

# 在FDM管理的FTD上配置遠端訪問VPN

## 目錄

---

### [簡介](#)

### [必要條件](#)

[需求](#)

[授權](#)

[採用元件](#)

### [背景資訊](#)

### [設定](#)

[網路圖表](#)

[驗證FTD上的授權](#)

[定義受保護的網路](#)

[建立本地使用者](#)

[新增證書](#)

[配置遠端訪問VPN](#)

### [驗證](#)

### [疑難排解](#)

[AnyConnect客戶端問題](#)

[初始連線問題](#)

[流量特定的問題](#)

---

## 簡介

本文檔介紹如何配置運行6.5.0及更高版本的機箱內管理器FDM管理的FTD上的RA VPN部署。

## 必要條件

### 需求

思科建議您瞭解Firepower裝置管理器(FDM)上的遠端訪問虛擬專用網(RA VPN)配置。

### 授權

- Firepower威脅防禦(FTD)已在啟用匯出控制功能的智慧許可門戶中註冊 ( 以便啟用RA VPN配置頁籤 )
- 任何已啟用的AnyConnect許可證 ( APEX、Plus或僅VPN )

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行6.5.0-115版的Cisco FTD
- Cisco AnyConnect安全行動化使用者端版本4.7.01076

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。

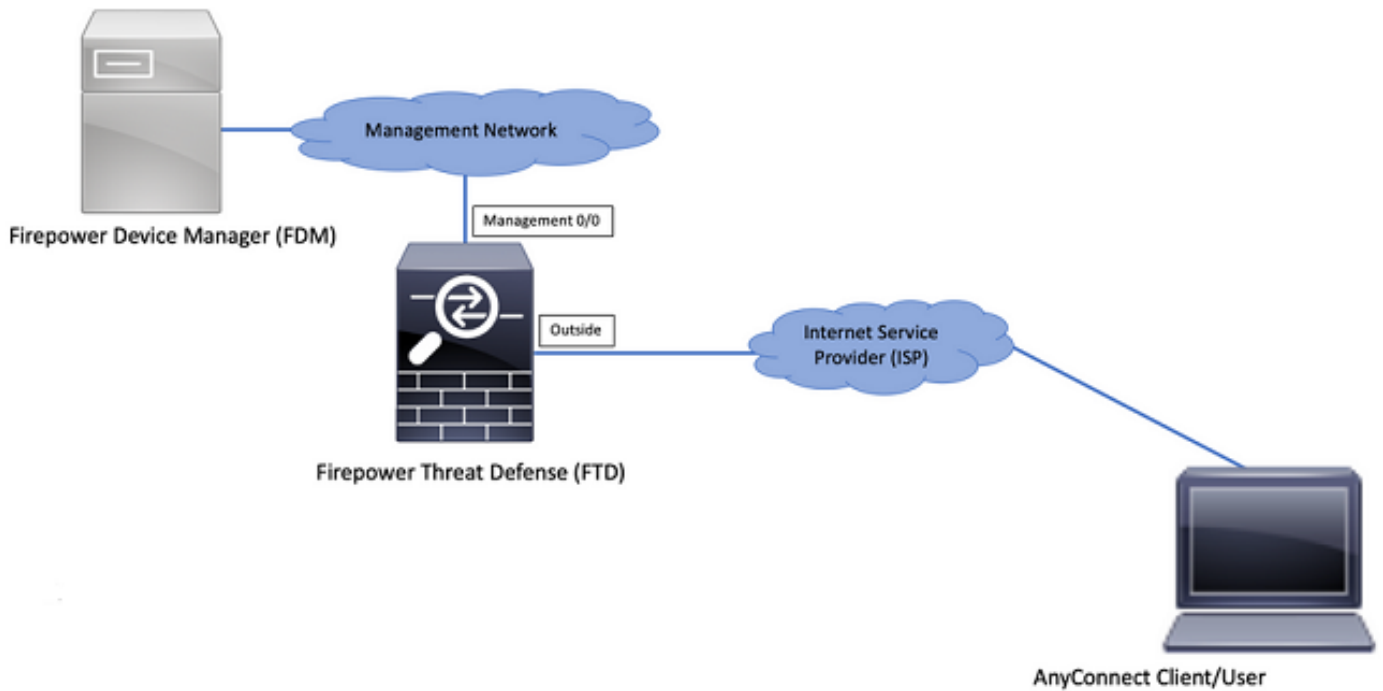
## 背景資訊

通過FDM配置FTD時，當您嘗試通過外部介面為AnyConnect客戶端建立連線時，會遇到一些困難，而通過同一介面訪問管理。這是FDM的已知限制。已針對此問題[提交增強請求CSCvm76499](#)。

## 設定

### 網路圖表

AnyConnect Client Authentication with use of Local (使用本地的AnyConnect客戶端身份驗證)。



### 驗證FTD上的授權

步驟 1. 驗證裝置是否已註冊到智慧許可，如下圖所示：

Firepower Device Manager

Monitoring Policies Objects Device: firepower

Model: Cisco Firepower Threat Defense for VMWa... Software: 6.5.0-115 VDB: 309.0 Rule Update: 2019-08-12-001-vrt High Availability: Not Configured

Inside Network Cisco Firepower Threat Defense for V... ISP/WAN/Gateway Internet DNS Server NTP Server Smart License

