

De Cisco VPN 3000 Concentrator 4.7.x configureren om een digitaal certificaat en een SSL-certificaat te verkrijgen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Installeer digitale certificaten op de VPN-centrator.](#)

[Installeer SSL-certificaten op de VPN-centrator](#)

[Verleng SSL-certificaten op VPN-centrator](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document bevat stap-voor-stap instructies over de manier waarop u Cisco VPN 3000 Series Concentrators kunt configureren om te authenticeren met het gebruik van digitale of identiteitsbewijzen en SSL-certificaten.

N.B.: In de VPN-centrator moet de taakverdeling worden uitgeschakeld voordat u een ander SSL-certificaat genereert omdat dit verhindert dat een certificaat wordt gegenereerd.

Raadpleeg [Hoe u een digitaal certificaat kunt verkrijgen van een Microsoft Windows CA met behulp van ASDM op een ASA](#) om meer te weten te komen over hetzelfde scenario met PIX/ASA 7.x.

Raadpleeg [Cisco IOS certificaatinschrijving met behulp van uitgebreide inschrijving Opdrachten Configuration Voorbeeld](#) om meer te weten te komen over hetzelfde scenario met Cisco IOS®-platforms.

[Voorwaarden](#)

[Vereisten](#)

Er zijn geen specifieke vereisten van toepassing op dit document.

[Gebruikte componenten](#)

De informatie in dit document is gebaseerd op Cisco VPN 3000 Concentrator die versie 4.7 draait.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

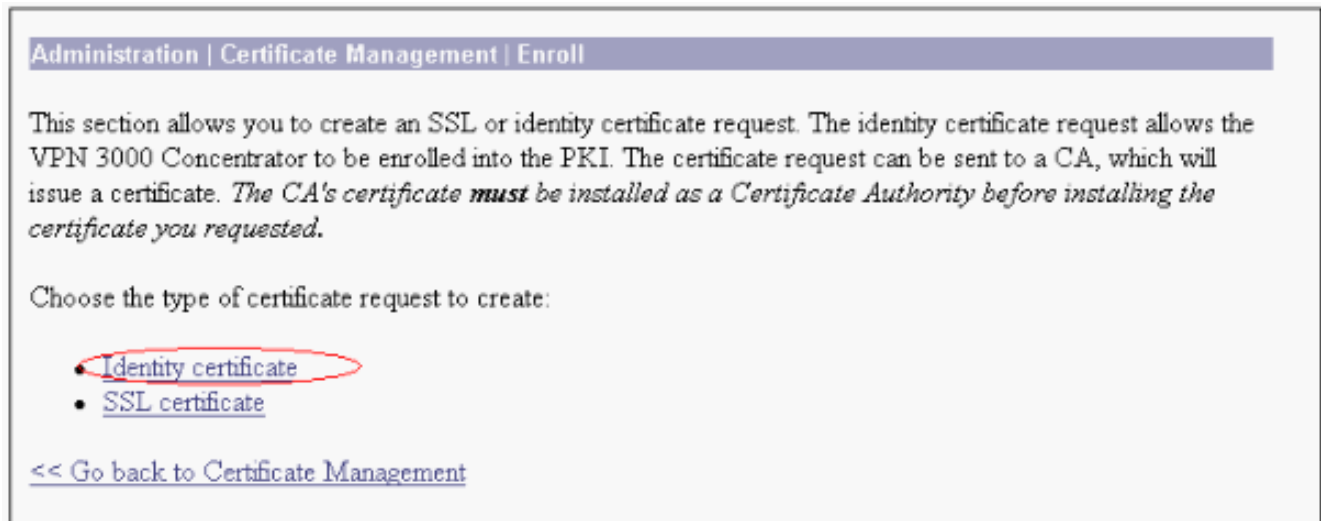
Conventies

Raadpleeg de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

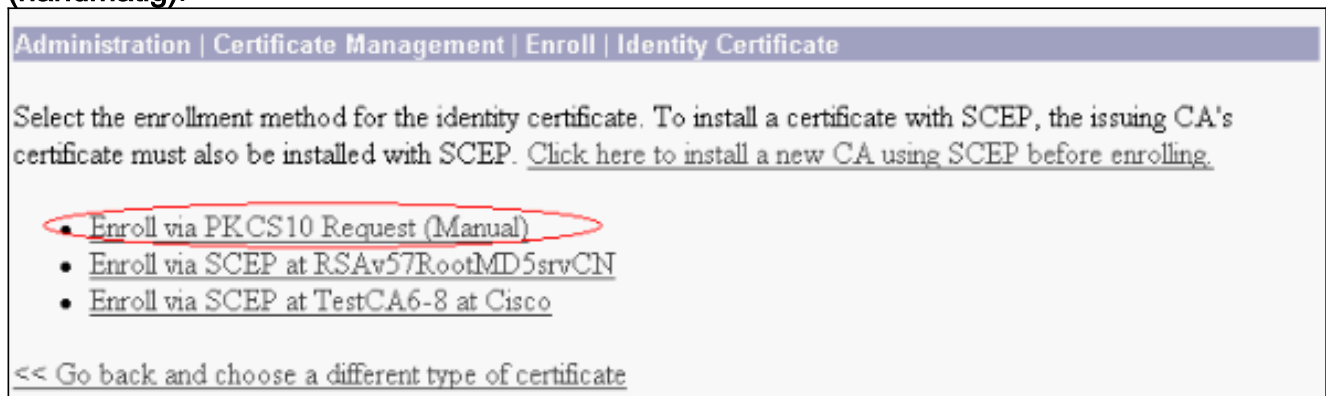
Installeer digitale certificaten op de VPN-centrator.

Voer de volgende stappen uit:

1. Kies **Administratie > certificaatbeheer > Inschrijven** om het digitale verzoek of de identiteitsaanvraag te selecteren.



2. Kies **Administratie > certificaatbeheer > inschrijving > Identiteitscertificaat** en klik op **Inschrijven via PKCS10-aanvraag (handmatig)**.



