

# ل ن ي ي ج را خ ل ا ض ي و ف ت ل ا و ة ق د ا ص م ل ا ن ي و ك ت RADIUS م ا د خ ت س ا ب ISE م ا د خ ت س ا ب FDM

## ت ا ي و ت ح م ل ا

[ة م د ق م ل ا](#)

[ة ي س ا س ا ل ا ت ا ب ل ط ت م ل ا](#)

[ت ا ب ل ط ت م ل ا](#)

[ي ن ي ب ل ا ل ي غ ش ت ل ا ة ي ل ب ا ق](#)

[ص ي خ ر ت ل ا](#)

[ة ي س ا س ا ت ا م و ل ع م](#)

[ة ك ب ش ل ل ي ط ي ط خ ت ل ا م س ر ل ا](#)

[ن ي و ك ت ل ا](#)

[FDM ن ي و ك ت](#)

[ISE ن ي و ك ت](#)

[ة ح ص ل ا ن م ق ق ح ت ل ا](#)

[ا ه ج ا ل ص ا و ا ط خ ا ل ا ف ا ش ك ت س ا](#)

[ة ع ئ ا ش ل ا ت ا ل ك ش م ل ا](#)

[د و ي ق ل ا](#)

[ة ب و ج ا و ة ل ئ س ا](#)

## ة م د ق م ل ا

Cisco Firepower Device Manager (FDM) م Identity Services Engine (ISE) ل و ك و ت و ر ب ع م ل و و س م ل ا ي م د خ ت س م ة ق د ا ص م ل ا ا ذ ه ف ص ي ة ه ج ا و ي ل ل و ص و ل ل RADIUS ل و ك و ت و ر ب ع م ل و و س م ل ا ي م د خ ت س م ة ق د ا ص م ل ا ا ذ ه ف ص ي ر م ا و ا ل ر ط س ة ه ج ا و و (GUI) ة ي م و س ر ل ا م د خ ت س م ل ا (CLI).

## ة ي س ا س ا ل ا ت ا ب ل ط ت م ل ا

### ت ا ب ل ط ت م ل ا

ة ي ل ا ت ل ا ع ي ض ا و م ل ا ب ة ف ر ع م ك ي د ل ن و ك ت ن ا ب Cisco ي ص و ت:

- Firepower (FDM) ز ا ه ج ر ي د م
- (ISE) ة ي و ه ل ا ت ا م د خ ك ر ح م
- RADIUS ل و ك و ت و ر ب

### ة م د خ ت س م ل ا ت ا ن و ك م ل ا

ة ي ل ا ت ل ا ة ي د ا م ل ا ت ا ن و ك م ل ا و ج م ا ر ب ل ا ت ا ر ا د ص ل ا ي ل ل د ن ت س م ل ا ا ذ ه ي ف ة د ر ا و ل ا ت ا م و ل ع م ل ا د ن ت س ت:

- ر ي د م ن م 6.3.0+ ر ا د ص ل ا ة ي س ا س ا ل ا ة م ظ ن ا ل ا ع ي م ج ، Firepower (FTD) د ي د ه ت ن ع ع ا ف د ل ا ز ا ه ج FirePOWER (FDM) ة ز ه ج ا
- 3.0 ر ا د ص ل ا ISE

ة ص ا خ ة ي ل م ع م ة ئ ي ب ي ف ة د و ج و م ل ا ة ز ه ج ا ل ا ن م د ن ت س م ل ا ا ذ ه ي ف ة د ر ا و ل ا ت ا م و ل ع م ل ا ع ا ش ن ا م ت

تتأكد إذا (يضايرتفا) حوسمم نيوكتب دننسملا اذف ةمدختسُملا ةزهجالا عيمج تأدب رمايال لمحتحملا ريثأتلل كمهف نم دكأف، ليغشلتل ديقتكتكبش

## ينيبلا ليغشلتلا ةيلباق

- نيمدختسم راودأب مهنيوكت مت نيمدختسمب دوزملا RADIUS مداخل
- Cisco-AV ةزهجالا جوز مداخلتساب RADIUS مداخل ع نيمدختسملا راودأ نيوكتب جي
- Cisco-av-pair = fdm.userRole.authority.admin
- RADIUS مداخلك ISE مداخلتسا نكمي

## صيخرتلا

فاكيساسألا صيخرتلا، ددحم صيخرت بلطتي ال

## ةيساسأ تامولعم

نيمدختسملا راودأو RADIUS مداخلتساب ةيجراخلا ةقداصملا نيوكت العالمعلل ةزيملا هذه حيتت نيمدختسملا ةالؤهل ةددعتملا

نيمدختسملا ماطنلا ةطساوب ةددحم راودأ 3 لالخنم ةرادإلا يلا لوصولل RADIUS معد

- Read\_Only
- READ\_WRITE (امو ةداعتسال او ةيقرتلا لثم ماطنلل ةماهلا تاءارجالا ذيفنت نكمي ال) (كلذ يلا)
- لوؤسملا

