Configurar o ASA: Instalação e renovação do certificado digital SSL

Contents

Introduction

Este documento descreve a instalação de certificado digital SSL confiável de terceiros no ASA para conexões de VPN sem cliente e AnyConnect.

Informações de Apoio

Um certificado GoDaddy é usado neste exemplo. Cada etapa contém o procedimento do Adaptive Security Device Manager (ASDM) e a CLI equivalente.

Prerequisites

Requirements

Este documento requer acesso a uma CA (autoridade de certificação) de terceiros confiável para a inscrição de certificado. Os exemplos de fornecedores de CA de terceiros incluem, mas não se limitam a, Baltimore, Cisco, Entrust, GeoTrust, G, Microsoft, RSA, Thawte e VeriSign.

Antes de iniciar, verifique se o ASA tem a hora, a data e o fuso horário corretos. Com a autenticação de certificado, é recomendável usar um Network Time Protocol (NTP) para sincronizar a hora no ASA. O Guia de configuração da CLI de operações gerais do Cisco ASA 9.1 detalha as etapas a serem seguidas para configurar corretamente a hora e a data no ASA

Componentes Utilizados

Este documento usa um ASA 5500-X que executa a versão de software 9.4.1 e ASDM versão 7.4(1).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

O protocolo SSL exige que o servidor SSL forneça ao cliente um certificado de servidor para que o cliente execute a autenticação do servidor. A Cisco não recomenda o uso de um certificado autoassinado, devido à possibilidade de um usuário configurar inadvertidamente um navegador para confiar em um certificado de um servidor invasor. Também há a inconveniência de os usuários responderem a um aviso de segurança quando ele se conectar ao gateway seguro. Para essa finalidade, é recomendável usar CAs de terceiros confiáveis para emitir certificados SSL para o ASA.

O ciclo de vida de um certificado de terceiros no ASA essencialmente inclui estas etapas :

Geração de CSR

A geração de CSR é a primeira etapa no ciclo de vida de qualquer certificado digital X.509.

Depois que o par de chaves privada/pública Rivest-Shamir-Adleman (RSA) ou o par de chaves do Algoritmo de Assinatura Digital de Curvas Elípticas (ECDSA) é gerado (O Apêndice A detalha a diferença entre o uso de RSA ou ECDSA), uma Solicitação de Assinatura de Certificado (CSR) é criada.

Um CSR é uma mensagem formatada PKCS10 que contém a chave pública e as informações de identidade do host que envia a solicitação. Formatos de dados PKI explica os diferentes formatos de certificado aplicáveis ao ASA e ao Cisco IOS®.

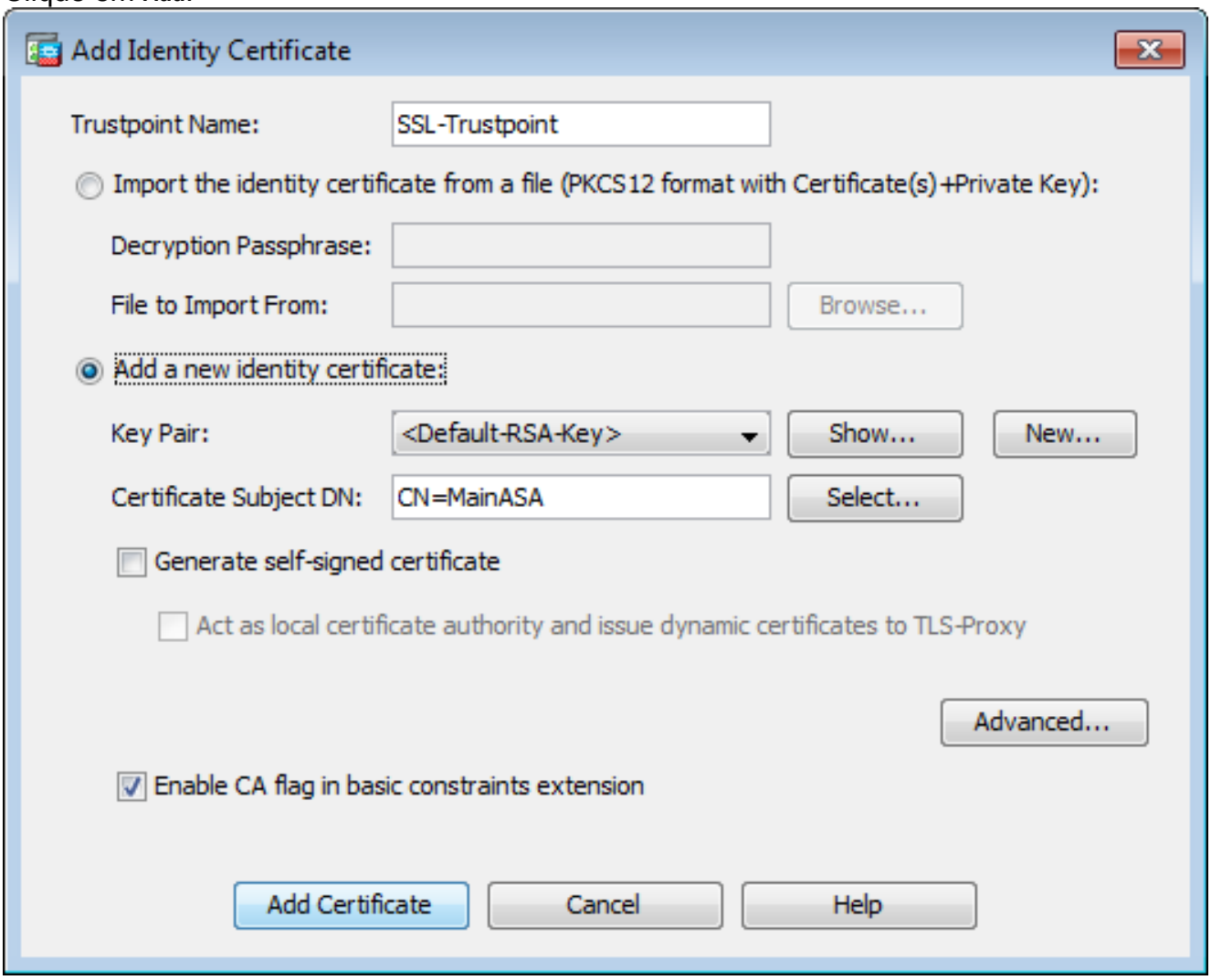
> **Notas:**
> 1. Verifique com a CA no tamanho do par de chaves necessário. O CA/Browser Forum ordenou que todos os certificados gerados pelas CAs membros tenham um tamanho mínimo de 2048 bits.
> 2. Atualmente, o ASA não oferece suporte a chaves de 4096 bits (ID de bug da Cisco CSCut53512) para autenticação de servidor SSL. No entanto, o IKEv2 suporta o uso de certificados de servidor de 4096 bits somente nas plataformas ASA 5580, 5585 e 5500-X.
> 3. Use o nome DNS do ASA no campo FQDN do CSR para evitar avisos de certificado não confiáveis e passar na verificação de certificado rigorosa.

Há três métodos para gerar CSR.

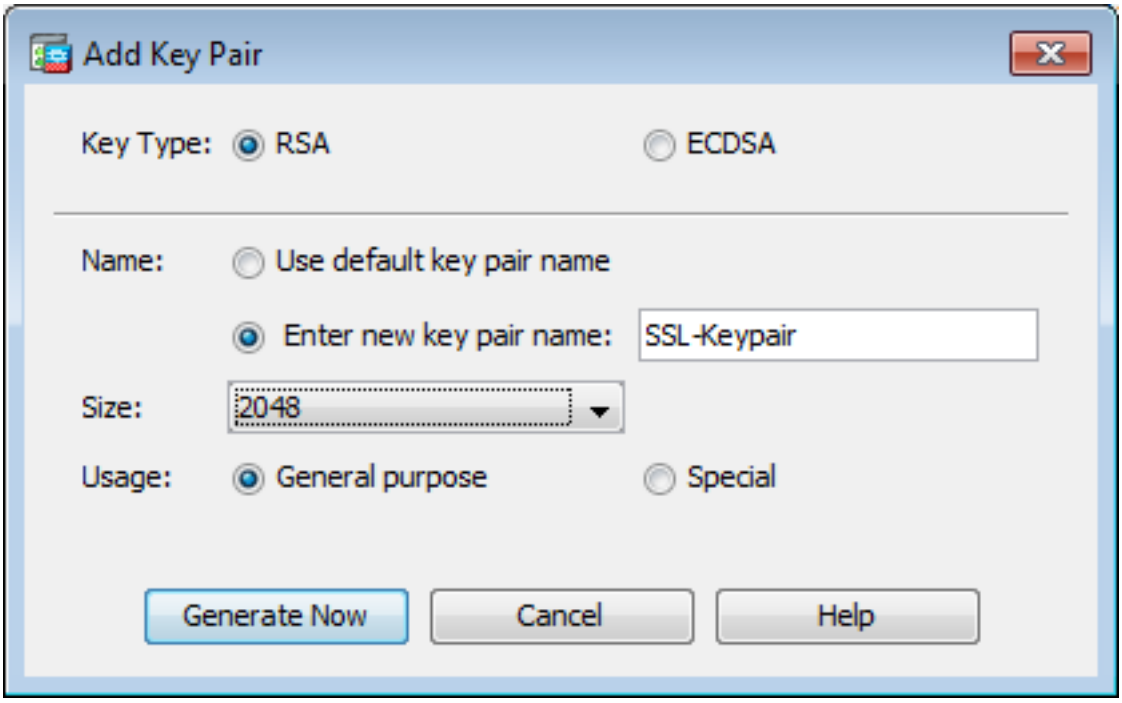
- Configurar com ASDM
- Configure com a CLI do ASA
- Use o OpenSSL para gerar o CSR

1. Configure com o ASDM

1. Navegar para **Configuration > Remote Access VPN > Certificate Managemente** escolha **Identity Certificates**.
2. Clique em **Add**.



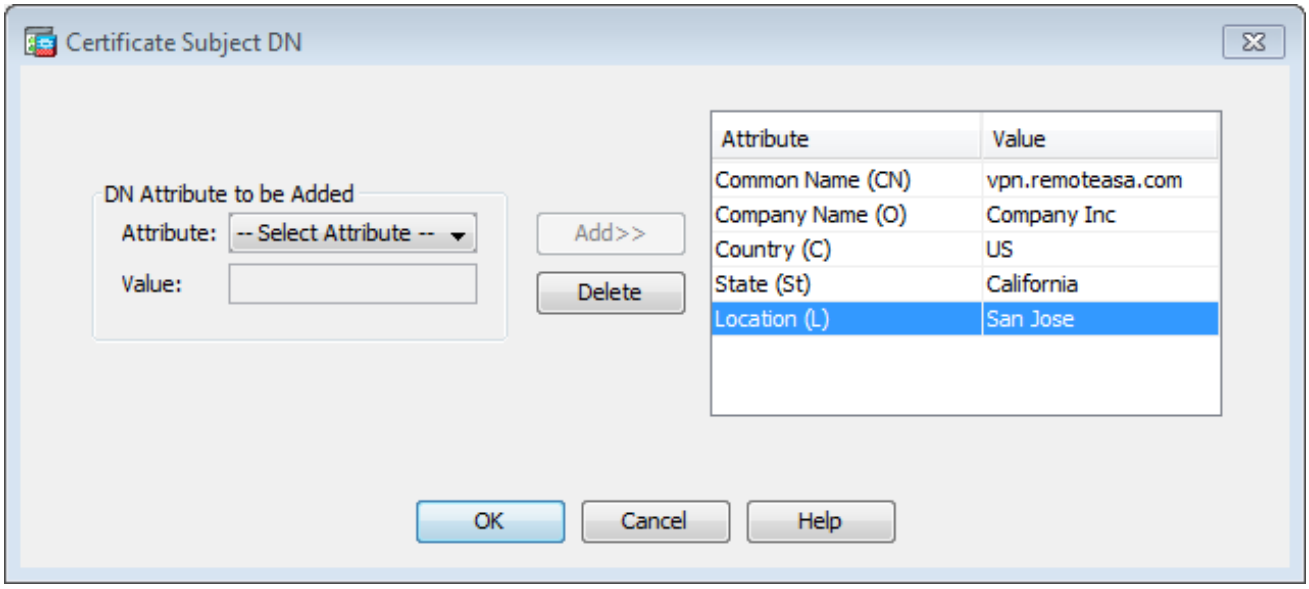
3. Defina um nome de ponto confiável no campo de entrada Nome do ponto confiável.
4. Clique no botão**Add a new identity certificate**botão de opção.
5. Para o par de chaves, clique em**New**.



