

# Configura il certificato su router VPN RV320 e RV325

## Obiettivo

I certificati vengono utilizzati per verificare l'identità di una persona o di un dispositivo, autenticare un servizio o crittografare i file. In RV320 è possibile aggiungere un massimo di 50 certificati autocertificando o autorizzando terze parti. È possibile esportare un certificato per un client o un amministratore e salvarlo su un PC o un dispositivo USB, quindi importarlo.

Lo scopo di questo documento è mostrare come selezionare un certificato primario, esportare un certificato e importare un certificato sui router VPN serie RV32x.

## Dispositivi interessati

- RV320 Dual WAN VPN Router
- RV325 Gigabit Dual WAN VPN Router

## Versione del software

- v1.1.0.09

## Certificato

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Gestione certificati > Certificato**. Verrà visualizzata la pagina *Certificato*:



The screenshot shows the 'My Certificate' web utility interface. It features a table with columns for 'Used', 'Type', 'Subject', 'Duration', 'Details', and 'Export'. The first row is highlighted in green and shows a 'Self-Signed' certificate with subject 'CN=6c:20:56:c6:16:52 OU=RV320' and duration 'From: 2013-Apr-08 To: 2023-Apr-06'. The second row shows a 'Certificate Signing Request' with subject 'CN=com OU=so'. The third row shows another 'Self-Signed' certificate with subject 'CN=jwdnkf OU=jdnd' and duration 'From: 2013-Apr-29 To: 2013-May-29'. Below the table are buttons for 'Add', 'Delete', and 'Select as Primary Certificate'.

Used	Type	Subject	Duration	Details	Export
<input checked="" type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input type="radio"/>	Certificate Signing Request	CN=com OU=so			
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		

Esistono due tipi di certificati:

- Autofirmato: certificato SSL (Secure Socket Layer) firmato dal proprio creatore. Questo tipo è meno sicuro perché non può essere annullato se la chiave privata è compromessa da un utente non autorizzato.

- Richiesta di firma del certificato: un'infrastruttura a chiave pubblica (PKI) inviata all'autorità di certificazione per richiedere un certificato di identità digitale. È più sicuro della firma automatica, in quanto la chiave privata è mantenuta segreta.

Passaggio 2. Fare clic sul pulsante di opzione desiderato nella *tabella Certificati personali* per scegliere un certificato.

Passaggio 3. Fare clic su **Seleziona come certificato principale** per rendere il certificato selezionato il certificato principale.

Passaggio 4. (Facoltativo) Per visualizzare informazioni dettagliate sul certificato, fare clic sull'icona **Dettagli**.



My Certificate Table					
Used	Type	Subject	Duration	Details	Export
<input checked="" type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input type="radio"/>	Certificate Signing Request	CN=com OU=so			
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		

Viene visualizzata la finestra *Dettagli certificato*:

### Certificate Details

**Certificate Information**

Version: 3  
 Serial Number: D8 AF 62 26 26 36 5D D1

**Subject Information**

Subject: CN=6c:20:56:c6:16:52  
 OU=RV320  
 O=Cisco Systems, Inc.  
 L=Irvine  
 C=US  
 ST=California

Public Key Algorithm: rsaEncryption -  
 Subject Key Identifier: 2D E3 89 6D FC 43 76 2B AF 1D AC 2B F1 EB 11 D3 19 FE AD 63

**Issuer Information**

Issuer: CN=6c:20:56:c6:16:52  
 OU=RV320  
 O=Cisco Systems, Inc.  
 L=Irvine  
 C=US  
 ST=California

Valid From: Apr 8 19:12:48 2013 GMT  
 Valid Through: Apr 6 19:12:48 2023 GMT  
 Signature Algorithm: sha1WithRSAEncryption  
 Authority Key Identifier: 2D E3 89 6D FC 43 76 2B AF 1D AC 2B F1 EB 11 D3 19 FE AD 63  
 Fingerprint: 33 C4 E6 40 7D DD 1F 44 32 57 18 A9 AA D1 66 FB 5A B2 CD 36

Passaggio 5. (Facoltativo) Per eliminare un certificato, fare clic sul pulsante di opzione del certificato che si desidera eliminare e quindi su **Elimina**.

Passaggio 6. Fare clic su **Save** per salvare le impostazioni.

## Esportare un certificato autofirmato

Passaggio 1. Fare clic sul pulsante dell'icona desiderato nella colonna *Esporta* per esportare un certificato autofirmato.

