透過FDM為FTD上的安全使用者端驗證設定憑證比對

目錄

簡介

本檔案介紹如何使用憑證比對進行驗證，透過FDM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裝置管理員(FDM)虛擬
- 防火牆威脅防禦(FTD)虛擬
- VPN身份驗證流程

採用元件

- 思科Firepower裝置管理器虛擬7.2.8
- 思科防火牆威脅防禦虛擬7.2.8

- 思科安全客戶端5.1.4.74
- 設定檔編輯器(Windows) 5.1.4.74

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

CertificateMatch功能允許管理員配置客戶端必須使用的條件，以選擇用於VPN伺服器身份驗證的客戶端證書。此配置在客戶端配置檔案中指定，這是一個XML檔案，可使用配置檔案編輯器進行管理或手動編輯。CertificateMatch功能可用於增強VPN連線的安全性，方法是確保只有具有特定屬性的證書用於VPN連線。

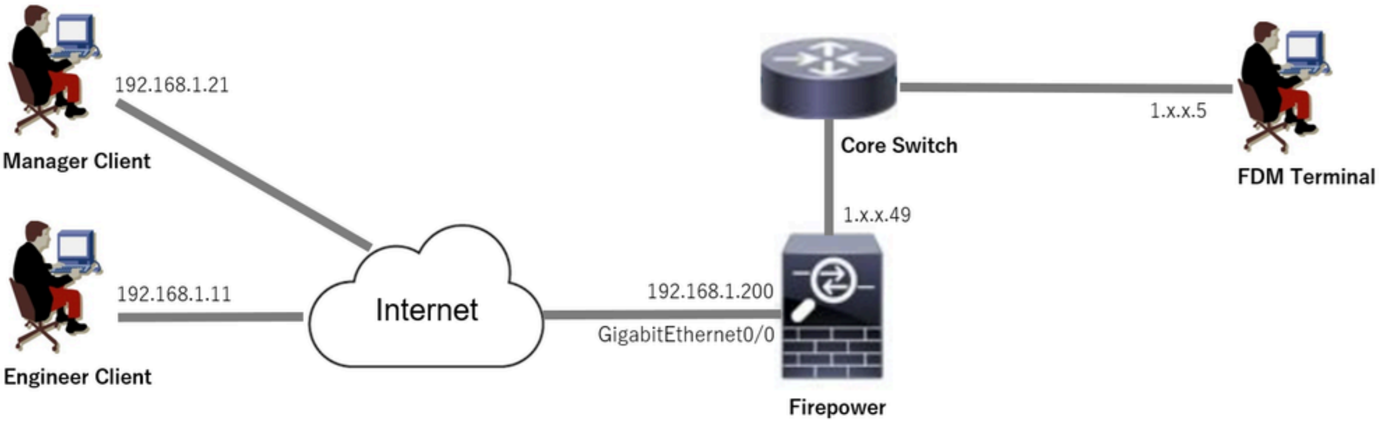
本文檔介紹如何使用SSL證書中的公用名稱對Cisco Secure Client進行身份驗證。

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

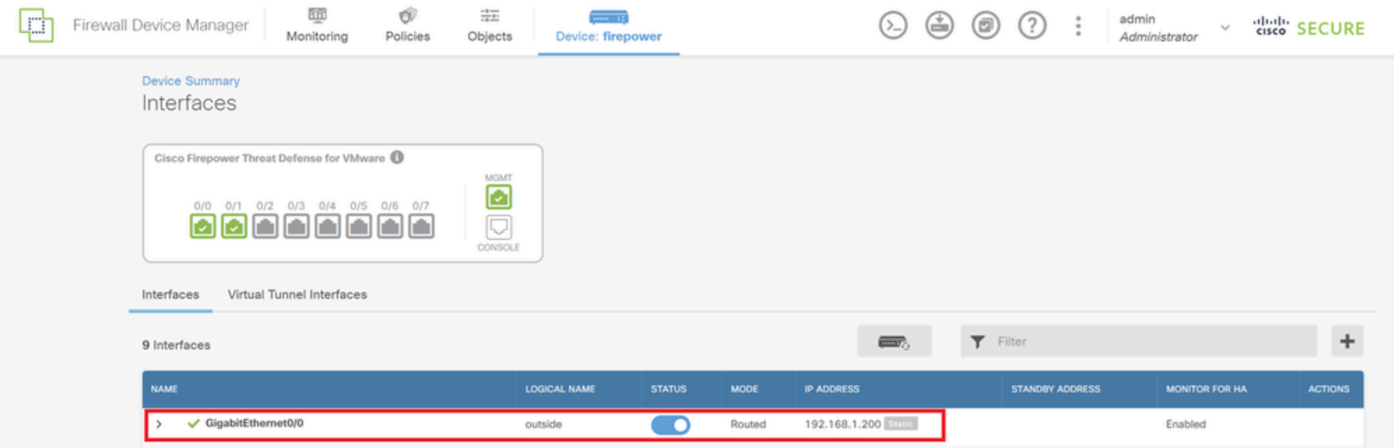
FDM中的組態

步驟 1.設定FTD介面

導覽至Device > Interfaces > View All Interfaces，在Interfaces索引標籤中設定FTD的內部和外部介面。

對於GigabitEthernet0/0，

- 名稱：outside
- IP地址：192.168.1.200/24



Device Summary
Interfaces

Interfaces | Virtual Tunnel Interfaces

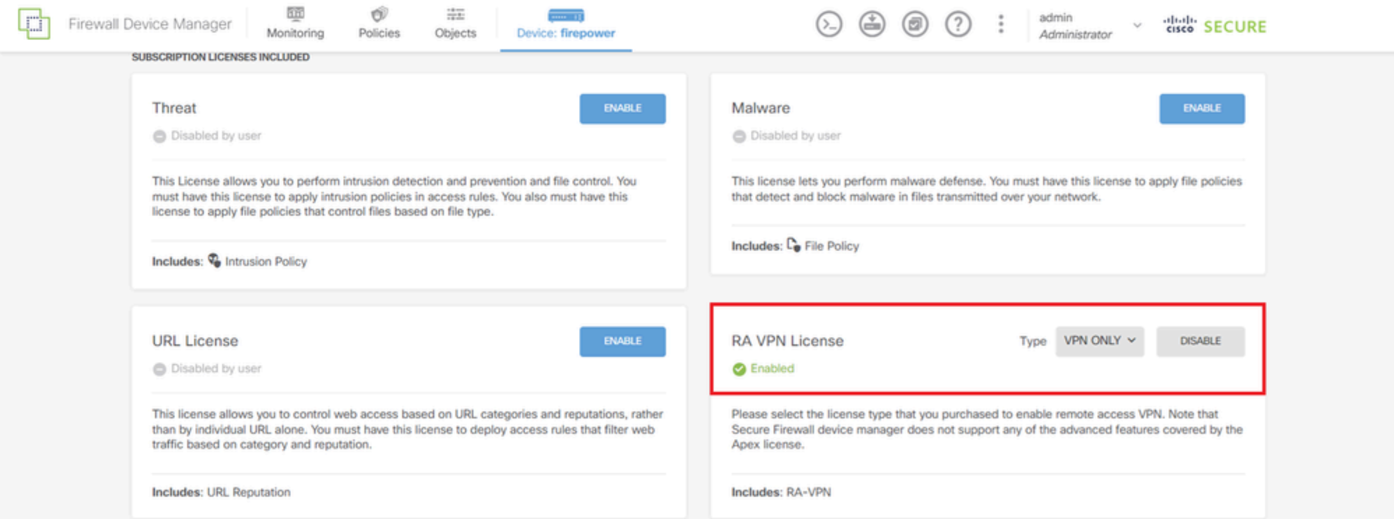
9 Interfaces

NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
> ✓ GigabitEthernet0/0	outside	●	Routed	192.168.1.200 Static		Enabled	

FTD介面

步驟 2.確認思科安全客戶端許可證

導航到裝置>智慧許可證>檢視配置，確認RA VPN許可證專案中的思科安全客戶端許可證。



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 lets you perform malware defense. You must have this license to apply file policies that detect and block malware in files transmitted over your network.
Includes: File Policy

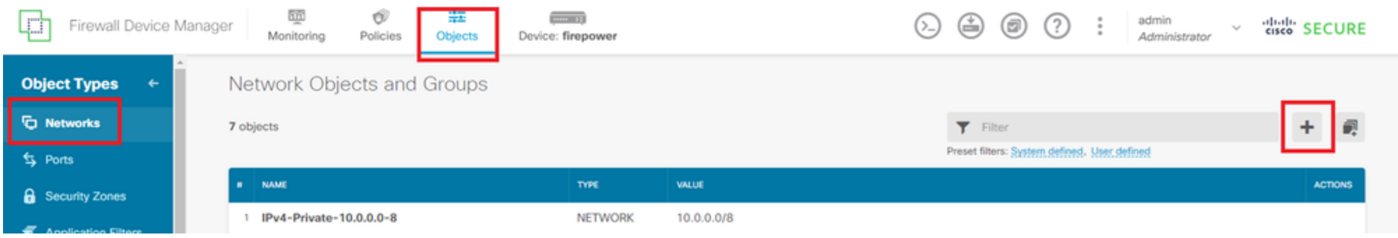
URL License — ENABLE
Disabled by user
This license allows you to control web access based on URL categories and reputations, rather than by individual URL alone. You must have this license to deploy access rules that filter web traffic based on category and reputation.
Includes: URL Reputation

RA VPN License — Type: VPN ONLY — DISABLE
Enabled
Please select the license type that you purchased to enable remote access VPN. Note that Secure Firewall device manager does not support any of the advanced features covered by the Apex license.
Includes: RA-VPN

