

# Configure FDM External Authentication and Authorization with ISE using RADIUS

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Interoperability](#)

[Licensing](#)

[Background Information](#)

[Network Diagram](#)

[Configure](#)

[FDM Configuration](#)

[ISE Configuration](#)

[Verify](#)

[Troubleshoot](#)

[Common Issues](#)

[Limitations](#)

[Q&A](#)

## Introduction

This document describes the procedure to integrate Cisco Firepower Device Manager (FDM) with Identity Services Engine (ISE) for administrator users authentication with RADIUS Protocol for both GUI and CLI access.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

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

### Components Used

The information in this document is based on these software and hardware versions:

- Firepower Threat Defense (FTD) Device, all platforms Firepower Device Manager (FDM) version 6.3.0+
- ISE version 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. If your network is live, ensure that you understand the potential impact of any command.

## Interoperability

- RADIUS server with users configured with user roles
- User roles must be configured on RADIUS server with cisco-av-pair
- Cisco-av-pair = fdm.userrole.authority.admin
- ISE can be used as a RADIUS server

## Licensing

No specific license requirement, the base license is sufficient

## Background Information

This feature allows customers to configure External Authentication with RADIUS and multiple user roles for those users.

RADIUS support for Management Access with 3 system-defined user roles:

- READ\_ONLY
- READ\_WRITE (cannot perform system critical actions like Upgrade, Restore etc.)
- ADMIN

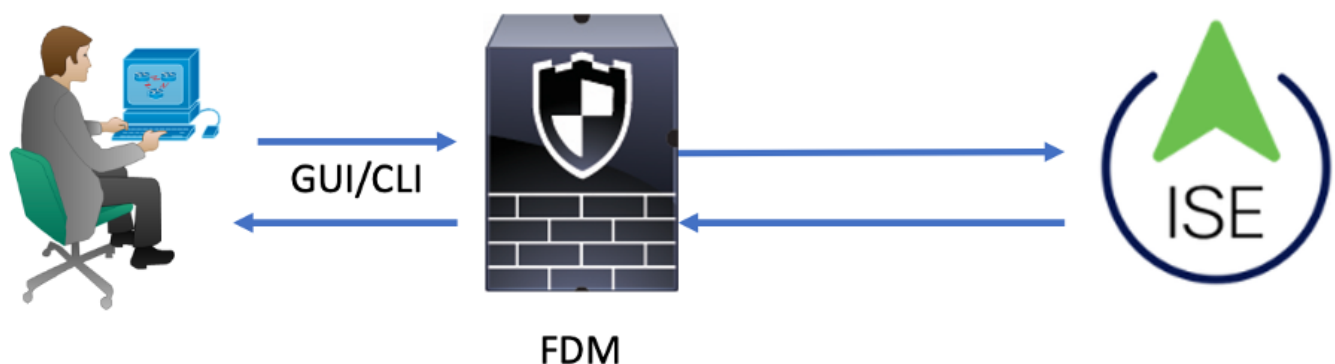
There is the ability to test the RADIUS server's configuration and to monitor active user sessions and delete a user session.

The feature was implemented in FDM version 6.3.0. Prior to the 6.3.0 release, FDM had support for one user(admin) only.

By default, Cisco Firepower Device Manager authenticates and authorizes users locally, in order to have a centralized authentication and authorization method you can use Cisco Identity Service Engine through RADIUS protocol.

## Network Diagram

The next image provides an example of a network topology



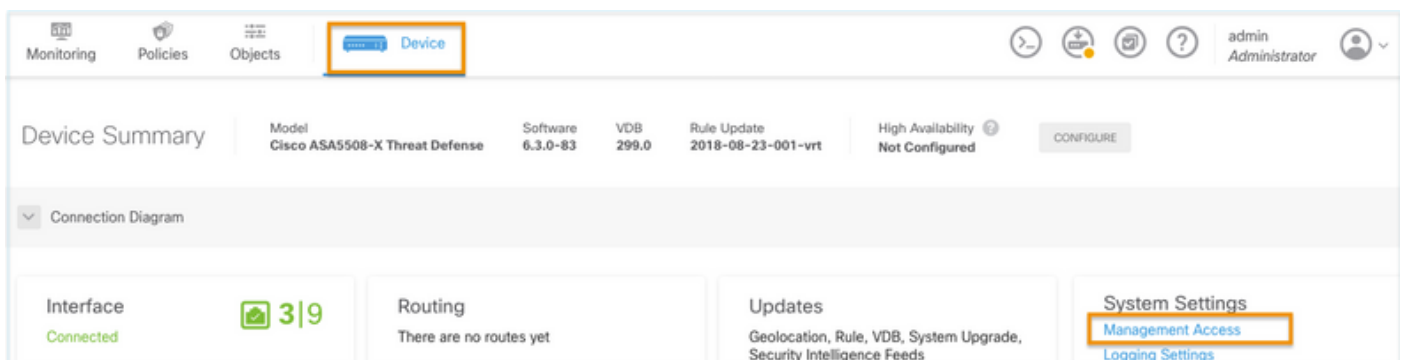
Process:

