

使用ISE作為RADIUS伺服器配置FMC和FTD外部身份驗證

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[FMC的外部驗證](#)

[FTD的外部驗證](#)

[網路拓撲](#)

[設定](#)

[ISE 組態](#)

[FMC配置](#)

[FTD組態](#)

[驗證](#)

簡介

本文檔介紹安全防火牆管理中心和防火牆威脅防禦的外部身份驗證配置示例。

必要條件

需求

建議您瞭解以下主題：

- 透過GUI和/或外殼進行Cisco Secure Firewall Management Center初始配置。
- 在ISE上配置身份驗證和授權策略。
- 基本RADIUS知識。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- vFMC 7.2.5
- vFTD 7.2.5。
- ISE 3.2。

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。

背景資訊

當您為Secure Firewall系統的管理和管理使用者啟用外部身份驗證時，裝置會使用外部身份驗證對象中指定的輕型目錄訪問協定(LDAP)或RADIUS伺服器驗證使用者憑據。

FMC和FTD裝置可以使用外部驗證物件。您可以在不同的裝置/裝置型別之間共用相同的對象，或建立單獨的對象。

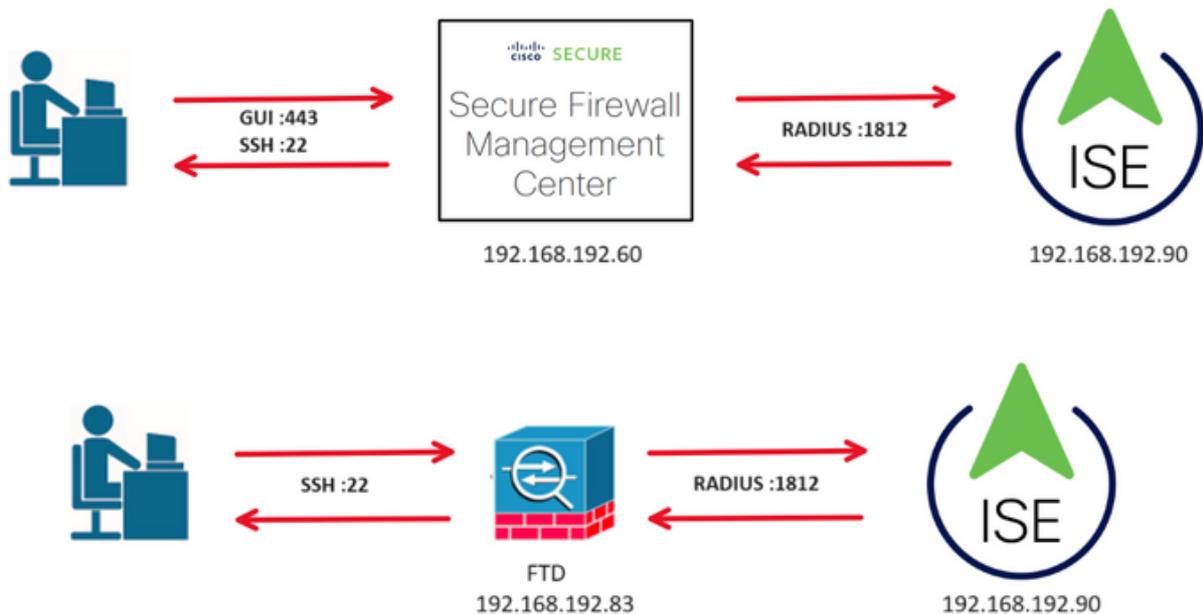
FMC的外部驗證

您可以為Web介面存取設定多個外部驗證物件。只有一個外部身份驗證對象可用於CLI或外殼訪問。

FTD的外部驗證

對於FTD，您只能啟用一個外部身份驗證對象。

網路拓撲



設定

ISE 組態



注意：有多種方法可以為網路訪問裝置(NAD) (例如FMC) 設定ISE身份驗證和授權策略。本文檔中介紹的示例是一個參考點，在此參考點中，我們建立了兩個配置檔案 (一個具有管理員許可權，另一個為只讀) ，可以對其進行調整以符合訪問網路的基線。可以在ISE上定義一個或多個授權策略，並返回RADIUS屬性值到FMC，然後對映到FMC系統策略配置中定義的本地使用者組。



步驟 1.新增網路裝置。導航到位於左上角的漢堡圖示
>管理>網路資源>網路裝置> +增加。

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 2

Edit + Add Duplicate Import Export Generate PAC Delete

Name	IP/Mask	Profile Name	Location	Type	Description
------	---------	--------------	----------	------	-------------

步驟 2. 為網路裝置對象分配名稱並插入FMC IP地址。

選中RADIUS 覈取方塊並定義共用金鑰。

稍後必須使用相同的金鑰來設定FMC。

完成後，按一下Save。

Administration - Network Resources

Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences | NAC Managers | More

Network Devices

Default Device
Device Security Settings

Network Devices List > FMC

Network Devices

Name FMC

Description

IP Address * IP: 192.168.192.60 / 32

Device Profile Cisco

Model Name vFMC

Software Version 7.2.5

Network Device Group

Location All Locations Set To Default

IPSEC No Set To Default

Device Type All Device Types Set To Default

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

Shared Secret ***** Show

Use Second Shared Secret

Second Shared Secret Show

步驟 2.1. 重複相同步驟以新增FTD。

為網路裝置對象分配名稱並插入FTD IP地址。

選中RADIUS 覈取方塊並定義共用金鑰。

完成後，按一下Save。

The screenshot shows the configuration page for a Network Device named 'FTD'. The IP Address is 192.168.192.83/32. The Device Profile is Cisco, Model Name is vFTD, and Software Version is 7.2.5. The RADIUS Authentication Settings section is expanded, and the RADIUS Authentication checkbox is checked. The Shared Secret is masked with asterisks.

