

使用RADIUS配置ISE的FDM外部身份驗證和授權

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[互通性](#)

[授權](#)

[背景資訊](#)

[網路圖表](#)

[設定](#)

[FDM 組態](#)

[ISE 組態](#)

[驗證](#)

[疑難排解](#)

[常見問題](#)

[限制](#)

[問答](#)

簡介

本文檔介紹將Cisco Firepower裝置管理器(FDM)與身份服務引擎(ISE)整合以便管理員使用者通過RADIUS協定進行GUI和CLI訪問的過程。

必要條件

需求

思科建議您瞭解以下主題：

- Firepower裝置管理器(FDM)
- 身分識別服務引擎 (ISE)
- RADIUS通訊協定

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Firepower威脅防禦(FTD)裝置，所有平台Firepower裝置管理器(FDM)版本6.3.0+
- ISE版本3.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

互通性

- 使用者配置使用者角色的RADIUS伺服器
- 必須在RADIUS伺服器上使用cisco-av-pair配置使用者角色
- Cisco-av-pair = fdm.userrole.authority.admin
- ISE可用作RADIUS伺服器

授權

無特定許可證要求，基本許可證足夠

背景資訊

此功能允許客戶使用RADIUS為這些使用者配置外部身份驗證和多個使用者角色。

RADIUS支援，適用於具有3個系統定義使用者角色的管理存取：

- 只讀
- READ_WRITE (無法執行系統關鍵操作，如升級、還原等)
- 管理員

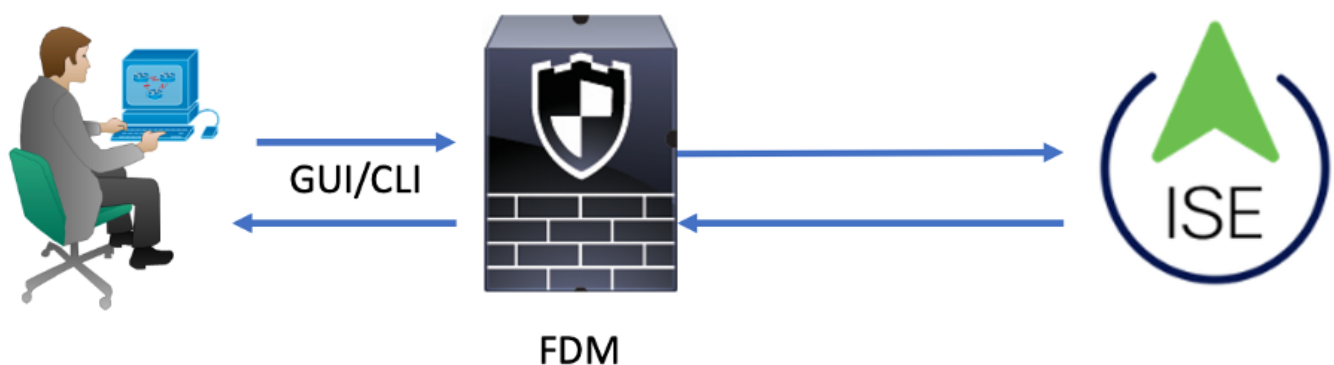
能夠測試RADIUS伺服器的配置，監控活動使用者會話和刪除使用者會話。

此功能在FDM 6.3.0版中實施。在6.3.0版之前，FDM僅支援一個使用者（管理員）。

預設情況下，思科Firepower裝置管理器在本地對使用者進行身份驗證和授權，以便採用集中式身份驗證和授權方法，您可通過RADIUS協定使用思科身份服務引擎。

網路圖表

下一張影象提供了網路拓撲示例



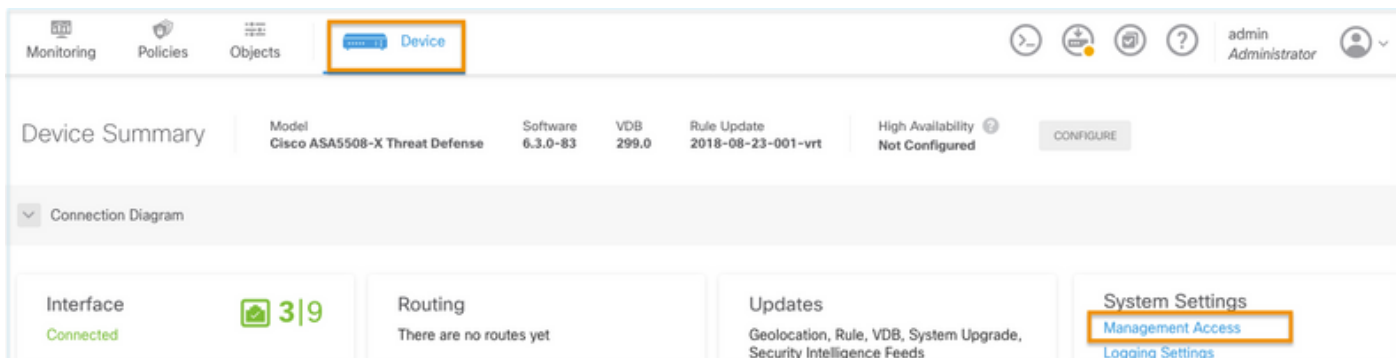
流程：

1. 管理員使用者引入其憑證。
2. 身份驗證過程已觸發，ISE在本地或通過Active Directory驗證憑證。
3. 身份驗證成功後，ISE會向FDM傳送用於身份驗證和授權資訊的允許資料包。
4. 帳戶在ISE上執行，並且身份驗證活動日誌成功。

