Configuración de ASA: instalación y renovación de certificados digitales SSL

Contenido

Introducción

En este documento se describe la instalación del certificado digital SSL de confianza de terceros en el ASA para las conexiones Clientless SSLVPN y AnyConnect.

Antecedentes

En este ejemplo se utiliza un certificado de GoDaddy. Cada paso contiene el procedimiento Adaptive

Security Device Manager (ASDM) y la CLI equivalente.

Prerequisites

Requirements

Este documento requiere acceso a una entidad emisora de certificados (CA) de terceros de confianza para la inscripción de certificados. Algunos ejemplos de proveedores de CA de terceros son, entre otros, Baltimore, Cisco, Entrust, Geotrust, G, Microsoft, RSA, Thawte y VeriSign.

Antes de comenzar, verifique que el ASA tenga la hora del reloj, la fecha y la zona horaria correctas. Con la autenticación de certificados, se recomienda utilizar un servidor de protocolo de tiempo de la red (NTP) para sincronizar la hora en el ASA. La Guía de Configuración de CLI de Operaciones Generales de la Serie ASA de Cisco, 9.1, detalla los pasos a seguir para configurar la hora y la fecha correctamente en el ASA.

Componentes Utilizados

Este documento utiliza un ASA 5500-X que ejecuta la versión de software 9.4.1 y la versión de ASDM 7.4(1).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

El protocolo SSL exige que el servidor SSL proporcione al cliente un certificado de servidor para que el cliente realice la autenticación del servidor. Cisco no recomienda el uso de un certificado autofirmado debido a la posibilidad de que un usuario pueda configurar inadvertidamente un navegador para confiar en un certificado de un servidor no autorizado. También existe la molestia para los usuarios de tener que responder a una advertencia de seguridad cuando se conecta al gateway seguro. Se recomienda utilizar CA de terceros de confianza para emitir certificados SSL al ASA con este fin.

El ciclo de vida de un certificado de terceros en ASA se lleva a cabo básicamente con estos pasos:

Generación de CSR

La generación de CSR es el primer paso en el ciclo de vida de cualquier certificado digital X.509.

Una vez generado el par de claves privado/público Rivest-Shamir-Adleman (RSA) o algoritmo de firma digital de curva elíptica (ECDSA) (el apéndice A detalla la diferencia entre el uso de RSA o ECDSA), se crea una solicitud de firma de certificado (CSR).

Un CSR es un mensaje con formato PKCS10 que contiene la clave pública y la información de identidad del host que envía la solicitud. Formatos de datos PKI explica los diferentes formatos de certificado aplicables a ASA y Cisco IOS®.

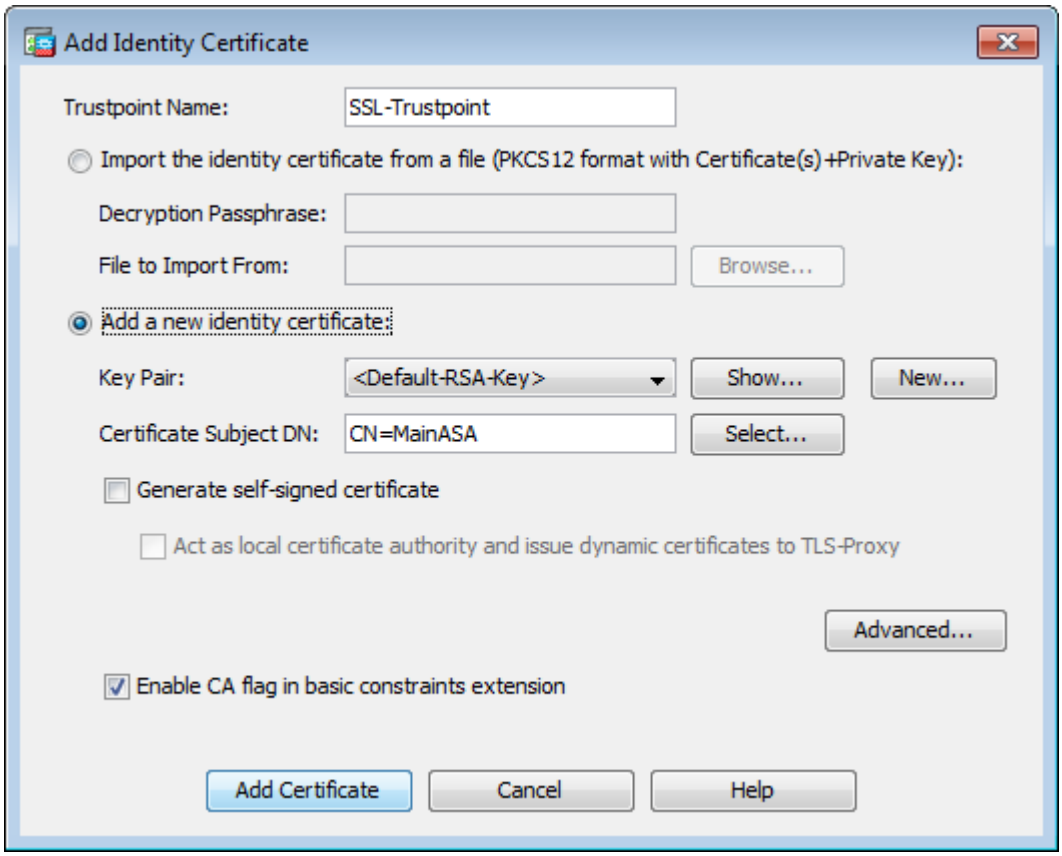
Notas:
1. Verifique con la CA el tamaño de par de claves requerido. El foro de CA/navegador ha establecido que todos los certificados generados por sus CA miembro tengan un tamaño mínimo de 2048 bits.
2. Actualmente, ASA no admite claves de 4096 bits (Id. de error de Cisco CSCut53512) para la autenticación del servidor SSL. Sin embargo, IKEv2 sí admite el uso de certificados de servidor de 4096 bits solo en las plataformas ASA 5580, 5585 y 5500-X.
3. Utilice el nombre DNS del ASA en el campo FQDN del CSR para evitar las advertencias de certificado no confiable y pasar la verificación de certificado estricto.

Existen tres métodos para generar CSR.

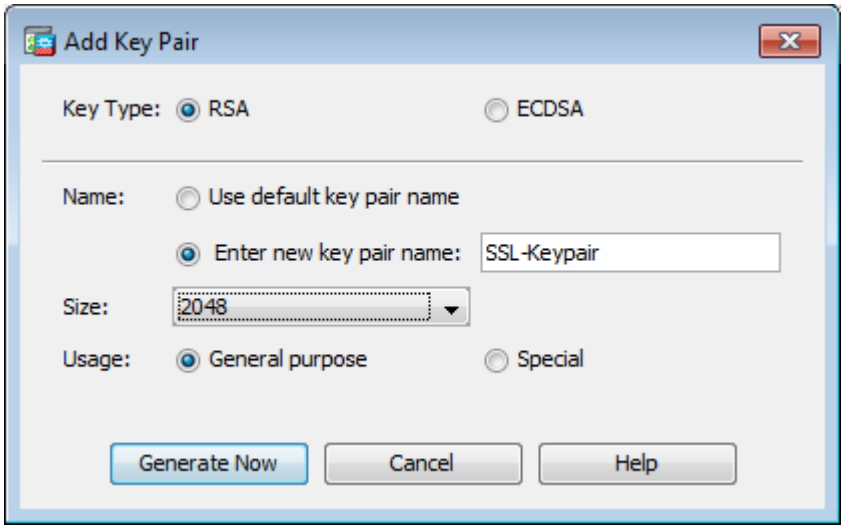
- Configuración con ASDM
- Configuración con ASA CLI
- Utilice OpenSSL para generar el CSR

1. Configure con el ASDM

1. Desplácese hasta **Configuration > Remote Access VPN > Certificate Management**y elija **Identity Certificates.**
2. Haga clic en **Add.**



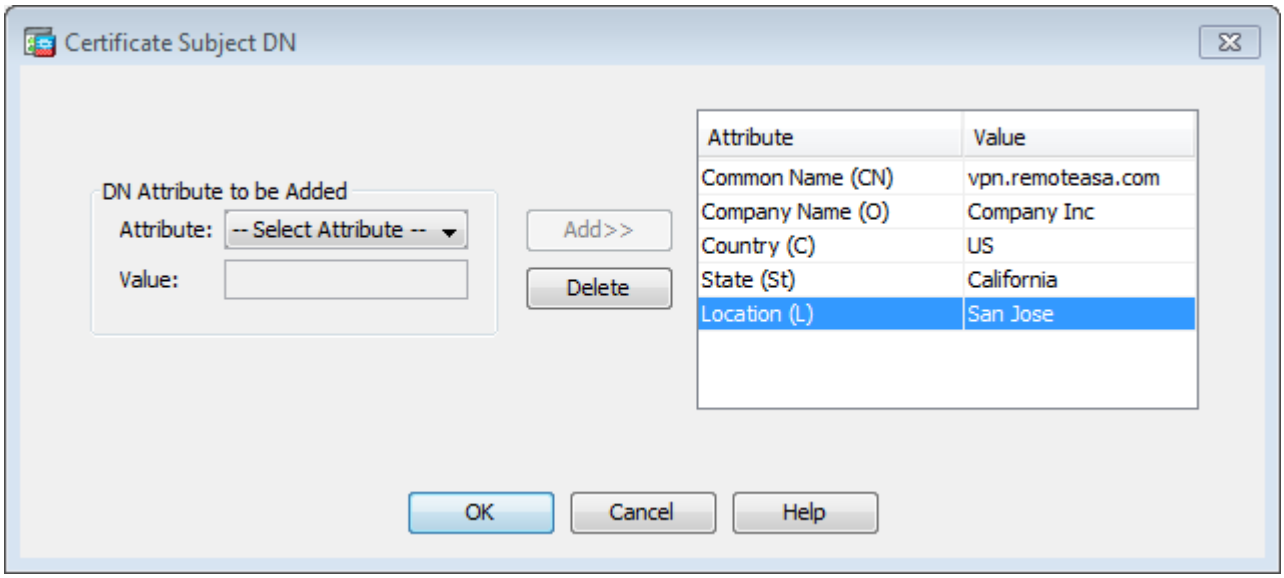
3. Defina un nombre de punto de confianza en el campo de entrada Nombre de punto de confianza.
4. Haga clic en el**Add a new identity certificate**botón de opción.
5. Para el par de claves, haga clic en**New**.



