

在FMC上配置RAVPN證書身份驗證和ISE授權

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[第1步：安裝受信任的CA證書](#)

[第2步：配置ISE/Radius伺服器組和連線配置檔案](#)

[第3步：配置ISE](#)

[第3.1步：建立使用者、組和證書身份驗證配置檔案](#)

[第3.2步：配置身份驗證策略](#)

[第3.3步：配置授權策略](#)

[驗證](#)

[疑難排解](#)

簡介

本文檔介紹在FMC上由CSF管理的RAVPN連線中配置證書身份驗證的ISE伺服器授權策略。

必要條件

需求

思科建議您瞭解以下主題：

- 思科安全防火牆(CSF)
- 思科安全防火牆管理中心(FMC)
- 思科身分辨識服務引擎(ISE)
- 證書註冊和SSL基礎知識。
- 憑證授權單位(CA)

採用元件

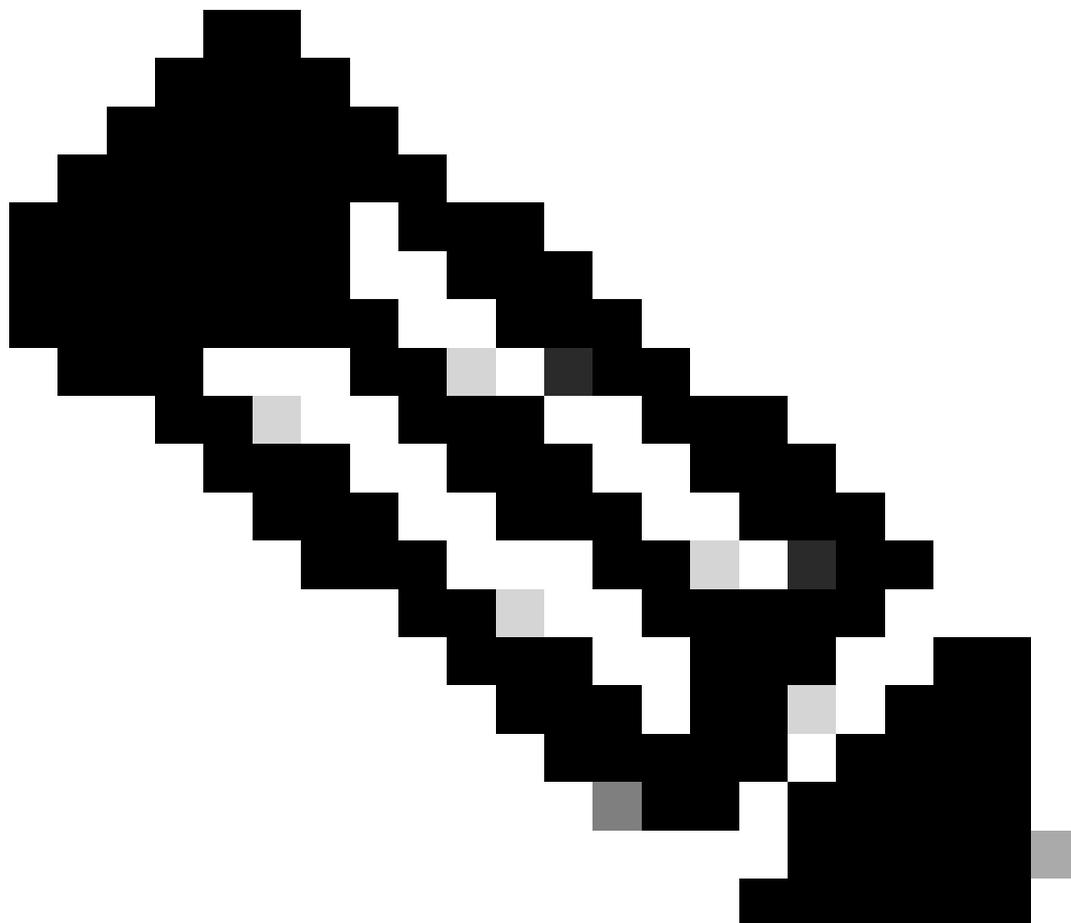
本檔案內容以這些軟體和硬體版本為基礎。

- 思科安全使用者端5.1.6版
- 思科安全防火牆版本7.2.8
- 思科安全防火牆管理中心版本7.2.8

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。

設定

第1步：安裝受信任的CA證書



注意：如果CA證書與用於伺服器身份驗證的證書不同，則需要執行此步驟。如果同一CA伺服器向使用者頒發證書，則無需再次導入同一CA證書。

Firewall Management Center
Devices / Certificates

Overview Analysis Policies **Devices** Objects Integration

Name	Domain	Enrollment Type	Status
FTD1			
cisco.com	Global	PKCS12 file	Server Certificate
InternalCA Server	Global	Manual (CA Only)	Internal CA certificate

- a. 導航到 Devices > Certificates 並按一下 Add。
- b. 輸入 trustpoint name 並選擇 Manual 作為 CA 資訊下的登記型別。
- c. 檢查 CA Only 並貼上採用 pem 格式的受信任/內部 CA 證書。
- d. 選中 Skip Check for CA flag in basic constraints of the CA Certificate 並按一下 Save。

Add Cert Enrollment

Name*
InternalCA Server

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: Manual

CA Only
Check this option if you do not require an identity certificate to be created from this CA

CA Certificate:
-----BEGIN CERTIFICATE-----
MIIB/
zCCAWigAwIBAgIBATANBgkqhki
G9w0BAQsFADATMREwDwYDV
QQDEwhDQVNI
cnZlclAeFw0yNDEwMTcxMDU5
MDBaFw0yNTEwMjAxMDU5MDBB
aMBMxETAPBgNVBAMT
CENBU2VydMvyMIGfMA0GCSq
GS1b3DQEBAQUAA4GNADCBiQ
KPaOC+IDQA2/wcPQW

Validation Usage: IPsec Client SSL Client SSL Server

Skip Check for CA flag in basic constraints of the CA Certificate

Cancel Save

- e. 在 Cert Enrollment 下，從剛建立的下拉選單中選擇 trustpoint，然後按一下 Add。

Add New Certificate



Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

Cert Enrollment*:

Cert Enrollment Details:

Name:	InternalCAServer
Enrollment Type:	Manual (CA Only)
Enrollment URL:	N/A

Cancel

Add

第2步：配置ISE/Radius伺服器組和連線配置檔案

a. 導航到 Objects > AAA Server > RADIUS Server Group 並按一下 Add RADIUS Server Group。選中 Enable authorize only 選項。



警告：如果未選中「僅啟用授權」選項，則防火牆將傳送身份驗證請求。但是，ISE期望接收該請求的使用者名稱和密碼，並且證書中未使用密碼。因此，ISE將請求標籤為身份驗證失敗。

Edit RADIUS Server Group



Name:*

ISE_Authorization

Description:

Group Accounting Mode:

Single

Retry Interval:* (1-10) Seconds

10

Realms:

Enable authorize only

Enable interim account update

Interval:* (1-120) hours

24

Enable dynamic authorization

Port:* (1024-65535)

b. 按一下Add (+)圖示，然後使用IP地址或主機名增加Radius server/ISE server。

Edit RADIUS Server



IP Address/Hostname:*

ISELocal

Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:* (1-65535)

1812

Key:*

•••••

Confirm Key:*

•••••

Accounting Port: (1-65535)

1813

Timeout: (1-300) Seconds

10

Connect using:

Routing Specific Interface

Default: Management/Diagnostic ▾ +

Redirect ACL:

▾ +

Cancel

Save

C. 導航到 **Devices > Remote Access configuration**。建立 new connection profile 並將驗證方法設定為 Client Certificate Only。對於授權伺服器，請選擇在之前步驟中建立的授權伺服器。

確保您選中 **Allow connection only if user exists in authorization database** 選項。此設定可確保僅當授權允許時才完

成與RAVPN的連線。

Edit Connection Profile ?

