

Soluzione per caricare il certificato del router serie RV32x

Riepilogo

Un certificato digitale certifica la proprietà di una chiave pubblica da parte del soggetto specificato del certificato. In questo modo le relying party possono dipendere da firme o asserzioni effettuate dalla chiave privata corrispondente alla chiave pubblica certificata. Un router può generare un certificato autofirmato, ovvero un certificato creato da un amministratore di rete. Può inoltre inviare richieste alle Autorità di certificazione (CA) per richiedere un certificato di identità digitale. È importante disporre di certificati legittimi provenienti da applicazioni di terze parti.

I certificati possono essere firmati da CA in due modi:

1. La CA firma il certificato con chiavi private.
2. CA firma i certificati utilizzando CSR generato da RV320/RV325.

RV320 e RV325 supportano solo certificati in formato .pem. In entrambi i casi è necessario ottenere certificati in formato .pem da Autorità di certificazione. Se si ottiene un altro certificato di formato, è necessario convertire il formato personalmente o richiedere nuovamente il certificato di formato .pem dalla CA.

La maggior parte dei fornitori di certificati commerciali utilizza certificati intermedi. Poiché il certificato intermedio viene rilasciato dalla CA radice attendibile, tutti i certificati emessi dal certificato intermedio ereditano l'attendibilità della radice attendibile, come una catena di certificati.

In questa guida viene descritto come importare i certificati rilasciati da Intermediate Certificate Authority su RV320/RV325.

Data identificazione

24 febbraio 2017

Data risoluzione

N/D

Prodotti interessati

RV320/RV325	1.1.1.06 e successive

Firma del certificato tramite chiavi private

Nell'esempio, si presume che la CA intermedia di terze parti abbia fornito un file RV320.pem. Il contenuto del file è il seguente: chiave privata, certificato, certificato CA radice, certificato CA intermedio.

Nota: Il recupero di più file da una CA intermedia anziché di un solo file è facoltativo. Ma si possono trovare più di quattro parti dai diversi file.

Verificare se il file del certificato CA contiene sia il certificato CA radice che il certificato intermedio. RV320/RV325 richiede il certificato intermedio e il certificato radice in un determinato ordine nel bundle CA, prima il certificato radice e poi il certificato intermedio. In secondo luogo, è necessario combinare il certificato RV320/RV325 e la chiave privata in un unico file.

Nota: È possibile utilizzare qualsiasi editor di testo per aprire e modificare i file. È importante assicurarsi che eventuali righe vuote, spazi o ritorni a capo aggiuntivi non facciano andare il piano come previsto.

Combinazione dei certificati

Passaggio 1. Aprire RV320.pem, copiare il secondo certificato (certificato radice) e il terzo certificato (certificato intermedio), incluso il messaggio di inizio/fine.

Nota: In questo esempio, la stringa di evidenziazione del testo è il certificato radice.

```
RV320 - Notepad
File Edit Format View Help
Bag Attributes
  localKeyID: 01 00 00 00
  friendlyName: {XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXX}
  Microsoft CSP Name: Microsoft Enhanced
Cryptographic Provider v1.0
Key Attributes
  X509v3 Key Usage: 10
-----BEGIN PRIVATE KEY-----
MIEVQIBADNABgkqhkiG9w0BAQEFAASCBCkCWJgSjAgEAAoIBAQCjEOq
Te
.....

Sv3RH/fSHuP
+NayfgYHixQDcObJF1Lhy0uzD/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
.....

M14iyDX3GLii7gKZOFaw4unJvcoOtw0387AMGb//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/FlUqqNNGqz9IgoA38corog14=
-----END CERTIFICATE-----
```