安全使用者端授權

步驟 3.增加地址池

導航到對象>網路，點選+按鈕。

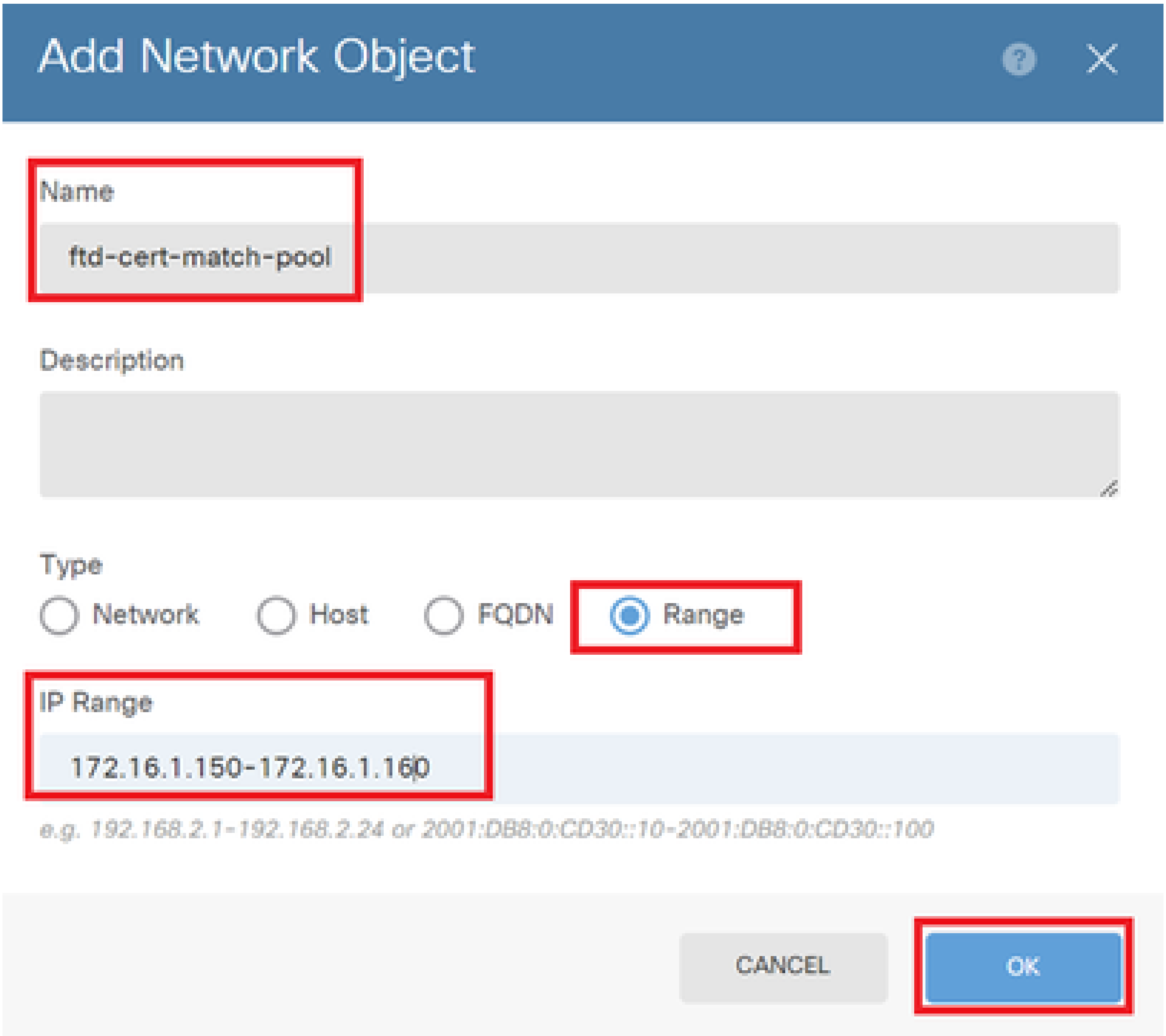


#	NAME	TYPE	VALUE	ACTIONS
1	IPv4-Private-10.0.0.0-8	NETWORK	10.0.0.0/8	

增加地址池

輸入必要資訊以增加新的IPv4地址池。按一下OK 按鈕。

- 名稱：ftd-cert-match-pool
- 型別：範圍
- IP範圍：172.16.1.150-172.16.1.160



Add Network Object

Name

ftd-cert-match-pool

Description

Type

○ Network ○ Host ○ FQDN ● Range

IP Range

172.16.1.150-172.16.1.160

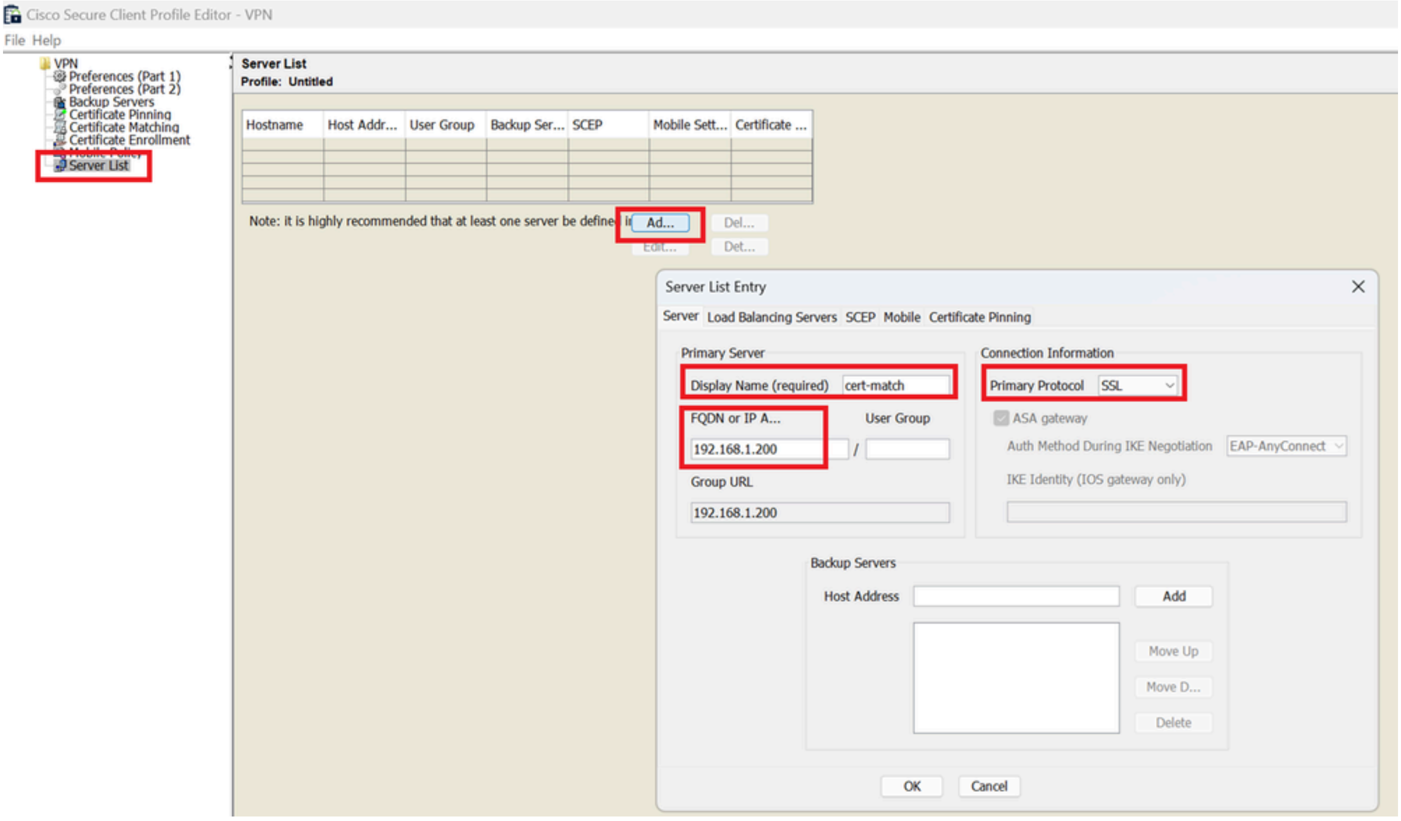
e.g. 192.168.2.1-192.168.2.24 or 2001:DB8:0:CD30::10-2001:DB8:0:CD30::100

IPv4地址池的詳細資訊

步驟 4.建立安全客戶端配置檔案

從思科軟體站點下載並安裝安全客戶端配置檔案編輯器。 導航到伺服器清單，點選增加按鈕。 輸入增加伺服器清單條目所需的資訊，然後按一下OK按鈕。

- 顯示名稱：cert-match
- FQDN或IP地址：192.168.1.200
- 主要通訊協定：SSL



Server List
Profile: Untitled

Note: it is highly recommended that at least one server be defined i

Display Name (required): cert-match

FQDN or IP A...: 192.168.1.200 / User Group:

Group URL: 192.168.1.200

Primary Protocol: SSL

Auth Method During IKE Negotiation: EAP-AnyConnect

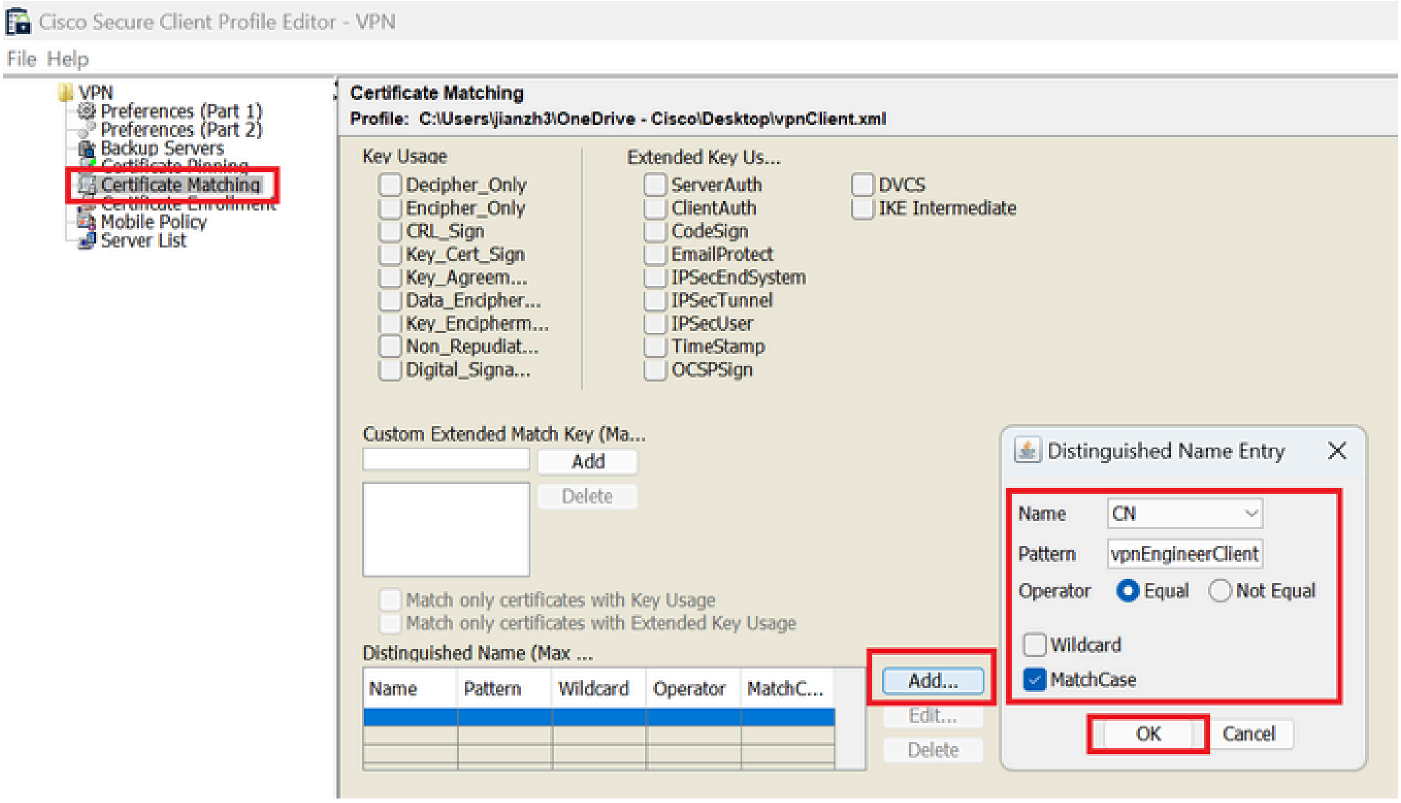
IKE Identity (IOS gateway only):

伺服器清單專案

導航到證書匹配，按一下增加按鈕。 輸入增加可分辨名稱條目的必要資訊，然後按一下OK按鈕。

- 名稱：CN
- 模式：vpnEngineerClientCN
- 運算子：等於

附註：檢查本檔案中的MatchCase選項。



Cisco Secure Client Profile Editor - VPN

File Help

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

Certificate Matching

Profile: C:\Users\jianzh3\OneDrive - Cisco\Desktop\vpnClient.xml

Key Usage
- □ Decipher_Only
- □ Encipher_Only
- □ CRL_Sign
- □ Key_Cert_Sign
- □ Key_Agreem...
- □ Data_Encipher...
- □ Key_Encipherm...
- □ Non_Repudiat...
- □ Digital_Signa...

Extended Key Us...
- □ ServerAuth
- □ ClientAuth
- □ CodeSign
- □ EmailProtect
- □ IPSecEndSystem
- □ IPSecTunnel
- □ IPSecUser
- □ TimeStamp
- □ OCSPSign
- □ DVCS
- □ IKE Intermediate

Custom Extended Match Key (Ma...

□ Match only certificates with Key Usage

□ Match only certificates with Extended Key Usage

Distinguished Name (Max ...

Name	Pattern	Wildcard	Operator	MatchC...