Connection Profile:*

Group Policy:* +
[Edit Group Policy](#)

Client Address Assignment **AAA** Aliases

Authentication

Authentication Method: Enable multiple certificate authentication

▼ Map username from client certificate

Map specific field

Primary Field: Secondary Field:

Use entire DN (Distinguished Name) as username

Authorization

Authorization Server: Allow connection only if user exists in authorization database

Accounting

來自客戶端證書的Map Username是指從證書獲取的資訊以標識使用者。在本例中，您將保留預設配置，但可以根據用於標識使用者的資訊進行更改。

點選Save。

d. 導航至Advanced > Group Policies。按一下右側的Add (+)圖示。

Firewall Management Center
Devices / VPN / Edit Advanced

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin | **SECURE**

FTD_PolicyVPN Save Cancel

Enter Description Policy Assignments (1)

Local Realm: None Dynamic Access Policy: None

Connection Profile Access Interfaces **Advanced**

AnyConnect Client Images
Address Assignment Policy
Certificate Maps
Group Policies
LDAP Attribute Mapping
Load Balancing
IPsec
Crypto Maps
IKE Policy
IPsec/IKEv2 Parameters

Group Policies
Group policy can be assigned to VPN user through connection profile or by RADIUS server during authentication.
Following are the group policies that are associated with this Remote Access VPN configuration. Add a group policy if it is required to be assigned by RADIUS server during authentication.

Name	Protocol	DNS Servers	VPN Filter
DfltGrpPolicy	SSL_IKEV2		
Marketing_Group	SSL_IKEV2		
IT_Group	SSL_IKEV2		

e. 建立group policies。每個組策略都根據組織組和每個組可以訪問的網路進行配置。

Group Policy ?

Available Group Policy ↻ +

DfltGrpPolicy
FTD1_GPCertAuth
FTD1_GPISE
FTD1_GPLocalFull

Add

Selected Group Policy

DfltGrpPolicy

Cancel OK

f. 在組策略上，執行每個組特定的配置。可以增加一條標語消息以在成功連線後顯示。

Add Group Policy



Name:*

IT_Group

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

Banner:

Maximum total size: 3999, Maximum characters in a line : 497.

In case of a line spanning more than 497 characters, split the line into multiple lines.

** Only plain text is supported (symbols '<' and '>' are not allowed)

IT Group

1

Cancel

Save

g. 選擇左側的 group policies，然後按一下 Add 將其移動到右側。這指定了配置中正在使用的組策略。

Group Policy



Available Group Policy  

Q Search

FTD1_GPCertAuth

FTD1_GPISE

FTD1_GPLocalFull

IT_Group

Marketing_Group

Add

Selected Group Policy

DfltGrpPolicy 

Marketing_Group 

IT_Group 

Cancel

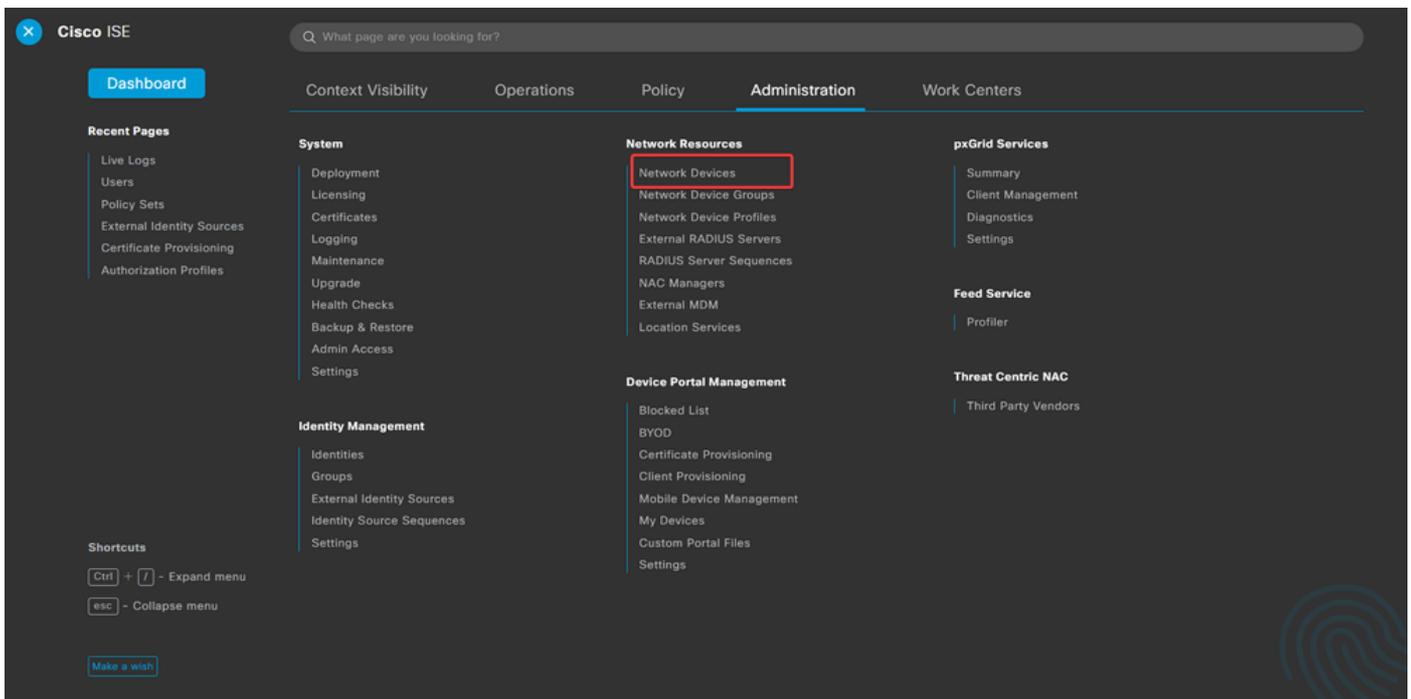
OK

e. 部署更改。

第3步：配置ISE

第3.1步：建立使用者、組和證書身份驗證配置檔案

a. 登入到ISE伺服器並導航至 **Administration > Network Resources > Network Devices**。



b. 按一下Add將防火牆配置為AAA客戶端。

Network Devices

[Edit](#)
[+ Add](#)
[Duplicate](#)
[Import](#)
[Export](#)
[Generate PAC](#)
[Delete](#)

<input type="checkbox"/>	Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/>	FTD		Cisco	All Locations	All Device Types	

c. 輸入網路裝置名稱和IP地址欄位，然後選中RADIUS Authentication Settings 覈取方塊，並增加Shared Secret。「此值必須與在FMC上建立RADIUS伺服器對象時使用的值相同」。按一下Save。

