在ASDM管理的ASA上安装并续订证书

目录

简介

本文档介绍如何在通过ASDM管理的Cisco ASA软件上请求、安装、信任和续订特定类型的证书。

先决条件

要求

- 开始之前，请确认自适应安全设备(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。检查相关信息以供参考。
- 要请求使用证书签名请求(CSR)的证书，需要具有访问受信任的内部或第三方证书颁发机构(CA)的权限。第三方CA供应商的示例包括（但不限于）Entrust、Geotrust、GoDaddy、Thawte和VeriSign。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ASAv 9.18.1
- 创建PKCS12时，使用OpenSSL。

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

此文档处理的证书类型为：

- 自签名证书
- 由第三方证书颁发机构或内部CA签名的证书

安全套接字层(SSL)、传输层安全(TLS)和用于EAP身份验证协议的IKEv2 rfc7296要求SSL/TLS/IKEv2服务器为客户端提供服务器证书，以便客户端执行服务器身份验证。为此，建议使用受信任第三方 CA 将 SSL 证书颁发给 ASA。

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。

使用ASDM请求并安装新的身份证书

可以通过两种方式从证书颁发机构(CA)请求证书并在ASA上安装：

- 使用证书签名请求(CSR)。生成密钥对，通过CSR从CA请求身份证书，安装从CA获取的签名身份证书。
- 使用从CA获取或从其他设备导出的PKCS12文件。PKCS12文件包含密钥对、身份证书、

CA证书。

请求并安装具有证书签名请求(CSR)的新身份证书

在需要身份证书的设备上创建CSR，使用设备上创建的密钥对。

CSR包含：

- 证书请求信息 — 请求的主题和其他属性，密钥对中的公钥，
- 签名算法信息，
- 证书请求信息的数字签名，使用密钥对中的私钥签名。

CSR被传递到证书颁发机构(CA)，以便其以PKCS#10形式对其进行签名。

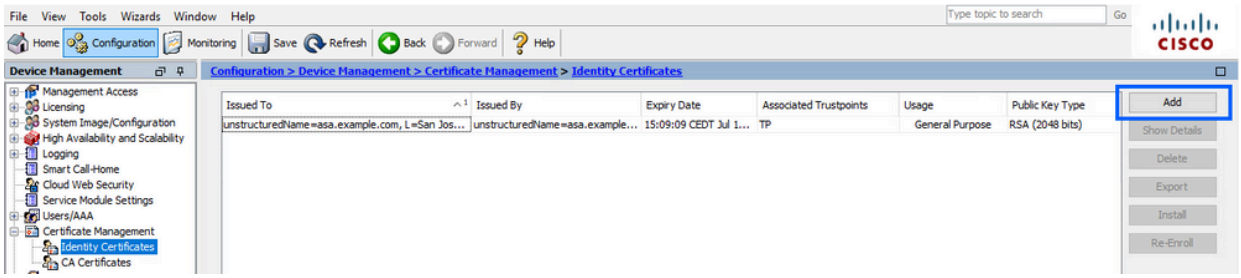
签名证书以PEM形式从CA返回。

注意：CA可在签署CSR并创建签名身份证书时更改信任点中定义的FQDN和主题名称参数。

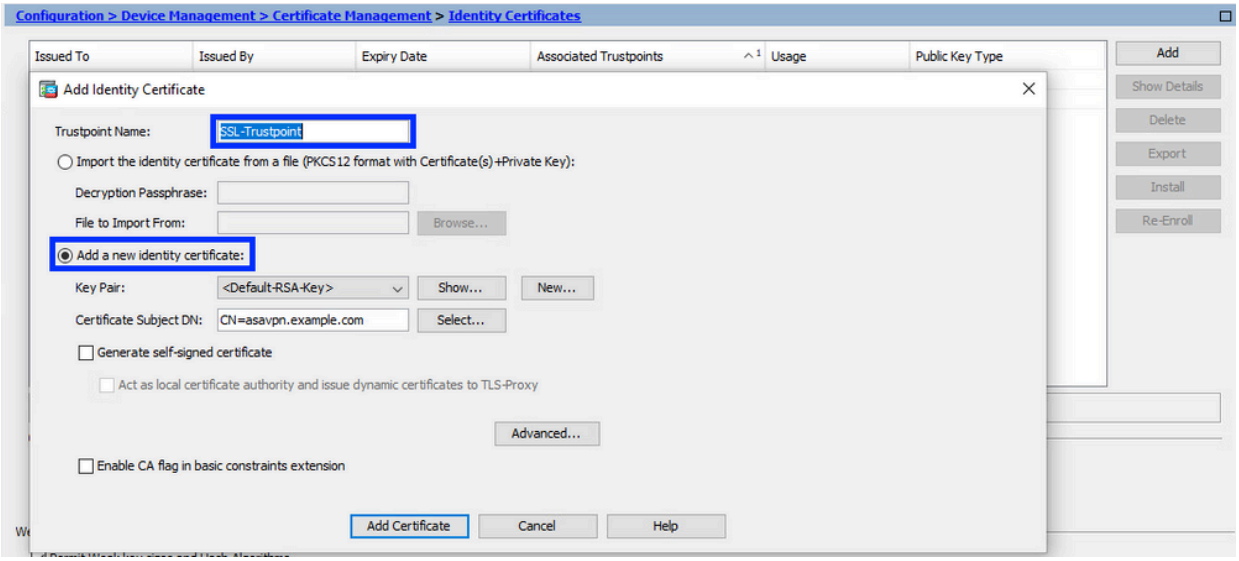
使用ASDM生成CSR

1. 创建具有特定名称的信任点

   a. 导航到Configuration > Device Management > Certificate Management > Identity Certificates。



   b. 单击 Add。
   c. 定义信任点名称。



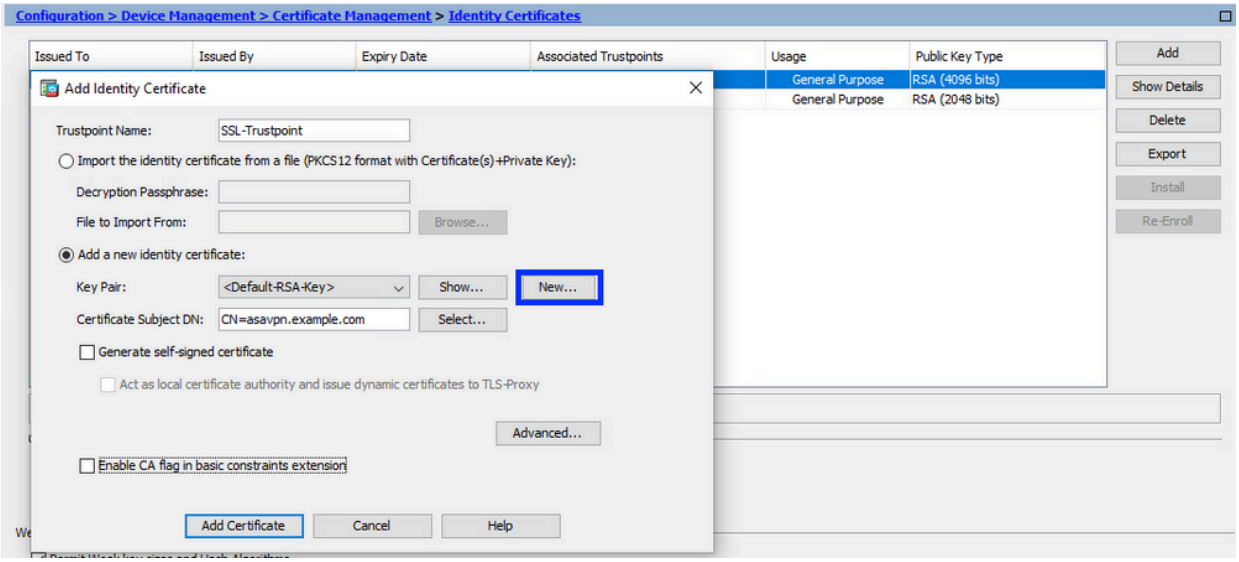
d. 单击 Add a new identity certificate 单选按钮。

2. （可选）创建新密钥对

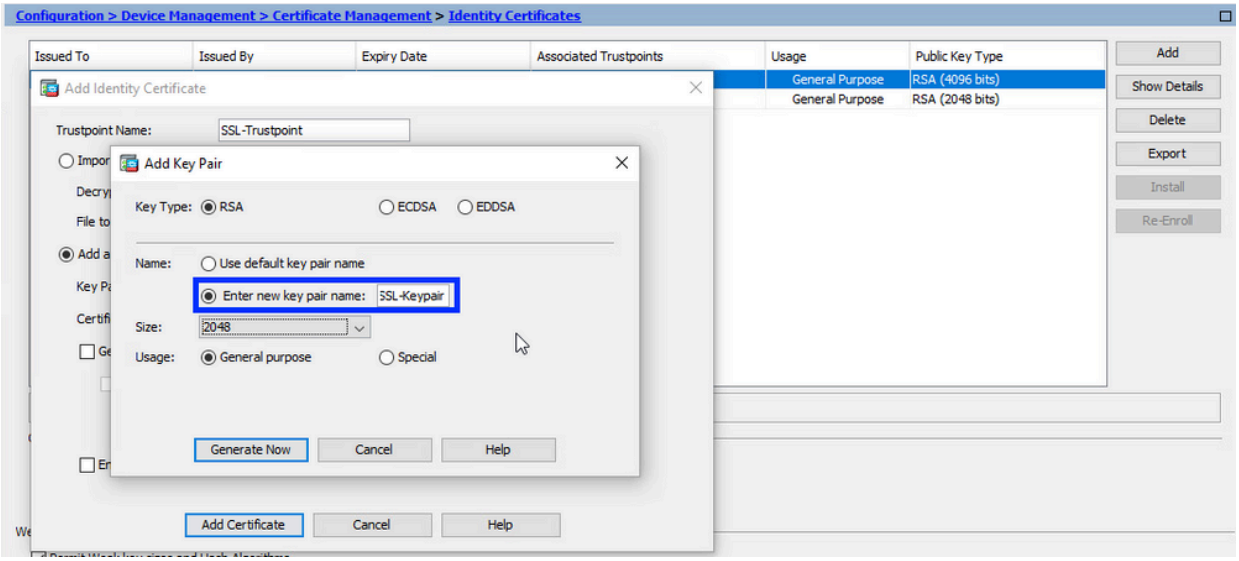
注意：默认情况下，使用名称为Default-RSA-Key且大小为2048的RSA密钥；但是，建议为每个身份证书使用唯一的专用/公共密钥对。

---

a. 单击New生成新的密钥对。

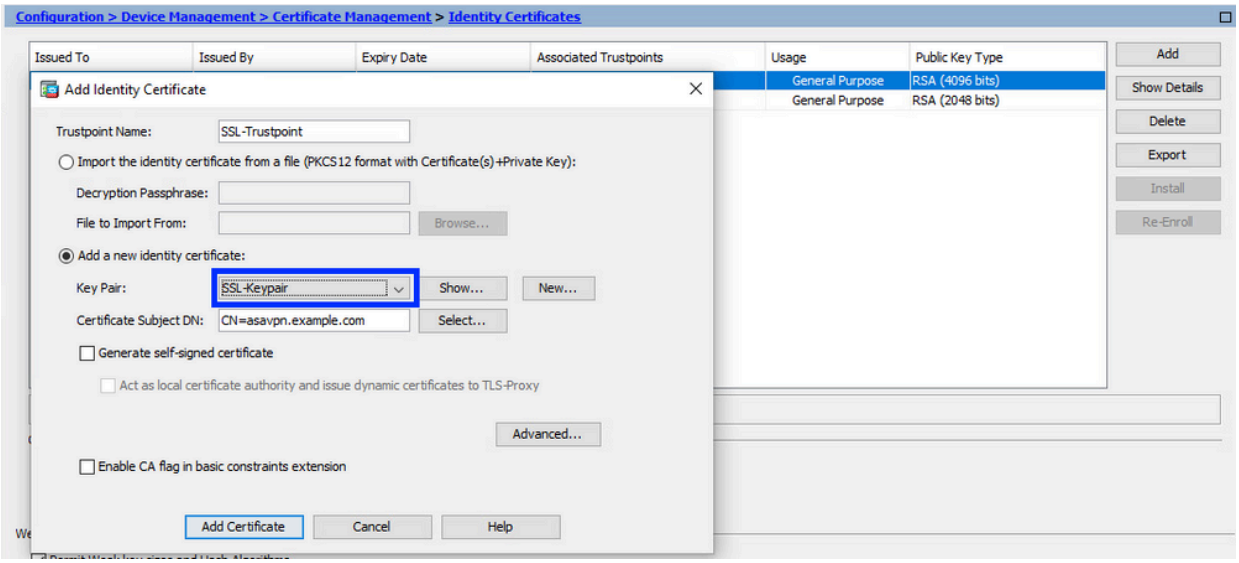


b. 选择输入新密钥对名称选项，然后输入新密钥对的名称。
c. 选择密钥类型 - RSA或ECDSA。
d. 选择Key Size；对于RSA，选择General purpose for Usage。
e. 单击 Generate Now。密钥对现已创建。



3. 选择密钥对名称

选择密钥对以签署CSR并将与新证书绑定。

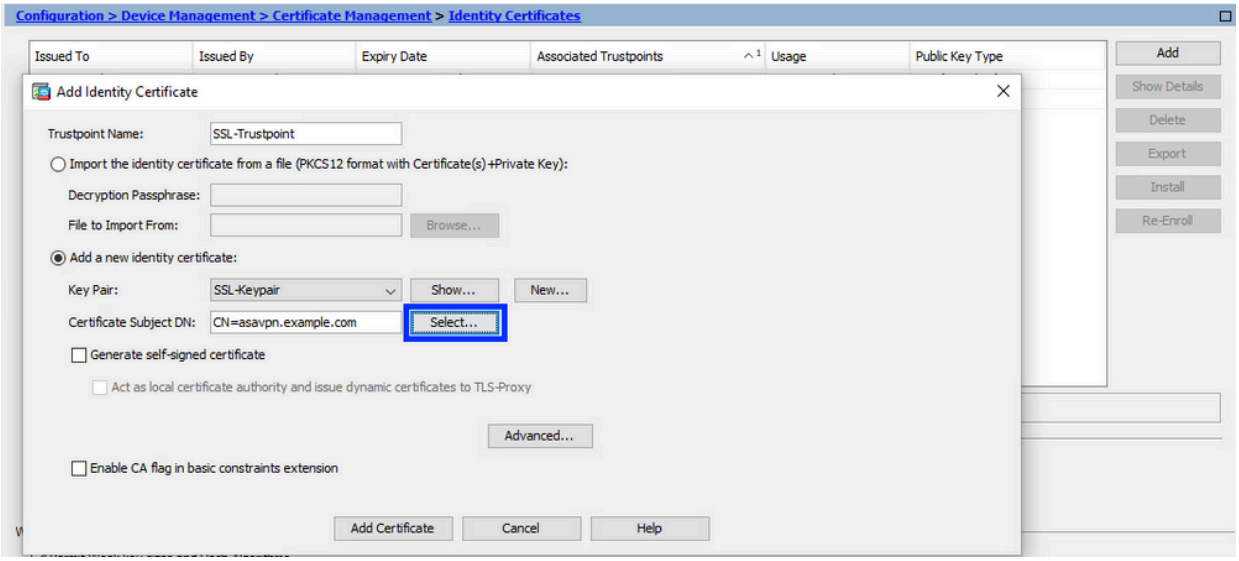


4. 配置证书主题和完全限定域名(FQDN)

