

配置Cisco VPN 3000 Concentrator 4.7.x以獲取數位證書和SSL證書

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[在VPN集中器上安裝數位證書](#)

[在VPN集中器上安裝SSL證書](#)

[在VPN集中器上續訂SSL證書](#)

[相關資訊](#)

簡介

本文檔包含有關如何配置Cisco VPN 3000系列集中器以使用數字或身份證書和SSL證書進行身份驗證的逐步說明。

注意：在VPN集中器中，必須在生成另一個SSL證書之前禁用負載平衡，因為這樣可以防止證書生成。

請參閱[如何使用ASA上的ASDM從Microsoft Windows CA獲取數位證書](#)，以瞭解有關PIX/ASA 7.x的相同方案的詳細資訊。

請參閱[使用增強型註冊命令的Cisco IOS證書註冊配置示例](#)，以瞭解更多有關Cisco IOS®平台相同方案的資訊。

必要條件

需求

本文件沒有特定需求。

採用元件

本文檔中的資訊基於運行版本4.7的Cisco VPN 3000集中器。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

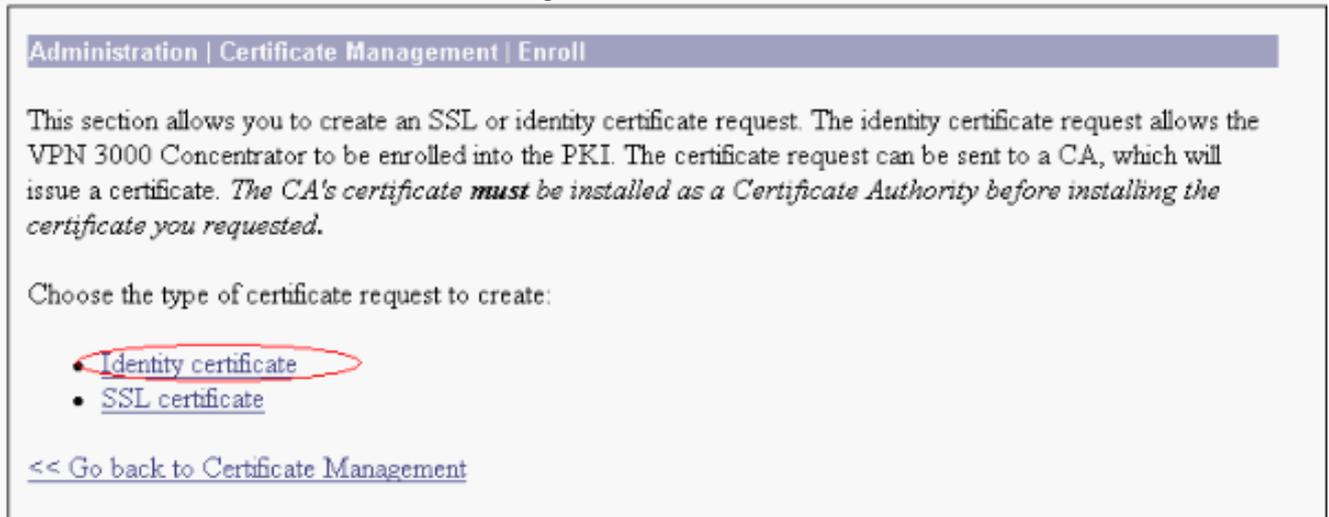
慣例

請參閱[思科技術提示慣例](#)以瞭解更多有關文件慣例的資訊。

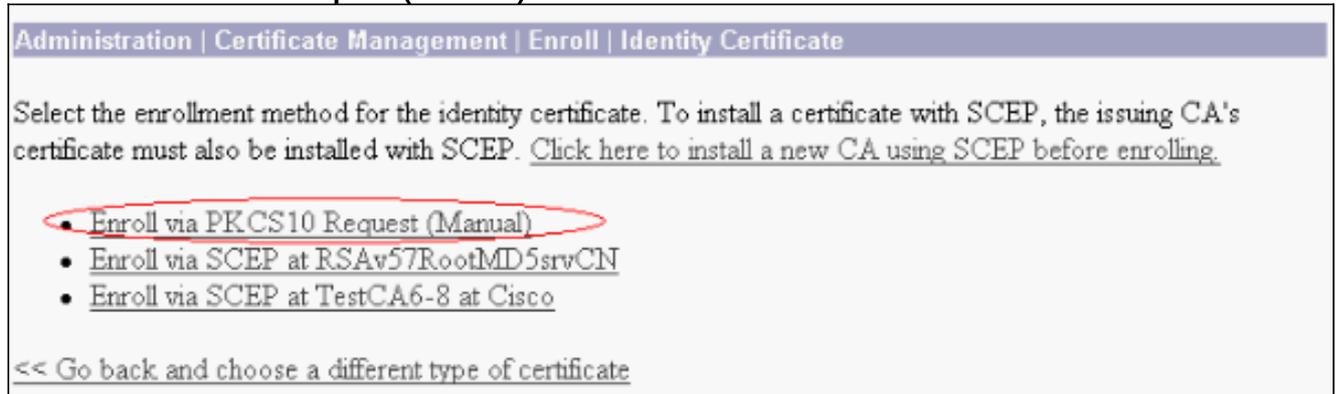
在VPN集中器上安裝數位證書

請完成以下步驟：

1. 選擇Administration > Certificate Management > Enroll 以選擇數位證書或身份證書請求。



2. 選擇Administration > Certificate Management > Enrollment > Identity Certificate，然後按一下Enroll via PKCS10 Request(Manual)。



3. 填寫請求的欄位，然後按一下Enroll。本示例中填寫了這些欄位。常用名稱 — altiga30組織單位 — IPSECCERT (OU應與配置的IPsec組名匹配) 組織- Cisco Systems位置- RTP州/省 — 北卡羅萊納國家 — 美國完全限定域名 — (此處未使用) 金鑰大小 — 512注意：如果使用「簡單證書註冊協定」(SCEP)請求SSL證書或身份證書，則只有這些RSA選項可用。RSA 512位RSA 768位RSA 1024位RSA 2048位DSA 512位DSA 768位DSA 1024位

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.

