配置 ASA：SSL 数字证书安装和续约

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- CSR 生成
  - 1. 使用 ASDM 配置
  - 2.使用ASACLI配置
  - 3. 使用 OpenSSL 生成 CSR
- CA 上的 SSL 证书生成
  - GoDaddy CA 上的 SSL 证书生成示例
- ASA 上的 SSL 证书安装
  - 1.1 使用 ASDM 安装 PEM 格式身份证书
  - 1.2.使用CLI安装PEM证书
  - 2.1使用ASDM安装PKCS12证书
  - 2.2使用CLI安装PKCS12证书

验证

- 通过 ASDM 查看已安装的证书
- 通过 CLI 查看已安装的证书
- 使用 Web 浏览器验证为 WebVPN 安装的证书
- 在 ASA 上续订 SSL 证书

常见问题解答

- 1. 将身份证书从一个 ASA 传输至另一个 ASA 的最佳方式是什么？
- 2. 如何生成用于 VPN 负载均衡 ASA 的 SSL 证书？
- 3. 证书是否需要从主 ASA 复制到 ASA 故障切换对中的辅助 ASA？
- 4. 如果使用的是 ECDSA 密钥，SSL 证书生成过程是否不同？

故障排除

- 故障排除命令
- 常见问题

Appendix

- 附录 A：ECDSA 或 RSA
- 附录 B：使用 OpenSSL 从身份证书、CA 证书和私钥生成 PKCS12 证书
- 附录 C：受信任CA证书安全注意事项
  - 证书身份验证风险和建议
  - 授权风险和建议

其它资源

相关信息

简介

本文档介绍在 ASA 上为无客户端 SSLVPN 和 AnyConnect 连接安装第三方可信 SSL 数字证书。

先决条件

要求

本文档需要访问受信任的第三方证书颁发机构（CA）才可注册证书。第三方 CA 供应商的示例包括但不限于 Baltimore、思科、Entrust、Geotrust、 G、Microsoft、RSA、Thawte 和 VeriSign。

开始之前，请验证ASA具有正确的时钟时间、日期和时区。对于证书身份验证，建议使用网络时间协议 (NTP) 服务器同步 ASA 上的时间。《Cisco ASA 系列常规操作 CLI 配置指南 9.1》详细介绍了在 ASA 上正确设置时间和日期所需执行的步骤。

使用的组件

本文档使用运行软件版本 9.4.1 和 ASDM 版本 7.4(1) 的 ASA 5500-X。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本示例中使用的是 GoDaddy 证书。各步骤均包含自适应安全设备管理器 (ASDM) 操作步骤和 CLI 等效操作。

配置

SSL 协议要求 SSL 服务器向客户端提供服务器证书，以便客户端执行服务器身份验证。思科不建议使用自签证书，因为用户可能会无意中将浏览器配置为信任来自欺诈服务器的证书。连接到安全网关后，用户必须对安全警告作出响应，这也会给用户带来不便。为此，建议使用受信任第三方 CA 将 SSL 证书颁发给 ASA。

实际上，ASA 上第三方证书的生命周期包括以下步骤：



CSR 生成

CSR 生成是任何 x.509 数字证书生命周期中的第一步。

生成专用/公共 Rivest-Shamir-Adleman (RSA) 或椭圆曲线数字签名算法 (ECDSA) 密钥对后（附录 A 详细介绍使用 RSA 和 ECDSA 之间的区别），系统将创建证书签名请求 (CSR)。

CSR 是一条 PKCS10 格式的消息，包含发送请求的主机的公钥和身份信息。PKI 数据格式说明了适用于 ASA 和 Cisco IOS® 的不同证书格式。

注意：
1. 请向 CA 咨询所需的密钥对大小。CA/浏览器论坛已强制要求，其成员 CA 生成的所有证书的最小为 2048 位。
2. ASA 目前不支持用于 SSL 服务器身份验证的 4096 位密钥（思科漏洞 ID CSCut53512）。但是，IKEv2 不支持仅在 ASA 5580、5585 和 5500-X 平台上使用 4096 位服务器证书。
3. 在 CSR 的 FQDN 字段中使用 ASA 的 DNS 名称，以防出现“不受信任的证书”警告并确保通过严格的证书检查。

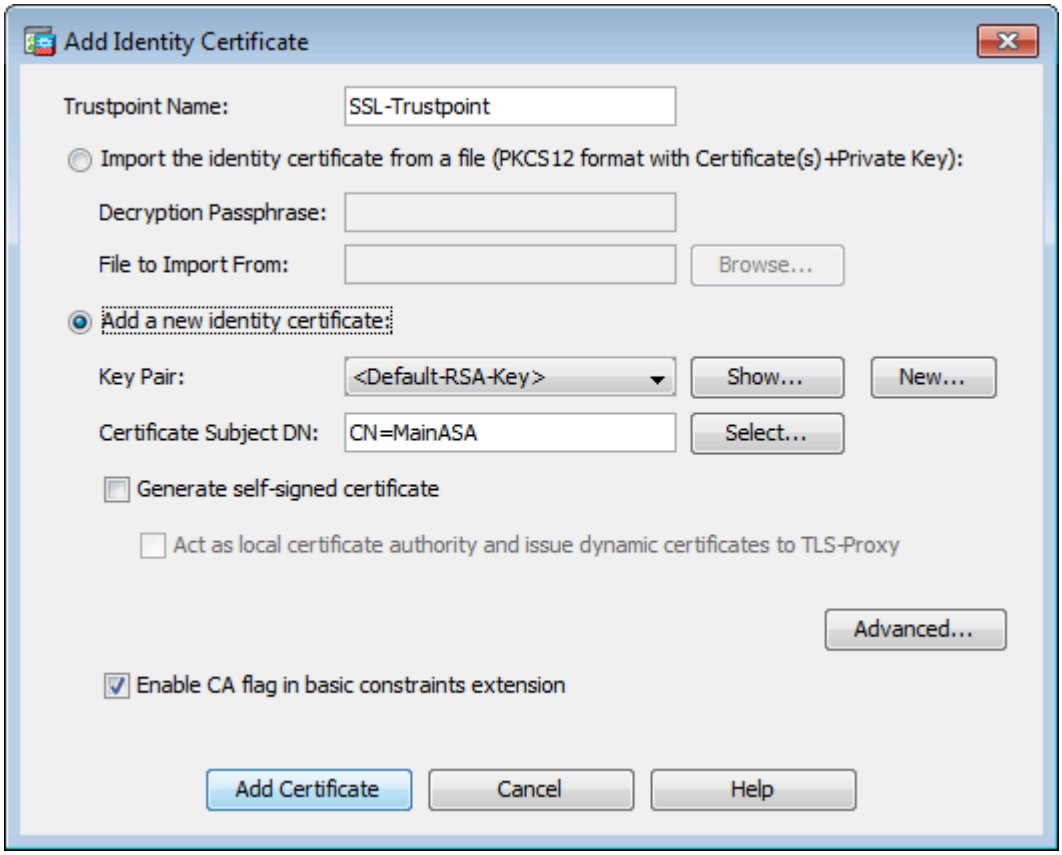
可以通过三种方式来生成 CSR。

1. 使用 ASDM 配置.

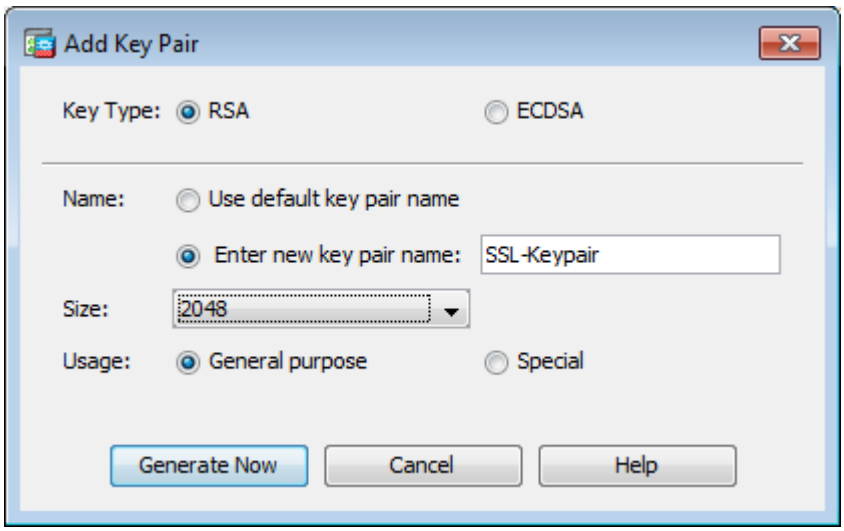
2. 使用 ASA CLI 配置.
3. 使用 OpenSSL 生成 CSR.

1. 使用 ASDM 配置

1. 导航到**Configuration > Remote Access VPN > Certificate Management**并选择 **Identity Certificates**.
2. 点击 **Add**.



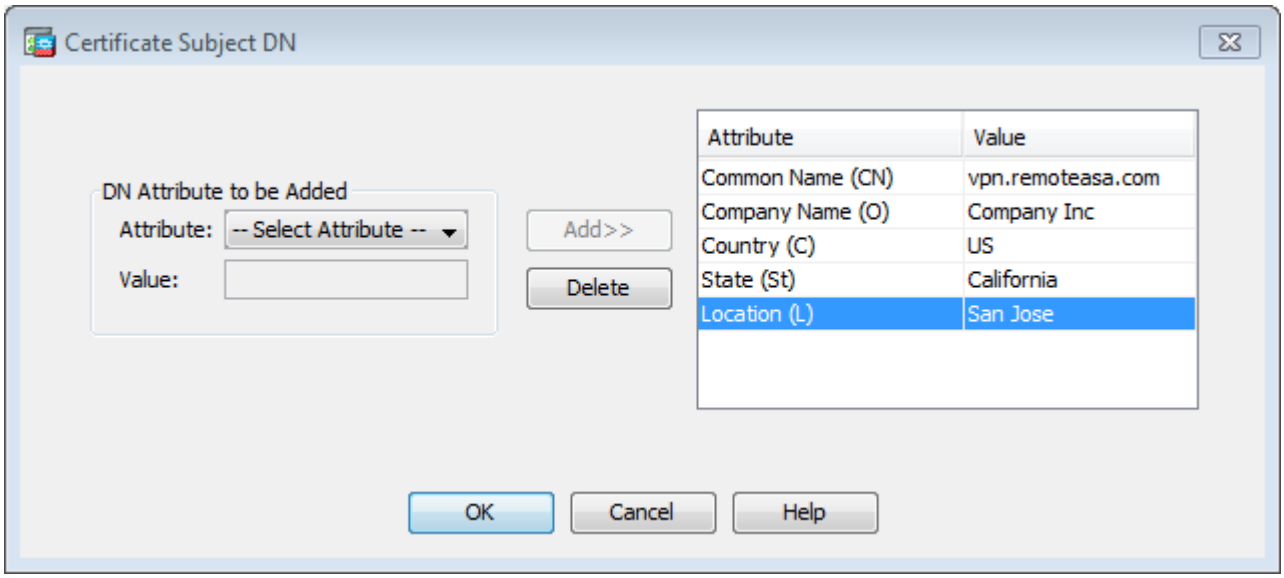
3. 在“信任点名称”输入字段下定义信任点名称。
4. 单击**Add a new identity certificate**Radio按钮。
5. 对于密钥对，请单击**New**.



