

Certificate (Import/Export/Generate CSR) on the RV160 and RV260 Series Router

Objective

The objective of this document is to show you how to generate a Certificate Signing Request (CSR) as well as importing and exporting certificates on the RV160 and RV260 Series Routers.

Introduction

Digital Certificates are important in the communication process. It provides digital identification for authentication. A digital certificate includes information that identifies a device or user, such as the name, serial number, company, department, or IP address.

Certificate Authorities (CA) are trusted authorities that “sign” certificates to verify their authenticity, which guarantees the identity of the device or user. It ensures that the certificate holder is really who they claim to be. Without a trusted signed certificate, data may be encrypted, but the party you are communicating with may not be the one whom you think. CA uses Public Key Infrastructure (PKI) when issuing digital certificates, which uses public key or private key encryption to ensure security. CAs are responsible for managing certificate requests and issuing digital certificates. Some examples of CA are: IdenTrust, Comodo, GoDaddy, GlobalSign, GeoTrust, Verisign and many more.

Certificates are used for Secure Socket Layer (SSL), Transport Layer Security (TLS), Datagram TLS (DTLS) connections, such as Hypertext Transfer Protocol (HTTPS) and Secure Lightweight Directory Access Protocol (LDAPS).

Applicable Devices

- RV160
- RV260

Software Version

- 1.0.00.15

Table of Contents

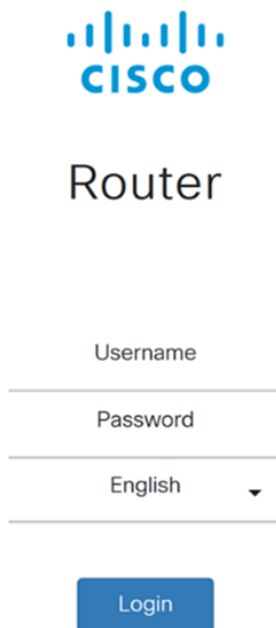
Through this article, you will:

1. [Generate CSR/Certificate](#)
2. [Viewing Certificate](#)

3. [Export Certificate](#)
4. [Import Certificate](#)
5. [Conclusion](#)

Generate CSR/Certificate

Step 1. Log in to the web configuration page.

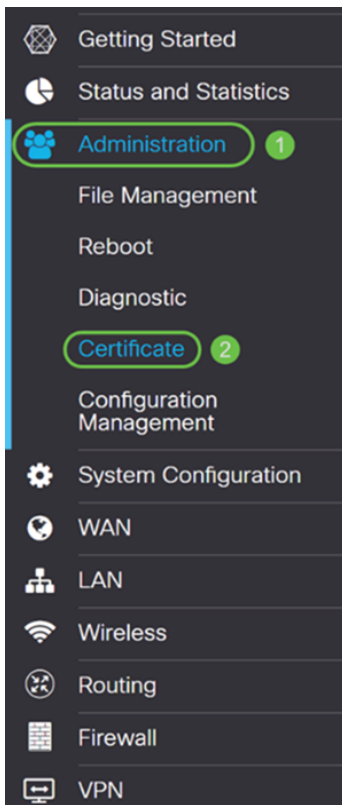


The image shows the Cisco Router login page. At the top is the Cisco logo, which consists of a stylized signal icon above the word "CISCO". Below the logo is the word "Router". Underneath, there are three input fields: "Username", "Password", and a language dropdown menu currently set to "English". At the bottom of the form is a blue "Login" button.

©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.

Step 2. Navigate to **Administration > Certificate**.



Step 3. In the *Certificate* page, click on **Generate CSR/Certificate...** button.

Certificate

Certificate Table

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...

Step 4. Select the type of certificate to generate from one of the following options in the drop-down list.

- **Self-Signed Certificate** – This is a Secure Socket Layer (SSL) certificate which is signed by its own creator. This certificate is less trusted, as it cannot be cancelled if the private key is compromised somehow by an attacker. You must provide the valid duration in days.
- **CA Certificate** – Select this certificate type to make your router act like an internal certificate authority and issue certificates. In a security standpoint, it is similar to a self-signed certificate. This can be used for OpenVPN.
- **Certificate Signing Request** – This is a Public Key Infrastructure (PKI) which is sent to the certificate authority to apply for a digital identity certificate. It is more secure than self-signed as the private key is kept secret. This option is recommended.
- **Certificate Signed by CA Certificate** – Select this certificate type and provide relevant details to get the certificate signed by your internal certificate authority.

In this example, we will be selecting **Certificate Signing Request**.

Generate CSR/Certificate

Type: Certificate Signing Request

Certificate Name: ✘
Please enter a valid name.

Subject Alternative Name:

IP Address FQDN Email

Step 5. Enter the *Certificate Name*. In this example, we will be entering **CertificateTest**.

Type: Certificate Signing Request

Certificate Name: CertificateTest

Subject Alternative Name:

IP Address FQDN Email

Step 6. In the *Subject Alternative Name* field, select one of the following: **IP Address**, **FQDN** (Fully Qualified Domain Name), or **Email** and then enter the appropriate name from what you have selected. This field allows you to specify additional host names.

