

# 透過FMC為FTD上的安全使用者端設定AAA和憑證驗證

## 目錄

---

### [簡介](#)

### [必要條件](#)

#### [需求](#)

#### [採用元件](#)

### [背景資訊](#)

### [網路圖表](#)

### [組態](#)

#### [FMC中的配置](#)

##### [步驟 1.設定FTD介面](#)

##### [步驟 2.確認思科安全客戶端許可證](#)

##### [步驟 3.增加策略分配](#)

##### [步驟 4.連線配置檔案的配置詳細資訊](#)

##### [步驟 5.為連線配置檔案增加地址池](#)

##### [步驟 6.新增連線設定檔的群組原則](#)

##### [步驟 7.設定連線設定檔的安全使用者端映像](#)

##### [步驟 8.設定連線設定檔的存取與憑證](#)

##### [步驟 9.確認連線設定檔摘要](#)

#### [在FTD CLI中確認](#)

#### [在VPN客戶端中確認](#)

##### [步驟 1.確認使用者端憑證](#)

##### [步驟 2.確認CA](#)

### [驗證](#)

#### [步驟 1.啟動VPN連線](#)

#### [步驟 2.確認FMC中的活動會話](#)

#### [步驟 3.在FTD CLI中確認VPN作業階段](#)

#### [步驟 4.確認與伺服器的通訊](#)

### [疑難排解](#)

### [參考](#)

---

## 簡介

本檔案介紹在由FMC管理的FTD上透過SSL設定Cisco Secure Client，並使用AAA和憑證驗證的步驟。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- Cisco Firepower管理中心(FMC)
- 防火牆威脅防禦虛擬(FTD)
- VPN身份驗證流程

## 採用元件

- 適用於VMWare的Cisco Firepower管理中心7.4.1
- 思科防火牆威脅防禦虛擬7.4.1
  
- 思科安全使用者端5.1.3.62

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

隨著組織採取更嚴格的安全措施，將雙因素身份驗證(2FA)與基於證書的身份驗證相結合已成為一種常見做法，可增強安全性並防止未經授權的訪問。可以顯著改善使用者體驗和安全性的功能之一是能夠預填充Cisco Secure Client中的使用者名稱。此功能簡化了登入過程，並提高了遠端訪問的整體效率。

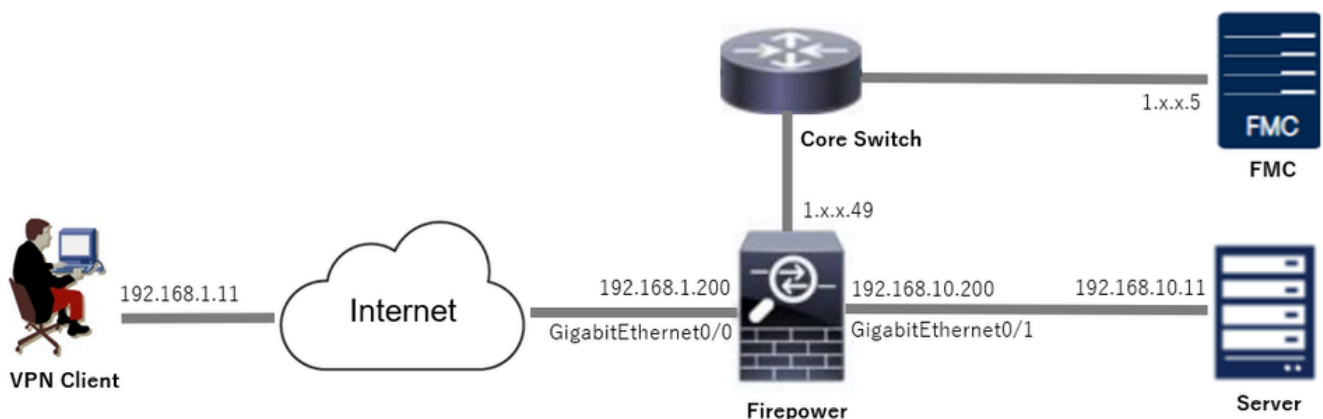
本檔案介紹如何將預先填入的使用者名稱與FTD上的Cisco Secure Client整合，以確保使用者可以快速安全地連線到網路。

