

配置 ASA : SSL 数字证书安装和续约

目录

[简介](#)

[背景信息](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[CSR 生成](#)

[1. 使用 ASDM 配置](#)

[2. 使用ASA CLI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](#)

[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。

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。

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。

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。

- 使用 ASDM 配置
- 使用 ASA CLI 配置

- 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. 单击。Add

Add Identity Certificate

Trustpoint Name:

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

Decryption Passphrase:

File to Import From:

Add a new identity certificate:

Key Pair:

Certificate Subject DN:

Generate self-signed certificate

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

Enable CA flag in basic constraints extension

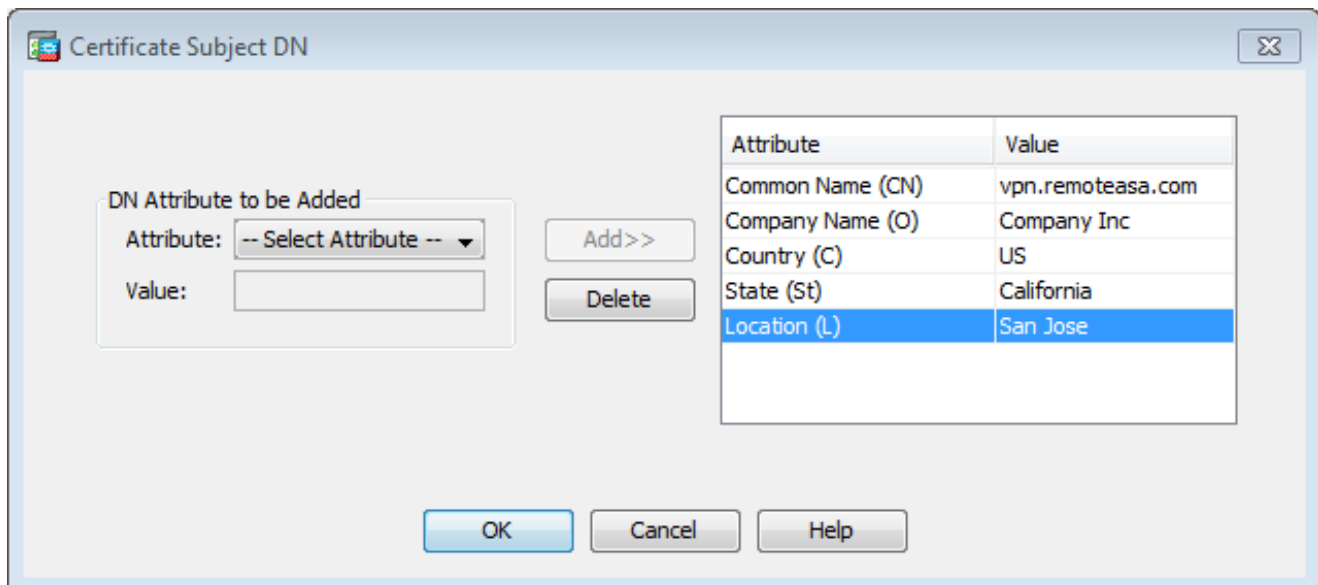
3. 在“信任点名称”输入字段下定义信任点名称。
4. 单击Add a new identity certificateRadio按钮。
5. 对于“密钥对”，请单击New。


The screenshot shows a dialog box titled "Add Key Pair". It has a close button (X) in the top right corner. The "Key Type" section has two radio buttons: "RSA" (selected) and "ECDSA". The "Name" section has two radio buttons: "Use default key pair name" and "Enter new key pair name" (selected). The text box next to the selected radio button contains "SSL-Keypair". The "Size" section has a dropdown menu with "2048" selected. The "Usage" section has two radio buttons: "General purpose" (selected) and "Special". At the bottom, there are three buttons: "Generate Now" (highlighted in blue), "Cancel", and "Help".

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 nameRadio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. 要定义证书使用者DN，请点击Select，然后配置下表中列出的属性：

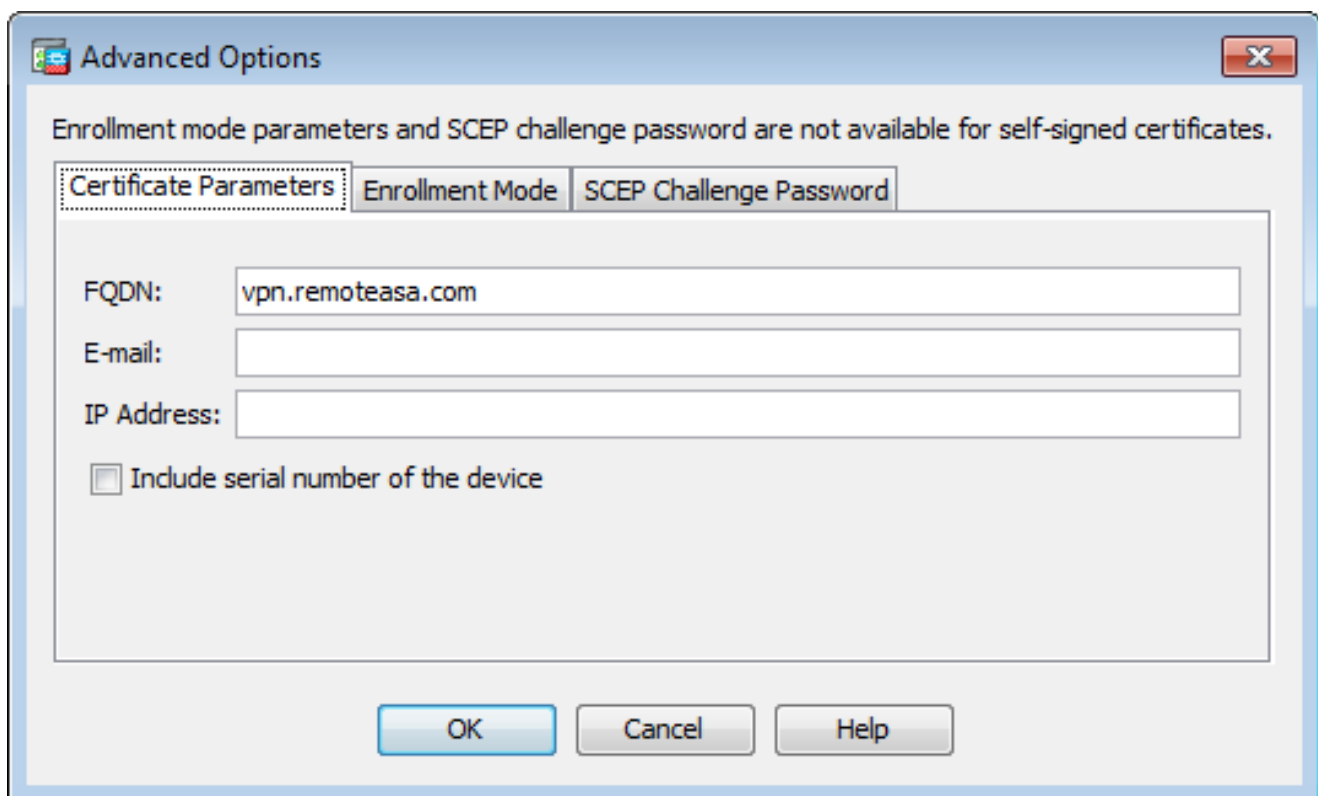
Attribute	Description
CN	FQDN (Full Qualified Domain Name) that will be used for connections to your firewall. For example, webvpn.cisco.com
OU	Department Name
O	Company Name (Avoid using Special Characters)
C	Country Code (2 Letter Code without Punctuation)
St	State (Must be spelled out completely.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



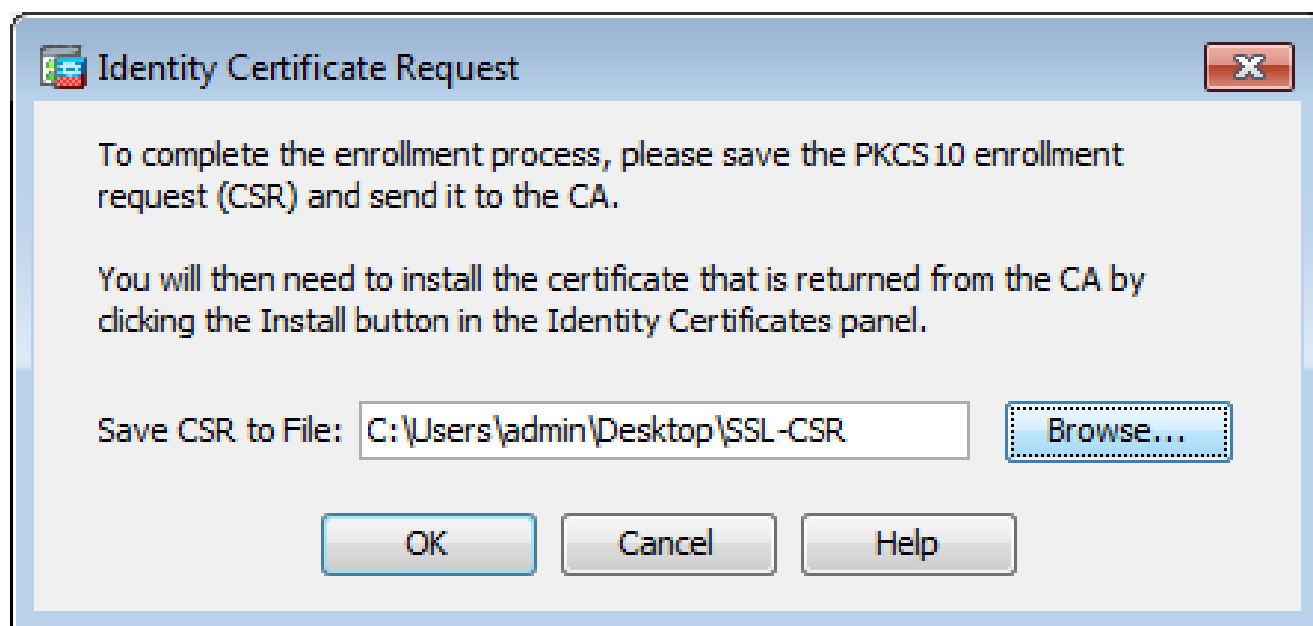
 **注意：**某些第三方供应商要求在颁发身份证书之前包含特定属性。如果不确定所需属性，请咨询供应商以获取详细信息。

