

# Configurer l'authentification et l'autorisation externes FDM avec ISE à l'aide de RADIUS

## Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Interfonctionnement](#)

[Licences](#)

[Informations générales](#)

[Diagramme du réseau](#)

[Configurer](#)

[Configuration de FDM](#)

[Configuration ISE](#)

[Vérifier](#)

[Dépannage](#)

[Problèmes courants](#)

[Limites](#)

[Q&R](#)

## Introduction

Ce document décrit la procédure d'intégration de Cisco Firepower Device Manager (FDM) avec Identity Services Engine (ISE) pour l'authentification des utilisateurs administrateurs avec le protocole RADIUS pour l'accès GUI et CLI.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Gestionnaire de périphériques Firepower (FDM)
- Identity Services Engine (ISE)
- protocole RADIUS

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Périphérique Firepower Threat Defense (FTD), toutes plates-formes 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Interfonctionnement

- Serveur RADIUS avec des utilisateurs configurés avec des rôles d'utilisateur
- Les rôles utilisateur doivent être configurés sur le serveur RADIUS avec cisco-av-pair
- Cisco-av-pair = fdm.userrole.authority.admin
- ISE peut être utilisé comme serveur RADIUS

## Licences

Aucune exigence de licence spécifique, la licence de base est suffisante

## Informations générales

Cette fonctionnalité permet aux clients de configurer l'authentification externe avec RADIUS et plusieurs rôles d'utilisateur pour ces utilisateurs.

Prise en charge RADIUS pour Management Access avec 3 rôles utilisateur définis par le système :

- LECTURE\_SEULE
- READ\_WRITE (impossible d'effectuer des actions système critiques telles que la mise à niveau, la restauration, etc.)
- ADMIN

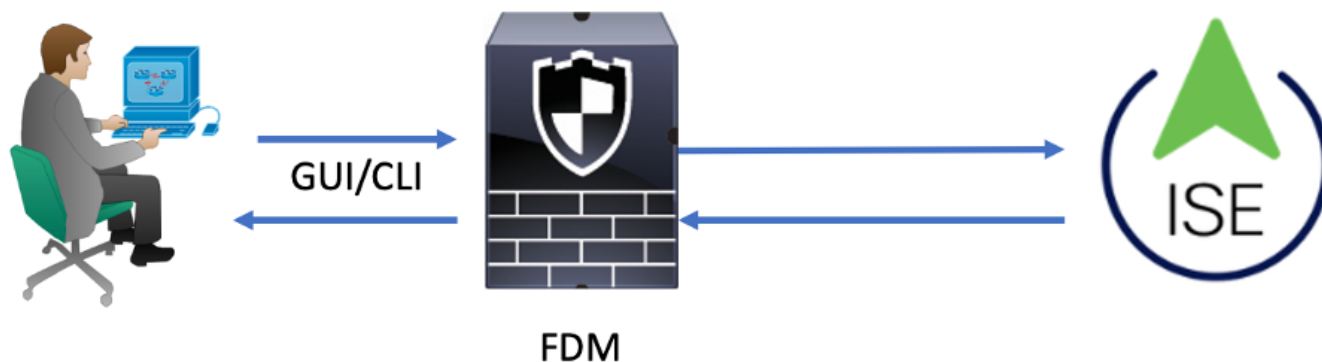
Il est possible de tester la configuration du serveur RADIUS, de surveiller les sessions utilisateur actives et de supprimer une session utilisateur.

La fonctionnalité a été implémentée dans FDM version 6.3.0. Avant la version 6.3.0, FDM ne prenait en charge qu'un seul utilisateur (admin).

Par défaut, Cisco Firepower Device Manager authentifie et autorise les utilisateurs localement, afin d'avoir une méthode d'authentification et d'autorisation centralisée, vous pouvez utiliser Cisco Identity Service Engine via le protocole RADIUS.