3. Vul de gevraagde velden in en klik vervolgens op **Invoegen**. Deze velden zijn in dit voorbeeld ingevuld. **Algemene naam:** altiga30**Organisatorische eenheid**—IPSECCERT (de OU dient dezelfde naam te hebben als de geconfigureerde IPsec-groepsnaam)**Organisatie**-Cisco systemen**Localiteit**—RTP**Staat/provincie**—NorthCarolina**Land** — VS**Full Qualified Domain Name**— (niet hier gebruikt)**Sleutelgrootte**—512**N.B.:** Als u een SSL-certificaat of een identiteitsbewijs wenst met behulp van Simple certificaatinschrijving Protocol (SCEP), zijn dit

de enige beschikbare RSA-opties. 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. Nadat u op **Inschrijven** klikt, verschijnen er verschillende vensters. Het eerste venster bevestigt dat u een certificaat hebt aangevraagd.

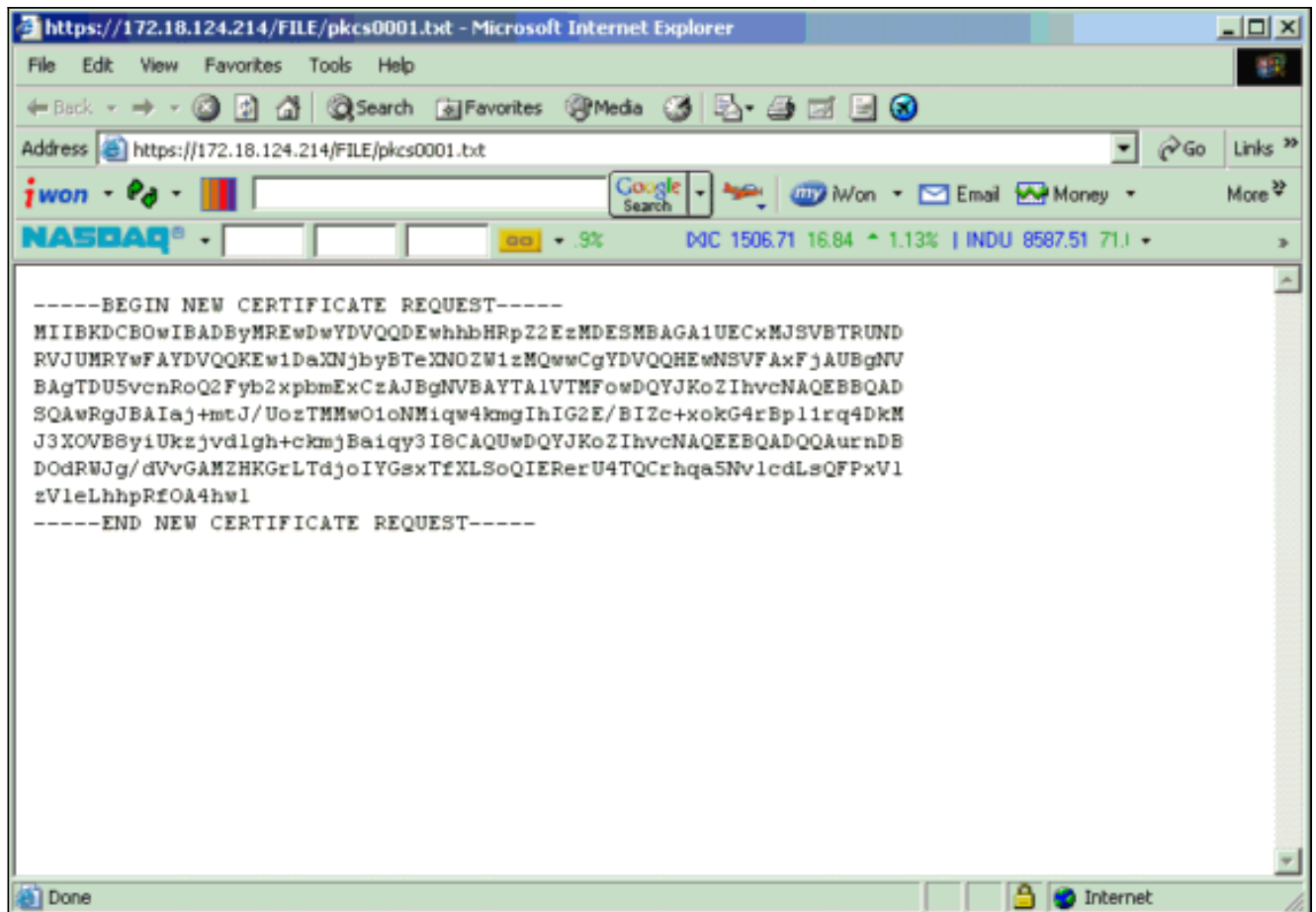
Administration | Certificate Management | Enrollment | Request Generated

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.

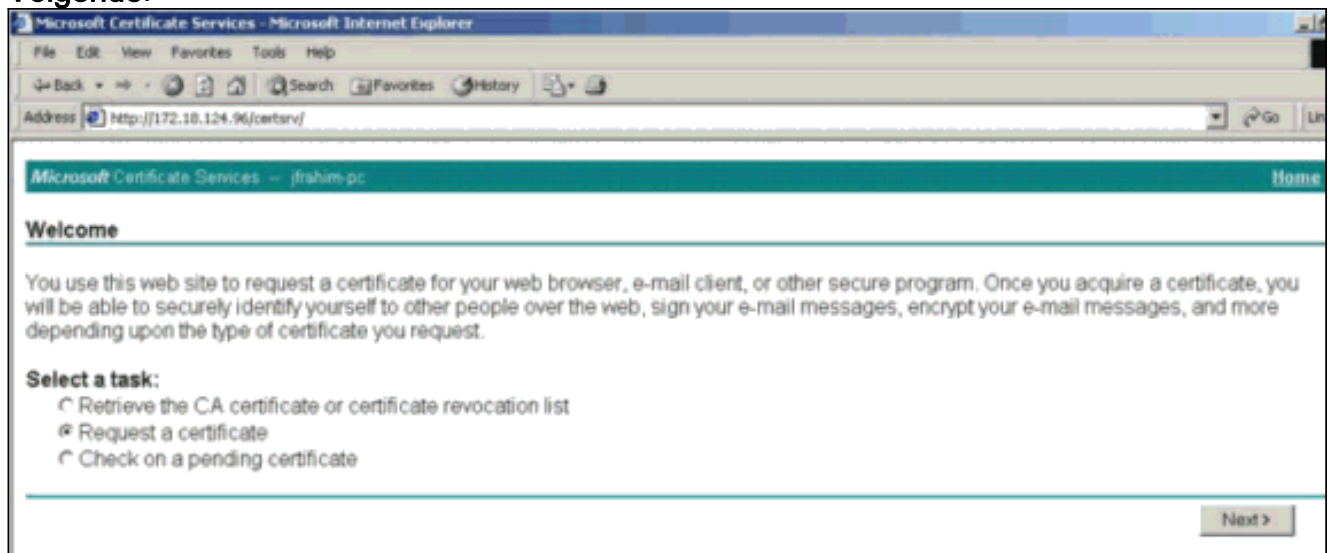
The request is located on the VPN 3000 Concentrator with the filename **pkcs0001.txt** . When you are done, you should delete this file, go to the [File Management page](#) to delete the certificate request.

