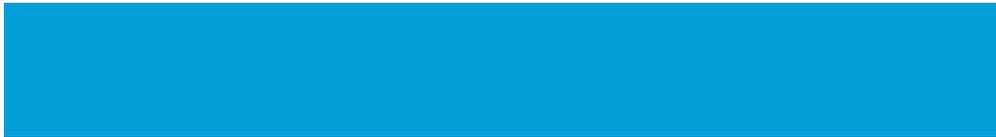
User Groups

⋮ FMC and FTD ReadOnly ▾ ⓘ +

Cancel

Paso 6. Cree el perfil de autorización para el usuario administrador.

Vaya a



> Política > Elementos de política > Resultados > Autorización > Perfiles de autorización > +Agregar.

Defina un nombre para el perfil de autorización, deje Tipo de acceso como ACCESS_ACCEPT y, en Configuración de atributos avanzados, agregue un Radio > Clase [25] con el valor Administrador y haga clic en Enviar.

The screenshot shows the Cisco ISE web interface for configuring a Policy Element. The breadcrumb trail is: Policy > Policy Elements > Results > Authorization Profiles > FMC and FTD Admins. The left sidebar shows a navigation menu with categories: Authentication (Allowed Protocols), Authorization (Authorization Profiles, Downloadable ACLs), Profiling, Posture, and Client Provisioning. The main content area is titled 'Authorization Profile' and contains the following configuration fields:

- * Name: FMC and FTD Admins
- Description: (Empty text box)
- * Access Type: ACCESS_ACCEPT (dropdown menu)
- Network Device Profile: Cisco (dropdown menu)
- Service Template: (Empty dropdown menu)

Dictionaryes Conditions **Results**

Authentication >

Authorization >

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

Advanced Attributes Settings

⋮ Radius:Class = Administrator - +

Attributes Details

Access Type = ACCESS_ACCEPT
Class = Administrator

Submit Cancel

Paso 7. Repita el paso anterior para crear el perfil de autorización para el usuario de sólo lectura. Cree la clase Radius con el valor ReadUser en su lugar Administrator esta vez.

Dictionaryes Conditions **Results**

Authentication >

Allowed Protocols

Authorization >

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name FMC and FTD ReadUser

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Navigation tabs: Dictionaries, Conditions, **Results**

Left sidebar menu:

- Authentication >
- Authorization ▾
 - Authorization Profiles**
 - Downloadable ACLs
- Profiling >
- Posture >
- Client Provisioning >

Main content area:

- Advanced Attributes Settings
 - Radius:Class = ReadUser
- Attributes Details
 - Access Type = ACCESS_ACCEPT
 - Class = ReadUser

Buttons: **Submit** (highlighted with a red box), Cancel

Paso 8. 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 > icono



ubicado en la esquina superior izquierda.

Cisco ISE Policy · Policy Sets

Policy Sets Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
+	Default	Default policy set		Default Network Access	45	⚙️	➔

Reset Save

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.

Conditions Studio

Library

Search by Name

5G
Catalyst_Switch_Local_Web_Authentication
Source FMC
Switch_Local_Web_Authentication
Switch_Web_Authentication
Wired_802.1X
Wired_MAB
Wireless_802.1X
Wireless_Access

Editor

OR

Radius-NAS-IP-Address
Equals 192.168.192.60

Radius-NAS-IP-Address
Equals 192.168.192.83

NEW AND OR

Set to 'is not'

Duplicate Save

Close Use

Paso 8.2. Una vez finalizado, pulse Guardar.

