

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](#)

[Composants utilisés](#)

[Conventions](#)

[Installez les Certificats numériques sur le concentrateur VPN](#)

[Installez les Certificats SSL sur le concentrateur VPN](#)

[Renouvelez les Certificats SSL sur le concentrateur VPN](#)

[Informations connexes](#)

Introduction

Ce document comporte des instructions pas à pas sur la façon dont configurer les Concentrateurs de la gamme Cisco VPN 3000 authentifier avec l'utilisation de numérique ou des certificats d'identité et des Certificats SSL.

Note: Dans le concentrateur VPN, l'Équilibrage de charge doit être désactivé avant que vous génériez un autre certificat ssl puisque ceci empêche la génération de certificat.

Référez-vous à [comment obtenir un certificat numérique de Microsoft Windows CA utilisant l'ASDM sur une ASA](#) afin d'apprendre un scénario plus à peu près identique avec PIX/ASA 7.x.

Référez-vous à [l'inscription de certificat de Cisco IOS utilisant l'exemple amélioré de configuration de commandes d'inscription](#) afin d'apprendre un scénario plus à peu près identique avec des Plateformes de Cisco IOS®.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur le concentrateur de Cisco VPN 3000 qui exécute la version 4.7.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

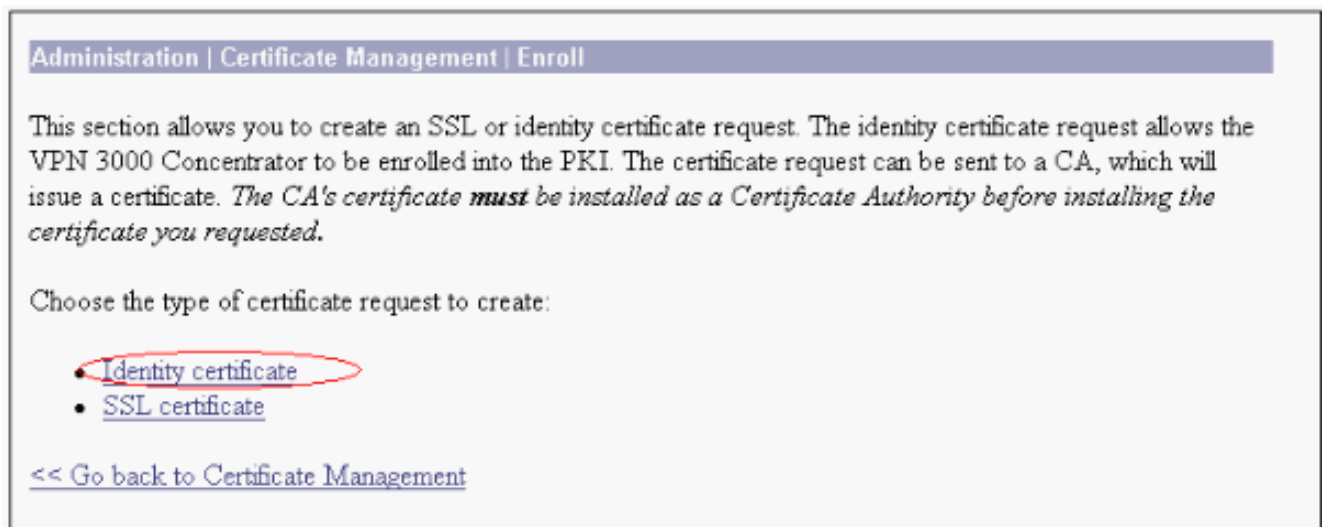
Conventions

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

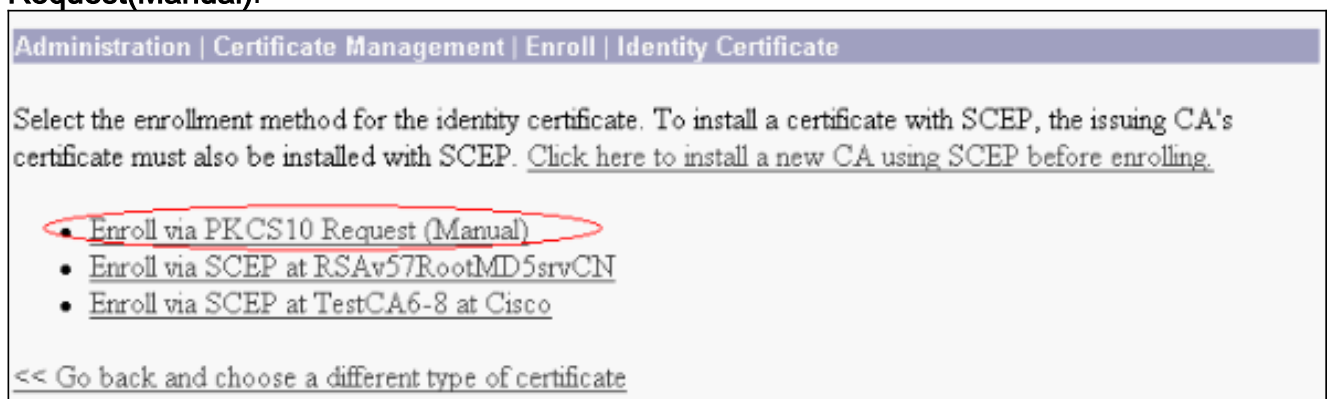
Installez les Certificats numériques sur le concentrateur VPN

Procédez comme suit :

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



2. Choisissez l'**Administration > Certificate Management > l'inscription > le certificat d'identité** et le clic **s'inscrivent** par l'intermédiaire de PKCS10 Request(Manual).



