

# RADIUSを使用したISEでのFDM外部認証および認可の設定

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[相互運用性](#)

[ライセンス](#)

[背景説明](#)

[ネットワーク図](#)

[設定](#)

[FDM による構成](#)

[ISE の設定](#)

[確認](#)

[トラブルシューティング](#)

[一般的な問題](#)

[制限](#)

[Q&A](#)

## 概要

このドキュメントでは、GUIとCLIの両方のアクセスのために、Cisco Firepower Device Manager(FDM)を管理者ユーザ認証のIdentity Services Engine(ISE)とRADIUSプロトコルに統合する手順について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Firepower Device Manager(FDM)
- Identity Services Engine ( ISE )
- RADIUS プロトコル

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Firepower Threat Defense(FTD)デバイス、すべてのプラットフォームFirepower Device Manager(FDM)バージョン6.3.0+
- ISE バージョン 3.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 相互運用性

- ユーザロールが設定されたユーザを持つRADIUSサーバ
- ユーザロールは、cisco-av-pairを使用してRADIUSサーバ上で設定する必要があります
- Cisco-av-pair = fdm.userrole.authority.admin
- ISEはRADIUSサーバとして使用可能

## ライセンス

特定のライセンス要件はありません。基本ライセンスで十分です

## 背景説明

この機能を使用すると、RADIUSを使用して外部認証を設定し、それらのユーザに対して複数のユーザロールを設定できます。

3つのシステム定義ユーザロールによる管理アクセスのRADIUSサポート：

- 読み取り専用
- READ\_WRITE ( アップグレード、リストアなどのシステム・クリティカルなアクションを実行できない )
- ADMIN

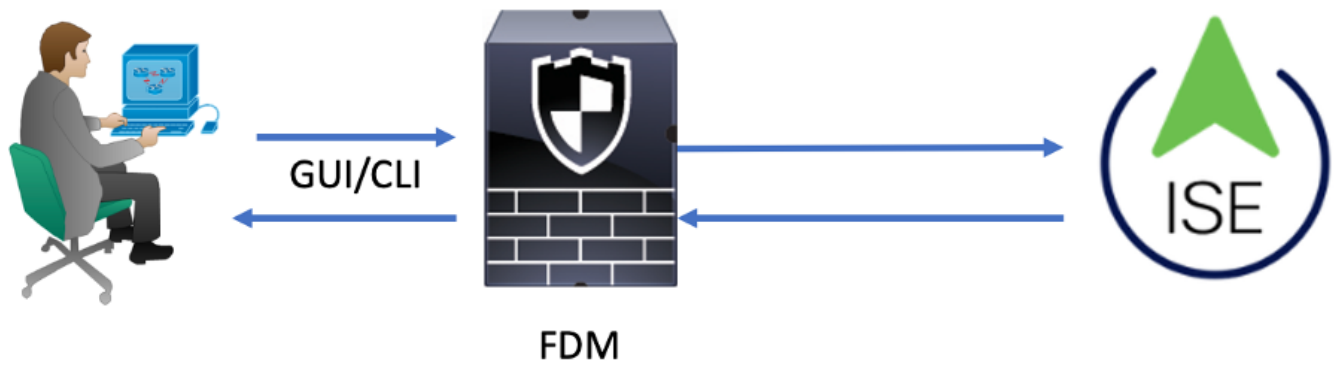
RADIUSサーバの設定をテストし、アクティブなユーザセッションを監視してユーザセッションを削除する機能があります。

この機能は、FDMバージョン6.3.0で実装されました。6.3.0より前のリリースでは、FDMは1人のユーザ(admin)のみをサポートしていました。

デフォルトでは、Cisco Firepower Device Manager(FDM)はローカルでユーザを認証および許可します。RADIUSプロトコルを介してCisco Identity Service Engineを使用できる中央集中型の認証および許可方式が必要です。

## ネットワーク図

次の図は、ネットワークトポロジの例を示しています



プロセス：

1. 管理者ユーザがクレデンシャルを入力します。
2. 認証プロセスがトリガーされ、ISEがクレデンシャルをローカルまたはActive Directory経由で検証します。
3. 認証が成功すると、ISEは認証および許可情報の許可パケットをFDMに送信します。
4. アカウントはISEで実行され、認証の成功のライブログが発生します。

## 設定

### FDM による構成

ステップ 1：FDMにログインし、「デバイス」>「システム設定」>「管理アクセス」タブに移動します

The screenshot shows the FDM web interface. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device' (highlighted with an orange box). The user is logged in as 'admin Administrator'. The main content area shows 'Device Summary' for a Cisco ASA5508-X Threat Defense. Below this, there are sections for 'Interface' (3/9), 'Routing', 'Updates', and 'System Settings'. The 'System Settings' section has a sub-tab 'Management Access' highlighted with an orange box.