### My Certificate

**My Certificate Table**

Used	Type	Subject	Duration	Details	Export
<input checked="" type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input type="radio"/>	Certificate Signing Request	CN=com OU=so			
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		

I pulsanti disponibili per le icone sono definiti come segue:

- Esporta certificato per client — Esporta un certificato client utilizzato per connettere il client alla rete privata virtuale (VPN).
- Esporta certificato per amministratore — Esporta un certificato amministratore. Viene generata una chiave privata e ne viene conservata una copia per il backup.
- Esporta chiave privata — Esporta una chiave privata per il software client VPN, che richiede credenziali separate per una connessione VPN.

Passaggio 2. Fare clic su **Apri** per visualizzare la chiave.

Passaggio 3. Fare clic su **Save** per salvare la chiave.

## Esporta una richiesta di firma del certificato

Passaggio 1. Fare clic su **CSR** (Export Certificate Signing Request).



My Certificate					
My Certificate Table					
Used	Type	Subject	Duration	Details	Export
<input type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input checked="" type="radio"/>	Certificate Signing Request	CN=com OU=so			<b>CSR</b>
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		

Passaggio 2. Fare clic su **Apri** per visualizzare.

Passaggio 3. Fare clic su **Save** per salvare la chiave sul PC o sulla porta USB.

## Importa certificato

Passaggio 1. Fare clic su **Aggiungi** per importare un certificato.



My Certificate					
My Certificate Table					
Used	Type	Subject	Duration	Details	Export
<input type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input checked="" type="radio"/>	Certificate Signing Request	CN=com OU=so			CSR
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		

Viene visualizzata la seguente finestra:

**My Certificate**

3rd-Party Authorized  
 Self-Signed

---

**Import Full Certificate Set**

Import from PC

CA Certificate:  No file chosen ( PEM format )

Certificate + Private Key:  No file chosen ( PEM format )

Import from USB Device

USB Device Status: No Device Attached

Passaggio 2. Fare clic sul pulsante di opzione desiderato per definire il tipo di certificato da importare.

**My Certificate**

3rd-Party Authorized  
 Self-Signed

---

**Import Full Certificate Set**

Import from PC

CA Certificate:  No file chosen ( PEM format )

Certificate + Private Key:  No file chosen ( PEM format )

Import from USB Device

USB Device Status: No Device Attached

·Autorizzato da terze parti: un'infrastruttura a chiave pubblica (PKI) in cui l'autorità di certificazione fornisce la firma digitale.

·Autofirmato: certificato SSL (Secure Socket Layer) firmato dal proprio creatore.

Passaggio 3. Fare clic sul pulsante di opzione desiderato per scegliere la modalità di importazione del certificato.

**My Certificate**

3rd-Party Authorized  
 Self-Signed

**Import Full Certificate Set**

Import from PC  
 CA Certificate:  No file chosen ( PEM format )  
 Certificate + Private Key:  No file chosen ( PEM format )  
 Import from USB Device

·Importa da PC: il certificato viene importato dal PC in cui è stato salvato.

·Importa da USB: il certificato viene importato dall'unità USB.

## Importa certificato da PC

Passaggio 1. Se si sta importando un certificato autorizzato di terze parti, fare clic su **Scegli file** accanto a *Certificato CA* per individuare il percorso del file e selezionarlo.

Passaggio 2. Fare clic su **Scegli file** accanto a *Certificato + chiave privata* per individuare il percorso del file e selezionarlo.

Passaggio 3. Fare clic su **Save** per salvare le impostazioni. Il certificato importato verrà visualizzato nella *tabella Certificati*.

