

Configuración de VPN Client 3.x para Obtener un Certificado Digital

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configure el cliente VPN](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

[Introducción](#)

Este documento muestra cómo configurar el Cisco VPN Client 3.x para conseguir un certificado digital.

[Prerequisites](#)

[Requirements](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

La información de este documento se basa en una PC que ejecuta Cisco VPN Client 3.x.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

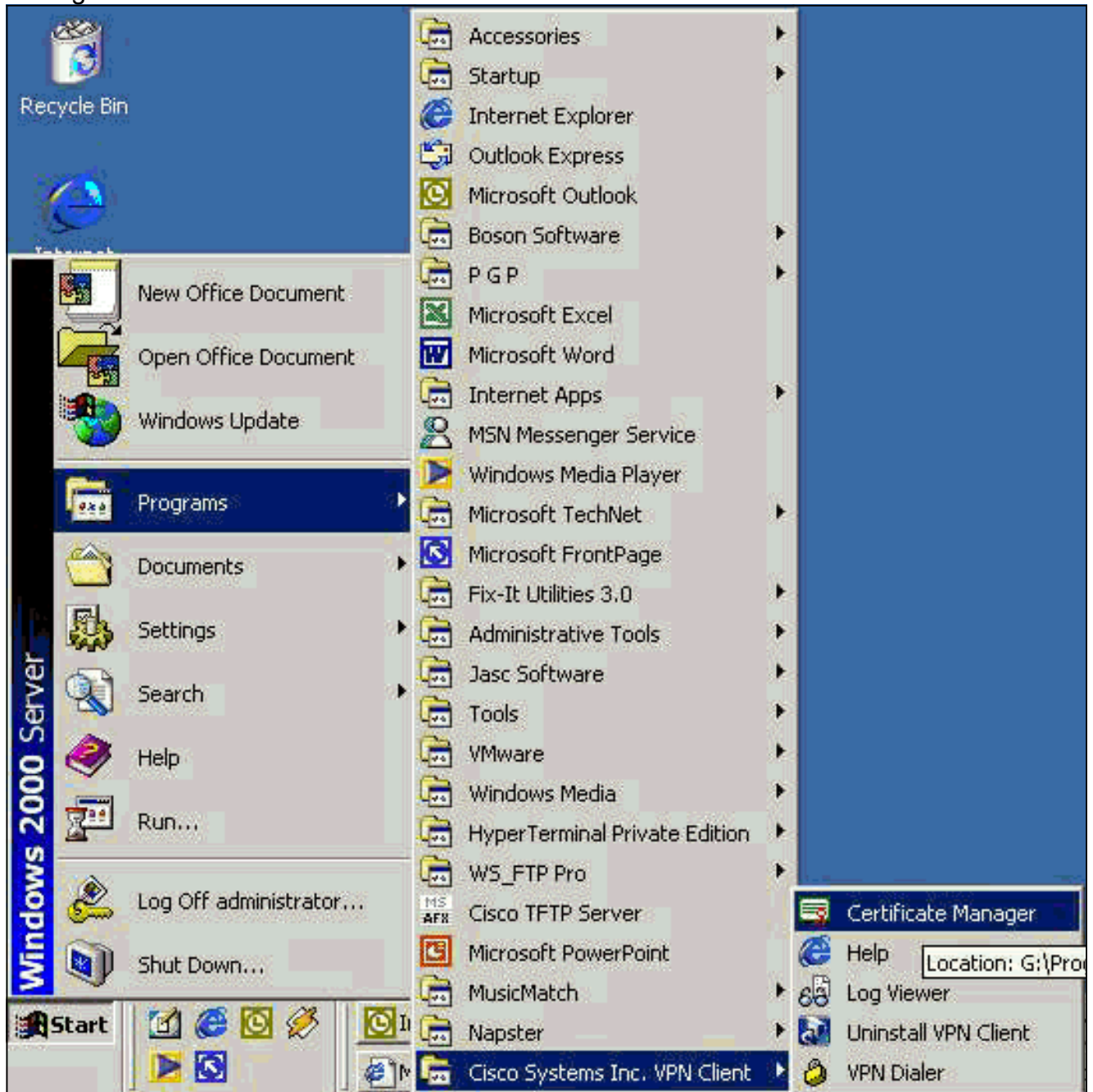
[Convenciones](#)

Consulte [Convenciones de Consejos Técnicos Cisco para obtener más información sobre las convenciones del documento.](#)

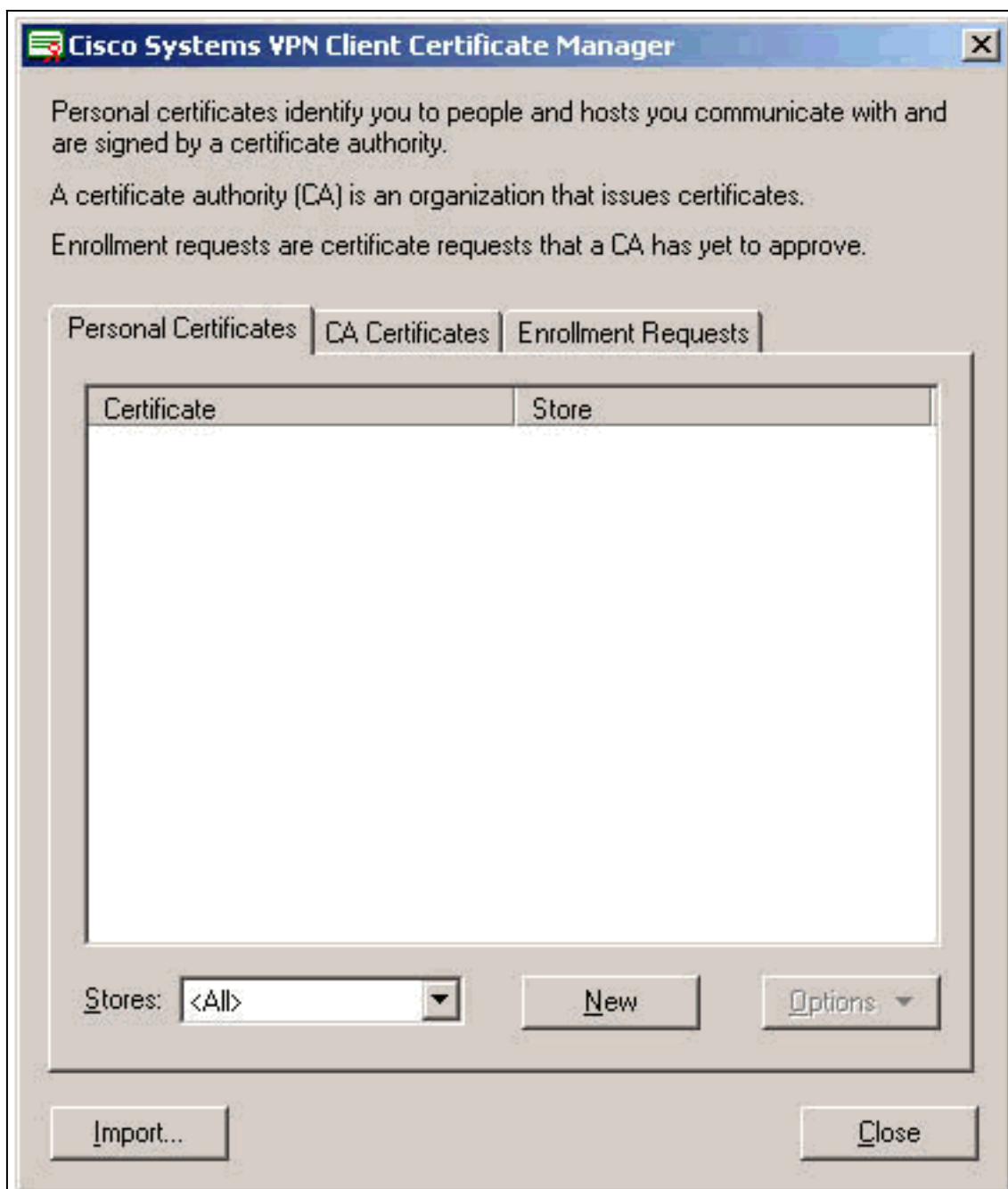
[Configure el cliente VPN](#)

Complete estos pasos para configurar el VPN Client.

