

# 在FTD上設定SSL AnyConnect管理VPN

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[限制](#)

[設定](#)

[組態](#)

[步驟1.建立AnyConnect管理VPN配置檔案](#)

[步驟2.建立AnyConnect VPN配置檔案](#)

[步驟3.將AnyConnect管理VPN配置檔案和AnyConnect VPN配置檔案上傳到FMC](#)

[步驟4.建立組策略](#)

[步驟5.建立新的AnyConnect配置](#)

[步驟6.建立URL對象](#)

[步驟7.定義URL別名](#)

[驗證](#)

[疑難排解](#)

## 簡介

本檔案介紹如何在思科Firepower管理中心(FMC)管理的Cisco Firepower威脅防禦(FTD)上配置Cisco AnyConnect管理隧道。在下面的示例中，安全套接字層(SSL)用於在FTD和Windows 10客戶端之間建立虛擬專用網路(VPN)。

作者：Daniel Perez Vertti Vazquez，思科TAC工程師。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- Cisco AnyConnect Profile Editor
- 通過FMC配置SSL AnyConnect。
- 客戶端證書身份驗證

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco FTD版本6.7.0 ( 內部版本65 )

- Cisco FMC 6.7.0版 ( 內部版本65 )
- Cisco AnyConnect 4.9.01095安裝在Windows 10電腦上

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 ( 預設 ) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

自6.7版起，思科FTD支援配置AnyConnect管理隧道。此修復了先前開啟的增強功能請求 [CSCvs78215](#)。

AnyConnect管理功能允許在終端完成啟動後立即建立VPN隧道。使用者無需手動啟動AnyConnect應用，只要他們的系統通電，AnyConnect VPN代理服務就會檢測管理VPN功能，並使用AnyConnect管理VPN配置檔案的伺服器清單中定義的Host Entry啟動AnyConnect會話。

## 限制

- 僅支援客戶端證書身份驗證。
- Windows客戶端僅支援電腦證書儲存。
- Cisco Firepower裝置管理器(FDM) [CSCvx90058](#)上不支援。
- Linux客戶端不支援。

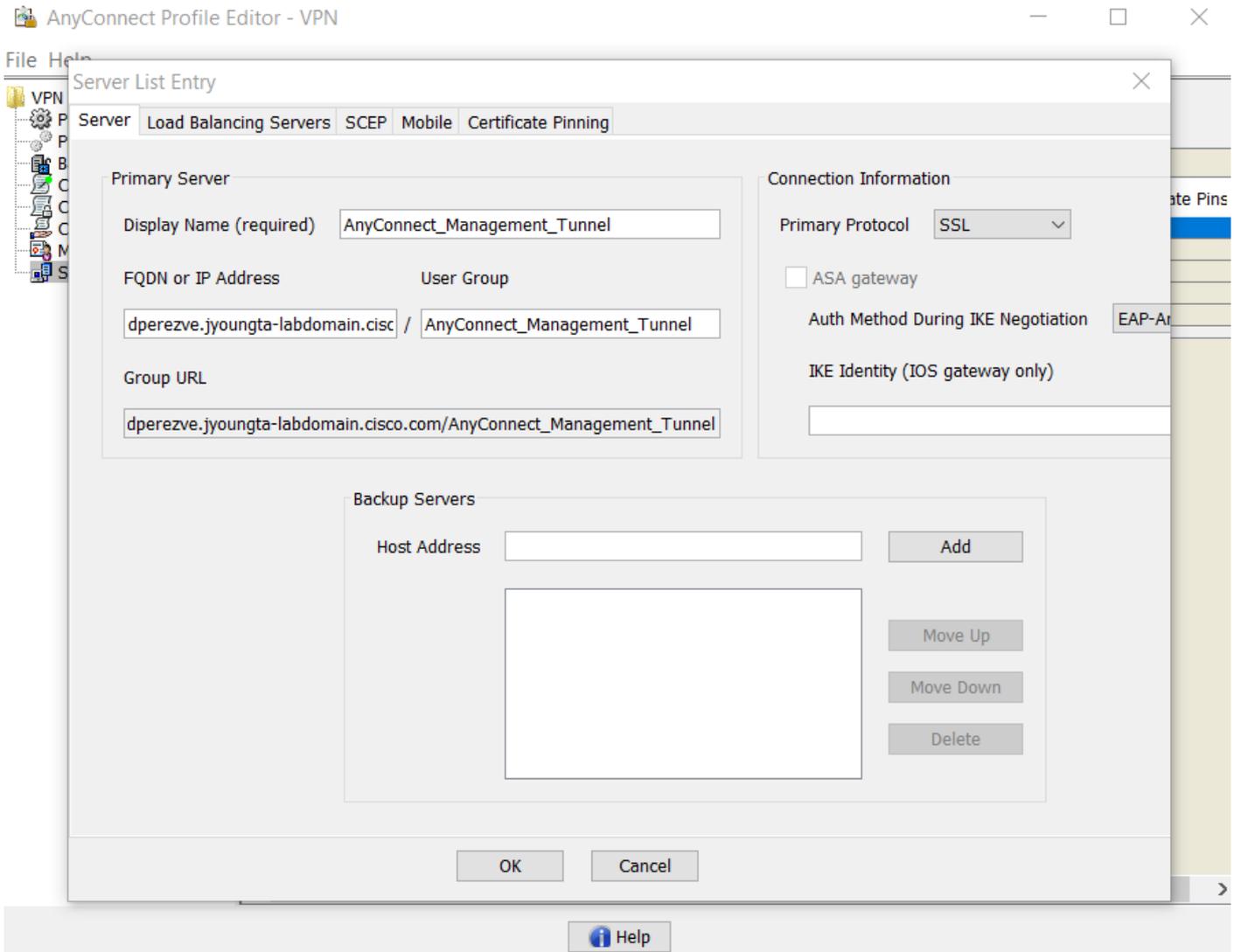
## 設定

### 組態

#### 步驟1.建立AnyConnect管理VPN配置檔案

開啟AnyConnect配置檔案編輯器以建立AnyConnect管理VPN配置檔案。管理配置檔案包含終端啟動後用於建立VPN隧道的所有設定。

在此示例中，定義了一個指向完全限定域名(FQDN)dperezve.jyoungta-labdomain.cisco.com的伺服器清單條目，並選定SSL作為主要協定。要新增伺服器清單，請導航到**伺服器清單**並選擇**新增**按鈕，填寫所需欄位並儲存更改。