3. Complétez les champs demandés, et cliquez sur alors **s'inscrivent**. Ces champs sont complétés cet exemple. **Nom commun** — altiga30 **Unité organisationnelle** — IPSECCERT (l'OU devrait apparier le groupname configuré d'IPsec) **Organisation** — Cisco Systems **Localité** — RTP **État/province** — La Caroline du Nord **Pays** — Les USA **Nom de domaine complet** — (non utilisé ici) **Taille de clé** — 512 **Note:** Si vous demandez un certificat ssl ou un certificat d'identité utilisant l'inscription de certificat simple Protocol (SCEP), ce sont

les seules options 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="eltiga30"/>	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 que vous clic **vous inscrivez**, plusieurs fenêtres apparaissent. La première fenêtre confirme que vous avez demandé un certificat.

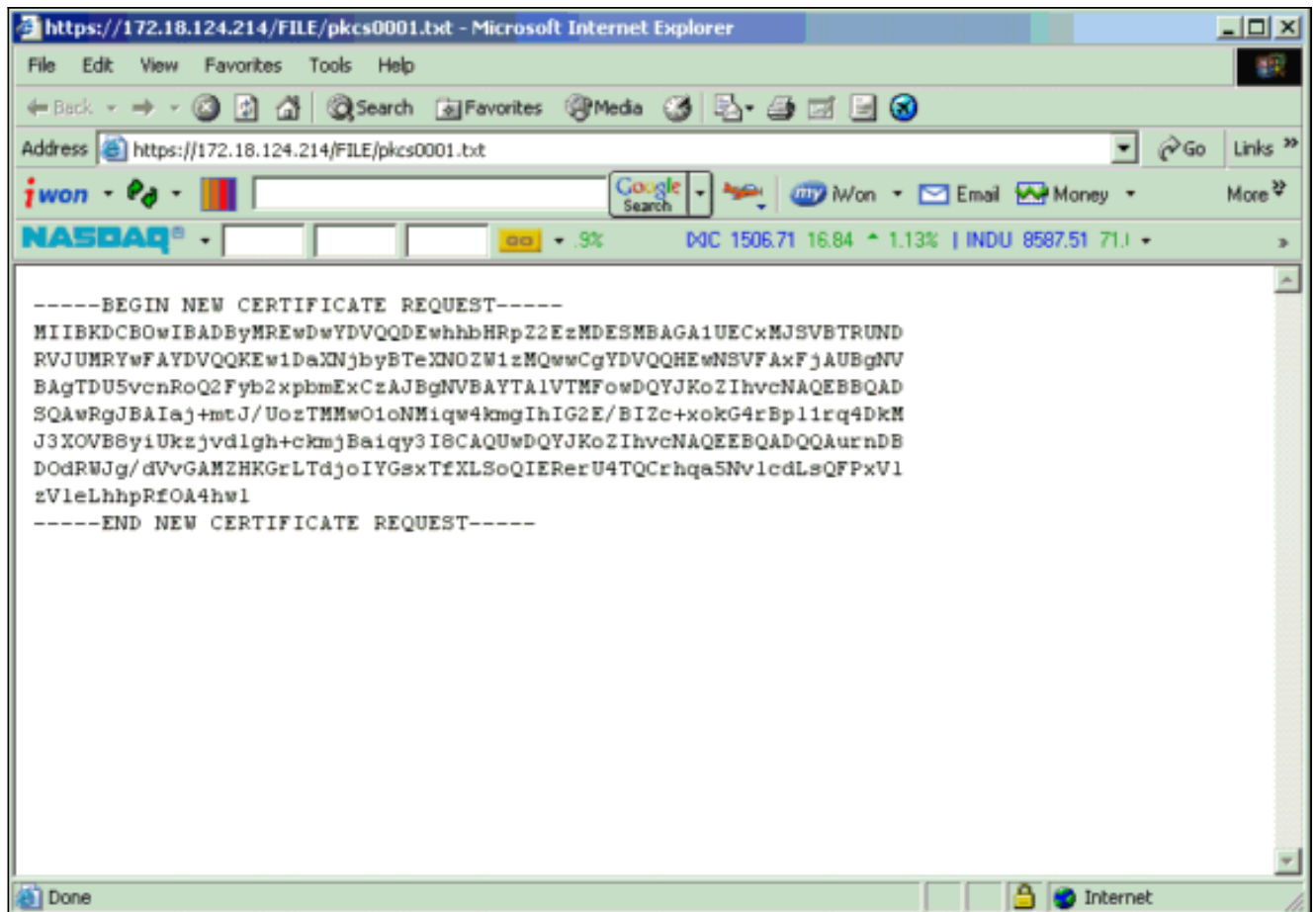
Administration | Certificate Management | Enrollment | Request Generated

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.

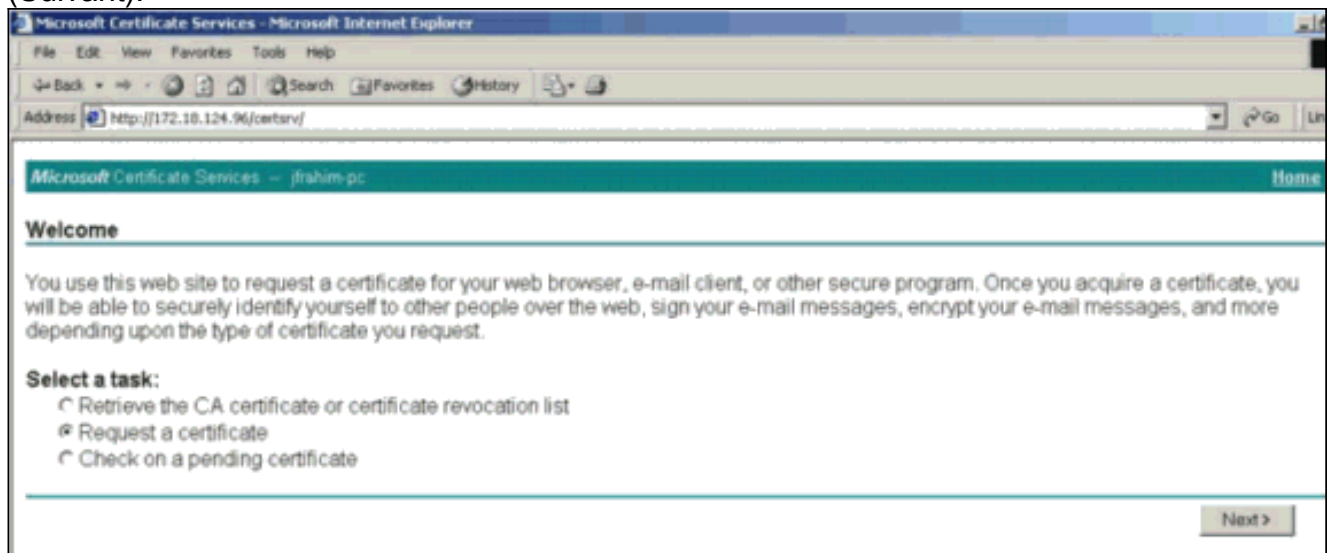
The request is located on the VPN 3000 Concentrator with the filename **pkcs0001.txt** . When you are done, you should delete this file, go to the [File Management page](#) to delete the certificate request.