ステップ 2：新しいRADIUSサーバグループの作成

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

ステップ 3 : 新しいRADIUSサーバの作成

# Add RADIUS Server Group



Name

Dead Time i

10

minutes

0-1440

Maximum Failed Attempts

3

1-5

RADIUS Server

i 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 Authentication Port

10.81.127.185 1812

Timeout ⓘ

10 seconds

1-300

Server Secret Key

●●●●●●●●

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

TEST CANCEL OK

ステップ 4 : RADIUSサーバグループへのRADIUSサーバの追加

### Add RADIUS Server Group

Name 3

radius-server-group

Dead Time ⓘ  minutes 0-1440

Maximum Failed Attempts  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

ステップ 5 : 作成したグループを[Server Group for Management]として選択します

### 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**

## 手順 6 : 設定の保存

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 の設定

ステップ 1 : 3行アイコンに移動  左上隅にある [Administration] > [Network Resources] > [Network Devices] を選択します。



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

ステップ 2 : +Addボタンを選択し、Network Access Device Name ( NAD ; ネットワークアクセスデバイス名 ) とIPアドレスを定義し、次にRADIUSチェックボックスをオンにして、共有秘密を定義します。送信時に選択

Cisco ISE   Administration · Network Resources   Evaluation Mode 89 Days

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

Network Devices

Default Device

Device Security Settings

Network Devices

Name

Description

IP Address

Device Profile

Model Name

Software Version

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol   RADIUS

Shared Secret   .....   Show

Use Second Shared Secret   ⓘ

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	

ステップ 3 : 3行アイコンに移動  
[Groups]を選択します。



左上隅にある[Administration] > [Identity Management] >

Administration - Identity Management

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

### 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

ステップ 4 : [User Identity Groups]を選択し、[on +Add] ボタンを選択します。名前を定義し、[Submit]を選択します。

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

**注意：**この例では、FDM\_AdminおよびFDM\_ReadOnlyのIDグループが作成されています。FDMで使用する管理者ユーザーのタイプごとに手順4を繰り返すことができます。

**ステップ 5：**左上隅にある3行アイコンに移動し、[Administration] > [Identity Management] > [Identities] を選択します。+Addを選択してユーザ名とパスワードを定義し、ユーザが属するグループを選択します。この例では、fdm\_adminおよびfdm\_readonlyユーザーが作成され、それぞれFDM\_AdminおよびFDM\_ReadOnlyグループに割り当てられています。

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

Edit + Add Change Status Import Export Delete Duplicate

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

手順 6 : 左上隅にある3行のアイコンを選択し、[Policy] > [Policy Elements] > [Results] > [Authorization] > [Authorization Profiles] に移動し、[on] +[Add] を選択して、認可プロファイルの名前を定義します。Radius Service-typeを選択し、Administrativeを選択してからCisco-av-pairを選択し、adminユーザが取得するルールを貼り付けます。この場合、ユーザは完全なadmin権限(fdm.userrole.authority.admin)を受け取ります。[Submit] を選択します。このドキュメントの別の例として設定されている読み取り専用ユーザのルールごとに、この手順を繰り返します。

- Authentication >
- Authorization ▾
- Authorization Profiles
- Downloadable ACLs
- Profiling >
- Posture >
- Client Provisioning >

Authorization Profiles > New Authorization Profile

### Authorization Profile

\* Name

Description

\* Access Type

Network Device Profile

Service Template

Track Movement  ⓘ

Agentless Posture  ⓘ

Passive Identity Tracking  ⓘ

### Advanced Attributes Settings

⋮	<input type="text" value="Radius:Service-Type"/>	=	<input type="text" value="Administrative"/>	-
⋮	<input type="text" value="Cisco:cisco-av-pair"/>	=	<input type="text" value="fdm.userrole.authority.admin"/>	- +

### Attributes Details

Access Type = ACCESS\_ACCEPT

Service-Type = 6

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

## Advanced Attributes Settings

The screenshot shows two attribute assignments in a list:

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

The second assignment is highlighted with a blue underline and a green plus icon to its right.

