

# 透過FMC在FTD上設定安全使用者端驗證的憑證對應

## 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IPv4地址池](#)

##### [步驟 4. 增加組策略](#)

##### [步驟 5. 新增FTD憑證](#)

##### [步驟 6. 為工程師連線配置檔案增加策略分配](#)

##### [步驟 7. 設定工程師連線設定檔的詳細資訊](#)

##### [步驟 8. 為工程師連線配置檔案配置安全客戶端映像](#)

##### [步驟 9. 配置工程師連線配置檔案的訪問和證書](#)

##### [步驟 10. 確認工程師連線設定檔摘要](#)

##### [步驟 11. 為Manager VPN客戶端增加連線配置檔案](#)

##### [步驟 12. 增加證書對映](#)

##### [步驟 13. 將證書對映繫結到連線配置檔案](#)

#### [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](#)

### [疑難排解](#)

### [相關資訊](#)

---

## 簡介

本檔案介紹如何使用憑證對應進行驗證，透過FMC在FTD上設定具有SSL的Cisco Secure Client。

## 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(FTD)虛擬
- 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

憑證對映是在VPN連線中使用的方法，其中使用者端憑證對映至本機使用者帳戶，或使用憑證內的屬性進行授權。這是使用數位憑證作為辨識使用者或裝置的方式。透過使用證書對映，它利用SSL協定對使用者進行身份驗證，而無需他們輸入憑證。

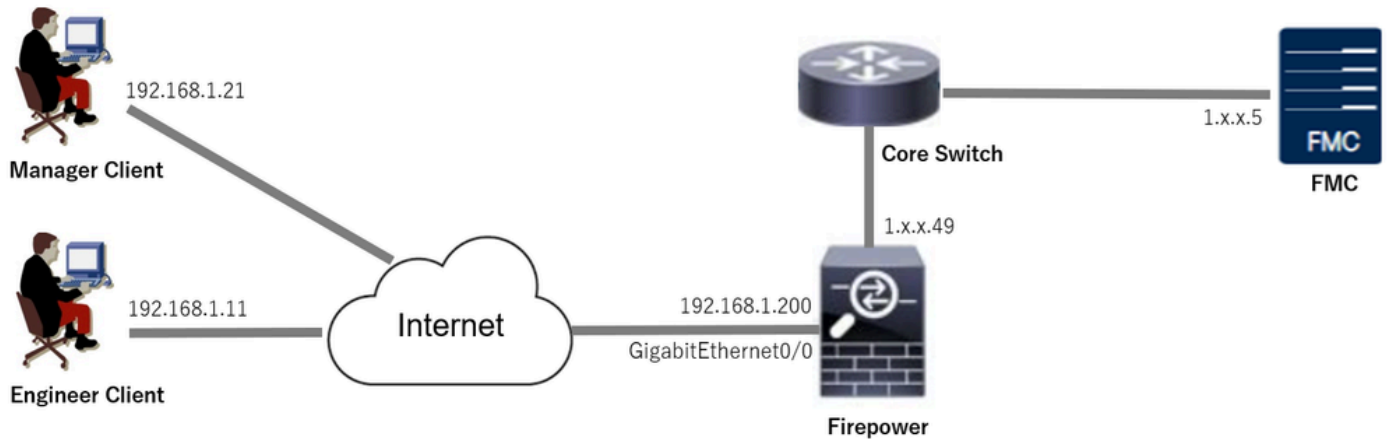
本文檔介紹如何使用SSL證書中的公用名稱對Cisco Secure Client進行身份驗證。

這些憑證中包含用於授權目的的通用名稱。

- CA：ftd-ra-ca-common-name
- 工程師VPN客戶端證書：vpnEngineerClientCN
- Manager VPN客戶端證書：vpnManagerClientCN
- 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，編輯目標FTD裝置，然後為FTD設定外部介面inInterfacestab。

對於GigabitEthernet0/0，

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

Firewall Management Center  
Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ admin 🔒 **SECURE**

1.1.1.1.49 Save Cancel

Cisco Firepower Threat Defense for VMware

Device Routing **Interfaces** Inline Sets DHCP VTEP

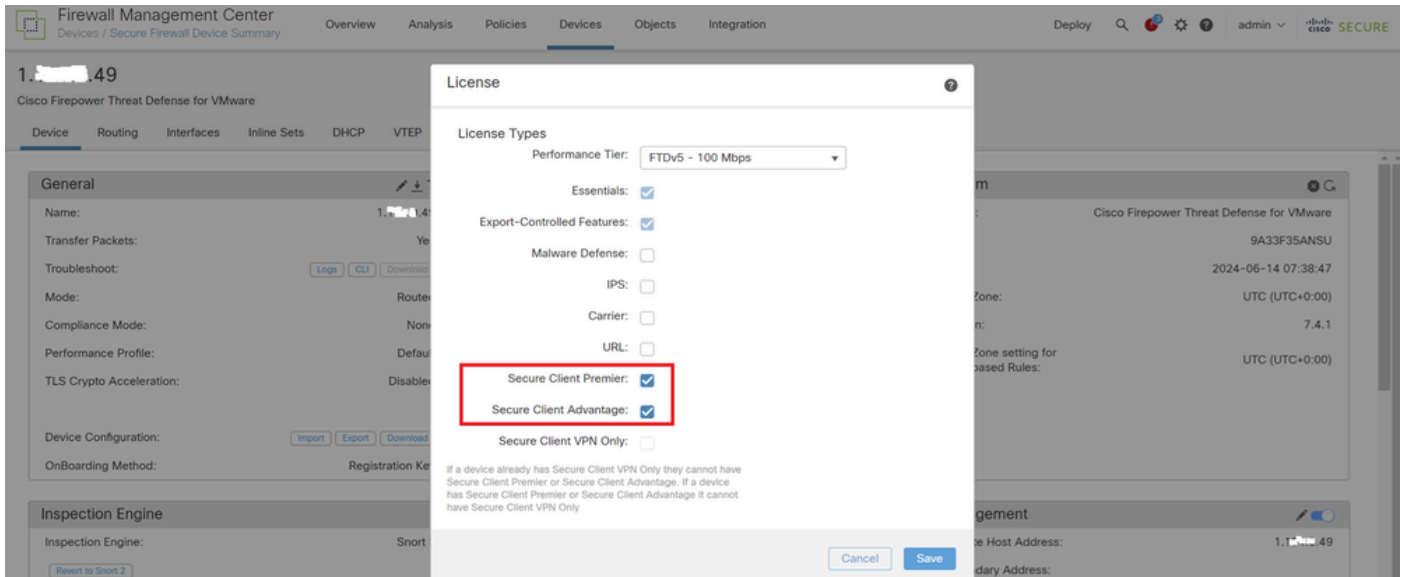
All Interfaces Virtual Tunnels 🔍 Search by name Sync Device Add Interfaces

