

# Configurar Autenticação e Autorização Externa do FDM com ISE usando RADIUS

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Interoperabilidade](#)

[Licenciamento](#)

[Informações de Apoio](#)

[Diagrama de Rede](#)

[Configurar](#)

[Configuração do FDM](#)

[Configuração do ISE](#)

[Verificar](#)

[Troubleshoot](#)

[Problemas comuns](#)

[Limitações](#)

[Perguntas e respostas](#)

## Introduction

Este documento descreve o procedimento para integrar o Cisco Firepower Device Manager (FDM) ao Identity Services Engine (ISE) para autenticação de usuários administradores com o protocolo RADIUS para acesso via GUI e CLI.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Firepower Device Manager (FDM)
- Identity services engine (ISE)
- protocolo RADIUS

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Dispositivo Firepower Threat Defense (FTD), todas as plataformas Firepower Device Manager (FDM) versão 6.3.0+
- ISE versão 3.0

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Interoperabilidade

- Servidor RADIUS com usuários configurados com funções de usuário
- As funções de usuário devem ser configuradas no servidor RADIUS com cisco-av-pair
- Cisco-av-pair = fdm.userrole.authority.admin
- O ISE pode ser usado como um servidor RADIUS

## Licenciamento

Sem necessidade de licença específica, a licença básica é suficiente

## Informações de Apoio

Esse recurso permite que os clientes configurem a Autenticação externa com RADIUS e várias funções de usuário para esses usuários.

Suporte RADIUS para Acesso de Gerenciamento com 3 funções de usuário definidas pelo sistema:

- SOMENTE\_LEITURA
- READ\_WRITE (não é possível executar ações críticas do sistema, como Atualizar, Restaurar etc.)
- ADMIN

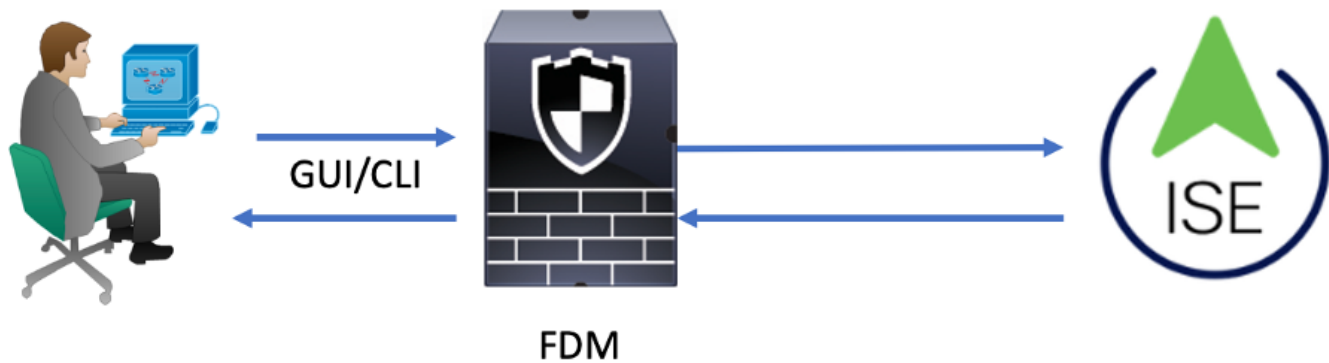
Há a capacidade de testar a configuração do servidor RADIUS, monitorar sessões de usuário ativas e excluir uma sessão de usuário.

O recurso foi implementado no FDM versão 6.3.0. Antes da versão 6.3.0, o FDM tinha suporte apenas para um usuário (admin).

Por padrão, o Cisco Firepower Device Manager autentica e autoriza usuários localmente, para ter um método de autenticação e autorização centralizado, você pode usar o Cisco Identity Service Engine através do protocolo RADIUS.