6. 选择密钥类型 - RSA 或 ECDSA。（请参阅附录 A，了解差异。）
7. 单击**Enter new key pair name**Radio按钮。为便于识别，请标识密钥对名称。
8. 选择**Key Size**。选择**General Purpose for Usage**“使用RSA”。
9. 单击。**Generate Now**已创建密钥对。
10. **Select**,要定义证书使用者DN，请点击并配置下表中列出的属性:

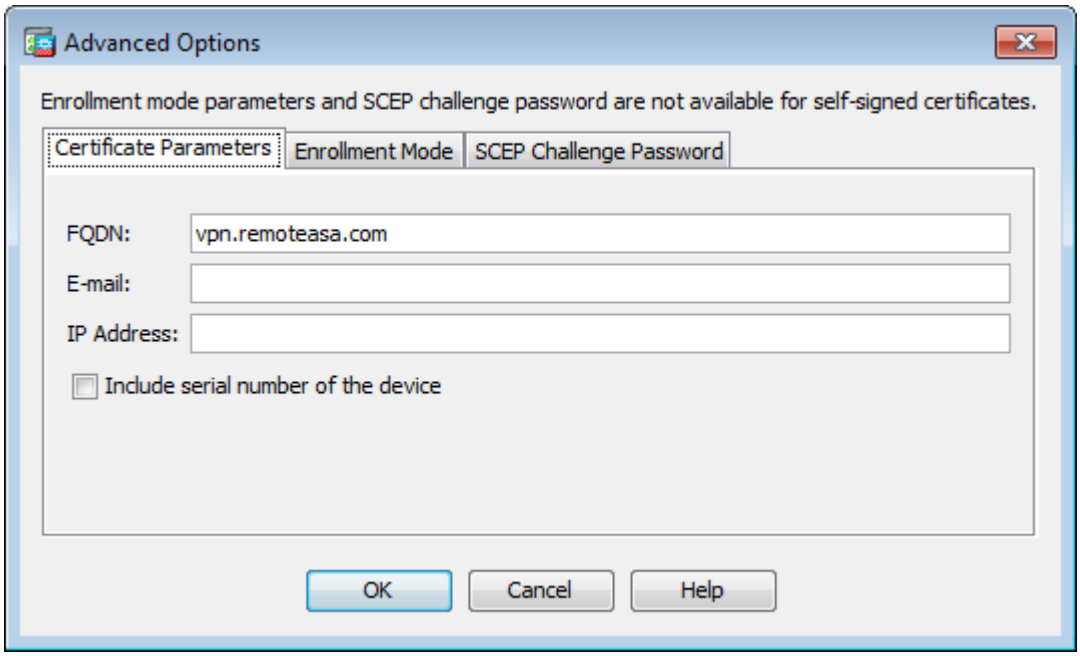
Attribute	Description
CN	FQDN (Full Qualified Domain Name) that will be used for connections to your firewall. For example, webvpn.cisco.com
OU	Department Name
O	Company Name (Avoid using Special Characters)
C	Country Code (2 Letter Code without Punctuation)
St	State (Must be spelled out completely.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

要配置这些值，请从属性下拉列表中选择一个值，输入值并点击添加。

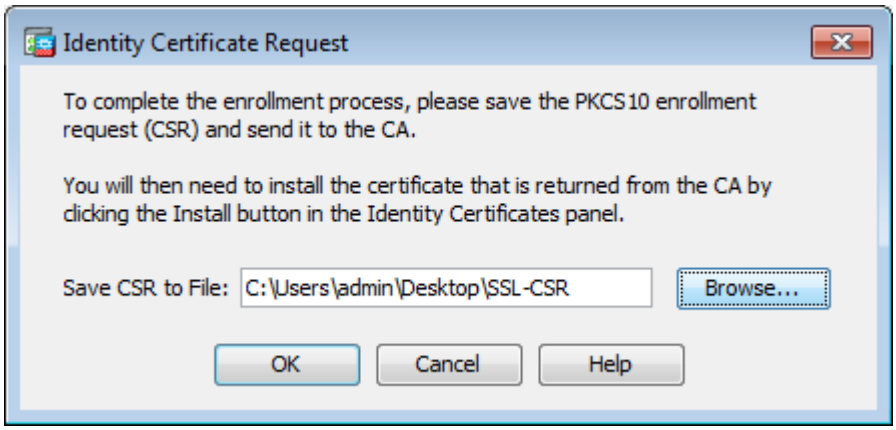


注意：某些第三方供应商要求在颁发身份证书前包含特定属性。如果不确定所需属性，请咨询供应商以获取详细信息。

11. 添加适当的值后**OK**.，点击Add Identity Certificate对话框，其中填充了Certificate Subject DN字段。
12. 单击 Advanced。



13. 在字FQDN段中，输入用于从Internet访问设备的FQDN。点击OK.
14. 选中“在基本约束扩展中启用 CA 标志”选项。默认情况下，不带 CA 标志的证书现在不能作为 CA 证书安装在 ASA 上。基本约束扩展可确定证书的主题是否为 CA，及包含此证书的有效证书路径的最大深度。取消选中该选项以跳过此要求。
15. 单击OK,，然后单击Add Certificate.“A prompt displayed（显示提示符）”，将CSR保存到本地计算机上的文件。



16. 点击Browse,，选择位置以保存CSR，并使用.txt扩展名保存文件。

> 注意：当文件以 .txt 扩展名保存时，可以使用文本编辑器（例如记事本）打开和查看 PKCS#10 请求。

2. 使用 ASA CLI 配置

在 ASDM 中，生成 CSR 或安装 CA 证书后，系统会自动创建信任点。在 CLI 中，必须手动创建信任点。

<#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
uR3Q4TmksyuRMqJNrb9kXpvA6H2OOPuBfQvSF4rVnSwKOmu3c8nweEvYcdVWV6Bz
BhjXeovTVi17FlNTceaUTGikeIdXC+mw1iE7eRsynS/d4mzMWJmrvrsDNzpAW/EM
SzTca+BvqF7X2r3LU8Vsv6Oi8ylhco9Fz7bWvRWVtO3NDDbyolC9b/VgXMuBitcc
rzfUbVnm7VZDOf4jr9EXgUwXxcQidWEABlFrXrtYpFgBo9aqJmRp2YABQ1ieP4cY
3rBtgRjLcF+S9TvHG5m4v7v755meV4YqsZIXvytIOzVBihemVxaGA1oDwfkoYSFi
4CzXbFvdG6kCAwEAAaA/MD0GCSqGSIb3DQEJDjEwMC4wDgYDVR0PAQH/BAQDAgWg
MBwGA1UdEQQVMBOCEXZwbi5yZW1vdGVhc2EuY29tMA0GCSqGSIb3DQEBBQUAA4IB
AQBZuQzUXGEB0ix1yuPK0ZkRz8bPnwIqLTfxZhagmuyEhrN7N4+aQnCHj85oJane
4ztZDiCCoWTerBS4RSkKEHEspu9oohjCYuNnp5qa91SPrZNEjTWwOeRn+qKbId2J
jE6Qy4vdPCexavMLYVQxCny+gVkzPN/sFRk3EcTTVq6DxxaebpJijmiqa7gCph52
YkHXnFne1LQd41BgoLlCr9+hx74XsTHGBmI1s/9T5oAX26Ym+B2l/i/DP5BktIUA
8GvIY1/ypj9KO49fP5ap8alOqvLtYYcCcfwrCt+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. 使用 OpenSSL 生成 CSR

OpenSSL使用文OpenSSL config件来提取CSR生成中使用的属性。此过程会生成 CSR 和私钥。

⚠ 警告：确认未与任何其他人共享生成的私钥，否则可能损害证书的完整性。

---

1. 确保在运行此进程的系统上安装 OpenSSL。对于 Mac OSX 和 GNU/Linux 用户，会默认安装 OpenSSL。
2. 切换到功能目录。

   在 Windows 上：默认情况下，实用程序安装在C:\Openssl\bin.Open a command prompt中。

   在 Mac OSX/Linux 上：在创建 CSR 所需的目录中打开终端窗口。

3. 使用具有给定属性的文本编辑器创建OpenSSL 配置文件。完成后，将文件另存为 openssl.cnf，该文件位于上一步中提到的位置（如果使用版本0.9.8h及更高版本，则文件 isopenssl.cfg）。
   <#root>

```
[req]

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


[req_distinguished_name]

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

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

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

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

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


[req_ext]

subjectAltName = @alt_names


[alt_names]

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

4. 使用以下命令生成 CSR 和私钥：

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]:
```

将已保存的 CSR 提交给第三方 CA 供应商。颁发证书后，CA 提供要在 ASA 上安装的身份证书和 CA 证书。

CA 上的 SSL 证书生成

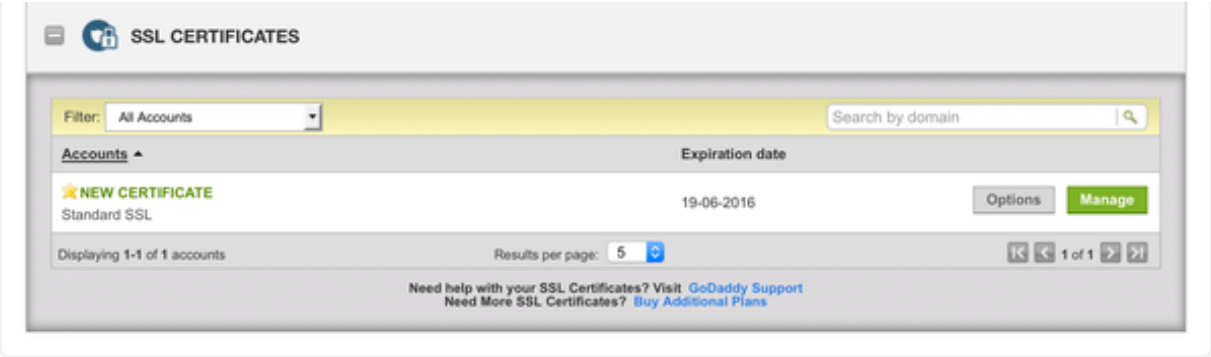
下一步是获取 CA 签署的 CSR。CA提供新生成的PEM编码身份证书，或提供PKCS12证书以及CA证书捆绑包。

如果 CSR 是在 ASA 外生成的（通过 OpenSSL 或 CA 本身），则具有私钥和 CA 证书的 PEM 编码身份证书将作为单独的文件提供。附录B提供了将这些元素捆绑到单个PKCS12文件（.p12或.pfx格式）中的步骤。

在本文档中，GoDaddy CA 用作向 ASA 颁发身份证书的示例。此流程与其他CA供应商不同。在继续操作之前，请仔细阅读CA文档。

GoDaddy CA 上的 SSL 证书生成示例

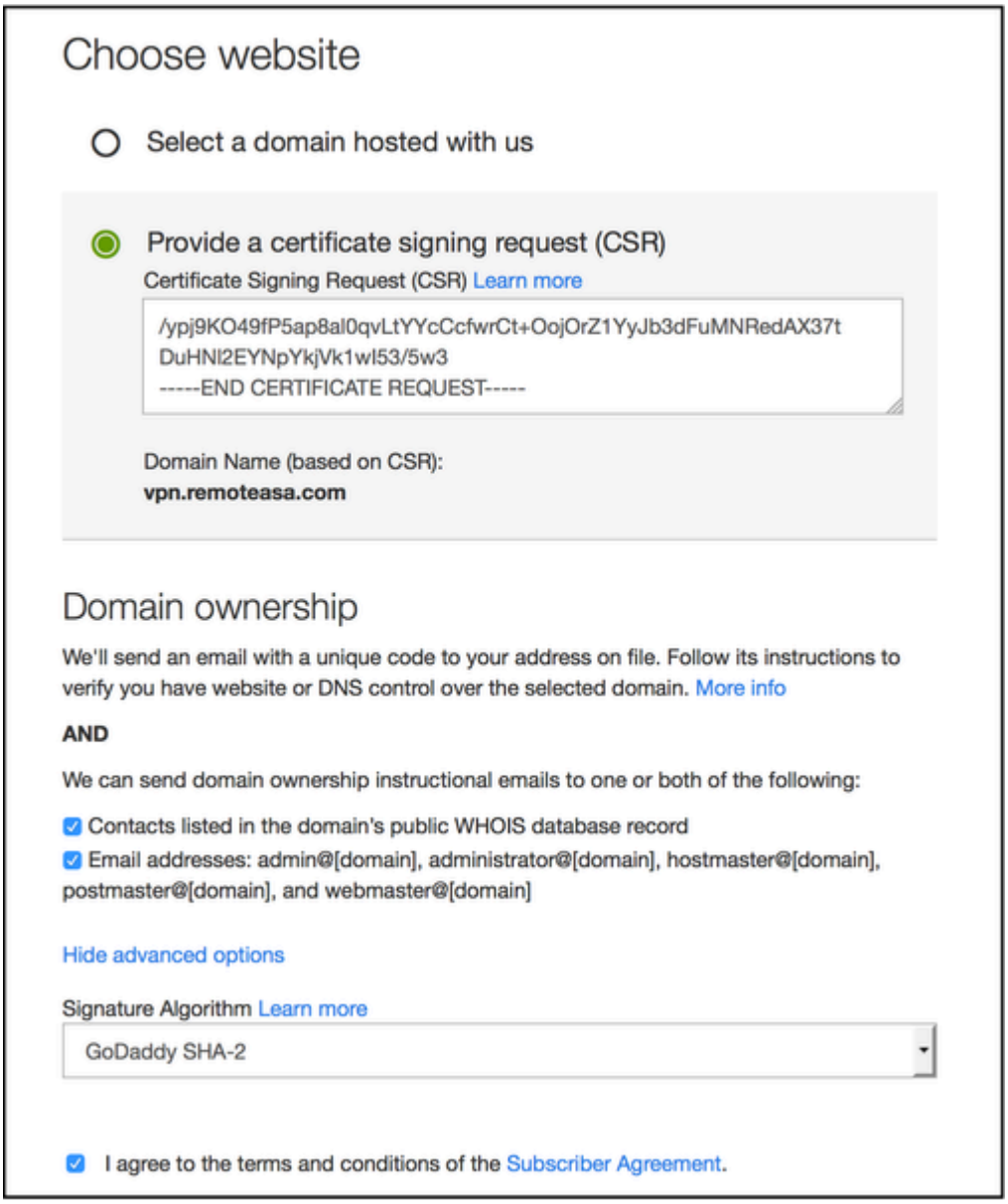
购买后，在SSL证书的初始设置阶段，导航到GoDaddy帐户并查看SSL证书。必须有新证书。点击 **Manage** ，继续。



