使用ISE作為RADIUS伺服器配置FMC和FTD外部身份驗證

目錄

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。

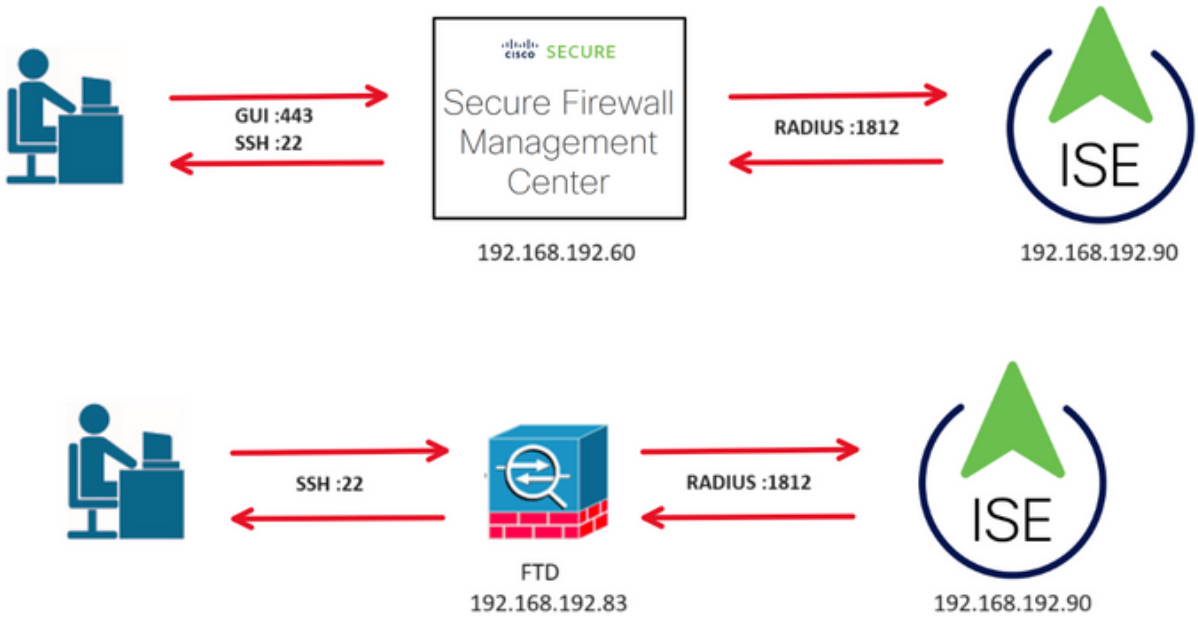
FMC的外部驗證

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

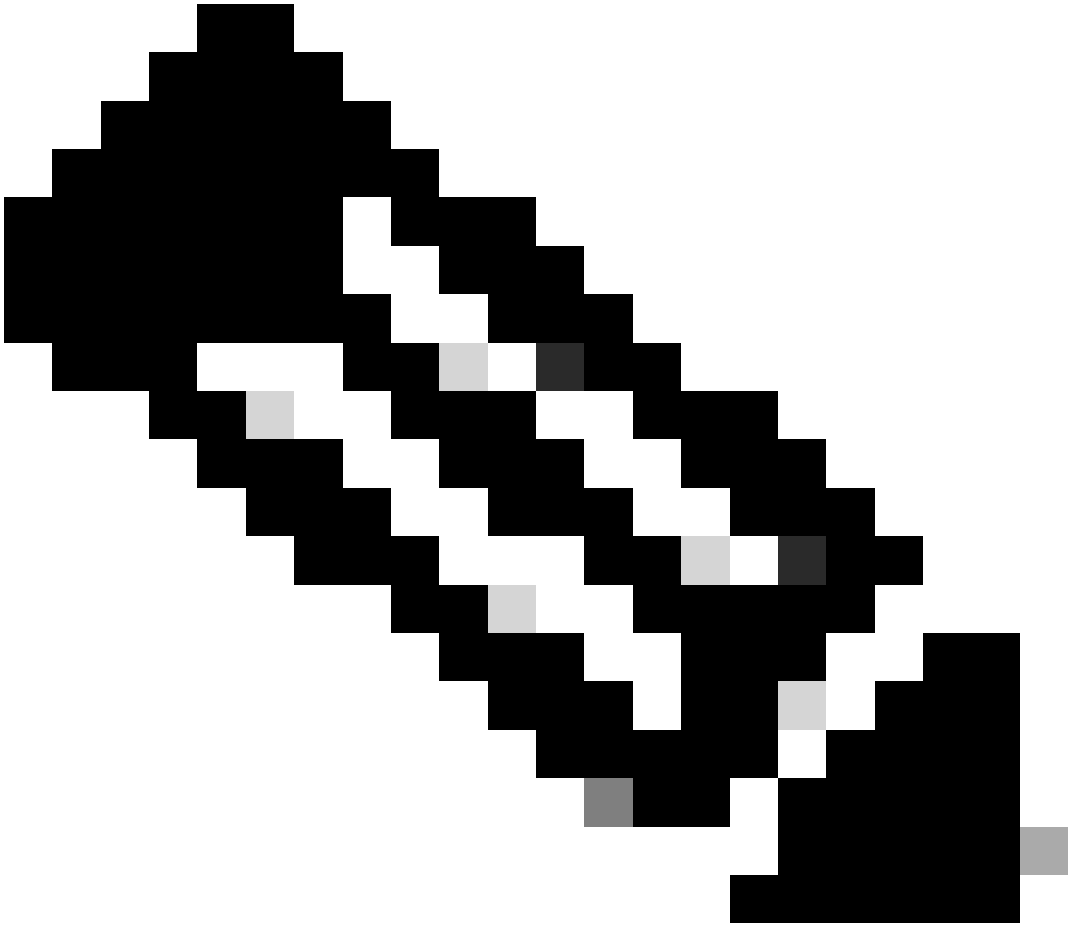
對於FTD，您只能啟用一個外部身份驗證對象。

網路拓撲



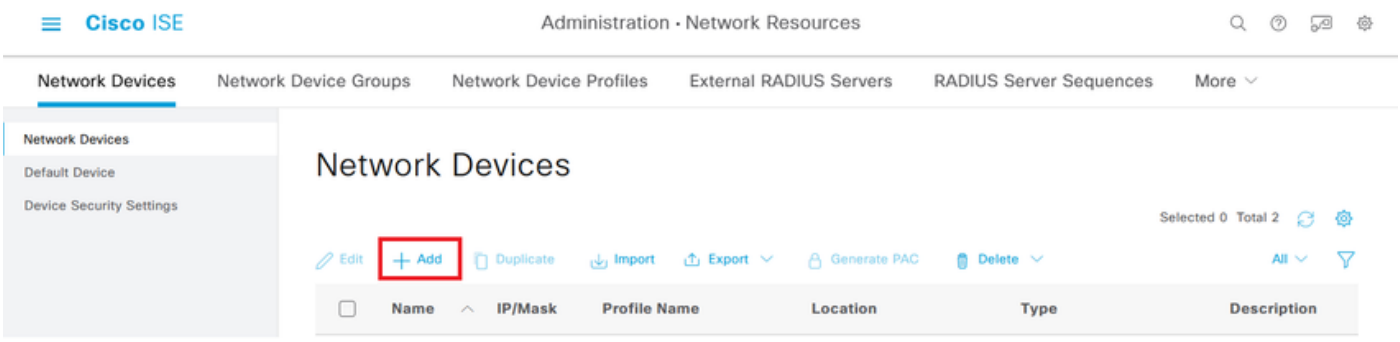
設定

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。

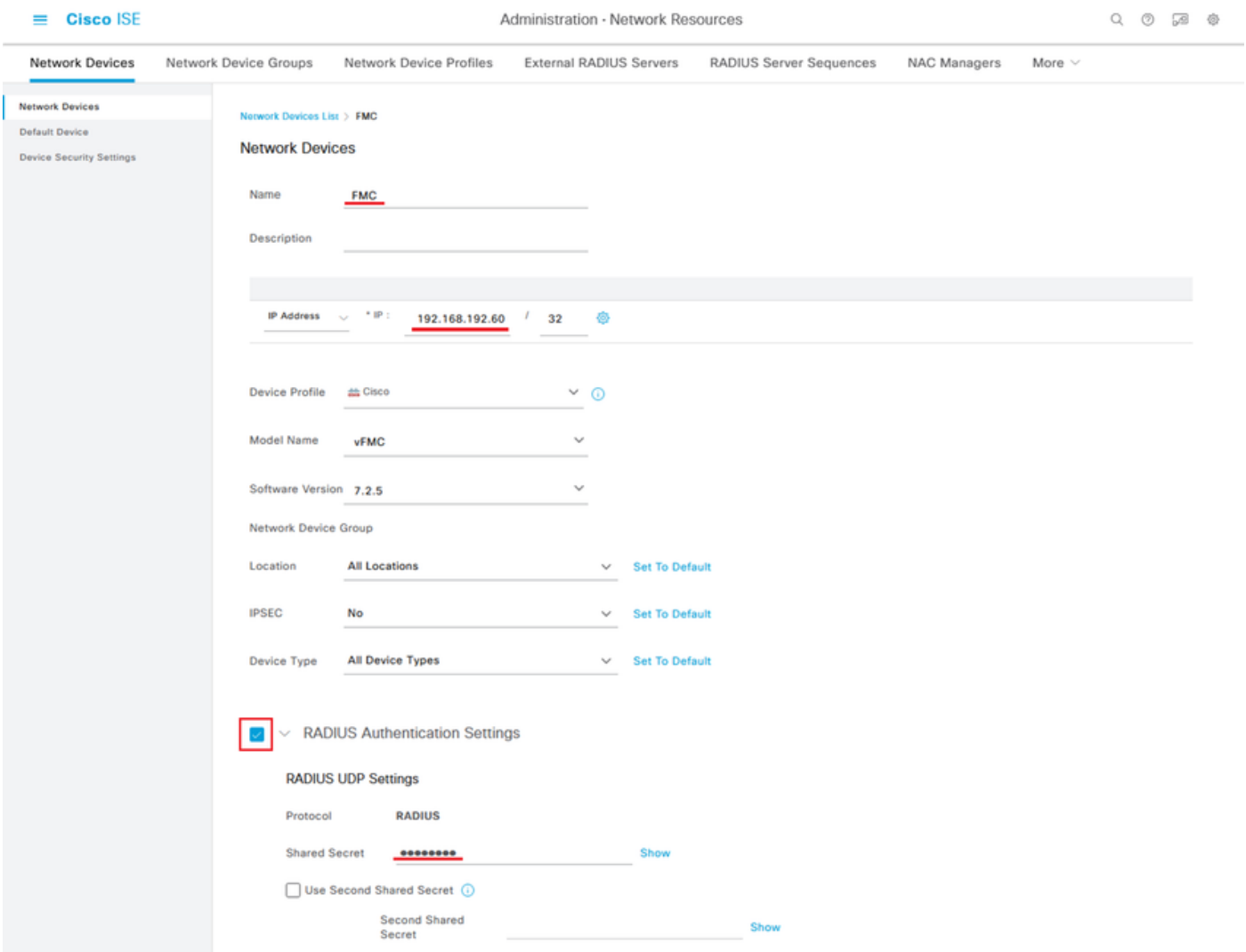


步驟 2.為網路裝置對象分配名稱並插入FMC IP地址。

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。