11. 添加适当的值后，单击OK。系统将显示Add Identity Certificate对话框，其中包含证书Subject DN field populated.
12. 单击 Advanced。




13. 在FQDN字段中，输入用于从Internet访问设备的FQDN。单击。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，选择保存CSR的位置，并以.txt扩展名保存文件。

 注意：使用.txt扩展名保存文件时，可以使用文本编辑器（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-----
```

```
MIIDDjCCAfyCAQAwgYkxETAPBgNVBACTCFNhbiBkb3NlMRMwEQYDVQIQIEwpDYWxp  
Zm9ybmlhMQswCQYDVQQGEwJVUzEUMBIGA1UEChMLQ29tcGFueSBJamMxGjAYBgNV  
BAMTEXZwbi5yZW1vdGVhc2EuY29tMSAwHgYJKoZIhvcNAQkCFhF2cG4ucmVtb3Rl  
YXNhLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK62Nhb9kt1K  
uR3Q4TmksyuRMqJNrb9kXpvA6H200PuBfQvSF4rVnSwK0mu3c8nweEvYcdVwV6Bz  
BhjXeovTVi17F1NTceaUTGikeIdXC+mw1iE7eRsynS/d4mzMWJmrvrsDNzpAw/EM  
SzTca+BvqF7X2r3LU8Vsv60i8y1hco9Fz7bWvRWVt03NDDbyo1C9b/VgXMuBitcc  
rzfUubVnm7VZD0f4jr9EXgUwXxcQidWEAB1FrXrtYpFgBo9aqJmRp2YABQ1ieP4cY  
3rBtgRjLcF+S9TvHG5m4v7v755mev4YqsZIXvytIOzVBihemVxaGA1oDwfkoySFi  
4CzXbFvdG6kCAwEAaA/MD0GCSqGSIb3DQEJJDjEwMC4wDgYDVROPAQH/BAQDAgWg  
MBwGA1UdEQQVMB0CEXZwbi5yZW1vdGVhc2EuY29tMA0GCSqGSIb3DQEBAQUAA4IB  
AQBZuZuXGEB0ix1yuPK0ZkRz8bPnwIqLTfxZhagmuyEhrN7N4+aQnCHj85oJane
```



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


Redisplay enrollment request? [yes/no]:

no

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

3. 使用 OpenSSL 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。

 注意：验证生成的私钥未与其他人共享，因为它会破坏证书的完整性。

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。在此位置打开命令提示符。

在Mac OSX/Linux上：在创建CSR所需的目录中打开Terminal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，在上一步中提到的位置将该文件另存为openssl.cnf(如果版本为0.9.8h及更高版本，则该文件为openssl.cfg)

```
<#root>
```

```
[req]
```

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

```
[req_distinguished_name]
```

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

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

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

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

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

```
[req_ext]
```

```
subjectAltName = @alt_names
```

```
[alt_names]
```

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

4. 使用以下命令生成 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 编码身份证书或带有 PKCS12 证书的 CA 证书捆绑包。

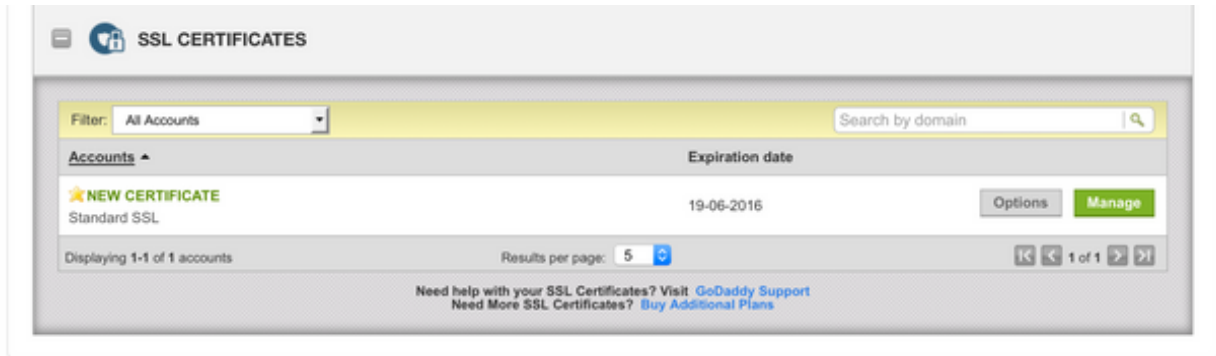
如果 CSR 是在 ASA 外生成的（通过 OpenSSL 或 CA 本身），则具有私钥和 CA 证书的 PEM 编

码身份证书将作为单独的文件提供。[附录 B](#) 介绍了将这些元素捆绑为单个 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。此过程与其他CA供应商不同。继续操作前，请仔细阅读CA文档。

GoDaddy CA 上的 SSL 证书生成示例

购买 SSL 证书并完成初始设置阶段后，请导航至 GoDaddy 账户并查看 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。

Choose website

Select a domain hosted with us

Provide a certificate signing request (CSR)

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

