

# RV34xシリーズルータでの証明書の管理

## 目的

デジタル証明書は、証明書の名前付きサブジェクトによって公開キーの所有権を証明します。これにより、証明書利用者は、認証された公開キーに対応する秘密キーによる署名やアサーションに依存できます。ルータは、自己署名証明書、つまりネットワーク管理者によって作成された証明書を生成できます。また、認証局(CA)に要求を送信して、デジタルID証明書を申請することもできます。サードパーティアプリケーションから正当な証明書を取得することが重要です。

認証局(CA)からの証明書の取得について説明します。CAは認証に使用されます。証明書は、任意の数のサードパーティサイトから購入します。これは、あなたのサイトが安全であることを証明する公式の方法です。基本的に、CAは正当なビジネスであり、信頼できることを検証する信頼できるソースです。必要に応じて、最小限のコストで証明書を発行します。CAによってチェックアウトされ、情報を確認すると、証明書が発行されます。この証明書は、コンピュータ上のファイルとしてダウンロードできます。その後、ルータ(またはVPNサーバ)に移動し、そこにアップロードできます。

この記事の目的は、RV34xシリーズルータで証明書を生成、エクスポート、インポートする方法を説明することです。

## 該当するデバイス | ソフトウェアバージョン

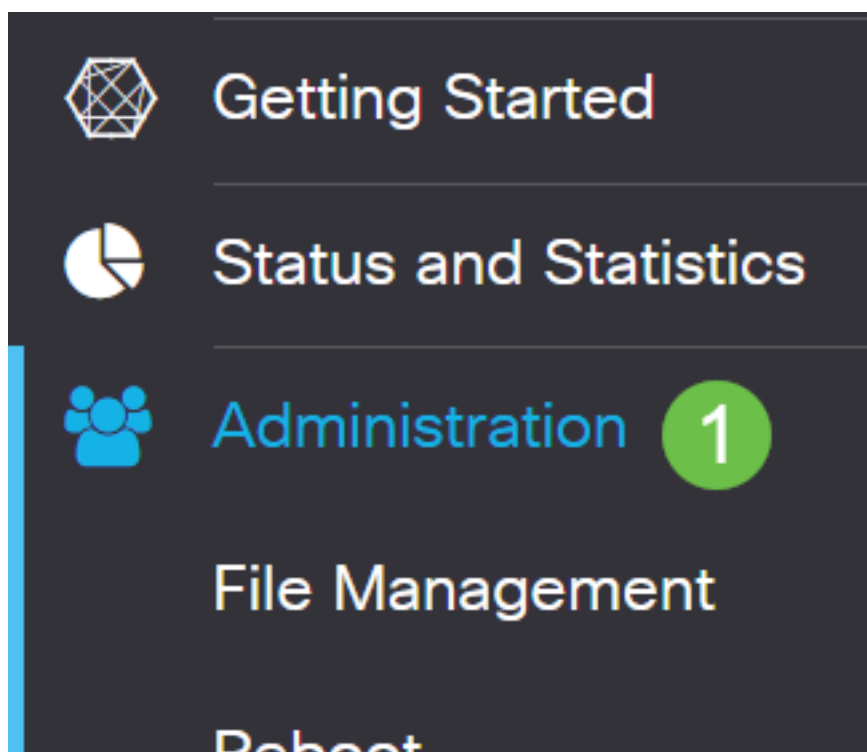
- RV34xシリーズ | 1.0.03.20

## ルータでの証明書の管理

### CSR/証明書の生成

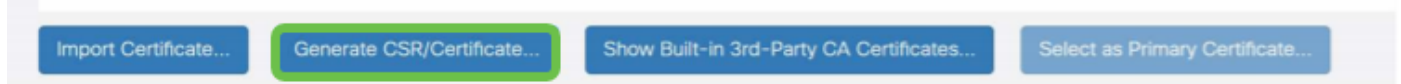
#### 手順 1

ルータのWebベースのユーティリティにログインし、[Administration] > [Certificate]を選択します。



## 手順 2

[Generate CSR/Certificate]をクリックします。[Generate CSR/Certificate]ページが表示されます。



## 手順 3

次の項目を入力します。

- 適切な証明書タイプを選択します
  - 自己署名証明書：これは、独自の作成者によって署名されたSecure Socket Layer(SSL)証明書です。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。
  - 認定署名要求(CSR)：これは、デジタルID証明書を申請するために認証局に送信される公  
開キーインフラストラクチャ(PKI)です。秘密キーは秘密にされるため、自己署名よりも  
安全です。
- 要求を識別する証明書の名前を[証明書名]フィールドに入力します。このフィールドは空白に  
したり、スペースや特殊文字を含めることはできません。
- ( オプション ) [Subject Alternative Name]領域で、オプションボタンをクリックします。次  
のオプションがあります。
  - [IP Address]：インターネットプロトコル(IP)アドレスを入力します
  - [FQDN]：完全修飾ドメイン名(FQDN)を入力します
  - [電子メール]：電子メールアドレスを入力します
- [Subject Alternative Name]フィールドに、FQDNを入力します。
- [国名(Country Name)]ドロップダウンリストから、組織が登録されている国名を選択します。
- 組織が所在する州、州、地域、または地域の名前または省略形を、[州または県名(ST)]フィー  
ルドに入力します。
- 組織が登録されている地域または市区町村の名前を「局所名」フィールドに入力します。
- 会社が法的に登録されている名前を入力します。小規模企業または個人事業主として登録す  
る場合は、[組織名]フィールドに証明書要求者の名前を入力します。特殊文字は使用できませ  
ん。
- 「組織単位名」(Organization Unit Name)フィールドに名前を入力して、組織内の部門間で区  
別します。
- 「共通名」フィールドに名前を入力します。この名前は、証明書を使用するWebサイトの完  
全修飾ドメイン名である必要があります。
- 証明書を生成する個人の電子メールアドレスを入力します。
- [Key Encryption Length]ドロップダウンリストから、キーの長さを選択します。オプションは  
512、1024、および2048です。キーの長さが長いほど、証明書の安全性が高くなります。
- [有効な期間]フィールドに、証明書が有効になる日数を入力します。デフォルト値は 360 で  
す。
- [Generate] をクリックします。

## Certificate

2

Generate

Cancel


## Generate CSR/Certificate









Type:	Self-Signing Certificate
Certificate Name:	TestCACertificate
Subject Alternative Name:	spprtfrms
