

設定 ASA：安裝和更新 SSL 數位憑證

目錄

[簡介](#)

[背景資訊](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[CSR 產生](#)

[1. 使用 ASDM 設定](#)

[2. 使用ASA CLI配置](#)

[3. 使用 OpenSSL 產生 CSR](#)

[在 CA 產生 SSL 憑證](#)

[在 GoDaddy CA 產生 SSL 憑證的範例](#)

[在 ASA 安裝 SSL 憑證](#)

[1.1 使用ASDM安裝PEM格式的身份證書](#)

[1.2. 使用CLI安裝PEM證書](#)

[2.1 使用ASDM安裝PKCS12證書](#)

[2.2 使用CLI安裝PKCS12證書](#)

[驗證](#)

[透過 ASDM 檢視安裝的憑證](#)

[透過 CLI 檢視安裝的憑證](#)

[使用Web瀏覽器驗證WebVPN的安裝證書](#)

[在 ASA 更新 SSL 憑證](#)

[常見問題](#)

[1. 什麼是從一個 ASA 將身分識別憑證傳輸至不同 ASA 的最佳方式？](#)

[2. 如何產生 SSL 憑證以搭配 VPN 負載平衡 ASA 使用？](#)

[3. 在 ASA 容錯移轉配對中，憑證是否需要從主要 ASA 複製到次要 ASA？](#)

[4. 如果使用 ECDSA 金鑰，SSL 憑證產生程序是否會不同？](#)

[疑難排解](#)

[指令疑難排解](#)

[常見問題](#)

[附錄](#)

[附錄A: ECDSA或RSA](#)

[附錄B：使用OpenSSL根據身份證書、CA證書和私鑰生成PKCS12證書](#)

[相關資訊](#)

簡介

本文件說明如何在 ASA 上安裝可信任的第三方 SSL 數位憑證，用於無用戶端的 SSLVPN 和 AnyConnect 連線。

背景資訊

此範例使用 GoDaddy 憑證。每個步驟皆包含 Adaptive Security Device Manager (ASDM) 程序和 CLI 對等項目。

必要條件

需求

本文件需要存取受信任的第三方 Certificate Authority (CA) 進行憑證註冊。第三方 CA 廠商的範例包括 (但不限於) Baltimore、思科、Entrust、Geotrust、G、Microsoft、RSA、Thawte 及 VeriSign。

在您開始執行前，請確認 ASA 具有正確的時鐘時間、日期及時區。進行憑證驗證時，建議使用網路時間通訊協定 (NTP) 伺服器同步化 ASA 的時間。[Cisco ASA 系列一般操作 CLI 組態設定指南 9.1 版](#)會詳細說明在 ASA 正確設定時間和日期應採取的步驟。

採用元件

本文件使用執行軟體 9.4.1 版和 ASDM 7.4(1) 版的 ASA 5500-X。

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

SSL 通訊協定會要求 SSL 伺服器向用戶端提供伺服器憑證，以使用戶端執行伺服器驗證。思科建議不要使用自我簽署憑證，因為使用者可能會不當設定瀏覽器信任惡意伺服器的憑證。如此亦可能造成使用者不便，必須在連線至安全閘道時回應安全性警告。建議使用受信任的第三方 CA，以便向 ASA 核發 SSL 憑證做為此用途。

ASA 的第三方憑證生命週期基本上會透過以下步驟進行：



CSR 產生

產生CSR是任何X.509數位憑證生命週期的第一步。

私密/公開 Rivest-Shamir-Adleman (RSA) 或橢圓曲線數位簽章演算法 (ECDSA) 金鑰組產生後 ([附錄 A](#) 會詳細說明使用 RSA 或 ECDSA 之間的差異) ，憑證簽署要求 (CSR) 隨即建立。

CSR是包含傳送請求的主機的公鑰和身份資訊的PKCS10格式化訊息。 [PKI資料格式](#) 說明適用於ASA和Cisco IOS的不同證書格式[®]。

附註：

1. 向 CA 確認需要的金鑰組大小。CA/Browser Forum 已要求成員 CA 產生的所有憑證大小必須在 2048 位元以上。
2. ASA 目前不支援 4096 位元金鑰 (思科錯誤 ID [CSCut53512](#)) 進行 SSL 伺服器驗證。但是，IKEv2 會支援在單獨 ASA 5580、5585 及 5500-X 平台上使用 4096 位元伺服器憑證。
3. 使用 CSR 之 FQDN 欄位的 ASA 的 DNS 名稱，以防止不受信任的憑證警告，並傳遞嚴格憑證檢查。

產生CSR的方法有三種。

- 使用ASDM配置
- 使用ASA CLI配置

- 使用OpenSSL產生CSR

1. 使用 ASDM 設定

1. 導航到Configuration > Remote Access VPN > Certificate Management並選擇Identity Certificates。
2. 按一下Add。

Add Identity Certificate

Trustpoint Name:

Import the identity certificate from a file (PKCS12 format with Certificate(s) +Private Key):

Decryption Passphrase:

File to Import From:

Add a new identity certificate:

Key Pair:

Certificate Subject DN:

Generate self-signed certificate

Act as local certificate authority and issue dynamic certificates to TLS-Proxy

Enable CA flag in basic constraints extension

3. 在Trustpoint Name輸入欄位中定義信任點名稱。
4. 按一下「Add a new identity certificateRadio (刪除)」按鈕。
5. 對於金鑰對，按一下New。

Add Key Pair

Key Type: RSA ECDSA

Name: Use default key pair name
 Enter new key pair name:

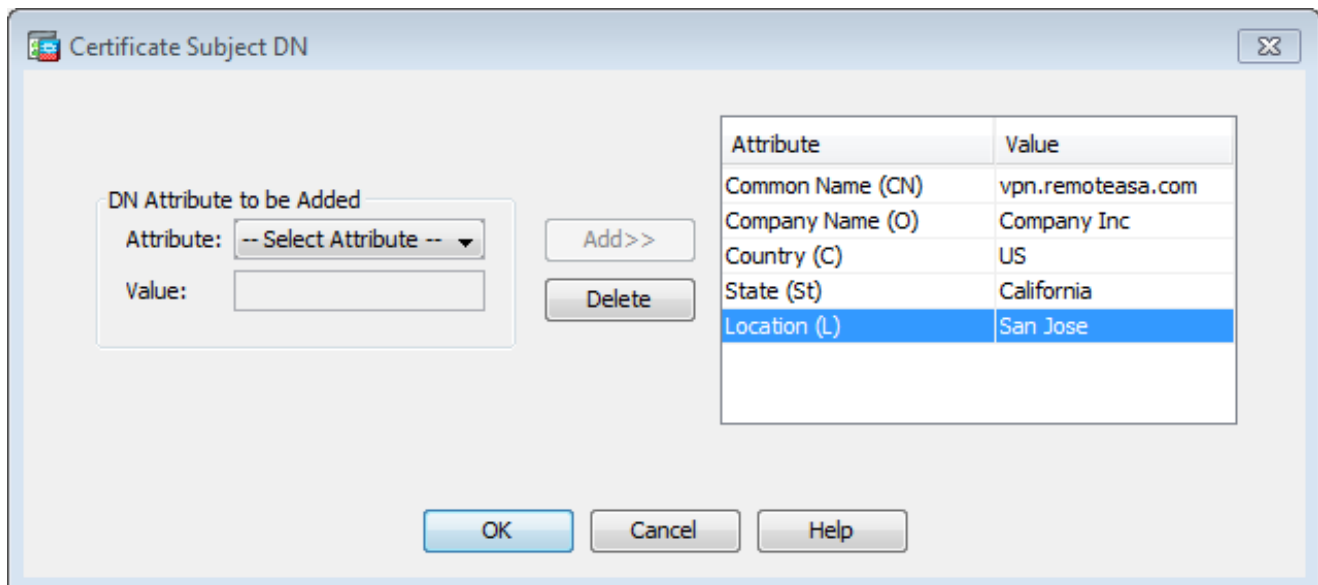
Size: ▼


Usage: General purpose Special

6. 選擇金鑰型別 — RSA或ECDSA。(請參閱[附錄A](#)以瞭解區別。)
7. 按一下「Enter new key pair nameRadio (刪除)」按鈕。為識別目的標識金鑰對名稱。
8. 選擇Key Size。選擇General Purpose for Usage RSA。
9. 按一下Generate Now。金鑰對已建立。
10. 要定義證書主題DN，請按一下Select，然後配置下表中列出的屬性：

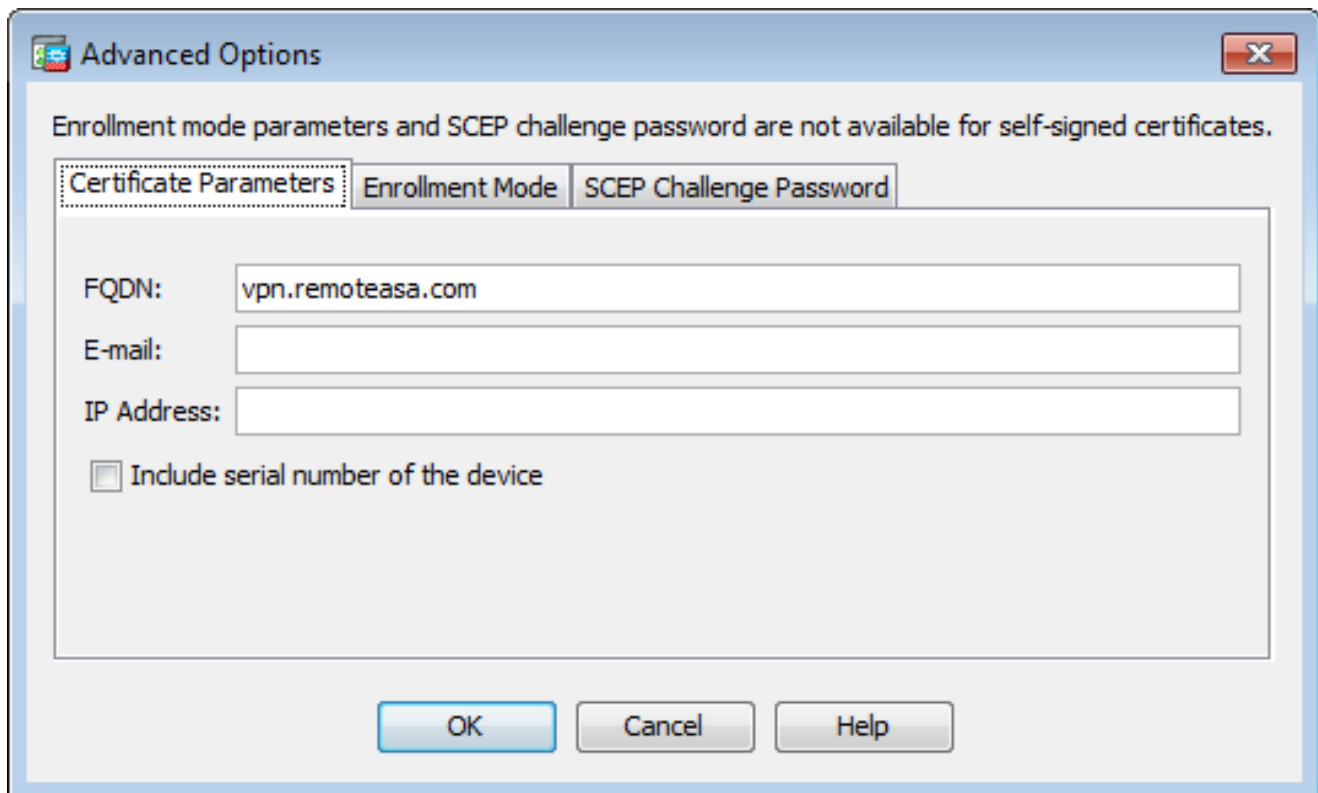
Attribute	Description
CN	FQDN (Full Qualified Domain Name) that will be used for connections to your firewall. For example, webvpn.cisco.com
OU	Department Name
O	Company Name (Avoid using Special Characters)
C	Country Code (2 Letter Code without Punctuation)
St	State (Must be spelled out completely. For example, North Carolina)
L	City
EA	Email Address

