セキュアファイアウォールでのセキュアクライアントVPN管理トンネルの設定

内容

はじめに

このドキュメントでは、Cisco FMCによって管理されるセキュアファイアウォールの脅威対策でセキュアクライアントVPN管理トンネルを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco AnyConnect Profile Editor
- Firewall Management Center(FMC)によるSSL AnyConnectの設定
- クライアント証明書認証

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Firewall Threat Defense(FTD)バージョン6.7.0（ビルド65）

- Cisco FMCバージョン6.7.0（ビルド65）
- Windows 10マシンにインストールされたCisco AnyConnect 4.9.01095

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

この例では、Secure Sockets Layer(SSL)を使用して、FTDとWindows 10クライアントの間にバーチャルプライベートネットワーク(VPN)を作成します。

リリース6.7以降、Cisco FTDはAnyConnect管理トンネルの設定をサポートしています。この修正により、以前にオープンされた拡張要求Cisco Bug ID CSCvs78215が修正されます。

AnyConnect Management機能を使用すると、エンドポイントの起動が完了した直後にVPNトンネルを作成できます。ユーザがAnyConnectアプリを手動で起動する必要はありません。システムの電源が入るとすぐに、AnyConnect VPNエージェントサービスが管理VPN機能を検出し、AnyConnect管理VPNプロファイルのサーバリストで定義されているホストエントリを使用してAnyConnectセッションを開始します。

制限事項

- クライアント証明書認証のみがサポートされます。
- Windowsクライアントでは、マシン証明書ストアのみがサポートされます。
- Cisco Firepower Device Manager(FDM)ではサポートされていません。Cisco Bug ID CSCvx90058。
- Linuxクライアントではサポートされません。

すべての制限事項については、『Cisco Secure Client管理者ガイドリリース5』を参照してください。

設定

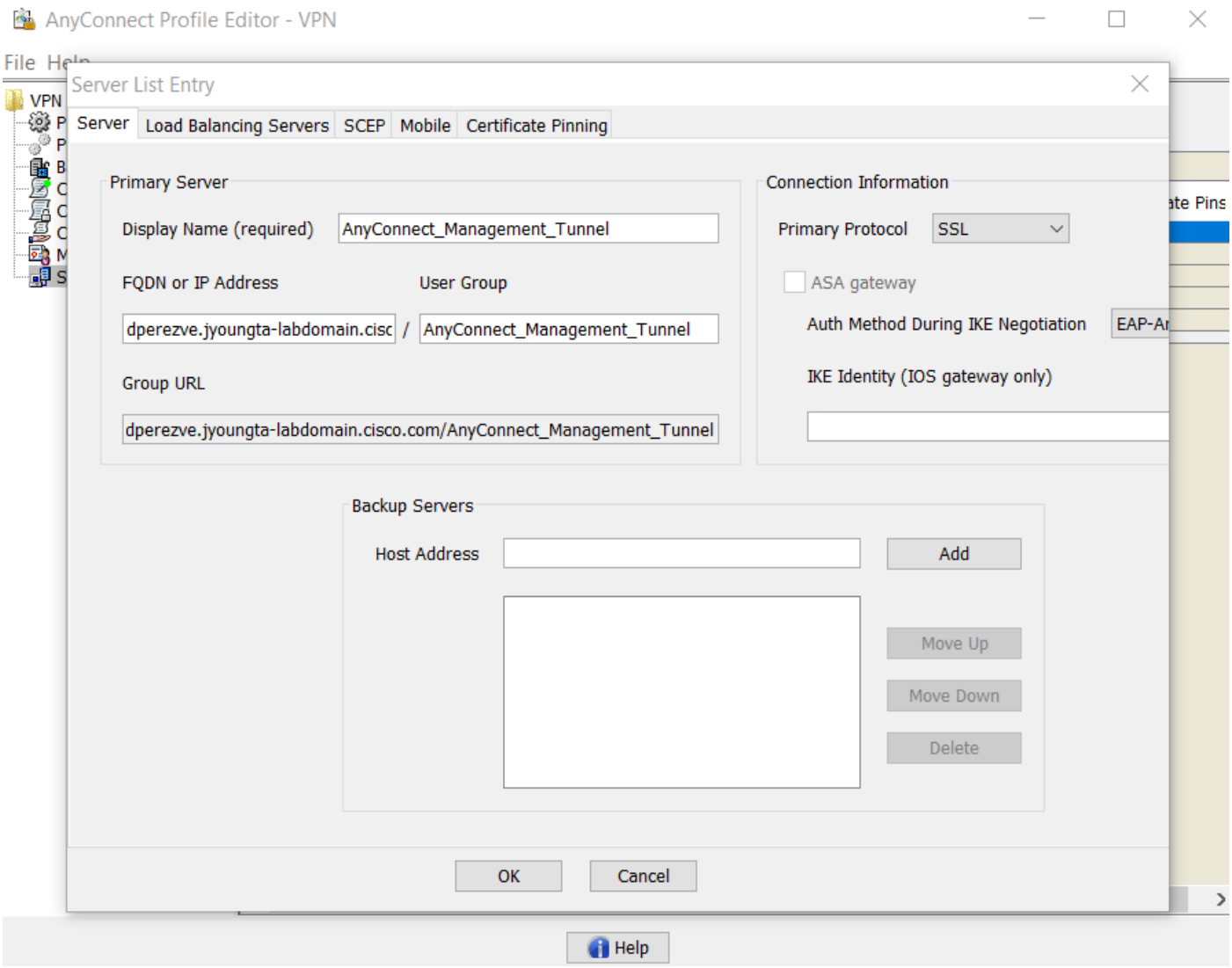
コンフィギュレーション

ステップ 1：AnyConnect管理VPNプロファイルの作成

AnyConnect管理VPNプロファイルを作成するには、AnyConnectプロファイルエディタを開きます。管理プロファイルには、エンドポイントのブートアップ後にVPNトンネルを確立するために使用されるすべての設定が含まれています。

この例では、完全修飾ドメイン名(FQDN)dperezve.jyoungta-labdomain.cisco.comを指すサーバリストエントリが定義され、プライマリプロトコルとしてSSLが選択されます。サーバリストを追加するには、サーバリストに移動し、追加ボタンを選択します。必須フィールドに入力し、変更

