

RV160和RV260系列路由器上的證書 (匯入/匯出 /生成CSR)

目標

本文的目標是向您展示如何在RV160和RV260系列路由器上生成證書簽名請求(CSR)以及匯入和匯出證書。

簡介

數位證書在通訊過程中非常重要。它為身份驗證提供數字標識。數位證書包括標識裝置或使用者的資訊，如名稱、序列號、公司、部門或IP地址。

證書頒發機構(CA)是「簽署」證書以驗證其真實性的受信任頒發機構，可保證裝置或使用者的身份。它確保證書持有者確實是他們所聲稱的。如果沒有受信任的簽名證書，資料可能會被加密，但您與之通訊的一方可能不是您認為的那方。CA在頒發數位證書時使用公鑰基礎架構(PKI)，它使用公鑰或私鑰加密來確保安全。CA負責管理證書請求和頒發數位證書。CA的一些範例如下：IdenTrust、Comodo、GoDaddy、GlobalSign、GeoTrust、Verisign等等。

證書用於安全套接字層(SSL)、傳輸層安全(TLS)、資料包TLS(DTLS)連線，例如超文本傳輸協定(HTTPS)和安全輕量目錄訪問協定(LDAPS)。

適用裝置

- RV160
- RV260

軟體版本

- 1.0.00.15

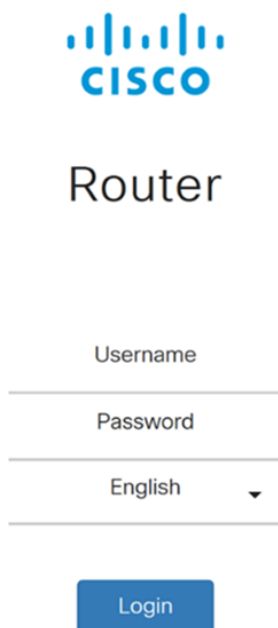
目錄

通過本文您將：

1. [產生CSR/憑證](#)
2. [檢視證書](#)
3. [匯出證書](#)
4. [匯入證書](#)
5. [結論](#)

產生CSR/憑證

步驟1. 登入Web組態頁面。

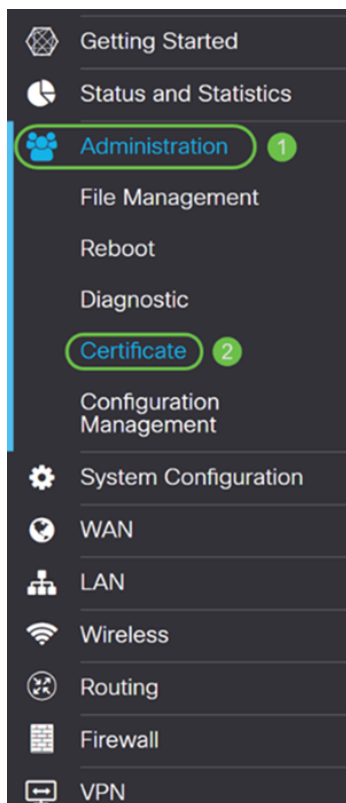


The image shows the Cisco Router login page. At the top is the Cisco logo, followed by the word "Router". Below this are three input fields: "Username", "Password", and a language dropdown menu currently set to "English". A blue "Login" button is positioned below the language dropdown.

©2018 Cisco Systems, Inc. All Rights Reserved.

Cisco, the Cisco Logo, and the Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

步驟2. 導覽至Administration > Certificate。



步驟3. 在Certificate頁面中，按一下Generate CSR/Certificate...按鈕。

Certificate

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
1	Default	NETCONF WebServer RESTCONF	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048- Dec-13, 00:00:00		

Import Certificate... Generate CSR/Certificate... Show built-in 3rd party CA Certificates... Select as Primary Certificate...

步驟4.從下拉選單的以下選項之一中選擇要生成的證書型別。

- **自簽名證書** — 這是由自己的建立者簽署的安全套接字層(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。您必須提供有效的持續時間(天)。
- **CA Certificate** 從安全形度來看，它類似於自簽證書。這可用於OpenVPN。
- **證書簽名請求 (PKI)** 它比自簽名更安全，因為私鑰是保密的。建議使用此選項。
- **CA證書簽名的證書** — 選擇此證書型別並提供相關詳細資訊，以讓您的內部證書頒發機構簽署證書。

在本例中，我們將選擇**Certificate Signing Request**。

Generate CSR/Certificate

Type:

Certificate Name:

Please enter a valid name.

Subject Alternative Name:

IP Address FQDN Email

步驟5.輸入憑證名稱。在本例中，我們將輸入**CertificateTest**。

Type:

Certificate Name:

Subject Alternative Name:

IP Address FQDN Email

步驟6.在 *Subject Alternative Name* 欄位中，選擇以下選項之一：IP Address、**FQDN** (完全限定域名) 或 Email，然後輸入所選內容的適當名稱。此欄位允許您指定其他主機名。

在本示例中，我們將選擇**FQDN**並輸入**ciscoesupport.com**。

Type: Certificate Signing Request

Certificate Name: CertificateTest

Subject Alternative Name: **2** ciscoesupport.com

1 IP Address FQDN Email

步驟7.從Country Name(C)下拉式清單中選擇國家/地區。

Country Name (C): United States

State or Province Name (ST):

Locality Name (L):

Organization Name (O):

Organization Unit Name (OU):

Common Name (CN):

Email Address (E):

Key Encryption Length: 2048

步驟8.在「State or Province Name」欄位中輸入州名或省名。

Country Name (C): United States

State or Province Name (ST): CA

Locality Name (L):

Organization Name (O):

Organization Unit Name (OU):

Common Name (CN):

Email Address (E):