Field	Value	Action
Name	FTD	
Description		
IP Address	192.168.192.83 / 32	
Device Profile	Cisco	
Model Name	vFTD	
Software Version	7.2.5	
Network Device Group		
Location	All Locations	Set To Default
IPSEC	No	Set To Default
Device Type	All Device Types	Set To Default
<input checked="" type="checkbox"/> RADIUS Authentication Settings		
Protocol	RADIUS	
Shared Secret	*****	Show
<input type="checkbox"/> Use Second Shared Secret		
Second Shared Secret		Show

步驟 2.3.驗證「Network Devices (網路裝置)」下顯示的兩個裝置。

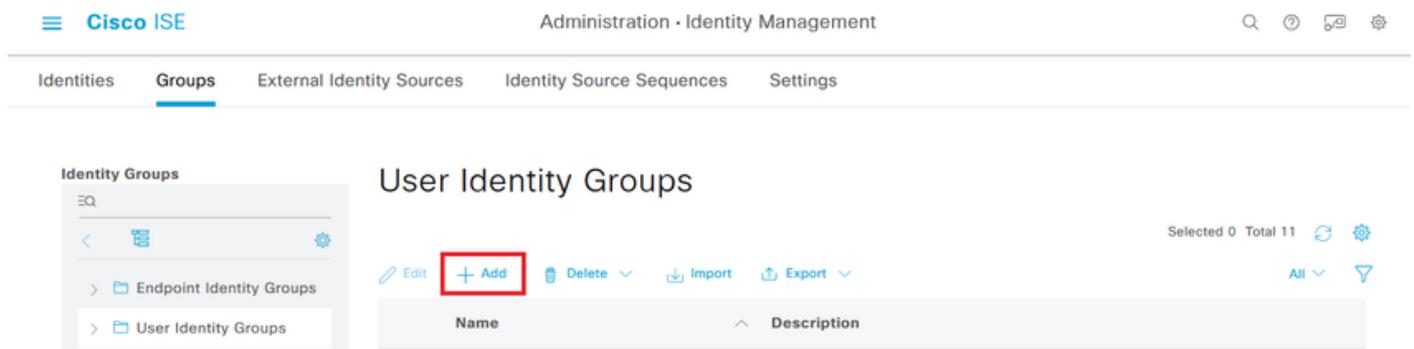
The screenshot shows the Network Devices list in Cisco ISE. Two devices are listed: FMC and FTD. The FTD device is highlighted in blue.

Name	IP/Mask	Profile Name	Location	Type	Description
FMC	192.168.192.60/32	Cisco	All Locations	All Device Types	
FTD	192.168.192.83/32	Cisco	All Locations	All Device Types	

步驟 3. 建立所需的使用者身份組。導航到位於左上角的漢堡圖示



>管理>身份管理>組>使用者身份組> +增加



步驟 4. 為每個組指定名稱並單獨儲存。在此範例中，我們將為管理員使用者建立群組，為唯讀使用者建立另一個群組。首先，為具有管理員許可權的使用者建立組。

Cisco ISE Administration · Identity Management

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

Identity Groups

User Identity Groups > FMC and FTD admins

Identity Group

* Name FMC and FTD admins

Description FMC and FTD admins ISE local.

Save Reset

步驟 4.1. 為只讀使用者建立第二個組。

Cisco ISE Administration · Identity Management

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

Identity Groups

User Identity Groups > FMC and FTD ReadOnly

Identity Group

* Name FMC and FTD ReadOnly

Description FMC and FTD ReadOnly.

Save Reset

步驟 4.2. 驗證兩個群組會顯示在[使用者身份群組清單]下。使用過濾器可以輕鬆找到它們。

Cisco ISE Administration · Identity Management

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

Identity Groups

User Identity Groups

Selected 0 Total 2

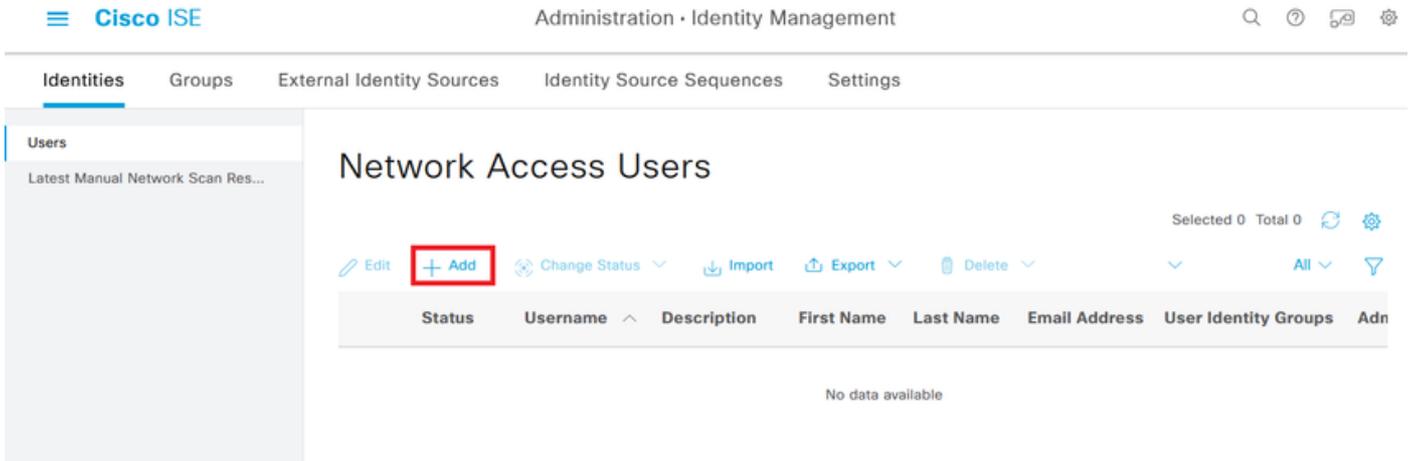
Edit + Add Delete Import Export Quick Filter

Name	Description
fmc	
<input type="checkbox"/> FMC and FTD ReadOnly	FMC and FTD ReadOnly
<input type="checkbox"/> FMC and FTD admins	FMC and FTD admins ISE local.

步驟 5. 建立本地使用者並將他們增加到其對應組。導航到



> Administration > Identity Management > Identities > + Add.



步驟 5.1. 首先建立具有管理員許可權的使用者。為它指定名稱、密碼和組FMC和FTD管理員。

Users

Latest Manual Network Scan Res...