1. Admin User introduces its credentials.
2. Authentication process triggered and ISE validates the credentials locally or through Active Directory.
3. Once authentication is successful ISE sends a Permit packet for authentication and authorization information to FDM.
4. Account performs on ISE and a successful authentication live log happens.

## Configure

### FDM Configuration

Step 1. Log in into FDM and navigate to Device > System Settings > Management Access tab



**Step 2.** Create New RADIUS Server Group

The screenshot displays the Cisco SD-WAN management interface. At the top, there are navigation tabs: Monitoring, Policies, Objects, and Device (highlighted with an orange box and labeled 1). On the left sidebar, under 'System Settings', 'Management Access' is highlighted with an orange box and labeled 2. Below it are 'Logging Settings' (labeled 2), 'DHCP Server', 'DNS Server', 'Management Interface', 'Hostname', 'NTP', and 'Cloud Services'. Under 'Traffic Settings', 'URL Filtering Preferences' is listed. The main content area is titled 'Device Summary' and 'Management Access'. It has sub-tabs: 'AAA Configuration' (highlighted with an orange box and labeled 3), 'Management Interface', and 'Data Interfaces'. Below the sub-tabs, there is a section for 'HTTPS Connection' and 'Server Group for Management/REST API' (labeled 4). A table with a 'Filter' header (highlighted with an orange box) shows one entry: 'LocalIdentitySource' with a checked checkbox. Below the table, it says 'Nothing found'. At the bottom, there is a button 'Create New RADIUS Server Group' (highlighted with an orange box and labeled 5).

**Step 3.** Create new RADIUS Server

## 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

**Step 4.** Add RADIUS Server into the 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

**i** 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

**i** 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

## Step 6. Save the configuration

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

**i** 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

## ISE Configuration

**Step 1.** Navigate to three lines icon  located in the upper left corner and select on **Administration > Network Resources > Network Devices**



Cisco ISE

Administration · Network Resources

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

Network Devices

Edit

+ Add

Duplicate

Import

Export

Generate PAC

Delete

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

**Step 2.** Select the **+Add** button and define Network Access Device Name and IPAddress, then check the RADIUS checkbox and define a shared secret. Select on **Submit**

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

FDM

Description

IP Address

\* IP: 10.122.111.2 / 32

Device Profile

Cisco

Model Name

Software Version

☒ **RADIUS Authentication Settings**

**RADIUS UDP Settings**

Protocol **RADIUS**

Shared Secret ..... **Show**

☐ Use Second Shared Secret **i**

networkDevices.secondSharedSecret **Show**

CoA Port 1700 **Set To Default**

Administration - Network Resources

Network Devices

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	

**Step 3.** Navigate to three lines icon  located in the upper left corner and Select on **Administration > Identity Management > Groups**

Administration - Identity Management

Identities Groups External Identity Sources Identity Source Sequences Settings

Identity Groups

EQ

< >

> Endpoint Identity Groups

> User Identity Groups

User Identity Groups

Edit Add Delete Import Export

Name	Description
ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
Employee	Default Employee User Group
GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
GuestType_Contractor (default)	Identity group mirroring the guest type
GuestType_Daily (default)	Identity group mirroring the guest type
GuestType_SocialLogin (default)	Identity group mirroring the guest type
GuestType_Weekly (default)	Identity group mirroring the guest type
OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group



**Step 4.** Select on User Identity Groups and select on **+Add** button. Define a name and select on **Submit**


**Cisco ISE** Administration - Identity Management Evaluation Mode 89 Days


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

**Identity Groups**

EQ

<  

>  Endpoint Identity Groups

>  User 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 Evaluation Mode 89 Days


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

**Identity Groups**

EQ

<  

>  Endpoint Identity Groups

>  User Identity Groups

User Identity Groups > New User Identity Group

**Identity Group**

\* Name FDM\_ReadOnly

Description

**Submit** [Cancel](#)

**Note:** In this example, FDM\_Admin and FDM\_ReadOnly Identity groups created, you can repeat Step 4 for each type of Admin Users used on FDM.