```
/ypj9KO49fP5ap8al0qvLtYYcCcfwrCt+OojOrZ1YyJb3dFuMNRRedAX37t
DuHNI2EYNpYkjVklwI53/5w3
-----END CERTIFICATE REQUEST-----
```

Domain Name (based on CSR):

vpn.remoteasa.com

Domain ownership

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

AND

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


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

[Hide advanced options](#)

Signature Algorithm [Learn more](#)

GoDaddy SHA-2

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

 注意:GoDaddy和大多数其他CA使用SHA-2或SHA256作为默认证书签名算法。ASA支持SHA-2签名算法,该算法从8.2(5)[8.3之前版本]和8.4(1)[8.3之后版本]开始(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会先验证请求,然后再颁发证书。

验证证书请求后，GoDaddy 将证书颁发给该账户。

然后，可下载证书以在 ASA 上安装。单击页面以继续操作Download。

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

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

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

选择Other“服务器类型”并下载证书zip捆绑包。

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

The "Server type" dropdown menu is open, showing the following options: Select ..., Apache, Exchange, IIS, Mac OS X, Tomcat, and Other. The "Other" option is highlighted in blue. To the right of the dropdown menu, there are "File" and "Cancel" buttons.

.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。

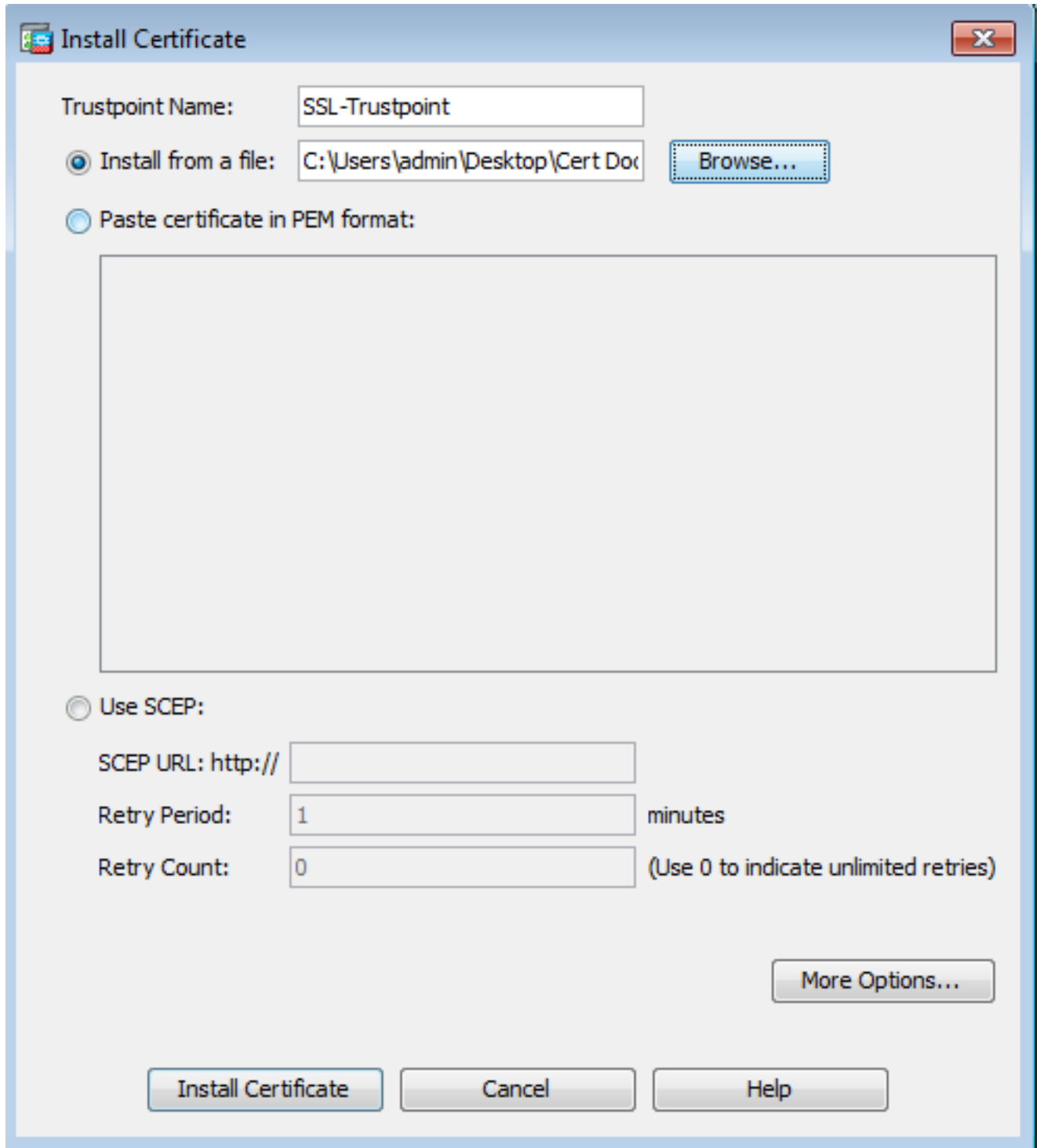


注：如果 CA 提供 CA 证书链，则仅在用于生成 CSR 的信任点上的层次结构中安装直接中间 CA 证书。根 CA 证书和任何其他中间 CA 证书均可安装于新的信任点中。

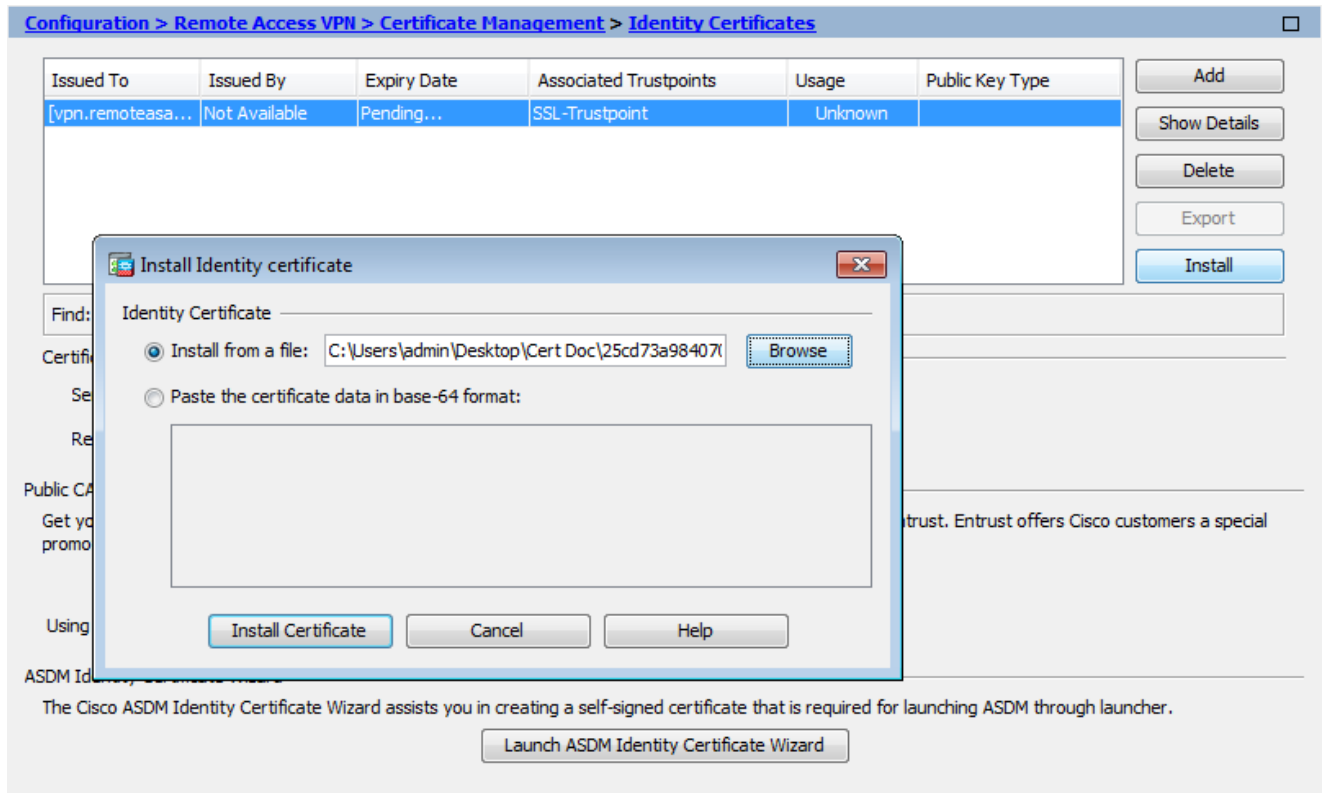
1.1 使用 ASDM 安装 PEM 格式身份证书

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。

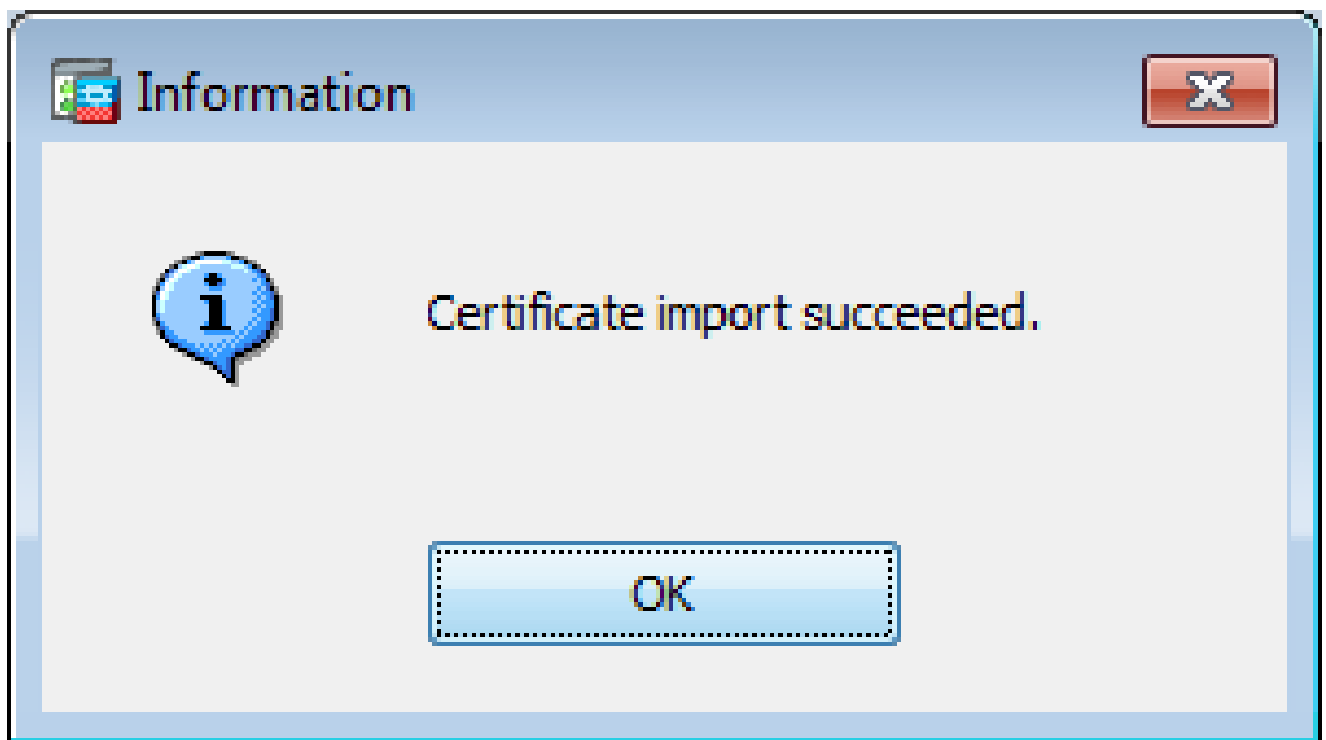
1. 导航至 **Configuration > Remote Access VPN > Certificate Management**，然后选择 **CA Certificates**。
2. 在文本编辑器中使用 PEM 编码的证书，并将第三方供应商提供的 base64 CA 证书复制和粘贴到文本字段中。



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



7. 单击。Add Certificate

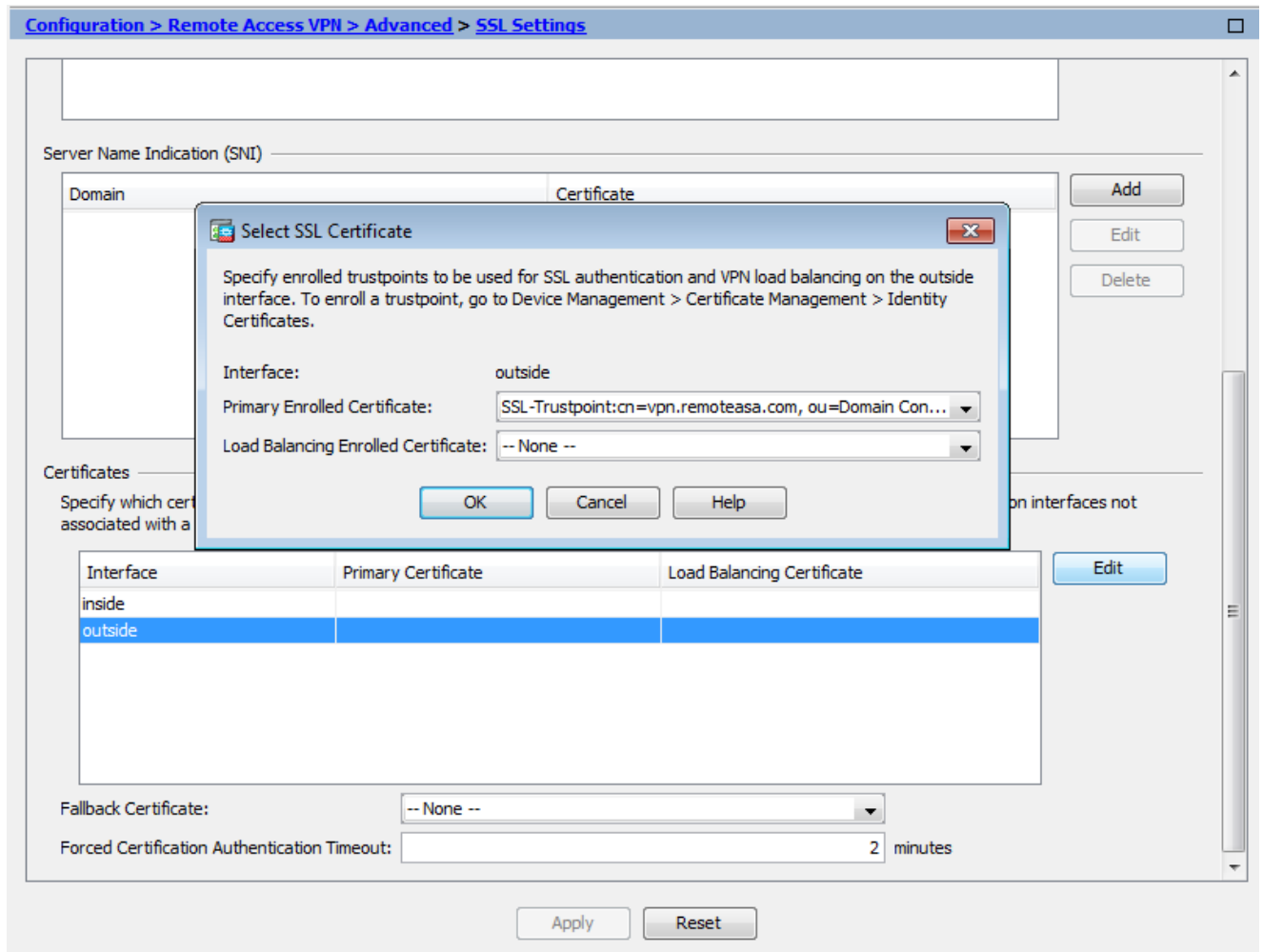


8. 导航至 Configuration > Remote Access VPN > Advanced > SSL Settings。

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. 单击。Edit

11. 在“证书”下拉菜单中，选择新安装的证书。



12. 单击。OK

13. 单击。Apply新证书现已用于在指定接口上端接的所有 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----- MIIEDCCAuigAwIBAgIBADANBgkqhkiG9w0BAQUFADBjMQswCQYDVQQGEwJVUzEh MB8GA1UECh
```

