DAP- und HostScan-Migration von ASA zu FDM über REST-API

Inhalt

Einführung

Dieses Dokument beschreibt die Migration von Dynamic Access Policies (DAP) und HostScan-Konfigurationen von Cisco Adaptive Security Appliances (ASA) zu Cisco FirePOWER Threat Defense (FTD), die lokal vom FirePOWER Device Manager (FDM) verwaltet werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundkenntnisse der RA VPN-Konfiguration auf FDM.
- Arbeiten von DAP und Hostscan auf ASA.
- Grundkenntnisse der REST API und des FDM Rest API Explorer.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco FTD mit Version 6.7.0
- Cisco AnyConnect Secure Mobility Client Version 4.9.0086
- Postman oder ein anderes API-Entwicklungstool

Hinweis: Die Informationen in diesem Dokument wurden von Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer

leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen von Konfigurationsänderungen verstehen.

Hintergrundinformationen

Obwohl FTD über RAVPN-Konfigurationsunterstützung (Remote Access VPN) verfügt, bietet es keine Unterstützung für DAP. Ab Version 6.7.0 wird die API-Unterstützung für DAP im FTD hinzugefügt. Sie soll den sehr grundlegenden Anwendungsfall der Migration von ASA zu FTD unterstützen. Benutzer, die DAP auf ihren ASAs konfiguriert haben und gerade auf FTDs migrieren, haben jetzt die Möglichkeit, ihre DAP-Konfiguration zusammen mit ihrer RA VPN-Konfiguration zu migrieren.

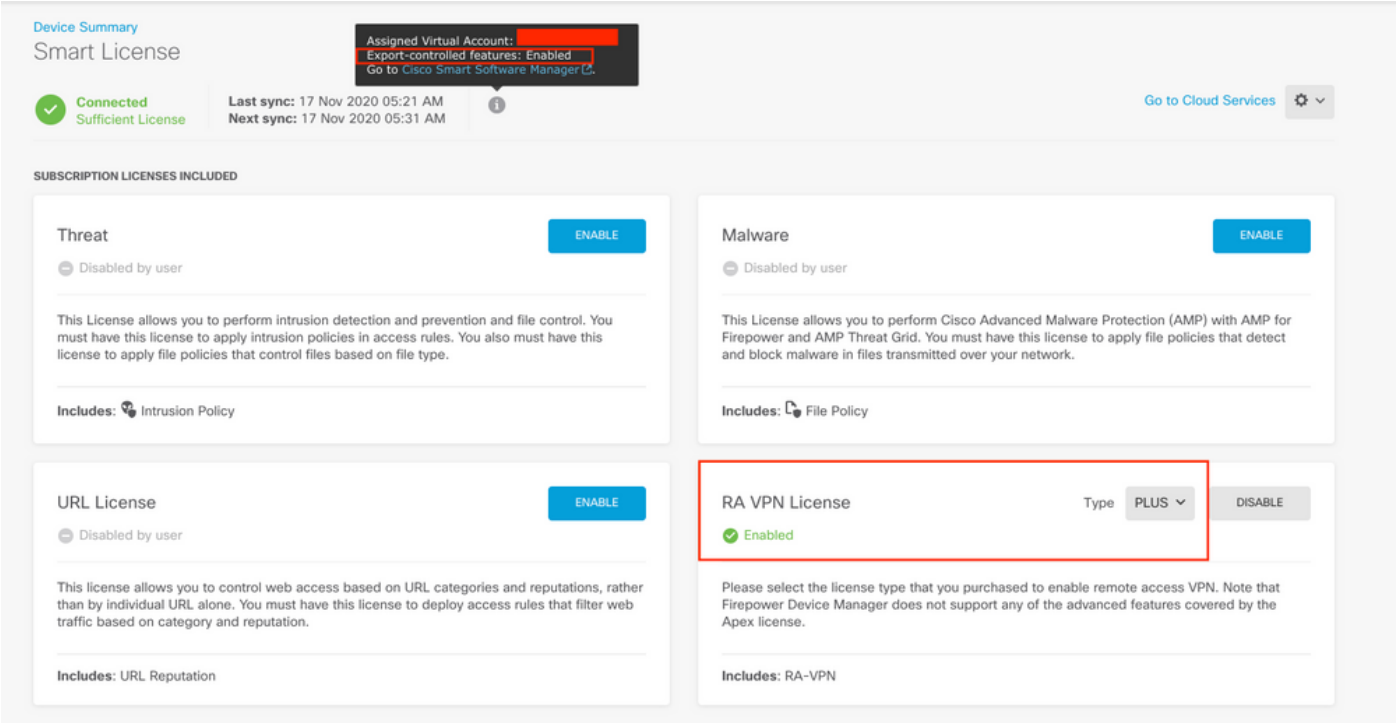
Um die DAP-Konfiguration erfolgreich von ASA zu FTD zu migrieren, müssen folgende Bedingungen erfüllt sein:

- ASA mit konfiguriertem DAP/Hostscan.
- TFTP-/FTP-Serverzugriff von der ASA oder ASDM-Zugriff auf die ASA
- Cisco FTD mit Version 6.7.0 und höher wird vom FirePOWER Device Manager (FDM) verwaltet.
- RA VPN ist konfiguriert und arbeitet mit FTD.

Lizenzierung

- FTD im Smart Licensing-Portal mit aktivierten "Export Controlled Features" registriert (um die Aktivierung der Registerkarte "RA VPN Configuration" zu ermöglichen).
- Alle aktivierten AnyConnect-Lizenzen (APEX, Plus oder VPN Only).

So überprüfen Sie die Lizenzierung: Navigieren Sie zu **Geräte > Smart Licenses.**



Einschränkungen bei Funktionen

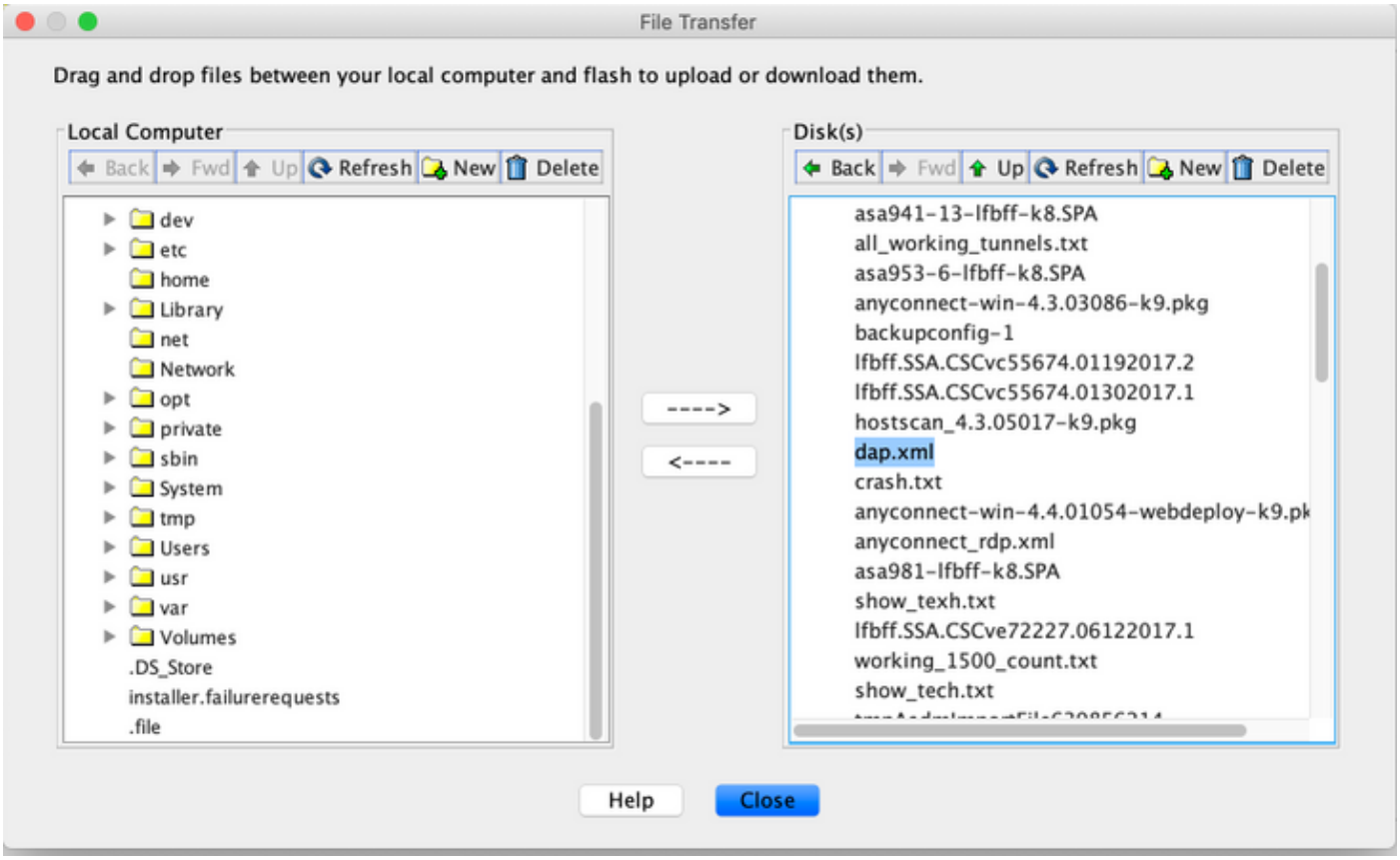
- Diese Funktionen werden nur über die REST-API-Schnittstelle FDM/FTD unterstützt.
- Der DAP-Name darf keine Leerzeichen mit REST API enthalten.

