

Konfiguration von AnyConnect-Modulen für Remote Access VPN On FTD

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfiguration](#)

[Konfiguration auf FirePOWER Management Center \(FMC\)](#)

[Konfiguration im FirePOWER Device Manager \(FDM\)](#)

[Überprüfen](#)

[Fehlerbehebung](#)

Einführung

In diesem Dokument wird beschrieben, wie AnyConnect-Module für Remote Access VPN (RA VPN)-Konfiguration konfiguriert werden, die bereits auf einer FirePOWER Threat Defense (FTD) vorhanden ist, die von einem FirePOWER Management Center (FMC) über FirePOWER Device Manager (FDM) verwaltet wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundlegende Kenntnisse der RA VPN-Arbeit.
- Verständnis der Navigation durch das FMC/FDM.
- Grundkenntnisse der REST API und des FDM Rest API Explorer.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- 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 mit 4.9.0086
- Postman oder ein anderes API-Entwicklungstool

Hinweis: FMC/FDM verfügen nicht über einen integrierten Profil-Editor, und der [AnyConnect Profile-Editor](#) für Windows muss zum Erstellen eines Profils verwendet werden.

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

Der Cisco AnyConnect Secure Mobility Client ist nicht auf seine Unterstützung als VPN-Client beschränkt, sondern bietet eine Reihe weiterer Optionen, die als Module integriert werden können. Die folgenden Module werden für AnyConnect unterstützt:

- **Start Before Login (SBL) (Vor Anmeldung starten):** Mit diesem Modul kann der Benutzer eine VPN-Verbindung im Unternehmen herstellen, bevor er sich bei Windows anmeldet.
- **Diagnostic and Reporting Tool (DART):** Dieses Modul wird verwendet, um Diagnosen durchzuführen und Berichte über die Installation und Verbindung von AnyConnect zu erstellen. DART wird durch das Zusammenstellen der Protokolle, des Status und der Diagnoseinformationen für die Analyse verwendet.
- **Advanced Malware Protection (AMP):** Dieses Modul ist eine Cloud-basierte Lösung der nächsten Generation, die verschiedene Bedrohungen erkennt, verhindert und darauf reagiert.
- **ISE-Status:** Die Cisco Identity Services Engine (ISE) bietet eine Identitäts- und Zugriffskontrollrichtlinie der nächsten Generation. Dieses Modul ermöglicht die Identifizierung des Betriebssystems (BS), des AntiVirus, des AntiSpyware usw., die derzeit auf einem Host installiert sind. Diese Informationen werden dann zusammen mit einer Richtlinie verwendet, um zu bestimmen, ob der Host eine Verbindung zum Netzwerk herstellen kann.
- **Network Visibility-Modul:** Das Netzwerktransparenzmodul überwacht die Nutzung von Endgeräte-Anwendungen, um potenzielle Verhaltensanomalien zu erkennen und fundiertere Entscheidungen bezüglich des Netzwerkdesigns zu treffen.
- **Umbrella:** Cisco Umbrella Roaming ist ein über die Cloud bereitgestellter Sicherheitsservice, der Geräte schützt, die sich außerhalb des Unternehmensnetzwerks befinden.
- **Web-Sicherheit:** Die von Cisco Talos unterstützte Cisco Web Security Appliance (WSA) schützt das Endgerät, indem sie riskante Websites automatisch blockiert und unbekannte Websites testet.
- **Network Access Manager:** Network Access Manager stellt ein sicheres Layer-2-Netzwerk gemäß den Richtlinien bereit. Es erkennt und wählt das optimale Layer-2-Zugangsnetzwerk aus und führt eine Geräteauthentifizierung für den Zugriff auf kabelgebundene und Wireless-Netzwerke durch.
- **Feedback:** Dieses Modul erfasst die Informationen und sendet sie regelmäßig an den Server. Sie unterstützt das Produktteam dabei, die Qualität, Zuverlässigkeit, Leistung und Benutzerfreundlichkeit von AnyConnect zu verbessern.