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

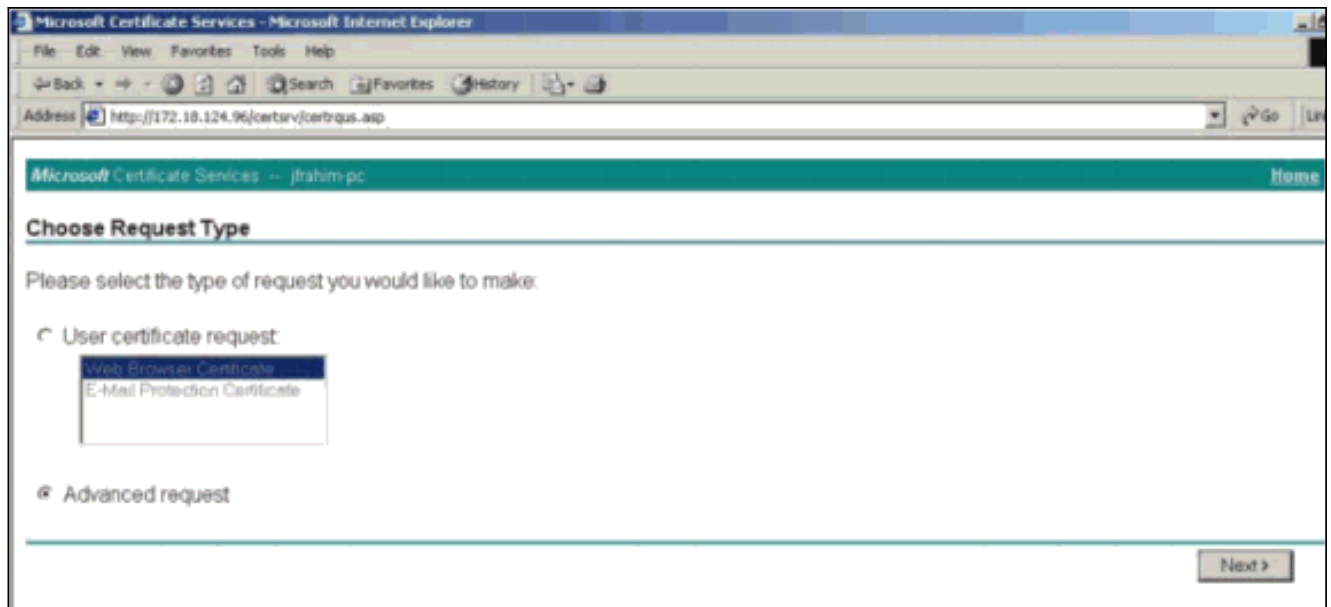
Een nieuw browser venster wordt ook geopend en weergegeven in uw PKCS-aanvraagbestand.



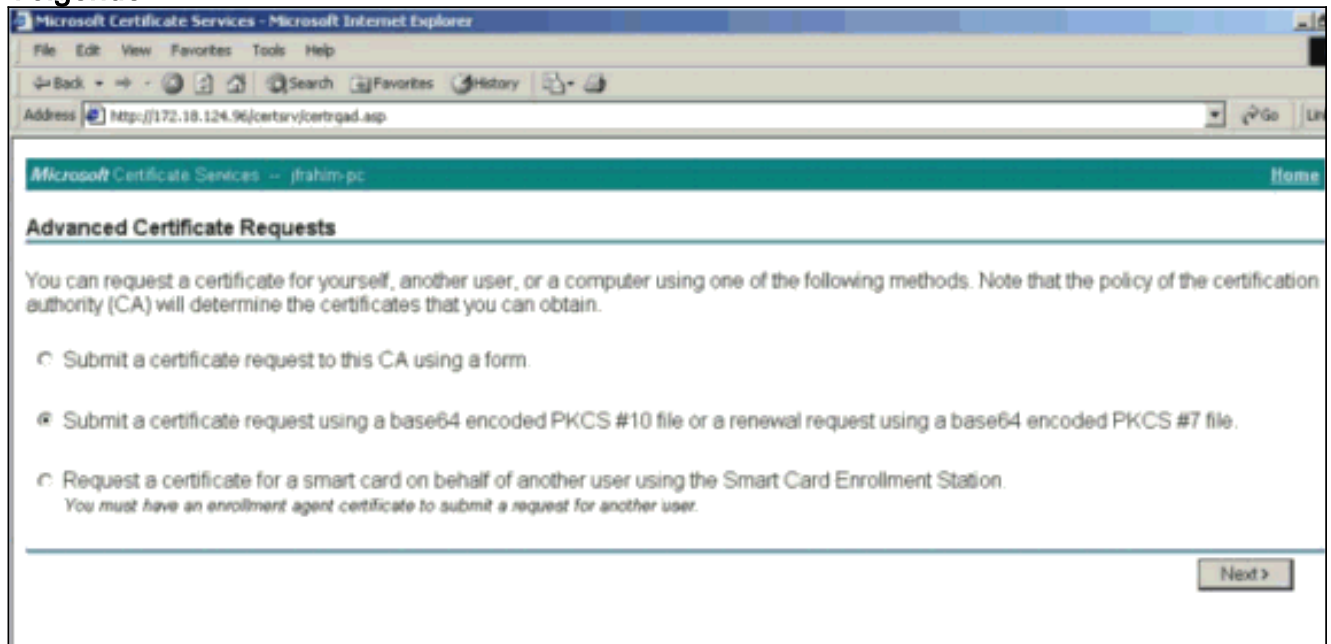
5. Op uw CA-server (Certification Authority) markeren u het verzoek en plakken het op uw CA-server om uw verzoek in te dienen. Klik op **Volgende**.