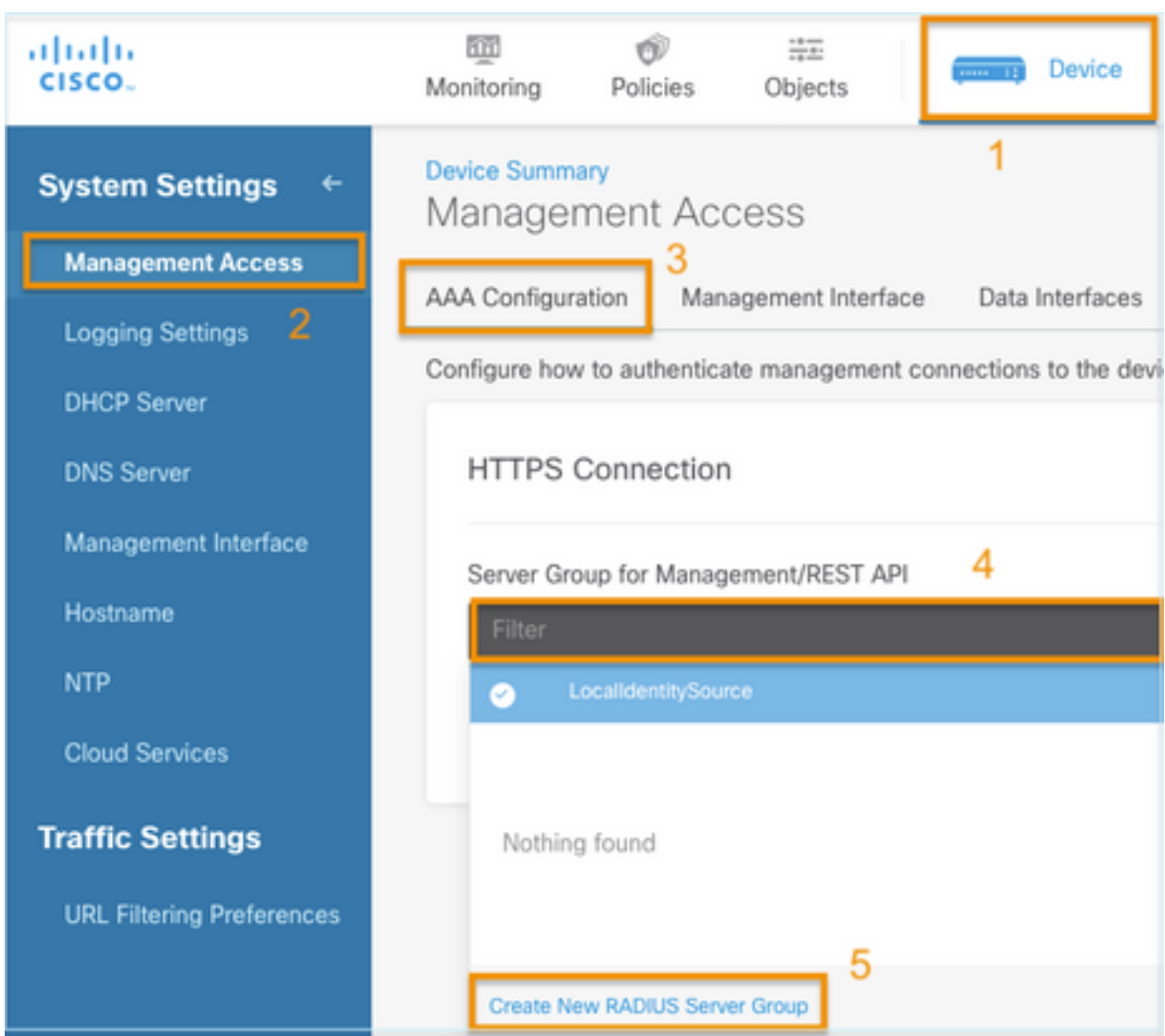
設定

FDM 組態

步驟1.登入到FDM，然後導航到Device > System Settings > Management Access頁籤



步驟2.建立新的RADIUS伺服器群組



步驟3.創建新的RADIUS伺服器

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

步驟4.將RADIUS伺服器新增到RADIUS伺服器群組

Add RADIUS Server Group

Name 3

radius-server-group

Dead Time ⓘ minutes 0-1440

Maximum Failed Attempts 1-5

RADIUS Server

i The servers in the group should be backups of each other

+

Filter 1

radius-server ⓘ

CANCEL OK 4

Create new RADIUS Server CANCEL OK 2

步驟5.選擇建立的組作為管理伺服器組

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

步驟6.儲存組態

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 組態

步驟1. 導航至三行圖示  位於左上角，在 Administration > Network Resources > Network Devices 中選擇

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

步驟2.選擇+Add按鈕並定義Network Access Device Name和IPAddress，然後選中RADIUS覈取方塊並定義共用金鑰。提交時選擇

Network Devices

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

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](#)

Network Devices

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

步驟3. 導航至三行圖示  位於左上角，選擇管理>身份管理>組

User Identity Groups

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

步驟4. 在User Identity Groups上選擇，然後選擇on +Add按鈕。定義名稱並在提交時選擇

New User Identity Group

Identity Group

* Name: FDM_admin

Description:



Submit Cancel





User Identity Groups

Selected 0 Total 2  




 Edit  Add  Delete  Import  Export

Quick Filter 

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

Cisco ISE Administration - Identity Management Evaluation Mode 89 Days    