6. Escolha o tipo de chave-RSA ou ECDSA. (Consulte o Apêndice A para entender as diferenças.)
7. Clique no botãoEnter new key pair namebotão de opção. Identifique o nome do par de chaves para fins de reconhecimento.
8. Escolha oKey Size. EscolherGeneral Purpose for Usage se estiver usando RSA.
9. Clique emGenerate Now. O par de chaves é criado.
10. Para definir o DN do assunto do certificado, clique emSelecte configure os atributos listados nesta tabela:

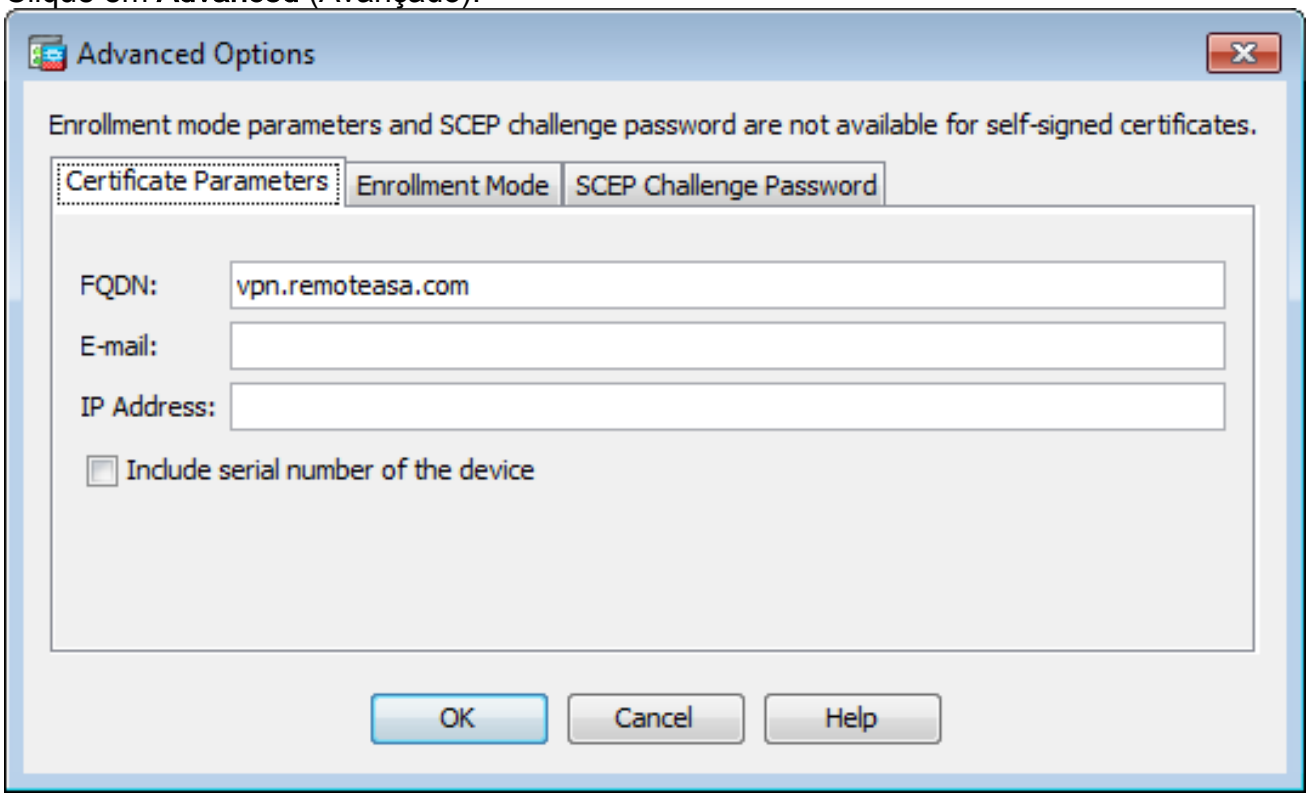
Attribute	Description
CN	FQDN (Full Qualified Domain Name) that will be used for connections to your firewall. For example, webvpn.cisco.com
OU	Department Name
O	Company Name (Avoid using Special Characters)
C	Country Code (2 Letter Code without Punctuation)
St	State (Must be spelled out completely.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

Para configurar esses valores, escolha um valor na lista suspensa **Atributo**, insira o valor e clique em
Adicionar.

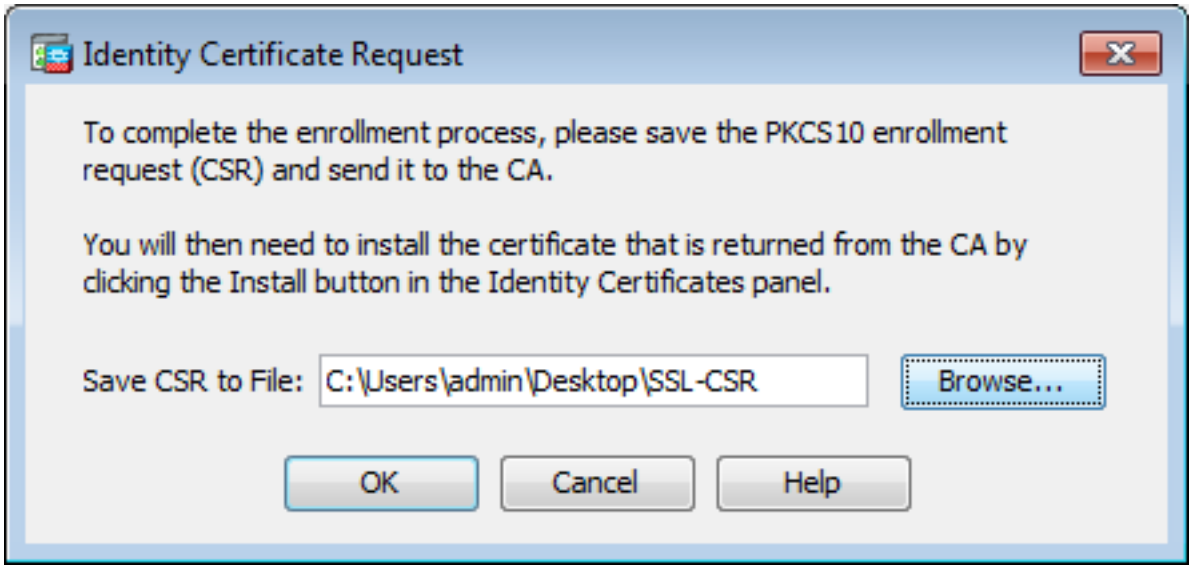


Note: Alguns fornecedores terceirizados exigem que determinados atributos sejam incluídos antes da emissão de um certificado de identidade. Se não tiver certeza dos atributos necessários, verifique os detalhes com o fornecedor.

11. Depois que os valores apropriados forem adicionados, clique em**OK**. A caixa de diálogo Adicionar certificado de identidade é exibida com o certificado**Subject DN** field populated.
12. Clique em **Advanced** (Avançado).



13. No**FQDN**insira o FQDN usado para acessar o dispositivo da Internet. Clique em**OK**.
14. Deixe a opção Enable CA flag in basic constraints (Ativar sinalizador de CA) em extensão de restrições básicas) marcada. Como padrão, agora os certificados sem o sinalizador de CA não podem ser instalados no ASA como certificados de CA. A extensão de restrições básicas identifica se o assunto do certificado é uma CA e a profundidade máxima de caminhos de certificação válidos que incluem esse certificado. Desmarque a opção para ignorar este requisito.
15. Clique em**OK**e, em seguida, clique em**Add Certificate.** Um prompt é exibido para salvar o CSR em um arquivo na máquina local.



16. Clique em**Browse**, escolha um local no qual salvar o CSR e salve o arquivo com a extensão .txt. **Note**: Quando o arquivo é salvo com uma extensão .txt, a solicitação PKCS#10 pode ser aberta e visualizada com um editor de texto (como o bloco de notas).

2. Configure com a CLI do ASA

No ASDM, o trustpoint é criado automaticamente quando um CSR é gerado ou quando o certificado da CA é instalado. Na CLI, o trustpoint deve ser criado manualmente.

```
! 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 will be: 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 vpn.remoteasa.com
MainASA(config-ca-trustpoint)# subject-name CN=vpn.remoteasa.com,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 will be
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 will be: subject-name CN=vpn.remoteasa.com,
O=Company Inc,C=US,St=California,L=San Jose % The fully-qualified domain name in the certificate
will be: vpn.remoteasa.com % Include the device serial number in the subject name? [yes/no]: no

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

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDDjCCAfYCAQAwgYkxETAPBgNVBAcTCFNhbiBKb3NlMRMwEQYDVQQIEwpDYWxp
Zm9ybmlhMQswCQYDVQQGEwJVUzEUMBIGA1UEChMLQ29tcGFueSBJbmMxGjAYBgNV
BAMTEXZwbi5yZW1vdGVhc2EuY29tMSAwHgYJKoZIhvcNAQkCFhF2cG4ucmVtb3Rl
YXNhLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK62Nhb9ktlK
uR3Q4TmksyuRMqJNrb9kXpvA6H200PuBfQvSF4rVnSwKOmu3c8nweEvYcdVWV6Bz
BhjXeovTVi17FlNTceaUTGikeIdXC+mw1iE7eRsynS/d4mzMWJmrvrsDNzpAW/EM
SzTca+BvqF7X2r3LU8Vsv6Oi8ylhco9Fz7bWvRWVtO3NDDbyolC9b/VgXMuBitcc
rzfUbVnm7VZDOf4jr9EXgUwXxcQidWEABlFrXrtYpFgBo9aqJmRp2YABQ1ieP4cY
3rBtgRjLcF+S9TvHG5m4v7v755meV4YqsZIXvytIOzVBihemVxaGA1oDwfkoYSFi
4CzXbFvdG6kCAwEAAaA/MD0GCSqGSIb3DQEJDjEwMC4wDgYDVR0PAQH/BAQDAgWg
MBwGA1UdEQQVMBOCEXZwbi5yZW1vdGVhc2EuY29tMA0GCSqGSIb3DQEBBQUAA4IB
AQBZuQzUXGEB0ix1yuPK0ZkRz8bPnwIqLTfxZhagmuyEhrN7N4+aQnCHj85oJane
4ztZDiCCoWTerBS4RSkKEHEspu9oohjCYuNnp5qa91SPrZNEjTWw0eRn+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. Use o OpenSSL para gerar o CSR

O OpenSSL usa o comando**OpenSSL config**para extrair os atributos a serem usados na geração CSR. Esse processo resulta na geração de um CSR e de uma chave privada.

> Caution: Verifique se a chave privada gerada não é compartilhada com mais ninguém, pois compromete a integridade do certificado.

1. Verifique se o OpenSSL está instalado no sistema em que esse processo é executado. Para usuários Mac OSX e GNU/Linux, isso é instalado por padrão.
2. Alterne para um diretório de trabalho. No Windows: Por padrão, os utilitários são instalados em **c:\Openssl\bin**. Abra um prompt de comando neste local.No Mac OSX/Linux: Abra a janela do terminal no diretório necessário para criar o CSR.
3. Crie um arquivo de configuração OpenSSL usando um editor de texto com os atributos fornecidos . Depois de concluído, salve o arquivo como **openssl.cnf** no local mencionado na etapa anterior (se você tiver a versão 0.9.8h e posterior, o arquivo será**openssl.cfg**)

```
 [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 = vpn.remoteasa.com

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 = *.remoteasa.com
```

4. Gere o CSR e a chave privada com este comando: **openssl req -new -nodes -out CSR.csr -config openssl.cnf**

```
 # Sample CSR Generation:

 openssl req -new -nodes -out CSR.csr -config openssl.cnf
Generating 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) [vpn.remoteasa.com]: 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]:
```

   Envie o CSR salvo para o fornecedor de CA de terceiros. Depois que o certificado é emitido, a CA fornece o certificado de identidade e o certificado da CA a serem instalados no ASA.

Geração de certificado SSL em CA

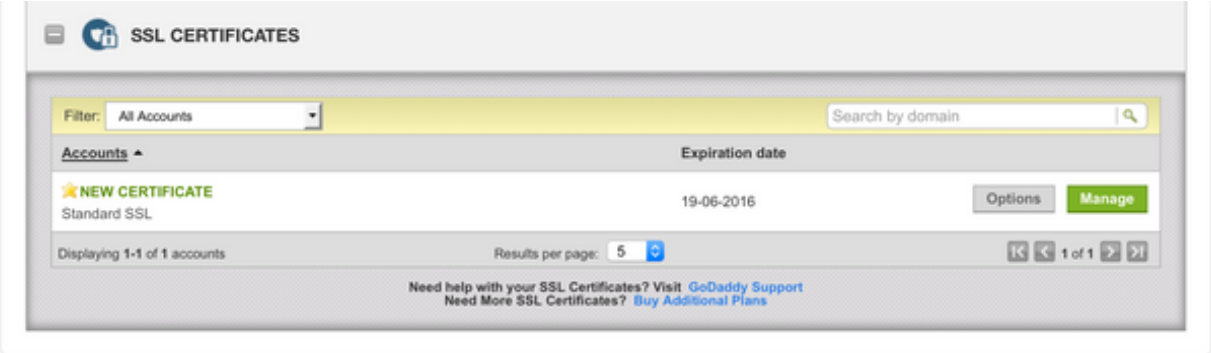
A próxima etapa é fazer com que o CSR assine a CA. A CA fornece um certificado de identidade codificada em PEM recém-gerado ou com um certificado PKCS12 juntamente com o pacote de certificado da CA.

Se o CSR for gerado fora do ASA (via OpenSSL ou na própria CA), o certificado de identidade codificado PEM com a chave privada e o certificado CA estarão disponíveis como arquivos separados. O Apêndice B fornece as etapas para reunir esses elementos em um único arquivo PKCS12 (formato .p12 ou .pfx).

Neste documento, a CA GoDaddy é usada como exemplo para emitir certificados de identidade para o ASA. Esse processo pode ser diferente em outros fornecedores de CA.Leia a documentação da CA cuidadosamente antes de continuar.

Exemplo de geração de certificado SSL em CA GoDaddy

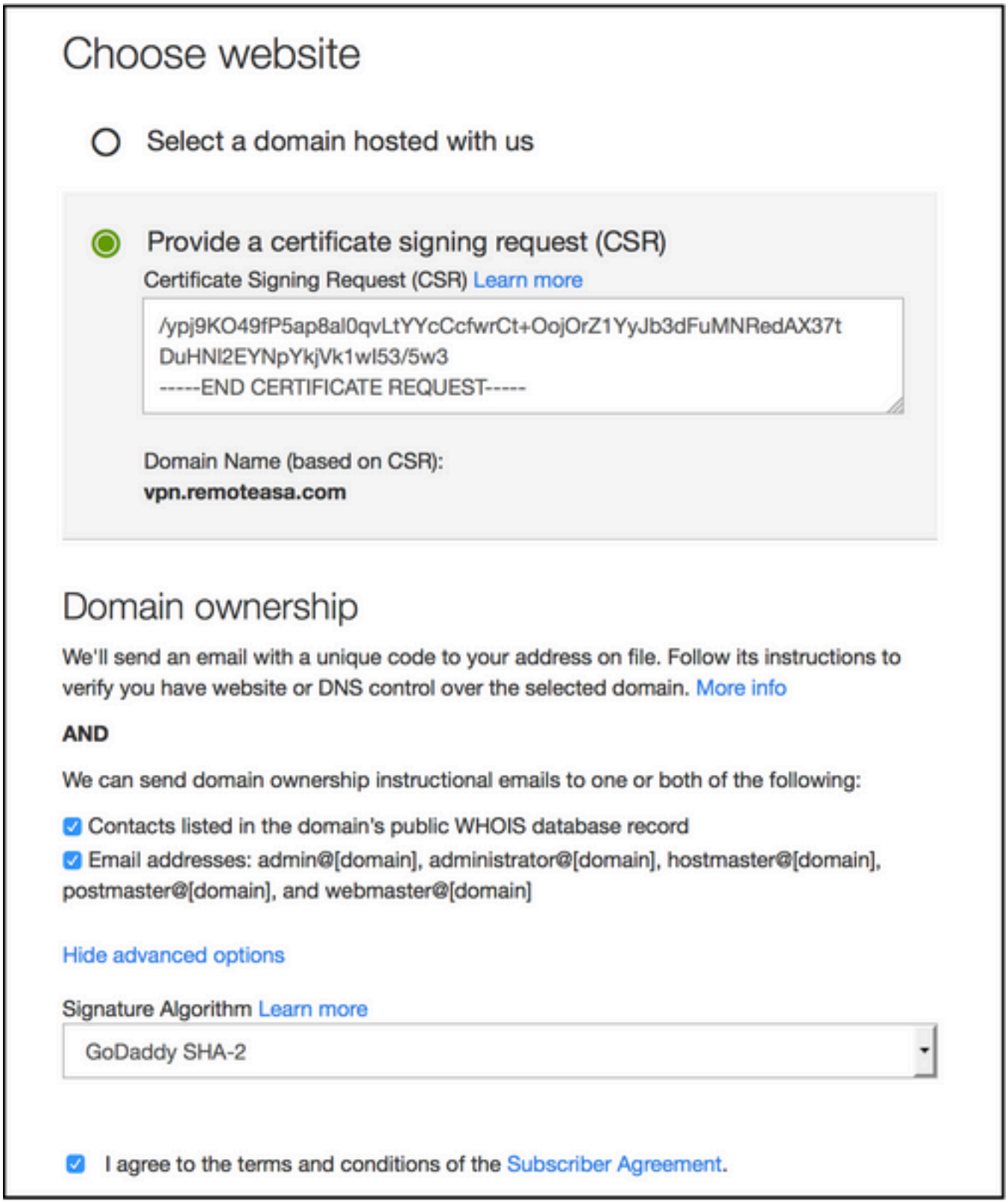
Após a compra e a fase de configuração inicial do certificado SSL, navegue até a conta GoDaddy e exiba os certificados SSL. Deve haver um novo certificado. Clique em**Manage** para prosseguir.



Em seguida, exibe uma página para fornecer ao CSR como visto nessa imagem.

Com base no CSR inserido, a CA determina o nome do domínio para o qual o certificado será emitido.

Verifique se isso corresponde ao FQDN do ASA.

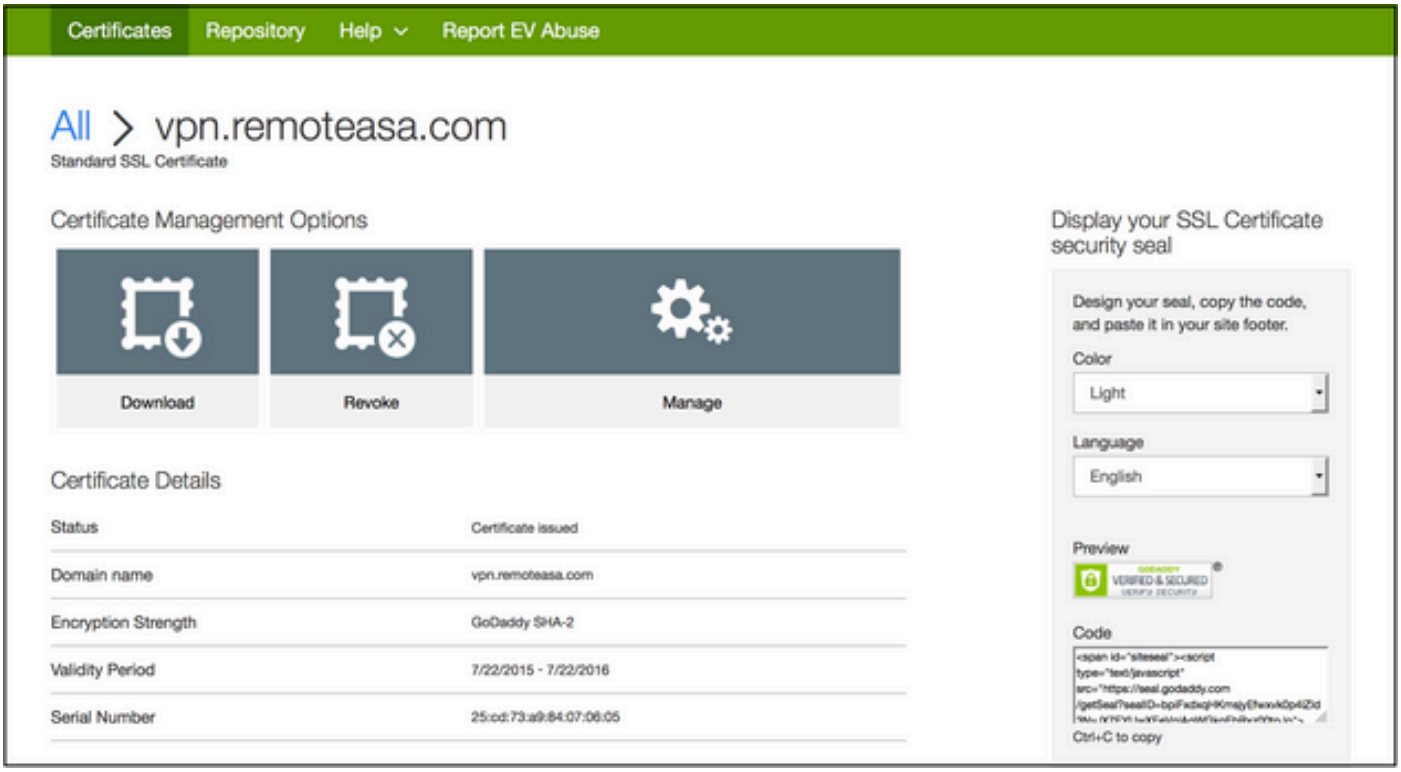


Nota: GoDaddy e a maioria das outras CAs usam SHA-2 ou SHA256 como o algoritmo de assinatura de certificado padrão. O ASA suporta o algoritmo de assinatura SHA-2 a partir de **8.2(5)** [versões anteriores a 8.3] e **8.4(1)** [versões posteriores a 8.3] (ID de bug da Cisco CSCti30937). Escolha o algoritmo de assinatura SHA-1 se for usada uma versão mais antiga que 8.2(5) ou 8.4(1).

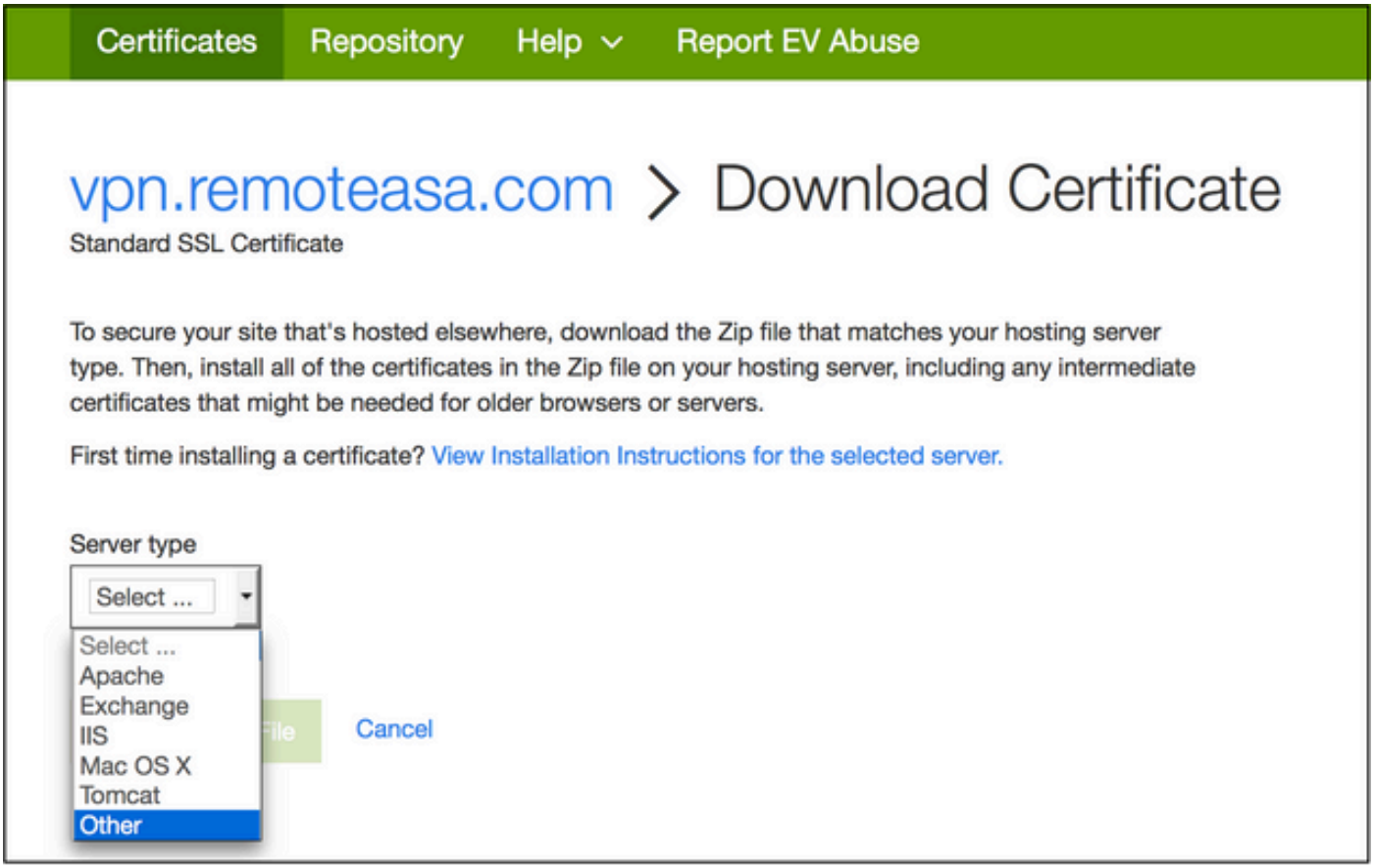
Assim que a solicitação for enviada, o GoDaddy verifica a solicitação antes de emitir o certificado.

Depois que a solicitação de certificado é validada, o GoDaddy emite o certificado para a conta.

O certificado pode ser baixado para instalação no ASA. Clique em**Download** na página para prosseguir.



Escolher**Other** como o tipo de servidor e faça o download do pacote zip de certificado.



O arquivo .zip contém o certificado de identidade e a cadeia de certificados de CA de GoDaddy como dois arquivos .CRT separados. Vá para a instalação do certificado SSL para instalar esses certificados no ASA.

Instalação do certificado SSL no ASA

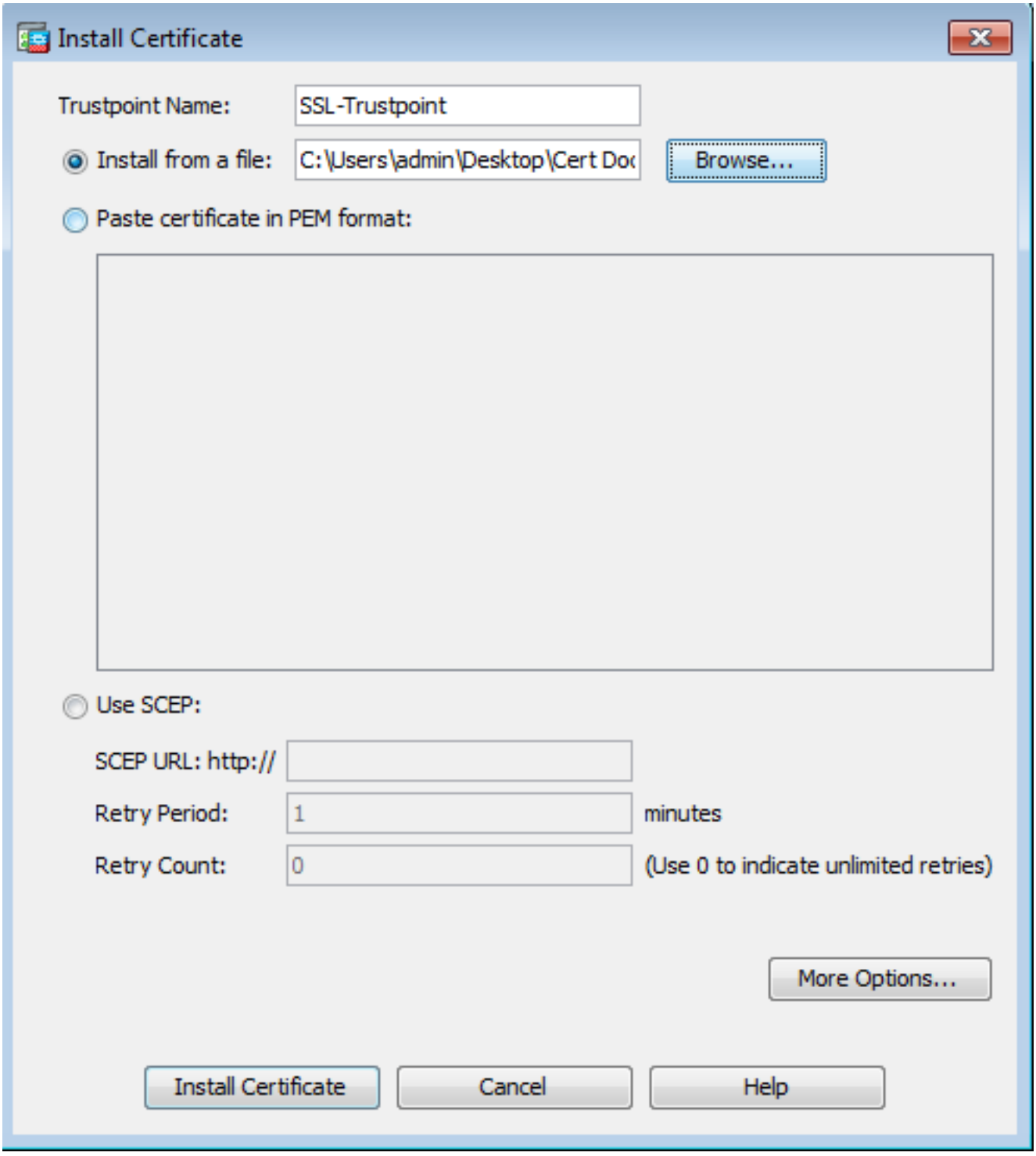
O certificado SSL pode ser instalado no ASA com o ASDM ou CLI de duas maneiras:

1. Importe a CA e o certificado de identidade separadamente em formatos PEM.
2. Ou importe o arquivo PKCS12 (codificado em base64 para CLI) onde o certificado de identidade, o certificado de CA e a chave privada são agrupados no arquivo PKCS12. **Nota**: se a CA fornece uma cadeia de certificados de CA, instale apenas o certificado de CA intermediário imediato na hierarquia do trustpoint usado para gerar o CSR. O certificado da CA raiz e quaisquer outros certificados de CA intermediários podem ser instalados em novos trustpoints.

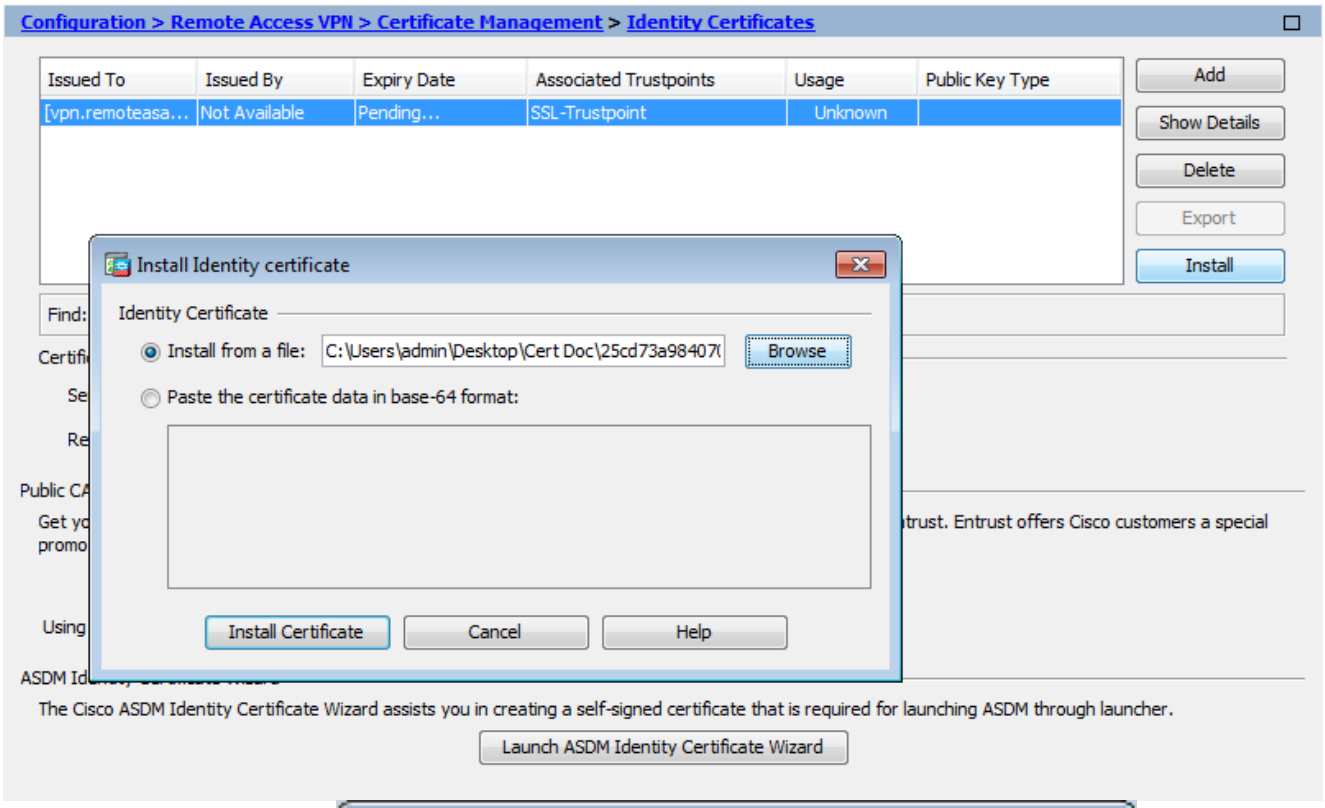
1.1 Instalação do certificado de identidade no formato PEM com o ASDM

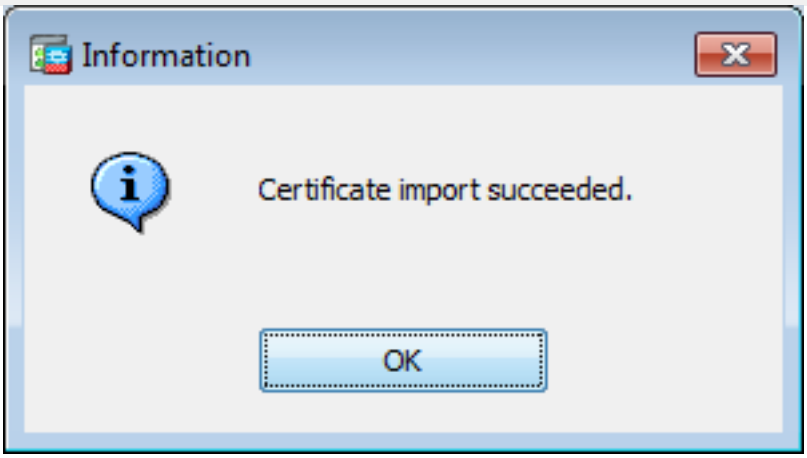
As etapas de instalação indicaram que a CA fornece um pacote de certificado de identidade e certificado de CA codificado (.pem, .cer, .crt) do PEM.

1. Navegar para **Configuration > Remote Access VPN > Certificate Managemente** escolha Certificados CA.
2. O certificado codificado de PEM em um editor de texto e copie e cole o certificado CA de base64 do fornecedor terceirizado no campo de texto.

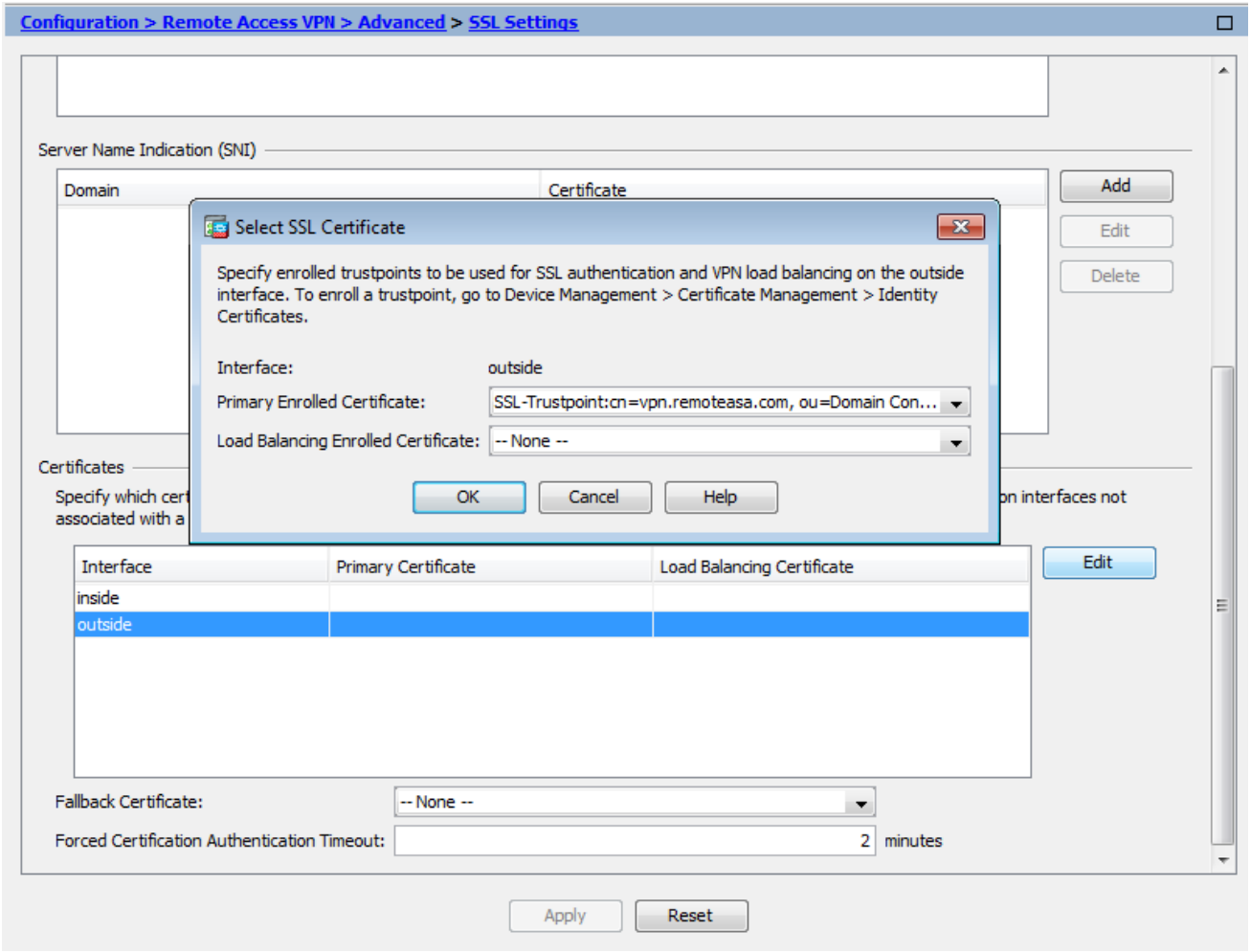


3. Clique em **Install certificate** (Instalar certificado).
4. Navegar para **Configuration > Remote Access VPN > Certificate Management** e escolha Certificados de identidade.
5. Selecione o certificado de identidade criado anteriormente. Clique em **Install**.
6. Clique na opção **Install from a file** e escolha o certificado de identidade codificado PEM ou abra o certificado codificado PEM em um editor de texto e copie e cole o certificado de identidade base64 fornecido pelo fornecedor terceirizado no campo de texto.





7. Clique em **Add Certificate**.
8. Navegar para **Configuration > Remote Access VPN > Advanced > SSL Settings**.
9. Em Certificates (Certificados), selecione a interface usada para encerrar sessões de WebVPN. Neste exemplo, a interface externa é usada.
10. Clique em **Edit**.
11. Na lista suspensa Certificado e escolha o certificado recém-instalado.



12. Clique emOK.
13. Clique emApply. O novo certificado agora é utilizado para todas as sessões WebVPN terminadas na interface especificada.

1.2. Instalação de um certificado PEM com a CLI