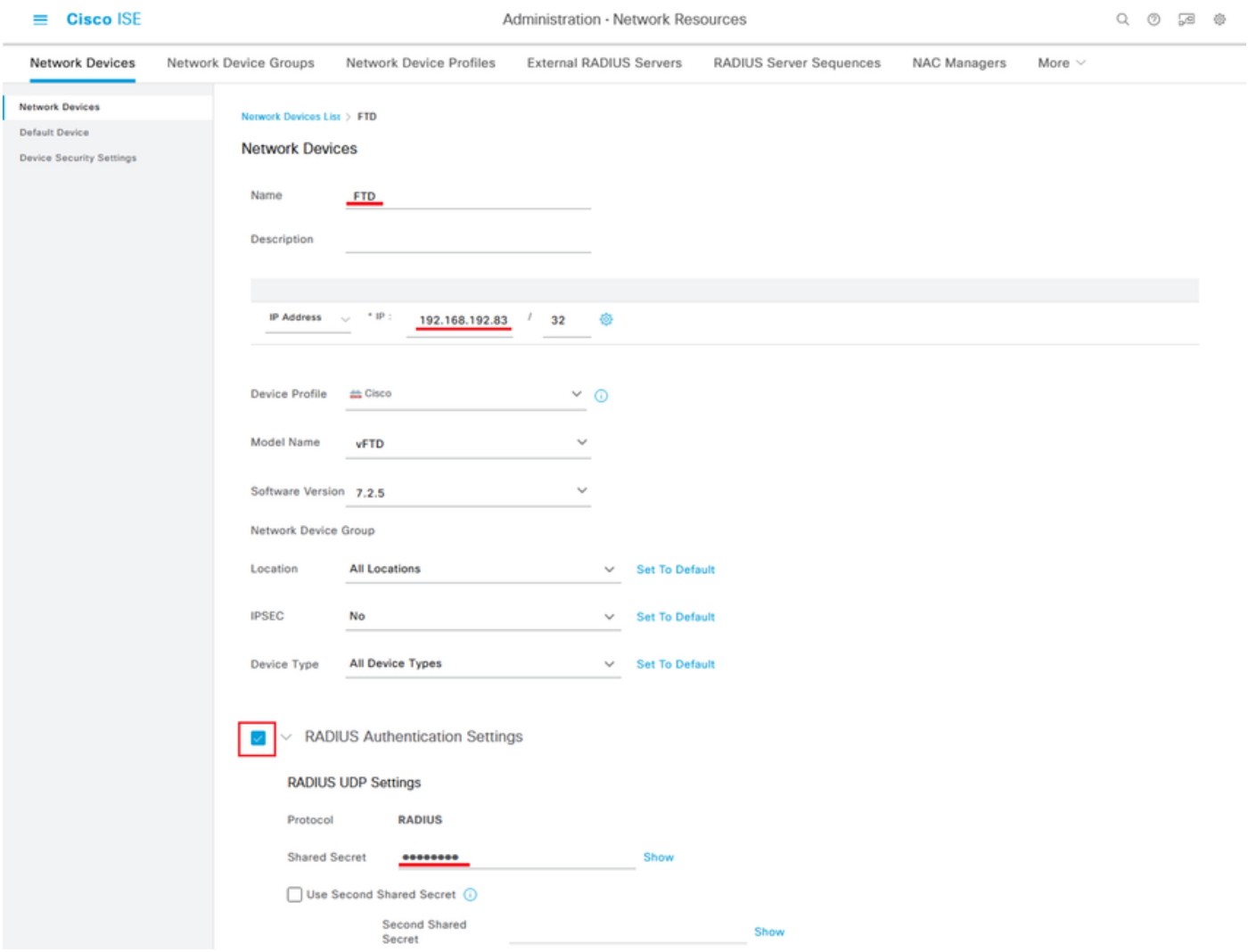


步驟 2.1.重複相同步驟以新增FTD。

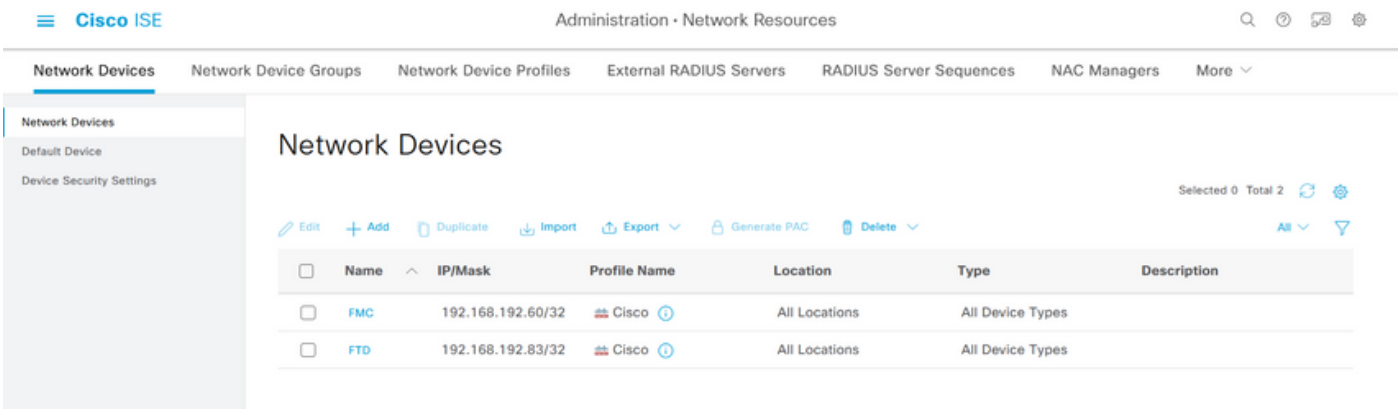
為網路裝置對象分配名稱並插入FTD IP地址。

選中RADIUS 覈取方塊並定義共用金鑰。

完成後，按一下Save。

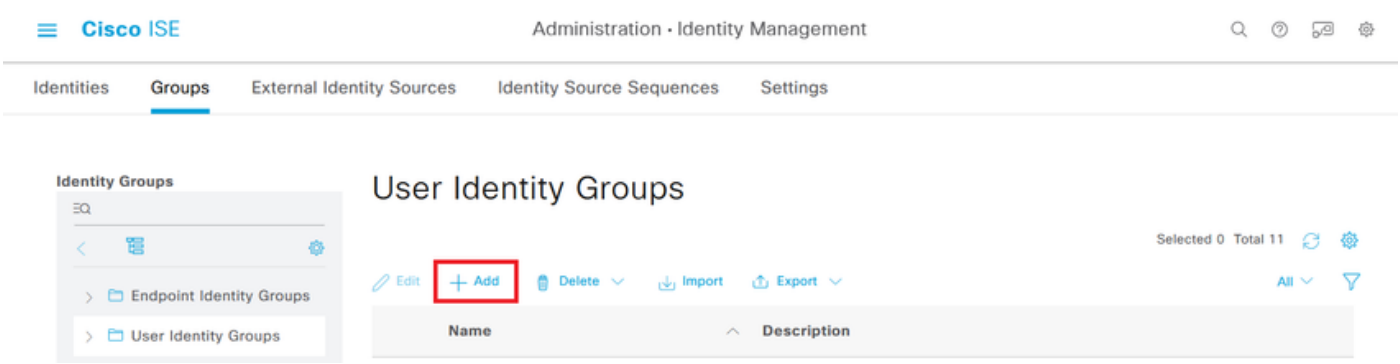


步驟 2.3.驗證「Network Devices（網路裝置）」下顯示的兩個裝置。

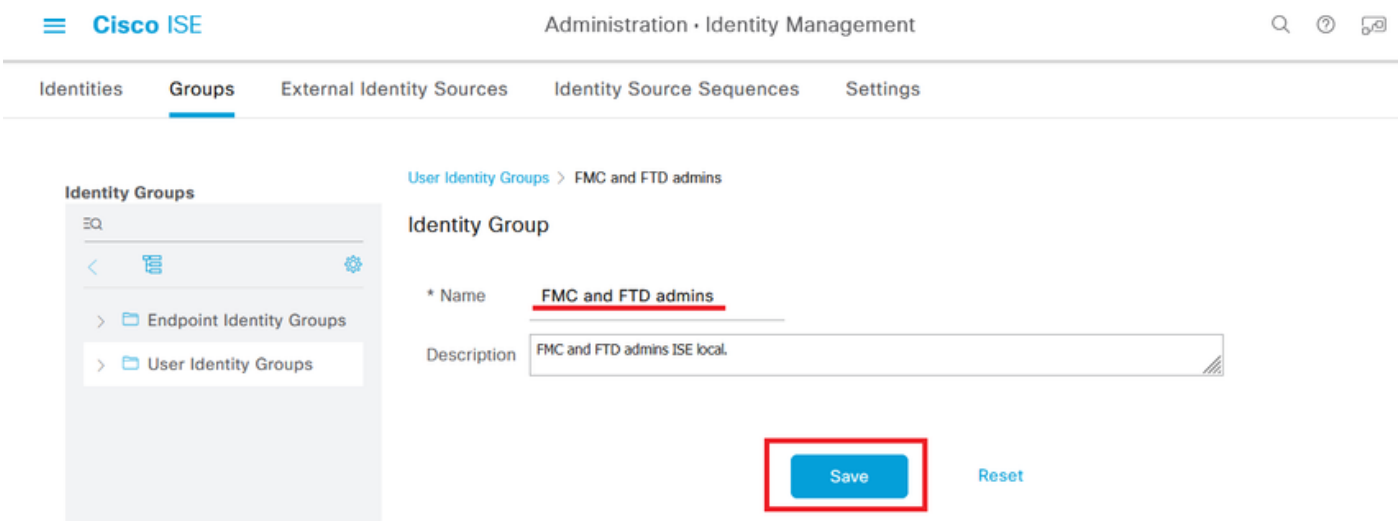


步驟 3. 建立所需的使用者身份組。導航到位於左上角的漢堡圖示

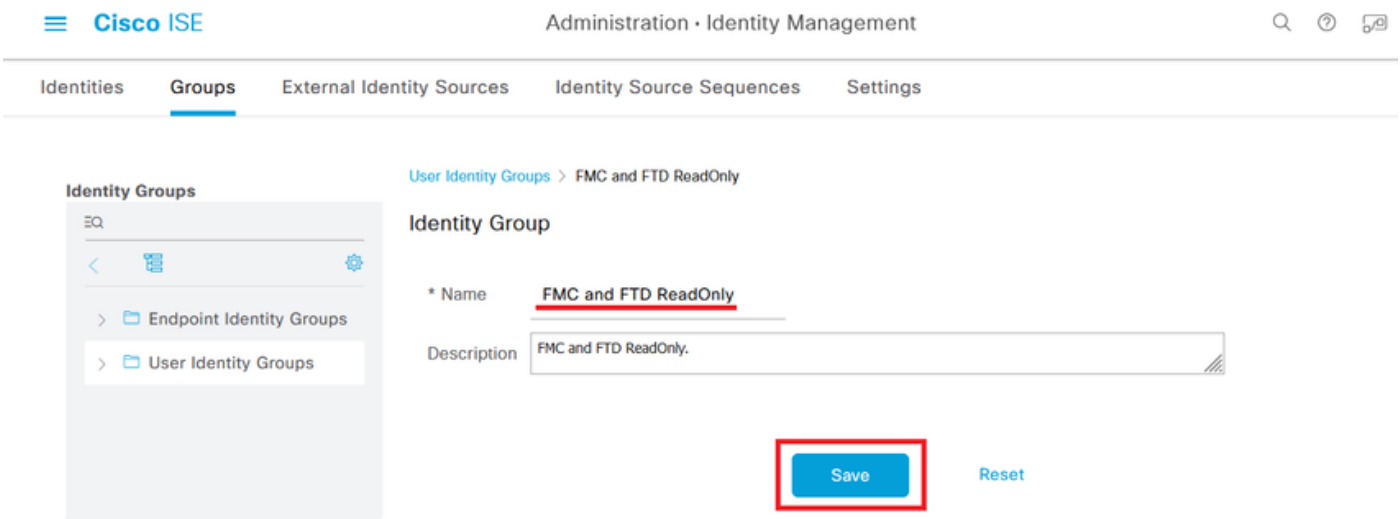
>管理>身份管理>組>使用者身份組> +增加



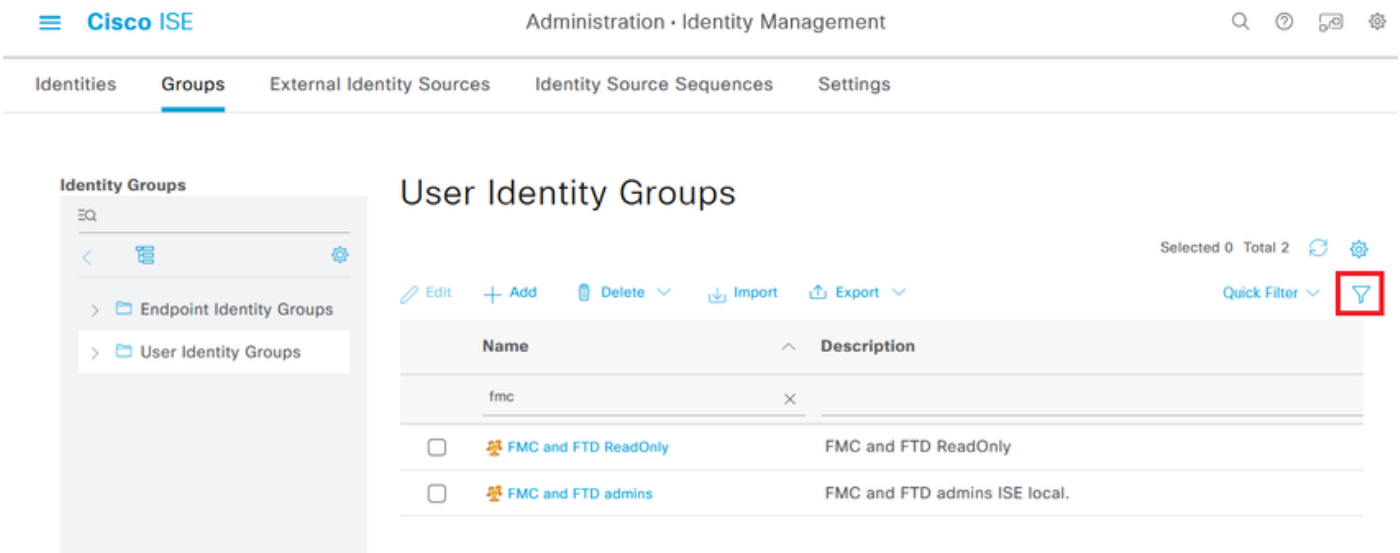
步驟 4.為每個組指定名稱並單獨儲存。在此範例中，我們將為管理員使用者建立群組，為唯讀使用者建立另一個群組。首先，為具有管理員許可權的使用者建立組。