Distinguished Name Entry

Name: CN

Pattern: vpnEngineerClient

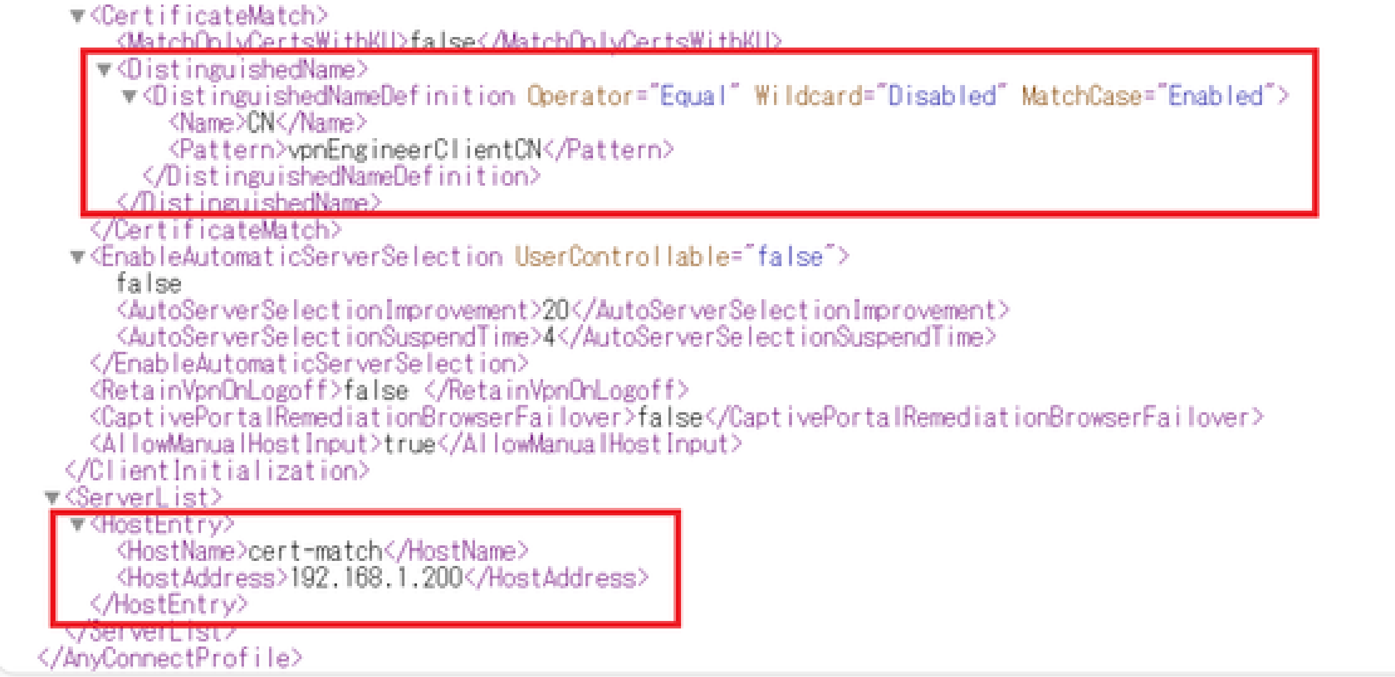
Operator: ● Equal ○ Not Equal

□ Wildcard

☑ MatchCase

辨別名稱專案

將安全使用者端設定檔儲存到本機電腦，並確認設定檔的詳細資訊。

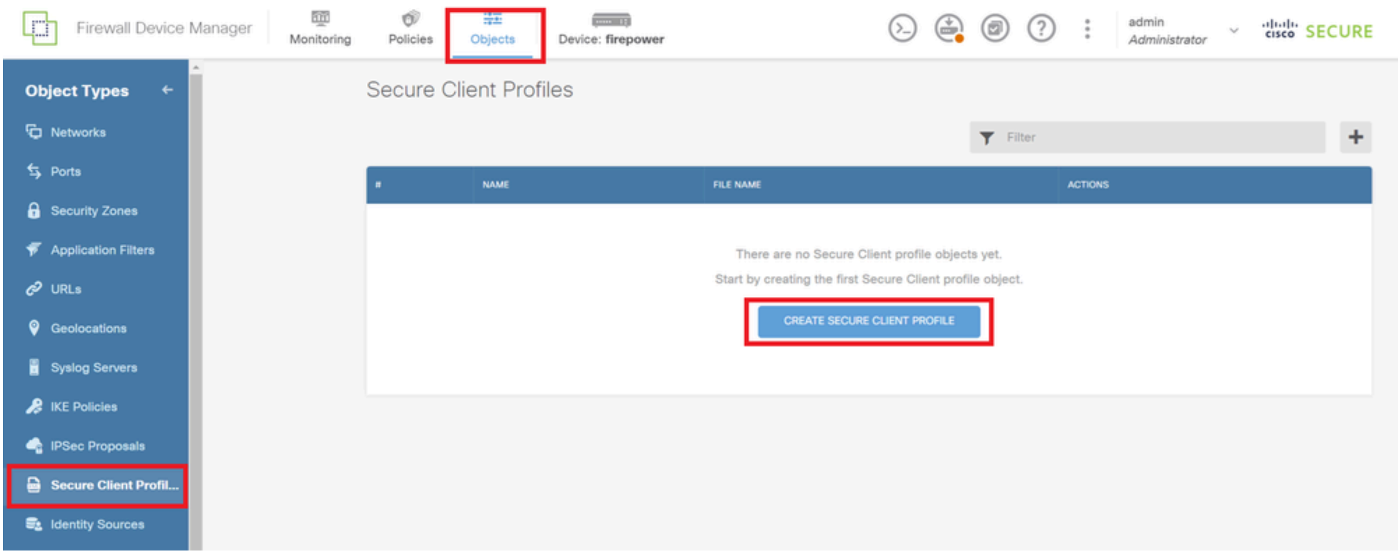


```
▼<CertificateMatch>
    <MatchOnlyCertsWithKU>false</MatchOnlyCertsWithKU>
  ▼<DistinguishedName>
    ▼<DistinguishedNameDefinition Operator="Equal" Wildcard="Disabled" MatchCase="Enabled">
        <Name>CN</Name>
        <Pattern>vpnEngineerClientCN</Pattern>
      </DistinguishedNameDefinition>
    </DistinguishedName>
  </CertificateMatch>
▼<EnableAutomaticServerSelection UserControllable="false">
    false
    <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
    <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
  </EnableAutomaticServerSelection>
  <RetainVpnOnLogoff>false</RetainVpnOnLogoff>
  <CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
  <AllowManualHostInput>true</AllowManualHostInput>
</ClientInitialization>
▼<ServerList>
  ▼<HostEntry>
      <HostName>cert-match</HostName>
      <HostAddress>192.168.1.200</HostAddress>
    </HostEntry>
  </ServerList>
</AnyConnectProfile>
```

安全使用者端設定檔

步驟 5.上傳安全使用者端設定檔至FDM

導航到對象>安全客戶端配置檔案，點選建立安全客戶端配置檔案按鈕。



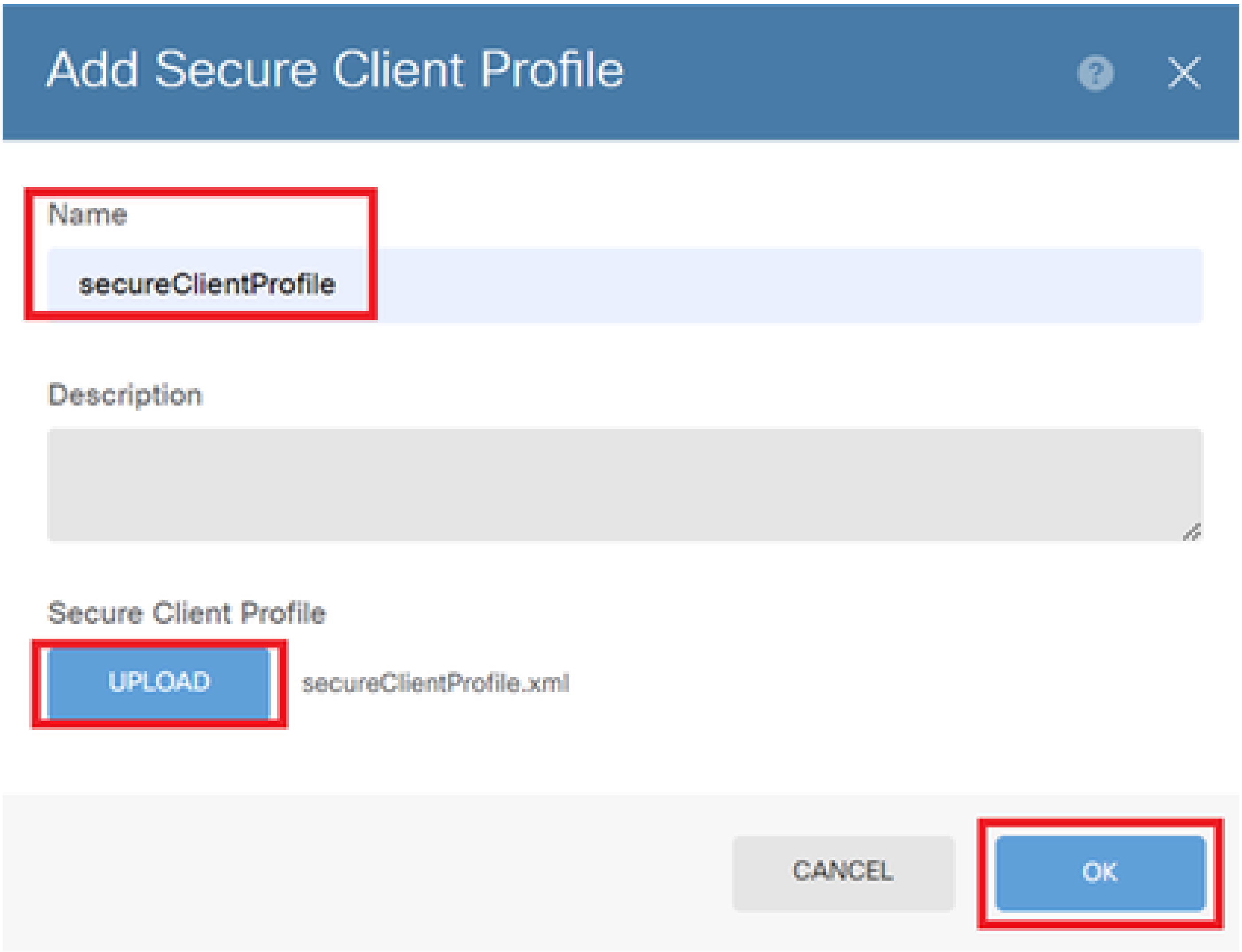
There are no Secure Client profile objects yet.

Start by creating the first Secure Client profile object.

