使用Configuration.zip檔案通過FMT將FDM遷移到FMC

目錄

簡介

本文說明如何使用FMT生成要遷移到FMC的安全防火牆裝置管理器(FDM)的配置檔案.zip。

必要條件

需求

思科建議您瞭解以下主題：

- 思科防火牆威脅防禦(FTD)
- 思科防火牆管理中心(FMC)
- 防火牆移轉工具(FMT)
- Postman API平台

採用元件

本檔案中的資訊是根據以下軟體版本。

FTD 7.4.2

FMC 7.4.2

FMT 7.7.0.1

Postman 11.50.0

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

- FDM現在可以通過不同方式遷移到FMC。在本檔案中，將要探索的情形是使用API請求生成配置.zip檔案，然後將該檔案上傳到FMT以將配置遷移到FMC。
- 本文檔中顯示的步驟直接開始使用Postman，因此建議您先安裝Postman。要使用的PC或筆記型電腦必須能夠訪問FDM和FMC，還必須安裝和運行FMT。

注意事項

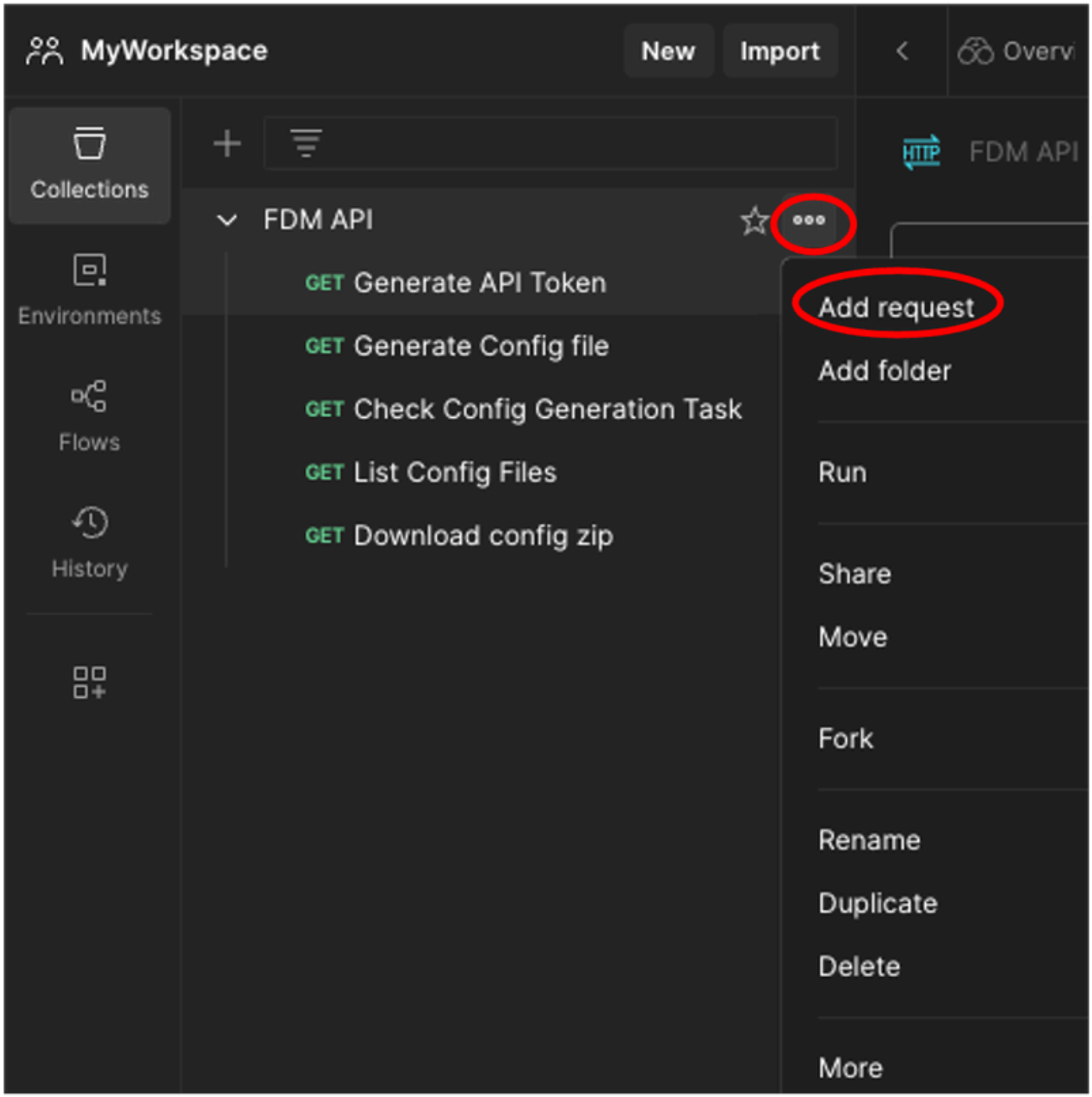
- 本文檔重點介紹配置.zip檔案的生成，而不是在FMT中使用。
- 使用配置.zip檔案的FDM遷移用於非即時遷移，無需立即將目標FTD作為目標。

警告：選擇此模式，僅允許遷移訪問控制策略(ACP)、網路地址轉換策略(NAT)和對象。對於要遷移的ACP規則或NAT中必須使用的對象，否則將忽略這些對象。

組態

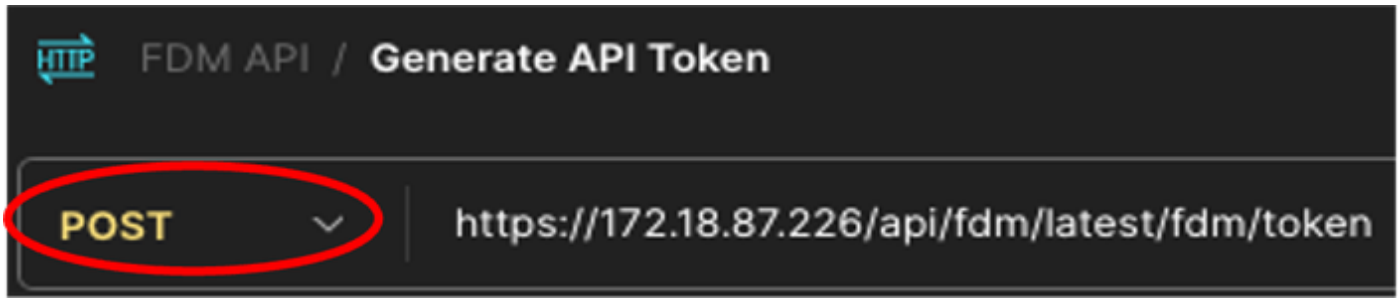
API請求 — Postman

1. 在Postman中，建立新的集合（在此情況下使用FDM API）。
2. 按一下3個點，然後按一下Add request。



Postman — 集合建立和請求新增

3. 呼叫此新請求：生成API令牌。它將作為GET請求建立，但在執行此請求時，必須從下拉選單中選擇POST。在POST旁邊的文本框中，引入下一行https://<FDM IP ADD>/api/fdm/latest/fdm/token