Interfaces: Connected, Enabled 3 of 4. View All Interfaces

Routing: There are no routes yet. Create the first static route

Updates: Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds. View Configuration

System Settings: Management Access, Logging Settings, DHCP Server, DNS Server, Management interface, Hostname, NTP, Cloud Services, Reboot/Shutdown, Traffic Settings, URL Filtering Preferences

Smart License: Registered. View Configuration

Backup and Restore: No files created yet. View Configuration

Troubleshoot: No files created yet. REQUEST FILE TO BE CREATED

Site-to-Site VPN: There are no connections yet. View Configuration

Remote Access VPN: Requires RA VPN license, No connections | 1 Group Policy. View Configuration

Advanced Configuration: Includes: FlexConfig, Smart CLI. View Configuration

Device Administration: Audit Events, Deployment History, Download Configuration. View Configuration

步驟 2. 驗證裝置上是否已啟用AnyConnect許可證，如下圖所示。

Device Summary  
Smart License

CONNECTED SUFFICIENT LICENSE
Last sync: 04 Apr 2020 02:10 PM
Next sync: 04 Apr 2020 02:20 PM
Go to Cloud Services

SUBSCRIPTION LICENSES INCLUDED

**Threat** ENABLE

Disabled by user

This License allows you to perform intrusion detection and prevention and file control. You must have this license to apply intrusion policies in access rules. You also must have this license to apply file policies that control files based on file type.

Includes: Intrusion Policy

**Malware** ENABLE

Disabled by user

This License allows you to perform Cisco Advanced Malware Protection (AMP) with AMP for Firepower and AMP Threat Grid. You must have this license to apply file policies that detect and block malware in files transmitted over your network.

Includes: File Policy

**URL License** ENABLE

Disabled by user

This license allows you to control web access based on URL categories and reputations, rather than by individual URL alone. You must have this license to deploy access rules that filter web traffic based on category and reputation.

Includes: URL Reputation

**RA VPN License** Type: APEX AND PLUS DISABLE

Enabled

Please select the license type that you purchased to enable remote access VPN. Note that Firepower Device Manager does not support any of the advanced features covered by the Apex license.

Includes: RA-VPN

PERPETUAL LICENSES INCLUDED

**Base License** ENABLED ALWAYS

Enabled

步驟 3. 驗證權杖中是否已啟用匯出控制功能，如下圖所示：

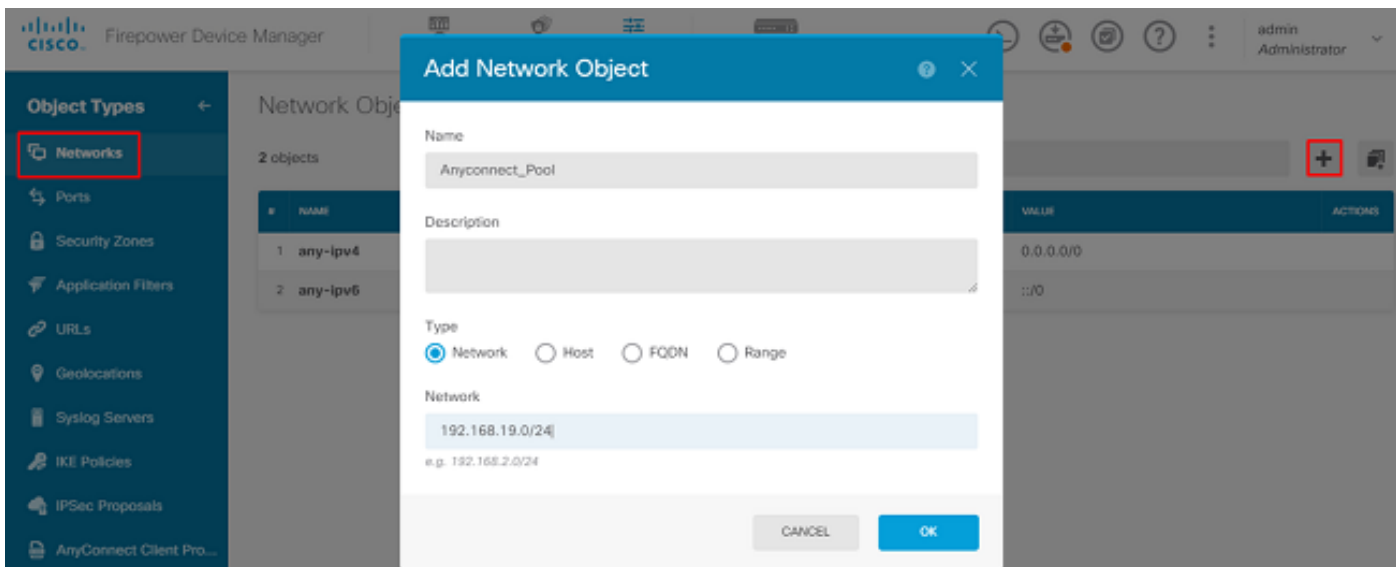
Device Summary  
Smart License

CONNECTED SUFFICIENT LICENSE
Last sync: 04 Apr 2020 02:10 PM
Next sync: 04 Apr 2020 02:20 PM