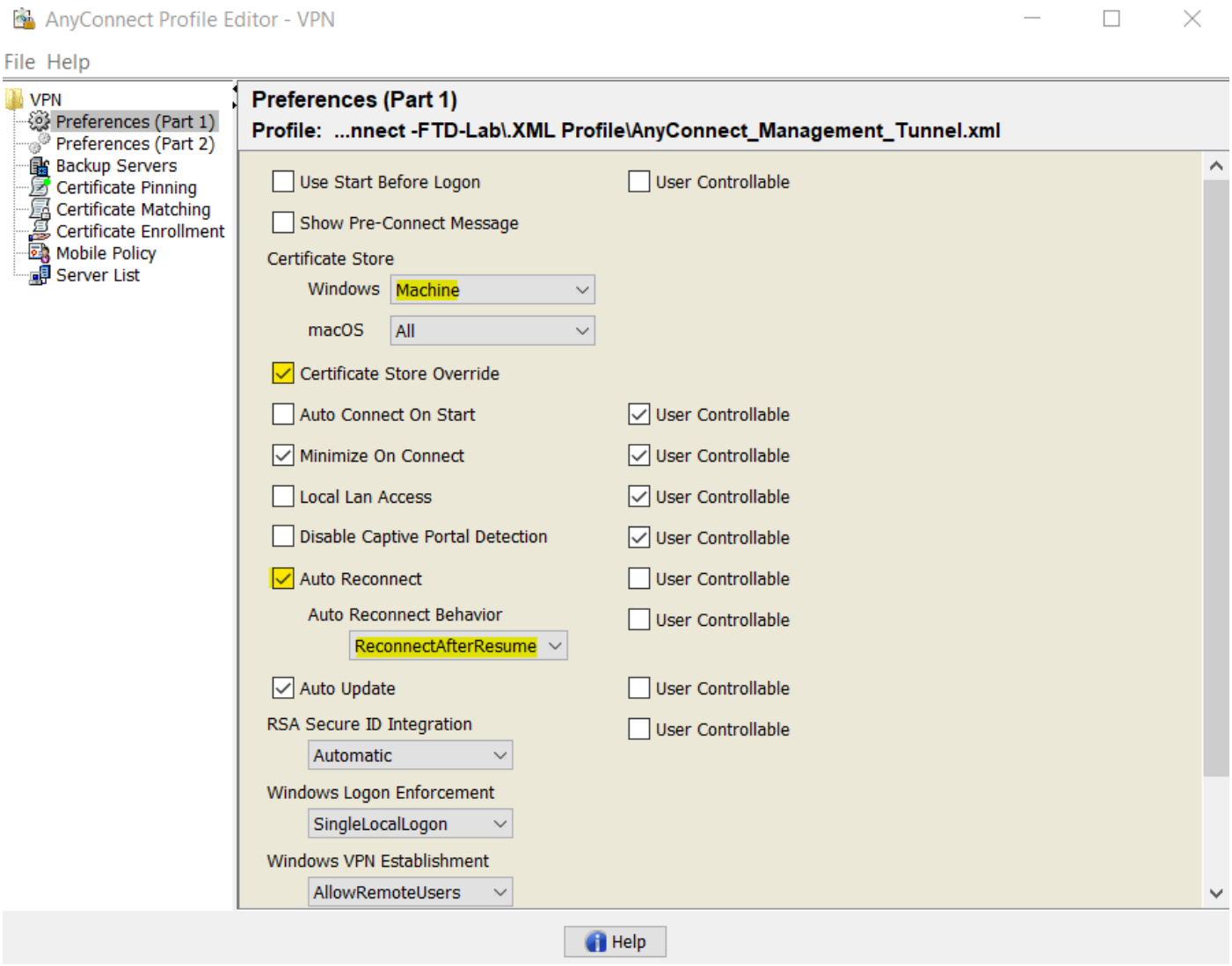
を保存します。



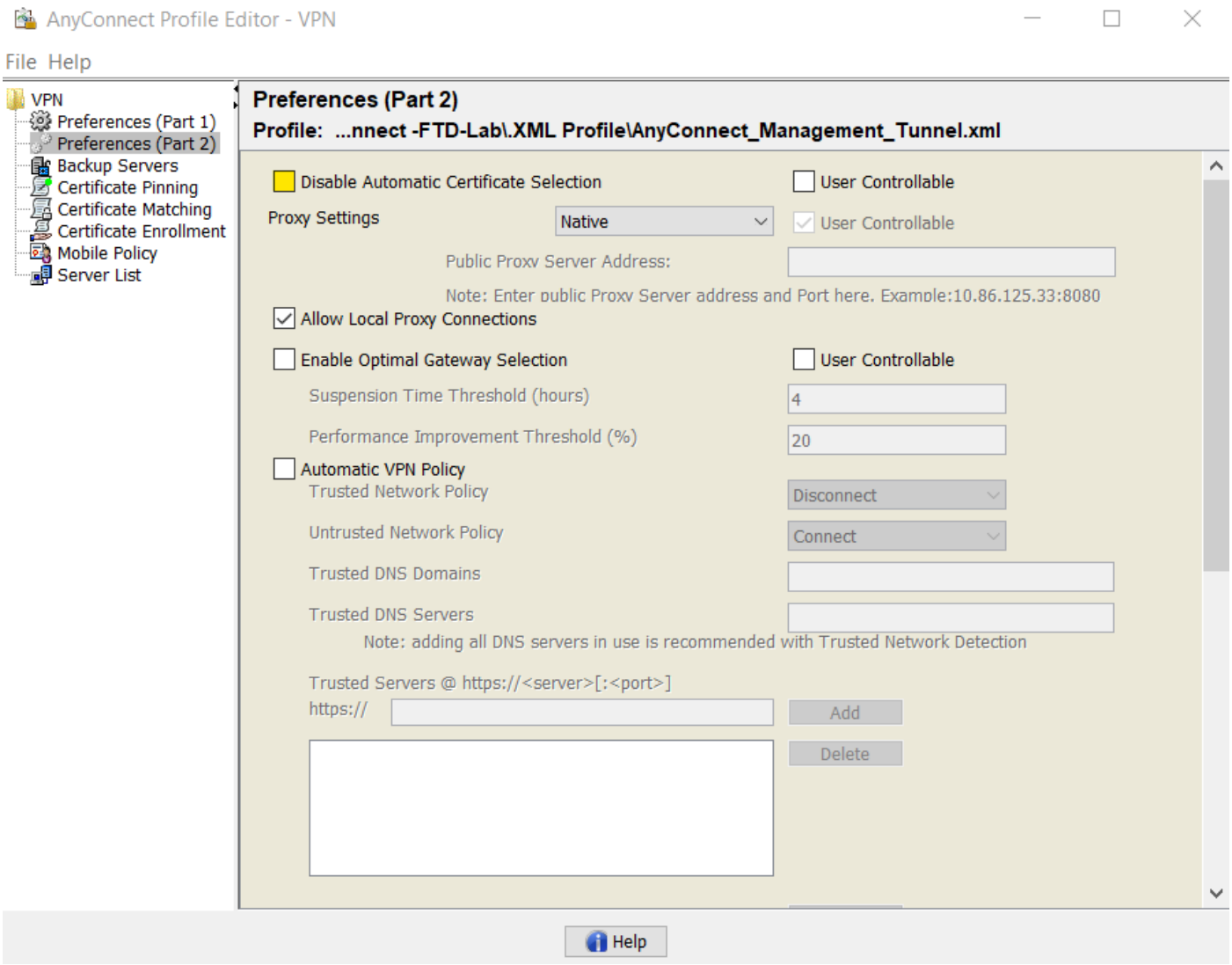
管理VPNプロファイルには、サーバリストに加えて、次の必須設定が含まれている必要があります。

- AutomaticCertSelectionをtrueに設定する必要があります。
- AutoReconnectをtrueに設定する必要があります。
- AutoReconnectBehaviorをReconnectAfterResume用に構成する必要があります。
- AutoUpdateをfalseに設定する必要があります。
- BlockUntrustedServersをtrueに設定する必要があります。
- CertificateStoreをMachineStore用に構成する必要があります。
- CertificateStoreOverrideをtrueに設定する必要があります。
- EnableAutomaticServerSelectionをfalseに設定する必要があります。
- EnableScriptingをfalseに設定する必要があります。
- RetainVPNOnLogoffはtrueに設定する必要があります。

AnyConnect Profile Editorで、Preferences(Part 1)に移動し、次のように設定を調整します。



次に、Preferences(Part 2)に移動し、Disable Automatic Certificate Selectionオプションのチェックマークを外します。



ステップ 2：AnyConnect VPNプロファイルの作成

管理VPNプロファイルに加えて、通常のAnyConnect VPNプロファイルを設定する必要があります。AnyConnect VPNプロファイルは、最初の接続試行で使用されます。このセッション中に、管理VPNプロファイルがFTDからダウンロードされます。

AnyConnect VPNプロファイルを作成するには、AnyConnect Profile Editorを使用します。この場合、両方のファイルに同じ設定が含まれているため、同じ手順を実行できます。

