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

目錄

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。

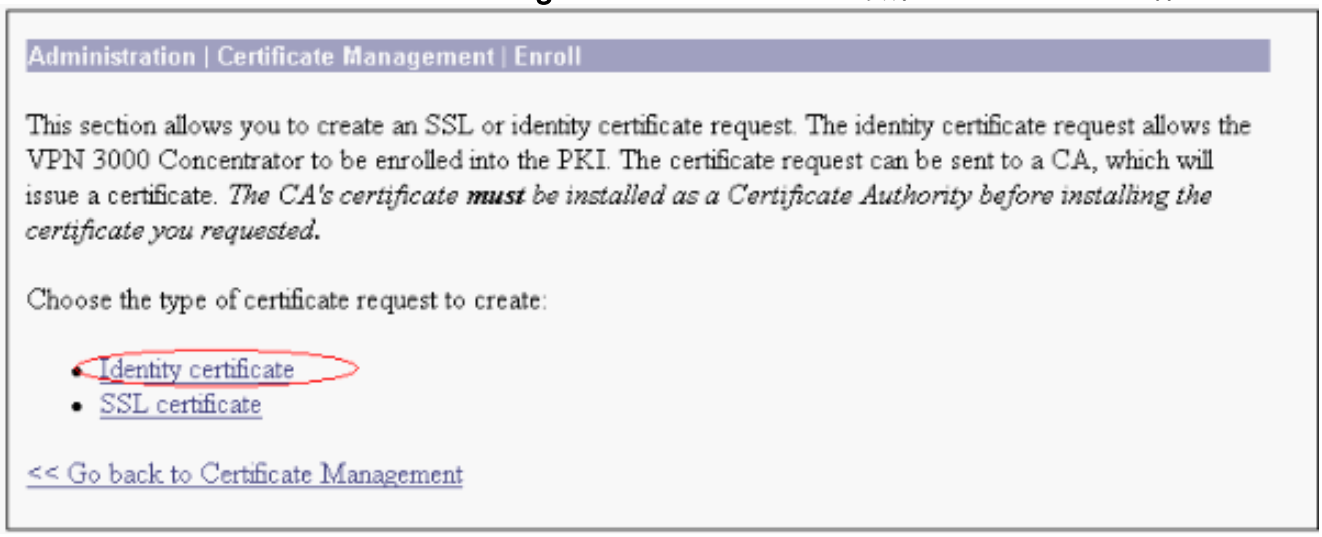
慣例

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。

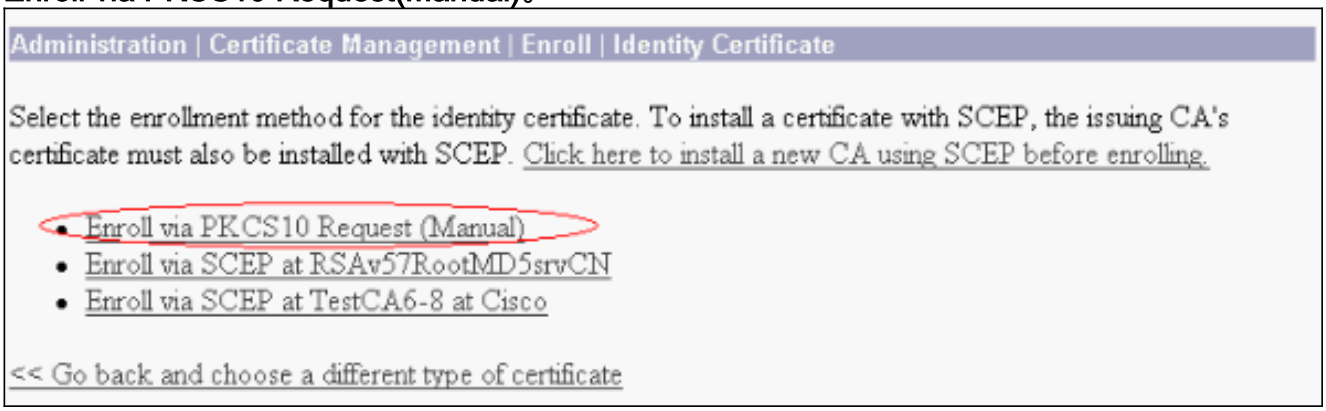
在VPN集中器上安裝數位證書

請完成以下步驟：

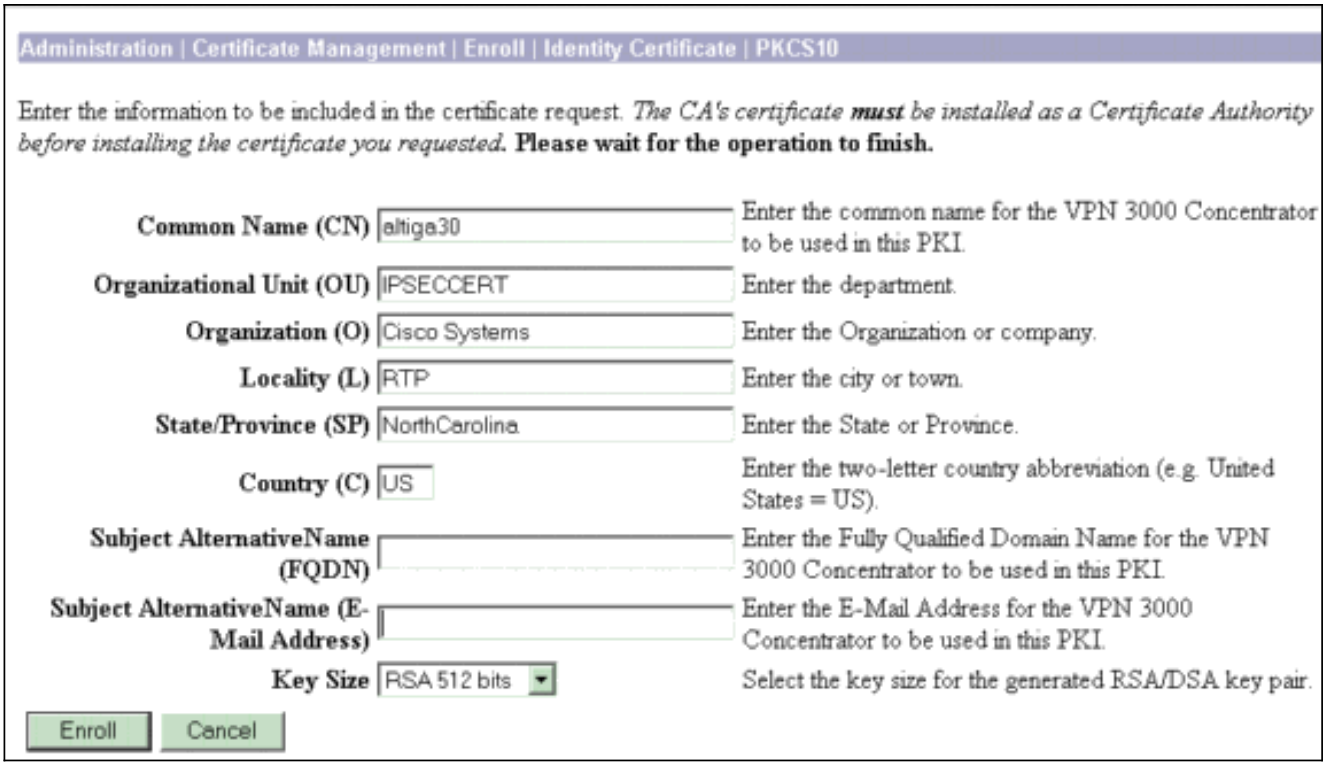
1. 選擇**Administration > Certificate Management > Enroll** 以選擇數位證書或身份證書請求。