## Diagrama de Rede

A próxima imagem fornece um exemplo de uma topologia de rede



Processo:

1. Usuário Admin apresenta suas credenciais.
2. O processo de autenticação é acionado e o ISE valida as credenciais localmente ou por meio do Active Directory.
3. Quando a autenticação for bem-sucedida, o ISE enviará um pacote de Permissão para informações de autenticação e autorização ao FDM.
4. A conta é executada no ISE e ocorre um registro ativo de autenticação bem-sucedido.

## Configurar

### Configuração do FDM

Etapa 1. Faça logon no FDM e navegue até Dispositivo > Configurações do Sistema > guia Acesso de Gerenciamento

Etapa 2. Criar Novo Grupo de Servidores RADIUS

The screenshot displays the Cisco Meraki dashboard interface for configuring a device's management access. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device' (highlighted with a red box and labeled '1'). The left sidebar shows 'System Settings' with 'Management Access' highlighted (labeled '2'). The main content area is titled 'Device Summary Management Access' and includes sub-sections for 'AAA Configuration' (highlighted with a red box and labeled '3'), 'Management Interface', and 'Data Interfaces'. Below these, the 'HTTPS Connection' section is visible, with a 'Server Group for Management/REST API' section highlighted (labeled '4'). This section contains a 'Filter' dropdown menu with 'LocalIdentitySource' selected. At the bottom of the page, a button labeled 'Create New RADIUS Server Group' is highlighted with a red box and labeled '5'.