除了伺服器清單，管理VPN配置檔案還必須包含一些必需的首選項：

- **AutomaticCertSelection**必須設定為**true**。
- **AutoReconnect**必須設定為**true**。
- 必須為**ReconnectAfterResume**配置**AutoReconnectBehavior**。
- **AutoUpdate**必須設定為**false**。
- **BlockUntrustedServers**必須設定為**true**。
- 必須為**MachineStore**配置**CertificateStore**。
- **CertificateStoreOverride**必須設定為**true**。
- **EnableAutomaticServerSelection**必須設定為**false**。
- **EnableScripting**必須設定為**false**。
- **RetainVPNOnLogoff**必須設定為**true**。

在AnyConnect Profile Editor中，導航至**首選項（第1部分）**，並按如下方式調整設定：

File Help

**VPN**

- Preferences (Part 1)
- Preferences (Part 2)
- Backup Servers
- Certificate Pinning
- Certificate Matching
- Certificate Enrollment
- Mobile Policy
- Server List

### Preferences (Part 1)

Profile: ...nnect -FTD-Lab1.XML Profile\AnyConnect\_Management\_Tunnel.xml

Use Start Before Logon  User Controllable

Show Pre-Connect Message

Certificate Store

Windows **Machine** ▾

macOS **All** ▾

Certificate Store Override

Auto Connect On Start  User Controllable

Minimize On Connect  User Controllable

Local Lan Access  User Controllable

Disable Captive Portal Detection  User Controllable

Auto Reconnect  User Controllable

Auto Reconnect Behavior

**ReconnectAfterResume** ▾

Auto Update  User Controllable

RSA Secure ID Integration  User Controllable

Automatic ▾

Windows Logon Enforcement

SingleLocalLogon ▾

Windows VPN Establishment

AllowRemoteUsers ▾

Help

然後導覽至首選項（第2部分），並取消選中Disable Automatic Certificate Selection選項。

File Help

**Preferences (Part 2)**  
Profile: ...nnect -FTD-Lab1.XML ProfileAnyConnect\_Management\_Tunnel.xml

Disable Automatic Certificate Selection  User Controllable

Proxy Settings: Native  User Controllable

Public Proxv Server Address:

Note: Enter public Proxv Server address and Port here. Example:10.86.125.33:8080

Allow Local Proxy Connections

Enable Optimal Gateway Selection  User Controllable

Suspension Time Threshold (hours): 4

Performance Improvement Threshold (%): 20

Automatic VPN Policy

Trusted Network Policy: Disconnect

Untrusted Network Policy: Connect

Trusted DNS Domains:

Trusted DNS Servers:

Note: adding all DNS servers in use is recommended with Trusted Network Detection

Trusted Servers @ https://<server>[:<port>]

https://

## 步驟2.建立AnyConnect VPN配置檔案

除管理VPN配置檔案外，還需要配置常規AnyConnect VPN配置檔案。AnyConnect VPN配置檔案用於第一次連線嘗試，在此會話期間，管理VPN配置檔案從FTD下載。

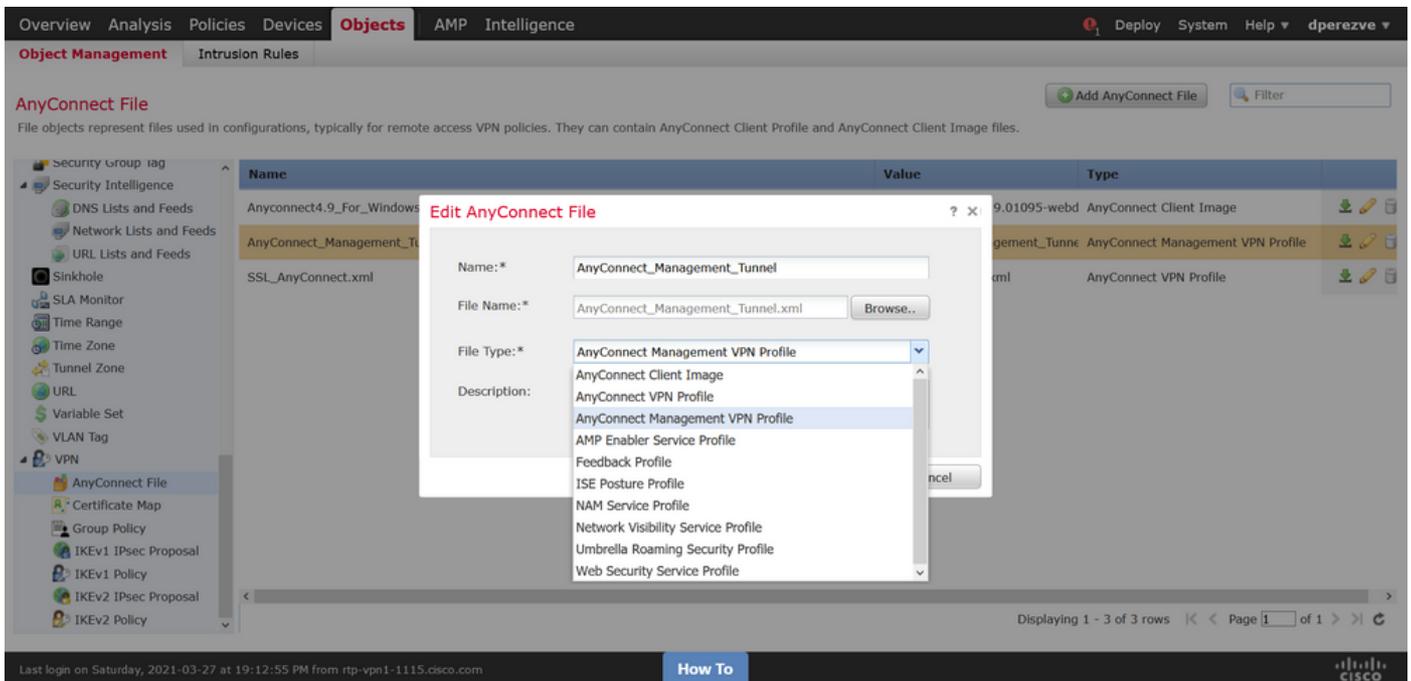
使用AnyConnect配置檔案編輯器建立AnyConnect VPN配置檔案。在這種情況下，兩個檔案都包含相同的設定，以便可以遵循相同的過程。

