

# Certificat (Import/Export/Generate CSR) sur les routeurs des gammes RV160 et RV260

## Objectif

L'objectif de ce document est de vous montrer comment générer une demande de signature de certificat (CSR) ainsi que importer et exporter des certificats sur les routeurs des gammes RV160 et RV260.

## Introduction

Les certificats numériques sont importants dans le processus de communication. Ils fournissent une identification numérique pour l'authentification. Un certificat numérique inclut des informations qui identifient un périphérique ou un utilisateur, telles que le nom, le numéro de série, la société, le service ou l'adresse IP.

Les autorités de certification sont des autorités de confiance qui "signent" des certificats pour vérifier leur authenticité, ce qui garantit l'identité du périphérique ou de l'utilisateur. Elles assurent que le titulaire du certificat est vraiment celui qu'il prétend être. Sans certificat signé de confiance, les données peuvent être chiffrées, mais la personne avec laquelle vous communiquez n'est peut-être pas celle à qui vous pensez. L'autorité de certification utilise l'infrastructure à clé publique (PKI) lors de la délivrance de certificats numériques, qui utilise le chiffrement à clé publique ou privée pour assurer la sécurité. Les CA sont responsables de la gestion des demandes de certificat et de la délivrance des certificats numériques. Voici quelques exemples de CA : IdenTrust, Comodo, GoDaddy, GlobalSign, GeoTrust, Verisign et bien d'autres encore.

Les certificats sont utilisés pour les connexions SSL (Secure Socket Layer), TLS (Transport Layer Security), DTLS (Datagram TLS), telles que HTTPS (Hypertext Transfer Protocol) et LDAPS (Secure Lightweight Directory Access Protocol).

## Périphériques pertinents

- RV160
- RV260

## Version du logiciel

- 1.0.00.15

## Table des matières

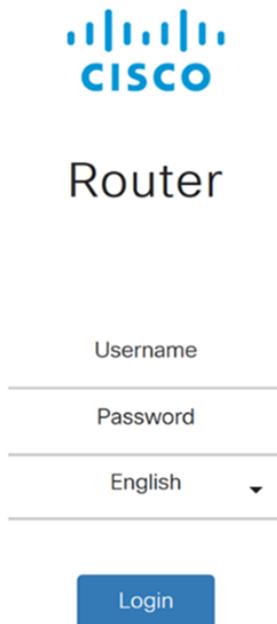
Dans cet article, vous allez :

1. [Générer CSR/Certificat](#)

2. [Affichage du certificat](#)
3. [Exporter le certificat](#)
4. [Importer le certificat](#)
5. [Conclusion](#)

## Générer CSR/Certificat

Étape 1. Connectez-vous à la page de configuration Web.

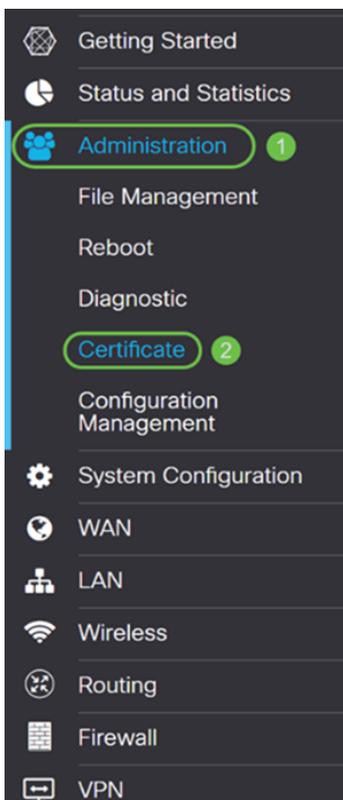


The image shows the Cisco Router login page. At the top is the Cisco logo, which consists of a stylized signal icon above the word "CISCO". Below the logo is the word "Router". There are three input fields: "Username", "Password", and a language dropdown menu currently set to "English". Below these fields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

Étape 2. Accédez à **Administration > Certificate**.



Étape 3. Dans la page *Certificate*, cliquez sur **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...

Étape 4. Sélectionnez le type de certificat à générer dans l'une des options suivantes de la liste déroulante.

- **Certificat auto-signé** - Il s'agit d'un certificat SSL (Secure Socket Layer) signé par son propre créateur. Ce certificat est moins fiable, car il ne peut pas être annulé si la clé privée est compromise d'une manière ou d'une autre par un pirate. Vous devez indiquer la durée valide en jours.
- **certificat CA** - Sélectionnez ce type de certificat pour faire de votre routeur une autorité de certification interne et émettre des certificats. Du point de vue de la sécurité, il est similaire à un certificat auto-signé. Ceci peut être utilisé pour OpenVPN.
- **Demande de signature de certificat** - Il s'agit d'une infrastructure à clé publique (ICP) qui est envoyée à l'autorité de certification pour demander un certificat d'identité numérique. Il est plus sécurisé que autosigné car la clé privée est gardée secrète. Cette option est recommandée.

- **certificat signé par un certificat CA** - Sélectionnez ce type de certificat et fournissez les détails pertinents pour obtenir le certificat signé par votre autorité de certification interne.

Dans cet exemple, nous allons sélectionner **Demande de signature de certificat**.

Generate CSR/Certificate

Type: Certificate Signing Request

Certificate Name:  ✘  
Please enter a valid name.