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

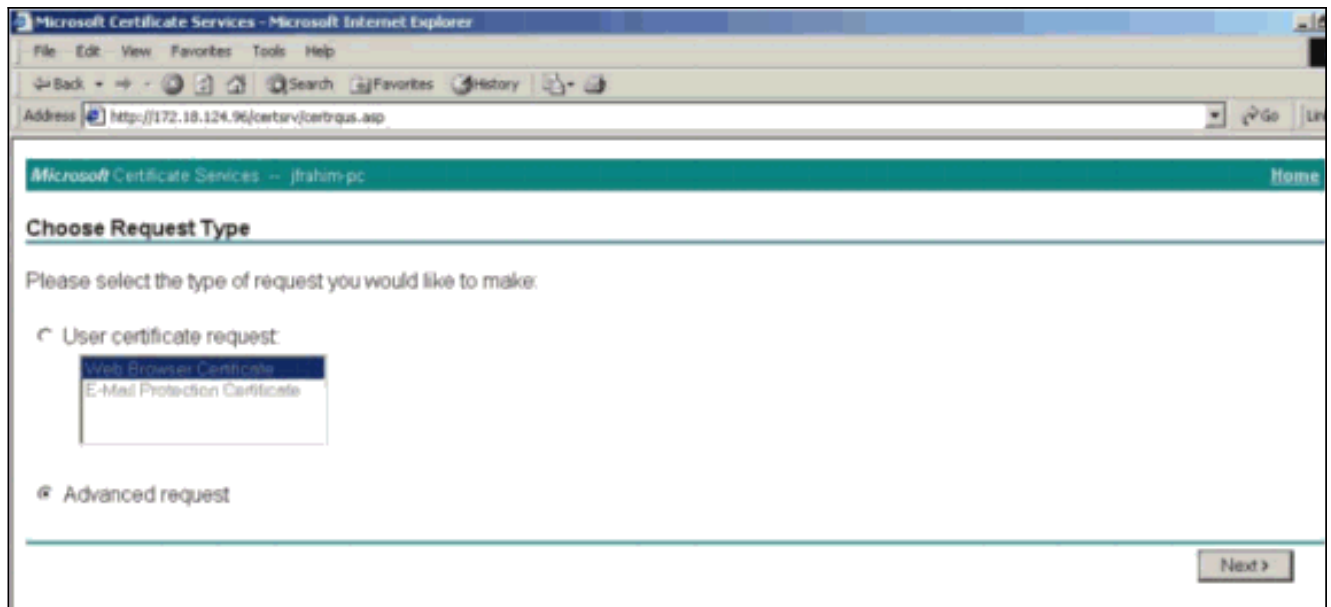
Une nouvelle fenêtre du navigateur également ouvre et affiche votre fichier de demande PKCS.



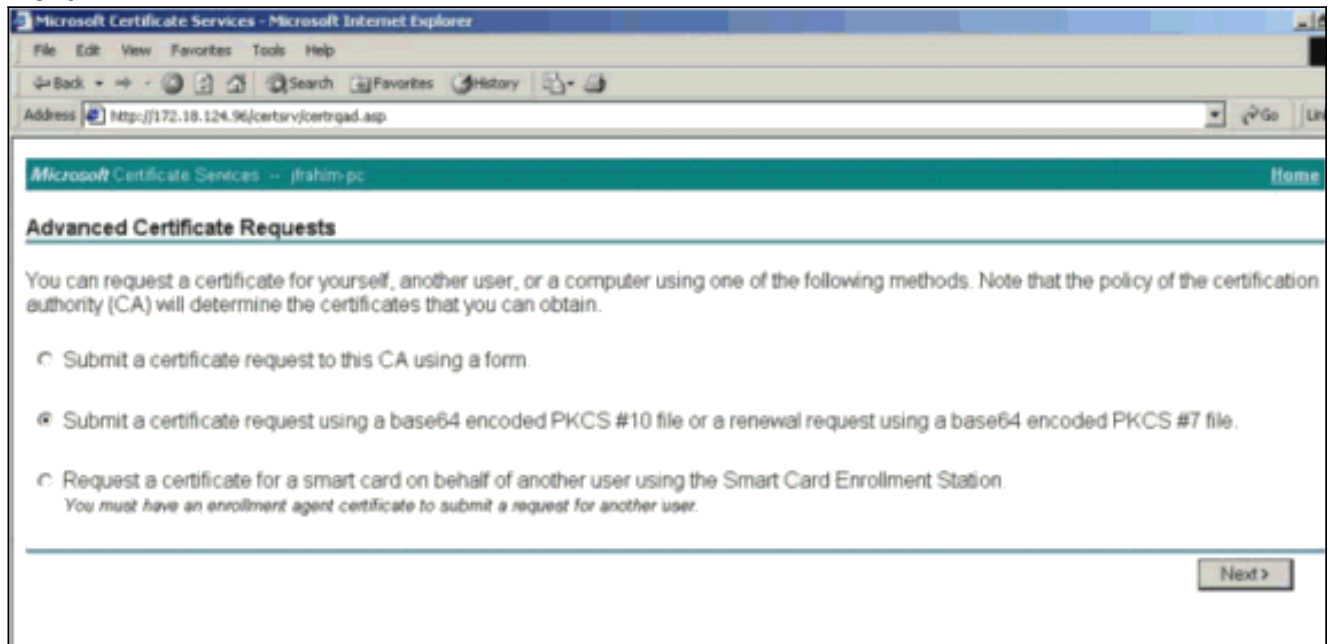
5. Sur votre serveur de l'autorité de certification (CA), mettez en valeur la demande et collez-la dans votre serveur CA afin de soumettre votre demande. Cliquez sur **Next** (Suivant).



