Konfigurieren von SSL AnyConnect Management VPN auf FTD

Inhalt

Einführung

Dieses Dokument beschreibt die Konfiguration eines Cisco AnyConnect Management-Tunnels auf einer Cisco FirePOWER Threat Defense (FTD), die vom Cisco FirePOWER Management Center (FMC) verwaltet wird. Im Beispiel unten wird Secure Sockets Layer (SSL) zum Erstellen eines Virtual Private Network (VPN) zwischen FTD und einem Windows 10-Client verwendet.

Mitarbeiter: Daniel Perez Vertti Vazquez, Cisco TAC Engineer.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco AnyConnect Profile Editor
- SSL AnyConnect-Konfiguration über FMC
- Client-Zertifikatsauthentifizierung

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco FTD Version 6.7.0 (Build 65)
- Cisco FMC Version 6.7.0 (Build 65)
- Auf dem Windows 10-Computer installierter Cisco AnyConnect 4.9.01095

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Ab Version 6.7 unterstützt Cisco FTD die Konfiguration von AnyConnect Management-Tunneln. Dadurch wird der zuvor geöffnete Verbesserungsantrag CSCvs78215 behoben.

Die AnyConnect Management-Funktion ermöglicht die Erstellung eines VPN-Tunnels unmittelbar nach dem Start des Endpunkts. Die Benutzer müssen die AnyConnect-App nicht manuell starten, sobald ihr System hochgefahren ist. Der AnyConnect VPN-Agent-Dienst erkennt die Management-VPN-Funktion und initiiert eine AnyConnect-Sitzung mithilfe des in der Serverliste des AnyConnect Management VPN-Profils definierten Host Entry.

Einschränkungen

- Es wird nur die Client-Zertifikatsauthentifizierung unterstützt.
- Für Windows-Clients wird nur der Machine Certificate Store unterstützt.
- Wird vom Cisco FirePOWER Device Manager (FDM) CSCvx90058 nicht unterstützt.
- Nicht unterstützt auf Linux-Clients.

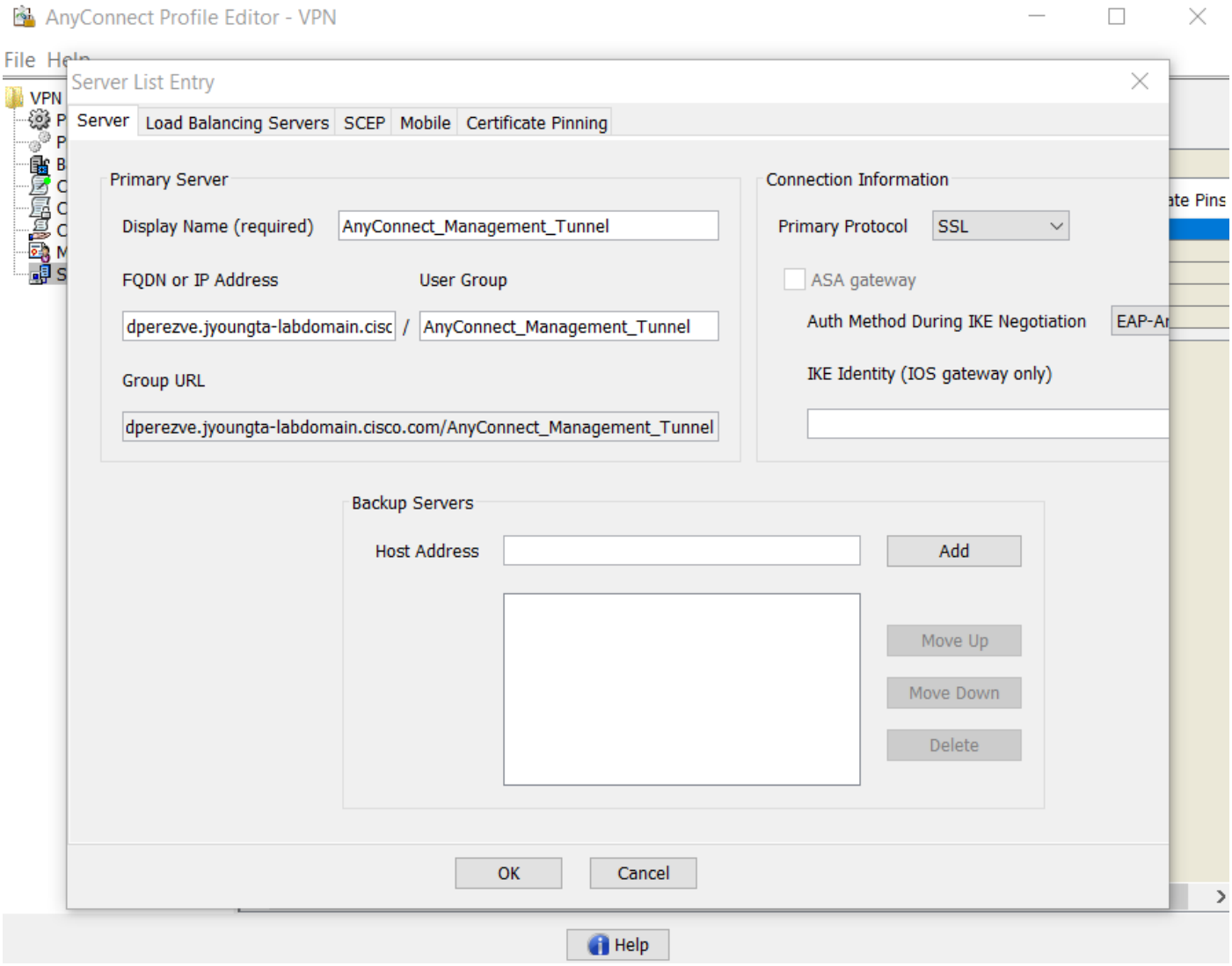
Konfiguration

Konfigurationen

Schritt 1: AnyConnect Management VPN-Profil erstellen

Öffnen Sie den AnyConnect Profile Editor, um ein AnyConnect Management VPN-Profil zu erstellen. Das Verwaltungsprofil enthält alle Einstellungen, die zum Einrichten des VPN-Tunnels nach dem Hochfahren des Endpunkts verwendet werden.

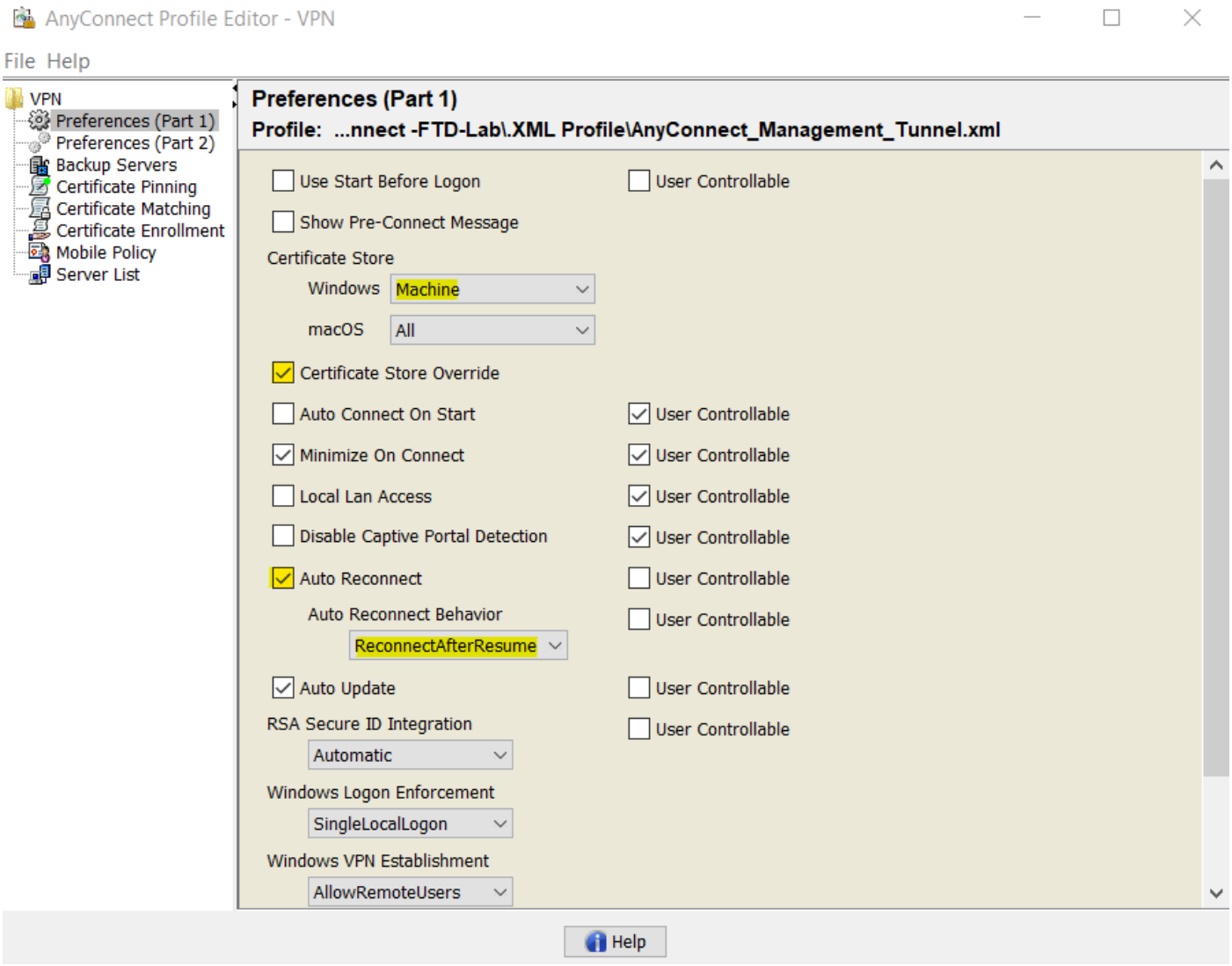
In diesem Beispiel wird ein Server List-Eintrag definiert, der auf Fully Qualified Domain Name (FQDN) dperezve.jyoungta-labdomain.cisco.com zeigt, und SSL wird als primäres Protokoll ausgewählt. Um eine Serverliste hinzuzufügen, navigieren Sie zur **Serverliste**, und wählen Sie die Schaltfläche **Hinzufügen aus**, füllen Sie die erforderlichen Felder aus, und speichern Sie die Änderungen.