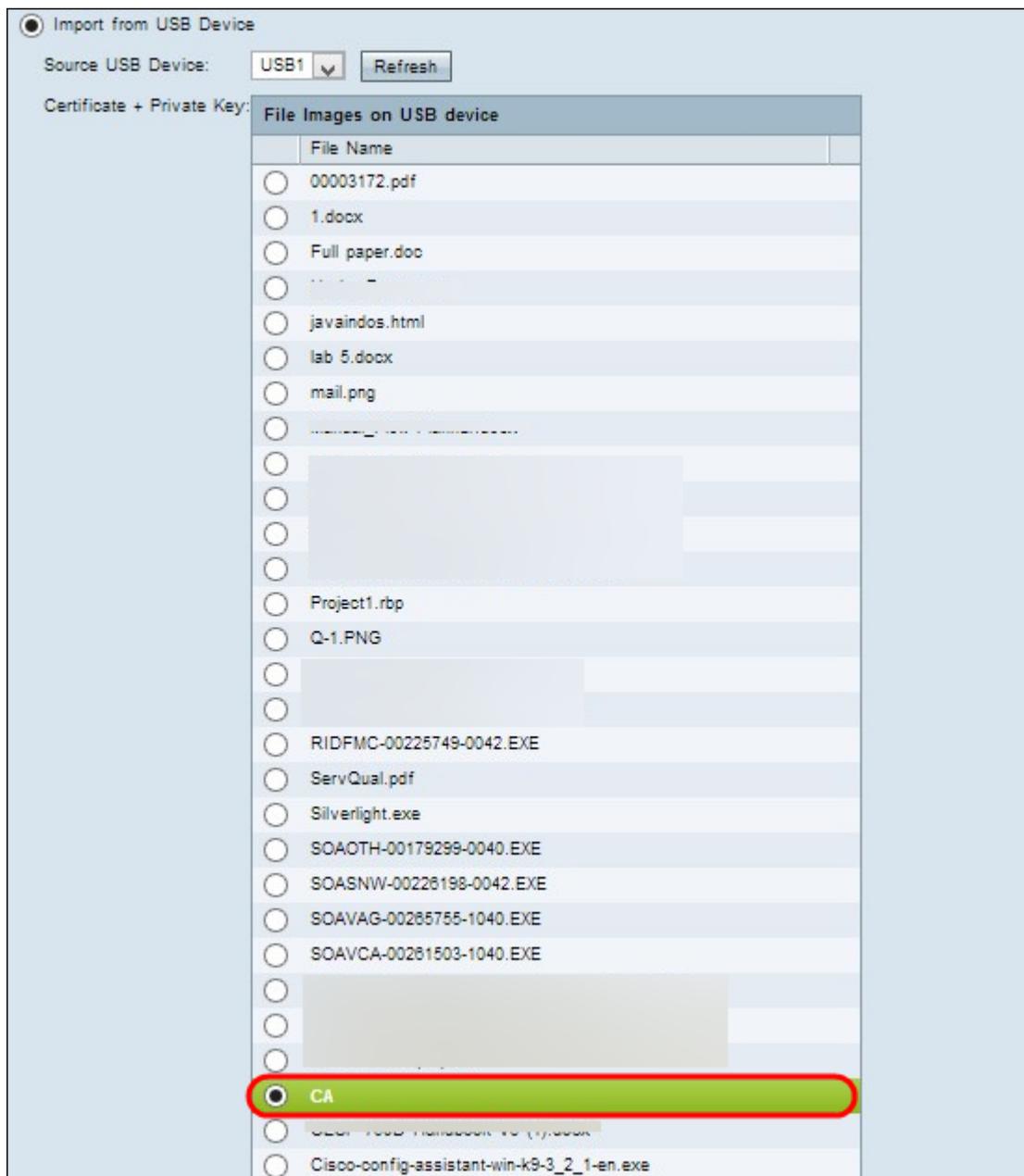
**My Certificate**

**My Certificate Table**

Used	Type	Subject	Duration	Details	Export
<input checked="" type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input type="radio"/>	Certificate Signing Request	CN=com OU=so			
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		
<input type="radio"/>	Self-Signed	CN= OU=			

## Importa certificato da USB

Passaggio 1. Selezionare il dispositivo USB appropriato dall'elenco a discesa *Source USB Device (Dispositivo USB di origine)*.



Passaggio 2. Se si sta importando un certificato autorizzato di terze parti, fare clic sul pulsante di opzione appropriato per importare il certificato CA salvato sulla porta USB.

Passaggio 3. Scegliere il pulsante di opzione appropriato per importare il certificato + la chiave privata salvati sull'USB.

Passaggio 4. Fare clic su **Save** per salvare le impostazioni. Il certificato importato verrà visualizzato nella *tabella Certificati*.

## My Certificate

My Certificate Table					
Used	Type	Subject	Duration	Details	Export
<input checked="" type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		  
<input type="radio"/>	Certificate Signing Request	CN=com OU=so			 CSR
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		  
<input type="radio"/>	Self-Signed	CN= OU=			  