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

Identity Groups   

- Endpoint Identity Groups
- User Identity Groups

User Identity Groups > New User Identity Group





Identity Group

* Name

Description

附註：在此示例中，建立了FDM_Admin和FDM_ReadOnly身份組，您可以對FDM上使用的每種型別的管理員使用者重複步驟4。

步驟5.導航至位於左上角的三行圖示，然後選擇**管理>身份管理>身份**。選擇on **+Add**並定義使用者名稱和密碼，然後選擇使用者所屬的組。在此示例中，分別建立了fdm_admin和fdm_readonly使用者並將其分配給FDM_Admin和FDM_ReadOnly組。

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



The screenshot shows the Cisco ISE Administration console for Identity Management. The main content area displays a table titled "Network Access Users". The table has columns for Status, Username, Description, First Name, Last Name, Email Address, User Identity Group, and Admin. Two users are listed: "fdm_admin" and "fdm_readonly", both with a status of "Enabled".

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

步驟6.選擇位於左上角的三個行圖示，然後導航到Policy > Policy Elements > Results > Authorization > Authorization Profiles，選擇on +Add，為Authorization Profile定義名稱。選擇Radius Service-type並選擇Administrative，然後選擇Cisco-av-pair，並貼上管理員使用者獲得的角色，在這種情況下，使用者將獲得完整的管理員許可權(fdm.serrole.authority.admin)。選擇Submit。為每個角色（配置為本文檔中的另一個示例的只讀使用者）重複此步驟。

The screenshot shows the Cisco ISE Administration console for Policy - Policy Elements. The main content area displays the "Authorization Profile" configuration form. The form has fields for Name, Description, Access Type, Network Device Profile, Service Template, Track Movement, Agentless Posture, and Passive Identity Tracking.

