

# Configurar la coincidencia de certificados para la autenticación de cliente seguro en FTD a través de FDM

## Contenido

---

### [Introducción](#)

### [Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

### [Antecedentes](#)

### [Diagrama de la red](#)

### [Configuraciones](#)

#### [Configuración en FDM](#)

[Paso 1. Configuración de la interfaz FTD](#)

[Paso 2. Confirmar licencia de cliente seguro de Cisco](#)

[Paso 3. Agregar conjunto de direcciones](#)

[Paso 4. Crear perfil de cliente seguro](#)

[Paso 5. Cargar perfil de cliente seguro en FDM](#)

[Paso 6. Agregar directiva de grupo](#)

[Paso 7. Agregar certificado FTD](#)

[Paso 8. Agregar CA al FTD](#)

[Paso 9. Agregar perfil de conexión VPN de acceso remoto](#)

[Paso 10. Confirmar resumen para perfil de conexión](#)

#### [Confirmar en CLI de FTD](#)

#### [Confirmar en cliente VPN](#)

[Paso 1. Copiar perfil de cliente seguro en cliente VPN](#)

[Paso 2. Confirmar certificado de cliente](#)

[Paso 3. Confirmar CA](#)

### [Verificación](#)

[Paso 1. Iniciar conexión VPN](#)

[Paso 2. Confirmar sesiones VPN en CLI de FTD](#)

### [Troubleshoot](#)

### [Información Relacionada](#)

---

## Introducción

Este documento describe cómo configurar Cisco Secure Client con SSL en FTD a través de FDM mediante la coincidencia de certificados para la autenticación.

## Prerequisites

## Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Firepower Device Manager (FDM) Virtual
- Firewall Threat Defence (FTD) Virtual
- Flujo de autenticación VPN

## Componentes Utilizados

- Cisco Firepower Device Manager Virtual 7.2.8
- Cisco Firewall Threat Defence Virtual 7.2.8
  
- Cisco Secure Client 5.1.4.74
- Editor de perfiles (Windows) 5.1.4.74

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

CertificateMatch es una función que permite a los administradores configurar criterios que el cliente debe utilizar para seleccionar un certificado de cliente para la autenticación con el servidor VPN. Esta configuración se especifica en el perfil de cliente, que es un archivo XML que se puede administrar mediante el Editor de perfiles o editarse manualmente. La función CertificateMatch se puede utilizar para mejorar la seguridad de las conexiones VPN asegurándose de que sólo se utilice un certificado con atributos específicos para la conexión VPN.

Este documento describe cómo autenticar Cisco Secure Client utilizando el nombre común de un certificado SSL.

Estos certificados contienen un nombre común que se utiliza para fines de autorización.

- CA: ftd-ra-ca-common-name
- Certificado de cliente VPN del ingeniero: vpnEngineerClientCN
- Certificado de cliente VPN del administrador: vpnManagerClientCN
- Certificado de servidor: 192.168.1.200

## Diagrama de la red

Esta imagen muestra la topología utilizada para el ejemplo de este documento.

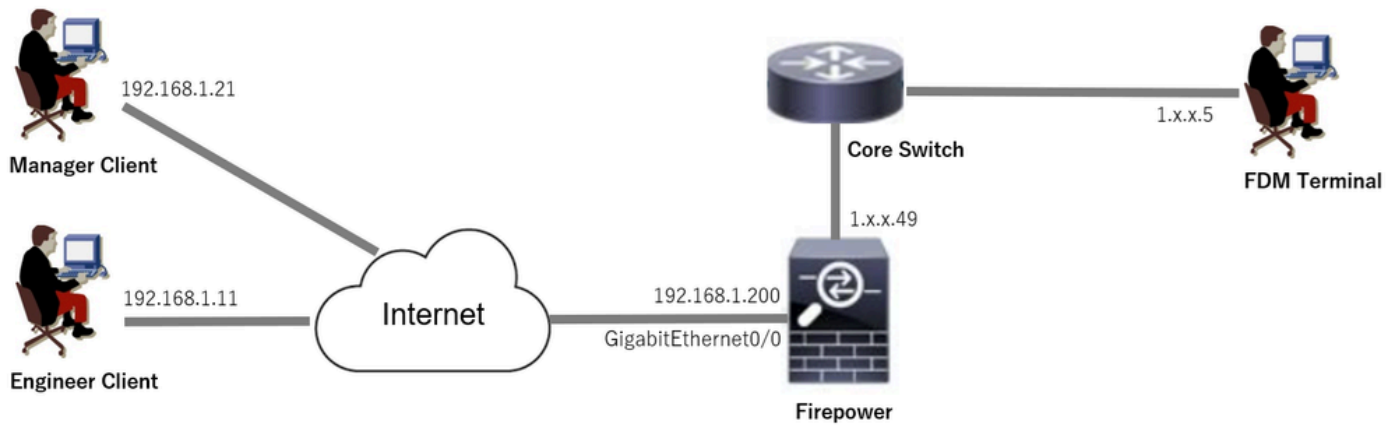


Diagrama de la red

## Configuraciones

### Configuración en FDM

#### Paso 1. Configuración de la interfaz FTD

Navegue hasta Device > Interfaces > View All Interfaces, configure la interfaz interna y externa para FTD en la pestaña Interfaces.

Para GigabitEthernet0/0,

- Nombre: fuera
- Dirección IP: 192.168.1.200/24

Device Summary  
Interfaces

Cisco Firepower Threat Defense for VMware

0/0 0/1 0/2 0/3 0/4 0/5 0/6 0/7

MGMT  
CONSOLE

Interfaces Virtual Tunnel Interfaces

9 Interfaces

NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
> ✓ GigabitEthernet0/0	outside	Enabled	Routed	192.168.1.200/24		Enabled	

Interfaz FTD

#### Paso 2. Confirmar licencia de cliente seguro de Cisco

Vaya a Device > Smart License > View Configuration, confirme la licencia de Cisco Secure Client en el elemento RA VPN License.

The screenshot shows the 'SUBSCRIPTION LICENSES INCLUDED' page in the Cisco Firepower Device Manager. The 'RA VPN License' is highlighted with a red box. It is currently 'Enabled' and has a 'Type' dropdown set to 'VPN ONLY'. Other licenses shown include Threat, Malware, and URL License, all of which are disabled by the user.

Licencia de cliente seguro

### Paso 3. Agregar conjunto de direcciones

Navigue hasta Objetos > Redes, haga clic en el botón +.

The screenshot shows the 'Network Objects and Groups' page in the Cisco Firepower Device Manager. The 'Objects' menu item is highlighted with a red box. The 'Networks' option in the left sidebar is also highlighted with a red box. A red box highlights the '+' button in the top right corner of the main content area.

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

Agregar conjunto de direcciones

Introduzca la información necesaria para agregar un nuevo conjunto de direcciones IPv4. haga clic en el botón Aceptar.

- Nombre: ftd-cert-match-pool
- Tipo: Rango
- Intervalo IP: 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*

