DAP and HostScan Migration from ASA to FDM through REST API

Contents

Introduction

This document describes the migration of Dynamic Access Policies (DAP) and HostScan configuration from Cisco Adaptive Security Appliances (ASA) to Cisco Firepower Threat Defense (FTD) managed locally by Firepower Device Manager (FDM).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of RA VPN configuration on FDM.
- Working of DAP and Hostscan on ASA.
- Basic knowledge of REST API and FDM Rest API Explorer.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco FTD running version 6.7.0
- Cisco AnyConnect Secure Mobility Clientversion 4.9.00086
- Postman or any other API development tool

Note: The information in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of

any configuration change.

Background Information

Even though FTD has Remote Access VPN (RAVPN) configuration support, it lacks support for DAP. As of release 6.7.0, API support is added for DAP on the FTD. It is intended to support the very basic use case of migration from ASA to FTD. Users who have DAP configured on their ASA's and are in the process of migrating to FTD's now have a path to migrate their DAP configuration along with their RA VPN configuration.

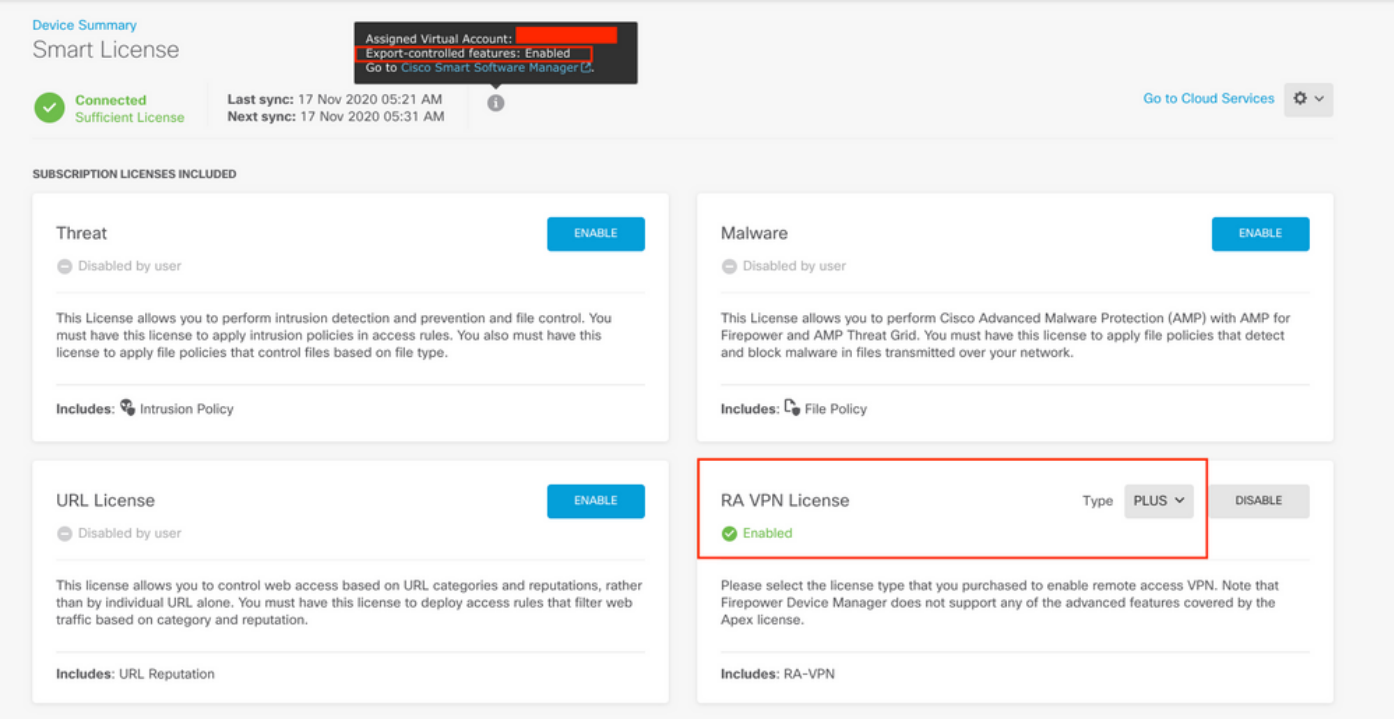
In order to successfully migrate DAP configuration from ASA to FTD, ensure these conditions:

- ASA with DAP/Hostscan configured.
- TFTP/FTP server access from the ASA or ASDM access to the ASA.
- Cisco FTD running version 6.7.0 and above managed by Firepower Device Manager (FDM).
- RA VPN configured and working on FTD.

Licensing

- FTD registered to the smart licensing portal with Export Controlled Features enabled (in order to allow RA VPN configuration tab to be enabled).
- Any one of the AnyConnect Licenses enabled (APEX, Plus, or VPN-Only).

In order to check the licensing: Navigate to **Devices > Smart Licenses**



Feature Limitations

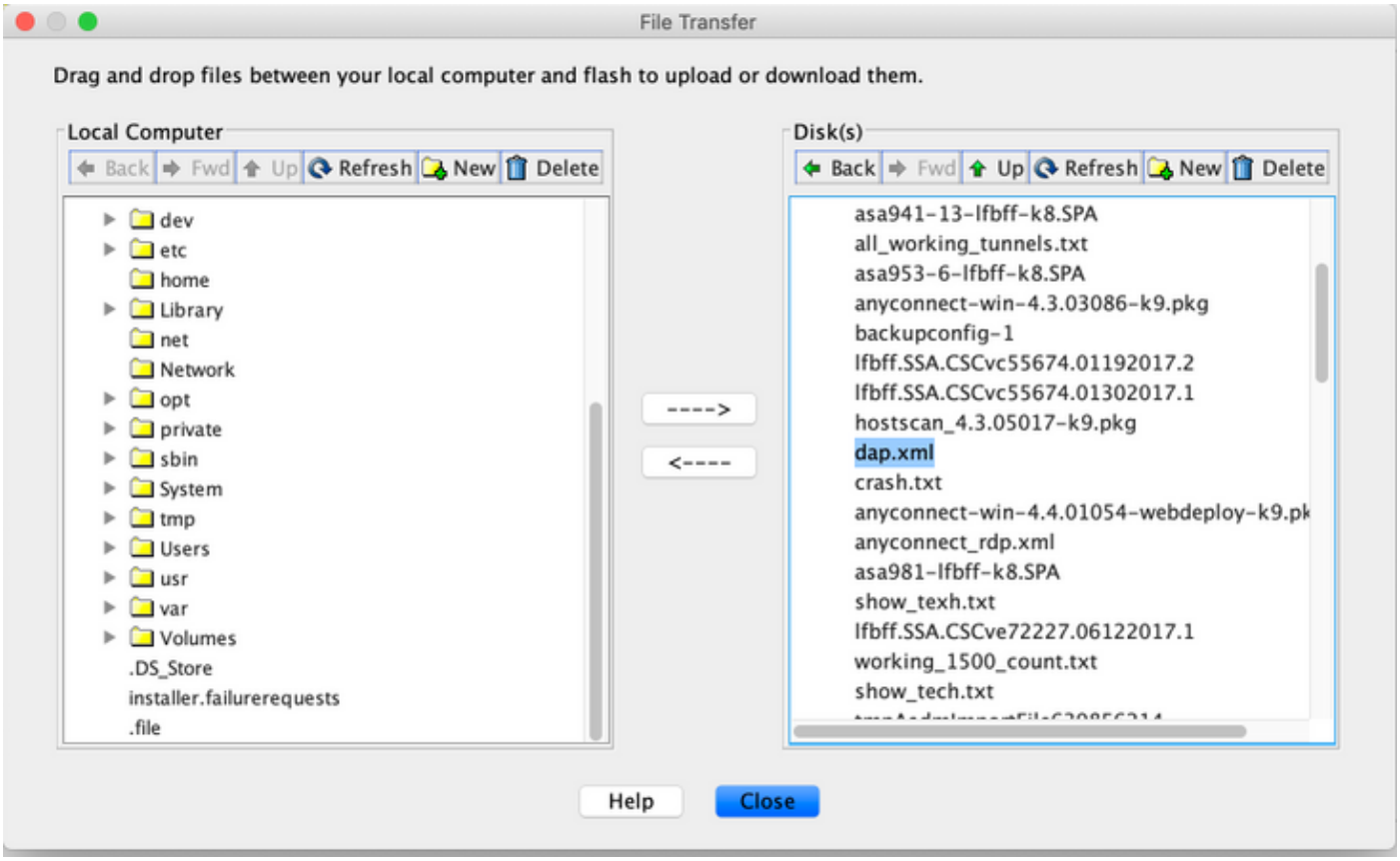
- These features are only supported via FDM/FTD REST API interface.
- DAP name cannot contain space characters with REST API.