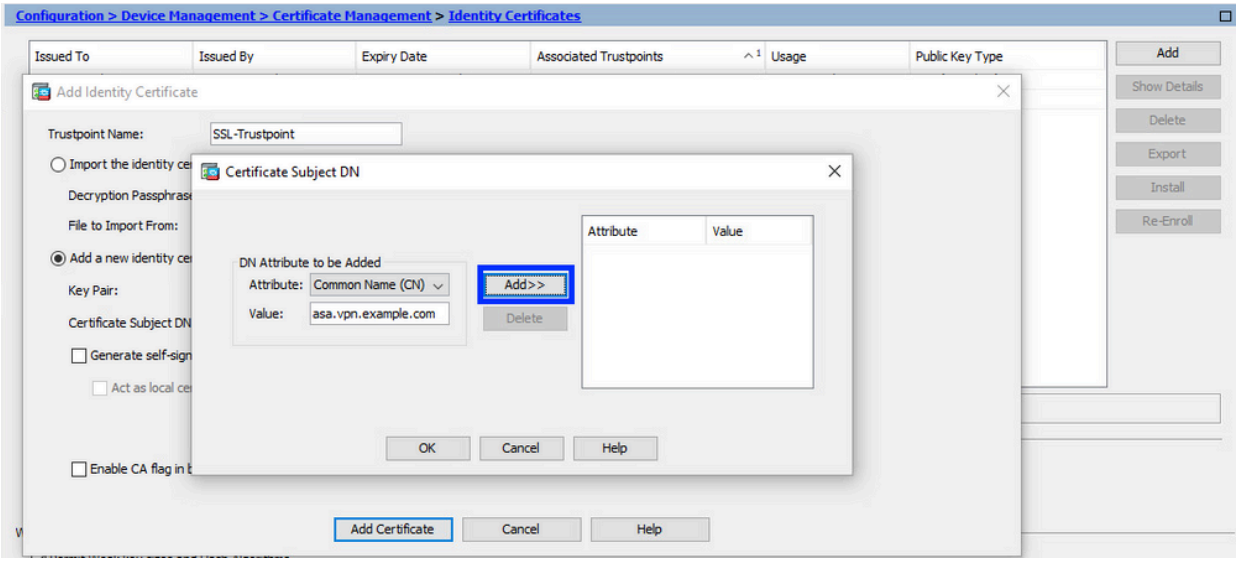
注意:FQDN参数必须与身份证书用于的ASA接口的FQDN或IP地址匹配。此参数为身份证书设置请求的主题备用名称(SAN)扩展。SSL/TLS/IKEv2客户端使用SAN扩展来验证证书是否与其连接的FQDN匹配。

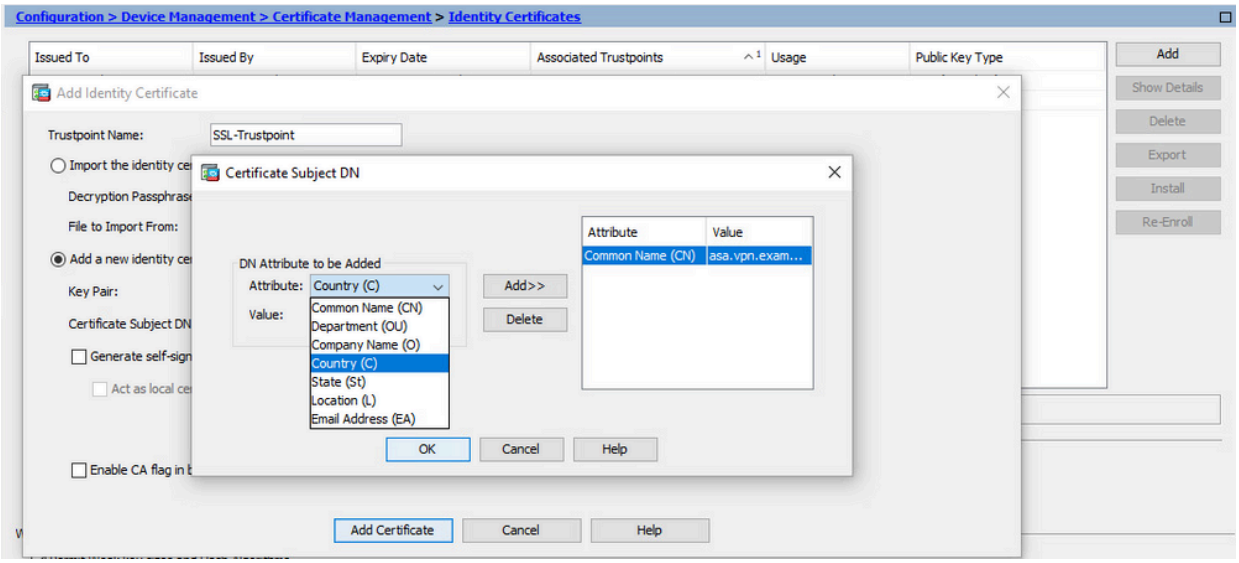
---

a. 单击选择。



b. 在Certificate Subject DN窗口中，配置证书属性 — 从下拉列表中选择属性，输入值，然后点击Add。



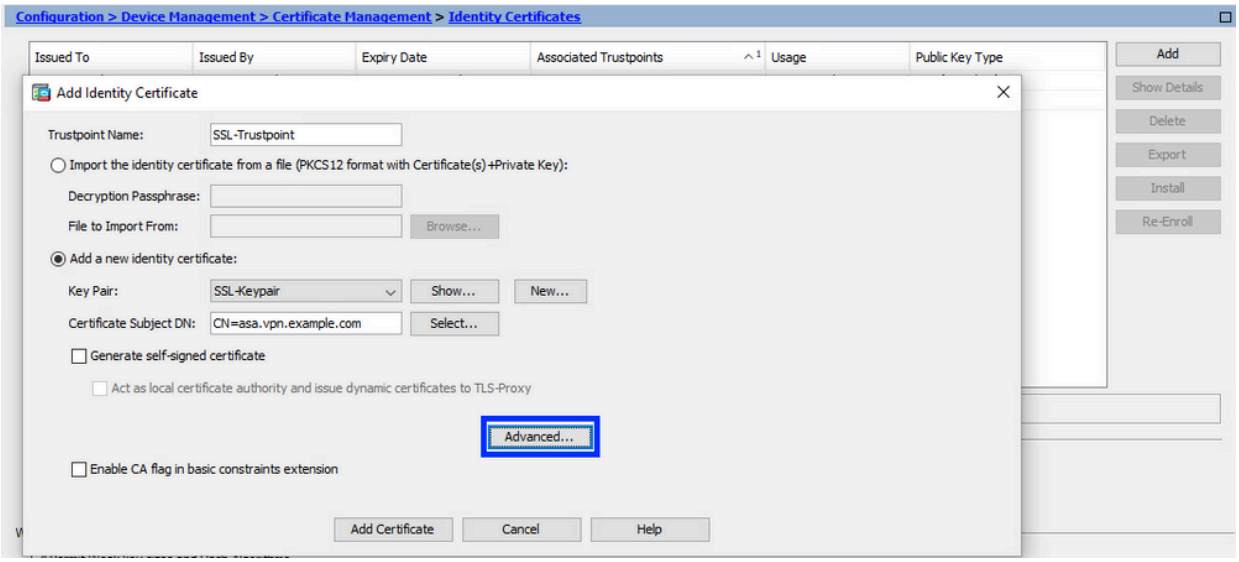


属性	描述
CN	用于访问防火墙的名称(通常为完全限定域名，例如vpn.example.com)。
OU	组织内您所在部门的名称
O	您的组织/公司的合法注册名称
C	国家/地区代码（不带标点的 2 位字母代码）
ST	您的组织所在的州。
L	组织所在的城市。
企业协议 (EA)	电子邮件地址

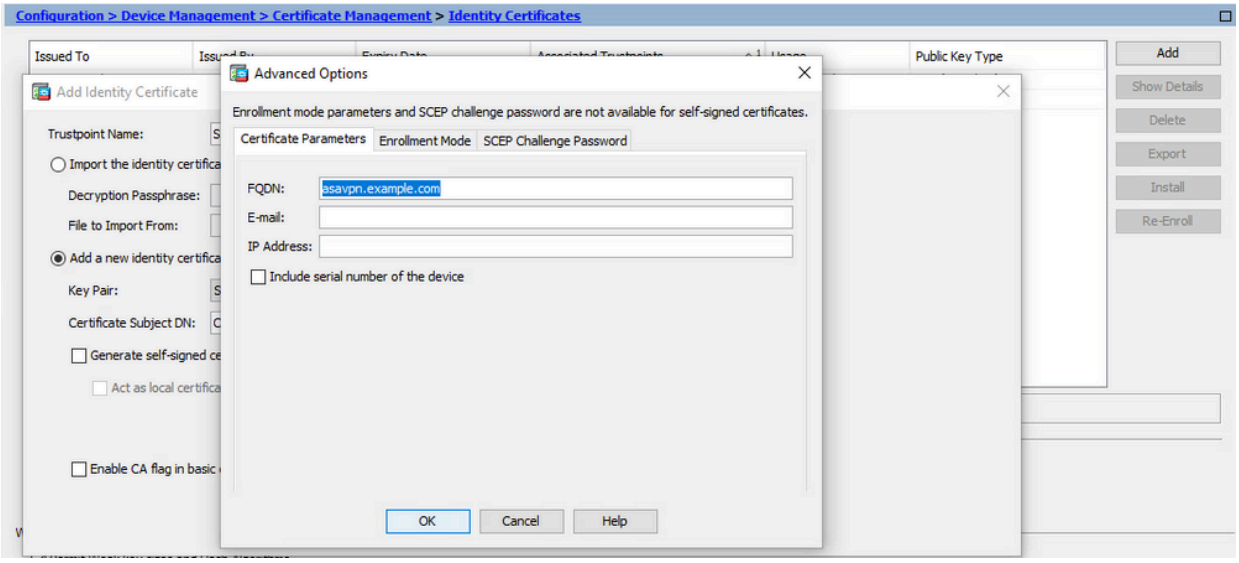
注：前面任何一个字段值都不能超过64个字符的限制。值越长，可能导致身份证书安装问题。此外，无需定义所有DN属性。

添加完所有属性后，单击OK。

c. 配置设备FQDN — 单击Advanced。

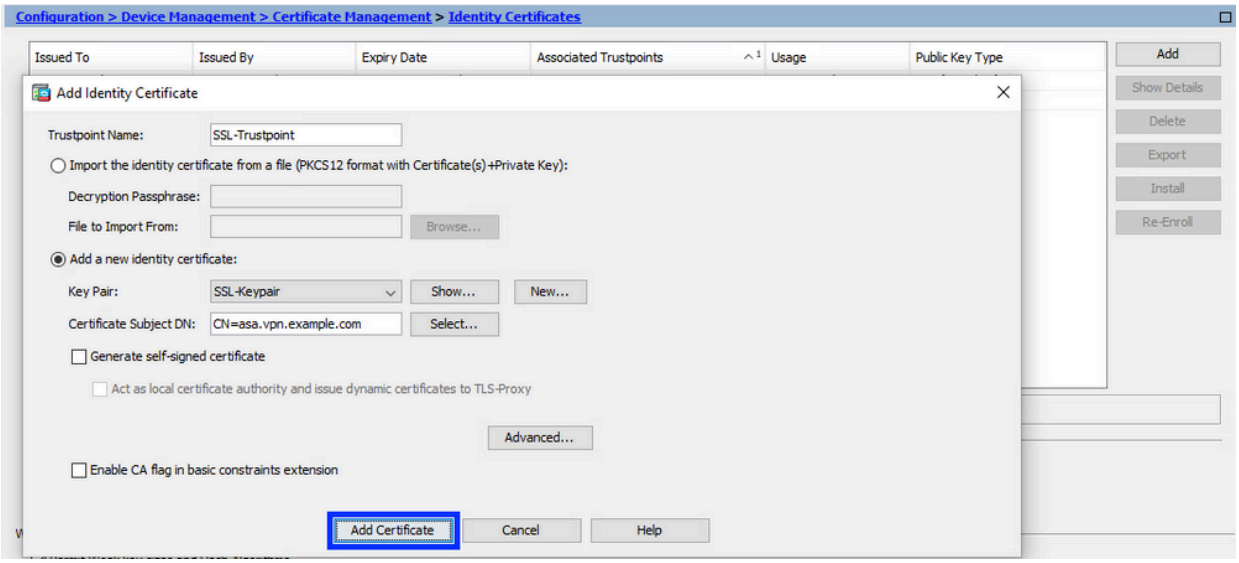


d. 在FQDN字段中，输入从互联网访问设备的完全限定域名。Click OK.

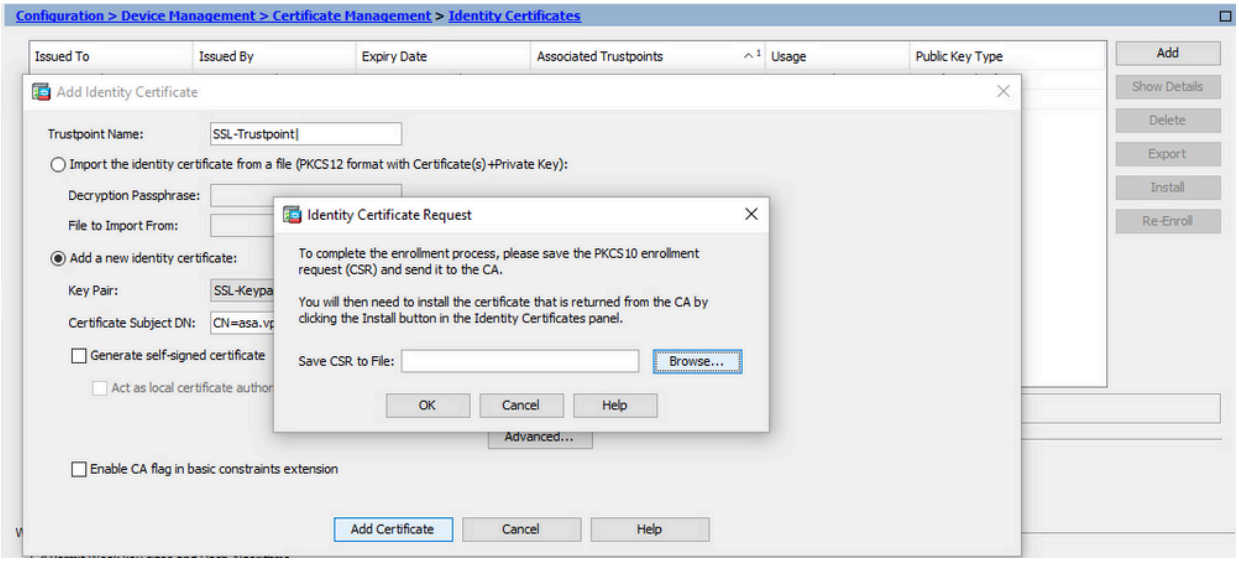


5. 生成并保存CSR

a. 点击添加证书。



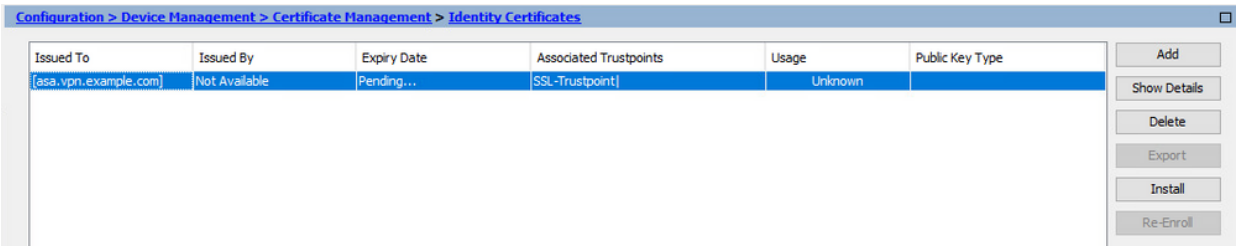
b. 系统显示一则提示，以将 CSR 保存到本地计算机上的文件中。



单击 Browse，选择用于保存 CSR 的位置，然后使用 .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。

c. 现在，新信任点显示为Pending状态。

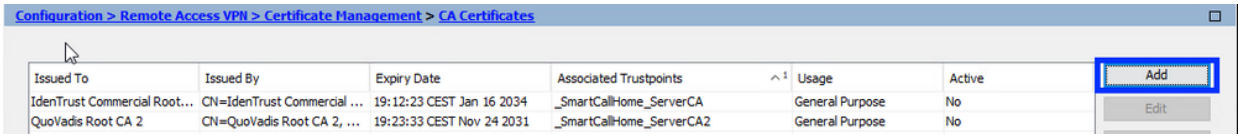


使用ASDM安装PEM格式的身份证书

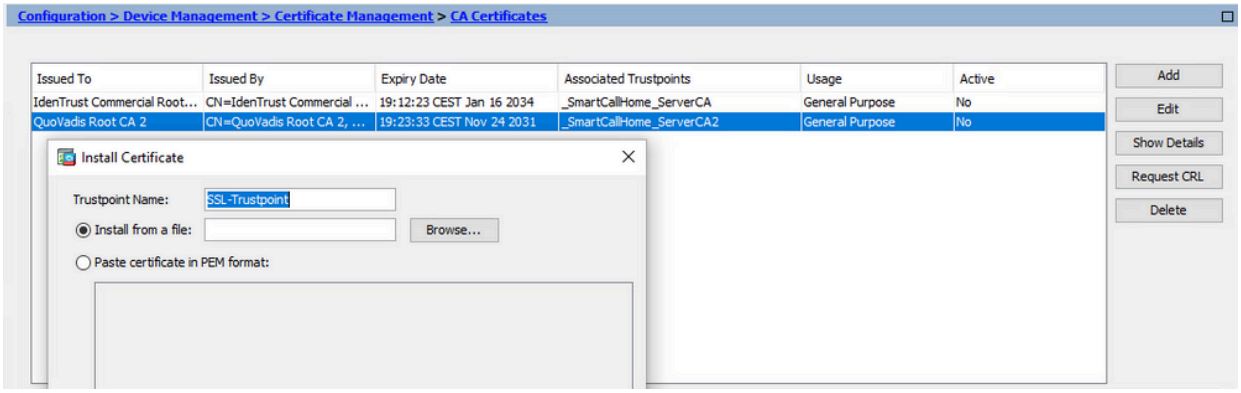
安装步骤假设CA对CSR签名，并提供PEM编码(.pem、.cer、.crt)身份证书和CA证书捆绑包。