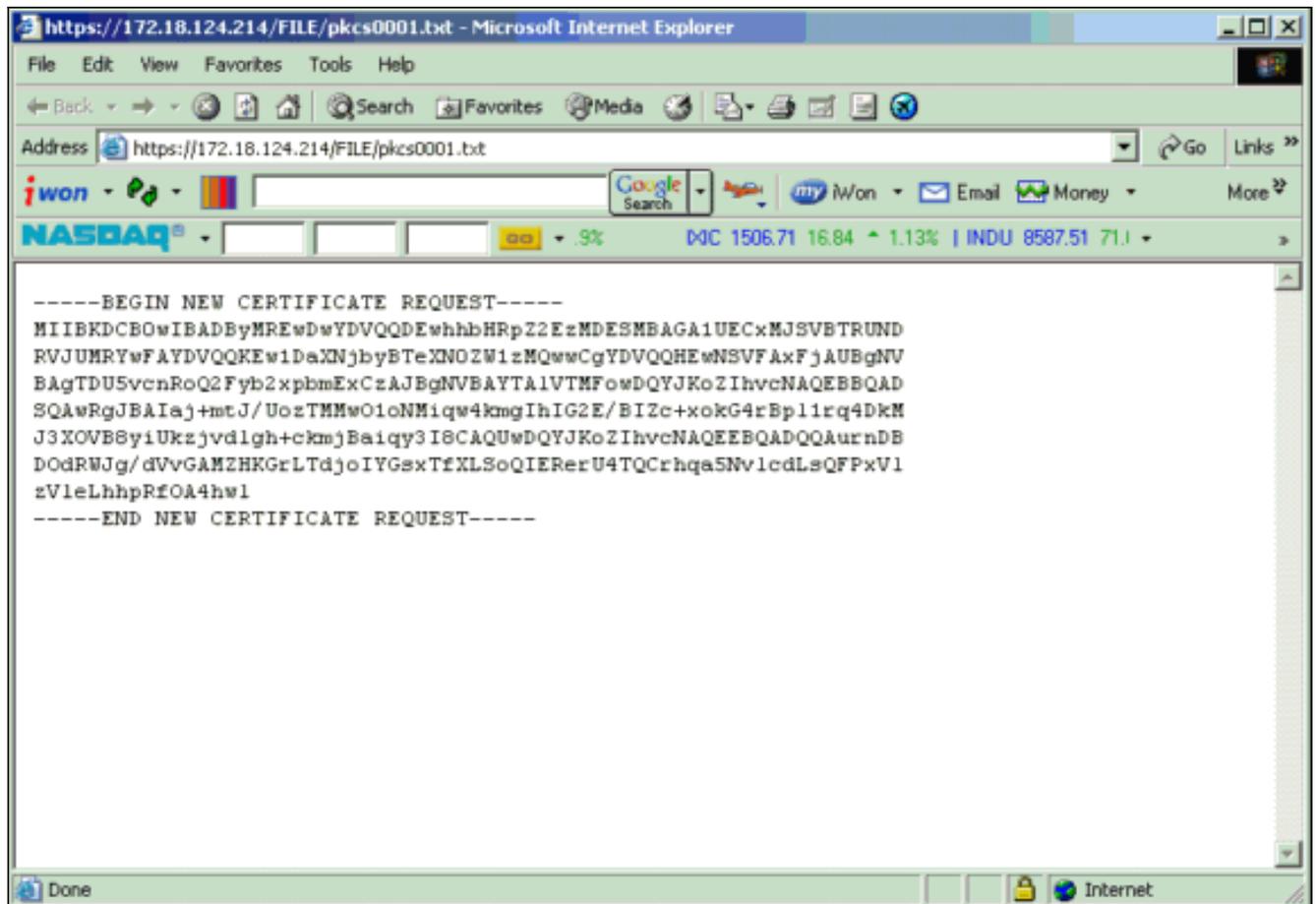
4. 按一下**Enroll**後，將顯示多個視窗。第一個視窗確認您已請求證書。

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.

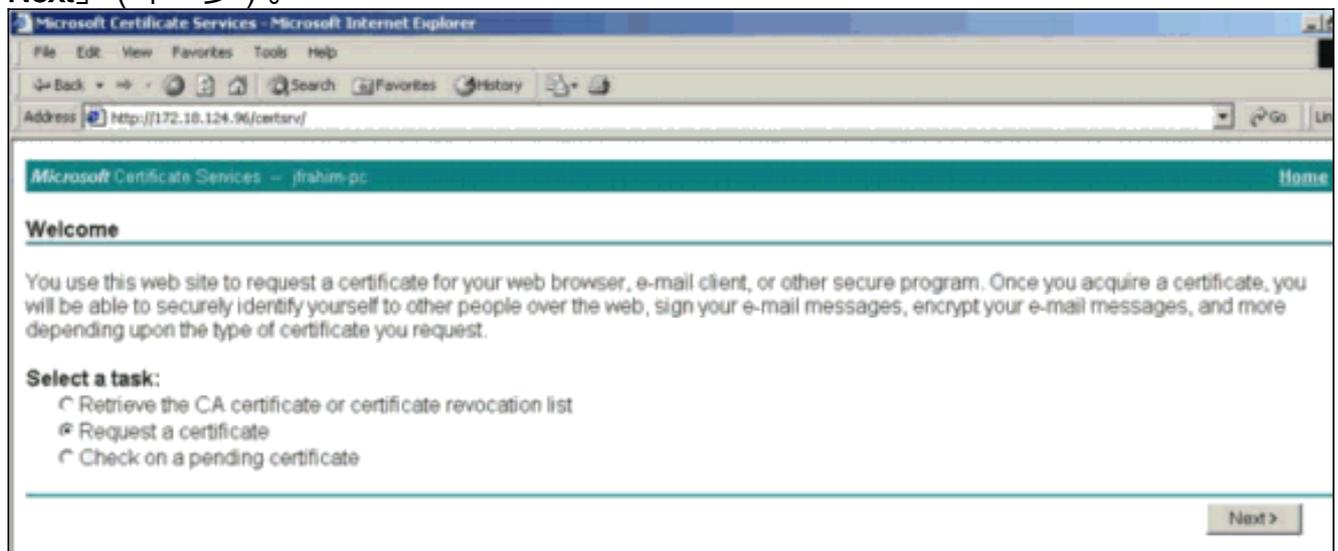
The request is located on the VPN 3000 Concentrator with the filename **pkcs0001.txt**. When you are done, you should delete this file; go to the [File Management page](#) to delete the certificate request.