Subject Alternative Name:

IP Address  FQDN  Email

Étape 5. Entrez le *nom du certificat*. Dans cet exemple, nous allons entrer **CertificateTest**.

Type: Certificate Signing Request

Certificate Name: CertificateTest

Subject Alternative Name:

IP Address  FQDN  Email

Étape 6. Dans le champ *Nom alternatif du sujet*, sélectionnez l'une des options suivantes : **Adresse IP**, **FQDN** (Fully Qualified Domain Name) ou **E-mail** et entrez le nom approprié à partir de ce que vous avez sélectionné. Ce champ vous permet de spécifier des noms d'hôtes supplémentaires.

Dans cet exemple, nous allons sélectionner **FQDN** et entrer **ciscoesupport.com**.

Type: Certificate Signing Request

Certificate Name: CertificateTest

Subject Alternative Name: ciscoesupport.com

1  IP Address  FQDN  Email

Étape 7. Sélectionnez un **pays** dans la liste déroulante *Nom du pays (C)*.

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"/>

Étape 8. Entrez un **nom d'état** ou de **province** dans le champ *Nom de l'état ou de la province*.

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"/>

Étape 9. Dans le *nom de la localité*, saisissez un nom de **ville**.

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"/>

Étape 10. Entrez le nom de l'**organisation** dans le champ *Nom de l'organisation*.

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"/>

Étape 11. Entrez le nom de l'**unité d'organisation** (formation, assistance, etc.).

Dans cet exemple, nous allons entrer **eSupport** comme nom d'unité de l'organisation.

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

Étape 12. Entrez un **nom commun**. C'est le nom de domaine complet du serveur Web qui recevra ce certificat.

Dans cet exemple, **ciscosmbsupport.com** a été utilisé comme nom commun.

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

Étape 13. Entrez une **adresse e-mail**.

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

Étape 14. Sélectionnez **Key Encryption Length** dans le menu déroulant. Les options sont les suivantes : **512, 1024 ou 2048**. Plus la taille de la clé est grande, plus le certificat est sécurisé. Plus la taille de la clé est grande, plus le temps de traitement est important.

**Meilleure pratique** : Il est recommandé de choisir la longueur de cryptage de clé la plus élevée, ce qui permet un cryptage plus strict.

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

Étape 15. Cliquez sur **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:

Étape 16. Une fenêtre contextuelle *Informations* s'affiche avec un certificat " Générer !" message. Cliquez sur **OK** pour continuer.

### Information ✕

Generate certificate successfully!

**OK**

Étape 17. Exporter le CSR à partir de la *table de certificats*.

Certificate Table <span style="float: right;">▲</span>							
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...

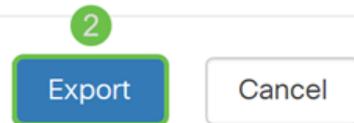
Étape 18. Une fenêtre *Export Certificate* apparaît. Sélectionnez **PC** pour l'*exportation vers*, puis cliquez sur **Exporter**.

# Export Certificate



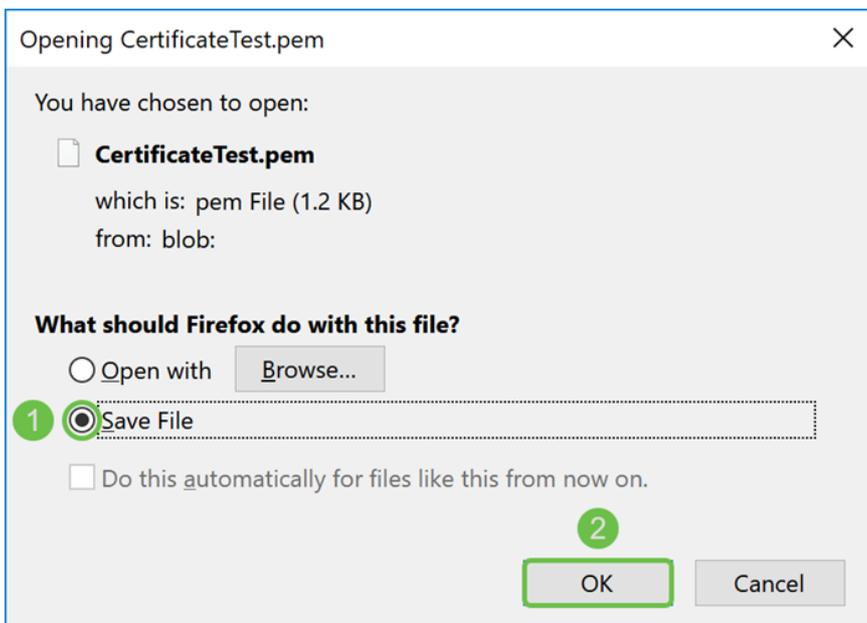
Export as PEM format

Export to:



Étape 19. Une autre fenêtre doit apparaître pour vous demander si vous voulez ouvrir ou enregistrer le fichier.