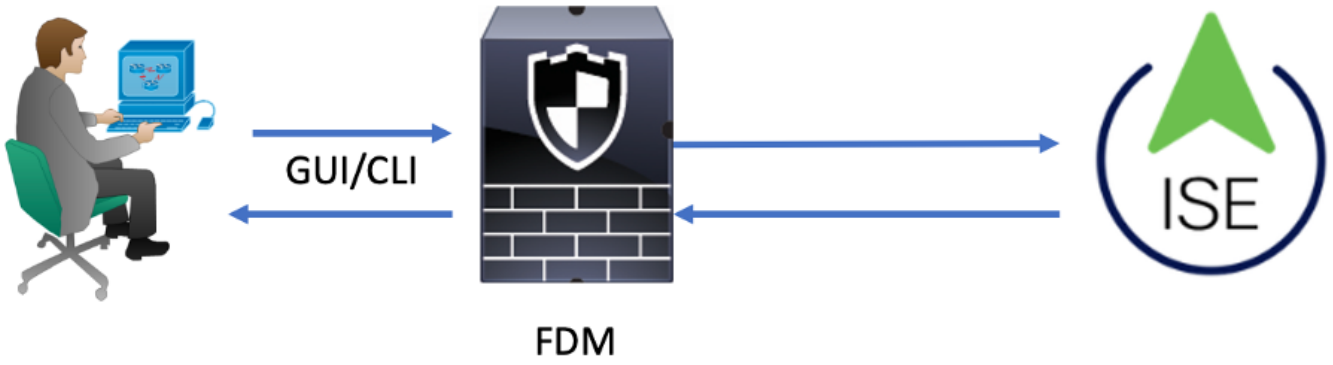
فذحو ةطاشنلا مداخلتسملا لمع تاسلج ةبقارمو RADIUS مداخل نيوكت رابختلا يلع ةردقلا كانه مداخلتسملا لمع ةسلج

مداخلتسملا معد FDM يدلناك، 6.3.0 رادصإ لبق FDM. نم 6.3.0 رادصإلا يفة زيملا ذيفنت مت طقف (لوؤسم) دحاو

نيمدختسملا ةقداصمب Cisco نم FirePOWER ةزهجالا ريديم موقبي، يضايرتفا لكشبو كرحم مداخلتسا كنكمي ةيزكرم ضيوفتو ةقداصم ةقيرط يلع لوصحلل، ايلحم مهلويختو RADIUS لوكوتورب لالخنم Cisco نم ةيوهلا ةمدخ

## ةكبشلا ليطيختلا مسرلا

ةكبشلا ايجولوبطل الاثمة يلاتلا ةروصلا رفوت



ةملا لعل:

1. هب ةصاخلا دامتعالا تانايب لوؤسملا مدختسم مدقي .
2. وأ ايلحم دامتعالا تانايب ةحص نم ققحتلاب ISE موقيو ةقداصملا ةلمع ليغشت مت .  
Active Directory لالخنم
3. إلى ضيوفتلاو ةقداصملا تامولعمل حامسلا ةمزح ISE لسري ،ةقداصملا حاجن درجمبو .  
FDM.
4. ةحجانلا ةقداصملا ل طشن لجس ثدحيو ISE إلى ع باسحلا ذيفنت متي .

## نيوكتلا

### FDM نيوكت

لوصولا بيوت ةمالع > ماظنلا تاداع | > زاه إلى لقتناو FDM في لوخدلا لجس . 1. ةوطخلا  
ةرادإ إلى

ةديج RADIUS مداو ةومجم ءاشنإ . 2. ةوطخلا

The screenshot displays the Cisco Meraki Device Management 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' and includes sub-sections for 'AAA Configuration' (labeled '3'), 'Management Interface', and 'Data Interfaces'. Below this, the 'HTTPS Connection' section is visible, with a 'Server Group for Management/REST API' (labeled '4') section containing a 'Filter' dropdown and a list with 'LocalIdentitySource' selected. At the bottom, a 'Create New RADIUS Server Group' button is highlighted (labeled '5').

