

Configuration du concentrateur Cisco VPN 3000 version 4.7.x pour obtenir un certificat numérique et un certificat SSL

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Installer des certificats numériques sur le concentrateur VPN](#)

[Installer des certificats SSL sur le concentrateur VPN](#)

[Renouveler les certificats SSL sur le concentrateur VPN](#)

[Informations connexes](#)

[Introduction](#)

Ce document inclut des instructions détaillées sur la façon de configurer les concentrateurs de la gamme Cisco VPN 3000 pour s'authentifier à l'aide de certificats numériques ou d'identité et de certificats SSL.

Remarque : Dans le concentrateur VPN, l'équilibrage de charge doit être désactivé avant de générer un autre certificat SSL, car cela empêche la génération du certificat.

Référez-vous à [Comment obtenir un certificat numérique d'une autorité de certification Microsoft Windows utilisant ASDM sur un ASA](#) afin d'en savoir plus sur le même scénario avec PIX/ASA 7.x.

Référez-vous à [Exemple de configuration de l'inscription des certificats Cisco IOS à l'aide des commandes d'inscription avancées](#) afin d'en savoir plus sur le même scénario avec les plateformes Cisco IOS®.

[Conditions préalables](#)

[Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

[Components Used](#)

Les informations de ce document sont basées sur le concentrateur Cisco VPN 3000 qui exécute la version 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.

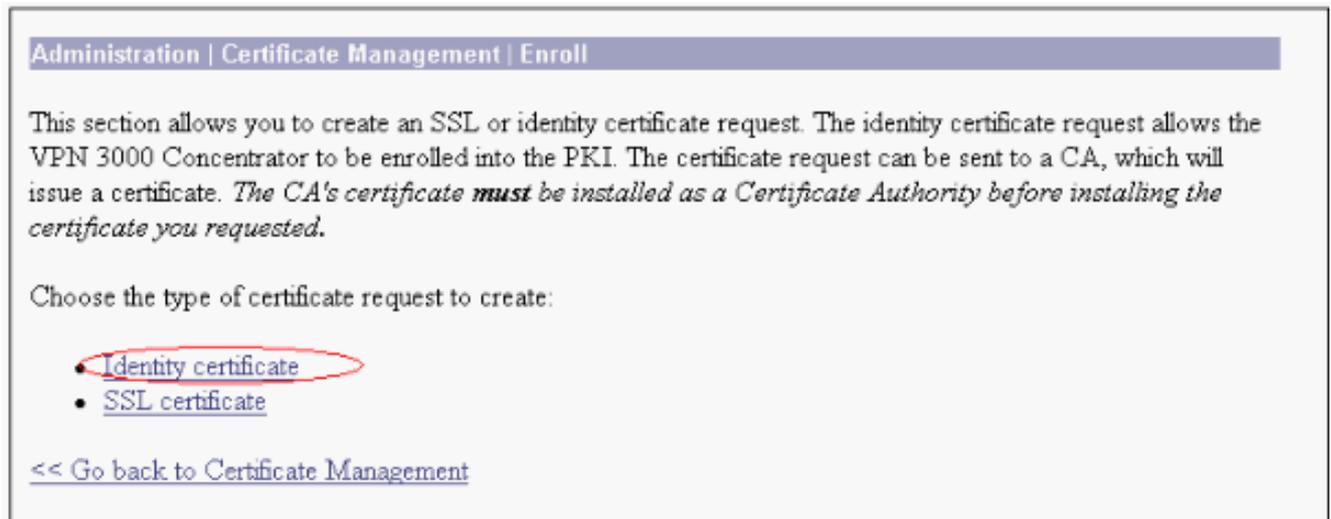
Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

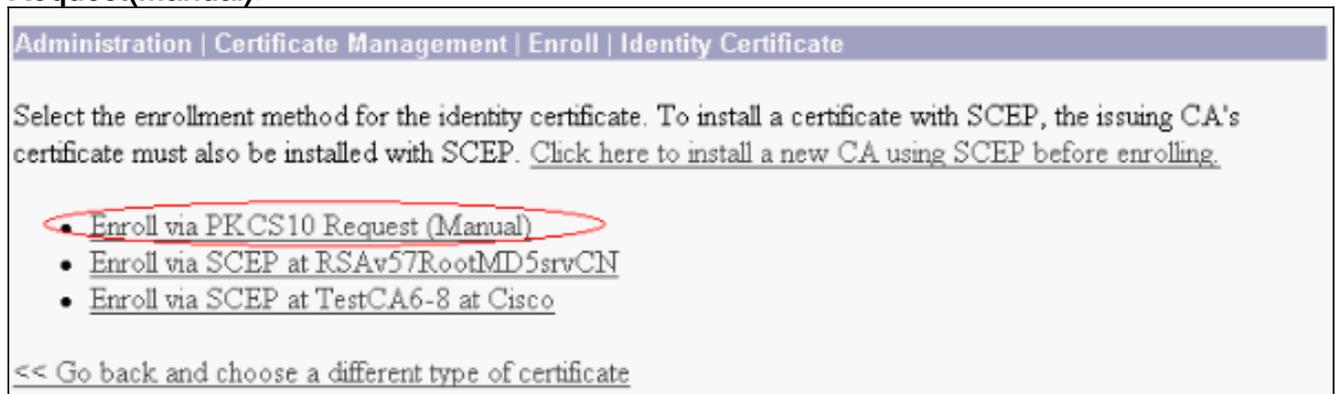
Installer des certificats numériques sur le concentrateur VPN

Procédez comme suit :

1. Choisissez **Administration > Certificate Management > Enroll** afin de sélectionner la demande de certificat numérique ou d'identité.



2. Choisissez **Administration > Certificate Management > Enrollment > Identity Certificate** et cliquez sur **Enroll via PKCS10 Request(Manual)**.