1. 安装签署CSR的CA证书

   a. 导航到配置>设备管理>证书管理>，然后选择CA证书。单击 Add。

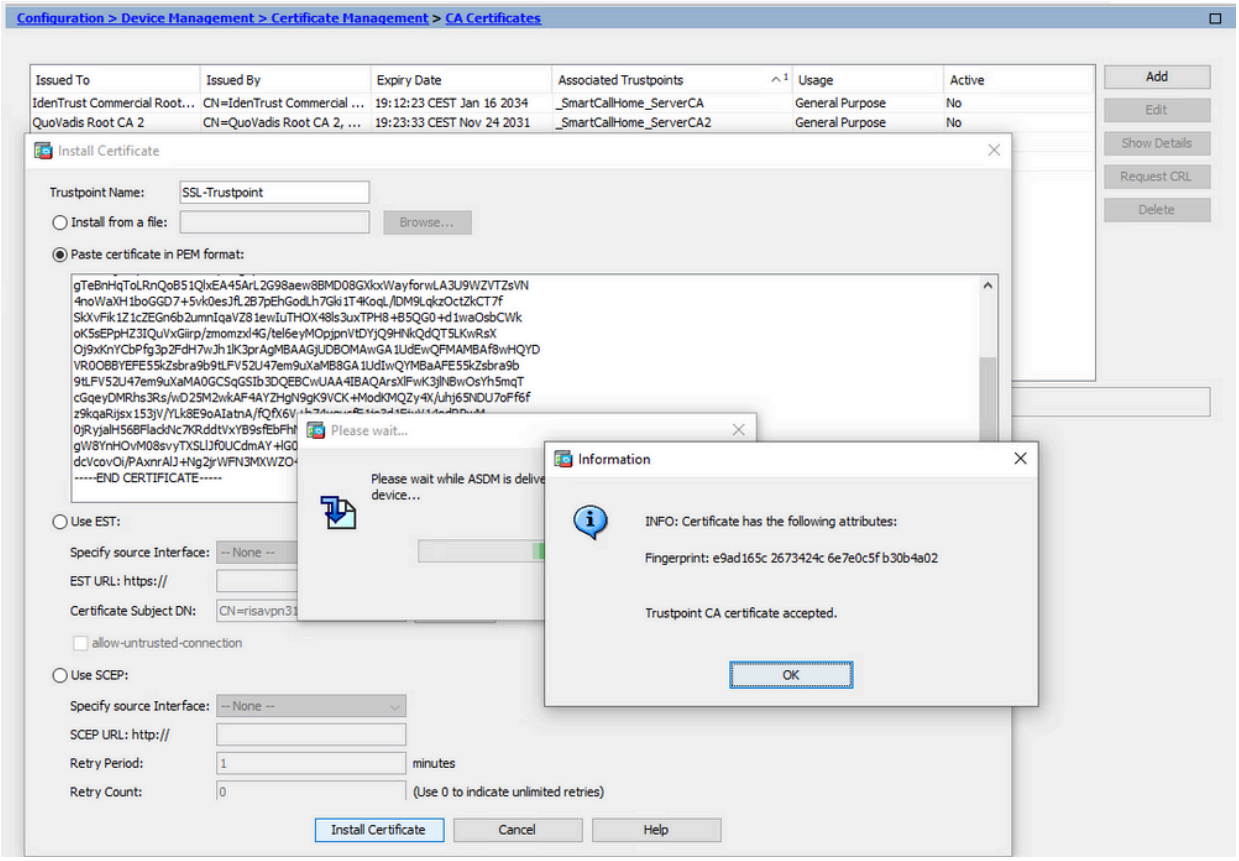


   b. 输入信任点名称并选择从文件安装，点击浏览按钮，然后选择中间证书。或者，将PEM编码的CA证书从文本文件粘贴到文本字段中。



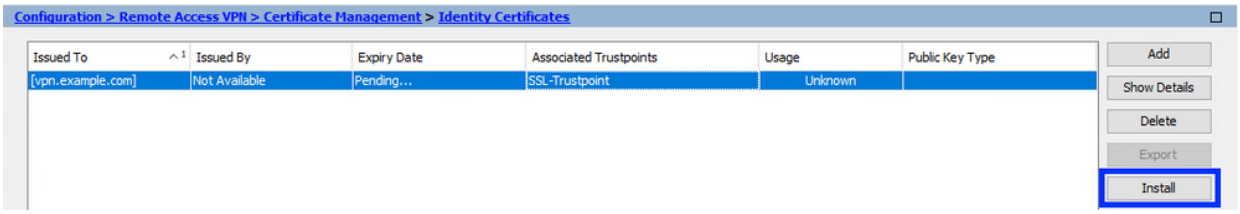
> 注意：安装签署CSR的CA证书，并使用与身份证书相同的信任点名称。PKI层次结构中较高的其他CA证书可以安装在单独的信任点中。

   c. 单击 Install Certificate。



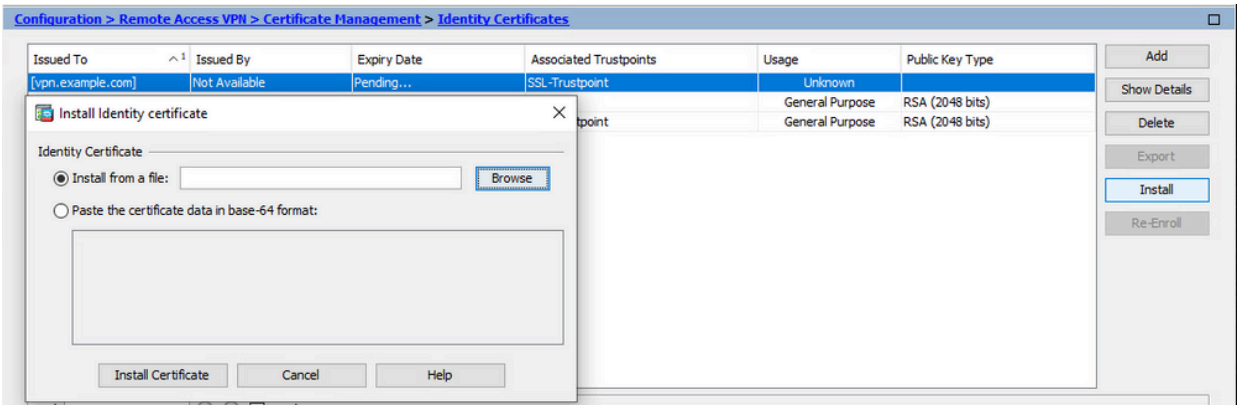
2. 安装身份证书

a. 选择之前在CSR生成期间创建的身份证书。单击 Install。



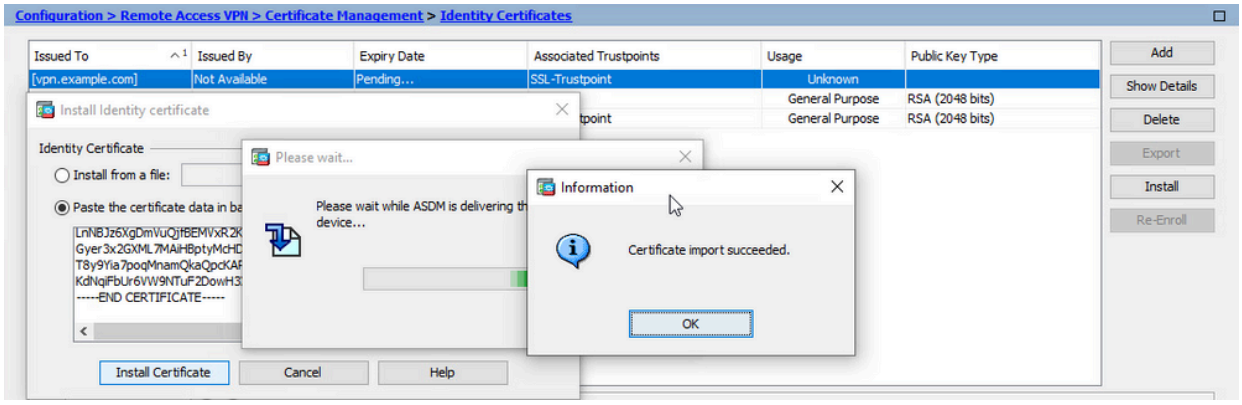
注意：身份证书的Issued By字段可用，Expiry Date字段可用作Pending。

b. 选择包含从CA接收的PEM编码身份证书的文件，或在文本编辑器中打开PEM编码证书，然后将CA提供的身份证书复制并粘贴到文本字段中。



注：身份证书可以采用.pem、.cer、.crt格式进行安装。

c. 单击 Install Certificate。



3. 使用ASDM将新证书绑定到接口

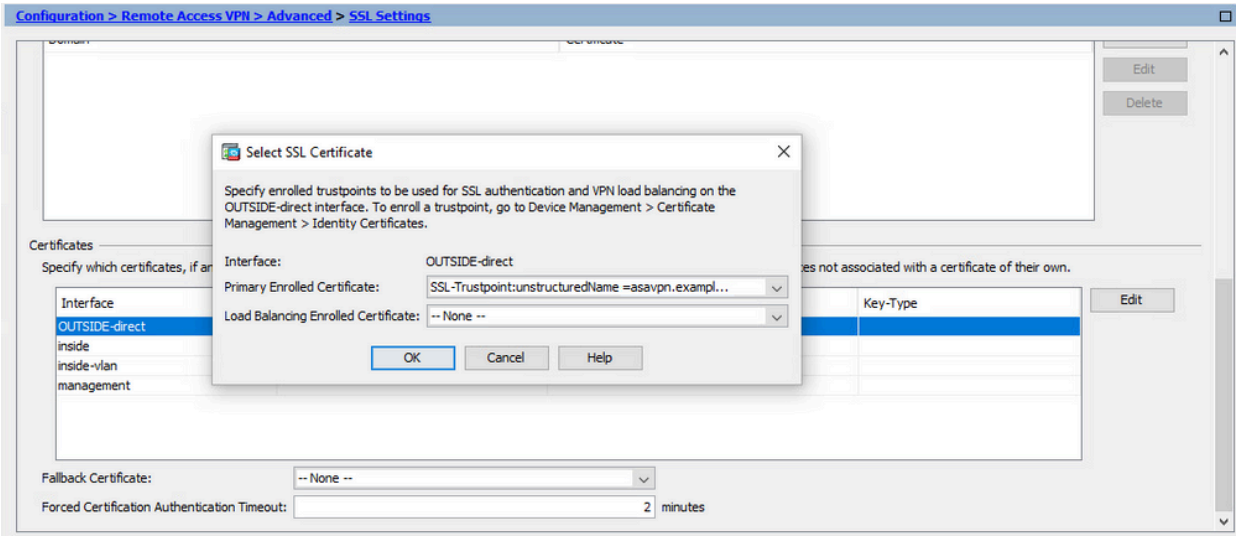
需要将ASA配置为使用新的身份证书，以便在指定接口上终止的WebVPN会话使用。

a. 导航到Configuration > Remote Access VPN > Advanced > SSL Settings。

b. 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。

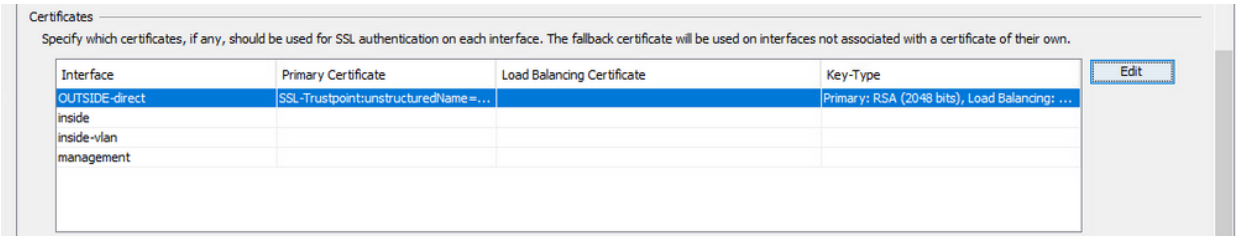
单击 Edit。

c. 在“证书”下拉菜单中，选择新安装的证书。



d. Click OK.

e. 单击 Apply。



现在新的身份证书正在使用。

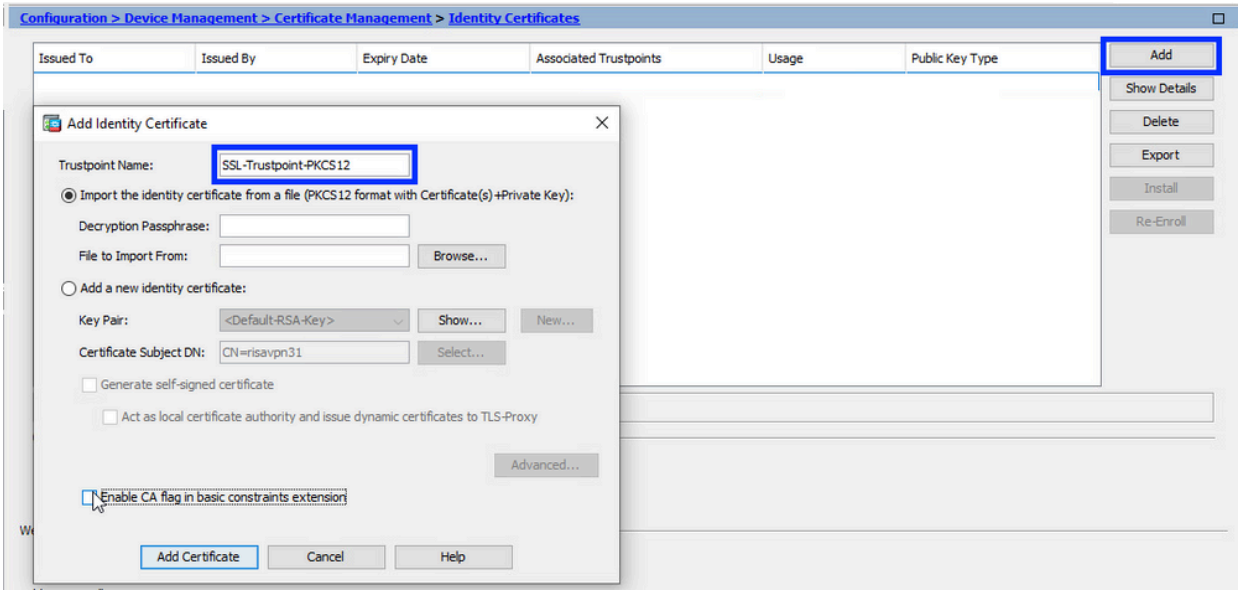
使用ASDM安装以PKCS12格式收到的身份证书

PKCS12文件（.p12或.pfx格式）包含身份证书、密钥对和CA证书。它由CA创建，例如使用通配符证书，或者从其他设备导出。它是二进制文件，不能使用文本编辑器查看。

