使用FMC配置被動身份代理

目錄

簡介

本文檔介紹如何配置將會話資料傳送到FMC的被動身份代理源

必要條件

需求

- 運行版本7.6+的Cisco安全防火牆管理中心
- 運行版本7.6+的思科安全防火牆
- 在Windows Active Directory伺服器中，伺服器必須運行Windows Server 2008或更高版本。
- 必須在安全防火牆威脅防禦裝置上啟用Snort 3。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科安全防火牆管理中心7.6.5
- 思科安全防火牆7.6.5
- Windows Server 2022上運行的Microsoft Active Directory。

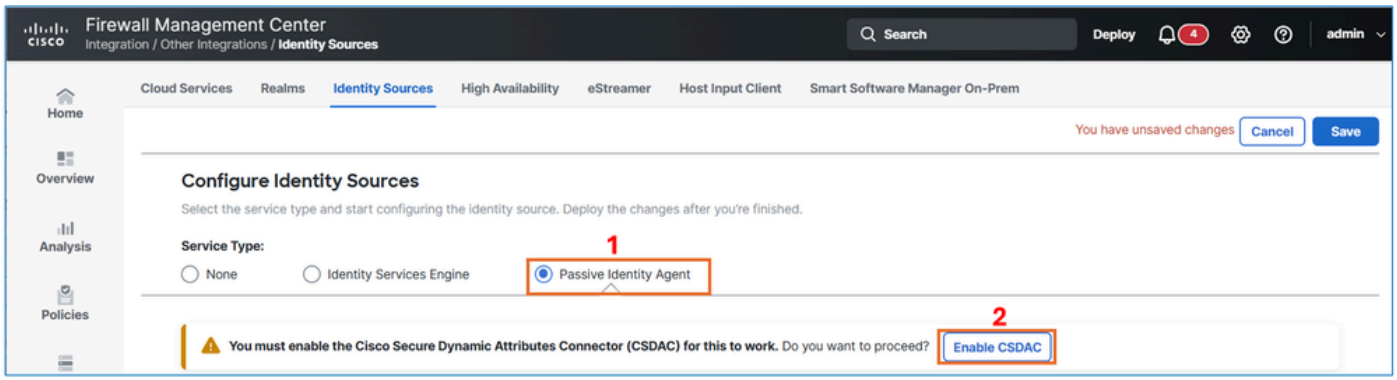
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

組態

在配置代理之前，請完成AD和FMC整合。

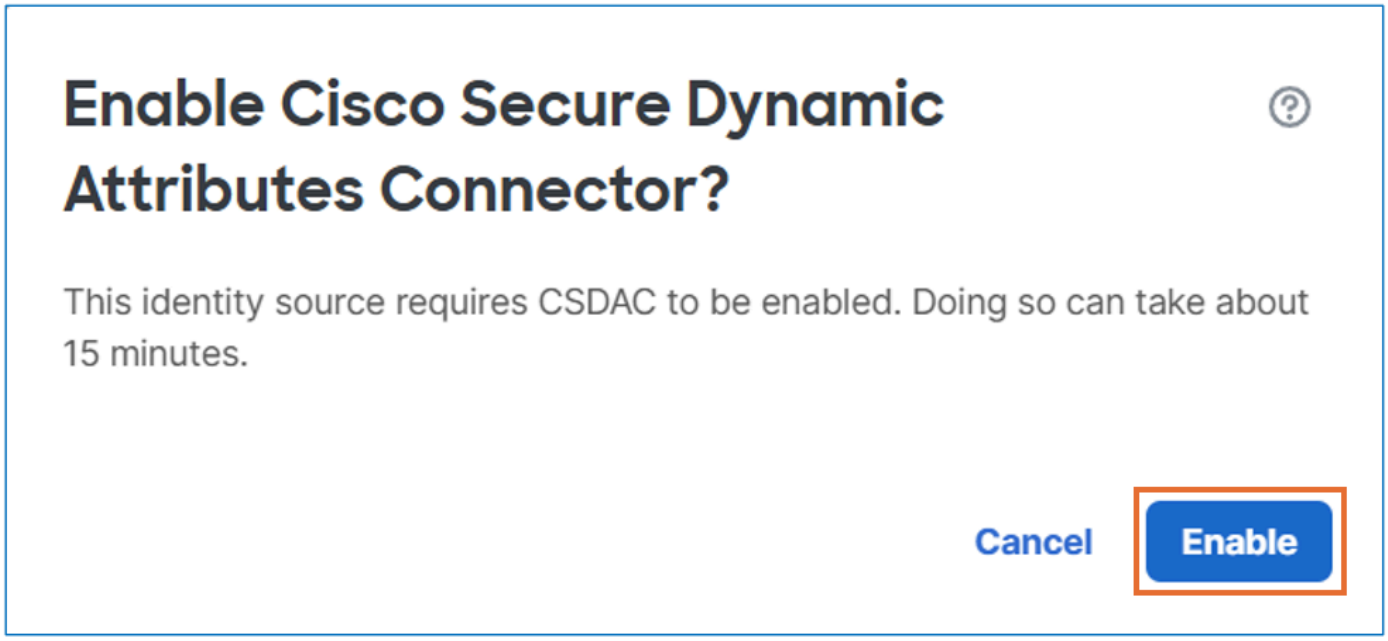
配置被動身份代理源

在FMC UI中，導航至Integration > Other Integrations > Identity Sources，然後點選Passive Identity Agent。 如果尚未啟用Cisco Secure Dynamic Attributes Connector，則會通過按一下Enable CSDAC來提示您啟用它。