## Diagramme du réseau

L'image suivante fournit un exemple de topologie de réseau



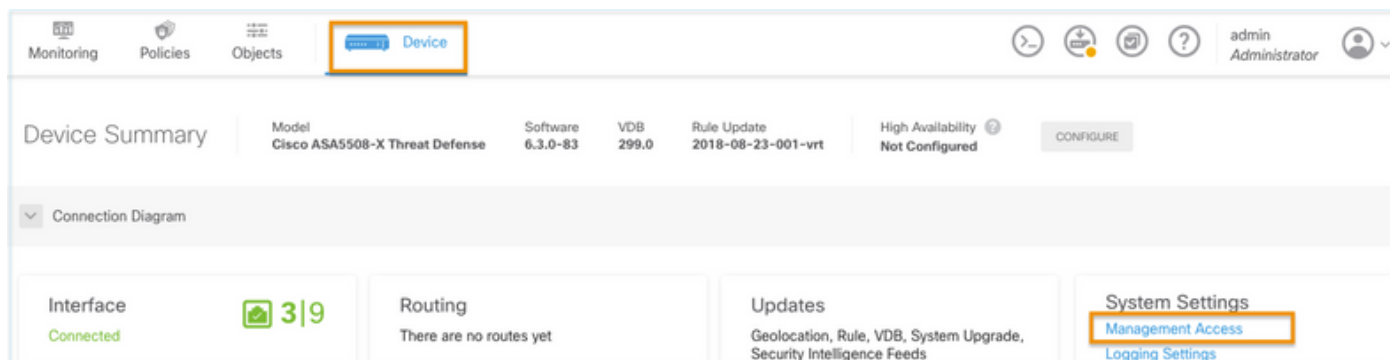
Process:

1. Admin User présente ses informations d'identification.
2. Processus d'authentification déclenché et ISE valide les informations d'identification localement ou via Active Directory.
3. Une fois l'authentification réussie, ISE envoie un paquet d'autorisation pour les informations d'authentification et d'autorisation à FDM.
4. Le compte est exécuté sur ISE et un journal en direct d'authentification réussi se produit.

## Configurer

### Configuration de FDM

Étape 1. Connectez-vous à FDM et sélectionnez Device > System Settings > Management Access



Étape 2. Créer un groupe de serveurs RADIUS

The screenshot displays the Cisco Meraki dashboard 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 'Device Summary' and 'Management Access' (labeled 3). Under 'Management Access', there are tabs for 'AAA Configuration' (highlighted with an orange box and labeled 3), 'Management Interface', and 'Data Interfaces'. The 'AAA Configuration' tab is active, showing a section for 'HTTPS Connection' and 'Server Group for Management/REST API' (labeled 4). Below this, a table with a 'Filter' header (highlighted with an orange box) lists 'LocalIdentitySource' with a checked status. At the bottom, a button labeled 'Create New RADIUS Server Group' is highlighted with an orange box and labeled 5.

Étape 3. Créer un nouveau serveur 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

Étape 4. Ajouter un serveur RADIUS au groupe de serveurs RADIUS



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

## Étape 6. Enregistrez la 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

*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

## Configuration ISE

Étape 1. Icône Naviguer jusqu'à trois lignes  situé dans l'angle supérieur gauche et sélectionnez **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
------	---------	--------------	----------	------	-------------

Étape 2. Cliquez sur le bouton **+Add** et définissez Network Access Device Name et IPAddress, puis cochez la case RADIUS et définissez un secret partagé. Sélectionner sur **envoi**

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

Network Devices

Default Device

Device Security Settings

## Network Devices

Selected 0 Total 1

Edit + Add Duplicate Import Export Generate PAC Delete

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

Étape 3. Icône Naviguer jusqu'à trois lignes  situé dans l'angle supérieur gauche et sélectionnez **Administration > Identity Management > Groups**

Administration - Identity Management

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

## User Identity Groups

Identity Groups

EQ

< [Icon] [Icon]

> Endpoint 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

Étape 4. Sélectionnez sur Groupes d'identités d'utilisateurs et cliquez sur **+bouton Ajouter**. Définissez un nom et sélectionnez sur **Soumettre**

Cisco ISE

Administration - Identity Management

Evaluation Mode 89 Days

IdentitiesGroupsExternal Identity SourcesIdentity Source SequencesSettings

Identity Groups

EQ

<

>

Endpoint Identity Groups

User Identity Groups

User Identity Groups > New User Identity Group

Identity Group

\* NameFDM\_admin

Description

SubmitCancel

## User Identity Groups

Selected 0 Total 2

EditAddDeleteImportExportQuick Filter

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

Cisco ISE

Administration - Identity Management

Evaluation Mode 89 Days

IdentitiesGroupsExternal Identity SourcesIdentity Source SequencesSettings

Identity Groups

EQ

<

>

Endpoint Identity Groups

User Identity Groups

User Identity Groups > New User Identity Group

Identity Group

\* NameFDM\_ReadOnly

Description

SubmitCancel

**Remarque :** dans cet exemple, les groupes d'identités FDM\_Admin et FDM\_ReadOnly créés, vous pouvez répéter l'étape 4 pour chaque type d'utilisateur Admin utilisé sur FDM.