6. Elija el tipo de clave: RSA o ECDSA. (Consulte el Apéndice A para conocer las diferencias.)
7. Haga clic en el**Enter new key pair name**botón de opción. Identifique el nombre del par de claves con fines de reconocimiento.
8. Elija el**Key Size**. Elegir**General Purpose for Usage** con RSA.
9. Haga clic en**Generate Now**. Se creará el par de claves.
10. Para definir el DN de asunto de certificado, haga clic en**Select**y configure los atributos enumerados en esta tabla:

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

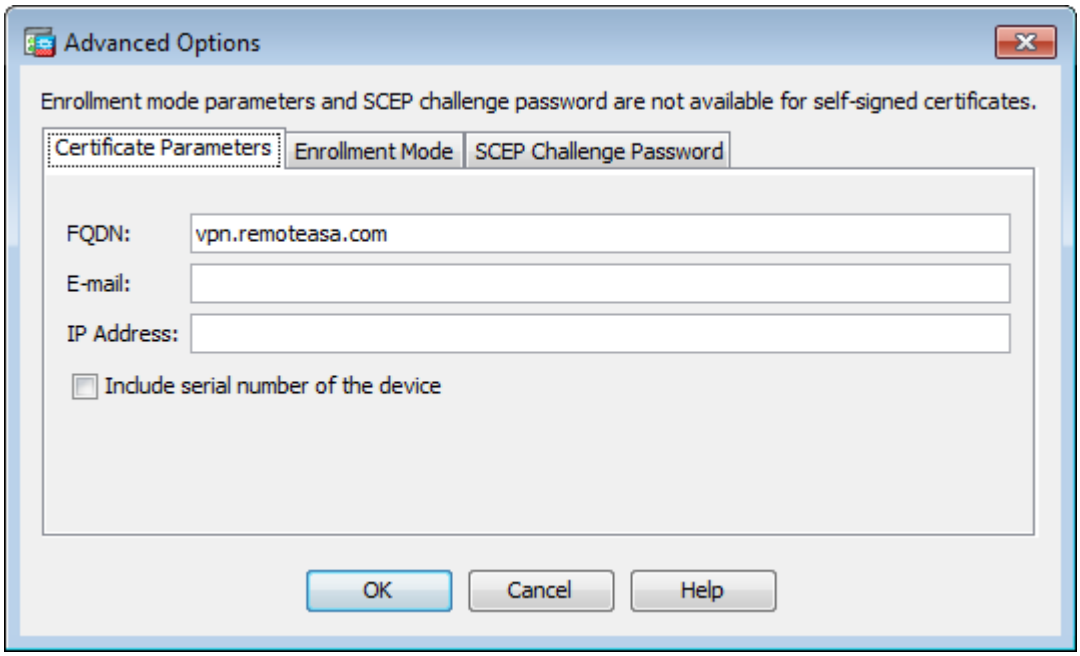
Para configurar estos valores, elija un valor de la lista desplegable **Atributo**, introduzca el valor y haga clic en **Agregar**.



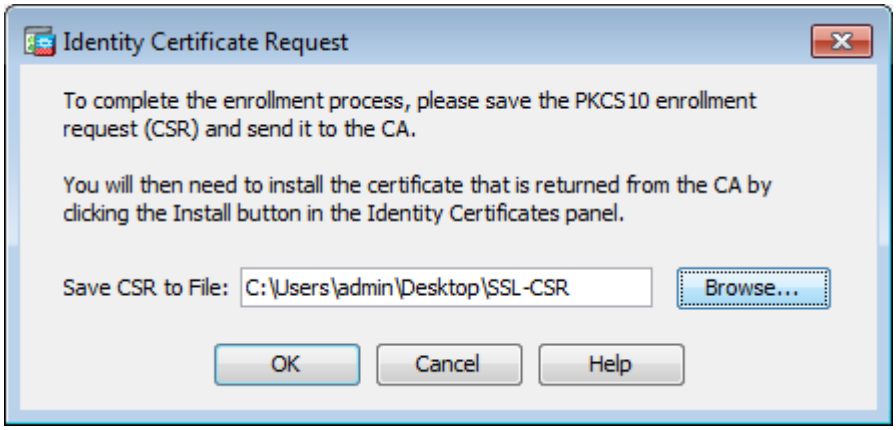
Nota: algunos proveedores externos requieren que se incluyan atributos específicos antes de emitir un certificado de identidad. Si no está seguro de cuáles son los atributos necesarios, consulte al proveedor para obtener más información.

---

11. Una vez agregados los valores adecuados, haga clic en**OK**. Aparecerá el cuadro de diálogo Agregar certificado de identidad con el certificado**Subject DN** field populated.
12. Haga clic en **Advanced**.



13. En el**FQDN**introduzca el FQDN que se utiliza para acceder al dispositivo desde Internet. Haga clic en**OK**.
14. Deje marcada la opción Habilitar CA en la extensión de restricciones básicas. Los certificados sin el indicador de CA ahora no se pueden instalar en ASA como certificados de CA de forma predeterminada. La extensión de restricciones básicas identifica si el sujeto del certificado es una CA y la profundidad máxima de las rutas de certificación válidas que incluyen este certificado. Desactive la opción para omitir este requisito.
15. Haga clic en**OK**y, a continuación, en**Add Certificate.** Se muestra un mensaje para guardar el CSR en un archivo en la máquina local.



16. Haga clic en**Browse**, elija una ubicación en la que guardar el CSR y guarde el archivo con la extensión .txt.

> **Nota**: Cuando el archivo se guarda con una extensión .txt, la solicitud PKCS#10 se puede abrir y ver con un editor de texto (como el Bloc de notas).

---

2. Configuración con la CLI de ASA

En el ASDM, el punto de confianza se crea automáticamente cuando se genera un CSR o cuando se instala el certificado de la CA. En la CLI, el punto de confianza se debe crear 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 trustpoint with attributes to be used on the SSL certificate

MainASA(config)#

crypto ca trustpoint SSL-Trustpoint

MainASA(config-ca-trustpoint)#

enrollment terminal

MainASA(config-ca-trustpoint)#

fqdn (remoteasavpn.url)

MainASA(config-ca-trustpoint)#

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

MainASA(config-ca-trustpoint)#

keypair SSL-Keypair

MainASA(config-ca-trustpoint)#

exit

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

MainASA(config)#

crypto ca enroll SSL-Trustpoint

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

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

yes

% Start certificate enrollment ..
% The subject name in the certificate is: subject-name CN=

(remoteasavpn.url)

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

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

(remoteasavpn.url)

```
,

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

no

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

yes

```
Certificate Request:
-----BEGIN CERTIFICATE REQUEST-----
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. Utilice OpenSSL para generar el CSR

OpenSSL hace uso del**OpenSSL config**para extraer los atributos que se utilizarán en la generación de CSR. Este proceso da como resultado la generación de una CSR y una clave privada.

> **Precaución**: compruebe que la **clave privada** generada no se comparte con nadie, ya que compromete la integridad del certificado.

---

1. Asegúrese de que OpenSSL está instalado en el sistema en el que se ejecuta este proceso. Para los usuarios de Mac OSX y GNU/Linux, se instala de forma predeterminada.
2. Cambie a un directorio funcional.

   En Windows: de forma predeterminada, las utilidades se instalan en **C:\Openssl\bin**. Abra un símbolo del sistema en esta ubicación.

   En Mac OSX/Linux: Abra la ventana Terminal en el directorio necesario para crear el CSR.

3. Cree un archivo de configuración de OpenSSL con un editor de texto con los atributos dados . Una

vez hecho esto, guarde el archivo como **openssl.cnf** en la ubicación mencionada en el paso anterior (Si tiene la versión 0.9.8h y posteriores, el archivo es**openssl.cfg**)
<#root>

```
[req]

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


[req_distinguished_name]

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

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

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

localityName = Locality Name (eg, city)
localityName_default = San Jose

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


[req_ext]

subjectAltName = @alt_names


[alt_names]

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

4. Genere la CSR y la clave privada con este 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]:
```

Envíe la CSR guardada al proveedor de CA de terceros. Una vez emitido el certificado, la CA proporciona el certificado de identidad y el certificado de CA que se instalará en el ASA.

Generación de certificados SSL en la CA

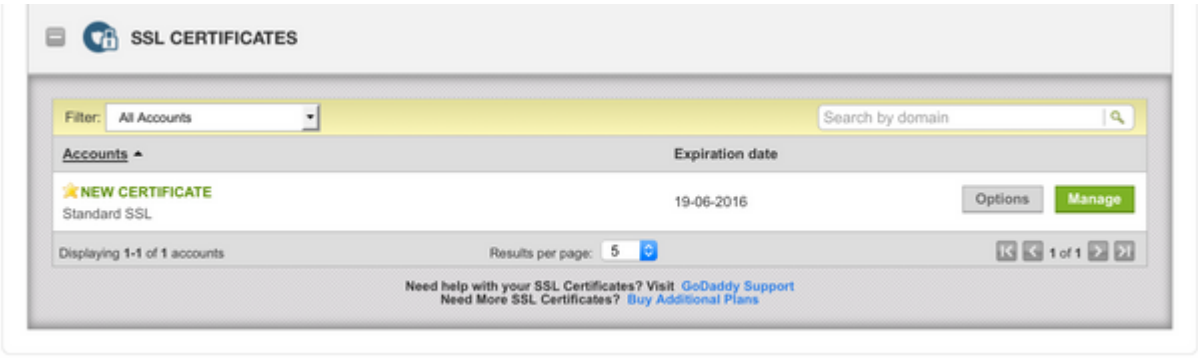
El siguiente paso es obtener la CSR firmada desde la CA. La CA proporciona un certificado de identidad codificado PEM recién generado o un certificado PKCS12 junto con el paquete de certificados de la CA.

Si el CSR se genera fuera del ASA (ya sea a través de OpenSSL o en la propia CA), el certificado de identidad codificado por PEM con la clave privada y el certificado de CA están disponibles como archivos independientes. El Apéndice B proporciona los pasos para agrupar estos elementos en un único archivo PKCS12 (formato .p12 o .pfx) .

En este documento, la CA de GoDaddy se utiliza como ejemplo para emitir certificados de identidad al ASA. Este proceso difiere en otros proveedores de CA. Lea detenidamente la documentación de CA antes de continuar.