In this example, we will be selecting **FQDN** and entering **ciscoesupport.com**.

Type: Certificate Signing Request

Certificate Name: CertificateTest

Subject Alternative Name: ciscoesupport.com

IP Address FQDN Email

Step 7. Select a **country** from the *Country Name (C)* drop-down list.

Country Name (C):	<input type="text" value="United States"/>
State or Province Name (ST):	<input type="text"/>
Locality Name (L):	<input type="text"/>
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"/>

Step 8. Enter a **state** or **province name** in the *State or Province Name* field.

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"/>
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"/>

Step 9. In the *Locality Name*, enter a **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"/>

Step 10. Enter the name of the **organization** in the *Organization Name* field.

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"/>

Step 11. Enter the name of the **organization unit** (i.e Training, Support, etc.).

In this example, we will be entering **eSupport** as our organization unit name.

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

Step 12. Enter a **common name**. It is the FQDN of the web server that will be receiving this certificate.

In this example, **ciscosmbsupport.com** was used as the common name.

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

Step 13. Enter an **email address**.

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

Step 14. Select the **Key Encryption Length** from the drop-down menu. The options are: **512**, **1024**, or **2048**. The larger the key size, the more secure the certificate. The larger the key size, the greater the processing time.

Best Practice: It is recommended to choose the highest key encryption length – enabling tougher encryption.

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

Step 15. Click **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:


Step 16. An *Information* popup will appear with a “Generate certificate successfully!” message. Click **OK** to continue.

Information ✕

 Generate certificate successfully!

OK

Step 17. Export the CSR from the *Certificate Table*.

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...

Step 18. An *Export Certificate* window appears. Select **PC** for the *Export to* and then click **Export**.

Export Certificate



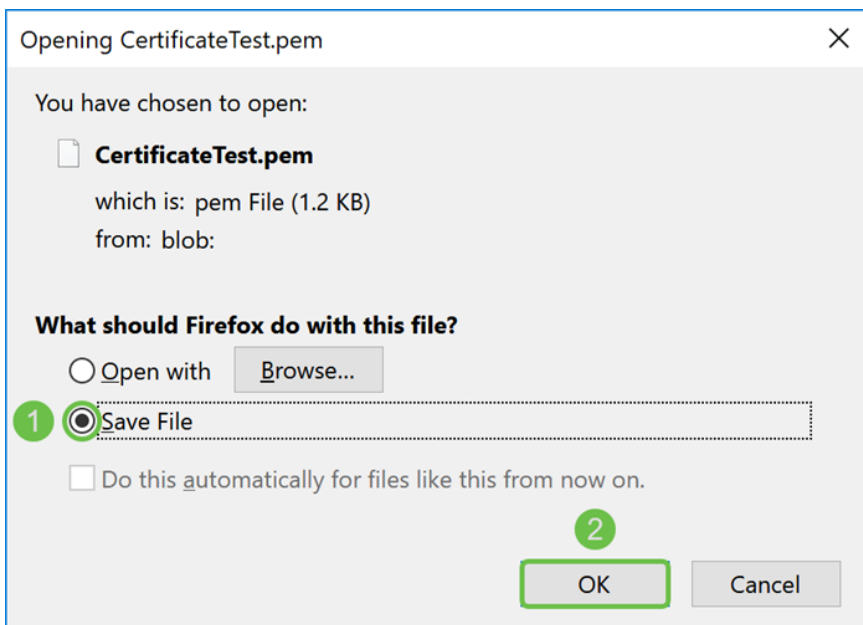
Export as PEM format

Export to:



Step 19. Another window should appear asking whether to open or save the file.

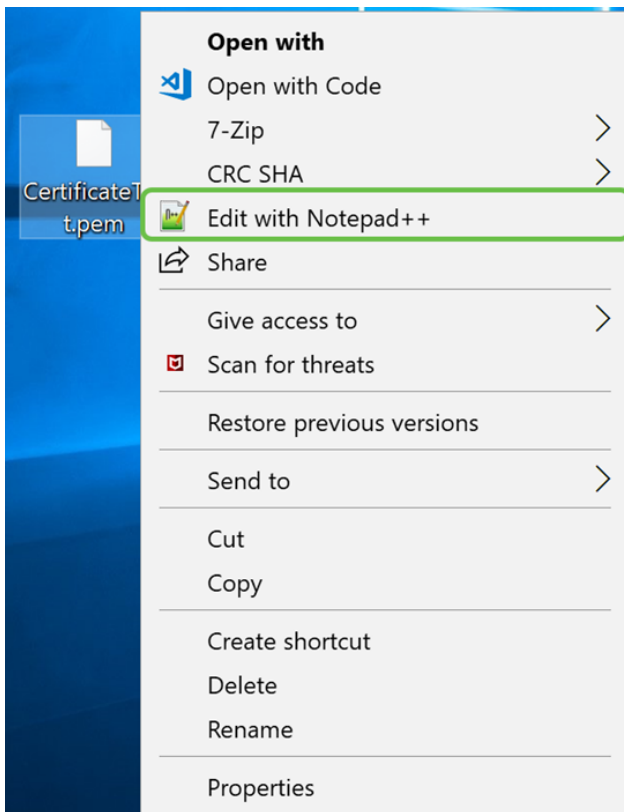
In this example, we will be selecting **Save File** and then click **OK**.