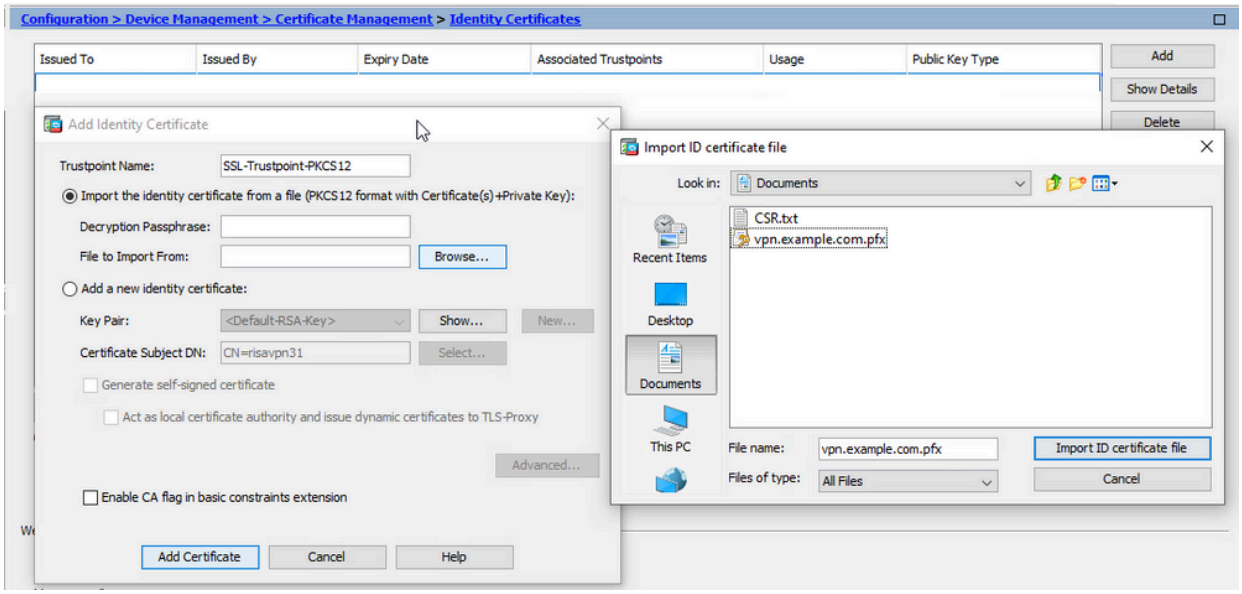
1. 从PKCS12文件安装身份和CA证书

身份证书、CA证书和密钥对需要捆绑到单个PKCS12文件中。

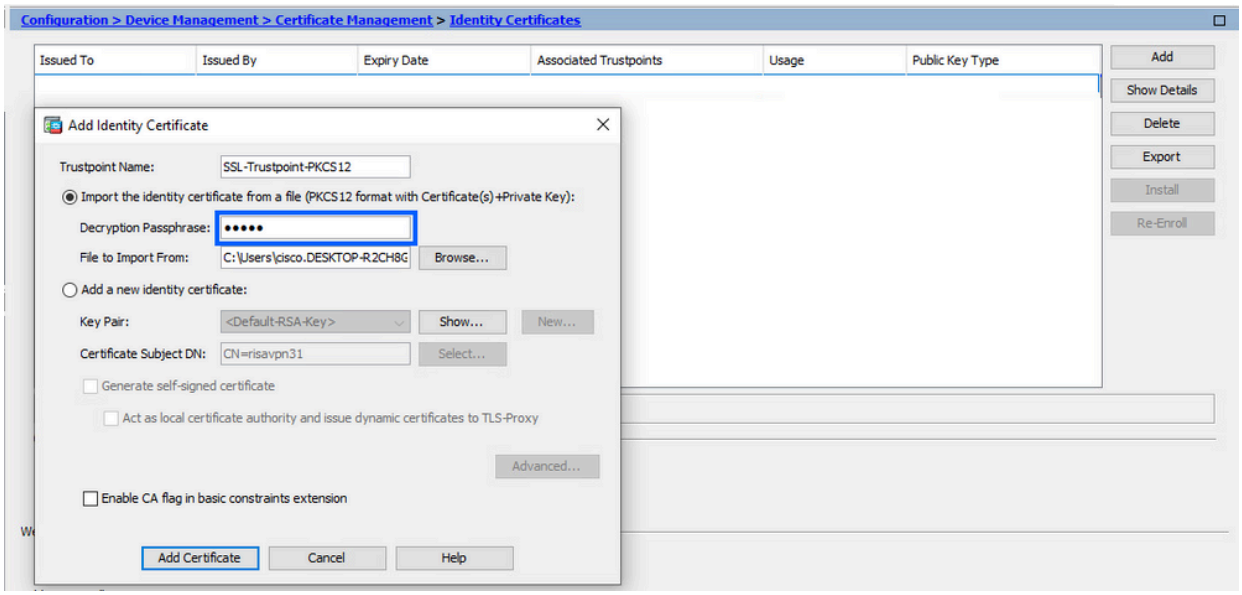
a. 导航到Configuration > Device Management > Certificate Management，然后选择Identity Certificates。
b. 单击 Add。
c. 指定信任点名称。



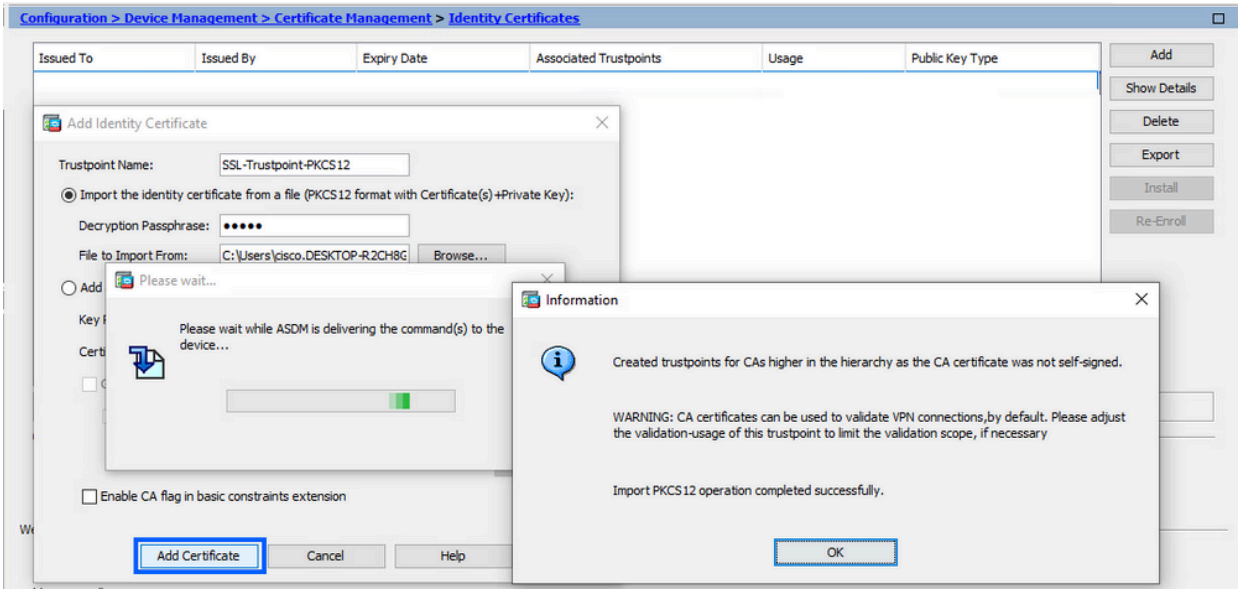
d. 单击Import The Identity Certificate from a File单选按钮。



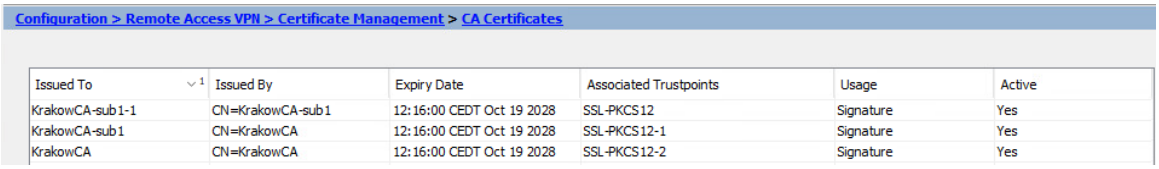
e. 输入用于创建 PKCS12 文件的密码。



f. 点击添加证书。



注意：导入带CA证书链的PKCS12时，ASDM会自动创建带有添加了 — number后缀的名称的上游CA信任点。



Configuration > Remote Access VPN > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
KrakowCA-sub1-1	CN=KrakowCA-sub1	12:16:00 CEDT Oct 19 2028	SSL-PKCS12	Signature	Yes
KrakowCA-sub1	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-1	Signature	Yes
KrakowCA	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-2	Signature	Yes

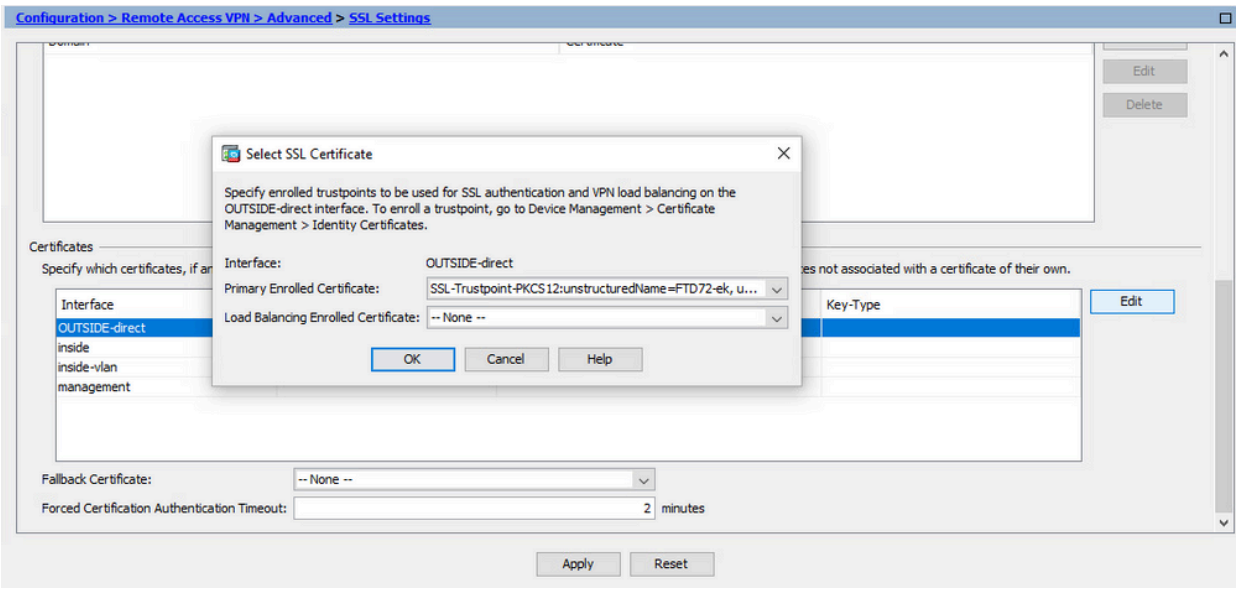
2. 使用ASDM将新证书绑定到接口

需要将ASA配置为使用新的身份证书，以便在指定接口上终止的WebVPN会话使用。

a. 导航到Configuration > Remote Access VPN > Advanced > SSL Settings。

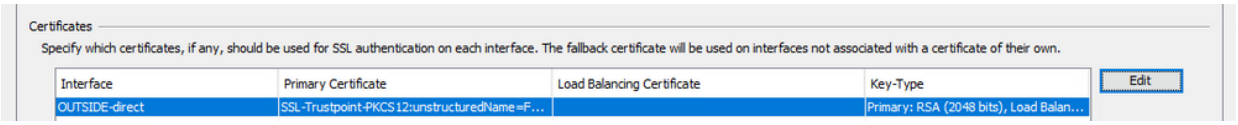
b. 在“证书”下，选择用于端接 WebVPN 会话的接口。在本例中，使用的是外部接口。单击 Edit。

c. 在“证书”下拉菜单中，选择新安装的证书。



d. Click OK.

e. 单击 Apply。



现在新的身份证书正在使用。

证书续订

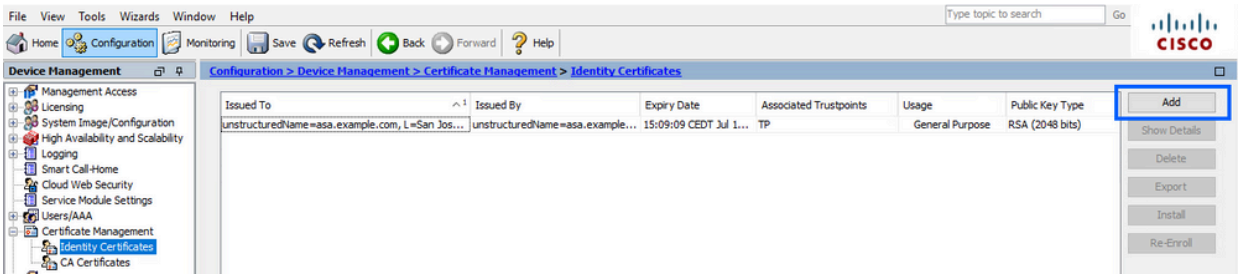
使用ASDM续订使用证书签名请求(CSR)注册的证书

CSR注册证书的证书续订需要创建和注册新的信任点。它需要具有不同的名称（例如，具有注册年份后缀的旧名称）。它可以使用与旧证书相同的参数和密钥对，也可以使用不同的参数和密钥对。

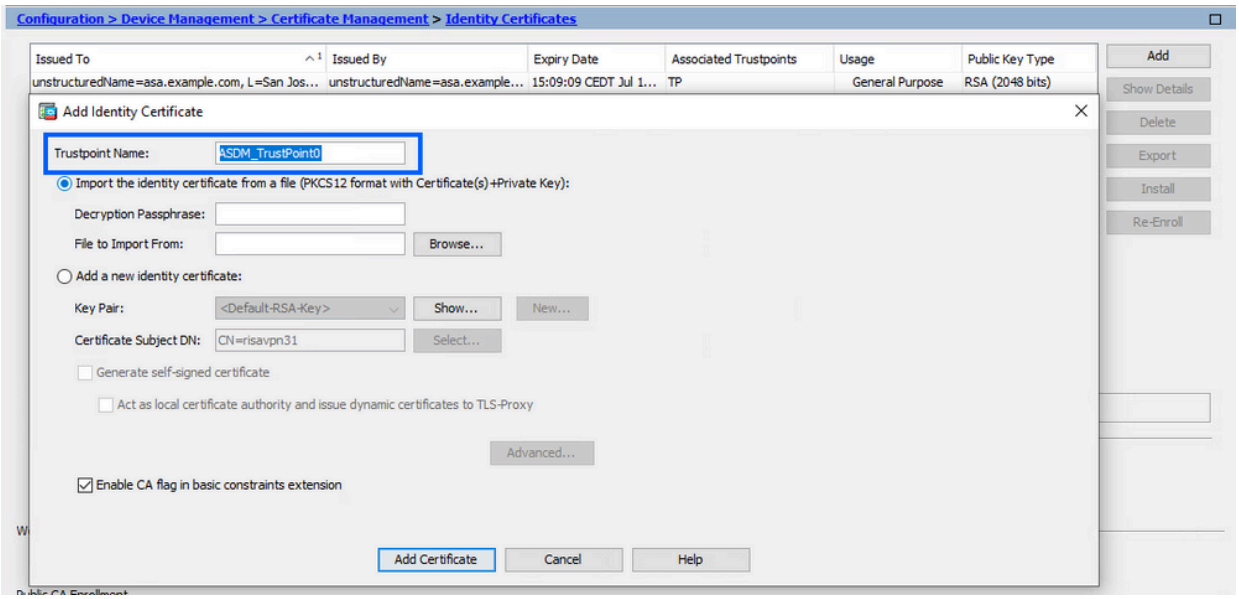
使用ASDM生成CSR

1. 创建具有特定名称的新信任点。

a. 导航到Configuration > Device Management > Certificate Management > Identity Certificates。