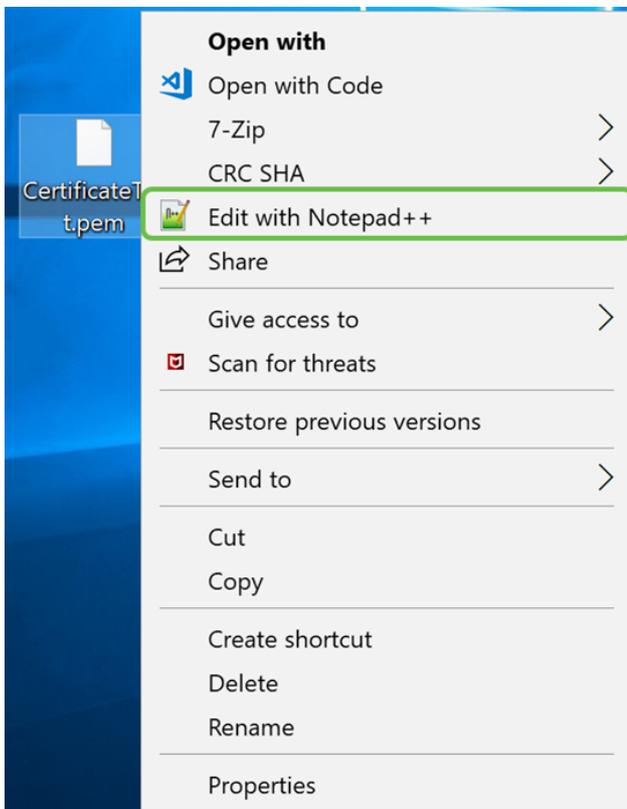
Dans cet exemple, nous allons sélectionner **Enregistrer le fichier** puis cliquez sur **OK**.



Étape 20. Rechercher l'emplacement d'enregistrement du fichier .pem. **Cliquez avec le bouton droit** sur le fichier .pem et ouvrez-le avec votre éditeur de texte préféré.

Dans cet exemple, nous allons ouvrir le fichier .pem avec Notepad++.

**Note:** N'hésitez pas à l'ouvrir avec le Bloc-notes.



Étape 21. Assurez-vous que la — **DEMANDE DE CERTIFICAT DE DÉBUT**— et — **DEMANDE DE CERTIFICAT DE FIN**— se trouve sur sa propre ligne.

**Note:** Certaines parties du certificat ont été brouillées.

```
CertificateTest.pem x
1 -----BEGIN CERTIFICATE REQUEST----- 1
2 [redacted] VBAYTA1VTMQSwCQYDVQQIDAJDQTERMA8GA1UE
3 BwwIU2FuIEpvc2UxdjAMBgNVBAoMBUNpc2NmREwDwYDVQLDAh1U3VwcG9ydDEC
4 MBoGA1UEAwTY2lzMzY2ZmVzZXBw3J0 [redacted]
5 eWVuQGNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ/r
6 J02/H2TfmIrv1vcs0c+tXmvt8PpCcCFuEaoEvdCcV6kP+TaeDmndcgIdDXNRXplu
7 wSyiqrpS8+kbhzPTF8sHO94Q8wyA8mEu/SjYs0DWuqa2+3LafOLlp8Cg+e3l0cjs
8 VJS8efDI5j1ECMABvB5Tv [redacted]
9 soTqNBrYqR8h46NHh0J5fMXDsPY1j2LWmS1VbkskoiMdr5SZlwmhkrqqLby+bfma
10 eOhl0DyX3D7xTV14tvzxYrmDilmprieLQc9zME/bZqZgTgY5MgSTGPAis27m29PR
11 oZK/Rpg6Scywbx1X/G0CAwEAAaCBkTCBjgYJKoZIhvcNAQkOMYGAMH4wCQYDVR0T
12 BA1w [redacted].gXg
13 MCcGA1UdJQogMB4GCCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUIAgIwHAYDVR0R
14 BBUwE4IRY21zY29lc3VwcG9ydC5jb20wDQYJKoZIhvcNAQELBQADggEBAILUeIUy
15 TqFZ2wQx3r29E1SOWU5bmqCj+9IfrsFLR909VdAIJXoUP16CJtc4JJy5+XEhYSnu
16 [redacted]
17 [redacted]
18 [redacted]
19 [redacted]
20 [redacted]
21 -----END CERTIFICATE REQUEST----- 2
22 [redacted]
```

Étape 22. Lorsque vous avez votre CSR, vous devez vous rendre sur votre site d'hébergement ou sur un site d'autorité de certification (GoDaddy, Verisign, etc.) et demander un certificat. Une fois que vous avez envoyé une demande, il communiquera avec le serveur de certificats pour s'assurer qu'il n'y a aucune raison de ne pas émettre le certificat.

**Note:** Contactez l'autorité de certification ou le support du site d'hébergement si vous ne savez pas où se trouve la demande de certificat sur leur site.

Étape 23. Téléchargez le certificat une fois qu'il est terminé. Il doit s'agir d'un fichier **.cer** ou **.crt**. Dans cet exemple, nous avons reçu les deux fichiers.

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

Étape 24. Revenez à la page *Certificate* de votre routeur et importez le fichier de certificat en cliquant sur la **flèche pointant vers l'icône du périphérique**.

#### 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	-	-		  

Étape 25. Dans le champ *Nom du certificat*, saisissez le **nom du certificat**. Il ne peut pas être du même nom que la demande de signature de certificat. Dans la section *Télécharger le fichier de certificat*, sélectionnez **Importer à partir du PC** et cliquez sur **Parcourir...** pour télécharger votre fichier de certificat.