Authorization Profile

- * Name: FDM_Profile_Admin
- Description: [Empty text area]
- * 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	▼	=	<u>fdm.userrole.authority.admin</u>	▼	— +

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>	▼	— +

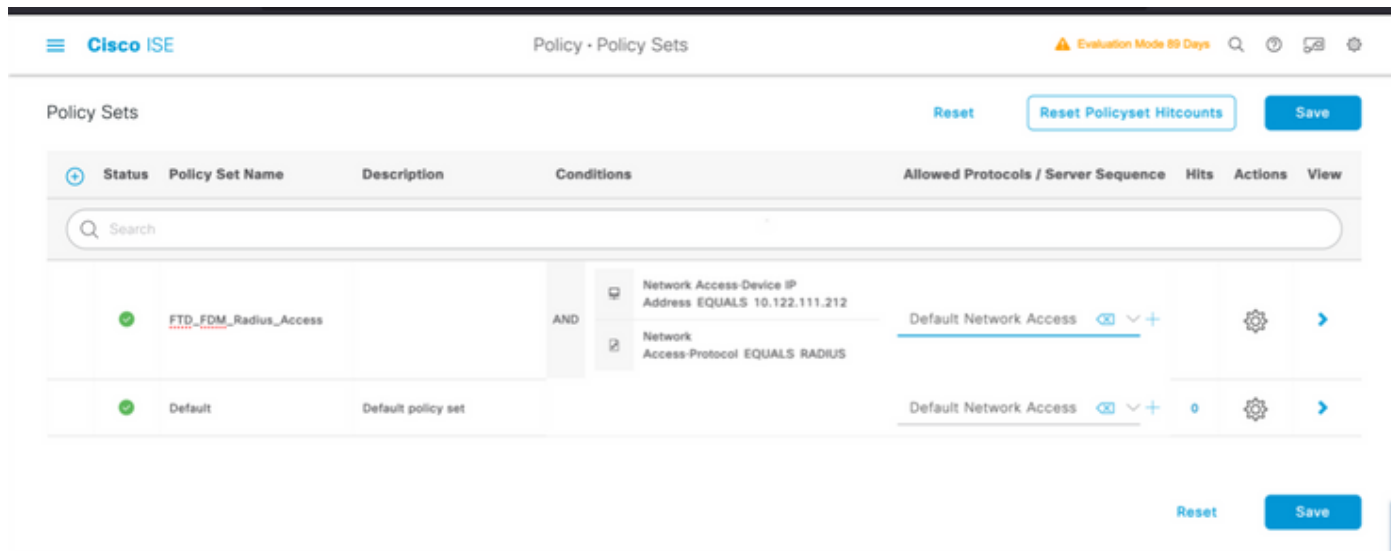
Attributes Details

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

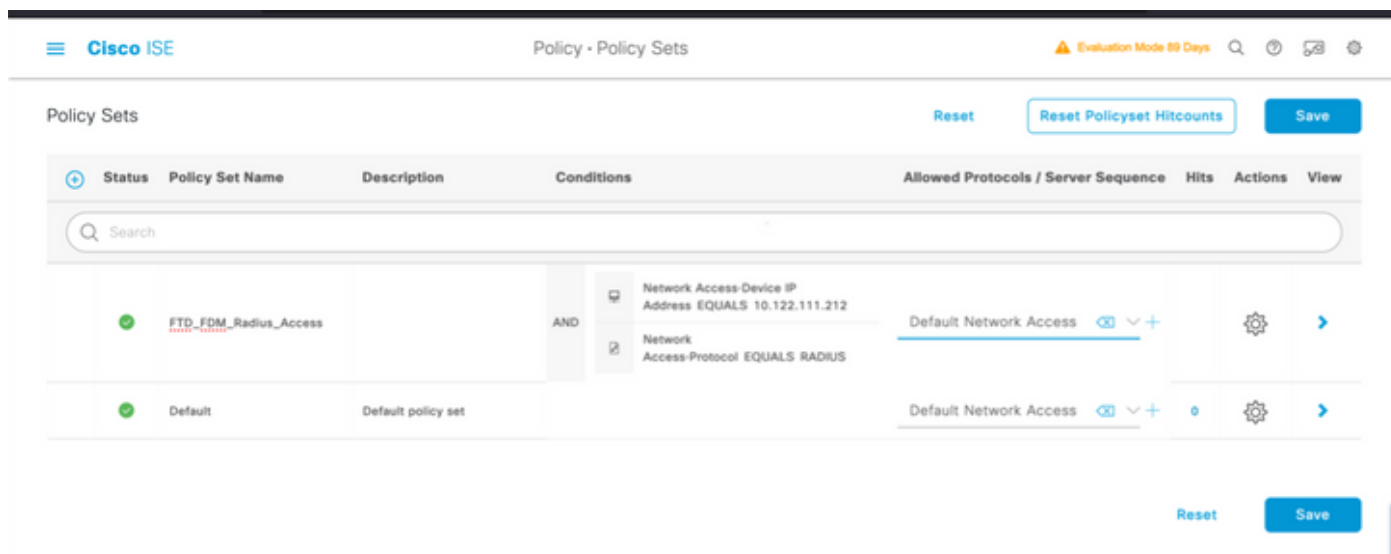
附註：確保「高級屬性」部分的順序與影象示例的順序相同，以避免在使用GUI和CLI登入時產生意外結果。