步驟 4.1.為只讀使用者建立第二個組。

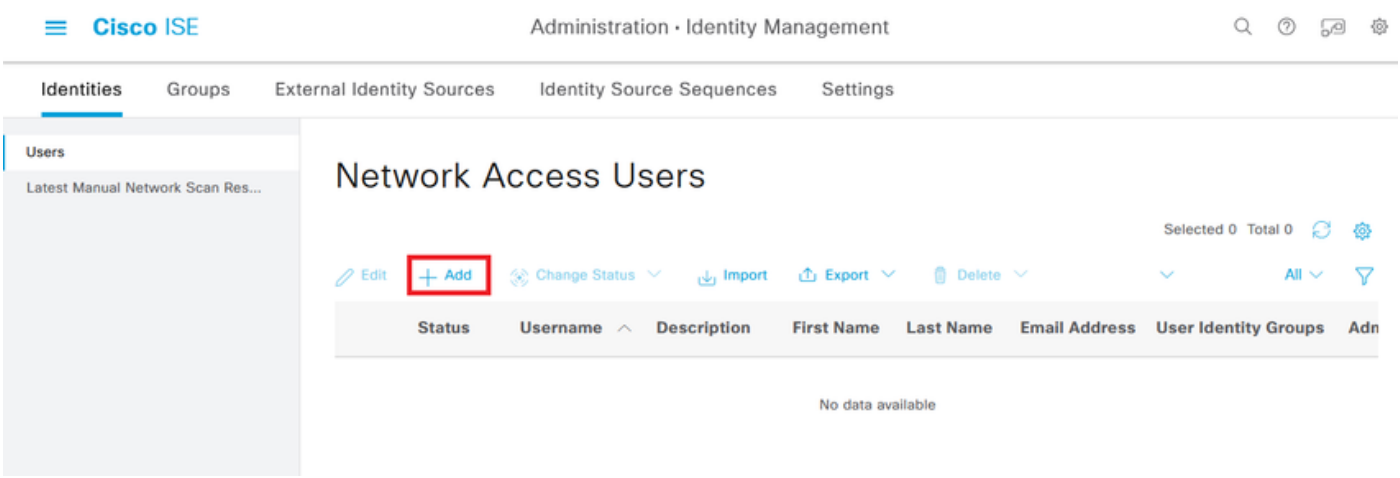


步驟 4.2.驗證兩個群組會顯示在[使用者身份群組清單]下。使用過濾器可以輕鬆找到它們。

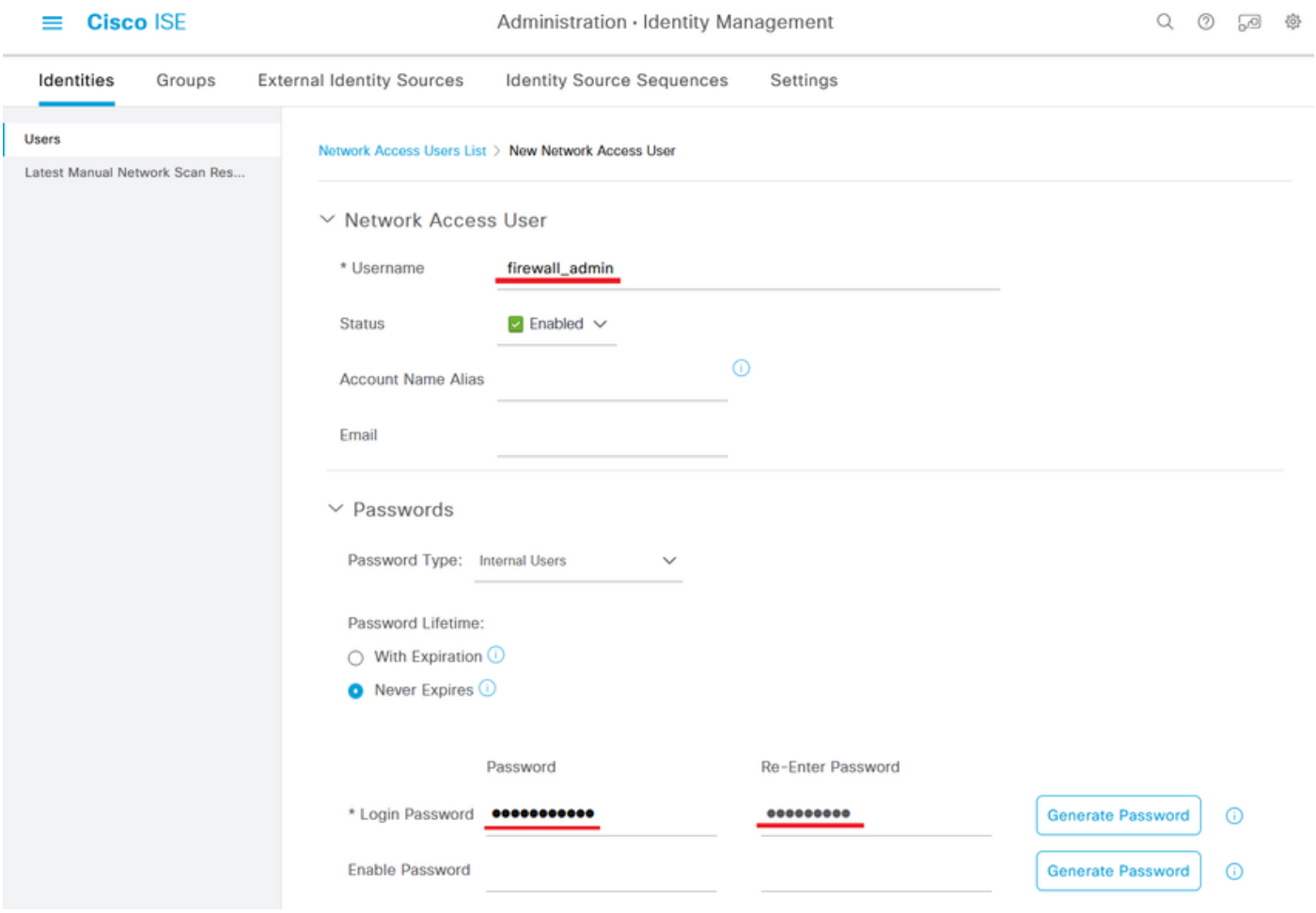


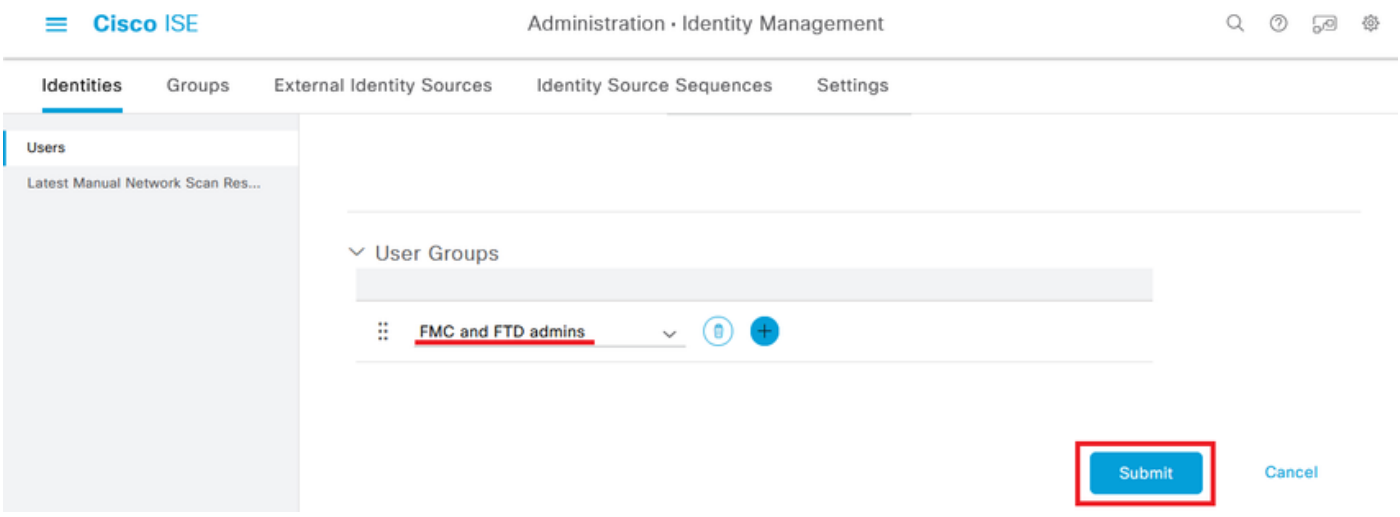
步驟 5. 建立本地使用者並將他們增加到其對應組。導航到

> Administration > Identity Management > Identities > + Add。

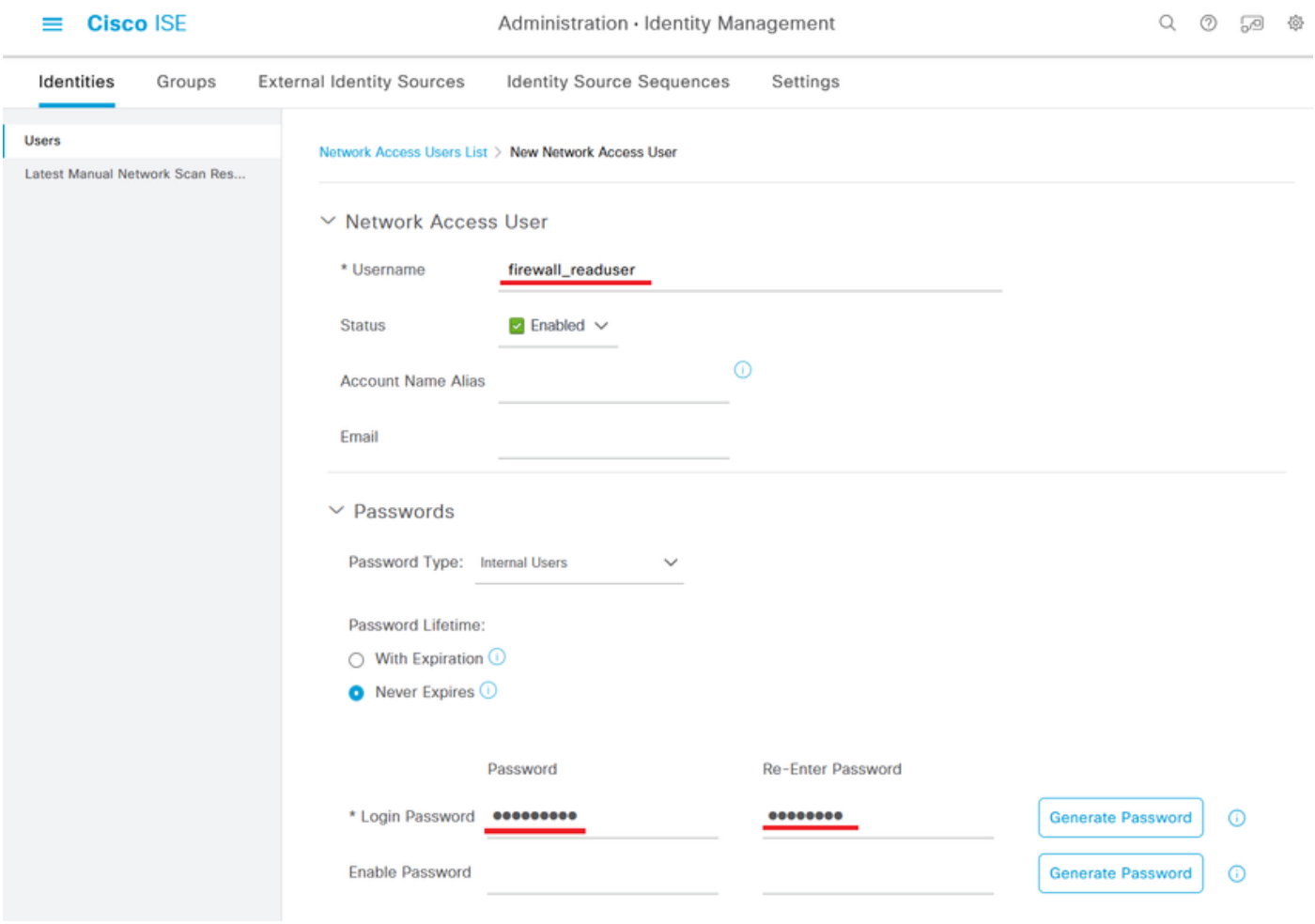


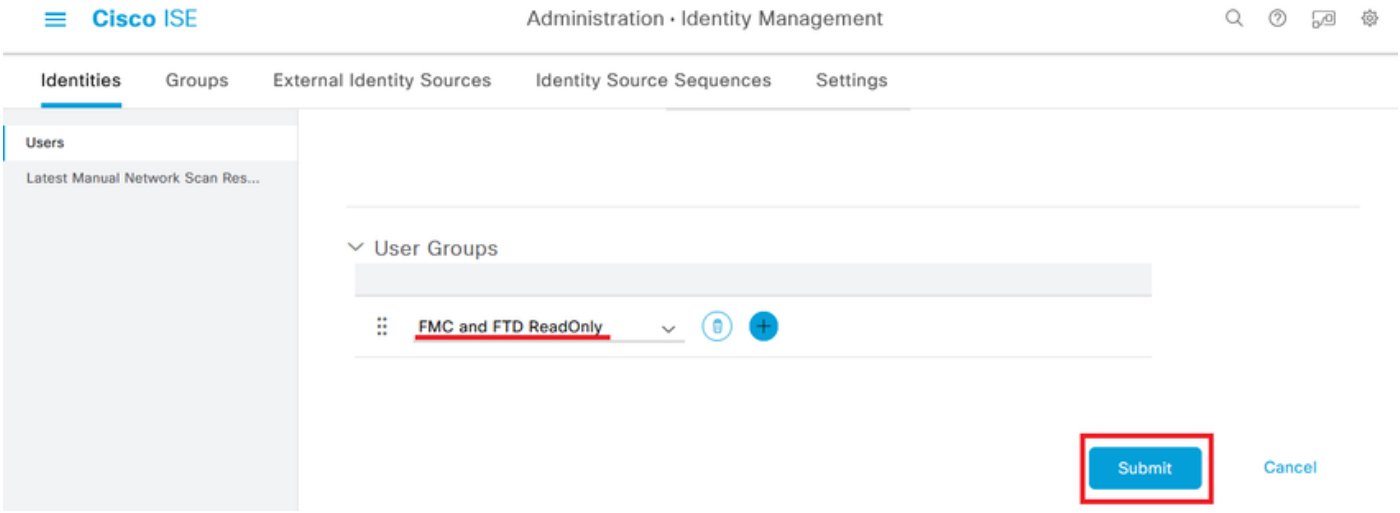
步驟 5.1.首先建立具有管理員許可權的使用者。為它指定名稱、密碼和組FMC和FTD管理員。