要配置這些值，請從Attribute下拉選單中選擇一個值，輸入值，然後按一下Add。



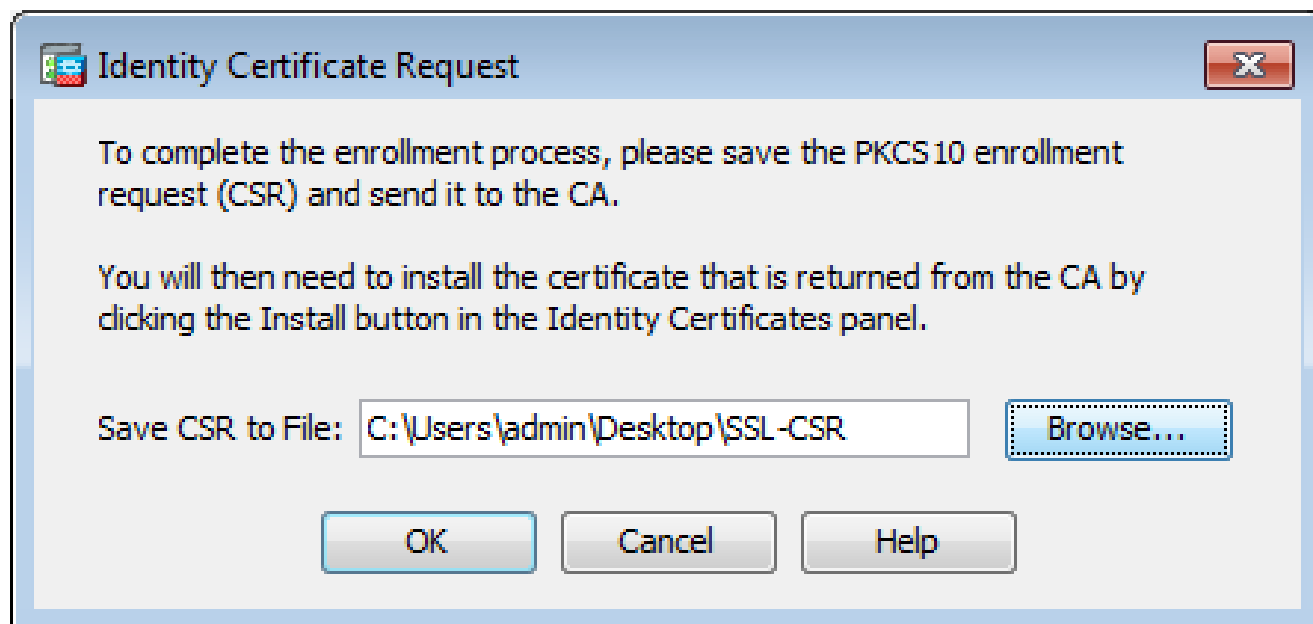
 注意：某些第三方供應商要求在頒發身份證書之前包含特定屬性。如果不確定需要的屬性，請向廠商確認詳細資料。

11. 新增適當的值後，按一下OK。系統將顯示Add Identity Certificate對話方塊，其中包含證書 Subject DN field populated.
12. 按一下「Advanced」。



13. 在FQDN欄位中，輸入用於從Internet訪問裝置的FQDN。按一下OK。
14. 在核取的基本限制延伸選項中保留啟用 CA 旗標。未具有 CA 旗標的憑證目前依預設無法安裝於 ASA 做為 CA 憑證。基本限制延伸會識別憑證的主體是否為 CA，以及包含此憑證之有效憑證路徑的最大深度。取消選中該選項以繞過此要求。
15. 按一下OK，然後按一下Add Certificate。「A prompt (顯示提示)」以將CSR儲存到本地電腦上的

檔案中。



16. 按一下Browse，選擇要儲存CSR的位置，並以.txt延伸名稱儲存檔案。

 注意：當檔案以.txt副檔名儲存時，可以使用文本編輯器（如記事本）開啟和檢視PKCS#10請求。

2. 使用 ASA CLI 設定

在 ASDM 中，當系統產生 CSR 或安裝 CA 憑證後，信任點會自動建立。在CLI中，必須手動建立信任點。

```
<#root>
```

```
! Generates 2048 bit RSA key pair with label SSL-Keypair.
```

```
MainASA(config)#
```

```
crypto key generate rsa label SSL-Keypair modulus 2048
```

```
INFO: The name for the keys are: SSL-Keypair  
Keypair generation process begin. Please wait...
```

```
! Define trustpoint with attributes to be used on the SSL certificate
```

```
MainASA(config)#
```

```
crypto ca trustpoint SSL-Trustpoint
```

```
MainASA(config-ca-trustpoint)#
```

```
enrollment terminal
```

```
MainASA(config-ca-trustpoint)#
```

```
fqdn (remoteasavpn.url)
```

MainASA(config-ca-trustpoint)#

```
subject-name CN=(asa.remotevpn.url),O=Company Inc,C=US,  
St=California,L=San Jose
```

MainASA(config-ca-trustpoint)#

```
keypair SSL-Keypair
```

MainASA(config-ca-trustpoint)#

```
exit
```

! Initiates certificate signing request. This is the request to be submitted via Web or Email to the third party vendor.

MainASA(config)#

```
crypto ca enroll SSL-Trustpoint
```

WARNING: The certificate enrollment is configured with an fqdn that differs from the system fqdn. If this certificate is used for VPN authentication this may cause connection problems.

Would you like to continue with this enrollment? [yes/no]:

```
yes
```

```
% Start certificate enrollment ..
```

```
% The subject name in the certificate is: subject-name CN=
```

```
(remoteasavpn.url)
```

```
,  
O=Company Inc,C=US,St=California,L=San Jose
```

```
% The fully-qualified domain name in the certificate will be:
```

```
(remoteasavpn.url)
```

```
,  
% Include the device serial number in the subject name? [yes/no]:
```

```
no
```

Display Certificate Request to terminal? [yes/no]:

```
yes
```

Certificate Request:

```
-----BEGIN CERTIFICATE REQUEST-----
```

```
MIIDDjCCAfyCAQAwwYkxETAPBgNVBACTCFNhbiBkb3NlMRMwEQYDVQIQIEwpDYWxp  
Zm9ybmlhMQswCQYDVQQGEwJVUzEUMBIGA1UEChMLQ29tcGFueSBJamMxGjAYBgNV  
BAMTEXZwbi5yZW1vdGVhc2EuY29tMSAwHgYJKoZIhvcNAQkCFhF2cG4ucmVtb3Rl  
YXNhLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK62Nhb9kt1K  
uR3Q4TmksyuRMqJNrb9kXpvA6H200PuBfQvSF4rVnSwK0mu3c8nweEvYcdVwV6Bz  
BhjXeovTVi17F1NTceaUTGikeIdXC+mw1iE7eRsynS/d4mzMWJmrvrsDNzpAw/EM  
SzTca+BvqF7X2r3LU8Vsv60i8y1hco9Fz7bWvRWVt03NDDbyo1C9b/VgXMuBitcc  
rzfUubVnm7VZD0f4jr9EXgUwXxcQidWEAB1FrXrtYpFgBo9aqJmRp2YABQ1ieP4cY  
3rBtgRjLcF+S9TvHG5m4v7v755mev4YqsZIXvytIOzVBihemVxaGA1oDwfkoySFi  
4CzXbFvdG6kCAwEAaA/MD0GCSqGSIb3DQEJJDjEwMC4wDgYDVROPAQH/BAQDAgWg  
MBWGA1UdEQQVMB0CEXZwbi5yZW1vdGVhc2EuY29tMA0GCSqGSIb3DQEBAQUAA4IB  
AQBZuZuXGEB0ix1yuPK0ZkRz8bPnwIqLTfxZhagmuyEhrN7N4+aQnCHj85oJane
```



```
4ztZDiCCoWTerBS4RSkKEHEspu9oohjCYuNnp5qa91SPrZNEjTww0eRn+qKbId2J
jE6Qy4vdPCexavMLYVQxCny+gVgzPN/sFRk3EcTTVq6DxxaebpJijmiqa7gCph52
YkHXnFne1LQd41BgoL1Cr9+hx74XsTHGBmI1s/9T5oAX26Ym+B21/i/DP5BktIUA
8GvIY1/ypj9K049fP5ap8a10qvLtYYcCcfwrCt+0oj0rZ1YyJb3dFuMNRdAX37t
DuHN12EYNpYkjVk1wI53/5w3
-----END CERTIFICATE REQUEST-----
```


Redisplay enrollment request? [yes/no]:

no

! Displays the PKCS#10 enrollment request to the terminal. Copy this from the terminal to a text file to submit to the third party CA.

3. 使用 OpenSSL 產生 CSR

OpenSSL會使用OpenSSL config檔案來擷取CSR產生中使用的屬性。此程序會導致 CSR 和私密金鑰產生。

 注意：驗證所生成的私鑰是否未與其他人共用，因為它會破壞證書的完整性。

1. 務必將 OpenSSL 安裝於執行此程序的系統。對於Mac OSX和GNU/Linux使用者，預設情況下會安裝此程式。
2. 切換到功能目錄。

在Windows上：預設情況下，實用程式安裝在C:\Openssl\bin中。在此位置開啟命令提示字元。

在Mac OSX/Linux上：在建立CSR所需的目錄中開啟「終端」視窗。

3. 使用具有給定屬性的文本編輯器建立OpenSSL配置檔案。完成後，在上一步中提到的位置將檔案另存為 openssl.cnf(如果版本為0.9.8h及更高版本，則檔案為openssl.cfg)

```
<#root>
```

```
[req]
```

```
default_bits = 2048
default_keyfile = privatekey.key
distinguished_name = req_distinguished_name
req_extensions = req_ext
```

```
[req_distinguished_name]
```

```
commonName = Common Name (eg, YOUR name)
commonName_default = (asa.remotevpn.url)
```

```
countryName = Country Name (2 letter code)
countryName_default = US
```

```
stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = California
```

```
localityName = Locality Name (eg, city)
```

```
localityName_default = San Jose

0.organizationName = Organization Name (eg, company)
0.organizationName_default = Company Inc
```

```
[req_ext]

subjectAltName = @alt_names
```

```
[alt_names]

DNS.1 = *.remotearsa.com
```

4. 使用此指令產生 CSR 和私密金鑰：

```
openssl req -new -nodes -out CSR.csr -config openssl.cnf
```

```
<#root>
```

```
# Sample CSR Generation:
```

```
openssl req -new -nodes -out CSR.csr -config openssl.cnf
```

```
Generate a 2048 bit RSA private key
```

```
.....+++
```

```
.....+++
```

```
writing new private key to 'privatekey.key'
```

```
-----
```

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
```

```
What you are about to enter is what is called a Distinguished Name or a DN.
```

```
There are quite a few fields but you can leave some blank
```

```
For some fields there will be a default value,
```

```
If you enter '.', the field will be left blank.
```

```
-----
```

```
Common Name (eg, YOUR name) [(asa.remotevpn.url)]:
```

```
Country Name (2 letter code) [US]:
```

```
State or Province Name (full name) [California]:
```

```
Locality Name (eg, city) [San Jose]:
```

```
Organization Name (eg, company) [Company Inc]:
```

將儲存的 CSR 提交至第三方 CA 廠商。憑證核發後，CA 會提供身分識別憑證和 CA 憑證安裝於 ASA。

在 CA 產生 SSL 憑證

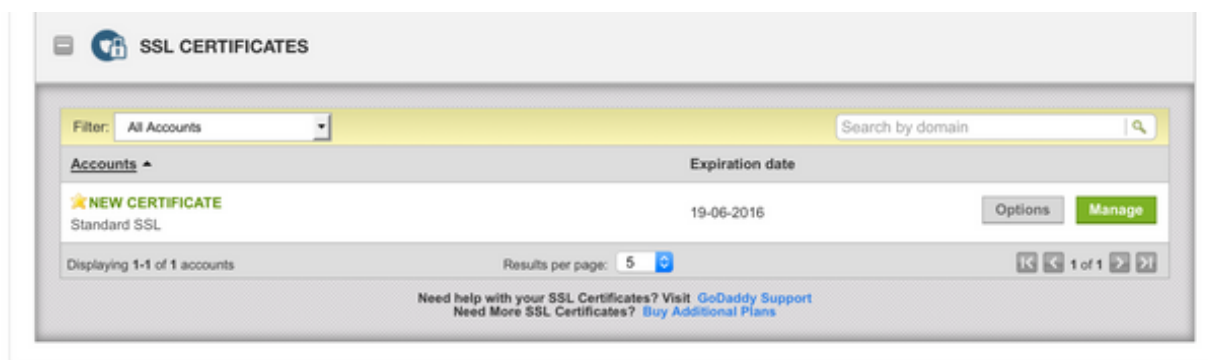
下一步是從 CA 取得簽署的 CSR。CA 會提供新產生之經 PEM 編碼的身分識別憑證，或 PKCS12 憑證及 CA 憑證套件。

如果CSR是在ASA外部（通過OpenSSL或在CA本身）產生的，則具有私鑰和CA證書的PEM編碼身份證書可作為單獨的檔案使用。[附錄B](#)提供了將這些元素捆綁到單個PKCS12檔案（.p12或.pfx格式）中的步驟。

在本文件中，我們使用 GoDaddy CA 做為範例，將身分識別憑證核發至 ASA。此程式與其他CA廠商不同。在繼續之前，請仔細閱讀CA檔案。

在 GoDaddy CA 產生 SSL 憑證的範例

經 SSL 憑證購買與初始設定階段後，請導覽至 GoDaddy 帳戶並檢視 SSL 憑證。其中必定會有新的憑證。按一下Manage「繼續」。



接著會顯示提供 CSR 的頁面（如圖所示）。

根據輸入的 CSR，CA 會判斷要核發憑證的網域名稱。

確認此網域名稱符合 ASA 的 FQDN。

Choose website

Select a domain hosted with us

Provide a certificate signing request (CSR)

Certificate Signing Request (CSR) [Learn more](#)