Step 20. Find the location of where the .pem file was saved. **Right-click** the .pem file and open it with your favorite text editor.

In this example, we will be opening the .pem file with Notepad++.

Note: Feel free to open it with Notepad.



Step 21. Ensure that the **-----BEGIN CERTIFICATE REQUEST-----** and **-----END CERTIFICATE REQUEST-----** is on its own line.

Note: Some parts of the certificate were blurred out.

```



CertificateTest.pem x
1 -----BEGIN CERTIFICATE REQUEST----- 1
2 [blurred] VBAYTA1VTMQSwCQYDVQQIDAJDQTERMA8GA1UE
3 BwWIU2FuIEpvc2UxDjAMBGNVBAoMBUNpc2NmREwDwYDVQLDAh1U3VwcG9ydDEC
4 MBoGA1UEAwTY2lzMzY2ZmVzZXBw3J0 [blurred]
5 eWVuQGNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ/r
6 J02/H2TfmIrv1vcs0c+tXmvt8PpCcCFuEaoEvdCcV6kP+TaeDmndcgIdDXNRXplu
7 wSyiqrpS8+kbhzPTF8sHO94Q8wyA8mEu/SjYs0DWuqa2+3LAFOLlp8Cg+e3l0cjs
8 VJS8efDI5j1ECMABvB5Tv [blurred]
9 soTqNBrYqR8h46NHh0J5fMXDsPYlj2LWmS1VbkskoiMdr5SZlwmhkrqgLby+bfma
10 eOhl0DyX3D7xTV14tvzxYrmDilmprieLQc9zME/bZqZgTgY5MgSTGPAis27m29PR
11 oZK/Rpg6Scywbx1X/G0CAwEAAaCBkTCBjgYJKoZIhvcNAQkOMYGAMH4wCQYDVR0T
12 BAIw [blurred].gXg
13 MCcGA1UdJQogMB4GCCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUIAgIwHAYDVR0R
14 BBUwE4IRY2lzMzY2ZmVzZXBw3J0wDQYJKoZIhvcNAQELBQADggEBAILUeIUy
15 TqFZ2wQx3r29E1SWOU5bmqCj+9IfrsFLR909VdAIJXoUP16CJtc4JJy5+XEhYSnu
16 [blurred]
17 [blurred]
18 [blurred]
19 [blurred]
20 [blurred]
21 -----END CERTIFICATE REQUEST----- 2
22 [blurred]

```

Step 22. When you have your CSR, you would need to go to your hosting services or a certificate authority site (i.e. GoDaddy, Verisign, etc.) and request a certificate. Once you have submitted a request, it will communicate with the certificate server to make sure there isn't any reason not to issue the certificate.







Note: Contact the CA or hosting site support if you don't know where the certificate request is on their site.

Step 23. Download the certificate once it is completed. It should be either a **.cer** or **.crt** file. In this example, we were provided with both files.

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

Step 24. Go back to the *Certificate* page in your router and import the certificate file by clicking the **arrow pointing to the device** icon.

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	-	-		  

Step 25. In the *Certificate Name* field, enter the **certificate name**. It can't be the same name as the certificate signing request. In the *Upload Certificate file* section, select **import from PC** and click **Browse...** to upload your certificate file.

