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

Contenu

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 assemblant 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, 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	Type de module
.fsp	COMMENTAIRES
.asp ou .xml	AMP_ENABLER
.sip ou .xml	POSTURE_ISE
.nvmsp ou .xml	VISIBILITÉ_RÉSEAU
.nsp ou .xml	NETWORK_ACCESS_MANAGER
.json ou .xml	PARAPLUIE
.wsp ou .xml	SÉCURITÉ_WEB

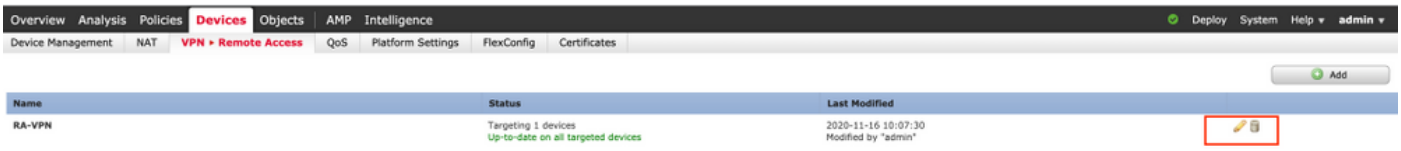
Remarque : les modules DART et SBL ne nécessitent aucun profil.

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

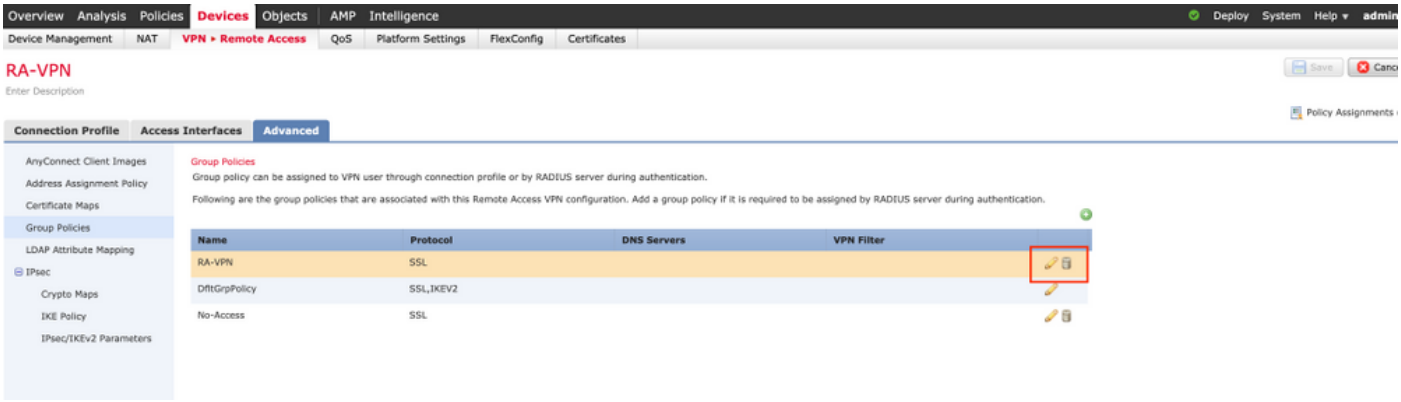
Configuration

Configuration sur Firepower Management Center (FMC)

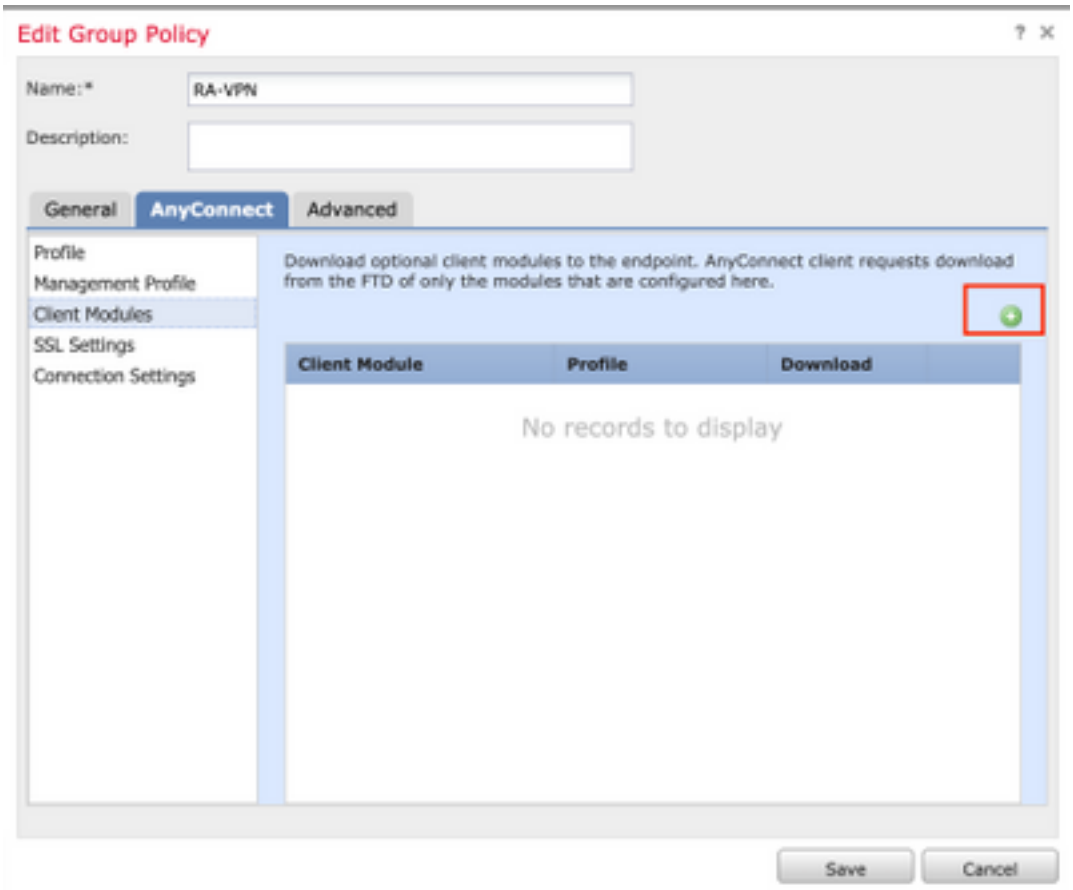
Étape 1. Accédez à **Device > VPN > Remote Access** et cliquez sur **Edit** pour la configuration VPN RA.



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

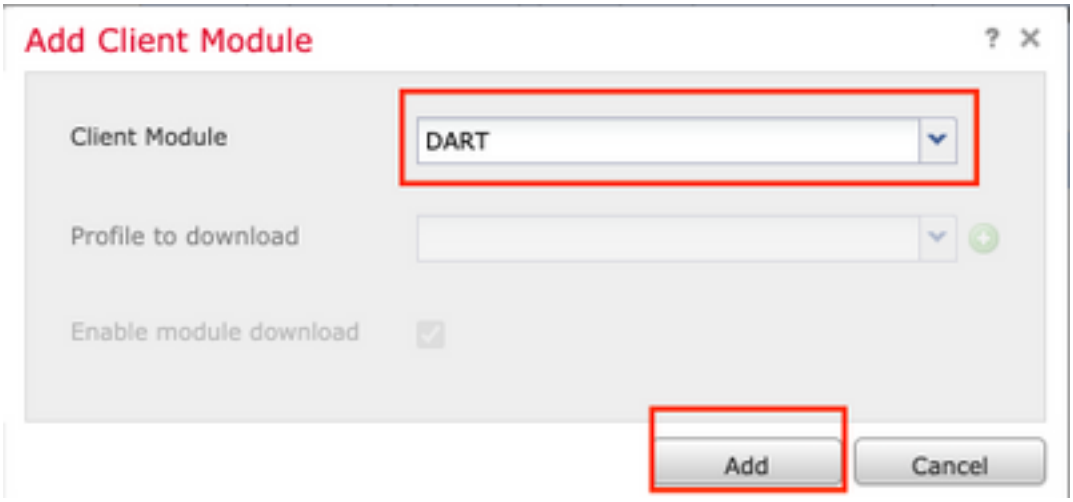


Étape 3. Accédez à **AnyConnect > Client Modules** et cliquez sur **+ pour ajouter les modules**, comme illustré dans cette image.

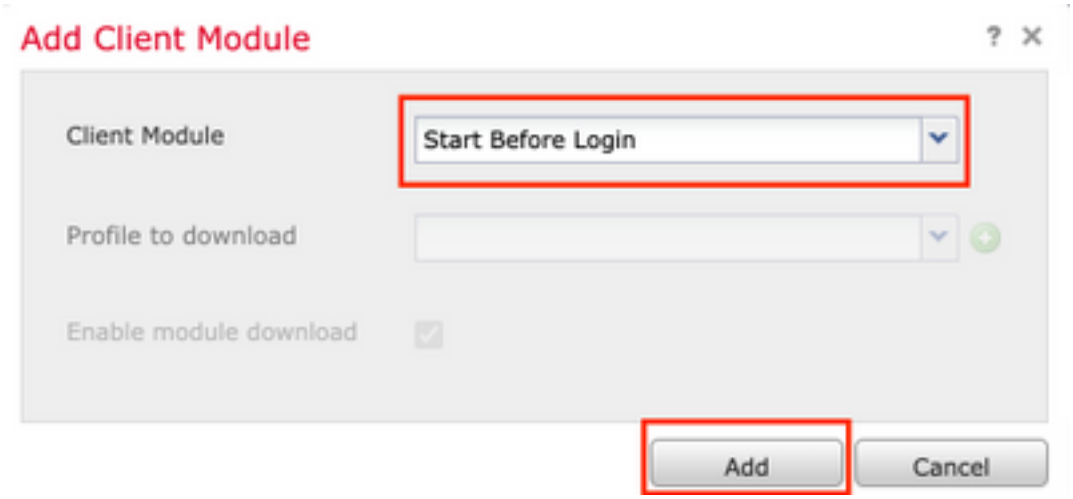


Àdes fins de démonstration, le déploiement des modules AMP, DART et SBL est illustré.