Key Encryption Length: 2048

步驟9.在Locality Name中，輸入city name。

Country Name (C):	<input type="text" value="United States"/>
State or Province Name (ST):	<input type="text" value="CA"/>
Locality Name (L):	<input type="text" value="San Jose"/>
Organization Name (O):	<input type="text"/>
Organization Unit Name (OU):	<input type="text"/>
Common Name (CN):	<input type="text"/>
Email Address (E):	<input type="text"/>
Key Encryption Length:	<input type="text" value="2048"/>

步驟10.在「組織名稱」字段中輸入組織名稱。

Country Name (C):	<input type="text" value="United States"/>
State or Province Name (ST):	<input type="text" value="CA"/>
Locality Name (L):	<input type="text" value="San Jose"/>
Organization Name (O):	<input type="text" value="Cisco"/>
Organization Unit Name (OU):	<input type="text"/>
Common Name (CN):	<input type="text"/>
Email Address (E):	<input type="text"/>
Key Encryption Length:	<input type="text" value="2048"/>

步驟11.輸入組織單位的名稱 (如培訓、支援等)。

在本示例中，我們將輸入eSupport作為我們的組織單位名稱。

Country Name (C):	United States
State or Province Name (ST):	CA
Locality Name (L):	San Jose
Organization Name (O):	Cisco
Organization Unit Name (OU):	eSupport
Common Name (CN):	
Email Address (E):	
Key Encryption Length:	2048

步驟12.輸入公用名稱。將要接收此證書的Web伺服器的FQDN。

在本示例中，**ciscosmbsupport.com** 用作公用名。

Country Name (C):	United States
State or Province Name (ST):	CA
Locality Name (L):	San Jose
Organization Name (O):	Cisco
Organization Unit Name (OU):	eSupport
Common Name (CN):	ciscosmbsupport.com
Email Address (E):	
Key Encryption Length:	2048

步驟13.輸入電子郵件地址。

Country Name (C):	United States
State or Province Name (ST):	CA
Locality Name (L):	San Jose
Organization Name (O):	Cisco
Organization Unit Name (OU):	eSupport
Common Name (CN):	ciscosmbsupport.com
Email Address (E):	k[redacted]@cisco.com
Key Encryption Length:	2048

步驟14.從下拉選單中選擇**Key Encryption Length**。選項包括：512、1024或2048年。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。

最佳實踐：建議選擇最高金鑰加密長度 — 啟用更嚴格的加密。

Country Name (C):	United States
State or Province Name (ST):	CA
Locality Name (L):	San Jose
Organization Name (O):	Cisco
Organization Unit Name (OU):	eSupport
Common Name (CN):	ciscosmbsupport.com
Email Address (E):	k[redacted]@cisco.com
Key Encryption Length:	2048

步驟15.按一下**Generate**。

Generate CSR/Certificate Generate Cancel

Certificate Name:

Subject Alternative Name:
 IP Address FQDN Email

Country Name (C):

State or Province Name (ST):

Locality Name (L):

Organization Name (O):

Organization Unit Name (OU):

Common Name (CN):

Email Address (E):

Key Encryption Length:

步驟16.將顯示Information彈出視窗，其中包含「Generate certificate successfully！」消息。按一下「OK」以繼續。

Information ✕

Generate certificate successfully!

OK

步驟17.從憑證表中匯出CSR。

Certificate Table ▲							
Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
<input checked="" type="radio"/> 1	Default	NETCONF WebServer RESTCONF	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048- Dec-13, 00:00:00		
<input type="radio"/> 2	CertificateTest	-	Certificate Signing Request	-	-		

Import Certificate...
Generate CSR/Certificate...
Show built-in 3rd party CA Certificates...
Select as Primary Certificate...

步驟18.出現Export Certificate視窗。為Export to選擇PC，然後按一下Export。

Export Certificate



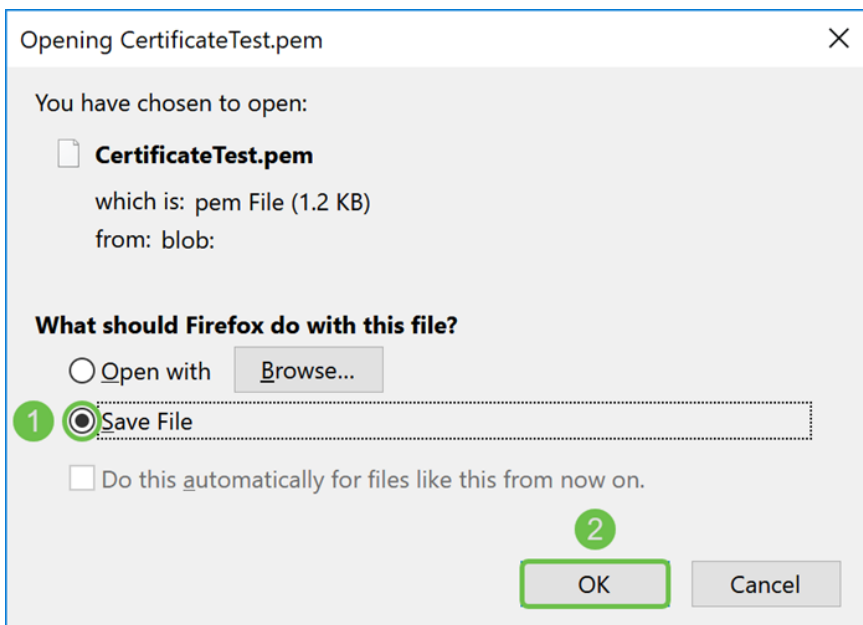
Export as PEM format

Export to:



步驟19.應出現另一視窗，詢問是開啟還是儲存檔案。

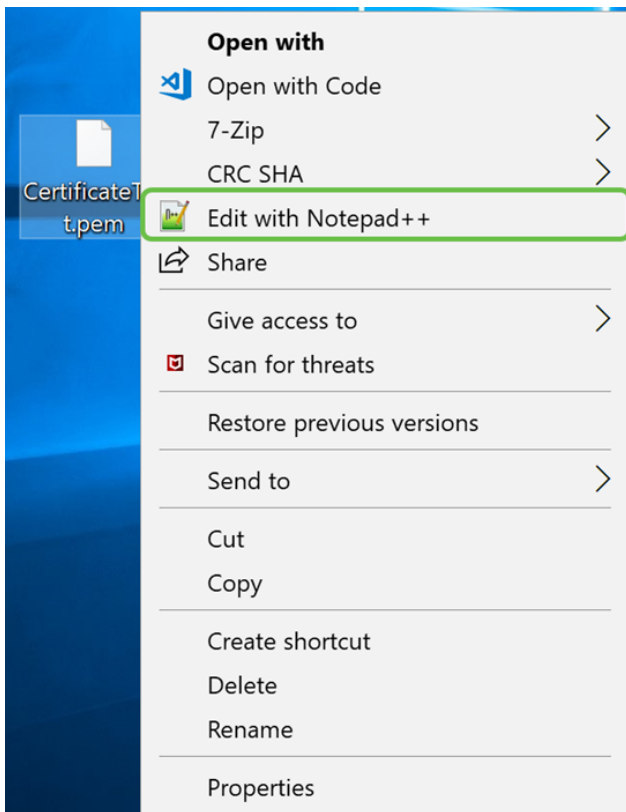
在本例中，我們將選擇**Save File**，然後按一下**OK**。



步驟20.查詢.pem檔案儲存的位置。按一下右鍵.pem檔案並使用您喜歡的文本編輯器將其開啟。

在本例中，我們將使用記事本++開啟.pem檔案。

附註：使用記事本隨時開啟。



步驟21.確保----**BEGIN CERTIFICATE REQUEST**---- 和 ----**END CERTIFICATE REQUEST**位於自己的行上。

附註：證書的某些部分被模糊了。

```
CertificateTest.pem x
1 -----BEGIN CERTIFICATE REQUEST----- 1
2 [blurred] VBAYTA1VTMQSwCQYDVQQIDAJDQTERMA8GA1UE
3 BwwIU2FuIEpvc2UxDjAMBgNVBAoMBUNpc2NmREwDwYDVQLDAh1U3VwcG9ydDEC
4 MBoGA1UEAwTY2lzMzY2Y29zbWJzdXBwb3J0 [blurred]
5 eWVuQGNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ/r
6 J02/H2TfmIrv1vcs0c+tXmvt8PpCcCFuEaoEvdCcV6kP+TaeDmndcgIdDXNRXplu
7 wSyiqrpS8+kbhzPTF8sHO94Q8wyA8mEu/SjYs0DWuqa2+3LafOLlp8Cg+e3l0cjs
8 VJS8efDI5j1ECMABvB5Tv [blurred]
9 soTqNBrYqR8h46NHh0J5fMXDsPYlj2LWmS1VbkskoiMdr5SZlwmhkrqqLby+bfma
10 eOhl0DyX3D7xTV14tvzxYrmDilmpr1eLQc9zME/bZqZgTgY5MgSTGPAis27m29PR
11 oZK/Rpg6Scywbx1X/G0CAwEAAACBkTCBjgYJKoZIhvcNAQkOMYGAMH4wCQYDVR0T
12 BA1w [blurred].gXg
13 MCcGA1UdJQQgMB4GCCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUIAgIwHAYDVR0R
14 BBUwE4IRY2lzMzY2Y29lc3VwcG9ydC5jb20wDQYJKoZIhvcNAQELBQADggEBAI1UeIUy
15 TqFZ2wQx3r29E1SWOU5bmqCj+9IfrsFLR909VdAIJXoUP16CJtc4JJy5+XEhYSnu
16 [blurred]
17 [blurred]
18 [blurred]
19 [blurred]
20 [blurred]
21 -----END CERTIFICATE REQUEST----- 2
22 [blurred]
```

步驟22.當您擁有CSR時，您需要前往您的託管服務或證書頒發機構站點（即GoDaddy、Verisign等）並請求證書。提交請求後，它將與證書伺服器通訊，以確保沒有任何原因不頒發證書。

附註：如果您不知道證書請求在其網站上的位置，請與CA或託管網站支援聯絡。

步驟23.憑證完成後立即下載。它應該是.cer或.crt檔案。在本例中，我們獲得了這兩個檔案。

Name	Date modified	Type	Size
CertificateTest.cer	4/10/2019 2:03 PM	Security Certificate	2 KB
CertificateTest.crt	4/10/2019 2:04 PM	Security Certificate	3 KB

步驟24. 返回路由器的 *Certificate* 頁面，然後按一下指向裝置圖示的箭頭匯入證書檔案。

Certificate Table

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
<input checked="" type="radio"/> 1	Default	NETCONF WebServer RESTCONF	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048- Dec-13, 00:00:00		
<input type="radio"/> 2	CertificateTest	-	Certificate Signing Request	-	-		

步驟25. 在「*Certificate Name*」欄位中，輸入 **certificate name**。不能與證書簽名請求同名。在 *Upload Certificate file* 部分，選擇 **import from PC**，然後按一下 **Browse...** 以上傳證書檔案。

