# Configurazione delle appliance ASA: installazione e rinnovo del certificato digitale SSL

## Sommario

# Introduzione

In questo documento viene descritto come installare il certificato digitale SSL attendibile di terze parti sull'ASA per le connessioni Clientless SSLVPN e AnyConnect.

# Premesse

Nell'esempio viene utilizzato un certificato GoDaddy. Ogni passaggio contiene la procedura ASDM (Adaptive Security Device Manager) e l'equivalente CLI.

# Prerequisiti

## Requisiti

Questo documento richiede l'accesso a un'Autorità di certificazione (CA) di terze parti attendibile per la registrazione dei certificati. Esempi di fornitori di CA di terze parti includono, senza limitazioni, Baltimora, Cisco, Entrust, Geotrust, G, Microsoft, RSA, Thawte e VeriSign.

Prima di iniziare, verificare che l'ora, la data e il fuso orario dell'appliance ASA siano corretti. Con l'autenticazione dei certificati, si consiglia di usare un server Network Time Protocol (NTP) per sincronizzare l'ora sull'appliance ASA. La guida alla configurazione della CLI per le operazioni generali della serie Cisco ASA, versione 9.1, descrive i passaggi da eseguire per configurare correttamente l'ora e la data sull'appliance ASA.

## Componenti usati

Questo documento utilizza un'appliance ASA 5500-X con software versione 9.4.1 e ASDM versione 7.4(1).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Configurazione

Il protocollo SSL richiede che il server SSL fornisca al client un certificato server per eseguire l'autenticazione del server. Cisco sconsiglia di utilizzare un certificato autofirmato perché potrebbe essere impossibile configurare inavvertitamente un browser per considerare attendibile un certificato rilasciato da un server non autorizzato. Vi è inoltre l'inconveniente per gli utenti di dover rispondere a un avviso di sicurezza quando si connette al gateway sicuro. A tale scopo, è consigliabile utilizzare CA di terze parti attendibili per rilasciare certificati SSL all'appliance ASA.

Il ciclo di vita di un certificato di terze parti sull'appliance ASA ha luogo essenzialmente con i seguenti passaggi:


## Generazione CSR

La generazione di CSR è il primo passaggio del ciclo di vita di qualsiasi certificato digitale X.509.

Una volta generata la coppia di chiavi privata/pubblica Rivest-Shamir-Adleman (RSA) o Elliptic Curve Digital Signature Algorithm (ECDSA) (l'Appendice A spiega in dettaglio la differenza tra l'uso di RSA o ECDSA), viene creata una Richiesta di firma del certificato (CSR).

Un CSR è un messaggio in formato PKCS10 che contiene la chiave pubblica e le informazioni sull'identità dell'host che invia la richiesta. In Formati di dati PKI vengono illustrati i diversi formati di certificato applicabili alle appliance ASA e Cisco IOS®.

---

Note:
1. Verificare con la CA le dimensioni della tastiera richieste. Il forum CA/browser ha stabilito che tutti i certificati generati dalle CA membri abbiano una dimensione minima di 2048 bit.
2. Al momento, l'ASA non supporta le chiavi a 4096 bit (ID bug Cisco CSCut53512) per l'autenticazione del server SSL. Tuttavia, IKEv2 supporta l'uso di certificati server a 4096 bit solo sulle piattaforme ASA 5580, 5585 e 5500-X.
3. Utilizzare il nome DNS dell'appliance ASA nel campo FQDN del CSR per impedire la visualizzazione di avvisi relativi a certificati non attendibili e superare la verifica dei certificati rigorosi.

---

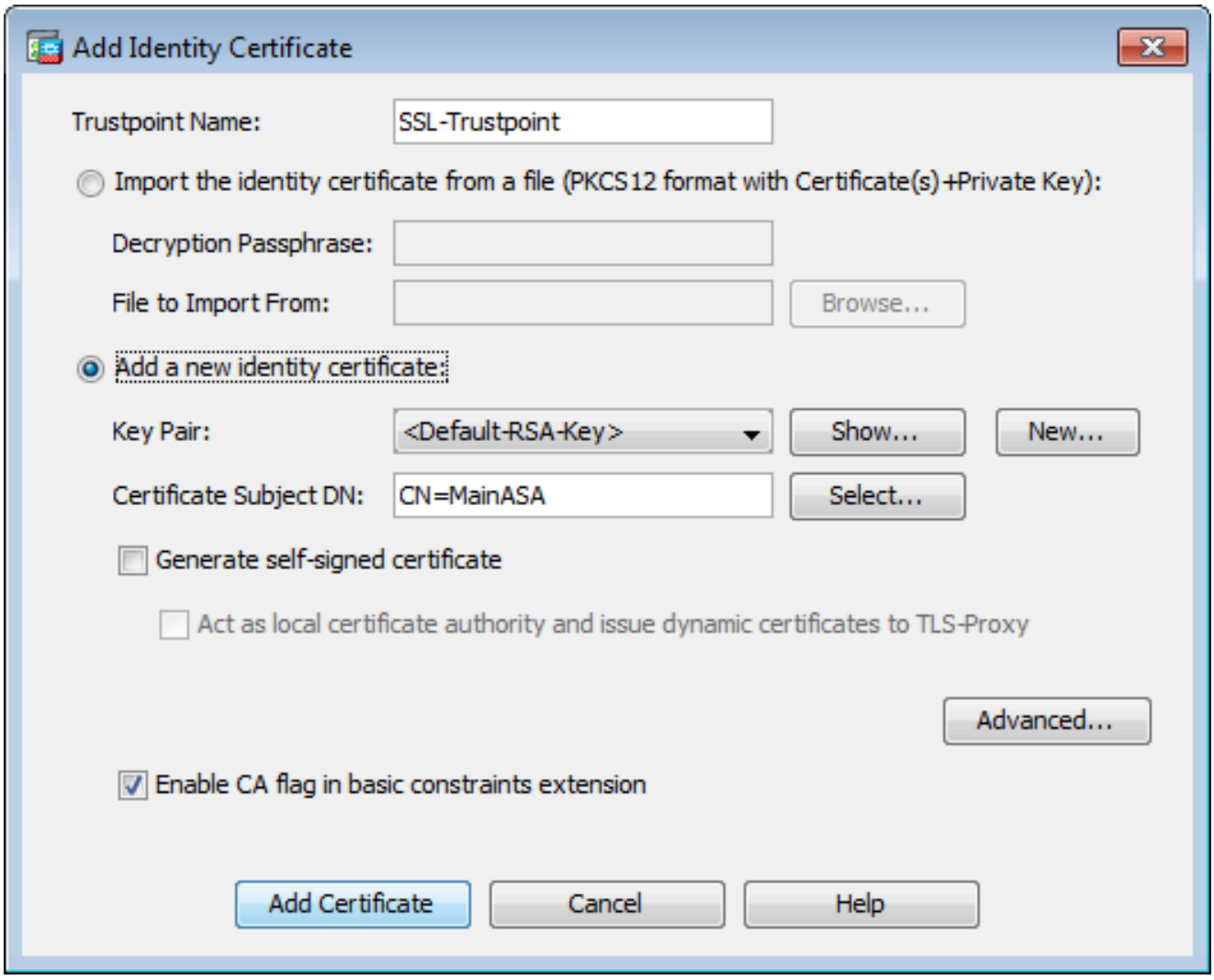
Esistono tre metodi per generare la RSI.

- Configurazione con ASDM
- Configurazione con la CLI di ASA
- Utilizzare OpenSSL per generare il CSR

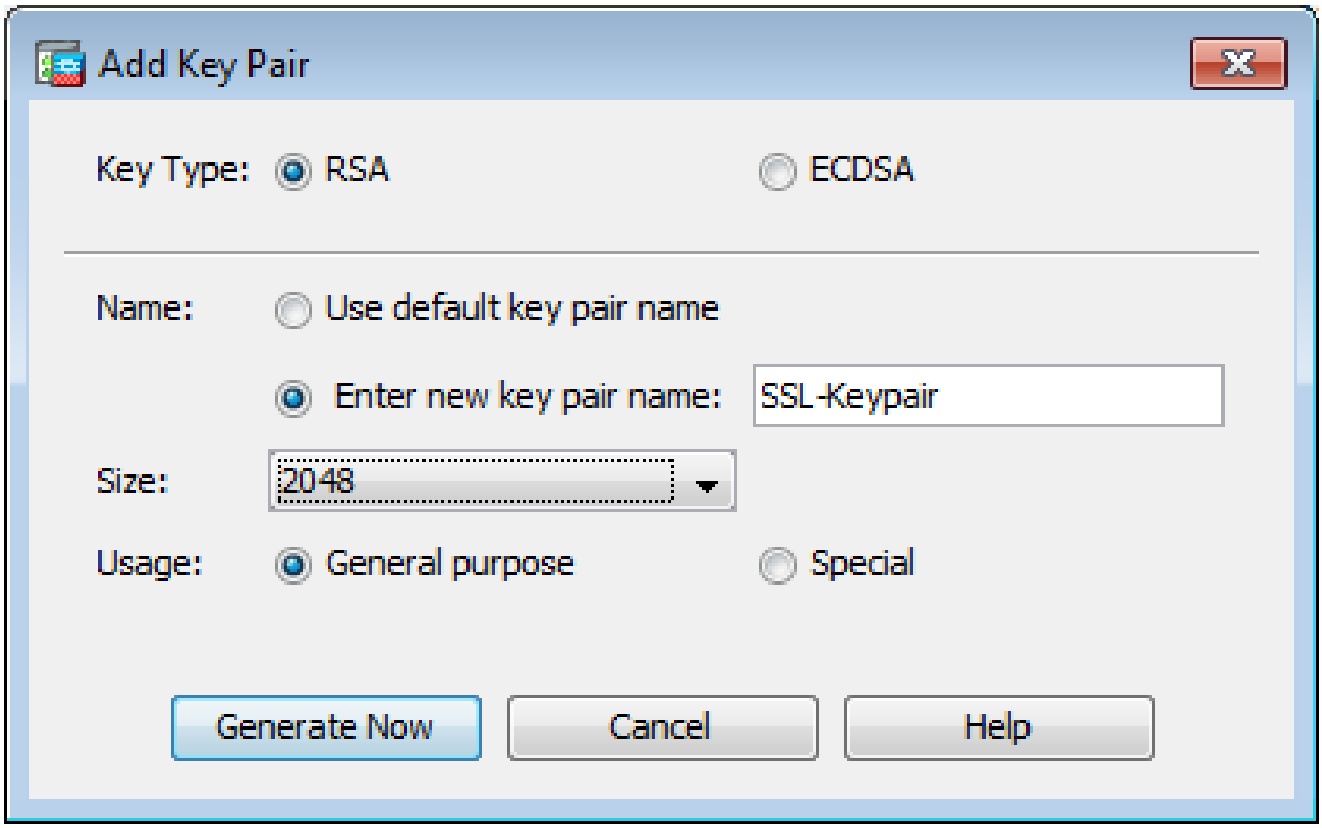
## 1. Configurare con ASDM

1. Passare a **Configuration** > **Remote Access VPN** > **Certificate Management** e scegliere **Identity Certificates**.

   - Fare clic su . **Add**



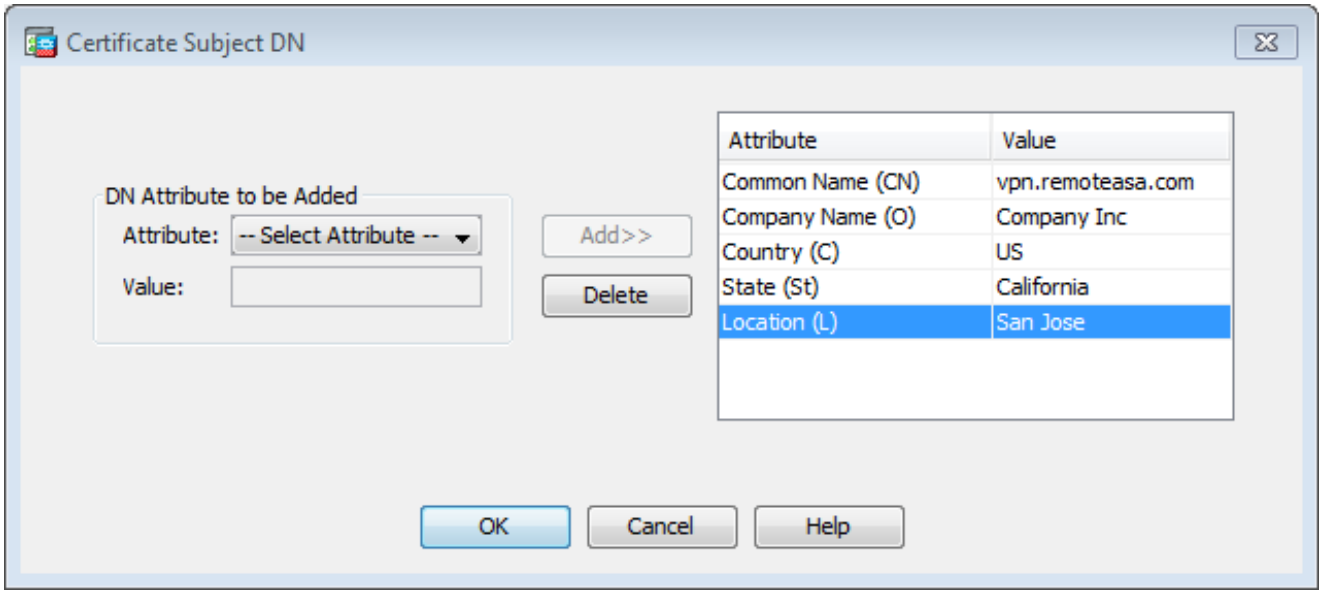

   - Definire un nome di trust nel campo di input Nome trust.
   - Fare clic sul pulsante **Add a new identity certificate**Audio.
   - Per la coppia di chiavi, fare**New** clic su.




