

在RV34x系列路由器上使用第三方SSL證書替換預設自簽名證書

簡介

數位證書通過證書的指定主題來證明公共金鑰的所有權。這允許依賴方依賴於由與經認證的公鑰對應的私鑰進行的簽名或斷言。路由器可以生成自簽名證書，即由網路管理員建立的證書。它還可以向證書頒發機構(CA)發出申請數位身份證書的請求。必須擁有來自第三方應用程式的合法證書。

CA簽署憑證的方式有兩種：

1. CA使用私鑰簽署憑證。
2. CA使用RV34x產生的憑證簽署請求(CSR)來簽署憑證。

大多數商業憑證供應商使用中間憑證。由於中間證書由受信任的根CA頒發，因此由中間證書頒發的任何證書都繼承受信任的根的信任，如信任證書鏈。

目標

本文旨在展示如何請求和上傳由CA頒發的第三方安全套接字層(SSL)證書，以替換RV34x路由器上的自簽名證書。

適用裝置

- RV340
- RV340W
- RV345
- RV345P

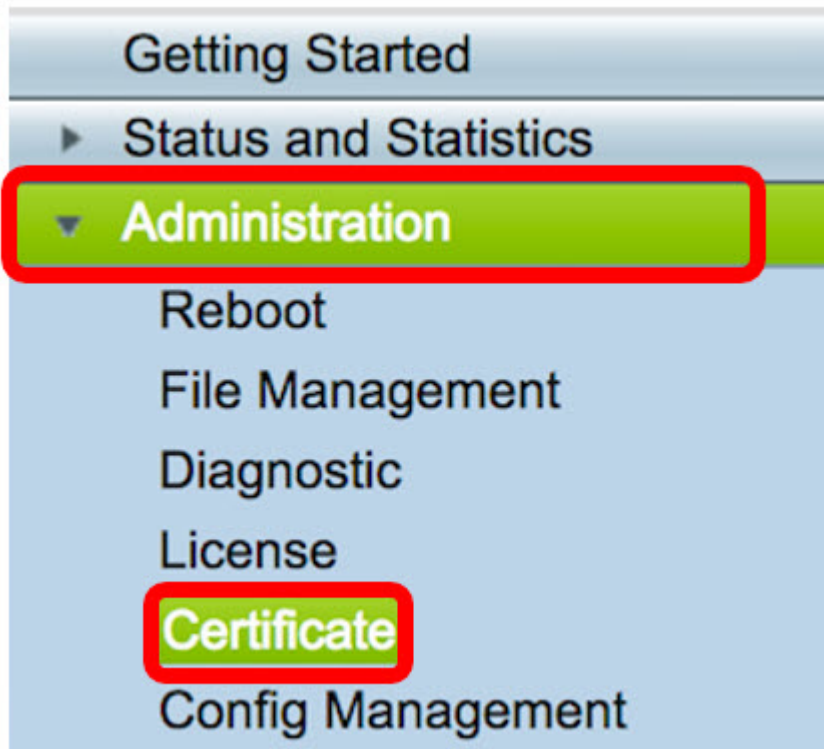
軟體版本

- 1.0.01.17

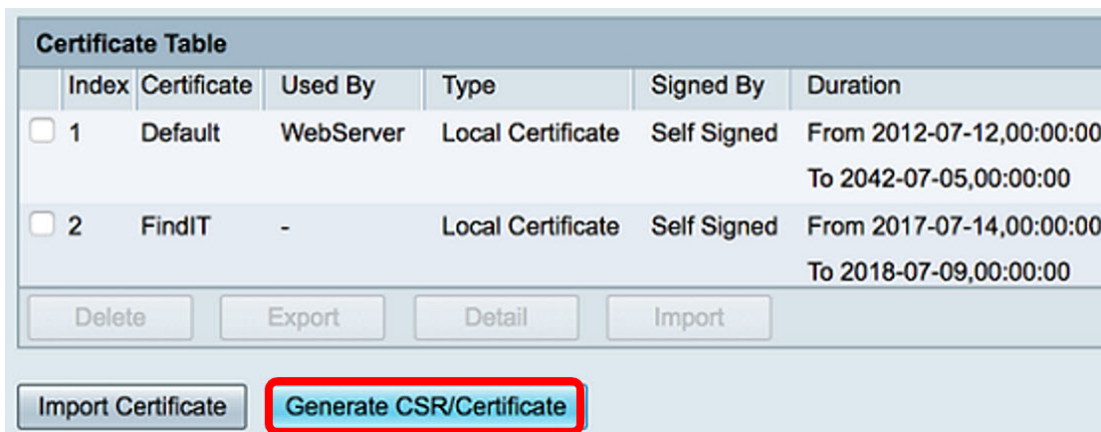
使用第三方SSL證書替換預設自簽名證書

產生CSR

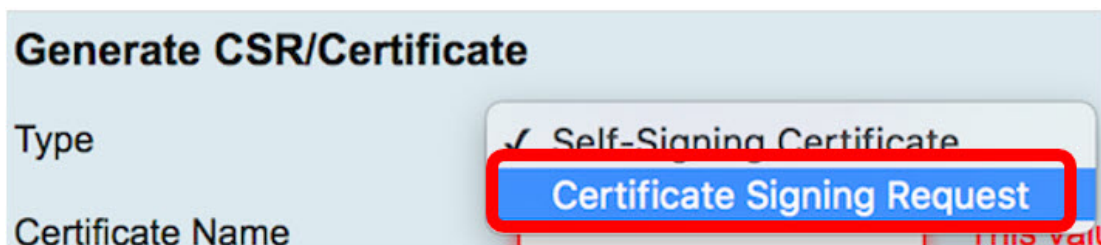
步驟1. 登入到路由器的基於Web的實用程式，然後選擇Administration > Certificate。



步驟2.在「Certificate Table」下，按一下**Generate CSR/Certificate**按鈕。



步驟3.在產生CSR/憑證視窗中，按一下 *Type* 下拉箭頭，然後選擇**Certificate Signing Request**。



步驟4.在 *Certificate Name* 欄位中輸入憑證的名稱。

Generate CSR/Certificate

Type

Certificate Name

附註：本範例中使用的是34xrouter。

步驟5.在 *Subject Alternative Name* 欄位中輸入備用名稱，然後按一下其下方的 **FQDN** 單選按鈕進行匹配。備用名稱是可用於訪問路由器的域名。

