ASA 8.x:使用ASDM續訂和安裝SSL證書

目錄

簡介

本文檔中的過程是一個示例，可作為任何證書供應商或您自己的根證書伺服器的指南。您的證書供應商有時需要特殊證書引數要求，但本文檔旨在提供續訂SSL證書並將其安裝在使用8.0軟體的ASA上所需的一般步驟。

必要條件

需求

本文件沒有特定需求。

採用元件

此過程適用於ASA版本8.x和ASDM版本6.0(2)或更高版本。

本文檔中的過程基於安裝證書並用於SSL VPN訪問的有效配置。只要未刪除當前證書，此過程不會影響您的網路。此程式是有關如何為當前憑證核發新的CSR的逐步程式，該當前憑證與核發原始根CA的根憑證相同。

本文中的資訊是根據特定實驗室環境內的裝置所建立。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。

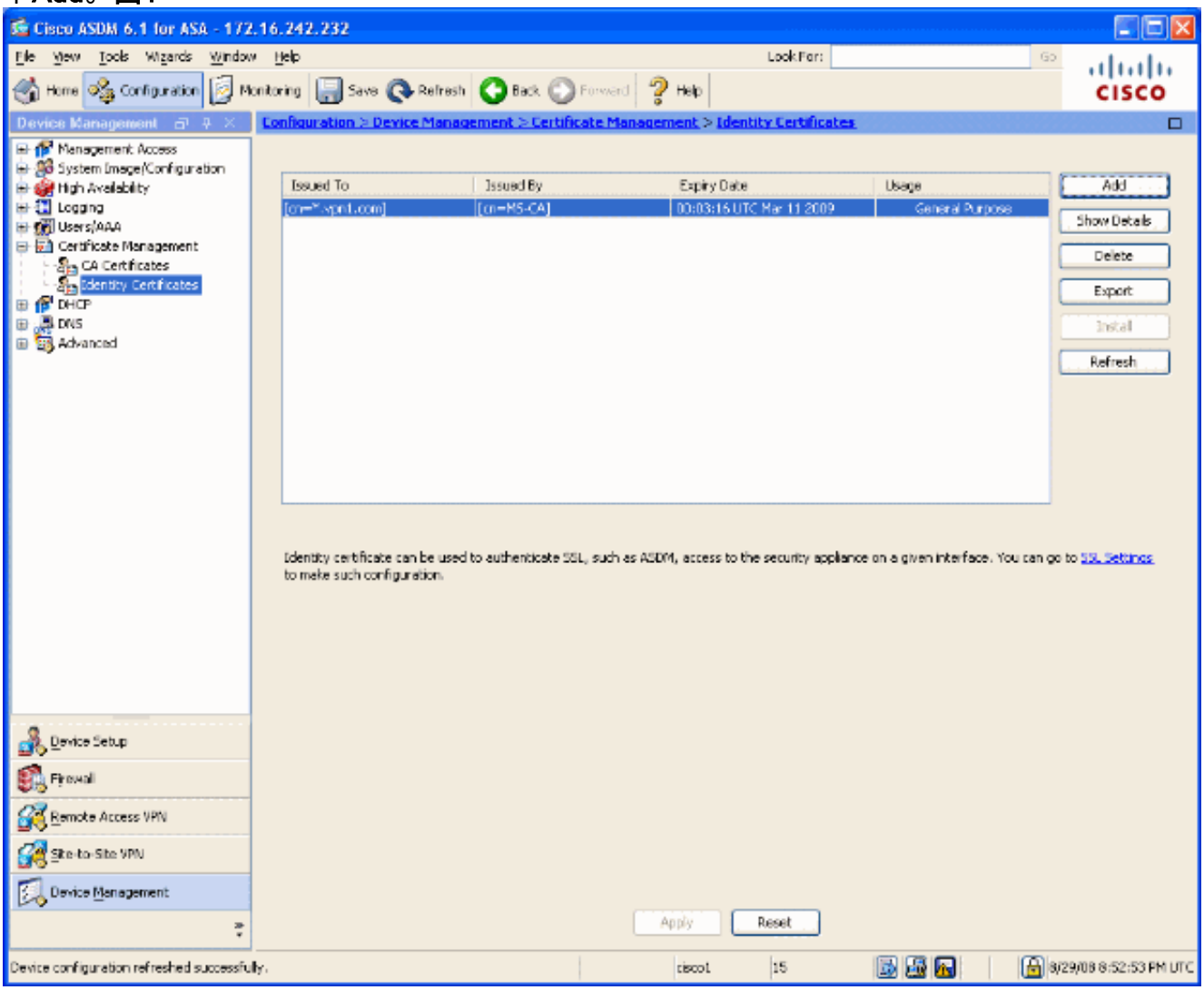
慣例

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。

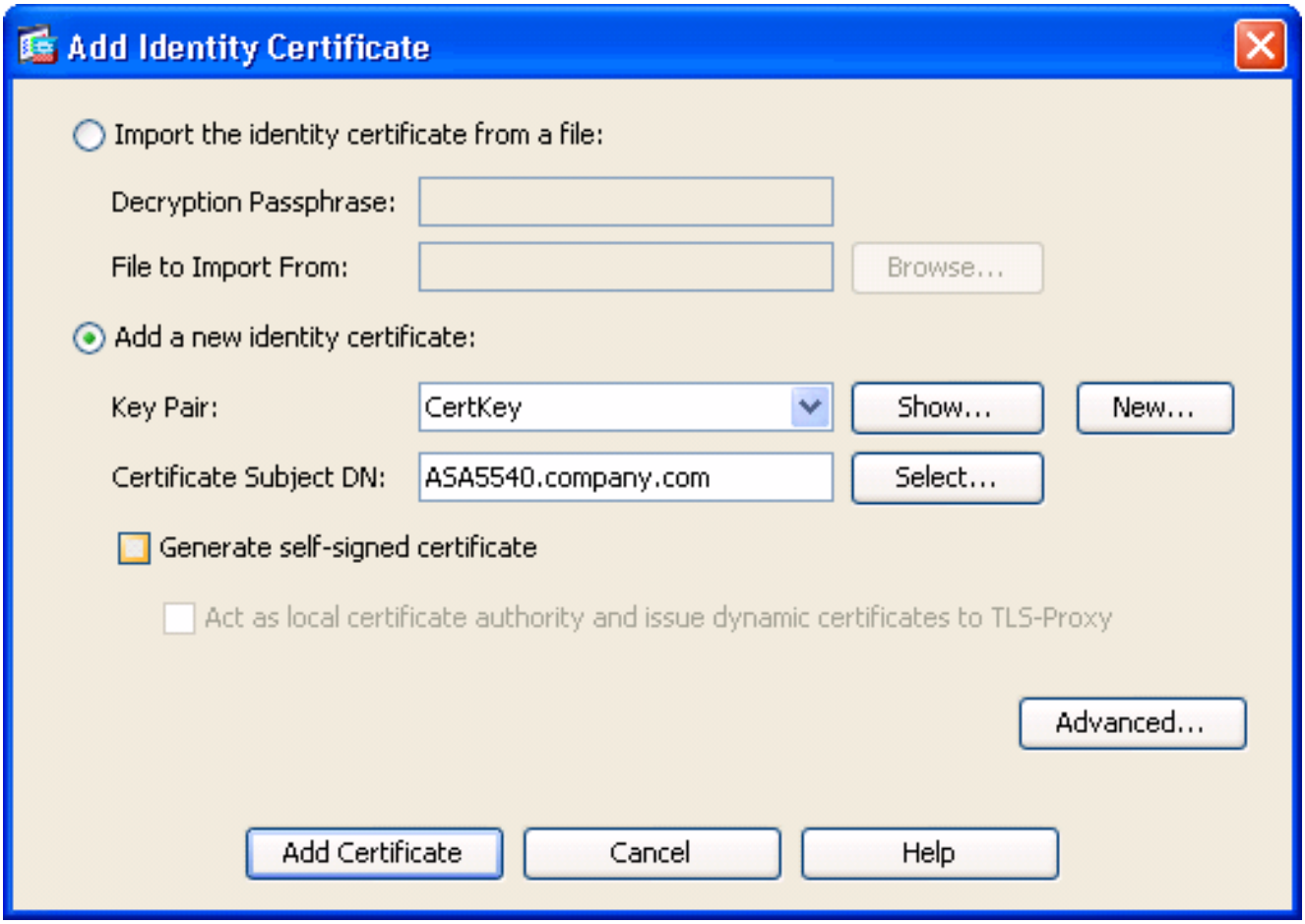
程式

請完成以下步驟：

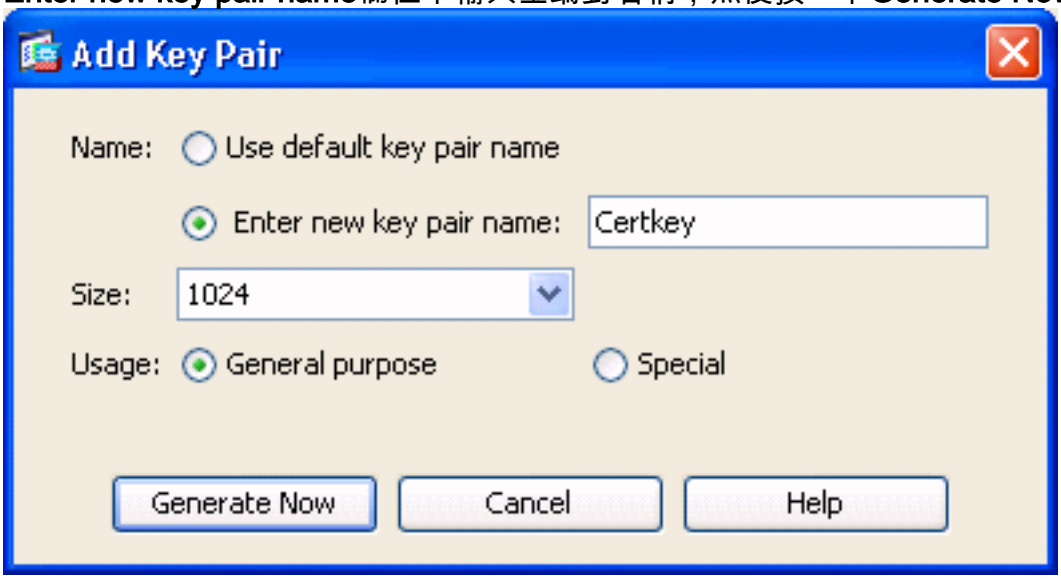
1. 在Configuration > Device Management > Identity Certificates下選擇要續訂的證書，然後按一下**Add**。**圖1**



