

Configurar el Cisco VPN 3000 Concentrator 4.7.x para conseguir un certificado digital y un certificado SSL

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Instale los Certificados digitales en el concentrador VPN](#)

[Instale los Certificados SSL en el concentrador VPN](#)

[Renueve los Certificados SSL en el concentrador VPN](#)

[Información Relacionada](#)

Introducción

Este documento incluye las instrucciones paso a paso en cómo configurar el Concentradores Cisco VPN de la serie 3000 para autenticar con el uso de digital o de los certificados de identidad y de los Certificados SSL.

Note: En el concentrador VPN, el Equilibrio de carga debe ser inhabilitado antes de que usted genere otro certificado SSL puesto que éste previene la generación del certificado.

Refiérase a [cómo obtener un certificado digital de Microsoft Windows CA usando el ASDM en un ASA](#) para aprender un escenario más casi igual con el PIX/ASA 7.x.

Refiera a la [inscripción del certificado del Cisco IOS usando el ejemplo aumentado de los comandos Configuration de la inscripción](#) para aprender un escenario más casi igual con las Plataformas de Cisco IOS®.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

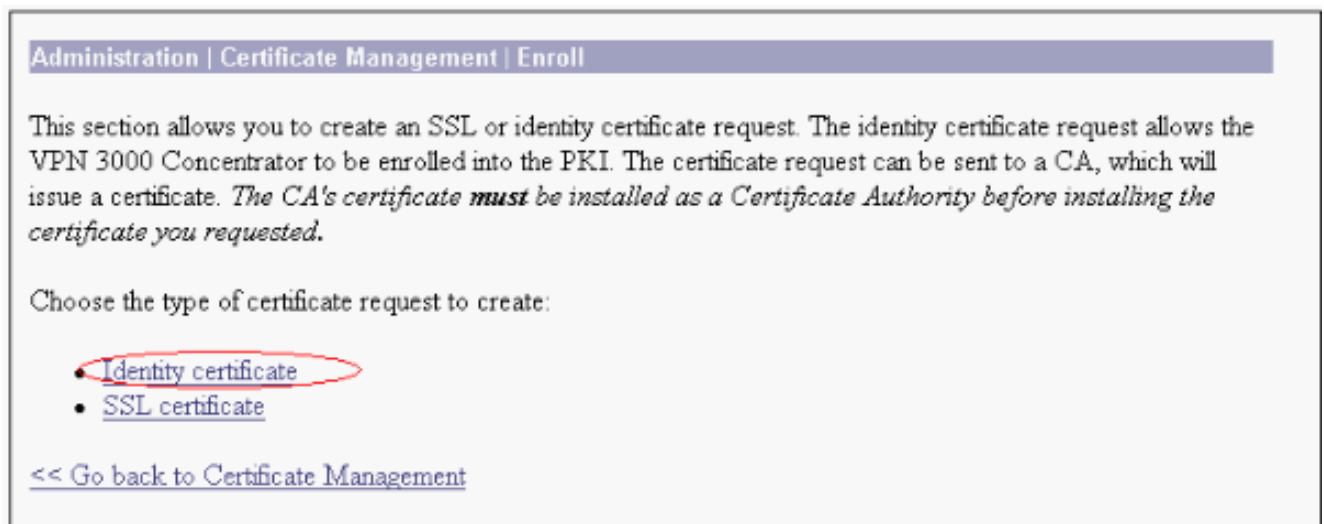
Convenciones

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

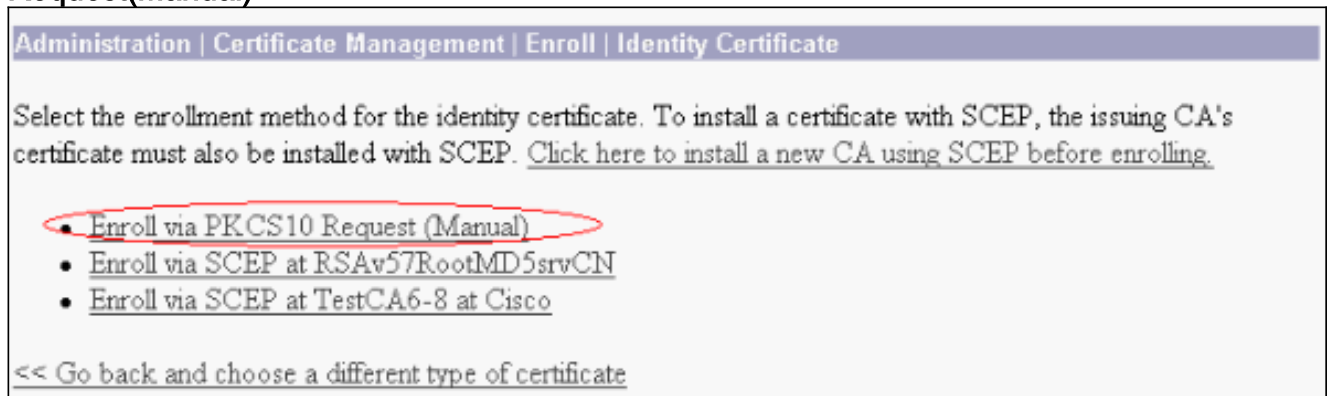
Instale los Certificados digitales en el concentrador VPN

Complete estos pasos:

1. Elija el **Administration (Administración) > Certificate Management (Administración de certificados) > Enroll (Registrar)** para seleccionar la petición digital o del certificado de identidad.



2. Elija el **Administration (Administración) > Certificate Management (Administración de certificados) > Enrollment (Inscripción) > Identity Certificate (Certificado de identidad)** y el tecleo **alista** vía **PKCS10 Request(Manual)**.



