

上传RV32x系列路由器证书的解决方法

摘要

数字证书通过证书的指定主题对公钥的所有权进行认证。这允许依赖方依赖由私钥所作的签名或断言，该私钥对应于经认证的公钥。路由器可以生成自签名证书，即由网络管理员创建的证书。它还可以向证书颁发机构(CA)发出申请数字身份证书的请求。从第三方应用获得合法证书非常重要。

CA通过两种方式签署证书：

1. CA使用私钥对证书签名。
2. CA使用RV320/RV325生成的CSR签名证书。

RV320和RV325仅支持.pem格式证书。对于这两种情况，您都应从证书颁发机构获取.pem格式证书。如果您获得其他格式证书，则需要自行转换格式或从CA再次请求.pem格式证书。

大多数商业证书供应商使用中间证书。由于中间证书由受信任根CA颁发，因此中间证书颁发的任何证书都继承受信任根的信任，如信任的证书链。

本指南介绍如何导入由RV320/RV325上的中级证书颁发机构颁发的证书。

确定日期

2017年2月24日

解决日期

不适用

受影响的产品

RV320/RV325	1.1.1.06 及更高版本

使用私钥进行证书签名

在本例中，我们假设您从第三方中间CA获得了RV320.pem。文件具有以下内容：私钥、证书、根CA证书、中间CA证书。

注意：从中间CA获取多个文件（而不是只获取一个文件）是可选的。但是，您可以从几个文件中找到以上四个部分。

检查CA证书文件是否同时包含根CA证书和中间证书。RV320/RV325要求在CA捆绑包中按一定顺序提供中间证书和根证书，首先提供根证书，然后提供中间证书。其次，您需要将

RV320/RV325证书和私钥合并到一个文件中。

注意：任何文本编辑器都可用于打开和编辑文件。必须确保任何额外的空行、空格或回车都不会使计划按预期进行。

组合证书

步骤1.打开RV320.pem，复制第二个证书（根证书）和第三个证书（中间证书），包括开始/结束消息。

注意：在本例中，突出显示的文本字符串是根证书。



```
RV320 - Notepad
File Edit Format View Help
Bag Attributes
  localKeyID: 01 00 00 00
  friendlyName: {XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXX}
  Microsoft CSP Name: Microsoft EnhNACed
Cryptographic Provider v1.0
Key Attributes
  X509v3 Key Usage: 10
  -----BEGIN PRIVATE KEY-----
MIIEVQIBADNABgkqhkiG9w0BAQEFAASCBCkCWJgSjAgEAAoIBAQCjE0q
Te
.....

Sv3RH/fSHuP
+NayfgYHIpXQDCobJF1LhY0UzD/cgz7f7BdkzC0fqPTEJA90=
-----END PRIVATE KEY-----
Bag Attributes
  localKeyID: 01 00 00 00
  friendlyName: StartCom PFX Certificate
subject=/description=XXXXXXXX/C=US/ST=XXXX/L=Xxxxx/O=XX
XX/CN=xxx.xxx.net/emailAddress=xx.xx@xx.com
issuer=/C=IL/O=StartCom Ltd./OU=S4cure Digital
Certificate Signing/CN=StartCom Class 2 Primary
Intermediate S4rver CA
  -----BEGIN CERTIFICATE-----
MIIG2jCCBCKgAwIBAgINAgBbMA0GCsqGSib3DQEBBQUAMIGNNQswCQY
.....

Ml4iyDx3GLii7gKZOFaw4unJvcoOtw0387AMGb//IfNIwqFNpuXtuUq
0Esc
-----END CERTIFICATE-----
Bag Attributes
  friendlyName: StartCom Certification Authority
subject=/C=IL/O=StartCom Ltd./OU=S4cure Digital
Certificate Signing/CN=StartCom Certification Authority
issuer=/C=IL/O=StartCom Ltd./OU=S4cure Digital
Certificate Signing/CN=StartCom Certification Authority
  -----BEGIN CERTIFICATE-----
MIIHytCCBbGgAwIBAgIBATNABgkqhkiG9w0BAQUFADB9MQswCQYDVQ
.....

Bj6y6koQ0djQK/w/7HA/lwr
+bMEkxN9P/F1UqqNNGqz9IgoGAg38corogI4=
-----END CERTIFICATE-----
```