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

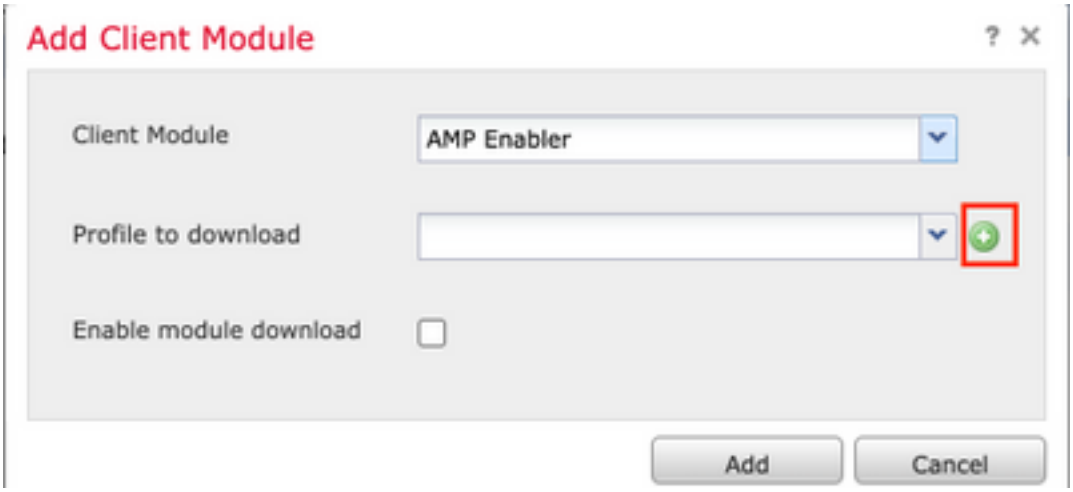


Étape 5. Cliquez sur **+** pour ajouter un autre module et sélectionnez **Démarrer avant de vous connecter** module, comme illustré dans cette image.

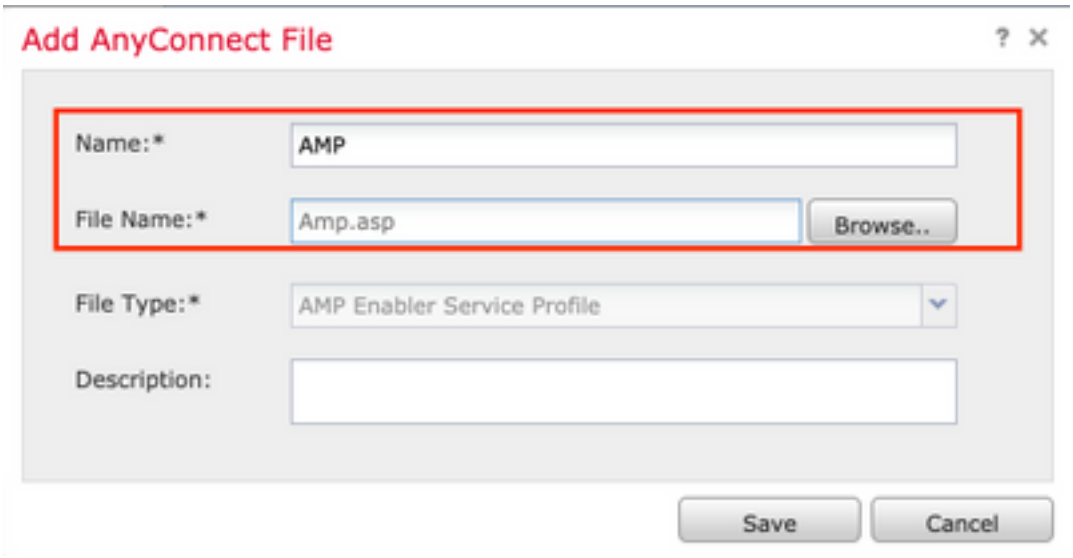


Note: Cette étape vous permet de télécharger le module SBL. SBL doit également activer dans un profil client anyconnect, qui est téléchargé lorsque vous naviguez vers **AnyConnect > Profile** sous la stratégie de groupe.

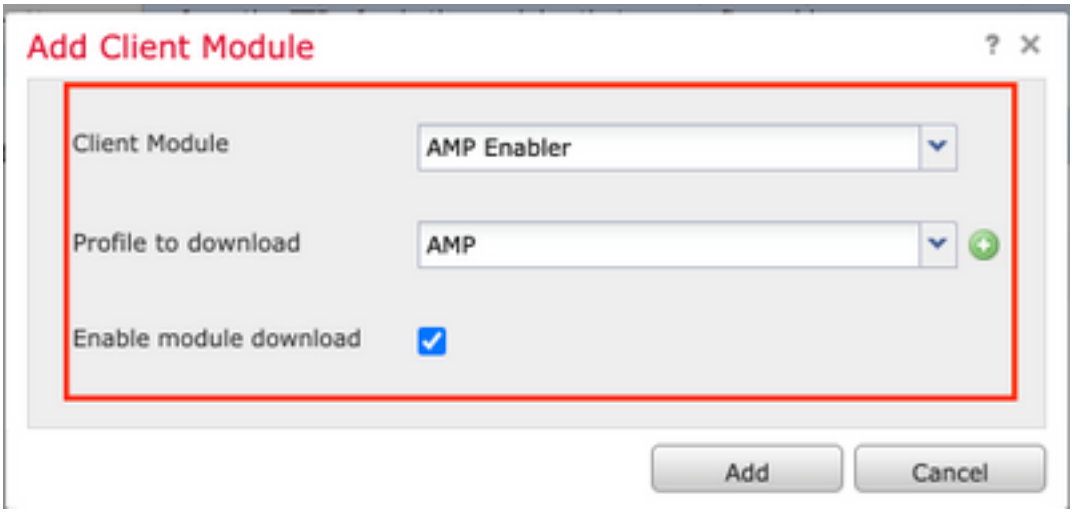
Étape 6. Cliquez sur **+** pour ajouter un autre module et sélectionnez **AMP Enabler.** Cliquez sur **+** pour ajouter un profil client, comme illustré dans cette image.



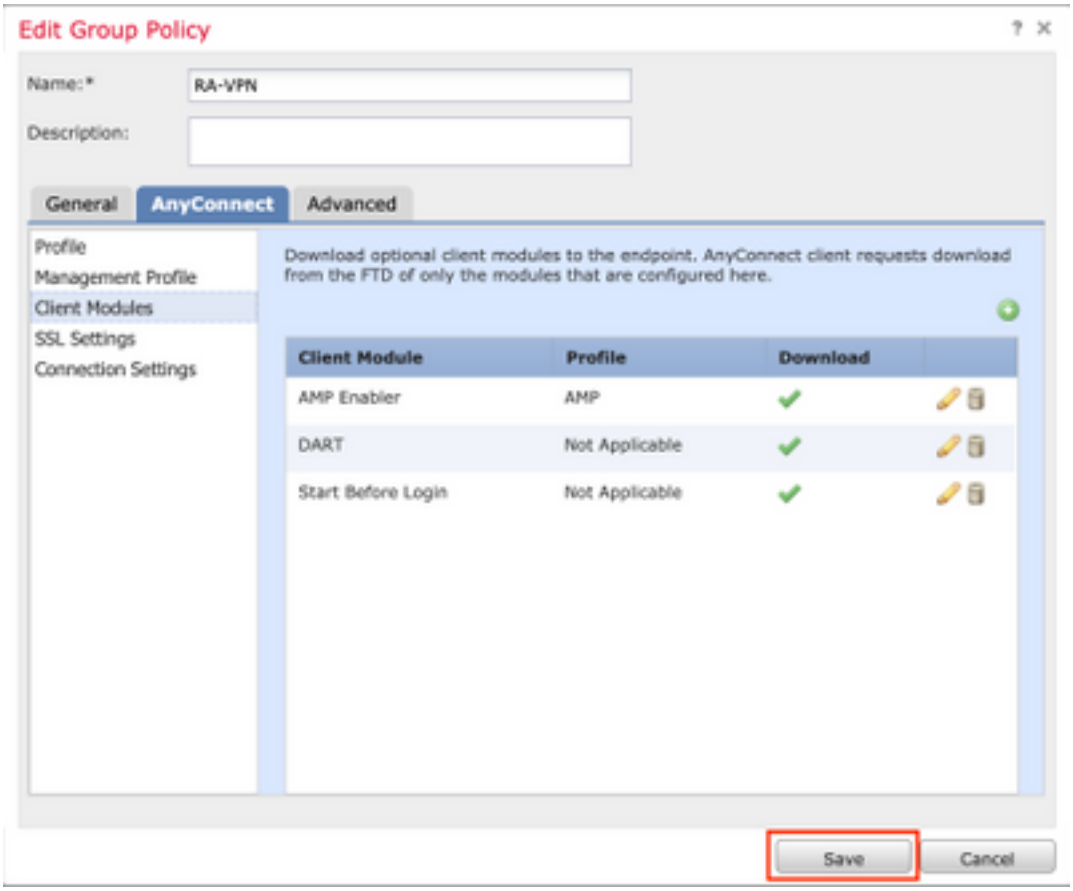
Indiquez le **nom** du profil et téléchargez le **profil AMP**. Cliquez sur **Enregistrer**, comme illustré dans cette image.