3. Complete los campos pedidos, y después haga clic **alistan**. Estos campos se completan hacia fuera este ejemplo. **Common Name** — altiga30Unidad organizativa — IPSECCERT (el OU debe hacer juego el nombre de grupo configurado del IPsec) **Organización** — Cisco Systems **Lugar** — RTP **Estado/provincia** — Carolina del Norte **País** — Los E.E.U.U. **Nombre de dominio totalmente calificado (FQDN)** — (no utilizado aquí) **Tamaño de clave** — 512 **Note:** Si

usted pide un certificado SSL o un certificado de identidad usando el protocolo simple certificate enrollment (SCEP), éstas son las únicas opciones de RSA disponibles. Bits RSA 512 Bits RSA 768 Bits RSA 1024 Bits RSA 2048 Bits DSA 512 Bits DSA 768 Bits DSA 1024

Administration | Certificate Management | Enroll | Identity Certificate | PKCS10

Enter the information to be included in the certificate request. *The CA's certificate **must** be installed as a Certificate Authority before installing the certificate you requested. Please wait for the operation to finish.*

Common Name (CN)	<input type="text" value="altiga30"/>	Enter the common name for the VPN 3000 Concentrator to be used in this PKI.
Organizational Unit (OU)	<input type="text" value="IPSECCERT"/>	Enter the department.
Organization (O)	<input type="text" value="Cisco Systems"/>	Enter the Organization or company.
Locality (L)	<input type="text" value="RTP"/>	Enter the city or town.
State/Province (SP)	<input type="text" value="NorthCarolina"/>	Enter the State or Province.
Country (C)	<input type="text" value="US"/>	Enter the two-letter country abbreviation (e.g. United States = US).
Subject AlternativeName (FQDN)	<input type="text"/>	Enter the Fully Qualified Domain Name for the VPN 3000 Concentrator to be used in this PKI.
Subject AlternativeName (E-Mail Address)	<input type="text"/>	Enter the E-Mail Address for the VPN 3000 Concentrator to be used in this PKI.
Key Size	<input type="text" value="RSA 512 bits"/>	Select the key size for the generated RSA/DSA key pair.

4. Después de que usted tecleo **aliste**, varias ventanas aparecen. La primera ventana confirma que usted ha pedido un certificado.

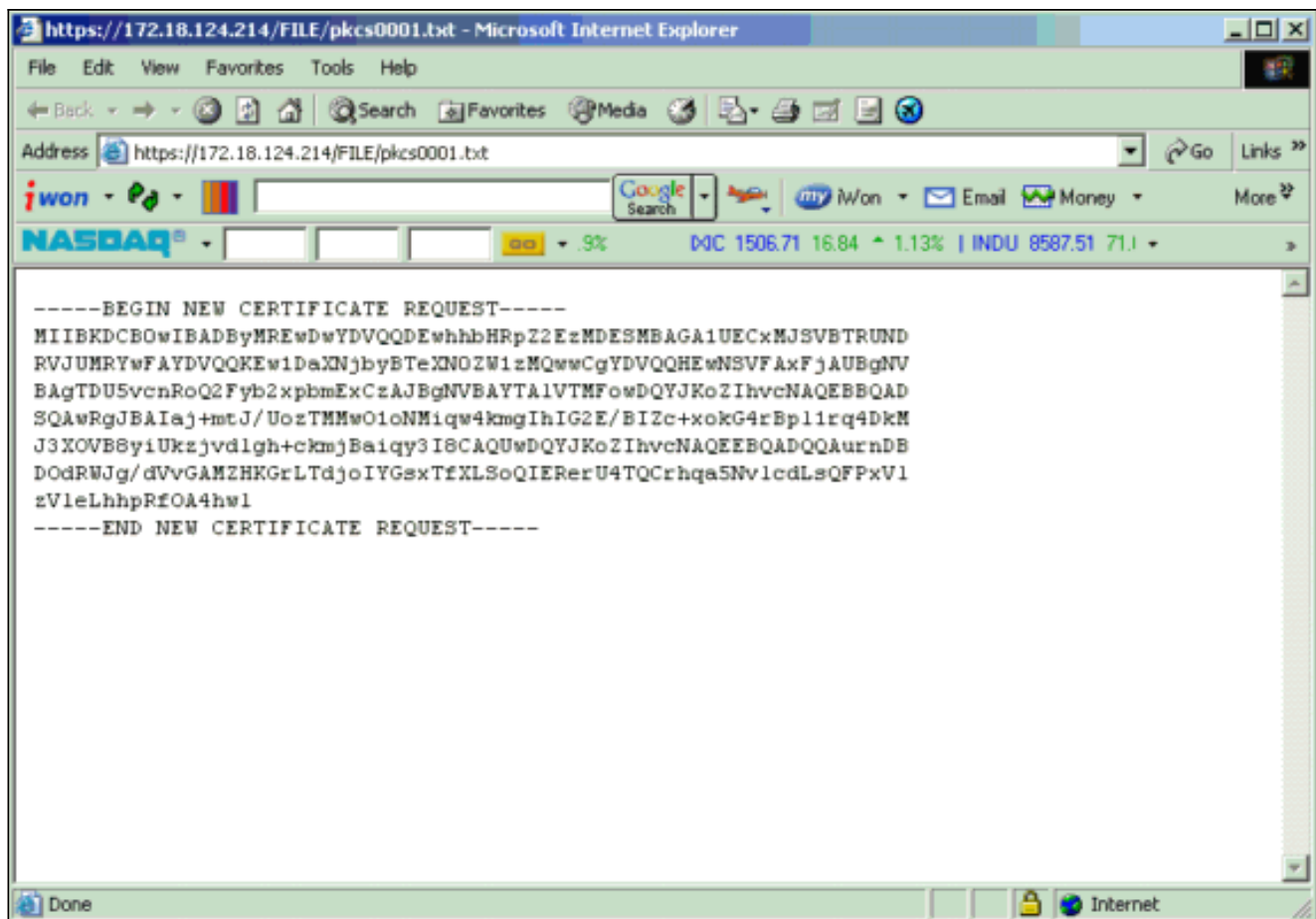
Administration | Certificate Management | Enrollment | Request Generated

A certificate request has been generated. In a few seconds, a new browser window will open up with the certificate request. The request can be saved as a file, or copied then pasted into a CA's management interface.