Configuration

Step 1. Copy **dap.xml** from ASA to your local PC / TFTP Server. There are two ways to achieve the same:

ASDM:

Navigate to **Tools > File Management > FIle Transfer >Between Local PC and Flash**.



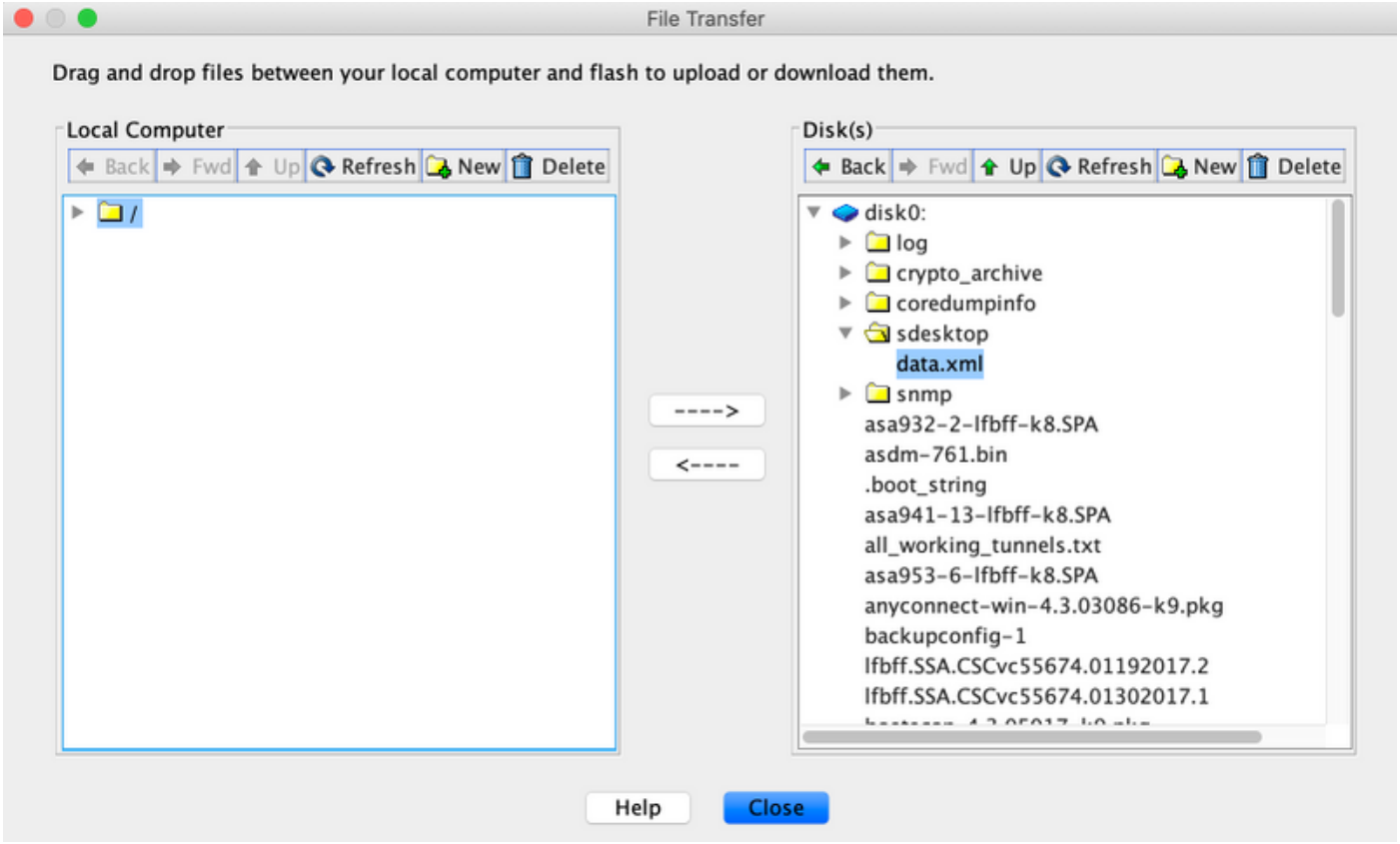
CLI:

```
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
```