Cisco ISE

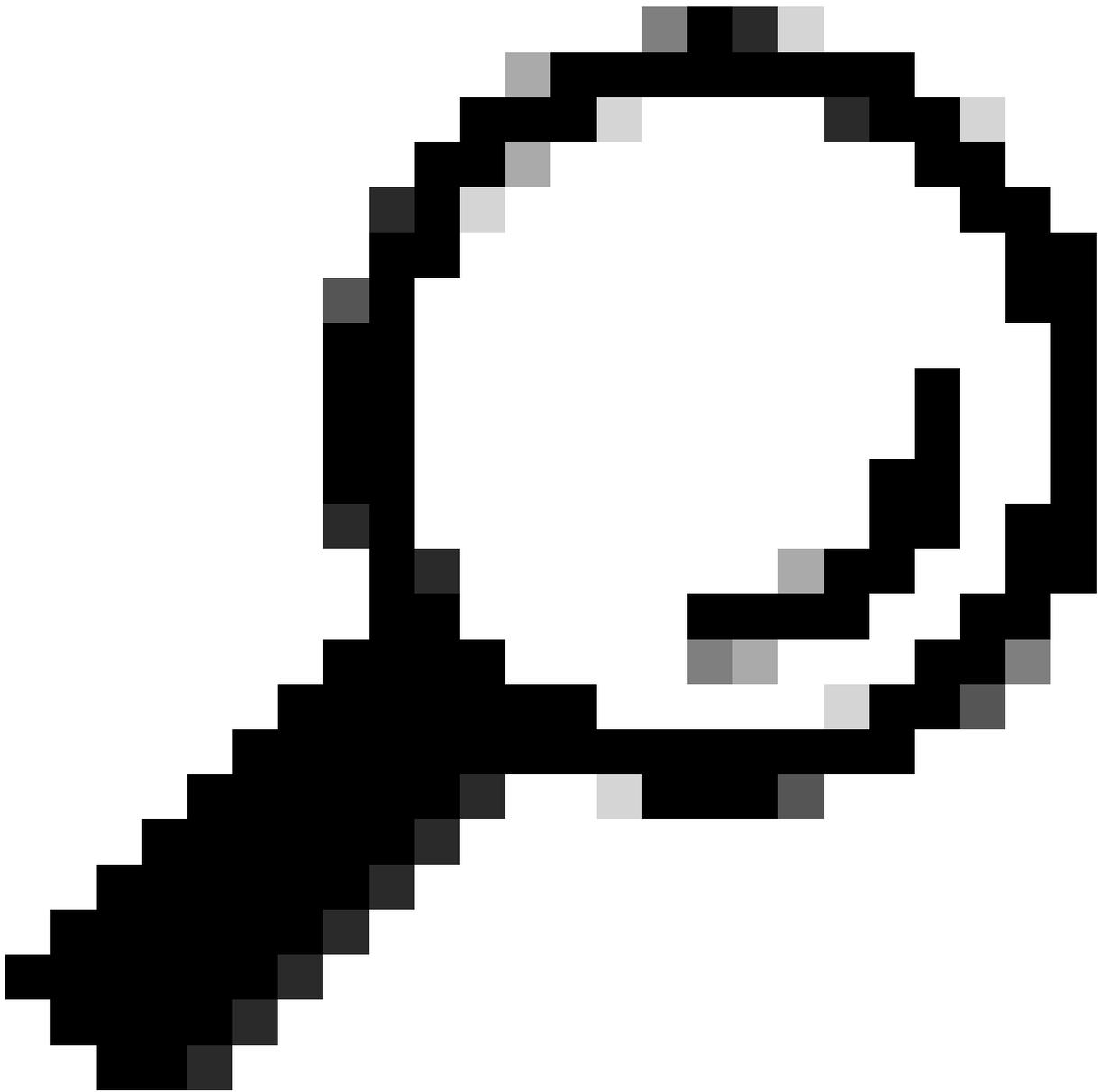
Policy · Policy Sets

Policy Sets

Reset Reset Policyset Hitcounts Save

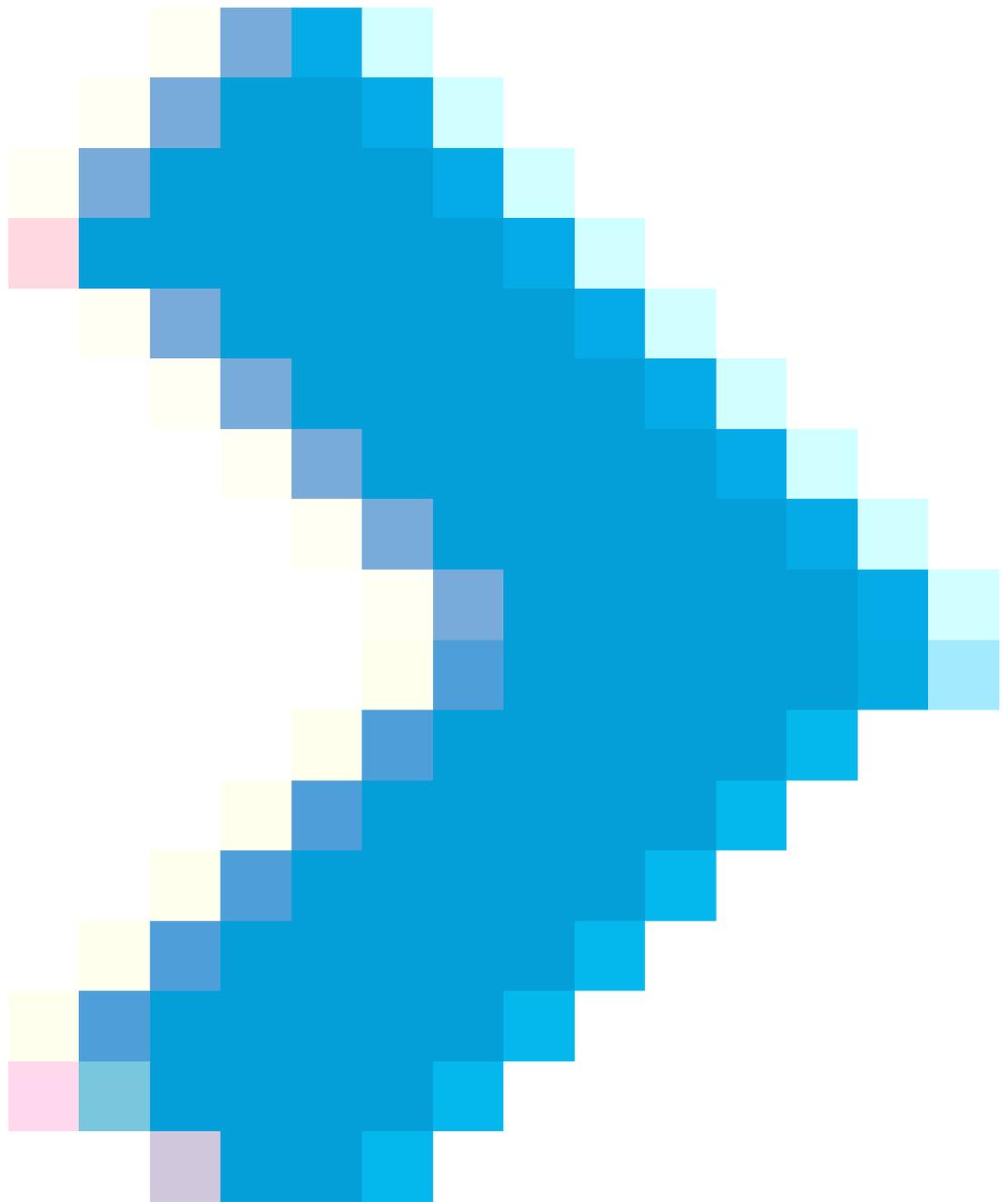
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	FMC and FTD Access	Management Access	OR Radius-NAS-IP-Address EQUALS 192.168.192.60 Radius-NAS-IP-Address EQUALS 192.168.192.83	Default Network Access	0	⚙️ →	→
✓	Default	Default policy set		Default Network Access	0	⚙️ →	→

Reset Save



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

Paso 9. Para ver el nuevo conjunto de políticas, pulse el



icono situado al final de la fila.

Expanda el menú Directiva de autorización y presione el



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 con Nombre de Atributo Equivale a Grupos de Identidad de Usuario: Administradores de FMC y FTD (el nombre de grupo creado en el Paso 4) y haga clic en Usar.

Establezca las condiciones para que el Grupo de Identidad de Diccionario con Nombre de Atributo sea Igual a Grupos de Identidad de Usuario: FMC y FTD ReadOnly (el nombre de grupo creado en el Paso 4) y haga clic en Usar.