這些憑證中包含用於授權目的的通用名稱。

- CA：ftd-ra-ca-common-name
- 客戶端證書：ssIVPNClientCN
- 伺服器證書：192.168.1.200

## 網路圖表

下圖顯示本文檔示例中使用的拓撲。



網路圖表

# 組態

## FMC中的配置

### 步驟 1. 設定FTD介面

導覽至Devices > Device Management，在Interfaces索引標籤中編輯目標FTD裝置、設定FTD的內部和外部介面。

對於GigabitEthernet0/0，

- 名稱：outside
- 安全區域：outsideZone
- IP地址：192.168.1.200/24

對於GigabitEthernet0/1，

- 名稱：inside
- 安全區域：insideZone
- IP地址：192.168.10.200/24

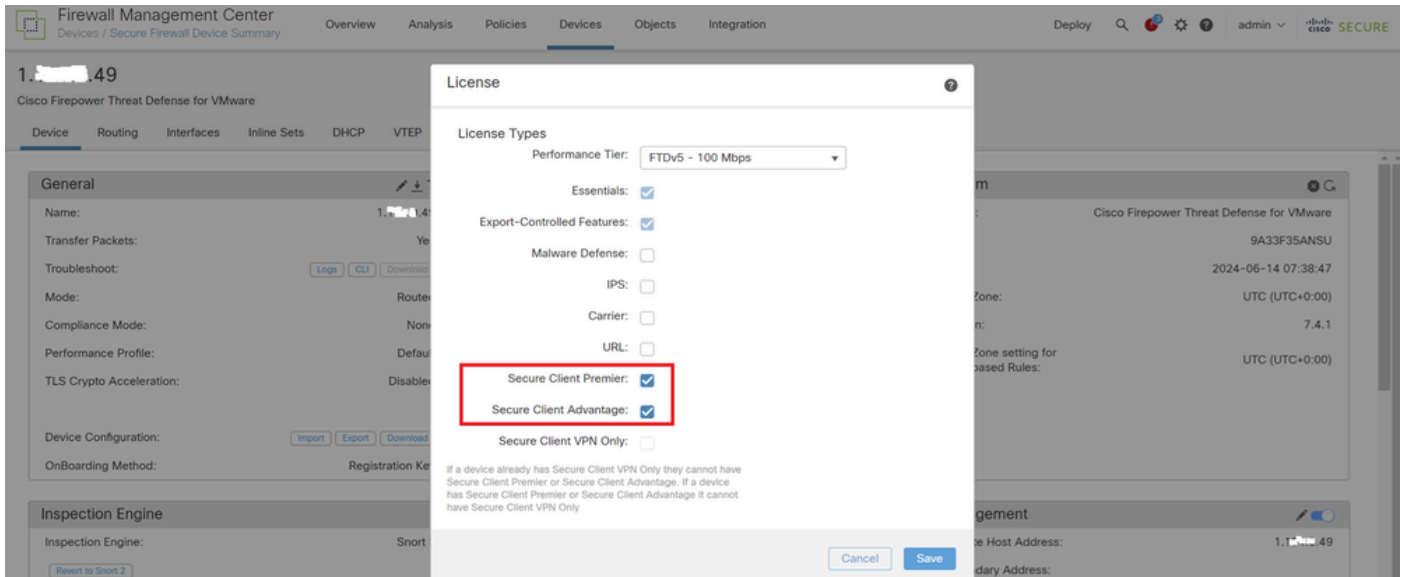
The screenshot shows the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Devices' tab is active, and the 'Interfaces' sub-tab is selected. The device name is '1. .49' and the model is 'Cisco Firepower Threat Defense for VMware'. The 'Interfaces' section shows a table of configured interfaces:

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Management0/0	management	Physical				Disabled	Global
GigabitEthernet0/0	outside	Physical	outsideZone		192.168.1.200/24(Static)	Disabled	Global
GigabitEthernet0/1	inside	Physical	insideZone		192.168.10.200/24(Static)	Disabled	Global
GigabitEthernet0/2		Physical				Disabled	
GigabitEthernet0/3		Physical				Disabled	

### FTD介面

### 步驟 2. 確認思科安全客戶端許可證

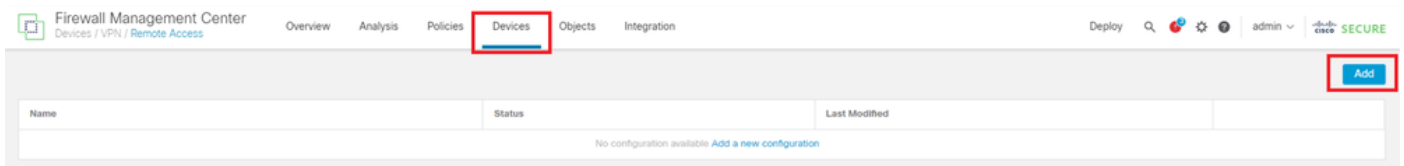
導覽至Devices > Device Management，編輯目標FTD裝置，在Device索引標籤中確認Cisco Secure Client授權。



安全使用者端授權

### 步驟 3. 增加策略分配

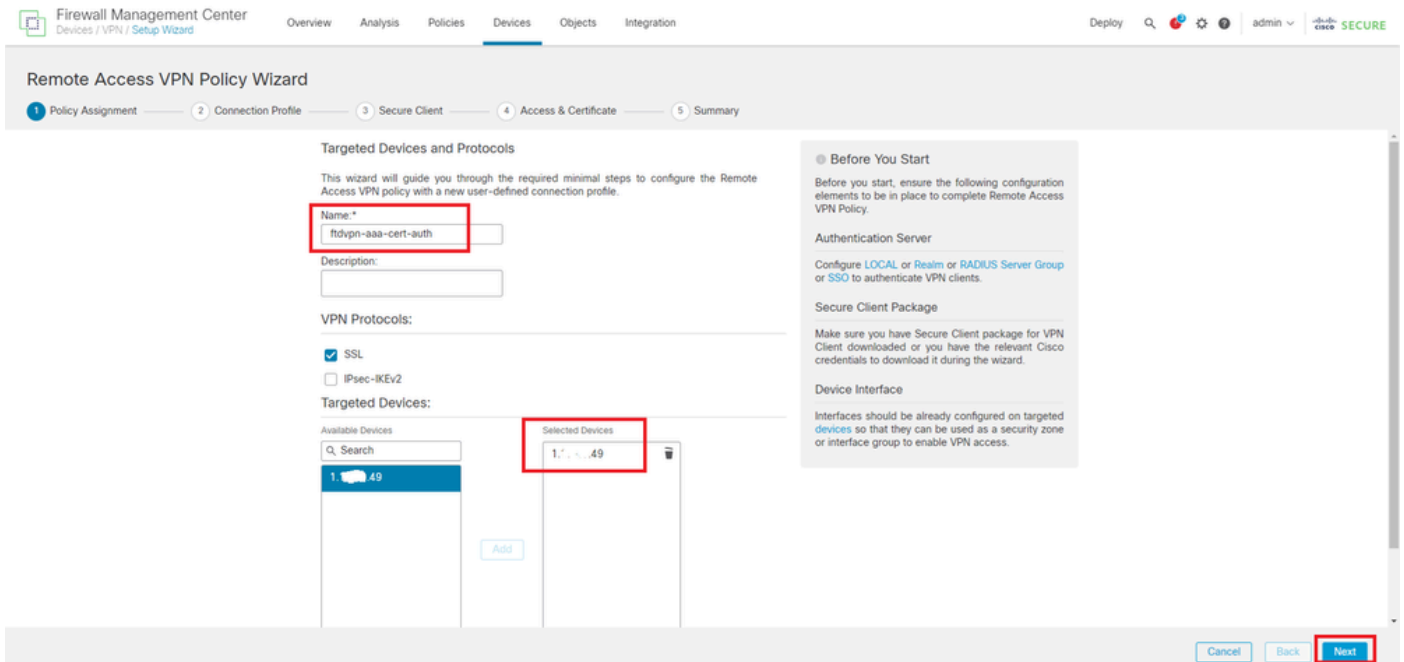
導航到 Devices > VPN > Remote Access，按一下 Add 按鈕。