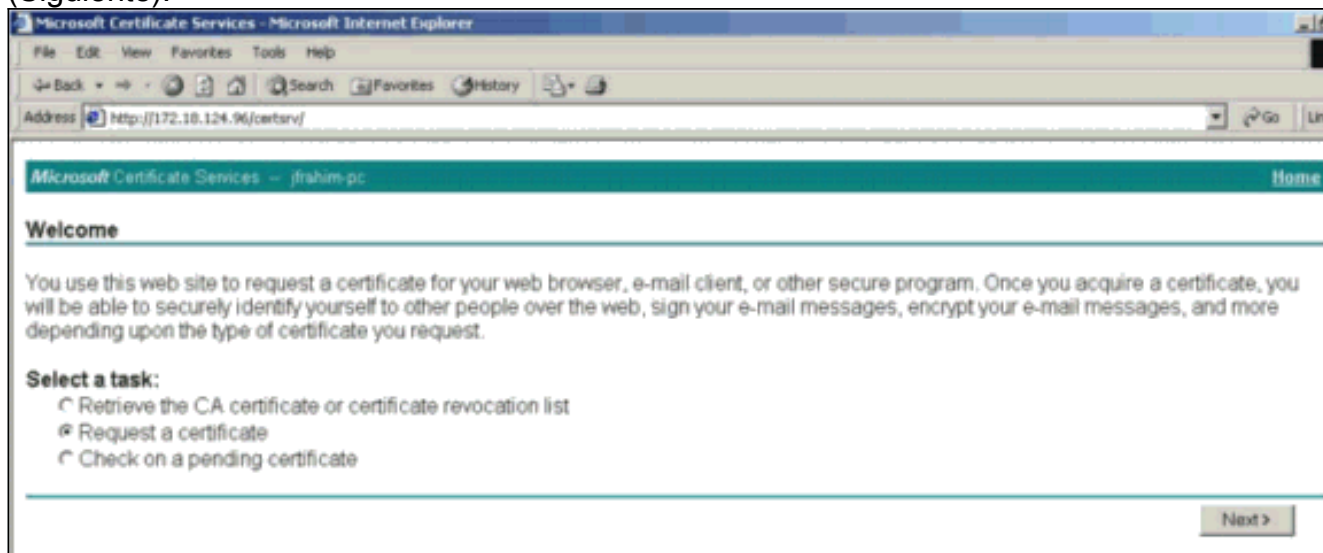
The request is located on the VPN 3000 Concentrator with the filename **pkcs0001.txt**. When you are done, you should delete this file; go to the [File Management page](#) to delete the certificate request.

- [Go to Certificate Management](#)
- [Go to Certificate Enrollment](#)
- [Go to Certificate Installation](#)

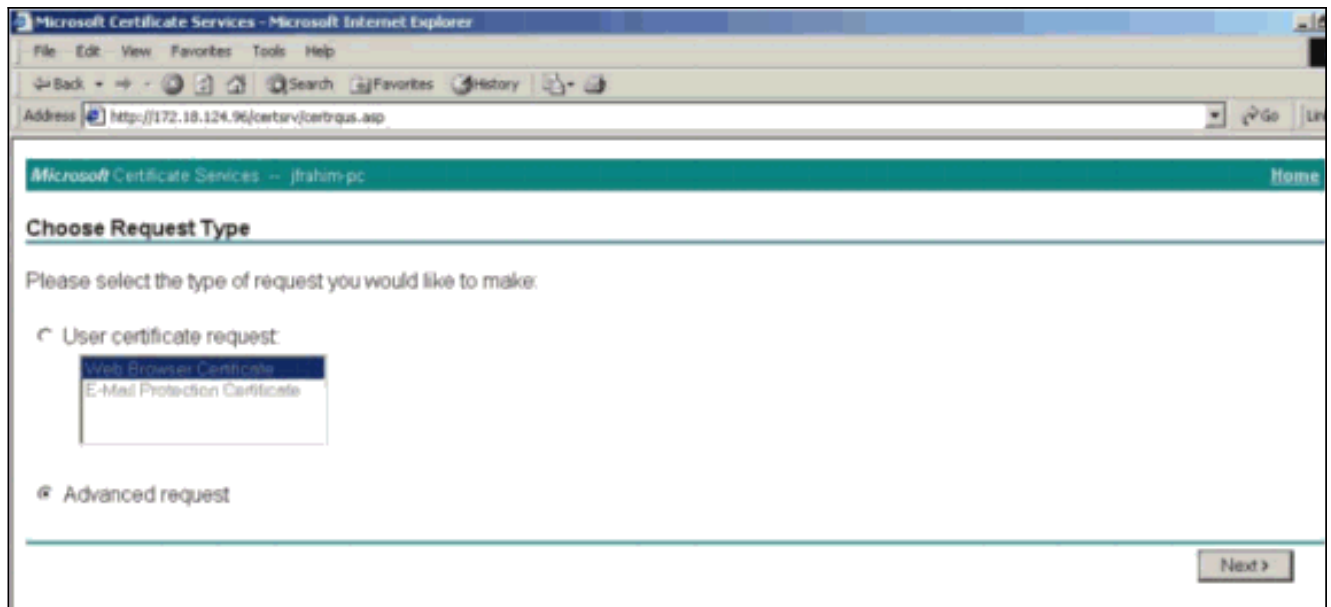
Una nueva ventana del buscador también abre y visualiza su archivo de la petición PKCS.



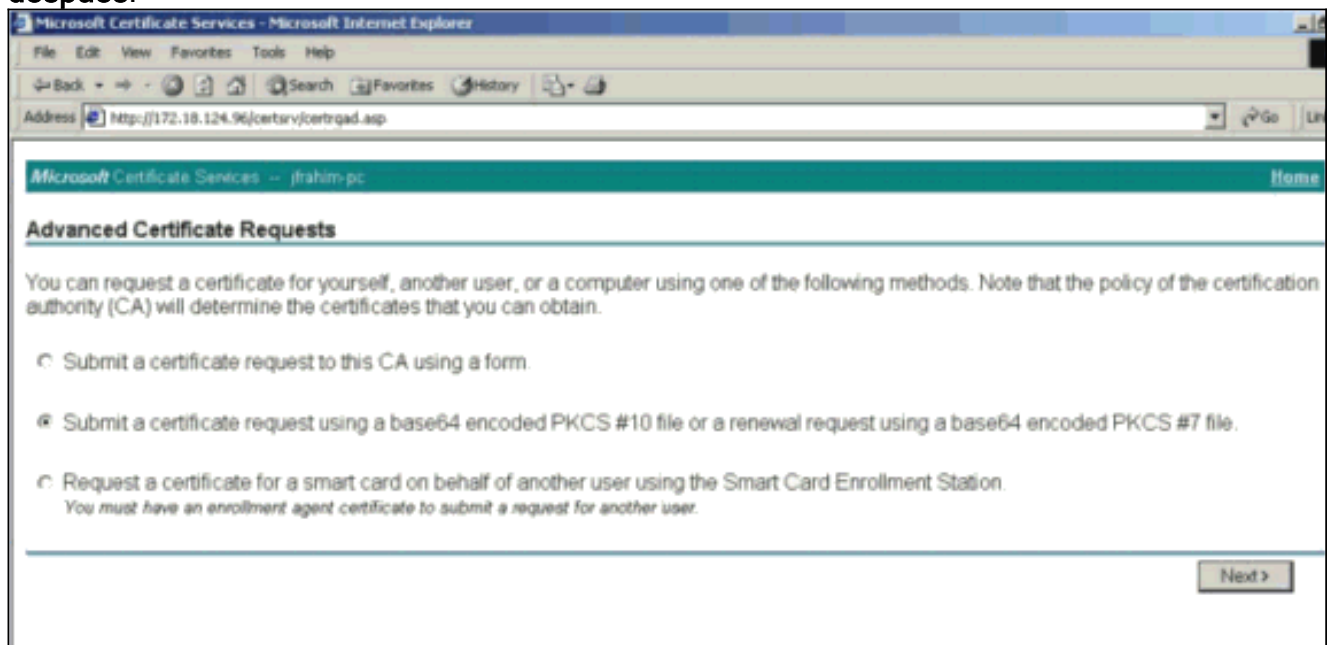
5. En su servidor del Certification Authority (CA), resalte la petición y péguela en su servidor de CA para someter su petición. Haga clic en Next (Siguiente).