In FirePOWER 6.7 wird die Unterstützung für die FMC UI und die FTD Device REST API hinzugefügt, um die nahtlose Bereitstellung aller genannten AnyConnect-Module zu ermöglichen.



In dieser Tabelle sind die Profilerweiterungen und die zugeordneten Modultypen, die für die erfolgreiche Bereitstellung der Endpunktfunktionalität erforderlich sind.

Profilerweiterungen

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

Modultyp

- FEEDBACK
- AMP_ENABLER
- ISE-POSTEN
- NETZWERK_TRANSPARENZ
- NETWORK_ACCESS_MANAGER
- UMBRELLA
- WEB_SECURITY

Hinweis: DART- und SBL-Module benötigen kein Profil.

Hinweis: Für die Verwendung dieser Funktion ist keine zusätzliche Lizenzierung erforderlich.

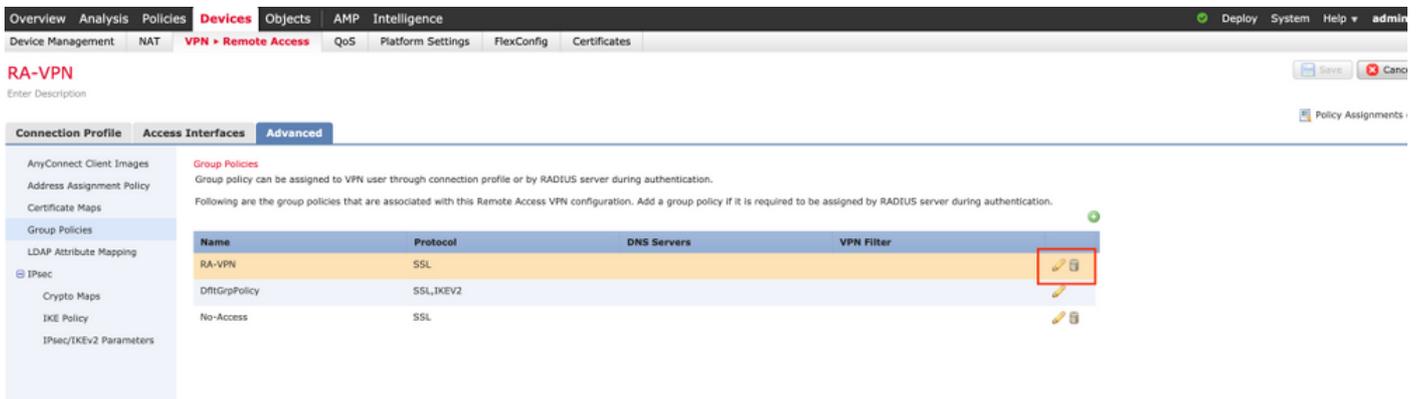
Konfiguration

Konfiguration auf FirePOWER Management Center (FMC)