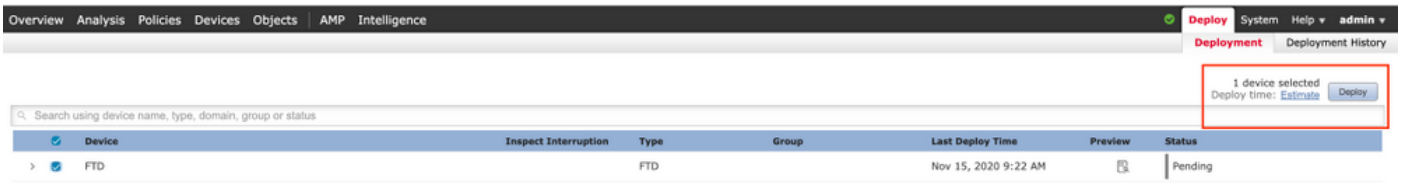
Choisissez le profil créé à l'étape précédente et cliquez sur la **case Activer le téléchargement de module**, comme indiqué dans cette image.



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.



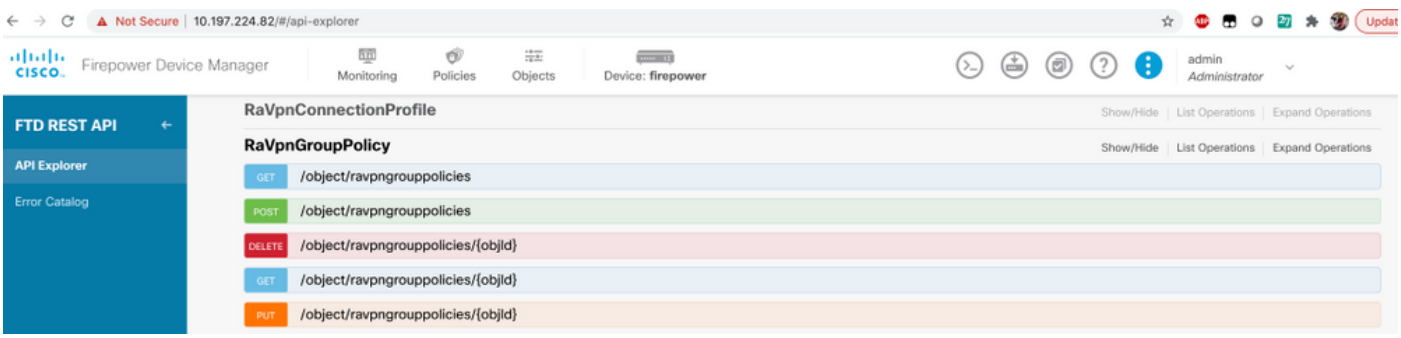
Configuration sur Firepower Device Manager (FDM)

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

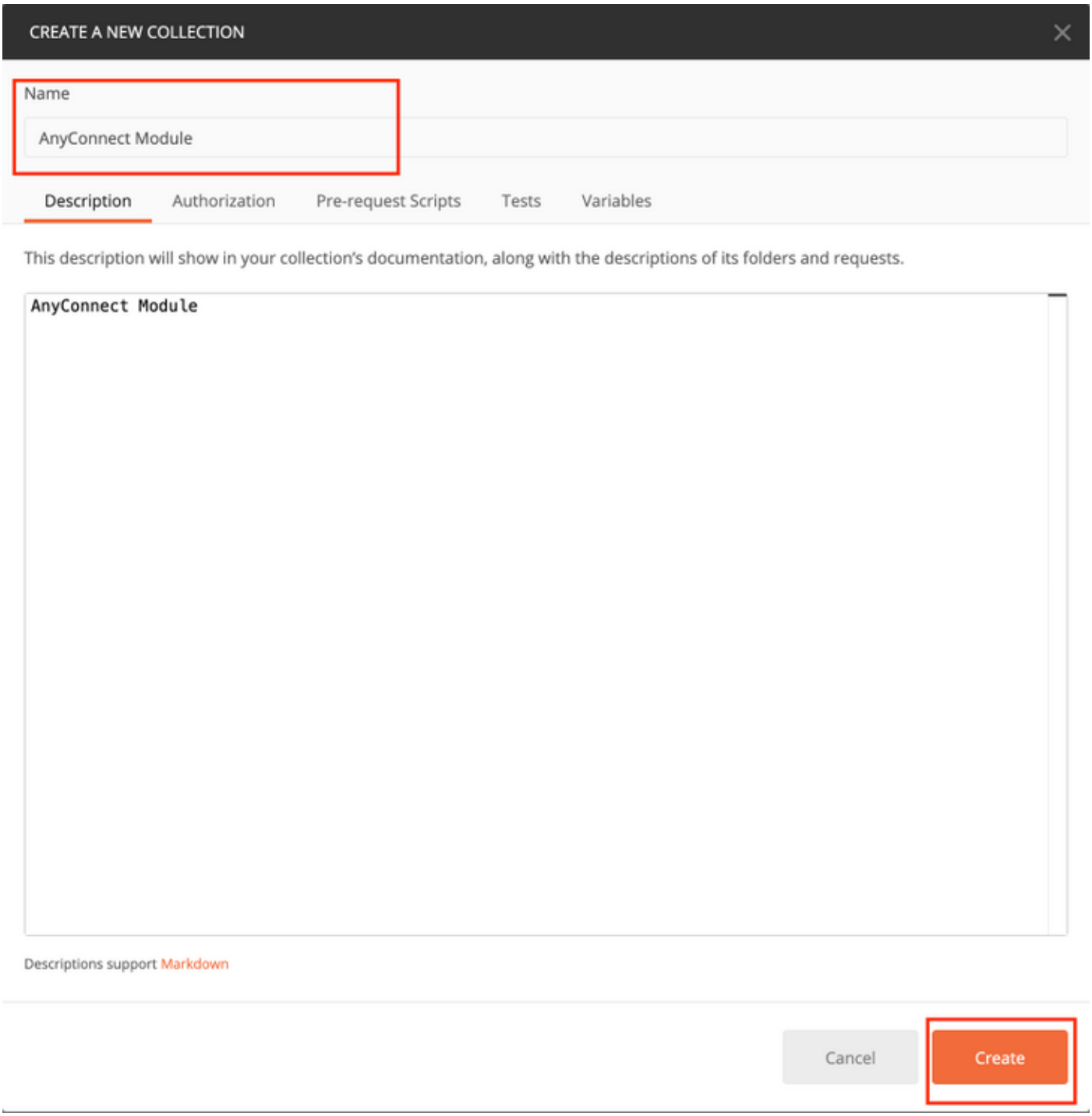
Accédez à **tohttps://<FTD Management IP>/api-explorer**

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.

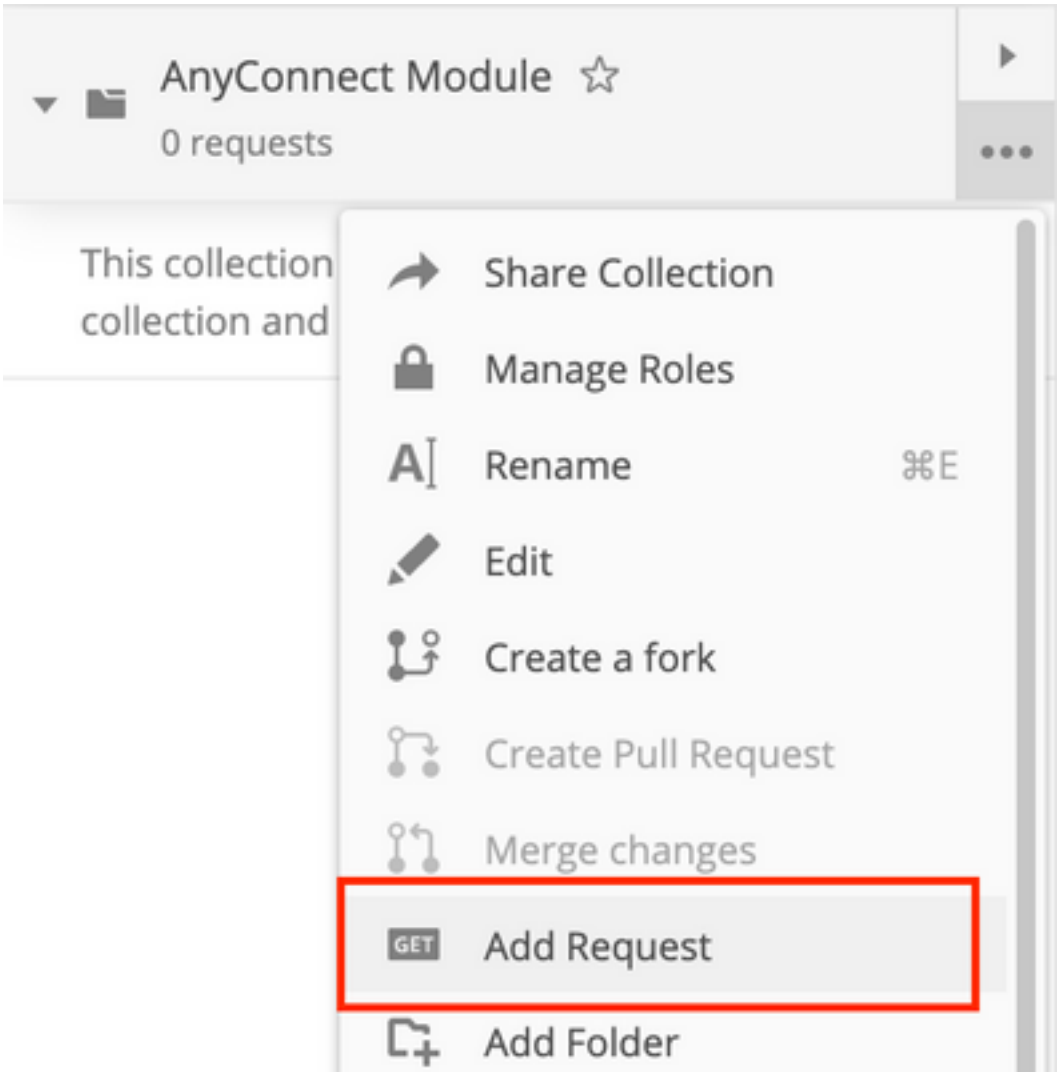
RaVpnGroupPolicy est l'API utilisée.