这将打开一个页面以提供 CSR，如图所示。

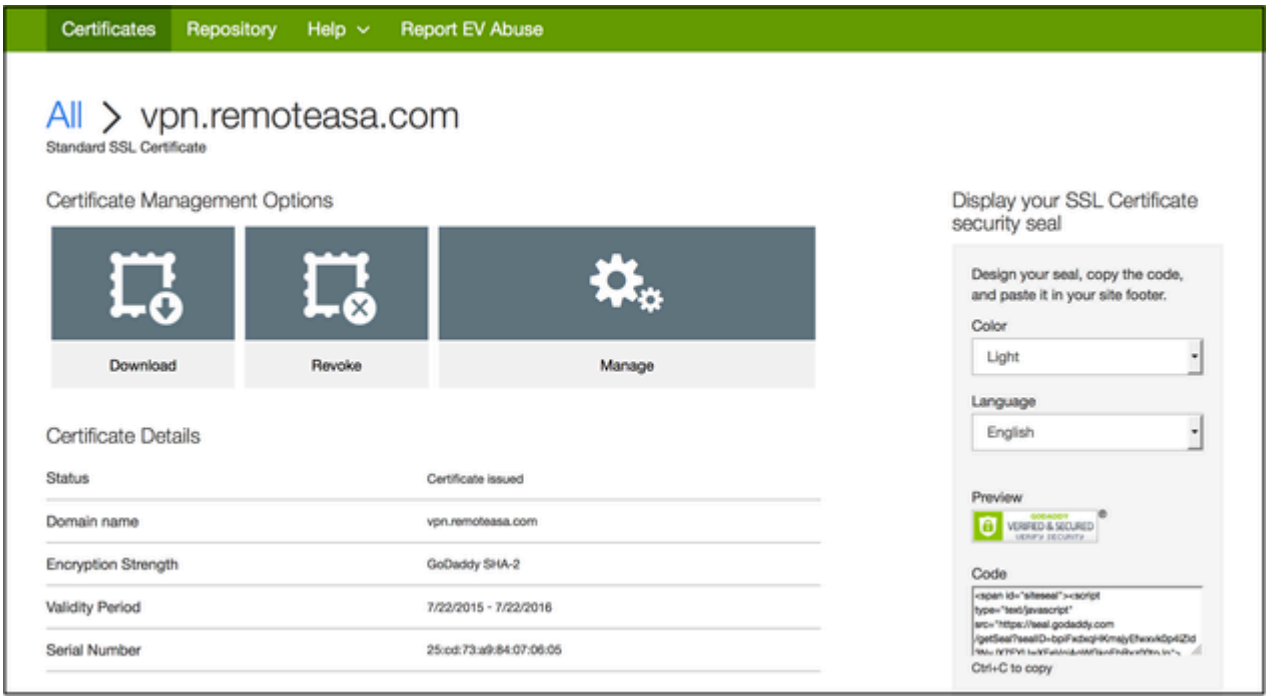
根据输入的 CSR，CA 确定要将证书颁发给哪个域名。

验证该域名与 ASA 的 FQDN 是否匹配。

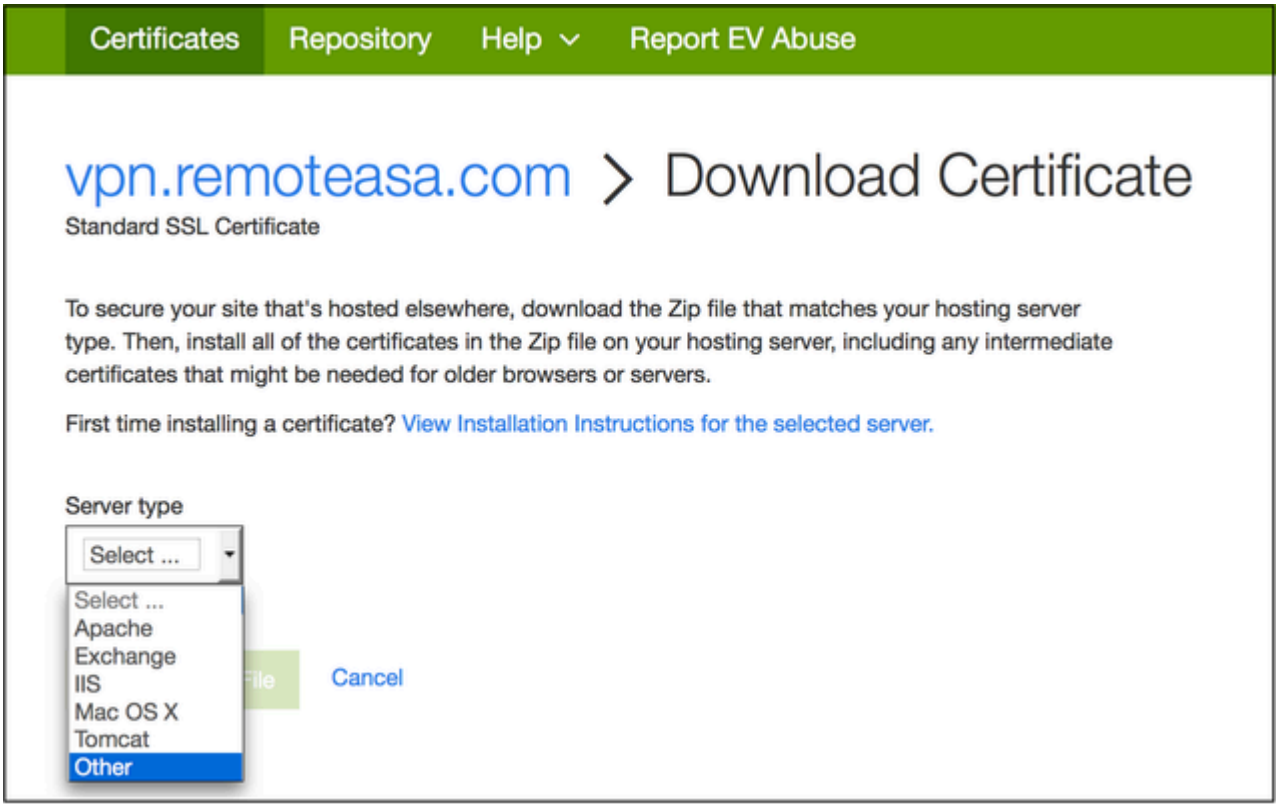


注意： GoDaddy 和大多数其他 CA 使用 SHA-2 或 SHA256 作为默认证书签名算法。ASA支持从8.2(5)[8.3之前版本]和8.4(1)[8.3之后版本]开始的SHA-2签名算法(Cisco Bug ID CSCti30937)。 如果使用的版本早于 8.2(5) 或 8.4(1)，请选择 SHA-1 签名算法。

提交请求后，GoDaddy将验证该请求，然后颁发证书。在验证证书请求后，GoDaddy将证书颁发给帐户。然后可以下载证书，以便在ASA上安装。单击页面以继续操作**Download**。



选择Other“Server Type”并下载certificate zip捆绑包。



.zip 文件包含身份证书和 GoDaddy CA 证书链捆绑包，作为两个单独的 .crt 文件。继续进行 SSL 证书安装，以便在 ASA 上安装这些证书。

ASA 上的 SSL 证书安装

可通过使用 ASDM 或 CLI 这两种方式在 ASA 上安装 SSL 证书：

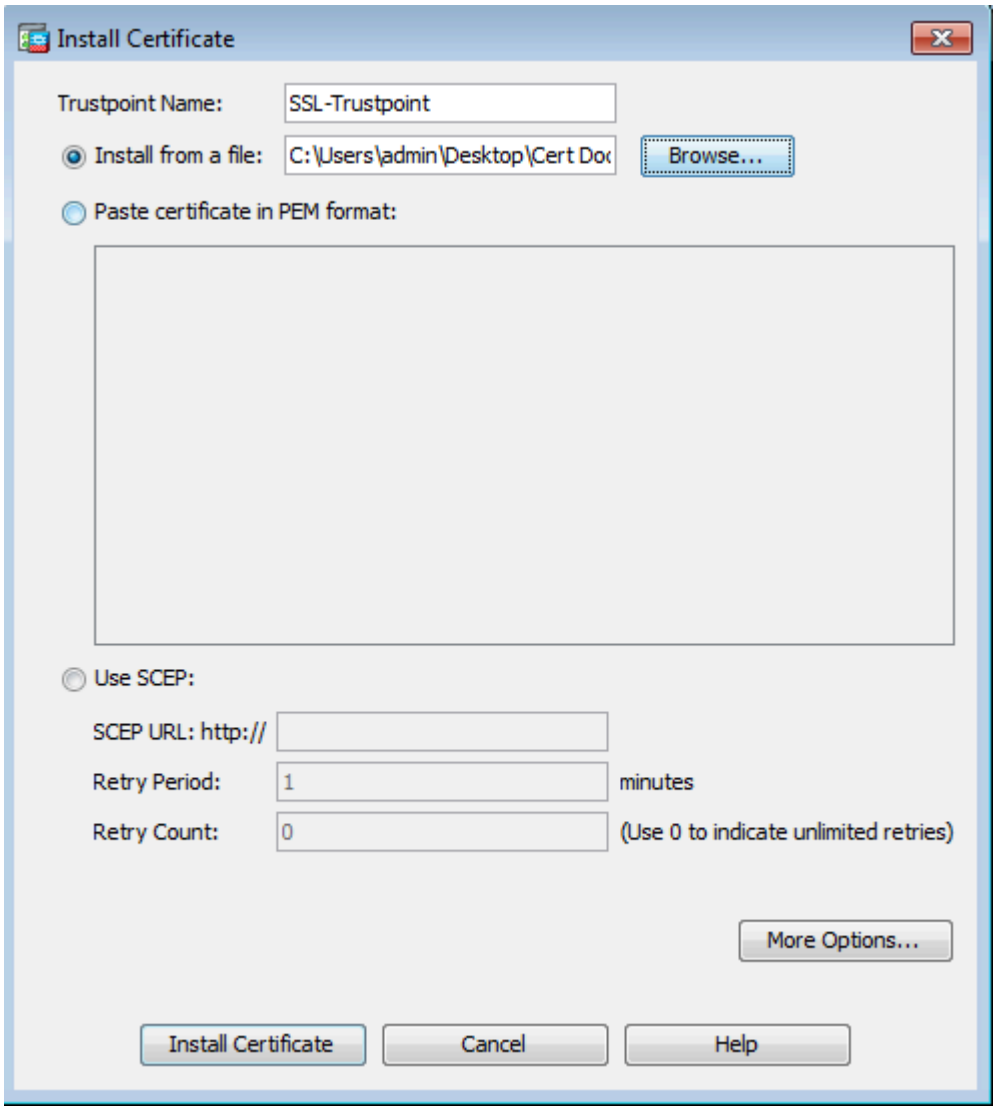
1. 以 PEM 格式分别导入 CA 和身份证书。
2. 或导入 PKCS12 文件（对于 CLI，则为 base64 编码文件），其中身份证书、CA 证书和私钥捆绑在 PKCS12 文件中。

> 注意： 如果 CA 提供 CA 证书链，请仅在用于生成 CSR 的信任点的层次结构中安装直接中间 CA 证书。根 CA 证书和任何其他中间 CA 证书均可安装于新的信任点中。