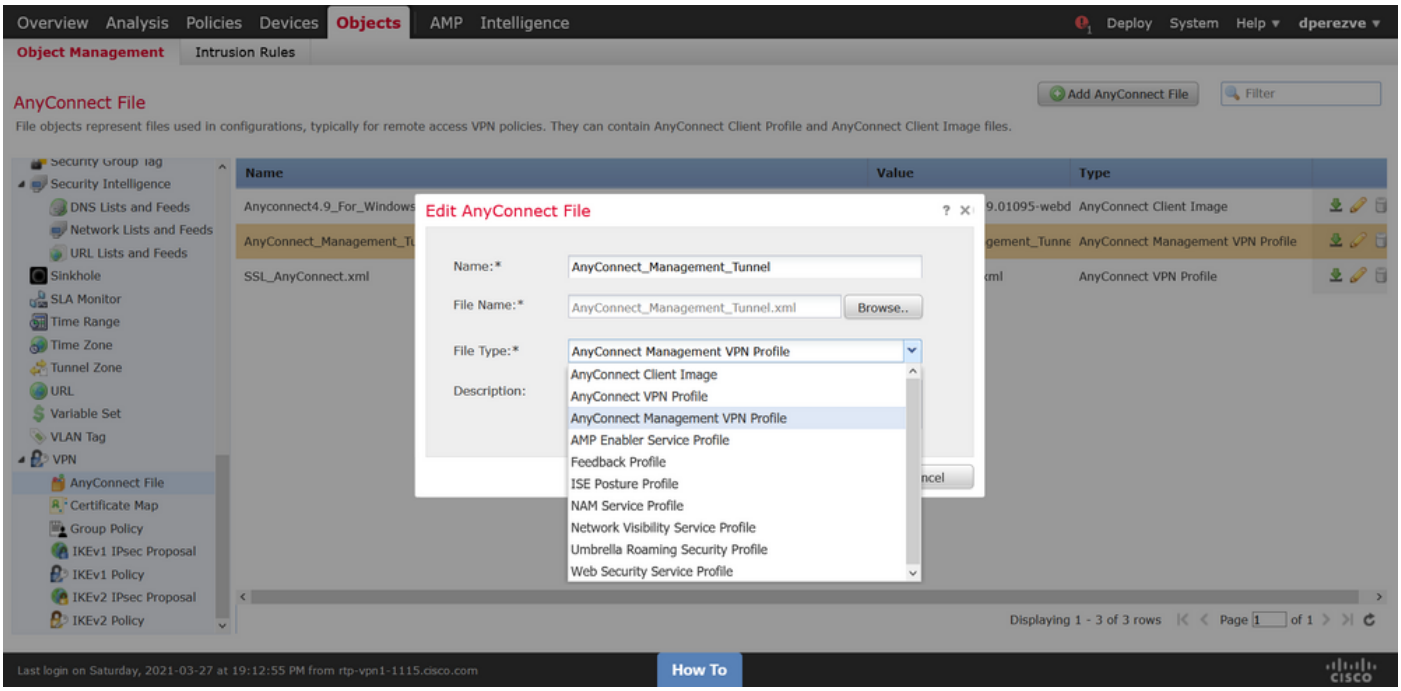
ステップ 3：AnyConnect管理VPNプロファイルおよびAnyConnect VPNプロファイルのFMCへのアップロード

プロファイルが作成されたら、次の手順でプロファイルをAnyConnectファイルオブジェクトとしてFMCにアップロードします。

新しいAnyConnect Management VPN ProfileをFMCにアップロードするには、Objects > Object Managementの順に移動し、目次からVPNオプションを選択してから、Add AnyConnect Fileボタンを選択します。

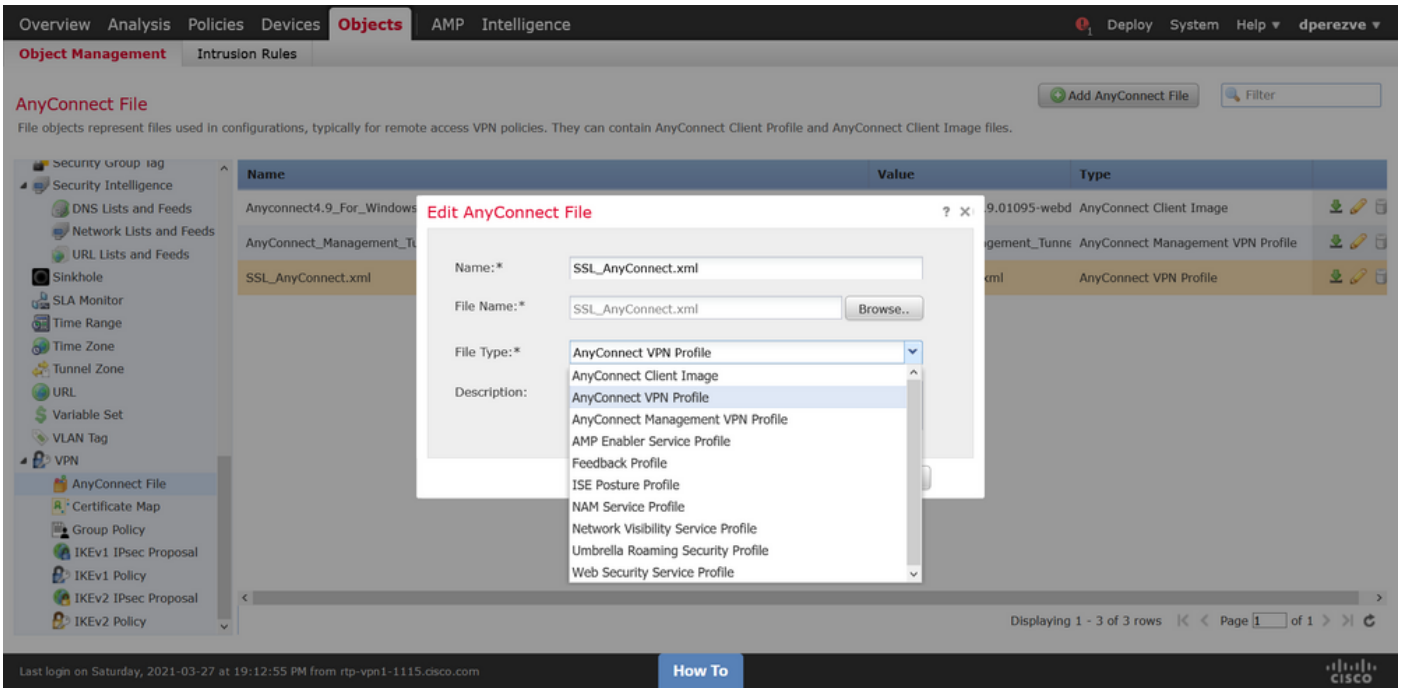
ファイルの名前を指定します。ファイルタイプとしてAnyConnect Management VPN Profileを選

択し、オブジェクトを保存します。

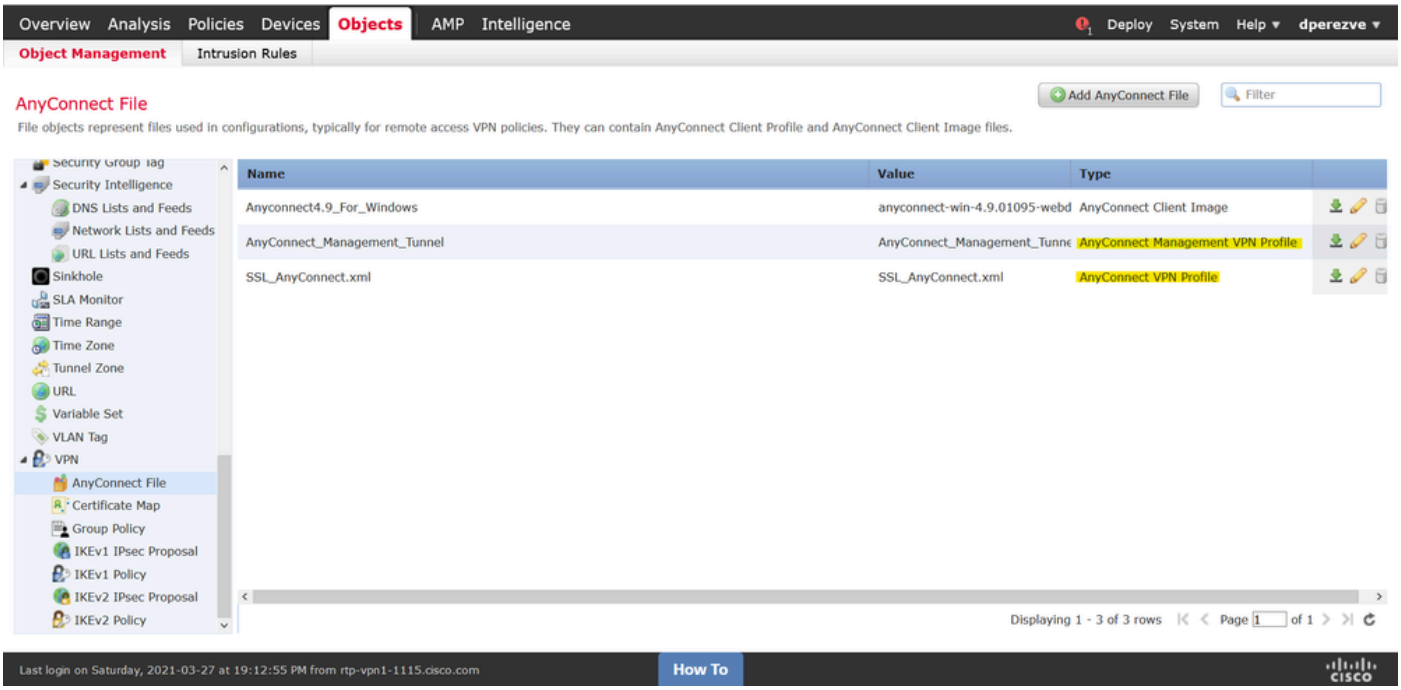


AnyConnect VPNプロファイルをアップロードするには、再度Objects > Object Managementに移動し、目次からVPNオプションを選択してから、Add AnyConnect Fileボタンを選択します。