Conditions Studio

Library

Search by Name

5G

BYOD_Is_Registered

Catalyst_Switch_Local_Web_Authentication

Compliance_Unknown_Devices

Editor

IdentityGroup-Name

Equals User Identity Groups:FMC and FTD ReadOnly

Set to 'Is not'

Duplicate Save

NEW AND OR

Close Use

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

Cisco ISE Policy - Policy Sets

Policy Sets → FMC and FTD Access

Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	FMC and FTD Access	Management Access	OR <ul style="list-style-type: none"> Radius-NAS-IP-Address EQUALS 192.168.192.60 Radius-NAS-IP-Address EQUALS 192.168.192.83 	Default Network Access	0

> Authentication Policy (1)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

∨ Authorization Policy (3)

Status	Rule Name	Conditions	Results			Hits	Actions
			Profiles	Security Groups			
✓	FMC and FTD read user access	IdentityGroup-Name EQUALS User Identity Groups:FMC and FTD ReadOnly	FMC and FTD ReadUser	Select from list	0	⚙️	
✓	FMC and FTD admin user access	IdentityGroup-Name EQUALS User Identity Groups:FMC and FTD admins	FMC and FTD Admins	Select from list	0	⚙️	
✓	Default		DenyAccess	Select from list	0	⚙️	

Reset Save

Configuración de 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 RADIUS Class que se configuraron en los pasos 6 y 7 de la configuración de ISE: Administrator y ReadUser para firewall_admin y firewall_readuser respectivamente.

RADIUS-Specific Parameters

Timeout (Seconds)

Retries

Access Admin

Administrator

Discovery Admin

External Database User

Intrusion Admin

Maintenance User

Network Admin

Security Analyst

Security Analyst (Read Only)

Security Approver

Threat Intelligence Director (TID) User

Default User Role

To specify the default user role if user is not found in any group



Nota: 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.

Paso 4. Rellene la Lista de usuarios de acceso CLI del administrador en Filtro de acceso CLI con los nombres de usuario permitidos para obtener acceso CLI.

Haga clic en Guardar una vez hecho.

CLI Access Filter

(For Firewall Management Center (all versions) and Firewall Threat Defense (6.2.3 and 6.3), define users for CLI access. For Firewall Threat Defense 6.4 and later, we recommend defining users on the RADIUS server. Click [here](#) for more information)

Administrator CLI Access User List ex. user1, user2, user3 (lowercase letters only).

▸ Define Custom RADIUS Attributes

Additional Test Parameters

User Name

Password

*Required Field

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

Firewall Management Center

System / Users / External Authentication

Overview Analysis Policies Devices Objects Integration Deploy

Users User Roles External Authentication Single Sign-On (SSO)

Default User Role: None Shell Authentication Enabled (ISE_Radius) + Add External Authentication Object

Name	Method	Enabled
1. ISE_Radius	RADIUS	<input checked="" type="checkbox"/>

Configuración de FTD

Paso 1. En la GUI de FMC, navegue hasta Devices > Platform Settings. 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.