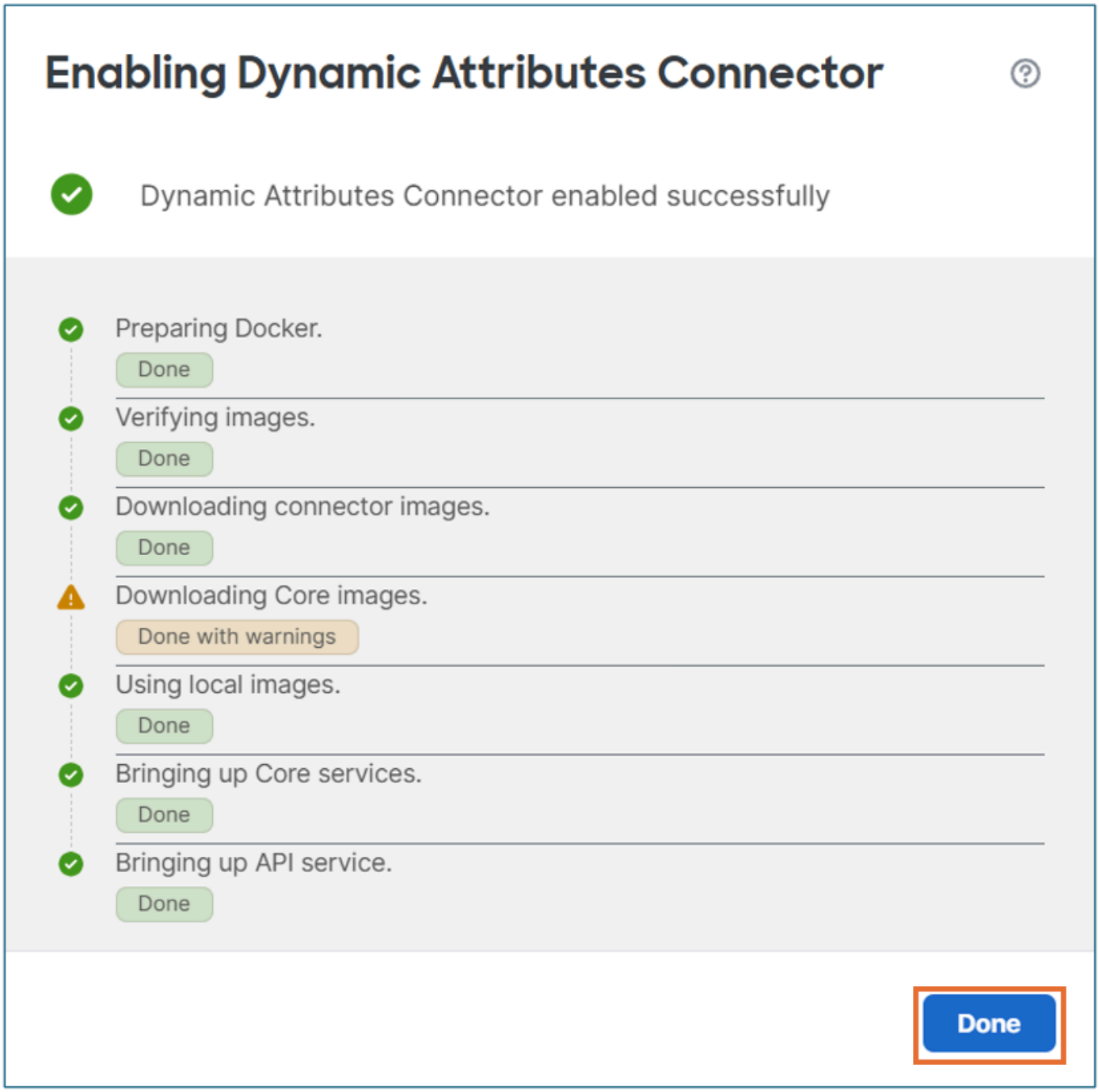
被動身分識別代理

按一下Enablebutton以啟用CSDAC。



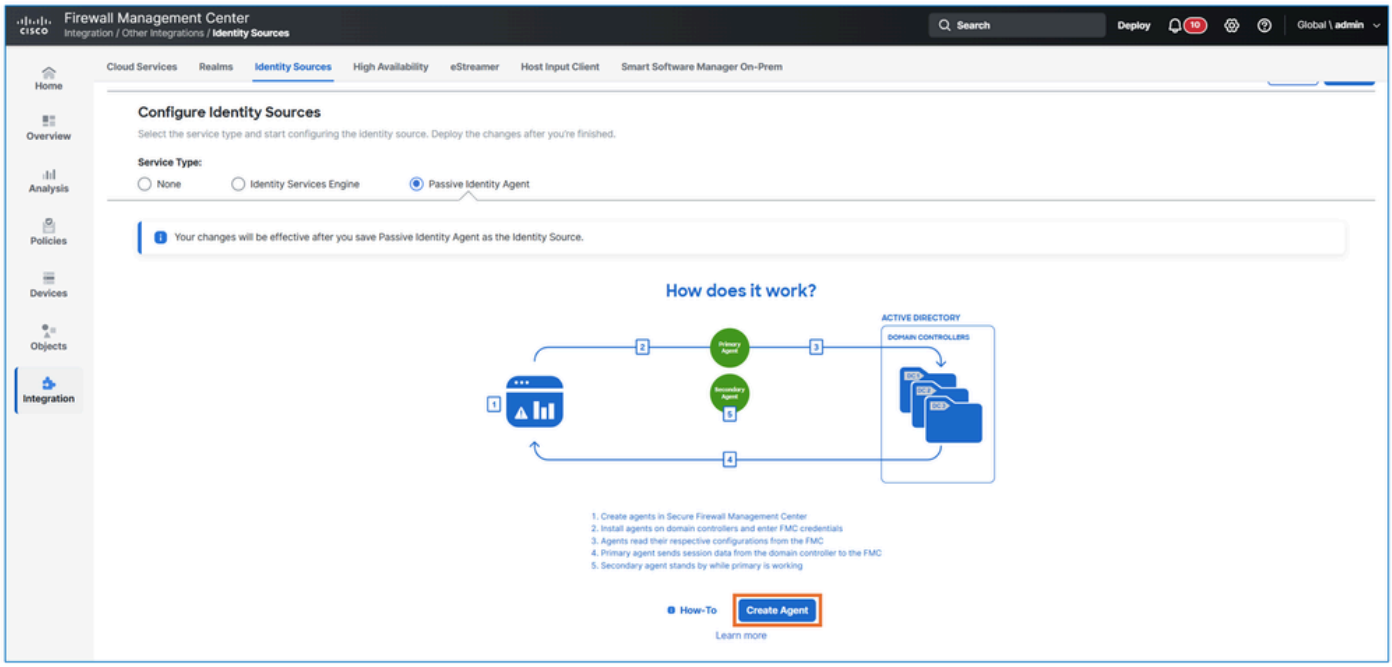
啟用CSDAC

此步驟大約需要10分鐘。正確啟用CSDAC後，按一下Donebutton繼續。



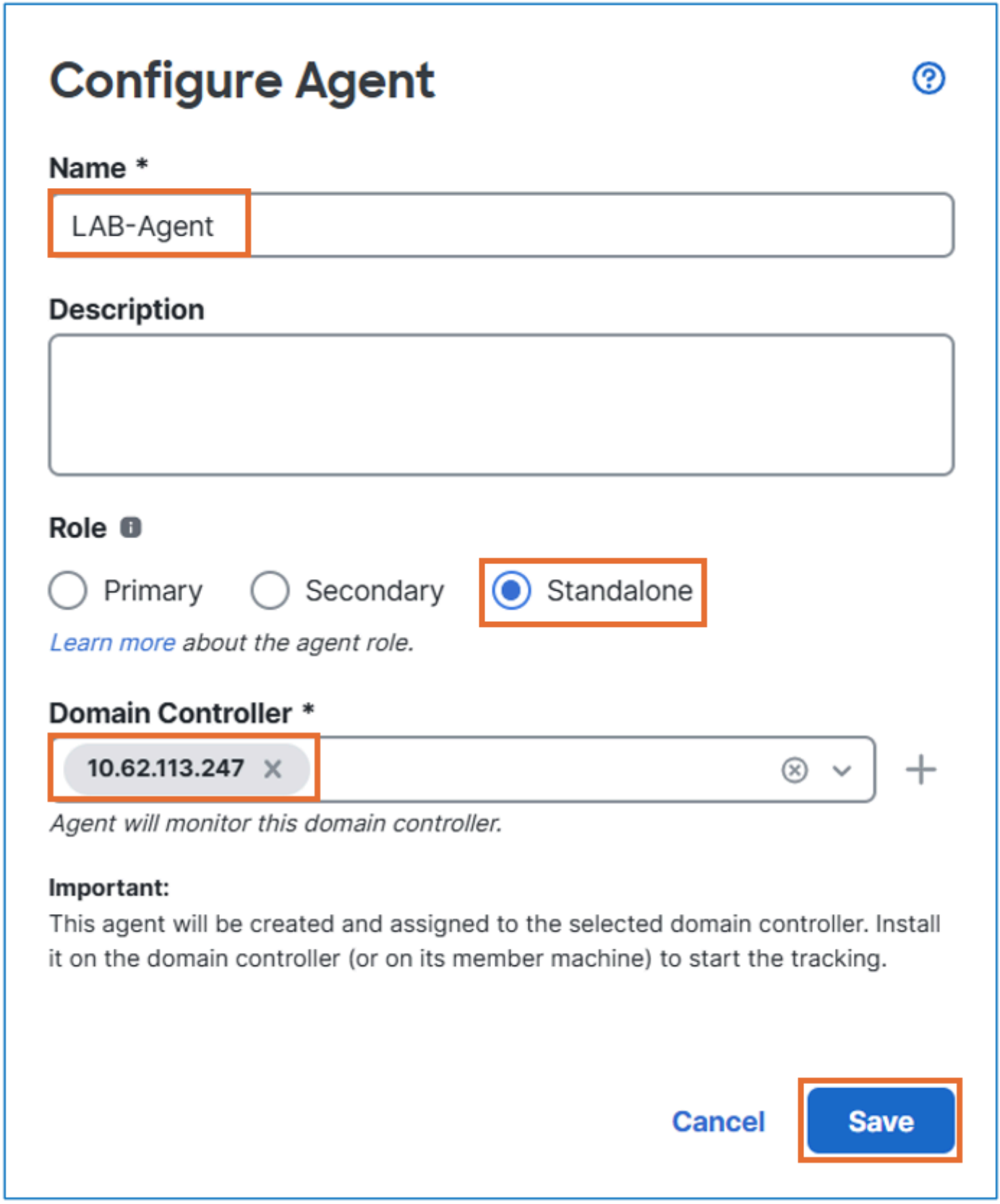
已啟用CSDAC

按一下Create Agent按鈕。



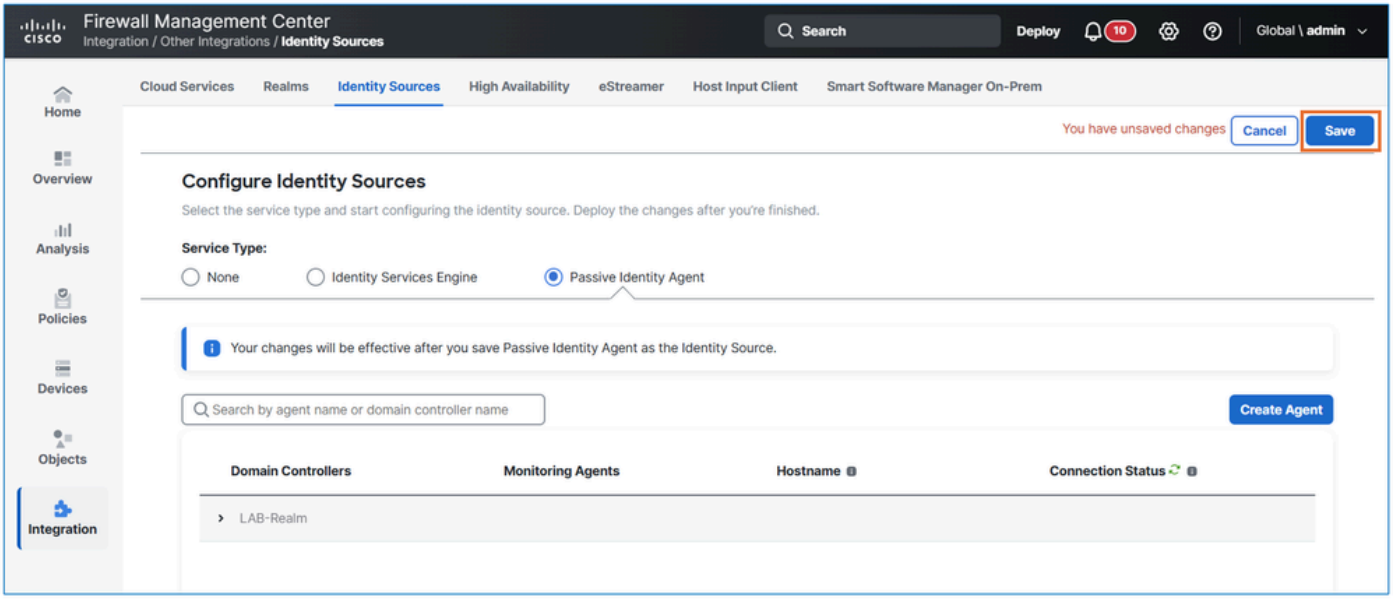