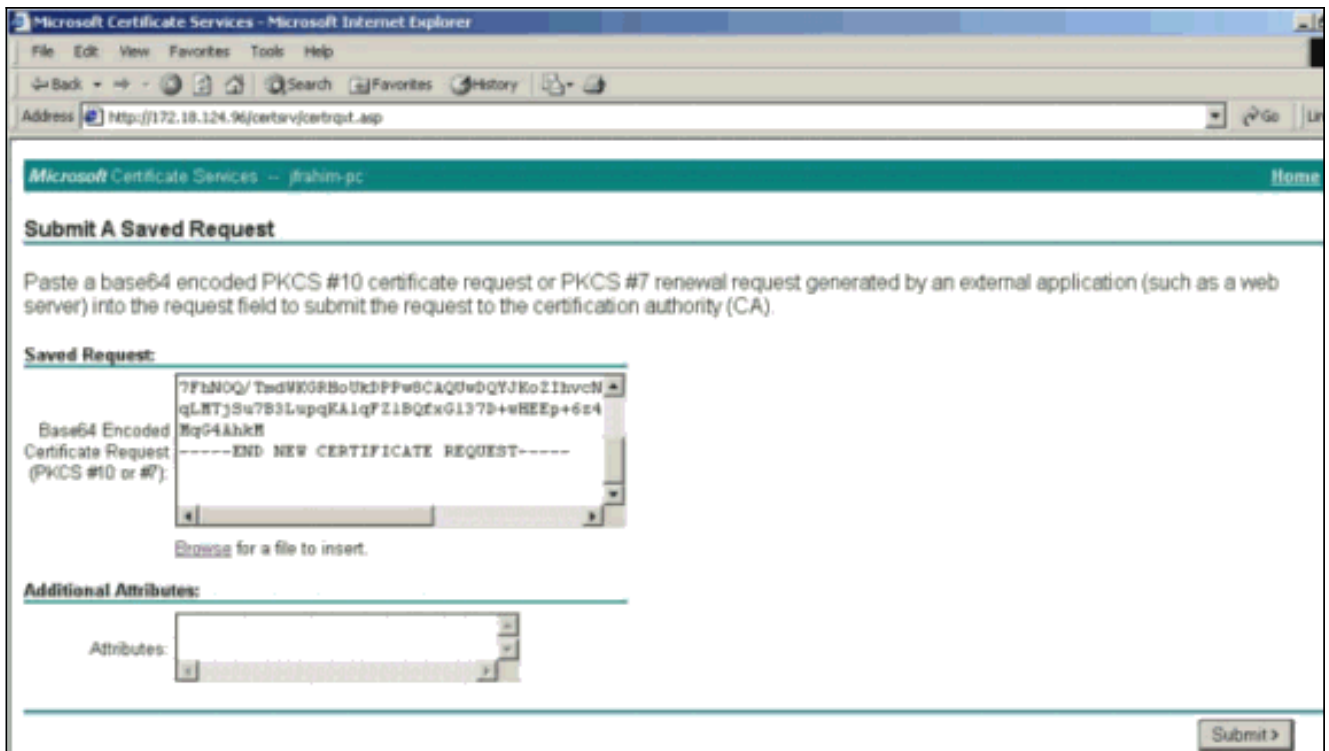
6. La demande avancée choisie et cliquent sur Next.



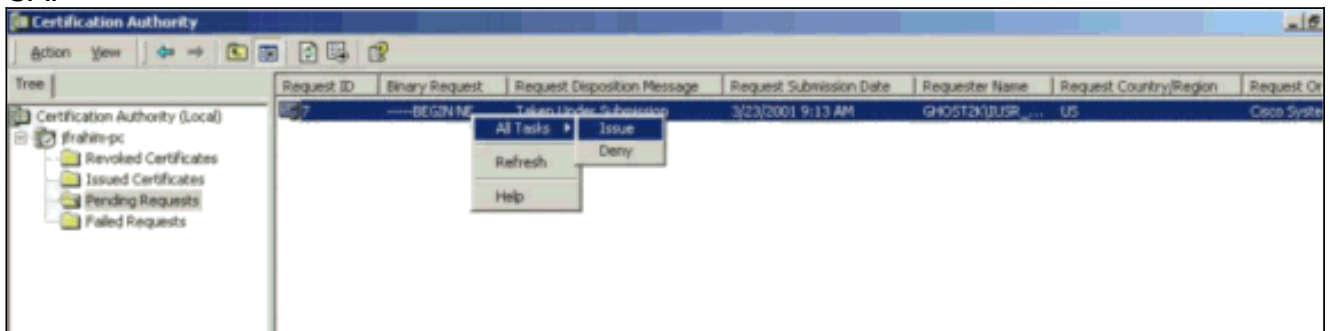
7. Choisissez une demande de certificat utilisant un fichier PKCS encodé par base64 #10 ou une demande de renouvellement utilisant un fichier PKCS encodé par base64 #7, et puis cliquez sur Next.