```
/ypj9KO49fP5ap8al0qvLtYYcCcfwrCt+OojOrZ1YyJb3dFuMNRRedAX37t
DuHNI2EYNpYkjVk1wI53/5w3
-----END CERTIFICATE REQUEST-----
```

Domain Name (based on CSR):

vpn.remoteasa.com

Domain ownership

We'll send an email with a unique code to your address on file. Follow its instructions to verify you have website or DNS control over the selected domain. [More info](#)

AND

We can send domain ownership instructional emails to one or both of the following:


- Contacts listed in the domain's public WHOIS database record
- Email addresses: admin@[domain], administrator@[domain], hostmaster@[domain], postmaster@[domain], and webmaster@[domain]

[Hide advanced options](#)

Signature Algorithm [Learn more](#)

GoDaddy SHA-2

I agree to the terms and conditions of the [Subscriber Agreement](#).

 注意:GoDaddy和大多數其他CA使用SHA-2或SHA256作為預設證書簽名演算法。ASA支援SHA-2簽名演算法，該演算法從8.2(5)[8.3前版本]和8.4(1)[8.3後版本]開始(思科漏洞ID [CSCti30937](#))。如果使用8.2(5)或8.4(1)以前的版本，請選擇SHA-1簽章演算法。

提交要求後，GoDaddy 會先驗證要求，再核發憑證。

驗證憑證要求後，GoDaddy 會將憑證核發至帳戶。

接著您可在 ASA 下載憑證進行安裝。按一下頁面上的Download，以便繼續操作。

The screenshot shows the GoDaddy SSL Certificate Management interface. At the top, there are navigation links: Certificates, Repository, Help, and Report EV Abuse. The main heading is "All > vpn.remoteasa.com" with "Standard SSL Certificate" below it. Under "Certificate Management Options", there are three buttons: "Download" (with a download icon), "Revoke" (with a revoke icon), and "Manage" (with a gear icon). Below this is a "Certificate Details" table:

Status	Certificate issued
Domain name	vpn.remoteasa.com
Encryption Strength	GoDaddy SHA-2
Validity Period	7/22/2015 - 7/22/2016
Serial Number	25:cd:73:a9:84:07:06:05

On the right side, there is a section titled "Display your SSL Certificate security seal". It includes instructions: "Design your seal, copy the code, and paste it in your site footer." Below this are dropdown menus for "Color" (set to "Light") and "Language" (set to "English"). A "Preview" section shows a green security seal with the text "VERIFIED & SECURED" and "GO DADDY". Below the preview is a "Code" section with a text area containing the following code:

```
<script id="siteSeal"><script
type="text/javascript"
src="https://seal.godaddy.com
/getSeal?sealID=bpFAdxgHkmsyEhewKp4Ztd
/MA...</script>
Ctrl+C to copy
```

選擇Other「Server Type (伺服器型別)」並下載證書zip捆綁包。

The screenshot shows the "Download Certificate" page for vpn.remoteasa.com. The heading is "vpn.remoteasa.com > Download Certificate" with "Standard SSL Certificate" below it. The main text reads: "To secure your site that's hosted elsewhere, download the Zip file that matches your hosting server type. Then, install all of the certificates in the Zip file on your hosting server, including any intermediate certificates that might be needed for older browsers or servers." Below this is a link: "First time installing a certificate? [View Installation Instructions for the selected server.](#)"

The "Server type" dropdown menu is open, showing the following options:

- Select ...
- Select ...
- Apache
- Exchange
- IIS
- Mac OS X
- Tomcat
- Other


The "Other" option is highlighted in blue. To the right of the dropdown menu, there are two buttons: "File" and "Cancel".

.zip 檔案包含身分識別憑證和 GoDaddy CA 憑證鏈結套件做為兩項個別 .crt 檔案。請繼續安裝 SSL 證書，以便在 ASA 上安裝這些證書。

在 ASA 安裝 SSL 憑證

SSL 憑證可以下列兩種方式，透過 ASDM 或 CLI 在 ASA 安裝：

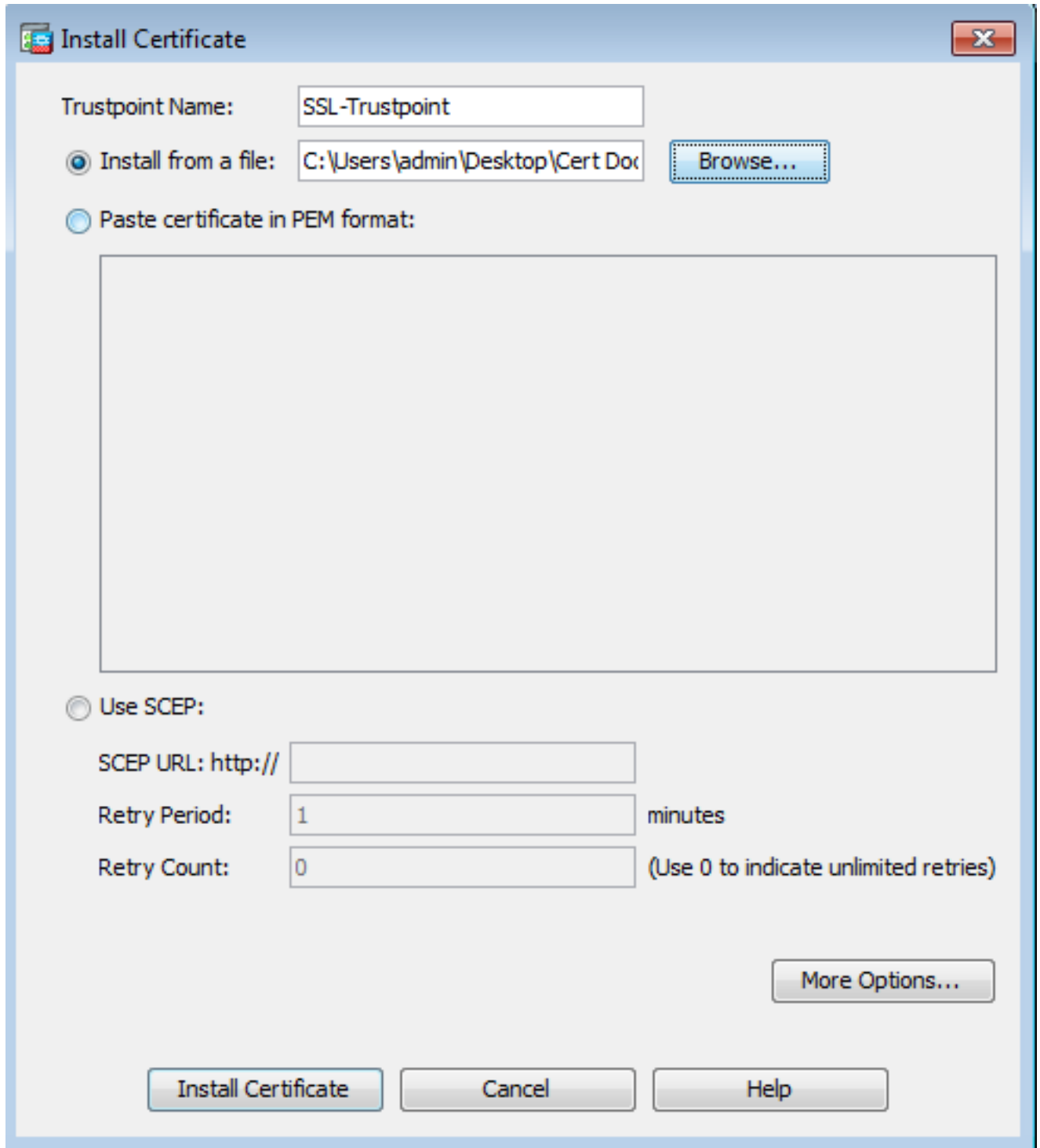
1. 以 PEM 格式分別匯入 CA 和身分識別憑證。
2. 或匯入 PKCS12 檔（經 CLI 的 base64 編碼），其中身分識別憑證、CA 憑證及私密金鑰會合併在 PKCS12 檔案中。

 註：如果 CA 提供 CA 證書鏈，則只需在用於生成 CSR 的信任點上的層次結構中安裝即時中間 CA 證書。根 CA 憑證和任何其他中繼 CA 憑證可安裝於新的信任點。

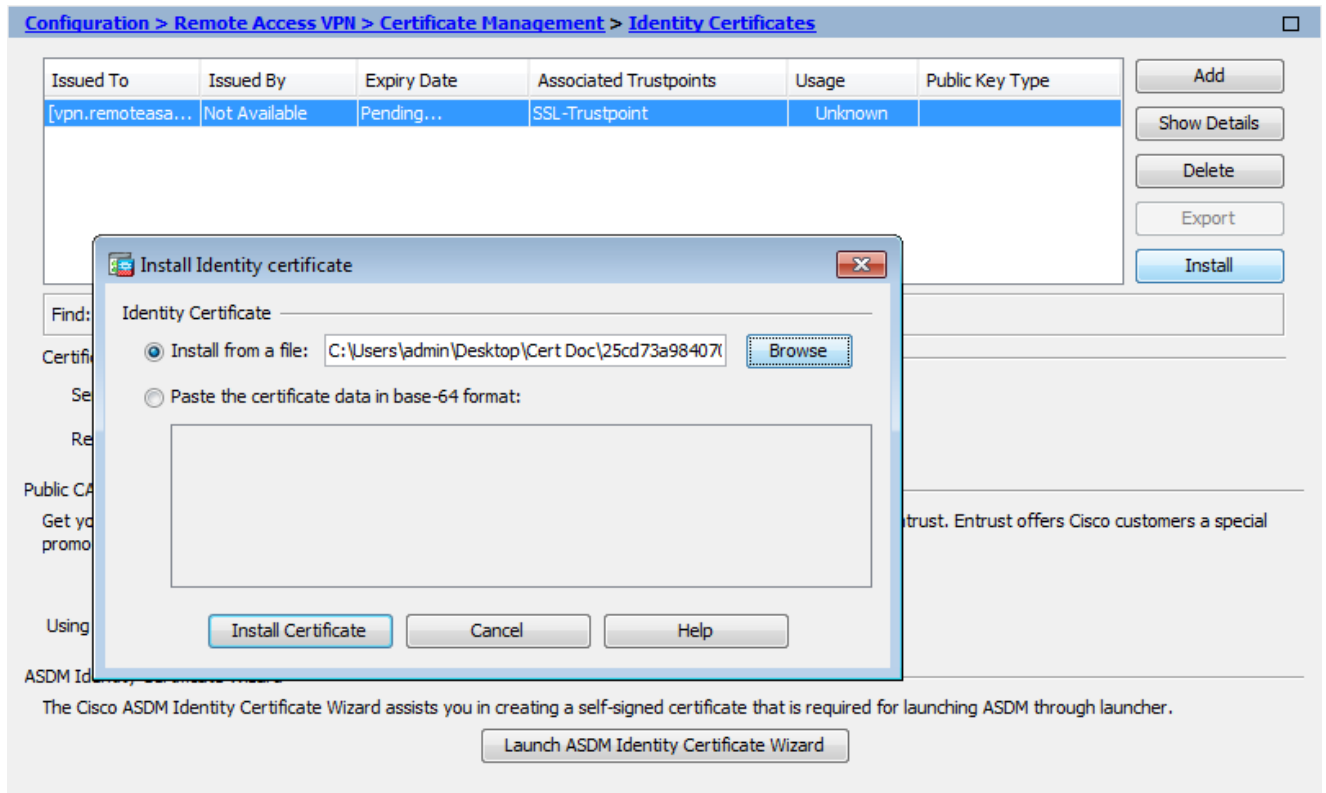
1.1 使用 ASDM 安裝 PEM 格式的身分識別憑證

提供的安裝步驟已假設 CA 會提供經 PEM 編碼（.pem、.cer、.crt）的身分識別憑證和 CA 憑證套件

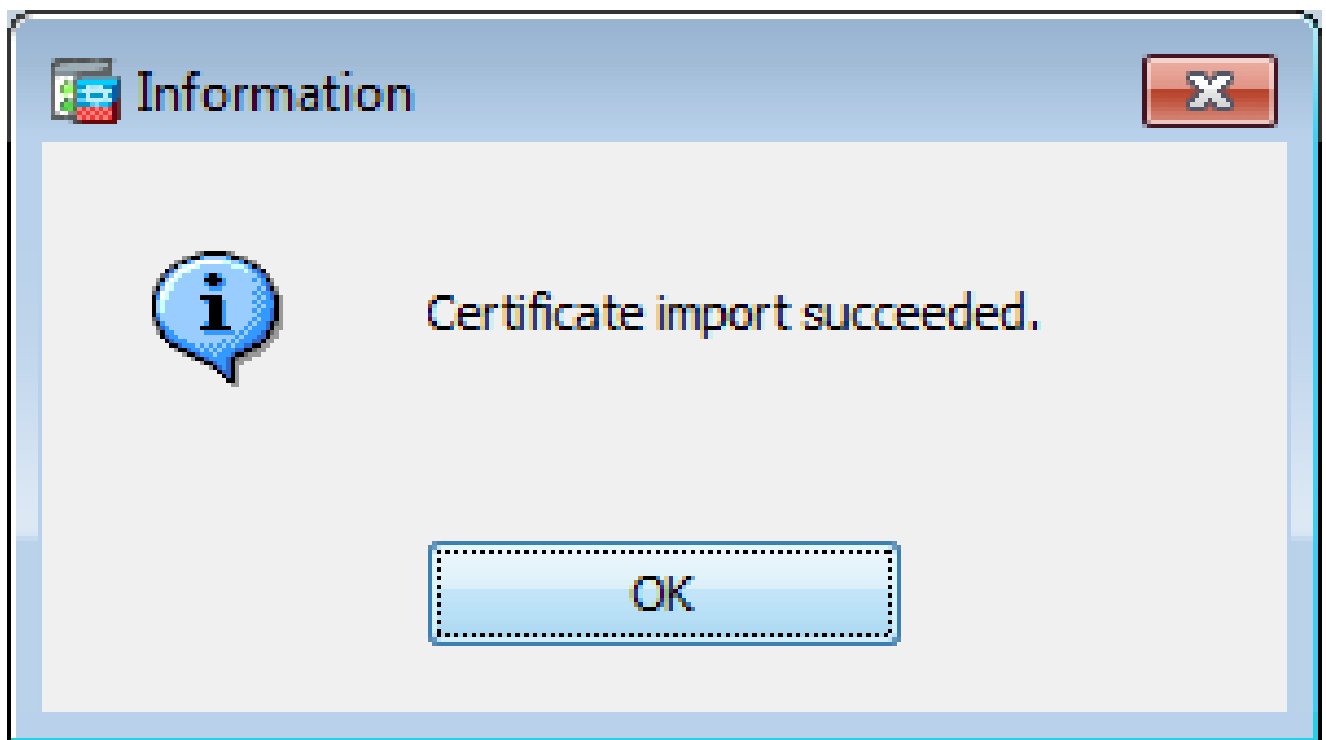
1. 導航到 **Configuration > Remote Access VPN > Certificate Management**，然後選擇 **CA Certificates**。
2. 開啟文字編輯器中經 PEM 編碼的憑證，然後將第三方廠商提供的 base64 CA 憑證複製並貼上文字欄位。



3. 按一下「Install certificate」。
4. 導航至 **Configuration > Remote Access VPN > Certificate Management**，然後選擇身份證書。
5. 選取先前建立的身分識別憑證。按一下 **Install** 下。
6. 按一下選項單選按鈕並選擇 PEM 編碼的身份證書 **Install from a file**，或者在文本編輯器中開啟 PEM 編碼的證書，然後複製第三方供應商提供的 base64 身份證書並將其貼上到文本欄位中。



7. 按一下Add Certificate。

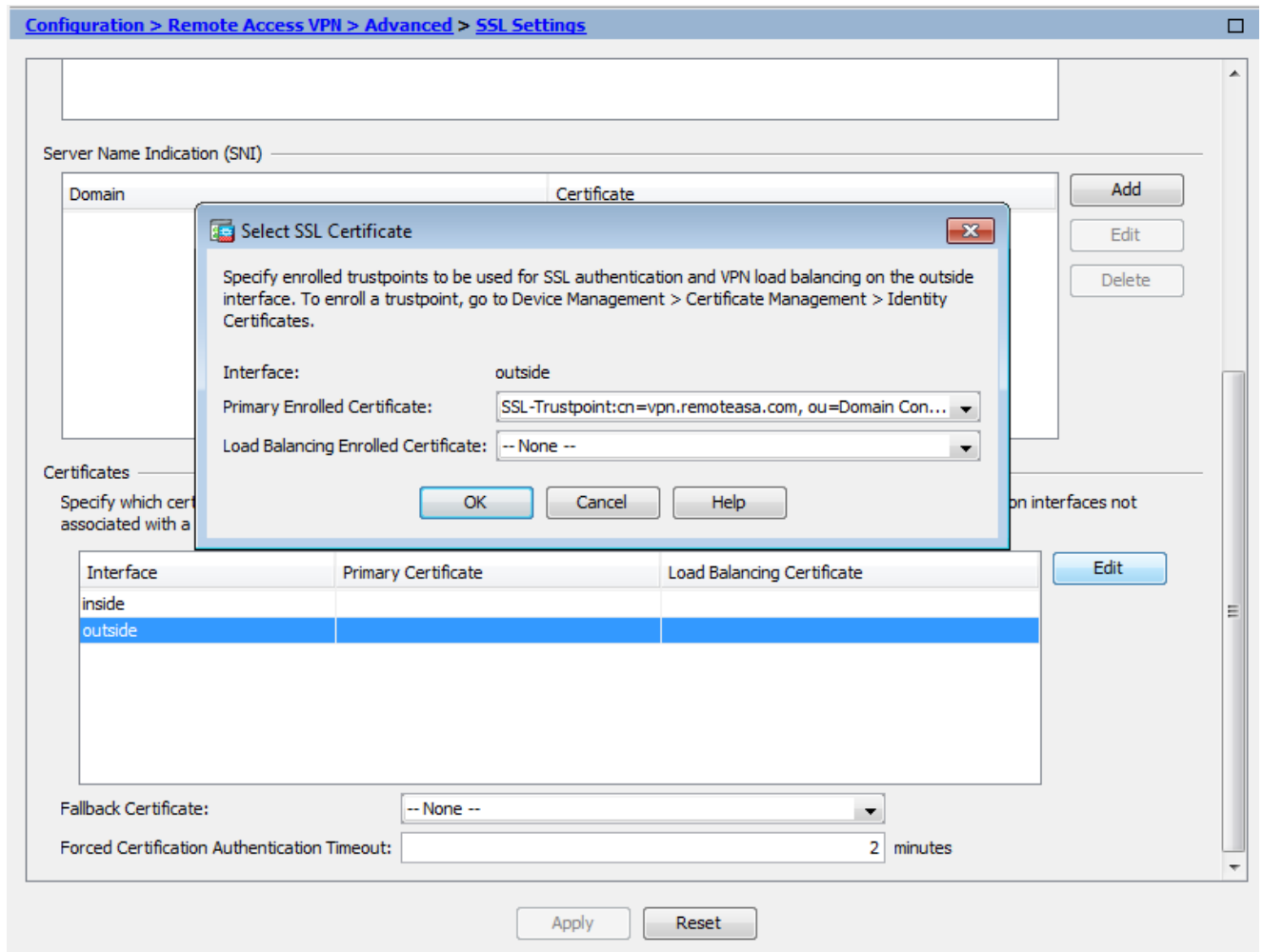


8. 導航到Configuration > Remote Access VPN > Advanced > SSL Settings。

9. 在「憑證」下方，選取用於終止 WebVPN 作業階段的介面。在此範例中，所使用的是外部介面。

10. 按一下Edit。

11. 在「Certificate」下拉選單中，並選擇新安裝的證書。



12. 按一下OK。

13. 按一下Apply。新證書現在用於終止於指定介面的所有WebVPN會話。

1.2. 使用 CLI 安裝 PEM 憑證

