

# Configurazione dell'autenticazione e dell'autorizzazione esterne di FDM con ISE utilizzando RADIUS

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Interoperabilità](#)

[Licenze](#)

[Premesse](#)

[Esempio di rete](#)

[Configurazione](#)

[Configurazione di FDM](#)

[Configurazione di ISE](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Problemi comuni](#)

[Limitazioni](#)

[Domande e risposte](#)

## Introduzione

In questo documento viene descritta la procedura per integrare Cisco Firepower Device Manager (FDM) con Identity Services Engine (ISE) per autenticare gli utenti amministratori con il protocollo RADIUS per l'accesso GUI e CLI.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Firepower Device Manager (FDM)
- Identity Services Engine (ISE)
- protocollo RADIUS

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Dispositivo Firepower Threat Defense (FTD), tutte le piattaforme Firepower Device Manager

(FDM) versione 6.3.0+

- ISE versione 3.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Interoperabilità

- Server RADIUS con utenti configurati con ruoli utente
- I ruoli utente devono essere configurati sul server RADIUS con cisco-av-pair
- Cisco-av-pair = fdm.userrole.authority.admin
- ISE può essere utilizzato come server RADIUS

## Licenze

Nessuna licenza specifica richiesta, la licenza di base è sufficiente

## Premesse

Questa funzionalità consente agli utenti di configurare l'autenticazione esterna con RADIUS e più ruoli utente per tali utenti.

Supporto RADIUS per Management Access con 3 ruoli utente definiti dal sistema:

- SOLA\_LETTURA
- READ\_WRITE (impossibile eseguire azioni critiche del sistema come l'aggiornamento, il ripristino e così via)
- ADMIN

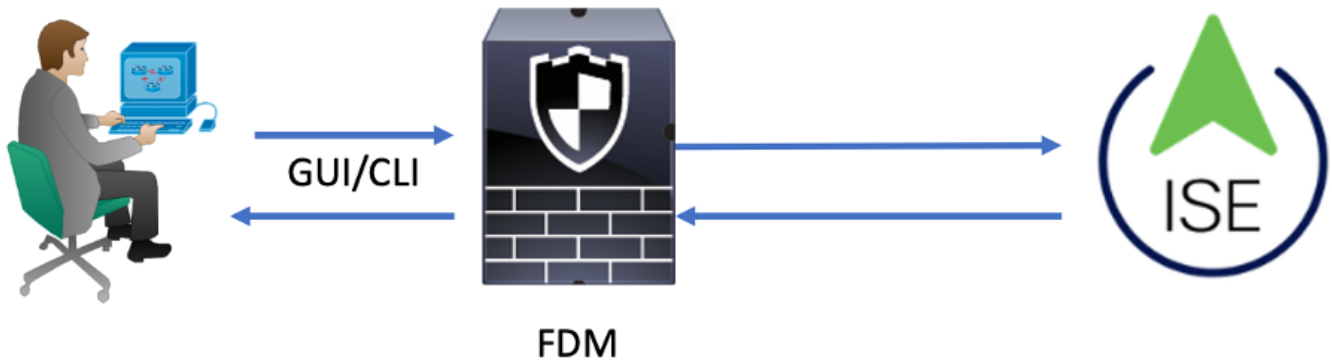
È possibile testare la configurazione del server RADIUS, monitorare le sessioni utente attive ed eliminare una sessione utente.

La funzionalità è stata implementata in FDM versione 6.3.0. Prima della release 6.3.0, FDM era in grado di supportare un solo utente (amministratore).

Per impostazione predefinita, Cisco Firepower Device Manager autentica e autorizza gli utenti in locale, in modo da disporre di un metodo di autenticazione e autorizzazione centralizzato e da poter utilizzare Cisco Identity Service Engine tramite il protocollo RADIUS.

## Esempio di rete

Nell'immagine seguente viene illustrato un esempio di topologia di rete



Processo:

1. L'utente Admin introduce le proprie credenziali.
2. Processo di autenticazione attivato e ISE convalida le credenziali localmente o tramite Active Directory.
3. Una volta completata l'autenticazione, ISE invia un pacchetto Permit per le informazioni di autenticazione e autorizzazione a FDM.
4. L'account viene eseguito su ISE e l'autenticazione viene eseguita correttamente dal vivo.