3. Remplissez les champs demandés, puis cliquez sur **S'inscrire**. Ces champs sont remplis dans cet exemple. **Nom commun** : altiga30 **Unité organisationnelle** - IPSECCERT (l'unité d'organisation doit correspondre au nom de groupe IPsec configuré) **Organisation** - Cisco Systems **Localité** : RTP **État/Province**—Caroline du Nord **Pays**—États-Unis **Nom de domaine complet** - (non utilisé ici) **Taille de clé**—512 **Remarque** : Si vous demandez un certificat SSL ou un certificat d'identité à l'aide du protocole SCEP (Simple Certificate Enrollment Protocol),

ce sont les seules options RSA disponibles. RSA 512 bits RSA 768 bits RSA 1024 bits RSA 2048 bits DSA 512 bits DSA 768 bits DSA 1024 bits

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. Après avoir cliqué sur **S'inscrire**, plusieurs fenêtres s'affichent. La première fenêtre confirme que vous avez demandé un certificat.

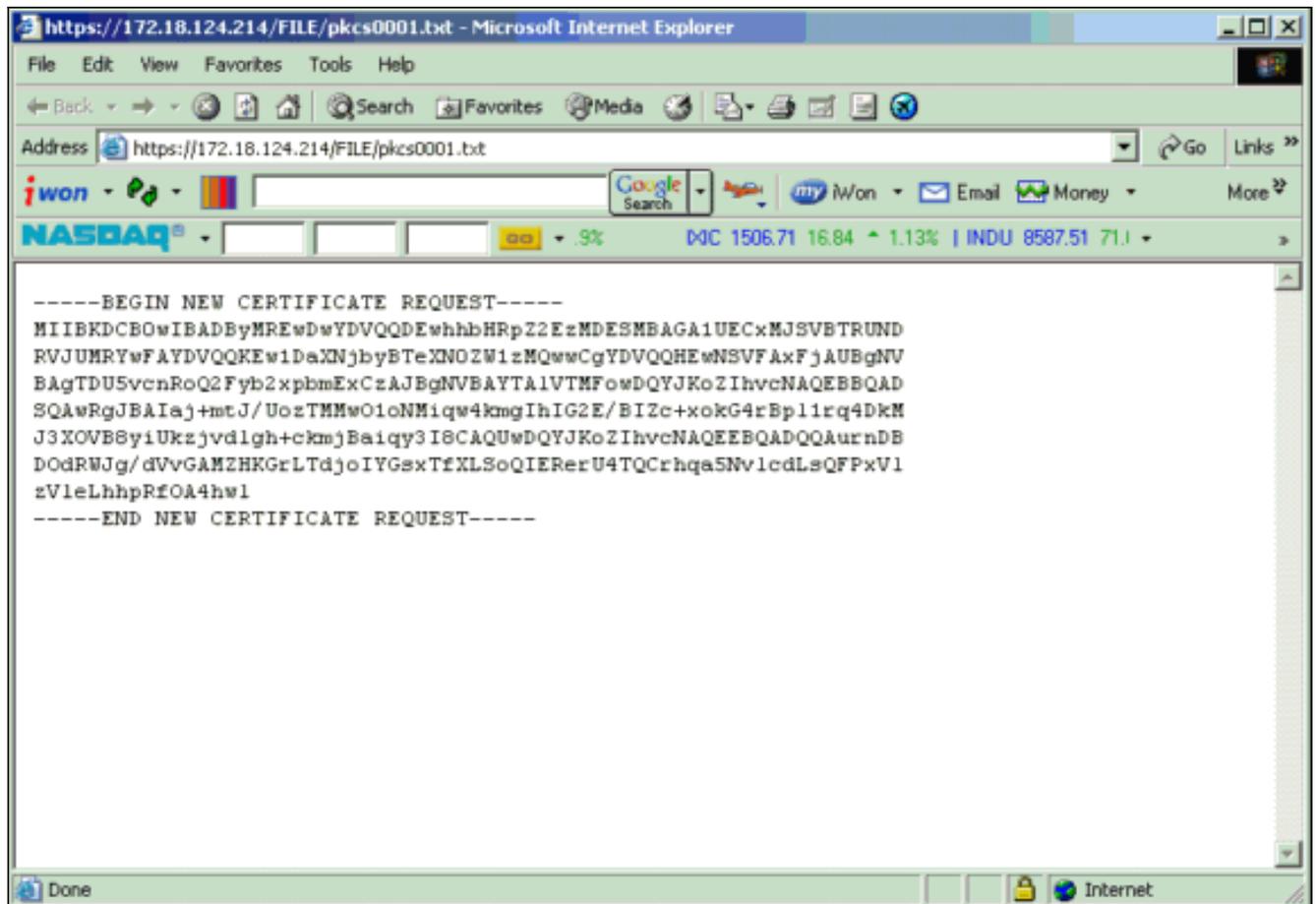
Administration | Certificate Management | Enrollment | Request Generated

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.

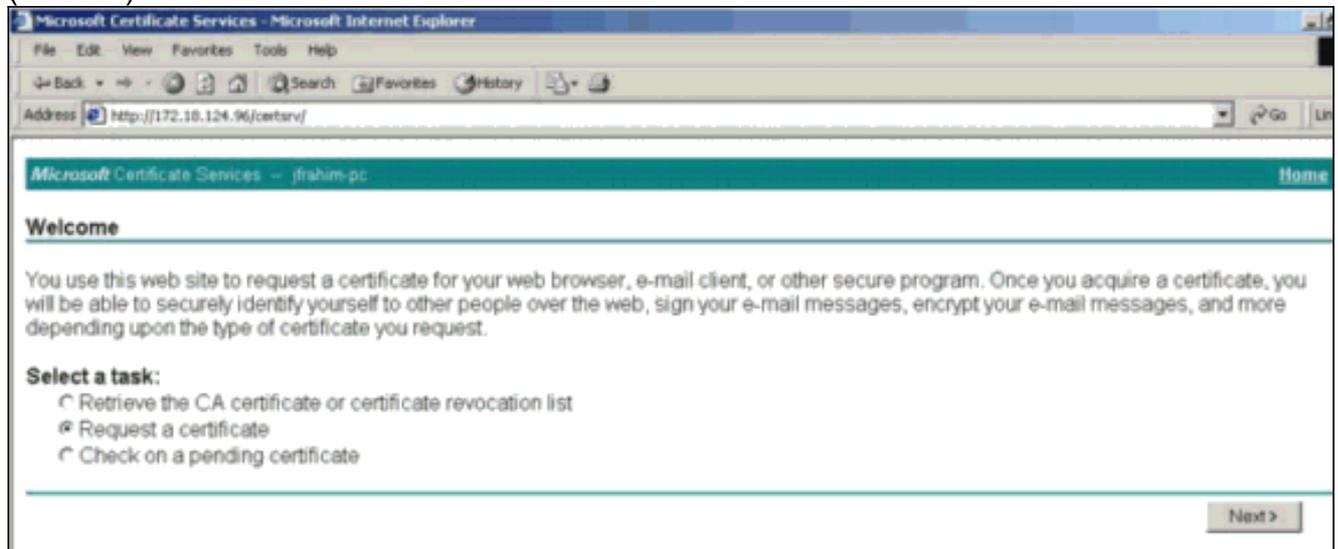
The request is located on the VPN 3000 Concentrator with the filename **pkcs0001.txt** . When you are done, you should delete this file, go to the [File Management page](#) to delete the certificate request.