**Step 5.** Navigate to three lines icon located in the upper left corner and select **Administration > Identity Management > Identities**. Select on **+Add** and define the username and password, then select the group where the user belongs to. In this example, fdm\_admin and fdm\_readonly users were created and assigned to FDM\_Admin and FDM\_ReadOnly group respectively.

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	fdm_admin				FDM_admin	
<input type="checkbox"/>	<input checked="" type="checkbox"/> Enabled	fdm_readonly				FDM_ReadOnly	

**Step 6.** Select the three lines icon located in the upper left corner and navigate to **Policy > Policy Elements > Results > Authorization > Authorization Profiles**, select on **+Add**, define a name for the **Authorization Profile**. Select **Radius Service-type** and select **Administrative**, then select **Cisco-av-pair** and paste the role the admin user gets, in this case, the user receives a full admin privilege (fdm.userrole.authority.admin). Select on **Submit**. Repeat this step for each role, read-only user configured as another example in this document.

Dictionaries

Conditions

**Results**

Authentication &gt;

Authorization ▾

Authorization Profiles

Downloadable ACLs

Profiling &gt;

Posture &gt;

Client Provisioning &gt;

[Authorization Profiles](#) > New Authorization Profile

## Authorization Profile

\* Name

FDM\_Profile\_Admin

Description

\* Access Type

ACCESS\_ACCEPT ▾

Network Device Profile

 Cisco ▾ ⊕Service Template ☐Track Movement ☐ ⓘAgentless Posture ☐ ⓘPassive Identity Tracking ☐ ⓘ

## ✕ Advanced Attributes Settings



Radius:Service-Type ▾

=

Administrative ▾



Cisco:cisco-av-pair ▾

=

fdm.userrole.authority.admin| ▾



## ✕ Attributes Details

Access Type = ACCESS\_ACCEPT

Service-Type = 6

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

## 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

**Note:** Ensure the order of the Advance attributes section is as with the images example in order to avoid unexpected result when log in with GUI and CLI.

**Step 8.** Select the three lines icon and navigate to **Policy > Policy Sets**. Select on







 button located below **Policy Sets** title, define a name and select on the + button in the middle to add a new condition.

**Step 9.** Under Condition window, select to add an attribute and then select on **Network Device** Icon followed by Network access device IP address. Select **Attribute Value** and add the FDM IP address. Add a new condition and select on **Network Access** followed by Protocol option, select on **RADIUS** and select on Use once done.

 Policy · Policy Sets Evaluation Mode 89 Days

Policy Sets

Reset Reset Policyset Hitcounts Save

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

Reset Save

**Step 10.** Under allow protocols section, select **Device Default Admin**. Select on **Save**

**Step 11.** Select on the right arrow icon of the Policy Set to Define authentication and authorization policies



**Step 12.** Select on located below Authentication Policy title, define a name and select on the + in the middle to add a new condition. Under Condition window, select to add an attribute and then select on Network Device Icon followed by Network access device IP address. Select on Attribute Value and add the FDM IP address. Select on Use once done

**Step 13.** Select Internal Users as the Identity Store and select on Save

**Note:** Identity Store can be changed to AD store if ISE is joined to an Active Directory.



**Step 14.** Select on located below Authorization Policy title, define a name and select on the + in the middle to add a new condition. Under Condition window, select to add an attribute and then select on Identity Group icon followed by Internal User:Identity Group. Select the FDM\_Admin Group, Select the AND along with NEW option to add a new condition, select on port icon followed by RADIUS NAS-Port-Type:Virtual and select on 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

+

NEW AND OR

Set to 'Is not'

Duplicate Save

**Step 15. Under Profiles, select the profile created in Step 6 and then select on Save**

Repeat Step 14 and 15 for FDM\_ReadOnly group

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	<div>IdentityGroup-Name EQUALS User Identity Groups:FDM_admin</div> <div>Radius-NAS-Port-Type EQUALS Virtual</div>	FDM_Profile_Admin	Select from list	3	⚙️
✓	FTD_FDM_Authz_RORole	AND	<div>IdentityGroup-Name EQUALS User Identity Groups:FDM_ReadOnly</div> <div>Radius-NAS-Port-Type EQUALS Virtual</div>	FDM_Profile_RO	Select from list	0	⚙️
✓	Default			DenyAccess	Select from list	4	⚙️

**Step 16 (Optional).** Navigate to three lines icon located in the upper left corner and select on Administration > System > Maintenance > Repository and select on +Add to add a repository used to store TCP Dump file for troubleshoot purposes.

**Step 17 (Optional).** Define a repository Name, protocol, Server Name, path and Credentials. Select on Submit once done.