CANCEL

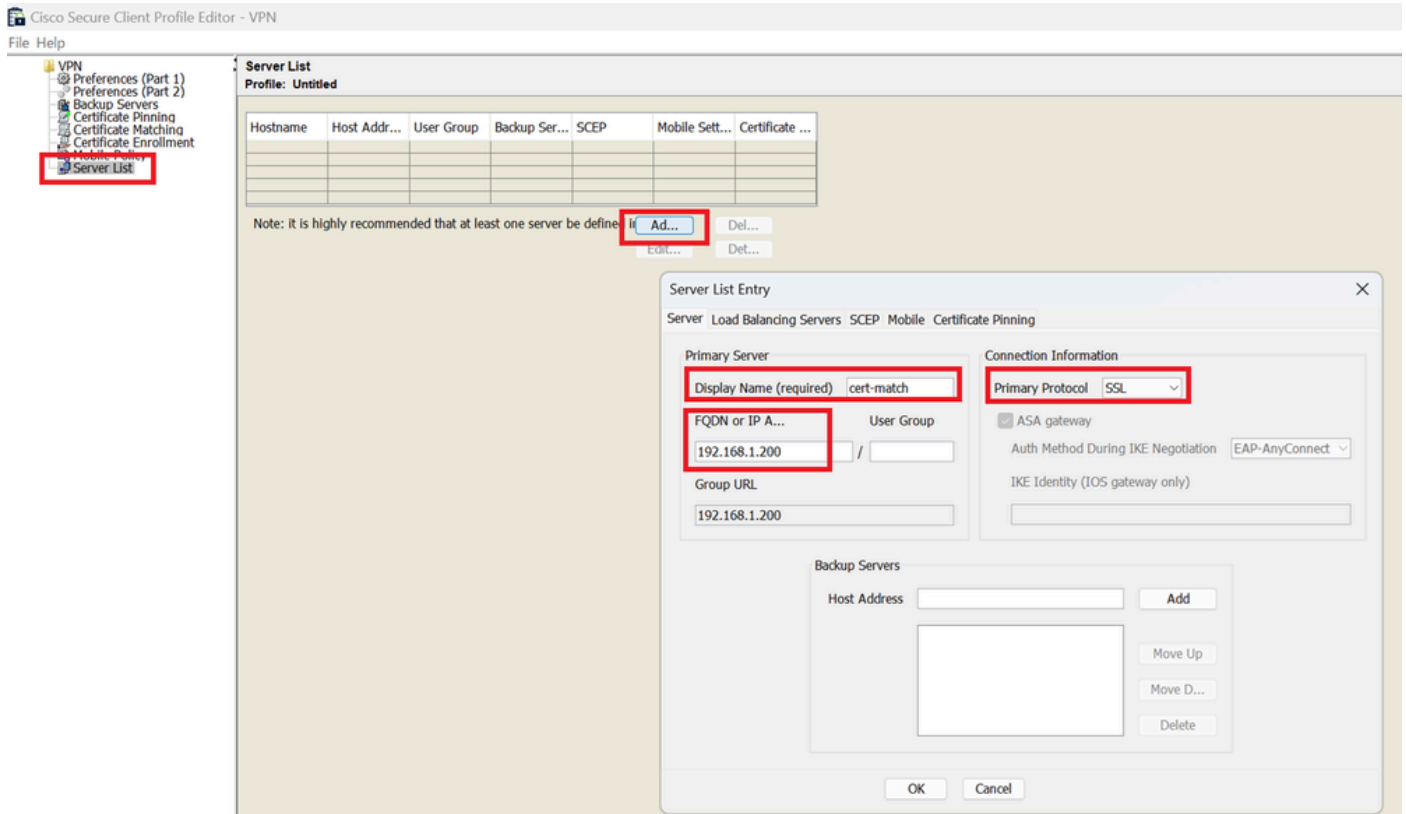
OK

Detalle del pool de direcciones IPv4

### Paso 4. Crear perfil de cliente seguro

Descargue e instale Secure Client Profile Editor desde el sitio [Cisco Software](#). Navegue hasta Lista de servidores, haga clic en el botón Agregar. Introduzca la información necesaria para agregar una entrada de lista de servidores y haga clic en el botón Aceptar.

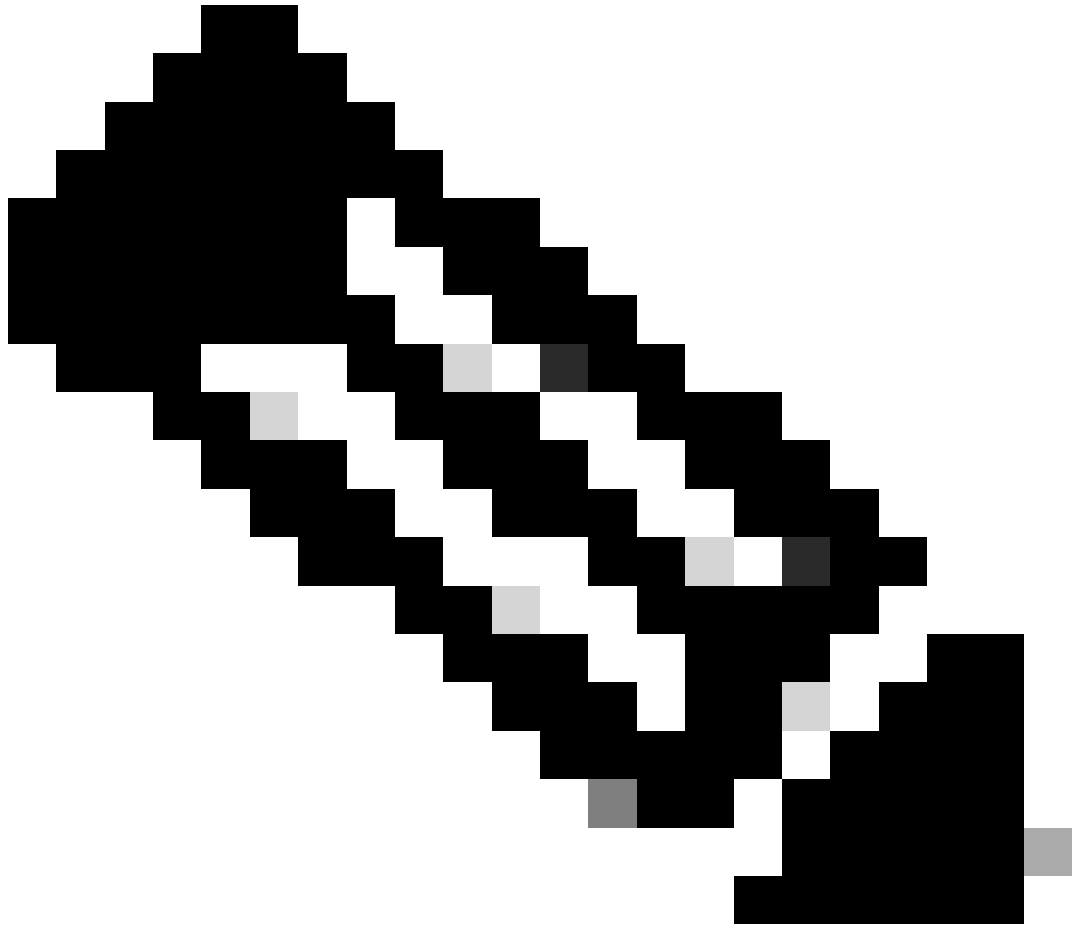
- Nombre para mostrar: cert-match
- FQDN o dirección IP: 192.168.1.200
- Protocolo principal: SSL



Entrada de lista de servidores

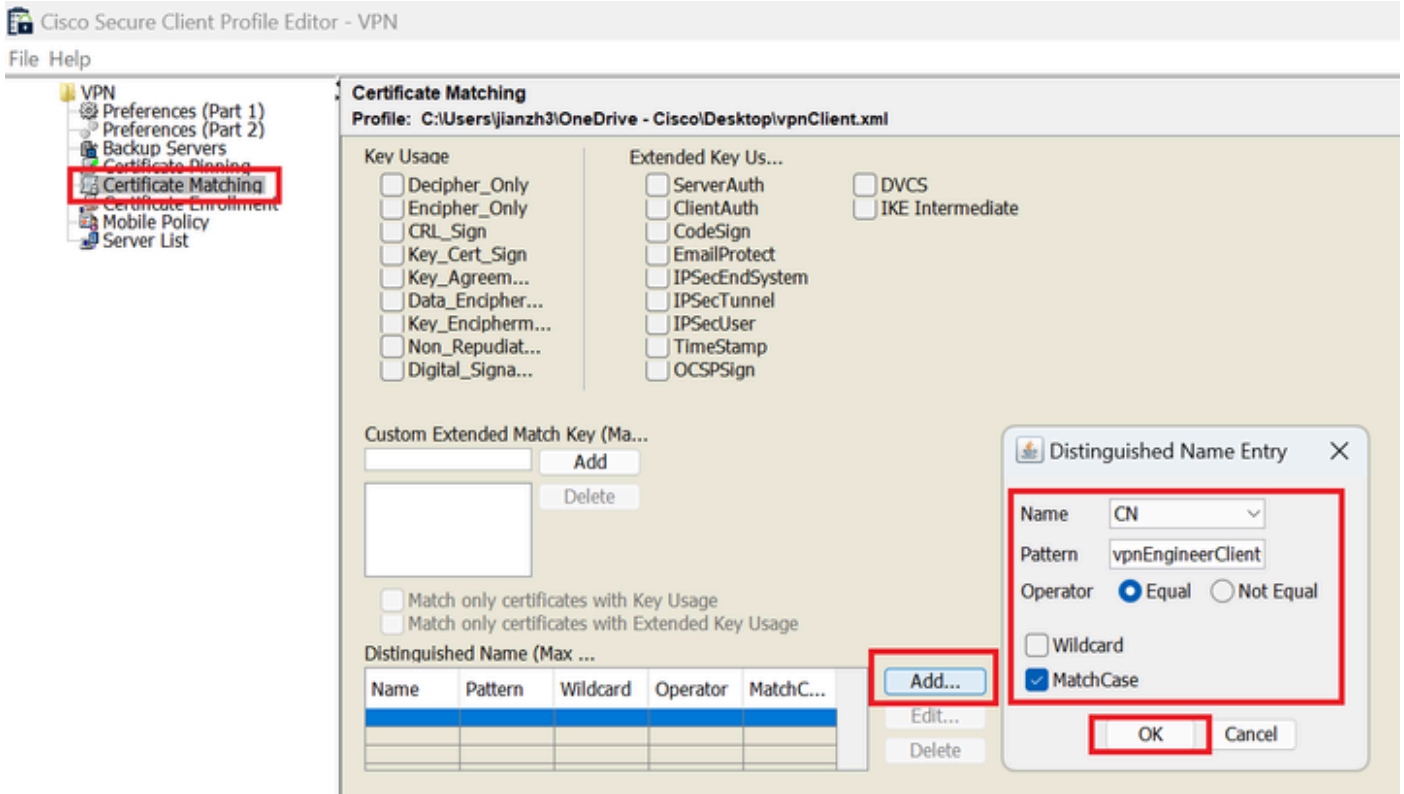
Navegue hasta Coincidencia de certificado, haga clic en el botón Agregar. Introduzca la información necesaria para agregar una entrada de nombre distinguido y haga clic en el botón Aceptar.