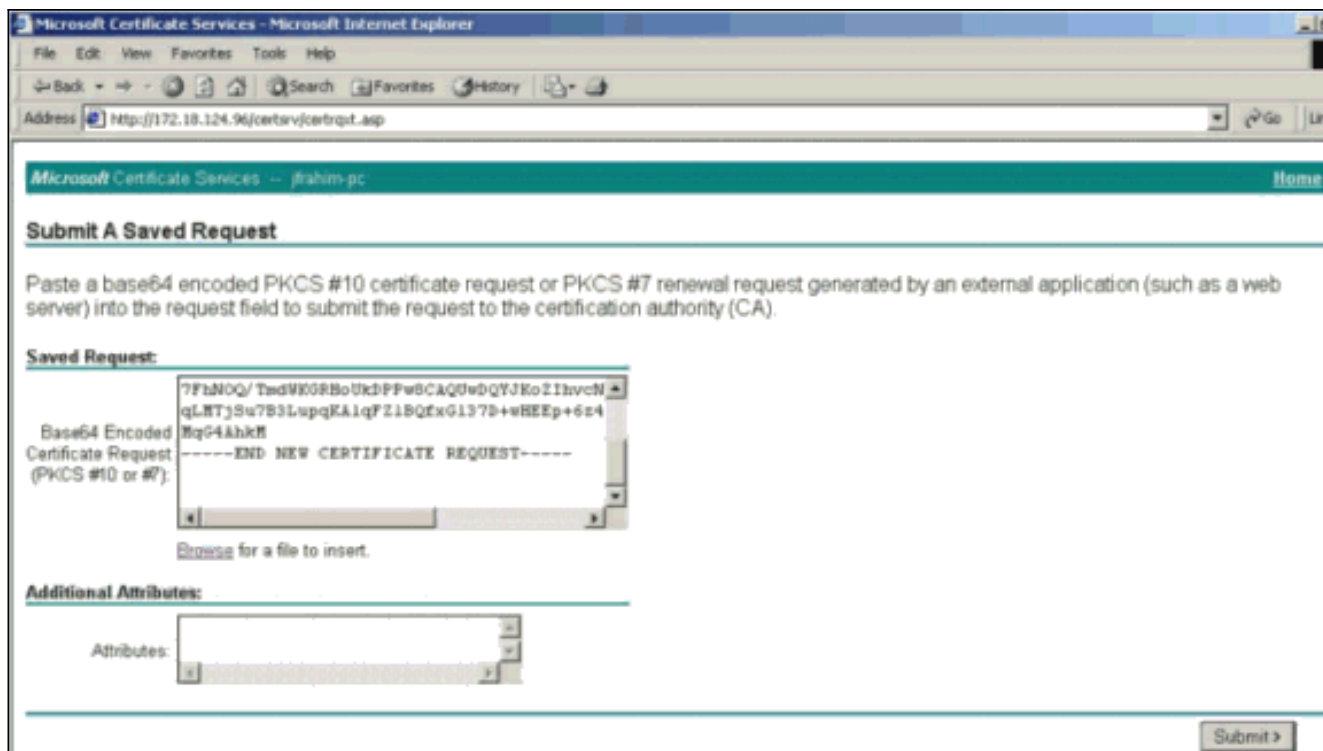
6. Selecteer **Geavanceerd verzoek** en klik op **Volgende**.



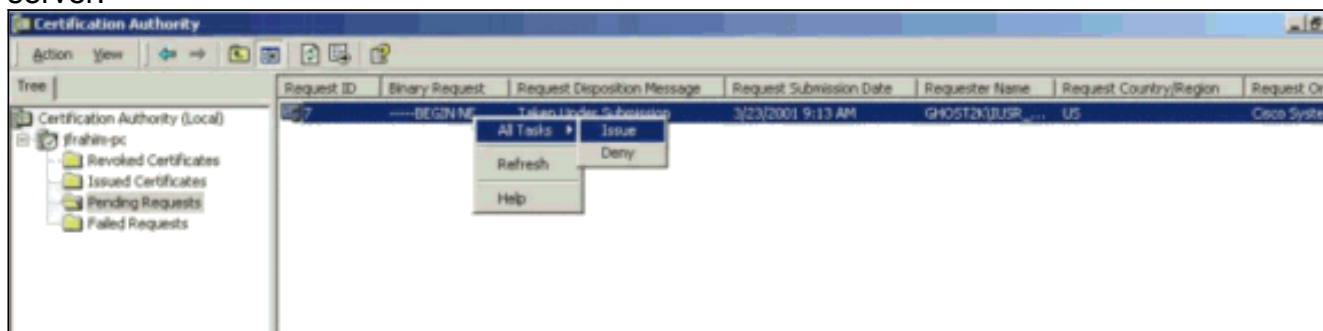
7. Selecteer **Een certificaataanvraag indienen met behulp van een Base64 gecodeerde PKCS #10-bestand** of een **hervernieuwingsaanvraag met behulp van een Base64 gecodeerde PKCS #7-bestand** en klik vervolgens op **Volgende**.



