Configurar la autenticación de certificado de cliente seguro en FTD administrado por FMC

Contenido

Introducción

Este documento describe el proceso de configuración de VPN de acceso remoto en Firepower Threat Defense (FTD) administrado por Firepower Management Center (FMC) con autenticación de certificados.

Colaboración de Dolly Jain y Rishabh Aggarwal, ingeniero del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

· Inscripción manual de certificados y aspectos básicos de SSL
· FMC
· Conocimientos básicos de autenticación para VPN de acceso remoto
· Autoridad de certificación (CA) de terceros como Entrust, Geotrust, GoDaddy, Thawte y VeriSign

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

· Secure Firepower Threat Defense versión 7.4.1
· Firepower Management Center (FMC) versión 7.4.1
· Secure Client versión 5.0.05040
· Microsoft Windows Server 2019 como servidor de la CA

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.

Configurar

Diagrama de la red

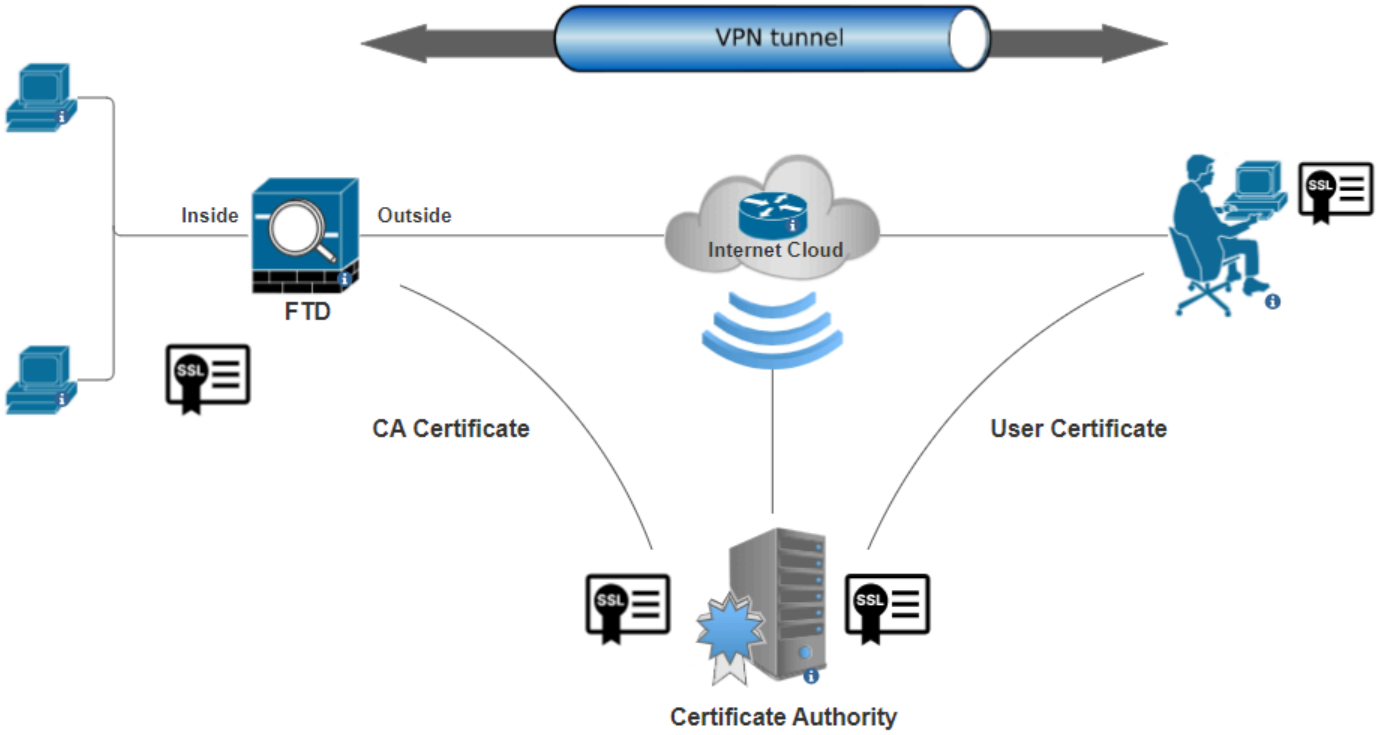
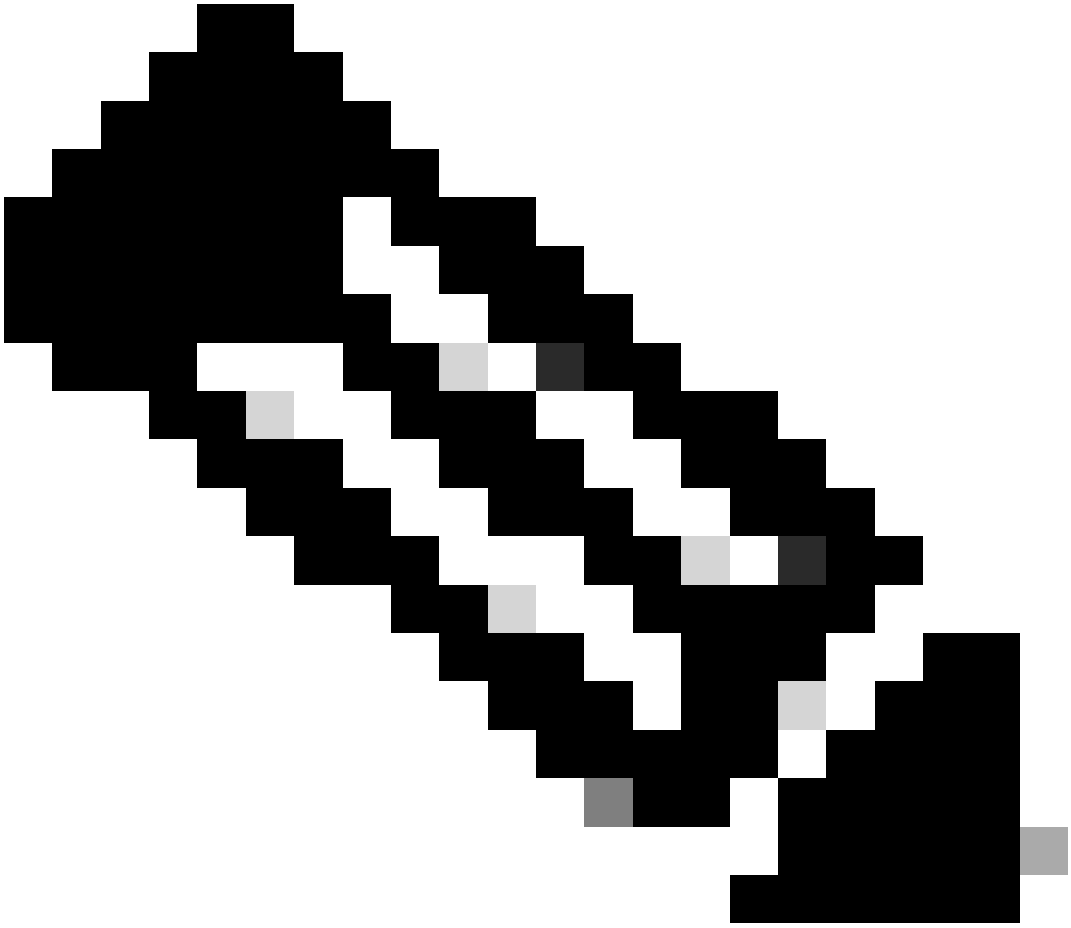


Diagrama de la red

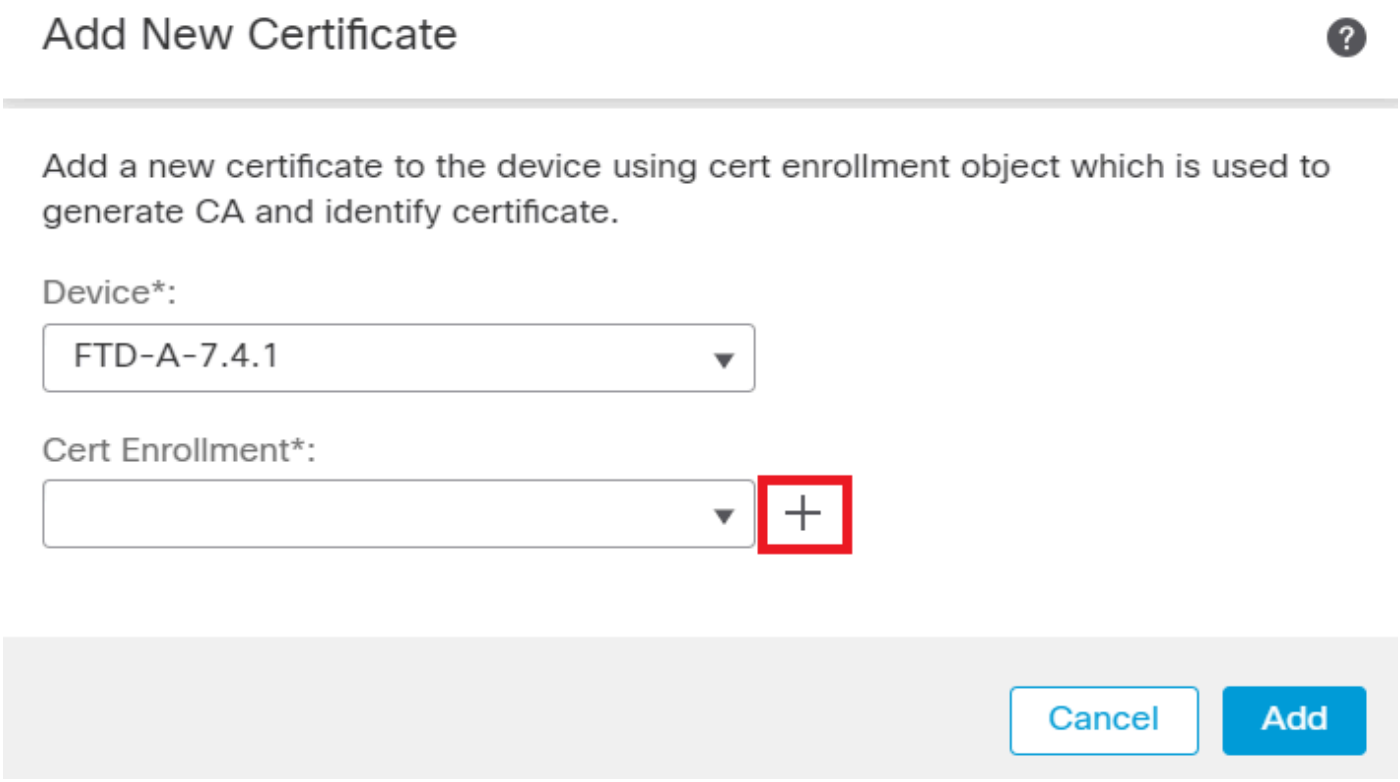
Configuraciones

a. Crear/importar un certificado utilizado para la autenticación del servidor



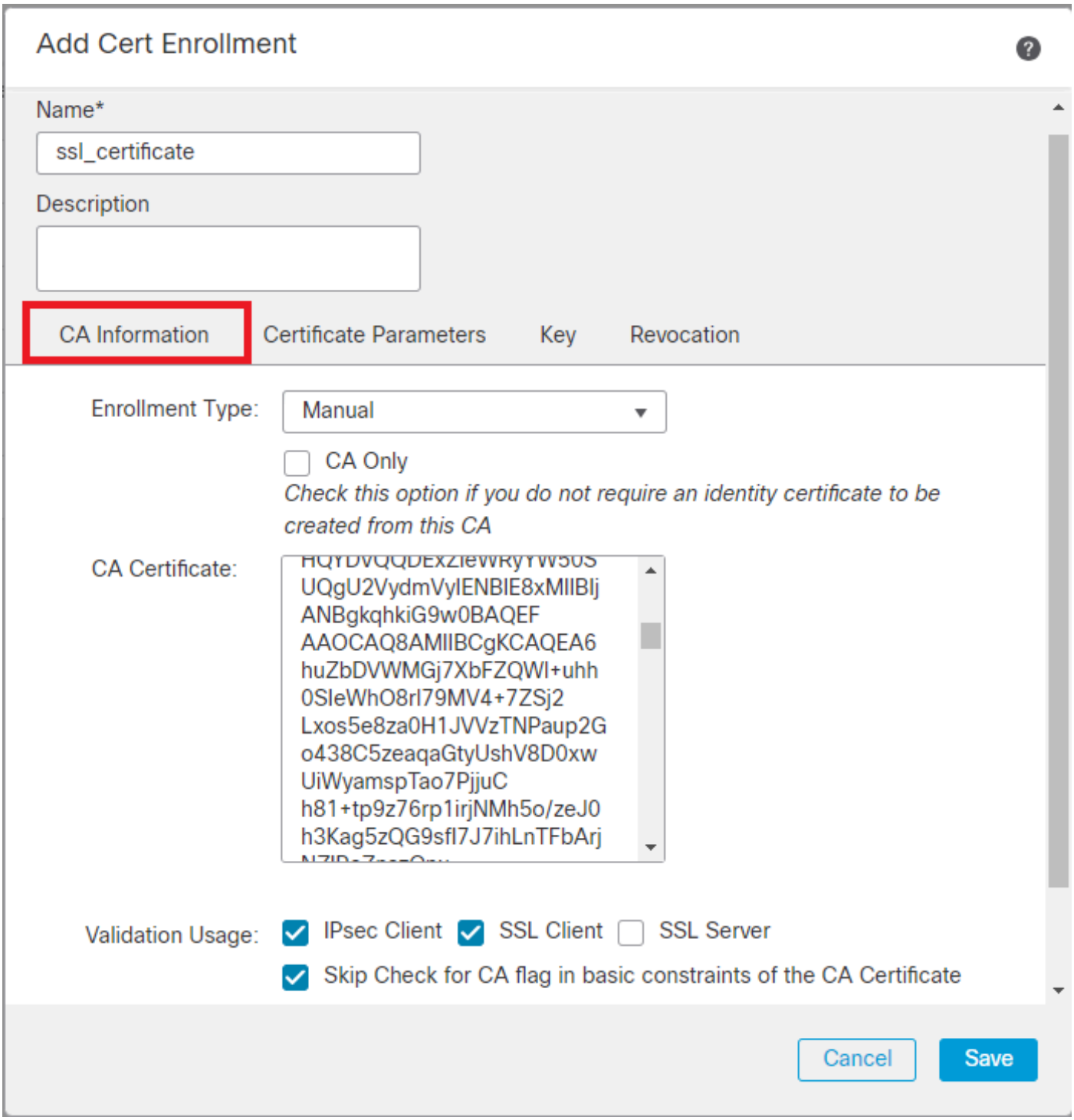
Nota: En FMC, se necesita un certificado de CA para poder generar el CSR. Si se genera CSR a partir de una fuente externa (OpenSSL o de terceros), el método manual falla y se debe utilizar el formato de certificado PKCS12.

Paso 1. Desplácese hasta Devices > Certificatesy haga clic en Add. Seleccione Dispositivo y haga clic en el signo más (+) en Inscripción de certificados.