- Nombre: CN
- Patrón: vpnEngineerClientCN
- Operador: Equal



Nota: Marque la opción MatchCase en este documento.

---



Entrada de nombre distinguido

Guarde el perfil de cliente seguro en el equipo local y confirme los detalles del perfil.

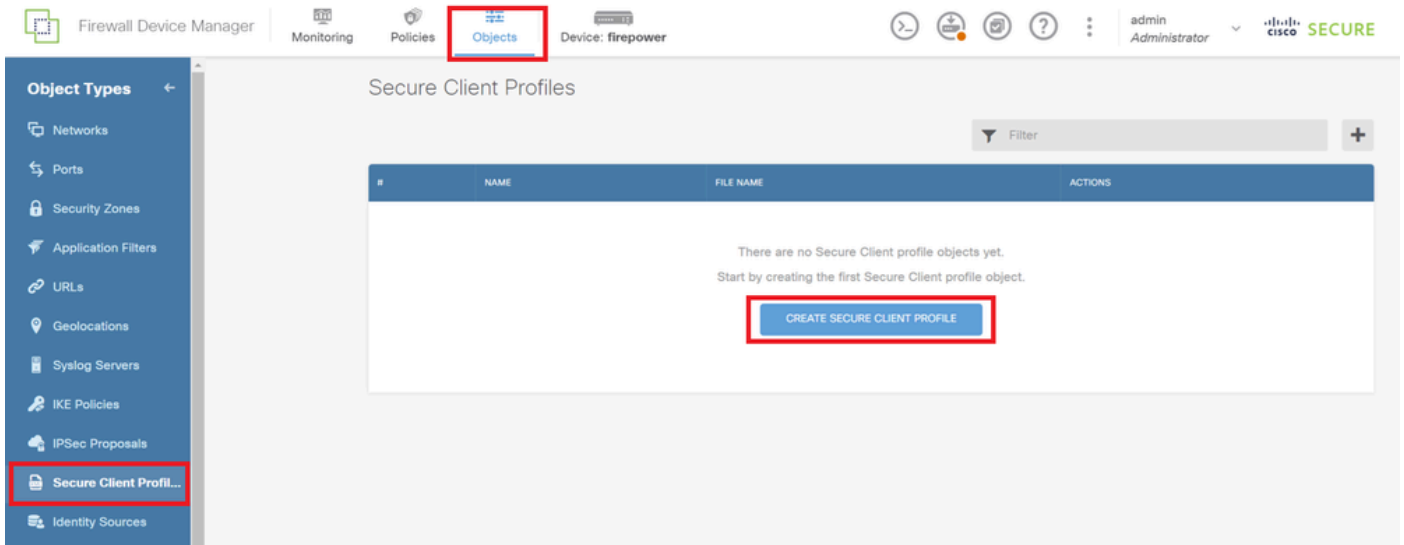


Perfil de cliente seguro

### Paso 5. Cargar perfil de cliente seguro en FDM

Navegue hasta Objetos > Perfil de cliente seguro, haga clic en el botón CREAR PERFIL DE CLIENTE SEGURO.

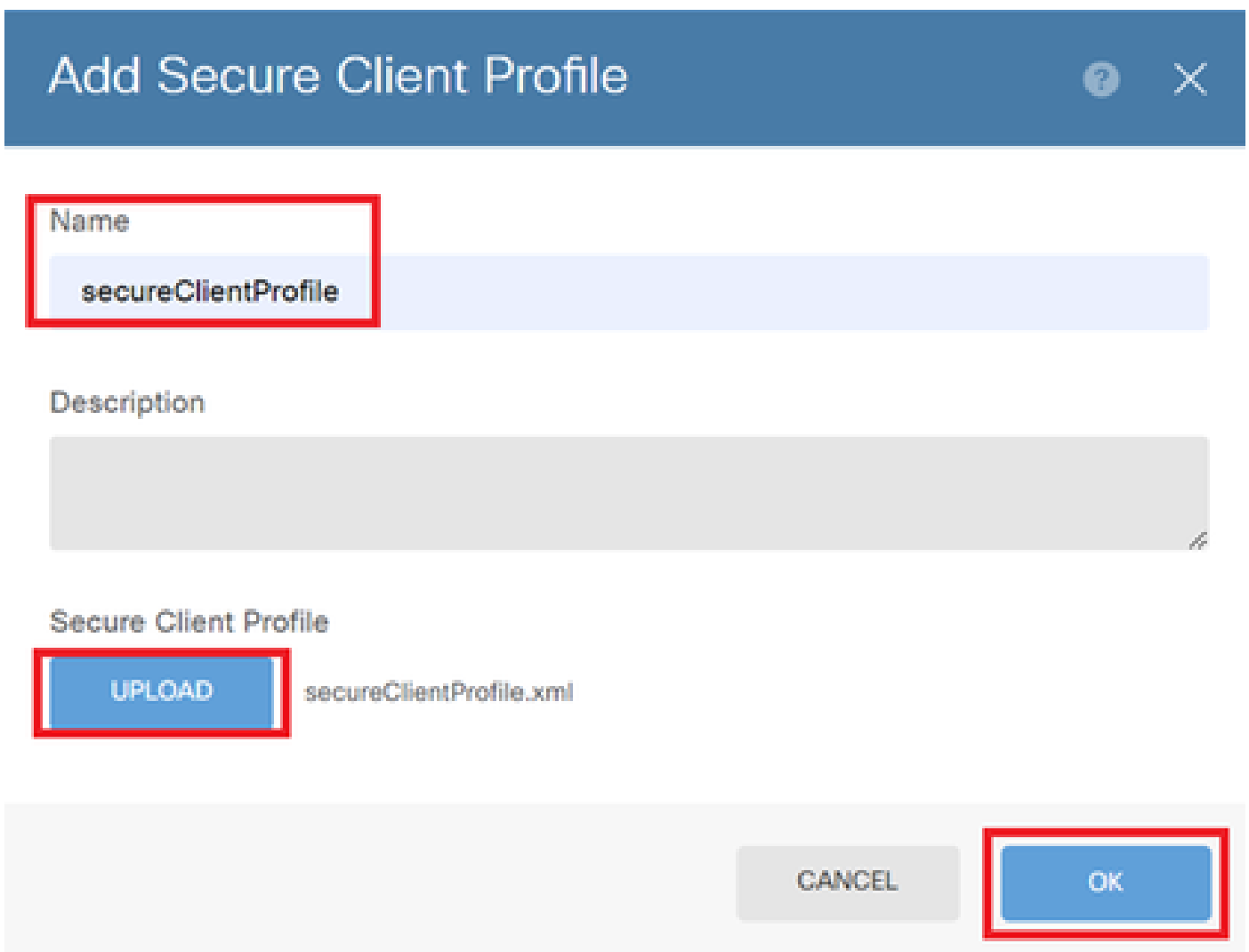




Crear perfil de cliente seguro

Introduzca la información necesaria para agregar un perfil de cliente seguro y haga clic en el botón Aceptar.