Network Access Users List > New Network Access User

Network Access User

* Username firewall_admin

Status Enabled ▾

Account Name Alias ⓘ

Email

Passwords

Password Type: Internal Users ▾

Password Lifetime:

- With Expiration ⓘ
- Never Expires ⓘ

	Password	Re-Enter Password	
* Login Password	<input type="password"/>	<input type="password"/>	<input type="button" value="Generate Password"/> ⓘ
Enable Password	<input type="password"/>	<input type="password"/>	<input type="button" value="Generate Password"/> ⓘ

Users

Latest Manual Network Scan Res...

User Groups

⋮ FMC and FTD admins ▾ ⓘ +

步驟 5.2. 增加具有只讀許可權的使用者。分配名稱、口令和組FMC和FTD ReadOnly。

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 firewall_readuser

Status Enabled ▾

Account Name Alias ⓘ

Email

Passwords

Password Type: Internal Users ▾

Password Lifetime:

- With Expiration ⓘ
- Never Expires ⓘ

Password Re-Enter Password

* Login Password ⓘ

Enable Password ⓘ

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Res...

User Groups

⋮ FMC and FTD ReadOnly ▾ ⓘ +

Cancel

步驟 6. 為管理員使用者建立授權配置檔案。

導航到



>策略>策略元素>結果>授權>授權配置檔案>+增加。

定義授權配置檔案的名稱，保留Access Type為ACCESS_ACCEPT，並在Advanced Attributes Settings下增加值為Administrator的Radius > Class—[25]，然後按一下Submit。

The screenshot shows the Cisco ISE web interface for configuring an Authorization Profile. The breadcrumb navigation is "Policy > Policy Elements > Authorization Profiles > FMC and FTD Admins". The "Results" tab is selected in the top navigation. On the left, a sidebar menu shows "Authentication", "Authorization", "Profiling", and "Posture", with "Authorization Profiles" highlighted under the "Authorization" section. The main configuration area is titled "Authorization Profile" and contains the following fields:

- * Name: FMC and FTD Admins
- Description: (Empty text box)
- * Access Type: ACCESS_ACCEPT (dropdown menu)
- Network Device Profile: Cisco (dropdown menu)
- Service Template: (Empty dropdown menu)

Dictionarys Conditions **Results**

Authentication >

Authorization >

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

Advanced Attributes Settings

⋮ Radius:Class = Administrator - +

Attributes Details

Access Type = ACCESS_ACCEPT
Class = Administrator

Submit Cancel

步驟 7. 重複上一步為只讀使用者建立授權配置檔案。這次使用值ReadUser而非Administrator建立RADIUS類。

Dictionarys Conditions **Results**

Authentication >

Allowed Protocols

Authorization >

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name FMC and FTD ReadUser

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Navigation: Dictionaries | Conditions | **Results**

Left sidebar menu:

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

Main content area:

Advanced Attributes Settings

⋮ Radius:Class ▾ = ReadUser ▾ - +

Attributes Details

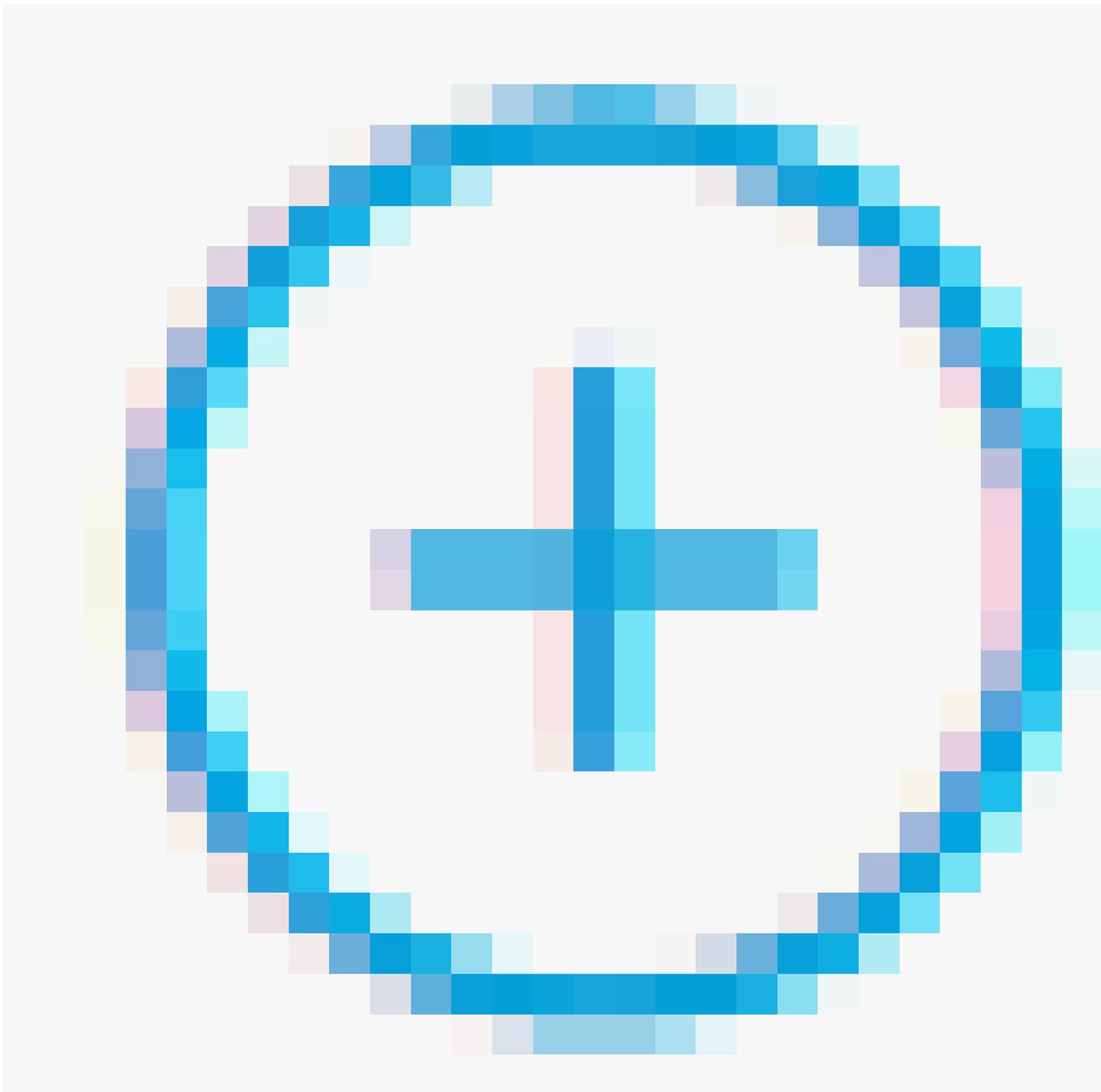
```
Access Type = ACCESS_ACCEPT
Class = ReadUser
```