Nota: In questo esempio, la stringa di testo evidenziata è il certificato intermedio.

```
RV320 - Notepad
File Edit Format View Help
-----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-----
MIIG2jCCBCKgAwIBAgINAgBbMA0GCSqGSIB3DQEBBQUAMIGNNQswCQY
.....

M14iyDX3GLii7gKZOFaw4unJvco0tw0387AMGb//IfNIWqFNpuxtuUq
OEsc
-----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/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-----
MIIGNDCCBBygAwIBAgIBGjNABgkqhkiG9w0BAQUFADB9MQswCQYDVQ
.....

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

Passaggio 2. Incollare il contenuto in un nuovo file e salvarlo come CA.pem.

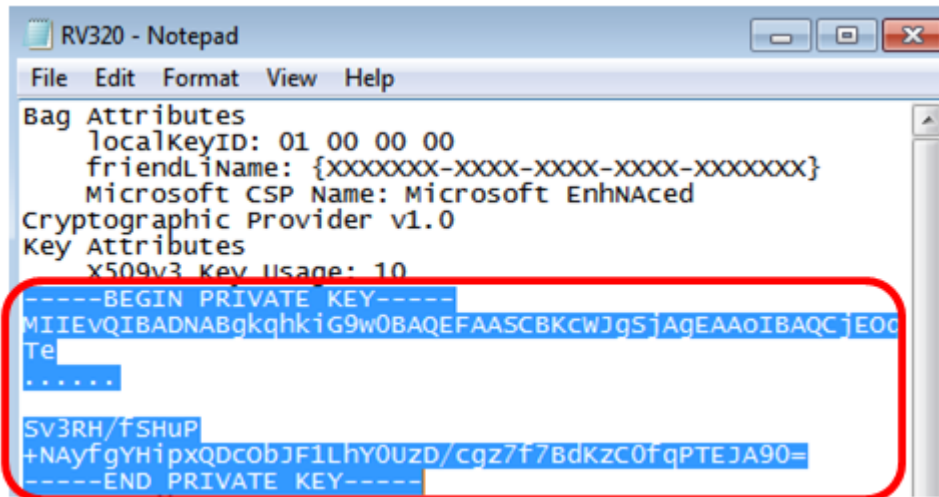
```
CA.pem - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE-----
MIIHytCCBbGgAwIBAgIBATNABgkqhkiG9w0BAQUFADB9MQswCQYDVQ
.....

Bj6y6koQ0djQK/W/7HA/lwr+bMEkXN9P/FlUQqNNGqz9IgOgA38corog14=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIGNDCCBBygAwIBAgIBGjNABgkqhkiG9w0BAQUFADB9MQswCQYDVQ
.....

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

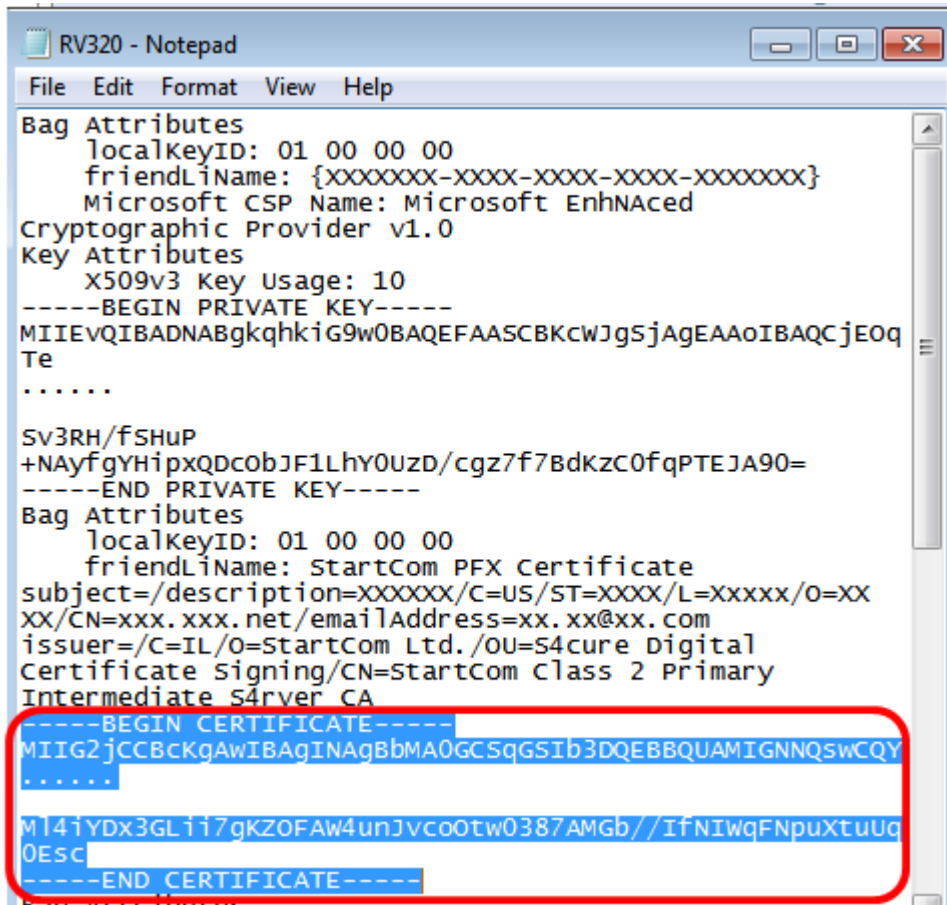
Passaggio 3. Aprire il file RV320.pem e copiare la sezione della chiave privata e il primo certificato, incluso il messaggio di inizio/fine.