```
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
MB8GA1UEChMYVGhlIEdvIERhZGR5IEdyb3VwLCBJbmMuMTEwLwYDVQQLEyhHbyBE
YWRkeSBDbGFzcyAyIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MB4XDTA0MDYyOTE3
MDYyMFoXDTM0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFRo
ZSBHbyBEYWRkeSBHcm91cCwgSW5jLjExMC8GA1UECxMoR28gRGFkZHkgQ2xhc3Mg
MiBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTCCASAwDQYJKoZIhvcNAQEBBQADggEN
ADCCAQgCggEBAN6d1+pXGEmhW+vXX0iG6r7d/+TvZxz0ZWizV3GgXne77ZtJ6XCA
PVYYYwhv2vLM0D9/AlQiVBDYsoHUwHU9S3/Hd8M+eKsaA7Ugay9qK7HFiH7Eux6w
wdhFJ2+qN1j3hybX2C32qRe3H3I2TqYXP2WYktsqbl2i/ojgC95/5Y0V4evLOtXi
EqITLdiOr18SPaAIBQi2XKVlOARFmR6jYGB0xUGlcmIbYsUfb18aQr4CUWWoriMY
avx4A6lNf4DD+qta/KFApMoZFv6yyO9ecw3ud72a9nmYvLEHZ6IVDd2gWMZEewo+
YihfukEHU1jPEX44dMX4/7VpkI+EdOqXG68CAQOjgcAwgb0wHQYDVR0OBBYEFNLE
sNKR1EwRcbNhyz2h/t2oatTjMIGNBgNVHSMEgYUwgYKAFNLEsNKR1EwRcbNhyz2h
/t2oatTjoWekZTBjMQswCQYDVQQGEwJVUzEhMB8GA1UEChMYVGhlIEdvIERhZGR5
IEdyb3VwLCBJbmMuMTEwLwYDVQQLEyhHbyBEYWRkeSBDbGFzcyAyIENlcnRpZmlj
YXRpb24gQXV0aG9yaXR5ggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQAD
ggEBADJL87LKPpH8EsahB4yOd6AzBhRckB4Y9wimPQoZ+YeAEW5p5JYXMP80kWNy
OO7MHAGjHZQopDH2esRU1/blMVgDoszOYtuURXO1v0XJJLXVggKtI3lpjbi2Tc7P
TMozI+gciKqdi0FuFskg5YmezTvacPd+mSYgFFQlq25zheabIZ0KbIIOqPjCDPoQ
```

```
HmyW74cNxA9hi63ugyuV+I6ShHI56yDqg+2DzZduCLzrTia2cyvk0/ZM/iZx4mER
dEr/VxqHD3VILs9RaRegAhJhldXRQLIQTO7ErBBDpqWeCtWVYpoNz4iCxTIM5Cuf ReYNnyicsbkqWletNw+vHX/bvZ8= --
---END CERTIFICATE----- quit INFO: Certificate has the following attributes: Fingerprint:
96c25031 bc0dc35c fba72373 1e1b4140 Do you accept this certificate? [yes/no]: yes Trustpoint
'SSL-Trustpoint' is a subordinate CA and holds a non self-signed certificate. Trustpoint CA
certificate accepted. % Certificate successfully imported
```

!!! - 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
oCOGIWh0dHA6Ly9jcmwuZ29kYWRkeS5jb20vZ2Ryb290LmNybDBGBgNVHSAEPzA9
MDsGBFUdIAAwMzAxBggrBgEFBQcCARYlaHR0cHM6Ly9jZXJ0cy5nb2RhZGR5LmNv
bS9yZXBvc2l0b3J5LzANBgkqhkiG9w0BAQsFAAOCAQEAWQtTvZKGEacke+1bMc8d
H2xwxbhuvk679r6XUOEwf7ooXGKUwuN+M/f7QnaF25UcjCJYdQkMiGVnOQoWCcWg
OJekxSOTP7QYpgEGRJHjp2kntFolfzq3Ms3dhP8qOCkzpN1nsoX+oYggHFCJyNwq
9kIDN0zmiN/VryTyscPfzLXs4Jlet0lUIDyUGAzHHFIYSaRt4bNYC8nY7NmuHDKO
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)#
```