Buttons: **Submit** (highlighted with a red box) | Cancel

步驟 8. 建立與FMC IP地址匹配的策略集。這是為了防止其他裝置向使用者授予訪問許可權。



導航到位於左上角的
>策略>策略集>



o

Policy Sets

Reset

Reset Policyset Hitcounts

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
--------	-----------------	-------------	------------	-------------------------------------	------	---------	------

Search

	Default	Default policy set		Default Network Access	45		
--	---------	--------------------	--	------------------------	----	--	--

Reset

Save

步驟 8.1. 新行位於策略集的頂部。

為新策略命名，並為匹配FMC IP地址的RADIUS NAS-IP-Address 屬性增加一個頂級條件。

將第二個條件與OR結合以包括FTD的IP位址。

按一下Use以保留更改並退出編輯器。

Conditions Studio

Library

Search by Name

5G

Catalyst_Switch_Local_Web_Authentication

Source FMC

Switch_Local_Web_Authentication

Switch_Web_Authentication

Wired_802.1X

Wired_MAB

Wireless_802.1X

Wireless_Access

Editor

Radius-NAS-IP-Address

Equals 192.168.192.60

Radius-NAS-IP-Address

Equals 192.168.192.83

OR

NEW AND OR

Set to 'Is not'

Duplicate Save

Close Use

步驟 8.2. 完成後按一下Save。

Cisco ISE

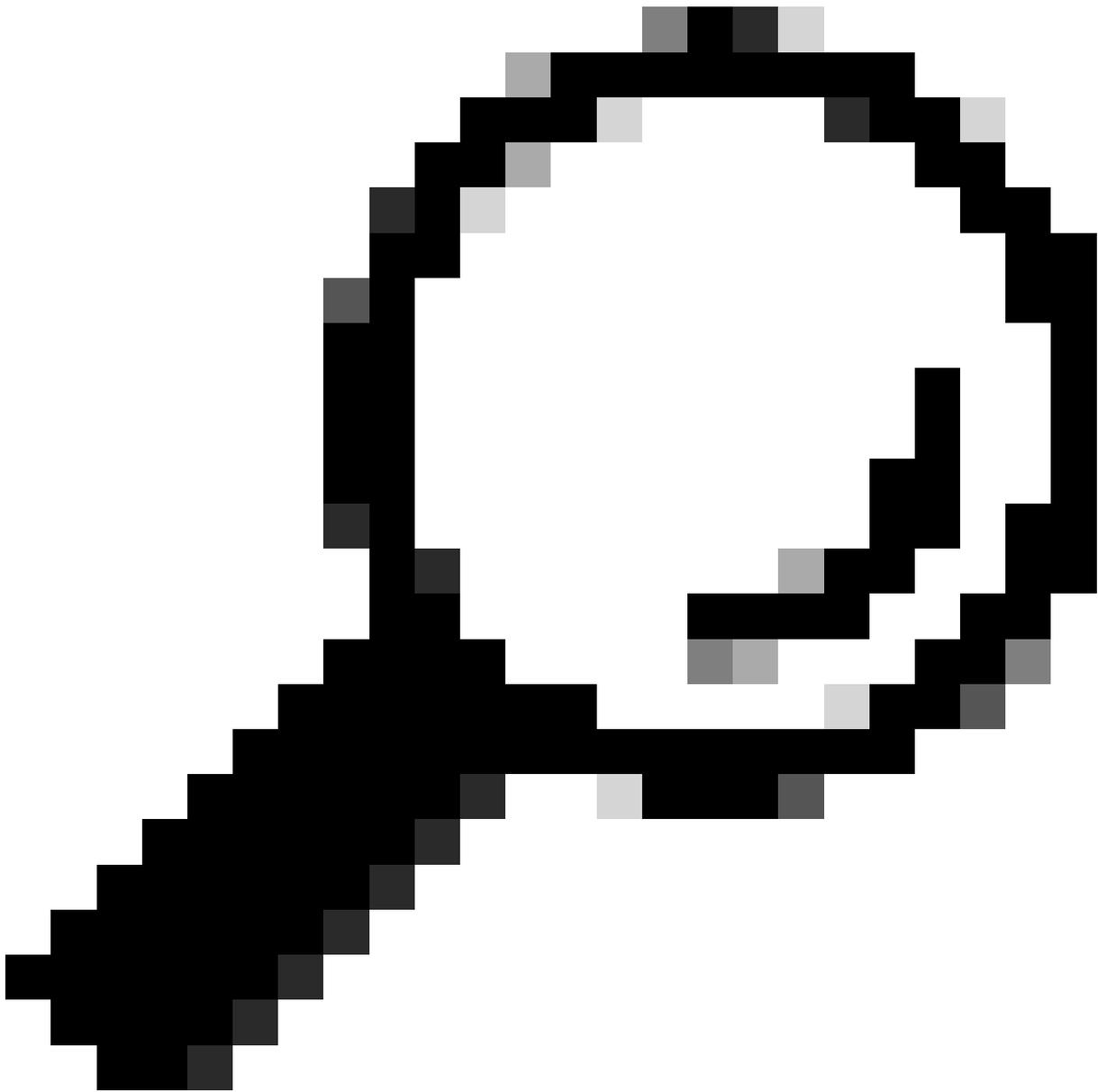
Policy · Policy Sets

Policy Sets

Reset Reset Policyset Hitcounts Save

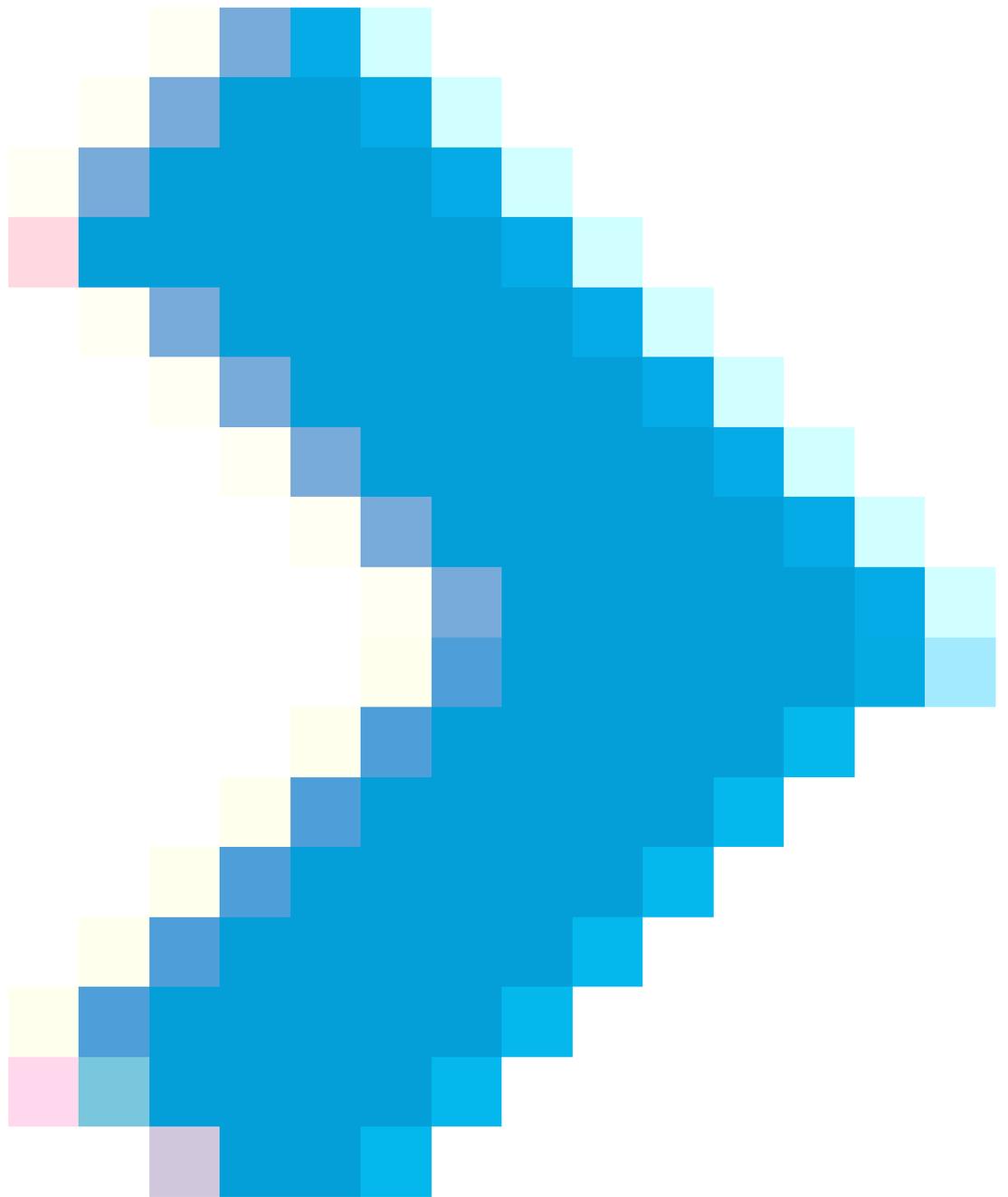
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	FMC and FTD Access	Management Access	OR Radius-NAS-IP-Address EQUALS 192.168.192.60 Radius-NAS-IP-Address EQUALS 192.168.192.83	Default Network Access	0	⚙️	➔
●	Default	Default policy set		Default Network Access	0	⚙️	➔

Reset Save



提示：在本練習中，我們允許預設網路訪問協定清單。您可以建立一個新清單，並根據需要縮小其範圍。

步驟 9. 透過按一下位於行末尾的



圖示來檢視新的策略集。

展開Authorization Policy選單並推送



圖示以增加新規則，以允許對具有管理員許可權的使用者進行訪問。

給它一個名字。

設定條件以匹配Dictionary Identity Group(其屬性名稱為Equals User Identity Groups : FMC and FTD admins) (在步驟4中建立的組名)，然後按一下Use。

Conditions Studio



Library

- Search by Name
- 5G
 - BYOD_is_Registered
 - Catalyst_Switch_Local_Web_Authentication
 - Compliance_Unknown_Devices
 - Compliant_Devices
 - EAP-MSCHAPv2
 - EAP-TLS
 - FMC and FTD Admin

