

# FMC を使用した Firepower Threat Defense 向けの高度な AnyConnect VPN の展開

初版：2020 年 4 月 7 日

最終更新：2020 年 4 月 28 日

## FMC を使用した Firepower Threat Defense に向けた、高度な AnyConnect VPN の展開

このドキュメントでは、ダイナミック スプリット トンネリングや LDAP 属性マップなど、FlexConfig を使用して Cisco FMC に Cisco FTD 用の高度な AnyConnect VPN を展開する方法を示します。

### ダイナミック スプリット トンネリング

次のトピックでは、Cisco Firepower Threat Defense (FTD) のダイナミック スプリット トンネリングと、Cisco Firepower Management Center (FMC) 6.4 で FlexConfig を使用して設定する方法について説明します。この構成は、ダイナミック スプリット トンネリングを直接サポートしない後続のリリースに適用できます。

### ダイナミック スプリット トンネリングについて

スタティック スプリット トンネリングでは、リモートアクセス VPN トンネルに含めるか、またはリモートアクセス VPN トンネルから除外する必要があるホストおよびネットワークの IP アドレスの定義を伴います。ダイナミック スプリット トンネリングを定義することで、スプリット トンネリングを強化できます。

ダイナミック スプリット トンネリングにより、DNS ドメイン名に基づいてスプリット トンネリングを微調整できます。完全修飾ドメイン名 (FQDN) に関連付けられた IP アドレスは、変化するか、または単純に地域によって異なることがあるため、DNS 名に基づいてスプリット トンネリングを定義することで、リモートアクセス VPN トンネルに含める必要のあるトラフィックと含める必要のないトラフィックをよりダイナミックに定義できます。除外されたドメイン名に対して返されたアドレスが VPN に含まれるアドレスプール内にある場合、これらのアドレスは除外されます。

除外されたドメインはブロックされません。代わりに、これらのドメインへのトラフィックは VPN トンネルの外部に保持されます。たとえば、パブリックインターネット上の Cisco WebEx にトラフィックを送信することで、保護されたネットワーク内のサーバーへのトラフィック用に VPN トンネル内の帯域幅を解放できます。

バージョン 7.0 以降では、FMC UI を使用してこの機能を設定できます。詳細については、「[Configure AnyConnect Dynamic Split Tunnel on FTD Managed by FMC](#)」を参照してください。古いバージョンの FMC の場合は、[FlexConfig を使用したダイナミック スプリット トンネリングの設定 \(2 ページ\)](#) の指示に従って FlexConfig を使用してこの機能を設定する必要があります。

## FlexConfig を使用したダイナミック スプリット トンネリングの設定

ダイナミック スプリット トンネル構成は、**dynamic-split-exclude-domains** タイプのカスタム AnyConnect 属性を作成してから、その属性を RA VPN 接続プロファイルで使用されるグループポリシーに追加することに基づいています。

また、**dynamic-split-include-domains** カスタム属性を作成して、IP アドレスに基づいて除外されるトンネルに含めるドメインを定義することもできます。ただし、この例ではドメインの除外について説明します。

### 始める前に

この構成には、最低限 AnyConnect 4.5 が必要です。

この例では、リモートアクセス VPN がすでに設定されており、正しく機能していることを前提としています。これには、ダイナミック スプリット トンネリングの属性を追加するグループポリシーの作成が含まれます。グループポリシーの作成には FlexConfig を使用しないでください。既存のグループポリシーの編集にのみ使用します。

ダイナミックブロックリストを定義する際に、スタティック IP アドレスベースのスプリット トンネリングを設定する必要はありません。ただし、ダイナミック許可リストを作成する場合は、スプリット トンネリングを有効にし、一部の IP アドレスを除外する必要があります。ドメインを含めるダイナミック スプリット トンネリングは、IP アドレスベースのスプリット トンネリングの状況で除外されるトラフィックを含める場合にのみ意味があります。

### 手順

**ステップ 1** ダイナミック スプリット トンネリングのカスタム属性を作成し、VPN トンネルから除外して代わりにパブリックインターネット経由で送信する必要があるドメイン名を割り当てる、`deploy-once/append FlexConfig` オブジェクトを作成します。

- [**オブジェクト (Objects)**] > [**オブジェクト管理 (Object Management)**] を選択します。
- 目次から [**FlexConfig**] > [**FlexConfig オブジェクト (FlexConfig Object)**] を選択します。
- [**FlexConfig オブジェクトの追加 (Add FlexConfig Object)**] をクリックし、次のプロパティを設定して、[**保存 (Save)**] をクリックします。

- [**名前 (Name)**]: オブジェクト名。たとえば、`Enable_Dynamic_Split_Tunnel` などです。
- [**展開 (Deployment)**]: [**1回 (Once)**] を選択します。これらのコマンドは一度に設定する必要があります。
- [**タイプ (Type)**]: デフォルトの [**後に付加 (Append)**] を維持します。コマンドは、直接サポートされている機能のコマンドの後にデバイスに送信されます。

- **[オブジェクト本体 (Object body)]** : オブジェクト本体で、**dynamic-split-exclude-domains** タイプの属性を作成するために必要なコマンドを入力してから、属性名と除外するドメイン名のリストであるデータを追加します。たとえば、**excludeddomains** という名前の属性を作成し、**webex.com** ドメインと **ciscospark.com** ドメインを除外するには、コマンドは次のようになります。説明は省略できますが、説明が含まれている場合は個別のコマンドではなく、**anyconnect-custom-attr** コマンドの一部であることに注意してください。ドメイン名はカンマで区切りますが、スペースは含めないでください。

```
webvpn
anyconnect-custom-attr dynamic-split-exclude-domains description traffic for
these domains will not be sent to the VPN headend
anyconnect-custom-data dynamic-split-exclude-domains excludeddomains
webex.com,ciscospark.com
```

オブジェクトは、次のようになります。

- ステップ 2** (推奨) カスタムグループポリシーを使用する場合は、**deploy-once/append** FlexConfig オブジェクトを作成して、グループポリシーでダイナミック スプリット トンネルのカスタム属性を設定します。

システムは、カスタムグループポリシーに加えた変更を無効にしません。そのため、変更を 1 回展開する必要があります。複数のグループポリシーを使用する場合は、単一の FlexConfig オブジェクトを使用してカスタム属性を各ポリシーに順番に追加できます。あるいは、グループポリシーごとに 1 つの FlexConfig オブジェクトを作成できます。結果は同じになるため、FlexConfig ポリシーをモジュール化するための独自の要件に基づいて選択します。

[FlexConfigオブジェクト (FlexConfig Objects)] ページで、[FlexConfigオブジェクトの追加 (Add FlexConfig Object)] をクリックし、次のプロパティを設定して、[保存 (Save)] をクリックします。

- [名前 (Name)] : オブジェクト名。たとえば、Add\_Dynamic\_Split\_Tunnel\_Sales です。
- [展開 (Deployment)] : [1回 (Once)] を選択します。
- [タイプ (Type)] : デフォルトの [後に付加 (Append)] を維持します。
- [オブジェクト本体 (Object body)] : オブジェクト本体で、グループポリシーにカスタム属性を追加するために必要なコマンドを入力します。たとえば、作成した属性の名前が excludeddomains で、グループポリシーの名前が「sales」の場合、コマンドは次のとおりです。

```
group-policy sales attributes
  anyconnect-custom dynamic-split-exclude-domains value excludeddomains
```

オブジェクトは、次のようになります。

The screenshot shows the configuration page for a FlexConfig object. The 'Name' field is filled with 'Add\_Dynamic\_Split\_Tunnel\_Sales'. The 'Description' field is empty. A yellow warning banner states: 'Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.' Below this, the 'Deployment' dropdown is set to 'Once' and the 'Type' dropdown is set to 'Append'. The main text area contains the following CLI commands:

```
group-policy sales attributes
  anyconnect-custom dynamic-split-exclude-domains value excludeddomains
```

At the bottom, there is a 'Variables' table with the following columns: Name, Dimension, Default Value, Property (Typ..., Override, and Description. The table is currently empty, displaying 'No records to display'.

**ステップ 3** (Not recommended.) DfltGrpPolicy という名前のデフォルトグループポリシーを使用する場合は、deploy-everytime/append FlexConfig オブジェクトを作成して、グループポリシーにダイナミック スプリット トンネルのカスタム属性を設定します。

このオブジェクトは毎回展開する必要があります。これは、展開のたびに、システムがデフォルトポリシーに対するカスタム変更を無効にするためです。

DfltGroupPolicy を使用するのではなく、カスタムグループポリシーを作成することを推奨します。

[FlexConfigオブジェクト (FlexConfig Objects) ] ページで、[FlexConfigオブジェクトの追加 (Add FlexConfig Object) ] をクリックし、次のプロパティを設定して、[保存 (Save) ] をクリックします。

- [名前 (Name) ] : オブジェクト名。たとえば、Add\_Dynamic\_Split\_Tunnel\_DfltGrpPolicy です。
- [展開 (Deployment) ] : [毎回 (Everytime) ] を選択します。これらのコマンドは一度に設定する必要があります。
- [タイプ (Type) ] : デフォルトの [後に付加 (Append) ] を維持します。このコマンドは、システムがデフォルトのグループポリシーのカスタム属性を無効にした後に送信する必要があります。
- [オブジェクト本体 (Object body) ] : オブジェクト本体で、グループポリシーにカスタム属性を追加するために必要なコマンドを入力します。たとえば、作成した属性の名前が `excludeddomains` の場合、コマンドは次のとおりです。

```
group-policy DfltGrpPolicy attributes
  anyconnect-custom dynamic-split-exclude-domains value excludeddomains
```

オブジェクトは、次のようになります。

The screenshot shows the configuration page for a FlexConfig object. The 'Name' field contains 'Add\_Dynamic\_Split\_Tunnel\_DfltGrpPolicy'. The 'Description' field is empty. A yellow warning banner states: 'Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.' Below this, there is a toolbar with an 'Insert' button and a 'Deployment' dropdown set to 'Everytime' and a 'Type' dropdown set to 'Append'. The main text area contains the CLI commands: `group-policy DfltGrpPolicy attributes` and `anyconnect-custom dynamic-split-exclude-domains value excludeddomains`. At the bottom, there is a 'Variables' section with a table header: 'Name', 'Dimension', 'Default Value', 'Property (Typ...', 'Override', and 'Description'. The table is currently empty, displaying 'No records to display'.