ファイルの名前を指定しますが、ここではファイルタイプとしてAnyConnect VPN Profileを選択し、新しいオブジェクトを保存します。



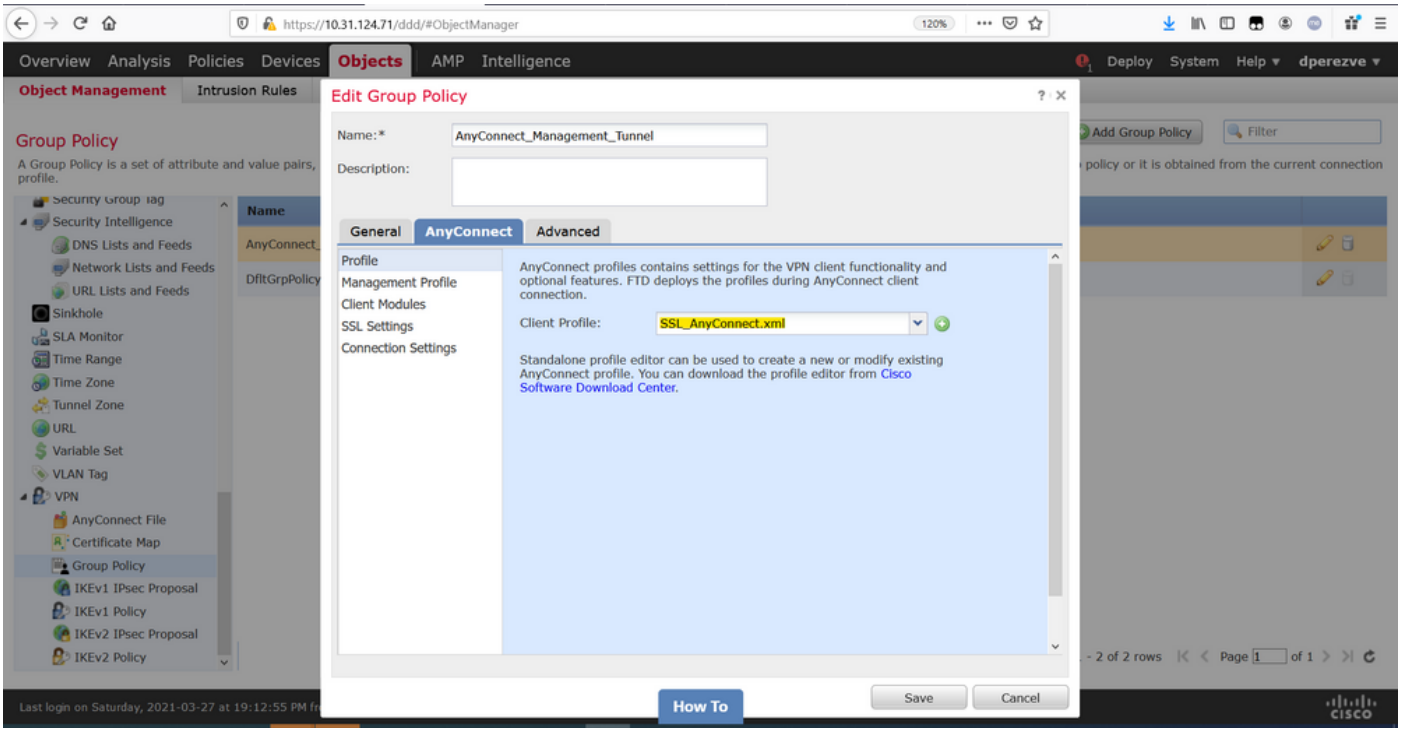
プロファイルをオブジェクトリストに追加し、AnyConnect Management VPN ProfileおよびAnyConnect VPN Profileとしてそれぞれマークする必要があります。



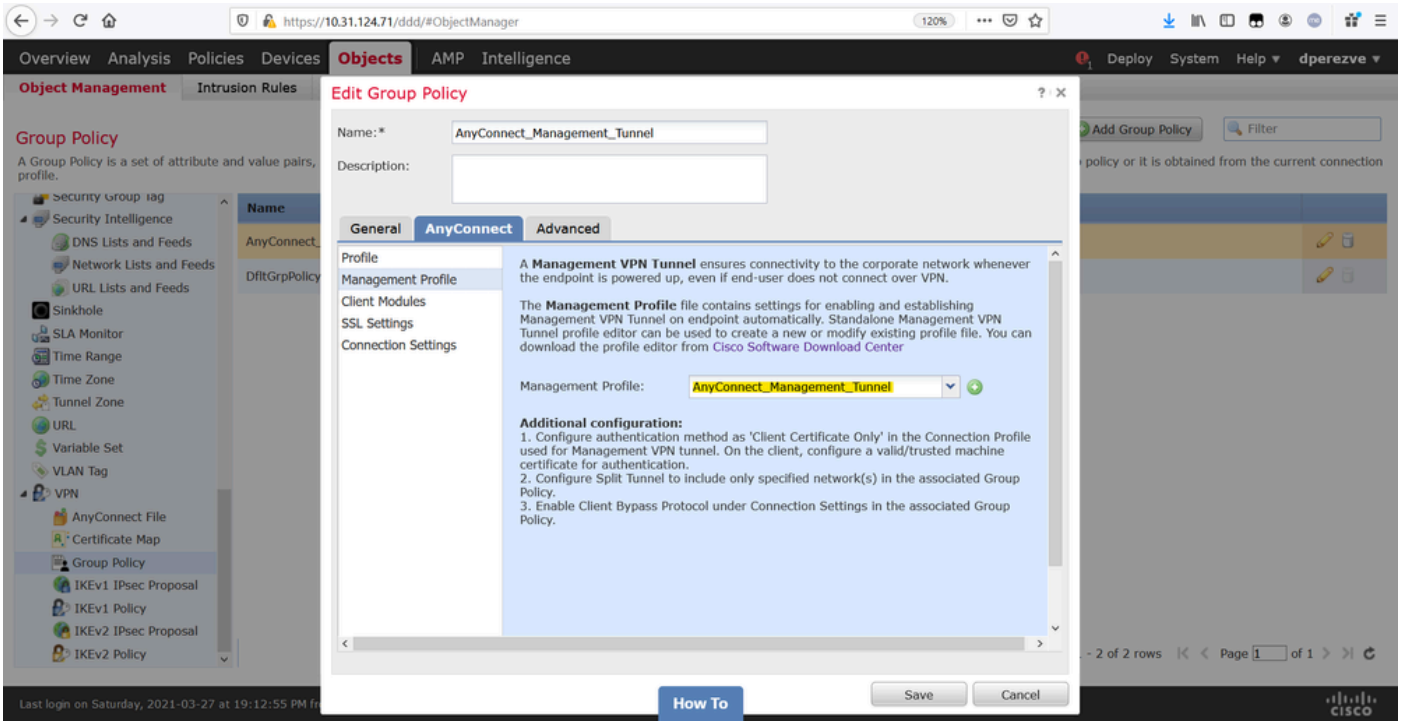
ステップ 4：グループポリシーの作成

新しいグループポリシーを作成するには、Objects > Object Managementに移動し、目次からVPNオプションを選択してから、Group Policyを選択し、Add Group Policyボタンをクリックします。