## Attributes Details

```
Access Type = ACCESS_ACCEPT
Service-Type = 7
cisco-av-pair = fdm.userrole.authority.ro
```

注：GUIおよびCLIでログインする際に予期しない結果が生じるのを防ぐため、高度な属性のセクションの順序は、イメージの例と同じにしてください。

ステップ 8：3行アイコンを選択し、[Policy] > [Policy Sets] に移動します。オンを選択

 [Policy Sets] タイトルの下にあるボタンで名前を定義し、中央にある[+] ボタンを選択して新しい条件を追加します。

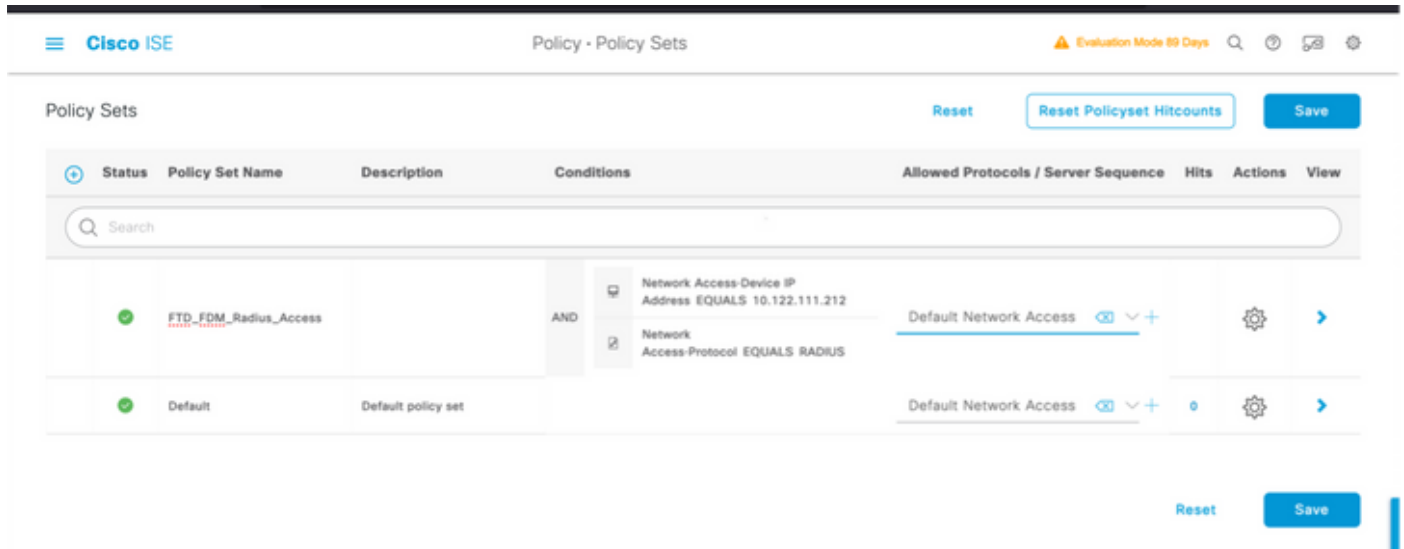
ステップ 9：[Condition] ウィンドウで、属性を選択して追加し、[Network Device] アイコンを選択してから、[Network access device IP address] を選択します。[Attribute Value] を選択し、FDMのIPアドレスを追加します。新しい条件を追加し、[Network Access] を選択してから [Protocol] オプションを選択し、[on RADIUS] を選択して、[Use once done] を選択します。

The screenshot shows the Cisco ISE Policy Sets configuration page. The page title is "Policy - Policy Sets". There is a search bar and a "Search" button. The main table lists policy sets:


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

At the bottom right, there are "Reset" and "Save" buttons.

ステップ 10 : [allow protocols]セクションで、[Device Default Admin] を選択します。保存時に選択




ステップ 11右矢印を選択します。 ➤ 認証および認可ポリシーを定義するポリシーセットのアイコン

ステップ 12オンを選択  [Authentication Policy title]の下にある名前を定義し、中央の[+]を選択して新しい条件を追加します。[Condition]ウィンドウで、属性を選択して追加し、[Network Device] アイコンを選択してから、[Network access device IP address]を選択します。 [Attribute Value] を選択し、FDMのIPアドレスを追加します。 [Use once done] を選択します。