Import Signed-Certificate

Type: Local Certificate

Certificate Name: 1

Upload Certificate file

2

Import from PC

3

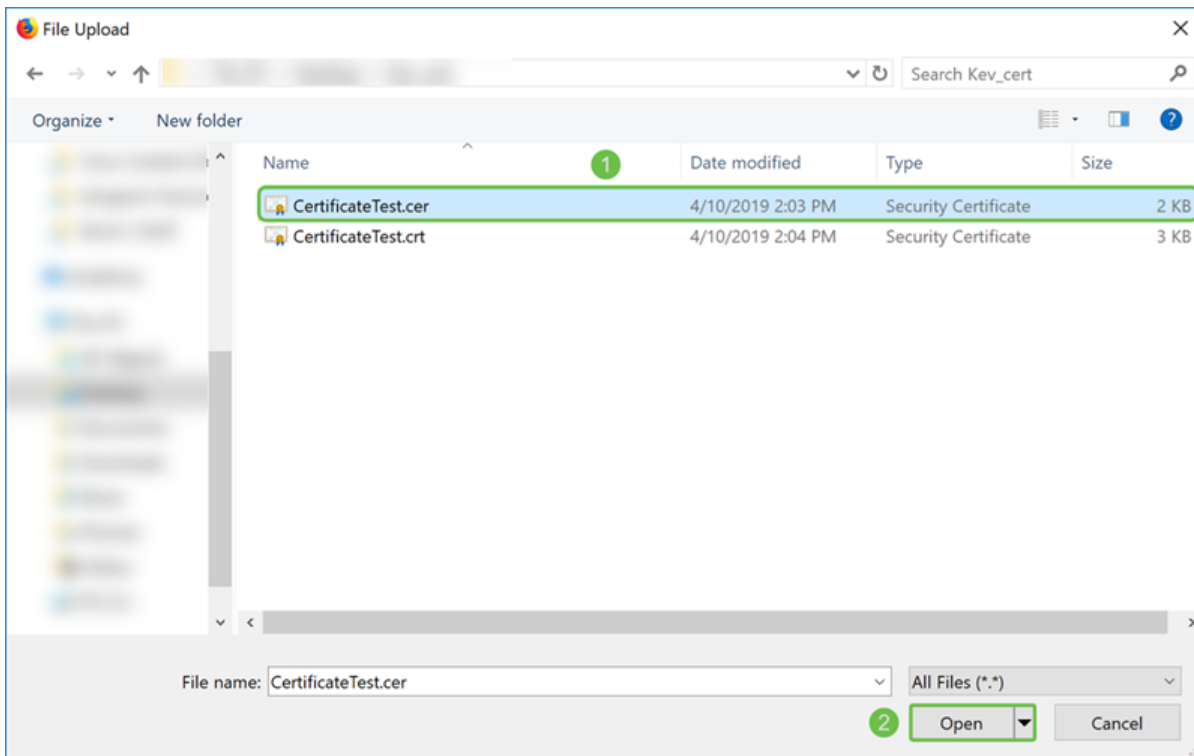
No file is selected

Import from USB



No file is selected

步驟26. 出現 *File Upload* 視窗。導航到證書檔案的位置。選擇要上傳的憑證檔案，然後按一下 **Open**。在本示例中，選擇了 **CertificateTest.cer**。



步驟27.按一下**Upload**按鈕，開始將憑證上傳到路由器。

附註：如果您在無法上傳.cer檔案時收到錯誤，則可能是因為您的路由器要求憑證採用pem編碼。您將需要將der編碼（.cer副檔名）轉換為pem編碼（.crt副檔名）。

Import Signed-Certificate



Type: Local Certificate

Certificate Name: CiscoSMB

Upload Certificate file

Import from PC

Browse...

CertificateTest.cer

Import from USB



Browse...

No file is selected

Upload

Cancel






步驟28.如果匯入成功，應顯示資訊視窗，告知您匯入成功。按一下「OK」以繼續。

 Import certificate successfully!

OK

步驟29.您的憑證應成功更新。您應該能夠看到您的證書是由誰簽名的。在本例中，我們可以看到我們的憑證是由CiscoTest-DC1-CA簽署。若要使證書成為我們的主要證書，請使用左側的單選按鈕選擇證書，然後按一下選擇為主要證書.....按鈕。

Certificate Table

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action	
<input type="radio"/>	1	Default	NETCONF WebServer RESTCONF	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048- Dec-13, 00:00:00		
<input checked="" type="radio"/>	2	CiscoSMB	-	Local Certificate	CiscoTest- DC1-CA	From 2019-Apr-10, 00:00:00 To 2021- Apr-09, 00:00:00		 

Import Certificate... Generate CSR/Certificate... Show built-in 3rd party CA Certificates... **Select as Primary Certificate...**

附註：更改主證書可能會使您返回到警告頁面。如果您使用的是Firefox，並且它會顯示為灰色空白頁面，則需要在Firefox上調整某些配置。Mozilla wiki上的本文檔對此進行了一些解釋：[CA/AddRootToFirefox](#)。為了能夠再次看到警告頁面，請執行在[Mozilla社群支援頁面](#)中找到的以下步驟。

步驟30.在Firefox警告頁面中，按一下Advanced...，然後按一下Accept the Risk and Continue以繼續返回路由器。

附註：這些警告螢幕因瀏覽器而異，但執行相同的功能。



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to 192.168.2.1. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

[Learn more...](#)

Go Back (Recommended)

Advanced...

Websites prove their identity via certificates. Firefox does not trust this site because it uses a certificate that is not valid for 192.168.2.1. The certificate is only valid for ciscoesupport.com.