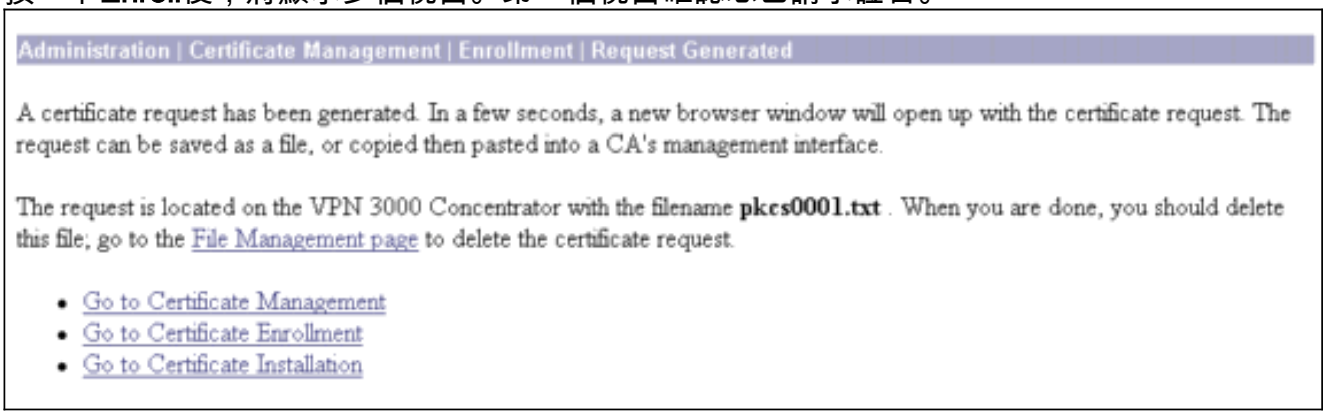
2. 選擇**Administration > Certificate Management > Enrollment > Identity Certificate**，然後按一下**Enroll via PKCS10 Request(Manual)**。



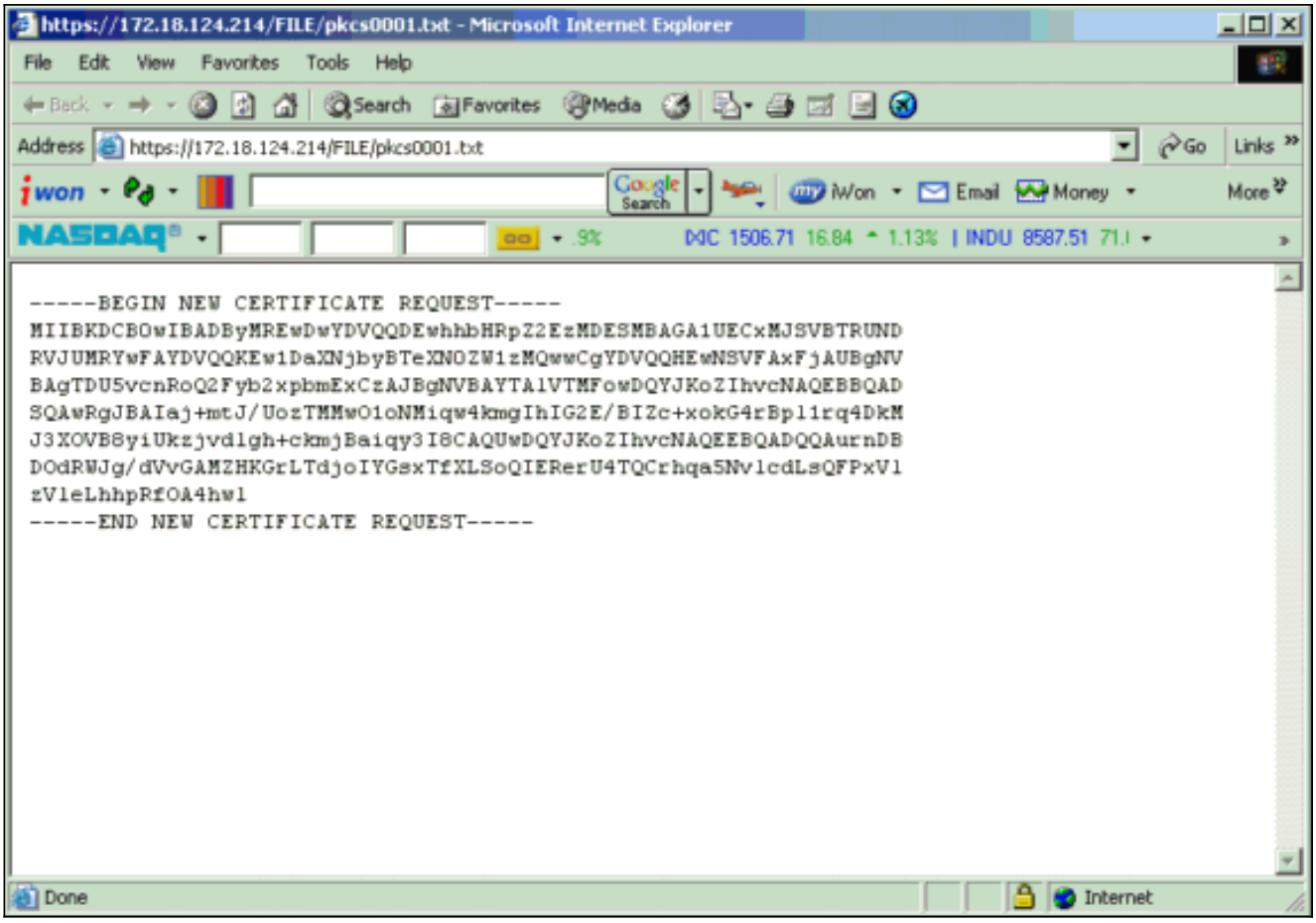
3. 填寫請求的欄位，然後按一下**Enroll**。本示例中填寫了這些欄位。**常用名**稱 — altiga30**組織單**位 — IPSECCERT（OU應與配置的IPsec組名匹配）**組織**- Cisco Systems**位置**- RTP**州/省** — **北**卡羅萊納**國家** — 美國**完全限定域名** —（此處未使用）**金鑰大**小 — 512**注意：**如果使用「簡單證書註冊協定」(SCEP)請求SSL證書或身份證書，則只有這些RSA選項可用。RSA 512位RSA 768位RSA 1024位RSA 2048位DSA 512位DSA 768位DSA 1024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



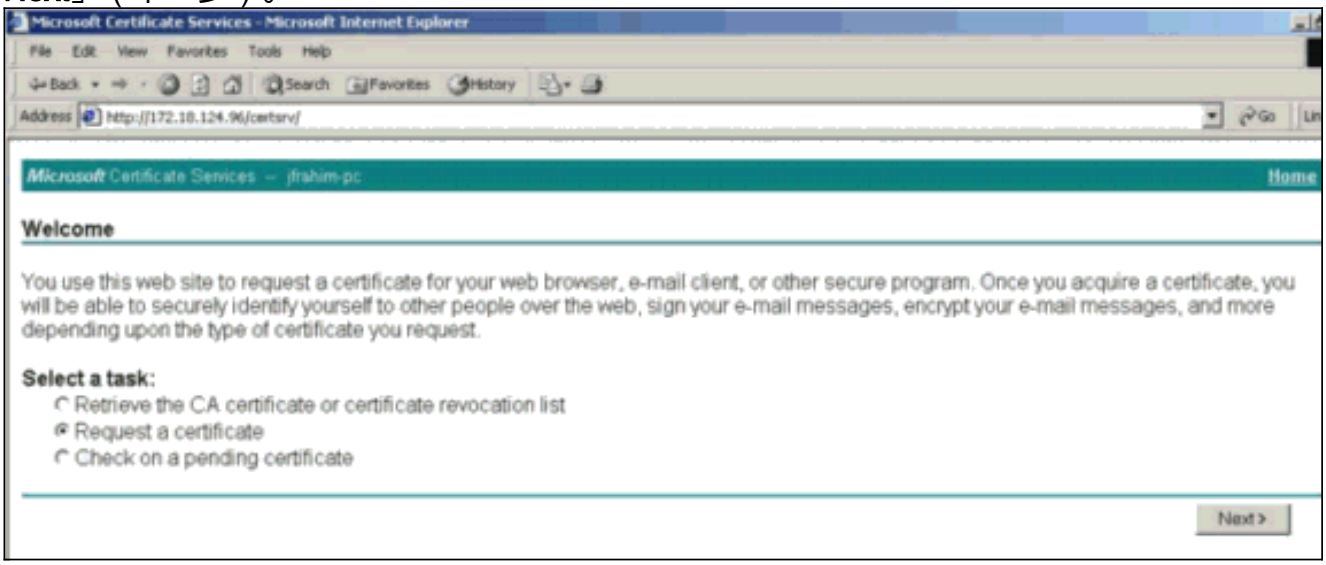
4. 按一下**Enroll**後，將顯示多個視窗。第一個視窗確認您已請求證書。