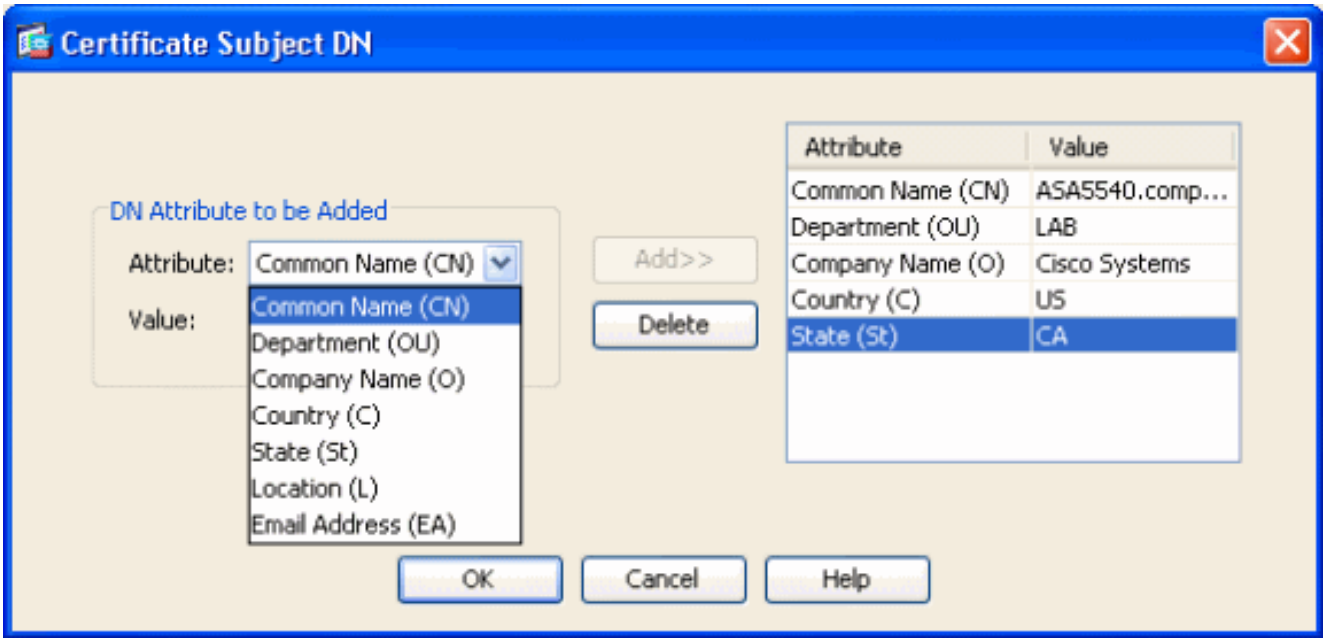
2. 在Add Identity Certificate下，選擇**Add a new identity certificate**單選按鈕，然後從下拉選單中選擇金鑰對。**注意：**不建議使用<Default-RSA-Key>，因為如果您重新生成SSH金鑰，則會使證書無效。如果沒有RSA金鑰，請完成步驟a和b。否則，請繼續執行步驟3。**圖2**



（可選）如果尚未配置RSA金鑰，請完成這些步驟，否則跳到步驟3。按一下**新建.....**在**Enter new key pair name**欄位中輸入金鑰對名稱，然後按一下**Generate Now**。**圖3**