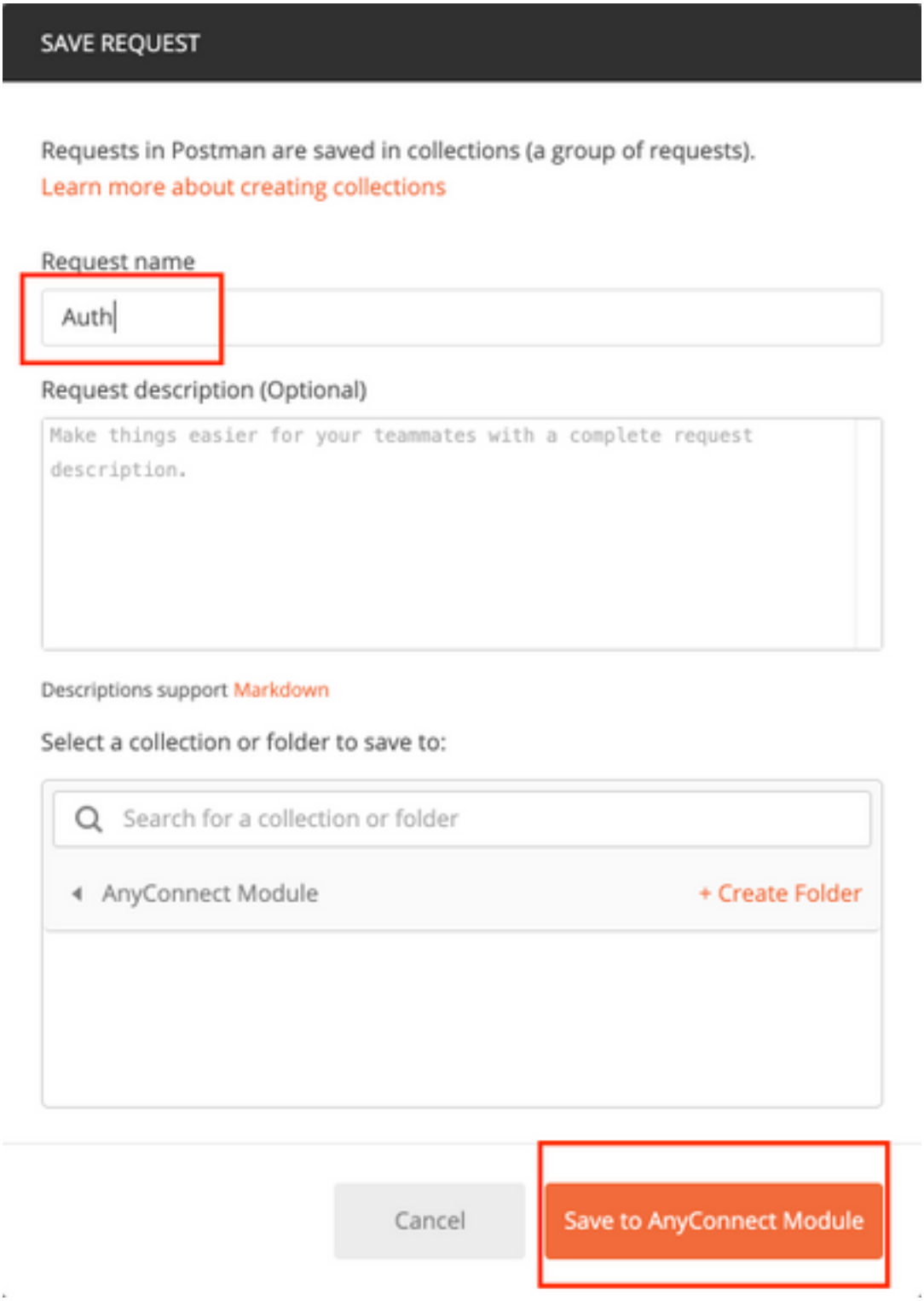


Étape 2. Ajoutez une collection Postman pour **les modules AnyConnect.** Indiquez un **nom** pour la collection. Cliquez sur **Créer**.



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**.

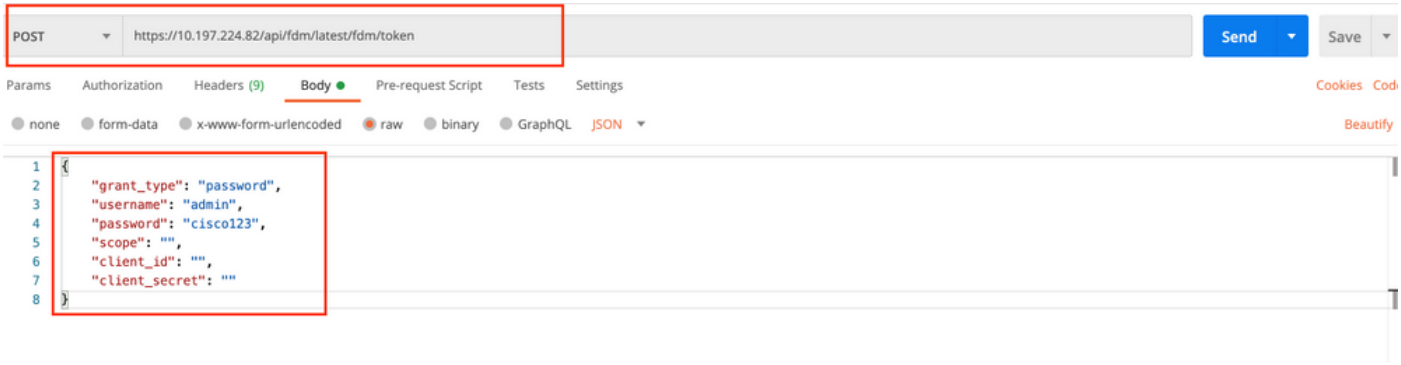

AnyConnect Module
0 requests
This collection
collection and
Share Collection
Manage Roles
Rename
⌘E
Edit
Create a fork
Create Pull Request
Merge changes
GET
Add Request
Add Folder