**Etapas 3.** Criar novo 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

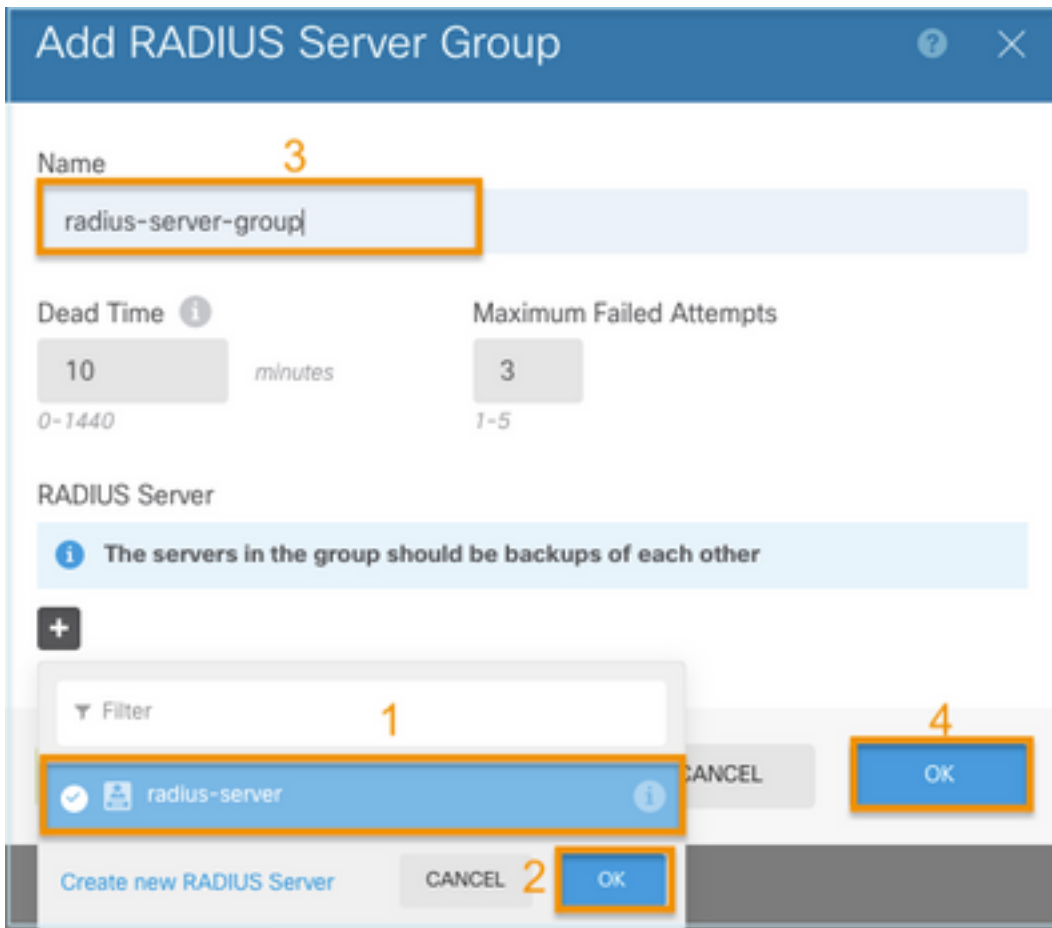
Server Secret Key

●●●●●●●●

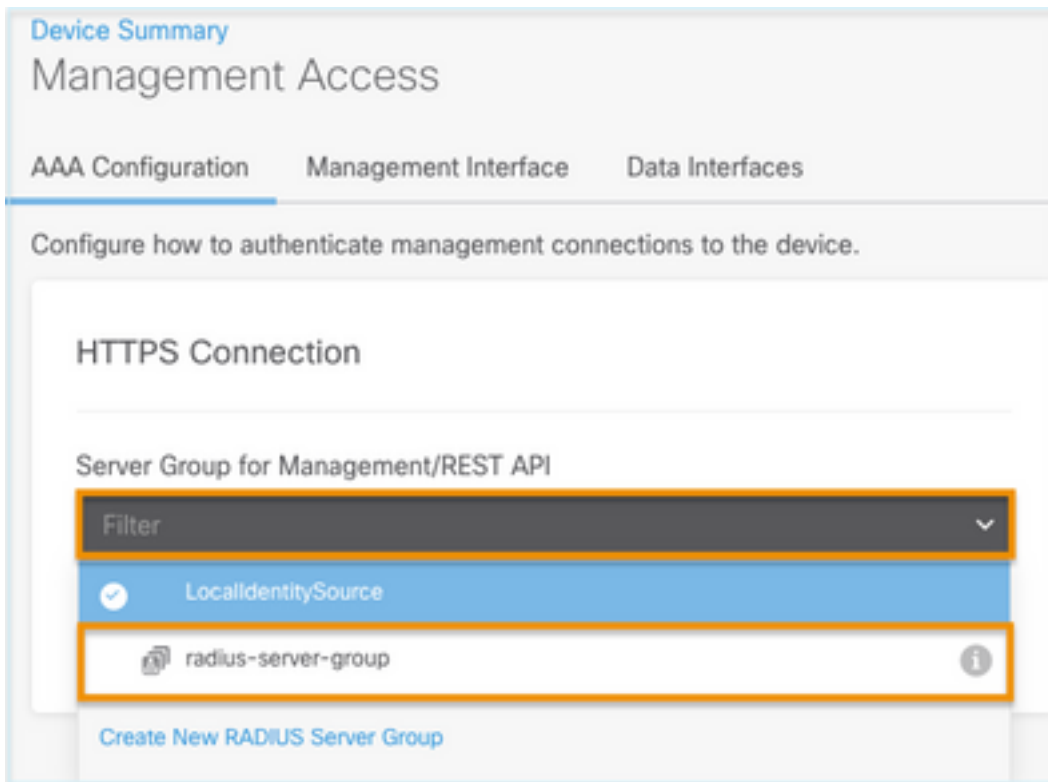
RA VPN Only (if this object is used in RA VPN Configuration)

TEST CANCEL OK

**Etapas 4.** Adicionar servidor RADIUS ao grupo de servidores RADIUS



**Etapa 5.** Selecionar grupo criado como Grupo de Servidores para Gerenciamento



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

## Etapa 6. Salve a configuração

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

## Configuração do ISE

Etapa 1. Ícone Navegar até três linhas  localizado no canto superior esquerdo e selecione Administration > Network Resources > Network Devices