Postman — 令牌請求

4.在正文頁籤中，選擇raw選項，然後引入憑據以使用此格式訪問FTD(FDM)裝置。

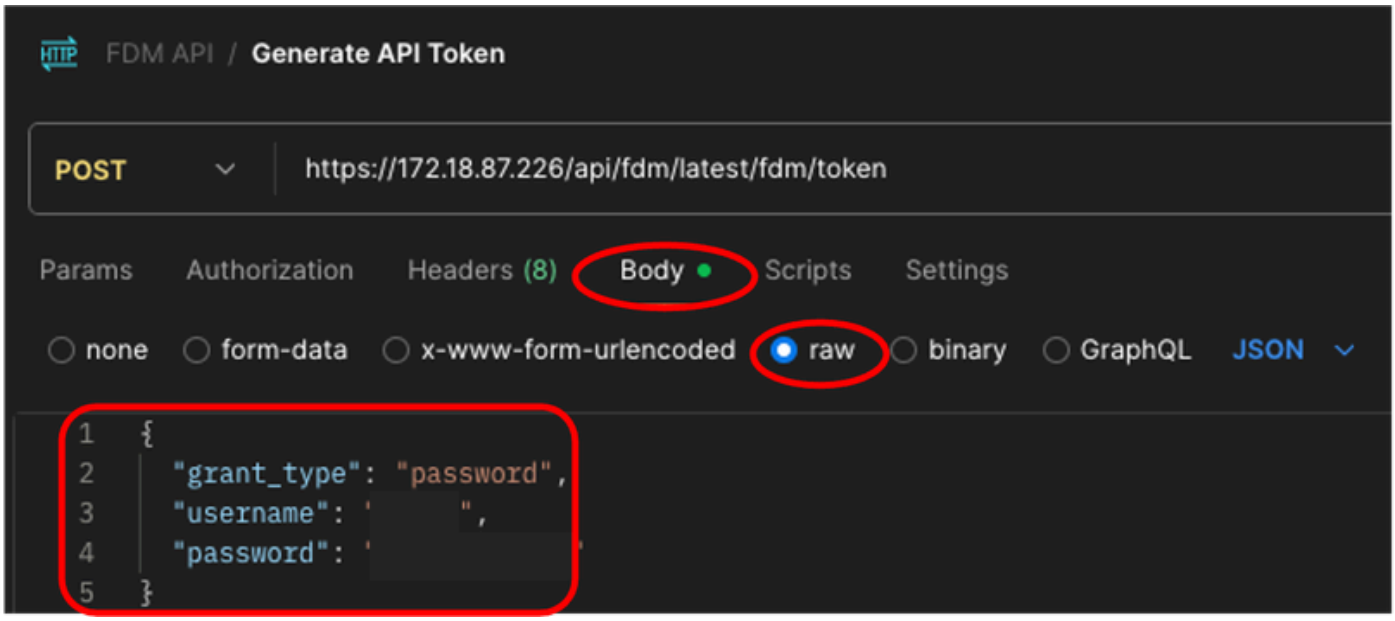
{

"grant_type":"密碼",

"使用者名稱":"使用者名稱",

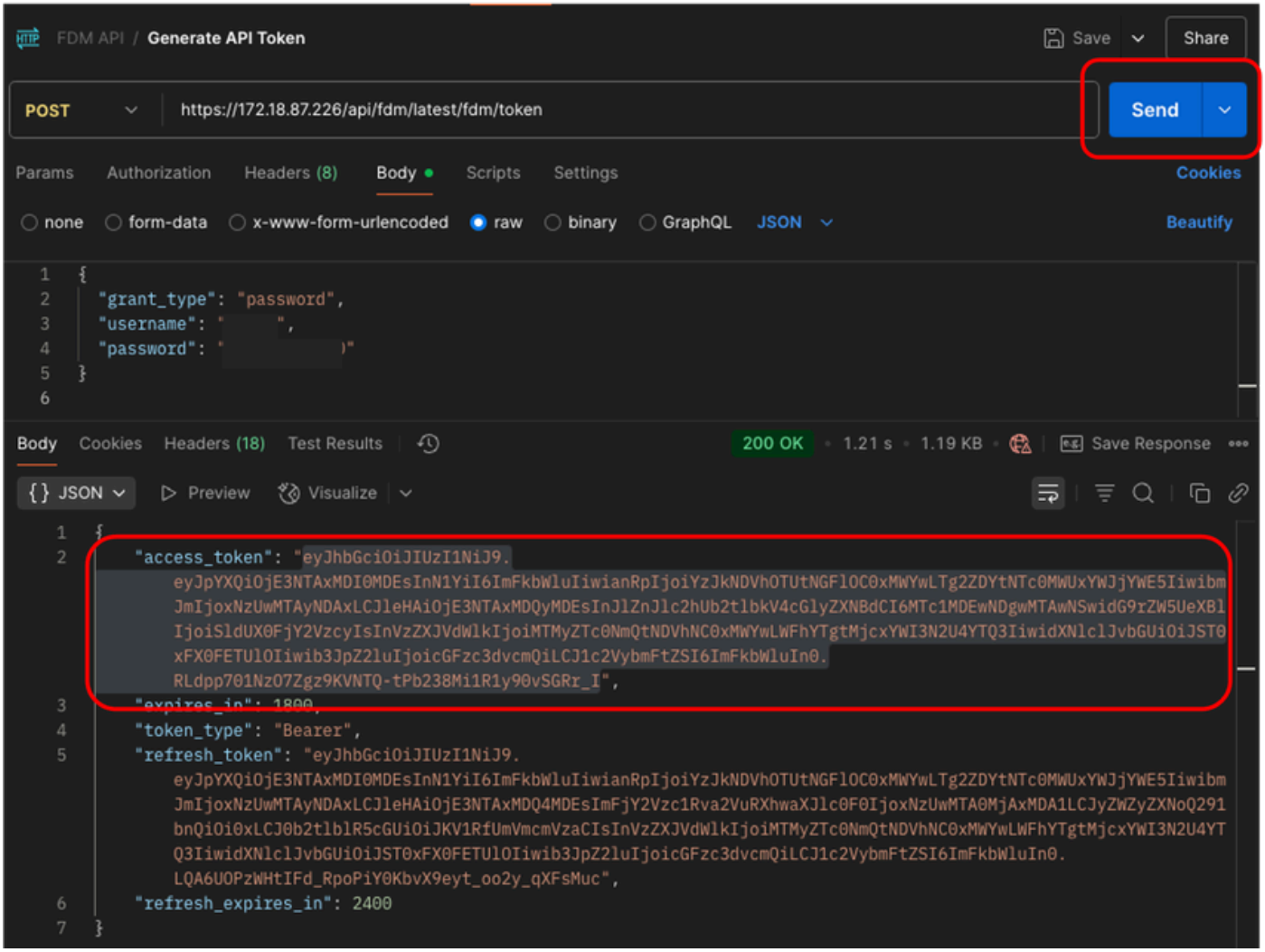
"密碼":"密碼"

}



Postman — 令牌請求正文

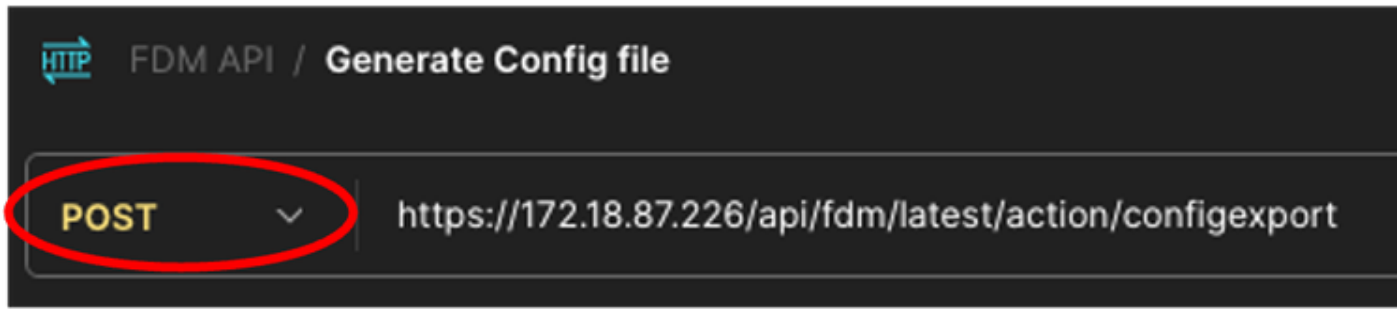
5.最後，按一下Send獲取您的訪問令牌。如果一切正常，您會收到200 OK響應。複製整個令牌（在雙引號內），因為稍後將使用該令牌。



Postman — 已成功生成令牌

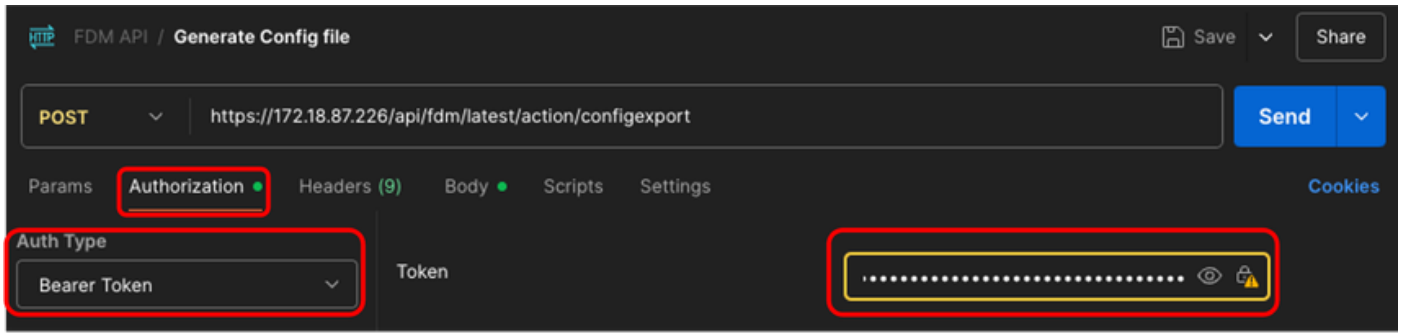
6.重複步驟2，建立新的請求,POST將再次使用。

7.呼叫此新請求：生成配置檔案。它將作為GET請求建立，但在執行此請求時，必須從下拉選單中選擇POST。在POST旁邊的文本框中，引入下一行https://<FDM IP ADD>/api/fdm/latest/action/configexport



Postman — 生成配置檔案請求

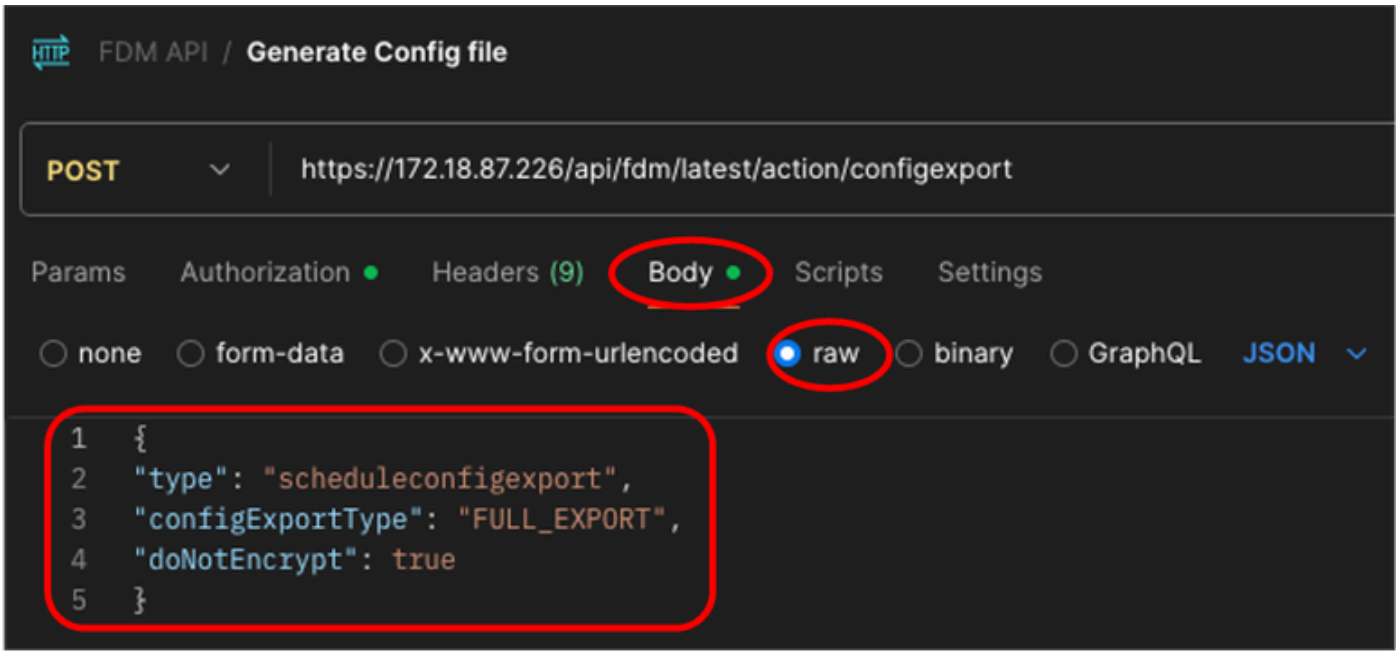
8.在Authorization 頁籤中，從下拉選單中選擇Bearer Token作為Auth Type，然後在Token旁邊的文本框中貼上步驟5中複製的令牌。



Postman — 生成配置檔案請求 — 授權

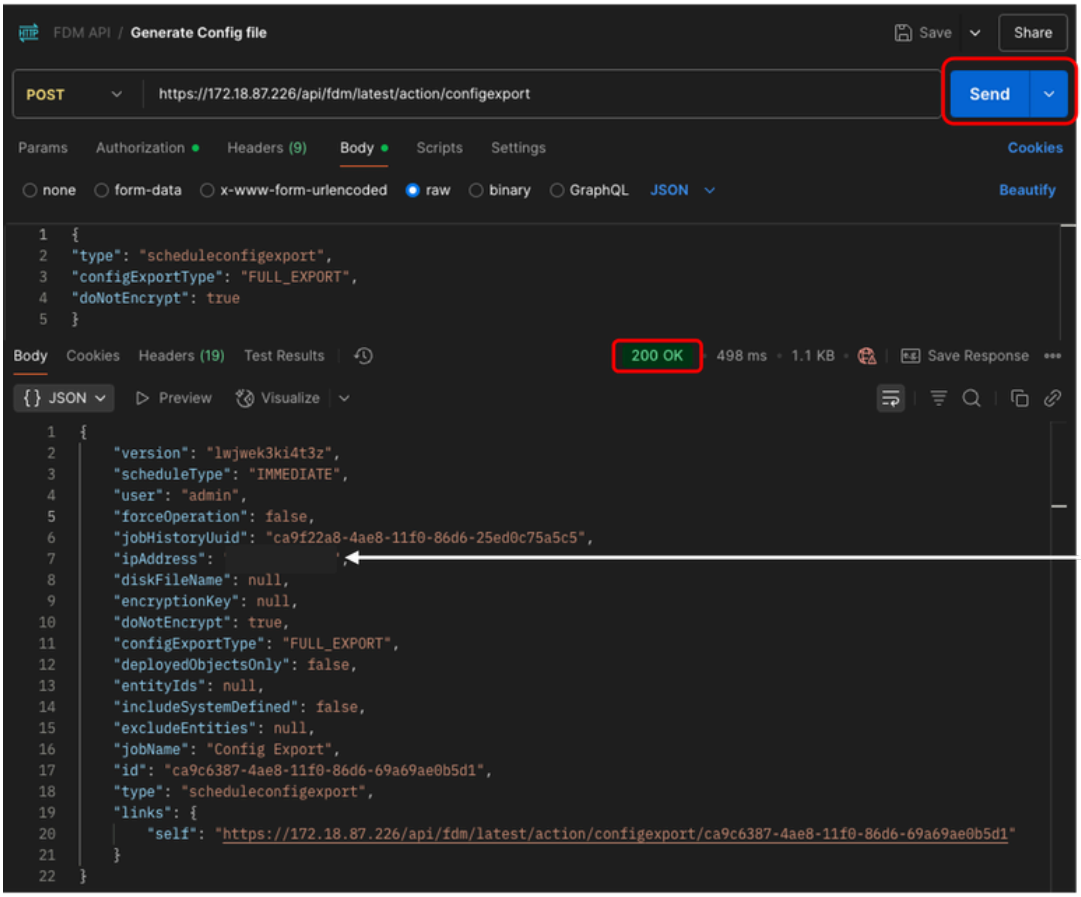
9.在正文頁籤中，選擇raw選項並引入此資訊。

```
{
  "型別":"scheduleconfigexport",
  "configExportType":"FULL_EXPORT",
  "DoNotEncrypt":true
}
```