建立代理

定義代理的名稱，選擇Standaloneoption，然後將其與上一個任務中建立的Domain Controller關聯。



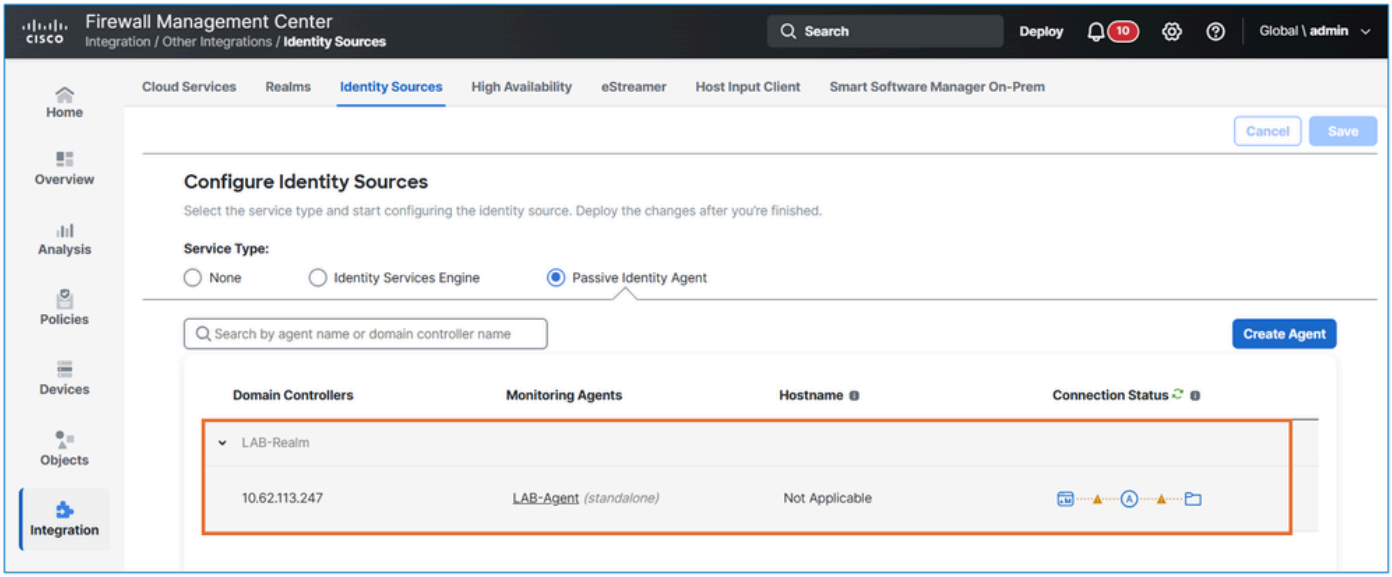
配置代理

按一下「儲存」按鈕。



儲存組態

結果。



驗證狀態

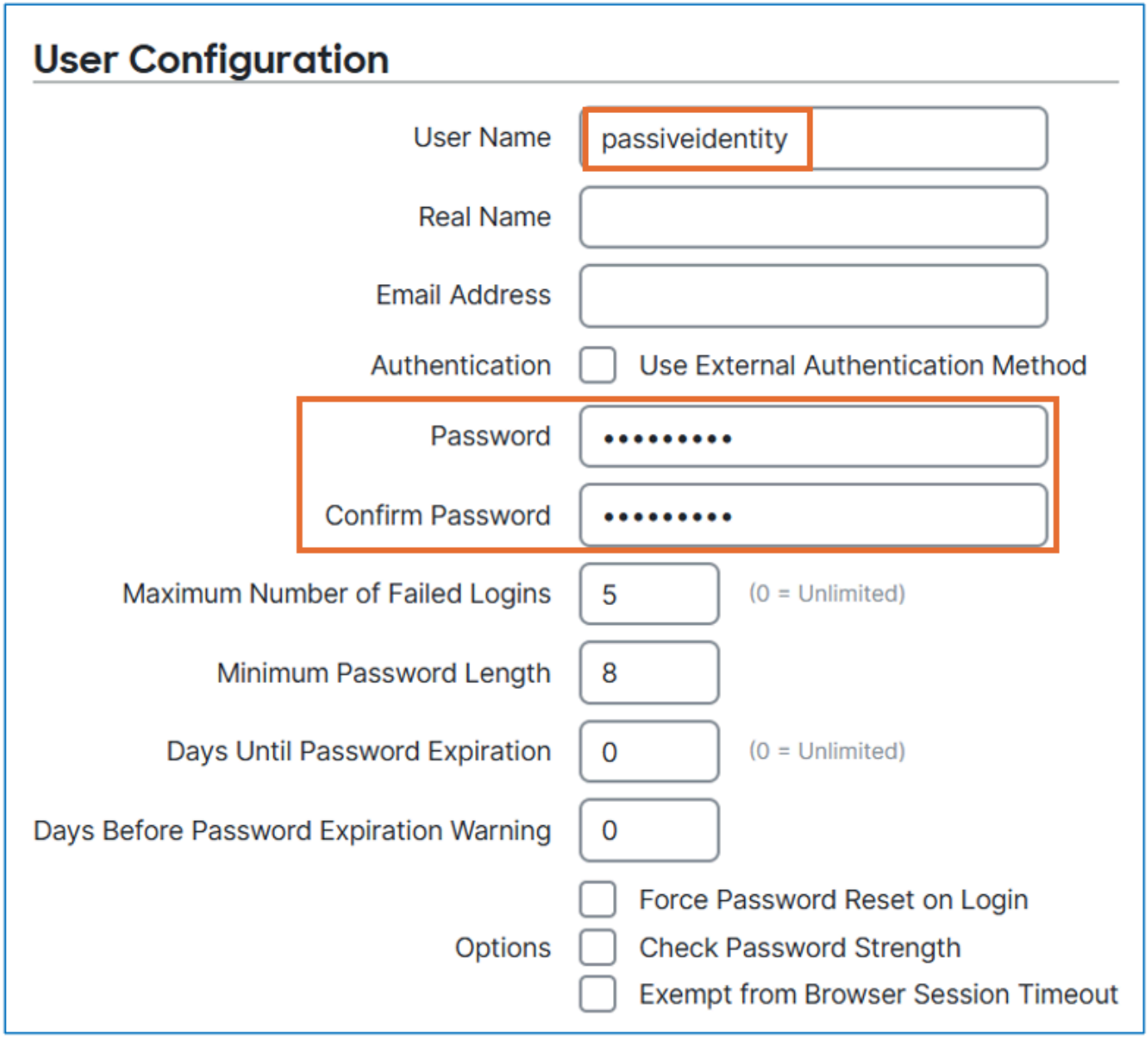
附註：被動身份代理使用線路指示狀態，琥珀色表示該代理從未成功與安全防火牆管理中心通訊。新建立的代理線路為琥珀色，在配置完成前保持琥珀色。