Agregar inscripción de certificados

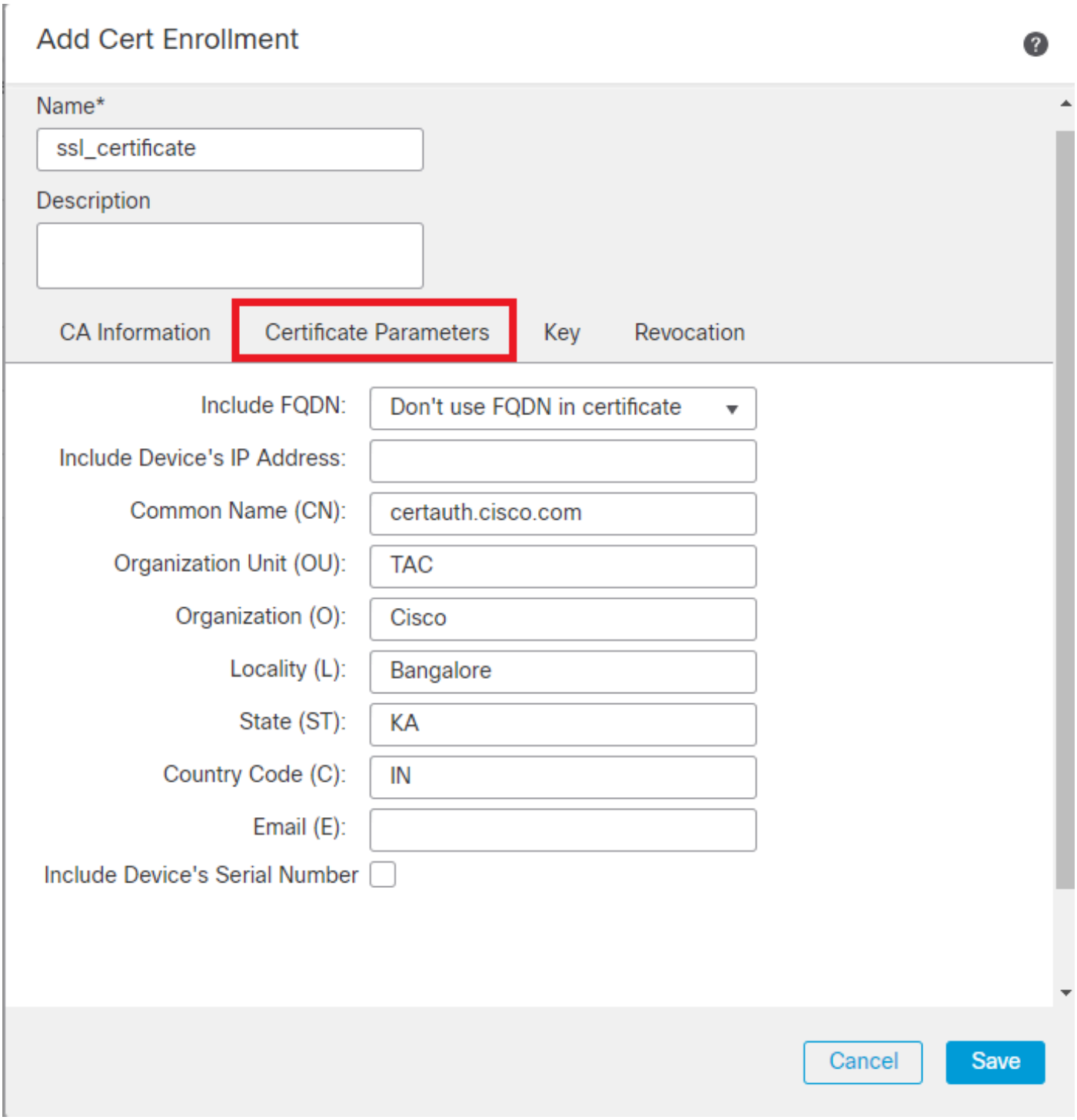
Paso 2. En la CA Information, seleccione el Tipo de inscripción como Manual y pegue el certificado de la Autoridad de certificación (CA) utilizado para firmar el CSR.



Agregar información de CA

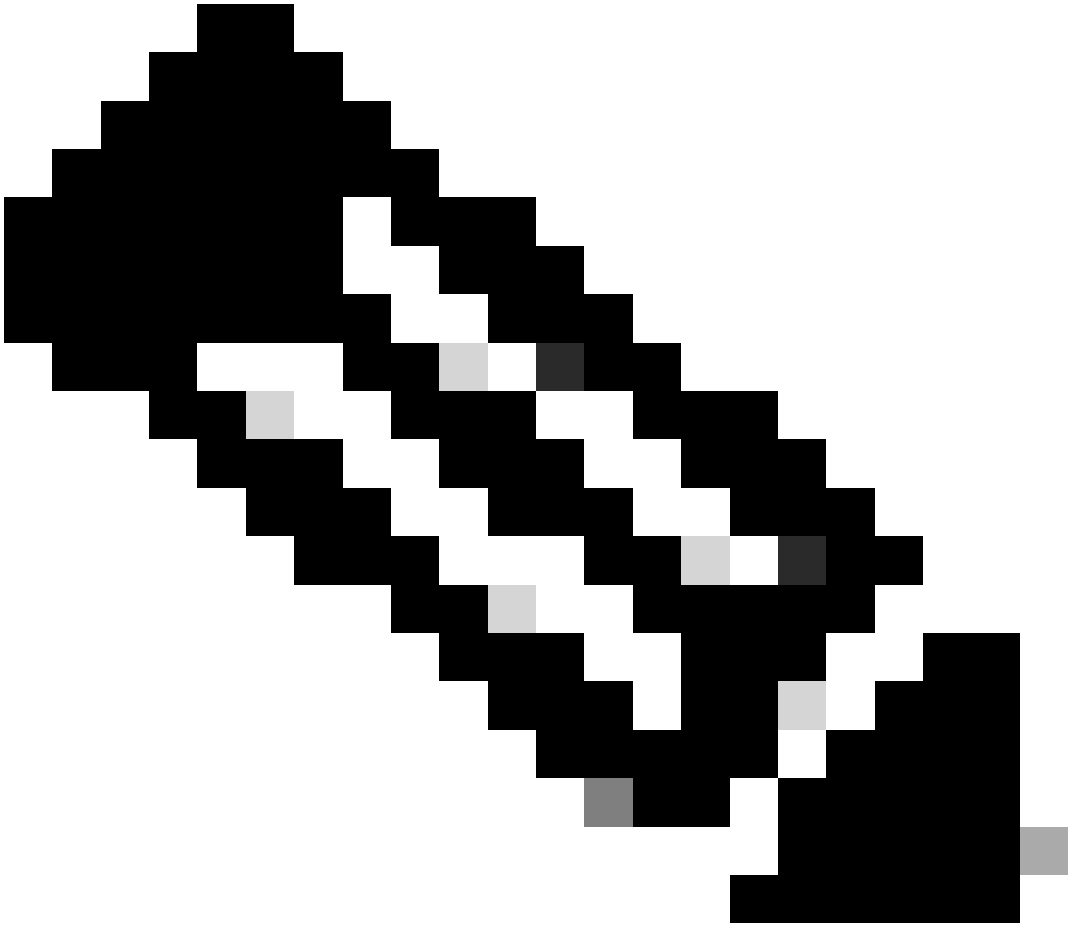
Paso 3. Para el uso de validación, seleccione IPsec Client, SSL Client y Skip Check for CA flag in basic constraints of the CA Certificate.

Paso 4. En Certificate Parameters, rellene los detalles del nombre del sujeto.

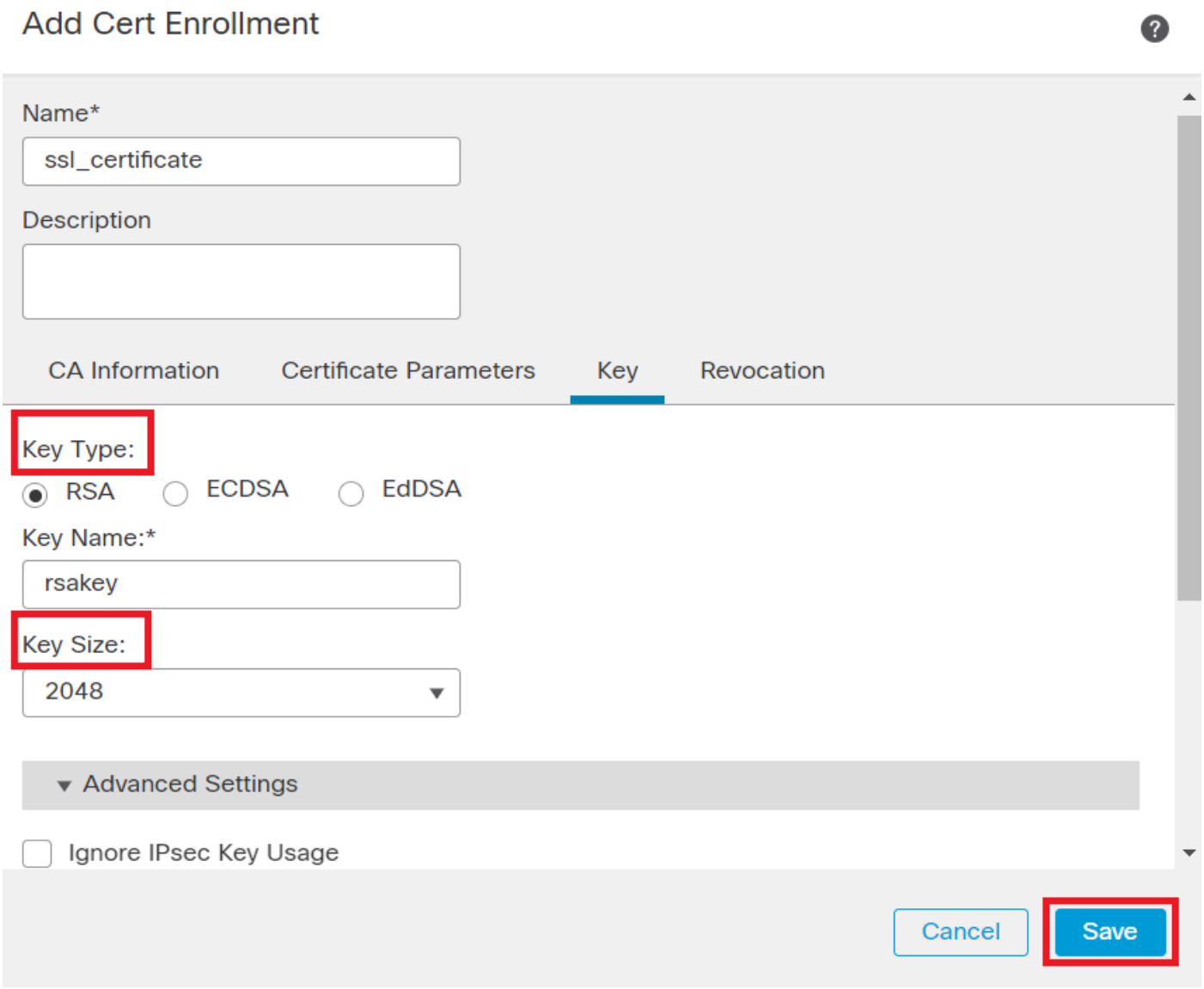


Agregar parámetros de certificado

Paso 5. En Keyseleccione el tipo de clave como RSA con un nombre y tamaño de clave. Haga clic en Save.

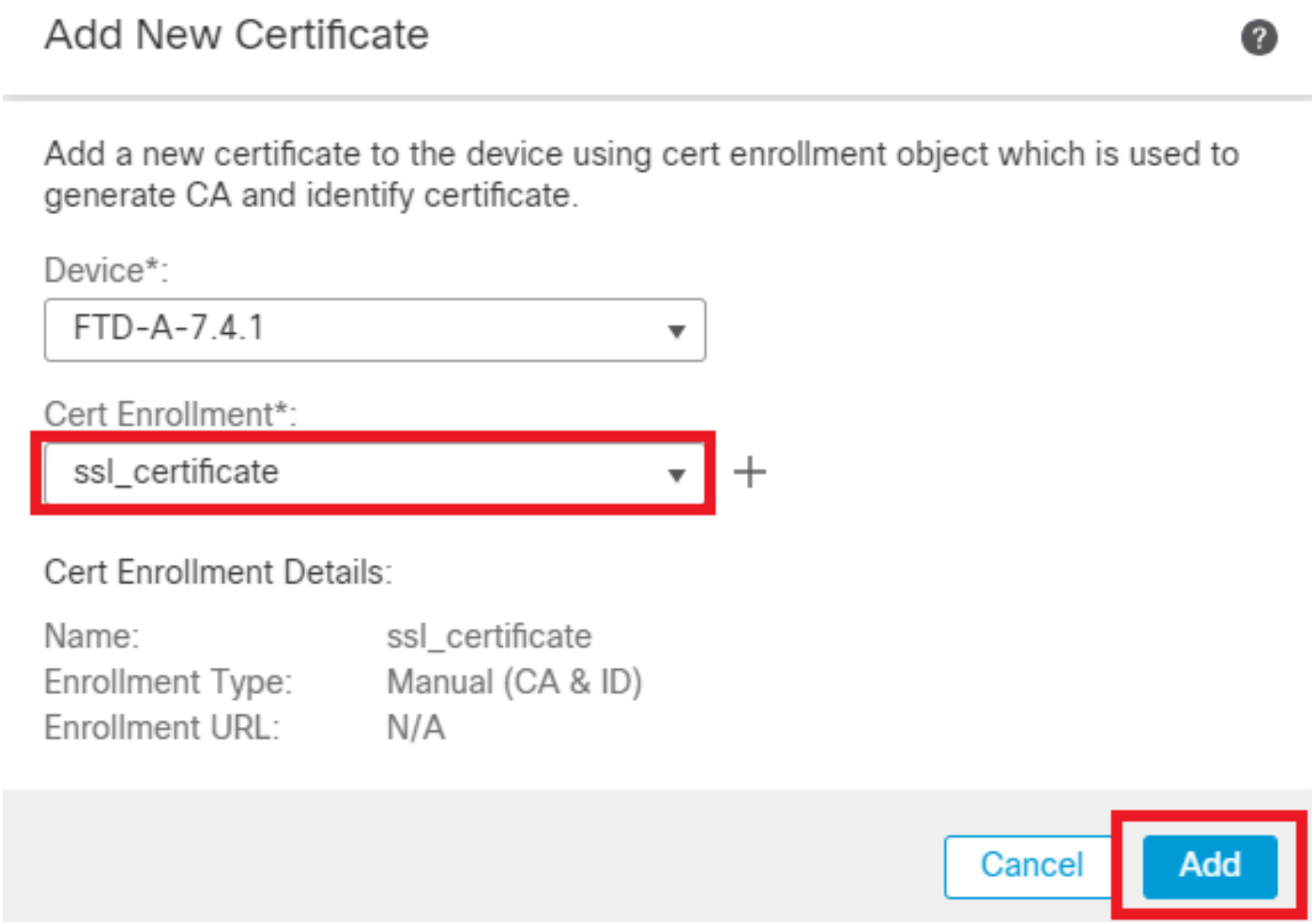


Nota: Para el tipo de clave RSA, el tamaño mínimo de clave es 2048 bits.



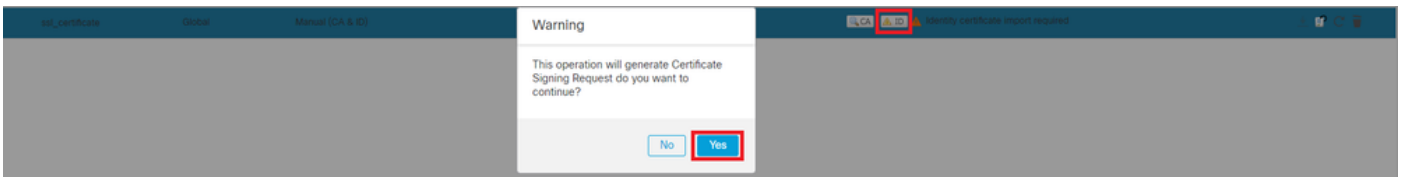
Agregar clave RSA

Paso 6. En Cert Enrollment, seleccione el punto de confianza en el menú desplegable que acaba de crear y haga clic en Add.



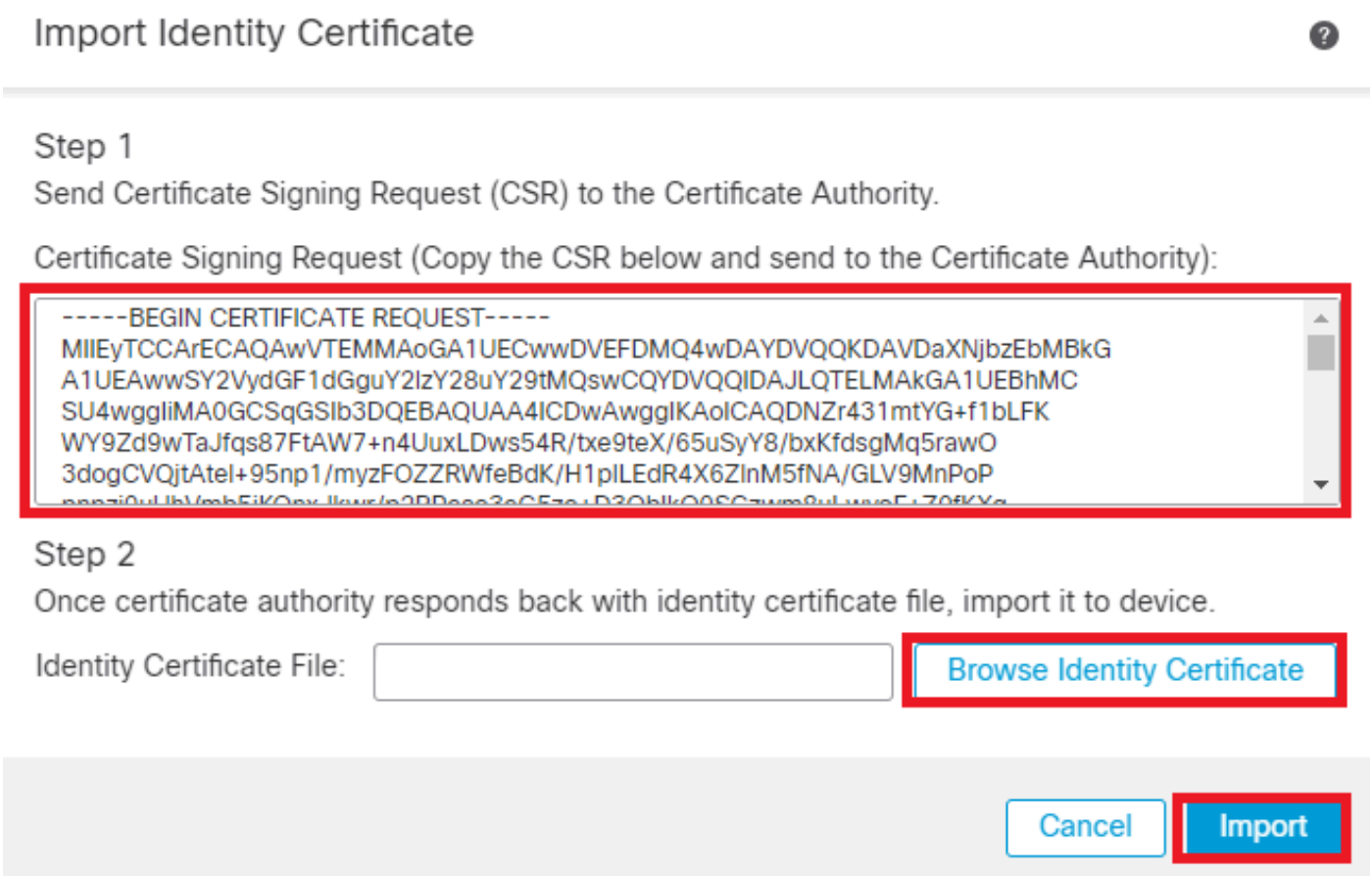
Agregar nuevo certificado

Paso 7. Haga clic en ID y, a continuación, haga clic Yes en el mensaje adicional para generar el CSR.