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

FTD介面

#### 步驟 2. 確認思科安全客戶端許可證

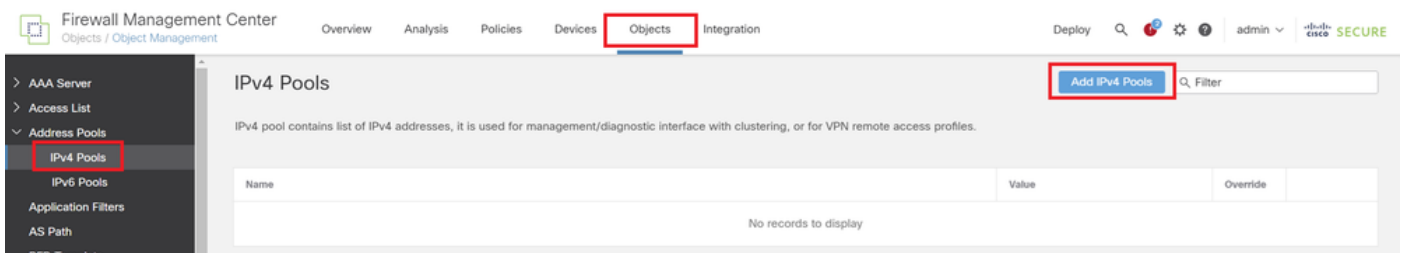
導航到裝置>裝置管理，編輯目標FTD裝置，在裝置頁籤中確認Cisco安全客戶端許可證。



安全使用者端授權

### 步驟 3. 增加IPv4地址池

導航到對象>對象管理>地址池> IPv4池，點選Add IPv4池按鈕。



增加IPv4地址池

輸入必要資訊，為工程師VPN客戶端建立IPv4地址池。

- 名稱：ftd-vpn-engineer-pool
- IPv4地址範圍：172.16.1.100-172.16.1.110
- 掩碼：255.255.255.0

## Edit IPv4 Pool



Name\*  
ftd-vpn-engineer-pool

Description

IPv4 Address Range\*  
172.16.1.100-172.16.1.110

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

工程師VPN客戶端的IPv4地址池

輸入必要的資訊為管理器VPN客戶端建立IPv4地址池。

- 名稱：ftd-vpn-manager-pool
- IPv4地址範圍：172.16.1.120-172.16.1.130
- 掩碼：255.255.255.0

# Add IPv4 Pool



Name\*

ftd-vpn-manager-pool

Description

IPv4 Address Range\*

172.16.1.120-172.16.1.130

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

Mask\*

255.255.255.0

Allow Overrides

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

Manager VPN客戶端的IPv4地址池

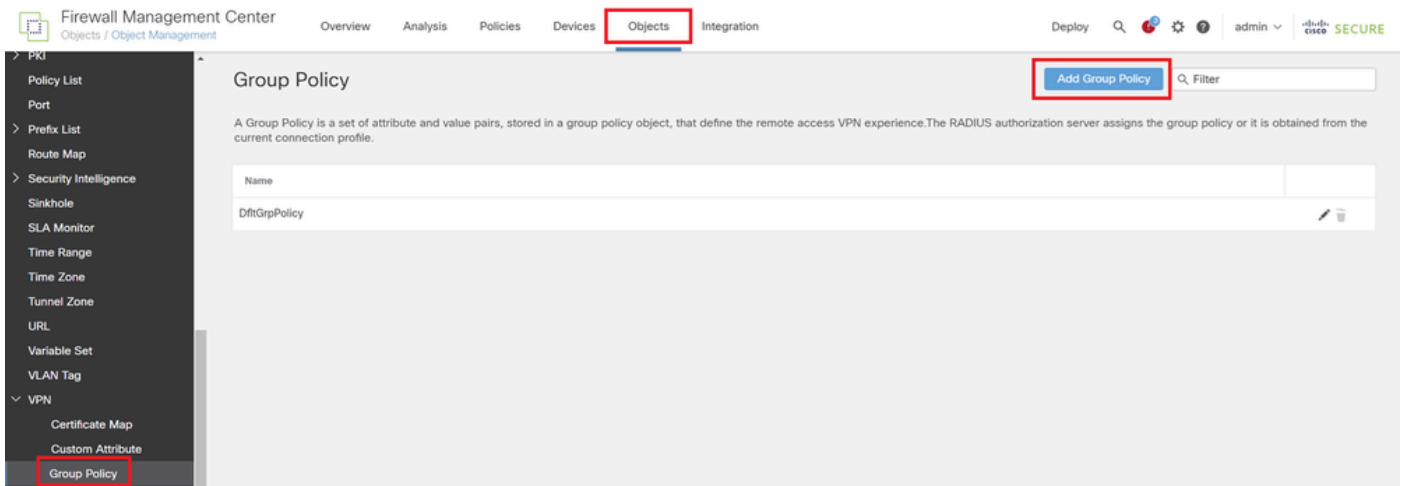
確認新的IPv4地址池。

Name	Value	Override	
ftd-vpn-engineer-pool	172.16.1.100-172.16.1.110	<span style="color: green;">●</span>	
ftd-vpn-manager-pool	172.16.1.120-172.16.1.130	<span style="color: green;">●</span>	

新的IPv4地址池

## 步驟 4. 增加組策略

導航到對象>對象管理> VPN >組策略，點選增加組策略按鈕。



增加組策略

輸入為工程師VPN客戶端建立組策略所需的資訊。

- 名稱：ftd-vpn-engineer-grp
- VPN協定：SSL

## Add Group Policy

Name:\*

ftd-vpn-engineer-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

工程師VPN客戶端的組策略

輸入為管理器VPN客戶端建立組策略所需的資訊。

- 名稱：ftd-vpn-manager-grp
- VPN協定：SSL

## Add Group Policy



**Name:\***  
ftd-vpn-manager-grp

**Description:**

**General**   **Secure Client**   **Advanced**

**VPN Protocols**

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

IP Address Pools  
Banner  
DNS/WINS  
Split Tunneling

Manager VPN客戶端的組策略

確認新的群組原則。

Firewall Management Center  
Objects / Object Management

Overview   Analysis   Policies   Devices   **Objects**   Integration

Deploy   Search   Settings   Help   admin   cisco   **SECURE**

**Group Policy**   Add Group Policy   Filter

A Group Policy is a set of attribute and value pairs, stored in a group policy object, that define the remote access VPN experience. The RADIUS authorization server assigns the group policy or it is obtained from the current connection profile.