**ステップ 4** これらのオブジェクトを展開する FlexConfig ポリシーを作成します。

- a) [デバイス (Devices)] > [FlexConfig] を選択します。
- b) [新しいポリシー (New Policy)] をクリックするか、既存の FlexConfig ポリシーをターゲットデバイスに割り当て (または割り当て済み)、このポリシーを編集するだけです。

新しいポリシーを作成する場合、ポリシーに名前を付けるダイアログボックスでターゲットデバイスをポリシーに割り当てます。

- c) Ctrl を押しながらかlickして、目次の [ユーザー定義 (User Defined)] フォルダ内にある [FlexConfig オブジェクト (FlexConfig Object)] を選択し、[>] をクリックしてポリシーに追加します。

オブジェクトが [選択済み追加 FlexConfig (Selected Append FlexConfigs)] リストに追加されます。

- d) ドラッグアンドドロップを使用して、オブジェクトが正しい順序であることを確認します。

カスタム属性オブジェクトを作成するオブジェクトは、その属性をグループポリシーに割り当てるオブジェクトの前に配置する必要があります。そうしない場合は、まだ存在しないカスタム属性を追加しようとすると、エラーが発生します。

カスタムグループポリシーを設定する単一のオブジェクトがある場合、リストは次のようになります。

| Selected Append FlexConfigs |                                |
|-----------------------------|--------------------------------|
| #.                          | Name                           |
| 1.                          | Enable_Dynamic_Split_Tunnel    |
| 2.                          | Add_Dynamic_Split_Tunnel_Sales |

- e) [保存 (Save)] をクリックします。
- f) すべてのターゲットデバイスがポリシーにまだ割り当てられていない場合は、[保存 (Save)] の下にある [ポリシー割り当て (Policy Assignment)] リンクをクリックし、ここで割り当てを行います。
- g) [設定のプレビュー (Preview Config)] をクリックし、[プレビュー (Preview)] ダイアログボックスで割り当てられているデバイスのいずれかを選択します。

システムでは、デバイスに送信される設定 CLI のプレビューが生成されます。オブジェクトから生成されたコマンドが正しいことを確認します。これらはプレビューの最後に表示されます。また、管理対象機能に加えた他の変更から生成されたコマンドも表示されることに注意してください。ダイナミック スプリット トンネル コマンドでは、次のような内容が表示されます。

```
###Flex-config Appended CLI ###
webvpn
  anyconnect-custom-attr dynamic-split-exclude-domains description traffic for these
  domains will not be sent to the VPN headend
  anyconnect-custom-data dynamic-split-exclude-domains excludeddomains
  webex.com,ciscopark.com
  group-policy sales attributes
  anyconnect-custom dynamic-split-exclude-domains value excludeddomains
```

ステップ5 変更を展開します。

ステップ6 設定を確認します。

- 各FTDデバイスでコマンドが設定されていることを確認できます。デバイスへのSSHセッション、またはFMCのCLIツールを使用します ([システム (System)] > [正常性 (Health)] > [モニター (Monitor)] で、デバイスをクリックしてから、[高度なトラブルシューティング (Advanced Troubleshooting)] をクリックし、[脅威に対する防御CLI (Threat Defense CLI)] タブを選択します)。次に、構成を表示するコマンドを示します。
  - `show running-config webvpn`
  - `show running-config anyconnect-custom-data`
  - `show running-config group-policy name`、ここで、`name` を sales などのグループポリシー名に置き換えます。
- AnyConnect クライアントからシステムが正しく動作していることを確認できます。クライアント統計情報を開くと、[ダイナミックトンネル除外 (Dynamic Tunnel Exclusions)] フィールドに、除外するドメイン名のリストが表示されます。

## FlexConfig を使用したダイナミック スプリット トンネリングの削除

スプリットトンネリングを使用しない場合は、FlexConfig オブジェクトを作成して、機能を展開したデバイスから構成を削除する必要があります。FlexConfig ポリシーから FlexConfig オブジェクトを削除するだけでは不十分です。

### 手順

ステップ1 使用する各グループポリシーからカスタム属性を削除する `deploy-once/append FlexConfig` オブジェクトを作成してから、属性を削除します。

削除する前に、まずカスタムポリシーから属性を削除する必要があります。現在使用されている属性を削除しようとする、システムによって阻止され、展開エラーが表示されます。したがって、このオブジェクトが正しく動作するには、コマンドを正しい順序で挿入する必要があります。

- a) [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- b) 目次から [FlexConfig] > [FlexConfig オブジェクト (FlexConfig Object)] を選択します。
- c) [FlexConfig オブジェクトの追加 (Add FlexConfig Object)] をクリックし、次のプロパティを設定して、[保存 (Save)] をクリックします。
  - [名前 (Name)] : オブジェクト名。たとえば、Disable\_Dynamic\_Split\_Tunnel です。
  - [展開 (Deployment)] : [1回 (Once)] を選択します。これらのコマンドは一度に設定する必要があります。

## FlexConfig を使用したダイナミック スプリット トンネリングの削除

- [タイプ (Type) ]: デフォルトの [後に付加 (Append) ] を維持します。コマンドは、直接サポートされている機能のコマンドの後にデバイスに送信されます。
- [オブジェクト本体 (Object body) ]: オブジェクト本体で、それを使用する各グループポリシーからカスタム属性を削除するために必要なコマンドを入力し、カスタム属性を削除します。たとえば、セールスグループポリシーでカスタム属性が使用され、その属性の名前が `excludeddomains` の場合、コマンドは次のようになります。

```
group-policy sales attributes
no anyconnect-custom dynamic-split-exclude-domains

no anyconnect-custom-data dynamic-split-exclude-domains excludeddomains

webvpn
no anyconnect-custom-attr dynamic-split-exclude-domains
```

オブジェクトは、次のようになります。

- ステップ 2** FlexConfig ポリシーを編集して、ダイナミック スプリット トンネリング オブジェクトを削除し、構成を削除するオブジェクトを追加します。
- a) [デバイス (Devices) ] > [FlexConfig] を選択します。
  - b) FlexConfig ポリシーを編集します。
  - c) [選択済み追加FlexConfig (Selected Appended FlexConfigs) ] リストで、各ダイナミック スプリット トンネル オブジェクトの削除アイコンをクリックします。これにより、カスタム属性が有効になり、グループポリシーに属性が追加されます。



- d) 目次の [ユーザー定義 (User Defined)] フォルダ内でダイナミック スプリット トンネリングを無効にする [FlexConfig オブジェクト (FlexConfig Object)] を選択し、[>] をクリックしてポリシーに追加します。

オブジェクトが [選択済み追加 FlexConfig (Selected Append FlexConfigs)] リストに追加されます。

リストは次のようになります。

| Selected Append FlexConfigs |                              |
|-----------------------------|------------------------------|
| #.                          | Name                         |
| 1.                          | Disable_Dynamic_Split_Tunnel |

- e) [保存 (Save)] をクリックします。  
 f) [設定のプレビュー (Preview Config)] をクリックし、[プレビュー (Preview)] ダイアログボックスで割り当てられているデバイスのいずれかを選択します。

システムでは、デバイスに送信される設定 CLI のプレビューが生成されます。オブジェクトから生成されたコマンドが正しいことを確認します。これらはプレビューの最後に表示されます。また、管理対象機能に加えた他の変更から生成されたコマンドも表示されることに注意してください。ダイナミック スプリット トンネル コマンドでは、次のような内容が表示されます。

```
###Flex-config Appended CLI ###
group-policy sales attributes
  no anyconnect-custom dynamic-split-exclude-domains

no anyconnect-custom-data dynamic-split-exclude-domains excludeddomains

webvpn
  no anyconnect-custom-attr dynamic-split-exclude-domains
```

**ステップ 3** 変更を展開します。

## AnyConnect 構成用の LDAP 属性マップ

リモートアクセス VPN ユーザーの認証に Active Directory (AD) /LDAP を使用する場合は、LDAP 属性マップを使用して、AD/LDAP サーバーから返される属性に基づいて AnyConnect の構成と動作を調整できます。

### LDAP 属性マップについて

LDAP 属性マップにより、Active Directory (AD) または LDAP サーバーに存在する属性が、シスコの属性名と同一視されるようになります。その後、リモートアクセス VPN 接続の確立中に AD または LDAP サーバーが FTD デバイスに認証を返すと、FTD デバイスは、その情報を使用して、AnyConnect クライアントが接続を完了する方法を調整できます。

たとえば、AD/LDAP **memberOf** 属性を Cisco **Group-Policy** 属性にマッピングできます。次に、AD/LDAP から取得する値を、VPN に対して定義した RA VPN グループポリシーの名前と一致させます。FTD デバイスがユーザーの **Group-Policy** 属性を検出すると、AnyConnect はそのグループポリシー名を使用して RA VPN 接続を確立しようとします。

LDAP 属性マップを作成した後、AD/LDAP サーバー構成に付加します。したがって、AD/LDAP サーバーごとに異なるマップを作成できます。マップは RA VPN 接続プロファイルまたはグループポリシーに直接関連付けられません。

LDAP 承認でサポートされる Cisco 属性のリストは、ASA 8.4/8.6 のコンフィギュレーションガイドに記載されています。[https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa\\_84\\_cli\\_config/ref\\_extserver.html#pgfId-1773708](https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/ref_extserver.html#pgfId-1773708)

バージョン 6.7 以降では、FMC UI を使用してこの機能を設定できます。詳細については、「[Configure RA VPN with LDAP Authentication and Authorization for FTD](#)」を参照してください。古いバージョンの FMC の場合は、[LDAP 属性マップによるグループポリシーの使用の制御 \(10 ページ\)](#) の指示に従って FlexConfig を使用してこの機能を設定する必要があります。

## LDAP 属性マップによるグループポリシーの使用の制御

LDAP 属性マップの一般的な用途は、ユーザーの AD/LDAP グループメンバーシップに基づいてユーザーに割り当てられるグループポリシーを制御することです。これを行うには、**memberOf** AD/LDAP 属性の値を Cisco **Group-Policy** 属性の値にマッピングします。

概要として、LDAP マップを使用するには、次の手順を実行する必要があります。

1. **ldap attribute-map name** コマンドを使用してマップを作成します。ここでの *name* は属性の名前ではなく、マップの名前です。
2. **map-name ldap\_attribute\_name Cisco\_attribute\_name** コマンドを使用して、AD/LDAP 属性を Cisco 属性に名前でもマッピングします。
3. **map-value ldap\_attribute\_name ldap\_value Cisco\_value** コマンドを使用して、AD/LDAP 属性に表示されると予想される値を Cisco 属性の関連する値にマッピングします。
4. **ldap-attribute-map name** コマンドを使用して、LDAP 属性マップを 1 つ以上の AD/LDAP サーバーに付加します。AD/LDAP サーバーにマップを追加するコマンドと、マップ自体を作成するコマンドの微妙な相違点に注意してください。唯一の違いとして、コマンド全体はハイフンで連結されていますが、マップを作成する基本コマンドは単に **ldap** です。  
**aaa-server name host server\_address** コマンドを使用して正しいモードを開始し、マップを付加する必要があることに注意してください。