Subject Alternative Name

IP Address FQDN Email

附註：在此示例中，使用RVrouter.com。

步驟6.按一下 *Country Name* 下拉箭頭選擇您所在的國家/地區。

IP Address FQDN Email

Country Name

附註：在本示例中，選擇了US - United States。

步驟7.在 *State or Province Name(ST)* 欄位中輸入州或省的名稱。

Country Name

State or Province Name(ST)

附註：在本示例中，使用California。

步驟8.在 *Locality Name(L)* 欄位中輸入 *locality*。

State or Province Name(ST)

Locality Name(L)

附註：在本示例中，使用了Irvine。

步驟9.在提供的欄位中輸入組織名稱(O)。

Locality Name(L)	Irvine
Organization Name(O)	Cisco

附註：在本範例中使用的是Cisco。

步驟10.在提供的欄位中輸入組織單位名稱(OU)。

Organization Name(O)	Cisco
Organization Unit Name(OU)	SBKM

附註：本示例使用SBKM。

步驟11.在Common Name(CN)欄位中輸入名稱。

Organization Unit Name(OU)	SBKM
Common Name(CN)	34xrouter

附註：本範例中使用的是34xrouter。

步驟12.輸入您的電子郵件地址或您希望將證書傳送到的任何電子郵件地址。

Common Name(CN)	34xrouter
Email Address(E)	@gmail.com

附註：在此示例中，使用gmail.com電子郵件地址。

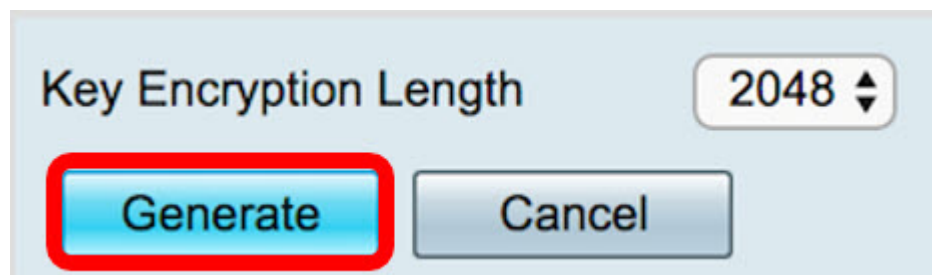
步驟13.從下拉選單中選擇Key Encryption Length，以設定金鑰中的位數。預設長度為512。