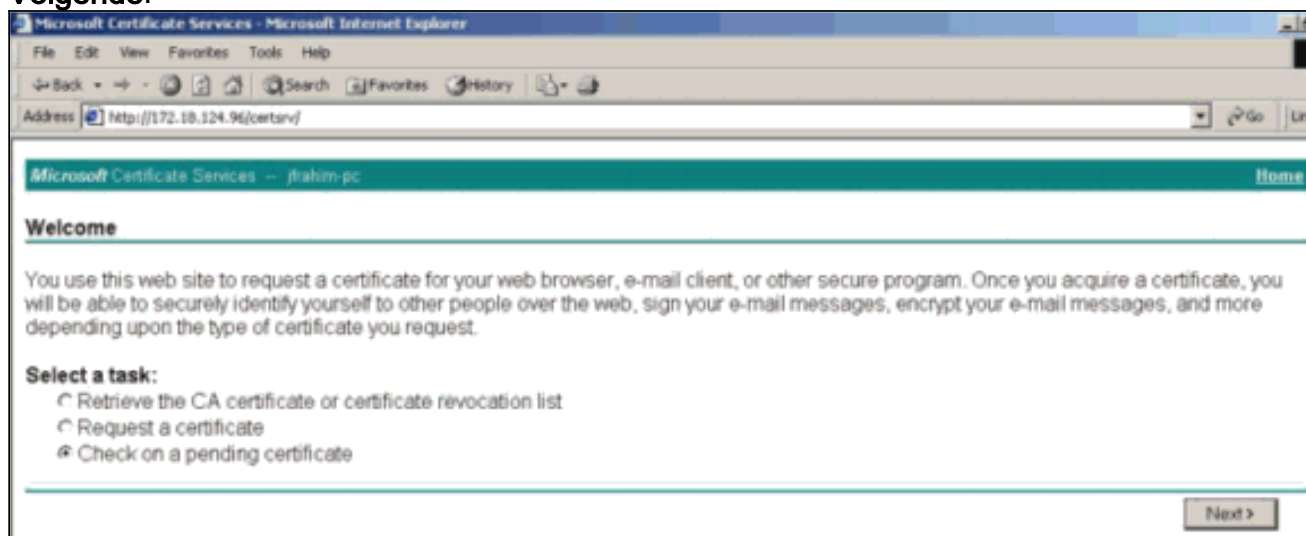
8. Snijd en plak uw PKCS-bestand naar het tekstveld onder de sectie **Opgeslagen aanvraag**. Klik vervolgens op **Inzenden**.



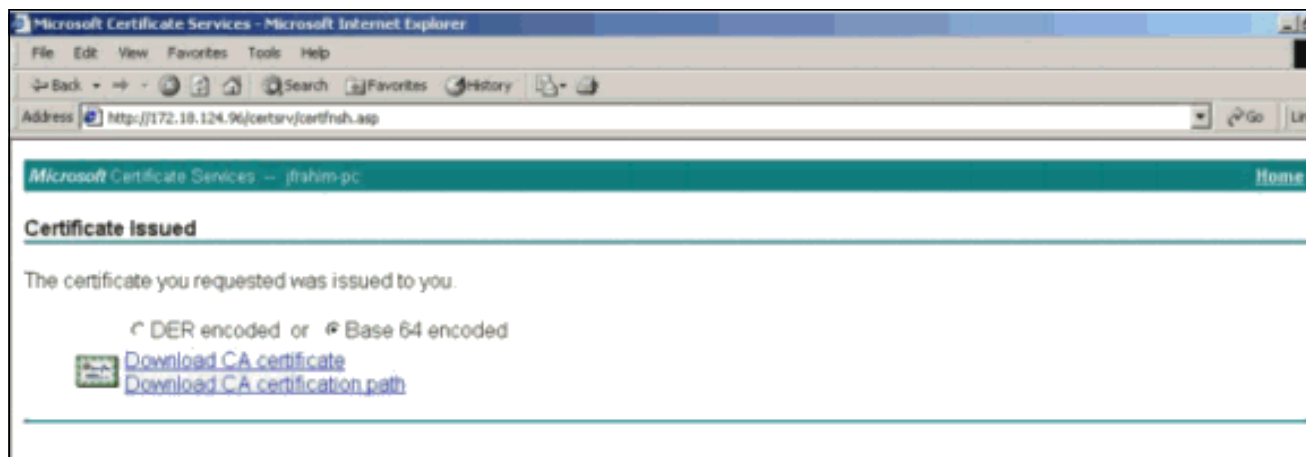
9. Geef het identiteitsbewijs af op de CA server.