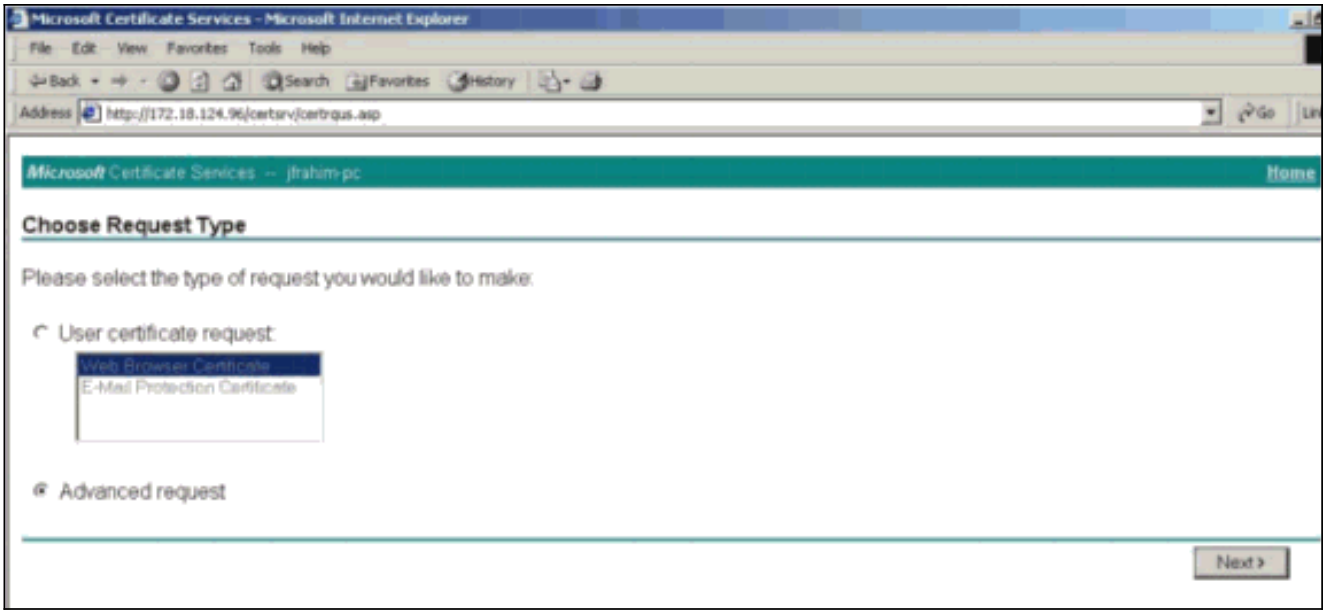
還會開啟一個新的瀏覽器視窗，並顯示您的PKCS請求檔案。



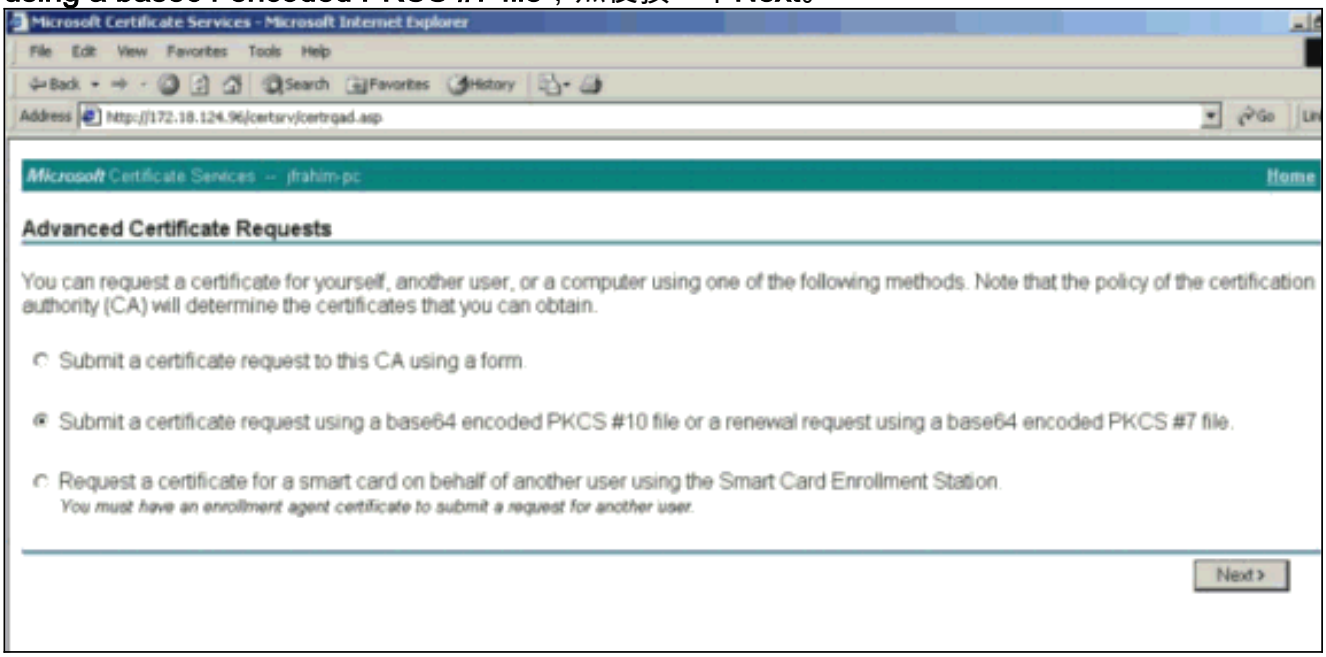
5. 在證書頒發機構(CA)伺服器上，突出顯示請求並將其貼上到CA伺服器以提交請求。按「Next」（下一步）。