## Configurazione

### Configurazione di FDM

Passaggio 1. Accedere a FDM e selezionare Dispositivo > Impostazioni di sistema > scheda Accesso gestione

Passaggio 2. Crea nuovo gruppo di server RADIUS

The screenshot displays the Cisco Meraki management console interface. 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 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 by a red box and labeled '4'. This section contains a 'Filter' dropdown menu with 'LocalIdentitySource' selected. At the bottom, a button labeled 'Create New RADIUS Server Group' is highlighted with a red box and labeled '5'.

**Passaggio 3.** Crea nuovo server 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

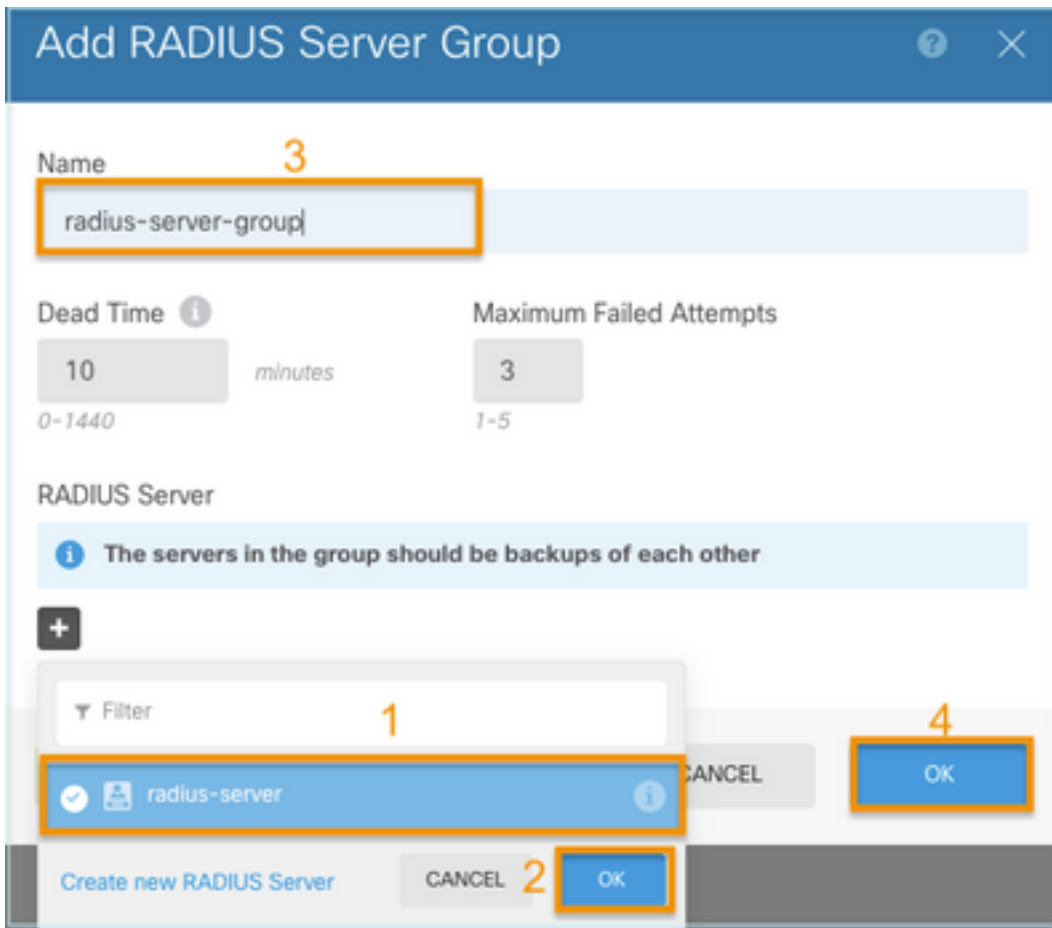
Server Secret Key

●●●●●●●●

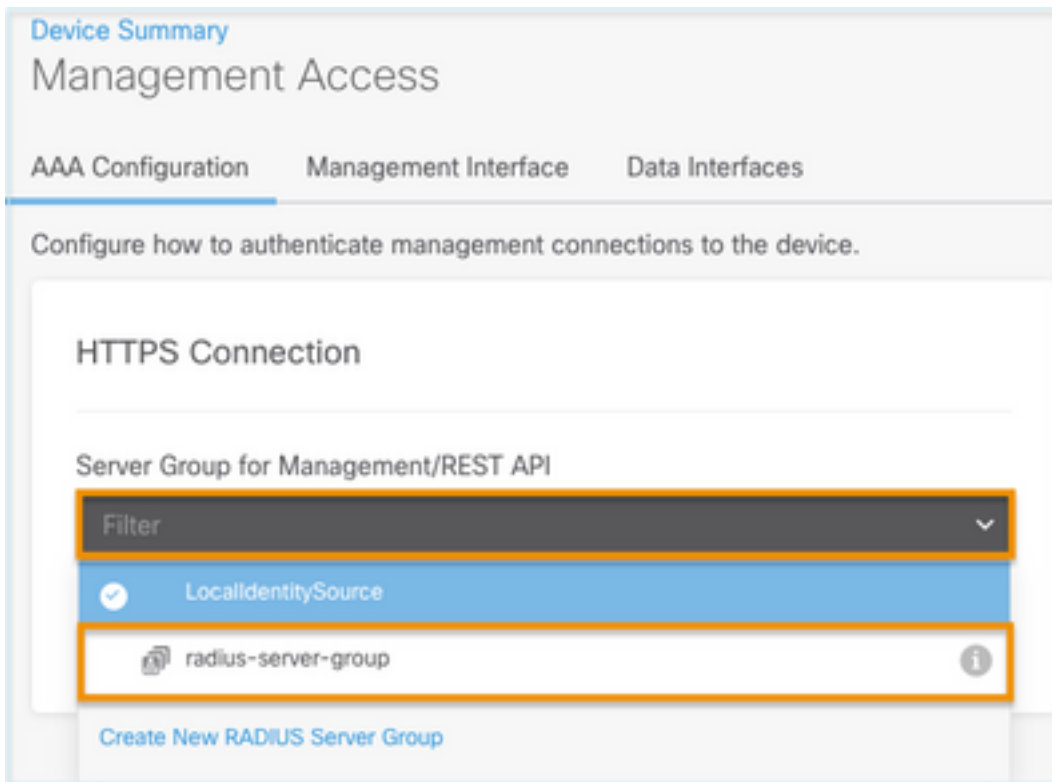
RA VPN Only (if this object is used in RA VPN Configuration)

TEST CANCEL OK

**Passaggio 4.** Aggiungi server RADIUS al gruppo di server RADIUS



Passaggio 5. Selezionare il gruppo creato come gruppo di server per la gestione



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**

## Passaggio 6. Salvare la configurazione

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**

## Configurazione di ISE

Passaggio 1. Icona tre righe  nell'angolo superiore sinistro e selezionare **Amministrazione > Risorse di rete > Dispositivi di rete**



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
------	---------	--------------	----------	------	-------------

**Passaggio 2.** Selezionare il pulsante **+Aggiungi** e definire Nome dispositivo di accesso alla rete e Indirizzo IP, quindi selezionare la casella di controllo RADIUS e definire un segreto condiviso. Seleziona all'invio

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

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](#)

Network Devices

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

Passaggio 3. Icona tre righe  nell'angolo superiore sinistro e selezionare **Amministrazione > Gestione delle identità > Gruppi**

User Identity Groups

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

Passaggio 4. Selezionare Gruppi identità utente e fare clic sul pulsante **+Aggiungi**. Definire un nome e selezionarlo in **Invia**

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:** in questo esempio, sono stati creati i gruppi di identità FDM\_Admin e FDM\_ReadOnly, è possibile ripetere il passo 4 per ogni tipo di utente Admin utilizzato in FDM.