Konfiguration

Schritt 1: Kopieren Sie **dap.xml** von ASA auf Ihren lokalen PC/TFTP-Server. Es gibt zwei Möglichkeiten, dies zu erreichen:

ASDM:

Navigieren Sie zu **Extras > Dateiverwaltung > FIle Transfer > zwischen lokalem PC und Flash**.



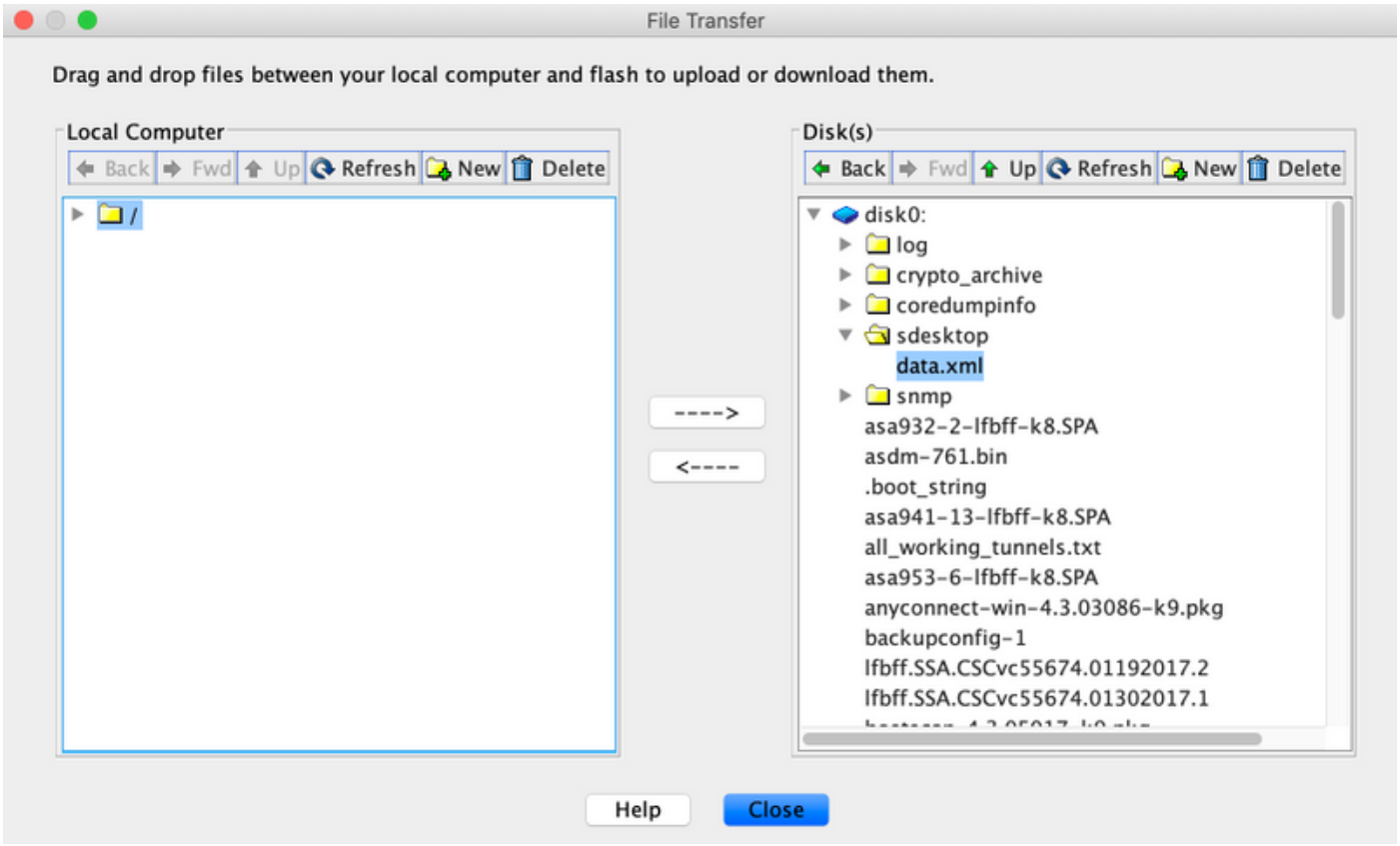
CLI:

```
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
```

Schritt 2: Kopieren Sie die HostScan-Konfigurationsdatei (data.xml) und das Hostscan-Image von ASA auf das lokale Gerät.

ASDM:

Navigieren Sie zu **Extras > Dateiverwaltung > FIle Transfer >zwischen lokalem PC und Flash**.



CLI:

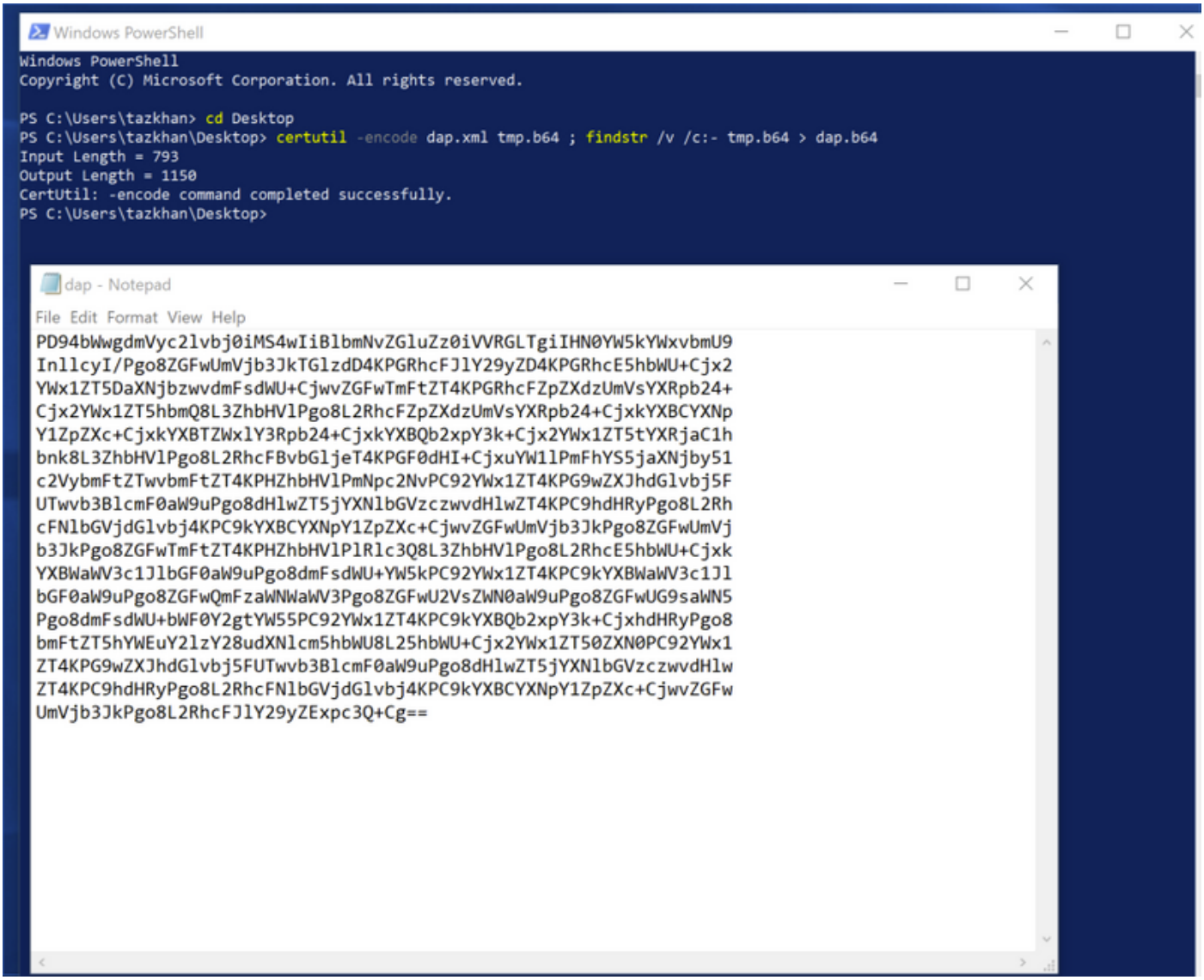
```
ASA# copy flash: tftp:
Source filename []? data.xml

Address or name of remote host []? 10.197.161.160

Destination filename [data.xml]?

500 bytes copied in 0.40 secs

ASA# copy flash: tftp:

Source filename []? hostscan_4.9.03047-k9.pkg

Address or name of remote host []? 10.197.161.160

Destination filename [hostscan_4.9.03047-k9.pkg]?
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
56202408 bytes copied in 34.830 secs (1653012 bytes/sec)
ASA#
```

Schritt 3: Abrufen des base64-codierten Werts von **dap.xml** und **data.xml**.

