Configuración del Cisco VPN 3000 Concentrator 4.7.x para Obtener un Certificado Digital y un Certificado SSL

Contenido

Introducción

Este documento incluye instrucciones paso a paso sobre cómo configurar los Cisco VPN 3000 Series Concentrators para autenticarse con el uso de certificados digitales o de identidad y certificados SSL.

Nota: En el VPN Concentrator, el balanceo de carga debe desactivarse antes de generar otro certificado SSL, ya que esto impide la generación del certificado.

Refiérase a Cómo obtener un Certificado Digital de una CA de Microsoft Windows utilizando ASDM en un ASA para obtener más información sobre el mismo escenario con PIX/ASA 7.x.

Consulte Ejemplo de Configuración de la Inscripción de Certificados de Cisco IOS Usando Comandos de Inscripción Mejorados para obtener más información sobre el mismo escenario con las Plataformas Cisco IOS®.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en el Cisco VPN 3000 Concentrator que ejecuta la versión 4.7.

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.

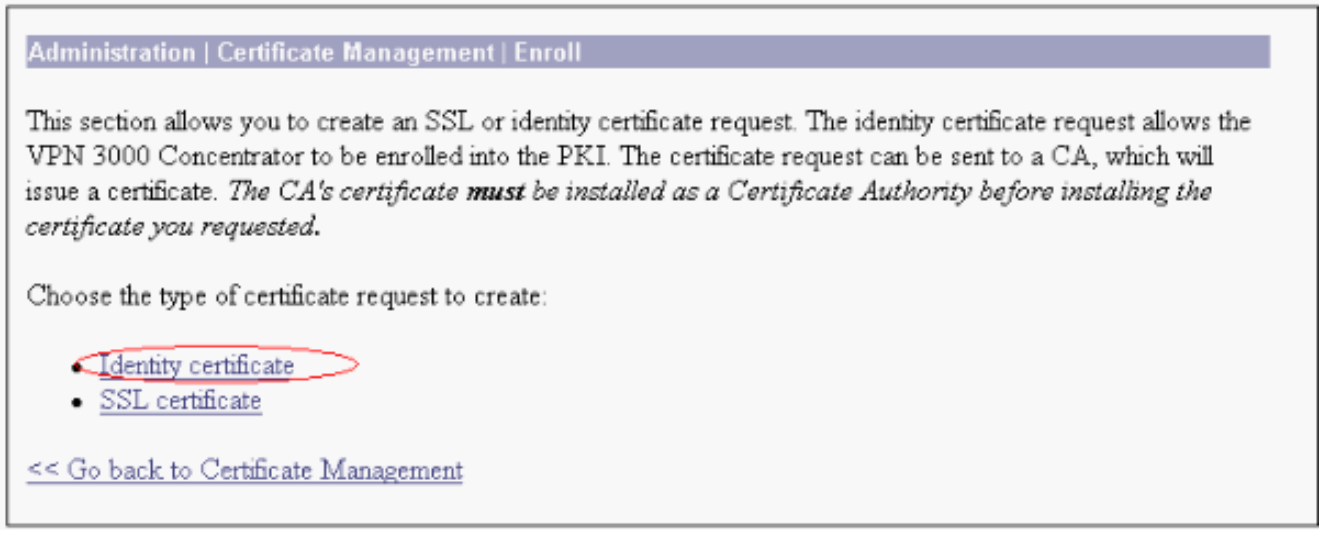
Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

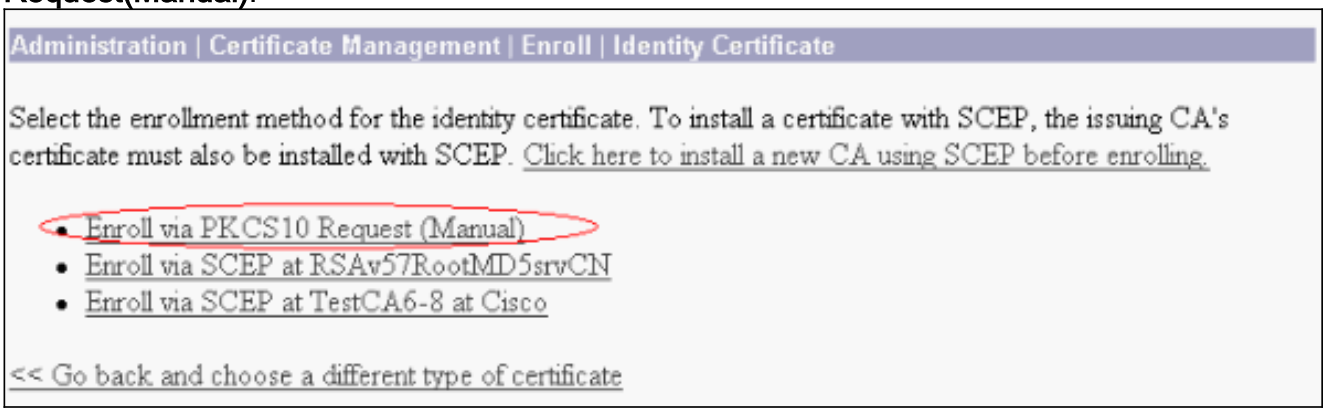
Instalación de certificados digitales en el concentrador VPN

Complete estos pasos:

1. Elija **Administration > Certificate Management > Enroll** para seleccionar la solicitud de certificado digital o de identidad.

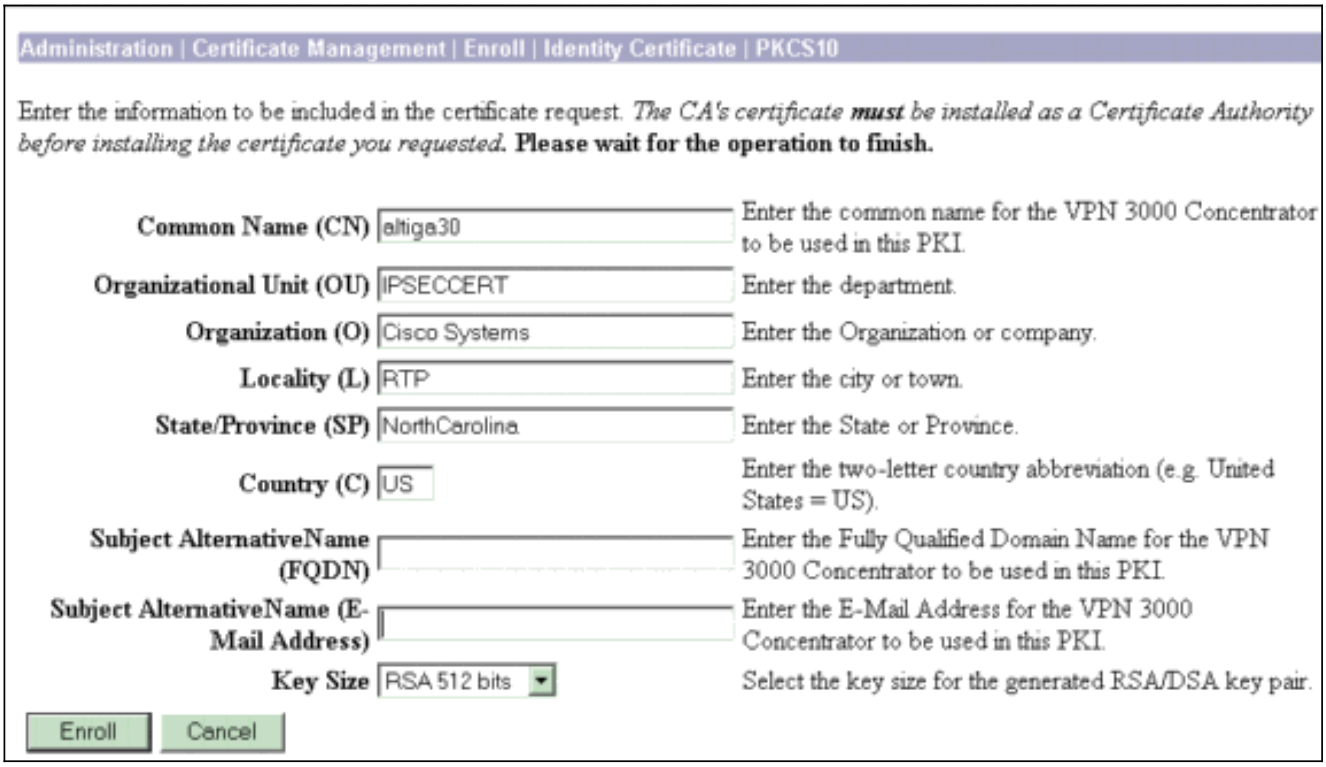


2. Elija **Administration > Certificate Management > Enrollment > Identity Certificate** y haga clic en **Enroll via PKCS10 Request(Manual)**.