**Passaggio 5.** Passare all'icona a tre linee situata nell'angolo superiore sinistro e selezionare **Amministrazione > Gestione delle identità > Identità**. Selezionare **+Aggiungi** e definire nome utente e password, quindi selezionare il gruppo a cui appartiene l'utente. In questo esempio, gli utenti `fdm_admin` e `fdm_readonly` sono stati creati e assegnati rispettivamente ai gruppi `FDM_Admin` e `FDM_ReadOnly`.

Cisco ISE Administration - Identity Management Evaluation Mode 89 Days

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 Evaluation Mode 89 Days

Identities Groups External Identity Sources Identity Source Sequences Settings

Users Latest Manual Network Scan Res...

Network Access Users

Selected 0 Total 2

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

**Passaggio 6.** Selezionare l'icona a tre righe nell'angolo superiore sinistro e selezionare **Criterio > Elementi criterio > Risultati > Autorizzazione > Profili di autorizzazione**, selezionare **+Aggiungi**, definire un nome per il **Profilo di autorizzazione**. Selezionare **Radius Service-type** e **Amministrativo**, quindi selezionare **Cisco-av-pair** e incollare il ruolo che l'utente amministratore ottiene, in questo caso, l'utente riceve un privilegio di amministratore completo (fdm.userrole.authority.admin). Selezionare **Invia**. Ripetere questo passaggio per ogni ruolo, utente di sola lettura configurato come un altro esempio in questo documento.

Dictionarys 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

⋮	<u>Radius:Service-Type</u> ▾	=	<u>Administrative</u> ▾	⊖
⋮	<u>Cisco:cisco-av-pair</u> ▾	=	<u>fdm.userrole.authority.admin </u> ▾	⊖ ⊕










### Attributes Details

Access Type = ACCESS\_ACCEPT

Service-Type = 6

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

## Advanced Attributes Settings

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

## Attributes Details

Access Type = ACCESS\_ACCEPT

Service-Type = 7

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

**Nota:** assicurarsi che l'ordine della sezione Advance Attributes sia quello dell'esempio di immagini per evitare risultati imprevisti quando si esegue il login con GUI e CLI.

**Passaggio 8.** Selezionare l'icona a tre righe e passare a Criterio > Set di criteri. Seleziona su

 situato sotto il titolo Set di criteri, definire un nome e selezionare il pulsante + al centro per aggiungere una nuova condizione.


**Passaggio 9.** Nella finestra Condizione, selezionare per aggiungere un attributo, quindi **selezionare** Icona periferica di rete seguito da Indirizzo IP periferica di accesso alla rete. Selezionare **Valore attributo** e aggiungere l'indirizzo IP di FDM. Aggiungere una nuova condizione e selezionare **Accesso rete** seguito da Protocollo, selezionare **RADIUS** e selezionare Usa al termine.

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	FTD_FDM_Radius_Access		AND <ul style="list-style-type: none"> <li>Network Access-Device IP Address EQUALS 10.122.111.212</li> <li>Network Access-Protocol EQUALS RADIUS</li> </ul>	Default Network Access [v] +		[gear] [arrow]	
●	Default	Default policy set		Default Network Access [v] +	0	[gear] [arrow]	

Passaggio 10. Nella sezione Consenti protocolli selezionare **Amministratore predefinito dispositivo**. Seleziona al **salvataggio**


Passaggio 11. Fare clic sulla freccia destra  icona del set di criteri per la definizione dei criteri di autenticazione e autorizzazione

Passaggio 12. Seleziona su  situato sotto il titolo del criterio di autenticazione, definire un nome e selezionare il segno + al centro per aggiungere una nuova condizione. Nella finestra Condizione, selezionare per aggiungere un attributo, quindi fare clic su Icona Periferica di rete seguita da Indirizzo IP periferica di accesso alla rete. Selezionare Valore attributo e aggiungere l'indirizzo IP di FDM. Selezionare una volta utilizzato

Passaggio 13. Selezionare Utenti interni come archivio identità e selezionare Salva

Status	Rule Name	Conditions	Use	Hits	Actions
<span style="color: green;">●</span>	FDM_Users	Network Access-Device IP Address EQUALS 10.122.111.212	Internal Users		
			> Options		

**Nota:** l'archivio identità può essere modificato in archivio Active Directory se ISE viene aggiunto a un Active Directory.

