配置FDM主動身份驗證（強制網路門戶）

目錄

簡介

本文檔介紹具有主動身份驗證（強制網路門戶）整合的Firepower裝置管理器(FDM)的配置示例。此配置使用Active Directory(AD)作為源和自簽名證書。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Firepower威脅防禦(FTD)
- Active Directory(AD)
- 自簽名證書。
- 安全通訊端層 (SSL)

採用元件

本檔案中的資訊是根據以下軟體版本：

- Firepower威脅防禦6.6.4
- Active Directory
- PC測試

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。

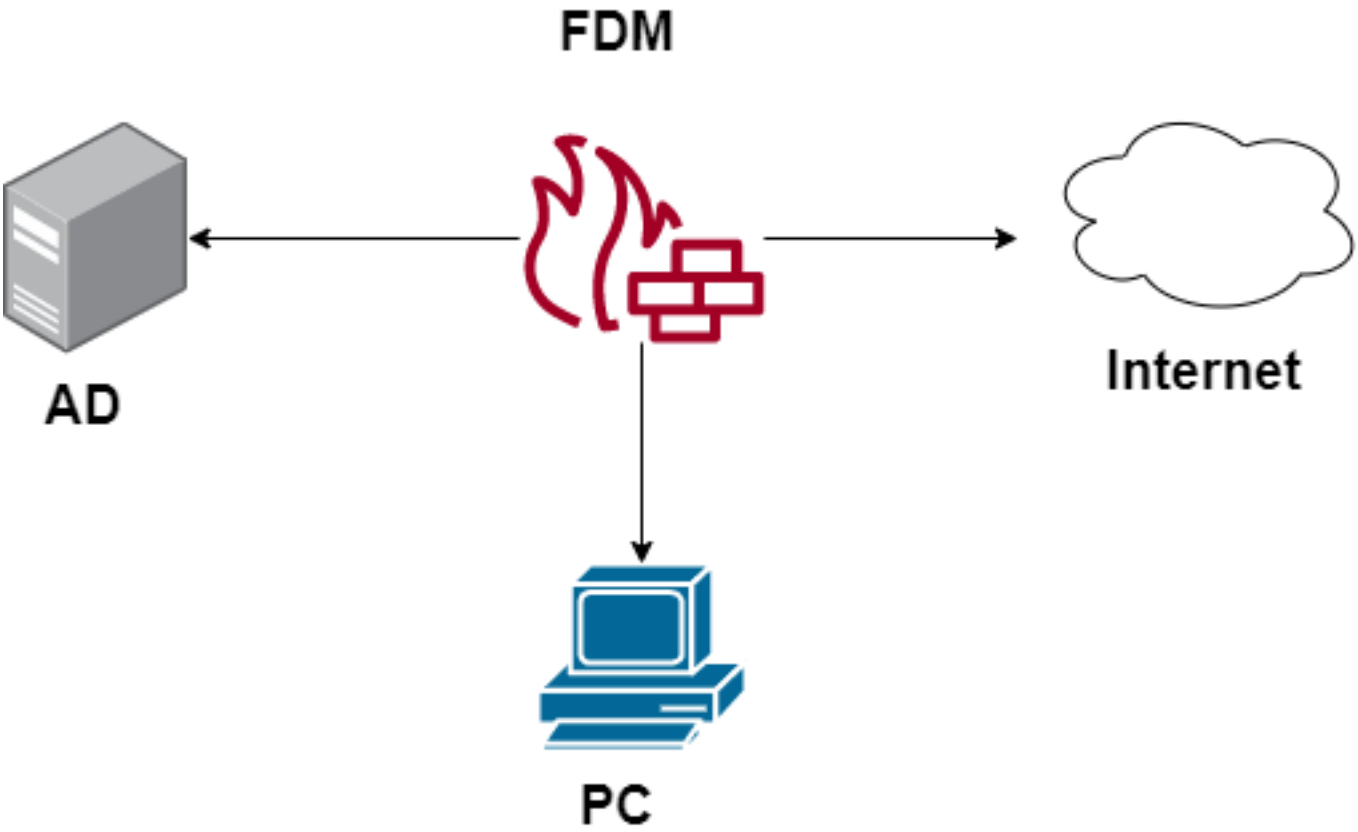
背景資訊

通過主動身份驗證建立使用者身份

身份驗證是確認使用者身份的行為。使用主動身份驗證，當HTTP流量來自系統沒有使用者身份對映的IP地址時，可以決定是否根據為系統配置的目錄對啟動流量流的使用者進行身份驗證。如果使用者成功進行身份驗證，則IP地址被視為具有已身份驗證使用者的身份。