1. Seleccione **Inicio > Programas > Cisco Systems Inc. VPN client > Administrador de certificados** para iniciar VPN Client Certificate Manager.



2. Seleccione la ficha **Certificados personales** y haga clic en



Nuevo.

Nota:

Los certificados de equipo para autenticar usuarios para conexiones VPN no se pueden realizar con IPsec.

3. Cuando el cliente VPN le pida una contraseña, especifique una contraseña para proteger el certificado. Cualquier operación que requiera acceso a la clave privada del certificado requiere la contraseña especificada para

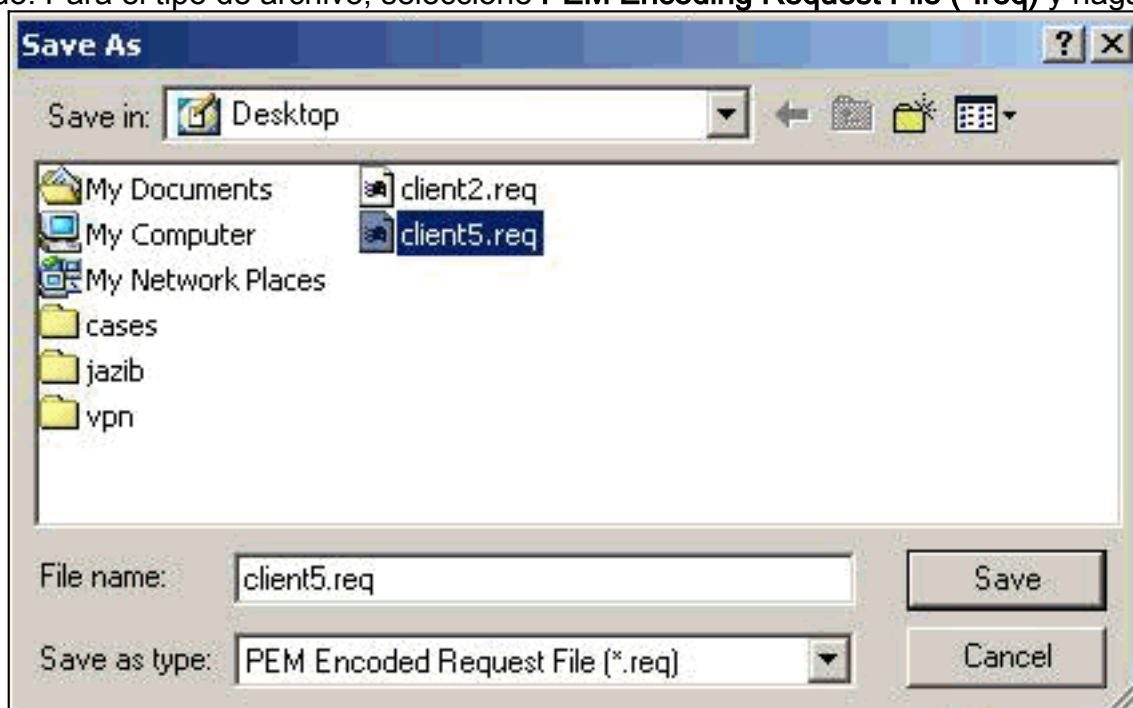


continuar.

4. Seleccione **Archivo** para solicitar un certificado utilizando el formato PKCS #10 en la página Inscripción. Luego haga clic en Next (Siguiete).



5. Haga clic en **Examinar** y especifique un nombre de archivo para el archivo de solicitud de certificado. Para el tipo de archivo, seleccione **PEM Encoding Request File (*.req)** y haga clic



en **Save**.

6. Haga clic en **Next** en la página VPN Client Enrollment.

Enrollment - File Location



To create an enrollment request file, please select the type of file you wish to generate.

Contact your network administrator if you are not sure which encoded file type is required.

When you select a file extension in the Browse dialog the associated file type will be selected on this page.

File name: *

C:\My Documents\client5.req Browse

File type:

Base 64 encoded (.req)

Binary encoded (.p10)


* Required Field

< Back Next > Cancel Help

7. Rellene los campos del formulario de inscripción. Este ejemplo muestra los campos: Nombre común = Usuario1 Departamento = IPSECCERT (debe coincidir con la unidad organizativa (OU) y el nombre del grupo en el concentrador VPN 3000). Empresa = Cisco Systems Estado = Carolina del Norte País = EE. UU. Correo electrónico = User1@email.com Dirección IP = (opcional; se utiliza para especificar la dirección IP en la solicitud de certificado) Dominio = cisco.com Haga clic en **Siguiente** cuando haya terminado.

Enrollment - Form [X]

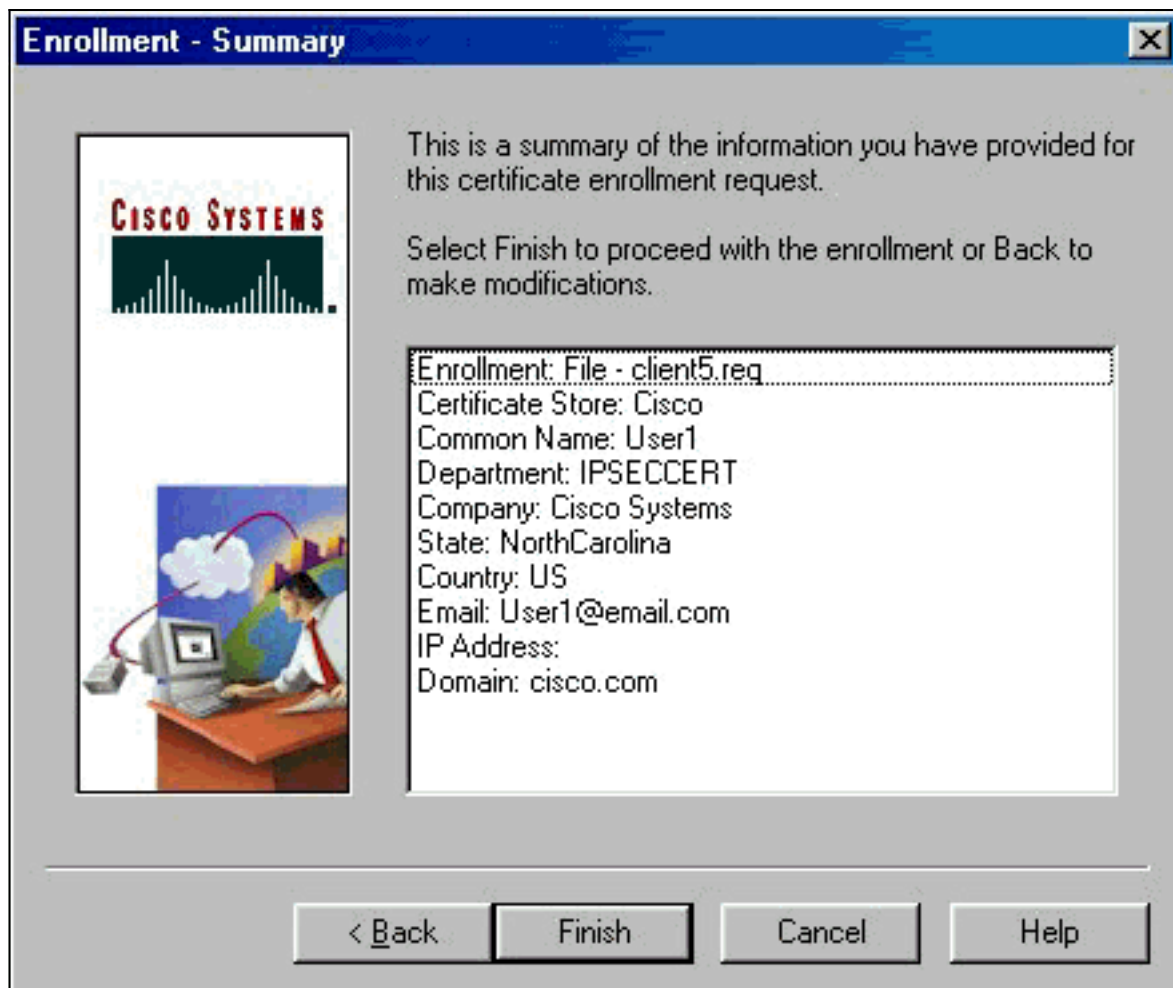
Enter your certificate enrollment information in the fields provided below.