Ejemplo de generación de certificados SSL en CA GoDaddy

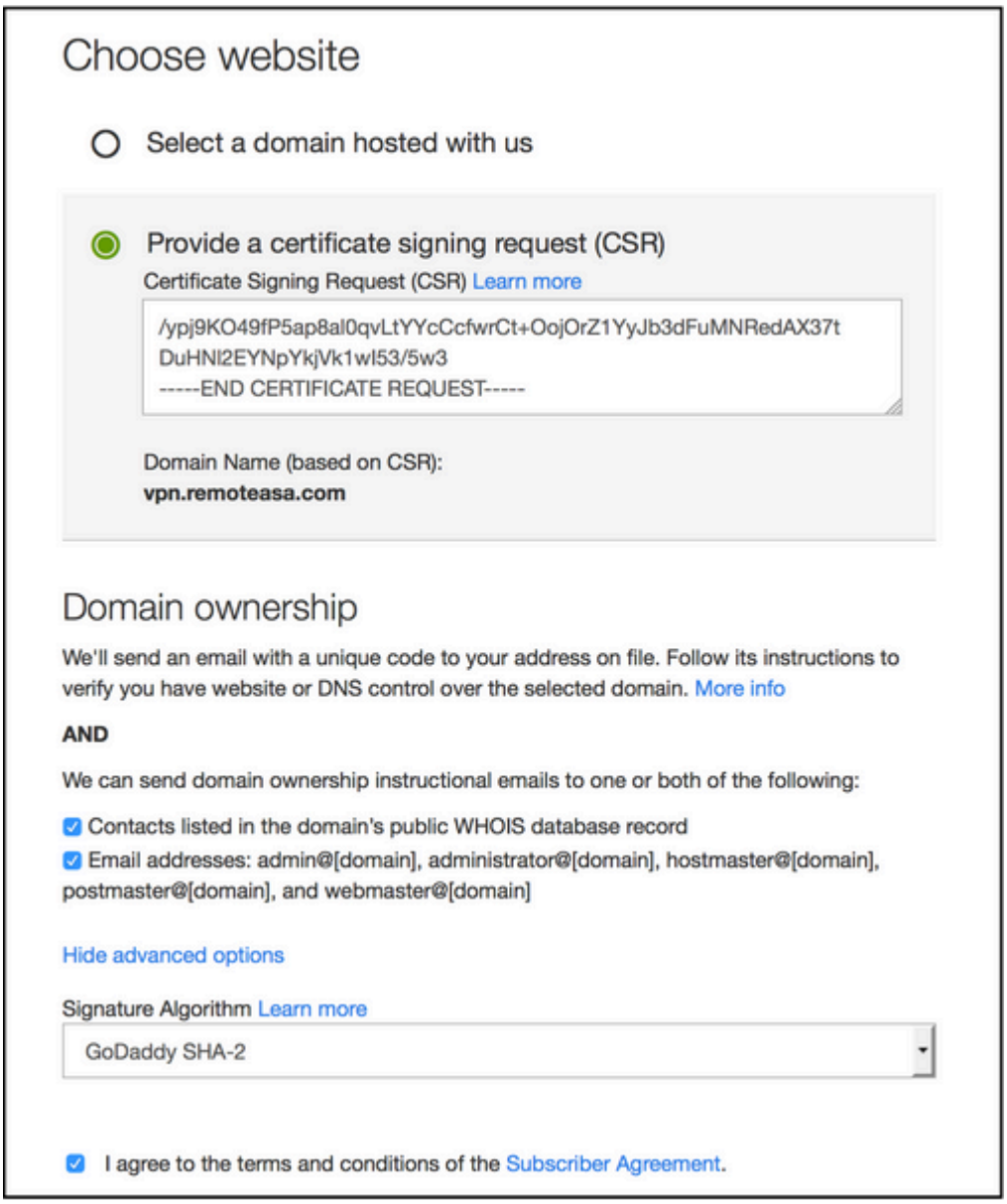
Después de la compra y de la fase de configuración inicial del certificado SSL, navegue hasta la cuenta de GoDaddy y vea los certificados SSL. Debe haber un nuevo certificado. Haga clic en**Manage** para continuar.



A continuación, se abre una página para proporcionar la CSR tal como se ve en esta imagen.

Según la CSR especificada, la CA determina el nombre de dominio al que se va a emitir el certificado.

Verifique que coincida con el FQDN del ASA.

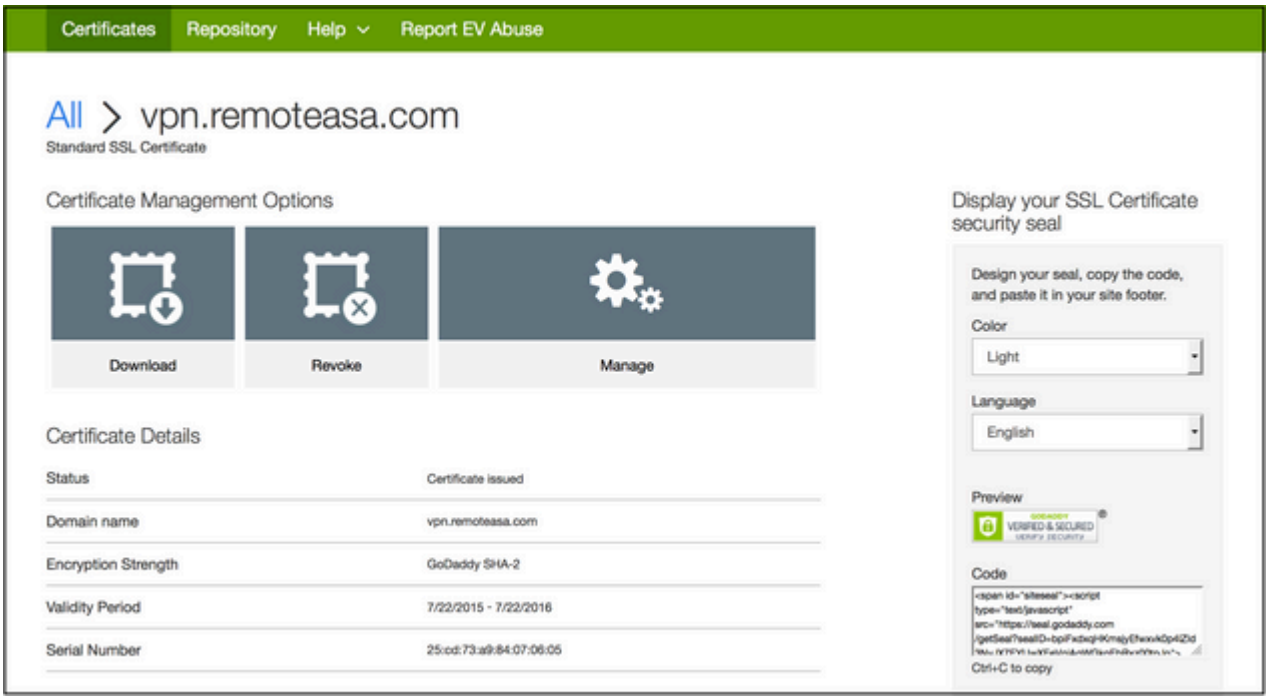


> **Nota**: GoDaddy y la mayoría de las demás CA utilizan SHA-2 o SHA256 como el algoritmo de firma de certificado predeterminado. ASA soporta el algoritmo de firma SHA-2 que comienza desde **8.2(5)** [versiones anteriores a 8.3] y **8.4(1)** [versiones posteriores a 8.3] en adelante (Id. de bug Cisco CSCti30937). Elija el algoritmo de firma SHA-1 si se utiliza una versión anterior a 8.2(5) u 8.4(1).

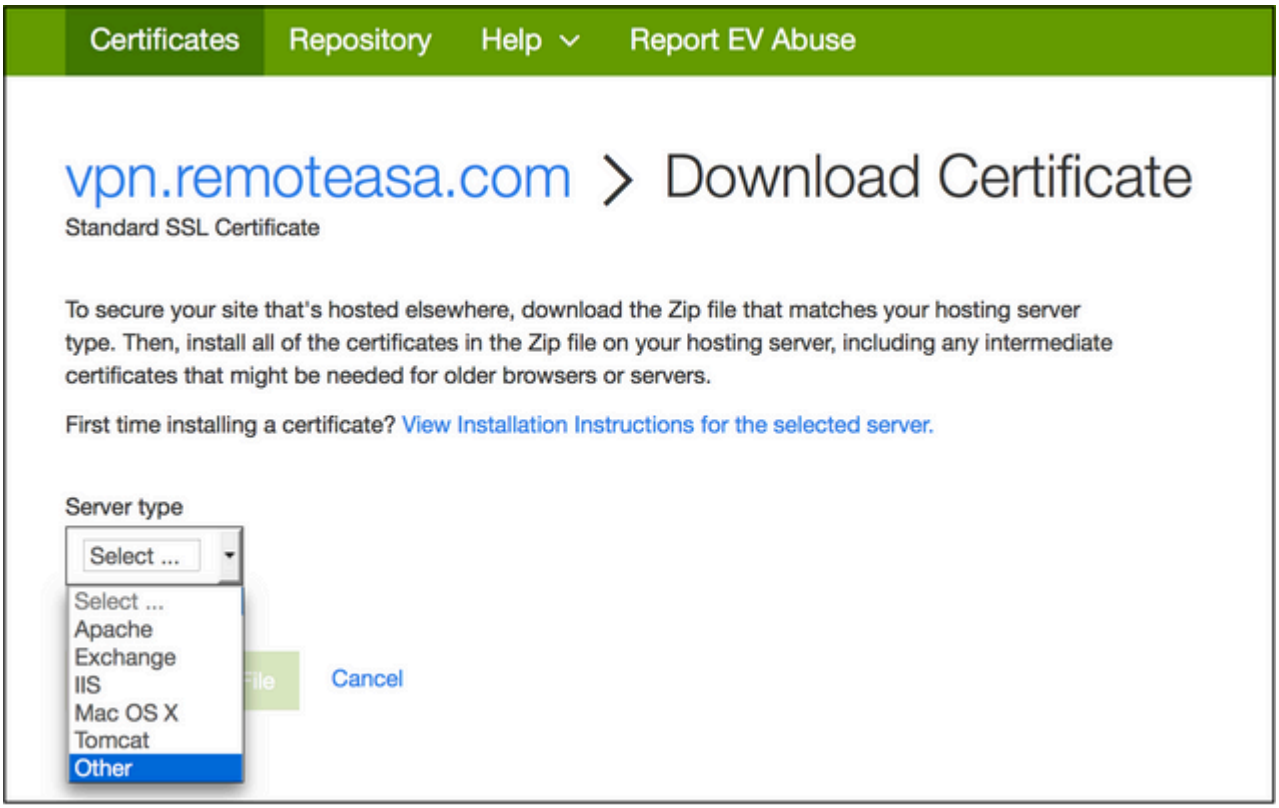
Una vez enviada la solicitud, GoDaddy la verifica antes de emitir el certificado.

Una vez validada la solicitud de certificado, GoDaddy envía el certificado a la cuenta.

El certificado se puede descargar para su instalación en el ASA. Haga clic en**Download** en la página para continuar.



Elegir**Other** como tipo de servidor y descargar el paquete zip de certificados.



El archivo .zip contiene el certificado de identidad y los paquetes de cadena de certificados de CA de GoDaddy como dos archivos .crt independientes. Vaya a la instalación del certificado SSL para instalar estos certificados en el ASA.