次の手順では、エンドツーエンドのプロセスについて説明します。

### 始める前に

この手順は、すべての AnyConnect バージョンで機能します。

この例では、リモートアクセス VPN がすでに設定されており、正しく機能していることを前提としています。VPN は認証サーバーとして AD/LDAP を使用する必要があります、これを設定す

する必要があります。また、すべてのグループポリシーを設定する必要がありますが、FlexConfig では設定しないでください。

目的は、次の RA VPN グループポリシーにユーザーをマッピングすることです。

- APP-SSL-VPN Managers (AD/LDAP) ユーザーは、LabAdminAccessGroupPolicy という名前のグループポリシーを使用する必要があります。
- Engineering (AD/LDAP) ユーザーは、VPNAccessGroupPolicy という名前のグループポリシーを使用する必要があります。

## 手順

**ステップ 1** 属性と値のマッピングを含む LDAP マップを作成する deploy-once/append FlexConfig オブジェクトを作成します。このオブジェクトはマップのみを作成し、マップを AD/LDAP サーバーに割り当てません。

- a) [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- b) 目次から [FlexConfig] > [FlexConfig オブジェクト (FlexConfig Object)] を選択します。
- c) [FlexConfig オブジェクトの追加 (Add FlexConfig Object)] をクリックし、次のプロパティを設定して、[保存 (Save)] をクリックします。
  - [名前 (Name)] : オブジェクト名。たとえば、Create\_LDAP\_Map\_for\_VPN\_Access です。
  - [展開 (Deployment)] : [1回 (Once)] を選択します。これらのコマンドは一度に設定する必要があります。
  - [タイプ (Type)] : デフォルトの [後に付加 (Append)] を維持します。コマンドは、直接サポートされている機能のコマンドの後にデバイスに送信されます。
  - [オブジェクト本体 (Object body)] : オブジェクト本体で、LDAP マップの作成に必要なコマンドを入力し、AD/LDAP 属性を Cisco 属性にマッピングしてから、その属性の値 (AD/LDAP から返される) を Cisco 属性にとって意味のある値にマッピングします。

次の例で、

- **LDAP\_Map\_for\_VPN\_Access** は、LDAP 属性マップの名前です。これには任意の名前を指定できます。
- **memberOf** は、サーバー自体で定義されている AD/LDAP 属性の名前です。これはランダムな文字列ではありません。
- **Group-Policy** は Cisco 属性の名前であり、ランダムな文字列でもありません。
- **CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=example,DC=com** は、認証中に AD/LDAP によって **memberOf** 属性で返されることが予想される値です。この文字列は、AD/LDAP サーバーの設定方法に基づいています。この文字列は、

ユーザーが APP-SSL-VPN Managers ユーザーグループのメンバーであることを示します。

- **LabAdminAccessGroupPolicy** は、FMC で定義したグループポリシーの名前で、RA VPN 接続プロファイルで使用します。この文字列は、既存のグループポリシーの名前と一致する必要があります。
- **CN=Engineering,CN=Users,OU=stbu,DC=example,DC=com** は、**memberOf** 属性で返されることが予想される値です。この文字列は、ユーザーが Engineering ユーザーグループのメンバーであることを示します。
- **VPNAccessGroupPolicy** は、すでに存在し、RA VPN で使用されるグループポリシーの名前です。

この構成のコマンドは次のとおりです。

```
ldap attribute-map LDAP_Map_for_VPN_Access
map-name memberOf Group-Policy
map-value memberOf CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=example,DC=com
LabAdminAccessGroupPolicy
map-value memberOf CN=Engineering,CN=Users,OU=stbu,DC=example,DC=com
VPNAccessGroupPolicy
```

オブジェクトは、次のようになります。

Name:

Description:

⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Deployment: Once Type: Append

```
ldap attribute-map LDAP_Map_for_VPN_Access
map-name memberOf Group-Policy
map-value memberOf CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=example,DC=com
LabAdminAccessGroupPolicy
map-value memberOf CN=Engineering,CN=Users,OU=stbu,DC=example,DC=com VPNAccessGroupPolicy
```

| Name                  | Dimension | Default Value | Property (Typ... | Override | Description |
|-----------------------|-----------|---------------|------------------|----------|-------------|
| No records to display |           |               |                  |          |             |

**ステップ 2** マップを AD/LDAP サーバーに割り当てる deploy-everytime/append FlexConfig オブジェクトを作成します。

Firepower Management Center で AD/LDAP レルムを直接定義するため、レルムへの FlexConfig の変更は各展開時に削除されます。したがって、各展開ジョブの最後に再度設定する必要があります。

[FlexConfigオブジェクト (FlexConfig Objects) ] ページで、[FlexConfigオブジェクトの追加 (Add FlexConfig Object) ] をクリックし、次のプロパティを設定して、[保存 (Save) ] をクリックします。

- [名前 (Name) ] : オブジェクト名。たとえば、Attach\_LDAP\_Map\_for\_VPN\_Access です。
- [展開 (Deployment) ] : [毎回 (Everytime) ] を選択します。
- [タイプ (Type) ] : デフォルトの [後に付加 (Append) ] を維持します。
- [オブジェクト本体 (Object body) ] : オブジェクト本体で、RA VPN に使用される AD サーバーにマップを割り当てるために必要なコマンドを入力します。

次の例で、

- **LDAP\_Map\_for\_VPN\_Access** は、前の FlexConfig オブジェクトで作成した LDAP 属性マップの名前です。
- **ad\_realm** は、RA VPN で使用している AD/LDAP レルムの名前です。**10.100.10.10** は、レルム内のサーバーの IP アドレスです。この例では、サーバーが 1 台しかないことを前提としています。複数ある場合は、サーバーごとに **aaa-server** コマンドおよび後続の **ldap-attribute-map** コマンドを繰り返す必要があります。レルム名は任意のものを選択できますが、このコマンドでは、変更する RA VPN 接続で作成して使用したレルムの名前と正確に一致する必要があります。同様に、サーバーアドレスは、レルム内で実際に設定されているアドレスである必要があります。


この構成のコマンドは次のとおりです。

```
aaa-server ad-realm host 10.100.10.10
  ldap-attribute-map LDAP_Map_for_VPN_Access
exit
```

オブジェクトは、次のようになります。

Name:

Description:

 Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Deployment:  Type:

```

aaa-server ad-realm host 10.100.10.10
  ldap-attribute-map LDAP_Map_for_VPN_Access
exit

```

Variables

| Name                  | Dimension | Default Value | Property (Typ... | Override | Description |
|-----------------------|-----------|---------------|------------------|----------|-------------|
| No records to display |           |               |                  |          |             |

**ステップ 3** これらのオブジェクトを展開する FlexConfig ポリシーを作成します。

- [デバイス (Devices)] > [FlexConfig] を選択します。
- [新しいポリシー (New Policy)] をクリックするか、既存の FlexConfig ポリシーをターゲットデバイスに割り当て (または割り当て済み)、このポリシーを編集するだけです。

新しいポリシーを作成する場合、ポリシーに名前を付けるダイアログボックスでターゲットデバイスをポリシーに割り当てます。

- Ctrl を押しながらかlickして、目次の [ユーザー定義 (User Defined)] フォルダ内にある [FlexConfig オブジェクト (FlexConfig Object)] を選択し、[>] をクリックしてポリシーに追加します。

オブジェクトが [選択済み追加 FlexConfig (Selected Append FlexConfigs)] リストに追加されます。

- ドラッグアンドドロップを使用して、オブジェクトが正しい順序であることを確認します。

LDAP 属性マップを作成するオブジェクトは、AD/LDAP サーバーにマップを割り当てるオブジェクトの前に配置する必要があります。そうしない場合は、まだ存在していない LDAP 属性マップを割り当てようとすると、エラーが発生します。

リストは次のようになります。

| Selected Append FlexConfigs |                                |
|-----------------------------|--------------------------------|
| #.                          | Name                           |
| 1.                          | Create_LDAP_Map_for_VPN_Access |
| 2.                          | Attach_LDAP_Map_for_VPN_Access |

- e) [保存 (Save)] をクリックします。
- f) すべてのターゲットデバイスがポリシーにまだ割り当てられていない場合は、[保存 (Save)] の下にある [ポリシー割り当て (Policy Assignment)] リンクをクリックし、ここで割り当てを行います。
- g) [設定のプレビュー (Preview Config)] をクリックし、[プレビュー (Preview)] ダイアログボックスで割り当てられているデバイスのいずれかを選択します。

システムでは、デバイスに送信される設定 CLI のプレビューが生成されます。オブジェクトから生成されたコマンドが正しいことを確認します。これらはプレビューの最後に表示されます。また、管理対象機能に加えた他の変更から生成されたコマンドも表示されることに注意してください。LDAP 属性コマンドでは、次のように表示されます。

```
###Flex-config Appended CLI #####Flex-config Appended CLI ###
ldap attribute-map LDAP_Map_for_VPN_Access

map-name memberOf Group-Policy

map-value memberOf CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=example,DC=com
LabAdminAccessGroupPolicy

map-value memberOf CN=Engineering,CN=Users,OU=stbu,DC=example,DC=com
VPNAccessGroupPolicy

aaa-server ad-realm host 10.100.10.10

ldap-attribute-map LDAP_Map_for_VPN_Access

exit
```

**ステップ 4** 変更を展開します。

**ステップ 5** 設定を確認します。

各 FTD デバイスでコマンドが設定されていることを確認できます。デバイスへの SSH セッション、または FMC の CLI ツールを使用します ([システム (System)] > [正常性 (Health)] > [モニター (Monitor)] で、デバイスをクリックしてから、[高度なトラブルシューティング (Advanced Troubleshooting)] をクリックし、[脅威に対する防御 CLI (Threat Defense CLI)] タブを選択します)。次に、構成を表示するコマンドを示します。

- **show running-config aaa-server** は、AD/LDAP サーバーの構成を表示します。
- **show running-config ldap** は、属性マップを表示します。

## LDAP 属性マップの削除

LDAP 属性マップを使用しない場合は、FlexConfig オブジェクトを作成して、機能を展開したデバイスから構成を削除する必要があります。FlexConfig ポリシーから FlexConfig オブジェクトを削除するだけでは不十分です。

ただし、手っ取り早い解決策として、AD/LDAP サーバーにマップを割り当てる FlexConfig オブジェクトを単純に削除し、変更を展開できます。展開プロセスでは、管理対象機能に加えられたすべての変更が削除されるため、サーバーにマップを割り当てる `ldap-attribute-map` コマンドは削除されます。これは、マップがデバイス構成に存在し続けますが、どの AD/LDAP サーバーでも使用されないことを意味します。

