# 在FTD上为远程访问VPN配置AnyConnect模块

## 目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[背景信息](#)
[配置](#)
[Firepower管理中心(FMC)上的配置](#)
[在Firepower设备管理器(FDM)上配置](#)
[验证](#)
[故障排除](#)

## 简介

本文档介绍如何为远程访问VPN(RA VPN)配置AnyConnect模块，该配置在由Firepower管理中心(FMC)通过Firepower设备管理器(FDM)管理的Firepower威胁防御(FTD)上预存。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 基本了解RA VPN工作。
- 了解通过FMC/FDM的导航。
- REST API和FDM Rest API资源管理器的基本知识。

### 使用的组件

本文档中的信息基于以下软件版本：

- 思科Firepower管理中心(FMC)版本6.7.0
- 思科Firepower威胁防御(FTD)版本6.7.0
- 思科Firepower设备管理器(FDM)版本6.7.0
- 运行4.9.0086的Cisco AnyConnect安全移动客户端
- 邮递员或任何其他API开发工具

**注意**：FMC/FDM没有内置配置文件编辑器，Windows的AnyConnect配置文件编辑器必须用于创建配置文件。

**注意**：本文档中的信息是从特定实验环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解任何配置更改的潜在影响。

# 背景信息

Cisco AnyConnect安全移动客户端不限于作为VPN客户端的支持，它还有许多其他选项可集成为模块。Anyconnect支持以下模块：

- 登录前启动(SBL)：此模块允许用户在登录Windows之前建立到企业的VPN连接。
- 诊断和报告工具(DART)：此模块用于执行有关AnyConnect安装和连接的诊断和报告。DART的工作方式是组合日志、状态和诊断信息进行分析。
- 高级恶意软件防护 (AMP)：此模块提供云交付的下一代解决方案，可检测、预防和应对各种威胁。
- ISE状态：思科身份服务引擎(ISE)提供下一代身份和访问控制策略。此模块提供识别主机上当前安装的操作系统(OS)、防病毒、反间谍软件等的功能。然后，此信息与策略一起使用，以确定主机是否能够连接到网络。
- 网络可视性模块：网络可视性模块监控终端应用的使用情况，以发现潜在的行为异常并做出更明智的网络设计决策。
- Umbrella：思科Umbrella漫游是一种云交付的安全服务，可在设备脱离公司网络时对其进行保护。
- 网络安全：思科网络安全设备(WSA)由思科Talos提供支持，通过自动阻止危险站点和测试未知站点来保护终端。
- 网络接入管理器：网络接入管理器根据其策略提供安全的第2层网络。它检测并选择最佳第2层接入网络，并执行设备身份验证以访问有线和无线网络。
- 反馈:此模块收集信息并定期将其发送到服务器，帮助产品团队提高AnyConnect的质量、可靠性、性能和用户体验。

在Firepower 6.7中，添加了FMC UI和FTD设备REST API支持，以实现所有上述AnyConnect模块的无缝部署。


此表列出了配置文件扩展和关联 成功部署终端功能所需的模块类型。

| 配置文件扩展 | 模块类型 |
| --- | --- |
| .fsp | 反馈 |
| .asp或.xml | AMP_ENABLER |

| | |
|---|---|
| .sip或.xml | ISE_POSTURE |
| .nvmsp或.xml | 网络可视性 |
| .nsp或.xml | NETWORK_ACCESS_MANAGER |
| .json或.xml | 雨伞 |
| .wsp或.xml | WEB_SECURITY |