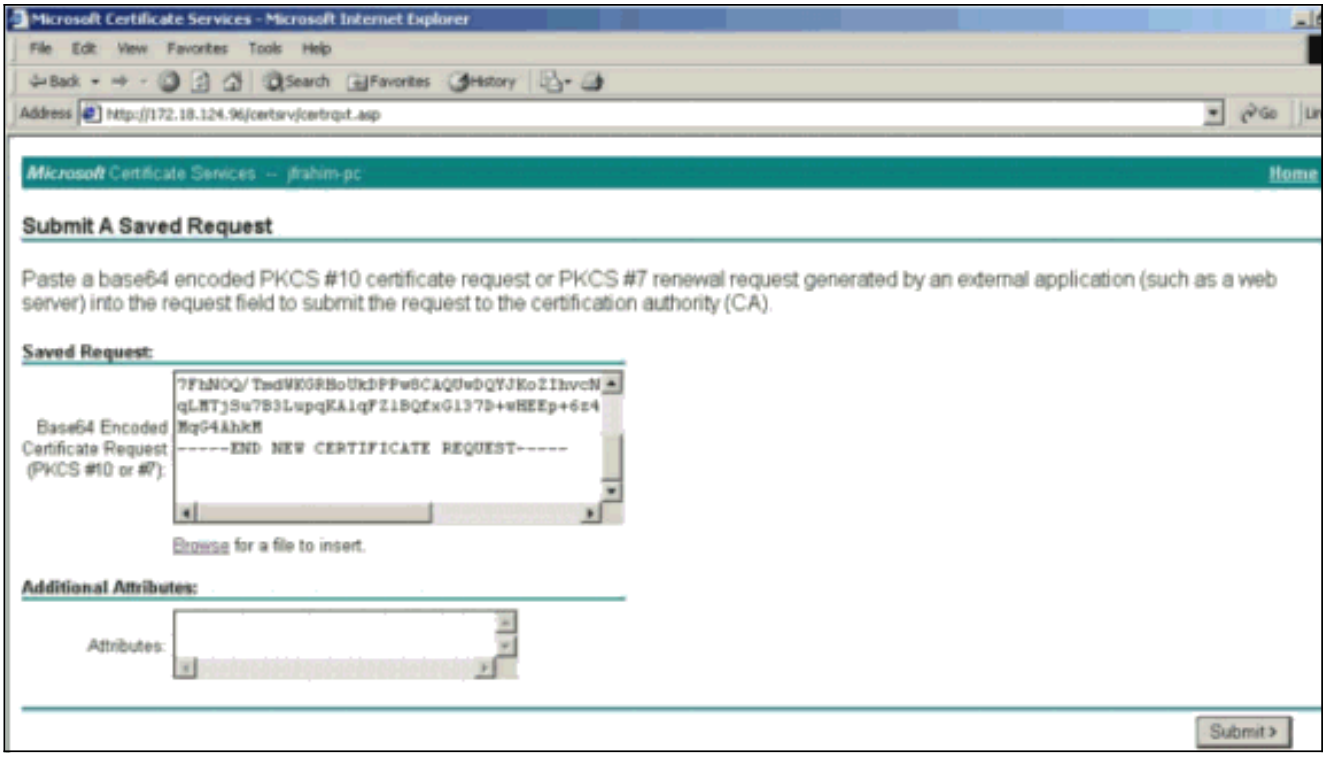
6. 選擇Advanced request，然後按一下Next。



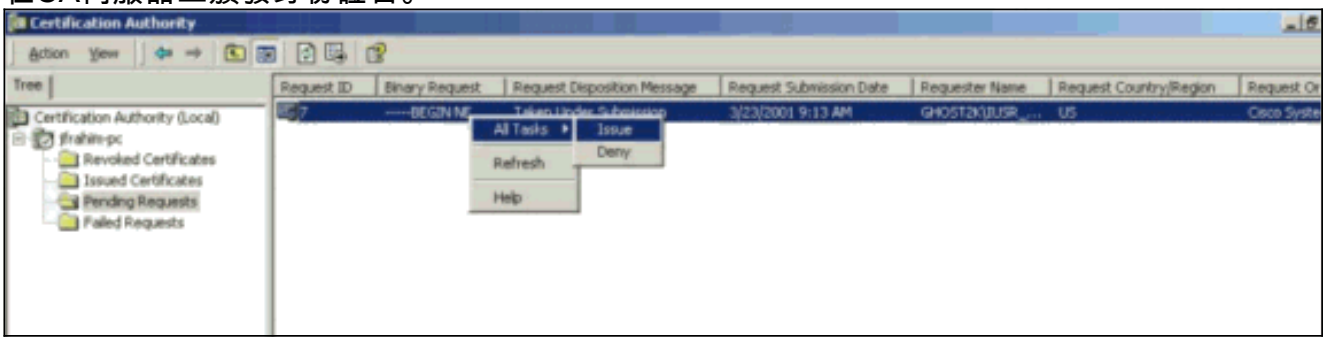
7. 選擇**Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file**，然後按一下**Next**。



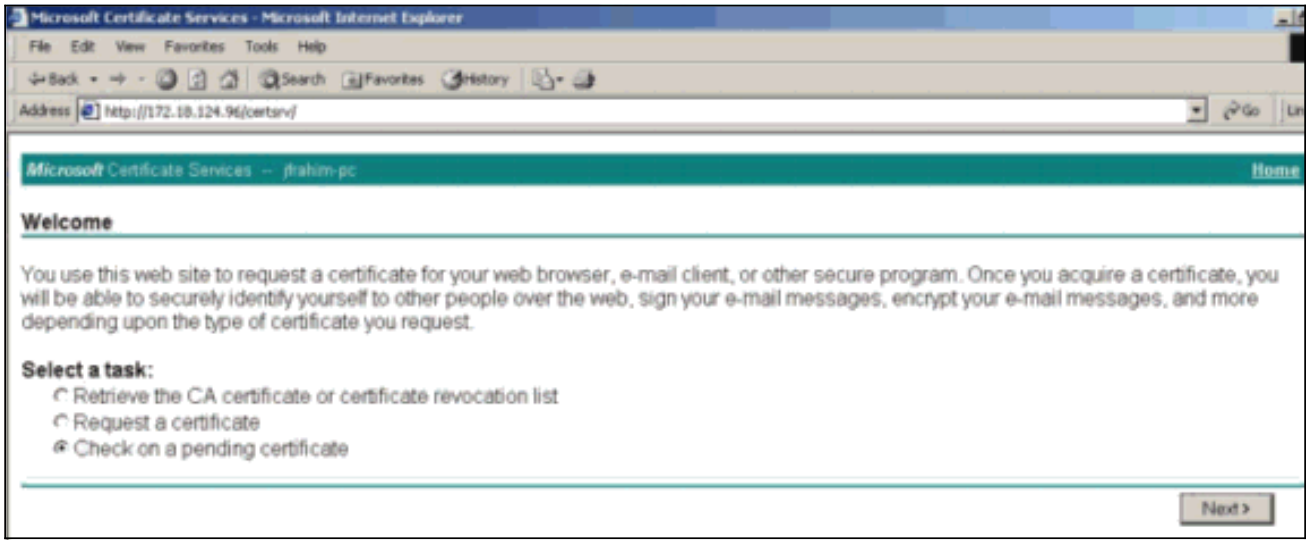
8. 將PKCS檔案剪下並貼上到Saved Request部分下的文本欄位中。然後按一下**Submit**。



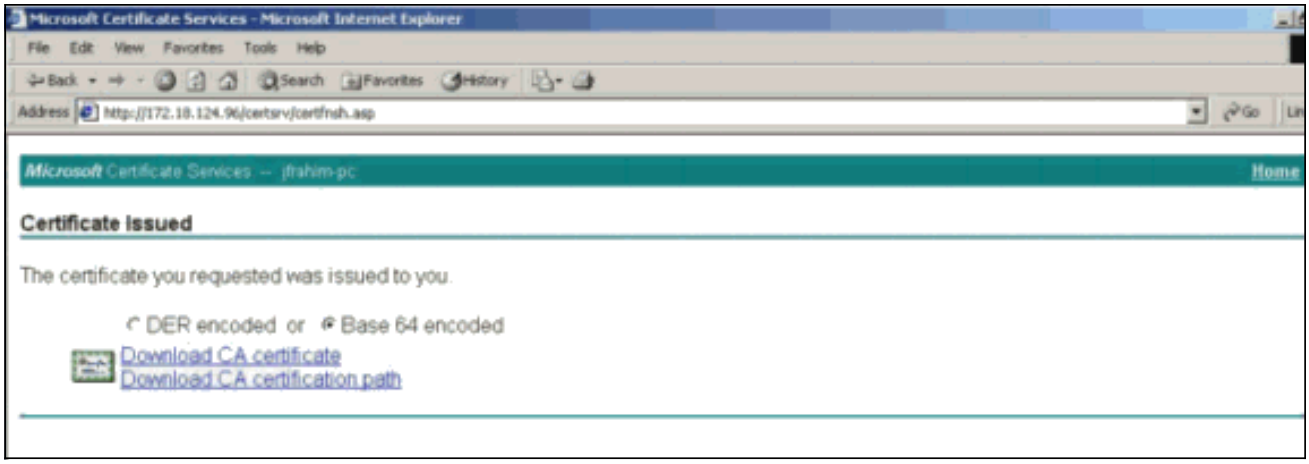
9. 在CA伺服器上頒發身份證書。



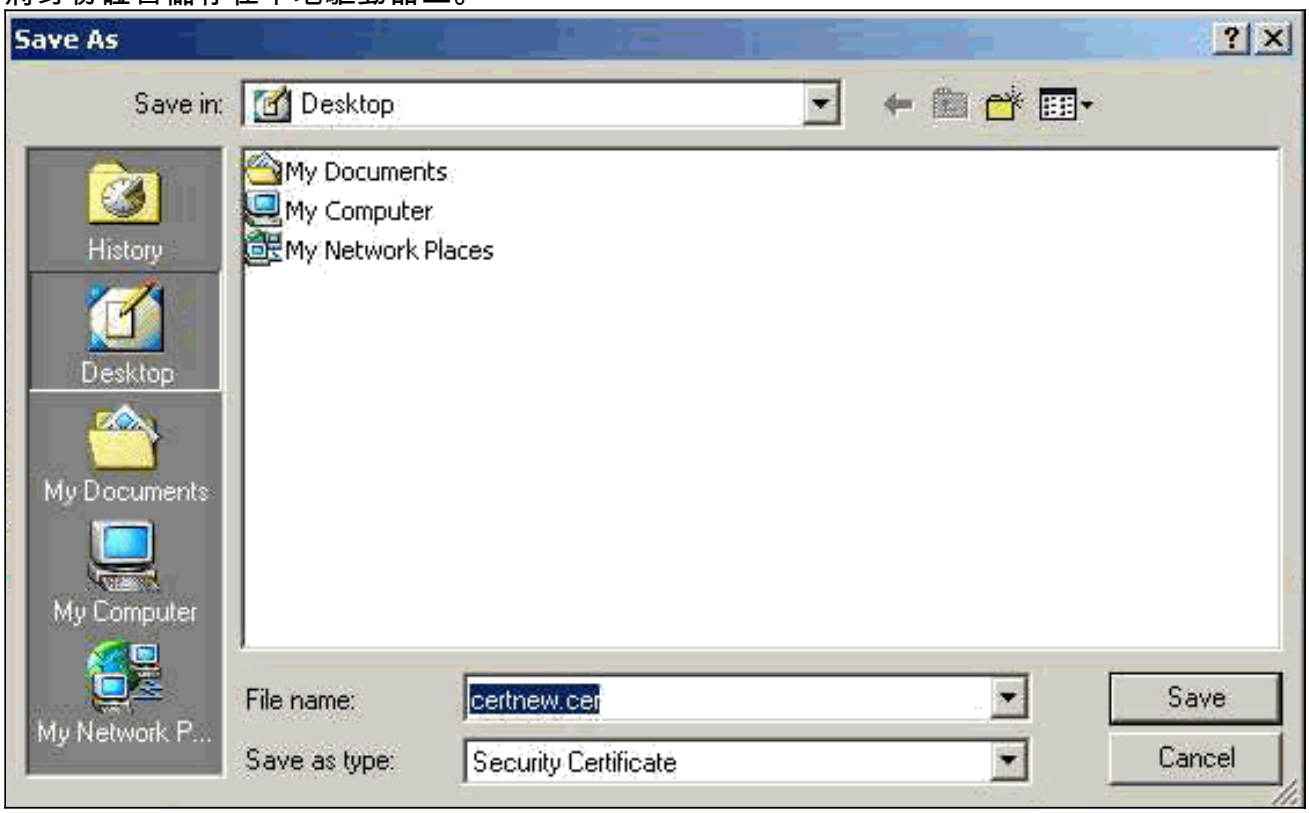
10. 下載根和身份證書。在CA伺服器上，選擇**Check on a pending certificate**，然後按一下**Next**。



