管理RV34x系列路由器上的證書

目標

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。

讓我們討論如何從證書頒發機構(CA)獲取證書。CA用於身份驗證。可以從任意數量的第三方站點購買證書。這是證明您的站點安全的官方方式。實質上，CA是受信任的來源，用於驗證您的企業是否合法以及是否值得信任。根據您的需要，以最低成本獲得證書。您會由CA簽出，他們驗證您的資訊後，會向您頒發證書。此證書可以作為檔案下載到您的電腦上。然後，您可以進入您的路由器（或VPN伺服器）並上傳到那裡。

本文的目的是向您展示如何在RV34x系列路由器上生成、匯出和匯入證書。

適用裝置 |軟體版本

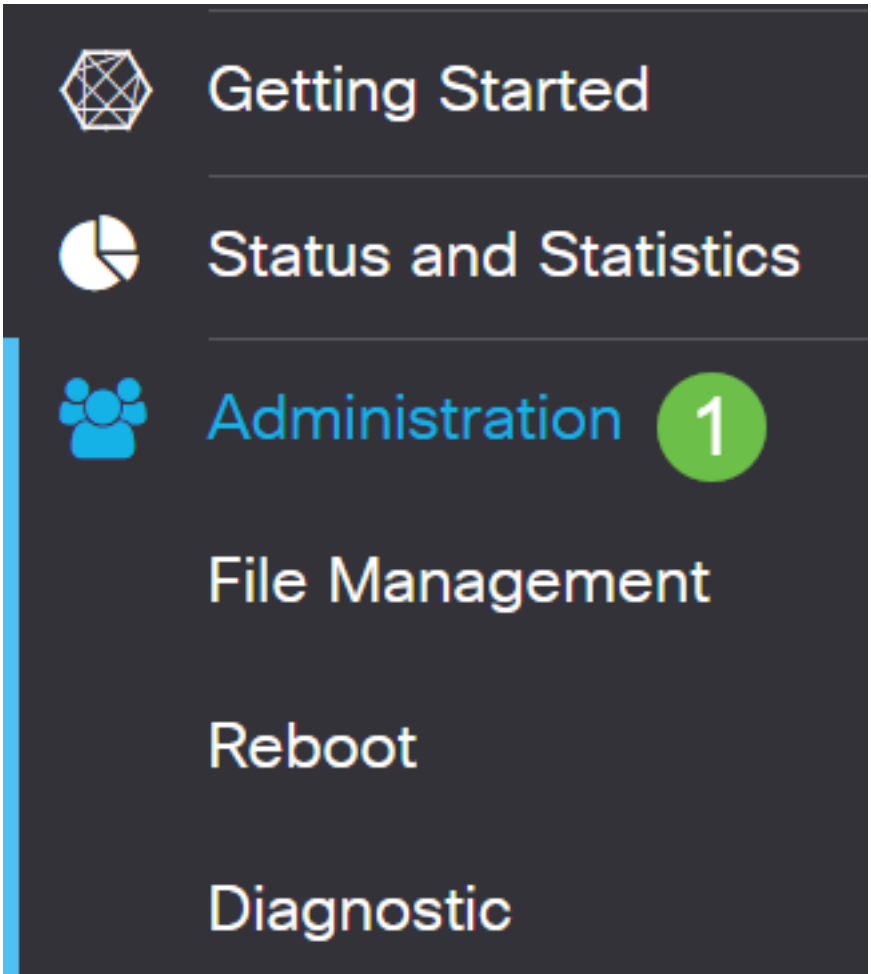
- RV34x系列 | 1.0.03.20

管理路由器上的證書

產生CSR/憑證

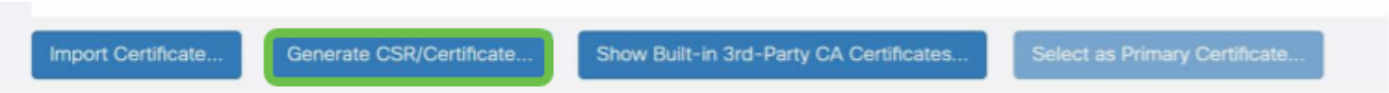
步驟1

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



步驟2

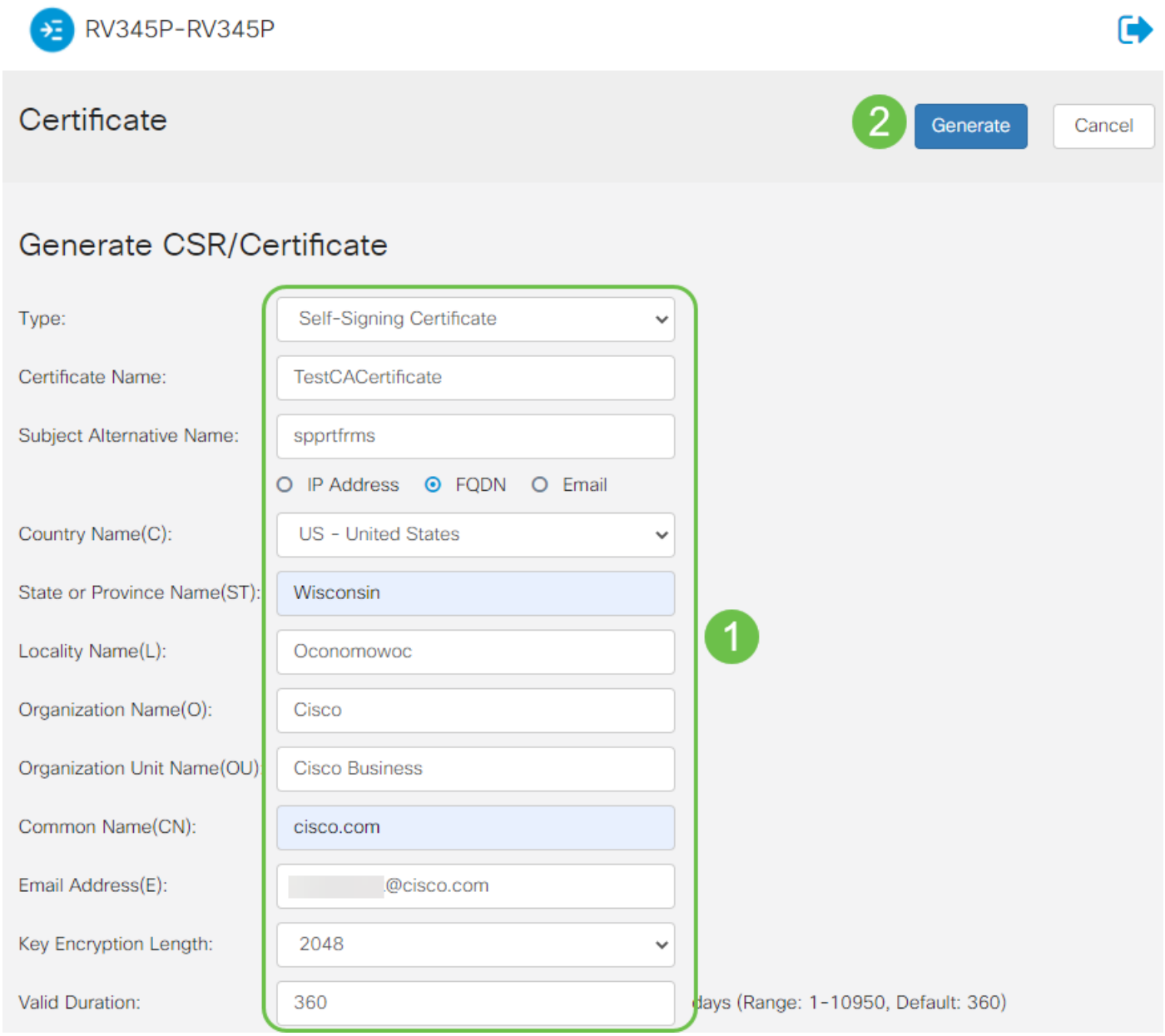
按一下「**Generate CSR/Certificate**」。您將進入「產生CSR/憑證」頁面。