Import Signed-Certificate

Type: Local Certificate


Certificate Name: 1

Upload Certificate file

2

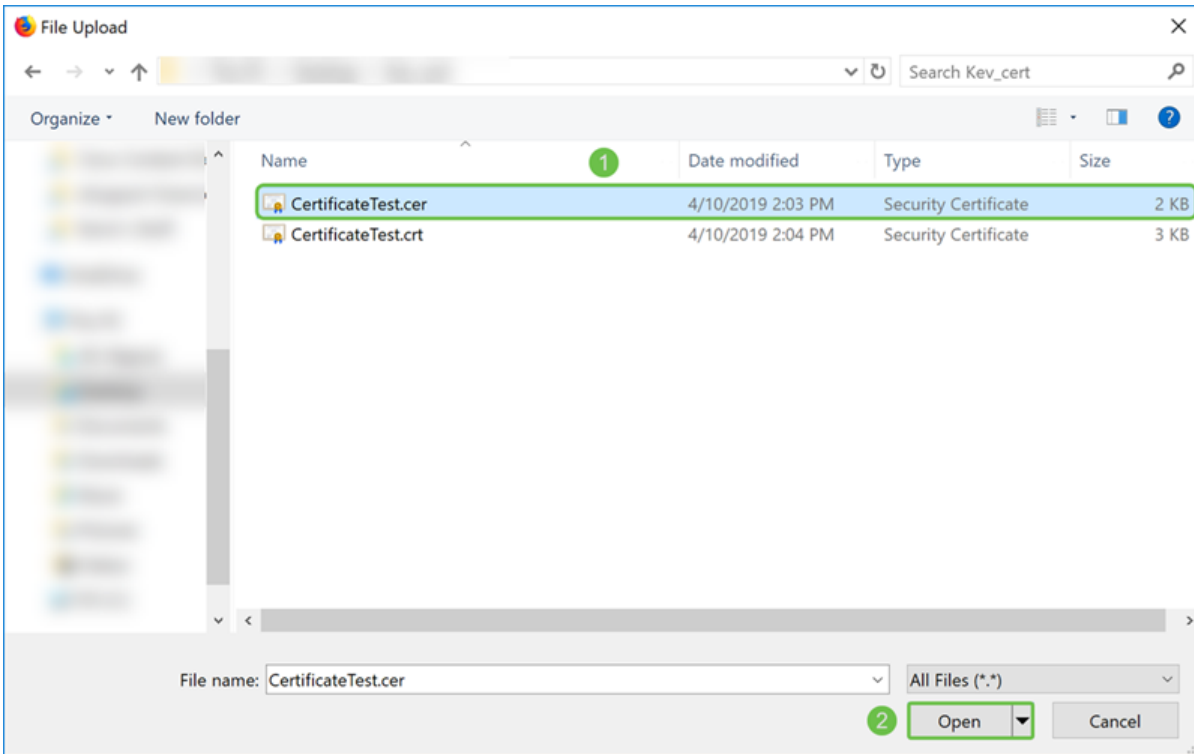
Import from PC

3 No file is selected

Import from USB 

No file is selected

Step 26. A *File Upload* window appears. Navigate to the location of where your certificate file is. Select the **certificate** file that you want to upload and click **Open**. In this example, **CertificateTest.cer** was selected.



Step 27. Click the **Upload** button to start uploading your certificate to the router.

Note: If you get an error where you can't upload your .cer file, it might be because your router requires the certificate to be in a pem encoding. You would need to convert your der encoding (.cer file extension), to a pem encoding (.crt file extension).

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






Step 28. If the import was successful, an *information* window should appear letting you know that it was successful. Click **OK** to continue.

 Import certificate successfully!

OK

Step 29. Your certificate should be successfully updated. You should be able to see who your certificate was signed by. In this example, we can see that our certificate was signed by *CiscoTest-DC1-CA*. To make the certificate as our primary certificate, select the certificate by using the radio button on the left side and click **Select as Primary Certificate...** button.

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		 

2

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

Note: Changing the primary certificate might bring you back to a warning page. If you are using Firefox and it comes up as a gray blank page, you would need to adjust some configuration on your Firefox. This document on Mozilla wiki gives some explanation about it: [CA/AddRootToFirefox](#). To be able to see the warning page again, [follow these steps that was found in Mozilla community support page](#).

Step 30. In the Firefox warning page, click **Advanced...** and then **Accept the Risk and Continue** to proceed back into the router.

Note: These warnings screen vary browser to browser but perform the same functions.



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

Step 31. In the *Certificate Table*, you should see that the *NETCONF*, *WebServer*, and *RESTCONF* has swapped to your new certificate instead of using the *Default* certificate.

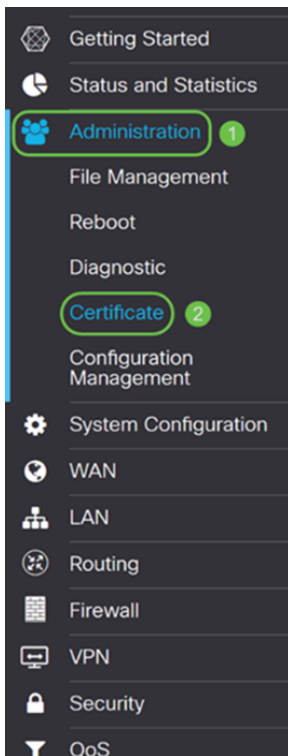
Certificate Table

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		

You should now have successfully installed a certificate onto your router.






Viewing Certificate

Step 1. If you have navigated away from the *Certificate* page, navigate to **Administration > Certificate**.



Step 2. In the *Certificate Table*, click the **Details** icon located under the *Details* section.

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		 

Step 3. The *Certificate Detail* page appears. You should be able to see all the information about your certificate.

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

Step 4. Click the **lock** icon located on the left side of the Uniform Resource Locator (URL) bar.