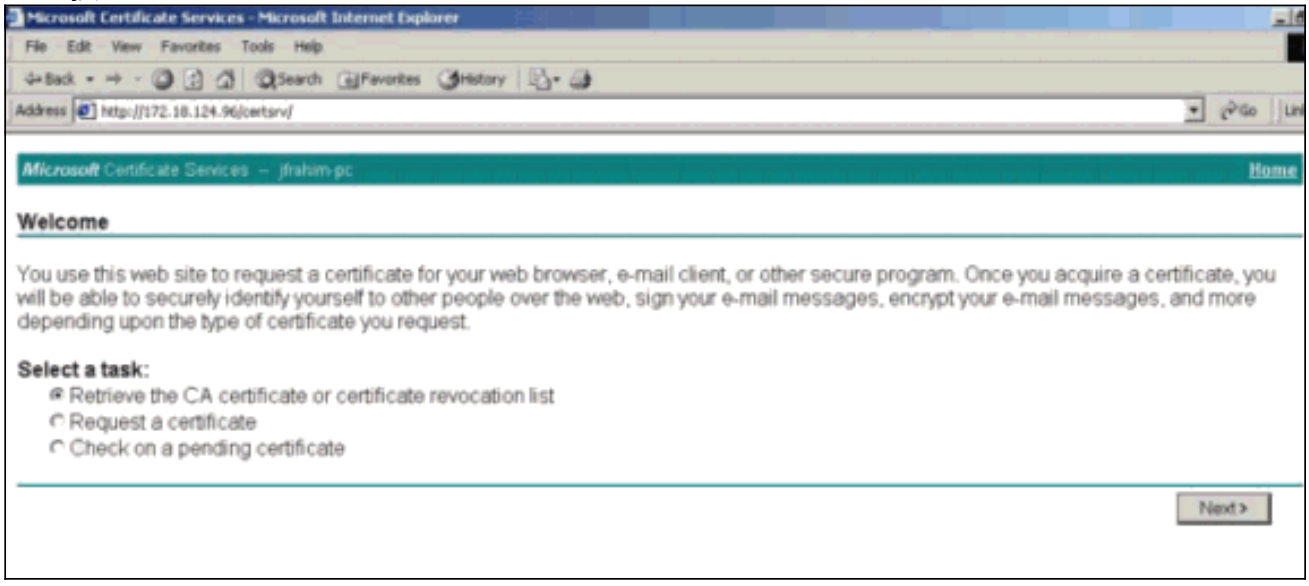
11. 選擇**Base 64 encoded**，然後按一下**Download CA certificate** on the CA server。



