

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

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Lizenzierung](#)

[Einschränkungen bei Funktionen](#)

[Konfiguration](#)

[Überprüfen](#)

[Bereitstellungsüberprüfung über FTD-GUI](#)

[Bereitstellungsüberprüfung von FTD CLI](#)

[Fehlerbehebung](#)

## 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 konfigurierter 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**.

The screenshot displays the 'Smart License' page in the Cisco Smart Licensing portal. At the top, it shows 'Device Summary' and 'Smart License' status as 'Connected' with a 'Sufficient License'. A notification box indicates 'Assigned Virtual Accounts: [redacted]', 'Export-controlled features: Enabled', and a link to 'Go to Cisco Smart Software Manager'. Below this, the 'SUBSCRIPTION LICENSES INCLUDED' section lists four licenses:

- Threat License:** Disabled by user. Description: 'This License allows you to perform intrusion detection and prevention and file control. You must have this license to apply intrusion policies in access rules. You also must have this license to apply file policies that control files based on file type.' Includes: Intrusion Policy. An 'ENABLE' button is visible.
- Malware License:** Disabled by user. Description: 'This License allows you to perform Cisco Advanced Malware Protection (AMP) with AMP for Firepower and AMP Threat Grid. You must have this license to apply file policies that detect and block malware in files transmitted over your network.' Includes: File Policy. An 'ENABLE' button is visible.
- URL License:** Disabled by user. Description: 'This license allows you to control web access based on URL categories and reputations, rather than by individual URL alone. You must have this license to deploy access rules that filter web traffic based on category and reputation.' Includes: URL Reputation. An 'ENABLE' button is visible.
- RA VPN License:** Enabled. Description: 'Please select the license type that you purchased to enable remote access VPN. Note that Firepower Device Manager does not support any of the advanced features covered by the Apex license.' Includes: RA-VPN. A dropdown menu is set to 'PLUS' and a 'DISABLE' button is visible.

## Einschränkungen bei Funktionen

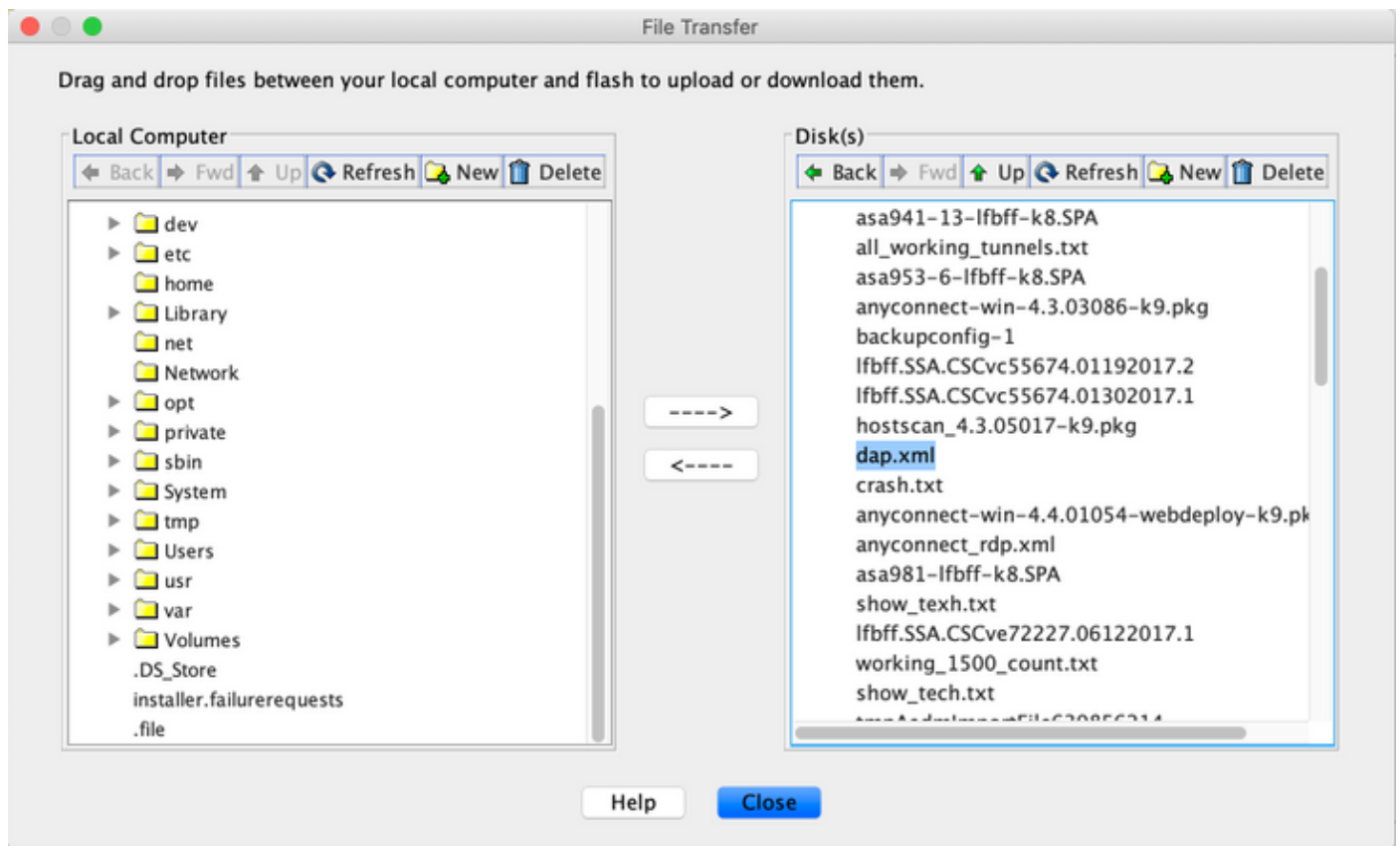
- Diese Funktionen werden nur über die REST-API-Schnittstelle FDM/FTD unterstützt.
- Der DAP-Name darf keine Leerzeichen mit REST API enthalten.

## 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

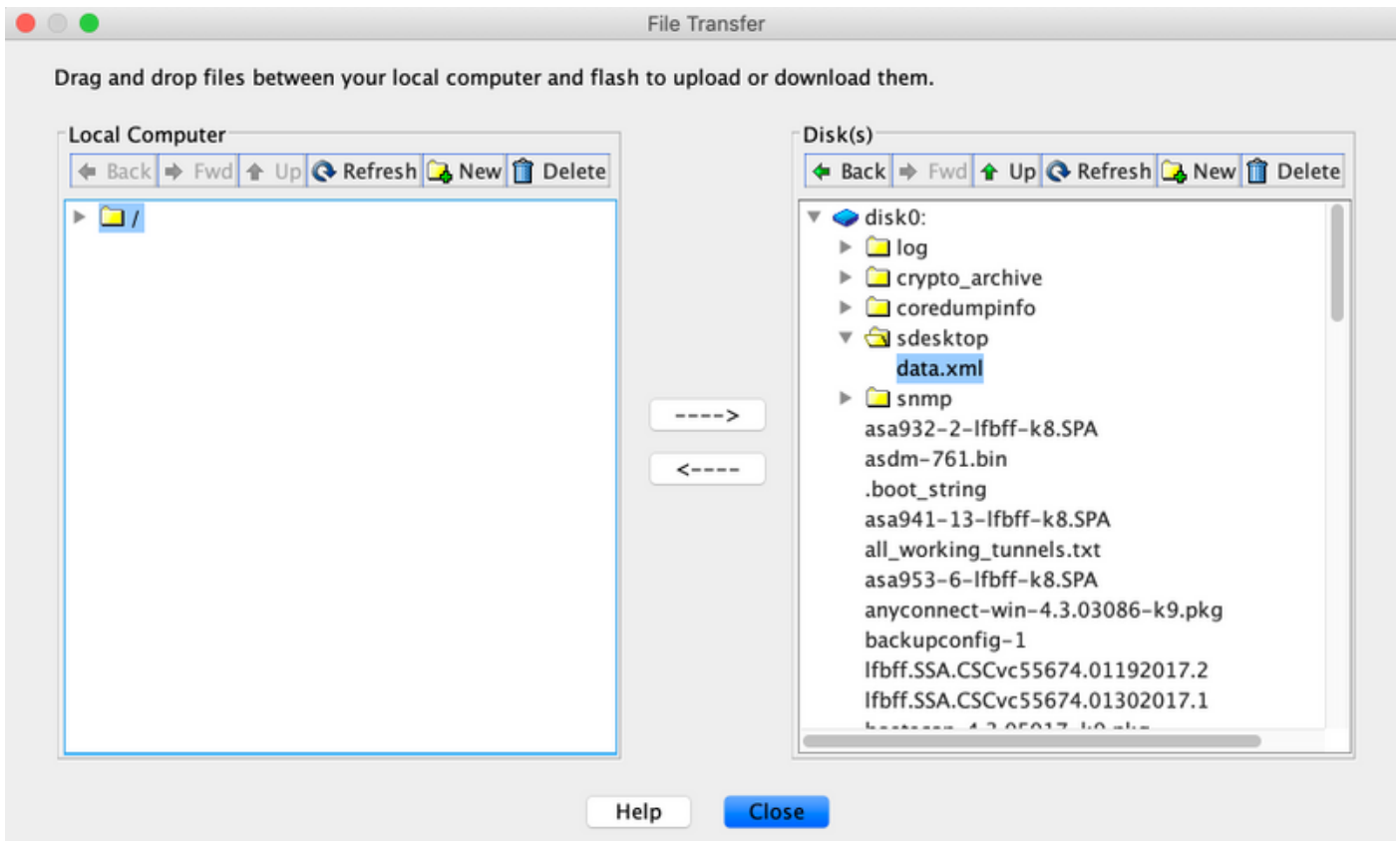
Destination filename [dap.xml]?

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

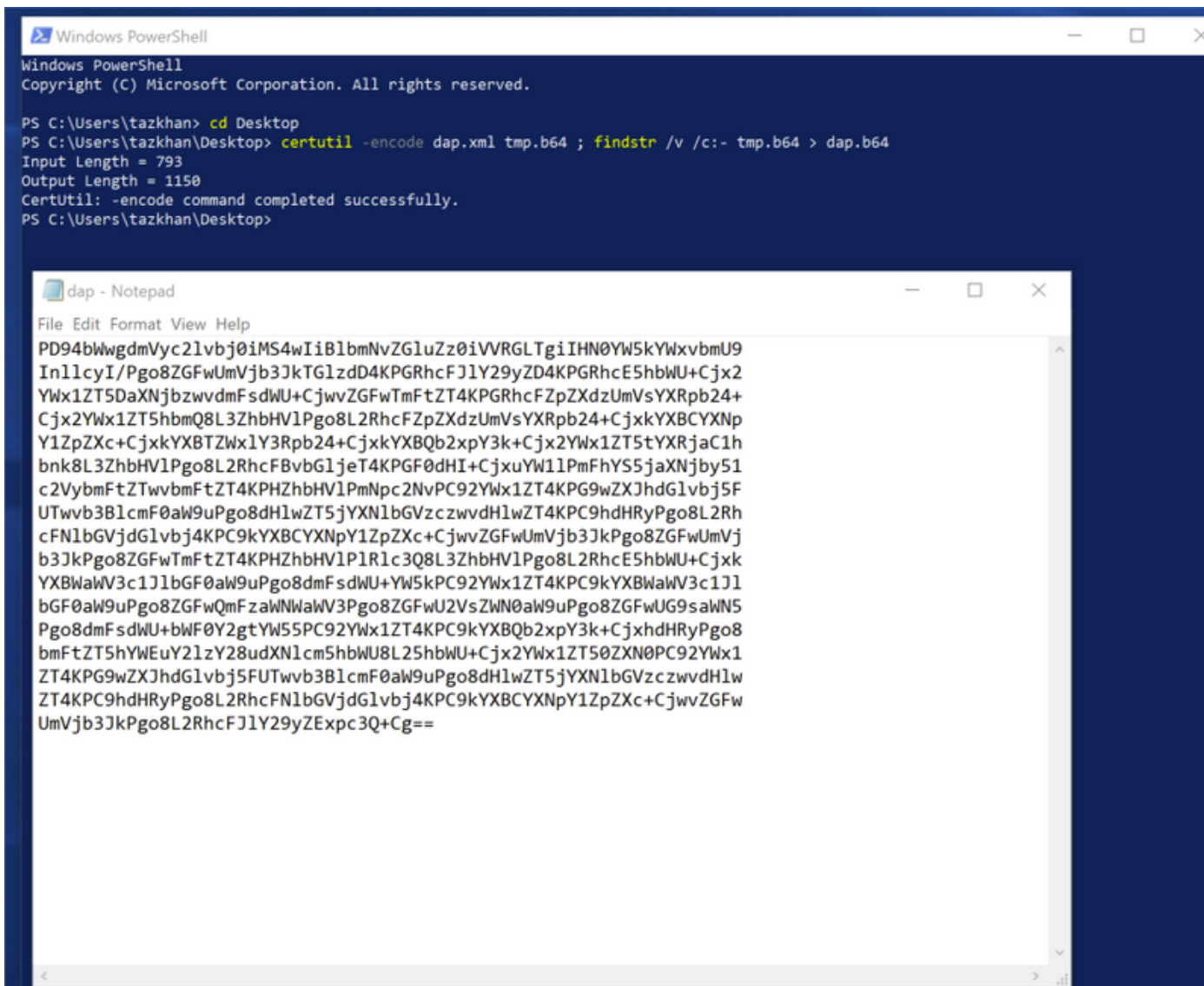
Destination filename [hostscan_4.9.03047-k9.pkg]?
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
56202408 bytes copied in 34.830 secs (1653012 bytes/sec)
ASA#
```

**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
PD94bWwgdMvYc2l1bWVj0iMS4wIiB1bWVZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9InllcyI/Pgo8ZGFwUmVjb3JkTG1zdD4KPGRhcFJlY29yZD4
KPGRhcE5hbWU+Cjx2YXw1ZT5XaW5kb3dzPC92YXw1ZT4KPC9kYXBOYW1lPgo8ZGFwVmlld3NSZWxhdG1vbG1vbj4KPHZhbHVlPmFuZDwvdmFsdWU+Cj
wvZGFwVmlld3NSZWxhdG1vbG1vbj4KPGRhcEJhc2l1jVmlldz4KPGRhcFNlbGVjdG1vbG1vbj4KPGRhcFBvbG1jeT4KPHZhbHVlPm1hdGNoLWFueTwvdmFsd
WU+CjwvZGFwUG9saWN5Pgo8YXR0cj4KPG5hbWU+YWVhLmNpc2NvLnVzZXJlYXN0PC9uYXw1Pgo8dmFsdWU+Y2l1Z288L3ZhbHVlPgo8b3B1cmF0
aW9uPkVVRPC9vcGVyYXRpb24+Cjx0eXB1PmNhc2VsZXNzPC90eXB1Pgo8L2F0dHI+CjwvZGFwU2VsZWN0aW9uPgo8ZGFwU2VsZWN0aW9uPgo8ZGF
wUG9saWN5Pgo8dmFsdWU+bW0yZ2tYW55PC92YXw1ZT4KPC9kYXBOYW1lPgo8ZGFwU2VsZWN0aW9uPgo8ZGFwU2VsZWN0aW9uPgo8ZGFwU2VsZWN0aW9u
5tYXRjaC1hbGw8L3ZhbHVlPgo8L2RhcFBvbG1jeT4KPGF0dHI+CjxuYXw1PmVlPmVhZBvaW50LmFueWVvbm5lY3QucGxhdGZvc08L25hbWU+Cjx2Y
Wx1ZT53aW48L3ZhbHVlPgo8b3B1cmF0aW9uPkVVRPC9vcGVyYXRpb24+CjwvYXR0cj4KPC9kYXBTdWJlYXN0PC9uYXw1Pgo8dmFsdWU+Y2l1Z288L3ZhbHVlPgo8b3B1cmF0