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

## Verify

**Step 1. Navigate to Objects > Identity Sources tab and verify RADIUS Server and Group Server configuration**

CISCO 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

Object Types

- Networks
- Ports
- Security Zones
- Application Filters
- URLs
- Geolocations
- Syslog Servers
- IKE Policies
- IPSec Proposals
- Identity Sources**
- Users

**Step 2. Navigate to Device > System Settings > Management Access tab and select the TEST button**

The screenshot displays the Cisco SD-WAN configuration interface. At the top, the navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device' (highlighted with an orange box and labeled '1'). On the left sidebar, 'System Settings' is expanded, and 'Management Access' is selected (highlighted with an orange box and labeled '2'). The main content area shows the 'Device Summary' for 'Management Access' (labeled '3'). Below this, the 'AAA Configuration' tab is active (highlighted with an orange box). The configuration page is titled 'Configure how to authenticate management connections to the device.' and contains a 'HTTPS Connection' section. Within this section, the 'Server Group for Management/REST API' is set to 'radius-server-group' (highlighted with an orange box). A green 'TEST' button is highlighted with an orange box and labeled '4'. Below this, the 'Authentication with LOCAL' is set to 'Before External Server'. A 'SAVE' button is at the bottom of the configuration panel.

**Step 3.** Insert user credentials and select the **TEST** button

## 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.*

**Step 4.** Open a new window browser and type [https://FDM\\_ip\\_Address](https://FDM_ip_Address), use fdm\_admin username and password created on step 5 under ISE configuration section.



# Firepower Device Manager

**Successfully logged out**

fdm\_admin

.....

LOG IN

Successful log in attempt can be verified on ISE RADIUS live logs

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

X

Identity

Authentication Policy

Authorization Policy

Authorization Profiles

Jul 06, 2021 04:54:12.41...

fdm\_admin

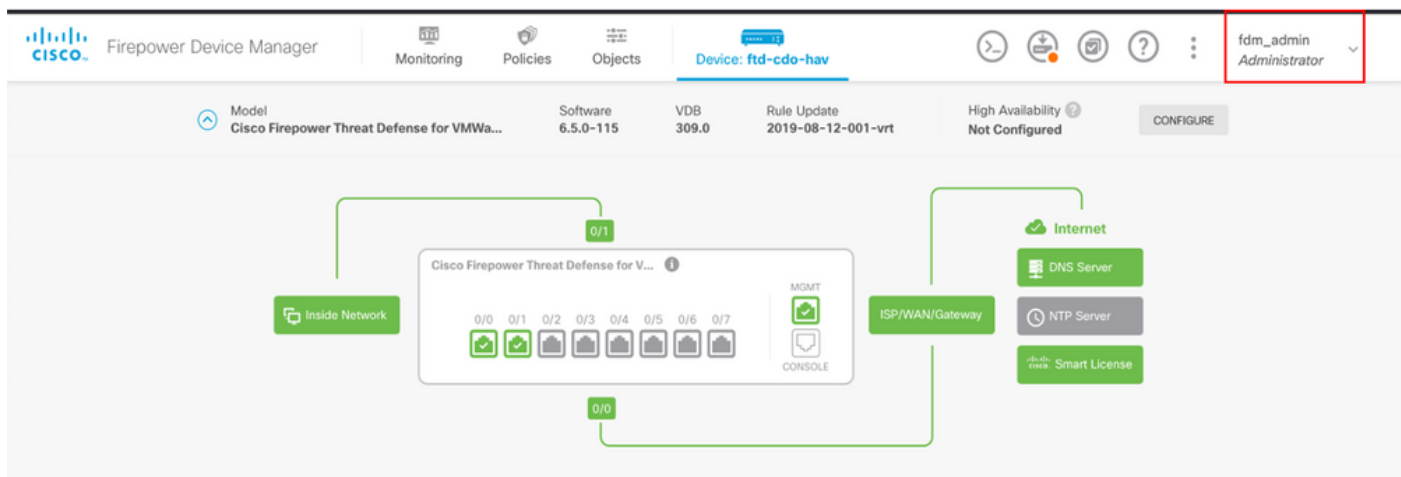
FTD\_FDM\_Radius\_Access >> FDM\_...

FTD\_FDM\_Radius\_Access >> FTD\_FDM...

