

# 在FMC管理的FTD上設定安全使用者端憑證驗證

## 目錄

---

### [簡介](#)

### [必要條件](#)

#### [需求](#)

#### [採用元件](#)

### [設定](#)

#### [網路圖表](#)

#### [組態](#)

##### [a. 建立/匯入用於伺服器驗證的憑證](#)

##### [b. 增加受信任/內部CA證書](#)

##### [c. 配置VPN使用者的地址池](#)

##### [d. 上傳安全客戶端映像](#)

##### [e. 建立和上傳XML配置檔案](#)

#### [遠端訪問VPN配置](#)

### [驗證](#)

### [疑難排解](#)

---

## 簡介

本檔案介紹在由Firepower管理中心(FMC)透過憑證驗證管理的Firepower威脅防禦(FTD)上設定遠端存取VPN的程式。

作者：Dolly Jain和Rishabh Aggarwal，思科TAC工程師。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 手動註冊憑證及SSL的基本概念
- FMC
- 遠端訪問VPN的基本身份驗證知識
- 第三方證書頒發機構(CA)，如Entrust、Geotrust、GoDaddy、Thawte和VeriSign

### 採用元件

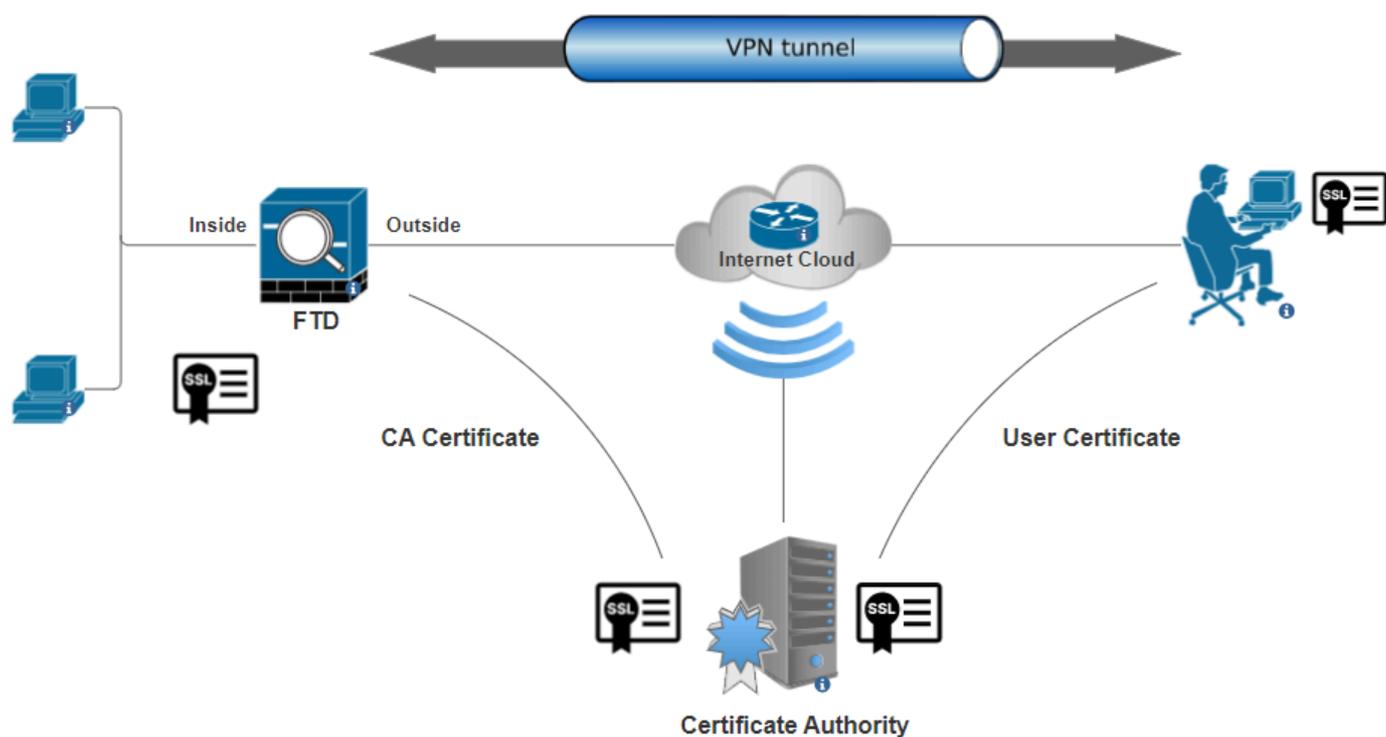
本檔案中的資訊是根據以下軟體版本：

- 安全Firepower威脅防禦7.4.1版
- Firepower管理中心(FMC)版本7.4.1
- 安全使用者端5.0.05040版
- Microsoft Windows Server 2019作為CA伺服器

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。

## 設定

### 網路圖表



網路圖表

### 組態

- 建立/匯入用於伺服器驗證的憑證



附註：在FMC上，產生CSR之前需有CA憑證。如果從外部源（OpenSSL或第三方）生成CSR，則手動方法失敗，必須使用PKCS12證書格式。

---

步驟 1. 導航到 `Devices > Certificates`，然後按一下 `Add`。選擇 `Device`（裝置），然後點選 `Cert Enrollment`（證書註冊）下的加號（+）。

## Add New Certificate



Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device\*:

Cert Enrollment\*:

Cancel

Add

增加證書註冊

步驟 2. 在CA Information下，選擇「Enrollment Type」作為Manual，並貼上用於簽署CSR的證書頒發機構(CA)證書。

## Add Cert Enrollment



Name\*

ssl\_certificate

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

Manual

CA Only

*Check this option if you do not require an identity certificate to be created from this CA*

