

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

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Interoperabilidad](#)

[Licencias](#)

[Antecedentes](#)

[Diagrama de la red](#)

[Configurar](#)

[Configuración del FDM](#)

[Configuración de ISE](#)

[Verificación](#)

[Troubleshoot](#)

[Problemas comunes](#)

[Limitaciones](#)

[Preguntas y respuestas](#)

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

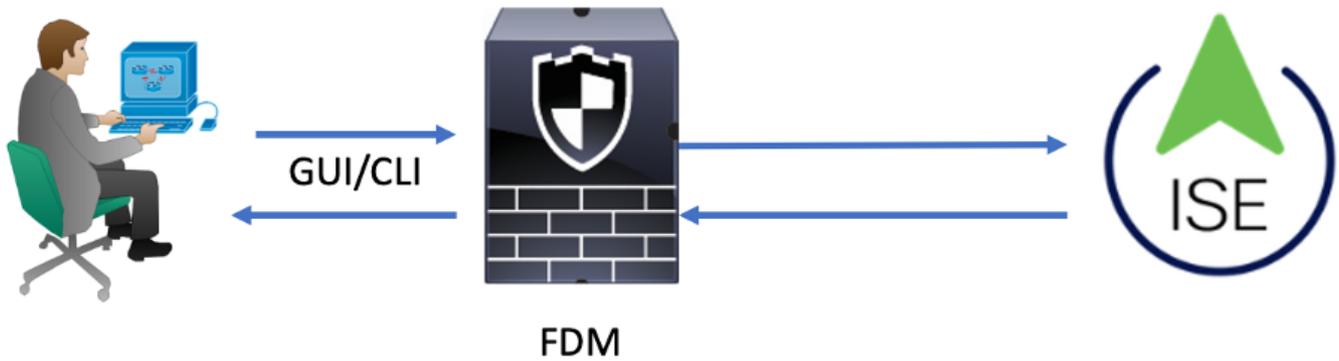
Existe la posibilidad de probar la configuración del servidor RADIUS y supervisar las sesiones de usuario activas y eliminar una sesión de usuario.

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

The screenshot displays the Cisco configuration interface for a device's Management Access settings. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device' (highlighted with a callout 1). The left sidebar shows 'System Settings' with 'Management Access' selected (callout 2). The main content area is titled 'Device Summary Management Access' (callout 1) and includes sections for 'AAA Configuration' (callout 3), 'Management Interface', and 'Data Interfaces'. Below these is a section for 'HTTPS Connection' and 'Server Group for Management/REST API' (callout 4). The 'Server Group' section has a 'Filter' dropdown and a list containing 'LocalIdentitySource' (checked). At the bottom, there is a 'Create New RADIUS Server Group' button (callout 5).

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

Nothing found

2

Create new RADIUS Server

CANCEL

OK

CANCEL

OK

Edit RADIUS Server

Capabilities of RADIUS Server ⓘ

Authentication Authorization

Name

ISE

Server Name or IP Address

10.81.127.185

Authentication Port

1812

Timeout ⓘ

10 seconds

1-300

Server Secret Key

●●●●●●●●

RA VPN Only (if this object is used in RA VPN Configuration)

TEST CANCEL OK

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

Add RADIUS Server Group

Name **3**

radius-server-group

Dead Time **10** minutes 0-1440

Maximum Failed Attempts **3** 1-5

RADIUS Server

i The servers in the group should be backups of each other

+

Filter **1**

radius-server **i**

4 OK

2 OK

Cancel

Cancel

Create new RADIUS Server

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

Device Summary

Management Access

AAA Configuration Management Interface Data Interfaces

Configure how to authenticate management connections to the device.

HTTPS Connection

Server Group for Management/REST API

Filter

LocalIdentitySource

radius-server-group **i**

Create New RADIUS Server Group

AAA Configuration Management Interface Data Interfaces Management Web Server

Configure how to authenticate management connections to the device.

HTTPS Connection

Server Group for Management/REST API

To use a RADIUS server successfully, you must configure the RADIUS user accounts with the required authorization values, as described in the [help](#).