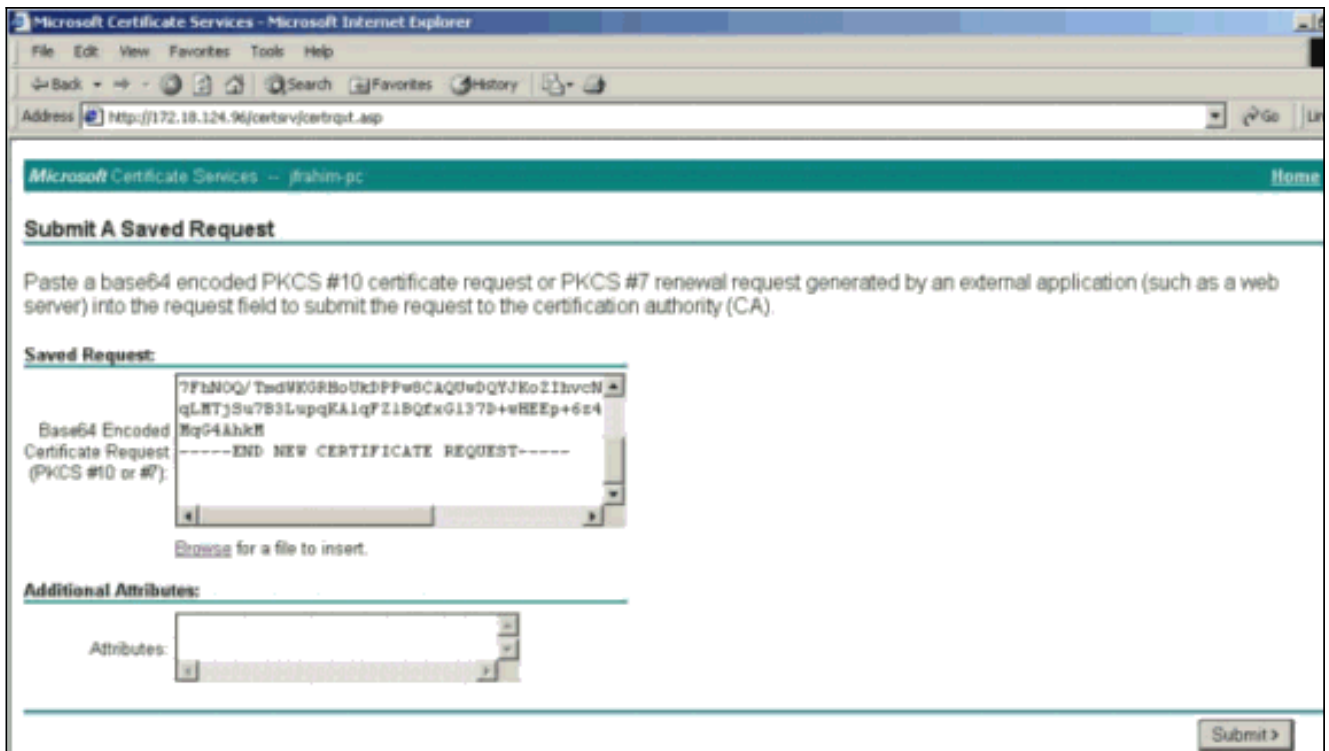
6. Seleccione el pedido avanzado y haga clic después.



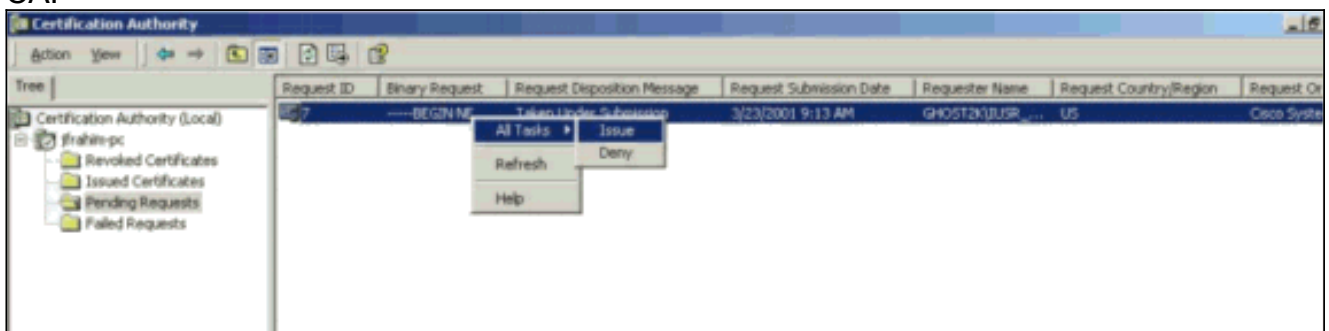
7. Selecto presente un pedido de certificado usando PKCS-10 un archivo codificado base64 o un pedido de renovación usando PKCS-7 un archivo codificado base64, y después haga clic después.