建立安全客戶端配置檔案

輸入必要資訊增加安全客戶端配置檔案，並按一下OK按鈕。

- 名稱：secureClientProfile
- 安全使用者端設定檔：secureClientProfile.xml （從本機電腦上傳）



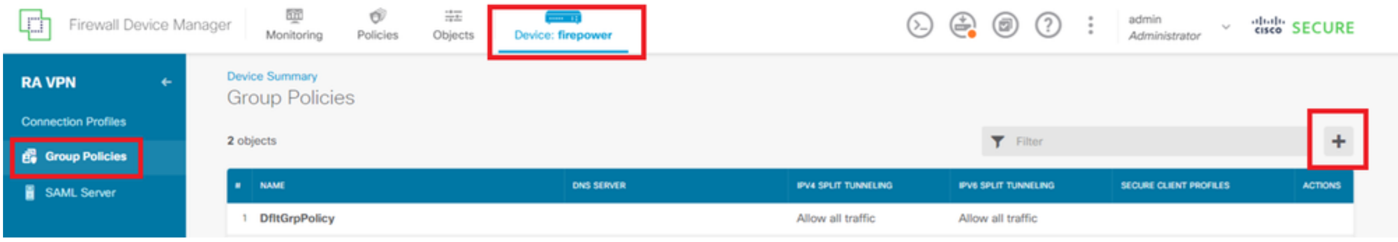
Name: secureClientProfile

Secure Client Profile: secureClientProfile.xml

增加安全客戶端配置檔案

步驟 6.增加組策略

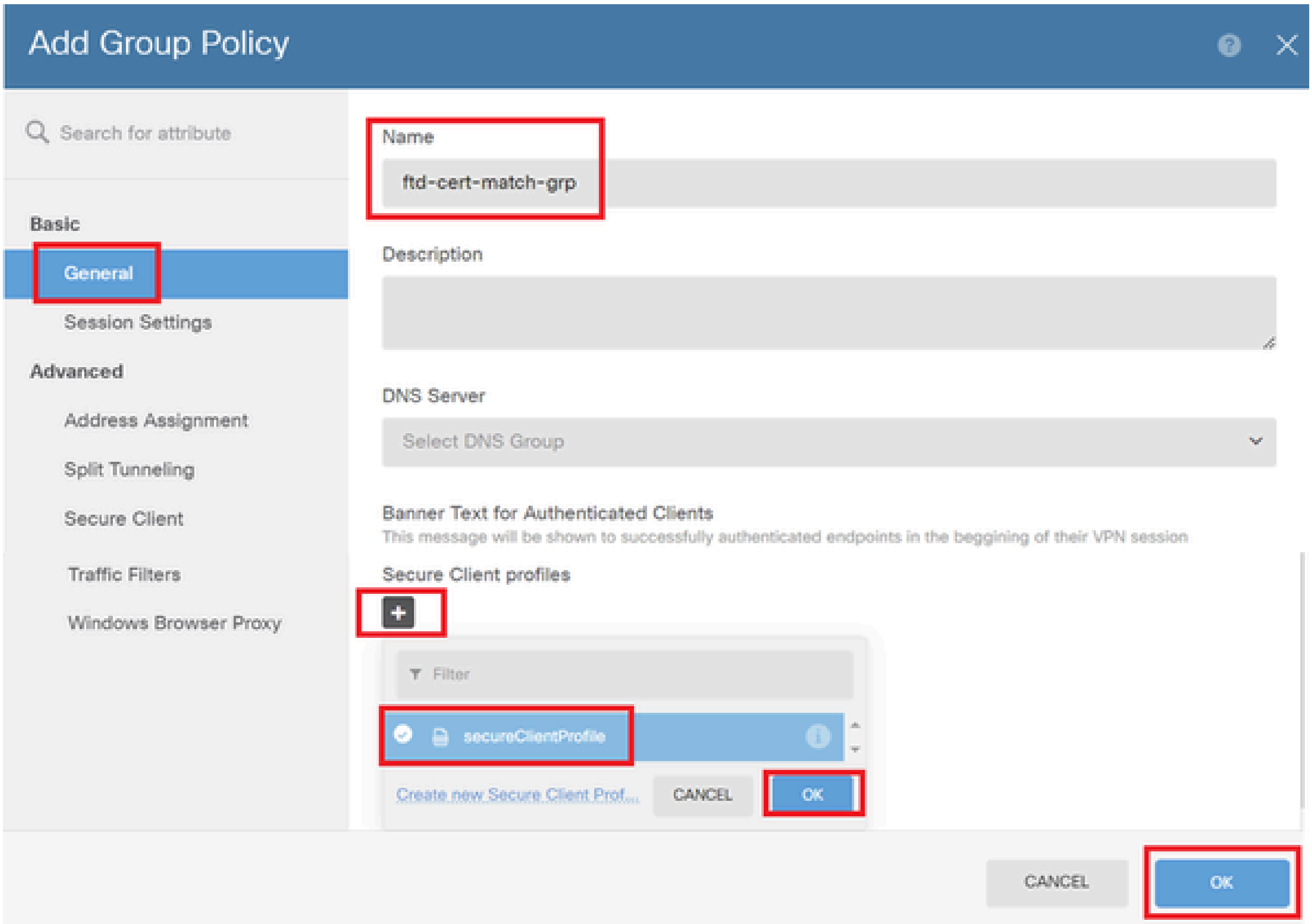
導航到裝置>遠端接入VPN >檢視配置>組策略，點選+按鈕。



增加組策略

輸入增加組策略所需的資訊，並按一下OK按鈕。

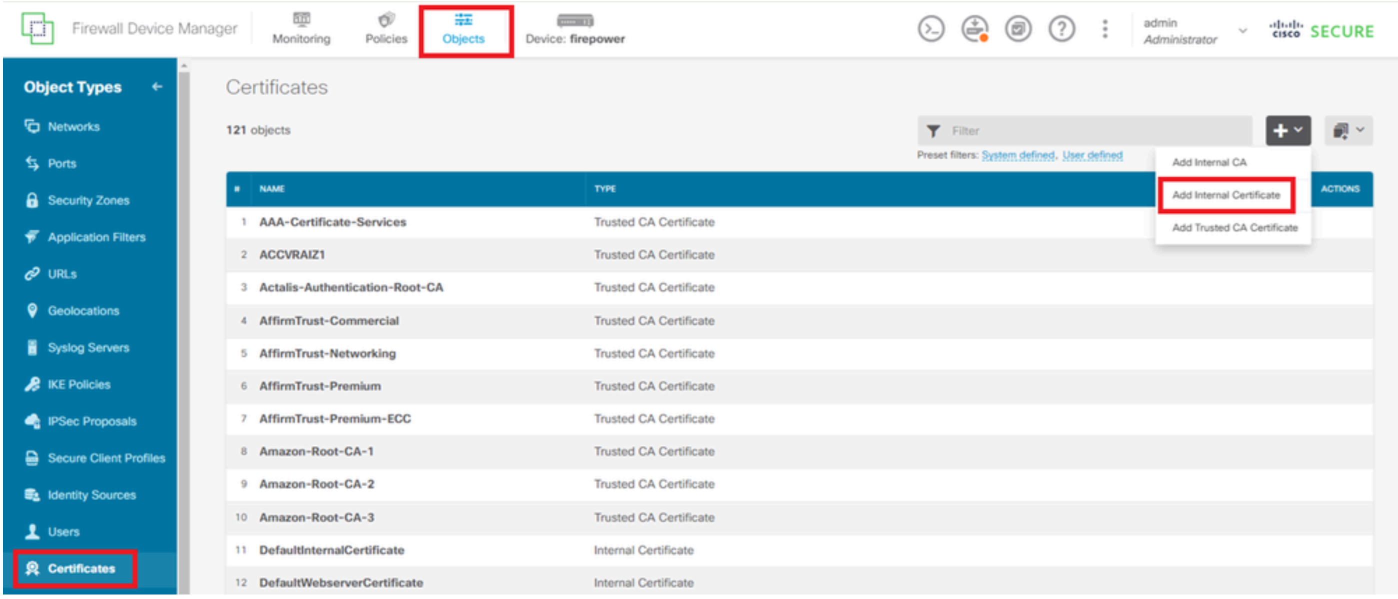
- 名稱：ftd-cert-match-grp
- 安全客戶端配置檔案：secureClientProfile



組策略的詳細資訊

步驟 7.新增FTD憑證

導航到對象>證書，從+專案按一下增加內部證書。



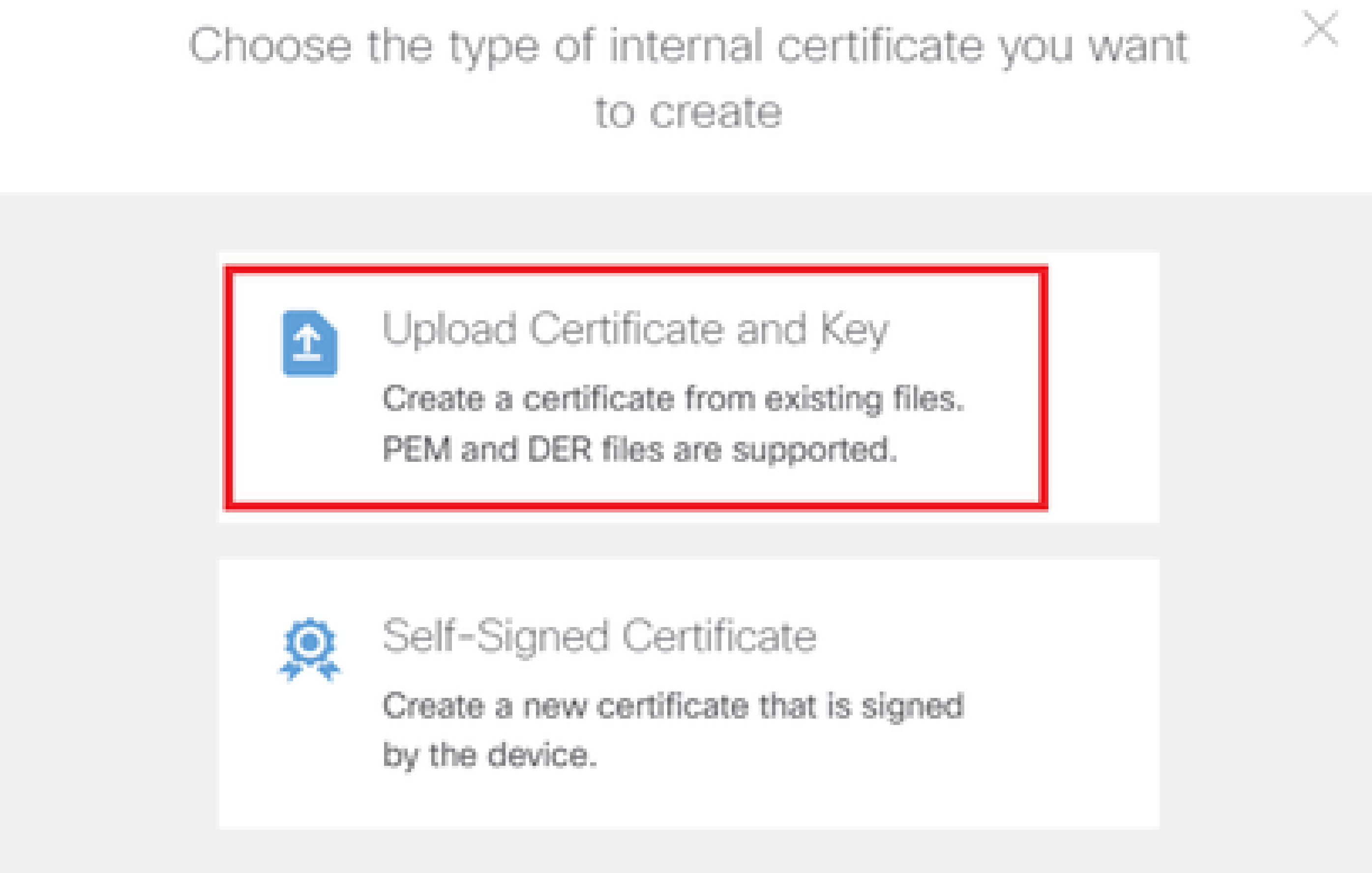
Certificates

121 objects

#	NAME	TYPE	ACTIONS
1	AAA-Certificate-Services	Trusted CA Certificate	
2	ACCVRAIZ1	Trusted CA Certificate	
3	Actalis-Authentication-Root-CA	Trusted CA Certificate	
4	AffirmTrust-Commercial	Trusted CA Certificate	
5	AffirmTrust-Networking	Trusted CA Certificate	
6	AffirmTrust-Premium	Trusted CA Certificate	
7	AffirmTrust-Premium-ECC	Trusted CA Certificate	
8	Amazon-Root-CA-1	Trusted CA Certificate	
9	Amazon-Root-CA-2	Trusted CA Certificate	
10	Amazon-Root-CA-3	Trusted CA Certificate	
11	DefaultInternalCertificate	Internal Certificate	
12	DefaultWebserverCertificate	Internal Certificate	

增加內部證書

按一下Upload Certificate and Key。



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.

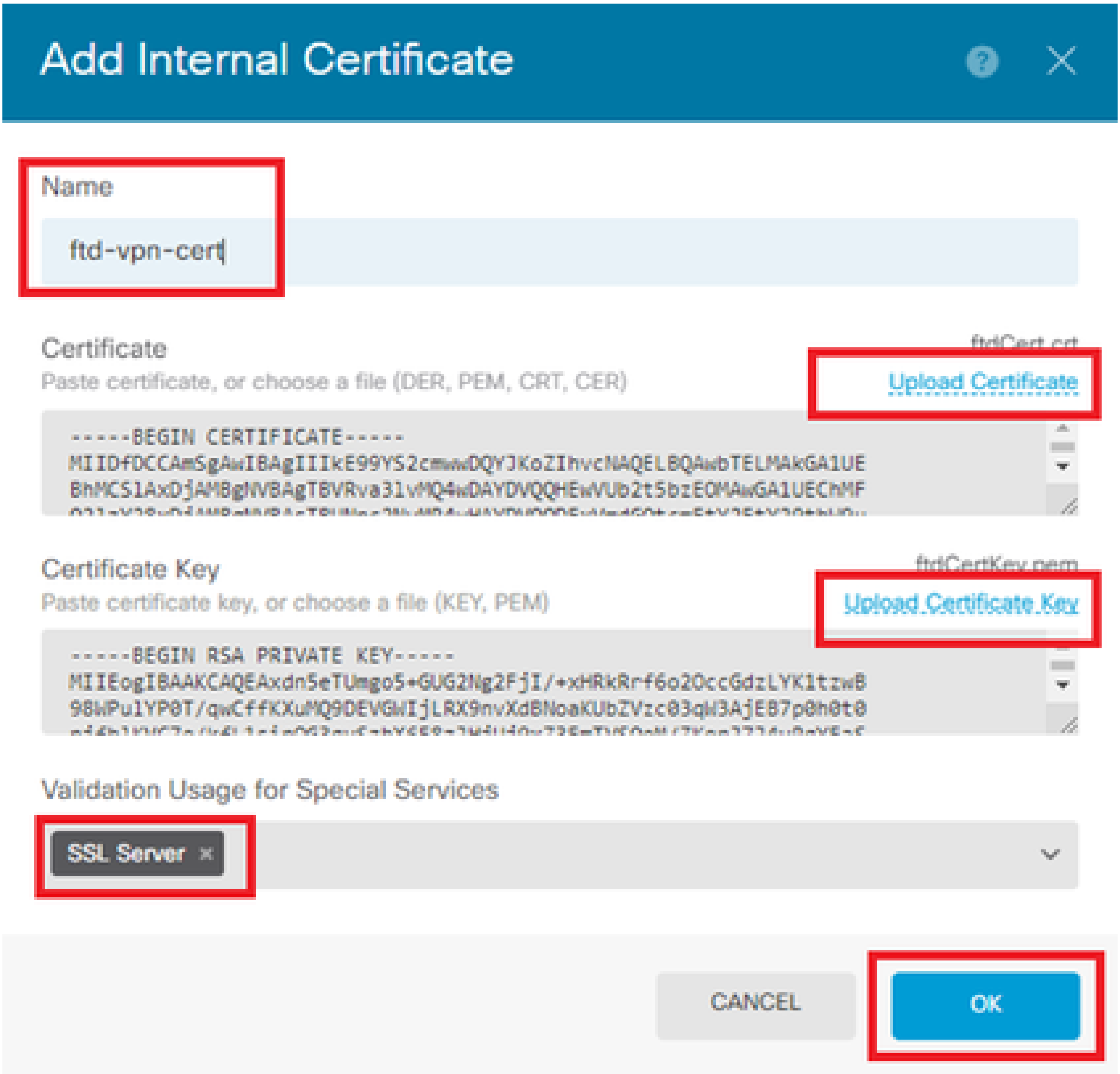
Self-Signed Certificate

Create a new certificate that is signed by the device.