次の手順では、マップを削除する方法について説明します。

### 手順

**ステップ 1** LDAP 属性マップを削除する `deploy-once/append` FlexConfig オブジェクトを作成します。

通常、オブジェクトを削除する前に、まずオブジェクトを使用するコマンドを削除する必要があります。ただし、AD/LDAP レルムは管理対象機能であるため、展開ジョブによってこれらのコマンドはすでに削除されています。したがって、属性マップを単純に削除する必要があります。

- [**オブジェクト (Objects)**] > [**オブジェクト管理 (Object Management)**] を選択します。
- 目次から [**FlexConfig**] > [**FlexConfig オブジェクト (FlexConfig Object)**] を選択します。
- [**FlexConfig オブジェクトの追加 (Add FlexConfig Object)**] をクリックし、次のプロパティを設定して、[**保存 (Save)**] をクリックします。

- [**名前 (Name)**] : オブジェクト名。たとえば、`Delete_LDAP_Map_for_VPN_Access` です。
- [**展開 (Deployment)**] : [**1回 (Once)**] を選択します。これらのコマンドは一度に設定する必要があります。
- [**タイプ (Type)**] : デフォルトの [**後に付加 (Append)**] を維持します。コマンドは、直接サポートされている機能のコマンドの後にデバイスに送信されます。LDAP 属性マップを使用するコマンドを削除するには展開ジョブに依存するため、これは特に重要です。
- [**オブジェクト本体 (Object body)**] : オブジェクト本体で、LDAP 属性マップを削除するために必要なコマンドを入力します。マップの内容を削除する必要がないことに注意してください。マップを削除すると、その内容も削除されます。たとえば、マップの名前が `LDAP_Map_for_VPN_Access` の場合、コマンドは次のとおりです。


```
no ldap attribute-map LDAP_Map_for_VPN_Access
```

オブジェクトは、次のようになります。



Name:

Description:

 Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Deployment:  Type:

```
no ldap attribute-map LDAP_Map_for_VPN_Access
```

| Name                  | Dimension | Default Value | Property (Typ... | Override | Description |
|-----------------------|-----------|---------------|------------------|----------|-------------|
| No records to display |           |               |                  |          |             |

**ステップ 2** FlexConfig ポリシーを編集して、LDAP 属性マップの作成と割り当てを行うオブジェクトを削除し、マップを削除するオブジェクトを追加します。

- [デバイス (Devices) ] > [FlexConfig] を選択します。
- FlexConfig ポリシーを編集します。
- [選択済み追加FlexConfig (Selected Appended FlexConfigs) ] リストで、LDAP 属性マップを作成して割り当てるオブジェクトの削除アイコンをクリックします。
- 目次の [ユーザー定義 (User Defined) ] フォルダ内でマップを削除する [FlexConfig オブジェクト (FlexConfig Object) ] を選択し、[>] をクリックしてポリシーに追加します。

オブジェクトが [選択済み追加FlexConfig (Selected Append FlexConfigs) ] リストに追加されます。

リストは次のようになります。

| Selected Append FlexConfigs |                                |
|-----------------------------|--------------------------------|
| #.                          | Name                           |
| 1..                         | Delete_LDAP_Map_for_VPN_Access |

- [保存 (Save) ] をクリックします。
- [設定のプレビュー (Preview Config) ] をクリックし、[プレビュー (Preview) ] ダイアログボックスで割り当てられているデバイスのいずれかを選択します。

システムでは、デバイスに送信される設定 CLI のプレビューが生成されます。オブジェクトから生成されたコマンドが正しいことを確認します。これらはプレビューの最後に表示

されます。また、管理対象機能に加えた他の変更から生成されたコマンドも表示されることに注意してください。この例では、次のような内容が表示されます。

```
###Flex-config Appended CLI ###
no ldap attribute-map LDAP_Map_for_VPN_Access
```

ステップ3 変更を展開します。

## AnyConnect のアイコンとロゴのカスタマイズ

Windows および Linux クライアントマシン上の AnyConnect アプリケーションのアイコンとロゴをカスタマイズできます。アイコンの名前は事前定義されており、アップロードする画像のファイルタイプとサイズには特定の制限があります。

独自の実行可能ファイルを展開して GUI をカスタマイズする場合は、任意のファイル名を使用できますが、この例では、完全にカスタマイズされたフレームワークを展開せずに、アイコンとロゴを置き換えるだけであることを前提としています。

置き換えることができる画像はいくつかあり、それらのファイル名はプラットフォームによって異なります。カスタマイズオプション、ファイル名、タイプ、およびサイズの詳細については、『Cisco AnyConnect Secure Mobility Client Administrator Guide』の「customizing and localizing the AnyConnect client and installer」の章を参照してください。たとえば、4.8 クライアントに関する章は次の場所にあります。

[https://www.cisco.com/c/en/us/td/docs/security/vpn\\_client/anyconnect/anyconnect48/administration/guide/b\\_AnyConnect\\_Administrator\\_Guide\\_4-8/customize-localize-anyconnect.html](https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect48/administration/guide/b_AnyConnect_Administrator_Guide_4-8/customize-localize-anyconnect.html)



(注) 管理に使用するツールに関係なく、任意のFTDデバイスでこのカスタマイズを実行できます。ただし、これらのコマンドの FlexConfig は FMC でのみ動作します。

### 始める前に

この例では、Windows クライアントの次の画像を置き換えます。画像のサイズが最大サイズと異なる場合、自動的に最大サイズに変更され、必要に応じて画像が拡大されます。

- app\_logo.png

このアプリケーションロゴ画像はアプリケーションアイコンであり、最大サイズは 128 X 128 ピクセルです。

- company\_logo.png

この企業ロゴ画像は、トレイライアウトと [詳細 (Advanced) ] ダイアログの左上隅に表示されます。最大サイズは 97 X 58 ピクセルです。

- company\_logo\_alt.png

この代替企業ロゴ画像は、[バージョン情報 (About)] ダイアログの右下隅に表示されます。最大サイズは 97 X 58 ピクセルです。

これらのファイルをアップロードするには、FTD デバイスがアクセスできるサーバーにファイルを配置する必要があります。TFTP、FTP、HTTP、HTTPS、または SCP サーバーを使用できます。これらのファイルから画像を取得するための URL には、サーバーのセットアップに必要なパスとユーザー名/パスワードを含めることができます。この例では、TFTP を使用します。

## 手順

**ステップ 1** カスタマイズされたアイコンとロゴを使用する必要がある、RA VPN ヘッドエンドとして機能している各 FTD デバイスに画像ファイルをアップロードします。

- a) SSH クライアントを使用してデバイス CLI にログインします。
- b) CLI で、**system support diagnostic-cli** コマンドを入力して、診断 CLI モードを開始します。

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
ftdvl>
```

(注) メッセージに示されているように、診断 CLI を終了して通常の FTD CLI モードに戻るには、**Ctrl + A** キーを押してから **D** キーを押す必要があります。

- c) コマンドプロンプトに注意してください。通常の CLI では > だけが表示されますが、診断 CLI のユーザー EXEC モードではホスト名と > が表示されます。この例では、ftdvl> です。特権 EXEC モードを開始する必要があります。このモードでは、ftdvl# のように、# が終了文字として使用されます。プロンプトにすでに # が表示されている場合は、この手順をスキップしてください。それ以外の場合は、**enable** コマンドを入力し、パスワードプロンプトではパスワードを入力せずに単に **Enter** キーを押します。

```
ftdvl> enable
Password:
ftdvl#
```

- d) **copy** コマンドを使用して、ホスティングサーバーから FTD デバイスの disk0 に各ファイルをコピーします。それらのファイルは disk0:/anyconnect-images/ などのサブディレクトリに配置できます。**mkdir** コマンドを使用して新しいフォルダを作成できます。

たとえば、TFTP サーバーの IP アドレスが 10.7.0.80 であり、新しいディレクトリを作成する場合、コマンドは次のようになります。最初の例の後には **copy** コマンドへの応答が省略されていることに注意してください。

```
ftdvl# mkdir disk0:anyconnect-images

Create directory filename [anyconnect-images]? yes

Created dir disk0:/anyconnect-images
```

```
ftdvl# copy /noconfirm tftp://10.7.0.80/app_logo.png
disk0:/anyconnect-images/app_logo.png

Accessing tftp://10.7.0.80/app_logo.png...!!!!!!
Writing file disk0:/anyconnect-images/app_logo.png...
!!!!!!
12288 bytes copied in 1.000 secs (12288 bytes/sec)

ftdvl# copy /noconfirm tftp://10.7.0.80/company_logo.png
disk0:/anyconnect-images/company_logo.png
ftdvl# copy /noconfirm tftp://10.7.0.80/company_logo_alt.png
disk0:/anyconnect-images/company_logo_alt.png
```

**ステップ 2** 診断 CLI で **import webvpn** コマンドを使用して、AnyConnect に、クライアントマシンへの AnyConnect のインストール時にこれらの画像をダウンロードするように指示します。

```
import webvpn AnyConnect-customization type resource platform win name filename
disk0:/directoryname/filename
```

このコマンドは Windows 用です。Linux では、クライアントに応じて、**win** キーワードを **linux** または **linux-64** に置き換えます。

たとえば、前の手順でアップロードしたファイルをインポートする場合、引き続き診断 CLI を使用していると想定すると、次のようになります。

```
ftdvl# import webvpn AnyConnect-customization type resource platform win
name app_logo.png disk0:/anyconnect-images/app_logo.png

ftdvl# import webvpn AnyConnect-customization type resource platform win
name company_logo.png disk0:/anyconnect-images/company_logo.png

ftdvl# import webvpn AnyConnect-customization type resource platform win
name company_logo_alt.png disk0:/anyconnect-images/company_logo_alt.png
```

(注) FlexConfig を使用してこの手順を実行するには、**deploy-once/append FlexConfig** オブジェクトに **import webvpn** コマンドを入力し、FlexConfig ポリシーにオブジェクトを追加してから、関連する FTD デバイスに FlexConfig ポリシーを割り当てます。ただし、各デバイスで診断 CLI の特権 EXEC モードを開始してイメージをアップロードする必要があるため、イメージを同時にインポートするのが実用的です。

**ステップ 3** 設定を確認します。

- インポートしたファイルを確認するには、診断 CLI の特権 EXEC モードで **show import webvpn AnyConnect-customization** コマンドを使用します。
- 画像がクライアントにダウンロードされたことは、ユーザーがクライアントを実行したときに画像が表示されることで確認できます。Windows クライアントで次のフォルダを確認することもできます。ここで、**%PROGRAMFILES%** は、通常、**c:\Program Files** に置き換えられます。