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

```
.
```

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

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

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

```
-----BEGIN CERTIFICATE-----
MIIEFTCCA2WgAwIBAgIDG+cVMA0GCSqGSIb3DQEBCwUAMGMxCzAJBgNVBAYTA1VT
MSEwHwYDVQQKEWhUaGUgR28gRGFkZHKgR3JvdXAsIE1uYy4xMTAvBgNVBAsTKEdv
IERhZGR5IENsYXNzIDIgQ2VydG1maWNhdG1vbiBBdXRob3JpdHkwHhcNMTQwMTAx
MDcwMDAwWhcNMzEwNTMwMDcwMDAwWjCBgzELMAkGA1UEBhMCVVMxEDA0BgNVBAGT
B0FYaXpvcjEwMTpsUgQwE7hPHmhUmFJ+r2hBt0oLTbcJjHMgGxBT4H
Y29tLCBjbmuMTEwLWYDVQQDEyHhbyBEYWRkeSBSb290IEN1cnRpZm1jYXR1IEF1
dGhvcml0eSAtIEcyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3Fi
CPH6WTT3G8kYo/eASVjPjIoMTpsUgQwE7hPHmhUmFJ+r2hBt0oLTbcJjHMgGxBT4H
Tu70+k8vWTAi56sZvmvigaF88xZ1gD1Re+X5NbZ0TqmNghPktj+pA4P6or6KFWp/
3gvDthkUBcrqw6gE1DtGfDIN8wBmIsiNaW02jBEYt90yHGC00PoCjM7T3UYH3go+
6118yHz7sCtTpJJiaVE1BWEaRIGMLK1D1iPfrDqBmg4pxRyp6V0etp6eMAo5zvGI
gPtLXcwy7IViQyU0A1YnAZG003AqP26x6JyIAX2f1PnbU21gnb8s51iruF9G/M7E
GwM8CetJMVxpRrPgrWIDAQABo4IBFzCCARMwDwYDVR0TAQH/BAUwAwEB/zA0BgNV
HQ8BAf8EBAMCAQYwHQYDVR0OBBYEFdqahQcQZyi27/a9BUFuIMGU2g/eMB8GA1Ud
IwQYMBaAFNLEsNKR1EwRcbNhyz2h/t2oatTjMDQGCCsGAQUFBwEBBCgwJjAkBggr
BgEFBQcwAYYYaHR0cDovL29jc3AuZ29kYWRkeS5jb20vMDIGA1UdHwQrMCKwJ6A1
oCOGIWh0dHA6Ly9jcmwuZ29kYWRkeS5jb20vZ2Ryb290LmNybDBGBgNVHSAEPzA9
MDsGBFUdIAAwMzAxBggrBgEFBQcCARY1aHR0cHM6Ly9jZXJ0cy5nb2RlZGR5LmNv
bS9yZXBvc210b3J5LzANBgkqhkiG9w0BAQsFAAOCAQEAWQtTvZKGEacke+1bMc8d
H2xwxbhuvk679r6XU0Ewf7ooXGKUwuN+M/f7QnaF25UcjCJYdQkMiGvN0QowCcWg
0JekxS0TP7QYpgEGRJHjP2kntFo1fzq3Ms3dhP8q0CkzPn1nsoX+oYggHFCJyNwq
9kIDN0zmiN/VryTyscPzfLXs4J1et01UIDyUGAZHHFIYSaRt4bNYC8nY7NmuHDK0
KHAN4v6mF56ED71XcLNa6R+gh10773z/aQvgSM03kwvIC1TErF0UZzdsyqUvMQg3
qm5vjLyb41ddJIGv15echK1srDdMZvNhkREg5L4wn3qkKQmw4TRfZHCyQFHfjDCm
rw==
-----END CERTIFICATE-----
quit
```

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

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

Trustpoint CA certificate accepted.

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

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

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

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

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

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

(asa.remotevpn.url)

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

```
-----BEGIN CERTIFICATE-----  
MIIFRjCCBC6gAwIBAgIIJc1zqYQHbGUDQYJKoZIhvcNAQELBQAwgbcCzAJBgNV  
BAYTA1VTMRAwDgYDVoQIEwdbcm16b25hMRMwEQYDVoQHewpTY290dHNkYWx1MRow  
GAYDVQQKEwFhb0RhZGR5LmNvbSw5jLjEtMCsGA1UECxMkaHR0cDovL2N1cnRz  
LmdvZGFkZGZkZHUy29tL3J1cG9zaXRvcnkVMTMwMQYDVoQDEypHbyBEYWRkeSBTZW51  
cmUgQ2VydG1maWNhdGUgQXV0aG9yaXR5IC0gRzIwHhcNMTUwNzIyMTIwNDM4WhcN  
MTYwNzIyMTIwNDM4WjA/MSEwHwYDVoQLEXhEb21haW4gQ29udHJvbCBWYXpZGF0  
ZWQxGjAYBgNVBAMTEXWbi5yZW1vdGVhc2EuY29tMIIBIjANBgkqhkiG9w0BAQEF  
AAOCAQ8AMIIIBCgKCAQEArrY2Fv2S2Uq5HdDh0aSzK5Eyok2tv2Rem8DofbTQ+4F9  
C9IXitWdLao6a7dzyfB4S9hx1VZXoHMGgNd6i9NWLXsWU1Nx5pRMaKR4h1cL6bDW  
ITt5GzKdL93ibMxYmau+uwM30kBb8QxLNNxr4G+oXtFavctTxWy/o6LzKWFyJ0XP  
tta9FZW07c0MNvKiUL1v9WBcy4GK1xyvN9RtWebtVkM5/i0v0ReBTBFfXcJ1YQAG  
UWteu1ikWAGj1qomZGnZgAFDwJ4/hxjesG2BGMtwX5L108cbmbi/u/vnmZ5Xhiqx  
<snip>  
CCsGAQUFBwIBFitodHRwOi8vY2VydG1maWNhdGVzLmdvZGFkZHUy29tL3J1cG9z  
aXRvcnkVMTMwMQYDVoQIEwdbcm16b25hMRMwEQYDVoQHewpTY290dHNkYWx1MRow  
Z29kYWRkeSB5jb20vMEAGCCsGAQUFBzAChjRodHRwOi8vY2VydG1maWNhdGVzLmdv  
ZGFkZHUy29tL3J1cG9zaXRvcnkVZ2RrZzIuY3J0MB8GA1UdIwQYMBaAFEDCvSe0  
zDSDMKIz1/tss/COLIDOMEYGA1UdEQQ/MD2CEXZwbi5yZW1vdGVhc2EuY29tghV3  
d3cudnBuLj1bW90ZWFzYS5jb22CEXZwbi5yZW1vdGVhc2EuY29tMB0GA1UdDgQW  
BBT7en7YS3PH+s4z+wTR1pHr2tSzejANBgkqhkiG9w0BAQsFAAOCQAEO9H8TLN  
x2Y0rYdI6gS8n4imaSYg9Ni/9Nb6mote3J2LELG9HY9m/zUCR5yVkra9azdrNUAN  
1hjBJ7kKQScLC4sZLONdG1uTP5rbWR0yikF5wSzyMwd03kOR+vM8q6T57vRst5  
69vzBUUJc5bSu1IjyfPP19z1l+B2eBwUFbVfXLnd9bTfiG9mSmC+4V63TXFxt10q  
xkGNys3GgYuCUy6yRP2cAUV11c2tYtaxoCL8yo72YUDDgZ3a4Py01EvC1F0aUtgv  
6QNEOYwmbJkyumdPUwko6wGOC0Wlumzv5gHhni168HYSZ/4XI1p3B9Y8yfG5pwb  
n7puhazH+xgQRdg==  
-----END CERTIFICATE-----  
quit
```

INFO: Certificate successfully imported

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

MainASA(config)#

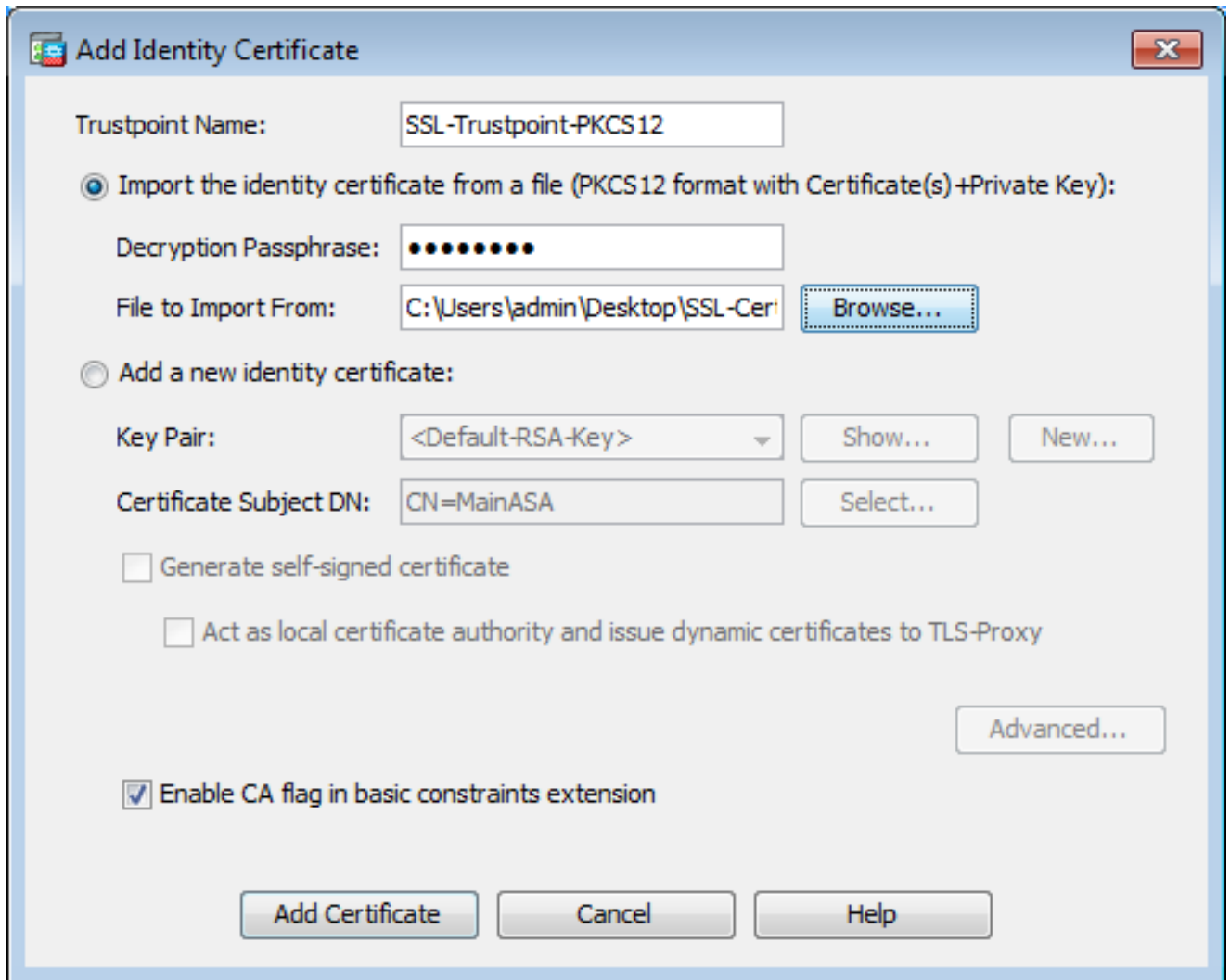
```
ssl trust-point SSL-Trustpoint outside
```

