

在RV320和RV325 VPN路由器上生成證書

目標

公鑰密碼是當今最常見的密碼學形式之一。公鑰加密使用公鑰和私鑰。該系統首先通過使用公鑰對資訊進行加密。然後，只能通過使用私鑰解密資訊。公鑰加密的一個常見用途是通過使用安全套接字層(SSL)或傳輸層安全(TLS)連線對應用流量進行加密。證書是一種用於分發公鑰以及有關伺服器 and 負責伺服器的組織的其他資訊的方法。證書可以由證書頒發機構(CA)進行數位簽章。CA是受信任的第三方，已驗證憑證中包含的資訊是否準確。

本文說明如何在RV32x VPN路由器系列上生成證書。

適用裝置

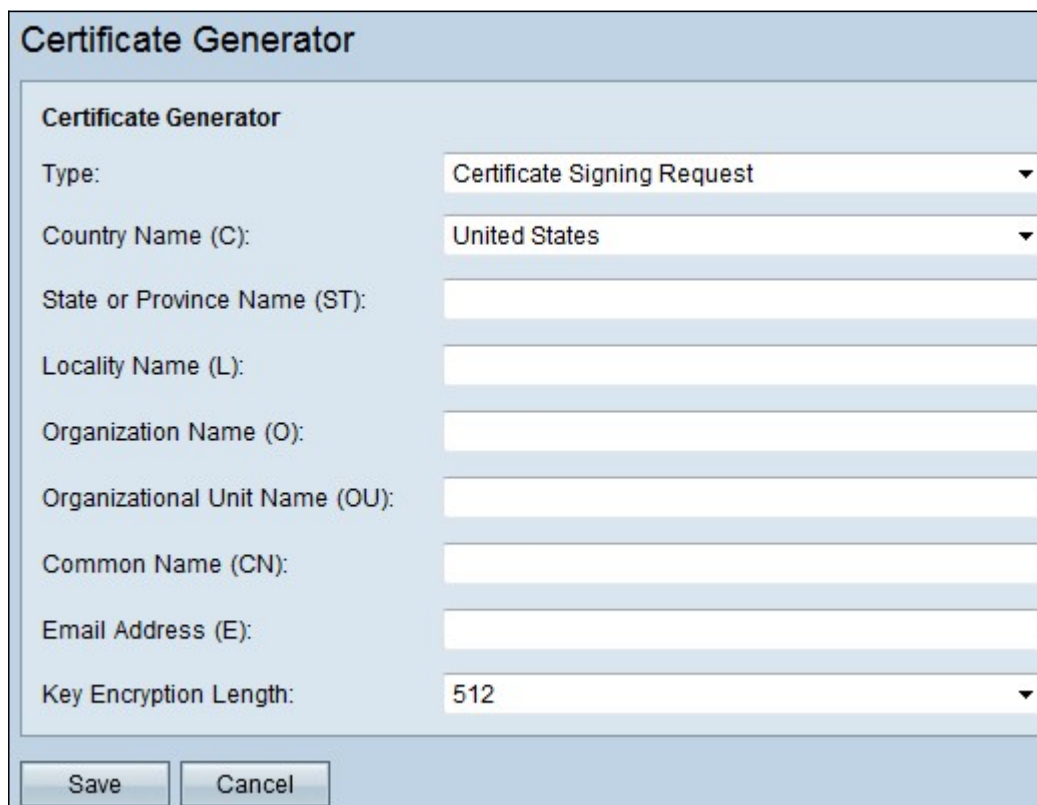
- RV320 Dual WAN VPN路由器
- RV325 Gigabit Dual WAN VPN路由器

軟體版本

·v1.1.0.09

生成證書

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



Certificate Generator

Certificate Generator

Type: Certificate Signing Request

Country Name (C): United States

State or Province Name (ST):

Locality Name (L):

Organization Name (O):