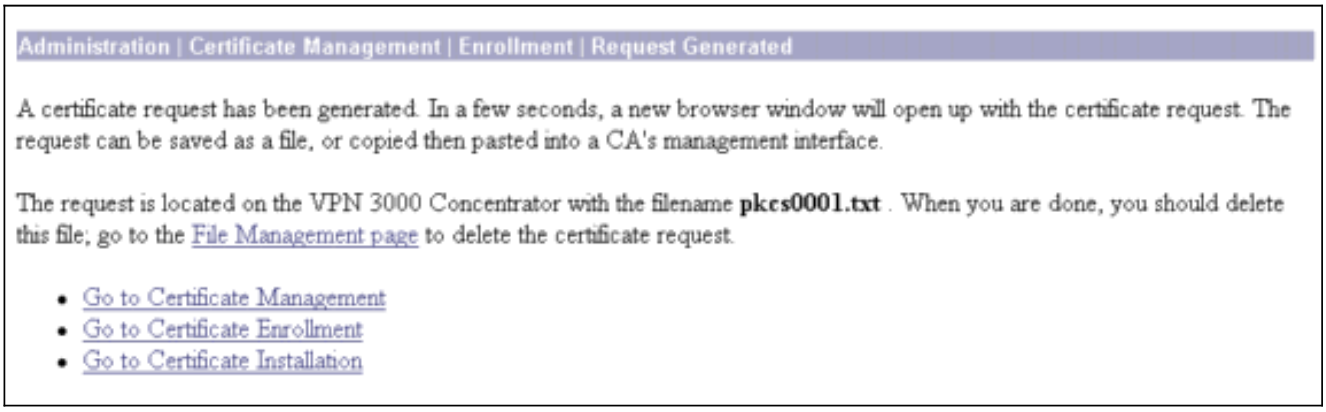


3. Rellene los campos solicitados y, a continuación, haga clic en **Inscribirse**.Estos campos se rellenan en este ejemplo.**Nombre común**: altiga30**Unidad organizativa**: IPSECCERT (la OU debe coincidir con el nombre de grupo IPsec configurado)**Organización**: Cisco Systems**Localidad**: RTP**Estado/Provincia**: Carolina del Norte**País**: EE. UU.**Nombre de dominio completamente calificado** —(no se utiliza aquí)**Tamaño de clave**: 512**Nota:** Si solicita un certificado SSL o un certificado de identidad mediante el protocolo simple de

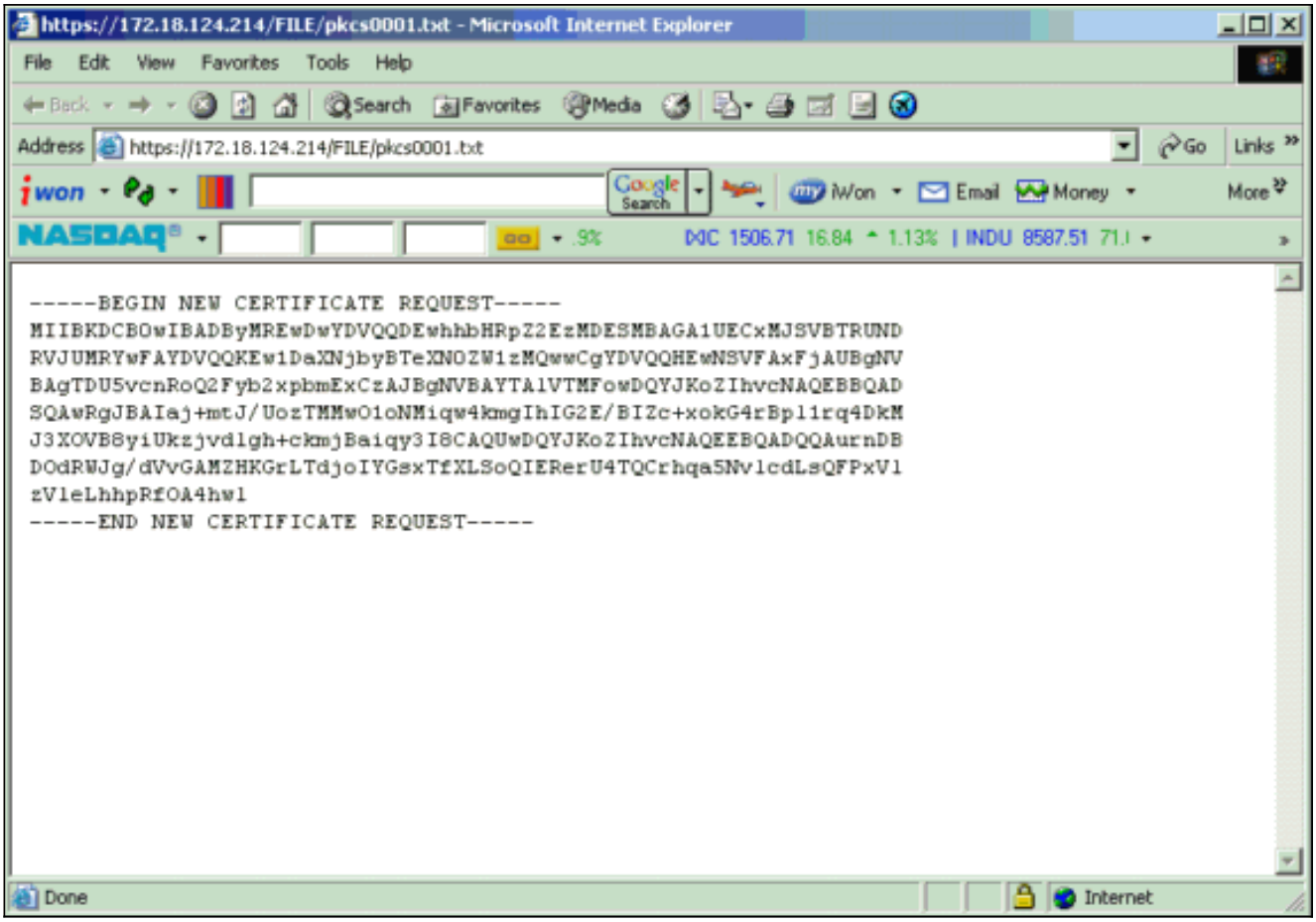
inscripción de certificados (SCEP), estas son las únicas opciones RSA disponibles.512 bits RSA768 bits RSA1024 bits RSA2048 bits RSADSA 512 bitsDSA 768 bitsDSA 1024 bits



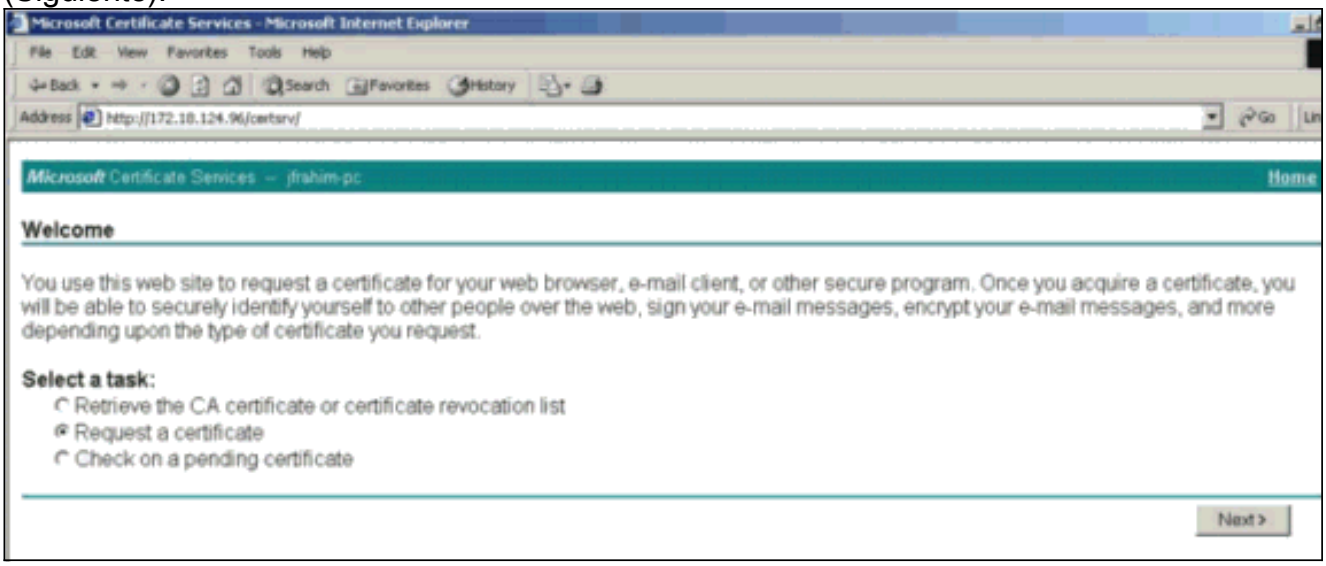
4. Después de hacer clic en **Inscribirse**, aparecen varias ventanas. La primera ventana confirma que ha solicitado un certificado.