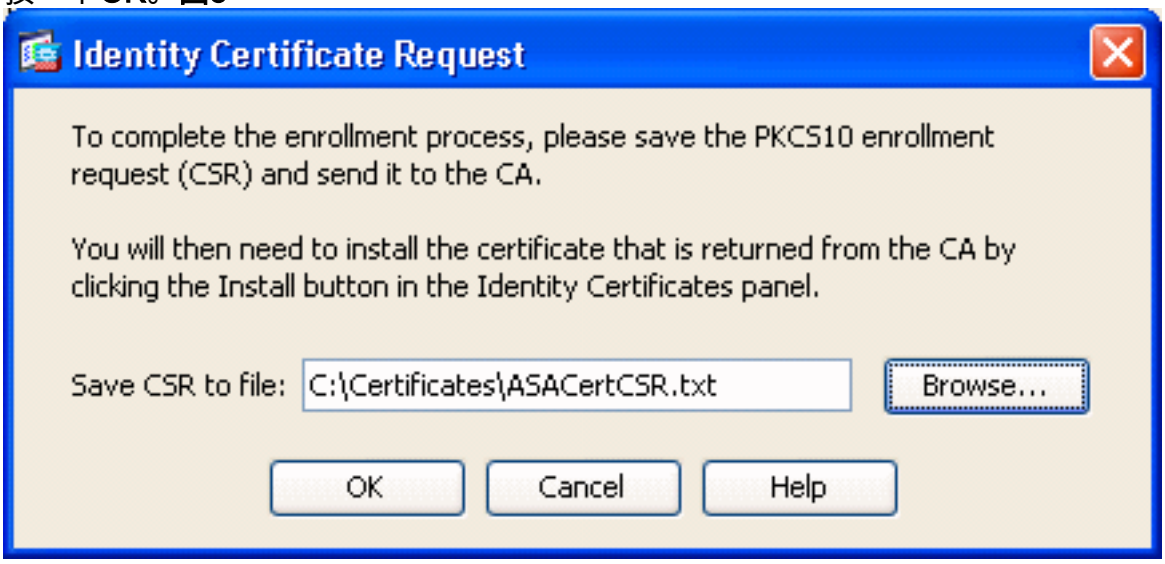
3. 按一下「**Select**」。
4. 輸入適當的證書屬性，如圖4所示。完成後，按一下**OK**。然後按一下「**Add Certificate**」。**圖4**



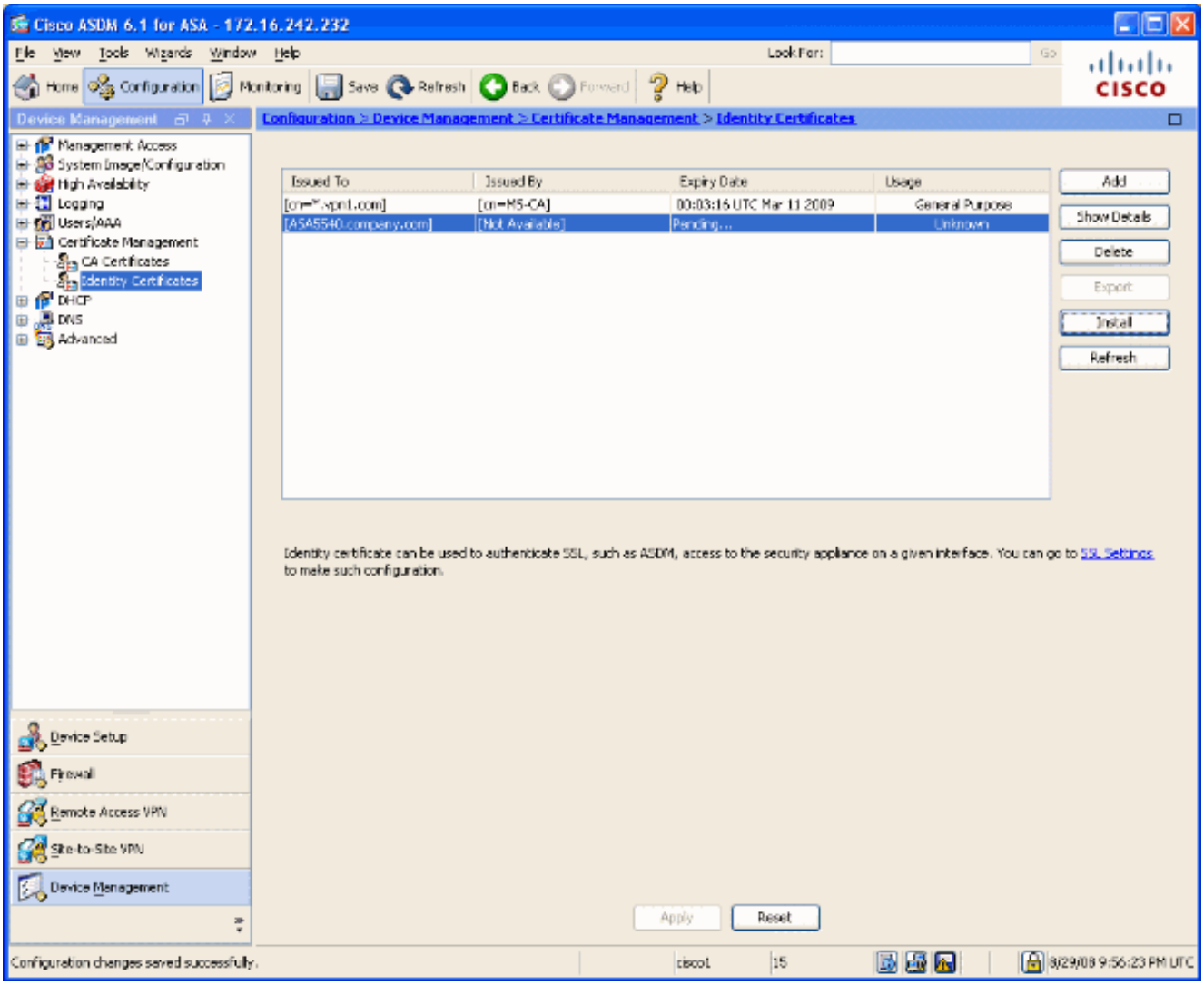
CLI輸出：

```
crypto ca trustpoint ASDM_TrustPoint0
        keypair CertKey
        id-usage ssl-ipsec
        fqdn 5540-uwe
        subject-name CN=ASA5540.company.com,OU=LAB,O=Cisco ystems,C=US,St=CA
        enrollment terminal
 crypto ca enroll ASDM_TrustPoint0
```