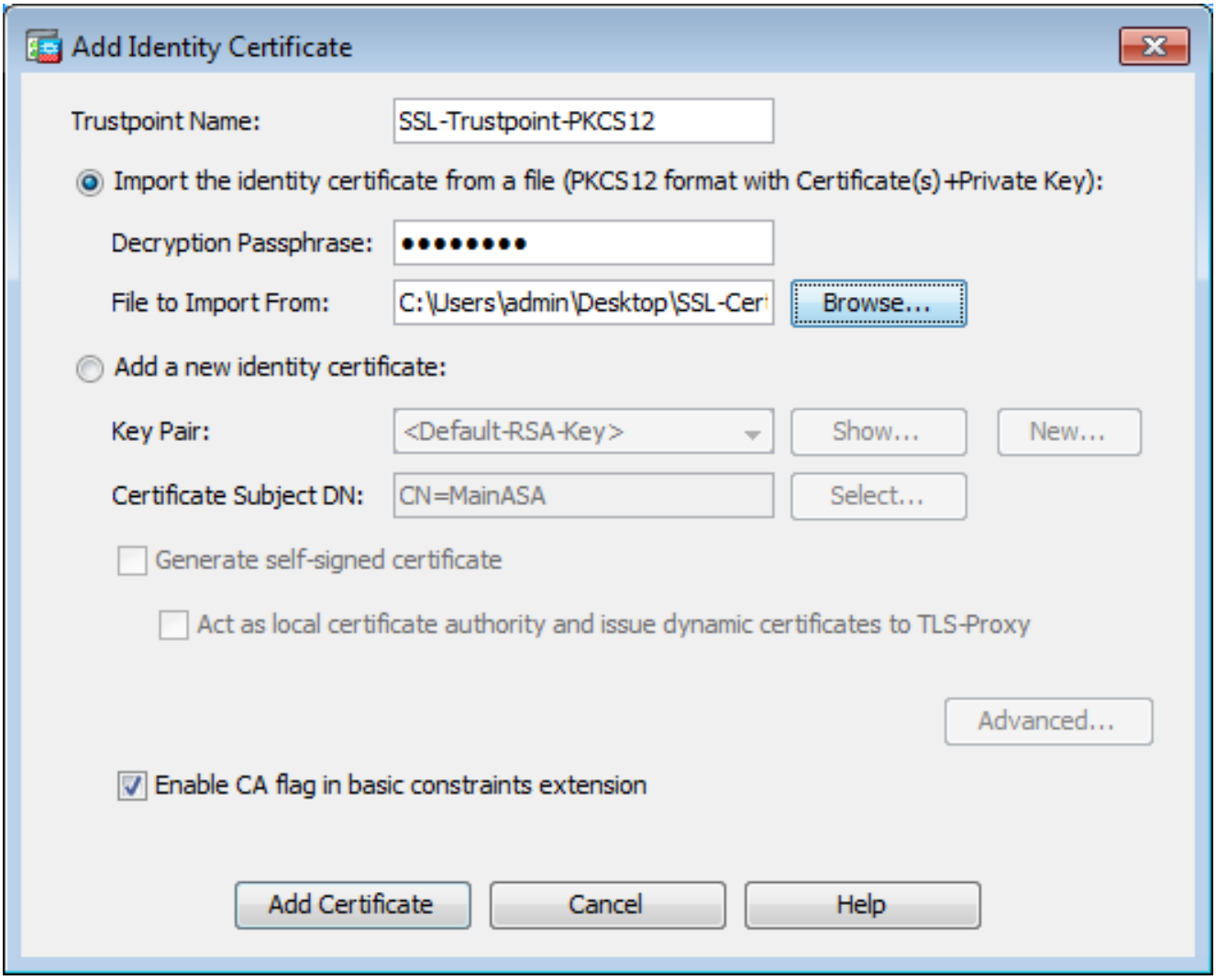
!!! - Similarly create additional trustpoints (of the name "SSL-Trustpoint-n",
where n is number thats incremented for every level in the PKI hierarchy) to
import the CA certificates leading up to the Root CA certificate.

```
!!! - 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 this certificate will be used for VPN authentication this may cause connection
problems. Would you like to continue with this enrollment? [yes/no]: yes % The fully-qualified
domain name in the certificate will be: vpn.remoteasa.com Enter the base 64 encoded certificate.
End with the word "quit" on a line by itself ----BEGIN CERTIFICATE-----
MIIFRjCCBC6gAwIBAgIIJc1zqYQHBgUwDQYJKoZIhvcNAQELBQAwgbQxCzAJBgNV
BAYTAlVTMRAwDgYDVQQIEwdBcml6b25hMRMwEQYDVQQHEwpTY290dHNkYWxlMRow
GAYDVQQKExFHb0RhZGR5LmNvbSwgSW5jLjEtMCsGA1UECxMkaHR0cDovL2NlcnRz
LmdvZGFkZHkuY29tL3JlcG9zaXRvcnkvMTMwMQYDVQQDEypHbyBEYWRkeSBTZWN1
cmUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5IC0gRzIwHhcNMTUwNzIyMTIwNDM4WhcN
MTYwNzIyMTIwNDM4WjA/MSEwHwYDVQQLExhEb21haW4gQ29udHJvbCBWYWxpZGF0
ZWQxGjAYBgNVBAMTEXZwbi5yZW1vdGVhc2EuY29tMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEArrY2Fv2S2Uq5HdDhOaSzK5Eyok2tv2Rem8DofbTQ+4F9
C9IXitWdLAo6a7dzyfB4S9hx1VZXoHMGGNd6i9NWLXsWU1Nx5pRMaKR4h1cL6bDW
ITt5GzKdL93ibMxYmau+uwM3OkBb8QxLNNxr4G+oXtfavctTxWy/o6LzKWFyj0XP
tta9FZW07c0MNvKiUL1v9WBcy4GK1xyvN9RtWebtVkM5/iOv0ReBTBfFxCJ1YQAG
UWteu1ikWAGj1qomZGnZgAFDWJ4/hxjesG2BGMtwX5L1O8cbmbi/u/vnmZ5Xhiqx <snip>
CCsGAQUFBwIBFitodHRwOi8vY2VydGlmaWNhdGVzLmdvZGFkZHkuY29tL3JlcG9z
aXRvcnkvMHYGCCsGAQUFBwEBBGowaDAkBggrBgEFBQcwAYYYaHR0cDovL29jc3Au
Z29kYWRkeS5jb20vMEAGCCsGAQUFBzAChjRodHRwOi8vY2VydGlmaWNhdGVzLmdv
ZGFkZHkuY29tL3JlcG9zaXRvcnkvZ2RpZzIuY3J0MB8GA1UdIwQYMBaAFEDCvSeO
zDSDMKIz1/tss/C0LIDOMEYGA1UdEQQ/MD2CEXZwbi5yZW1vdGVhc2EuY29tghV3
d3cudnBuLnJlbW90ZWFzYS5jb22CEXZwbi5yZW1vdGVhc2EuY29tMB0GA1UdDgQW
BBT7en7YS3PH+s4z+wTRlpHr2tSzejANBgkqhkiG9w0BAQsFAAOCAQEAO9H8TLNx
2Y0rYdI6gS8n4imaSYg9Ni/9Nb6mote3J2LELG9HY9m/zUCR5yVktra9azdrNUAN
1hjBJ7kKQScLC4sZLONdqG1uTP5rbWR0yikF5wSzgyMWd03kOR+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
```

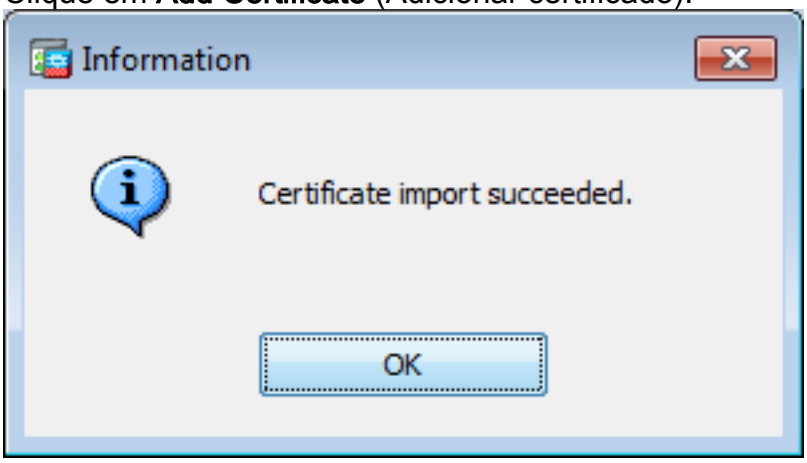
2.1 Instalação de um certificado PKCS12 com ASDM

Nos casos em que o CSR não é gerado no ASA, como no caso de um certificado curinga ou quando um certificado UC é gerado, um certificado de identidade associado à chave privada pode ser recebido como arquivos separados ou um único arquivo PKCS12 agrupado (formato .p12 ou pfx). Para instalar esse tipo de certificado, siga estes passos.

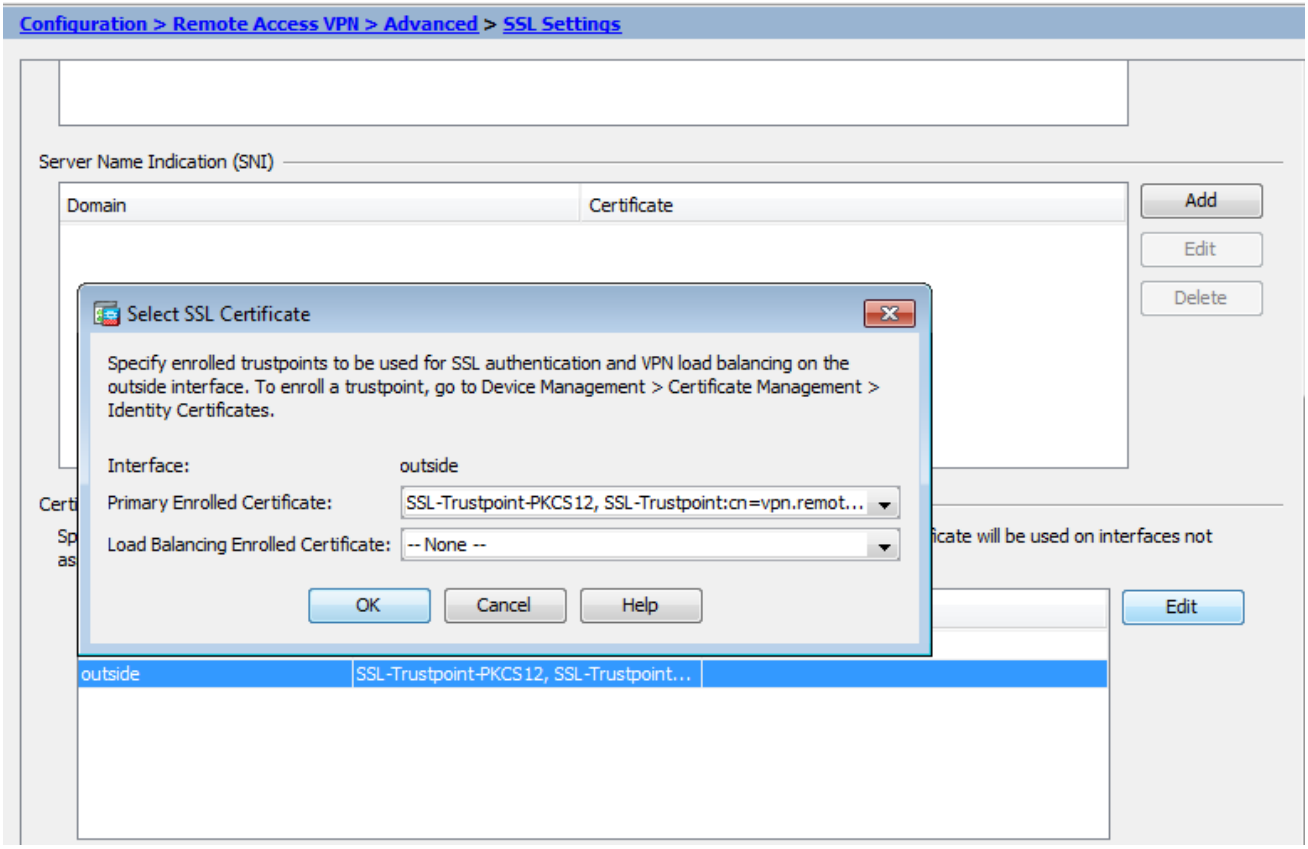
1. O certificado de identidade, agrupe o certificado CA e a chave privada em um único arquivo PKCS12. O Apêndice B fornece as etapas para fazer isso com o OpenSSL. Se já estiver agrupado na CA, prossiga para a próxima etapa.
2. Navegar para **Configuration > Remote Access VPN > Certificate Management,** e escolha **Identity Certificates.**
3. Clique em **Add**.
4. Especifique um nome de Trustpoint.
5. Clique no botão **Import the identity certificate from a file** botão de opção.
6. Insira a senha usada para criar o arquivo PKCS12. Procure e selecione o arquivo PKCS12. Insira a senha do certificado.



7. Clique em **Add Certificate** (Adicionar certificado).



8. Navegar para **Configuration > Remote Access VPN > Advanced** e escolha **SSL Settings.**
9. Em certificados, escolha a interface usada para encerrar sessões de WebVPN. Neste exemplo, a interface externa é usada.
10. Clique em **Edit**.
11. Na lista suspensa Certificate (Certificado), escolha o certificado recém-instalado.



12. Clique emOK.
13. Clique emApply. O novo certificado agora é utilizado para todas as sessões WebVPN terminadas na interface especificada.