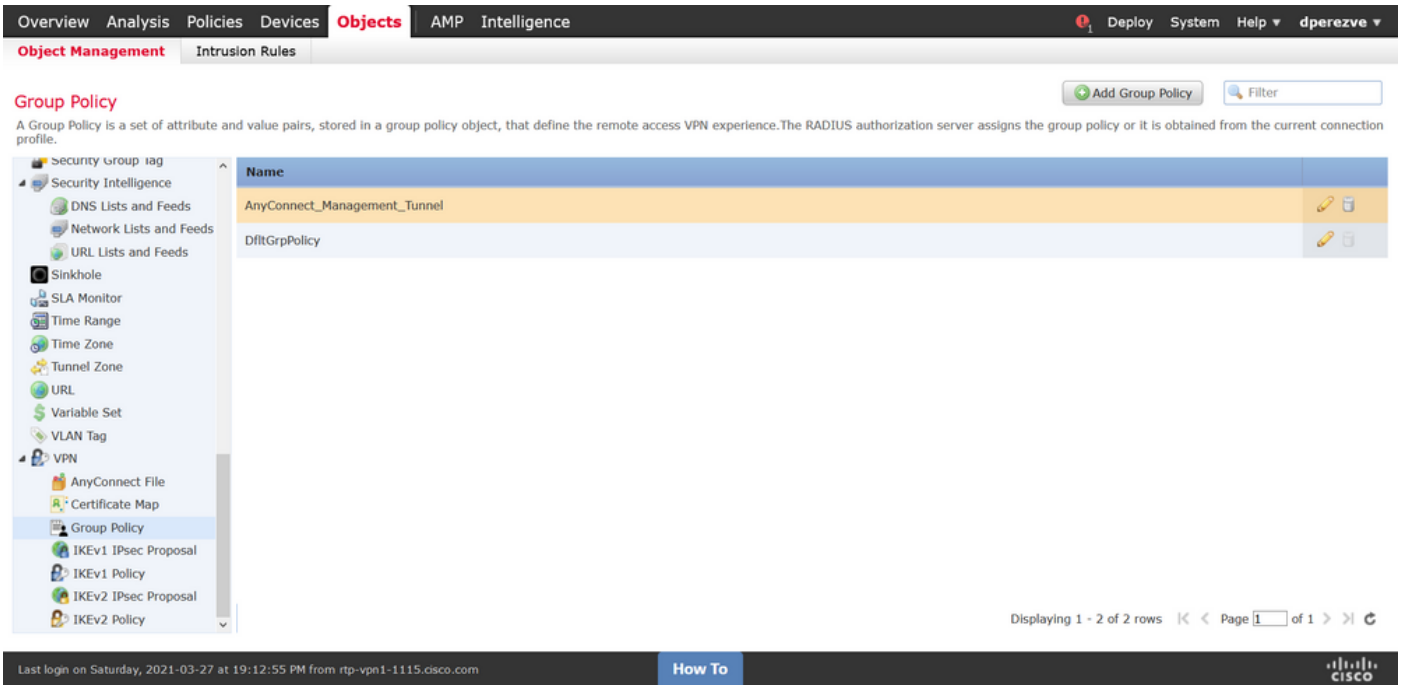
Add Group Policyウィンドウが開いたら、名前を割り当て、AnyConnectプールを定義し、AnyConnectタブを開きます。Profileに移動し、Client Profileドロップダウンメニューで通常のAnyConnect VPNプロファイルを表すオブジェクトを選択します。



次に、Management Profileタブに移動し、Management Profileドロップダウンメニューで Management VPN Profileを含むオブジェクトを選択します。