CA Certificate:

```
HQYDVQQDEZXIEWRyYw50S
UQgU2VydMvYlENBIE8xMIIBlj
ANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEA6
huZbDVWWMGj7XbFZQWI+uhh
0SleWhO8rI79MV4+7ZSj2
Lxos5e8za0H1JVVzTNPaup2G
o438C5zeaqaGtyUshV8D0xw
UiWyamspTao7PjjuC
h81+tp9z76rp1irjNMh5o/zeJ0
h3Kag5zQG9sfI7J7ihLnTFbArj
N7ID=ZeeQw
```

Validation Usage:

IPsec Client  SSL Client  SSL Server

Skip Check for CA flag in basic constraints of the CA Certificate

Cancel

Save

增加CA資訊

步驟 3.對於驗證用法，選擇IPsec Client, SSL Client和Skip Check for CA flag in basic constraints of the CA Certificate。

步驟 4.在Certificate Parameters下，填寫主題名稱詳細資訊。

## Add Cert Enrollment



Name\*

ssl\_certificate

Description

CA Information

Certificate Parameters

Key

Revocation

Include FQDN:

Don't use FQDN in certificate

Include Device's IP Address:

Common Name (CN):

certauth.cisco.com

Organization Unit (OU):

TAC

Organization (O):

Cisco

Locality (L):

Bangalore

State (ST):

KA

Country Code (C):

IN

Email (E):

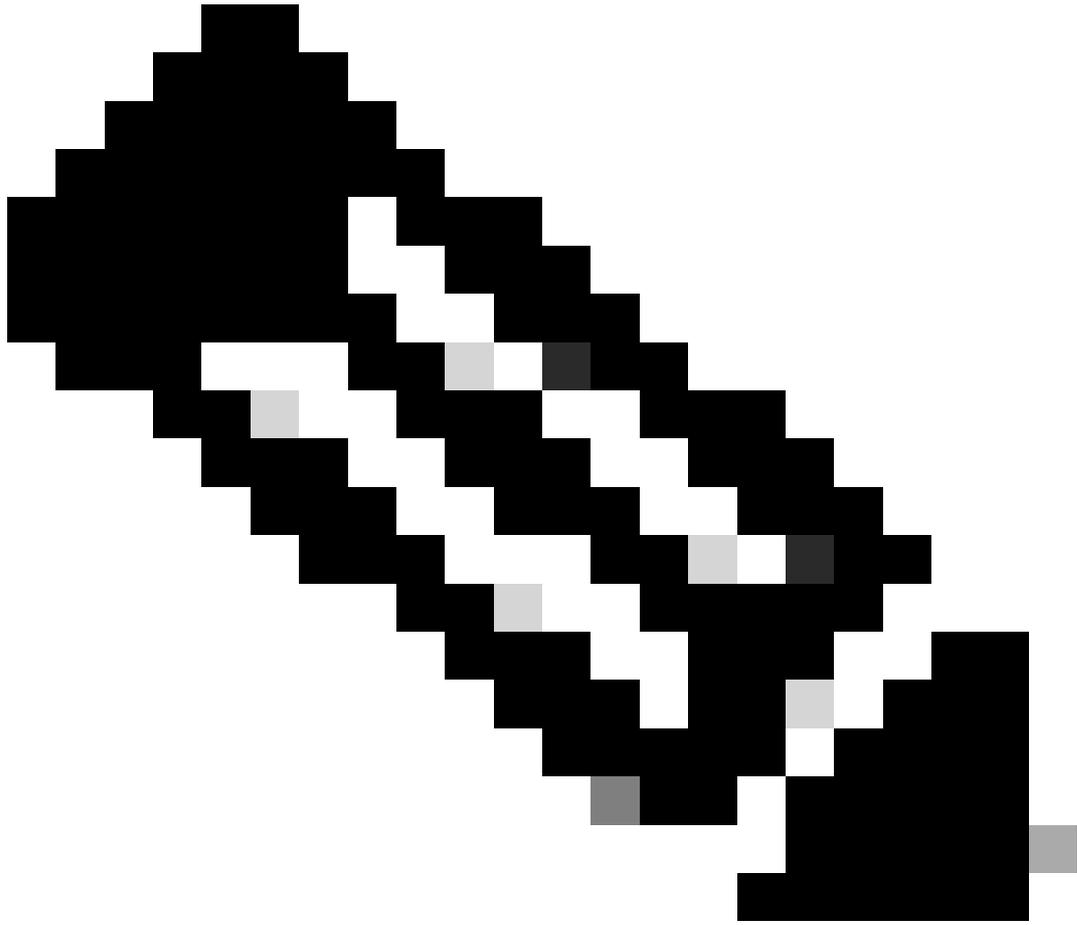
Include Device's Serial Number

Cancel

Save

增加證書引數

步驟 5. 在Key下選擇金鑰型別為RSA且具有金鑰名稱和大小。按一下Save。



注意：對於RSA金鑰型別，最小金鑰大小為2048位。



## Add Cert Enrollment



Name\*  
ssl\_certificate

Description

CA Information   Certificate Parameters   **Key**   Revocation

**Key Type:**  
 RSA    ECDSA    EdDSA

Key Name:\*  
rsa\_key

**Key Size:**  
2048 ▼

▼ Advanced Settings

Ignore IPsec Key Usage

Cancel   **Save**

增加RSA金鑰

步驟 6. 在 Cert Enrollment 下，從剛建立的下拉選單中選擇信任點，然後按一下 Add。

## Add New Certificate



Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device\*:

FTD-A-7.4.1

Cert Enrollment\*:

ssl\_certificate +

Cert Enrollment Details:

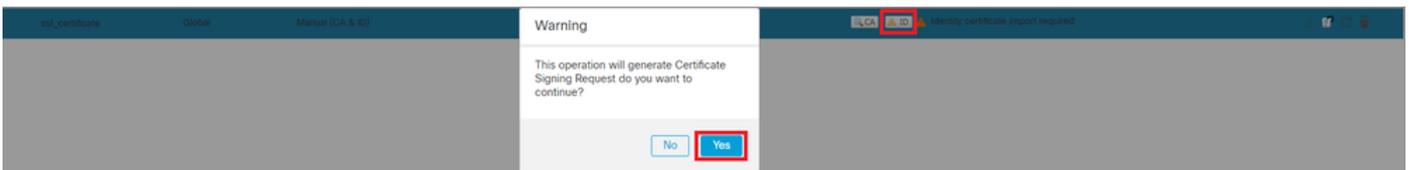
Name: ssl\_certificate  
Enrollment Type: Manual (CA & ID)  
Enrollment URL: N/A

Cancel

Add

增加新證書

步驟 7. 點選ID，然後點選Yes，顯示進一步的提示，生成CSR。



產生CSR

步驟 8. 複製CSR並由憑證授權單位簽署。身份證書由CA發佈之後，透過按一下Browse Identity Certificate和Import進行導入。

# Import Identity Certificate



## Step 1

Send Certificate Signing Request (CSR) to the Certificate Authority.

Certificate Signing Request (Copy the CSR below and send to the Certificate Authority):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIEyTCCArECAQAwVTEMMAoGA1UECwwDVVEFDMQ4wDAYDVQQKDAVDaXNjbzEbMBkG
A1UEAwwSY2VydGF1dGguY2lzY28uY29tMQswCQYDVQQIDAJLQTELMakGA1UEBhMC
SU4wggliMA0GCsqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDNZr431mtYG+f1bLFK
WY9Zd9wTaJfqs87FtAW7+n4UuxLDws54R/txe9teX/65uSyY8/bxKfdsgMq5rawO
3dogCVQjtAtel+95np1/myzFOZZRWfeBdK/H1plLEdR4X6ZlnM5fNA/GLV9MnPoP
ppzi0ulIbVmb5iKQexllaur/e3PBccc3eC57e+D3QhKQ9SC7um8ulwueF+70fKYe
```

## Step 2

Once certificate authority responds back with identity certificate file, import it to device.

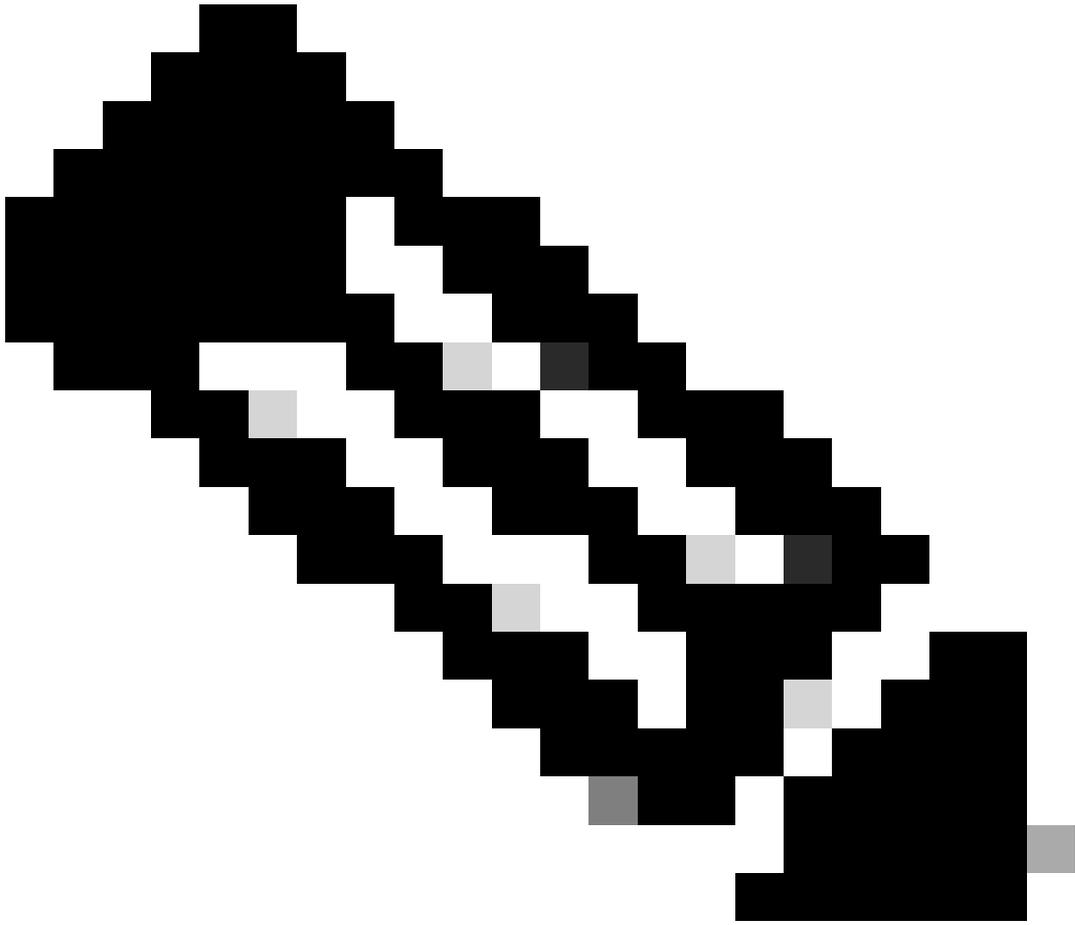
Identity Certificate File:

[Browse Identity Certificate](#)

[Cancel](#)

[Import](#)