## Network Devices

Default Device

Device Security Settings

## Network Devices

[Edit](#) [+ Add](#) [Duplicate](#) [Import](#) [Export](#) [Generate PAC](#) [Delete](#)

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

**Etapa 2. Selecione o botão +Add** e defina Network Access Device Name e IPAddress, depois marque a caixa de seleção RADIUS e defina um segredo compartilhado. Selecionar ao **Enviar**

## Network Devices

Default Device

Device Security Settings

## Network Devices

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](#)

Administration - Network Resources

Network Devices

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

Network Devices

Default Device

Device Security Settings

### Network Devices

Selected 0 Total 1

Edit + Add Duplicate Import Export Generate PAC Delete

Name	IP/Mask	Profile Name	Location	Type	Description
FDM	10.122.111...	Cisco	All Locations	All Device Types	

**Etapa 3.** Ícone Navegar até três linhas  localizado no canto superior esquerdo e selecione em **Administration > Identity Management > Groups**

Administration - Identity Management

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

### Identity Groups

EQ

< [Grid Icon] [Settings Icon]

- > Endpoint Identity Groups
- > **User Identity Groups**

### User Identity Groups

Edit + Add Delete Import Export

Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/> Employee	Default Employee User Group
<input type="checkbox"/> GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
<input type="checkbox"/> GuestType_Contractor (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Daily (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_SocialLogin (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Weekly (default)	Identity group mirroring the guest type
<input type="checkbox"/> OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

**Etapa 4.** Selecione em **User Identity Groups** e selecione no botão **+Add**. Defina um nome e selecione **Enviar**

Cisco ISE Administration - Identity Management

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

Identity Groups

User 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

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

Identity Groups

User Identity Groups > New User Identity Group

Identity Group

\* Name FDM\_ReadOnly

Description

Submit Cancel

**Observação:** Neste exemplo, os grupos FDM\_Admin e FDM\_ReadOnly Identity criados, você pode repetir a Etapa 4 para cada tipo de Usuários Admin usados no FDM.

**Etapa 5.** Navegue até o ícone de três linhas localizado no canto superior esquerdo e selecione **Administração > Gerenciamento de identidades > Identidades**. Selecione em **+Add**, defina o nome de usuário e a senha e, em seguida, selecione o grupo ao qual o usuário pertence. Neste exemplo, os usuários `fdm_admin` e `fdm_readonly` foram criados e atribuídos aos grupos `FDM_Admin` e `FDM_ReadOnly`, respectivamente.

Cisco ISE Administration - Identity Management

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

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

Latest Manual Network Scan Res...

Network Access Users

Selected 0 Total 2

Edit Add Change Status Import Export Delete Duplicate

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	

**Etapa 6.** Selecione o ícone de três linhas localizado no canto superior esquerdo e navegue para **Política > Elementos de política > Resultados > Autorização > Perfis de autorização**, selecione **+Adicionar**, defina um nome para o **Perfil de autorização**. Selecione **Radius Service-type** e selecione **Administrative**, em seguida, selecione **Cisco-av-pair** e cole a função que o usuário admin recebe, neste caso, o usuário recebe um privilégio admin total (fdm.userrole.authority.admin). Selecione **Enviar**. Repita esta etapa para cada função, usuário somente leitura configurado como outro exemplo neste 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

The screenshot shows two attribute assignments in a list:

- Attribute: Radius:Service-Type, Value: NAS Prompt
- Attribute: Cisco:cisco-av-pair, Value: fdm.userrole.authority.ro


## Attributes Details

The screenshot displays the following attribute details:

- Access Type = ACCESS\_ACCEPT
- Service-Type = 7
- cisco-av-pair = fdm.userrole.authority.ro

**Observação:** certifique-se de que a ordem da seção Atributos avançados seja a mesma do exemplo de imagens para evitar resultados inesperados ao fazer login com a GUI e a CLI.