上傳憑證和金鑰

輸入FTD憑證的必要資訊、從本機電腦匯入憑證和憑證金鑰，然後按一下OK按鈕。

- 名稱：ftd-vpn-cert
- 特殊服務的驗證用法：SSL伺服器



Name

ftd-vpn-cert

Certificate

Paste certificate, or choose a file (DER, PEM, CRT, CER)

ftdCert.crt

```
-----BEGIN CERTIFICATE-----
MIIDfDCCAmSgAwIBAgIIIkE99YS2cmwwDQYJKoZIhvcNAQELBQAwbTELMAkGA1UE
BhMCS1AxDjAMBgNVBAgTBVRva3lvMQ4wDAYDVQQHEwVUb2t5bzEOMAwGA1UEChMF
```

Certificate Key

Paste certificate key, or choose a file (KEY, PEM)

ftdCertKey.pem

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAxdn5eTUmgo5+GUG2Ng2FjI/+xHRkRrf6o2OccGdzLYK1tzwB
98WPulYP0T/qwCffKXuMQ9DEVGWIjLRX9nvXdBNoaKUbZVzc03qW3AjEB7p0h0t0
```

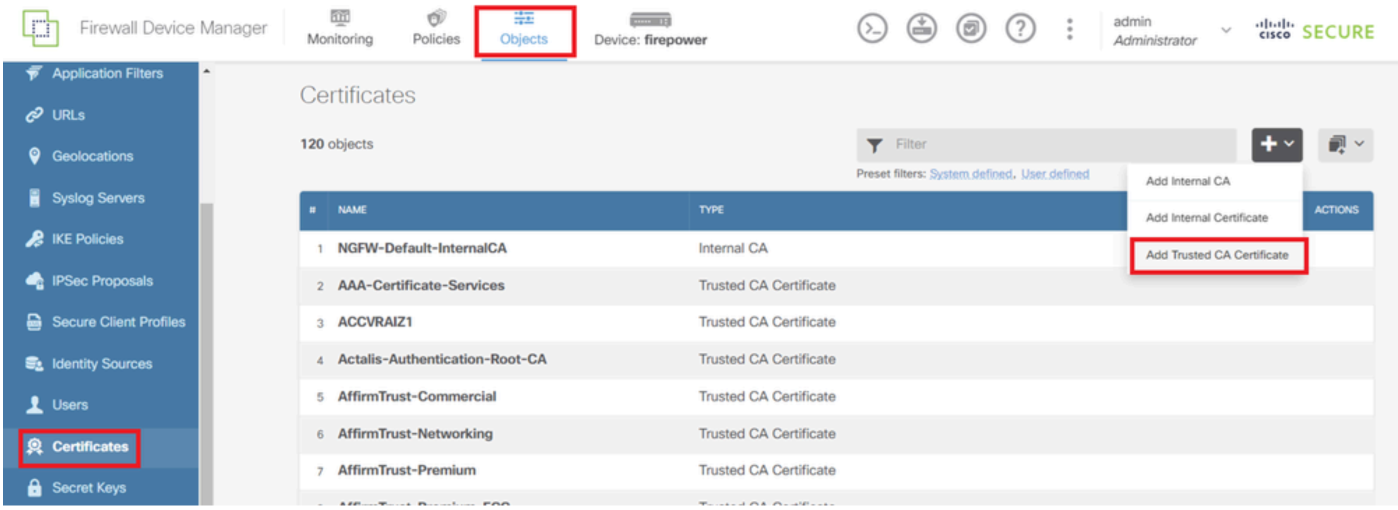
Validation Usage for Special Services

SSL Server ×

內部證書的詳細資訊

步驟 8.新增CA至FTD

導航到對象>證書，從+專案按一下增加受信任CA證書。



Certificates

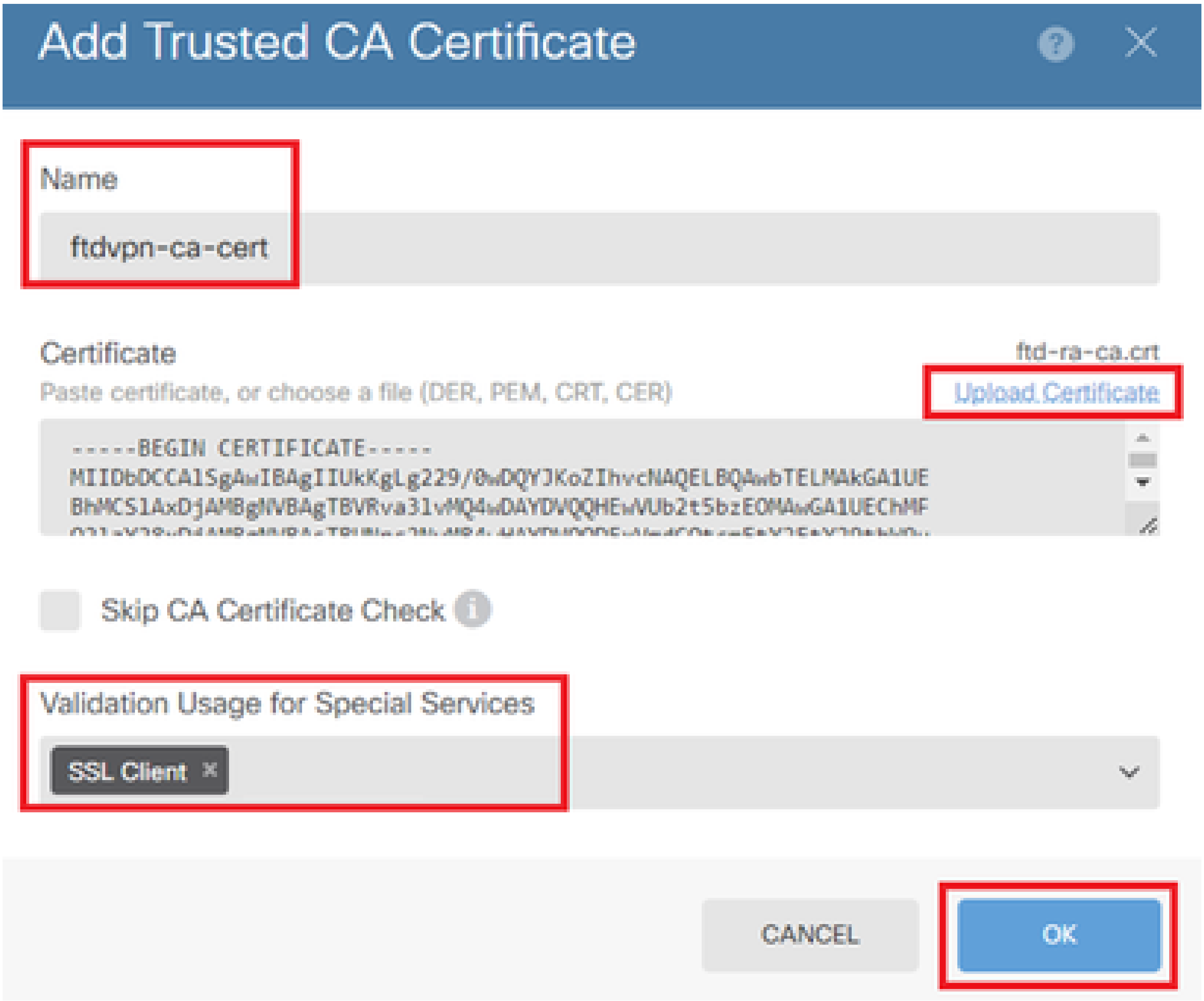
120 objects

#	NAME	TYPE
1	NGFW-Default-InternalCA	Internal CA
2	AAA-Certificate-Services	Trusted CA Certificate
3	ACCVRAIZ1	Trusted CA Certificate
4	Actalis-Authentication-Root-CA	Trusted CA Certificate
5	AffirmTrust-Commercial	Trusted CA Certificate
6	AffirmTrust-Networking	Trusted CA Certificate
7	AffirmTrust-Premium	Trusted CA Certificate

增加受信任的CA證書

輸入CA的必要資訊，從本機電腦匯入憑證。

- 名稱：ftdvpn-ca-cert
- 特殊服務的驗證用法：SSL客戶端



Add Trusted CA Certificate

Name

ftdvpn-ca-cert

Certificate

Paste certificate, or choose a file (DER, PEM, CRT, CER)

ftd-ra-ca.crt