**注意：** DART和SBL模块不需要任何配置文件。

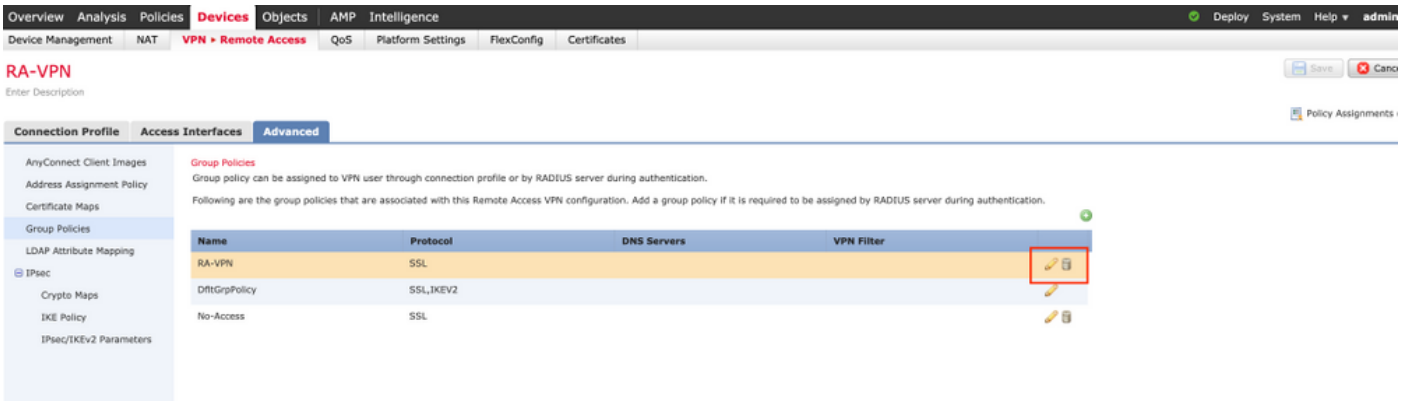
**注意：**使用此功能无需额外许可。

# 配置

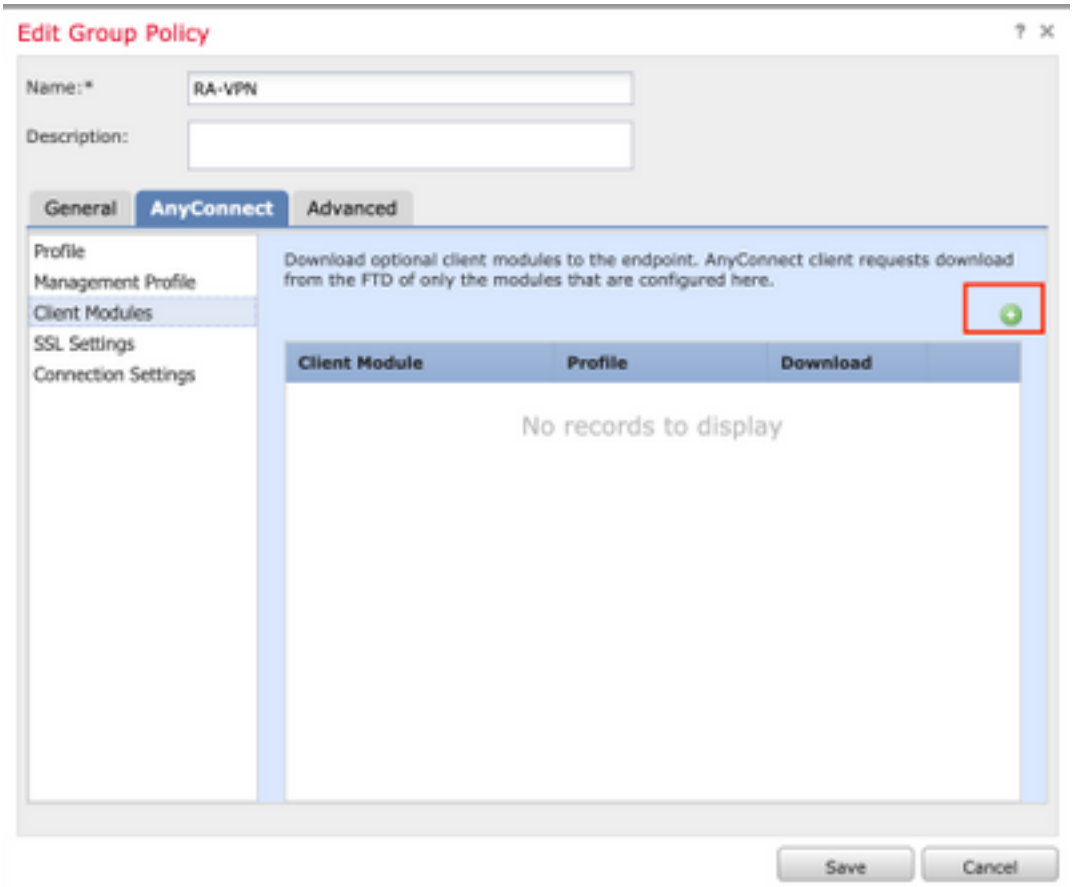
## Firepower管理中心(FMC)上的配置

**步骤1:** 导航至**Device > VPN > Remote Access**，然**后点击Edit** 以进行RA VPN配置。


**第二步：** 导航至**Advanced > Group Policies**，然后单击相关组策略的Edit，如下图所示。

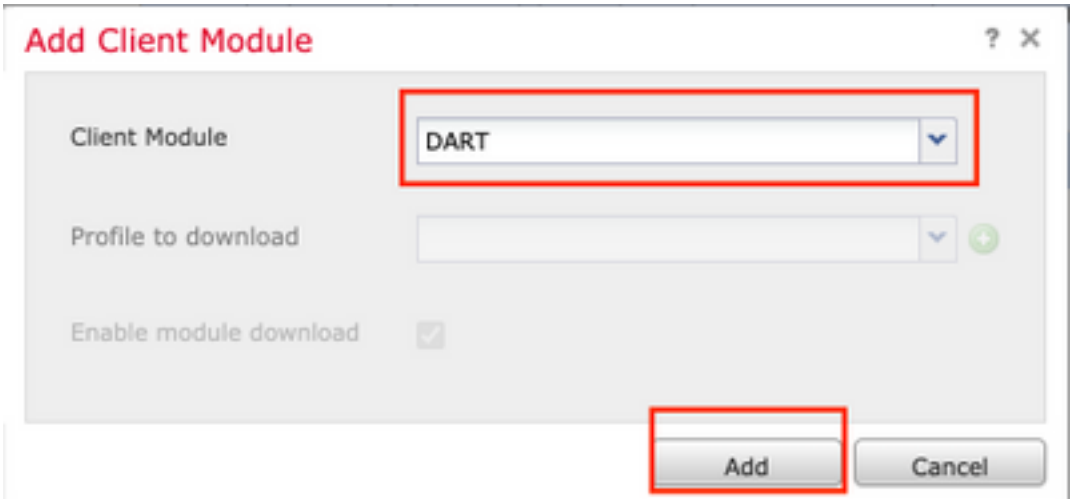



**第三步：** 导航至**AnyConnect > Client Modules**并单击**+以添加模块，如此图所示。**

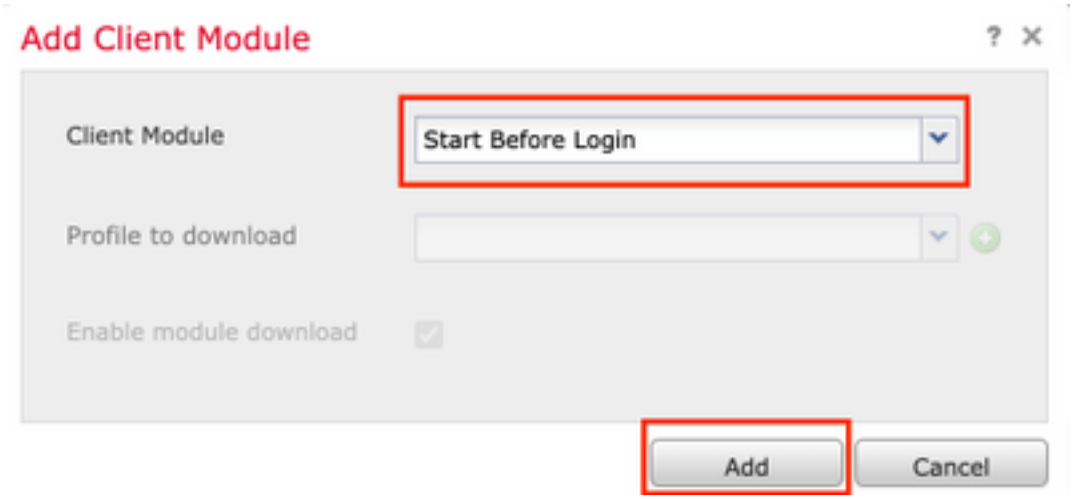



为了进行演示，显示了AMP、DART和SBL模块的部署。

**第四步：** 选择**DART模**块并单击**Add**，如下图所示。

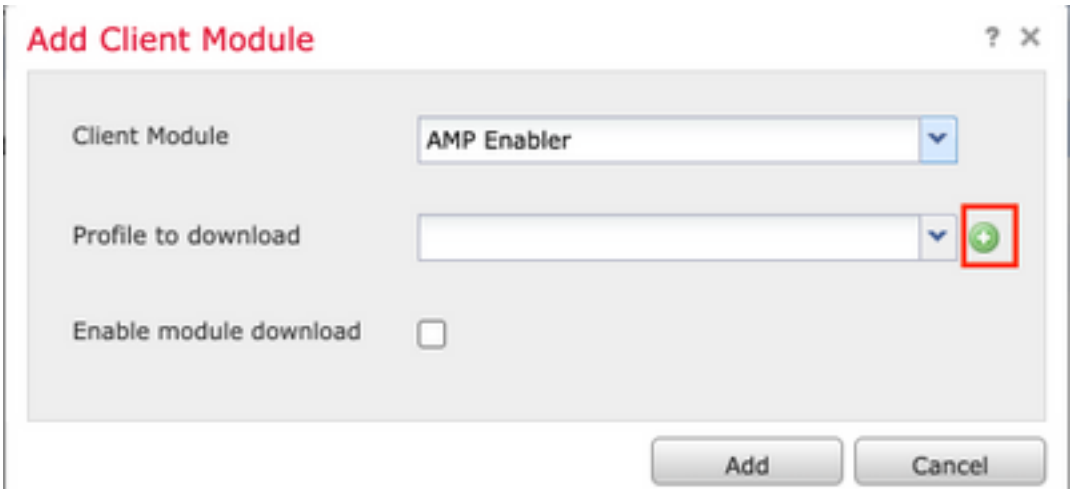



**第五步：** 单击**+以添**加另一个模块，并选**择"登录**前开始"模块，如下图所示。

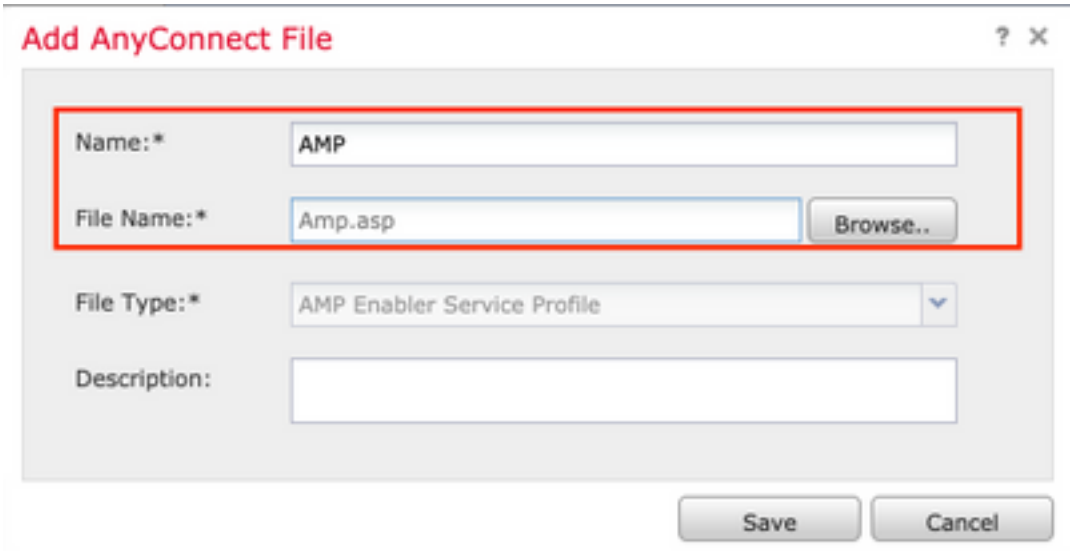



**注意**：此步骤允许您下载SBL模块。SBL还必须在anyconnect客户端配置文件中启用，在您导航至组策略下的AnyConnect**>配置文件时**，会上传该配置文件。

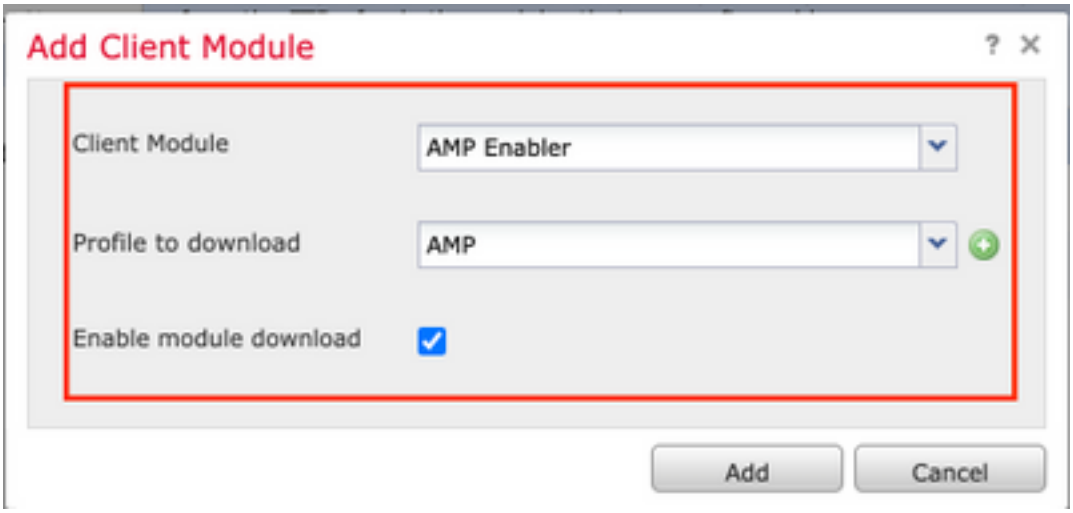
**第六步**： 单击+**以添**加另一个模块并选**择AMP启用码。** 单击+添加客户端配置文件，如此图所示。