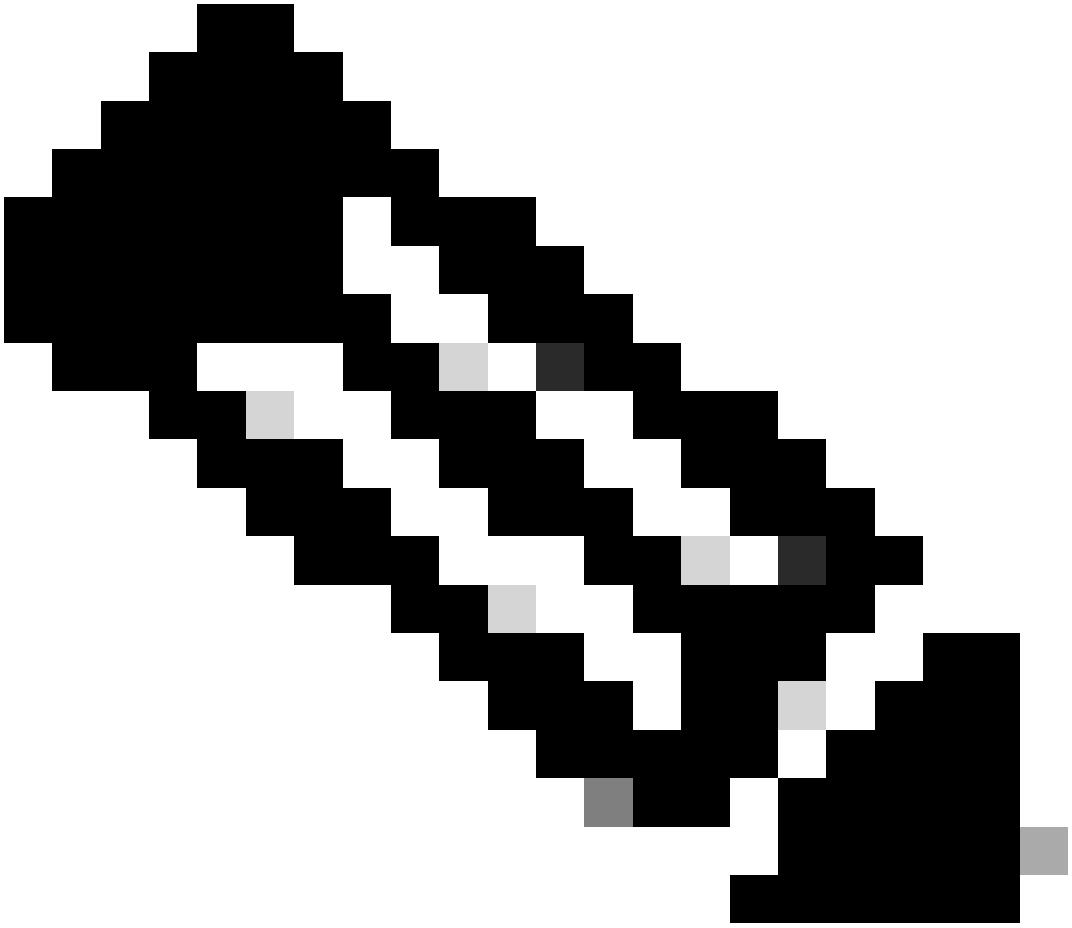


Generar CSR

Paso 8. Copie la CSR y consígala firmada por la autoridad de certificación. Una vez que la CA haya emitido el certificado de identidad, impórtelo haciendo clic en Browse Identity Certificate y haga clic en Import .

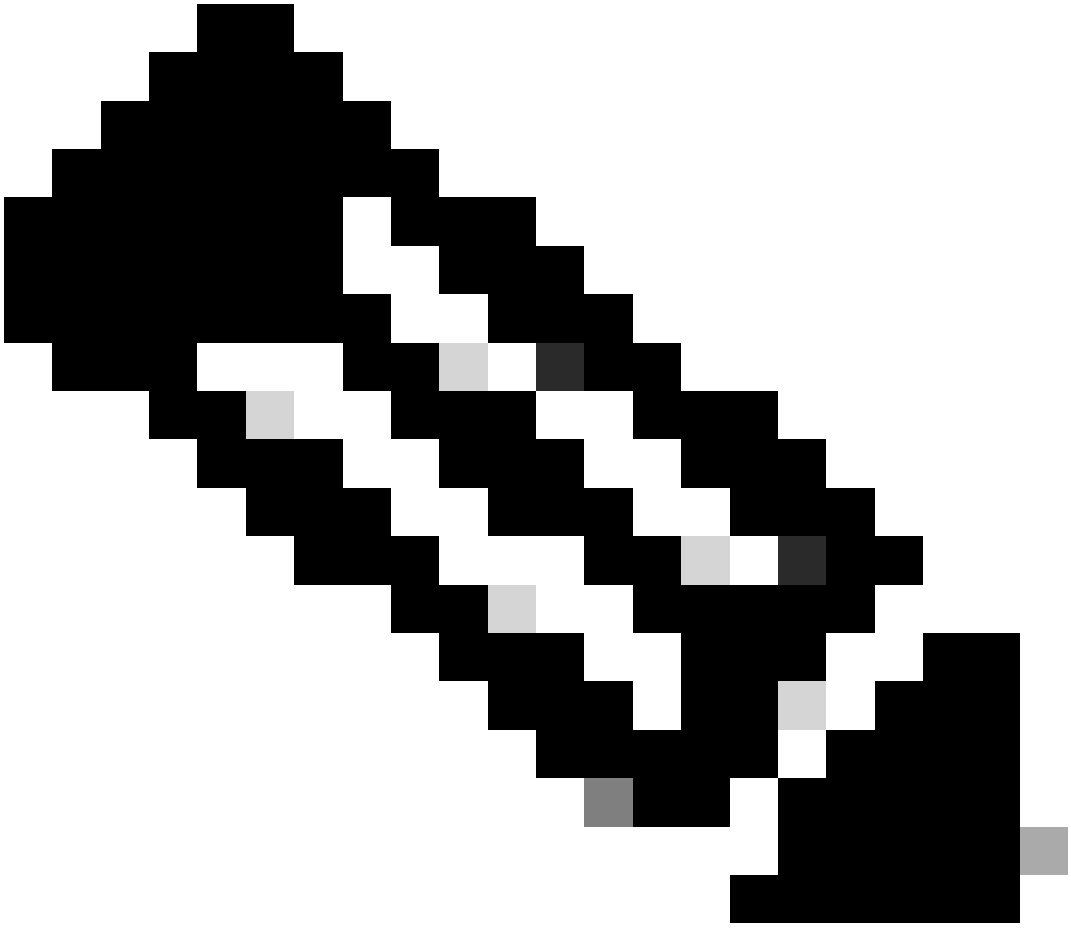


Importar certificado de ID



Nota: Si la emisión del certificado de ID lleva tiempo, puede repetir el paso 7 más tarde. Esto generará la misma CSR y podemos importar el certificado de ID.

b. Agregar un certificado de CA interna/de confianza

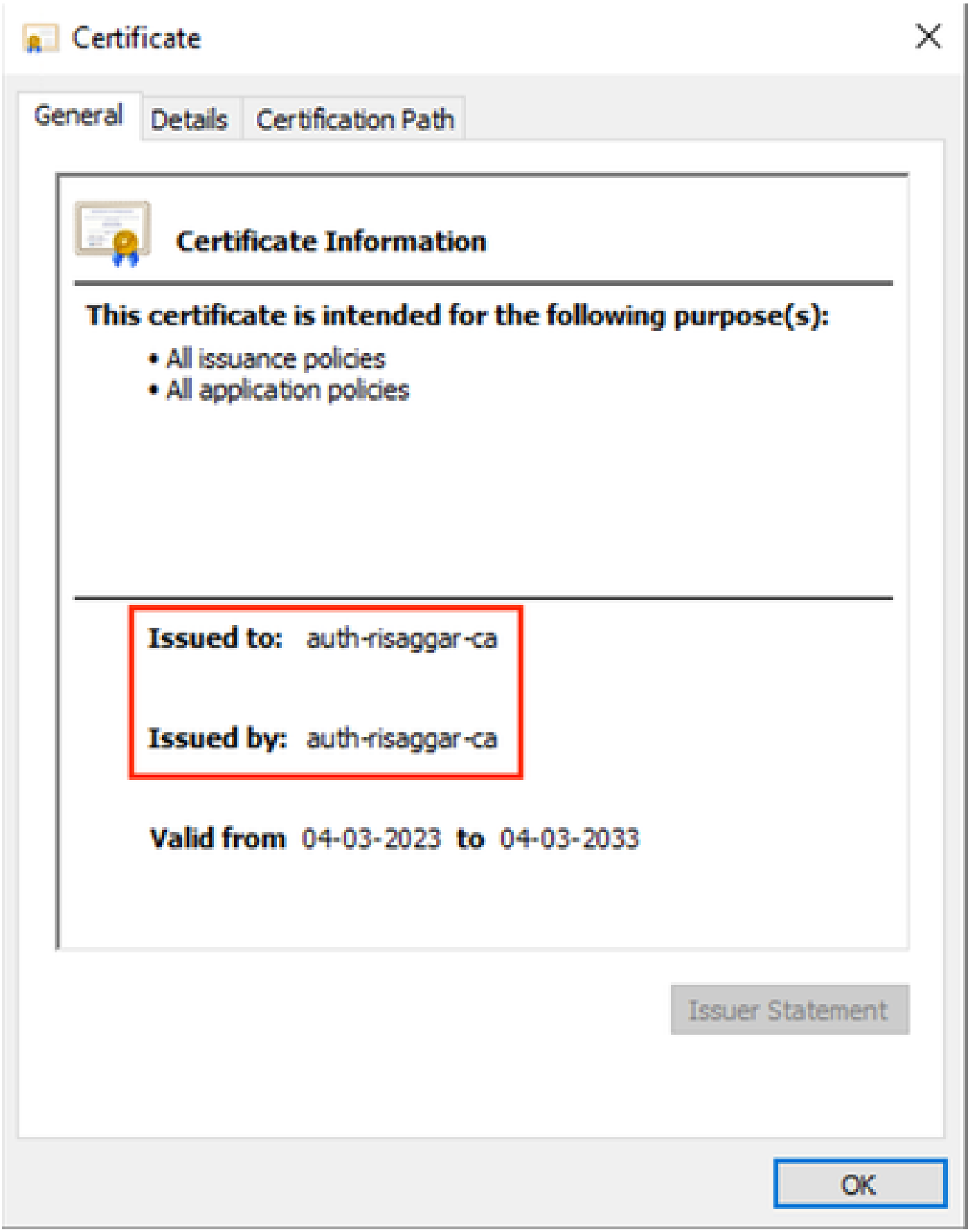


Nota: Si la autoridad de certificación (CA) utilizada en el paso (a), **"Crear/importar un certificado utilizado para la autenticación del servidor"** también emite certificados de usuario, puede omitir el **paso (b), "Agregar un certificado de CA de confianza/interno".** No es necesario volver a agregar el mismo certificado de CA, por lo que también se debe evitar. Si se agrega el mismo certificado de CA nuevamente, el punto de confianza se configura con "validation-usage none" que puede afectar la autenticación del certificado para RAVPN.

Paso 1. Desplácese hasta Devices > Certificates y haga clic en Add.

Seleccione Dispositivo y haga clic en el signo más (+) en Inscripción de certificados.

Aquí, "auth-risaggar-ca" se utiliza para emitir certificados de identidad/usuario.

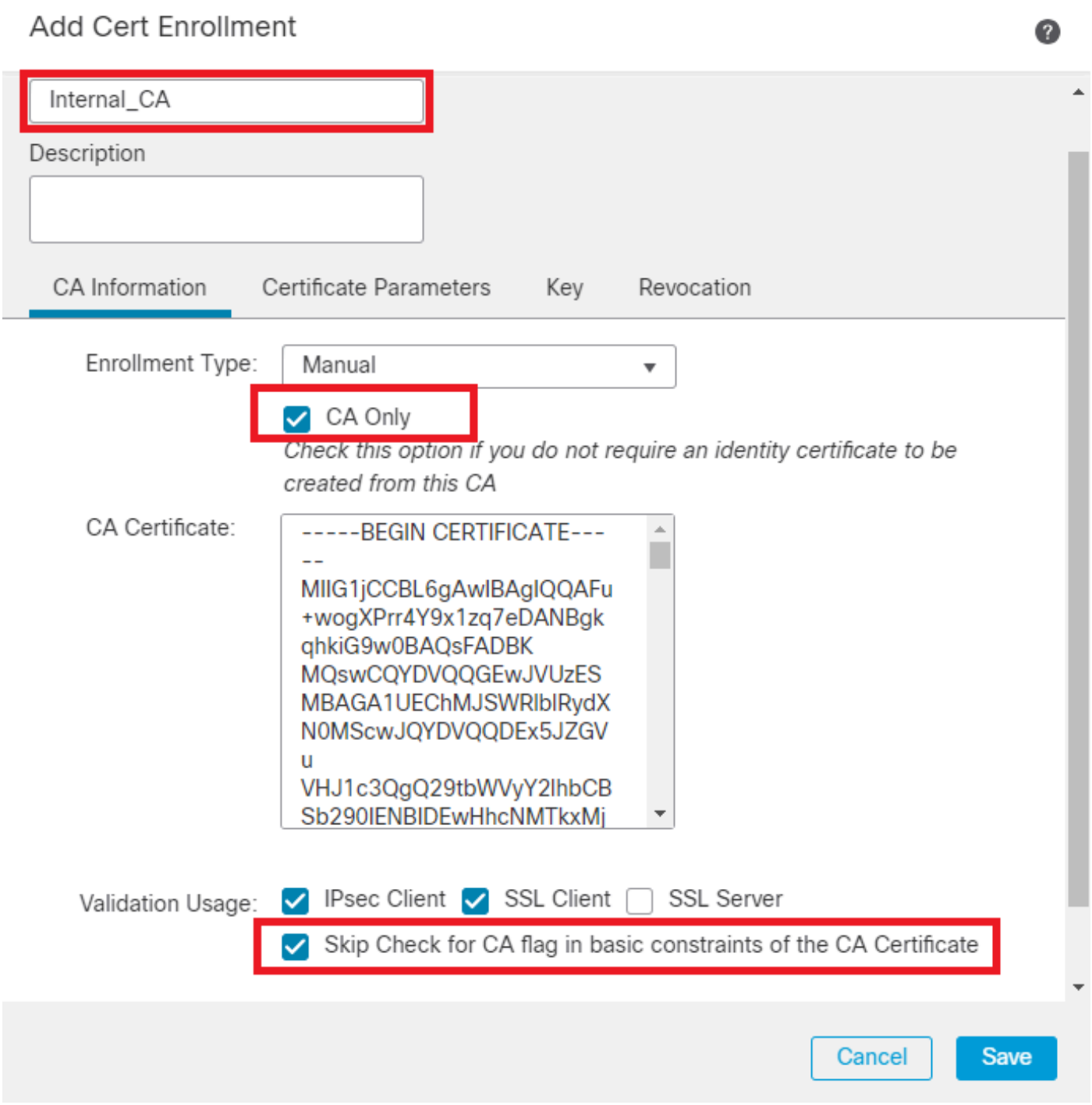


auth-risaggar-ca

Paso 2. Introduzca un nombre de punto de confianza y seleccioneManual como tipo de inscripción en CA information.