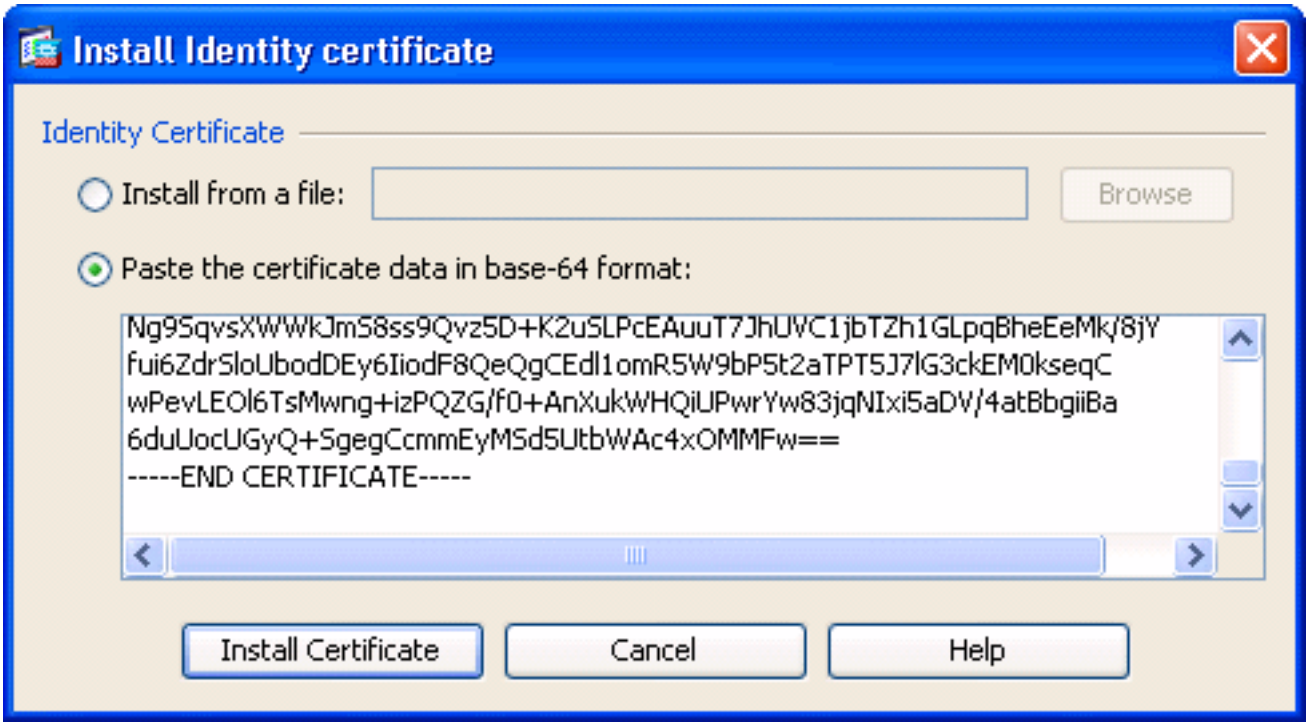
5. 在「**Identity Certificate Request**」彈出視窗中，將證書簽名請求(CSR)儲存到文本檔案，然後按一下**OK**。**圖5**



6. （可選）在ASDM中驗證CSR是否處於掛起狀態，如圖6所示。**圖6**



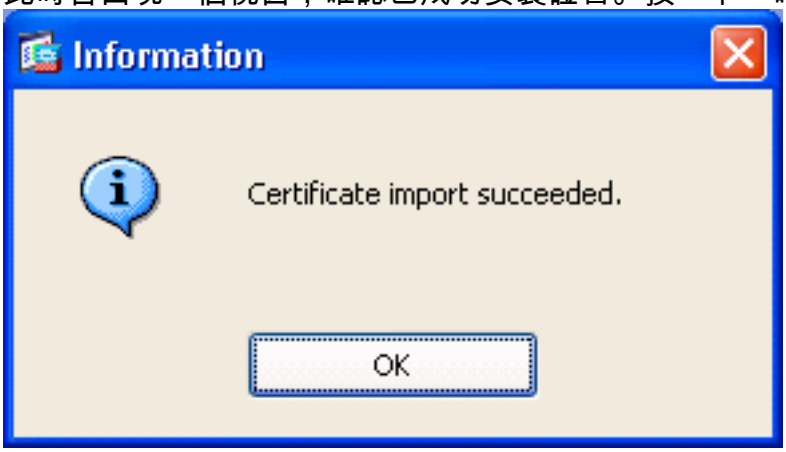
7. 向證書管理員提交證書請求，證書管理員在伺服器上頒發證書。這可以通過Web介面和電子郵件進行，也可以直接到根CA伺服器進行證書頒發過程。
8. 完成以下步驟即可安裝續訂的憑證。在Configuration > Device Management > Identity Certificates下選擇掛起的證書請求，如圖6所示，然後按一下**Install**。在「安裝身份證書」視窗中，選擇**Paste the certificate data in base-64 format**單選按鈕，然後按一下**Install Certificate**。**注意**：或者，如果證書是在.cer檔案中頒發，而不是在基於文本的檔案或電子郵件中頒發，則您也可以選擇**Install from a file**，瀏覽到PC上的相應檔案，按一下**Install ID certificate file**，然後按一下**Install Certificate**。**圖7**