Nota: Nell'esempio seguente, la stringa di testo evidenziata è la sezione della chiave privata.



```
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
+NAYfgyHipxQDCobJF1Lhy0uzD/cgz7f7BdkZc0fqpTEJA90=
-----END PRIVATE KEY-----
```

Nota: Nell'esempio seguente, la stringa di testo evidenziata è il primo certificato.



```
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
+NAYfgyHipxQDCobJF1Lhy0uzD/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-----
MIIG2jCCBCKgAwIBAgINAgBbMA0GCSqGSIb3DQEBBQUAMIGNNQswCQY
.....
M141YDx3GL117gKZOFaw4unJvco0tw0387AMGb//IfNIwqFNpuXtuUq
0Esc
-----END CERTIFICATE-----
```

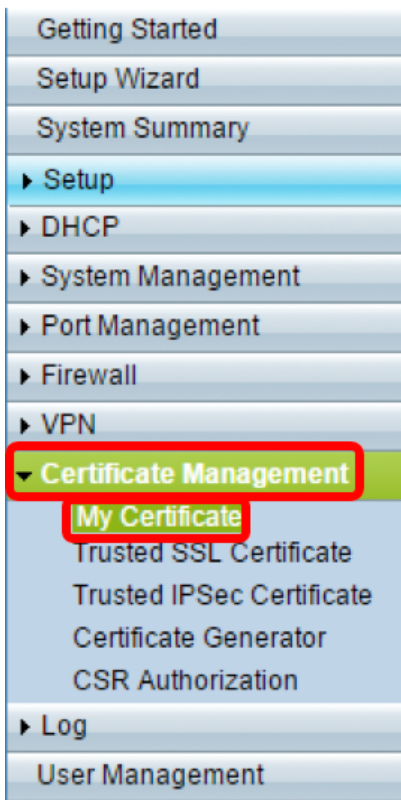
Passaggio 4. Incollare il contenuto in un nuovo file e salvarlo come cer_plus_private.pem

```
cer_plus_private.pem - Notepad
File Edit Format View Help
-----BEGIN PRIVATE KEY-----
MIIEvQIBADNABgkqhkiG9w0BAQEFAASCBCkCWJgSjAgEAAoIBAQCjEOqTe
.....
Sv3RH/fSHuP+NAYfgYHipxQDcObJF1LhY0UzD/cgz7f7BdKzC0fqPTEJA90=
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIG2jCCBcKgAwIBAgINAgBbMA0GCSqGSIb3DQEBBQUAMIGNNQswCQY
.....
Ml4iYDx3GLii7gKZOFaw4unJvco0tw0387AMGb//IfNIWqFNpuXtuUq0Esc
-----END CERTIFICATE-----
```

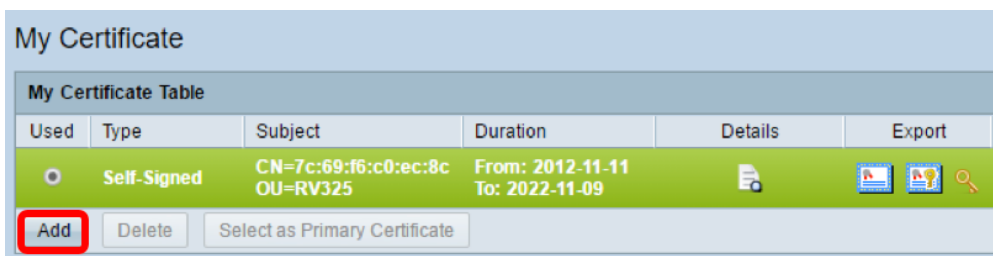
Nota: Se la versione del firmware RV320/RV325 è inferiore a 1.1.1.06, assicurarsi che alla fine del file siano presenti due avanzamenti di riga (cer_plus_private.pem). Nel firmware dopo la versione 1.1.1.06, non è necessario aggiungere altri due avanzamenti di linea. In questo esempio, una versione abbreviata del certificato viene visualizzata solo a scopo dimostrativo.