**Etapa 8.** Selecione o ícone de três linhas e navegue para Política > Conjuntos de políticas.

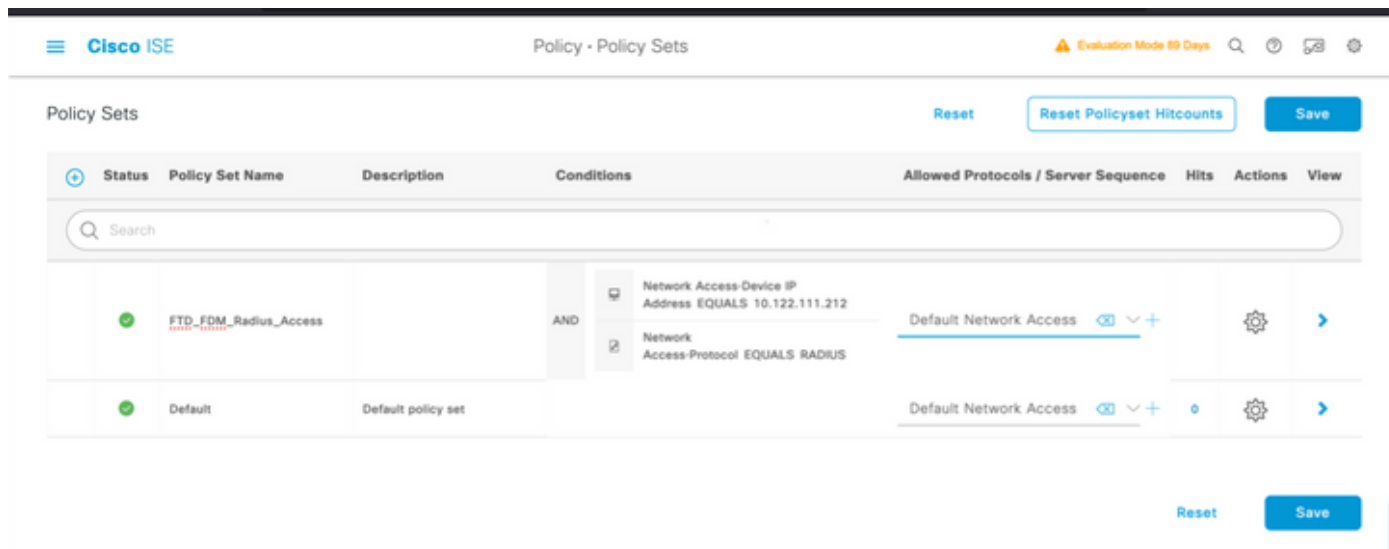
Selecione em  localizado abaixo do título Conjuntos de políticas, defina um nome e selecione no botão + no meio para adicionar uma nova condição.

**Etapa 9.** Na janela Condição, selecione para adicionar um atributo e, em seguida, selecione no ícone **Network Device** seguido pelo endereço IP do dispositivo de acesso à rede. Selecione **Valor do Atributo** e adicione o endereço IP do FDM. Adicione uma nova condição e selecione **Network Access** seguido pela opção Protocol, selecione on **RADIUS** e selecione on Use once done.


The screenshot shows the Cisco ISE Policy Sets configuration page. The table below represents the data visible in the interface:

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	<u>FTD_FDM_Radius_Access</u>		AND Network Access-Device IP Address EQUALS 10.122.111.212 Network Access-Protocol EQUALS RADIUS	Default Network Access	0		
	Default	Default policy set		Default Network Access	0		

Etapa 10. Na seção permitir protocolos, selecione **Device Default Admin**. Selecionar ao **Salvar**




Etapa 11. Selecione na seta para a direita  ícone do Conjunto de políticas para definir políticas de autenticação e autorização

Etapa 12. Selecionar em  localizado abaixo do título Authentication Policy (Política de autenticação), defina um nome e selecione no sinal + no meio para adicionar uma nova condição. Na janela Condição, selecione para adicionar um atributo e, em seguida, selecione no ícone Network Device seguido pelo endereço IP do dispositivo de acesso à rede. Selecione em Valor do Atributo e adicione o endereço IP do FDM. Selecione em Uso depois de concluído

Etapa 13. Selecione Internal Users como o Identity Store e selecione on Save



**Observação:** o Repositório de identidades poderá ser alterado para o repositório do AD se o ISE ingressar em um Active Directory.