Email Address(E)	@gmail.com	
Key Encryption Length	✓ 512 1024 2048	
Generate	Cancel	2048

附註：本示例使用2048。強烈建議這樣做，因為較長的加密比較短的金鑰更難解碼，因此更

安全。

步驟14.按一下**Generate**。



您建立的證書請求現在將顯示在「證書表」中。

Certificate Table					
	Index	Certificate	Used By	Type	Signed By
<input type="checkbox"/>	1	Default	WebServer	Local Certificate	Self Signed
<input type="checkbox"/>	2	FindIT	-	Local Certificate	Self Signed
<input type="checkbox"/>	3	34xRouter	-	Certificate Signing Request	-

現在，您已成功產生CSR。

匯出CSR

步驟1. 勾選「Certificate Table」中憑證要求旁邊的方塊，然後按一下「Export」。

Certificate Table				
	Index	Certificate	Used By	Type
<input type="checkbox"/>	1	Default	WebServer	Local Certificate
<input type="checkbox"/>	2	FindIT	-	Local Certificate
<input checked="" type="checkbox"/>	3	34xRouter	-	Certificate Signing Request

Delete Export Detail Import

步驟2. 在「Export Certificate」視窗中按一下「Download」，以PEM格式將檔案下載到您的電腦中。



現在，您已成功將CSR匯出到您的電腦。

將CSR上傳到憑證提供者

步驟1。使用記事本開啟下載的檔案並複製CSR，然後將其貼到第三方SSL憑證提供者網站中提供的欄位中。

1. Copy and paste your CSR into this box:	<pre>STZJWoGLiyqRIPPHKREghzRfRh9WVW9KWdXzAgMI UzBRMAkGA1UdEwQCMAAwHQYDVR0OBBYEFB24F/ A1UdDwQEAWIF4DAYBgNVHREETAPgg0zNHhyb3VC CwUAA4IBAQA8J/x6+BLOGr797UeHxBH8sCuBSwQ dYGbl7qzZVVO+b/TvJii7jG52ojYzNDGFWamfYnoCrhv x7+ooeOn9ihoOXxEFKhrn2ueaMZJKQAnFpCwapbsxf pVBnwK74cfF8NBVivtX08SK6qn9qgsvxJcGxmlyBiffV YZITBEWG2Q1TVIY0brOkNbir2VuGoqpsplRqMcq/yE 1WkB91P7hA6X4AB80cKZQEdDsCvrjtgI -----END CERTIFICATE REQUEST-----</pre>
2. Select the server software used to generate the CSR:	Select from list: <input type="text"/>

附註：在此示例中，Comodo.com用作證書提供程式。

步驟2.選擇用於產生CSR的伺服器軟體。在這種情況下，由於RV34x路由器不在清單中，因此選擇OTHER。

1. Copy and paste your CSR into this box:	<pre>STZJWoGLiyqRIPPHKREghzRfRh9WVW9KWdXzAgMI UzBRMAkGA1UdEwQCMAAwHQYDVR0OBBYEFB24F/ A1UdDwQEAWIF4DAYBgNVHREETAPgg0zNHhyb3VC CwUAA4IBAQA8J/x6+BLOGr797UeHxBH8sCuBSwQ dYGbl7qzZVVO+b/TvJii7jG52ojYzNDGFWamfYnoCrhv x7+ooeOn9ihoOXxEFKhrn2ueaMZJKQAnFpCwapbsxf pVBnwK74cfF8NBVivtX08SK6qn9qgsvxJcGxmlyBiffV YZITBEWG2Q1TVIY0brOkNbir2VuGoqpsplRqMcq/yE 1WkB91P7hA6X4AB80cKZQEdDsCvrjtgI -----END CERTIFICATE REQUEST-----</pre>
2. Select the server software used to generate the CSR:	<input type="text" value="OTHER"/>