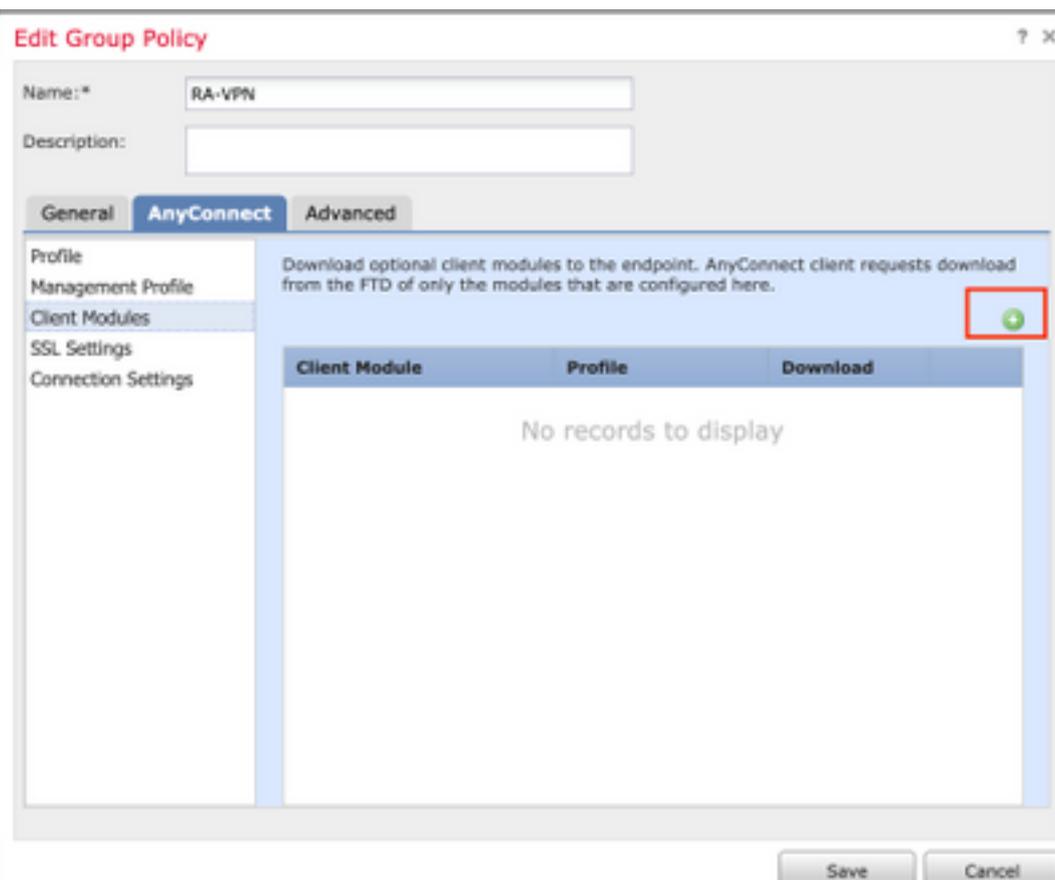
Schritt 1: Navigieren Sie zu **Gerät > VPN > Remote Access** und klicken Sie für die RA VPN-Konfiguration auf **Bearbeiten**.



Schritt 2: Navigieren Sie zu **Erweitert > Gruppenrichtlinien** und klicken Sie auf **Bearbeiten** für die betreffende Gruppenrichtlinie, wie in diesem Bild gezeigt.



Schritt 3: Navigieren Sie zu **AnyConnect > Client Modules**, und klicken Sie auf **+**, um die Module hinzuzufügen, wie in diesem Bild gezeigt.



Zur Demonstration werden die Module AMP, DART und SBL bereitgestellt.

Schritt 4: Wählen Sie das **DART-Modul** aus und klicken Sie auf **Hinzufügen**, wie in diesem Bild gezeigt.

Add Client Module ? X

Client Module: DART

Profile to download: [Empty]

Enable module download:

Add Cancel

Schritt 5: Klicken Sie auf +, um ein weiteres Modul hinzuzufügen, und wählen Sie **Start Before Login** module aus, wie in diesem Bild gezeigt.

Add Client Module ? X

Client Module: Start Before Login

Profile to download: [Empty]

Enable module download:

Add Cancel

Hinweis: In diesem Schritt können Sie das SBL-Modul herunterladen. SBL muss auch in jedem Connect-Clientprofil aktiviert werden, das hochgeladen wird, wenn Sie unter Gruppenrichtlinie zu **AnyConnect> Profile** navigieren.

Schritt 6: Klicken Sie auf +, um ein weiteres Modul hinzuzufügen, und wählen Sie **AMP Enabler** aus. Klicken Sie auf +, um ein Clientprofil hinzuzufügen, wie in diesem Bild gezeigt.