增加遠端訪問VPN

輸入必要資訊，然後按一下 Next 按鈕。

- 名稱：ftdvpn-aaa-cert-auth
- VPN協定：SSL
- 目標裝置：1.x.x.49

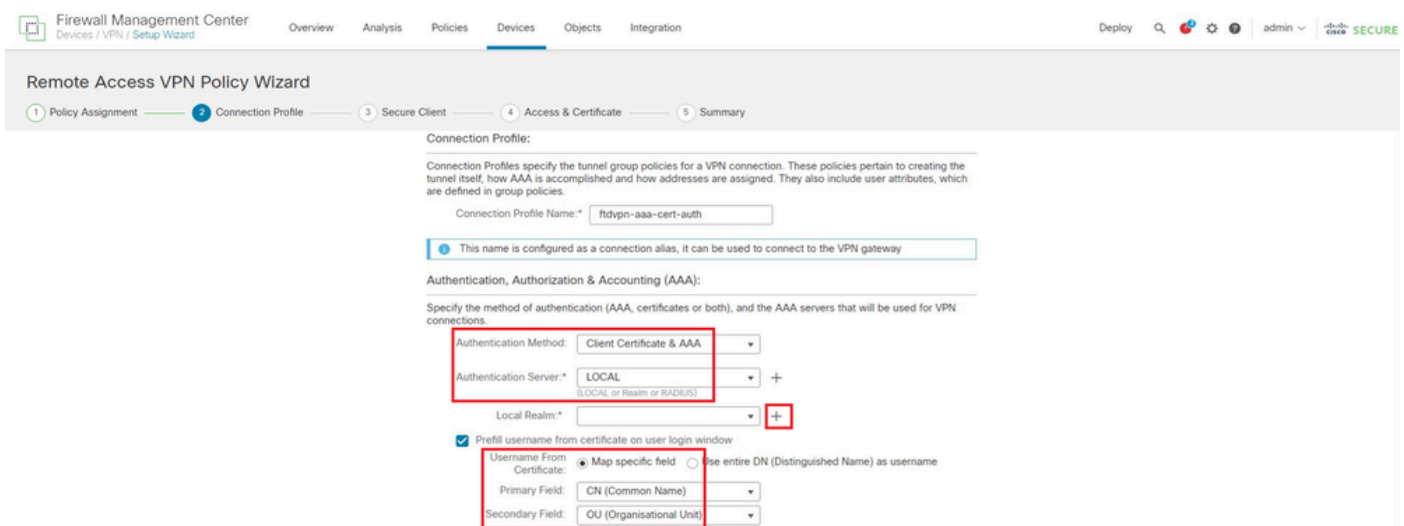


策略分配

## 步驟 4.連線配置檔案的配置詳細資訊

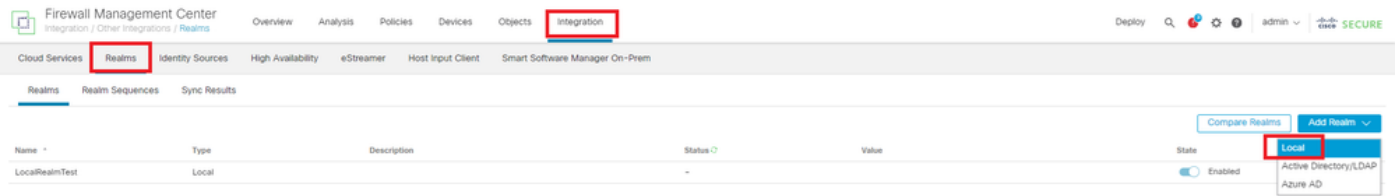
輸入連線配置檔案的必要資訊，然後按一下本地領域項旁邊的+按鈕。

- 身份驗證方法：客戶端證書和AAA
- 身份驗證伺服器：本地
- 證書使用者名稱：對映特定欄位
- 主欄位：CN (公用名)
- 輔助欄位：OU (組織單位)