b. 单击 Add。
c. 定义信任点名称。

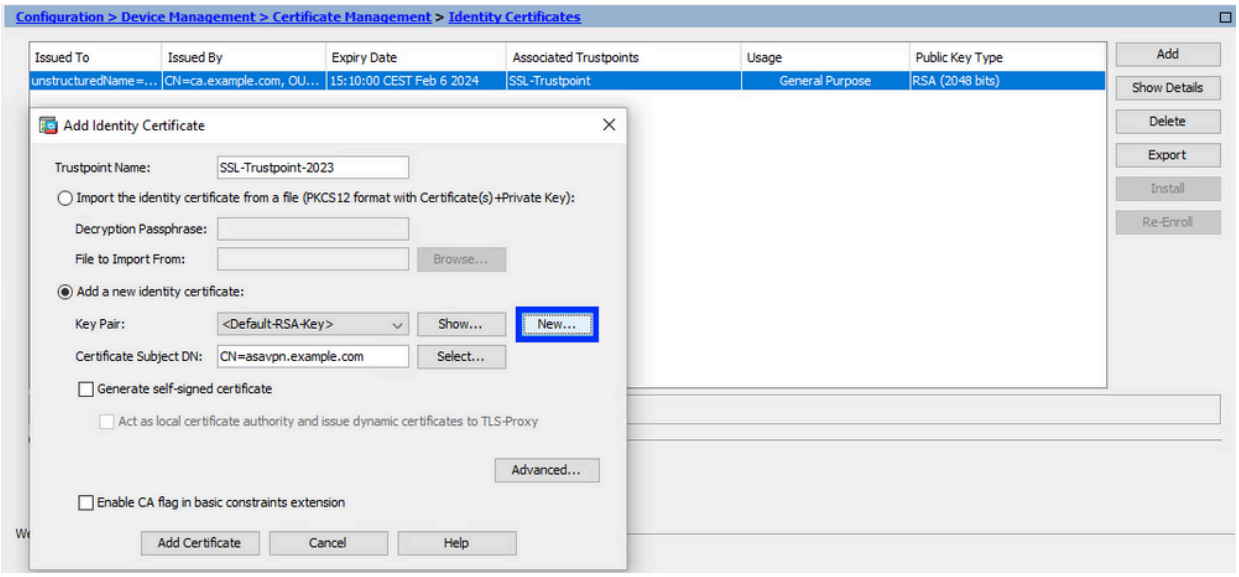


d. 单击 Add a new identity certificate 单选按钮。

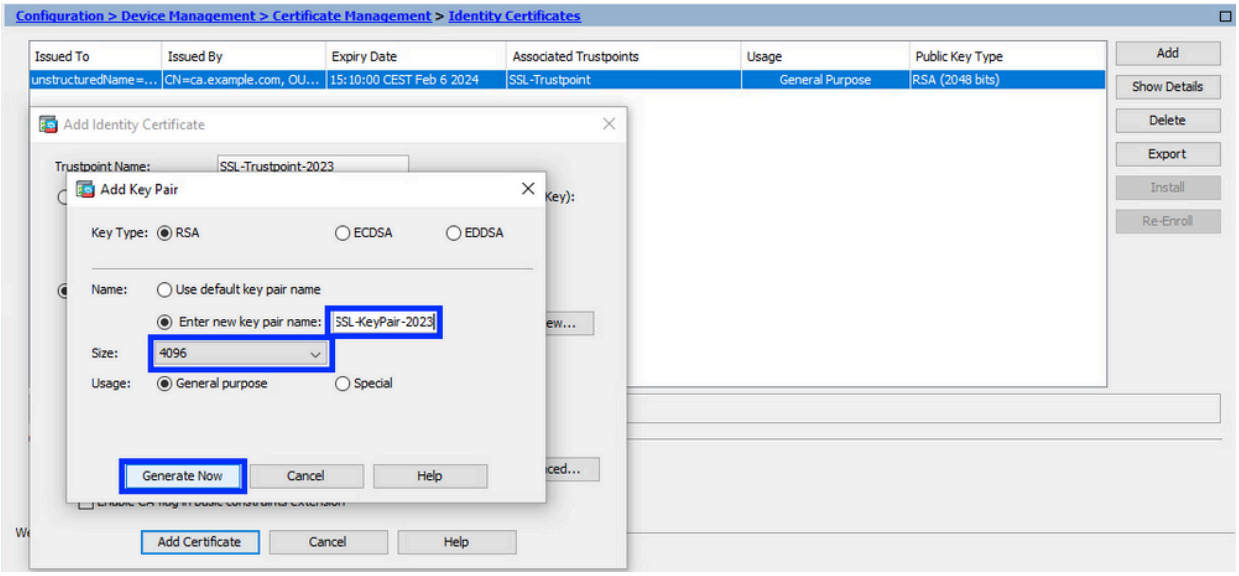
2. （可选）创建新密钥对

> 注意：默认情况下，使用名称为Default-RSA-Key且大小为2048的RSA密钥；但是，建议为每个身份证书使用唯一的专用/公共密钥对。

a. 单击New生成新的密钥对。

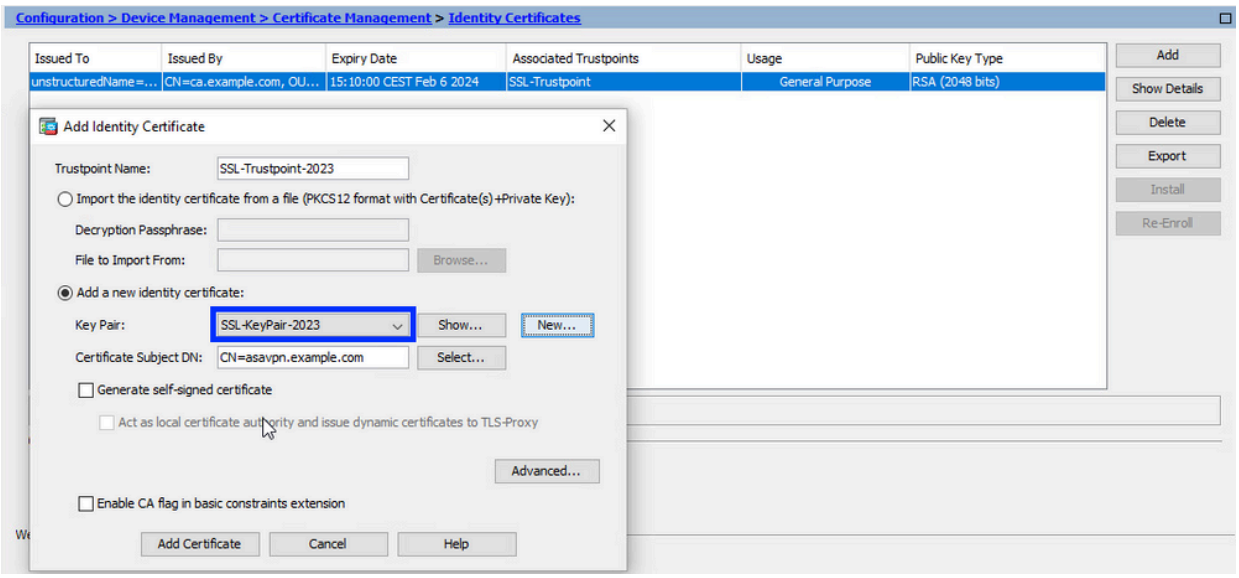


b. 选择选项Enter new Key Pair name并输入新密钥对的名称。
c. 选择Key Type - RSA或ECDSA。
d. 选择Key Size；对于RSA，选择General purpose for Usage。
e. 单击 Generate Now。密钥对现已创建。



3. 选择密钥对名称

选择密钥对以签署CSR并将与新证书绑定。

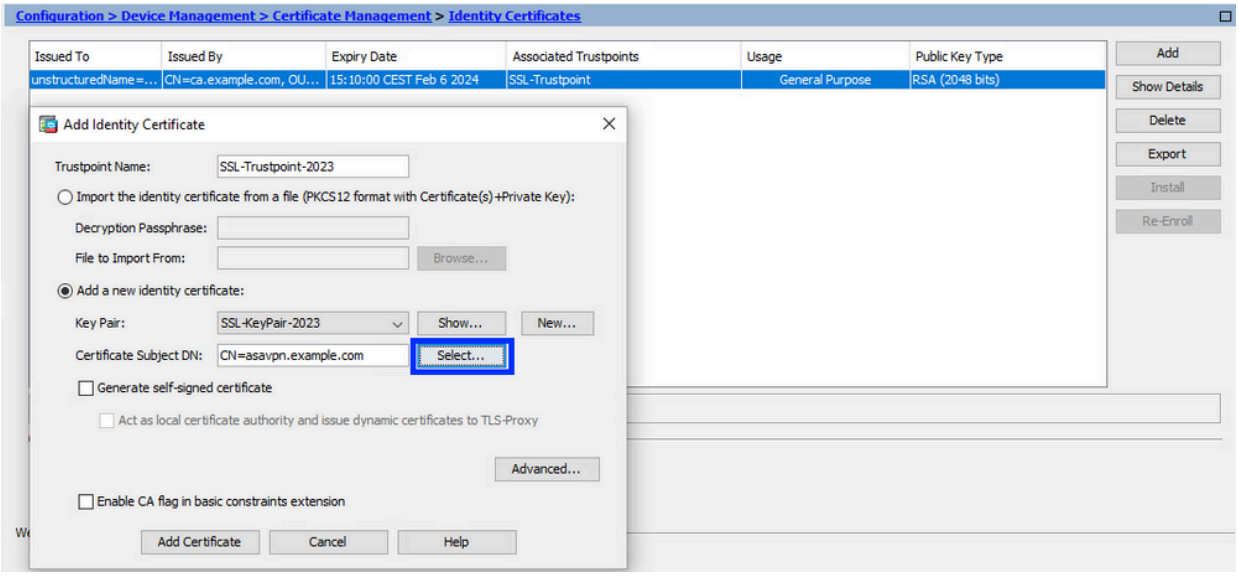


4. 配置证书主题和完全限定域名(FQDN)

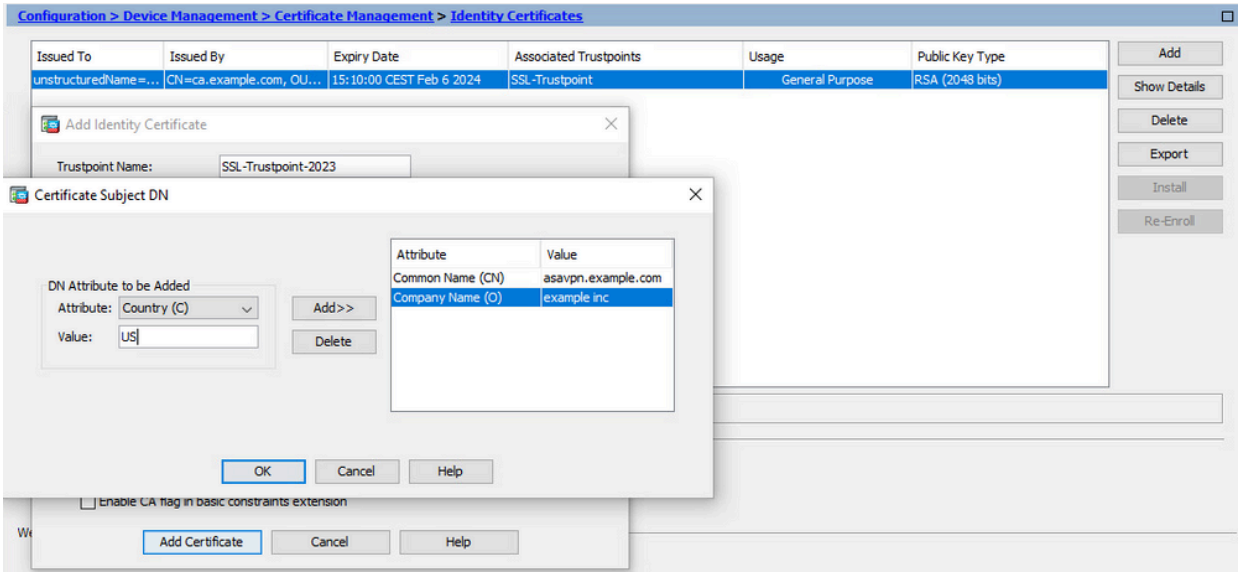
注意：FQDN参数必须与证书使用的ASA接口的FQDN或IP地址匹配。此参数设置证书的主题备用名称(SAN)。SSL/TLS/IKEv2客户端使用SAN字段验证证书是否与其连接的FQDN匹配。

注意：CA可在签署CSR并创建签名身份证书时更改信任点中定义的FQDN和主题名称参数。

a. 单击选择。



b. 在Certificate Subject DN窗口中，配置证书属性 — 从下拉列表中选择属性，输入值，然后点击Add。



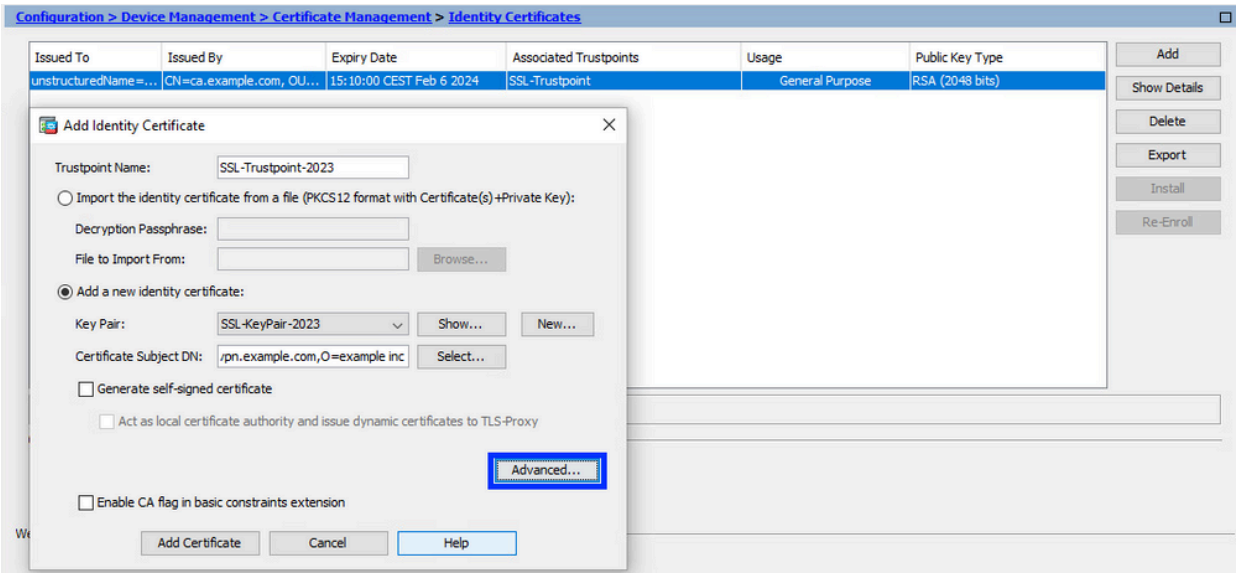
属性	描述
CN	用于访问防火墙的名称(通常为完全限定域名，例如vpn.example.com)。
OU	组织内您所在部门的名称
O	您的组织/公司的合法注册名称
C	国家/地区代码（不带标点的 2 位字母代码）

属性	描述
ST	您的组织所在的州。
L	组织所在的城市。
企业协议 (EA)	电子邮件地址

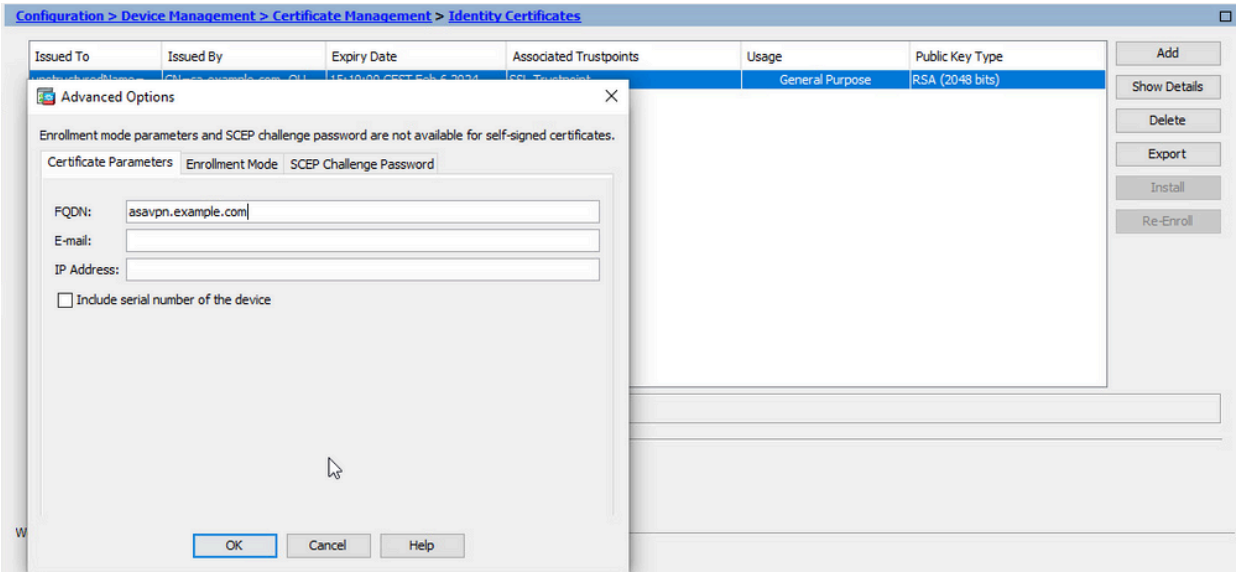
注：前面的所有字段都不能超过64个字符的限制。值越长，可能导致身份证书安装问题。此外，无需定义所有DN属性。

添加完所有属性后，单击OK。

c. 要配置设备FQDN，请单击Advanced。

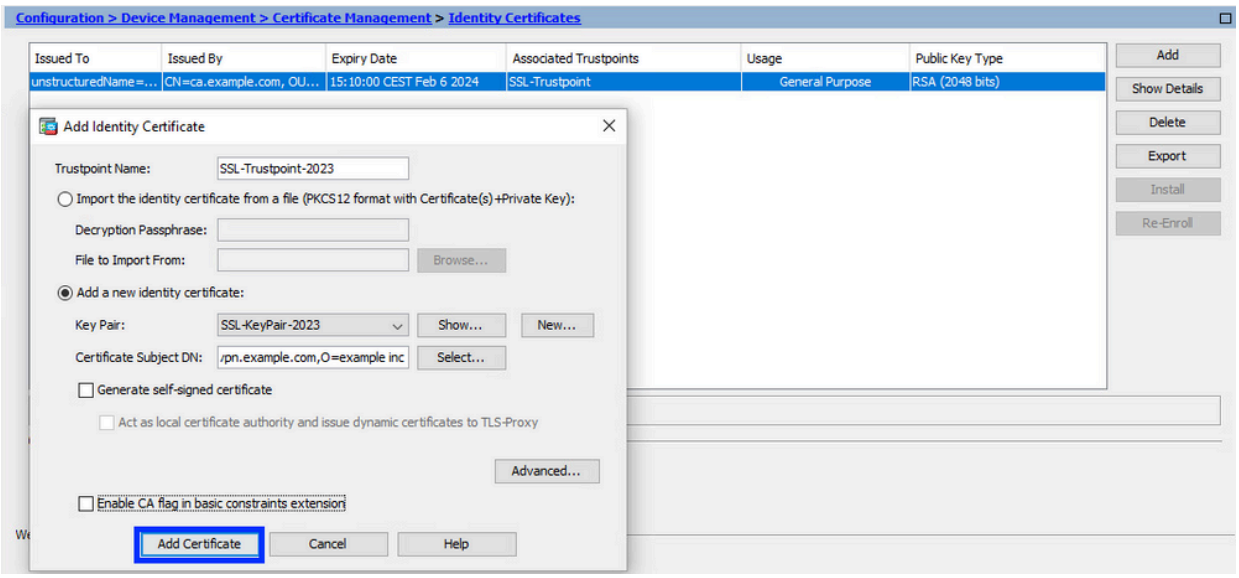


d. 在FQDN字段中，输入从互联网访问设备的完全限定域名。Click OK.