身份驗證失敗不會阻止使用者訪問網路。您的訪問規則最終決定向這些使用者提供哪些訪問許可權。

網路圖表



設定

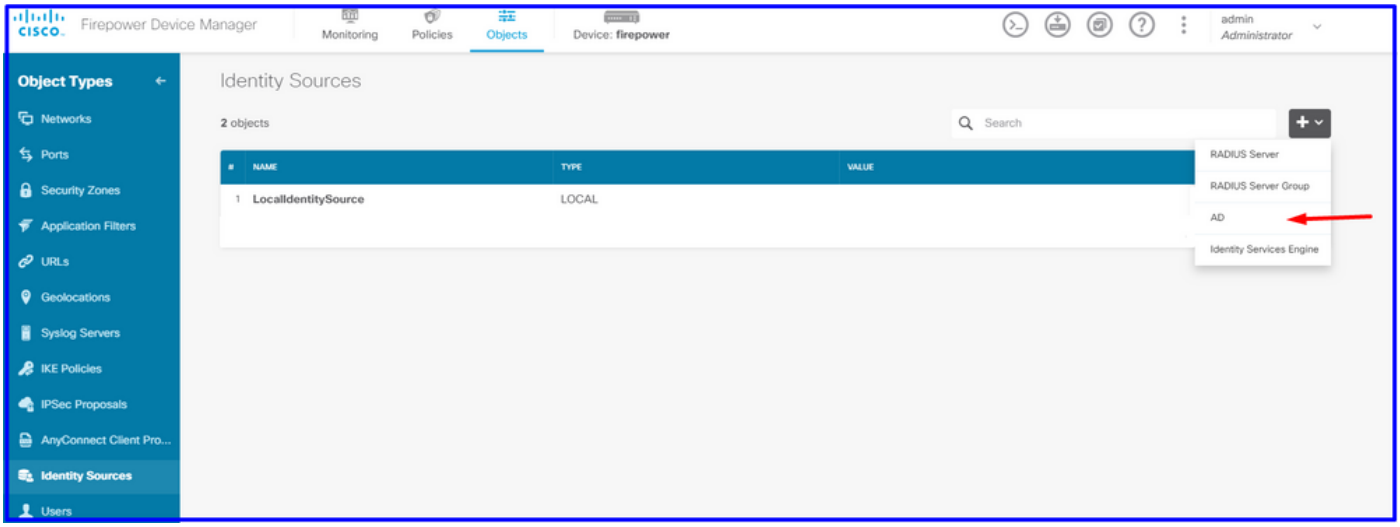
實施身份策略

要啟用使用者身份獲取，以便知道與IP地址關聯的使用者，您需要配置多個專案

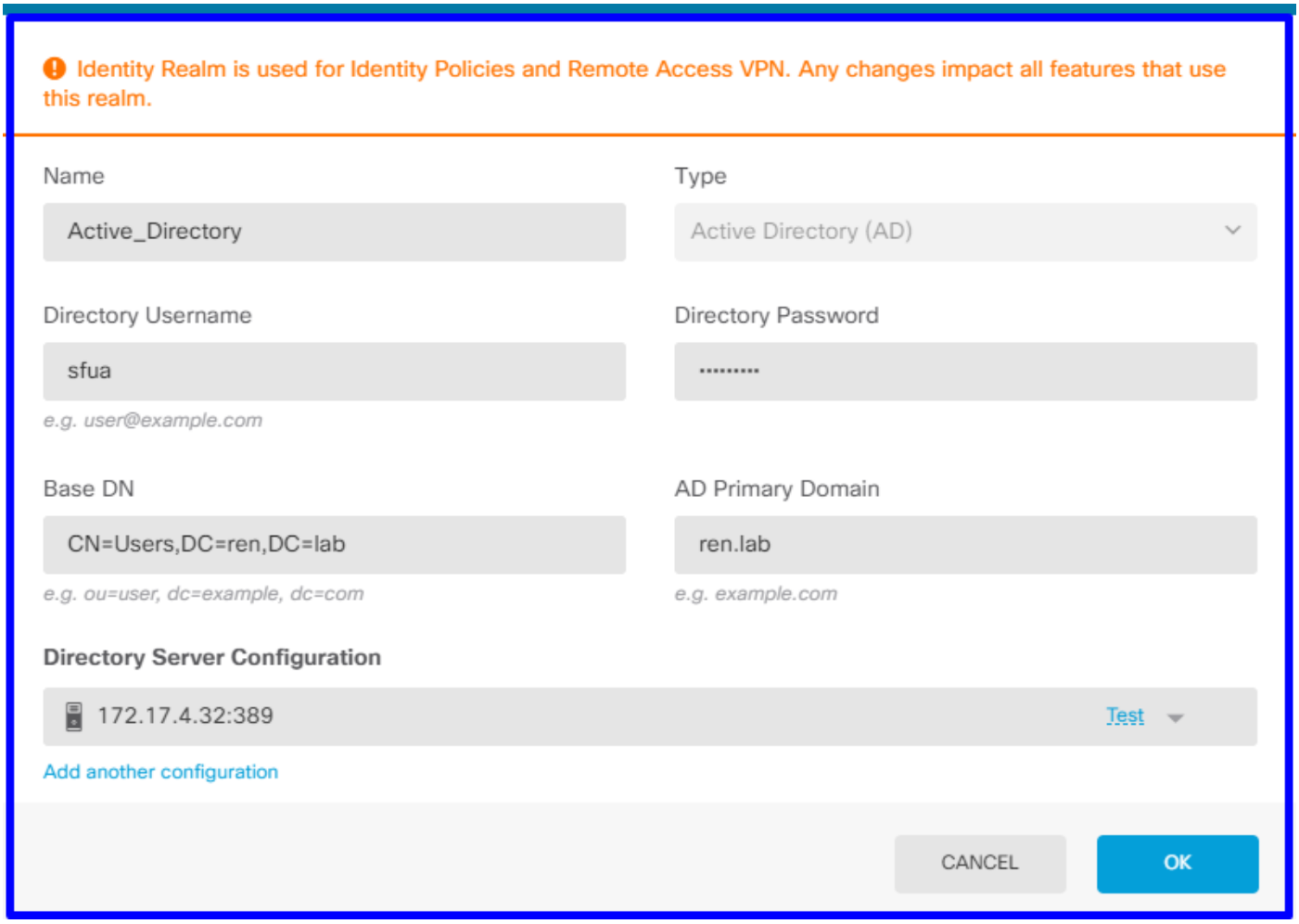
步驟1.配置AD身份領域

無論主動收集使用者身份（通過提示使用者身份驗證）還是被動收集使用者身份，都需要配置具有使用者身份資訊的Active Directory(AD)伺服器。