Instalación del certificado SSL en el ASA

El certificado SSL se puede instalar en el ASA con ASDM o CLI de dos maneras:

1. Importe la CA y el certificado de identidad por separado en formatos PEM.

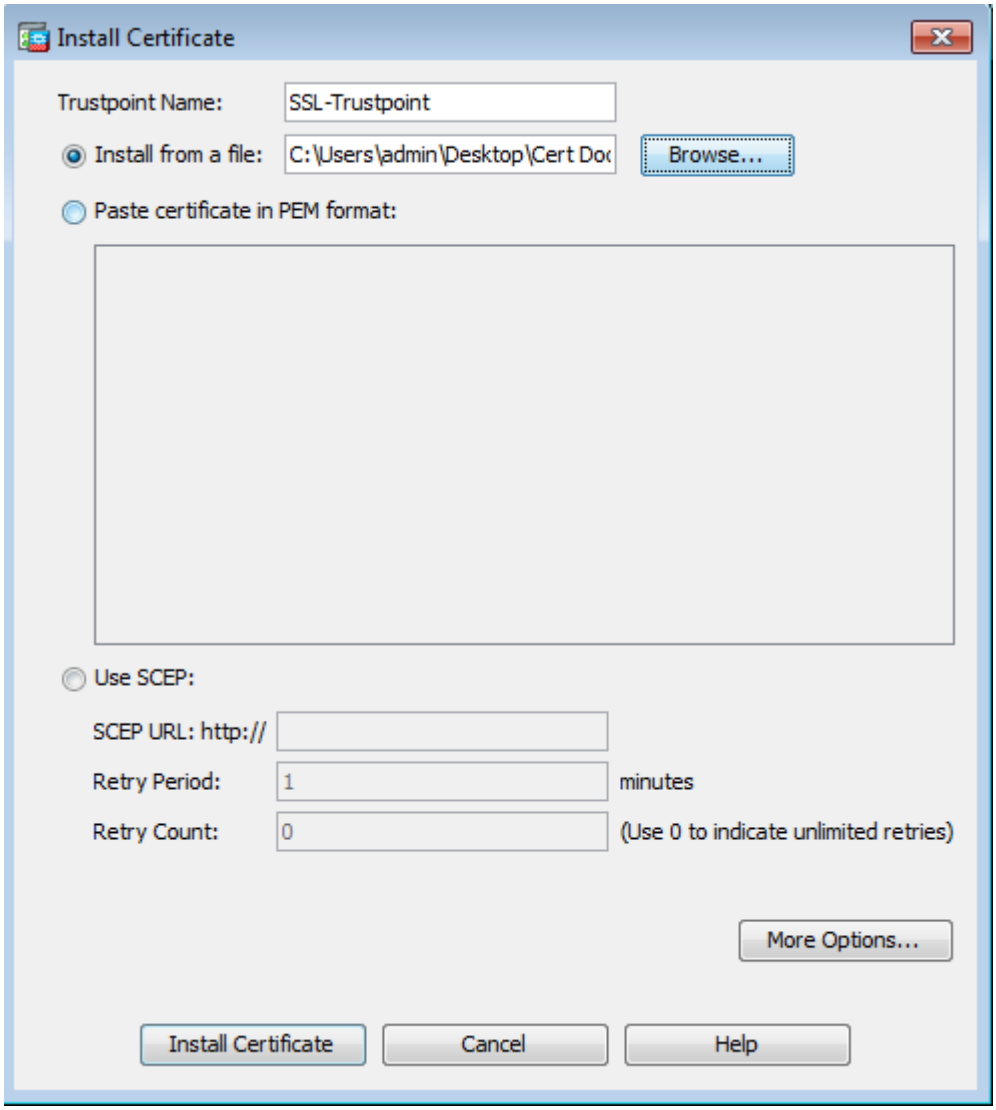
2. O importe el archivo PKCS12 (codificado en base64 para CLI) en el que el certificado de identidad, el certificado de CA y la clave privada se incluyen en el archivo PKCS12.

> **Nota**: si la CA proporciona una cadena de certificados de CA, instale únicamente el certificado de CA intermedio inmediato en la jerarquía del punto de confianza utilizado para generar la CSR. El certificado de CA raíz y cualquier otro certificado de CA intermedio se pueden instalar en nuevos puntos de confianza.

1.1 Instalación del Certificado de Identidad en Formato PEM con ASDM

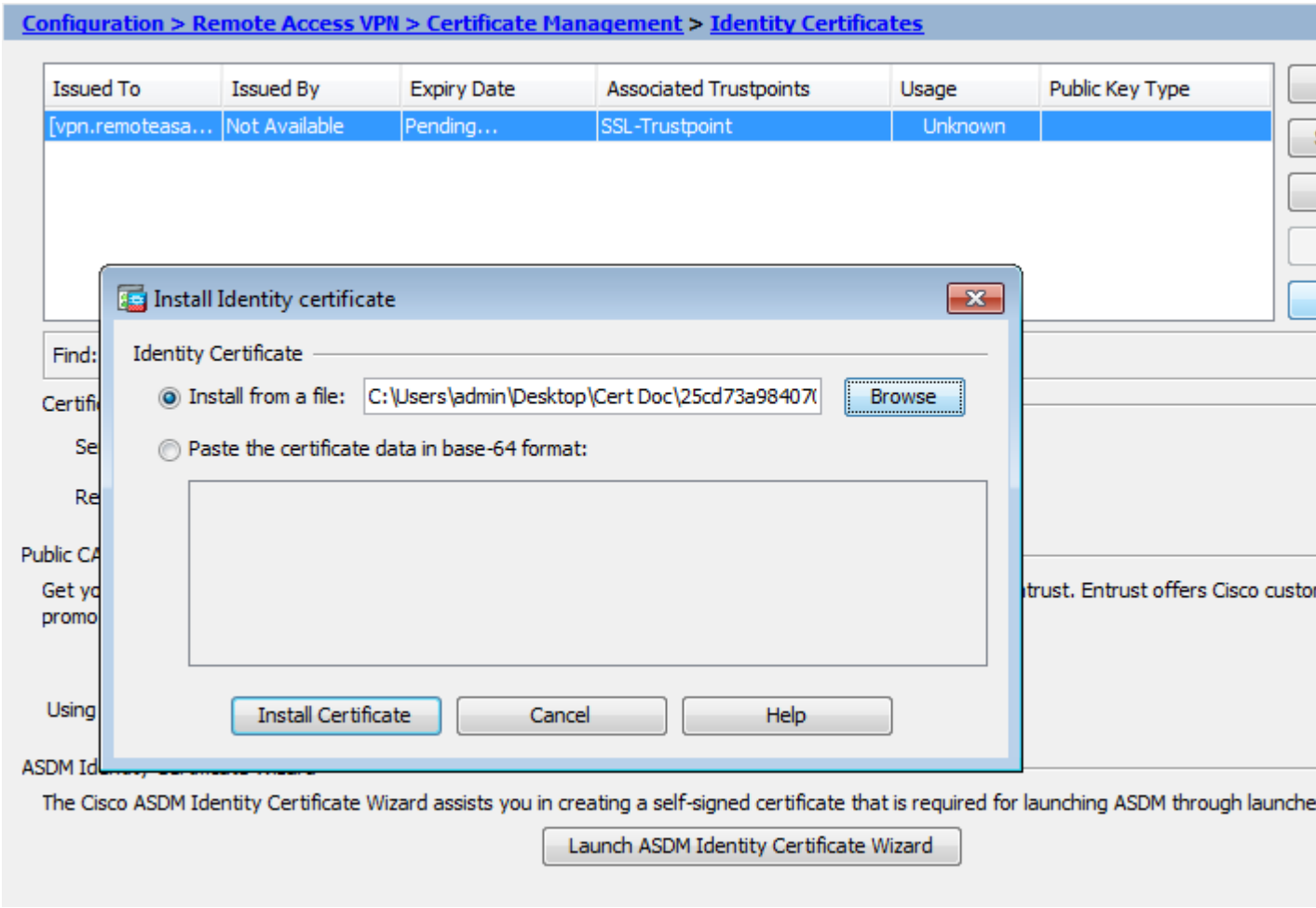
Los pasos de instalación dados suponen que la CA proporciona un certificado de identidad con codificación PEM (.pem, .cer, .crt) y un paquete de certificados de CA.

1. Desplácese hasta **Configuration > Remote Access VPN > Certificate Management**y seleccione Certificados de la CA.
2. El certificado codificado PEM en un editor de texto y copie y pegue el certificado de CA base64 proporcionado por el proveedor externo en el campo de texto.

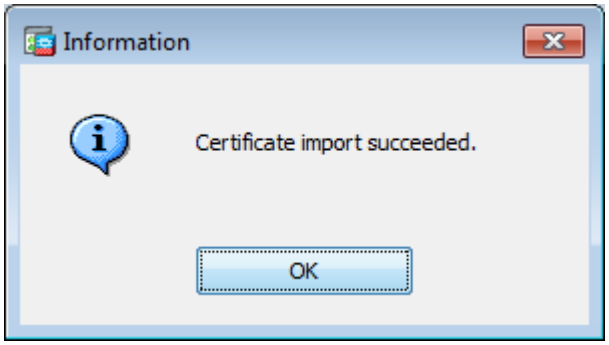


3. Haga clic en **Instalar certificado**.
4. Desplácese hasta**Configuration > Remote Access VPN > Certificate Management**y seleccione Certificados de identidad.
5. Seleccione el certificado de identidad creado anteriormente. Haga clic en **Install**.

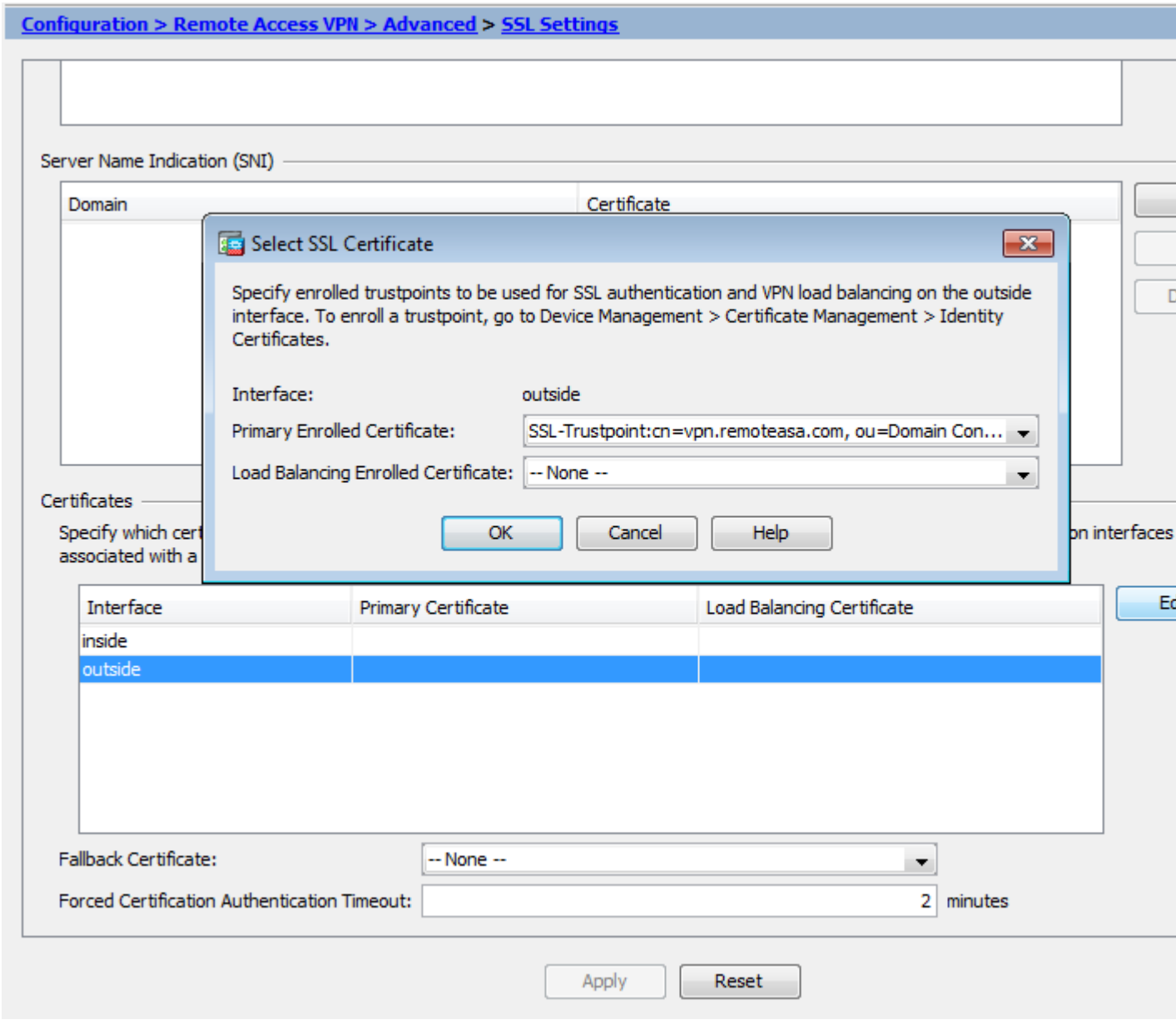
6. Haga clic en la opción**Install from a file** y seleccione el certificado de identidad codificado por PEM o abra el certificado codificado por PEM en un editor de texto y copie y pegue el certificado de identidad base64 proporcionado por el proveedor externo en el campo de texto.