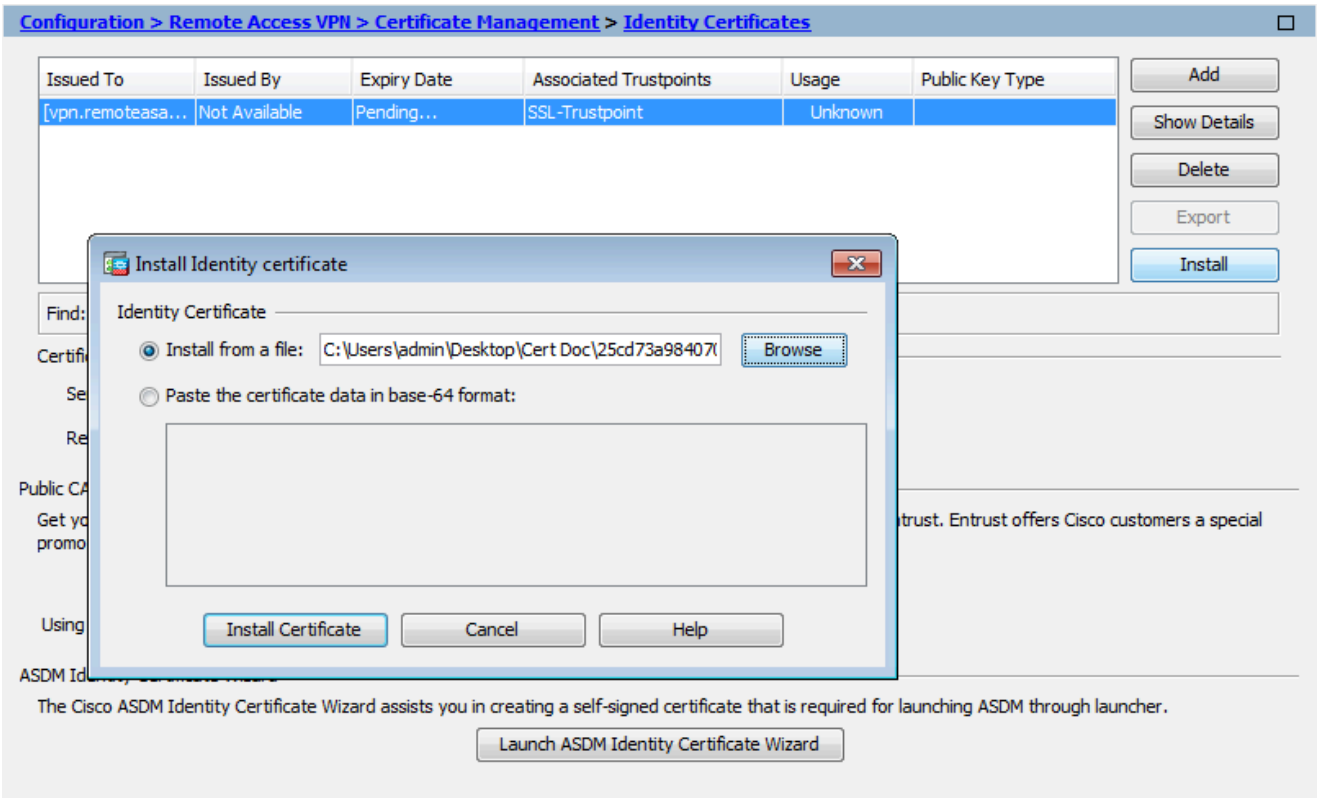
1.1 使用 ASDM 安装 PEM 格式身份证书

给定的安装步骤假定 CA 提供的是 PEM 编码的（.pem、.cer 和 .crt）身份证书和 CA 证书捆绑包。

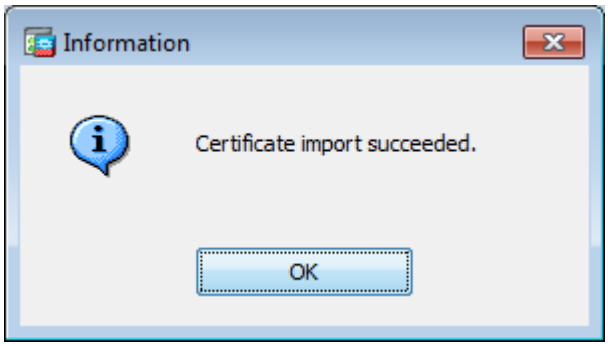
1. 导航至 **Configuration > Remote Access VPN > Certificate Management**，，然后选择CA Certificates。
2. 在文本编辑器中使用 PEM 编码的证书，并将第三方供应商提供的 base64 CA 证书复制和粘贴到文本字段中。



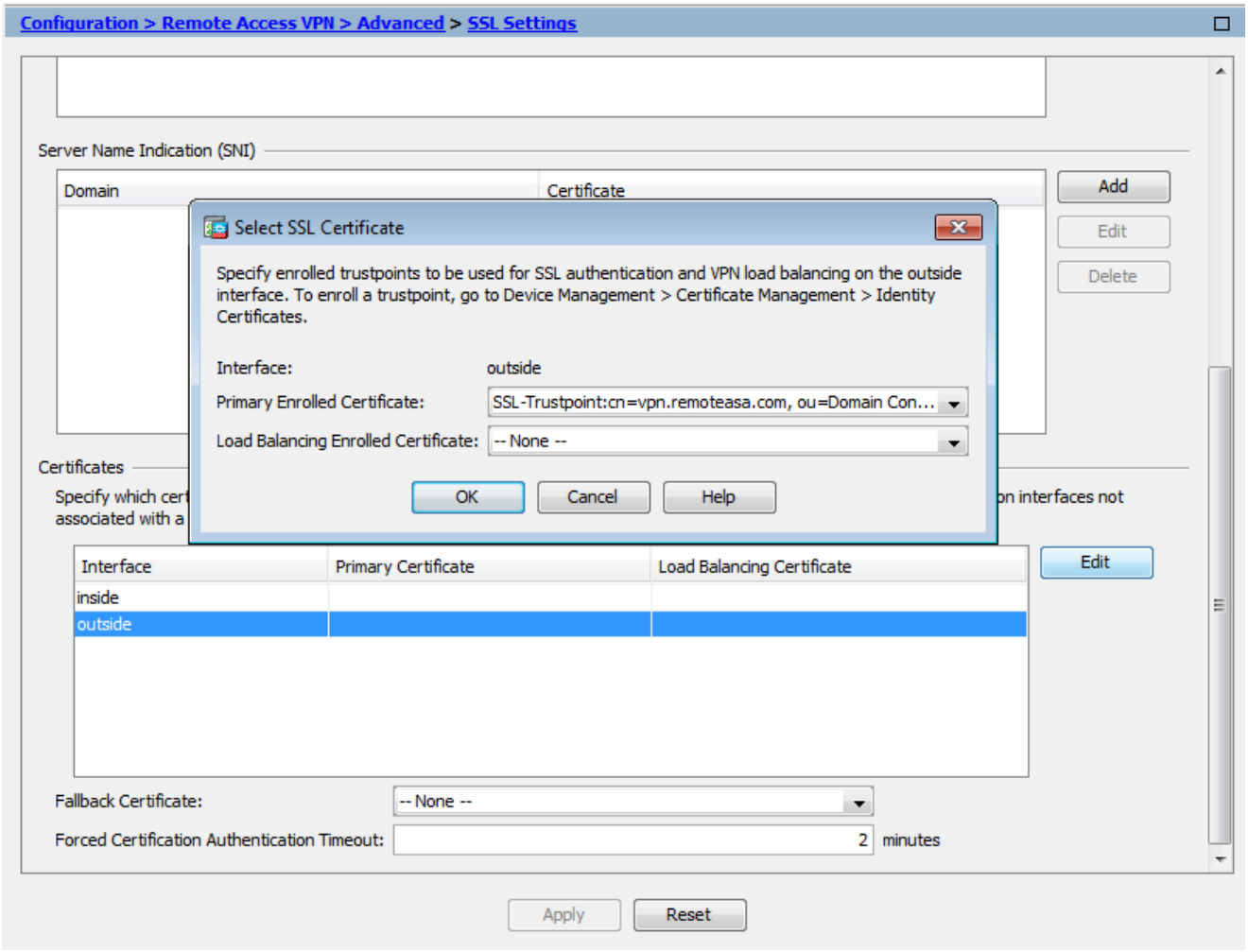
3. 单击 Install Certificate。
4. 导航至**Configuration > Remote Access VPN > Certificate Management**，然后选择身份证书。
5. 选择先前创建的身份证书。点击 **Install**.
6. 单击选项单选按钮并选择PEM编码的身份证书**Install from a file**，或者打开文本编辑器中的PEM编码的证书，复制并粘贴第三方供应商提供的base64身份证书到文本字段中。



7. 点击**Add Certificate**.



8. 依次导航至 **Configuration > Remote Access VPN > Advanced > SSL Settings**.
9. 在“证书”下，选择用于端接 WebVPN 会话的接口。在本例中，使用的是外部接口。
10. 点击**Edit**.
11. 在“证书”下拉菜单中，选择新安装的证书。



12. 点击OK.
13. 点击Apply.“新证书现在用于终止于指定接口的所有WebVPN会话”。

1.2. 使用 CLI 安装 PEM 证书

<#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 MB8GA1UEChI

!!! - 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
Y29tLCBJbmMuMTEwLwYDVQQDEyhHbyBEYWRkeSBSb29tIENlcnRpZmljYXRlIEF1
dGhvcml0eSAtIEcyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAv3Fi
CPH6WTT3G8kYo/eASVjpIoMTpsUgQwE7hPHmhUmfJ+r2hBtOoLTbcJjHMgGxBT4H
Tu70+k8vWTAi56sZVmvigAf88xZ1gDlRe+X5NbZ0TqmNghPktj+pA4P6or6KFWp/
3gvDthkUBcrqw6gElDtGfDIN8wBmIsiNaW02jBEYt9OyHGC0OPoCjM7T3UYH3go+
6118yHz7sCtTpJJiaVElBWEaRIGMLKlDliPfrDqBmg4pxRyp6V0etp6eMAo5zvGI
gPtLXcwy7IViQyU0AlYnAZG0O3AqP26x6JyIAX2f1PnbU21gnb8s51iruF9G/M7E
GwM8CetJMVxpRrPgRwIDAQABo4IBFzCCARMwDwYDVR0TAQH/BAUwAwEB/zAOBgNV
HQ8BAf8EBAMCAQYwHQYDVR0OBBYEFDqahQcQZyi27/a9BUFuIMGU2g/eMB8GA1Ud
IwQYMBaAFNLEsNKR1EwRcbNhyz2h/t2oatTjMDQGCCsGAQUFBwEBBCgwJjAkBggr
BgEFBQcwAYYYaHR0cDovL29jc3AuZ29kYWRkeS5jb20vMDIGA1UdHwQrMCkwJ6Al
oCOGIWh0dHA6Ly9jcmwuZ29kYWRkeS5jb20vZ2Ryb29LmNybDBGBgNVHSAEPzA9
MDsGBFUdIAAwMzAxBggrBgEFBQcCARYlaHR0cHM6Ly9jZXJ0cy5nb2RhZGR5LmNv
bS9yZXBvc2l0b3J5LzANBgkqhkiG9w0BAQsFAAOCAQEAWQtTvZKGEacke+1bMc8d
H2xwxbhuvk679r6XUOEwf7ooXGKUwuN+M/f7QnaF25UcjCJYdQkMiGVnOQoWCcWg
OJekxSOTP7QYpgEGRJHjp2kntFolfzq3Ms3dhP8qOCkzpN1nsoX+oYggHFCJyNwq
9kIDN0zmiN/VryTyscPfzLXs4JletOlUIDyUGAzHHFIYSaRt4bNYC8nY7NmuHDKO
KHAN4v6mF56ED71XcLNa6R+ghlO773z/aQvgSMO3kwvIClTErF0UZzdsyqUvMQg3
qm5vjLyb4lddJIGvl5echK1srDdMZvNhkREg5L4wn3qkKQmw4TRfZHcYQFHfjDCm
rw==
-----END CERTIFICATE-----
quit

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

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

Trustpoint CA certificate accepted.

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

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

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

MainASA(config)#

crypto ca import SSL-Trustpoint certificate

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

yes

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

(asa.remotevpn.url)