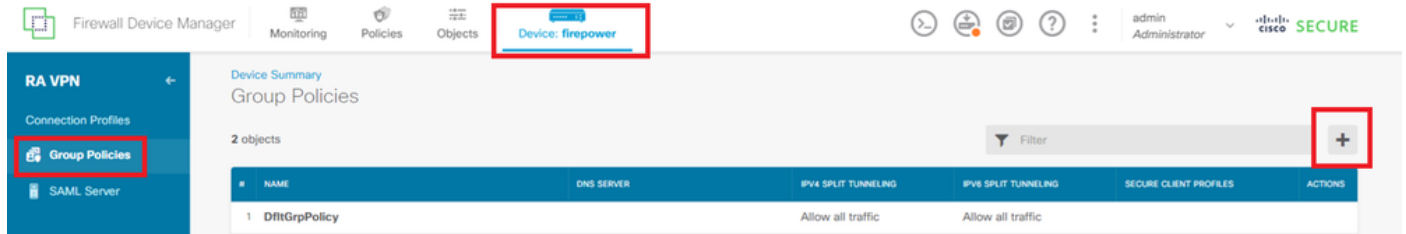
- Nombre: secureClientProfile
- Perfil de cliente seguro: secureClientProfile.xml (carga desde el equipo local)



Agregar perfil de cliente seguro

## Paso 6. Agregar directiva de grupo

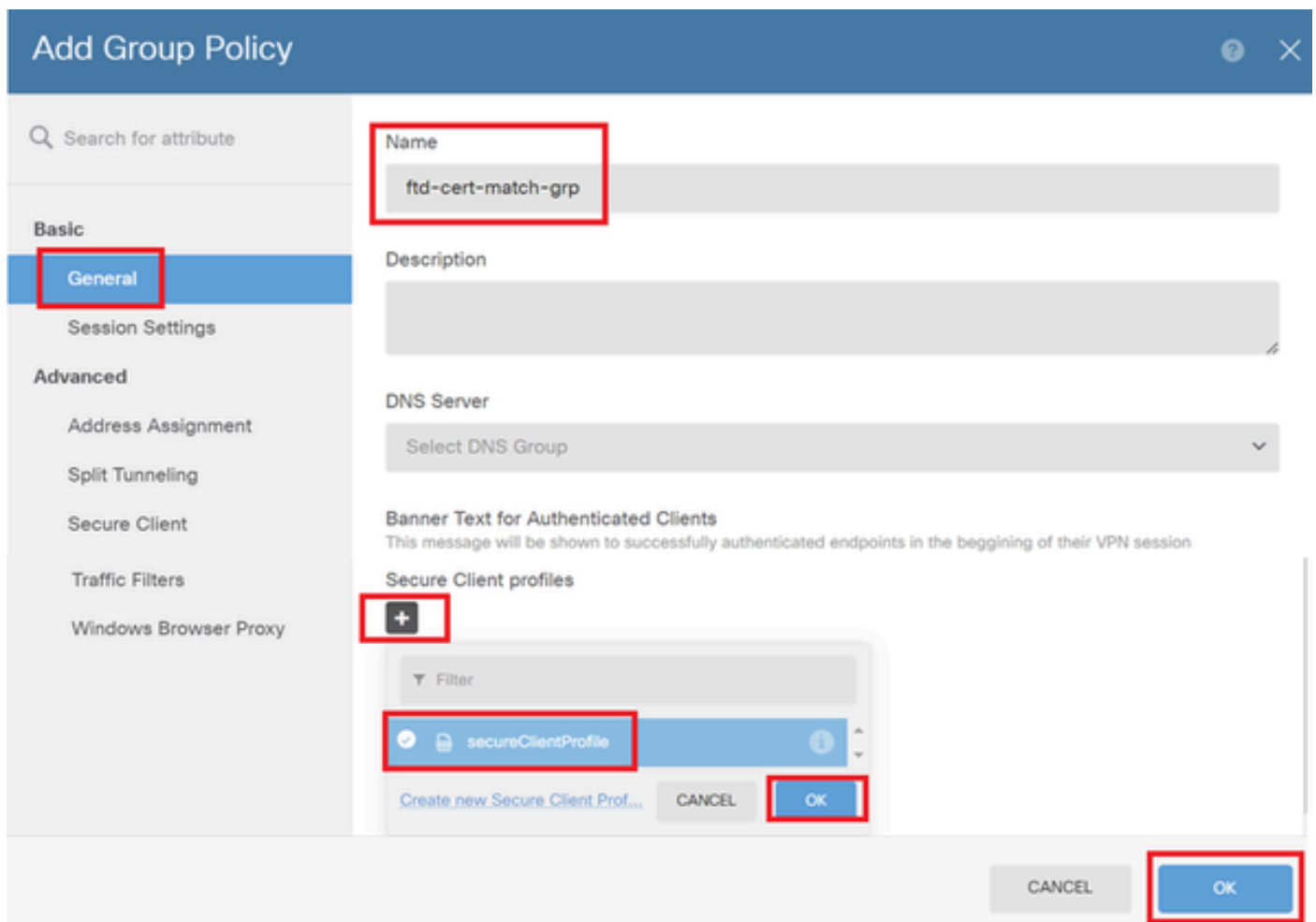
Vaya a Device > Remote Access VPN > View Configuration > Group Policies, haga clic en el botón +.



Agregar directiva de grupo

Introduzca la información necesaria para agregar una directiva de grupo y haga clic en el botón Aceptar.

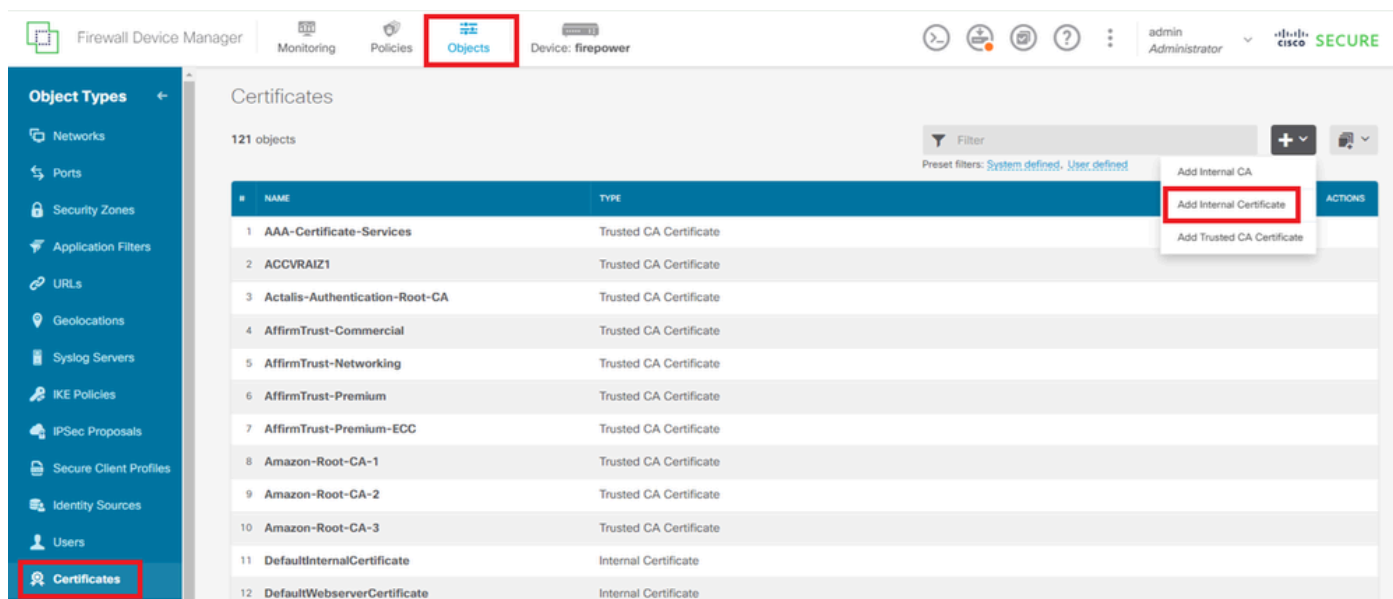
- Nombre: ftd-cert-match-grp
- Perfiles de Secure Client: secureClientProfile



Detalles de la directiva de grupo

## Paso 7. Agregar certificado FTD

Navegue hasta Objetos > Certificados, haga clic en Agregar certificado interno desde el elemento +.