7. Haga clic en**Add Certificate.**



8. Desplácese hasta**Configuration > Remote Access VPN > Advanced > SSL Settings.**
9. En Certificados, seleccione la interfaz que se utiliza para terminar las sesiones WebVPN. En este ejemplo, se utiliza la interfaz externa.
10. Haga clic en**Edit.**
11. En la lista desplegable Certificado, seleccione el certificado recién instalado.



12. Haga clic en**OK**.
13. Haga clic en**Apply**. El nuevo certificado se utiliza ahora para todas las sesiones WebVPN que terminan en la interfaz especificada.

1.2. Instalación de un certificado 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
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 thi
```

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
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)#
```

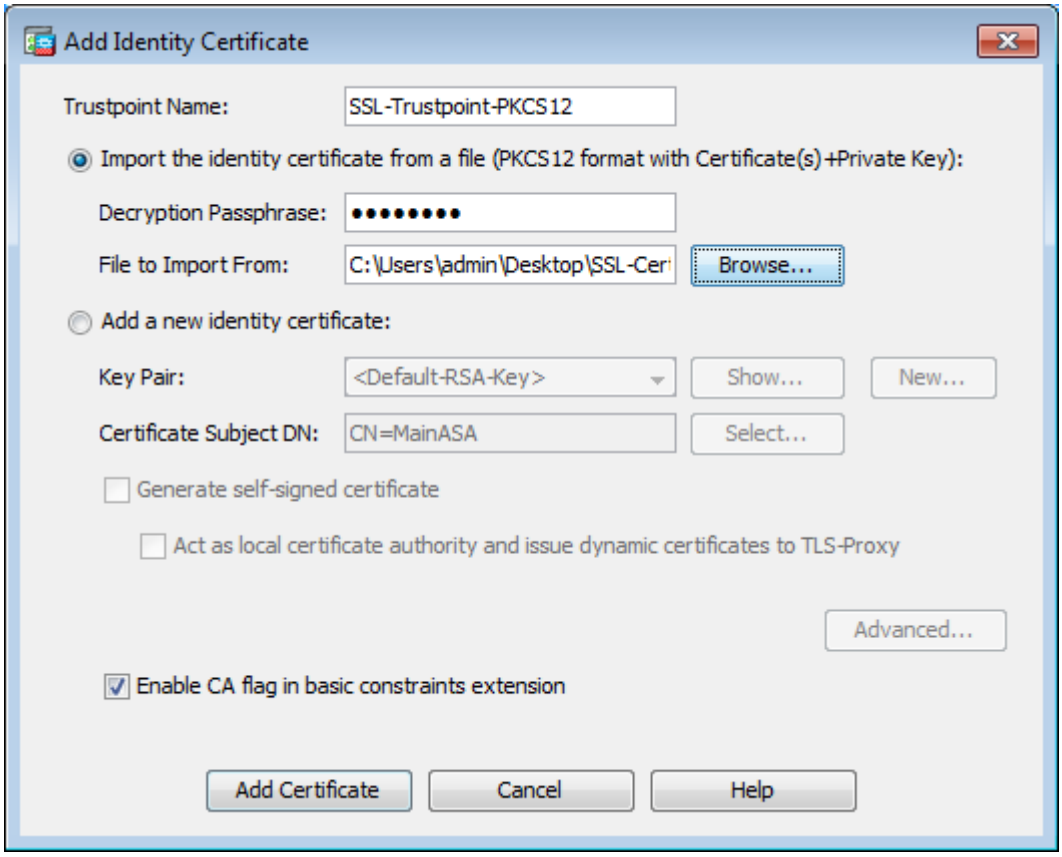
ssl trust-point SSL-Trustpoint outside

2.1 Instalación de un Certificado PKCS12 con ASDM

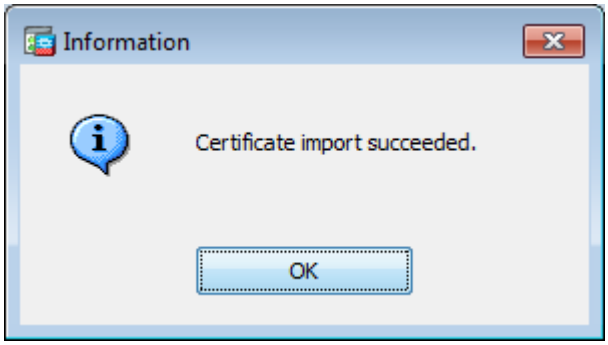
En los casos en los que no se genera la CSR en ASA, como en el caso de un certificado comodín o cuando se genera un certificado de UC, se recibe un certificado de identidad junto con la clave privada como

archivos independientes o un único archivo PKCS12 agrupado (formato .p12 o pfx). Para instalar este tipo de certificado, complete estos pasos.

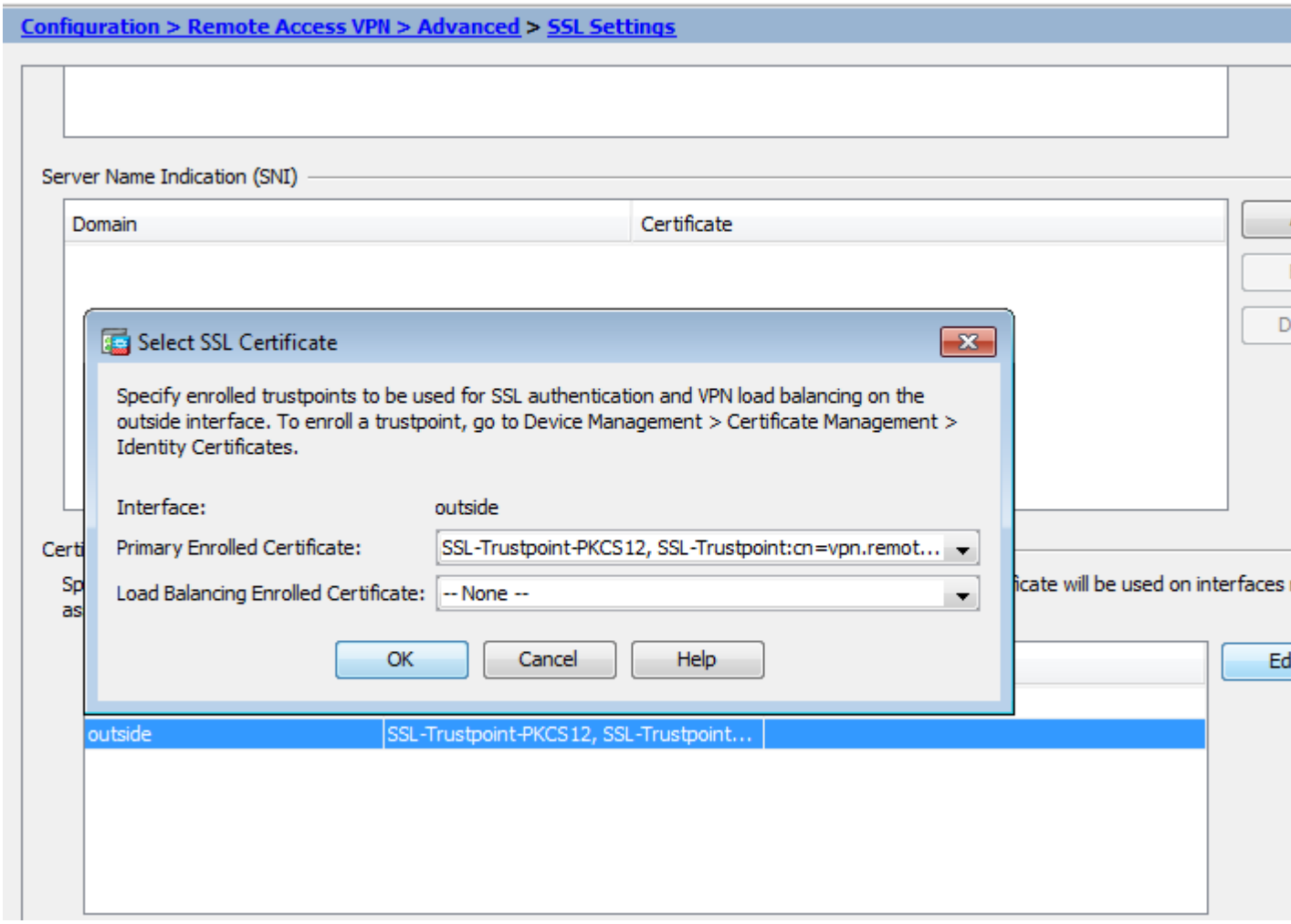
1. El certificado de identidad, agrupe el certificado de la CA y la clave privada en un único archivo PKCS12. El Apéndice B proporciona los pasos para hacerlo con OpenSSL. Si la CA ya la incluye, continúe con el siguiente paso.
2. Desplácese hasta**Configuration > Remote Access VPN > Certificate Management,** y elija **Identity Certificates.**
3. Haga clic en**Add.**
4. Especifique un nombre de Trustpoint.
5. Haga clic en el **Import the identity certificate from a file**botón de opción.
6. Introduzca la frase de paso utilizada para crear el archivo PKCS12. Busque y seleccione el archivo PKCS12. Introduzca la frase de contraseña del certificado.



7. Haga clic en **Agregar certificado**.



8. Desplácese hasta**Configuration > Remote Access VPN > Advanced**y elija **SSL Settings.**
9. En Certificados, elija la interfaz que se utiliza para terminar las sesiones WebVPN. En este ejemplo, se utiliza la interfaz externa.
10. Haga clic en**Edit.**
11. En la lista desplegable Certificado, seleccione el certificado recién instalado.