Firewall Management Center

Devices / Platform Settings Editor

Overview Analysis Policies Devices Objects Integration

Deploy

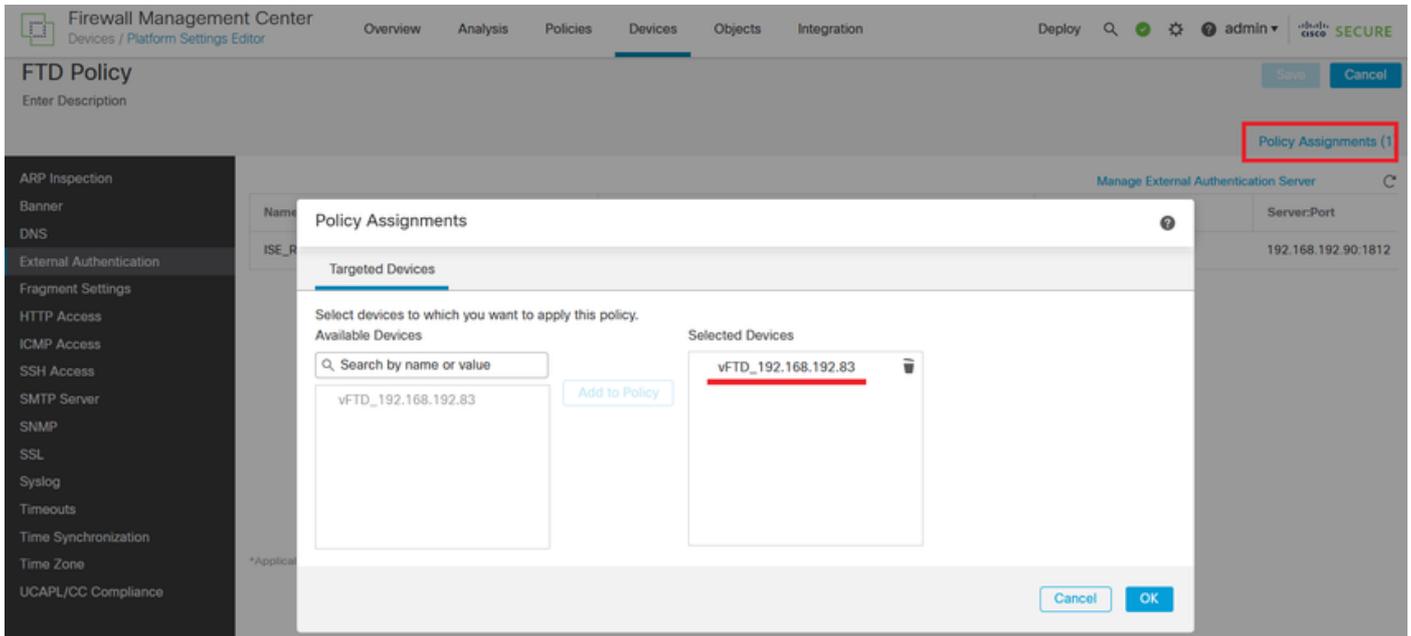
FTD Policy You have unsaved changes

Enter Description

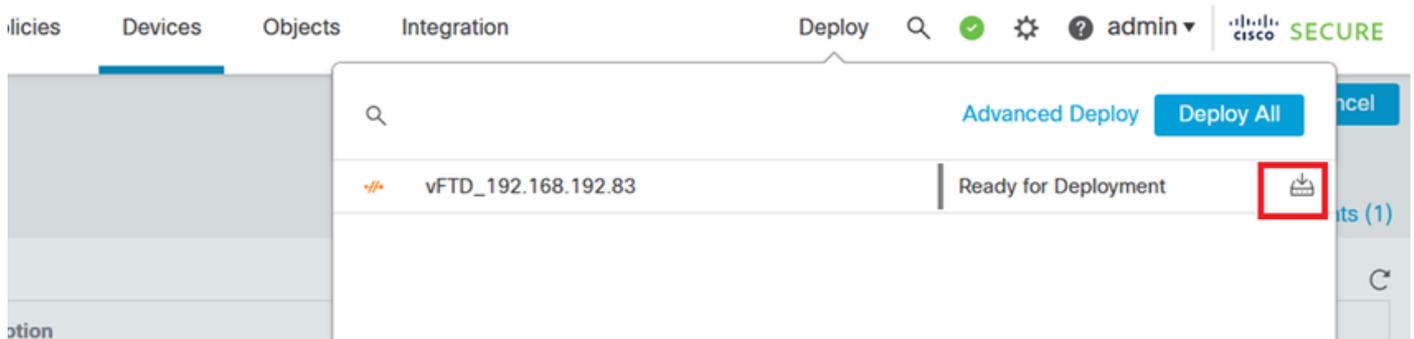
Policy Assignments (1)

Name	Description	Method	Server/Port	Encryption	Enabled
ISE_Radius		RADIUS	192.168.192.90:1812	no	<input checked="" type="checkbox"/>

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



Paso 3. Implemente los cambios.



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.



Success
Test Complete.

External Authentication Object

Authentication Method

Name *

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

▸ Define Custom RADIUS Attributes

Additional Test Parameters

User Name

Password

Test Output

Show Details ▾

```
check_auth_radius: szUser: firewall_admin
RADIUS config file: /var/tmp/4VQqxhXof/radiusclient_0.conf
radiusauth - response: [User-Name=firewall_admin]
radiusauth - response: [Class=Administrator]
radiusauth - response: [Class=CACS:c0a8c05a_cNaQKf8ZB2sOTPFOSbmj8V6n727Es2627TeUjzXUdA:ISE-LVILLAFR/479011358/67]
"firewall_admin" RADIUS Authentication OK
check_is_radius_member attrib match found: [Class=Administrator] - [Class=Administrator] *****
role_bee2eb18-e129-11df-a04a-42c66f0a3b36:
```

*Required Field

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).