

# 通過REST API從ASA遷移到FDM的DAP和HostScan

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[授權](#)

[功能限制](#)

[組態](#)

[驗證](#)

[從FTD GUI進行部署驗證](#)

[從FTD CLI進行部署驗證](#)

[疑難排解](#)

## 簡介

本檔案介紹將動態存取原則(DAP)和HostScan組態從思科調適型安全裝置(ASA)遷移到由Firepower裝置管理員(FDM)本地管理的Cisco Firepower威脅防禦(FTD)的過程。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 有關FDM上的RA VPN配置的基本知識。
- 在ASA上使用DAP和Hostscan。
- REST API和FDM Rest API資源管理器基礎知識。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行6.7.0版的Cisco FTD
- Cisco AnyConnect安全行動化使用者端版本4.9.00086
- Postman或任何其他API開發工具

**注意：**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。如果您的網路正在作用，請確保您已瞭解任何組態變更的潛在影響。

。

# 背景資訊

即使FTD具有遠端存取VPN(RAVPN)組態支援，它仍缺乏對DAP的支援。自6.7.0版起，FTD上新增對DAP的API支援。它旨在支援從ASA遷移到FTD的基本使用案例。在ASA上配置了DAP並正在遷移到FTD的使用者現在具有遷移其DAP配置及其RA VPN配置的路徑。