在安全防火牆管理中心上建立被動身份代理使用者

建立有足夠許可權與被動身份代理通訊的Secure Firewall Management Center使用者。此使用者執

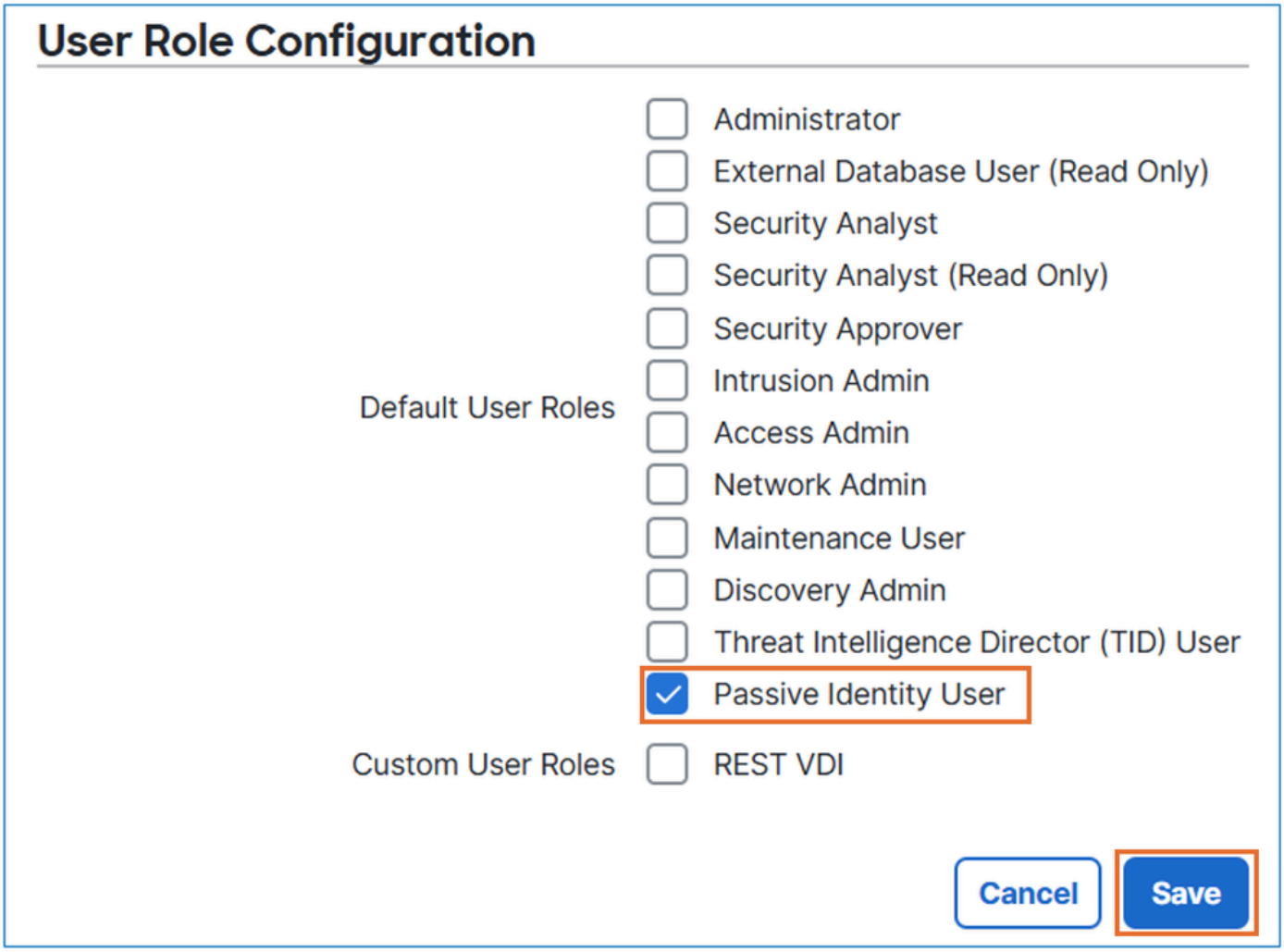
行其他任務的許可權有限；使用者應僅啟用與被動身份代理的通訊。

在FMC UI中，導航至System > Users，然後點選Create User。根據任務要求填寫使用者詳細資訊。



建立使用者

僅分配被動身份使用者角色。按一下「儲存」按鈕。

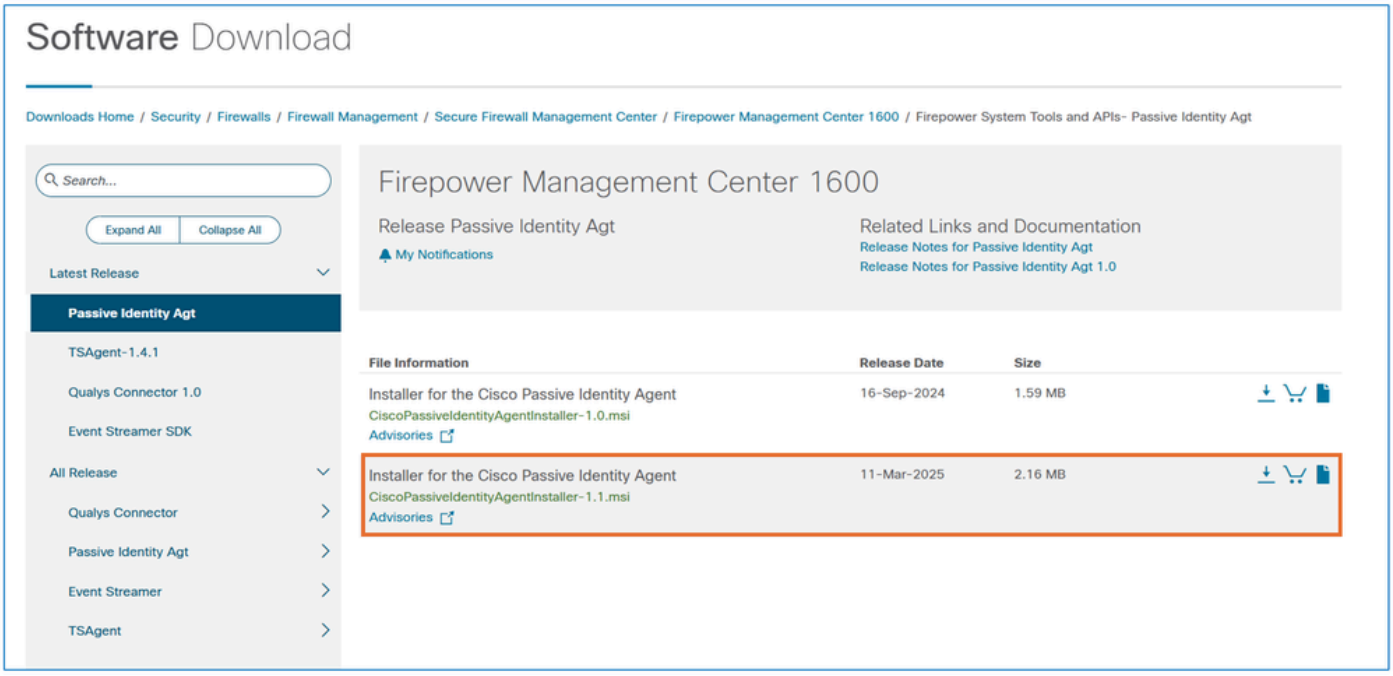


選擇被動身份使用者

安裝和配置被動身份代理軟體

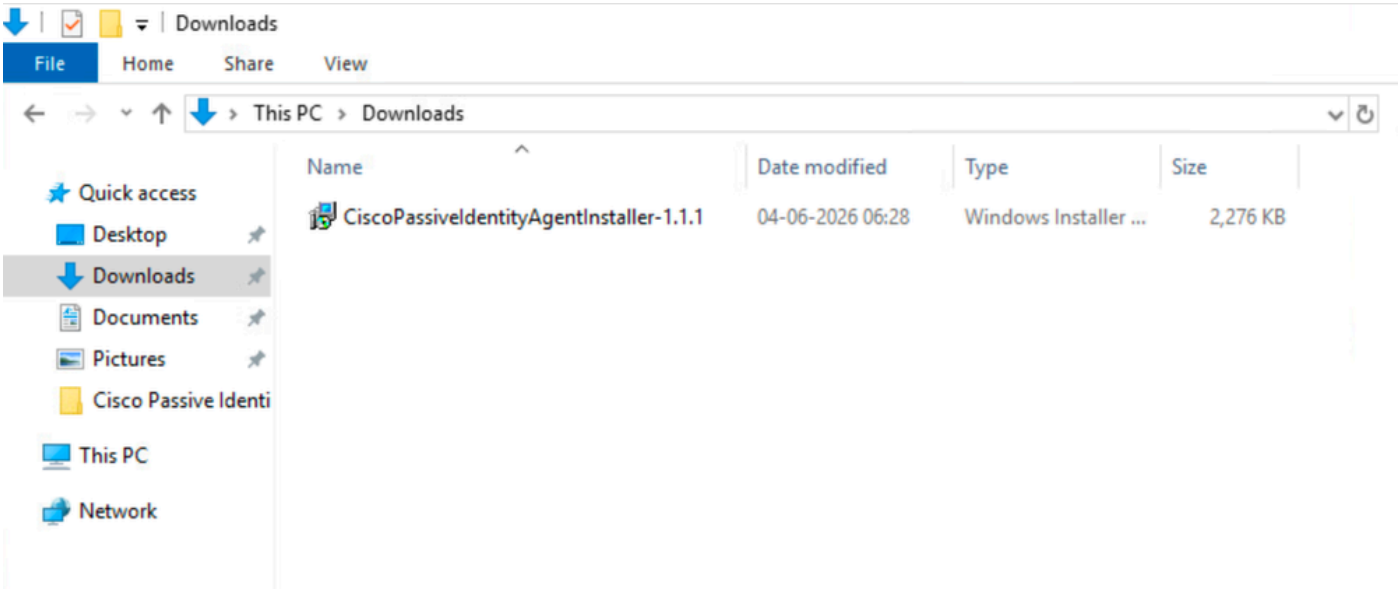
在指定的域控制器上安裝並配置被動身份代理軟體。

從software.cisco.com下載被動身份代理。



下載軟體

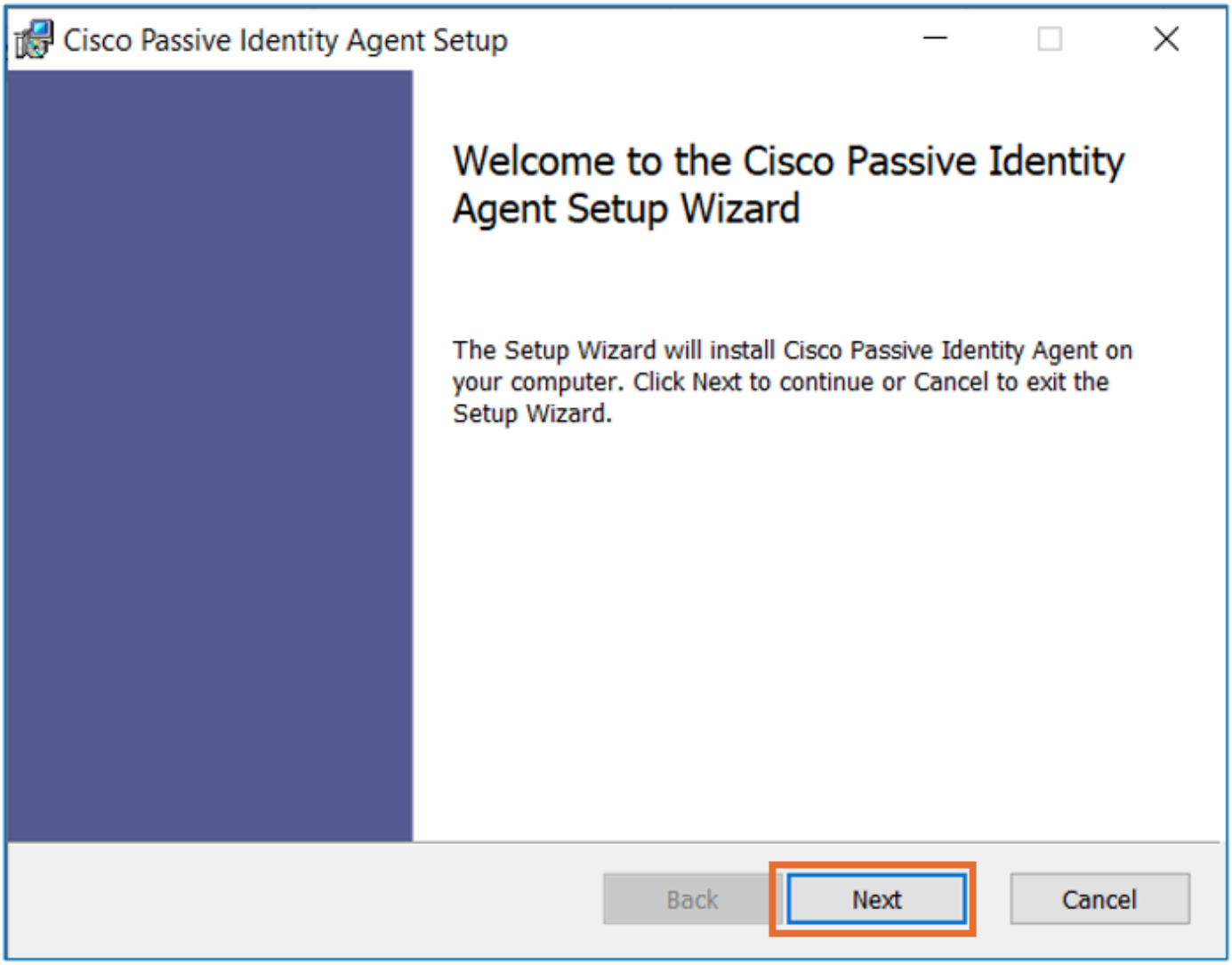
下載代理後，在域控制器上開始安裝過程。



代理

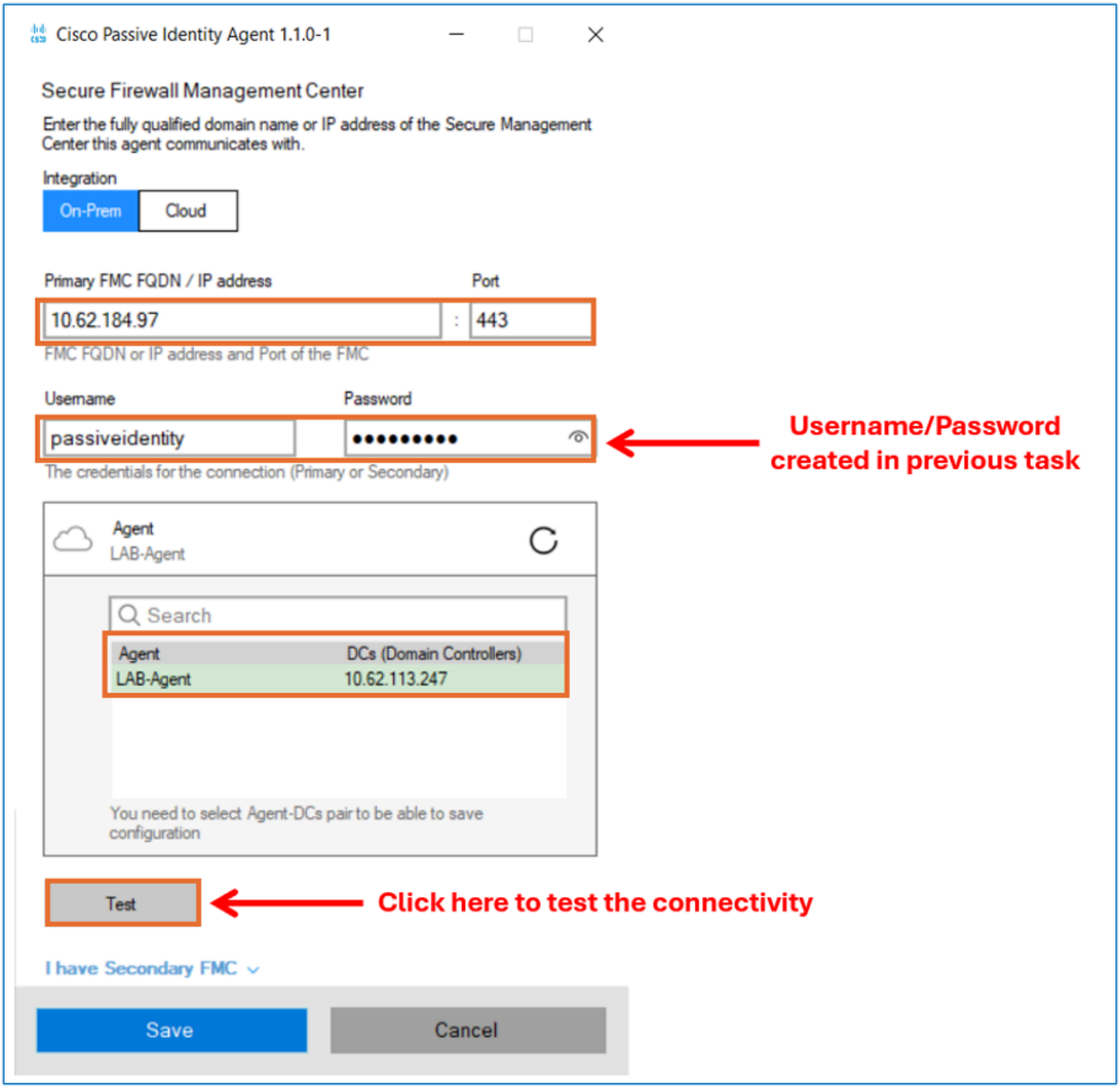
]