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

```
----BEGIN CERTIFICATE-----
MIIFRjCCBC6gAwIBAgIIJc1zqYQHBgUwDQYJKoZIhvcNAQELBQAwgbQxCzAJBgNV
BAYTAlVTMRAwDgYDVQQIEwdBcml6b25hMRMwEQYDVQQHEwpTY29OdHNkYWxlMRow
GAYDVQQKExFHb0RhZGR5LmNvbSwgSW5jLjEtMCsGA1UECxMkaHR0cDovL2NlcnRz
LmdvZGFkZHkuY29tL3JlcG9zaXRvcnkvMTMwMQYDVQQDEypHbyBEYWRkeSBTZWN1
cmUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5IC0gRzIwHhcNMTUwNzIyMTIwNDM4WhcN
MTYwNzIyMTIwNDM4WjA/MSEwHwYDVQQLExhEb21haW4gQ29udHJvbCBWYWxpZGF0
ZWQxGjAYBgNVBAMTEXZwbi5yZW1vdGVhc2EuY29tMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEArrY2Fv2S2Uq5HdDhOaSzK5Eyok2tv2Rem8DofbTQ+4F9
C9IXitWdLAo6a7dzyfB4S9hx1VZXoHMGGNd6i9NWLXsWU1Nx5pRMaKR4h1cL6bDW
ITt5GzKdL93ibMxYmau+uwM3OkBb8QxLNNxr4G+oXtfavctTxWy/o6LzKWFyjOXP
tta9FZWO7cOMNvKiUL1v9WBcy4GK1xyvN9RtWebtVkM5/iOvOReBTBfFxCJ1YQAG
UWteu1ikWAGj1qomZGnZgAFDWJ4/hxjesG2BGMtwX5L1O8cbmbi/u/vnmZ5Xhiqx
<snip>
CCsGAQUFBwIBFitodHRwOi8vY2VydGlmaWNhdGVzLmdvZGFkZHkuY29tL3JlcG9z
aXRvcnkvMHYGCCsGAQUFBwEBBGowaDAkBggrBgEFBQcwAYYYaHR0cDovL29jc3Au
Z29kYWRkeS5jb20vMEAGCCsGAQUFBzAChjRodHRwOi8vY2VydGlmaWNhdGVzLmdv
ZGFkZHkuY29tL3JlcG9zaXRvcnkvZ2RpZzIuY3JOMB8GA1UdIwQYMBaAFEDCvSeO
zDSDMKIz1/tss/C0LIDOMEYGA1UdEQQ/MD2CEXZwbi5yZW1vdGVhc2EuY29tghV3
d3cudnBuLnJlbW9OZWFzYS5jb22CEXZwbi5yZW1vdGVhc2EuY29tMB0GA1UdDgQW
BBT7en7YS3PH+s4z+wTRlpHr2tSzejANBgkqhkiG9w0BAQsFAAOCAQEAO9H8TLNx
2YOrYdI6gS8n4imaSYg9Ni/9Nb6mote3J2LELG9HY9m/zUCR5yVktra9azdrNUAN
1hjBJ7kKQScLC4sZLONdqG1uTP5rbWROyikF5wSzgyMWdO3kOR+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

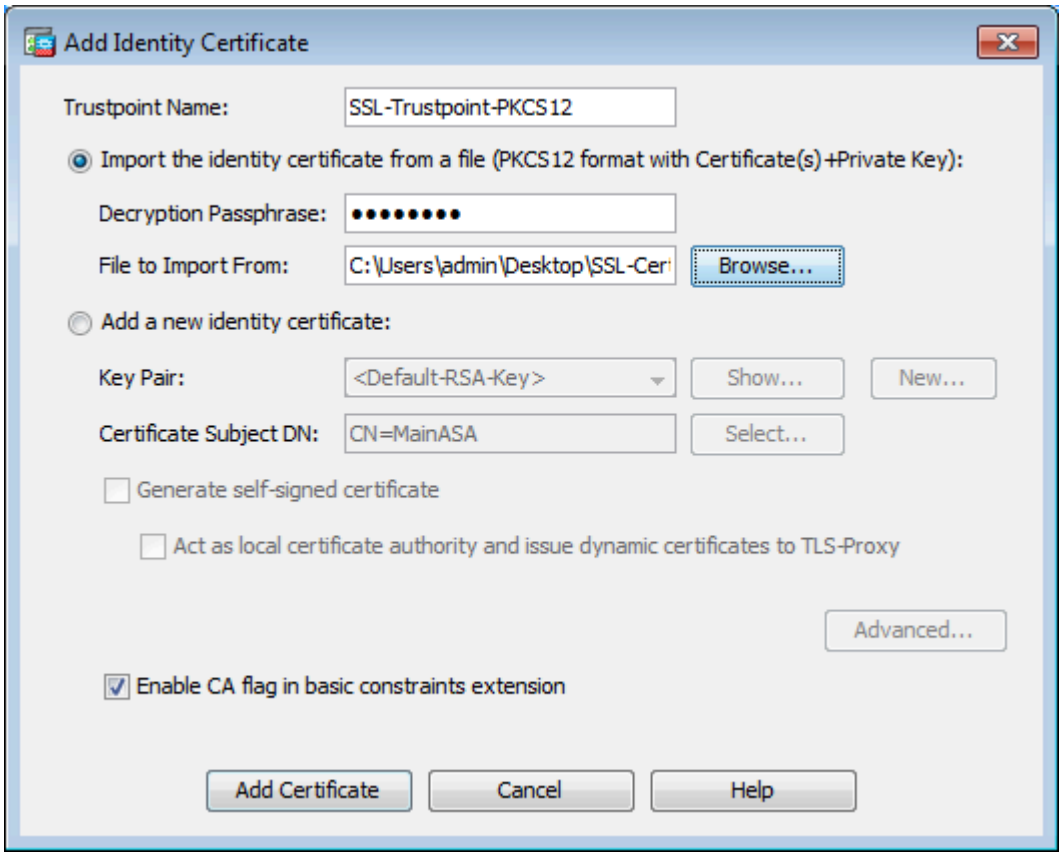
MainASA(config)#
```

ssl trust-point SSL-Trustpoint outside

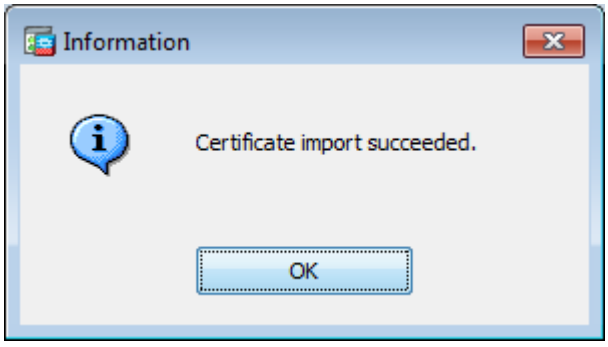
2.1 使用 ASDM 安装 PKCS12 证书

在ASA上未生成CSR的情况下，例如通配符证书或生成UC证书时，身份证书和私钥作为单独的文件或单个捆绑的PKCS12文件（.p12或pfx格式）接收。 要安装此类型的证书，请完成以下步骤。

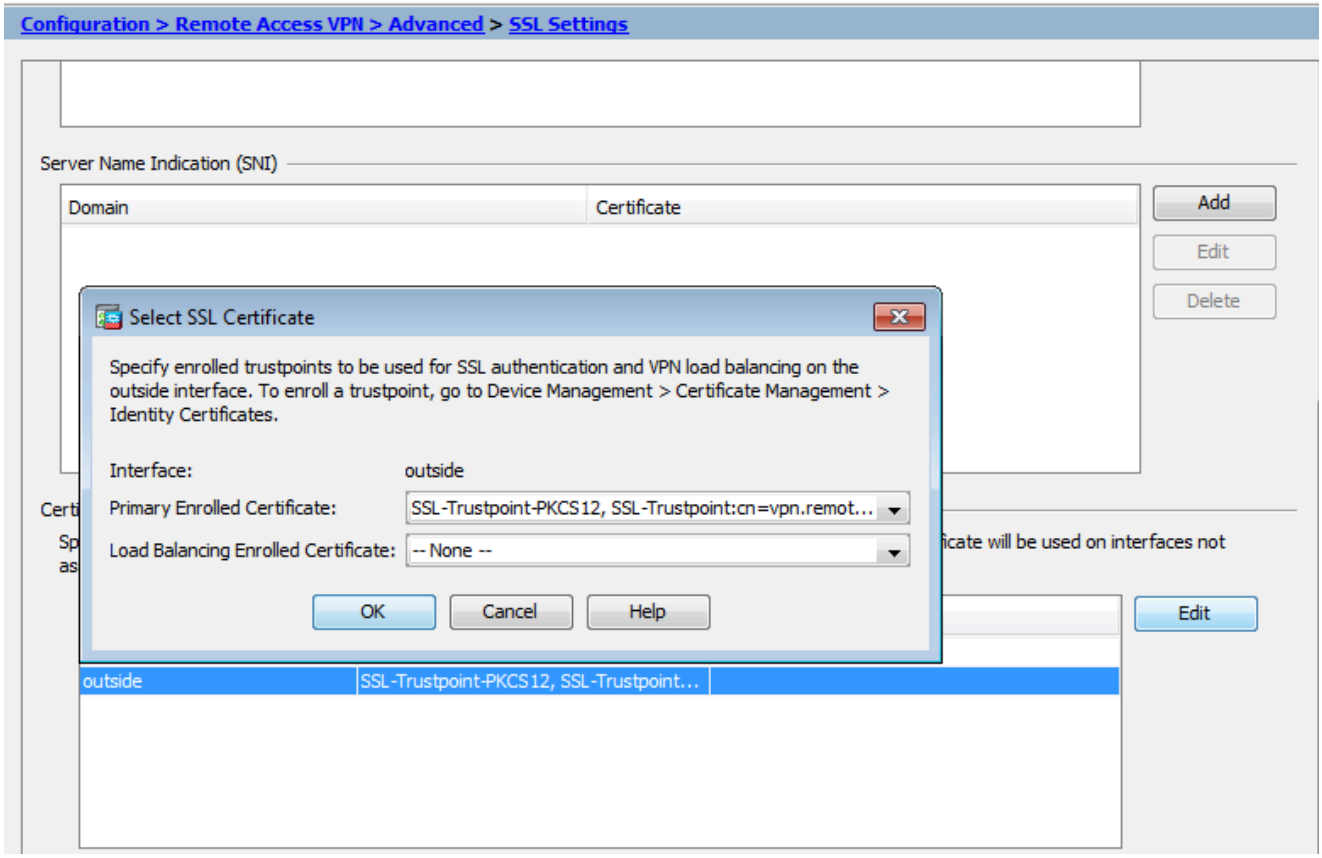
1. 在身份证书中，将CA证书和私钥捆绑到单个PKCS12文件中。 附录 B 介绍了使用 OpenSSL 执行此操作的步骤。如果已由 CA 进行捆绑，请继续下一步。
2. 导航至**Configuration > Remote Access VPN > Certificate Management**，，然后选择 **Identity Certificates**.
3. 点击**Add**.
4. 指定信任点名称。
5. 点击单**Import the identity certificate from a file**选按钮。
6. 输入用于创建 PKCS12 文件的密码。浏览并选择 PKCS12 文件。输入证书密码。



7. 点击添加证书。



8. 导航Configuration > Remote Access VPN > Advanced,至并选择 SSL Settings.
9. 在“证书”下，选择用于端接 WebVPN 会话的接口。在本例中，使用的是外部接口。
10. 点击Edit.
11. 在“证书”下拉菜单中，选择新安装的证书。



12. 点击OK.
13. Apply.点击New certificate is now used for all WebVPN sessions that terminate on the interface specified.