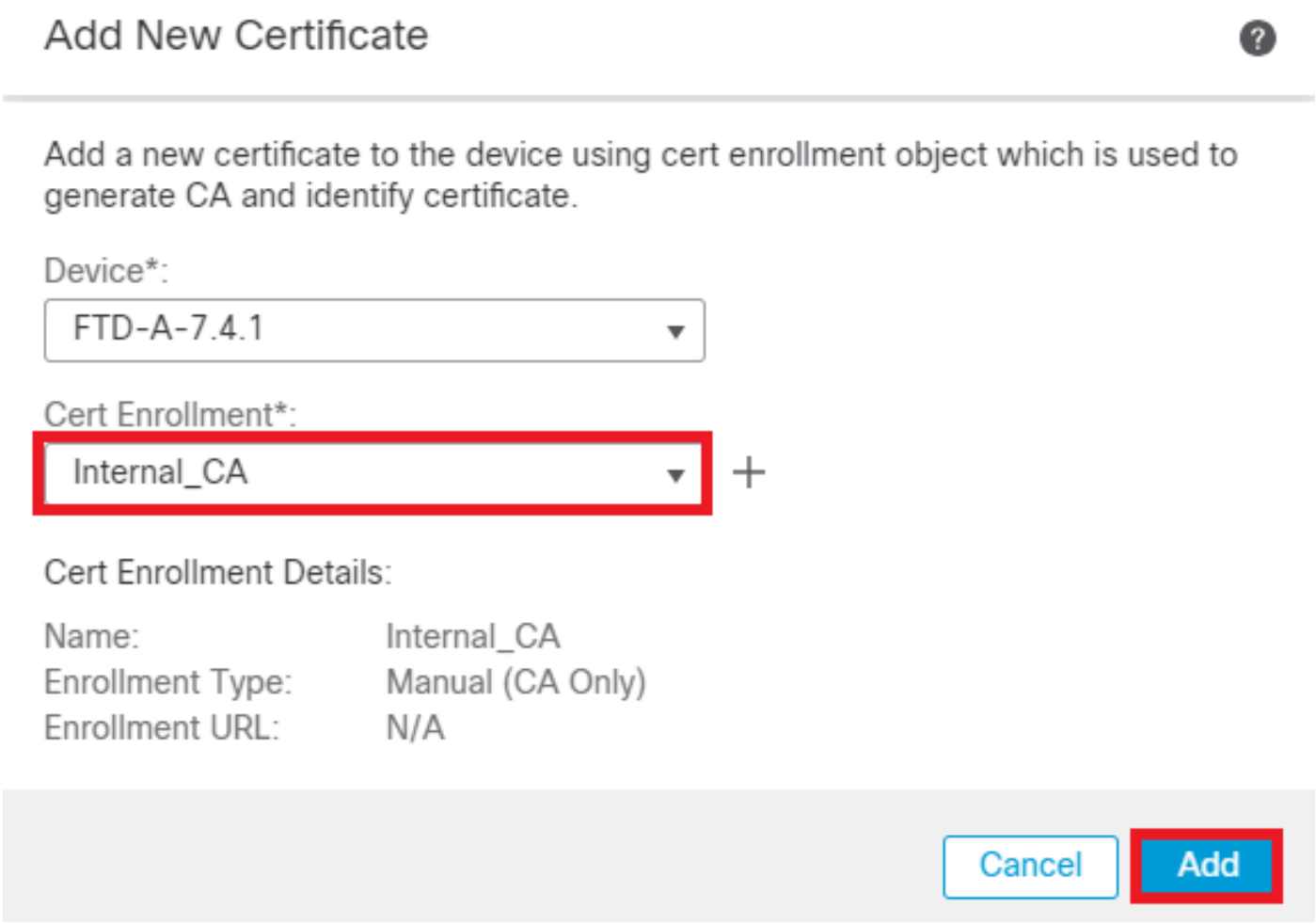
Paso 3. Verifique CA Onlyy pegue el certificado de CA interna/de confianza en formato pem.

Paso 4. Marque **Skip Check for CA flag in basic constraints of the CA Certificate**y haga clic en Save.



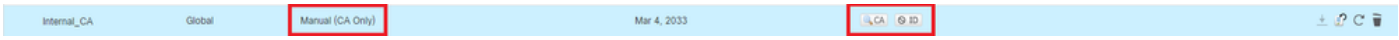
Agregar punto de confianza

Paso 5. En Cert Enrollment, seleccione el punto de confianza en el menú desplegable que acaba de crear y haga clic en Add.



Agregar CA interna

Paso 6. El certificado agregado anteriormente se muestra como:

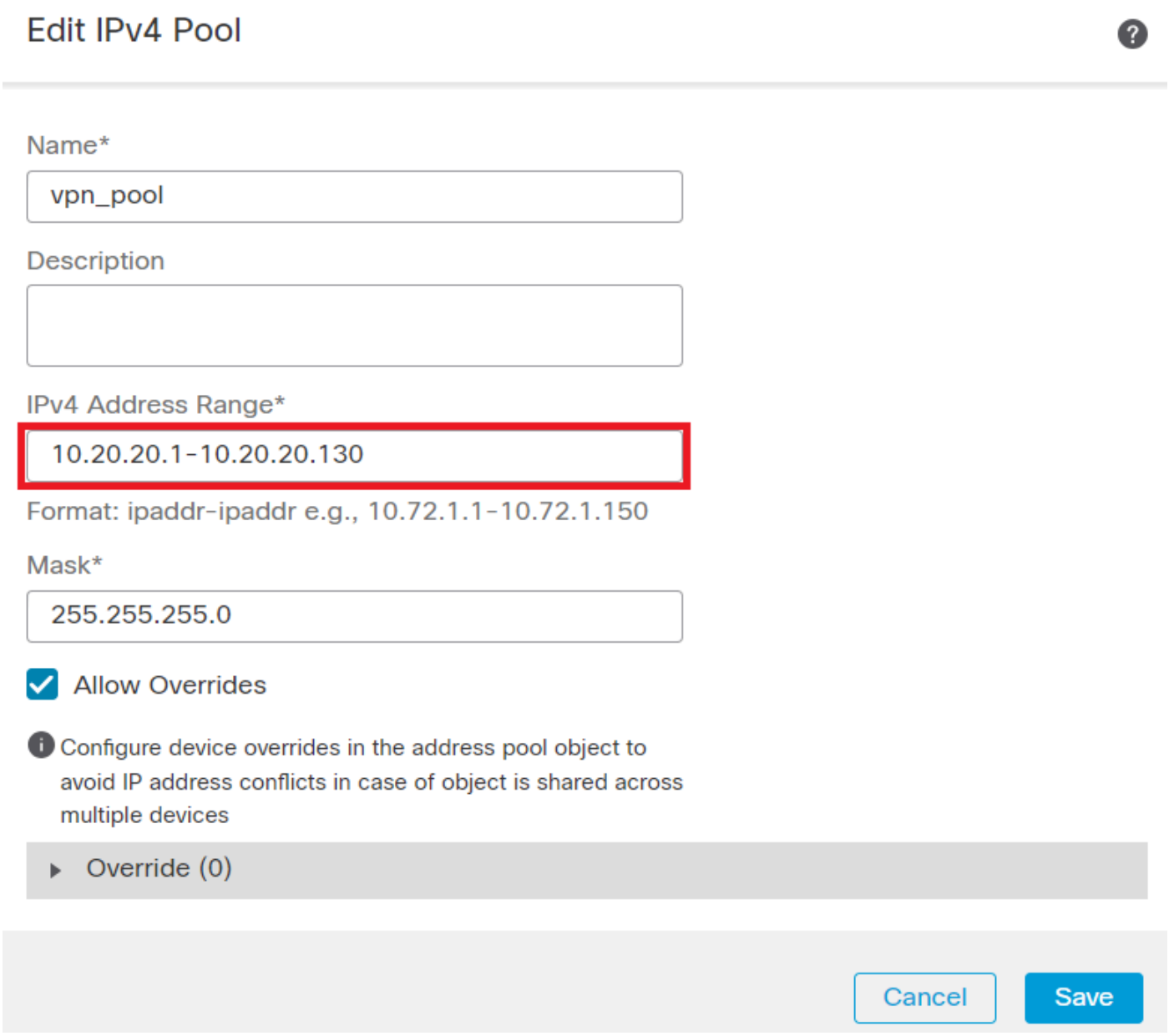


Certificado agregado

c. Configure el Pool de Direcciones para los Usuarios de VPN

Paso 1. Vaya a Objects > Object Management > Address Pools > IPv4 Pools .

Paso 2. Introduzca el nombre y el intervalo de direcciones IPv4 con una máscara.



Agregar conjunto IPv4

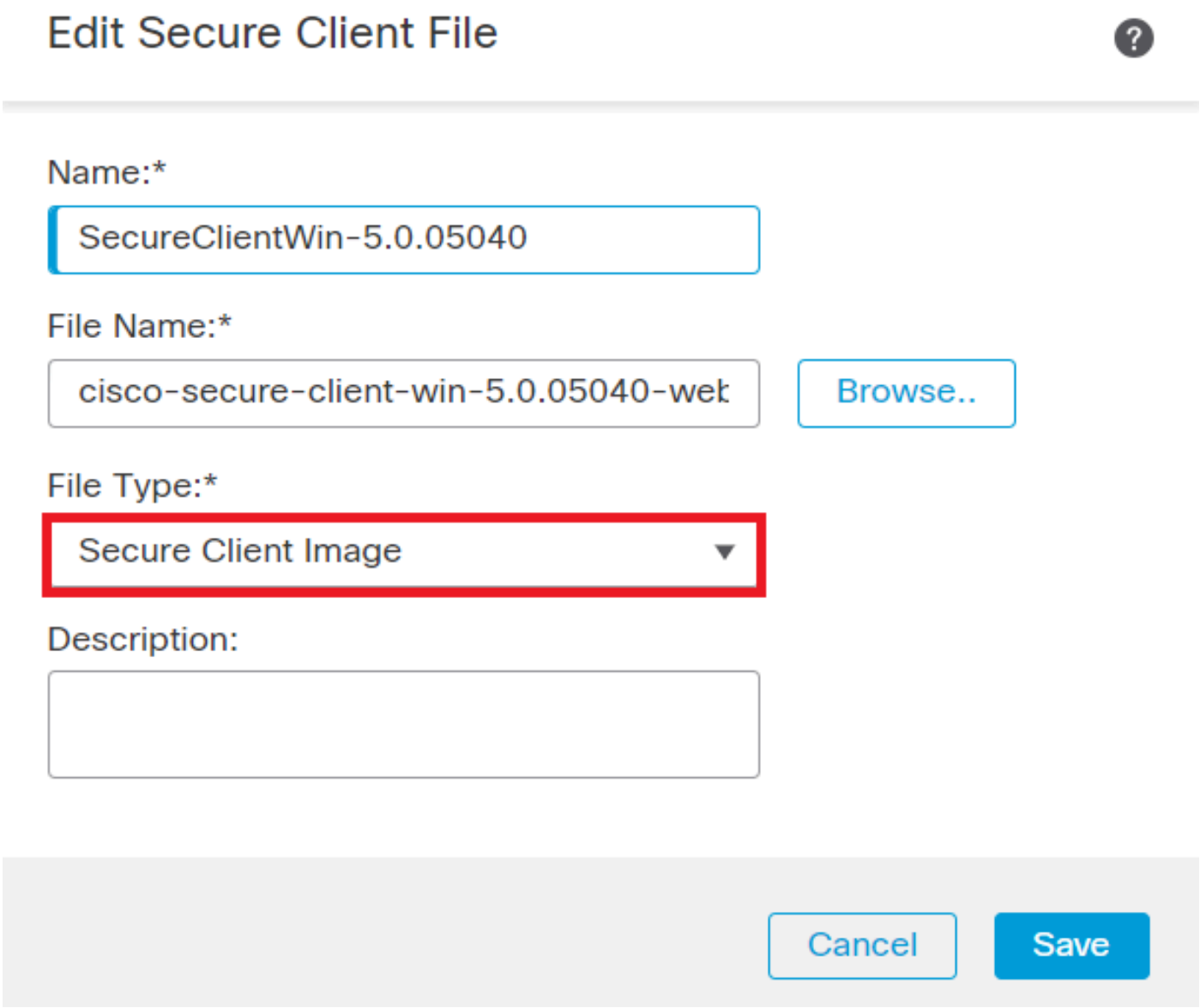
d. Cargar imágenes de Secure Client

Paso 1. Descargue las imágenes de cliente seguras de implementación web según el sistema operativo desde el sitio Cisco Software.

Paso 2. Vaya a Objects > Object Management > VPN > Secure Client File > Add Secure Client File .

Paso 3. Introduzca el nombre y seleccione el archivo Secure Client del disco.

Paso 4. Seleccione el tipo de archivo como Secure Client Image y haga clic en Save.



Agregar imagen de cliente seguro

e. Crear y cargar perfil XML

Paso 1. Descargue e instale Secure Client Profile Editor desde el sitio Cisco Software.

Paso 2. Cree un nuevo perfil y selecciónelo All en el menú desplegable Selección de certificado de cliente. Controla principalmente los almacenes de certificados que Secure Client puede utilizar para almacenar y leer certificados.

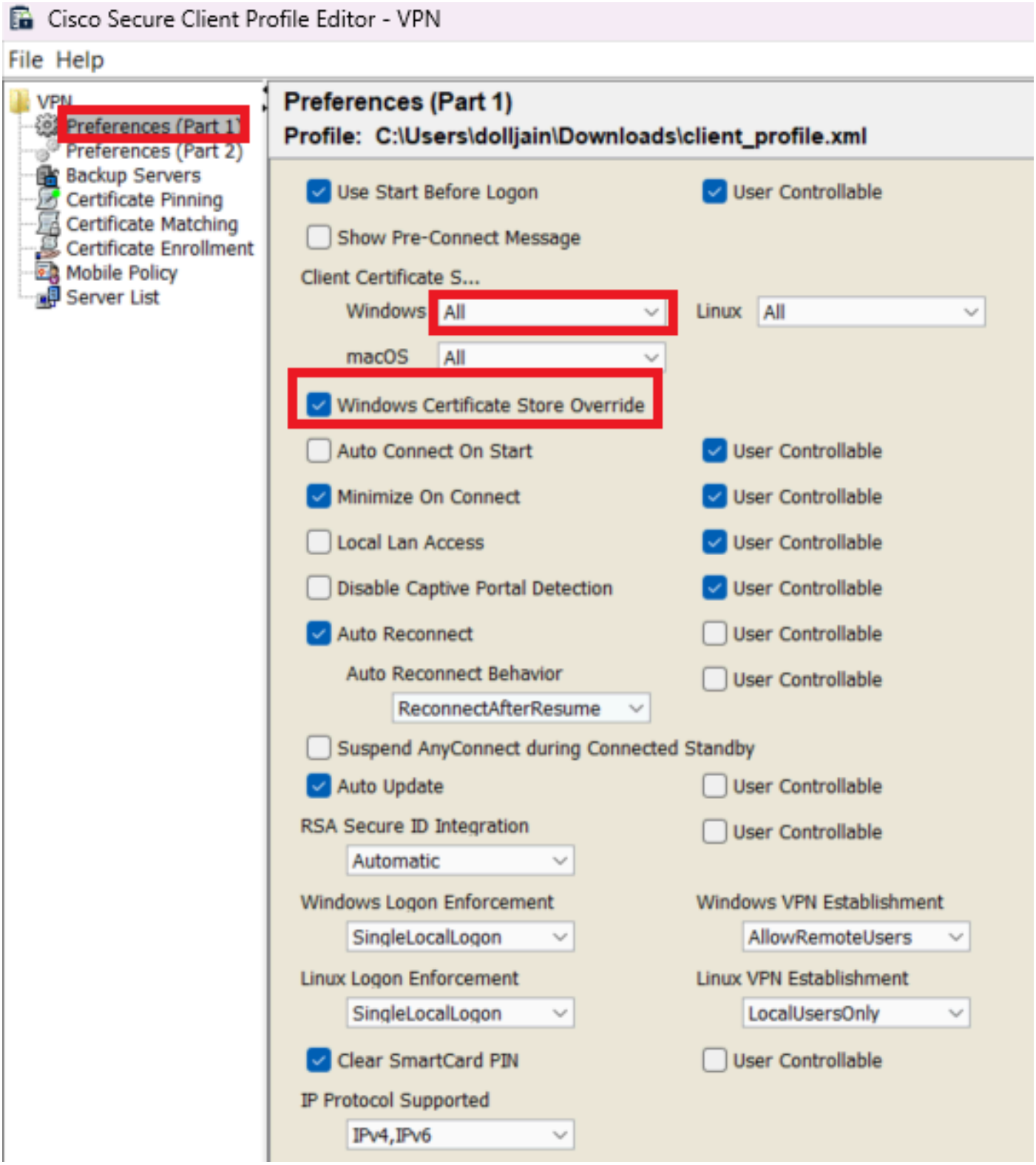
Otras dos opciones disponibles son:

- **Equipo**: Secure Client está restringido a la búsqueda de certificados en el almacén de certificados del equipo local de Windows.
- **Usuario**: Secure Client está restringido a la búsqueda de certificados en el almacén de certificados de usuario local de Windows.

