

Konfigurieren des Zertifikats auf RV320- und RV325-VPN-Routern

Ziel

Zertifikate werden verwendet, um die Identität einer Person oder eines Geräts zu überprüfen, einen Dienst zu authentifizieren oder Dateien zu verschlüsseln. Auf dem RV320 können Sie maximal 50 Zertifikate durch Selbstsignierung oder Autorisierung von Drittanbietern hinzufügen. Sie können ein Zertifikat für einen Client oder Administrator exportieren, es auf einem PC oder USB-Gerät speichern und dann importieren.

In diesem Dokument wird erläutert, wie Sie ein primäres Zertifikat auswählen, ein Zertifikat exportieren und ein Zertifikat in die VPN-Router der Serie RV32x importieren.

Anwendbare Geräte

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

Softwareversion

- v1.1.0.09

Mein Zertifikat

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Zertifikatsverwaltung > Mein Zertifikat** aus. Die Seite *Mein Zertifikat* wird geöffnet:



The screenshot shows a web interface titled "My Certificate". It contains a table with the following columns: "Used", "Type", "Subject", "Duration", "Details", and "Export". There are three rows of certificates. The first row is selected and highlighted in green. Below the table are three buttons: "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		

Es gibt zwei Arten von Zertifikaten:

- Selbst signiert - Ein SSL-Zertifikat (Secure Socket Layer), das vom eigenen Ersteller signiert wird. Dieser Typ ist weniger sicher, da er nicht abgebrochen werden kann, wenn der private Schlüssel von einem Angreifer kompromittiert wird.
- Certificate Signing Request - Eine Public Key Infrastructure (PKI), die an die Zertifizierungsstelle gesendet wird, um ein digitales Identitätszertifikat zu beantragen. Sie ist sicherer als selbstsignierte Schlüssel, da der private Schlüssel geheim gehalten wird.

Schritt 2: Klicken Sie in der *Tabelle "Mein Zertifikat"* auf das entsprechende Optionsfeld, um ein Zertifikat auszuwählen.

Schritt 3: Klicken Sie auf **Als primäres Zertifikat auswählen**, um das ausgewählte Zertifikat zum primären Zertifikat zu machen.

Schritt 4: (Optional) Um detaillierte Informationen zum Zertifikat anzuzeigen, klicken Sie auf das Symbol **Details**.



The screenshot shows a window titled "My Certificate" containing a table of certificates. The table has columns for "Used", "Type", "Subject", "Duration", "Details", and "Export". The first row is selected and highlighted in green. The "Details" icon for this row is circled in red. 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		

Buttons: Add, Delete, Select as Primary Certificate

Das Fenster *Zertifikatdetails* wird geöffnet:

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

Schritt 5: (Optional) Um ein Zertifikat zu löschen, klicken Sie auf das Optionsfeld des Zertifikats, das Sie löschen möchten, und klicken Sie dann auf **Löschen**.

Schritt 6: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Exportieren eines selbst signierten Zertifikats

Schritt 1: Klicken Sie in der Spalte *Exportieren* auf das gewünschte Symbol, um ein selbstsigniertes Zertifikat zu exportieren.

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		

Die verfügbaren Symbolschaltflächen sind wie folgt definiert:

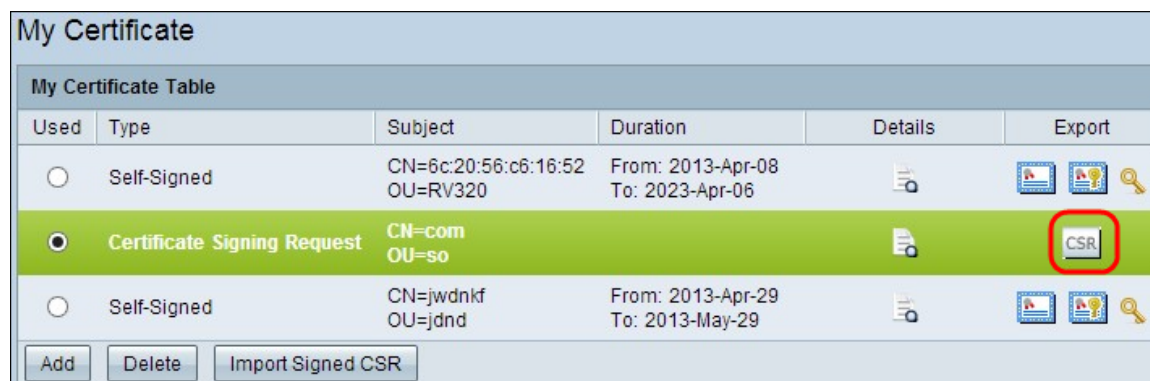
- Zertifikat exportieren für Client - Exportieren eines Client-Zertifikats, das verwendet wird, um den Client mit dem Virtual Private Network (VPN) zu verbinden.
- Zertifikat für Administrator exportieren - Administratorzertifikat exportieren. Ein privater Schlüssel wird generiert, und eine Kopie wird zur Sicherung aufbewahrt.
- Private Schlüssel exportieren - Einen privaten Schlüssel für VPN-Client-Software exportieren, der separate Anmeldeinformationen für eine VPN-Verbindung benötigt.