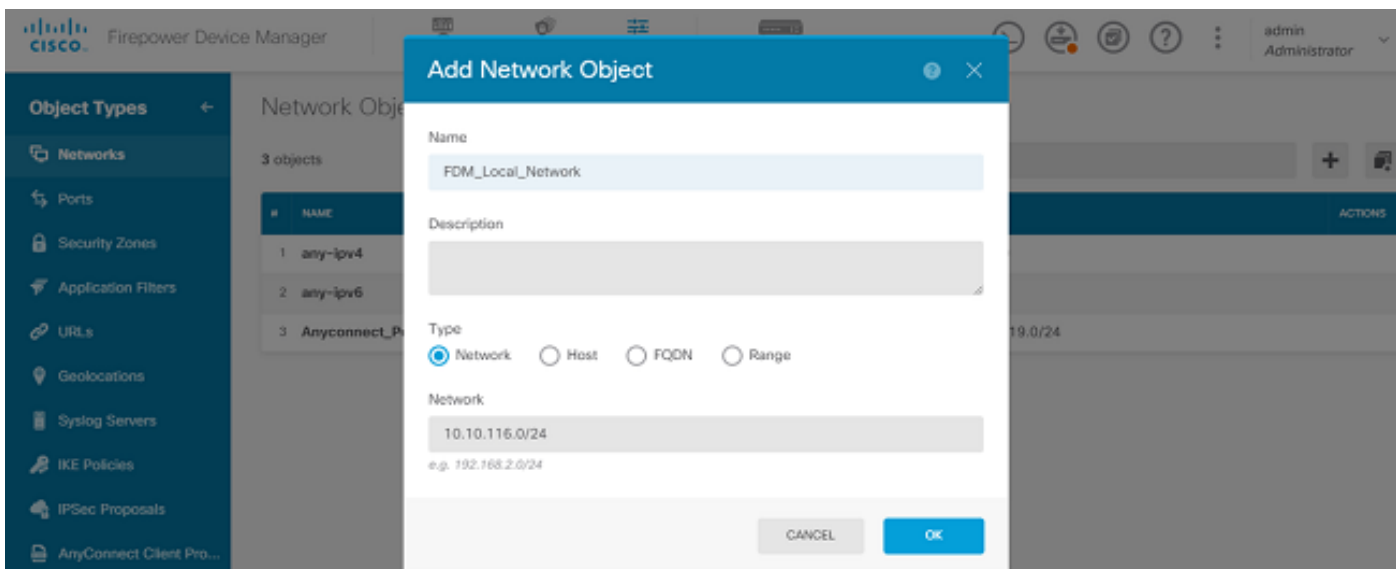
Assigned Virtual Account: SEC TAC  
Export-controlled features: Enabled  
Go to [Cisco Smart Software Manager](#).

## 定義受保護的網路

導航至 `Objects > Networks > Add new Network`. 通過FDM GUI配置VPN池和LAN網路。 建立VPN池以用於AnyConnect使用者的本地地址分配，如下圖所示：