	<u>C</u> ommon Name (cn):*	User1
	<u>D</u> epartment (ou):	IPSECCERT
	<u>C</u> ompany (o):	Cisco Systems
	<u>S</u> tate (st):	NorthCarolina
	<u>C</u> ountry (c):	US
	<u>E</u> mail (e):	User1@email.com
	<u>I</u> P Address:	
	<u>D</u> omain:	cisco.com

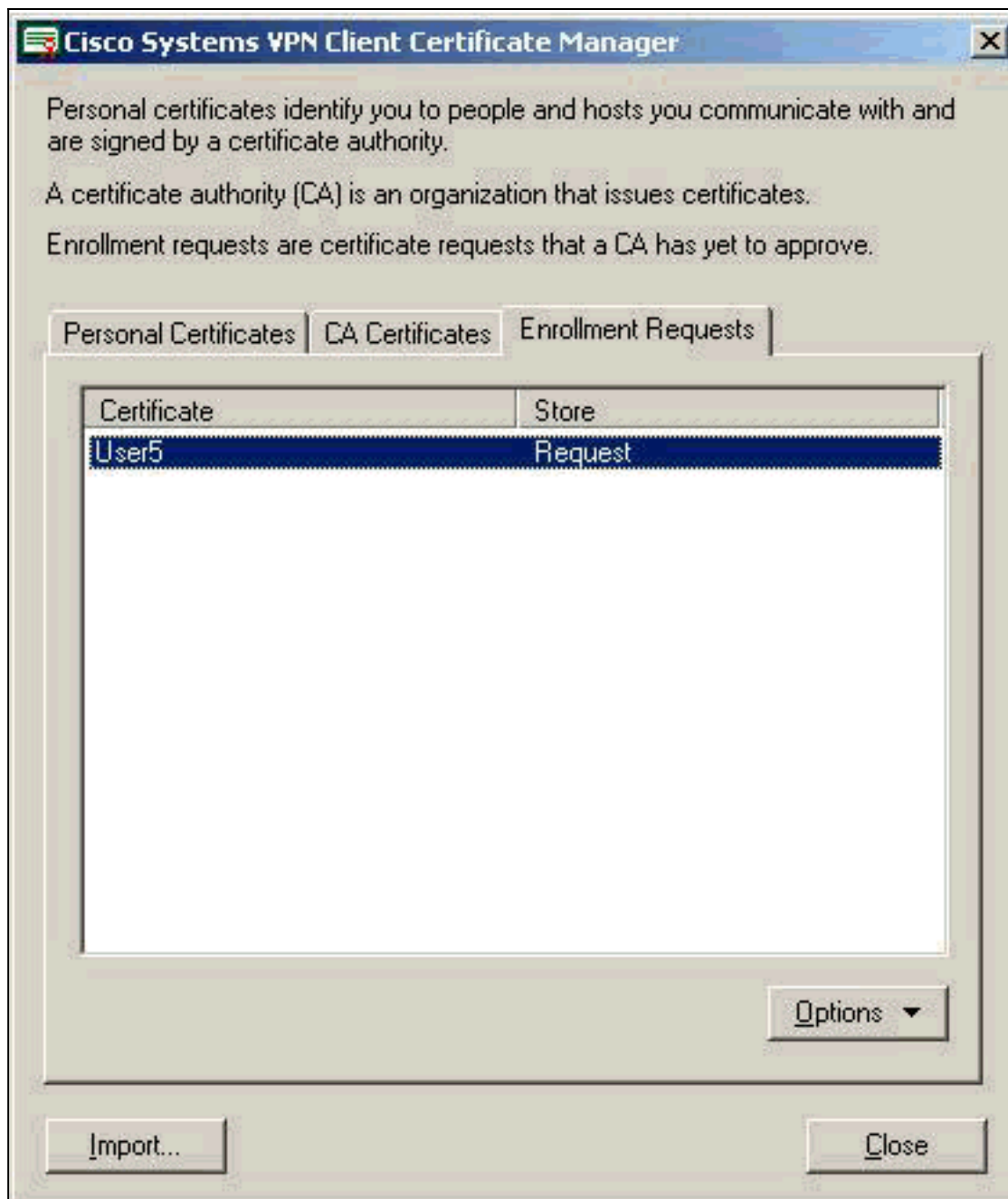
* Required Field

< Back Next > Cancel Help

8. Haga clic en **Finalizar** para continuar con la inscripción.

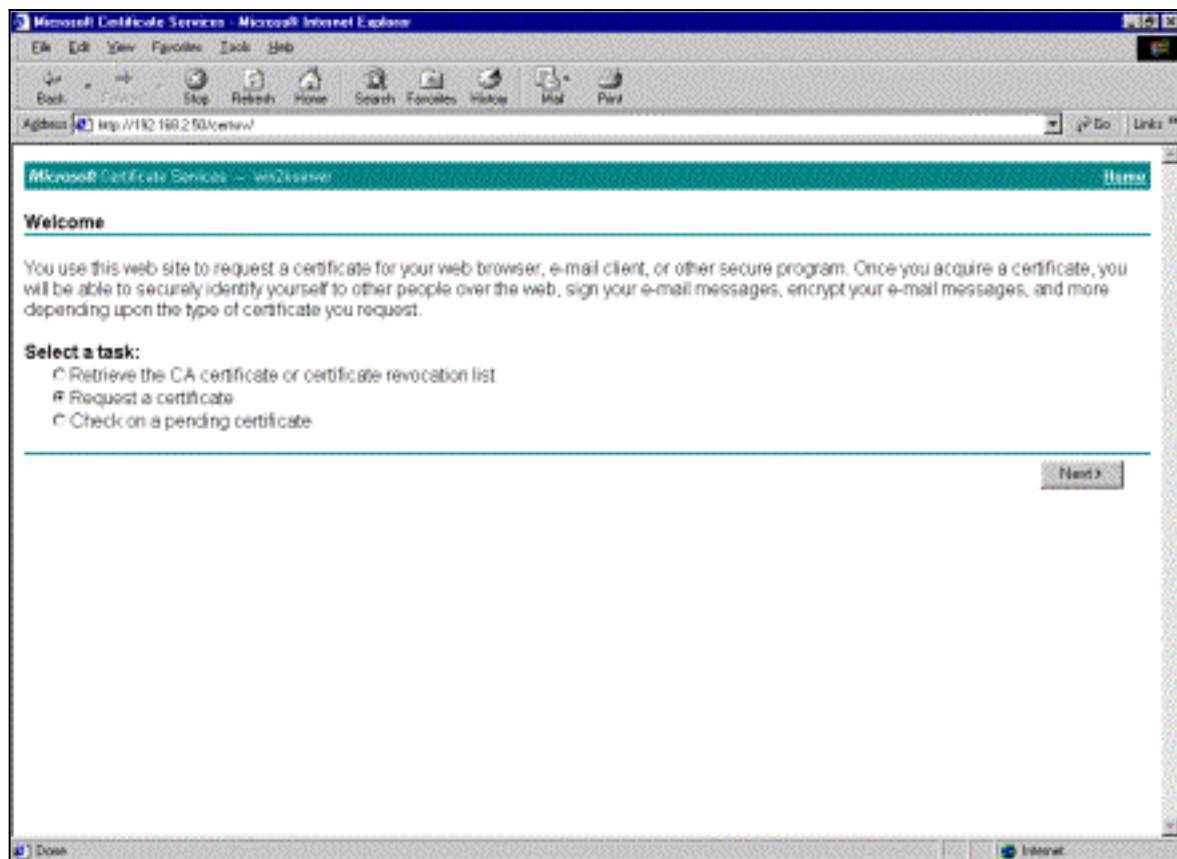


9. Seleccione la pestaña Solicitudes de inscripción para verificar la solicitud en el Administrador de certificados de cliente