	<input type="radio"/> IP Address <input checked="" type="radio"/> FQDN <input type="radio"/> Email
Country Name(C):	US - United States
State or Province Name(ST):	Wisconsin
Locality Name(L):	Oconomowoc
Organization Name(O):	Cisco
Organization Unit Name(OU):	Cisco Business
Common Name(CN):	cisco.com
Email Address(E):	_____@cisco.com
Key Encryption Length:	2048
Valid Duration:	360 days (Range: 1-10950, Default: 360)

1

注：生成された証明書が証明書テーブルに表示されます。

Certificate Table ^



<input type="checkbox"/>	Index	Certificate	Used By	Type	Signed By	Duration	Details	Action
<input type="checkbox"/>	1	Default	WebServ...	Local ...	Self Signed	From 2012-Jul-12, 00:00:00 GM To 2042-Jul-05, 00:00:00 GMT		
<input type="checkbox"/>	2	TestCACert...	-	CA C...	Self Signed	From 2018-Apr-04, 00:00:00 GM To 2023-Apr-04, 00:00:00 GMT		
<input type="checkbox"/>	3	Router	-	Local ...	CiscoTest-...	From 2020-Oct-01, 00:00:00 GM To 2022-Oct-01, 00:00:00 GMT		
<input type="checkbox"/>	4	TestCACert...	-	Local ...	Self Signed	From 2020-Nov-19, 00:00:00 GM To 2021-Nov-14, 00:00:00 GMT		


これで、RV345Pルータに証明書が正常に作成されたはずです。









## 証明書のエクスポート

### 手順 1

証明書テーブルで、エクスポートする証明書のチェックボックスをオンにし、エクスポートアイコンをクリックします。

Certificate Table ^



<input type="checkbox"/>	Index	Certificate	Used By	Type	Signed By	Duration	Details	Action
<input type="checkbox"/>	1	Default	WebServ...	Local ...	Self Signed	From 2012-Jul-12, 00:00:00 GM To 2042-Jul-05, 00:00:00 GMT		
<input type="checkbox"/>	2	TestCACert...	-	CA C...	Self Signed	From 2018-Apr-04, 00:00:00 GM To 2023-Apr-04, 00:00:00 GMT		
<input type="checkbox"/>	3	Router	-	Local ...	CiscoTest-...	From 2020-Oct-01, 00:00:00 GM To 2022-Oct-01, 00:00:00 GMT		
<input checked="" type="checkbox"/>	4	TestCACert...	-	Local ...	Self Signed	From 2020-Nov-19, 00:00:00 GM To 2021-Nov-14, 00:00:00 GMT		

1 2

### 手順 2

- 証明書をエクスポートする形式をクリックします。次のオプションがあります。
  - PKCS #12 : 公開鍵暗号規格(PKCS)#12は、.p12拡張子に含まれるエクスポートされた証明書です。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:Privacy Enhanced Mail(PEM)は、メモ帳などの簡単なテキストエディタを使用して簡単に読み取り可能なデータに変換できるように、Webサーバでよく使用されます。
- PEMを選択した場合は、[Export]をクリックします。
- エクスポートするファイルを保護するためのパスワードを[パスワードの入力]フィールドに入力します。
- [パスワードの確認]フィールドにパスワードを再入力します。
- [Select Destination]エリアでは、PCが選択されており、現在利用可能な唯一のオプションです。
- [Export] をクリックします。

## Export Certificate

1

Export as PKCS#12 format

Enter Password

.....