## Import Signed-Certificate

Type: Local Certificate

Certificate Name:  1

### Upload Certificate file

2

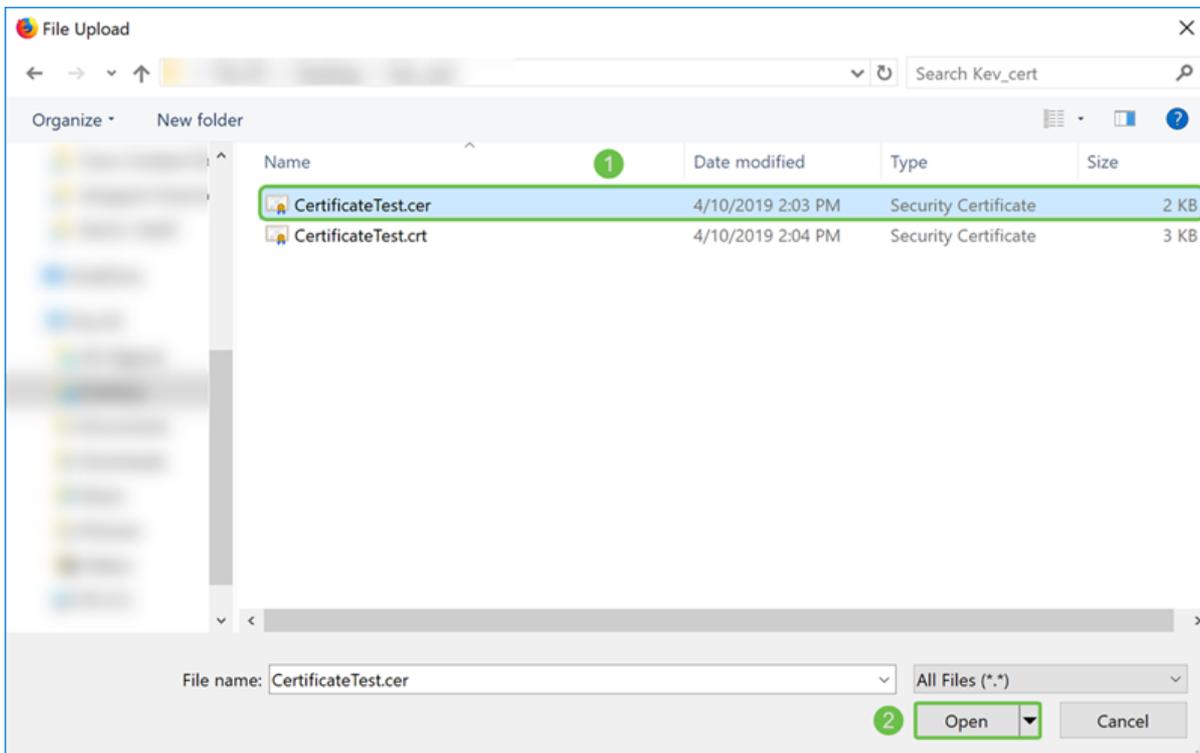
Import from PC

3  No file is selected

Import from USB 

No file is selected

Étape 26. Une fenêtre *File Upload* apparaît. Accédez à l'emplacement du fichier de certificat. Sélectionnez le fichier **de certificat** que vous voulez télécharger et cliquez sur **Ouvrir**. Dans cet exemple, **CertificateTest.cer** a été sélectionné.



Étape 27. Cliquez sur le bouton **Upload** pour commencer à télécharger votre certificat sur le routeur.

**Note:** Si vous obtenez une erreur dans laquelle vous ne pouvez pas télécharger votre fichier .cer, c'est peut-être parce que votre routeur nécessite que le certificat soit codé en pem. Vous devez convertir votre codage der (extension de fichier .cer) en codage pem (extension de fichier .crt).

## 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

Étape 28. Si l'importation a réussi, une fenêtre *d'informations* doit apparaître pour vous indiquer qu'elle a réussi. Cliquez sur **OK** pour continuer.

## Information

 Import certificate successfully!

OK

Étape 29. Votre certificat doit être mis à jour. Vous devriez être en mesure de voir par qui votre certificat a été signé. Dans cet exemple, nous pouvons voir que notre certificat a été signé par *CiscoTest-DC1-CA*. Pour faire du certificat notre certificat principal, sélectionnez le certificat à l'aide de la case d'option située sur le côté gauche et cliquez sur **Sélectionner comme certificat principal...** bouton.

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		 

1

2

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

**Note:** La modification du certificat principal peut vous ramener à une page d'avertissement. Si vous utilisez Firefox et qu'il s'agit d'une page blanche grise, vous devez ajuster une certaine configuration sur votre Firefox. Ce document sur Mozilla wiki donne quelques explications à ce sujet : [CA/AddRootToFirefox](#). Pour voir à nouveau la page d'avertissement, [suivez ces étapes qui ont été trouvées dans la page de support de la communauté Mozilla](#).

Étape 30. Dans la page d'avertissement de Firefox, cliquez sur **Avancé...** puis **Acceptez le risque et continuez** pour revenir au routeur.

**Note:** Ces avertissements varient d'un navigateur à l'autre, mais remplissent les mêmes fonctions.



## 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

Étape 31. Dans la table des certificats, vous devriez voir que NETCONF, WebServer et RESTCONF a basculé vers votre nouveau certificat au lieu d'utiliser le *certificat par défaut*.

