

RV160およびRV260シリーズルータの証明書 (CSRのインポート/エクスポート/生成)

目的

このドキュメントの目的は、証明書署名要求(CSR)の生成方法、およびRV160およびRV260シリーズルータでの証明書のインポートとエクスポートの方法を示すことです。

概要

デジタル証明書は、通信プロセスにおいて重要です。認証のためのデジタル識別を提供する。デジタル証明書には、デバイスまたはユーザを識別する情報 (名前、シリアル番号、会社、部署、IPアドレスなど) が含まれます。

認証局(CA)は、デバイスまたはユーザのIDを保証する、証明書の信頼性を検証するために「署名」する信頼できる認証局です。証明書の所有者が本当に誰であるかを確認します。信頼できる署名付き証明書がないと、データが暗号化される可能性があります。通信相手が考えている相手ではない可能性があります。CAは、デジタル証明書を発行するときに公開キーインフラストラクチャ(PKI)を使用します。これは、公開キーまたは秘密キーの暗号化を使用してセキュリティを確保します。CAは、証明書要求の管理とデジタル証明書の発行を担当します。CAの例を次に示します。identrust、コモド、GoDaddy、GlobalSign、GeoTrust、Verisignなど。

証明書は、Secure Socket Layer(SSL)、Transport Layer Security(TLS)、Datagram TLS(DTLS)接続(Hypertext Transfer Protocol(HTTPS)、Secure Lightweight Directory Access Protocol(LDAPS)など)に使用されます。

該当するデバイス

RV160

RV260

[Software Version]

•1.0.00.15

目次

この記事では、次の内容について説明します。

1. [CSR/証明書の生成](#)
2. [証明書の表示](#)

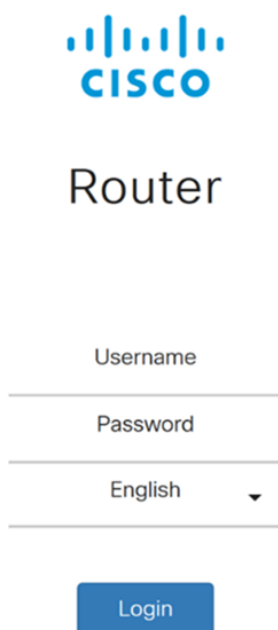
を選択します。 [証明書のエクスポート](#)

4. [証明書インポート](#)

5. [結論](#)

CSR/証明書の生成

ステップ1: Web設定ページにログインします。

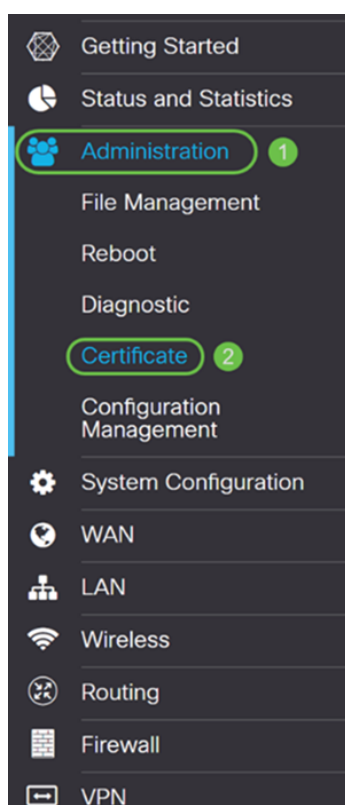


The image shows the Cisco Router login page. At the top is the Cisco logo, followed by the word "Router". Below this are three input fields: "Username", "Password", and a language dropdown menu currently set to "English". A blue "Login" button is positioned below the input fields.

©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.

ステップ2: [Administration] > [Certificate]に移動します。



ステップ3:[Certificate]ページで、[Generate CSR/Certificate...]ボタンをクリックします。

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...

ステップ4：ドロップダウンリストの次のいずれかのオプションから、生成する証明書のタイプを選択します。

自己署名証明書 Σεχυρη Σοχηκετ Λογηρ(ΣΣΛ) この証明書は、攻撃者によって秘密キーが侵害された場合に取り消すことができないため、信頼できません。有効な期間を日数で指定する必要があります。

・ **CA Certificate** セキュリティの観点では、自己署名証明書に似ています。これは OpenVPN に使用できます。

・ **証明書署名要求(CSR)** ΙΔ(ΠΚΙ) 秘密キーは秘密にされるため、自己署名よりも安全です。このオプションが推奨されます。

・ **Certificate Signed by CA Certificate**

この例では、[Certificate Signing Request]を選択します。

Generate CSR/Certificate

Type:

Certificate Signing Request

Certificate Name:

Please enter a valid name.