Radius-server-group TEST

Authentication with LOCAL

After External Server

SAVE

SSH Connection

Server Group

To use a RADIUS server successfully, you must configure the RADIUS user accounts with the required authorization values, as described in the [help](#).

Radius-server-group TEST

Authentication with LOCAL

Before External Server

SAVE

Paso 6. Guarde la configuración

Device Summary

Management Access

AAA Configuration Management Interface Data Interfaces

Configure how to authenticate management connections to the device.

HTTPS Connection

Server Group for Management/REST API

To use a RADIUS server successfully, you must configure the RADIUS user accounts with the required authorization values, as described in the [help](#).

radius-server-group TEST

Authentication with LOCAL

Before External Server

SAVE

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**

Network Devices

Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network Devices

Default Device

Device Security Settings

Edit + Add Duplicate Import Export Generate PAC Delete

Name	IP/Mask	Profile Name	Location	Type	Description
------	---------	--------------	----------	------	-------------

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**

Cisco ISE

Administration · Network Resources

Evaluation Mode 89 Days

Network Devices

Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences More

Network Devices

Default Device

Device Security Settings

Name

Description

IP Address

Device Profile

Model Name

Software Version

RADIUS Authentication Settings

RADIUS UDP Settings

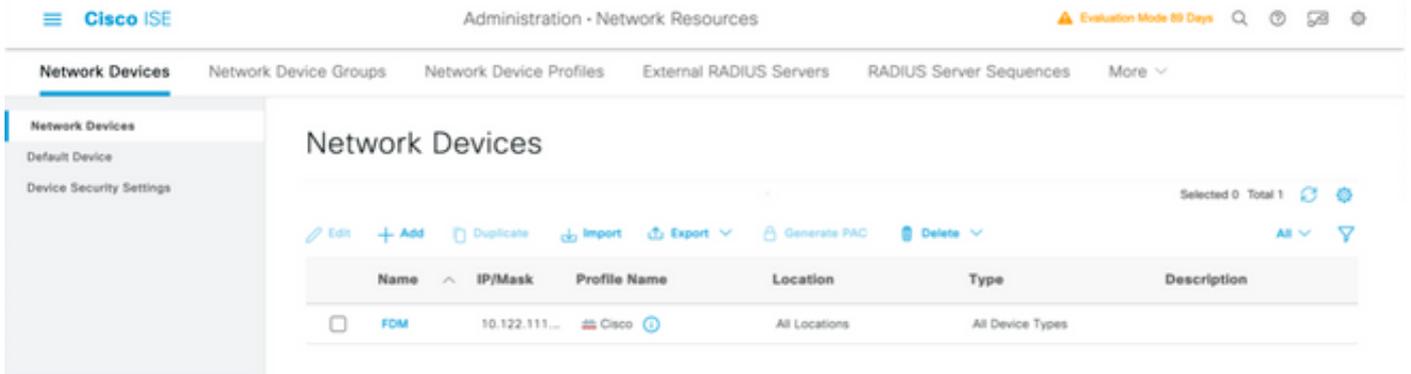
Protocol

Shared Secret [Show](#)