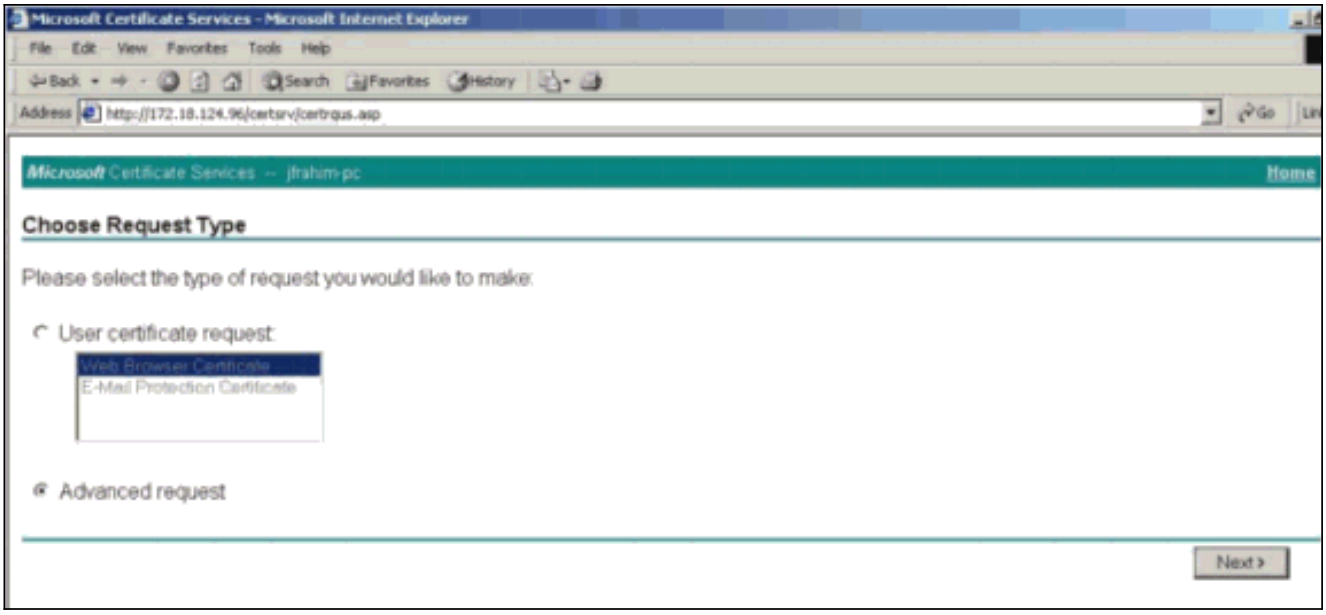
También se abre una nueva ventana del navegador que muestra el archivo de solicitud PKCS.



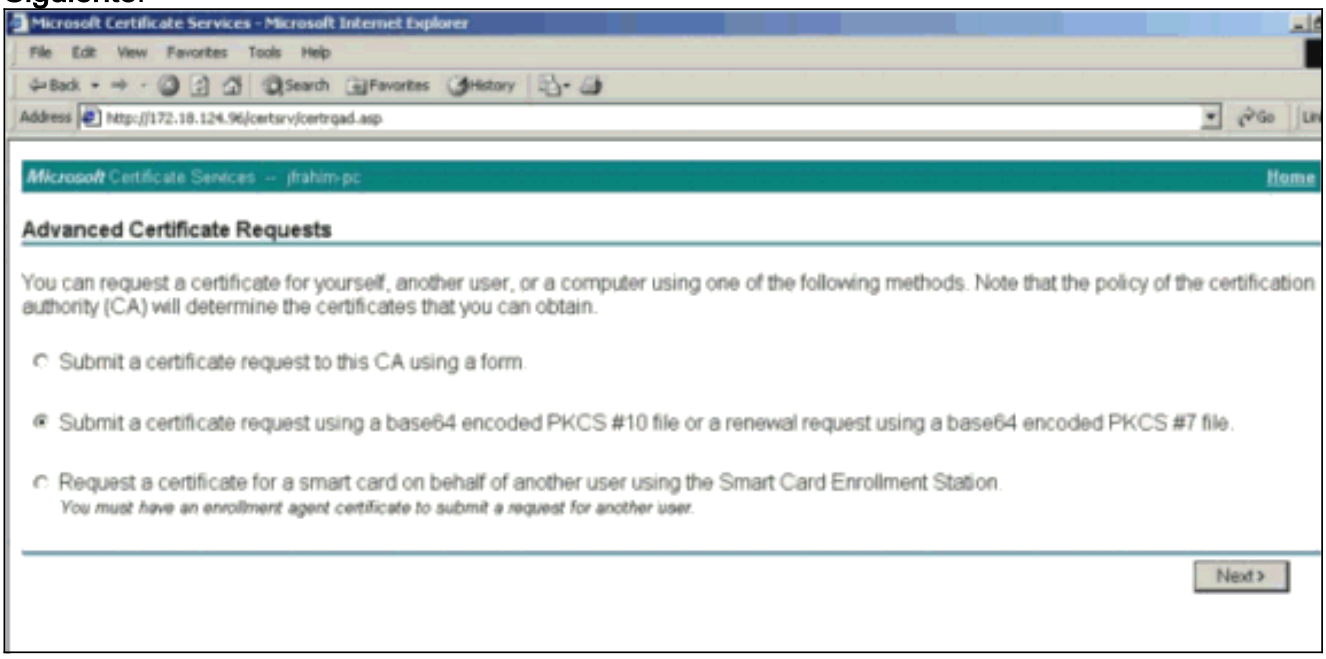
5. En el servidor de la Autoridad de certificación (CA), resalte la solicitud y péguela en el servidor de la CA para enviar la solicitud. Haga clic en Next (Siguiente).



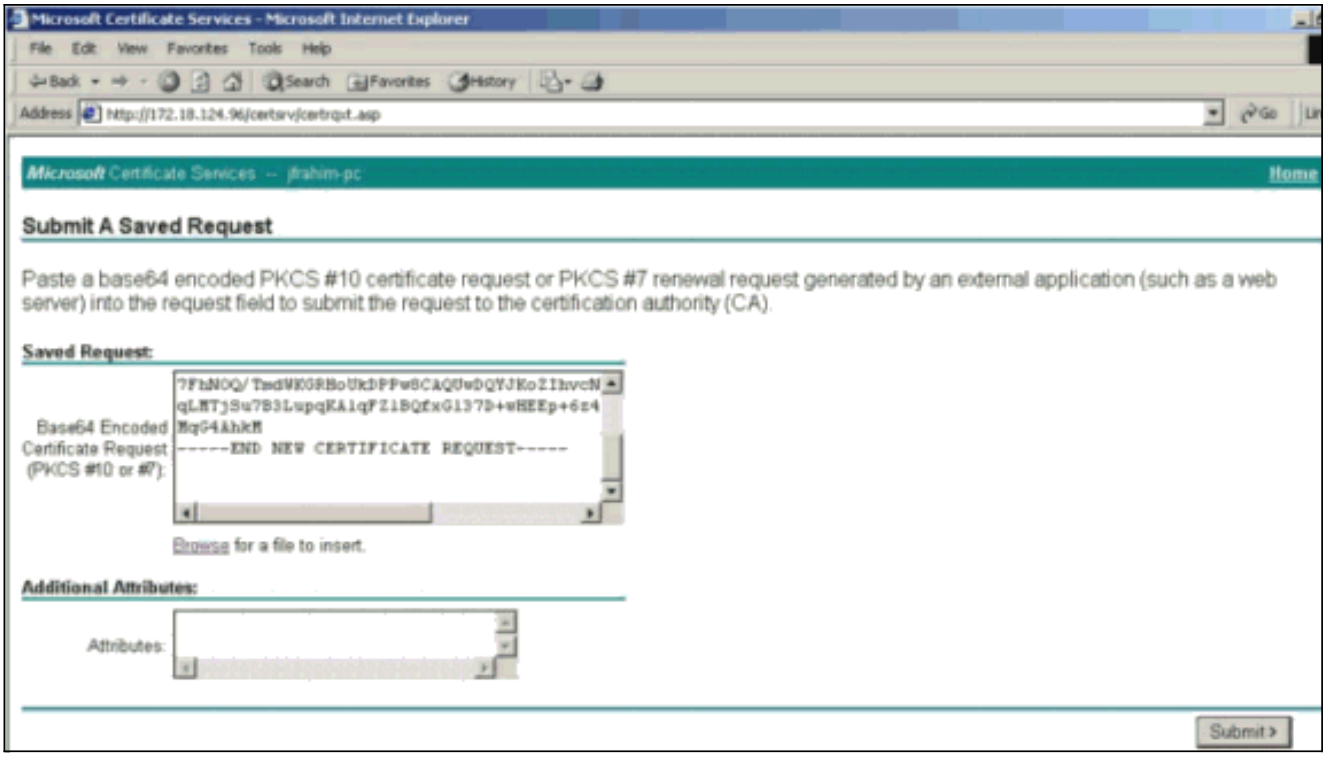
6. Seleccione **Advanced request** y haga clic en **Next**.