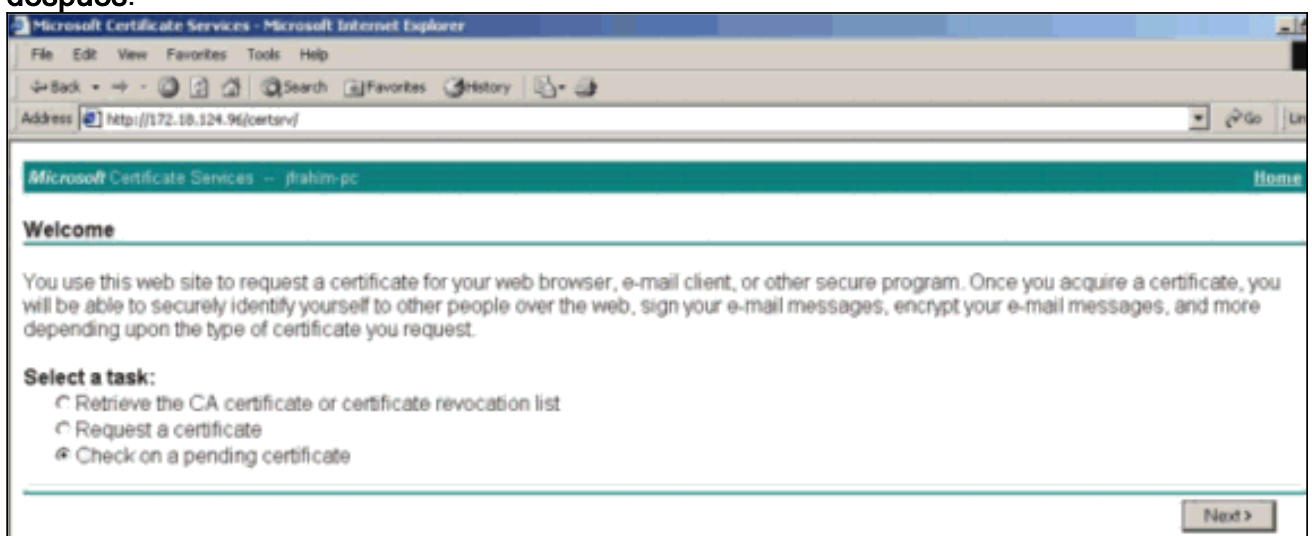
8. Corte y pegar su archivo PKCS en el campo de texto bajo sección del Saved Request. Entonces haga clic someten.



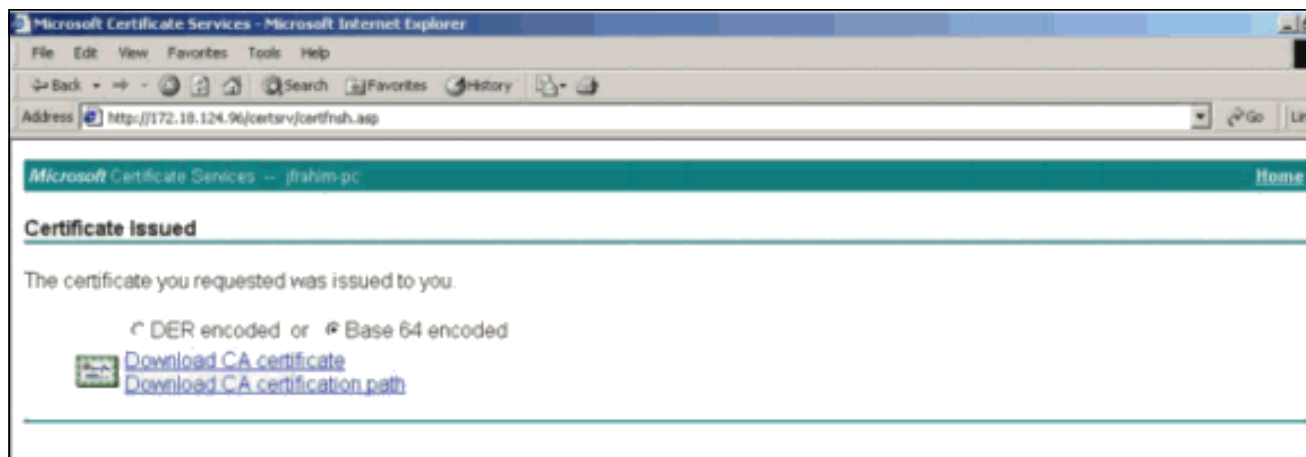
9. Publique el certificado de identidad en el servidor de CA.



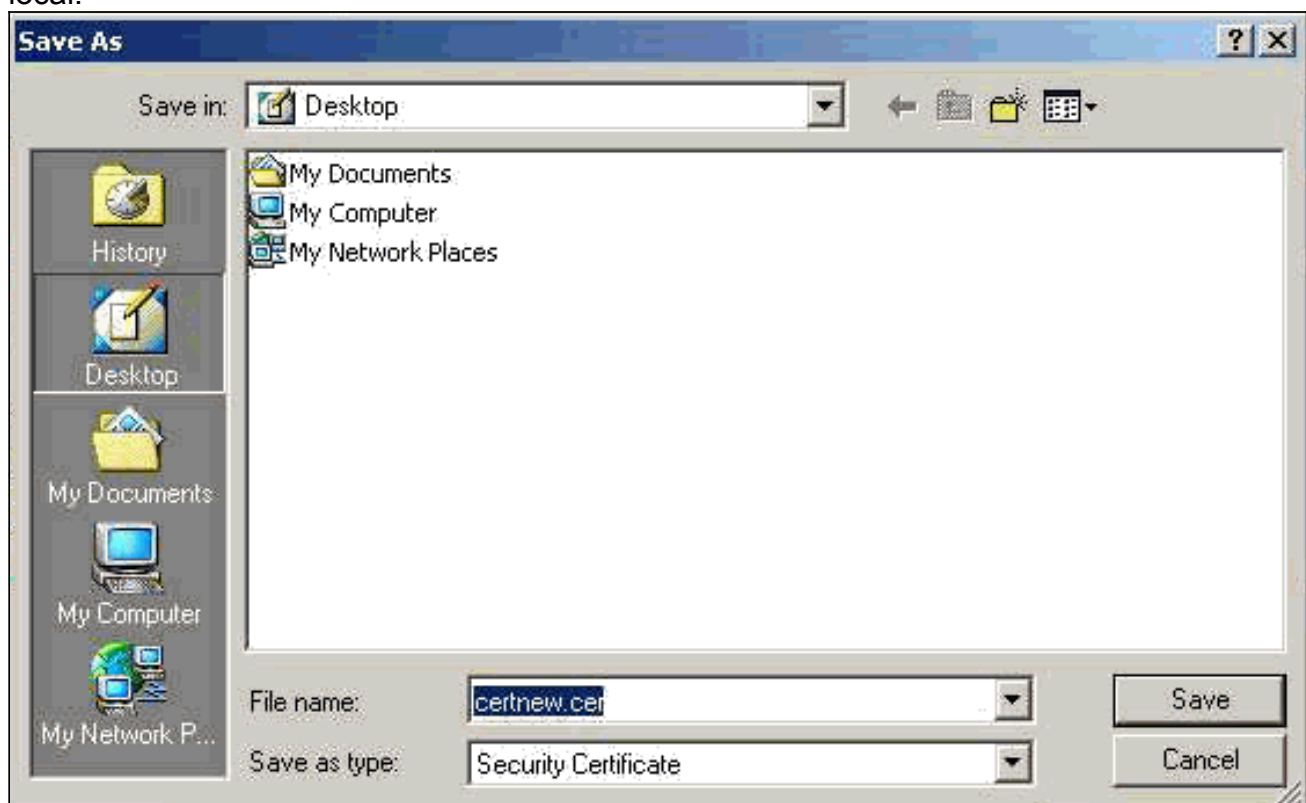
10. Descargue la raíz y los certificados de identidad. En su servidor de CA, seleccione el control en un certificado pendiente, y haga clic después.