Name	
DfltGrpPolicy	
ftd-vpn-engineer-grp	
ftd-vpn-manager-grp	

新增群組原則

## 步驟 5. 新增FTD憑證

導航到對象>對象管理> PKI >證書註冊，點選增加證書註冊按鈕。

Firewall Management Center  
Objects / Object Management

Overview   Analysis   Policies   Devices   **Objects**   Integration

Deploy   Search   Settings   Help   admin   cisco   **SECURE**

**Cert Enrollment**   Add Cert Enrollment   Filter

A certificate enrollment object contains the Certification Authority (CA) server information and enrollment parameters that are required for creating Certificate Signing Requests (CSRs) and obtaining Identity Certificates from the specified CA. These activities occur in your Private Key Infrastructure (PKI).

Name	Type	Override
No records to display		

PKI  
**Cert Enrollment**  
External Cert Groups



輸入FTD憑證的必要資訊，並從本機電腦匯入PKCS12檔案。

- 名稱：ftd-vpn-cert
- 註冊型別：PKCS12檔案

## Add Cert Enrollment



**Name\***  
ftd-vpn-cert

Description

This certificate is already enrolled on devices. Remove the enrolment from Device>Certificate page to edit/delete this Certificate.

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](#)

證書註冊詳細資訊

確認新的憑證註冊。

Firewall Management Center  
Objects / Object Management

Overview   Analysis   Policies   Devices   **Objects**   Integration

Deploy   Search   Settings   Help   admin   **SECURE**

### Cert Enrollment

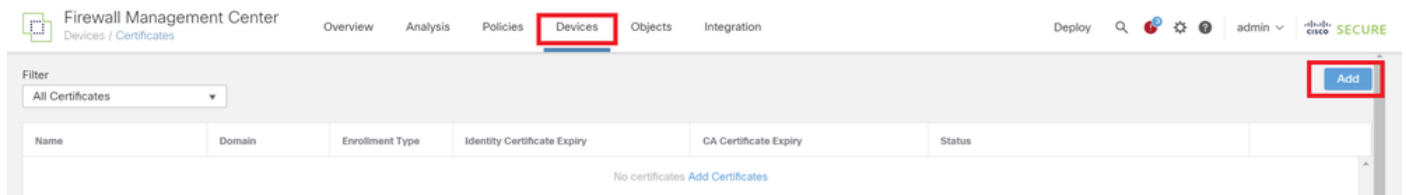
Add Cert Enrollment

A certificate enrollment object contains the Certification Authority (CA) server information and enrollment parameters that are required for creating Certificate Signing Requests (CSRs) and obtaining Identity Certificates from the specified CA. These activities occur in your Private Key Infrastructure (PKI).

Name	Type	Override	
ftd-vpn-cert	PKCS12 File		

新憑證註冊

導航到裝置>證書，點選增加按鈕。



新增FTD憑證

輸入將新憑證註冊連結到FTD的必要資訊。

- 裝置：1.x.x.49
- 證書註冊：ftd-vpn-cert

## Add New Certificate



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

Device\*:  
1.1.1.1.49

Cert Enrollment\*:  
ftd-vpn-cert

### Cert Enrollment Details:

Name: ftd-vpn-cert  
Enrollment Type: PKCS12 file  
Enrollment URL: N/A

Cancel

Add

將憑證連結到FTD

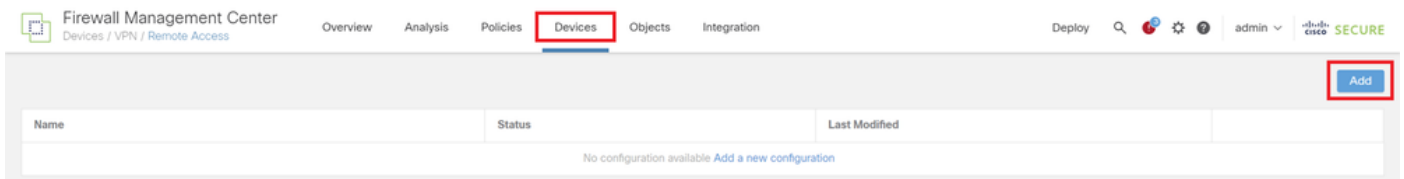
確認憑證繫結的狀態。

Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status
ftd-vpn-cert	Global	PKCS12 file	Jun 16, 2025	Jun 16, 2029	CA, ID

憑證繫結的狀態

步驟 6. 為工程師連線配置檔案增加策略分配

導航到 Devices > VPN > Remote Access , Add button。



增加遠端訪問VPN

輸入必要資訊，然後按一下「下一步」按鈕。

- 名稱：ftd-vpn-engineer
- VPN協定：SSL
- 目標裝置：1.x.x.49

策略分配

步驟 7. 設定工程師連線設定檔的詳細資訊

輸入必要資訊，然後按一下「下一步」按鈕。

- 驗證方法：僅使用者端憑證
- 來自證書的使用者名稱：對映特定欄位

- 主要欄位：CN（一般名稱）
- 次要欄位：OU（組織單位）
- IPv4地址池：ftd-vpn-engineer-pool
- 組策略：ftd-vpn-engineer-grp

Firewall Management Center  
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin

Remote Access VPN Policy Wizard

1 Policy Assignment 2 **Connection Profile** 3 Secure Client 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:\* ftd-vpn-engineer

① 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: Client Certificate Only

Username From Certificate:  Map specific field  Use entire DN (Distinguished Name) as username

Primary Field: CN (Common Name)

Secondary Field: OU (Organisational Unit)

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)

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools: ftd-vpn-engineer-pool

IPv6 Address Pools:

**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:\* ftd-vpn-engineer-grp

Edit Group Policy

Cancel Back **Next**

連線設定檔的詳細資訊

步驟 8. 為工程師連線配置檔案配置安全客戶端映像

選擇安全客戶端映像檔案，然後按一下Nextbutton。

Firewall Management Center  
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⓘ admin 🔒 cisco SECURE

