

# Configureer FDM externe verificatie en autorisatie met ISE met RADIUS

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Interoperabiliteit](#)

[Licentie](#)

[Achtergrondinformatie](#)

[Netwerkdigram](#)

[Configureren](#)

[FDM-configuratie](#)

[ISE-configuratie](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Veelvoorkomende problemen](#)

[Beperkingen](#)

[Vraag en antwoord](#)

## Inleiding

Dit document beschrijft de procedure om Cisco Firepower Device Manager (FDM) te integreren met Identity Services Engine (ISE) voor verificatie van beheerdergebruikers met RADIUS-protocol voor zowel GUI- als CLI-toegang.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Firepower Threat Defense (FTD) apparaat, alle platforms Firepower Device Manager (FDM) versie 6.3.0+
- ISE, versie 3.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Interoperabiliteit

- RADIUS-server met gebruikers geconfigureerd met gebruikersrollen
- Gebruikersrollen moeten op RADIUS-server met cisco-av-paar worden geconfigureerd
- Cisco 8-av-paar = fdm.userrole.authority.admin
- ISE kan als RADIUS-server worden gebruikt

## Licentie

Geen specifieke vergunningsvereiste, is de basisvergunning voldoende

## Achtergrondinformatie

Met deze functie kunnen klanten externe verificatie configureren met RADIUS en meerdere gebruikersrollen voor die gebruikers.

RADIUS-ondersteuning voor Management Access met 3 systeemgedefinieerde gebruikersrollen:

- ALLEEN READ\_ONLY
- READ\_Write (kan geen systeemkritische acties uitvoeren zoals Upgrade, Herstel enz.)
- BEHEERDER

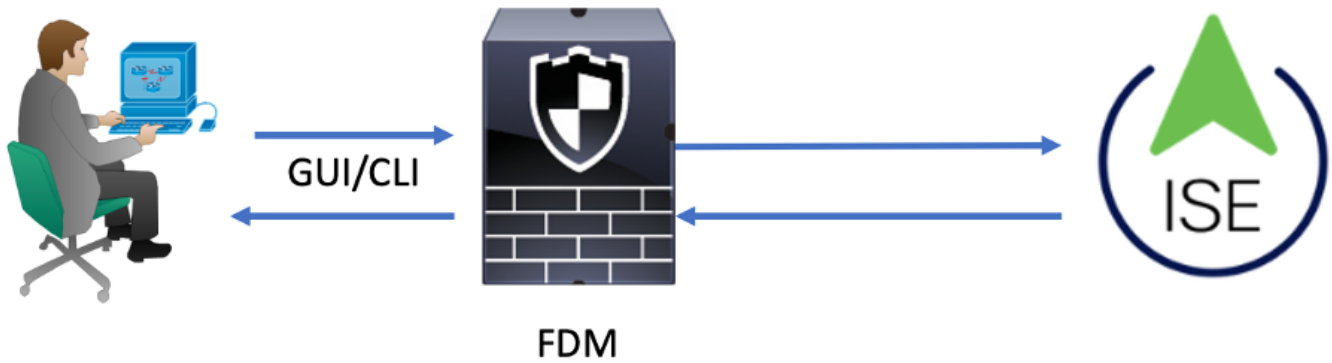
Er is de mogelijkheid om de configuratie van de RADIUS-server te testen en actieve gebruikerssessies te bewaken en een gebruikerssessie te verwijderen.

De functie werd geïmplementeerd in FDM versie 6.3.0. Voorafgaand aan de 6.3.0 release had FDM slechts ondersteuning voor één gebruiker (admin).

Standaard zal Cisco Firepower Device Manager gebruikers lokaal verifiëren en machtigen om een gecentraliseerde verificatie- en autorisatiemethode te hebben. U kunt Cisco Identity Service Engine via RADIUS-protocol gebruiken.

## Netwerkdigram

Het volgende beeld verstrekt een voorbeeld van een netwerktopologie



Proces:

1. Beheerder introduceert de referenties.
2. Verificatieproces geactiveerd en ISE valideert de referenties lokaal of via Active Directory.
3. Zodra de verificatie succesvol is, stuurt ISE een Permit-pakket voor verificatie- en autorisatiegegevens naar FDM.
4. De account wordt uitgevoerd op ISE en er gebeurt een succesvol live verificatielogboek.