Postman — 生成配置檔案請求 — 正文

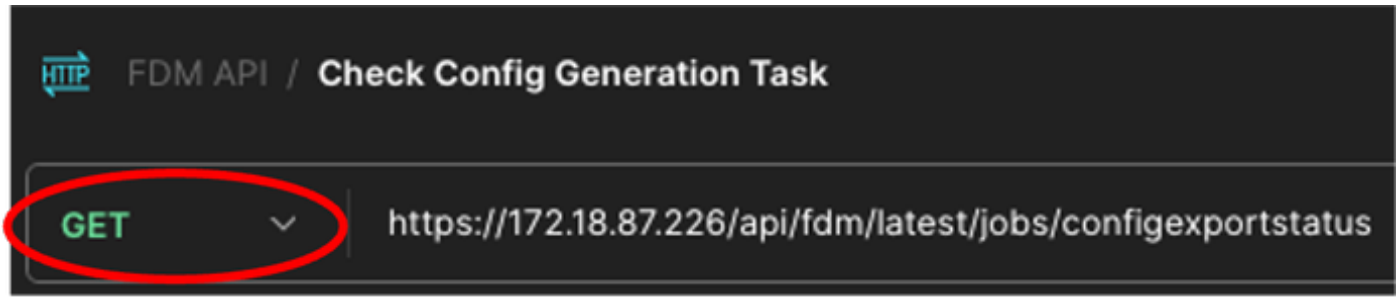
10.最後，按一下Send。如果一切正常，您會收到200 OK響應。



Postman — 生成配置檔案請求 — 輸出

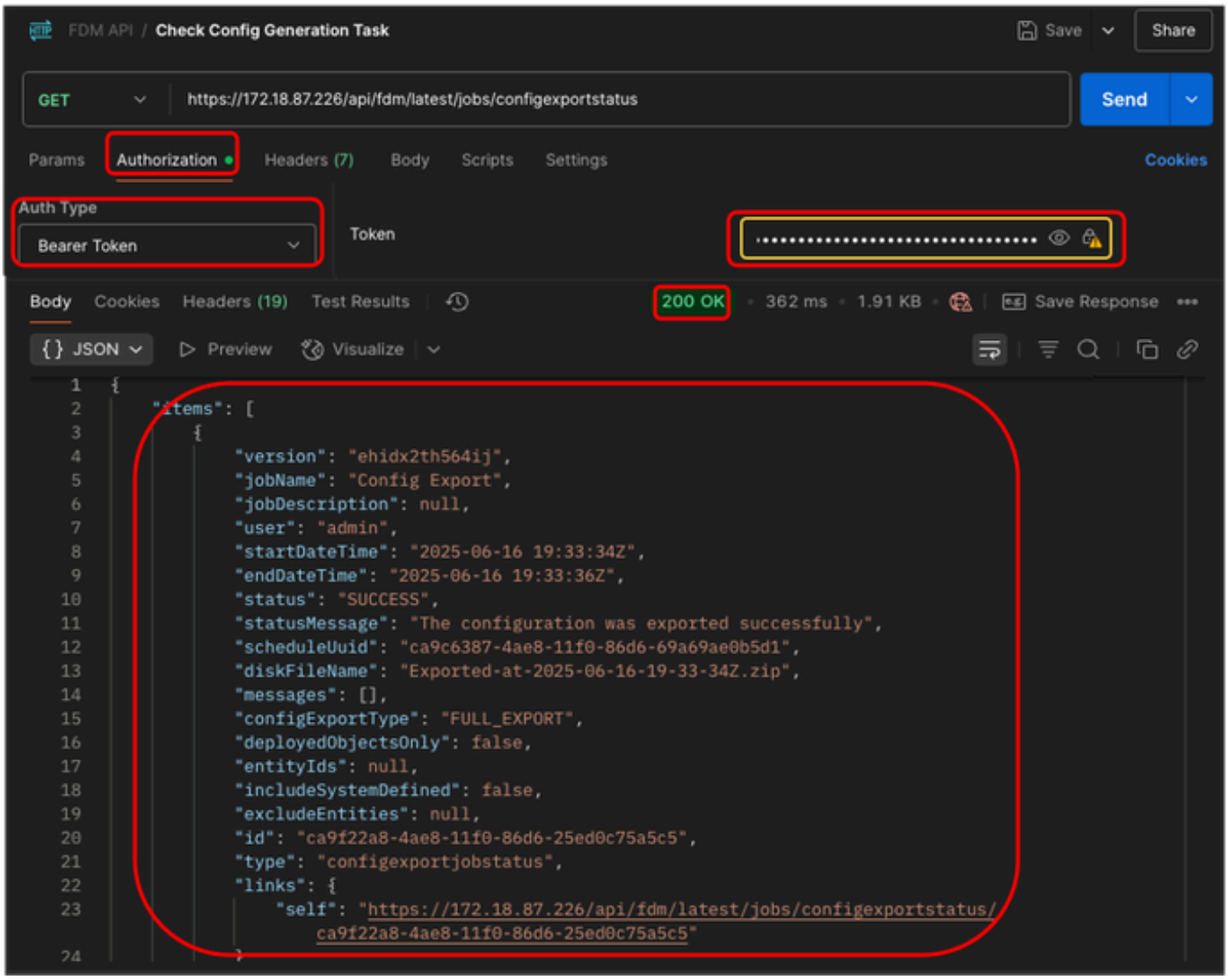
11.重複步驟2，建立新的請求。這次將使用GET。

12.將這項新請求稱為：檢查配置生成任務。它將作為GET請求創建。此外，執行此命令時，必須從下拉選單中選擇GET。在GET旁邊的文本框中，引入下一行https://<FDM IP ADD>/api/fdm/latest/jobs/configexportstatus



Postman — 檢查配置匯出狀態請求

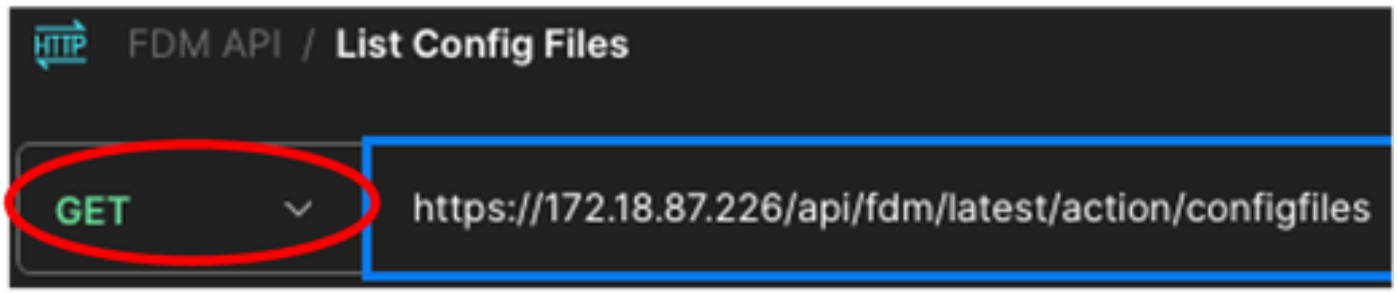
13.在Authorization頁籤中，從下拉選單中選擇Bearer Token作為Auth Type，然後在Token旁邊的文本框中貼上步驟5中複製的token。最後，按一下Send。如果一切正常，您會收到200 OK響應，在JSON欄位中可以看到任務狀態和其他詳細資訊。



Postman — 配置匯出狀態請求 — 授權和輸出

14.重複步驟2，建立新的請求，這次將使用GET。

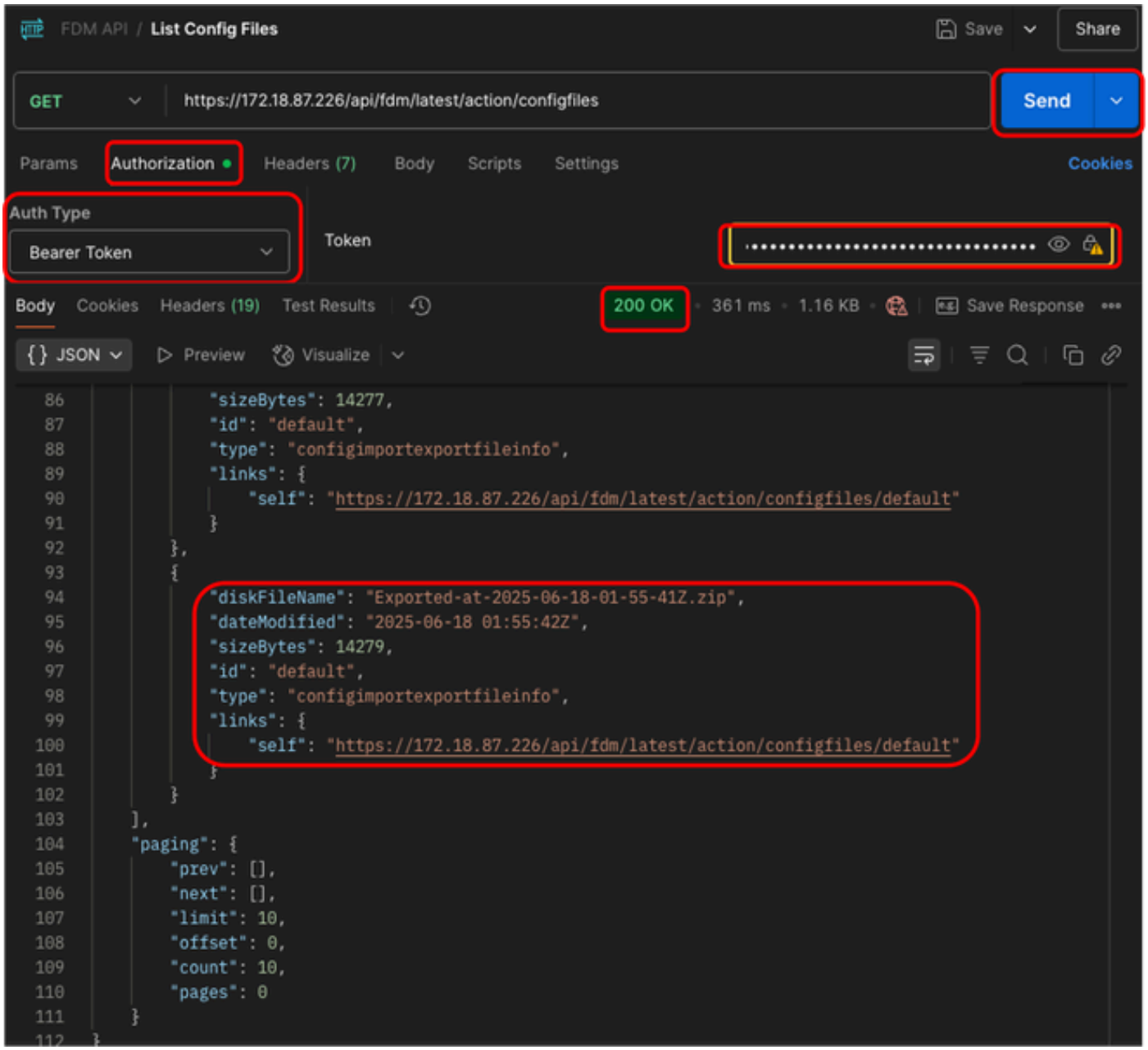
15.給此新請求打電話：列出配置檔案。它將建立為GET請求，而且在執行此請求時，必須從下拉選單中選擇GET。在GET旁邊的文本框中，引入下一行https://<FDM IP ADD>/api/fdm/latest/action/configfiles