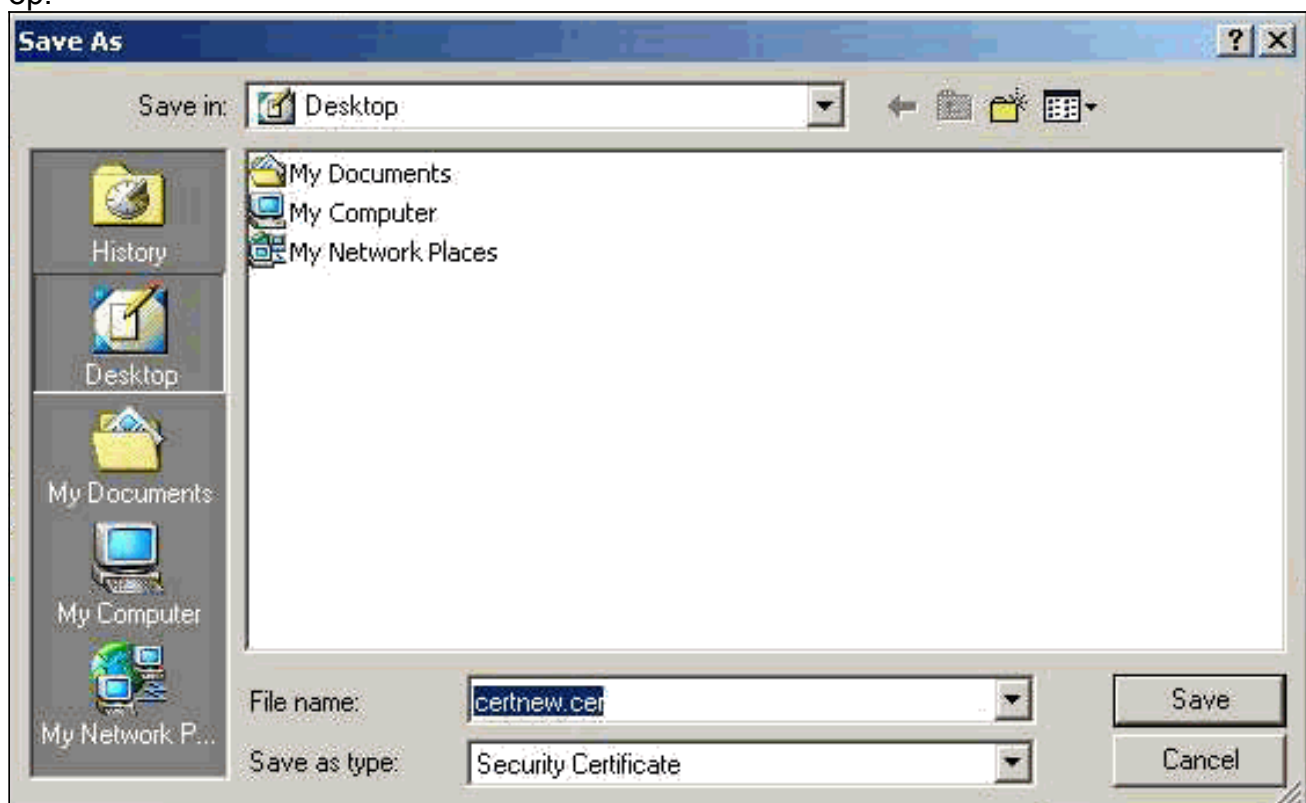
10. Download de wortel en de identiteitsbewijzen. Selecteer op uw CA-server de optie controleren op een hangend certificaat en klik op Volgende.



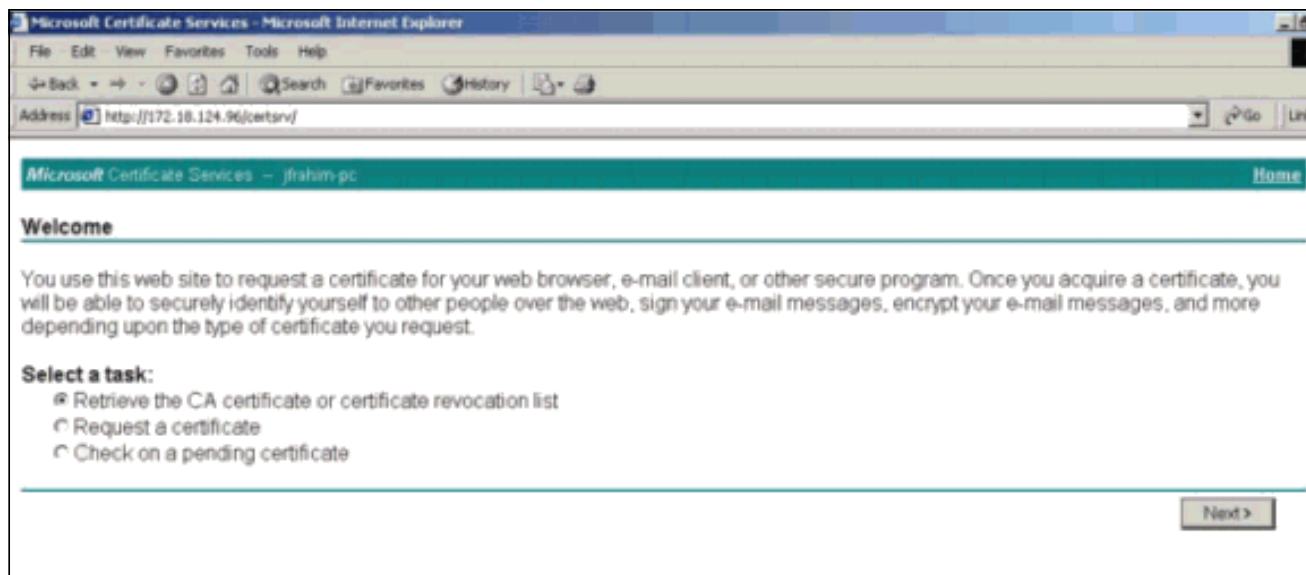
11. Selecteer Base 64 ingesloten en klik op Download CA certificaat op de CA server.