## Configureren

### FDM-configuratie

Stap 1. Inloggen in FDM en navigeren naar apparaat > Systeeminstellingen > tabblad Management Access

The screenshot shows the FDM web interface. At the top, there are navigation tabs: 'Monitoring', 'Policies', 'Objects', and 'Device' (which is highlighted with an orange box). To the right of these tabs are several icons and the user name 'admin Administrator'. Below the navigation bar, the main content area displays 'Device Summary' for a 'Cisco ASA5508-X Threat Defense' device. It shows details like 'Software 6.3.0-83', 'VDB 299.0', and 'Rule Update 2018-08-23-001-vrt'. There is a 'CONFIGURE' button next to the 'High Availability' status, which is 'Not Configured'. Below this is a 'Connection Diagram' section. At the bottom, there are four main sections: 'Interface' (status: Connected, with a green icon and '3|9'), 'Routing' (status: There are no routes yet), 'Updates' (status: Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds), and 'System Settings' (with a sub-tab 'Management Access' highlighted by an orange box and a 'Logging Settings' link below it).

Stap 2. Nieuwe RADIUS-servergroep maken

The screenshot displays the Cisco ISE configuration interface. At the top, the 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' (labeled '1'). Below this, there are three tabs: 'AAA Configuration' (labeled '3'), 'Management Interface', and 'Data Interfaces'. The 'AAA Configuration' tab is active, showing the 'HTTPS Connection' section. Under 'Server Group for Management/REST API' (labeled '4'), there is a 'Filter' dropdown menu with 'LocalIdentitySource' selected. Below the filter, it says 'Nothing found'. At the bottom of the page, there is a button labeled 'Create New RADIUS Server Group' (labeled '5').

Stap 3. Nieuwe RADIUS-server maken

# 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

Stap 4. RADIUS-server toevoegen aan de RADIUS-servergroep

## Add RADIUS Server Group

Name 3

radius-server-group

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

+

Filter 1

radius-server ⓘ

CANCEL 4 OK

Create new RADIUS Server CANCEL 2 OK

Stap 5. Geselecteerde groep als servergroep voor beheer selecteren

## Device Summary

### Management Access

AAA Configuration Management Interface Data Interfaces

Configure how to authenticate management connections to the device.

#### HTTPS Connection

Server Group for Management/REST API

Filter

LocalIdentitySource

radius-server-group ⓘ

Create New RADIUS Server Group

AAA Configuration Management Interface Data Interfaces Management Web Server

Configure how to authenticate management connections to the device.

### HTTPS Connection

Server Group for Management/REST API

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

Radius-server-group TEST

Authentication with LOCAL

After External Server

**SAVE**

### SSH Connection

Server Group

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

Radius-server-group TEST

Authentication with LOCAL

Before External Server

**SAVE**

**Stap 6.** Sla de configuratie op

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**

## ISE-configuratie

**Stap 1.** Navigeren naar het pictogram met drie lijnen  bevindt zich in de linkerbovenhoek en selecteer **Beheer > Netwerkbronnen > Netwerkapparaten**



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

**Stap 2.** Selecteer de knop **+Add** en definieer de naam en het IP-adres van het netwerktoegangsapparaat, controleer vervolgens het selectievakje RADIUS en stel een gedeeld geheim in. Selecteer bij **Verzenden**