請參閱提供的安裝說明以完成設定。



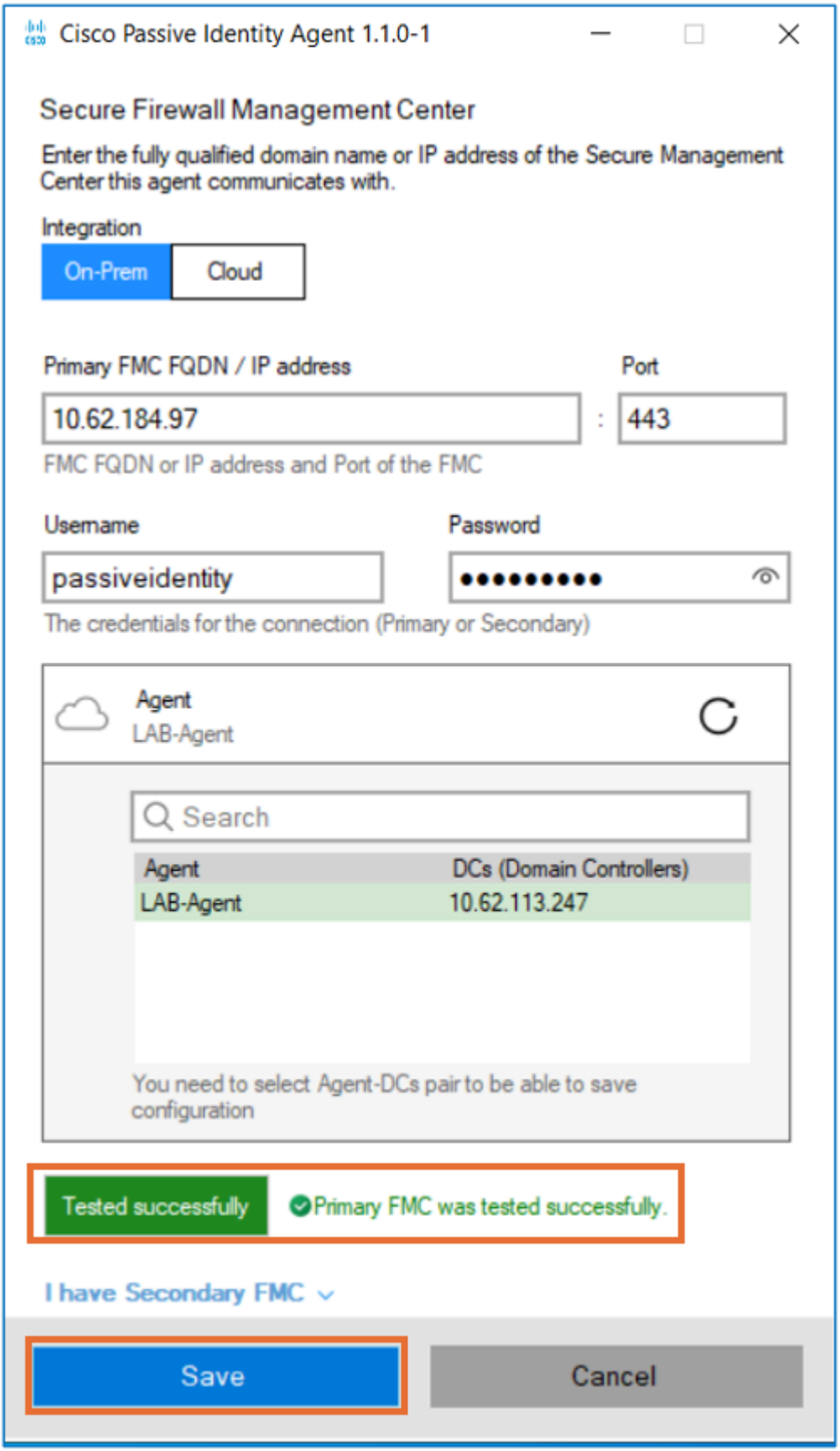
安裝

安裝完成後，開啟被動Identity Agent軟體，然後按照任務要求中的指定輸入所需的資訊。按一下Test按鈕驗證與FMC的連線。



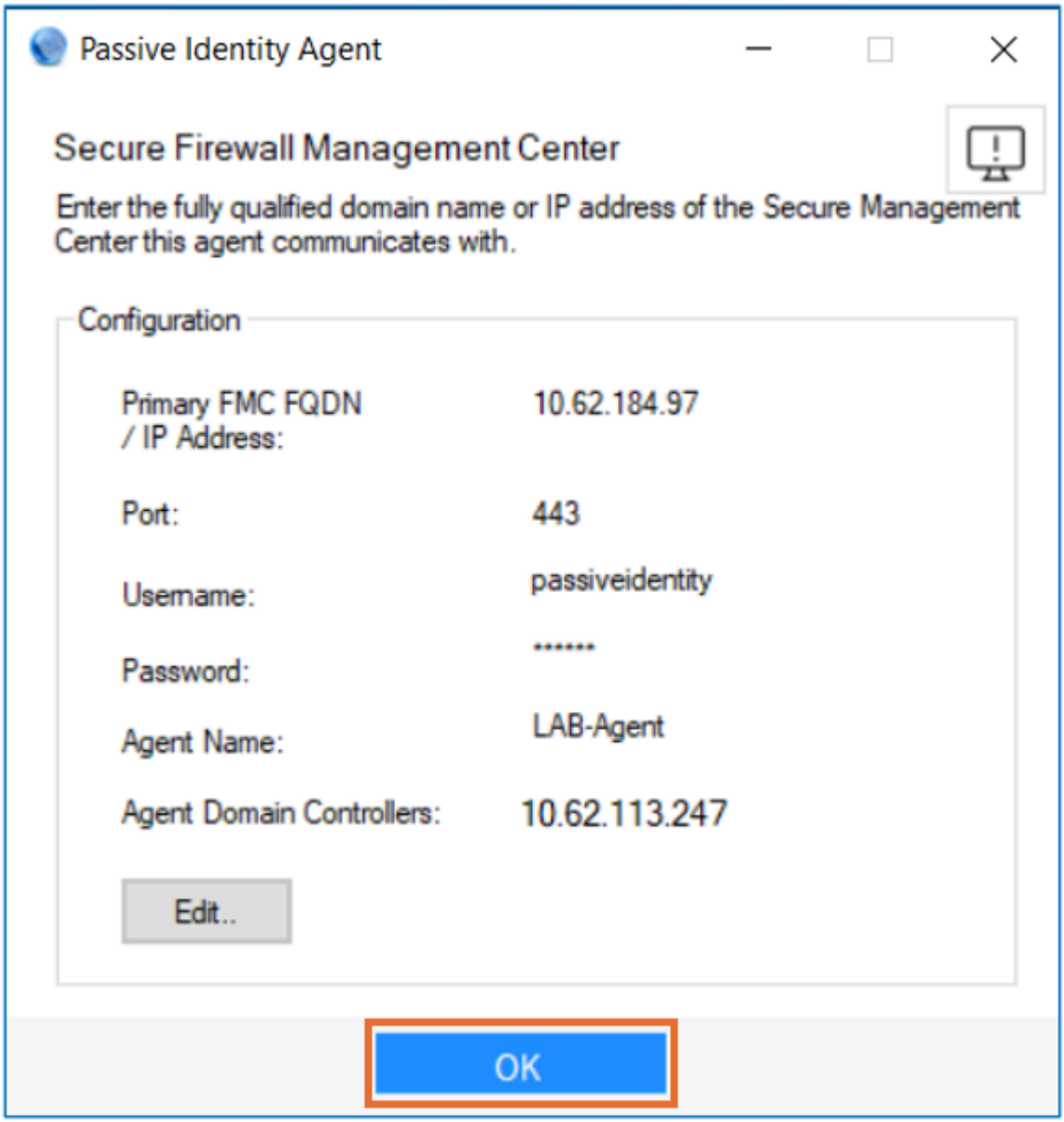
配置代理。

成功測試連線後，按一下Savebutton。



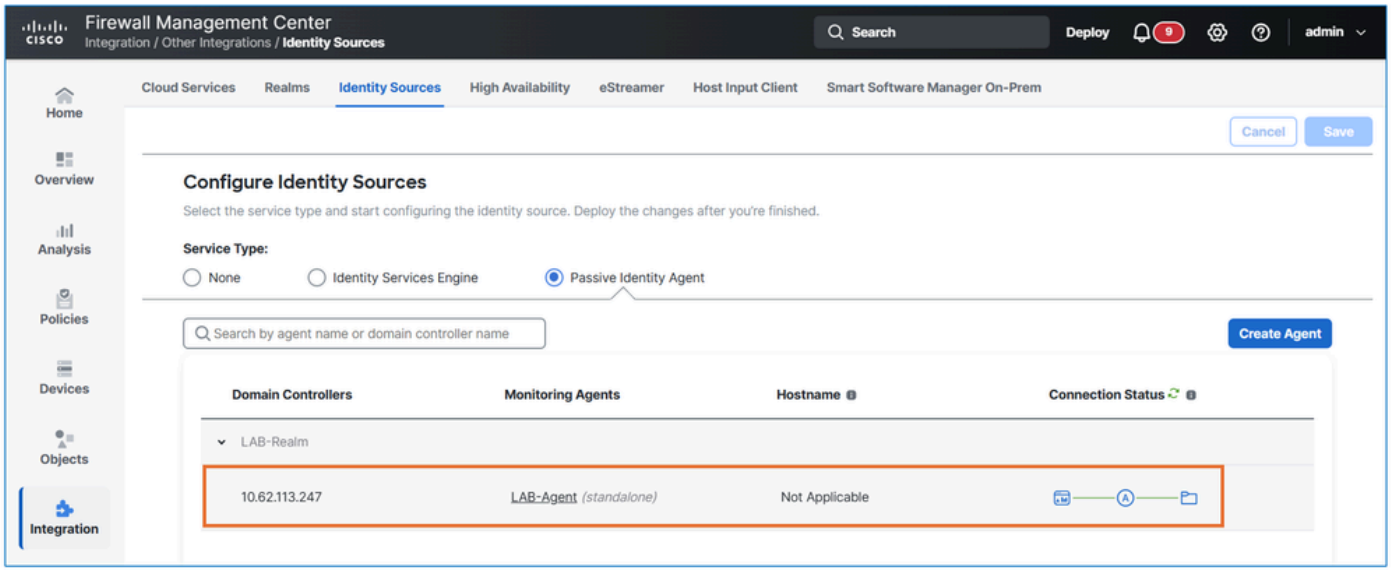
測試

按一下OK按鈕完成代理配置。



代理正在運行

在FMC UI中，導航到整合>其他整合>身份源>被動身份代理。確認被動身份代理顯示綠色狀態。



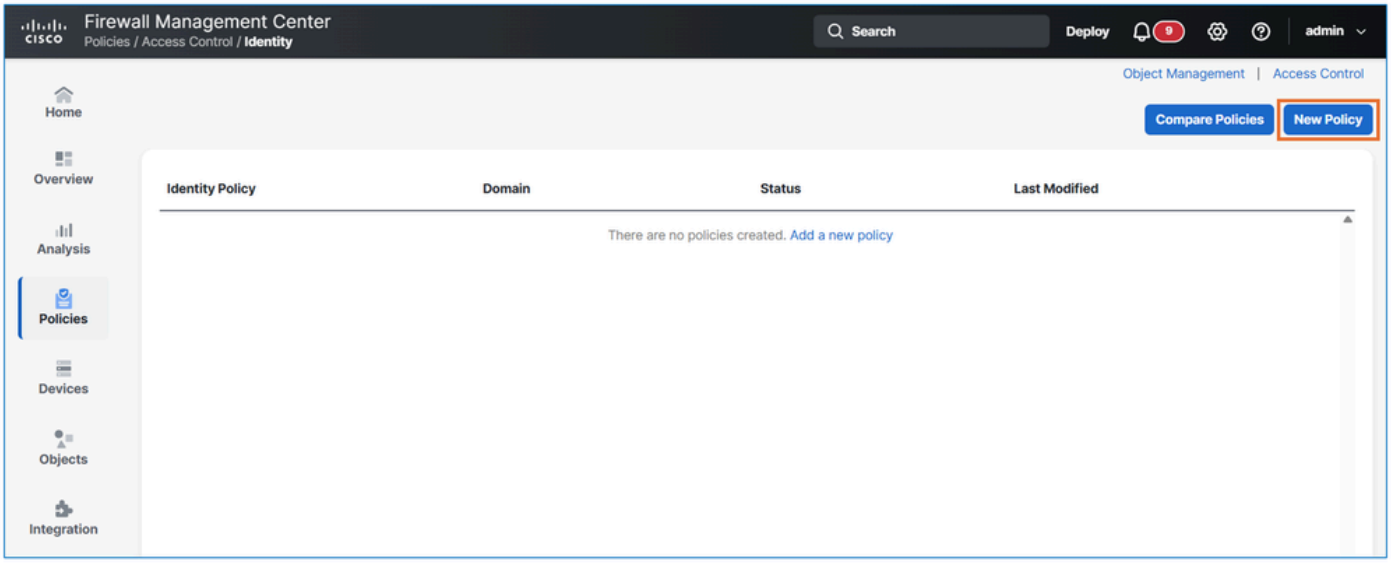
驗證來自fmc的通訊

配置身份策略

根據提供的表建立身份策略。

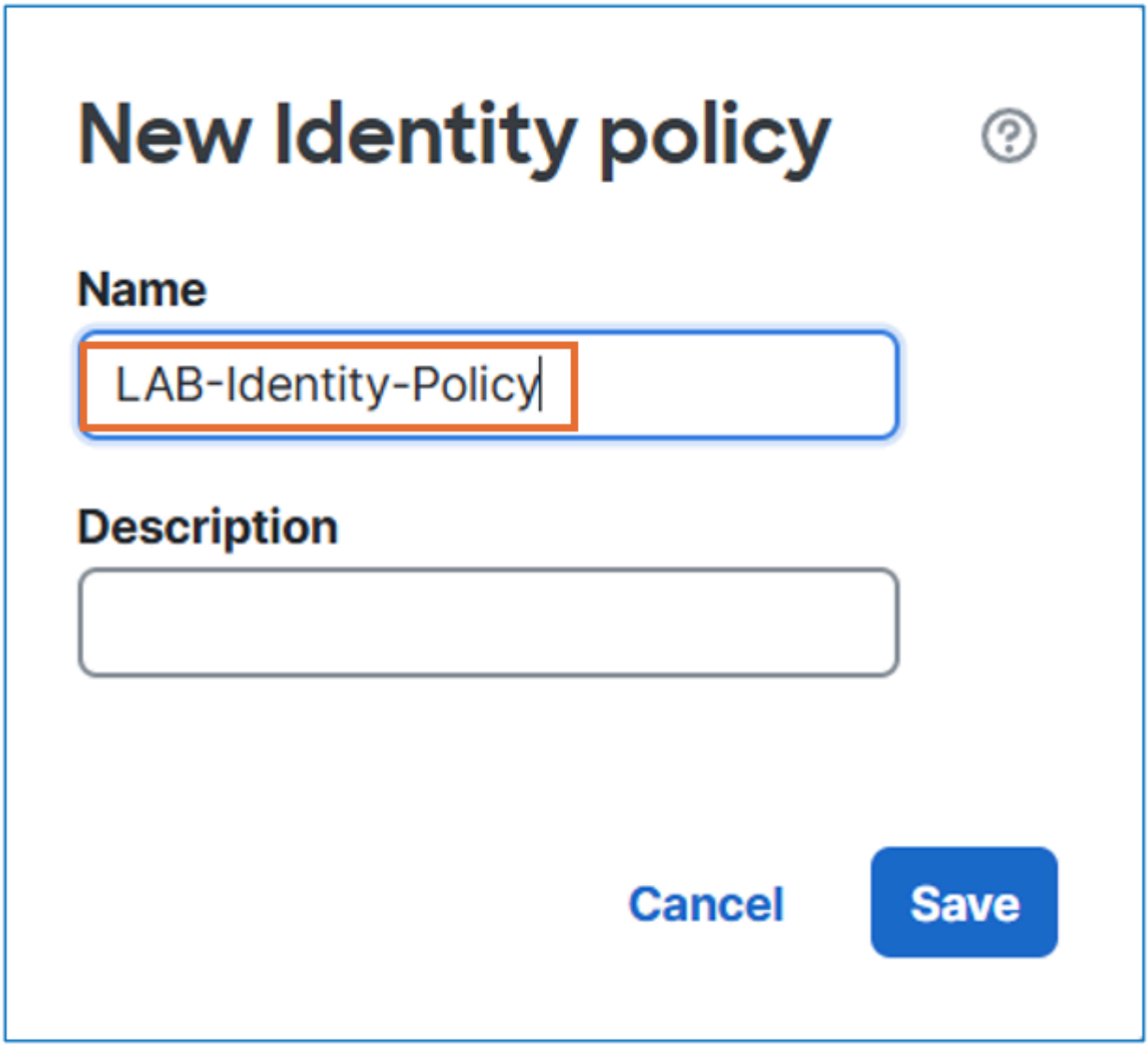
策略名稱	規則名稱	身份驗證領域	剩餘設定
LAB-Identity-Policy	Rule1	實驗室領域	保留為預設值