注意：在本例中，突出显示的文本字符串是中间证书。

```
RV320 - Notepad
File Edit Format View Help
-----END PRIVATE KEY-----
Bag Attributes
  localkeyID: 01 00 00 00
  friendLiName: StartCom PFX Certificate
subject=/description=XXXXXX/C=US/ST=XXXX/L=XXXX/O=XX
XX/CN=xxx.xxx.net/emailAddress=xx.xx@xx.com
issuer=/C=IL/O=StartCom Ltd./OU=S4cure Digital
Certificate Signing/CN=StartCom Class 2 Primary
Intermediate S4rver CA
-----BEGIN CERTIFICATE-----
MIIG2jCCBCKgAwIBAgINAgBbMA0GCSqGSIB3DQEBBQUAMIGNNQswCQY
.....

M14iyDX3GLii7gKZOFaw4unJvco0tw0387AMGb//IfNIWqFNpuxtuUq
0Esc
-----END CERTIFICATE-----
Bag Attributes
  friendLiName: StartCom Certification Authority
subject=/C=IL/O=StartCom Ltd./OU=S4cure Digital
Certificate Signing/CN=StartCom Certification Authority
issuer=/C=IL/O=StartCom Ltd./OU=S4cure Digital
Certificate Signing/CN=StartCom Certification Authority
-----BEGIN CERTIFICATE-----
MIIHytCCBbGgAwIBAgIBATNABgkqhkiG9w0BAQUFADB9MQswCQYDVQ
.....

Bj6y6koQ0djQK/w/7HA/lwr
+bMEkXN9P/FlUQqNNGqz9IgOgA38corog14=
-----END CERTIFICATE-----
Bag Attributes
subject=/C=IL/O=StartCom Ltd./OU=S4cure Digital
Certificate Signing/CN=StartCom Class 2 Primary
Intermediate S4rver CA
issuer=/C=IL/O=StartCom Ltd./OU=S4cure Digital
Certificate Signing/CN=StartCom Certification Authority
-----BEGIN CERTIFICATE-----
MIIGNDCCBBygAwIBAgIBGjNABgkqhkiG9w0BAQUFADB9MQswCQYDVQQ
.....

WZP8P3PXLrQsldiL98l/ydrHIEH9LMF/TtNGCbnkqXBP7dcgqhykquA
zx/Q=
-----END CERTIFICATE-----
```

步骤2.将内容粘贴到新文件中，并将其另存为CA.pem。

```
CA.pem - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE-----
MIIHytCCBbGgAwIBAgIBATNABgkqhkiG9w0BAQUFADB9MQswCQYDVQ
.....

Bj6y6koQ0djQK/W/7HA/lwr+bMEkXN9P/FlUQqNNGqz9IgOgA38corog14=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIGNDCCBBygAwIBAgIBGjNABgkqhkiG9w0BAQUFADB9MQswCQYDVQQ
.....

WZP8P3PXLrQsldiL98l/ydrHIEH9LMF/TtNGCbnkqXBP7dcgqhykquA
zx/Q=
-----END CERTIFICATE-----
```

步骤3.打开RV320.pem，并复制私钥部分和第一个证书，包括开始/结束消息。

注意：在以下示例中，突出显示的文本字符串是私钥部分。

```
RV320 - Notepad
File Edit Format View Help
Bag Attributes
  localKeyID: 01 00 00 00
  friendlyName: {XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXX}
  Microsoft CSP Name: Microsoft EnhNaced
Cryptographic Provider v1.0
Key Attributes
  X509v3 Key Usage: 10
-----BEGIN PRIVATE KEY-----
MIIEvQIBADNABgkqhkiG9w0BAQEFAASCBCwJgSjAgEAAoIBAQCjEOq
Te
.....
SV3RH/fSHuP
+NAYfgyHixQDCobJF1LhY0uzD/cgz7f7BdkzC0fqPTEJA90=
-----END PRIVATE KEY-----
```