2.1 使用 ASDM 安装 PKCS12 证书

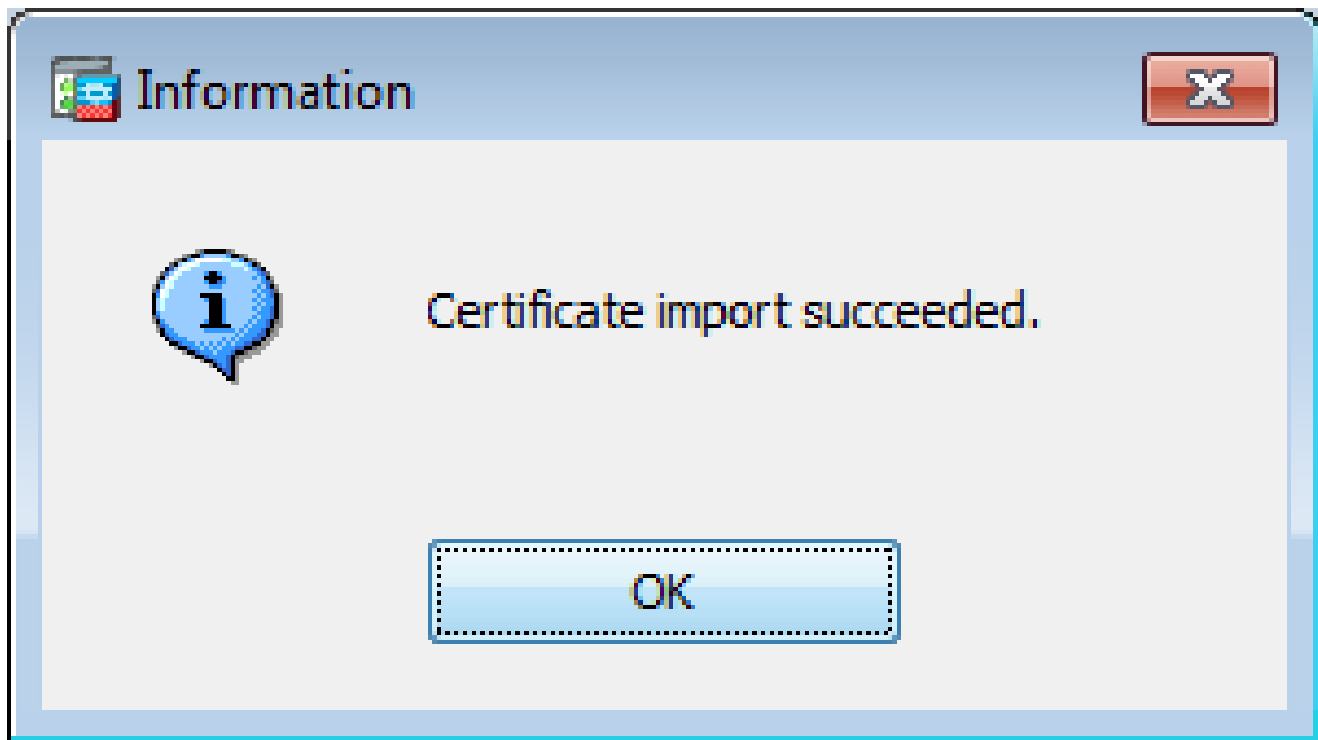
在ASA上未生成CSR的情况下，例如通配符证书或生成UC证书时，身份证书和私钥作为单独的文件或单个捆绑的PKCS12文件（.p12或pfx格式）接收。要安装此类型的证书，请完成以下步骤。

1. 将身份证书、CA证书和私钥捆绑至单个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. 单击 **Add**。
4. 指定信任点名称。

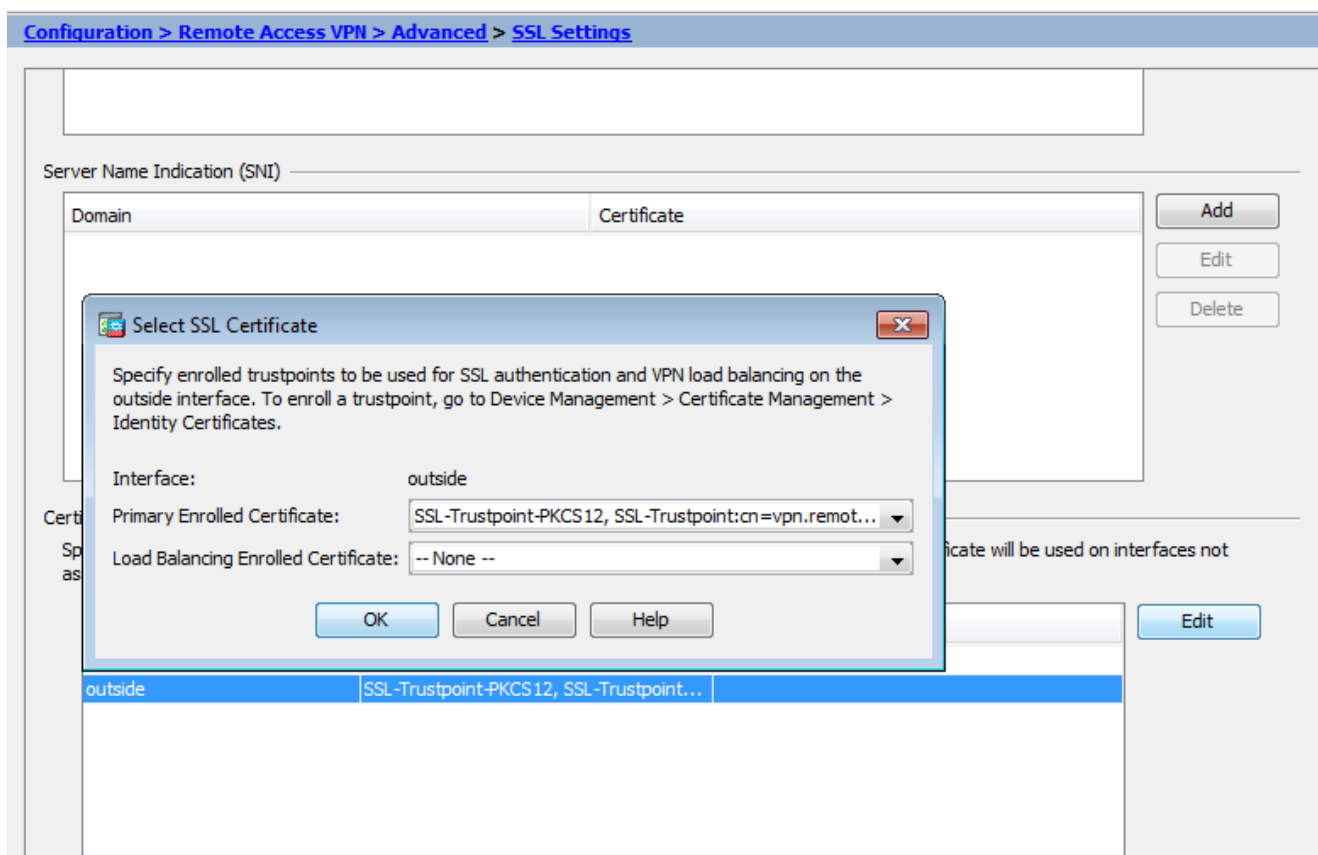
5. 点击单 **Import the identity certificate from a file** 选按钮。
6. 输入用于创建 PKCS12 文件的密码。浏览并选择 PKCS12 文件。输入证书密码。



7. 点击添加证书。



8. 导航至 **Configuration > Remote Access VPN > Advanced**，然后选择 **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. 单击。 **Edit**
11. 在“证书”下拉菜单中，选择新安装的证书。