Add Client Module ? X

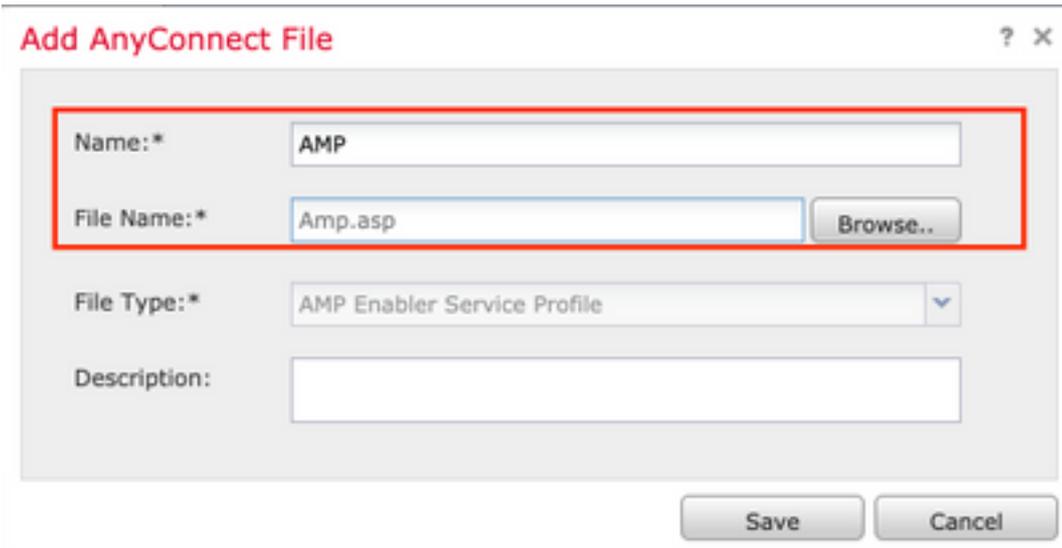
Client Module: AMP Enabler

Profile to download: [Empty] +

Enable module download:

Add Cancel

Geben Sie den **Namen** des Profils an, und laden Sie das **AMP-Profil hoch**. Klicken Sie auf **Speichern**, wie in diesem Bild gezeigt.



Add AnyConnect File ? X

Name:* AMP

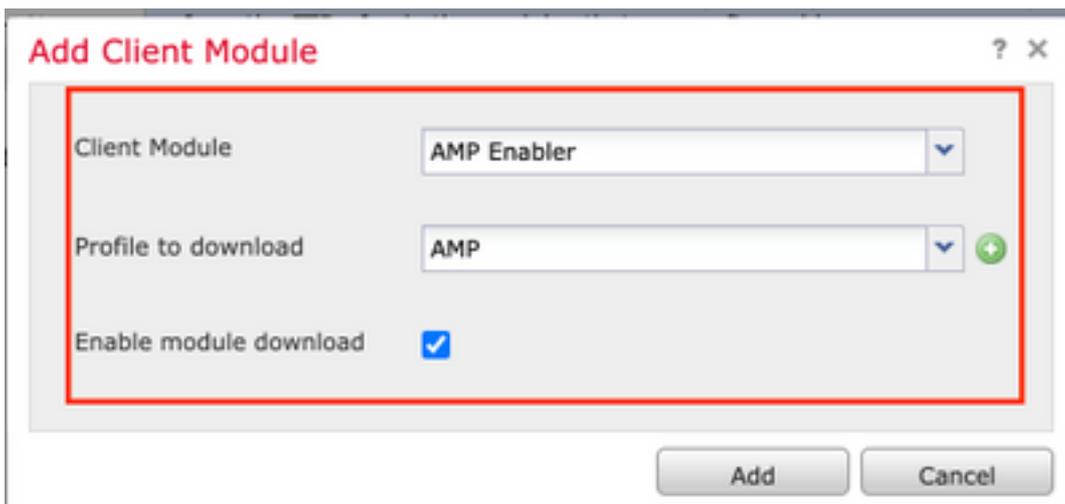
File Name:* Amp.asp Browse..