Postman — 列出匯出的配置檔案請求

16.在Authorization頁籤中，從下拉選單中選擇Bearer Token作為Auth Type，然後在Token旁邊的文本框中貼上步驟5中複製的token。最後，按一下Send。如果一切正常，您會收到200 OK響應，並在JSON欄位中顯示匯出檔案的清單。最新的版本列在底部。複製最新檔名（檔名中較新的日

期），因為該檔案將在最後一步中使用。



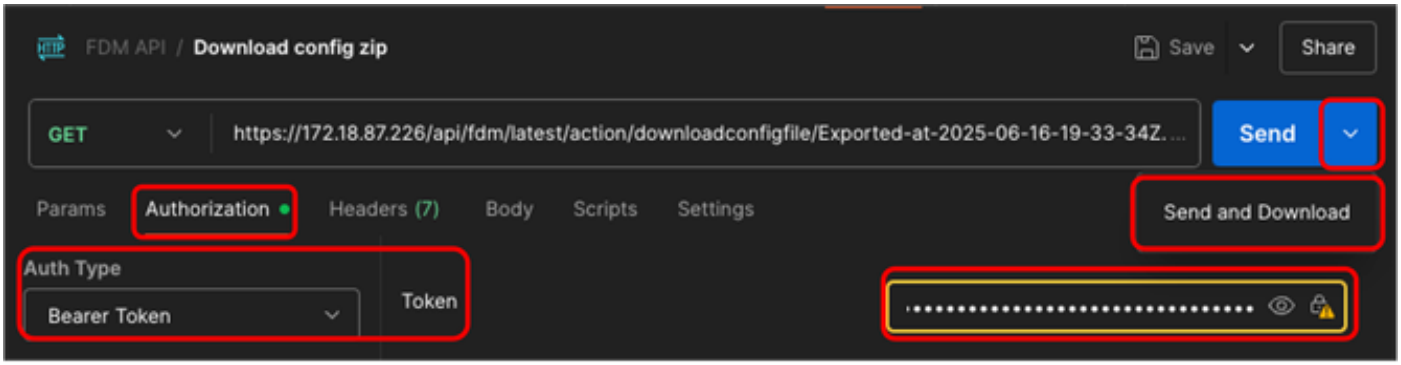
Postman — 列出匯出的配置檔案請求 — 授權和輸出

17.重複步驟2，建立新的請求，這次將使用GET。

18.將這項新請求稱為：Download config zip.它將建立為GET請求，而且在執行此請求時，必須從下拉選單中選擇GET。在GET旁邊的文本框中，介紹下一行，在末尾貼上您在第16步複製的檔名。
https://<FDM IP ADD>/api/fdm/latest/action/downloadconfigfile/<Exported_File_name.zip >

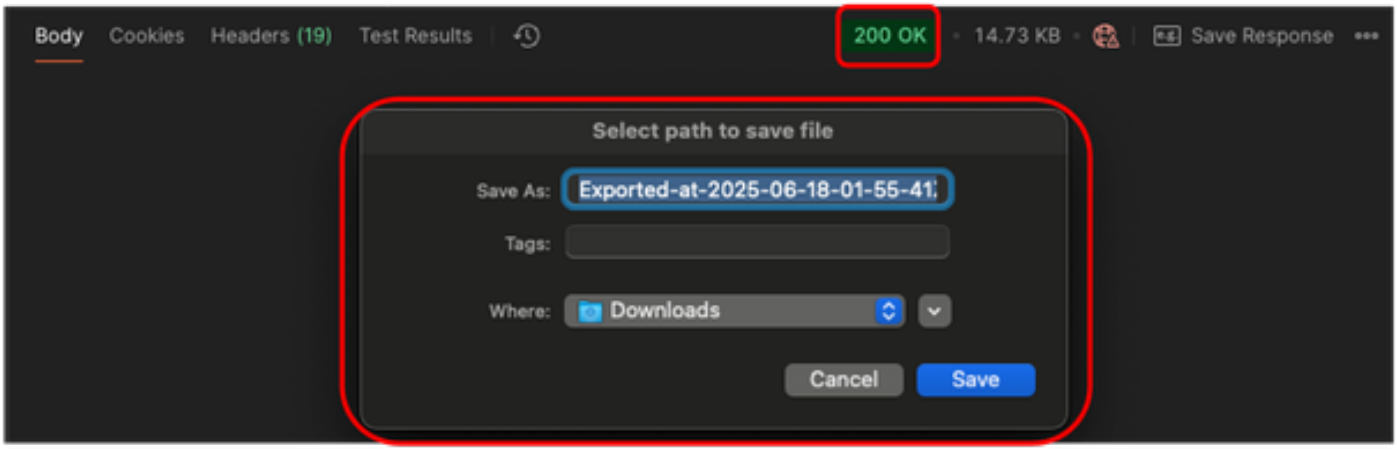
Postman — 下載Config.zip檔案要求

19.在「授權」選項卡，從下拉選單中選擇Bearer Token作為Auth Type，然後在「令牌」旁邊的文本框中貼上步驟5中複製的令牌。最後，按一下「傳送」旁邊的向下箭頭並選擇Send and Download。



Postman — 下載Config.zip檔案請求 — 授權

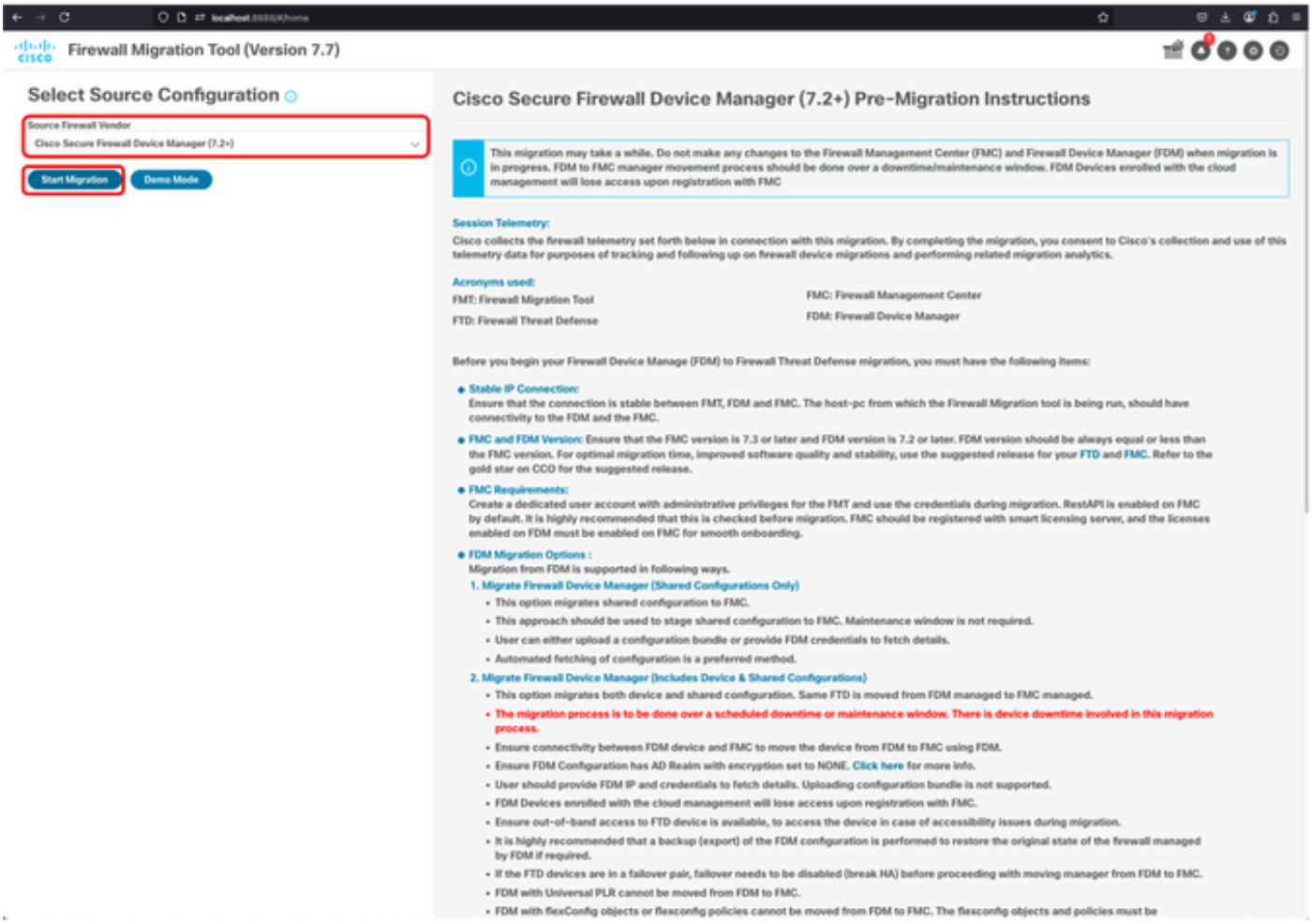
20.如果一切正常，您會收到200 OK響應，並且會顯示一個彈出視窗，詢問要儲存configuration.zip檔案的目標資料夾。現在可以將此.zip檔案上傳到防火牆遷移工具。