2.2 使用 CLI 安装 PKCS12 证书

```
<#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/LkNbmGDVhwGBmYWiOS7npgaUqOeoqiJRK+Yc7
LNOnbho6I5WfL56/JiceAMlXDLr/IqqLg2QAApGdN+F5vANsHse2GsAATewBDLt7
Jy+SKfoNvvIw9QvzCiUzMjYZBANmBdMCQ13H+YQTHitT3vn2/iCDlzRSuXcqypEV
q5e3heiOO75lE8TDLWmO3PMvwIZqi8yzWesjcTt1Kd4FoJBZpB70/v9LntoIUOY7
kIQM8fHb4ga8BYfbgRmG6mkMmO1STtbSvlvTa19WTmdQdTyCa+G5PkrryRsy3Ww1
lkGFMhImmrnNADF7HmzbyslVohQZ7h09iVQY9krJogoXHjmQYxG9brf0oEwxSJDa
mGDhhESh+s/WuFSV9Z9kiTXpJNZxpTASoWBQrrwmO5v8ZwbjbVNJ7sVdbwpUl6d+
NNFGR7LTqO8hpupeeJnY9eJc2yYqeAXWXQ5kLOZo6/gBEdGtEaZBgCFK9JZ3bl3A
xqxGifanWPnLYG611NKuNjTgbjhnEEYI2uZzUOqxnlKa8zyXw+lzrKuJscDbkAPZ
wKtw8K+p4OzXVHhuANo6MDvffNRY1KQDtyK1inoPH5ksVSE5awkVam4+HTcqEUfa
16LMana+4QRgSetJhUOLtSMaQfRJGkha4JLq2t+JrCAPz2osARlTsBOjQBNq6YNj
0uB+gGk2Gl8Q5Nln6K1fz0XBFZLWEDBLsaBRO5MAnE7wWtOO+4awGYqVdmIF1lkf
XIRKAiQEr1pZ6BVPuvsCNJxaaUHzufhYI2ZAckasKBZOT8/7YK3fnAaGoBCz4cHa
o2EEQhq2aYb6YTv0+wtLEWGHzsbGZEM/u54XmsXAI7g28LGJYdfWi5O9KyV+Ac1V
KzHqXZMM2BbUQCNcTF5JIMiW+r62k42FdahfaQb0vJsIe/IwkAKG7y6DIQFs0hwg
ZlPXiDbNr1k4e8L4gqupMKWg853PY+oY22rLDC7bul1CKtixIYBCvbn7dAYsI4GQ
l6xXhNu3+iye0HgbUQQCfTU/mBrA0ZO+bpKjWOCfqNBuYnZ6kUEdCI7GFLH9QqtM
K7YinFLoHwTWbi3MsmqVv+Z4ttVWy7XmikoO2nMynJMP6/CNV8OMxMKdC2qm+c1j
s4QlKcAmFsQmNp/7SIP1wnvOc6JbUmC1O52OU/r8ftTzn8C7WL62W79cLK4HOr7J
sNsZnOz0JOZ/xdZT+cLTCtVevKJOQMK3vMsiOuy52FkuF3HnfrmBqDkbR7yZxELG
RCELOEDdbp8VP0+IhNlyz1q7975SscdxFSLOTvjnHGFWd14ndoqN+bLhWbdPjQWV
l3W2NCI95tmHDLGgp3POOlS+RjdCEGGMg+9cpgBfFC1JocuTDIEcUbJBY8QRUNiS
/ubyUagdzUKt1ecfb9hMLP65ZNQ93VIw/NJKbIm7b4P/1Zp/lFP5eq7LkQPAxE4/
bQ4mHcnwrs+JGFkN19B8hJmmGoowH3p4IEvwZy7CThB3E1ejw5R4enqmrgvHqpQe
B7odN1OFLAHdo1G5BsHExluNEsEb4OQOpmKXidDB5BOO1bJsr748fZ6L/LGx8Al3
<snip>
ijDqxyfQXY4zSytljSMwMtYA9hG5I79Sg7pnME1E9xq1DOoRGg8vgxlwiciKtLxp
LLOReDY31KRYvOOvWOgf+tE7lST/3TKZvh0sQ/BEOV3kHnwldejMFH+dvyAA9Y1E
c8O+tdafBFX4B/HP46E6heP6ZSt0xAfRW1/JF4ljNvUNVO9VtVfR2FTyWpzZFY8A
GG5XPIA8OWF6wKEPFHIcN8scY+Vot8kXxG96hwt2Cm5NQ2OnVzxUZQbpKsjs/2jC
3HVFe3UJFBsY9UxTLcPXYBSIG+VeqkI8hWZp6clTfNDLY2ELDylQzp1mBg2FujZa
YuEOavjCJzBzZUG2umtS5mHQnwPF+XkOujEyhGMauhGxHp4nghSzrUZrBeuL9lUF
2mbpsOcgZkzxMS/rjdNXjCmPFloRBvKkZSlxHFrE/5ZopAhn4i7YtHQNrz9U4RjQ
xo9cUuaJ+LNmvzE8Yg3epAMYZ16UNGQQkVQ6ME4BcjRONzW8BYgTq4+pmT1ZNq1P
X87CXCPtYRpHF57eSo+tHDINCgfqYXD6e/7r2ngfiCeUeNDZ4aVl2XxvZDaUlBPP
Tx5fMARqx/Z8BdDyBJDVBjdsxmQau9HLkhPvdfGlZIWdTe13CzKqXA5Ppmpjt4q9
GnCpC53m76x9Su4ZDw6aUdBcgCTMvfaqJC9gzObee2Wz+aRRwzSxu6tEWVZolPEM
v0AA7po3vPeklgOnLRAwEoTTn4SdgNLWeRoxqZgkw1FC1GrotxF1so7uA+z0aMeU
lw73reonsNdZvRAcVX3Y6UNFdyt7OIxvo1H4VLzWmOK/oP62C9/eqqMwZ8zoCMPt
ENna7T+7Os66SCbMmXCHwyhOOtygNKZFFw/AATFyjqPMWPAxGuPNOrnB6uYCn0Hk
1BU7tF143RNIZaQQEH3XnaPvUuAA4C0FCoE3h+/tVjtfNKDvFmb6ZLZHYQmUYpyS
uhdFEpoDrJH1VmI2Tik/iqYWaZ+oDqXPHQXnJhw25h9ombR4qnD+FCfwFCGtPFON
o3QffZ53C95n5jPHVMyUrOxDdpwnvzCQPdj6yQm564TwLAmiz7uDlpqJZJe5QxHD
nolv+4MdGSfVtBq+ykFoVCaamqeaq6sKgvAVujLXXEs4KEmIgcPqATVRG49ElndI
LO1DEQyKhVoDGebAuVRBjzwAm/qxWxxFv3hrbCjpHCwEYms4Wgt/vKKRFsuWJNZf
efHldwlltkd5dKwSvDocPT/7mSLtLJa94c6AfgxXy9zO+FTLDQwzxga7xC2krAN1
yHxR2KHN5YeRL+KDzu+u6dYoKAz+YAgwlW6KbeavALSuH4EYqcvg8hUEhp/ySiSc
RDhuygxEovIMGfES4FP5V52lPyDhM3DqwhnOvuYUmYnX8EXURkay44iwwI5HhqYJ
lptWyYo8Bdr4WNwt5xqszGzYR6mmGeAIin7bDunsF1uBHWYF4dyKlz1tsdRNMYqQ
```

```
+W5q+QjVdrjldWv/bMFOaqEjxeNWBRqjzcff3BxMnwvVxtgqxFvRh+DZxiJoiBG+
yx7x8np2AQ1rOMETSSxbnZzfnKZKVvBVMkIC6Jsmt2WEVTQvoFJ8em+nemOWgTi/
hHSBzjE7RhAucnHuifOCXOgvR1SDDqyCQbiduc1QjXNOsvA8Fqbea9WEH5khOPv3
pbtsL4gsfl2pv8diBQkVQgiZDi8Wb++7PR6ttiY65kVwrdsoNl1/qq+xWOd3tB4/
zoH9LEMgTy9Sz7myWrB9EOOZ8BIjL1M8oMigEYrTDOc3KbyW1S9dd7QAxiuOBaX1
8J8q1OydvTBzmqcjeSsFH4/1NHn5VnfOZnNpui4uhpOXBG+K2zJUJXm6dq1AHBlE
KQFsFZpNNyaveOKk8JzQnLAPd7OUU/IksyOCGQozGBH+HSzVp1RDjrrbC342rkBj
wnI+j+/1JdWBmHdJMZCfoMZFLSI9ZBqFirdii1/NRu6jh76TQor5TnNjxIyNREJC
FE5FZnMFvhM9OOLaiUZff8WWCOfeRDMttLXb1nuxPFl+lRk+LNlPLVptWgcxzfsr
JXrGiwjxybBB9oCOrACq8fGAtEs8WRxJyDH3Jjmn9i/Gl6J1mMCUF//LxAH2WQx8
Ld/qS5OM2iFCffDQjxAj0K6DEN5pUebBv1Em5SOHXvyq5nxgUh4/y84CWaKjw0MQ
5tbbLMlnc7ALIJ9LxZ97YiXSTyeM6oBXBFx6RpklkDvO5mlBghSpVQiMcQ2ORIkh
UVVNbSHOl9S3cb5wqxaWqAKBqb4h1uLGVbYWZf2mzLZ8U5U5ioiqoMBqNZbzTXpO
EqEFuatTllQvCRbcKS3xou4MAixcYUxKwEhbZA/6hd1OXSBJwe7jKBV9M6wliKab
UfoJCGTAf3sY68lqrMPrbBtOeeWf1CO2Sd9Mn+V/jvnil7mxYFFUpruRq3r1LeqP
J5camfTtHwyL8N3Q/Zwp+zQeWZiLA8a/iAVu/hYLR1bpF2WCKOlOtJqkvVmrLVLz
maZZjbJeOft5cP/lRxbKlS6Gd5dFTEKDE15c6gWUX8RKZP6Q7iaE5hnGmQjm8Ljl
kXwF+ivoxOQ8a+Gg1bVTROc7tqW9e9/ewisV1mwvEB6Ny7TDS1oPUDHM84pY6dqi
1+Oio07Ked4BySwNlYy9yaJtBTZSCstfP+ApLidN7pSBvvXf1aHmeNbkPOZJ+c+t
fGpUdL6V2UTXfCsOPHTCOezA15sOHwCuPchrDIj/eGUwMS3NfS25XgcMuvnLqGVO
RzcRzlZIg8GOoLYwOCuzoYOD/m9O1OO1ahePyA9tmVB7HRRbytLdaW7gYeEikoCv
7qtBqJFF17ntWJ3EpQHZUcVClbHIKqjNqRbDCY7so4AlIW7kSEUGWMIUDhprE8Ks
NpnvPH2i9JrYrTeROyUIOtL/7SATd2POa2lxz/zUWekeqdObmVCsAgQNbB2XkrR3
XSOB52ol+63e8KDqS2zL2TZd3daDFidHlB8QB26tfbfOAcaObJH5/dWP8ddo8UYo
Y3JqTlOmalxSJhaMHmQdZIQp49utW3TcjqGllYS4HEmcqtHudOShaUysC6239jlQ
KlFWrwXTlBC5vnq5IcOMqx5zyNbfxXz28969cWoMCyU6+kRwOTyF6kF7EEv6XWca
XLEwABx+tKRUKHJ673SyDMu96KMV3yZN+RtKbCjqCPVTP/3ZeIp7nCMUcj5sW9HI
N34yeI/ORCLyeGsOEiBLkucikC32LI9ik5HvImVTELQOUz3ceFqU/PkasjJUve6S
/n/1ZVUHbUk71xKR2bWZgECl7fIel7wlrbjpF3Wbk+ErOkfYcsNRHxeTDpKPSt9s
u/UsyQJiyNARG4X3iYQlsTce/O6Ycyri6GcLHAu58BO2nj4CxolCplABZ2N79HtN
/7Kh5LOpS9MwsDCHuUI8KFrTsET7TB1tIU99FdB19L64sl/shYAHbccvVWU5OWht
PdLoaErrX81Tof41IxbSZbI8grUC4KfG2sdPLJKu3HVTeQ8LfllbBLxfs8ZBS+Oc
v8rHlQO12kY6LsFGLehJ+/yJ/uvXORivOESp4EhFpFfkp+o+YcFeLUUPd+jzb62K
HfSCCbLpCKyEay8OdyWkHfgylqxmb9udOoMO5OaFJyqRONjNt6pcxBRY2A6AJR5S
IIC26YNwbhOGjF9qL2FiUqnNH/7GTqPnd2qmsB6FTIwSBT6d854qN7PRt+ZXgdtQ
OjcYt1r9qpWDZpNFK8EzizwKiAYTsiEh2pzPt6YUpksRb6CXTkIzoG+KLsv2m3b8
OHyZ9a8z81/gnxrZlls5SCTfOSU7OpHWh8VAYKVHHK+MWgQrOm/2ocV32dkRBLMy
2R6P4WfHyI/+9de1x3PtIuOiv2knpxHv2fKM6sQw45F7XkmwHxjq1YRJ6vIwPTAh
MAkGBSsOAwIaBQAEFFTRETzpisHKZR+Kmen68VrTwpV7BBSQiOIesQ4n4E/bSVsd
qJSzcwhOhgICBAA=
-----END PKCS12-----
quit
```

INFO: Import PKCS12 operation completed successfully

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

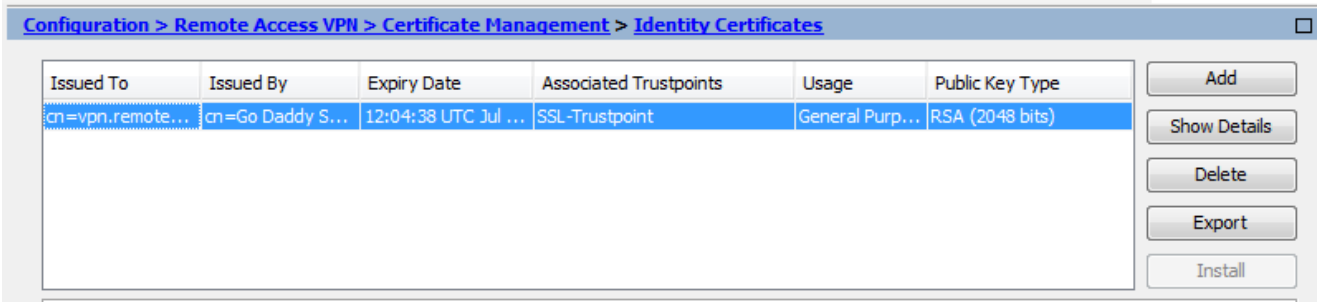
ssl trust-point SSL-Trustpoint-PKCS12 outside

验证

使用这些步骤验证第三方供应商证书的成功安装和 SSLVPN 连接的使用。

通过 ASDM 查看已安装的证书

1. 导航**Configuration > Remote Access VPN > Certificate Management**,至并选择 **Identity Certificates.**
2. 随即显示由第三方供应商颁发的身份证书。