連線設定檔的詳細資訊

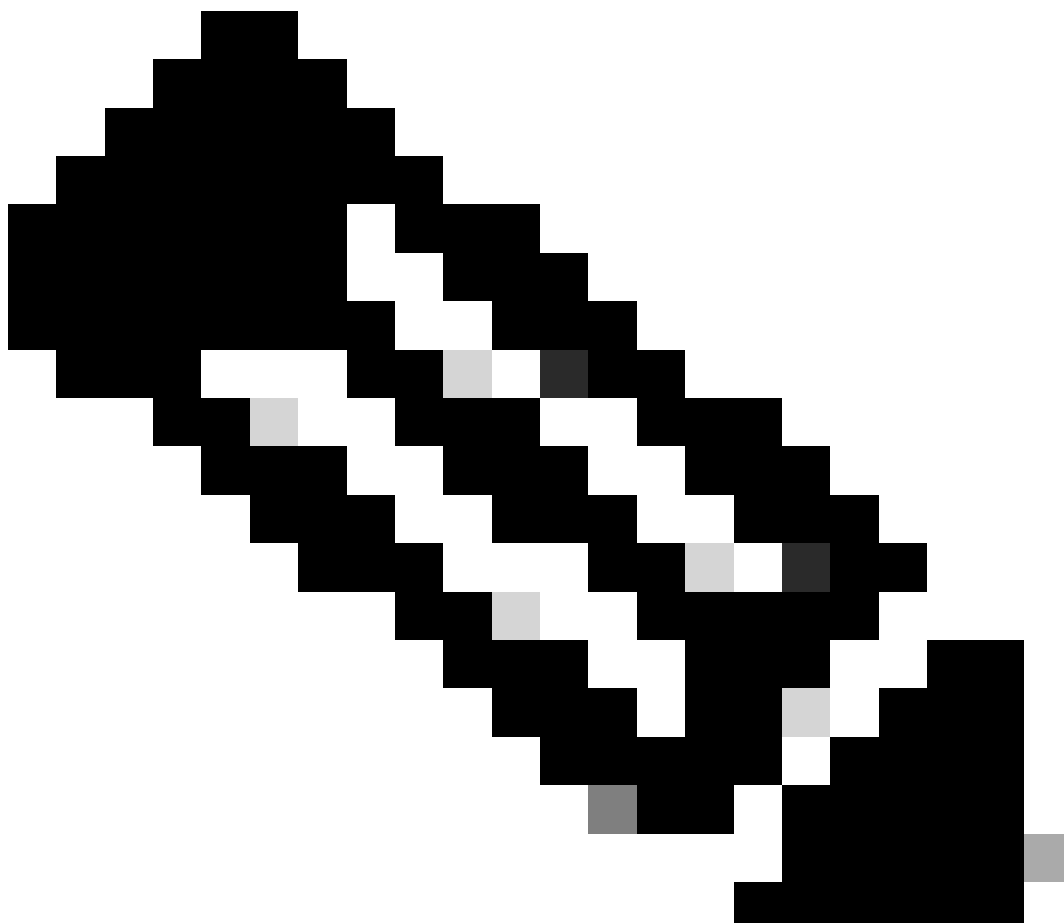
從增加領域下拉選單中按一下本地，以增加新的本地領域。



新增本機範圍

輸入本地領域所需的資訊，然後按一下Save按鈕。

- 名稱：LocalRealmTest
- 使用者名稱：ssIVPNClientCN



注意：使用者名稱與客戶端證書中的公用名相同

## Add New Local Realm



Name*	Description
LocalRealmTest	

### Local User Configuration

^ ssIVPNCilentCN

Username	ssIVPNCilentCN
Password	Confirm Password
.....	.....

[Add another local user](#)

[Cancel](#) [Save](#)

本機範圍詳細資訊

### 步驟 5. 為連線配置檔案增加地址池

按一下IPv4地址池專案旁邊的edit按鈕。

#### 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) ●

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools:

IPv6 Address Pools:

增加IPv4地址池

輸入必要的資訊以新增新的IPv4位址集區。為連線配置檔案選擇新的IPv4地址池。

- 名稱：ftdvpn-aaa-cert-pool
- IPv4地址範圍：172.16.1.40-172.16.1.50
- 掩碼：255.255.255.0

## Add IPv4 Pool



**Name\***  
ftdvpn-aaa-cert-pool

Description

**IPv4 Address Range\***  
172.16.1.40-172.16.1.50

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

IPv4地址池的詳細資訊

### 步驟 6.新增連線設定檔的群組原則

點選組策略專案旁邊的+按鈕。

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](#)

Cancel

Back

Next

增加組策略

輸入必要的資訊以新增群組原則。為連線配置檔案選擇新的組策略。

- 名稱 : ftdvpn-aaa-cert-grp



- VPN協定：SSL

## Add Group Policy



Name:\*

ftdvpn-aaa-cert-grp

Description:

General Secure Client Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

VPN Tunnel Protocol:  
Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

SSL

IPsec-IKEv2

Cancel

Save

組策略的詳細資訊

步驟 7.設定連線設定檔的安全使用者端映像

選擇secure client image file並按一下Next按鈕。

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 Secure Client — 4 Access & Certificate — 5 Summary

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](#).

Secure Client File Object Name	Secure Client Package Name	Operating System
<input checked="" type="checkbox"/>	cisco-secure-client-win-5.1.3.62-webdepl...	Windows

Cancel Back **Next**

選擇安全客戶端映像

## 步驟 8. 設定連線設定檔的存取與憑證

為VPN連線選擇Security Zone，然後按一下Certificate Enrollment專案旁邊的+按鈕。

- 介面組/安全區域：outsideZone

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 Secure Client — 4 Access & Certificate — 5 Summary

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:\* outsideZone +

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:\* [ ] +

選擇安全區域

輸入FTD憑證的必要資訊，並從本機電腦匯入PKCS12檔案。

- 名稱：ftdvpn-cert
- 註冊型別：PKCS12檔案

## Add Cert Enrollment



Name\*  
ftdvpn-cert

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: PKCS12 File

PKCS12 File\*: ftdCert.pfx [Browse PKCS12 File](#)