Editor

IdentityGroup Name

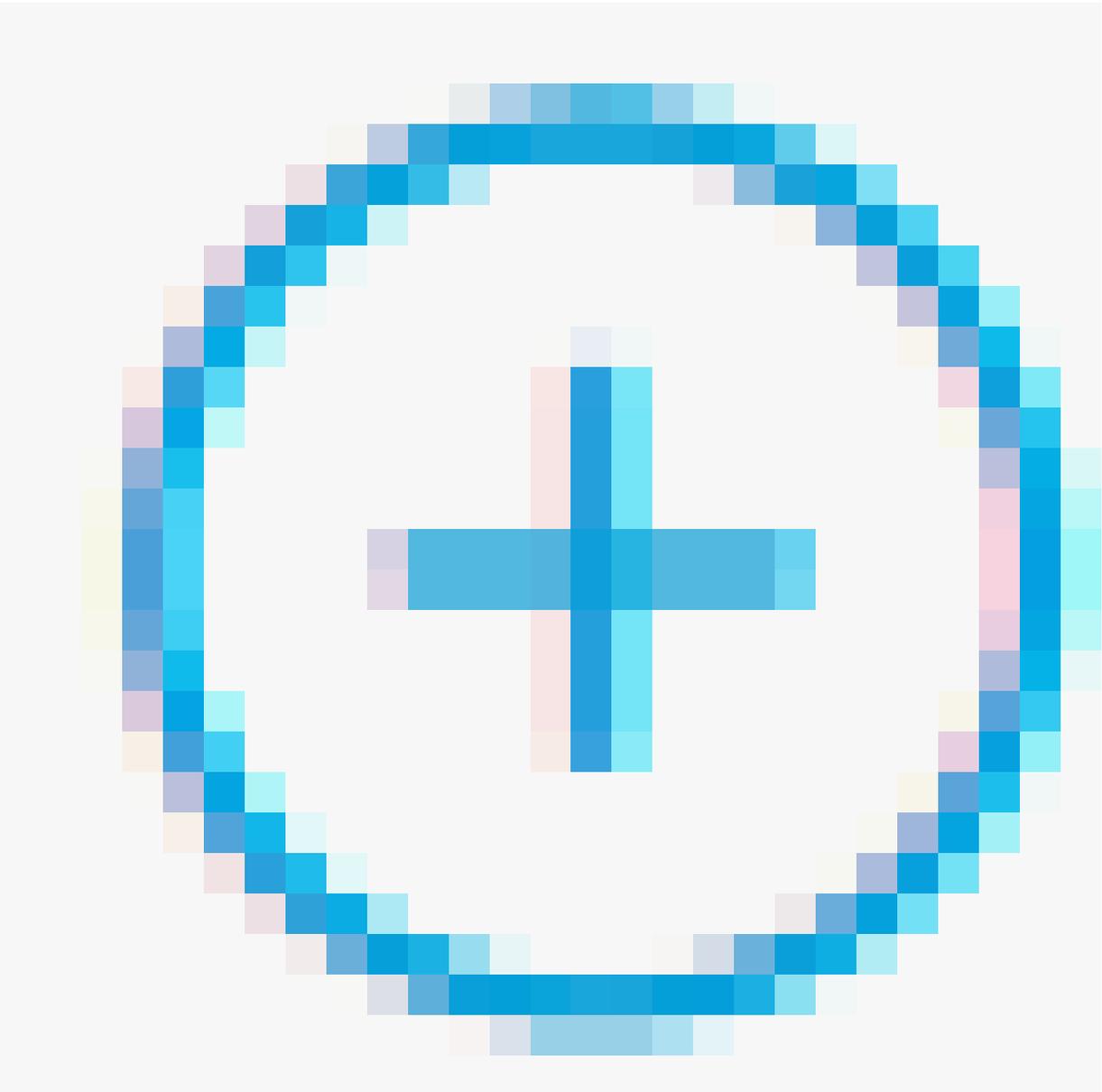
Equals User Identity Groups:FMC and FTD admins

Set to 'is not'

Duplicate Save

NEW AND OR

Close



步驟 10. 點選

圖示增加第二條規則，以允許訪問具有只讀許可權的使用者。

給它一個名字。

設定條件以匹配屬性Name Equals User Identity Groups : FMC和FTD ReadOnly (在步驟4中建立的組名) 的詞典身份組，然後按一下Use。

Conditions Studio

The screenshot shows the 'Conditions Studio' interface. On the left is a 'Library' with a search bar and a list of conditions: 5G, BYOD_is_Registered, Catalyst_Switch_Local_Web_Authentication, and Compliance_Unknown_Devices. On the right is the 'Editor' where a condition is being configured: 'IdentityGroup-Name' equals 'User Identity Groups:FMC and FTD ReadOnly'. Below the editor are 'NEW AND OR' options. At the bottom right, a red box highlights the 'Use' button.

步驟 11.分別為每個規則設定授權配置檔案並點選Save。

The screenshot shows the 'Policy - Policy Sets' configuration page in Cisco ISE. The main table lists policy sets with columns for Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. The 'FMC and FTD Access' policy set is expanded to show two conditions: 'Radius-NAS-IP-Address EQUALS 192.168.192.60' and 'Radius-NAS-IP-Address EQUALS 192.168.192.83'. Below this, the 'Results' table shows three rules: 'FMC and FTD read user access' (with condition 'IdentityGroup-Name EQUALS User Identity Groups:FMC and FTD ReadOnly'), 'FMC and FTD admin user access' (with condition 'IdentityGroup-Name EQUALS User Identity Groups:FMC and FTD admins'), and 'Default'. A red box highlights the 'Save' button at the bottom right.

FMC配置

步驟 1.在System > Users > External Authentication > + Add External Authentication Object下建立

外部身份驗證對象。

The screenshot shows the 'External Authentication' configuration page in the Firewall Management Center. The breadcrumb is 'System / Users / External Authentication'. The page has tabs for 'Users', 'User Roles', 'External Authentication', and 'Single Sign-On (SSO)'. At the top right, there are buttons for 'Save', 'Cancel', and 'Save and Apply'. Below these, there are fields for 'Default User Role' (set to 'None') and 'Shell Authentication' (set to 'Disabled'). A red box highlights a '+ Add External Authentication Object' button. Below this is a table with columns 'Name', 'Method', and 'Enabled', which is currently empty with the text 'No data to Represent'.

步驟 2.選擇RADIUS作為「Authentication Method」。

在External Authentication Object下，為新對象指定Name。

接下來，在主伺服器設定中插入ISE IP地址和您在ISE配置的步驟2中使用的同一RADIUS金鑰。

The screenshot shows the 'Create External Authentication Object' configuration page. The breadcrumb is 'System / Users / Create External Authentication Object'. The page has tabs for 'Users', 'User Roles', 'External Authentication', and 'Single Sign-On (SSO)'. The main configuration area is titled 'External Authentication Object' and contains the following fields:

- Authentication Method:** A dropdown menu set to 'RADIUS'.
- Name:** A text input field containing 'ISE_Radius'.
- Description:** An empty text input field.
- Primary Server:**
 - Host Name/IP Address:** A text input field containing '192.168.192.90'.
 - Port:** A text input field containing '1812'.
 - RADIUS Secret Key:** A text input field containing a series of dots.
- Backup Server (Optional):**
 - Host Name/IP Address:** An empty text input field.
 - Port:** A text input field containing '1812'.
 - RADIUS Secret Key:** An empty text input field.
- RADIUS-Specific Parameters:**
 - Timeout (Seconds):** A text input field containing '30'.