在FMC UI中，導航至Policies > Access Control > Identity。按一下New Policy按鈕。



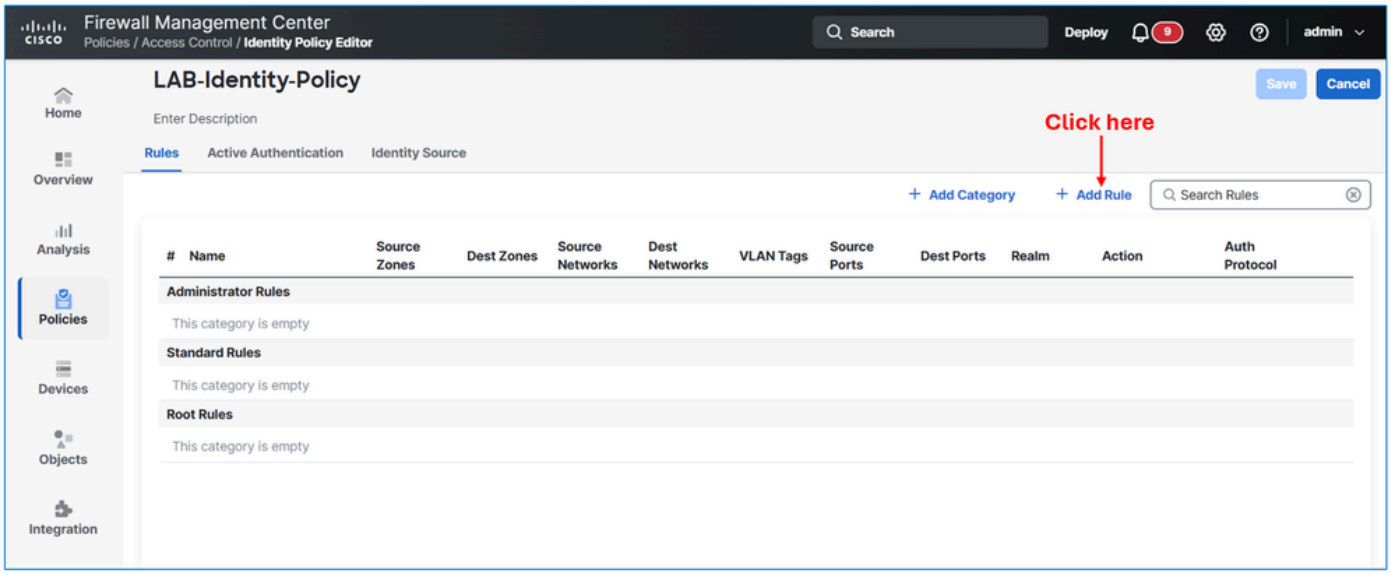
新策略

根據任務要求輸入策略名稱。



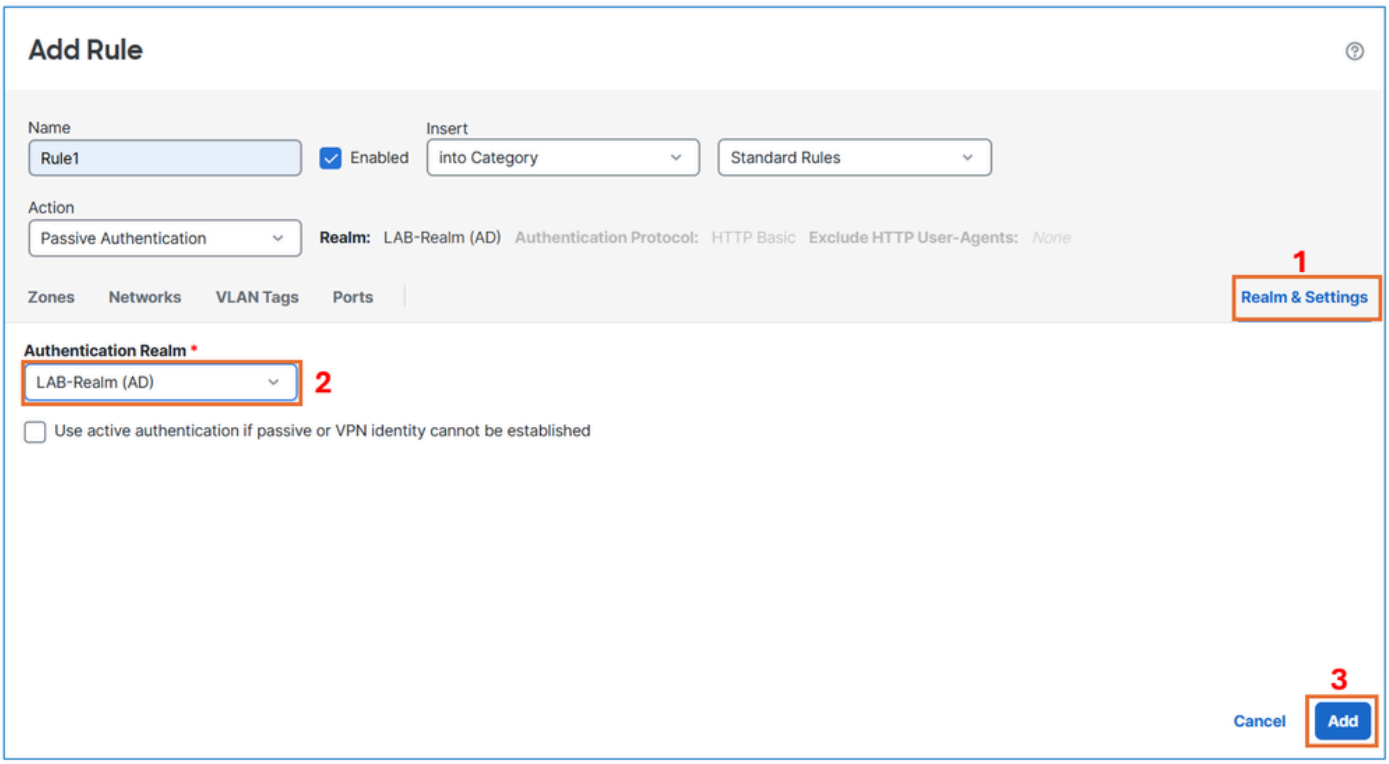
新策略

按一下Add Rule按鈕。



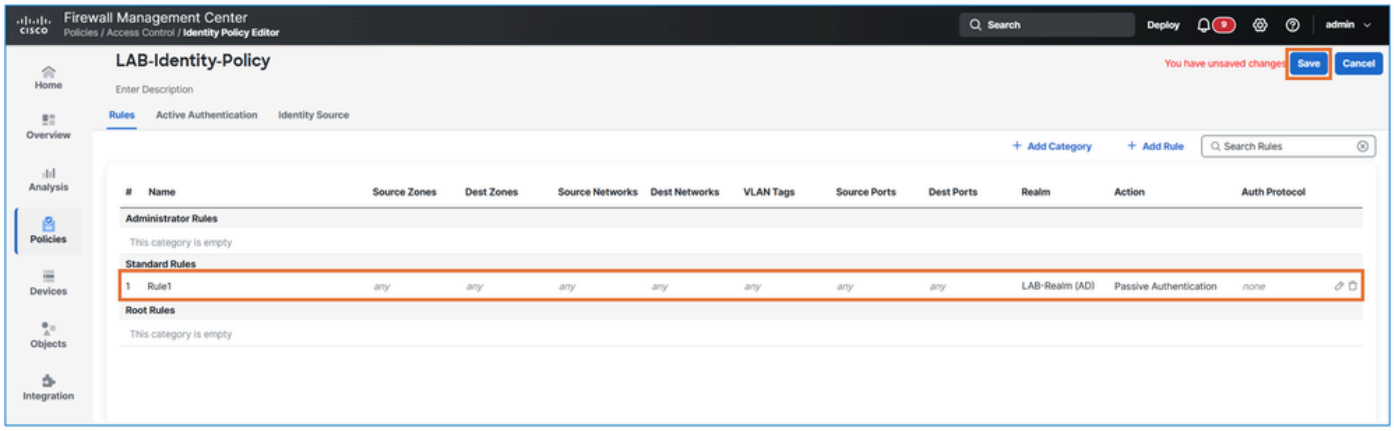
建立規則

導覽至Realm & Settings表，然後根據任務要求選擇Authentication。最後，按一下Addbutton。



領域設定

按一下「儲存」按鈕。



儲存組態

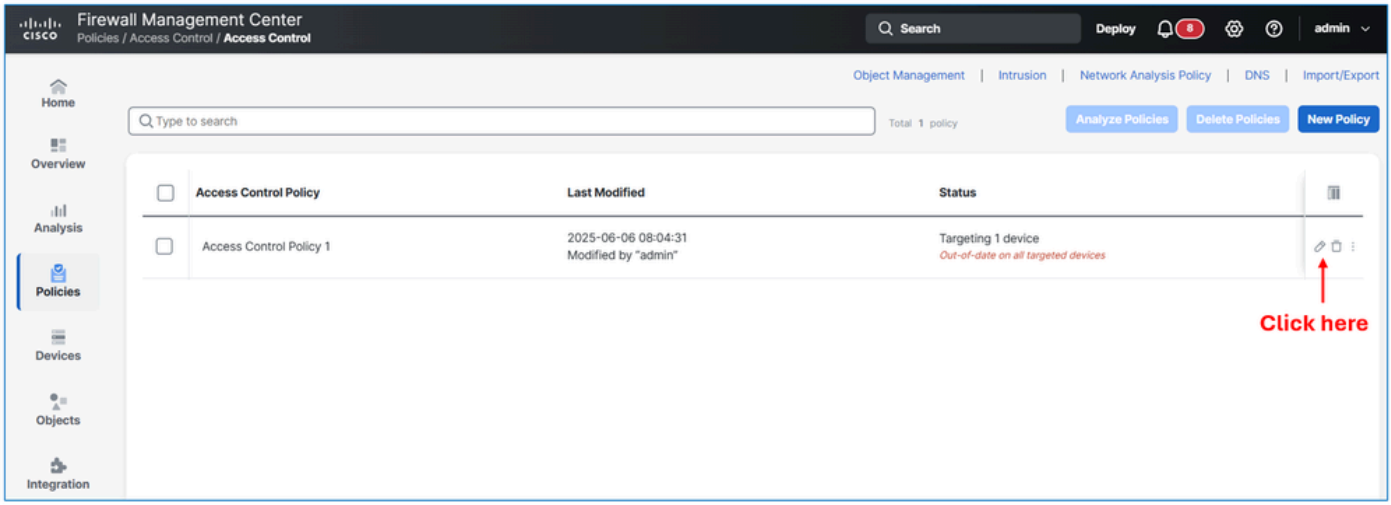
配置訪問控制策略

將身份策略連結到訪問控制策略，並建立具有以下屬性的訪問策略Rule:

屬性名稱	價值
規則名稱	Rule1
動作	允許
源區域	INSIDE
目標區域	OUTSIDE
來源網路	10.10.10.0/24
目的地網路	10.48.62.98/32
服務	目標埠TCP 80(HTTP)
使用者	實驗室領域/組1
日誌記錄	在連線結束時

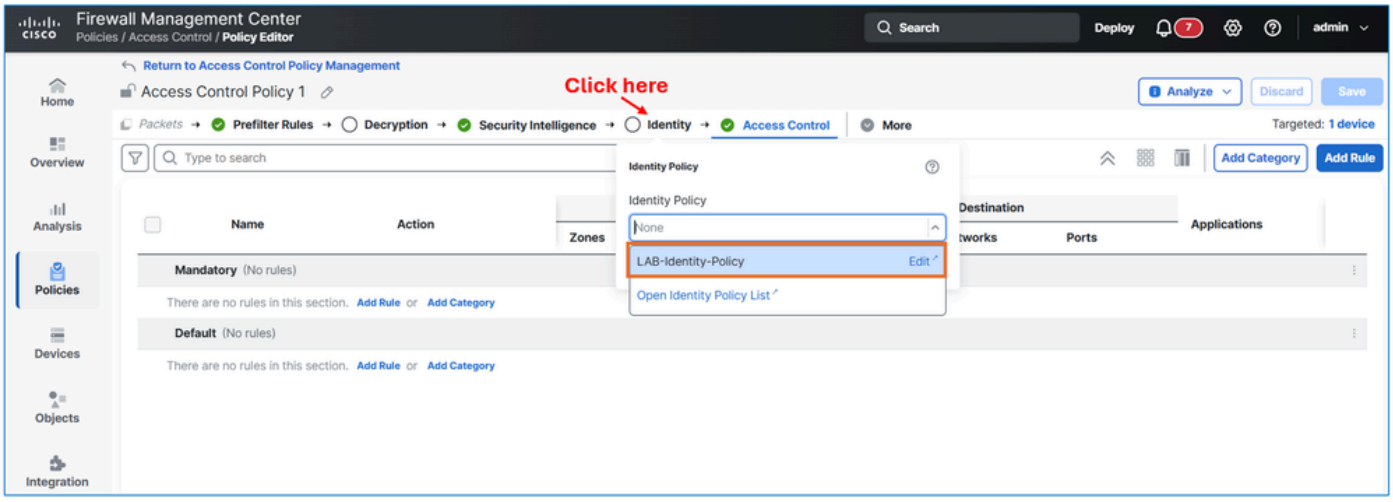
步驟1.將Identity 策略連結到Access Control 策略

在FMC UI中，導航至Policies > Access Control > Access Control。按一下策略的「編輯」按鈕。



編輯策略

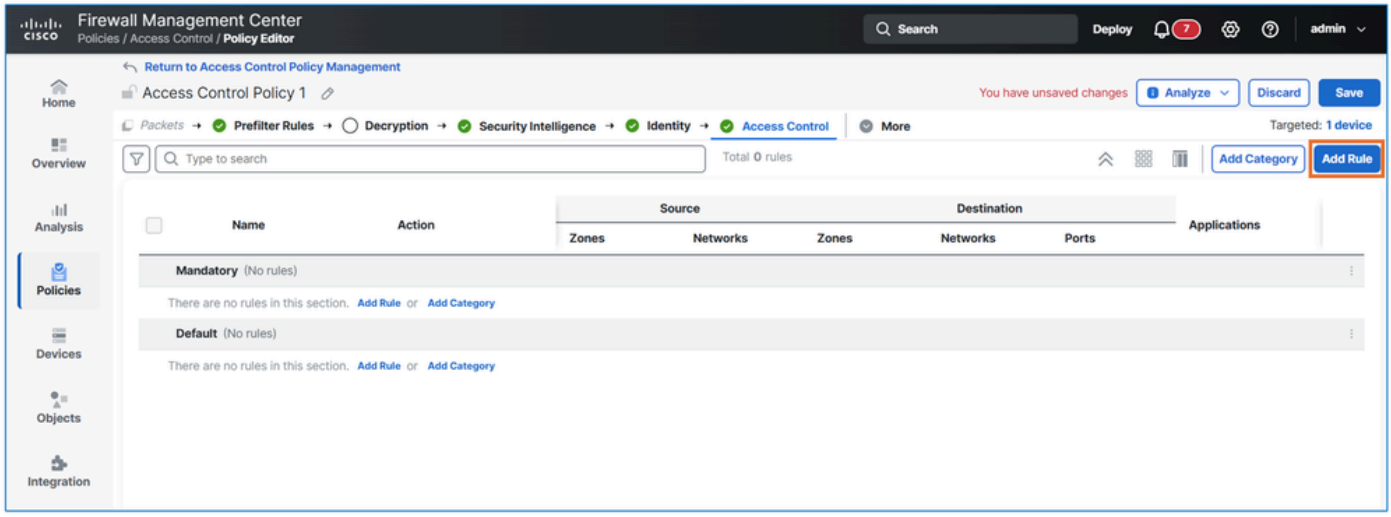
導航到Identitysection並連結在上一個任務中建立的Identity Policy。