Step 2. Copy the hostscan config file (data.xml) and hostscan image from ASA to the local device.

ASDM:

Navigate to **Tools** > **File Management > FIle Transfer >Between Local PC and Flash**.



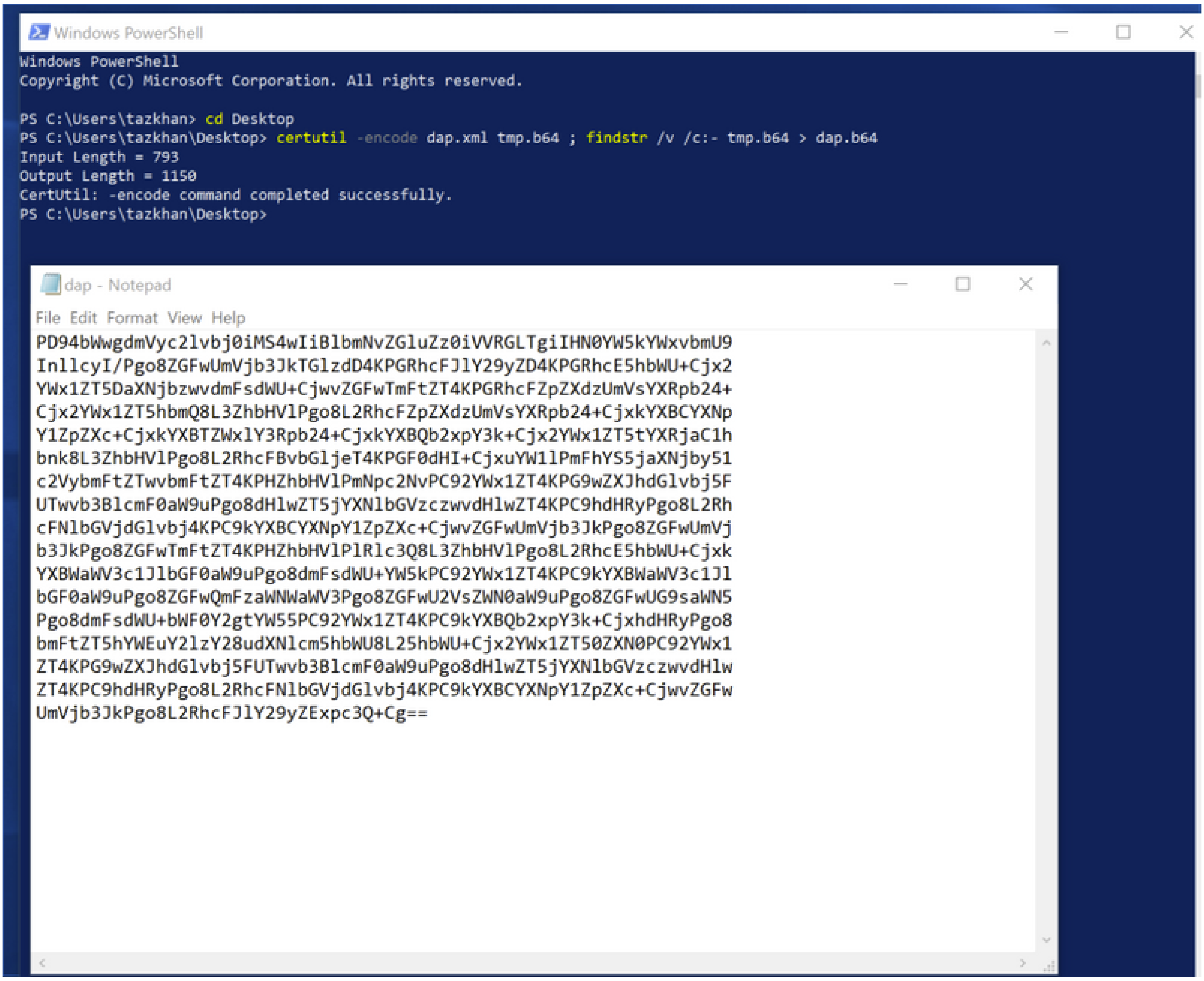
CLI:

```
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#
```