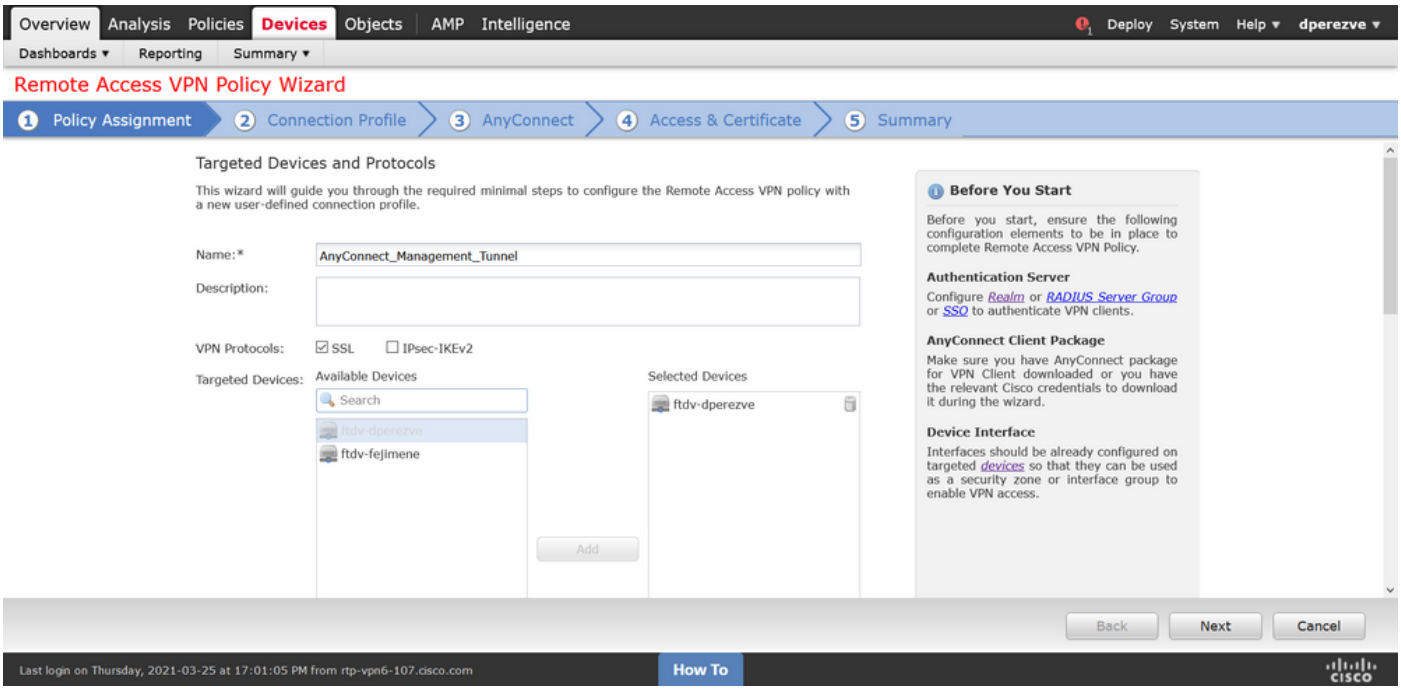
変更を保存して、新しいオブジェクトを既存のグループポリシーに追加します。



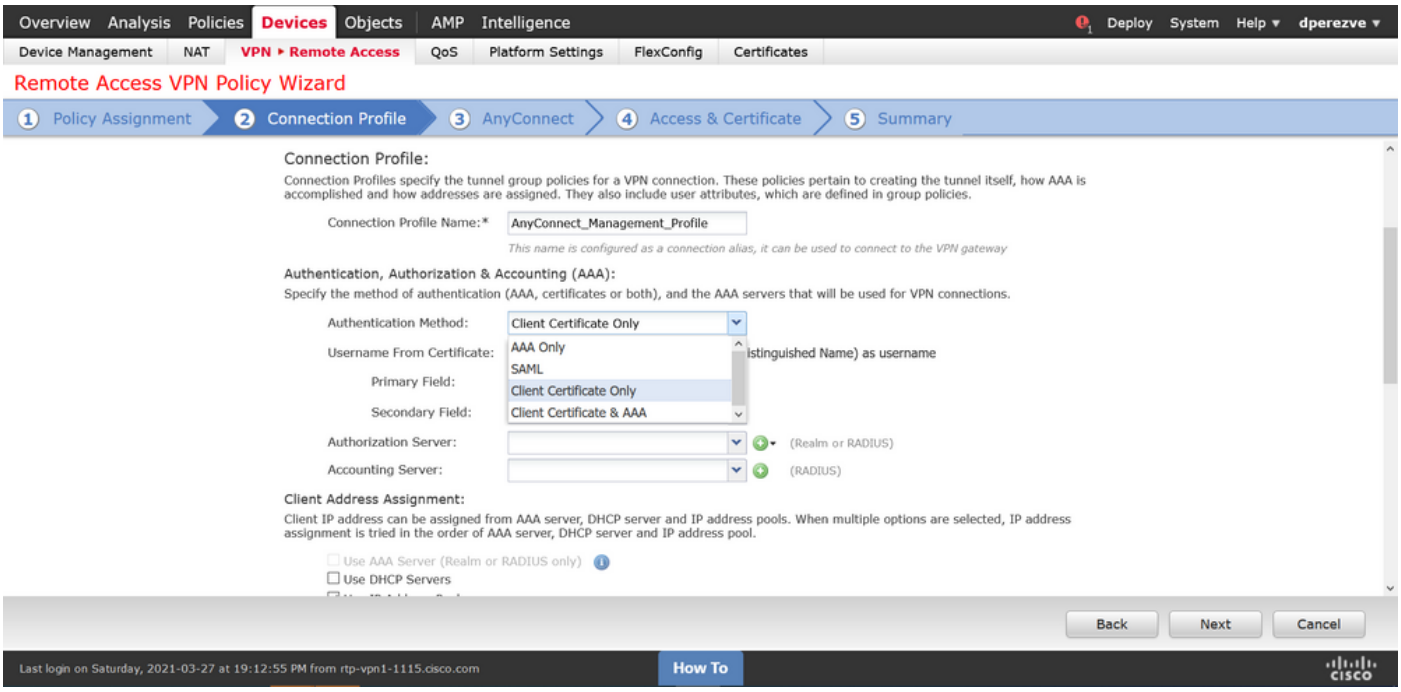
ステップ 5：新しいAnyConnect設定の作成

FMCでのSSL AnyConnectの設定は、4つの異なる手順で構成されます。AnyConnectを設定するには、Devices > VPN > Remote Accessの順に選択し、Addボタンを選択します。これにより、リモートアクセスVPNポリシーウィザードが開きます。

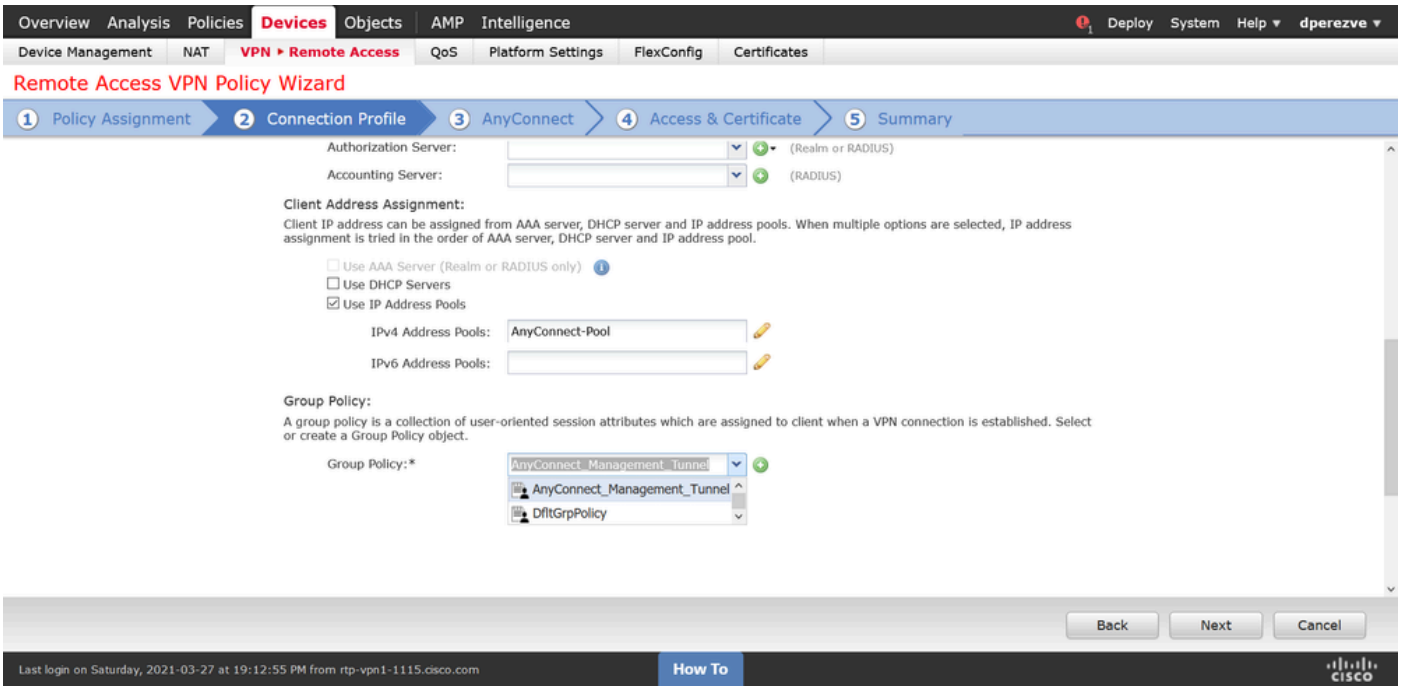
Policy Assignmentタブで、手元にあるFTDデバイスを選択し、接続プロファイルの名前を定義して、SSLチェックボックスをオンにします。



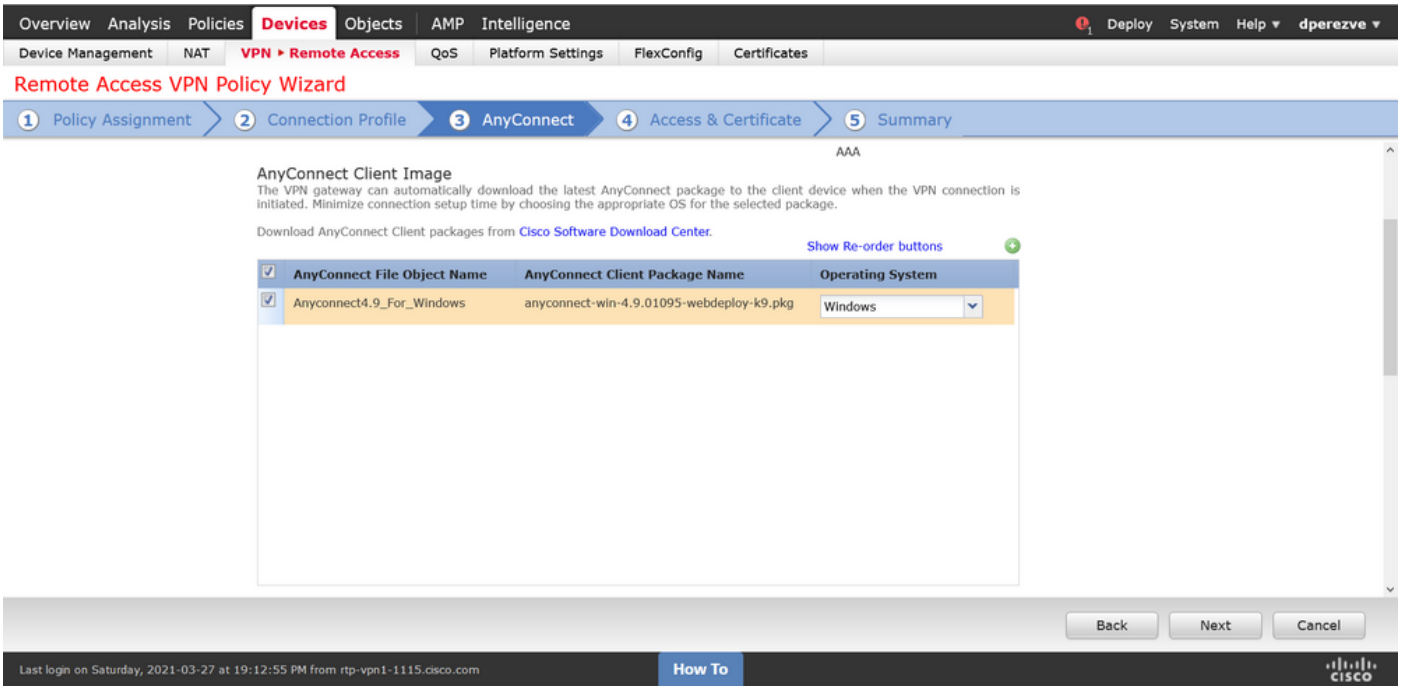
Connection Profileで、認証方式としてClient Certificate Onlyを選択します。これは、この機能でサポートされる唯一の認証です。