Subject Alternative Name:

IP Address FQDN Email

ステップ5：証明書名を入力します。この例では、CertificateTestと入力します。

Type:

Certificate Signing Request

Certificate Name:

CertificateTest

Subject Alternative Name:

IP Address FQDN Email

ステップ6:[Subject Alternative Name]フィールドで、次のいずれかを選択します。IPアドレス、FQDN (完全修飾ドメイン名)、または電子メールで、選択した名前から適切な名前を入力します。このフィールドでは、追加のホスト名を指定できます。

この例では、FQDNを選択し、ciscoesupport.comと入力する必要があります。

Type:	<input type="text" value="Certificate Signing Request"/>
Certificate Name:	<input type="text" value="CertificateTest"/>
Subject Alternative Name:	<input type="text" value="ciscoesupport.com"/>
	<input type="radio"/> IP Address <input checked="" type="radio"/> FQDN <input type="radio"/> Email

ステップ7:[国名(C)]ドロップダウンリストから国を選択します。

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"/>

ステップ8:[州名]または[県名]フィールドに都道府県の名前を入力します。

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"/>

ステップ9:「局所性名」に市名を入力します。

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

ステップ10: 「組織名」フィールドに組織の名前を入力します。

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

ステップ11: 組織ユニットの名前 (トレーニング、サポートなど) を入力します。

この例では、組織単位名としてeSupportを入力します。

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

ステップ12：共通名を入力します。この証明書を受信するWebサーバのFQDNです。

この例では、**ciscosbsupport.com**が共通名として使用されています。

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

ステップ13：電子メールアドレスを入力します。

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

ステップ14：ドロップダウンメニューから[Key Encryption Length]を選択します。次のオプションがあります。512、1024 または 2048.キーサイズが大きいほど、証明書の安全性が高くなります。キーサイズが大きいほど、処理時間が長くなります。

ベスト プラクティス:最も長いキー暗号化長を選択し、より強力な暗号化を有効にすることを推奨します。

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

ステップ15:[Generate]をクリックします。

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:







ステップ16:[Information]ポップアップに「Generate certificate successfully!」と表示されます。メッセージに応答します。[OK]をクリックして、次に進みます。

Information ×

 Generate certificate successfully!

OK

ステップ17：証明書テーブルからCSRをエクスポートします。

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...

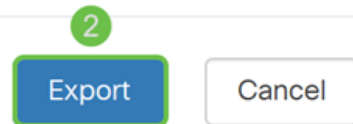
ステップ18:[証明書のエクスポート(Export Certificate)]ウィンドウが表示されます。[書き出し先]の[PC]を選択し、[書き出し]をクリックします。

Export Certificate



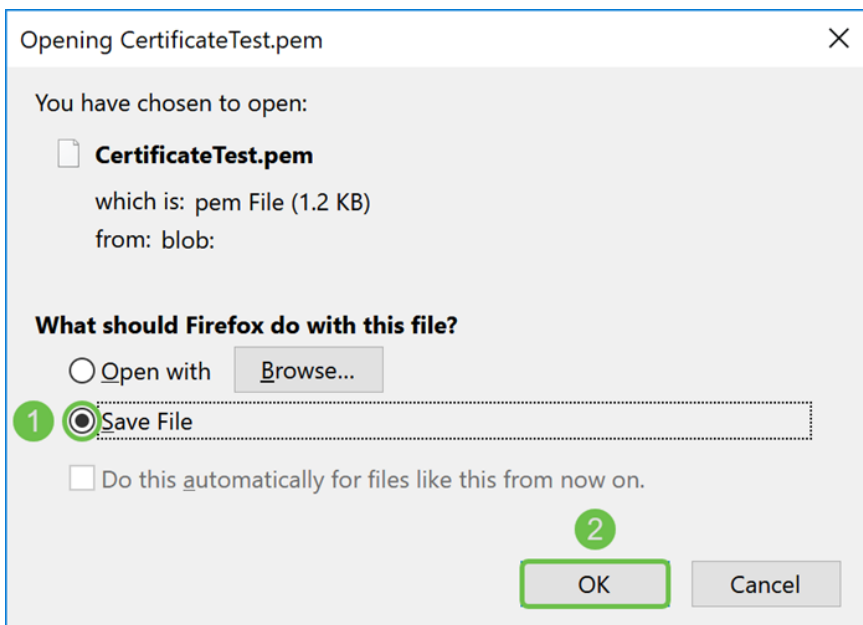
Export as PEM format

Export to:



ステップ19: ファイルを開くか保存するかを尋ねる別のウィンドウが表示されます。

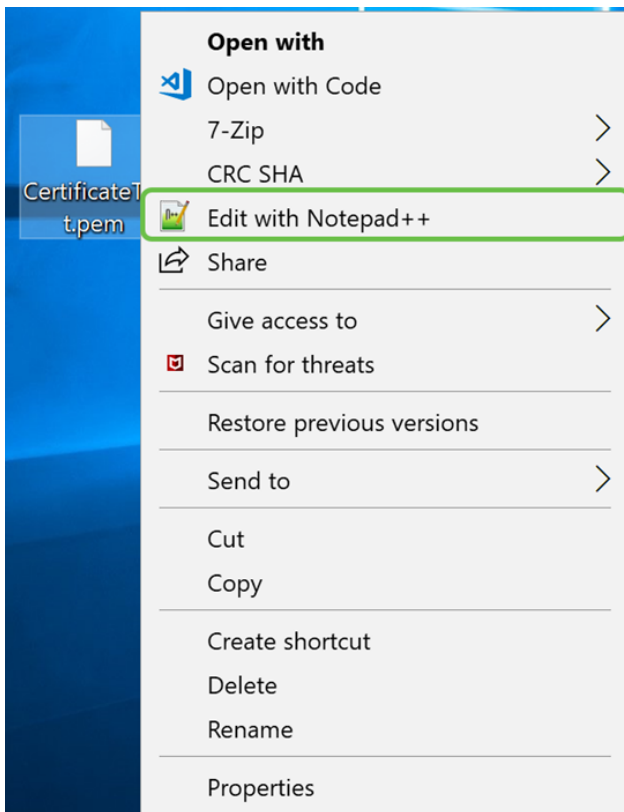
この例では、[ファイルの保存]を選択し、[OK]をクリックします。



ステップ20: .pemファイルが保存された場所を探します。 .pemファイルを右クリックし、お気に入りのテキストエディタで開きます。

この例では、.pemファイルをメモ帳++で開きます。

注: メモ帳で開いてください。



ステップ21:—BEGIN CERTIFICATE REQUEST—および—END CERTIFICATE REQUEST—が独自の行にあることを確認します。

注：証明書の一部がぼやけています。



```
CertificateTest.pem x
1 -----BEGIN CERTIFICATE REQUEST----- 1
2 VBAYTA1VTMQSwCQYDVQQIDAJDQTERMA8GA1UE
3 BwWIU2FuIEpvc2UxDjAMBGNVBAoMBUNpc2NmREwDwYDVQLDAh1U3VwcG9ydDEC
4 MBoGA1UEAwTY21zY29zbWJzdXBwb3J0
5 eWVuQGNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ/r
6 J02/H2TfmIrv1vcs0c+tXmvt8PpCcCFuEaoEvdCcV6kP+TaeDmndcgIdDXNRXplu
7 wSyiqrpS8+kbhzPTF8sHO94Q8wyA8mEu/SjYs0DWuqa2+3LAFOLlp8Cg+e3l0cjs
8 VJS8efDI5j1ECMABvB5Tv
9 soTqNBrYqR8h46NHh0J5fMXDsPY1j2LWmS1VbkskoiMdr5SZlwmhkrqqLby+bfma
10 eOhl0DyX3D7xTV14tvzxYrmDilmpr1eLQc9zME/bZqZgTgY5MgSTGPAis27m29PR
11 oZK/Rpg6Scywbx1X/G0CAwEAAACBkTCBjgYJKoZIhvcNAQkOMYGAMH4wCQYDVR0T
12 BAIw
13 MCcGA1UdJQogMB4GCCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUIAgIwHAYDVR0R
14 BBUwE4IRY21zY29lc3VwcG9ydC5jb20wDQYJKoZIhvcNAQELBQADggEBAI1UeIUy
15 TqFZ2wQx3r29E1SWOU5bmqCj+9IfrsFLR909VdAIJXoUP16CJtc4JJy5+XEhYSnu
16
17
18
19
20
21 -----END CERTIFICATE REQUEST----- 2
22
```

ステップ22:CSRを所有している場合は、ホスティングサービスまたは認証局サイト (GoDaddy、Verisignなど) にアクセスして、証明書を要求する必要があります。要求を送信すると、証明書サーバと通信して、証明書を発行しない理由がないことを確認します。

注：証明書要求がサイトのどこにあるのかわからない場合は、CAまたはホスティングサイトのサポートに連絡してください。







ステップ23：証明書が完了したら、ダウンロードします。ファイルは.cerまたは.crtのいずれ

れかを指定します。この例では、両方のファイルが提供されています。

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

ステップ24：ルータの[Certificate]ページに戻り、デバイスのアイコンを指す矢印をクリックして証明書ファイルをインポートします。

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	-	-		  

ステップ25:[証明書名]フィールドに、証明書の名前を入力します。証明書署名要求と同じ名前を指定することはできません。[証明書ファイルのアップロード]セクションで[PCからインポート]を選択して、[参照]をクリックして証明書ファイルをアップロードします。