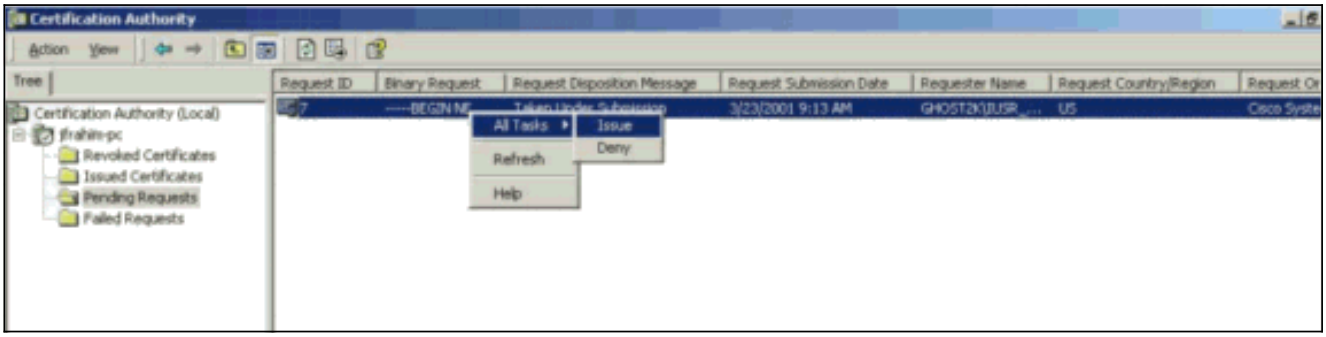
7. Seleccione **Enviar una solicitud de certificado utilizando un archivo PKCS #10 codificado en base64 o una solicitud de renovación usando un archivo PKCS #7 codificado en base64** y, a continuación, haga clic en **Siguiente**.



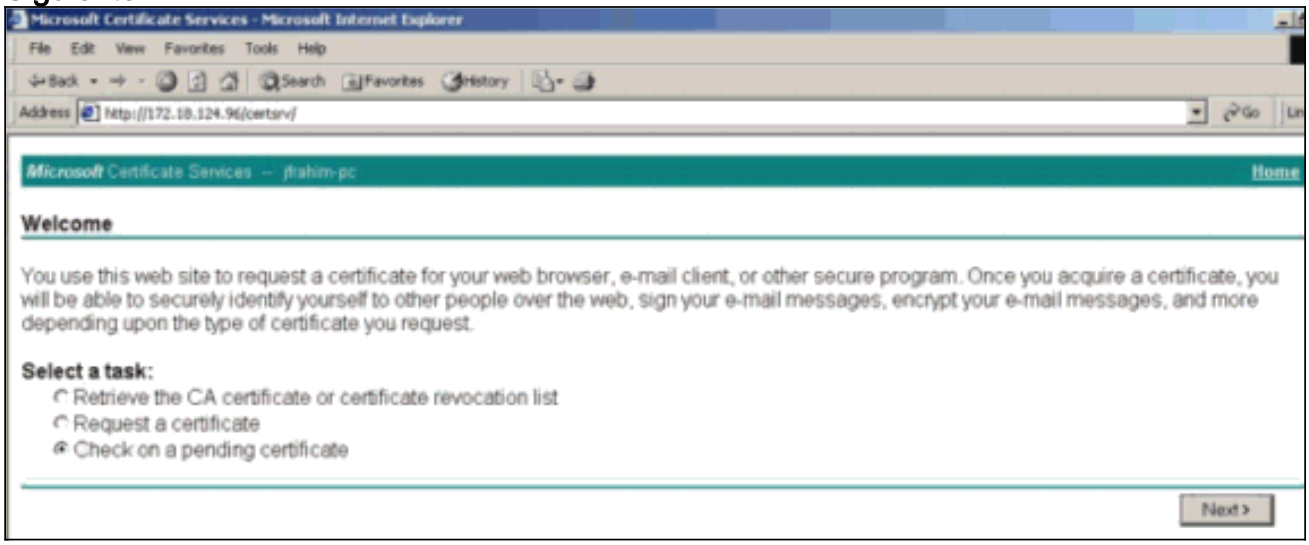
8. Corte y pegue el archivo PKCS en el campo de texto de la sección Solicitud guardada. A continuación, haga clic en **Enviar**.



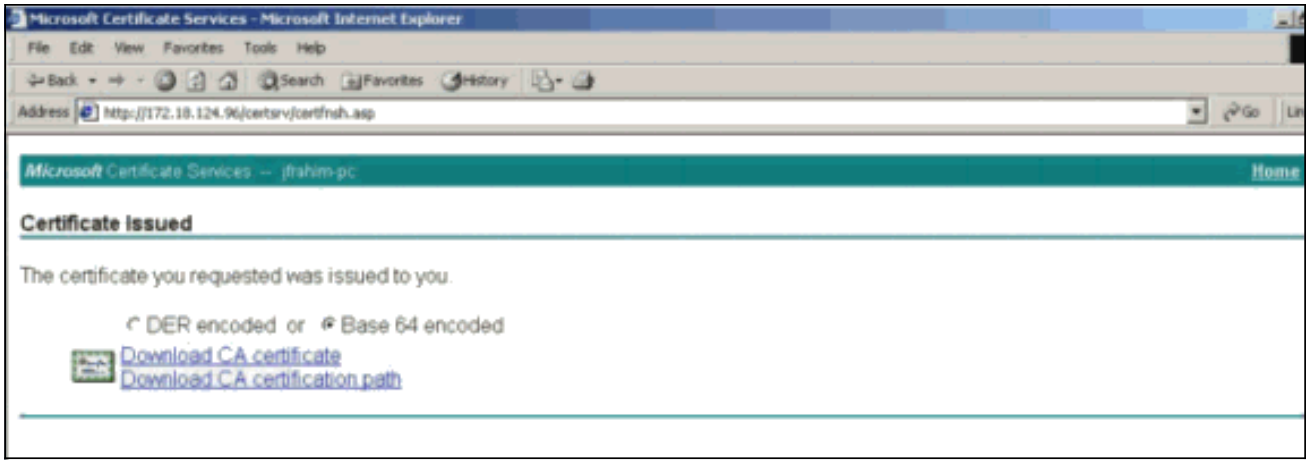
9. Ejecute el certificado de identidad en el servidor de la CA.



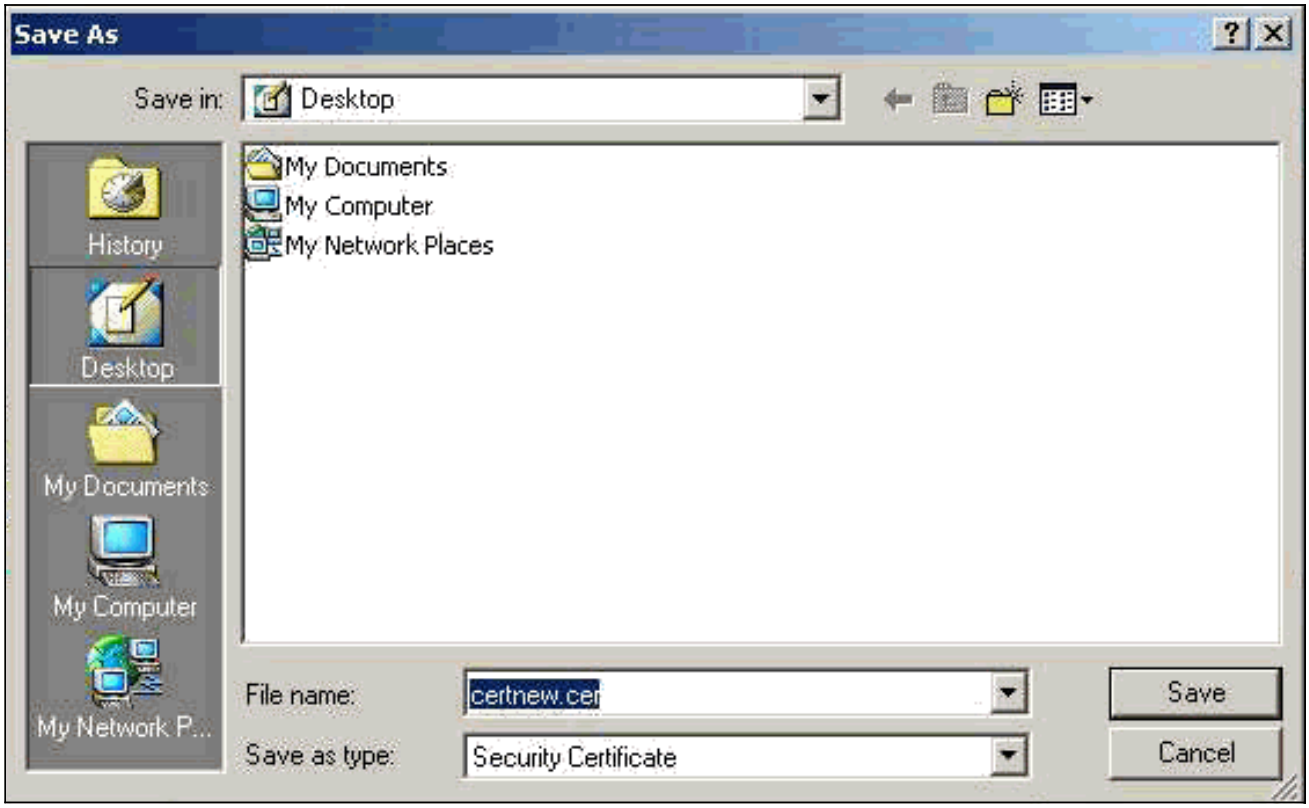
10. Descargue los certificados raíz y de identidad. En el servidor de la CA, seleccione **Comprobar un certificado pendiente** y haga clic en **Siguiente**.