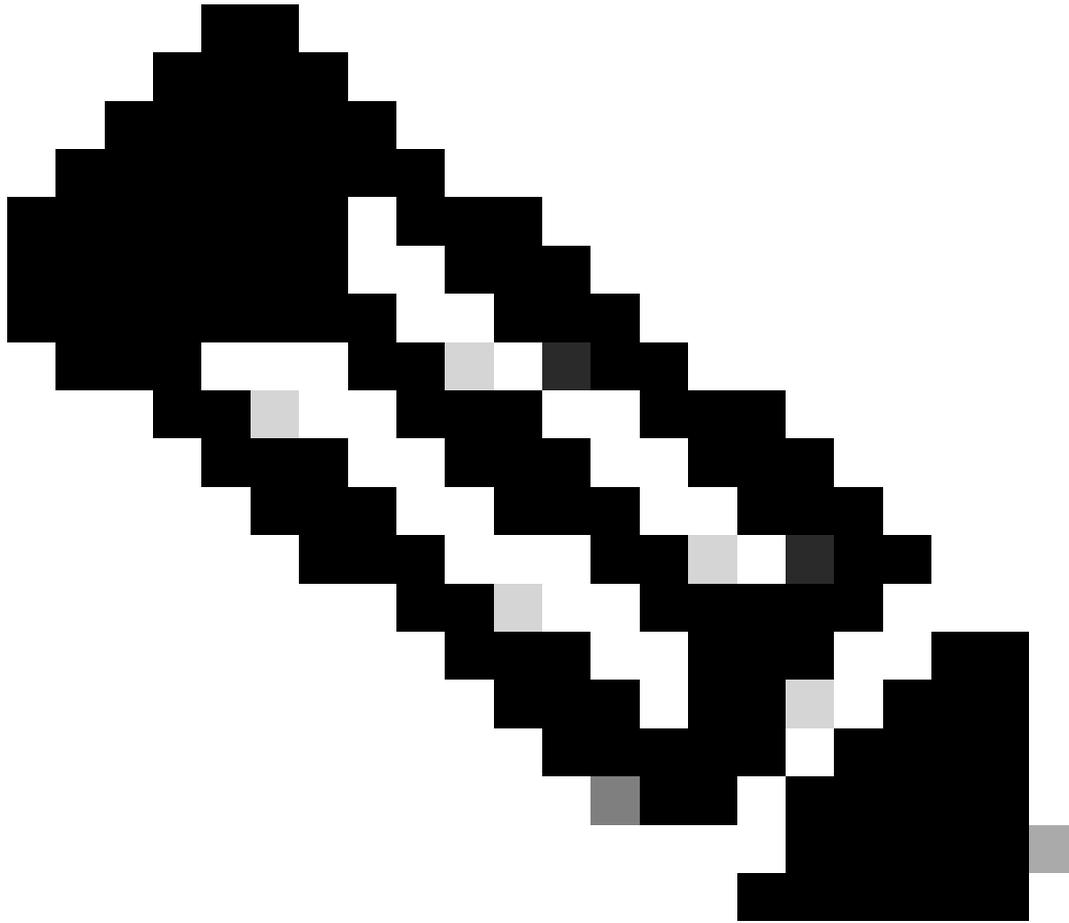
匯入ID憑證



**注意：**如果頒發ID證書需要時間，則可在以後重複步驟7。這將生成相同的CSR，我們可以導入ID證書。

---

#### **b.增加受信任/內部CA證書**



**注意：**如果步驟(a)「**建立/匯入用於伺服器驗證的憑證**」中使用的憑證授權(CA)也會發出使用者憑證，您可以跳過步驟(b)，「**新增受信任/內部CA憑證**」。不需要再次增加相同的CA證書，也必須避免這種情況。如果再次增加相同的CA證書，則信任點配置為「validation-usage none」，這可能會影響RAVPN的證書身份驗證。

---

步驟 1. 導航到Devices > Certificates，然後按一下Add。

選擇Device (裝置)，然後點選Cert Enrollment (證書註冊) 下的加號(+)

此處，「auth-risaggar-ca」用於頒發身份/使用者證書。

General

Details

Certification Path



### Certificate Information

**This certificate is intended for the following purpose(s):**

- All issuance policies
- All application policies

**Issued to:** auth-risaggar-ca

**Issued by:** auth-risaggar-ca

**Valid from** 04-03-2023 **to** 04-03-2033

Issuer Statement

OK

*auth-risaggar-ca*

步驟 2. 輸入信任點名稱，然後在CA information下選擇Manual作為註冊型別。

步驟 3. 選中CA Only並貼上採用pem格式的受信任/內部CA證書。

步驟 4. 選中Skip Check for CA flag in basic constraints of the CA Certificate並按一下Save。

### Add Cert Enrollment ?

Internal\_CA

Description

CA InformationCertificate ParametersKeyRevocation

Enrollment Type: Manual

CA Only

*Check this option if you do not require an identity certificate to be created from this CA*

CA Certificate:

```
-----BEGIN CERTIFICATE-----  
--  
MIIG1jCCBL6gAwIBAgIQQAFu  
+wogXPrr4Y9x1zq7eDANBgk  
qhkiG9w0BAQsFADBK  
MQswCQYDVQQGEwJVUzES  
MBAGA1UEChMJSWRlbiRydX  
N0MScwJQYDVQQDEx5JZGV  
u  
VHJ1c3QgQ29tbWVyY2lhbCB  
Sb290IENBIDUwHhcNMTkxMj
```

Validation Usage:  IPsec Client  SSL Client  SSL Server

Skip Check for CA flag in basic constraints of the CA Certificate

Cancel Save

步驟 5. 在Cert Enrollment下，從剛建立的下拉選單中選擇信任點，然後按一下Add。

## Add New Certificate



Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device\*:

Cert Enrollment\*:

 +

Cert Enrollment Details:

Name: Internal\_CA  
Enrollment Type: Manual (CA Only)  
Enrollment URL: N/A

Cancel

Add

增加內部CA

步驟 6.之前增加的證書顯示為：

Internal_CA	Global	Manual (CA Only)	Mar 4, 2033	CA ID	⌵ ⌶ ⌷ ⌸
-------------	--------	------------------	-------------	-------	---------

已增加證書

### c.配置VPN使用者的地址池

步驟 1.導航到Objects > Object Management > Address Pools > IPv4 Pools。

步驟 2.輸入名稱及帶掩碼的IPv4地址範圍。

## Edit IPv4 Pool



Name\*

vpn\_pool

Description

IPv4 Address Range\*

10.20.20.1-10.20.20.130

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask\*

255.255.255.0

Allow Overrides

**i** Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

▶ Override (0)

Cancel

Save

增加IPv4池

### d.上傳安全客戶端映像

步驟 1. 根據OS從[思科軟體](#)站點下載webdeploy安全客戶端映像。

步驟 2. 導航到Objects > Object Management > VPN > Secure Client File > Add Secure Client File。

步驟 3. 輸入名稱，然後從磁碟中選擇Secure Client檔案。

步驟 4. 選取檔案型別作為Secure Client Image，然後按一下Save。

# Edit Secure Client File



Name:\*

File Name:\*

File Type:\*

Description:

增加安全客戶端映像

## e. 建立和上傳XML配置檔案

步驟 1. 從[Cisco軟體](#)站點下載並安裝Secure Client Profile Editor。

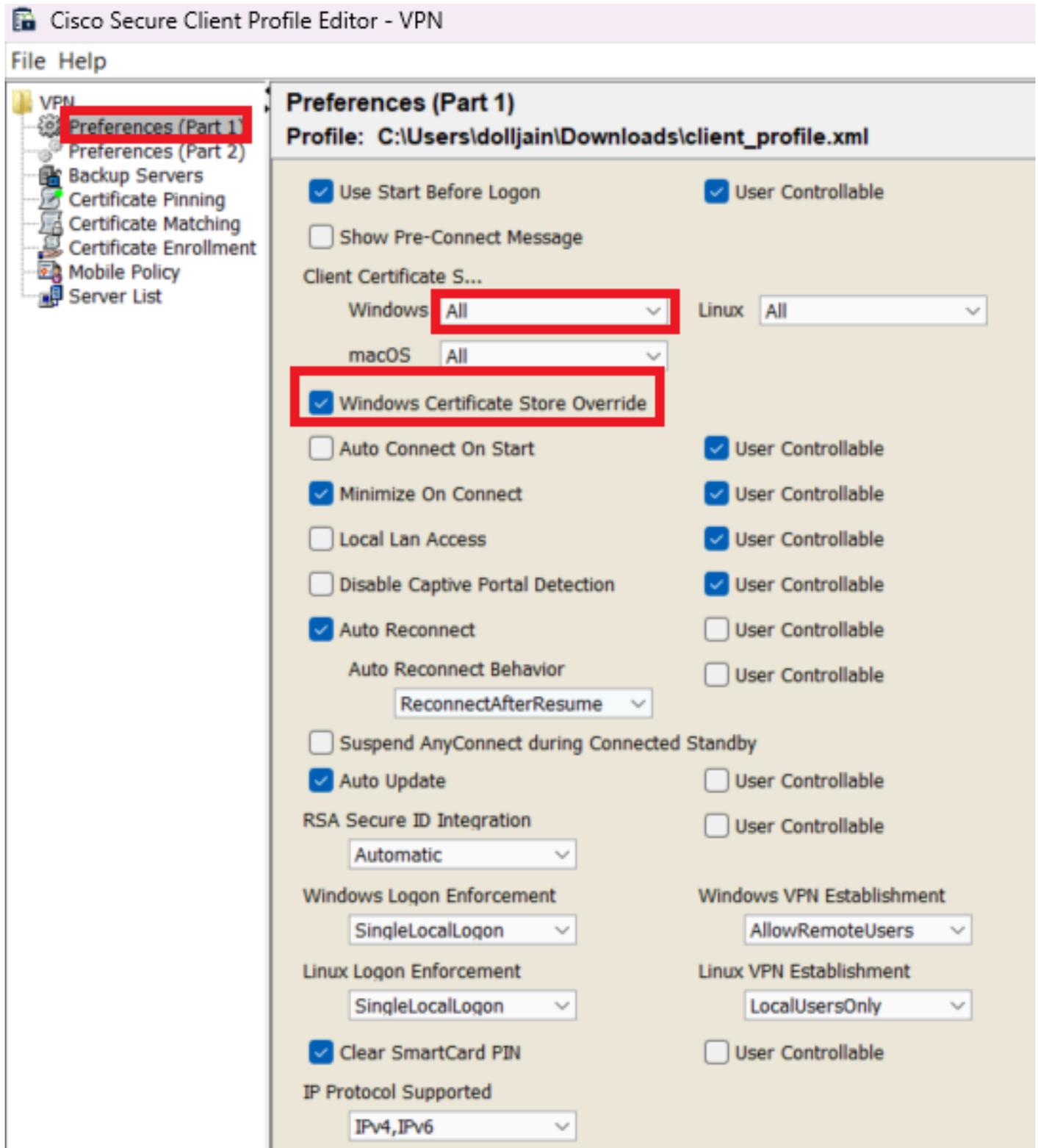
步驟 2. 建立新配置檔案並從Client Certificate Selection下拉選單中選擇All。它主要控制Secure Client可以使用哪些證書儲存區來儲存和讀取證書。

其他兩個可用選項為：

- 電腦 - 安全客戶端被限制為在Windows本地電腦證書儲存上查詢證書。
- User - Secure Client受限於在本地Windows使用者證書儲存上查詢證書。

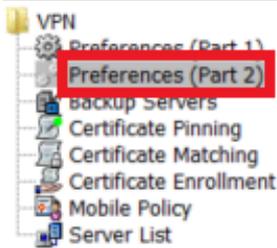
將證書儲存覆蓋設定為True。

這允許管理員指示Secure Client利用Windows電腦（本地系統）證書儲存中的證書進行客戶端證書身份驗證。憑證存放區覆寫僅適用於SSL，依預設，UI處理作業會在此起始連線。使用IPSec/IKEv2時，安全客戶端配置檔案中的此功能不適用。



加入偏好設定（第1部分）

步驟3.（可選）取消選中Disable Automatic Certificate Selection，因為它避免了提示使用者選擇身份驗證證書。



## Preferences (Part 2)

Profile: C:\Users\dolljain\Downloads\client\_profile.xml

Disable Automatic Certificate Selection

User Controllable

Proxy Settings

Native

User Controllable

Public Proxy Server Address:

Note: Enter public Proxy 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)

Performance Improvement Threshold (%)

Automatic VPN Policy

Trusted Network Policy

Disconnect

Untrusted Network Policy

Connect

Bypass connect upon VPN session timeout

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://

Add

Delete

Certificate Hash:

Set

Disable interfaces without trusted server connectivity while in truste...

Always On

(More Information)

Allow VPN Disconnect

Allow access to the following hosts with VPN disconn...

Connect Failure Policy

Closed

Allow Captive Portal Remediation

Remediation Timeout (min.)

Apply Last VPN Local Resource Rules

Captive Portal Remediation Browser Failover

Allow Manual Host Input

PPP Exclusion

Disable

User Controllable

PPP Exclusion Server IP

User Controllable

Enable Scripting

User Controllable

Terminate Script On Next Event

Enable Post SBL On Connect Script

Retain VPN on Logoff

User Enforcement

Same User Only

Authentication Timeout (seconds)

注意：安全客戶端使用此ACL向內部資源增加安全路由。

步驟 2. 導航到 Devices > VPN > Remote Access，然後按一下 Add。

步驟 3. 輸入設定檔的名稱，然後選取 FTD 裝置，再按下一步。

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 Secure Client — 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

Q Search

- FTD-A-7.4.1
- FTD-B-7.4.0
- FTD-ZTNA-7.4.1

Add

Selected Devices

- FTD-A-7.4.1

### Before You Start

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

Authentication Server

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

Secure Client Package

Make sure you have Secure Client 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.

新增設定檔名稱

步驟 4. 在「Authentication, Authorization and Accounting (AAA)」下，輸入 Connection Profile Name 並選擇 Client Certificate Only 「Authentication Method」。

## 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:\*

**i** 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:  Map specific field  Use entire DN (Distinguished Name) as username

Primary Field:

Secondary Field:

Authorization Server:  +  
(Realm or RADIUS)

Accounting Server:  +  
(RADIUS)

選取驗證方法

步驟 5. 按一下 Client Address Assignment 下的 Use IP Address Pools 並選擇之前建立的 IPv4 地址池。

## 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

IPv4 Address Pools:  

IPv6 Address Pools:  

選擇客戶端地址分配

步驟 6. 編輯組策略。

## Group Policy:

---

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.

Group Policy:\*  +  
[Edit Group Policy](#)

編輯組策略

步驟 7. 導航到 General > Split Tunneling，選擇 Tunnel networks specified below，然後在 Split Tunnel Network List Type 下選擇 Standard Access List。

選擇之前建立的 ACL。

## Edit Group Policy



Name:\*

DfltGrpPolicy

Description:

General

Secure Client

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

IPv4 Split Tunneling:

Tunnel networks specified below ▼

IPv6 Split Tunneling:

Allow all traffic over tunnel ▼

Split Tunnel Network List Type:

Standard Access List  Extended Access List

Standard Access List:

Split\_ACL ▼ +

DNS Request Split Tunneling

DNS Requests:

Send DNS requests as per split t ▼

Domain List:

Cancel