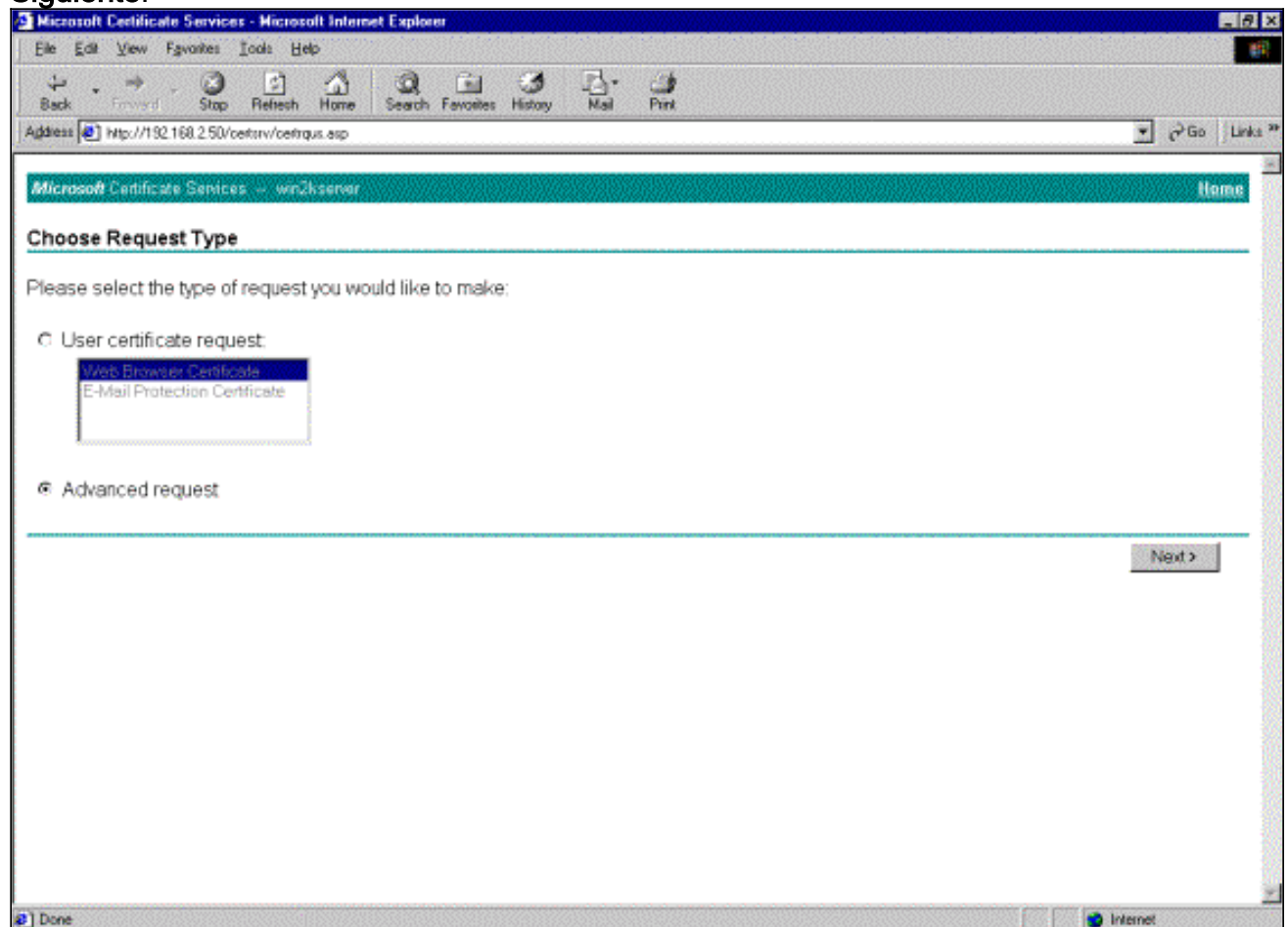
VPN.

10. Active el servidor de la Autoridad de certificación (CA) y las interfaces del cliente VPN simultáneamente para enviar la solicitud.
11. Seleccione **Request a certificate** y haga clic en **Next** en el servidor de la



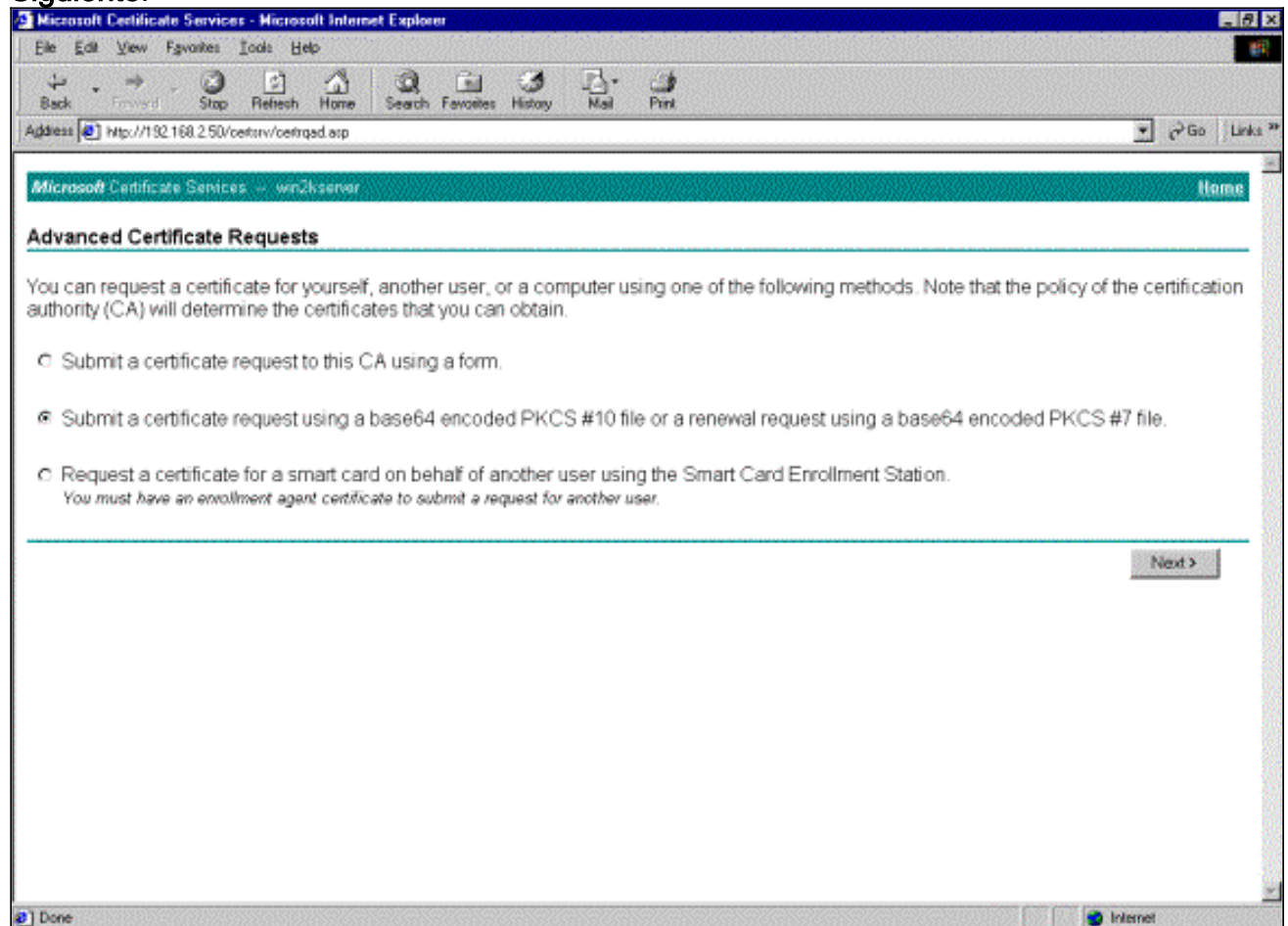
CA.