Postman — 下載Config.zip檔案要求 — 儲存

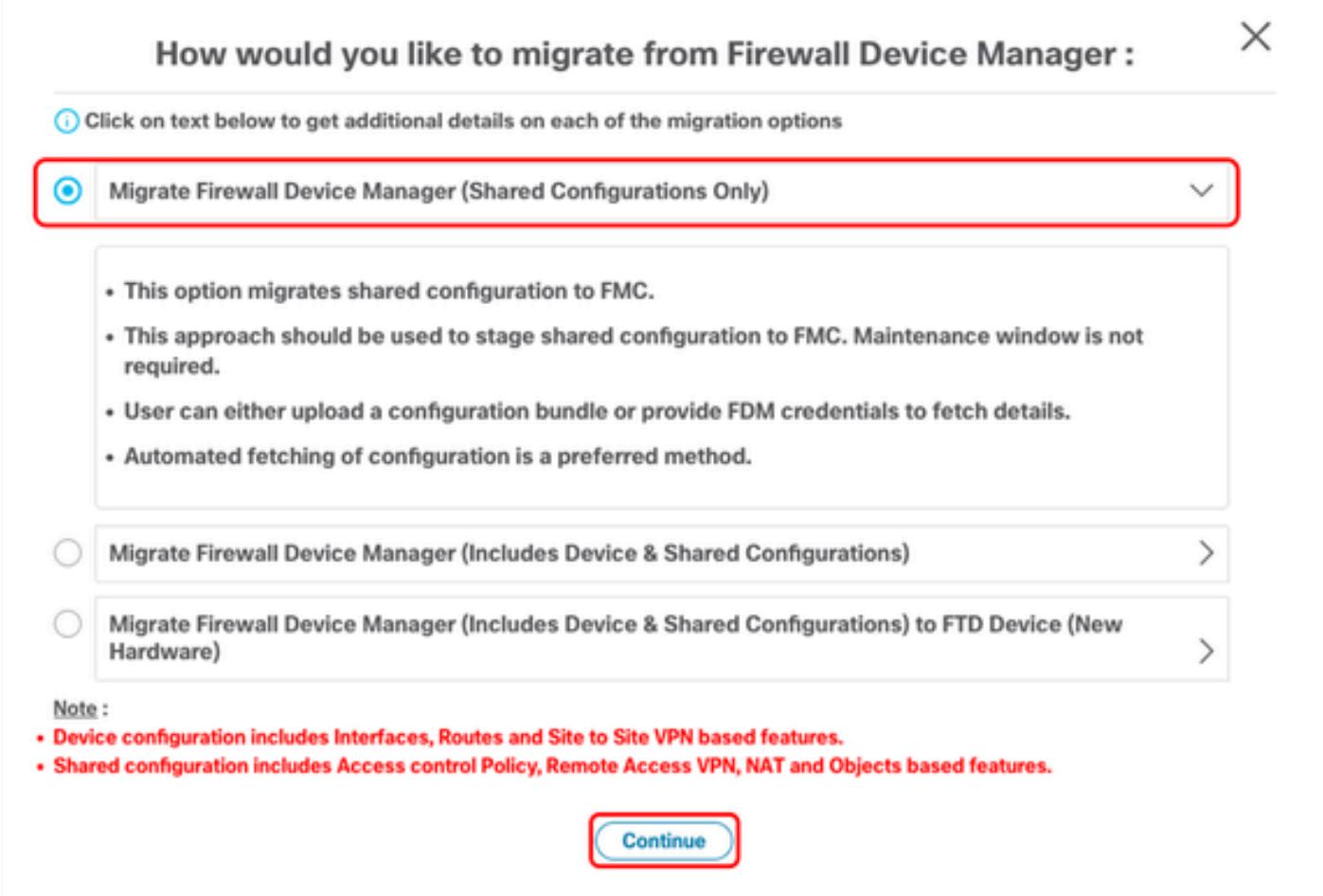
防火牆移轉工具

21.開啟「防火牆遷移工具」，在「選擇源配置」下拉選單中，選擇「Cisco Secure Firewall Device Manager(7.2+)」，然後單擊「Start Migration」。



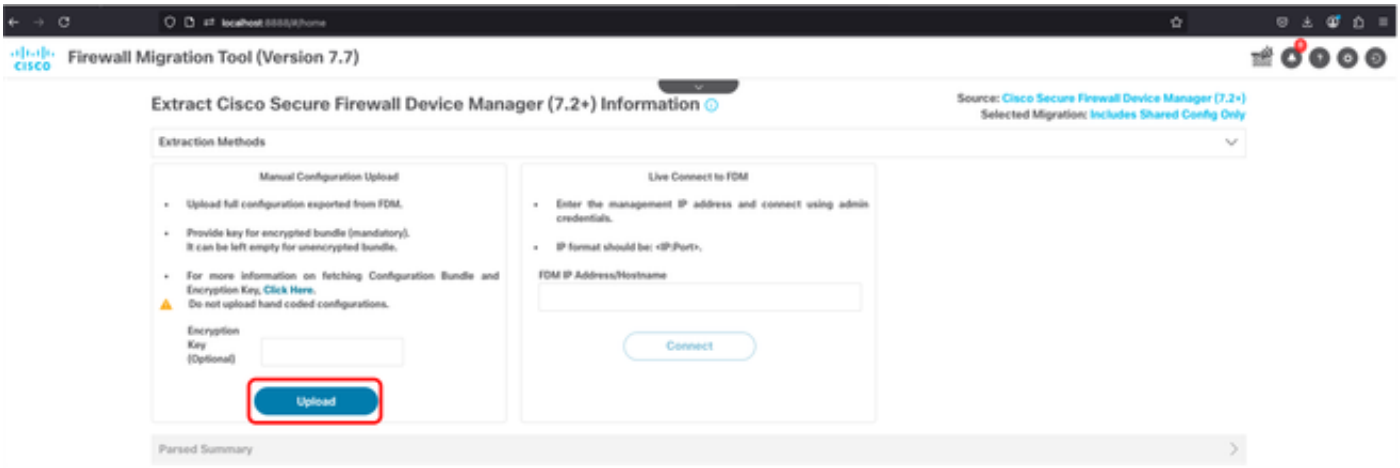
FMT - FDM選擇

22.選中第一個單選按鈕Migrate Firewall Device Manager(Shared Configurations Only)，然後單擊Continue。