Step 3. Get the base64-encoded value of **dap.xml** and **data.xml**.

On Mac: **base64 -i <file>**

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



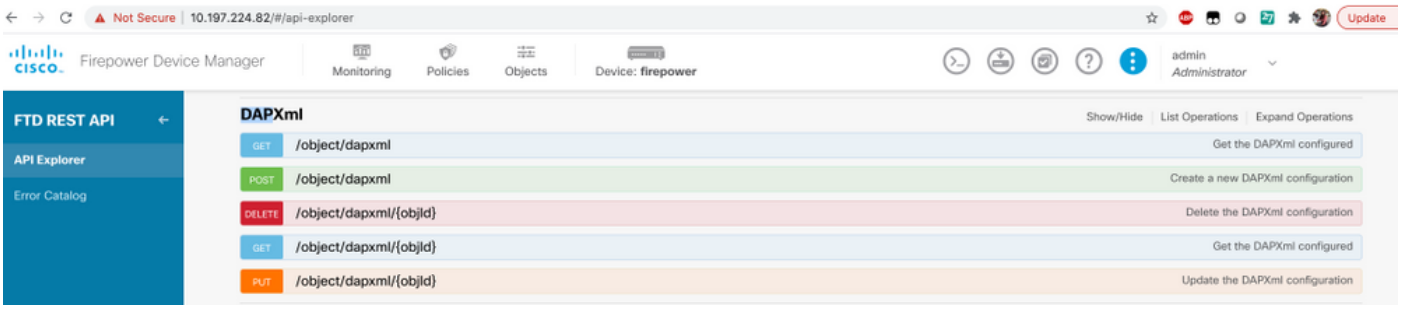
Follow the same procedure for data.xml.

Step 4. Launch the API Explorer of the FTD on a Browser Window.