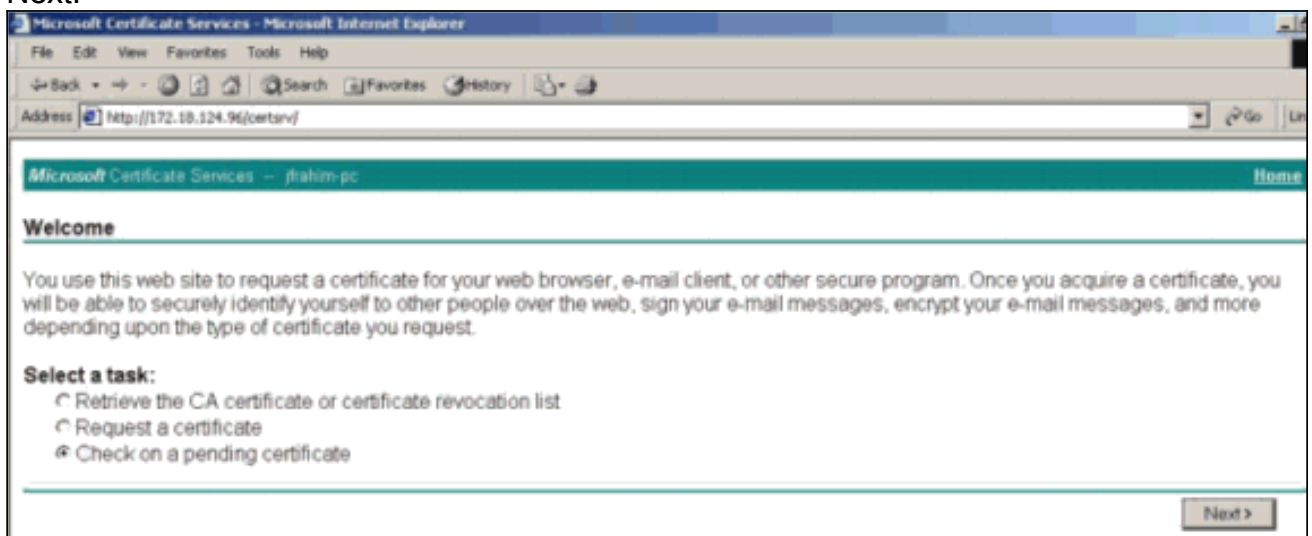
8. Coupez-collez votre fichier PKCS dans le champ texte sous la section enregistrée de demande. Cliquez sur Submit alors.



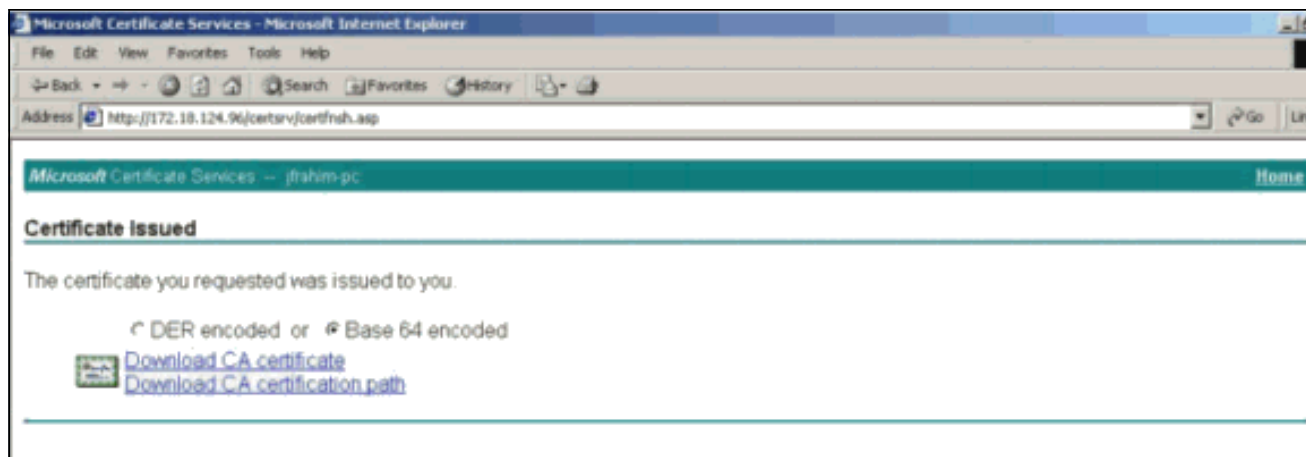
9. Délivrez le certificat d'identité sur le serveur CA.



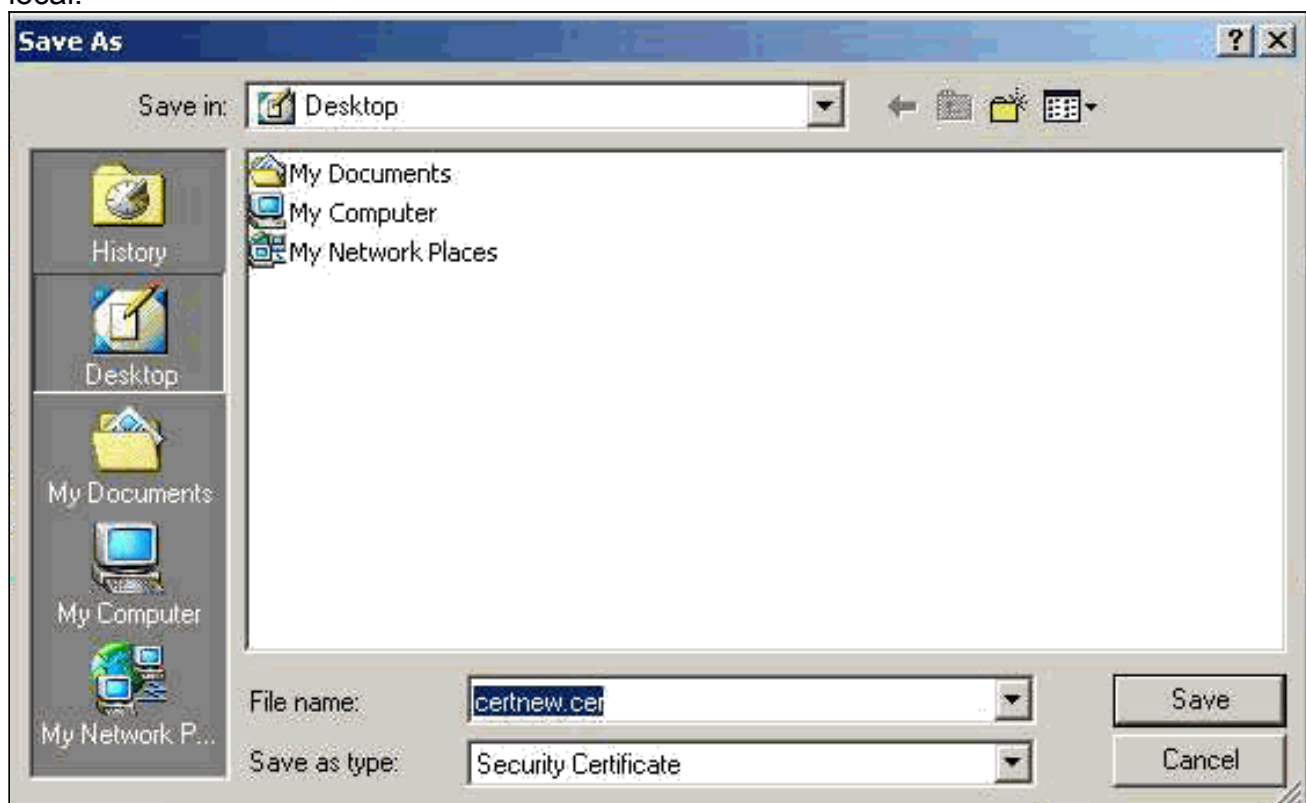
10. Téléchargez la racine et les certificats d'identité. Sur votre serveur CA, sélectionnez le **contrôle sur un certificat en attente**, et cliquez sur **Next**.