導航到**對象** > **Identity Services**，然後選擇**AD**選項以新增Active Directory。



新增Active Directory配置：

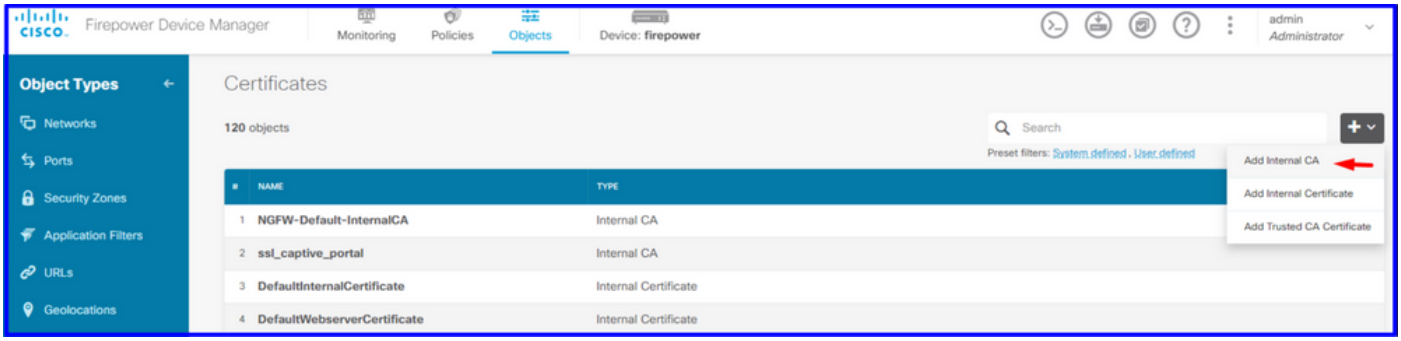


步驟2.建立自簽名證書

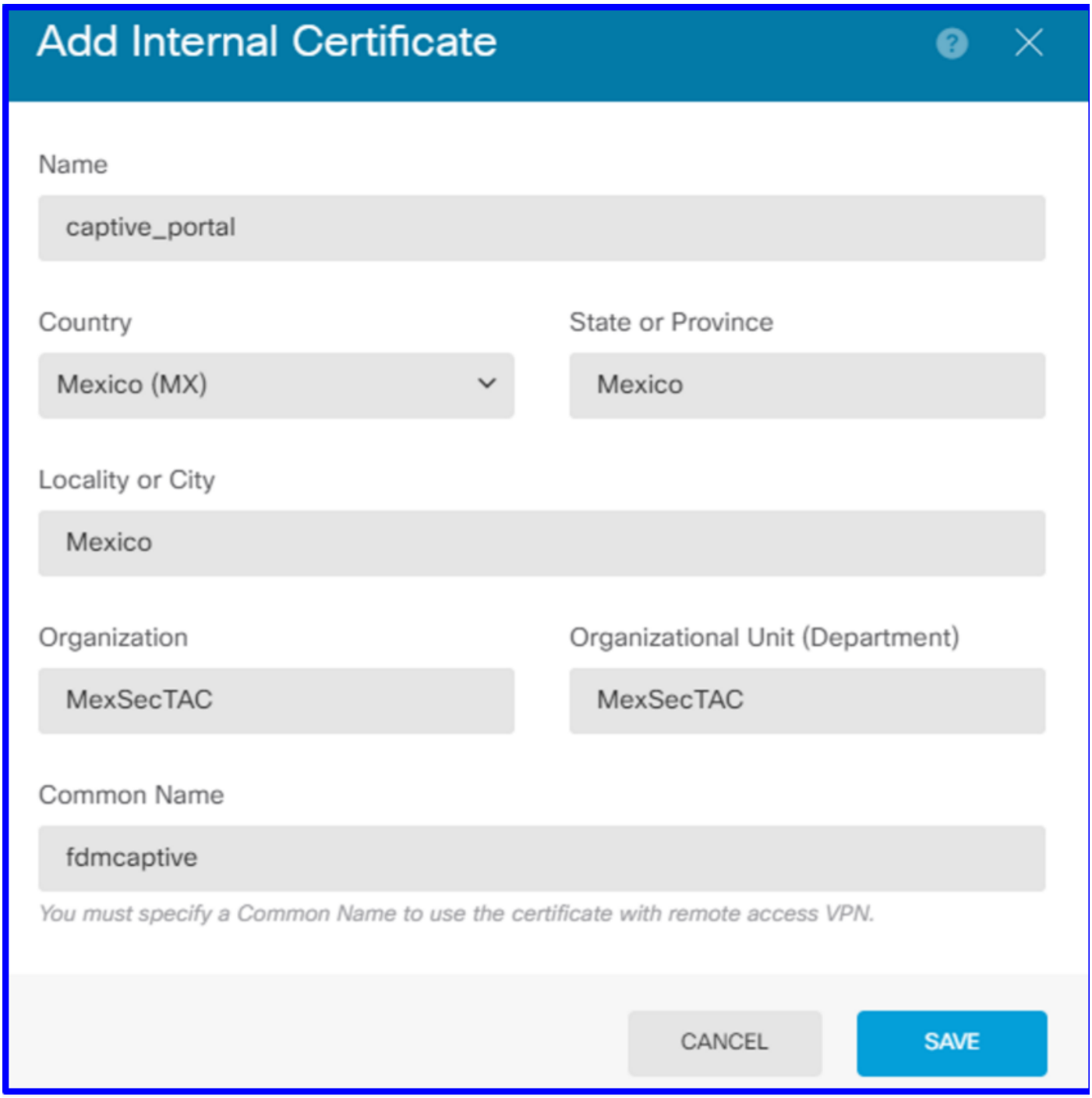
要建立強制網路門戶配置，需要兩個證書，一個用於強制網路門戶，另一個用於SSL解密。