**Étape 5.** Accédez à l'icône de trois lignes située dans le coin supérieur gauche et sélectionnez **Administration > Identity Management > Identities**. Sélectionnez on **+Add** et définissez le nom d'utilisateur et le mot de passe, puis sélectionnez le groupe auquel l'utilisateur appartient. Dans cet exemple, les utilisateurs fdm\_admin et fdm\_readonly ont été créés et affectés respectivement au groupe FDM\_Admin et 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	fdm_admin				FDM_admin	
<input type="checkbox"/>	<input checked="" type="checkbox"/> Enabled	fdm_readonly				FDM_ReadOnly	

**Étape 6.** Sélectionnez l'icône des trois lignes située dans l'angle supérieur gauche et accédez à **Stratégie > Éléments de stratégie > Résultats > Autorisation > Profils d'autorisation**, sélectionnez **+Ajouter**, définissez un nom pour le **profil d'autorisation**. Sélectionnez **Radius Service-type** et sélectionnez **Administrative**, puis sélectionnez **Cisco-av-pair** et collez le rôle que l'utilisateur admin obtient, dans ce cas, l'utilisateur reçoit un privilège admin complet (fdm.userrole.authority.admin). Sélectionnez sur **Soumettre**. Répétez cette étape pour chaque rôle, utilisateur en lecture seule configuré comme un autre exemple dans ce 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

**Remarque** : assurez-vous que l'ordre de la section des attributs avancés est identique à celui de l'exemple d'image afin d'éviter un résultat inattendu lors de la connexion avec l'interface graphique et l'interface de ligne de commande.

**Étape 8.** Sélectionnez l'icône des trois lignes et accédez à Policy > Policy Sets. Sélectionner sur

 situé sous le titre Jeux de stratégies, définissez un nom et sélectionnez le bouton + au milieu pour ajouter une nouvelle condition.

**Étape 9.** Dans la fenêtre Condition, sélectionnez pour ajouter un attribut, puis sélectionnez sur **Network Device** Icon suivi de Network access device IP address. Sélectionnez **Attribute Value** et ajoutez l'adresse IP FDM. Ajoutez une nouvelle condition et sélectionnez sur **Network Access** suivi de Protocol option, sélectionnez sur **RADIUS** et sélectionnez sur Use once done.

Cisco ISE 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
+	FTD_FDM_Radius_Access		AND	Network Access-Device IP Address EQUALS 10.122.111.212 Network Access-Protocol EQUALS RADIUS	Default Network Access		
+	Default	Default policy set		Default Network Access	0		

Reset Save

Étape 10. Dans la section Autoriser les protocoles, sélectionnez **Device Default Admin**. Sélectionner sur **Enregistrer**


Cisco ISE 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
+	FTD_FDM_Radius_Access		AND	Network Access-Device IP Address EQUALS 10.122.111.212 Network Access-Protocol EQUALS RADIUS	Default Network Access		
+	Default	Default policy set		Default Network Access	0		

Reset Save

Étape 11. Sélectionnez sur la flèche droite de l'ensemble de stratégies pour définir les stratégies d'authentification et d'autorisation

Étape 12. Sélectionner sur  situé sous le titre Authentication Policy, définissez un nom et sélectionnez le signe + au milieu pour ajouter une nouvelle condition. Dans la fenêtre Condition, sélectionnez pour ajouter un attribut, puis sélectionnez sur Network Device Icon suivi de Network access device IP address. Sélectionnez sur Attribute Value et ajoutez l'adresse IP FDM. Sélectionnez sur Utiliser une fois terminé

Étape 13. Sélectionnez Internal Users comme magasin d'identités et sélectionnez on Enregistrer


Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
			Internal Users		
			> Options		

+	FDM_Users	Network Access-Device IP Address EQUALS 10.122.111.212			
---	-----------	--	--	--	--