Passaggio 14. Seleziona su  situato sotto il titolo del criterio di autorizzazione, definire un nome e selezionare il segno + al centro per aggiungere una nuova condizione. Nella finestra Condizione, selezionare per aggiungere un attributo, quindi selezionare l'icona Gruppo di identità seguita da Utente interno: Gruppo di identità. Selezionare il gruppo FDM\_Admin, selezionare l'opzione AND insieme all'opzione NEW per aggiungere una nuova condizione, selezionare l'icona della porta seguita da RADIUS NAS-Port-Type:Virtual e selezionare l'opzione Use.

## 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

Passaggio 15. In Profili, selezionare il profilo creato al punto 6, quindi scegliere Salva

Ripetere i passaggi 14 e 15 per il gruppo FDM\_ReadOnly



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

			Results			
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 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	⚙️

**Passaggio 16 (facoltativo).** Passare all'icona a tre righe nell'angolo superiore sinistro e selezionare Amministrazione > Sistema > Manutenzione > Repository e selezionare +Aggiungi per aggiungere un repository utilizzato per memorizzare il file di dump TCP per la risoluzione dei problemi.

**Passaggio 17 (facoltativo).** Definire un nome repository, un protocollo, un nome server, un percorso e le credenziali. Al termine, selezionare Invia.

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 .....

## Verifica

**Passaggio 1.** Passare a Oggetti > scheda Origini identità e verificare la configurazione del server e del server RADIUS

The screenshot shows the Cisco configuration interface. The top navigation bar includes 'Monitoring', 'Policies', 'Objects' (highlighted with an orange box), and 'Device'. The left sidebar lists 'Object Types' such as Networks, Ports, Security Zones, Application Filters, URLs, Geolocations, Syslog Servers, IKE Policies, IPSec Proposals, Identity Sources (highlighted with an orange box), and Users. The main content area is titled 'Identity Sources' and shows '3 objects' in a table:

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

Passaggio 2. Selezionare Periferica > Impostazioni di sistema > Scheda Accesso gestione e selezionare il pulsante TEST

The screenshot shows the Cisco configuration interface for 'Device' (highlighted with an orange box and '1'). The left sidebar shows 'System Settings' (highlighted with an orange box and '2') with 'Management Access' selected. The main content area is titled 'Device Summary Management Access' (highlighted with an orange box and '3'). Below this, 'AAA Configuration' is selected (highlighted with an orange box). The configuration page is titled 'Configure how to authenticate management connections to the device.' and shows the 'HTTPS Connection' section. A message states: 'To use a RADIUS server successfully, you must configure the RADIUS user accounts with the required authorization values, as described in the help.' Below this, a dropdown menu is set to 'radius-server-group' and a green 'TEST' button (highlighted with an orange box and '4') is visible. Other options include 'Authentication with LOCAL' set to 'Before External Server' and a 'SAVE' button.

Passaggio 3. Inserire le credenziali utente e selezionare il pulsante 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.*

**Passaggio 4.** Aprire una nuova finestra del browser e digitare <https://FDM ip Address>, utilizzare il nome utente e la password `fdm_admin` creati nel passaggio 5 della sezione di configurazione ISE.



# Firepower Device Manager

**Successfully logged out**

fdm\_admin

.....|

LOG IN

È possibile verificare l'esito positivo del tentativo di accesso ai log live di ISE RADIUS