Importa CA.pem e cer_plus_private.pem in RV320/RV325

Passaggio 1. Accedere all'utilità basata sul Web di RV320 o RV325 e scegliere **Gestione certificati > Certificato**.



Passaggio 2. Fare clic su **Aggiungi** per importare il certificato.



Passaggio 3. Fare clic sul pulsante di opzione *Autorizzato da terze parti* per importare il certificato.

My Certificate

3rd-Party Authorized
 Self-Signed

Import Full Certificate Set

Import from PC

CA Certificate: C:\Users\zhenwan2\Desktop\certs\CA.pem Browse... (PEM format)

Certificate + Private Key: \wan2\Desktop\certs\cer_plus_private.pem Browse... (PEM format)

Import from USB Device

USB Device Status: No Device Attached Refresh

Save Cancel

Passaggio 4. Nell'area *Importa set di certificati completo* fare clic su un pulsante di opzione per scegliere l'origine dei certificati salvati. Le opzioni sono:

- *Importa dal PC*: selezionare questa opzione se i file vengono trovati nel computer.
- *Importa da USB*: selezionare questa opzione per importare i file da un'unità flash.

Nota: Nell'esempio viene scelto *Importa da PC*.

My Certificate

3rd-Party Authorized
 Self-Signed

Import Full Certificate Set

Import from PC

CA Certificate: C:\Users\zhenwan2\Desktop\certs\CA.pem Browse... (PEM format)

Certificate + Private Key: \wan2\Desktop\certs\cer_plus_private.pem Browse... (PEM format)

Import from USB Device

USB Device Status: No Device Attached Refresh

Save Cancel

Passaggio 5. Nell'area *Certificato CA*, fare clic su **Sfoggia...** e individuare il file CA.pem. file.

Nota: Se il firmware in esecuzione è successivo alla versione 1.1.0.6, fare clic sul pulsante *Scegli* e individuare il file necessario.

My Certificate

3rd-Party Authorized
 Self-Signed

Import Full Certificate Set

Import from PC

CA Certificate: C:\Users\zhenwan2\Desktop\certs\CA.pem **Browse...** (PEM format)

Certificate + Private Key: zhenwan2\Desktop\certs\cer_plus_private.pem **Browse...** (PEM format)

Import from USB Device

USB Device Status: No Device Attached **Refresh**

Save **Cancel**

Passaggio 6. Nell'area *Certificato + chiave privata*, fare clic su **Sfoggia...** e individuare il file `cer_plus_private.pem`.

Nota: Se il firmware in esecuzione è successivo alla versione 1.1.0.6, fare clic sul pulsante **Scegli** e individuare il file necessario.

My Certificate

3rd-Party Authorized
 Self-Signed

Import Full Certificate Set

Import from PC

CA Certificate: C:\Users\zhenwan2\Desktop\certs\CA.pem **Browse...** (PEM format)

Certificate + Private Key: zhenwan2\Desktop\certs\cer_plus_private.pem **Browse...** (PEM format)

Import from USB Device

USB Device Status: No Device Attached **Refresh**

Save **Cancel**

Passaggio 7. Fare clic su **Salva**.

My Certificate

3rd-Party Authorized
 Self-Signed

Import Full Certificate Set

Import from PC

CA Certificate: C:\Users\zhenwan2\Desktop\certs\CA.pem **Browse...** (PEM format)

Certificate + Private Key: zhenwan2\Desktop\certs\cer_plus_private.pem **Browse...** (PEM format)