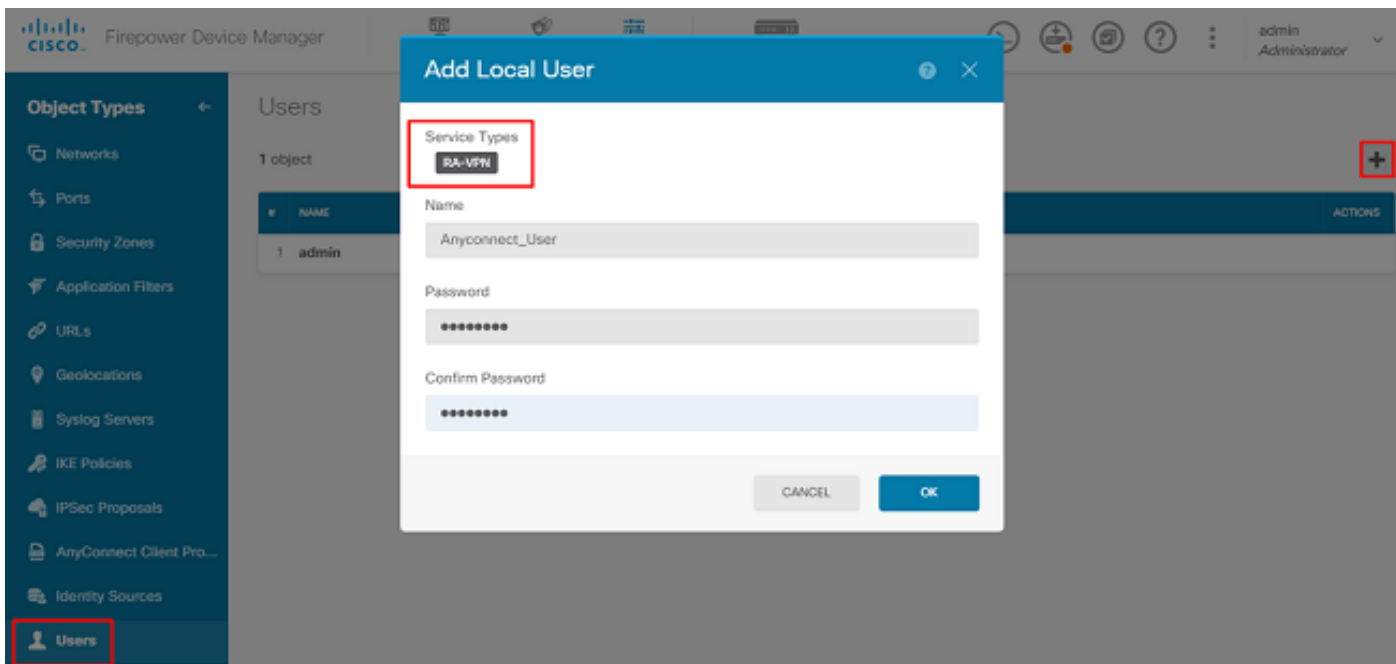


在FDM裝置後為本地網路建立對象，如下圖所示：



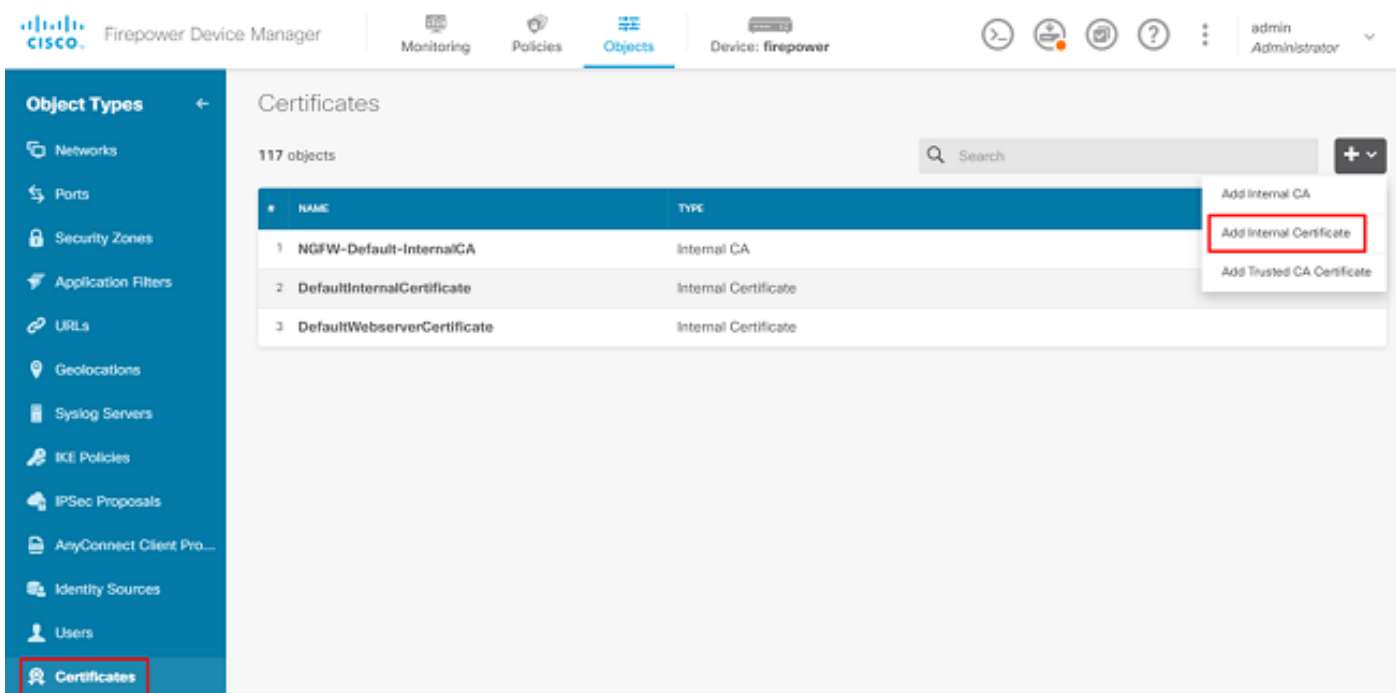
## 建立本地使用者

導航至 `Objects > Users > Add User`. 新增通過Anyconnect連線到FTD的VPN本地使用者。建立本地使用者，如下圖所示：



## 新增證書

導航至 Objects > Certificates > Add Internal Certificate. 設定憑證，如下圖所示：



上傳憑證和私鑰，如下圖所示：



Choose the type of internal certificate you want to create



### Upload Certificate and Key

Create a certificate from existing files.  
PEM and DER files are supported.



### Self-Signed Certificate

Create a new certificate that is signed  
by the device.

您可以透過複製和貼上或每個檔案的upload按鈕上傳憑證和金鑰，如下圖所示：

## Add Internal Certificate



Name

Anyconnect\_Certificate

SERVER CERTIFICATE (USER AGENT)

Paste certificate, or choose file:

UPLOAD CERTIFICATE

The supported formats are: PEM, DER.

```
wkM7QqtRuyzBzGhnoSebJkP/Hiky/Q+r6UrYSnv++UJSrg777/9NgonwTpLI/8/J
idGSN0b/ic6iPh2aGpB1Lra3MGCL1pJaRqxq3+1yBDsfVFCaKT9wWcnUveQd6LZp
k+iaN+V24yOj3vCJILihtxwdllqeSs8F8XdaL4LQObcTfZ/3YNBWqvwV2TL
-----END CERTIFICATE-----
```

CERTIFICATE KEY

Paste key, or choose file:

UPLOAD KEY

The supported formats are: PEM, DER.

```
QzYPpjKcGyEAqJ9nlk8sfPfmotyOwprlBEdwMMDeKLX3KDY58jviv1/8a/wsX+uz
3A7VQn6gA6ISWHgxHdmqYnD38P6kCuK/hQMUCqdIKUITXkh0ZpglQbfW2lJ0VD4M
gKugRI5t0Zva5j+bO5q0f8D/mtYYTBf8JGgqEfSju0Zsy2ifWtsbJrE=
-----END RSA PRIVATE KEY-----
```

CANCEL

OK

## 配置遠端訪問VPN

導航至 Remote Access VPN > Create Connection Profile. 在FDM上瀏覽RA VPN嚮導，如下圖所示：



The screenshot shows the Cisco Firepower Device Manager interface for a device named 'firepower'. At the top, there are navigation tabs for Monitoring, Policies, and Objects. The main dashboard is divided into several sections:

- Model:** Cisco Firepower Threat Defense for VMWa... (Software: 6.5.0-115, VDB: 309.0, Rule Update: 2019-08-12-001-vrt)
- High Availability:** Not Configured
- Network Diagram:** Shows an 'Inside Network' connected to the device via interface 'G1'. The device has interfaces 'G0/0', 'G0/1', and 'G0/2'. It is also connected to an 'Internet' cloud via an 'ESP/WAN/Gateway'. Services shown include DNS Server, NTP Server, and Smart License.
- Configuration Summary:**
  - Interfaces:** Connected, Enabled 3 of 4. [View All Interfaces](#)
  - Smart License:** Registered. [View Configuration](#)
  - Routing:** There are no routes yet. [Create the first static route](#)
  - Updates:** Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds. [View Configuration](#)
  - System Settings:** Management Access, Logging Settings, DHCP Server, DNS Server, Management Interface, Hostname, NTP, Cloud Services, Reboot/Shutdown, Traffic Settings, URL Filtering Preferences.
  - Backup and Restore:** No files created yet. [View Configuration](#)
  - Troubleshoot:** No files created yet. [REQUEST FILE TO BE CREATED](#)
  - Site-to-Site VPN:** There are no connections yet. [View Configuration](#)
  - Remote Access VPN:** Configured, No connections | 1 Group Policy. [View Configuration](#) (highlighted with a red border)
  - Advanced Configuration:** Includes: FlexConfig, Smart CLI. [View Configuration](#)
  - Device Administration:** Audit Events, Deployment History, Download Configuration. [View Configuration](#)

The screenshot shows the 'Remote Access VPN Connection Profiles' page in the Cisco Firepower Device Manager. The page has a left-hand navigation menu with 'RA VPN', 'Connection Profiles', and 'Group Policies'. The main content area displays a table with the following columns: NAME, AAA, GROUP POLICY, and ACTIONS. The table is currently empty, and a message states: 'There are no Remote Access Connections yet. Start by creating the first Connection.' A button labeled 'CREATE CONNECTION PROFILE' is highlighted with a red border.

建立連線設定檔並啟動組態，如下圖所示：

## Connection and Client Configuration

Specify how to authenticate remote users and the AnyConnect clients they can use to connect to the inside network.

### Connection Profile Name

*This name is configured as a connection alias, it can be used to connect to the VPN gateway*

Anyconnect

### Group Alias

Anyconnect

[Add Group Alias](#)

### Group URL

[Add Group URL](#)

選擇驗證方法，如下圖所示。本指南使用本地身份驗證。

## Primary Identity Source

### Authentication Type

AAA Only  Client Certificate Only  AAA and Client Certificate

### Primary Identity Source for User Authentication

LocalIdentitySource

### Fallback Local Identity Source

Please Select Local Identity Source

Strip Identity Source server from username

Strip Group from Username

---

## Secondary Identity Source

### Secondary Identity Source for User Authentication

Please Select Identity Source

### Advanced

---

### Authorization Server

Please select

### Accounting Server

Please select

選擇 Anyconnect\_Pool 對象，如下圖所示：

## Client Address Pool Assignment

### IPv4 Address Pool

Endpoints are provided an address from this pool



Anyconnect\_Pool

### IPv6 Address Pool

Endpoints are provided an address from this pool



### DHCP Servers



CANCEL

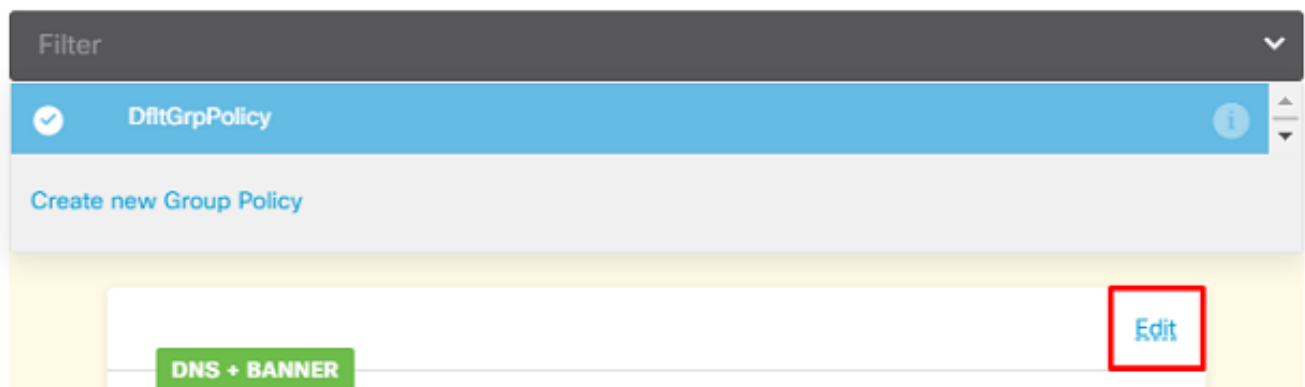
NEXT

預設組策略的摘要顯示在下一頁上。當您點選下拉選單並選擇以下選項時，可以建立新的組策略  
Create a new Group Policy. 在本指南中，使用預設組策略。選擇策略頂部的編輯選項，如下圖所示：