Navigate to **https://<FTD Management IP>/api-explorer**

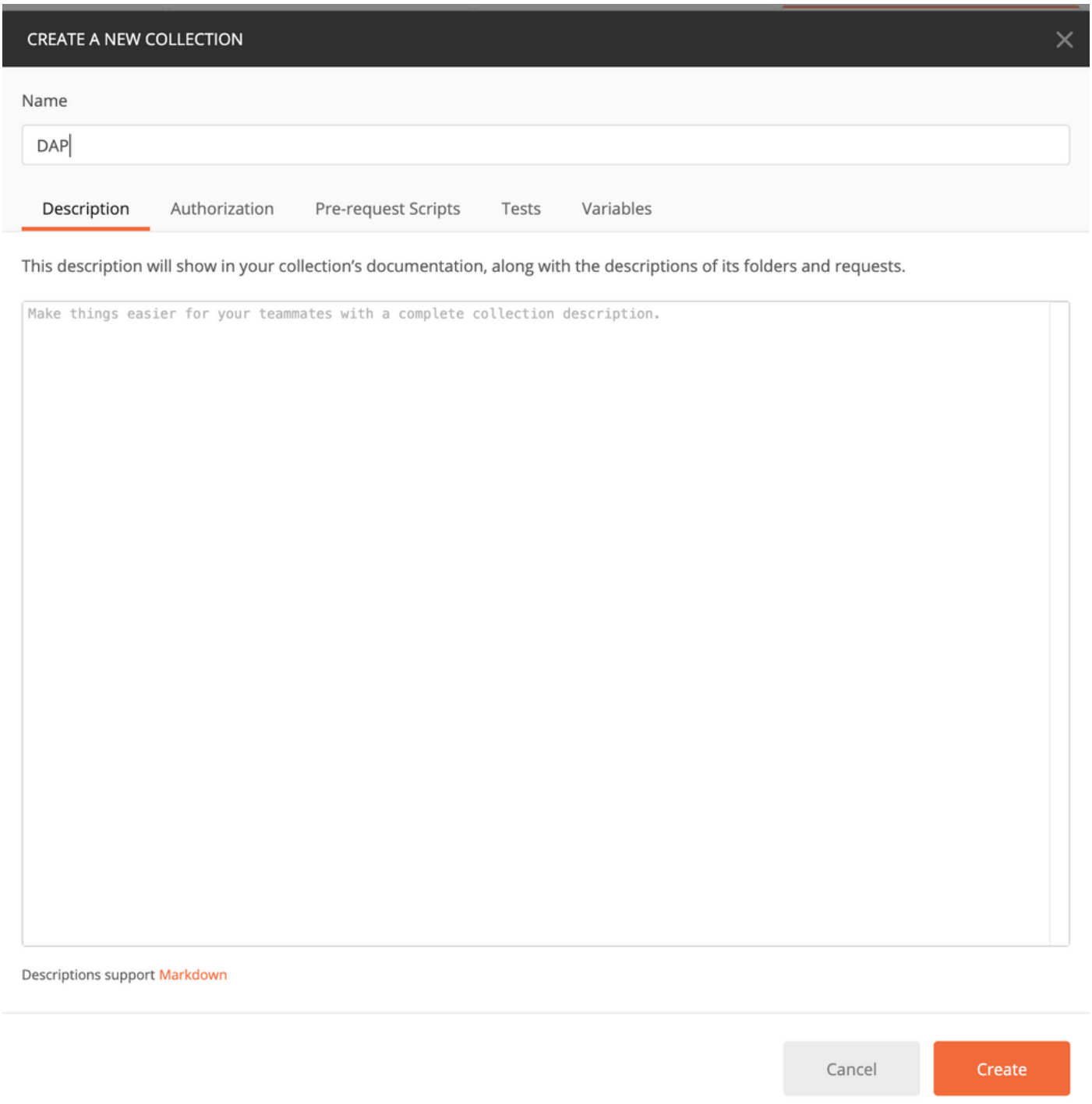
This contains the entire list of API's available on the FTD. It is divided based on the main feature with multiple GET/POST/PUT/DELETE requests which is supported by the FDM.

DAPXml and **HostScanPackageFile** are the API used.



Step 5. Add a Postman collection for DAP.

Provide a **Name** for the collection. Click on **Create**, as shown in this image.



Step 6. Add a new request **Auth** to create a login POST request to the FTD in order to get the token to authorize any POST/GET/PUT requests. Click on **Save**.