Establecer la invalidación del almacén de certificados como True .

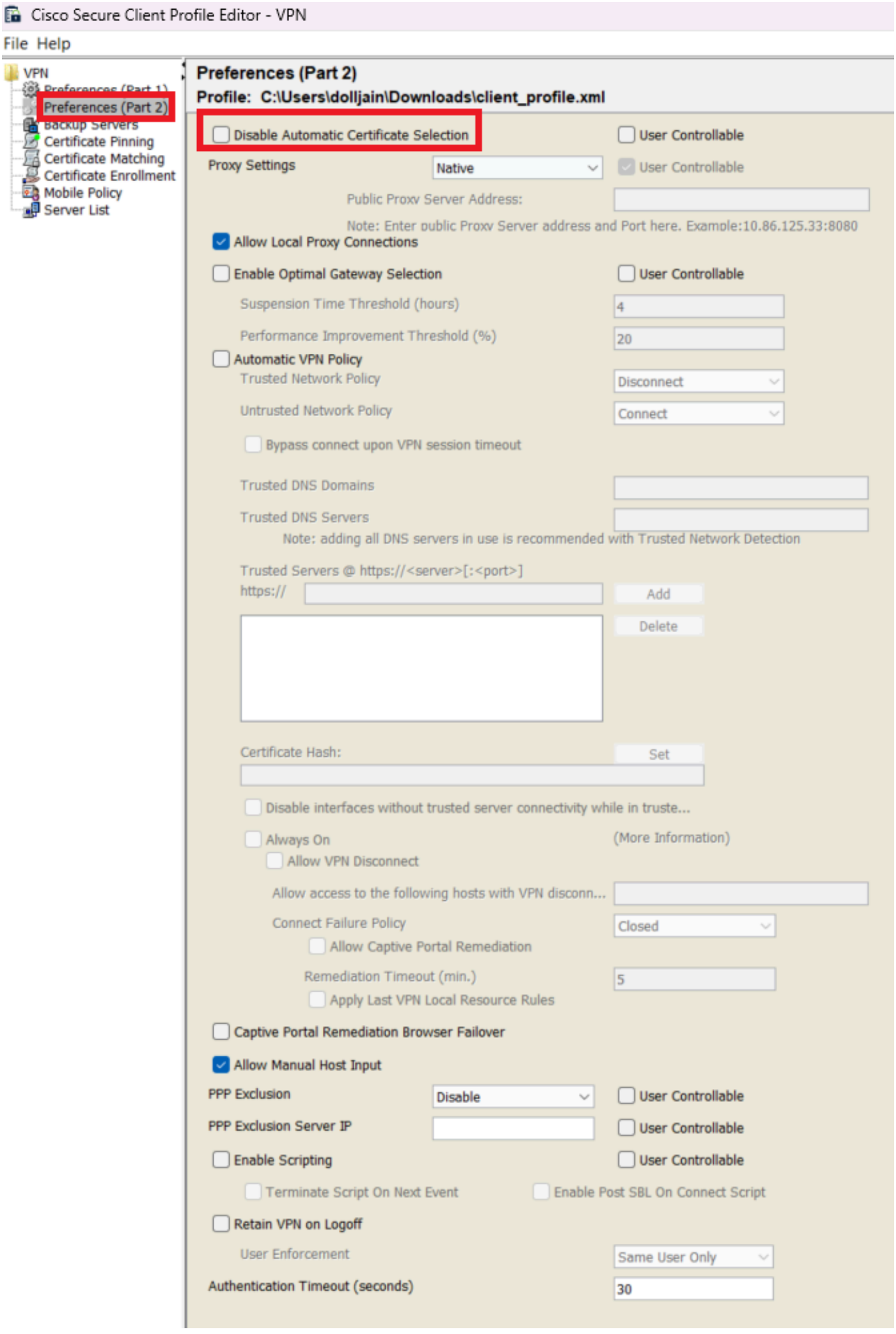
Esto permite a un administrador indicar a Secure Client que utilice certificados del almacén de certificados del equipo Windows (sistema local)

para la autenticación de certificados de cliente. La invalidación del almacén de certificados sólo se aplica a SSL, donde la conexión se inicia, de forma predeterminada, mediante el proceso de la interfaz de usuario. Cuando se utiliza IPSec/IKEv2, esta función del perfil de cliente seguro no es aplicable.



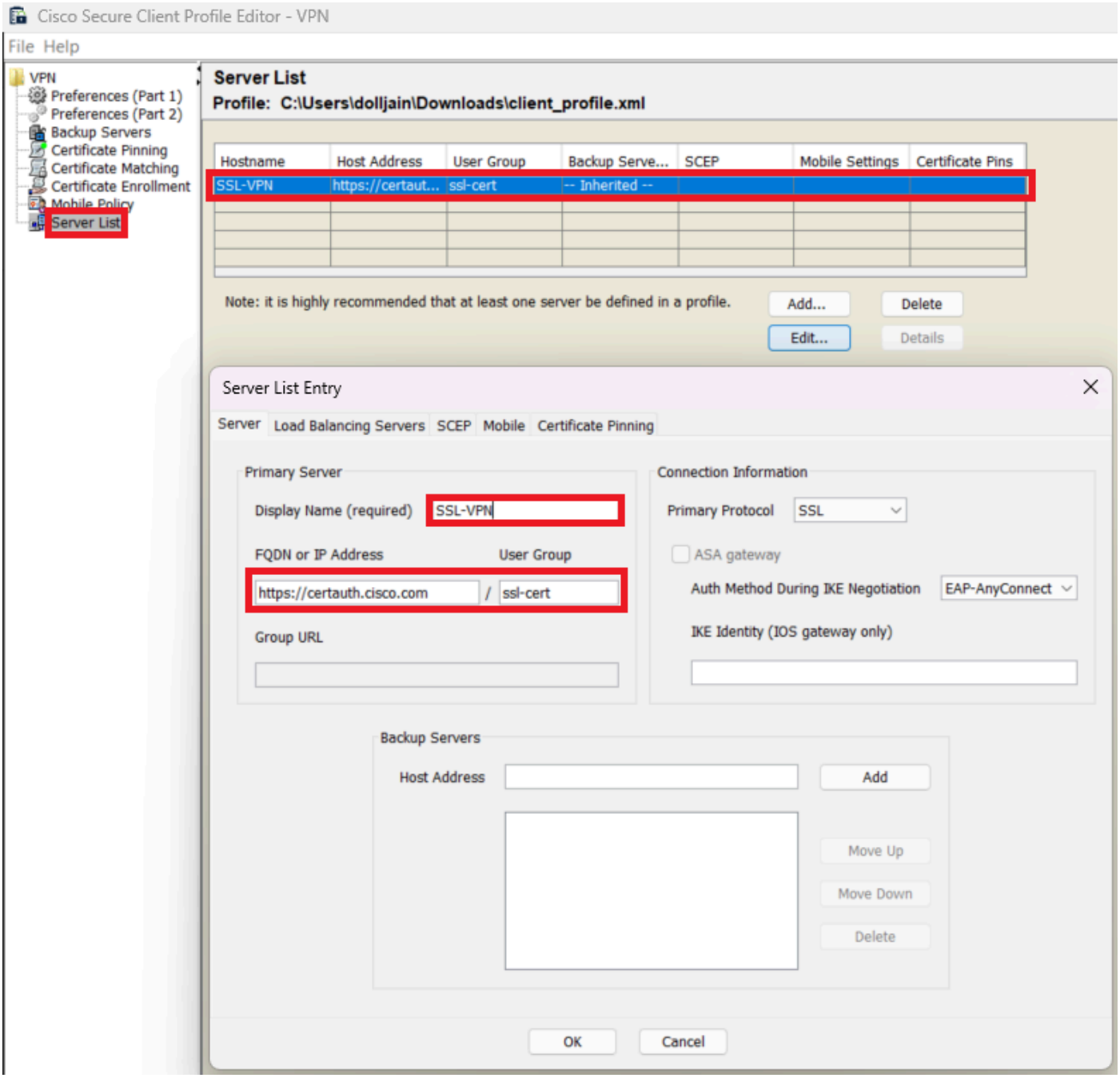
Agregar preferencias (parte 1)

Paso 3. (Opcional) Desmarque la opción Disable Automatic Certificate Selection, ya que evita que el usuario solicite seleccionar el certificado de autenticación.



Agregar preferencias (parte 2)

Server List Entry para configurar un perfil en Secure Client VPN proporcionando group-alias y group-url en la Lista de servidores y guarde el perfil XML.



Agregar lista de servidores

Paso 5. Por último, el perfil XML está listo para utilizarse.

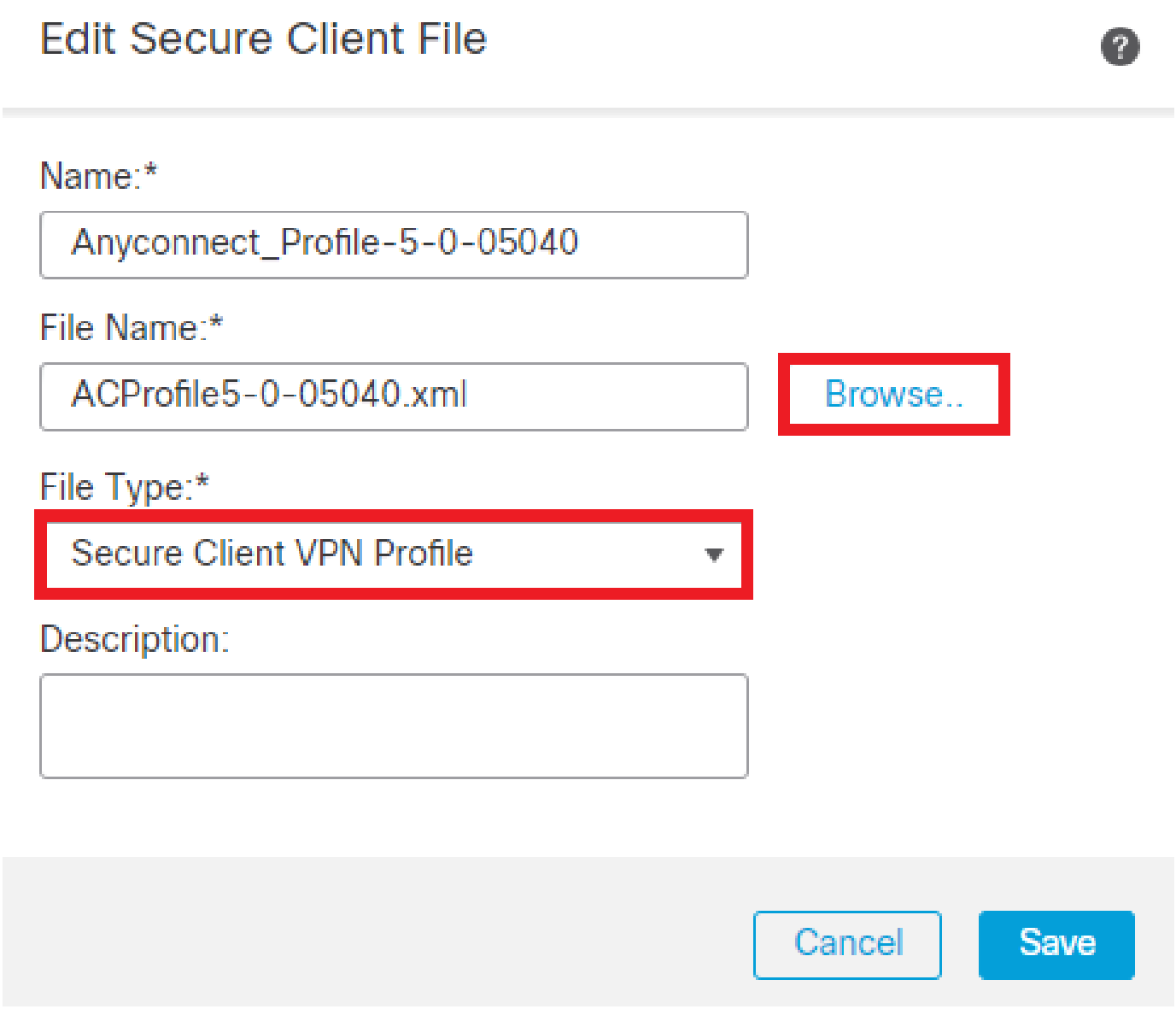
Perfil XML

Ubicación de perfiles XML para varios sistemas operativos:

- **Windows** - C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile
- **MacOS**: /opt/cisco/anyconnect/profile
- **Linux**: /opt/cisco/anyconnect/profile

Paso 6. Vaya a Objects > Object Management > VPN > Secure Client File > Add Secure Client Profile .

Introduzca el nombre del archivo y haga clic en Browse para seleccionar el perfil XML. Haga clic en Save.