Import from USB Device

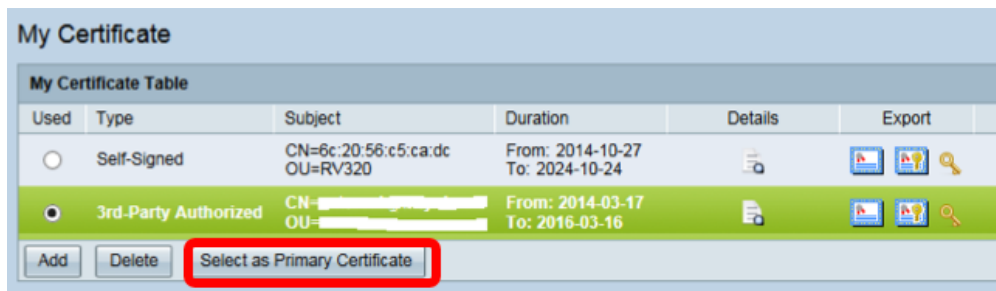
USB Device Status: No Device Attached **Refresh**

Save **Cancel**

Importazione dei certificati completata. Ora può essere utilizzato per l'accesso HTTPS, la

VPN SSL o la VPN IPsec.

Passaggio 8. (Facoltativo) Per utilizzare il certificato per HTTPS o SSL VPN, fare clic sul pulsante di opzione del certificato e quindi sul pulsante **Seleziona come certificato primario**.

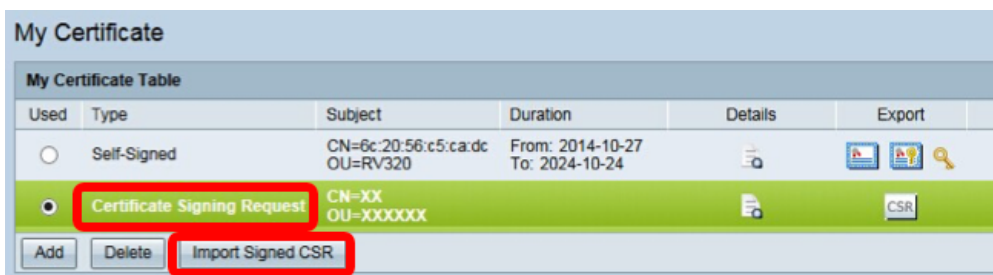


L'importazione di un certificato dovrebbe essere stata completata.

Firma del certificato tramite CSR

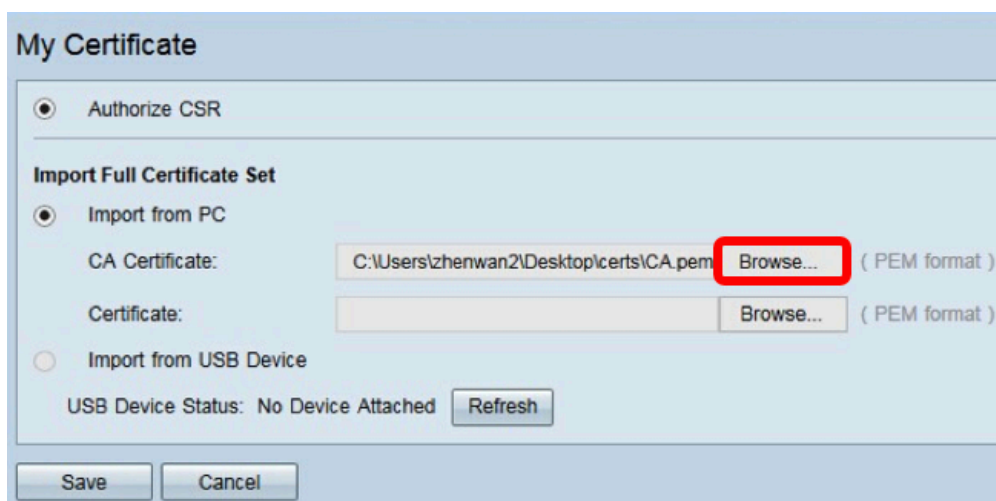
Passaggio 1. Generare una richiesta di firma del certificato (CSR) su RV320/RV325. Per informazioni su come generare un CSR, fare clic [qui](#).

Passaggio 2. Per importare il certificato, scegliere **Richiesta di firma certificato** e fare clic su **Importa CSR firmato**.