您可以建立自簽名證書，如本例所示。

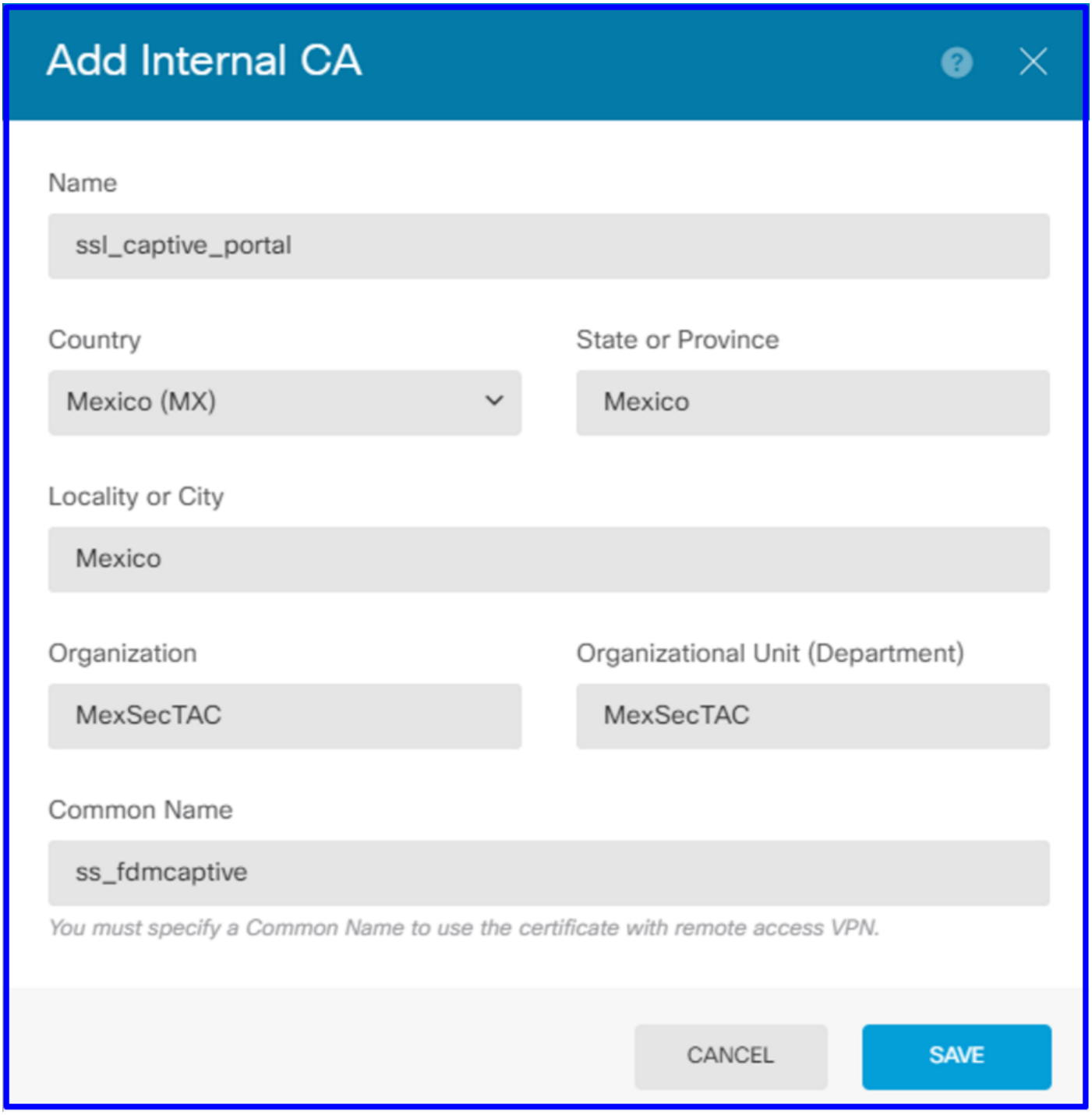
導覽至**Objects > Certificates**



強制網路門戶自簽名證書：



SSL自簽名證書：

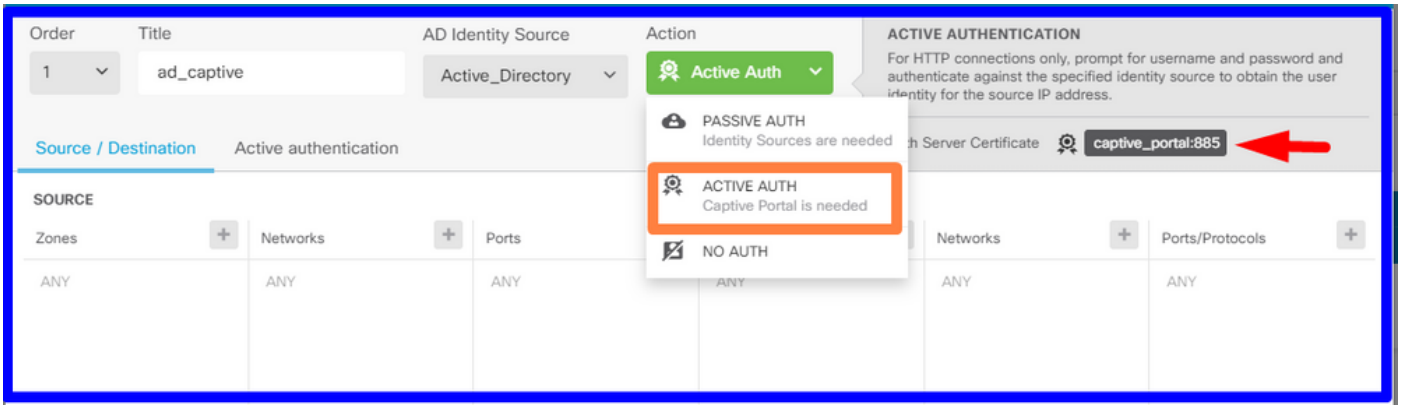


步驟3.創建身份規則

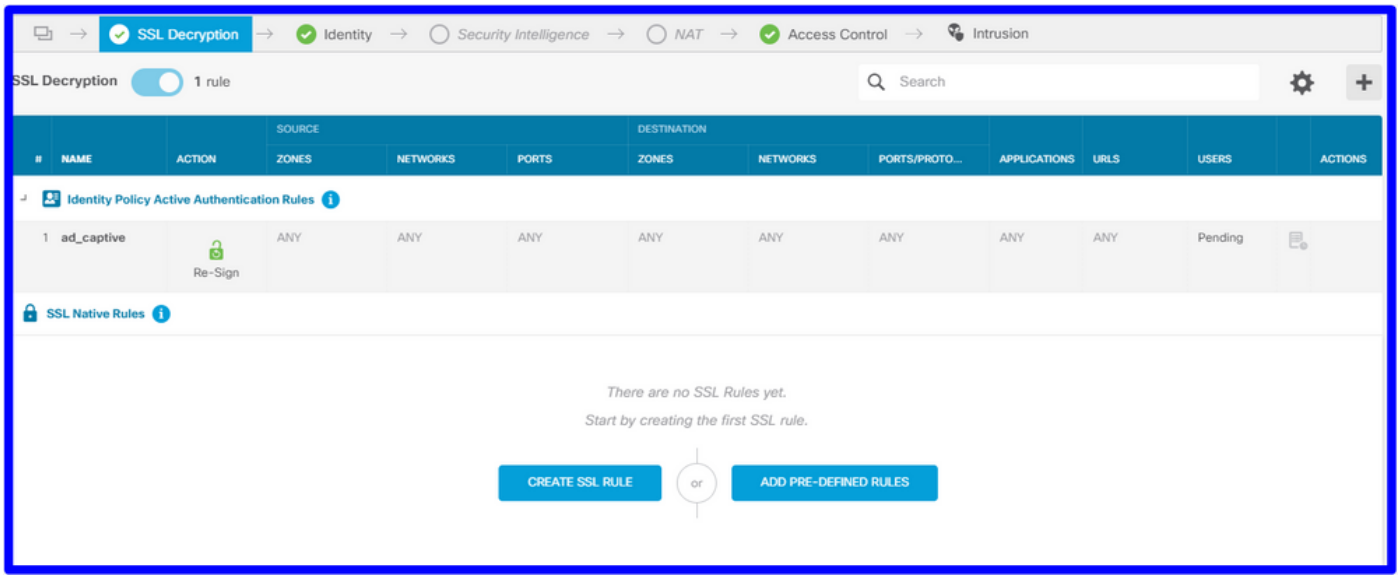