Save

增加分割隧道

步驟 8. 導航到 Secure Client > Profile，選擇 Client Profile，然後按一下 Save。

# Edit Group Policy



Name:\*

DfltGrpPolicy

Description:

General

Secure Client

Advanced

## Profile

Management Profile

Client Modules

SSL Settings

Connection Settings

Custom Attributes

Secure Client profiles contains settings for the VPN client functionality and optional features. The Firewall Threat Defense deploys the profiles during Secure Client connection.

Client Profile:

Anyconnect\_Profile-5-0-05040 +

Standalone profile editor can be used to create a new or modify existing Secure Client profile. You can download the profile editor from [Cisco Software Download Center](#).

增加安全客戶端配置檔案

步驟 9. 點選Next，然後選擇Secure Client Image，然後點選Next。

## Secure Client Image

The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download Secure Client packages from [Cisco Software Download Center](#).

Show Re-order buttons +

<input type="checkbox"/>	Secure Client File Object Name	Secure Client Package Name	Operating System
<input checked="" type="checkbox"/>	AnyconnectWin-5.0.05040	cisco-secure-client-win-5.0.05040-webde...	Windows

增加安全客戶端映像

步驟 10. 選擇VPN訪問的網路介面，選擇Device Certificates並選中sysopt permit-vpn，然後按一下Next。

## Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:\*  +  
 Enable DTLS on member interfaces

⚠ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

## Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:\*  +  
 Enroll the selected certificate object on the target devices

## Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

- Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)  
*This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.*

為VPN流量增加訪問控制

步驟 11.最後，檢視所有配置並按一下Finish。

## Remote Access VPN Policy Configuration

---

Firewall Management Center will configure an RA VPN Policy with the following settings

Name:	RAVPN
Device Targets:	FTD-B-7.4.0
Connection Profile:	RAVPN-CertAuth
Connection Alias:	RAVPN-CertAuth
AAA:	
Authentication Method:	Client Certificate Only
Username From Certificate:	-
Authorization Server:	-
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	vpn_pool
Address Pools (IPv6):	-
Group Policy:	DfltGrpPolicy
Secure Client Images:	AnyconnectWin-5.0.05040
Interface Objects:	outside-zone
Device Certificates:	ssl_certificate

### Device Identity Certificate Enrollment

---

Certificate enrollment object 'ssl\_certificate' is not installed on one or more targeted devices. Certificate installation will be initiated on the targeted devices on finishing the wizard. Go to the [Certificates](#) page to check the status of the installation.

遠端訪問VPN策略配置

步驟 12.完成遠端訪問VPN的初始設定後，編輯建立的連線配置檔案，並轉到Aliases。

步驟 13.透過點選加號圖示(+)配置group-alias。