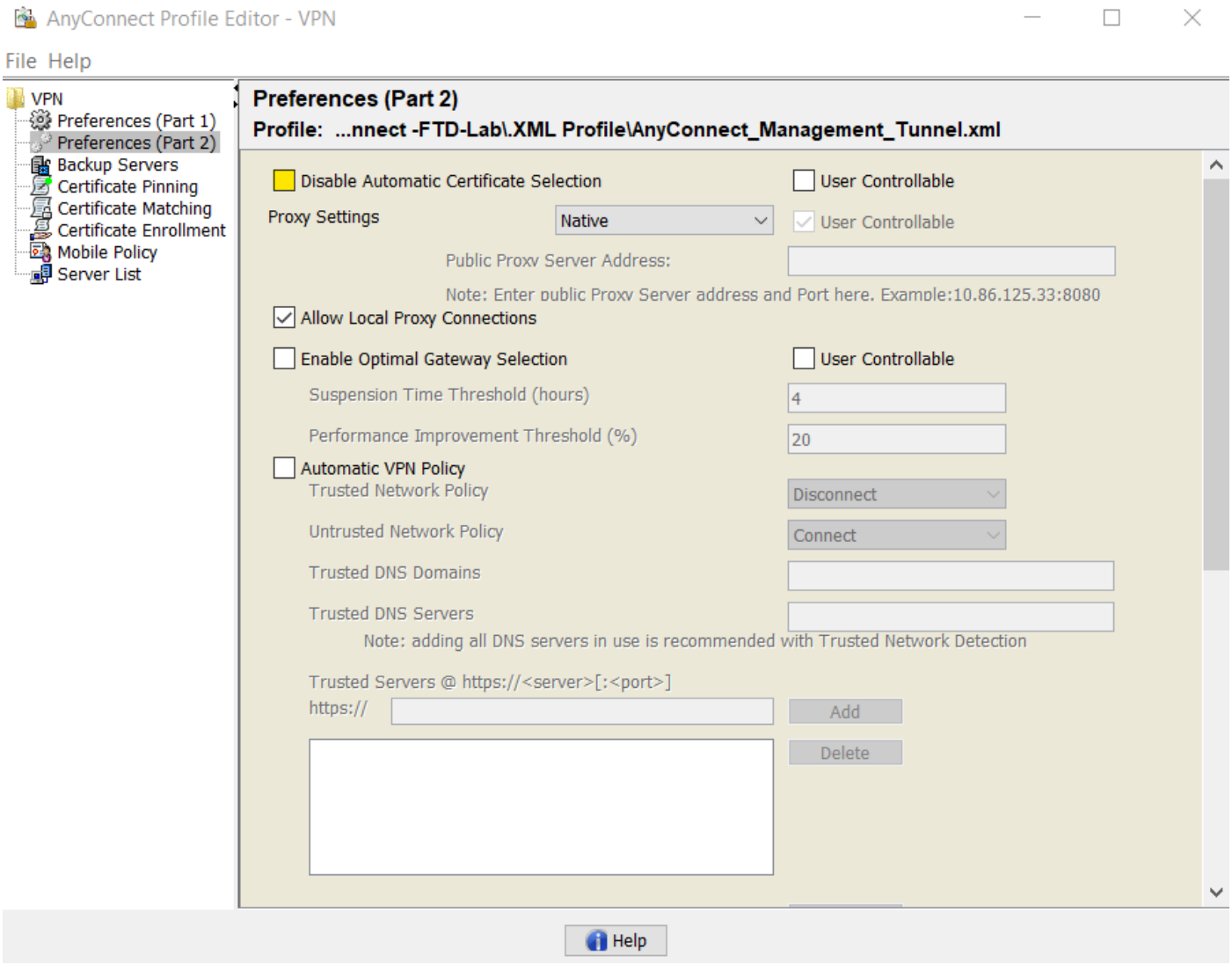
Neben der Serverliste muss das Management-VPN-Profil einige erforderliche Voreinstellungen enthalten:

- **AutomaticCertSelection** muss auf **true** festgelegt werden.
- **AutoReconnect** muss auf **true** eingestellt sein.
- **AutoReconnectBehavior** muss für **ReconnectAfterResume** konfiguriert werden.
- **AutoUpdate** muss auf **false** eingestellt sein.
- **BlockUntrustedServers** muss auf **true** festgelegt werden.
- **CertificateStore** muss für **MachineStore** konfiguriert werden.
- **CertificateStoreOverride** muss auf **true** festgelegt werden.
- **EnableAutomaticServerSelection** muss auf **false** festgelegt werden.
- **EnableScripting** muss auf **false** festgelegt werden.
- **RetainVPNOnLogoff** muss auf **true** eingestellt sein.

Navigieren Sie im AnyConnect Profile Editor zu **Voreinstellungen (Teil 1)** und passen Sie die Einstellungen wie folgt an:



Navigieren Sie dann zu **Voreinstellungen (Teil 2),** und deaktivieren Sie die Option **Automatische Zertifikatauswahl deaktivieren**.



Schritt 2: AnyConnect VPN-Profil erstellen

Zusätzlich zum Management-VPN-Profil muss das reguläre AnyConnect VPN-Profil konfiguriert werden. Das AnyConnect VPN-Profil wird beim ersten Verbindungsversuch verwendet. Während dieser Sitzung wird das Management-VPN-Profil von FTD heruntergeladen.