[Network Devices List](#) > FTD

Network Devices

Name

Description

IP Address / 32

RADIUS Authentication Settings

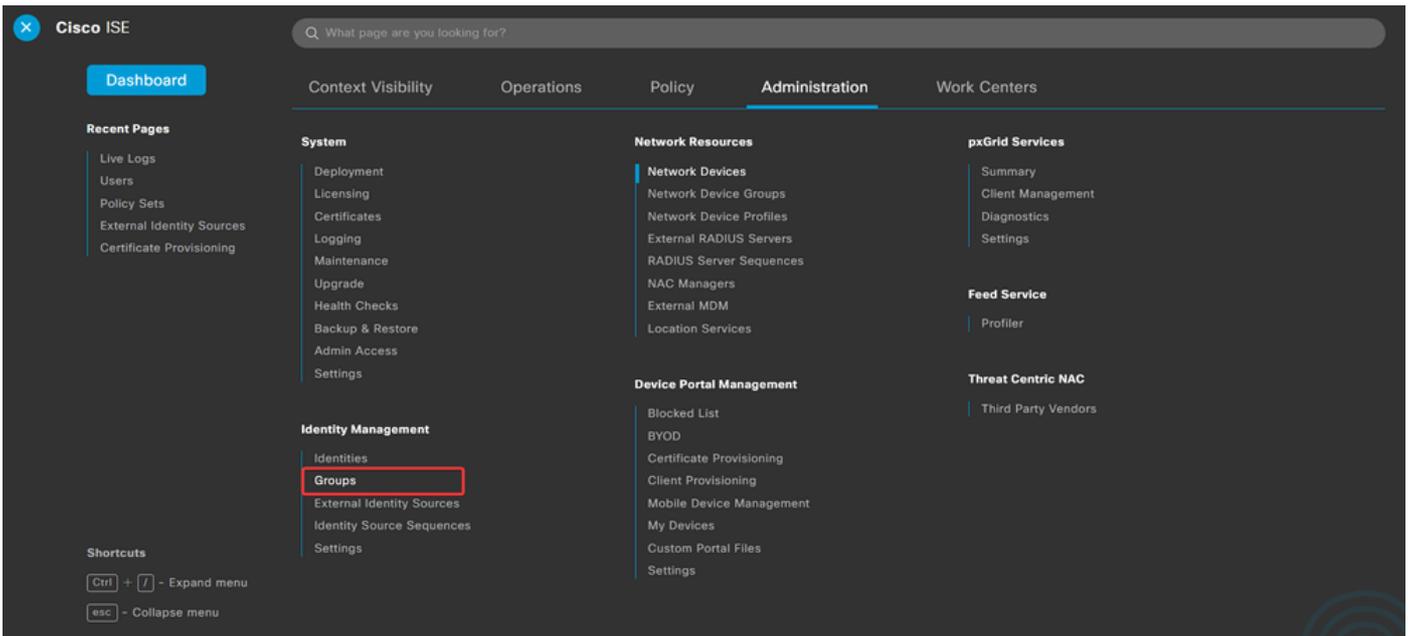
RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret Show