2.2 Instalação de um certificado PKCS12 com a CLI

```
  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-----
MIISNwIBAzCCEfEGCSqGSIb3DQEHAaCCEeIEghHeMIIR2jCCEdYGCSqGSIb3DQEH
BqCCEccwghHDAgEAMIIRvAYJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIWO3D
hDti/uECAQGAghGQ9ospee/qtIbVZh2T8/Z+5dxRPBcStDTqyKy7q3+9ram5AZdG
Ce9n5UCckqT4WcTjs7XZtCrUrt/LkNbmGDVhwGBmYWiOS7npgaUq0eoqiJRK+Yc7
LN0nbho6I5WfL56/JiceAMlXDLr/IqqLg2QAApGdN+F5vANsHse2GsAATewBDLt7
Jy+SKfoNvvIw9QvzCiUzMjYZBANmBdMCQ13H+YQTHitT3vn2/iCDlzRSuXcqypEV
q5e3heiOO75lE8TDLWmO3PMvwIZqi8yzWesjcTt1Kd4FoJBZpB70/v9LntoIUOY7
kIQM8fHb4ga8BYfbgRmG6mkMmO1STtbSvlvTa19WTmdQdTyCa+G5PkrryRsy3Ww1
lkGFMhImmrnNADF7HmzbyslVohQZ7h09iVQY9krJogoXHjmQYxG9brf0oEwxSJDa
mGDhhESh+s/WuFSV9Z9kiTXpJNZxpTASoWBQrrwmO5v8ZwbjbVNJ7sVdbwpUl6d+
NNFGR7LTqO8hpupeeJnY9eJc2yYqeAXWXQ5kLOZo6/gBEdGtEaZBgCFK9JZ3bl3A
xqxGifanWPnLYG611NKuNjTgbjhnEEYI2uZzU0qxnlKa8zyXw+lzrKuJscDbkAPZ
wKtw8K+p4OzXVHhuANo6MDvffNRY1KQDtyK1inoPH5ksVSE5awkVam4+HTcqEUfa
16LMana+4QRgSetJhU0LtSMaQfRJGkha4JLq2t+JrCAPz2osARlTsBOjQBNq6YNj
0uB+gGk2Gl8Q5Nln6K1fz0XBFZLWEDBLsaBRO5MAnE7wWtO0+4awGYqVdmIF1lkf
XIRKAiQEr1pZ6BVPuvsCNJxaaUHzufhYI2ZAckasKBZOT8/7YK3fnAaGoBCz4cHa
o2EEQhq2aYb6YTv0+wtLEWGHzsbGZEM/u54XmsXAI7g28LGJYdfWi509KyV+Ac1V
KzHqXZMM2BbUQCNcTF5JIMiW+r62k42FdahfaQb0vJsIe/IwkAKG7y6DIQFs0hwg
ZlPXiDbNr1k4e8L4gqupMKWg853PY+oY22rLDC7bul1CKtixIYBCvbn7dAYsI4GQ
```

l6xXhNu3+iye0HgbUQQCfTU/mBrA0ZO+bpKjWOCfqNBuYnZ6kUEdCI7GFLH9QqtM
K7YinFLoHwTWbi3MsmqVv+Z4ttVWy7XmikoO2nMynJMP6/CNV8OMxMKdC2qm+c1j
s4QlKcAmFsQmNp/7SIP1wnvOc6JbUmC1O520U/r8ftTzn8C7WL62W79cLK4HOr7J
sNsZnOz0JOZ/xdZT+cLTCtVevKJOQMK3vMsiOuy52FkuF3HnfrmBqDkbR7yZxELG
RCEL0EDdbp8VP0+IhNlyz1q7975SscdxFSL0TvjnHGFWd14ndoqN+bLhWbdPjQWV
l3W2NCI95tmHDLGgp3P0OlS+RjdCEGGMg+9cpgBfFC1JocuTDIEcUbJBY8QRUNiS
/ubyUagdzUKt1ecfb9hMLP65ZNQ93VIw/NJKbIm7b4P/1Zp/lFP5eq7LkQPAxE4/
bQ4mHcnwrs+JGFkN19B8hJmmGoowH3p4IEvwZy7CThB3E1ejw5R4enqmrgvHqpQe
B7odN1OFLAHdo1G5BsHExluNEsEb4OQ0pmKXidDB5B001bJsr748fZ6L/LGx8Al3
<snip>
ijDqxyfQXY4zSytljSMwMtYA9hG5I79Sg7pnME1E9xq1DOoRGg8vgxlwiciKtLxp
LL0ReDY31KRYv00vW0gf+tE7lST/3TKZvh0sQ/BE0V3kHnwldejMFH+dvyAA9Y1E
c8O+tdafBFX4B/HP46E6heP6ZSt0xAfRW1/JF4ljNvUNVO9VtVfR2FTyWpzZFY8A
GG5XPIA80WF6wKEPFHIcN8scY+Vot8kXxG96hwt2Cm5NQ2OnVzxUZQbpKsjs/2jC
3HVFe3UJFBsY9UxTLcPXYBSIG+VeqkI8hWZp6clTfNDLY2ELDylQzp1mBg2FujZa
YuE0avjCJzBzZUG2umtS5mHQnwPF+XkOujEyhGMauhGxHp4nghSzrUZrBeuL9lUF
2mbpsOcgZkzxMS/rjdNXjCmPFloRBvKkZSlxHFrE/5ZopAhn4i7YtHQNrz9U4RjQ
xo9cUuaJ+LNmvzE8Yg3epAMYZ16UNGQQkVQ6ME4BcjRONzW8BYgTq4+pmT1ZNq1P
X87CXCPtYRpHF57eSo+tHDINCgfqYXD6e/7r2ngfiCeUeNDZ4aVl2XxvZDaUlBPP
Tx5fMARqx/Z8BdDyBJDVBjdsxmQau9HLkhPvdfGlZIWdTe13CzKqXA5Ppmpjt4q9
GnCpC53m76x9Su4ZDw6aUdBcgCTMvfaqJC9gzObee2Wz+aRRwzSxu6tEWVZolPEM
v0AA7po3vPeklgOnLRAwEoTTn4SdgNLWeRoxqZgkw1FC1GrotxF1so7uA+z0aMeU
lw73reonsNdZvRAcVX3Y6UNFdyt70Ixvo1H4VLzWm0K/oP62C9/eqqMwZ8zoCMPt
ENna7T+7Os66SCbMmXCHwyhO0tygNKZFFw/AATFyjqPMWPAxGuPNOrnB6uYCn0Hk
1BU7tF143RNIZaQQEH3XnaPvUuAA4C0FCoE3h+/tVjtfNKDvFmb6ZLZHYQmUYpyS
uhdFEpoDrJH1VmI2Tik/iqYWaZ+oDqXPHQXnJhw25h9ombR4qnD+FCfwFCGtPFON
o3QffZ53C95n5jPHVMyUrOxDdpwnvzCQPdj6yQm564TwLAmiz7uDlpqJZJe5QxHD
nolv+4MdGSfVtBq+ykFoVCaamqeaq6sKgvAVujLXXEs4KEmIgcPqATVRG49ElndI
LO1DEQyKhVoDGebAuVRBjzwAm/qxWxxFv3hrbCjpHCwEYms4Wgt/vKKRFsuWJNZf
efHldwlltkd5dKwSvDocPT/7mSLtLJa94c6AfgxXy9zO+FTLDQwzxga7xC2krAN1
yHxR2KHN5YeRL+KDzu+u6dYoKAz+YAgwlW6KbeavALSuH4EYqcvg8hUEhp/ySiSc
RDhuygxEovIMGfES4FP5V52lPyDhM3Dqwhn0vuYUmYnX8EXURkay44iwwI5HhqYJ
lptWyYo8Bdr4WNwt5xqszGzYR6mmGeAIin7bDunsF1uBHWYF4dyKlz1tsdRNMYqQ
+W5q+QjVdrjldWv/bMFOaqEjxeNWBRqjzcff3BxMnwvVxtgqxFvRh+DZxiJoiBG+
yx7x8np2AQ1r0METSSxbnZzfnKZKVvBVMkIC6Jsmt2WEVTQvoFJ8em+nemOWgTi/
hHSBzjE7RhAucnHuifOCXOgvR1SDDqyCQbiduc1QjXN0svA8Fqbea9WEH5khOPv3
pbtsL4gsfl2pv8diBQkVQgiZDi8Wb++7PR6ttiY65kVwrdsoNl1/qq+xWOd3tB4/
zoH9LEMgTy9Sz7myWrB9EOOZ8BIjL1M8oMigEYrTDOc3KbyW1S9dd7QAxiuOBaX1
8J8q1OydvTBzmqcjeSsFH4/1NHn5VnfOZnNpui4uhpOXBG+K2zJUJXm6dq1AHBlE
KQFsFZpNNyave0Kk8JzQnLAPd7OUU/IksyOCGQozGBH+HSzVp1RDjrrbC342rkBj
wnI+j+/1JdWBmHdJMZCfoMZFLSI9ZBqFirdii1/NRu6jh76TQor5TnNjxIyNREJC
FE5FZnMFvhM900LaiUZff8WWCOfeRDMttLXb1nuxPFl+lRk+LNlPLVptWgcxzfsr
JXrGiwjxybBB9oCOrACq8fGAtEs8WRxJyDH3Jjmn9i/Gl6J1mMCUF//LxAH2WQx8
Ld/qS5OM2iFCffDQjxAj0K6DEN5pUebBv1Em5SOHXvyq5nxgUh4/y84CWaKjw0MQ
5tbbLMlnc7ALIJ9LxZ97YiXSTyeM6oBXBFx6RpklkDv05mlBghSpVQiMcQ2ORIkh
UVVNbSHOl9S3cb5wqxaWqAKBqb4h1uLGVbYWZf2mzLZ8U5U5ioiqoMBqNZbzTXpO
EqEFuatTllQvCRbcKS3xou4MAixcYUxKwEhbZA/6hd10XSBJwe7jKBV9M6wliKab
UfoJCGTAf3sY68lqrMPrbBt0eeWf1C02Sd9Mn+V/jvnil7mxYFFUpruRq3r1LeqP
J5camfTtHwyL8N3Q/Zwp+zQeWZiLA8a/iAVu/hYLR1bpF2WCK0lOtJqkvVmrLVLz
maZZjbJeOft5cP/lRxbKlS6Gd5dFTEKDE15c6gWUX8RKZP6Q7iaE5hnGmQjm8Ljl
kXwF+ivoxOQ8a+Gg1bVTROc7tqW9e9/ewisV1mwvEB6Ny7TDS1oPUDHM84pY6dqi
1+Oio07Ked4BySwNlYy9yaJtBTZSCstfP+ApLidN7pSBvvXf1aHmeNbkPOZJ+c+t
fGpUdL6V2UTXfCsOPHTC0ezA15sOHwCuPchrDIj/eGUwMS3NfS25XgcMuvnLqGVO
RzcRzlZIg8G0oLYwOCuzoY0D/m9010O1ahePyA9tmVB7HRRbytLdaW7gYeEikoCv
7qtBqJFF17ntWJ3EpQHZUcVClbHIKqjNqRbDCY7so4AlIW7kSEUGWMIUDhprE8Ks
NpnvPH2i9JrYrTeROyUI0tL/7SATd2P0a2lxz/zUWekeqd0bmVCsAgQNbB2XkrR3
XS0B52ol+63e8KDqS2zL2TZd3daDFidHlB8QB26tfbfOAcaObJH5/dWP8ddo8UYo
Y3JqTl0malxSJhaMHmQdZIQp49utW3TcjqGllYS4HEmcqtHud0ShaUysC6239jlQ
KlFWrwXTlBC5vnq5IcOMqx5zyNbfxXz28969cWoMCyU6+kRw0TyF6kF7EEv6XWca
XLEwABx+tKRUKHJ673SyDMu96KMV3yZN+RtKbCjqCPVTP/3ZeIp7nCMUcj5sW9HI
N34yeI/0RCLyeGsOEiBLkucikC32LI9ik5HvImVTELQ0Uz3ceFqU/PkasjJUve6S
/n/1ZVUHbUk71xKR2bWZgECl7fIel7wlrbjpF3Wbk+Er0kfYcsNRHxeTDpKPSt9s
u/UsyQJiyNARG4X3iYQlsTce/06Ycyri6GcLHAu58B02nj4CxolCplABZ2N79HtN
/7Kh5L0pS9MwsDCHuUI8KFrTsET7TB1tIU99FdB19L64sl/shYAHbccvVWU50Wht

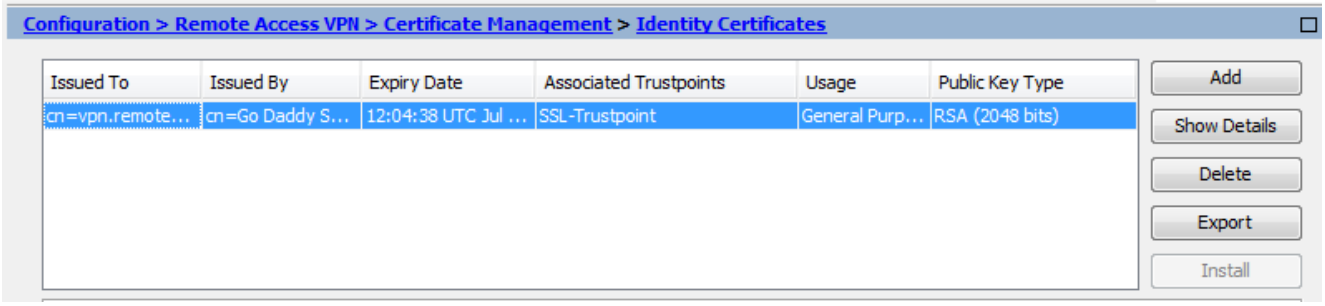
```
PdLoaErrX81Tof41IxbSZbI8grUC4KfG2sdPLJKu3HVTeQ8LfllbBLxfs8ZBS+Oc
v8rHlQ012kY6LsFGLehJ+/yJ/uvXORiv0ESp4EhFpFfkp+o+YcFeLUUPd+jzb62K
HfSCCbLpCKyEay80dyWkHfgylqxmb9ud0oMO50aFJyqR0NjNt6pcxBRY2A6AJR5S
IIC26YNwbh0GjF9qL2FiUqnNH/7GTqPnd2qmsB6FTIwSBT6d854qN7PRt+ZXgdtQ
OjcYt1r9qpWDZpNFK8EzizwKiAYTsiEh2pzPt6YUpksRb6CXTkIzoG+KLsv2m3b8
OHyZ9a8z81/gnxrZlls5SCTfOSU70pHWh8VAYKVHHK+MWgQr0m/2ocV32dkRBLMy
2R6P4WfHyI/+9de1x3PtIuOiv2knpxHv2fKM6sQw45F7XkmwHxjq1YRJ6vIwPTAh
MAkGBSsOAwIaBQAEFFTRETzpisHKZR+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
```

Verificar

Use estas etapas para verificar a instalação bem-sucedida do certificado de fornecedor terceirizado e use-as para conexões SSLVPN.