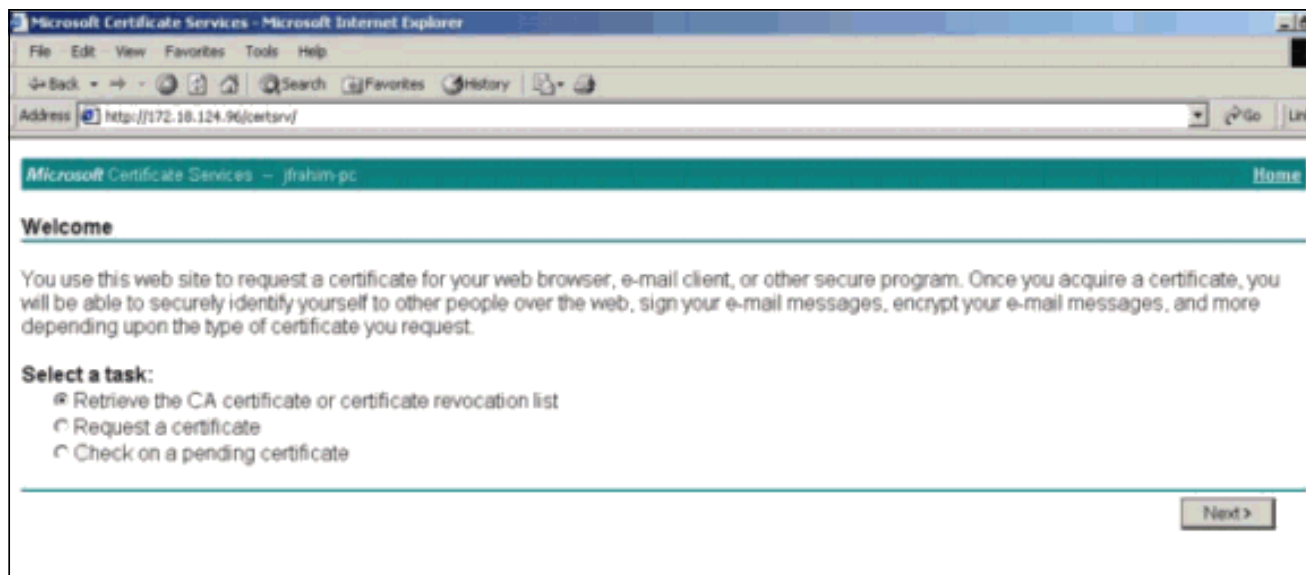
11. La base choisie **64 encodée**, et cliquent sur **Download le certificat de CA** sur le serveur CA.