- Scegliere il tipo di chiave: RSA o ECDSA. Per ulteriori informazioni sulle differenze, consultare l'Appendice A.
- Fare clic sul pulsante **Enter new key pair name**Audio. Identificare il nome della coppia di chiavi a scopo di riconoscimento.
- Scegliere il comando**Key Size**. **General Purpose for Usage** Scegliere RSA.
- Fare clic su .**Generate Now** Viene creata la coppia di chiavi.
- Per definire il DN del soggetto del certificato, fare**Select** clic su e configurare gli attributi elencati nella tabella seguente:

| 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 |

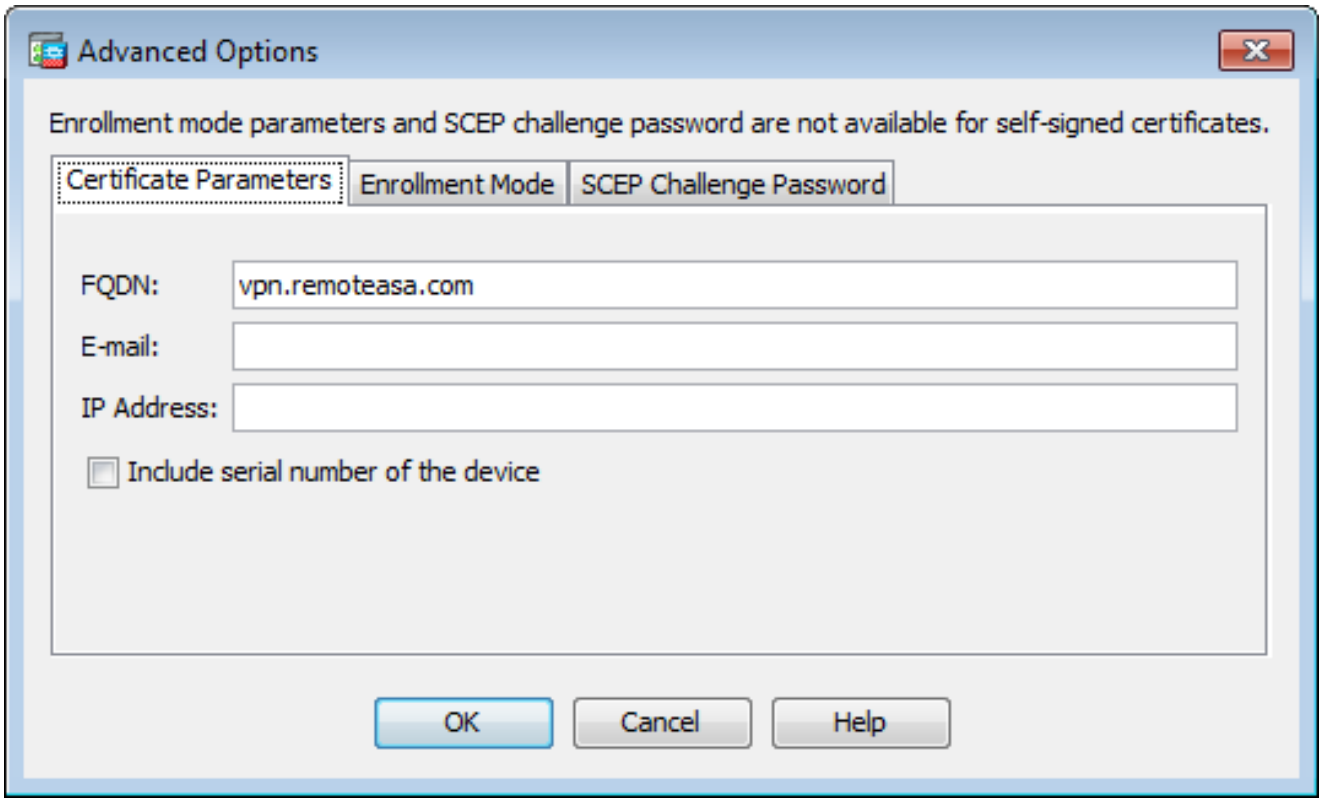
Per configurare questi valori, scegliere un valore dall'elenco a discesa **Attributo**, immettere il valore e fare clic su **Aggiungi**.




**Nota**: alcuni fornitori di terze parti richiedono l'inclusione di attributi specifici prima del rilascio di un certificato di identità. Se non si è certi degli attributi richiesti, contattare il fornitore per i dettagli.

- Dopo aver aggiunto i valori appropriati, fare clic**OK** su. Verrà visualizzata la finestra di dialogo Aggiungi certificato di identità con il certificato**Subject DN** field populated.

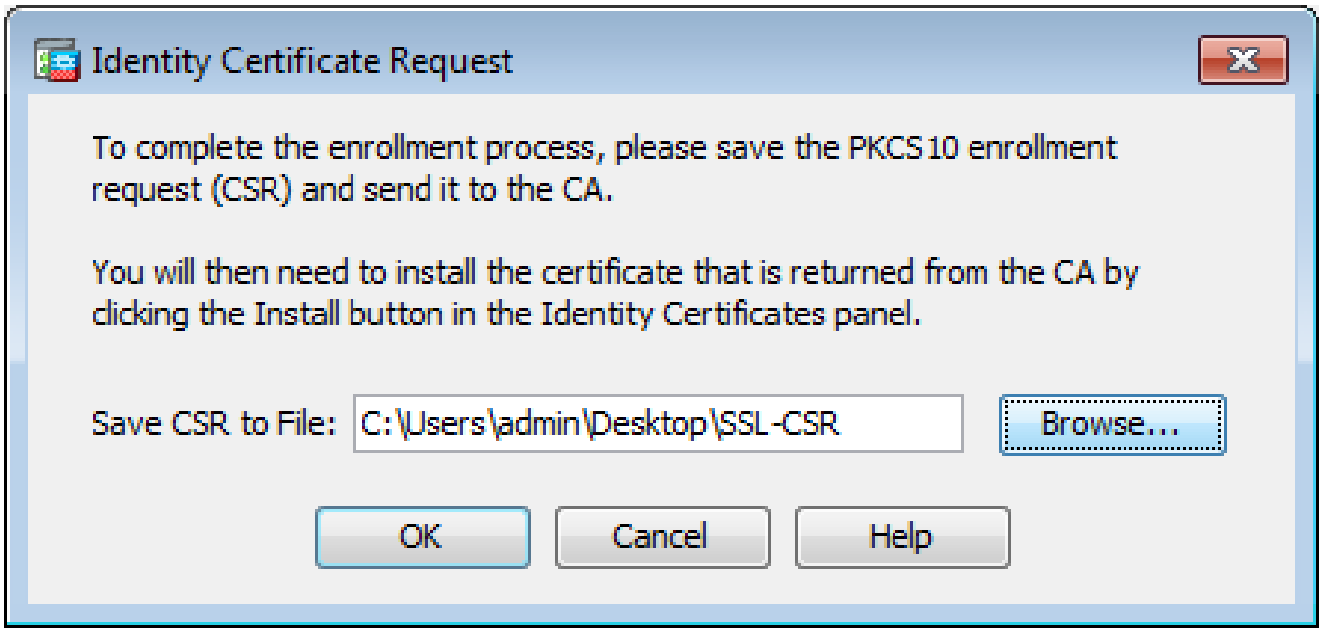
- Fare clic su **Avanzate**.




- Immettere **FQDN**nel campo il nome di dominio completo utilizzato per accedere al dispositivo da Internet. Fare clic su .**OK**

- Lasciare selezionata l'opzione Attiva flag CA nell'estensione dei vincoli di base. Per impostazione predefinita, i certificati senza il flag CA non possono essere installati sull'appliance ASA come certificati CA. L'estensione Limiti di base identifica se il soggetto del certificato è una CA e la profondità massima dei percorsi di certificazione validi che includono questo certificato. Deselezionare l'opzione per ignorare questo requisito.

- Fare**OK** clic su, quindi **Add Certificate.** su Viene visualizzato un prompt per salvare il CSR in un file nel computer locale.




- Fare**Browse** clic su, scegliere una posizione in cui salvare il CSR e salvare il file con estensione .txt.

**Nota**: quando il file viene salvato con estensione .txt, è possibile aprire e visualizzare la richiesta PKCS#10 con un editor di testo, ad esempio Blocco note.

2. Configurare con la CLI di ASA

In ASDM, il trust point viene creato automaticamente quando viene generato un CSR o quando viene installato il certificato CA. Nella CLI, il trust point deve essere creato manualmente.

<#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

**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 t

**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 b

**(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-----
MIIDDjCCAfYCAQAwgYkxETAPBgNVBAcTCFNhbiBKb3NlMRMwEQYDVQQIEwpDYWxp
Zm9ybmlhMQswCQYDVQQGEwJVUzEUMBIGA1UEChMLQ29tcGFueSBJbmMxGjAYBgNV
BAMTEXZwbi5yZW1vdGVhc2EuY29tMSAwHgYJKoZIhvcNAQkCFhF2cG4ucmVtb3Rl
YXNhLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK62Nhb9ktlK
uR3Q4TmksyuRMqJNrb9kXpvA6H2OOPuBfQvSF4rVnSwKOmu3c8nweEvYcdVWV6Bz
BhjXeovTVi17FlNTceaUTGikeIdXC+mw1iE7eRsynS/d4mzMWJmrvrsDNzpAW/EM
SzTca+BvqF7X2r3LU8Vsv6Oi8ylhco9Fz7bWvRWVtO3NDDbyolC9b/VgXMuBitcc
rzfUbVnm7VZDOf4jr9EXgUwXxcQidWEABlFrXrtYpFgBo9aqJmRp2YABQ1ieP4cY
3rBtgRjLcF+S9TvHG5m4v7v755meV4YqsZIXvytIOzVBihemVxaGA1oDwfkoYSFi
4CzXbFvdG6kCAwEAAaA/MD0GCSqGSIb3DQEJDjEwMC4wDgYDVR0PAQH/BAQDAgWg
MBwGA1UdEQQVMBOCEXZwbi5yZW1vdGVhc2EuY29tMA0GCSqGSIb3DQEBBQUAA4IB
AQBZuQzUXGEB0ix1yuPK0ZkRz8bPnwIqLTfxZhagmuyEhrN7N4+aQnCHj85oJane
4ztZDiCCoWTerBS4RSkKEHEspu9oohjCYuNnp5qa91SPrZNEjTWwOeRn+qKbId2J
jE6Qy4vdPCexavMLYVQxCny+gVkzPN/sFRk3EcTTVq6DxxaebpJijmiqa7gCph52
YkHXnFne1LQd41BgoLlCr9+hx74XsTHGBmI1s/9T5oAX26Ym+B2l/i/DP5BktIUA
8GvIY1/ypj9KO49fP5ap8al0qvLtYYcCcfwrCt+OojOrZ1YyJb3dFuMNRedAX37t
DuHNl2EYNpYkjVk1wI53/5w3
-----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. Utilizzare OpenSSL per generare il CSR

OpenSSL utilizza **OpenSSL config**il file per eseguire il pull degli attributi da utilizzare nella generazione CSR. Questo processo determina la generazione di un CSR e di una chiave privata.

---

⚠ **Attenzione**: verificare che la **chiave privata** generata non sia condivisa con altri utenti in quanto compromette l'integrità del certificato.

---

- Verificare che OpenSSL sia installato nel sistema in cui viene eseguito il processo. Per gli utenti Mac OSX e GNU/Linux, questa opzione è installata per impostazione predefinita.

- Passare a una directory funzionale.

In Windows: per impostazione predefinita, le utilità vengono installate in **C:\Openssl\bin**. Aprire un prompt dei comandi in questa posizione.

Su Mac OSX/Linux: aprire la finestra del terminale nella directory necessaria per creare il CSR.

- Creare un file di configurazione OpenSSL con un editor di testo con gli attributi specificati. Al termine, salvare il file come **openssl.cnf** nel percorso indicato nel passaggio precedente (se la versione è 0.9.8h e successive, il file è**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

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

[req_ext]

subjectAltName = @alt_names

[alt_names]

DNS.1 = *.remoteasa.com
```

- Generare la CSR e la chiave privata con questo comando:

**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]:
```

Inviare il CSR salvato al fornitore CA di terze parti. Una volta rilasciato il certificato, l'autorità di certificazione fornisce il certificato di identità e il certificato CA da installare sull'appliance ASA.

Generazione del certificato SSL sulla CA

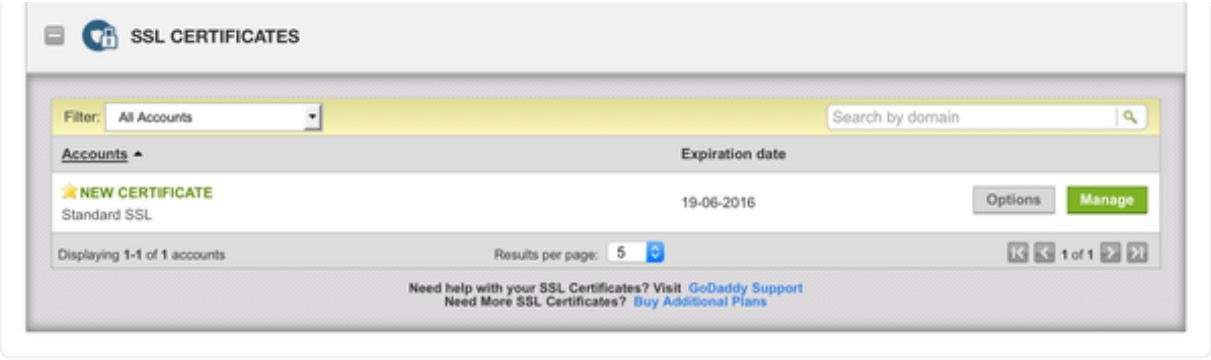
Il passo successivo è ottenere la firma del CSR dall'autorità di certificazione. L'autorità di certificazione fornisce un certificato di identità con codifica PEM appena generato oppure un certificato PKCS12 insieme al bundle del certificato CA.