Exibir certificados instalados via ASDM

1. Navegar para**Configuration > Remote Access VPN > Certificate Management,**e escolha **Identity Certificates.**
2. O certificado de identidade emitido pelo fornecedor terceirizado é exibido.



Exibir certificados instalados através da CLI

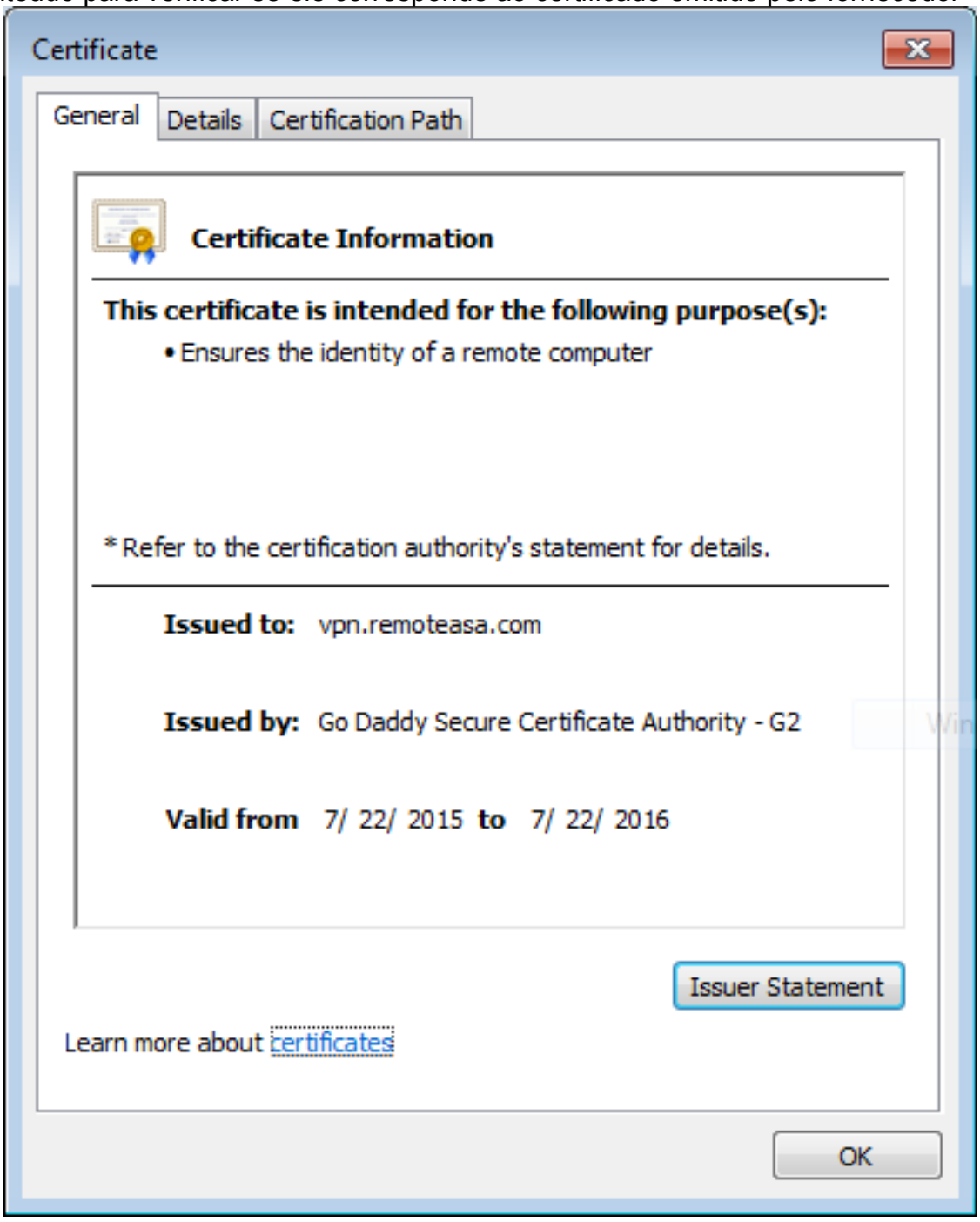
```
 MainASA(config)# show crypto ca certificate

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=vpn.remoteasa.com
    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)
```

Verificar o certificado instalado para WebVPN com um navegador da Web

Verifique se o WebVPN usa o novo certificado.

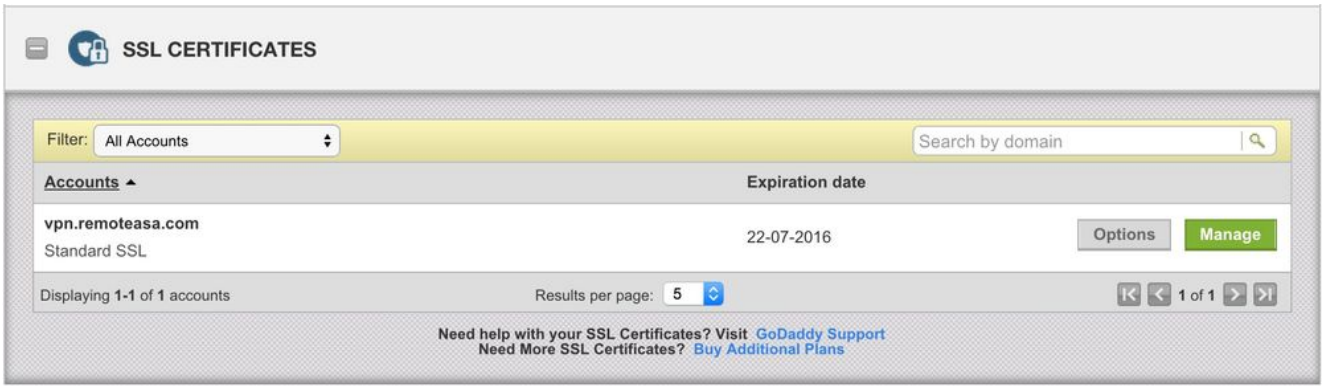
1. Conecte-se à interface WebVPN por meio de um navegador da Web. Use https:// junto com o FQDN usado para solicitar o certificado (por exemplo, https://vpn.remoteasa.com).
2. Clique duas vezes no ícone de cadeado exibido no canto inferior direito da página de login do WebVPN. As informações de certificado instaladas devem ser exibidas.
3. Revise o conteúdo para verificar se ele corresponde ao certificado emitido pelo fornecedor terceirizado.



Renovar certificado SSL no ASA

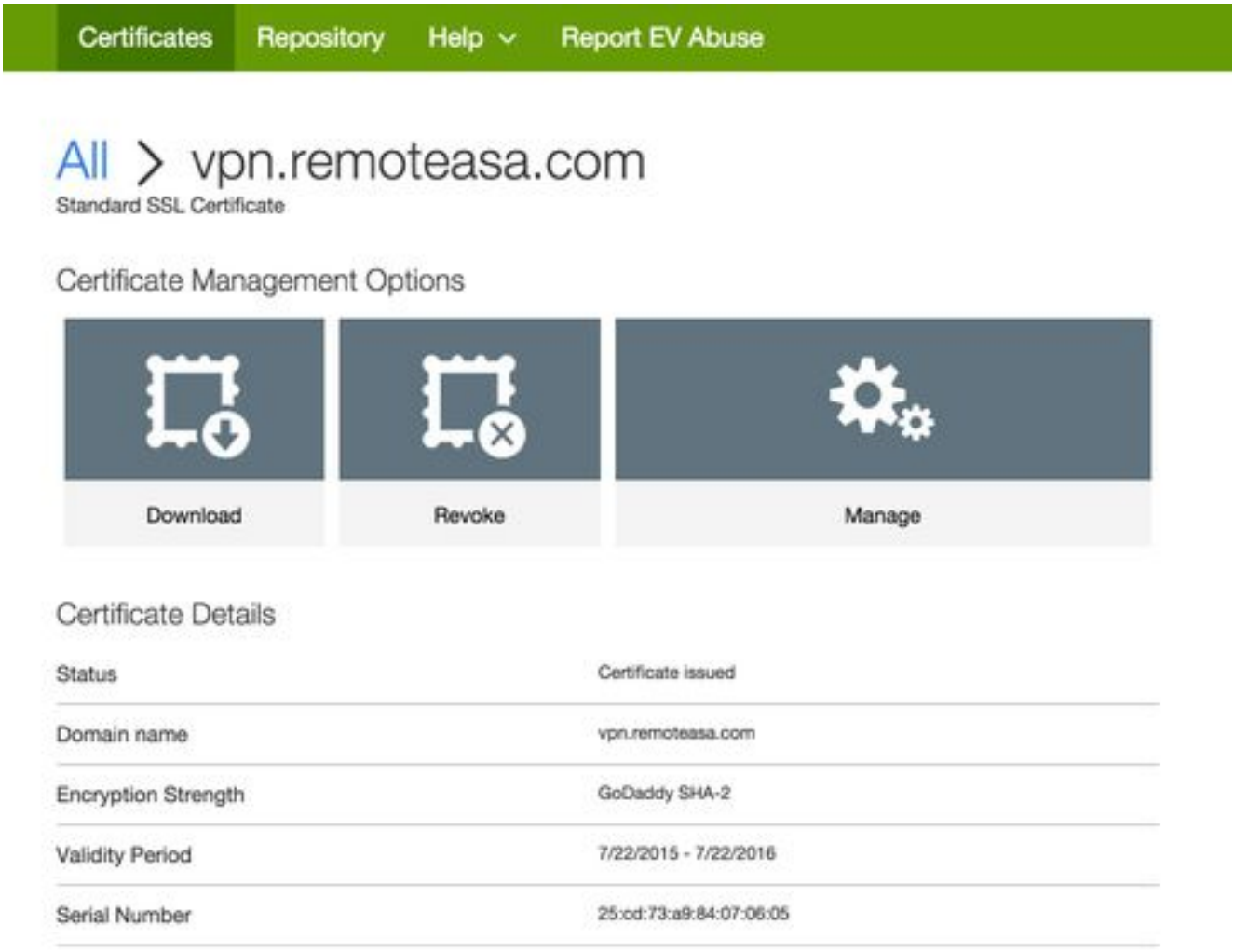
1. Gere novamente o CSR no ASA ou com OpenSSL ou na CA usando os mesmos atributos do certificado antigo. Siga as etapas fornecidas em Geração do CSR.
2. Envie o CSR na CA e gere um novo certificado de identidade no formato PEM (.pem, .cer, .crt) juntamente com o certificado CA. No caso de um certificado PKCS12, também haverá uma nova chave privada. No caso da CA GoDaddy, o certificado pode ser recodificado com

um novo CSR gerado.Acesse o GoDaddyaccount e clique em **Manage (Gerenciar)** em certificados
SSL.

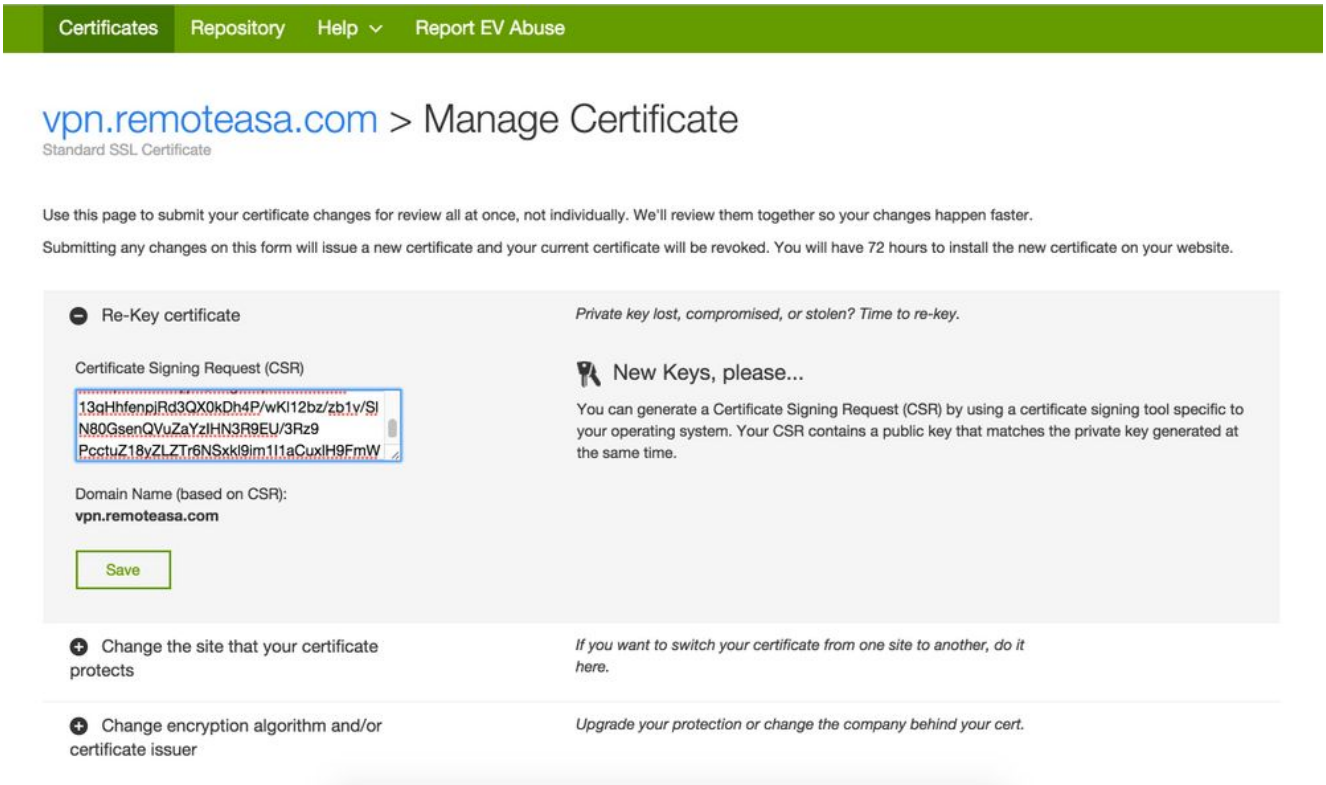


Clique **View Status** (Exibir status) para o nome de domínio necessário.

Clique em **Gerenciar** para fornecer opções para digitar novamente o certificado.