Auf Mac: **base64 -i <Datei>**

```
tazkhan@TAZKHAN-M-32A3 Desktop % base64 -i dap.xml
PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9InllcyI/Pgo8ZGFwUmVjb3JkTGlzdD4KPGRhcFJlY29yZD4
KPGRhcE5hbWU+Cjx2YWx1ZT5XaW5kb3dzPC92YWx1ZT4KPC9kYXBOYW1lPgo8ZGFwVmlld3NSZWxhdGlvbj4KPHZhbHVlPmFuZDwvdmFsdWU+Cj
wvZGFwVmlld3NSZWxhdGlvbj4KPGRhcEJhc2ljVmlldz4KPGRhcFNlbGVjdGlvbj4KPGRhcFBvbGljeT4KPHZhbHVlPm1hdGNoLWFueTwvdmFsd
WU+CjwvZGFwUG9saWN5Pgo8YXR0cj4KPG5hbWU+YWFhLmNpc2NvLnVzZXJuYW1lPC9uYW1lPgo8dmFsdWU+Y2lzY288L3ZhbHVlPgo8b3BlcmF0
aW9uPkVRPC9vcGVyYXRpb24+Cjx0eXBlPmNhc2VsZXNzPC90eXBlPgo8L2F0dHI+CjwvZGFwUG9saWN5Pgo8dmFsdWU+cGVyYXRpb24+CjwvZG
wUG9saWN5Pgo8dmFsdWU+bWF0Y2gtYW55PC92YWx1ZT4KPC9kYXBQb2xpY3k+CjxjdHRyPgo8
bmFtZT5hYWEuY2lzY28udXNlcm5hbWU8L25hbWU+Cjx2YWx1ZT50ZXN0PC92YWx1
ZT4KPG9wZXJhdGlvbj5FUTwvb3BlcmF0aW9uPgo8dHlwZT5YXNlbGVzczwvdHlw
ZT4KPC9hdHRyPgo8YXR0cj4KPG5hbWU+YWFhLmNpc2NvLnVzZXJuYW1lPC9uYW1l
UmVjb3JkPgo8L2RhcFJlY29yZExpc3Q+Cg==
```

Unter Windows PowerShell: **certutil-encode dap.xml tmp.b64 ; findstr /v /c:- tmp.b64 > dap.b64**



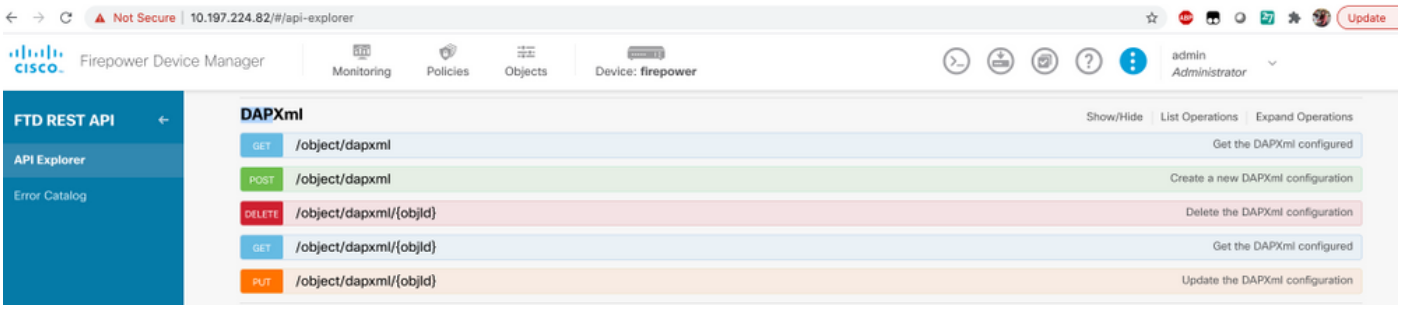
Befolgen Sie die gleiche Prozedur für data.xml.

Schritt 4: Starten Sie den API-Explorer des FTD in einem Browserfenster.