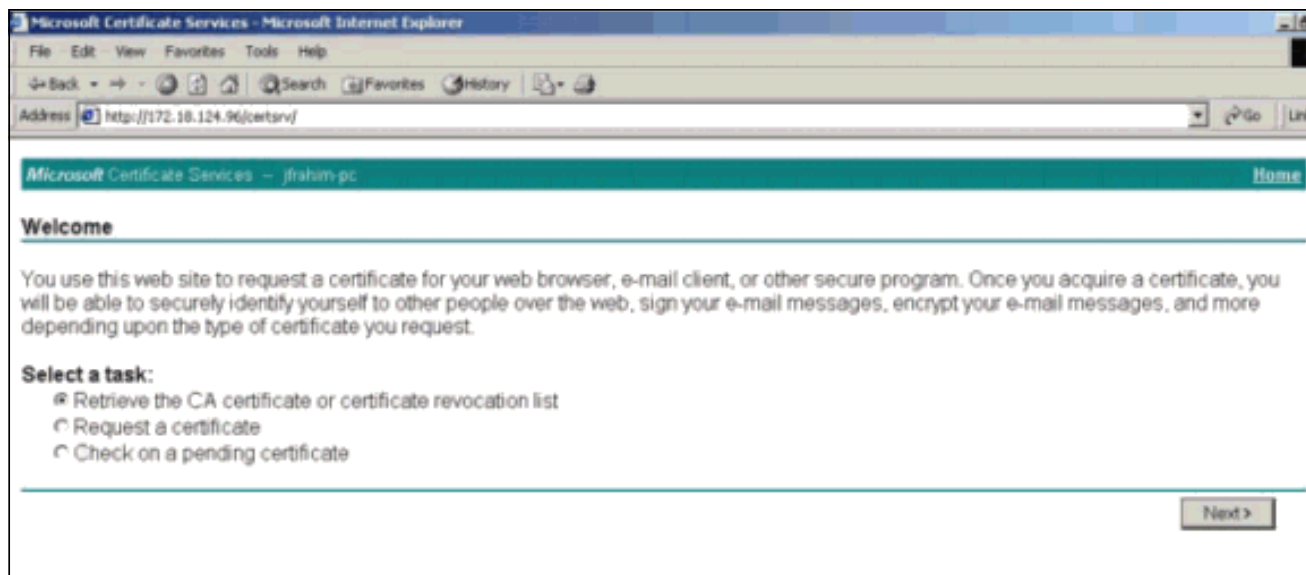
11. Seleccione el base 64 codificado, y haga clic el certificado de CA de la descarga en el servidor de CA.



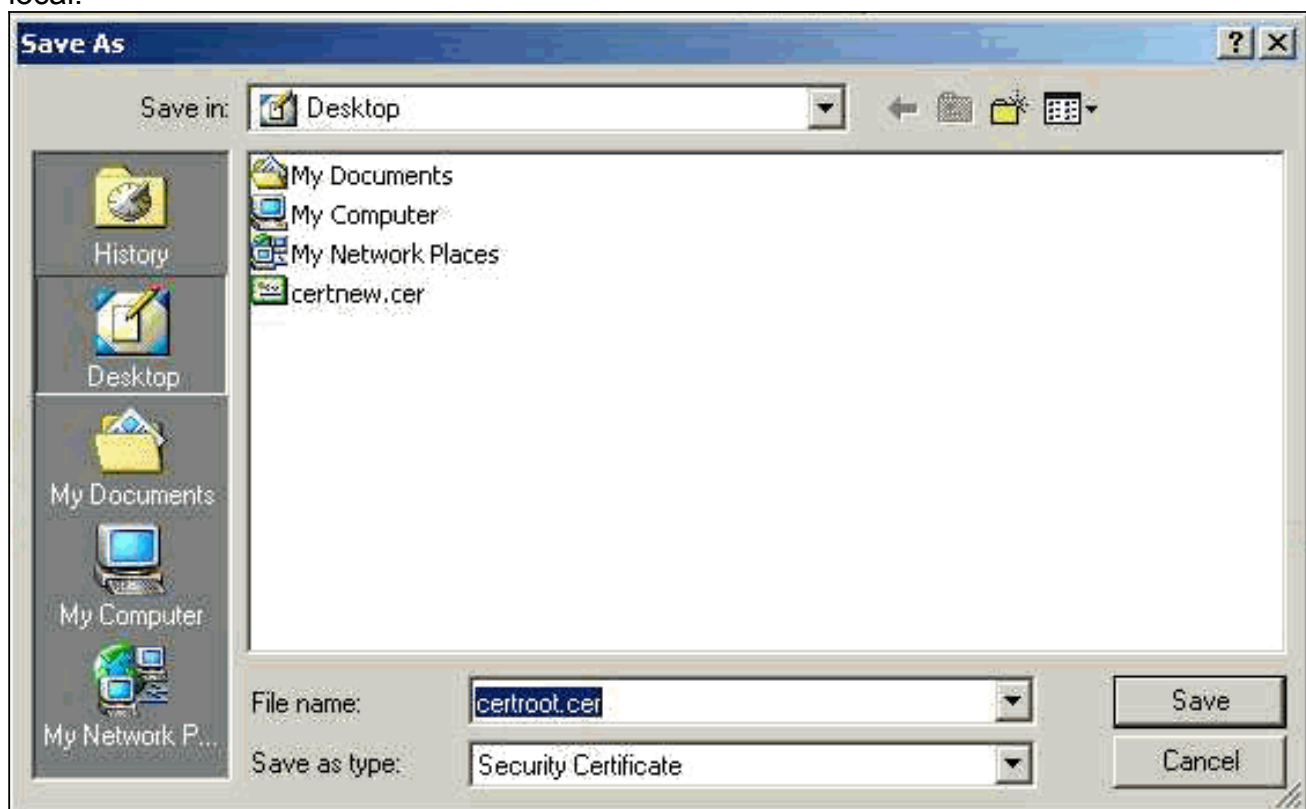
12. Salve el certificado de identidad en su unidad local.