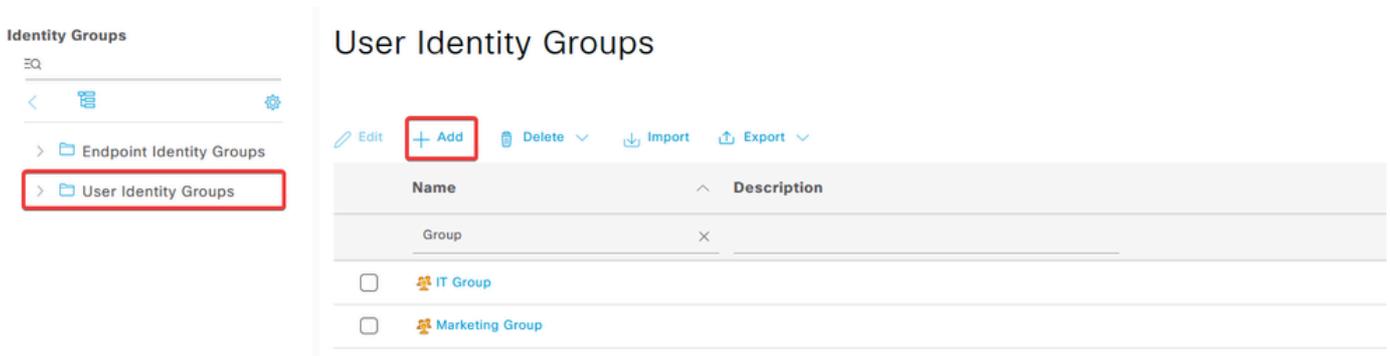
Use Second Shared Secret ⓘ

d. 導航至 Administration > Identity Management > Groups。



e. 按一下 User Identity Groups，然後按一下 Add。

輸入 group Name 並按一下 Submit。



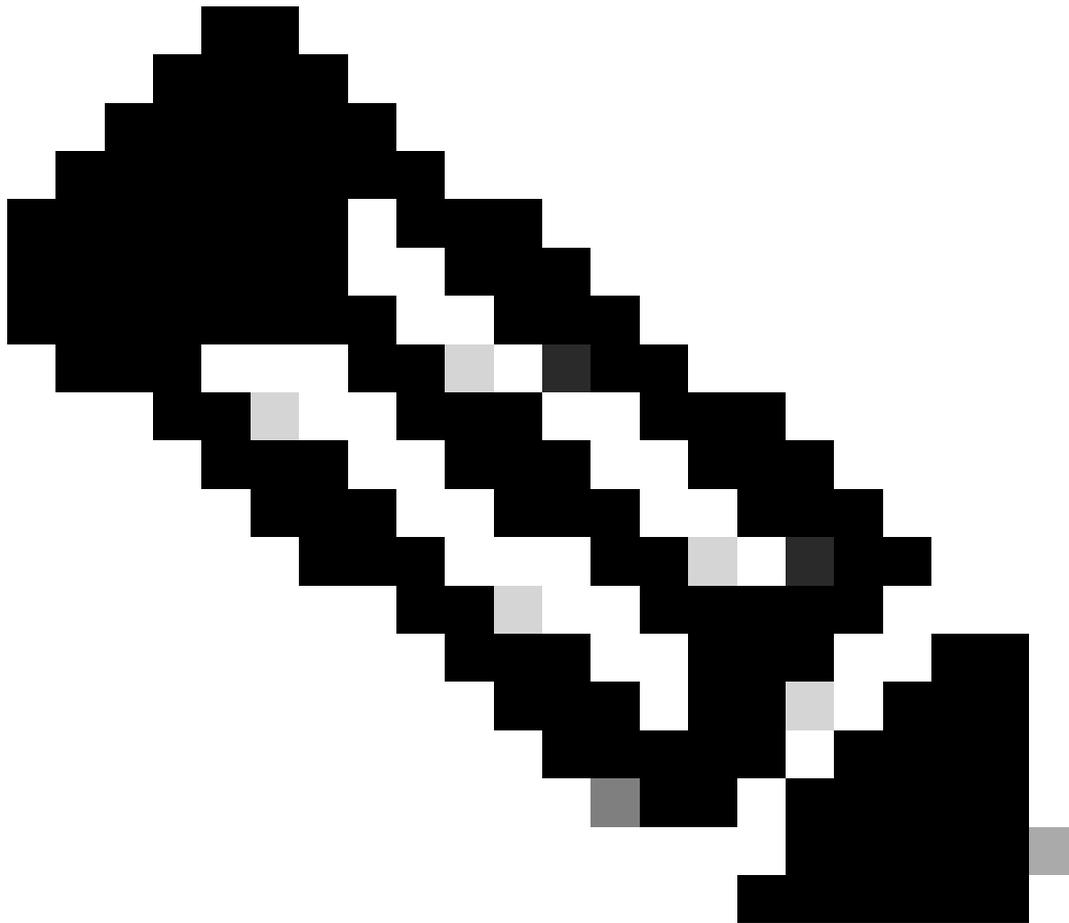
Identity Group

* Name

Description

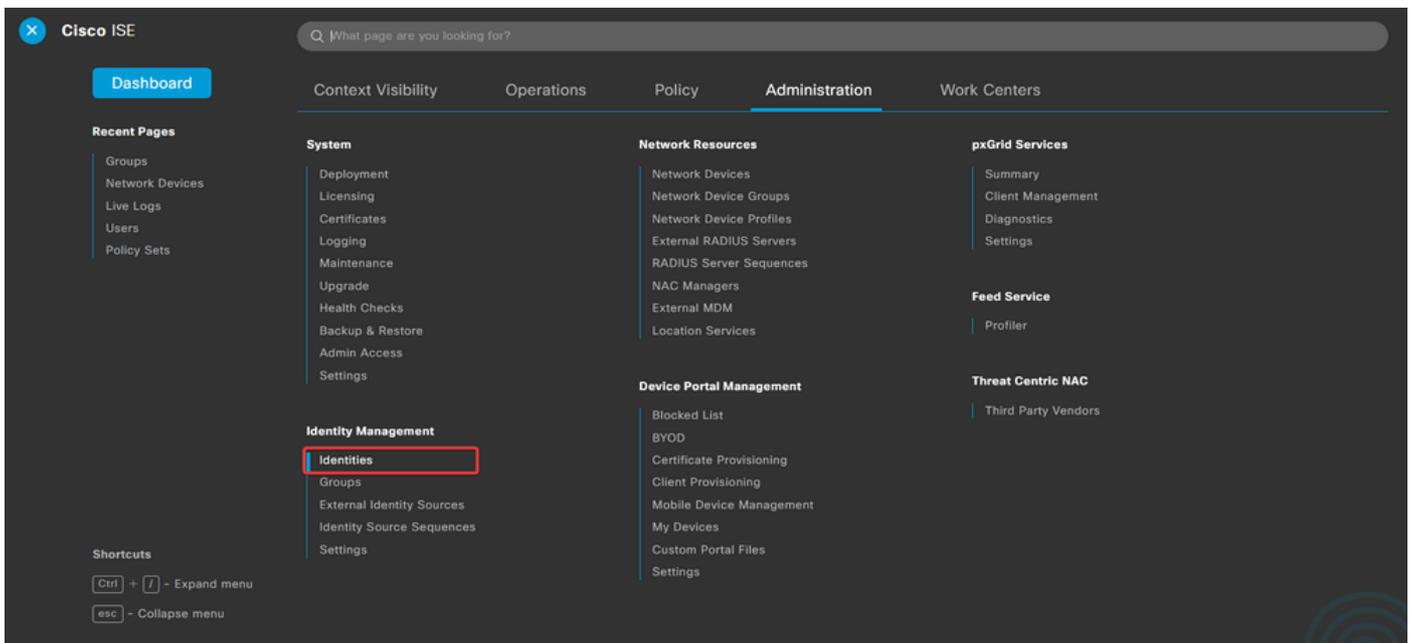
Submit

Cancel



注意：重複此步驟可根據需要建立任意多個組。

d. 導航至 Administration > Identity Management > Identities。



e. 按一下Add，以便在伺服器本地資料庫中建立新使用者。

輸入Username和Login Password。然後，導航到此頁末尾，選擇User Group。

點選Save。

Network Access Users

Status	Username	Description	First Name	Last Name	Email Address	User Identity Grou...	Admin
<input type="checkbox"/>	Enabled	user1				IT Group	
<input type="checkbox"/>	Enabled	user2				Marketing Group	