ステップ 13[Identity Store]として[Internal Users] を選択し、[on]を選択します。保存します。



注:ISEがActive Directoryに参加している場合は、IDストアをADストアに変更できます。

ステップ 14 : オンを選択  [Authorization Policy title]の下にある名前を定義し、中央の[+]を選択して新しい条件を追加します。[Condition]ウィンドウで、属性を選択して追加し、[Identity Group] アイコンを選択してから、[Internal User:Identity Group] を選択します。FDM\_Adminグループを選択し、「AND」オプションと「NEW」オプションを選択して新しい条件を追加し、「on port」アイコンを選択してから「RADIUS NAS-Port-Type:Virtual」を選択して「on Use」を選択します。

# Conditions Studio

## Library

Search by Name



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

## Editor

IdentityGroup-Name  
Equals User Identity Groups:FDM\_admin

Radius-NAS-Port-Type  
Equals Virtual

AND

NEW AND OR

Set to 'Is not'

Duplicate Save

ステップ 15 : [Profiles]で、ステップ6で作成したプロファイルを選択し、[Save] を選択します

FDM\_ReadOnlyグループに対してステップ14と15を繰り返します

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

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

ステップ 16 ( オプション ) : 左上隅にある3行のアイコンに移動し、[Administration] > [System] > [Maintenance] > [Repository] を選択し、[on +Add] を選択して、トラブルシューティング用にTCPダンプファイルの保存に使用するリポジトリを追加します。

ステップ 17 ( オプション ) : リポジトリ名、プロトコル、サーバ名、パス、およびクレデンシャルを定義します。[Submit] を選択します。



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 .....

## 確認

ステップ1:[Objects] > [Identity Sources]タブに移動し、RADIUSサーバとグループサーバの設定を確認します。

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

ステップ2 : [Device] > [System Settings] > [Management Access] タブに移動し、[TEST] ボタンを選択します

The screenshot displays the Cisco management interface. At the top, there is a navigation bar with icons for Monitoring, Policies, Objects, and Device (1). On the left, a sidebar contains 'System Settings' (2) with 'Management Access' highlighted. The main area shows 'Device Summary Management Access' (3) with tabs for 'AAA Configuration' (3), 'Management Interface', and 'Data Interfaces'. The 'AAA Configuration' tab is active, showing a configuration page for 'HTTPS Connection'. A dropdown menu is set to 'radius-server-group', and a green 'TEST' button (4) is visible. A 'SAVE' button is at the bottom of the configuration area.

ステップ3 : ユーザクレデンシャルを挿入し、[TEST] ボタンを選択します

## 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.*

ステップ 4 : 新しいウィンドウ・ブラウザを開き、<https://FDM ip Address>と入力し、手順5のISE構成セクションで作成したfdm\_adminユーザー名とパスワードを使用します。



# Firepower Device Manager

**Successfully logged out**

fdm\_admin

.....|

LOG IN

ログインの成功は、ISE RADIUSライブログで確認できます

Cisco ISE Operations · RADIUS Evaluation Mode 79 Days

Live Logs Live Sessions

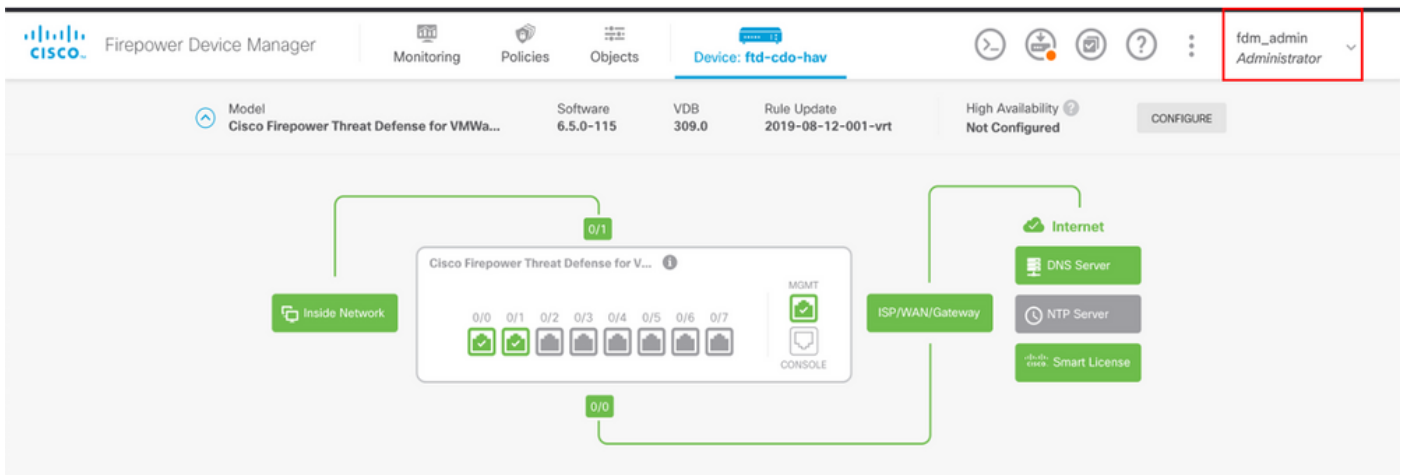
Click here to do visibility setup Do not show this again.