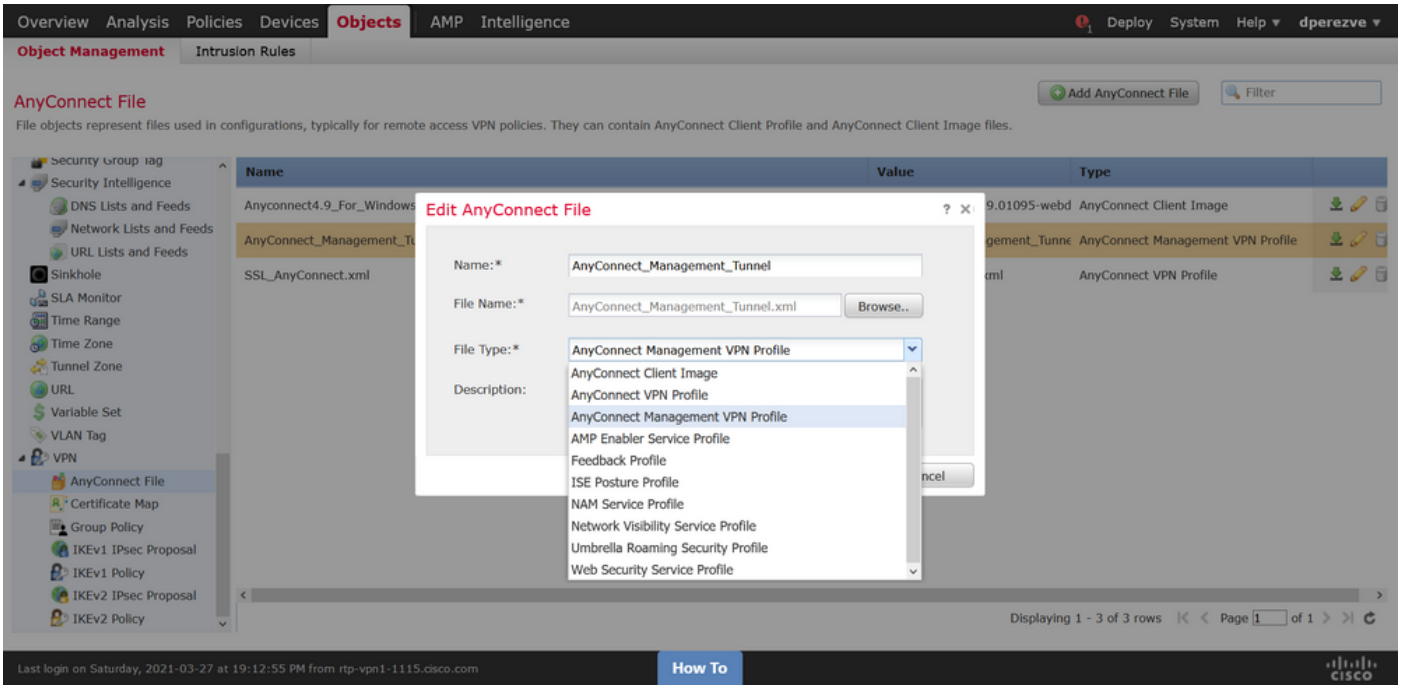
Erstellen Sie das AnyConnect VPN-Profil mit dem AnyConnect Profile Editor. In diesem Fall enthalten beide Dateien die gleichen Einstellungen, sodass das gleiche Verfahren ausgeführt werden kann.

Schritt 3: Laden Sie das AnyConnect Management VPN-Profil und das AnyConnect VPN-Profil auf FMC hoch.

Nachdem die Profile erstellt wurden, werden sie als AnyConnect-Dateiobjekte in das FMC hochgeladen.

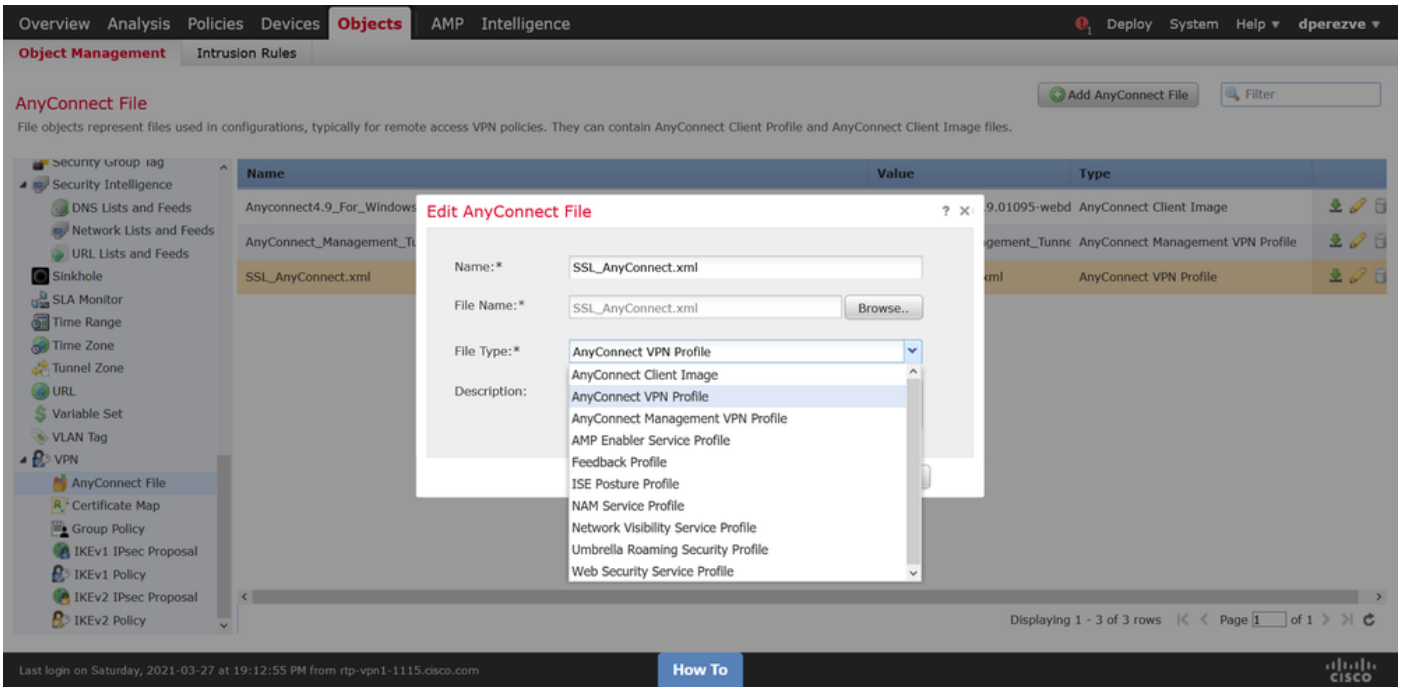
Um das neue AnyConnect Management VPN-Profil in FMC hochzuladen, navigieren Sie zu **Objects > Object Management** und wählen Sie die **VPN-**Option aus dem Inhaltsverzeichnis aus, und wählen Sie dann die Schaltfläche **AnyConnect-Datei hinzufügen aus**.

Geben Sie einen Namen für die Datei an, wählen Sie **AnyConnect Management VPN Profile** als Dateityp aus, und speichern Sie das Objekt.

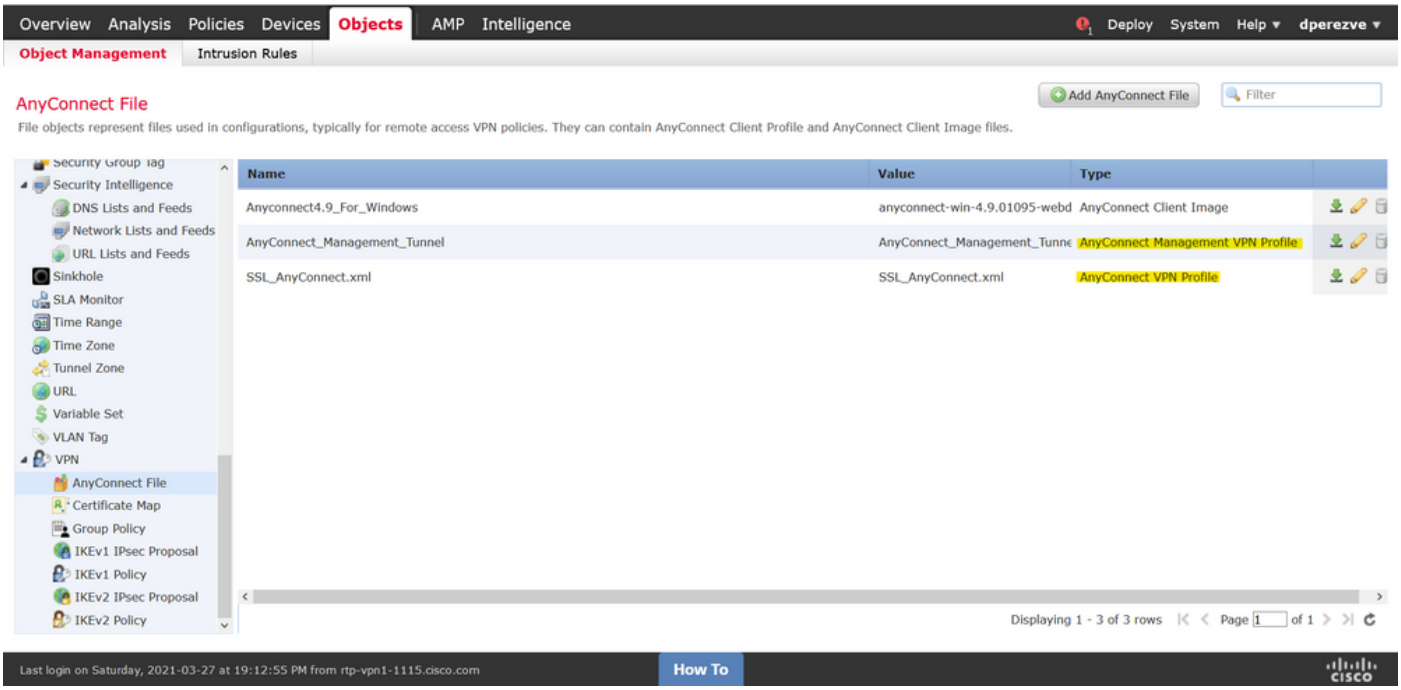


Um das AnyConnect VPN-Profil hochzuladen, navigieren Sie erneut zu **Objects > Object Management** und wählen Sie die **VPN-**Option aus dem Inhaltsverzeichnis aus, und wählen Sie dann die Schaltfläche **AnyConnect-Datei hinzufügen aus**.