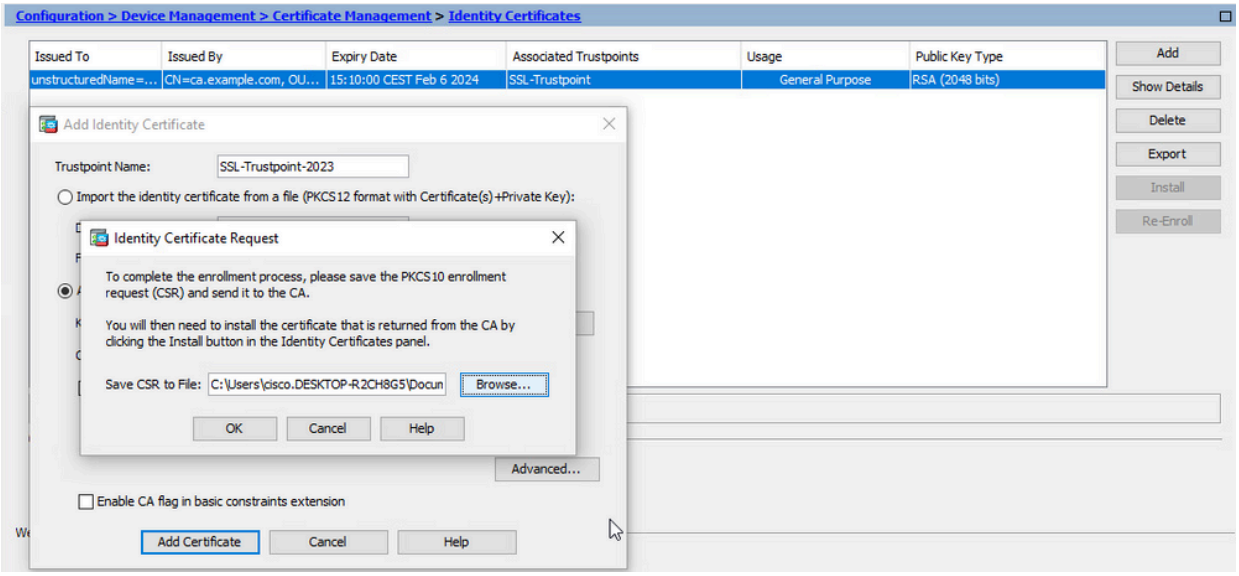


5. 生成并保存CSR

a. 点击添加证书。



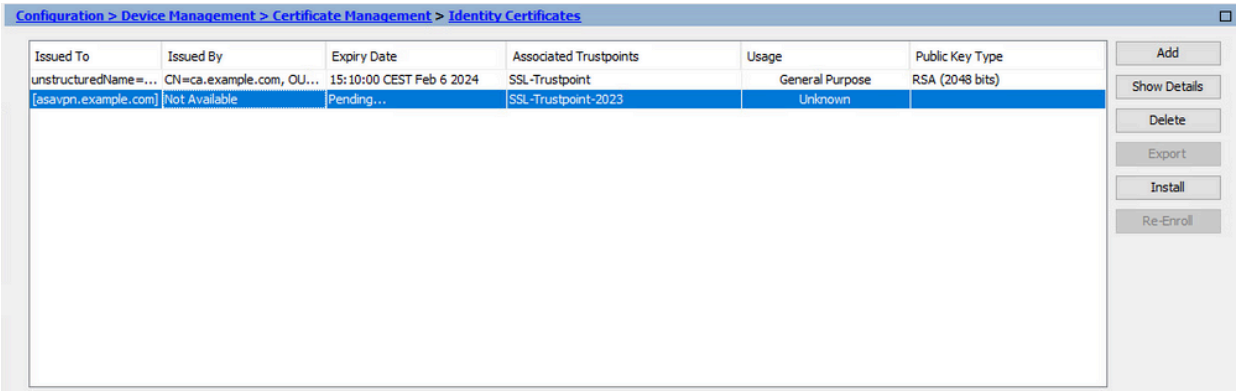
b. 系统显示一则提示，以将 CSR 保存到本地计算机上的文件中。



单击浏览。 选择保存CSR的位置，并保存扩展名为.txt的文件。

> 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。

c. 现在，新信任点显示为Pending状态。



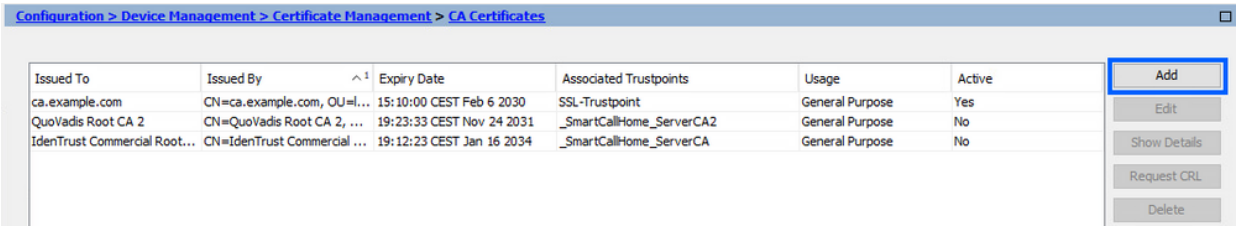
使用ASDM安装PEM格式的身份证书

安装步骤假设CA对CSR进行签名，并提供PEM编码(.pem、.cer、.crt)的新身份证书和CA证书捆绑包。

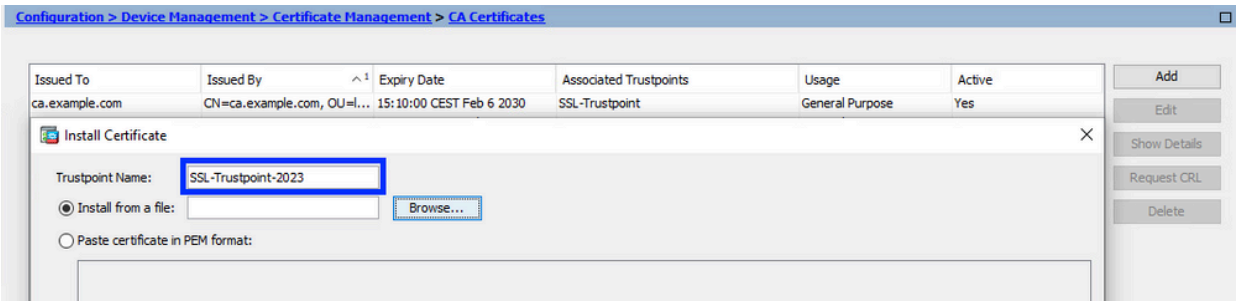
1. 安装签署CSR的CA证书

签名身份证书的CA证书可以安装在为身份证书创建的信任点中。如果身份证书由中间CA签名，则此CA证书可以安装在身份证书信任点中。层次结构中上游的所有CA证书可以安装在单独的CA信任点中。

a. 导航到Configuration > Device Management > Certificate Management >，然后选择CA Certificates。单击 Add。

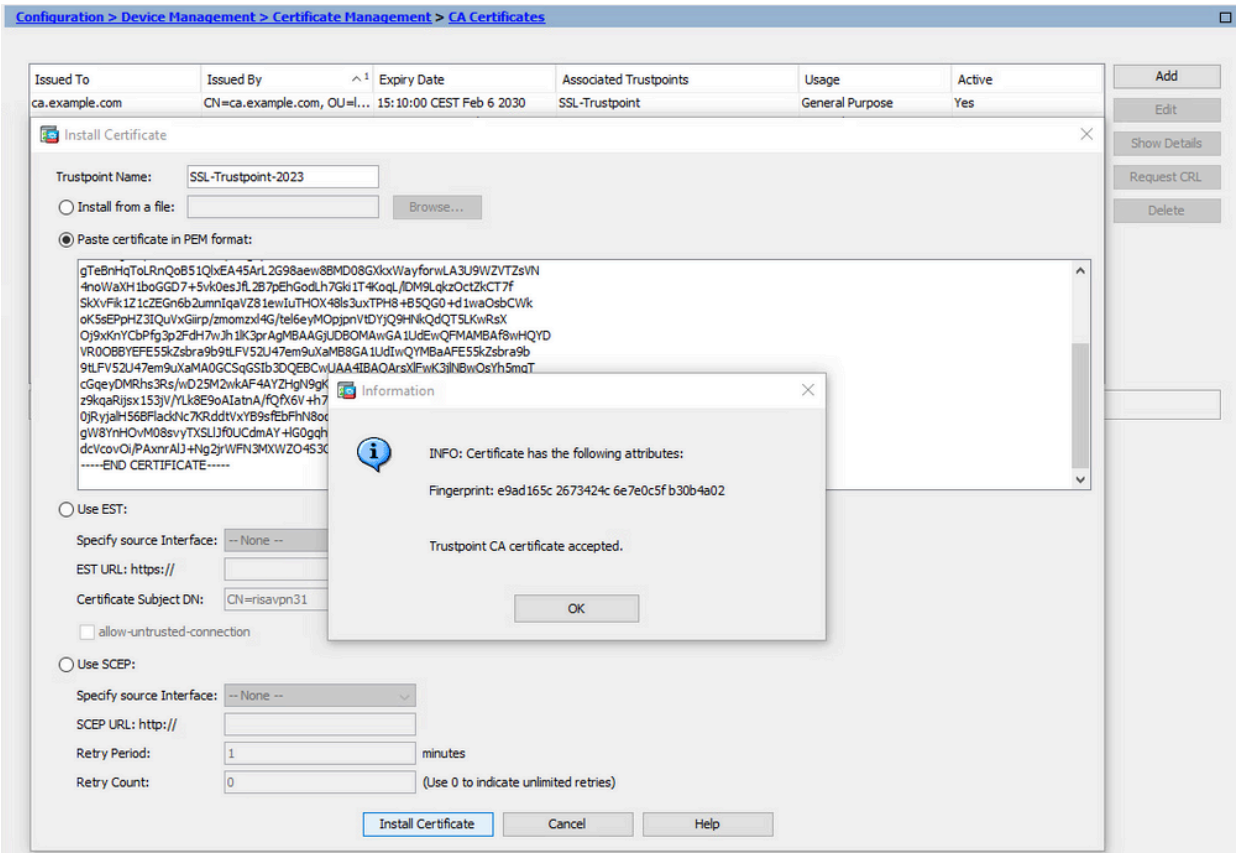


b. 输入信任点名称并选择从文件安装，单击浏览按钮，然后选择中间证书。或者，将PEM编码的CA证书从文本文件粘贴到文本字段中。

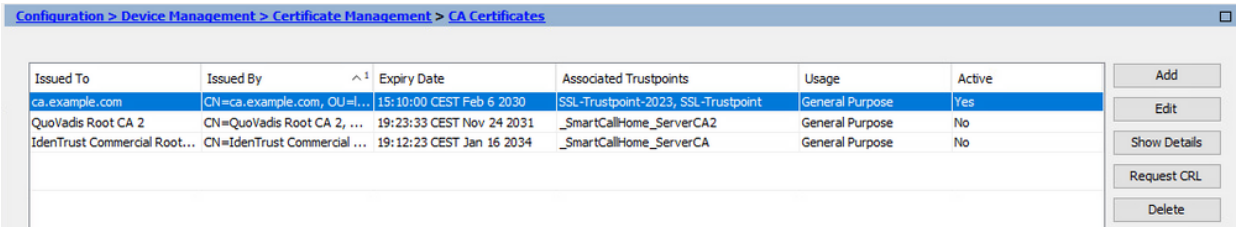


注意：如果身份证书由中间CA证书签名，请安装信任点名称与身份证书信任点名称相同的中间证书。

c. 单击 Install Certificate。

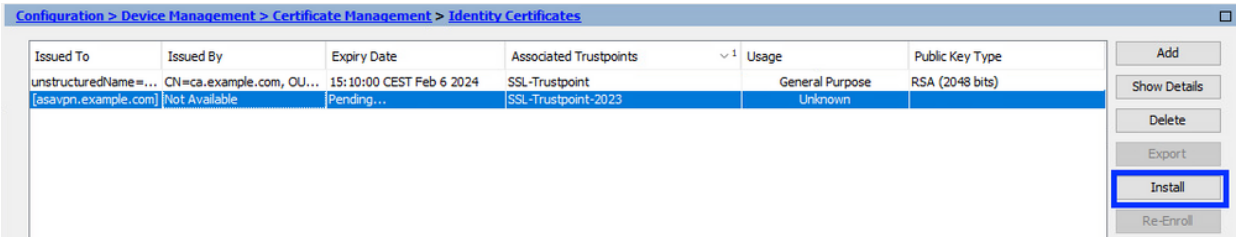


在本例中，新证书使用与旧证书相同的CA证书签名。同一个CA证书现在与两个信任点关联。



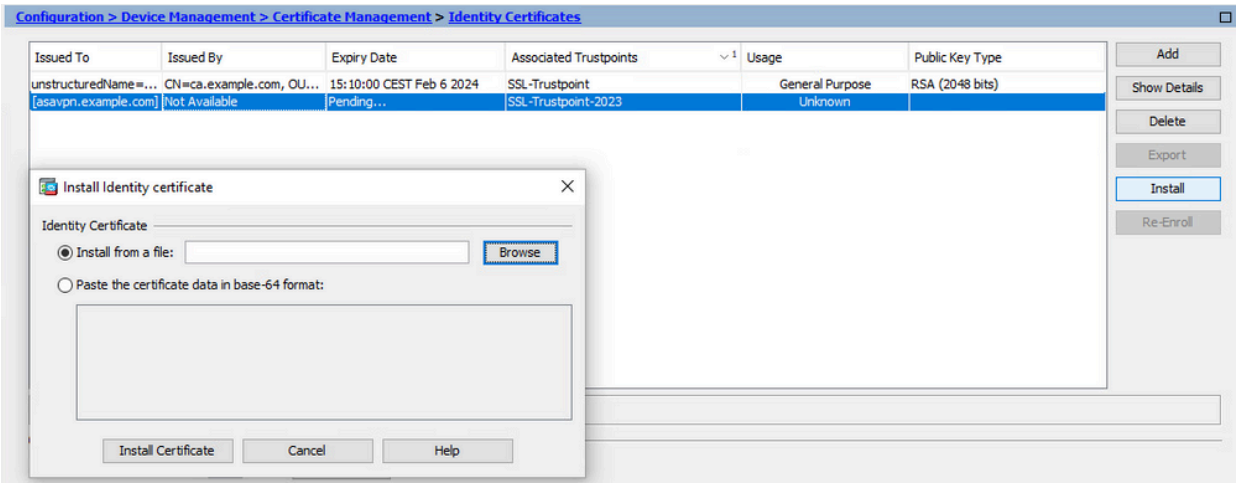
2. 安装身份证书

a. 选择之前通过CSR生成创建的身份证书。单击 Install。



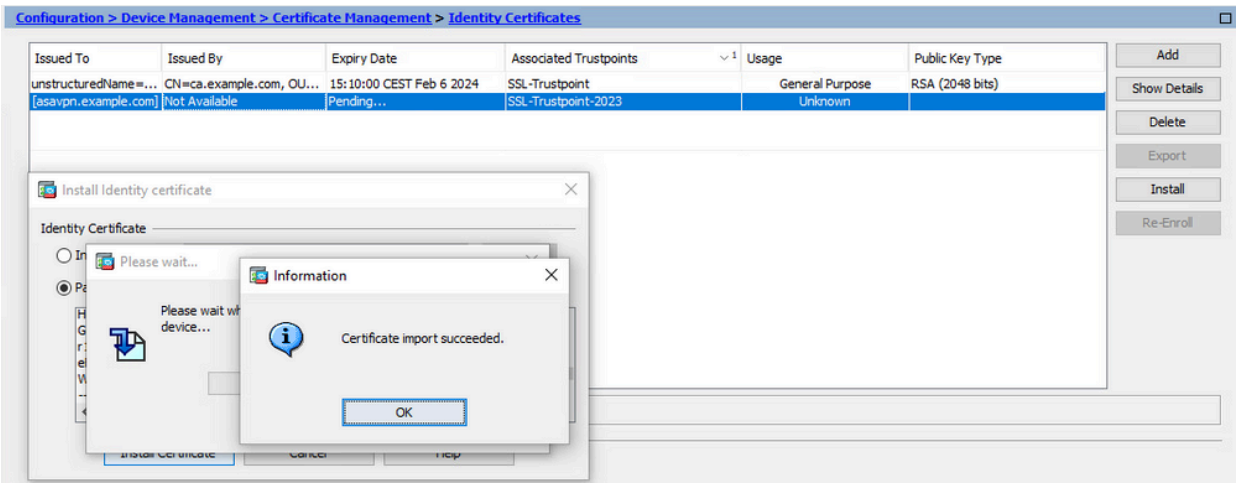
> 注意：身份证书的Issued By字段可为Not available，而Expiry Date字段为Pending。