注意：在以下示例中，突出显示的文本字符串是第一个证书。

```
RV320 - Notepad
File Edit Format View Help
Bag Attributes
  localKeyID: 01 00 00 00
  friendlyName: {XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXX}
  Microsoft CSP Name: Microsoft EnhNaced
Cryptographic Provider v1.0
Key Attributes
  X509v3 Key Usage: 10
-----BEGIN PRIVATE KEY-----
MIIEvQIBADNABgkqhkiG9w0BAQEFAASCBCwJgSjAgEAAoIBAQCjEOq
Te
.....
SV3RH/fSHuP
+NAYfgyHixQDCobJF1LhY0uzD/cgz7f7BdkzC0fqPTEJA90=
-----END PRIVATE KEY-----
Bag Attributes
  localKeyID: 01 00 00 00
  friendlyName: StartCom PFX Certificate
subject=/description=XXXXXX/C=US/ST=XXXX/L=XXXX/O=XX
XX/CN=xxx.xxx.net/emailAddress=xx.xx@xx.com
issuer=/C=IL/O=StartCom Ltd./OU=S4cure Digital
Certificate Signing/CN=StartCom Class 2 Primary
Intermediate S4rver CA
-----BEGIN CERTIFICATE-----
MIIG2jCCBCKgAwIBAgINAgBbMA0GC5qGS1b3DQEIBBQUAMIGNNQswCQY
.....
M14iYDx3GLi17gkZ0FAw4unJvco0tw0387AMGb//IfNIwqFNpuxtUuq
0Esc
-----END CERTIFICATE-----
```

步骤4.将内容粘贴到新文件中，并将其另存为cer_plus_private.pem

```

cer_plus_private.pem - Notepad
File Edit Format View Help
-----BEGIN PRIVATE KEY-----
MIIEvQIBADNABgkqhkiG9w0BAQEFAASCBCkCWJgSjAgEAAoIBAQCjEOqTe
.....
Sv3RH/fSHuP+NAYfgYHipxQDcObJF1LhY0UzD/cgz7f7BdKzC0fqPTEJA90=
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIG2jCCBcKgAwIBAgINAgBbMA0GCSqGSIb3DQEBBQUAMIGNNQswCQY
.....
Ml4iYDx3GLii7gKZOFaw4unJvcoOtw0387AMGb//IfNIWqFNpuXtuUq0Esc
-----END CERTIFICATE-----

```

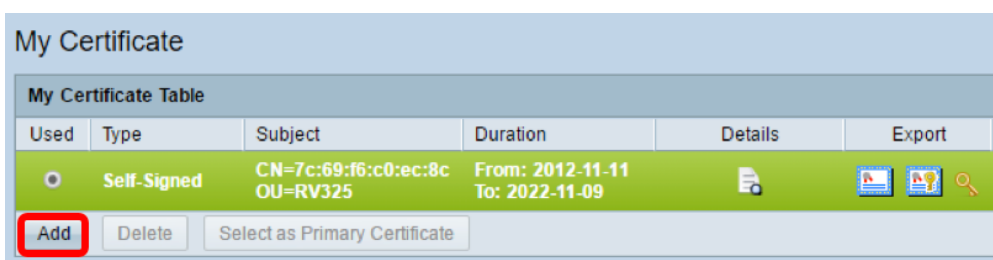
注意：如果RV320/RV325固件版本低于1.1.1.06，请确保文件末尾有两个线路馈送 (cerplusprivate.pem)。在1.1.1.06之后的固件中，您无需再添加两个线路源。在本示例中，仅为演示目的而显示证书的缩短版本。