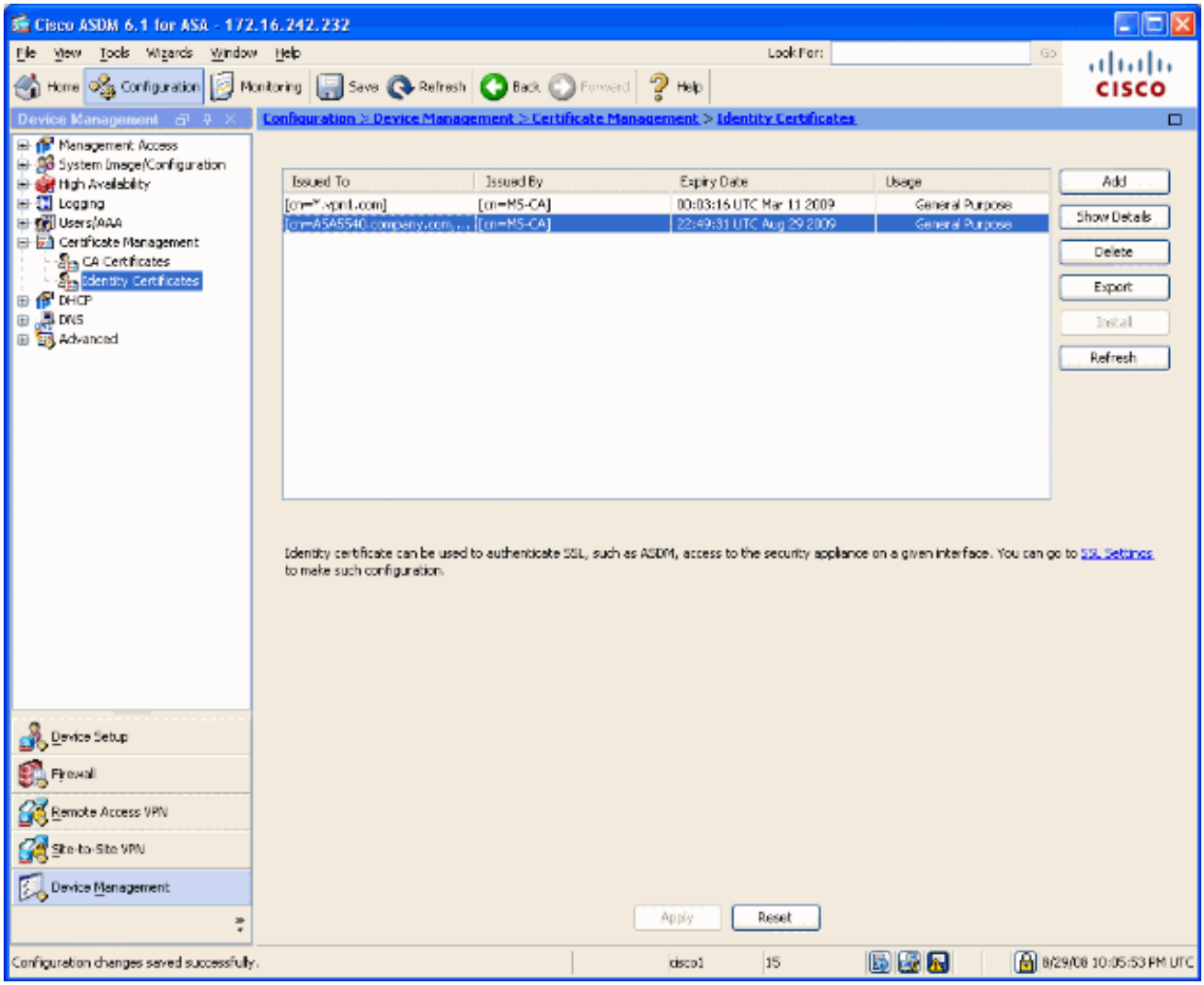
CLI輸出：

```
crypto ca import ASDM_TrustPoint0 certificate
WIID2DCCAsCgAwIBAgIKYb9wewAAAAAAJzANBgkqhkiG9w0BAQUFADAQMQ
!--- output truncated wPevLEOl6TsMwng+izPQZG/f0+AnXukWHQiUPwrYw83jqNIxi5aDV/4atBbgiiBa
6duUocUGyQ+SgegCcmmEyMSd5UtbWAc4xOMMFw== quit
```