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

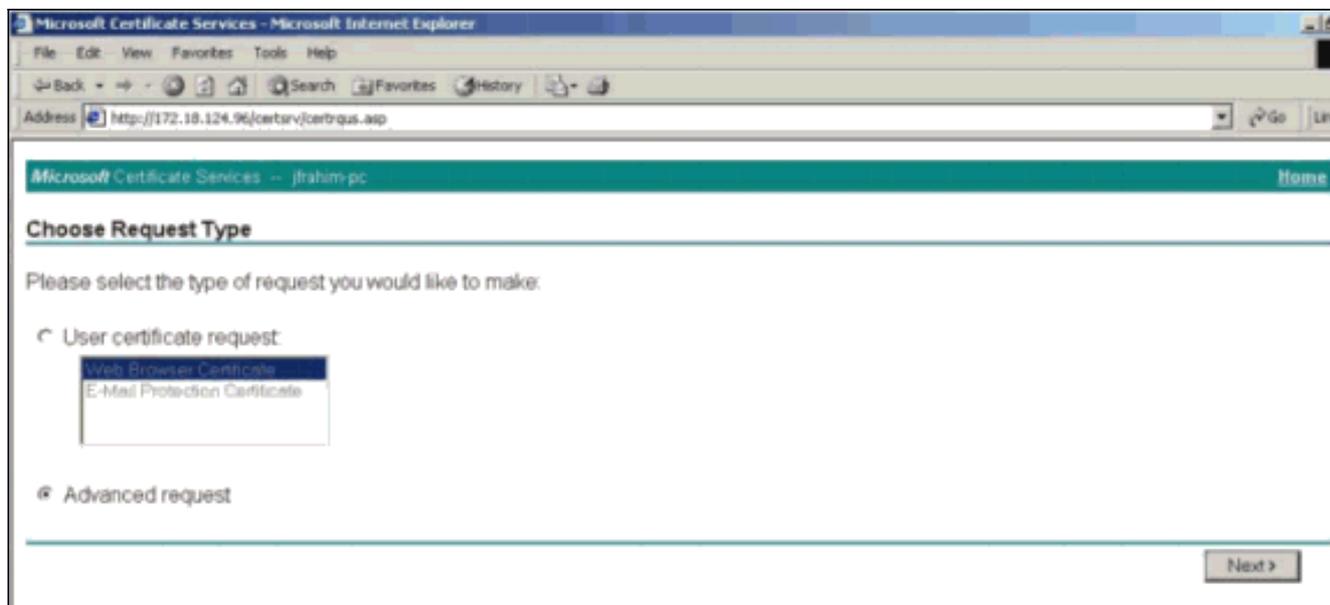
還會開啟一個新的瀏覽器視窗，並顯示您的PKCS請求檔案。



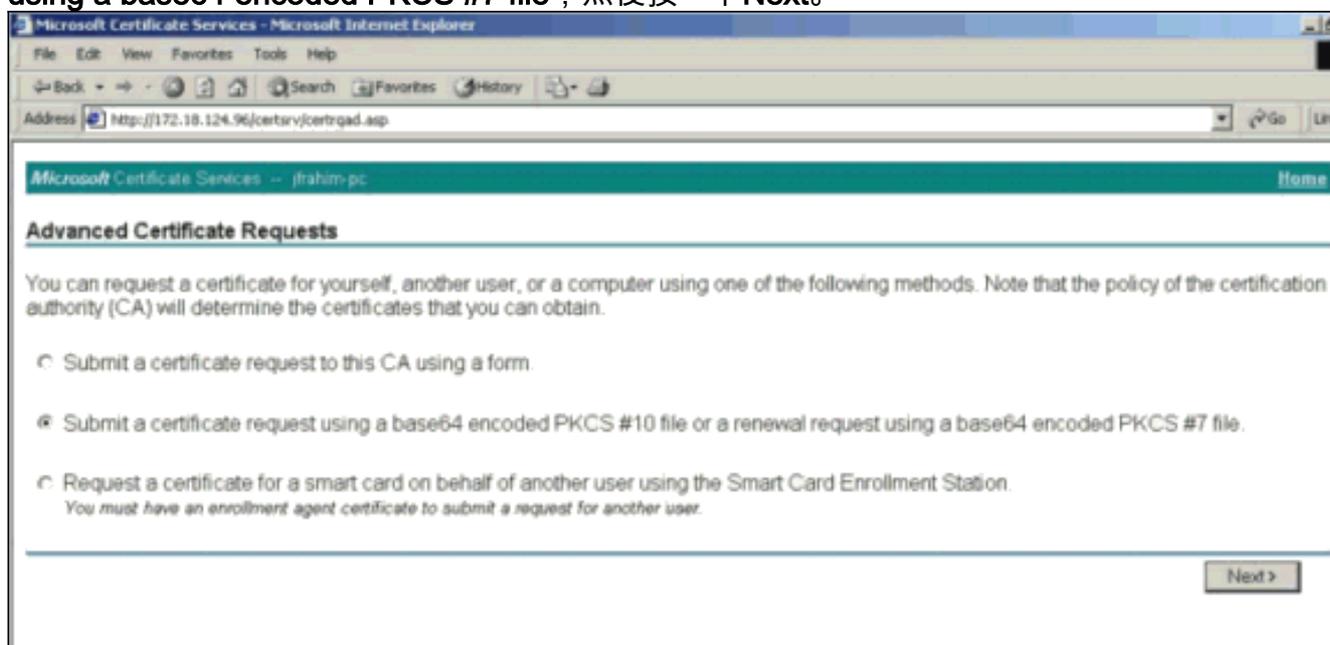
5. 在證書頒發機構(CA)伺服器上，突出顯示請求並將其貼上到CA伺服器以提交請求。按「Next」(下一步)。