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

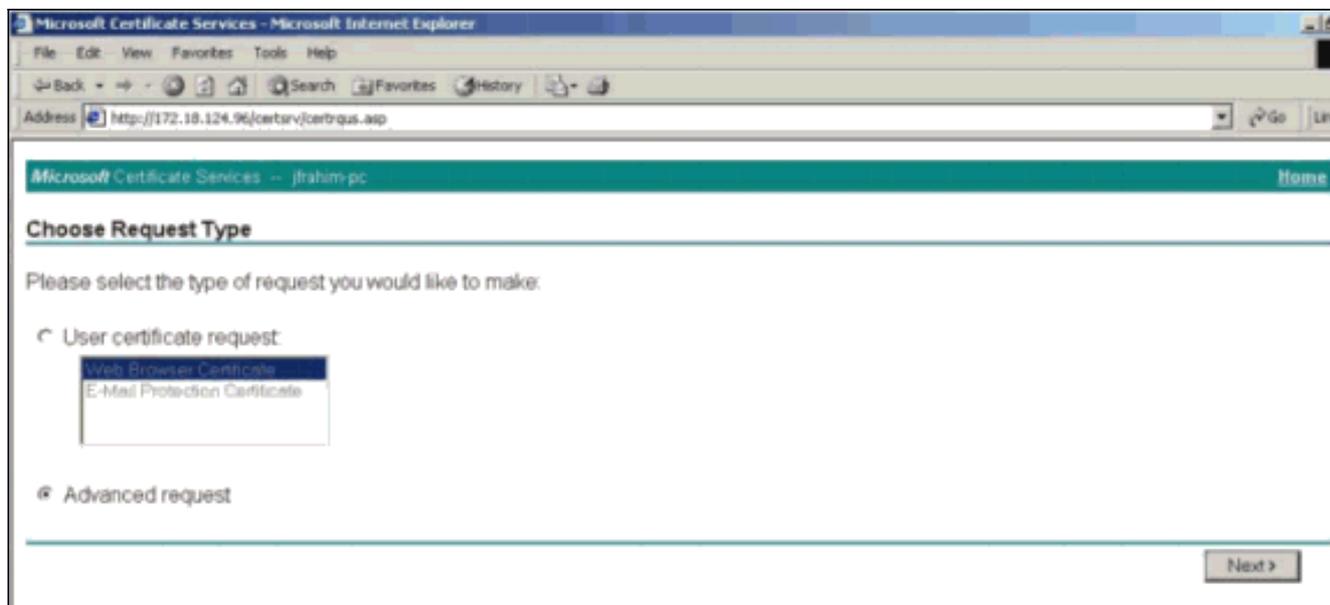
Une nouvelle fenêtre de navigateur s'ouvre également et affiche votre fichier de demande PKCS.



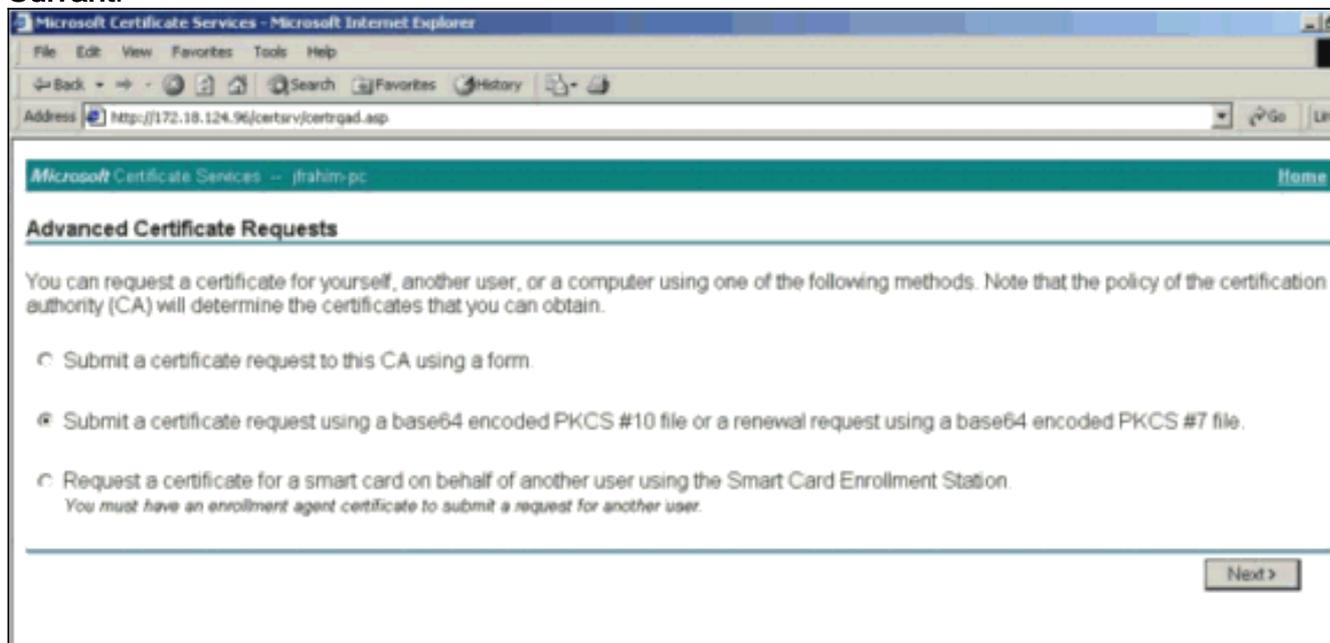
5. Sur votre serveur d'autorité de certification, mettez en surbrillance la demande et collez-la dans votre serveur d'autorité de certification afin d'envoyer votre demande. Cliquez sur **Next** (Suivant).