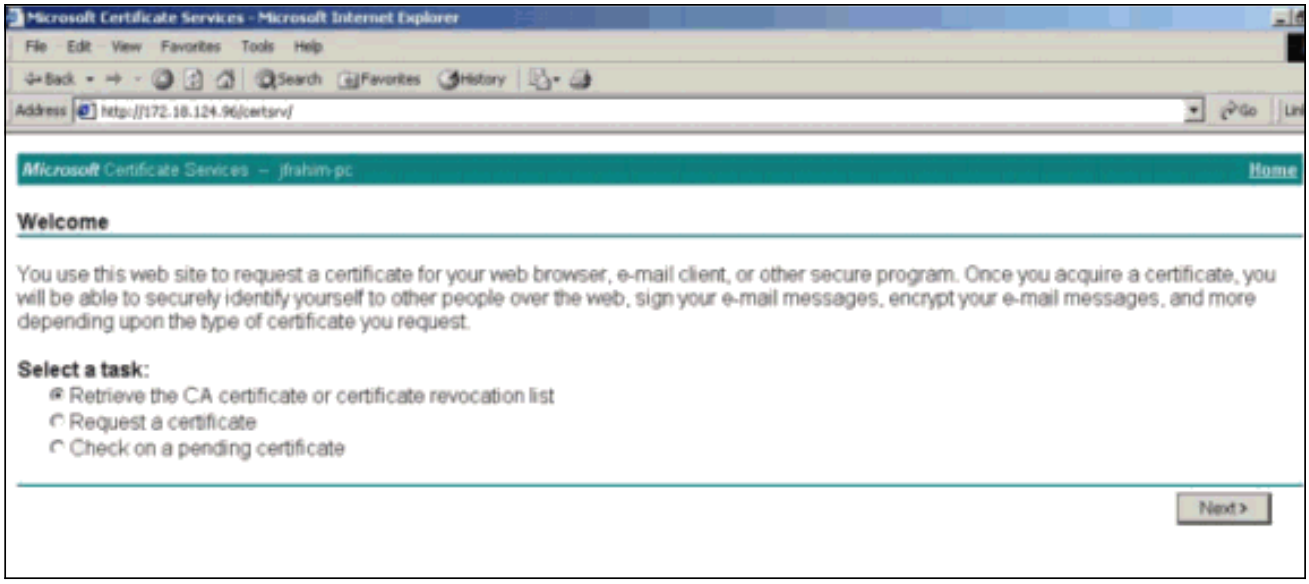
11. Seleccione **Base 64 codificada** y haga clic en **Descargar certificado de CA** en el servidor de CA.



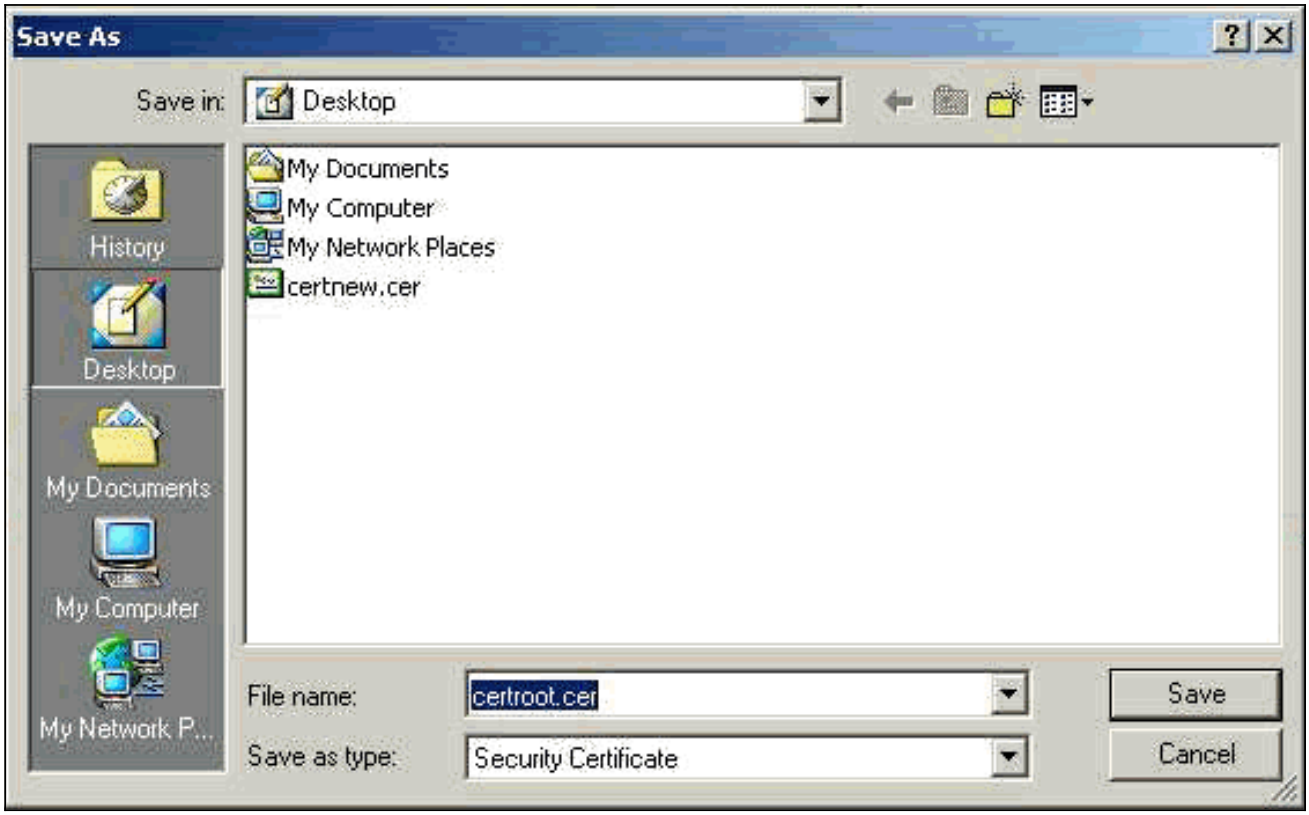
12. Guarde el certificado de identidad en la unidad local.



13. En el servidor de la CA, seleccione **Recuperar el certificado de la CA o la lista de revocación de certificados** para obtener el certificado raíz. Luego haga clic en Next (Siguiente).