b. 选择包含从CA接收的PEM编码身份证书的文件，或在文本编辑器中打开PEM编码证书，然后将CA提供的身份证书复制并粘贴到文本字段中。

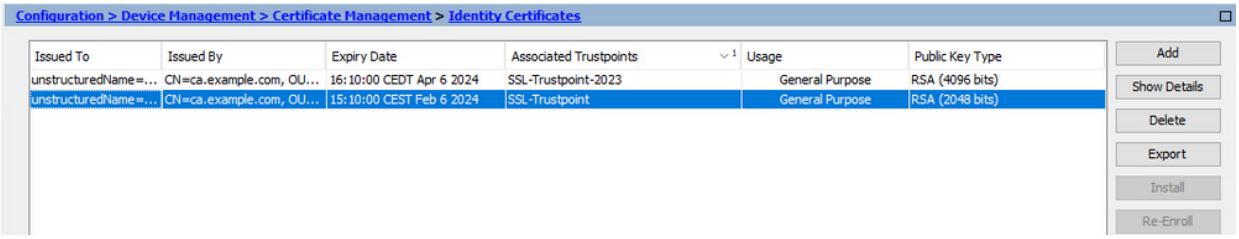


> 注：身份证书可以采用.pem、.cer、.crt格式进行安装。

c. 单击 Install Certificate。



安装后，存在旧身份证书和新身份证书。



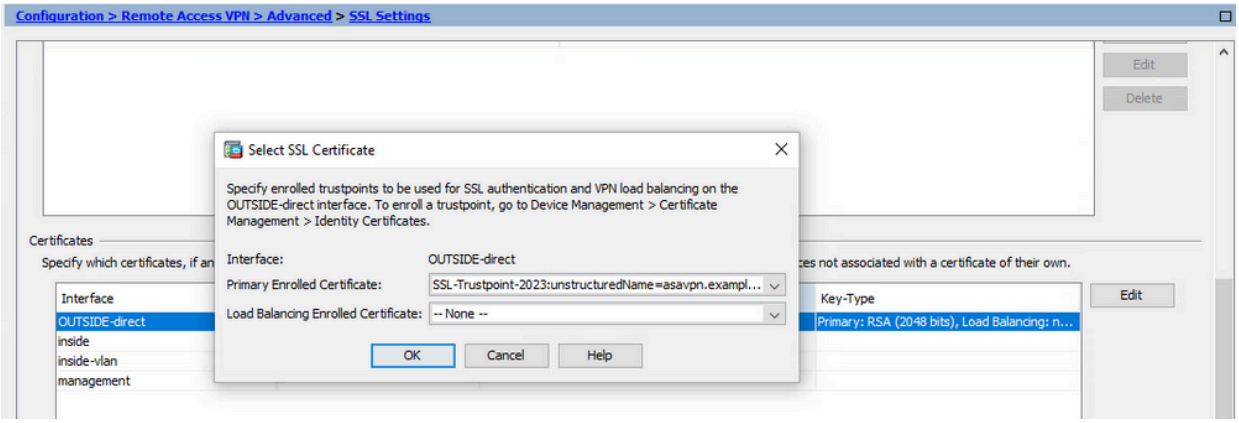
3. 使用ASDM将新证书绑定到接口

需要将ASA配置为使用新的身份证书，以便在指定接口上终止的WebVPN会话使用。

a. 导航到Configuration > Remote Access VPN > Advanced > SSL Settings。

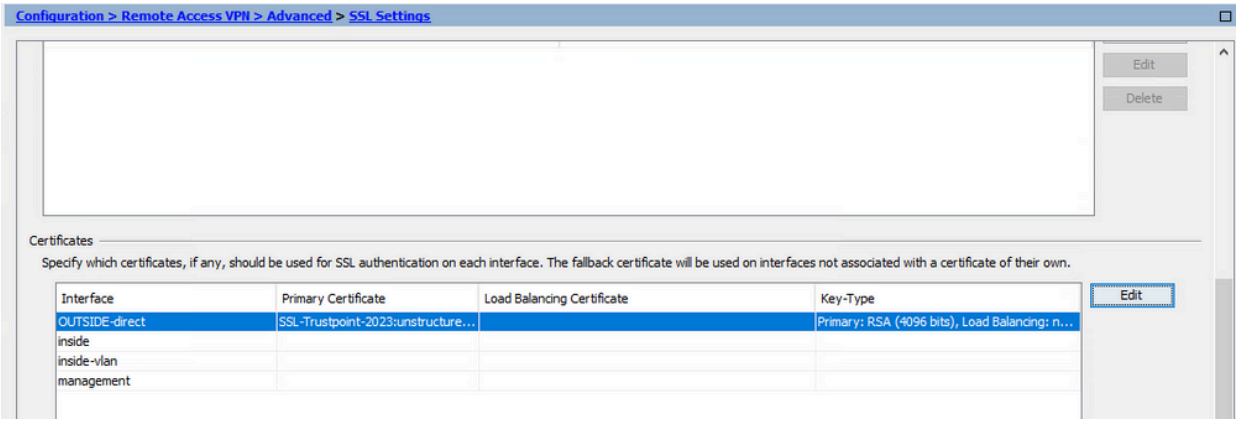
b. 在“证书”下，选择用于端接 WebVPN 会话的接口。在本例中，使用的是外部接口。单击 Edit。

c. 在“证书”下拉菜单中，选择新安装的证书。



d. Click OK.

e. 单击 Apply。现在新的身份证书正在使用。



使用ASDM续订使用PKCS12文件注册的证书

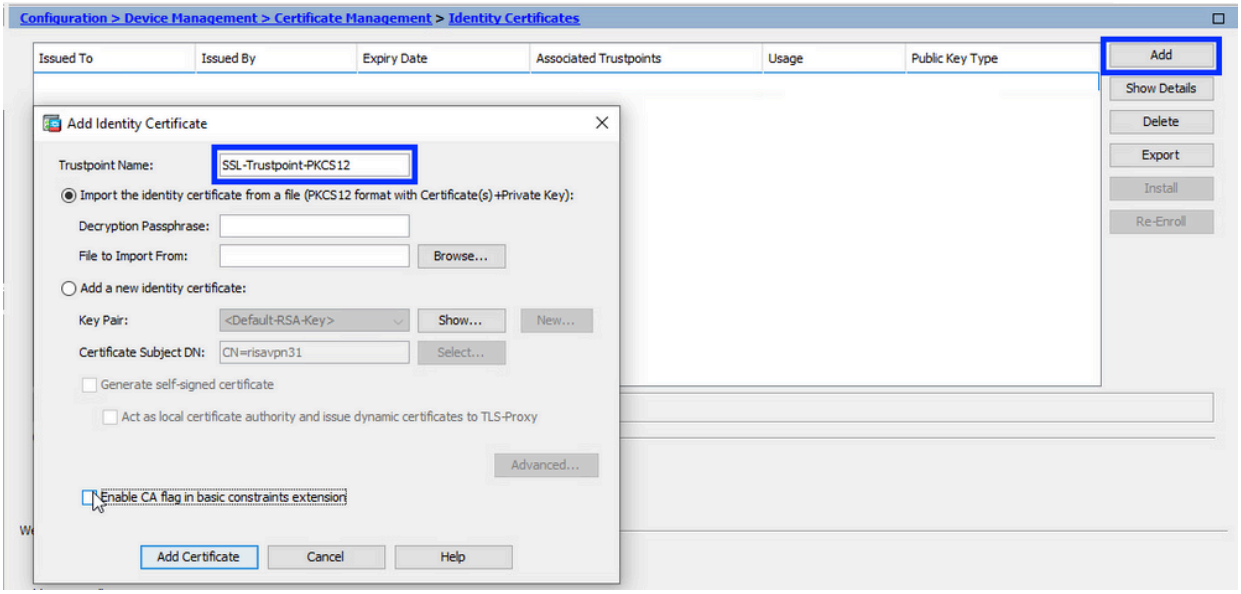
PKCS12注册证书的证书续订需要创建和注册新的信任点。它需要具有不同的名称（例如，具有注册年份后缀的旧名称）。

PKCS12文件（.p12或.pfx格式）包含身份证书、密钥对和CA证书。例如，通配符证书由CA创建，或从其他设备导出。它是二进制文件，不能通过文本编辑器查看。

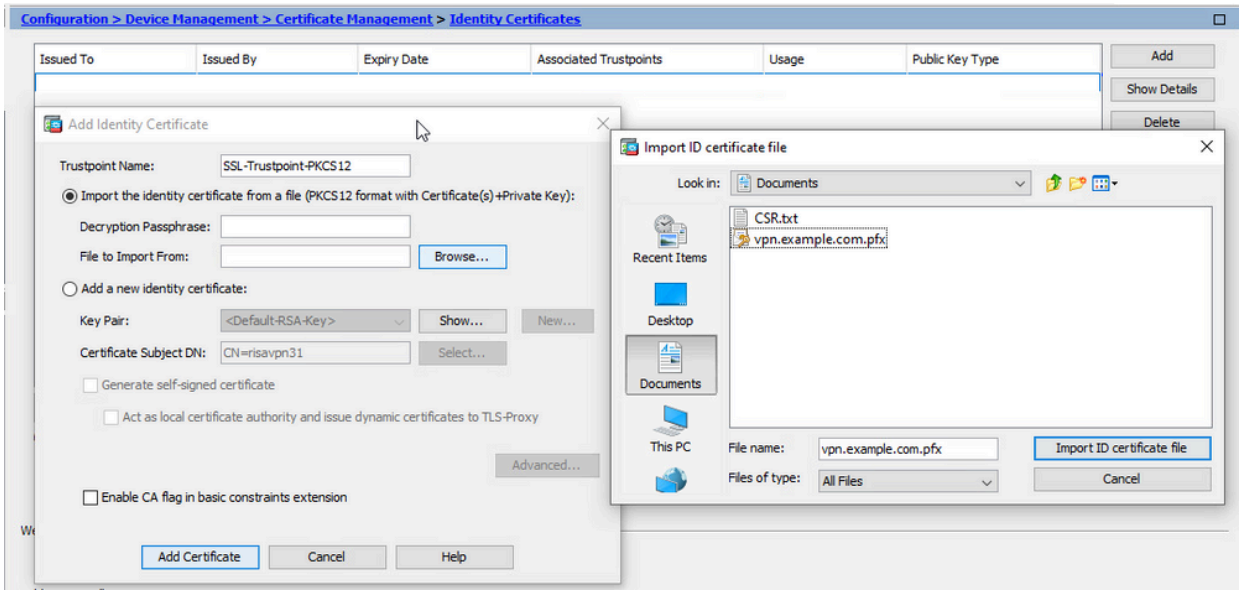
1. 从PKCS12文件安装更新的身份证书和CA证书

身份证书、CA证书和密钥对需要捆绑到单个PKCS12文件中。

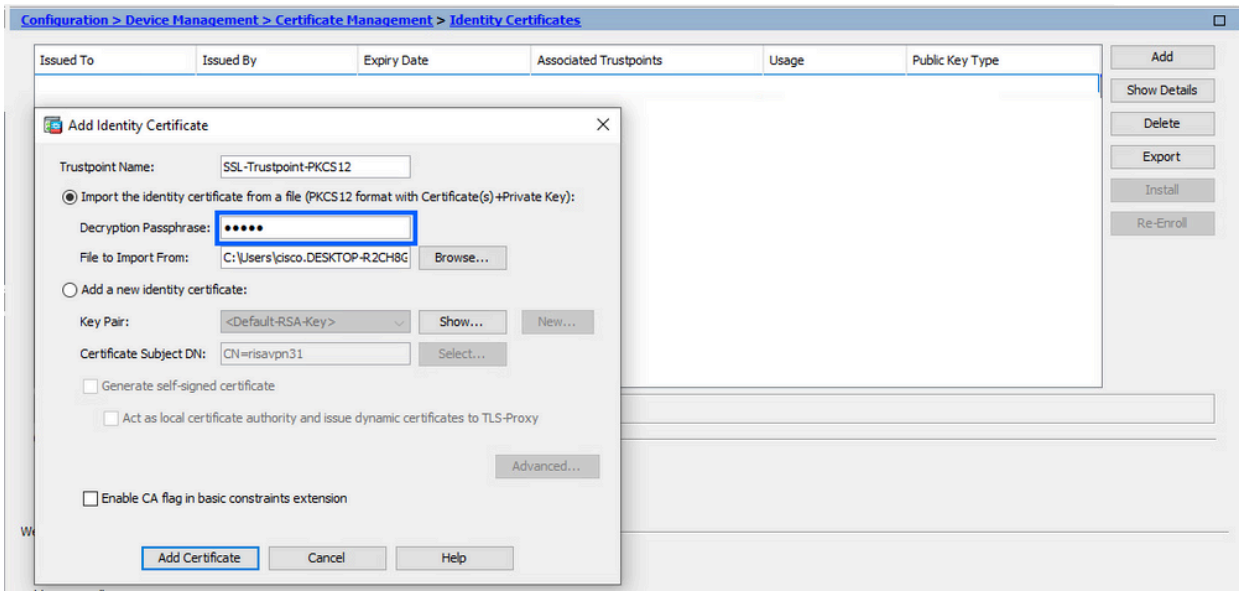
a. 导航到Configuration > Device Management > Certificate Management，然后选择Identity Certificates。
b. 单击 Add。
c. 指定新的信任点名称。



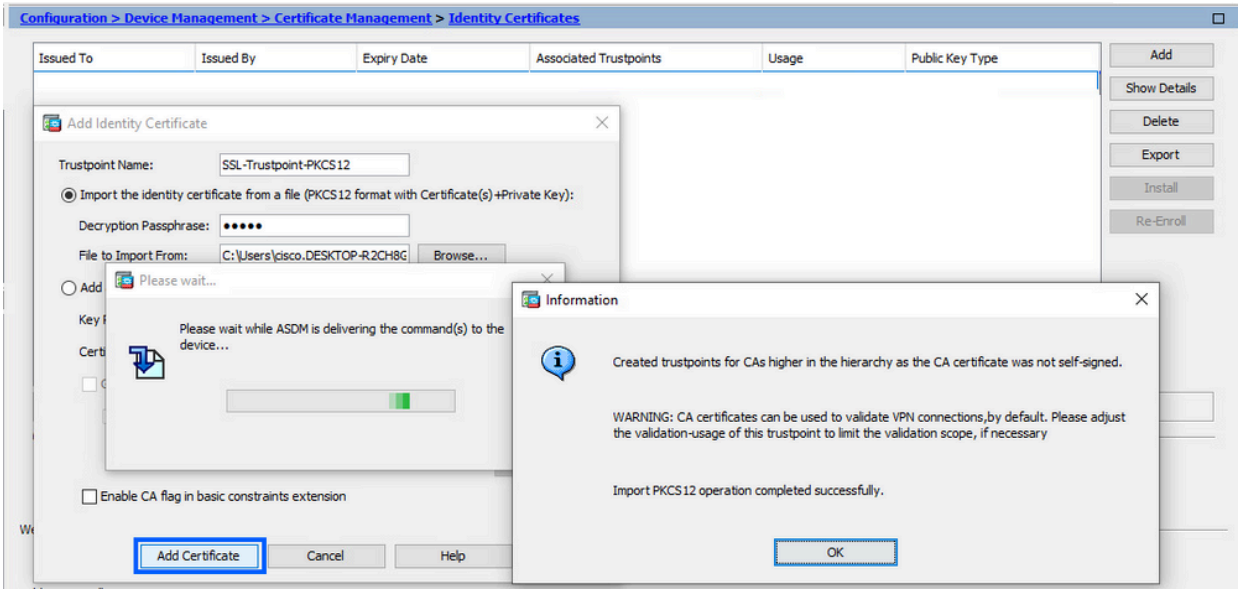
d. 单击Import The Identity Certificate from a File单选按钮。