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

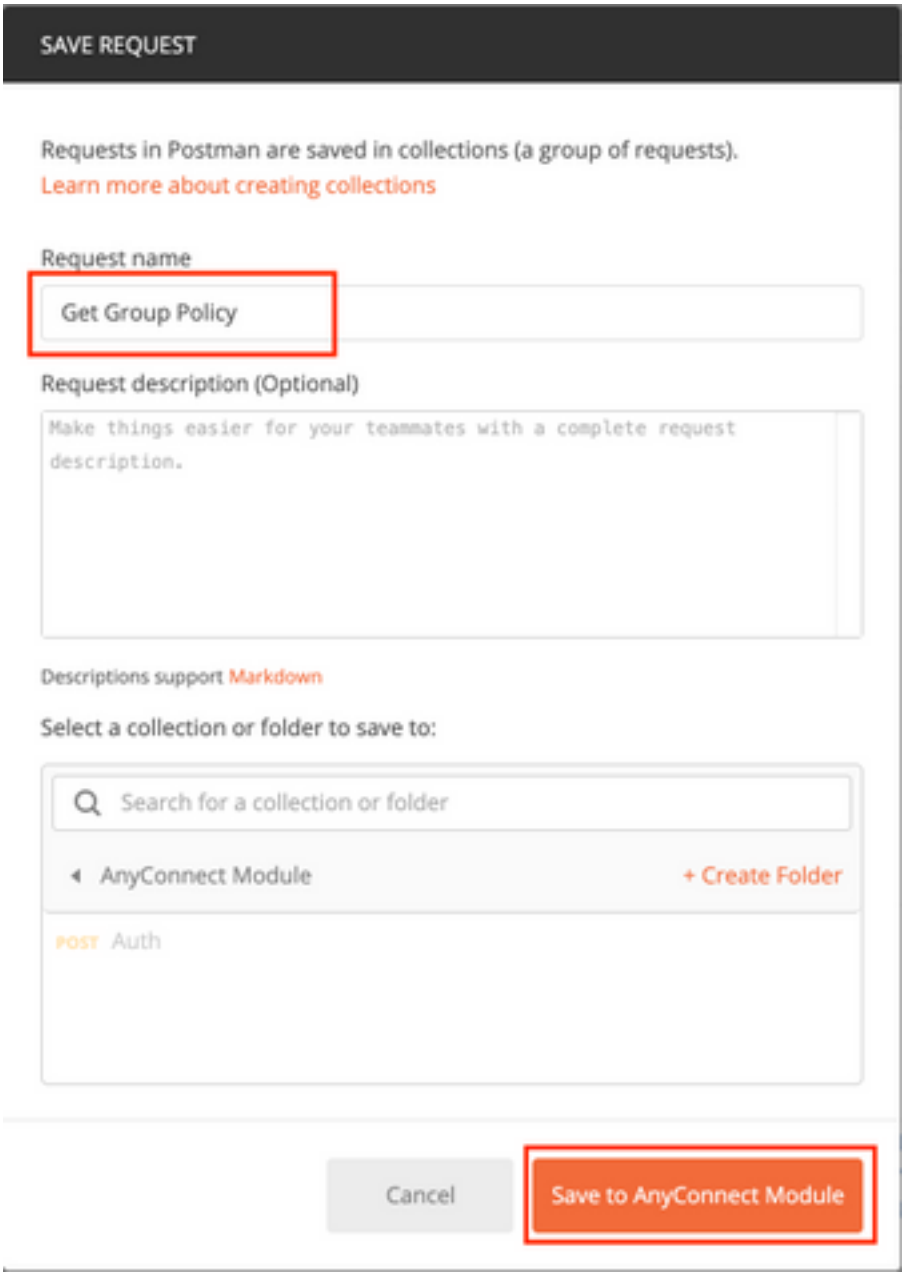
Type	raw - JSON (application/json)
type_subvention	mot de passe
username (nom d'utilisateur)	Admin Username afin de se connecter au FTD
mot de passe	Mot de passe associé au compte d'utilisateur admin

Requête POST : **https://<FTD Management IP>/api/fdm/last/fdm/token**



Le corps de la réponse contient le jeton d'accès qui est utilisé pour envoyer toute requête PUT/GET/POST à/à partir du FTD.

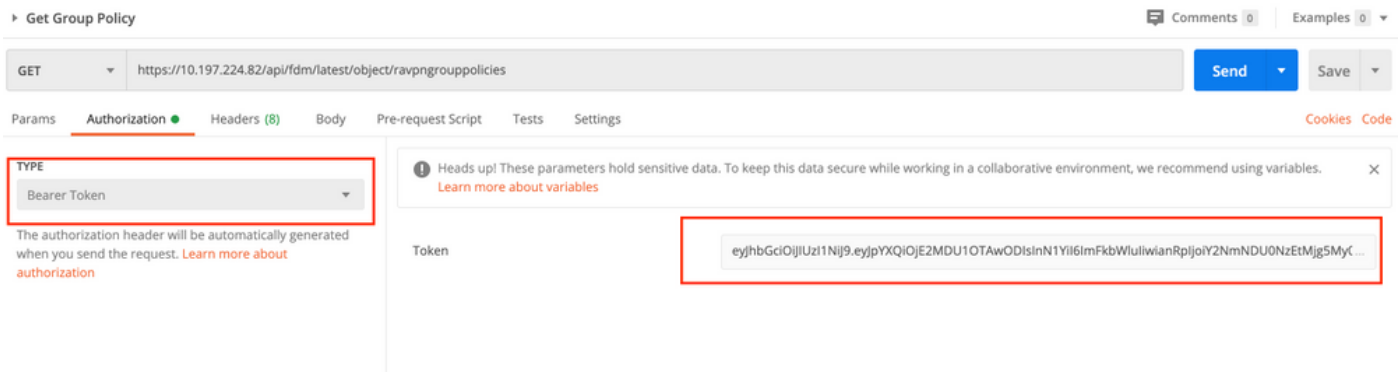
Étape 4. Créer une demande **Obtenir une stratégie de groupe** pour ajouter des détails sur les stratégies de groupe existantes. Cliquez sur **Enregistrer**, comme illustré dans cette image.



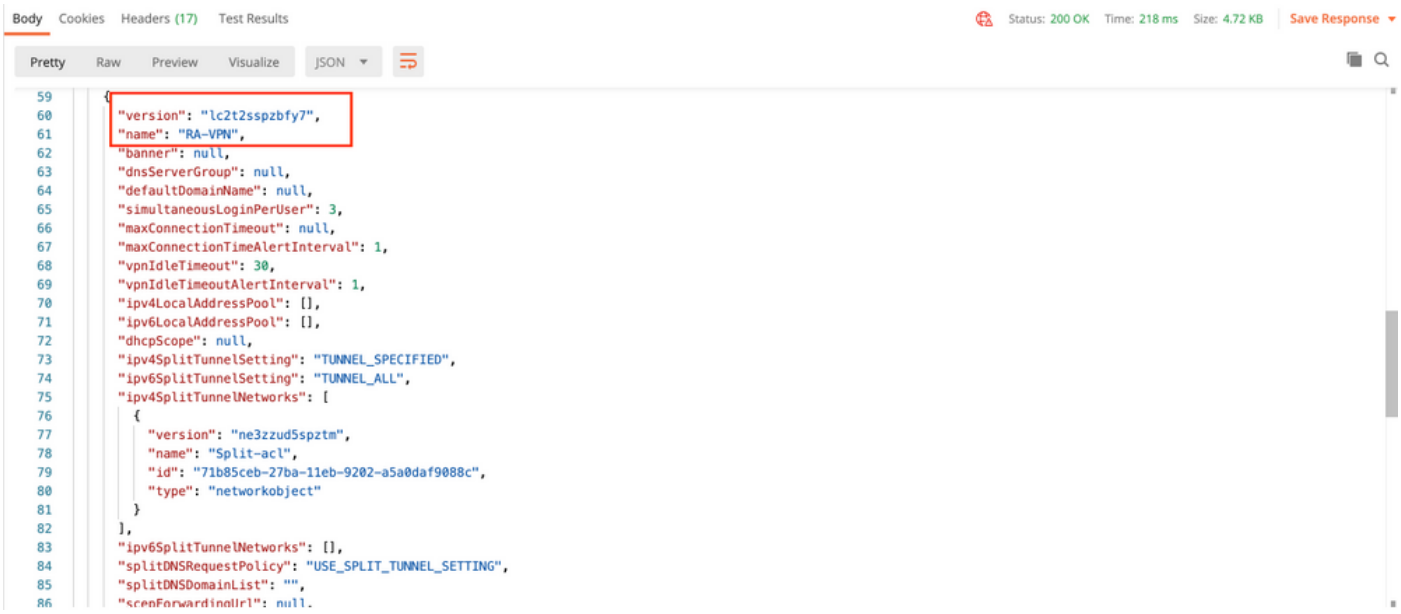
L'onglet Autorisation doit contenir ceci pour toutes les demandes GET/POST suivantes :

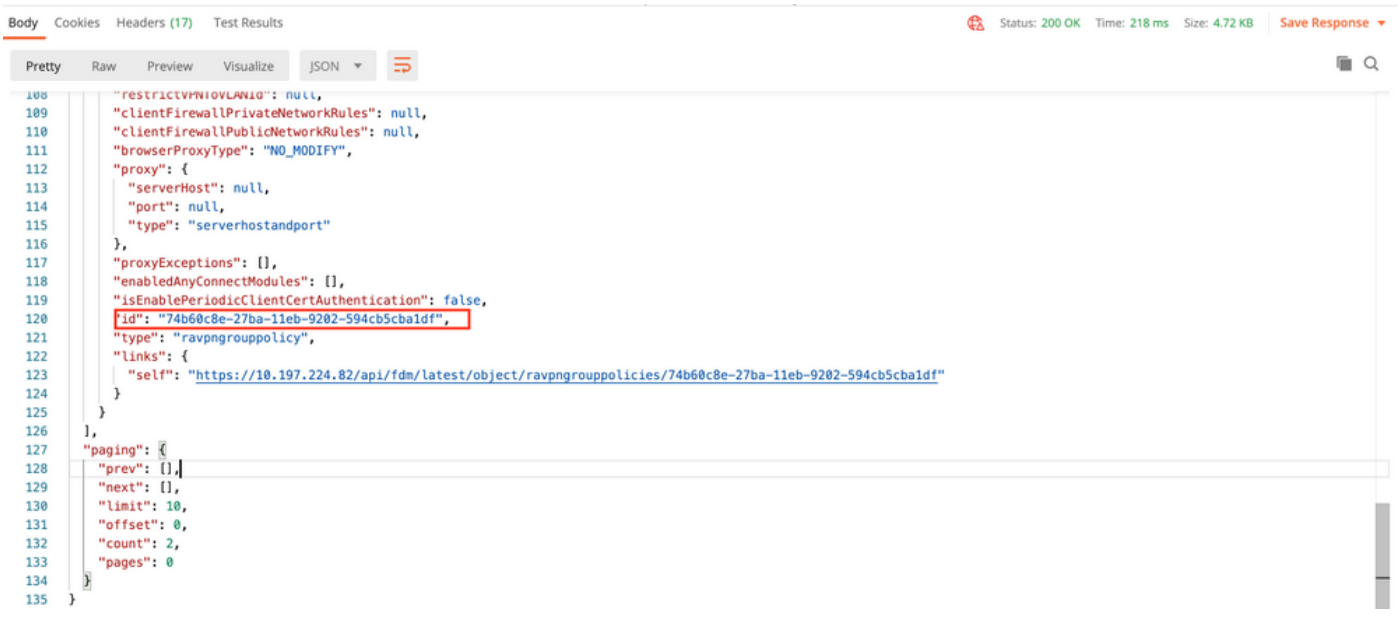
Type Jeton porteur
Jeton Jeton d'accès reçu en exécutant la demande auth POST

GET REQUEST : **https://<FTD Management IP>/api/fdm/last/object/ravpngrouppolicies**



Le corps de la réponse affiche toutes les stratégies de groupe configurées sur le périphérique. **ID** de la stratégie de groupe est utilisé pour mettre à jour la stratégie de groupe spécifique.