**Remarque** : le magasin d'identités peut être remplacé par un magasin AD si ISE est joint à Active Directory.

Étape 14. Sélectionner sur  situé sous le titre de la stratégie d'autorisation, définissez un nom et sélectionnez le signe + au milieu pour ajouter une nouvelle condition. Dans la fenêtre Condition, sélectionnez pour ajouter un attribut, puis cliquez sur l'icône Identity Group suivie de Internal User:Identity Group. Sélectionnez le groupe FDM\_Admin, sélectionnez l'option AND avec NEW pour ajouter une nouvelle condition, sélectionnez l'icône de port suivie de RADIUS NAS-Port-Type:Virtual et sélectionnez 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

AND

Radius-NAS-Port-Type

Equals Virtual

+ NEW AND OR

Set to 'Is not'

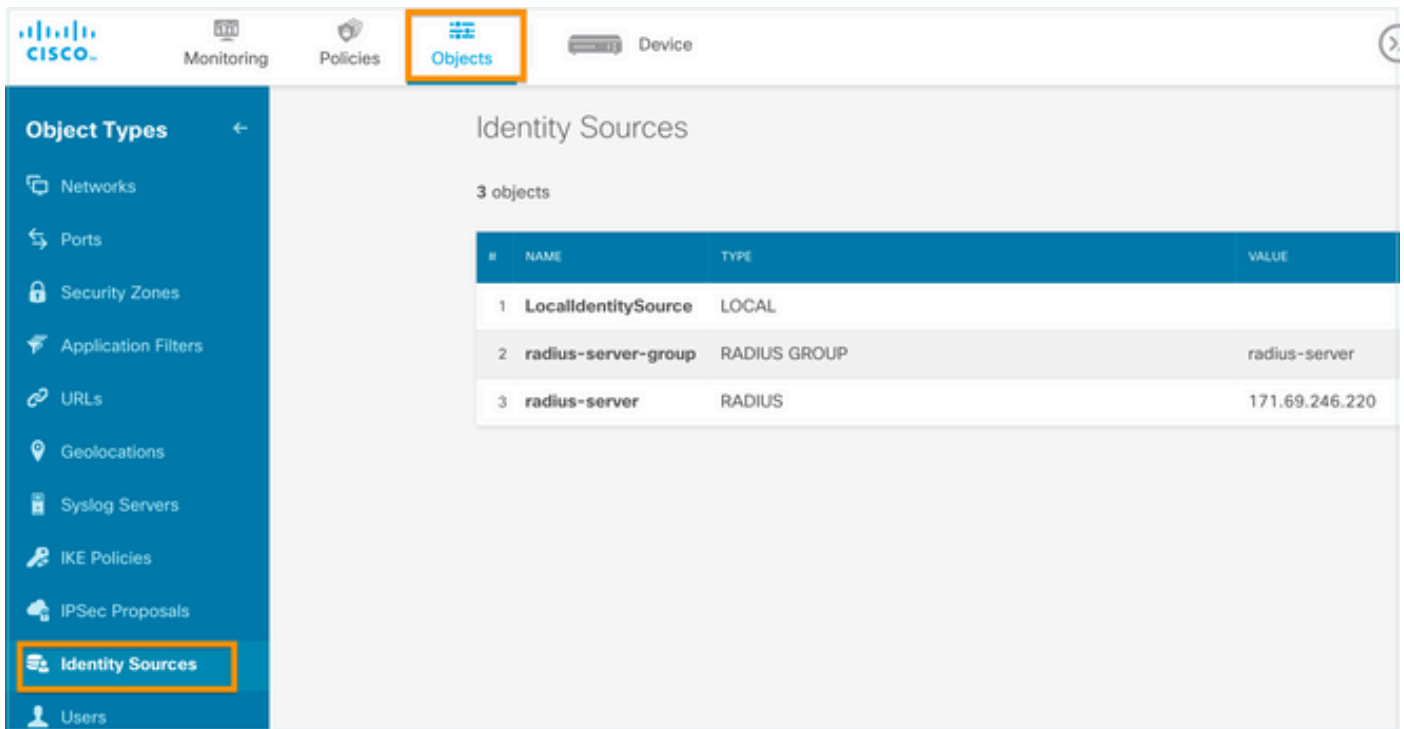
Duplicate Save

Étape 15. Sous Profils, sélectionnez le profil créé à l'étape 6, puis cliquez sur Enregistrer