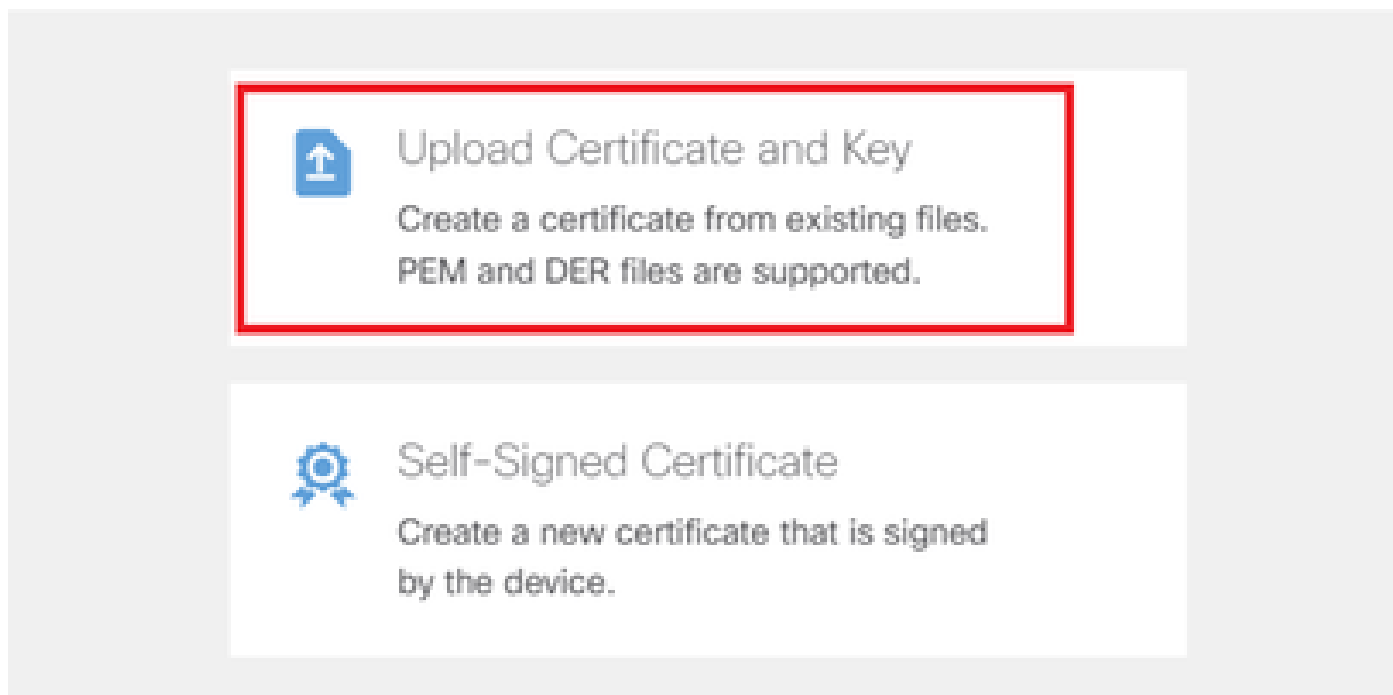
The screenshot shows the Cisco Firepower Firewall Device Manager interface. The 'Objects' menu item is highlighted in red. A dropdown menu is open over the 'Add Internal Certificate' option, which is also highlighted in red. The table below shows a list of certificates:

#	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	

Agregar certificado interno

Haga clic en Cargar certificado y clave.

Choose the type of internal certificate you want to create



The dialog box shows two options for creating an internal certificate:

- 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.

Cargar certificado y clave

Introduzca la información necesaria para el certificado FTD, importe un certificado y una clave de certificado desde el equipo local y, a continuación, haga clic en el botón Aceptar.

- Nombre: ftd-vpn-cert
- Uso de validación para servicios especiales: servidor SSL

## Add Internal Certificate

Name

ftd-vpn-cert

Certificate

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

Upload Certificate

```
-----BEGIN CERTIFICATE-----
MIIDfDCCAmSgAwIBAgIIIkE99YS2cmwDQYJKoZIhvcNAQELBQAwTELMAkGA1UE
BhMCS1AxOjQjAMBgNVBAgTBVRva31vMQ4wDAYDVQQHEwVUB2t5bzEOMAwGA1UE
ChMF
O31-V38-w04AMP-d8D4-TD18k-z78k-MQ4-UAYV8Q9CE-ufA-dC9t-zwE-V3E-V30-kLD...
```