导入 CA.pem 和 cer_plus_private.pem 到RV320/RV325

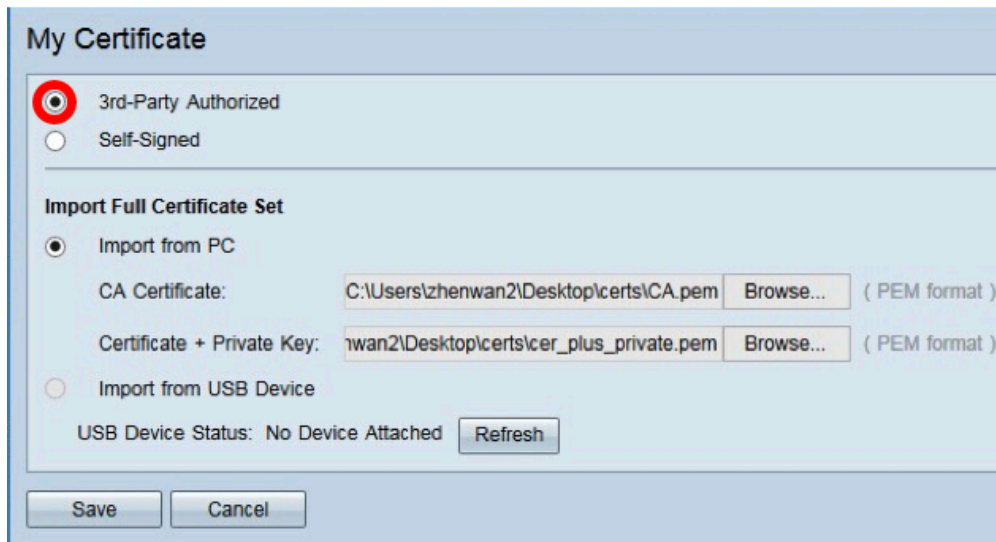
步骤1. 登录到RV320或RV325的基于Web的实用程序，然后选择**Certificate Management > My Certificate**。