9. 此時會出現一個視窗，確認已成功安裝證書。按一下「確定」確認。**圖8**

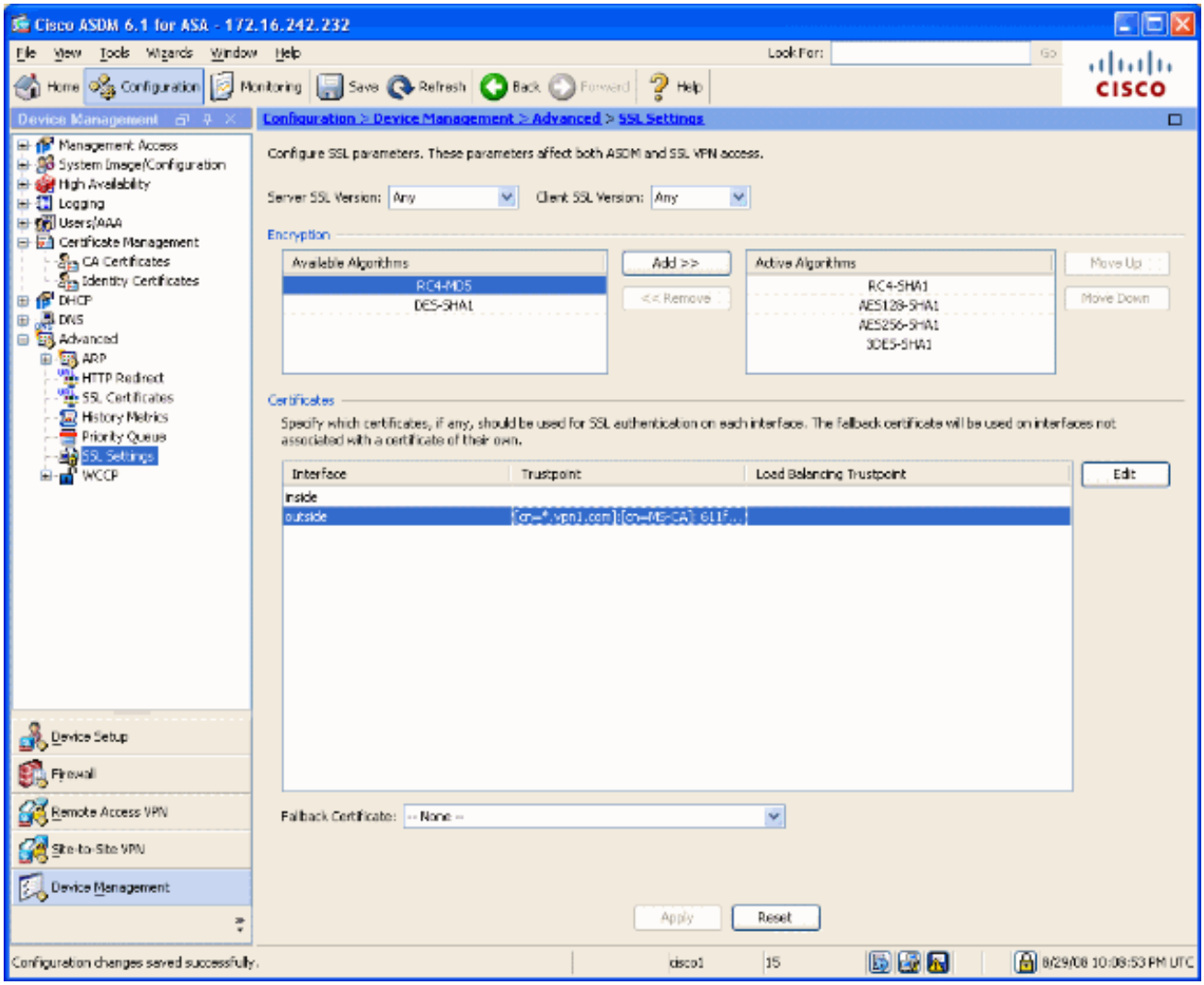


10. 確保新證書出現在「身份證書」下。**圖9**



11. 完成以下步驟，即可將新憑證繫結到介面：選擇**Configuration > Device Management > Advanced > SSL Settings**，如圖10所示。在Certificates下選擇您的介面，然後按一下**Edit**。