導航到**Policies > Identity >** select **[+]**按鈕以新增新的身份規則。

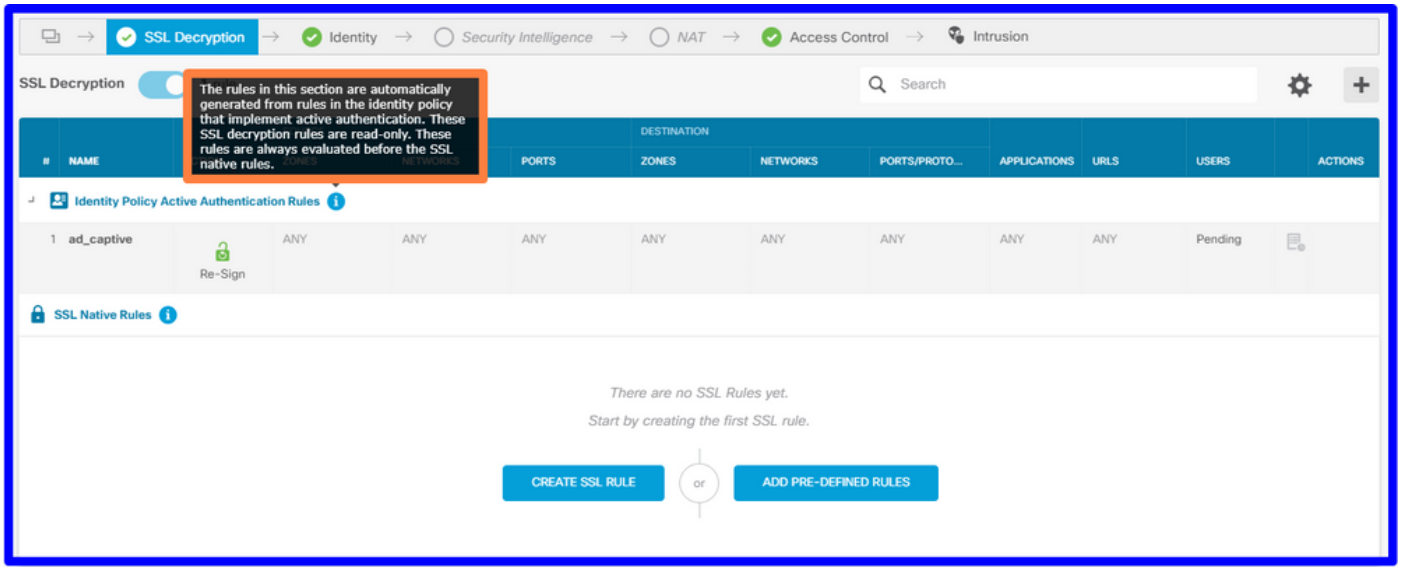
您需要建立身份策略才能配置活動身份驗證，該策略必須具有以下元素：

- AD身份源：與您在步驟編號1中新增的相同
- Action:主動身份驗證
- 伺服器證書：您在[In this scenario captive_portal]之前建立的相同自簽名證書
- Type:HTTP Basic（在此示例場景中）