Se il CSR viene generato all'esterno dell'ASA (tramite OpenSSL o sulla CA stessa), il certificato di identità con codifica PEM con la chiave privata e il certificato CA sono disponibili come file separati. L'Appendice B fornisce i passaggi per raggruppare questi elementi in un unico file PKCS12 (formato .p12 o .pfx).

In questo documento, l'autorità di certificazione GoDaddy viene usata come esempio per rilasciare i certificati di identità all'appliance ASA. Questo processo è diverso negli altri fornitori CA.Leggere attentamente la documentazione dell'autorità di certificazione prima di procedere.

Esempio di generazione di un certificato SSL su una CA di GoDaddy

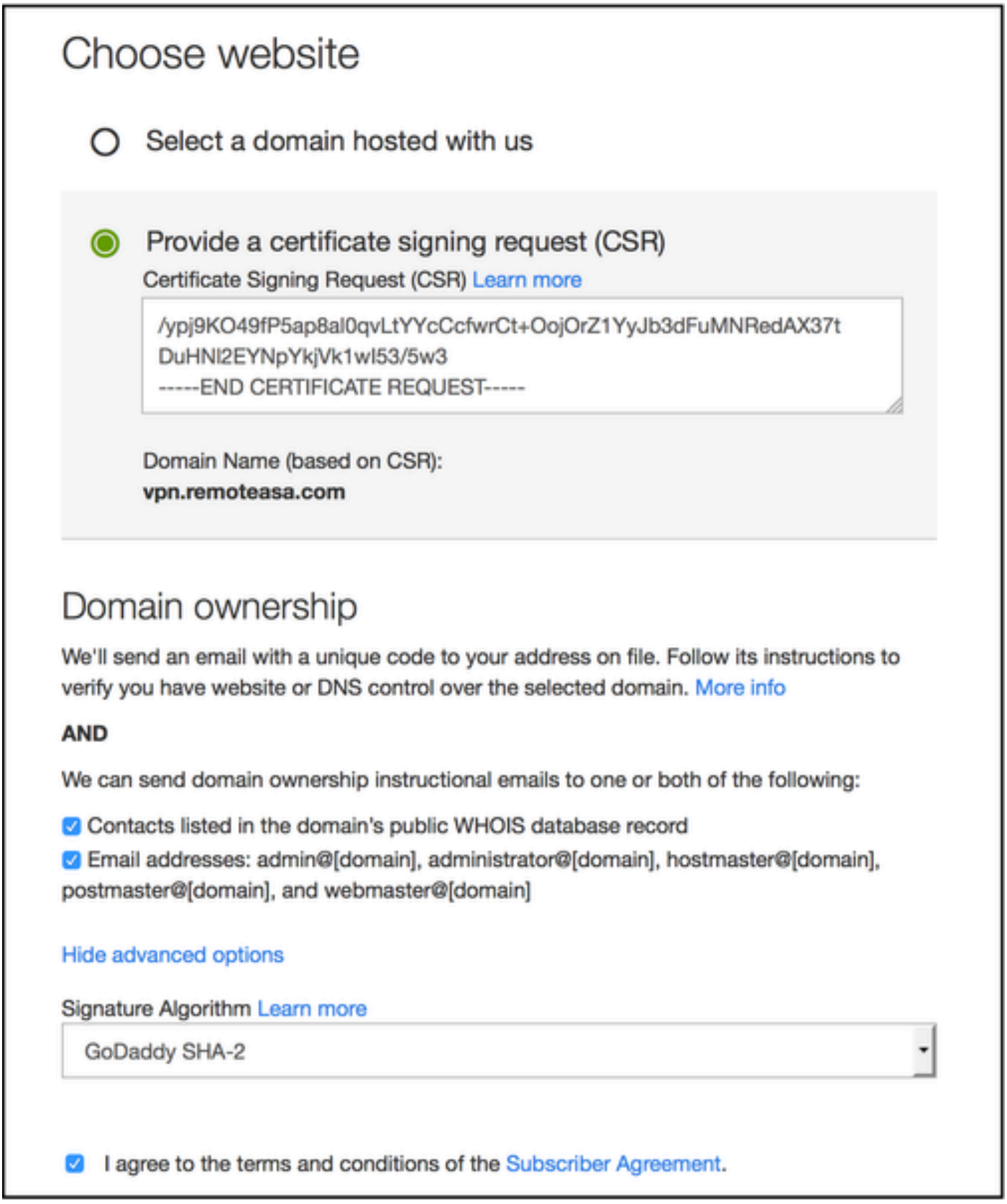
Dopo l'acquisto e la fase di configurazione iniziale del certificato SSL, passare all'account GoDaddy e visualizzare i certificati SSL. Deve essere presente un nuovo certificato. **Manage** Fare clic per continuare.




Verrà visualizzata una pagina in cui è disponibile il CSR illustrato nell'immagine.

In base al CSR immesso, la CA determina il nome di dominio a cui deve essere rilasciato il certificato.

Verificare che corrisponda all'FQDN dell'ASA.

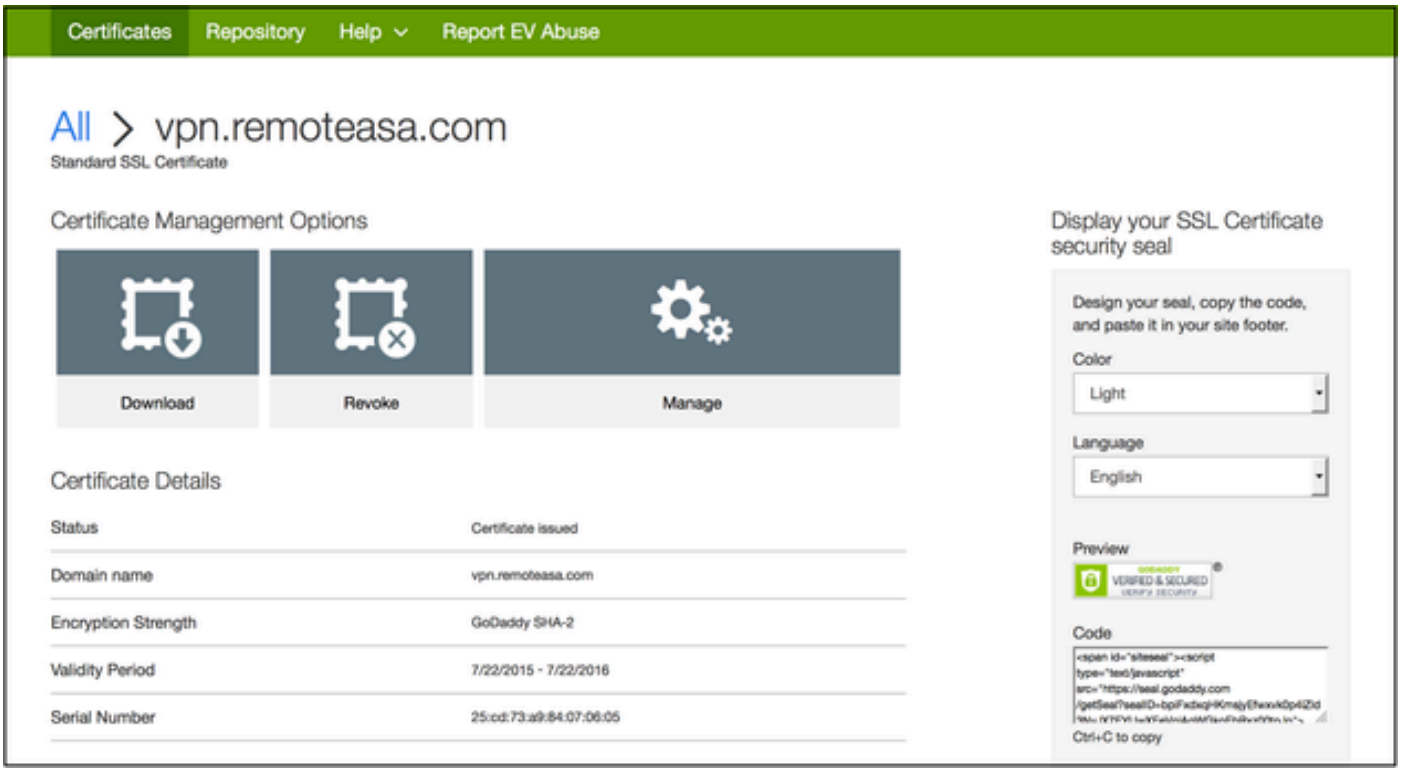



**Nota**: GoDaddy e la maggior parte delle altre CA utilizzano SHA-2 o SHA256 come algoritmo di firma del certificato predefinito. ASA supporta l'algoritmo di firma SHA-2 che inizia dalla versione **8.2(5)** [versioni precedenti alla 8.3] e dalla versione **8.4(1)** [versioni successive alla 8.3] in avanti (ID bug Cisco CSCti30937 ). Scegliere l'algoritmo di firma SHA-1 se viene utilizzata una versione precedente alla 8.2(5) o alla 8.4(1).

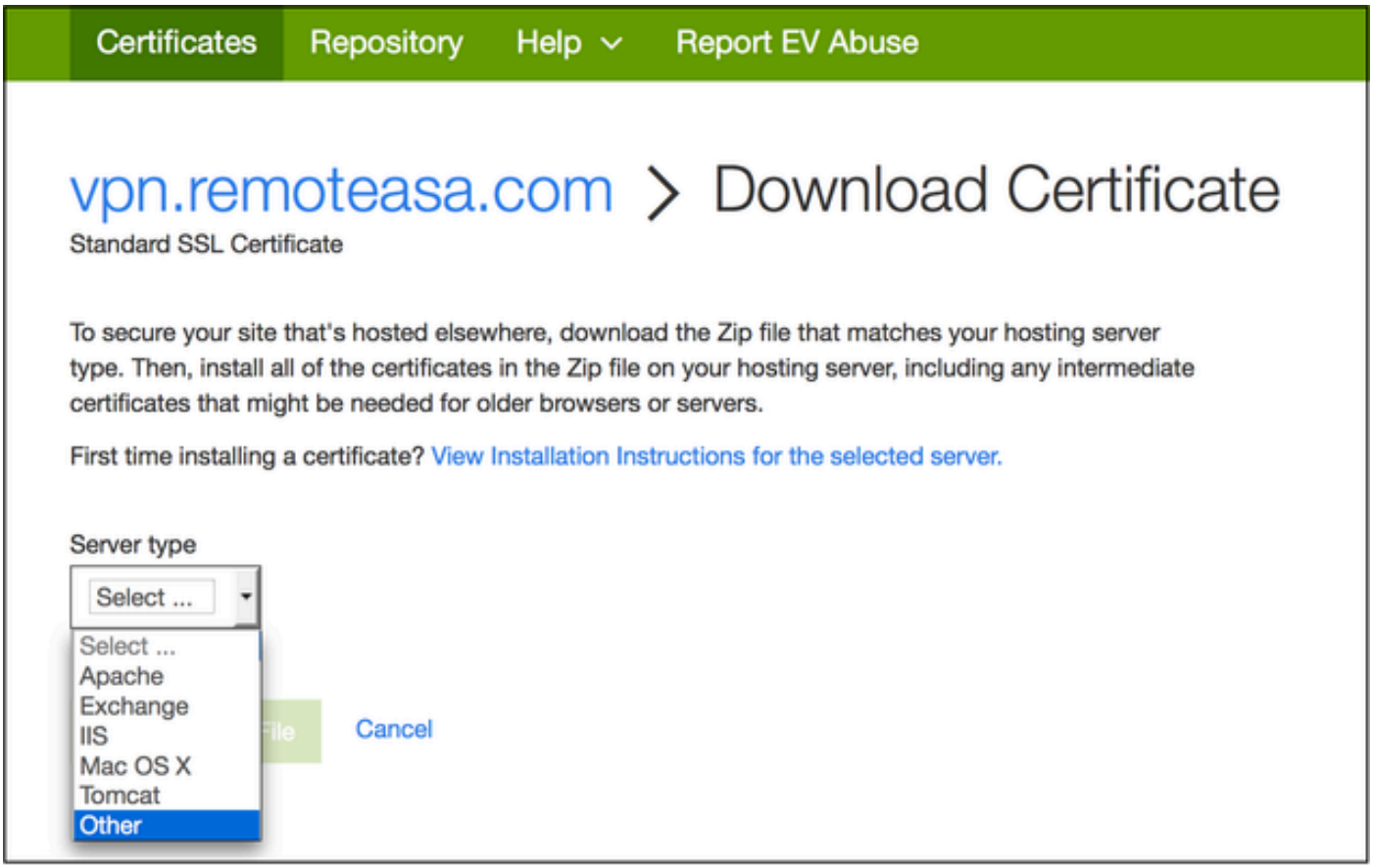
Una volta inviata la richiesta, GoDaddy la verifica prima di rilasciare il certificato.

Dopo la convalida della richiesta di certificato, GoDaddy rilascia il certificato all'account.

Il certificato può quindi essere scaricato per l'installazione sull'appliance ASA. **Download** Fare clic sulla pagina per continuare.




**Other** Scegliere il tipo di server e scaricare il pacchetto zip del certificato.




Il file .zip contiene il certificato di identità e i bundle della catena di certificati CA GoDaddy come due file .crt separati. Procedere

all'installazione del certificato SSL per installare questi certificati sull'appliance ASA.