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 \* IP:  /

Device Profile

Model Name

Software Version

RADIUS Authentication Settings

RADIUS UDP Settings

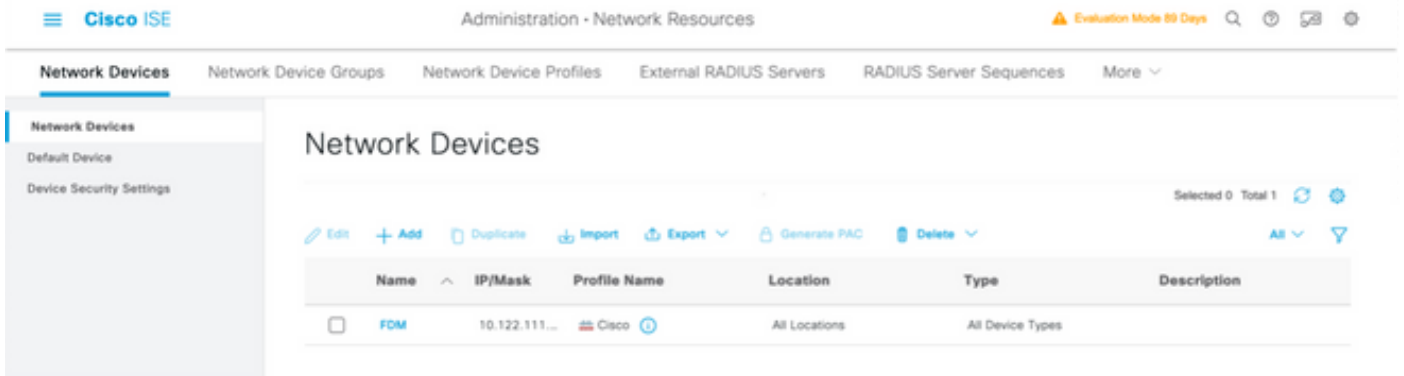
Protocol


Shared Secret  [Show](#)

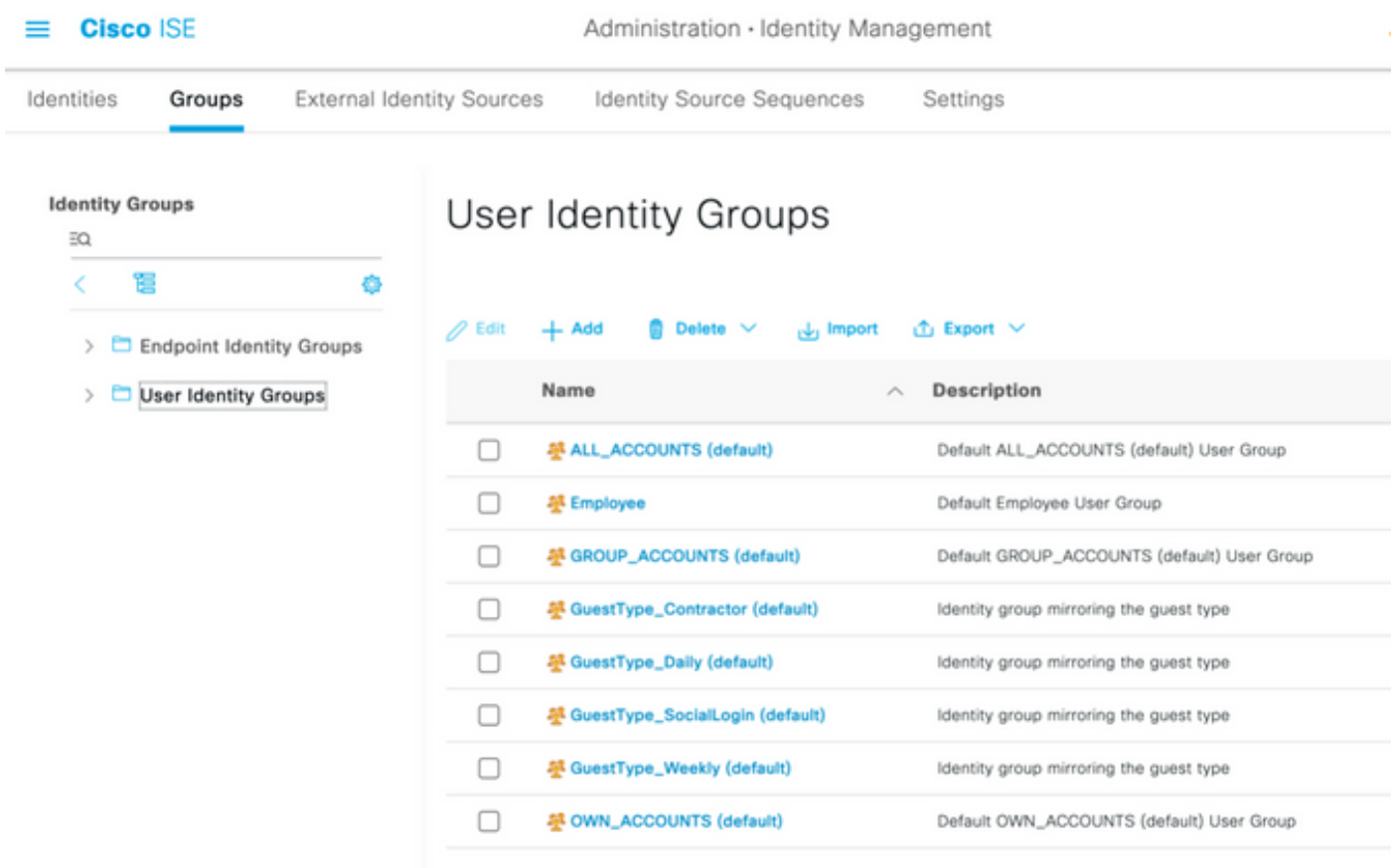
Use Second Shared Secret [i](#)