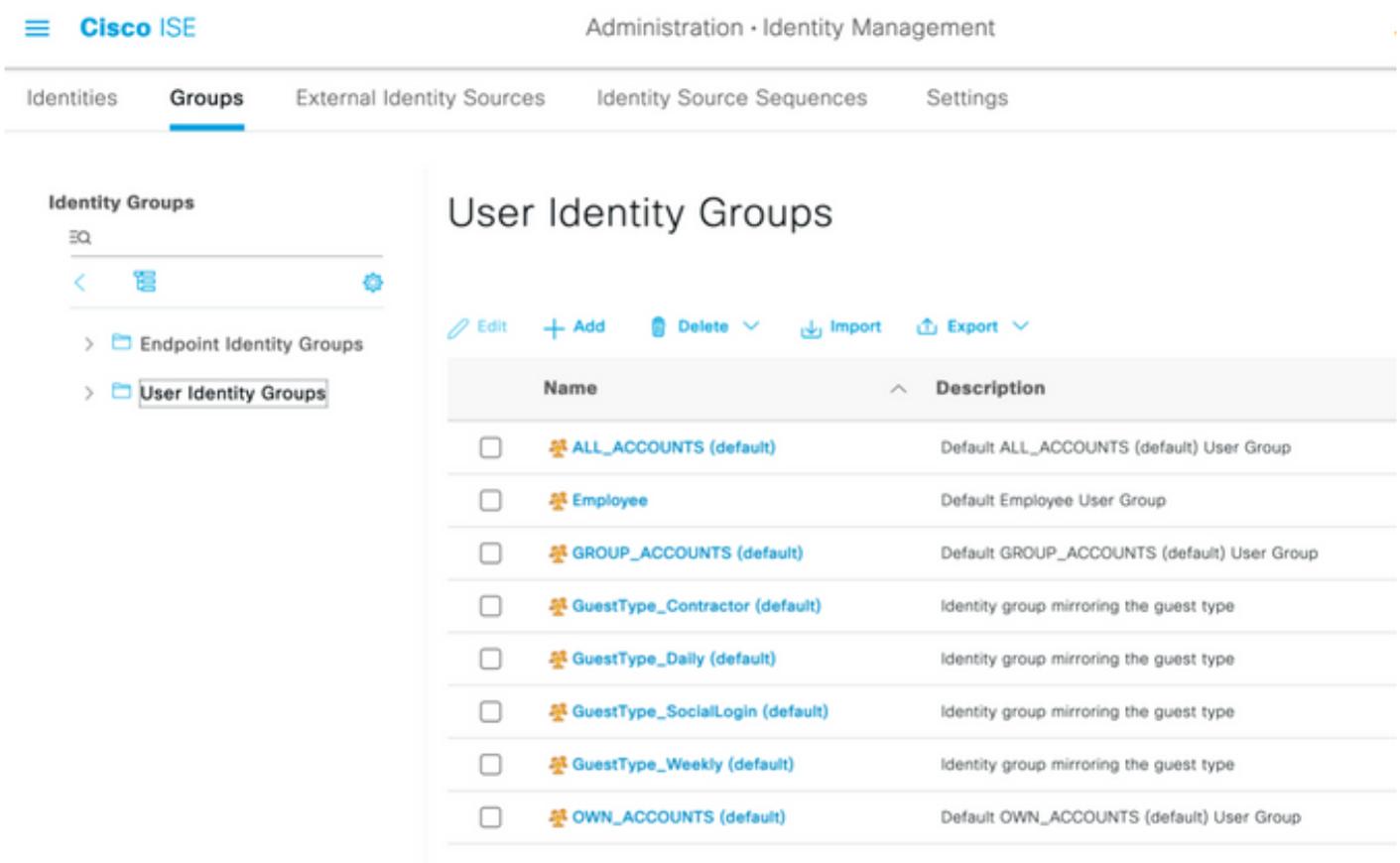
Use Second Shared Secret [i](#)

networkDevices.secondSharedSecret [Show](#)

CoA Port [Set To Default](#)



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**

Cisco ISE Administration - Identity Management

Identity Groups > New User Identity Group

Identity Group

* Name FDM_admin

Description

Submit Cancel

User Identity Groups

Selected 0 Total 2

Edit Add Delete Import Export Quick Filter

Name	Description
FDM	
<input type="checkbox"/> FDM_ReadOnly	
<input type="checkbox"/> FDM_admin	

Cisco ISE Administration - Identity Management

Identity Groups > New User Identity Group

Identity Group

* Name FDM_ReadOnly

Description

Submit Cancel

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.

Cisco ISE Administration - Identity Management

Identities | Groups | External Identity Sources | Identity Source Sequences | Settings

Users

Network Access Users List > New Network Access User

Network Access User

* Username:

Status: Enabled

Email:

Passwords

Password Type:

Password: Re-Enter Password:

* Login Password:

Enable Password:

User Groups

FDM_admin

⋮

⌵

⊖

⊕

Cisco ISE Administration - Identity Management

Identities | Groups | External Identity Sources | Identity Source Sequences | Settings

Users

Network Access Users

Selected 0 Total 2

⌵ Edit + Add Change Status Import Export Delete Duplicate All

Status	Username	Description	First Name	Last Name	Email Address	User Identity Grou...	Admin
<input type="checkbox"/>	Enabled	fdm_admin				FDM_admin	
<input type="checkbox"/>	Enabled	fdm_readonly				FDM_ReadOnly	

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.