دېج RADIUS م داخ عاشن | 3. قوطخ لا

# 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 Authentication Port

10.81.127.185 1812

Timeout ⓘ

10 seconds

1-300

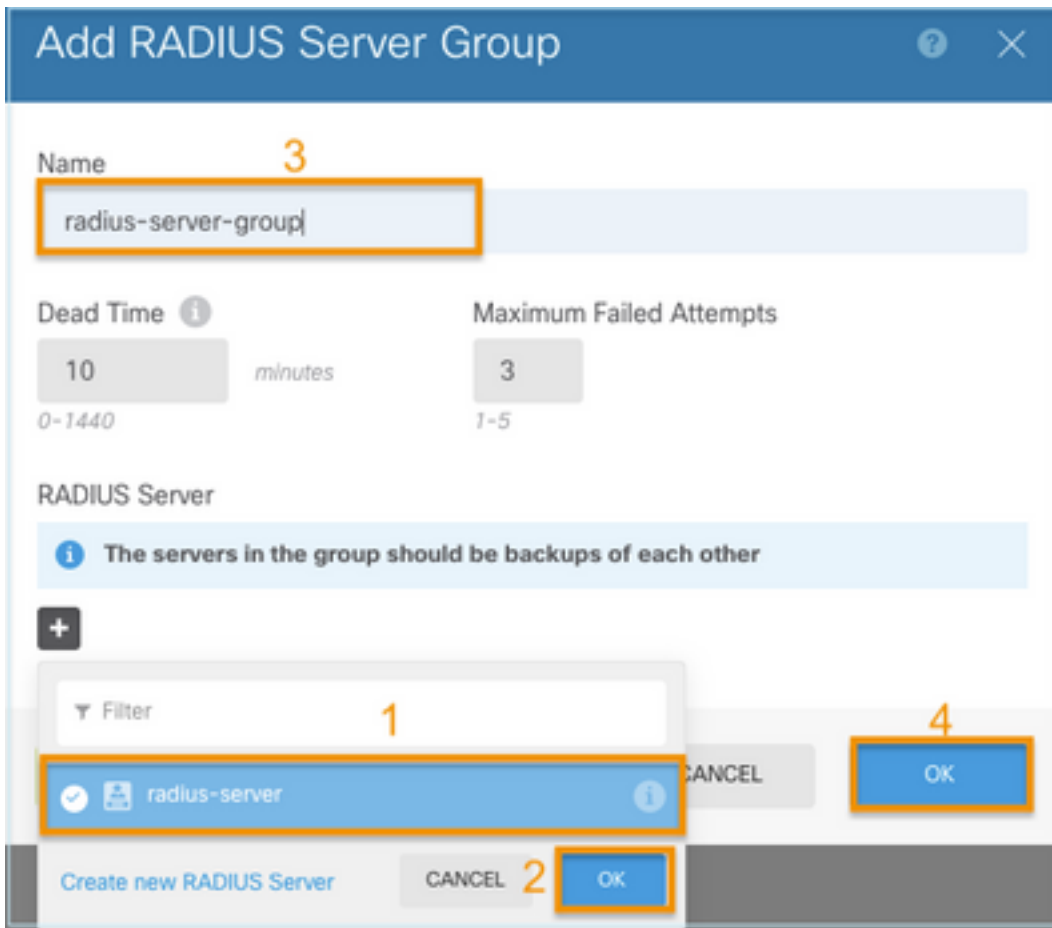
Server Secret Key

●●●●●●●●

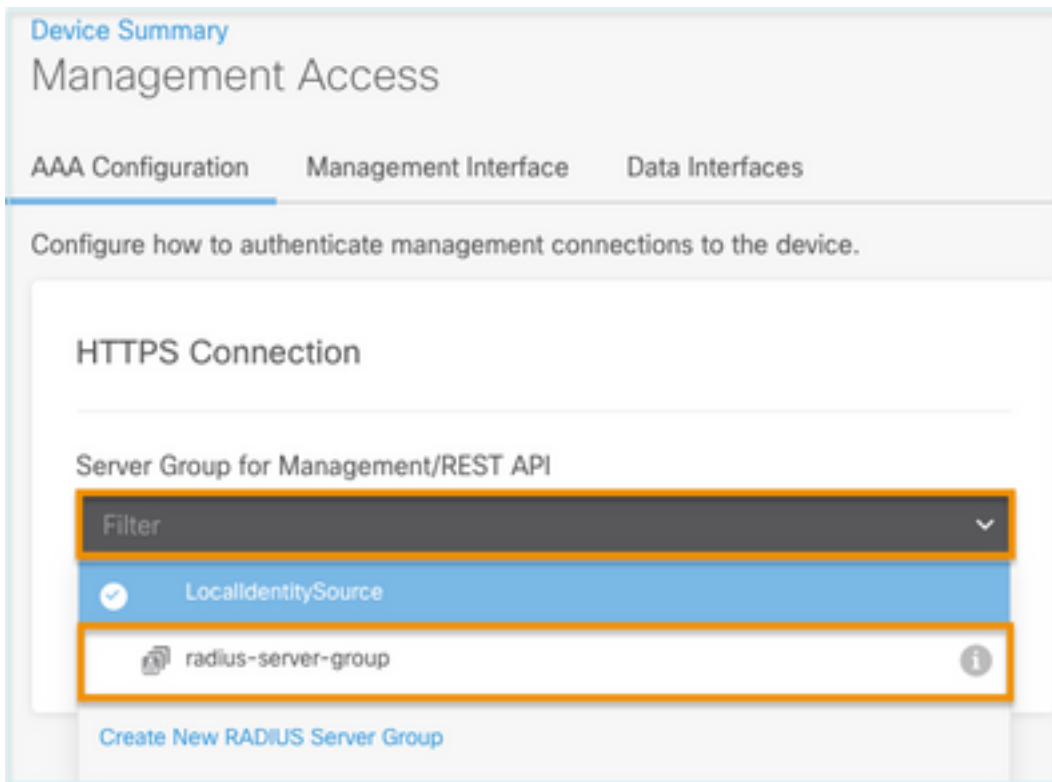
RA VPN Only (if this object is used in RA VPN Configuration)