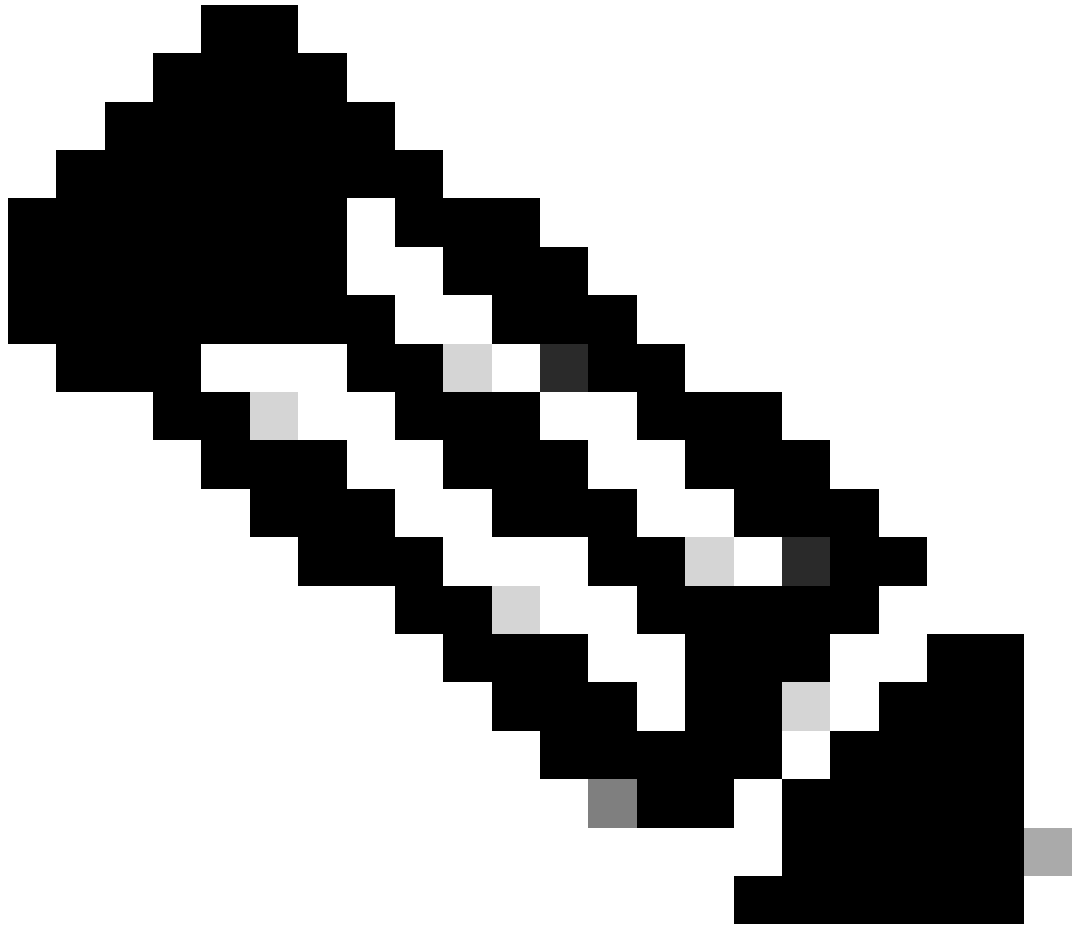
Passphrase\*: .....

Validation Usage:  IPsec Client  SSL Client  SSL Server  
 Skip Check for CA flag in basic constraints of the CA Certificate

[Cancel](#) [Save](#)

新增FTD憑證

確認在Access & Certificate嚮導中輸入的資訊，然後按一下Next按鈕。



注意：為解密的流量啟用繞過訪問控制策略(sysopt permit-vpn)，以便解密VPN流量不會受到訪問控制策略檢查。

---

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 Secure Client — 4 Access & Certificate — 5 Summary

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.

Cancel Back **Next**

確認「存取與憑證」中的設定

## 步驟 9. 確認連線設定檔摘要

確認輸入的VPN連線資訊，然後按一下Finish按鈕。

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 Secure Client — 4 Access & Certificate — 5 Summary

Remote Access VPN Policy Configuration

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

Name:	ftdvpn-aaa-cert-auth
Device Targets:	1.1.1.149
Connection Profile:	ftdvpn-aaa-cert-auth
Connection Alias:	ftdvpn-aaa-cert-auth
AAA:	
Authentication Method:	Client Certificate & AAA
Username From Certificate:	CN (Common Name) & OU (Organisational Unit)
Authentication Server:	LocalRealmTest (Local)
Authorization Server:	-
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	ftdvpn-aaa-cert-pool
Address Pools (IPv6):	-
Group Policy:	ftdvpn-aaa-cert-grp
Secure Client Images:	cisco-secure-client-win-5.1.3.62-webdeploy-k9.pk.g
Interface Objects:	outsideZone
Device Certificates:	ftdvpn-cert

Device Identity Certificate Enrollment

Certificate enrollment object 'ftdvpn-cert' 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.

Additional Configuration Requirements

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- Access Control Policy Update  
An [Access Control](#) rule must be defined to allow VPN traffic on all targeted devices.
- NAT Exemption  
If NAT is enabled on the targeted devices, you must define a [NAT Policy](#) to exempt VPN traffic.
- DNS Configuration  
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using [FlexConfig Policy](#) on the targeted devices.
- Port Configuration  
SSL will be enabled on port 443. Please ensure that these ports are not used in [NAT Policy](#) or other services before deploying the configuration.
- ▲ Network Interface Configuration  
Make sure to add interface from targeted devices to SecurityZone object 'outsideZone'

Cancel Back **Finish**

確認VPN連線的設定

確認遠端存取VPN原則的摘要並將設定部署到FTD。

The screenshot shows the Cisco FMC interface for configuring a connection profile. The profile name is 'ftdvpn-aaa-cert-auth'. The AAA configuration is as follows:

Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DefaultGrpPolicy
ftdvpn-aaa-cert-auth	Authentication: Client Certificate & LOCAL Authorization: None Accounting: None	ftdvpn-aaa-cert-grp