通过 CLI 查看已安装的证书

<#root>

```
 MainASA(config)#
```

show crypto ca certificate

Certificate

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

SSL-Trustpoint

CA Certificate

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

SSL-Trustpoint

CA Certificate

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

```
    [1]  http://crl.godaddy.com/gdroot.crl
  Validity Date:
    start date: 07:00:00 UTC Jan 1 2014
    end   date: 07:00:00 UTC May 30 2031
  Associated Trustpoints:

SSL-Trustpoint-1

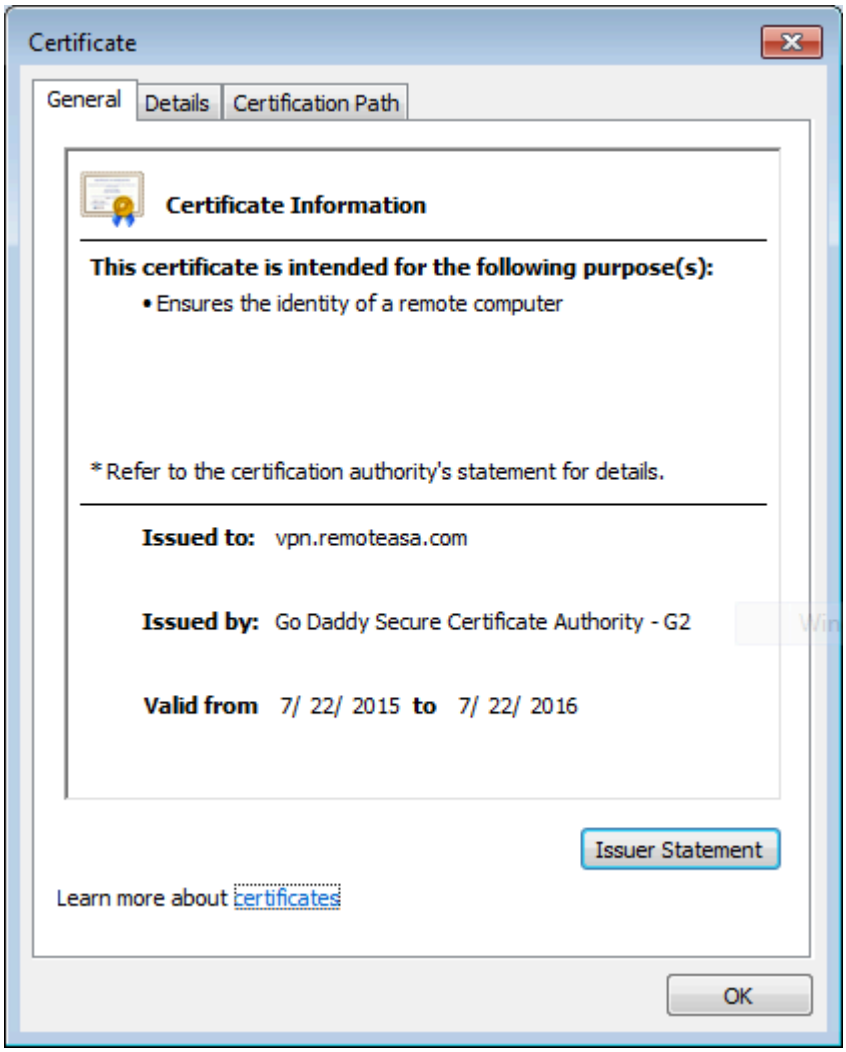


...(and the rest of the Sub CA certificates till the Root CA)
```

使用 Web 浏览器验证为 WebVPN 安装的证书

验证 WebVPN 已使用新证书。

1. 通过 Web 浏览器连接至 WebVPN 界面。将https://与用于请求证书的FQDN一起使用（例如，WebVPN接口）
2. 双击WebVPN登录页面右下角出现的lock图标。系统必须显示已安装的证书信息。
3. 查看内容，以验证其是否与第三方供应商颁发的证书匹配。

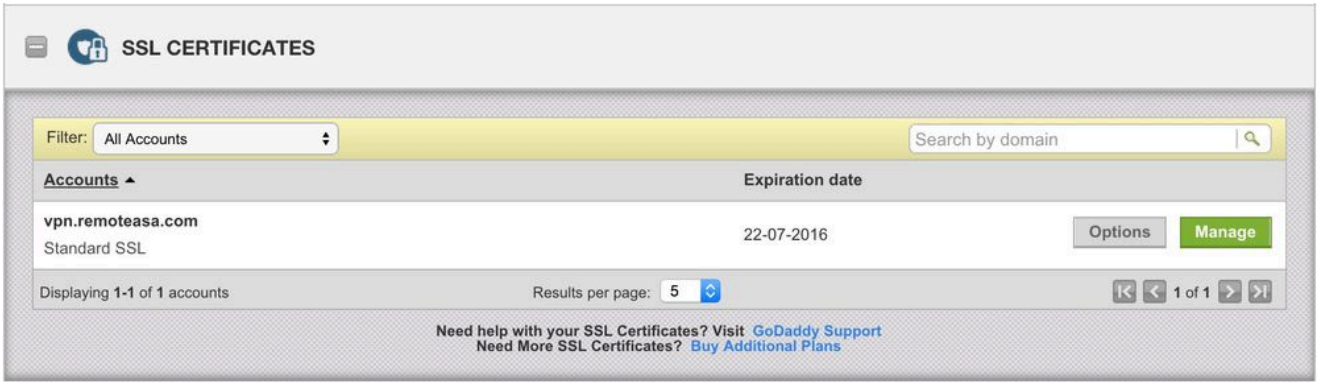


在 ASA 上续订 SSL 证书

1. 在ASA、OpenSSL或CA上重新生成CSR，其属性与旧证书相同。完成CSR Generation中给定的步骤。
2. 在 CA 上提交 CSR，并与 CA 证书一起生成 PEM 格式（.pem、.cer 和 .crt）的新身份证书。对于PKCS12证书，还有一个新的私钥。

   对于 GoDaddy CA，可使用生成的新 CSR 重新获取证书密钥。

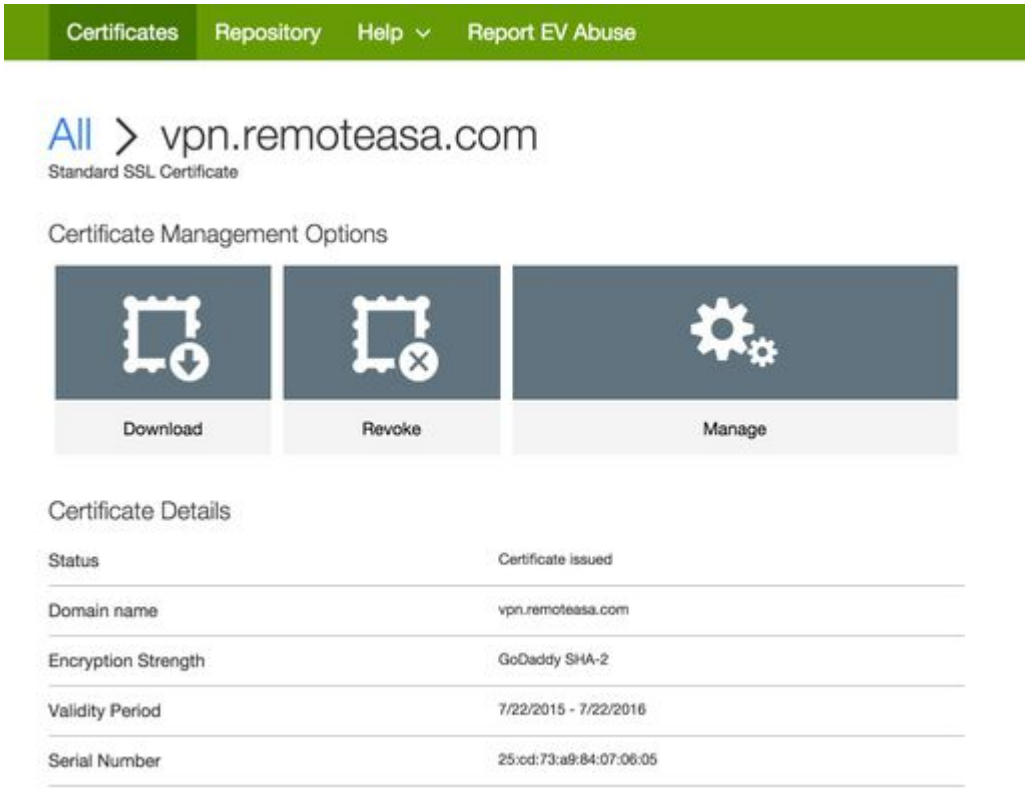
   导航到GoDaddy帐户，然后单击SSL Certificates下的Manage。



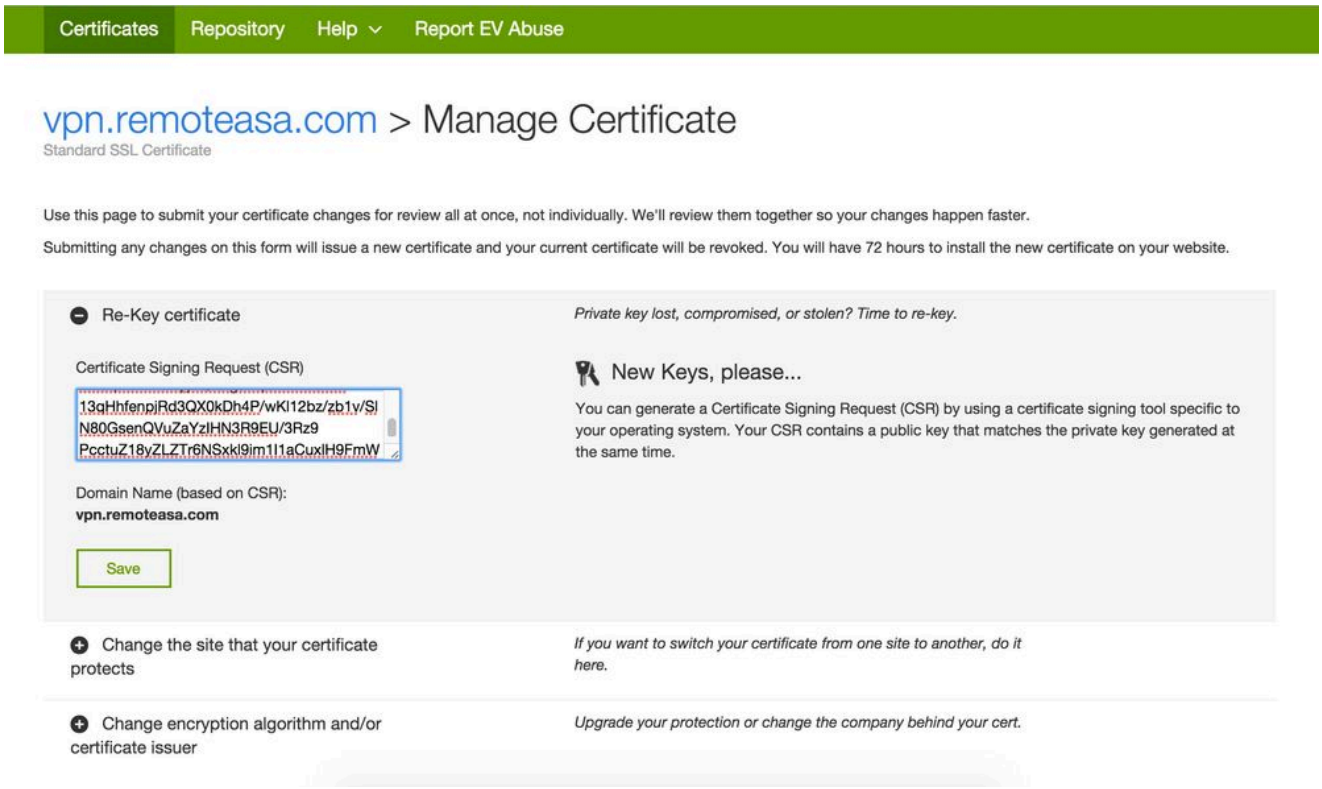
点击与所需域名对应的查看状态。



点击管理，以便提供用于重新获取证书密钥的选项。



展开选项重新获取证书密钥并添加新的 CSR。



保存并继续下一步。GoDaddy根据提供的CSR颁发新证书。

3. 如 ASA 部分“SSL 证书安装”所示，在新的信任点上安装新证书。

常见问题解答

1. 将身份证书从一个 ASA 传输至另一个 ASA 的最佳方式是什么？

将证书和密钥一起导出至 PKCS12 文件。

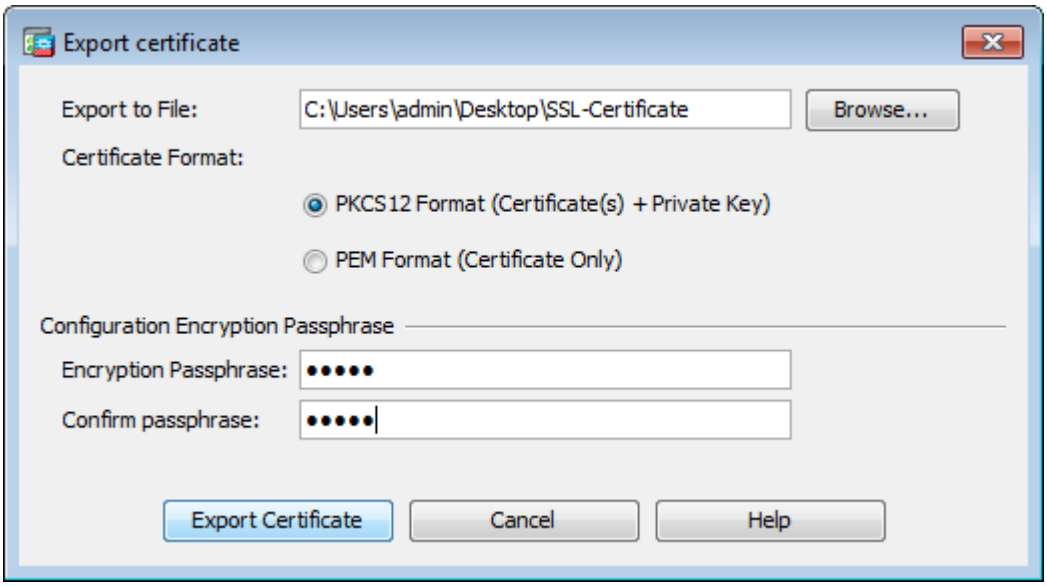
使用以下命令通过 CLI 从原始 ASA 导出证书：

```
<#root>
ASA(config)#

crypto ca export


      pkcs12
```