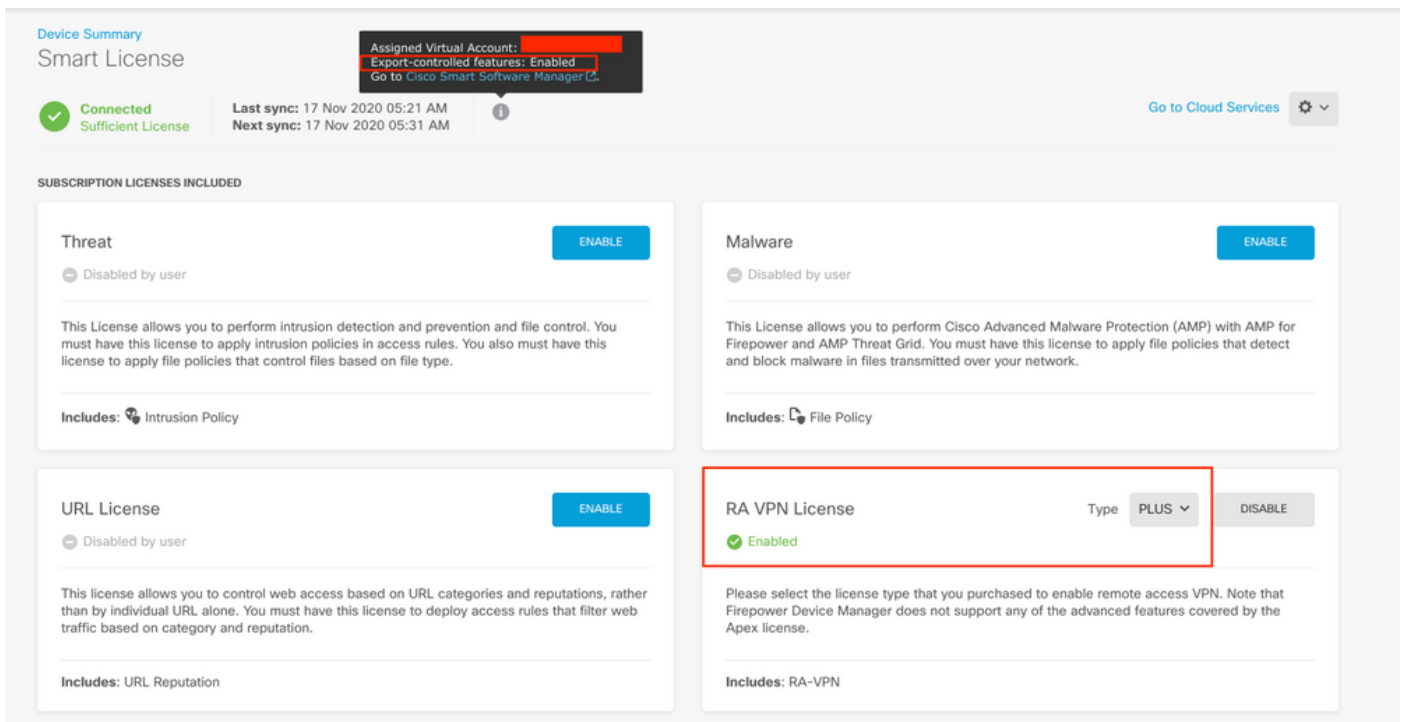
若要成功將DAP配置從ASA遷移到FTD，請確保以下條件：

- 配置了DAP/Hostscan的ASA。
- TFTP/FTP伺服器從ASA訪問，或ASDM訪問ASA。
- 運行版本6.7.0及更高版本的Cisco FTD，由Firepower裝置管理器(FDM)管理。
- 已配置RA VPN並正在處理FTD。