## Remote User Experience

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

### View Group Policy



在組策略中，新增分割隧道，以便連線到Anyconnect的使用者僅通過Anyconnect客戶端傳送目的地為內部FTD網路的流量，而所有其他流量都流出使用者的ISP連線，如下圖所示：

## Corporate Resources (Split Tunneling)

### IPv4 Split Tunneling

Allow specified traffic over tunnel ▼

### IPv6 Split Tunneling

Allow all traffic over tunnel ▼

### IPv4 Split Tunneling Networks

+

FDM\_Local\_Network

在下一頁上，選擇 `Anyconnect_Certificate` 已新增到證書部分。接下來，選擇FTD偵聽AnyConnect連線的介面。為解密的流量選擇旁路訪問控制策略(`sysopt permit-vpn`)。這是一個可選命令，如果 `sysopt permit-vpn` 未選擇。必須建立訪問控制策略，以允許來自Anyconnect客戶端的流量訪問內部網路，如下圖所示：

## Global Settings

These settings control the basic functioning of the connection. Changes to any of these options apply to all connection profiles; you cannot configure different settings in different profiles.

### Certificate of Device Identity

Anyconnect\_Certificate ▼

### Outside Interface

outside (GigabitEthernet0/0) ▼

### Fully-qualified Domain Name for the Outside Interface

e.g. `ravpn.example.com`

### Access Control for VPN Traffic

Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic

Bypass Access Control policy for decrypted traffic (`sysopt permit-vpn`)

NAT豁免可以手動配置在 `Policies > NAT` 也可以由嚮導自動配置。選擇Anyconnect客戶端訪問所需的內部介面和網路，如下圖所示。

## NAT Exempt



### Inside Interfaces

The interfaces through which remote access VPN users can connect to the internal networks



inside (GigabitEthernet0/1)

### Inside Networks

The internal networks remote access VPN users are allowed to use. The IP versions of the internal networks and address pools must match, either IPv4, IPv6, or both.



FDM\_Local\_Network

為使用者可以連線的每個作業系統(Windows/Mac/Linux)選擇Anyconnect軟體包，如下圖所示。

## AnyConnect Package

If a user does not already have the right AnyConnect package installed, the system will launch the AnyConnect installer when the client authenticates for the first time. The user can then install the package from the system.

You can download AnyConnect packages from [software.cisco.com](https://software.cisco.com).

You must have the necessary AnyConnect software license.