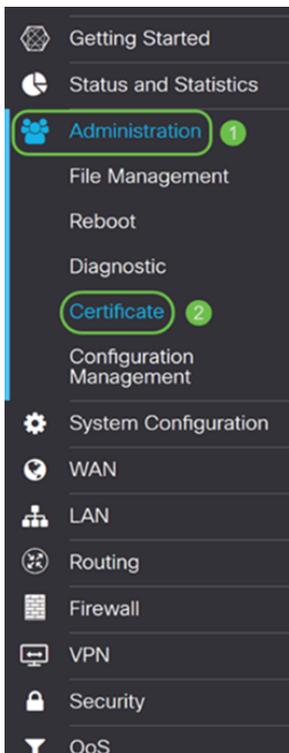
Certificate Table

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		

Vous devez maintenant avoir correctement installé un certificat sur votre routeur.

## Affichage du certificat

Étape 1. Si vous êtes éloigné de la page *Certificat*, accédez à **Administration > Certificat**.



Étape 2. Dans la *table des certificats*, cliquez sur l'icône **Détails** située sous la section *Détails*.

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		 

Étape 3. La page *Certificate Detail* s'affiche. Vous devriez pouvoir voir toutes les informations concernant votre certificat.

## Certificate Detail

x

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

Étape 4. Cliquez sur l'icône de **verrouillage** située sur le côté gauche de la barre URL (Uniform Resource Locator).

**Note:** Les étapes suivantes sont utilisées dans un navigateur Firefox.

Cisco RV160 VPN Router

https://192.168.2.1/#/certificate

RV160--router5680AA

cisco(admin) English

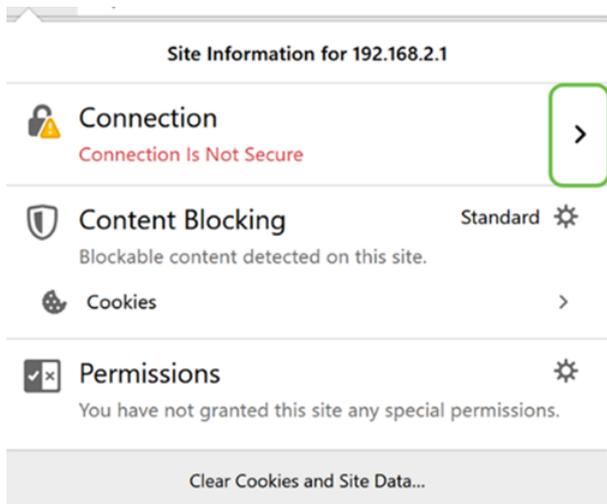
### Certificate

Certificate Table

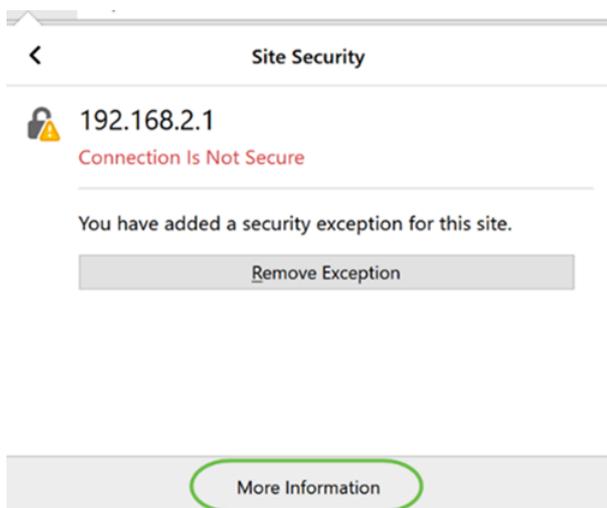
Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
1	Default	-	Local Certificate	-	From 2018-Dec-21, 00:00:00 To 2048-Dec-13, 00:00:00		
2	CiscoSMB	NETCONF WebServer RESTCONF	Local Certificate	CiscoTest-DC1-CA	From 2019-Apr-10, 00:00:00 To 2021-Apr-09, 00:00:00		

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

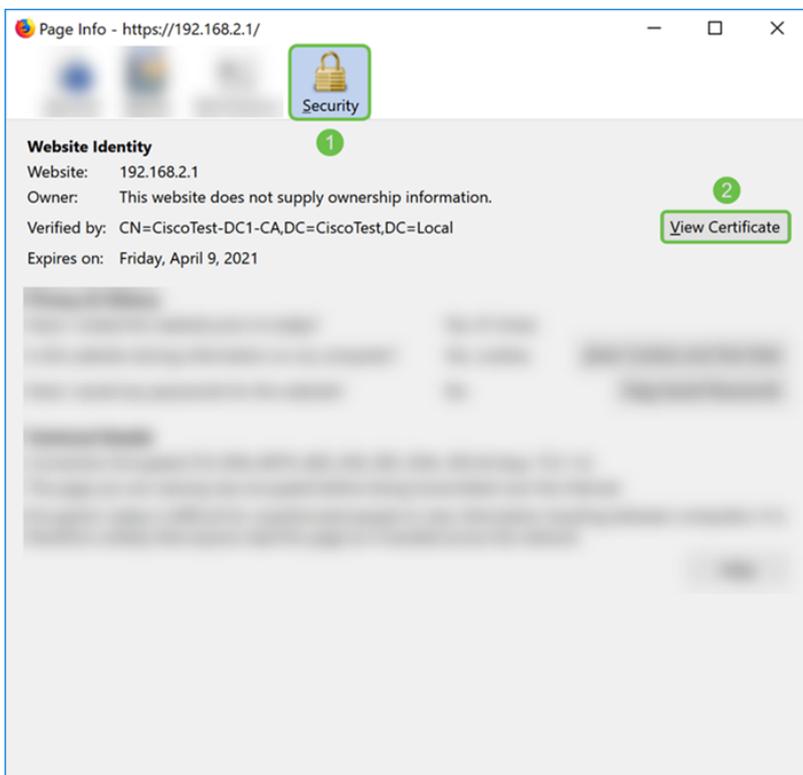
Étape 5. Une liste déroulante de choix s'affiche. Cliquez sur l'icône **Flèche** en regard du champ *Connexion*.