12. Seleccione **Solicitud avanzada** para el tipo de solicitud y haga clic en **Siguiente**.

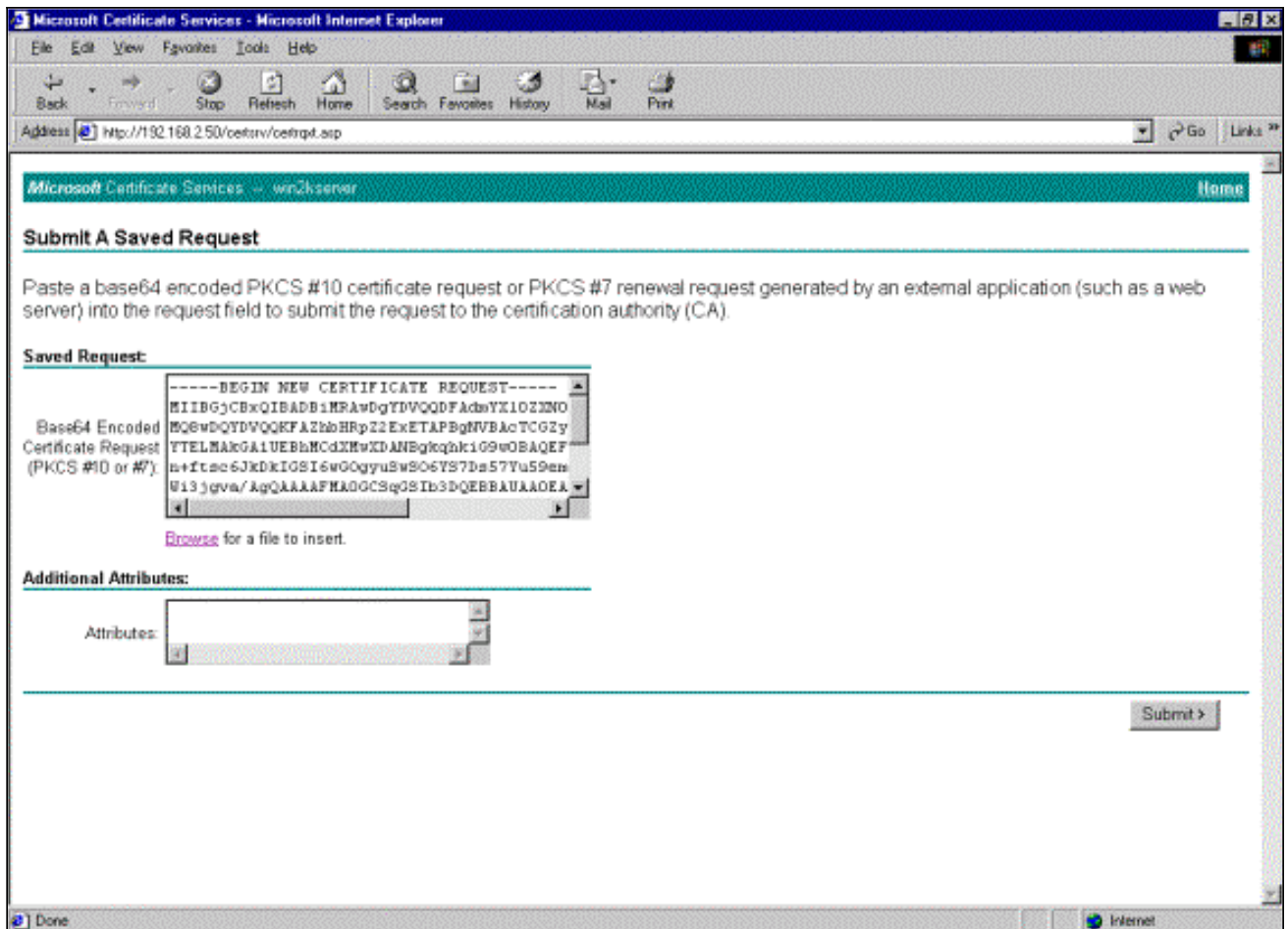


13. Seleccione **Enviar una solicitud de certificado utilizando un archivo PKCS #10 codificado en base64** o una solicitud de renovación utilizando un archivo PKCS #7 codificado en base64 en Solicitudes de certificado avanzadas y, a continuación, haga clic en

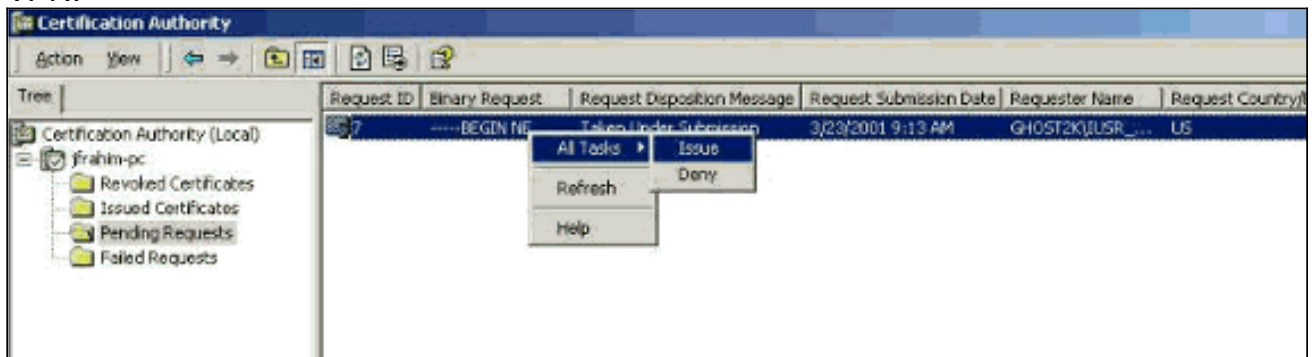
Siguiente.



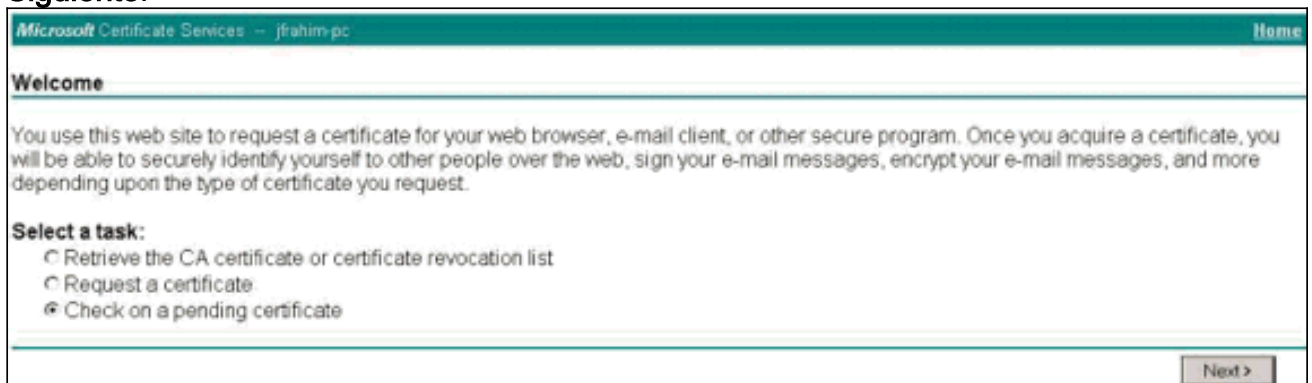
14. Resalte el archivo de solicitud de VPN Client y péguelo en el servidor de la CA bajo Solicitud guardada. A continuación, haga clic en **Enviar**.