## 步驟3.將AnyConnect管理VPN配置檔案和AnyConnect VPN配置檔案上傳到FMC

建立配置檔案後，下一步是將其作為AnyConnect檔案對象上傳到FMC。

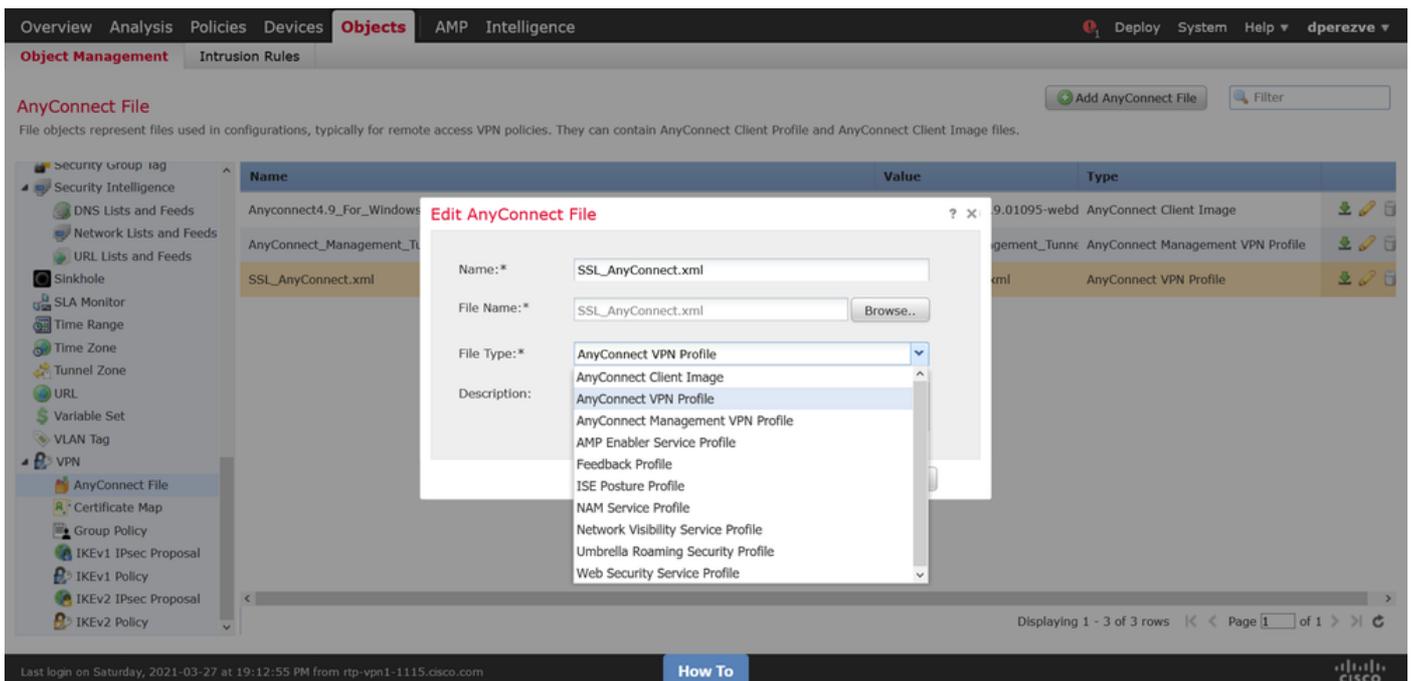
若要將新的AnyConnect管理VPN配置檔案上傳到FMC，請導航到Objects > Object Management，然後從目錄中選擇VPN選項，然後選擇Add AnyConnect File按鈕。

提供檔案的名稱，選擇AnyConnect Management VPN Profile作為檔案型別並儲存對象。

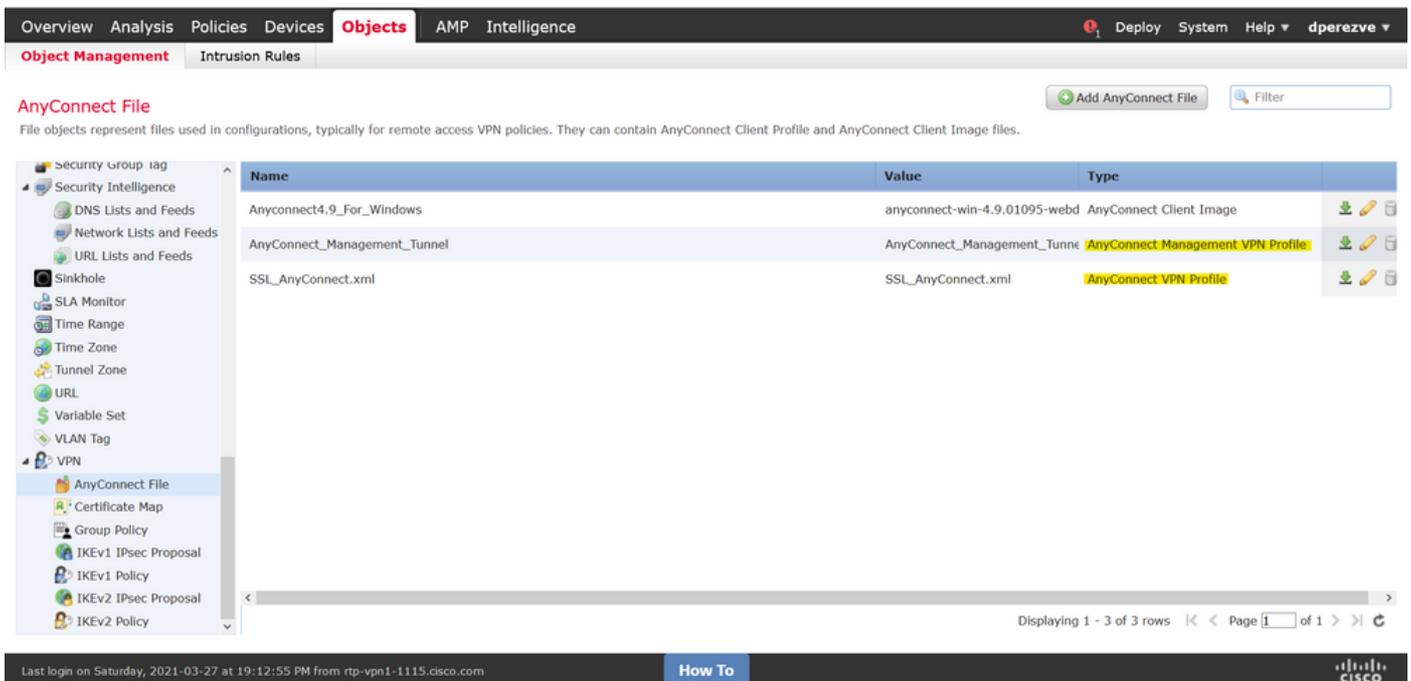


現在，若要上傳AnyConnect VPN配置檔案，請再次導航到Objects > Object Management，然後從目錄中選擇VPN選項，然後選擇Add AnyConnect File按鈕。