Etapa 14. Selecionar em  localizado abaixo do título Política de autorização, defina um nome e selecione no sinal + no meio para adicionar uma nova condição. Na janela Condição, selecione para adicionar um atributo e, em seguida, selecione no ícone Grupo de identidades seguido por Usuário interno:Grupo de identidades. Selecione o Grupo FDM\_Admin, selecione a opção AND juntamente com NEW para adicionar uma nova condição, selecione o ícone de porta seguido por RADIUS NAS-Port-Type:Virtual e selecione em Usar.

# Conditions Studio

## Library

Search by Name



- BYOD\_is\_Registered
- Catalyst\_Switch\_Local\_Web\_Authentication
- Compliance\_Unknown\_Devices
- Compliant\_Devices
- EAP-MSCHAPv2

## Editor

IdentityGroup-Name  
Equals User Identity Groups:FDM\_admin

Radius-NAS-Port-Type  
Equals Virtual

AND

NEW AND OR

Set to 'Is not'

Duplicate Save

Etapa 15. Em Perfis, selecione o perfil criado na Etapa 6 e, em seguida, selecione em Salvar

Repita as Etapas 14 e 15 para o grupo FDM\_ReadOnly

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

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

Etapa 16 (opcional). Navegue até o ícone de três linhas localizado no canto superior esquerdo e selecione Administration > System > Maintenance > Repository e selecione on +Add para adicionar um repositório usado para armazenar o arquivo de despejo TCP para fins de solução de problemas.

Etapa 17 (opcional). Defina um Nome de repositório, protocolo, Nome do servidor, caminho e Credenciais. Selecione Enviar quando terminar.



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

\* Protocol

Location

\* Server Name

\* Path

Credentials

\* User Name

\* Password

## Verificar

Etapa 1. Navegue até a guia **Objetos > Fontes de identidade** e verifique a configuração do servidor RADIUS e do servidor de grupo

Monitoring Policies **Objects** Device

### 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

Etapa 2. Navegue até **Device > System Settings > Management Access** e selecione o botão **TEST**

The screenshot shows the Cisco SD-WAN configuration interface. At the top, there are navigation tabs: Monitoring, Policies, Objects, and Device (highlighted with a blue box and labeled '1'). On the left, there is a 'System Settings' sidebar with 'Management Access' highlighted (labeled '2'). The main content area is titled 'Device Summary Management Access' (labeled '3') and has three sub-tabs: 'AAA Configuration' (highlighted with a blue box and labeled '3'), 'Management Interface', and 'Data Interfaces'. Below the sub-tabs, there is a heading 'HTTPS Connection' and a section for 'Server Group for Management/REST API'. A blue information box contains text about RADIUS server configuration. Below this, there is a dropdown menu set to 'radius-server-group' and a green 'TEST' button (highlighted with a blue box and labeled '4'). Underneath, there is a section for 'Authentication with LOCAL' with a dropdown menu set to 'Before External Server'. At the bottom of the configuration area is a blue 'SAVE' button.

Etapa 3. Insira as credenciais do usuário e selecione o botão 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.*

**Etapa 4.** Abra um novo navegador de janela e digite <https://FDM ip Address>, use o nome de usuário e a senha `fdm_admin` criados na etapa 5 da seção de configuração do ISE.