12. 单击。 **OK**
13. 单击。 **Apply** 新证书现已应用于在指定接口上端接的所有 WebVPN 会话。

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-----
```

```
MIISNwIBAzCCEfEGCSqGSIb3DQEHAaCCEeIEghHeMIIR2jCCEdYGCsGSIb3DQEH  
BqCCEccwghHDAgEAMIIRvAYJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIWO3D  
hDtI/uECAQGAgHQospee/qtIbVZh2T8/Z+5dxRPBcStDTqyKy7q3+9ram5AZdG  
Ce9n5UCckqT4WcTjs7XZtCrUrt/LkNbmGDVhwGBmYWi0S7npgaUq0eoqiJRK+Yc7  
LN0nbho6I5WfL56/JiceAM1XDLr/IqqLg2QAAPGdN+F5vANsHse2GsAATewBDLt7  
Jy+SKfoNvvIw9QvzCiUzMjYZBANmBdMCQ13H+YQTHitT3vn2/iCD1zRSuXcqypEV  
q5e3hei00751E8TDLWm03PMvWIZqi8yzWesjcTt1Kd4FoJBZpB70/v9LntoIUOY7  
kIQM8fHb4ga8BYfbgRmG6mkMm01STtbSv1vTa19WTmdQdTyCa+G5PkrryRsy3Ww1  
1kGFMhImmrrnNADF7Hmzbys1VohQZ7h09iVQY9krJogoXHjmQYxG9brf0oEwxSJD  
mGDhhESH+s/WuFSV929kITXpJNZxpTASoWBQRrwm05v8ZwbjbnVNJ7svdbwpU16d+  
NNFGR7LTq08hpupeJny9eJc2yYqeAXWXQ5kLOzo6/gBEEdGtEaZBgCFK9JZ3b13A  
xqxGi fanWpNLyG611NKUnjTgbjhnEEYI2uZzU0qxn1Ka8zyXw+1zrKuJscDbkAPZ  
wKtw8K+p40zXVHhuANo6MDvffNRY1KQDtyK1inoPH5ksVSE5awkVam4+HTcqEUfa  
16LMAna+4QRgSetJhUOLtSmaQfRjGkha4JLq2t+JrCAPz2osAR1TsB0jQBNq6YNj  
OuB+gGk2G18Q5N1n6K1fz0XBFLWEDBLsaBR05ManE7wWt00+4awGYqVdmIF11kf  
XIRKAiQEr1pZ6BVPuvsCNJxaaUHzyfhYI2ZAckasKBZ0T8/7YK3fnAaGoBCz4cHa  
o2EEQhQ2aYb6YTv0+wtLEWGHZsbGZEM/u54XmsXAI7g28LGJYdfwi509KyV+Ac1V  
KzHqXZMM2BbUQCNCtF5JIMiW+r62k42FdahfaQb0vJsIe/IwkAKG7y6DIQFs0hwwg  
Z1PXiDbNr1k4e8L4gqumMKWg853PY+oY22rLDC7bu11CKtixIYBCvbn7dAYSi4GQ  
16xXhNu3+iye0HgbUQCfTU/mBRaOZO+bpKjWOCfqNBuYnZ6kUEdCI7GFLH9QqtM  
K7YinFLoHwTbwi3MsmqVv+Z4ttVwy7Xmi ko2nMynJMP6/CNV80MxMKdC2qm+c1j  
s4Q1KcAmFsQmNp/7SIP1wnv0c6JbUmC10520U/r8ftTzn8C7WL62W79cLK4H0r7J  
sNsZnOz0J0Z/xdZT+cLTCTtVevKJQOMK3vMsiOuy52FkuF3HnfrmbqDkbR7yZxELG  
RCELOEDdbp8VP0+IhN1yz1q7975SscdxFSL0TvjnHGFwd14ndoqN+bLhWbdPjQWV  
13W2NCI95tmHDLGgp3P001S+rjdCEGMg+9cpgBFFC1JocutDIEcUbJBY8QRUNiS  
/ubyUagdzUKt1ecfb9hMLP65ZnQ93VIw/NJKbIm7b4P/1Zp/1FP5eq7LkQPAXE4/  
bQ4mHcnwrs+JGfkn19B8hJmmGoowH3p4IEvwZy7CThB3E1ejw5R4enqmrgrvHqpQe  
B7odN10FLAHdo1G5BsHExlunEsEb40Q0pmKXi dDB5B001bJsr748fZ6L/LGx8A13
```