networkDevices.secondSharedSecret  [Show](#)

CoA Port  [Set To Default](#)



**Stap 3.** Navigeren naar het pictogram met drie lijnen  in de linkerbovenhoek en selecteer **Beheer > Identity Management > Groepen**



**Stap 4.** Selecteer Gebruikersidentiteitsgroepen en selecteer de knop **+Add**. Bepaal een naam en selecteer bij **Verzenden**

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

**Opmerking:** in dit voorbeeld, FDM\_Admin en FDM\_ReadOnly Identity groepen gemaakt, kunt u Stap 4 herhalen voor elk type Admin Gebruikers gebruikt op FDM.

**Stap 5.** Navigeer naar het pictogram met drie lijnen linksboven en selecteer **Beheer > Identity Management > Identities**. Selecteer op **+Add** en definieer de gebruikersnaam en het wachtwoord en selecteer vervolgens de groep waartoe de gebruiker behoort. In dit voorbeeld, werden `fdm_admin` en `fdm_readonly` gebruikers gecreëerd en toegewezen aan respectievelijk `FDM_Admin` en `FDM_ReadOnly` groep.

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](#) [All](#)

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	

**Stap 6.** Selecteer het pictogram met drie regels linksboven en ga naar **Policy > Policy Elements > Results > Authorisation > Authorisation Profiles**, selecteer on **+Add**, definieer een naam voor het autorisatieprofiel. Selecteer **Radius Service-type** en selecteer **Administratief**, selecteer vervolgens **Cisco-av-paar** en plak de rol die de beheerder krijgt, in dit geval ontvangt de gebruiker een volledige admin-voorrecht (fdm.userrole.authority.admin). Selecteer bij **Verzenden**. Herhaal deze stap voor elke rol, alleen-lezen gebruiker die als een ander voorbeeld in dit document is geconfigureerd.