步骤2. 单击Add导入证书。



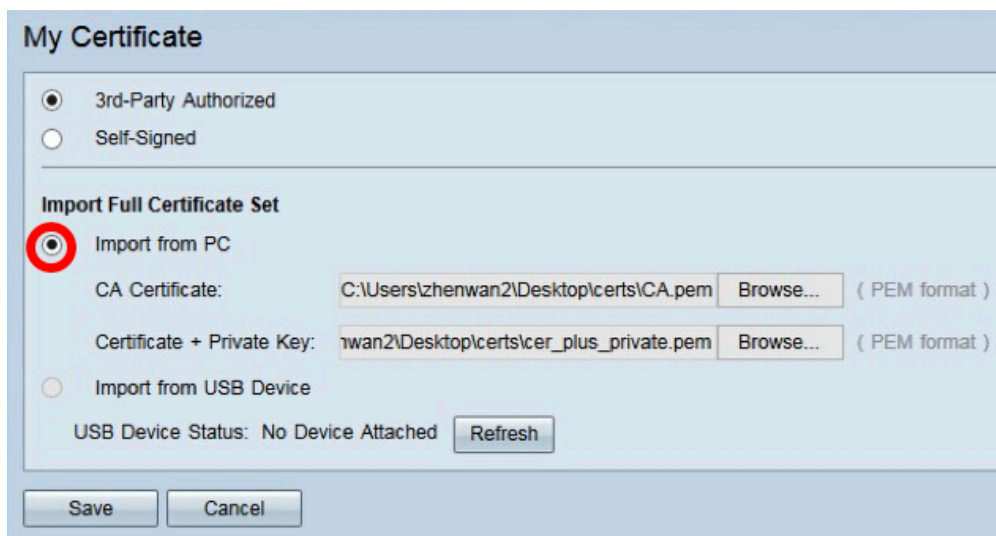
步骤3. 单击“第三方授权”单选按钮导入证书。



步骤4.在“导入完整证书集”区域，单击单选按钮以选择保存的证书的源。选项有：

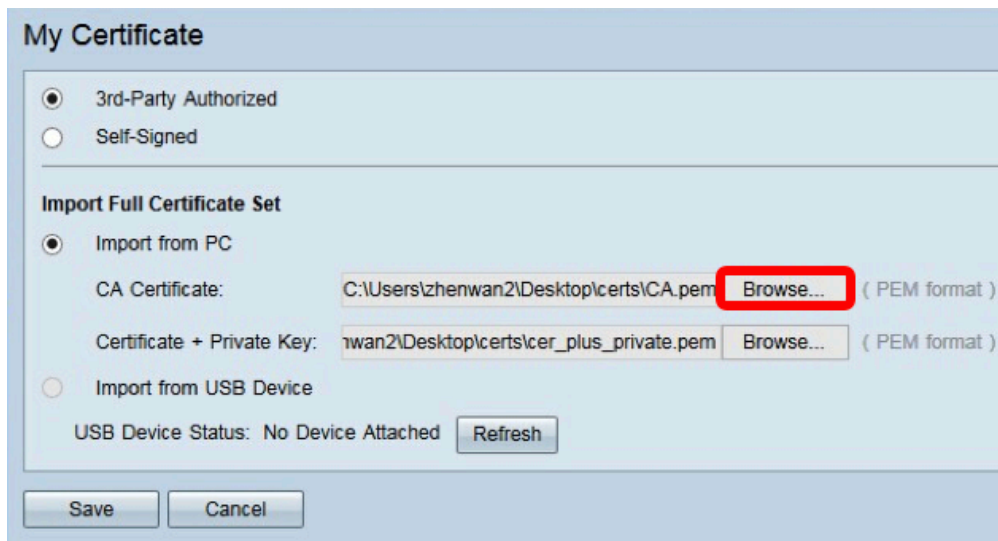
- 从PC导入 — 如果在计算机上找到文件，请选择此选项。
- 从USB导入 — 选择此选项可从闪存驱动器导入文件。