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。



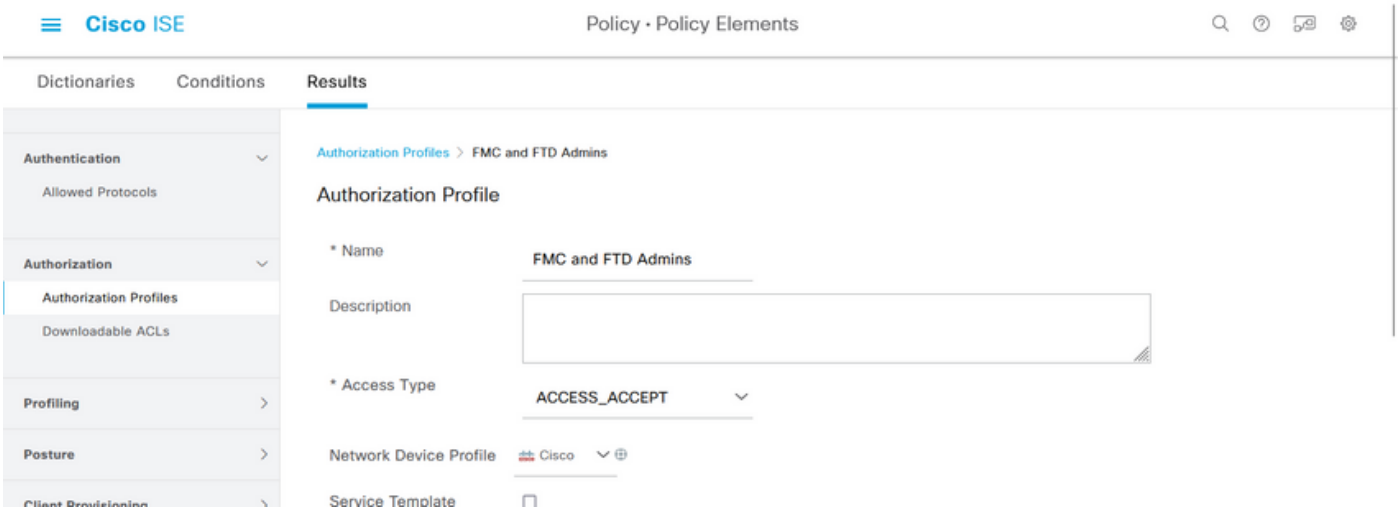


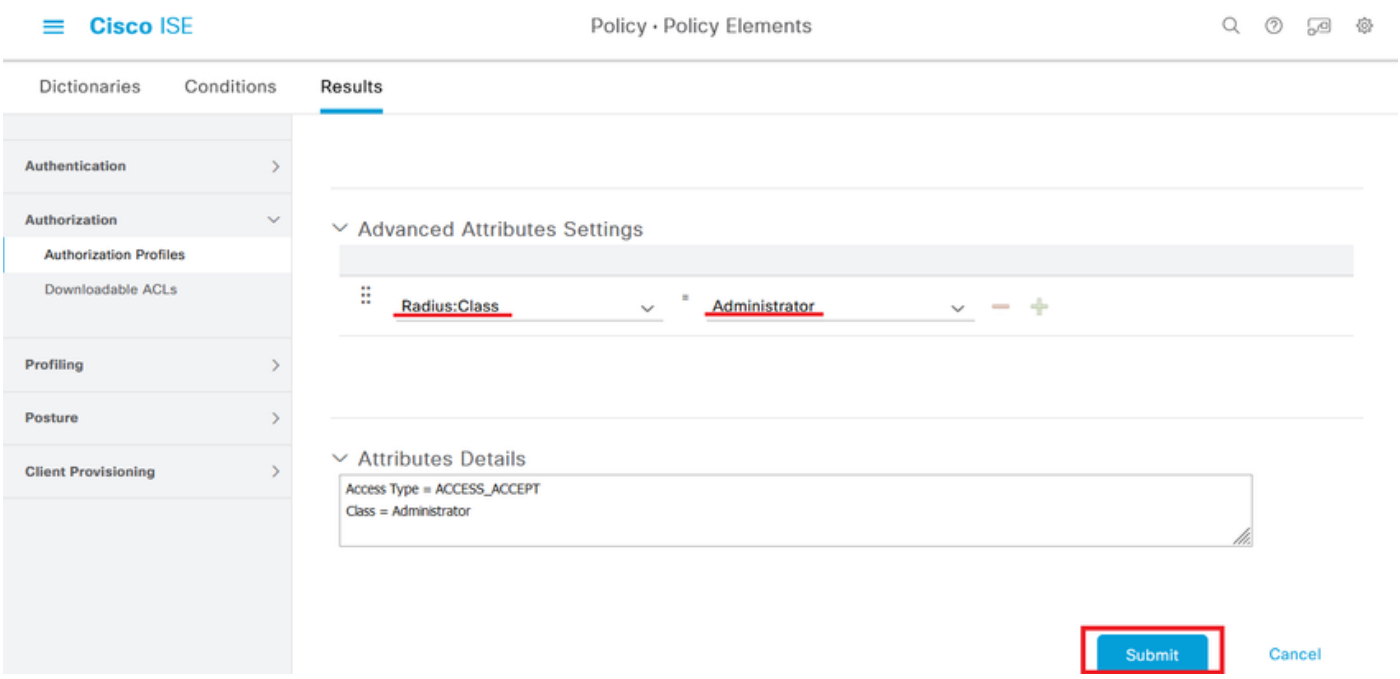
步驟 6.為管理員使用者建立授權配置檔案。

導航到

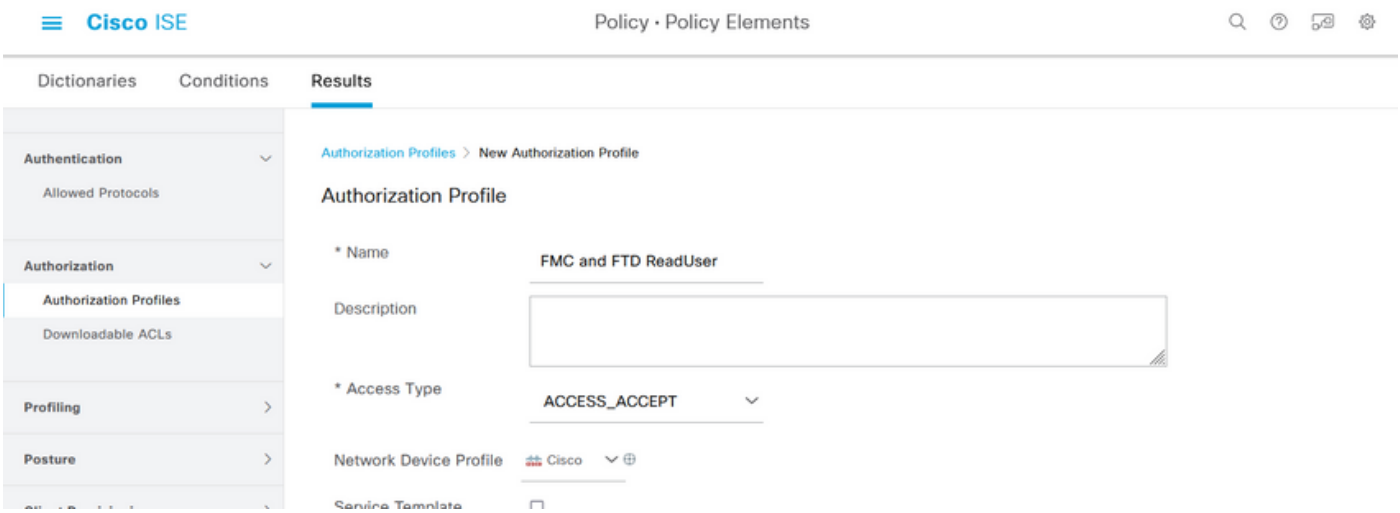
>策略>策略元素>結果>授權>授權配置檔案>+增加。

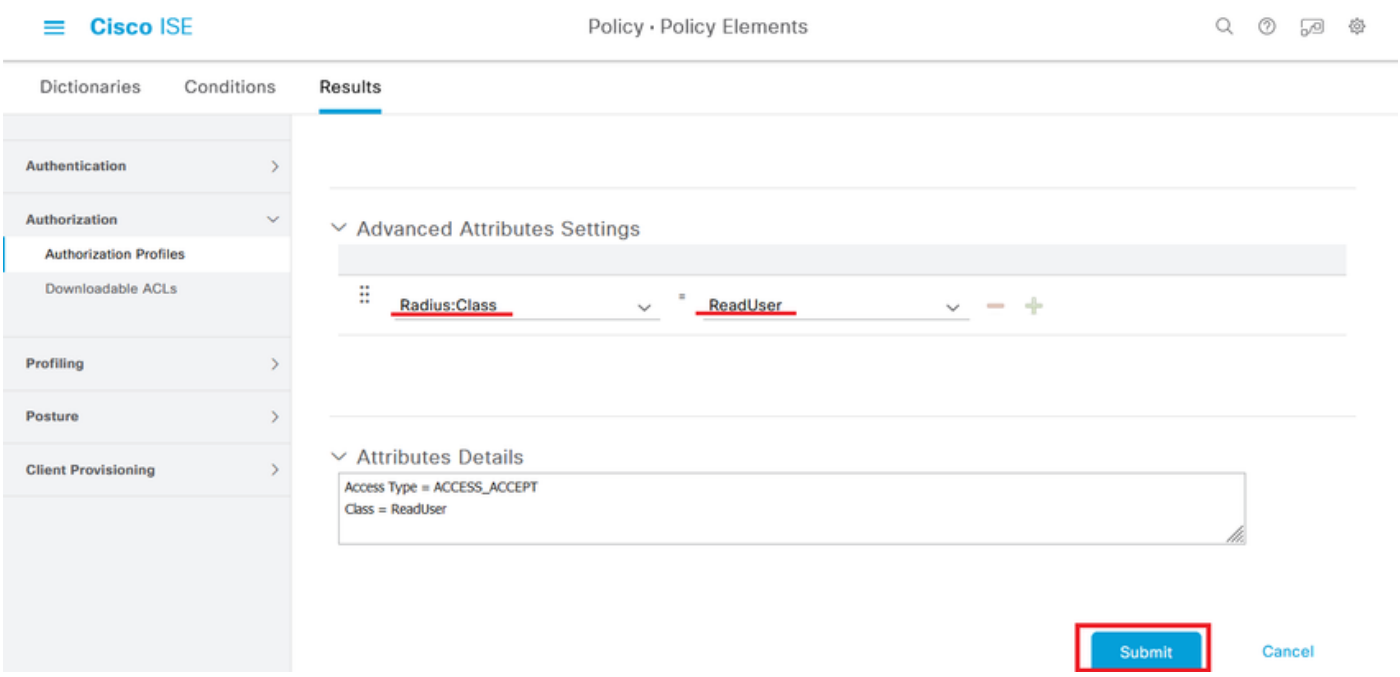
定義授權配置檔案的名稱，保留Access Type為ACCESS_ACCEPT，並在Advanced Attributes Settings下增加值為Administrator的Radius > Class—[25]，然後按一下Submit。