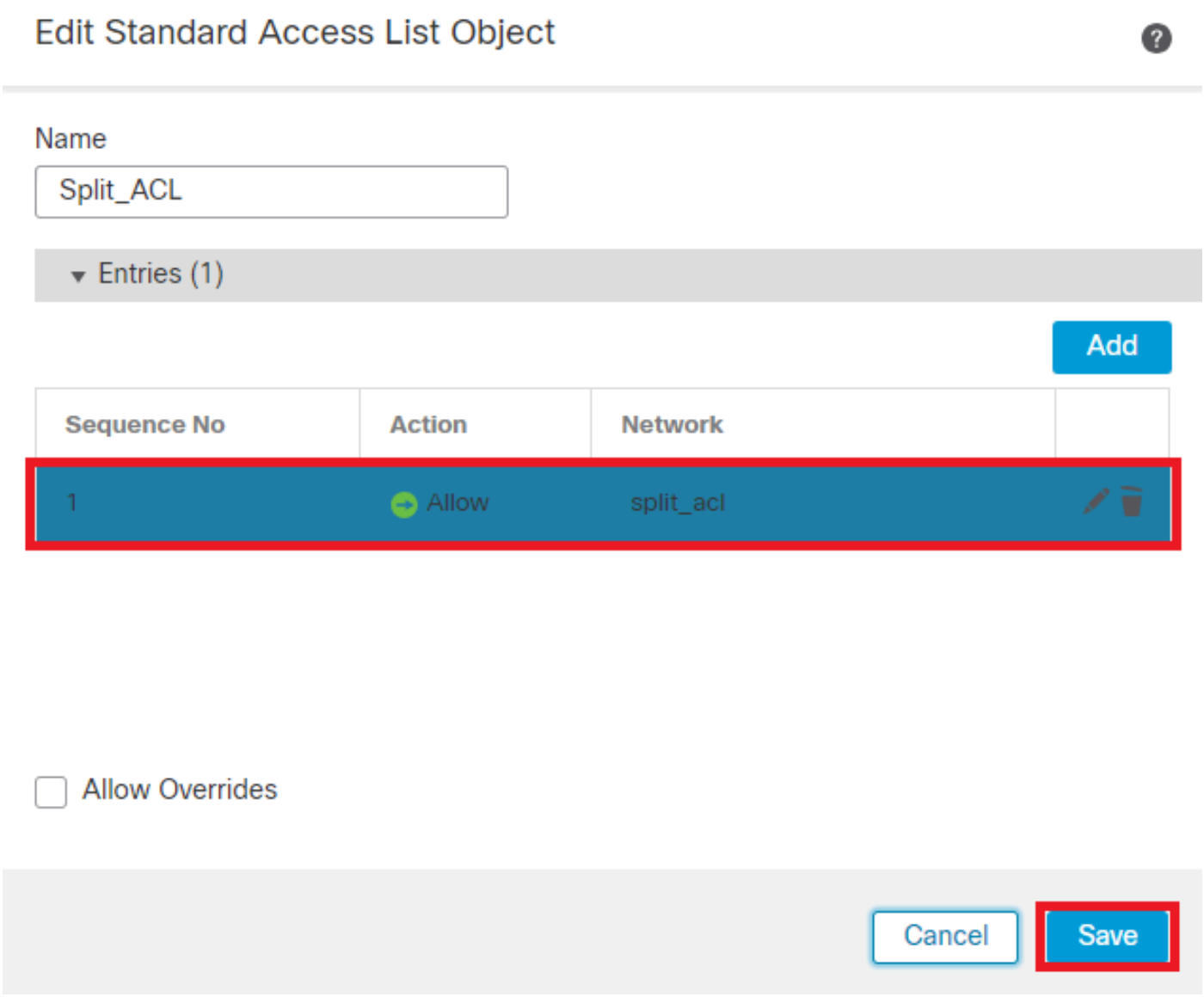


Agregar perfil VPN de cliente seguro

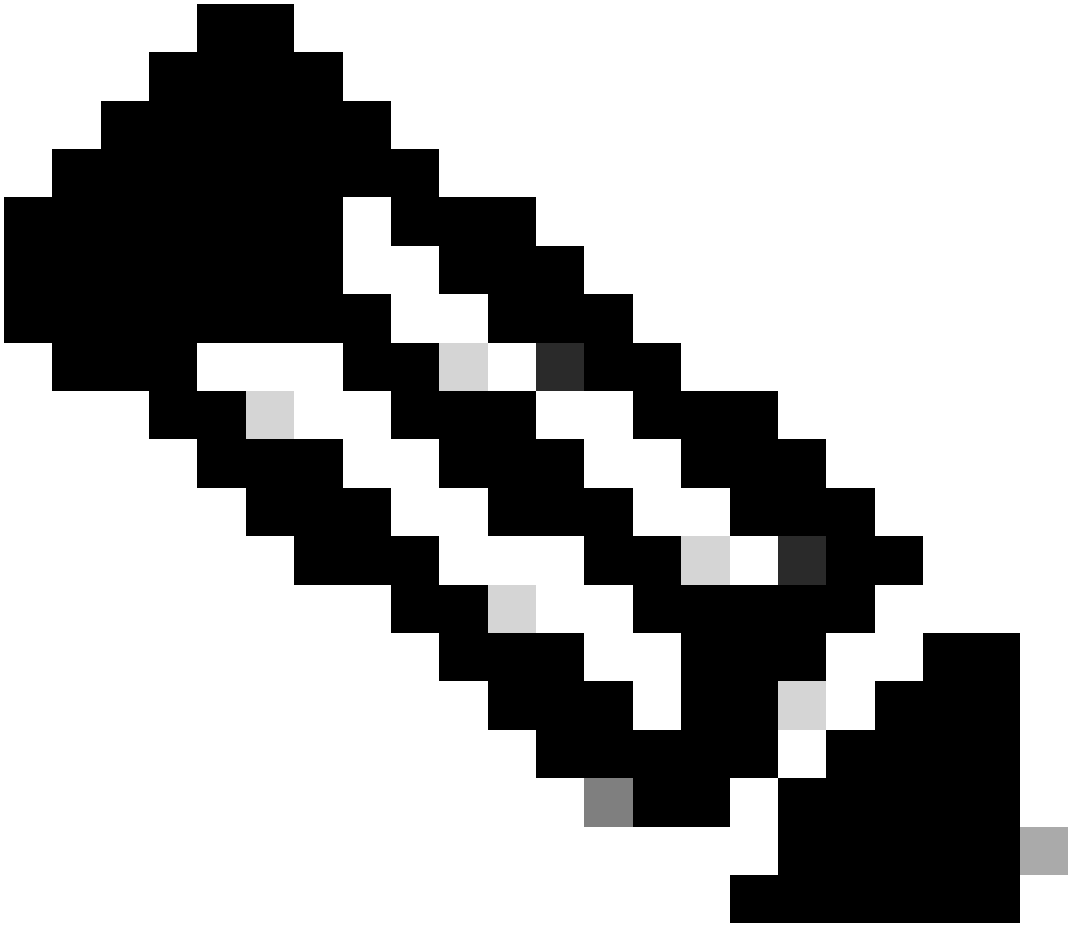
Configuración de VPN de acceso remoto

Paso 1. Cree una ACL según los requisitos para permitir el acceso a los recursos internos.

Desplácese hasta Objects > Object Management > Access List > Standard y haga clic en Add Standard Access List.



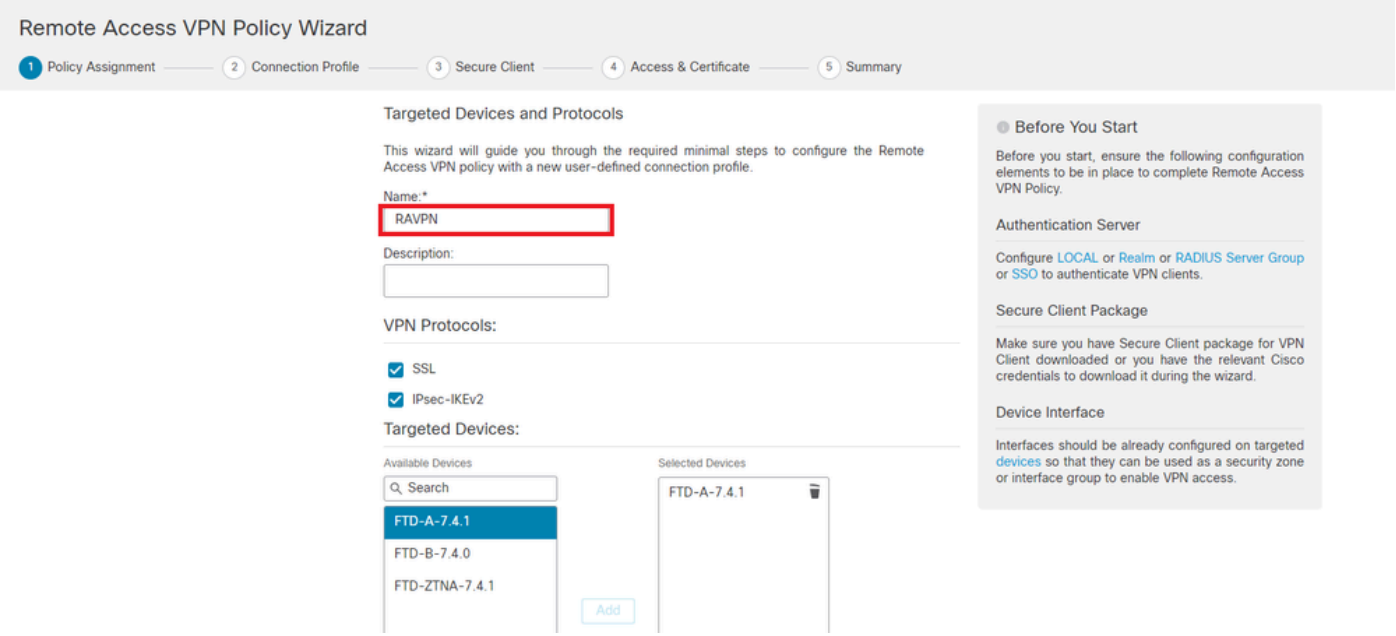
Agregar ACL estándar



Nota: Secure Client utiliza esta ACL para agregar rutas seguras a los recursos internos.

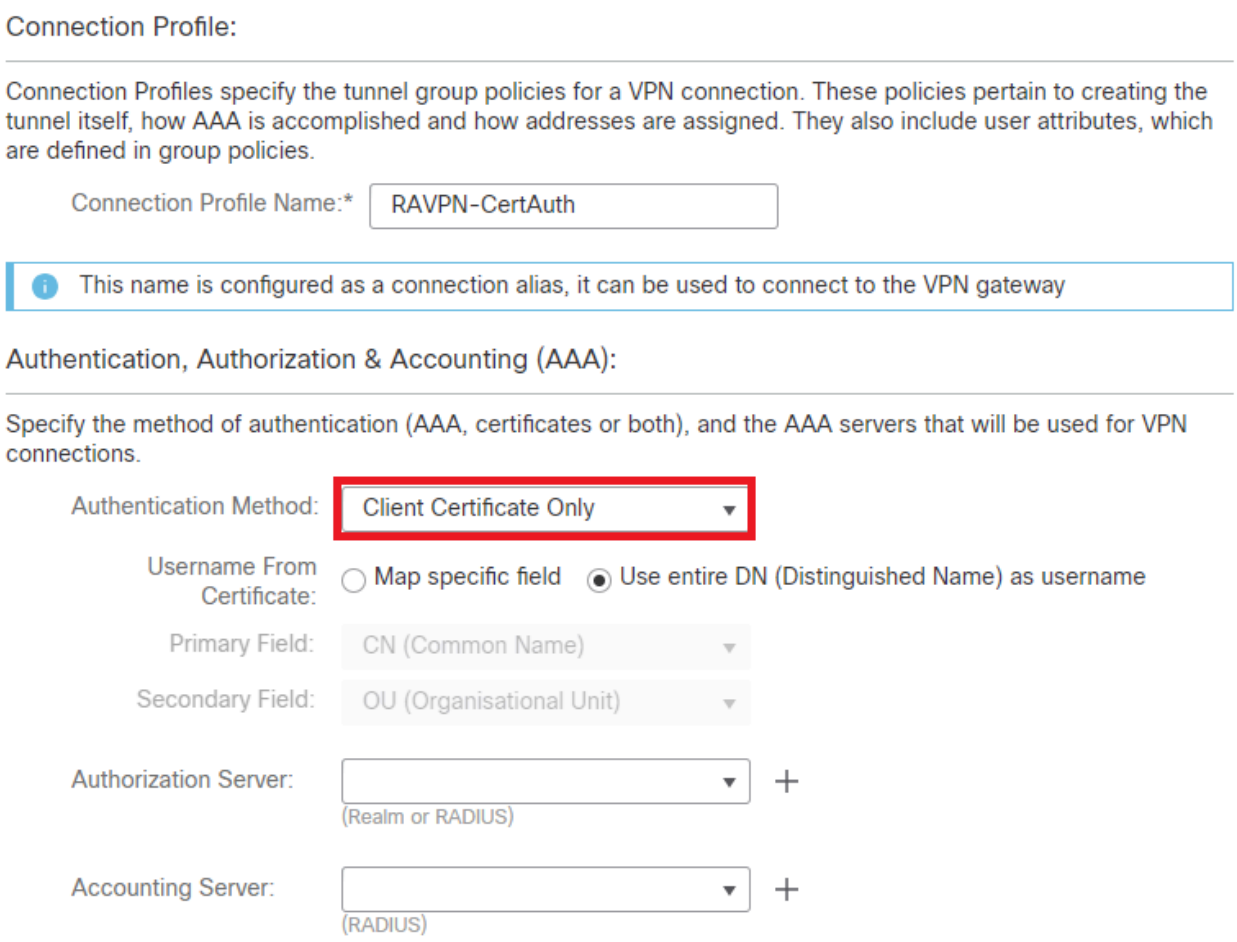
Paso 2. Desplácese hasta Devices > VPN > Remote Access y haga clic en Add.

Paso 3. Introduzca el nombre del perfil, seleccione el dispositivo FTD y haga clic en Next (Siguiente).



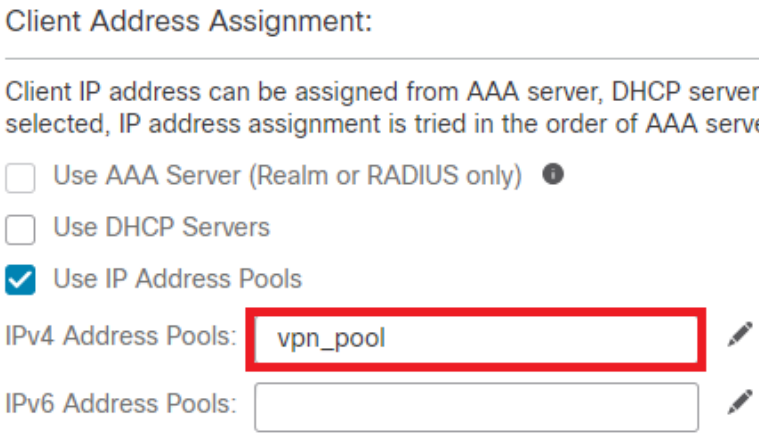
Agregar nombre de perfil

Paso 4. Introduzca el Connection Profile Namey seleccione el método de autenticación como Client Certificate Only en Autenticación, autorización y contabilidad (AAA).



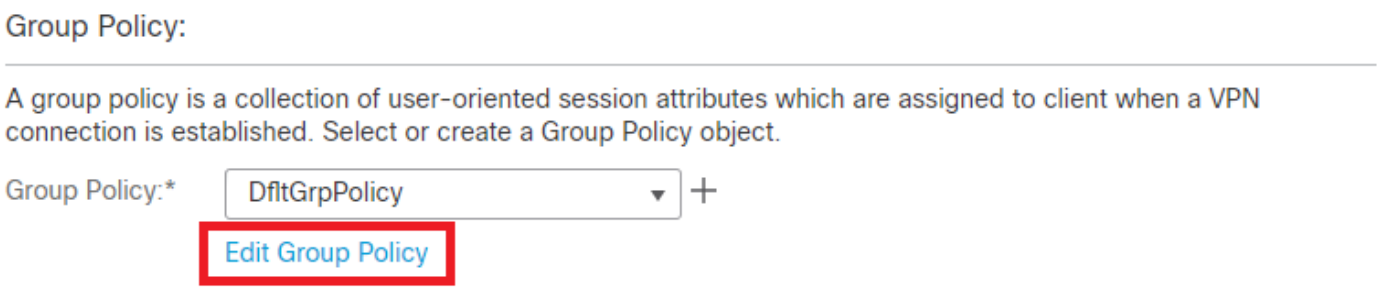
Seleccionar método de autenticación

Paso 5. Haga clic Use IP Address Pools en Asignación de dirección de cliente y seleccione el pool de direcciones IPv4 creado anteriormente.



Seleccionar asignación de dirección de cliente

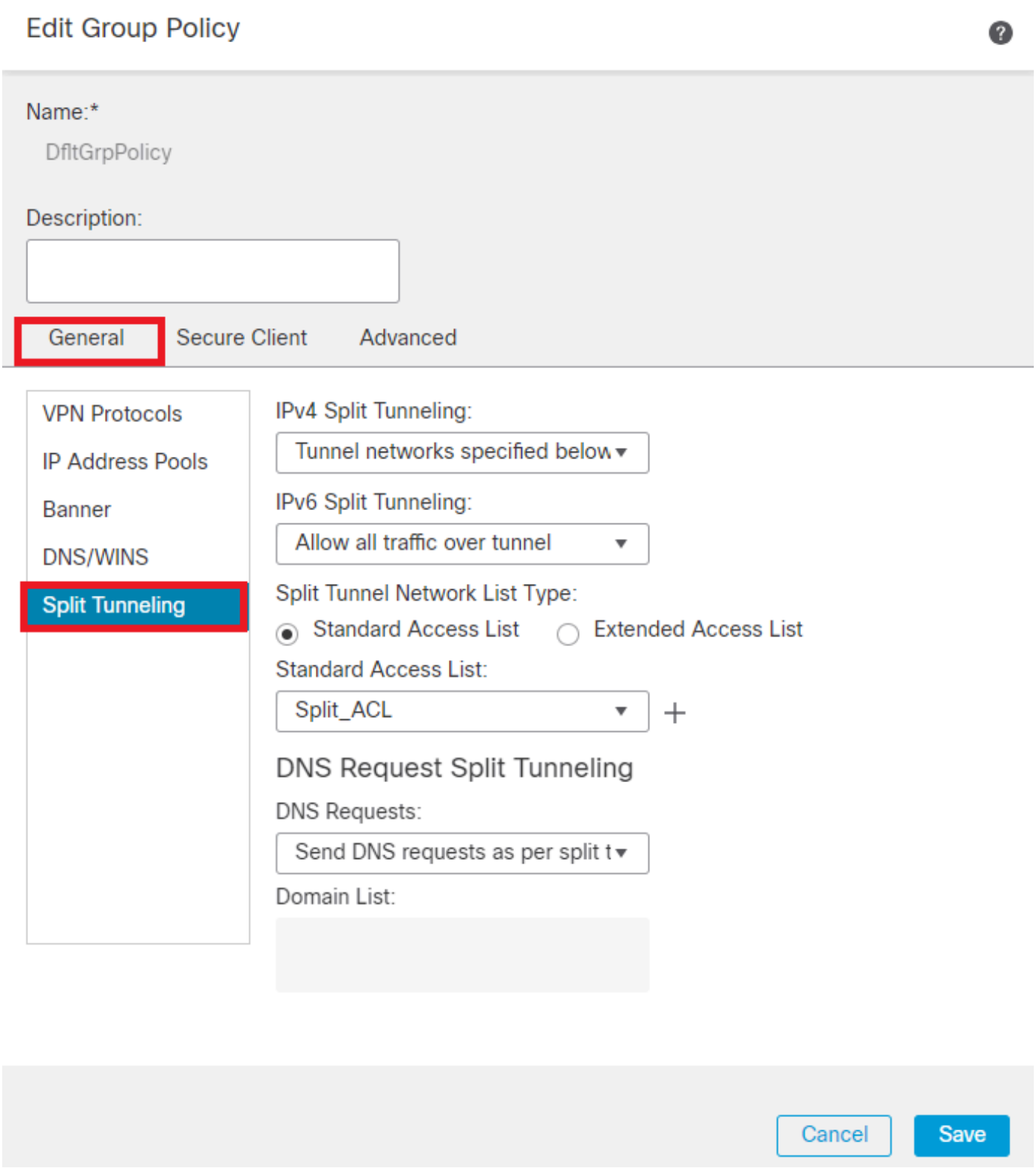
Paso 6. Edite la directiva de grupo.