### Edit Connection Profile

Connection Profile:\* RAVPN-CertAuth

Group Policy:\* DfltGrpPolicy +

[Edit Group Policy](#)

Client Address Assignment   AAA   **Aliases**

Alias Names:

Incoming users can choose an alias name upon first login. Aliases from all connections configured on this device can be turned on or off for display.

Name	Status	
ssl-cert	Enabled	

URL Alias:

Configure the list of UR following URLs, system

URL
-----

#### Edit Alias Name

Alias Name:

  
 Enabled

Cancel   OK

Cancel   Save

編輯群組別名

步驟 14.透過點選加號圖示(+)配置group-url。使用使用者端設定檔中之前設定的相同群組URL。

## Edit Connection Profile

Connection Profile:\* RAVPN-CertAuth

Group Policy:\* DfltGrpPolicy

Client Address Assignment   AAA   **Aliases**

Incoming users can choose an alias name upon first login. Aliases from all connections configured on this device can be turned on or off.

### Edit URL Alias

URL Alias:

certauth

Enabled

Cancel   OK

URL Alias:

Configure the list of URL aliases. If users choose the following URLs, system will automatically log them in via this connection profile.

URL	Status
certauth (https://certauth.cisco.com/ssl-cert)	Enabled

Cancel   Save

編輯群組URL

步驟 15. 導航至Access Interfaces。在SSL settings下選擇Interface Trustpoint和SSL Global Identity Certificate。

## RAVPN

Enter Description

Connection Profile   **Access Interfaces**   Advanced

Local Realm: cisco-local   Policy Assignments (1)   Dynamic Access Policy: None

Interfaces of the targeted device which belong to below specified interface groups will support incoming Remote Access VPN connections

Name	Interface Trustpoint	DTLS	SSL	IPsec-IKEv2
outside-zone	ssl_certificate	●	●	●

Access Settings

Allow Users to select connection profile while logging in

SSL Settings

Web Access Port Number:\* 443

DTLS Port Number:\* 443

SSL Global Identity Certificate: ssl\_certificate

Note: Ensure the port used in VPN configuration is not used in other services

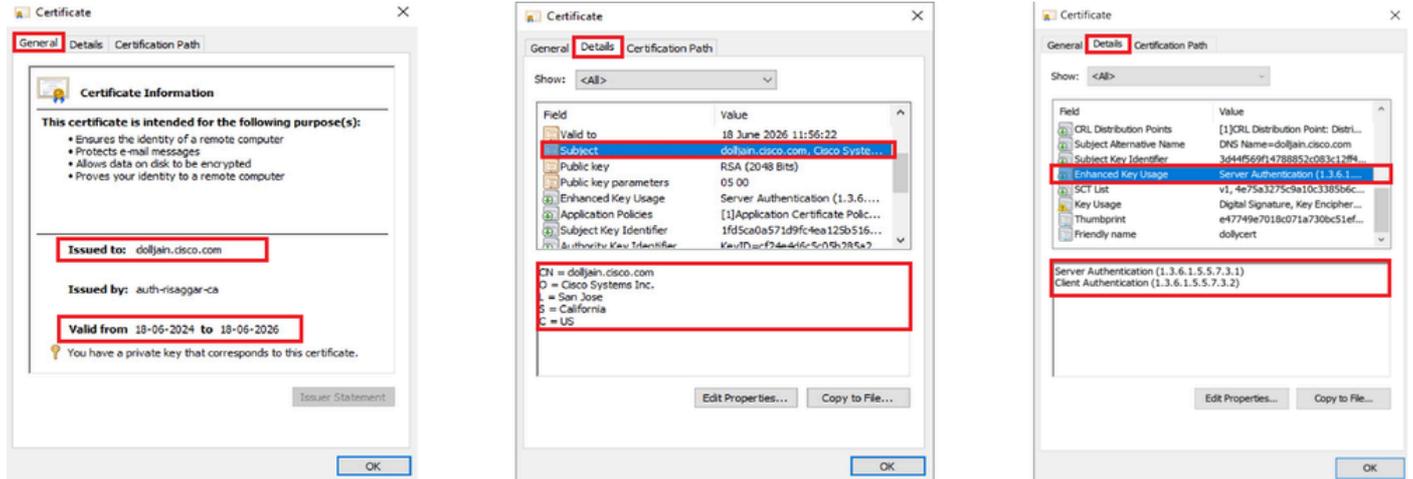
編輯訪問介面

步驟 16. 點選Save，部署這些更改。

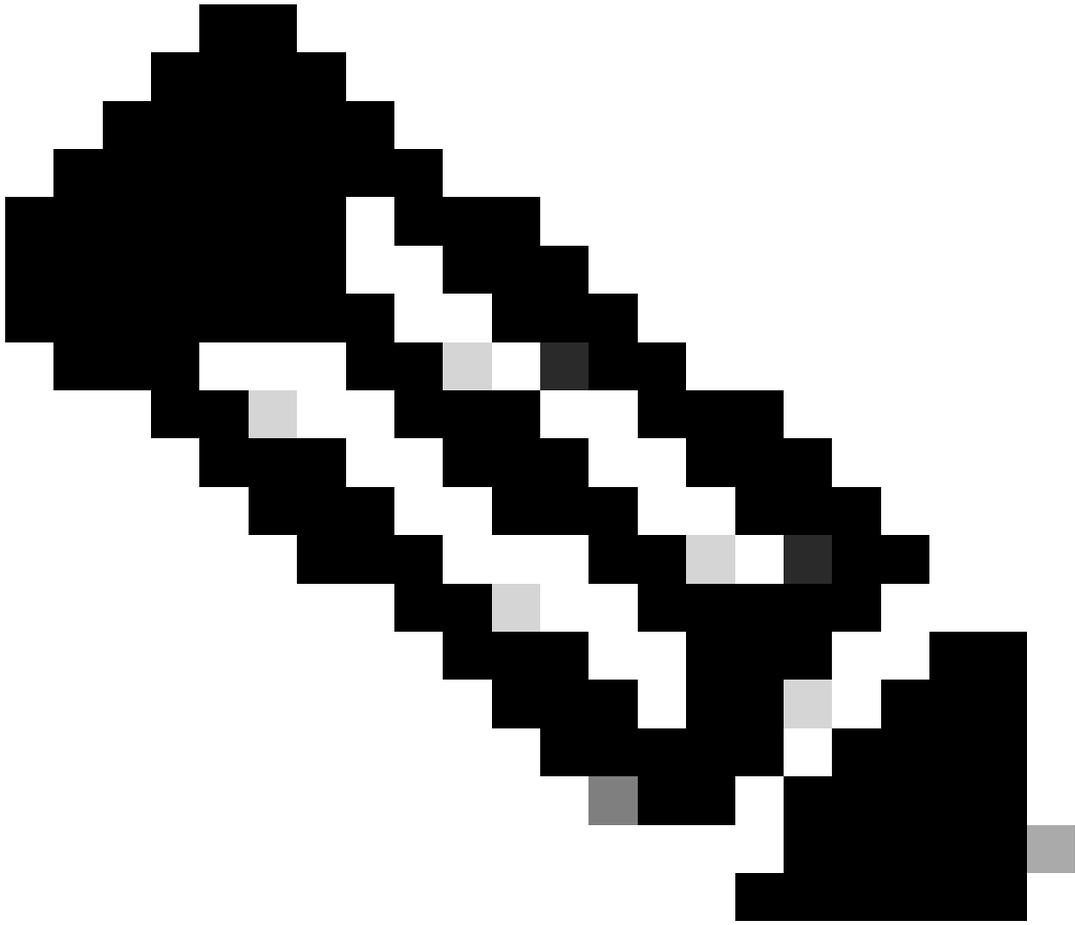
## 驗證

使用本節內容，確認您的組態是否正常運作。

1. 安全客戶端PC必須在使用者PC上安裝具有有效日期、主題和EKU的證書。此憑證必須是由其憑證安裝在FTD上的CA核發，如先前所示。此處，身份或使用證書由「auth-risaggar-ca」頒發。



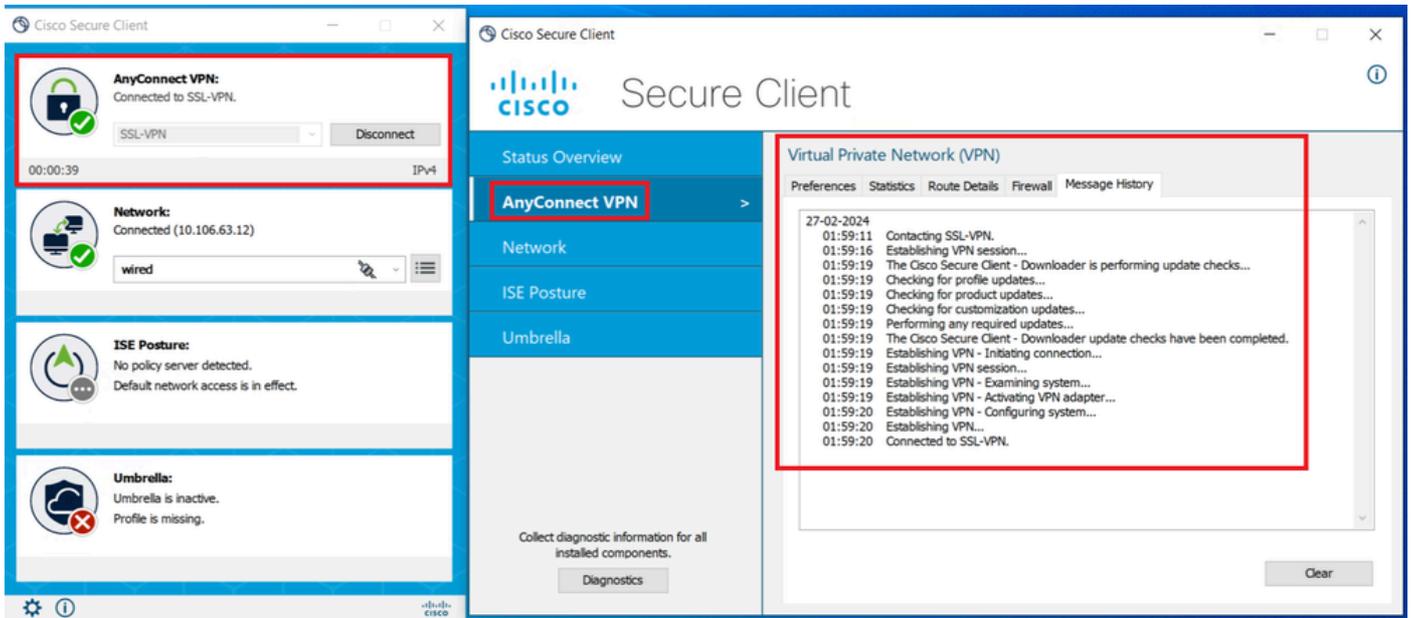
憑證亮點



**注意：**客戶端證書必須具有「客戶端身份驗證」增強型金鑰使用(EKU)。

---

2. 安全客戶端必須建立連線。



成功的安全客戶端連線

3. 運行show vpn-sessiondb anyconnect以確認使用隧道組下活動使用者的連線詳細資訊。

```
firepower# show vpn-sessiondb anyconnect Session Type: AnyConnect Username : dolljain.cisco.com Index :
```

## 疑難排解

本節提供的資訊可用於對組態進行疑難排解。

1. 可以從FTD的診斷CLI執行偵錯：

```
debug crypto ca 14  
debug webvpn anyconnect 255  
debug crypto ike-common 255
```

2. 有關常見問題，請參閱本[指南](#)。

## 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）。