ASDM 配置：



使用以下命令通过 CLI 将证书导入目标 ASA：

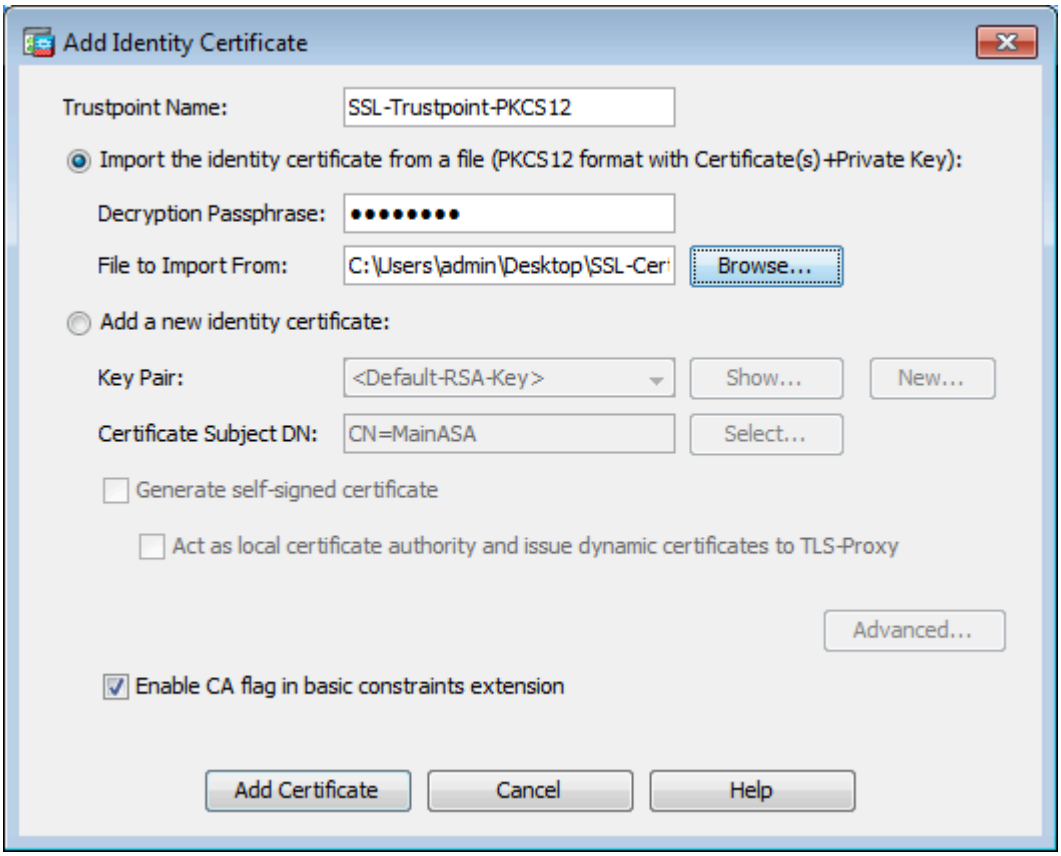
<#root>

ASA(config)#

crypto ca import

pkcs12

ASDM 配置：



也可使用以下步骤通过 ASDM 上的“备份/还原”功能完成此操作：

1. 通过ASDM登录到ASA并选择**Tools > Backup Configuration**.
2. 备份所有配置或仅备份身份证书。
3. 在目标ASA上，打开ASDM并选择**Tools > Restore Configuration**.

2. 如何生成用于 VPN 负载均衡 ASA 的 SSL 证书？

有多种方法可用于为 VPN 负载平衡环境设置具有 SSL 证书的 ASA。

1. 使用单个统一通信/多域证书 (UCC)，其中将负载平衡 FQDN 作为 DN，并将各 ASA FQDN 作为单独的主题别名 (SAN)。 有许多知名 CA，例如 GoDaddy、Entrust、Comodo 和其他支持此类证书的 CA。选择此方法时，请务必记住，ASA 当前不支持创建具有多个 SAN 字段的 CSR。增强版Cisco Bug ID CSCso70867已对此进行了记录。在这种情况下，有两个选项可用于生成CSR
    1. 通过 CLI 或 ASDM。将 CSR 提交给 CA 后，请在 CA 门户本身上添加多个 SAN。
    2. 使用 OpenSSL 生成 CSR，并将多个 SAN 包含在 openssl.cnf 文件中。

    将 CSR 提交给 CA 并生成证书后，请将此 PEM 证书导入生成 CSR 的 ASA。完成后，将此证书以 PKCS12 格式导出并导入至其他成员 ASA 中。

2. 使用通配符证书。与UC证书相比，这种方法不够安全且不够灵活。如果CA不支持UC证书

，则会在CA上或使用OpenSSL生成CSR，其中FQDN的形式为*.domain.com。将 CSR 提交给 CA 并生成证书后，将 PKCS12 证书导入集群中的所有 ASA。
3. 为各个成员 ASA 以及负载均衡 FQDN 使用单独的证书。这是效率最低的解决方案。如本文档所示，可创建用于各 ASA 的证书。在一个ASA上创建VPN负载均衡FQDN的证书，并将其作为PKCS12证书导出到其他ASA上。

3. 证书是否需要从主 ASA 复制到 ASA 故障切换对中的辅助 ASA？

无需手动将证书从主ASA复制到辅助ASA，因为只要配置了状态故障切换，证书就会在ASA之间同步。如果在对故障切换进行初始设置时，在备用设备上未看到证书，则发出命令 write standby 以强制同步。

4. 如果使用的是 ECDSA 密钥，SSL 证书生成过程是否不同？

唯一的配置差异是密钥对生成步骤，在此步骤中生成ECDSA密钥对，而不是RSA密钥对。其余步骤保持不变。

用于生成ECDSA密钥的CLI命令如下所示：

<#root>

```
 MainASA(config)#

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

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

故障排除

故障排除命令

如果 SSL 证书安装失败，应于 CLI 上收集以下调试命令输出：

debug crypto ca 255

debug crypto ca messages 255

debug crypto ca transactions 255

在较新的软件版本中，可以使用一个debug命令：

debug crypto ca 14

常见问题

在带有9.4(1)及更高版本的ASA上的外部接口上使用有效的第三方SSL证书的不可信证书警告。

解决方案：

RSA 密钥对与证书一起使用时，就会出现此问题。在9.4(1)以后的ASA版本上，默认情况下启用所有ECDSA和RSA密码，并使用最强密码（通常是ECDSA密码）进行协商。如果发生这种情况，ASA 将显示自签证书，而不是当前配置的基于 RSA 的证书。当基于RSA的证书安装在接口上并由Cisco Bug ID CSCuu跟踪时，已具备更改行为的增强功能02848

建议操作：使用以下 CLI 命令禁用 ECDSA 密码：

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

或者，使用ASDM，导航到**Configuration > Remote Access VPN > Advanced**,Encryption（加密）部分下选择**SSL Settings**.Tlsv1.2 Cipher version，然后使用自定义字符串AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA:RC4-SHA:DHA RC4-MD5

Appendix

附录 A：ECDSA 或 RSA

ECDSA 算法是椭圆曲线密码学 (ECC) 的一部分，使用椭圆曲线方程式生成公钥，而 RSA 算法使用两个素数加较小数的乘积生成公钥。这意味着使用 ECDSA 可以达到与 RSA 相同的安全级别，但密钥较小。这会减少计算时间并增加使用 ECDSA 证书的站点的连接时间。

有关下一代加密的文档提供了更详细的信息。

附录 B：使用 OpenSSL 从身份证书、CA 证书和私钥生成 PKCS12 证书

1. 确认在运行此进程的系统上安装了 OpenSSL。对于 Mac OSX 和 GNU/Linux 用户，会默认安装 OpenSSL。
2. 切换到有效目录。

   在 Windows 上：默认情况下，实用程序安装在 C:\Openssl\bin 中。在此位置打开命令提示符。

   在 Mac OSX/Linux 上：在创建 PKCS12 证书所需的目录中，打开终端窗口。

3. 在上一步提到的目录中，保存私钥 (privateKey.key)、身份证书 (certificate.crt) 和根 CA 证书链 (CACert.crt) 文件。

   将私钥、身份证书和根 CA 证书链组合至 PKCS12 文件中。输入密码以保护您的 PKCS12 证书。

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

4. 将生成的 PKCS12 证书转换为 Base64 编码的证书：
   <#root>

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

接下来，导入在最后一步中生成的用于 SSL 的证书。

附录 C：受信任CA证书安全注意事项

证书身份验证风险和建议

默认信任点验证 — 使用行为

安装受信任的CA证书时，可使用该**crypto ca trustpoint authenticate**,证书对使用证书身份验证的不同类型的VPN连接进行身份验证。它通过trustpoint命令**validation-usage**进行控制。validation-usage类型为：

- ipsec-client:验证IPsec客户端连接。
- ssl-client:验证SSL客户端连接。
- ssl-

server:验证SSL服务器证书。

默认情况下，命令允许验证ipsec-client和ssl-client。

默认配置风险

- 默认情况下，可以作为受信任身份安装的任何CA证书可用于使用证书身份验证对任何隧道组的传入客户端身份证书进行身份验证。
- 如果您不知道该默认设置，可能会带来安全风险。

建议操作

禁用非预期信任点的验证使用。如果CA证书不是用于对VPN对等体或用户进行身份验证，请禁用该信任点的验证使用。

配置示例:

```
trustpoint public-root-ca
    no validation-usage
```

授权风险和建议

默认情况下，受信任CA证书可用于对连接到任何隧道组的VPN对等体或用户进行身份验证。需要设计适当的授权。

建议操作

使用证书映射和隧道组映射确保仅授权证书用于特定隧道组。设置默认隧道组映射规则，该规则指向无访问隧道组，以限制未经授权的访问。

配置示例

证书身份验证仅允许用于：

- 具有cn=example.com颁发的证书且证书主题中具有OU=machines的计算机。
- 证书由cn=example.com颁发，且证书主题中具有OU=users的用户。

默认情况下，具有其他证书的用户会通过命令分配到no_access tunnel-group**tunnel-group-map default-group no_access**中。由于使用命令，证书映射规则的优先级高于group-**tunnel-group-map enable rules**url。了解group-url无助于绕过证书映射规则。

```
tunnel-group mgmt-tunnel type remote-access
tunnel-group mgmt-tunnel general-attributes
address-pool vpn_pool
default-group-policy mgmt-tunnel
tunnel-group mgmt-tunnel webvpn-attributes
authentication certificate
group-url https://ftd.example.com/mgmt enable
!
tunnel-group users_access type remote-access
tunnel-group usets_access general-attributes
default-group-policy user_access_gp
address-pool vpn_pool
tunnel-group users_access webvpn-attributes
authentication certificate
group-url https://ftd.example.com/users enable
!
tunnel-group no_access type remote-access
tunnel-group no_access general-attributes
default-group-policy no_access_gp
address-pool vpn_pool
tunnel-group no_access webvpn-attributes
authentication certificate
!
group-policy no_access_gp internal
group-policy no_access_gp attributes
banner value NO ACCESS GROUP POLICY
(...)
vpn-simultaneous-logins 0
!
crypto ca certificate map mgmt_tunnel 10
issuer-name attr cn eq example.com
subject-name attr ou eq machines
crypto ca certificate map users 10
issuer-name attr cn eq example.com
subject-name attr ou eq users
!
webvpn
(...)
certificate-group-map mgmt_tunnel 10 mgmt-tunnel
certificate-group-map no-access 10 users_access
!
tunnel-group-map enable rules
tunnel-group-map default-group no_access
```

其它资源

有关更详细的配置说明，请参阅以下思科文档：

- 验证使用配置- Cisco Secure Firewall ASA Series Command Reference，T - Z Commands
- 证书映射配置- Cisco安全防火墙ASA系列命令参考，T - Z命令
- 隧道组映射配置 — Cisco Secure Firewall ASA Series Command Reference、T - Z命令
- Tunnel-Group-Map Enable Configuration - Cisco Secure Firewall ASA Series Command Reference，T - Z Commands

相关信息

- ASA 9.x配置指南 — 配置数字证书
- 如何通过ASA上的ASDM从Microsoft Windows CA获取数字证书
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。