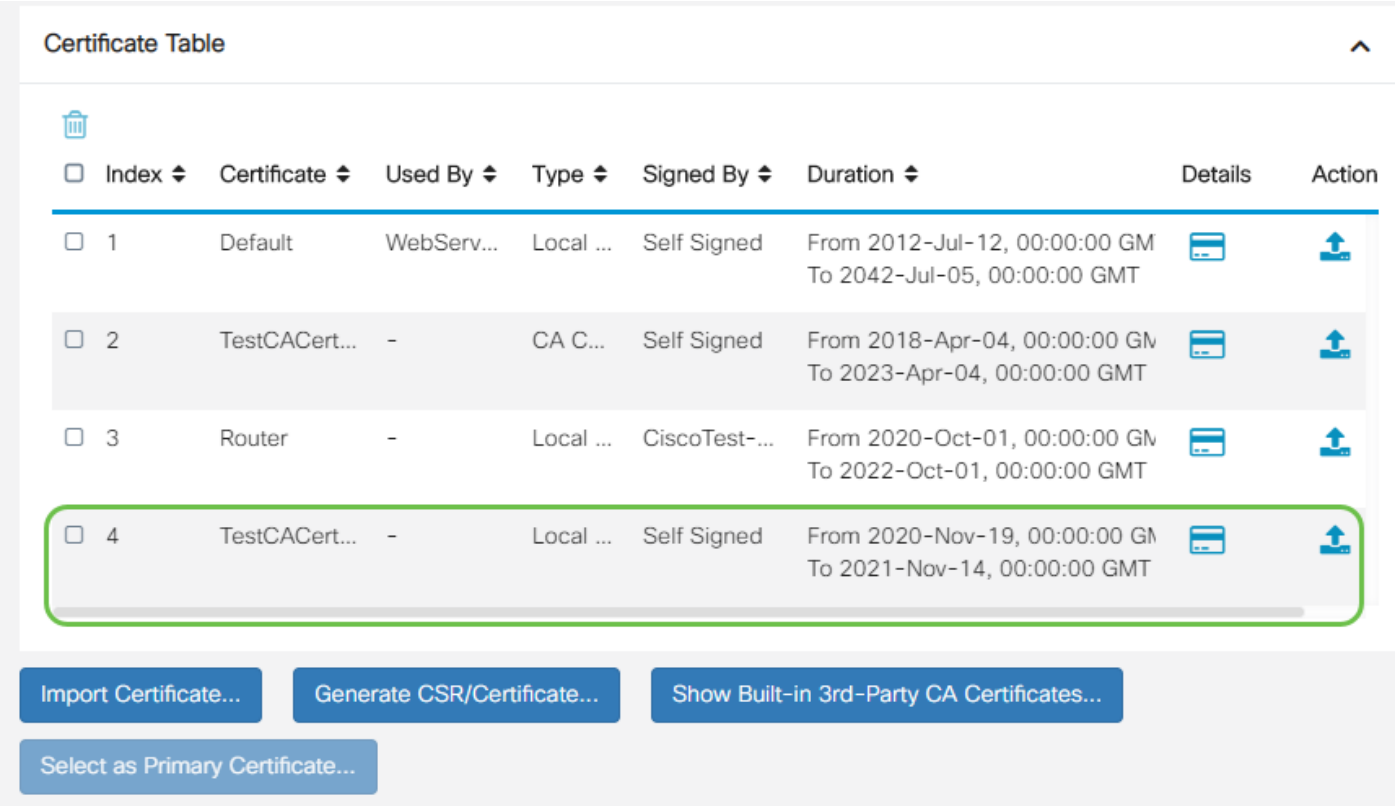
步驟3

在框中填寫以下內容：

- 選擇適當的證書型別
  - 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。此證書不受信任，因為如果攻擊者以某種方式破壞私鑰，則無法取消此證書。
  - 認證簽名請求 — 這是公鑰基礎設施(PKI)，傳送到證書頒發機構以申請數位身份證書。它比自簽名更安全，因為私鑰是保密的。
- 在*Certificate Name*欄位中輸入證書名稱以標識請求。此欄位不能為空，也不能包含空格和特殊字元。
- （可選）在Subject Alternative Name區域下，按一下單選按鈕。選項包括：
  - IP地址 — 輸入網際網路協定(IP)地址
  - FQDN — 輸入完全限定域名(FQDN)
  - 電子郵件 — 輸入電子郵件地址
- 在「*Subject Alternative Name*」欄位中，輸入FQDN。
- 從Country Name下拉選單中選擇組織合法註冊的國家/地區名稱。
- 在「*State or Province Name(ST)*」欄位中輸入組織所在的州、省、地區或地區的名*稱或縮*寫。
- 在*Locality Name*欄位中輸入您的組織註冊或所在的地點或城市的名稱。
- 輸入企業合法註冊的名稱。如果您以小型企業或獨資企業身份註冊，請在「組織名稱」(*Organization Name*)欄位中輸入證書申請者的名稱。不能使用特殊字元。
- 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。
- 在*Common Name*(公用名*稱)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。
- 輸入希望生成證書的人員的電子郵件地址。
- 從Key Encryption Length下拉選單中，選擇金鑰長度。選項為512、1024和2048。金鑰長度越大，證書就越安全。
- 在「*Valid Duration*」欄位中，輸入證書有效的天數。預設值為360。
- 按一下「**Generate**」。