Geben Sie einen Namen für die Datei an, wählen Sie jedoch dieses Mal **AnyConnect VPN Profile** als Dateityp aus, und speichern Sie das neue Objekt.



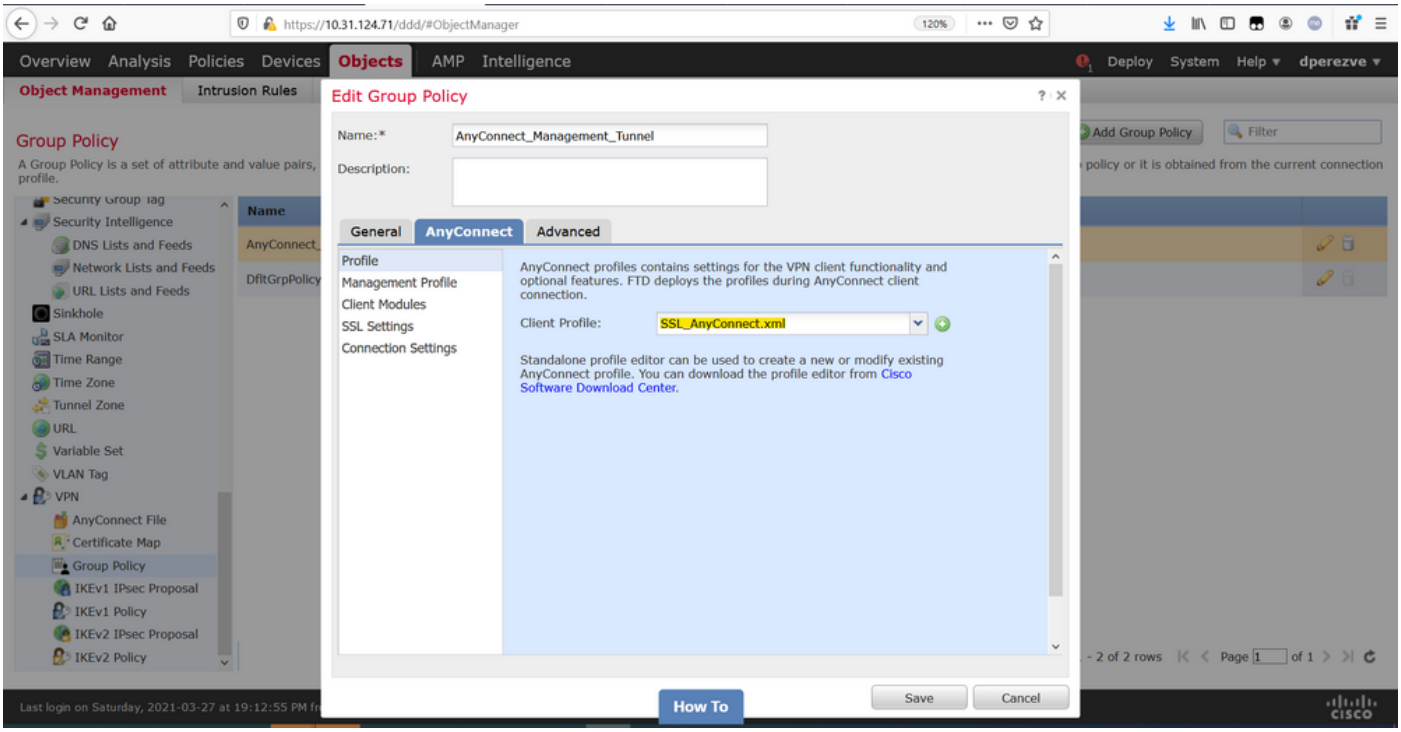
Profile müssen der Objektliste hinzugefügt und als **AnyConnect Management VPN Profile** und **AnyConnect VPN Profile** markiert werden.



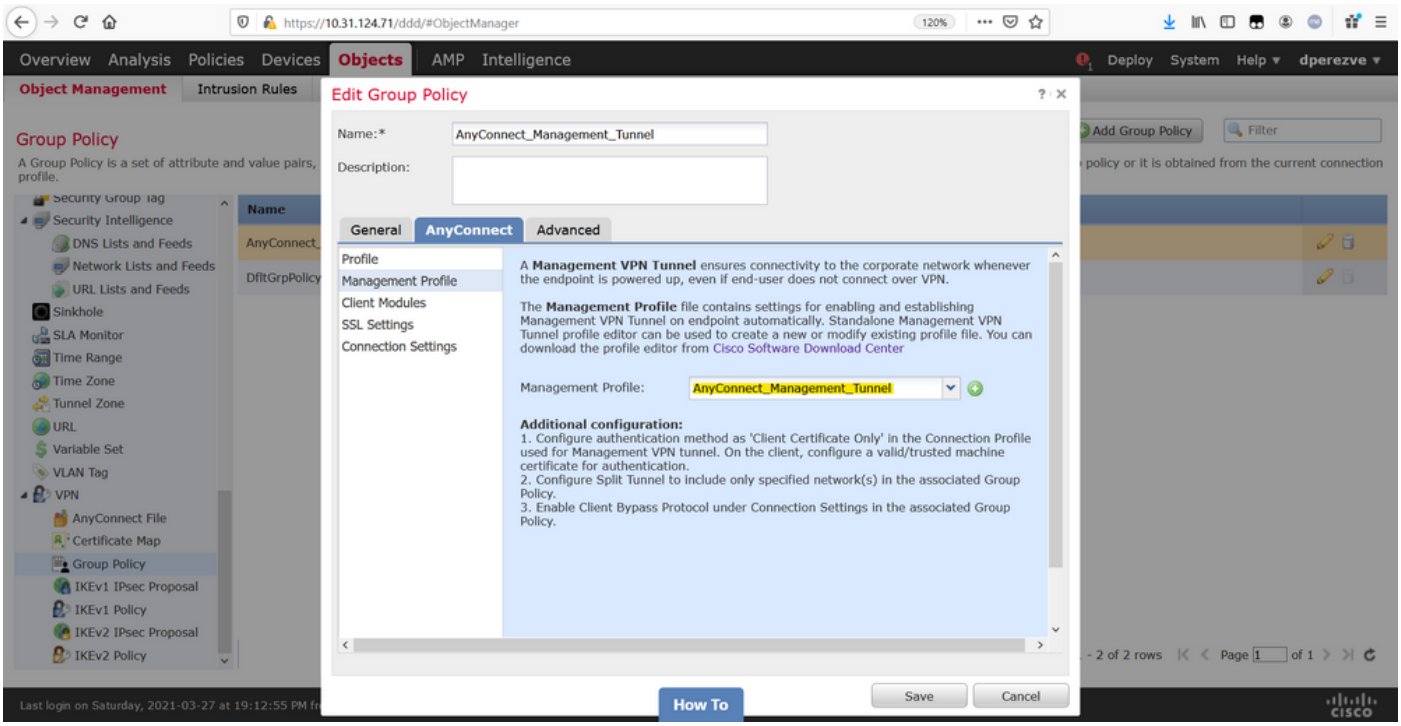
Schritt 4: Gruppenrichtlinie erstellen

Um eine neue Gruppenrichtlinie zu erstellen, navigieren Sie zu **Objects > Object Management** und wählen Sie im Inhaltsverzeichnis die **VPN-**Option aus, wählen Sie dann **Gruppenrichtlinie aus** und klicken Sie auf die Schaltfläche **Gruppenrichtlinie hinzufügen**.