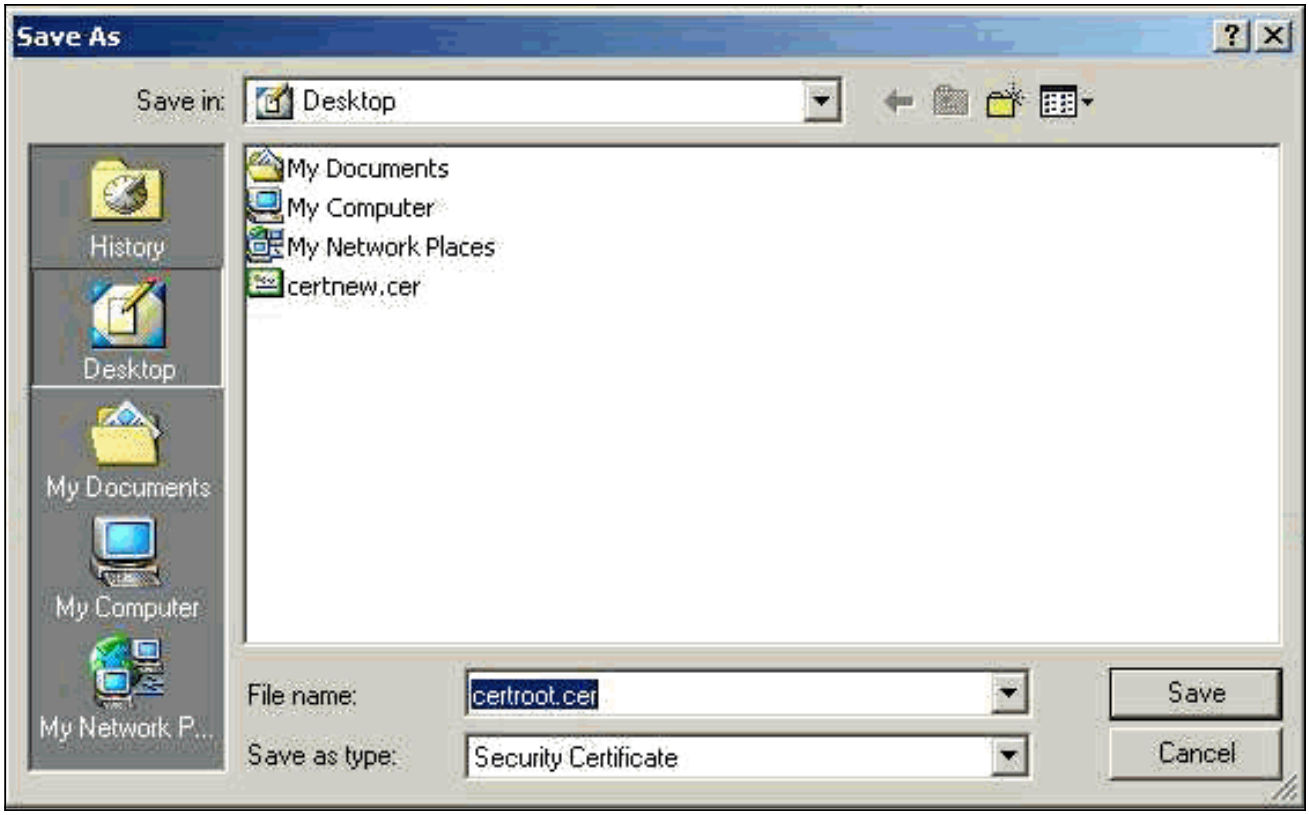
12. 將身份證書儲存在本地驅動器上。



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**。

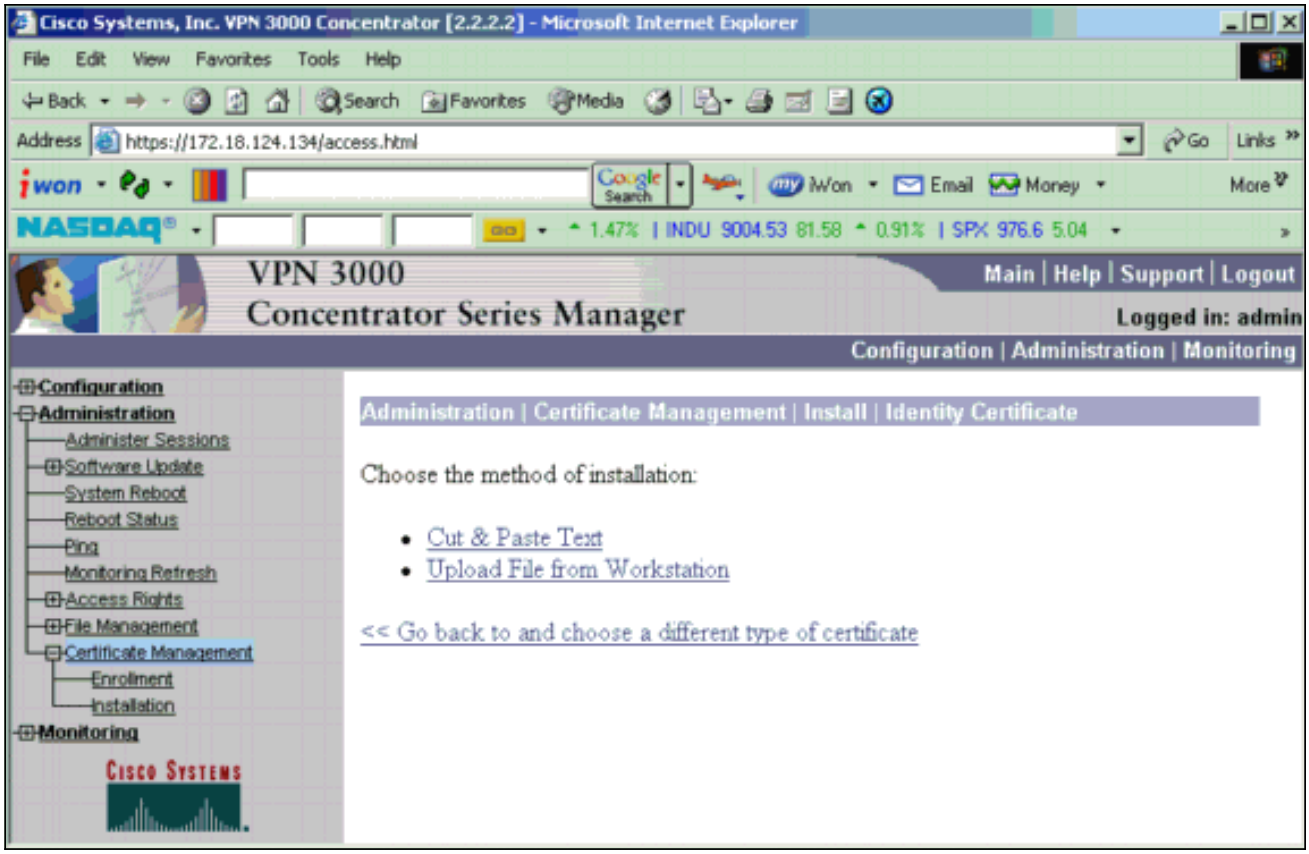


14. 將根證書儲存在本地驅動器上。

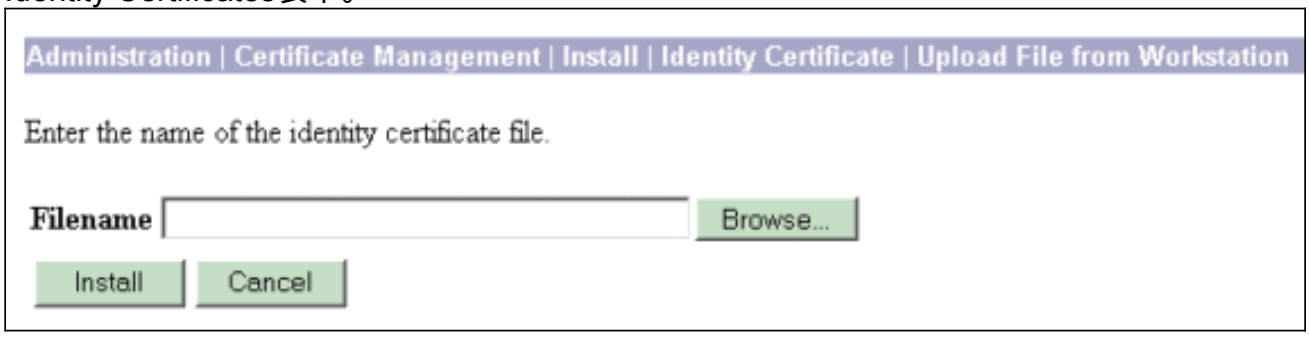


15. 在VPN 3000 Concentrator上安裝根和身份證書。若要執行此操作，請選擇**管理 > Certificate Manager > Installation > 安裝通過註冊獲取的證書**。在Enrollment Status下，按一下**Install**。

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。



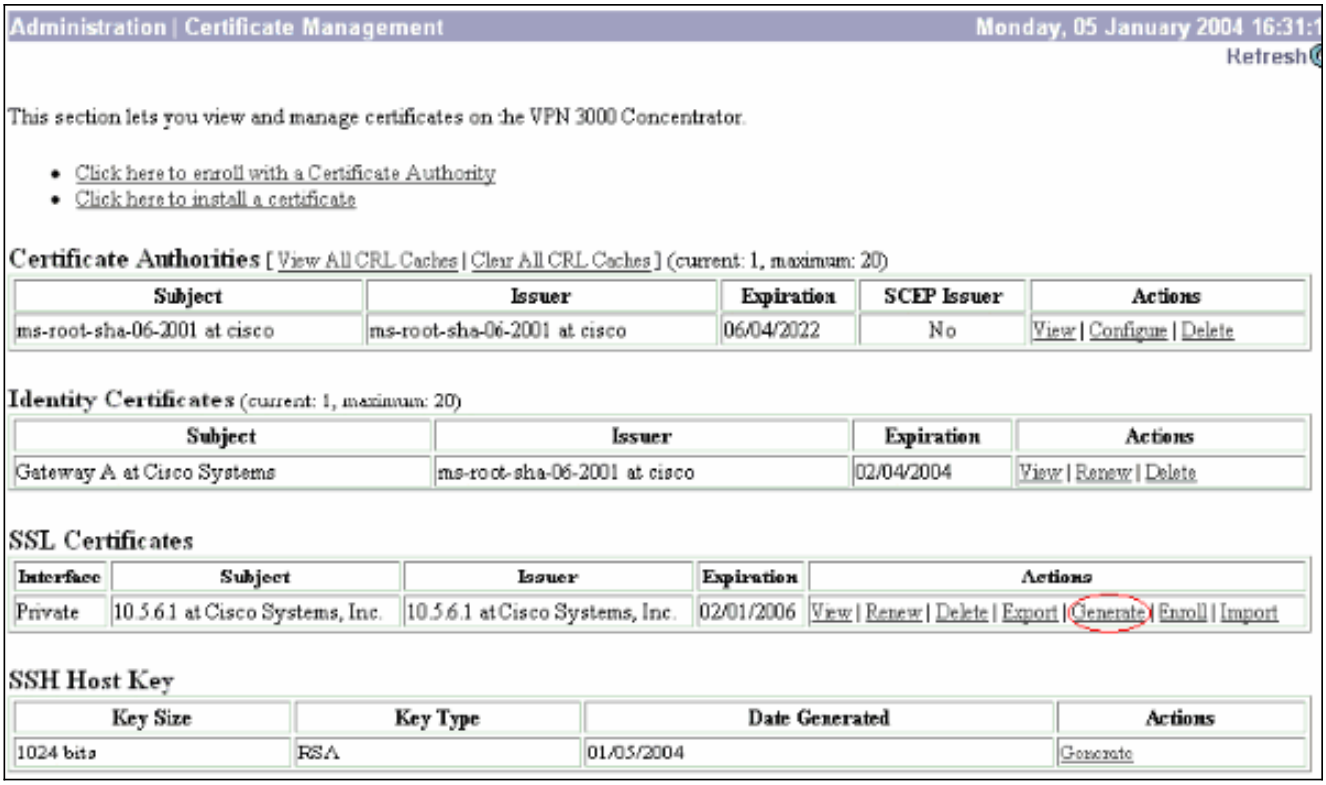
注意：如果證書失敗，請完成以下步驟以生成新證書。選擇**Administration > Certificate Management**。在SSL Certificate清單的Actions框中按一下**Delete**。選擇**Administration > System Reboot**。選擇**Save the active configuration at time of reboot**，選擇**Now**，然後按一下**Apply**。現在，您可以在重新載入完成後產生新憑證。