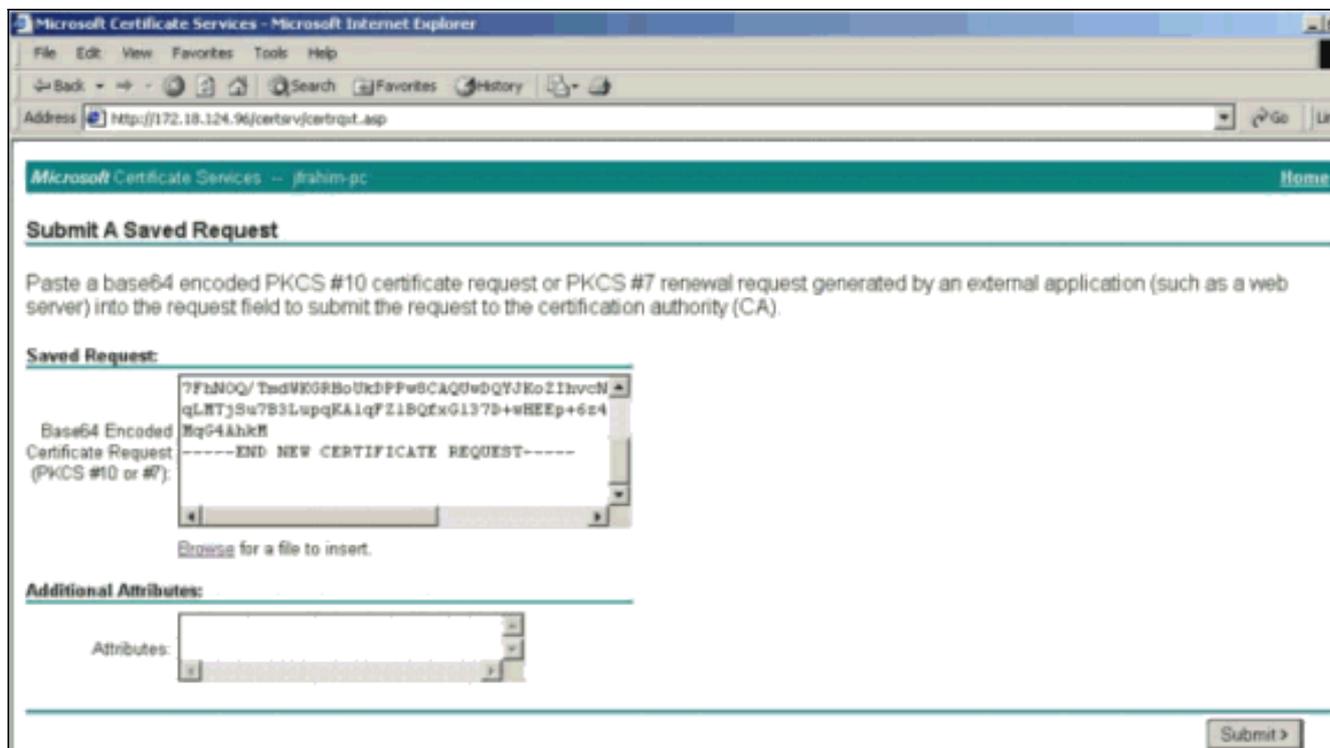
6. Sélectionnez **Demande avancée** et cliquez sur **Suivant**.



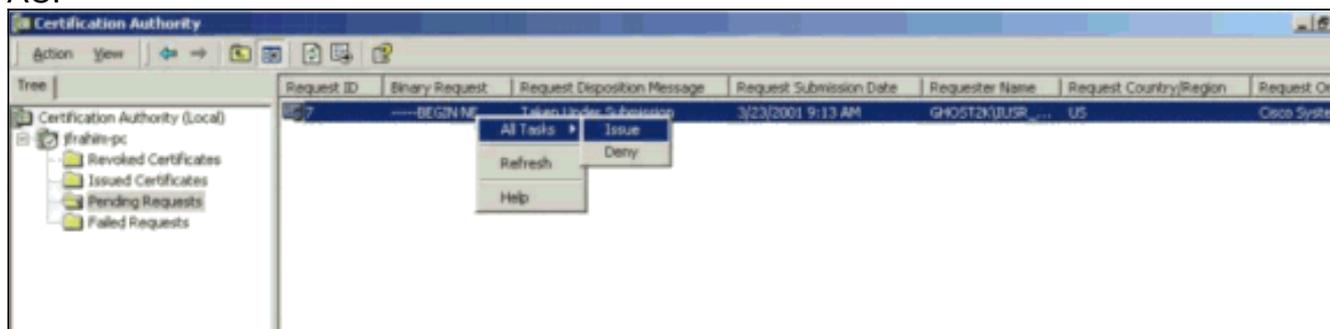
7. Sélectionnez **Soumettre une demande de certificat à l'aide d'un fichier PKCS #10 codé en base64** ou d'une demande de renouvellement à l'aide d'un fichier PKCS #7 codé en base64, puis cliquez sur **Suivant**.