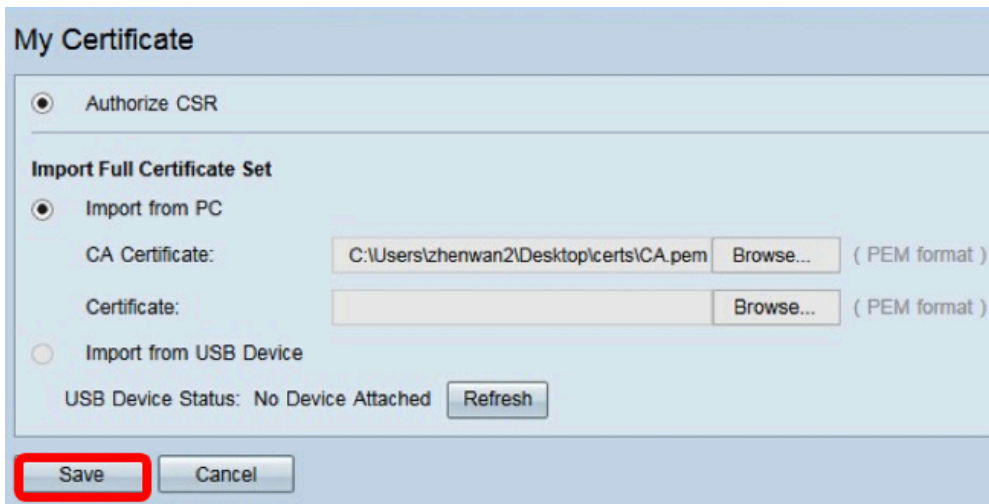


Passaggio 3. Fare clic su **Sfoggia...** e scegliere il file del certificato CA. Contiene il certificato CA radice + CA intermedia.

Nota: In questo esempio, la chiave privata non è necessaria poiché il certificato viene generato utilizzando CSR.



Passaggio 4. Fare clic su **Salva**.



A questo punto è necessario aver caricato correttamente un certificato utilizzando CSR.

Appendice:

Contenuto di RV320.pem

Attributi bag

IDChiaveLocale: 01 00 00 00

FriendLiName: {{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXX}}

Nome CSP Microsoft: Provider del servizio di crittografia EnhNAced Microsoft v1.0

Attributi chiave

Utilizzo chiave X509v3: 10

—BEGIN PRIVATE KEY—

MIIEvQIBADNABgkqhkiG9w0BAQEFAASCBCkCWJgSjAgEAAoIBAQCjEOqTe

.....

Sv3RH/fSHuP+NAYfgYHipxQDcObJF1LhY0UzD/cgz7f7BdKzC0fqPTEJA90=

—END PRIVATE KEY—

Attributi bag

IDChiaveLocale: 01 00 00 00

FriendLiName: Certificato PFX StartCom

oggetto=/description=XXXXXX/C=US/ST=XXXX/L=Xxxxx/O=XX/CN=xxx.xxx.net/emailAddress=xx.xx@xx.com

autorità emittente=/C=IL/O=StartCom Ltd./OU=S4cure Digital Certificate Signing/CN=StartCom Class 2 CA primaria intermedia S4rver

—BEGIN CERTIFICATE—

MIG2jCCBcKgAwIBAgINAgBbMA0GCSqGSIb3DQEBBQUAMNQswCQY

.....

MI4iYDx3GLii7gKZOF4W4unJvcoOtw0387AMGb/IfNIWqFNpuXtuUq0Esc

—END CERTIFICATE—

Attributi bag

FriendLiName: Autorità di certificazione StartCom

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—

MIHyTCCBbGgAwIBAgIBATNABgkqhkiG9w0BAQUFADB9MQswCQYDVQ

.....

Bj6y6koQOdjQK/W/7HA/lwr+bMEkXN9P/FIUQnNGqz9lgOgA38corog14=

—END CERTIFICATE—

Attributi bag

Subject=/C=IL/O=StartCom Ltd./OU=S4cure Digital Certificate Signing/CN=StartCom Class 2 CA primaria intermedia S4rver

issuer=/C=IL/O=StartCom Ltd./OU=S4cure Digital Certificate Signing/CN=StartCom Certification Authority

—BEGIN CERTIFICATE—

MIGNDCCBBygAwIBAgIBGjNABgkqhkiG9w0BAQUFADB9MQswCQYDVQQ

.....

WZP8P3PXLrQsldiL98l/ydrHIEH9LMF/TtNGCbnkqXBP7dgcgqhykguAzx/Q=

—END CERTIFICATE—