TEST CANCEL OK

RADIUS مداخله و مخرجى لى RADIUS مداخله فاضا. 4. ةوطخ لى



قرا دلل مداوخ ةعومجكم اهؤاشنإ مت يتل ةعومجمل ديحت 5 ةوطخلا



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**

## نويوكتال ظفح 6. ةوطخلال

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 نويوكت

رطسأ ةثالث ةنوقيأ لىل لقتنا 1. ةوطخلال  
 ةكبشلال ةزهجأ > ةكبشلال دراوم >



ةرادل ددحو ىرسىلال ةيولعلال ةيوازلال يف دوجوم



## 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
------	---------	--------------	----------	------	-------------

2. ةوطخلال  
 لاسرلال دن ع ديدحت .اكرتشم ارس ددحو RADIUS راي تخ  
 رورملا ةم لك و ةكبشلا لىل لوصولا زاهج مسا ددحو ةفاضل+ رزلا ددح .

## Network Devices

Default Device

Device Security Settings

## Network Devices

Name Description 

IP Address Device Profile Model Name Software Version 
 RADIUS Authentication Settings

## RADIUS UDP Settings

Protocol Shared Secret  [Show](#)
 Use Second Shared Secret [i](#)
networkDevices.secondSharedSecret  [Show](#)CoA Port  [Set To Default](#)

دحو یرسی لای وولعل ای وازلای ف دحو م رطسأ ةثالث ةنوقی ای لای لقتنا 3. ةوطخل تاعومجم لای > ةیوه لای ةرادل > ةرادل یل

دن ع دحو م سا دی دحتب مق .رز ةفاضل+ یل ع دحو مدختسم لای ةیوه تاعومجم یل ع دحو 4. ةوطخل لاسرلال





- 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

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

## Attributes Details

Access Type = ACCESS\_ACCEPT  
Service-Type = 7  
cisco-av-pair = fdm.userrole.authority.ro

ةجيتن بنجتل روصلا لاثم لثم وه مدقتملا تامس مسق بيترت نأ نم دكأت :ةظالم  
CLI و GUI مادختساب لوخدلا ليحست دنع ةعقوتم ريغ

ديحت .تاسايسلا تاعومجم > ةسايسلا ىل لقتناو ةثالثلا رطسالا ةنوقي دح .8 ةوطخلا  
ي + رزلا ىل دحو مسا فيرعتب مق ،جهنلا تاعومجم ناو نع لفسأ دوجوملا رزلا ىل  
ديج طرش ةفاضال فصت نملا

IP ناو نع اعوبتم ةكبشلا زاغ زمر ىل دح مثة مس ةفاضل دح ،طرشلا راطل تحت .9 ةوطخلا  
دحو اديج اطرش فضا .FDM ل IP ناو نع فضا ةمسالا ةميق دح .ةكبشلا ىل لوصولا زاغل  
مادختسالا دنع دحو RADIUS ىل دحو ،لوكون ووربلا راخب اعوبتم ةكبشلا ىل لوصولا ىل  
ءاهتالا درجمب

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

Reset Save

دي دحت لآ. زاهج لآ يضا رت فآ لآ لوؤس م لآ ددح ، تآ لوك وت و ر ب لآ ب حآ م س لآ م س ق ت ح ت . 10 ة و ط خ لآ ظآ ف ح لآ د ن ع

ة ق دآ ص م لآ تآ سآ ي س ف ي ر ع ت ل "ج ه ن لآ ة و م ج م" ز م ر ن م ي أ لآ م ه س لآ ي ل ع د ي د ح ت . 11 ة و ط خ لآ و ض ي و ف ت لآ و

+ ي ل ع د د ح و م س آ د ي د ح ت ب م ق ، ة ق دآ ص م لآ ج ه ن نآ و ن ع ل ف س أ د و ج و م ي ل ع د ي د ح ت . 12 ة و ط خ لآ زآ ه ج ز م ر ي ل ع د د ح م ت ة م س ة فآ ض آ د د ح ، ط ر ش لآ رآ ط ل ت ح ت . د ي د ج ط ر ش ة فآ ض آ ل ف ص ت ن م لآ ي ف IP نآ و ن ع ف ض آ و ة م س لآ ة م ي ق ي ل ع د د ح . ة ك ب ش لآ لآ ل و و ص و لآ زآ ه ج ل IP نآ و ن ع ه ع ب ت ي ة ك ب ش لآ ءآ ه ت نآ لآ د ر ج م ب مآ د خ ت س لآ لآ د ن ع د ي د ح ت . FDM ل

ظآ ف ح ي ل ع د د ح و ة ي و ه ن ز خ م ك ن ي ن ي ل خ آ د لآ ن ي م د خ ت س م لآ د د ح . 13 ة و ط خ لآ

Active Directory لآ ISE مآ م ض نآ ة لآ ح ي ف AD ن ز خ م ي لآ ة ي و ه لآ ن ز خ م ر ي ي غ ت ن ك م ي : ة ظ ح آ ل م Directory.