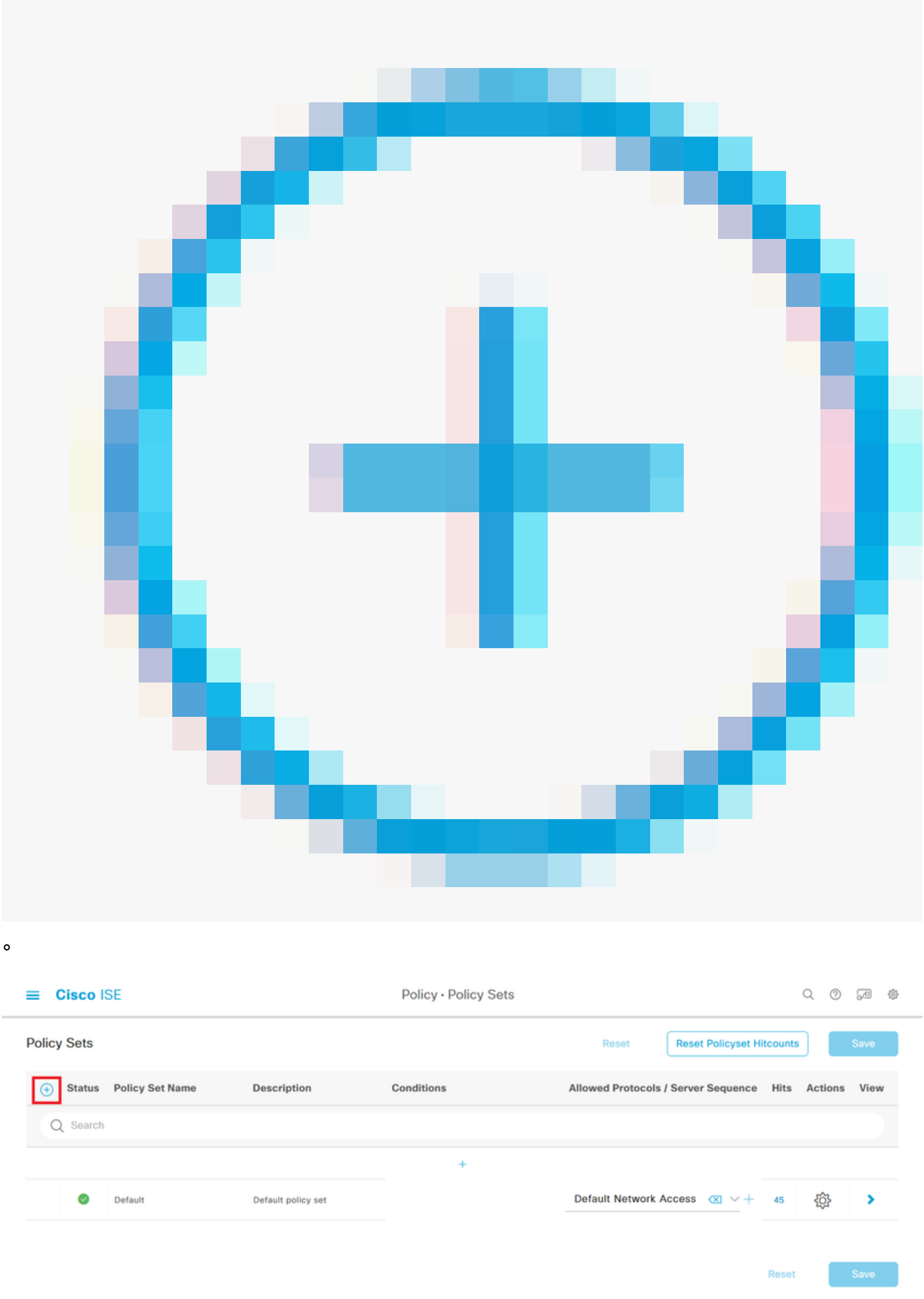
步驟 7.重複上一步為只讀使用者建立授權配置檔案。這次使用值ReadUser而非Administrator建立RADIUS類。





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>

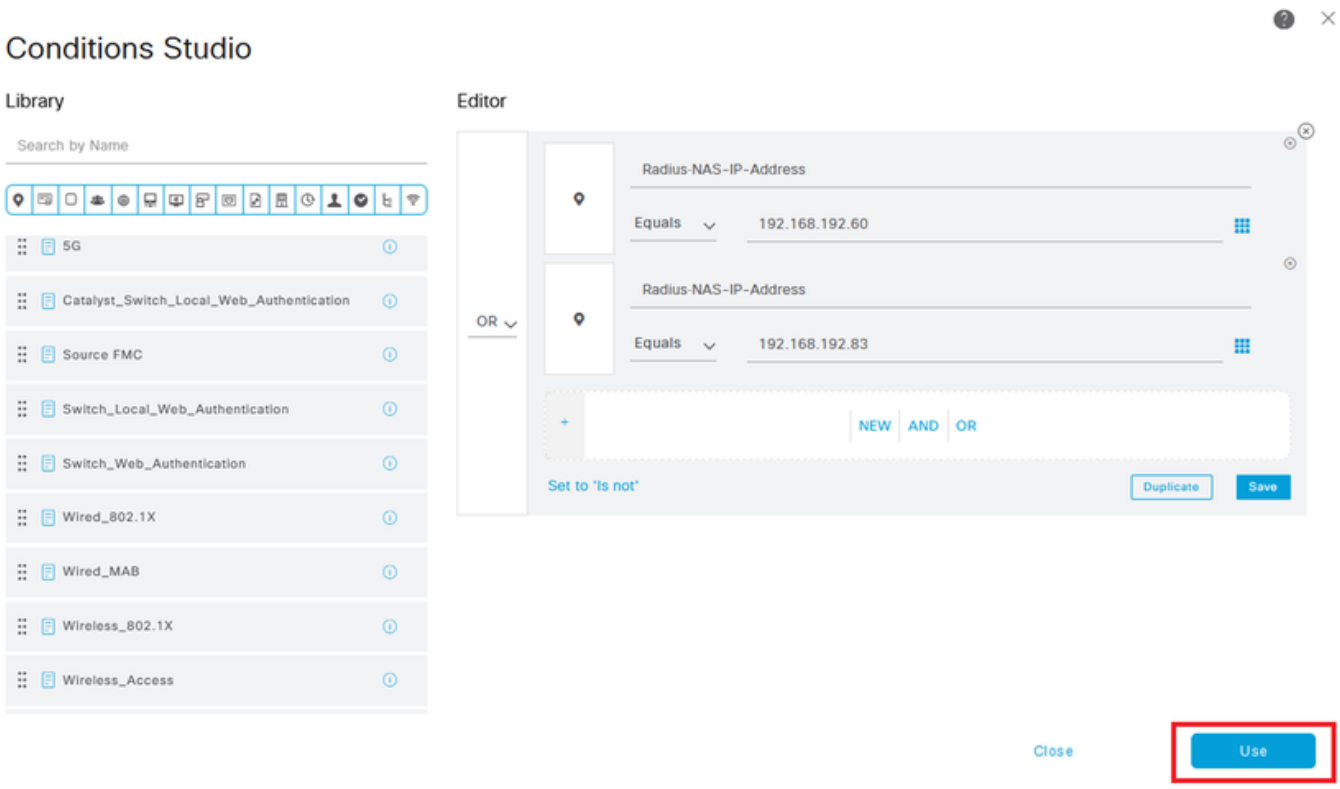
- 
Cisco ISE
Policy · Policy Sets
Policy Sets
Reset
Reset Policyset Hitcounts
Save
Status
Policy Set Name
Description
Conditions
Allowed Protocols / Server Sequence
Hits
Actions
View
Search
Default
Default policy set
Default Network Access
45
Reset
Save

步驟 8.1.新行位於策略集的頂部。

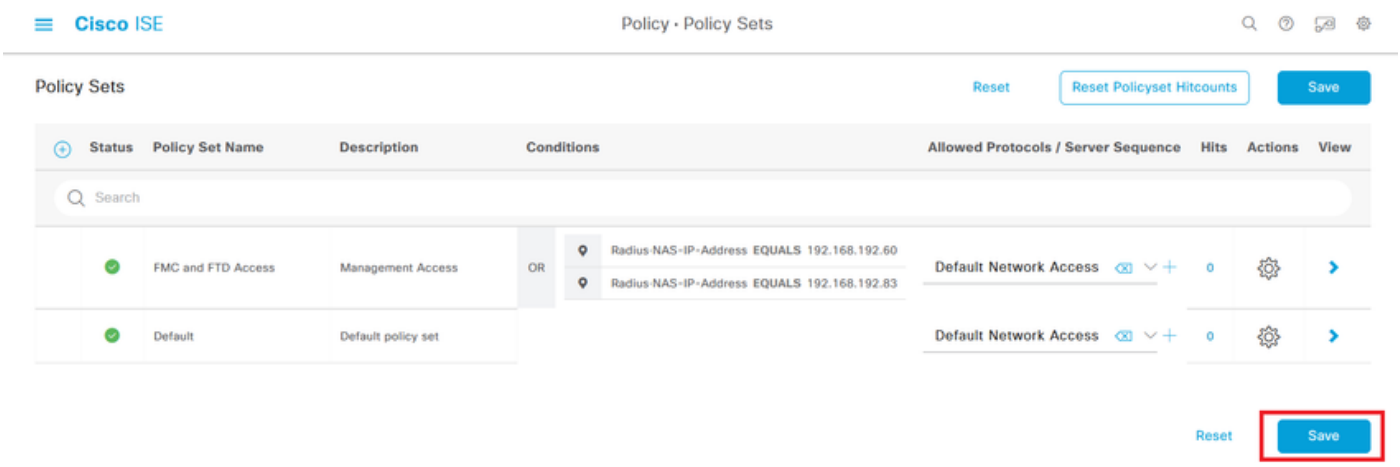
為新策略命名，並為匹配FMC IP地址的RADIUS NAS-IP-Address 屬性增加一個頂級條件。