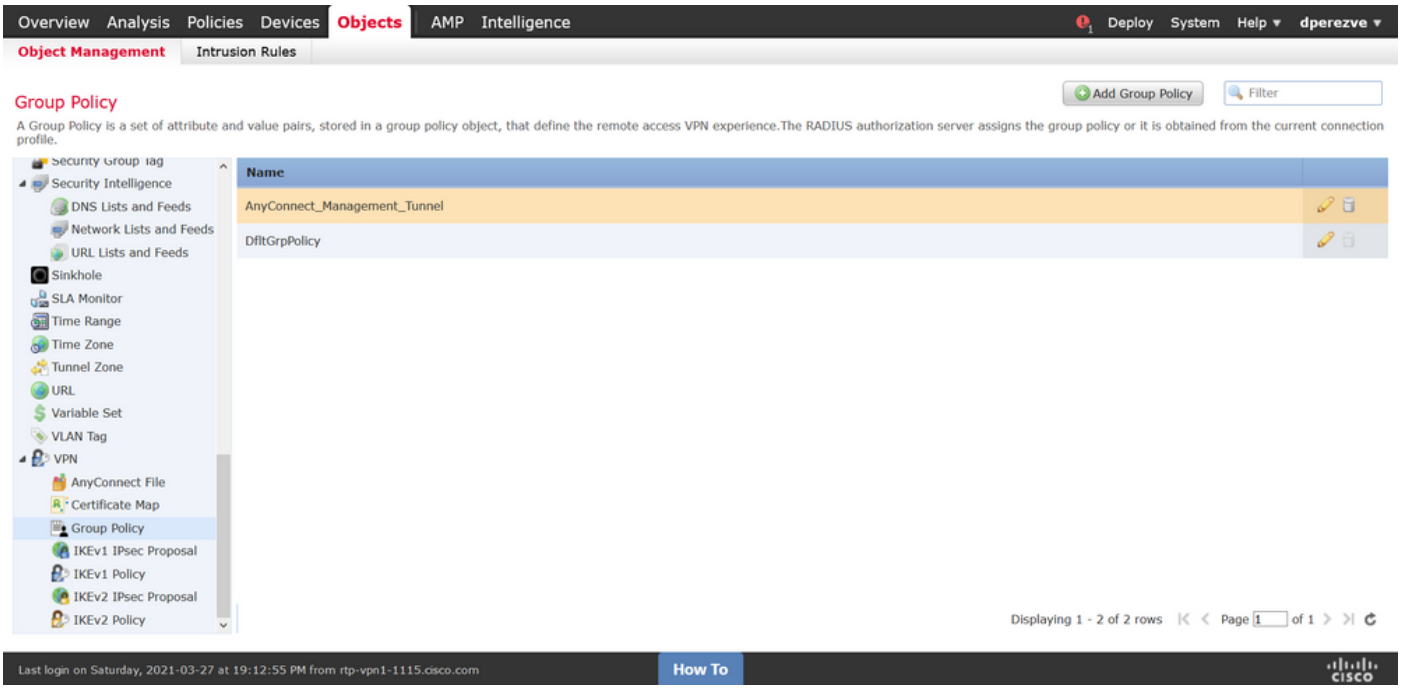
Wenn das Fenster **Gruppenrichtlinie hinzufügen** geöffnet wird, weisen Sie einen Namen zu, definieren Sie einen AnyConnect-Pool, und öffnen Sie die Registerkarte **AnyConnect**. Navigieren Sie zu **Profile**, und wählen Sie im Dropdown-Menü **Client Profile** das Objekt aus, das das reguläre AnyConnect VPN-Profil darstellt.



Navigieren Sie anschließend zur Registerkarte **Management Profile** (**Verwaltungsprofil**), und wählen Sie im Dropdown-Menü für das **Verwaltungsprofil** das Objekt aus, das das Management-VPN-Profil enthält.



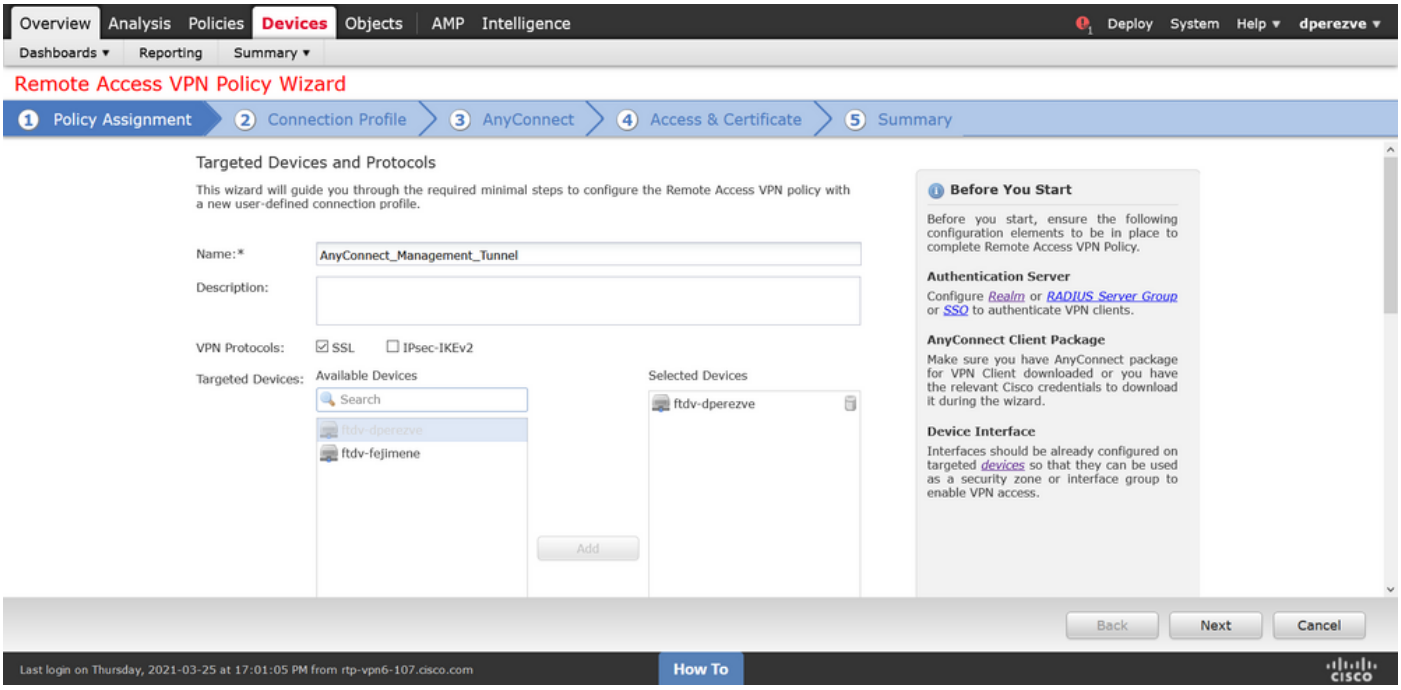
Speichern Sie die Änderungen, um das neue Objekt den vorhandenen Gruppenrichtlinien hinzuzufügen.