+ ي ف د د ح و م س آ د ي د ح ت ب م ق ، ل ي و خ ت لآ ج ه ن نآ و ن ع ل ف س أ د و ج و م ي ل ع د ي د ح ت . 14 ة و ط خ لآ ة ن و ق ي أ ي ل ع د د ح م ت ة م س ة فآ ض آ د د ح ، ط ر ش لآ ة ذ ف آ ن ت ح ت . د ي د ج ط ر ش ة فآ ض آ ل ف ص ت ن م لآ ي ف AND with FDM\_Admin ة و م ج م د د ح . ة ي و ه ة و م ج م : ي ل خ آ د م د خ ت س م ب ة و ب ت م ة ي و ه لآ ة و م ج م RADIUS NAS-Port-type: Virtual ز م ر آ ه ع ب ت ي ذ ف ن م لآ ة ن و ق ي أ ي ل ع د د ح م ت ، د ي د ج ط ر ش ة فآ ض آ ل NEW مآ د خ ت س لآ لآ د ن ع د د ح و

# 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

دع ددح م٦ ةوطخال ي هؤاشن| مت يذلا فيصوتلا ددح ،تافيصوتلا تحت 15 ةوطخال ظفحلا

FDM\_ReadOnly ةومجم ل 15 و 14 ةوطخال ررك

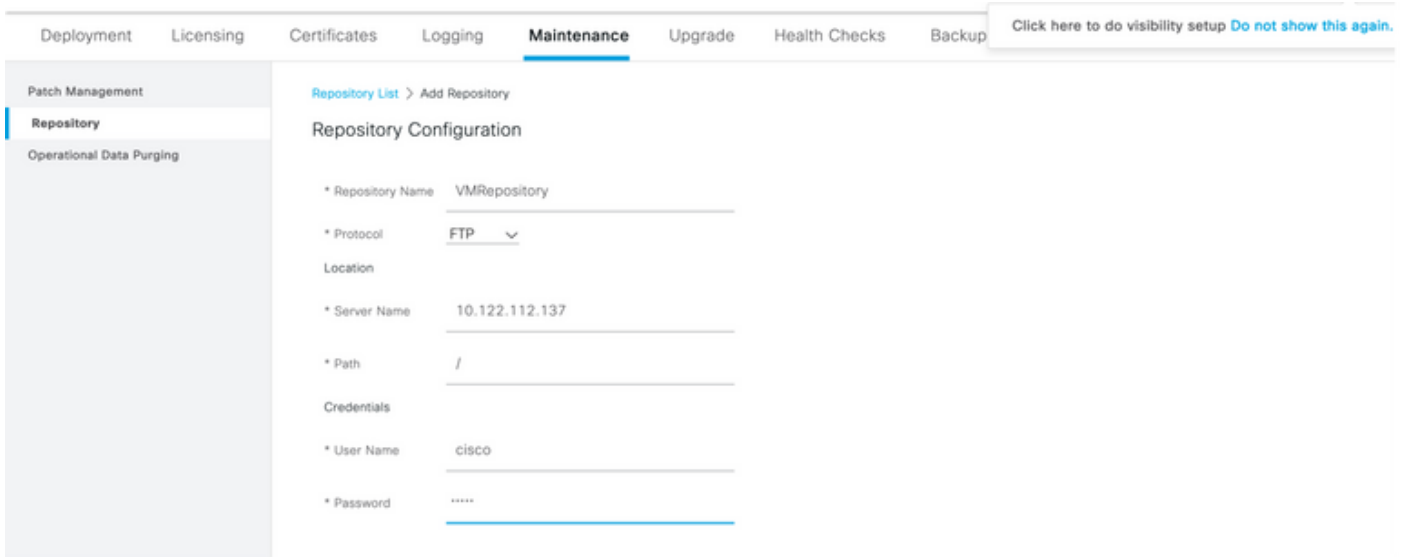
Authorization Policy (3) [Click here to do visibility setup Do not show this again.](#)

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	⚙️

ددح ورسيال يولعل نكرلا ي ددحوم رطسأ ةثالث ةنوقي اىل لقتنا .(ةيرايخا) 16 ةوطخال نينختل مدختسي ةدوتسم ةفاضال ةفاضلا+ اىل ددح و ةدوتسم > ةنايصب > ماظن > ةراد اىل عاهالص او عاطخال فاشكتسا ضارغال TCP غيرفت فلم