Certificate Key

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

Upload Certificate Key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAxdn5eTUngo5+GUG2Ng2FjI/+xHRkR-f6o2OccGdzLYK1tzwB
98WPu1YP0T/qwCf-fkXuMQ9DEVGMIjLRX9nvXdBNoakUbZVzc03qM3AjE87p0h0t0
-42b188PT-zh41-1-1-w03-zwE-V3E9-1u4140-73E-Tk4G-w17k-w373A-0-wE-c
```

Validation Usage for Special Services

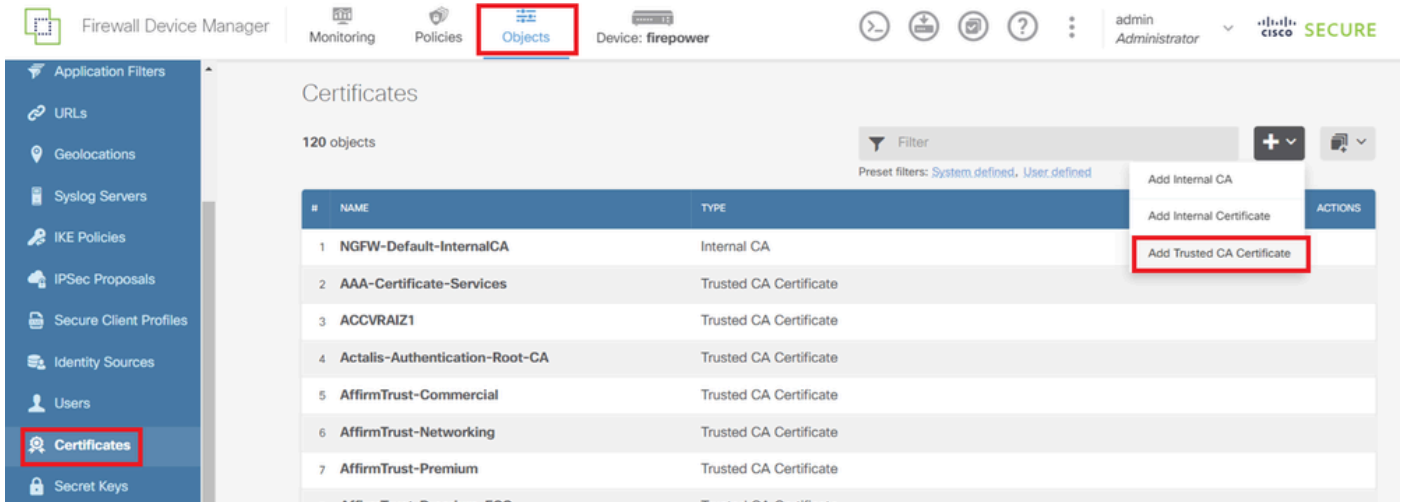
SSL Server

CANCEL OK

Detalles del certificado interno

### Paso 8. Agregar CA al FTD

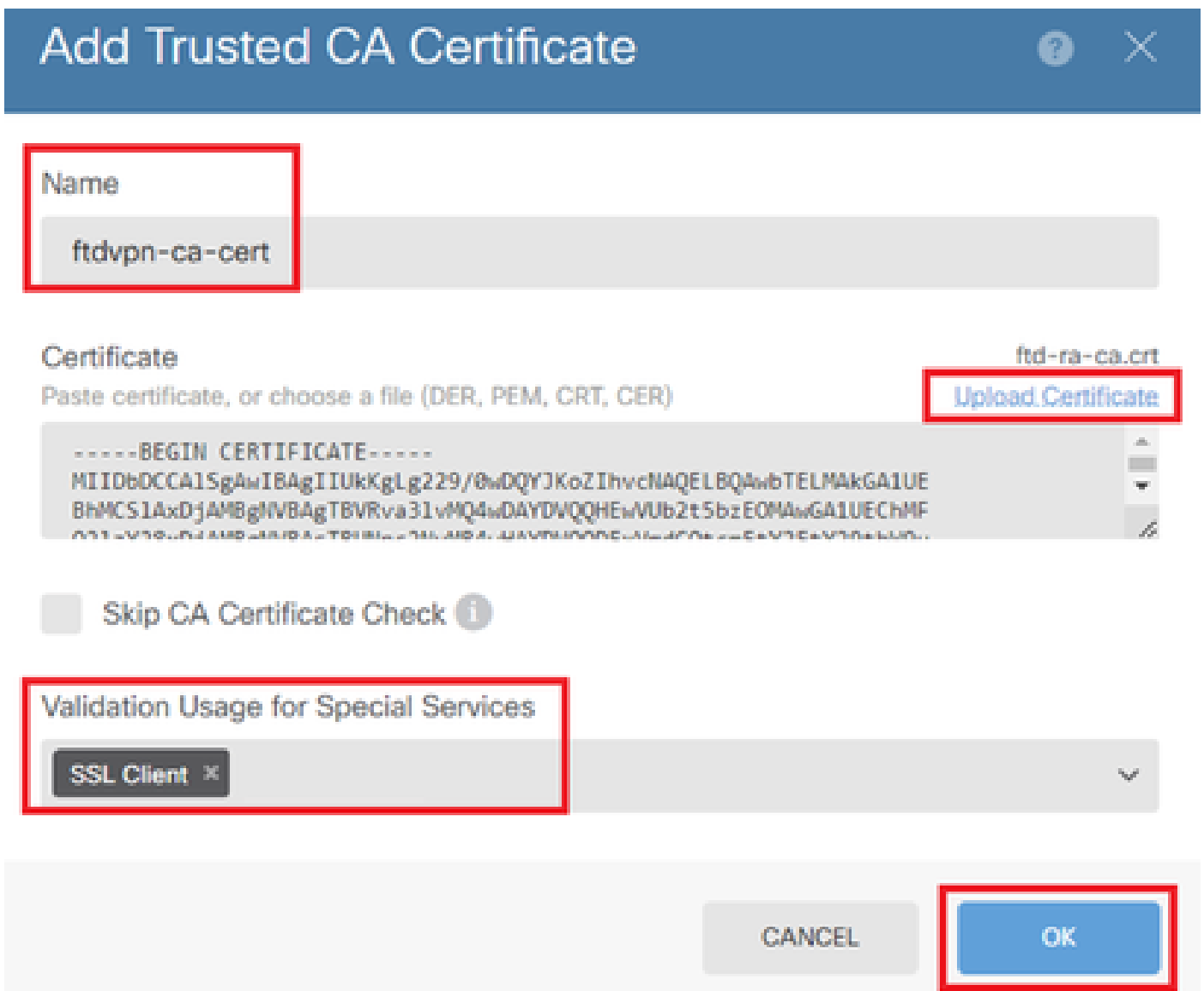
Navegue hasta Objetos > Certificados, haga clic en Agregar certificado de CA de confianza desde el elemento +.



Agregar certificado de CA de confianza

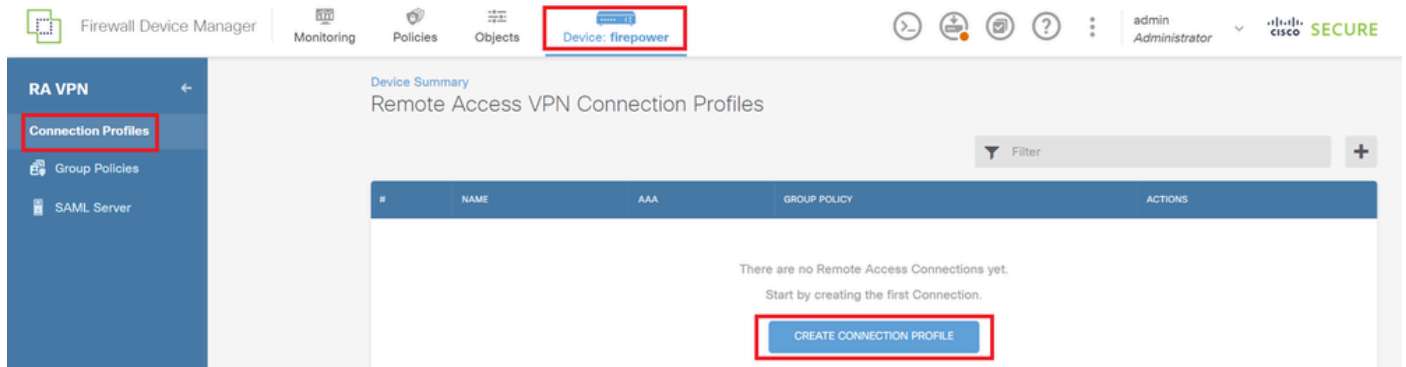
Introduzca la información necesaria para la CA e importe un certificado desde el equipo local.

- Nombre: ftdvpn-ca-cert
- Uso de validación para servicios especiales: cliente SSL



## Paso 9. Agregar perfil de conexión VPN de acceso remoto

Vaya a Device > Remote Access VPN > View Configuration > Connection Profiles, haga clic en el botón CREATE CONNECTION PROFILE.



Agregar perfil de conexión VPN de acceso remoto

Introduzca la información necesaria para el perfil de conexión y haga clic en el botón Next.

- Nombre del perfil de conexión: ftd-cert-match-vpn
- Tipo de autenticación: sólo certificado de cliente
- Nombre de usuario del certificado: campo específico de asignación
- Campo principal: CN (nombre común)
- Campo secundario: OU (unidad organizativa)
- Conjuntos de direcciones IPv4: ftd-cert-match-pool

Remote Access VPN | 1 Connection and Client Configuration | 2 Remote User Experience | 3 Global Settings | 4 Summary



### 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

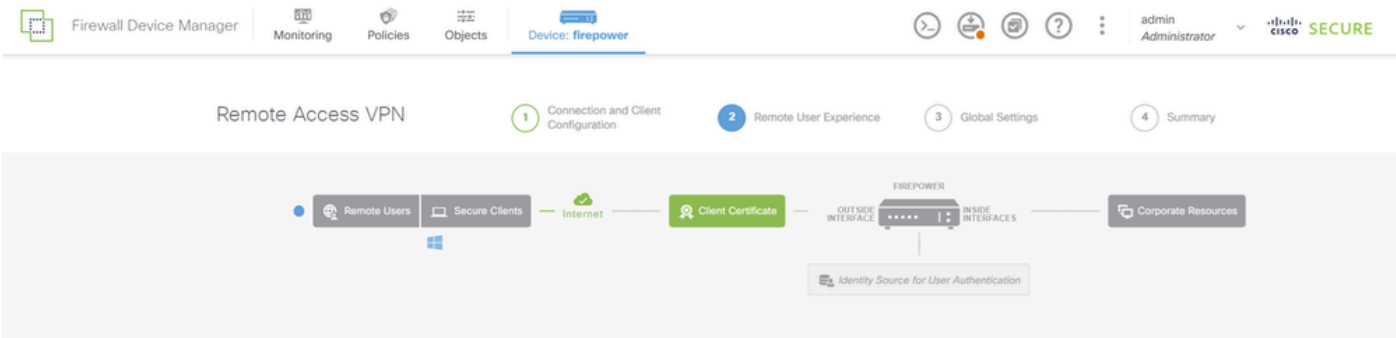
+

CANCEL | NEXT

Detalles del perfil de conexión VPN

Introduzca la información necesaria para la política de grupo y haga clic en el botón Next.

- Ver directiva de grupo: 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

DNS + BANNER [Edit](#)

DNS Server None

Banner Text for Authentication

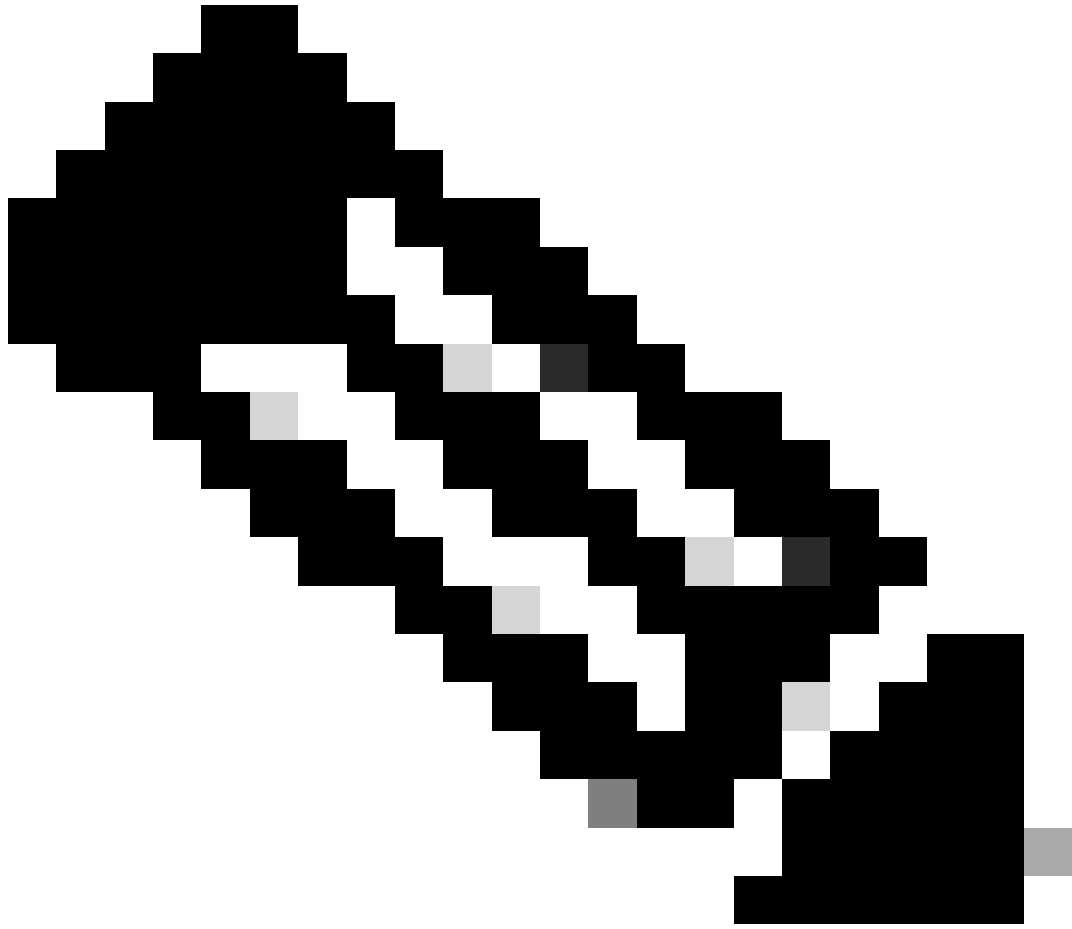
[BACK](#) [NEXT](#)

Seleccionar directiva de grupo

Selecione Certificate of Device Identity, Outside Interface, Secure Client Package para la conexión VPN.

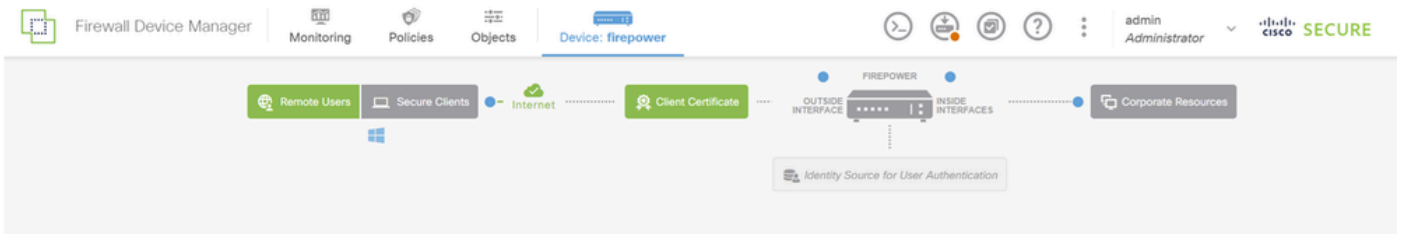
- Certificado de identidad del dispositivo: ftd-vpn-cert
- Interfaz externa: externa (GigabitEthernet0/0)
- Paquete Secure Client: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg





Nota: la función NAT Exempt inhabilitada en este documento.

---



## 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.

<b>Certificate of Device Identity</b> ftd-vpn-cert (Validation Usage: SSL Se...)	<b>Outside Interface</b> outside (GigabitEthernet0/0)
Fully-qualified Domain Name for the Outside Interface e.g. ravn.example.com	Port 443 e.g. 8080
<b>Access Control for VPN Traffic</b> 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. <input type="checkbox"/> Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)	
<b>NAT Exempt</b> <input type="checkbox"/>	
<b>Secure Client Package</b> 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 <a href="https://software.cisco.com">software.cisco.com</a> . You must have the necessary secure client software license.	
<b>Packages</b> UPLOAD PACKAGE Windows: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg	
BACK NEXT	

Detalles de la configuración global

## Paso 10. Confirmar resumen para perfil de conexión

Confirme la información introducida para la conexión VPN y haga clic en el botón FINISH.

^ 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

BACK FINISH

Confirmar resumen para perfil de conexión

### Confirmar en CLI de FTD

Confirme la configuración de la conexión VPN en la CLI de FTD después de la implementación desde FDM.