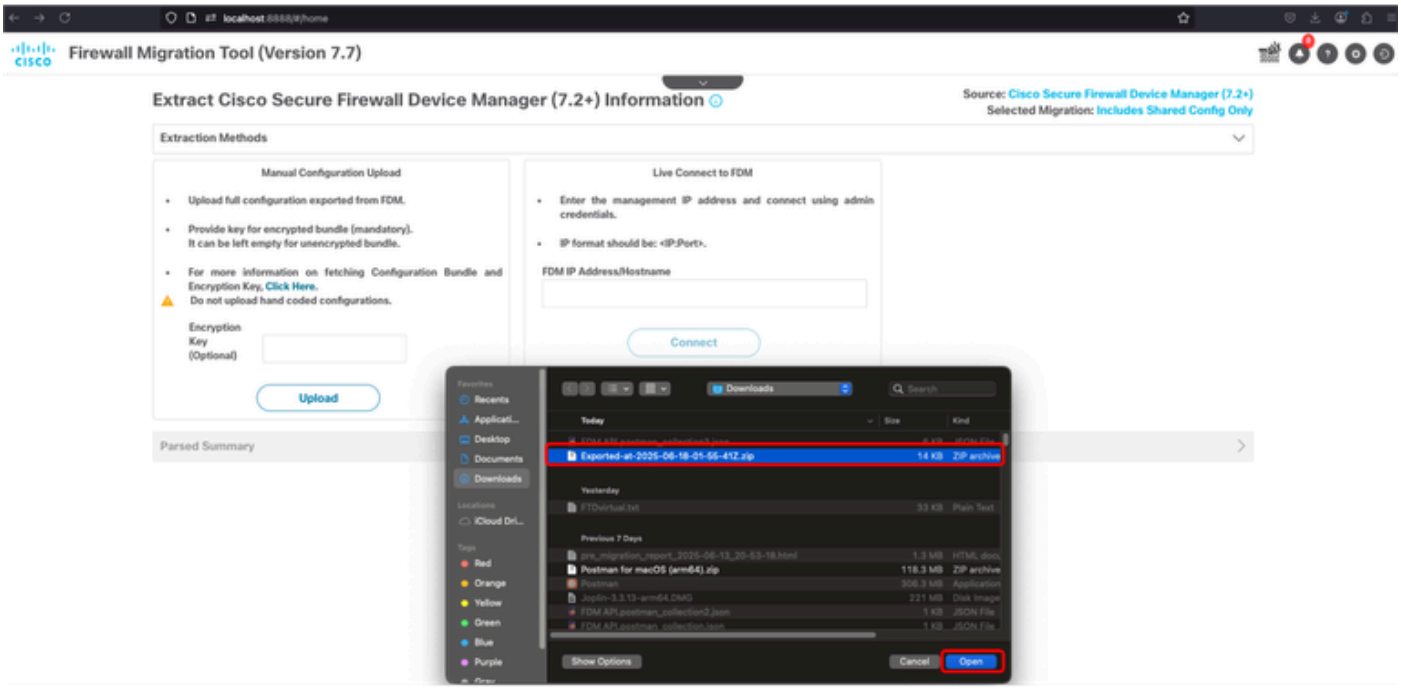
FMT — 僅限FDM遷移共用配置

23.在左側面板(手動配置上傳)中，按一下Upload。



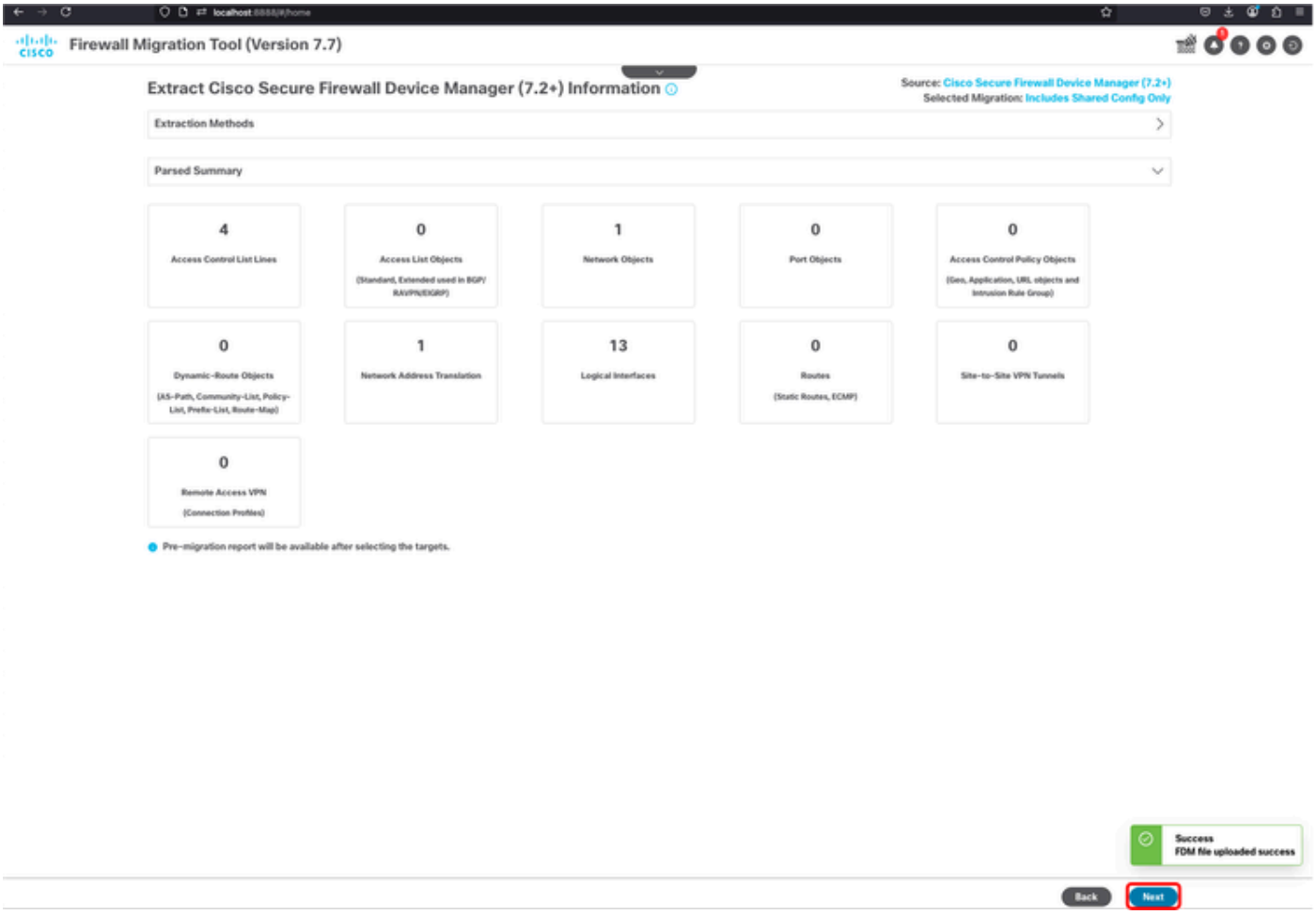
FMT — 上傳Config.zip檔案

24.在先前儲存的資料夾中選擇匯出的zip配置檔案，然後按一下Open。



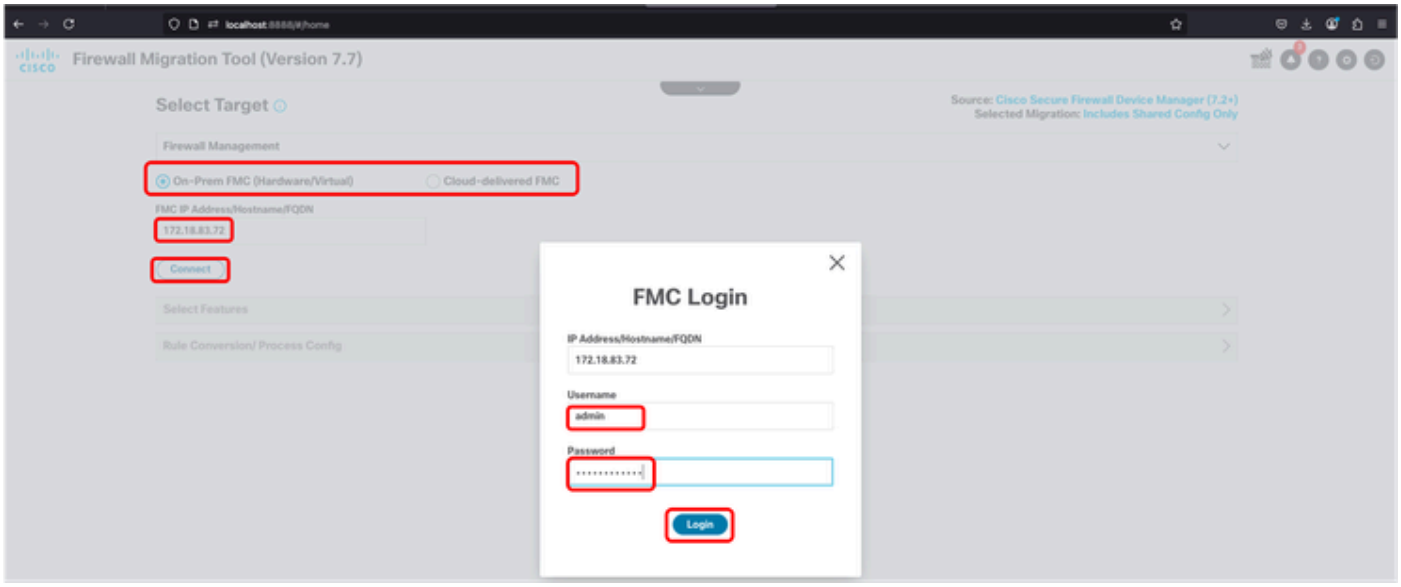
FMT - Config.zip檔案選擇

25.如果一切按預期進行，則顯示分析摘要。此外，在右下角可以看到一個彈出視窗，通知已成功上載FDM檔案。按「Next」（下一步）。



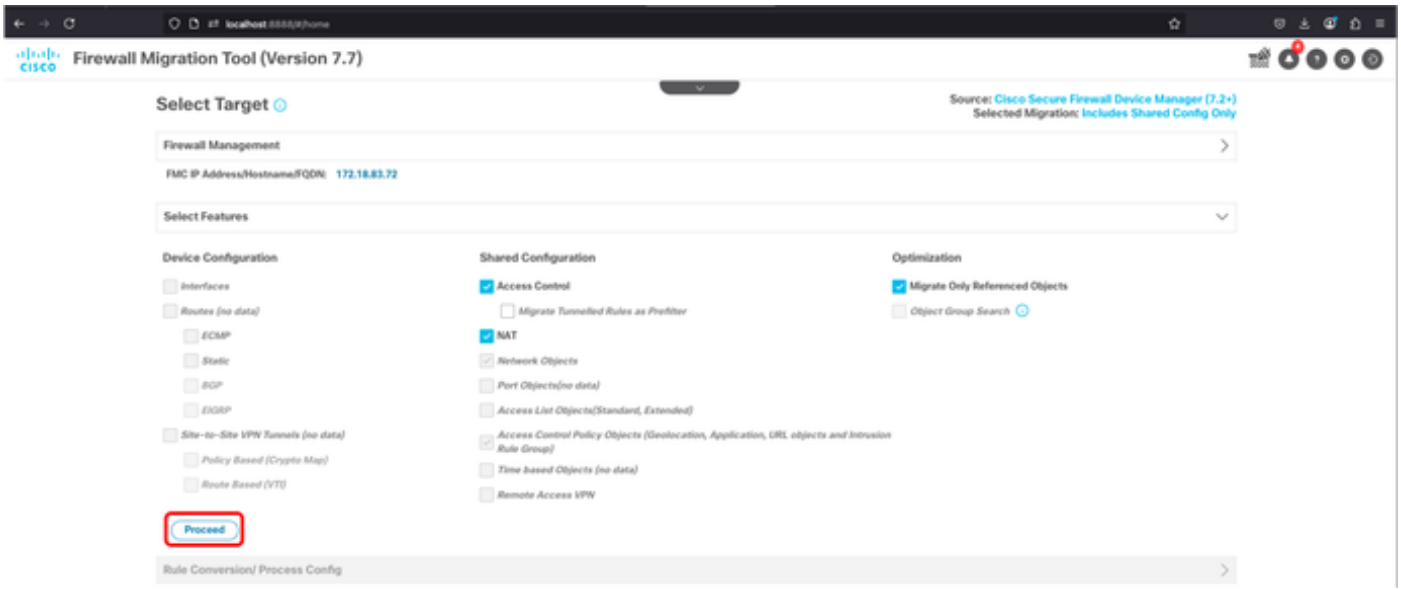
FMT — 分析摘要

26.選擇更適合您環境的選項（本地FMC或Cd-FMC）。 在此案例中，使用內部型FMC。鍵入FMC IP地址，然後按一下Connect。出現一個新的彈出視窗，要求輸入FMC憑證，在輸入此資訊後，按一下Login。