Import Signed-Certificate

Type: Local Certificate

Certificate Name: 1

Upload Certificate file

2

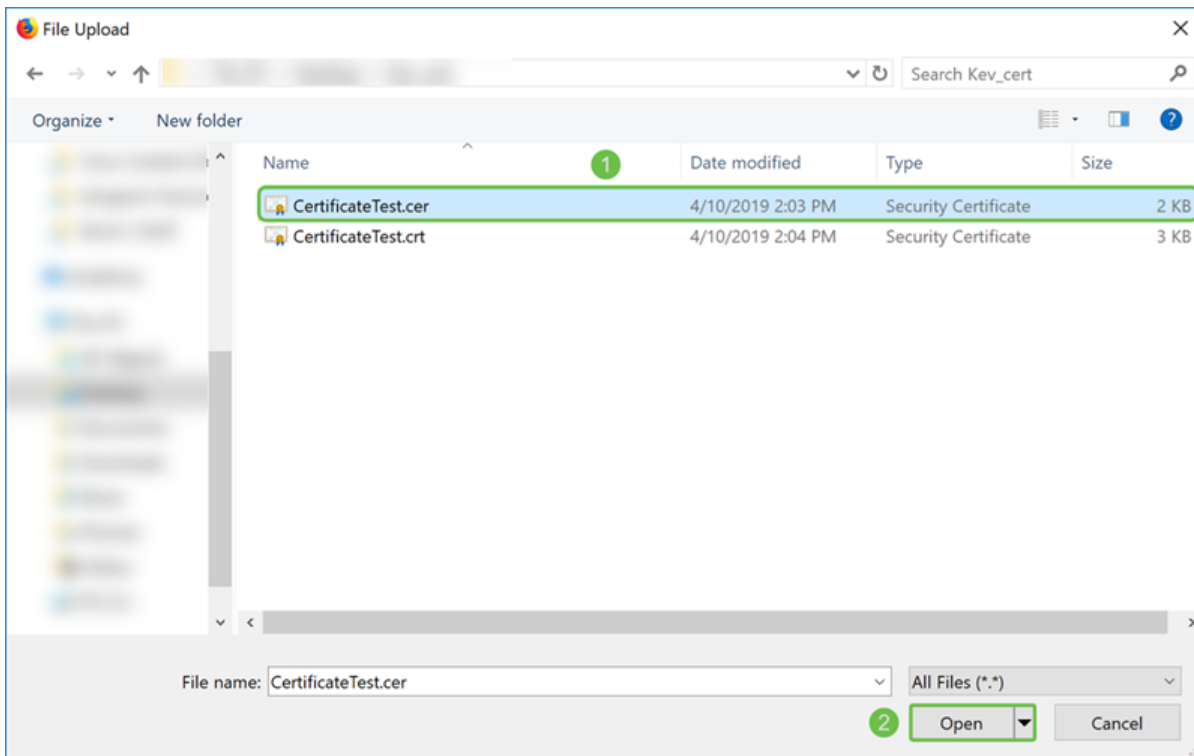
Import from PC

3 No file is selected

Import from USB 

No file is selected

ステップ26:[File Upload]ウィンドウが表示されます。証明書ファイルがある場所に移動します。アップロードする証明書ファイルを選択し、[開く]をクリックします。この例では、CertificateTest.cerが選択されています。



ステップ27:[Upload]ボタンをクリックして、ルータへの証明書のアップロードを開始します。

注：.cerファイルをアップロードできないエラーが発生した場合は、ルータが証明書をpemエンコードで要求している可能性があります。derエンコーディング(.cerファイル拡張子)をpemエンコーディング(.crtファイル拡張子)に変換する必要があります。

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






ステップ28：インポートが正常に完了した場合は、情報ウィンドウが表示されます。[OK]をクリックして、次に進みます。

 Import certificate successfully!

OK

ステップ29：証明書が正常に更新されます。証明書の署名者を確認できます。この例では、証明書が *CiscoTest-DC1-CA* によって署名されていることがわかります。証明書をプライマリ証明書にするには、左側のオプションボタンを使用して証明書を選択し、[プライマリ証明書として選択...] ボタンをクリックします。

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		
① 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...

② Select as Primary Certificate...

注：プライマリ証明書を変更すると、警告ページが表示されることがあります。Firefoxを使用していて、グレーの空白ページとして表示される場合は、Firefoxの設定を調整する必要があります。Mozilla wikiに関するこのドキュメントでは、次の点について説明します。[CA/AddRootToFirefox](#)。警告ページを再び表示するには、Mozillaコミュニティのサポートページで見つかった次の手順に従います。

ステップ30:Firefoxの警告ページで、[Advanced...]をクリックして、[Accept the Risk and Continue]をクリックして、ルータに戻ります。

注：これらの警告画面はブラウザによって異なりますが、同じ機能を実行します。



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...](#)

1
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](#)

2
Go Back (Recommended)

Accept the Risk and Continue

ステップ31：証明書テーブルでは、NETCONF、WebServer、およびRESTCONFが、Default証明書を使用する代わりに新しい証明書とスワップされていることを確認できます。

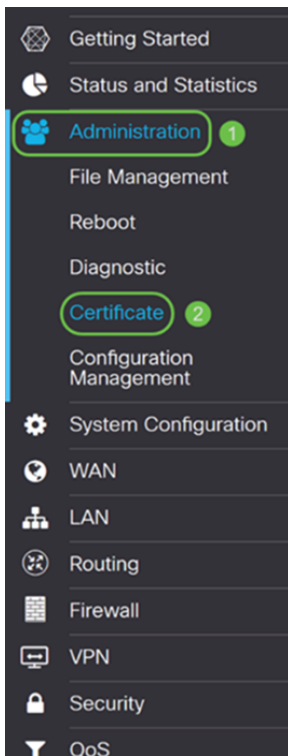
Certificate Table

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		

これで、証明書がルータに正常にインストールされたはずです。

証明書の表示

ステップ1:[証明書]ページから移動した場合、[管理] > [証明書]に移動します。



ステップ2：証明書テーブルで、[詳細]セクションの下にある[詳細]アイコンをクリックします。

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		

ステップ3:[Certificate Detail]ページが表示されます。証明書に関するすべての情報が表示されます。

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

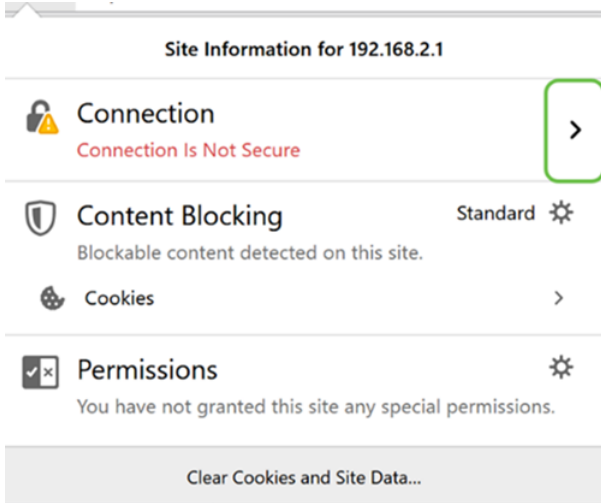
ステップ4:[Uniform Resource Locator (URL)]バーの左側にあるロックアイコンをクリックします。