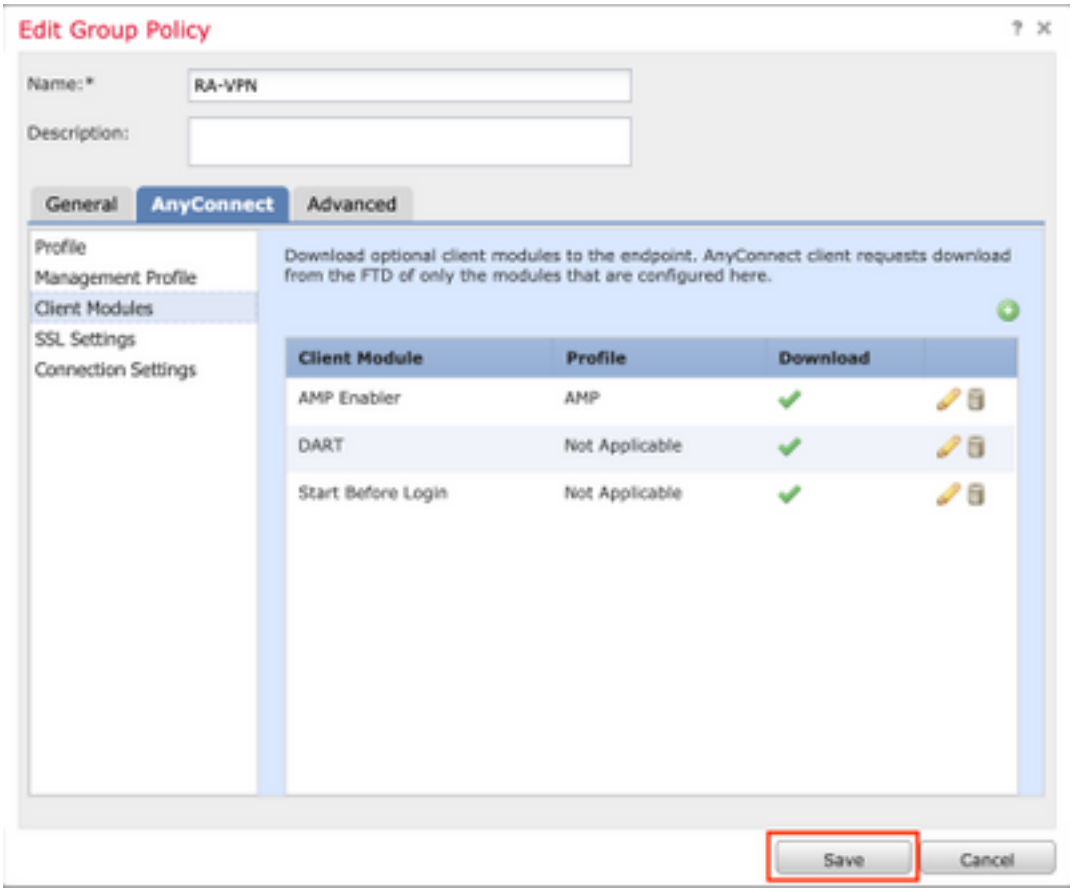

提供配**置文**件的名称并上传**AMP配置文件**。单击**Save**，如此图所示。



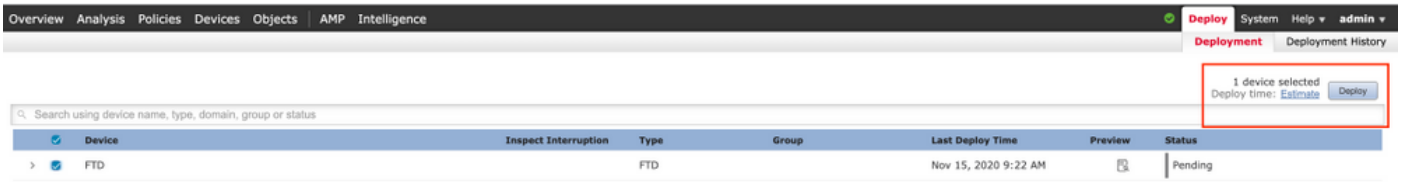

选择在上一步中创建的配置文件，然后单击"**启用模块下载**"复选框，如此图所示。




**步骤 7. 添加所有所需**模块后，单击“保存”。




**步骤8.**导航至“**部署**”>“**部署**”，并将配置部署到FTD。



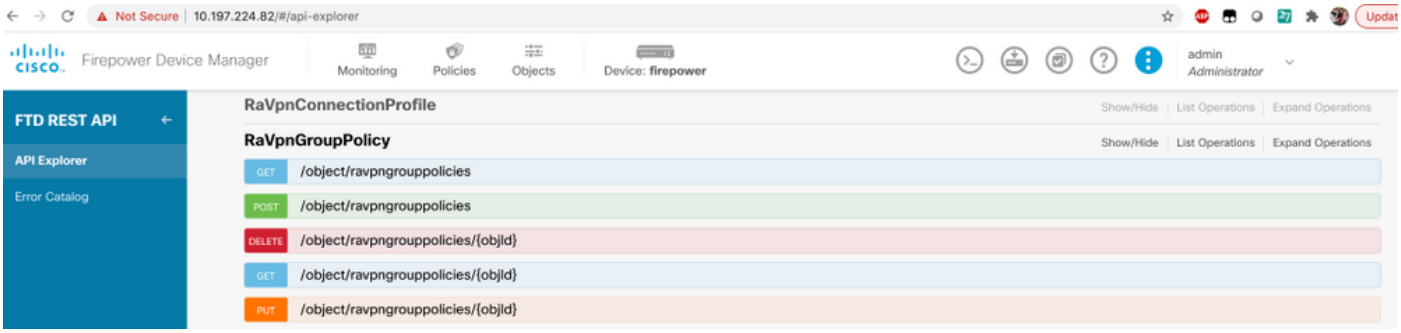

## 在Firepower设备管理器(FDM)上配置

**步骤1.**在浏览器窗口中启动FTD的API浏览器。

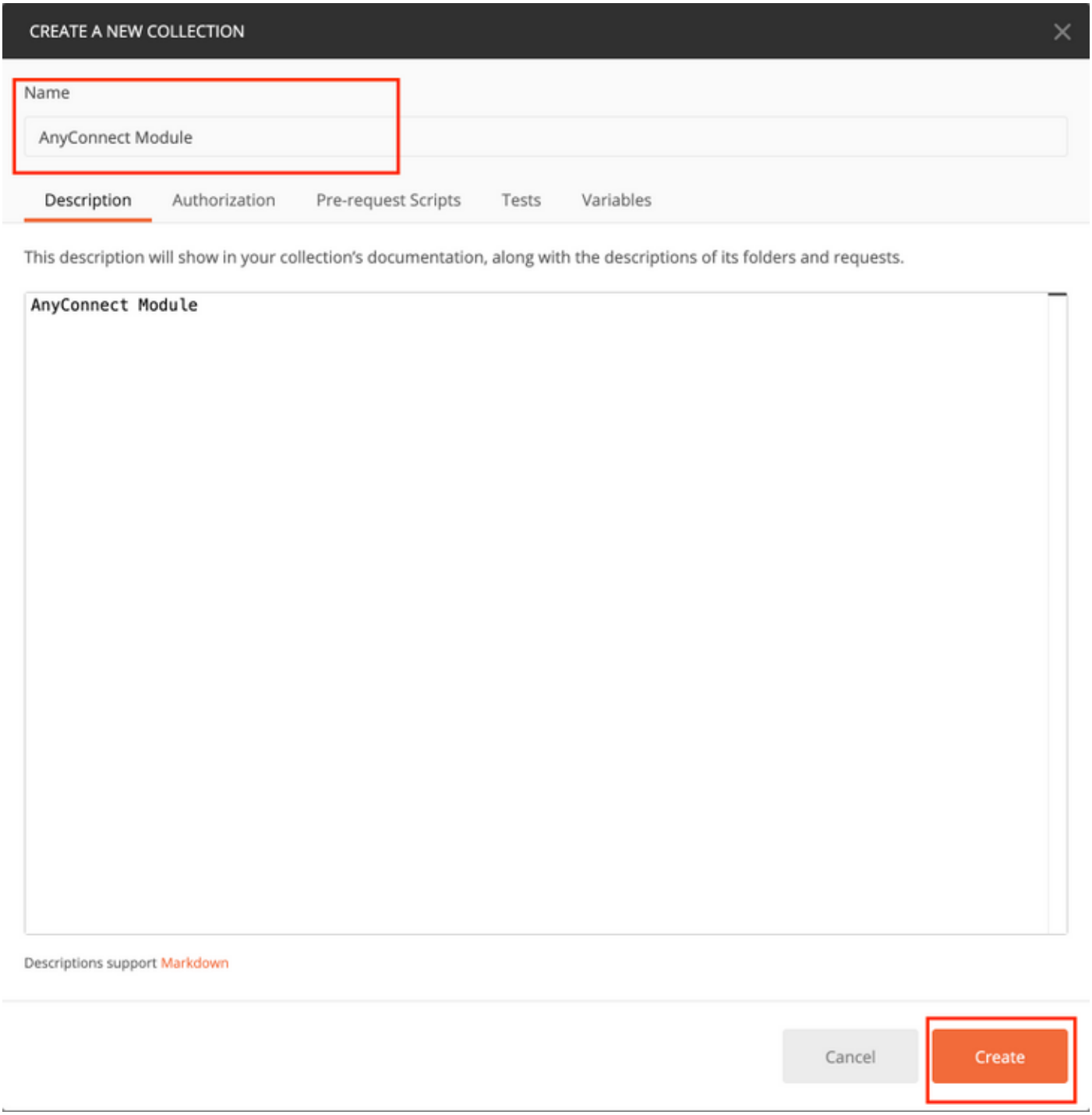
导航tohttps://<FTD Management IP>/api-explorer