FMT - FMC Target登入

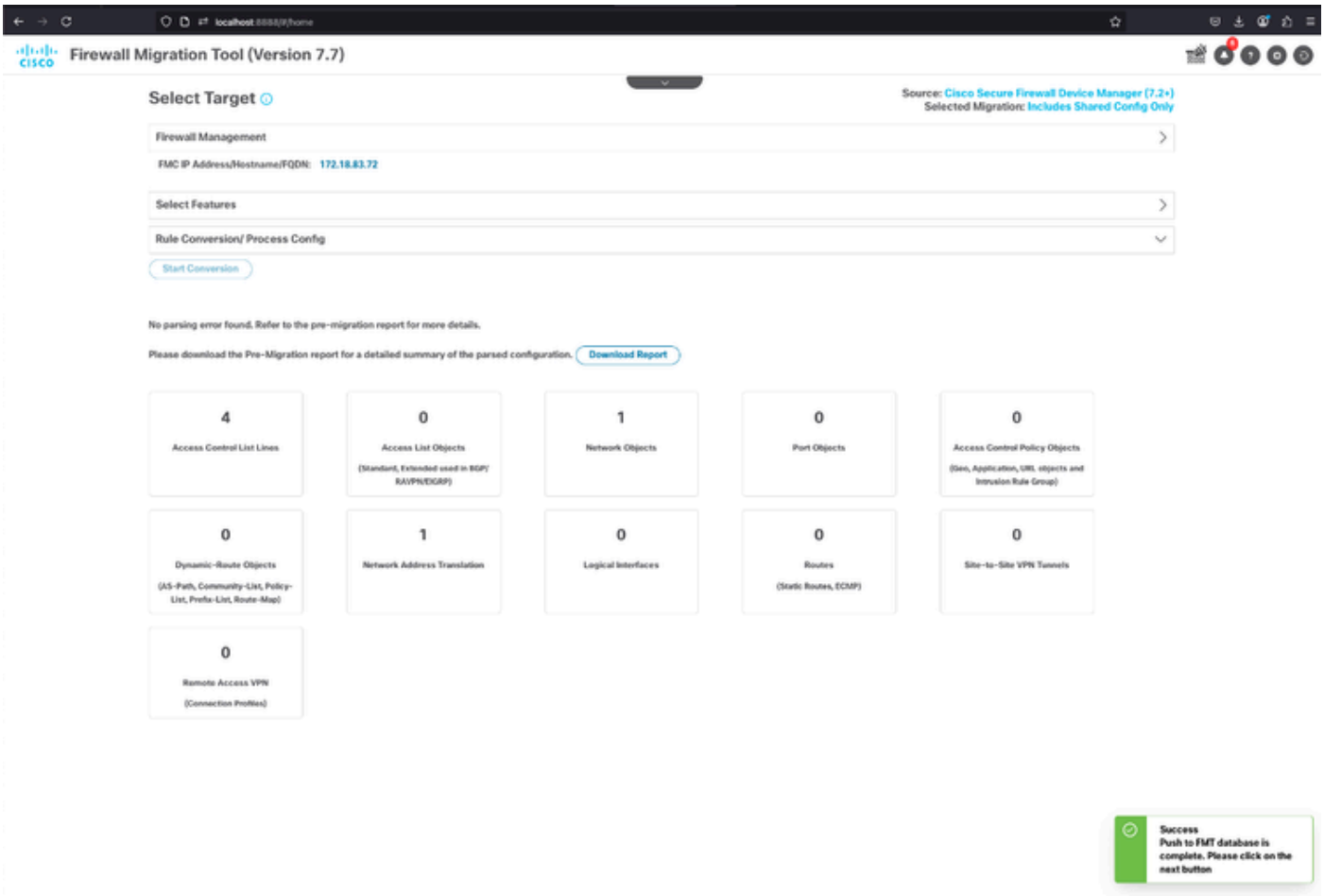
27.下一個螢幕顯示目標FMC和要遷移的功能。按一下「Proceed」。



FMT - FMC目標 — 功能選擇

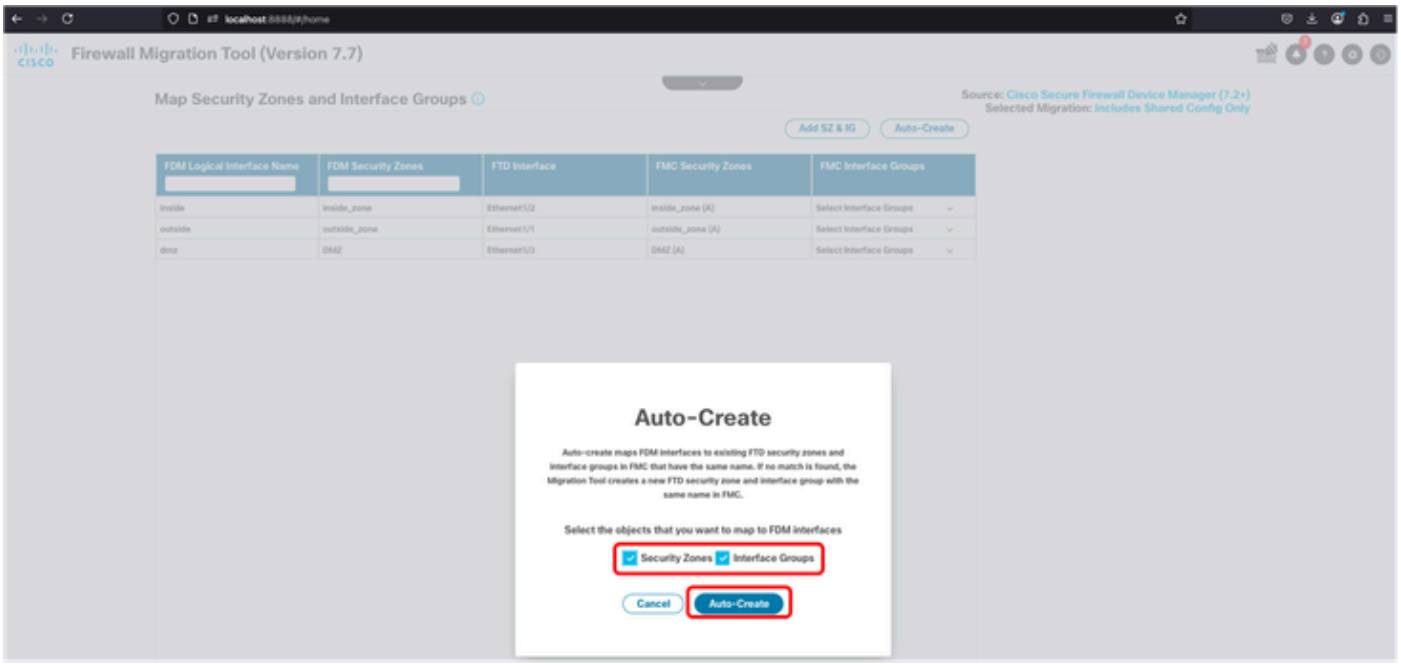
28.確認FMC目標後，按一下Start Conversion按鈕。

29.如果一切按預期進行，則右下角將顯示一個彈出視窗，通知向FMT資料庫推送的工作已完成。按「Next」（下一步）。



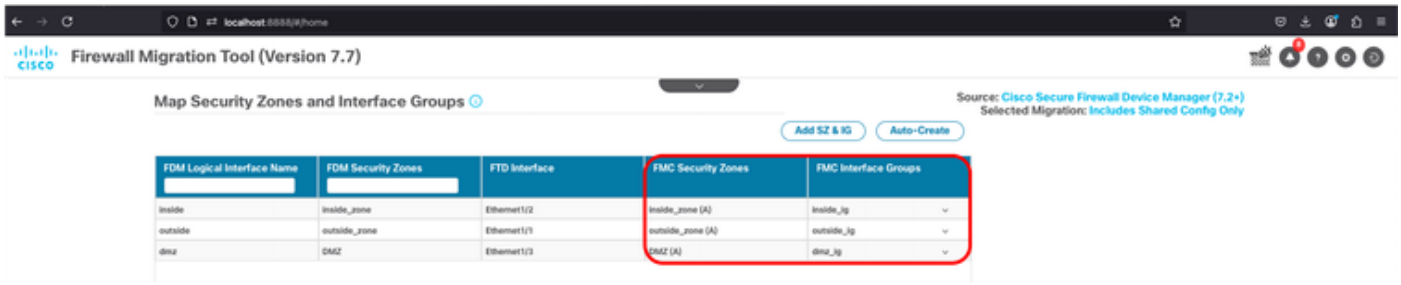
FMT — 資料庫推送已成功完成

30.在下一個螢幕中，您必須手動建立，或選擇自動建立安全區域和介面組。在此案例中，使用自動建立。



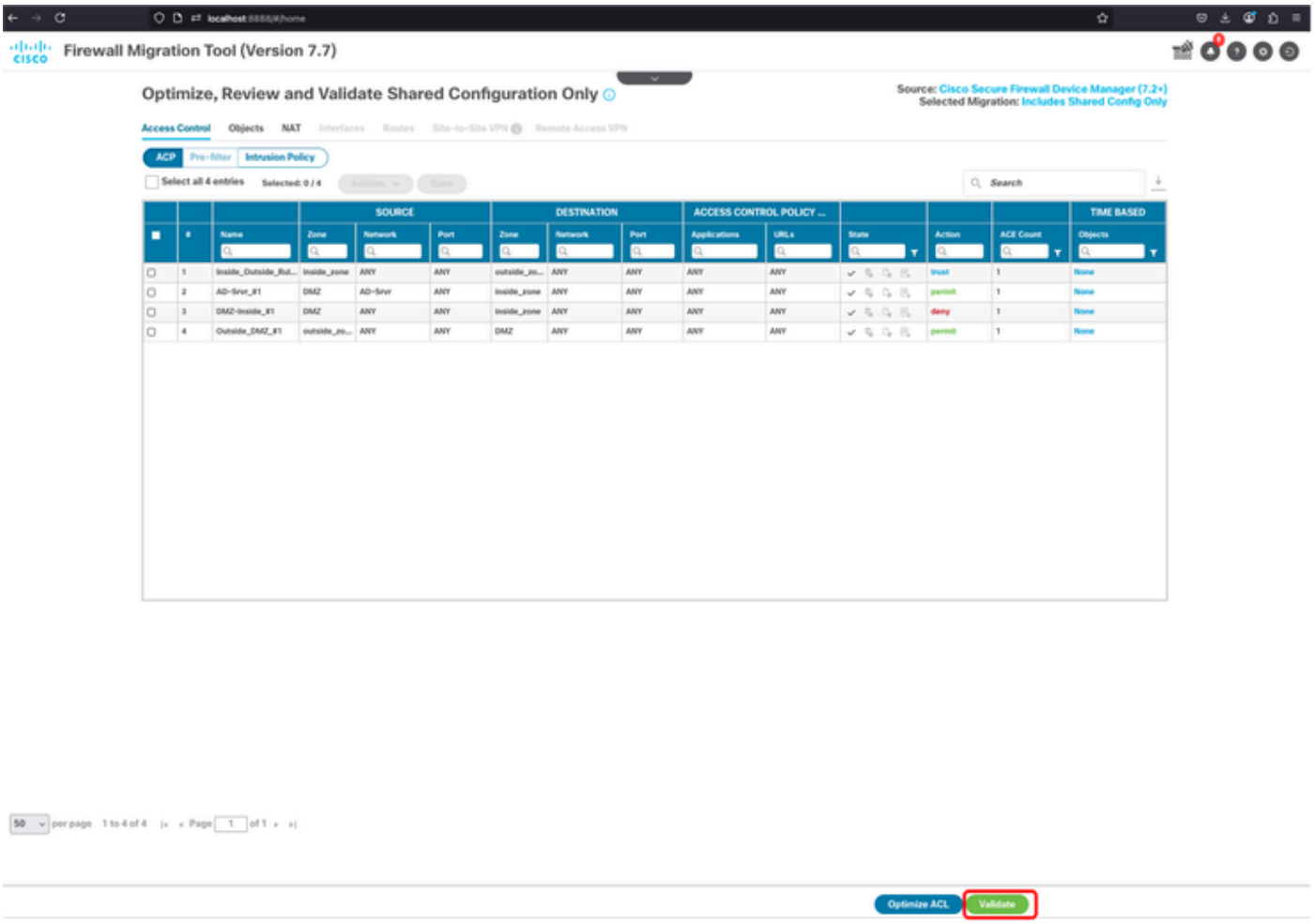
FMT — 自動建立安全區域和介面組

31.表格一經填寫，分別在第4欄和第5欄，即安全區和介面組顯示。



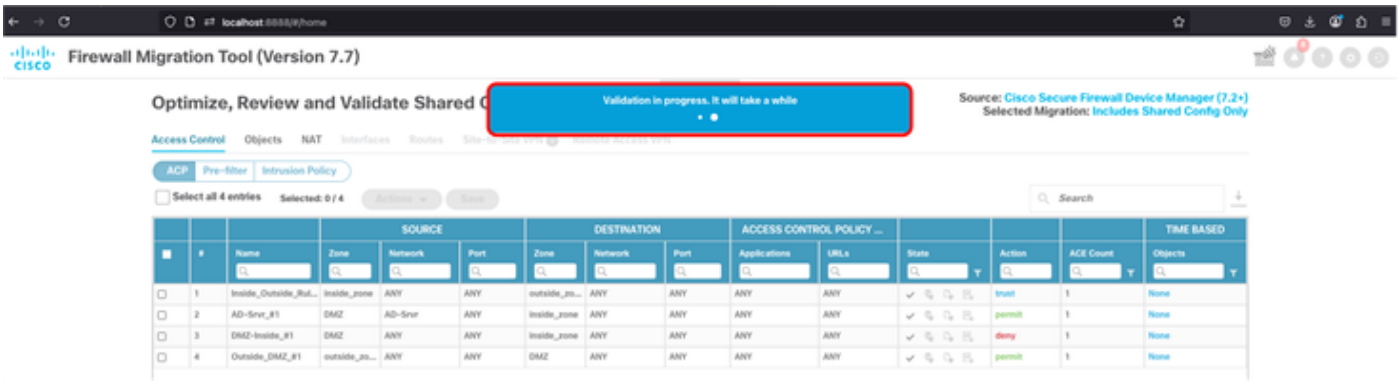
FMT — 安全區域和介面組已成功建立

32.在下一個螢幕中，您可以最佳化ACL或僅驗證ACP、對象和NAT。完成後，按一下Validate按鈕。