```
<#root>
```

```
MainASA(config)#
```

```
crypto ca authenticate SSL-Trustpoint
```

Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE----- MIIEDCCAuigAwIBAgIBADANBgkqhkiG9w0BAQUFADBjMQswCQYDVQQGEwJVUzEhMB8GA1UECh
```

```
!!! - Installing Next-level SubCA in the PKI hierarchy
```

```
.
```

```
!!! - Create a separate trustpoint to install the next subCA certificate (if present)  
in the hierarchy leading up to the Root CA (including the Root CA certificate)
```

```
MainASA(config)#crypto ca trustpoint SSL-Trustpoint-1
```

```
MainASA(config-ca-trustpoint)#enrollment terminal
MainASA(config-ca-trustpoint)#exit
MainASA(config)#
MainASA(config)# crypto ca authenticate SSL-Trustpoint-1
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
```

```
-----BEGIN CERTIFICATE-----
MIIEFTCCA2WgAwIBAgIDG+cVMA0GCSqGSIb3DQEBCwUAMGMxCzAJBgNVBAYTA1VT
MSEwHwYDVQQKEWhUaGUgR28gRGFkZHKgR3JvdXAsIE1uYy4xMTAvBgNVBAsTKEdv
IERhZGR5IENsYXNzIDIgQ2VydG1maWNhdG1vbiBBdXRob3JpdHkwHhcNMTQwMTAx
MDcwMDAwWhcNMzEwNTMwMDcwMDAwWjCBgzELMAkGA1UEBhMCVVMxEDA0BgNVBAGT
B0FYaXpvcjEwMTpsUgQwE7hPHmhUmFJ+r2hBt0oLTbcJjHMgGxBT4H
Y29tLCBjbMUMTEwLWYDVQQDEYhHbyBEYWRkeSBSb290IEN1cnRpZm1jYXR1IEF1
dGhvcml0eSAtIEcyMIIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3Fi
CPH6WTT3G8kYo/eASVjPjIoMTpsUgQwE7hPHmhUmFJ+r2hBt0oLTbcJjHMgGxBT4H
Tu70+k8vWTAi56sZvmvigaF88xZ1gD1Re+X5NbZ0TqmNghPktj+pA4P6or6KFWp/
3gvDthkUBcrqw6gE1DtGfDIN8wBmIisiNaW02jBEYt90yHGC00PoCjM7T3UYH3go+
6118yHz7sCtTpJJiaVE1BWEaRIGMLK1D1iPfrDqBmg4pxRyp6V0etp6eMAo5zvGI
gPtLXcwy7IViQyU0A1YnAZG003AqP26x6JyIAX2f1PnbU21gnb8s51iruF9G/M7E
GwM8CetJMVxpRrPgrWIDAQABo4IBFzCCARMwDwYDVR0TAQH/BAUwAwEB/zA0BgNV
HQ8BAf8EBAMCAQYwHQYDVR0OBBYEFdqahQcQZyi27/a9BUFuIMGU2g/eMB8GA1Ud
IwQYMBaAFNLEsNKR1EwRcbNhyz2h/t2oatTjMDQGCCsGAQUFBwEBBCgwJjAkBggr
BgEFBQcwAYYYaHR0cDovL29jc3AuZ29kYWRkeS5jb20vMDIGA1UdHwQrMCKwJ6A1
oCOGIWh0dHA6Ly9jcmwuZ29kYWRkeS5jb20vZ2Ryb290LmNybDBGBgNVHSAEPzA9
MDsGBFUdIAAwMzAxBggrBgEFBQcCARY1aHR0cHM6Ly9jZXJ0cy5nb2RlZGR5LmNv
bS9yZXBvc210b3J5LzANBgkqhkiG9w0BAQsFAAOCAQEAWQtTvZKGEacke+1bMc8d
H2xwxbhuvk679r6XU0Ewf7ooXGKUwuN+M/f7QnaF25UcjCJYdQkMiGVn0QowCcWg
0JekxS0TP7QYpgEGRJHj2kntFo1fzq3Ms3dhP8q0CkzpN1nsoX+oYggHFCJyNwq
9kIDN0zmiN/VryTyscPzfLXs4J1et01UIDyUGAZHHFIYSaRt4bNYC8nY7NmuHDK0
KHAN4v6mF56ED71XcLNa6R+gh10773z/aQvgSM03kwvIC1TErF0UZzdsyqUvMQg3
qm5vjLyb41ddJIGv15echK1srDdMZvNhkREg5L4wn3qkKQmw4TRfZHCyQFHfjDCm
rw==
-----END CERTIFICATE-----
quit
```

```
INFO: Certificate has the following attributes:
Fingerprint:      81528b89 e165204a 75ad85e8 c388cd68
Do you accept this certificate? [yes/no]: yes
```

Trustpoint 'SSL-Trustpoint-1' is a subordinate CA and holds a non self-signed certificate.

Trustpoint CA certificate accepted.

```
% Certificate successfully imported
BGL-G-17-ASA5500-8(config)#
```

!!! - Similarly create additional trustpoints (of the name "SSL-Trustpoint-n", where n is number thats incremented for every level in the PKI hierarchy) to import the CA certificates leading up to the Root CA certificate.