步驟3.將證書下載到電腦中。

上傳第3個SSL參與方證書

步驟1.在路由器的基於Web的實用程式中，按一下Certificate Table下的Import Certificate按鈕

o

Certificate Table						
	Index	Certificate	Used By	Type	Signed By	Duration
<input type="checkbox"/>	1	Default	WebServer	Local Certificate	Self Signed	From 2012-07-12,00:00:00 To 2042-07-05,00:00:00
<input type="checkbox"/>	2	FindIT	-	Local Certificate	Self Signed	From 2017-07-14,00:00:00 To 2018-07-09,00:00:00
<input type="checkbox"/>	3	34xRouter	-	Certificate Signing Request	-	-

Delete Export Detail Import

Import Certificate Generate CSR/Certificate

步驟2.在 *Import Certificate* 視窗中，按一下 *Type* 下拉式功能表並選擇 *CA Certificate*。

Import Certificate

Type Local Certificate
CA Certificate

Certificate Name PKCS#12 encoded file

步驟3.在所提供的欄位中輸入證書名稱。

Import Certificate

Type CA Certificate

Certificate Name **RV34xCert**

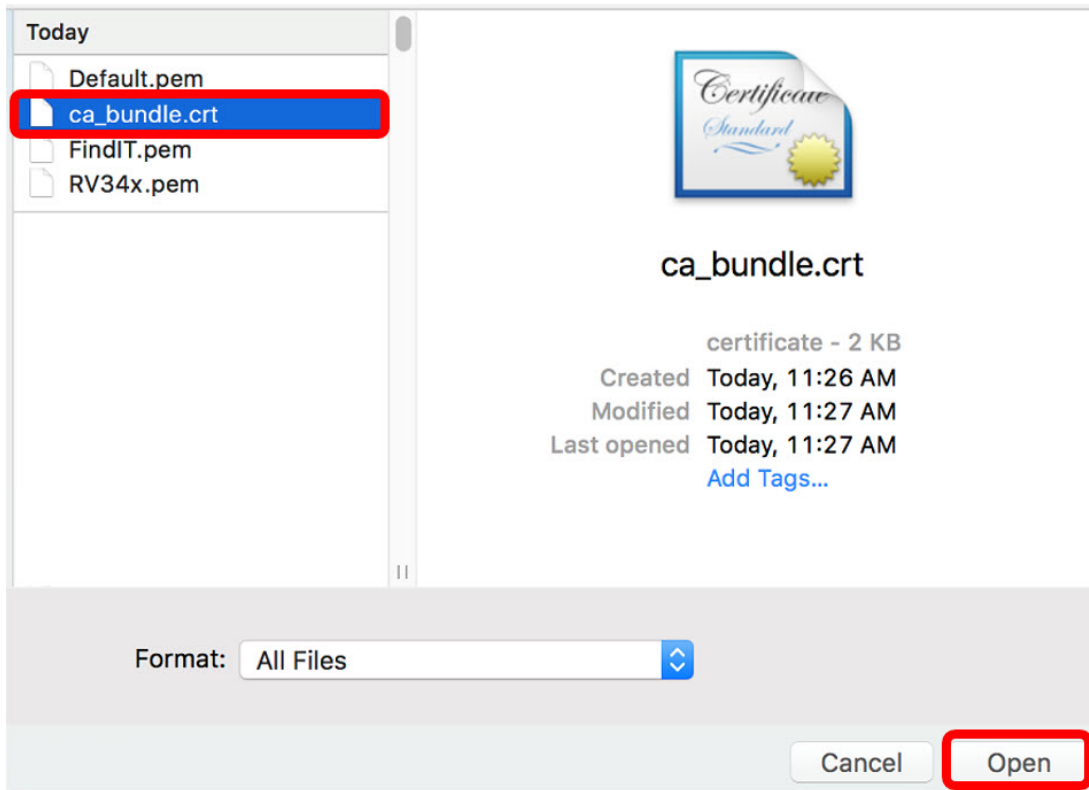
附註：本示例使用RV34xCert。

步驟4.按一下 **Choose File** 按鈕，並找到您從CA下載的憑證檔案。

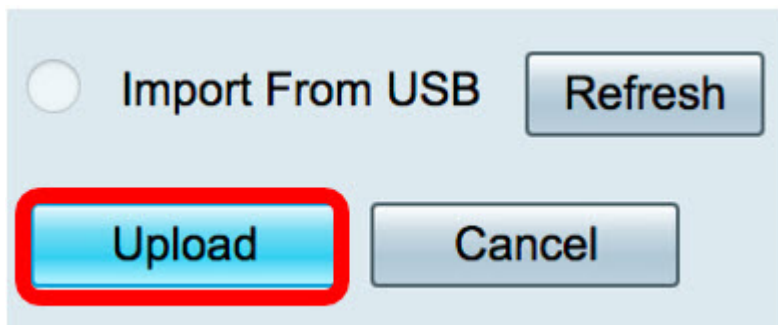
Import From PC

Choose File No file chosen

步驟5.按一下檔案，然後按一下 **Open**。



步驟6. 按一下Upload。



「證書表」現在將顯示新證書名稱，該型別現在將替換為CA證書，該證書帶有由第三方CA簽名的標籤。

Certificate Table						
	Index	Certificate	Used By	Type	Signed By	Duration