新增身份策略

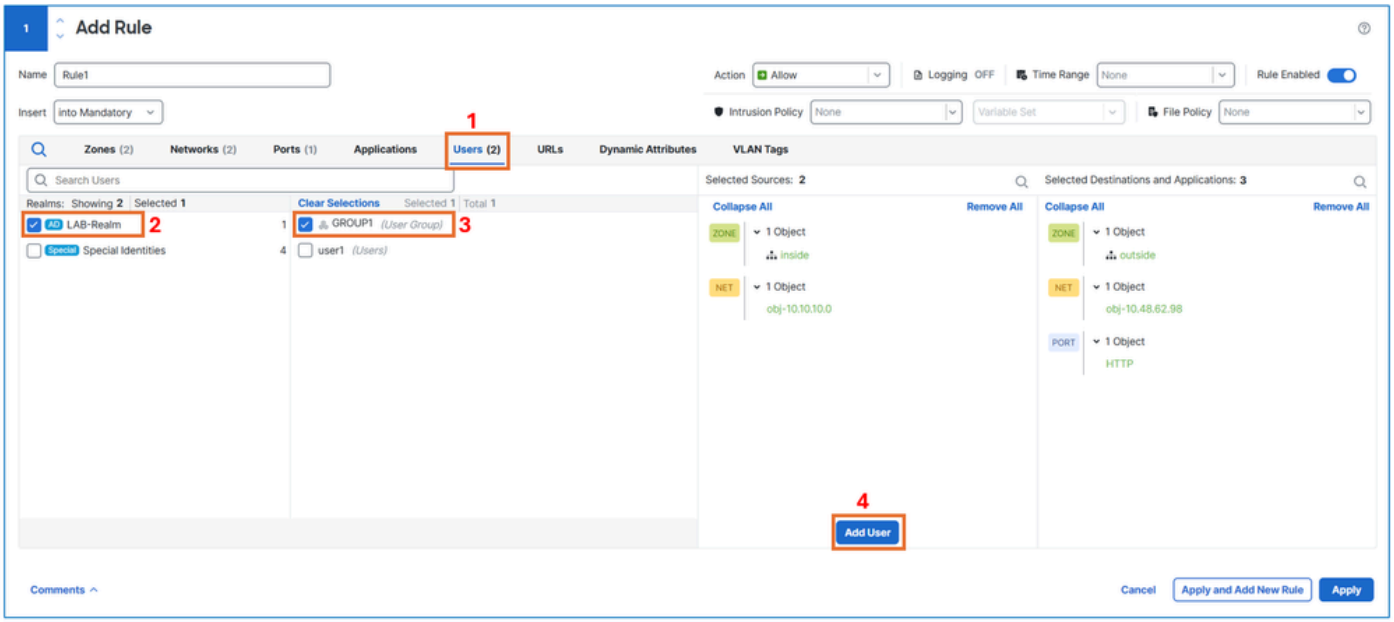
按一下Applybutton

步驟2.建立存取控制規則。



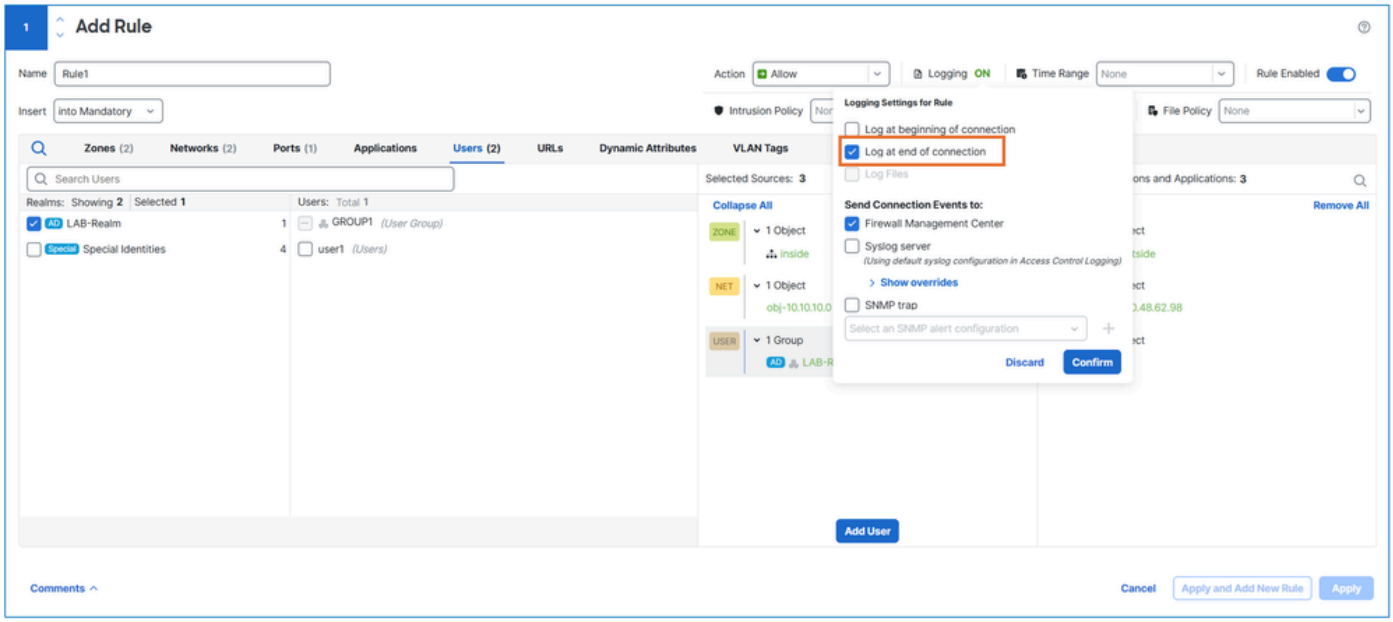
建立ACP

根據任務要求輸入詳細資訊，最重要的是，在Userstab下，從LAB-Realm新增GROUP1。



在規則中新增使用者

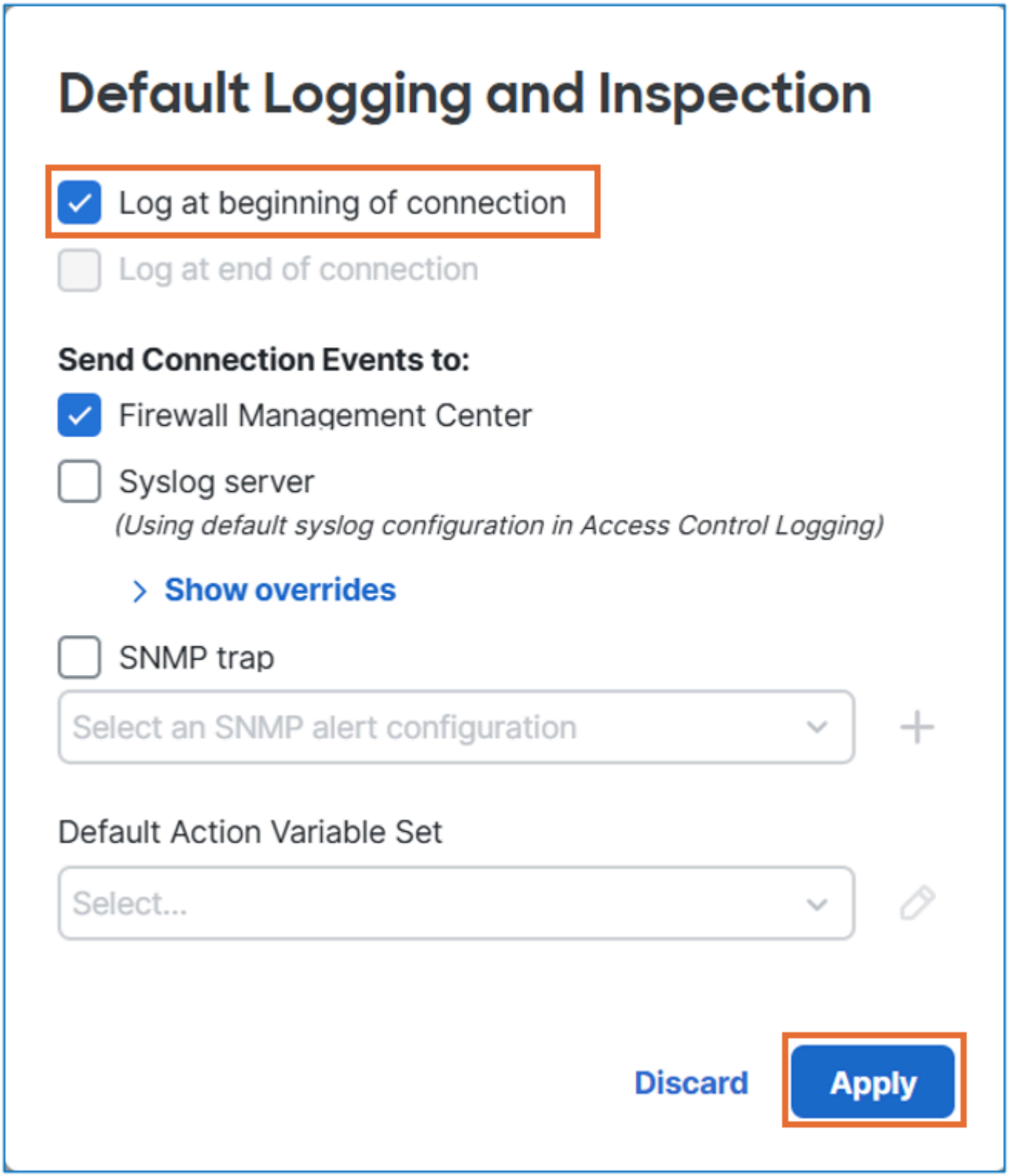
通過在連線結束時選擇Log啟用規則的日誌記錄。



啟用記錄

步驟3.為預設操作啟用logging。

按一下這些設定圖示可修改預設操作日誌設定。



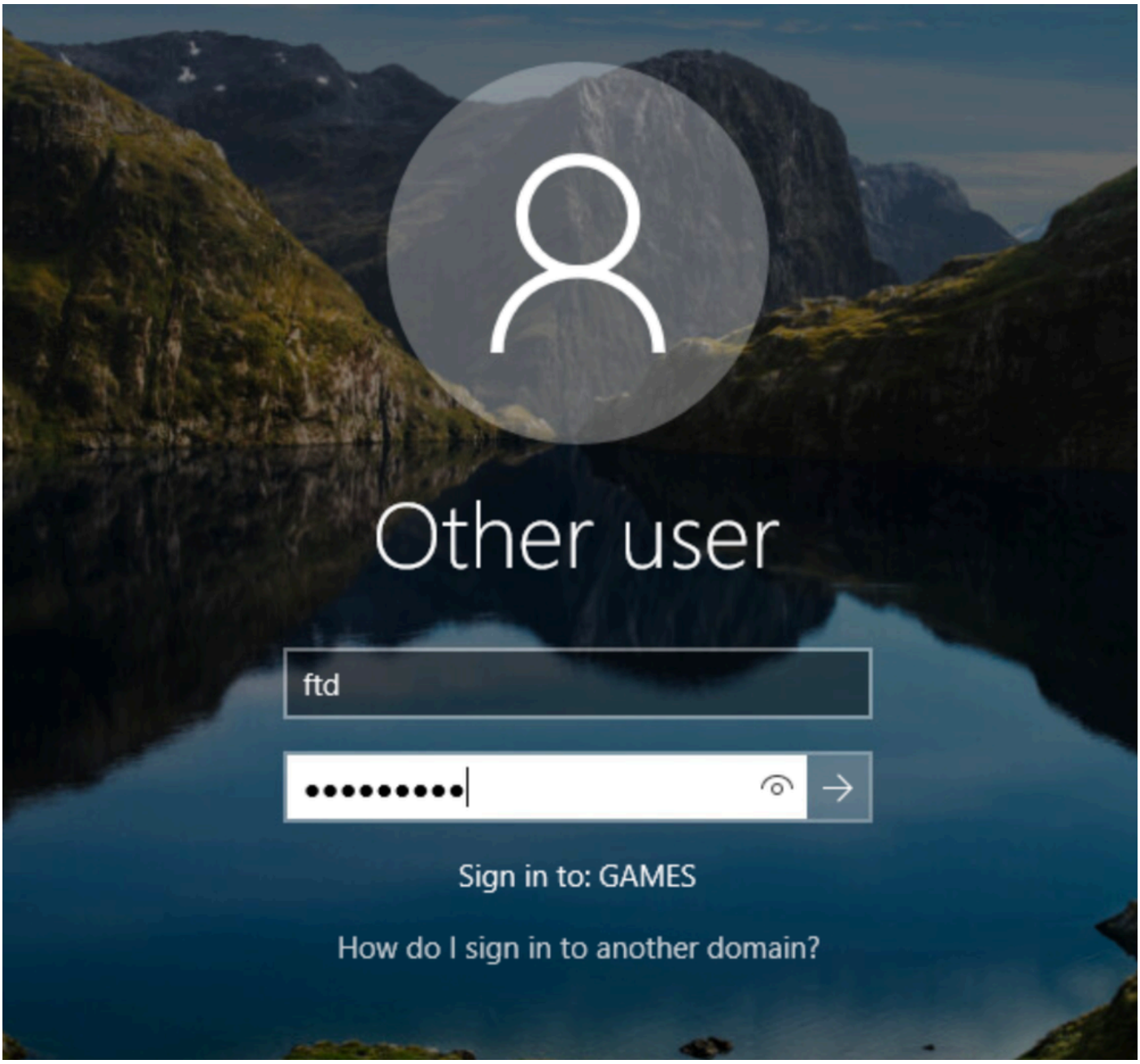
啟用記錄

儲存並部署FTD上的組態。

驗證

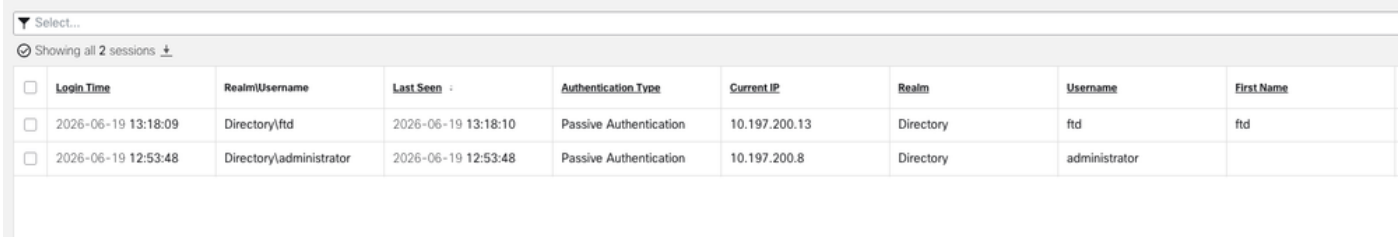
通過確認允許流量專門用於ftd來驗證被動身份操作。

從使用者電腦登入到域使用者。



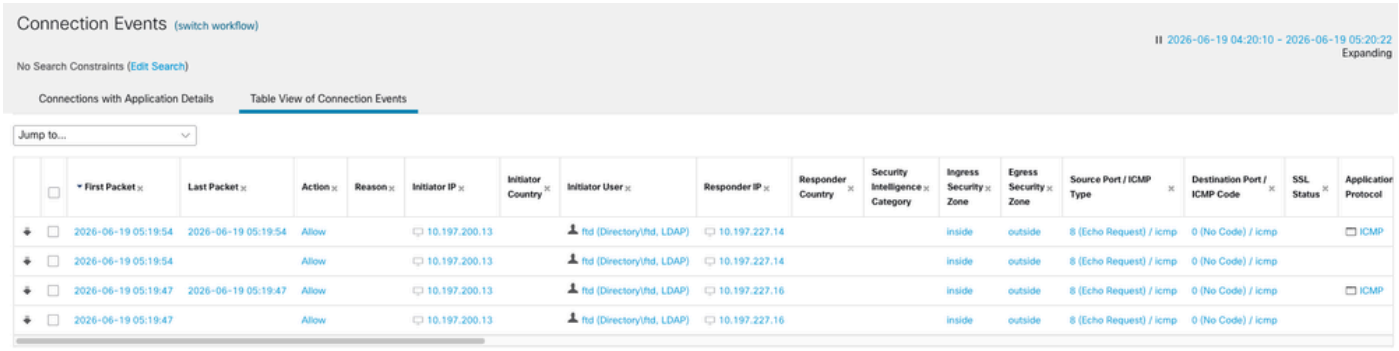
使用者登入

使用者成功登入後，在Analysis> user >active session下從FMC進行驗證，以檢視活動使用者詳細資訊。



活動會話

從連線事件啟動某些流量驗證後，請參閱連線事件中的使用者詳細資訊。

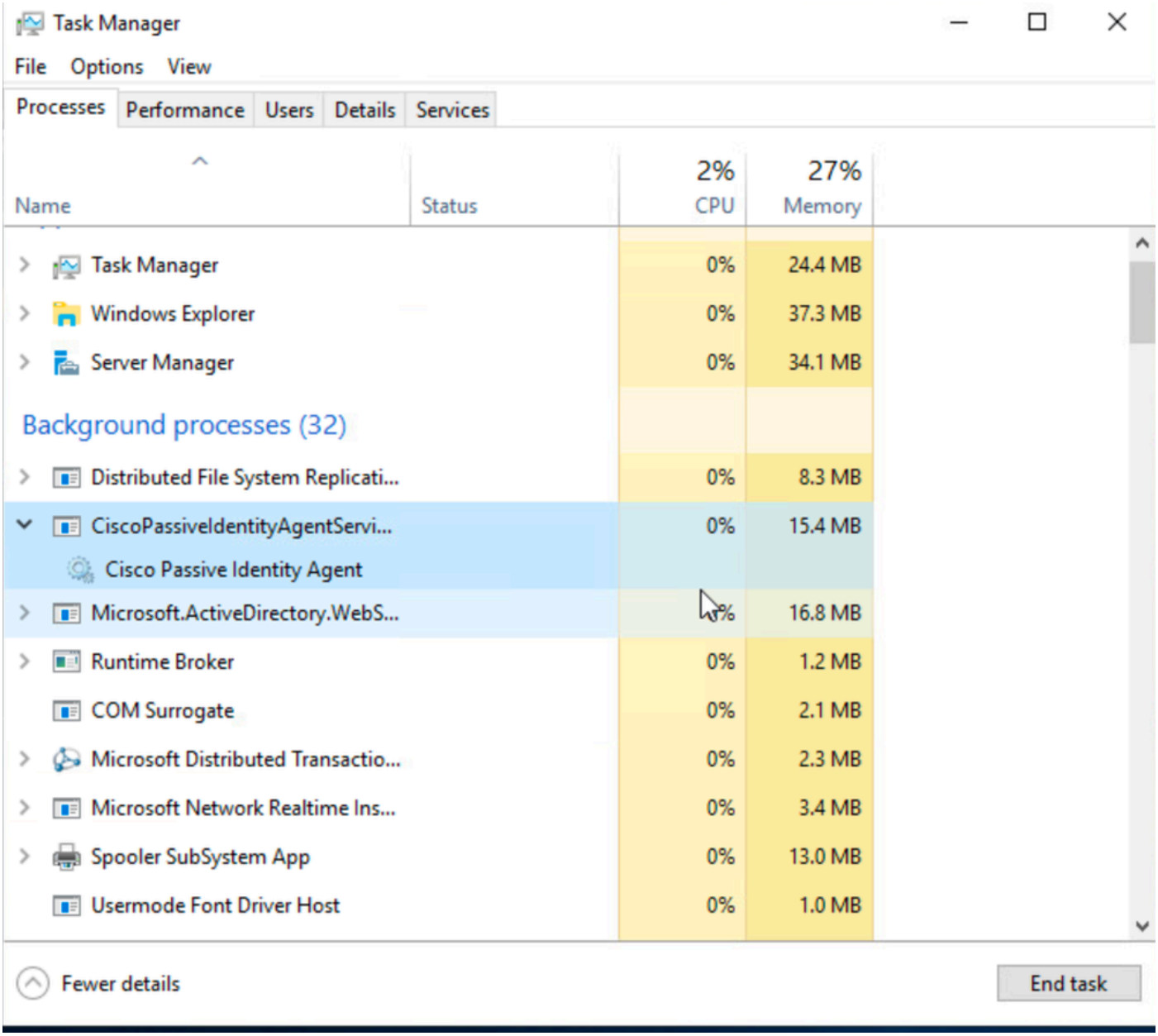


活動會話

疑難排解

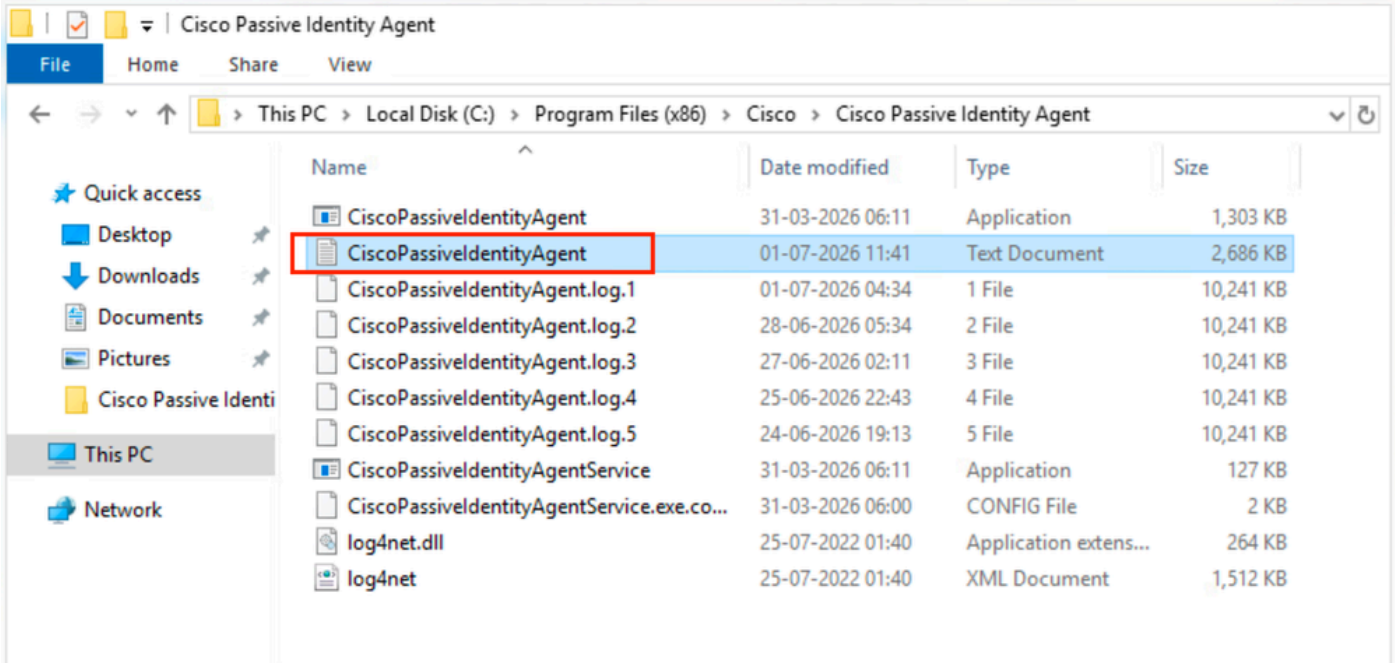
檢查代理日誌

在承載代理的Windows電腦上，開啟任務管理器，並驗證後台進程CiscoPassiveIdentityAgentServiceis是否正在運行。



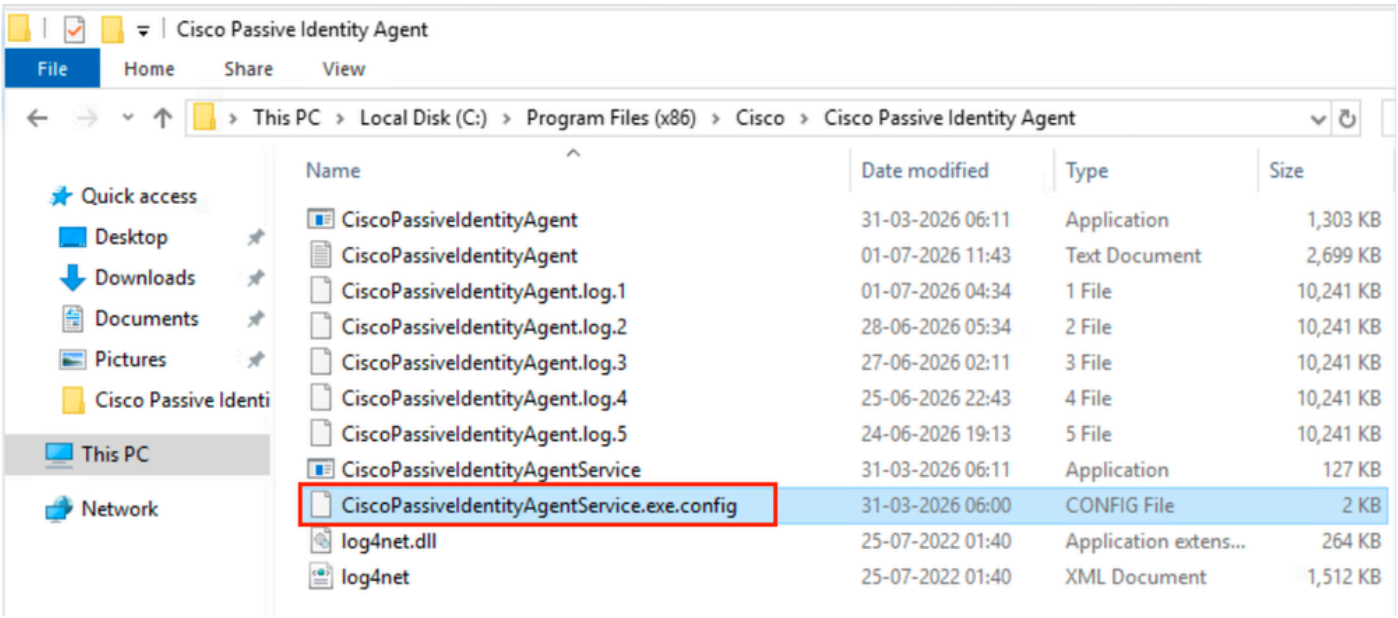
正在運行任務

可以在CiscoPassiveIdentityAgent檔案中找到代理日誌，預設位置為："C:\Program Files(x86)\Cisco\Cisco Passive Identity Agent\"。



代理