Étape 6. Cliquez sur **Plus d'informations**.

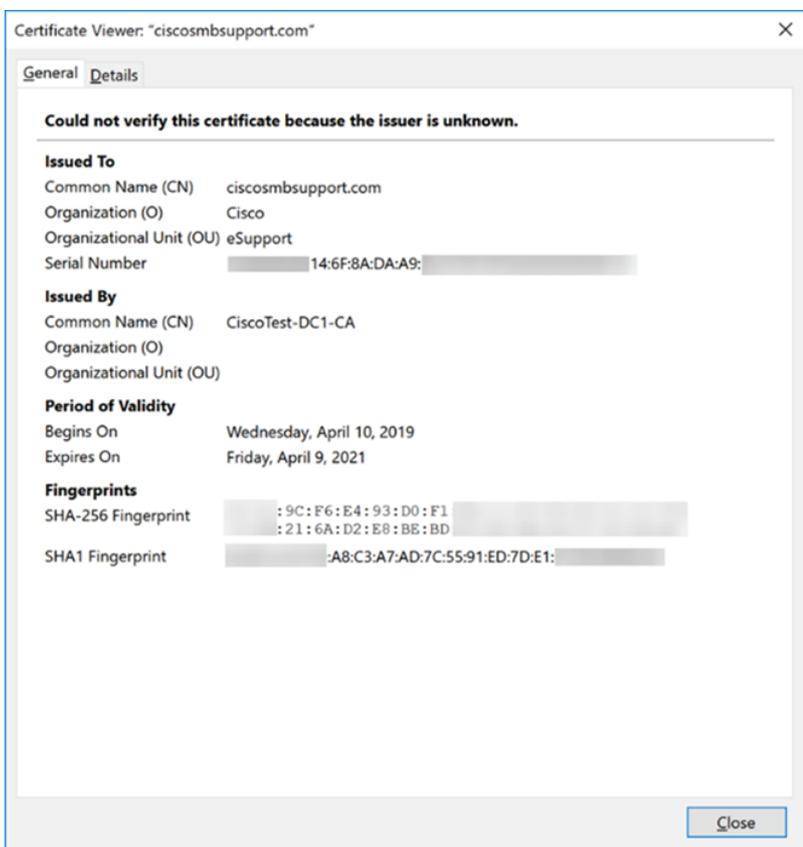


Étape 7. Dans la fenêtre *Info page*, vous devriez voir une brève information sur votre certificat sous la section *Identité du site Web*. Vérifiez que vous vous trouvez dans l'onglet **Sécurité**, puis cliquez sur **Afficher le certificat** pour afficher plus d'informations sur votre certificat.



Étape 8. La page *Visualiseur de certificats* doit s'afficher. Vous devriez être en mesure de voir toutes les informations concernant votre certificat, la période de validité, les empreintes digitales et les personnes qui l'ont délivré.

**Note:** Puisque ce certificat a été émis par notre serveur de certificats de test, l'émetteur est inconnu.



## Exportation du certificat

Pour télécharger votre certificat pour l'importer sur un autre routeur, procédez comme suit.

Étape 1. Dans la page *Certificat*, cliquez sur l'icône **Exporter** en regard du certificat à exporter.

#### 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		

Étape 2. Un *certificat d'exportation* apparaît. Sélectionnez un format pour exporter le certificat. Les options sont les suivantes :

- **PKCS#12** - Public Key Cryptography Standards (PKCS) #12 est un certificat exporté qui est fourni dans une extension .p12. Un mot de passe est nécessaire pour chiffrer le fichier afin de le protéger lors de son exportation, de son importation et de sa suppression.
- **PEM** - Privacy Enhanced Mail (PEM) est souvent utilisé pour les serveurs Web pour leur capacité à être facilement traduites en données lisibles à l'aide d'un éditeur de texte simple tel que le bloc-notes.

Sélectionnez **Exporter au format PKCS#12** et entrez un **mot de passe** et **confirmez le mot de passe**. Sélectionnez ensuite **PC** comme *Exporter vers* : champ. Cliquez sur **Exporter** pour commencer à exporter le certificat vers votre ordinateur.