步驟8.選擇三行圖示並導航至Policy > Policy Sets。選擇時間  按鈕位於Policy Sets標題下，定義名稱並在中間的+按鈕上選擇以新增新條件。


步驟9.在「條件」視窗中，選擇新增屬性，然後選擇Network Device Icon,後跟Network access device IP address。 選擇屬性值並新增FDM IP地址。新增新條件，依次選擇Network Access和Protocol選項，選擇RADIUS，然後選擇使用一次。



步驟10.在allow protocols部分，選擇Device Default Admin。儲存時選擇



步驟11.選擇右箭頭  用於定義身份驗證和授權策略的策略集的圖示


步驟12.選擇  位於身份驗證策略標題下方，定義名稱並在中間的+上選擇以新增新條件。在「條件」視窗下，選擇新增屬性，然後在網路裝置圖示上依次選擇網路接入裝置IP地址。 選擇屬性值並新增FDM IP地址。完成後在使用時選擇

步驟13.選擇Internal Users作為Identity Store並選擇 儲存

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
+	FDM_Users	Network Access-Device IP Address EQUALS 10.122.111.212	Internal Users		Options

附註：如果ISE加入到Active Directory，可以將身份儲存更改為AD儲存。

步驟14. 選擇於  位於授權策略標題下方，定義名稱並在中間的+上選擇以新增新條件。在「條件」視窗下，選擇新增屬性，然後選擇Identity Group圖示，後跟Internal User:Identity Group。選擇FDM_Admin組，選擇AND和NEW選項以新增新條件，選擇埠圖示後跟RADIUS NAS-Port-Type:Virtual，然後選擇使用。

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

步驟15.在配置檔案下，選擇在步驟6中建立的配置檔案，然後選擇Save

對FDM_ReadOnly組重複步驟14和15

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

			Results			
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	⚙️

第16步 (可選)。 導航到位於左上角的三行圖示，在Administration > System > Maintenance > Repository上選擇，然後選擇+ Add以新增用於儲存TCP轉儲檔案以進行故障排除的儲存庫。