Schritt 2: Klicken Sie auf **Öffnen**, um den Schlüssel anzuzeigen.

Schritt 3: Klicken Sie auf **Speichern**, um den Schlüssel zu speichern.

Zertifikatssignierungsanforderung exportieren

Schritt 1: Klicken Sie auf **CSR** (Signierungsanfrage für Zertifikat exportieren).



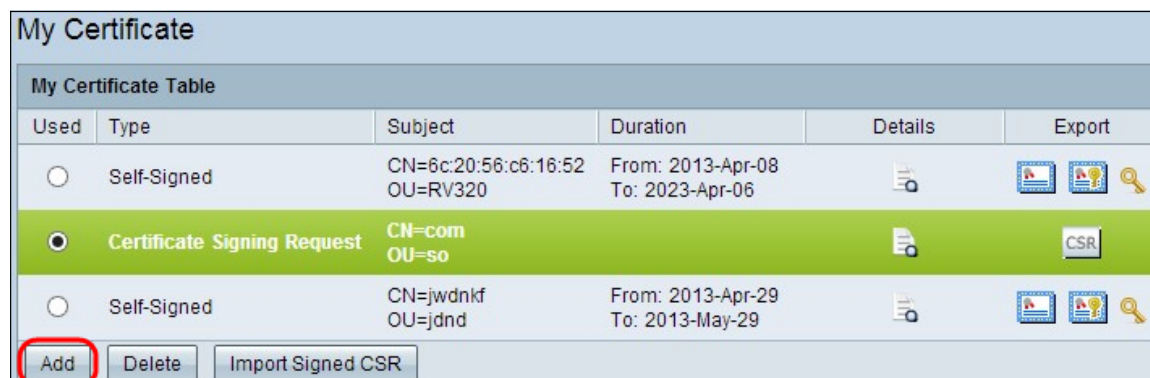
My Certificate					
My Certificate Table					
Used	Type	Subject	Duration	Details	Export
<input type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input checked="" type="radio"/>	Certificate Signing Request	CN=com OU=so			CSR
<input type="radio"/>	Self-Signed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

Schritt 2: Klicken Sie zum Anzeigen auf **Öffnen**.

Schritt 3: Klicken Sie auf **Speichern**, um den Schlüssel auf Ihrem PC oder USB zu speichern.

Importieren eines Zertifikats

Schritt 1: Klicken Sie auf **Hinzufügen**, um ein Zertifikat zu importieren.



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		

Das folgende Fenster wird angezeigt:

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

Schritt 2: Klicken Sie auf das gewünschte Optionsfeld, um den Typ des Zertifikats festzulegen, das Sie importieren.

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

·Drittanbieter Authorized (Autorisiert) - eine Public Key Infrastructure (PKI), in der die Zertifizierungsstelle die digitale Signatur bereitstellt.

·Selbst signiert - Ein SSL-Zertifikat (Secure Socket Layer), das vom eigenen Ersteller signiert wird.

Schritt 3: Klicken Sie auf das gewünschte Optionsfeld, um festzulegen, wie das Zertifikat importiert werden soll.

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

·Importieren von PC: Das Zertifikat wird von Ihrem PC importiert, wo Sie es gespeichert haben.

·Import from USB (Aus USB importieren) - Zertifikat wird von Ihrem USB-Laufwerk importiert.

Zertifikat vom PC importieren

Schritt 1: Wenn Sie ein von einem Drittanbieter autorisiertes Zertifikat importieren, klicken Sie neben dem *Zertifizierungsstellenzertifikat* auf **Datei auswählen**, um nach dem Speicherort der Datei zu suchen und diese auszuwählen.

Schritt 2: Klicken Sie auf **Datei auswählen** neben *Zertifikat + Privater Schlüssel*, um nach dem Speicherort der Datei zu suchen und diese auszuwählen.

Schritt 3: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern. Das importierte Zertifikat wird in der *Tabelle "Mein Zertifikat"* angezeigt.