注意：在本例中，选择从PC导入。



步骤5.在“CA证书”区域，单击“浏览……”并找到CA.pem。文件。

注意：如果运行的固件版本高于1.1.0.6，请点击“选择”按钮并找到所需的文件。

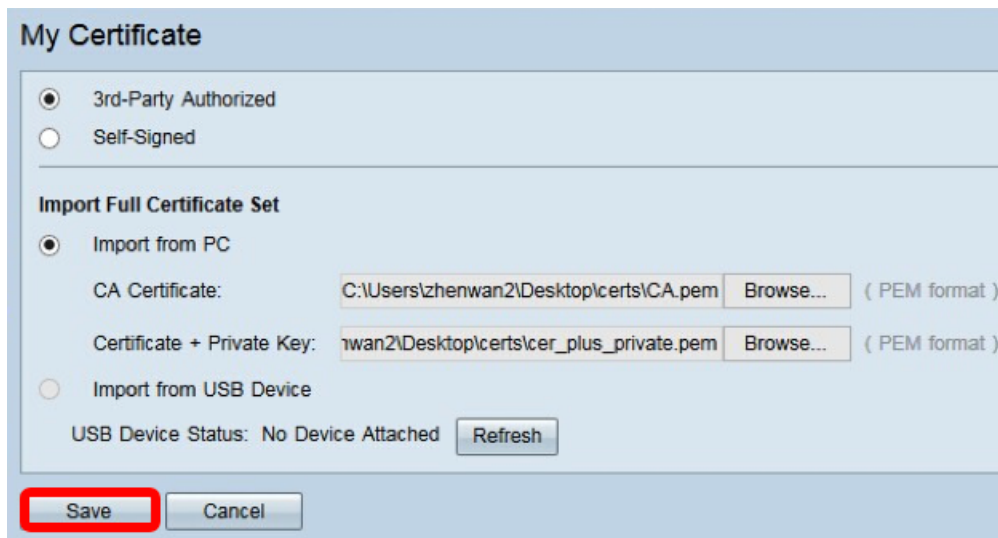


步骤6.在“证书+私钥”区域，单击“浏览……”并找到cer_plus_private.pem文件。

注意：如果运行的固件版本高于1.1.0.6，请点击“选择”按钮并找到所需的文件。

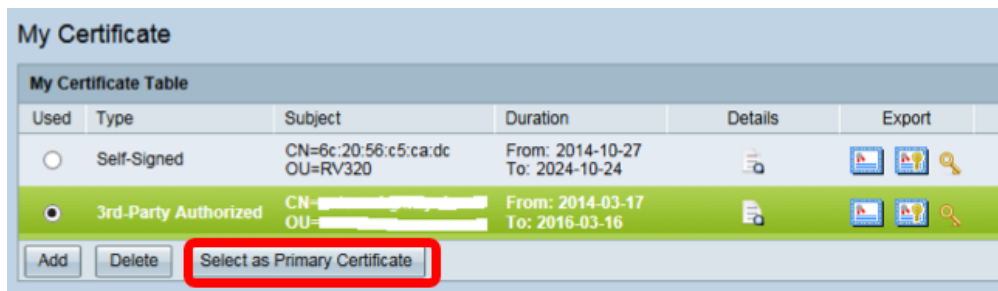


步骤7.单击“保存”。



证书已成功导入。现在，它可用于HTTPS访问、SSL VPN或IPSec VPN。

第8步。（可选）要将证书用于HTTPS或SSL VPN，请点击证书的单选按钮，然后点击 **Select as Primary Certificate** 按钮。

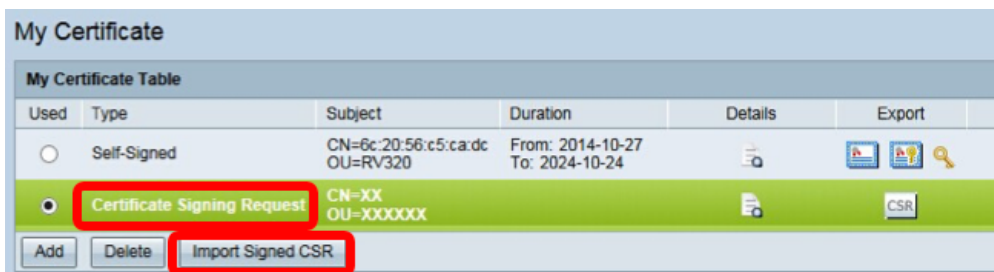


您现在应该已成功导入证书。

使用CSR的证书签名

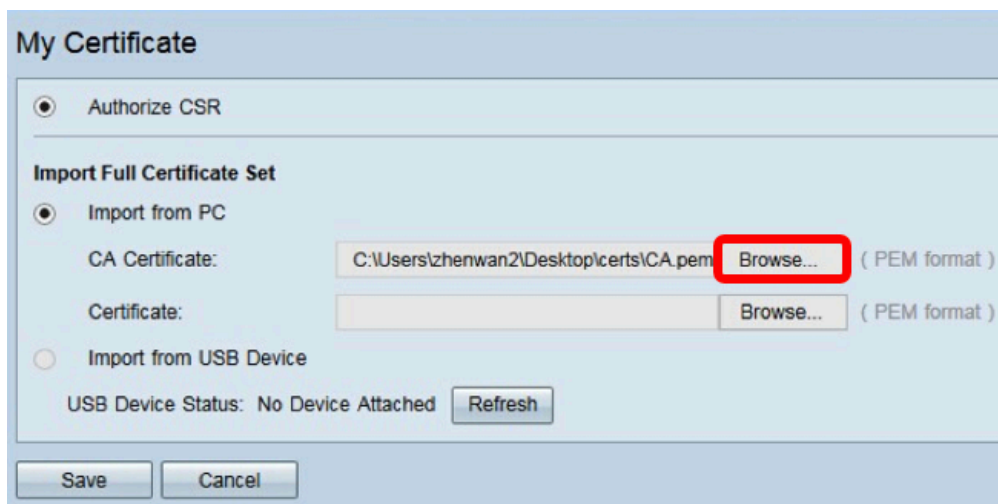
步骤1.在RV320/RV325上生成证书签名请求(CSR)。若要了解如何生成CSR，请单击[此处](#)。

步骤2.要导入证书，请选择Certificate Signing Request(证书签名请求),然后单击Import Signed CSR(导入签名的CSR)。