2

Confirm Password

.....

Export as PEM format

Select Destination to Export:

PC

3

4

Export

Cancel

### 手順 3

ダウンロードの成功を示すメッセージが[Download]ボタンの下に表示されます。ファイルのダウンロードがブラウザで開始されます。[OK] をクリックします。



Success

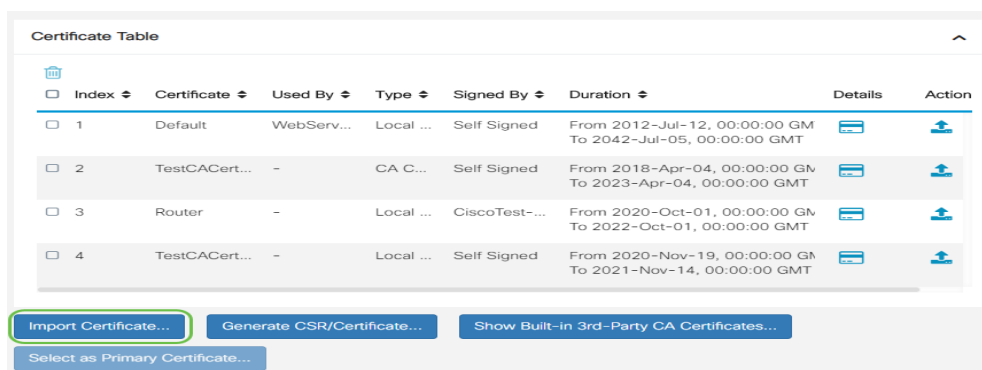
Ok

これで、Rv34xシリーズルータで証明書が正常にエクスポートされました。

## 証明書のインポート

### 手順 1

[Import Certificate...]をクリックします。



### 手順 2

- 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。次のオプションがあります。
  - ローカル証明書：ルータで生成された証明書。
  - 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。
  - PKCS #12 Encodedファイル：公開鍵暗号規格(PKCS)#12は、サーバ証明書を保存する形式です。
- [Certificate Name]フィールドに証明書の名前を入力します。
- PKCS #12を選択した場合は、[Import Password]フィールドにファイルのパスワードを入力します。それ以外の場合は、ステップ 3 に進みます。
- 証明書をインポートするソースをクリックします。次のオプションがあります。
  - PCからのインポート
  - USBからのインポート
- ルータがUSBドライブを検出しない場合、[Import from USB]オプションはグレー表示されます。
- [USBからインポート]を選択し、USBがルータで認識されない場合は、[更新]をクリックします。
- [Choose File]ボタンをクリックし、適切なファイルを選択します。

- [Upload] をクリックします。

### Certificate

3 Upload Cancel  

#### Import Certificate

Type: PKCS#12 encoded file

Certificate Name: cisco 1

Import Password: .....

#### Upload certificate file

Import From PC

2 Browse... TestCACertificate

Import From USB

成功すると、自動的にメインの[Certificate]ページに移動します。証明書テーブルに、最近インポートされた証明書が入力されます。

#### Certificate Table

<input type="checkbox"/>	Index	Certificate	Used By	Type	Signed By	Duration	Details	Action
<input type="checkbox"/>	1	Default	WebServ...	Local ...	Self Signed	From 2012-Jul-12, 00:00:00 GM To 2042-Jul-05, 00:00:00 GMT		
<input type="checkbox"/>	2	TestCACert...	-	CA C...	Self Signed	From 2018-Apr-04, 00:00:00 GM To 2023-Apr-04, 00:00:00 GMT		
<input type="checkbox"/>	3	Router	-	Local ...	CiscoTest-...	From 2020-Oct-01, 00:00:00 GM To 2022-Oct-01, 00:00:00 GMT		
<input type="checkbox"/>	4	TestCACert...	-	Local ...	Self Signed	From 2020-Nov-19, 00:00:00 GM To 2021-Nov-14, 00:00:00 GMT		

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

これで、RV34xシリーズルータに証明書が正常にインポートされたはずです。