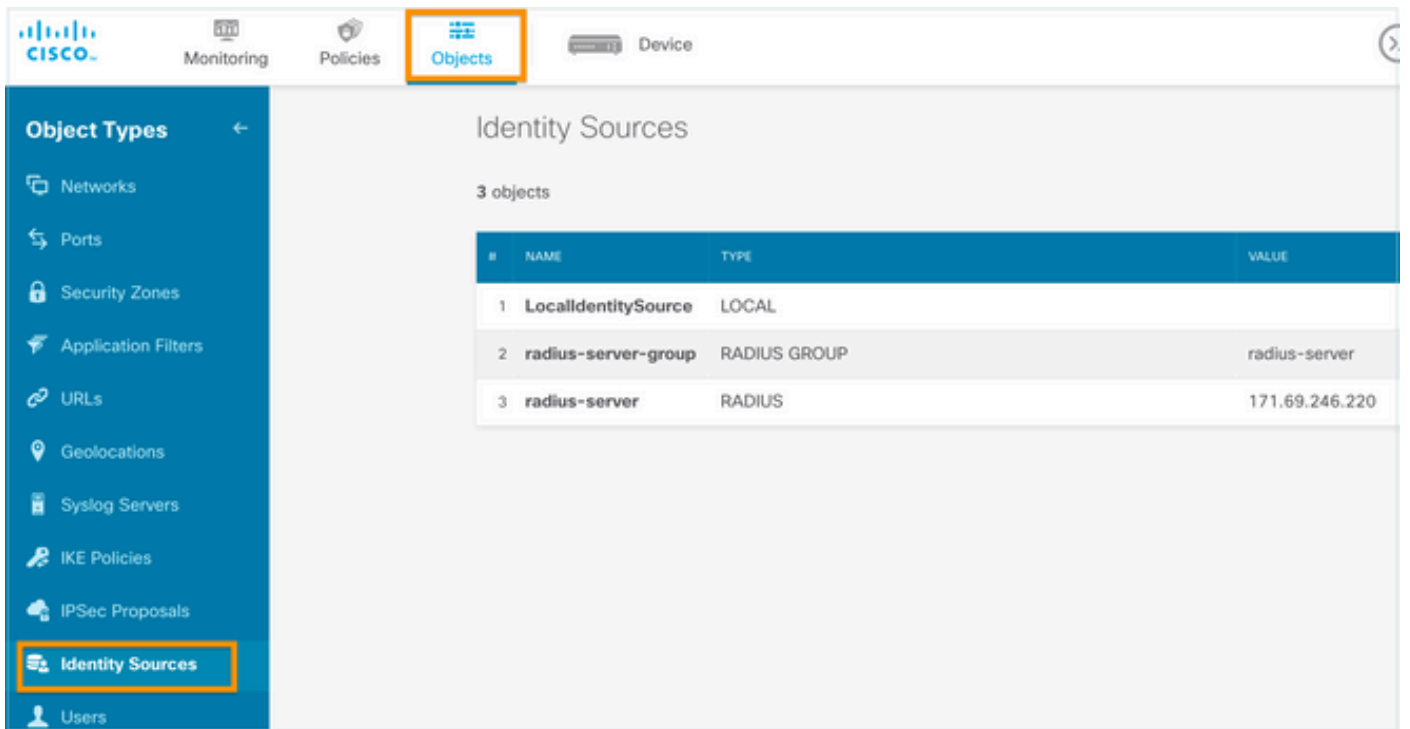
راسملا و مداخل مسا و لوكوت و ربل او ةدوتسم ل مسا فيرعتب مق .(ةيرايخا) 17 ةوطخال ءاهتال درجمب لاسرالا دنع ددح .دامتعالا تانايبو





## ةحصلال نم ققحتال

مداخ نيوكت نم ققحتو ةيوهال رداصم بيوبتل ةمالع > تانئالال ال لقتنا 1. ةوطخال ةومحمل مداخو RADIUS



رز ددحو ةرادال ال لوصولو بيوبتل ةمالع > ماظنل تاداع > زاهال ال لقتنا 2. ةوطخال رابتخال

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

رابطه‌ی زیر در دسترس شماست تا آن را به‌جای خودتان تنظیم کنید. 3. ویرایش

## 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. radius-server

Server Credentials

radiusreadwriteuser1

.....

Please provide the credentials for testing.

CANCEL

TEST

مدخستسم مسا مدختساو، <https://fdm ip address> بتكاو ديديج ةذفان ضرعتسم حتفا. 4 ةوطخلا  
ISE نيوكت مسق نمض 5 ةوطخلا يف اهؤاشن مت يتلا رورملا ةملاك و fdm\_admin