## 授權

- FTD已註冊到已啟用匯出控制功能的智慧許可門戶（以便啟用RA VPN配置頁籤）。
- 任何一個AnyConnect許可證已啟用（APEX、Plus或僅VPN）。

若要檢查授權：導覽至Devices > Smart Licenses



## 功能限制

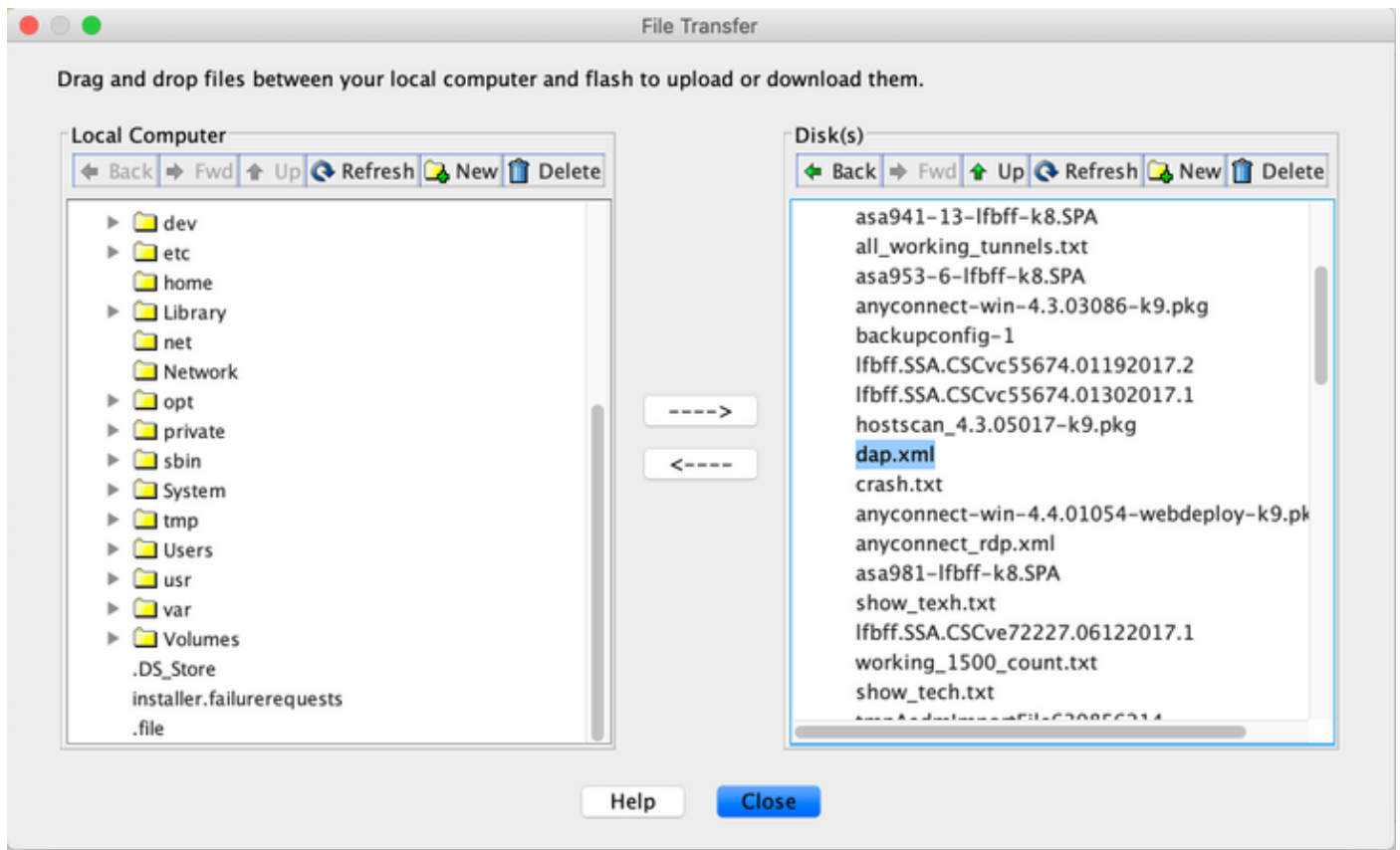
- 僅通過FDM/FTD REST API介面支援這些功能。
- DAP名稱不能包含帶有REST API的空格字元。