在VPN集中器上安裝SSL證書

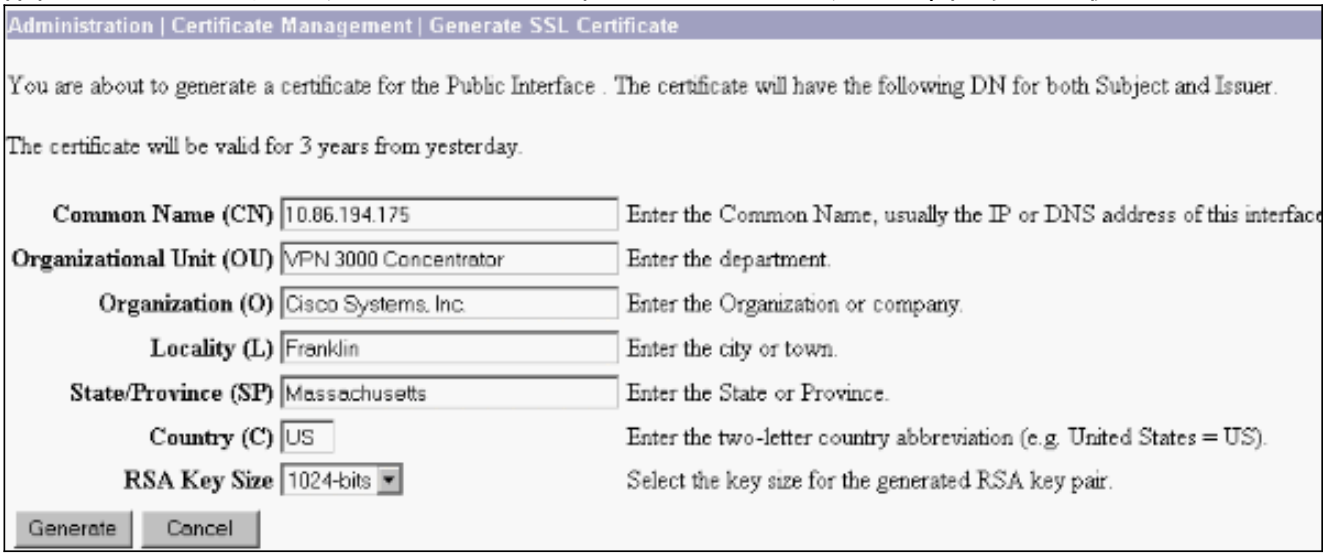
如果您在瀏覽器和VPN集中器之間使用安全連線，則VPN集中器需要SSL證書。您還需要在用於管理VPN集中器和WebVPN的介面以及終止WebVPN隧道的每個介面上獲得SSL證書。

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**。



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。



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。

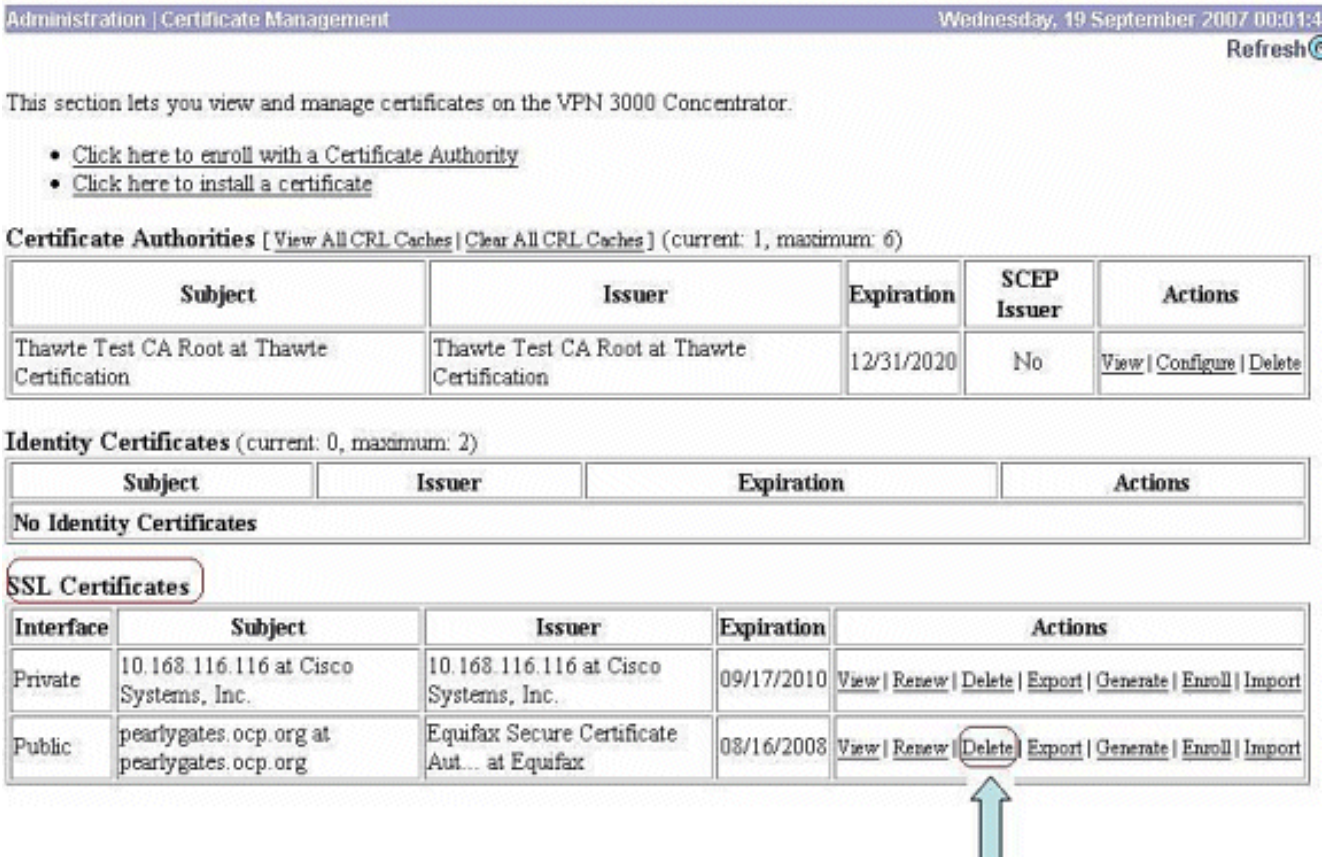
在VPN集中器上續訂SSL證書

本節介紹如何續訂SSL證書：

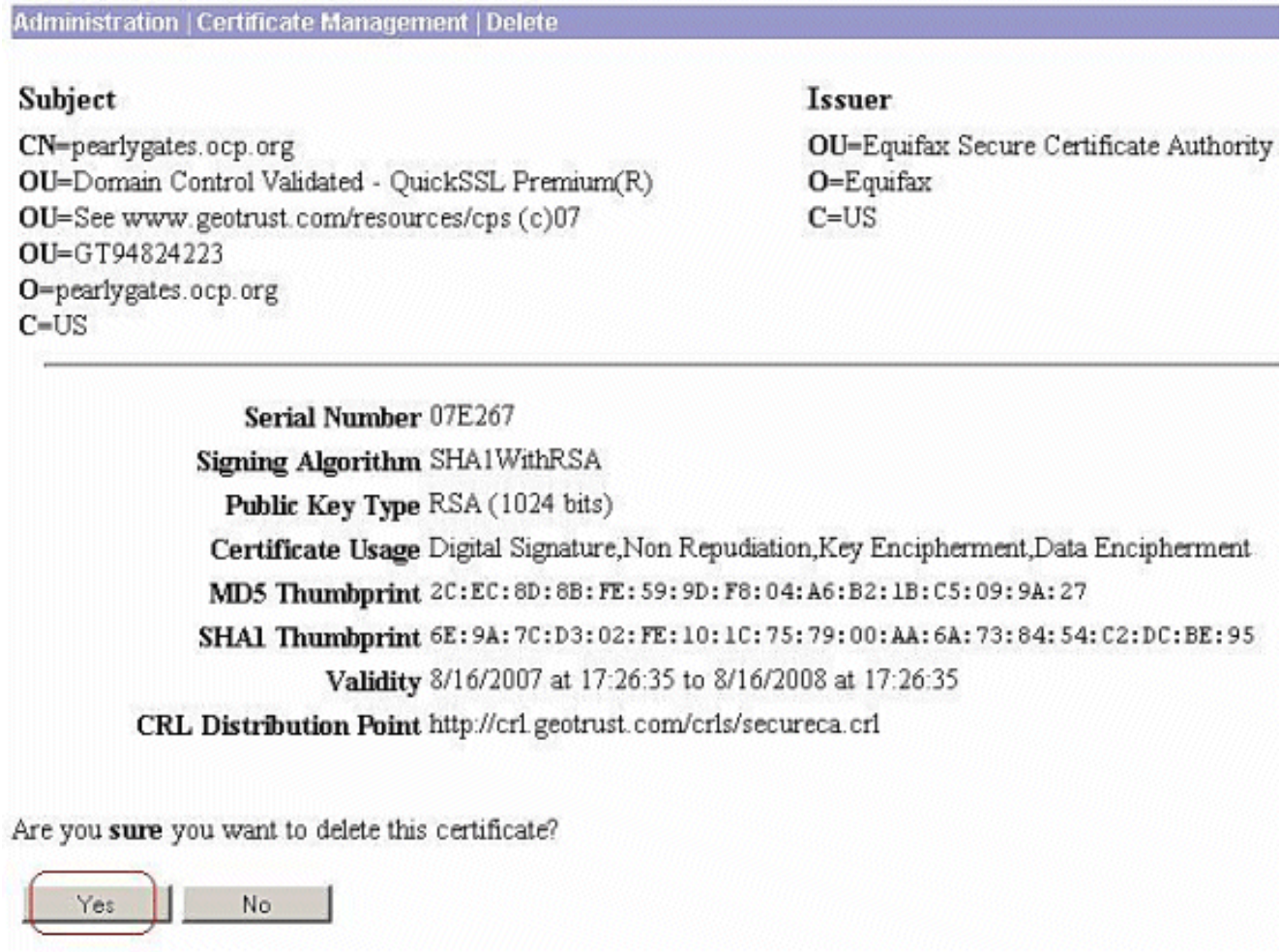
如果這是針對VPN集中器生成的SSL證書，請轉到SSL部分上的**管理>證書管理**。按一下「**renew**」選項，就會更新SSL憑證。