第17步 (可選)。 定義儲存庫名稱、協定、伺服器名稱、路徑和憑據。完成後在Submit上選擇。

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 /

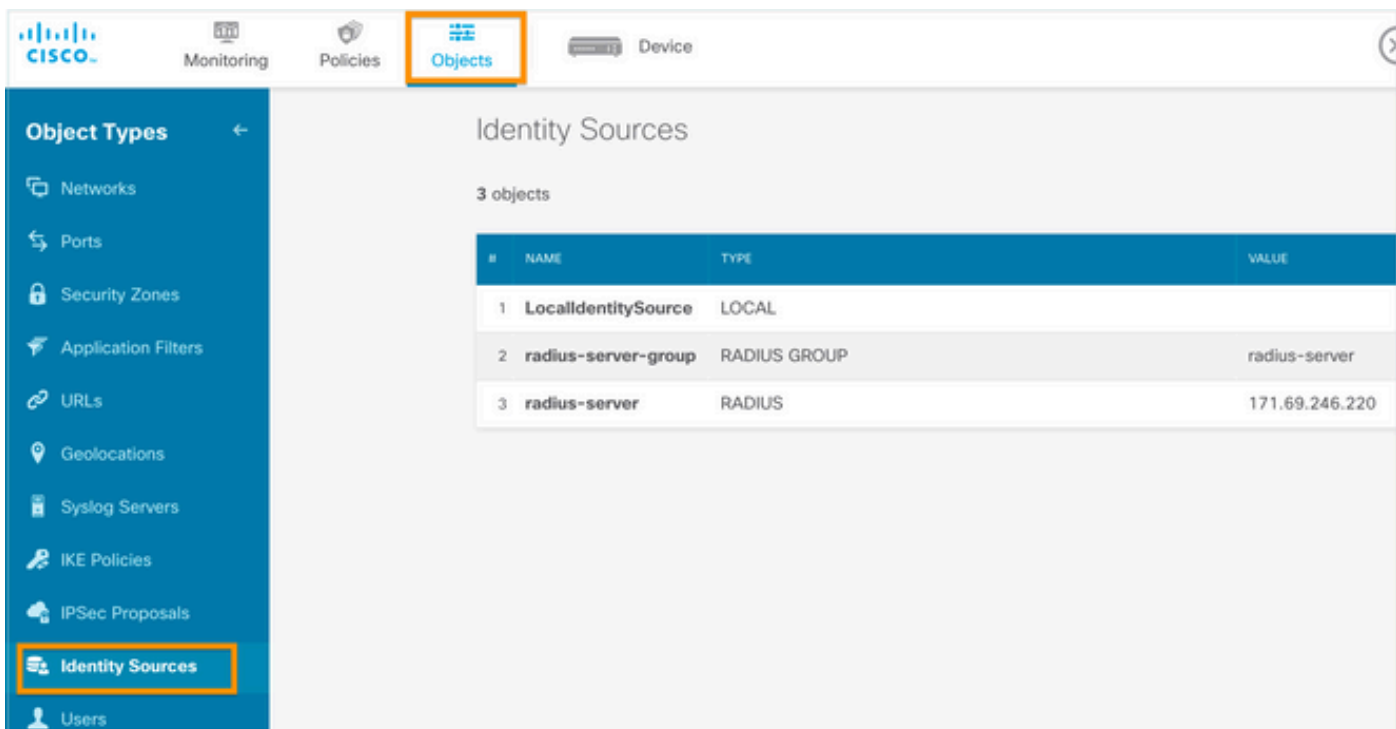
Credentials

* User Name cisco

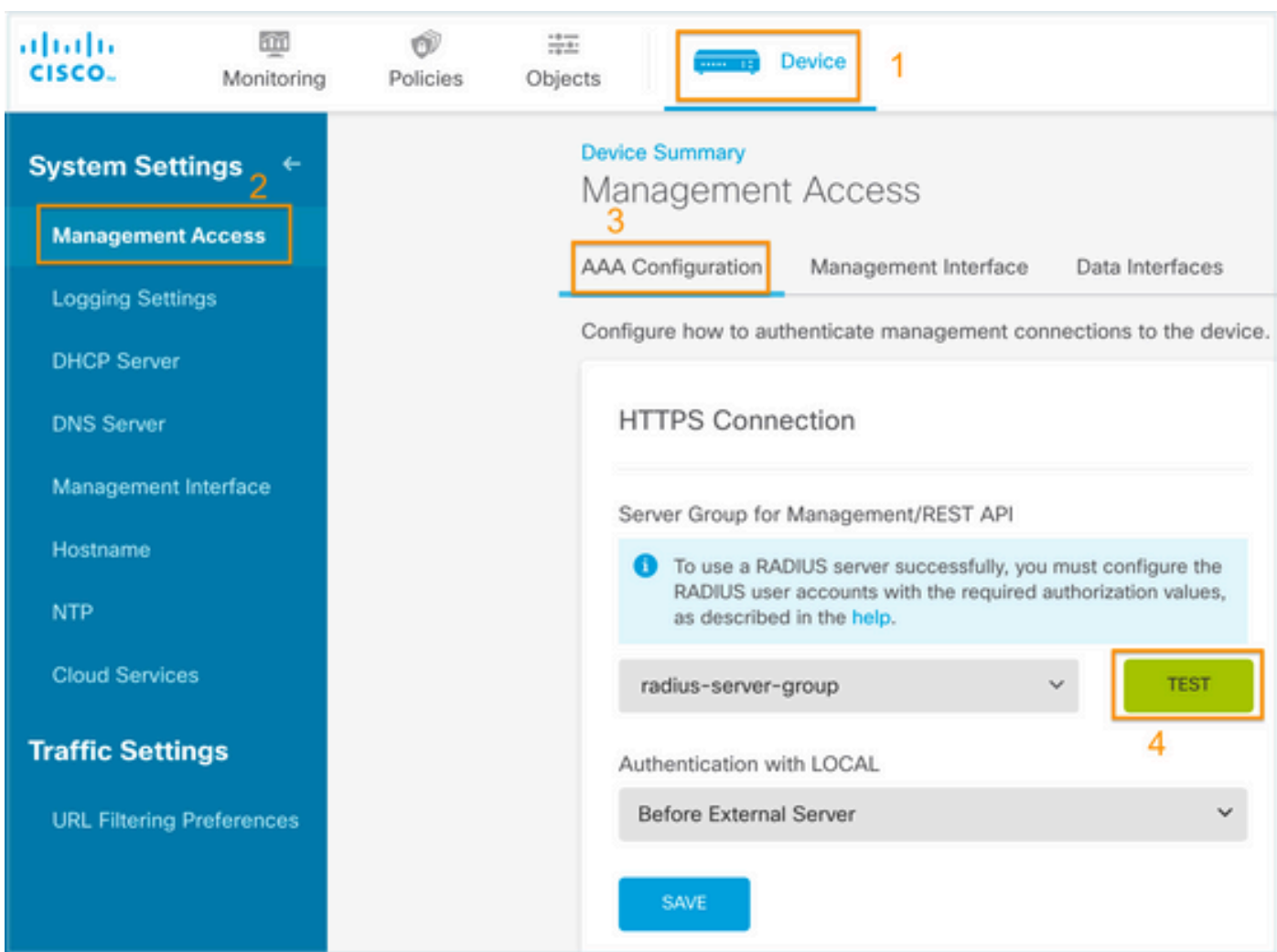
* Password

驗證

步驟1.導覽至Objects > Identity Sources選項卡，然後驗證RADIUS伺服器 and 組伺服器配置



步驟2.導覽至Device > System Settings > Management Access選項卡，然後選擇TEST按鈕



步驟3.插入使用者憑證並選擇TEST按鈕

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.