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

[Authorization Profiles](#) > New Authorization Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

Advanced Attributes Settings

⋮	<input type="text" value="Radius:Service-Type"/>	=	<input type="text" value="Administrative"/>	-
⋮	<input type="text" value="Cisco:cisco-av-pair"/>	=	<input type="text" value="fdm.userrole.authority.admin"/>	- +

Attributes Details

Access Type = ACCESS_ACCEPT

Service-Type = 6

cisco-av-pair = fdm.userrole.authority.admin

Advanced Attributes Settings

⋮	Radius:Service-Type	▼	=	NAS Prompt	▼	—
⋮	Cisco:cisco-av-pair	▼	=	<u>fdm.userrole.authority.ro</u>	▼	— +

Attributes Details

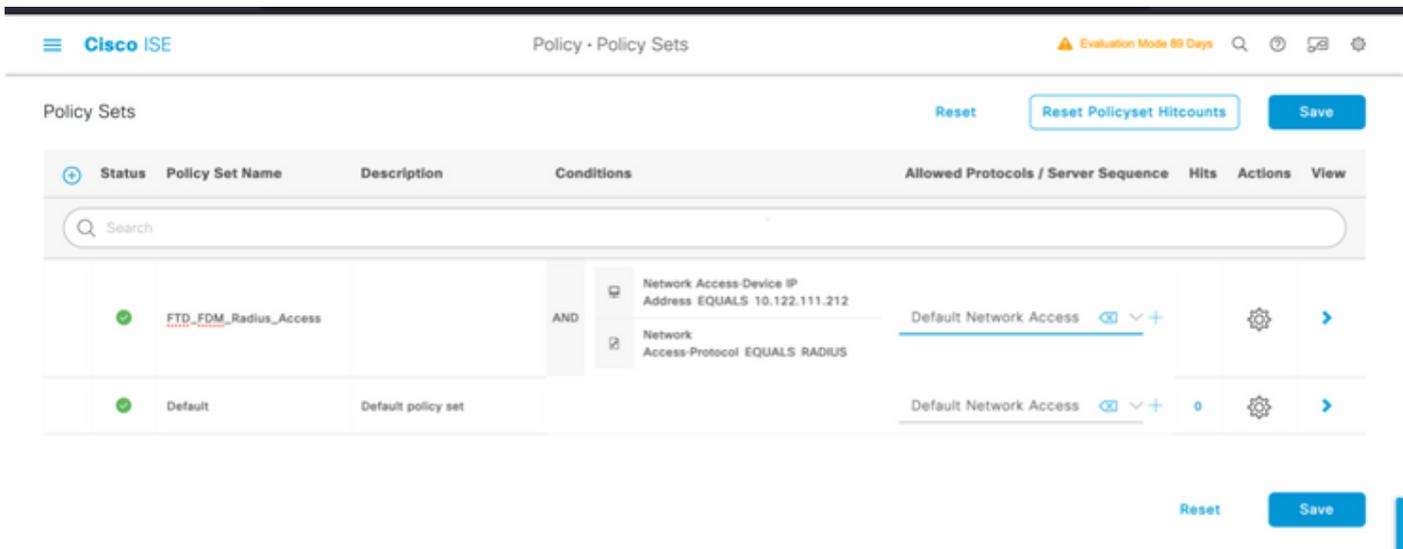
Access Type = ACCESS_ACCEPT
Service-Type = 7
cisco-av-pair = fdm.userrole.authority.ro

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.