```
// 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
cr1 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
cr1 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:/anyconnprofs/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
```

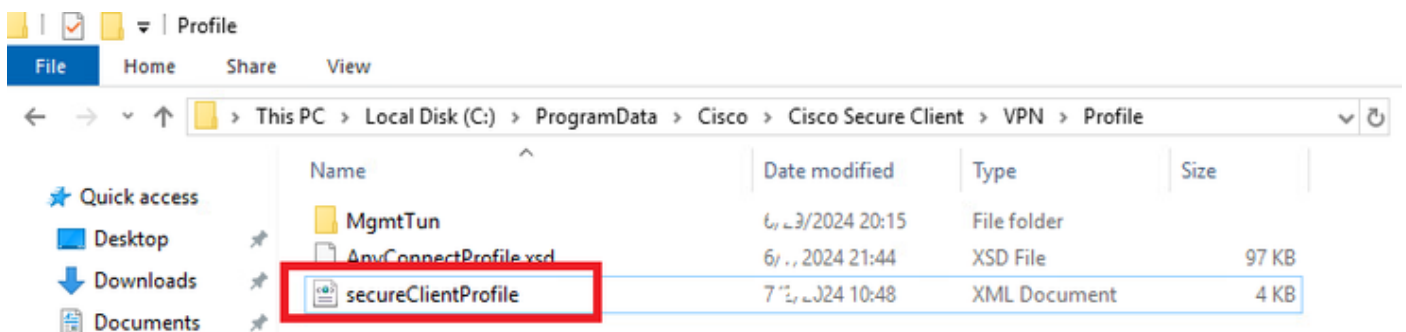
```
// Configures the tunnel-group to use the certificate authentication
tunnel-group ftd-cert-match-vpn type remote-access
tunnel-group ftd-cert-match-vpn general-attributes
address-pool ftd-cert-match-pool
default-group-policy ftd-cert-match-grp
tunnel-group ftd-cert-match-vpn webvpn-attributes
authentication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

## Confirmar en cliente VPN

### Paso 1. Copiar perfil de cliente seguro en cliente VPN

Copie el perfil de cliente seguro para diseñar el cliente VPN y el cliente VPN administrador.

Nota: El directorio del perfil de cliente seguro en el equipo con Windows:  
C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile



Copiar perfil de cliente seguro en cliente VPN

## Paso 2. Confirmar certificado de cliente

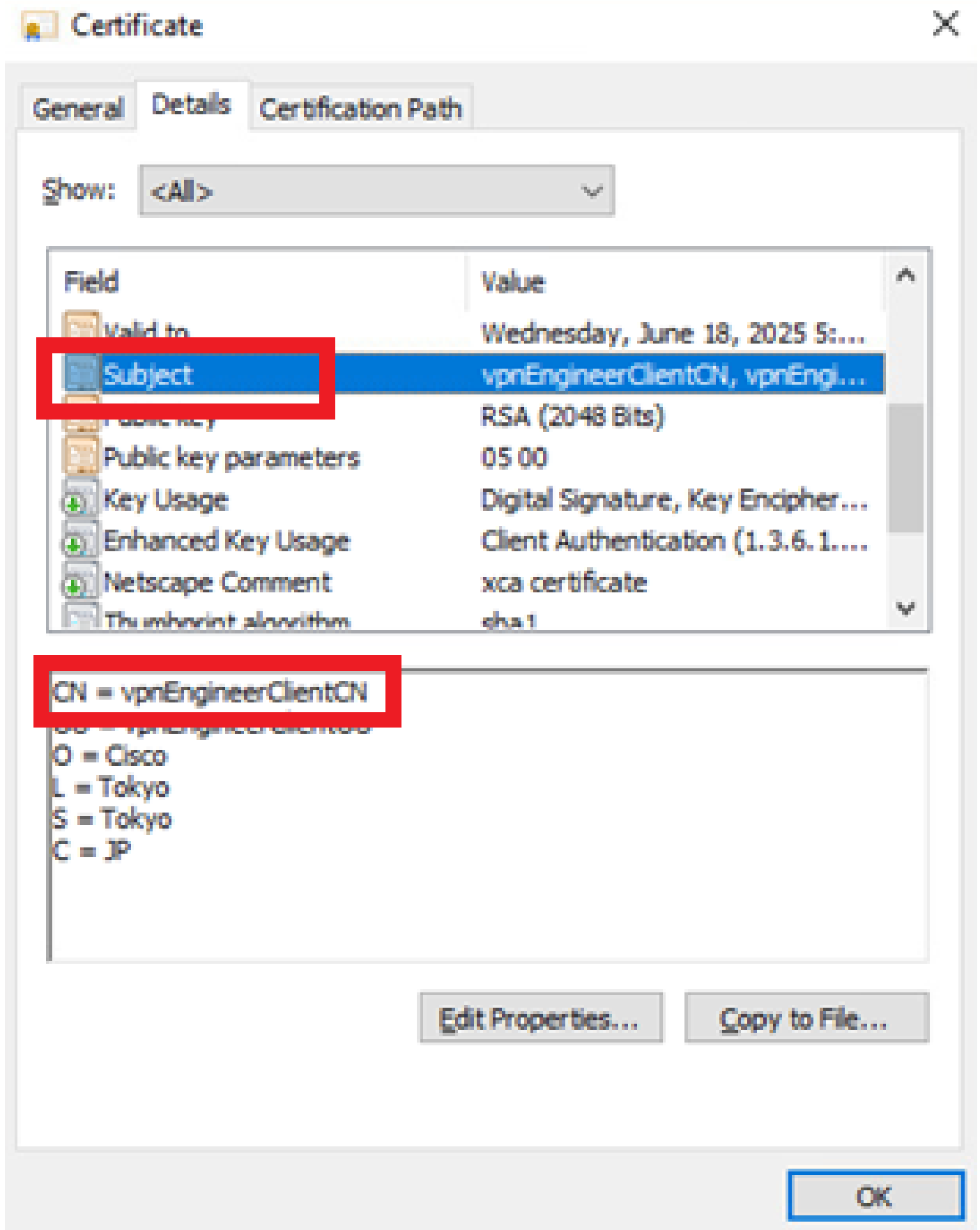
En Engineer VPN Client, navegue hasta Certificates - Current User > Personal > Certificates, verifique el certificado de cliente utilizado para la autenticación.