如果這是外部CA伺服器授予的憑證，請完成以下步驟：

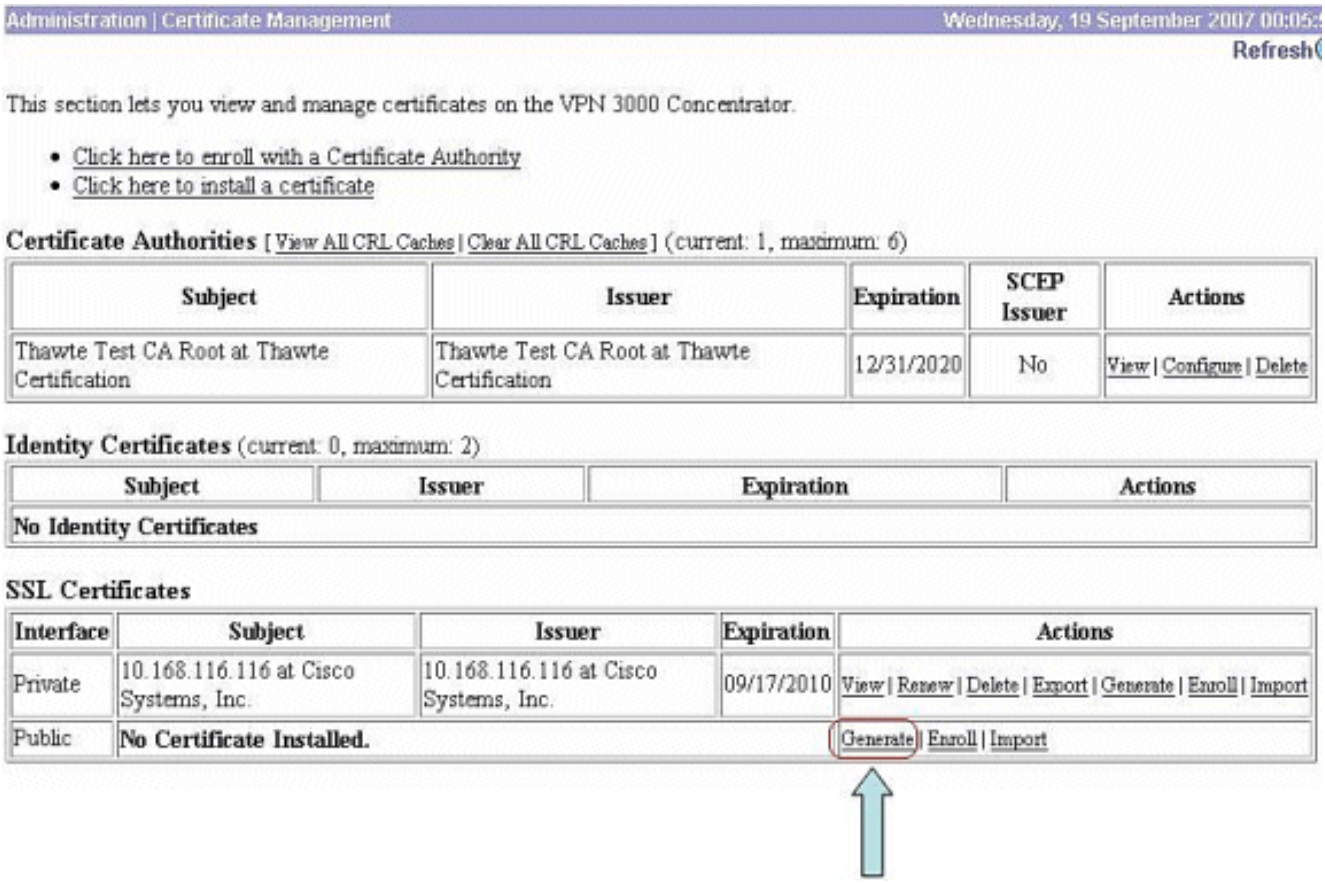
1. 在*SSL Certificates*下選擇**Administration > Certificate Management >Delete**，以便從公共介面刪除過期的證書。



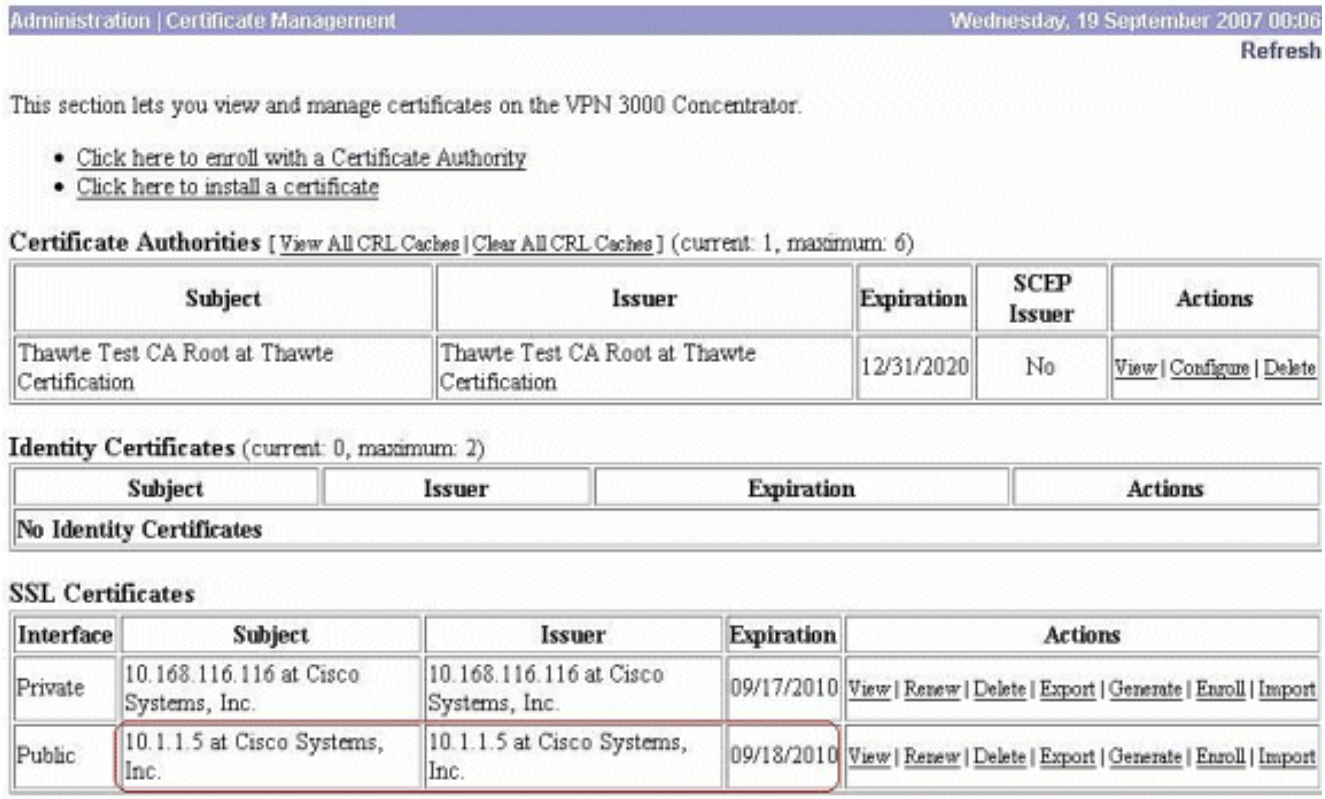
按一下「**Yes**」以確認刪除SSL憑證。



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



系統將顯示公共介面的新SSL證書。



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