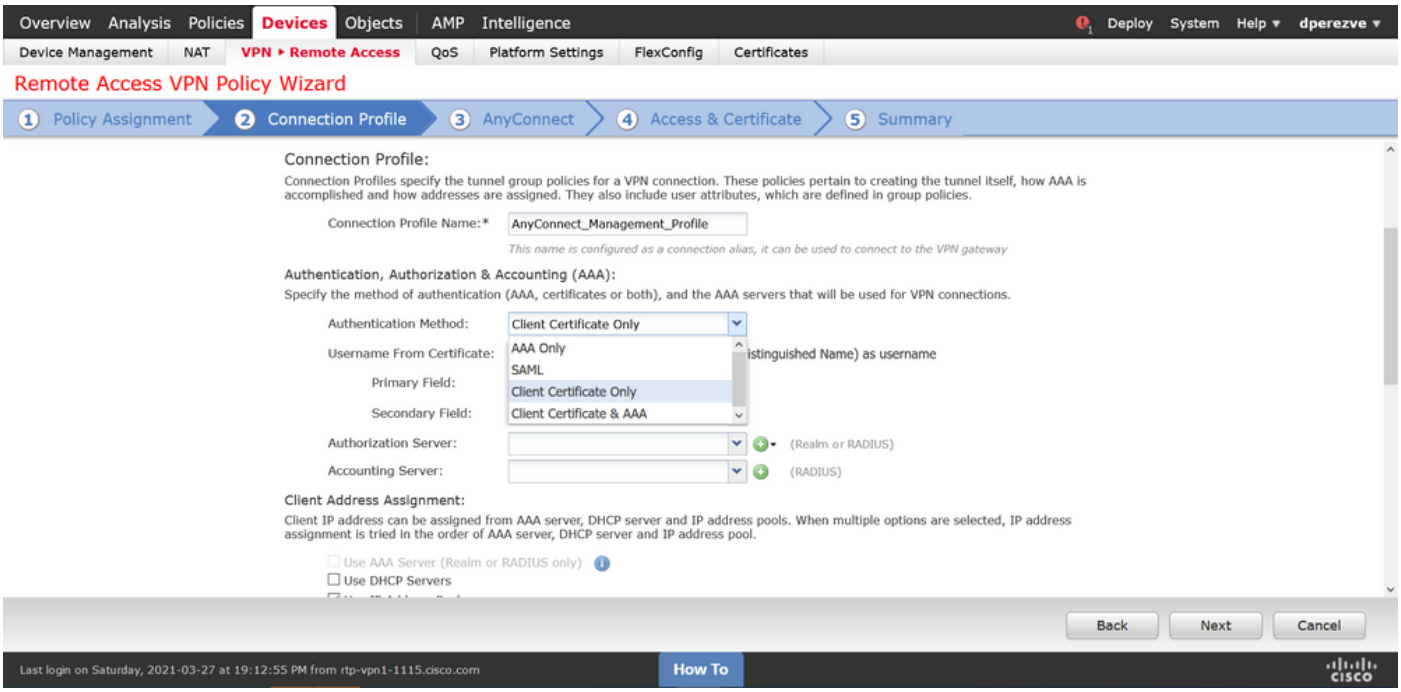
Schritt 5: Neue AnyConnect-Konfiguration erstellen

Die Konfiguration von SSL AnyConnect in FMC umfasst vier verschiedene Schritte. Um AnyConnect zu konfigurieren, navigieren Sie zu **Devices > VPN > Remote Access** und wählen die Schaltfläche **Add (Hinzufügen)** aus. Hiermit muss der **Remote Access VPN Policy Wizard** geöffnet **werden**.

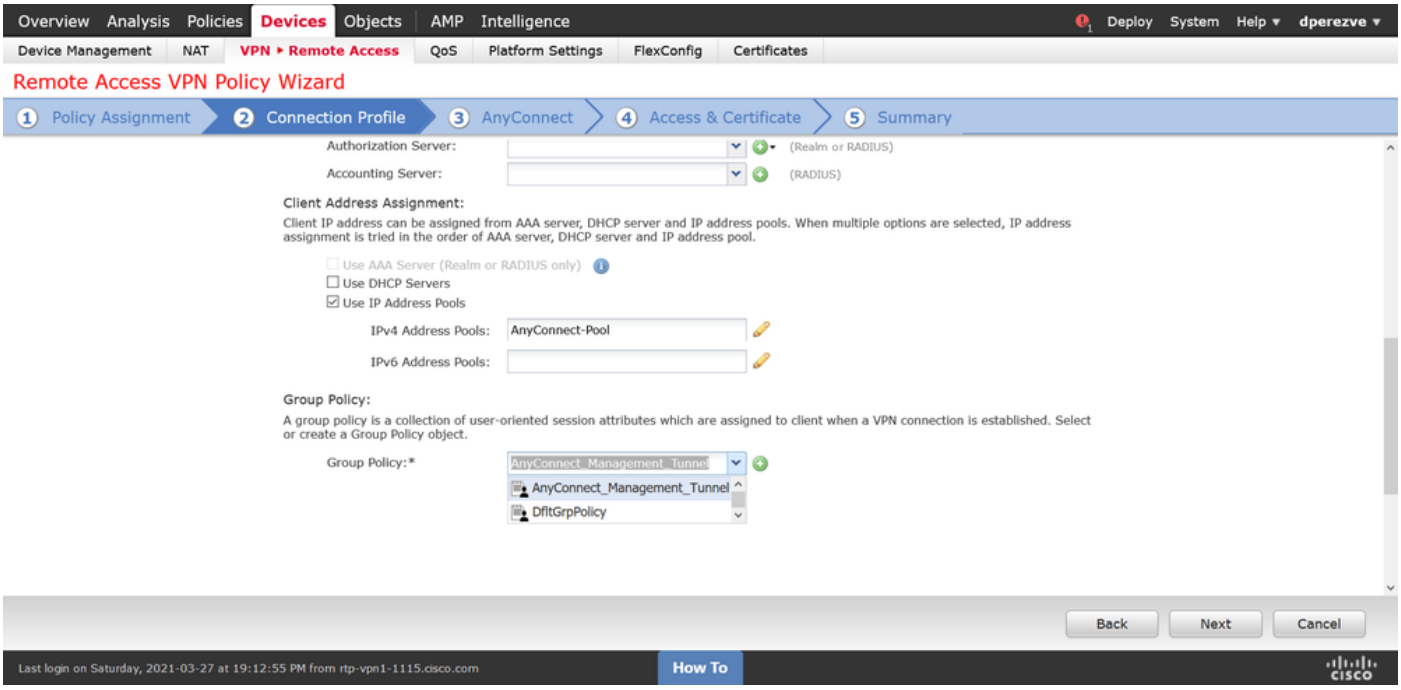
Wählen Sie auf der Registerkarte "**Richtlinienzuweisung**" das jeweilige FTD-Gerät aus, legen Sie einen Namen für das Verbindungsprofil fest, und aktivieren Sie das Kontrollkästchen SSL.



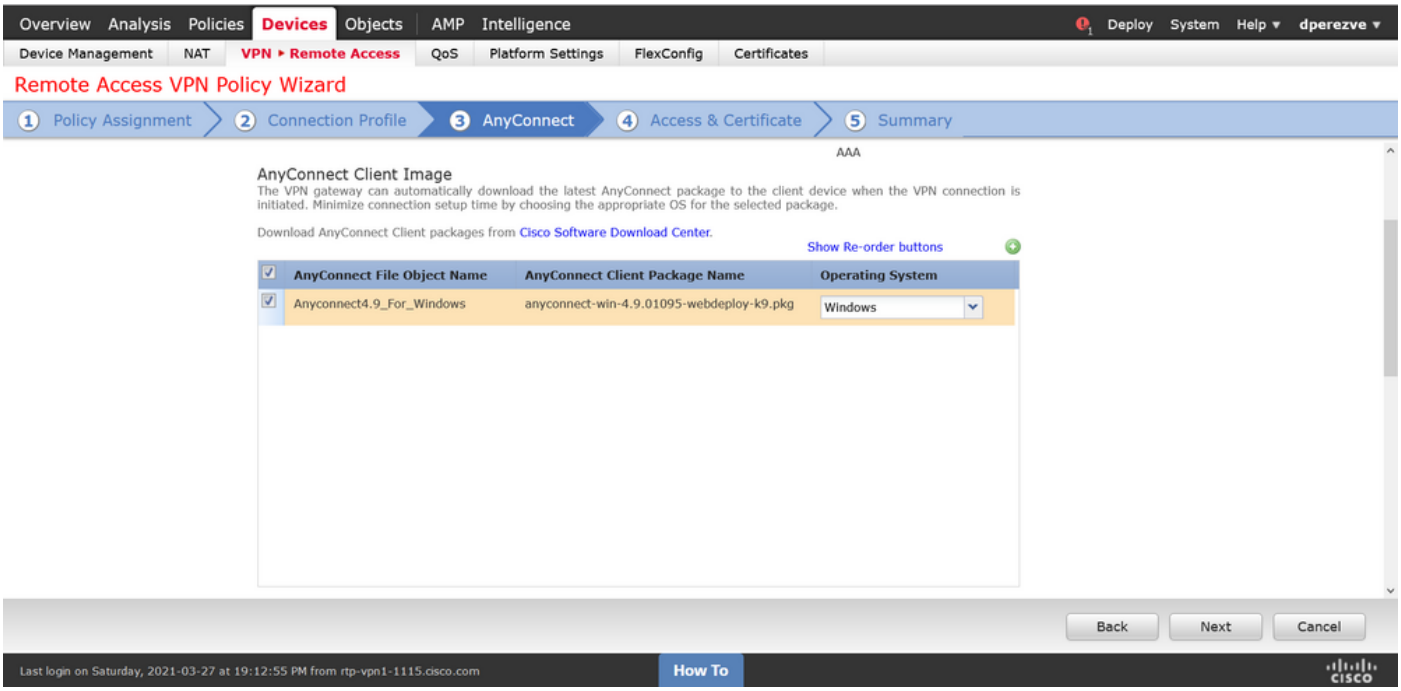
Wählen Sie im **Verbindungsprofil Client Certificate Only** als Authentifizierungsmethode aus. Dies ist die einzige für die Funktion unterstützte Authentifizierung.