aW9uPgo8L2RhcEJhc2l1jVmlldz4KPC9kYXBSZWVvc0+CjxkYXBSZWVvc0+CjxkYXBOYW1lPgo8dmFsdWU+Y2l1Z288L3ZhbHVlPgo8b3B1cmF0aW9uPgo8L2RhcFJlY29yZExp
c3Q+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.

The screenshot shows the Cisco Firepower Device Manager API Explorer interface. The browser address bar displays '10.197.224.82/#api-explorer'. The page title is 'FTD REST API'. The left sidebar contains 'API Explorer' and 'Error Catalog'. The main content area is titled 'DAPXml' and lists several REST API endpoints with their methods and descriptions:

Method	Endpoint	Description
GET	/object/dapxml	Get the DAPXml configured
POST	/object/dapxml	Create a new DAPXml configuration
DELETE	/object/dapxml/{objId}	Delete the DAPXml configuration
GET	/object/dapxml/{objId}	Get the DAPXml configured
PUT	/object/dapxml/{objId}	Update the DAPXml configuration

**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.

The screenshot shows the 'CREATE A NEW COLLECTION' dialog in Postman. The 'Name' field contains 'DAP'. Below the name field are tabs for 'Description', 'Authorization', 'Pre-request Scripts', 'Tests', and 'Variables'. The 'Description' tab is selected and contains the text: 'Make things easier for your teammates with a complete collection description.' At the bottom of the dialog are 'Cancel' and 'Create' buttons.

**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**.