次に、ステップ3で作成したグループポリシーオブジェクトをGroup Policyドロップダウンで選択します。



AnyConnectタブで、エンドポイントのオペレーティングシステム(OS)に応じてAnyConnect File Objectを選択します。

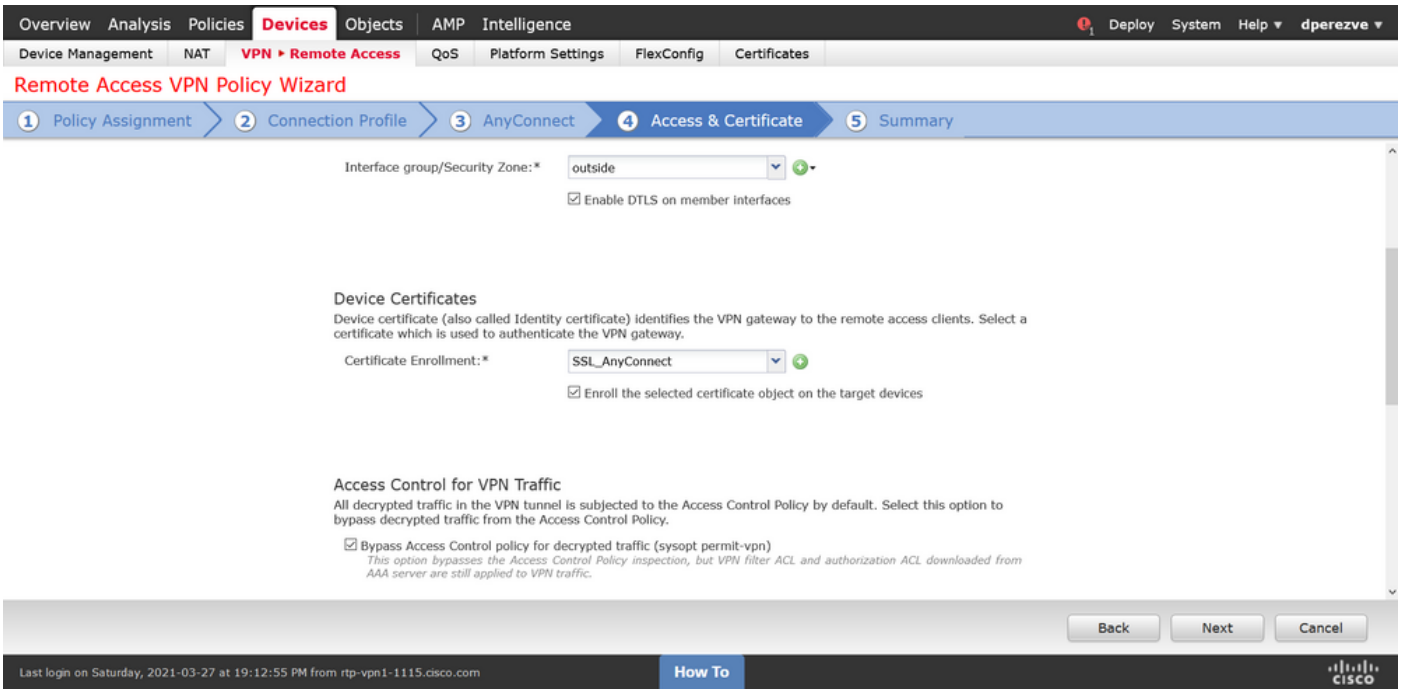


Access & Certificateで、FTDがWindowsクライアントに対してそのIDをプローブするために使用する必要がある証明書を指定します。

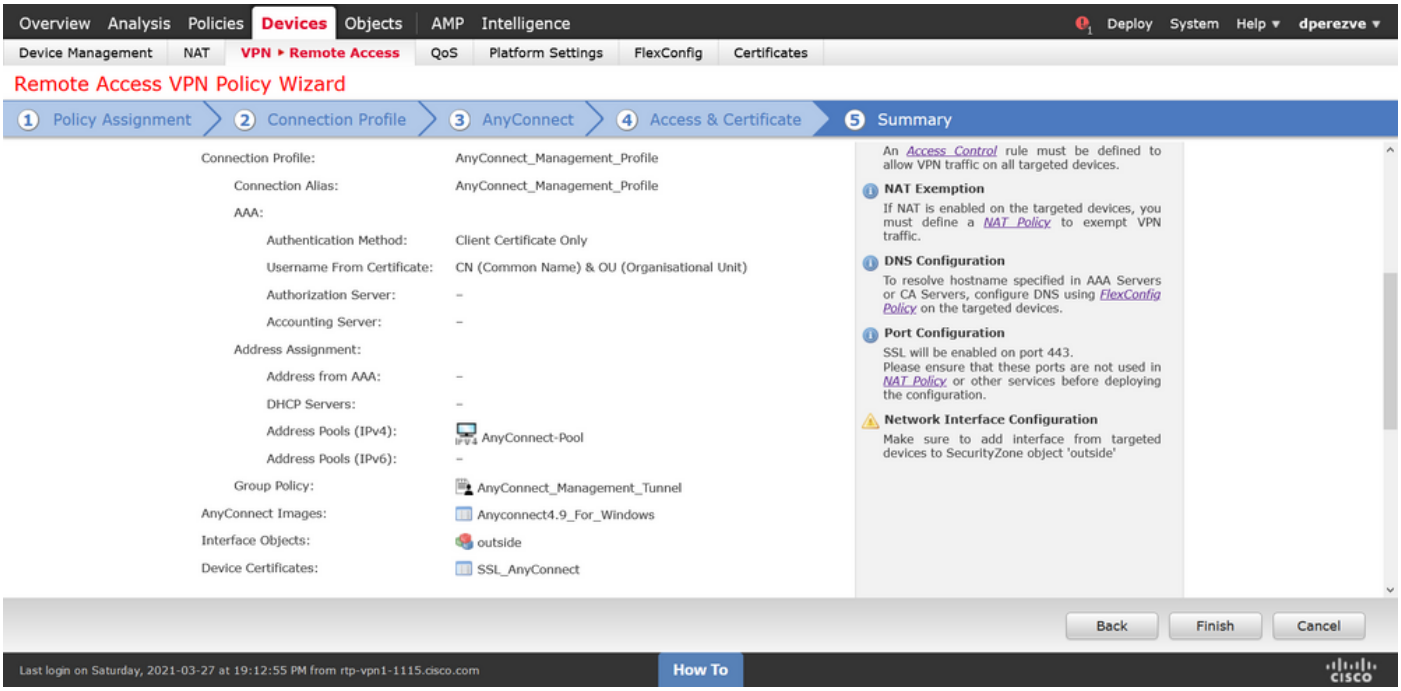
注：ユーザは管理VPN機能を使用する際にAnyConnectアプリケーションと対話できないため、証明書は完全に信頼されている必要があり、警告メッセージを表示してはなりません。

注：証明書の検証エラーを防ぐには、証明書のサブジェクト名に含まれる共通名(CN)フィールドが、XMLプロファイルのサーバリスト（ステップ1およびステップ2）で定義されて