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

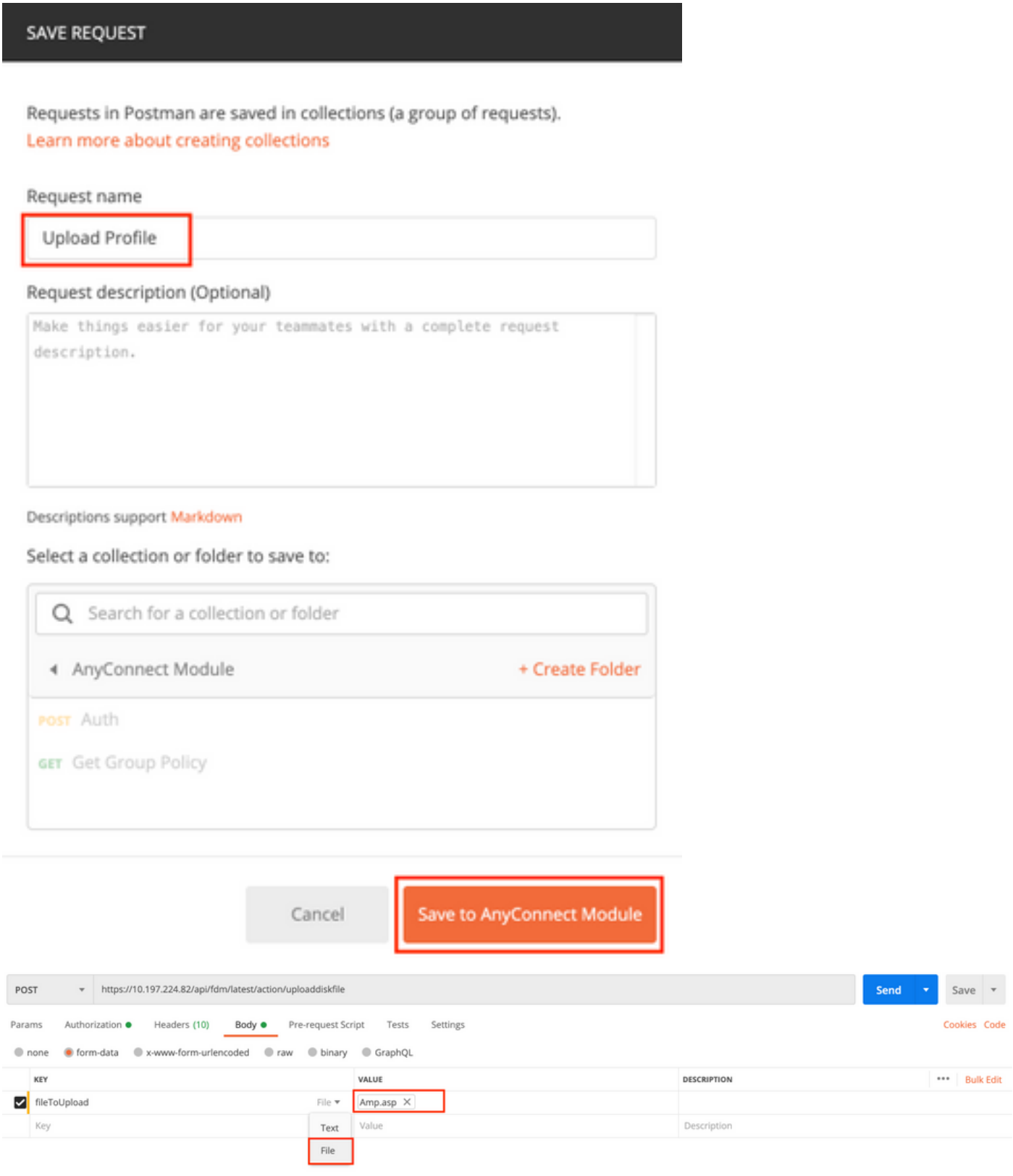
Étape 5. Créez une demande pour **télécharger un profil.** Cette étape est nécessaire uniquement

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/last/action/uploaddiskfile**

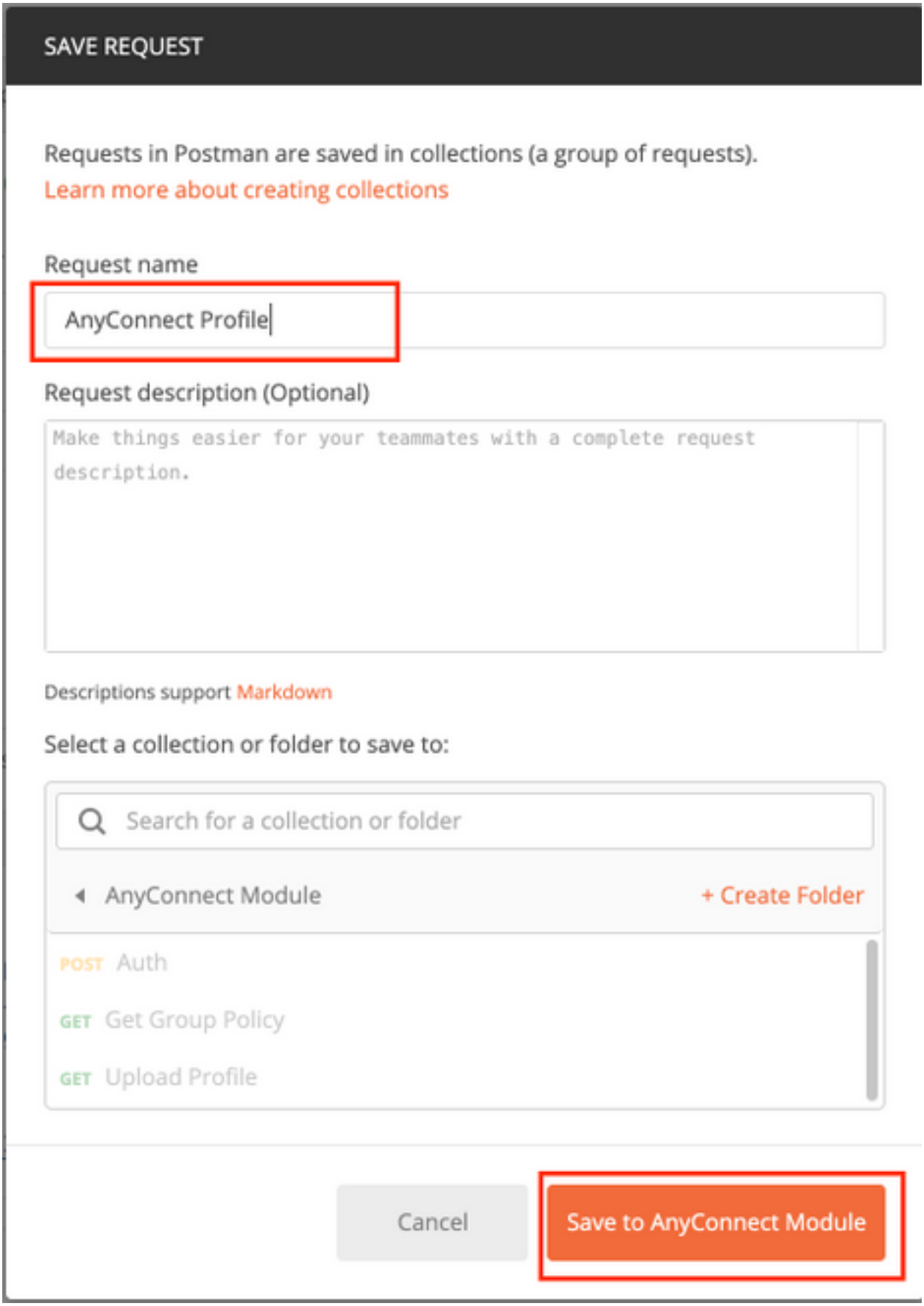
Le corps de la requête doit contenir le fichier de profil ajouté dans Body au format de données de formulaire. Le profil doit être créé à l'aide de [AnyConnect Profile Editor pour Windows]

Le type de clé doit **être FileforfiletoUpload**.



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

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.