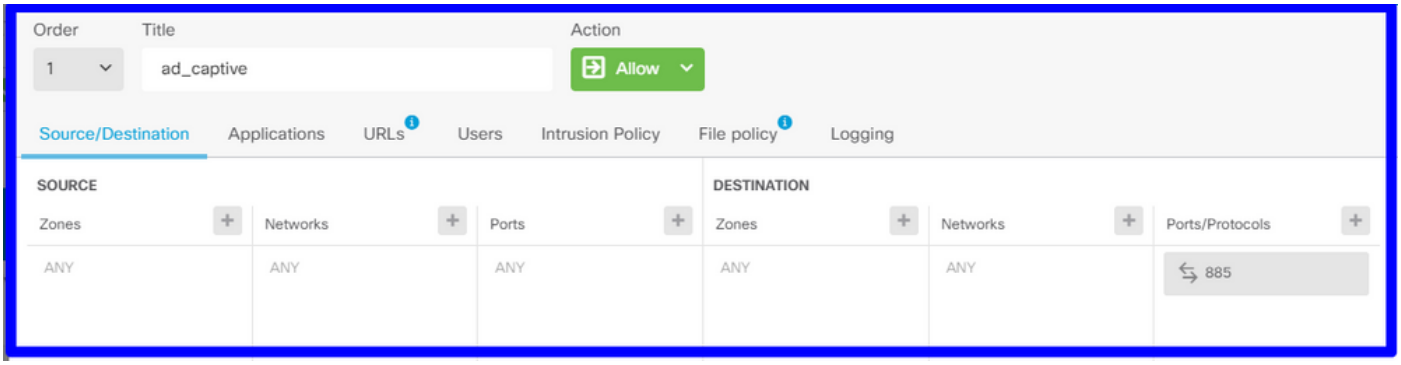
身份策略建立為活動身份驗證後，自動建立SSL規則，預設情況下，此規則設定為具有**Decrypt-Resign**的any規則，這意味著此規則中沒有SSL修改。