13. En el servidor de CA, selecto **extraiga el certificado de CA o el Lista de revocación de certificados (CRL)** para conseguir el certificado raíz. Luego haga clic en Next (Siguiete).



14. Salve el certificado raíz en su unidad local.

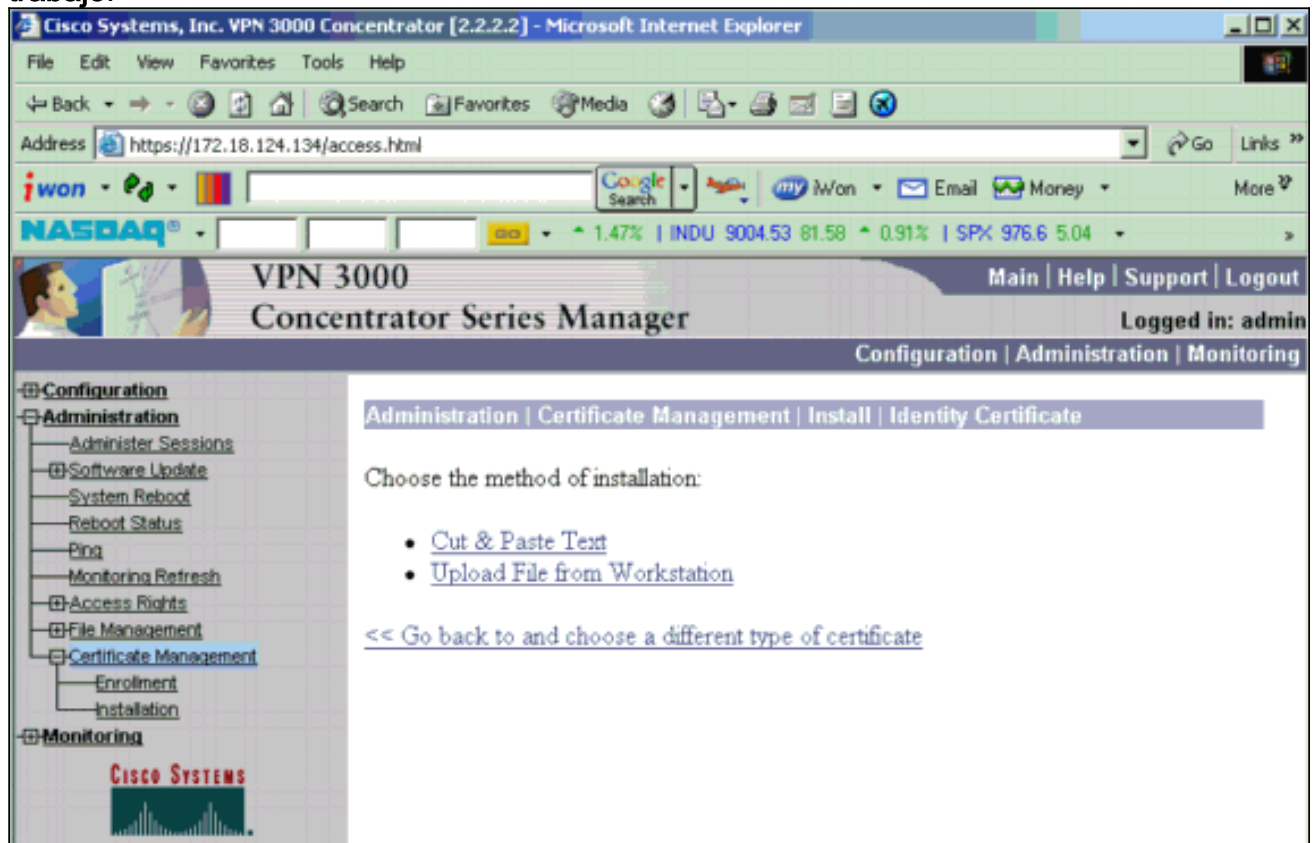


15. Instale la raíz y los certificados de identidad en el concentrador VPN 3000. Para hacer esto, la administración selecta > el **Certificate Manager** > la **instalación** > **instalan el certificado obtenido vía la inscripción**. Bajo estatus de la inscripción, el teclado **instala**.

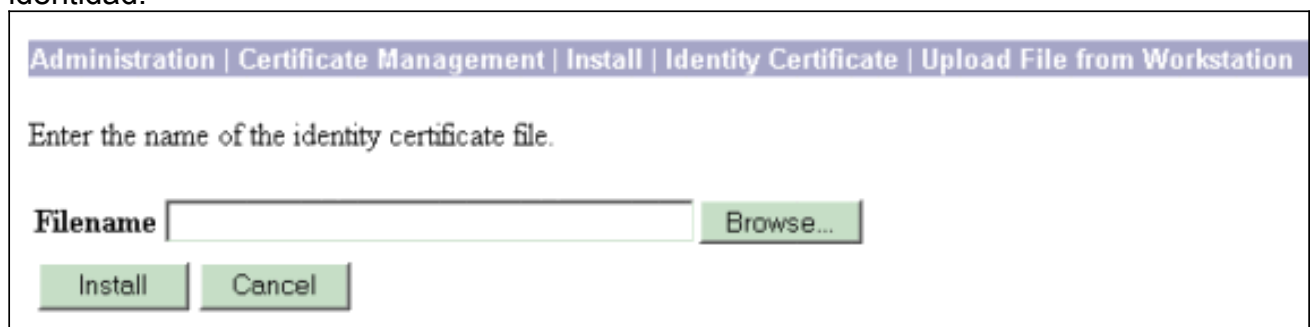


16. Archivo de la carga del teclado del puesto de

trabajo.



17. Haga clic **hojean** y seleccionan el archivo de certificado raíz que usted guardó a su unidad local. **Selecto instale** para instalar el certificado de identidad en el concentrador VPN. La administración | La ventana de la administración de certificados aparece como confirmación, y su nuevo certificado de identidad aparece en la tabla de los certificados de identidad.