FDM\_Profile\_Admin

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

Admin User can also be reviewed on FDM on the upper right corner



## Cisco Firepower Device Manager CLI (Admin User)

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

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

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

```
Connection to 10.122.111.212 _closed.
```

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

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

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

[> █
```

## Troubleshoot

This section provides the information you can use to troubleshoot your configuration.

### Communication validation with TCP Dump tool on ISE

**Step 1.** Log in on ISE and select the three lines icon located in the upper left corner and navigate

to **Operations > Troubleshoot > Diagnostic Tools**.

**Step 2.** Under General tools select on TCP Dumps and then select on **Add+**. Select Hostname, Network Interface File Name, Repository, and optionally a filter to gather only FDM IP address communication flow. Select on **Save and Run**

The screenshot displays the Cisco ISE web interface for configuring a TCP Dump. The left sidebar shows the navigation menu with 'Diagnostic Tools' selected, and 'TCP Dump' highlighted under 'General Tools'. The main content area is titled 'TCP Dump > New' and 'Add TCP Dump'. It includes a description: 'Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.' The configuration fields are as follows:

- Host Name:** A dropdown menu with 'ise31' selected.
- Network Interface:** A dropdown menu with 'GigabitEthernet 0 [Up, Running]' selected.
- Filter:** A text input field containing 'ip host 10.122.111.212'. Below the field, an example is provided: '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.
- File Size:** A numeric input field with '10' and a unit dropdown set to 'Mb'.
- Limit to:** A numeric input field with '1' and a unit dropdown set to 'File(s)'.
- Time Limit:** A numeric input field with '5' and a unit dropdown set to 'Minute(s)'.
- Promiscuous Mode:** An unchecked checkbox.

**Step 3.** Log in on FDM UI and type the admin credentials.

**Step 4.** On ISE, select on **Stop** button and verify the pcap file has been sent to the defined repository.

Operations · Troubleshoot

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

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
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		
FDM_Tshoot.pcap	545	473	PCAP File	7/6/2021 5:21 ...	3A095B10

Total 1 file, 545 bytes

**Step 5.** Open the pcap file to validate the successful communication between FDM and 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_admi n.....
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..
  
```

If no entries are shown on pcap file validate the next options:

1. Right ISE IP address has been added on FDM configuration
2. In case of a firewall is in the middle verify port 1812-1813 is permitted.
3. Check communication between ISE and FDM

### Communication validation with FDM generated file.

In troubleshoot file generated from FDM Device page look for keywords:

- FdmPasswordLoginHelper
- NGFWDefaultUserMgmt
- AAIdentitySourceStatusManager
- RadiusIdentitySourceManager

All the logs related to this feature can be found in /var/log/cisco/ngfw-onbox.log

References:

[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)



# Common Issues

## Case 1 - External Auth not working

- Check secretKey, port, or hostname
- Misconfiguration of AVPs on RADIUS
- Server can be in 'Dead Time'

## Case 2 -Test IdentitySource fails

- Make sure the changes to object are saved
- Make sure the credentials are correct

# Limitations

- FDM allows max of 5 active FDM sessions.
- Creation of 6th session results in the 1st session revoked
- Name of RadiusIdentitySourceGroup cannot be "LocalIdentitySource"
- Max of 16 RadiusIdentitySources to a RadiusIdentitySourceGroup
- Misconfiguration of AVPs on RADIUS result in Denying access to FDM

# Q&A

Q: Does this feature work in Evaluation mode?

A: Yes

Q: If two read-only users log in, where have access to read-only user 1, and they log in from two diff browsers. How will it show? What will happen?

A: Both user's sessions are shown in the active user sessions page with the same name. Each entry shows an individual value for the time stamp.

Q: What is the behavior is the external radius server provides an access reject vs. "no response" if you have local auth configured 2nd?

A: You can try LOCAL auth even if you get Access reject or no response if you have local auth configured 2nd.

Q: How ISE differentiates a RADIUS request for admin log in vs. RADIUS request to authenticate an RA VPN user

A: ISE doesn't differentiate a RADIUS request for Admin Vs RAVPN users. FDM looks at cisco-avpair attribute to figure out Authorization for Admin access. ISE sends all the attributes configured for the user in both the cases.

Q: That means ISE logs is not be able to differentiate between an FDM admin log in and that same user accessing remote access VPN on same device. Is there any RADIUS attribute passed to ISE in the access request that ISE can key on?

A: Following are the upstream RADIUS attributes that are sent from the FTD to ISE during RADIUS authentication for RAVPN. These are not sent as part of External Auth Management Access Request and can be used to differentiate a FDM administration log in Vs RAVPN user log in.

146 - Tunnel Group Name or Connection Profile Name.

150 – Client Type (Applicable values: 2 = AnyConnect Client SSL VPN, 6 = AnyConnect Client IPsec VPN (IKEv2).

151 – Session Type (Applicable values: 1 = AnyConnect Client SSL VPN, 2 = AnyConnect Client IPsec VPN (IKEv2).