Network Access User

* Username user1

Status Enabled

Email

Passwords

Password Type: Internal Users

	Password	Re-Enter Password
* Login Password	●●●●●●●●	●●●●●●●●

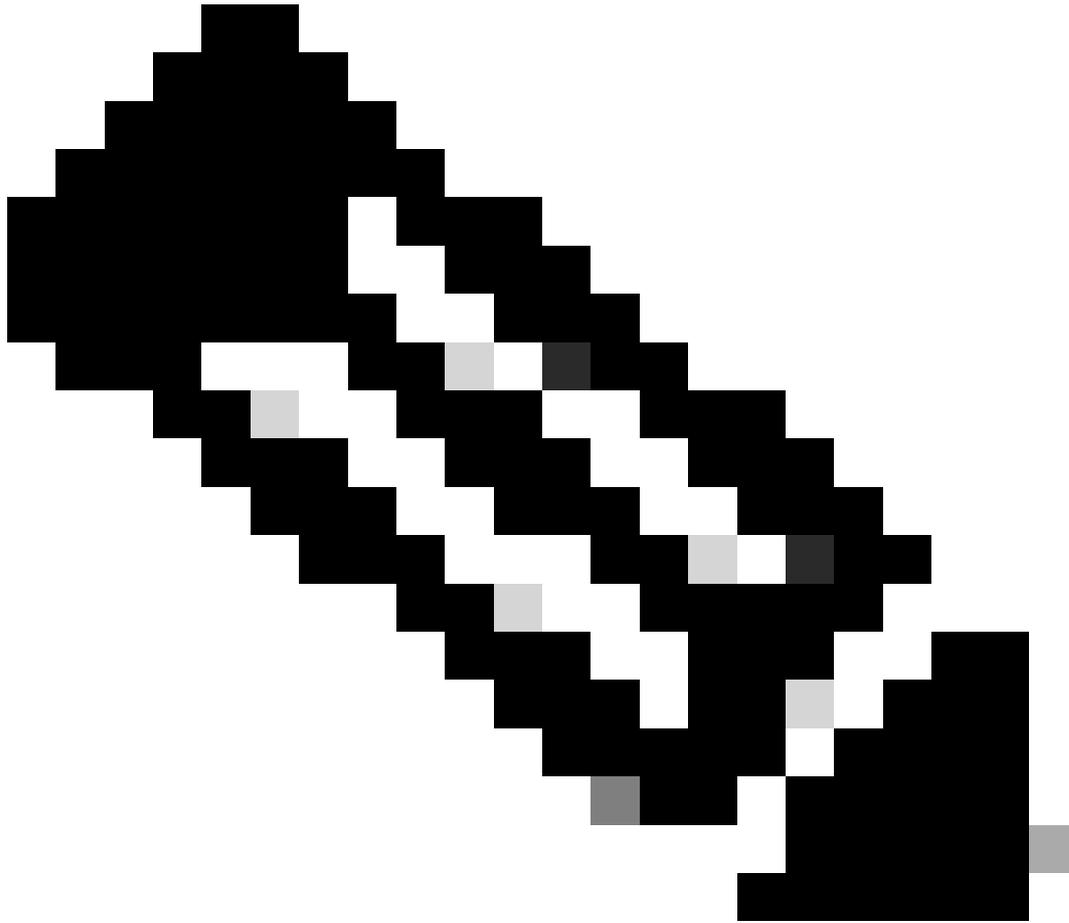
Generate Password ⓘ

Enable Password

Generate Password ⓘ

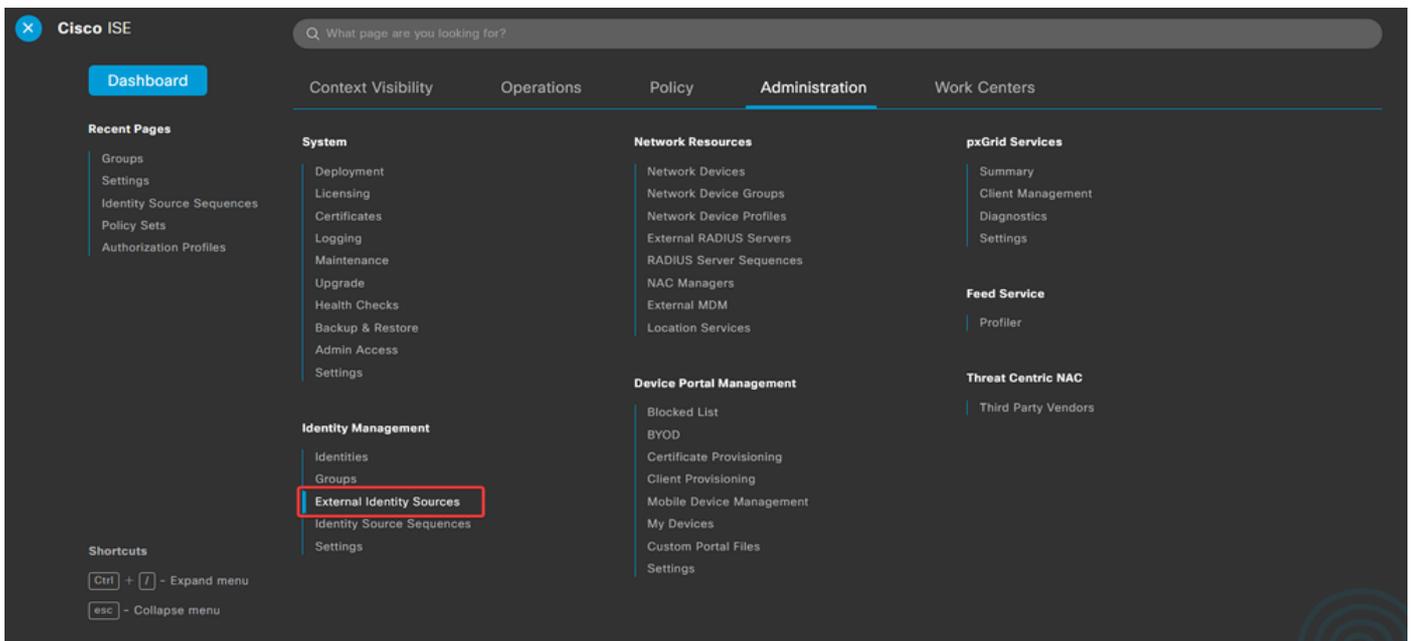
User Groups

IT Group



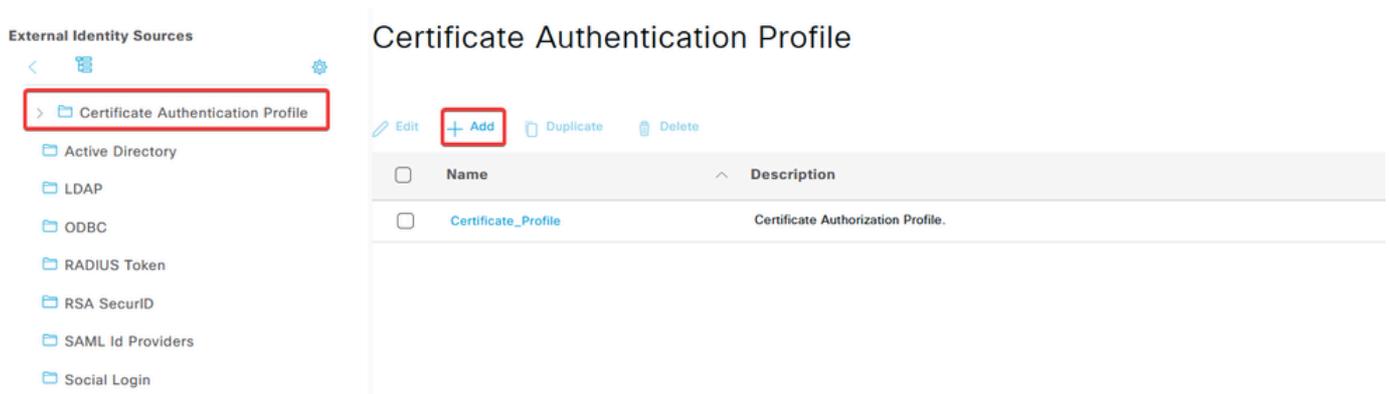
注意：必須配置使用者名稱和密碼才能建立內部使用者。即使在使用證書執行的RAVPN身份驗證中不需要此功能，這些使用者也可以用於其他需要密碼的內部服務。因此，請確保使用強密碼。

f. 導航到 [Administration > Identity Management > External Identify Sources](#)。



g. 按一下Add建立Certificate Authentication Profile。

憑證驗證設定檔指定如何驗證使用者端憑證，包括可以檢查憑證中的哪些欄位（主體替代名稱、一般名稱等）。



Certificate Authentication Profile

* Name

Description

Identity Store

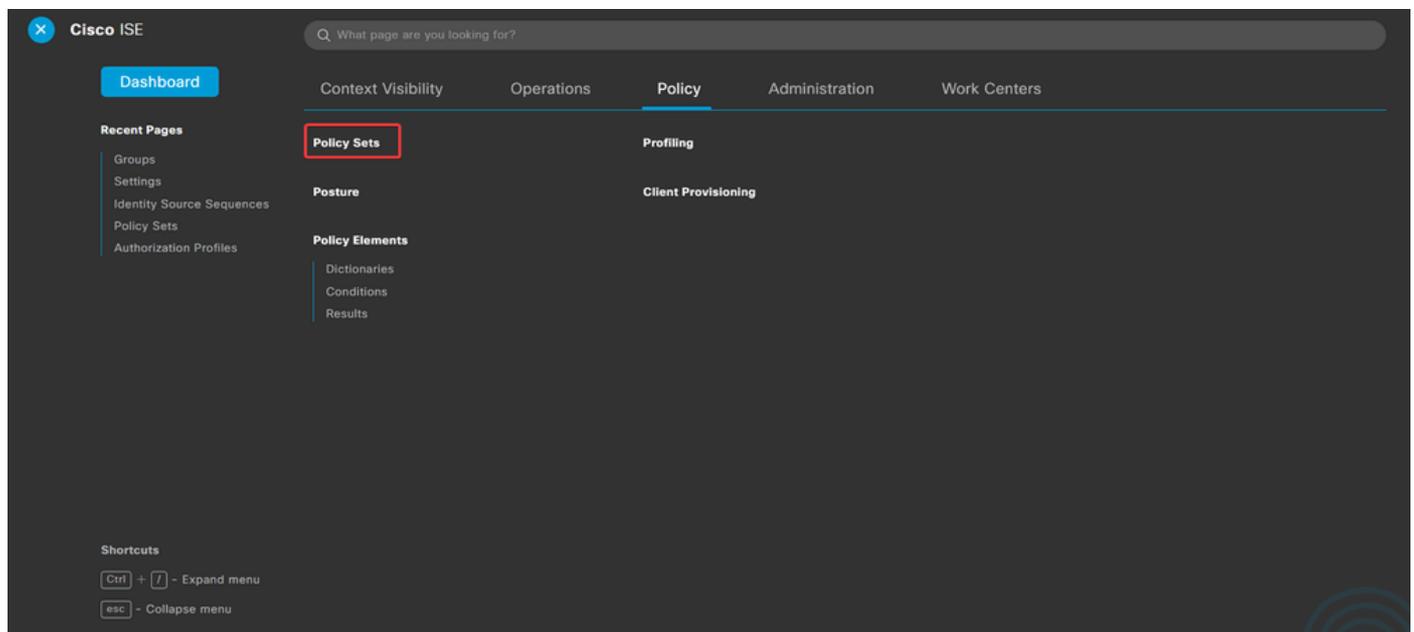
Use Identity From Certificate Attribute Subject - Common Name Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

Match Client Certificate Against Certificate In Identity Store Never Only to resolve identity ambiguity Always perform binary comparison