```
%PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client\res
```

## 次のタスク

デフォルトの画像に戻す場合は、カスタマイズしたイメージごとに **revert webvpn** コマンドを（診断 CLI の特権 EXEC モードで）使用します。これは **deploy-once/append FlexConfig** で実行できますが、RA VPN がしばらく動作した後に実行することになるため、より合理的です。FlexConfig を使用すると、各デバイスへの SSH 接続を作成する手間が省け、1 つの展開ジョブでタスクを達成できます。コマンドは、次のとおりです。

```
revert webvpn AnyConnect-customization type resource platform win name filename
```

**import webvpn** の場合と同様に、当該のクライアントプラットフォームをカスタマイズしている場合は **win** を **linux** または **linux-64** に置き換え、インポートした画像ファイル名ごとに個別にコマンドを発行してください。次に例を示します。

```
ftdvl# revert webvpn AnyConnect-customization type resource platform win  
name app_logo.png
```

```
ftdvl# revert webvpn AnyConnect-customization type resource platform win  
name company_logo.png
```

```
ftdvl# revert webvpn AnyConnect-customization type resource platform win  
name company_logo_alt.png
```

# FlexConfig を使用した AnyConnect モジュールとプロファイルの設定

AnyConnect パッケージには、AMP イネーブラなどのさまざまな機能のモジュールが含まれており、RA VPN 接続に追加のサービスを提供するためにオプションで使用できます。各モジュールには、要件に応じてモジュールを機能させるために編集できるプロファイルが含まれています。FTD でこれらのモジュールとプロファイルを有効にするには、FlexConfig を使用する必要があります。

使用するモジュールのみを設定する必要があります。各モジュールには独自のプロファイルエディタがあり、Windows システムにダウンロードしてインストールできる AnyConnect プロファイルエディタ パッケージに含まれています。

AnyConnect パッケージファイルにはすべてのモジュールが含まれているため、モジュール自体はアップロードしません。モジュールで使用されるプロファイルをアップロードするだけで、リモートアクセス VPN 構成で機能するようにモジュールの動作をカスタマイズできます。

バージョン 6.7 以降では、FMC UI を使用してこの機能を設定できます。詳細については、「[Configure Secure Client Modules on a Threat Defense using Cisco Secure Firewall Management Center.](#)」を参照してください。

バージョン 6.4 ~ 6.6 では、FlexConfig を使用して FTD でアプリごとに VPN を有効にできます。この設定には、次の手順を実行します。

## 始める前に

クライアントプロファイルをアップロードするには、その前に、以下の作業を行う必要があります。

- AnyConnect の「Profile Editor - Windows / Standalone installer インストーラ (MSI)」をダウンロードしてインストールします。このインストールファイルは Windows 専用で、ファイル名は `tools-anyconnect-profileeditor-win-<version>-k9.msi` です。ここで、<version> は AnyConnect のバージョンです。たとえば、`tools-anyconnect-win-4.8.03036-profileeditor-k9.msi` です。プロファイルエディタをインストールする前に、Java JRE (1.6以降) もインストールする必要があります。software.cisco.com から、[AnyConnectセキュアモビリティクライアント (AnyConnect Secure Mobility Client)] カテゴリに分類されている AnyConnect プロファイルエディタを入手します。
- プロファイルエディタを使用して、必要なプロファイルを作成します。詳細については、エディタのオンラインヘルプを参照してください。

この例では、プロファイルをアップロードし、すべてのモジュールを有効にします。この例では、すでに機能している RA VPN があり、FMC を使用してすべてのグループポリシーを作成していることを前提としています。

## 手順

**ステップ 1** カスタマイズされたモジュールのプロファイルを使用する必要がある、RA VPN ヘッドエンドとして機能している各 FTD デバイスにプロファイルをアップロードします。

- SSH クライアントを使用してデバイス CLI にログインします。
- CLI で、**system support diagnostic-cli** コマンドを入力して、診断 CLI モードを開始します。

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
ftdv1>
```

(注) メッセージに示されているように、診断 CLI を終了して通常の FTD CLI モードに戻るには、**Ctrl + A** キーを押してから **D** キーを押す必要があります。

- コマンドプロンプトに注意してください。通常の CLI では > だけが表示されますが、診断 CLI のユーザー EXEC モードではホスト名と > が表示されます。この例では、ftdv1> です。特権 EXEC モードを開始する必要があります。このモードでは、ftdv1# のように、# が終了文字として使用されます。プロンプトにすでに # が表示されている場合は、この手順をスキップしてください。それ以外の場合は、enable コマンドを入力し、パスワードプロンプトではパスワードを入力せずに単に Enter キーを押します。

```
ftdv1> enable
Password:
ftdv1#
```

- d) **copy** コマンドを使用して、ホスティングサーバーから FTD デバイスの `disk0` に各ファイルをコピーします。それらのファイルは `disk0:/modules/` などのサブディレクトリに配置できます。**mkdir** コマンドを使用して新しいフォルダを作成できます。

たとえば、TFTP サーバーの IP アドレスが 10.7.0.80 であり、新しいディレクトリを作成する場合、コマンドは次のようになります。最初の例の後には **copy** コマンドへの応答が省略されていることに注意してください。

```
ftdvl# mkdir disk0:modules

Create directory filename [modules]? yes

Created dir disk0:/modules

ftdvl# copy /noconfirm tftp://10.7.0.80/amp.asp
disk0:/modules/amp.asp

Accessing tftp://10.7.0.80/amp.asp...!!!
Writing file disk0:/modules/amp.asp...
!
676 bytes copied in 0.0 secs (812800 bytes/sec)

ftdvl# copy /noconfirm tftp://10.7.0.80/ACManifestUmbrella-01.xml
disk0:/modules/ACManifestUmbrella-01.xml
ftdvl# copy /noconfirm tftp://10.7.0.80/feedback.fsp
disk0:/modules/feedback.fsp
ftdvl# copy /noconfirm tftp://10.7.0.80/iseposture.isp
disk0:/modules/iseposture.isp
ftdvl# copy /noconfirm tftp://10.7.0.80/nam.nsp
disk0:/modules/nam.nsp
ftdvl# copy /noconfirm tftp://10.7.0.80/networkvisibility.nvmosp
disk0:/modules/networkvisibility.nvmosp
ftdvl# copy /noconfirm tftp://10.7.0.80/websecurity.wso
disk0:/modules/websecurity.wso
ftdvl# copy /noconfirm tftp://10.7.0.80/vpn.xml
disk0:/modules/vpn.xml
```

**ステップ 2** 各モジュールのプロファイルを識別し、RA VPN の各グループプロファイルのモジュールを有効にする、`deploy-everytime/append` FlexConfig オブジェクトを作成します。

- [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- 目次から [FlexConfig] > [FlexConfig オブジェクト (FlexConfig Object)] を選択します。
- [FlexConfig オブジェクトの追加 (Add FlexConfig Object)] をクリックし、次のプロパティを設定して、[保存 (Save)] をクリックします。

- [名前 (Name)] : オブジェクト名。たとえば、`Enable_AnyConnect_Module_Profiles` です。
- [展開 (Deployment)] : [毎回 (Everytime)] を選択します。FMC によってアクティブに管理される機能を変更しているため、変更は各展開ジョブ中に削除されます。したがって、変更を展開するたびに再設定する必要があります。
- [タイプ (Type)] : デフォルトの [後に付加 (Append)] を維持します。
- [オブジェクト本体 (Object body)] : オブジェクト本体で、プロファイルの識別、モジュールの有効化、およびプロファイルを使用する各グループポリシーのプロファイ

ルの適用に必要なコマンドを入力します。設定する必要があるコマンドは次のとおりです。

- **anyconnect profiles** *profile\_name file\_location*

このコマンドは、webvpn コンフィギュレーション モードで、プロファイルの名前、および FTD デバイスのディスク上のプロファイルの完全なパスとファイル名を指定します。このコマンドは、プロファイルを AnyConnect とそのモジュールで使用できるようにします。

- **anyconnect modules value** *module\_names*

このコマンドは、グループポリシーの webvpn コンフィギュレーション モードで、グループポリシーに対して有効にする AnyConnect モジュールを指定します。モジュールを使用する各グループポリシーでこのコマンドを使用する必要があります。複数のモジュールは、スペースを入れずにカンマで区切って指定できます。

- 有効なモジュール名は次のとおりです。

- **dart** : AnyConnect Diagnostics and Reporting Tool (DART)
- **nam** : AnyConnect ネットワーク アクセス マネージャ
- **vpngina** : AnyConnect Start Before Logon (SBL)
- **websecurity** : AnyConnect Web セキュリティモジュール
- **telemetry** : AnyConnect テレメトリモジュール
- **posture** : AnyConnect ポスチャモジュール
- **ampenabler** : AnyConnect AMP イネーブラ
- **iseposture** : AnyConnect ISE Posture
- **umbrella** : AnyConnect Umbrella

- **anyconnect profiles value** *profile\_name type module\_name*

このコマンドは、グループポリシーの webvpn コンフィギュレーション モードで、**anyconnect modules** コマンドにより有効にしたモジュールに使用するプロファイルを指定します。例外は **feedback** モジュールで、最初に有効にする必要はありません。モジュール名は **anyconnect modules** コマンドで使用されているものと同じですが、タイプが **user** の **vpngina** は例外です。

たとえば、次のコマンドは、G10 という名前のグループポリシーに対して以前にアップロードしたモジュールを設定します。追加のグループポリシーがある場合は、グループポリシーごとに **group-policy** コマンドで始まるコマンドセットを繰り返す必要があります。

```
webvpn
  anyconnect profiles ACManifestUmbrella-01.xml
disk0:/modules/ACManifestUmbrella-01.xml
  anyconnect profiles amp.asp disk0:/modules/amp.asp
```



```

anyconnect profiles feedback.fsp disk0:/modules/feedback.fsp
anyconnect profiles iseposture.isp disk0:/modules/iseposture.isp
anyconnect profiles nam.nsp disk0:/modules/nam.nsp
anyconnect profiles networkvisibility.nvmsp disk0:/modules/networkvisibility.nvmsp

anyconnect profiles vpn.xml disk0:/modules/vpn.xml
anyconnect profiles websecurity.wso disk0:/modules/websecurity.wso
group-policy GP10 attributes
webvpn
  anyconnect modules value
  ampenabler,dart,iseposture,nam,nvm,umbrella,vpngina,websecurity
  anyconnect profiles value amp.asp type ampenabler
  anyconnect profiles value feedback.fsp type feedback
  anyconnect profiles value iseposture.isp type iseposture
  anyconnect profiles value nam.nsp type nam
  anyconnect profiles value networkvisibility.nvmsp type nvm
  anyconnect profiles value ACManifestUmbrella-01.xml type umbrella
  anyconnect profiles value websecurity.wso type websecurity
  anyconnect profiles value vpn.xml type user