File Type:* AMP Enabler Service Profile

Description:

Save Cancel

Wählen Sie das Profil aus, das im vorherigen Schritt erstellt wurde, und klicken Sie auf das **Kontrollkästchen Enable Module download (Moduldownload aktivieren)**, wie in diesem Bild gezeigt.



Add Client Module ? X

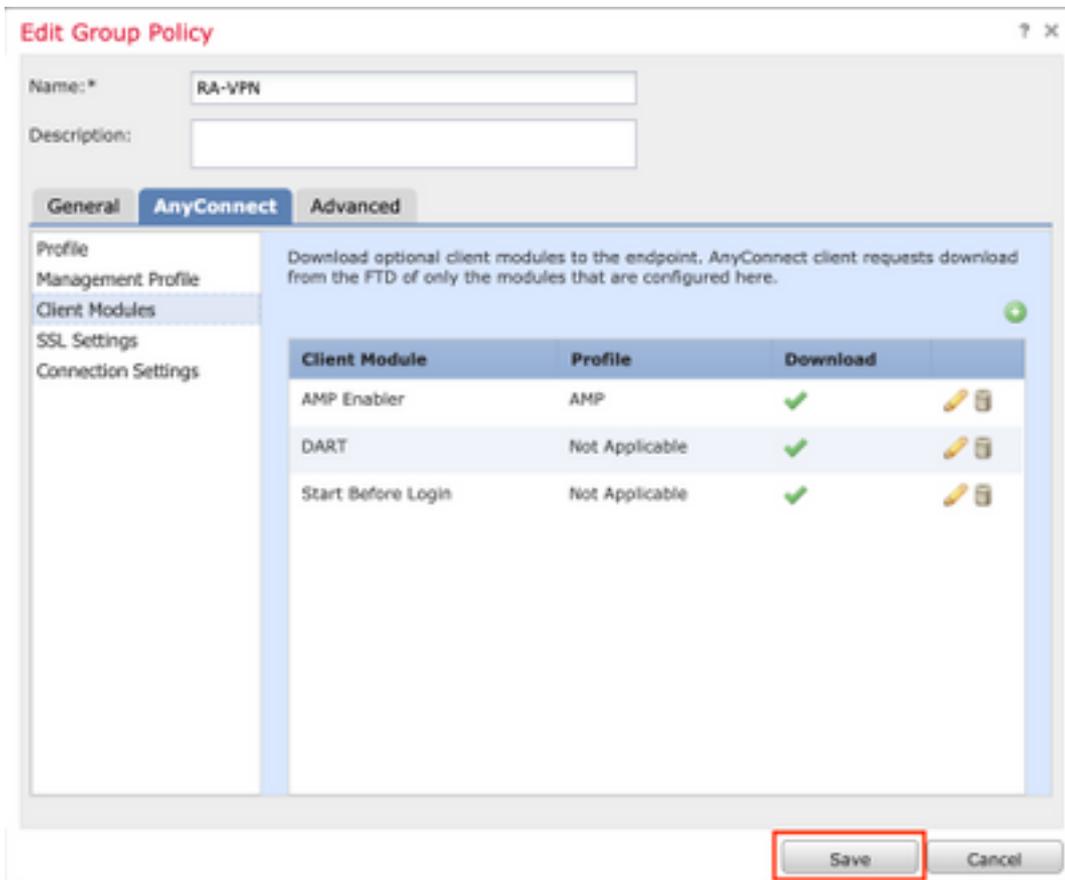
Client Module AMP Enabler

Profile to download AMP

Enable module download

Add Cancel

Schritt 7: Klicken Sie auf **Speichern**, sobald alle gewünschten Module hinzugefügt wurden.