提供檔案的名稱，但這次選擇AnyConnect VPN Profile作為檔案型別並儲存新對象。



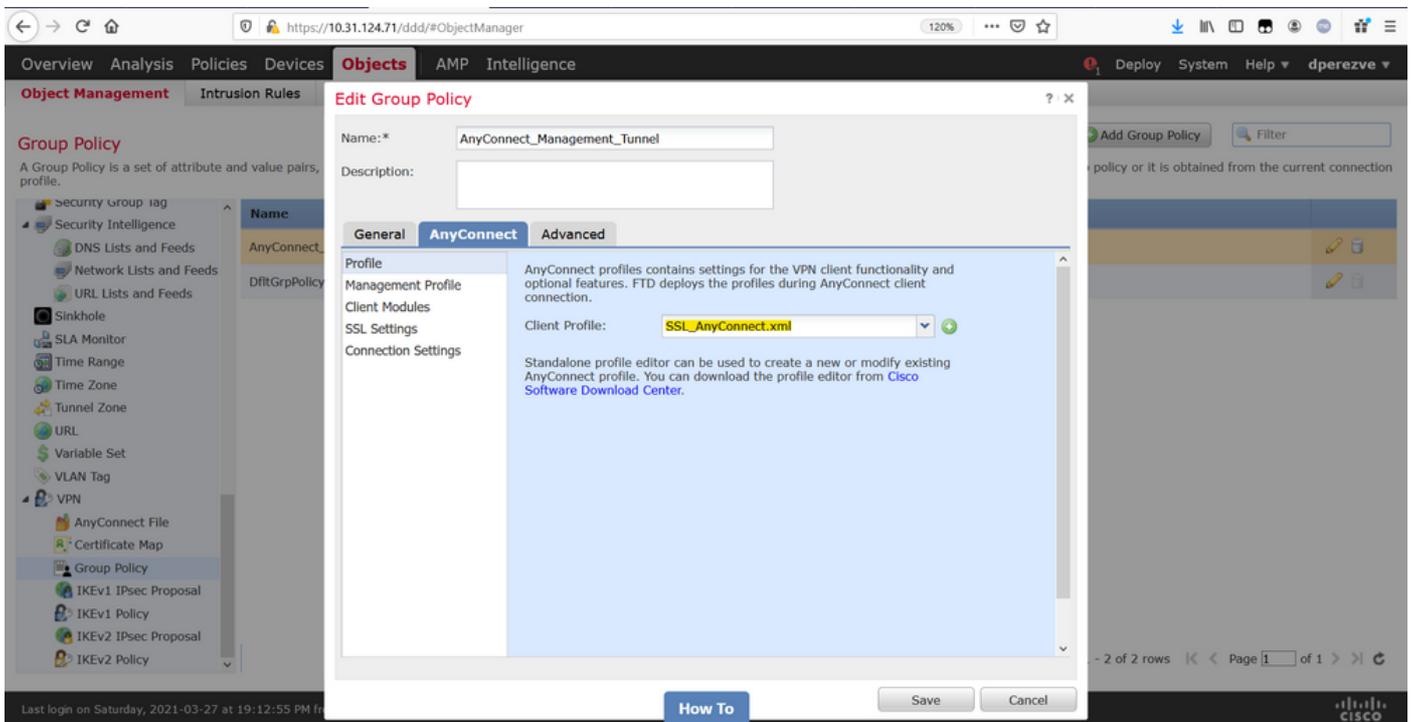
必須將配置檔案新增到對象清單，並分別標籤為AnyConnect Management VPN Profile 和 AnyConnect VPN Profile。



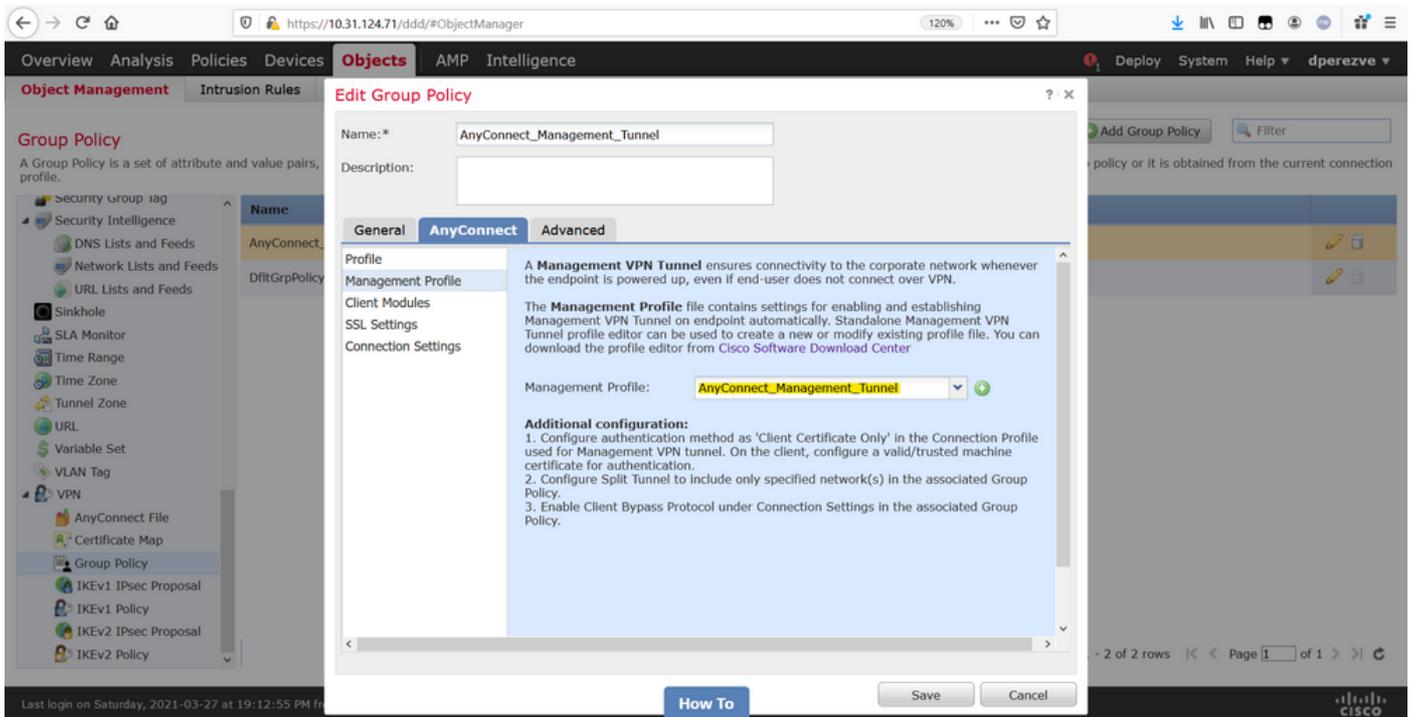
## 步驟4. 建立組策略

若要建立新的組策略，請導航到 **Objects > Object Management**，然後從目錄中選擇 **VPN** 選項，然後選擇 **Group Policy**，然後在 **Add Group Policy** 按鈕上按一下。