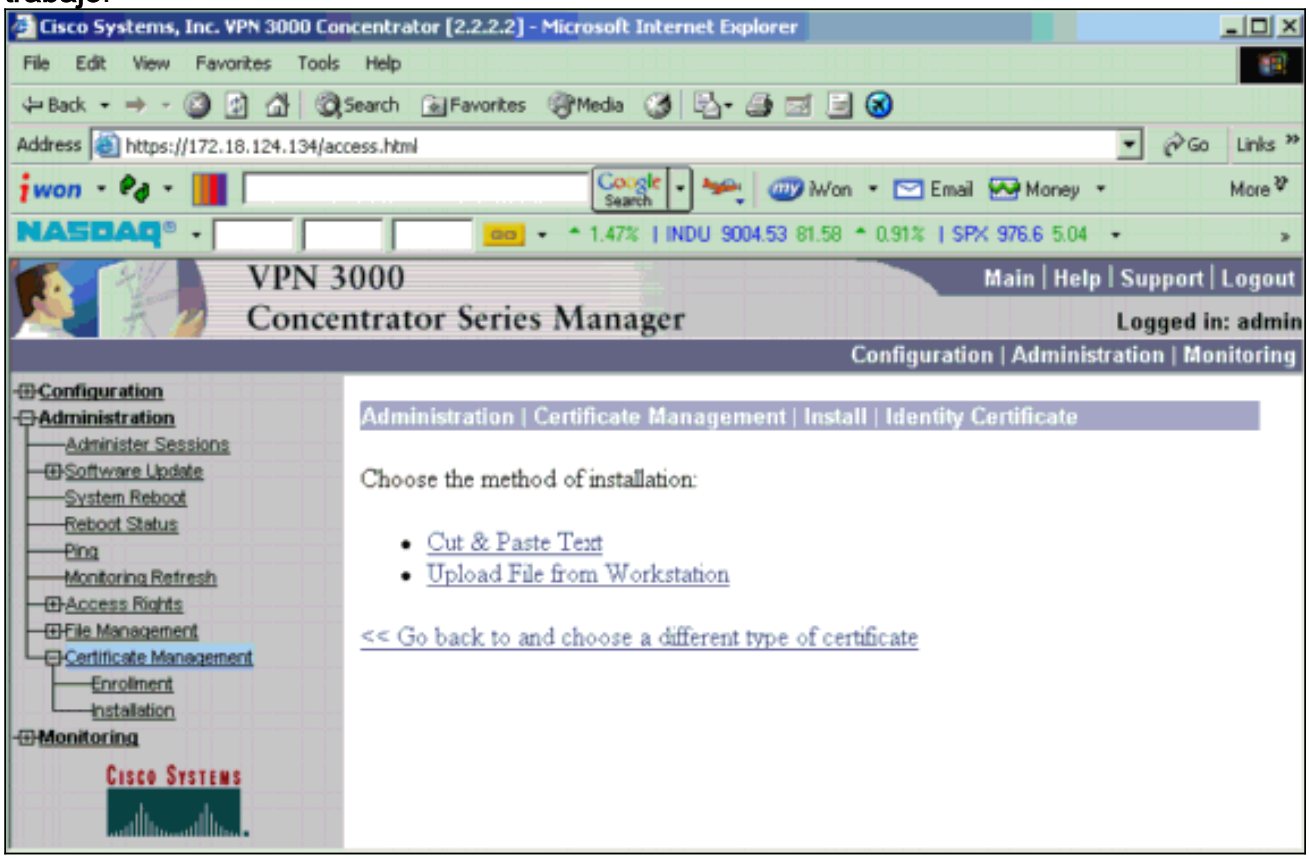
14. Guarde el certificado raíz en la unidad local.



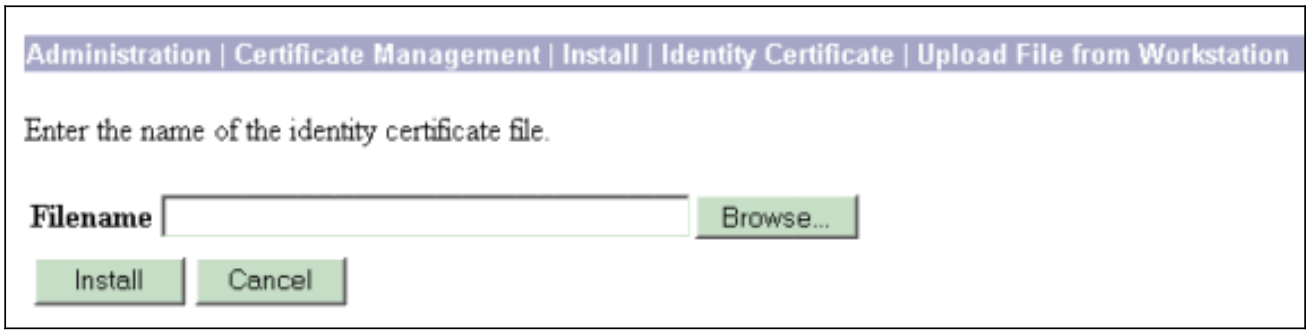
15. Instale los certificados raíz e identidad en el VPN 3000 Concentrator. Para hacer esto, seleccione **Administration > Certificate Manager > Installation > Install certificate from enrollment**. En Estado de inscripción, haga clic en **Instalar**.

16. Haga clic en **Cargar archivo desde la estación de**

trabajo.



17. Haga clic en **Examinar** y seleccione el archivo de certificado raíz que guardó en la unidad local.Seleccione **Install** para instalar el certificado de identidad en el concentrador VPN. La Administración | La ventana Administración de certificados aparece como confirmación y el nuevo certificado de identidad aparece en la tabla Certificados de identidad.



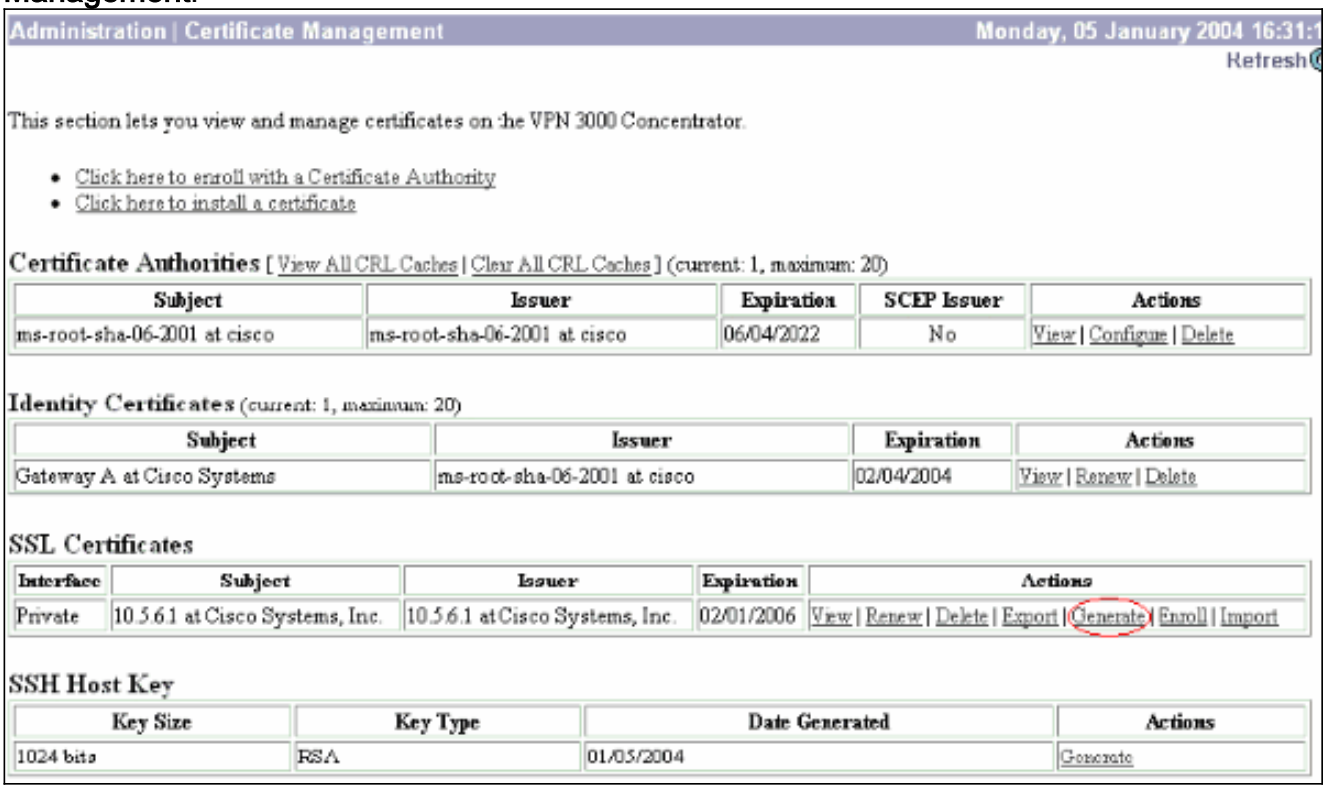
Nota: Complete estos pasos para generar un nuevo certificado si falla el certificado.Seleccione **Administration > Certificate Management**.Haga clic en **Eliminar** en el cuadro Acciones de la lista de certificados SSL.Seleccione **Administration > System Reboot**.Seleccione **Guardar la configuración activa en el momento del reinicio**, elija **Ahora** y haga clic en **Aplicar**. Ahora puede generar un nuevo certificado después de que se complete la recarga.

Instalación de certificados SSL en el concentrador VPN

Si utiliza una conexión segura entre su navegador y el concentrador VPN, el concentrador VPN requiere un certificado SSL. También necesita un certificado SSL en la interfaz que utiliza para administrar el concentrador VPN y para WebVPN, y para cada interfaz que termina los túneles WebVPN.

Los certificados SSL de la interfaz, si no existen, se generan automáticamente cuando el concentrador VPN 3000 se reinicia después de actualizar el software del concentrador VPN 3000. Dado que un certificado autofirmado se genera automáticamente, este certificado no se puede verificar. Ninguna autoridad certificadora ha garantizado su identidad. Sin embargo, este certificado le permite establecer un contacto inicial con el concentrador VPN mediante el navegador. Si desea sustituirlo por otro certificado SSL autofirmado, siga estos pasos:

1. Elija **Administration > Certificate Management**.



2. Haga clic en **Generar** para mostrar el nuevo certificado en la tabla de certificados SSL y reemplazar el certificado existente.Esta ventana le permite configurar campos para certificados SSL que el concentrador VPN genera automáticamente. Estos certificados SSL son para interfaces y para balanceo de carga.