### Packages

UPLOAD PACKAGE



Windows: anyconnect-win-4.7.04056-webdeploy-k9.pkg

BACK

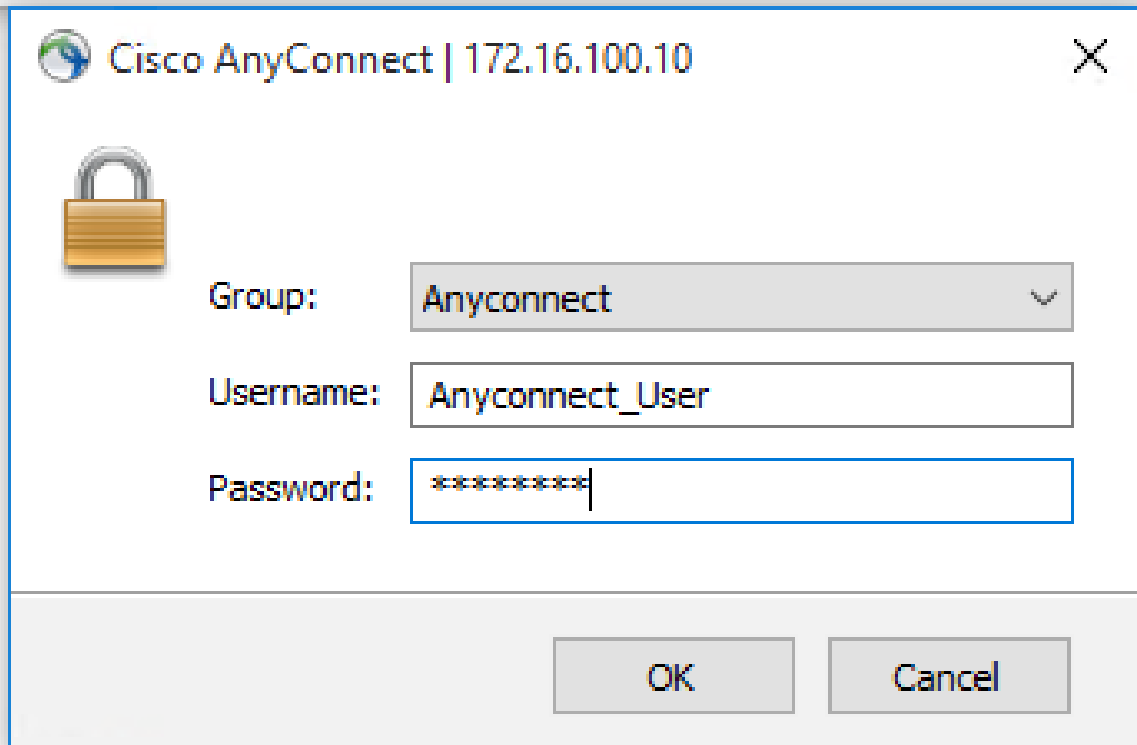
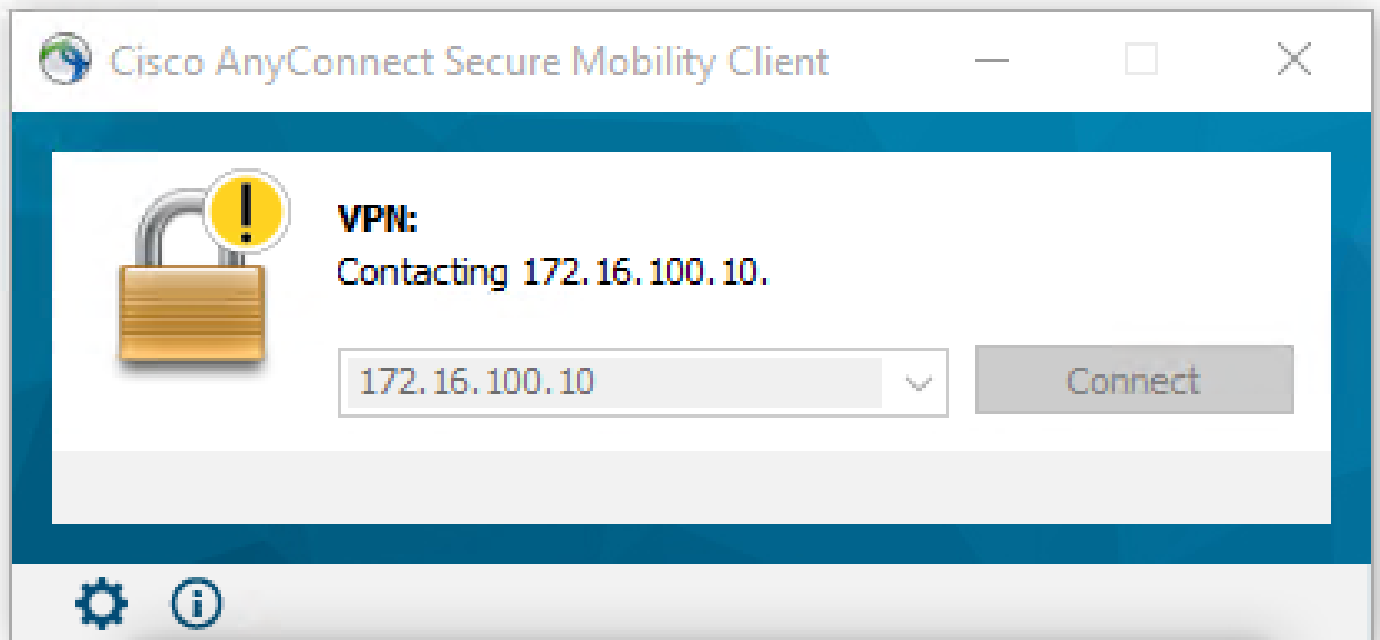
NEXT