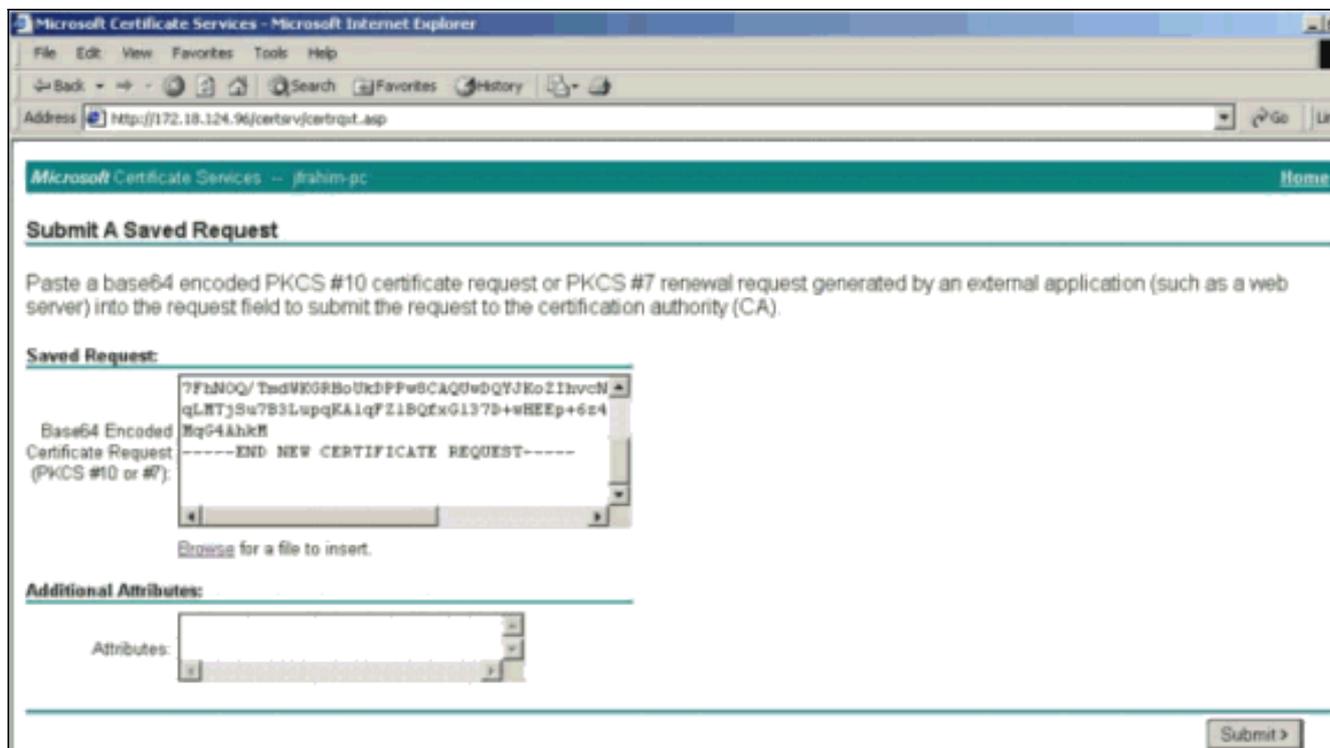
6. 選擇Advanced request，然後按一下Next。



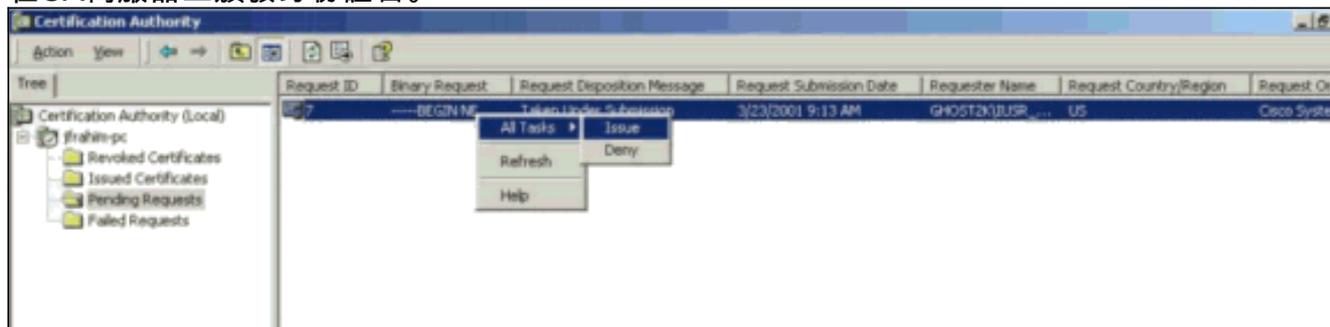
7. 選擇Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file，然後按一下Next。