# Firepower Device Manager

**Successfully logged out**

fdm\_admin

.....|

LOG IN

ةرشابم ال ISE RADIUS تالچس ىل ع ةحجانل ل وخذل ل لچس ت ةل و احم نم ققحتل نكمي

Cisco ISE Operations - RADIUS Evaluation Mode 79 Days

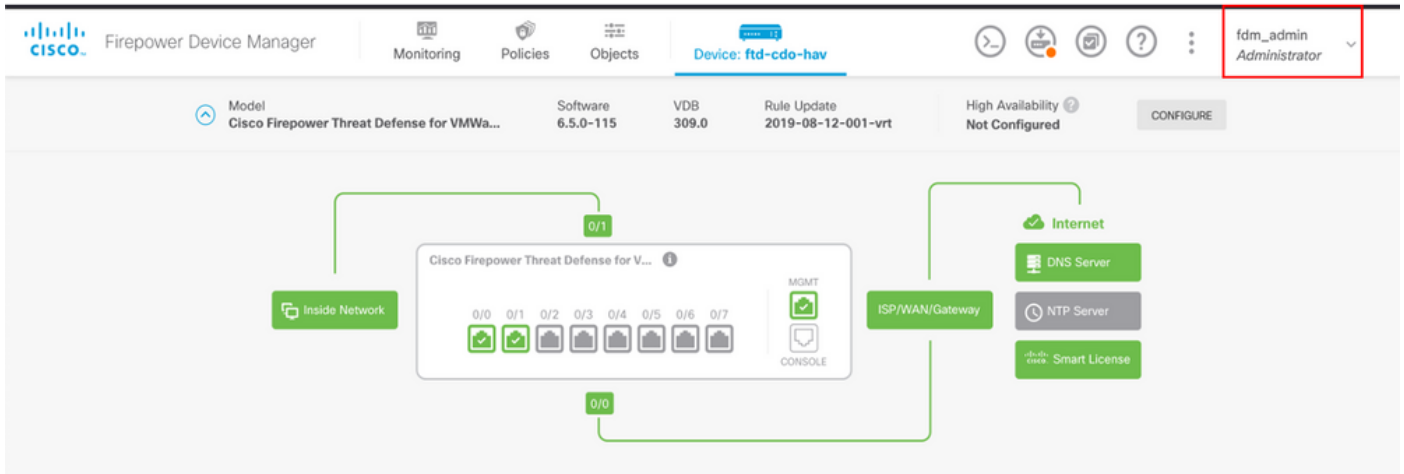
Live Logs Live Sessions

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

نم ىل و لعل ال نكرل ال ف فDM ل وؤس م ال م دختسم ةع ارم اضي نكمي



## Cisco Firepower Device Manager CLI (لوؤس م مدختسم)

```
[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)

[> █
```

## اهحالص او عاطخال فاشكتسا

اهحالص او نيوكتل عاطخال فاشكتسال اهم ادختس! كنكمي يتال تامولعمل مسقلا اذه رفوي

ISE على TCP غيرفت اءاد مادختساب لاصلتال نم ققحتال

ءيوازلا يف ءدوومال ءالثال طوطخال ءنوقيا ددحو ISE لىل لوخدلا ليجستب مق 1 ءوطخال

ص.يخشتلا تاوداً > اهجالصإو ءاطخأل افاشكتسأ > تايلعملال ل لقتناو ىرسيلال ةيولعلال

مس او فيضملا مسا دح .Add+ لىل دح م TCP تابكم لىل دح ، ةماع تاوداً تحت .2 ةوطخلال IP ناو نعالصتا قفدت عيمجتلا ايراي تخا ةيفصت لماعو عدوتسملال ةكبشلال ةهجال فللم ليغشتلال وظيفحال دن ع دح. FDM. طقف

The screenshot shows the Cisco ISE Diagnostic Tools interface. The left sidebar contains a menu with 'General Tools', 'TrustSec Tools', and 'TCP Dump' (which is selected). 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: 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)), and Time Limit (5 Minute(s)). There is also a checkbox for 'Promiscuous Mode' which is unchecked.

لوؤسملال دامتعا تانايب بكتكاو FDM مدختسم ةهجال لىل لوخدلال لىلجستب مق .3 ةوطخلال

عدوتسملال لىل هلاسرا مت دق PCAP فلم نا نم دكأتو فاقيل رز لىل دح ، ISE لىل .4 ةوطخلال ددحملال

Cisco ISE Operations - Troubleshoot Evaluation Mode 79 Days

Diagnostic Tools Download Logs Debug Wizard

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

### General Tools

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

## TCP Dump

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

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

Refresh + Add Edit Trash Start Stop Download Filter

Host Name	Network Interface	Filter	File Name	Repository	File S...	Number o
<input type="checkbox"/> ise31.cisco.se.lab	GigabitEthernet 0 [Up, Run...	ip host 10.122.111.212	FDM_Tshoot	VM	10	1

```
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185) 200 Type set to 1
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185) > STOR FDM_Tshoot.zip
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185) > 150 Opening data channel for file upload to server of "/FDM_Tshoot.zip"
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185) > 226 Successfully transferred "/FDM_Tshoot.zip"
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185) > QUIT
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185) > 221 Goodbye
(000029)7/6/2021 10:21:45 AM - cisco (10.81.127.185) > disconnected.
```

FDM\_Tshoot.zip (evaluation copy)

File Commands Tools Favorites Options Help

Add Extract To Test View Delete Find Wizard Info VirusScan Comment SFX

FDM\_Tshoot.zip - ZIP archive, unpacked size 545 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
<input type="checkbox"/> FDM_Tshoot.pcap	545	473	PCAP File	7/6/2021 5:21 ...	3A095B10