这包含FTD上可用的API的完整列表。它根据FDM支持的多个GET/POST/PUT/DELETE请求的主要功能进行划分。

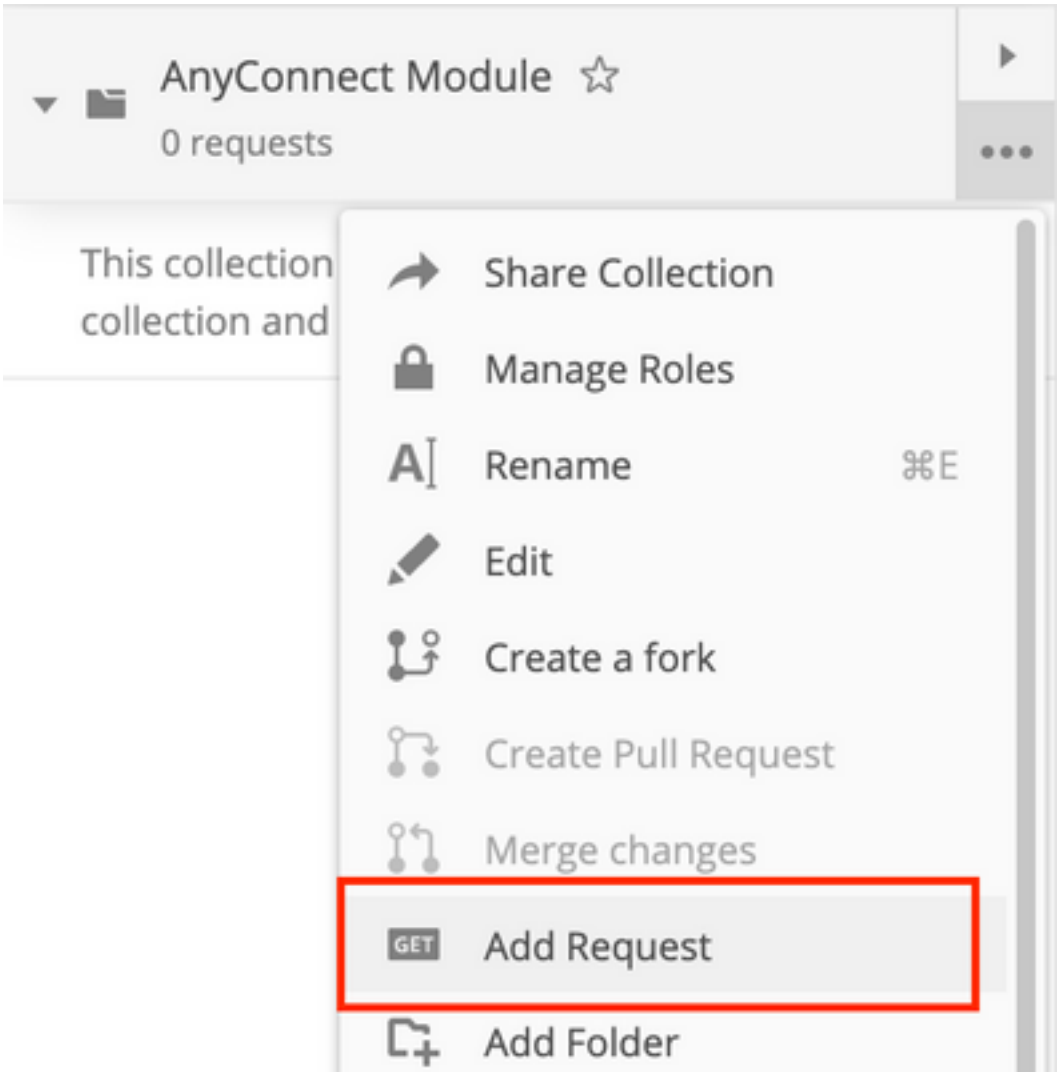
RaVpnGroupPolicy是使用的API。

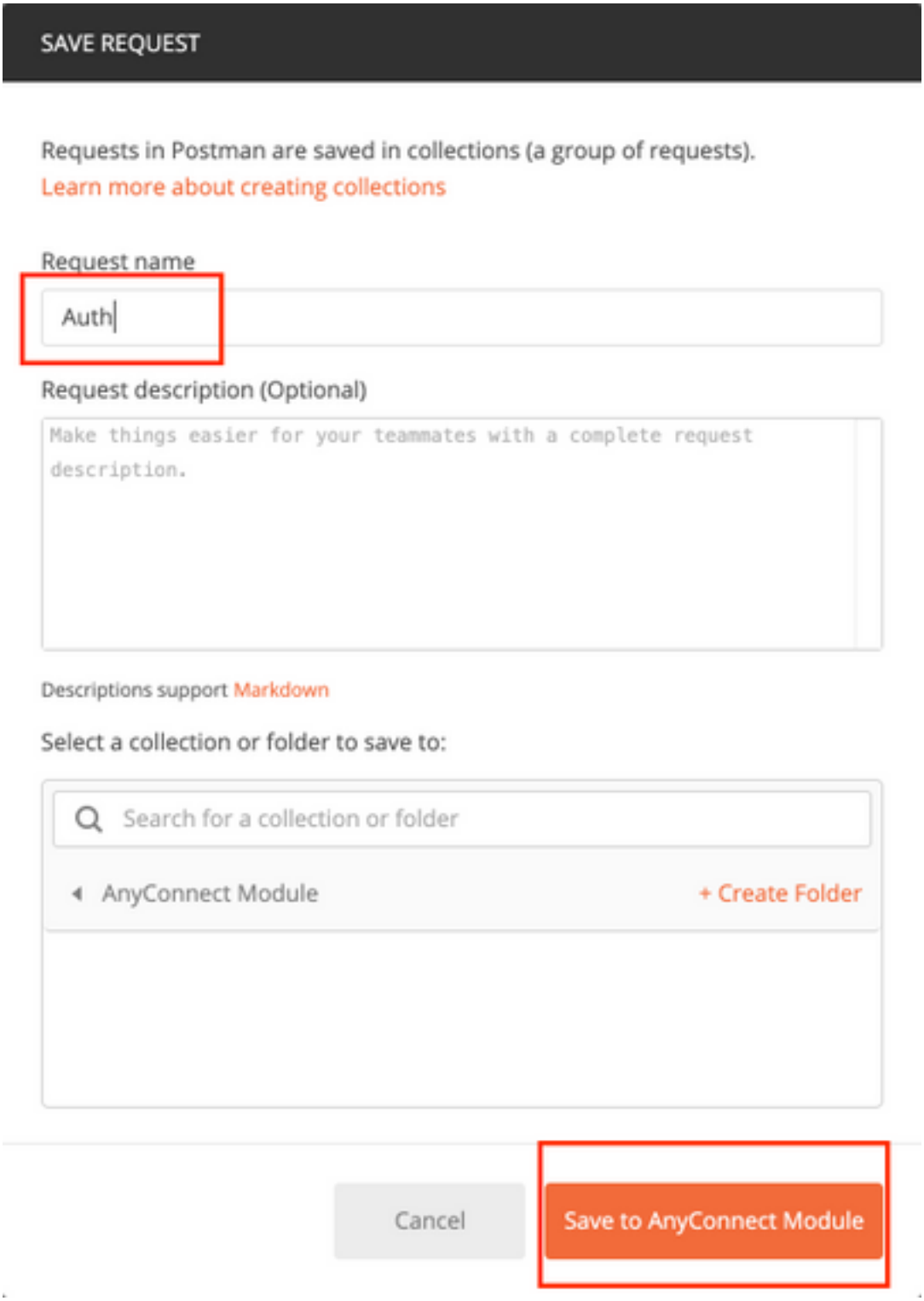



**第二步：** 为AnyConnect模块添加Postman集合。提供集合名称。单击“创建”。




**第三步：** 添加新请求 **auth** 创建到FTD的登录POST请求，以便获取令牌以授权任何POST/GET/PUT请求。单击“**Save(保存)**”。

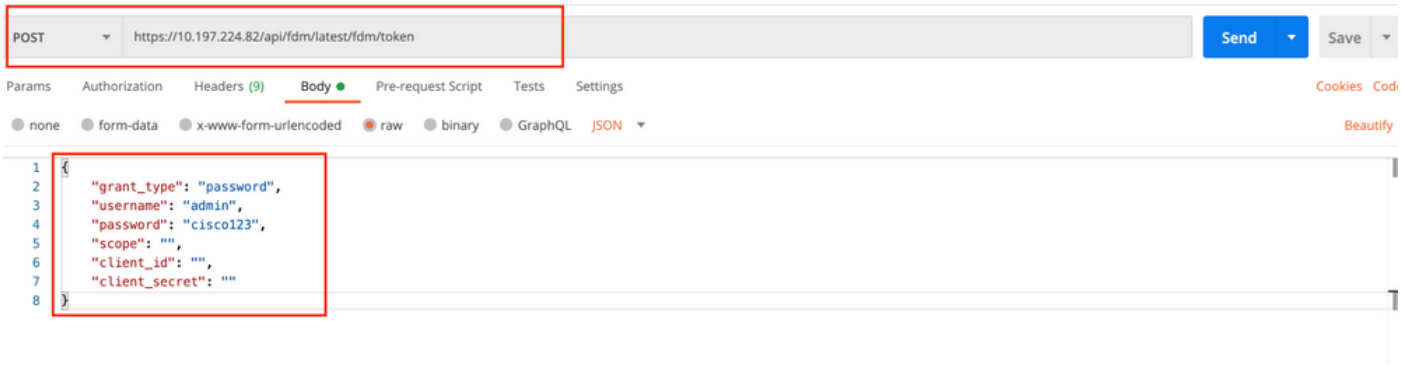

AnyConnect Module
0 requests
This collection
collection and
Share Collection
Manage Roles
Rename
⌘E
Edit
Create a fork
Create Pull Request
Merge changes
GET
Add Request
Add Folder




POST请求正文必须包含以下内容：

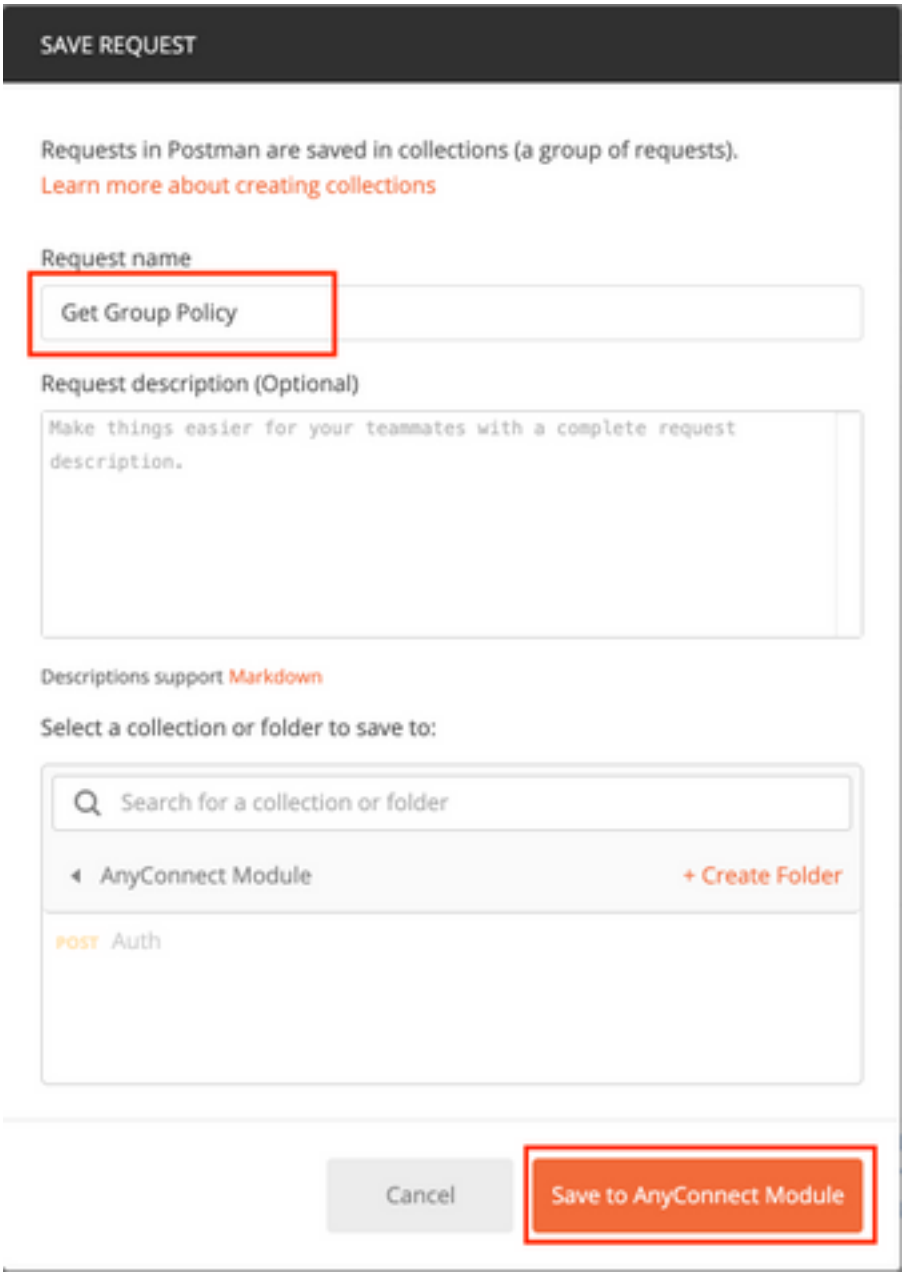
| | |
|---|---|
| **类型** | raw - JSON(application/json) |
| **grant_type** | 密码 |
| **用户名** | 登录FTD的管理员用户名 |
| **密码** | 与管理员用户帐户关联的密码 |