**Note:** Rappelez-vous ce mot de passe car vous l'utiliserez lors de son importation sur un routeur.

## Export Certificate



1

Export as PKCS#12 format

Enter Password:

2

Confirm Password:

Export as PEM format

Export to:

3

PC  USB



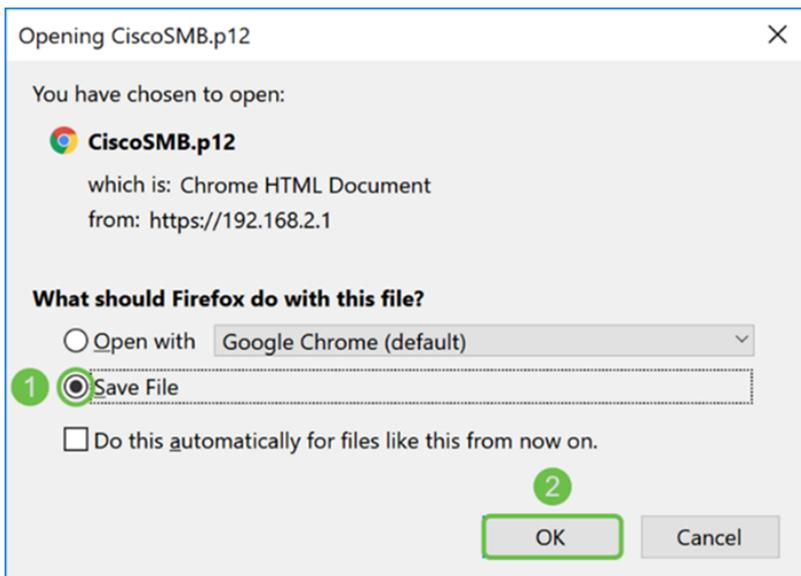
4

Export

Cancel

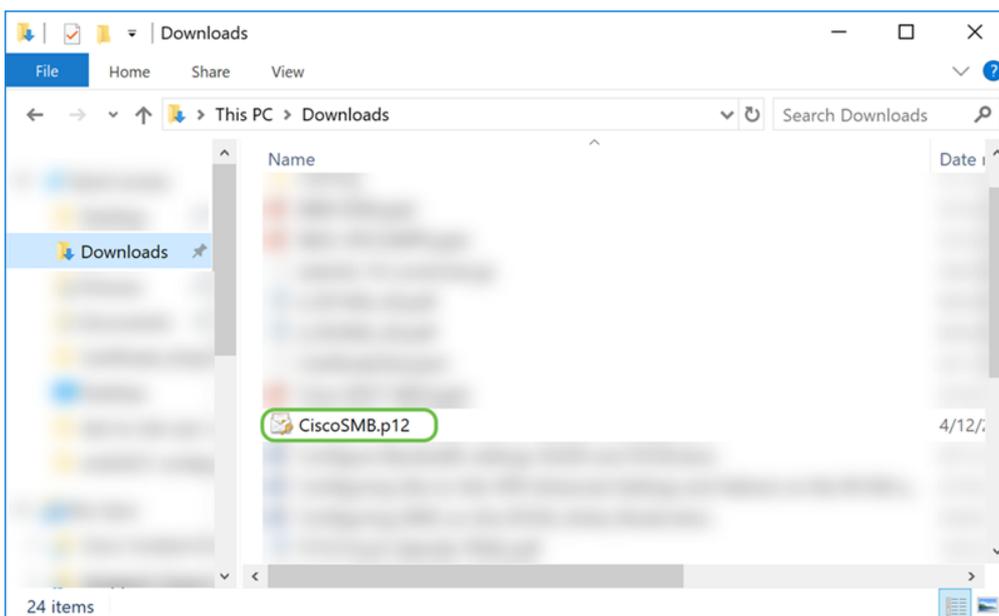
Étape 3. Une fenêtre s'affiche vous demandant ce que vous devez faire avec ce fichier.

Dans cet exemple, nous allons sélectionner **Enregistrer le fichier**, puis cliquez sur **OK**.



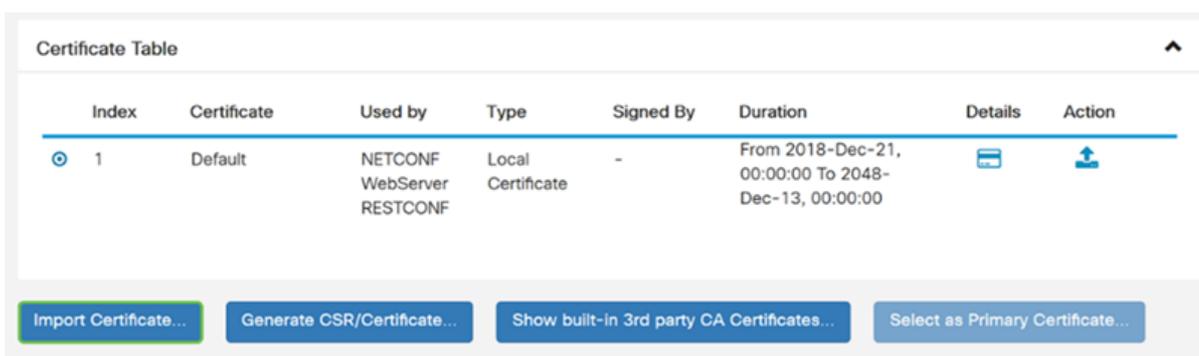
Étape 4. Le fichier doit être enregistré dans votre emplacement de sauvegarde par défaut.

Dans notre exemple, le fichier a été enregistré dans notre dossier *Téléchargements* sur notre ordinateur.