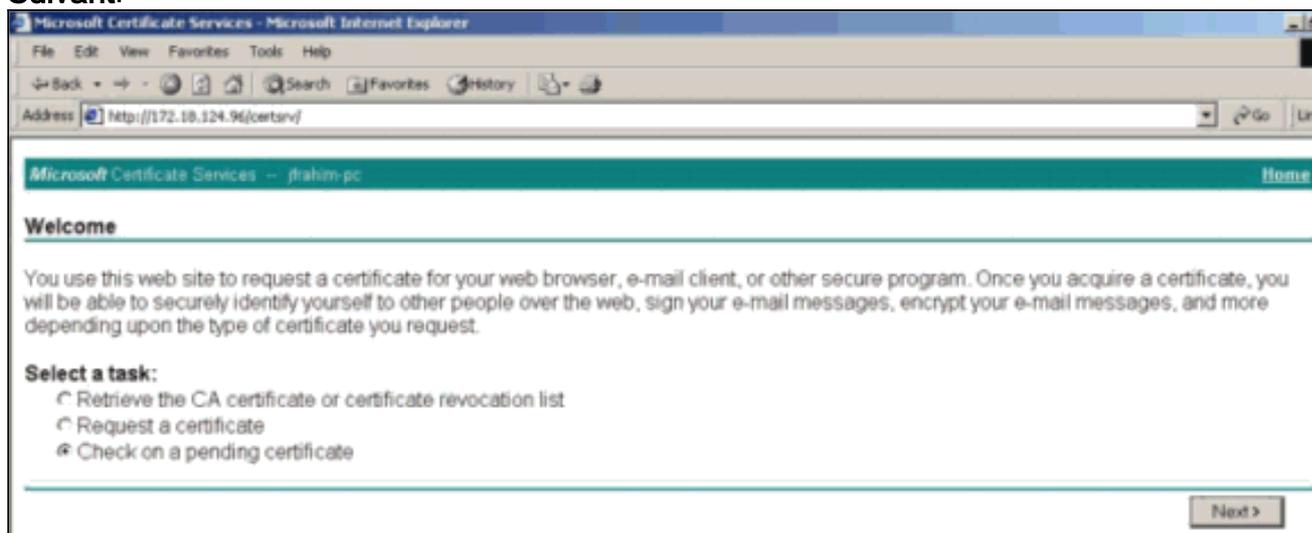
8. Coupez et collez votre fichier PKCS dans le champ de texte sous la section Requête enregistrée. Cliquez ensuite sur **Soumettre**.



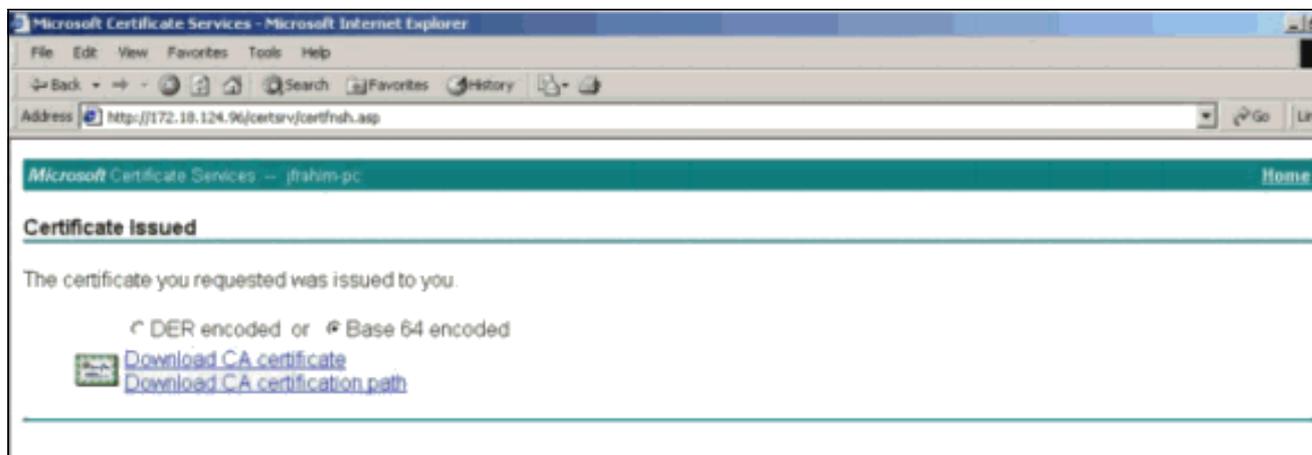
9. Émettez le certificat d'identité sur le serveur AC.



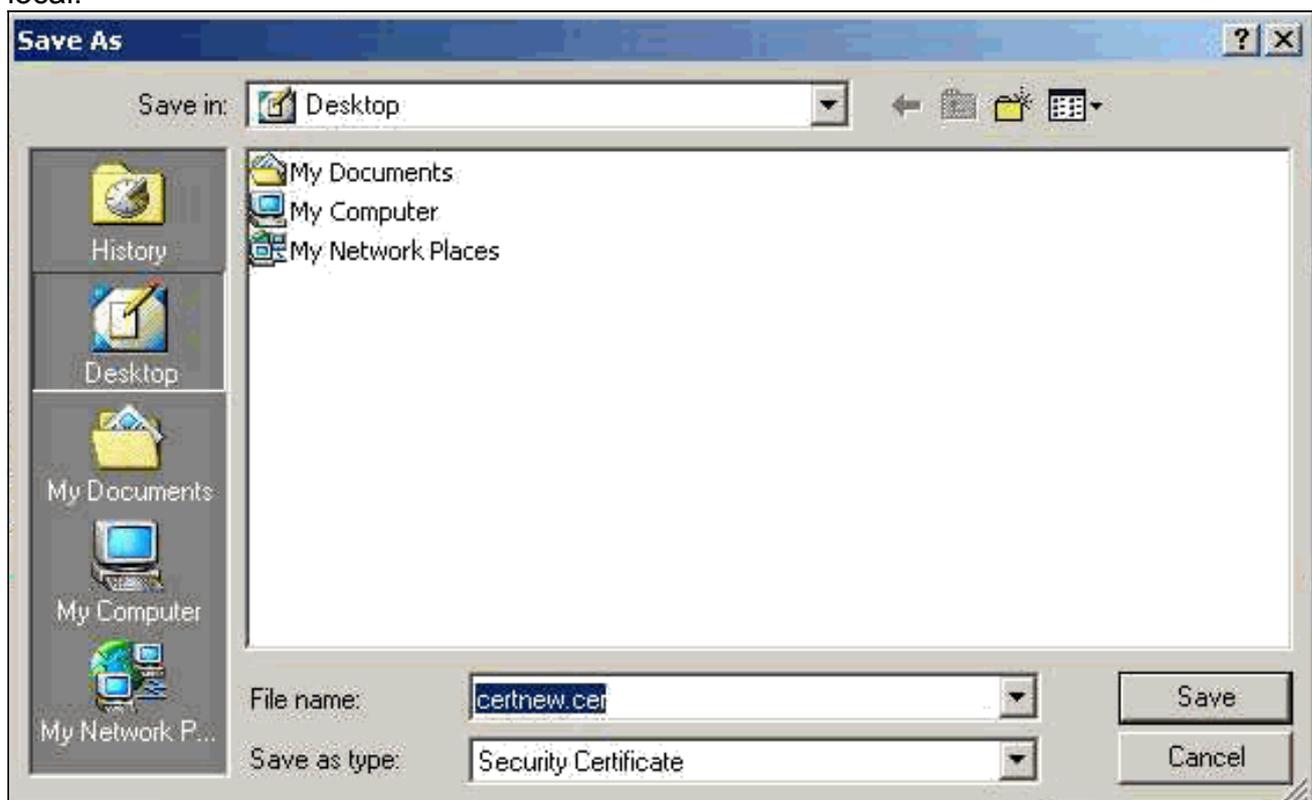
10. Téléchargez la racine et les certificats d'identité. Sur votre serveur AC, sélectionnez **Vérifier un certificat en attente**, puis cliquez sur **Suivant**.