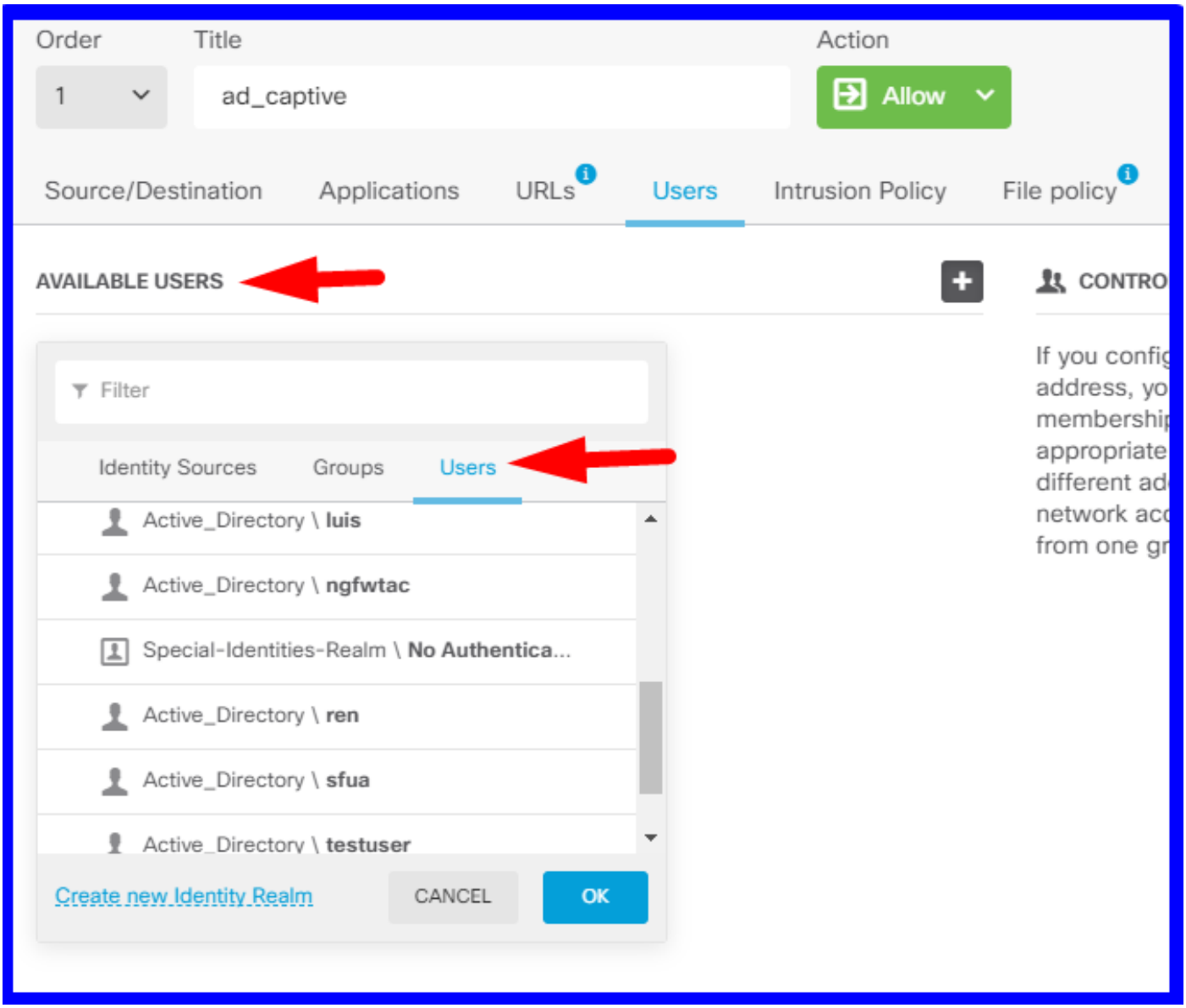


步驟4.在訪問控制策略中建立訪問規則

您需要允許埠885/tcp，它將流量重定向到強制網路門戶身份驗證。導覽至**Policies > Access Control**，然後新增訪問規則。



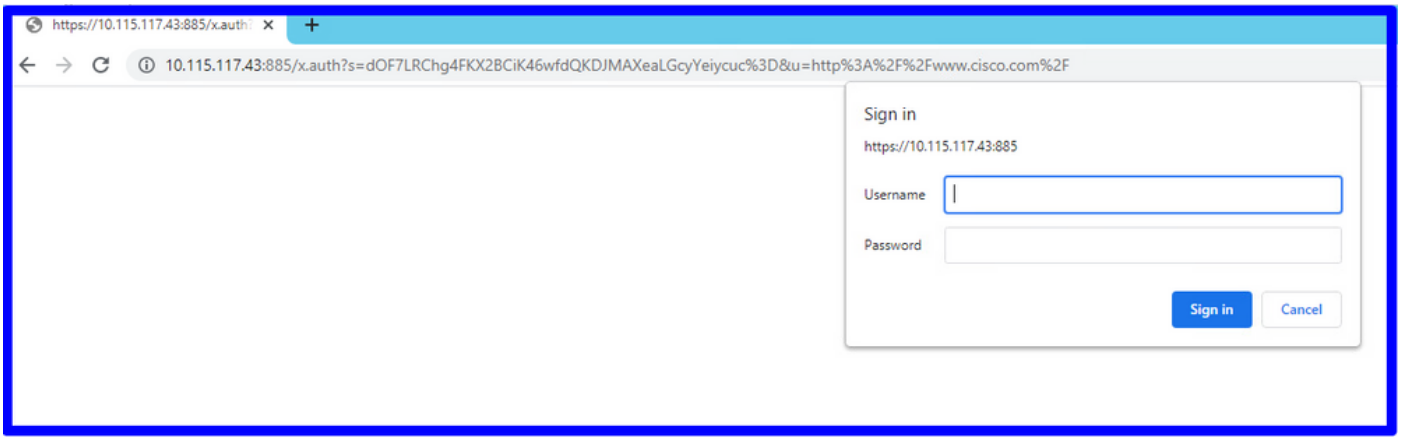
如果需要檢查使用者是否從AD下載，可以編輯訪問規則並導航到**Users**部分，然後在**AVAILABLE USERS**上，可以驗證FDM已經有多少使用者。