POST请求：**https://<FTD管理IP>/api/fdm/latest/fdm/token**




响应正文包含访问令牌，用于向FTD发送任何PUT/GET/POST请求。

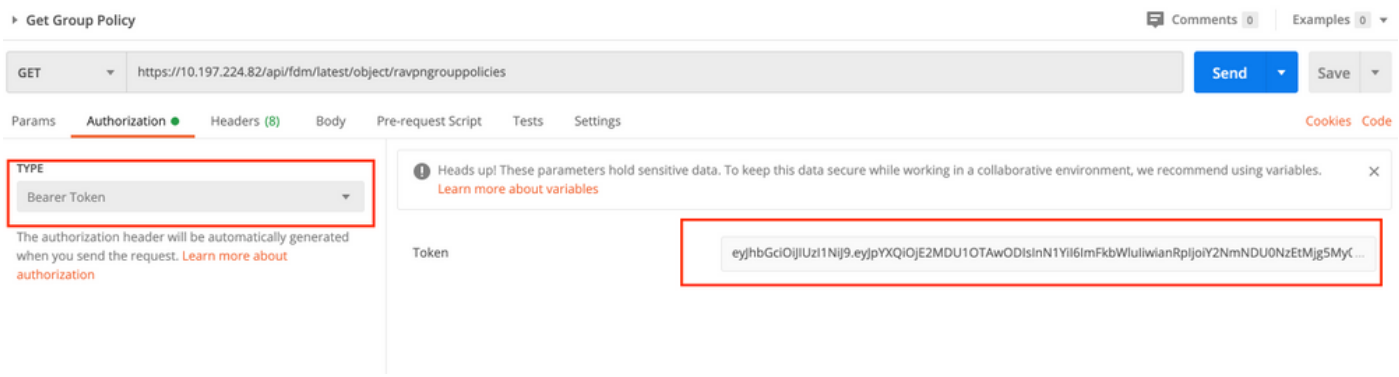

**第四步：** 创建**获取组**策略请求以添加现有组策略的获取详细信息。单击**保**存，如下图所示。



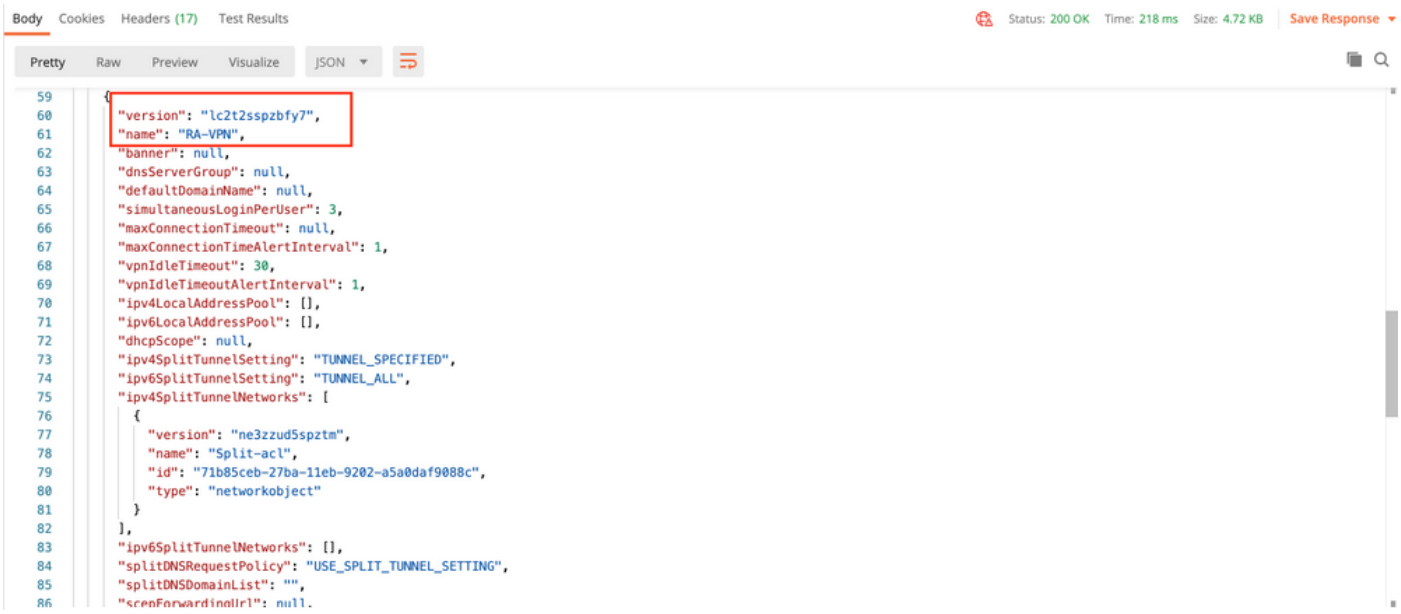

对于所有后续GET/POST请求，授权选项卡必须包含以下内容：

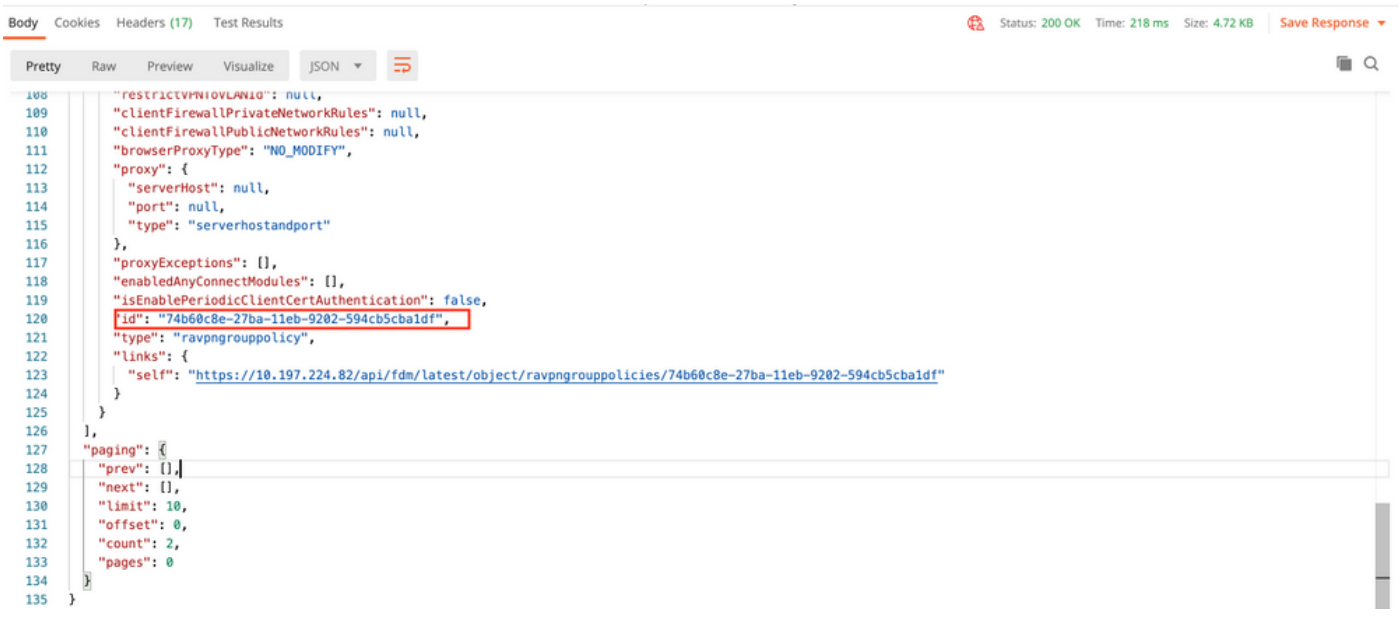
**类型** 承载令牌
**令牌** 通过运行Auth POST请求接收的访问令牌