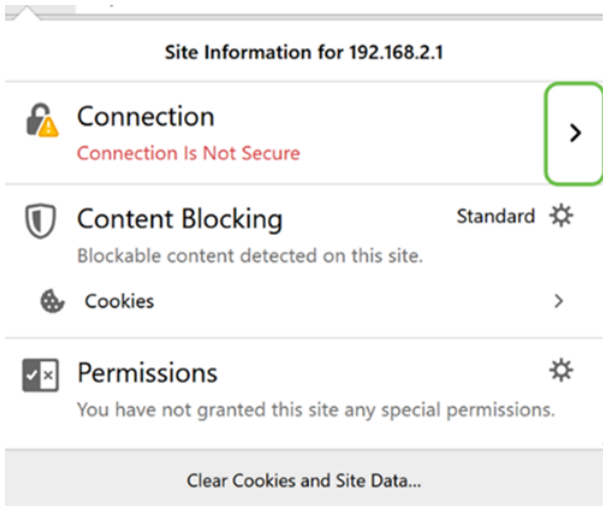
Note: The following steps are used in a Firefox browser.

The screenshot shows the Cisco RV160 VPN Router web interface. The browser's address bar displays the URL `https://192.168.2.1/#/certificate` with a lock icon on the left, which is circled in green. The interface shows the 'Certificate' configuration page with a 'Certificate Table' containing two entries:

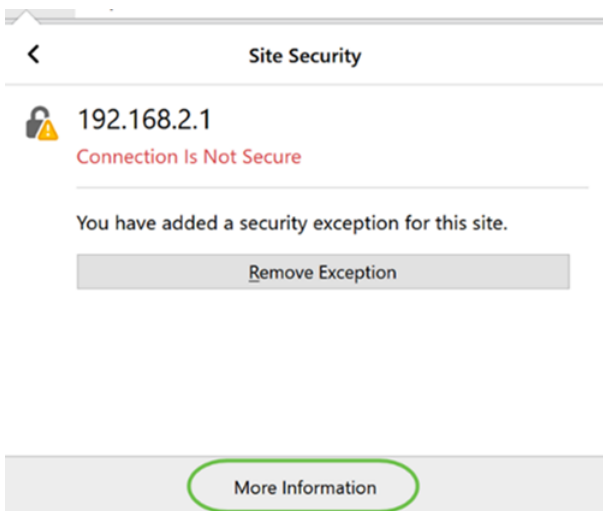
Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
1	Default	-	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048-Dec-13, 00:00:00		
2	CiscoSMB	NETCONF WebServer RESTCONF	Local Certificate	CiscoTest-DC1-CA	From 2019-Apr-10, 00:00:00 To 2021-Apr-09, 00:00:00		

Below the table, there are four buttons: 'Import Certificate...', 'Generate CSR/Certificate...', 'Show built-in 3rd party CA Certificates...', and 'Select as Primary Certificate...'.

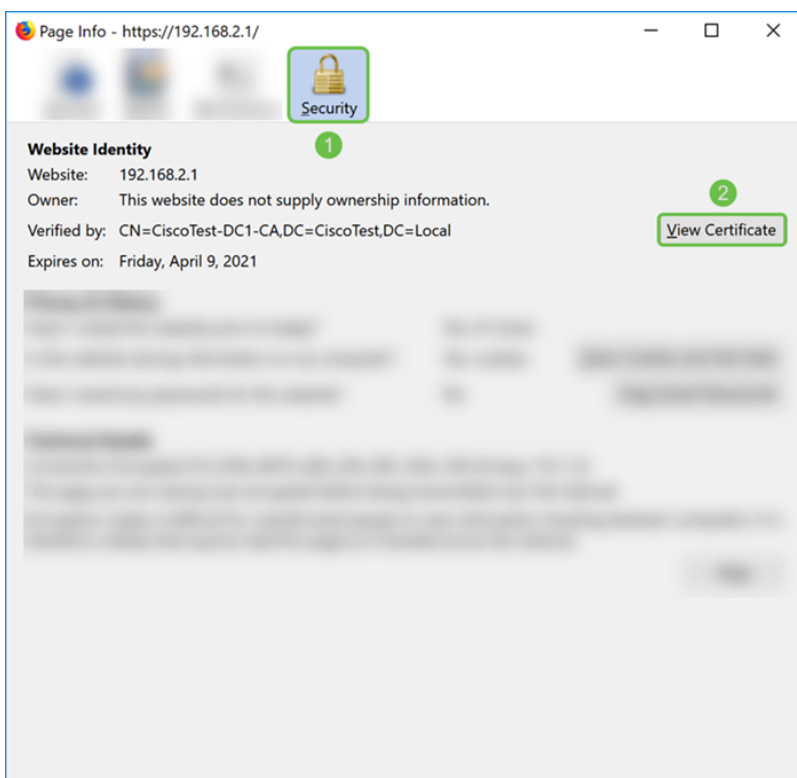
Step 5. A drop-down list of choices appears. Click the **Arrow** icon next to the *Connection* field.



Step 6. Click **More Information**.