最後一頁提供整個配置的摘要。確認已設定正確的引數，然後點選Finish (完成) 按鈕並部署新配置。

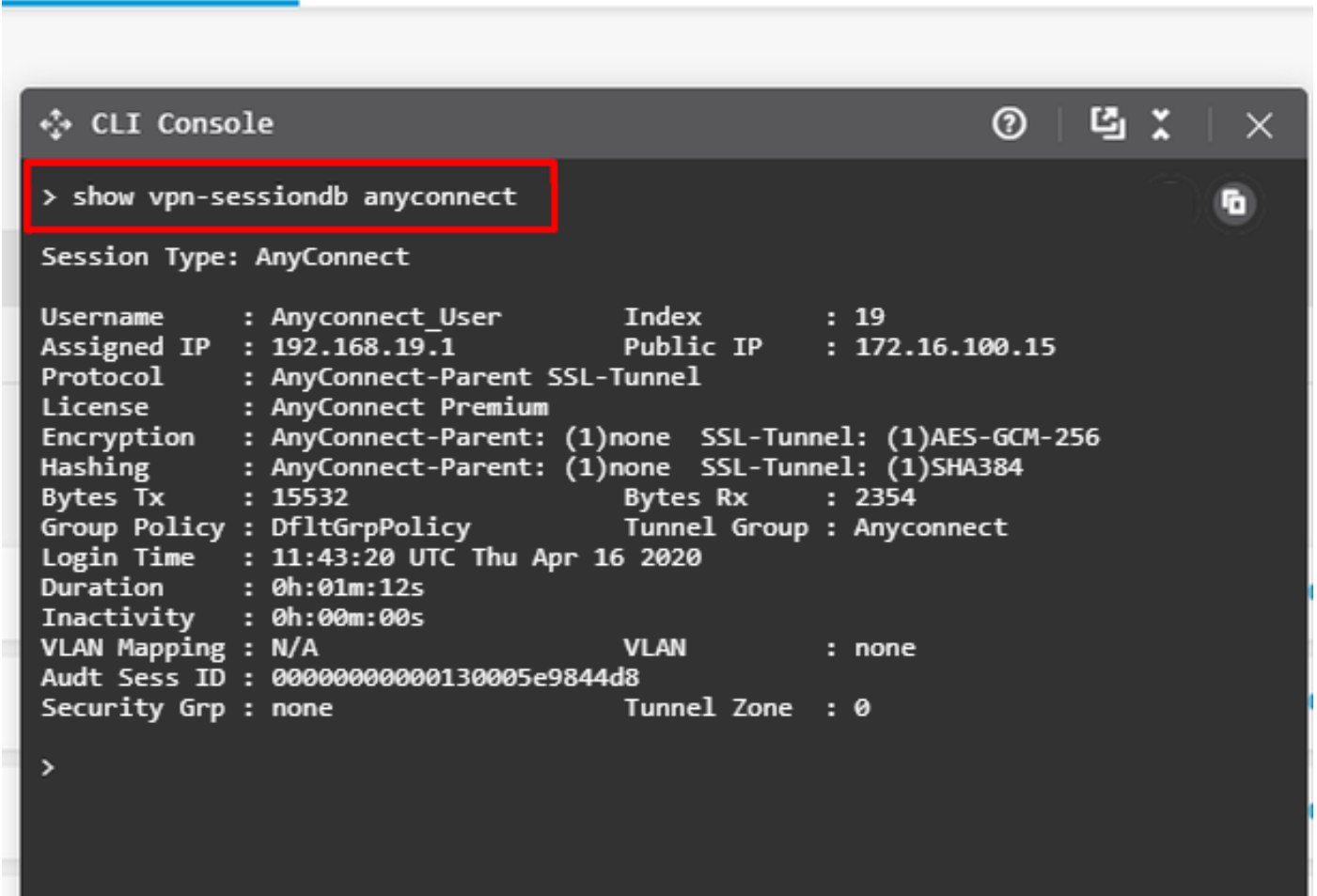
## 驗證

使用本節內容，確認您的組態是否正常運作。

部署配置後，嘗試連線。如果您的FQDN解析為FTD的外部IP，請在Anyconnect連線框中輸入它。在本範例中，使用FTD的外部IP位址。使用在FDM的objects部分中建立的使用者名稱/密碼，如下圖所示。



從FDM 6.5.0起，無法通過FDM GUI監視Anyconnect使用者。唯一的選項是通過CLI監控Anyconnect使用者。也可使用FDM GUI的CLI控制檯驗證使用者已連線。使用此命令，`Show vpn-sessiondb anyconnect`.



同一命令可以直接從CLI運行。

```
> show vpn-sessiondb anyconnect
```

Session Type: AnyConnect

```
Username      : Anyconnect_User      Index      : 15
Assigned IP   : 192.168.19.1         Public IP  : 172.16.100.15
Protocol      : AnyConnect-Parent SSL-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384
Bytes Tx      : 38830                Bytes Rx   : 172
Group Policy  : DfltGrpPolicy        Tunnel Group : Anyconnect
Login Time    : 01:08:10 UTC Thu Apr 9 2020
Duration      : 0h:00m:53s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                  VLAN       : none
Audt Sess ID  : 000000000000f0005e8e757a
Security Grp  : none                  Tunnel Zone : 0
```



## 疑難排解

本節提供的資訊用於對組態進行疑難排解。

如果使用者無法使用SSL連線到FTD，請執行以下步驟以隔離SSL交涉問題：

1. 驗證是否可通過使用者的電腦對FTD以外的IP位址執行Ping。
2. 使用外部監聽器驗證TCP三次握手是否成功。

## AnyConnect客戶端問題

本節提供了對兩個最常見的AnyConnect VPN客戶端問題進行故障排除的指南。AnyConnect客戶端故障排除指南可以在以下位置找到：[AnyConnect VPN客戶端故障排除指南](#)。

### 初始連線問題

如果使用者存在初始連線問題，請啟用調試 `webvpn` FTD上的AnyConnect並分析偵錯訊息。偵錯必須在FTD的CLI上執行。使用命令 `debug webvpn anyconnect 255`。

從客戶端電腦收集DART捆綁包，以便從AnyConnect獲取日誌。有關如何收集DART捆綁包的說明可以在以下位置找到：[收集DART捆綁包](#)。

### 流量特定的問題

如果連線成功，但流量通過SSL VPN隧道失敗，請檢視客戶端上的流量統計資訊，以驗證客戶端正在接收和傳輸流量。詳細的客戶端統計資訊在AnyConnect的所有版本中均可用。如果使用者端顯示正在傳送和接收流量，請檢查FTD以瞭解已接收和已傳輸流量。如果FTD套用過濾器，則會顯示過濾器名稱，您可以檢視ACL專案，以檢查您的流量是否遭捨棄。使用者遇到的常見流量問題包括：

- FTD背後的路由問題 — 內部網路無法將封包路由回指派的IP位址和VPN使用者端
- 訪問控制清單阻止流量
- VPN流量未繞過網路地址轉換

有關由FDM管理的FTD上的遠端訪問VPN的詳細資訊，請在此處找到完整的配置指南：[由FDM管理的遠端訪問FTD](#)。

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。