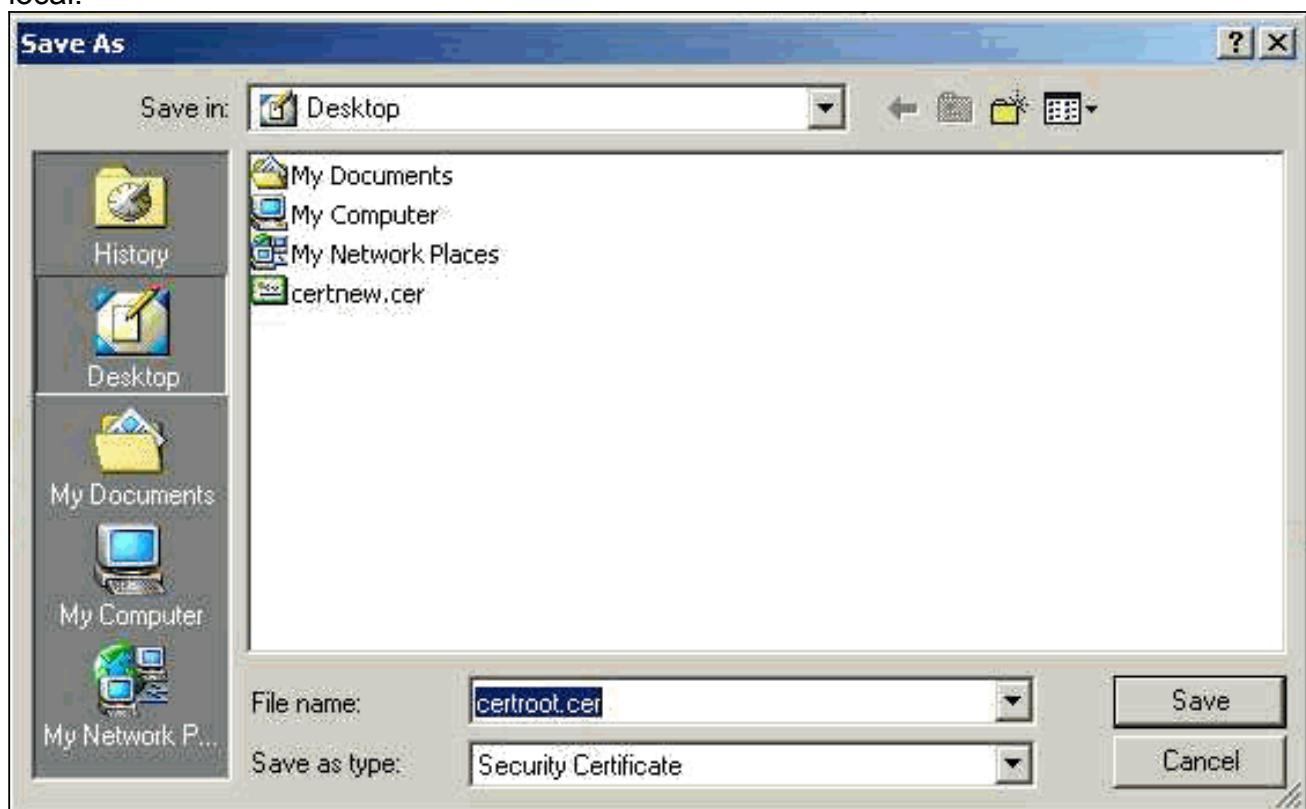
12. Sauvegardez le certificat d'identité sur votre lecteur local.



13. Sur le serveur CA, choisi **récupérez le certificat de CA ou la liste des révocations de certificat** afin d'obtenir le certificat racine. Cliquez ensuite sur **Next**.



14. Sauvegardez le certificat racine sur votre lecteur local.

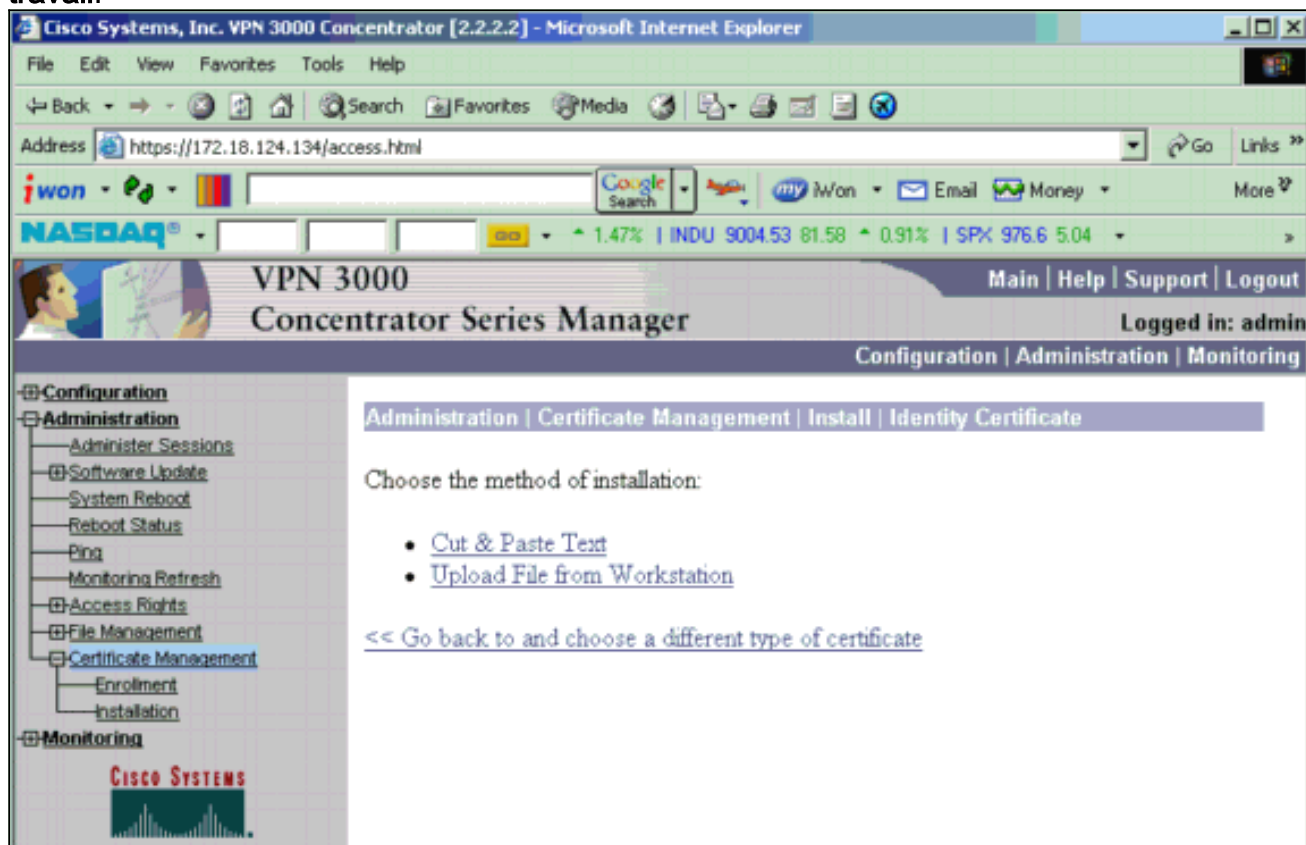


15. Installez la racine et les certificats d'identité sur le concentrateur VPN 3000. Afin de faire ceci, la **gestion** choisie > le **gestionnaire** > l'**installation de certificat** > **installent le certificat obtenu par l'intermédiaire de l'inscription**. Sous l'état d'inscription, le clic **installent**.