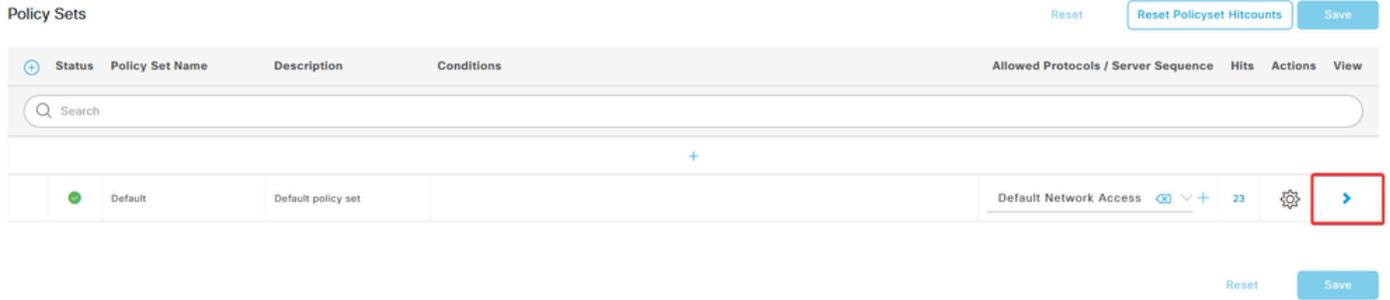
第3.2步：配置身份驗證策略

身份驗證策略用於驗證請求是否源自防火牆和特定連線配置檔案。

a. 導航至Policy > Policy Sets。



透過點選螢幕右側的箭頭選擇default authorization policy：



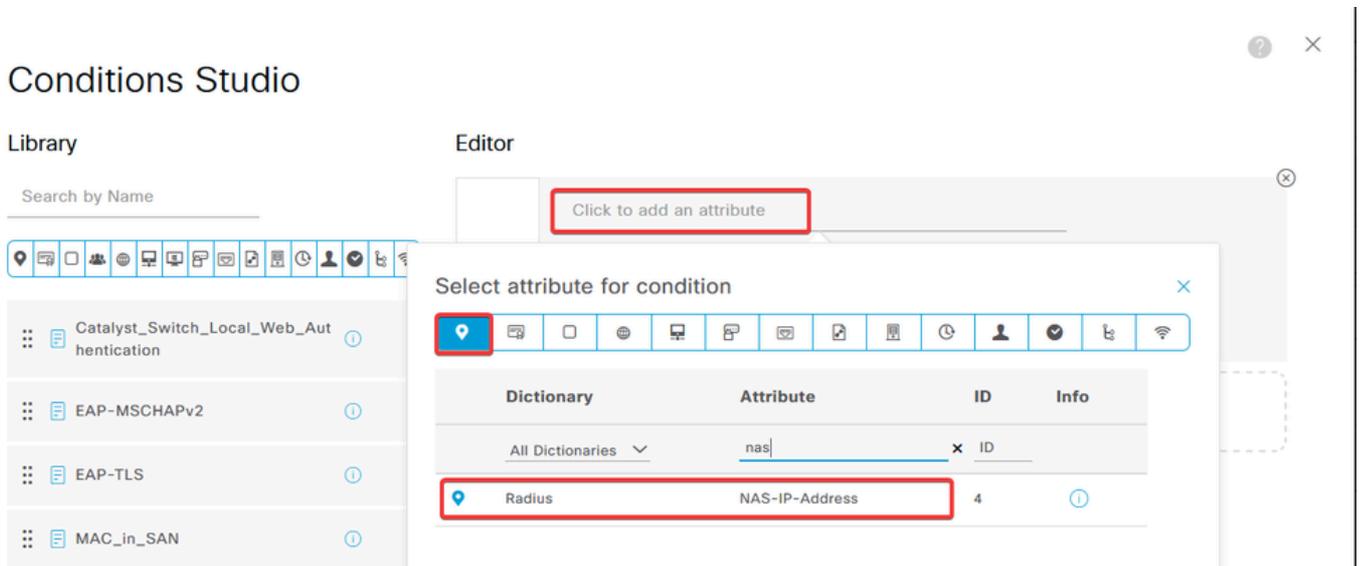
b. 按一下 Authentication Policy 旁邊的下拉選單箭頭將其展開。然後，按一下 add (+) 圖示以增加新規則。



輸入規則的名稱，然後選擇條件列下的 add (+) 圖示。



c. 按一下屬性編輯器文本框並按一下 NAS-IP-Address 圖示。輸入防火牆的 IP 地址。



d. 按一下 New 然後增加其他屬性 Tunnel-Group-name。 Connection Profile 輸入在 FMC 上配置的名稱。

Conditions Studio

Library

Search by Name



- Catalyst_Switch_Local_Web_Authentication
- EAP-MSCHAPv2
- EAP-TLS
- MAC_in_SAN
- Switch_Local_Web_Authentication
- Switch_Web_Authentication

Editor

Dictionary	Attribute	ID	Info
All Dictionaries	tunnel-group-name	x	
Cisco-VPN3000	CVPN3000/ASA/PIX7x-Tunnel-Group-Name	146	

Conditions Studio

Library

Search by Name



- Catalyst_Switch_Local_Web_Authentication
- EAP-MSCHAPv2
- EAP-TLS
- MAC_in_SAN
- Switch_Local_Web_Authentication