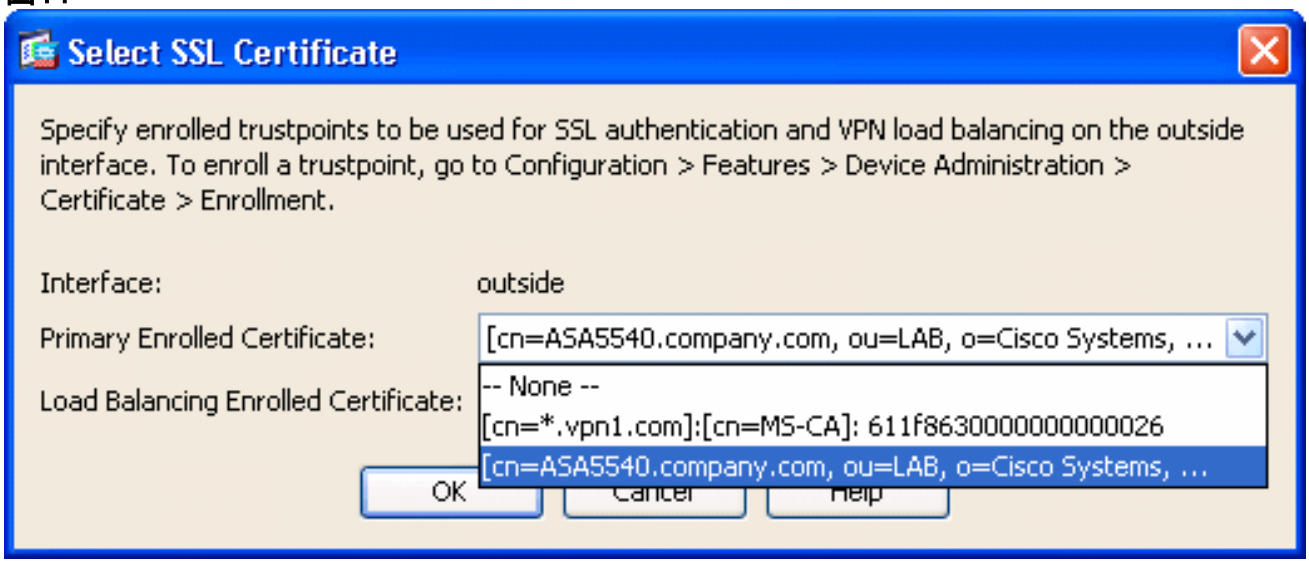
圖10



12. 從下拉選單中選擇新證書，按一下**OK**，然後按一下**Apply**。

```
ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1
ssl trust-point ASDM_TrustPoint0 outside
```

圖11



13. 在ASDM或CLI中儲存配置。

驗證

您可以使用CLI介面驗證新證書是否正確安裝到ASA，如以下輸出示例所示：

```
ASA(config)#show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 61bf707b000000000027
  Certificate Usage: General Purpose
  Public Key Type: RSA (1024 bits)
  Issuer Name:
    cn=MS-CA
  Subject Name:
    cn=ASA5540.company.com !---new certificate ou=LAB o=Cisco Systems st=CA c=US CRL
Distribution Points: [1] http://win2k3-base1/CertEnroll/MS-CA.crl [2] file://\\win2k3-
base1\CertEnroll\MS-CA.crl Validity Date: start date: 22:39:31 UTC Aug 29 2008 end date:
22:49:31 UTC Aug 29 2009 Associated Trustpoints: ASDM_TrustPoint0 CA Certificate Status:
Available Certificate Serial Number: 211020a79cfd96b34ba93f3145d8e571 Certificate Usage:
Signature Public Key Type: RSA (2048 bits) Issuer Name: cn=MS-CA Subject Name: cn=MS-CA !---
'old' certificate CRL Distribution Points: [1] http://win2k3-base1/CertEnroll/MS-CA.crl [2]
file://\\win2k3-base1\CertEnroll\MS-CA.crl Validity Date: start date: 00:26:08 UTC Jun 8 2006
end date: 00:34:01 UTC Jun 8 2011 Associated Trustpoints: test Certificate Status: Available
Certificate Serial Number: 611f8630000000000026 Certificate Usage: General Purpose Public Key
Type: RSA (1024 bits) Issuer Name: cn=MS-CA Subject Name: cn=*.vpn1.com CRL Distribution Points:
[1] http://win2k3-base1/CertEnroll/MS-CA.crl [2] file://\\win2k3-base1\CertEnroll\MS-CA.crl
Validity Date: start date: 23:53:16 UTC Mar 10 2008 end date: 00:03:16 UTC Mar 11 2009
Associated Trustpoints: test ASA(config)#
```

疑難排解

（可選）在CLI上驗證是否已向介面應用正確的證書：

```
ASA(config)#show running-config ssl
ssl trust-point ASDM_TrustPoint0 outside
!--- Shows that the correct trustpoint is tied to the outside interface that terminates SSL VPN.
ASA(config)#
```

如何將SSL證書從一個ASA複製到另一個ASA

如果已生成可匯出金鑰，則可以執行此操作。您需要將證書匯出到PKCS檔案。這包括匯出所有關聯的金鑰。

使用以下命令通過CLI匯出證書：

```
ASA(config)#crypto ca export
```

注意：口令 — 用於保護pkcs12檔案。

使用以下命令通過CLI匯入證書：

```
SA(config)#crypto ca import
```

注意：此密碼應與匯出檔案時使用的密碼相同。

也可以通過ASDM為ASA故障轉移對執行此操作。請完成以下步驟以執行此操作：

1. 通過ASDM登入到主ASA並選擇**Tools—> Backup Configuration**。
2. 您可以備份所有內容或僅備份證書。
3. 在備用模式下，開啟ASDM並選擇**Tools —> Restore Configuration**。

相關資訊

- Cisco Adaptive Security Appliance(ASA)支援頁面
- ASA 8.x手動安裝第三方供應商證書以用於WebVPN配置示例
- 技術支援與文件 - Cisco Systems