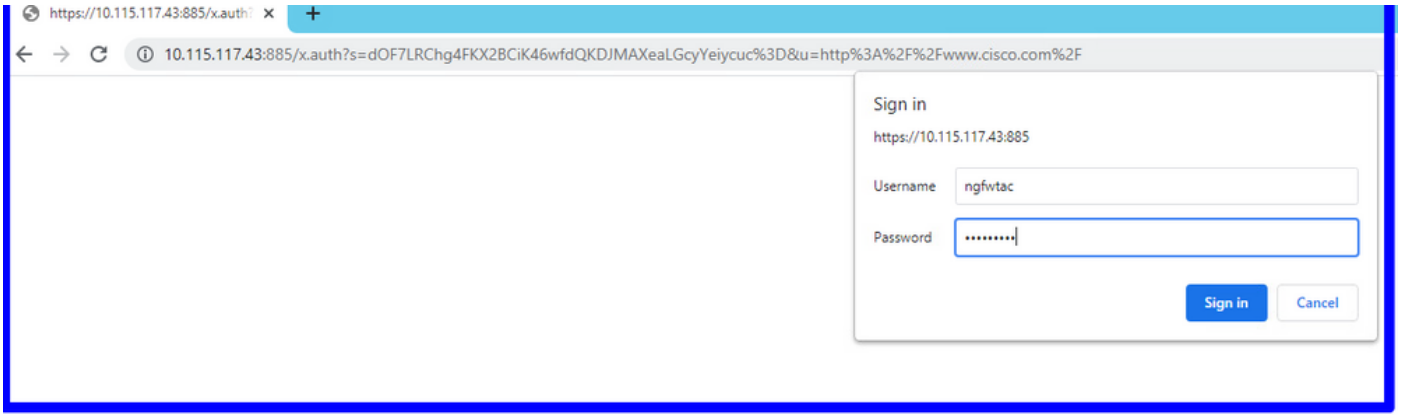
請記得部署配置更改。

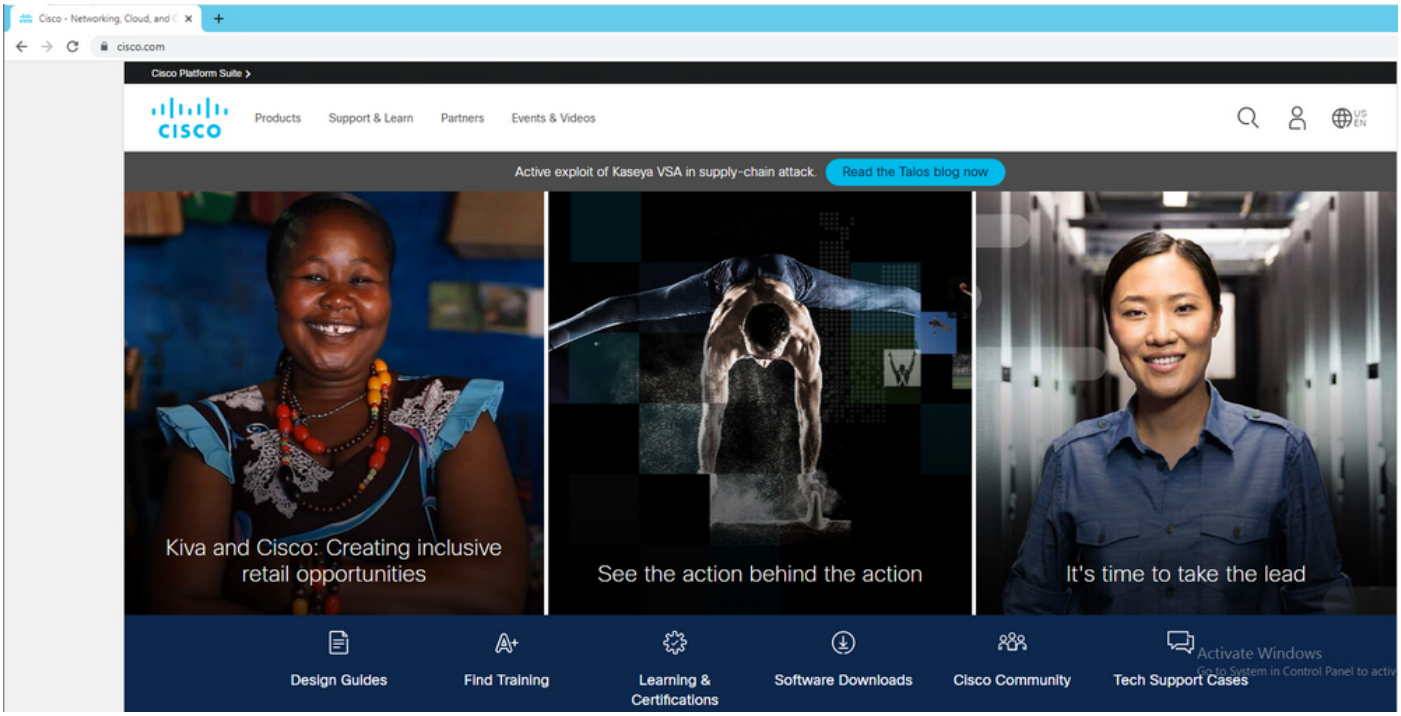
驗證

驗證使用者裝置在導航到HTTPS站點時是否收到此覈取方塊。



輸入使用者AD憑據。





疑難排解

可以使用**user_map_query.pl指令碼驗**證FDM具有使用者ip對映

```
user_map_query.pl -u username ---> for users
user_map_query.pl -i x.x.x.x  ---> for ip addresses
root@firepower:~# user_map_query.pl -u ngfwtac
```

```
WARNING: This script was not tested on this major version (6.6.0)! The results may be
unexpected.
Current Time: 06/24/2021 20:45:54 UTC
Getting information on username(s)...
---
User #1: ngfwtac
---
ID:         8
Last Seen:  06/24/2021 20:44:03 UTC
 for_policy: 1
 Realm ID:   4

==============================
|          Database          |
==============================

##) IP Address [Realm ID]
 1) ::ffff:10.115.117.46 [4]

##) Group Name (ID) [realm: Realm Name (ID)]
 1) Domain Users (12) [realm: Active_Directory (4)]
```

在清潔模式下，您可以配置：

系統支援identity-debug以驗證重定向是否成功。

```
> system support identity-debug
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol:
Please specify a client IP address: 10.115.117.46
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring identity and firewall debug messages

10.115.117.46-55809 > 72.163.47.11-53 17 AS 1-1 I 1 deleting firewall session flags = 0x10001,
fwFlags = 0x100
10.115.117.46-55809 > 72.163.47.11-53 17 AS 1-1 I 1 Logging EOF as part of session delete with
rule_id = 1 ruleAction = 2 ruleReason = 0
10.115.117.46-50611 > 142.250.138.94-443 6 AS 1-1 I 0 Got end of flow event from hardware with
flags 00010001. Rule Match Data: rule_id 0, rule_action 0 rev_id 0, rule_flags 2
10.115.117.46-50611 > 142.250.138.94-443 6 AS 1-1 I 0 Logging EOF for event from hardware with
rule_id = 1 ruleAction = 2 ruleReason = 0
10.115.117.46-50611 > 142.250.138.94-443 6 AS 1-1 I 0 : Received EOF, deleting the snort
session.
10.115.117.46-50611 > 142.250.138.94-443 6 AS 1-1 I 0 deleting firewall session flags = 0x10003,
fwFlags = 0x114
10.115.117.46-65489 > 72.163.47.11-53 17 AS 1-1 I 1 deleting firewall session flags = 0x10001,
fwFlags = 0x100
10.115.117.46-65489 > 72.163.47.11-53 17 AS 1-1 I 1 Logging EOF as part of session delete with
rule_id = 1 ruleAction = 2 ruleReason = 0
10.115.117.46-65489 > 173.36.131.10-53 17 AS 1-1 I 1 deleting firewall session flags = 0x10001,
fwFlags = 0x100
10.115.117.46-65489 > 173.36.131.10-53 17 AS 1-1 I 1 Logging EOF as part of session delete with
rule_id = 1 ruleAction = 2 ruleReason = 0

10.115.117.46-53417 > 72.163.47.11-53 17 AS 1-1 I 0 deleting firewall session flags = 0x10001,
fwFlags = 0x100
10.115.117.46-53417 > 72.163.47.11-53 17 AS 1-1 I 0 Logging EOF as part of session delete with
rule_id = 1 ruleAction = 2 ruleReason = 0
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 Starting authentication (sfAuthCheckRules
params) with zones 2 -> 3, port 63784 -> 53, geo 16671760 -> 16671778
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 looked for user_id with realm_id 4 auth_type
```

```
2, returning realm_id 4 auth_type 2 user_id 8
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 found active binding for user_id 8 in realm
4
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 matched auth rule id = 2023803385 user_id =
8 realm_id = 4
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 new firewall session
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 using HW or preset rule order 4, 'Default
Action', action Allow and prefilter rule 0
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 HitCount data sent for rule id: 1,
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 allow action
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 Starting authentication (sfAuthCheckRules
params) with zones 2 -> 3, port 50619 -> 443, geo 16671760 -> 16671778
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 looked for user_id with realm_id 4
auth_type 2, returning realm_id 4 auth_type 2 user_id 8
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 found active binding for user_id 8 in
realm 4
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 matched auth rule id = 2023803385 user_id
= 8 realm_id = 4
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 new firewall session
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 using HW or preset rule order 4, 'Default
Action', action Allow and prefilter rule 0
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 HitCount data sent for rule id: 1,
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 allow action
```

参考：

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptd-fdm-identity.html#id_71535

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptd-fdm-identity-sources.html#task_83008ECD0DBF4E388B28B6247CB2E64B