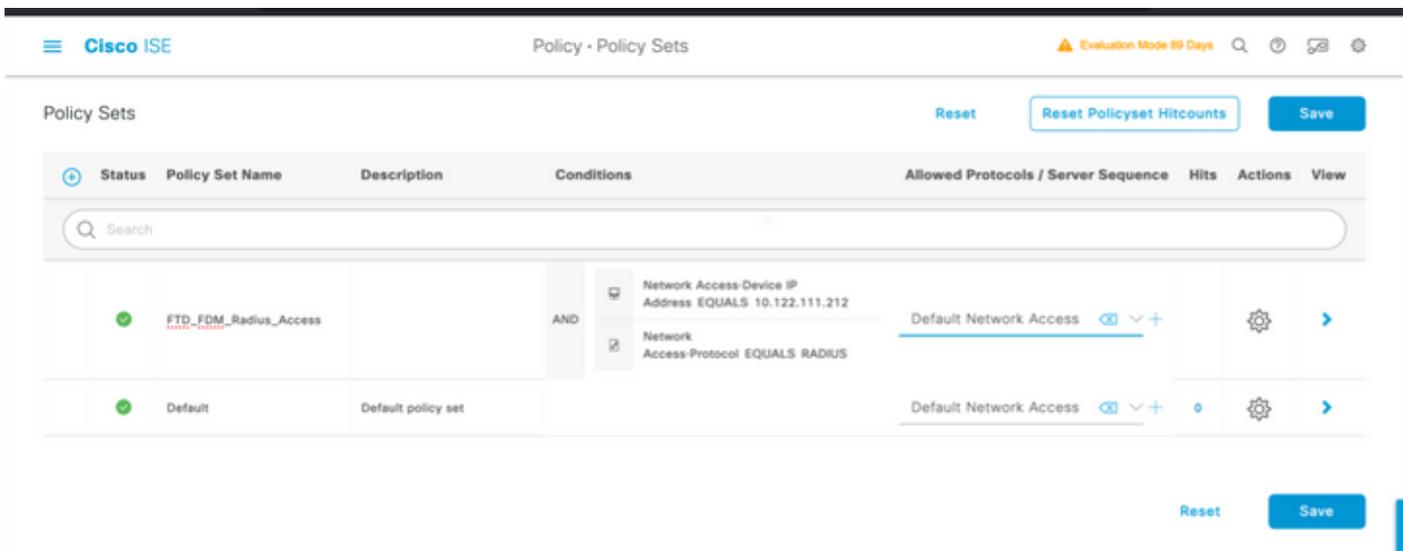
Paso 8. Seleccione el icono de tres líneas y desplácese hasta Directiva > Juegos de políticas.

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

Authorization Policy (3) [Click here to do visibility setup Do not show this again.](#)

			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
+	Search					
✓	FTD_FDM_Authz_AdminRole	AND IdentityGroup-Name EQUALS User Identity Groups:FDM_admin Radius-NAS-Port-Type EQUALS Virtual	FDM_Profile_Admin x	Select from list	3	⚙️
✓	FTD_FDM_Authz_RORole	AND IdentityGroup-Name EQUALS User Identity Groups:FDM_ReadOnly Radius-NAS-Port-Type EQUALS Virtual	FDM_Profile_RO x	Select from list	0	⚙️
✓	Default		DenyAccess x	Select from list	4	⚙️

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.

Deployment Licensing Certificates Logging **Maintenance** Upgrade Health Checks Backup [Click here to do visibility setup Do not show this again.](#)

Patch Management
Repository
 Operational Data Purging

Repository List > Add Repository

Repository Configuration

* Repository Name VMRepository

* Protocol FTP

Location

* Server Name 10.122.112.137

* Path /

Credentials

* User Name cisco

* Password

Verificación

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

Identity Sources

3 objects

#	NAME	TYPE	VALUE
1	LocalIdentitySource	LOCAL	
2	radius-server-group	RADIUS GROUP	radius-server
3	radius-server	RADIUS	171.69.246.220

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

Device Summary

Management Access

AAA Configuration Management Interface Data Interfaces

Configure how to authenticate management connections to the device.

HTTPS Connection

Server Group for Management/REST API

To use a RADIUS server successfully, you must configure the RADIUS user accounts with the required authorization values, as described in the help.

radius-server-group TEST

Authentication with LOCAL

Before External Server

SAVE

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

Add RADIUS Server Group

Name

Dead Time i minutes 0-1440

Maximum Failed Attempts 1-5

RADIUS Server

i The servers in the group should be backups of each other

+

1. radius-server

Server Credentials

Please provide the credentials for testing.