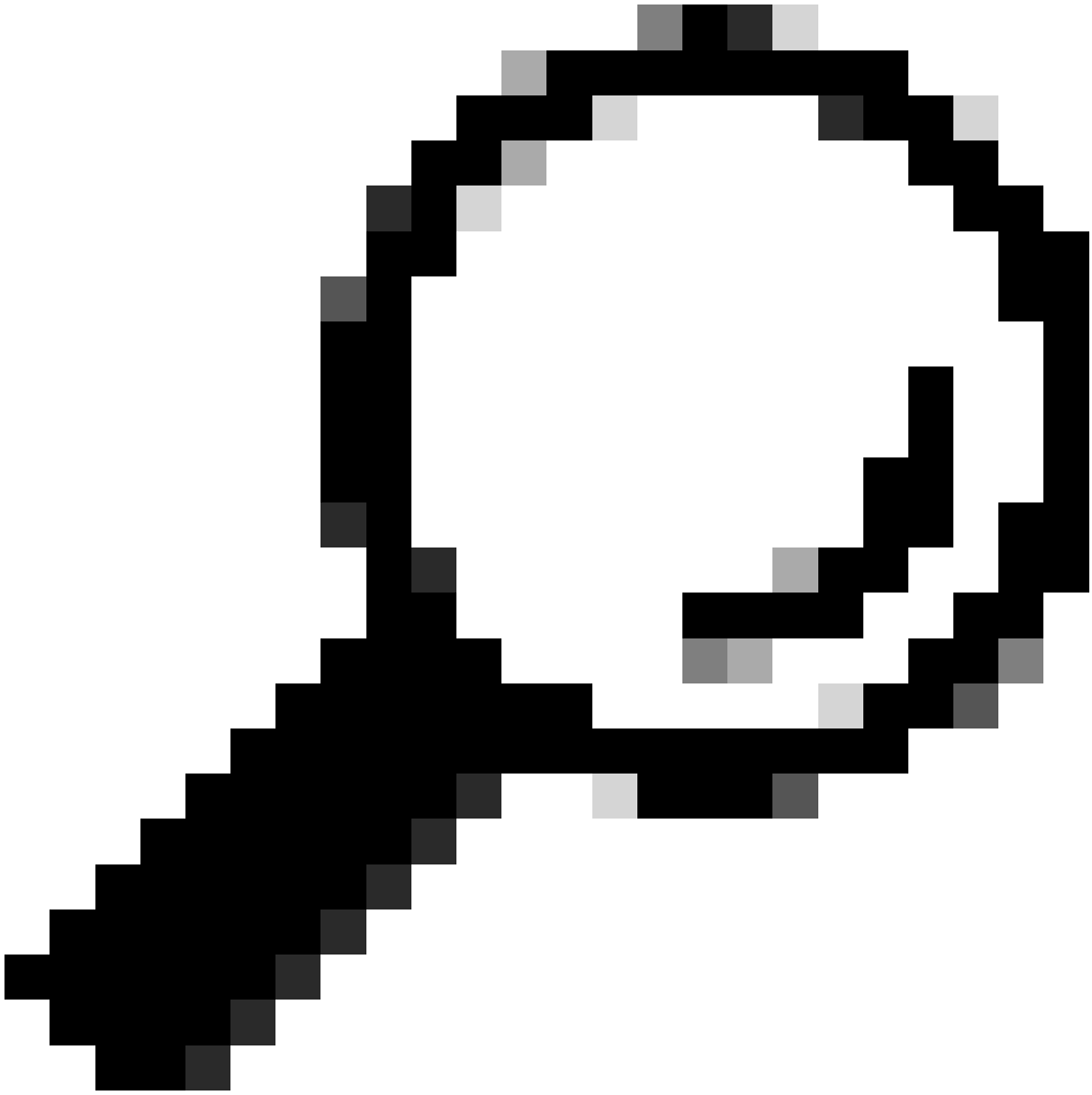
將第二個條件與OR結合以包括FTD的IP位址。

按一下Use以保留更改並退出編輯器。



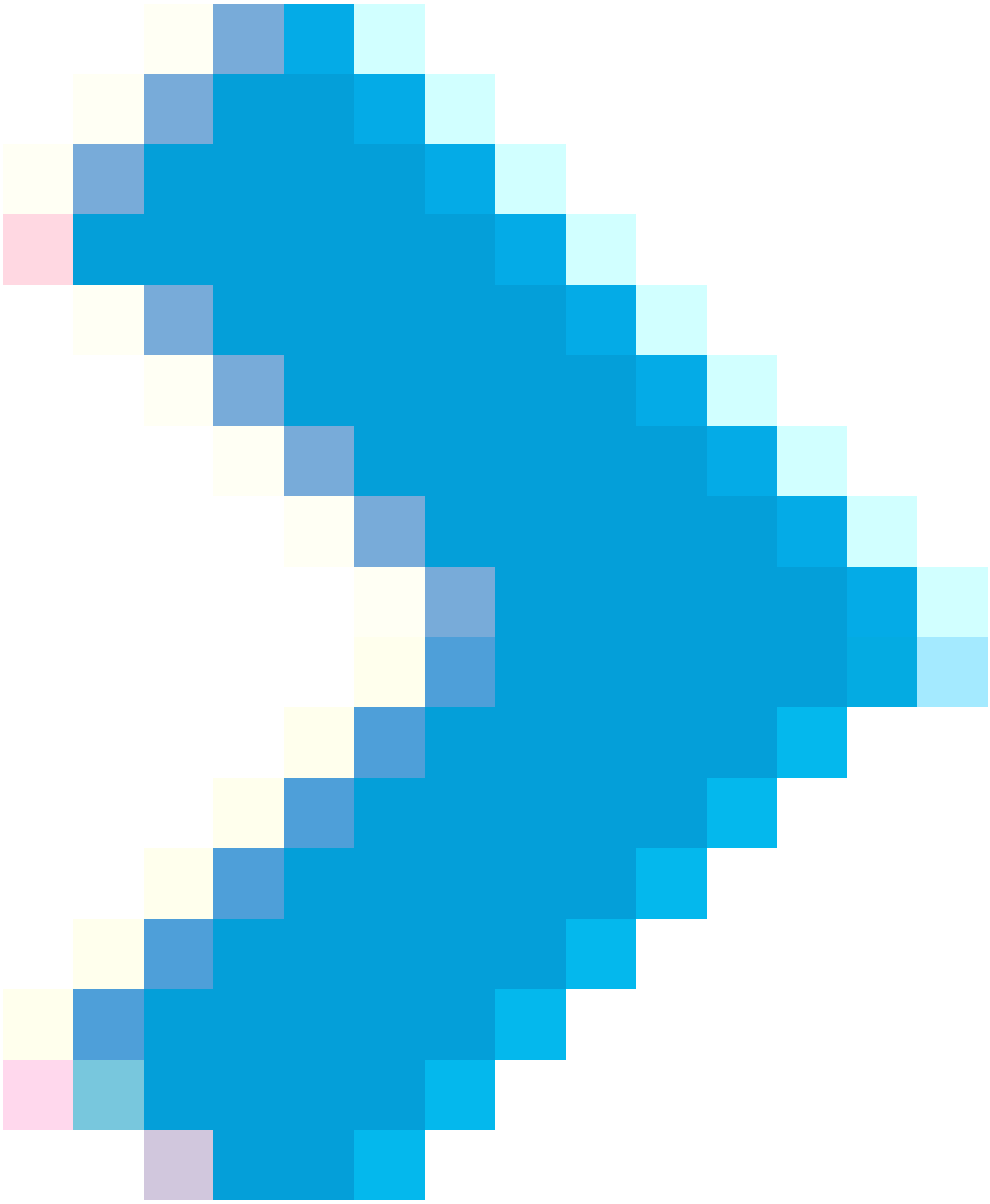
步驟 8.2.完成後按一下Save。





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



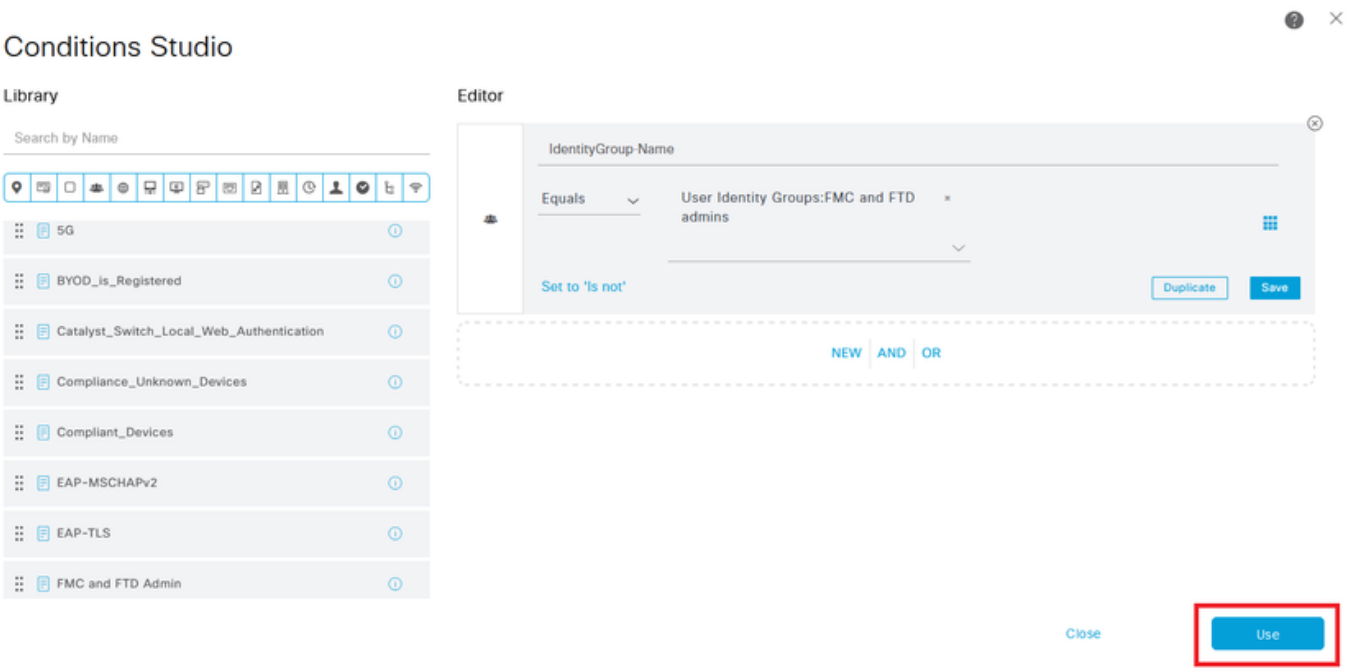
圖示來檢視新的策略集。

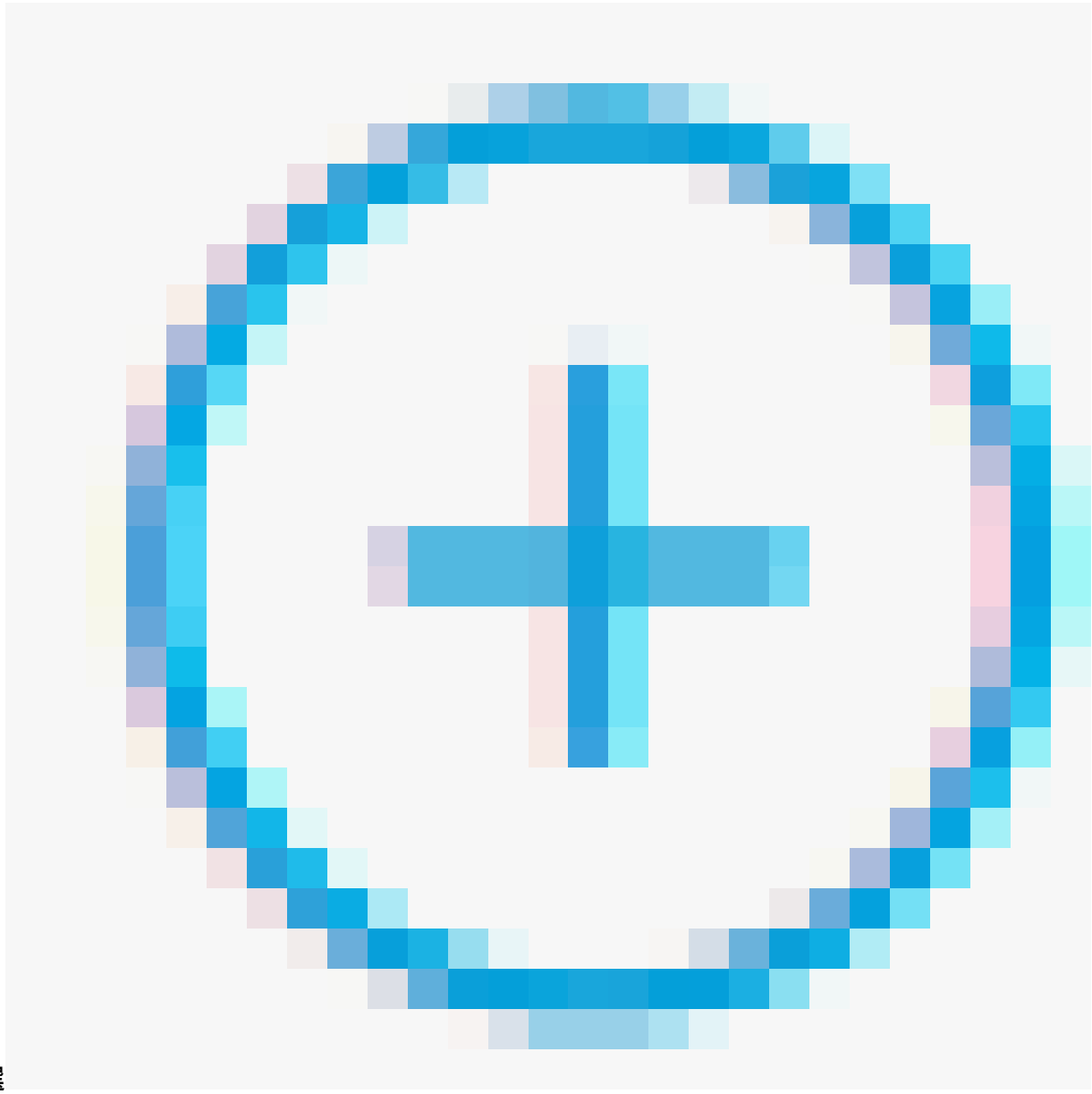
展開Authorization Policy選單並推送

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
Use

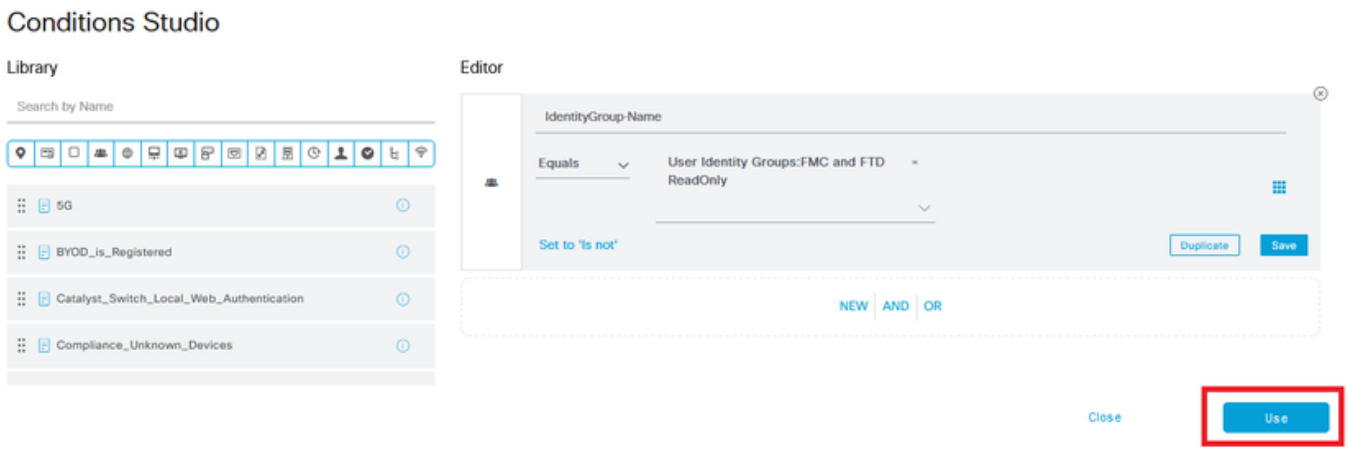


步驟 10.點選

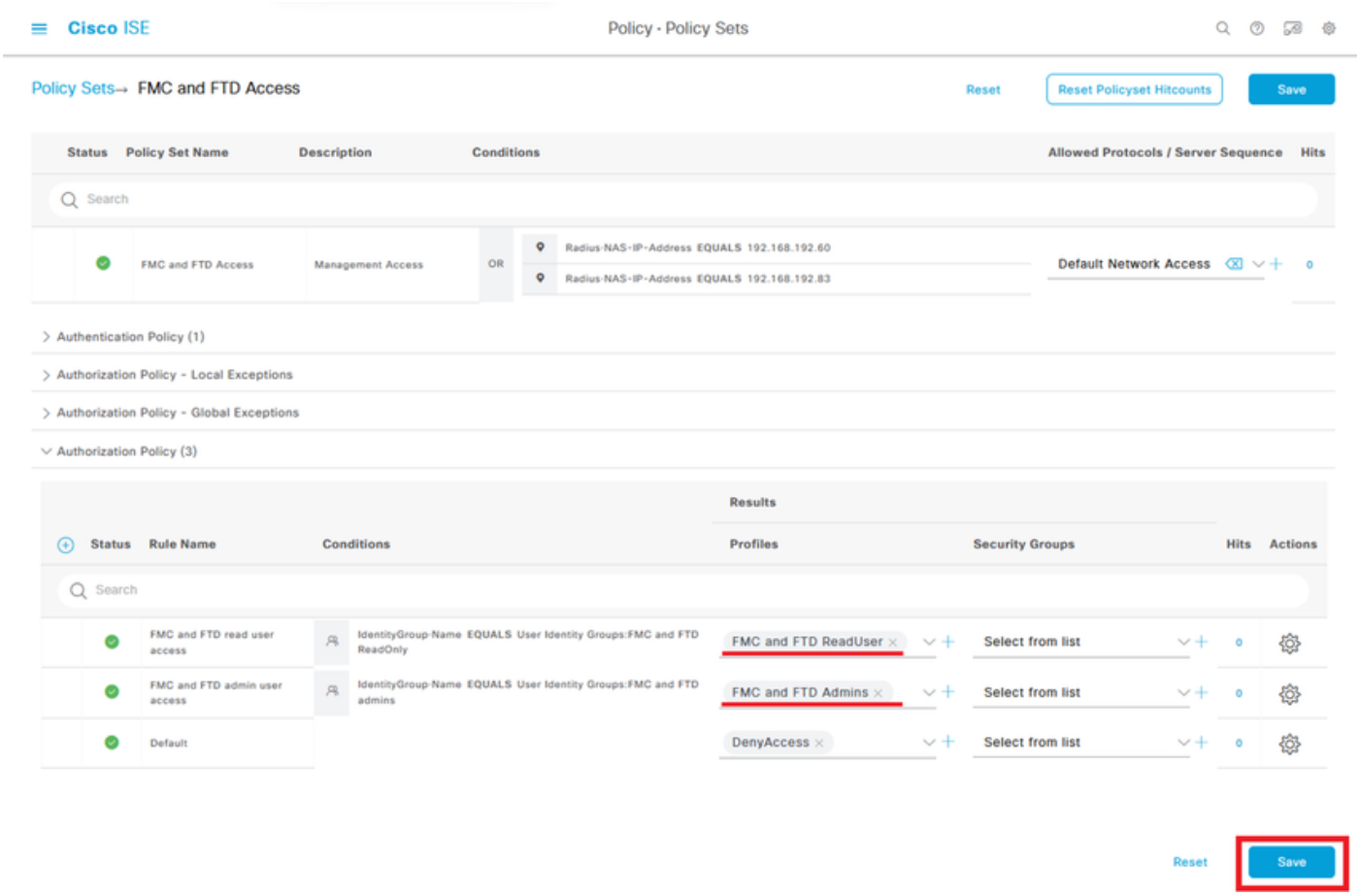
圖示增加第二條規則，以允許訪問具有只讀許可權的使用者。

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。



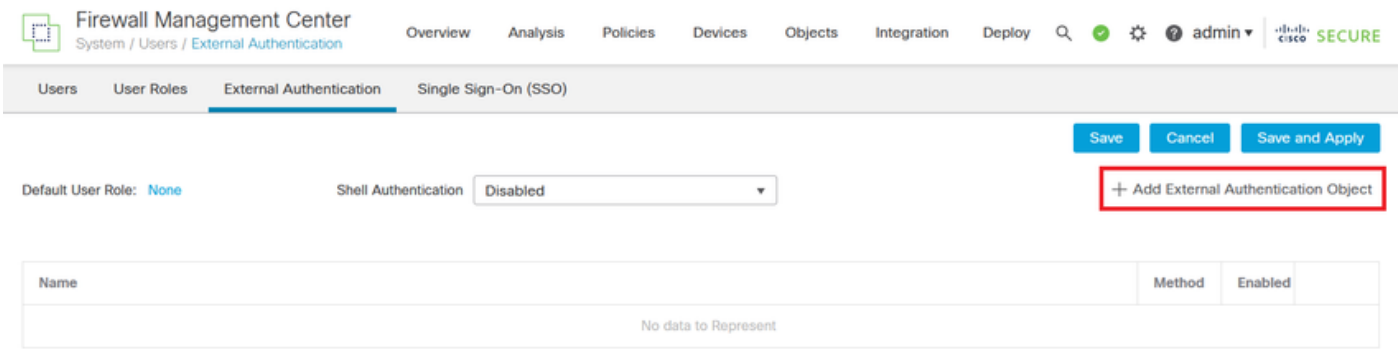
步驟 11.分別為每個規則設定授權配置檔案並點選Save。



FMC配置