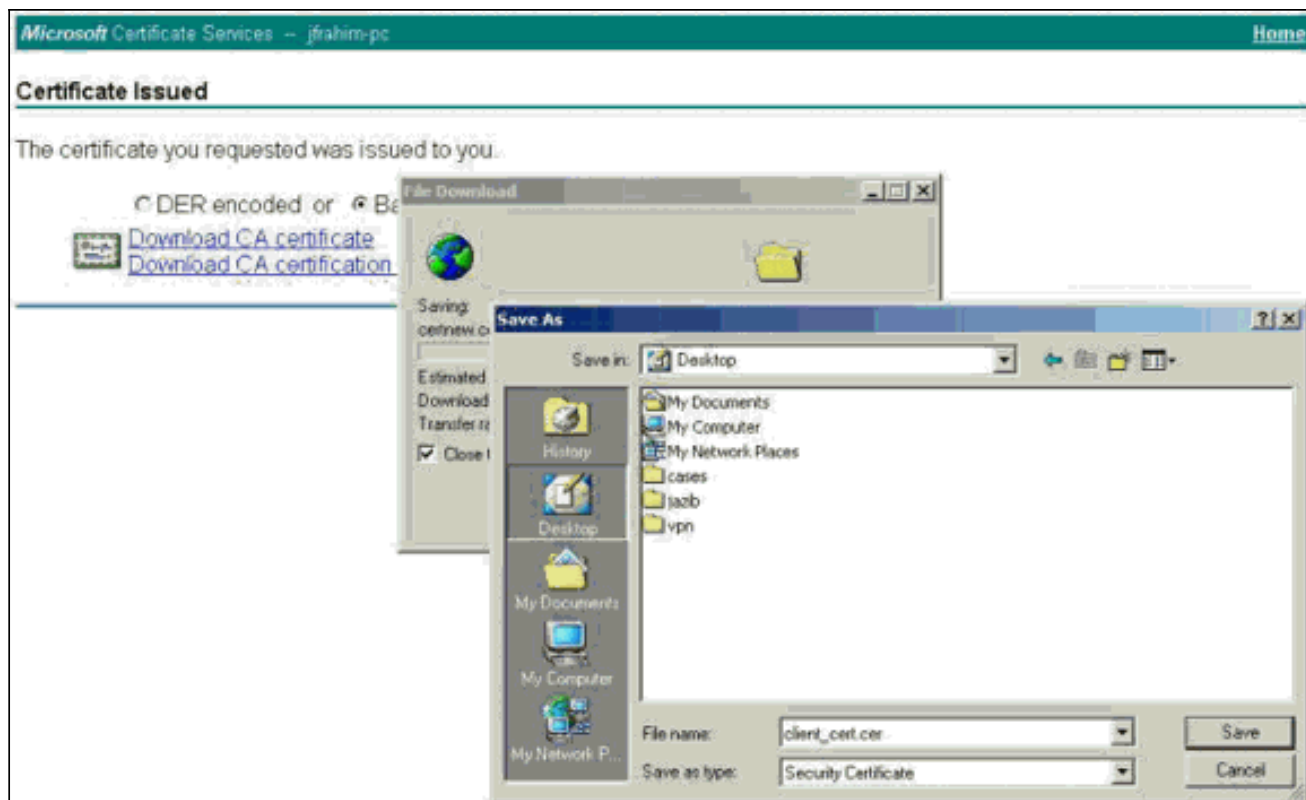
15. En el servidor de la CA, ejecute el certificado de identidad para la solicitud del cliente VPN.



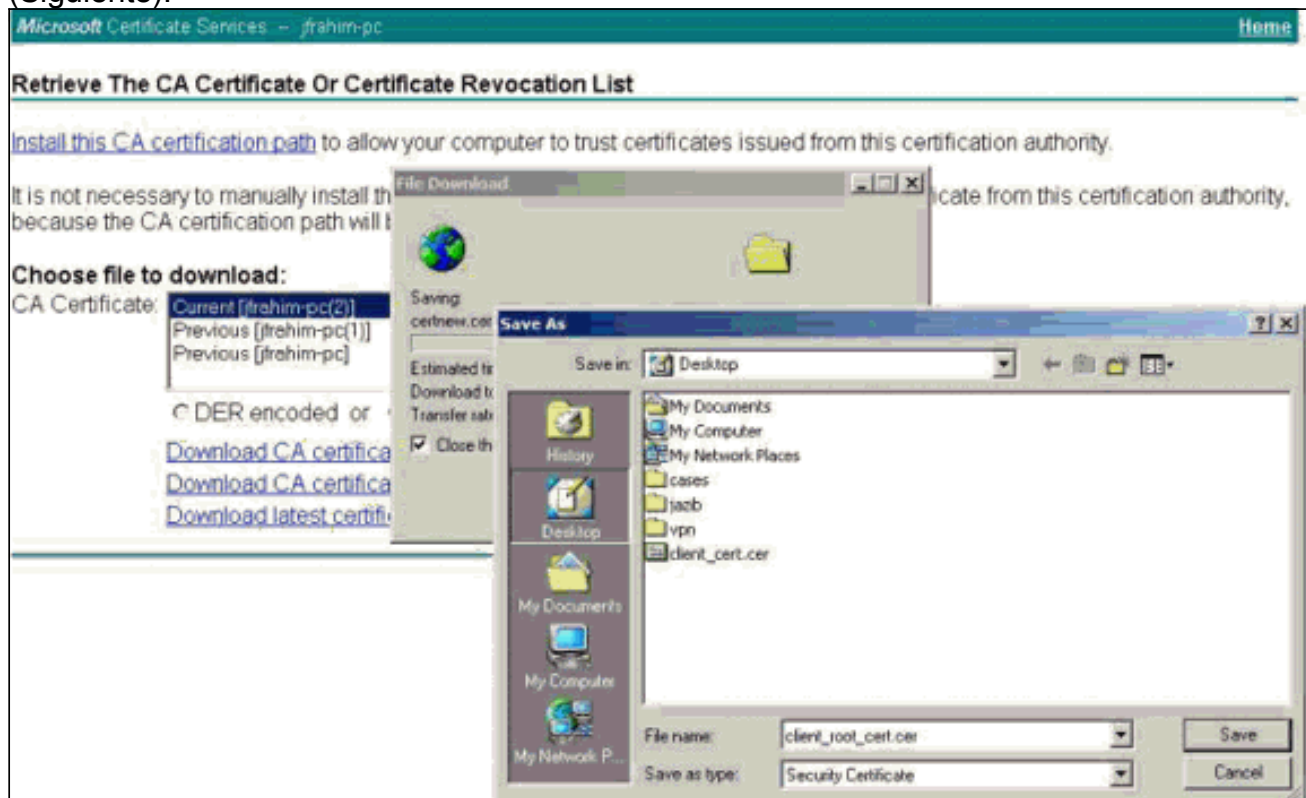
16. Descargue los certificados raíz e identidad al VPN Client. En el servidor de la CA, seleccione **Comprobar un certificado pendiente** y, a continuación, haga clic en **Siguiente**.