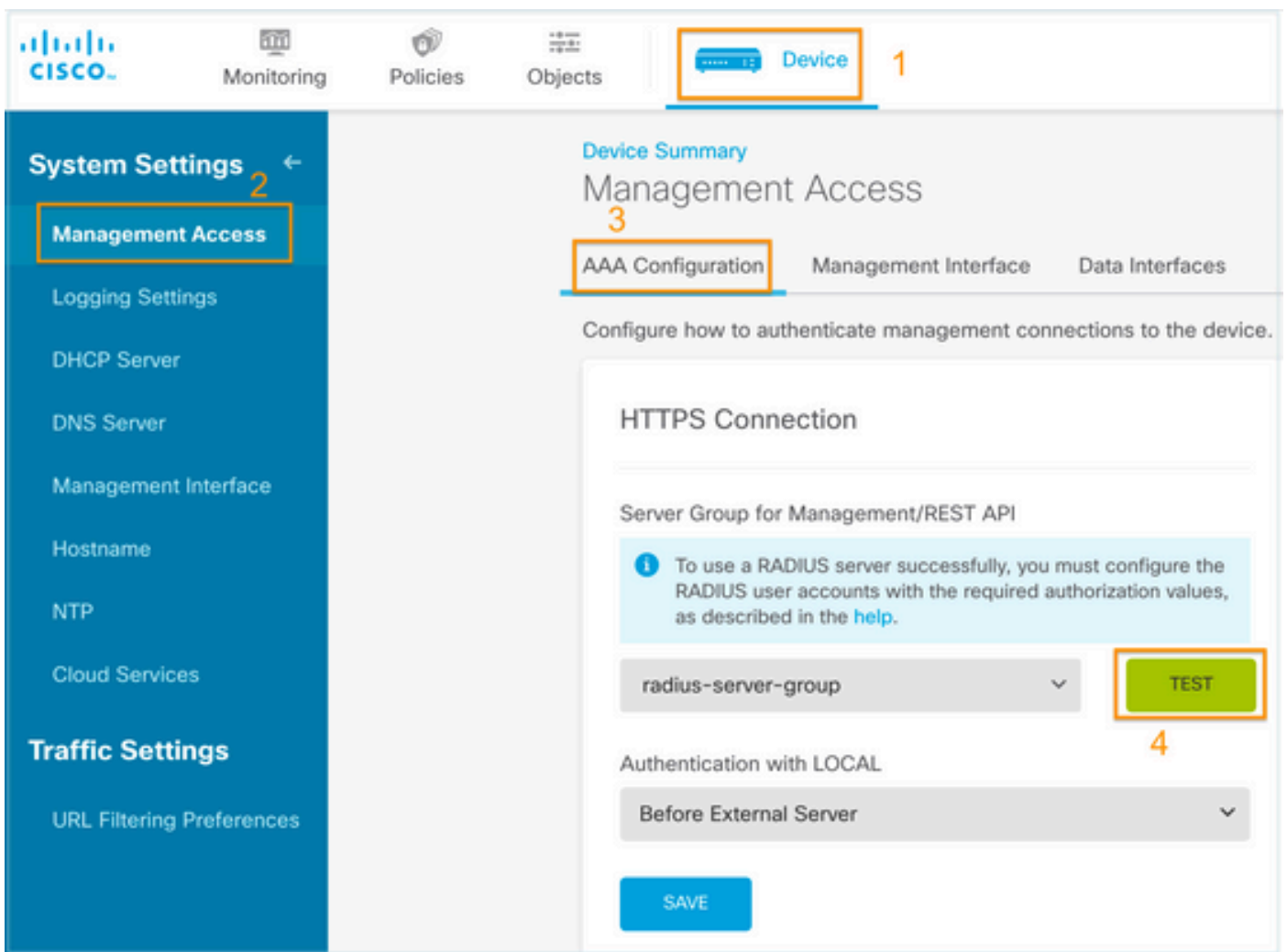
Répétez les étapes 14 et 15 pour le groupe FDM\_ReadOnly







Étape 2. Accédez à Device > System Settings > Management Access tab et sélectionnez le bouton TEST



Étape 3. Insérez les informations d'identification de l'utilisateur et sélectionnez le bouton 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.*

**Étape 4.** Ouvrez une nouvelle fenêtre de navigateur et tapez [https://FDM\\_ip\\_Address](https://FDM_ip_Address), utilisez le nom d'utilisateur et le mot de passe fdm\_admin créés à l'étape 5 sous la section de configuration ISE.