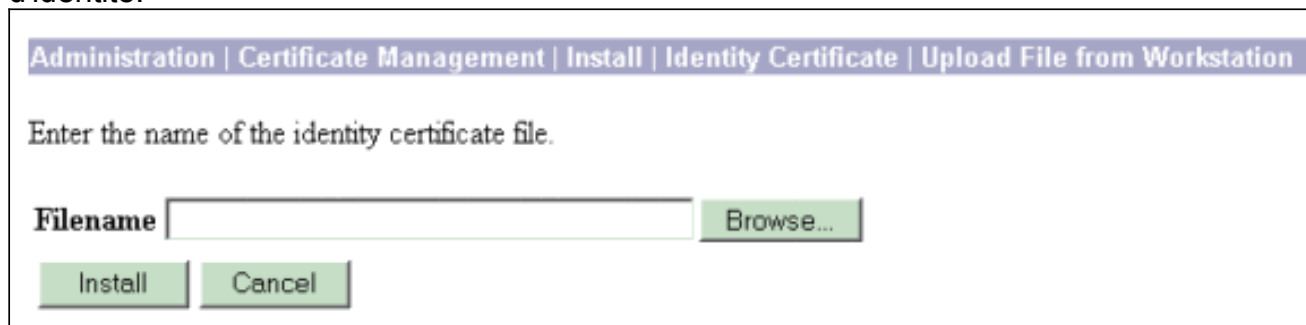


16. Cliquez sur Upload le fichier du poste de

travail.



17. Cliquez sur **parcourent** et sélectionnent le fichier de certificat racine que vous avez enregistré à votre lecteur local. Choisissez **installez** pour installer le certificat d'identité sur le concentrateur VPN. La gestion | La fenêtre de Gestion de certificat apparaît comme confirmation, et votre nouveau certificat d'identité apparaît dans la table de certificats d'identité.



Note: Terminez-vous ces étapes pour générer un nouveau certificat si le certificat échoue. **Administration > Certificate Management** choisi. Cliquez sur Delete dans la case d'actions pour répertorier de certificat ssl. **Réinitialisation** choisie de **gestion > de système**. Sélectionnez la **sauvegarde la configuration active à la période de la réinitialisation**, choisissez **maintenant**, et cliquez sur Apply. Vous pouvez maintenant générer un nouveau certificat après que la recharge soit complète.

[Installez les Certificats SSL sur le concentrateur VPN](#)

Si vous utilisez une connexion sécurisée entre votre navigateur et le concentrateur VPN, le concentrateur VPN exige un certificat ssl. Vous avez besoin également d'un certificat ssl sur l'interface que vous utilisez pour gérer le concentrateur VPN et pour le webvpn, et pour chaque interface qui termine des tunnels de webvpn.

Les Certificats SSL d'interface, s'inexistants, sont automatiquement générés quand les réinitialisations de concentrateur VPN 3000 après que vous amélioriez le logiciel de concentrateur VPN 3000. Puisqu'un certificat auto-signé auto-est généré, ce certificat n'est pas vérifiable. Aucune autorité de certification n'a garanti son identité. Mais ce certificat te permet pour établir le contact initial avec le concentrateur VPN utilisant le navigateur. Si vous voulez le remplacer par un autre certificat ssl auto-signé, terminez-vous ces étapes :

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

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

- Certificate Authorities**: A table with columns for Subject, Issuer, Expiration, SCEP Issuer, and Actions. One entry is shown: 'ms-root-sha-06-2001 at cisco' with an expiration of '06/04/2022'.
- Identity Certificates**: A table with columns for Subject, Issuer, Expiration, and Actions. One entry is shown: 'Gateway A at Cisco Systems' with an expiration of '02/04/2004'.
- SSL Certificates**: A table with columns for Interface, Subject, Issuer, Expiration, and Actions. One entry is shown for the 'Private' interface, with the 'Generate' button circled in red.
- SSH Host Key**: A table with columns for Key Size, Key Type, Date Generated, and Actions. One entry is shown: '1024 bits' RSA key generated on '01/05/2004'.

2. Cliquez sur **se produisent** afin d'afficher le nouveau certificat dans la table de certificat ssl et remplacer existant. Cette fenêtre te permet pour configurer des champs pour le SSL délivre un certificat le concentrateur VPN se produit automatiquement. Ces Certificats SSL sont pour des interfaces et pour l'Équilibrage de charge.

The screenshot shows the 'Administration | Certificate Management | Generate SSL Certificate' page. It contains a form for generating a certificate. The form includes the following fields and instructions:

- 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 of the form are 'Generate' and 'Cancel' buttons.

Si vous voulez obtenir un certificat ssl vérifiable (c'est-à-dire, un émis par une autorité de certification), voyez les [Certificats numériques d'installer sur la](#) section de [concentrateur VPN de](#) ce document afin d'utiliser la même procédure que vous utilisez pour obtenir des

certificats d'identité. Mais cette fois, sur l'**Administration > Certificate Management > s'inscrivent la fenêtre, certificat ssl de clic** (au lieu du certificat d'identité). **Note:** Référez-vous à la *gestion / Section Gestion de certificat de [volume de référence de concentrateur VPN 3000 II : Gestion et version 4.7 de surveillance](#)* pour des informations complètes sur des Certificats numériques et des Certificats SSL.

Renouvelez les Certificats SSL sur le concentrateur VPN

Cette section décrit comment renouveler les Certificats SSL :

Si c'est pour le certificat ssl généré par le concentrateur VPN, allez à l'**Administration > Certificate Management** sur la section SSL. Cliquez sur l'option de **renouveler**, et cela renouvelle le certificat ssl.

Si c'est pour un certificat accordé par un serveur externe CA, terminez-vous ces étapes :

1. Choisissez le **>Delete d'Administration > Certificate Management** sous des *Certificats SSL* afin de supprimer les Certificats expirés de l'interface publique.

Administration | Certificate Management Wednesday, 19 September 2007 00:01:44
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



Clic **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 l'**Administration > Certificate Management > se produisent** 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](#)