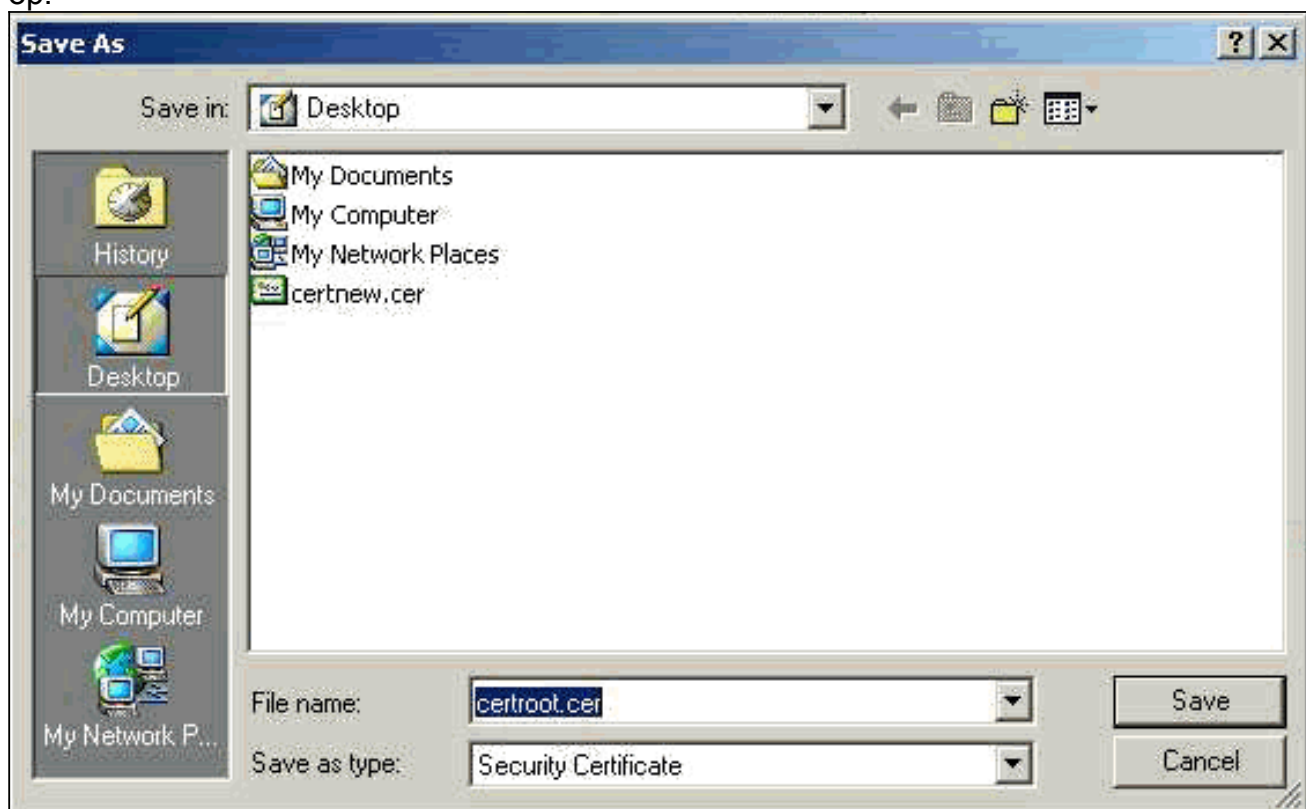
12. Sla het identiteitsbewijs op het lokale station op.



13. Selecteer op de CA-server de optie **CA-certificaat** of de lijst voor intrekking van het **certificaat** ophalen om het basiscertificaat te verkrijgen. Klik op **Volgende**.



14. Sla het basiscertificaat op het lokale station op.

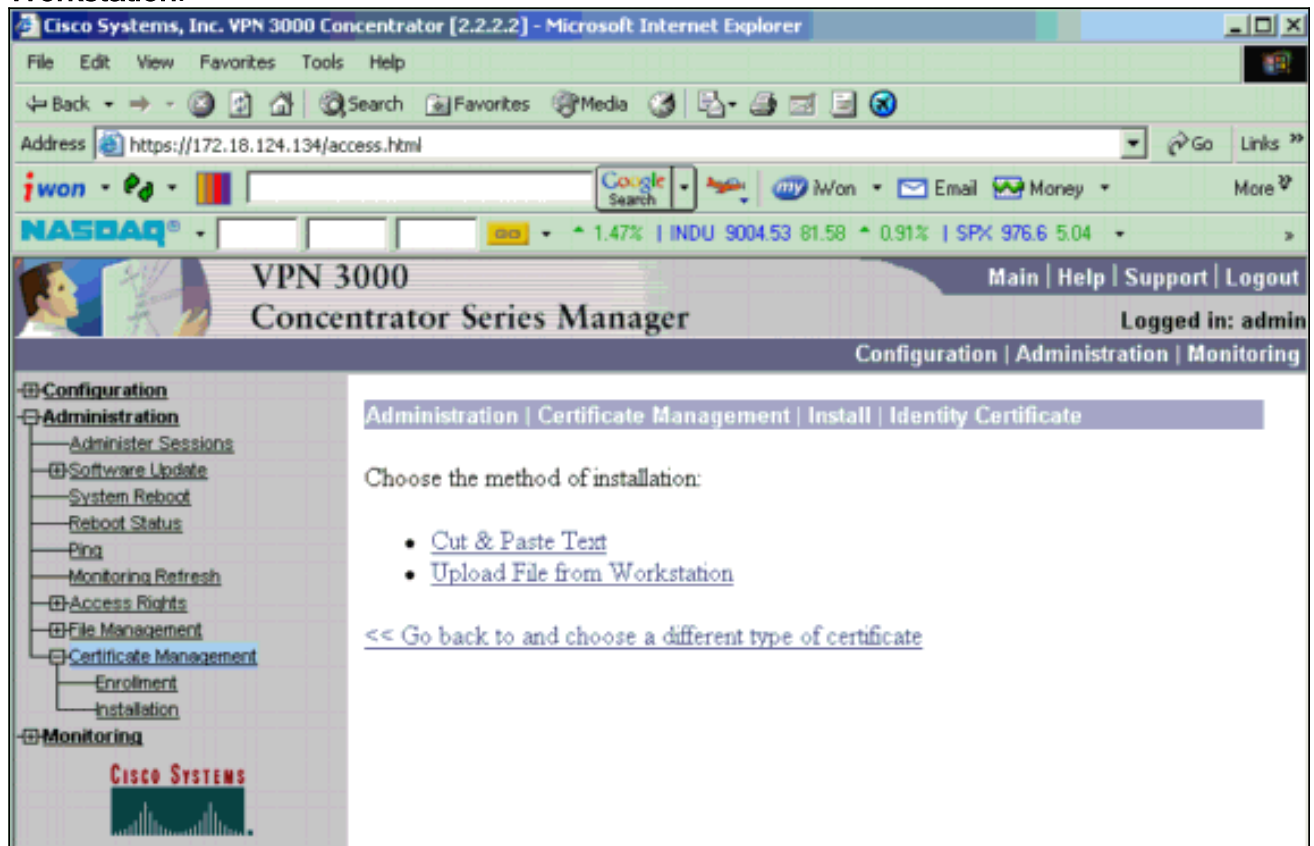


15. Installeer de wortel- en identiteitsbewijzen op de VPN 3000 Concentrator. Selecteer hiervoor **Administratie > certificaatbeheer > Installatie > Installeer het certificaat dat u via inschrijving hebt verkregen**. Klik onder Invoerstatus op **Installatie**.