Schritt 8: Navigieren Sie zu **Deploy > Deployment** und stellen Sie die Konfiguration im FTD bereit.



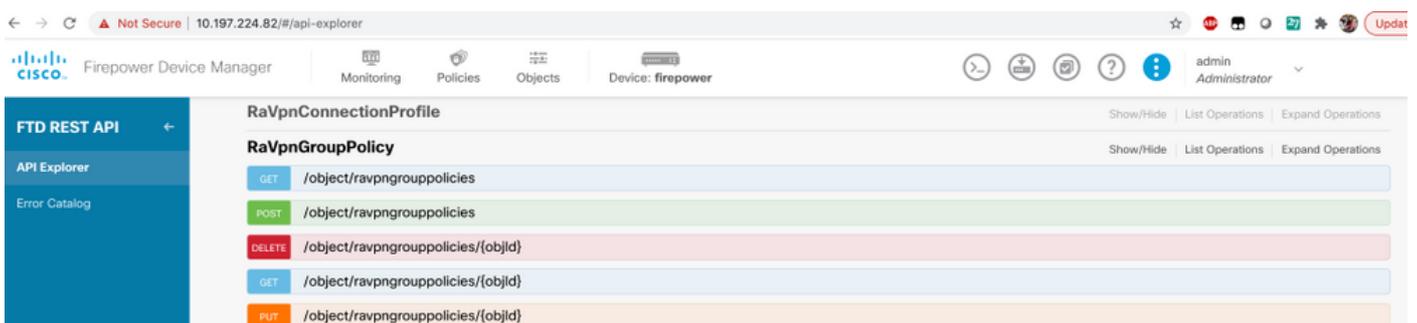
Konfiguration im FirePOWER Device Manager (FDM)

Schritt 1: Starten Sie den API-Explorer des FTD in einem Browserfenster.

Navigieren Sie zu <https://<FTD Management IP>/api-explorer>

Diese enthält die gesamte API-Liste, die im FTD verfügbar ist. Sie wird basierend auf der Hauptfunktion durch mehrere GET/POST/PUT/DELETE-Anfragen aufgeteilt, die vom FDM unterstützt werden.

RaVpnGroupPolicy wird als API verwendet.



Schritt 2: Fügen Sie eine Postman-Auflistung für **AnyConnect-Module** hinzu. Geben Sie einen **Namen** für die Auflistung ein. Klicken Sie auf **Erstellen**.

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

Schritt 3: 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**.

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

Der Haupttext der POST-Anfrage muss folgende Angaben enthalten:

Typ raw - JSON (Antrag/Json)

Grant_Type Kennwort

Benutzername Admin-Benutzername, um sich bei FTD anzumelden

Kennwort Das Kennwort für das Administratorkonto

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

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

Die Registerkarte Authorization (Autorisierung) muss diese Informationen für alle nachfolgenden GET-/POST-Anforderungen enthalten:

Typ Träger-Token

Token Das Zugriffstoken, das durch Ausführen der Auth POST-Anforderung empfangen wurde.

GET-ANFRAGE: <https://<FTD Management IP>/api/fdm/latest/object/ravpngrouppolicies>

Get Group Policy Comments 0 Examples 0

GET

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

Der Haupttext der Antwort zeigt alle auf dem Gerät konfigurierten Gruppenrichtlinien. Die ID der Gruppenrichtlinie wird zum Aktualisieren der spezifischen Gruppenrichtlinie verwendet.