Editar directiva de grupo

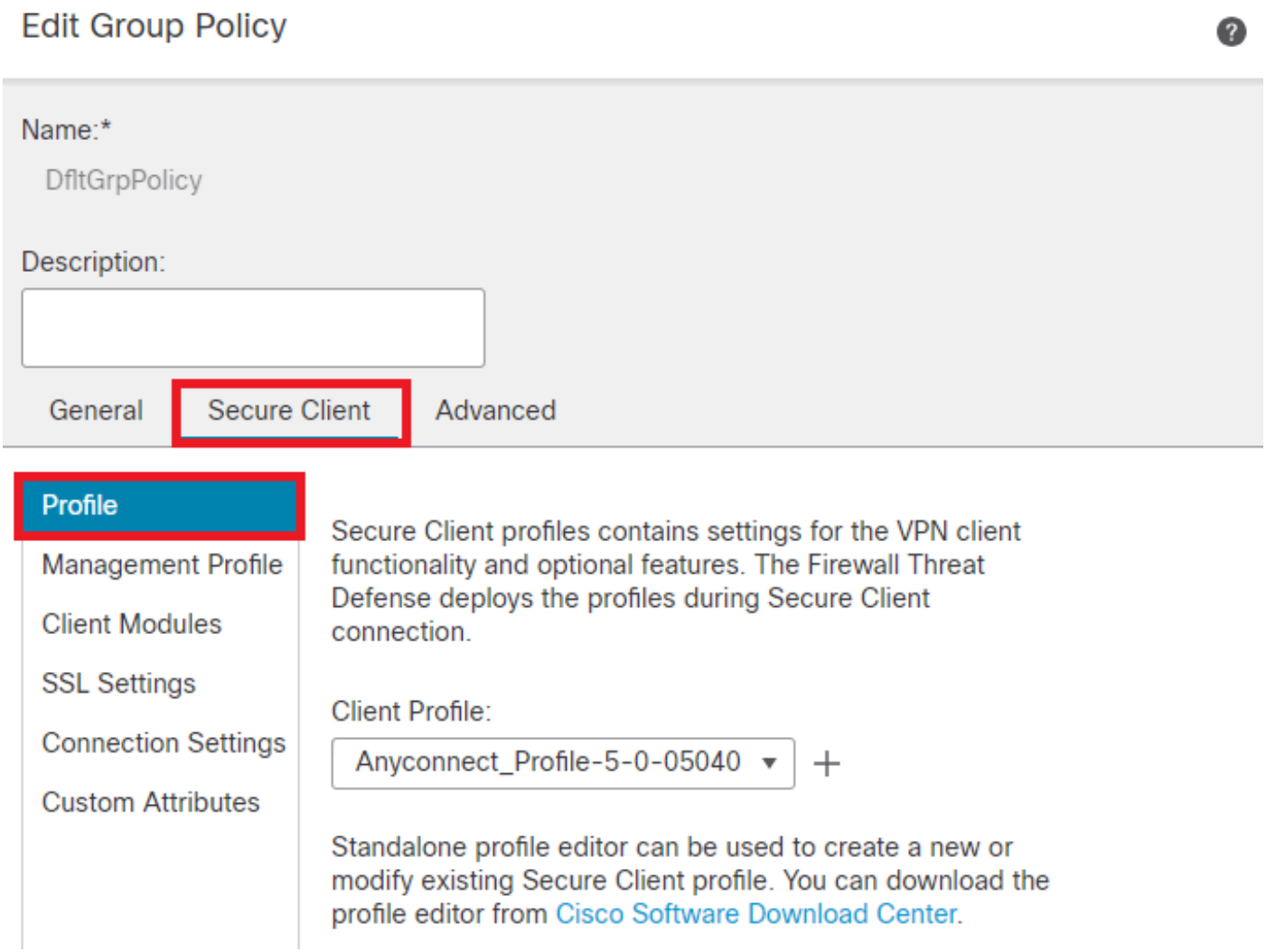
Paso 7. Desplácese hasta General > Split Tunneling , seleccione Tunnel networks specified below y seleccione Standard Access List en Tipo de lista de red de túnel dividido.

Seleccione la ACL creada anteriormente.



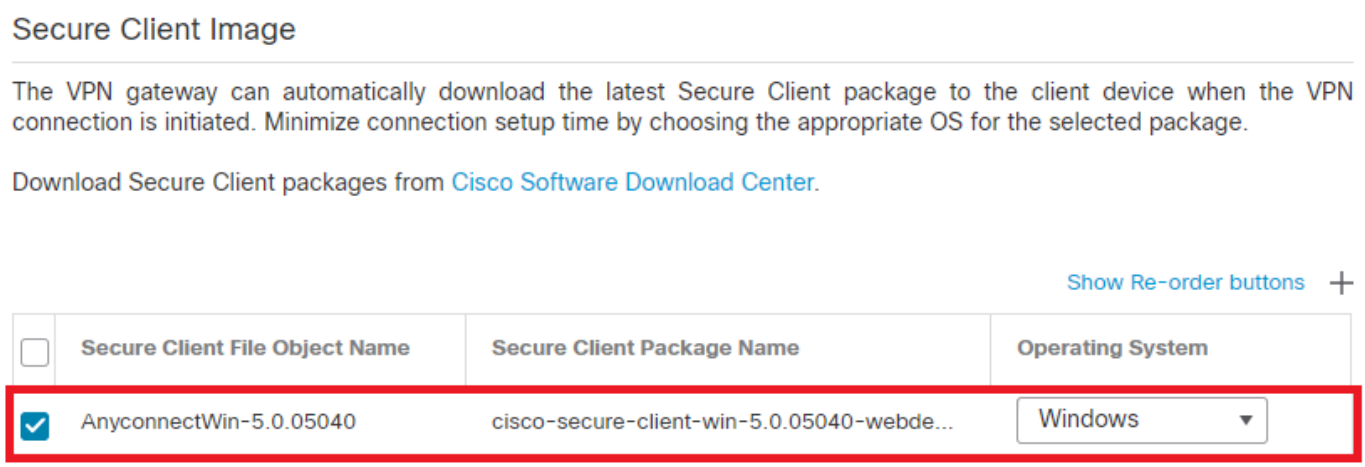
Agregar túnel dividido

Paso 8. Desplácese hasta Secure Client > Profile , seleccione el Client Profile y haga clic en Save.



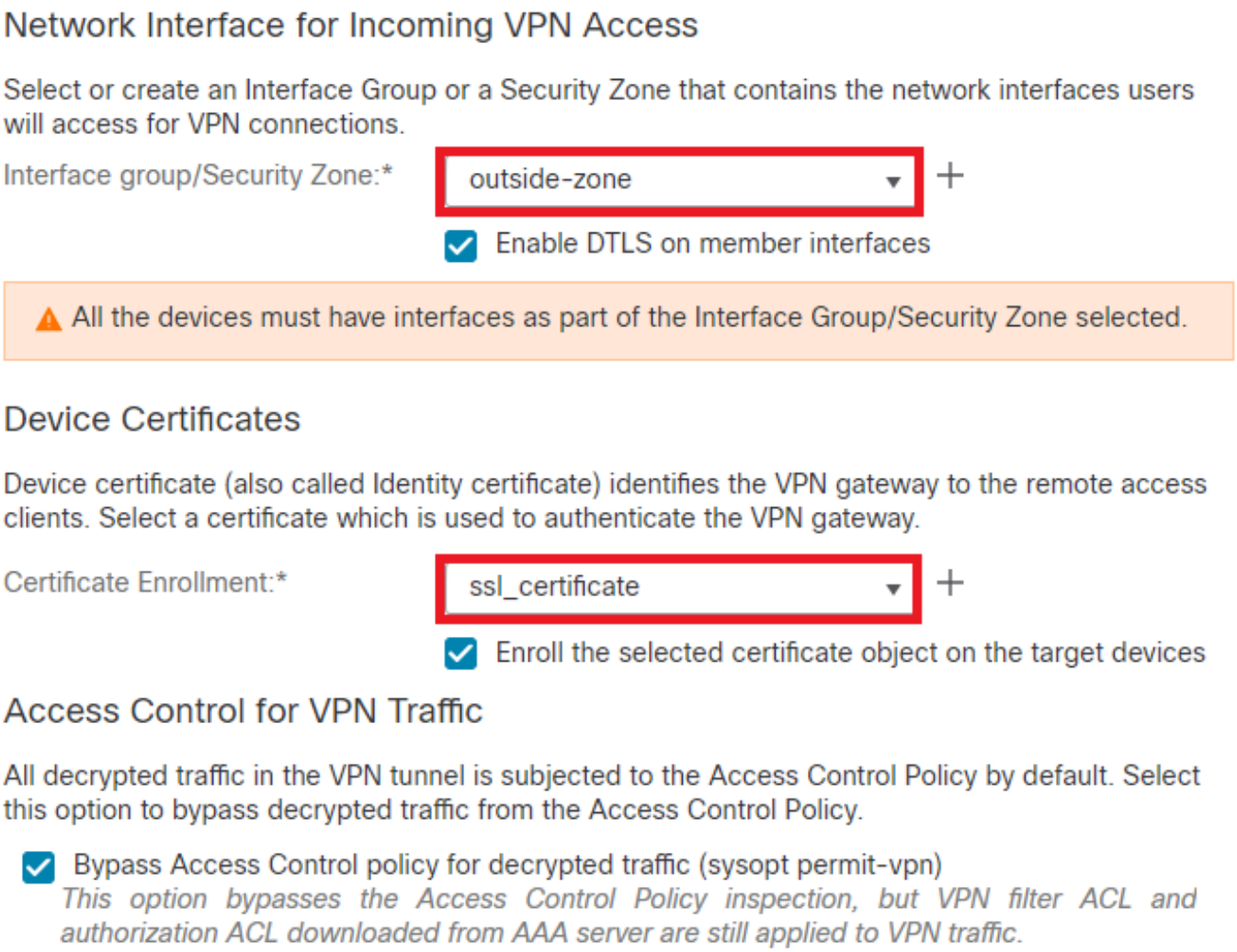
Agregar perfil de cliente seguro

Paso 9. Haga clic en Next, seleccione el Secure Client Image y haga clic en Next.



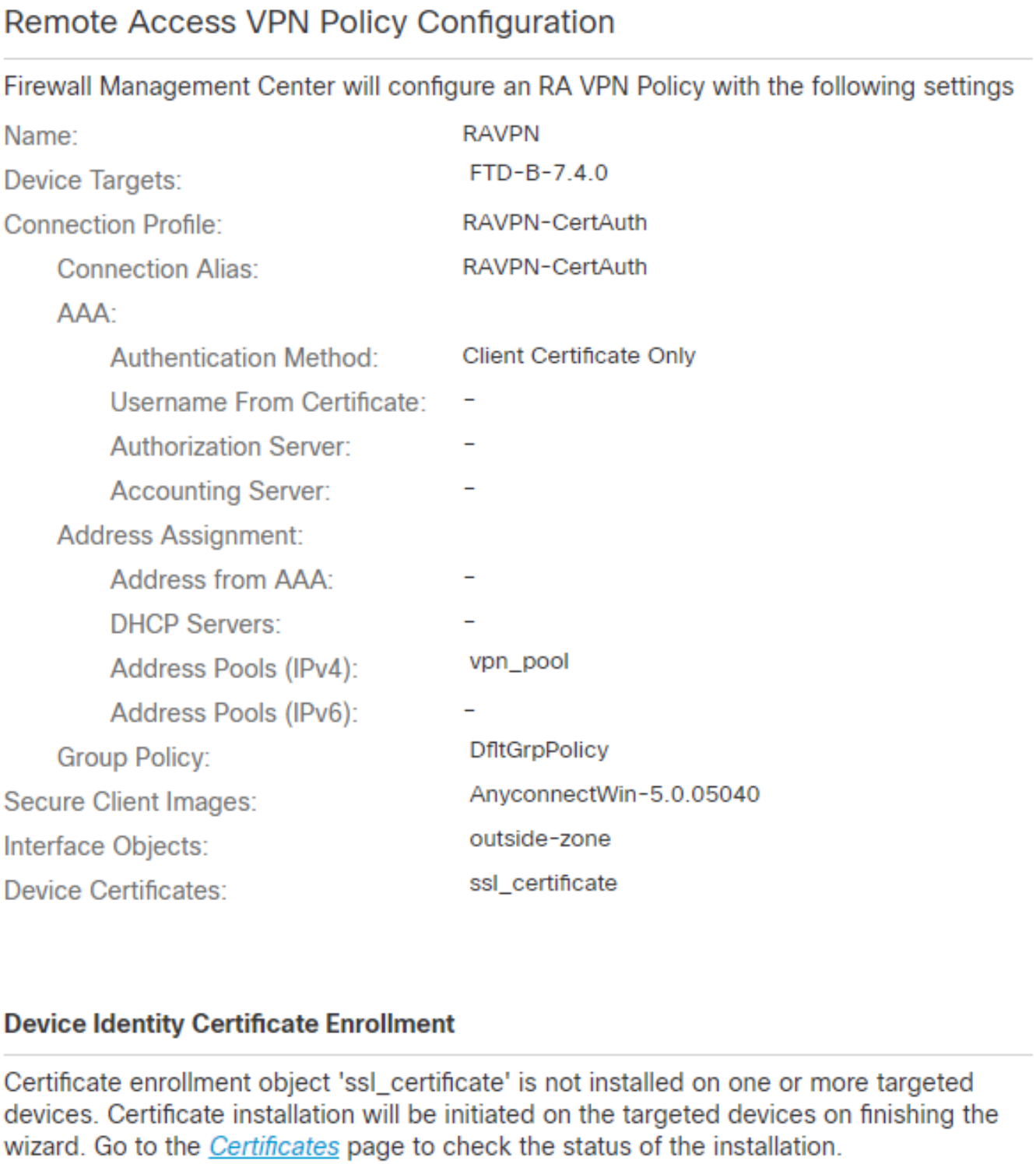
Agregar imagen de cliente seguro

Paso 10. Seleccione la interfaz de red para el acceso VPN, elija el Device Certificates y marque sysopt permit-vpn y haga clic en Next.