いるFQDNと一致する必要があります。



最後に、SummaryタブでFinishボタンを選択して、新しいAnyConnect設定を追加します。

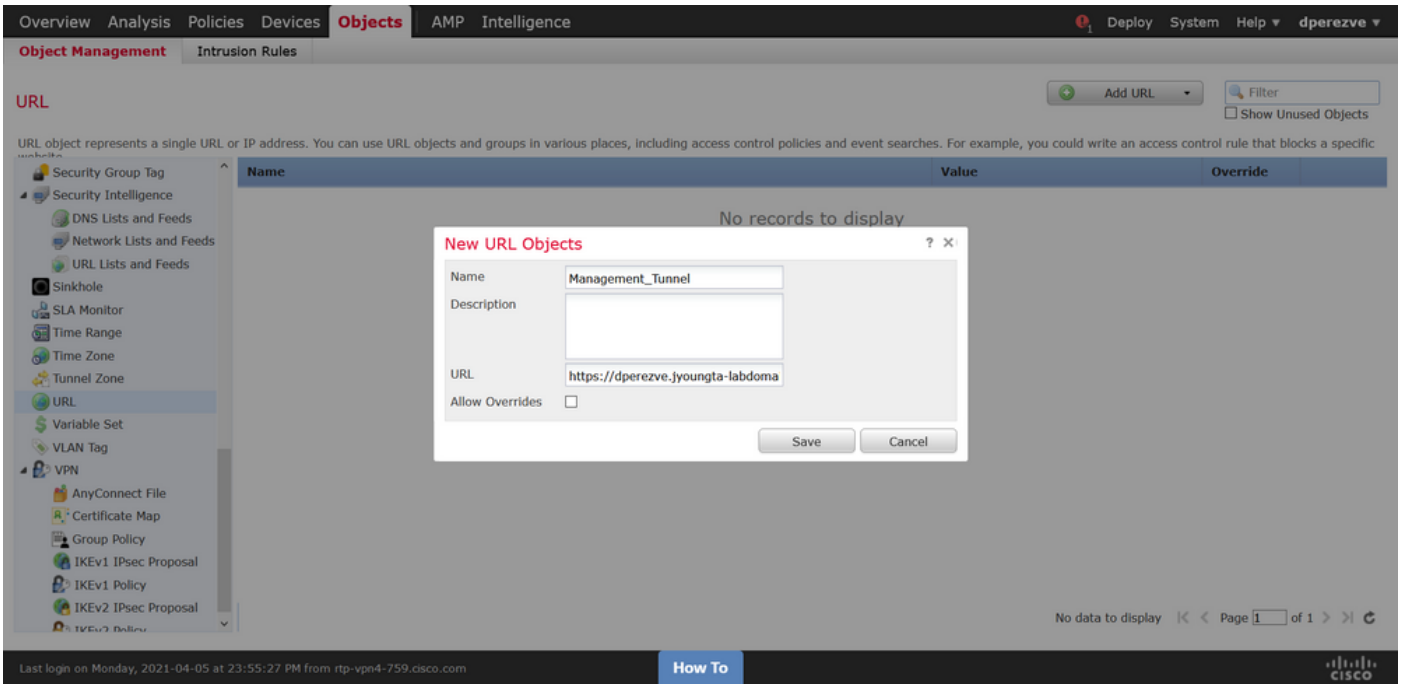


手順 6：URLオブジェクトの作成

Objects > Object Managementの順に移動し、目次からURLを選択します。次に、Add URLドロップダウンでAdd Objectを選択します。

オブジェクトの名前を指定し、管理VPNプロファイルサーバリスト（ステップ2）で指定したのと同じFQDN/ユーザグループを使用してURLを定義します。この例では、URLは dperezve.jyoungta-labdomain.cisco.com/AnyConnect_Management_Tunnelである必要があります

。

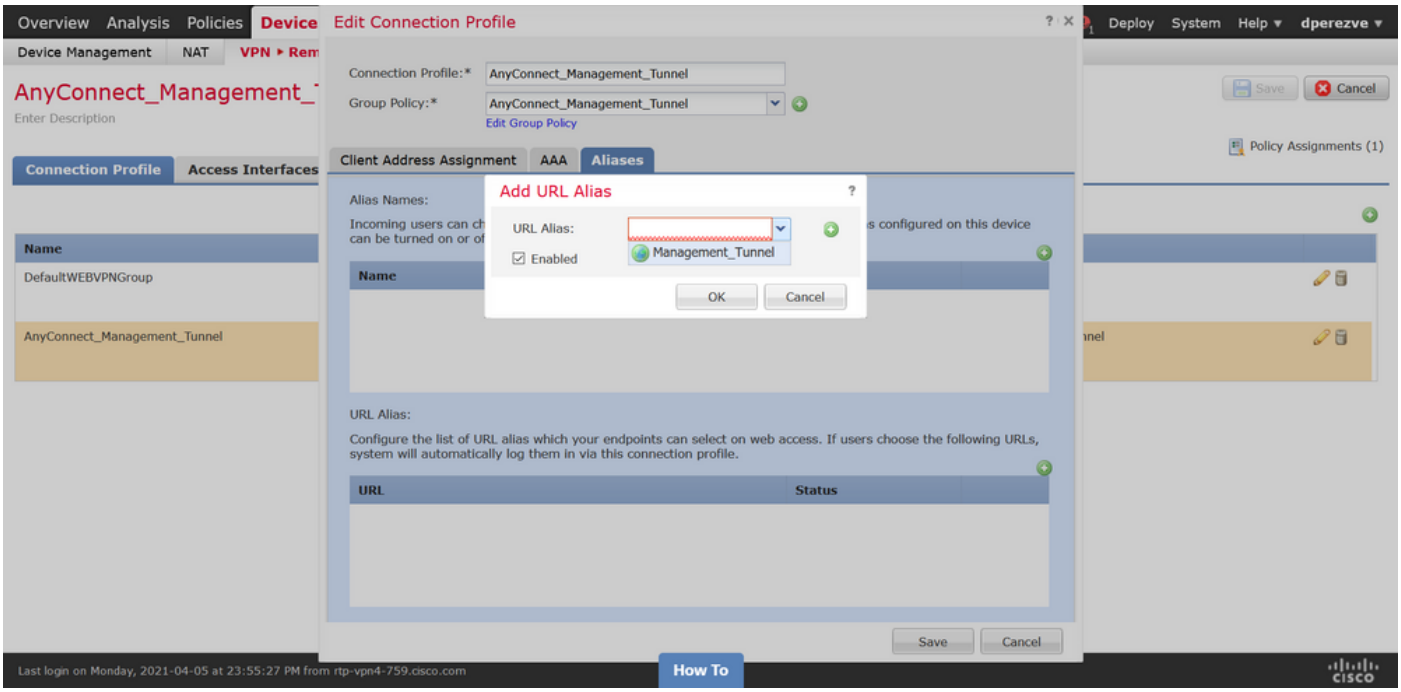


変更を保存して、オブジェクトをオブジェクトリストに追加します。

手順 7：URLエイリアスの定義

AnyConnect設定でURLエイリアスを有効にするには、Devices > VPN > Remote Accessの順に移動し、鉛筆アイコンをクリックして編集します。

次に、Connection Profileタブで手元の設定を選択し、Aliasesに移動してAddボタンをクリックし、URL Aliasドロップダウンで URL Objectを選択します（図1の矢印Aを参照）。Enabledチェックボックスがオンになっていることを確認します。



変更を保存し、FTDに設定を展開します。

確認

導入が完了したら、AnyConnect VPNプロファイルを使用した最初の手動AnyConnect接続が必要です。この接続中に、管理VPNプロファイルがFTDからダウンロードされ、C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTunに保存されます。この時点から、ユーザの操作なしで、管理VPNプロファイルを介して後続の接続を開始する必要があります。

トラブルシュート

証明書検証エラーの場合：

- 認証局(CA)のルート証明書がFTDにインストールされていることを確認します。
- 同じCAによって署名されたID証明書がWindowsマシンストアにインストールされていることを確認してください。
- CNフィールドが証明書に含まれており、管理VPNプロファイルのサーバリストで定義されているFQDNおよびURL工イリアスで定義されているFQDNと同じであることを確認します。

開始されていない管理トンネルの場合：

- 管理VPNプロファイルがダウンロードされ、C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTunに保存されていることを確認します。
- 管理VPNプロファイルの名前がVpnMgmtTunProfile.xmlであることを確認します。

接続の問題については、DARTバンドルを収集し、詳細な調査を行うためにCisco TACにお問い合わせください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。