# Firepower Device Manager

**Successfully logged out**

fdm\_admin

.....|

LOG IN

A tentativa de login bem-sucedida pode ser verificada nos logs ao vivo do ISE RADIUS

Cisco ISE Operations - RADIUS Evaluation Mode 79 Days

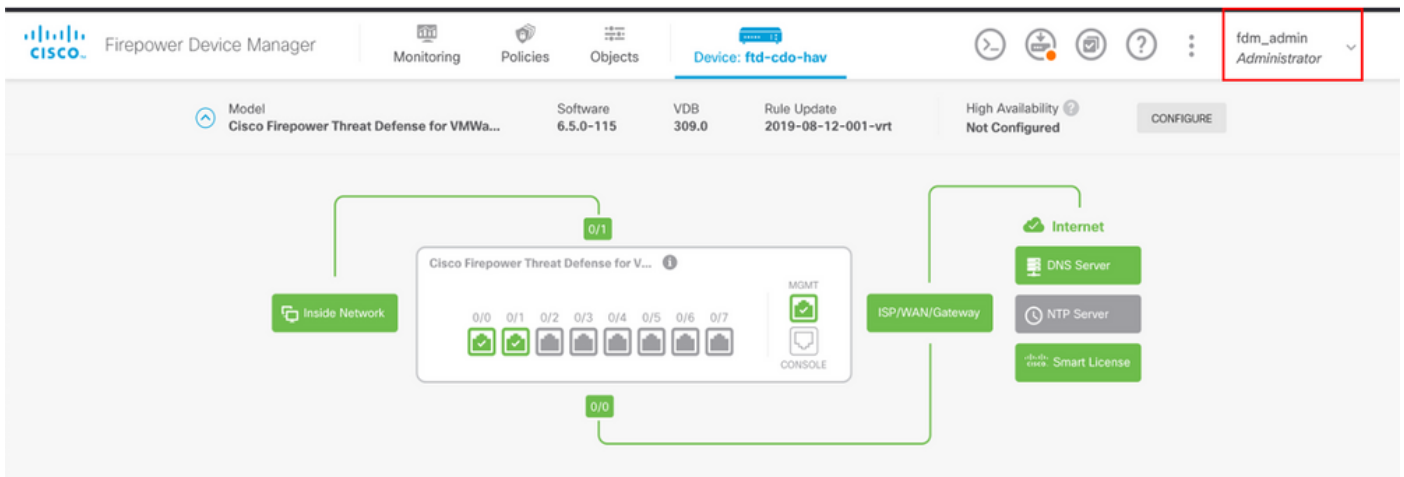
Live Logs Live Sessions Click here to do visibility setup Do not show this again.

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

O Usuário Administrador também pode ser revisado no FDM no canto superior direito



## CLI do Cisco Firepower Device Manager (usuário 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 seção fornece as informações que você pode usar para solucionar problemas da sua configuração.

### Validação de comunicação com a ferramenta TCP Dump no ISE

**Etapa 1.** Faça login no ISE e selecione o ícone de três linhas localizado no canto superior esquerdo e navegue para **Operações > Solução de problemas > Ferramentas de diagnóstico.**

**Etapa 2.** Em General tools (Ferramentas gerais), selecione on TCP Dumps (Despejos TCP) e, em seguida, selecione **Add+**. Selecione Nome do Host, Nome do Arquivo da Interface de Rede, Repositório e, opcionalmente, um filtro para coletar apenas o fluxo de comunicação do endereço IP do FDM. Selecionar ao **Salvar e Executar**

The screenshot shows the Cisco ISE web interface. The top navigation bar includes the Cisco ISE logo and tabs for 'Diagnostic Tools', 'Download Logs', and 'Debug Wizard'. The left sidebar is expanded to show 'General Tools', with 'TCP Dump' selected. The main content area is titled 'TCP Dump > New' and contains the 'Add TCP Dump' configuration form. The form includes the following fields and values:

- Host Name:** ise31
- Network Interface:** GigabitEthernet 0 [Up, Running]
- Filter:** ip host 10.122.111.212
- File Name:** FDM\_Tshoot
- Repository:** VM
- File Size:** 10 Mb
- Limit to:** 1 File(s)
- Time Limit:** 5 Minute(s)
- Promiscuous Mode:**