```

オブジェクトは、次のようになります。

Name:

Description:

Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Deployment:  Type:

```

webvpn
anyconnect profiles ACManifestUmbrella-01.xml disk0:/modules/ACManifestUmbrella-01.xml
anyconnect profiles amp.asp disk0:/modules/amp.asp
anyconnect profiles feedback.fsp disk0:/modules/feedback.fsp
anyconnect profiles iseposture.isp disk0:/modules/iseposture.isp
anyconnect profiles nam.nsp disk0:/modules/nam.nsp
anyconnect profiles networkvisibility.nvmsp disk0:/modules/networkvisibility.nvmsp
anyconnect profiles vpn.xml disk0:/modules/vpn.xml
anyconnect profiles websecurity.wso disk0:/modules/websecurity.wso
group-policy GP10 attributes
webvpn
  anyconnect modules value ampenabler,dart,iseposture,nam,nvm,umbrella,vpngina,websecurity
  anyconnect profiles value amp.asp type ampenabler
  anyconnect profiles value feedback.fsp type feedback

```

| Name                  | Dimension | Default Value | Property (Typ... | Override | Description |
|-----------------------|-----------|---------------|------------------|----------|-------------|
| No records to display |           |               |                  |          |             |

**ステップ 3** このオブジェクトを展開する FlexConfig ポリシーを作成します。

- a) [デバイス (Devices)] > [FlexConfig] を選択します。
- b) [新しいポリシー (New Policy)] をクリックするか、既存の FlexConfig ポリシーをターゲットデバイスに割り当て (または割り当て済み)、このポリシーを編集するだけです。

新しいポリシーを作成する場合、ポリシーに名前を付けるダイアログボックスでターゲットデバイスをポリシーに割り当てます。

- c) 目次の [ユーザー定義 (User Defined)] フォルダ内にある [FlexConfigオブジェクト (FlexConfig Object)] を選択し、[>] をクリックしてポリシーに追加します。

オブジェクトが [選択済み追加FlexConfig (Selected Append FlexConfigs)] リストに追加されます。

リストは次のようになります。

| Selected Append FlexConfigs |                                   |
|-----------------------------|-----------------------------------|
| #.                          | Name                              |
| 1..                         | Enable_AnyConnect_Module_Profiles |

- d) [保存 (Save)] をクリックします。
- e) すべてのターゲットデバイスがポリシーにまだ割り当てられていない場合は、[保存 (Save)] の下にある [ポリシー割り当て (Policy Assignment)] リンクをクリックし、ここで割り当てを行います。
- f) [設定のプレビュー (Preview Config)] をクリックし、[プレビュー (Preview)] ダイアログボックスで割り当てられているデバイスのいずれかを選択します。

システムでは、デバイスに送信される設定 CLI のプレビューが生成されます。オブジェクトから生成されたコマンドが正しいことを確認します。これらはプレビューの最後に表示されます。また、管理対象機能に加えた他の変更から生成されたコマンドも表示されることに注意してください。これらのコマンドについては、次のような内容が表示されます。

```
###Flex-config Appended CLI ###
webvpn

anyconnect profiles ACManifestUmbrella-01.xml disk0:/modules/ACManifestUmbrella-01.xml

anyconnect profiles amp.asp disk0:/modules/amp.asp

anyconnect profiles feedback.fsp disk0:/modules/feedback.fsp

anyconnect profiles iseposture.isp disk0:/modules/iseposture.isp

anyconnect profiles nam.nsp disk0:/modules/nam.nsp

anyconnect profiles networkvisibility.nvmisp disk0:/modules/networkvisibility.nvmisp

anyconnect profiles vpn.xml disk0:/modules/vpn.xml

anyconnect profiles websecurity.wso disk0:/modules/websecurity.wso

group-policy GP10 attributes

webvpn

anyconnect modules value
ampenabler,dart,iseposture,nam,nvm,umbrella,vpngina,websecurity

anyconnect profiles value amp.asp type ampenabler

anyconnect profiles value feedback.fsp type feedback
```

```
anyconnect profiles value iseposture.isp type iseposture

anyconnect profiles value nam.nsp type nam

anyconnect profiles value networkvisibility.nvmssp type nvm

anyconnect profiles value ACManifestUmbrella-01.xml type umbrella

anyconnect profiles value websecurity.wso type websecurity

anyconnect profiles value vpn.xml type user
```

#### ステップ 4 変更を展開します。

##### 次のタスク

管理対象機能を変更するため、モジュール構成を削除するには、単純に FlexConfig ポリシーから FlexConfig オブジェクトを削除してから、構成を再展開します。展開ジョブによって構成の変更が削除されます。

デバイスからプロファイルを削除する場合は、各デバイスの CLI にログインし、診断 CLI の特権 EXEC モードで **delete** コマンドを使用する必要があります。

## モバイルデバイスでのアプリケーションベース（アプリごと）のリモートアクセス VPN

Android または iOS を実行している電話などのモバイルデバイスをサポートする場合は、Mobile Device Manager (MDM) アプリケーションを使用して VPN アクセスを微調整し、サポートされているアプリケーションのみに VPN トンネルの使用を許可できます。リモートアクセス VPN を承認済みアプリケーションに制限することにより、VPN ヘッドエンドの負荷を削減し、これらのモバイルデバイスにインストールされている悪意のあるアプリケーションから企業のネットワークを保護することもできます。

アプリケーションごとのリモートアクセス VPN を使用するには、サードパーティの MDM アプリケーションをインストールして設定する必要があります。これは承認済みアプリケーションのリストを定義する MDM であり、VPN トンネル経由で使用できます。選択したサードパーティ MDM を設定および使用する方法の解説は、このドキュメントの対象範囲外です。

バージョン 7.0 以降では、FMC UI を使用してこの機能を設定できます。詳細については、「[Configure Application-Based Remote Access VPN \(Per App VPN\) on Mobile Devices Using Cisco Secure Firewall Management Center](#)」を参照してください。

バージョン 6.4 ~ 6.7 では、FlexConfig を使用して FTD でアプリごとに VPN を有効にできます。次のトピックでは、FTD ヘッドエンドで FlexConfig を使用してアプリごとの VPN を有効にして、MDM がモバイルデバイスにポリシーを適用できるようにする方法について説明します。

## アプリケーションベース（アプリごと）の VPN について

AnyConnect を使用してモバイルデバイスから VPN 接続を確立すると、個人アプリケーションからのトラフィックを含むすべてのトラフィックが VPN 経由でルーティングされます。

代わりに企業のアプリケーションのみを VPN 経由でルーティングし、企業以外のトラフィックを VPN から除外する場合は、アプリごとの VPN を使用して、VPN 経由でトンネリングするアプリケーションを選択できます。

**perapp** AnyConnect カスタム属性を使用してアプリごとの VPN を設定します。この属性をリモートアクセス VPN グループプロファイルに追加すると、トンネルが明示的に識別されたアプリケーションに自動的に制限されます。他のすべてのアプリケーションからのトラフィックは、トンネルから自動的に除外されます。

アプリごとの VPN を設定すると、次の主要なメリットがもたらされます。

- [パフォーマンス (Performance) ] : VPN 内のトラフィックを企業のネットワークに送信する必要があるトラフィックに制限します。したがって、RA VPN のヘッドエンドでリソースが解放されます。
- [保護 (Protection) ] : 承認済みのアプリケーションからのトラフィックのみが許可されるため、ユーザーが意図せずモバイルデバイスにインストールした可能性がある未承認の悪意のあるアプリケーションから企業のトンネルを保護します。これらのアプリケーションはトンネルに含まれないため、これらのアプリケーションからのトラフィックはヘッドエンドに送信されません。

モバイルエンドポイントで実行されている Mobile Device Manager (MDM) は、アプリケーションごとの VPN ポリシーをアプリケーションに適用します。

## モバイルアプリのアプリケーション ID の決定

モバイルデバイスからアプリケーションベースの VPN を許可するように FTD ヘッドエンドを設定する前に、トンネルで許可するアプリケーションを決定する必要があります。

ユーザーのモバイルデバイスにサービスを提供するために選択した Mobile Device Manager (MDM) にアプリケーションごとのポリシーを設定することを強く推奨します。これにより、ヘッドエンドの設定が大幅に簡素化されます。

代わりにまた、ヘッドエンドで許可されているアプリケーションのリストを設定することにした場合は、エンドポイントのタイプごとに各アプリケーションのアプリケーション ID を決定する必要があります。

iOS でバンドル ID と呼ばれるアプリケーション ID は、逆引き DNS 名です。ワイルドカードとしてアスタリスクを使用できます。たとえば、\*.\* はすべてのアプリケーションを示し、com.cisco.\* はすべてのシスコアプリケーションを示します。

アプリケーション ID を決定するには、次の手順を実行します。

- **Android** : Web ブラウザで Google Play に移動し、アプリカテゴリを選択します。許可するアプリケーションをクリック（またはマウスオーバー）して、URL を確認します。アプリ

ケーション ID は、URL 内の **id=**パラメータに示されます。たとえば、次は Facebook Messenger の URL であるため、アプリケーション ID は `com.facebook.orca` です。

`https://play.google.com/store/apps/details?id=com.facebook.orca`

独自のアプリケーションなどの Google Play を通じて入手できないアプリケーションの場合は、パッケージ名ビューアアプリケーションをダウンロードして、アプリケーション ID を抽出します。これらの多くの使用可能アプリケーションがあり、そのいずれかが必要なものを提供しますが、シスコはどれも推奨しません。

• **iOS** : バンドル ID を取得する簡単な方法はありません。次の方法で検索できます。

1. Chrome などのデスクトップの Web ブラウザを使用して、アプリケーション名を検索します。

2. 検索結果で、Apple App Store からアプリケーションをダウンロードするためのリンクを探します。たとえば、Facebook Messenger は次のようになります。

`https://apps.apple.com/us/app/messenger/id454638411`

3. **id** 文字列の後に数値をコピーします。この例では、**454638411** です。

4. 新しいブラウザウィンドウを開き、次の URL の末尾に数値を追加します。

`https://itunes.apple.com/lookup?id=`

この例では、次のとおりです。 `https://itunes.apple.com/lookup?id=454638411`

5. 通常は `1.txt` という名前のテキストファイルをダウンロードするように求められます。ファイルをダウンロードします。

6. ワードパッドなどのテキストエディタでファイルを開き、**bundleId** を検索します。次に例を示します。

`"bundleId": "com.facebook.Messenger"`

この例では、バンドル ID は「`com.facebook.Messenger`」です。これをアプリケーション ID として使用します。

アプリケーション ID のリストを取得したら、[アプリケーションベース（アプリごと）の VPN トンネルの設定（29 ページ）](#) で説明されているように、ポリシーを設定できます。