附註：生成的證書現在應該顯示在「證書表」中。

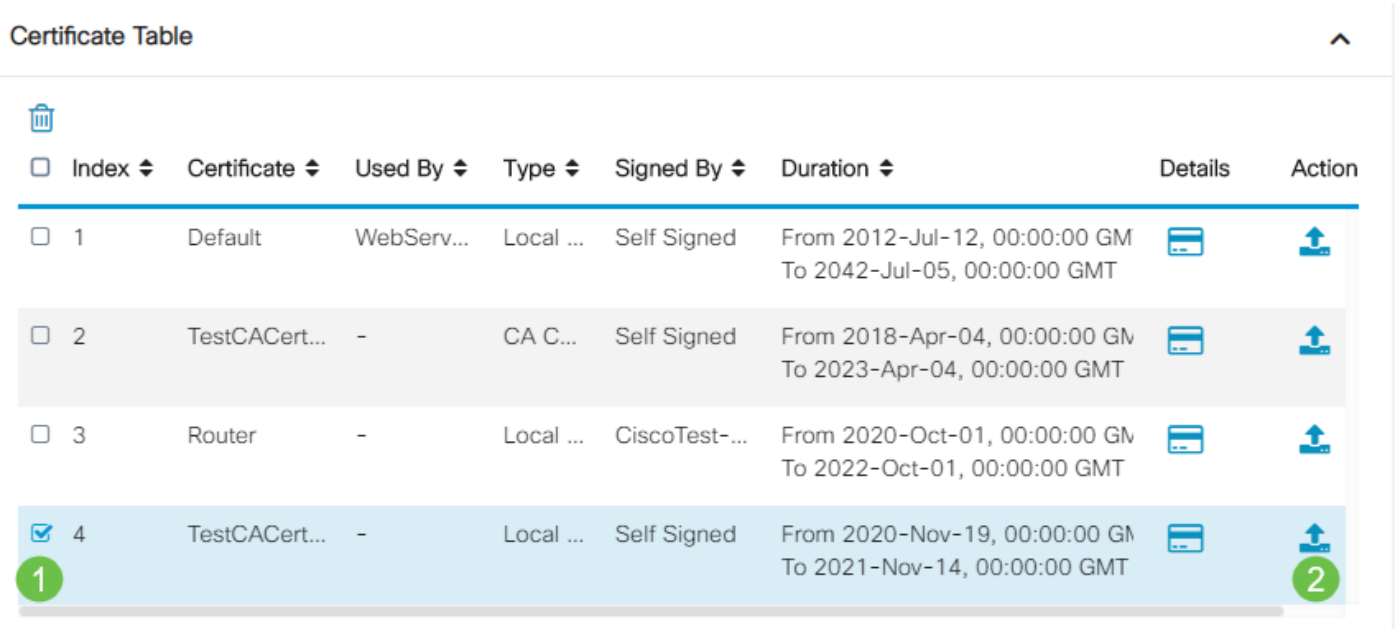


現在，您應該已經在RV345P路由器上成功建立了證書。

匯出證書

步驟1

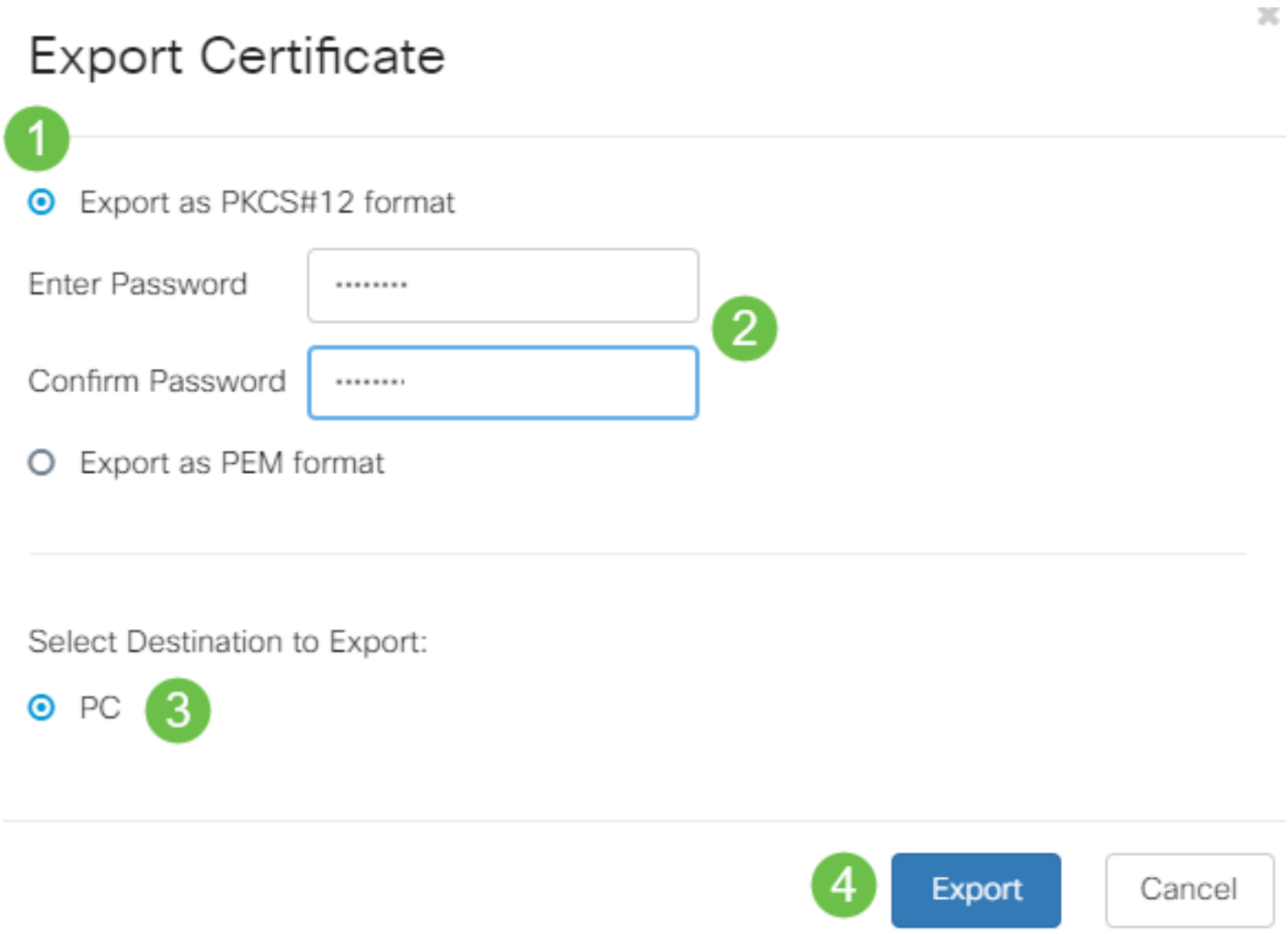
在「證書表」中，選中要匯出的證書的覈取方塊，然後點選**匯出圖示**。