Si desea obtener un certificado SSL verificable (es decir, uno emitido por una Autoridad de Certificación), vea la sección Instalación de Certificados Digitales en el Concentrador VPN de este documento para utilizar el mismo procedimiento que utiliza para obtener certificados

de identidad. Pero esta vez, en la ventana **Administration > Certificate Management > Enroll, haga clic en SSL certificate** (en lugar de Identity Certificate).**Nota:** Consulte la *Administración* | Sección *Administración de Certificados* del Volumen II de Referencia del Concentrador VPN 3000: Administración y Monitoreo Versión 4.7 para obtener información completa sobre certificados digitales y certificados SSL.

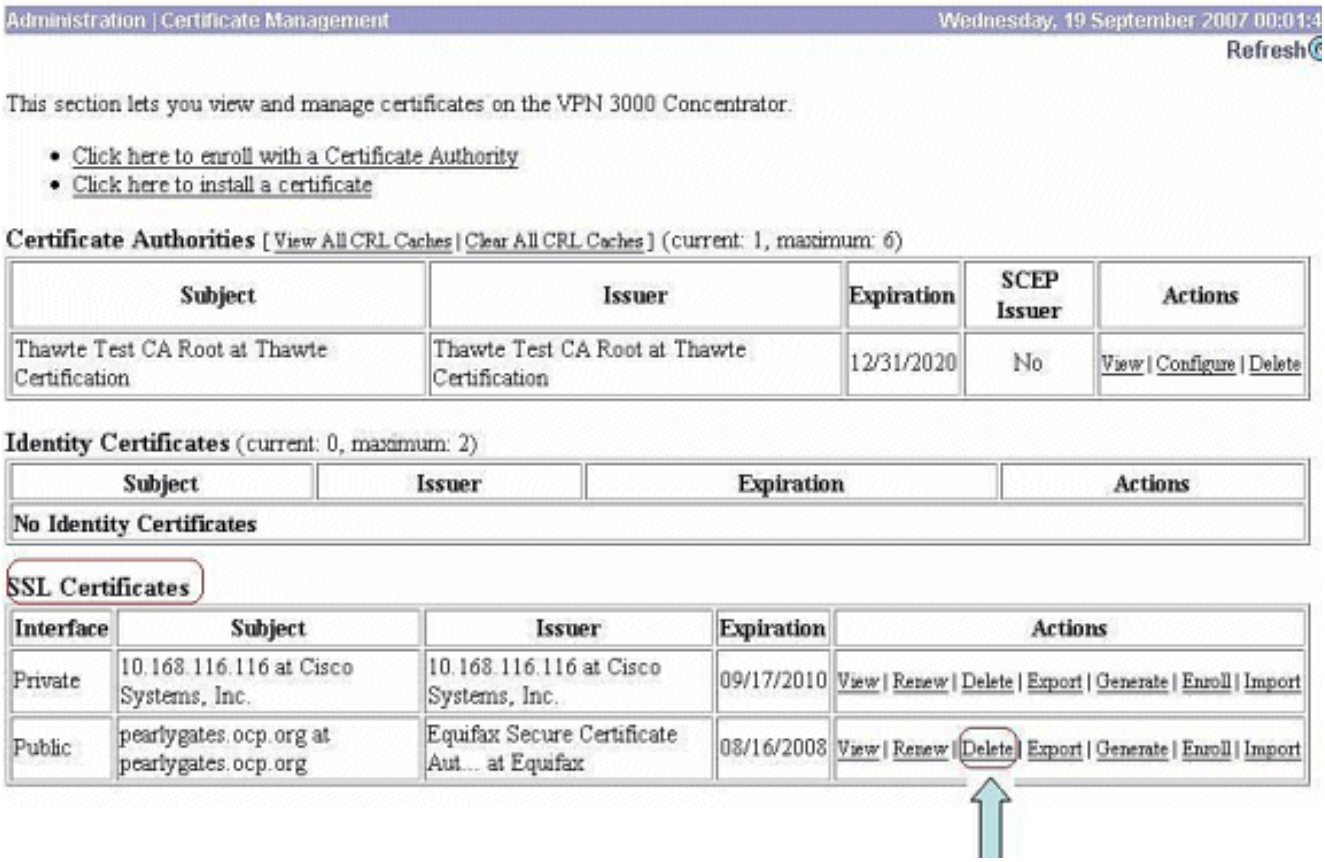
Renovación de Certificados SSL en el Concentrador VPN

Esta sección describe cómo renovar los certificados SSL:

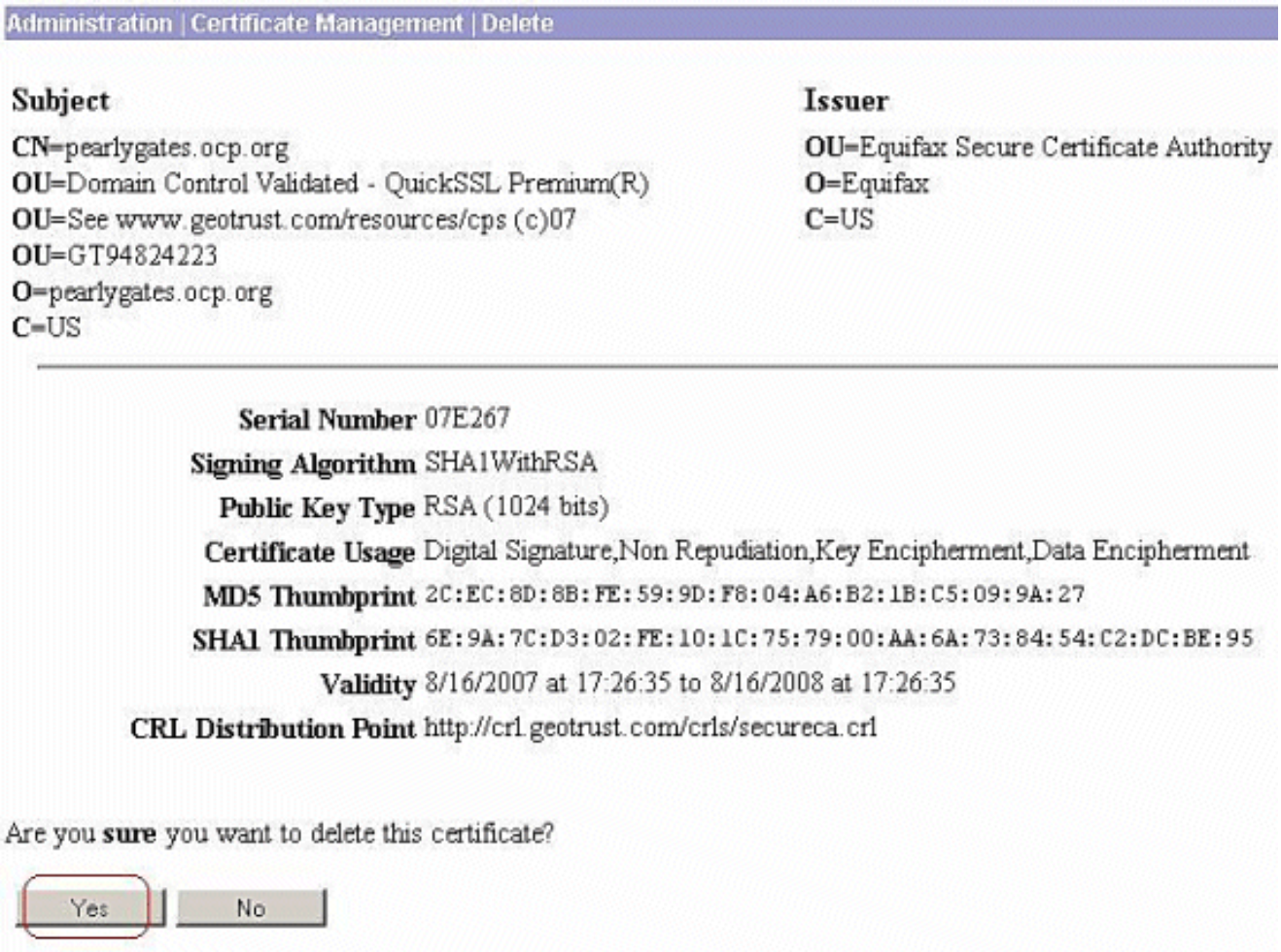
Si esto es para el certificado SSL generado por el VPN Concentrator, vaya a **Administration > Certificate Management** en la sección SSL. Haga clic en la opción **Renovar** y que renueva el certificado SSL.