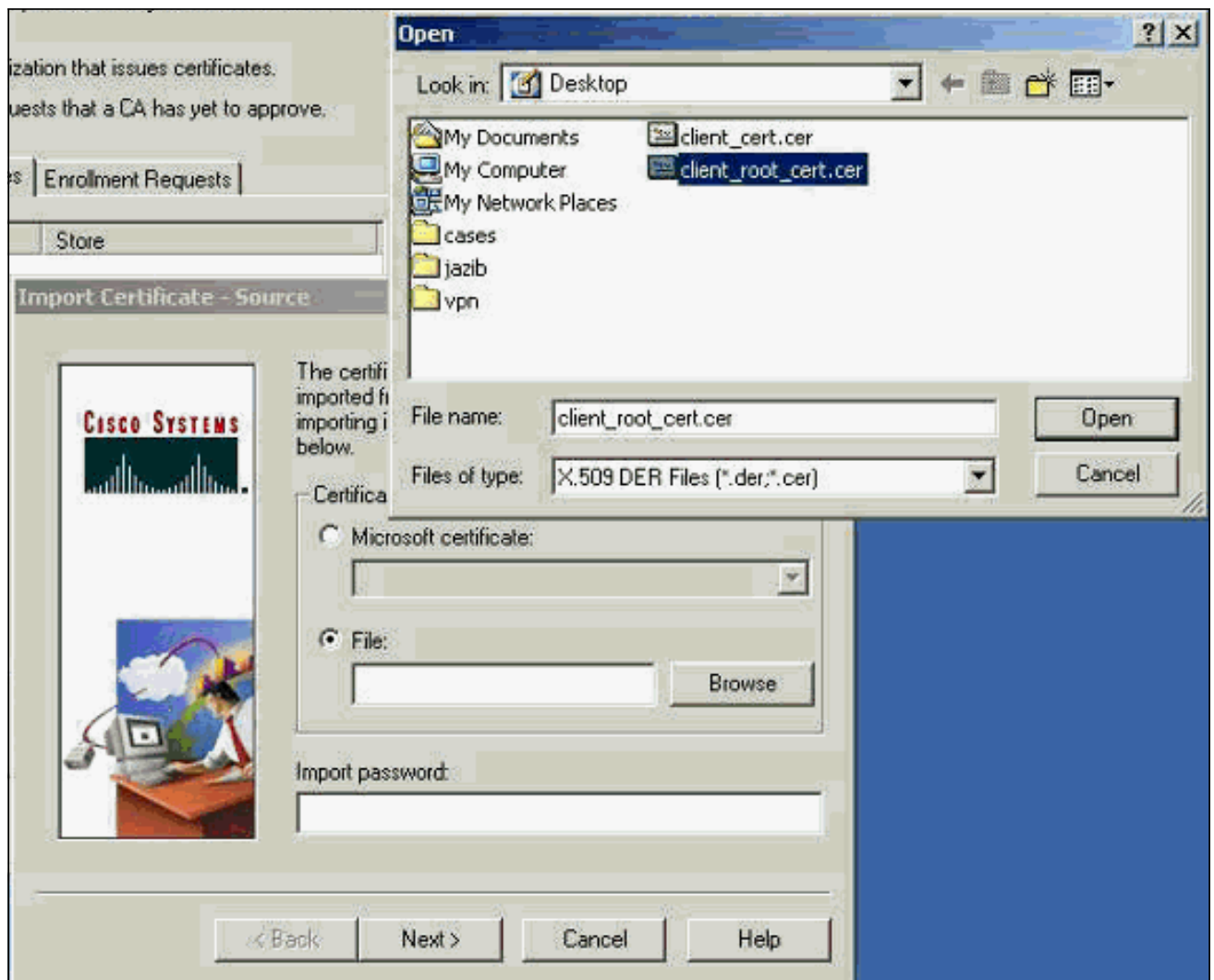
17. Seleccione **Base 64 codificada**. A continuación, haga clic en **Descargar certificado de CA** en el servidor de la CA.



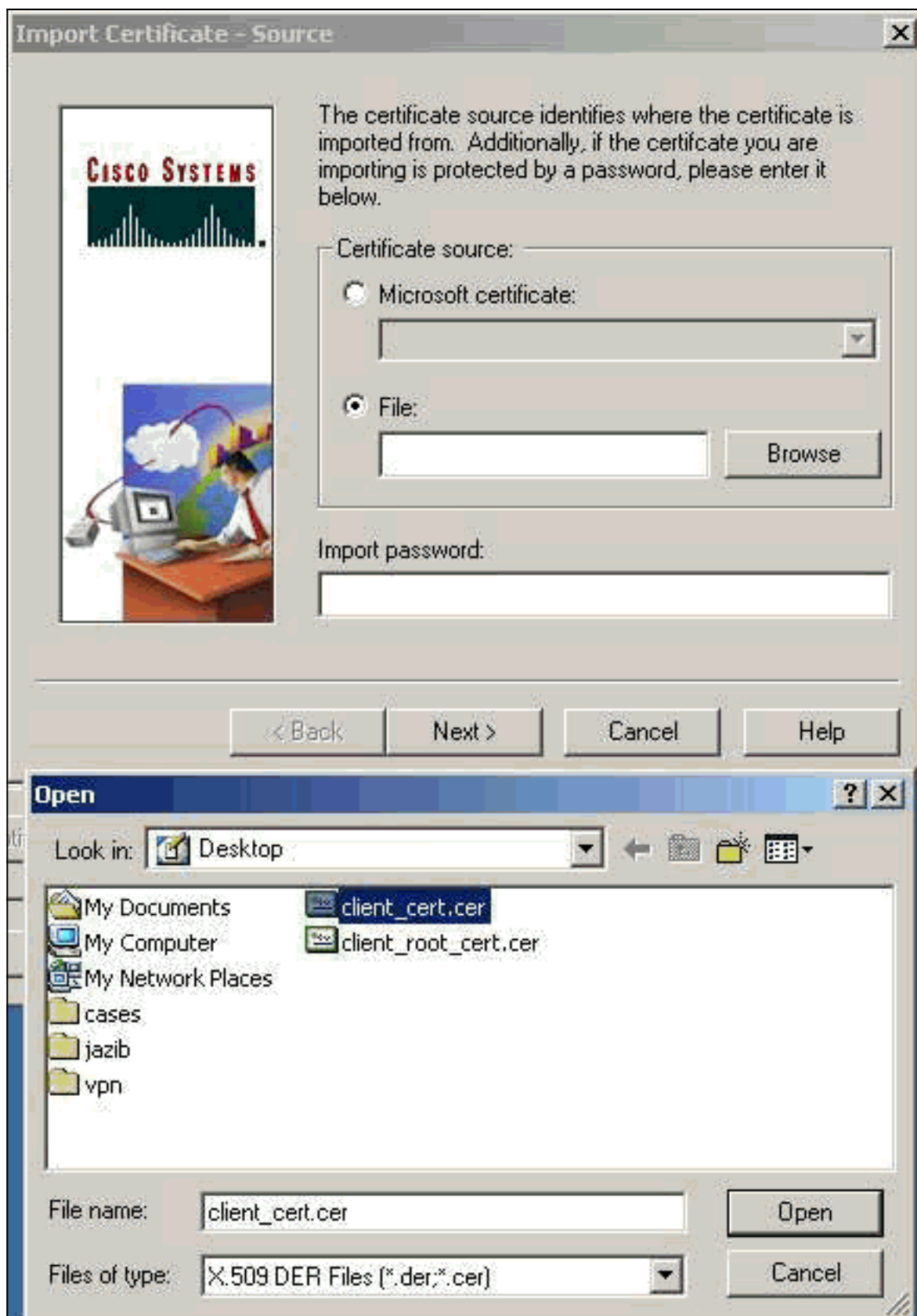
18. Seleccione un archivo para descargar de la página Recuperar el certificado de la CA o Lista de revocación de certificados para obtener el certificado raíz en el servidor de la CA. Luego haga clic en Next (Siguiente).