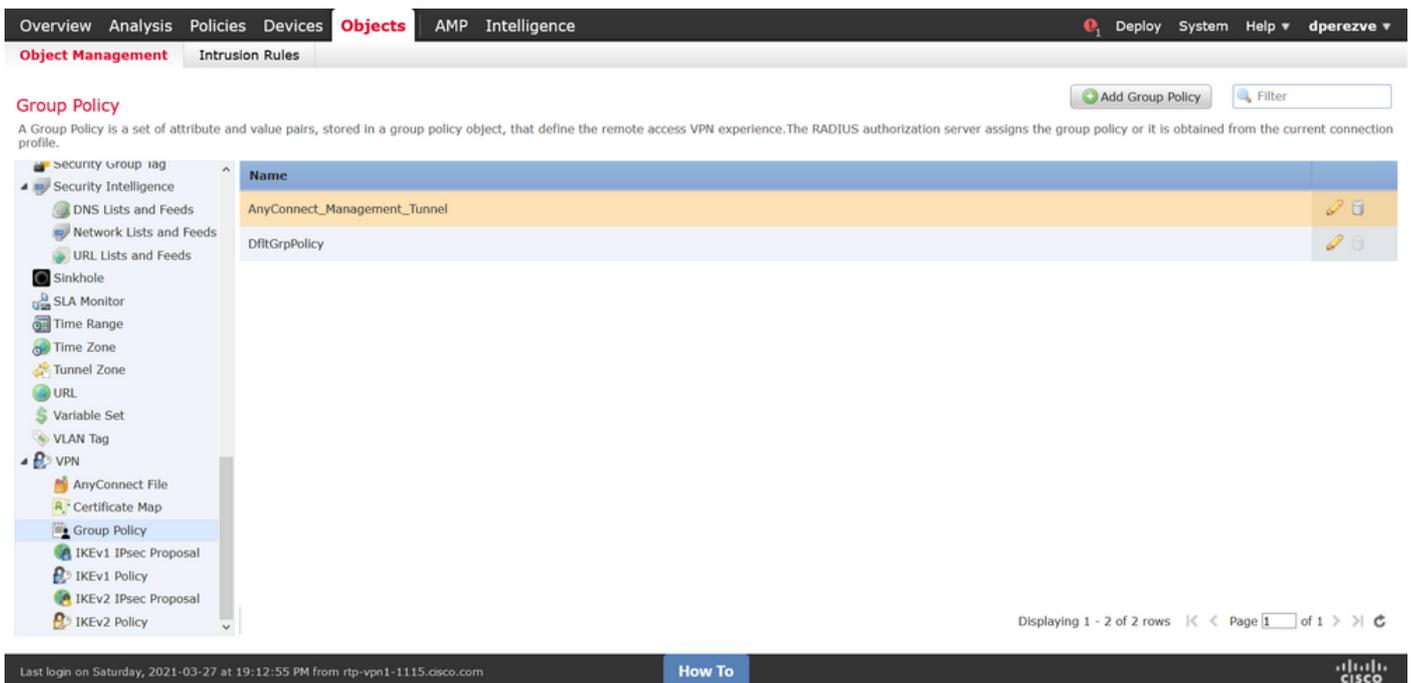
**Add Group Policy** 視窗開啟後，分配名稱，定義 AnyConnect 池並開啟 **AnyConnect** 頁籤。導航到 **Profile**，然後在 **Client Profile** 下拉選單中選擇代表常規 AnyConnect VPN 配置檔案的對象。



然後導航到 **Management Profile** 頁籤，然後在 **Management Profile** 下拉選單中選擇包含 **Management VPN Profile** 的對象。



儲存更改以將新對象新增到現有組策略。



## 步驟5. 建立新的AnyConnect配置

FMC中的SSL AnyConnect配置由4個不同的步驟組成。要配置AnyConnect，請導航到**Devices > VPN > Remote Access**，然後選擇**Add**按鈕。此操作必須開啟遠端訪問VPN策略嚮導。

在**Policy Assignment**索引標籤上選擇手邊的FTD裝置，定義連線配置檔案的名稱並勾選SSL覈取方塊。

○

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help dperezve

Dashboards Reporting Summary

### Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

**Targeted Devices and Protocols**

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:\*

Description:

VPN Protocols:  SSL  IPsec-IKEv2

Targeted Devices:

Available Devices:   
 ftdv-dperezve  
 ftdv-fejimene

Selected Devices:  ftdv-dperezve

**Before You Start**

Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

**Authentication Server**  
Configure [Realm](#) or [RADIUS Server Group](#) or [SSO](#) to authenticate VPN clients.

**AnyConnect Client Package**  
Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

**Device Interface**  
Interfaces should be already configured on targeted [devices](#) so that they can be used as a security zone or interface group to enable VPN access.

Last login on Thursday, 2021-03-25 at 17:01:05 PM from rtp-vpn6-107.cisco.com How To

在Connection Profile上選擇Client Certificate Only作為身份驗證方法。這是該功能支援的唯一身份驗證。

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help dperezve

Device Management NAT **VPN Remote Access** QoS Platform Settings FlexConfig Certificates

### Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

**Connection Profile:**

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name:\*   
This name is configured as a connection alias, it can be used to connect to the VPN gateway

**Authentication, Authorization & Accounting (AAA):**

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method:

Username From Certificate:  (Distinguished Name) as username

Primary Field:

Secondary Field:

Authorization Server:  (Realm or RADIUS)

Accounting Server:  (RADIUS)