```
<snip>
```

```
ijDqxyfQXY4zSyt1jSmWmtYA9hG5I79Sg7pnME1E9xq1D0oRGg8vgxlwiciKtLxp  
LL0REdY31KRYv00vwOgftE71ST/3TKZvh0sQ/BE0V3kHnw1dejMFH+dvYAA9Y1E  
c80+tdafBFX4B/HP46E6heP6ZSt0xAfRW1/JF41jNvUNV09vtVFR2FTyWpzZFY8A  
GG5XPIA80WF6wKEPFHICn8scY+Vot8kXxG96hwt2Cm5NQ20nVzxUZQbpKsjs/2jC  
3HVfE3UJFBsY9UxTLCpXYBSIG+VeqkI8hWZp6c1TFNDLY2ELDY1Qzp1mBg2FuJza  
YuE0avjCJzBzZUG2umtS5mHQnwPF+Xk0ujEyhGMauhGxHp4nghSzrUZrBeuL91UF  
2mbpsOcgZkzxMS/rjdNXjCmPF1oRBvKkZS1xHFrE/5ZopAhn4i7YtHQNrZ9U4RjQ  
xo9cUuaJ+LnmvzE8Yg3epAMYZ16UNGQqkVQ6ME4BcjRONzW8BYgTq4+pmT1ZNq1P
```

X87CXCPtYRpHF57eSo+tHDINCgfqYXD6e/7r2ngfiCeUeNDZ4aV12XxvZDaU1BPP
Tx5fMARqx/Z8BdDyBJDVBjdsxmQau9HLkhPvdfGTZIwdTe13CzKqXA5Pmpjt4q9
GnCpC53m76x9Su4ZDw6aUdBcgCTMvfaqJC9gzObee2Wz+aRRwzSxu6tEWVZo1PEM
v0AA7po3vPek1g0nLRAwEoTTn4SdgNLWeRoxqZgkw1FC1GrotxF1so7uA+z0aMeU
Tw73reonsNdZvRACvX3Y6UNFdyt70Ixvo1H4VLzWmOK/oP62C9/eqqMwZ8zoCMPt
ENna7T+70s66SCbMmXCHwyh00tygNKZFFw/AATFyjQPMWPaxGuPN0rnB6uYcN0Hk
1BU7tF143RNIzaQqEH3XnaPvUuAA4C0FCoE3h+/tVjtfNKDvFmb6ZLZHYQmUYpyS
uhdFEpoDrJH1VmI2TiK/iqYwaz+oDqXPHQXnJhw25h9ombR4qnD+FCfwFCGtPFON
o3Qffz53C95n5jPHVMYUr0xDdpwnvzCQPdj6yQm564TwLAmiZu7uD1pqJZJe5QxHD
no1v+4MdGSfVtBq+ykFoVcaamqeaq6sKgvAVujLXXEs4KEmIgcPqATVRG49E1ndI
L01DEQyKhVoDGebAuVRBjzwAm/qxWxxFv3hrbCjPHCwEYms4Wgt/vKKRFsuWJNZf
efH1dw11tkd5dKwSvDocPT/7mSLtLJa94c6AfgxXy9z0+FTLDQwzXga7xC2krAN1
yHxR2KHN5YeRL+KDzu+u6dYoKaz+YAgw1W6KbeavALSuH4EYqcvG8hUEhp/ySiSc
RDhuygXEvIMGfES4FP5V521PyDhM3Dqwhn0vuYUmYnX8EXURkay44iwwI5HhqYJ
TptWYyo8Bdr4Wnwt5xqsZgYR6mmGeAIin7bDunsF1uBHWYF4dyK1z1tsdRNMqQ
+W5q+QjVdrj1dwv/bmFOaqEjxeNwBRqjzccff3BxMnwvVxtgqxFvRh+DZxiJoiBG+
yx7x8np2AQ1r0METSSxbnZzfNkZKvBVMkIC6Jsm2WEVTQvoFJ8em+nem0Wgti/
hHSBzjE7RhAucnHuiFOCX0gvR1SDDqyCQbduc1QjXN0svA8Fqbea9WEH5khOPv3
pbtsL4gsf12pv8diBQkVQgiZDi8wb++7PR6ttiY65kVwrdson11/qq+xW0d3tB4/
zoH9LEMgTy9Ssz7myWrB9E00Z8BIjL1M8oMigEYrTD0c3KbyW1S9dd7QAxIU0BaX1
8J8q10ydvTBzmqcjsSfH4/1NHn5Vnf0ZnNpui4uHP0XBG+K2zJUJXm6dq1AHB1E
KQFsFzPNNyave0Kk8JzQnLAPd70UU/Iksy0CGQozGBH+HSzVp1RDjrrbC342rkBj
wnI+j+/1JdwBmHdJMZCfoMZFLSI9ZBqFirdii1/NRu6jh76TQor5TnNjxIyNREJC
FE5FZnmFvHm900LaiUZff8WWCOferDMttLXb1nuxPF1+1Rk+LN1PLVptWgcxzfSr
JXrGiWjxybBB9oCOrAcq8fGatEs8WRxJyDH3Jjmn9i/G16J1mMcuF//Lxah2Wqx8
Ld/qS50M2iFCffDQjXaj0K6DEN5pUebBv1Em5SOHXvyq5nxgUh4/y84CwaKjwOMQ
5tbbLM1nc7ALIj9LxZ97YiXSTyeM6oBxBfx6Rpk1kDv05m1BghSpVQiMcQ2ORikh
UVVnBSH019S3cb5wqxaWqAKBqb4h1uLGVbYWZf2mzLZ8U5U5ioiqoMBqNZbzTXp0
EqEFuatT11QvCRbcKS3xou4MAixcYUxKwEhbZA/6hd10XSBjwe7jKBV9M6w1iKab
UfoJCGTaf3sY681qrMPrbt0eewf1C02Sd9Mn+V/jvni17mxYFFUpruRq3r1LeqP
J5camfTtHwyL8N3Q/Zwp+zQeWziLA8a/iAVu/hYLR1bpF2WCK010tJqkvVmrLVLz
maZZjbJe0ft5cP/1RxbK1S6Gd5dFEKDE15c6gWUX8RKZP6Q7iaE5hnGmQjm8Lj1
kXwF+ivox0Q8a+Gg1bVTR0c7tqW9e9/ewisV1mwvEB6Ny7TDS1oPUDHM84pY6dqi
1+0io07Ked4BySwN1Yy9yaJtBTZSCstfP+ApLiDn7pSBvvXf1aHmeNbkPOZJ+c+t
fGpUdL6V2UTXfCsOPHTC0ezA15sOHwCuPchrDIj/eGUwMS3NfS25XgcMuvnLqGV0
RzcrZ1ZIG8G0oLYwOCuzoY0D/m901001ahePyA9tmVB7HRRbytLdaW7gYeEikoCv
7qtBqJFF17ntWJ3EpQHZUCVClbHIKqjNqRbDCY7so4A1IW7kSEUGWMIUDhprE8Ks
NpvnPH2i9JrYrTeRoYUI0tL/7SATd2P0a21xz/zUwekeqd0bmvCsAgQNbB2XkrR3
XS0B52o1+63e8KDqS2zL2TZd3daDFidH1B8QB26tfbf0Aca0bJH5/dWP8ddo8UYo
Y3JqT10malxSjhaMhMqDZIqP49utW3Tcjg11YS4HEmcqtHud0ShaUysC6239j1Q
K1FwrwXT1BC5vnq5IcOMqx5zyNbfXz28969cwoMcyU6+kRw0TyF6kF7EEv6XWca
XLEwABx+tKRUKHJ673SyDMu96KMV3yZN+RtKbCjqCPVTP/3ZeIp7nCMUcj5sw9HI
N34yeI/ORCLyeGs0EiBLkucikC32LI9ik5HvImVTELQ0Uz3ceFqU/PkasjJUve6S
/n/1ZVUHBUk71xKR2bwZgEC17fIe17w1rbjP3Wbk+Er0kfYcsNRHxeTDpKpSt9s
u/UsyQJiyNARG4X3iyQ1sTce/06Ycyri6GcLHAu58B02nj4Cxo1Cp1ABZ2N79Htn
/7Kh5L0pS9MwsDCHUUI8KFRtSEt7TB1tIU99FdB19L64s1/shYAHbccvVWU50Wht
PdLoaErrX81Tof41IxBSzBI8grUC4KfG2sdPLJKu3HVTeQ8Lfl1bBLxfs8ZBS+Oc
v8rH1Q012kY6LsFGLehJ+/yJ/uvXORiv0ESp4EhFpFfkp+o+YcFeLUUPd+jzb62K
HFSCCbLpKkyEay80dyWkHfgy1qXmb9ud0oM050aFJyqRONjnt6pcxBRY2A6AJR5S
IIC26YNwbh0GjF9qL2FiUqnNH/7GTqPnd2qmsB6FTIwSBT6d854qN7PRt+ZXgdtQ
Ojcyt1r9qpWZpNFK8EzizwKiAYtsiEh2pzPt6YUpxRb6CXTkIzoG+KLsv2m3b8
OHyZ9a8z81/gnxrZ11s5SCTf0SU70pHWh8VAYKVHhk+MwgQrOm/2ocV32dkRBLMy
2R6P4WfHyI/+9de1x3PtIu0iv2knpXhv2fKM6sQw45F7XkmwHxjq1YRJ6vIwPTAh
MAKGBSs0AwIaBQAeffTRETzpiSHKZR+Kmen68VrTwpV7BBSQi0IesQ4n4E/bSVsd
qJSzcwh0hgICBAA=
-----END PKCS12-----
quit

INFO: Import PKCS12 operation completed successfully

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

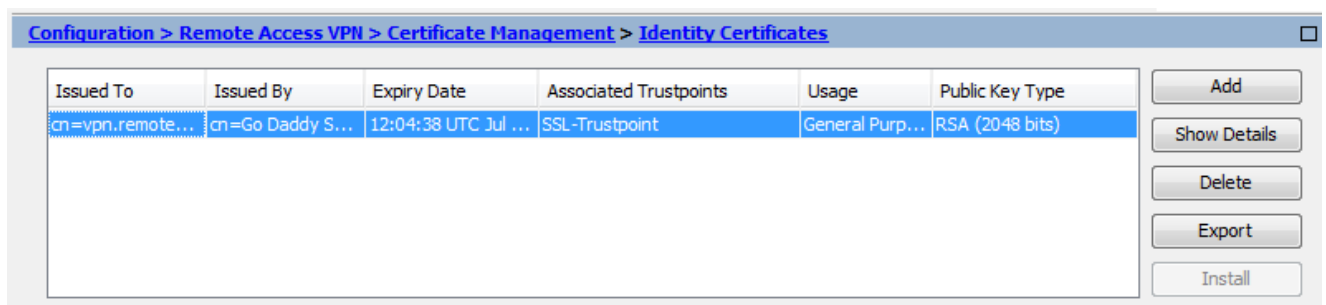
```
ssl trust-point SSL-Trustpoint-PKCS12 outside
```

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:

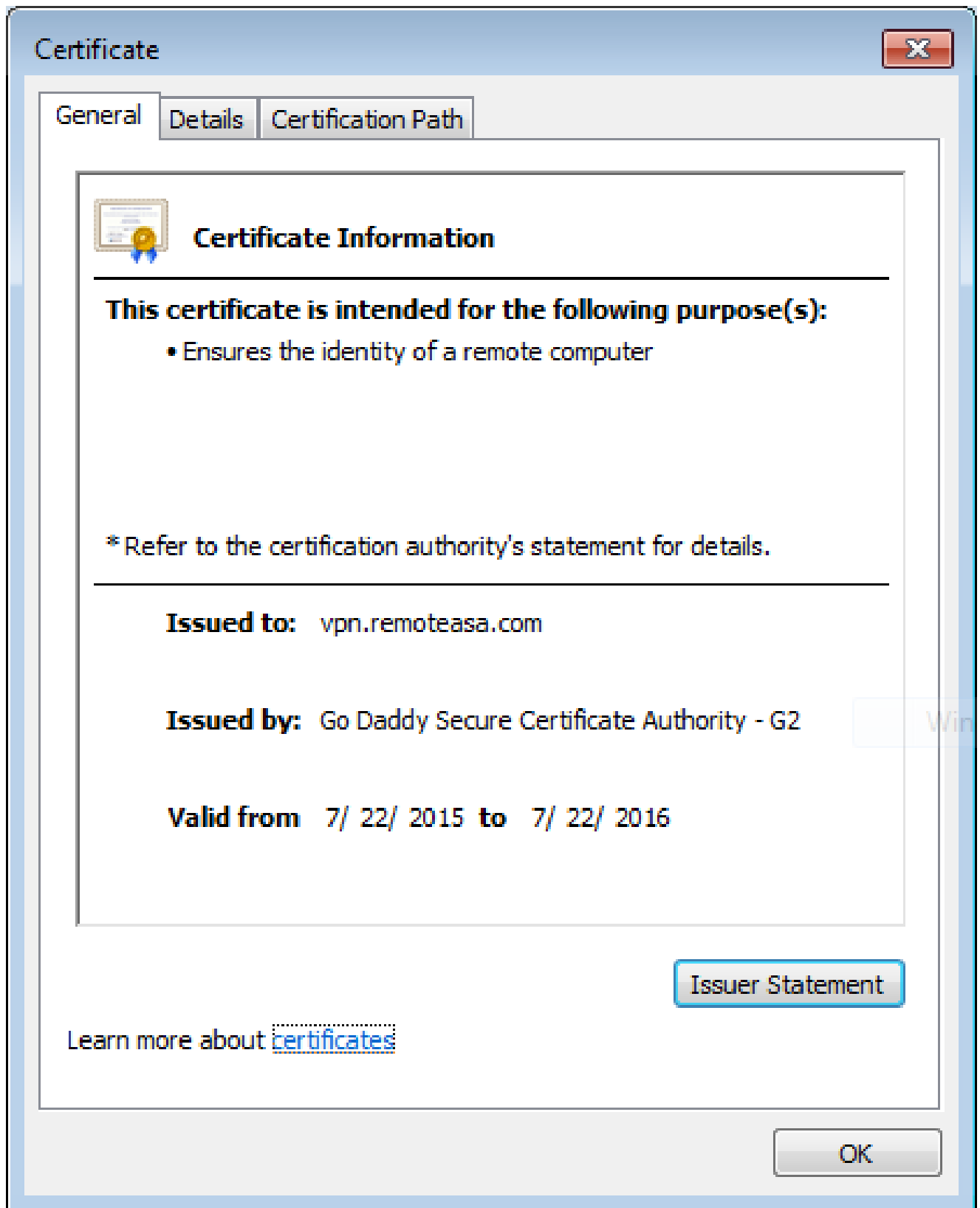
SSL-Trustpoint-1

...(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。使用https://以及所使用的FQDN来请求证书(例如 , [https://\(vpn.remoteasa.com\)](https://(vpn.remoteasa.com)))。
2. 双击 WebVPN 登录页右下角显示的锁图标。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。

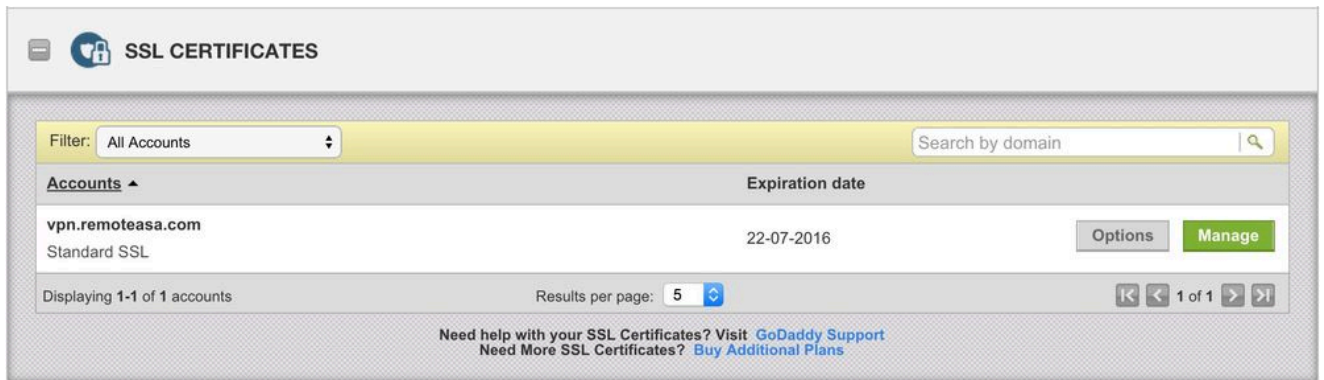


在 ASA 上续订 SSL 证书

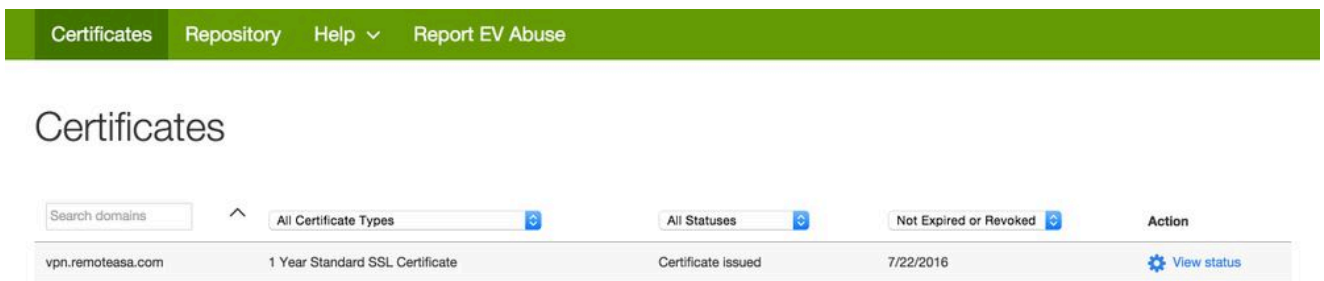
1. 在ASA、OpenSSL或CA上重新生成CSR，其属性与旧证书相同。完成[CSR Generation](#)中给定的步骤。
2. 在 CA 上提交 CSR，并与 CA 证书一起生成 PEM 格式（.pem、.cer 和 .cert）的新身份证书。对于PKCS12证书，还有一个新的私钥。

对于 GoDaddy CA，可使用生成的新 CSR 重新获取证书密钥。

转至 GoDaddyaccount，然后点击“SSL 证书”下的管理。



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。

All > vpn.remoteasa.com

Standard SSL Certificate

Certificate Management Options



Download



Revoke



Manage

Certificate Details

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

展开选项重新获取证书密钥并添加新的 CSR。

vpn.remoteasa.com > Manage Certificate

Standard SSL Certificate

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

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

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

Certificate Signing Request (CSR)