**Etapa 3.** Faça login na interface do usuário do FDM e digite as credenciais de administrador.

**Etapa 4.** No ISE, selecione o botão **Stop** e verifique se o arquivo pcap foi enviado para o repositório 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 >> / 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.cisco.se.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

Etapa 5. Abra o arquivo pcap para validar a comunicação bem-sucedida 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..

```

Se nenhuma entrada for mostrada no arquivo pcap, valide as próximas opções:

1. O endereço IP correto do ISE foi adicionado à configuração do FDM
2. No caso de um firewall estar no meio, verifique se a porta 1812-1813 é permitida.
3. Verificar a comunicação entre o ISE e o FDM

#### Validação de comunicação com arquivo gerado pelo FDM.

No arquivo de solução de problemas gerado na página Dispositivo do FDM, procure as palavras-chave:

- FdmPasswordLoginHelper
- NGFWDefaultUserMgmt
- GerentedeStatusdeOrigemdIdentidadeAAIA
- GerenciadorDeOrigemDIdentidadeRadius

Todos os logs relacionados a esse recurso podem ser encontrados em /var/log/cisco/ngfw-onbox.log

Referências:

[https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd-fdm-mgmt.html#id\\_73793](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 comuns

## Caso 1 - Autenticação externa não funcionando

- Verifique secretKey, porta ou nome do host
- Configuração incorreta de AVPs no RADIUS
- O servidor pode estar em "Dead Time"

## Caso 2 - Falha no teste do IdentitySource

- Verifique se as alterações feitas no objeto foram salvas
- Verifique se as credenciais estão corretas

# Limitações

- O FDM permite no máximo 5 sessões ativas do FDM.
- A criação da 6ª sessão resulta na 1ª sessão revogada
- O nome de RadiusIdentitySourceGroup não pode ser "LocalIdentitySource"
- Máximo de 16 RadiusIdentitySources para um RadiusIdentitySourceGroup
- A configuração incorreta de AVPs no RADIUS resulta na negação de acesso ao FDM

# Perguntas e respostas

P: Esse recurso funciona no modo de avaliação?

R: Sim

P: Se dois usuários somente leitura fizerem login, onde tiverem acesso ao usuário somente leitura 1, e fizerem login de dois navegadores diferentes. Como ele será exibido? O que acontecerá?

R: As duas sessões do usuário são mostradas na página de sessões do usuário ativo com o mesmo nome. Cada entrada mostra um valor individual para o carimbo de data/hora.

P: Qual é o comportamento do servidor radius externo que fornece uma rejeição de acesso vs. "no response" (sem resposta) se você tiver configurado a autenticação local em segundo lugar?

R: Você pode tentar a autenticação LOCAL mesmo se obtiver a rejeição do Access ou nenhuma resposta se tiver a autenticação local configurada em segundo lugar.

P: Como o ISE diferencia uma solicitação RADIUS para login de administrador em relação à solicitação RADIUS para autenticar um usuário de VPN RA

R: O ISE não diferencia uma solicitação RADIUS para usuários Admin X RAVPN. O FDM procura o atributo cisco-avpair para descobrir a Autorização para acesso de Administrador. O ISE envia todos os atributos configurados para o usuário em ambos os casos.

P: Isso significa que os logs do ISE não podem diferenciar entre um log de administrador do FDM e o mesmo usuário que está acessando a VPN de acesso remoto no mesmo dispositivo. Há algum atributo RADIUS passado para o ISE na solicitação de acesso que o ISE pode digitar?

R: A seguir estão os atributos RADIUS de upstream que são enviados do FTD para o ISE durante a autenticação RADIUS para RAVPN. Eles não são enviados como parte da Solicitação de Acesso de Gerenciamento de Autenticação Externa e podem ser usados para diferenciar um log de administração do FDM no log de usuário do Vs RAVPN.

146 - Nome do grupo de túneis ou nome do perfil de conexão.

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

151 - Tipo de sessão (Valores aplicáveis: 1 = AnyConnect Client SSL VPN, 2 = AnyConnect Client IPsec VPN (IKEv2).

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.