## アプリケーションベース（アプリごと）の VPN トンネルの設定

Mobile Device Manager (MDM) ソフトウェアソリューションをインストールして設定したら、FTD ヘッドエンドデバイスでアプリケーションベース（アプリごと）の VPN を有効にできます。ヘッドエンドで有効にすると、MDM ソフトウェアは、VPN を介して企業のネットワークにトンネリングされるアプリケーションの制御を開始します。

### 始める前に

この機能には、AnyConnect Plus または Apex ライセンスが必要です。Android および iOS デバイスでのみ動作します。

この例では、リモートアクセス VPN がすでに設定されており、正しく機能していることを前提としています。

また、サードパーティの Mobile Device Manager をすでにインストールして設定している必要があります。FTD ヘッドエンドデバイスではなく、MDM 自体の VPN で許可されるアプリケーションを設定します。代わりに、FTD でアプリごとの VPN を単純に有効にし、MDM を使用してアプリごとのポリシーを設定および導入することを推奨します。次の例では、FTD ヘッドエンドでアプリケーションを指定するのではなく、このアプローチを使用することを前提としています。

## 手順

**ステップ 1** software.cisco.com から **[Cisco AnyConnect 企業アプリケーションセレクタ (Cisco AnyConnect Enterprise Application Selector)]** をダウンロードします。このアプリケーションは、**[AnyConnect セキュア モビリティ クライアント v4.x (AnyConnect Secure Mobility Client v4.x)]** カテゴリにあります。

アプリケーションの jar ファイルを実行するには、Java 7 を実行している必要があります。

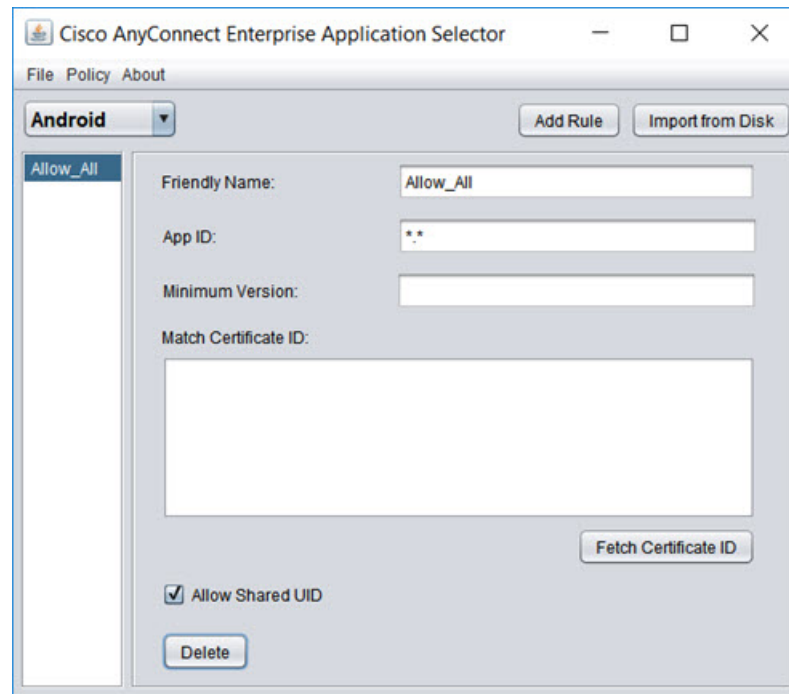
**ステップ 2** AnyConnect 企業アプリケーションセレクタを使用して、アプリごとの VPN ポリシーを定義します。

Allow All などの単純なポリシーを作成し、MDM 構成で許可するアプリケーションを定義することを推奨します。ただし、アプリケーションのリストを指定して、ヘッドエンドからリストを許可および制御できます。特定のアプリケーションを含める場合は、一意のフレンドリ名とアプリケーションのアプリケーション ID を使用して、アプリケーションごとに個別のルールを作成します。アプリケーション ID の取得については、「[モバイルアプリのアプリケーション ID の決定 \(28 ページ\)](#)」を参照してください。

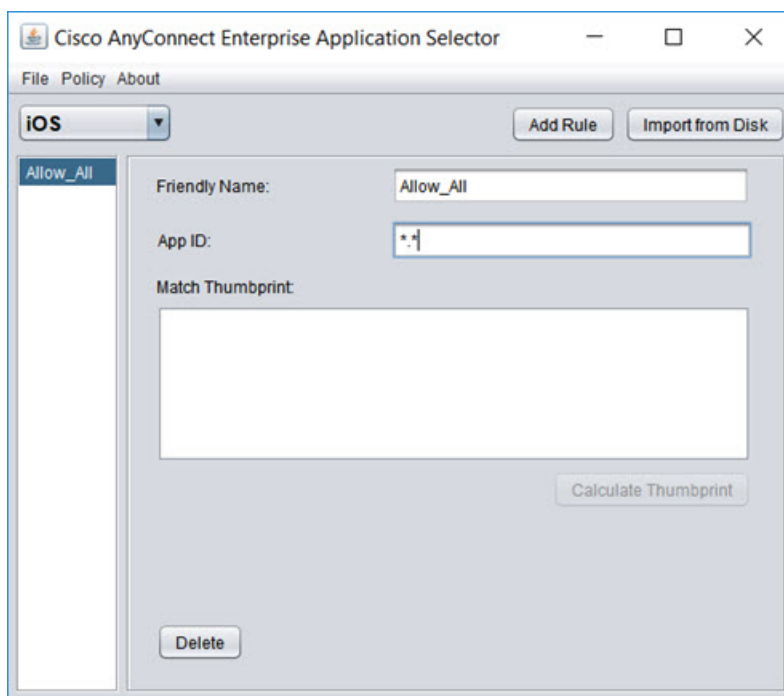
次の手順では、Android と iOS の両方のプラットフォームをサポートする [すべてを許可 (Allow All)] ポリシーを作成する方法について説明します。

a) AnyConnect 企業アプリケーションセレクタで、プラットフォームタイプとして **[Android]** を選択し、次のオプションを入力します。

- **[フレンドリ名 (Friendly Name)]** : Allow\_All などの意味のあるもの。
- **[アプリケーション ID (App ID)]** : \*.\* を入力して、使用可能なすべてのアプリケーションを照合します。
- その他のフィールドはすべて無視します。これらは、実際のアプリケーションとバージョンに合わせて微調整するために使用されます。

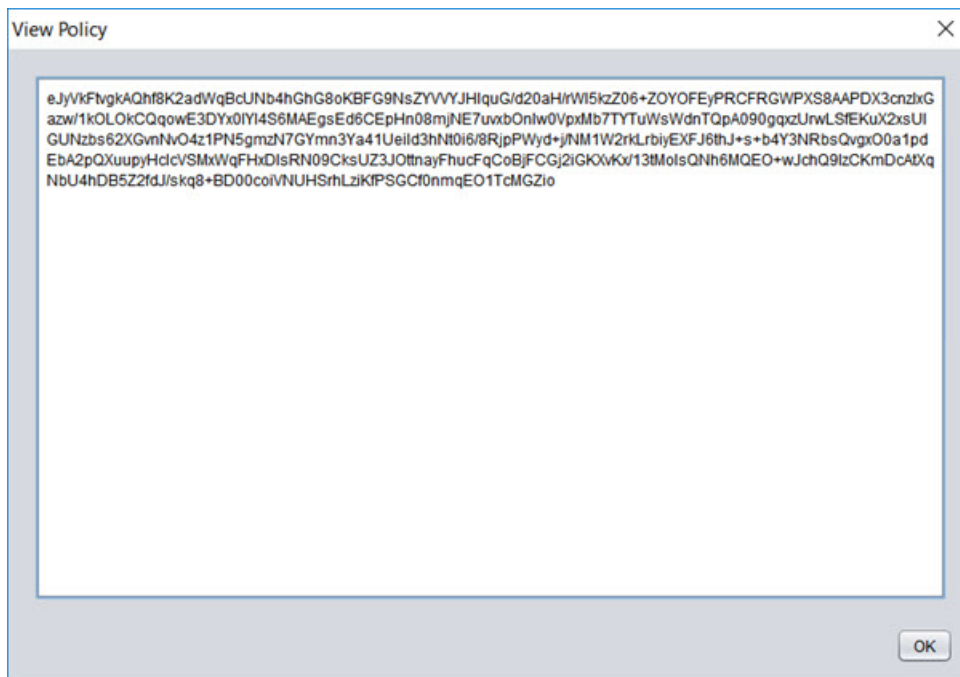


- b) プラットフォームタイプとして [iOS] を選択し、次のオプションを入力します。
- [フレンドリ名 (Friendly Name) ] : Allow\_All などの意味のあるもの。
  - [アプリケーションID (App ID) ] : \*.\* を入力して、使用可能なすべてのアプリケーションを照合します。
  - その他のフィールドはすべて無視します。



- c) [ポリシー（Policy）] > [ポリシーの表示（View Policy）] を選択します。

読み取り不可の base64 文字列を取得します。この文字列には、作成したポリシーを表示するために FTD システムが解凍する暗号化された XML ファイルが含まれています。以降の手順では、この文字列のコピーを使用します。





**ステップ 3** perapp カスタム属性を作成し、AnyConnect 企業アプリケーションセクタで作成されたアプリごとの base64 ポリシーを割り当てる、deploy-once/append FlexConfig オブジェクトを作成します。

- [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- 目次から [FlexConfig] > [FlexConfig オブジェクト (FlexConfig Object)] を選択します。
- [FlexConfig オブジェクトの追加 (Add FlexConfig Object)] をクリックし、次のプロパティを設定して、[保存 (Save)] をクリックします。