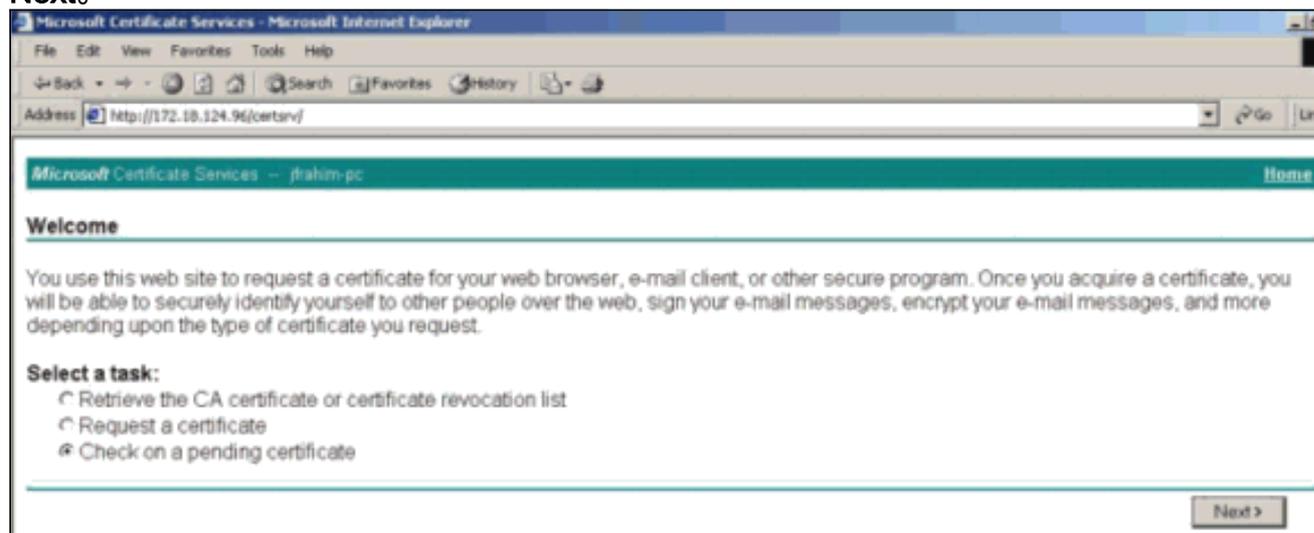
8. 將PKCS檔案剪下並貼上到Saved Request部分下的文本欄位中。然後按一下Submit。



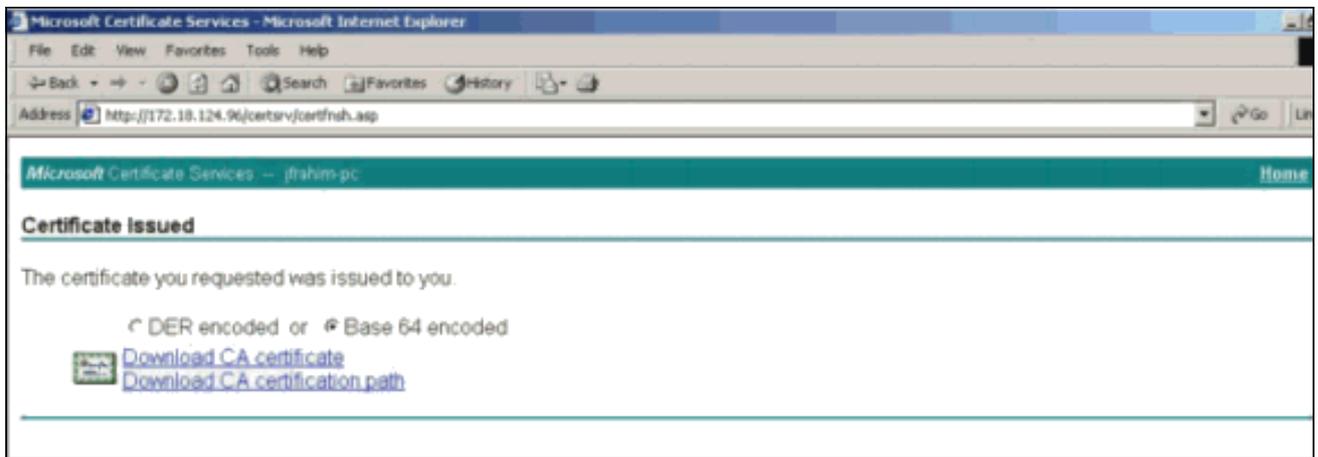
9. 在CA伺服器上頒發身份證書。



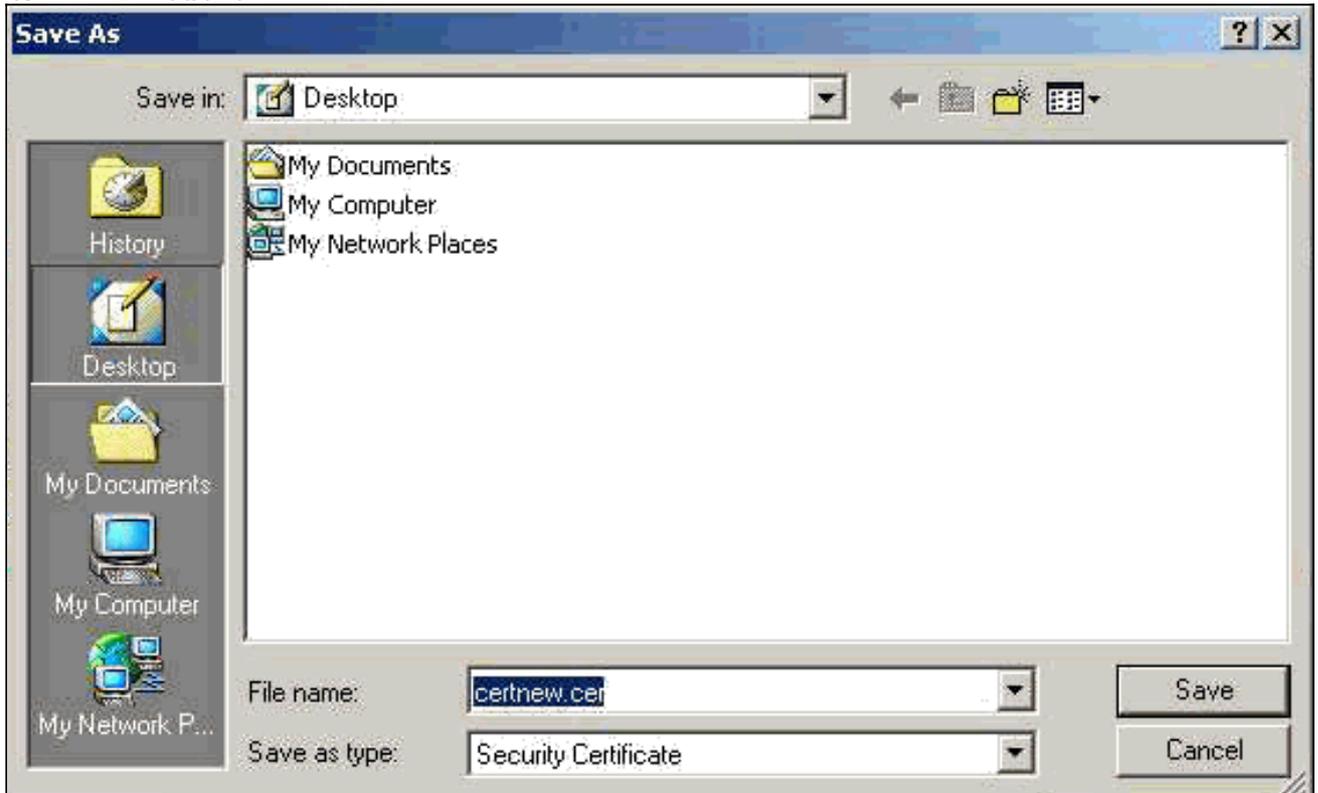
10. 下載根和身份證書。在CA伺服器上，選擇Check on a pending certificate，然後按一下Next。