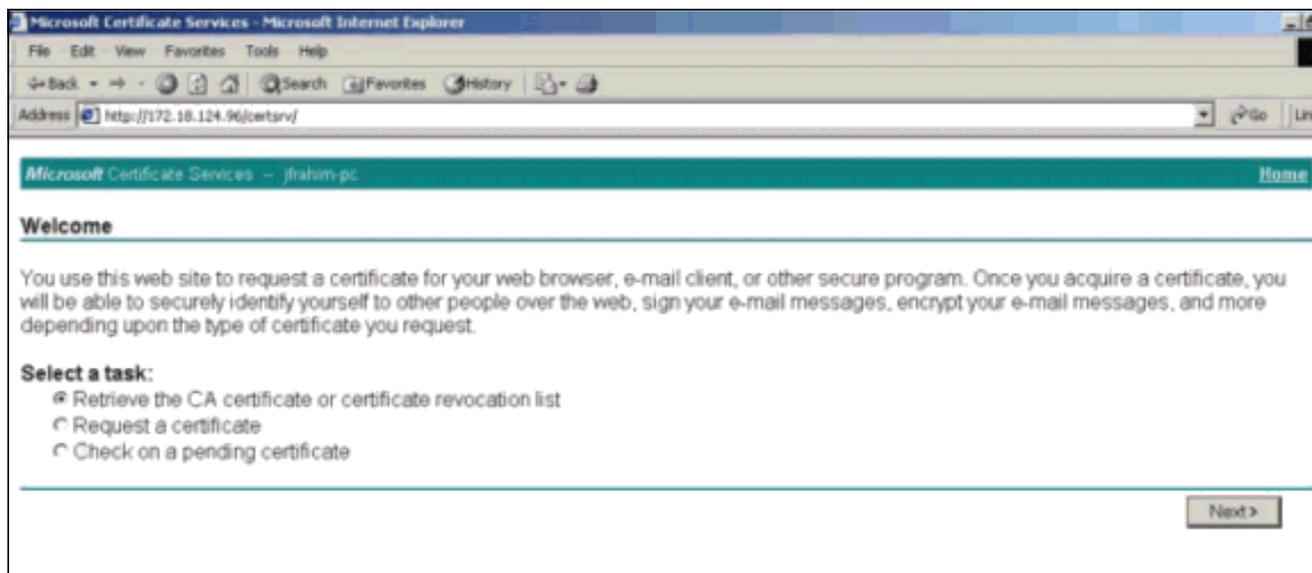
11. Sélectionnez **Codé Base 64**, puis cliquez sur **Télécharger le certificat d'Autorité de certification** sur le serveur d'Autorité de certification.



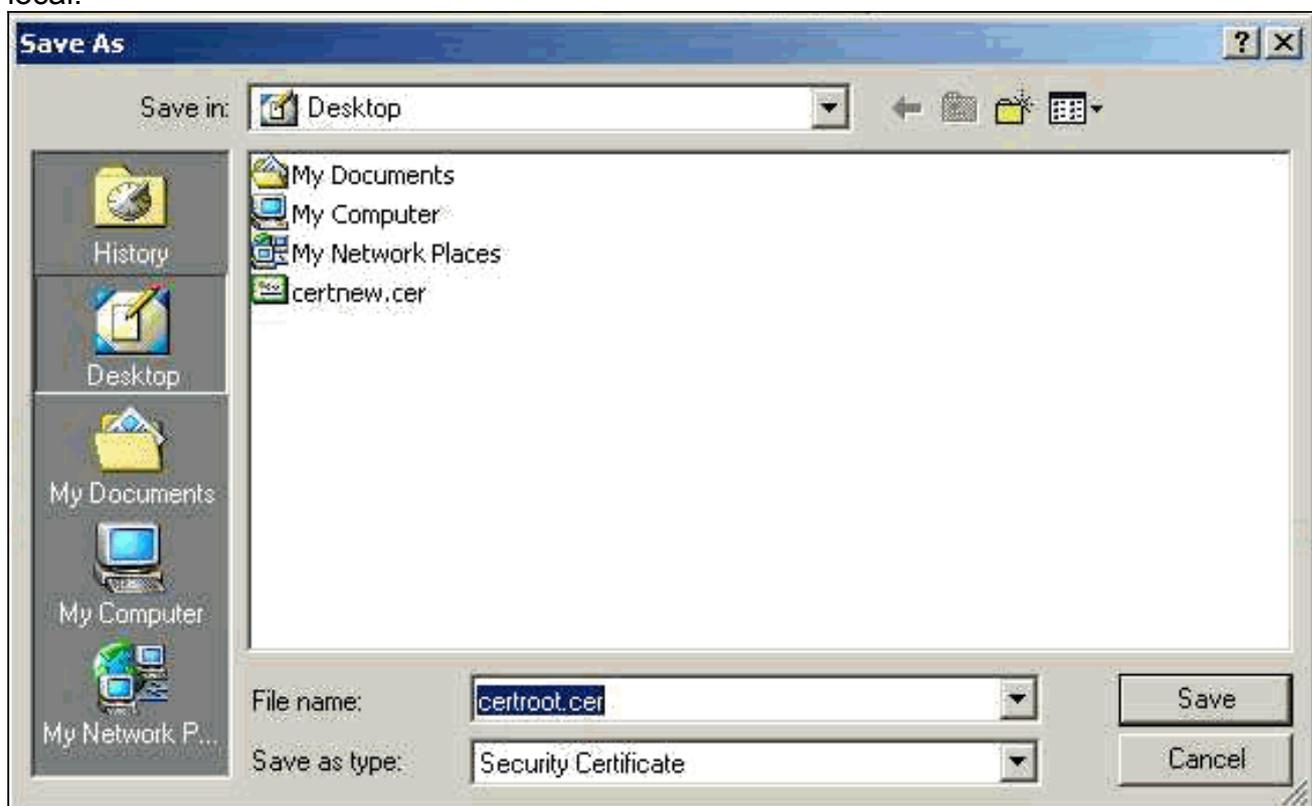
12. Enregistrez le certificat d'identité sur votre lecteur local.