- [名前 (Name)] : オブジェクト名。たとえば、Per\_App\_Allow\_All\_Policy です。
- [展開 (Deployment)] : [1回 (Once)] を選択します。これらのコマンドは一度に設定する必要があります。
- [タイプ (Type)] : デフォルトの [後に付加 (Append)] を維持します。コマンドは、直接サポートされている機能のコマンドの後にデバイスに送信されます。
- [オブジェクト本体 (Object body)] : オブジェクト本体で、perapp タイプの属性を作成するために必要なコマンドを入力し、属性名と base64 ポリシー文字列を追加します。データ要素は 420 文字に制限されているため、base64 文字列がそれよりも長い場合は、分割して複数の anyconnect-custom-data コマンドを使用する必要があります。特定の変数に対して複数のデータコマンドを使用する場合、2 番目以降のコマンドは単純に初期データ文字列に追加されます。base64 文字列を正確に 420 文字にカットすることも、簡単に処理できるチャンクにカットすることもできます。たとえば、perAppPolicy という名前の属性を作成し、Allow\_All ポリシーを使用する場合、コマンドは次のようになります。説明は省略できますが、説明が含まれている場合は個別のコマンドではなく、anyconnect-custom-attr コマンドの一部であることに注意してください。（この例では、読みやすくするために改行が追加されています）。

```
webvpn
anyconnect-custom-attr perapp description Per-App Allow All VPN Policy
anyconnect-custom-data perapp perAppPolicy
eJyVvKftvgkAQhf8K2adWgBcUNb4hGhG8oKBFG9NsZYVVYJH1quG/d20aH/rW15kzZ06+
ZOYOFeyPRCFRGWPXS8AAPDX3cnzlxGazw/1kOLOkCQqowE3DYx0IYI4S6MAEgEd6CEp
Hn08mjNE7uvxbOnIw0VpxMb7TYTuWswdnTQpA090gqzxUrwLSfEKuX2xsUlGUNzbs62X
GvnNvO4z1PN5gmzN7GYmn3Ya41Ueild3hNt0i6/8Rj
anyconnect-custom-data perapp perAppPolicy
pPWyd+j/NM1W2rkLrbiyEXFJ6thJ+s+b4Y3NRbsQvgx00a1pdEbA2pQXuupyHclcVSMxW
qFHxDlsRN09CksUZ3JOttnayFhucFqCoBjFCGj2iGKXvKx/13tMoIsQNh6MQEO+wJchQ9
IzCKmDcAtXqNbU4hDB5Z2fdJ/skq8+BD00coiVNUHSrhLziKfPSGCf0nmqEO1TcMGZio
```

オブジェクトは、次のようになります。

Name:

Description:

Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Deployment:  Type:

```
webvpn
anyconnect-custom-attr perapp description Per-App Allow All VPN Policy
anyconnect-custom-data perapp perAppPolicy
eJyVvKftvgkAQhf8K2adWqBcUNb4hGhG8oKBFG9NsZYVVYJH1quG/d20aH/rW15kzZ06+ZOYOFeyPRCFRGWPXS8AAPDX3cnzlxGazw/1
anyconnect-custom-data perapp perAppPolicy
pFWyd+j/NM1W2rkLrbiyEXFJ6thJ+s+b4Y3NRbsQvgx00a1pdEbA2pQXuupyHclcVSMxWqFHxD1sRN09CksUZ3JOttnayFhucFqCoBj
```

| Name                  | Dimension | Default Value | Property (Typ... | Override | Description |
|-----------------------|-----------|---------------|------------------|----------|-------------|
| No records to display |           |               |                  |          |             |

**ステップ 4** カスタムグループポリシーを使用する場合は、`deploy-once/append FlexConfig` オブジェクトを作成して、グループポリシーでダイナミックスプリットトンネルのカスタム属性を設定します。

`DfltGrpPolicy` という名前のデフォルトグループポリシーを使用する場合は、`deploy-everytime/append FlexConfig` オブジェクトを作成して、グループポリシーにダイナミックスプリットトンネルのカスタム属性を設定します。このオブジェクトは毎回展開する必要があります。これは、展開のたびに、システムがデフォルトポリシーに対するカスタム変更を無効にするためです。

カスタムグループポリシーでは、デフォルトのグループポリシーとは異なり、システムは変更を無効にしません。そのため、変更を1回展開する必要があります。複数のグループポリシーを使用する場合は、単一の `FlexConfig` オブジェクトを使用してカスタム属性を各ポリシーに順番に追加できます。あるいは、グループポリシーごとに1つの `FlexConfig` オブジェクトを作成できます。結果は同じになるため、`FlexConfig` ポリシーをモジュール化するための独自の要件に基づいて選択します。

次の手順は、「sales」カスタムグループポリシー用です。デフォルトグループではなく、カスタムグループを使用することを推奨します。

- [**オブジェクト (Objects)**] > [**オブジェクト管理 (Object Management)**] を選択します。
- 目次から [**FlexConfig**] > [**FlexConfig オブジェクト (FlexConfig Object)**] を選択します。
- [**FlexConfig オブジェクトの追加 (Add FlexConfig Object)**] をクリックし、次のプロパティを設定して、[**保存 (Save)**] をクリックします。

• [名前 (Name)]: オブジェクト名。たとえば、`Add_Per_App_VPN` などです。

- [展開 (Deployment)] : [1回 (Once)] を選択します。
- [タイプ (Type)] : デフォルトの [後に付加 (Append)] を維持します。
- [オブジェクト本体 (Object body)] : オブジェクト本体で、グループポリシーにカスタム属性を追加するために必要なコマンドを入力します。たとえば、作成した属性の名前が perAppPolicy で、グループポリシーの名前が「sales」の場合、コマンドは次のとおりです。

```
group-policy sales attributes
anyconnect-custom perapp value perAppPolicy
```

オブジェクトは、次のようになります。

**ステップ 5** これらのオブジェクトを展開する FlexConfig ポリシーを作成します。

- [デバイス (Devices)] > [FlexConfig] を選択します。
- [新しいポリシー (New Policy)] をクリックするか、既存の FlexConfig ポリシーをターゲットデバイスに割り当て（または割り当て済み）、このポリシーを編集するだけです。

新しいポリシーを作成する場合、ポリシーに名前を付けるダイアログボックスでターゲットデバイスをポリシーに割り当てます。

- Ctrl を押しながらかlickして、目次の [ユーザー定義 (User Defined)] フォルダ内にある [FlexConfig オブジェクト (FlexConfig Object)] を選択し、[>] をクリックしてポリシーに追加します。

オブジェクトが [選択済み追加 FlexConfig (Selected Append FlexConfigs)] リストに追加されます。

- d) ドラッグアンドドロップを使用して、オブジェクトが正しい順序であることを確認します。

カスタム属性オブジェクトを作成するオブジェクトは、その属性をグループポリシーに割り当てるオブジェクトの前に配置する必要があります。そうしない場合は、まだ存在しないカスタム属性を追加しようとすると、エラーが発生します。

カスタムグループポリシーを設定する単一のオブジェクトがある場合、リストは次のようになります。

| Selected Append FlexConfigs |                          |
|-----------------------------|--------------------------|
| #.                          | Name                     |
| 1..                         | Per_App_Allow_All_Policy |
| 2..                         | Add_Per_App_VPN          |

- e) [保存 (Save)] をクリックします。
- f) すべてのターゲットデバイスがポリシーにまだ割り当てられていない場合は、[保存 (Save)] の下にある [ポリシー割り当て (Policy Assignment)] リンクをクリックし、ここで割り当てを行います。
- g) [設定のプレビュー (Preview Config)] をクリックし、[プレビュー (Preview)] ダイアログボックスで割り当てられているデバイスのいずれかを選択します。

システムでは、デバイスに送信される設定 CLI のプレビューが生成されます。オブジェクトから生成されたコマンドが正しいことを確認します。これらはプレビューの最後に表示されます。また、管理対象機能に加えた他の変更から生成されたコマンドも表示されることに注意してください。これらのコマンドについては、次のような内容が表示されます。

```
###Flex-config Appended CLI ###
webvpn

anyconnect-custom-attr perapp description Per-App Allow All VPN Policy
anyconnect-custom-data perapp perAppPolicy eJyVkJtvgkAQhf8K2adWqBcUNb4hGh
anyconnect-custom-data perapp perAppPolicy pFWyd+j/NM1W2rkLrbiyEXFJ6thJ+s
group-policy sales attributes

anyconnect-custom perapp value perAppPolicy
```

**ステップ 6** 変更を展開します。

**ステップ 7** 設定を確認します。

- 各 FTD デバイスでコマンドが設定されていることを確認できます。デバイスへの SSH セッション、または FMC の CLI ツールを使用します ([システム (System)] > [正常性 (Health)] > [モニター (Monitor)] で、デバイスをクリックしてから、[高度なトラブルシューティング (Advanced Troubleshooting)] をクリックし、[脅威に対する防御 CLI (Threat Defense CLI)] タブを選択します)。次に、構成を表示するコマンドを示します。

- **show running-config webvpn**
  - **show running-config anyconnect-custom-data**
  - **show running-config group-policy name**、ここで、*name* を sales などのグループポリシー名に置き換えます。
- AnyConnect クライアントからシステムが正しく動作していることを確認できます。クライアント統計情報を開き、次の情報を探します。
- [トンネルモード (Tunnel Mode)] は、[全トラフィックをトンネリング (Tunnel All Traffic)] ではなく [アプリケーショントンネル (Application Tunnel)] と表示されます。

| VPN Statistics                |                    |
|-------------------------------|--------------------|
| <b>CONNECTION INFORMATION</b> |                    |
| Time Connected                | 00:00:53           |
| Status                        | Connected          |
| Tunneling Mode                | Application Tunnel |
| Tunneling Mode (IPv6)         | Application Tunnel |

- [トンネリングされたアプリケーション (Tunneled Apps)] には、MDM でトンネリングを有効にしたアプリケーションがリストされます。

| TUNNELED APPS |  |
|---------------|--|
|               | Teams (com.cisco.wx2.android)                                      |
|               | Cisco Jabber (com.cisco.im)  |
|               | Mobile Setup (com.cisco.ft.ystore.android.setup)                   |
|               | Network Setup Assistant (com.cisco.cpm.spw.android.wifisupplicant) |
|               | Outlook (com.microsoft.office.outlook)                             |

## 次のタスク

Per App VPN を使用しない場合は、FlexConfig オブジェクトを作成して、FTD デバイスから構成を削除する必要があります。さらに、MDM を削除する必要があります。手順については、MDM のマニュアルを参照してください。

FTD ヘッドエンドでは、それを使用する各グループポリシーからカスタム属性を削除するために必要なコマンドを含む、`deploy-once/append FlexConfig` オブジェクトを作成してから、カスタム属性を削除します。たとえば、`DfltGrpPolicy` と `sales` という 2 つのグループポリシーでカスタム属性が使用され、その属性の名前が `perAppPolicy` の場合、コマンドは次のようになります。

```
group-policy DfltGrpPolicy attributes
```

```
no anyconnect-custom perapp

group-policy sales attributes
no anyconnect-custom perapp

no anyconnect-custom-data perapp perAppPolicy

webvpn
no anyconnect-custom-attr perapp
```

次に、FlexConfig ポリシーで、属性の作成と割り当てを行うオブジェクトを削除し、この新しいオブジェクトを追加します。構成を展開すると、アプリごとの機能がグループポリシーから削除されます。



## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。