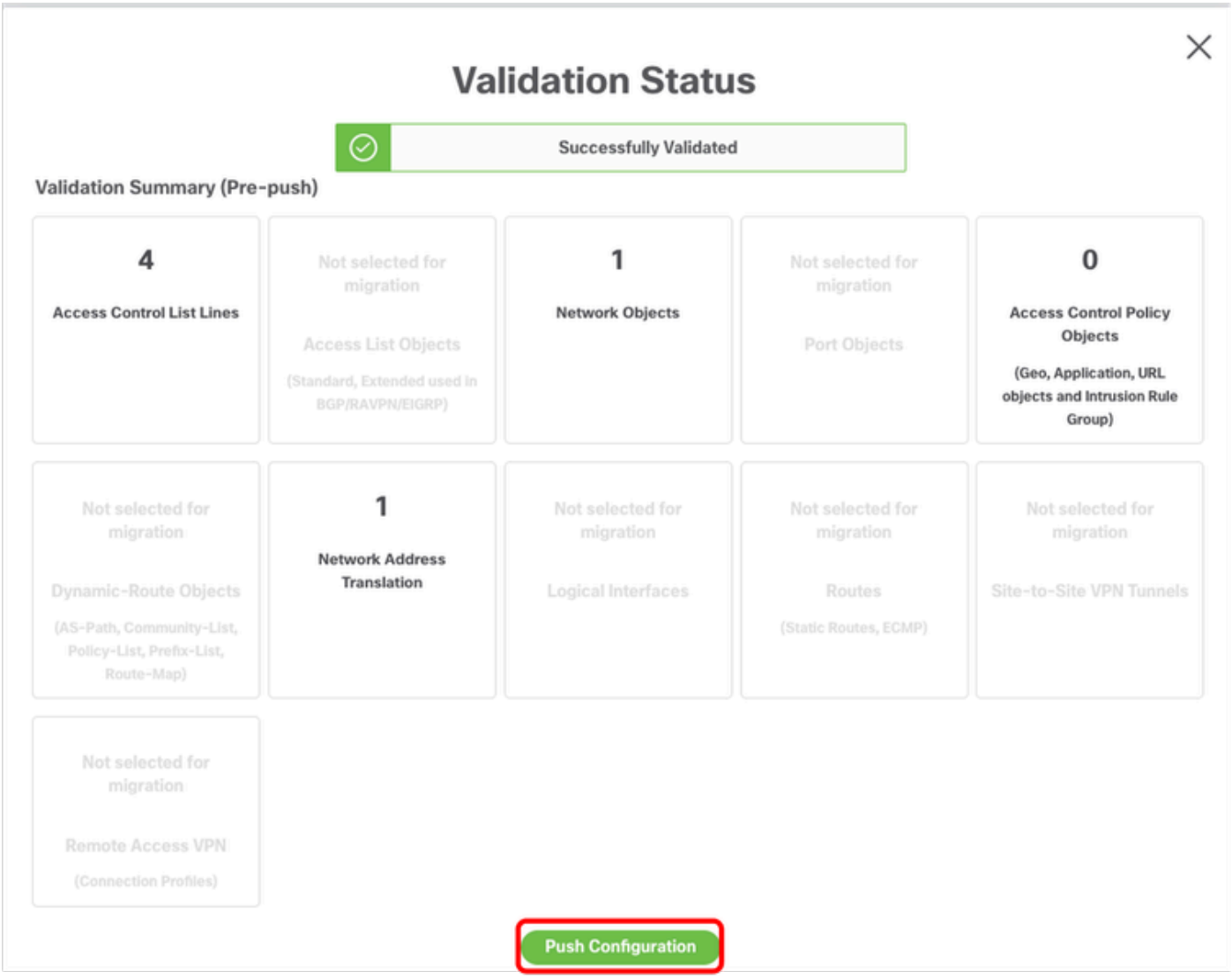
FMT — 最佳化ACL — 驗證遷移

33.驗證工作需要幾分鐘才能完成。



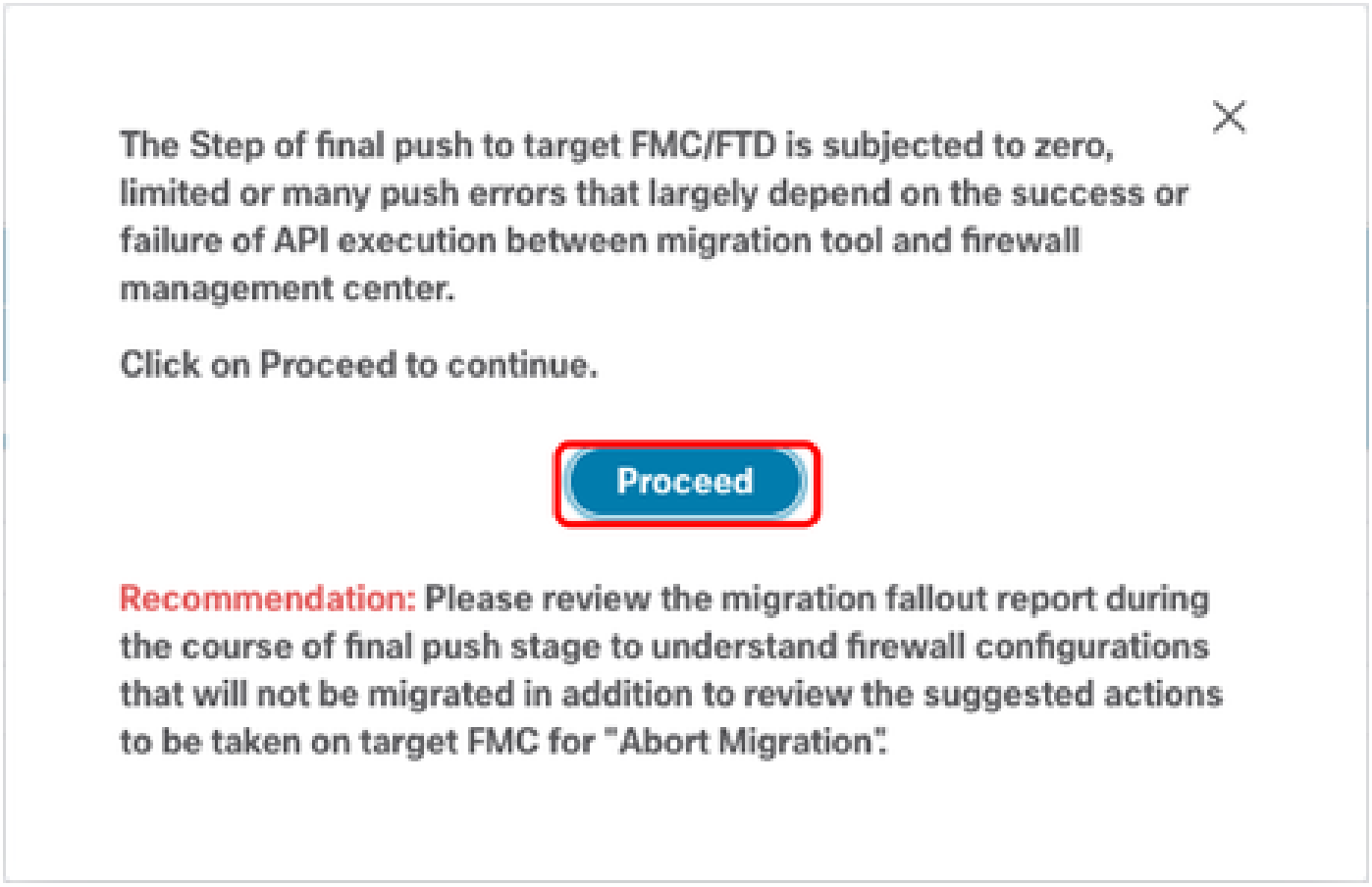
FMT — 正在進行驗證

34.完成後，FMT讓您知道配置已成功驗證，下一步是按一下Push Configuration按鈕。



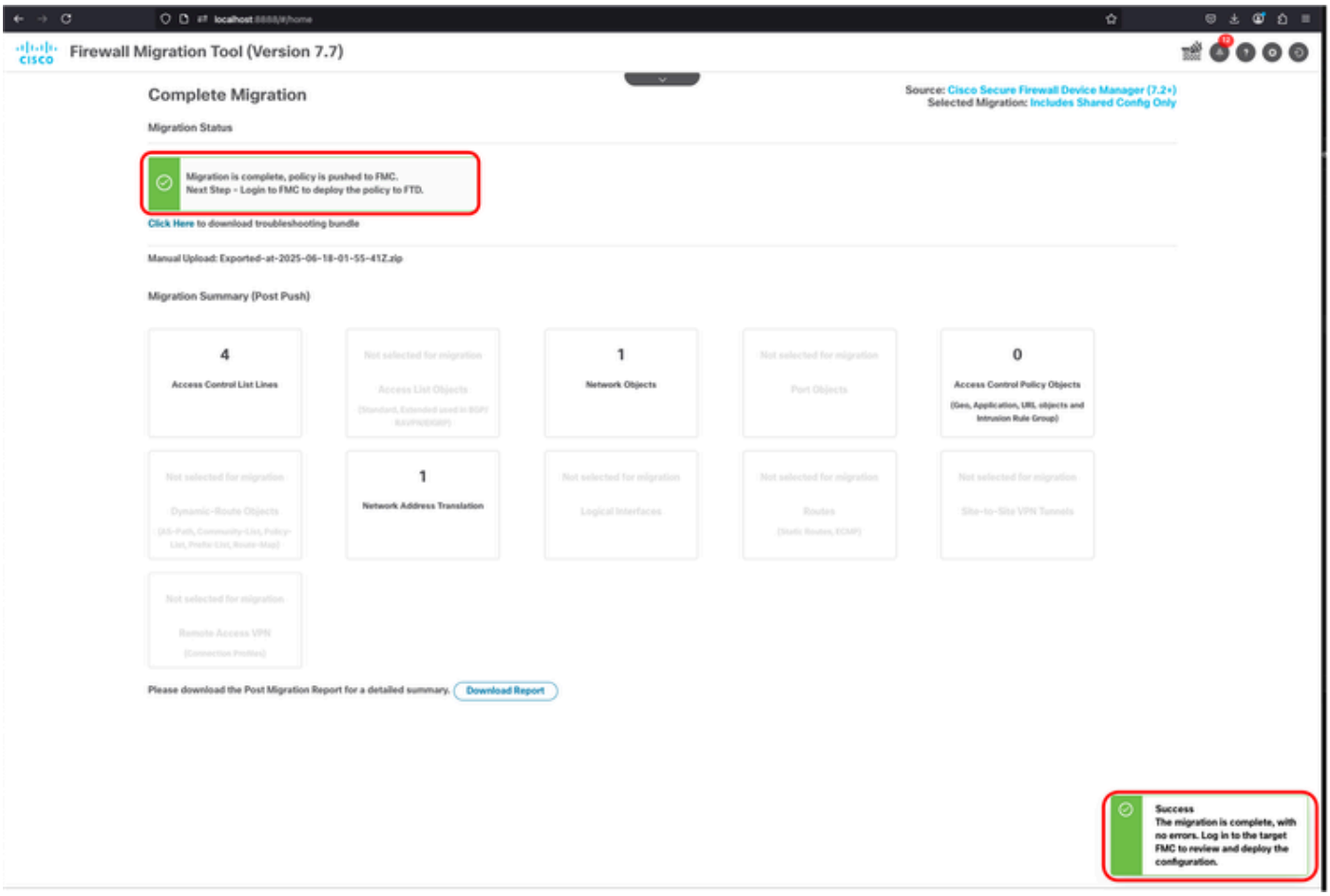
FMT — 驗證成功 — 將配置推送到FMC

35.最後，按一下Proceed按鈕。



FMT — 繼續配置推送

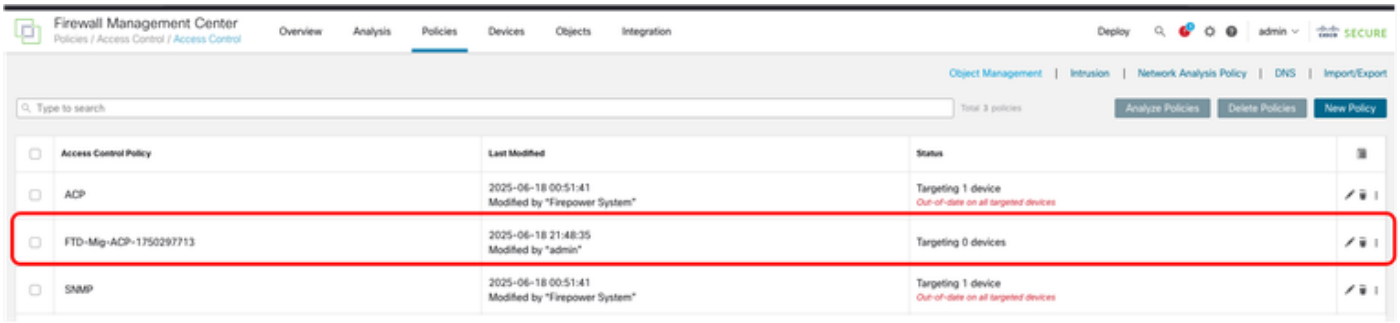
36.如果一切如期進行，將顯示遷移成功通知。FMT要求您登入FMC並將遷移的策略部署到FTD。



FMT — 遷移成功通知

FMC驗證

37.登入到FMC後，ACP和NAT策略顯示為FTD-Mig。現在，您可以繼續部署到新的FTD。



FMC - ACP已遷移

FMC - NAT策略已遷移

相關資訊

- FMT - FDM向FMC遷移指南
- 《FMT發行說明》

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）。