13. Sur le serveur d'autorité de certification, sélectionnez **Récupérer le certificat d'autorité de certification** ou **la liste de révocation de certificat** afin d'obtenir le certificat racine. Cliquez ensuite **Next**.



14. Enregistrez le certificat racine sur votre lecteur local.

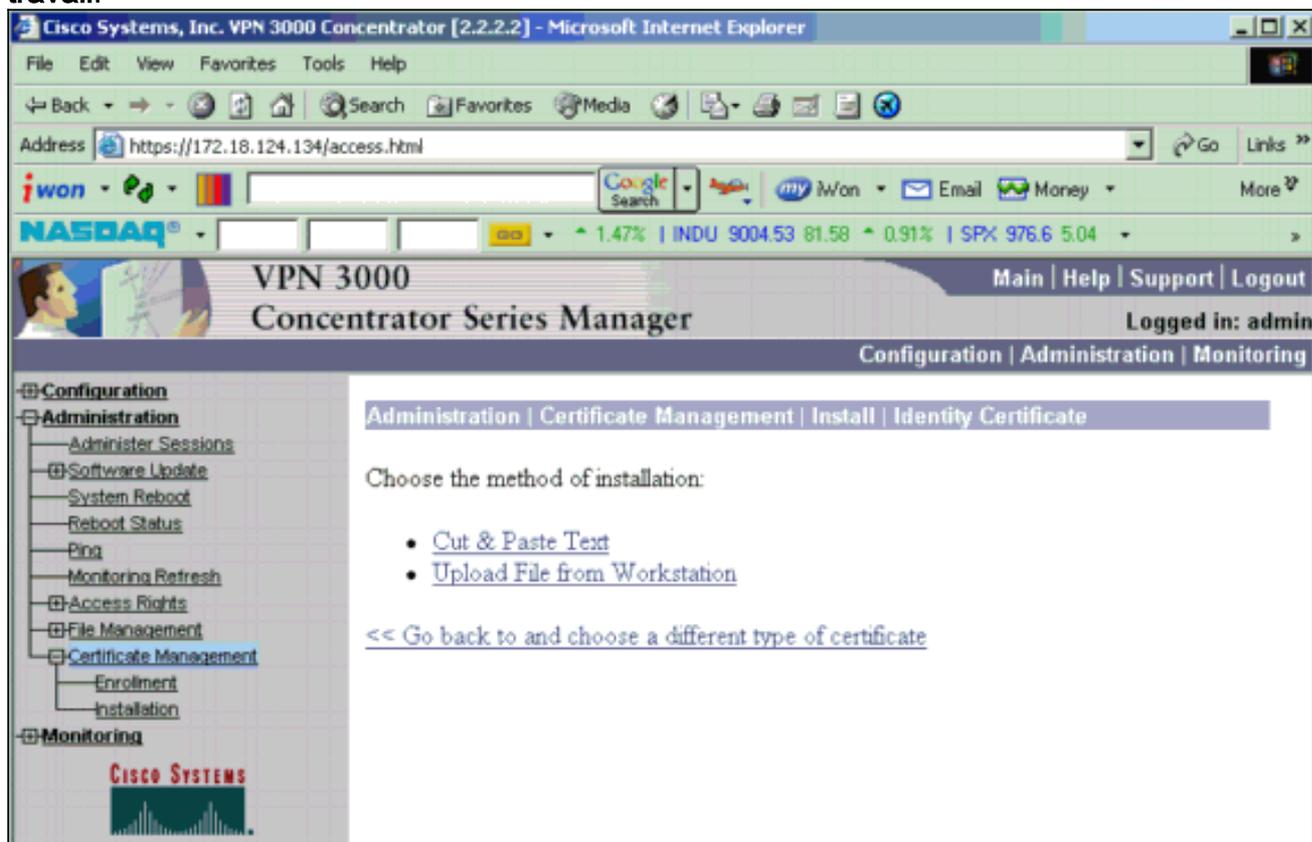


15. Installez les certificats racine et d'identité sur le concentrateur VPN 3000. Pour ce faire, sélectionnez **Administration > Certificate Manager > Installation > Install certificate obtenu par inscription**. Sous État de l'inscription, cliquez sur **Installer**.

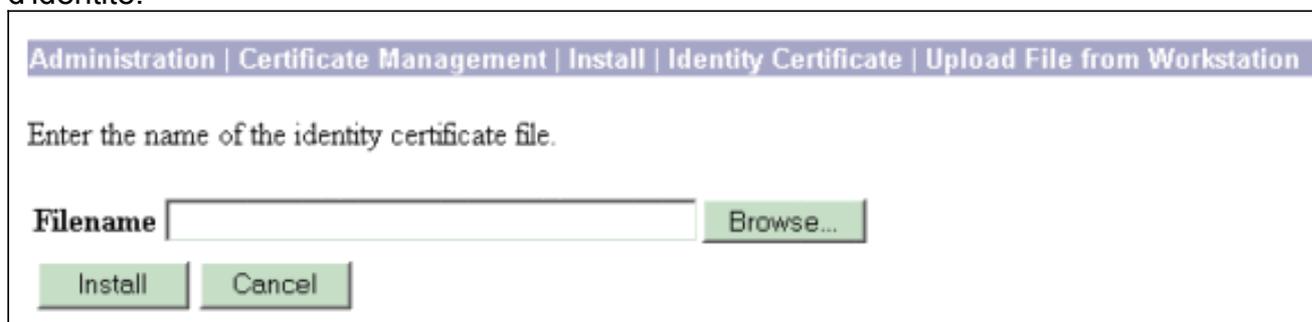


16. Cliquez sur **Télécharger le fichier à partir de la station de**

travail.