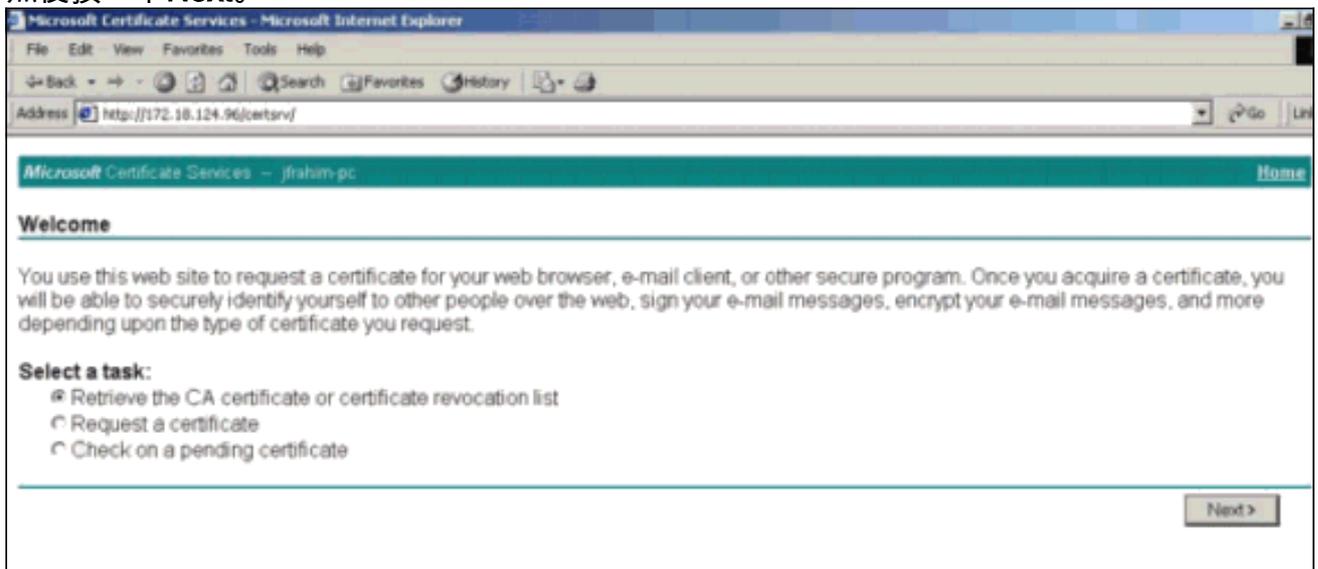
11. 選擇Base 64 encoded，然後按一下Download CA certificate on the CA server。