Error code: SEC_ERROR_UNKNOWN_ISSUER

[View Certificate](#)

Go Back (Recommended)

Accept the Risk and Continue

步驟31。在憑證表中，您應該會看到NETCONF、WebServer和RESTCONF已交換到您的新憑證，而不是使用Default憑證。

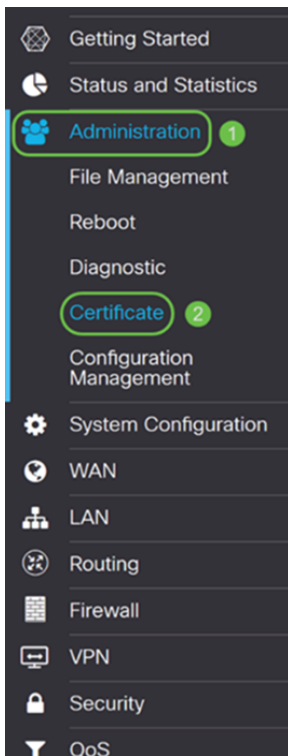
Certificate Table

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
1	Default	-	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048-Dec-13, 00:00:00		
2	CiscoSMB	NETCONF WebServer RESTCONF	Local Certificate	CiscoTest-DC1-CA	From 2019-Apr-10, 00:00:00 To 2021-Apr-09, 00:00:00		

現在，您應該已經成功地將證書安裝到路由器上。

檢視證書

步驟1。如果您已導航離開Certificate頁面，請導航到Administration > Certificate。



步驟2.在 *Certificate Table* 中，按一下 **Details** 部分底下的 **Details** 圖示。

Certificate Table

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
1	Default	-	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048-Dec-13, 00:00:00		
2	CiscoSMB	NETCONF WebServer RESTCONF	Local Certificate	CiscoTest-DC1-CA	From 2019-Apr-10, 00:00:00 To 2021-Apr-09, 00:00:00		

步驟3.顯示 *Certificate Detail* 頁面。您應該能夠看到有關憑證的所有資訊。

Certificate Detail

Name: CiscoSMB
Country: US
State Province: CA
Subject Alternative Name: ciscoesupport.com
Subject Alternative Type: Fqdn-Type
Subject-DN: C=US,ST=CA,L=San Jose,O=Cisco,OU=eSupport,CN=ciscosmbsupport.com,emailAddress=k[redacted]@cisco.com
Locality: San Jose
Organization: Cisco
Organization Unit Name: eSupport
Common: ciscosmbsupport.com
Email: k[redacted]@cisco.com
Key Encryption Length: 2048

Close

步驟4.按一下位於Uniform Resource Locator(URL)欄左側的lock圖示。

附註：以下步驟在Firefox瀏覽器中使用。

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
1	Default	-	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048-Dec-13, 00:00:00		
2	CiscoSMB	NETCONF WebServer RESTCONF	Local Certificate	CiscoTest-DC1-CA	From 2019-Apr-10, 00:00:00 To 2021-Apr-09, 00:00:00		

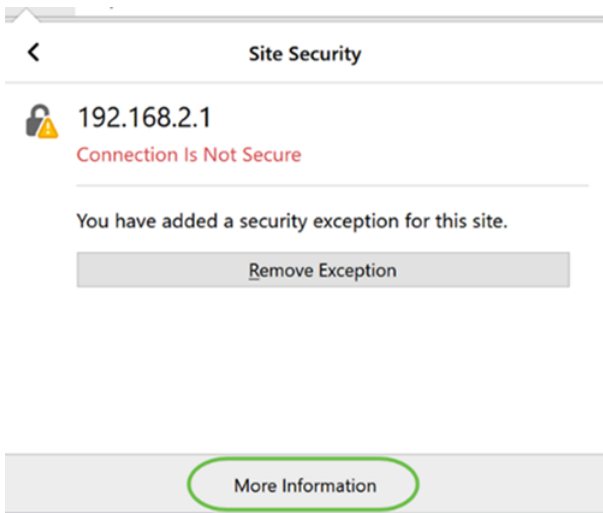
步驟5.系統會顯示選項下拉選單。按一下Connection欄位旁邊的箭頭圖示。

Site Information for 192.168.2.1

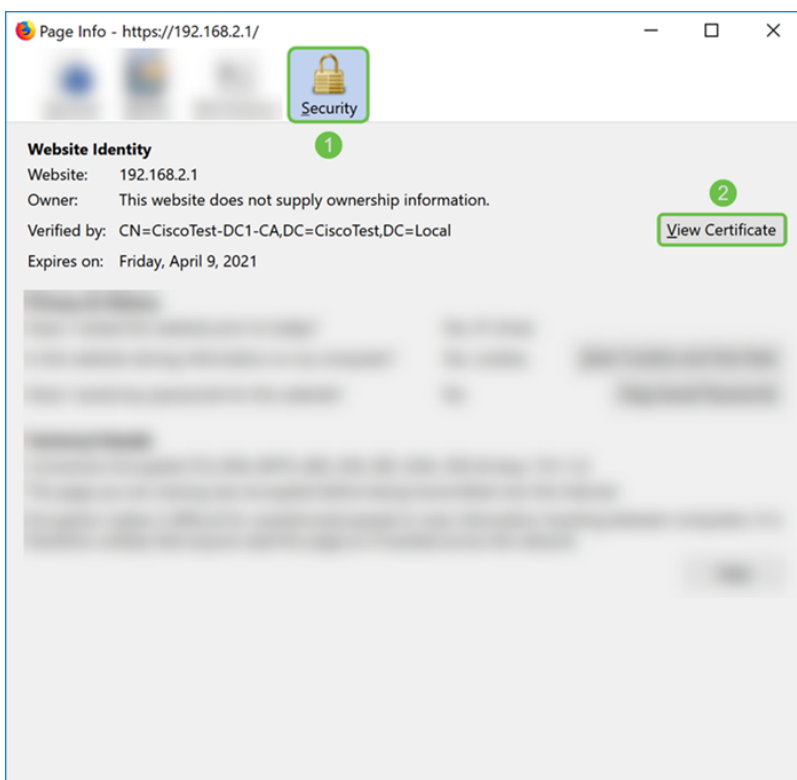
- Connection** >
Connection Is Not Secure
- Content Blocking** Standard ⚙️
Blockable content detected on this site.
- Cookies** >
- Permissions** ⚙️
You have not granted this site any special permissions.