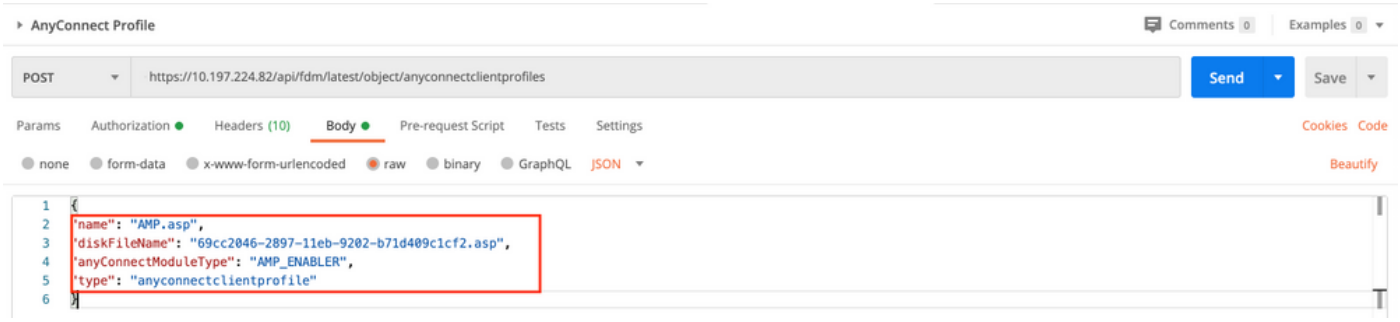


REQUÊTE POST : **https://<FDM IP>/api/fdm/last/object/anyconnectclientprofile**

Le corps de la demande contient ces informations :

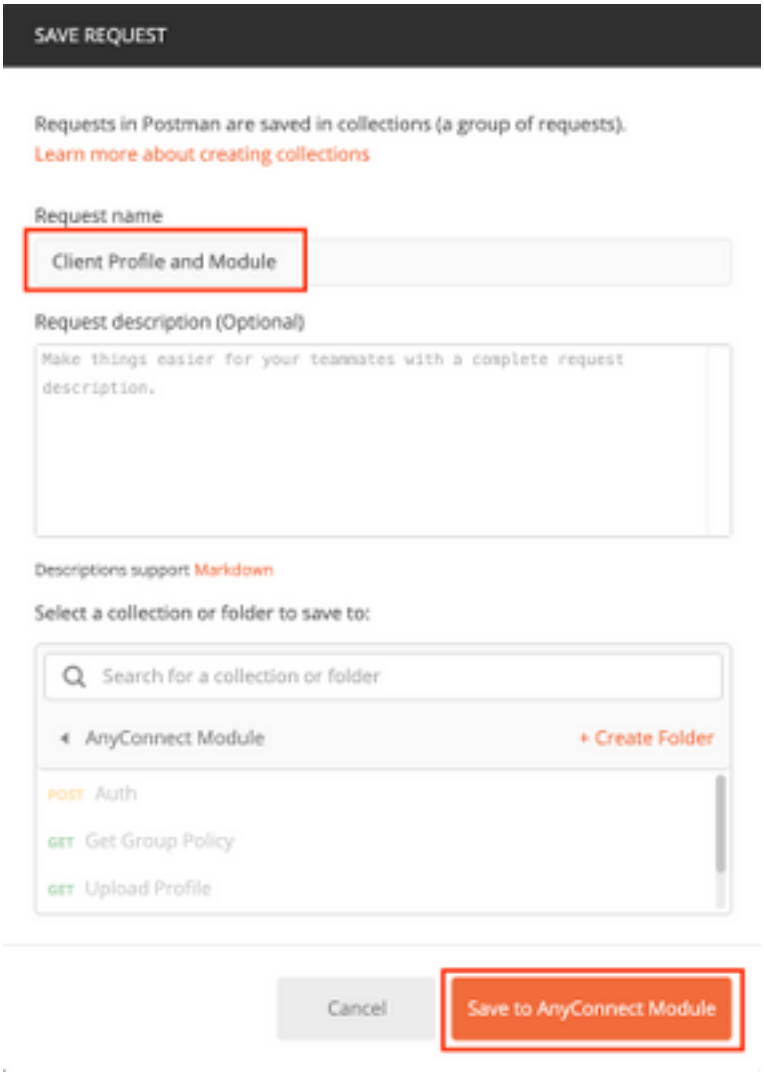
name (nom)	Nom logique que vous appelleriez le fichier
NomFichierDisque	Doit correspondre au nom de fichier reçu dans la réponse de test POST de p

	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.



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

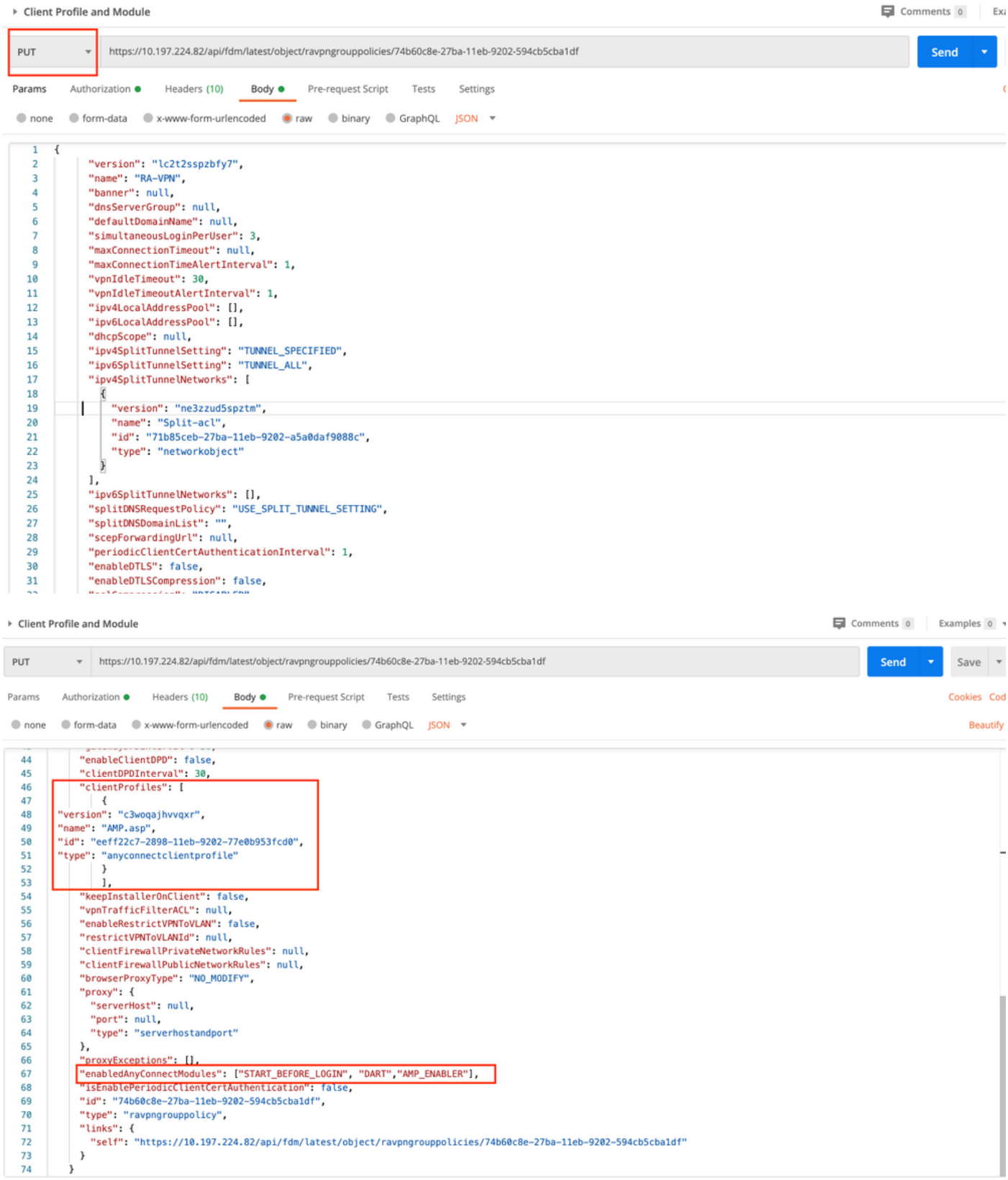
ObjId est l'ID obtenu à l'étape 4. Copiez le contenu de la politique de groupe concernée obtenue à l'étape 4 dans le corps de la demande et ajoutez ceci :