## 組態

步驟1. 將dap.xml從ASA複製到本地PC/TFTP伺服器。實現相同目標的方式有兩種：

ASDM:

導覽至Tools > File Management >File Transfer >Between Local PC and Flash。



CLI:

```
ASA# copy flash: tftp:
```

```
Source filename []? dap.xml
```

```
Address or name of remote host []? 10.197.161.160
```

```
Destination filename [dap.xml]?
```

```
440 bytes copied in 0.40 secs
```

**步驟2.** 將hostscan配置檔案(data.xml)和hostscan映像從ASA複製到本地裝置。

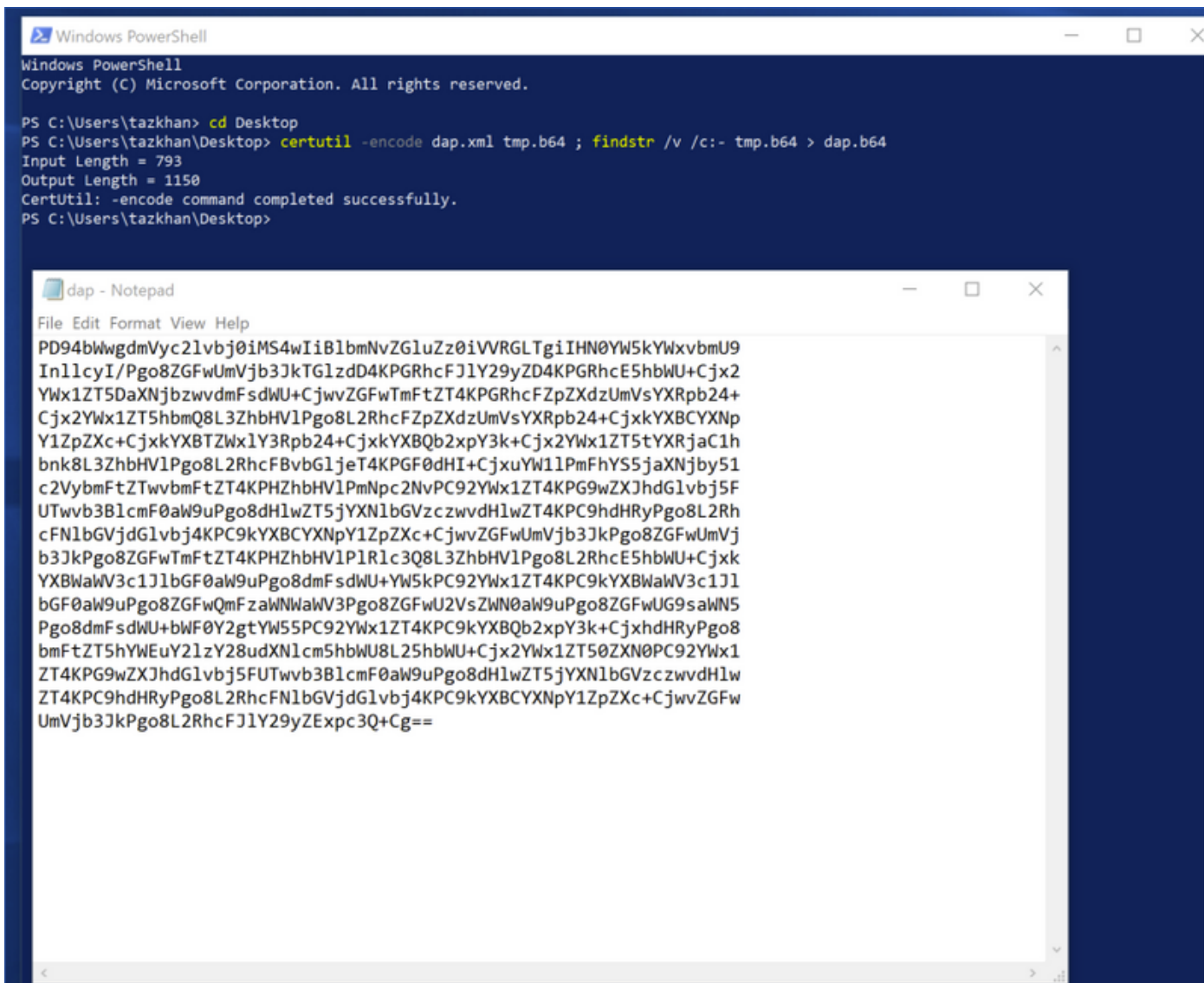
ASDM:

導航到Tools > File Management >File Transfer >Between Local PC and Flash。



```
tazkhan@TAZKHAN-M-32A3 Desktop % base64 -i dap.xml
PD94bWwgdMvYc2l1bWVj0iMS4wIiB1bWVZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9InllcyI/Pgo8ZGFwUmVjb3JkTG1zdD4KPGRhcFJlY29yZD4
KPGRhcE5hbWU+Cjx2YWx1ZT5XaW5kb3dzPC92YWx1ZT4KPC9kYXB0YW11Pgo8ZGFwVmlld3NSZWhhdG1vbG1jeT4KPHZhbHVlPmFuZDwvdmFsdWU+Cj
wvZGFwVmlld3NSZWhhdG1vbG1jeT4KPGRhcEJhc2l1Zm1ldz4KPC9kYXB0YW11Pgo8ZGFwUmVjb3JkTG1zdD4KPHZhbHVlPmFuZDwvdmFsd
WU+CjwvZGFwUG9saWN5Pgo8YXR0cjk4KPGRhcE5hbWU+YW5kPC92YWx1ZT4KPC9kYXB0YW11Pgo8dmFsdWU+Y2l2Y288L3ZhbHVlPgo8b3B1cmF0
aW9uPkvRRC9vcGVyYXRpb24+Cjx0eXB1PmNhc2VsZXR0eXB1Pgo8L2F0dHI+CjwvZGFwU2VsZWN0aW9uPgo8ZGFwU2VsZWN0aW9uPgo8ZGF
wUG9saWN5Pgo8dmFsdWU+bW0yZGtYW55PC92YWx1ZT4KPC9kYXB0b2xpY3k+CjxkYXB0dWJlZG1vbG1jeT4KPHZhbHVlPmFuZDwvdmFsd
WU+Cjx2YWx1ZT5tYXRjaC1hbGw8L3ZhbHVlPgo8L2RhcFBvbG1jeT4KPC9kYXB0dHI+Cjx2YWx1ZT5tYXRjaC1hbGw8L3ZhbHVlPmFuZDwvdmFsd
WU+Cjx2YWx1ZT5tYXRjaC1hbGw8L3ZhbHVlPgo8L2RhcFBvbG1jeT4KPC9kYXB0dHI+Cjx2YWx1ZT5tYXRjaC1hbGw8L3ZhbHVlPmFuZDwvdmFsd
WU+Cjx2YWx1ZT5tYXRjaC1hbGw8L3ZhbHVlPgo8L2RhcFBvbG1jeT4KPC9kYXB0dHI+Cjx2YWx1ZT5tYXRjaC1hbGw8L3ZhbHVlPmFuZDwvdmFsd
WU+Cjx2YWx1ZT5tYXRjaC1hbGw8L3ZhbHVlPgo8L2RhcFBvbG1jeT4KPC9kYXB0dHI+Cjx2YWx1ZT5tYXRjaC1hbGw8L3ZhbHVlPmFuZDwvdmFsd
WU+Cjx2YWx1ZT5tYXRjaC1hbGw8L3ZhbHVlPgo8L2RhcFBvbG1jeT4KPC9kYXB0dHI+Cjx2YWx1ZT5tYXRjaC1hbGw8L3ZhbHVlPmFuZDwvdmFsd
WU+Cjx2YWx1ZT5tYXRjaC1hbGw8L3ZhbHVlPgo8L2RhcFBvbG1jeT4KPC9kYXB0dHI+Cjx2YWx1ZT5tYXRjaC1hbGw8L3ZhbHVlPmFuZDwvdmFsd
WU+Cjx2YWx1ZT5tYXRjaC1hbGw8L3ZhbHVlPgo8L2RhcFBvbG1jeT4KPC9kYXB0dHI+Cjx2YWx1ZT5tYXRjaC1hbGw8L3ZhbHVlPmFuZDwvdmFsd
WU+Cjx2YWx1ZT5tYXRjaC1hbGw8L3ZhbHVlPgo8L2RhcFBvbG1jeT4KPC9kYXB0dHI+Cjx2YWx1ZT5tYXRjaC1hbGw8L3ZhbHVlPmFuZDwvdmFsd
WU+Cg==
```