Si se trata de un certificado concedido por un servidor CA externo, siga estos pasos:

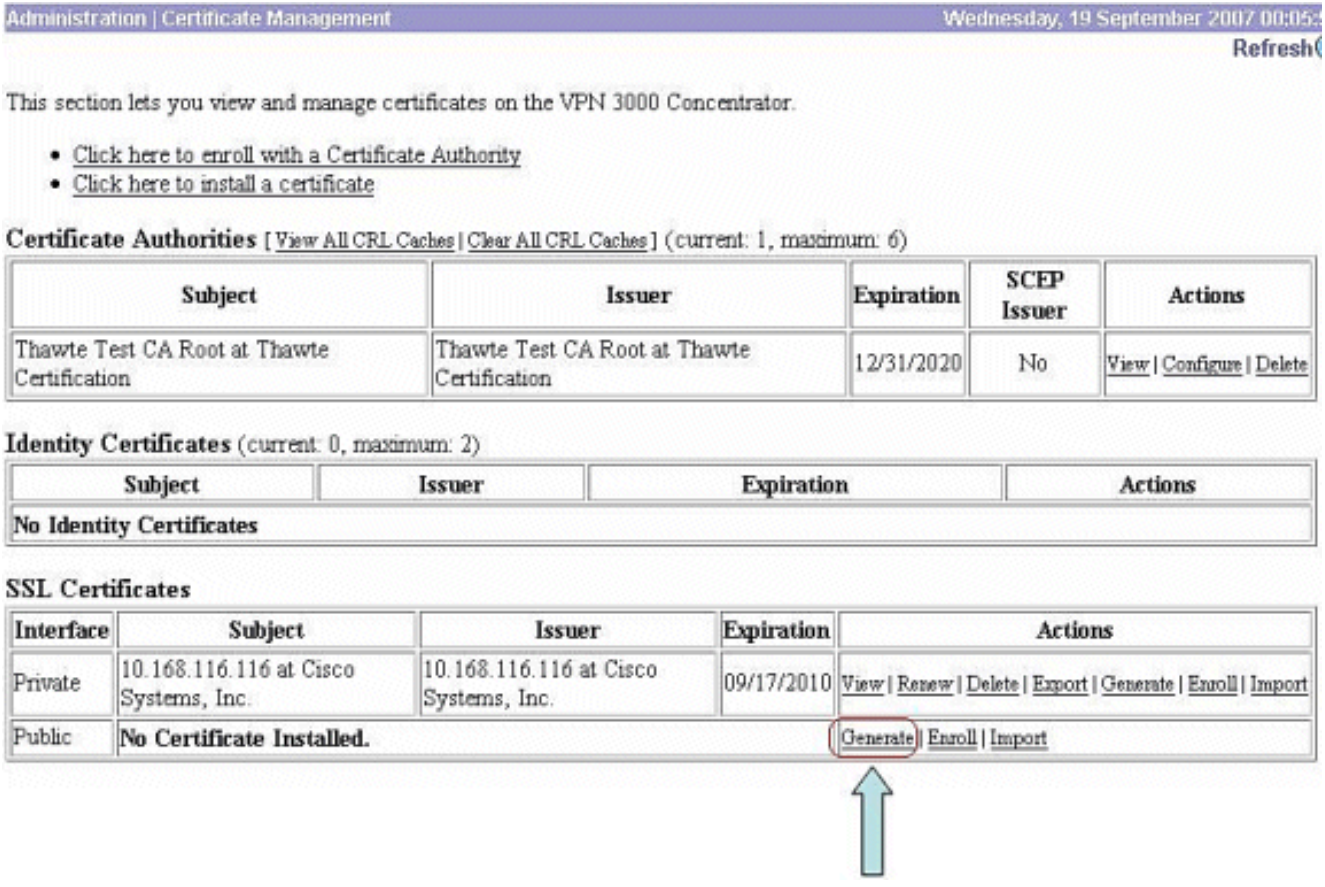
1. Elija **Administration > Certificate Management > Delete** bajo *SSL Certificates* para eliminar los certificados caducados de la interfaz pública.



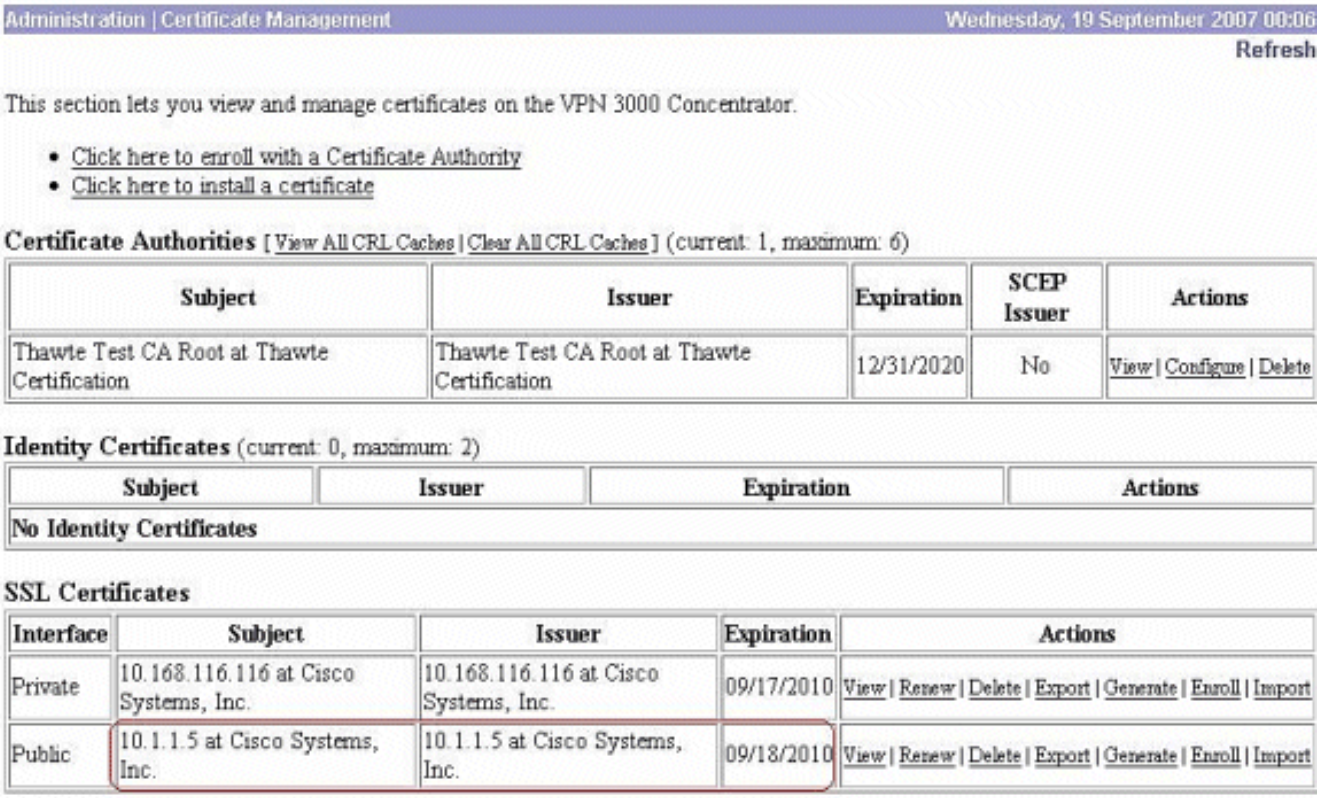
Haga clic en **Yes** para confirmar la eliminación del certificado SSL.



2. Elija **Administration > Certificate Management > Generate** para generar el nuevo certificado SSL.



Aparece el nuevo certificado SSL para la interfaz pública.



Administration | Certificate Management — Wednesday, 19 September 2007 00:06

Refresh

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- Click here to enroll with a Certificate Authority
- Click here to install a certificate

Certificate Authorities [View All CRL Caches | Clear All CRL Caches] (current: 1, maximum: 6)

Subject	Issuer	Expiration	SCEP Issuer	Actions
Thawte Test CA Root at Thawte Certification	Thawte Test CA Root at Thawte Certification	12/31/2020	No	View | Configure | Delete

Identity Certificates (current: 0, maximum: 2)

Subject	Issuer	Expiration	Actions
No Identity Certificates			

SSL Certificates

Interface	Subject	Issuer	Expiration	Actions
Private	10.168.116.116 at Cisco Systems, Inc.	10.168.116.116 at Cisco Systems, Inc.	09/17/2010	View | Renew | Delete | Export | Generate | Enroll | Import
Public	10.1.1.5 at Cisco Systems, Inc.	10.1.1.5 at Cisco Systems, Inc.	09/18/2010	View | Renew | Delete | Export | Generate | Enroll | Import

Información Relacionada

- Página de soporte del concentrador de la serie Cisco VPN 3000
- Negociación IPSec/Protocolos IKE
- Soporte Técnico y Documentación - Cisco Systems