注 : Firefoxブラウザでは、次の手順を使用します。

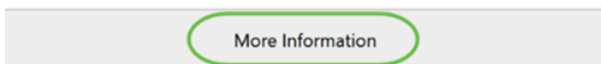
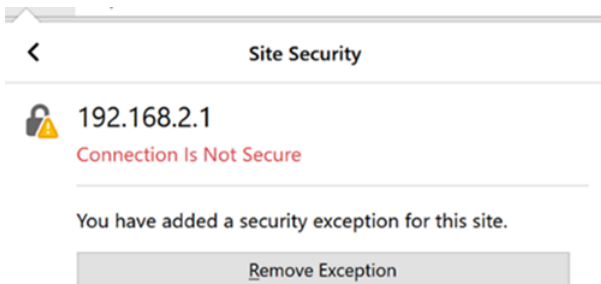
The screenshot shows the Cisco RV160 VPN Router web interface. The browser address bar displays the URL <https://192.168.2.1/#/certificate> with a lock icon highlighted. The interface shows the 'Certificate' configuration page with a table of certificates. The 'CiscoSMB' certificate is selected, and a dropdown menu is visible next to the 'Details' column for that certificate.

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		

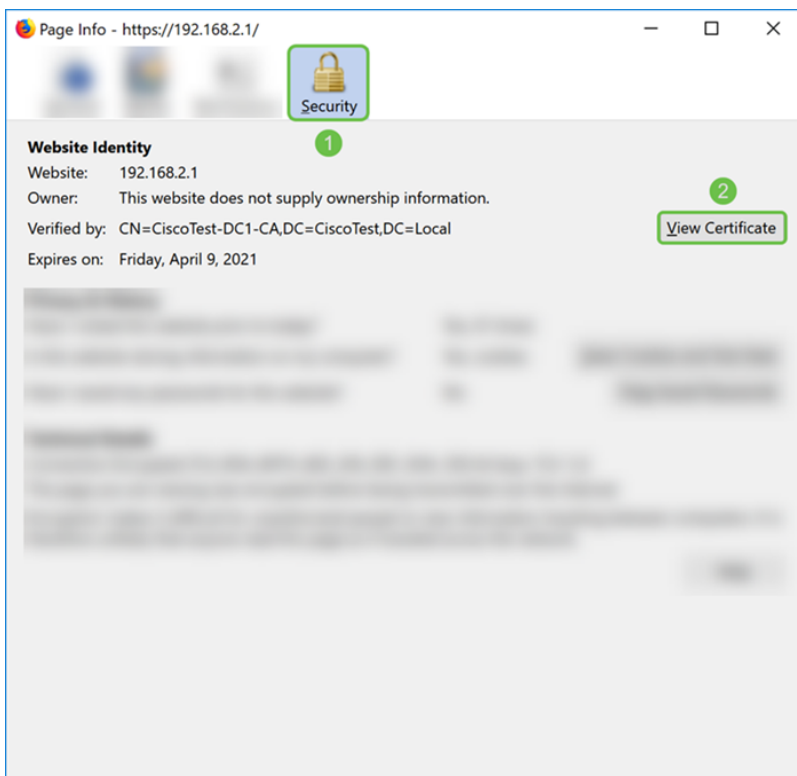
ステップ5 : 選択肢のドロップダウンリストが表示されます。[接続]フィールドの横にある矢印アイコンをクリックします。