Installazione del certificato SSL sull'appliance ASA

Il certificato SSL può essere installato sull'appliance ASA con ASDM o CLI in due modi:

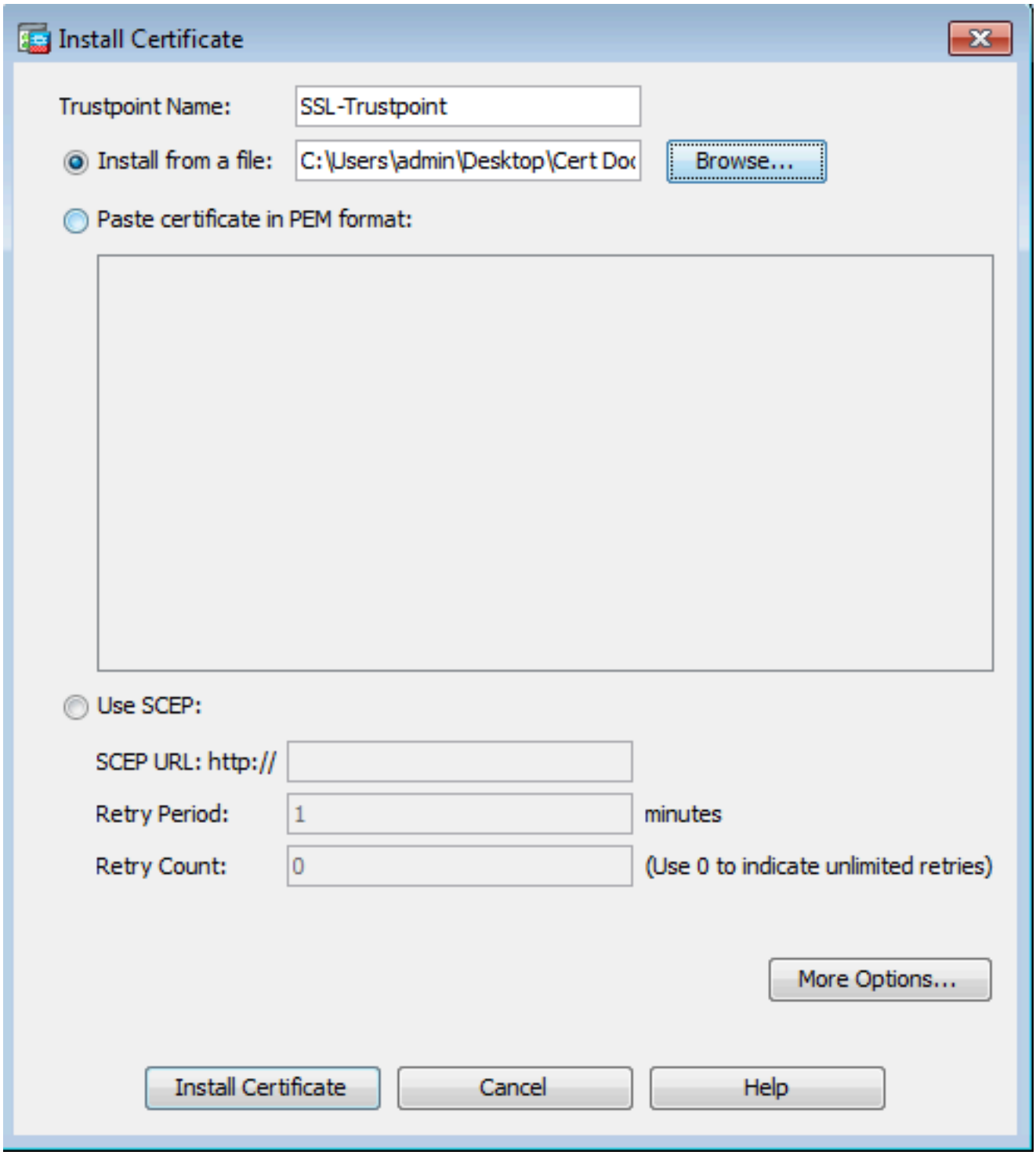
- Importare la CA e il certificato di identità separatamente nei formati PEM.
- In alternativa, importare il file PKCS12 (codifica base64 per CLI) in cui il certificato di identità, il certificato CA e la chiave privata sono inclusi nel file PKCS12.

**Nota**: se la CA fornisce una catena di certificati CA, installare solo il certificato CA intermedio immediato nella gerarchia del trust point utilizzato per generare il CSR. Il certificato CA radice e tutti gli altri certificati CA intermedi possono essere installati in nuovi trust point.

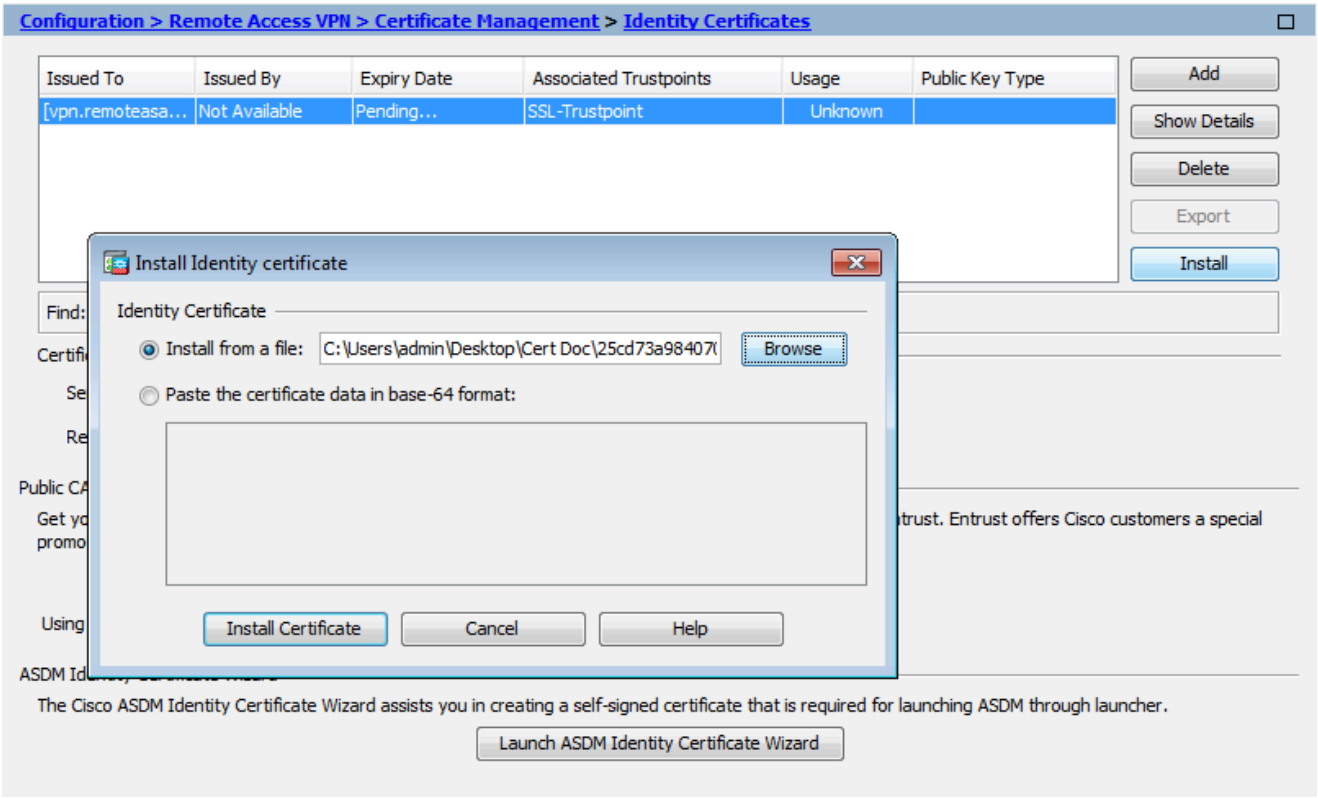
1.1 Installazione del certificato di identità in formato PEM con ASDM

Le procedure di installazione fornite presuppongono che la CA fornisca un certificato di identità con codifica PEM (.pem, .cer, .crt) e un bundle di certificati CA.

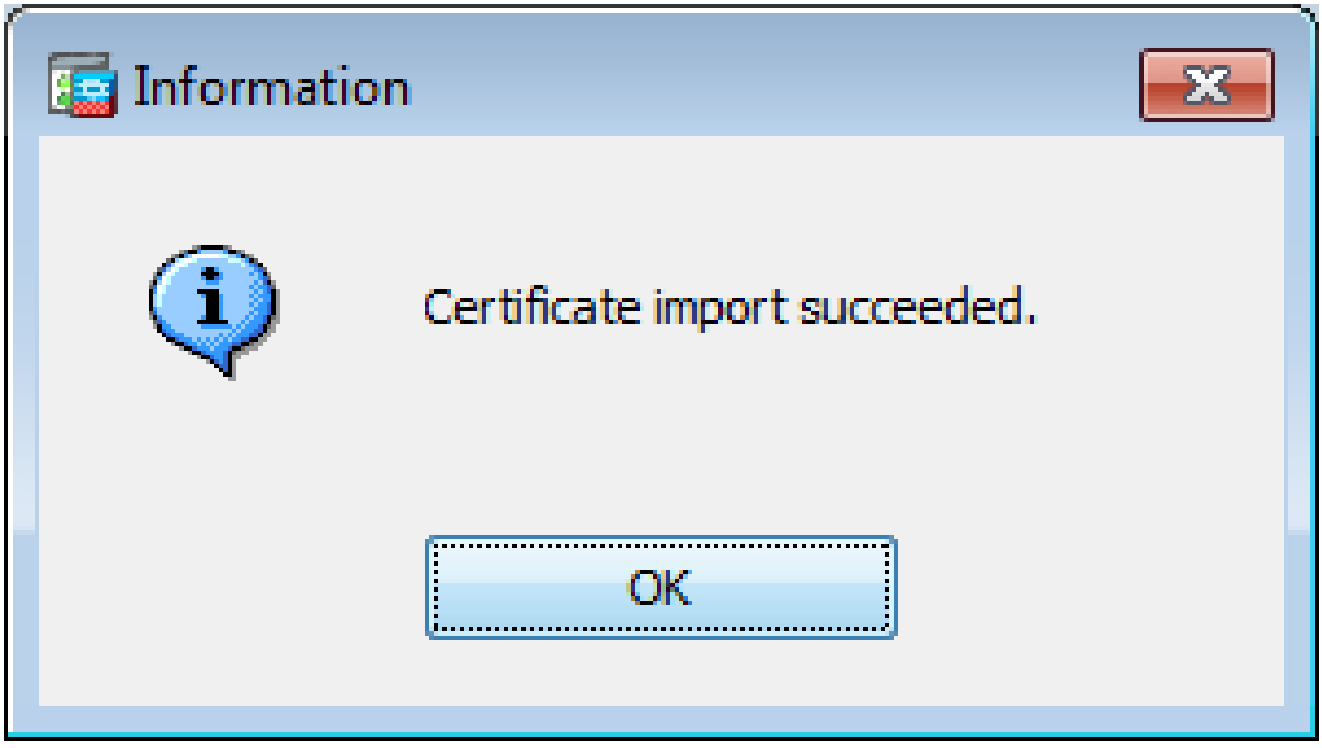
- Passare **Configuration > Remote Access VPN > Certificate Management** a Certificati CA e scegliere Certificati CA.
- Il certificato codificato PEM in un editor di testo e copiare e incollare nel campo di testo il certificato CA base64 fornito dal fornitore di terze parti.




- Fare clic su **Installa certificato**.
- Passare**Configuration > Remote Access VPN > Certificate Management** a Certificati identità e scegliere Certificati identità.
- Selezionare il certificato di identità creato in precedenza. Fare clic su . **Install**
- Fare clic sul pulsante di opzione **Install from a file** Opzione e scegliere il certificato di identità con codifica PEM oppure aprire il certificato con codifica PEM in un editor di testo e copiare e incollare il certificato di identità base64 fornito dal fornitore di terze parti nel campo di testo.