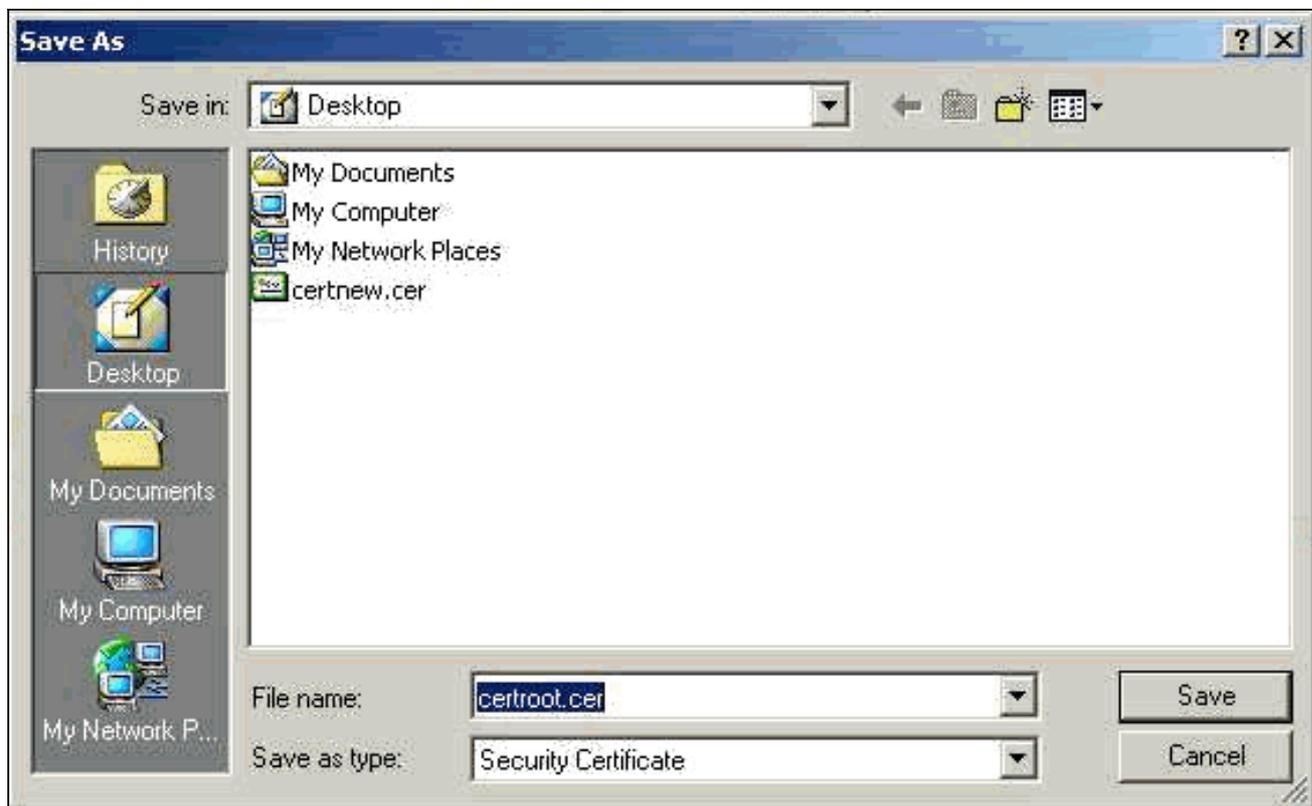
12. 將身份證書儲存在本地驅動器上。



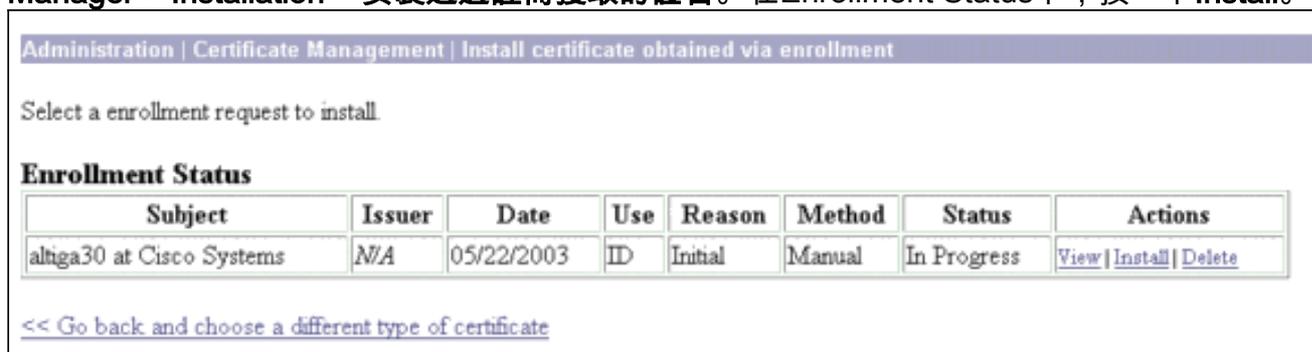
13. 在CA伺服器上，選擇Retrieve the CA certificate or certificate revocation list以取得根憑證。然後按一下Next。