GET请求：**https://<FTD管理IP>/api/fdm/latest/object/ravpngrouppolicies**




响应正文显示设备上配置的所有组策略。**组**策略的ID用于更新特定组策略。


为了进行演示，显示了AMP、DART和SBL模块的部署。

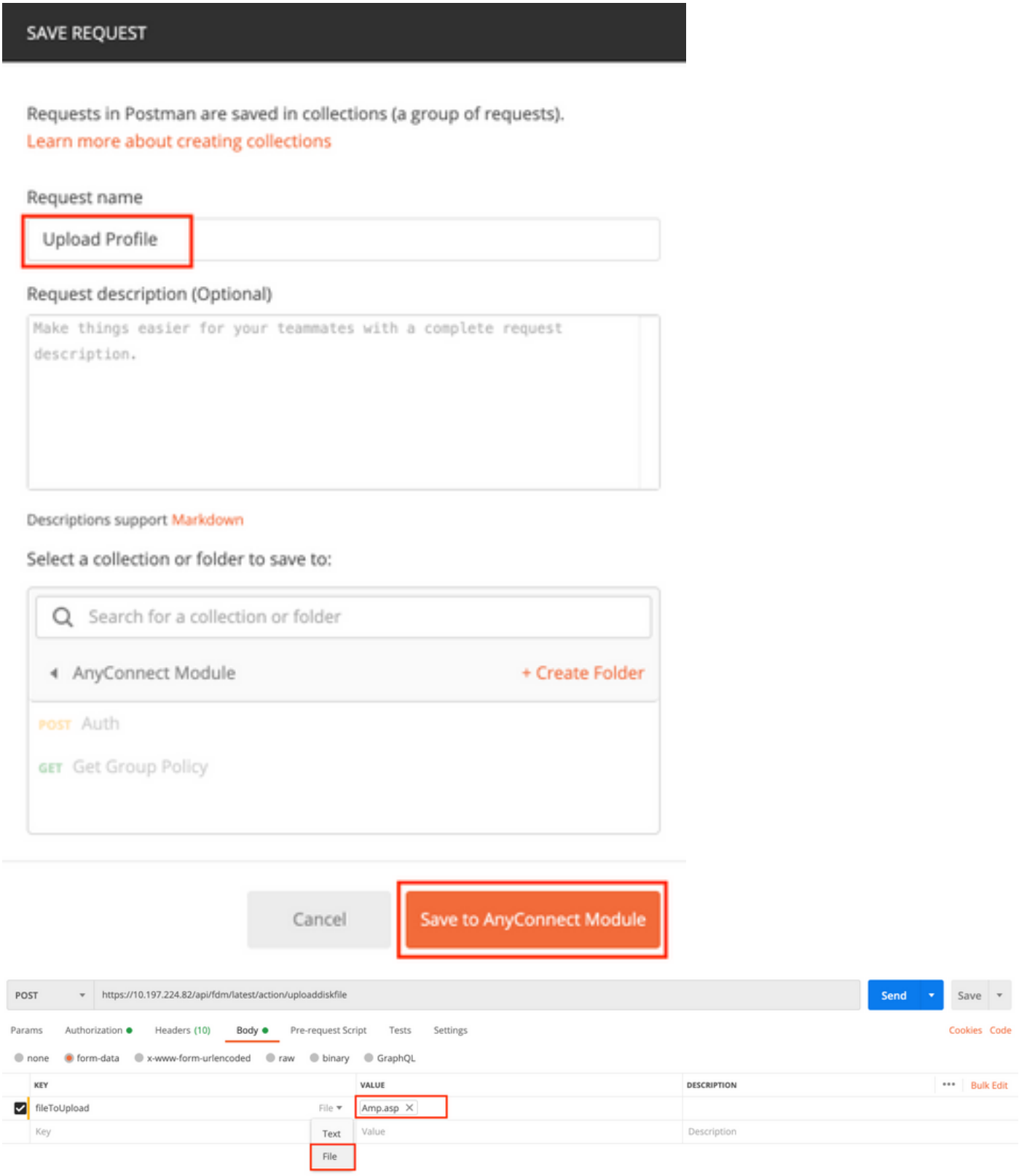
**步骤5.**创建请求**以上载配置**文件。此步骤仅对需要配置文件的模块需要。请在文件到上载部分中上

**载配置**文件。单击“**Save(保存)**”。

POST请求：**https://<FTD管理IP>/api/fdm/latest/action/uploaddiskfile**

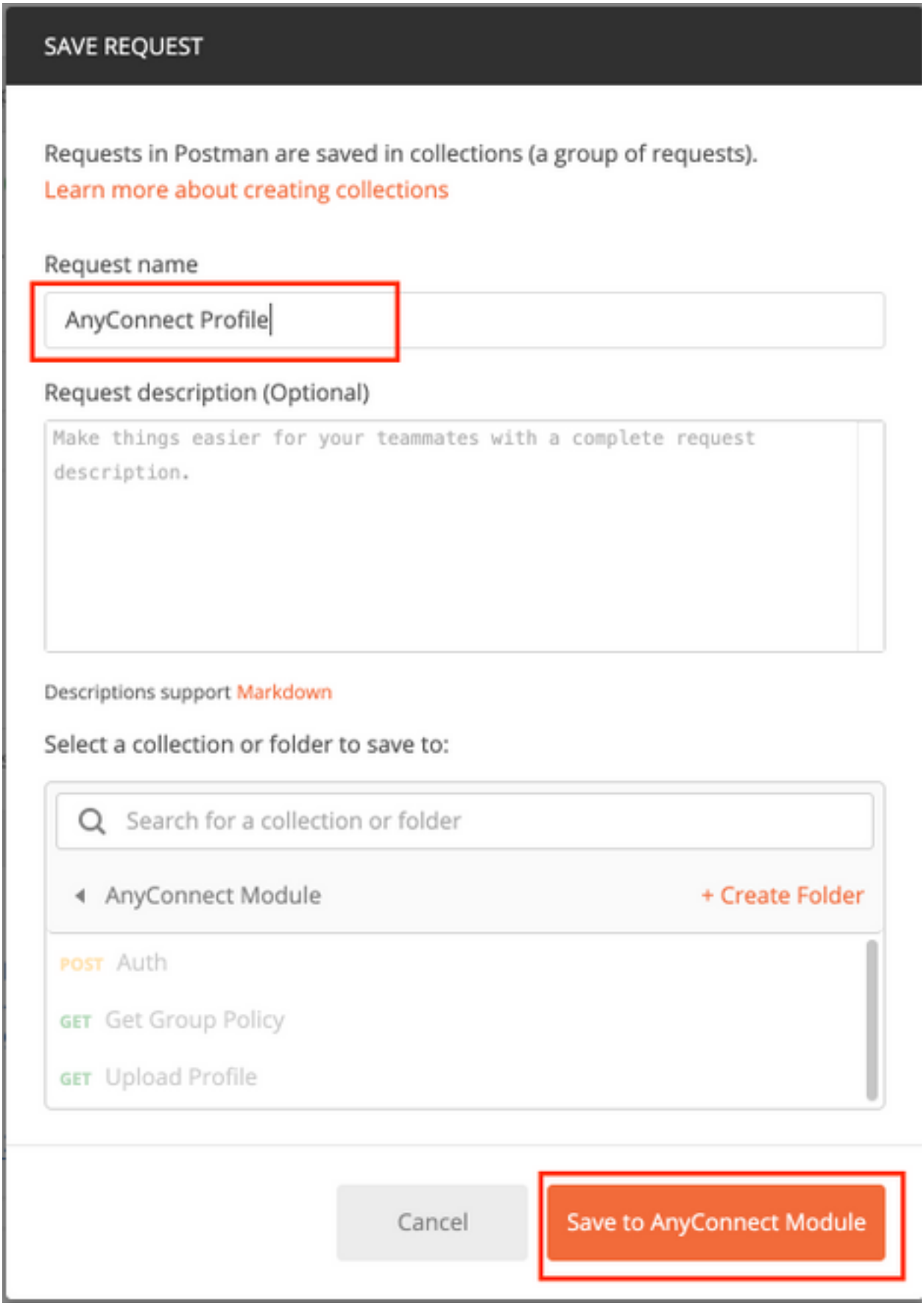
请求正文必须包含以表单数据格式添加在正文中的配置文件。需要使用AnyConnect Profile Editor for [Windows创建配置文件]