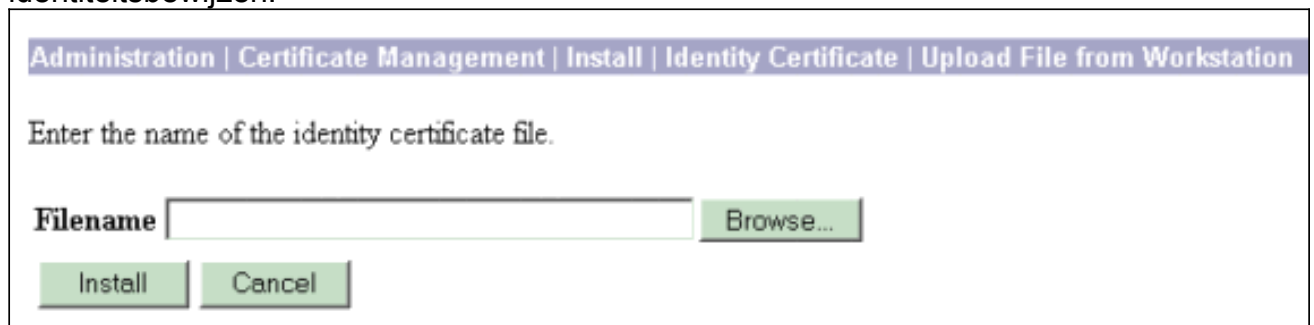


16. Klik op **Upload File** vanuit

Workstation.



17. Klik op **Bladeren** en selecteer het broncertificeringsbestand dat u hebt opgeslagen op uw lokale station. Selecteer **Installeer** om het identiteitsbewijs in de VPN-Concentrator te installeren. De administratie | Het venster certificaatbeheer verschijnt als bevestiging en uw nieuwe identiteitsbewijs verschijnt in de tabel met identiteitsbewijzen.



N.B.: Voltooi deze stappen om een nieuw certificaat te genereren als het Certificaat niet werkt. Selecteer **Beheer > certificaatbeheer**. Klik op **Verwijderen** in het vak Handelingen voor de SSL-certificaatlijst. Selecteer **Beheer > Systeem opnieuw opstarten**. Selecteer **de actieve configuratie opslaan op het moment dat de computer opnieuw wordt opgestart**, kies **Nu** en klik op **Toepassen**. U kunt nu een nieuw certificaat genereren nadat het opnieuw laden is voltooid.

[Installeer SSL-certificaten op de VPN-centrator](#)

Als u een veilige verbinding tussen uw browser en de VPN Concentrator gebruikt, vereist de VPN Concentrator een SSL-certificaat. U hebt ook een SSL certificaat op de interface nodig die u gebruikt om de VPN Concentrator en voor WebVPN te beheren, en voor elke interface die tunnels WebVPN beëindigt.

Als de interface-SSL-certificaten niet aanwezig zijn, worden automatisch gegenereerd wanneer de VPN 3000 Concentrator opnieuw wordt opgestart nadat u de VPN 3000 Concentrator-software hebt bijgewerkt. Omdat een zichzelf ondertekend certificaat zelf gegenereerd is, is dit certificaat niet controleerbaar. Geen enkele certificeringsinstantie heeft haar identiteit gegarandeerd. Maar met dit certificaat kunt u eerste contact maken met de VPN Concentrator via de browser. Als u het wilt vervangen door een ander zelfgetekend SSL-certificaat, voert u de volgende stappen in:

1. Kies **Beheer > certificaatbeheer.**

Administration | Certificate Management Monday, 05 January 2004 16:31:11 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: 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. Klik op **Generate** om het nieuwe certificaat in de SSL certificaattabel weer te geven en de bestaande te vervangen. In dit venster kunt u velden voor SSL-certificaten configureren en VPN-centrator automatisch genereren. Deze SSL certificaten zijn voor interfaces en voor het in evenwicht brengen van de lading.

Administration | Certificate Management | Generate SSL Certificate

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) Enter the Common Name, usually the IP or DNS address of this interface

Organizational Unit (OU) Enter the department.

Organization (O) Enter the Organization or company.

Locality (L) Enter the city or town.

State/Province (SP) Enter the State or Province.

Country (C) Enter the two-letter country abbreviation (e.g. United States = US).

RSA Key Size Select the key size for the generated RSA key pair.

Als u een verifieerbaar SSL-certificaat wilt verkrijgen (dat wil zeggen, een certificaat dat is afgegeven door een certificaatinstantie), zie de [Installeer Digitale Certificaten op het gedeelte VPN Concentrator](#) van dit document om de procedure te gebruiken die u gebruikt om

identiteitsbewijzen te verkrijgen. Maar deze keer klikt u op **SSL-certificaat** in het venster **Administration > certificaatbeheer > Inschrijven** in op **SSL-certificaat** (in plaats van identiteitsbewijs). **Opmerking:** Raadpleeg de *administratie / Deel van certificaatbeheer van VPN 3000 Concentrator Referentievolumen II: Beheer en bewaking release 4.7* voor volledige informatie over digitale certificaten en SSL-certificaten.

Verleng SSL-certificaten op VPN-centrator

In deze sectie wordt beschreven hoe de SSL-certificaten worden vernieuwd:

Als dit is voor het SSL-certificaat dat door de VPN-Concentrator is gegenereerd, gaat u naar **Administratie > certificaatbeheer** op de SSL-sectie. Klik op de **optie** vernieuwen en dat het SSL-certificaat vernieuwt.

Als dit voor een certificaat is dat door een externe CA server wordt verleend, Voltooi de volgende stappen:

1. Kies **Administratie > certificaatbeheer > Verwijderen** onder *SSL-certificaten* om de verlopen certificaten van de openbare interface te verwijderen.

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



Klik op **Ja** om het wissen van het SSL-certificaat te bevestigen.

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. Kies **Beheer > certificaatbeheer > Generate** om het nieuwe SSL certificaat te genereren.

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



Het nieuwe SSL certificaat voor de openbare interface verschijnt.

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

[Gerelateerde informatie](#)

- [Ondersteuning van Cisco VPN 3000 Series Concentrator-pagina](#)
- [IPsec-onderhandeling/IKE-protocollen](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)