```
-----BEGIN CERTIFICATE-----
MIIDbDCCA1SgAwIBAgIIUkKgLg229/0wDQYJKoZIhvcNAQELBQAwbTELMAkGA1UE
BhMCS1AxDjAMBgNVBAgTBVRva31vMQ4wDAYDVQQHEwVUb2t5bzEOMAwGA1UEChMF
```

□ Skip CA Certificate Check

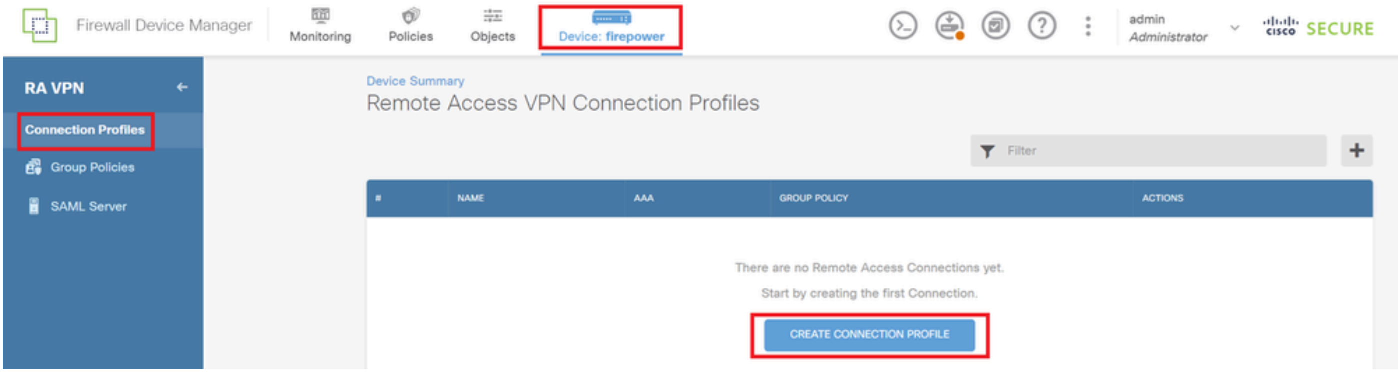
Validation Usage for Special Services

SSL Client ×

受信任CA憑證的詳細資料

步驟 9.增加遠端訪問VPN連線配置檔案

導航到裝置>遠端接入VPN >檢視配置>連線配置檔案，點選建立連線配置檔案按鈕。

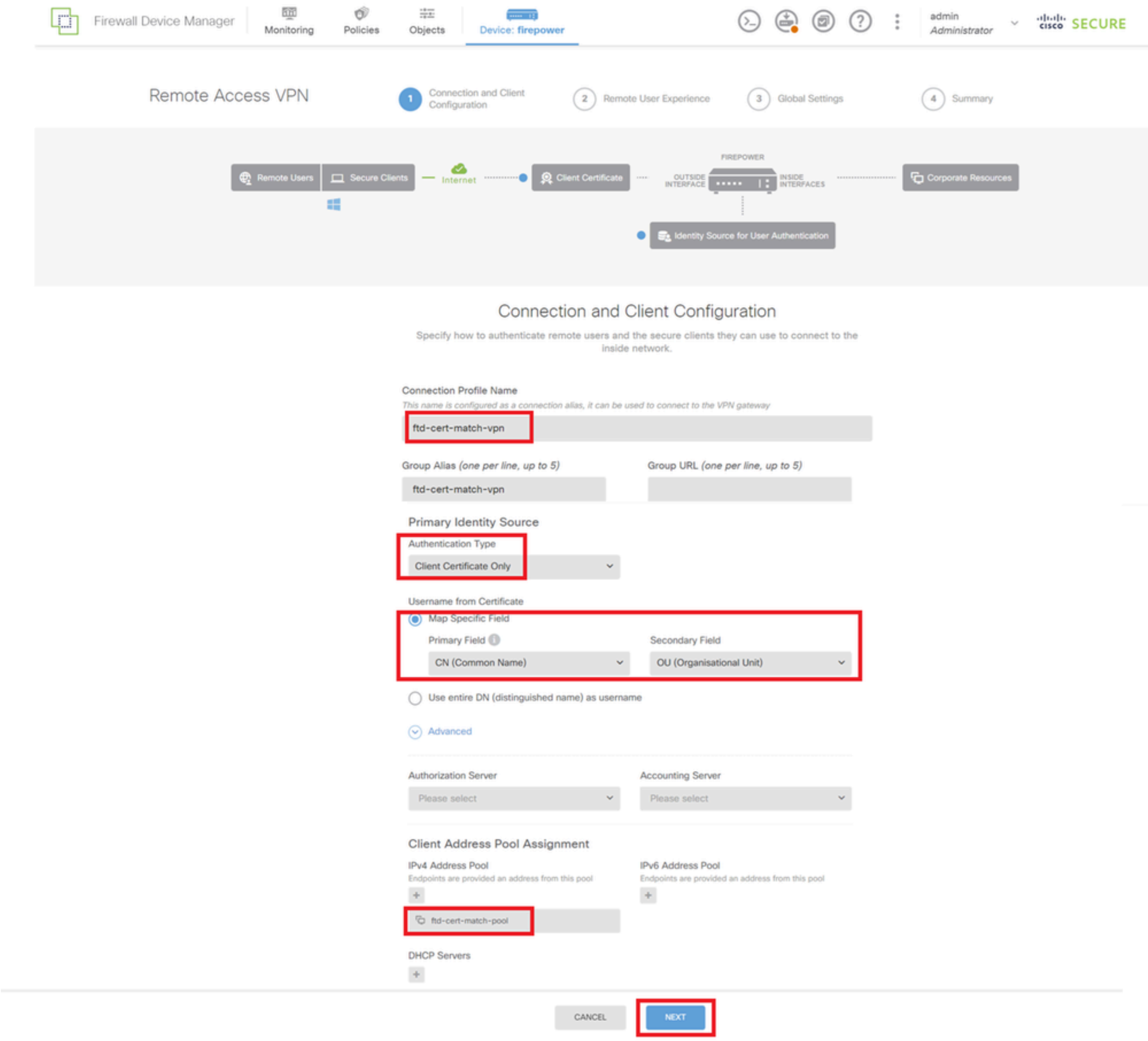


There are no Remote Access Connections yet.
Start by creating the first Connection.

增加遠端訪問VPN連線配置檔案

輸入連線配置檔案的必要資訊，然後按一下Next按鈕。

- 連線配置檔名稱：ftd-cert-match-vpn
- 驗證型別：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-cert-match-pool



Connection and Client Configuration

Specify how to authenticate remote users and the secure 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
ftd-cert-match-vpn

Group Alias *(one per line, up to 5)*: ftd-cert-match-vpn

Group URL *(one per line, up to 5)*

Primary Identity Source

Authentication Type: Client Certificate Only

Username from Certificate

● Map Specific Field

Primary Field: CN (Common Name)

Secondary Field: OU (Organisational Unit)

○ Use entire DN (distinguished name) as username

Advanced

Authorization Server: Please select

Accounting Server: Please select

Client Address Pool Assignment

IPv4 Address Pool
Endpoints are provided an address from this pool
ftd-cert-match-pool

IPv6 Address Pool
Endpoints are provided an address from this pool

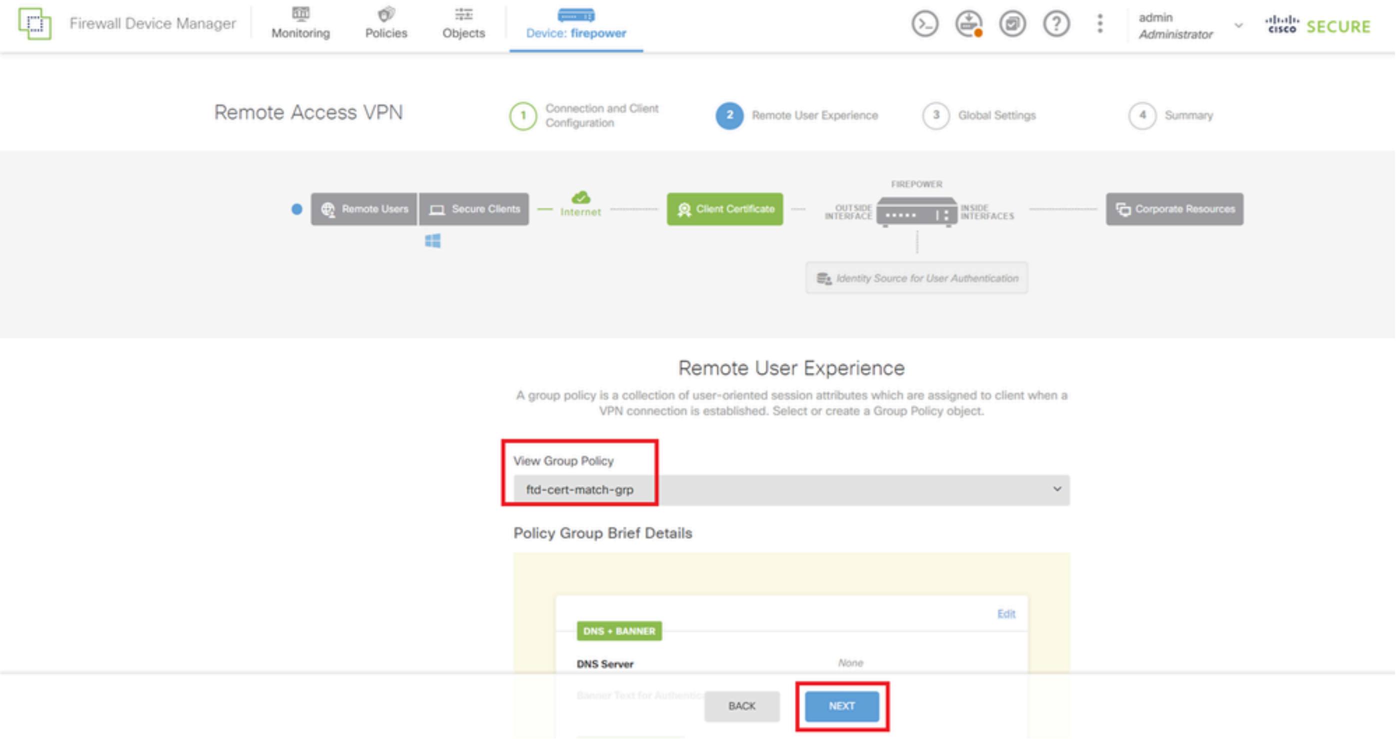
DHCP Servers

CANCEL NEXT

VPN連線配置檔案的詳細資訊

輸入組策略的必要資訊，並按一下Next按鈕。

- 檢視組策略：ftd-cert-match-grp



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: ftd-cert-match-grp

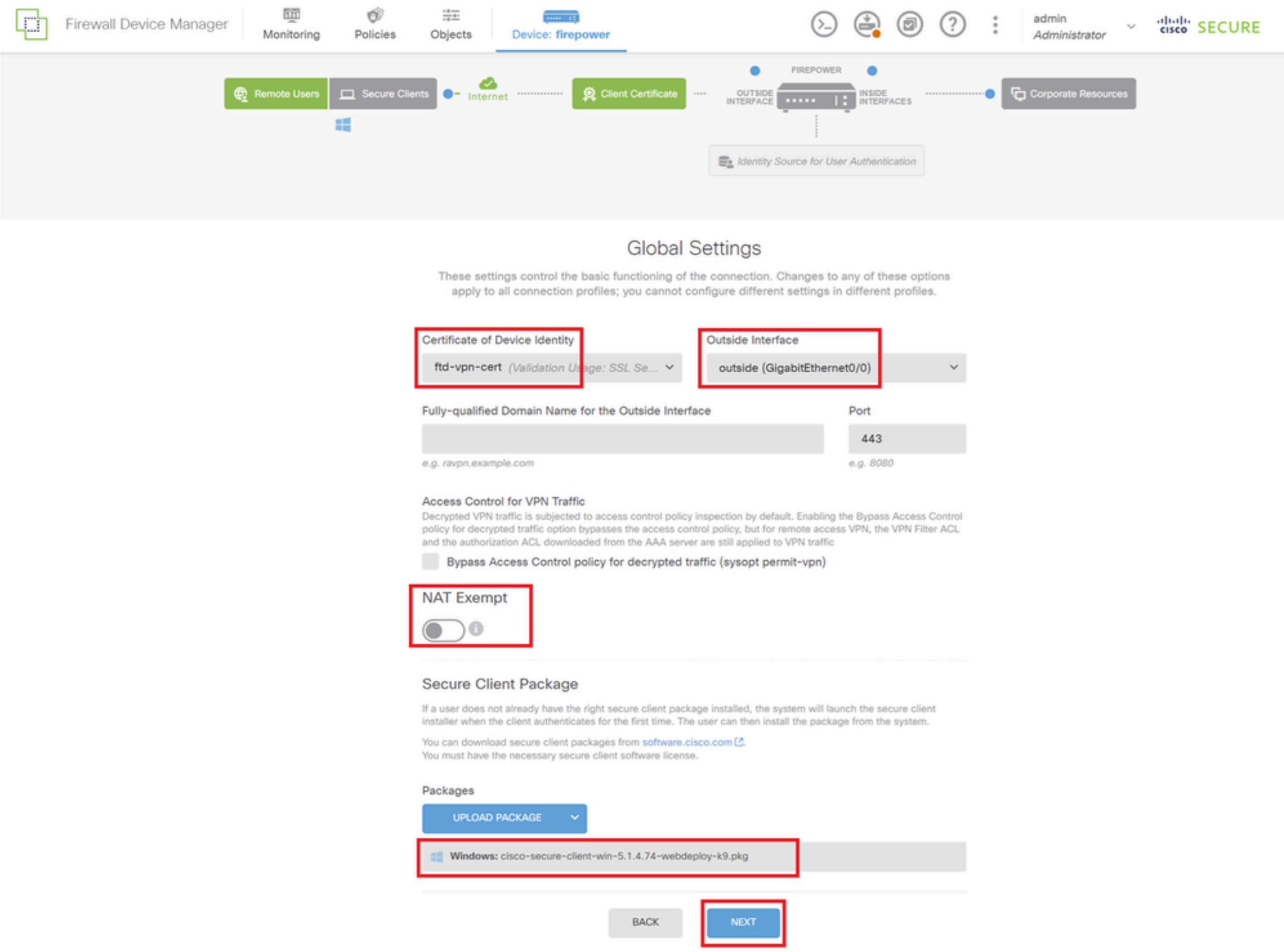
Policy Group Brief Details

選擇組策略

為VPN連線選擇Certificate of Device Identity、Outside Interface、Secure Client Package。

- 裝置身份證書：ftd-vpn-cert
- 外部介面：外部(GigabitEthernet0/0)
- 安全客戶端軟體套件：cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg

注意：本文檔中停用了NAT免除功能。



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: ftd-vpn-cert (Validation Usage: SSL Se...

Outside Interface: outside (GigabitEthernet0/0)

Fully-qualified Domain Name for the Outside Interface

e.g. ravpn.example.com

Port: 443

e.g. 8080

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 Exempt

Secure Client Package

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

You can download secure client packages from software.cisco.com.
You must have the necessary secure client software license.

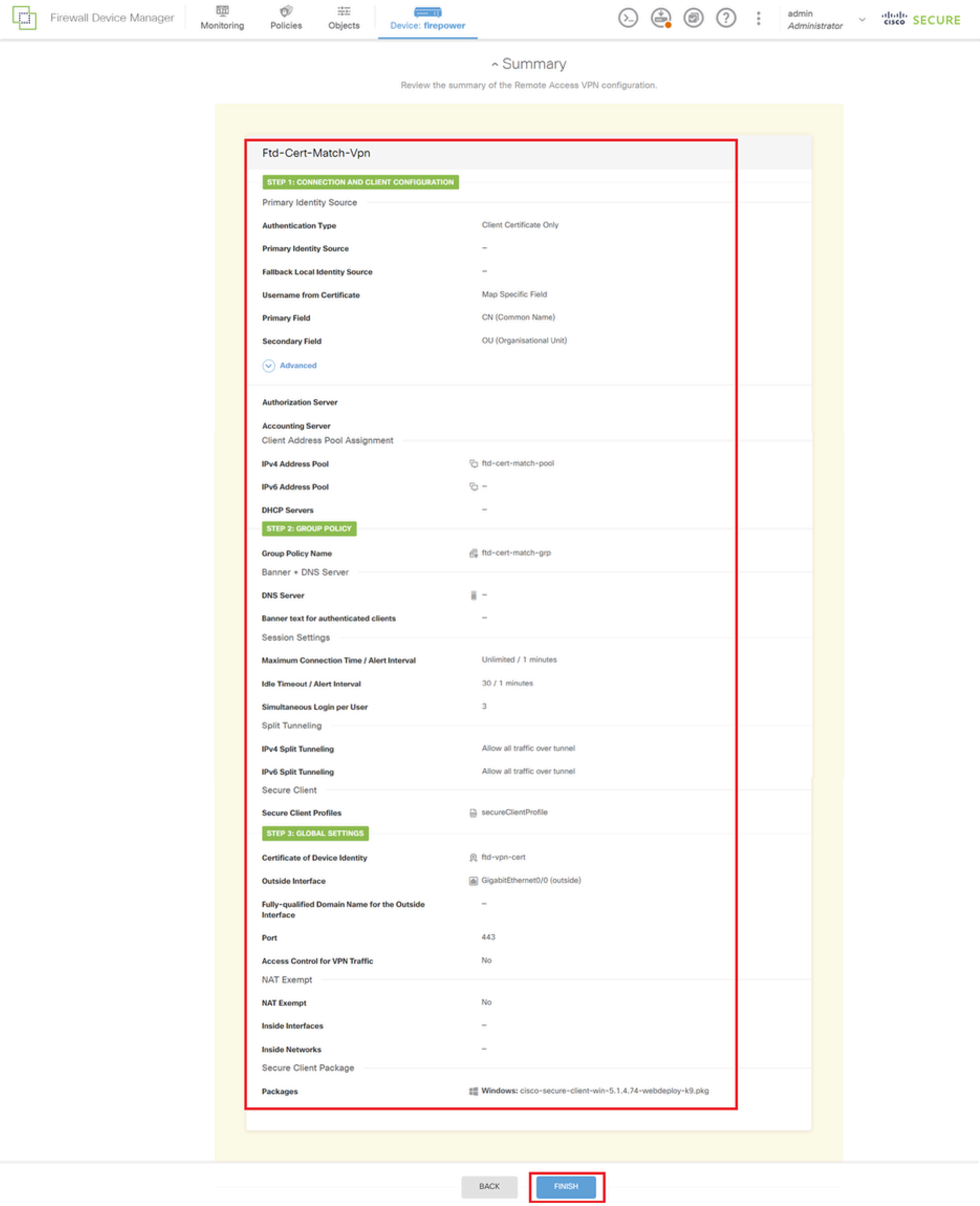
Packages

Windows: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg

全局設定的詳細資訊

步驟 10.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。



^ Summary

Review the summary of the Remote Access VPN configuration.

Ftd-Cert-Match-Vpn

STEP 1: CONNECTION AND CLIENT CONFIGURATION

Primary Identity Source

Authentication Type	Client Certificate Only
Primary Identity Source	–
Fallback Local Identity Source	–
Username from Certificate	Map Specific Field
Primary Field	CN (Common Name)
Secondary Field	OU (Organisational Unit)

Advanced

Authorization Server	
Accounting Server	

Client Address Pool Assignment

IPv4 Address Pool	ftd-cert-match-pool
IPv6 Address Pool	–
DHCP Servers	–

STEP 2: GROUP POLICY

Group Policy Name	ftd-cert-match-grp

Banner + DNS Server

DNS Server	–
Banner text for authenticated clients	–

Session Settings

Maximum Connection Time / Alert Interval	Unlimited / 1 minutes
Idle Timeout / Alert Interval	30 / 1 minutes
Simultaneous Login per User	3

Split Tunneling

IPv4 Split Tunneling	Allow all traffic over tunnel
IPv6 Split Tunneling	Allow all traffic over tunnel

Secure Client

Secure Client Profiles	secureClientProfile

STEP 3: GLOBAL SETTINGS

Certificate of Device Identity	ftd-vpn-cert
Outside Interface	GigabitEthernet0/0 (outside)
Fully-qualified Domain Name for the Outside Interface	–
Port	443
Access Control for VPN Traffic	No

NAT Exempt

NAT Exempt	No
Inside Interfaces	–
Inside Networks	–

Secure Client Package

Packages	Windows: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg

確認連線設定檔摘要

在FTD CLI中確認

從FDM部署後，在FTD CLI中確認VPN連線設定。