Wählen Sie anschließend im Dropdown-Menü **Gruppenrichtlinie** das in Schritt 3 erstellte Gruppenrichtlinienobjekt aus.



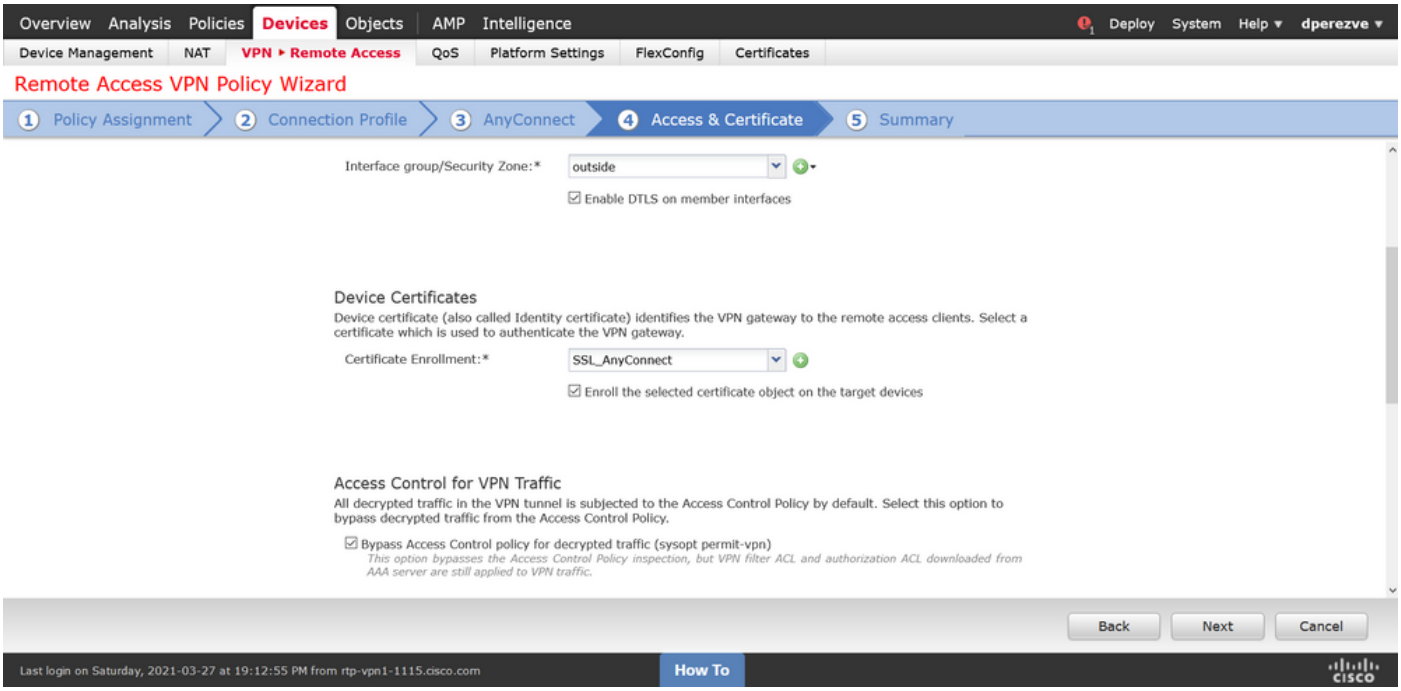
Wählen Sie auf der Registerkarte **AnyConnect** das **AnyConnect-Dateiobjekt** entsprechend dem Betriebssystem auf dem Endgerät aus.



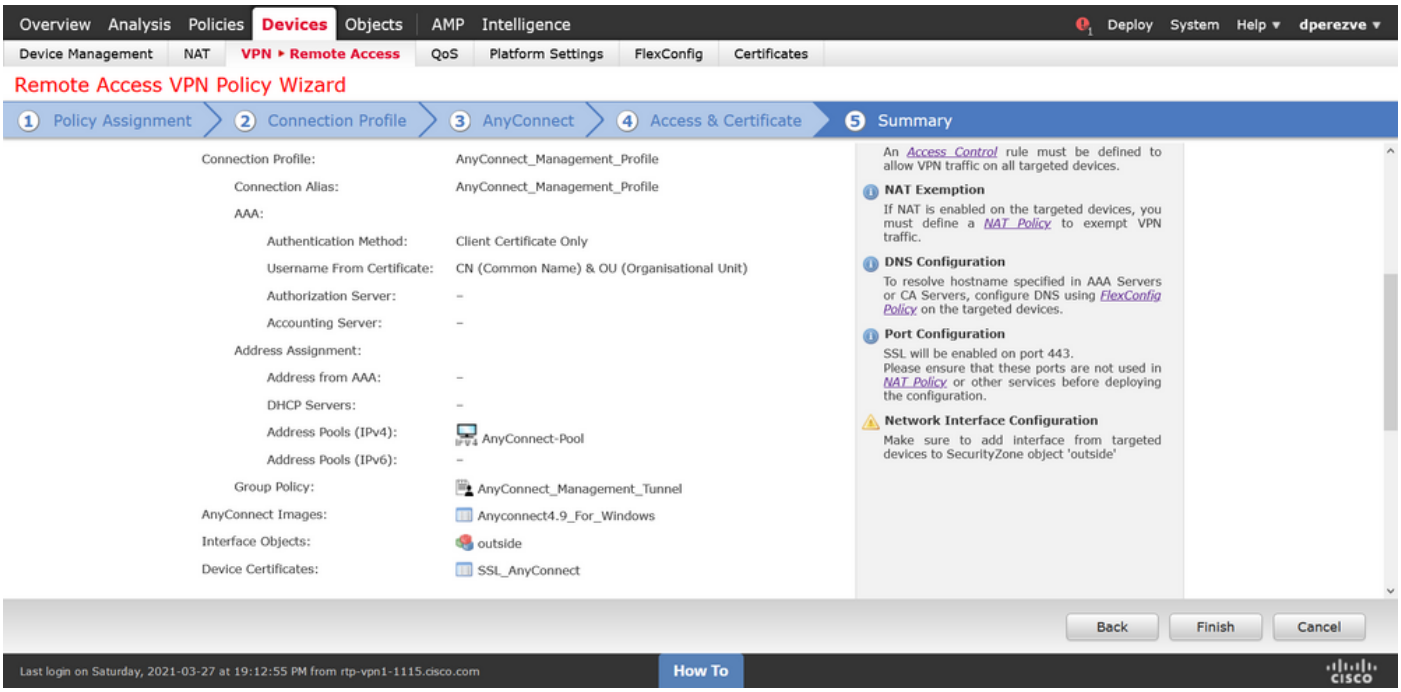
Geben Sie unter **Zugriff und Zertifikat** das Zertifikat an, das von der FTD verwendet werden muss, um seine Identität an den Windows-Client zu überprüfen.

> **Hinweis:** Da Benutzer bei Verwendung der Management-VPN-Funktion nicht mit der AnyConnect-App interagieren sollten, muss das Zertifikat voll vertrauenswürdig sein und darf keine Warnmeldung ausdrucken.

> **Hinweis:** Um Fehler bei der Zertifikatsvalidierung zu vermeiden, muss das Feld Common Name (CN) im Betreffnamen des Zertifikats mit dem in der Serverliste der XML-Profile definierten FQDN übereinstimmen (Schritt 1 und Schritt 2).