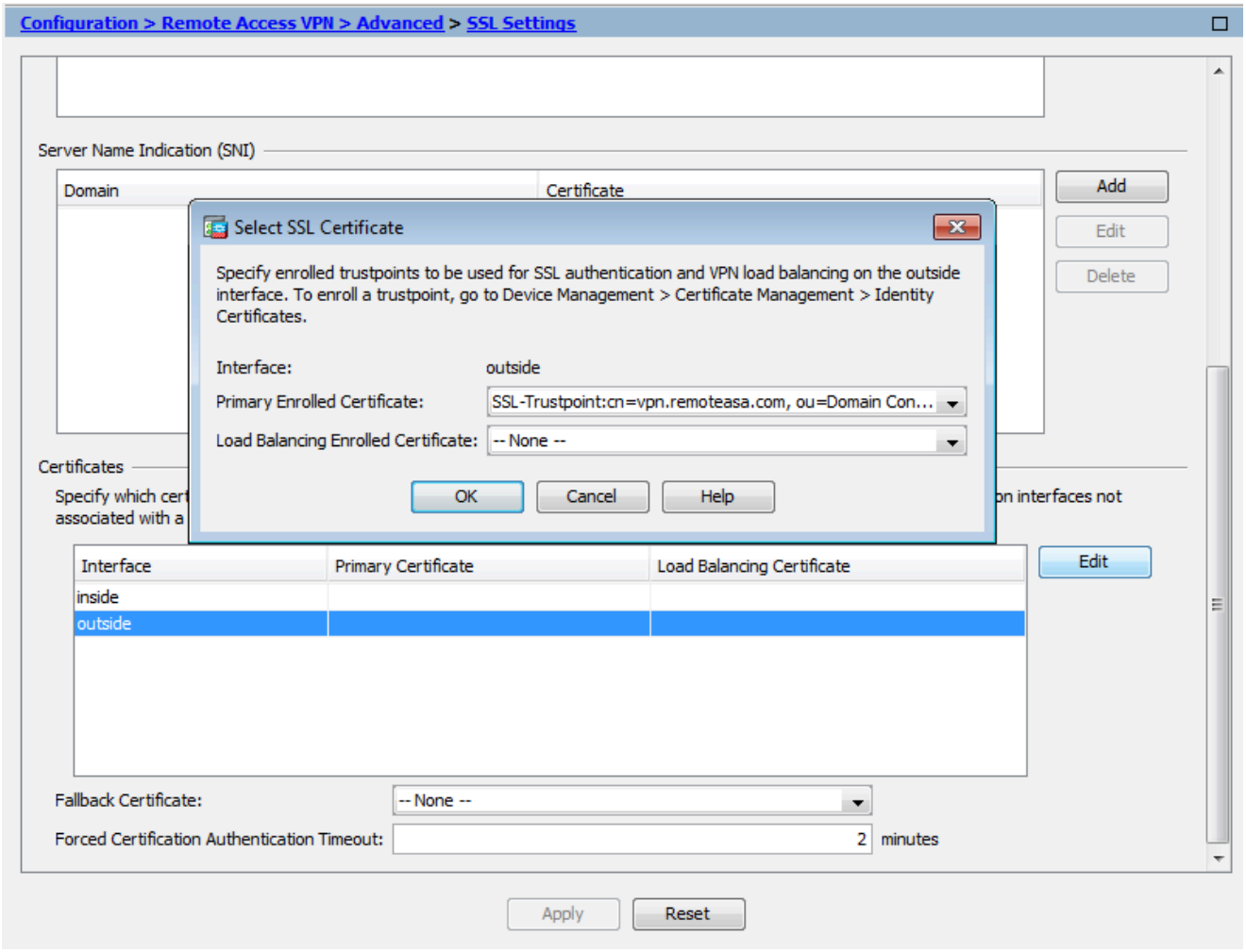



- Fare clic su .**Add Certificate**




- Passare**Configuration > Remote Access VPN > Advanced > SSL Settings** a.
- In Certificati selezionare l'interfaccia utilizzata per terminare le sessioni WebVPN. nell'esempio viene usata l'interfaccia esterna.
- Fare clic su .**Edit**

- Nell'elenco a discesa Certificato e scegliere il certificato appena installato.




- Fare clic su .**OK**
- Fare clic su .**Apply** Il nuovo certificato è ora utilizzato per tutte le sessioni WebVPN che terminano sull'interfaccia specificata.

1.2. Installazione di un certificato PEM con la CLI

<#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----- MIIEADCCAuigAwIBAgIBADANBgkqhkiG9w0BAQUFADBjMQswCQYDVQQGEwJVUzEh MB8GA1UEChM

**!!! - 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+cVMA0GCSqGSIb3DQEBCwUAMGMxCzAJBgNVBAYTAlVT
MSEwHwYDVQQKExhUaGUgR28gRGFkZHkgR3JvdXAsIEluYy4xMTAvBgNVBAsTKEdv
IERhZGR5IENsYXNzIDIgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNMTQwMTAx
MDcwMDAwWhcNMzEwNTMwMDcwMDAwWjCBgzELMAkGA1UEBhMCVVMxEDAOBgNVBAgT
B0FyaXpvbmExEzARBgNVBAcTClNjb3R0c2RhbGUxGjAYBgNVBAoTEUdvRGFkZHku
Y29tLCBJbmMuMTEwLwYDVQQDEyhHbyBEYWRkeSBSb290IENlcnRpZmljYXRlIEF1
dGhvcml0eSAtIEcyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAv3Fi
CPH6WTT3G8kYo/eASVjpIoMTpsUgQwE7hPHmhUmfJ+r2hBtOoLTbcJjHMgGxBT4H
Tu70+k8vWTAi56sZVmvigAf88xZ1gDlRe+X5NbZ0TqmNghPktj+pA4P6or6KFWp/
3gvDthkUBcrqw6gElDtGfDIN8wBmIsiNaW02jBEYt9OyHGC0OPoCjM7T3UYH3go+
6118yHz7sCtTpJJiaVElBWEaRIGMLKlDliPfrDqBmg4pxRyp6V0etp6eMAo5zvGI
gPtLXcwy7IViQyU0AlYnAZG0O3AqP26x6JyIAX2f1PnbU21gnb8s51iruF9G/M7E
GwM8CetJMVxpRrPgRwIDAQABo4IBFzCCARMwDwYDVR0TAQH/BAUwAwEB/zAOBgNV
HQ8BAf8EBAMCAQYwHQYDVR0OBBYEFDqahQcQZyi27/a9BUFuIMGU2g/eMB8GA1Ud
IwQYMBaAFNLEsNKR1EwRcbNhyz2h/t2oatTjMDQGCCsGAQUFBwEBBCgwJjAkBggr
BgEFBQcwAYYYaHR0cDovL29jc3AuZ29kYWRkeS5jb20vMDIGA1UdHwQrMCkwJ6Al
oCOGIWh0dHA6Ly9jcmwuZ29kYWRkeS5jb20vZ2Ryb29LmNybDBGBgNVHSAEPzA9
MDsGBFUdIAAwMzAxBggrBgEFBQcCARYlaHR0cHM6Ly9jZXJ0cy5nb2RhZGR5LmNv
bS9yZXBvc2l0b3J5LzANBgkqhkiG9w0BAQsFAAOCAQEAWQtTvZKGEacke+1bMc8d
H2xwxbhuvk679r6XUOEwf7ooXGKUwuN+M/f7QnaF25UcjCJYdQkMiGVnOQoWCcWg
OJekxSOTP7QYpgEGRJHjp2kntFolfzq3Ms3dhP8qOCkzpN1nsoX+oYggHFCJyNwq
9kIDN0zmiN/VryTyscPfzLXs4JletOlUIDyUGAzHHFIYSaRt4bNYC8nY7NmuHDKO
KHAN4v6mF56ED71XcLNa6R+ghlO773z/aQvgSMO3kwvIClTErF0UZzdsyqUvMQg3
qm5vjLyb4lddJIGvl5echK1srDdMZvNhkREg5L4wn3qkKQmw4TRfZHcYQFHfjDCm
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-----
MIIFRjCCBC6gAwIBAgIIJc1zqYQHBgUwDQYJKoZIhvcNAQELBQAwgbQxCzAJBgNV
BAYTAlVTMRAwDgYDVQQIEwdBcml6b25hMRMwEQYDVQQHEwpTY29OdHNkYWxlMRow
GAYDVQQKExFHb0RhZGR5LmNvbSwgSW5jLjEtMCsGA1UECxMkaHR0cDovL2NlcnRz
LmdvZGFkZHkuY29tL3JlcG9zaXRvcnkvMTMwMQYDVQQDEypHbyBEYWRkeSBTZWN1
cmUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5IC0gRzIwHhcNMTUwNzIyMTIwNDM4WhcN
MTYwNzIyMTIwNDM4WjA/MSEwHwYDVQQLExhEb21haW4gQ29udHJvbCBWYWxpZGF0
ZWQxGjAYBgNVBAMTEXZwbi5yZW1vdGVhc2EuY29tMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEArrY2Fv2S2Uq5HdDhOaSzK5Eyok2tv2Rem8DofbTQ+4F9
C9IXitWdLAo6a7dzyfB4S9hx1VZXoHMGGNd6i9NWLXsWU1Nx5pRMaKR4h1cL6bDW
ITt5GzKdL93ibMxYmau+uwM3OkBb8QxLNNxr4G+oXtfavctTxWy/o6LzKWFyj0XP
tta9FZWO7cOMNvKiUL1v9WBcy4GK1xyvN9RtWebtVkM5/iOv0ReBTBfFxCJ1YQAG
UWteu1ikWAGj1qomZGnZgAFDWJ4/hxjesG2BGMtwX5L1O8cbmbi/u/vnmZ5Xhiqx
<snip>
CCsGAQUFBwIBFitodHRwOi8vY2VydGlmaWNhdGVzLmdvZGFkZHkuY29tL3JlcG9z
aXRvcnkvMHYGCCsGAQUFBwEBBGowaDAkBggrBgEFBQcwAYYYaHR0cDovL29jc3Au
Z29kYWRkeS5jb20vMEAGCCsGAQUFBzAChjRodHRwOi8vY2VydGlmaWNhdGVzLmdv
ZGFkZHkuY29tL3JlcG9zaXRvcnkvZ2RpZzIuY3J0MB8GA1UdIwQYMBaAFEDCvSeO
zDSDMKIz1/tss/C0LIDOMEYGA1UdEQQ/MD2CEXZwbi5yZW1vdGVhc2EuY29tghV3
d3cudnBuLnJlbW9OZWFzYS5jb22CEXZwbi5yZW1vdGVhc2EuY29tMB0GA1UdDgQW
BBT7en7YS3PH+s4z+wTRlpHr2tSzejANBgkqhkiG9w0BAQsFAAOCAQEAO9H8TLNx
2YOrYdI6gS8n4imaSYg9Ni/9Nb6mote3J2LELG9HY9m/zUCR5yVktra9azdrNUAN
1hjBJ7kKQScLC4sZLONdqG1uTP5rbWROyikF5wSzgyMWd03kOR+vM8q6T57vRst5
69vzBUuJc5bSu1IjyfPP19z1l+B2eBwUFbVfXLnd9bTfiG9mSmC+4V63TXFxt1Oq
xkGNys3GgYuCUy6yRP2cAUV1lc2tYtaxoCL8yo72YUDDgZ3a4PyO1EvC1FOaUtgv
6QNEOYwmbJkyumdPUwko6wGOC0WLumzv5gHnhil68HYSZ/4XIlp3B9Y8yfG5pwbn
7puhazH+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 Installazione di un certificato PKCS12 con ASDM

Nei casi in cui la CSR non viene generata sull'appliance ASA, come nel caso di un certificato con caratteri jolly o quando viene generato un certificato UC, un certificato di identità e la chiave privata vengono ricevuti come file separati o come un singolo file PKCS12 (formato .p12 o pfx). Per installare questo tipo di certificato, attenersi alla seguente procedura.

- Il certificato di identità riunisce il certificato CA e la chiave privata in un unico file PKCS12. L'Appendice B illustra la procedura da seguire a tale scopo con OpenSSL. Se già fornito in bundle dalla CA, procedere al passaggio successivo.

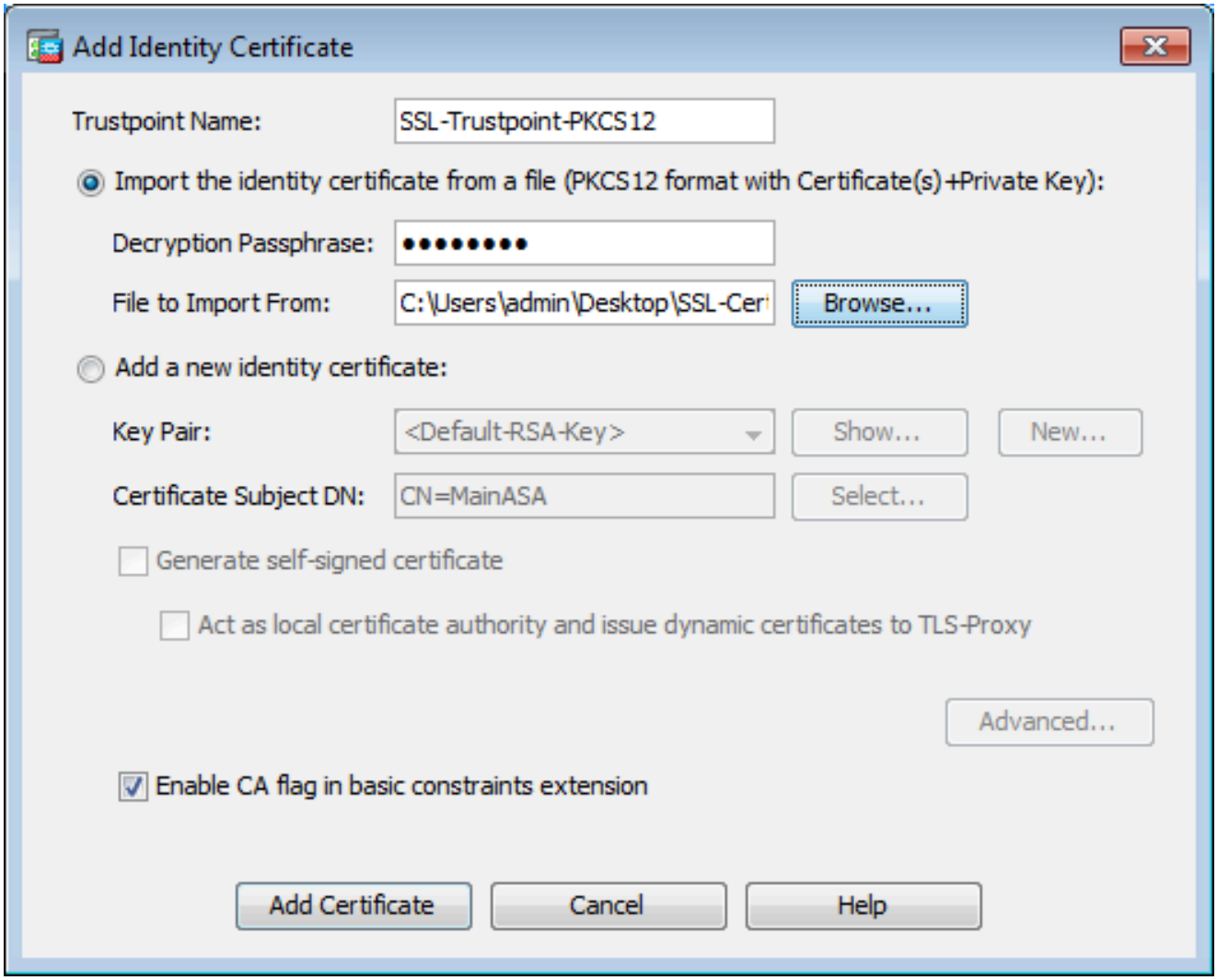
- Naviga **Configuration > Remote Access VPN > Certificate Management,** e scegli **Identity Certificates.**