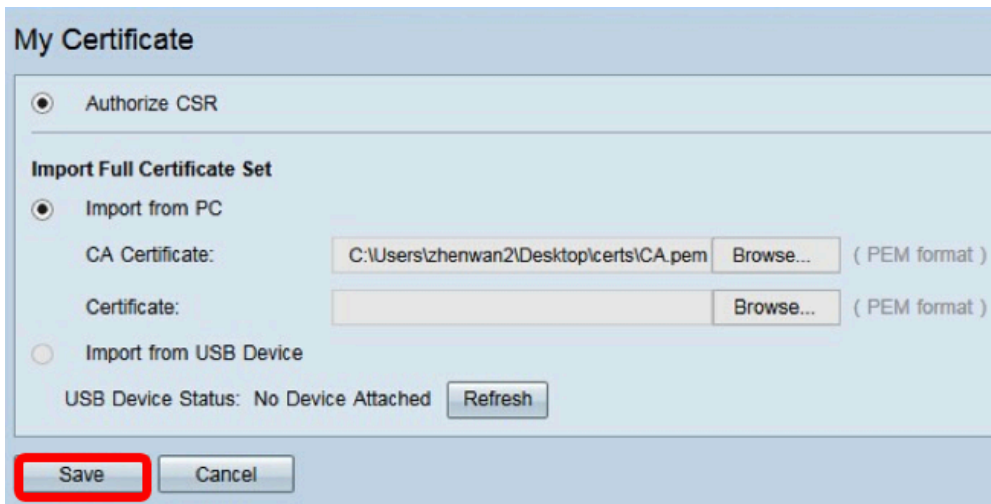


步骤3.单击Browse...并选择CA证书文件。这包含根CA + 中间CA证书。

注意：在本例中，由于证书是使用CSR生成的，因此不需要私钥。



步骤4.单击“保存”。



您现在应该已使用CSR成功上传证书。

Appendix:

RV320.pem的内容

包属性

localKeyId:01 00 00 00

friendlyName:{{XXXXXXXX-XXXX-XXXX-XXXX-XXXX-XXXXXXXX}}

Microsoft CSP名称 : Microsoft加强版加密提供程序v1.0

关键属性

X509v3密钥用法 : 10

— 开始私钥 —

```
MIIEvQIBADNABgkqhkiG9w0BAQEFAASCBCcWJgSjAgEAAoIBAQCjEOqTe
```

.....

```
Sv3RH/fSHuP+NAYfgYHipxQDcObJF1LhY0UzD/cgz7f7BdKzC0fqPTEJA90=
```

— 最终私钥 —

包属性

localKeyId:01 00 00 00

friendlyName:StartCom PFX证书

subject=/description=XXXXX/C=US/ST=XXXX/L=Xxxx/O=XX

XX/CN=xxx.xxx.net/emailAddress=xx.xx@xx.com

issuer=/C=IL/O=StartCom Ltd./OU=S4cure数字证书签名/CN=StartCom 2类主要中间S4rver
CA

— 开始证书 —

MIIG2jCCBcKgAwIBAgINA9BbMA0GCSqGSIb3DQEEBQUAMINQswCQY

.....

MI4iYDx3GLii7gKZOF4W4unJvcoOtw0387AMGb//IfNIWqFNpuXtuUq0Esc

— 最终证书 —

包属性

friendlyName:StartCom认证机构

subject=/C=IL/O=StartCom Ltd./OU=S4cure数字证书签名/CN=StartCom证书颁发机构

issuer=/C=IL/O=StartCom Ltd./OU=S4cure数字证书签名/CN=StartCom证书颁发机构

— 开始证书 —

MIIHyTCCBbGgAwIBAgIBATNABgkqhkiG9w0BAQFADB9MQswCQYDVQ

.....

Bj6y6koQOdjQK/W/7HA/lwr+bMEkXN9P/FIUQqNNGqz9lgOgA38corog14=

— 最终证书 —

包属性

subject=/C=IL/O=StartCom Ltd./OU=S4cure数字证书签名/CN=StartCom 2类主要中间S4rver
CA

issuer=/C=IL/O=StartCom Ltd./OU=S4cure数字证书签名/CN=StartCom证书颁发机构

— 开始证书 —

MIIGNDCCBBygAwIBAgIBGjNABgkqhkiG9w0BAQFADB9MQswCQYDVQ

.....

WZP8P3PXLrQsldiL98l/ydrHIEH9LMF/TtNGCbnkqXBP7dgcgqhykguAzx/Q=

— 最终证书 —