遠端訪問VPN策略摘要

## 在FTD CLI中確認

從FMC部署後，在FTD CLI中確認VPN連線設定。

```
// Defines IP of interface
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 192.168.1.200 255.255.255.0
interface GigabitEthernet0/1
nameif inside
security-level 0
ip address 192.168.10.200 255.255.255.0
```

```
// Defines a pool of addresses
ip local pool ftdvpn-aaa-cert-pool 172.16.1.40-172.16.1.50 mask 255.255.255.0
```

```
// Defines a local user
username sslVPNClientCN password ***** encrypted
```

```
// Defines Trustpoint for Server Certificate
crypto ca trustpoint ftdvpn-cert
keypair ftdvpn-cert
cr1 configure
```

```
// Server Certificate Chain
crypto ca certificate chain ftdvpn-cert
certificate 22413df584b6726c
3082037c 30820264 a0030201 02020822 413df584 b6726c30 0d06092a 864886f7
.....
quit
certificate ca 5242a02e0db6f7fd
3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7
.....
quit
```

```
// Configures the FTD to allow Cisco Secure Client connections and the valid Cisco Secure Client images
webvpn
enable outside
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
```

```
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/csm/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1 regex "Windows"
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable

// Bypass Access Control policy for decrypted traffic
// This setting is displayed in the 'show run all' command output
sysopt connection permit-vpn

// Configures the group-policy to allow SSL connections
group-policy ftdvpn-aaa-cert-grp internal
group-policy ftdvpn-aaa-cert-grp attributes
banner none
wins-server none
dns-server none
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-tunnel-network-list none
default-domain none
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
vlan none
address-pools none
webvpn
anyconnect ssl dtls enable
anyconnect mtu 1406
anyconnect firewall-rule client-interface public none
anyconnect firewall-rule client-interface private none
anyconnect ssl keepalive 20
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client 30
anyconnect dpd-interval gateway 30
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules value none
anyconnect ask none default anyconnect
anyconnect ssl df-bit-ignore disable

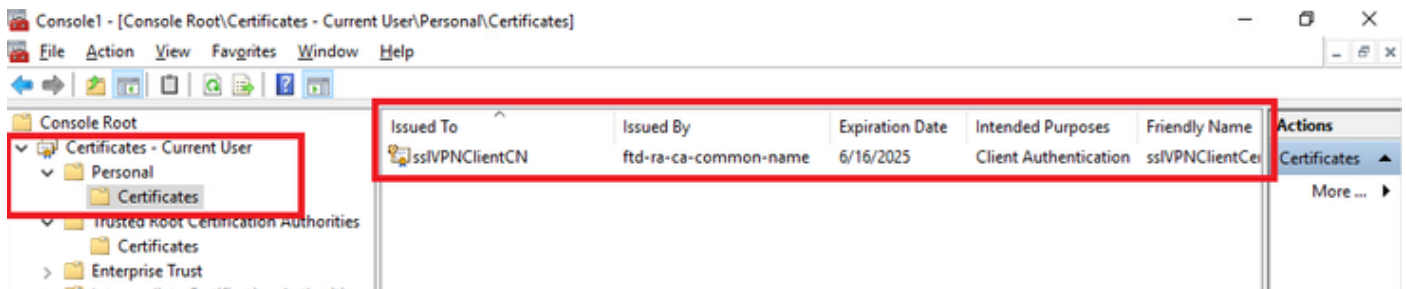
// Configures the tunnel-group to use the aaa & certificate authentication
tunnel-group ftdvpn-aaa-cert-auth type remote-access
tunnel-group ftdvpn-aaa-cert-auth general-attributes
address-pool ftdvpn-aaa-cert-pool
default-group-policy ftdvpn-aaa-cert-grp
// These settings are displayed in the 'show run all' command output. Start
authentication-server-group LOCAL
secondary-authentication-server-group none
```

```
no accounting-server-group
default-group-policy ftdvpn-aaa-cert-grp
username-from-certificate CN OU
secondary-username-from-certificate CN OU
authentication-attr-from-server primary
authenticated-session-username primary
username-from-certificate-choice second-certificate
secondary-username-from-certificate-choice second-certificate
// These settings are displayed in the 'show run all' command output. End
tunnel-group ftdvpn-aaa-cert-auth webvpn-attributes
authentication aaa certificate
pre-fill-username client
group-alias ftdvpn-aaa-cert-auth enable
```