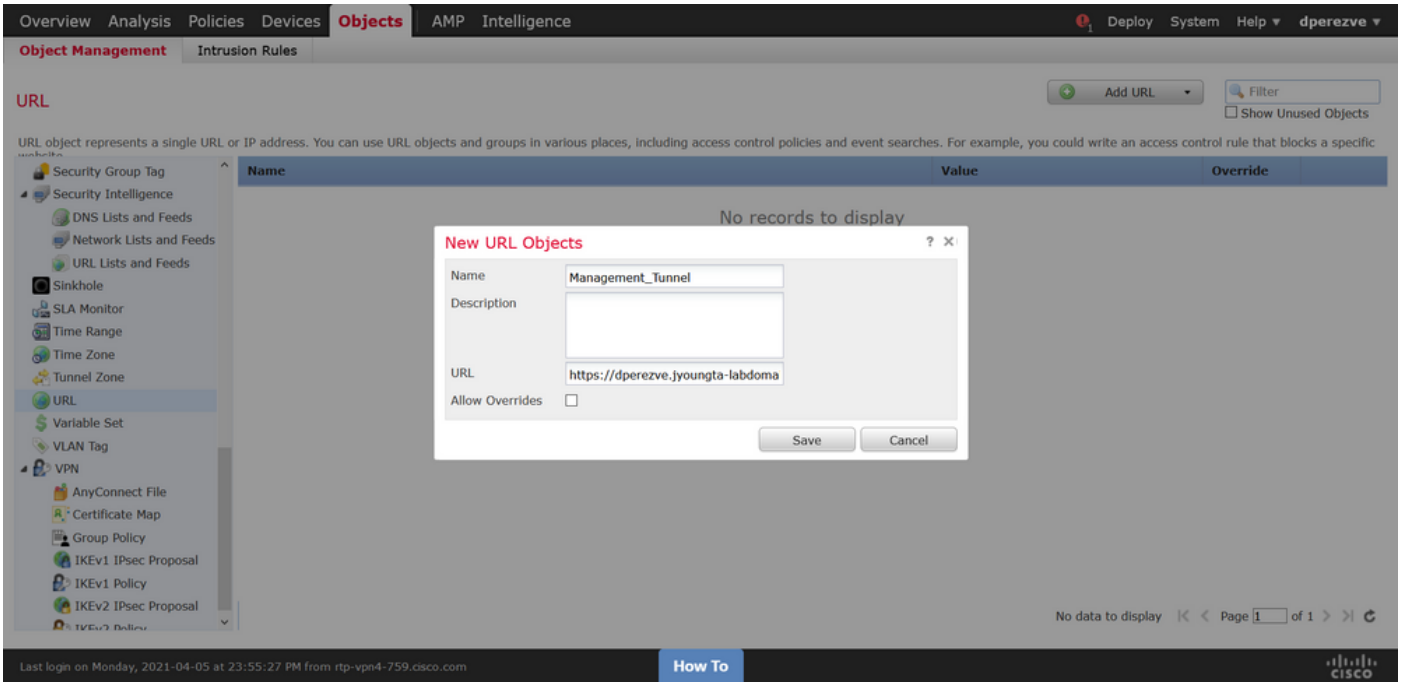
Wählen Sie abschließend auf der Registerkarte **Zusammenfassung die** Schaltfläche **Beenden**, um die neue AnyConnect-Konfiguration hinzuzufügen.



Schritt 6: URL-Objekt erstellen

Navigieren Sie zu **Objekte > Objektverwaltung**, und wählen Sie **URL** aus dem Inhaltsverzeichnis aus. Wählen Sie dann **Objekt hinzufügen** im Dropdown-Menü **URL hinzufügen aus**.

Geben Sie einen Namen für das Objekt ein, und definieren Sie die URL mithilfe desselben FQDN/Benutzergruppen, der in der Liste der Management-VPN-Profilserver (Schritt 2) angegeben ist. In diesem Beispiel muss die URL dperezve.jyoungta-labdomain.cisco.com/AnyConnect_Management_Tunnel lauten.

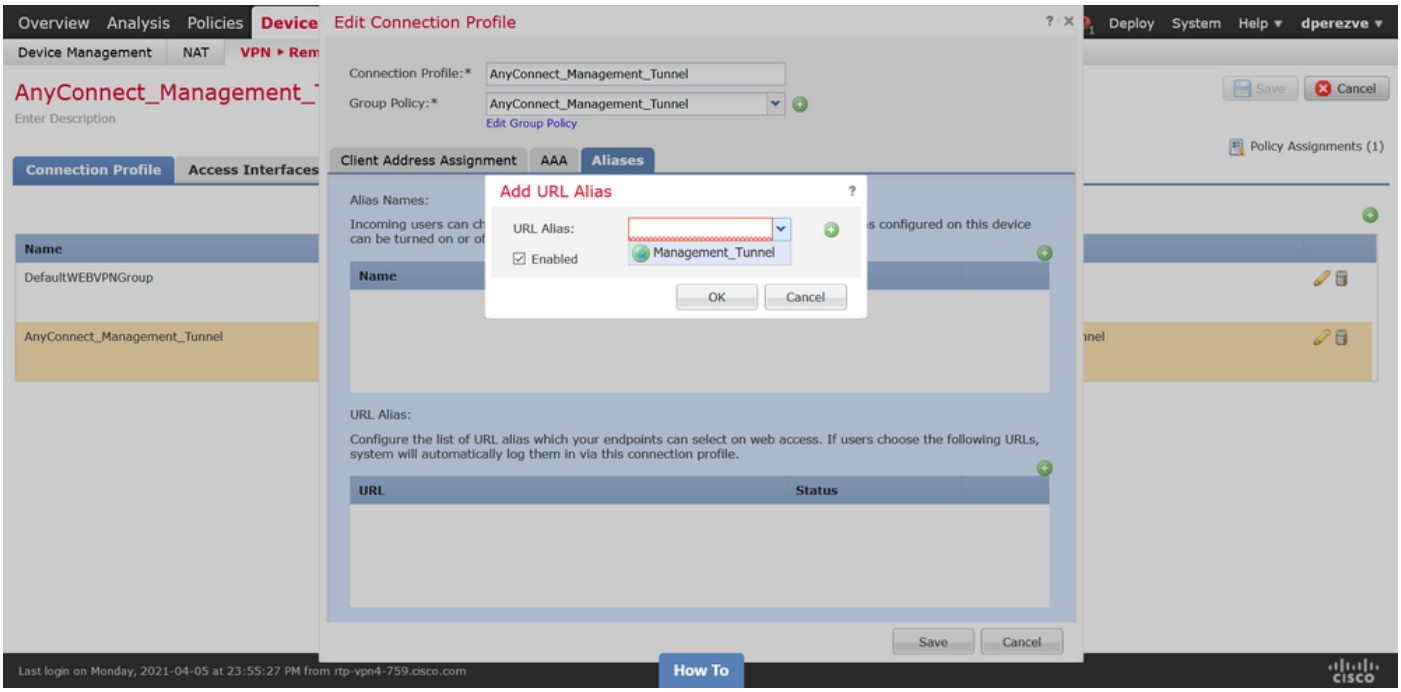


Speichern Sie die Änderungen, um das Objekt der Objektliste hinzuzufügen.

Schritt 7: URL-Alias definieren

Um die URL-Alias in der AnyConnect-Konfiguration zu aktivieren, navigieren Sie zu **Devices > VPN > Remote Access** und klicken Sie auf das Bleistiftsymbol, um die Alias zu bearbeiten.

Wählen Sie dann auf der Registerkarte **Verbindungsprofil** die aktuelle Konfiguration aus, navigieren Sie zu **Aliases**, klicken Sie auf die Schaltfläche **Hinzufügen,** und wählen Sie das **URL-Objekt** im **Dropdown-Menü URL-Alias aus.** Stellen Sie sicher, dass das Kontrollkästchen **Aktiviert** aktiviert aktiviert ist.



Speichern von Änderungen und Bereitstellen von Konfigurationen in FTD

Überprüfung

Nach Abschluss der Bereitstellung ist eine erste manuelle AnyConnect-Verbindung mit dem AnyConnect VPN-Profil erforderlich. Während dieser Verbindung wird das Management-VPN-Profil von FTD heruntergeladen und in **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun** gespeichert. Von diesem Zeitpunkt an müssen nachfolgende Verbindungen über das Management-VPN-Profil ohne Benutzerinteraktion initiiert werden.

Fehlerbehebung

Bei Zertifikatsvalidierungsfehlern:

- Stellen Sie sicher, dass das Stammzertifikat der Zertifizierungsstelle (Certificate Authority, CA) in der FTD installiert ist.
- Stellen Sie sicher, dass ein Identitätszertifikat, das von derselben Zertifizierungsstelle signiert wurde, im Windows Machine Store installiert ist.
- Stellen Sie sicher, dass das CN-Feld im Zertifikat enthalten ist und mit dem in der Serverliste des Management-VPN-Profils definierten FQDN und dem in URL-Alias definierten FQDN übereinstimmt.

Für Management-Tunnel nicht initiiert:

- Stellen Sie sicher, dass das Management-VPN-Profil heruntergeladen und in **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun** gespeichert wurde.

- Stellen Sie sicher, dass der Name für das Management-VPN-Profil **VpnMgmtTunProfile.xml lautet**.

Bei Verbindungsproblemen können Sie das DART-Paket sammeln und das Cisco TAC um weitere Informationen bitten.