```
13qHhfenpIRd3QX0kDh4P/wKI12bz/zb1v/SI  
N80GsenQVuZaYzIH-N3R9EU/3Rz9  
PcctuZ18yZLZTr6NSxki9m111aCuxlH9FmW
```

Domain Name (based on CSR):
vpn.remoteasa.com

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

Change the site that your certificate protects *If you want to switch your certificate from one site to another, do it here.*

Change encryption algorithm and/or certificate issuer *Upgrade your protection or change the company behind your cert.*

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：

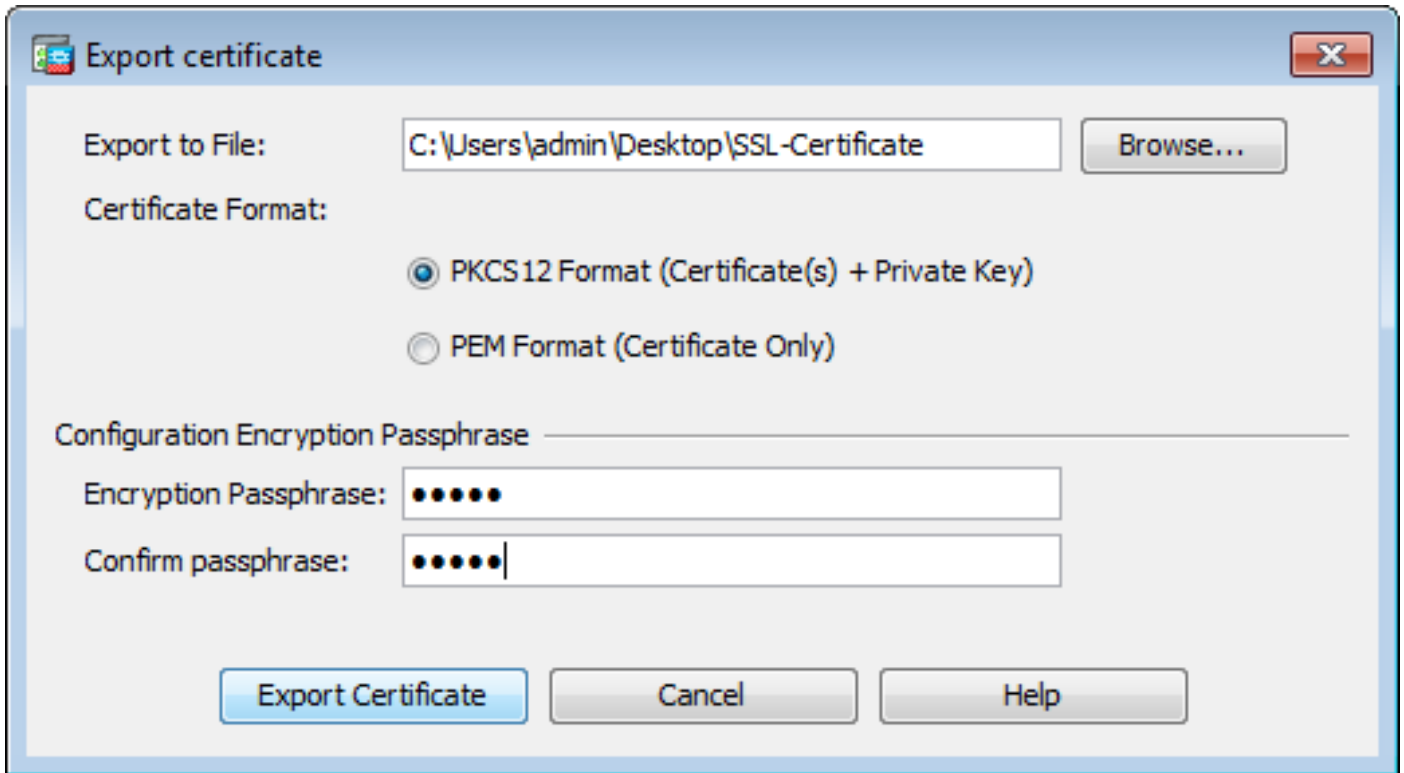
```
<#root>
```

```
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 :

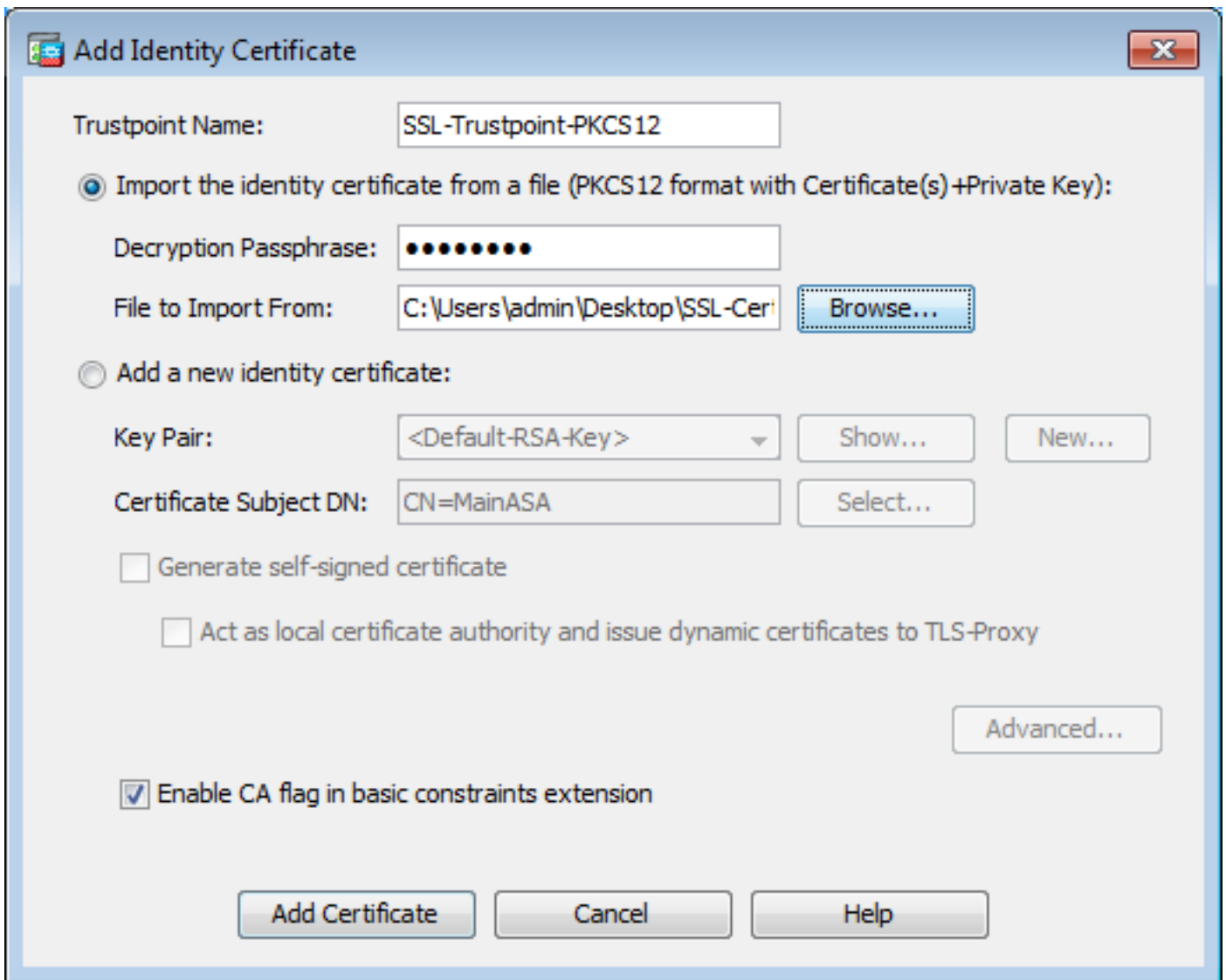
```
<#root>
```

```
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 负载均衡环境设置具有 SSL 证书的 ASA。

1. 使用单个统一通信/多域证书 (UCC)，其中将负载均衡 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。这已记录于增强功能思科漏洞 ID [CSCso70867](#) 中。在这种情况下，有两种方法可以生成 CSR
 - a. 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。
 - b. 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，则可以在 CA 上或使用 OpenSSL 生成 CSR，其中 FQDN 的格式为 *.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
```

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：将RSA密钥对与证书结合使用时，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。如果在接口上安装基于 RSA 的证书，则可以通过一种增强功能改变该行为，此增强功能记录于思科漏洞 ID [CSCuu02848](#) 中。

建议的操作：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导航至Configuration > Remote Access VPN > Advanced，然后选择SSL Settings。在“加密”部分下，选择 tlsv1.2 密码版本并使用自定义字符串 AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA:RC4-SHA:RC4-MD5 对它进行编辑

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。

[下一代密码学和 ASA](#) 文档提供了更深入的信息。

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Terminal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。

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）。