密钥类型应为**FileforfiletoUpload**。




响应的正文提供了ID/文件名，用于指代带有相关模块的配置文件。


**步骤6.**创建更新AnyConnect配置**文件的请**求。此步骤仅对需要配置文件的模块需要。单击**Save**，如此图所示。

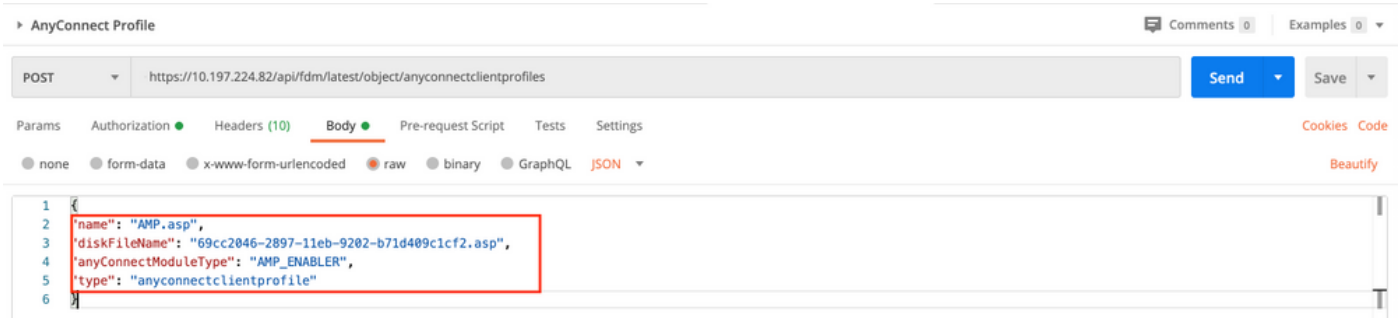



POST请求：**https://<FDM IP>/api/fdm/latest/object/anyconnectclientprofiles**

请求正文包含以下信息：

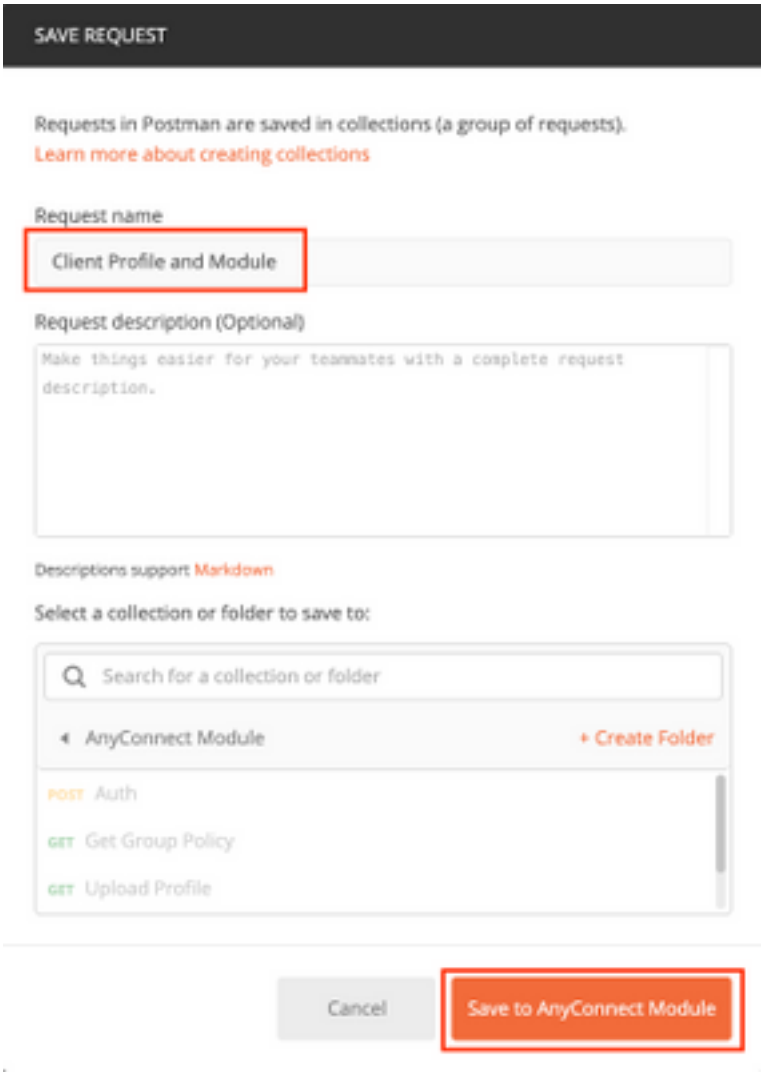
| 名称 | 要调用该文件的逻辑名称 |
| --- | --- |
| diskFileName | 需要与上传配置文件POST响应中收到的fileName匹配 |

| | |
|---|---|
| anyConnectModuleType | Meeds以匹配模块类型表中显示的相应模块 |
| 类型 | anyconnectclientprofile |




响应正文显示配置文件已准备好推送到设备。响应中收到的名称、版本、ID和类型将在下一步中用于将配置文件绑定到组策略。


**步骤6.创建PUT请求，将客户端配置文件和模块添加到现有单击Save，如此图所示。**




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

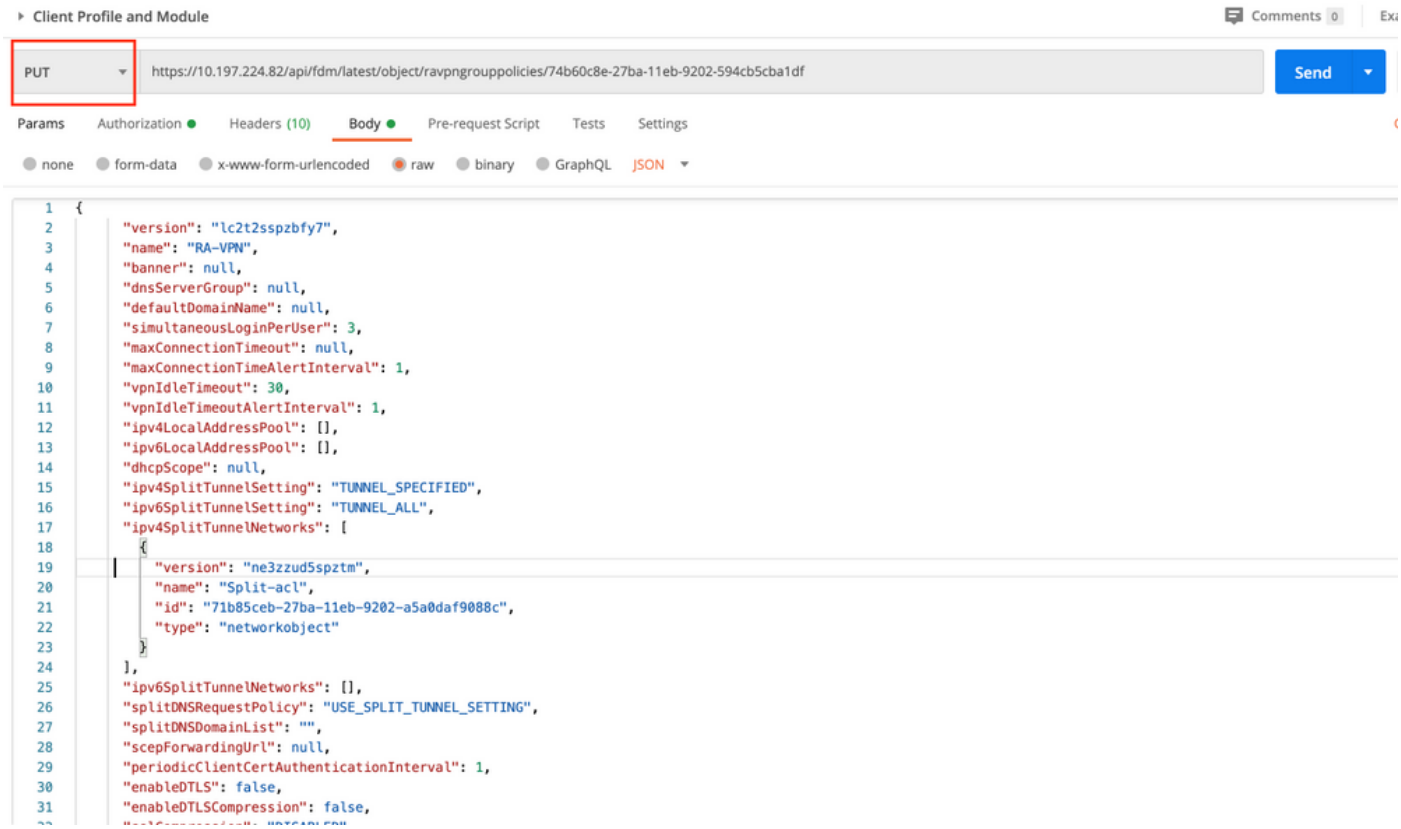
ObjId是在步骤4中获取的ID。将步骤4中获取的相关组策略的内容复制到请求的正文中，并添加以下内容：