Note: Complete estos pasos para generar un nuevo certificado si el certificado falla. Seleccione el **Administration (Administración) > Certificate Management (Administración de certificados)**. Haga clic la **cancelación** en el cuadro de las acciones para el anuncio del certificado SSL. Seleccione la **reinicialización de la administración > del sistema**. Seleccione la **salvaguardia la configuración activa en la época de la reinicialización, ahora elija, y el tecleo se aplica**. Usted puede ahora generar un nuevo certificado después de que la recarga sea completa.

[Instale los Certificados SSL en el concentrador VPN](#)

Si usted utiliza una conexión segura entre su navegador y el concentrador VPN, el concentrador VPN requiere un certificado SSL. Usted también necesita un certificado SSL en la interfaz que usted utiliza para manejar el concentrador VPN y para el WebVPN, y para cada interfaz que termine los túneles del WebVPN.

Los Certificados de la interfaz SSL, si son inexistentes, se generan automáticamente cuando las reinicializaciones concentradoras VPN 3000 después de que usted actualice el software concentrador VPN 3000. Porque uno mismo-se genera un certificado autofirmado, este certificado no es comprobable. Ningún Certificate Authority ha garantizado su identidad. Pero este certificado permite que usted haga el contacto inicial con el concentrador VPN usando el navegador. Si usted quiere substituirlo por otro certificado uno mismo-firmado SSL, complete estos pasos:

1. Elija el **Administration (Administración) > Certificate Management (Administración de certificados)**.

The screenshot shows the 'Administration | Certificate Management' page. It includes a navigation bar with the date 'Monday, 05 January 2004 16:31:1' and a 'Refresh' button. The main content area contains the following sections:

- Certificate Authorities** [View All CRL Caches | Clear All CRL Caches] (current: 1, maximum: 20)

Subject	Issuer	Expiration	SCEP Issuer	Actions
ms-root-sha-06-2001 at cisco	ms-root-sha-06-2001 at cisco	06/04/2022	No	View Configure Delete
- Identity Certificates** (current: 1, maximum: 20)

Subject	Issuer	Expiration	Actions
Gateway A at Cisco Systems	ms-root-sha-06-2001 at cisco	02/04/2004	View Renew Delete
- SSL Certificates**

Interface	Subject	Issuer	Expiration	Actions
Private	10.5.6.1 at Cisco Systems, Inc.	10.5.6.1 at Cisco Systems, Inc.	02/01/2006	View Renew Delete Export Generate Enroll Import
- SSH Host Key**

Key Size	Key Type	Date Generated	Actions
1024 bits	RSA	01/05/2004	Generate

2. El tecleo **genera** para visualizar el nuevo certificado en la tabla del certificado SSL y substituir el existencia. Esta ventana permite que usted configure los campos para el SSL certifica el concentrador VPN genera automáticamente. Estos Certificados SSL están para las interfaces y para el Equilibrio de carga.

The screenshot shows the 'Administration | Certificate Management | Generate SSL Certificate' dialog box. It contains the following information and fields:

- You are about to generate a certificate for the Public Interface . The certificate will have the following DN for both Subject and Issuer .
- The certificate will be valid for 3 years from yesterday.
- Common Name (CN)**: 10.86.194.175 (Enter the Common Name, usually the IP or DNS address of this interface)
- Organizational Unit (OU)**: VPN 3000 Concentrator (Enter the department.)
- Organization (O)**: Cisco Systems, Inc. (Enter the Organization or company.)
- Locality (L)**: Franklin (Enter the city or town.)
- State/Province (SP)**: Massachusetts (Enter the State or Province.)
- Country (C)**: US (Enter the two-letter country abbreviation (e.g. United States = US).)
- RSA Key Size**: 1024-bits (Select the key size for the generated RSA key pair.)
- Buttons: Generate, Cancel

Si usted quiere obtener un certificado comprobable SSL (es decir, uno publicado por un Certificate Authority), vea los [Certificados digitales del instalar en la sección del concentrador VPN de](#) este documento para utilizar el mismo procedimiento que usted utiliza para obtener

los certificados de identidad. Pero esta vez, en la ventana del **Administration (Administración) > Certificate Management (Administración de certificados) > Enroll (Registrar)**, certificado del teclado SSL (en vez del certificado de identidad). **Note:** Refiera a la *administración | Sección de administración de certificados del [volumen de referencia concentrador VPN 3000 II: La administración y la supervisión liberan 4.7](#)* para toda la información sobre los Certificados digitales y los Certificados SSL.

[Renueve los Certificados SSL en el concentrador VPN](#)

Esta sección describe cómo renovar los Certificados SSL:

Si esto está para el certificado SSL generado por el concentrador VPN, vaya al **Administration (Administración) > Certificate Management (Administración de certificados)** en la sección SSL. Haga clic la opción de la **renovación**, y eso renueva el certificado SSL.

Si esto está para un certificado concedido por un servidor externo de CA, complete estos pasos:

1. Elija el **>Delete del Administration (Administración) > Certificate Management (Administración de certificados)** conforme a los *Certificados SSL* para borrar los certificados vencidos de la interfaz pública.

Administration | Certificate Management Wednesday, 19 September 2007 00:01:4
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	pearlygates.ocp.org at pearlygates.ocp.org	Equifax Secure Certificate Aut... at Equifax	08/16/2008	View Renew Delete Export Generate Enroll Import



Tecleo **sí** para confirmar la cancelación del certificado SSL.

Subject

CN=pearlygates.ocp.org
 OU=Domain Control Validated - QuickSSL Premium(R)
 OU=See www.geotrust.com/resources/cps (c)07
 OU=GT94824223
 O=pearlygates.ocp.org
 C=US

Issuer

OU=Equifax Secure Certificate Authority
 O=Equifax
 C=US

Serial Number 07E267**Signing Algorithm** SHA1WithRSA**Public Key Type** RSA (1024 bits)**Certificate Usage** Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment**MD5 Thumbprint** 2C:EC:8D:8B:FE:59:9D:F8:04:A6:B2:1B:C5:09:9A:27**SHA1 Thumbprint** 6E:9A:7C:D3:02:FE:10:1C:75:79:00:AA:6A:73:84:54:C2:DC:BE:95**Validity** 8/16/2007 at 17:26:35 to 8/16/2008 at 17:26:35**CRL Distribution Point** http://crl.geotrust.com/crls/secureca.crlAre you **sure** you want to delete this certificate?

2. Elija el **Administration (Administración) > Certificate Management (Administración de certificados) > generar** para generar el nuevo certificado SSL.

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	No Certificate Installed.			Generate Enroll Import



El nuevo certificado SSL para la interfaz pública

aparece.

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](#)