Dictionarys Conditions **Results**

- 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

	<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
```

**Opmerking:** Zorg ervoor dat de volgorde van de sectie Geavanceerde eigenschappen gelijk is aan het voorbeeld van afbeeldingen om onverwachte resultaten te voorkomen bij inloggen met GUI en CLI.

**Stap 8.** Selecteer het pictogram met drie lijnen en navigeer naar Policy > Policy Sets. Selecteren

op  de knop onder de titel Beleidssets, definieert een naam en selecteert u in het midden op de +-toets om een nieuwe voorwaarde toe te voegen.

**Stap 9.** Selecteer onder het venster Voorwaarde de optie om een kenmerk toe te voegen en selecteer vervolgens het pictogram **Netwerkapparaat** gevolgd door het IP-adres van het Netwerkttoegangsapparaat. Selecteer **Attribute Value** en voeg het FDM IP-adres toe. Voeg een nieuwe voorwaarde toe en selecteer op **Network Access** gevolgd door de optie Protocol, selecteer op **RADIUS** en selecteer op Use once done.

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		⚙️	➔
✔	Default	Default policy set		Default Network Access	0	⚙️	➔

**Stap 10.** Selecteer onder Protocollen toestaan de optie **Standaard apparaatbeheer**. Selecteer dit bij Opslaan

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		⚙️	➔
✔	Default	Default policy set		Default Network Access	0	⚙️	➔


**Stap 11.** Selecteer dit met de juiste pijl  pictogram van het beleid dat is ingesteld om het verificatie- en autorisatiebeleid te definiëren

**Stap 12.** Selecteren op  onder de titel Verificatiebeleid, definieer een naam en selecteer + in het midden om een nieuwe voorwaarde toe te voegen. Selecteer onder het venster Voorwaarde de optie om een kenmerk toe te voegen en selecteer vervolgens het pictogram Netwerkapparaat gevolgd door het IP-adres van het netwerktoegangsapparaat. Selecteer op Attribute Value en voeg het FDM IP-adres toe. Selecteer deze optie op Use once done

**Stap 13.** Selecteer Interne Gebruikers als Identity Store en selecteer op Opslaan

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

**Opmerking:** Identity Store kan worden gewijzigd in AD Store als ISE wordt aangesloten bij een Active Directory.

Stap 14. Selecteren op  gevestigd onder de titel van het Beleid van de Vergunning, definieer een naam en selecteer op + in het midden om een nieuwe voorwaarde toe te voegen. Selecteer onder het venster Voorwaarde de optie om een kenmerk toe te voegen en selecteer vervolgens het pictogram Identity Group gevolgd door Internal User:Identity Group. Selecteer de FDM\_Admin Group, selecteer de EN samen met NEW optie om een nieuwe voorwaarde toe te voegen, selecteer op poortpictogram gevolgd door RADIUS NAS-Port-Type:Virtual en selecteer op Use.

## Conditions Studio

### Library

Search by Name



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

### Editor

AND

IdentityGroup-Name

Equals User Identity Groups:FDM\_admin

Radius-NAS-Port-Type

Equals Virtual

+ NEW AND OR

Set to 'Is not'

Duplicate
Save

Stap 15. Selecteer onder Profielen het profiel dat in Stap 6 is gemaakt en selecteer vervolgens Opslaan

Herhaal stap 14 en 15 voor FDM\_ReadOnly groep



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

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

**Stap 16 (optioneel).** Blader naar het pictogram met drie lijnen in de linkerbovenhoek en selecteer **Beheer > Systeem > Onderhoud > Opslagplaats** en selecteer op **+Add** om een opslagplaats toe te voegen die wordt gebruikt om TCP Dump-bestand op te slaan voor probleemoplossingsdoeleinden.

**Stap 17 (optioneel).** Definieer een naam, protocol, servernaam, pad en referenties van de repository. Selecteer op **Indienen** als u klaar bent.

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 .....

## Verifiëren

**Stap 1.** Navigeer naar **objecten > tabblad Identity Source** en controleer de configuratie van **RADIUS-server** en **-groepserver**

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' with 'Identity Sources' highlighted (orange box). 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

Stap 2. Navigeer naar Apparaat > Systeminstellingen > het tabblad Toegang beheren en selecteer de knop TEST

The screenshot shows the Cisco configuration interface. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device' (highlighted with an orange box and labeled '1'). The left sidebar lists 'System Settings' with 'Management Access' highlighted (orange box and labeled '2'). The main content area is titled 'Device Summary Management Access' and has 'AAA Configuration' highlighted (orange box and labeled '3'). Below this, there are tabs for 'Management Interface' and 'Data Interfaces'. A message states: 'Configure how to authenticate management connections to the device.' The 'HTTPS Connection' section includes a dropdown menu for 'Server Group for Management/REST API' set to 'radius-server-group' and a green 'TEST' button highlighted with an orange box and labeled '4'. Below this is a section for 'Authentication with LOCAL' with a dropdown menu set to 'Before External Server' and a 'SAVE' button.

Stap 3. Plaats gebruikersreferenties en selecteer de TEST-knop

## 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.*

**Stap 4.** Open een nieuwe vensterbrowser en typ [https://FDM\\_ip\\_Address](https://FDM_ip_Address), gebruik fdm\_admin gebruikersnaam en wachtwoord dat gecreëerd is in stap 5 onder de sectie ISE-configuratie.



# Firepower Device Manager

**Successfully logged out**

fdm\_admin

.....|

LOG IN

Succesvolle inlogpoging kan worden geverifieerd op de live-logs van ISE RADIUS

Cisco ISE Operations - RADIUS Evaluation Mode 79 Days

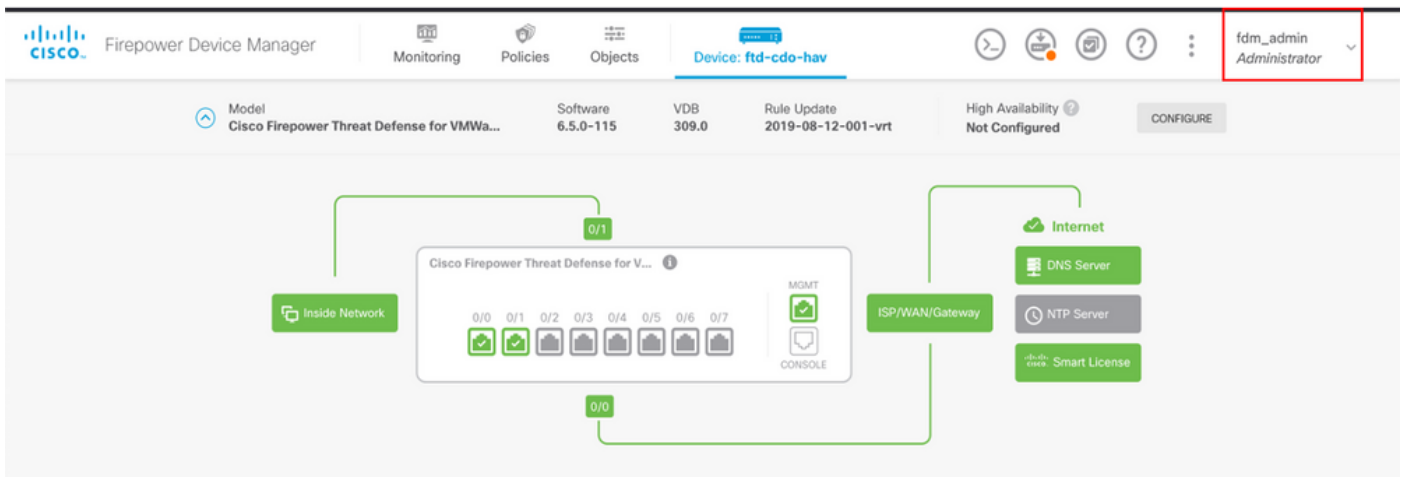
Live Logs Live Sessions

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

Admin User kan ook worden bekeken op FDM in de rechterbovenhoek



## Cisco Firepower Device Manager CLI (beheerder)