ステップ6:[More Information]をクリックします。

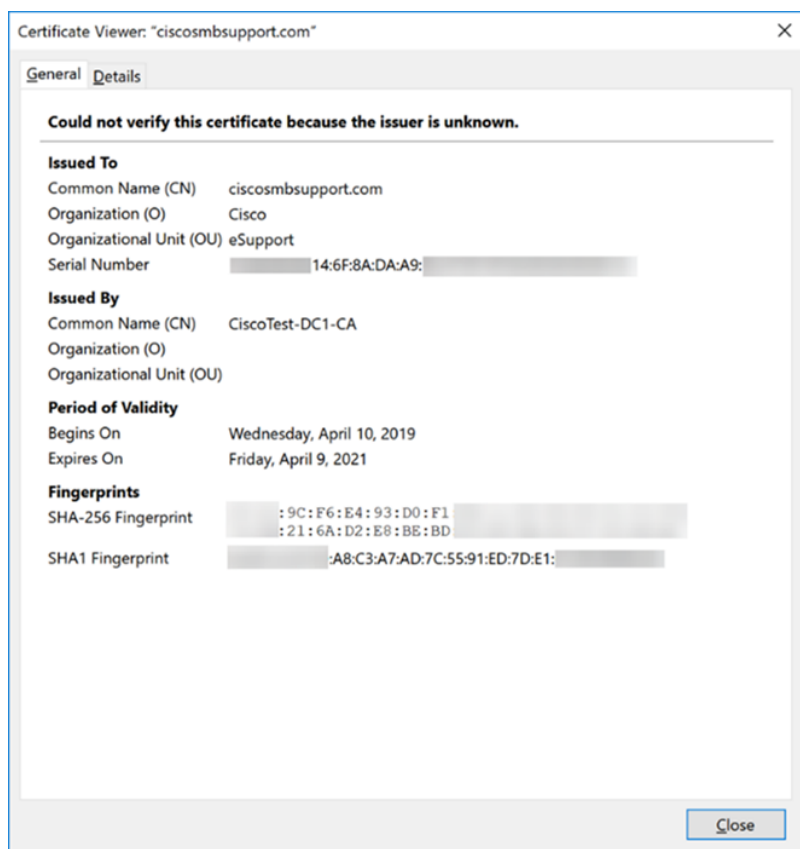


ステップ7:[ページ情報]ウィンドウで、[WebサイトのID]セクションの下に証明書に関する簡単な情報が表示されず。[セキュリティ]タブが表示されていることを確認し、[証明書の表示]をクリックして、証明書の詳細を確認します。



ステップ8:[証明書ビューワー]ページが表示されます。証明書、有効期間、フィンガープリント、発行元に関するすべての情報を確認できます。

注：この証明書はテスト証明書サーバーによって発行されたため、発行者は不明です。



証明書のエクスポート

証明書をダウンロードして別のルータにインポートするには、次の手順を実行します。

ステップ1:[証明書]ページで、エクスポートする証明書の横にあるエクスポートアイコンをクリックします。

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		

ステップ2:[Export Certificate]が表示されます。証明書をエクスポートする形式を選択します。次のオプションがあります。

- **PKCS#12**(ΠΚΧΣ)#12.π12 ファイルを暗号化して、エクスポート、インポート、および削除するときにファイルを保護するには、パスワードが必要です。
- **PEM** – Πρωτογενή Ενημερωθέντα Ματρί (PEM) Ωεβ

[Export as PKCS#12 format]を選択し、パスワードを入力してパスワードを確認します。次に、[エクスポート先]として[PC]を選択します。フィールドにプロンプト間隔値を入力します。[エクスポート]をクリックして、コンピュータへの証明書のエクスポートを開始します。

注：このパスワードは、ルータへのインポート時に使用するため、覚えておいてください。

Export Certificate

×

1

Export as PKCS#12 format

Enter Password:

2

Confirm Password:

Export as PEM format

Export to:

3

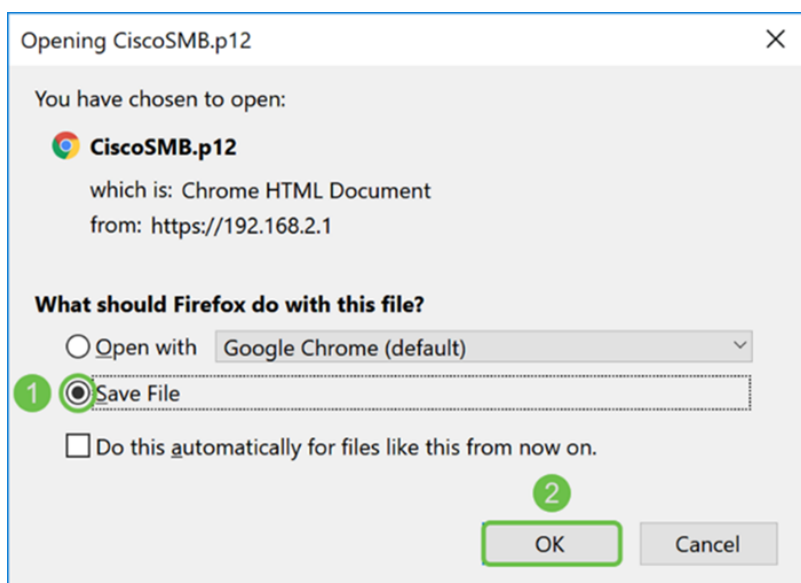
PC USB 

4

Export

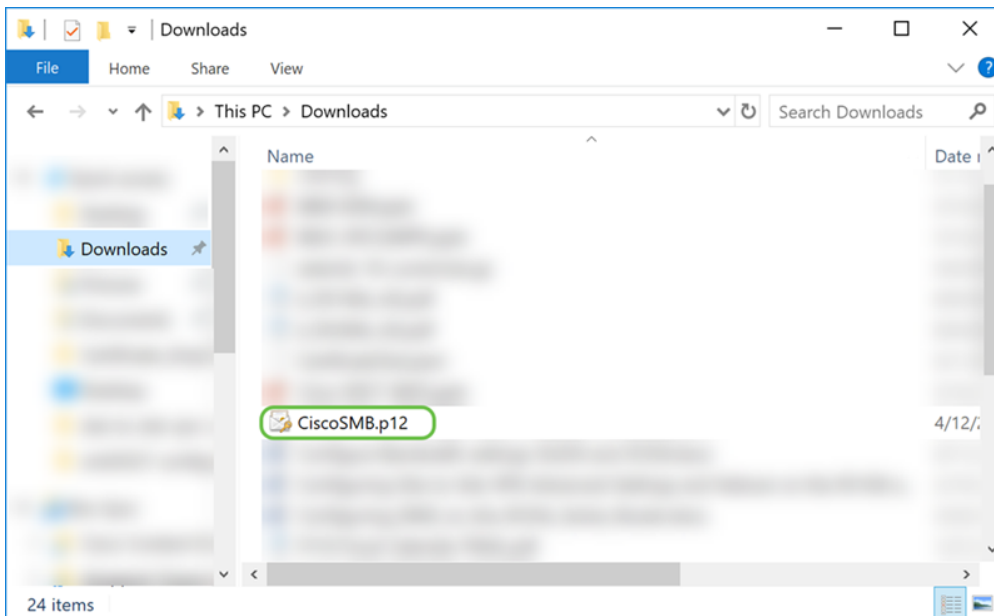
Cancel

ステップ3：このファイルの処理方法を尋ねるウィンドウが表示されます。この例では、[ファイルの保存]を選択し、[OK]をクリックします。



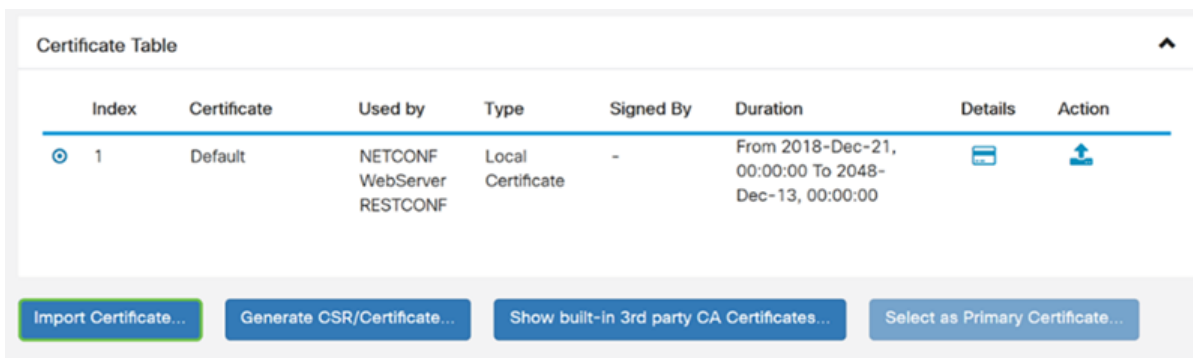
ステップ4：ファイルをデフォルトの保存場所に保存します。

この例では、ファイルはコンピュータのDownloadsフォルダに保存されています。



証明書のインポート

ステップ1:[Certificate]ページで、[Import Certificate...]ボタンをクリックします。



ステップ2:[Import Certificate]セクションの下の[Type]ドロップダウンリストから、インポートする証明書のタイプを選択します。オプションは次のように定義されます。

CA証明書：証明書に含まれる情報が正確であることを確認した、信頼できるサードパーティ認証局によって認証された証明書。

- ・ Local Device Certificate
- ・ PKCS#12エンコードされたファイル(PIKXS)#12.π12

この例では、タイプとして[PKCS#12 Encoded File]が選択されています。証明書の名前を入力し、使用したパスワードを入力します。

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

ステップ3:[証明書ファイルのアップロード]セクションで、[PCからインポート]または[USBからインポート]を選択します。この例では、[Import from PC]が選択されています。[参照...]をクリックして、アップロードするファイルを選択します。

Import Certificate

Type:


Certificate Name:

Import Password:

Upload Certificate file

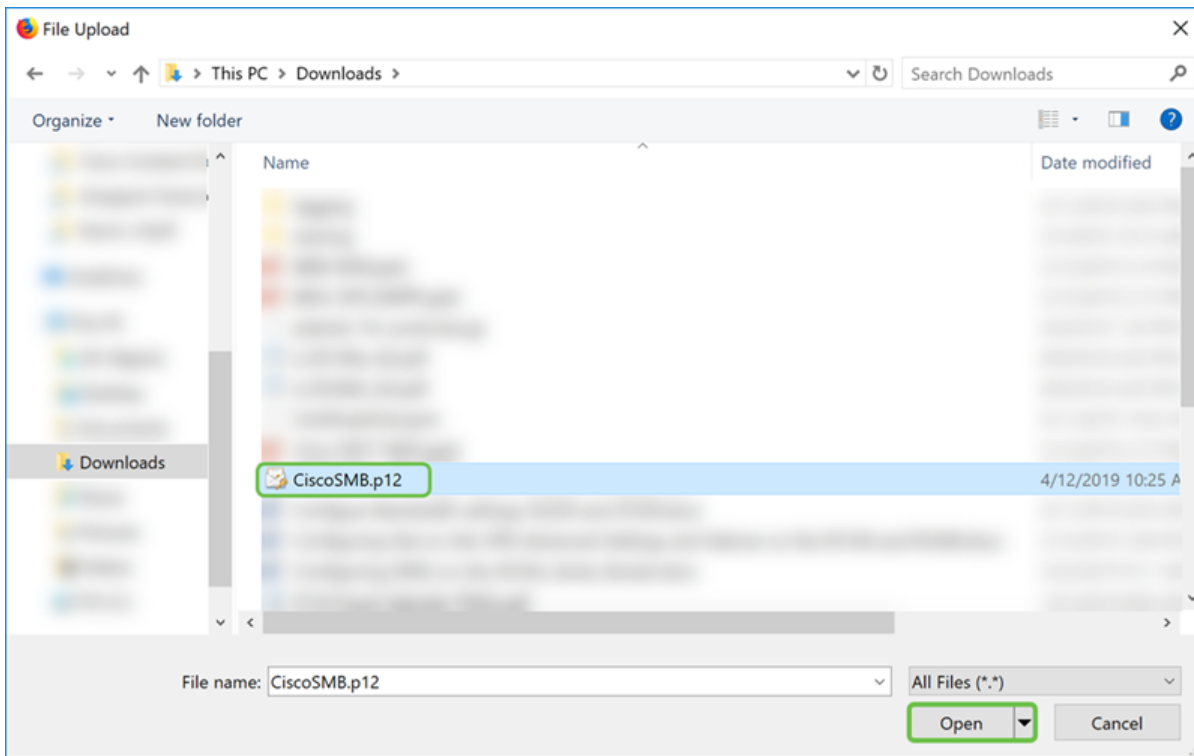
Import from PC

No file is selected

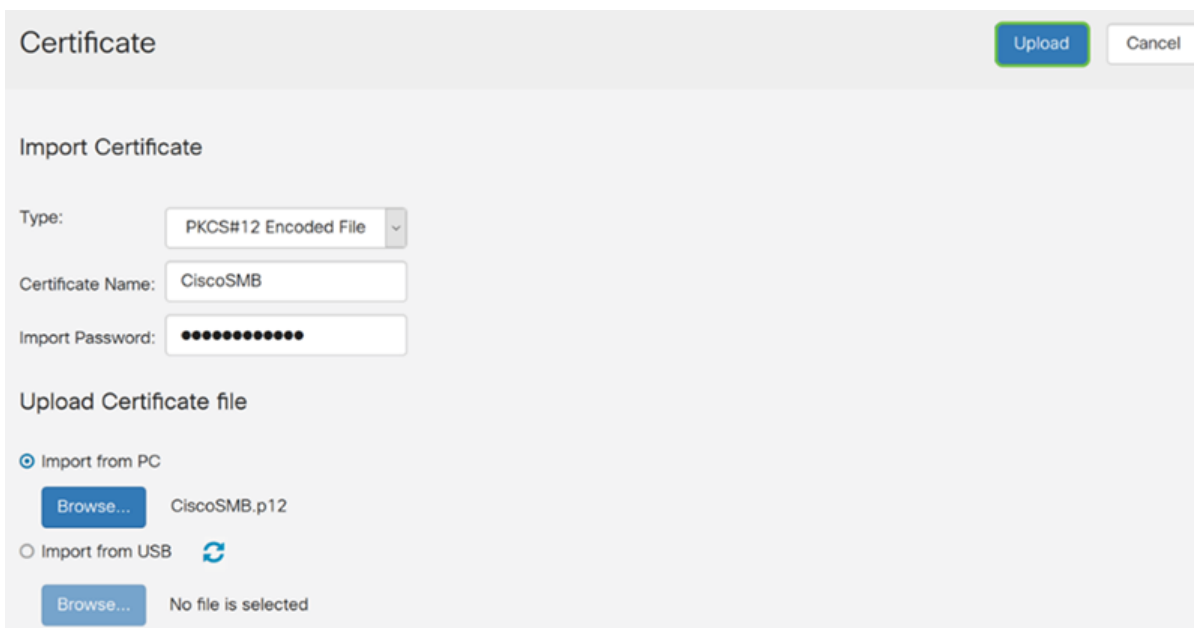
Import from USB 

No file is selected

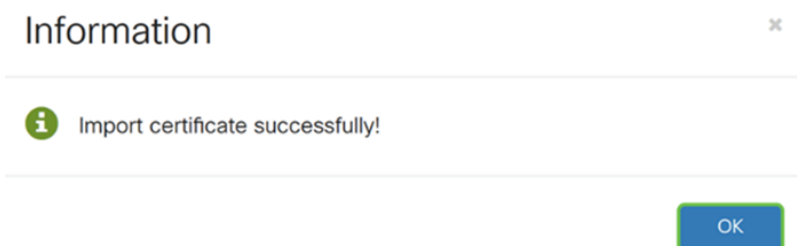
ステップ4:[ファイルのアップロード(File Upload)]ウィンドウで、PKCS#12エンコードされたファイル (.p12ファイル拡張子) がある場所に移動します。.p12ファイルを選択し、[開く]をクリックします。




ステップ5:[Upload]をクリックし、証明書のアップロードを開始します。



ステップ6：証明書が正常にインポートされたことを知らせる[Information]ウィンドウが表示されます。[OK]をクリックして、次に進みます。



ステップ7：証明書がアップロードされたことを確認します。

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		
2	CiscoSMB	-	Local Certificate	CiscoTest- DC1-CA	From 2019-Apr-10, 00:00:00 To 2021- Apr-09, 00:00:00		 

結論

RV160およびRV260シリーズルータでCSRを生成し、証明書をインポートしてダウンロードする方法を正しく学習できているはずです。