**Client Address Assignment:**

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

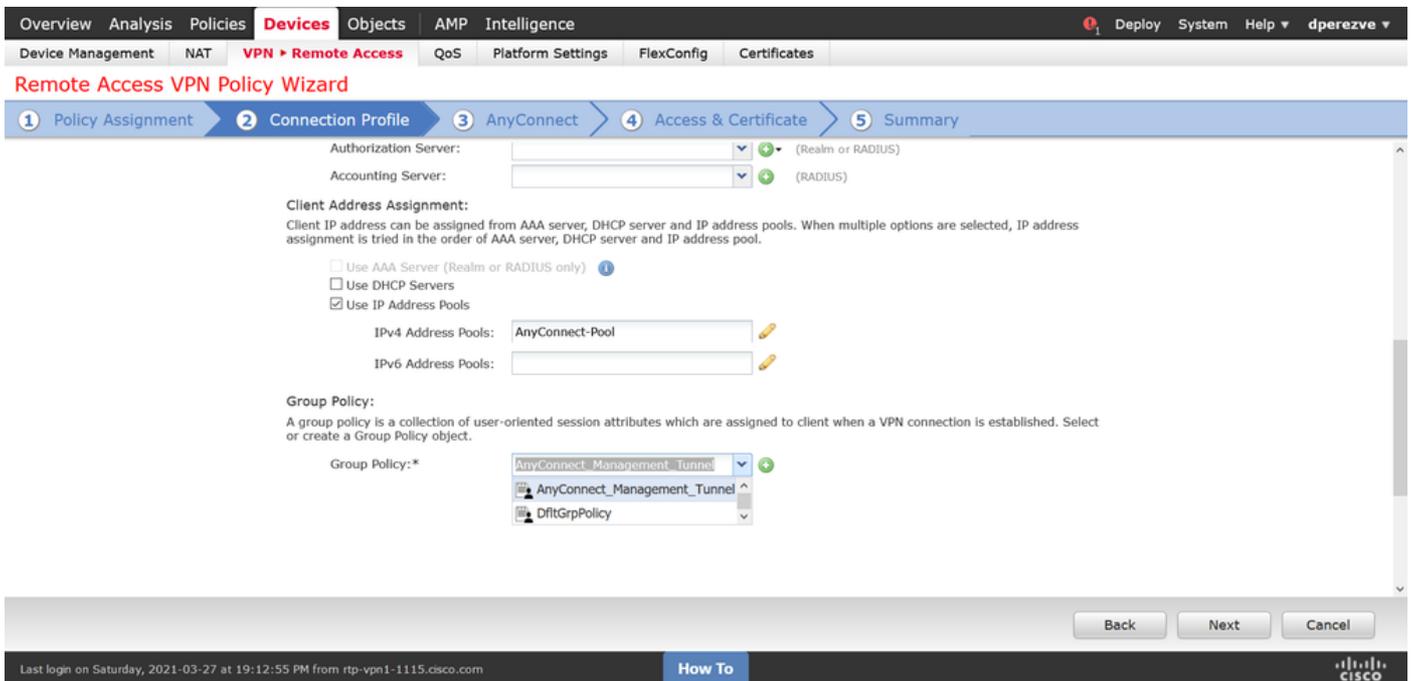
Use AAA Server (Realm or RADIUS only) i

Use DHCP Servers

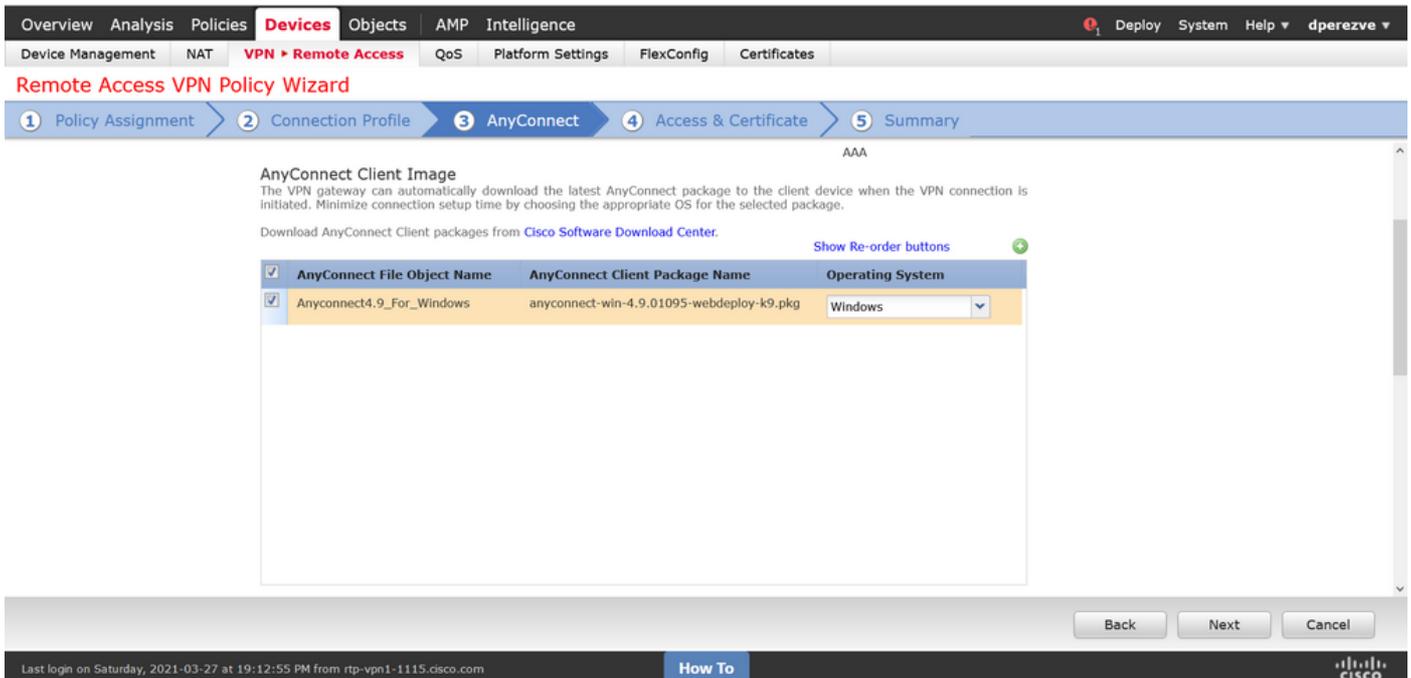
Use IP Address Pools

Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com How To

然後在「組策略」(Group Policy)下拉選單中，選擇在步驟3中建立的組策略對象。



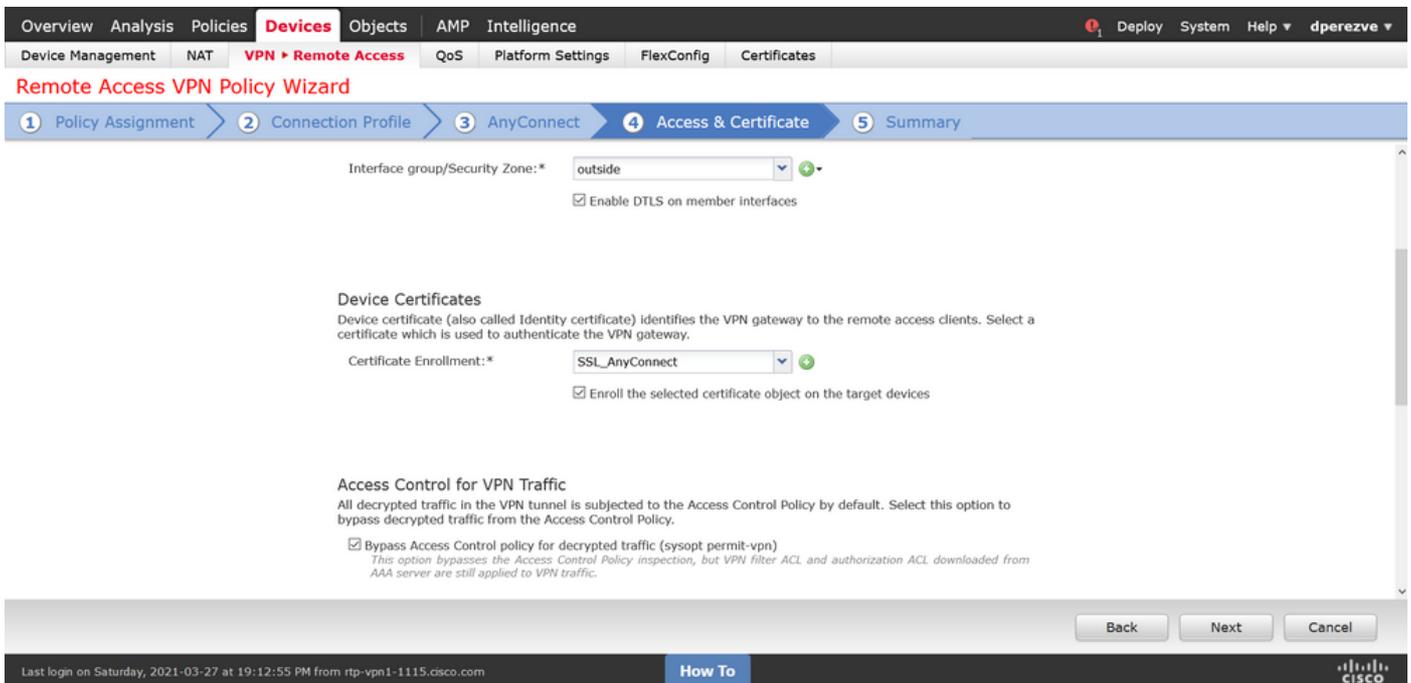
在AnyConnect頁籤上，根據終端上的作業系統(OS)選擇AnyConnect檔案對象。