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": "lc2t2sspzb7y7",
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  }

```

Zur Demonstration werden die Module AMP, DART und SBL bereitgestellt.

Schritt 5: Erstellen Sie eine Anforderung zum Hochladen eines Profils. Dieser Schritt ist nur für

Module erforderlich, die ein Profil erfordern. Laden Sie den Abschnitt "Profil in filetoUpload" hoch. Klicken Sie auf **Speichern**.

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

Der Text der Anforderung muss die im Haupttext hinzugefügte Profildatei im Formdatenformat enthalten. Das Profil muss mit dem [AnyConnect Profile Editor für Windows](#) erstellt werden.

Der Schlüsseltyp sollte **FileForfiletoUpload** sein.

The image shows a screenshot of the Postman application. 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 is filled with "Upload Profile" and is highlighted with a red box. 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 "AnyConnect Module" collection is selected and highlighted with a red box. A "+ Create Folder" button is visible to the right.

At the bottom of the dialog, there are two buttons: "Cancel" and "Save to AnyConnect Module", with the latter highlighted by a red box.

Below the dialog, the Postman interface for a POST request is visible. The URL is "https://10.197.224.82/api/fdm/latest/action/uploaddiskfile". The "Body" tab is selected, and the "form-data" radio button is chosen. A table of key-value pairs is shown:

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

The "fileToUpload" key and its value ".Amp.asp X" are highlighted with a red box. Below the table, the "File" radio button is selected and highlighted with a red box.

Der Text der Antwort gibt eine ID/Dateiname an, die verwendet wird, um auf das Profil mit dem betreffenden Modul zu verweisen.



The screenshot shows a REST client interface with the following elements:

- Top bar: Body, Cookies, Headers (17), Test Results, Status: 200 OK, Time: 325 ms, Size: 911 B, Save Response
- View options: Pretty, Raw, Preview, Visualize, JSON (selected)
- JSON response body:

```
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 }
```

Schritt 6: Erstellen Sie eine Anfrage zur Aktualisierung des **AnyConnect-Profiles**. Dieser Schritt ist nur für Module erforderlich, die ein Profil erfordern. Klicken Sie auf **Speichern**, wie in diesem Bild gezeigt.

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-ANFRAGE: <https://<FDM IP>/api/fdm/latest/object/anyconnectclientprofile>

Der Text der Anfrage enthält folgende Informationen:

Name

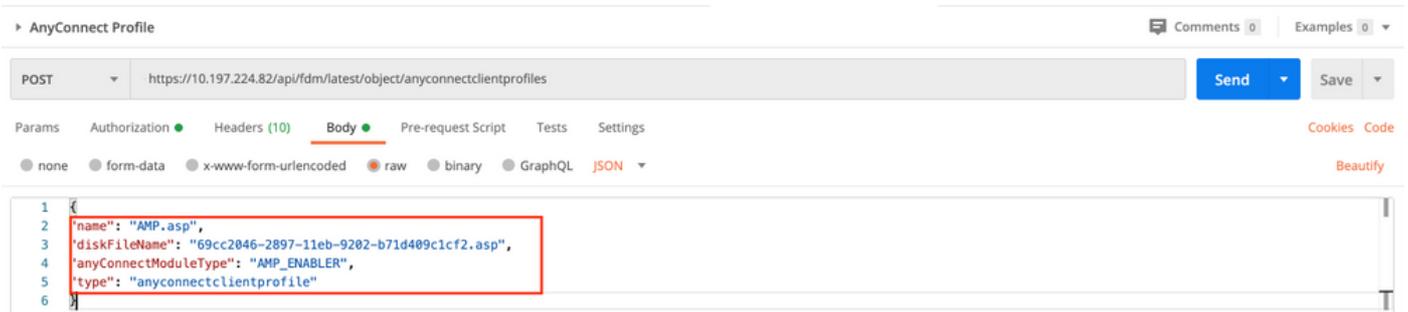
Logischer Name, den Sie die Datei aufrufen möchten

diskFileName

Muss dem fileName entsprechen, der in der Upload Profile POST-Antwort

empfangen wird.

AnyConnectModuleType Übereinstimmung mit dem entsprechenden Modul in der [Module](#) Type Table
Typ anyconnectClientProfil



Der Text der Antwort zeigt das Profil an, das auf das Gerät übertragen werden kann. Name, Version, ID und Typ, die als Antwort empfangen werden, werden im nächsten Schritt verwendet, um das Profil an Gruppenrichtlinie zu binden.



Schritt 6: Erstellen Sie eine **PUT**-Anforderung, um **Clientprofil** und **-modul** der vorhandenen **Gruppenrichtlinie** hinzuzufügen. Klicken Sie auf **Speichern**, wie in diesem Bild gezeigt.

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-ANFRAGE: <https://<FDM IP>/api/fdm/latest/object/ravpngrouppolicies/{objId}>

ObjId ist die in [Schritt 4](#) erhaltene ID. Kopieren Sie den Inhalt der in Schritt 4 erhaltenen Gruppenrichtlinie in den Text der Anfrage und fügen Sie Folgendes hinzu:

Clientprofil

Name, Version, ID und Typ des im vorherigen Schritt erhaltenen Profils.

Client-Module

Der Name des Moduls, das aktiviert werden muss, sollte genau der in der [Modultabelle](#) angegebenen entsprechen.

Client Profile and Module Comments 0 | Exi

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 Comments 0 | Examples 0

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 Cookies Cod

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