## Importation du certificat

Étape 1. Dans la page *Certificate*, cliquez sur le bouton **Import Certificate...**



Étape 2. Sélectionnez le **type** de certificat à importer dans la liste déroulante *Type* sous

*Importer un certificat.* Les options sont définies comme suit :

**Certificat • AC** - Certificat certifié par une autorité tierce de confiance qui a confirmé que les renseignements contenus dans le certificat sont exacts.

• **Certificat de périphérique local** : certificat généré sur le routeur.

• **PKCS#12 Encoded File** - Public Key Cryptography Standards (PKCS) #12 est un certificat exporté qui se trouve dans une extension .p12.

Dans cet exemple, le type **Fichier codé PKCS#12** a été sélectionné. Entrez un **nom** pour le certificat, puis entrez le **mot de passe** utilisé.

Import Certificate

Type: PKCS#12 Encoded File 1

Certificate Name: CiscoSMB 2

Import Password: ●●●●●●●●●● 3

Upload Certificate file

Import from PC

Browse... No file is selected

Import from USB 

Browse... No file is selected

Étape 3. Dans la section *Télécharger le fichier de certificat*, sélectionnez **Importer à partir du PC** ou **Importer à partir d'USB**. Dans cet exemple, **Importer à partir du PC** a été sélectionné. Cliquez sur **Parcourir...** pour choisir un fichier à télécharger.

### Import Certificate

Type:

Certificate Name:

Import Password:

### Upload Certificate file

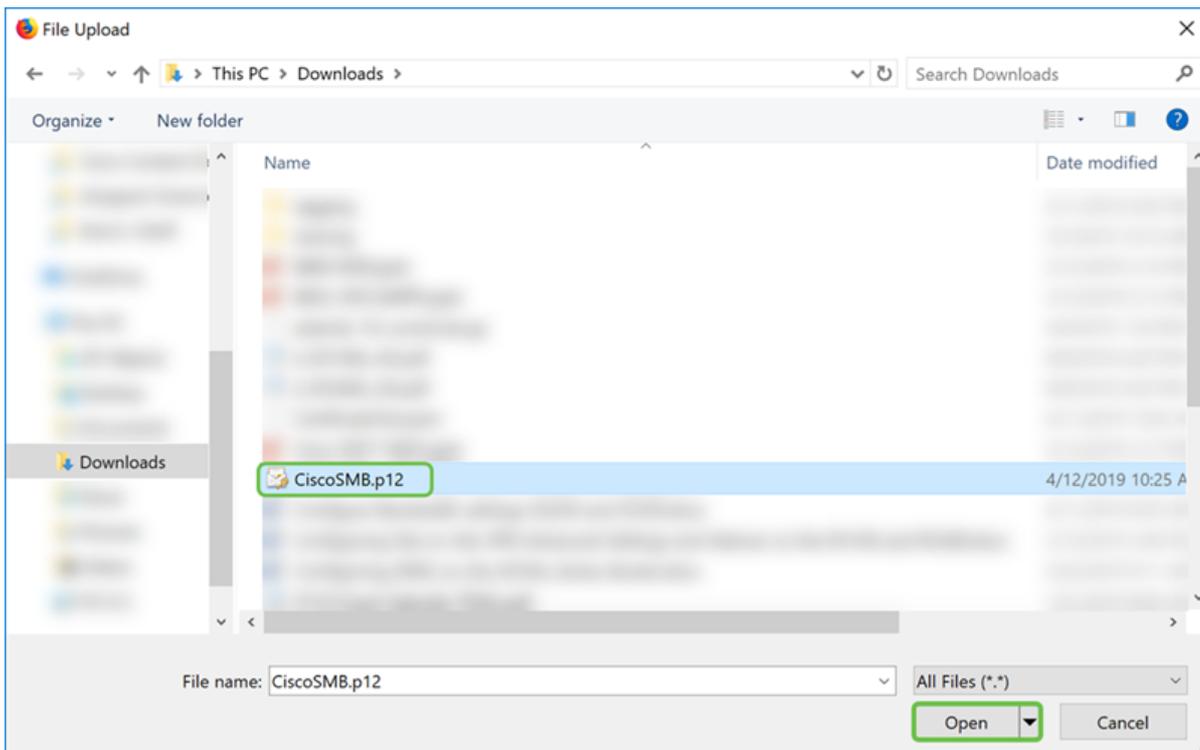
Import from PC

No file is selected

Import from USB 

No file is selected

Étape 4. Dans la fenêtre *File Upload*, accédez à l'emplacement du fichier codé PKCS#12 (extension de fichier .p12). Sélectionnez le fichier .p12, puis cliquez sur **Ouvrir**.



Étape 5. Cliquez sur **Upload** pour commencer à télécharger le certificat.

Certificate

Upload
Cancel

---

Import Certificate

Type: PKCS#12 Encoded File

Certificate Name: CiscoSMB

Import Password: ●●●●●●●●

Upload Certificate file

Import from PC

Browse... CiscoSMB.p12

Import from USB ↻

Browse... No file is selected

Étape 6. Une fenêtre *Informations* s'affiche pour vous indiquer que votre certificat a été importé avec succès. Cliquez sur **OK pour continuer**.

Information
✕

---

i
Import certificate successfully!

OK

Étape 7. Vous devriez voir que votre certificat a été téléchargé.

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

Vous devez avoir appris à générer une demande de service de contact, à importer et à télécharger un certificat sur les routeurs des gammes RV160 et RV260.