# Firepower Device Manager

**Successfully logged out**

fdm\_admin

.....

LOG IN

La réussite de la tentative de connexion peut être vérifiée sur les journaux en direct ISE RADIUS

Cisco ISE

Operations · RADIUS

Evaluation Mode 79 Days

Live Logs

Live Sessions

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

Never

Latest 20 records

Last 3 hours

Refresh

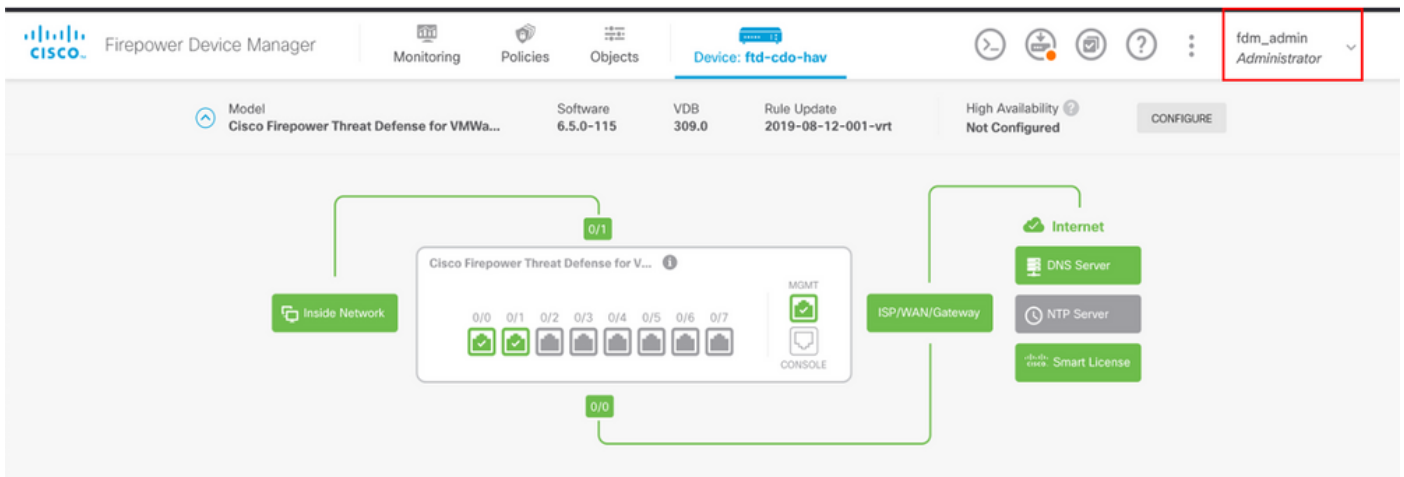
Reset Repeat Counts

Export To

Filter

Time	Status	Details	Repea...	Identity	Authentication Policy	Authorization Policy	Authorization Profiles
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

L'utilisateur Admin peut également être consulté sur FDM dans l'angle supérieur droit



## CLI de Cisco Firepower Device Manager (utilisateur administrateur)

```
[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)

[> █
```

## Dépannage

Cette section fournit les informations que vous pouvez utiliser pour dépanner votre configuration.

### Validation des communications avec l'outil de vidage TCP sur ISE

**Étape 1.** Connectez-vous à ISE et sélectionnez l'icône à trois lignes située dans le coin supérieur

gauche et accédez à **Operations > Troubleshoot > Diagnostic Tools**.

**Étape 2.** Sous General tools, sélectionnez on TCP Dumps, puis sélectionnez **Add+**. Sélectionnez Nom d'hôte, Nom de fichier d'interface réseau, Référentiel et éventuellement un filtre pour collecter uniquement le flux de communication d'adresse IP FDM. Sélectionner sur **Enregistrer et exécuter**

The screenshot shows the Cisco ISE web interface. On the left is a navigation menu with 'Diagnostic Tools' selected. The main area is titled 'TCP Dump > New' and 'Add TCP Dump'. It contains several configuration fields: '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 which is unchecked. Each field has a blue information icon to its right.