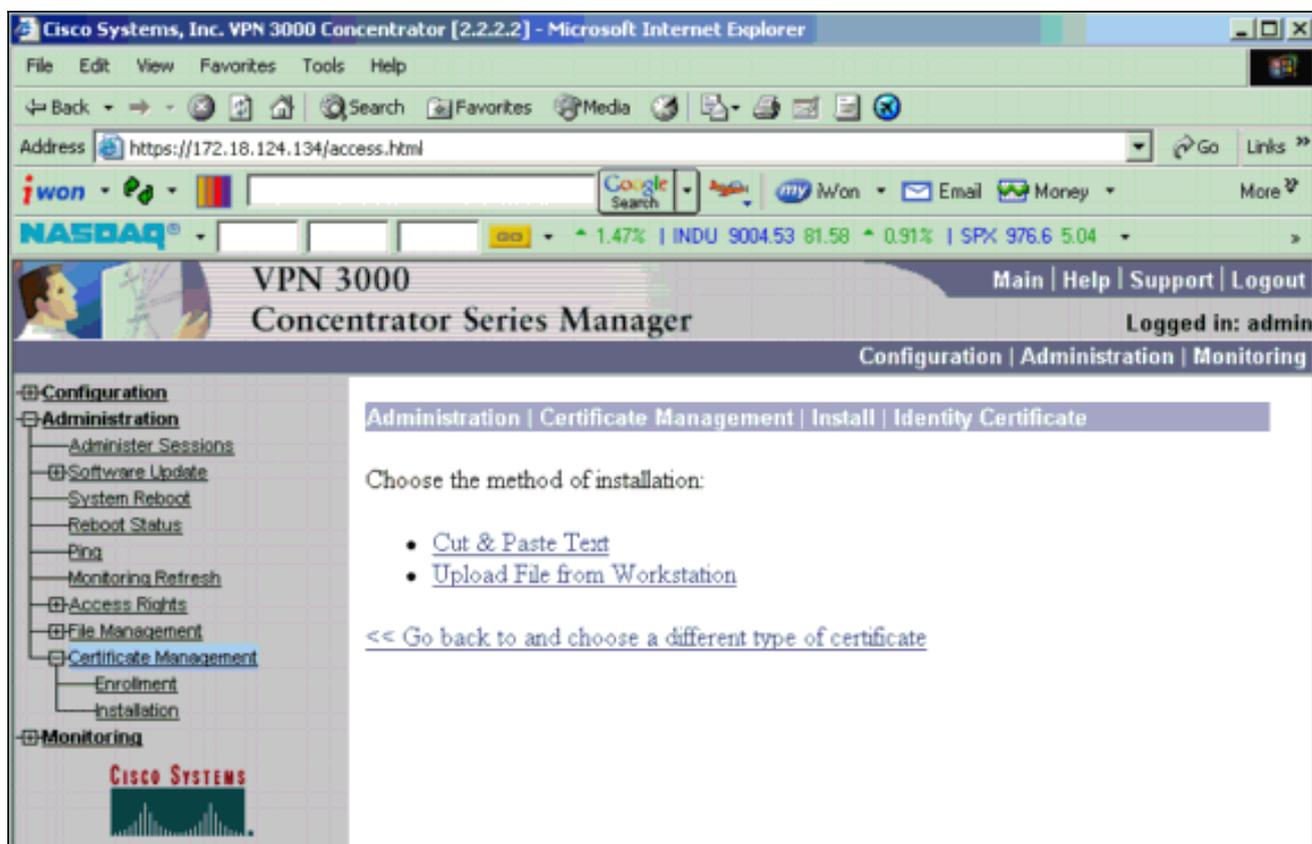
14. 將根證書儲存在本地驅動器上。



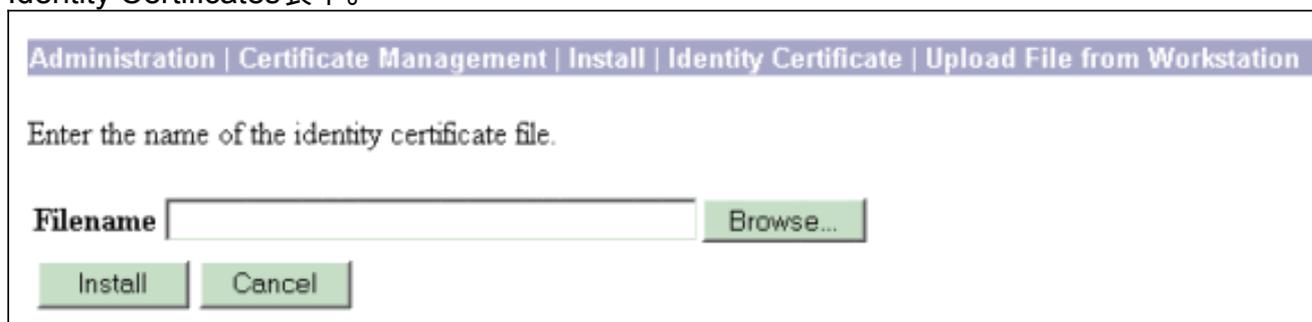
15. 在VPN 3000 Concentrator上安裝根和身份證書。若要執行此操作，請選擇**管理 > Certificate Manager > Installation > 安裝通過註冊獲取的證書**。在Enrollment Status下，按一下**Install**。



16. 按一下「Upload File from Workstation」。



17. 按一下**Browse**，然後選擇儲存到本地驅動器中的根證書檔案。選擇**安裝**以在VPN集中器上安裝身份證書。行政部門 | Certificate Management視窗顯示為確認，新的身份證書出現在 Identity Certificates表中。



注意：如果證書失敗，請完成以下步驟以生成新證書。選擇**Administration > Certificate Management**。在SSL Certificate清單的Actions框中按一下**Delete**。選擇**Administration > System Reboot**。選擇**Save the active configuration at time of reboot**，選擇**Now**，然後按一下**Apply**。現在，您可以在重新載入完成後產生新憑證。

在VPN集中器上安裝SSL證書

如果您在瀏覽器和VPN集中器之間使用安全連線，則VPN集中器需要SSL證書。您還需要在用於管理VPN集中器和WebVPN的介面以及終止WebVPN隧道的每個介面上獲得SSL證書。

升級VPN 3000集中器軟體後，當VPN 3000集中器重新啟動時，將自動生成介面SSL證書（如果不存在）。因為自簽名證書是自生成的，所以此證書不可驗證。沒有證書頒發機構保證其身份。但是此證書允許您使用瀏覽器與VPN集中器進行初始聯絡。如果要將其替換為另一個自簽名SSL證書，請完成以下步驟：

1. 選擇**Administration > Certificate Management**。

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. 按一下「**Generate**」可在「SSL Certificate」表中顯示新憑證並替換現有憑證。此視窗允許您配置VPN集中器自動生成的SSL證書的欄位。這些SSL證書用於介面和負載均衡。

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.

如果要獲取可驗證的SSL證書（即由證書頒發機構頒發的證書），若要使用獲取身份證書所使用的相同過程，請參閱本文檔的[在VPN集中器上安裝數位證書](#)部分。但這一次，在 **Administration > Certificate Management > Enroll** 視窗中，按一下 **SSL certificate**（而不是 Identity Certificate）。**注意：**請參閱管理 [VPN 3000集中器](#) 參考 [卷II的證書管理部分：管理和監控版本4.7](#) 瞭解有關數位證書和SSL證書的完整資訊。

在VPN集中器上續訂SSL證書

本節介紹如何續訂SSL證書：

如果這是針對VPN集中器生成的SSL證書，請轉到SSL部分上的**管理>證書管理**。按一下「**renew**」選項，就會更新SSL憑證。

如果這是外部CA伺服器授予的憑證，請完成以下步驟：

1. 在 *SSL Certificates* 下選擇 **Administration > Certificate Management > Delete**，以便從公共介面刪除過期的證書。

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



按一下「Yes」以確認刪除SSL憑證。

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. 選擇 **Administration > Certificate Management > Generate** 以生成新的SSL證書。

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



系統將顯示公共介面的新SSL證書。

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

相關資訊

- [Cisco VPN 3000系列集中器支援頁面](#)
- [IPSec 協商/IKE 通訊協定](#)
- [技術支援與文件 - Cisco Systems](#)