## 在VPN客戶端中確認

### 步驟 1. 確認使用者端憑證

導航到證書- Current User > Personal > Certificates，檢查用於身份驗證的客戶端證書。

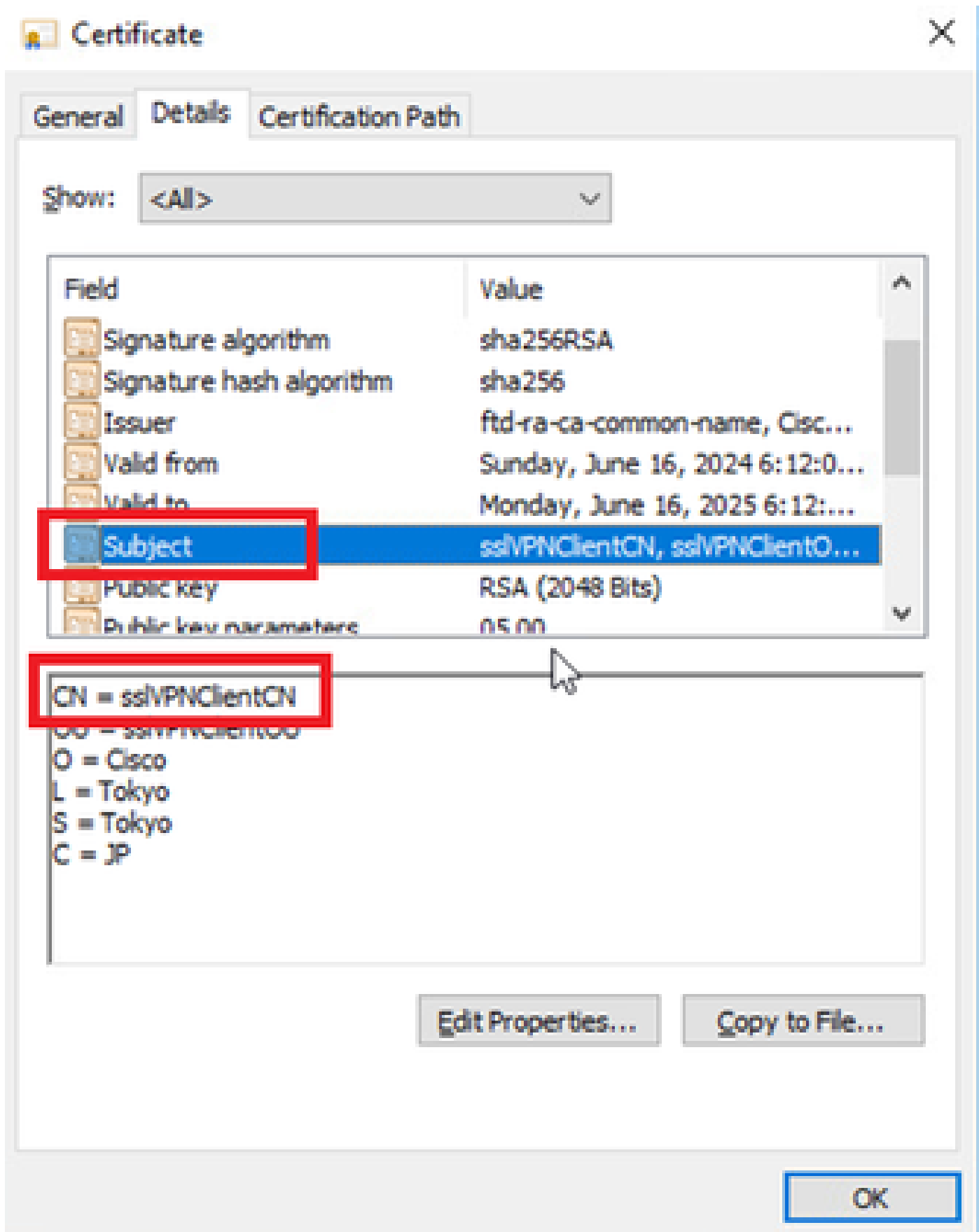


確認使用者端憑證

按兩下客戶端證書，導航到Details，檢查Subject的詳細資訊。

- 主題：CN = ssIVPNClientCN





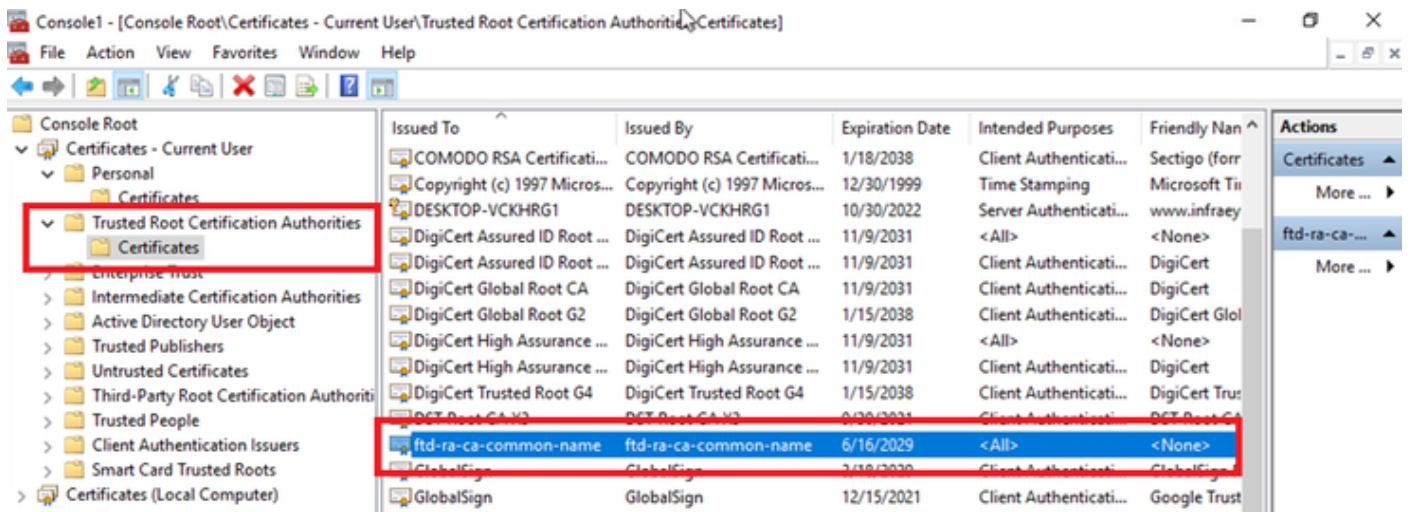
客戶端證書的詳細資訊

## 步驟 2. 確認CA

導航到證書- Current User > Trusted Root Certification Authorities > Certificates , 檢查用於身份驗

證的CA。

- 頒發者：ftd-ra-ca-common-name



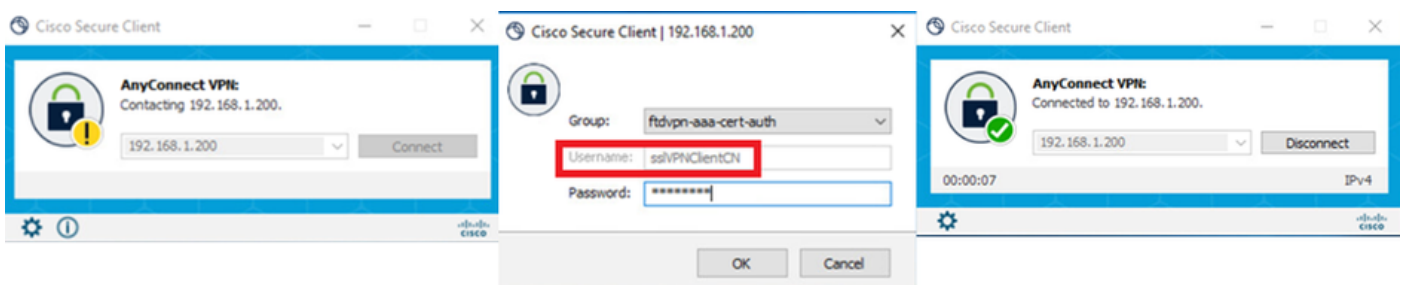
確認CA

## 驗證

### 步驟 1. 啟動VPN連線

在終端上，啟動Cisco Secure Client連線。使用者名稱從客戶端證書中提取，您需要輸入密碼進行VPN身份驗證。

注意：使用者名稱擷取自本檔案中使用者端憑證的CN（一般名稱）欄位。



啟動VPN連線

步驟 2. 確認FMC中的活動會話

導航到分析>使用者>活動會話，檢查活動會話以進行VPN身份驗證。

Session ID	Realtime Username	Last Seen	Authentication Type	Current IP	Realtime	Username	First Name	Last Name	Email	Department	Phone Number	Discovery Application	Device
2024-06-17 11:38:22	LocalRealmTestsslVPNClientCN	2024-06-17 11:38:22	VPN Authentication	172.16.1.40	LocalRealmTest	sslVPNClientCN						LDAP	1.149