Cisco ISE Operations - RADIUS Evaluation Mode 79 Days

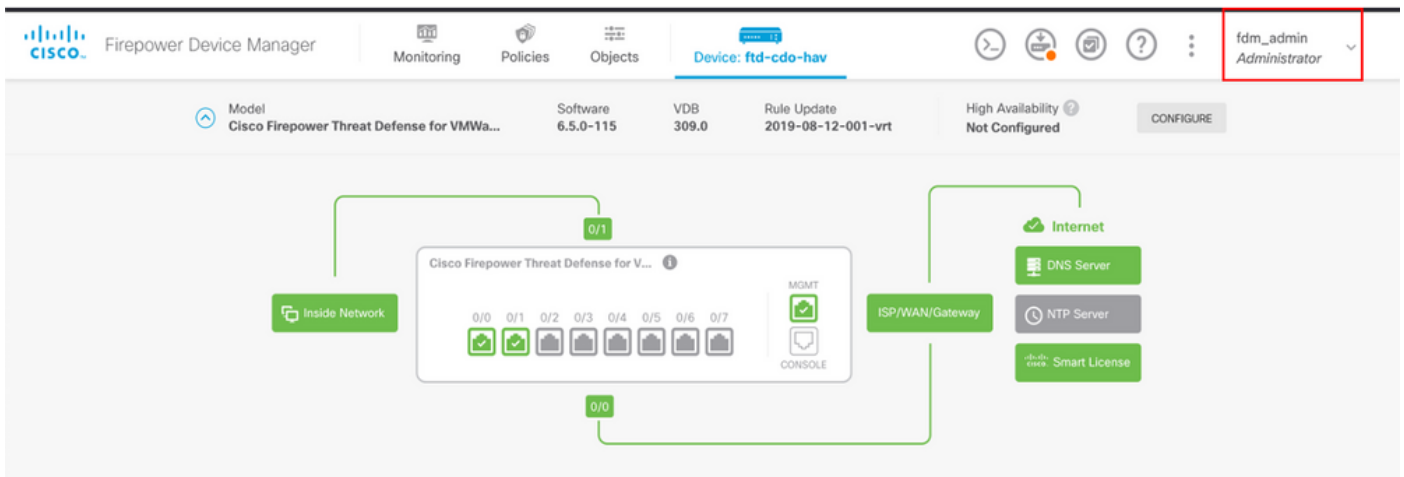
Live Logs Live Sessions

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

L'utente amministratore può anche essere rivisto su FDM nell'angolo superiore destro



## Cisco Firepower Device Manager CLI (utente amministratore)

```
[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)

[> █
```

## Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Convalida della comunicazione con lo strumento TCP Dump su ISE

**Passaggio 1.** Effettuare il login ad ISE, selezionare l'icona a tre linee situata nell'angolo superiore sinistro, quindi selezionare **Operations > Troubleshoot > Diagnostic Tools** (Operazioni > Risoluzione dei problemi > Strumenti diagnostici).

**Passaggio 2.** In Strumenti generali selezionare su Dump TCP e quindi fare clic su **Aggiungi+**. Selezionare Nome host, Nome file interfaccia di rete, Repository e, facoltativamente, un filtro per raccogliere solo il flusso di comunicazione dell'indirizzo IP di FDM. Selezionare **Salva ed esegui**

The screenshot shows the Cisco ISE web interface. The top navigation bar includes the Cisco ISE logo and the 'Diagnostic Tools' menu, which is expanded to show 'Download Logs' and 'Debug Wizard'. The left sidebar contains a tree view with 'General Tools' (expanded to show 'TCP Dump'), 'TrustSec Tools', and 'Session Trace Tests'. The main content area is titled 'TCP Dump > New' and contains the 'Add TCP Dump' form. The form fields are: '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)), and a 'Promiscuous Mode' checkbox.

**Diagnostic Tools**   Download Logs   Debug Wizard

**General Tools** ▾

- RADIUS Authentication Troubl...
- Execute Network Device Com...
- Evaluate Configuration Validat...
- Posture Troubleshooting
- Agentless Posture Troublesho...
- EndPoint Debug

**TCP Dump**

Session Trace Tests

**TrustSec Tools** >

**TCP Dump > New**

**Add TCP Dump**

Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.

Host Name \*  
ise31

Network Interface \*  
GigabitEthernet 0 [Up, Running]

Filter  
ip host 10.122.111.212

E.g: ip host 10.77.122.123 and not 10.177.122.119

File Name  
FDM\_Tshoot

Repository  
VM

File Size  
10 Mb

Limit to  
1 File(s)

Time Limit  
5 Minute(s)

Promiscuous Mode

**Passaggio 3.** Accedere all'interfaccia utente di FDM e digitare le credenziali dell'amministratore.

**Passaggio 4.** In ISE, selezionare il pulsante **Stop** e verificare che il file pcap sia stato inviato al repository definito.