17. Cliquez sur **Parcourir** et sélectionnez le fichier de certificat racine que vous avez enregistré sur votre lecteur local. Sélectionnez **Installer** pour installer le certificat d'identité sur le concentrateur VPN. L'administration | La fenêtre Gestion des certificats apparaît sous forme de confirmation et votre nouveau certificat d'identité apparaît dans le tableau Certificats d'identité.



Remarque : Complétez ces étapes pour générer un nouveau certificat en cas d'échec du certificat. Sélectionnez **Administration > Gestion des certificats**. Cliquez sur **Supprimer** dans la zone Actions de la liste des certificats SSL. Sélectionnez **Administration > Redémarrage du système**. Sélectionnez **Enregistrer la configuration active au moment du redémarrage**, choisissez **Maintenant**, puis cliquez sur **Appliquer**. Vous pouvez désormais générer un nouveau certificat une fois le rechargement terminé.

[Installer des certificats SSL sur le concentrateur VPN](#)

Si vous utilisez une connexion sécurisée entre votre navigateur et le concentrateur VPN, le concentrateur VPN nécessite un certificat SSL. Vous avez également besoin d'un certificat SSL sur l'interface que vous utilisez pour gérer le concentrateur VPN et pour WebVPN, et pour chaque interface qui termine les tunnels WebVPN.

Les certificats SSL d'interface, s'ils n'existent pas, sont générés automatiquement lorsque le concentrateur VPN 3000 redémarre après la mise à niveau du logiciel du concentrateur VPN 3000. Comme un certificat auto-signé est auto-généré, ce certificat n'est pas vérifiable. Aucune autorité de certification n'a garanti son identité. Mais ce certificat vous permet d'établir un premier contact avec le concentrateur VPN à l'aide du navigateur. Si vous souhaitez le remplacer par un autre certificat SSL autosigné, procédez comme suit :

1. Choisissez **Administration > Certificate Management**.

The screenshot shows the 'Administration | Certificate Management' page. At the top right, it displays 'Monday, 05 January 2004 16:31:1' and a 'Refresh' button. Below the header, there is a description: 'This section lets you view and manage certificates on the VPN 3000 Concentrator.' followed by two links: 'Click here to enroll with a Certificate Authority' and 'Click here to install a certificate'.

The 'Certificate Authorities' section shows a table with columns: Subject, Issuer, Expiration, SCEP Issuer, and Actions. One entry is visible: 'ms-root-sha-06-2001 at cisco' with an expiration of '06/04/2022' and 'No' for SCEP Issuer.

The 'Identity Certificates' section shows a table with columns: Subject, Issuer, Expiration, and Actions. One entry is visible: 'Gateway A at Cisco Systems' with an expiration of '02/04/2004'.

The 'SSL Certificates' section shows a table with columns: Interface, Subject, Issuer, Expiration, and Actions. One entry is visible: 'Private' interface with subject '10.5.6.1 at Cisco Systems, Inc.' and expiration '02/01/2006'. The 'Generate' link in the Actions column is circled in red.

The 'SSH Host Key' section shows a table with columns: Key Size, Key Type, Date Generated, and Actions. One entry is visible: '1024 bits' key size, 'RSA' key type, and '01/05/2004' date generated.

2. Cliquez sur **Generate** afin d'afficher le nouveau certificat dans la table de certificats SSL et de remplacer le certificat existant. Cette fenêtre vous permet de configurer des champs pour les certificats SSL que le concentrateur VPN génère automatiquement. Ces certificats SSL sont destinés aux interfaces et à l'équilibrage de charge.

The screenshot shows the 'Administration | Certificate Management | Generate SSL Certificate' window. It contains the following text: '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.'

The configuration fields are as follows:

- Common Name (CN):** 10.86.194.175 (Instruction: Enter the Common Name, usually the IP or DNS address of this interface)
- Organizational Unit (OU):** VPN 3000 Concentrator (Instruction: Enter the department.)
- Organization (O):** Cisco Systems, Inc. (Instruction: Enter the Organization or company.)
- Locality (L):** Franklin (Instruction: Enter the city or town.)
- State/Province (SP):** Massachusetts (Instruction: Enter the State or Province.)
- Country (C):** US (Instruction: Enter the two-letter country abbreviation (e.g. United States = US).)
- RSA Key Size:** 1024-bits (Instruction: Select the key size for the generated RSA key pair.)

At the bottom, there are 'Generate' and 'Cancel' buttons.

Si vous voulez obtenir un certificat SSL vérifiable (c'est-à-dire un certificat délivré par une autorité de certification), consultez la section [Installer des certificats numériques sur le concentrateur VPN](#) de ce document afin d'utiliser la même procédure que celle que vous

utilisez pour obtenir des certificats d'identité. Mais cette fois, dans la fenêtre **Administration > Certificate Management > Enroll**, cliquez sur **SSL certificate** (au lieu de Identity Certificate). **Remarque** : reportez-vous à la section *Administration / Section Gestion des certificats* du [Concentrateur VPN 3000 Référence Volume II : Administration et surveillance version 4.7](#) pour obtenir des informations complètes sur les certificats numériques et les certificats SSL.

Renouveler les certificats SSL sur le concentrateur VPN

Cette section décrit comment renouveler les certificats SSL :

S'il s'agit du certificat SSL généré par le concentrateur VPN, accédez à **Administration > Certificate Management** dans la section SSL. Cliquez sur l'option de renouvellement, qui renouvelle le certificat SSL.

S'il s'agit d'un certificat délivré par un serveur AC externe, procédez comme suit :

1. Choisissez **Administration > Certificate Management > Delete** sous *SSL Certificates* afin de supprimer les certificats expirés de l'interface publique.

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



Cliquez sur **Oui** afin de confirmer la suppression du certificat 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.crl

Are you **sure** you want to delete this certificate?

2. Choisissez **Administration > Certificate Management > Generate** afin de générer le nouveau certificat 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



Le nouveau certificat SSL pour l'interface publique

apparaît.

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

[Informations connexes](#)

- [Page d'assistance des concentrateurs VPN Cisco 3000](#)
- [Négociation IPSec/Protocoles IKE](#)
- [Support et documentation techniques - Cisco Systems](#)