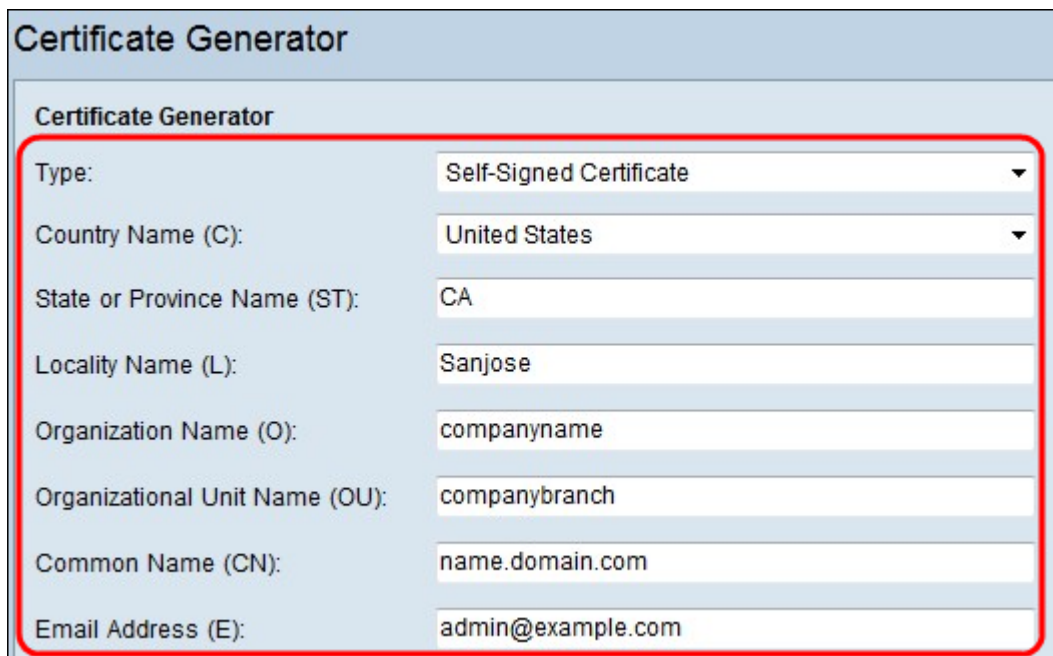
Organizational Unit Name (OU):

Common Name (CN):

Email Address (E):

Key Encryption Length: 512

Save Cancel



The image shows a web form titled "Certificate Generator". The form contains several input fields, each with a label and a value. A red rectangular box highlights the entire form area. The fields and their values are:

Field Label	Value
Type:	Self-Signed Certificate
Country Name (C):	United States
State or Province Name (ST):	CA
Locality Name (L):	Sanjose
Organization Name (O):	companyname
Organizational Unit Name (OU):	companybranch
Common Name (CN):	name.domain.com
Email Address (E):	admin@example.com

步驟2.從Type下拉選單中選擇相應的證書型別：

- 自簽名證書 — 這是由自己的建立者簽名的安全套接字層(SSL)證書。此證書不太可信，因為如果攻擊者以某種方式入侵私鑰，則無法取消此證書。
- 認證的簽名請求 — 這是向證書頒發機構傳送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3.從「國家/地區名稱」下拉選單中選擇組織合法註冊的國家/地區名稱。

步驟4.在「省(州)」或「省(州)」欄位中輸入組織所在省(州)、省(區)或地區的名稱或縮寫。

步驟5.在Locality Name欄位中輸入組織註冊/所在的城市/地區的名稱。

步驟6.輸入企業合法註冊的名稱，如果您註冊為小型企業/獨資經營者，請在「組織名稱」欄位中輸入證書申請者的名稱。

步驟7.在「組織單位名稱」欄位中輸入名稱，以區分組織內的各個部門。

步驟8.在「公用名」欄位中輸入名稱。此名稱必須是您對其使用證書的網站的完全限定域名。

步驟9.輸入希望生成證書的人員的電郵地址。

Certificate Generator

Certificate Generator

Type: Self-Signed Certificate

Country Name (C): United States

State or Province Name (ST): CA

Locality Name (L): Sanjose

Organization Name (O): companyname

Organizational Unit Name (OU): companybranch

Common Name (CN): name.domain.com

Email Address (E): admin@example.com

Key Encryption Length: 512

Valid Duration: 512
1024
2048 Days (Range: 1-10950, Default: 30)

Save Cancel

步驟10.從Key Encryption Length下拉式清單中選擇金鑰長度，金鑰大小越大，憑證就越安全。金鑰大小越大，處理時間就越長。

Certificate Generator

Certificate Generator

Type: Self-Signed Certificate

Country Name (C): United States

State or Province Name (ST): CA

Locality Name (L): Sanjose

Organization Name (O): companyname

Organizational Unit Name (OU): companybranch

Common Name (CN): name.domain.com

Email Address (E): admin@example.com

Key Encryption Length: 1024

Valid Duration: 500

Save Cancel

附註：如果選擇證書型別作為證書簽名請求，請跳過步驟11並繼續。

步驟11.輸入證書的有效天數。

步驟12.按一下**Save**以生成憑證。生成的證書顯示在「我的證書」(*My Certificate*)頁面上。若要檢視*My Certificate*頁面，請選擇**Certificate Management > My Certificate**。