Total 1 file, 545 bytes

ISE و FDM نېب حج انال لاصتال انم ققحتل ل PCAP فلم حت فا 5 ةوطخل

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  .h4@.@...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..

```

في حالات تاريخي نم ققحت، PCAP فلم يلع تالخدم يأ رهظت مل اذا:

1. FDM نيوكت يلع نم يأل IP ISE ناو نع ةفاض ا تمت
2. 1812-1813 ذف نم ب حامس ال متي، طس وأل ققحت ال ذف نم ي ف ةيامح راج دوجو ةلاح ي ف
3. FDM و ISE ني ب لاصت ال نم ققحت ال

**FDM. ةطساوب هؤاشن ا مت يذال فلم ال مادختسا ب لاصت ال نم ققحت ال**

نع ثحبا، FDM زا ه ةحفص نم هؤاشن ا مت يذال اه ا لصل واطخ ال فاشكتسا فلم ي ف ةسس ال تاملك ال:

- FDMpasswordLoginHelper
- NGFWDefaultUserMgmt
- AAAIdentitySourceStatusManager
- RadiusIdentitySourceManager

/var/log/cisco/ngfw-onbox.log ي ف ةزي مل ا هذ ب ةقلعت مل ال ج سل ا عي م ي ل ع رو ثع ال ن كم ي

ع ا رمل:

[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)



# ةعئاشلا تالكشمل

لمعت ال ةيچراخلا ةقداصملا - 1 ةلحال

- فيضملا مسا وأ ذفنملا وأ SecretKey نم ققحت
- RADIUS لىل AVPs ل ئطاخ نيوكت
- "تيملا تقولا" في مداخلا نيوكي نأ نكمي

لشفي Test IdentitySource - 2 ةلحال

- نئاللا لىل ةاربيغتلا ظفح نم دكأت
- دامتعالا تانايب ةحص نم دكأت

## دويقلا

- FDM ل ةطشن لمع تاسلج 5 نم ىصقأ دحب FDM حمسي
- لىل ةسلجلا في ةسداسلا لمعلا ةسلج ءاشن لاطب امت
- "LocalIdentitySource" وه RadiusIdentitySourceGroup مسا نيوكي نأ نكمي ال
- RadiusIdentitySourceGroup لىل 16 RadiusIdentitySources ل ىصقأ دحل
- FDM لىل لوصولا ضفر لىل RADIUS لىل AVPs ل ئطاخلا نيوكتلا يديوي

## ةبواجو ةلئسا

مبيقتلا عضو في ةزيملا هذه لمعت له :س

معن

لىل لوصولا قح امهل نيوكي شيج ، لوخدلا ليجستب طقف ةعارقل نامدختسم ماق اذا :س  
رهظتس فيك . نيفل تخم نيضرتسم نم لوخدلا نالجسيو ، طقف ةعارقل 1 مدختسملا  
؟ ثدحيس اذام

ةطشنلا مدختسملا لمع تاسلج ةحفص في ني مدختسملا نم لك لمع يتسلج ضرع متي :أ  
تقولا متخل ةدرفنم ةميقرهظي لخدم لك . مسالا سفن لمحت يتلا

ناك اذا "ةباجتسا ال" لباقم لوصولا ضفر رفو يچراخلا RADIUS مداخ نأ وه كولسلا :س  
ةيناثلا ةرمللا في اهنويوكت مت ةيلحم ةقداصم كي دل

كي دل تناك اذا درلا متي مل وأ لوصولا ضفر مت اذا يتح ةيلحملا ةقداصملا ةبرجت كنكمي :أ  
ةيناثلا اهنويوكت مت ةيلحم ةقداصم

RADIUS بلط لباقم لوؤسملا لوخد ليجستل RADIUS بلط ني ب ISE قرفي فيك :س  
RA VPN مدختسم ةقداصم

A: ةمس في FDM شحبت . RAPN لباقم Admin في مدختسملا RADIUS بلط ني ب ISE قرفي ال  
اهنويوكت مت يتلا تامسلا لك ISE لسري . لوؤسملا لوصولا وضيوفت نع شحبل Cisco-avpair  
نيتلالاللا في مدختسملا

سفن لاخدوا FDM لوؤسم لچس ني ب زييمتلا ISE تالجسل نكمي ال هنأ كلذ ينعي :ق  
RADIUS ةمس في اكانه له . هسفن زاخلا لىل دعب نع لوصوللا VPN ةكبش لىل مدختسملا  
هليلع حاتفملا عضو ISE نكمي يذلا لوصولا بلط في ISE لىل اهريرمت مت

ةقداصم ءانثأ ISE لىإ FTD نم اهلاسرا متي يتلا قفدتلل RADIUS تامس يلي اميف أ:  
ةقداصم لةرادى لىل لوصولا بلط نم عزجك رصانعلا هذه لاسرا متي ال RADIUS ل RAPN.  
VS RAPN م دختسم لوخذ لچس ي ف FDM ةرادى لچس نيب زي متلل اهم ادختسا نكميو ةيچراخلا

ل اصتالا فيرعت فلم مسا وأ قفنلا ةومجم مسا - 146

150 = AnyConnect Client SSL VPN، 6 = AnyConnect Client IPsec VPN (IKEv2) ليمعلا عون -

151 = AnyConnect Client SSL VPN، 2 = AnyConnect Client IPsec VPN (IKEv2) لمعلا ةسلج عون -

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت  
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م دخت س م ل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و  
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems ( ر ف و ت م ط ب ا ر ل ا ) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا