

Configurer les modules AnyConnect pour un VPN d'accès à distance sur FTD

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configuration](#)

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

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

[Vérification](#)

[Dépannage](#)

Introduction

Ce document décrit comment configurer des modules AnyConnect pour une configuration VPN d'accès distant (VPN RA) qui existe déjà sur un pare-feu de protection contre les menaces (FTD) géré par un Firepower Management Center (FMC) via Firepower Device Manager (FDM).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension de base du fonctionnement du VPN RA.
- Compréhension de la navigation à travers le FMC/FDM.
- Connaissance de base de l'API REST et de l'Explorateur d'API FDM Rest.

Components Used

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- 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
- Client Cisco AnyConnect Secure Mobility exécutant la version 4.9.0086
- Postman ou tout autre outil de développement d'API

Remarque : FMC/FDM n'a pas d'éditeur de profil intégré et l'[éditeur de profil AnyConnect](#) pour Windows doit être utilisé pour créer un profil.

Remarque : les informations de ce document ont été créées à partir de périphériques dans un environnement de travaux pratiques spécifique. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est actif, assurez-vous de bien comprendre l'impact potentiel de toute modification de configuration.

Informations générales

Le client Cisco AnyConnect Secure Mobility n'est pas limité à sa prise en charge en tant que client VPN, il dispose d'un certain nombre d'autres options pouvant être intégrées en tant que modules. Les modules suivants sont pris en charge pour Anyconnect :

- Start Before Login (SBL) : ce module permet à l'utilisateur d'établir une connexion VPN dans l'entreprise avant de se connecter à Windows.
- Outil de diagnostic et de rapport (DART) : ce module est utilisé pour effectuer des diagnostics et des rapports sur l'installation et la connexion d'AnyConnect. Le DART fonctionne en rassemblant les journaux, l'état et les informations de diagnostic pour analyse.
- Advanced Malware Protection (AMP) : Ce module fournit une solution cloud de nouvelle génération pour détecter, prévenir et répondre à diverses menaces.
- Position ISE : Cisco Identity Services Engine (ISE) fournit une politique de contrôle d'accès et d'identité de nouvelle génération. Ce module permet d'identifier le système d'exploitation (OS), l'antivirus, le logiciel espion, etc. actuellement installés sur un hôte. Ces informations sont ensuite utilisées avec une stratégie pour déterminer si l'hôte sera en mesure de se connecter au réseau.
- Module de visibilité réseau : Le module de visibilité du réseau surveille l'utilisation d'une application de point d'extrémité pour détecter les anomalies de comportement potentielles et prendre des décisions plus éclairées en matière de conception du réseau.
- Umbrella : Cisco Umbrella Roaming est un service de sécurité fourni dans le cloud qui protège les périphériques lorsqu'ils ne sont pas connectés au réseau de l'entreprise.
- Sécurité Web : L'appareil de sécurité Web (WSA) de Cisco, optimisé par Cisco Talos, protège le terminal en bloquant automatiquement les sites à risque et en testant les sites inconnus.
- Network Access Manager : Network Access Manager fournit un réseau de couche 2 sécurisé conformément à ses politiques. Il détecte et sélectionne le réseau d'accès optimal de couche 2 et effectue l'authentification des périphériques pour l'accès aux réseaux filaires et sans fil.
- Commentaires: Ce module collecte les informations et les envoie régulièrement au serveur. Il aide l'équipe produit à améliorer la qualité, la fiabilité, les performances et l'expérience utilisateur d'AnyConnect.

Dans Firepower 6.7, la prise en charge de l'interface FMC et de l'API REST de périphérique FTD est ajoutée pour permettre un déploiement transparent de tous les modules AnyConnect mentionnés.



Ce tableau répertorie les extensions de profils et associées Types de module nécessaires pour déployer correctement la fonctionnalité de point d'extrémité.

Extensions de profil

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

Type de module

- COMMENTAIRES
- AMP_ENABLER
- POSTURE_ISE
- VISIBILITÉ RÉSEAU
- NETWORK_ACCESS_MANAGER
- PARAPLUIE
- SÉCURITÉ_WEB

Remarque : les modules DART et SBL ne nécessitent aucun profil.

Remarque : aucune licence supplémentaire n'est requise pour l'utilisation de cette fonctionnalité.

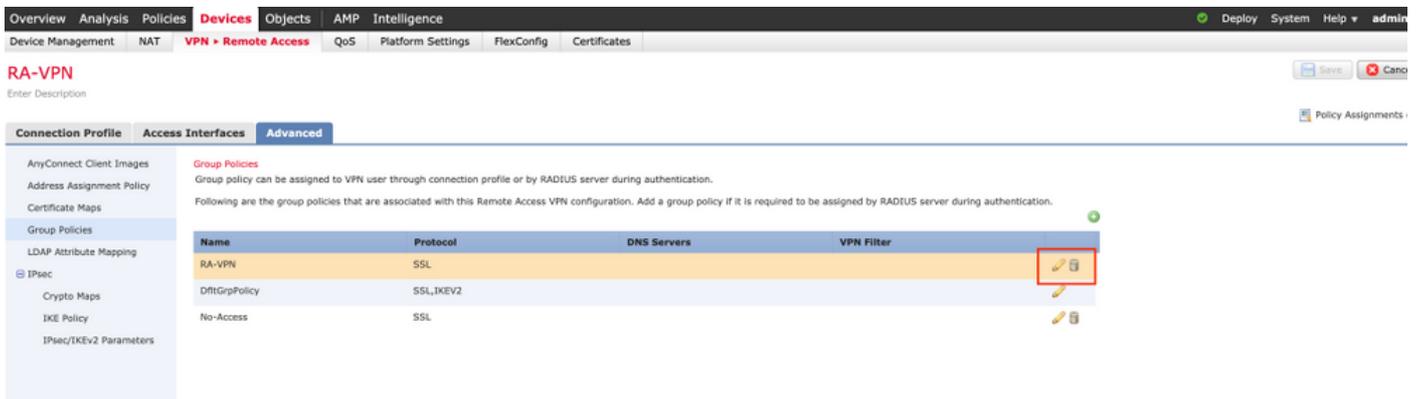
Configuration

Configuration sur Firepower Management Center (FMC)

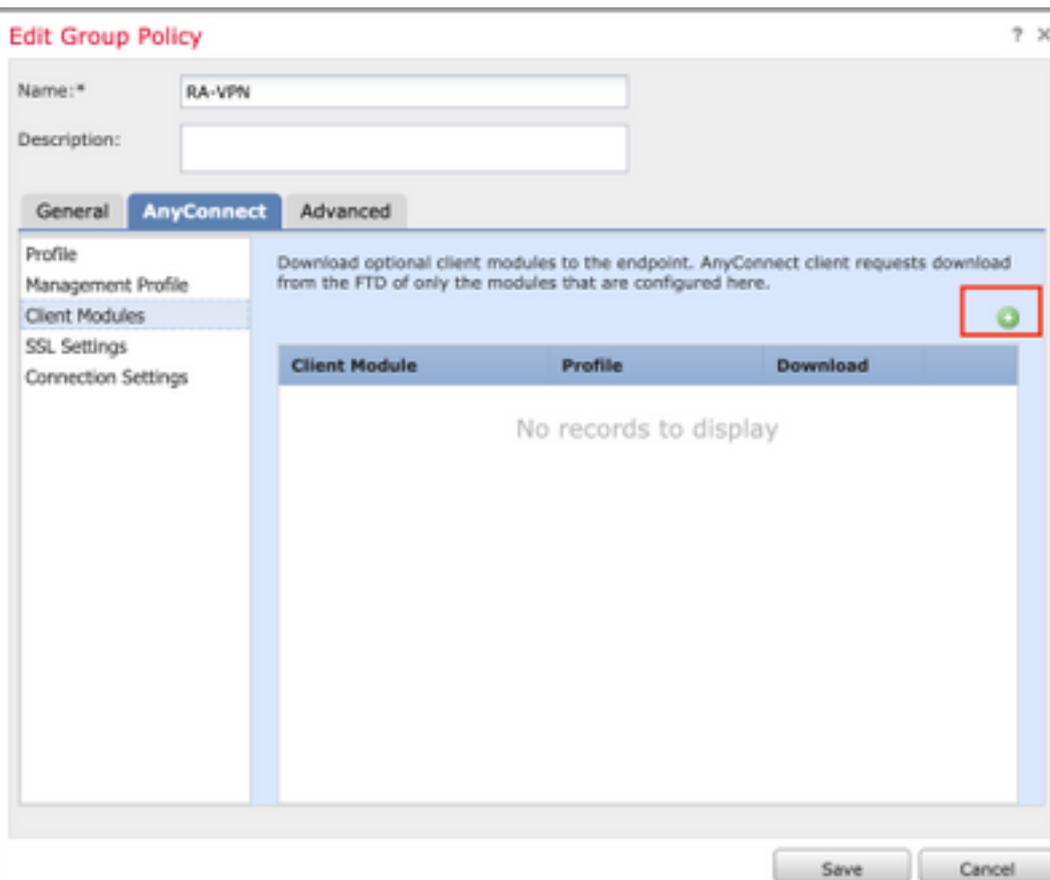
Étape 1. Accédez à **Device > VPN > Remote Access** et cliquez sur **Edit** pour la configuration VPN RA.



Étape 2. Accédez à **Advanced > Group Policies** et cliquez sur **Edit** pour la stratégie de groupe concernée, comme illustré dans cette image.



Étape 3. Accédez à **AnyConnect > Client Modules** et cliquez sur **+** pour ajouter les modules, comme illustré dans cette image.



À des fins de démonstration, le déploiement des modules AMP, DART et SBL est illustré.

Étape 4. Sélectionnez le module **DART** et cliquez sur **Ajouter**, comme illustré dans cette image.

Add Client Module ? X

Client Module: DART

Profile to download: [Empty]

Enable module download:

Add Cancel

Étape 5. Cliquez sur + pour ajouter un autre module et sélectionnez **Démarrer avant de vous connecter** module, comme illustré dans cette image.

Add Client Module ? X

Client Module: Start Before Login

Profile to download: [Empty]

Enable module download:

Add Cancel

Note: Cette étape vous permet de télécharger le module SBL. SBL doit également activer dans un profil client anyconnect, qui est téléchargé lorsque vous naviguez vers **AnyConnect > Profil** sous la stratégie de groupe.

Étape 6. Cliquez sur + pour ajouter un autre module et sélectionnez **AMP Enabler**. Cliquez sur + pour ajouter un profil client, comme illustré dans cette image.

Add Client Module ? X

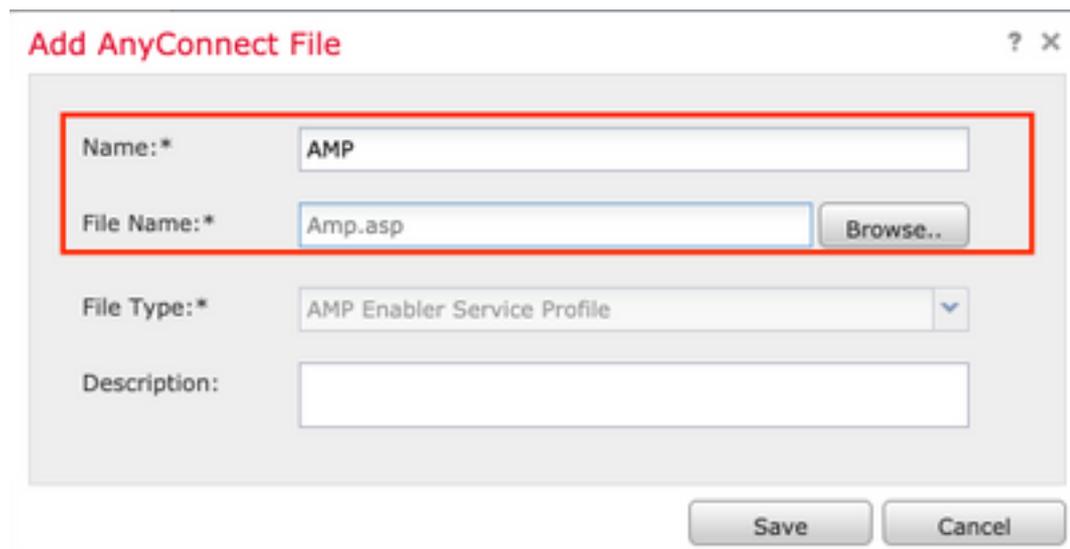
Client Module: AMP Enabler

Profile to download: [Empty] +

Enable module download:

Add Cancel

Indiquez le **nom** du profil et téléchargez le **profil AMP**. Cliquez sur **Enregistrer**, comme illustré dans cette image.



Add AnyConnect File ? X

Name:* AMP

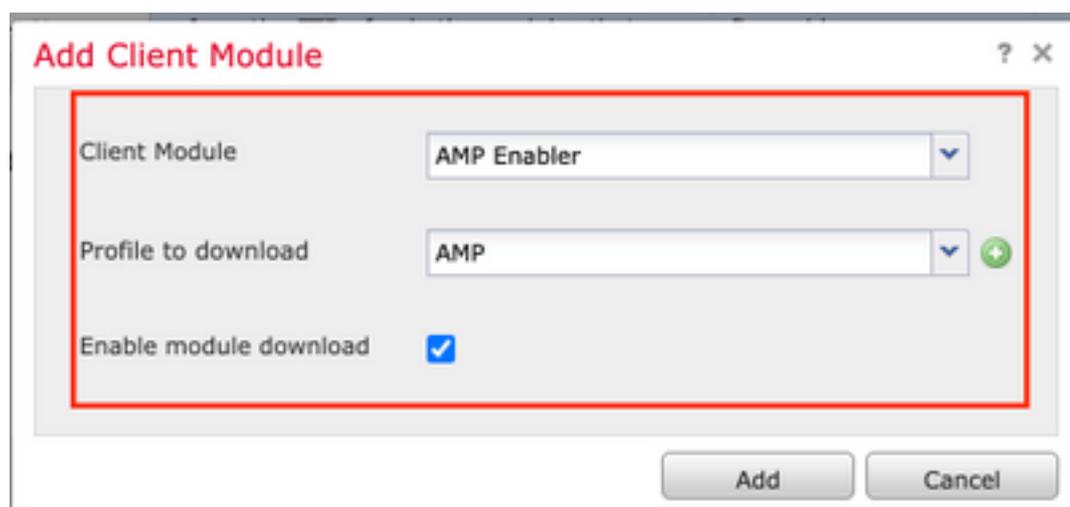
File Name:* Amp.asp Browse..

File Type:* AMP Enabler Service Profile

Description:

Save Cancel

Choisissez le profil créé à l'étape précédente et cliquez sur la **case Activer le téléchargement de module**, comme indiqué dans cette image.



Add Client Module ? X

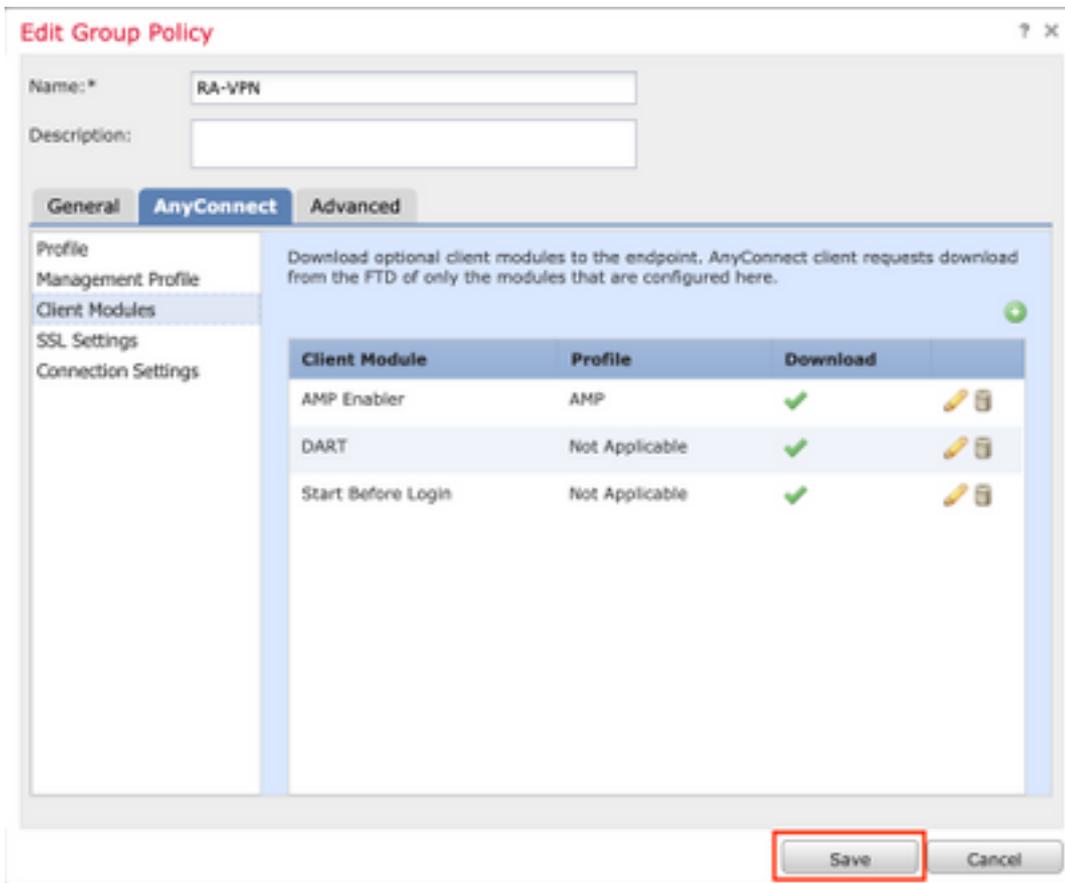
Client Module AMP Enabler

Profile to download AMP +

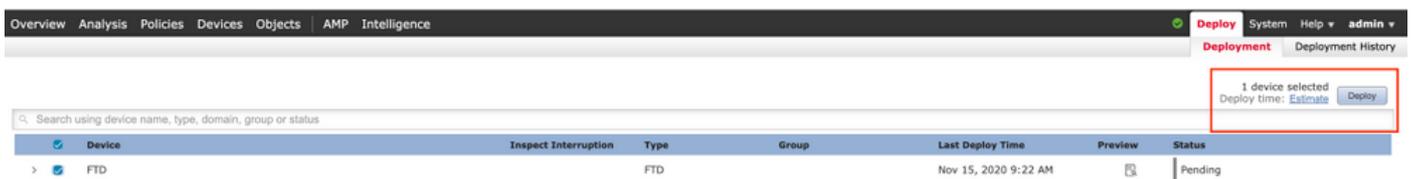
Enable module download

Add Cancel

Étape 7. Cliquez sur **Enregistrer** une fois tous les modules souhaités ajoutés.



Étape 8. Accédez à **Déployer > Déploiement** et déployez la configuration sur le FTD.



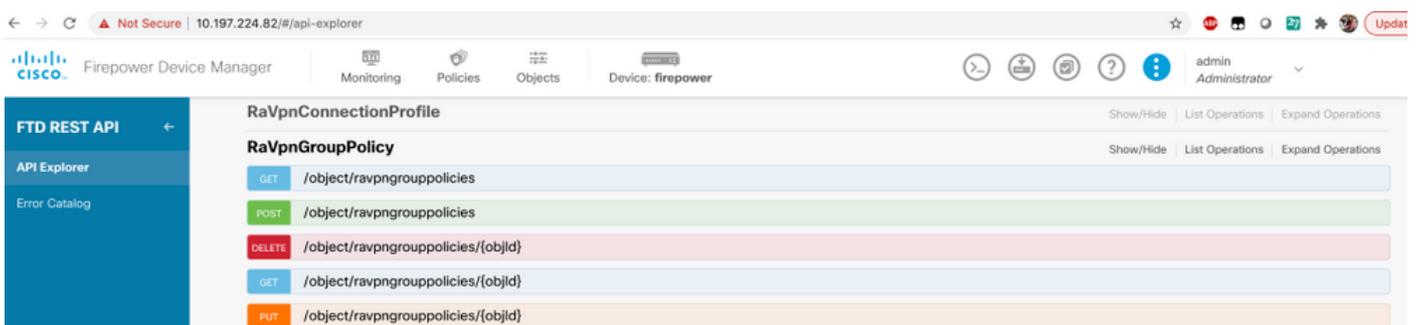
Configuration sur Firepower Device Manager (FDM)

Étape 1. Lancez l'Explorateur d'API du FTD dans une fenêtre de navigateur.

Accédez à <https://<FTD Management IP>/api-explorer>

Il contient la liste complète des API disponibles sur le FTD. Il est divisé en fonction de la fonction principale avec plusieurs requêtes GET/POST/PUT/DELETE prises en charge par le module FDM.

RaVpnGroupPolicy est l'API utilisée.



Étape 2. Ajoutez une collection Postman pour les modules AnyConnect. Indiquez un nom pour la collection. Cliquez sur **Créer**.

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

Étape 3. Ajouter une nouvelle demande **authentification** pour créer une requête POST de connexion au FTD afin d'obtenir le jeton pour autoriser toute requête POST/GET/PUT. Cliquez sur **Enregistrer**.

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

Le corps de la demande POST doit contenir les éléments suivants :

Type raw - JSON (application/json)

type_subvention mot de passe

username
(nom d'utilisateur) Admin Username afin de se connecter au FTD

mot de passe Mot de passe associé au compte d'utilisateur admin


```
Body Cookies Headers (17) Test Results Status: 200 OK Time: 218 ms Size: 4.72 KB Save Response
Pretty Raw Preview Visualize JSON
1
2 "items": [
3
4   {
5     "version": "ijtc7ii45gloz",
6     "name": "DfltGrpPolicy",
7     "banner": null,
8     "dnsServerGroup": null,
9     "defaultDomainName": null,
10    "simultaneousLoginPerUser": 3,
11    "maxConnectionTimeout": null,
12    "maxConnectionTimeAlertInterval": 1,
13    "vpnIdleTimeout": 30,
14    "vpnIdleTimeoutAlertInterval": 1,
15    "ipv4LocalAddressPool": [],
16    "ipv6LocalAddressPool": [],
17    "dhcpScope": null,
18    "ipv4SplitTunnelSetting": "TUNNEL_ALL",
19    "ipv6SplitTunnelSetting": "TUNNEL_ALL",
20    "ipv4SplitTunnelNetworks": [],
21    "ipv6SplitTunnelNetworks": [],
22    "splitDNSRequestPolicy": "USE_SPLIT_TUNNEL_SETTING",
23    "splitDNSDomainList": "",
24    "scepForwardingUrl": null,
25    "periodicClientCertAuthenticationInterval": 1,
26    "enableDTLS": false,
27    "enableDTLSCompression": false,
28    "sslCompression": "DISABLED",
29    "enableSSIRekey": false.
30  }
31 ]
32 }
```

```
Body Cookies Headers (17) Test Results Status: 200 OK Time: 218 ms Size: 4.72 KB Save Response
Pretty Raw Preview Visualize JSON
59
60   {
61     "version": "lc2t2sspzbfy7",
62     "name": "RA-VPN",
63     "banner": null,
64     "dnsServerGroup": null,
65     "defaultDomainName": null,
66     "simultaneousLoginPerUser": 3,
67     "maxConnectionTimeout": null,
68     "maxConnectionTimeAlertInterval": 1,
69     "vpnIdleTimeout": 30,
70     "vpnIdleTimeoutAlertInterval": 1,
71     "ipv4LocalAddressPool": [],
72     "ipv6LocalAddressPool": [],
73     "dhcpScope": null,
74     "ipv4SplitTunnelSetting": "TUNNEL_SPECIFIED",
75     "ipv6SplitTunnelSetting": "TUNNEL_ALL",
76     "ipv4SplitTunnelNetworks": [
77       {
78         "version": "ne3zzud5spztm",
79         "name": "Split-acl",
80         "id": "71b85ceb-27ba-11eb-9202-a5a0daf9088c",
81         "type": "networkobject"
82       }
83     ],
84     "ipv6SplitTunnelNetworks": [],
85     "splitDNSRequestPolicy": "USE_SPLIT_TUNNEL_SETTING",
86     "splitDNSDomainList": "",
87     "scepForwardingUrl": null.
88   }
89 ]
90 }
```

```
Body Cookies Headers (17) Test Results Status: 200 OK Time: 218 ms Size: 4.72 KB Save Response
Pretty Raw Preview Visualize JSON
108
109   "restrictVPNFlowLanId": null,
110   "clientFirewallPrivateNetworkRules": null,
111   "clientFirewallPublicNetworkRules": null,
112   "browserProxyType": "NO_MODIFY",
113   "proxy": {
114     "serverHost": null,
115     "port": null,
116     "type": "serverhostandport"
117   },
118   "proxyExceptions": [],
119   "enabledAnyConnectModules": [],
120   "isEnabledPeriodicClientCertAuthentication": false,
121   "id": "74b60c8e-27ba-11eb-9202-594cb5cbaldf",
122   "type": "ravpngrouppolicy",
123   "links": {
124     "self": "https://10.197.224.82/api/fdm/latest/object/ravpngrouppolicies/74b60c8e-27ba-11eb-9202-594cb5cbaldf"
125   }
126 },
127 "paging": {
128   "prev": [],
129   "next": [],
130   "limit": 10,
131   "offset": 0,
132   "count": 2,
133   "pages": 0
134 }
135 }
```

À des fins de démonstration, le déploiement des modules AMP, DART et SBL est illustré.

Étape 5. Créez une demande pour télécharger un profil. Cette étape est nécessaire uniquement

pour les modules qui nécessitent un profil. Téléchargez le **profil** dans la section **filetoUpload**. Cliquez sur **Enregistrer**.

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

Le corps de la requête doit contenir le fichier de profil ajouté dans Body au format de données de formulaire. Le profil doit être créé à l'aide de [AnyConnect Profile Editor pour Windows](#)

Le type de clé doit être **File**forfiletoUpload.

The image shows a Postman interface. At the top, a dark grey bar contains the text "SAVE REQUEST". Below this, a message states "Requests in Postman are saved in collections (a group of requests)." with a link "Learn more about creating collections".

The "Request name" field contains "Upload Profile". The "Request description (Optional)" field contains the text "Make things easier for your teammates with a complete request description." Below this, it says "Descriptions support Markdown".

The "Select a collection or folder to save to:" section shows a search bar and a list of collections. The selected collection is "AnyConnect Module", with a "+ Create Folder" button next to it. Below the collection list, there are two items: "POST Auth" and "GET Get Group Policy".

At the bottom of the dialog, there are two buttons: "Cancel" and "Save to AnyConnect Module".

Below the dialog, the Postman interface shows a POST request to "https://10.197.224.82/api/fdm/latest/action/uploaddiskfile". The "Body" tab is selected, and the "form-data" type is chosen. A table is visible with the following content:

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

The "File" type is selected for the "fileToUpload" key.

Le corps de la réponse donne un id/nom de fichier utilisé pour faire référence au profil du module concerné.



The screenshot shows a REST client interface with a JSON response. The response is displayed in a 'Pretty' view. The 'fileName' field is highlighted with a red box. The response is as follows:

```
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 }
```

Étape 6. Créez une demande de mise à jour du **profil AnyConnect**. Cette étape est nécessaire uniquement pour les modules qui nécessitent un profil. Cliquez sur **Enregistrer.**, comme illustré dans cette 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

REQUÊTE POST : <https://<FDM IP>/api/fdm/last/object/anyconnectclientprofile>

Le corps de la demande contient ces informations :

name (nom)

Nom logique que vous appelleriez le fichier

NomFichierDisque

Doit correspondre au nom de fichier reçu dans la réponse de test POST de p

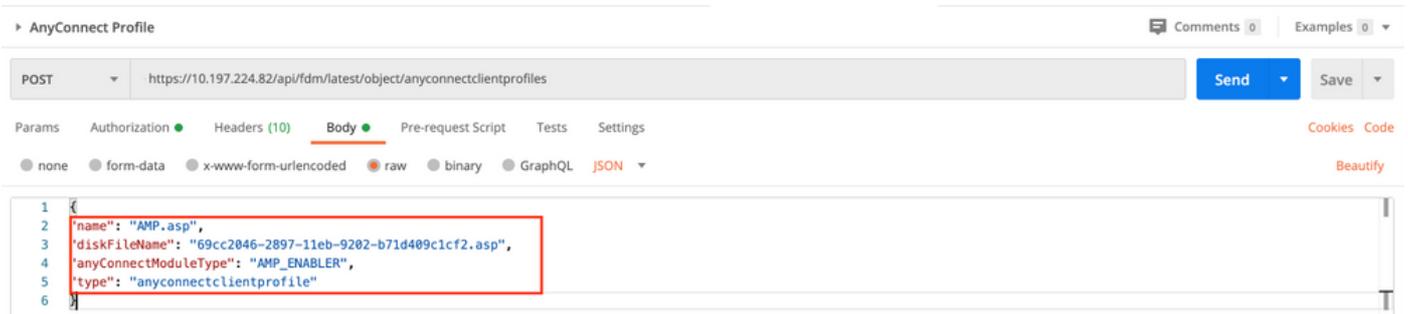
de téléchargement

TypeModuleAnyConnect

Moyens correspondant au module approprié indiqué dans la table de type [de module](#)

type

anyconnectclientprofile



Le corps de la réponse indique le profil prêt à être envoyé au périphérique. Le nom, la version, l'ID et le type reçus en réponse sont utilisés à l'étape suivante pour lier le profil à la stratégie de groupe.



Étape 6. Créez une demande PUT pour ajouter le profil et le module du client à la stratégie de groupe existante. Cliquez sur Enregistrer, comme illustré dans cette 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/last/object/ravpngroupolicies/{objId}>

ObjId est l'ID obtenu à l'[étape 4](#). Copiez le contenu de la politique de groupe concernée obtenue à l'étape 4 dans le corps de la demande et ajoutez ceci :

Profil client

Nom, version, ID et type de profil reçus à l'étape précédente.

Modules clients

Le nom du module qui doit être activé doit correspondre exactement à celui indiqué dans la table [du module](#).

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  "isEnablePeriodicClientCertAuthentication": 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 }
```

Le corps de la réponse affiche le profil et le module correctement liés à la stratégie de groupe.

```

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: Cette étape permet de télécharger le module SBL. SBL doit également activer dans n'importe quel profil client de connexion qui peut être téléchargé lorsque vous naviguez vers **Devices > Remote Access VPN > Group Policies > Edit Group Policy > General > AnyConnect Client Profile**.

Étape 7. Déployez la configuration sur le périphérique via FDM. Les modifications en attente indiquent le profil du client et les modules à pousser.

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	
<ul style="list-style-type: none"> — — — clientProfiles: — 	<div style="border: 1px solid red; padding: 5px;"> <ul style="list-style-type: none"> enabledAnyConnectModules[0]: DART enabledAnyConnectModules[1]: AMP_ENABLER enabledAnyConnectModules[2]: START_BEFORE_LOGIN </div> <ul style="list-style-type: none"> — AMP.asp
+ AnyConnect Client Profile Added: AMP.asp	
<ul style="list-style-type: none"> — — — — 	<div style="border: 1px solid red; padding: 5px;"> <ul style="list-style-type: none"> anyConnectModuleType: AMP_ENABLER md5Checksum: 8697131026bdbaf6a67e1191e8abe122 diskFileName: 69cc2046-2897-11eb-9202-b71d409c1cf2 ... name: AMP.asp </div>

MORE ACTIONS ▾
CANCEL

DEPLOY NOW ▾

Configuration poussée vers l'interface CLI FTD après un déploiement réussi :

!--- 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
```

Vérification

Établir une connexion réussie au FTD.

Accédez à **Paramètres > VPN > Historique des messages** pour afficher les détails relatifs aux modules téléchargés.



The screenshot displays the Cisco AnyConnect Secure Mobility Client interface. On the left is a navigation menu with 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 messages:

- 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%

Dépannage

[Collectez](#) DART pour résoudre les problèmes liés à l'installation des modules clients.