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.



Firepower Device Manager

Successfully logged out

fdm_admin

.....|

LOG IN

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

Cisco ISE Operations - RADIUS Evaluation Mode 79 Days

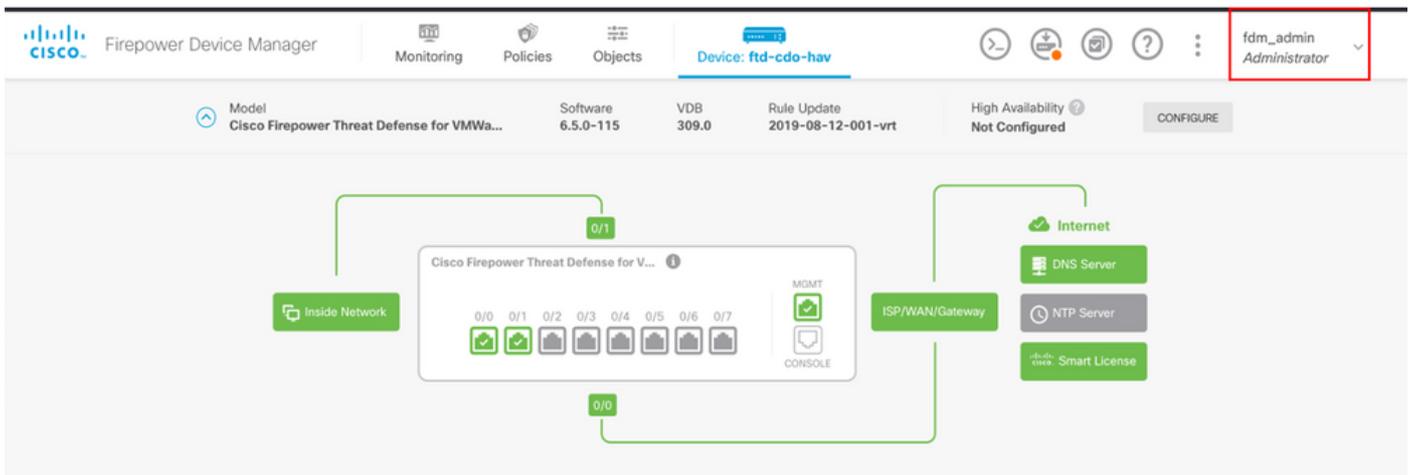
Live Logs Live Sessions Click here to do visibility setup Do not show this again.

Never Latest 20 records Last 3 hours

Refresh Reset Repeat Counts Export To Filter

Time	Status	Details	Repea...	Identity	Authentication Policy	Authorization Policy	Authorization Profiles
Jul 06, 2021 04:54:12.41...	✓			fdm_admin	FTD_FDM_Radius_Access >> FDM_...	FTD_FDM_Radius_Access >> FTD_FDM...	FDM_Profile_Admin

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:sqpyFmCcGBs1EjjDMdHnrkqdw40qvc7ne1I+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**

The screenshot shows the Cisco ISE web interface. The top navigation bar includes the Cisco ISE logo and three tabs: "Diagnostic Tools" (selected), "Download Logs", and "Debug Wizard". On the left, a sidebar menu lists "General Tools" (with a dropdown arrow), "TrustSec Tools" (with a right-pointing arrow), and "Session Trace Tests". Under "General Tools", several options are visible, including "TCP Dump" which is highlighted with a blue bar. The main content area is titled "TCP Dump > New" and contains the "Add TCP Dump" section. This section includes the following fields and controls:

- Host Name:** A dropdown menu with "ise31" selected.
- Network Interface:** A dropdown menu with "GigabitEthernet 0 [Up, Running]" selected and an information icon.
- Filter:** A text input field containing "ip host 10.122.111.212" and an information icon. Below it, an example reads: "E.g: ip host 10.77.122.123 and not 10.177.122.119".
- File Name:** A text input field containing "FDM_Tshoot".
- Repository:** A dropdown menu with "VM" selected and an information icon.
- File Size:** A spinner control set to "10" with "Mb" as the unit and an information icon.
- Limit to:** A spinner control set to "1" with "File(s)" as the unit and an information icon.
- Time Limit:** A spinner control set to "5" with "Minute(s)" as the unit and an information icon.
- Promiscuous Mode:** An unchecked checkbox.