Never Latest 20 records Last 3 hours

Refresh Reset Repeat Counts Export To Filter

Time	Status	Details	Repea...	Identity	Authentication Policy	Authorization Policy	Authorization Profiles
Jul 06, 2021 04:54:12.41...				fdm_admin	FTD_FDM_Radius_Access >> FDM_...	FTD_FDM_Radius_Access >> FTD_FDM...	FDM_Profile_Admin

管理者ユーザーは、右上隅のFDMでも確認できます



## Cisco Firepower Device Manager(FDM)CLI ( 管理ユーザ )

```
[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)

[> █
```

## トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を説明します。

### ISEのTCPダンプツールによる通信検証

ステップ 1 : ISEにログインし、左上隅にある3行のアイコンを選択して、[Operations] >

[Troubleshoot] > [Diagnostic Tools] に移動します。

ステップ 2 : [General tools]で[on TCP Dumps]を選択し、次に[Add+] を選択します。「ホスト名」、「ネットワーク・ インタフェース・ ファイル名」、「リポジトリ」、およびオプションで FDM IPアドレス通信フローのみを収集するフィルタを選択します。[Save and Run] を選択します。

The screenshot shows the Cisco ISE web interface for configuring a TCP Dump. The left sidebar contains a menu with 'General Tools', 'TCP Dump', and 'TrustSec Tools'. The 'TCP Dump' section is active. The main content area is titled 'TCP Dump > New' and 'Add TCP Dump'. It includes the following fields and options:

- 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 it, 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 spinner control set to '10' with 'Mb' as the unit.
- Limit to**: A spinner control set to '1' with 'File(s)' as the unit.
- Time Limit**: A spinner control set to '5' with 'Minute(s)' as the unit.
- Promiscuous Mode**: An unchecked checkbox.

ステップ 3 : FDM UIにログインし、管理者のログイン情報を入力します。

ステップ 4 : ISEで[Stop] ボタンを選択し、pcapファイルが定義されたリポジトリに送信されたことを確認します。

Cisco ISE Operations - Troubleshoot Evaluation Mode 79 Days

Diagnostic Tools Download Logs Debug Wizard

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

### General Tools

- RADIUS Authentication Troubl...
- Execute Network Device Com...
- Evaluate Configuration Validat...
- Posture Troubleshooting
- Agentless Posture Troublesho...
- EndPoint Debug
- TCP Dump**
- Session Trace Tests

## TCP Dump

The TCP Dump utility page is to monitor the contents of packets on a network interface and troubleshoot problems on the network as they appear

Rows/Page 1 << 1 >> Go 1 Total Rows

Refresh + Add Edit Trash Start Stop Download Filter

Host Name	Network Interface	Filter	File Name	Repository	File S...	Number o
<input type="checkbox"/> ise31.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		
<input type="checkbox"/> FDM_Tshoot.pcap	545	473	PCAP File	7/6/2021 5:21 ...	3A095B10

Total 1 file, 545 bytes

ステップ 5 : pcap ファイルを開き、FDM と ISE 間の正常な通信を検証します。

FDM\_Tshoot.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.122.111.212	10.81.127.185	RADIUS	115	Access-Request id=224
2	0.091018	10.81.127.185	10.122.111.212	RADIUS	374	Access-Accept id=224

```

> AVP: t=Class(25) l=77 val=434143533a3061353137666239334a305a746a736f524e766e616f5159744374454
> AVP: t=Vendor-Specific(26) l=50 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=68 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=64 vnd=ciscoSystems(9)
▼ AVP: t=Vendor-Specific(26) l=36 vnd=ciscoSystems(9)
  Type: 26
  Length: 36
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=30 val=fdm.userrole.authority.admin