**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

**Étape 3.** Connectez-vous à l'interface utilisateur FDM et tapez les informations d'identification d'administrateur.

**Étape 4.** Sur ISE, sélectionnez le bouton **Stop** et vérifiez que le fichier pcap a été envoyé au référentiel défini.

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.ciscoe.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

Étape 5. Ouvrez le fichier pcap pour valider la bonne communication entre FDM et 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_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..

```

Si aucune entrée n'est affichée sur le fichier pcap, validez les options suivantes :

1. L'adresse IP ISE correcte a été ajoutée à la configuration FDM
2. Si un pare-feu se trouve au milieu, vérifiez que le port 1812-1813 est autorisé.
3. Vérifier la communication entre ISE et FDM

### Validation des communications avec le fichier généré par FDM.

Dans le fichier de dépannage généré à partir de la page Périphérique FDM, recherchez les mots-clés suivants :

- AideConnexionMotDePasseFdm
- GestionUtilisateurDéfautNGFWD
- GestionnaireÉtatSourceIdentitéAAA
- GestionnaireSourceIdentitéRadius

Tous les journaux associés à cette fonctionnalité sont disponibles à l'adresse /var/log/cisco/ngfw-onbox.log

Références:

[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)



# Problèmes courants

Cas 1 - L'authentification externe ne fonctionne pas

- Vérifiez la clé secrète, le port ou le nom d'hôte
- Mauvaise configuration des AVP sur RADIUS
- Le serveur peut être en « Dead Time »

Cas 2 : échec du test IdentitySource

- Vérifiez que les modifications apportées à l'objet sont enregistrées
- Vérifiez que les informations d'identification sont correctes

## Limites

- FDM autorise un maximum de 5 sessions FDM actives.
- La création de la 6ème session entraîne la révocation de la 1ère session
- Le nom de RadiusIdentitySourceGroup ne peut pas être « LocalIdentitySource »
- 16 RadiusIdentitySources max. pour un RadiusIdentitySourceGroup
- Une mauvaise configuration des AVP sur RADIUS entraîne le refus de l'accès à FDM

## Q&R

Q : Cette fonction fonctionne-t-elle en mode Évaluation ?

R : Oui

Q : Si deux utilisateurs en lecture seule se connectent, où ont accès à l'utilisateur en lecture seule 1, et ils se connectent à partir de deux navigateurs diff. Comment cela se verra-t-il ? Que se passera-t-il ?

R : Les deux sessions utilisateur sont affichées dans la page des sessions utilisateur actives avec le même nom. Chaque entrée affiche une valeur individuelle pour l'horodatage.

Q : Quel est le comportement du serveur RADIUS externe qui fournit un refus d'accès par rapport à "aucune réponse" si l'authentification locale est configurée en 2e position ?

R : Vous pouvez essayer l'authentification LOCALE même si vous obtenez un refus d'accès ou aucune réponse si l'authentification locale est configurée en 2e position.

Q : Comment ISE différencie une demande RADIUS pour la connexion d'administrateur d'une demande RADIUS pour authentifier un utilisateur VPN RA

R : ISE ne fait pas la différence entre une requête RADIUS pour les utilisateurs Admin et RAVPN. FDM examine l'attribut cisco-avpair pour déterminer l'autorisation d'accès administrateur. ISE envoie tous les attributs configurés pour l'utilisateur dans les deux cas.

Q : Cela signifie que les journaux ISE ne peuvent pas faire la différence entre une connexion d'administrateur FDM et le même utilisateur accédant au VPN d'accès à distance sur le même périphérique. Y a-t-il un attribut RADIUS transmis à ISE dans la demande d'accès sur laquelle

ISE peut appuyer ?

R : Voici les attributs RADIUS en amont qui sont envoyés du FTD à ISE pendant l'authentification RADIUS pour RAVPN. Ils ne sont pas envoyés dans le cadre de la demande d'accès de gestion d'authentification externe et peuvent être utilisés pour différencier une connexion d'administration FDM de la connexion utilisateur RAVPN.

146 - Nom du groupe de tunnels ou nom du profil de connexion.

150 - Client Type (Valeurs applicables : 2 = AnyConnect Client SSL VPN, 6 = AnyConnect Client IPsec VPN (IKEv2).

151 - Session Type (Valeurs applicables : 1 = AnyConnect Client SSL VPN, 2 = AnyConnect Client IPsec VPN (IKEv2).

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.