### Remote Access VPN Policy Wizard

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

Remote User → Secure Client → Internet → VPN Device → Corporate Resources

**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 checked="" type="checkbox"/>	Secure Client File Object Name	Secure Client Package Name	Operating System
<input checked="" type="checkbox"/>	cisco-secure-client-win-5.1.3.6...	cisco-secure-client-win-5.1.3.62-webdepl...	Windows

Cancel Back **Next**

選取安全使用者端

## 步驟 9. 配置工程師連線配置檔案的訪問和證書

為介面組/安全區域和證書註冊項選擇值，然後按一下下一步按鈕。

- 介面組/安全區域：outsideZone
- 憑證註冊：ftd-vpn-cert

Firewall Management Center  
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⓘ admin 🔒 cisco SECURE

### Remote Access VPN Policy Wizard

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

AAA

**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:\* ftd-vpn-cert +

**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.

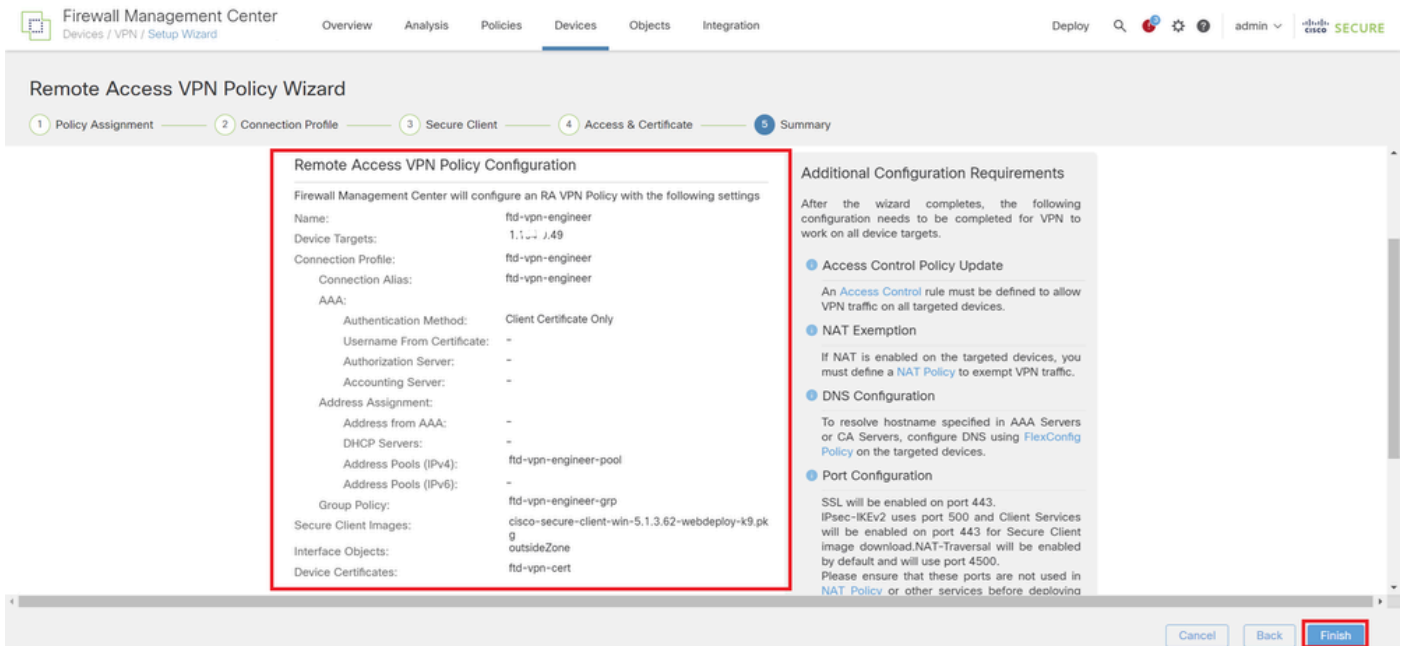
Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)  
*This option bypasses the Access Control Policy inspection, but VPN filter ACL and*

Cancel Back **Next**

訪問和證書的詳細資訊

## 步驟 10. 確認工程師連線設定檔摘要

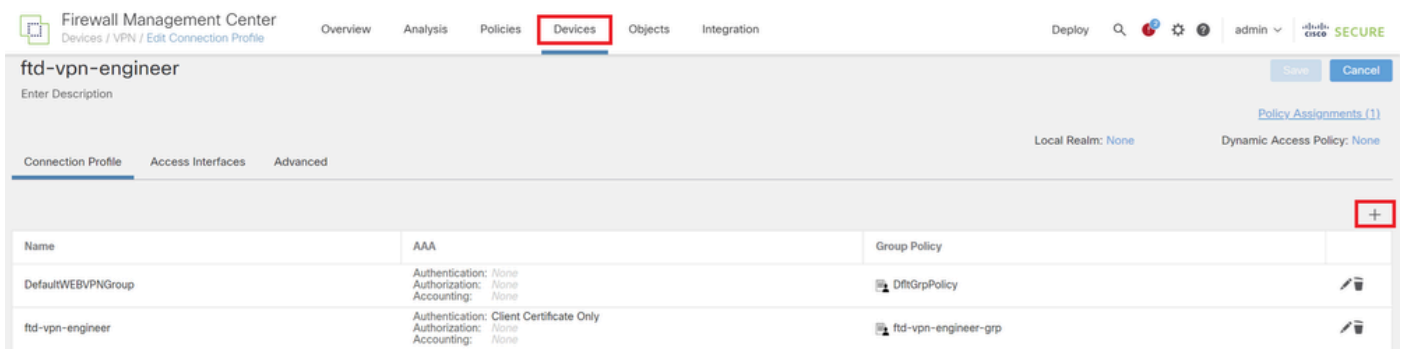
確認輸入的遠端訪問VPN策略資訊，然後按一下Finish按鈕。



遠端訪問VPN策略的詳細資訊

## 步驟 11. 為Manager VPN客戶端增加連線配置檔案

導航到Devices > VPN > Remote Access > Connection Profile，按一下+按鈕。



為Manager VPN客戶端增加連線配置檔案

輸入連線配置檔案的必要資訊，然後按一下Save按鈕。

- 名稱：ftd-vpn-manager
- 組策略：ftd-vpn-manager-grp
- IPv4地址池：ftd-vpn-manager-pool

## Add Connection Profile



Connection Profile:\*

Group Policy:\*  +

[Edit Group Policy](#)

**Client Address Assignment**   AAA   Aliases

IP Address for the remote clients can be assigned from local IP Address pools/DHCP Servers/AAA Servers. Configure the 'Client Address Assignment Policy' in the Advanced tab to define the assignment criteria.