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.

Cisco ISE Operations - Troubleshoot Evaluation Mode 79 Days

Diagnostic Tools Download Logs Debug Wizard

Click here to do visibility setup Do not show this again.

General Tools

- RADIUS Authentication Troubl...
- Execute Network Device Com...
- Evaluate Configuration Validat...
- Posture Troubleshooting
- Agentless Posture Troublesho...
- EndPoint Debug
- TCP Dump**
- Session Trace Tests

TCP Dump

The TCP Dump utility page is to monitor the contents of packets on a network interface and troubleshoot problems on the network as they appear

Rows/Page 1 << 1 >> Go 1 Total Rows

Refresh + Add Edit Trash Start Stop Download Filter

Host Name	Network Interface	Filter	File Name	Repository	File S...	Number o
<input type="checkbox"/> ise31.ciscoise.lab	GigabitEthernet 0 [Up, Run...	ip host 10.122.111.212	FDM_Tshoot	VM	10	1

```
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185) 200 Type set to 1
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185) STOR FDM_Tshoot.zip
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185) 150 Opening data channel for file upload to server of "/FDM_Tshoot.zip"
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185) 226 Successfully transferred "/FDM_Tshoot.zip"
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185) QUIT
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185) 221 Goodbye
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185) disconnected.
```

FDM_Tshoot.zip (evaluation copy)

File Commands Tools Favorites Options Help

Add Extract To Test View Delete Find Wizard Info VirusScan Comment SFX

FDM_Tshoot.zip - ZIP archive, unpacked size 545 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
<input type="checkbox"/> FDM_Tshoot.pcap	545	473	PCAP File	7/6/2021 5:21 ...	3A095B10

Total 1 file, 545 bytes

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

FDM_Tshoot.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.122.111.212	10.81.127.185	RADIUS	115	Access-Request id=224
2	0.091018	10.81.127.185	10.122.111.212	RADIUS	374	Access-Accept id=224

```

> AVP: t=Class(25) l=77 val=434143533a3061353137666239334a305a746a736f524e766e616f5159744374454
> AVP: t=Vendor-Specific(26) l=50 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=68 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=64 vnd=ciscoSystems(9)
▼ AVP: t=Vendor-Specific(26) l=36 vnd=ciscoSystems(9)
  Type: 26
  Length: 36
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=30 val=fdm.userrole.authority.admin

```

```

0000  90 77 ee 2b 0e bf 00 50 56 a4 d0 f1 08 00 45 00  .w.+...P V.....E.
0010  01 68 80 34 40 00 40 11 b4 f8 0a 51 7f b9 0a 7a  .h.4@.@. ...Q...z
0020  6f d4 07 14 d1 7e 01 54 05 be 02 e0 01 4c 89 62  o.....~T .....L.b
0030  90 cc eb ae 36 16 dd 51 49 9c 15 0c ab c1 01 0b  ....6..Q I.....
0040  66 64 6d 5f 61 64 6d 69 6e 06 06 00 00 00 06 19  fdm_admin.....
0050  4d 43 41 43 53 3a 30 61 35 31 37 66 62 39 33 4a  MCACS:0a 517fb93J
0060  30 5a 74 6a 73 6f 52 4e 76 6e 61 6f 51 59 74 43  0ZtjsoRN vnaoQYtC
0070  74 45 47 74 5a 75 4c 52 59 71 54 54 72 66 45 69  tEGtZuLR YqTTrfEi
0080  58 50 57 48 75 50 71 53 45 3a 69 73 65 33 31 2f  XPwHuPqS E:ise31/
0090  34 31 34 31 31 30 35 39 32 2f 32 38 1a 32 00 00  41411059 2/28.2..

```

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
- AAIdentitySourceStatusManager
- 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->

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).