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.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

**Passaggio 5.** Aprire il file pcap per verificare la corretta comunicazione tra 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)
v 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 nel file pcap non sono visualizzate voci, convalidare le opzioni successive:

1. L'indirizzo IP ISE destro è stato aggiunto alla configurazione FDM
2. Se al centro si trova un firewall, verificare che la porta 1812-1813 sia autorizzata.
3. Controllare la comunicazione tra ISE e FDM

**Convalida della comunicazione con il file generato da FDM.**

Nella pagina Risoluzione dei problemi relativi ai file generati dal dispositivo FDM cercare le parole chiave:

- HelperAccessoPasswordFdm
- NGFWDefaultUserMgmt
- GestoreStatoOrigineAAAA
- GestioneOriginiIdentitàRadius

Tutti i log relativi a questa funzione sono disponibili in /var/log/cisco/ngfw-onbox.log

Riferimenti:

[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)



# Problemi comuni

## Caso 1 - Autenticazione esterna non funzionante

- Verifica secretKey, port o hostname
- Configurazione errata di AVP su RADIUS
- Il server può trovarsi in un "tempo di inattività"

## Caso 2 - Test IdentitySource non riuscito

- Assicurarsi che le modifiche apportate all'oggetto siano state salvate
- Verificare che le credenziali siano corrette

# Limitazioni

- FDM consente un massimo di 5 sessioni FDM attive.
- La creazione dei risultati della 6a sessione nella 1a sessione è stata revocata
- Il nome di RadiusIdentitySourceGroup non può essere "LocalIdentitySource"
- Massimo 16 RadiusIdentitySources in un RadiusIdentitySourceGroup
- Una configurazione errata degli AVP su RADIUS comporta il rifiuto dell'accesso a FDM

# Domande e risposte

D: Questa funzione funziona in modalità di valutazione?

R: Sì

D: Se due utenti di sola lettura eseguono l'accesso, dove hanno accesso all'utente di sola lettura 1, e accedono da due browser diff. Come si presenterà? Cosa succederà?

R: Le sessioni di entrambi gli utenti vengono visualizzate nella pagina Sessioni utente attive con lo stesso nome. Ogni voce mostra un singolo valore per il timestamp.

D: Qual è il comportamento del server RADIUS esterno in caso di rifiuto di accesso rispetto a "nessuna risposta" se l'autenticazione locale è stata configurata per il secondo?

R: È possibile provare l'autenticazione LOCALE anche se si ottiene il rifiuto di Access o nessuna risposta se l'autenticazione locale è stata configurata per seconda.

D. In che modo ISE differenzia una richiesta RADIUS per l'accesso amministratore da una richiesta RADIUS per l'autenticazione di un utente VPN RA

R: ISE non distingue una richiesta RADIUS per gli utenti Admin da RAVPN. FDM analizza l'attributo cisco-avpair per stabilire come autorizzare l'accesso amministratore. ISE invia tutti gli attributi configurati per l'utente in entrambi i casi.

D: Ciò significa che i log ISE non sono in grado di distinguere tra un accesso amministratore FDM e lo stesso utente che accede alla VPN ad accesso remoto sullo stesso dispositivo. Esiste un attributo RADIUS passato ad ISE nella richiesta di accesso su cui ISE può scrivere la chiave?

R: Di seguito sono riportati gli attributi RADIUS upstream inviati da FTD ad ISE durante l'autenticazione RADIUS per RAVPN. Questi non vengono inviati come parte della richiesta di accesso alla gestione dell'autenticazione esterna e possono essere utilizzati per differenziare un log di amministrazione FDM in rispetto al login utente RAVPN.

146 - Nome gruppo tunnel o nome profilo connessione.

150 - Tipo di client (valori applicabili: 2 = AnyConnect Client SSL VPN, 6 = AnyConnect Client IPsec VPN (IKEv2)).

151 - Tipo di sessione (valori applicabili: 1 = AnyConnect Client, SSL VPN, 2 = AnyConnect Client, IPsec VPN (IKEv2)).

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).