Address Pools: +

Name	IP Address Range	
<b>ftd-vpn-manager-pool</b>	172.16.1.120-172.16.1.130	ftd-vpn-manager-pool

DHCP Servers: +

Name	DHCP Server IP Address	
------	------------------------	--

Manager VPN客戶端的連線配置檔案的詳細資訊

確認新增的連線設定檔。

Firewall Management Center  
Devices / VPN / Edit Connection Profile

Overview   Analysis   Policies   **Devices**   Objects   Integration

Deploy   🔍   ⚙️   🛡️   admin   🔒   **SECURE**

ftd-vpn-engineer   You have unsaved changes     

Enter Description

[Policy Assignments \(1\)](#)

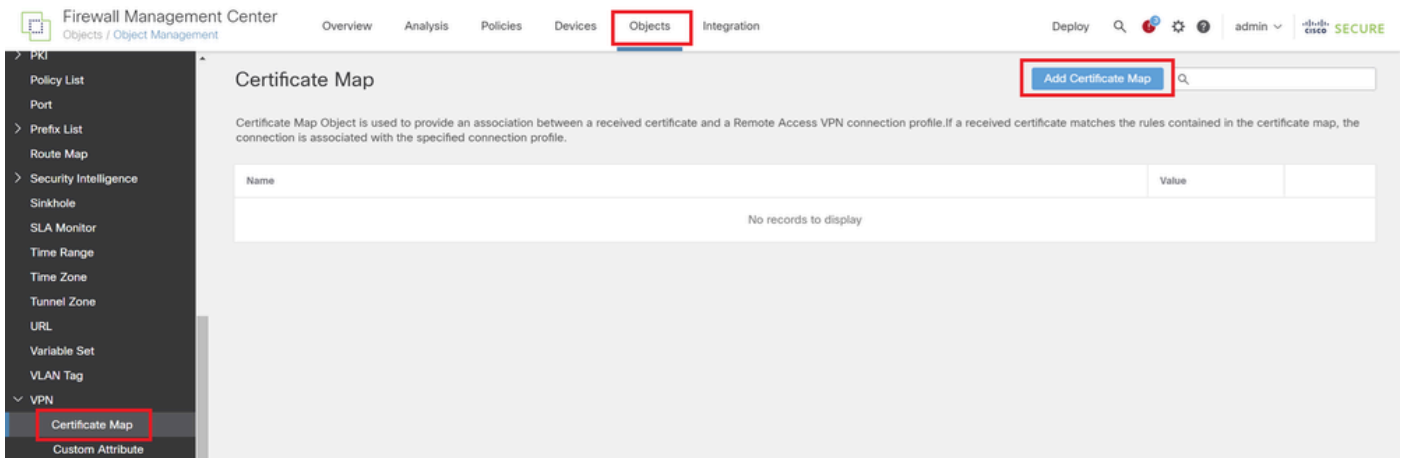
Local Realm: None   Dynamic Access Policy: None

Name	AAA	Group Policy	
DefaultWEBVPGGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy	🗑️
<b>ftd-vpn-engineer</b>	Authentication: Client Certificate Only Authorization: None Accounting: None	<b>ftd-vpn-engineer-grp</b>	🗑️
<b>ftd-vpn-manager</b>	Authentication: Client Certificate Only Authorization: None Accounting: None	<b>ftd-vpn-manager-grp</b>	🗑️

確認增加的連線配置檔案

## 步驟 12. 增加證書對映

導航到對象>對象管理> VPN >證書對映，點選增加證書對映按鈕。



增加證書對映

輸入工程師VPN客戶端的證書對映所需的資訊，然後按一下Save按鈕。

- 對映名稱：cert-map-engineer
- 對映規則：CN ( 公用名 ) 等於vpnEngineerClientCN



## Add Certificate Map



Map Name\*:

cert-map-engineer

Mapping Rule

Add Rule

Configure the certificate matching rule

#	Field	Component	Operator	Value		
1	Subject	CN (Common Name)	Equals	vpnEngineerCle...		

Cancel

Save

Engineer Client的證書對映

為管理器VPN客戶端的證書對映輸入必要資訊，然後按一下Save按鈕。

- 對映名稱：cert-map-manager
- 對映規則：CN ( 公用名 ) 等於vpnManagerClientCN

## Add Certificate Map



Map Name\*:

cert-map-manager

Mapping Rule

Configure the certificate matching rule

Add Rule

#	Field	Component	Operator	Value		
1	Subject	CN (Common Name)	Equals	vpnManagerClie...		

Cancel

Save

Manager客戶端的證書對映

確認新增的憑證對應。

Firewall Management Center  
Objects / Object Management

Overview Analysis Policies Devices **Objects** Integration

Deploy admin **SECURE**

### Certificate Map

Add Certificate Map

Certificate Map Object is used to provide an association between a received certificate and a Remote Access VPN connection profile. If a received certificate matches the rules contained in the certificate map, the connection is associated with the specified connection profile.

Name	Value		
cert-map-engineer	1 Criteria		
cert-map-manager	1 Criteria		

新憑證對應

步驟 13. 將證書對映繫結到連線配置檔案

導覽至 Devices > VPN > Remote Access，編輯ftd-vpn-engineer。然後，導航到高級>證書對映，點選增加對映按鈕。

ftd-vpn-engineer

Advanced

General Settings for Connection Profile Mapping

Use the configured rules to match a certificate to a Connection Profile

Certificate to Connection Profile Mapping

Please provide at least one Certificate Mapping.

Certificate Map	Connection Profile
No Records Found	

Add Mapping

繫結證書對映

將證書對映繫結到工程師VPN客戶端的連線配置檔案。

- 證書對映名稱：cert-map-engineer
- 連線Profile: ftd-vpn-engineer

## Add Connection Profile to Certificate Map ?

Choose a Certificate Map and associate Connection Profiles to selected Certificate Map.