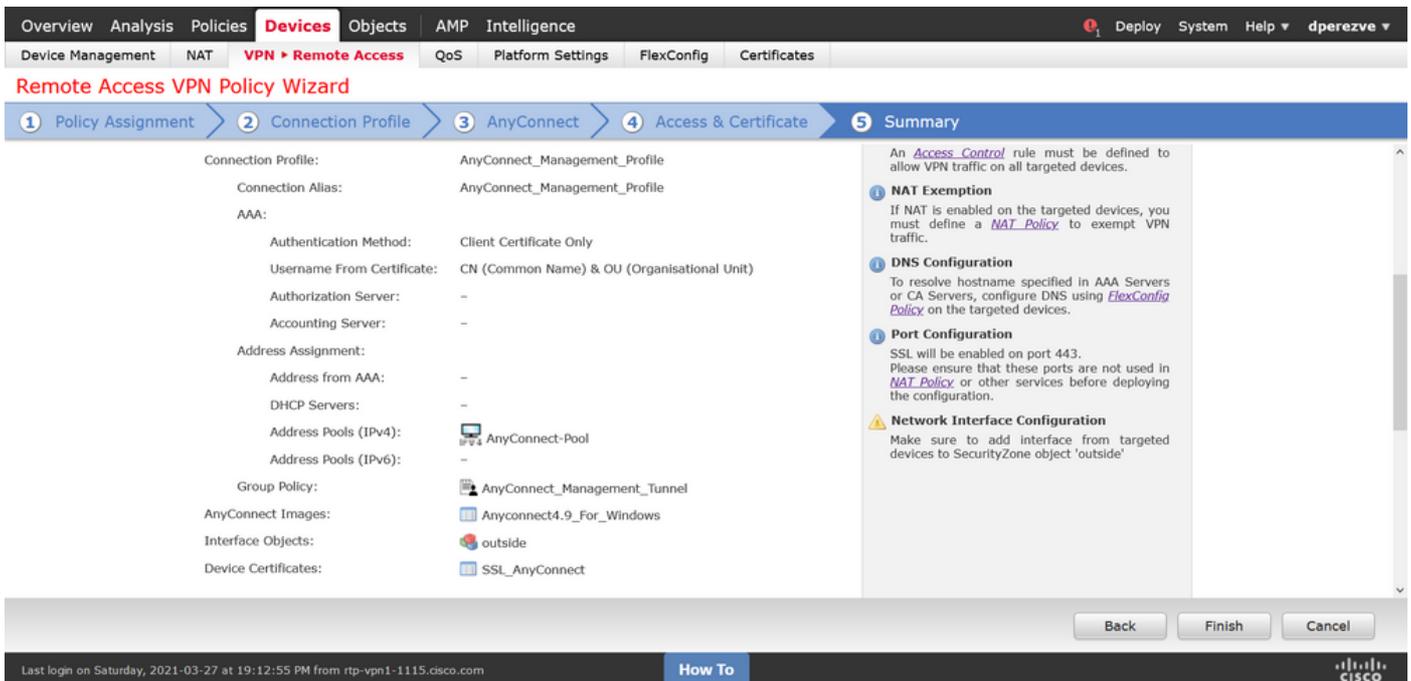
在Access & Certificate上，指定FTD必須使用的證書，以向Windows客戶端探測其身份。