```

```

0000  90 77 ee 2b 0e bf 00 50 56 a4 d0 f1 08 00 45 00  .w.+...P V.....E.
0010  01 68 80 34 40 00 40 11 b4 f8 0a 51 7f b9 0a 7a  .h.4@.@. ...Q...z
0020  6f d4 07 14 d1 7e 01 54 05 be 02 e0 01 4c 89 62  o.....~T .....L.b
0030  90 cc eb ae 36 16 dd 51 49 9c 15 0c ab c1 01 0b  ....6..Q I.....
0040  66 64 6d 5f 61 64 6d 69 6e 06 06 00 00 00 06 19  fdm_admin.....
0050  4d 43 41 43 53 3a 30 61 35 31 37 66 62 39 33 4a  MCACS:0a 517fb93J
0060  30 5a 74 6a 73 6f 52 4e 76 6e 61 6f 51 59 74 43  0ZtjsoRN vnaoQYtC
0070  74 45 47 74 5a 75 4c 52 59 71 54 54 72 66 45 69  tEGtZuLR YqTTrfEi
0080  58 50 57 48 75 50 71 53 45 3a 69 73 65 33 31 2f  XPwHuPqS E:ise31/
0090  34 31 34 31 31 30 35 39 32 2f 32 38 1a 32 00 00  41411059 2/28.2..

```

pcapファイルにエントリが表示されない場合は、次のオプションを検証します。

1. 右ISE IPアドレスがFDM構成に追加されました
2. ファイアウォールが中央にある場合は、ポート1812-1813が許可されていることを確認します。
3. ISEとFDM間の通信を確認します。

#### FDMで生成されたファイルとの通信検証。

FDMデバイス・ページから生成されたトラブルシューティング・ファイルで、キーワードを探します：

- FdmPasswordLoginHelper
- NGFWDefaultUserMgmt
- AAIdentitySourceStatusManager
- RadiusIdentitySource Manager

この機能に関連するすべてのログは、/var/log/cisco/ngfw-onbox.logにあります。

参照:

[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)



## 一般的な問題

ケース1：外部認証が機能していない

- secretKey、port、またはhostnameを確認します。
- RADIUSでのAVPの設定ミス
- サーバが「デッドタイム」状態になる可能性がある

ケース2:Test IdentitySource fails

- オブジェクトへの変更が保存されていることを確認します
- クレデンシャルが正しいことを確認します

## 制限

- FDMでは、最大5つのアクティブなFDMセッションが可能です。
- 6番目のセッションを作成すると、1番目のセッションが取り消されます
- RadiusIdentitySourceGroupの名前を"LocalIdentitySource"にすることはできません
- 1つのRadiusIdentitySourceGroupに対して最大16個のRadiusIdentitySources
- RADIUSでのAVPの設定ミスにより、FDMへのアクセスが拒否される

## Q&A

Q：この機能は評価モードで動作しますか。

A：はい

Q: 2人の読み取り専用ユーザがログインした場合、では読み取り専用ユーザ1にアクセスでき、2つの異なるブラウザからログインします。 どう見える？ 何が起こるか。

A：両方のユーザーのセッションが、アクティブユーザーセッションページに同じ名前で表示されます。 各エントリには、タイムスタンプの個々の値が表示されます。

Q：外部RADIUSサーバがアクセス拒否を提供するのに対し、2番目にローカル認証が設定されている場合、「応答なし」ですか。

A:2番目にローカル認証を設定している場合は、アクセス拒否または応答がない場合でも、ローカル認証を試すことができます。

Q:ISEがRA VPNユーザを認証するための管理者ログインのRADIUS要求とRADIUS要求を区別する方法

A:ISEでは、AdminユーザとRAVPNユーザのRADIUS要求は区別されません。FDMはcisco-avpair属性を参照して、Adminアクセスの許可を決定します。どちらの場合も、ISEはユーザ用に設定されたすべての属性を送信します。

Q：つまり、ISEログでは、FDM管理者ログインと、同じデバイス上のリモートアクセスVPNにアクセスしている同じユーザを区別できません。 ISEがキーを設定できるアクセス要求でISEに渡されるRADIUS属性はありますか。

A : 次に、RAVPNのRADIUS認証中にFTDからISEに送信されるアップストリームRADIUS属性を示します。これらは外部認証管理アクセス要求の一部として送信されず、FDM管理ログインとRAVPNユーザー・ログインを区別するために使用できます。

146 : トンネルグループ名または接続プロファイル名。

150:Client Type(Applicable values: 2 = AnyConnect Client SSL VPN、6 = AnyConnect Client IPsec VPN(IKEv2)。

151:Session Type(適用可能な値 : 1 = AnyConnect Client SSL VPN、2 = AnyConnect Client IPsec VPN(IKEv2)。

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。