12. Haga clic en**OK**.
13. Haga clic en**Apply**. El nuevo certificado se utiliza ahora para todas las sesiones WebVPN que terminan en la interfaz especificada.

2.2 Instalación de un certificado 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-----
```

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)#
```

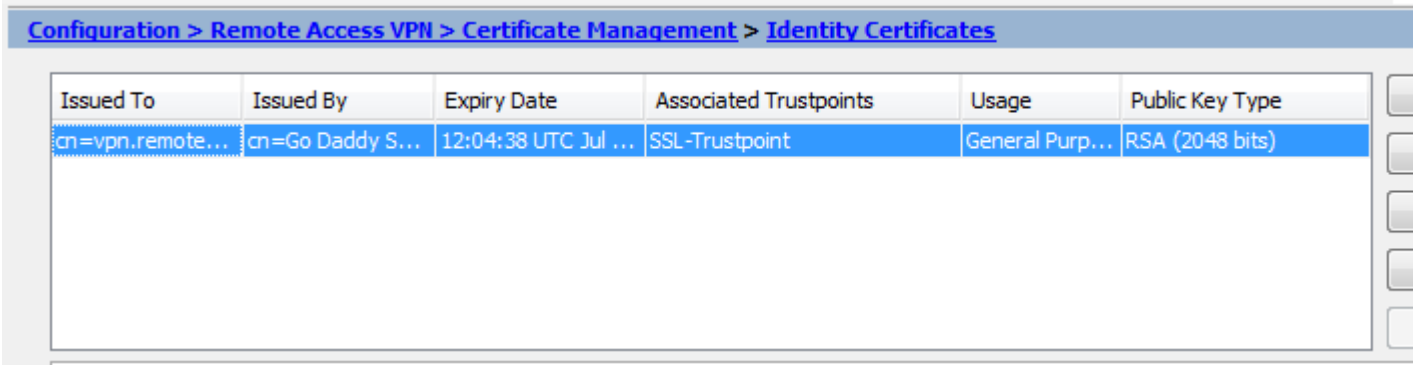
ssl trust-point SSL-Trustpoint-PKCS12 outside

Verificación

Siga estos pasos para verificar la correcta instalación del certificado de proveedor de terceros y su uso para las conexiones SSLVPN.

Ver certificados instalados mediante ASDM

1. Desplácese hasta**Configuration > Remote Access VPN > Certificate Management,**y elija **Identity Certificates.**
2. Aparece el certificado de identidad emitido por el proveedor externo.



Ver certificados instalados a través de CLI

<#root>

```
 MainASA(config)#
```

show crypto ca certificate

Certificate

```
  Status: Available
  Certificate Serial Number: 25cd73a984070605
  Certificate Usage: General Purpose
  Public Key Type: RSA (2048 bits)
  Signature Algorithm: SHA256 with RSA Encryption
  Issuer Name:
    cn=Go Daddy Secure Certificate Authority - G2
    ou=http://certs.godaddy.com/repository/
    o=GoDaddy.com\, Inc.
    l=Scottsdale
    st=Arizona
    c=US
  Subject Name:
    cn=(asa.remotevpn.url)
    ou=Domain Control Validated
  OCSP AIA:
    URL: http://ocsp.godaddy.com/
  CRL Distribution Points:
    [1]  http://crl.godaddy.com/gdig2s1-96.crl
  Validity Date:
    start date: 12:04:38 UTC Jul 22 2015
    end   date: 12:04:38 UTC Jul 22 2016
  Associated Trustpoints:
```

SSL-Trustpoint

CA Certificate

```
  Status: Available
  Certificate Serial Number: 07
  Certificate Usage: General Purpose
  Public Key Type: RSA (2048 bits)
  Signature Algorithm: SHA256 with RSA Encryption
  Issuer Name:
    cn=Go Daddy Root Certificate Authority - G2
```

```
    o=GoDaddy.com\, Inc.
    l=Scottsdale
    st=Arizona
    c=US
  Subject Name:
    cn=Go Daddy Secure Certificate Authority - G2
    ou=http://certs.godaddy.com/repository/
    o=GoDaddy.com\, Inc.
    l=Scottsdale
    st=Arizona
    c=US
  OCSP AIA:
    URL: http://ocsp.godaddy.com/
  CRL Distribution Points:
    [1]  http://crl.godaddy.com/gdroot-g2.crl
  Validity Date:
    start date: 07:00:00 UTC May 3 2011
    end   date: 07:00:00 UTC May 3 2031
  Associated Trustpoints:
```

SSL-Trustpoint

CA Certificate

```
  Status: Available
  Certificate Serial Number: 1be715
  Certificate Usage: General Purpose
  Public Key Type: RSA (2048 bits)
  Signature Algorithm: SHA256 with RSA Encryption
  Issuer Name:
    ou=Go Daddy Class 2 Certification Authority
    o=The Go Daddy Group\, Inc.
    c=US
  Subject Name:
    cn=Go Daddy Root Certificate Authority - G2
    o=GoDaddy.com\, Inc.
    l=Scottsdale
    st=Arizona
    c=US
  OCSP AIA:
    URL: http://ocsp.godaddy.com/
  CRL Distribution Points:
    [1]  http://crl.godaddy.com/gdroot.crl
  Validity Date:
    start date: 07:00:00 UTC Jan 1 2014
    end   date: 07:00:00 UTC May 30 2031
  Associated Trustpoints:
```

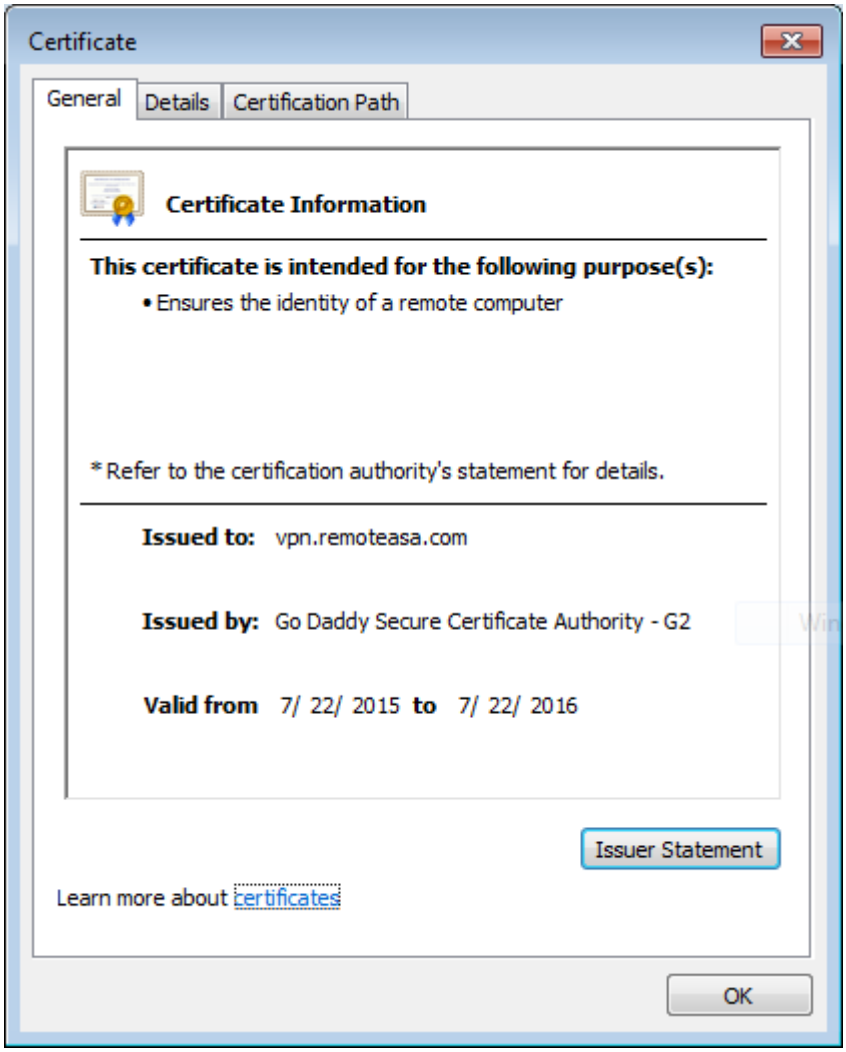
SSL-Trustpoint-1

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

Verificación del certificado instalado para WebVPN con un explorador Web

Verifique que WebVPN utilice el nuevo certificado.

1. Conéctese a la interfaz WebVPN a través de un explorador Web. Utilice https:// junto con el FQDN utilizado para solicitar el certificado (por ejemplo, https://(vpn.remoteasa.com)).
2. Haga doble clic en el icono de candado que aparece en la esquina inferior derecha de la página de inicio de sesión de WebVPN. Debe aparecer la información del certificado instalado.
3. Revise el contenido para verificar que coincide con el certificado emitido por el proveedor de terceros.