Clear Cookies and Site Data...

步驟6.按一下More Information。

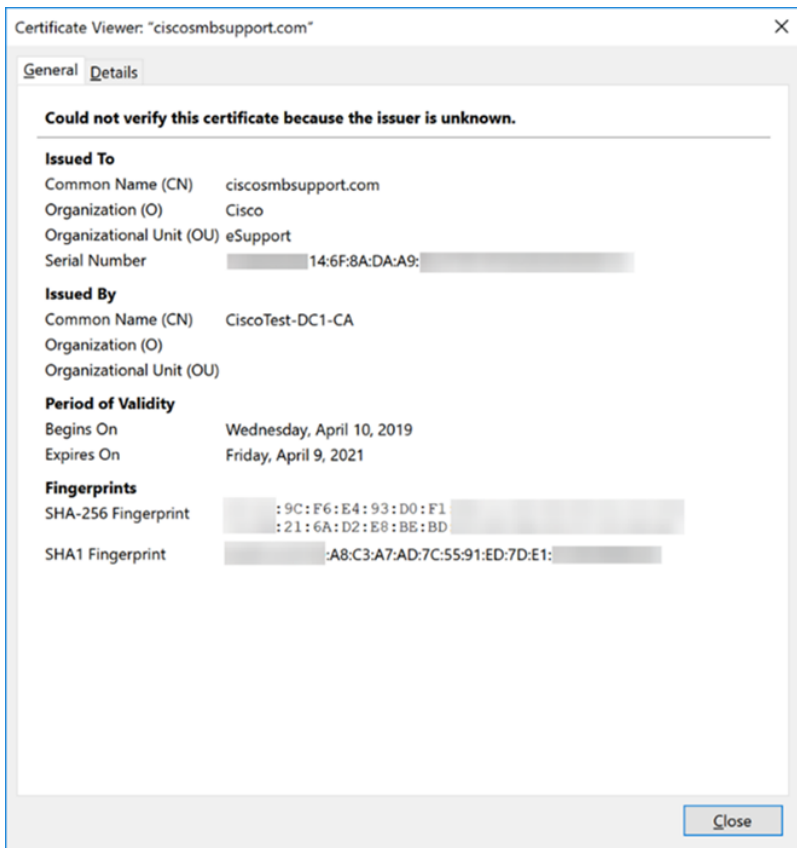


步驟7.在 *Page Info* 視窗中，您應該能夠在 *Website identity* 部分看到有關證書的簡短資訊。確保您位於 **Security** 索引標籤中，然後按一下 **View Certificate** 以檢視有關您的憑證的詳細資訊。



步驟8.應該會顯示 *Certificate Viewer* 頁面。您應該能夠看到有關您的證書、有效期、指紋以及頒發者的所有資訊。

附註：由於此證書是由測試證書伺服器頒發的，頒發者未知。



匯出證書

要下載證書以將其匯入另一台路由器上，請按照以下步驟操作。

步驟1。在 *Certificate* 頁面中，按一下您要匯出的憑證旁邊的 **export** 圖示。

Certificate Table

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
○ 1	Default	-	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048-Dec-13, 00:00:00		
● 2	CiscoSMB	NETCONF WebServer RESTCONF	Local Certificate	CiscoTest-DC1-CA	From 2019-Apr-10, 00:00:00 To 2021-Apr-09, 00:00:00		

步驟2.顯示 **匯出憑證**。選擇匯出證書的格式。選項包括：

• **PKCS#12** – Πύβλιχ Κεψ Χρψπητογραπηψ Στανδαρδσ(ΠΚΧΣ)#12.π12 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** (ΠΕΜ)Ωεβ

選擇 **Export as PKCS#12 format**，並輸入 **password** 和 **confirm password**。然後選擇 **PC** 作為 **Export to:** 欄位。按一下 **Export** 開始將證書匯出到電腦。

附註：請記住此密碼，因為在將其匯入到路由器時將使用該密碼。

Export Certificate



1

Export as PKCS#12 format

Enter Password:

2

Confirm Password:

Export as PEM format

Export to:

3

PC USB

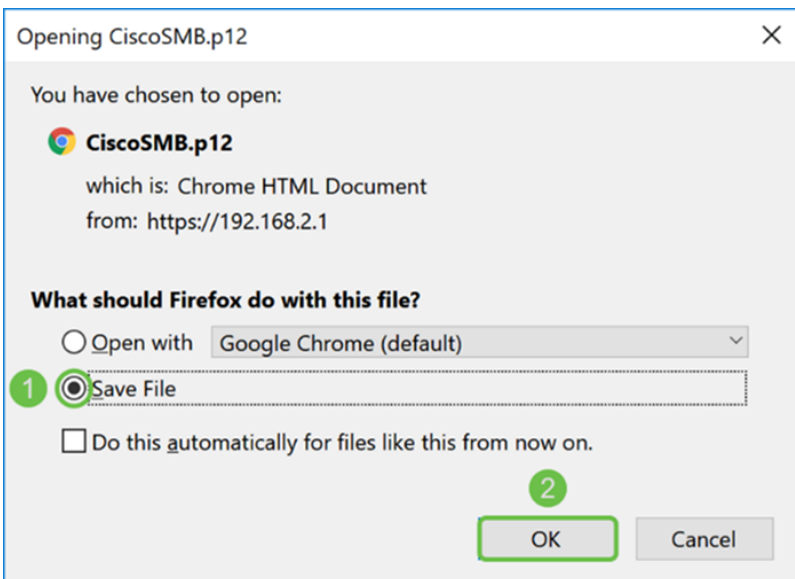


4

Export

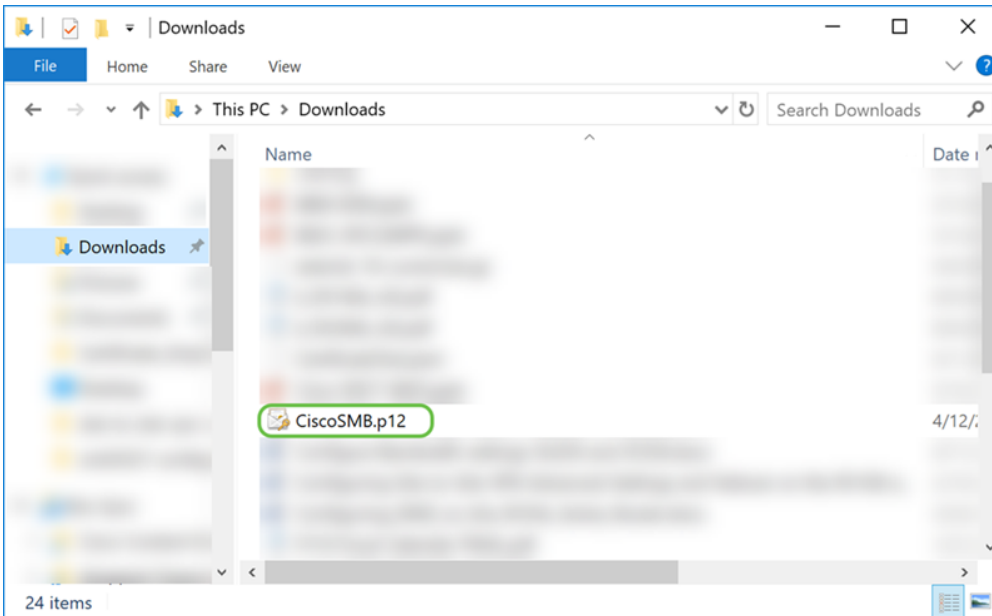
Cancel

步驟3.將出現一個視窗，詢問您應該如何處理此檔案。在本例中，我們將選擇**Save File**，然後按一下**OK**。



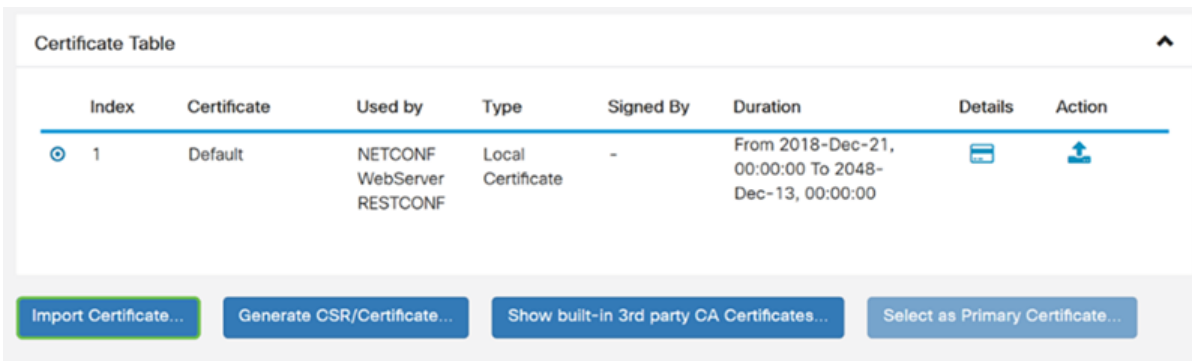
步驟4.檔案應儲存到預設儲存位置。

在我們的示例中，檔案已儲存到電腦上的 *Downloads* 資料夾中。



匯入證書

步驟1。在 *Certificate* 頁面中，按一下 **Import Certificate...** 按鈕。



步驟2。從 *Import Certificate* 部分的 *Type* 下拉式清單中選擇要匯入的證書型別。選項定義如下：

- CA證書
- Local Device Certificate
- PKCS#12 Encoded File – Πυβλιχ Κεψ Χρηππογραπηψ Στανδαρδσ(ΠΚΧΣ)#12.π12

在本示例中，選擇PKCS#12 Encoded File 作為型別。輸入憑證的名稱，然後輸入使用的密碼。

Import Certificate

Type: 1


Certificate Name: 2

Import Password: 3

Upload Certificate file

Import from PC

No file is selected

Import from USB 

No file is selected

步驟3.在 *Upload Certificate file* 部分下，選擇 **Import from PC** 或 **Import from USB**。在本示例中，**Import from PC**被選中。按一下 **Browse...**以選擇要上傳的檔案。

Import Certificate

Type:


Certificate Name:

Import Password:

Upload Certificate file

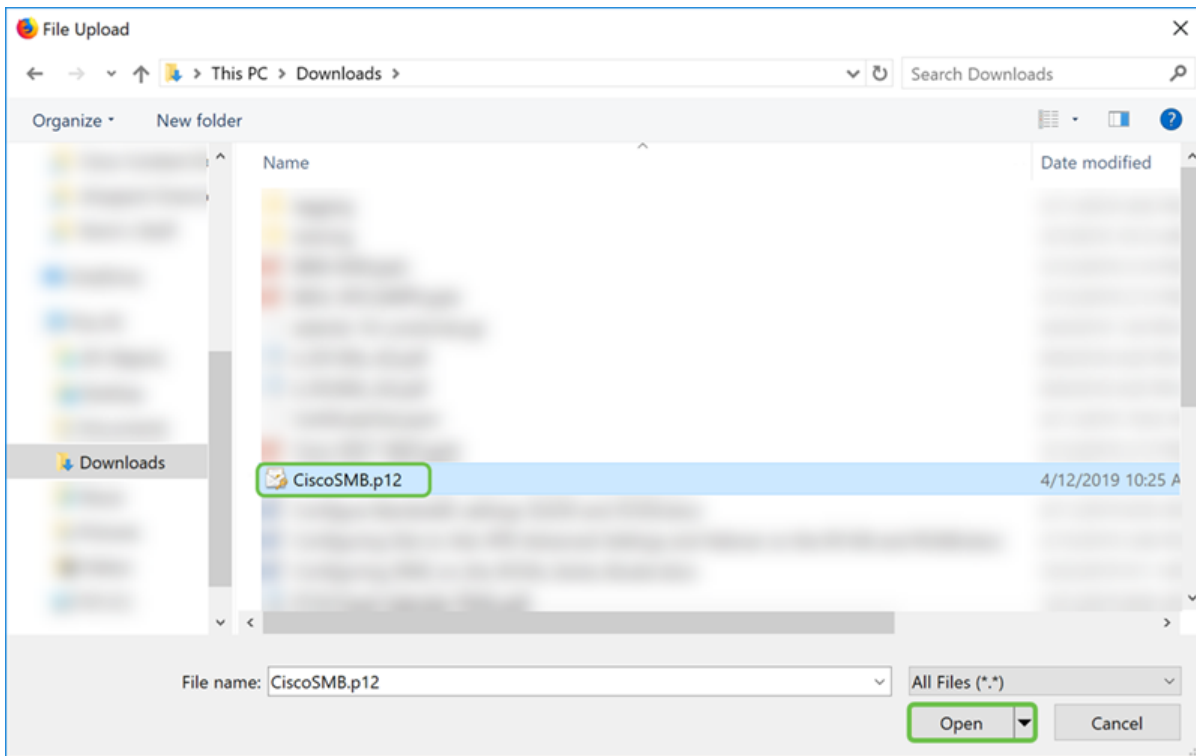
Import from PC

No file is selected

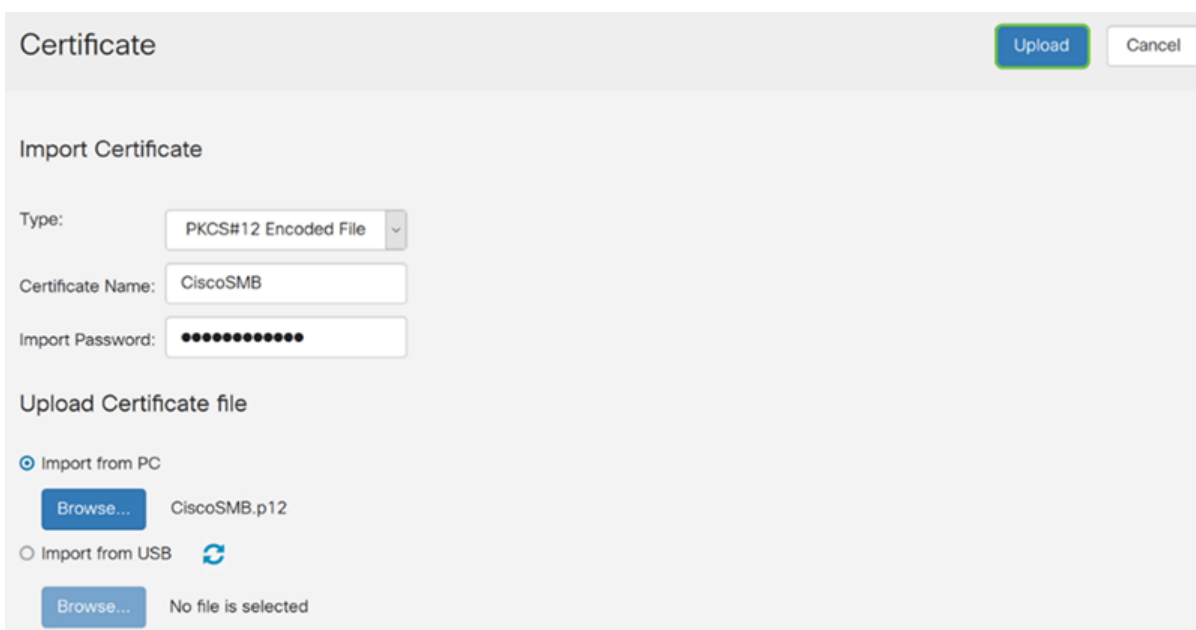
Import from USB 

No file is selected

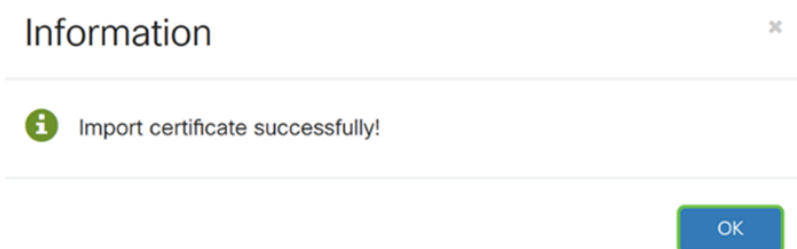
步驟4.在 *File Upload* 視窗中，導航到PKCS#12編碼檔案 (.p12副檔名) 所在的位置。選擇。**p12檔案**，然後按一下 **開啟**。



步驟5.按一下**Upload**以開始上傳憑證。







步驟6.將出現資訊視窗，讓你知道您的憑證已順利匯入。按一下**OK**繼續。



步驟7.您應該會看到您的憑證已上傳。

Certificate Table

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
<input checked="" type="radio"/> 1	Default	NETCONF WebServer RESTCONF	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048- Dec-13, 00:00:00		
<input type="radio"/> 2	CiscoSMB	-	Local Certificate	CiscoTest- DC1-CA	From 2019-Apr-10, 00:00:00 To 2021- Apr-09, 00:00:00		 

結論

您應該已經成功學習了如何在RV160和RV260系列路由器上生成CSR、匯入和下載證書。