!!! - Importing identity certificate (import it in the first trustpoint that was created namely "SSL-Trustpoint")

```
MainASA(config)#
crypto ca import SSL-Trustpoint certificate
```

WARNING: The certificate enrollment is configured with an fqdn that differs from the system fqdn. If th
yes

% The fully-qualified domain name in the certificate will be:

(asa.remotevpn.url)

Enter the base 64 encoded certificate. End with the word "quit" on a line by itself

----BEGIN CERTIFICATE-----

```
MIIFRjCCBC6gAwIBAgIIJc1zqYQHbGUDQYJKoZIhvcNAQELBQAwgbQxCzAJBgNV
BAYTA1VTMRAwDgYDVoQQIEwdBcm16b25hMRMwEQYDVoQQHEwpTY290dHNkYWx1MRow
GAYDVQQKEwFHb0RhZGR5LmNvbSw5jLjEtMCSGA1UECxMkaHR0cDovL2N1cnRz
LmdvZGFkZHZhY29tL3J1cG9zaXRvcnkVMTMwMQYDVoQQDEypHbyBEYWRkeSBTZW
cmUgQ2VydG1maWNhdGUgQXV0aG9yaXR5IC0gRzIwHhcNMTUwNzIyMTIwNDM4WhcN
MTYwNzIyMTIwNDM4WjA/MSEwHwYDVoQLEXhEb21haW4gQ29udHJvbCBWYXpZGF0
ZWQxGjAYBgNVBAMTEXWbi5yZW1vdGVhc2EuY29tMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIIBCgKCAQEArrY2Fv2S2Uq5HdDh0aSzK5Eyok2tv2Rem8DofbTQ+4F9
C9IXitWdLa06a7dzyfB4S9hx1VZXoHMGgNd6i9NWLXsWU1Nx5pRMaKR4h1cL6bDW
ITt5GzKdL93ibMxYmau+uwM30kBb8QxLNNxr4G+oXtFavctTxWy/o6LzKWFyj0XP
tta9FZW07c0MNvKiUL1v9WBcy4GK1xyvN9RtWebtVkM5/i0v0ReBTBfFxCJ1YQAG
UWteu1ikWAGj1qomZGnZgAFDwj4/hxjesG2BGMtwX5L108cbmbi/u/vnmZ5Xhiqx
<snip>
```

```
CCsGAQUFBwIBFitodHRwOi8vY2VydG1maWNhdGVzLmdvZGFkZHZhY29tL3J1cG9z
aXRvcnkVMTMwMQYDVoQQIEwdBcm16b25hMRMwEQYDVoQQHEwpTY290dHNkYWx1MRow
Z29kYWRkeS5jb20vMEAGCCsGAQUFBzAChjRodHRwOi8vY2VydG1maWNhdGVzLmdv
ZGFkZHZhY29tL3J1cG9zaXRvcnkVZ2RzZzIuY3J0MB8GA1UdIwQYMBaAFEDCvSe0
zDSDMKIz1/tss/COLIDOMEYGA1UdEQQ/MD2CEXZwbi5yZW1vdGVhc2EuY29tghV3
d3cudnBuLj1bW90ZWFzYS5jb22CEXZwbi5yZW1vdGVhc2EuY29tMB0GA1UdDgQW
BBT7en7YS3PH+s4z+wTR1pHr2tSzejANBgkqhkiG9w0BAQsFAAOCQAEO9H8TLN
x2Y0rYdI6gS8n4imaSYg9Ni/9Nb6mote3J2LELG9HY9m/zUCR5yVkra9azdrNUAN
1hjBJ7kKQScLC4sZLONdG1uTP5rbWR0yikF5wSzyMwD03kOR+vM8q6T57vRst5
69vzBUuJc5bSu1IjyfPP19z1l+B2eBwUFbVfXLnd9bTfiG9mSmC+4V63TXFxt10q
xkGNys3GgYuCUy6yRP2cAUV11c2tYtaxoCL8yo72YUDDgZ3a4Py01EvC1F0aUtgV
6QNEOYwmbJkyumdPUwko6wGOC0Wlumzv5gHhni168HYSZ/4XI1p3B9Y8yfG5pwbN
7puzH+xgQRdg==
```

-----END CERTIFICATE-----

quit

INFO: Certificate successfully imported

! Apply the newly installed SSL certificate to the interface accepting SSL connections

MainASA(config)#

```
ssl trust-point SSL-Trustpoint outside
```

2.1 使用 ASDM 安裝 PKCS12 憑證

在ASA上未生成CSR的情況下（例如萬用字元證書或生成UC證書），身份證書和私鑰作為單獨的檔案或單個捆綁的PKCS12檔案（.p12或pfx格式）接收。若要安裝此型別的憑證，請完成以下步驟。

1. 身份證書將CA證書和私鑰捆綁到單個PKCS12檔案中。[附錄 B 會提供使用 OpenSSL 執行此作業的步驟。](#) 如果已由 CA 合併，請繼續進行下一步。
2. 導航到 Configuration > Remote Access VPN > Certificate Management, , 然後選擇 Identity Certificates.
3. 按一下Add。
4. 指定信任點名稱。

5. 按一下單 **Import the identity certificate from a file** 選按鈕。
6. 輸入用於建立 PKCS12 檔案的複雜密碼。瀏覽並選取 PKCS12 檔案。輸入憑證複雜密碼。

Add Identity Certificate

Trustpoint Name:

Import the identity certificate from a file (PKCS12 format with Certificate(s) +Private Key):

Decryption Passphrase:

File to Import From:

Add a new identity certificate:

Key Pair:

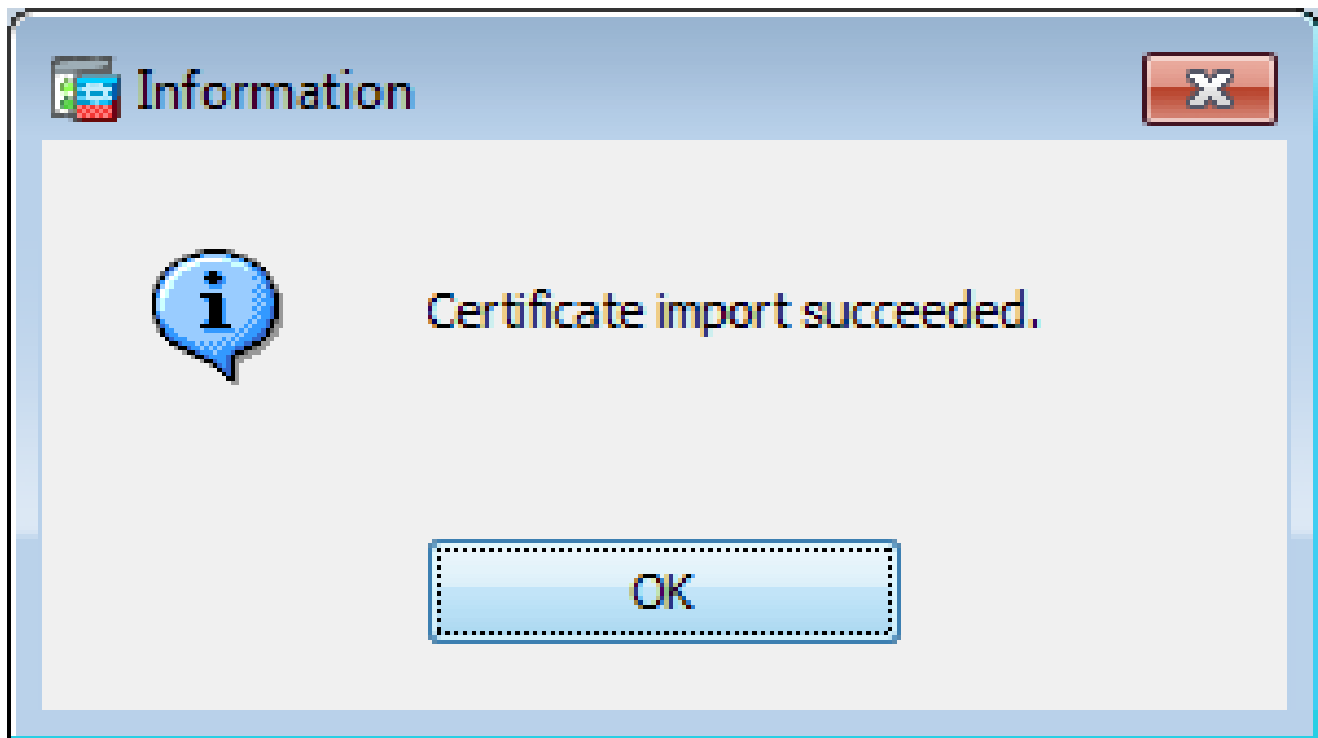
Certificate Subject DN:

Generate self-signed certificate

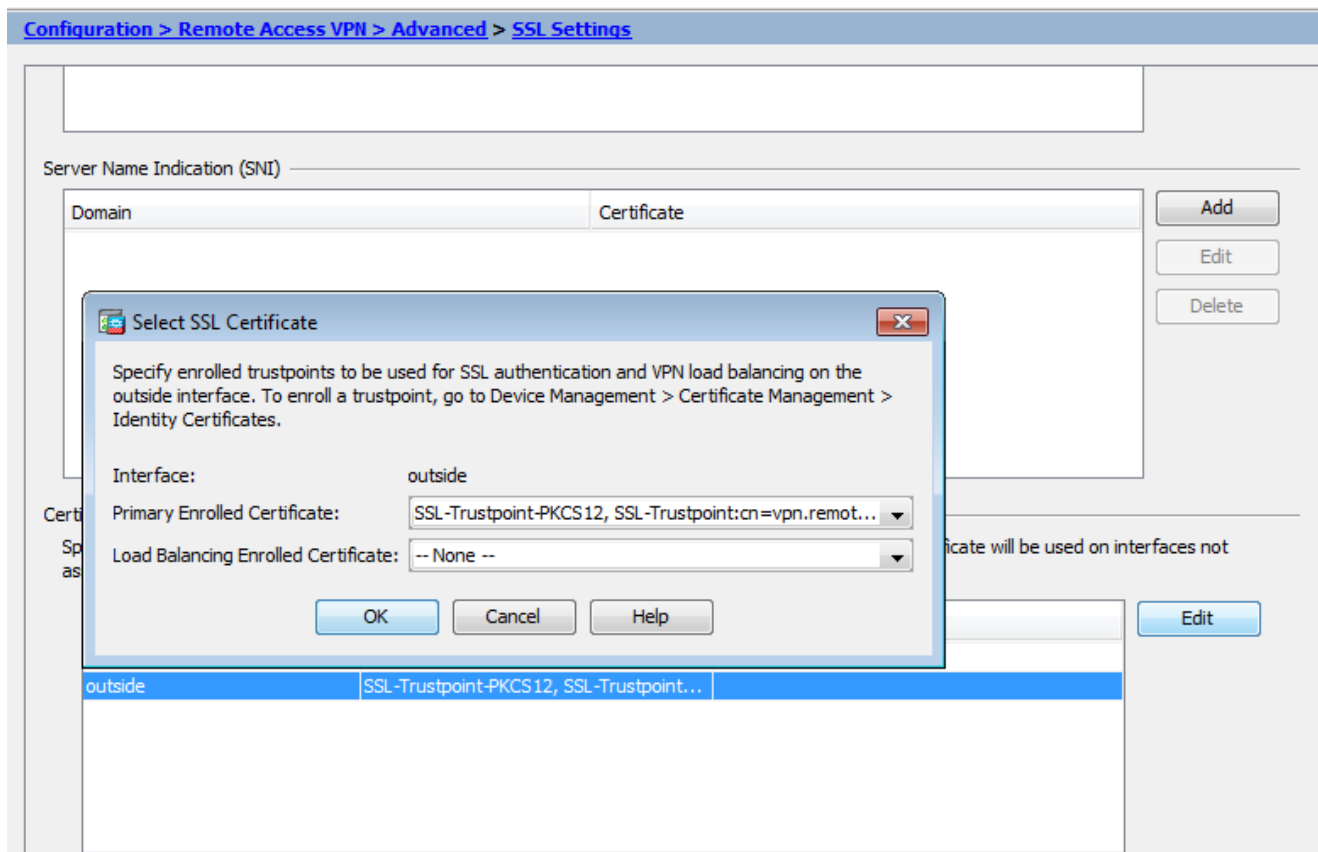
Act as local certificate authority and issue dynamic certificates to TLS-Proxy

Enable CA flag in basic constraints extension

7. 按一下「新增憑證」。



8. 導航到 **Configuration > Remote Access VPN > Advanced**，然後選擇 **SSL Settings**。
9. 在「憑證」下方，選擇用於終止 WebVPN 作業階段的介面。在此範例中，所使用的是外部介面。
10. 按一下 **Edit**。
11. 在「憑證」下拉式清單中，選擇新安裝的憑證。



12. 按一下 **OK**。

13. 按一下Apply。新證書現在用於終止於指定介面的所有WebVPN會話。

2.2 使用 CLI 安裝 PKCS12 憑證

```
<#root>
```

```
MainASA(config)#
crypto ca trustpoint SSL-Trustpoint-PKCS12
MainASA(config-ca-trustpoint)#
enrollment terminal
MainASA(config-ca-trustpoint)#
exit

MainASA(config)#
crypto ca import SSL-Trustpoint-PKCS12 pkcs12 cisco123
```

Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:

```
-----BEGIN PKCS12-----
MIISNwIBAzCCEfEGCSqGSIb3DQEHAaCCEeIEghHeMIIR2jCCEdYGCsGSIb3DQEH
BqCCEccwghHDAgEAMIIRvAYJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMDQIWO3D
hDtI/uECAQGAghGQ9ospee/qtIbVZh2T8/Z+5dxRPbcStDTqyKy7q3+9ram5AZdG
Ce9n5UCckqT4WcTjs7XZtCrUrt/LkNbmGDVhwGBmYWi0S7npgaUq0eoqiJRK+Yc7
LN0nbho6I5WfL56/JiceAMIXDLr/IqqLg2QAAPGdN+F5vANsHse2GsAATewBDLt7
Jy+SKfoNvvIw9QvzCiUzMjYZBANmBdMCQ13H+YQTHitT3vn2/iCD1zRSuXcypEV
q5e3hei00751E8TDLWm03PMvWIZqi8yzWesjcTt1Kd4FoJBZpB70/v9LntoIUOY7
kIQM8fHb4ga8BYfbgRmG6mkMm01STtbSv1vTa19WTmdQdTycA+G5PkrryRsy3Ww1
1kGFmHImmrrnNADF7Hmzbys1VohQZ7h09iVQY9krJogoXHjmQYxG9brf0oEwxSJDa
mGDhHESh+s/WuFSV9Z9kiTXpJNZxpTASoWBQrrwm05v8ZwbjbVnJ7sVdbwpU16d+
NNFGR7LTq08hpueeJnY9eJc2yYqeAXWXQ5kL0Zo6/gBEdGtEaZBgCFK9JZ3b13A
xqxGifanWpNLyG611NkuNjTgjbhNEEYI2uZzU0qxn1Ka8zyXw+1zrKuJscDbkAPZ
wKtw8k+p40zXVHhuANo6MDvffNRY1KQDtyK1inoPH5ksVSE5awkVam4+HTcqeUfa
16LMana+4QRgSetJhU0LtsMaQfRJKgha4JLq2t+JrCAPz2osAR1TsB0jQBNq6YNj
0uB+gGk2G18Q5N1n6K1fz0XBFZLWEDBLsaBR05MANE7wWt00+4awGYqVdmIF11kf
XIRKAiQEr1pZ6BVPuvsCNJxaaUHzufhYI2ZAckasKBZOT8/7YK3fnAaGoBCz4cHa
o2EEQhQ2aYb6YTv0+wtLEWGHZsbGZEM/u54XmsXAI7g28LGJYdfwi509KyV+Ac1V
KzhqXZMM2BbUQCncTF5JIMiW+r62k42FdahfaQb0vJsIe/IwkAKG7y6DIQFs0hwg
Z1PXiDbNr1k4e8L4gqumMKWg853PY+oY22rLDC7bu11CKtixIYBCvbn7dAYsI4GQ
T6xXhNu3+iye0HgbUQCfTU/mBra0Z0+bpKjWOCfqNBuYnZ6kUEdCI7GFLH9QqtM
K7YinFLoHwTWbi3MsmqVv+Z4ttVwy7Xmiko02nMynJMP6/CNV80MxMKdC2qm+c1j
s4Q1KcAmFsQmNp/7SIP1wnv0c6JbUmC10520U/r8ftTzn8C7WL62W79cLK4H0r7J
sNsZn0z0J0Z/xdZT+cLTCtVevKJQOMK3vMsi0uy52FkuF3HnfrmBqDkbr7yZxELG
RCELOEDdbp8VP0+IhN1yz1q7975SscdxFSL0TvjnHGFwd14ndoqN+blHwbdPjQWV
T3W2NCI95tmHDLGgp3P001S+rjdCEGGMg+9cpgBFFC1JocuTDIEcUbJBY8QRUNiS
/ubyUagdzUKt1ecfb9hMLP65ZnQ93Vw/NJKbIm7b4P/1Zp/1FP5eq7LkQPAXE4/
bQ4mHcnwrs+JGFkn19B8hJmmGoowH3p4IEvWzy7CThB3E1ejw5R4enqmrvgvHqpQe
B7odN10FLAHdo1G5BsHEXlUNEsEb40Q0pmKXiDDB5B001bJsr748fZ6L/LGx8A13
<snip>
ijDqxyfQXY4zSyt1jSMwMtYA9hG5I79Sg7pnME1E9xq1D0oRGg8vgx1wicKtLxp
LL0ReDY31KRYv00vW0gf+tE71ST/3TKZvh0sQ/BE0V3kHnw1dejMFH+dvyAA9Y1E
c80+tdafBFX4B/HP46E6heP6ZSt0xAfRW1/JF41jNvUNV09VtVfR2FTyWpzZFY8A
GG5XPIA80WF6wKEPFHICn8scY+Vot8kXxG96hwt2Cm5NQ20nVzxUZQbpKsjs/2jC
3HVFe3UJFBsY9UxTLCpXYBSIG+VeqkI8hWZp6c1TFNDLY2ELDY1Qzp1mBg2FujZa
```

YuE0avjCJzBzZUG2umtS5mHQnwPF+Xk0ujEyhGMauhGxHp4nghSzrUZrBeuL9lUF
2mbpsOcgZkzxMS/rjdNXjCmPF1oRBvKkZS1xHFRE/5ZopAhn4i7YtHQNrZ9U4RjQ
xo9cUuaJ+LNmvzE8Yg3epAMYZ16UNGQQkVQ6ME4BcjRONzW8BYgTq4+pmT1ZNq1P
X87CXCPtYrPHF57eSo+tHDINCgfqYXD6e/7r2ngfiCeUeNDZ4aV12XxvZDaU1BPP
Tx5fMARqx/Z8BdDyBJDVBjdsxmQau9HLkhPvdFG1ZIwdTe13CzKqXA5Pmpjt4q9
GnCpC53m76x9Su4ZDw6aUdBcgCTMvfaqJC9gz0bee2Wz+aRRwzSxu6tEWVZo1PEM
v0AA7po3vPek1g0nLRAwEoTTn4SdgNLWeRoxqZgkw1FC1GrotxF1so7uA+z0aMeU
1w73reonsNdZvRAcVX3Y6UNFDyt70Ixvo1H4VLzWmOK/oP62C9/eqqMwZ8zoCMPt
ENna7T+70s66SCbMmXCHwyh00tygNKZFFw/AATFyjQPMWPaxGuPNOrnB6uYcN0Hk
1BU7tF143RNIzaQqEH3XnaPvUuAA4C0FCoE3h+/tVjtfNKDvFmb6ZLZHYQmUYpyS
uhdFEpoDrJH1VmI2tik/iqYwaz+oDqXPHQXnJhw25h9ombR4qnd+FCfwFCGtPFON
o3Qffz53C95n5jPHVMYUrOxDdpwnvzCQPdj6yQm564TwLAmiZ7uD1pqJZJe5QxHD
no1v+4MdGSFvTbq+ykFoVcaamqeaq6sKgvAVujLXXEs4KEmIgcPqATVRG49E1ndI
L01DEQyKhVoDGebAuVRBjzwAm/qxWxxFv3hrbCjPHCwEYms4Wgt/vKKRFsuWJNZf
efH1dw11tkd5dKwSvDocPT/7mSLtLJa94c6AfgxXy9z0+FTLDQwzXga7xC2krAN1
yHxR2KHN5YeRL+KDzu+u6dYoKaz+YAgw1W6KbeavALSuH4EYqcvG8hUEhp/ySiSc
RDhuYgxEovIMGfES4FP5V521PyDhM3Dqwhn0vuYUmYnX8EXURkay44iwwI5HhqYJ
1ptWYyO8Bdr4Wnwt5xqsZgYR6mmGeAIin7bDunsF1uBHWYF4dyK1z1tsdRNMqYQ
+W5q+QjVdrj1dwv/bMF0aqEjxeNwBRqjzccff3BxMnwVxtgqxFvRh+DZxiJoiBG+
yx7x8np2AQ1r0METSSxbnZzfNkZKvBVMkIC6JsmT2WEVTQvoFJ8em+nem0WgTi/
hHSBzjE7RhAucnHuiFOCX0gvR1SDDqyCQbduc1QjXN0svA8Fqbea9WEH5khOPv3
pbtSL4gsf12pv8diBQkVQgiZDi8wb++7PR6ttiY65kVwrdson11/qq+xW0d3tB4/
zoH9LEMgTy9Ssz7myWrB9E00Z8BIjL1M8oMigEYrTD0c3KbyW1S9dd7QAxIU0BaX1
8J8q10ydvTBzmqcjesFH4/1NHn5Vnf0ZnNpui4uHP0XBG+K2zJUJXm6dq1AHB1E
KQFsFzPNNyave0Kk8JzQnLAPd70UU/Iksy0CGQozGBH+HSzVp1RDjrrbC342rkBj
wnI+j+/1JdwBmHdJMZCfoMZFLSI9ZBqFirdii1/NRu6jh76TQor5TnNjxIyNREJC
FE5FZnMFvhM900LaiUZff8WWC0ferDMttLXb1nuxPF1+1Rk+LN1PLVptWgcxzfSr
JXrGiWjxybBB9oCOrAcq8fGatEs8WRxJyDH3Jjmn9i/G16J1mMCUF//LxAH2WQx8
Ld/qS50M2iFCffDQjxAj0K6DEN5pUebBv1Em5SOHXvyq5nxgUh4/y84CwaKjwOMQ
5tbbLM1nc7ALIj9LxZ97YiXSTyeM6oBxBfx6Rpk1kDv05m1BghSpVQiMcQ20RIkh
UVVNBsh019S3cb5wqxaWqAKBqb4h1uLGVbYWZf2mzLZ8U5U5ioiqoMBqNZbzTxp0
EqEFuatT11QvCRbcKS3xou4MAixcYUxKwEhbZA/6hd10XSBjwe7jKBV9M6w1iKab
UfoJCGTaf3sY681qrMPrbt0eewf1C02Sd9Mn+V/jvni17mxYFFUpruRq3r1LeqP
J5camfTtHwyL8N3Q/Zwp+zQeWziLA8a/iAVu/hYLR1bpF2WCK010tJqkvVmrLVLz
maZZjbJe0ft5cP/1RxbK1S6Gd5dFEKDE15c6gWUX8RKZP6Q7iaE5hnGmQjm8Lj1
kXwF+ivox0Q8a+Gg1bVTR0c7tqW9e9/ewisV1mwvEB6Ny7TDS1oPUDHM84pY6dqi
1+0io07Ked4BySwN1Yy9yaJtBTZSCstfP+ApLiDn7pSBvvXf1aHmeNbkPOZJ+c+t
fGpUdL6V2UTXfCsOPHTC0ezA15sOHwCuPchrDIj/eGUwMS3NfS25XgcMuvnLqGV0
RzcrZ1ZIG8G0oLYwOCuzoY0D/m901001ahePyA9tmVB7HRRbytLdaW7gYeEikoCv
7qtBqJFF17ntWJ3EpQHZUCVClbHIKqjNqRbDCY7so4A1IW7kSEUGWMIUDhprE8Ks
NpvnPH2i9JrYrTeRoYUI0tL/7SATd2P0a21xz/zUwekeqd0bmvCsAgQNbB2XkrR3
XS0B52o1+63e8KDqS2zL2TZd3daDFidH1B8QB26tfbf0Aca0bJH5/dWP8ddo8UYo
Y3JqT10malxSjhaMhMqDZIqP49utW3Tcjg11YS4HEmcqtHud0ShaUysC6239j1Q
K1FwrwXT1BC5vnq5IcOMqx5zyNbfXz28969cwoMcyU6+kRw0TyF6kF7EEv6XWca
XLEwABx+tKRUKHJ673SyDMu96KMV3yZN+RtKbCjqCPVTP/3ZeIp7nCMUcj5sW9HI
N34yeI/ORCLyeGsOEiBLkucikC32LI9ik5HvImVTELQ0Uz3ceFqU/PkasjJUve6S
/n/1ZVUHBUk71xKR2bwZgEC17fIe17w1rbjP3Wbk+Er0kfYcsNRHxeTDpKPS9s
u/UsyQJiyNARG4X3iYQ1sTce/06Ycyri6GcLHAu58B02nj4Cxo1Cp1ABZ2N79HtN
/7Kh5L0pS9MwsDCHUUI8KFRtSET7TB1tIU99FdB19L64s1/shYAHbccvVWU50WhT
PdLoaErrX81Tof41IxbSZbI8grUC4KfG2sdPLJKu3HVTeQ8Lfl1bBLxfs8ZBS+Oc
v8rH1Q012kY6LsFGLehJ+/yJ/uvXORiv0ESp4EhFpFfkp+o+YcFeLUUPd+jzb62K
HfSCCbLpKCyEay80dyWkHfgy1qXmb9ud0oM050aFJyqRONjnt6pcxBRY2A6AJR5S
IIC26YNwbh0GjF9qL2FiUqnNH/7GTqPnd2qmsB6FTIwSBT6d854qN7PRt+ZXgdtQ
Ojcyt1r9qpWZpNFK8EzizwKiAYtsiEh2pzPt6YUpxRb6CXTkIzoG+Klsv2m3b8
OHyZ9a8z81/gnxrZ11sSCTf0SU70pHWh8VAYKVHhk+MwgQrOm/2ocV32dkRBLMy
2R6P4WfHyI/+9de1x3PtIu0iv2knpxHv2fKM6sQw45F7XkmwHxjq1YRJ6vIwPTAh
MAKGBSs0AwIaBQAEFFRETzpiSHKZR+Kmen68VrTwpV7BBSQi0IesQ4n4E/bSVsd
qJSzcwh0hgICBAA=
-----END PKCS12-----
quit