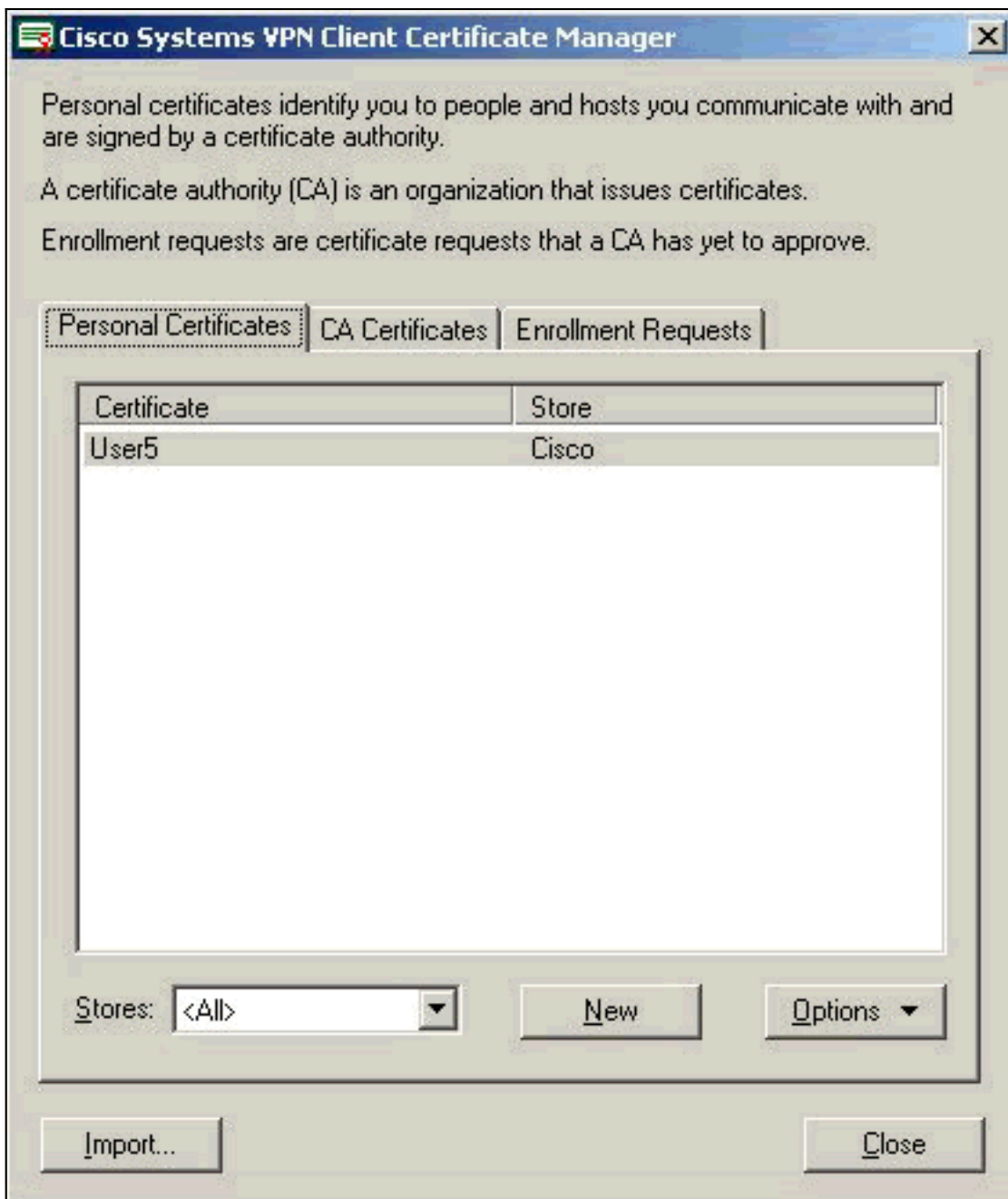
19. Seleccione **Certificate Manager > CA Certificate > Import on the VPN Client** y luego seleccione el archivo raíz CA para instalar los certificados raíz e identidad.



20. Seleccione **Administrador de certificados > Certificados personales > Importar** y elija el archivo de certificado de identidad.

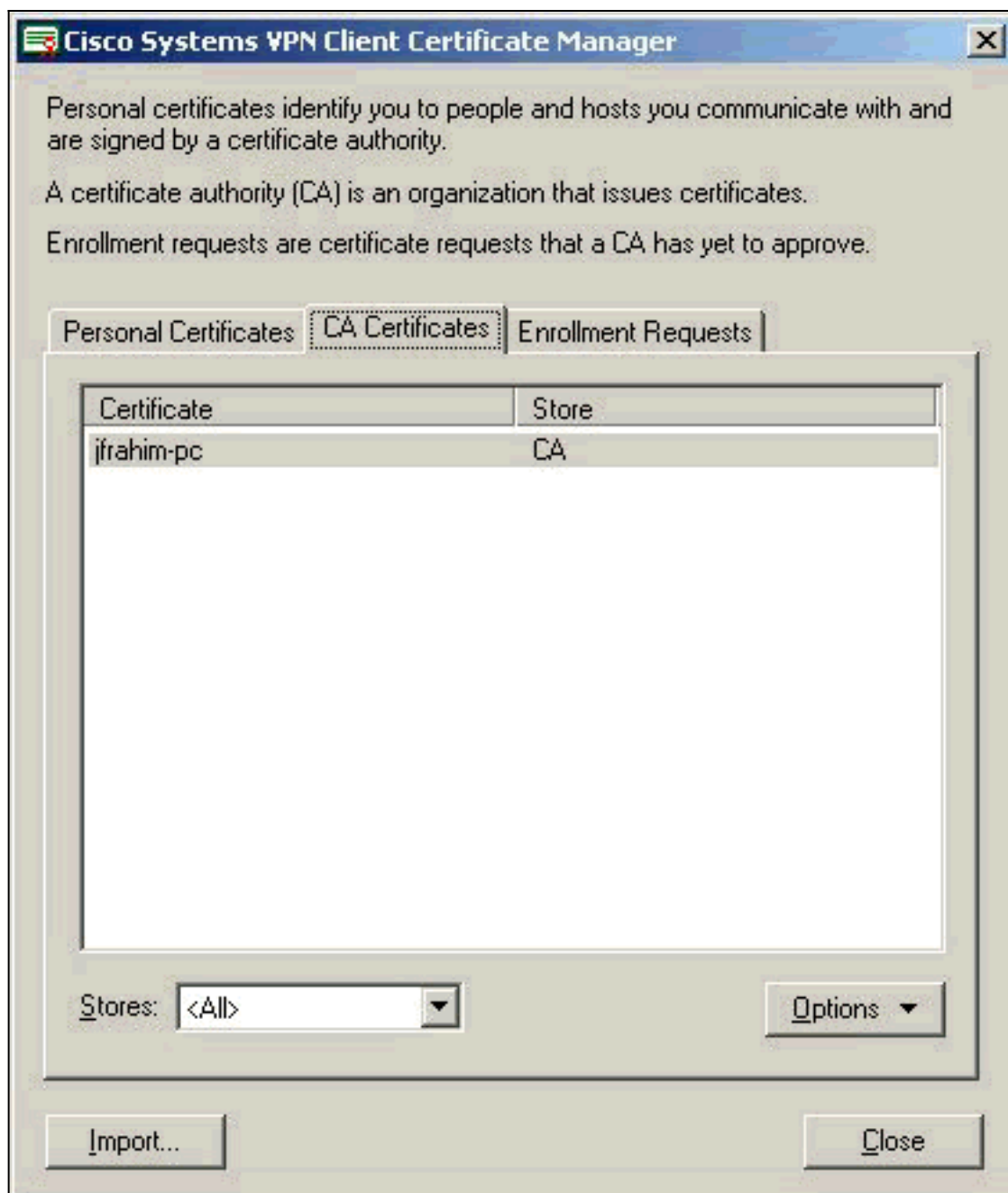


21. Asegúrese de que el certificado de identidad aparece en la ficha Certificados



personales.

22. Asegúrese de que el certificado raíz aparece en la ficha Certificados de



CA.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Cuando intenta inscribirse en Microsoft CA Server, puede generar este mensaje de error.

```
Initiating online request
Generating key pair
Generating self-signed Certificate
Initiating online request
Received a response from the CA
Your certificate request was denied
```

Si recibe este mensaje de error, consulte los registros de CA de Microsoft para obtener más

información o consulte estos recursos para obtener más información.

- [Windows no puede encontrar una autoridad de certificados que procese la solicitud](#)
- [XCCC: Se produce un mensaje de error "Se denegó su solicitud de certificado" al solicitar un certificado para conferencias seguras](#)

[Información Relacionada](#)

- [Negociación IPSec/Protocolos IKE](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)