步驟 3.插入在ISE配置的步驟6和步驟7分別為firewall_admin和firewall_readuser配置的RADIUS類屬性值。

RADIUS-Specific Parameters

Timeout (Seconds)

Retries

Access Admin

Administrator

Discovery Admin

External Database User

Intrusion Admin

Maintenance User

Network Admin

Security Analyst

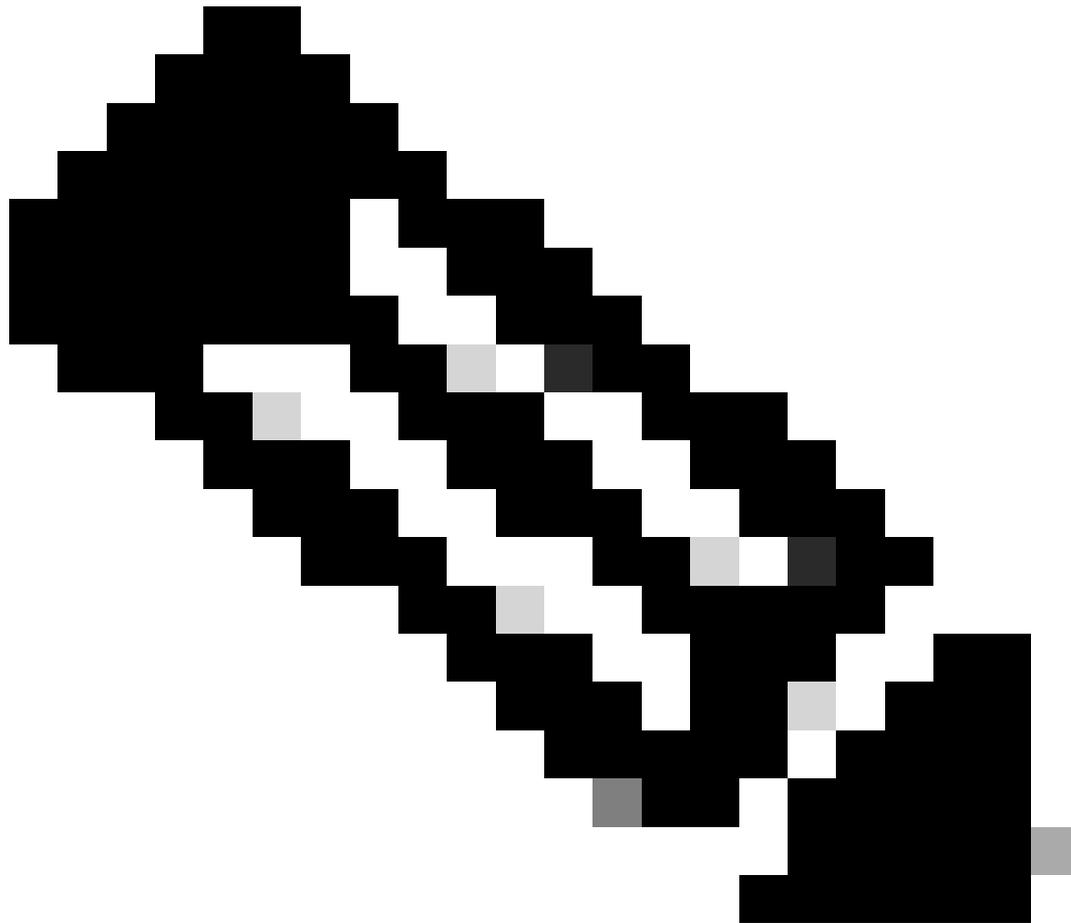
Security Analyst (Read Only)

Security Approver

Threat Intelligence Director (TID) User

Default User Role

To specify the default user role if user is not found in any group



注意：FTD和FMC的逾時範圍不同，因此如果您共用物件並變更預設值30秒，請確定FTD裝置的逾時範圍不要超過較小的範圍（1-300秒）。如果將超時設定為較高的值，則威脅防禦RADIUS配置不起作用。

步驟 4.用能夠獲得CLI訪問許可權的使用者名稱填充CLI訪問過濾器下的管理員CLI訪問使用者清單。

完成後，按一下Save。

CLI Access Filter

(For Firewall Management Center (all versions) and Firewall Threat Defense (6.2.3 and 6.3), define users for CLI access. For Firewall Threat Defense 6.4 and later, we recommend defining users on the RADIUS server. Click [here](#) for more information)

Administrator CLI Access User List ex. user1, user2, user3 (lowercase letters only).

▸ Define Custom RADIUS Attributes

Additional Test Parameters

User Name

Password

*Required Field

步驟 5. 啟用新物件。將其設定為FMC的Shell身份驗證方法，然後按一下「儲存並應用」。

Firewall Management Center
System / Users / External Authentication

Overview Analysis Policies Devices Objects Integration Deploy

Users User Roles External Authentication Single Sign-On (SSO)

Default User Role: None Shell Authentication Enabled (ISE_Radius) + Add External Authentication Object

Name	Method	Enabled
1. ISE_Radius	RADIUS	<input checked="" type="checkbox"/>

FTD組態

步驟 1. 在FMC GUI中，導航至裝置>平台設定。編輯您目前的原則，或建立新的原則（如果您沒有將任何原則指派給您需要存取的FTD）。啟用External Authentication下的RADIUS伺服器，然後按一下Save。

