# DAP and HostScan Migration from ASA to FDM through REST API

## Contents

Introduction Prerequisites Requirements Components Used Background Information Licensing Feature Limitations Configuration Verify Deployment Verification from FTD GUI Deployment Verification from FTD CLI Troubleshoot

# 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

# **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

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

On Mac: base64 -i <file>

#### tazkhan@TAZKHAN-M-32A3 Desktop % base64 -i dap.xml

PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9InllcyI/Pgo8ZGFwUmVjb3JkTGlzdD4KPGRhcFJlY29yZD4 KPGRhcE5hbWU+Cjx2YWx1ZT5XaW5kb3dzPC92YWx1ZT4KPC9kYXBOYW1lPgo8ZGFwVmlld3NSZWxhdGlvbj4KPHZhbHV1PmFuZDwvdmFsdWU+Cj wvZGFwVmlld3NSZWxhdGlvbj4KPGRhcEJhc2ljVmlldz4KPGRhcFNlbGVjdGlvbj4KPGRhcFBvbGljeT4KPHZhbHV1Pm1hdGNoLWFueTwvdmFsd WU+CjwvZGFwUG9saWN5Pgo8YXR0cj4KPG5hbWU+YWFhLmNpc2NvLnVzZXJuYW11PC9uYW11Pgo8dmFsdWU+Y2lzY288L3ZhbHV1Pgo8b3BlcmF0 aW9uPkVRPC9vcGVyYXRpb24+Cjx0eXB1PmNhc2VsZXNzPC90eXB1Pgo8L2F0dHI+CjwvZGFwUZVsZWN0aW9uPgo8ZGFwUZVsZWN0aW9uPgo8ZGF wUG9saWN5Pgo8dmFsdWU+bWF0Y2gtYW55PC92YWx1ZT4KPC9kYXB0b2xpY3k+CjxkYXBTdWJTZWx1Y3Rpb24+CjxkYXBQb2xpY3k+Cjx2YWx1ZT 5tYXRjaC1hbGw8L3ZhbHV1Pgo8b2RhcFBvbG1jeT4KPGF0dHI+CjxuYW11PmVuZHBvaW50LmFueWNvbm51Y3QucGxhdGZvcm08L25hbWU+Cjx2Y Wx1ZT53aW48L3ZhbHV1Pgo8b3B1cmF0aW9uPkVRPC9vcGVyYXRpb24+CjwvYXR0cj4KPC9kYXBTdWJTZWx1Y3Rpb24+CjwvZGFwUZVsZWN0aW9u Pgo8L2RhcEJhc21jVmlldz4KPC9kYXBSZWNvcmQ+CjxkYXBSZWNvcmQ+CjxkYXBOYW11Pgo8dmFsdWU+YTwvdmFsdWU+CjwvZGFwTFtZT4KPGR hcFzpZXdzUmVsYXRpb24+Cjx2YWx1ZT5hbmQ8L3ZhbHV1Pgo8L2RhcFZpZXdzUmVsYXRpb24+CjwvZGFwUmVjb3JkPgo8L2RhcFJ1Y29yZExpc3 Q+Cg==

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

2 Windows PowerShell		-	×
<pre>Windows PowerShell Copyright (C) Microsoft Corporation. All rights reserved. PS C:\Users\tazkhan&gt; cd Desktop PS C:\Users\tazkhan\Desktop&gt; certutil -encode dap.xml tmp.b64 ; findstr /v /c:- tmp.b64 Input Length = 793 Output Length = 1150 CertUtil: -encode command completed successfully.</pre>	> dap.b64		
PS C:\Users\tazkhan\Desktop>			
Image: Construct State   File Edit Format View Help   PD94bWwgdmVyc21vbj0iMS4wIiB1bmNvZG1uZz0iVVRGLTgiIHN0YW5kYWxvbmU9   InllcyI/Pgo8ZGFwUmVjb3JkTG1zdD4KPGRhcFJ1Y29yZD4KPGRhcE5hbWU+Cjx2   YWx1ZT5DaXNjbzwvdmFsdWU+CjwvZGFwTmFtZT4KPGRhcFZpZXdzUmVsYXRpb24+   Cjx2YWx1ZT5hbmQ8L3ZhbHV1Pgo8L2RhcFZpZXdzUmVsYXRpb24+cjxkYXBCYXNp   Y1ZpZXc+CjxkYXBTZWx1Y3Rpb24+cjxkYXBQb2xpY3k+cjx2YWx1ZT5tYXRjaC1h   bnk8L3ZhbHV1Pgo8L2RhcFBvbG1jeT4KPGF0dH1+cjxuYW11PmFhYS5jaXNjby51   c2WybmEtZTwybmEtZT4KPBL2hHV12mNnc2NvPG02YWw1ZT4KPG0w271hd51vbi55	_	×	
C2VybmFt2TWVbmFt2T4KPH2hbHv1Pmmpc2NVPC92YWX12T4KPG9w2XJhdG1Vbj5F UTwvb3B1cmF0aW9uPgo8dH1wZT5jYXNlbGVzczwvdH1wZT4KPC9hdHRyPgo8L2Rh cFNlbGVjdG1vbj4KPC9kYXBCYXNpY1ZpZXc+CjwvZGFwUmVjb3JkPgo8ZGFwUmVj b3JkPgo8ZGFwTmFtZT4KPHZhbHV1P1R1c3Q8L3ZhbHV1Pgo8L2RhcE5hbWU+Cjxk YXBWaWV3c1JlbGF0aW9uPgo8dmFsdWU+YW5kPC92YWx1ZT4KPC9kYXBWaWV3c1J1 bGF0aW9uPgo8ZGFwQmFzaWNWaWV3Pgo8ZGFwU2VsZWN0aW9uPgo8ZGFwUG9saWN5 Pgo8dmFsdWU+bWF0Y2gtYW55PC92YWx1ZT4KPC9kYXBQb2xpY3k+CjxhdHRyPgo8 bmFtZT5hYWEuY21zY28udXN1cm5hbWU8L25hbWU+Cjx2YWx1ZT50ZXN0PC92YWx1 ZT4KPG9wZXJhdG1vbj5FUTwvb3B1cmF0aW9uPgo8dH1wZT5jYXNlbGVzczwvdH1w ZT4KPC9hdHRyPgo8L2RhcFNlbGVjdG1vbj4KPC9kYXBCYXNpY1ZpZXc+CjwvZGFw UmVjb3JkPgo8L2RhcFJ1Y29yZExpc3Q+Cg==			
		~ ~	

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.

🗧 🔶 C 🔺 Not Secure   10.197.224.82/#/api-explorer			
cisco. Firepower Device	e Manager 🖗 🔅 🛱 manager Monitoring Policies Objects Device: firepower	(>) (admin Administrator	
FTD REST API 🔶	DAPXml	Show/Hide   List Operations   Expand Operations	
ADI Explorer	GET /object/dapxml	Get the DAPXml configured	
AFTEXPIORE	Post /object/dapxml	Create a new DAPXml configuration	
Error Catalog	CELETE /object/dapxml/{objid}	Delete the DAPXml configuration	
	GET /object/dapxml/{objld}	Get the DAPXml configured	
	evr /object/dapxml/{objid}	Update the DAPXml configuration	

Step 5. Add a Postman collection for DAP.

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

CREATE A NEW C	COLLECTION				×
Name					
DAP					
Description	Authorization	Pre-request Scripts	Tests	Variables	

This description will show in your collection's documentation, along with the descriptions of its folders and requests.

Make things easier for your teammates with a complete collection description.

Descriptions support Markdown

Cancel	Create
--------	--------

**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**.