確認活動會話

### 步驟 3. 在FTD CLI中確認VPN作業階段

在FTD (Lina) CLI中執行show vpn-sessiondb detail anyconnect命令以確認VPN作業階段。

```
ftd702# show vpn-sessiondb detail anyconnect
```

Session Type: AnyConnect Detailed

```
Username : sslVPNClientCN Index : 7
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384
Bytes Tx : 14780 Bytes Rx : 15386
Pkts Tx : 2 Pkts Rx : 37
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftdvpn-aaa-cert-grp Tunnel Group : ftdvpn-aaa-cert-auth
Login Time : 02:38:22 UTC Mon Jun 17 2024
Duration : 0h:01m:22s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb00718200007000666fa19e
Security Grp : none Tunnel Zone : 0
```

```
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
```

```
AnyConnect-Parent:
Tunnel ID : 7.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 50035 TCP Dst Port : 443
Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : win
Client OS Ver: 10.0.15063
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7390 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

```
SSL-Tunnel:
Tunnel ID : 7.2
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Encryption : AES-GCM-128 Hashing : SHA256
```

Ciphersuite : TLS\_AES\_128\_GCM\_SHA256  
Encapsulation: TLSv1.3 TCP Src Port : 50042  
TCP Dst Port : 443 Auth Mode : Certificate and userPassword  
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes  
Client OS : Windows  
Client Type : SSL VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62  
Bytes Tx : 7390 Bytes Rx : 2292  
Pkts Tx : 1 Pkts Rx : 3  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:

Tunnel ID : 7.3  
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11  
Encryption : AES-GCM-256 Hashing : SHA384  
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384  
Encapsulation: DTLSv1.2 UDP Src Port : 56382  
UDP Dst Port : 443 Auth Mode : Certificate and userPassword  
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
Client OS : Windows  
Client Type : DTLS VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62  
Bytes Tx : 0 Bytes Rx : 13094  
Pkts Tx : 0 Pkts Rx : 34  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

步驟 4. 確認與伺服器的通訊

從VPN客戶端向伺服器發出ping命令，確認VPN客戶端與伺服器之間的通訊成功。

```
C:\Users\CALO>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:
Reply from 192.168.10.11: bytes=32 time=12ms TTL=128
Reply from 192.168.10.11: bytes=32 time=87ms TTL=128
Reply from 192.168.10.11: bytes=32 time=3ms TTL=128
Reply from 192.168.10.11: bytes=32 time=3ms TTL=128

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 87ms, Average = 26ms
```

Ping成功

在FTD (Lina) CLI中執行capture in interface inside real-time命令以確認封包擷取。

<#root>

ftd702#

capture in interface inside real-time

Use ctrl-c to terminate real-time capture

```
1: 03:39:25.729881 172.16.1.40 > 192.168.10.11 icmp: echo request
2: 03:39:25.730766 192.168.10.11 > 172.16.1.40 icmp: echo reply
3: 03:39:26.816211 172.16.1.40 > 192.168.10.11 icmp: echo request
4: 03:39:26.818683 192.168.10.11 > 172.16.1.40 icmp: echo reply
5: 03:39:27.791676 172.16.1.40 > 192.168.10.11 icmp: echo request
6: 03:39:27.792195 192.168.10.11 > 172.16.1.40 icmp: echo reply
7: 03:39:28.807789 172.16.1.40 > 192.168.10.11 icmp: echo request
8: 03:39:28.808399 192.168.10.11 > 172.16.1.40 icmp: echo reply
```

## 疑難排解

您可以期待在Lina引擎的調試系統日誌和Windows PC上的DART檔案中找到有關VPN身份驗證的資訊。

以下是Lina引擎中的偵錯日誌範例。

// Certificate Authentication

Jun 17 2024 02:38:03: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 6EC79930B231EDAF, subject name: CN=sslV

Jun 17 2024 02:38:03: %FTD-6-717028: Certificate chain was successfully validated with warning, revocation status was not checked.

Jun 17 2024 02:38:03: %FTD-6-717022: Certificate was successfully validated. serial number: 6EC79930B231EDAF, subject name: CN=sslVPNClientC

// Extract username from the CN (Common Name) field

Jun 17 2024 02:38:03: %FTD-7-113028: Extraction of username from VPN client certificate has been requested. [Request 5]

Jun 17 2024 02:38:03: %FTD-7-113028: Extraction of username from VPN client certificate has completed. [Request 5]

// AAA Authentication

Jun 17 2024 02:38:22: %FTD-6-113012: AAA user authentication Successful : local database : user = sslVPNClientCN

Jun 17 2024 02:38:22: %FTD-6-113009: AAA retrieved default group policy (ftdvpn-aaa-cert-grp) for user = sslVPNClientCN

Jun 17 2024 02:38:22: %FTD-6-113008: AAA transaction status ACCEPT : user = sslVPNClientCN

您可以從FTD的診斷CLI執行這些偵錯，提供的資訊可用於排除組態故障。

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

## 參考

[在FTD上設定AnyConnect遠端存取VPN](#)

[為行動存取配置基於Anyconnect證書的身份驗證](#)

## 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）。