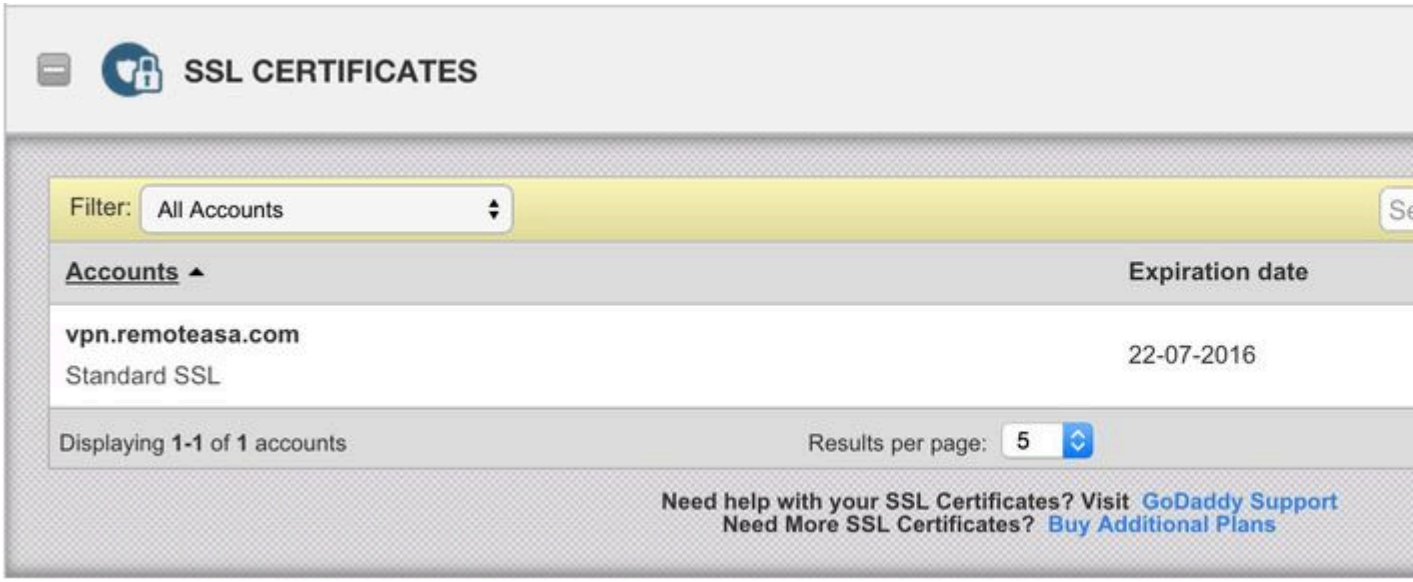


Renovación del certificado SSL en el ASA

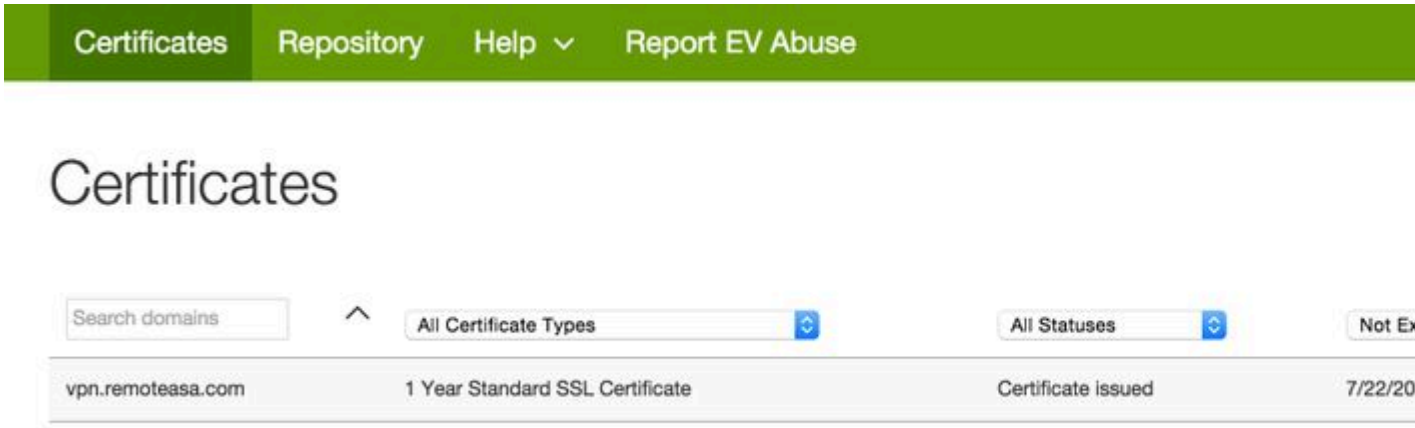
1. Regenere la CSR en el ASA, o con OpenSSL o en la CA con los mismos atributos que el certificado anterior. Complete los pasos proporcionados en Generación de CSR.
2. Envíe el CSR en la CA y genere un nuevo certificado de identidad en formato PEM (.pem, .cer, .crt) junto con el certificado de la CA. En el caso de un certificado PKCS12, también hay una nueva clave Private.

   En el caso de GoDaddy CA, el certificado se puede reintroducir con una nueva CSR generada.

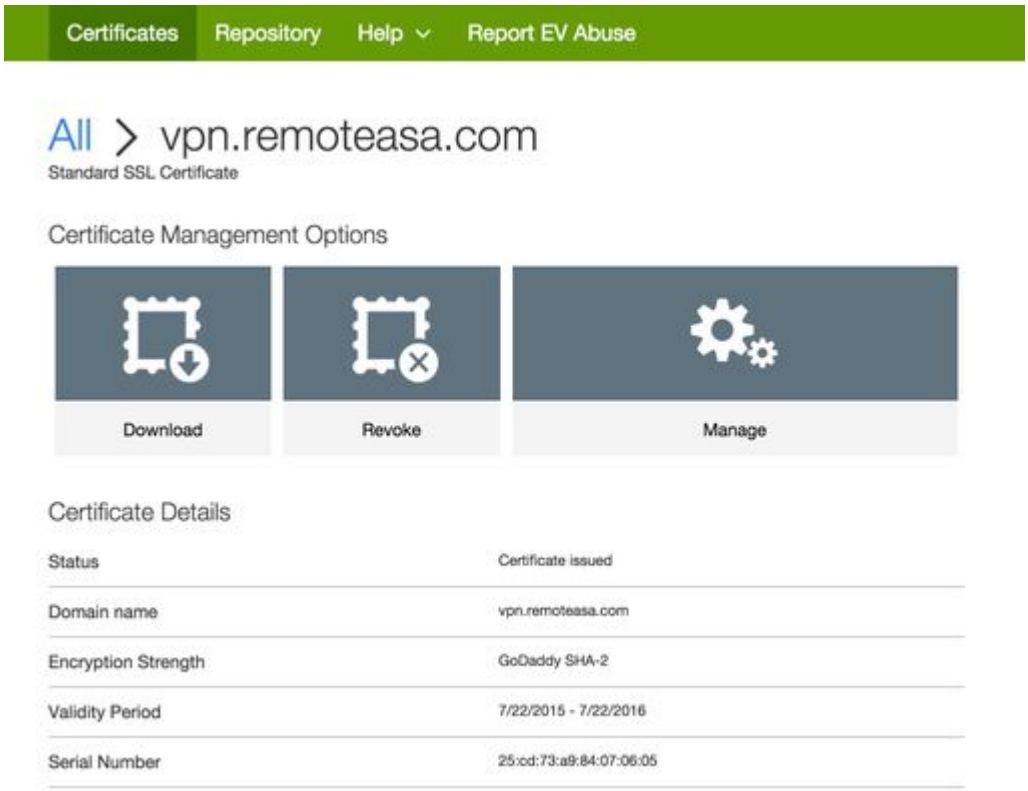
   Vaya a la cuenta GoDaddyaccount y haga clic en **Manage** bajo SSL Certificates.



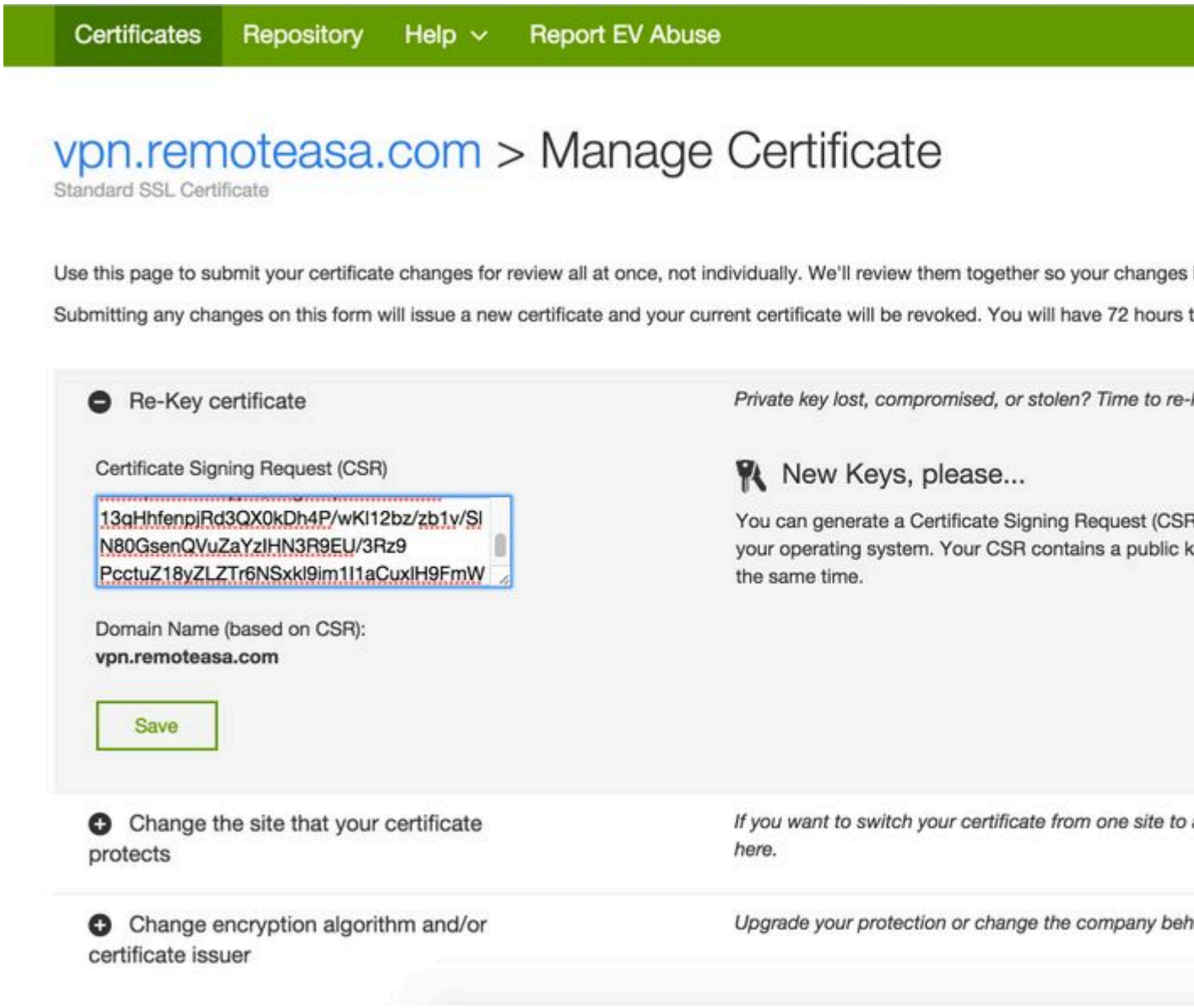
Haga clic en **Ver estado** para el nombre de dominio requerido.



Haga clic en **Administrar** para dar opciones para volver a escribir la clave del certificado.



Expanda la opción **Re-Key certificate** y agregue el nuevo CSR.



Guarde y continúe con el siguiente paso. GoDaddy emite un nuevo certificado basado en la CSR provista.

3. Instale el nuevo certificado en un nuevo punto de confianza, como se muestra en la sección Instalación del certificado SSL en ASA.

Preguntas Frecuentes

1. ¿Cuál es la mejor manera de transferir certificados de identidad de un ASA a un ASA diferente?

Exporte el certificado junto con las claves a un archivo PKCS12.