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

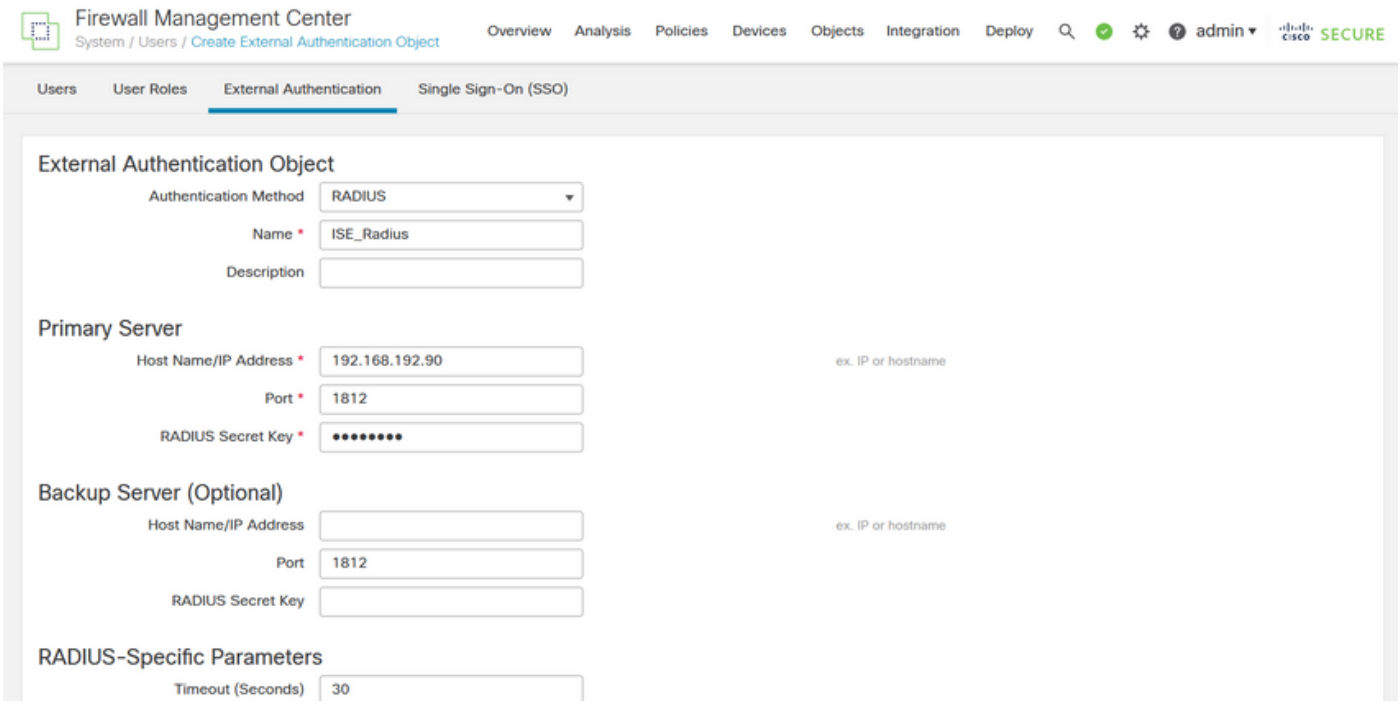
外部身份驗證對象。



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配置的第2步中使用的同一RADIUS金鑰。

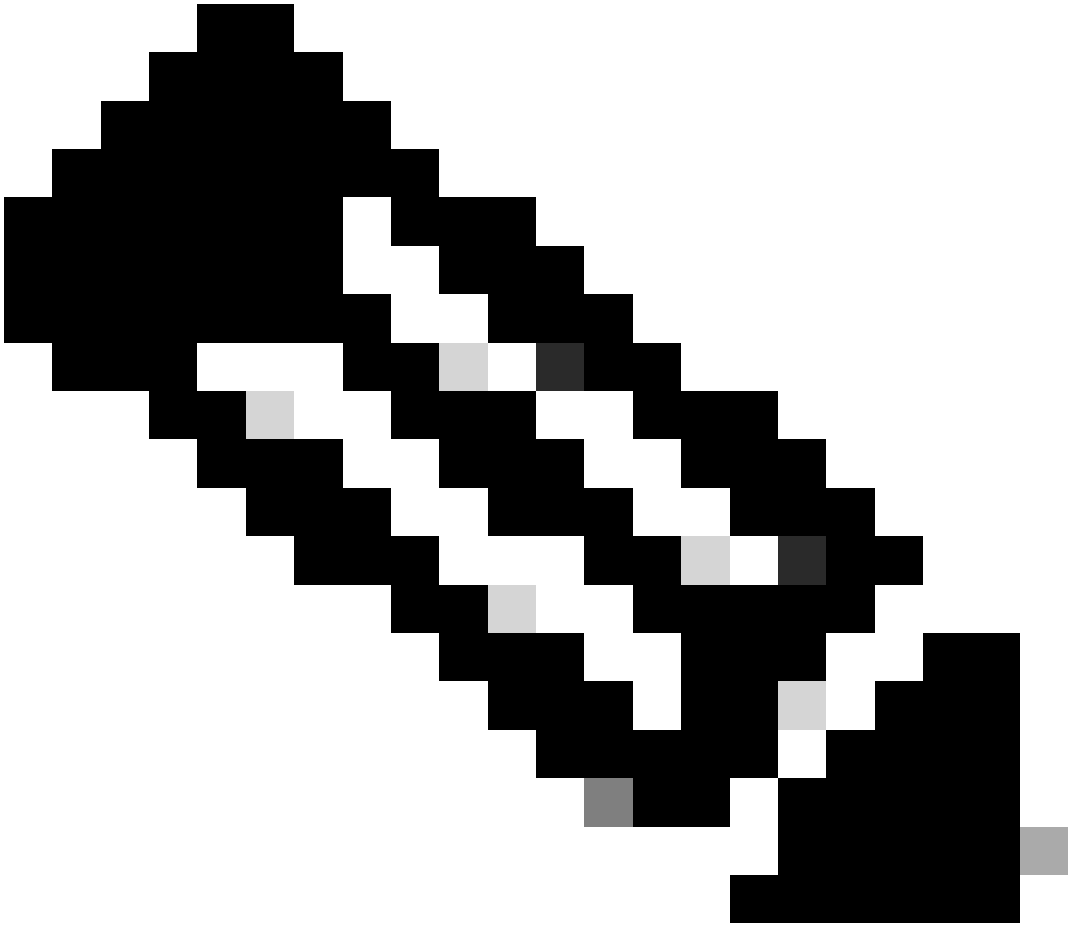


步驟 3.插入在ISE配置的步驟6和步驟7分別為firewall_admin和firewall_readuser配置的RADIUS類屬性值。

RADIUS-Specific Parameters

Timeout (Seconds)	30
Retries	3
Access Admin	
Administrator	Class=Administrator
Discovery Admin	
External Database User	
Intrusion Admin	
Maintenance User	
Network Admin	
Security Analyst	
Security Analyst (Read Only)	Class=ReadUser
Security Approver	
Threat Intelligence Director (TID) User	
Default User Role	Access Admin Administrator Discovery Admin External Database User