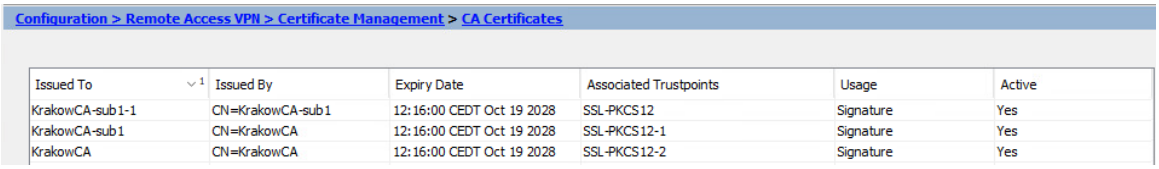
e. 输入用于创建 PKCS12 文件的密码。



f. 点击添加证书。



注意：导入带CA证书链的PKCS12时，ASDM会自动创建带有添加后缀的名称的上游CA信任点。



Configuration > Remote Access VPN > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
KrakowCA-sub1-1	CN=KrakowCA-sub1	12:16:00 CEDT Oct 19 2028	SSL-PKCS12	Signature	Yes
KrakowCA-sub1	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-1	Signature	Yes
KrakowCA	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-2	Signature	Yes

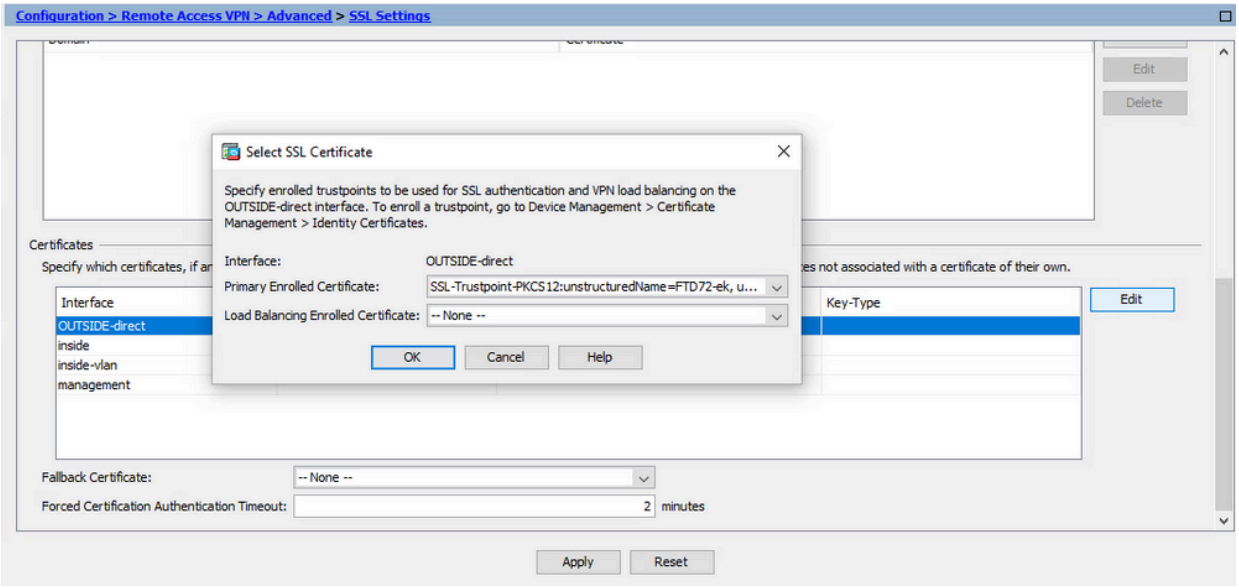
2. 使用ASDM将新证书绑定到接口

需要将ASA配置为使用新的身份证书，以便在指定接口上终止的WebVPN会话使用。

a. 导航到Configuration > Remote Access VPN > Advanced > SSL Settings。

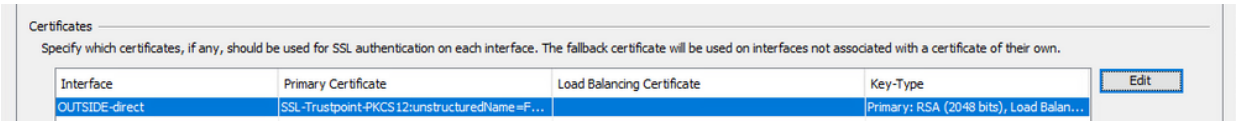
b. 在“证书”下，选择用于端接 WebVPN 会话的接口。在本例中，使用的是外部接口。单击 Edit。

c. 在“证书”下拉菜单中，选择新安装的证书。



d. Click OK.

e. 单击 Apply。



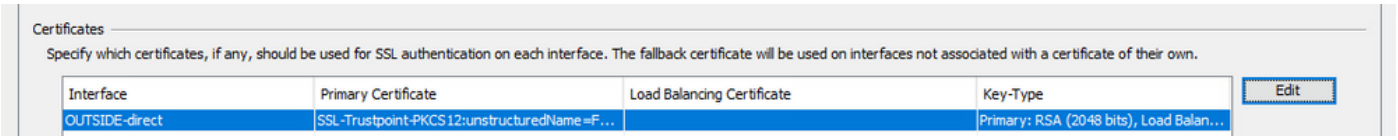
现在新的身份证书正在使用。

验证

使用以下步骤验证第三方供应商证书的安装是否成功以及是否用于SSL VPN连接。

通过 ASDM 查看已安装的证书

1. 导航至配置 > 远程接入 VPN > 证书管理，并选择身份证书。
2. 可能会显示第三方供应商颁发的身份证书。



故障排除

如果SSL证书安装失败，则将在CLI上收集此debug命令。

- debug crypto ca 14

常见问题解答

问：什么是PKCS12?
A.在加密中，PKCS12定义了一个存档文件格式，创建该格式以将多个加密对象存储为单个文件。它通常用于将私钥与其X.509证书捆绑在一起，或者用于捆绑信任链的所有成员。

问：什么是CSR?
A.在公钥基础设施(PKI)系统中，证书签名请求（也称为CSR或证书请求）是从申请人发送到公钥基础结构的注册机构以申请数字身份证书的消息。它通常包含可为其颁发证书的公钥、用于标识已签名证书的信息（例如主题中的域名）以及完整性保护（例如数字签名）。

问：PKCS12的密码在哪里？
A.当证书和密钥对导出到PKCS12文件时，在export命令中给出口令。 对于导入pkcs12文件，密码需要由所有者、从其他设备导出PKCS12的CA服务器或人员提供。

问：根和身份之间有什么区别？
答：在加密和计算机安全中，根证书是标识根证书颁发机构(CA)的公钥证书。根证书是自签名的（并且证书可以有多个信任路径，例如证书是否由交叉签名的根颁发），并构成基于X.509的公钥基础设施(PKI)的基础。公钥证书，也称为数字证书或身份证书，是一种用于证明公钥所有权的电子文档。证书包括有关密钥的信息、有关其所有者（称为主题）的标识的信息以及已验证证书内容的实体（称为颁发者）的数字签名。如果签名有效，并且检查证书的软件信任颁发者，那么它就可以使用该密钥与证书的使用者进行安全通信。

问：我安装了证书，为什么它不工作？
A.这可能有许多原因，例如：

1.已配置证书和信任点，但尚未将其绑定到应使用该证书和信任点的进程。 例如，要使用的信任点不会绑定到终止Anyconnect客户端的外部接口。

2.已安装PKCS12文件，但由于PKCS12文件中缺少中间CA证书而出现错误。如果客户端的中间CA证书为受信任的，但根CA证书不是受信任的，则无法验证整个证书链并将服务器身份证书报告为不受信任。

3.使用不正确的属性填充的证书可能会导致安装失败或客户端错误。例如，某些属性可能使用错误的格式进行编码。另一个原因是身份证书缺少主题备用名称(SAN)，或者用于访问服务器的域名没有作为SAN出现。

问：安装新证书是否需要维护窗口或导致停机时间？
A.安装新证书（身份或CA）不会带来干扰，不应导致停机或需要维护窗口。要启用新证书以用于现有的服务，需要更改并且可能需要更改请求/维护窗口。

问：添加或更改证书能否断开连接的用户？
答：不，当前连接的用户保持连接。证书用于连接建立。用户重新连接后，将使用新证书。

问：如何使用通配符创建CSR?或主题备用名称(SAN)?
A.目前，ASA/FTD无法使用通配符创建CSR；但是，此过程可以通过OpenSSL完成。要生成CSR和ID密钥，可以运行以下命令：

```
openssl genrsa -out id.key 2048
```

openssl req -out id.csr -key id.key -new

使用完全限定域名(FQDN)属性配置信任点时，ASA/FTD创建的CSR包含具有该值的SAN。当CA签署CSR时，可以添加更多SAN属性，也可以使用OpenSSL创建CSR

问：证书更换是否立即生效？

A.新服务器身份证书仅用于新连接。新证书可在更改后立即使用，但实际上用于新连接。

问：如何检查安装是否有效？

A.用于验证的CLI命令：show crypto ca cert <trustpointname>

问：如何从身份证书、CA证书和私钥生成PKCS12?

A.PKCS12可以通过OpenSSL使用以下命令创建：

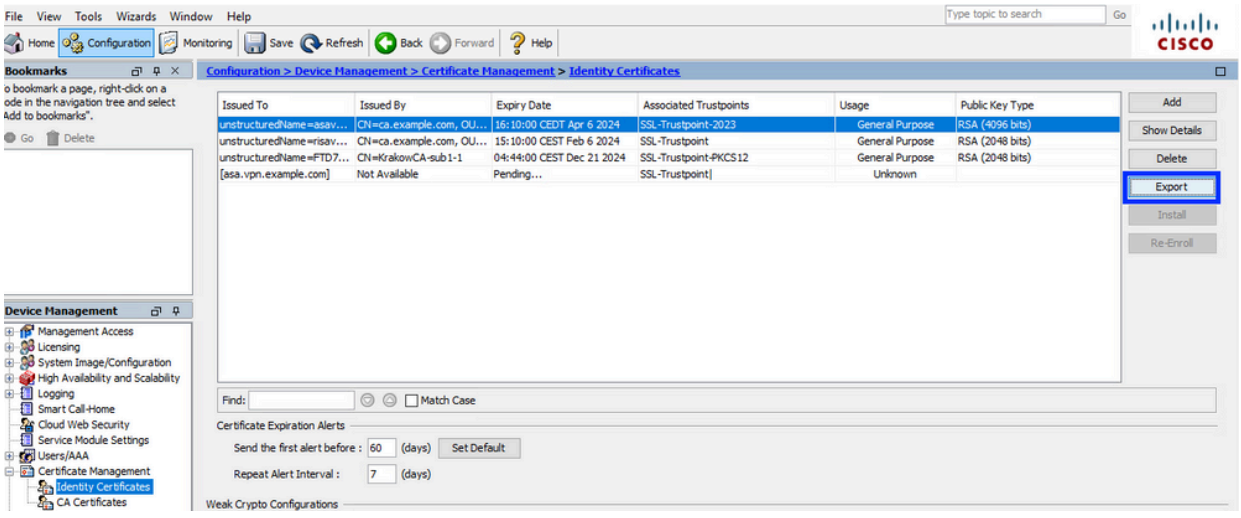
openssl pkcs12 -export -out p12.pfx -inkey id.key -in id.crt -certfile ca.crt

问：如何导出证书以将其安装在新的ASA中？

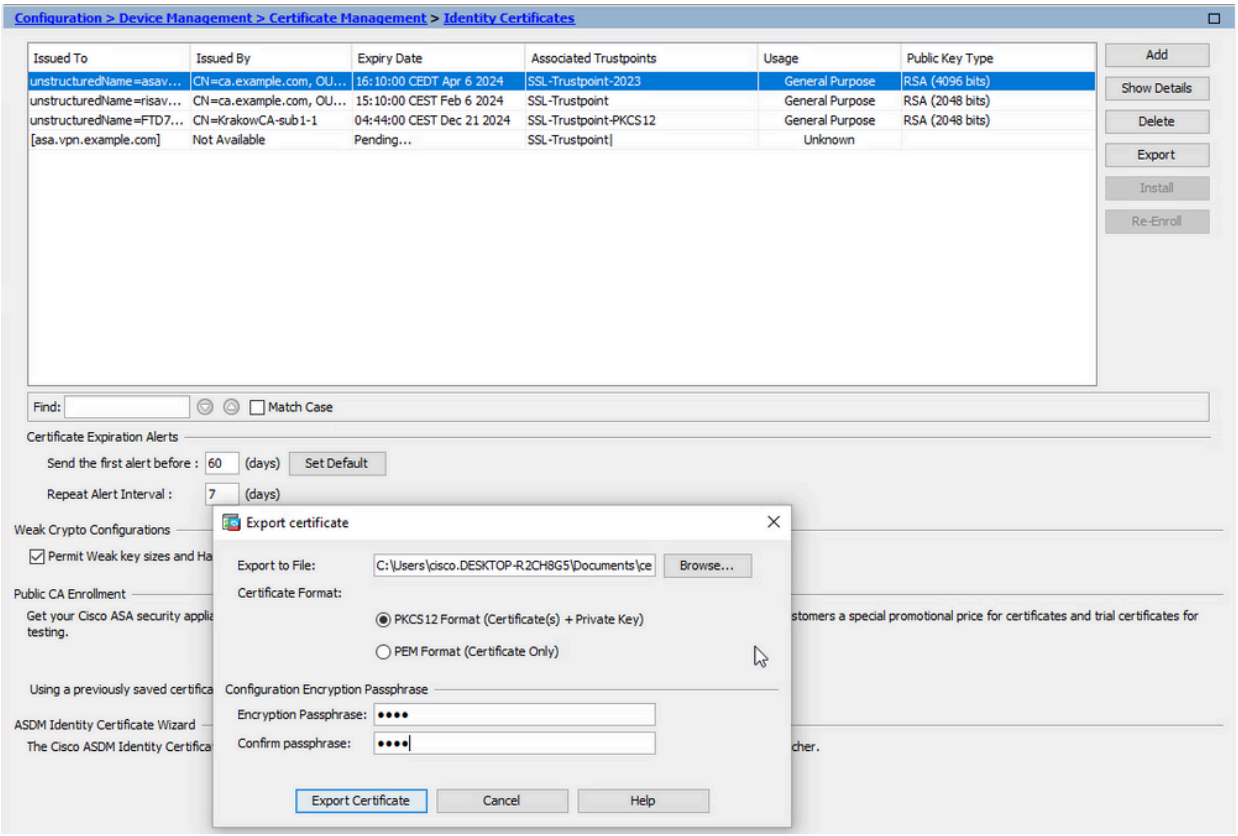
A.

- 使用CLI：使用命令crypto ca export <trustpointname> pkcs12 <password>
- 使用ASDM:

a. 导航到Configuration > Device Management > Certificate Management > Identity Certificates，然后选择Identity Certificate。单击Export。



b. 选择导出文件的位置，指定导出密码，然后点击Export Certificate。



导出的证书可以在计算机磁盘上。请注意安全位置的口令，否则文件将毫无用处。

问：如果使用ECDSA密钥，则SSL证书生成过程是否不同？
答：配置的唯一区别是密钥对生成步骤，在该步骤中可生成ECDSA密钥对，而不是RSA密钥对。其余步骤保持不变。

问：是否始终需要生成新的密钥对？
答：密钥对生成步骤是可选的。可以使用现有的密钥对，如果是PKCS12，则密钥对将与证书一起导入。有关各自的注册/重新注册类型，请参阅“选择密钥对名称”部分。

问：为新的身份证书生成新的密钥对是否安全？
答：只要使用新的密钥对名称，该过程就是安全的。在这种情况下，旧密钥对不会更改。

问：在更换防火墙时（如RMA），是否需要再次生成密钥？
A.新防火墙的设计没有在旧防火墙上提供密钥对。
运行配置的备份不包含密钥对。
使用ASDM完成的完全备份可以包含密钥对。
可以在身份证书发生故障之前，通过ASDM或CLI从ASA导出身份证书。
如果出现故障切换对，则使用write standby命令将证书和密钥对同步到备用设备。如果替换了故障切换对中的一个节点，则配置基本故障切换并将配置推送到新设备就足够了。
如果设备丢失了密钥对，并且没有备份，则需要使用新设备上存在的密钥对来签署新证书。

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）。