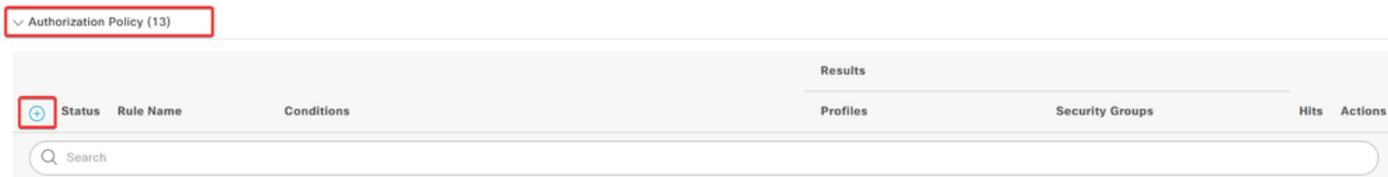
Editor

e.在「使用」列下，選擇已建立的Certificate Authentication Profile。藉由執行此動作，它會指定設定檔中定義用於辨識使用者的資訊。

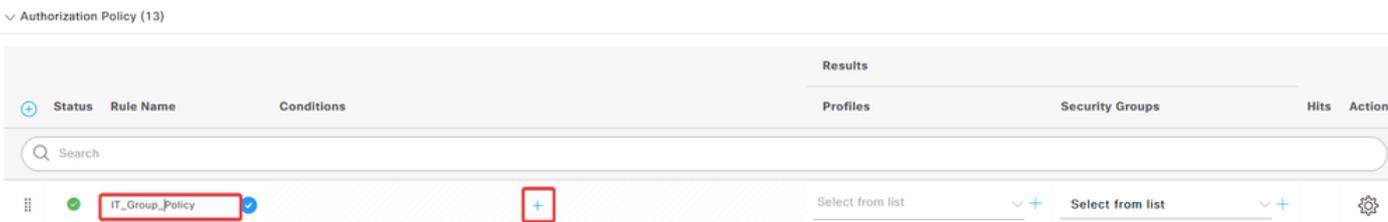
按一下Save。

第3.3步：配置授權策略

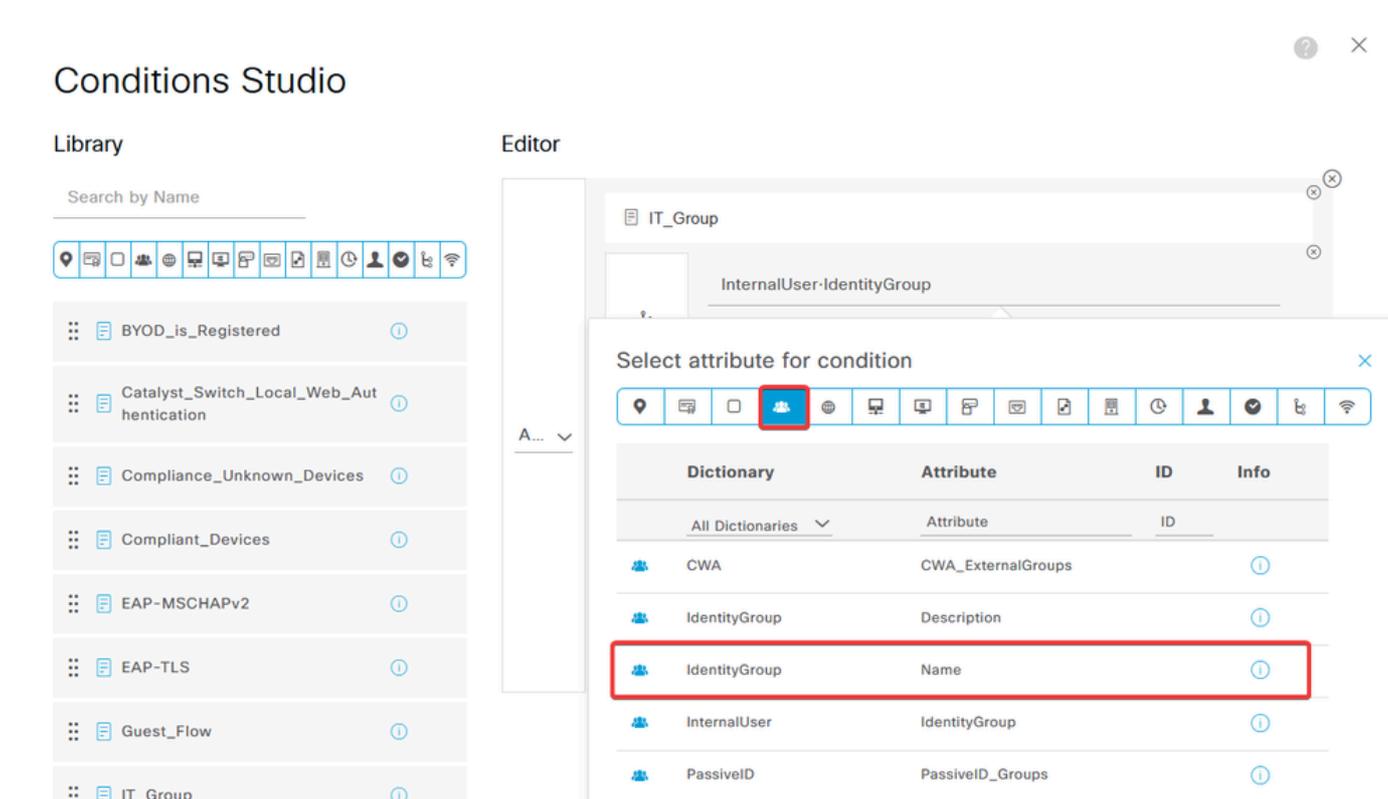
a. 按一下 Authorization Policy 旁邊的下拉選單箭頭將其展開。然後，按一下 add (+) 圖示以增加新規則。



輸入規則的名稱，然後選擇條件列下的圖示 add (+)。



b. 按一下屬性編輯器文本框並按一下 Identity group 圖示。選擇 Identity group - Name 屬性。



選擇 Equals 作為運算子，然後按一下下拉選單箭頭顯示可用選項並選擇 User Identity Groups:

o

Conditions Studio

Library

Search by Name

BYOD_is_Registered

Catalyst_Switch_Local_Web_Authentication

Compliance_Unknown_Devices

Compliant_Devices

EAP-MSCHAPv2

Editor

IT_Group

InternalUser-IdentityGroup

Equals

Choose from list or type

- User Identity Groups:GuestType_SocialLogin (default)
- User Identity Groups:GuestType_Weekly (default)
- User Identity Groups:IT Group
- User Identity Groups:Marketing Group
- User Identity Groups:OWN_ACCOUNTS (default)

Set to 'Is not'

c. 在配置檔案列中，按一下add (+)圖示並選擇Create a New Authorization Profile。

Authorization Policy (13)

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
●	IT_Group_Policy	AND IT_Group InternalUser-IdentityGroup EQUALS User Identity Groups:IT Group	Select from list	Select from list		⚙️
●	Wireless Black List Default	AND Wireless_Access IdentityGroup-Name EQUALS Endpoint Identity Groups:Blacklist	Create a New Authorization Profile	Select from list	0	⚙️

輸入profile Name。

Authorization Profile

* Name: IT_Group_Profile

Description: [Empty text area]

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement: ⓘ

Agentless Posture: ⓘ

Passive Identity Tracking: ⓘ

導航到Common Tasks並選中ASA VPN。然後，鍵入group policy name，該命令需要與FMC上建立的命令相同

。

∨ Common Tasks

ASA VPN

IT_Group



AVC Profile Name

UDN Lookup

下一個屬性已指定給每個群組：

∨ Attributes Details

Access Type = ACCESS_ACCEPT

Class = IT_Group

按一下Save。

注意：重複步驟3.3：為建立的每個組配置授權策略。

驗證

1. 運行命令 `show vpn-sessiondb anyconnect`，並驗證使用者是否使用了正確的組策略。

```
<#root>
```

```
firepower#
```

```
show vpn-sessiondb anyconnect
```

```
Session Type : AnyConnect
```

```
Username      : user1
```

```
Assigned IP   : 192.168.55.2      Index      : 64
```

```
Public IP    :
```

Protocol : AnyConnect-Parent
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none
Hashing : AnyConnect-Parent: (1)none
Bytes Tx : 15084 Bytes Rx : 99611
Group Policy : IT_Group Tunnel Group : FTD_CertAuth

Login Time : 22:21:43 UTC Tue Oct 22 2024
Duration : 3h:03m:50s
Inactivity : 0h:41m:44s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 96130a0f0004000067182577
Security Grp : none Tunnel Zone : 0