Firewall Management Center
Devices / Platform Settings Editor

Overview Analysis Policies Devices Objects Integration

Deploy You have unsaved changes

FTD Policy

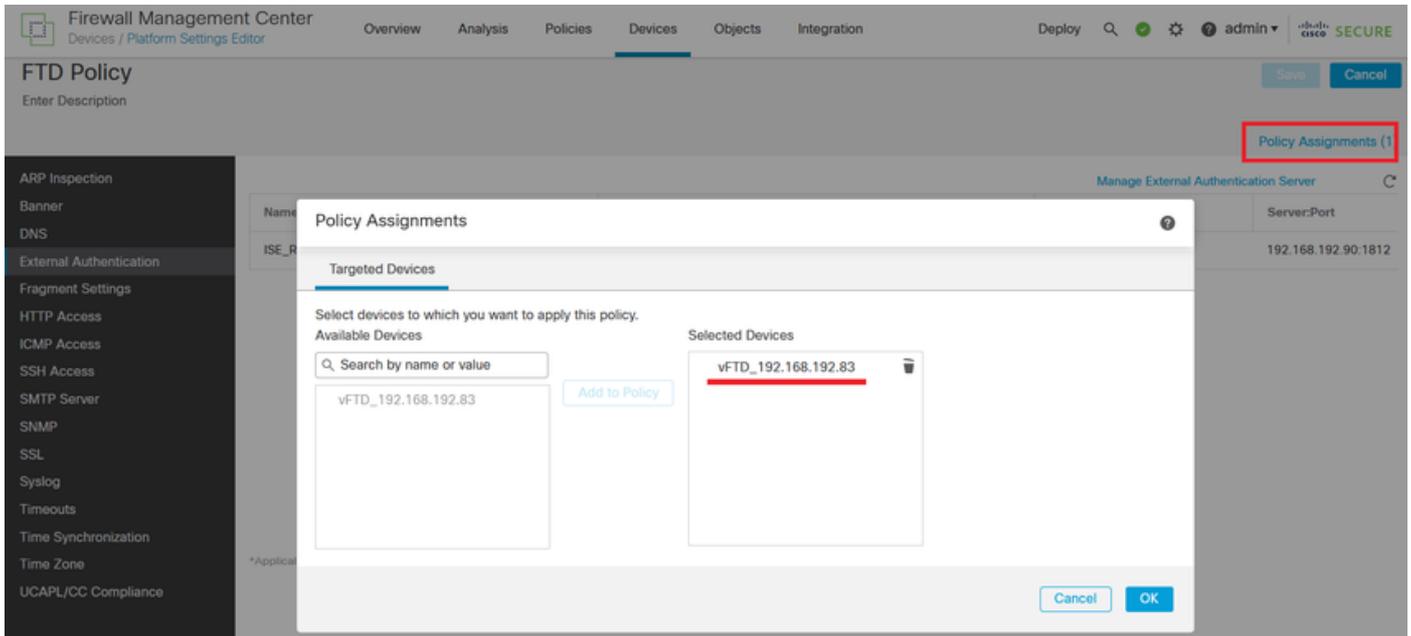
Enter Description

Policy Assignments (1)

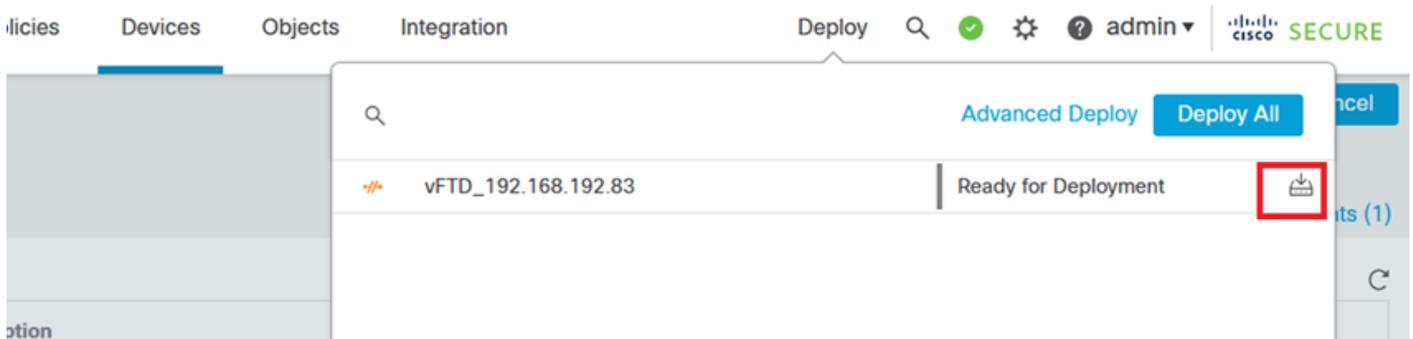
Manage External Authentication Server

Name	Description	Method	Server:Port	Encryption	Enabled
ISE_Radius		RADIUS	192.168.192.90:1812	no	<input checked="" type="checkbox"/>

步驟 2. 確定您需要存取的FTD列在「Policy Assignments as a Selected Device」下。

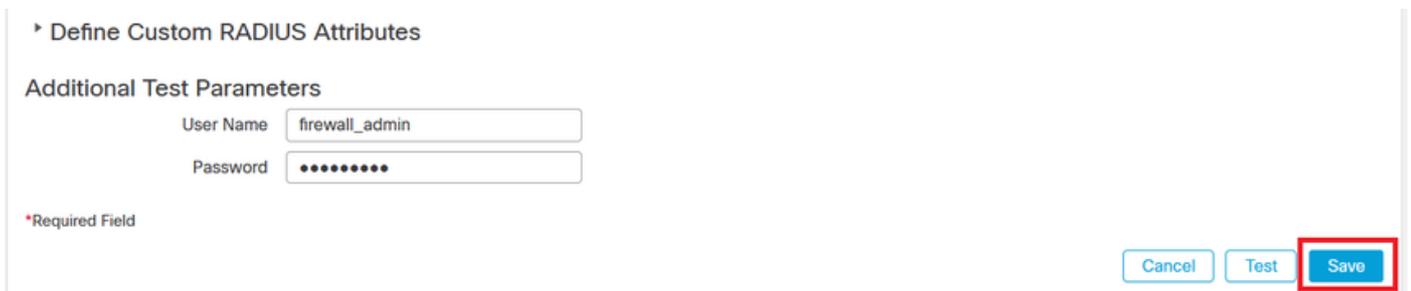


步驟 3. 部署變更。



驗證

- 測試您的新部署是否工作正常。
- 在FMC GUI中，導航到RADIUS伺服器設定，然後向下滾動到Additional Test Parameters部分。
- 輸入ISE使用者的使用者名稱和密碼，然後點選測試。



- 成功的測試在瀏覽器窗口的頂部顯示綠色的Success Test Complete 消息。



✔ Success
Test Complete. ✕

External Authentication Object

Authentication Method

Name *

- 有關詳細資訊，可以展開測試輸出下的Details。

▸ Define Custom RADIUS Attributes

Additional Test Parameters

User Name

Password

Test Output

Show Details ▾

```
check_auth_radius: szUser: firewall_admin
RADIUS config file: /var/tmp/4VQqxhXof/radiusclient_0.conf
radiusauth - response: [User-Name=firewall_admin]
radiusauth - response: [Class=Administrator]
radiusauth - response: [Class=CACS:c0a8c05a_cNaQKf8ZB2sOTPFOSbmj8V6n727Es2627TeUjzXUdA:ISE-LVILLAFR/479011358/67]
"firewall_admin" RADIUS Authentication OK
check_is_radius_member attrib match found: [Class=Administrator] - [Class=Administrator] *****
role_bee2eb18-e129-11df-a04a-42c66f0a3b36:
```

*Required Field

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）。