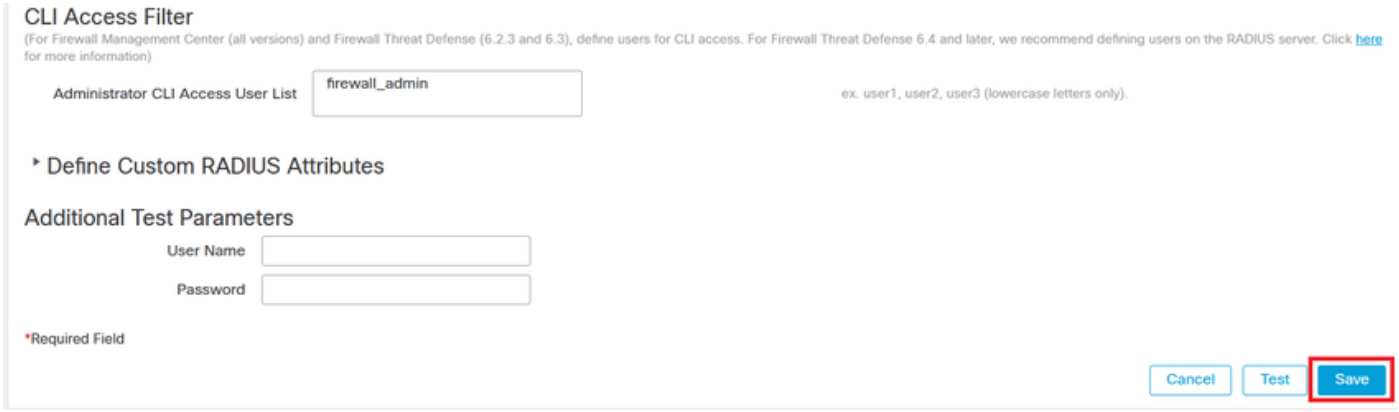
To specify the default user role if user is not found in any group



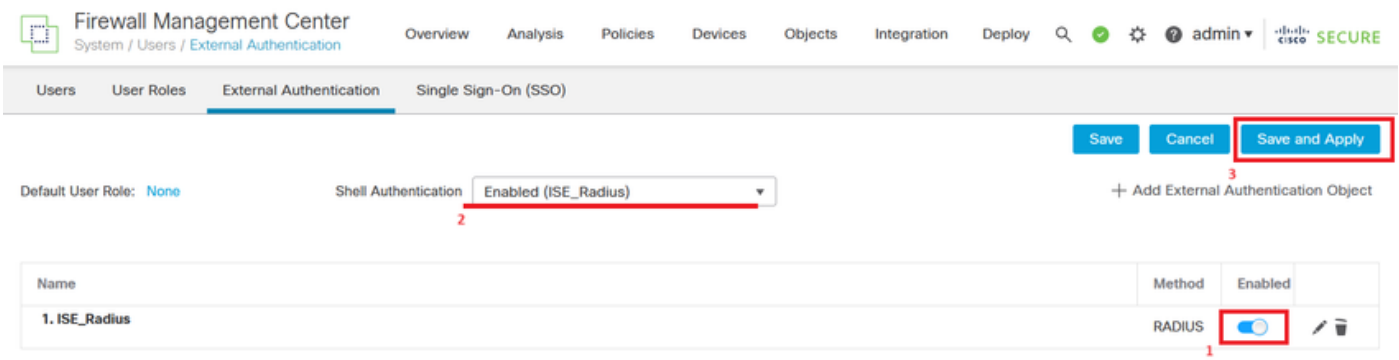
注意：FTD和FMC的逾時範圍不同，因此如果您共用物件並變更預設值30秒，請確定FTD裝置的逾時範圍不要超過較小的範圍（1-300秒）。如果將超時設定為較高的值，則威脅防禦RADIUS配置不起作用。

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。

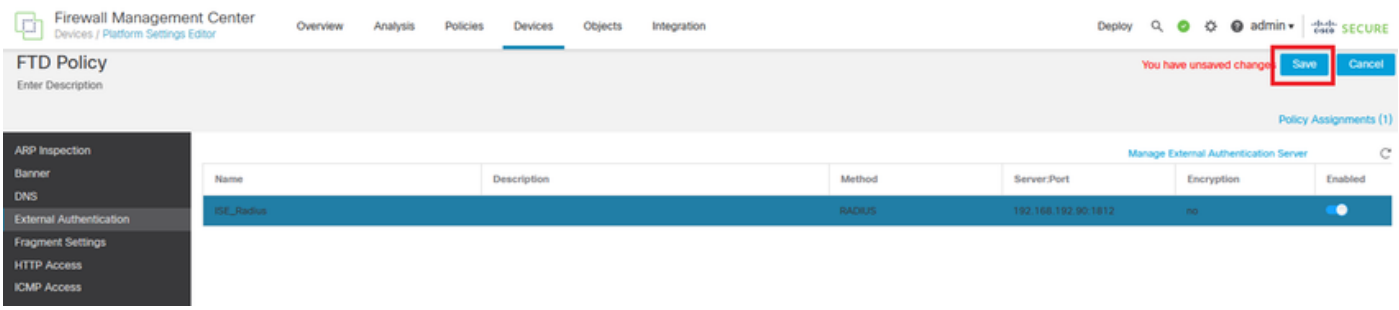


步驟 5.啟用新物件。將其設定為FMC的Shell身份驗證方法，然後按一下「儲存並應用」。

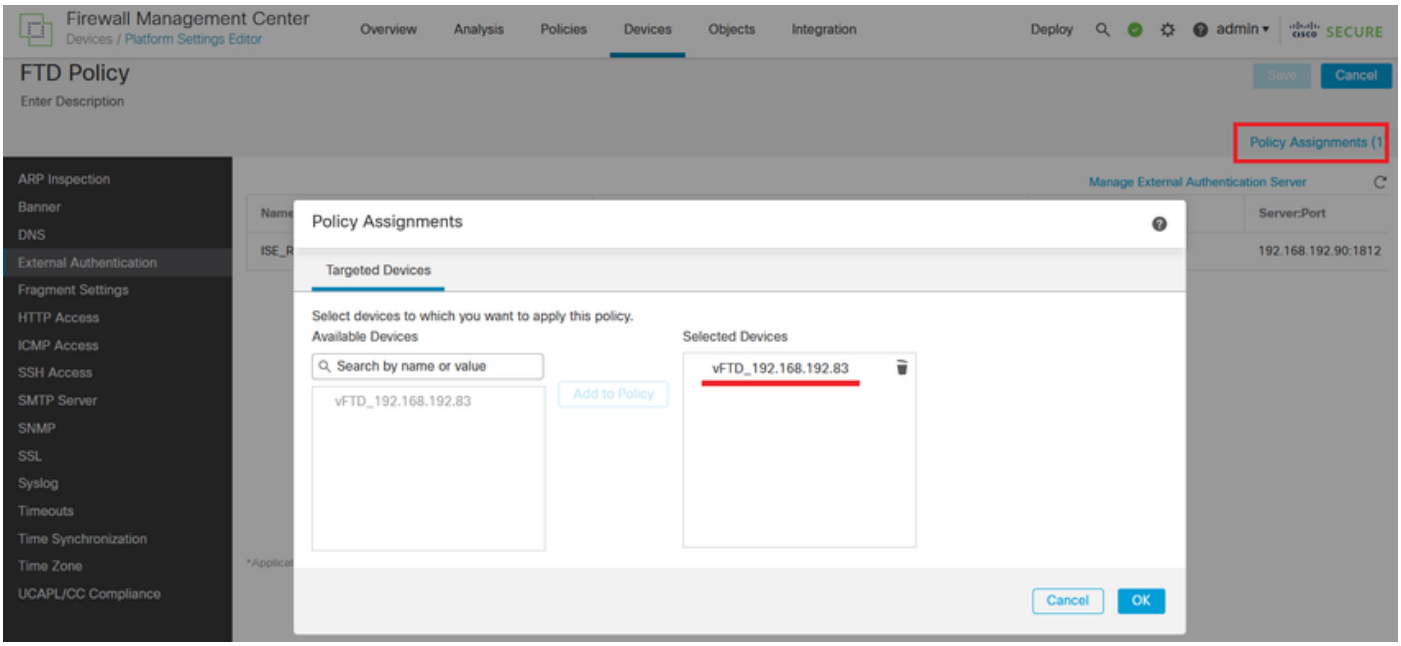


FTD組態

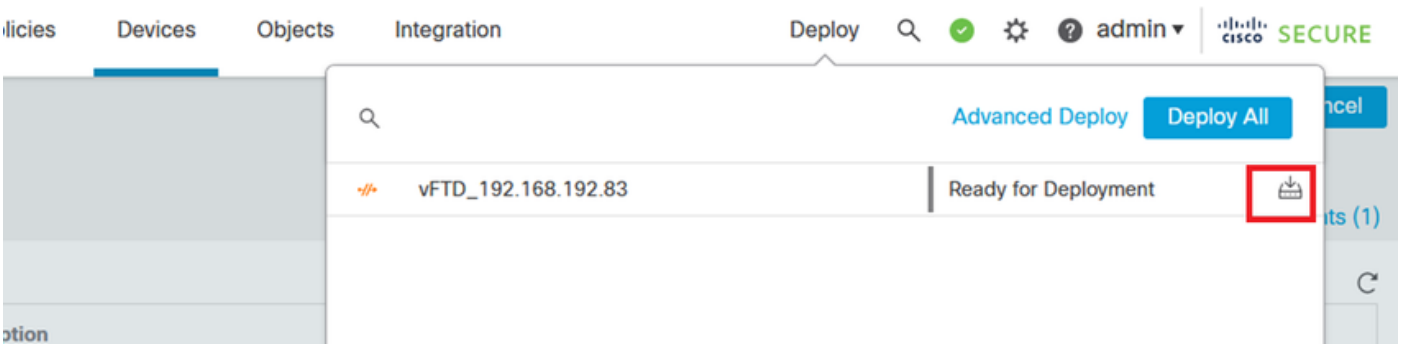
步驟 1.在FMC GUI中，導航至裝置>平台設定。編輯您目前的原則，或建立新的原則（如果您沒有將任何原則指派給您需要存取的FTD）。啟用External Authentication下的RADIUS伺服器，然後按一下Save。



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

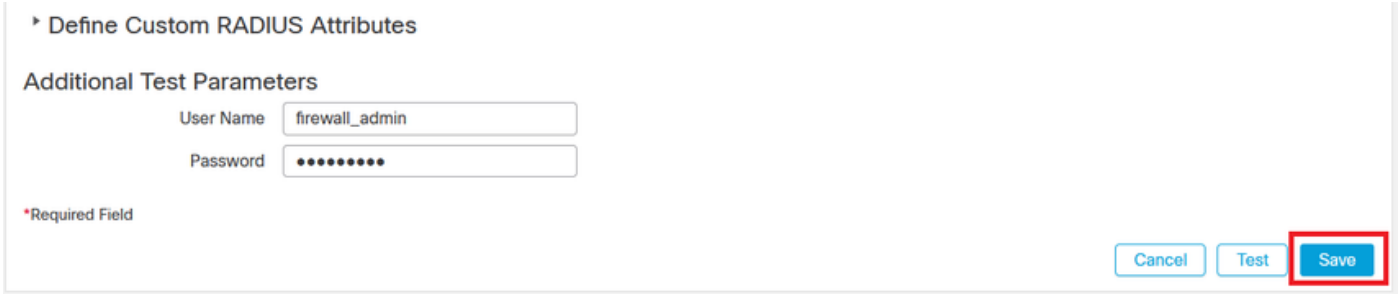


步驟 3.部署變更。

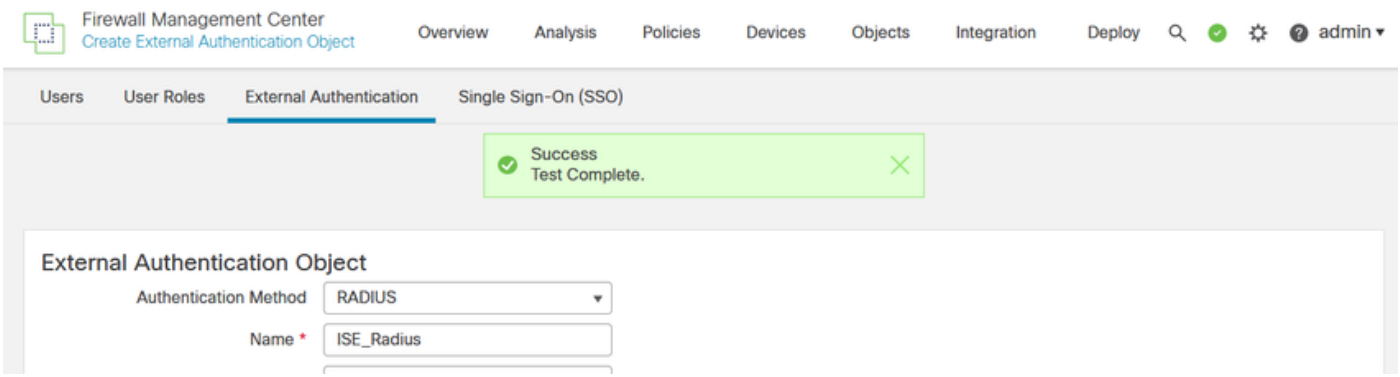


驗證

- 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。



- 有關詳細資訊，可以展開測試輸出下的Details。

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）。