```
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 }
```

Der Haupttext der Antwort zeigt das Profil und das Modul an, das erfolgreich an Gruppenrichtlinien gebunden ist.

```

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.

```

Hinweis: Dieser Schritt ermöglicht das Herunterladen des SBL-Moduls. SBL muss auch in jedem Connect-Clientprofil aktiviert werden, das hochgeladen werden kann, wenn Sie zu **Devices > Remote Access VPN>Group Policies> Edit Group Policy > General > AnyConnect Client Profile** navigieren.

Schritt 7: Bereitstellung der Konfiguration auf dem Gerät über FDM Ausstehende Änderungen zeigen an, dass Clientprofil und -module gepilt werden müssen.

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
<p>AnyConnect Group Edited: RA-VPN</p> <ul style="list-style-type: none"> — — — clientProfiles: — 	<ul style="list-style-type: none"> enabledAnyConnectModules[0]: DART enabledAnyConnectModules[1]: AMP_ENABLER enabledAnyConnectModules[2]: START_BEFORE_LOGIN AMP.asp
<p>+ AnyConnect Client Profile Added: AMP.asp</p> <ul style="list-style-type: none"> — — — — 	<ul style="list-style-type: none"> anyConnectModuleType: AMP_ENABLER md5Checksum: 8697131026bdbaf6a67e1191e8abe122 diskFileName: 69cc2046-2897-11eb-9202-b71d409c1cf2 ... name: AMP.asp

MORE ACTIONS ▾
CANCEL
DEPLOY NOW ▾

Konfiguration nach erfolgreicher Bereitstellung in die FTD-CLI übertragen:

!--- 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
```

Überprüfen

Stellen Sie eine erfolgreiche Verbindung zur FTD her.

Navigieren Sie zu **Einstellungen > VPN** Nachrichtenverlauf, um die Details der heruntergeladenen Module anzuzeigen.

The screenshot shows the Cisco AnyConnect Secure Mobility Client window. The left sidebar contains navigation options: Status Overview, VPN (selected), Network, Web Security, System Scan, and Roaming Security. The main content area is titled 'Virtual Private Network (VPN)' and has tabs for Preferences, Statistics, Route Details, Firewall, and Message History. The Message History log shows the following entries:

- 15-11-2020
- 21:49:41 Contacting 10.197.224.90.
- 21:49:52 User credentials entered.
- 21:49:52 Please respond to banner.
- 21:49:54 User accepted banner.
- 21:49:54 Establishing VPN session...
- 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%
- 21:50:00 Checking for customization updates...
- 21:50:00 Performing any required updates...
- 21:50:11 The AnyConnect Downloader updates have been completed.
- 21:50:16 Establishing VPN session...

Fehlerbehebung

[Ermitteln Sie](#) DART zur Fehlerbehebung bei Problemen mit der Installation von Clientmodulen.