INFO: Import PKCS12 operation completed successfully

!!! Link the SSL trustpoint to the appropriate interface
MainASA(config)#

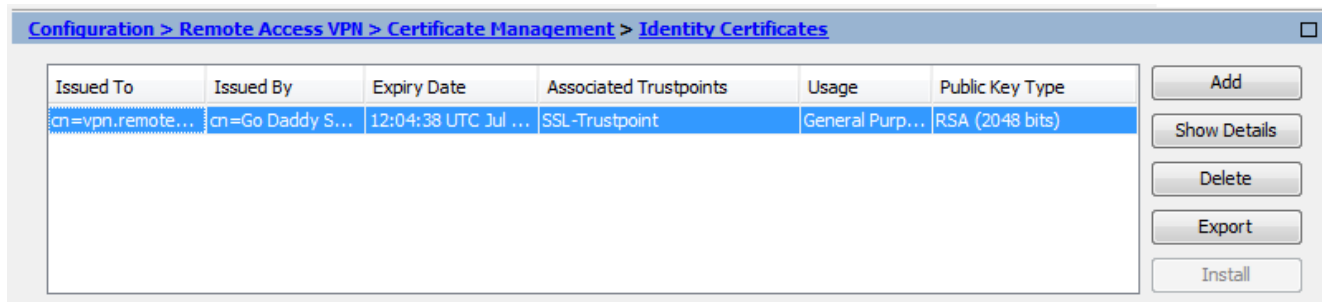
```
ssl trust-point SSL-Trustpoint-PKCS12 outside
```

驗證

使用以下步驟確認是否成功安裝第三方廠商憑證，並用於 SSLVPN 連線。

透過 ASDM 檢視安裝的憑證

1. 導覽 Configuration > Remote Access VPN > Certificate Management, 至並選擇 Identity Certificates.
2. 系統將顯示由第三方供應商頒發的身份證書。



透過 CLI 檢視安裝的憑證

```
<#root>
```

```
MainASA(config)#
```

```
show crypto ca certificate
```

Certificate

```
Status: Available
Certificate Serial Number: 25cd73a984070605
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA256 with RSA Encryption
Issuer Name:
  cn=Go Daddy Secure Certificate Authority - G2
  ou=http://certs.godaddy.com/repository/
  o=GoDaddy.com\, Inc.
  l=Scottsdale
  st=Arizona
  c=US
Subject Name:
  cn=(asa.remotevpn.url)
  ou=Domain Control Validated
OCSP AIA:
```


URL: <http://ocsp.godaddy.com/>
CRL Distribution Points:
[1] <http://crl.godaddy.com/gdig2s1-96.crl>
Validity Date:
start date: 12:04:38 UTC Jul 22 2015
end date: 12:04:38 UTC Jul 22 2016
Associated Trustpoints:

SSL-Trustpoint

CA Certificate

Status: Available
Certificate Serial Number: 07
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA256 with RSA Encryption
Issuer Name:
cn=Go Daddy Root Certificate Authority - G2
o=GoDaddy.com\, Inc.
l=Scottsdale
st=Arizona
c=US
Subject Name:
cn=Go Daddy Secure Certificate Authority - G2
ou=<http://certs.godaddy.com/repository/>
o=GoDaddy.com\, Inc.
l=Scottsdale
st=Arizona
c=US
OCSP AIA:
URL: <http://ocsp.godaddy.com/>
CRL Distribution Points:
[1] <http://crl.godaddy.com/gdroot-g2.crl>
Validity Date:
start date: 07:00:00 UTC May 3 2011
end date: 07:00:00 UTC May 3 2031
Associated Trustpoints:

SSL-Trustpoint

CA Certificate

Status: Available
Certificate Serial Number: 1be715
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA256 with RSA Encryption
Issuer Name:
ou=Go Daddy Class 2 Certification Authority
o=The Go Daddy Group\, Inc.
c=US
Subject Name:
cn=Go Daddy Root Certificate Authority - G2
o=GoDaddy.com\, Inc.
l=Scottsdale
st=Arizona
c=US

OCSP AIA:
URL: http://ocsp.godaddy.com/
CRL Distribution Points:
[1] http://crl.godaddy.com/gdroot.crl
Validity Date:
start date: 07:00:00 UTC Jan 1 2014
end date: 07:00:00 UTC May 30 2031
Associated Trustpoints:

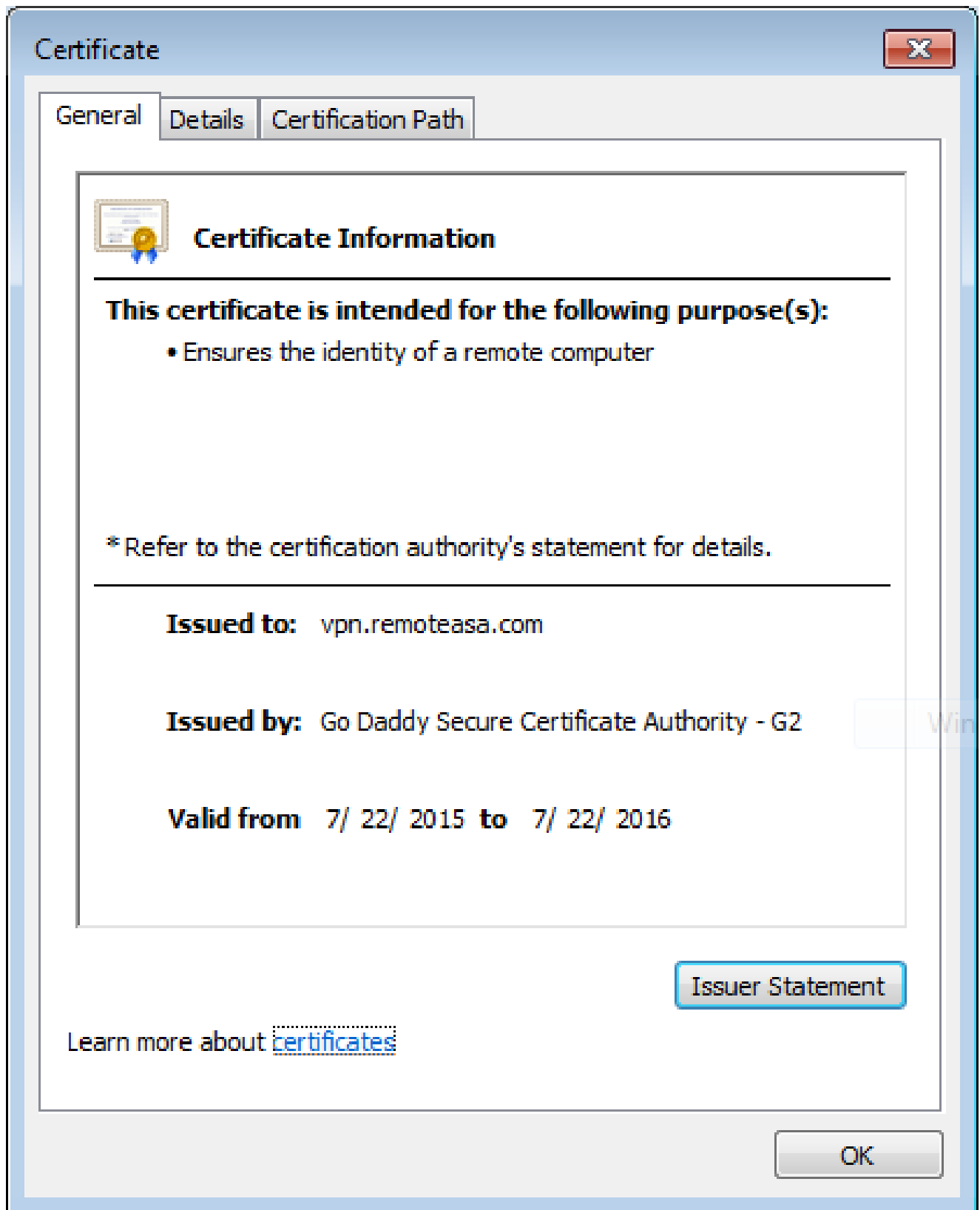
SSL-Trustpoint-1

...(and the rest of the Sub CA certificates till the Root CA)

使用Web瀏覽器驗證WebVPN的安裝證書

驗證WebVPN是否使用新證書。

1. 透過網頁瀏覽器連線至 WebVPN 介面。請將https://與用於請求證書的FQDN一起使用(例如 [https://\(vpn.remoteasa.com\)](https://(vpn.remoteasa.com)))。
2. 按兩下WebVPN登入頁面右下角顯示的鎖定圖示。安裝的憑證資訊必定會出現。
3. 檢閱內容以確認其符合第三方廠商核發的憑證。

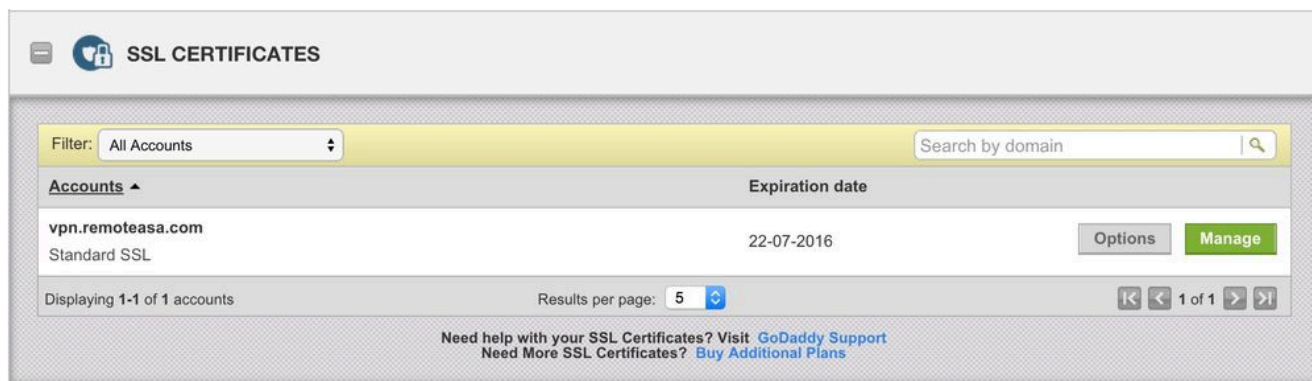


在 ASA 更新 SSL 憑證

1. 在ASA上、使用OpenSSL或在CA上使用與舊證書相同的屬性重新生成CSR。完成CSR生成中給定的[步驟](#)。
2. 在 CA 提交 CSR，然後產生 PEM 格式 (.pem、.cer、.crt) 的新身分識別憑證與 CA 憑證。在PKCS12證書的情況下，還有一個新的私鑰。

在使用 GoDaddy CA 情況下，憑證可透過產生的 CSR 重設金鑰。

前往 GoDaddy 帳戶，然後按一下「SSL 憑證」下方的「管理」。



按一下「檢視狀態以取得需要的網域名稱。



按一下「Manage」以提供選項，以便對憑證重新建立金鑰。

All > vpn.remoteasa.com

Standard SSL Certificate

Certificate Management Options

		
Download	Revoke	Manage

Certificate Details

Status	Certificate issued
Domain name	vpn.remoteasa.com
Encryption Strength	GoDaddy SHA-2
Validity Period	7/22/2015 - 7/22/2016
Serial Number	25:cd:73:a9:84:07:06:05

展開「重設憑證金鑰」選項，然後新增 CSR。

vpn.remoteasa.com > Manage Certificate

Standard SSL Certificate

Use this page to submit your certificate changes for review all at once, not individually. We'll review them together so your changes happen faster.

Submitting any changes on this form will issue a new certificate and your current certificate will be revoked. You will have 72 hours to install the new certificate on your website.


 Re-Key certificate*Private key lost, compromised, or stolen? Time to re-key.*

Certificate Signing Request (CSR)

```
13qHhfenpIRd3QX0kDh4P/wKI12bz/zb1v/SI
N80GsenQVuZaYzIH-N3R9EU/3Rz9
PcctuZ18yZLZTr6NSxki9im111aCuxlH9FmW
```

Domain Name (based on CSR):

vpn.remoteasa.com

 New Keys, please...

You can generate a Certificate Signing Request (CSR) by using a certificate signing tool specific to your operating system. Your CSR contains a public key that matches the private key generated at the same time.