Agregar control de acceso para tráfico VPN

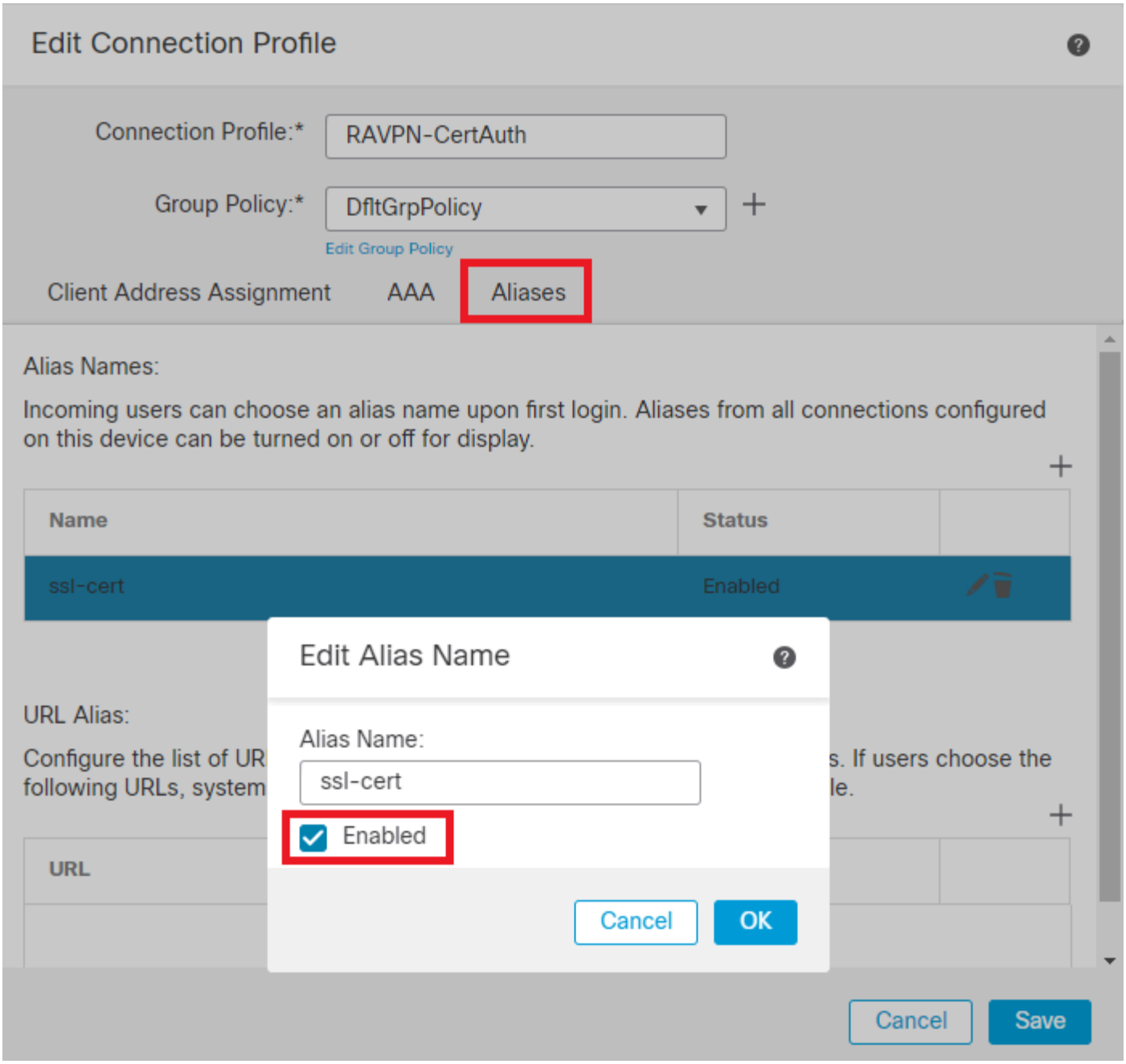
Paso 11. Por último, revise todas las configuraciones y haga clic en Finish.



Configuración de la directiva VPN de acceso remoto

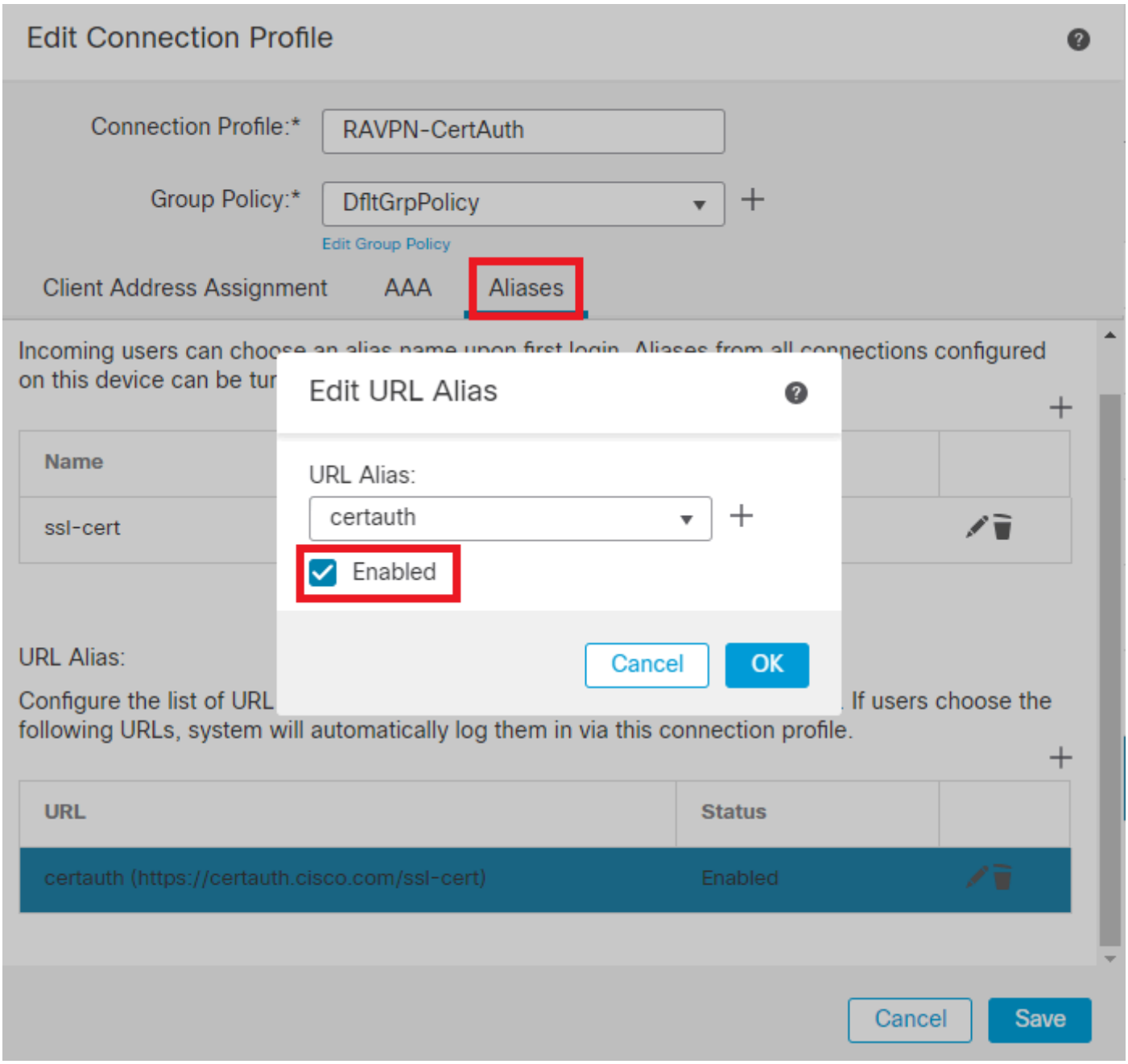
Paso 12. Una vez finalizada la configuración inicial de la VPN de acceso remoto, edite el perfil de conexión creado y vaya a Aliases.

Paso 13. Configure group-alias haciendo clic en el icono más (+).



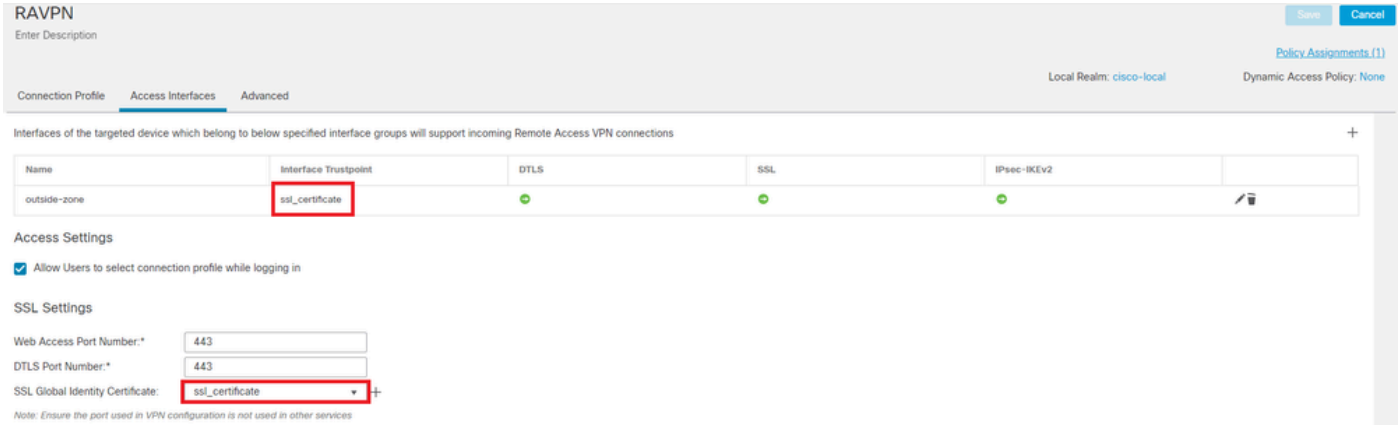
Editar alias de grupo

Paso 14. Configure group-url haciendo clic en el icono más (+). Utilice la misma URL de grupo configurada anteriormente en el perfil de cliente.



Editar URL de grupo

Paso 15. Vaya a Interfaces de acceso. Seleccione Interface Truspoint y SSL Global Identity Certificateen la configuración de SSL.



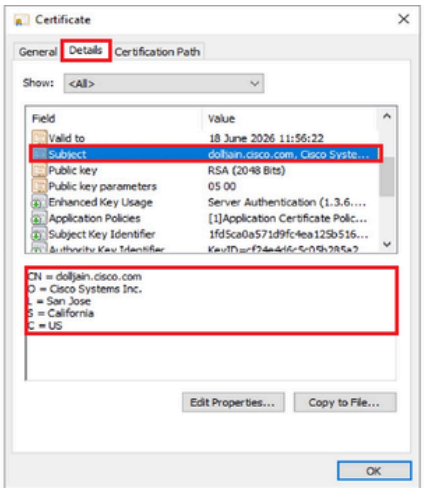
Editar interfaces de acceso

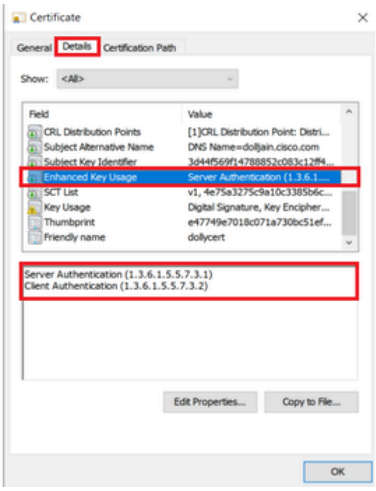
Paso 16. HagaSave clic e implemente estos cambios.

Verificación

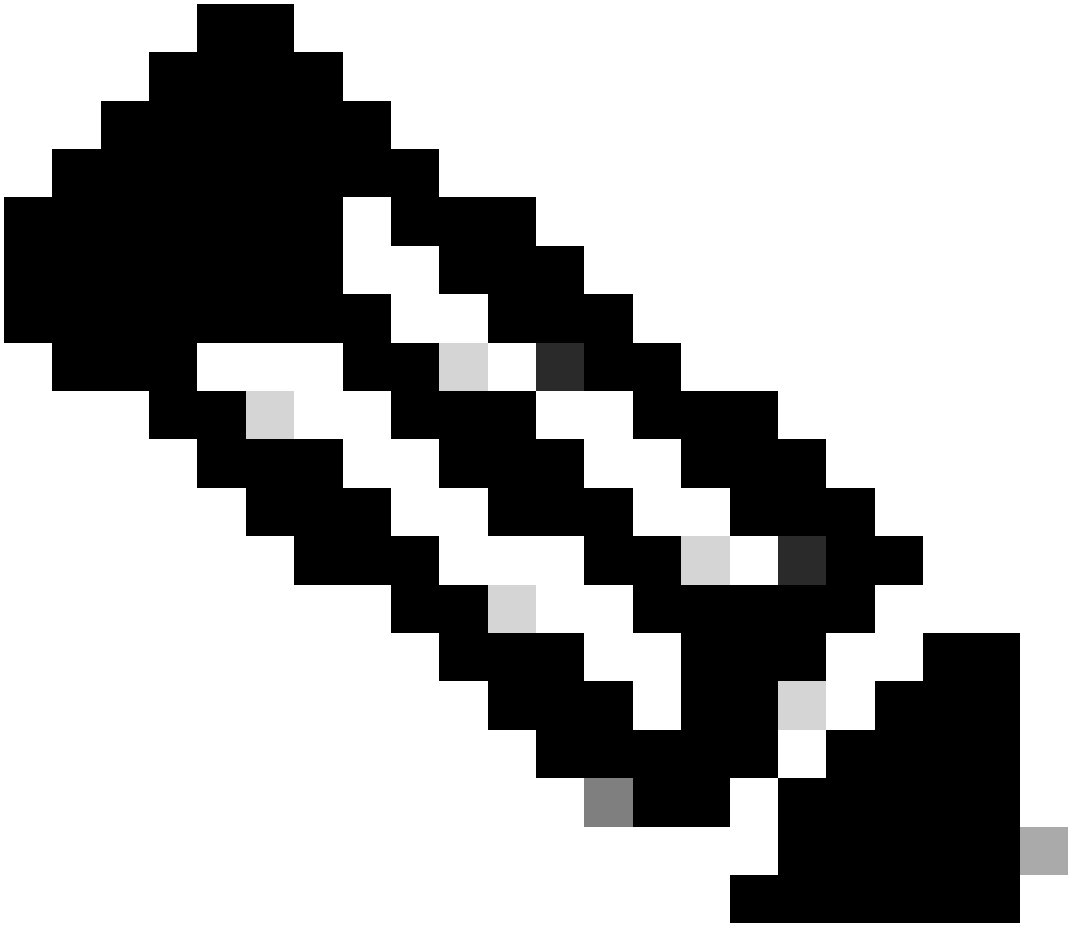
Utilize esta sección para confirmar que su configuración funcione correctamente.

1. El equipo cliente seguro debe tener el certificado instalado con una fecha, asunto y EKU válidos en el equipo del usuario. Este certificado debe ser emitido por la CA cuyo certificado esté instalado en FTD, como se muestra anteriormente. Aquí, la identidad o el certificado de usuario es emitido por "auth-risaggar-ca".



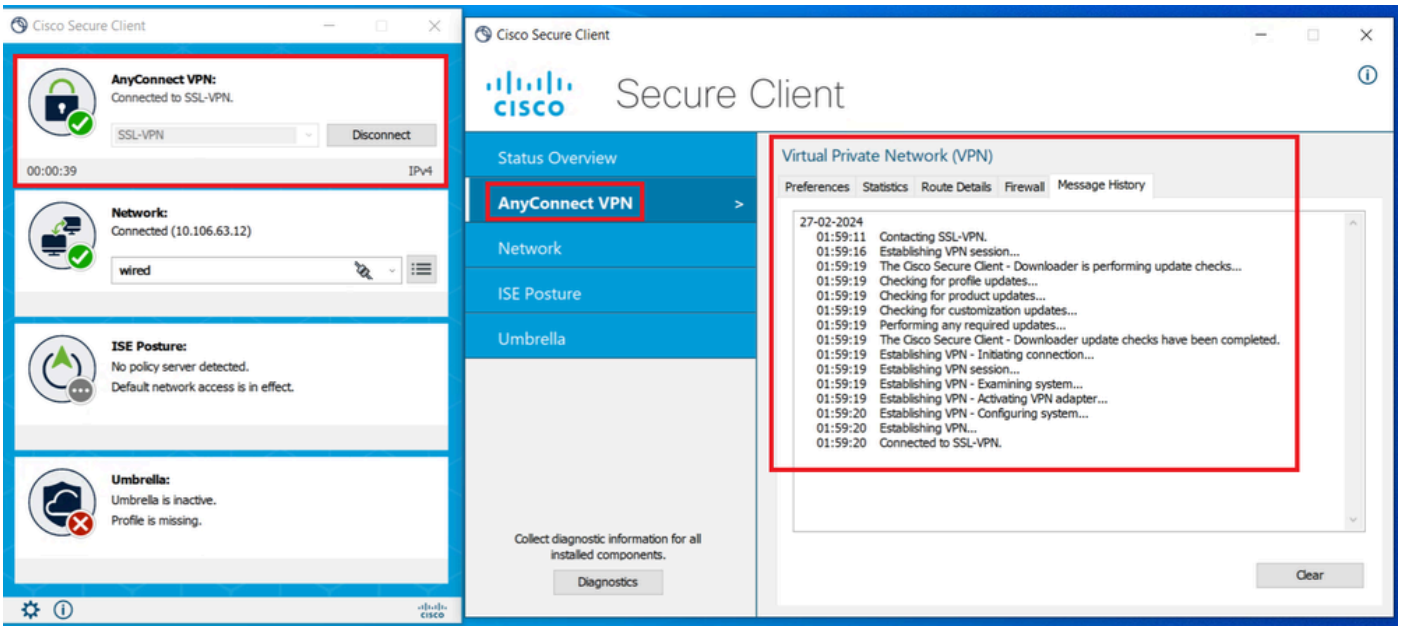


Características del certificado



Nota: el certificado de cliente debe tener el uso mejorado de claves (EKU) de "autenticación de cliente".

2. Secure Client debe establecer la conexión.



Conexión de cliente segura correcta

3. Ejecute show vpn-sessiondb anyconnect para confirmar los detalles de conexión del usuario activo en el grupo de túnel utilizado.

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

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

1. Las depuraciones se pueden ejecutar desde la CLI de diagnóstico del FTD:

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

2. Consulte esta guía para obtener información sobre problemas comunes.

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).