Certificate Map Name\*:  
cert-map-engineer

+

Connection Profile\*:  
ftd-vpn-engineer

Cancel OK

工程師VPN客戶端的繫結證書對映

將證書對映繫結到管理器VPN客戶端的連線配置檔案。

- 證書對映名稱：cert-map-manager
- 連線配置檔案：ftd-vpn-manager

# Add Connection Profile to Certificate Map



Choose a Certificate Map and associate Connection Profiles to selected Certificate Map.

Certificate Map Name\*:  
cert-map-manager

+

Connection Profile\*:  
ftd-vpn-manager

Cancel OK

Manager VPN客戶端的繫結證書對映

確認憑證繫結的設定。

Firewall Management Center  
Devices / VPN / Edit Advanced

Overview Analysis Policies Devices Objects Integration

Deploy Search Settings Help admin | Cisco SECURE

ftd-vpn-engineer  
Enter Description

You have unsaved changes Save Cancel

Policy Assignments (1)

Local Realm: None Dynamic Access Policy: None

Connection Profile Access Interfaces Advanced

Secure Client Images  
Secure Client Customization  
GUI Text and Messages  
Icons and Images  
Scripts  
Binaries  
Custom Installer Transforms  
Localized Installer Transforms  
Address Assignment Policy  
Certificate Maps  
Group Policies

General Settings for Connection Profile Mapping  
The device processes the policies in the order listed below until it finds a match

Use group URL if group URL and Certificate Map match different Connection Profiles  
 Use the configured rules to match a certificate to a Connection Profile

Certificate to Connection Profile Mapping  
Client request is checked against each Certificate Map, associated Connection Profile will be used when rules are matched. If none of the Certificate Map is matched, default connection profile will be chosen.

Certificate Map	Connection Profile	
cert-map-engineer	ftd-vpn-engineer	
cert-map-manager	ftd-vpn-manager	

Add Mapping

確認憑證繫結

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

// Defines a pool of addresses
ip local pool ftd-vpn-engineer-pool 172.16.1.100-172.16.1.110 mask 255.255.255.0
ip local pool ftd-vpn-manager-pool 172.16.1.120-172.16.1.130 mask 255.255.255.0

// Defines Trustpoint for Server Certificate
crypto ca trustpoint ftd-vpn-cert
keypair ftd-vpn-cert
crl configure

// Server Certificate Chain
crypto ca certificate chain ftd-vpn-cert
certificate 22413df584b6726c
3082037c 30820264 a0030201 02020822 413df584 b6726c30 0d06092a 864886f7
.....
quit

certificate ca 5242a02e0db6f7fd
3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7
.....
quit

// Defines Certificate Map for Engineer VPN Clients
crypto ca certificate map cert-map-engineer 10
subject-name attr cn eq vpnEngineerClientCN

// Defines Certificate Map for Manager VPN Clients
crypto ca certificate map cert-map-manager 10
subject-name attr cn eq vpnManagerClientCN

// 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
certificate-group-map cert-map-engineer 10 ftd-vpn-engineer
certificate-group-map cert-map-manager 10 ftd-vpn-manager
error-recovery disable

// Configures the group-policy to allow SSL connections from manager VPN clients
group-policy ftd-vpn-manager-grp internal
group-policy ftd-vpn-manager-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 ikev2 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 group-policy to allow SSL connections from engineer VPN clients
group-policy ftd-vpn-engineer-grp internal
group-policy ftd-vpn-engineer-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 certificate authentication for engineer VPN clients
tunnel-group ftd-vpn-engineer type remote-access
tunnel-group ftd-vpn-engineer general-attributes
address-pool ftd-vpn-engineer-pool
default-group-policy ftd-vpn-engineer-grp
tunnel-group ftd-vpn-engineer webvpn-attributes
authentication certificate
group-alias ftd-vpn-engineer enable
```