步驟2

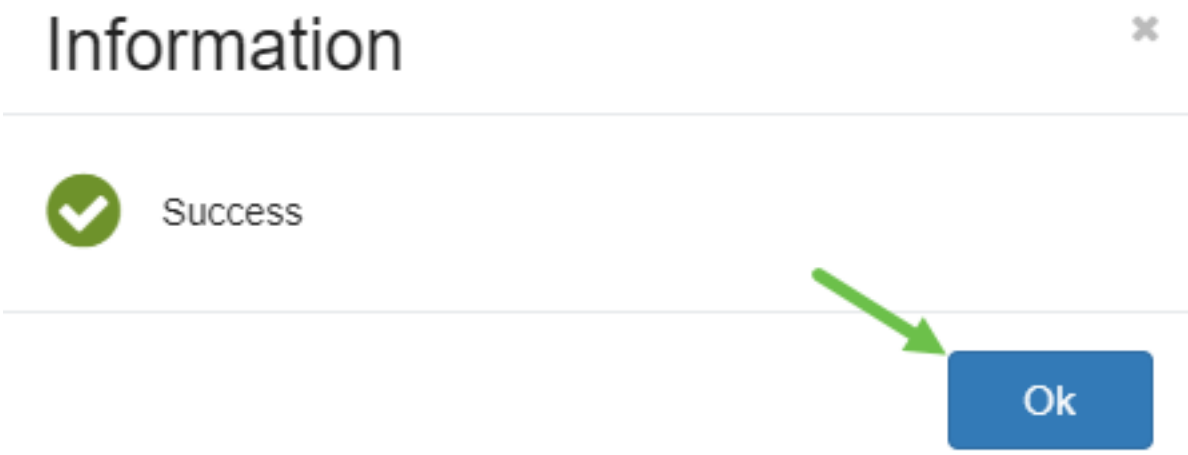
- 按一下格式以匯出證書。選項包括：
  - PKCS #12 — 公鑰加密標準(PKCS)#12是以.p12副檔名提供的匯出證書。需要密碼才能加密檔案，以便在匯出、匯入和刪除檔案時對其進行保護。
  - PEM — 隱私增強型郵件(PEM)通常用於Web伺服器，因為它可以使用記事本等簡單文本編輯器輕鬆轉換為可讀資料。

- 如果您選擇PEM，只需按一下**Export**。
- 在*Enter Password*欄位中輸入密碼以保護要匯出的檔案。
- 在*Confirm Password*欄位中重新輸入密碼。
- 在Select Destination區域，已選擇PC，是目前可用的唯一選項。
- 按一下「**Export**」。