Navigieren Sie zu **https://<FTD Management IP>/api-explorer.**

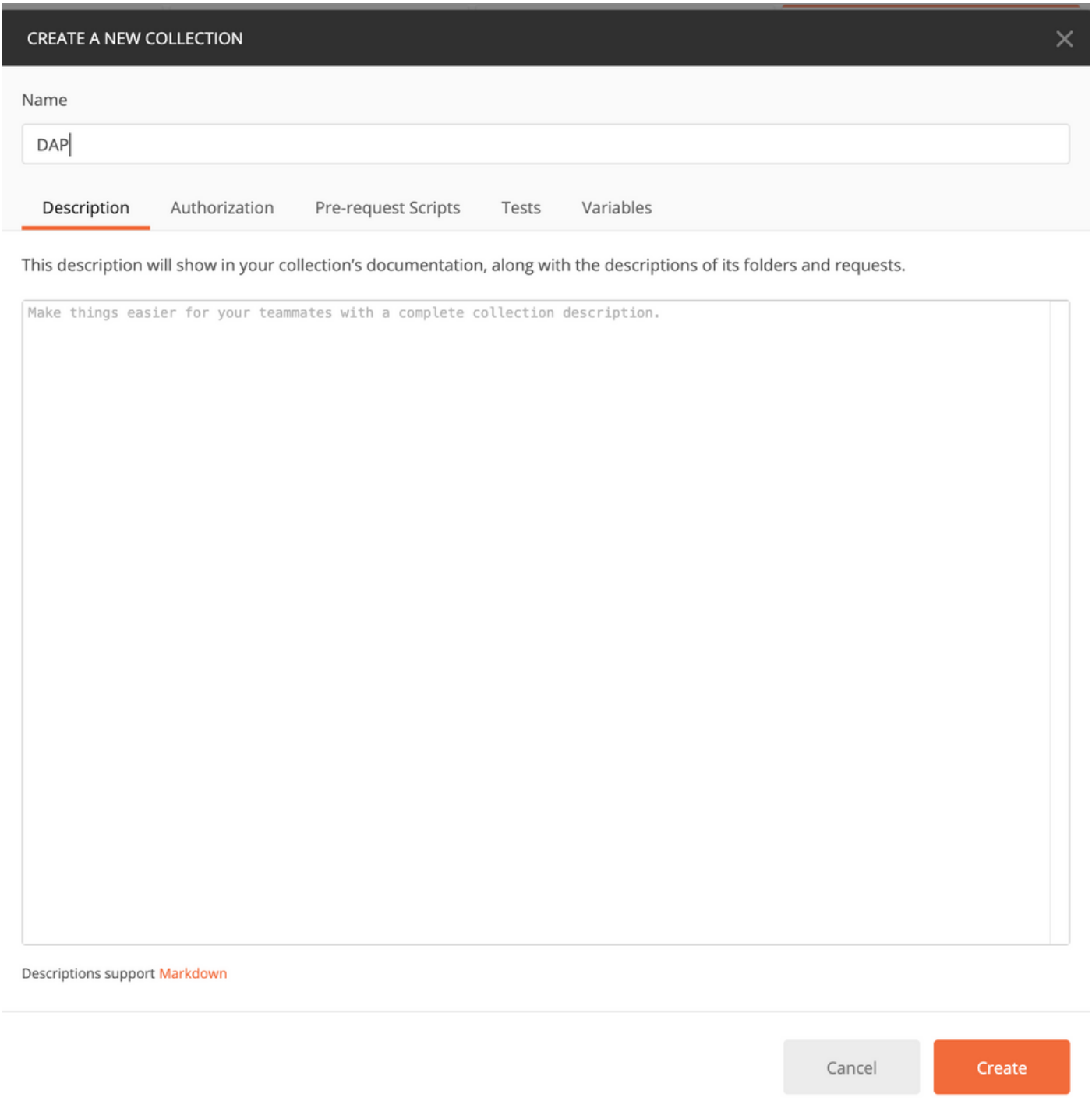
Diese enthält die gesamte Liste der APIs, die im FTD verfügbar sind. Sie wird basierend auf der Hauptfunktion durch mehrere GET/POST/PUT/DELETE-Anfragen aufgeteilt, die vom FDM unterstützt werden.

DAPXml und **HostScanPackageFile** werden API verwendet.



Schritt 5: Fügen Sie eine Postman-Sammlung für DAP hinzu.

Geben Sie einen **Namen** für die Auflistung ein. Klicken Sie auf **Erstellen**, wie in diesem Bild gezeigt.



Schritt 6: Neue Anforderung hinzufügen **Auth** um eine Login-POST-Anfrage bei der FTD zu

erstellen, um das Token zur Autorisierung von POST/GET/PUT-Anfragen zu erhalten. Klicken Sie auf **Speichern**.