```
// Configures the tunnel-group to use the certificate authentication for manager VPN clients
tunnel-group ftd-vpn-manager type remote-access
tunnel-group ftd-vpn-manager general-attributes
address-pool ftd-vpn-manager-pool
default-group-policy ftd-vpn-manager-grp
tunnel-group ftd-vpn-manager webvpn-attributes
authentication certificate
```

## 在VPN客戶端中確認

### 步驟 1. 確認使用者端憑證

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



確認工程師VPN客戶端的證書

按兩下客戶端證書，導航至詳細資訊，檢查主題的詳細資訊。

- 主題：CN = vpnEngineerClientCN

# Certificate



General Details Certification Path

Show: <All>

Field	Value
Valid to	Wednesday, June 18, 2025 5:...
Subject	vpnEngineerClientCN, vpnEngl...
Public key	RSA (2048 Bits)
Public key parameters	05 00
Key Usage	Digital Signature, Key Encipher...
Enhanced Key Usage	Client Authentication (1.3.6.1....
Netscape Comment	xca certificate
Thumbprint algorithm	sha1

CN = vpnEngineerClientCN

O = Cisco  
L = Tokyo  
S = Tokyo  
C = JP

Edit Properties...

Copy to File...

OK

工程師客戶端證書的詳細資訊

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





確認Manager VPN客戶端的證書

按兩下客戶端證書，導航至詳細資訊，檢查主題的詳細資訊。

- 主題：CN = vpnManagerClientCN

# Certificate



General Details Certification Path

Show: <All>

Field	Value
Issued	Thursday, June 19, 2025 9:41...
Subject	vpnManagerClientCN, vpnMan...
Public Key	RSA (2048 Bits)
Public key parameters	05 00
Key Usage	Digital Signature, Key Encipher...
Enhanced Key Usage	Client Authentication (1.3.6.1....
Netscape Comment	xca certificate
Thumbprint algorithm	sha1

CN = vpnManagerClientCN  
O = Cisco  
L = Tokyo  
S = Tokyo  
C = JP

Edit Properties...

Copy to File...

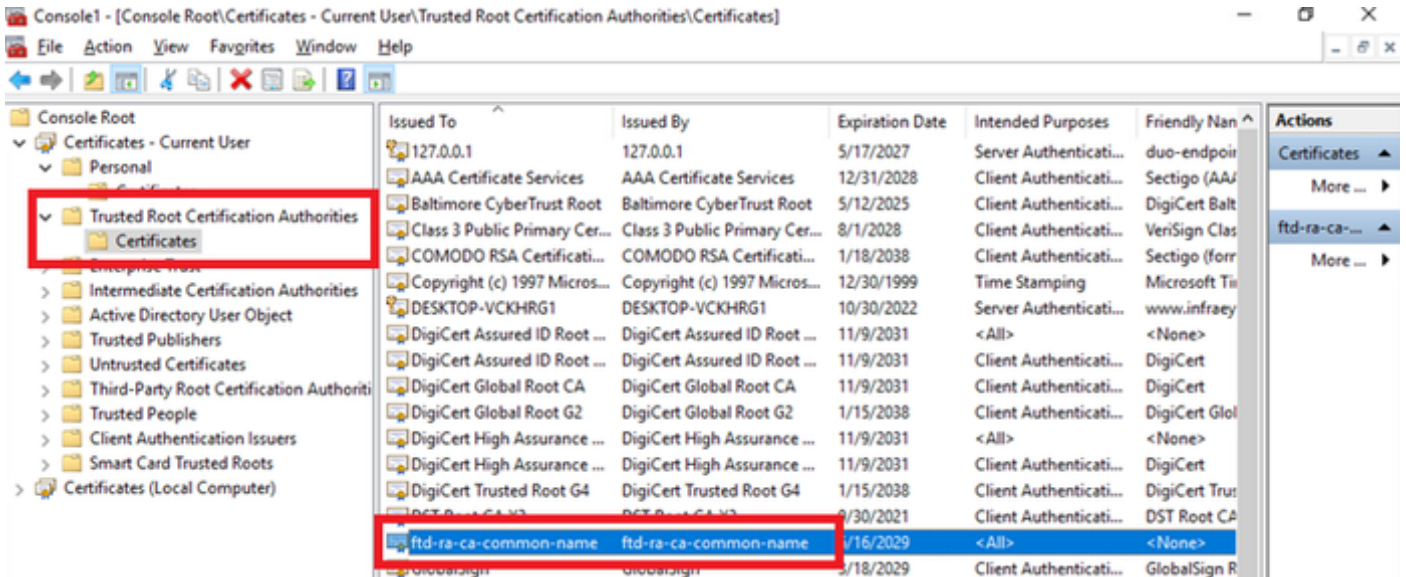
OK

Manager客戶端證書的詳細資訊

## 步驟 2. 確認CA

在工程VPN客戶端和管理器VPN客戶端中，導航到證書-當前使用者>受信任的根證書頒發機構>證書，檢查用於身份驗證的CA。

- 頒發者：ftd-ra-ca-common-name

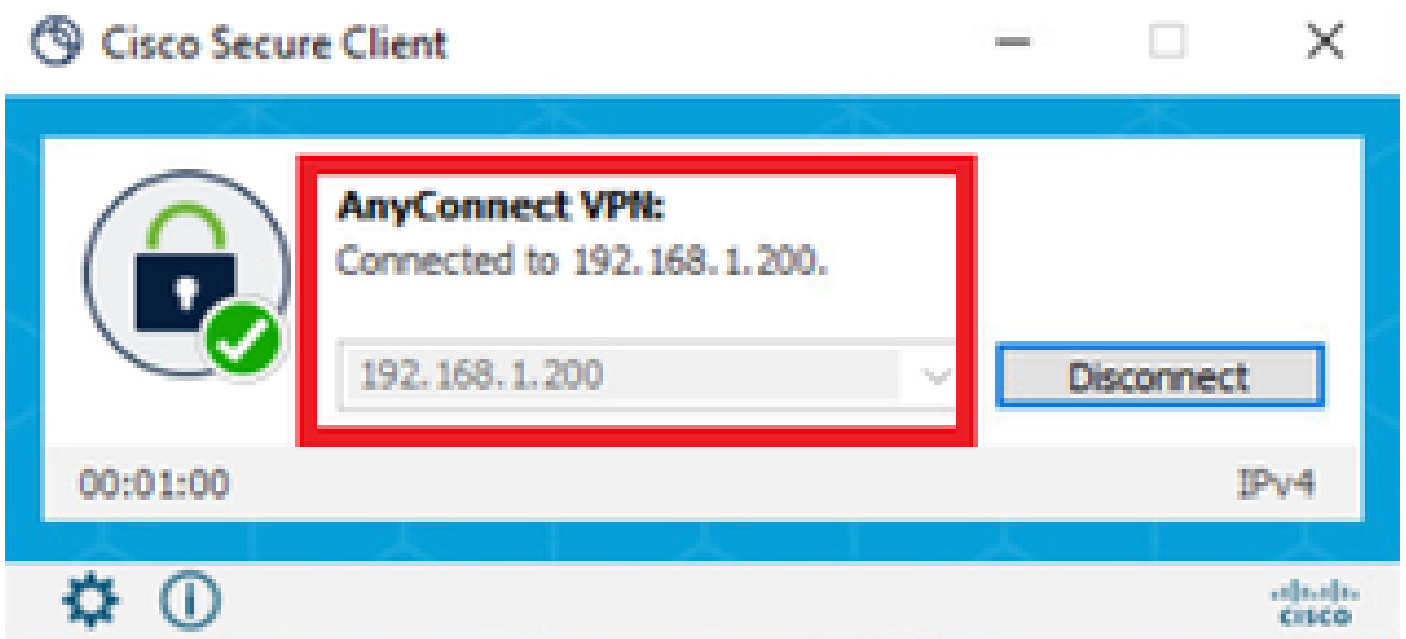


確認CA

## 驗證

### 步驟 1. 啟動VPN連線

在工程VPN客戶端中，啟動Cisco Secure Client連線。無需輸入使用者名稱和密碼，VPN連線成功。



從工程師客戶端啟動VPN連線

在Manager VPN客戶端中，啟動Cisco Secure Client連線。無需輸入使用者名稱和密碼，VPN連線成功。



從管理器客戶端啟動VPN連線

## 步驟 2. 確認FMC中的活動會話

導航到Analysis > Users > Active Sessions，檢查VPN身份驗證的活動會話。

Login Time	Realm/Username	Last Seen	Authentication Type	Current IP	Realm	Username	First Name	Last Name
2024-06-19 11:01:19	Discovered Identities\vpnManagerClientCN	2024-06-19 11:01:19	VPN Authentication	172.16.1.120	Discovered Identities	vpnManagerClientCN		
2024-06-19 11:00:35	Discovered Identities\vpnEngineerClientCN	2024-06-19 11:00:35	VPN Authentication	172.16.1.101	Discovered Identities	vpnEngineerClientCN		

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，以確認工程師和管理員的VPN作業階段。

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

Session Type: AnyConnect Detailed

Username : vpnEngineerClientCN Index : 13

Assigned IP : 172.16.1.101 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 : 14782 Bytes Rx : 12714

Pkts Tx : 2 Pkts Rx : 32

Pkts Tx Drop : 0 Pkts Rx Drop : 0

Group Policy : ftd-vpn-engineer-grp Tunnel Group : ftd-vpn-engineer

Login Time : 02:00:35 UTC Wed Jun 19 2024

Duration : 0h:00m:55s  
Inactivity : 0h:00m:00s  
VLAN Mapping : N/A VLAN : none  
Audt Sess ID : cb0071820000d00066723bc3  
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:  
Tunnel ID : 13.1  
Public IP : 192.168.1.11  
Encryption : none Hashing : none  
TCP Src Port : 50225 TCP Dst Port : 443  
Auth Mode : Certificate  
Idle Time Out: 30 Minutes Idle TO Left : 29 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 : 7391 Bytes Rx : 0  
Pkts Tx : 1 Pkts Rx : 0  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:  
Tunnel ID : 13.2  
Assigned IP : 172.16.1.101 Public IP : 192.168.1.11  
Encryption : AES-GCM-128 Hashing : SHA256  
Ciphersuite : TLS\_AES\_128\_GCM\_SHA256  
Encapsulation: TLSv1.3 TCP Src Port : 50232  
TCP Dst Port : 443 Auth Mode : Certificate  
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
Client OS : Windows  
Client Type : SSL VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62  
Bytes Tx : 7391 Bytes Rx : 1775  
Pkts Tx : 1 Pkts Rx : 2  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:  
Tunnel ID : 13.3  
Assigned IP : 172.16.1.101 Public IP : 192.168.1.11  
Encryption : AES-GCM-256 Hashing : SHA384  
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384  
Encapsulation: DTLSv1.2 UDP Src Port : 50825  
UDP Dst Port : 443 Auth Mode : Certificate  
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 : 10939  
Pkts Tx : 0 Pkts Rx : 30  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

Username : vpnManagerClientCN Index : 14  
Assigned IP : 172.16.1.120 Public IP : 192.168.1.21  
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 : 14782 Bytes Rx : 13521  
Pkts Tx : 2 Pkts Rx : 57  
Pkts Tx Drop : 0 Pkts Rx Drop : 0  
Group Policy : ftd-vpn-manager-grp Tunnel Group : ftd-vpn-manager  
Login Time : 02:01:19 UTC Wed Jun 19 2024  
Duration : 0h:00m:11s  
Inactivity : 0h:00m:00s  
VLAN Mapping : N/A VLAN : none  
Audt Sess ID : cb0071820000e00066723bef  
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:  
Tunnel ID : 14.1  
Public IP : 192.168.1.21  
Encryption : none Hashing : none  
TCP Src Port : 49809 TCP Dst Port : 443  
Auth Mode : Certificate  
Idle Time Out: 30 Minutes Idle TO Left : 29 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 : 7391 Bytes Rx : 0  
Pkts Tx : 1 Pkts Rx : 0  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:  
Tunnel ID : 14.2  
Assigned IP : 172.16.1.120 Public IP : 192.168.1.21  
Encryption : AES-GCM-128 Hashing : SHA256  
Ciphersuite : TLS\_AES\_128\_GCM\_SHA256  
Encapsulation: TLSv1.3 TCP Src Port : 49816  
TCP Dst Port : 443 Auth Mode : Certificate  
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
Client OS : Windows  
Client Type : SSL VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62  
Bytes Tx : 7391 Bytes Rx : 3848  
Pkts Tx : 1 Pkts Rx : 25  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:  
Tunnel ID : 14.3  
Assigned IP : 172.16.1.120 Public IP : 192.168.1.21  
Encryption : AES-GCM-256 Hashing : SHA384  
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384  
Encapsulation: DTLSv1.2 UDP Src Port : 65501  
UDP Dst Port : 443 Auth Mode : Certificate  
Idle Time Out: 30 Minutes Idle TO Left : 30 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 : 9673

Pkts Tx : 0 Pkts Rx : 32  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

## 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。

這是來自工程師客戶端的VPN連線期間Lina引擎中的調試日誌示例。

<#root>