Confirmar certificado para cliente de VPN de ingeniero

Haga doble clic en el certificado de cliente, navegue hasta Detalles, verifique los detalles de Asunto.

- Asunto: CN = vpnEngineerClientCN



Detalles del certificado de cliente de ingeniero

En manager VPN client, navegue hasta Certificates - Current User > Personal > Certificates, verifique el certificado de cliente utilizado para la autenticación.





Confirmar certificado para Manager VPN Client

Haga doble clic en el certificado de cliente, navegue hasta Detalles, verifique los detalles de Asunto.

- Asunto: 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...

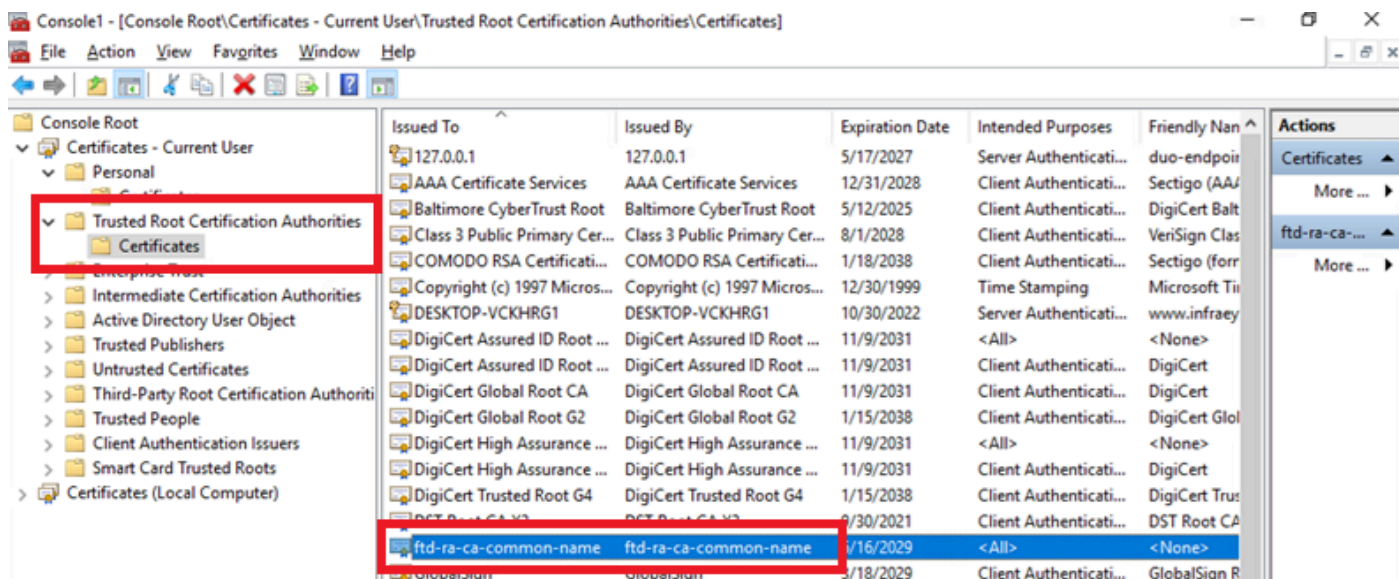
OK

Detalles del certificado de cliente del administrador

Paso 3. Confirmar CA

En el cliente VPN del ingeniero y en el cliente VPN del administrador, navegue hasta Certificados - Usuario actual > Autoridades de certificación raíz de confianza > Certificados, verifique la CA utilizada para la autenticación.

- Emitido por: ftd-ra-ca-common-name

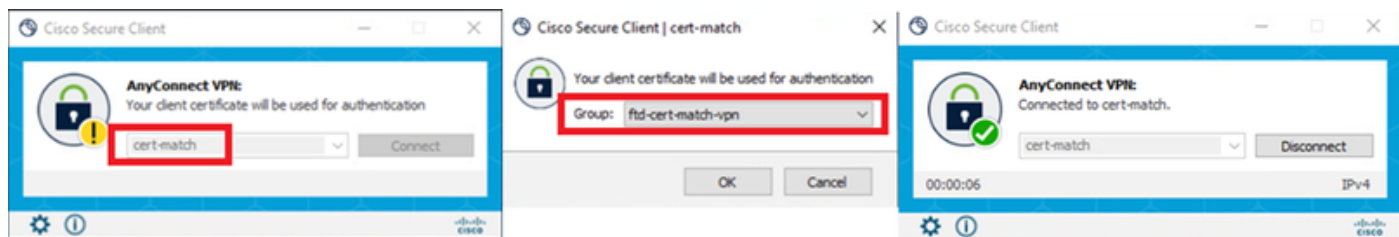


Confirmar CA

## Verificación

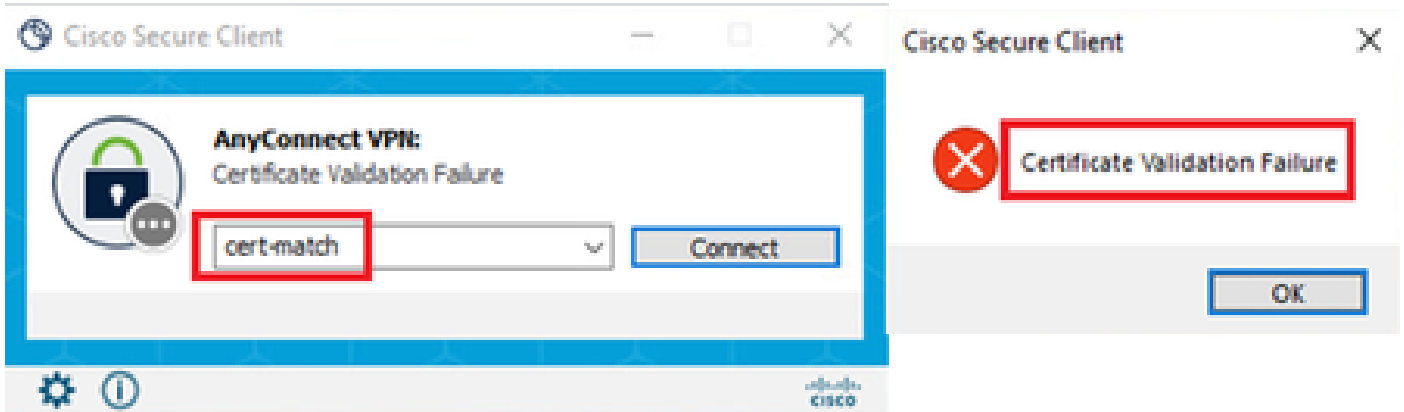
### Paso 1. Iniciar conexión VPN

En el cliente de ingeniería VPN, inicie la conexión de Cisco Secure Client. No es necesario introducir el nombre de usuario y la contraseña, ya que la VPN se ha conectado correctamente.



Conexión VPN correcta para Engineer VPN Client

En el cliente VPN del administrador, inicie la conexión de Cisco Secure Client. La VPN conectada falló debido a un error en la validación del certificado.



Error en la conexión VPN para el cliente VPN del administrador

## Paso 2. Confirmar sesiones VPN en CLI de FTD

**Ejecute** `show vpn-sessiondb detail anyconnect` el comando en la CLI de FTD (Line) para confirmar las sesiones VPN del ingeniero.

```
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

#### Troubleshoot

Puede esperar encontrar información sobre la autenticación VPN en el registro del sistema de depuración del motor de línea y en el archivo DART en el equipo con Windows.

Este es un ejemplo de los registros de depuración en el motor de línea durante la conexión VPN desde el cliente de ingeniería.

Jul 02 2024 04:16:03: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 7AF1C78ADCC8F941, subject name: CN=vpn

Jul 02 2024 04:16:03: %FTD-6-717022: Certificate was successfully validated. serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClic

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

#### Información Relacionada

[Configuración del servicio de gestión integrada de FDM para Firepower 2100](#)

[Configurar VPN de acceso remoto en FTD administrado por FDM](#)

[Configuración y verificación de Syslog en el administrador de dispositivos Firepower](#)

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).