步驟4. 開啟新視窗瀏覽器並鍵入 https://FDM_ip_Address，使用ISE配置部分下步驟5中建立的 `fdm_admin` 使用者名稱和密碼。



Firepower Device Manager

Successfully logged out

fdm_admin

.....|

LOG IN

可在ISE RADIUS即時日誌上驗證登入嘗試是否成功

Cisco ISE Operations · RADIUS Evaluation Mode 79 Days

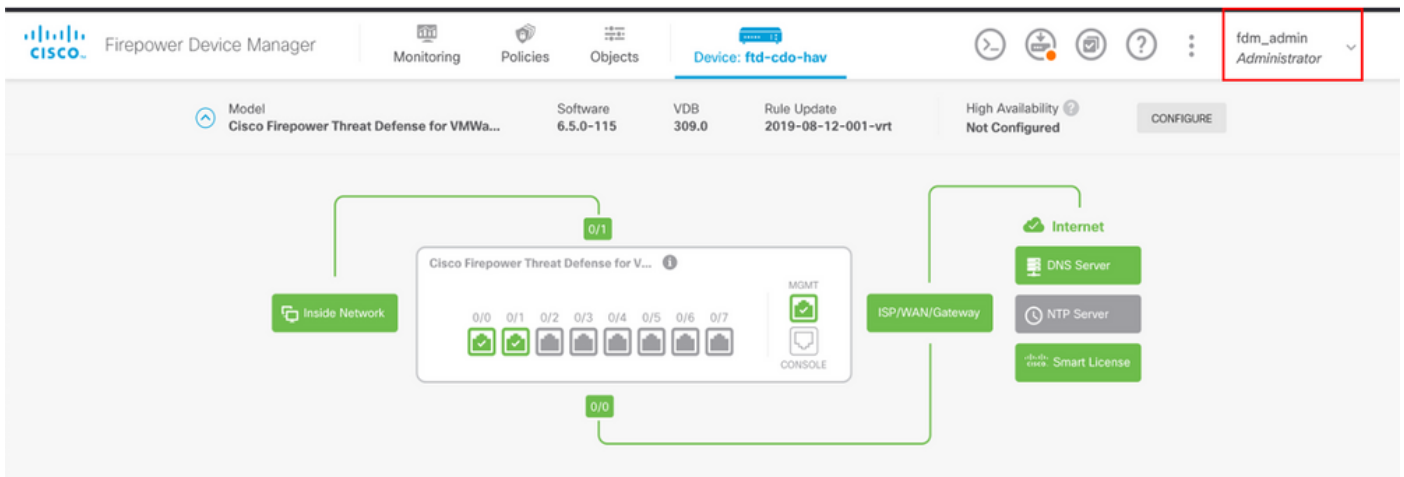
Live Logs Live Sessions

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

還可以檢視右上角的FDM上的管理員使用者



Cisco Firepower裝置管理器CLI (管理員使用者)

```
[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)

[> █
```