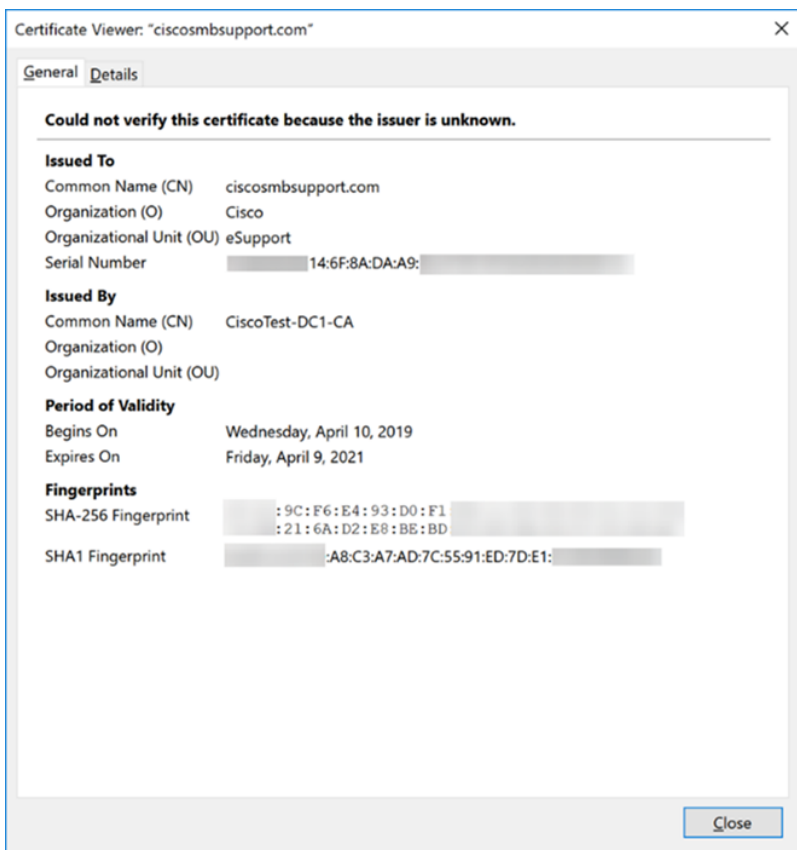
Step 7. In the *Page Info* window, you should be able to see a brief information about your certificate under the *Website identity* section. Ensure that you are in the **Security** tab and then click **View Certificate** to see more information about your certificate.



Step 8. The *Certificate Viewer* page should appear. You should be able to see all the

information about your certificate, period of validity, fingerprints, and who it was issued by.

Note: Since this certificate was issued by our test certificate server, the issuer is unknown.



Exporting Certificate

To download your certificate to import it on another router, follow the steps below.

Step 1. In the *Certificate* page, click the **export** icon next to the certificate that you want to export.

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		

Step 2. An *Export Certificate* appears. Select a format to export the certificate. The options are:

- **PKCS#12** – Public Key Cryptography Standards (PKCS) #12 is an exported certificate that comes in a .p12 extension. A password will be required in order to encrypt the file to protect it as it is exported, imported, and deleted.
- **PEM** – Privacy Enhanced Mail (PEM) is often used for web servers for their ability to be

easily translated into readable data by using a simple text editor such as notepad.

Select **Export as PKCS#12 format** and enter a **password** and **confirm password**. Then select **PC** as the *Export to:* field. Click **Export** to start exporting the certificate to your computer.

Note: Remember this password because you will be using it when importing it to a router.

Export Certificate ✕


1
 Export as PKCS#12 format

Enter Password: 2

Confirm Password:

Export as PEM format

Export to:


3
 PC USB 

4

Step 3. A window will appear asking what you should do with this file. In this example, we will be selecting **Save File** and then click **OK**.

Opening CiscoSMB.p12 ✕

You have chosen to open:

 **CiscoSMB.p12**
which is: Chrome HTML Document
from: https://192.168.2.1

What should Firefox do with this file?