```
[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)

[> █
```

## Problemen oplossen

Deze sectie verschaft de informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

### Communicatievalidatie met TCP Dump tool op ISE

**Stap 1.** Log in op ISE en selecteer het pictogram met drie lijnen in de linkerbovenhoek en navigeer naar **Operations > Probleemoplossing > Diagnostische tools**.

**Stap 2.** Selecteer onder Algemene gereedschappen de optie op TCP Dumps en selecteer vervolgens op **Add+**. Selecteer Hostname, Network Interface File Name, Repository en optioneel een filter om alleen FDM IP-adrescommunicatie stroom te verzamelen. Selecteer deze optie bij **Opslaan en uitvoeren**

The screenshot shows the Cisco ISE Diagnostic Tools interface. The left sidebar is expanded to show 'TCP Dump' under 'General Tools'. The main content area is titled 'TCP Dump > New' and 'Add TCP Dump'. Below the title, there is 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:** 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:**

**Stap 3.** Log in op FDM UI en typ de beheerdersreferenties.

**Stap 4.** Selecteer op ISE de knop **Stop** en controleer of het pcap-bestand naar de gedefinieerde repository is verstuurd.

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

Stap 5. Open het pcap-bestand om de succesvolle communicatie tussen FDM en ISE te valideren.



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..