Utilice este comando para exportar el certificado a través de la CLI desde el ASA original:

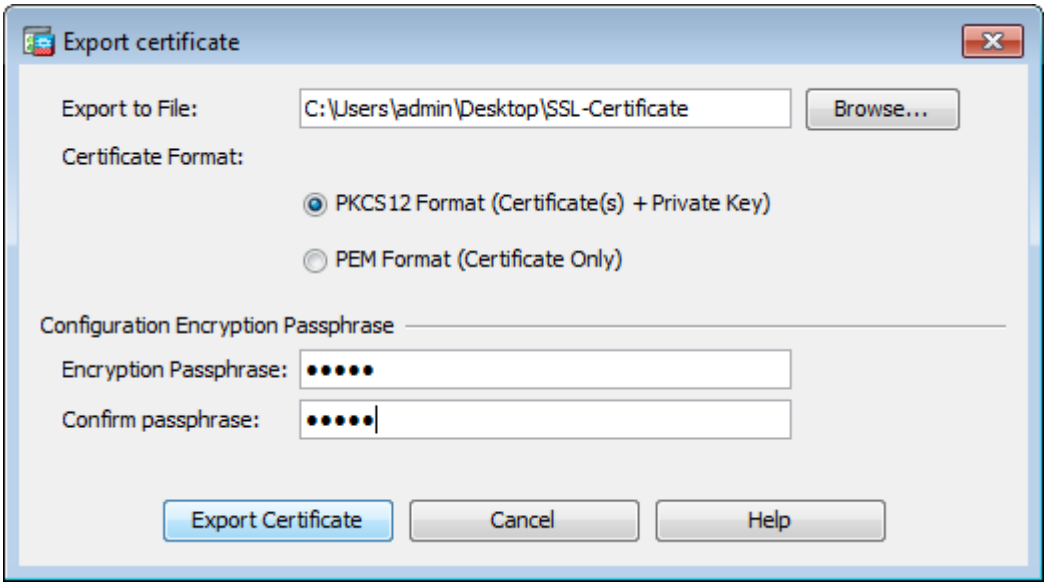
<#root>

```
ASA(config)#
```

crypto ca export

pkcs12

Configuración de ASDM:



Utilice este comando para importar el certificado a través de CLI al ASA de destino:

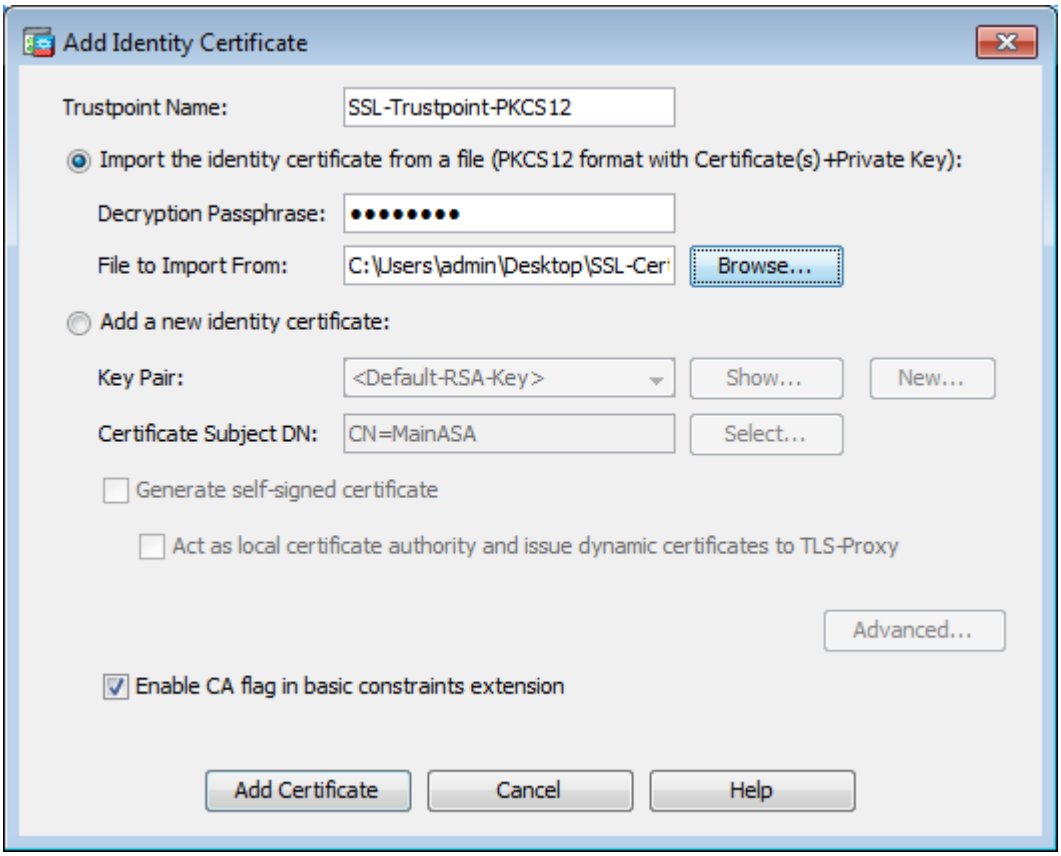
<#root>

ASA(config)#

crypto ca import

pkcs12

Configuración de ASDM:



Esto también se puede hacer a través de la función de respaldo/restauración en el ASDM con estos pasos:

1. Inicie sesión en ASA mediante ASDM y seleccione**Tools > Backup Configuration.**
2. Copia de seguridad de toda la configuración o sólo los certificados de identidad.
3. En el ASA de destino, abra el ASDM y elija**Tools > Restore Configuration.**

2. ¿Cómo generar certificados SSL para su uso con ASA de Balanceo de Carga VPN?

Existen varios métodos que se pueden utilizar para configurar ASA con certificados SSL para un entorno de equilibrio de carga VPN.

1. Utilice un único certificado de Unified Communications/varios dominios (UCC) que tenga el FQDN de equilibrio de carga como el DN y cada FQDN de ASA como un nombre alternativo de sujeto (SAN) independiente. Hay varias CAs bien conocidas como GoDaddy, Entrust, Comodo y otras que soportan tales certificados. Al elegir este método, es importante recordar que ASA no admite actualmente la creación de un CSR con varios campos SAN. Esto se ha documentado en la mejora del ID de bug de Cisco CSCso70867 . En este caso, hay dos opciones para generar la CSR
    a. A través de CLI o ASDM. Cuando el CSR se envía a la CA, agregue varias SAN en el propio portal de la CA.
    b. Utilice OpenSSL para generar el CSR e incluir las distintas SAN en el archivo openssl.cnf.

    Una vez que el CSR se ha enviado a la CA y se ha generado el certificado, importe este certificado

PEM al ASA que ha generado el CSR. Una vez hecho esto, exporte e importe este certificado en formato PKCS12 en los otros ASA miembros.

2. Utilice un certificado Comodín. Se trata de un método menos seguro y flexible en comparación con un certificado de UC. En caso de que la CA no admita certificados de UC, se generará una CSR en la CA o con OpenSSL, donde el FQDN tendrá el formato *.domain.com. Una vez que el CSR se ha enviado a la CA y se ha generado el certificado, importe el certificado PKCS12 a todos los ASA del clúster.
3. Utilice un certificado independiente para cada uno de los ASA miembros y para el FQDN de equilibrio de carga. Esta es la solución menos eficaz. Los certificados para cada uno de los ASA individuales se pueden crear como se muestra en este documento. El certificado para el FQDN de equilibrio de carga VPN se crea en un ASA y se exporta e importa como un certificado PKCS12 en los otros ASA.

3. ¿Es necesario copiar los certificados del ASA principal al ASA secundario en un par de failover ASA?

No es necesario copiar manualmente los certificados del ASA principal al secundario, ya que los certificados se sincronizan entre los ASA, siempre y cuando se configure la conmutación por fallas stateful. Si en la configuración inicial de failover, los certificados no se ven en el dispositivo en espera, ejecute el comando **write standby** para forzar una sincronización.

4. Si se utilizan claves ECDSA, ¿es diferente el proceso de generación de certificados SSL?

La única diferencia en la configuración es el paso de generación del par de claves, donde se genera un par de claves ECDSA en lugar de un par de claves RSA. El resto de los pasos siguen siendo los mismos. El comando CLI para generar claves ECDSA se muestra aquí:

<#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...
```

Troubleshoot

Comandos para Troubleshooting

Estos comandos de depuración deben recopilarse en la CLI en caso de que se produzca un error en la instalación del certificado SSL:

debug crypto ca 255

debug crypto ca messages 255

debug crypto ca transactions 255

Problemas comunes

Advertencia de certificado no fiable con un certificado SSL de terceros válido en la interfaz externa de ASA con 9.4(1) y versiones posteriores.

Solución: este problema se presenta cuando se utiliza un par de claves RSA con el certificado. En las versiones ASA a partir de la 9.4(1), todos los cifrados ECDSA y RSA están habilitados de forma predeterminada y el cifrado más fuerte (normalmente un cifrado ECDSA) se utiliza para la negociación. Si esto sucede, ASA presenta un certificado autofirmado en lugar del certificado basado en RSA configurado actualmente. Se ha implementado una mejora para cambiar el comportamiento cuando se instala un certificado basado en RSA en una interfaz y se realiza un seguimiento mediante el ID de bug de Cisco CSCuu02848.

Acción Recomendada: Inhabilite los cifrados ECDSA con estos 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"
```

O, con el ASDM, navegue hasta**Configuration > Remote Access VPN > Advanced**y elija**SSL Settings.** En la sección Encryption (Encriptación), seleccione tlsv1.2 **Cypher version** y edítelo con la cadena personalizada AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA:RC4-SHA:RC4-MD5

Appendix

Apéndice A: ECDSA o RSA

El algoritmo ECDSA forma parte de la criptografía de curva elíptica (ECC) y utiliza una ecuación de una curva elíptica para generar una clave pública, mientras que el algoritmo RSA utiliza el producto de dos primos más un número menor para generar la clave pública. Esto significa que con ECDSA se puede lograr el mismo nivel de seguridad que RSA, pero con claves más pequeñas. Esto reduce el tiempo de cálculo y aumenta los tiempos de conexión para los sitios que utilizan certificados ECDSA.

El documento sobre criptografía de última generación y ASA proporciona información más detallada.

Apéndice B: Utilice OpenSSL para generar un certificado PKCS12 a partir de un certificado de identidad, un certificado de CA y una clave privada

1. Verifique que OpenSSL esté instalado en el sistema en el que se ejecuta este proceso. Para los usuarios de Mac OSX y GNU/Linux, se instala de forma predeterminada.
2. Cambie a un directorio válido.

   En Windows: de forma predeterminada, las utilidades se instalan en C:\Openssl\bin. Abra un símbolo del sistema en esta ubicación.

   En Mac OSX/Linux: Abra la ventana Terminal en el directorio necesario para crear el certificado PKCS12.

3. En el directorio mencionado en el paso anterior, guarde los archivos de clave privada (privateKey.key), certificado de identidad (certificate.crt) y cadena de certificados de CA raíz (CACert.crt).

   Combine la clave privada, el certificado de identidad y la cadena de certificados de la CA raíz en un

archivo PKCS12. Introduzca una frase de paso para proteger el certificado PKCS12.

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

4. Convierta el certificado PKCS12 generado en un certificado codificado Base64:
<#root>

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

A continuación, importe el certificado generado en el último paso para utilizarlo con SSL.

Información Relacionada

- Guía de configuración de ASA 9.x: configuración de certificados digitales
- Cómo obtener un certificado digital de una CA de Microsoft Windows con ASDM en un ASA
- **Soporte Técnico y Documentación - Cisco Systems**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).