Expanda a opção **Re-key certificate** (Certificado de nova chave) e adicione o novo CSR.



Salve e prossiga para a próxima etapa. O GoDaddy emitirá um novo certificado com base no CSR fornecido.

3. Instale o novo certificado em um novo trustpoint, como mostrado na instalação do certificado SSL na seção ASA.

Perguntas mais freqüentes

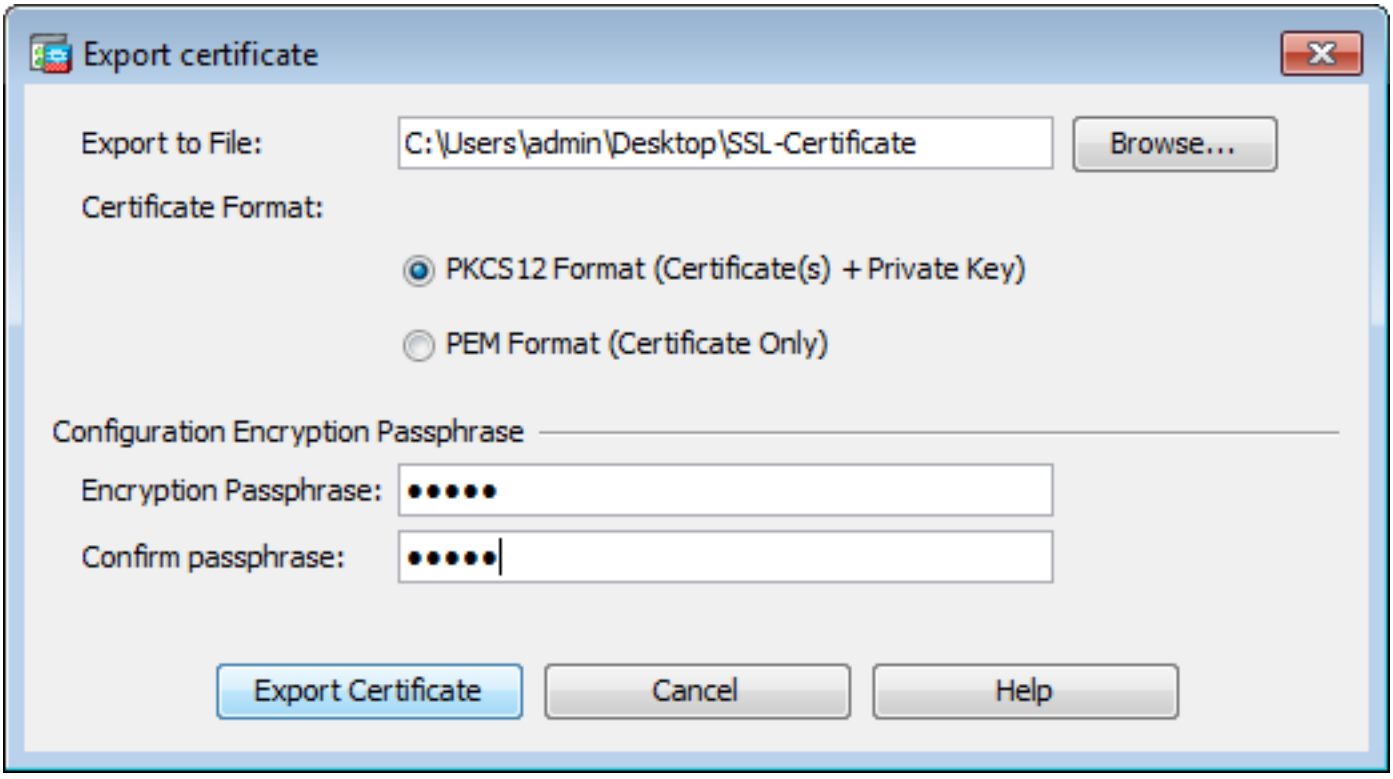
1. Qual é a melhor maneira de transferir certificados de identidade de um ASA para outro diferente?

Exporte o certificado juntamente com as chaves para um arquivo PKCS12.

Use esse comando para exportar o certificado por meio da CLI do ASA original:

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

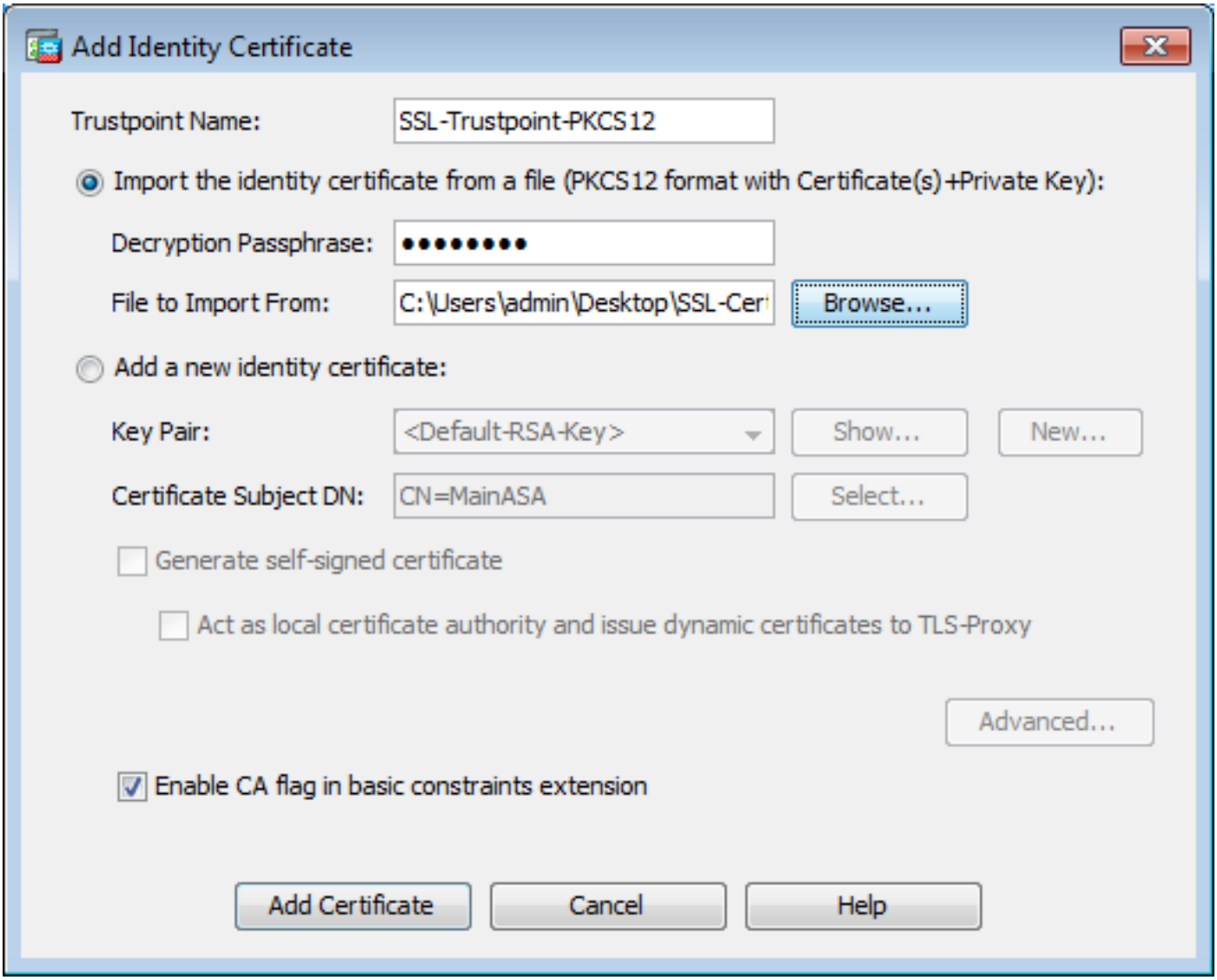
Configuração do ASDM correspondente:



Use esse comando para importar o certificado por meio da CLI do ASA de destino:

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

Configuração do ASDM correspondente:



Isso também pode ser feito pelo recurso de backup/restauração no ASDM com estas etapas:

1. Faça login no ASA via ASDM e escolha**Tools > Backup Configuration.**
2. Faça backup de todas as configurações ou apenas dos certificados de identidade.
3. No ASA de destino, abra o ASDM e escolha**Tools > Restore Configuration.**

2. Como gerar certificados SSL para uso com ASAs de balanceamento de carga de VPN?

Há vários métodos que podem ser usados para configurar os ASAs com certificados SSL para um ambiente de balanceamento de carga de VPN.

1. Use um único certificado de comunicação unificada/vários domínios (UCC) que tenha o FQDN de balanceamento de carga como o DN e cada um dos FQDNs do ASA, como um nome alternativo do assunto separado (SAN). Há várias CAs bem conhecidas como GoDaddy, Entrust, Comodo e outras que suportam esses certificados. Ao escolher esse método, é importante lembrar que o ASA atualmente não suporta a criação de um CSR com vários campos de SAN. Isso foi documentado no aprimoramento da ID de bug da Cisco CSCso70867. Nesse caso, há duas opções para gerar o CSR Via CLI ou ASDM. Quando o CSR é enviado para a CA, são adicionados os vários SANs no próprio portal da CA.Use o OpenSSL para gerar o CSR e incluir as várias SANs no arquivo

openssl.cnf.Depois que o CSR for enviado para a CA e o certificado gerado, importe o certificado PEM para o ASA que gerou o CSR. Depois de concluído, exporte e importe este certificado no formato PKCS12 para os outros ASAs membros.
2. Use um certificado curinga. Esse é um método menos seguro e flexível quando comparado ao uso de um certificado de UC. Caso a CA não ofereça suporte a certificados UC, um CSR será gerado na CA ou com o OpenSSL, onde o FQDN está na forma *.domain.com. Depois que o CSR for enviado para a CA e o certificado gerado, importe o certificado PKCS12 para todos os ASAs no cluster.
3. Use um certificado separado para cada membro ASAs e o para o FQDN de balanceamento de carga. Essa é a solução menos eficaz. Os certificados para cada um dos ASAs individuais podem ser criados conforme mostrado neste documento. O certificado para FQDN de balanceamento de carga de VPN será criado em um ASA e exportado e importado como um certificado PKCS12 para o outro ASAs.

3. Os certificados precisam ser copiados do ASA principal para o ASA secundário em um par de failover de ASA?

Não há necessidade de copiar manualmente os certificados do ASA principal para o secundário, pois eles devem ser sincronizados entre o ASAs, desde que o failover stateful esteja configurado. Se for a configuração inicial do failover, os certificados não serão vistos no dispositivo em standby, por isso, emita o comando write standby para forçar uma sincronização.

4. Se as chaves ECDSA forem usadas, o processo de geração de certificado SSL será diferente?

A única diferença na configuração é a etapa de geração do par de chaves, onde um par de chaves ECDSA será gerado em vez de um par de chaves RSA. O restante do endereço permanece o mesmo. O comando CLI para gerar chaves ECDSA é mostrado aqui:

```
 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...
```

Troubleshoot

Comandos para Troubleshooting

Esses comandos debug devem ser coletados na CLI no caso de uma falha na instalação do certificado SSL:

debug crypto ca 255

debug crypto ca messages 255

debug crypto ca transactions 255

Problemas comuns

Aviso de certificado não confiável ao usar um certificado SSL de terceiros válido na interface

externa no ASA executando o 9.4(1) e posterior.

Solução: Esse problema se apresenta quando um par de chaves RSA é usado com o certificado. Nas versões do ASA do 9.4(1) em diante, todas as ECDSAs e as cifras RSA são ativadas por padrão, e a cifra mais forte (geralmente uma cifra de ECDSA) será usada para negociação. Se isso acontecer, o ASA apresenta um certificado autoassinado em vez do certificado baseado em RSA configurado atualmente. Há uma melhoria no lugar para alterar o comportamento quando um certificado baseado em RSA é instalado em uma interface e é acompanhado pela ID de bug CSCuu02848.

Ação recomendada: Desativar cifras ECDSA com estes comandos 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"
```

Ou, com o ASDM, navegue para**Configuration > Remote Access VPN > Advanced**e escolha**SSL Settings**. Na seção Encryption, selecione tlsv1.2 **Cipher version** e edite-a com a string personalizada AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3-SHA:DA ES-CBC-SHA:RC4-SHA:RC4-MD5

Appendix

Apêndice A: ECDSA ou RSA

O algoritmo ECDSA é parte da criptografia de curva elíptica (ECC) e usa uma equação de uma curva elíptica para gerar uma chave pública, enquanto o algoritmo RSA usa o produto de dois primes, mais um número menor para gerar a chave pública. Isso significa que, com o ECDSA, o mesmo nível de segurança que o RSA pode ser obtido, mas com chaves menores. Isso reduz o tempo de computação e aumenta os tempos de conexão para sites que usam certificados ECDSA.

O documento em Criptografia de última geração e o ASA fornece informações mais detalhadas.

Apêndice B: Use o OpenSSL para gerar um certificado PKCS12 de um certificado de identidade, certificado de CA e chave privada

1. Verifique se o OpenSSL está instalado no sistema no qual esse processo está sendo executado. Para usuários do Mac OSX e GNU/Linux, ele será instalado por padrão.
2. Alterne para um diretório de trabalho. No Windows: Por padrão, os utilitários são instalados em C:\Openssl\bin. Abra um prompt de comando neste local.No Mac OSX/Linux: Abra a janela do terminal no diretório necessário para criar o certificado PKCS12.
3. No diretório mencionado na etapa anterior, salve a chave privada (privateKey.key), o certificado de identidade (certificado.crt) e os arquivos de cadeia de certificado de CA raiz (CACert.crt). Combine a chave privada, o certificado de identidade e a cadeia de certificado de CA raiz em um arquivo PKCS12. Insira uma senha para proteger seu certificado PKCS12.
   ```
   strong> openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in
   certificate.crt -certfile CACert.crt
   ```
4. Converta o certificado PKCS12 gerado em um certificado codificado Base64:
   openssl base64 -in certificate.pfx -out certificate.p12

Em seguida, importe o certificado que foi gerado na última etapa para uso com SSL.

Informações Relacionadas

- Guia de configuração do ASA 9.x - Configuração de certificados digitais
- Como obter um certificado digital de uma CA do Microsoft Windows usando o ASDM em um ASA
- **Suporte Técnico e Documentação - Cisco Systems**