- Fare clic su .**Add**

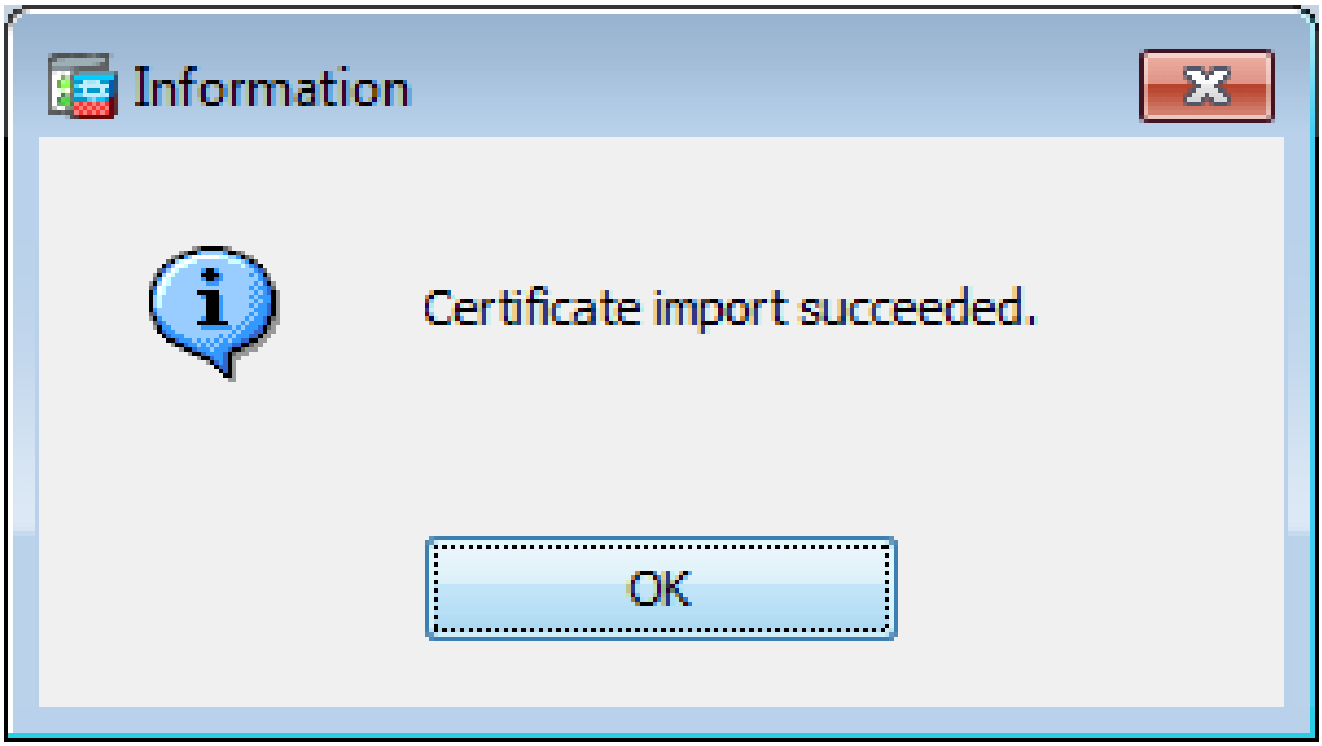
- Specificare il nome di un Trustpoint.

- Fare clic sul pulsante **Import the identity certificate from a file**di opzione.

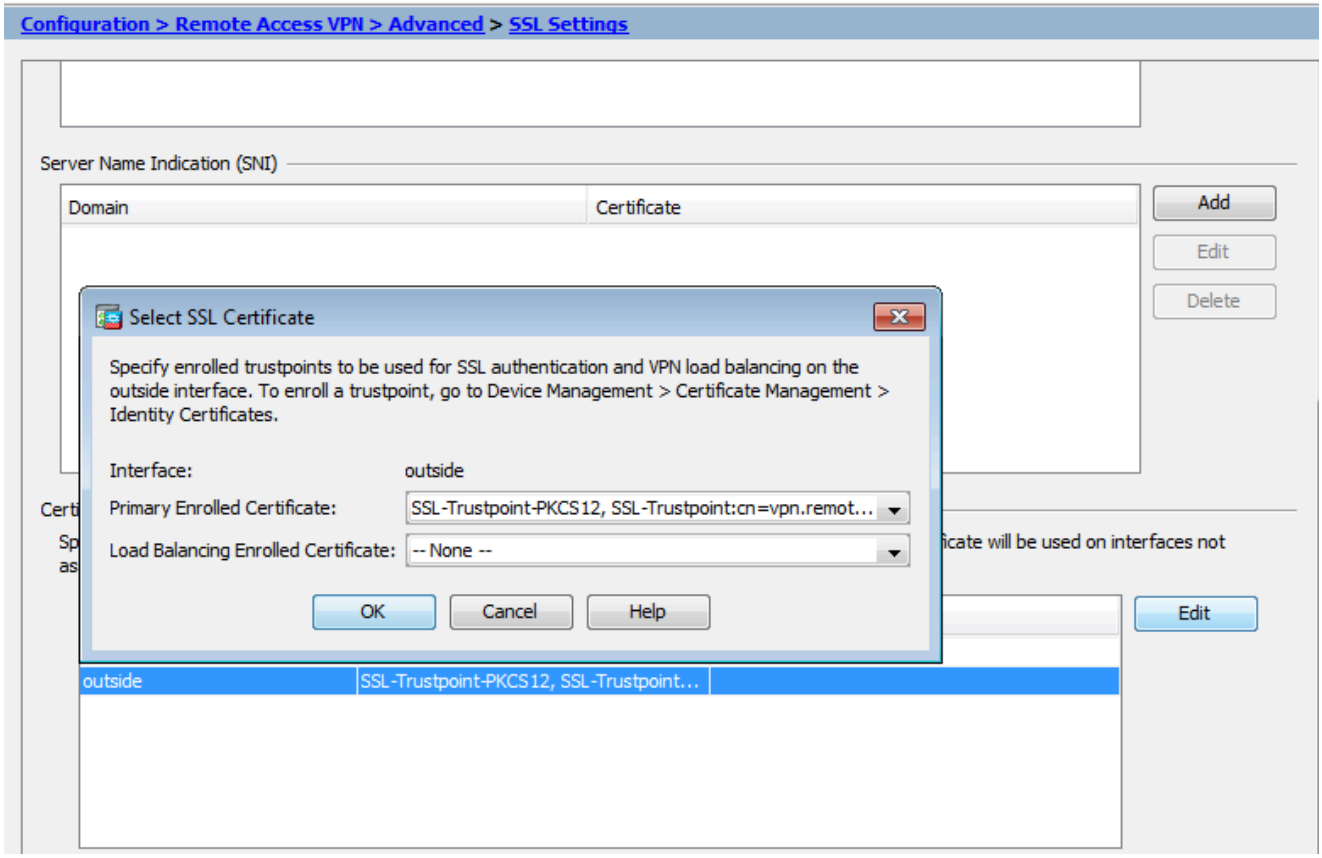
- Immettere la passphrase utilizzata per creare il file PKCS12. Individuare e selezionare il file PKCS12. Immettere la passphrase del certificato.




- Fare clic su **Aggiungi certificato**.




- Individuare**Configuration > Remote Access VPN > Advanced** e scegliere **SSL Settings.**
- In Certificati scegliere l'interfaccia utilizzata per terminare le sessioni WebVPN. nell'esempio viene usata l'interfaccia esterna.
- Fare clic su .**Edit**
- Nell'elenco a discesa Certificato scegliere il certificato appena installato.



- Fare clic su .**OK**
- Fare clic su .**Apply** Il nuovo certificato è ora utilizzato per tutte le sessioni WebVPN che terminano sull'interfaccia specificata.

2.2 Installazione di un certificato PKCS12 con la CLI

<#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-----

**INFO: Import PKCS12 operation completed successfully**

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

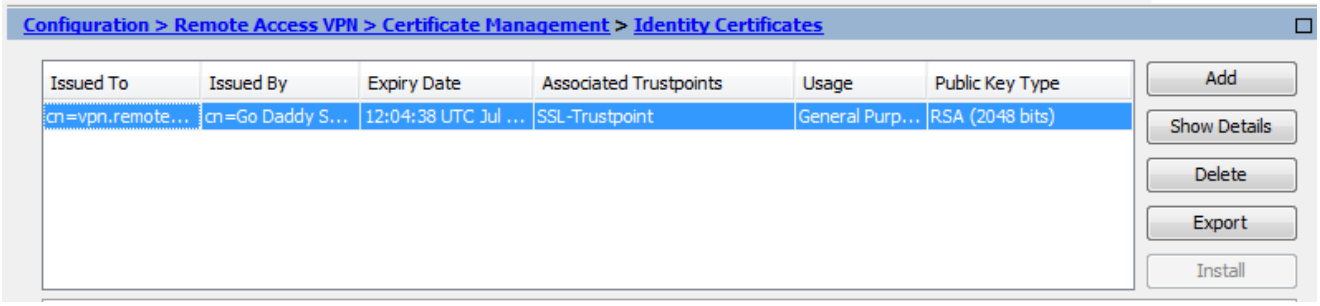
**ssl trust-point SSL-Trustpoint-PKCS12 outside**

Verifica

Utilizzare questa procedura per verificare la corretta installazione del certificato del fornitore di terze parti e utilizzarlo per le connessioni SSLVPN.

Visualizza certificati installati tramite ASDM

- Naviga **Configuration > Remote Access VPN > Certificate Management,**e scegli **Identity Certificates.**
- Viene visualizzato il certificato di identità rilasciato dal fornitore di terze parti.




Visualizzazione dei certificati installati tramite CLI

<#root>

MainASA(config)#

**show crypto ca certificate**

**Certificate**

Status: Available Certificate Serial Number: 25cd73a984070605 Certificate Usage: General Purpose Publi

**SSL-Trustpoint**

**CA Certificate**

Status: Available Certificate Serial Number: 07 Certificate Usage: General Purpose Public Key Type: RS