Username : User2

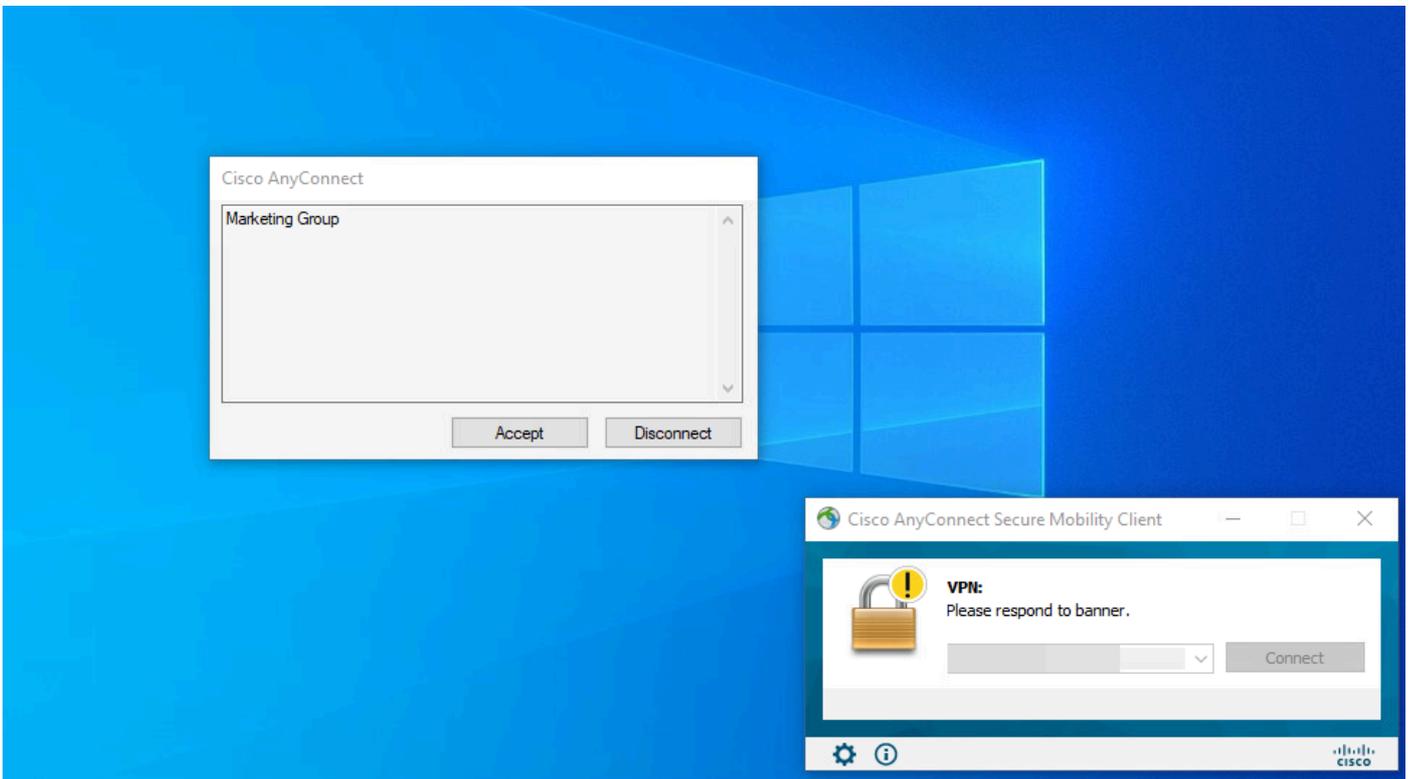
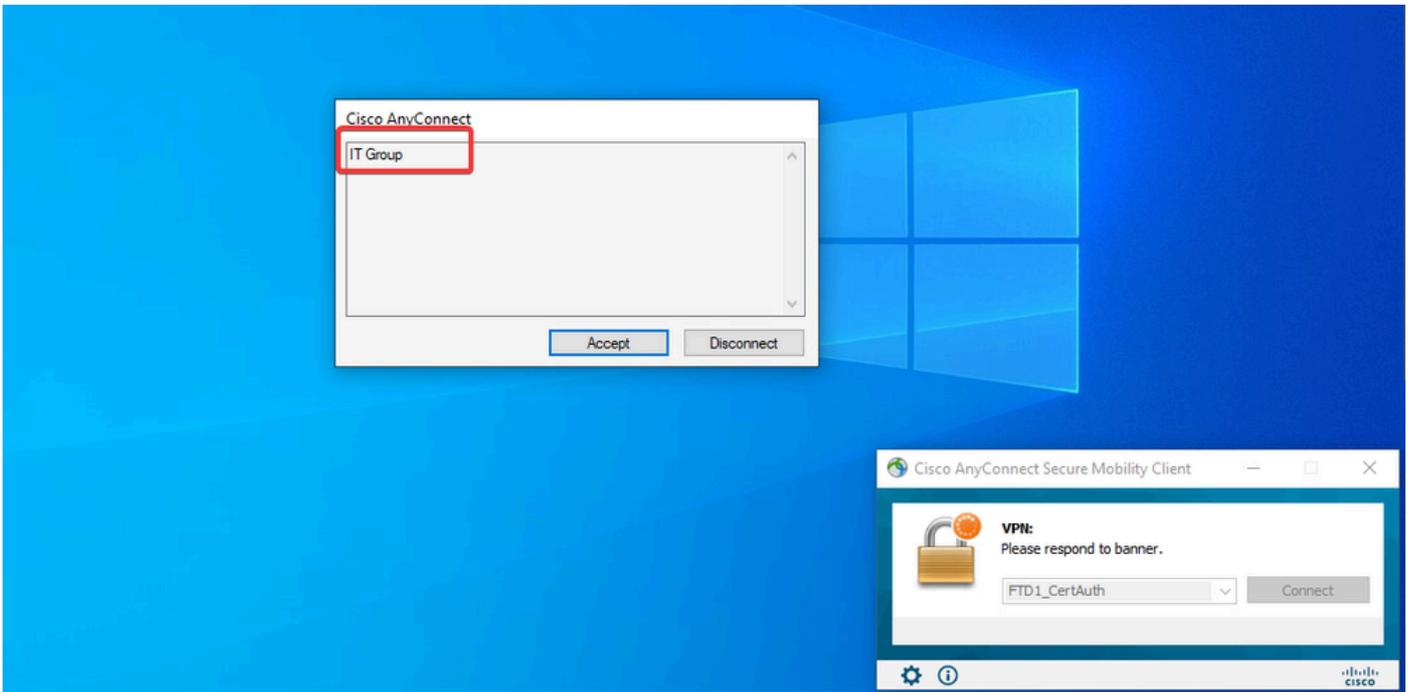
Index : 70

Assigned IP : 192.168.55.3 Public IP :
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx : 15112 Bytes Rx : 19738
Group Policy : Marketing_Group Tunnel Group : FTD_CertAuth

Login Time : 01:23:08 UTC Wed Oct 23 2024
Duration : 0h:02m:25s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 96130a0f0004600067184ffc
Security Grp : none Tunnel Zone : 0

firepower#

2. 在組策略中，可以配置當使用者成功連線時顯示的標語消息。每個標語都可用於標識具有授權的組。



3. 在即時日誌中，驗證連線是否使用適當的授權策略。按一下Details並顯示Authentication Report。

Live Logs Live Sessions

Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	0	0

Refresh: Never | Show: Latest 100 rec... | Within: Last 30 minu... | Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity G
Oct 25, 2024 08:38:03.6...	●	🔒	0	user1		Windows1...	Default	Default >>...	IT_Group_...				
Oct 25, 2024 08:38:03.6...	■	🔒		user1		Windows1...	Default	Default >>...	IT_Group_...		FTD		User Identit

Last Updated: Fri Oct 25 2024 14:42:41 GMT-0600 (GMT-06:00) Records Shown: 2

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

1. 可以從CSF的診斷CLI運行調試以進行證書身份驗證。

```
debug crypto ca 14
debug webvpn anyconnect 255
debug crypto ike-common 255
```

2. 使用AAA調試驗證本地和/或遠端屬性的分配。

```
debug aaa common 255
debug aaa shim 255
debug aaa authentication
debug aaa authorization
debug radius all
```

在ISE上：

1. 定位至Operations > RADIUS > Live Logs。

Cisco ISE

Q What page are you looking for?

Dashboard

Context Visibility Operations Policy Administration Work Centers

Recent Pages

- Policy Sets
- Authorization Profiles
- Results
- External Identity Sources
- Groups

RADIUS

- Live Logs
- Live Sessions

TACACS

- Live Logs

Adaptive Network Control

- Policy List
- Endpoint Assignment

Threat-Centric NAC Live Logs

Troubleshoot

- Diagnostic Tools
- Download Logs
- Debug Wizard

Reports

Shortcuts

- Ctrl + F - Expand menu
- esc - Collapse menu

Live Logs Live Sessions

Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 0 Client Stopped Responding 3 Repeat Counter 0

Refresh Never Show Latest 20 records Within Last 3 hours

Refresh Reset Repeat Counts Export To Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity G
Oct 23, 2024 01:26:29.3...	✓	🔒		User2		Windows1...	Default	Default >>...	Marketing...		FTD		User Identit
Oct 23, 2024 01:22:29.3...	✗	🔒		User2					DenyAccess		FTD		User Identit
Oct 23, 2024 01:21:46.9...	✗	🔒		User2					DenyAccess		FTD		User Identit
Oct 23, 2024 01:16:33.4...	✗	🔒		User2					DenyAccess		FTD		User Identit
Oct 22, 2024 10:25:14.1...	✓	🔒		user1		Windows1...	Default	Default >>...	IT_Group_...		FTD		User Identit
Oct 22, 2024 10:24:18.9...	✓	🔒		user1		Windows1...	Default	Default >>...	IT_Group_...		FTD		User Identit

Last Updated: Wed Oct 23 2024 12:33:54 GMT-0600 (GMT-06:00) Records Shown: 6

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）。