預設情況下，代理日誌設定為INFOlevel。要啟用DEBUG級別日誌記錄，請修改CiscoPassiveIdentityAgentService.exe.configfile並將日誌記錄級別設置為ALL或DEBUG。



代理配置

資訊日誌

檢查代理日誌 — 獲取代理配置。

INFO Rest客戶端，批次事件：[f"domain":"games.cisco.com", "srcIpAddress":"X.X.X.X", "使用者":"fdm","timestamp":「2026-07-01T19

INFO Rest客戶端，對映狀態：確定

INFO Rest客戶端，使用者Batch fdm的REST發佈成功，延遲= 0，當前DC時間(UTC):07/01/2026 19:47:34登入使用者

INFO Rest客戶端，請求代理配置

FMC日誌

運行此命令，檢視是否已從代理接收到使用者到IP的對映。

```
root@firepower123:/var/sf/user_enforcement# user_map_query.pl -u fdm

Current Time: 07/01/2026 11:36:03 UTC

Getting information on username(s)...


___
User #1: fdm
---

  ID:         10
  Last Seen:  Unknown
  for_policy: 1

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

No IP Addresses


##) Group Name (ID)
 1) Domain Users (18)
 2) Users (48)
root@firepower123:/var/sf/user_enforcement#
```

fmc輸出

如果上述命令未顯示任何對應，請收集這些日誌並與Cisco TAC聯絡。

這是FMC API的相關日誌清單。豬尾日誌包含所有這些資訊。

- /var/log/auth-daemon.log
- /var/log/messages
- /var/log/process_stdout.log
- /var/log/process_stderr.log

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）。