**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:
```

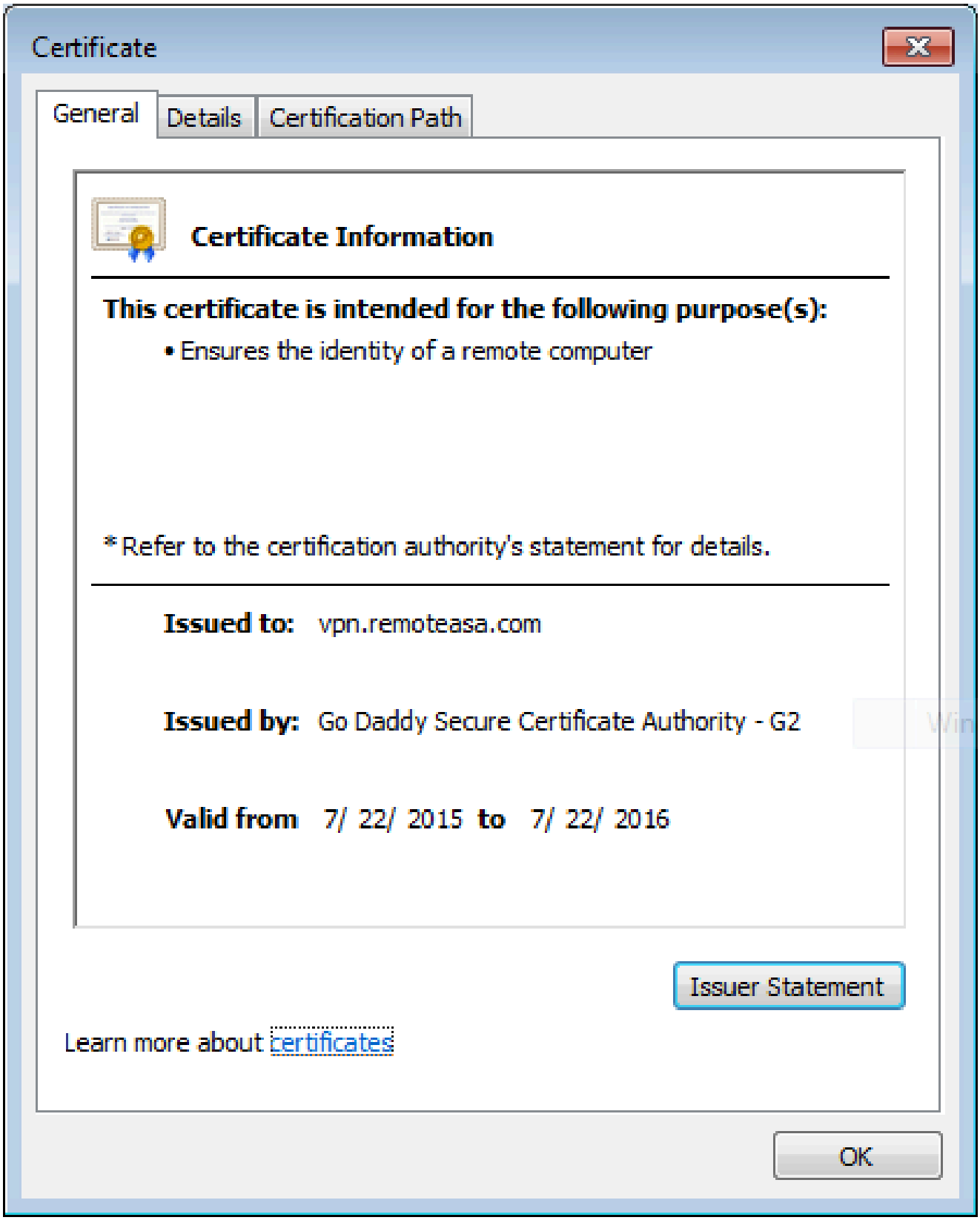
**SSL-Trustpoint-1**

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

Verifica del certificato installato per WebVPN con un browser Web

Verificare che WebVPN utilizzi il nuovo certificato.

- Connettersi all'interfaccia WebVPN tramite un browser Web. Utilizzare https:// insieme all'FQDN utilizzato per richiedere il certificato, ad esempio https://(vpn.remoteasa.com)).
- Fare doppio clic sull'icona del lucchetto visualizzata nell'angolo inferiore destro della pagina di accesso di WebVPN. È necessario visualizzare le informazioni sul certificato installato.
- Controllare il contenuto per verificare che corrisponda al certificato rilasciato dal fornitore di terze parti.



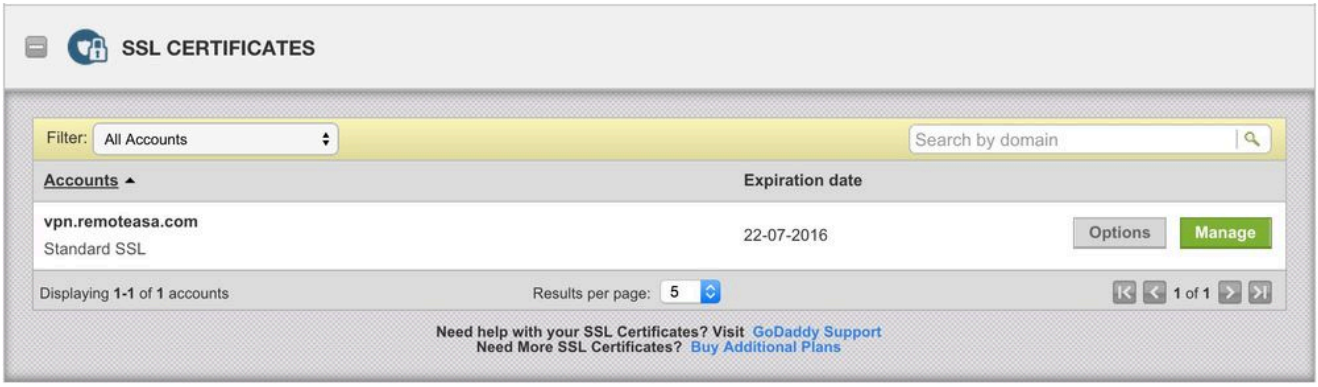

Rinnovo del certificato SSL sull'appliance ASA

- Rigenerare il CSR sull'appliance ASA, su OpenSSL o sulla CA con gli stessi attributi del vecchio certificato. Eseguire i passaggi descritti in Generazione di CSR.

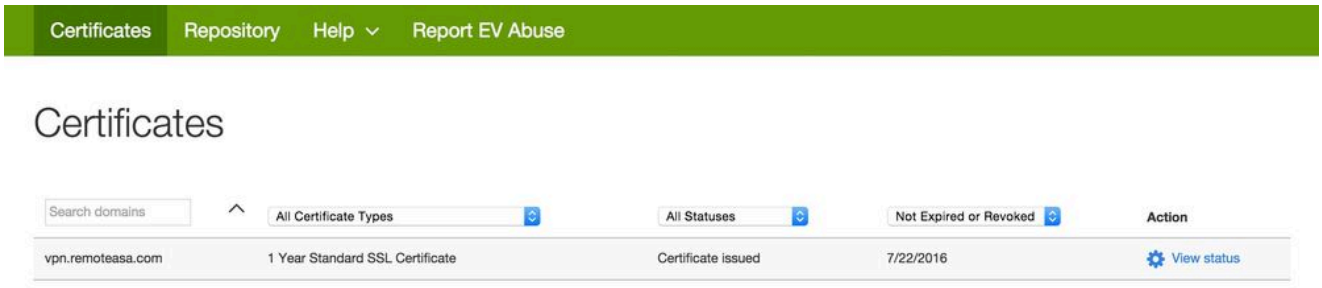
• Inviare il CSR nella CA e generare un nuovo certificato di identità in formato PEM (.pem, .cer, .crt) insieme al certificato CA. Nel caso di un certificato PKCS12 è inoltre disponibile una nuova chiave privata.

Nel caso di una CA di GoDaddy, è possibile reimpostare la chiave del certificato con un nuovo CSR generato.

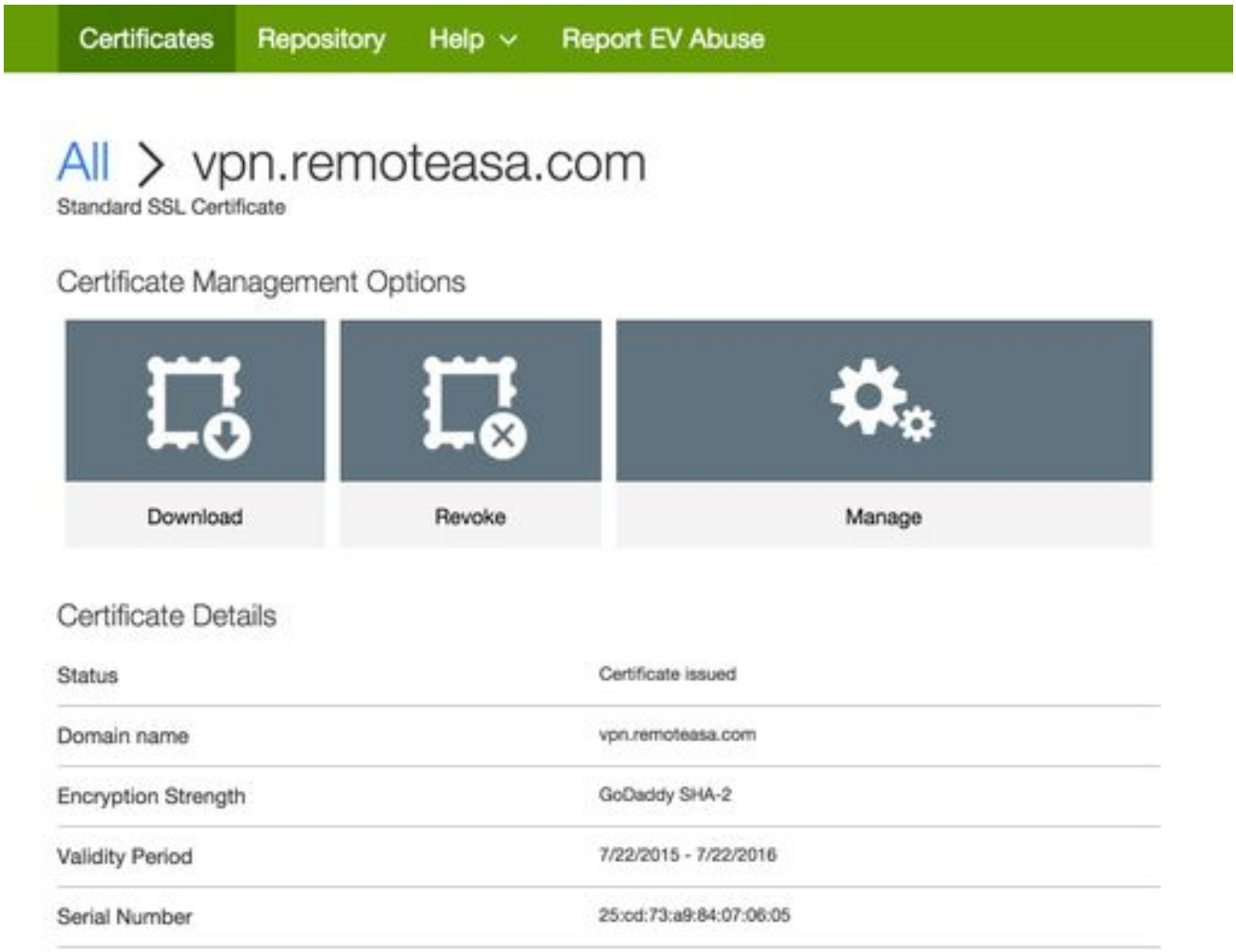
Accedere all'account GoAddyaccount e fare clic su **Gestisci** in Certificati SSL.



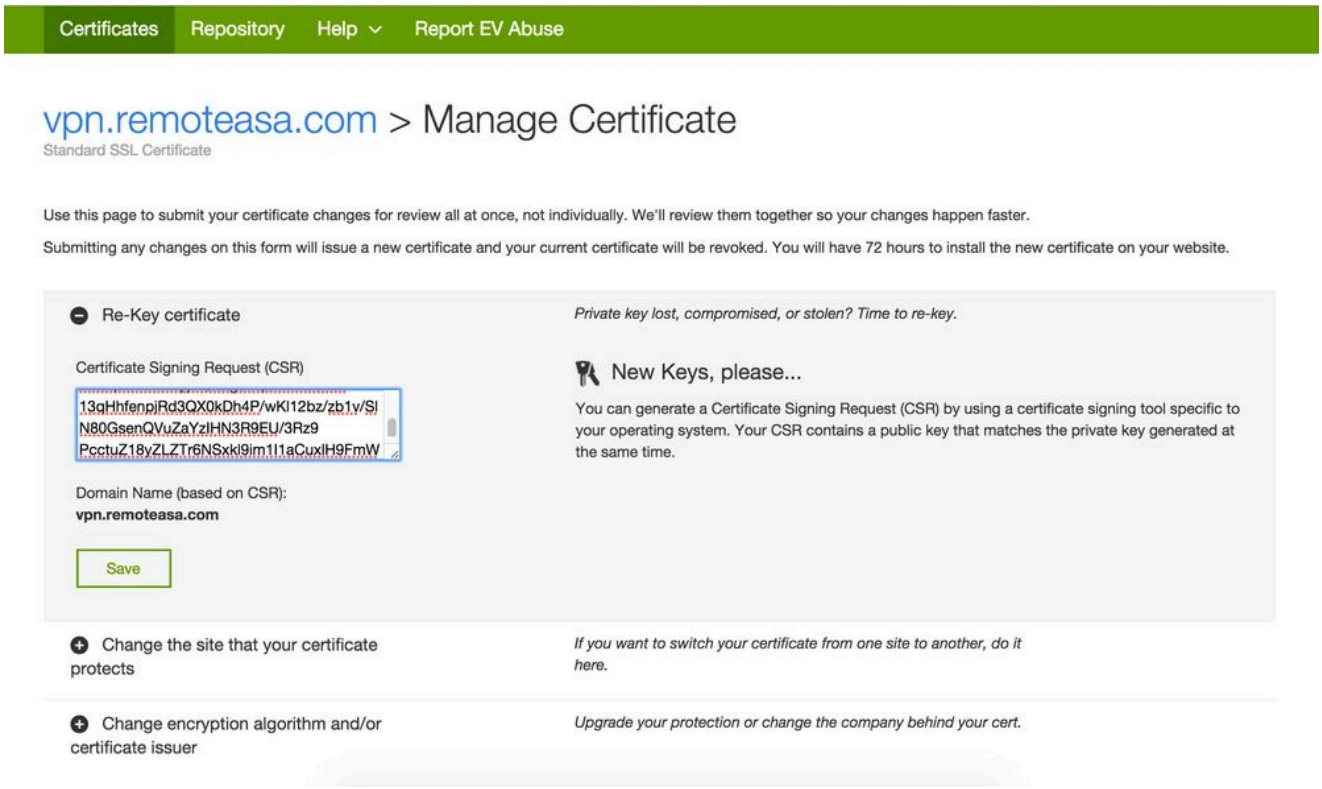

Fare clic su **Visualizza stato** per il nome di dominio richiesto.




Fare clic su **Gestisci** per fornire le opzioni per reimpostare la chiave del certificato.




Espandere l'opzione **Reimposta certificato chiave** e aggiungere il nuovo CSR.




Salvare e procedere al passaggio successivo. GoDaddy emette un nuovo certificato basato sul CSR fornito.

- Installare il nuovo certificato in un nuovo trust point, come mostrato nella sezione Installazione del certificato SSL sull'appliance ASA.

Domande frequenti

**1. Qual è il modo migliore per trasferire i certificati di identità da un'appliance ASA a un'altra appliance?**

Esportare il certificato e le chiavi in un file PKCS12.

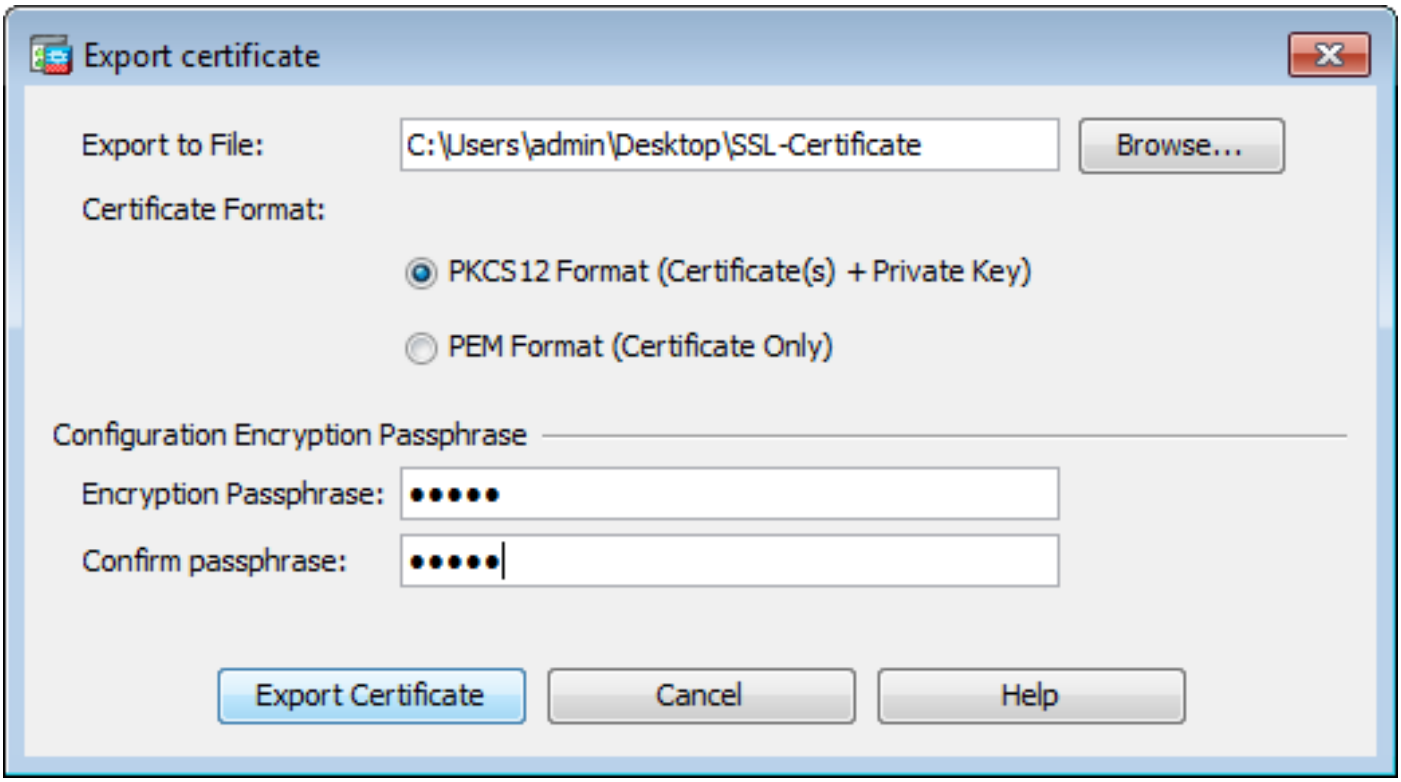
Per esportare il certificato dalla CLI dell'ASA originale, usare questo comando:

<#root>

ASA(config)#

**crypto ca export <trust-point-name> pkcs12 <passphrase>**

Configurazione ASDM:



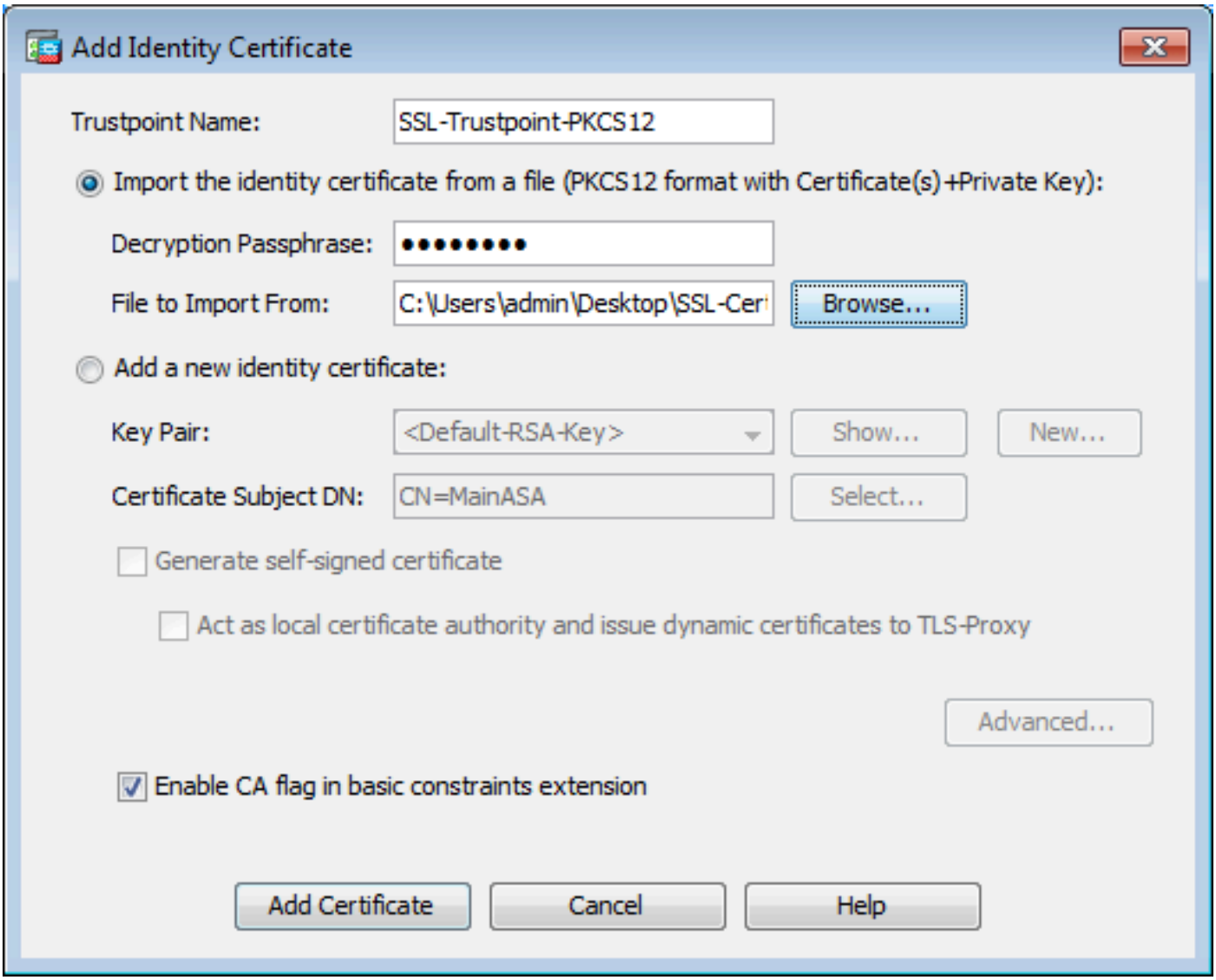

Per importare il certificato sull'appliance ASA di destinazione tramite CLI, usare questo comando:

<#root>

ASA(config)#

**crypto ca import <trust-point-name> pkcs12 <passphrase>**

Configurazione ASDM:




Questa operazione può essere eseguita anche tramite la funzione di backup/ripristino sull'ASDM con i seguenti passaggi:

- Accedere all'appliance ASA tramite ASDM e selezionare**Tools > Backup Configuration**.
- Eseguire il backup di tutta la configurazione o solo dei certificati di identità.
- Sull'appliance ASA di destinazione, aprire ASDM e scegliere**Tools > Restore Configuration.**

**2. Come generare i certificati SSL per l'utilizzo con le appliance ASA per il bilanciamento del carico VPN?**

Per configurare le appliance ASA con certificati SSL per un ambiente di bilanciamento del carico VPN, è possibile utilizzare diversi metodi.

- Utilizzare un singolo certificato UCC (Unified Communications/Multiple Domains Certificate) con FQDN di bilanciamento del carico come DN e ogni FQDN ASA come nome alternativo del soggetto (SAN) distinto. Ci sono diverse CA conosciute come GoDaddy, Entrust, Comodo e altre che supportano tali certificati. Quando si sceglie questo metodo, è importante ricordare che al momento l'ASA non supporta la creazione di un CSR con più campi SAN. Per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCso70867 (informazioni in lingua inglese). In questo caso sono disponibili due opzioni per generare la RSI

a. Tramite CLI o ASDM. Quando il CSR viene inviato alla CA, aggiungere le SAN multiple sul portale CA stesso.

b. Utilizzare OpenSSL per generare il CSR e includere le diverse SAN nel file openssl.cnf.

Dopo aver inviato il CSR alla CA e aver generato il certificato, importare il certificato PEM nell'appliance ASA che lo ha generato. Al termine, esportare e importare il certificato nel formato PKCS12 sulle altre appliance ASA membri.

- Utilizzare un certificato con caratteri jolly. Si tratta di un metodo meno sicuro e flessibile rispetto a un certificato UC. Nel caso in cui la CA non supporti i certificati UC, verrà generato un CSR sulla CA o con OpenSSL in cui il nome FQDN è nel formato *.domain.com. Dopo l'invio del CSR alla CA e la generazione del certificato, importare il certificato PKCS12 in tutte le appliance ASA del cluster.

- Utilizzare un certificato separato per ciascuna delle appliance ASA membro e per il nome di dominio completo (FQDN) di bilanciamento del carico. Questa è la soluzione meno efficace. È possibile creare i certificati per ciascuna appliance ASA come mostrato in questo documento. Il certificato per l'FQDN di bilanciamento del carico VPN viene creato su un'appliance ASA ed esportato e importato come certificato PKCS12 sulle altre appliance ASA.

**3. I certificati devono essere copiati dall'appliance ASA principale all'appliance ASA secondaria in una coppia di failover ASA?**

Non è necessario copiare manualmente i certificati dall'appliance ASA principale a quella secondaria perché i certificati vengono sincronizzati tra le appliance, a condizione che sia configurato il failover stateful. Se durante la configurazione iniziale del failover i certificati non vengono visualizzati sul dispositivo di standby, eseguire il comando **write standby** per forzare una sincronizzazione.

**4. Se vengono utilizzate chiavi ECDSA, il processo di generazione del certificato SSL è diverso?**

L'unica differenza nella configurazione è rappresentata dalla fase di generazione della coppia di chiavi, in cui viene generata una coppia di chiavi ECDSA anziché una coppia di chiavi RSA. Il resto dei gradini rimane lo stesso. Di seguito è riportato il comando CLI per generare le chiavi ECDSA:

<#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...

Risoluzione dei problemi

Comandi per la risoluzione dei problemi

Questi comandi di debug devono essere raccolti sulla CLI in caso di errore durante l'installazione di un certificato SSL:

**debug crypto ca 255**

**debug messaggi ca crypto 255**

**debug transazioni ca crittografiche 255**

Problemi comuni

Avviso relativo a certificati non attendibili con un certificato SSL di terze parti valido sull'interfaccia esterna dell'appliance ASA con versione 9.4(1) e successive.

**Soluzione**: questo problema si presenta quando si utilizza una coppia di chiavi RSA con il certificato. Nelle versioni ASA a partire dalla 9.4(1), tutte le cifrature ECDSA e RSA sono abilitate per impostazione predefinita e la cifratura più efficace (generalmente una cifratura ECDSA) viene utilizzata per la negoziazione. In questo caso, l'ASA presenta un certificato autofirmato anziché il certificato basato su RSA attualmente configurato. È disponibile una funzionalità migliorata per modificare il comportamento quando un certificato basato su RSA viene installato su un'interfaccia e registrato dall'ID bug Cisco CSCuu02848.

**Azione consigliata**: disabilitare i cifrari ECDSA con questi comandi CLI:

```
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"
```

In alternativa, con ASDM, passare**Configuration > Remote Access VPN > Advanced** a e scegliere**SSL Settings**. Nella sezione Encryption, selezionare tlsv1.2 **Cipher version** e modificarla con la stringa personalizzata AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA:RC4-SHA:RC4-MD5

Appendice

Appendice A: ECDSA o RSA

L'algoritmo ECDSA fa parte della crittografia a curva ellittica (ECC) e utilizza un'equazione di una curva ellittica per generare una chiave pubblica, mentre l'algoritmo RSA utilizza il prodotto di due numeri primi più un numero più piccolo per generare la chiave pubblica. Ciò significa che con ECDSA è possibile ottenere lo stesso livello di sicurezza di RSA, ma con chiavi più piccole. In questo modo si riducono i tempi di calcolo e si aumentano i tempi di connessione per i siti che utilizzano i certificati ECDSA.

Il documento sulla crittografia di nuova generazione e l'ASA fornisce informazioni più dettagliate.

Appendice B: utilizzare OpenSSL per generare un certificato PKCS12 da un certificato di identità, un certificato CA e una chiave privata

- Verificare che OpenSSL sia installato sul sistema su cui viene eseguito questo processo. Per gli utenti Mac OSX e GNU/Linux, questa opzione è installata per impostazione predefinita.
- Passare a una directory valida.

In Windows: per impostazione predefinita, le utilità vengono installate in C:\Openssl\bin. Aprire un prompt dei comandi in questa posizione.

Su Mac OSX/Linux: aprire la finestra del terminale nella directory necessaria per creare il certificato PKCS12.

- Nella directory indicata nel passaggio precedente salvare i file della chiave privata (privateKey.key), del certificato di identità (certificate.crt) e della catena di certificati della CA radice (CACert.crt).

Combinare la chiave privata, il certificato di identità e la catena di certificati della CA radice in un file PKCS12. Immettere una passphrase per proteggere il certificato PKCS12.

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

- Convertire il certificato PKCS12 generato in un certificato con codifica Base64:

<#root>

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

Importare quindi il certificato generato nell'ultimo passaggio per l'utilizzo con SSL.

Informazioni correlate

- Guida alla configurazione di ASA 9.x - Configurazione dei certificati digitali
- Come ottenere un certificato digitale da una CA di Microsoft Windows con ASDM su un'appliance ASA
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).