```

Als er geen items worden weergegeven in het pcap-bestand, valideert u de volgende opties:

1. Het juiste ISE-IP-adres is toegevoegd aan de FDM-configuratie
2. Als een firewall zich in het midden bevindt, is de verify-poort 1812-1813 toegestaan.
3. Controleer de communicatie tussen ISE en FDM

### Communicatievalidatie met FDM-gegenereerd bestand.

In probleemoplossing bestand gegenereerd vanuit FDM Apparaatpagina zoekt u naar trefwoorden:

- FDMPasswordLoginHelper
- Standaard NGFW-gebruikersbeheer
- AAIdentitySourceStatusManager
- RadiusIdentitySource Manager

Alle logbestanden die betrekking hebben op deze functie zijn te vinden op /var/log/cisco/ngfw-onbox.log

Referenties:

[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)



# Veelvoorkomende problemen

## Zaak 1 - Externe Autoriteit werkt niet

- Controleer de geheime sleutel, poort of hostnaam
- Misconfiguratie van AVP's op RADIUS
- De server kan zich in 'Dead Time' bevinden

## Case 2 - Test IdentitySource mislukt

- Zorg ervoor dat de wijzigingen in het object zijn opgeslagen
- Controleer of de referenties correct zijn

# Beperkingen

- FDM staat maximaal 5 actieve FDM-sessies toe.
- Verwezenlijking van de resultaten van de 6e sessie in de 1e herroepen sessie
- De naam van RadiusIdentitySourceGroup kan niet "LocalIdentitySource" zijn
- Max. aantal 16 RadiusIdentitySources voor een RadiusIdentitySourceGroup
- Misconfiguratie van AVP's op RADIUS leidt tot ontzegging van toegang tot FDM

# Vraag en antwoord

V: Werkt deze functie in evaluatiemodus?

A: Ja

Q: Als twee alleen-lezen gebruikers inloggen, waar hebben toegang tot alleen-lezen gebruiker 1, en ze inloggen van twee verschillende browsers. Hoe zal het uitwijzen? Wat zal er gebeuren?

A: Beide gebruikerssessies worden weergegeven op de pagina met actieve gebruikerssessies met dezelfde naam. Elke ingang toont een individuele waarde voor de tijdzegel.

V: Wat is het gedrag is de externe radius server biedt een toegangsweigering vs. "geen reactie" als u lokale auth ingesteld 2nd?

A: U kunt lokale auth proberen, zelfs als u toegang geweigerd of geen reactie krijgt als u lokale auth ingesteld 2nd.

V: Hoe ISE een RADIUS-verzoek voor admin-aanmelding onderscheidt van een RADIUS-verzoek om een RA VPN-gebruiker te authenticeren

A: ISE maakt geen onderscheid tussen een RADIUS-verzoek voor Admin vs RAVPN-gebruikers. FDM bekijkt de cisco-avpair attributen om te bepalen hoe u autorisatie kunt verkrijgen voor beheerderstoegang. ISE stuurt alle eigenschappen die voor de gebruiker zijn geconfigureerd in beide gevallen.

Q: Dat betekent de logboeken van ISE niet in staat is om tussen een FDM admin login en dat zelfde gebruiker te onderscheiden die tot verre toegang VPN op zelfde apparaat toegang hebben. Is er een RADIUS-kenmerk dat aan ISE wordt doorgegeven in het toegangsverzoek waarop ISE

kan intoetsen?

A: Hieronder staan de stroomopwaartse RADIUS-kenmerken die tijdens RADIUS-verificatie voor RAVPN van de FTD naar ISE worden verzonden. Deze worden niet verzonden als deel van Externe Autorisatie Management Access Aanvraag en kunnen worden gebruikt om een FDM-beheerlog in Vs RAVPN-gebruikersaanmelding te onderscheiden.

146 - Tunnel Group Name of Connection Profile Name.

150 - Clienttype (toepasselijke waarden: 2 = AnyConnect Client SSL VPN, 6 = AnyConnect Client IPsec VPN (IKEv2).

151 - Sessietype (toepasselijke waarden: 1 = AnyConnect Client SSL VPN, 2 = AnyConnect Client IPsec VPN (IKEv2).

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.