疑難排解

本節提供的資訊用於對組態進行疑難排解。

通過ISE上的TCP轉儲工具進行通訊驗證

步驟1.登入ISE並選擇位於左上角的三行圖示並導航到操作>故障排除>診斷工具。

步驟2.在General tools下，選擇on TCP Dumps，然後選擇Add+。選擇主機名、網路介面檔名、儲存庫（可選）以及過濾器，以僅收集FDM IP地址通訊流。在「儲存並運行」中選擇

The screenshot shows the Cisco ISE Diagnostic Tools interface. The left sidebar is expanded to 'TCP Dump'. 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:**

步驟3.登入FDM UI並鍵入管理員憑據。

步驟4.在ISE上，選擇Stop按鈕並驗證pcap檔案已傳送到定義的儲存庫。

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

步驟5.開啟pcap檔案驗證FDM和ISE之間的成功通訊。

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..

```

如果在pcap檔案上未顯示任何條目，則驗證以下選項：

1. 已在FDM配置中新增正確的ISE IP地址
2. 如果防火牆位於中間，驗證是否允許埠1812-1813。
3. 檢查ISE和FDM之間的通訊

與FDM生成的檔案的通訊驗證。

在排除從FDM裝置頁面生成的檔案故障時，查詢關鍵字：

- FdmPasswordLoginHelper
- NGFWDefaultUserMgmt
- AAIdentitySourceStatusManager
- RadiusIdentitySourceManager

有關此功能的所有日誌都可以在/var/log/cisco/ngfw-onbox.log中找到

參考資料：

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd-fdm-mgmt.html#id_73793

常見問題

案例1 — 外部驗證無法運作

- 檢查secretKey、埠或主機名
- RADIUS上的AVP組態錯誤
- 伺服器可能處於「Dead Time」

案例2 — 測試IdentitySource失敗

- 確保儲存對對象的更改
- 確保憑據正確

限制

- FDM最多允許5個活動的FDM會話。
- 建立第6個會話會導致第1個會話被吊銷
- RadiusIdentitySourceGroup的名稱不能為「LocalIdentitySource」
- 最多16個RadiusIdentitySource到RadiusIdentitySourceGroup
- 在RADIUS上錯誤配置AVP會導致拒絕訪問FDM

問答

Q: 此功能是否在「評估」模式下工作？

A:是

Q: 如果兩個只讀使用者登入（其中擁有只讀使用者1的訪問許可權），則他們從兩個不同的瀏覽器登入。它將如何顯示？會發生什麼？

A:兩個使用者的會話都以相同名稱顯示在活動使用者會話頁面中。每個條目顯示時間戳的單個值。

Q: 行為是外部radius伺服器提供存取拒絕與如果您在第二天配置了本地身份驗證，則為「無響應」？

A: 即使您配置了2nd的本地身份驗證，也可能會嘗試本地身份驗證，即使您獲得拒絕訪問或無響應。

Q: ISE如何區分管理員登入的RADIUS請求與驗證RA VPN使用者的RADIUS請求

A: ISE不會區分管理員和RAVPN使用者的RADIUS請求。FDM檢視cisco-avpair屬性以確定Admin訪問許可權的授權。在這兩種情況下，ISE都會傳送為使用者配置的所有屬性。

Q: 這意味著ISE日誌無法區分FDM管理員登入和同一使用者訪問同一裝置上的遠端訪問VPN。在ISE可以金鑰的訪問請求中，是否有任何RADIUS屬性傳遞到ISE？

A: 以下是在RADIUS身份驗證期間從FTD傳送到ISE的上行RADIUS屬性。這些屬性不會作為外部身份驗證管理訪問請求的一部分傳送，並且可用於區分FDM管理登入與RAVPN使用者登入。

150 — 客戶端型別(適用值：2 = AnyConnect Client SSL VPN , 6 = AnyConnect Client IPsec VPN(IKEv2))。

151 — 會話型別(適用值：1 = AnyConnect客戶端SSL VPN , 2 = AnyConnect客戶端IPSec VPN(IKEv2))。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。