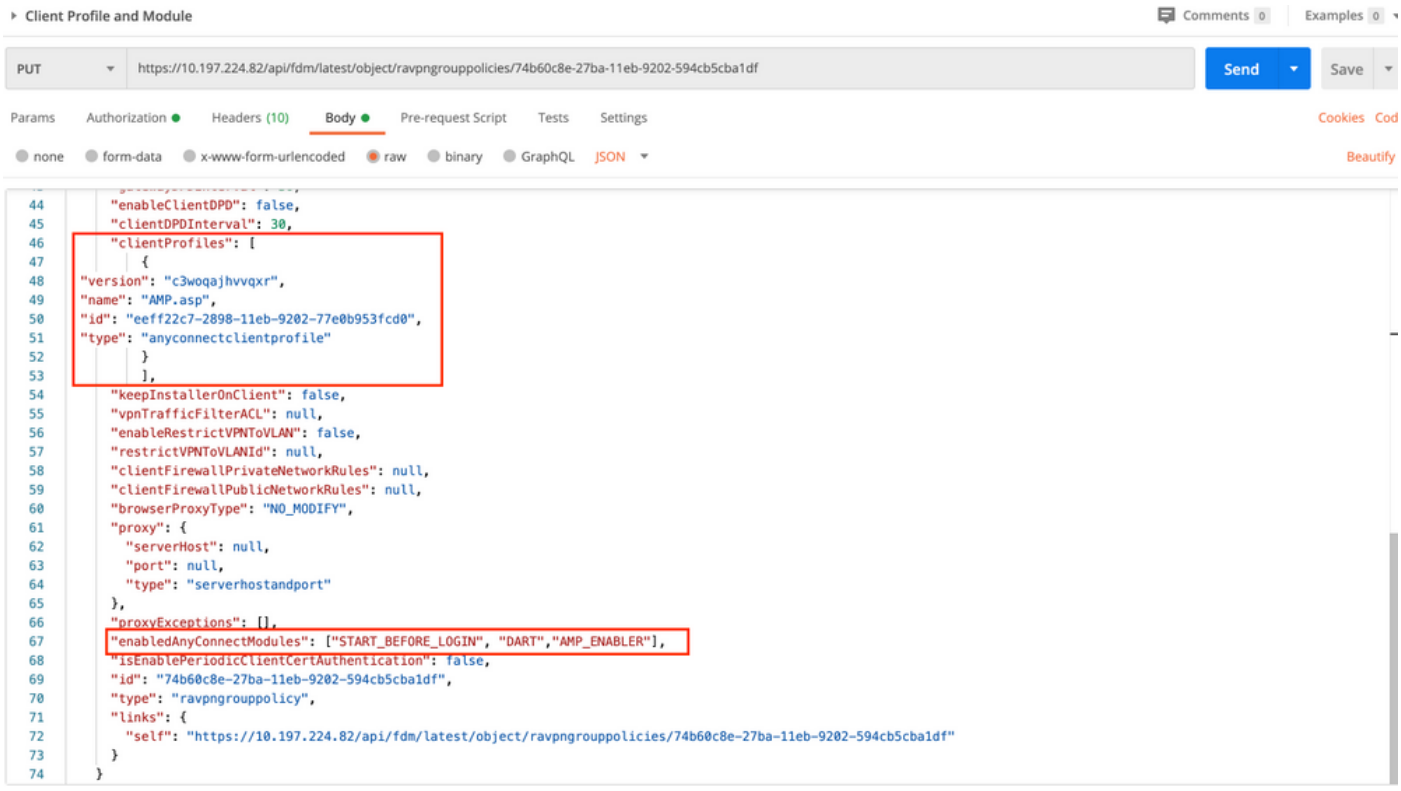
**客户端配置文件**

上一步中收到的配置文件的名称、版本、ID和类型。

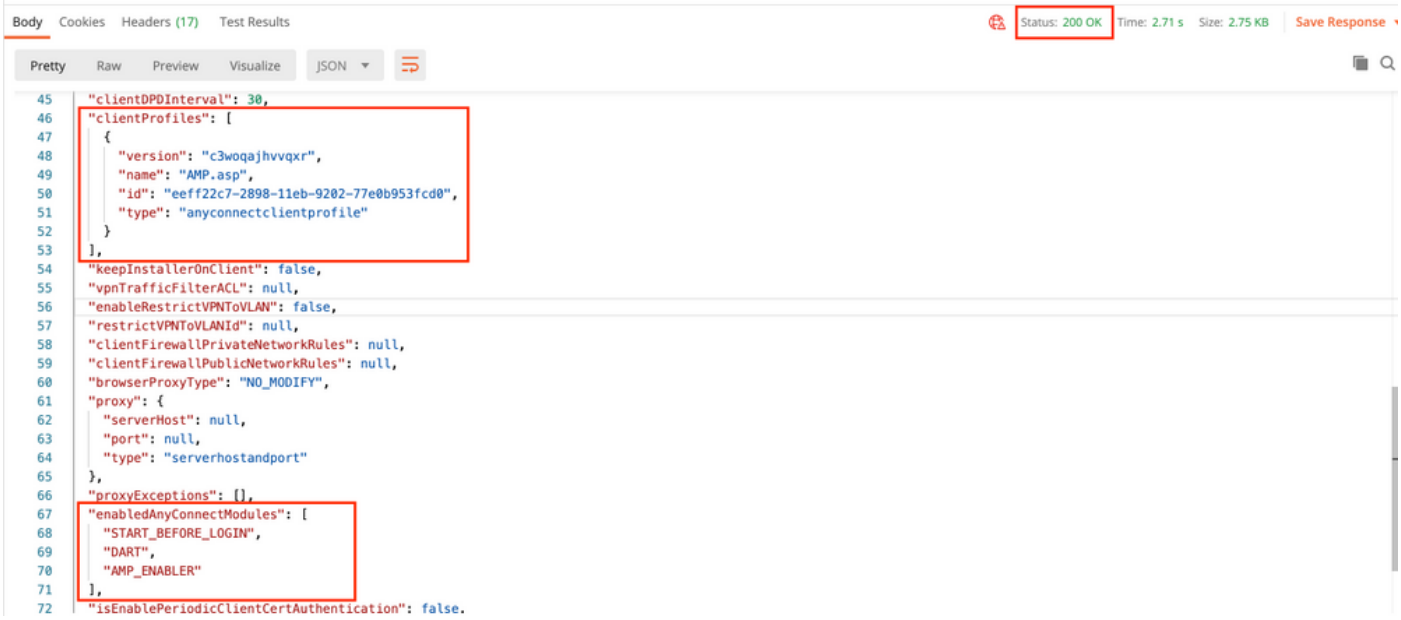
**客户端模块**

需要启用的模块的名称应与模块表中给定的名称完全匹配。



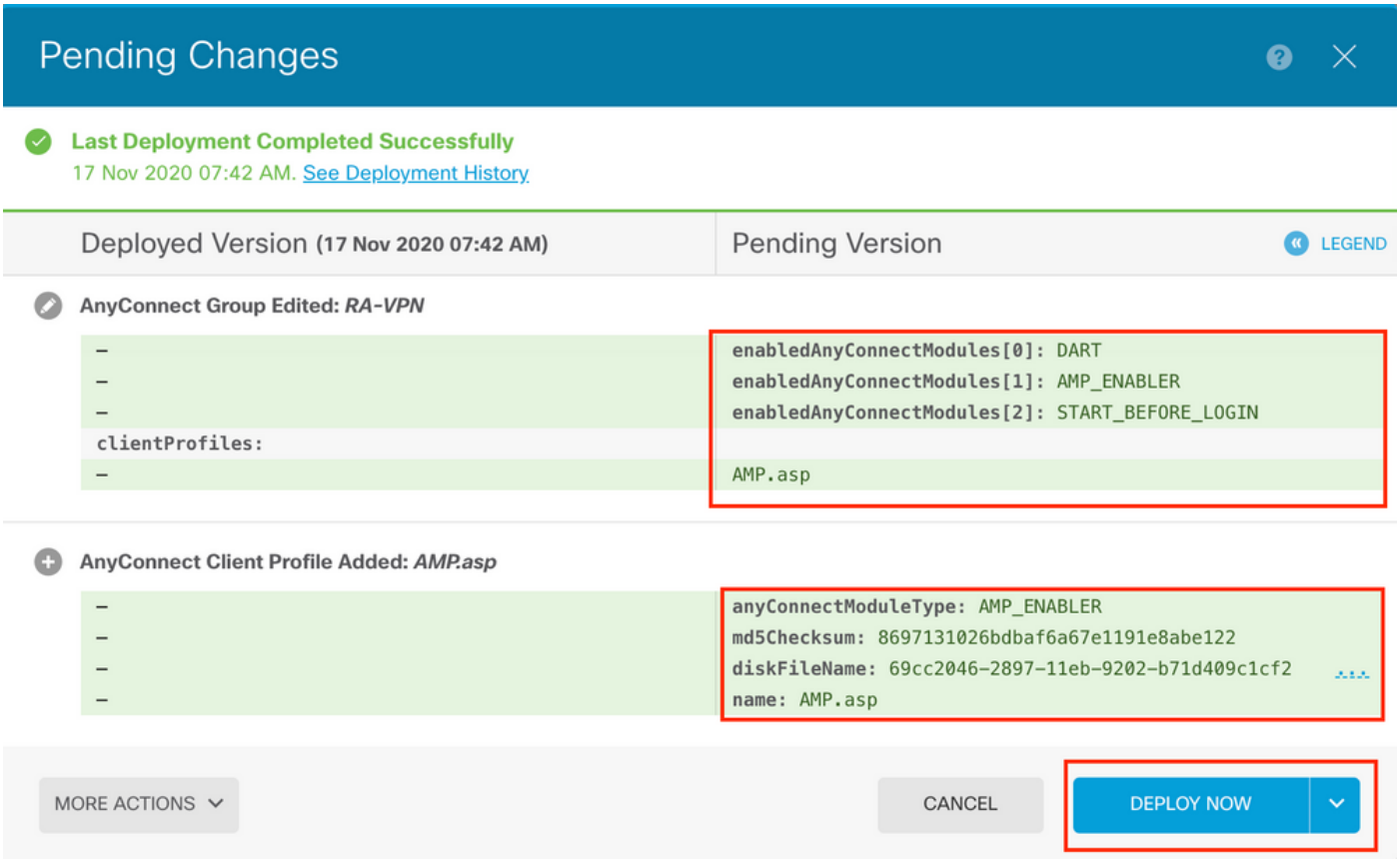




响应正文显示配置文件和模块已成功绑定到组策略。




**注意**：此步骤允许下载SBL模块。SBL还必须在anyconnect客户端配置文件中启用，当您导航到**Devices > Remote Access VPN > Group Policies > Edit Group Policy > General > AnyConnect Client Profile**时，可以上传该配置文件。

**步骤7.**通过FDM将配置部署到设备。挂起的更改显示要推送的客户端配置文件和模块。




成功部署后，将配置推送到FTD CLI:

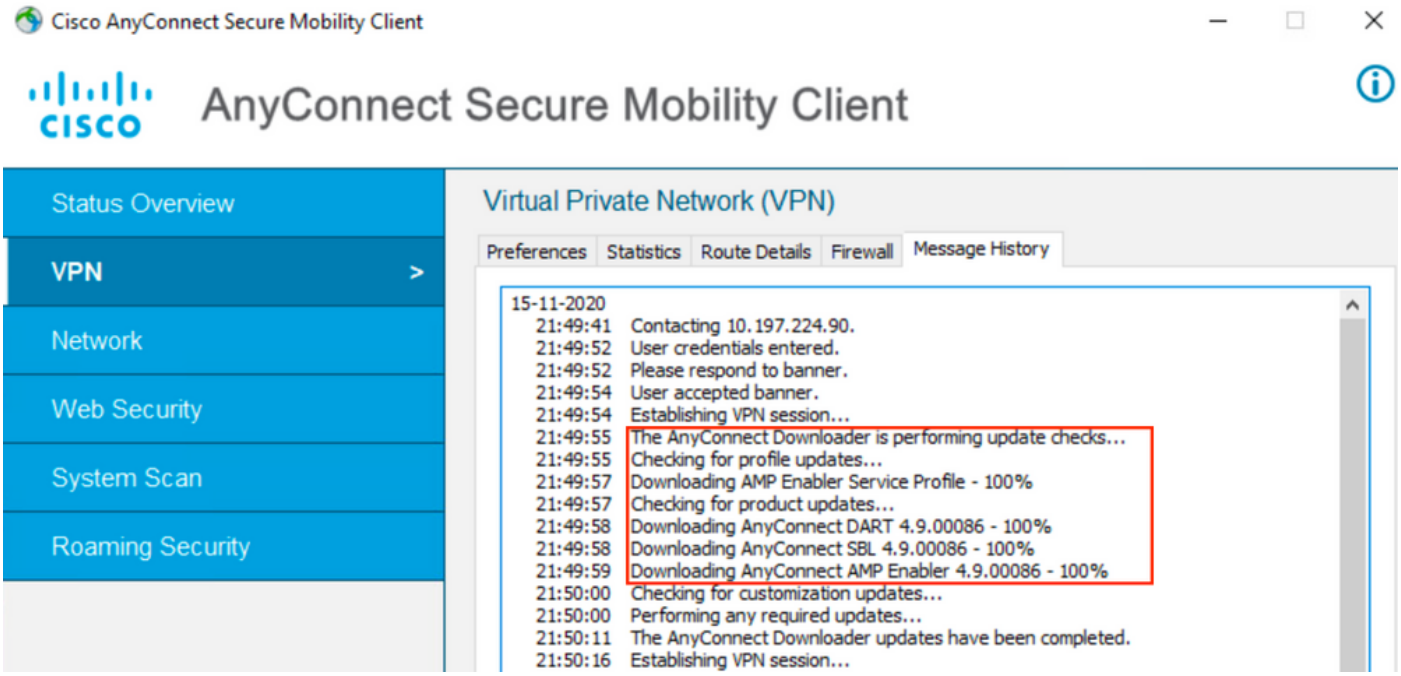
```
!--- RA VPN Configuration ---!

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
```

# 验证

建立与FTD的成功连接。

导航至**Settings > VPN > Message History**，查看有关已下载模块的详细信息。




# 故障排除

收集DART以排除客户端模块安装问题。