Profil client

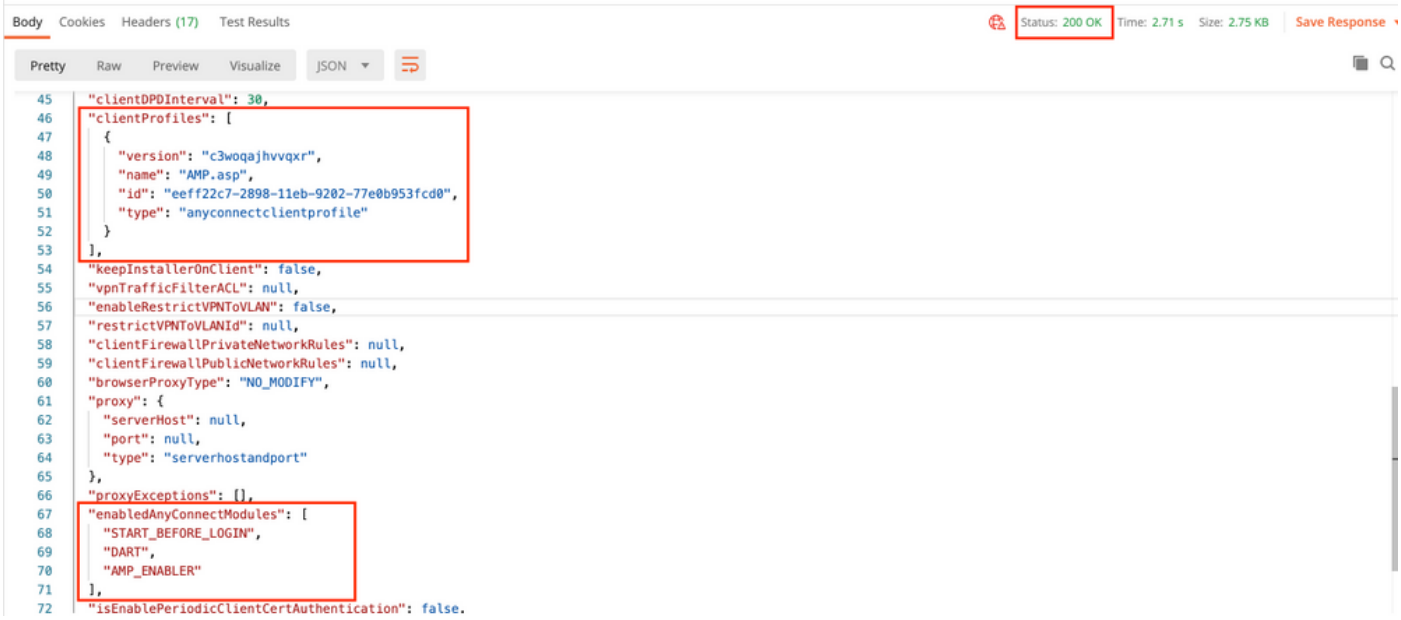
Nom, version, ID et type de profil reçus à l'étape précédente.

Modules clients

Le nom du module qui doit être activé doit correspondre exactement à celui indiqué dans la table du module.

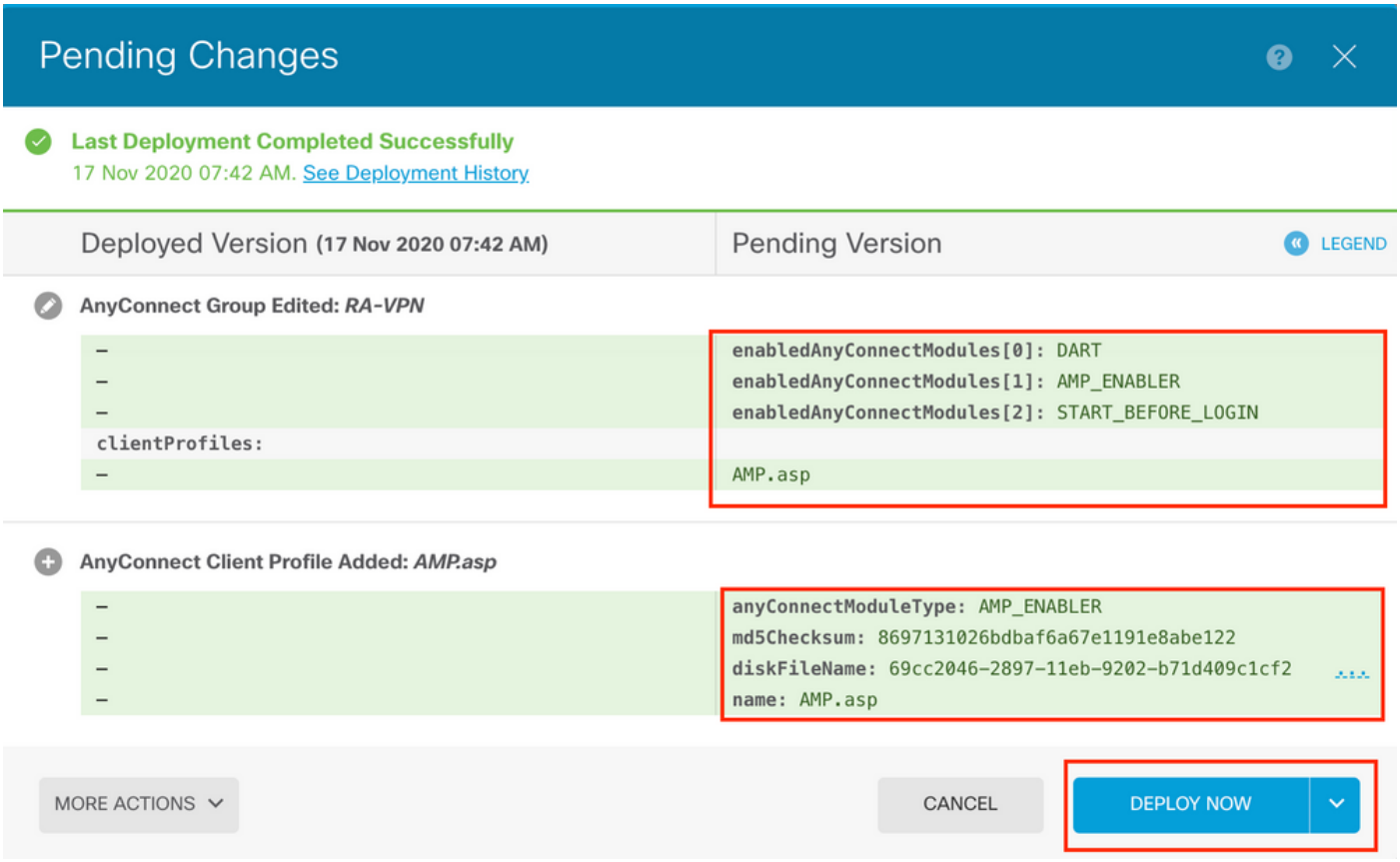


Le corps de la réponse affiche le profil et le module correctement liés à la stratégie de groupe.



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.



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

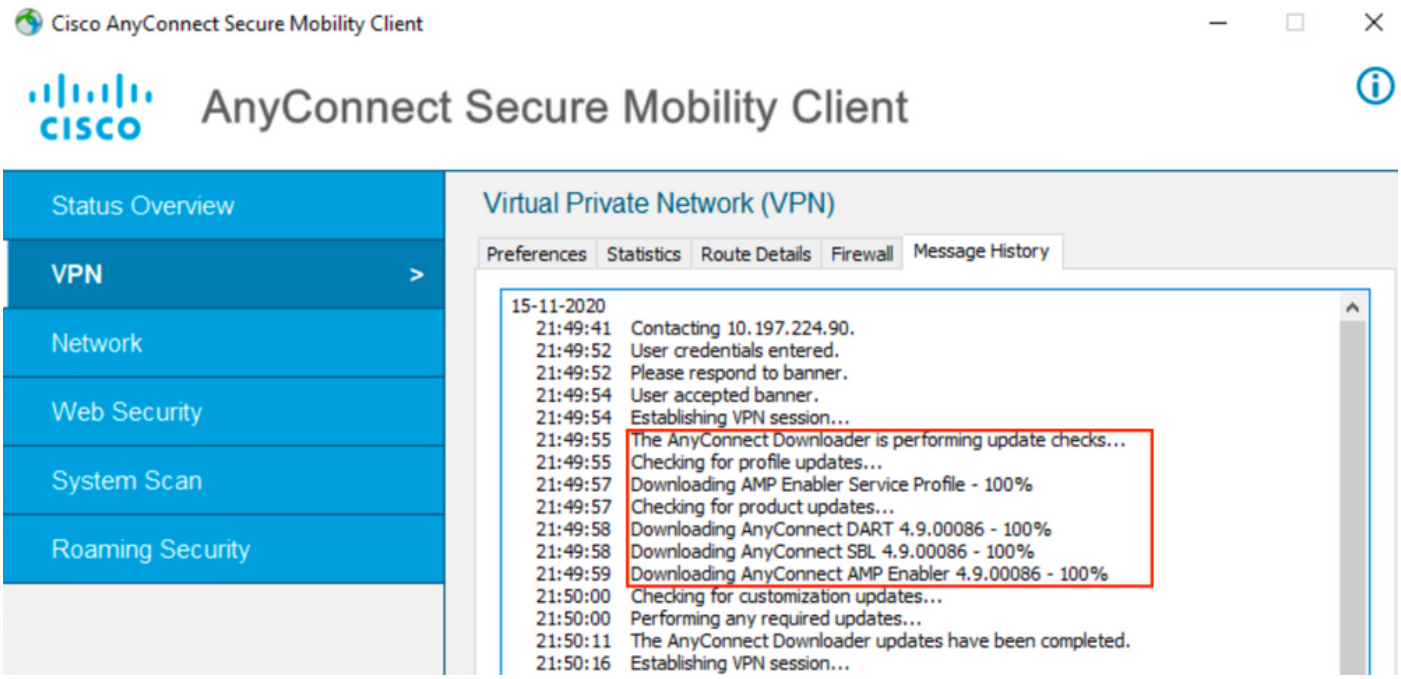
```
!--- RA VPN Configuration ---!
```

```
webvpn
enable outside
anyconnect image disk0:/anyconnpkgs/anyconnect-win-4.9.00086-webdeploy-k9.pkg 2
 anyconnect profiles AMP.asp disk0:/anyconncprofs/AMP.asp
 anyconnect profiles defaultClientProfile disk0:/anyconncprofs/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.



Dépannage

Collectez DART pour résoudre les problèmes liés à l'installation des modules clients.