

在RV320和RV325 VPN路由器上配置我的證書

目標

證書用於驗證個人或裝置的身份、驗證服務或加密檔案。在RV320上，您可以通過自簽名或第三方授權新增最多50個證書。您可以匯出客戶端或管理員的證書，並將其儲存在PC或USB裝置上，然後匯入該證書。

本文檔的目的是向您展示如何在RV32x系列VPN路由器上選擇主要證書、匯出證書和匯入證書。

適用裝置

- RV320 Dual WAN VPN路由器
- RV325 Gigabit Dual WAN VPN路由器

軟體版本

·v1.1.0.09

我的憑證

步驟1.登入到Web配置實用程式，然後選擇**Certificate Management > My Certificate**。*My Certificate*頁面隨即開啟：



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			

有兩種型別的證書：

- 自簽名 — 由自己的建立者簽名的安全套接字層(SSL)證書。此型別不太安全，因為如果攻擊者入侵了私鑰，則無法取消此型別。
- 證書簽名請求 — 傳送到證書頒發機構以申請數位身份證書的公鑰基礎架構(PKI)。它比自簽名更安全，因為私鑰是保密的。

步驟2.從*My Certificate Table*中按一下所需的單選按鈕以選擇證書。

步驟3.按一下**Select as Primary Certificate**，將所選憑證作為主要憑證。

步驟4. (可選) 要檢視有關證書的詳細資訊，請按一下**Details**圖示。

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=jwdnlf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		

*Certificate Details*視窗開啟：

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
<input type="button" value="Close"/>	

步驟5. (可選) 若要刪除憑證，請按一下您要刪除的憑證的單選按鈕，然後按一下**Delete**。

步驟6. 按一下**Save**以儲存設定。

匯出自簽名證書

步驟1. 在*Export*列中按一下所需的圖示按鈕以匯出自簽名證書。

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		

可用的圖示按鈕定義如下：

- 匯出客戶端證書 — 匯出用於將客戶端連線到虛擬專用網路(VPN)的客戶端證書。
- 匯出管理員證書 — 匯出管理員證書。生成私鑰並保留副本以供備份。
- 匯出私鑰 — 匯出VPN客戶端軟體的私鑰，該軟體需要單獨的VPN連線憑證。

步驟2.按一下**Open**以檢視金鑰。

步驟3.按一下**Save**以儲存金鑰。

匯出證書簽名請求

步驟1。按一下**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			
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		

步驟2.按一下「**Open**」以檢視。

步驟3.按一下**Save**將金鑰儲存到您的PC或USB上。

匯入證書

步驟1。按一下**Add**以匯入憑證。

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			
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		