**附註：**由於使用者在使用管理VPN功能時不應與AnyConnect應用互動，因此證書需要完全受信任，並且不得列印任何警告消息。

**附註：**為了防止證書驗證錯誤，證書的使用者名稱中包含的公用名(CN)欄位必須與伺服器XML配置檔案清單（步驟1和步驟2）中定義的FQDN匹配。



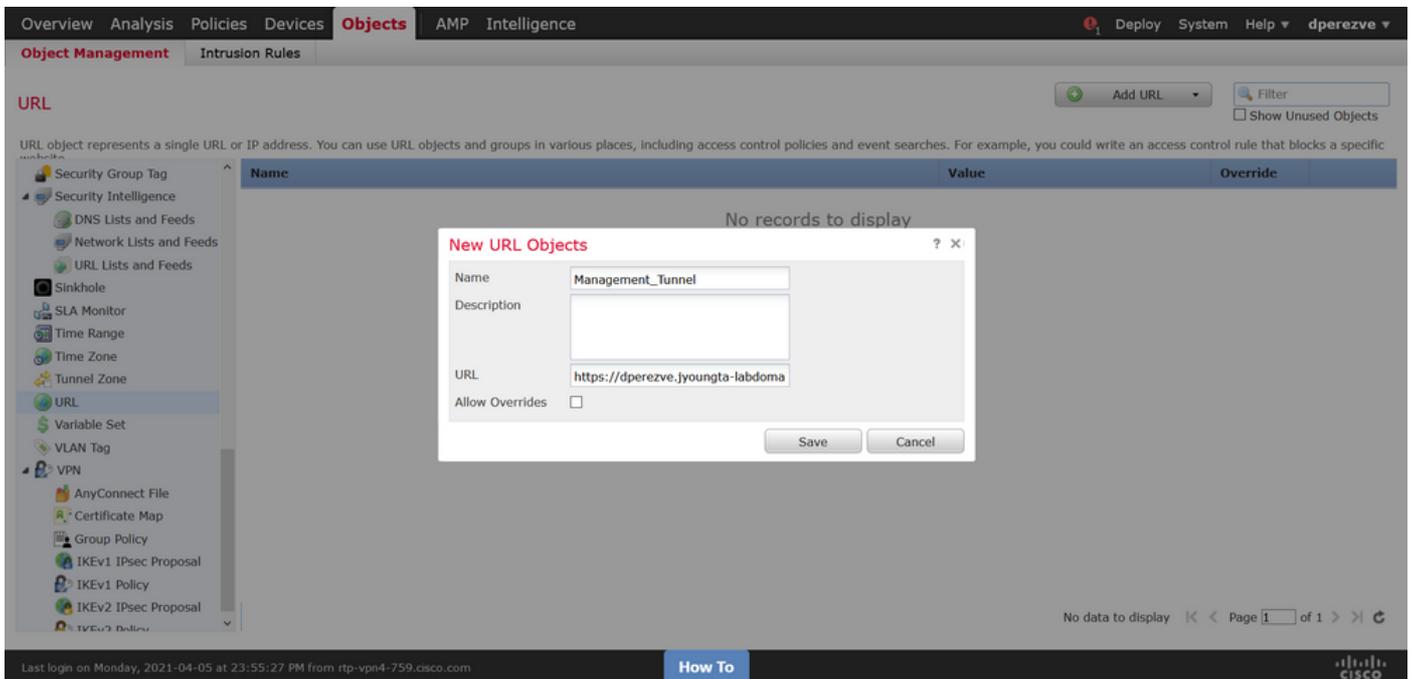
最後，在Summary頁籤上選擇Finish按鈕以新增新的AnyConnect配置。



## 步驟6.建立URL對象

導航到對象>對象管理，然後從目錄中選擇URL。然後在Add URL下拉選單中選擇Add Object。

提供對象的名稱，並使用在管理VPN配置檔案伺服器清單中指定的FQDN/使用者組定義URL ( 步驟 2 )。在本例中，URL必須是dperezve.jyoungta-labdomain.cisco.com/AnyConnect\_Management\_Tunnel。

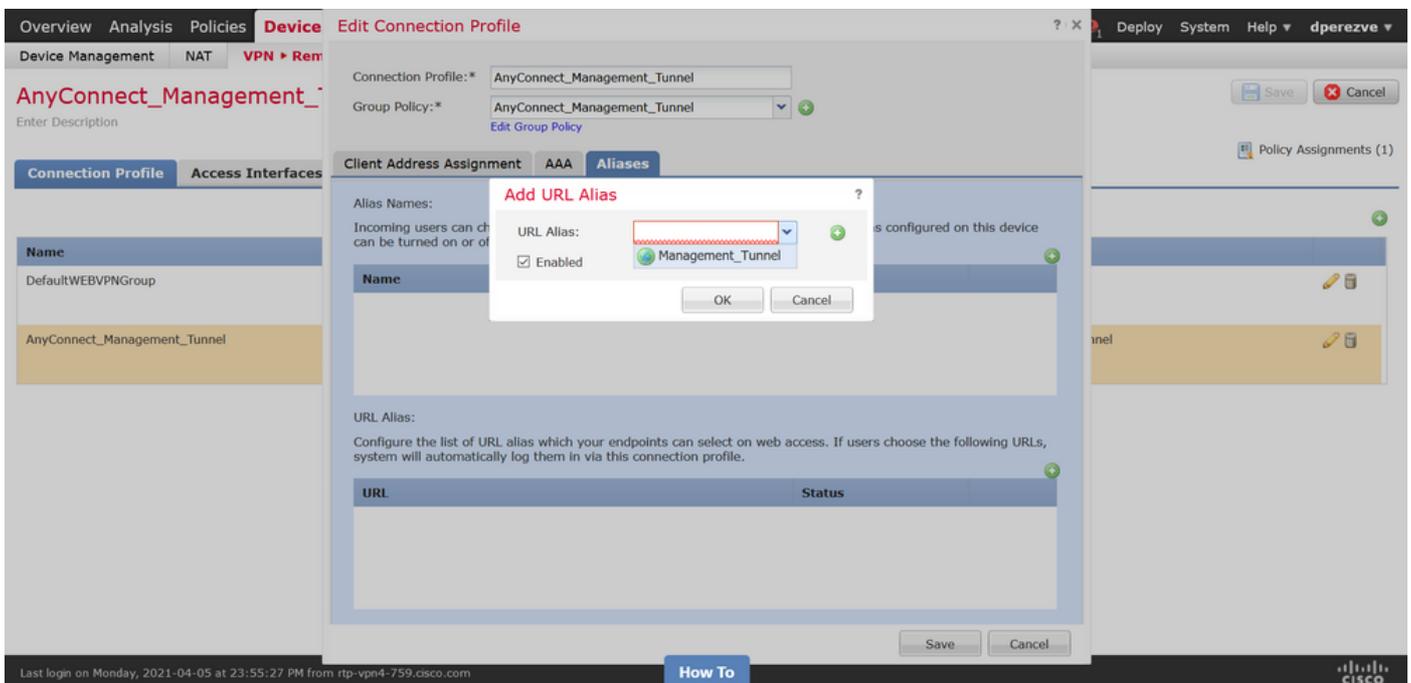


儲存更改以將對象新增到對象清單。

## 步驟7.定義URL別名

要在AnyConnect配置中啟用URL別名，請導航至Devices > VPN > Remote Access，然後按一下鉛筆圖示進行編輯。

然後，在Connection Profile選項卡上，選擇手頭的配置，導航到Aliases，在Add按鈕上按一下，然後在URL Alias下拉選單中選擇URL Object。確保選中Enabled覆取方塊。



儲存變更並將組態部署到FTD。

## 驗證

部署完成後，需要與AnyConnect VPN配置檔案進行第一個手動的AnyConnect連線。在此連線期間，管理VPN配置檔案從FTD下載並儲存在C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun中。此後，後續連線必須通過管理VPN配置檔案啟動，無需任何使用者互動。

## 疑難排解

對於證書驗證錯誤：

- 確保在FTD上安裝憑證授權單位(CA)的根憑證。
- 確保在Windows電腦應用商店上安裝由同一CA簽名的身份證書。
- 確保CN欄位包含在證書中，並且與管理VPN配置檔案的伺服器清單中定義的FQDN和URL別名中定義的FQDN相同。

對於未啟動的管理隧道：

- 確保管理VPN配置檔案已下載並儲存在C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun中。
- 確保管理VPN配置檔案的名稱為VpnMgmtTunProfile.xml。

對於連線問題，請收集DART捆綁包並聯絡Cisco TAC進行進一步研究。