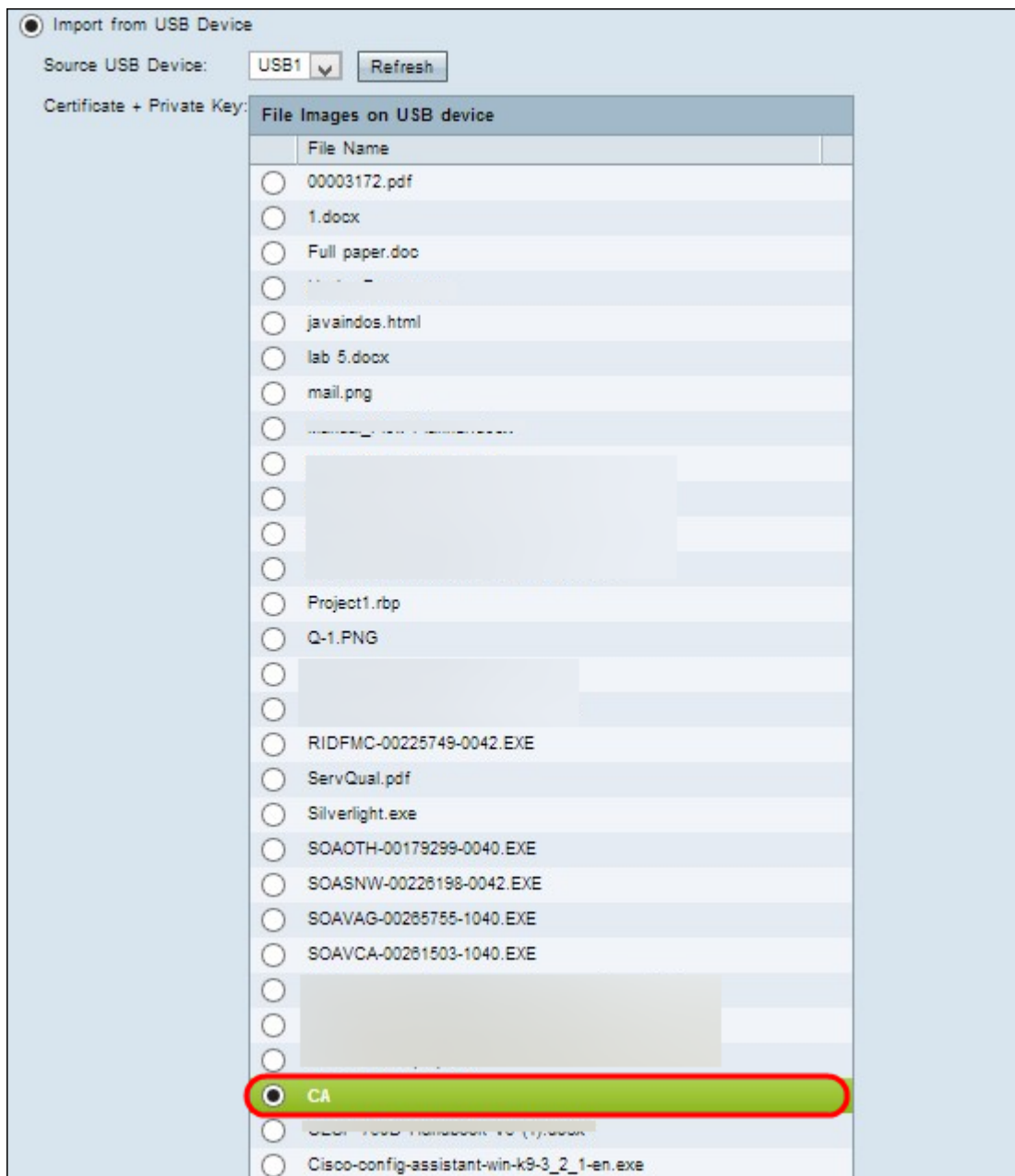
My Certificate

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=			

Zertifikat vom USB importieren

Schritt 1: Wählen Sie das passende USB-Gerät aus der Dropdown-Liste *Source USB Device* (*Quelle USB-Gerät*) aus.













Schritt 2: Wenn Sie ein von einem Drittanbieter autorisiertes Zertifikat importieren, klicken Sie auf das entsprechende Optionsfeld, um das Zertifizierungsstellenzertifikat zu importieren, das Sie auf Ihrem USB-Laufwerk gespeichert haben.

Schritt 3: Wählen Sie das entsprechende Optionsfeld, um das Zertifikat + den privaten Schlüssel zu importieren, das Sie auf Ihrem USB-Stick gespeichert haben.

Schritt 4: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern. Das importierte Zertifikat wird in der *Tabelle "Mein Zertifikat"* angezeigt.

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=		