```
// Defines IP of interface
interface GigabitEthernet0/0
speed auto
nameif outside
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.1.200 255.255.255.0

// Defines a pool of addresses
ip local pool ftd-cert-match-pool 172.16.1.150-172.16.1.160

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

// Server Certificate
crypto ca certificate chain ftdvpn-ca-cert
certificate ca 5242a02e0db6f7fd
3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7
......
quit

// Defines Trustpoint for CA
crypto ca trustpoint ftdvpn-ca-cert
enrollment terminal
validation-usage ssl-client
crl configure

// CA
crypto ca certificate chain ftdvpn-ca-cert
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:/anyconnpkgs/cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg 2
anyconnect profiles secureClientProfile disk0:/anyconncprofs/secureClientProfile.xml
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable

// Configures the group-policy to allow SSL connections
```

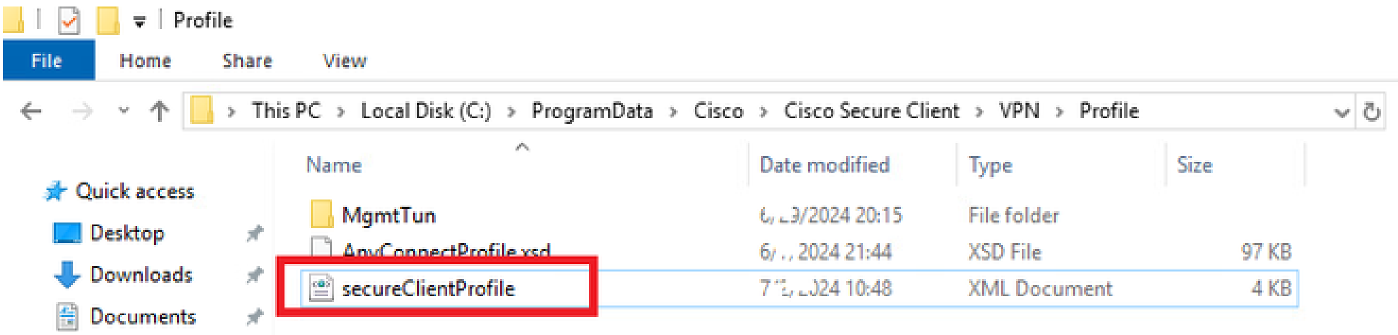
```
group-policy ftd-cert-match-grp internal
group-policy ftd-cert-match-grp attributes
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
msie-proxy method no-modify
vlan none
address-pools none
ipv6-address-pools none
webvpn
anyconnect ssl dtls none
anyconnect mtu 1406
anyconnect ssl keepalive none
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client none
anyconnect dpd-interval gateway none
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules none
anyconnect profiles value secureClientProfile type user
anyconnect ssl df-bit-ignore disable
always-on-vpn profile-setting

// Configures the tunnel-group to use the certificate authentication
tunnel-group ftd-cert-match-vpn type remote-access
tunnel-group ftd-cert-match-vpn general-attributes
address-pool ftd-cert-match-pool
default-group-policy ftd-cert-match-grp
tunnel-group ftd-cert-match-vpn webvpn-attributes
authentication certificate
group-alias ftd-cert-match-vpn enable
```

在VPN客戶端中確認

步驟 1.將安全客戶端配置檔案複製到VPN客戶端

將安全客戶端配置檔案複製到工程師VPN客戶端和管理員VPN客戶端。

注意：Windows電腦中Secure Client配置檔案的目錄：C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile



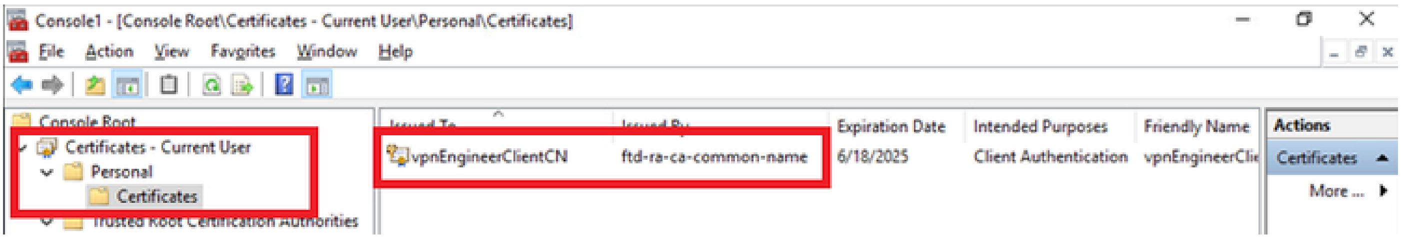
This PC > Local Disk (C:) > ProgramData > Cisco > Cisco Secure Client > VPN > Profile

Name	Date modified	Type	Size
MgmtTun	6/[illegible]3/2024 20:15	File folder	
AnyConnectProfile.xsd	6/[illegible]/2024 21:44	XSD File	97 KB
secureClientProfile	7/[illegible]/2024 10:48	XML Document	4 KB

將安全客戶端配置檔案複製到VPN客戶端

步驟 2.確認使用者端憑證

在工程VPN客戶端中，導航到證書-當前使用者>個人>證書，檢查用於身份驗證的客戶端證書。



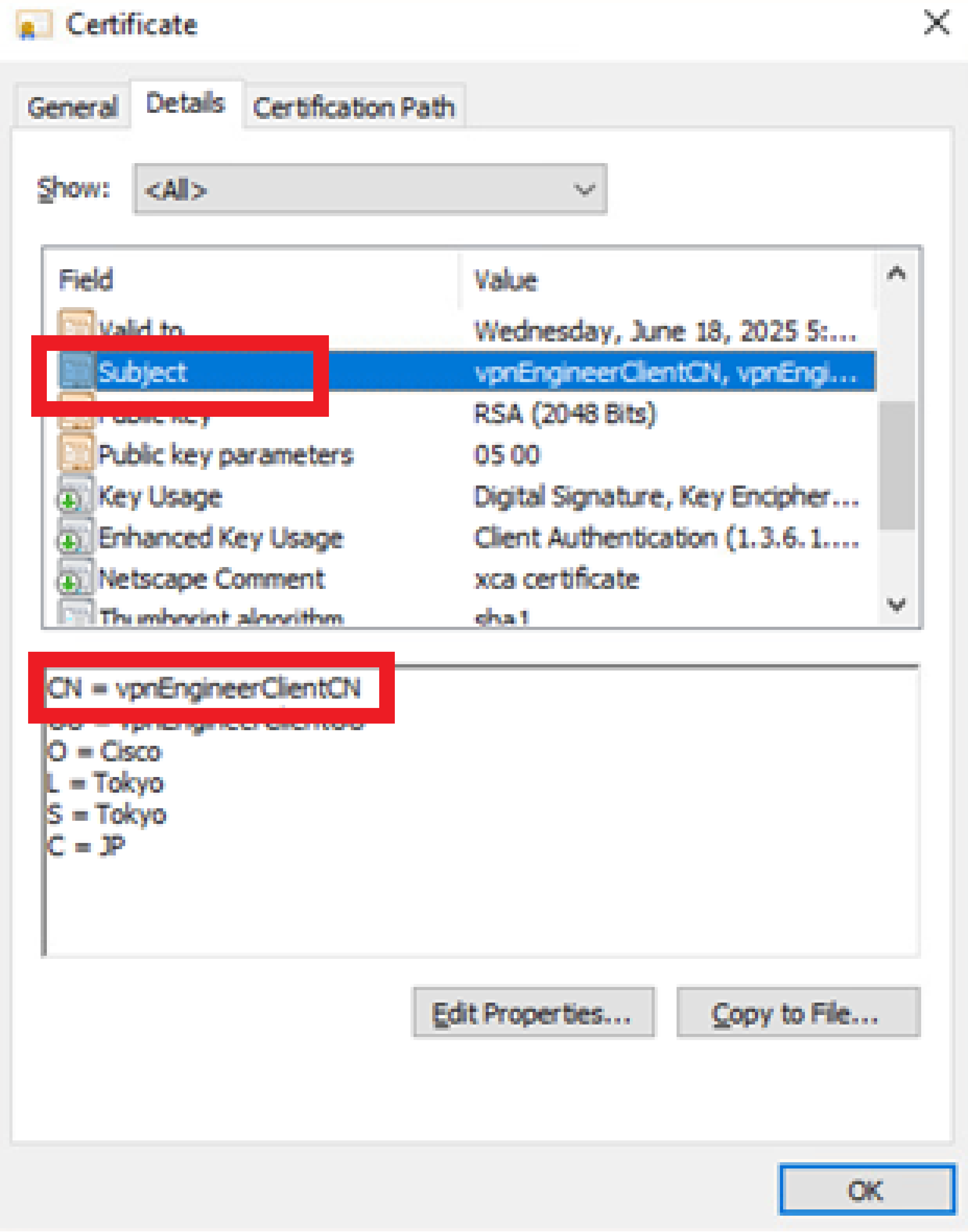
Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
vpnEngineerClientCN	ftd-ra-ca-common-name	6/18/2025	Client Authentication	vpnEngineerCli

確認工程師VPN客戶端的證書

按兩下客戶端證書，導航到Details，檢查Subject的詳細資訊。

- 主題：CN = vpnEngineerClientCN

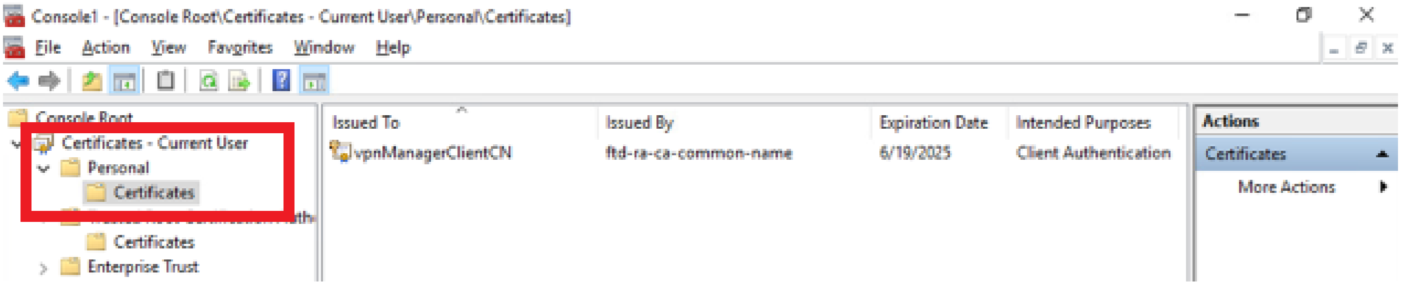


Field	Value
Valid to	Wednesday, June 18, 2025 5:...
Subject	vpnEngineerClientCN, vpnEngi...
Public key	RSA (2048 Bits)
Public key parameters	05 00
Key Usage	Digital Signature, Key Encipher...
Enhanced Key Usage	Client Authentication (1.3.6.1....
Netscape Comment	xca certificate
Thumbprint algorithm	sha1