```
Jun 19 2024 02:00:35: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClientCN
Jun 19 2024 02:00:35: %FTD-6-717022:
```

**Certificate was successfully validated**

```
. serial number: 7AF1C78ADCC8F941, subject name:
```

```
CN=vpnEngineerClientCN
```

```
,OU=vpnEngineerClientOU,O=Cisco,L=Tokyo,ST=Tokyo,C=JP.
```

```
Jun 19 2024 02:00:35: %FTD-7-717038: Tunnel group match found.
```

```
Tunnel Group: ftd-vpn-engineer
```

```
, Peer certificate: serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClientCN,OU=vpnEngineerClientOU,O=Cisco,L=Tokyo,ST=Tokyo,C=JP.
```

```
Jun 19 2024 02:00:35: %FTD-6-113009: AAA retrieved default group policy (ftd-vpn-engineer-grp) for user
```

```
Jun 19 2024 02:00:46: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.11/50
```

下面是來自管理器客戶端的VPN連線期間Lina引擎中的調試日誌示例。

<#root>

```
Jun 19 2024 02:01:19: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 1AD1B5EAE28C6D3C, subject name: CN=vpnManagerClientCN
```

```
Jun 19 2024 02:01:19: %FTD-6-717022:
```

**Certificate was successfully validated**

```
. serial number: 1AD1B5EAE28C6D3C, subject name:
```

```
CN=vpnManagerClientCN
```

```
,OU=vpnManagerClientOU,O=Cisco,L=Tokyo,ST=Tokyo,C=JP.
```

```
Jun 19 2024 02:01:19: %FTD-7-717038: Tunnel group match found.
```

```
Tunnel Group: ftd-vpn-manager
```

```
, Peer certificate: serial number: 1AD1B5EAE28C6D3C, subject name: CN=vpnManagerClientCN,OU=vpnManagerClientOU,O=Cisco,L=Tokyo,ST=Tokyo,C=JP.
```

```
Jun 19 2024 02:01:19: %FTD-6-113009: AAA retrieved default group policy (ftd-vpn-manager-grp) for user
```

```
Jun 19 2024 02:01:25: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.21/65
```

## 相關資訊

[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）。