Open with v

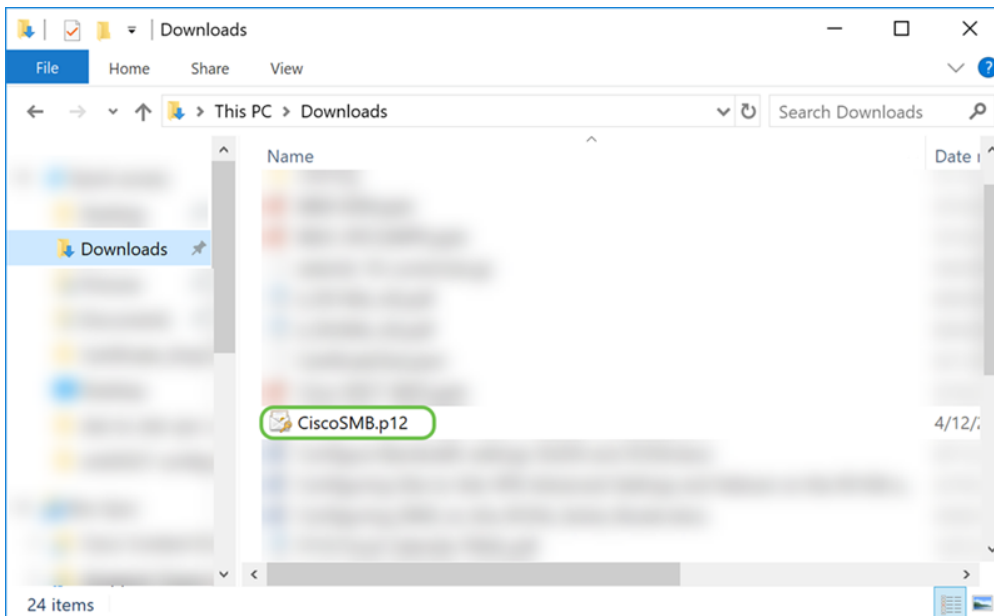
1 Save File

Do this automatically for files like this from now on.

2

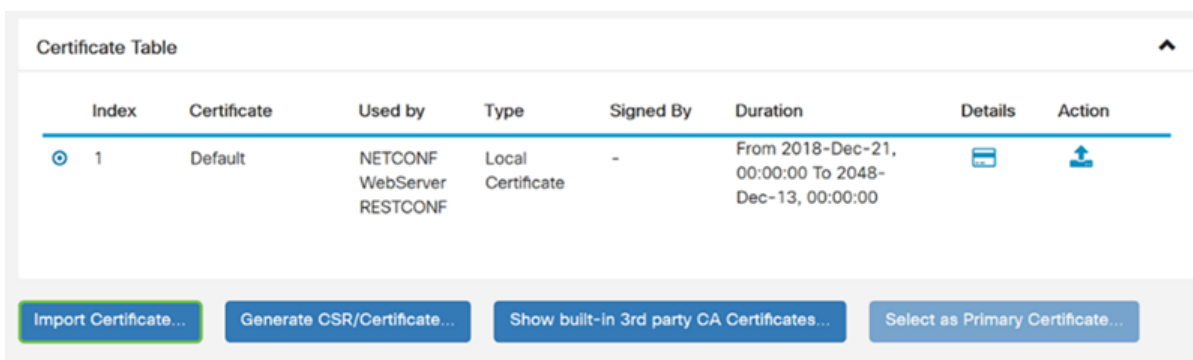
Step 4. The file should save to your default save location.

In our example, the file was saved to our *Downloads* folder on our computer.



Importing Certificate

Step 1. In the *Certificate* page, click the **Import Certificate...** button.



Step 2. Select the **type** of certificate to import from the *Type* drop-down list under *Import Certificate* section. The options are defined as:

- **CA Certificate** – A certificate that is certified by a trusted third-party authority that has confirmed that the information contained in the certificate is accurate.
- **Local Device Certificate** – A certificate generated on the router.
- **PKCS#12 Encoded File** – Public Key Cryptography Standards (PKCS) #12 is an exported certificate that comes in a .p12 extension.

In this example, **PKCS#12 Encoded File** was selected as the type. Enter a **name** for the certificate and then enter the **password** that was used.

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

Step 3. Under the *Upload Certificate file* section, select either **Import from PC** or **Import from USB**. In this example, **Import from PC** was selected. Click **Browse...** to choose a file to upload.

Import Certificate

Type:


Certificate Name:

Import Password:

Upload Certificate file

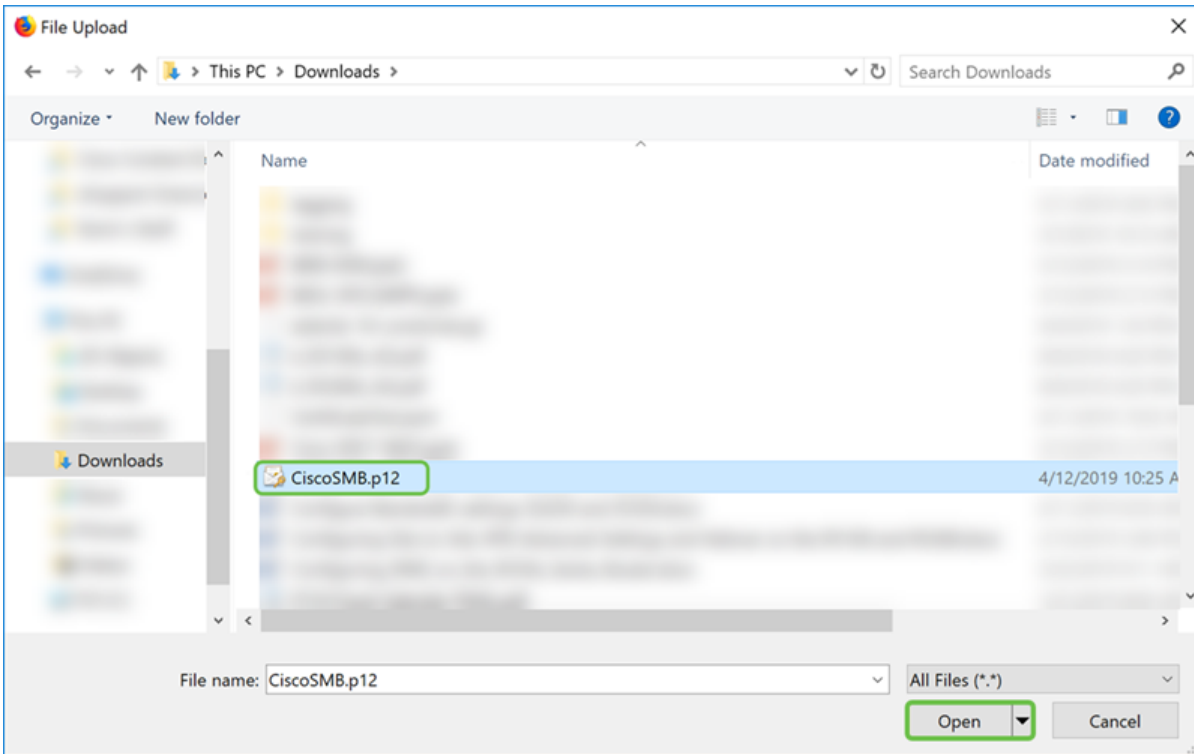
Import from PC

No file is selected

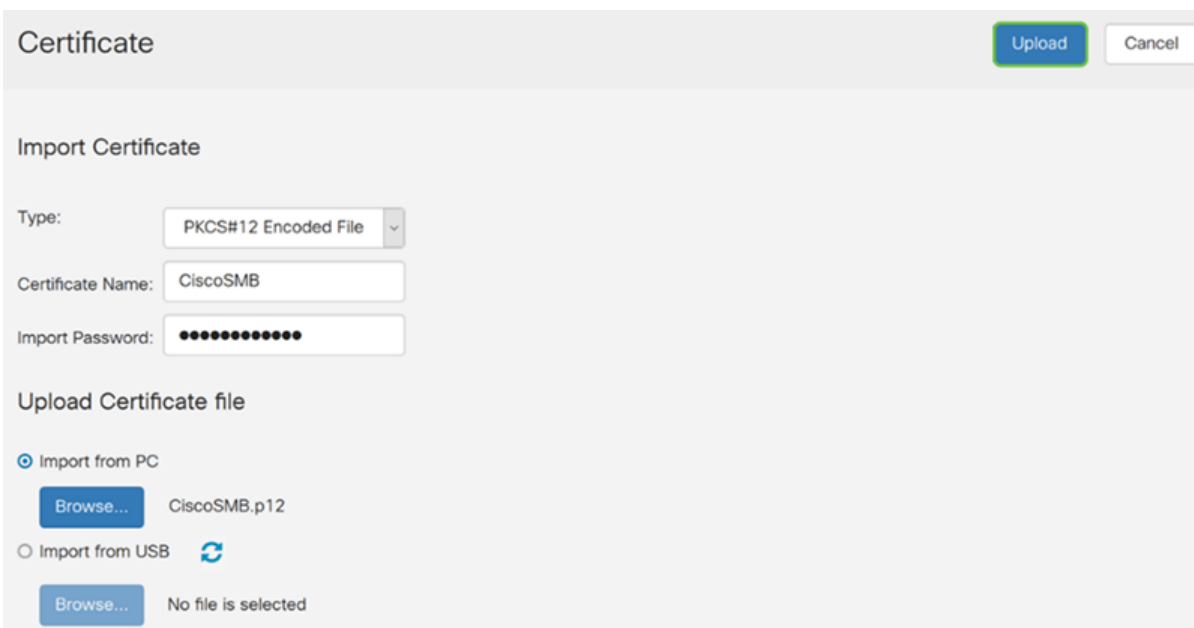
Import from USB 

No file is selected

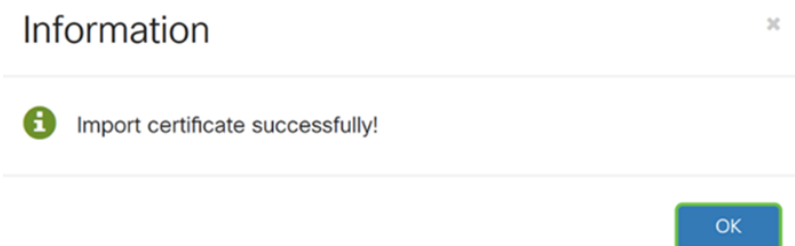
Step 4. In the *File Upload* window, navigate to the location of where the PKCS#12 Encoded File (.p12 file extension) is located. Select the **.p12** file and then click **Open**.



Step 5. Click **Upload** to start uploading the certificate.







Step 6. An *Information* window will appear letting you know that your certificate was imported successfully. Click **OK** to continue.



Step 7. You should see that your certificate was uploaded.

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		 

Conclusion

You should have successfully learned how to generate a CSR, import, and download a certificate on the RV160 and RV260 series router.