出現以下視窗：

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

步驟2.按一下所需的單選按鈕以定義要匯入的證書型別。

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

- 第三方授權 — 由證書頒發機構提供數位簽章的公開金鑰基礎設施(PKI)。
- 自簽名 — 由自己的建立者簽名的安全套接字層(SSL)證書。

步驟3.按一下所需的單選按鈕以選擇要匯入證書的方式。

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

·從PC匯入 — 證書從儲存它的PC匯入。

·從USB匯入 — 證書從USB驅動器匯入。

從PC匯入證書

步驟1. 如果您要匯入第三方授權證書，請按一下CA證書旁邊的**選擇檔案**以瀏覽檔案位置並將其選中。

步驟2. 按一下 *Certificate + Private Key* 旁邊的 **Choose File**，瀏覽找到檔案的位置並選擇它。

步驟3. 按一下 **Save** 以儲存設定。匯入的證書將顯示在 *My Certificate Table* 中。

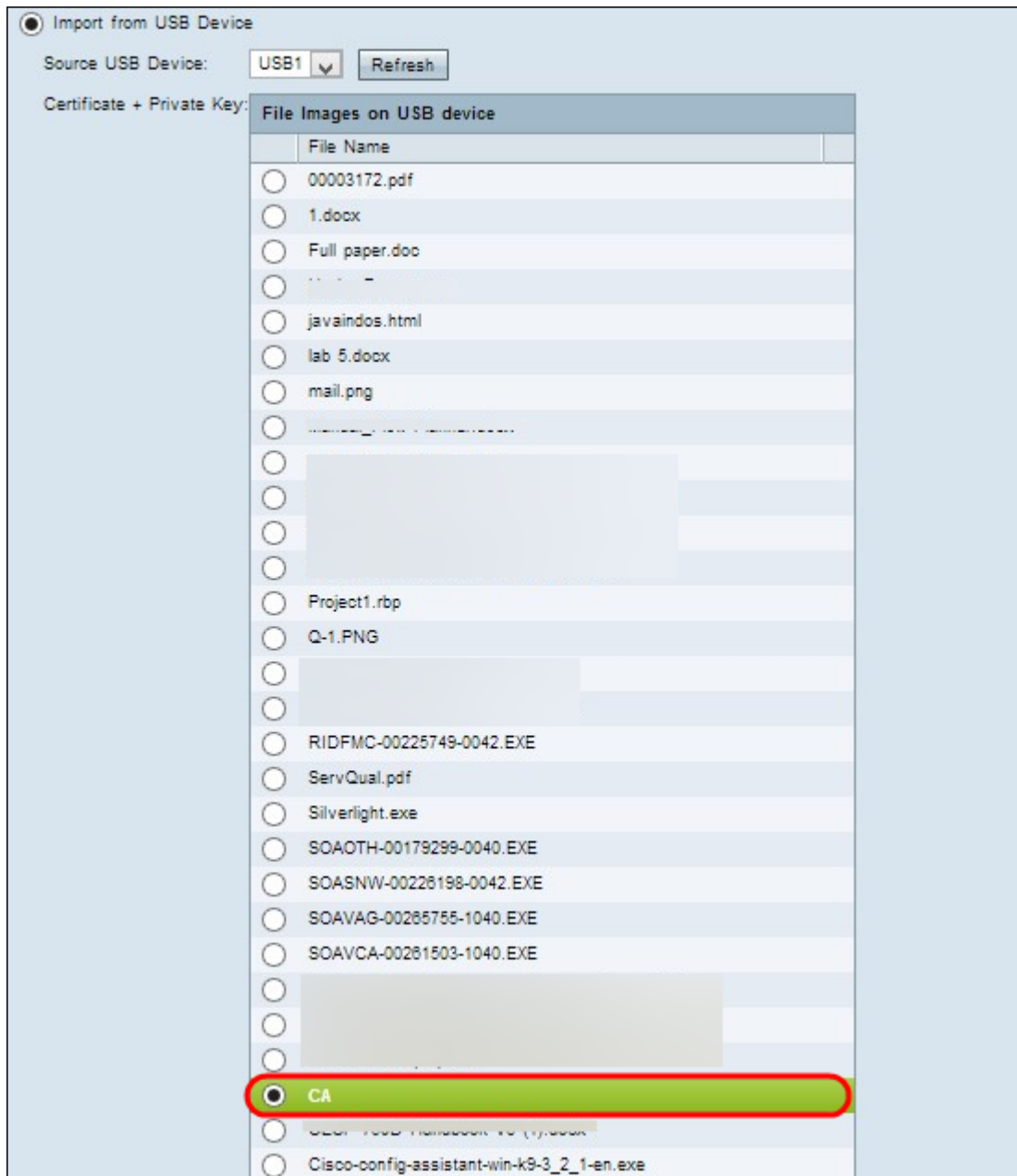
My Certificate

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=			

從USB匯入證書

步驟1. 從 *Source USB Device* 下拉選單中選擇適當的USB裝置。













步驟2.如果要匯入第三方授權證書，請按一下相應的單選按鈕以匯入儲存在USB上的CA證書。

步驟3.選擇適當的單選按鈕以匯入儲存在USB上的證書+私鑰。

步驟4.按一下Save以儲存設定。匯入的證書將顯示在My Certificate Table中。

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=		