在Windows powershell上：`certutil -encode dap.xml tmp.b64 ; findstr /v /c:- tmp.b64 > dap.b64`



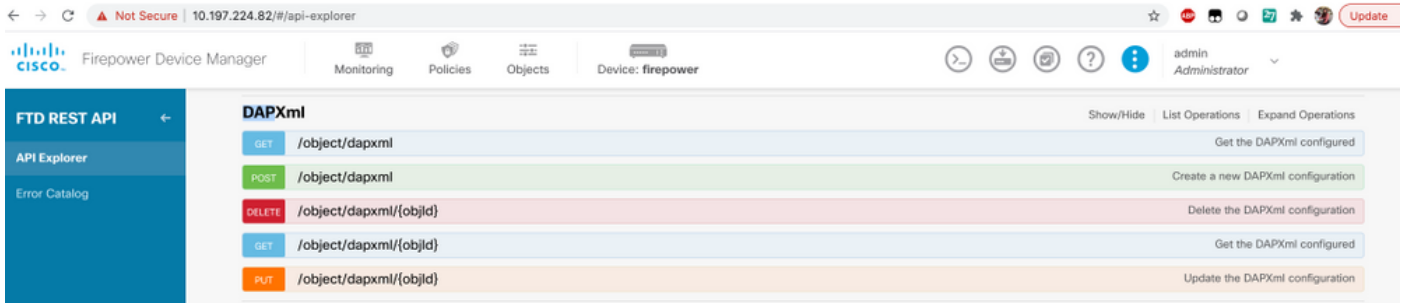
對data.xml執行相同的過程。

步驟4. 在瀏覽器視窗中啟動FTD的API瀏覽器。

導覽至<https://<FTD Management IP>/api-explorer>

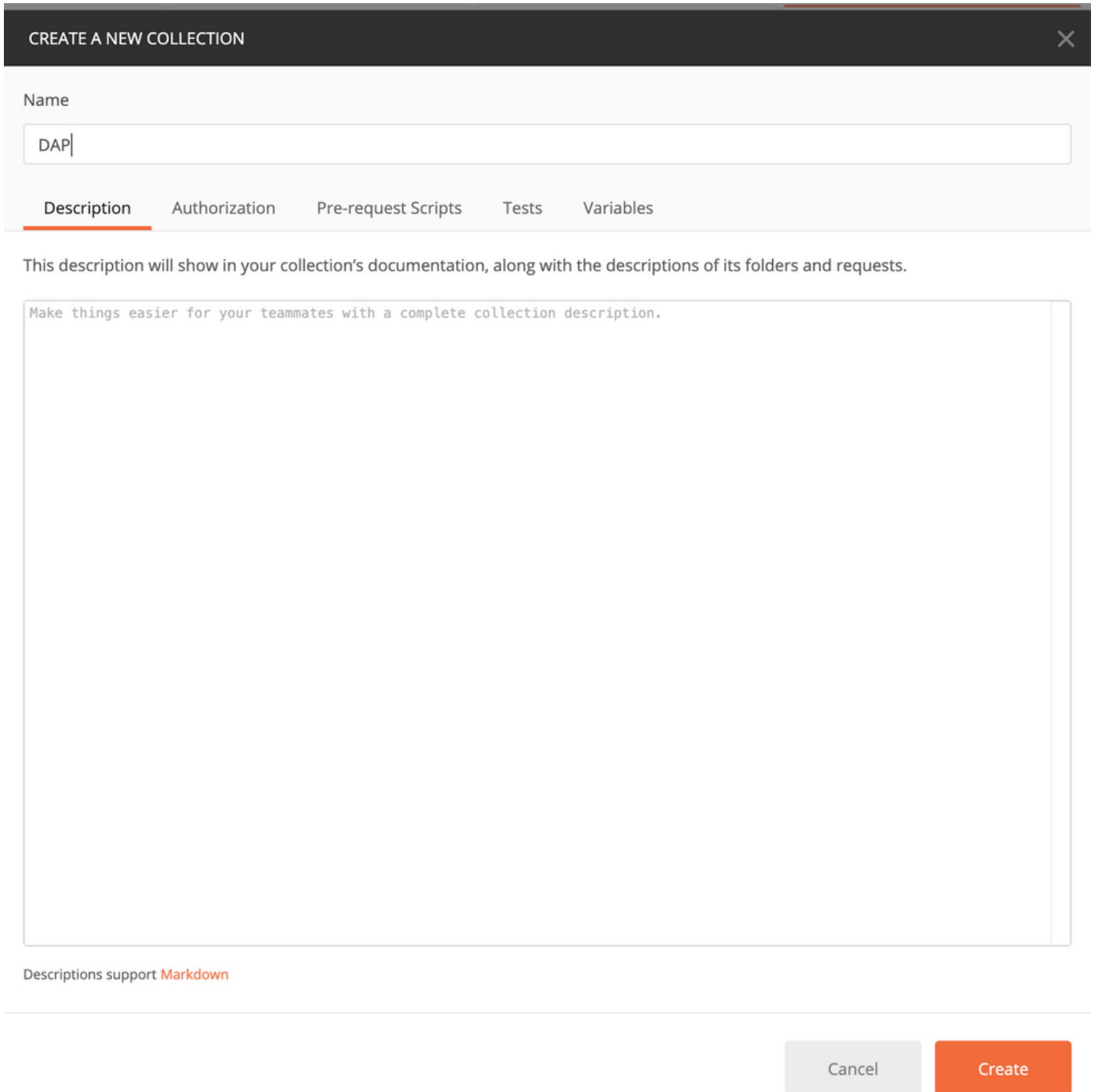
此清單包含FTD上可用的全部API清單。它基於FDM支援的多個GET/POST/PUT/DELETE請求的主要功能進行劃分。

使用的是DAPXml和HostScanPackageFile。



步驟5. 為DAP新增Postman集合。

為集合提供名稱。按一下「Create」，如下圖所示。



步驟6. 新增新請求 身份驗證 建立到FTD的登入POST要求，以取得權杖來授權任何 POST/GET/PUT要求。按一下Save。