```
CN = vpnEngineerClientCN
OU = vpnEngineerClientOU
O = Cisco
L = Tokyo
S = Tokyo
C = JP
```

工程師客戶端證書的詳細資訊

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

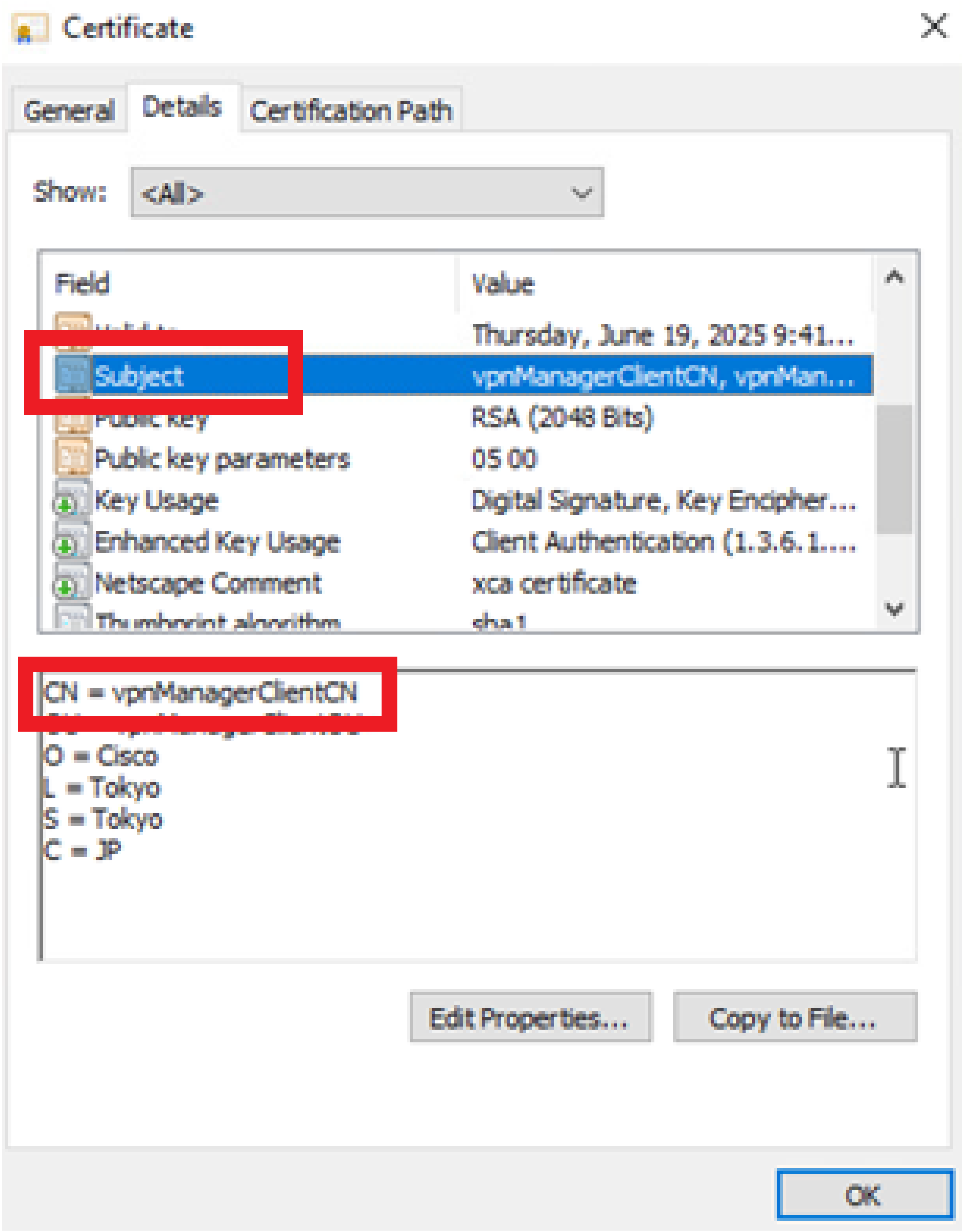


Issued To	Issued By	Expiration Date	Intended Purposes
vpnManagerClientCN	ftd-ra-ca-common-name	6/19/2025	Client Authentication

確認Manager VPN客戶端的證書

按兩下客戶端證書，導航到Details，檢查Subject的詳細資訊。

- 主題：CN = vpnManagerClientCN



Show: <All>

Field	Value
Validity	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

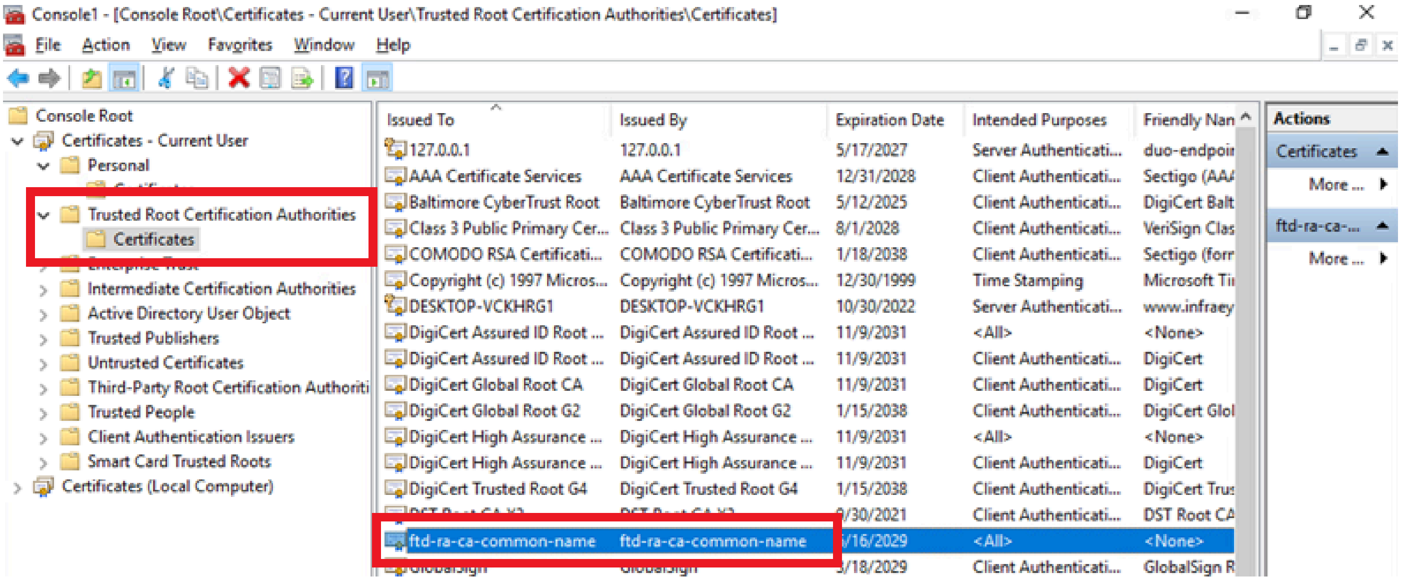
CN = vpnManagerClientCN
OU = vpnManagerClientOU
O = Cisco
L = Tokyo
S = Tokyo
C = JP

Manager客戶端證書的詳細資訊

步驟 3.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



Console1 - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certificates]

File Action View Favorites Window Help

- Console Root
  - Certificates - Current User
    - Personal
    - Trusted Root Certification Authorities
      - Certificates
    - Intermediate Certification Authorities
    - Active Directory User Object
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authoriti
    - Trusted People
    - Client Authentication Issuers
    - Smart Card Trusted Roots
  - Certificates (Local Computer)

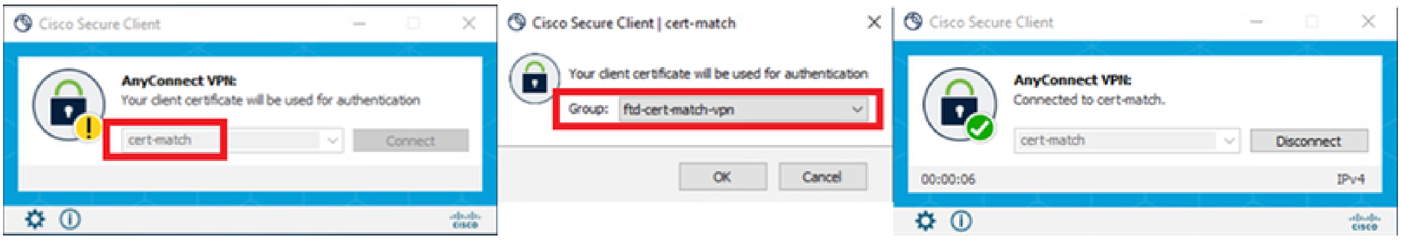
Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Nan
127.0.0.1	127.0.0.1	5/17/2027	Server Authenticati...	duo-endpoi
AAA Certificate Services	AAA Certificate Services	12/31/2028	Client Authenticati...	Sectigo (AA
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Client Authenticati...	DigiCert Balt
Class 3 Public Primary Cer...	Class 3 Public Primary Cer...	8/1/2028	Client Authenticati...	VeriSign Clas
COMODO RSA Certificati...	COMODO RSA Certificati...	1/18/2038	Client Authenticati...	Sectigo (forr
Copyright (c) 1997 Micros...	Copyright (c) 1997 Micros...	12/30/1999	Time Stamping	Microsoft Ti
DESKTOP-VCKHRG1	DESKTOP-VCKHRG1	10/30/2022	Server Authenticati...	www.infraey
DigiCert Assured ID Root ...	DigiCert Assured ID Root ...	11/9/2031	<All>	<None>
DigiCert Assured ID Root ...	DigiCert Assured ID Root ...	11/9/2031	Client Authenticati...	DigiCert
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Client Authenticati...	DigiCert
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authenticati...	DigiCert Glol
DigiCert High Assurance ...	DigiCert High Assurance ...	11/9/2031	<All>	<None>
DigiCert High Assurance ...	DigiCert High Assurance ...	11/9/2031	Client Authenticati...	DigiCert
DigiCert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038	Client Authenticati...	DigiCert Trus
DST Root CA X3	DST Root CA X3	9/30/2021	Client Authenticati...	DST Root CA
ftd-ra-ca-common-name	ftd-ra-ca-common-name	/16/2029	<All>	<None>
GlobalSign	GlobalSign	3/18/2029	Client Authenticati...	GlobalSign R

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。



Cisco Secure Client

AnyConnect VPN:
Your client certificate will be used for authentication

cert-match

Cisco Secure Client | cert-match

Your client certificate will be used for authentication

Group: ftd-cert-match-vpn

Cisco Secure Client

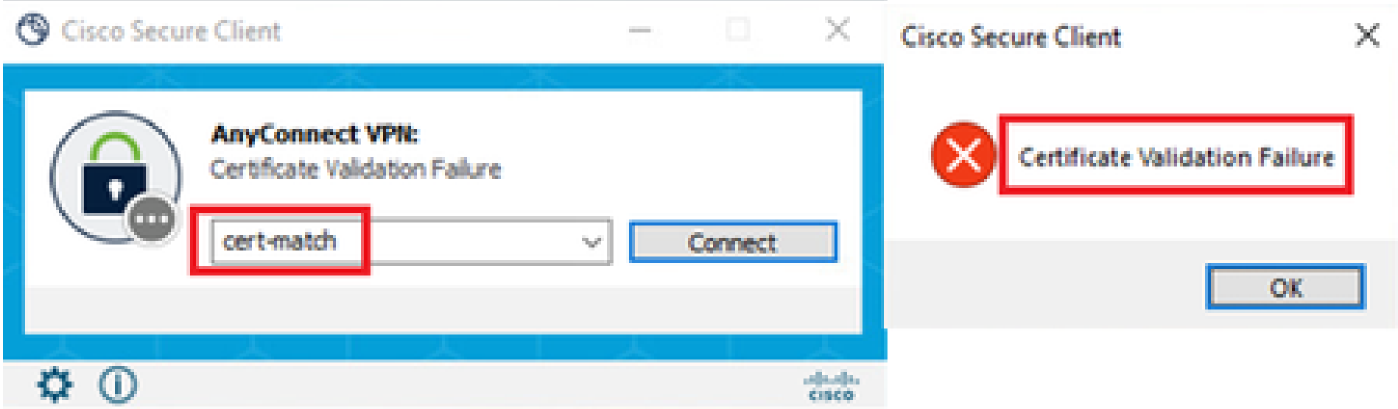
AnyConnect VPN:
Connected to cert-match.

cert-match

00:00:06 IPv4

工程師VPN客戶端的VPN連線成功

在管理器VPN客戶端中，啟動Cisco安全客戶端連線。由於證書驗證失敗，VPN連線失敗。



Cisco Secure Client

AnyConnect VPN:
Certificate Validation Failure

cert-match

Cisco Secure Client

Certificate Validation Failure

步驟 2.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，以確認工程師的VPN作業階段。

```
firepower# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : vpnEngineerClientCN Index : 32
Assigned IP : 172.16.1.150 Public IP : 192.168.1.11
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 : 14718 Bytes Rx : 12919
Pkts Tx : 2 Pkts Rx : 51
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftd-cert-match-grp Tunnel Group : ftd-cert-match-vpn
Login Time : 05:42:03 UTC Tue Jul 2 2024
Duration : 0h:00m:11s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 00000000000200006683932b
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:
Tunnel ID : 32.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 50170 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : win
Client OS Ver: 10.0.17763
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74
Bytes Tx : 7359 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 32.2
Assigned IP : 172.16.1.150 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 50177
TCP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74
```

```
Bytes Tx : 7359 Bytes Rx : 12919
Pkts Tx : 1 Pkts Rx : 51
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電腦上的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。

```
Jul 02 2024 04:16:03: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 7AF1C78ADCC8F941, subject name: CN=vpnE
Jul 02 2024 04:16:03: %FTD-6-717022: Certificate was successfully validated. serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClie
Jul 02 2024 04:16:04: %FTD-6-113009: AAA retrieved default group policy (ftd-cert-match-grp) for user = vpnEngineerClientCN
Jul 02 2024 04:16:09: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.11/50158 to 192.168.1.200/443 for TLSv1.2 sessi
```

相關資訊

設定Firepower 2100的FDM機上管理服務

在FDM管理的FTD上設定遠端存取VPN

在Firepower裝置管理器中配置和驗證系統日誌

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）。