

Configure AnyConnect Modules for Remote Access VPN On FTD

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configuration](#)

[Configuration on Firepower Management Center \(FMC\)](#)

[Configuration on Firepower Device Manager \(FDM\)](#)

[Verify](#)

[Troubleshoot](#)

Introduction

This document describes how to configure AnyConnect Modules for Remote Access VPN (RA VPN) configuration that pre-exists on a Firepower Threat Defense (FTD) managed by a Firepower Management Center (FMC) through Firepower Device Manager (FDM).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic understanding of RA VPN working.
- Understanding of navigation through the FMC/FDM.
- Basic knowledge of REST API and FDM Rest API Explorer.

Components Used

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

- Cisco Firepower Management Center (FMC) version 6.7.0
- Cisco Firepower Threat Defense (FTD) version 6.7.0
- Cisco Firepower Device Manager (FDM) version 6.7.0
- Cisco AnyConnect Secure Mobility Client running 4.9.0086
- Postman or any other API development tool

Note: FMC/FDM do not have an inbuilt Profile Editor and the [AnyConnect Profile Editor](#) for Windows has to be used to create a profile.

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

The Cisco AnyConnect Secure Mobility Client is not limited to its support as a VPN client, it has a number of other options that can be integrated as modules. Following modules are supported for Anyconnect :

- **Start Before Login (SBL):** This module allows the user to establish a VPN connection into the enterprise before logging into Windows.
- **Diagnostic and Reporting Tool (DART):** This module is used to perform both diagnostics and reporting about the AnyConnect installation and connection. DART works by assembling the logs, status, and diagnostic information for analysis.
- **Advanced Malware Protection (AMP):** This module provides a cloud-delivered next-generation solution to detect, prevent, and respond to various threats.
- **ISE Posture:** Cisco Identity Services Engine (ISE) provides a next-generation identity and access control policy. This module provides the ability to identify the Operating System (OS), the AntiVirus, the AntiSpyware, etc that are currently installed on a host. This information is then used along with a policy to determine whether the host will be able to connect to the network.
- **Network Visibility Module:** The network visibility module monitors an endpoint application usage to uncover potential behavior anomalies and to make more informed network design decisions.
- **Umbrella:** Cisco Umbrella Roaming is a cloud-delivered security service that protects devices when they are off the corporate network.
- **Web Security:** Cisco Web Security Appliance (WSA), powered by Cisco Talos, protects the endpoint by automatically blocking risky sites and testing unknown sites.
- **Network Access Manager:** Network Access Manager provides a secure Layer 2 network in accordance with its policies. It detects and selects the optimal Layer 2 access network and performs device authentication for access to both wired and wireless networks.
- **Feedback:** This module collects the information and periodically sends it to the server. It helps the product team to improve the quality, reliability, performance, and user experience of AnyConnect.

In Firepower 6.7, FMC UI, and FTD Device REST API support is added to enable seamless deployment of all the mentioned AnyConnect Modules.



This table lists the Profiles Extensions and associated Module types needed to successfully deploy the endpoint functionality.

Profile Extensions

- .fsp
- .asp or .xml
- .sip or .xml
- .nvmsp or .xml
- .nsp or .xml
- .json or .xml
- .wsp or .xml

Module Type

- FEEDBACK
- AMP_ENABLER
- ISE_POSTURE
- NETWORK_VISIBILITY
- NETWORK_ACCESS_MANAGER
- UMBRELLA
- WEB_SECURITY

Note: DART and SBL modules do not require any Profile.

Note: No additional licensing is required for the use of this feature.

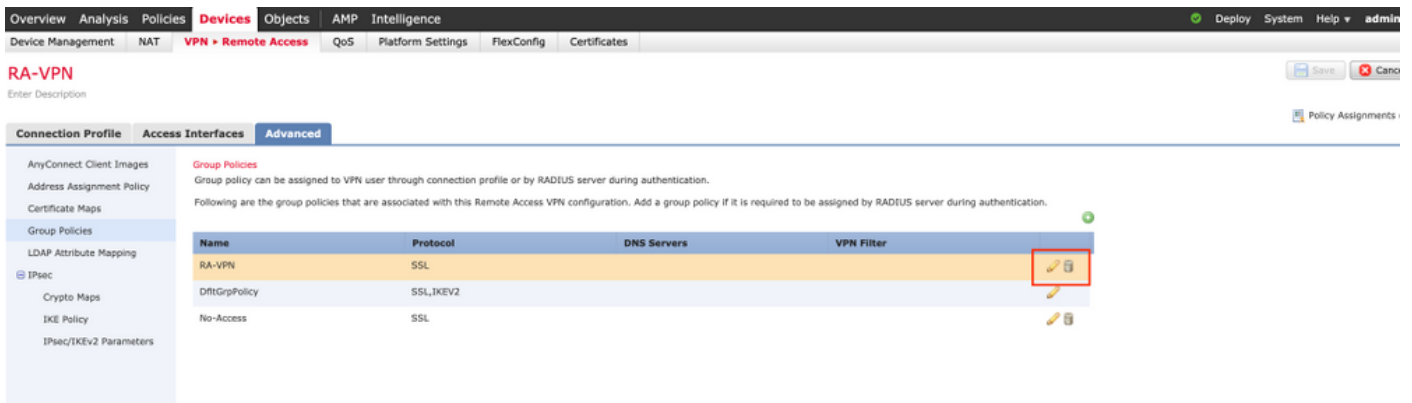
Configuration

Configuration on Firepower Management Center (FMC)

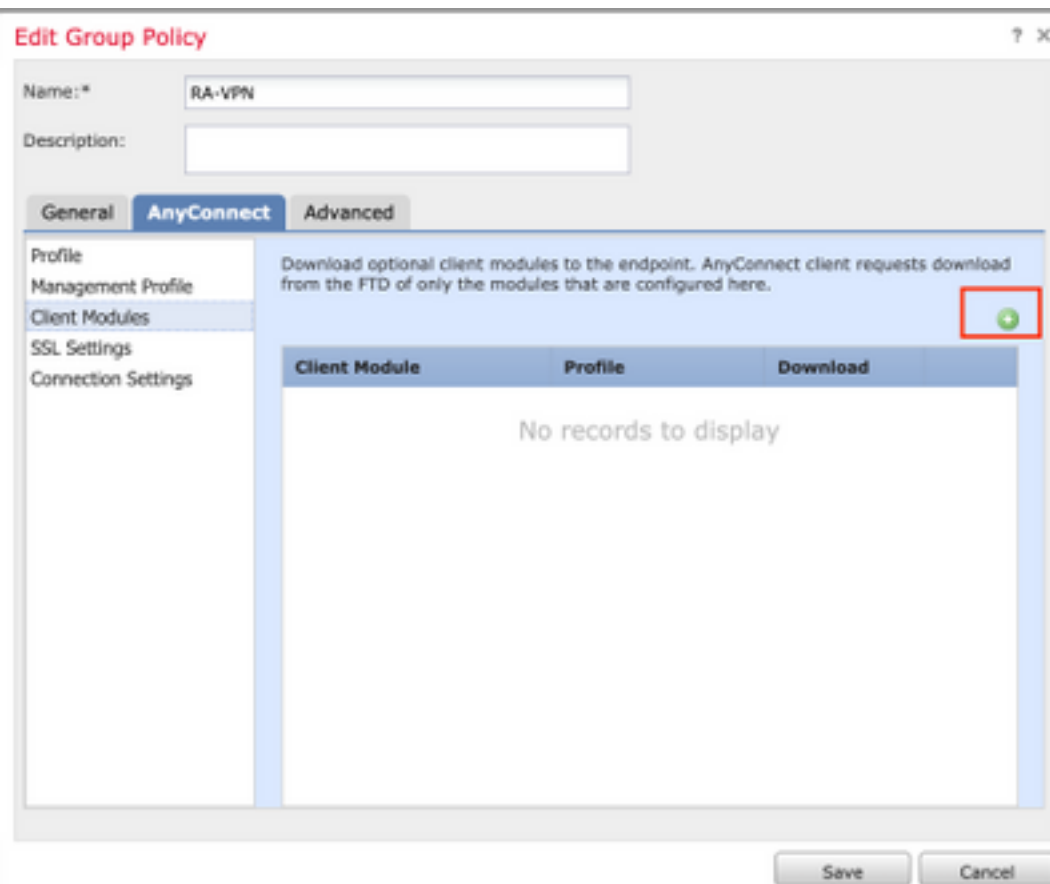
Step 1. Navigate to **Device > VPN > Remote Access** and click on **Edit** for the RA VPN configuration.



Step 2. Navigate to **Advanced > Group Policies** and click on **Edit** for the concerned Group-policy, as shown in this image.



Step 3. Navigate to **AnyConnect > Client Modules** and click on **+** to add the Modules, as shown in this image.



For the purpose of demonstration, Deployment of AMP, DART, and SBL modules are shown.

Step 4. Select the **DART** module and click on **Add**, as shown in this image.

Add Client Module ? X

Client Module: DART

Profile to download: [Empty]

Enable module download:

Add Cancel

Step 5. Click on + to add another module and select **Start Before Login** module, as shown in this image.

Add Client Module ? X

Client Module: Start Before Login

Profile to download: [Empty]

Enable module download:

Add Cancel

Note: This step allows you to download the SBL Module. SBL also has to enable in anyconnect client profile, which is uploaded as you navigate to **AnyConnect > Profile** under the Group Policy.

Step 6. Click on + to add another module and select **AMP Enabler**. Click on + to Add a Client Profile, as shown in this image.

Add Client Module ? X

Client Module: AMP Enabler

Profile to download: [Empty] +

Enable module download:

Add Cancel

Provide the **Name** of the Profile and upload the **AMP Profile**. Click on **Save**, as shown in this image.

The screenshot shows a dialog box titled "Add AnyConnect File" with a red border. It contains the following fields and controls:

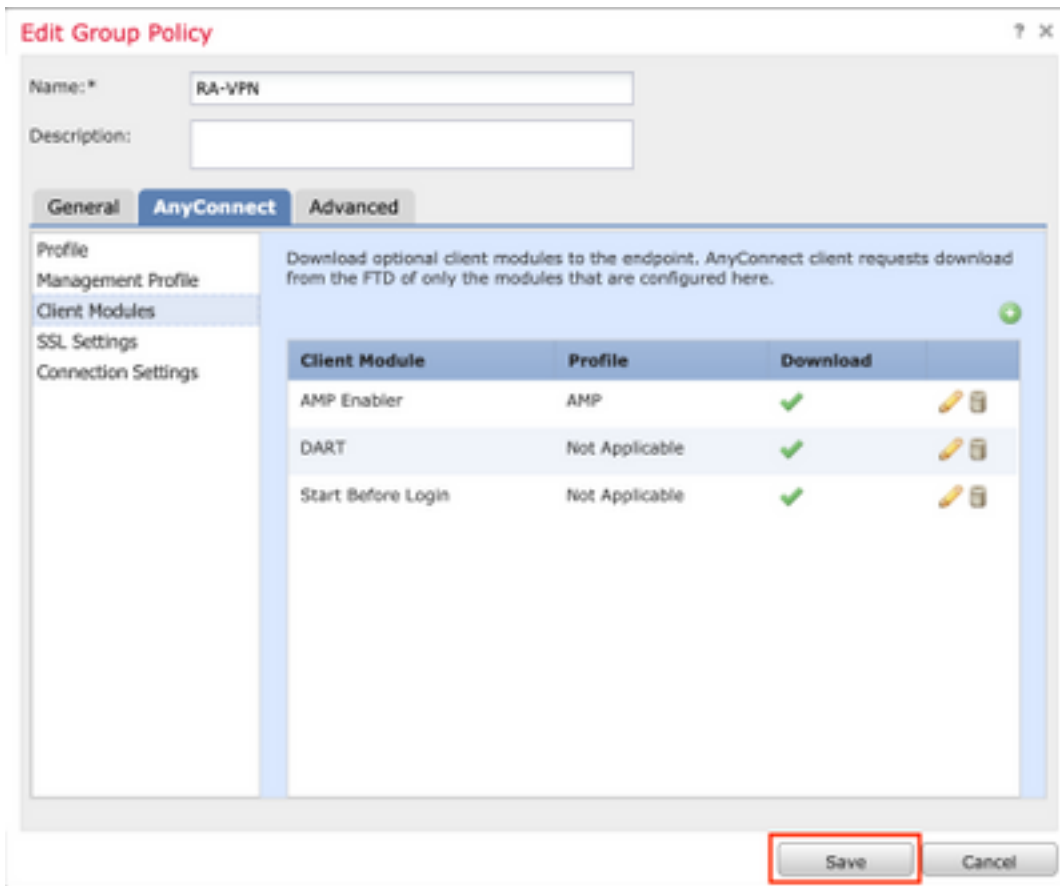
- Name:*** Text input field containing "AMP".
- File Name:*** Text input field containing "Amp.asp" and a "Browse.." button.
- File Type:*** Dropdown menu set to "AMP Enabler Service Profile".
- Description:** Empty text input field.
- Buttons: "Save" and "Cancel".

Choose the profile created in the previous step and click on **Enable Module download checkbox**, as shown in this image.

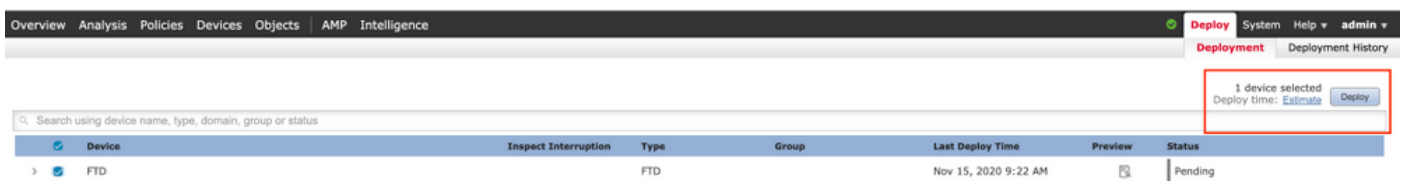
The screenshot shows a dialog box titled "Add Client Module" with a red border. It contains the following fields and controls:

- Client Module** Dropdown menu set to "AMP Enabler".
- Profile to download** Dropdown menu set to "AMP" with a green plus icon to its right.
- Enable module download** Checkbox that is checked.
- Buttons: "Add" and "Cancel".

Step 7. Click on **Save** once all the desired modules are added.



Step 8. Navigate to **Deploy > Deployment** and deploy the configuration to the FTD.



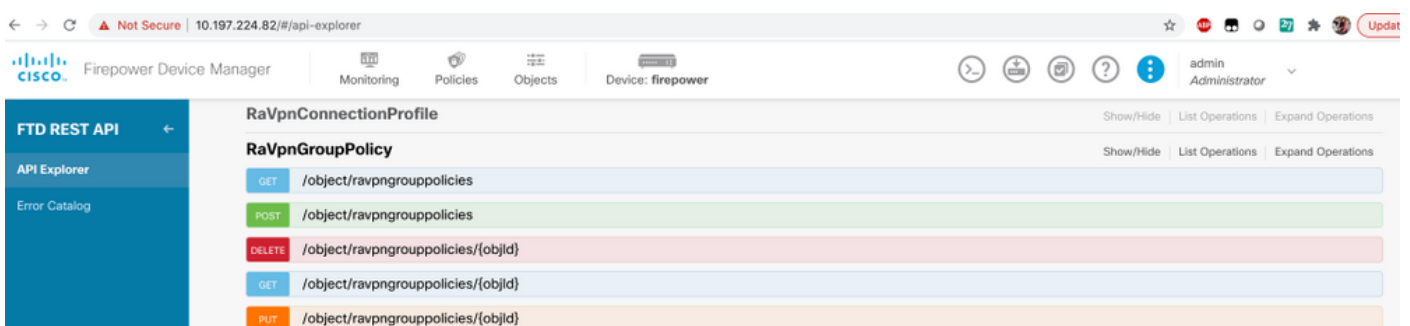
Configuration on Firepower Device Manager (FDM)

Step 1. 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 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.

RaVpnGroupPolicy is the API used.



Step 2. Add a Postman collection for **AnyConnect Modules**. Provide a **Name** for the collection. Click on **Create**.

CREATE A NEW COLLECTION

Name

AnyConnect Module

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.

AnyConnect Module

Descriptions support [Markdown](#)

Cancel Create

Step 3. 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**.

AnyConnect Module ☆
0 requests

This collection
collection and

- ➔ Share Collection
- 🔒 Manage Roles
- A| Rename ⌘E
- ✎ Edit
- 🔗 Create a fork
- 🔗 Create Pull Request
- 🔗 Merge changes
- GET** Add Request
- 📁 Add Folder

SAVE REQUEST

Requests in Postman are saved in collections (a group of requests).

[Learn more about creating collections](#)

Request name

Auth

Request description (Optional)

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

Descriptions support [Markdown](#)

Select a collection or folder to save to:

Search for a collection or folder

AnyConnect Module

+ Create Folder

Cancel

Save to AnyConnect Module

The Body of the POST request must contain these:

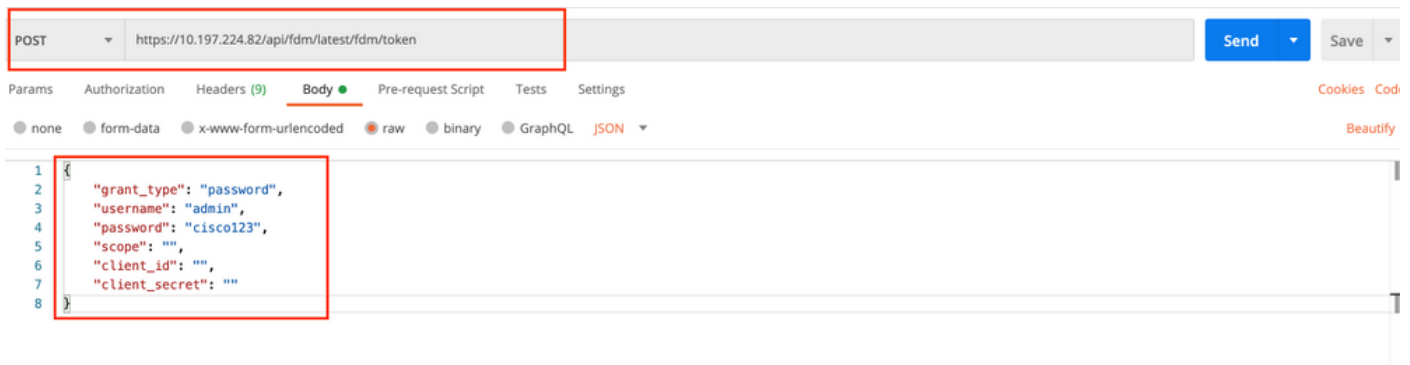
Type raw - JSON (application/json)

grant_type password

username Admin Username in order to log in to the FTD

password The password associated with the admin user account

POST Request: <https://<FTD Management IP>/api/fdm/latest/fdm/token>



The Body of the Response contains the access token which is used in order to send any PUT/GET/POST requests to/from the FTD.



Step 4. Create a **Get Group Policy** request to add get details of the existing Group Policies. Click on **Save**, as shown in this image.

SAVE REQUEST

Requests in Postman are saved in collections (a group of requests).
[Learn more about creating collections](#)

Request name

Request description (Optional)

Descriptions support [Markdown](#)

Select a collection or folder to save to:

◀ AnyConnect Module [+ Create Folder](#)

POST Auth

The Authorization tab must contain this for all subsequent GET/POST requests:

Type Bearer Token

Token The access token received by running the Auth POST Request

GET REQUEST: `https://<FTD Management IP>/api/fdm/latest/object/ravpngrouppolicies`

Get Group Policy Comments 0 Examples 0

GET `https://10.197.224.82/api/fdm/latest/object/ravpngrouppolicies`

Params **Authorization** Headers (8) Body Pre-request Script Tests Settings Cookies Code

TYPE
 Bearer Token

The authorization header will be automatically generated when you send the request. [Learn more about authorization](#)

Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. [Learn more about variables](#)

Token `eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXQCJ9.eyJ2IjoiOTAwODIsInN1IjoiImFkbWluciwianR5Y2NmNDU0NzEtMjg5MyC...`

The Body of the response shows all the Group Policies configured on the device. **ID** of the Group Policy is used to update the specific Group Policy.

Pretty Raw Preview Visualize JSON

```

1  {
2  "items": [
3  {
4    "version": "ijtc7ii45gloz",
5    "name": "DfltGrpPolicy",
6    "banner": null,
7    "dnsServerGroup": null,
8    "defaultDomainName": null,
9    "simultaneousLoginPerUser": 3,
10   "maxConnectionTimeout": null,
11   "maxConnectionTimeAlertInterval": 1,
12   "vpnIdleTimeout": 30,
13   "vpnIdleTimeoutAlertInterval": 1,
14   "ipv4LocalAddressPool": [],
15   "ipv6LocalAddressPool": [],
16   "dhcpScope": null,
17   "ipv4SplitTunnelSetting": "TUNNEL_ALL",
18   "ipv6SplitTunnelSetting": "TUNNEL_ALL",
19   "ipv4SplitTunnelNetworks": [],
20   "ipv6SplitTunnelNetworks": [],
21   "splitDNSRequestPolicy": "USE_SPLIT_TUNNEL_SETTING",
22   "splitDNSDomainList": "",
23   "scepForwardingUrl": null,
24   "periodicClientCertAuthenticationInterval": 1,
25   "enableDTLS": false,
26   "enableDTLSCompression": false,
27   "sslCompression": "DISABLED",
28   "enableSSIRekey": false.

```

Pretty Raw Preview Visualize JSON

```

59  {
60  "version": "lc2t2sspzbfy7",
61  "name": "RA-VPN",
62  "banner": null,
63  "dnsServerGroup": null,
64  "defaultDomainName": null,
65  "simultaneousLoginPerUser": 3,
66  "maxConnectionTimeout": null,
67  "maxConnectionTimeAlertInterval": 1,
68  "vpnIdleTimeout": 30,
69  "vpnIdleTimeoutAlertInterval": 1,
70  "ipv4LocalAddressPool": [],
71  "ipv6LocalAddressPool": [],
72  "dhcpScope": null,
73  "ipv4SplitTunnelSetting": "TUNNEL_SPECIFIED",
74  "ipv6SplitTunnelSetting": "TUNNEL_ALL",
75  "ipv4SplitTunnelNetworks": [
76    {
77      "version": "ne3zzud5spztm",
78      "name": "Split-acl",
79      "id": "71b85ceb-27ba-11eb-9202-a5a0daf9088c",
80      "type": "networkobject"
81    }
82  ],
83  "ipv6SplitTunnelNetworks": [],
84  "splitDNSRequestPolicy": "USE_SPLIT_TUNNEL_SETTING",
85  "splitDNSDomainList": "",
86  "scepForwardingUrl": null.

```

Pretty Raw Preview Visualize JSON

```

108  "restrictVPNtoOVLANid": null,
109  "clientFirewallPrivateNetworkRules": null,
110  "clientFirewallPublicNetworkRules": null,
111  "browserProxyType": "NO_MODIFY",
112  "proxy": {
113    "serverHost": null,
114    "port": null,
115    "type": "serverhostandport"
116  },
117  "proxyExceptions": [],
118  "enabledAnyConnectModules": [],
119  "isEnabledPeriodicClientCertAuthentication": false,
120  "id": "74b60c8e-27ba-11eb-9202-594cb5cbaldf",
121  "type": "ravpngrouppolicy",
122  "links": {
123    "self": "https://10.197.224.82/api/fdm/latest/object/ravpngrouppolicies/74b60c8e-27ba-11eb-9202-594cb5cbaldf"
124  }
125  },
126  ],
127  "paging": {
128    "prev": [],
129    "next": [],
130    "limit": 10,
131    "offset": 0,
132    "count": 2,
133    "pages": 0
134  }
135  }

```

For the purpose of demonstration, Deployment of AMP, DART, and SBL modules are shown.

Step 5. Create a request to Upload a Profile. This step is needed only for the modules which

require a profile. Upload the **Profile** in **filetoUpload** section. Click on **Save**.

POST REQUEST: <https://<FTD Management IP>/api/fdm/latest/action/uploaddiskfile>

The Body of the Request must contain the Profile file added in Body in form-data format. The profile needs to be created using [AnyConnect Profile Editor for Windows](#)

The key type should be **File** for **filetoUpload**.

SAVE REQUEST

Requests in Postman are saved in collections (a group of requests).
[Learn more about creating collections](#)

Request name

Request description (Optional)

Descriptions support [Markdown](#)

Select a collection or folder to save to:

AnyConnect Module + Create Folder
POST Auth
GET Get Group Policy

POST <https://10.197.224.82/api/fdm/latest/action/uploaddiskfile>

Params Authorization Headers (10) **Body** Pre-request Script Tests Settings [Cookies](#) [Code](#)

none form-data x-www-form-urlencoded raw binary GraphQL

KEY	VALUE	DESCRIPTION	...	Bulk Edit
<input checked="" type="checkbox"/> fileToUpload	File <input type="text" value="Amp.asp X"/>			
Key	Text Value	Description		
	File			

The body of the response gives an id/filename which is used to refer to the profile with the

concerned module.



The screenshot shows a REST client interface with a JSON response. The response is displayed in a code editor with line numbers 1 through 10. The JSON object contains the following fields: "version" (null), "name" (a long alphanumeric string), "fileName" (a long alphanumeric string, highlighted with a red box), "id" (a long alphanumeric string), "type" ("fileuploadstatus"), and "links" (an object with a "self" property pointing to a URL). The status bar at the top right indicates "Status: 200 OK", "Time: 325 ms", and "Size: 911 B".

```
1 {
2   "version": null,
3   "name": "69cc2046-2897-11eb-9202-b71d409c1cf2.asp",
4   "fileName": "69cc2046-2897-11eb-9202-b71d409c1cf2.asp",
5   "id": "69cc2046-2897-11eb-9202-b71d409c1cf2.asp",
6   "type": "fileuploadstatus",
7   "links": {
8     "self": "https://10.197.224.82/api/fdm/latest/action/uploaddiskfile/69cc2046-2897-11eb-9202-b71d409c1cf2.asp"
9   }
10 }
```

Step 6. Create a request to Update **AnyConnect Profile**. This step is needed only for the modules which require a profile. Click on **Save.**, as shown in this image.

SAVE REQUEST

Requests in Postman are saved in collections (a group of requests).

[Learn more about creating collections](#)

Request name

AnyConnect Profile

Request description (Optional)

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

Descriptions support [Markdown](#)

Select a collection or folder to save to:

Search for a collection or folder

AnyConnect Module

+ Create Folder

POST Auth

GET Get Group Policy

GET Upload Profile

Cancel

Save to AnyConnect Module

POST REQUEST: <https://<FDM IP>/api/fdm/latest/object/anyconnectclientprofiles>

The body of the request contains this information:

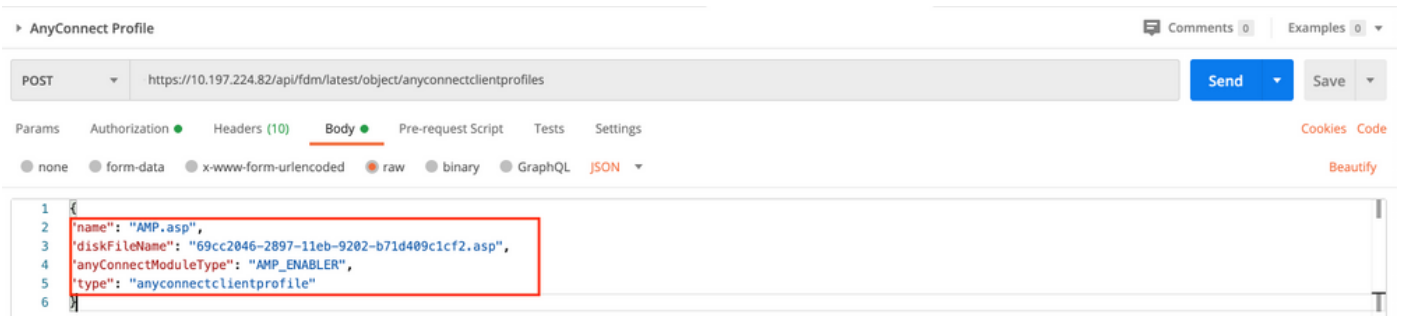
name

Logical name that you would call the file

diskFileName

Needs to match the fileName that is received in the Upload Profile POST resp

anyConnectModuleType Meeds to match the appropriate module shown in [Module](#) Type Table
type anyconnectclientprofile



The screenshot shows a REST client interface with a POST request to `https://10.197.224.82/api/fdm/latest/object/anyconnectclientprofiles`. The 'Body' tab is selected, and the request is in JSON format. The body content is:

```
1 {  
2   "name": "AMP.asp",  
3   "diskFileName": "69cc2046-2897-11eb-9202-b71d409c1cf2.asp",  
4   "anyConnectModuleType": "AMP_ENABLER",  
5   "type": "anyconnectclientprofile"  
6 }
```

The Body of the response shows the Profile ready to be pushed to the device. Name, version, id, and type received in response are used in the next step to bind the profile to Group Policy.



The screenshot shows the response body of the previous request. The status is 200 OK. The response is in JSON format and contains the following data:

```
1 {  
2   "version": "c3woqajhvqxr",  
3   "name": "AMP.asp",  
4   "md5Checksum": "8697131026bdbaf6a67e1191e8abe122",  
5   "description": null,  
6   "diskFileName": "69cc2046-2897-11eb-9202-b71d409c1cf2.asp",  
7   "anyConnectModuleType": "AMP_ENABLER",  
8   "id": "eef22c7-2898-11eb-9202-77e8b953fcd0",  
9   "type": "anyconnectclientprofile",  
10  "links": {  
11    "self": "https://10.197.224.82/api/fdm/latest/object/anyconnectclientprofiles/eef22c7-2898-11eb-9202-77e8b953fcd0"
```

Step 6. Create a **PUT** request to add **Client Profile and Module** to existing **Group Policy**. Click on **Save**, as shown in this image.

SAVE REQUEST

Requests in Postman are saved in collections (a group of requests).

[Learn more about creating collections](#)

Request name

Client Profile and Module

Request description (Optional)

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

Descriptions support [Markdown](#)

Select a collection or folder to save to:

Search for a collection or folder

AnyConnect Module [+ Create Folder](#)

- POST Auth
- GET Get Group Policy
- GET Upload Profile

Cancel

Save to AnyConnect Module

PUT REQUEST: `https://<FDM IP>/api/fdm/latest/object/ravpngrouppolicies/{objId}`

ObjId is the id obtained in [Step 4](#). Copy the contents of the concerned Group-policy obtained in Step 4 to the body of the request and add this:

Client Profile

Name, version, id, and type of Profile received in the previous Step.

Client Modules

The name of the Module which needs to be enabled should match exactly as given in [Module Table](#).

Client Profile and Module

PUT <https://10.197.224.82/api/fdm/latest/object/ravpngrouppolicies/74b60c8e-27ba-11eb-9202-594cb5cba1df> Send

Params Authorization Headers (10) **Body** Pre-request Script Tests Settings

none form-data x-www-form-urlencoded raw binary GraphQL JSON

```
1 {
2   "version": "lc2t2sspzbfy7",
3   "name": "RA-VPN",
4   "banner": null,
5   "dnsServerGroup": null,
6   "defaultDomainName": null,
7   "simultaneousLoginPerUser": 3,
8   "maxConnectionTimeout": null,
9   "maxConnectionTimeAlertInterval": 1,
10  "vpnIdleTimeout": 30,
11  "vpnIdleTimeoutAlertInterval": 1,
12  "ipv4LocalAddressPool": [],
13  "ipv6LocalAddressPool": [],
14  "dhcpScope": null,
15  "ipv4SplitTunnelSetting": "TUNNEL_SPECIFIED",
16  "ipv6SplitTunnelSetting": "TUNNEL_ALL",
17  "ipv4SplitTunnelNetworks": [
18    {
19      "version": "ne3zzud5spztm",
20      "name": "Split-acl",
21      "id": "71b85ceb-27ba-11eb-9202-a5a0daf9088c",
22      "type": "networkobject"
23    }
24  ],
25  "ipv6SplitTunnelNetworks": [],
26  "splitDNSRequestPolicy": "USE_SPLIT_TUNNEL_SETTING",
27  "splitDNSDomainList": "",
28  "scepForwardingUrl": null,
29  "periodicClientCertAuthenticationInterval": 1,
30  "enableDTLS": false,
31  "enableDTLSCompression": false,
32  "enableDTLSCompression": false
33 }
```

Client Profile and Module

PUT <https://10.197.224.82/api/fdm/latest/object/ravpngrouppolicies/74b60c8e-27ba-11eb-9202-594cb5cba1df> Send Save

Params Authorization Headers (10) **Body** Pre-request Script Tests Settings

none form-data x-www-form-urlencoded raw binary GraphQL JSON

```
44  "enableClientDPD": false,
45  "clientDPDInterval": 30,
46  "clientProfiles": [
47    {
48      "version": "c3woqajhvvqxr",
49      "name": "AMP.asp",
50      "id": "eeff22c7-2898-11eb-9202-77e0b953fcd0",
51      "type": "anyconnectclientprofile"
52    }
53  ],
54  "keepInstallerOnClient": false,
55  "vpnTrafficFilterACL": null,
56  "enableRestrictVPNTtoVLAN": false,
57  "restrictVPNTtoVLANid": null,
58  "clientFirewallPrivateNetworkRules": null,
59  "clientFirewallPublicNetworkRules": null,
60  "browserProxyType": "NO_MODIFY",
61  "proxy": {
62    "serverHost": null,
63    "port": null,
64    "type": "serverhostandport"
65  },
66  "proxyExceptions": [],
67  "enabledAnyConnectModules": ["START_BEFORE_LOGIN", "DART", "AMP_ENABLER"],
68  "isEnabledPeriodicClientCertAuthentication": false,
69  "id": "74b60c8e-27ba-11eb-9202-594cb5cba1df",
70  "type": "ravpngrouppolicy",
71  "links": {
72    "self": "https://10.197.224.82/api/fdm/latest/object/ravpngrouppolicies/74b60c8e-27ba-11eb-9202-594cb5cba1df"
73  }
74 }
```

The Body of the response shows the Profile and Module successfully bound to Group-Policy.

```

Body Cookies Headers (17) Test Results Status: 200 OK Time: 2.71 s Size: 2.75 KB Save Response
Pretty Raw Preview Visualize JSON
45 "clientDPDInterval": 30,
46 "clientProfiles": [
47   {
48     "version": "c3woqajhvvqxr",
49     "name": "AMP.asp",
50     "id": "eeff22c7-2898-11eb-9202-77e0b953fcd0",
51     "type": "anyconnectclientprofile"
52   }
53 ],
54 "keepInstallerOnClient": false,
55 "vpnTrafficFilterACL": null,
56 "enableRestrictVPNTovLAN": false,
57 "restrictVPNTovLANid": null,
58 "clientFirewallPrivateNetworkRules": null,
59 "clientFirewallPublicNetworkRules": null,
60 "browserProxyType": "NO_MODIFY",
61 "proxy": {
62   "serverHost": null,
63   "port": null,
64   "type": "serverhostandport"
65 },
66 "proxyExceptions": [],
67 "enabledAnyConnectModules": [
68   "START_BEFORE_LOGIN",
69   "DART",
70   "AMP_ENABLER"
71 ],
72 "isEnabledPeriodicClientCertAuthentication": false.

```

Note: This step allows the download SBL Module. SBL also has to enable in anyconnect client profile which can be uploaded as you navigate to **Devices > Remote Access VPN > Group Policies > Edit Group Policy > General > AnyConnect Client Profile**.

Step 7. Deploy the configuration to the device through FDM. Pending changes show client profile and modules to be pushed.

Pending Changes ? ✕

✔ **Last Deployment Completed Successfully**
 17 Nov 2020 07:42 AM. [See Deployment History](#)

Deployed Version (17 Nov 2020 07:42 AM)	Pending Version LEGEND
AnyConnect Group Edited: RA-VPN	
<pre> - - - clientProfiles: - </pre>	<pre> enabledAnyConnectModules[0]: DART enabledAnyConnectModules[1]: AMP_ENABLER enabledAnyConnectModules[2]: START_BEFORE_LOGIN AMP.asp </pre>
+ AnyConnect Client Profile Added: AMP.asp	
<pre> - - - - </pre>	<pre> anyConnectModuleType: AMP_ENABLER md5Checksum: 8697131026bdbaf6a67e1191e8abe122 diskFileName: 69cc2046-2897-11eb-9202-b71d409c1cf2 name: AMP.asp </pre>

MORE ACTIONS ▾
CANCEL
DEPLOY NOW ▾

Configuration pushed to the FTD CLI after successful deployment:

```
!--- RA VPN Configuration ---!
```

```
webvpn
enable outside
anyconnect image disk0:/anyconnpkgs/anyconnect-win-4.9.00086-webdeploy-k9.pkg 2
  anyconnect profiles AMP.asp disk0:/anyconnprofs/AMP.asp
  anyconnect profiles defaultClientProfile disk0:/anyconnprofs/defaultClientProfile.xml
anyconnect enable
tunnel-group-list enable
```


!--- Group Policy Configuration ---!

```
group-policy RA-VPN internal
group-policy RA-VPN attributes
webvpn
  anyconnect modules value ampenabler,dart,vpngina
  anyconnect profiles value AMP.asp type ampenabler
```

Verify

Establish a successful connection to the FTD.

Navigate to **Settings > VPN > Message History** to see the details about modules that were downloaded.



The screenshot displays the Cisco AnyConnect Secure Mobility Client interface. The left sidebar contains navigation options: Status Overview, VPN (selected), Network, Web Security, System Scan, and Roaming Security. The main window is titled 'Virtual Private Network (VPN)' and has tabs for Preferences, Statistics, Route Details, Firewall, and Message History. The Message History tab is active, showing a log of events for 15-11-2020. A red box highlights the following log entries:

- 21:49:55 The AnyConnect Downloader is performing update checks...
- 21:49:55 Checking for profile updates...
- 21:49:57 Downloading AMP Enabler Service Profile - 100%
- 21:49:57 Checking for product updates...
- 21:49:58 Downloading AnyConnect DART 4.9.00086 - 100%
- 21:49:58 Downloading AnyConnect SBL 4.9.00086 - 100%
- 21:49:59 Downloading AnyConnect AMP Enabler 4.9.00086 - 100%

Troubleshoot

[Collect DART](#) for troubleshooting issues with the installation of client modules.