 Change the site that your certificate protects*If you want to switch your certificate from one site to another, do it here.* Change encryption algorithm and/or certificate issuer*Upgrade your protection or change the company behind your cert.*

儲存並繼續執行下一步。GoDaddy根據提供的CSR頒發新證書。

3. 在新的信任點中安裝新的憑證 (如「在 ASA 安裝 SSL 憑證」一節所示) 。

常見問題

1. 什麼是從一個 ASA 將身分識別憑證傳輸至不同 ASA 的最佳方式？

將憑證連同金鑰一併匯出至 PKCS12 檔案。

使用此指令以透過 CLI 從原始 ASA 匯出憑證：

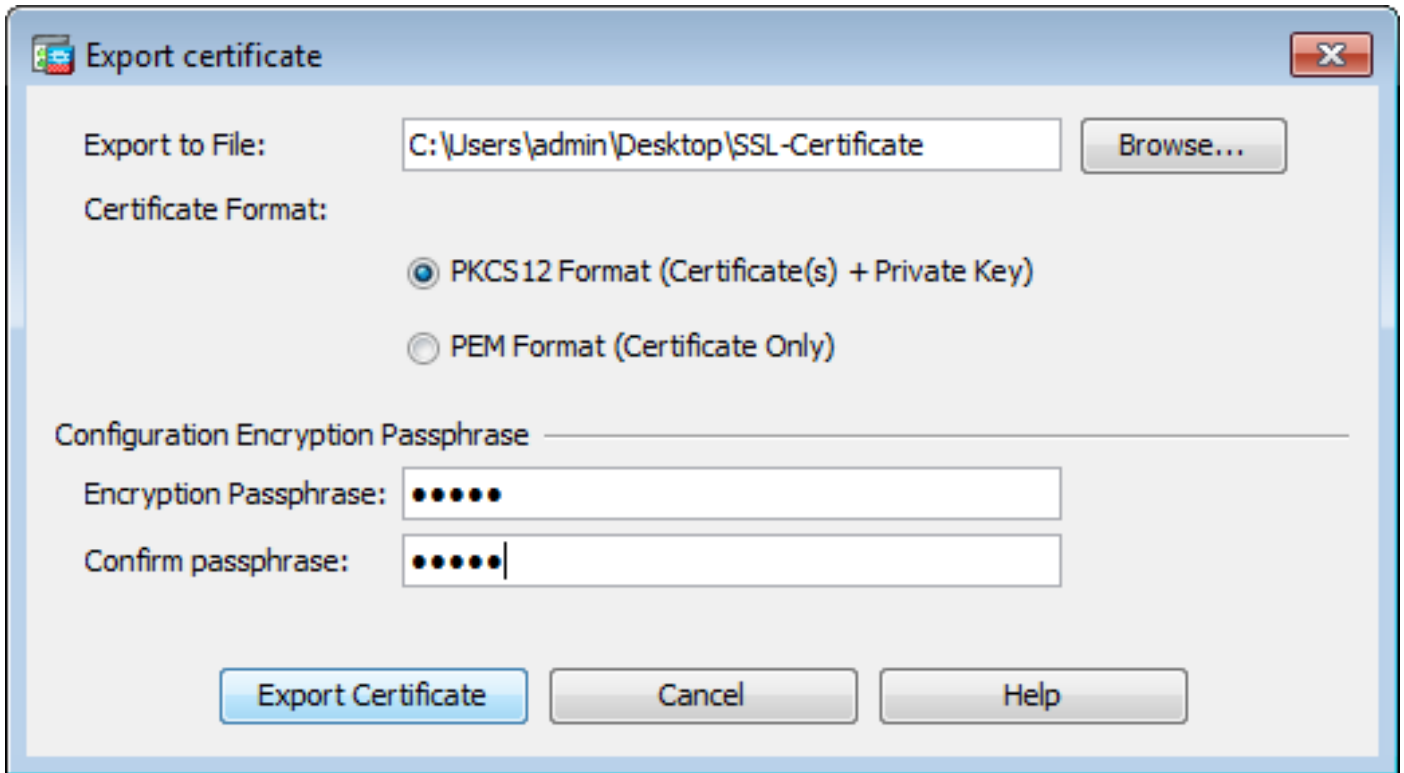
```
<#root>
```

```
ASA(config)#
```

```
crypto ca export
```

```
pkcs12
```

ASDM配置：



使用此指令以透過 CLI 將憑證匯入目標 ASA :

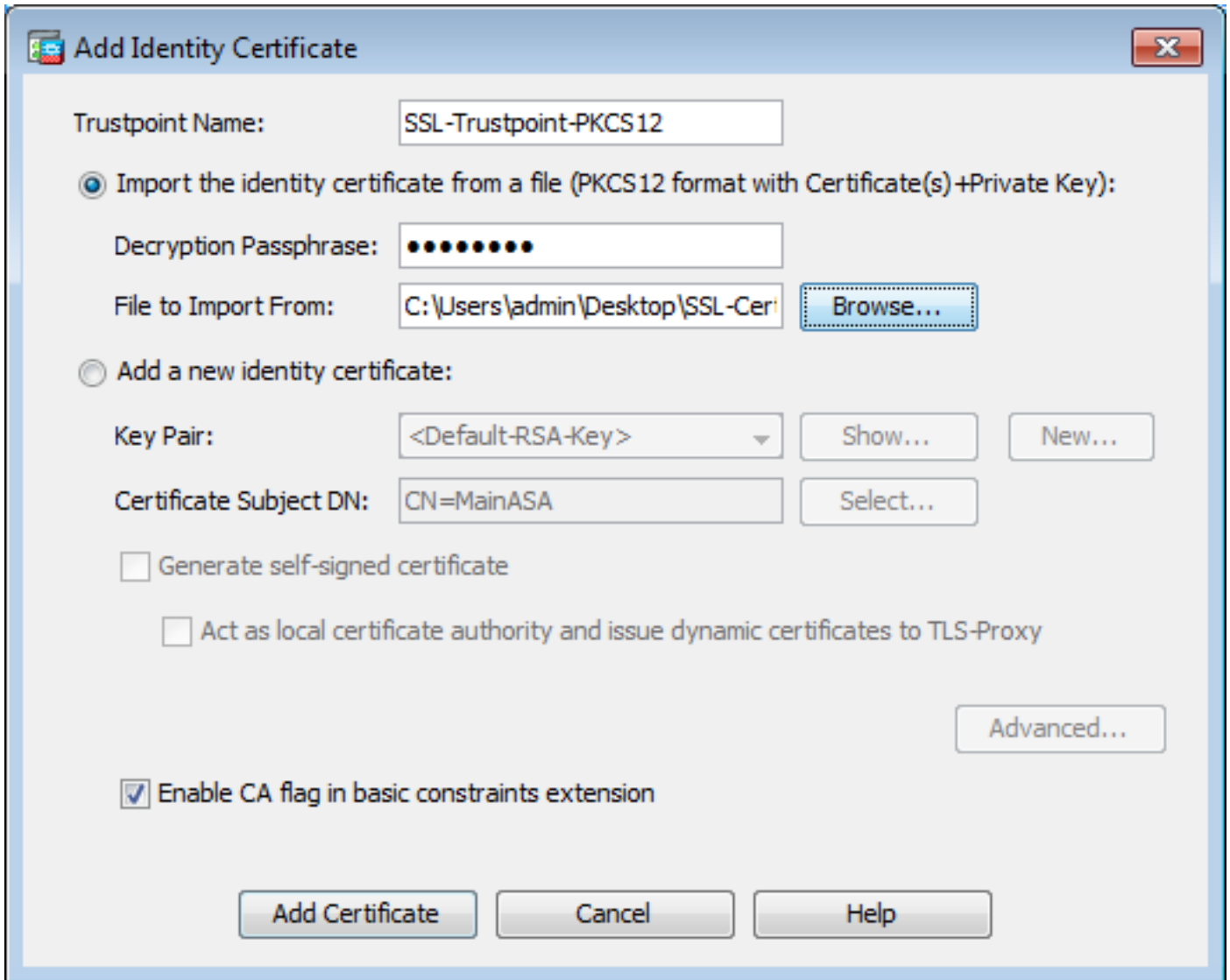
```
<#root>
```

```
ASA(config)#
```

```
crypto ca import
```

```
pkcs12
```

ASDM配置 :



此程序亦可使用以下步驟，透過 ASDM 的備份/還原功能完成：

1. 通過ASDM登入到ASA並選擇Tools > Backup Configuration。
2. 備份所有組態或僅限身分識別憑證。
3. 在目標ASA上，開啟ASDM並選擇Tools > Restore Configuration。

2. 如何產生 SSL 憑證以搭配 VPN 負載平衡 ASA 使用？

以下提供多種方法，可用於透過 VPN 負載平衡環境專用的 SSL 憑證設定 ASA。

1. 使用單一整合通訊憑證 (UCC)/多網域憑證，該憑證具有平衡負載 FQDN 做為 DN，或具有個別 ASA FQDN 做為獨立的主體替代名稱 (SAN)。GoDaddy、Entrust、Comodo 及其他廠商等多個知名 CA 支援此類憑證。當您選擇此方法時，請務必記得 ASA 目前不支援透過多個 SAN 欄位建立 CSR。此問題已記錄於增強功能思科錯誤 ID [CSCso70867](#)。在此案例中，有兩個選項可
 - a. 透過 CLI 或 ASDM 產生 CSR。當 CSR 提交至 CA 時，在 CA 入口網站本身中加入多個 SAN。
 - b. 使用OpenSSL產生CSR，並將多個SAN包含在openssl.cnf檔案中。

當 CSR 已提交至產生的 CA 和憑證，請將此 PEM 憑證匯入至產生 CSR 的 ASA。完成後

，以PKCS12格式將此證書匯出並匯入到其他成員ASA上。

2. 使用萬用字元憑證。與UC證書相比，這種方法安全性較低，也較為靈活。如果CA不支援UC憑證，則會在CA上或使用OpenSSL產生CSR，其中FQDN的格式為*.domain.com。當CSR已提交至產生的CA和憑證，請將此PKCS12憑證匯入至叢集中的所有ASA。
3. 使用每個成員ASA和負載平衡FQDN專用的個別憑證。這是效率最低的解決方案。系統可以為每個個別ASA建立憑證（如本文件所示）。VPN負載平衡FQDN的證書在一台ASA上建立，並匯出並作為PKCS12證書匯入到其他ASA上。

3. 在ASA容錯移轉配對中，憑證是否需要從主要ASA複製到次要ASA？

無需手動將證書從主ASA複製到輔助ASA，因為只要配置了狀態故障切換，證書在ASA之間同步。如果在容錯移轉初始設定時，未在待命裝置上看見憑證，請發出指令write standby以強制同步。

4. 如果使用ECDSA金鑰，SSL憑證產生程序是否會不同？

唯一的配置差異是金鑰對生成步驟，在此步驟中生成ECDSA金鑰對，而不是RSA金鑰對。其他步驟皆維持不變。用於生成ECDSA金鑰的CLI命令如下所示：

```
<#root>
```

```
MainASA(config)#
```

```
cry key generate ecdsa label SSL-Keypair elliptic-curve 256
```

```
INFO: The name for the keys will be: SSL-Keypair  
Keypair generation process begin. Please wait...
```

疑難排解

指令疑難排解

如果SSL憑證安裝失敗，以下偵錯指令皆會收集於CLI：

```
debug crypto ca 255
```

```
debug crypto ca messages 255
```

```
debug crypto ca transactions 255
```

常見問題

使用9.4(1)及更高版本的ASA上的外部介面上帶有有效第三方SSL證書的不可信證書警告。

解決方案：將RSA金鑰對與證書結合使用時，會出現此問題。從9.4(1)開始的ASA版本上，預設情況下啟用所有ECDSA和RSA密碼，並使用最強密碼（通常是ECDSA密碼）進行協商。若發生此問題，ASA會展示自我簽署憑證，而非目前設定的RSA型憑證。當RSA型憑證安裝於介面，且受到

思科錯誤 ID [CSCuu02848](#) 追蹤時，以下增強功能可變更行為。

建議的操作：使用以下CLI命令禁用ECDSA密碼：

```
ssl cipher tlsv1.2 custom "AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA:RC4-SHA:RC4-MD5"
```

或者，使用ASDM導航至Configuration > Remote Access VPN > Advanced，然後選擇SSL Settings。在「加密」區段，選取tlsv1.2加密版本，然後使用自訂字串AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA:RC4-SHA:RC4-MD5加以編輯

附錄

附錄A:ECDSA或RSA

ECDSA 演算法屬於橢圓曲線密碼編譯 (ECC) 的一部份，且使用橢圓曲線產生公開金鑰；而 RSA 演算法會使用兩個質數與一個更小的數字的產品產生公開金鑰。這表示透過 ECDSA 即可達到與 RSA 相同層級的安全性，而且使用更小的金鑰就能實現。如此可縮短運算時間，並為使用 ECDSA 憑證的網站延長連線時間。

《[新一代編譯與 ASA](#)》(Next Generation Cryptography and the ASA) 的文件提供更深入的資訊。

附錄B：使用OpenSSL根據身份證書、CA證書和私鑰生成PKCS12證書

1. 驗證運行此進程的系統上是否安裝了OpenSSL。對於Mac OSX和GNU/Linux使用者，預設情況下會安裝此程式。
2. 切換到有效目錄。

在Windows上：預設情況下，實用程式安裝在C:\Openssl\bin中。在此位置開啟命令提示字元。

在Mac OSX/Linux上：在建立PKCS12證書所需的目錄中開啟Terminal視窗。

3. 在先前步驟提及的目錄中，儲存私密金鑰 (privateKey.key)、身分識別憑證 (certificate.crt) 及根 CA 憑證鏈結 (CACert.crt) 檔案。

將私密金鑰、身分識別憑證及根 CA 憑證鏈結合併至 PKCS12 檔案。輸入密碼以保護 PKCS12證書。

```
strong> openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in certificate.crt -cer
```

4. 將生成的PKCS12證書轉換為Base64編碼的證書：
<#root>

```
openssl base64 -in certificate.pfx -out certificate.p12
```

接著，匯入上一步產生的憑證以搭配 SSL 使用。

相關資訊

- [ASA 9.x配置指南 — 配置數位證書](#)
- [如何使用ASA上的ASDM從Microsoft Windows CA獲取數位證書](#)
- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。