<input type="checkbox"/>	1	Default	WebServer	Local Certificate	Self Signed	From 2012-07-12,00:00:00 To 2042-07-05,00:00:00
<input type="checkbox"/>	2	FindIT	-	Local Certificate	Self Signed	From 2017-07-14,00:00:00 To 2018-07-09,00:00:00
<input checked="" type="checkbox"/>	3	RV34xCert	-	CA Certificate	DST Root CA X3	From 2016-03-17,00:00:00 To 2021-03-17,00:00:00

Buttons: Delete, Export, Detail, Import, Import Certificate, Generate CSR/Certificate

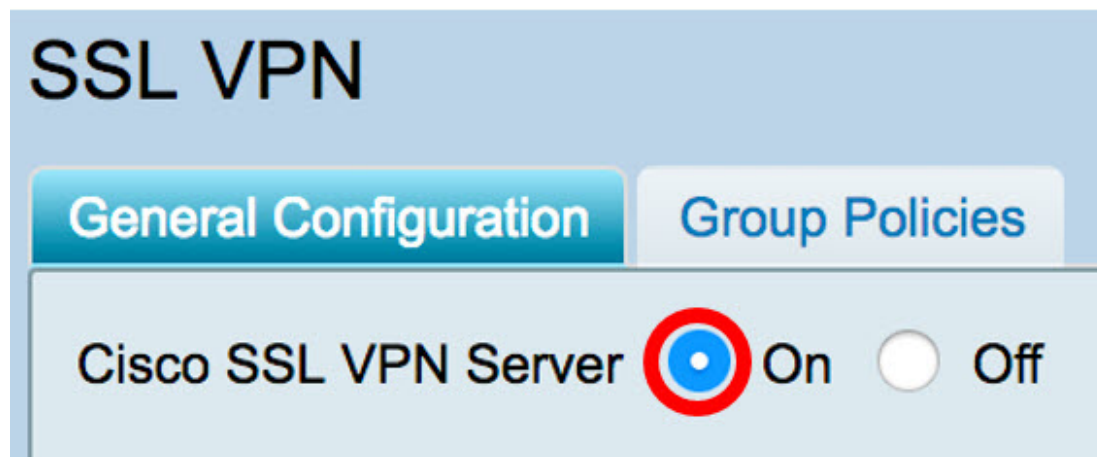
現在，您已成功在RV³⁴x路由器上上傳第三方SSL證書。

替換預設自簽名證書

步驟1.在基於Web的實用程式中，選擇VPN > SSL VPN。



步驟2.按一下On單選按鈕啟用Cisco SSL VPN伺服器。



步驟3.在Mandatory Gateway Settings下，點選Certificate File下拉選單，然後選擇新上傳的SSL證書來替換預設證書。

Mandatory Gateway Settings

Gateway Interface	WAN1
Gateway Port	8443 (Range: 1-65535)
Certificate File	✓ Default FindIT
Client Address Pool	RV34xCert

步驟4. 在提供的欄位中輸入所需的客戶端域。

Certificate File	RV34xCert
Client Address Pool	192.168.10.0
Client Netmask	255.255.255.0
Client Domain	RVrouter.com

附註：在此示例中，使用RVrouter.com。

步驟5. 按一下Apply。

Apply	Cancel
-------	--------

現在，您已成功地將預設自簽名證書替換為^第三方SSL證書。

您也可以參閱以下文章：[RV34x系列路由器常見問題\(FAQ\)](#)

此網站提供多個指向您可能感興趣的其他文章的連結：[RV34x系列路由器產品頁](#)