步驟3

「Download（下載）」按鈕下方將顯示一條指示下載成功的消息。檔案將開始在瀏覽器中下載。按一下「**OK**」（確定）。

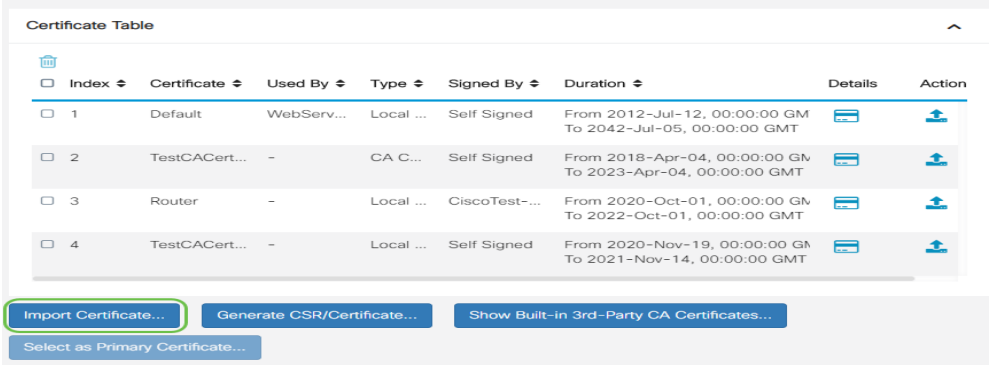


現在，您應該已經在Rv34x系列路由器上成功匯出證書。

匯入證書

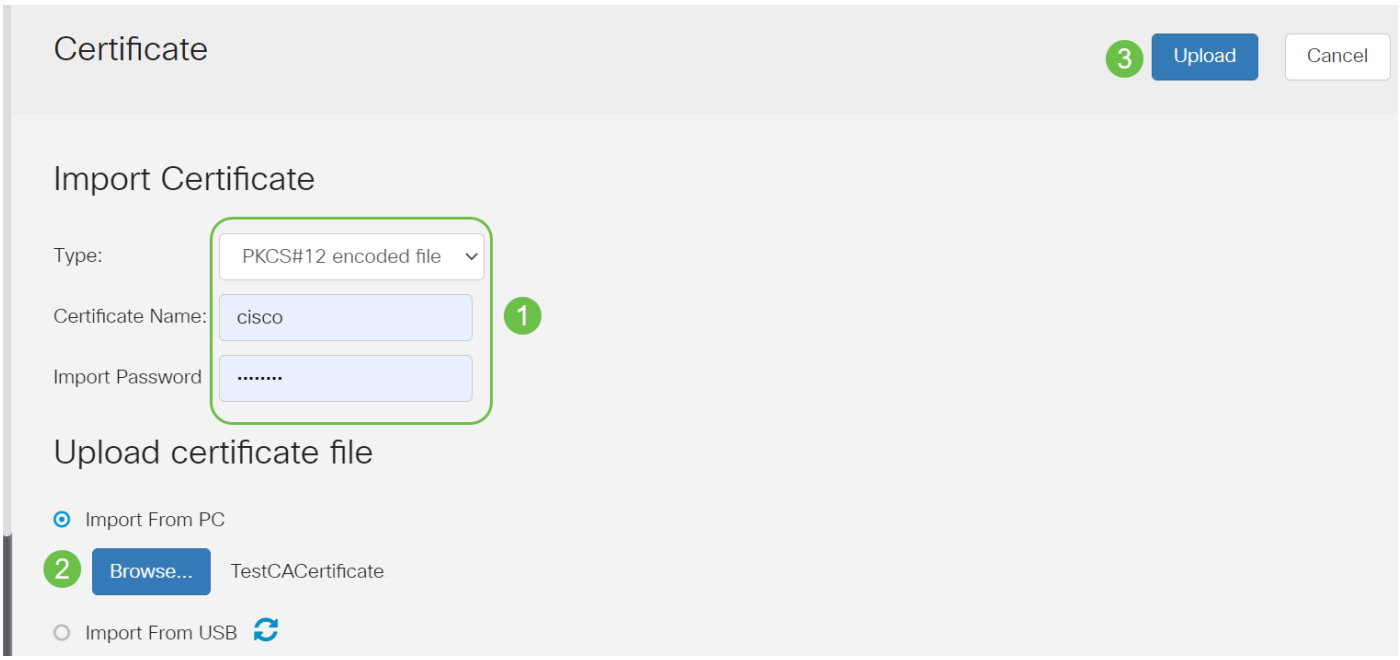
步驟1

按一下**Import Certificate...**。

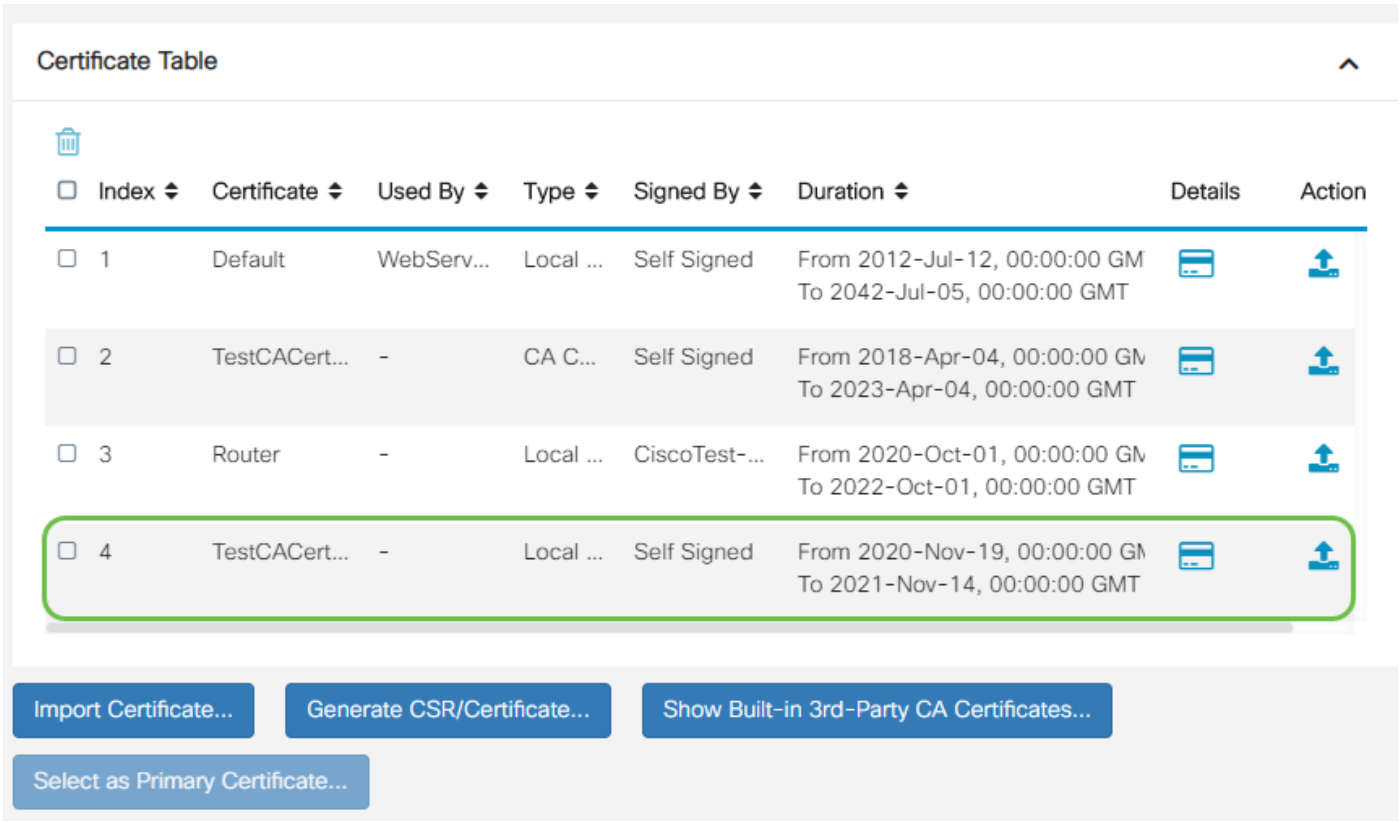


步驟2

- 從下拉選單中選擇要匯入的證書型別。選項包括：
  - 本地證書 — 路由器上生成的證書。
  - CA證書 — 由受信任的第三方頒發機構認證的證書，該第三方頒發機構已確認證書中包含的資訊是準確的。
  - PKCS #12 Encoded file — 公鑰加密標準(PKCS)#12是儲存伺服器憑證的格式。
- 在*Certificate Name*欄位中輸入證書的名稱。
- 如果選擇#12PKCS，請在*Import Password*欄位中輸入該檔案的密碼。否則，請跳至步驟3。
- 按一下某個源以匯入證書。選項包括：
  - 從PC匯入
  - 從USB匯入
- 如果路由器未檢測到USB驅動器，則「從USB匯入」選項將呈灰色顯示。
- 如果您選擇「從USB匯入」，並且路由器無法識別您的USB，請按一下「刷新」。
- 按一下「選擇檔案」按鈕並選擇適當的檔案。
- 按一下「**Upload**」。



成功後，您將自動進入主「證書」頁面。證書表將填充最近匯入的證書。



現在，您應該已經成功地在RV34x系列路由器上匯入了證書。