

RV34xシリーズルータのデフォルトの自己署名証明書をサードパーティのSSL証明書に置き換える

概要

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ク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規の証明書を取得することが重要です。

CAが証明書に署名する方法は2つあります。

1. CAは秘密キーを使用して証明書に署名します。
2. CAは、RV34xによって生成された証明書署名要求(CSR)を使用して証明書に署名します。

ほとんどの商用の証明書ベンダーは中間証明書を使用します。中間証明書が信頼ルートCAによって発行されると、中間証明書によって発行された証明書は、信頼の証明書チェーンのように、信頼ルートの信頼を継承します。

目的

この記事では、RV34xルータの自己署名証明書を置き換えるために、CAによって発行された3rd party Secure Sockets Layer(SSL)証明書を要求してアップロードする方法を説明します。

該当するデバイス

- RV340
- RV340W
- RV345
- RV345P

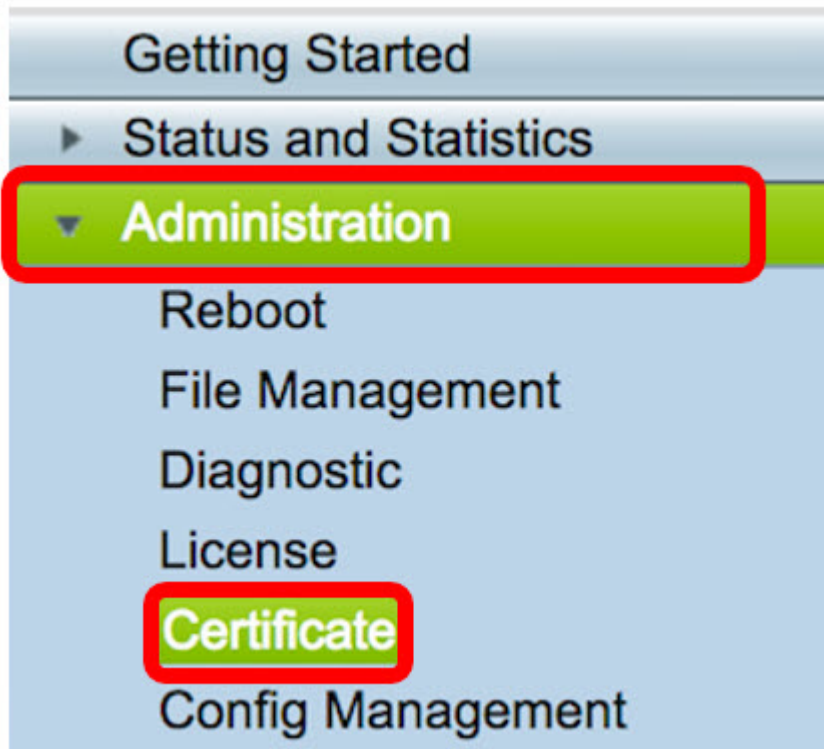
[Software Version]

- 1.0.01.17

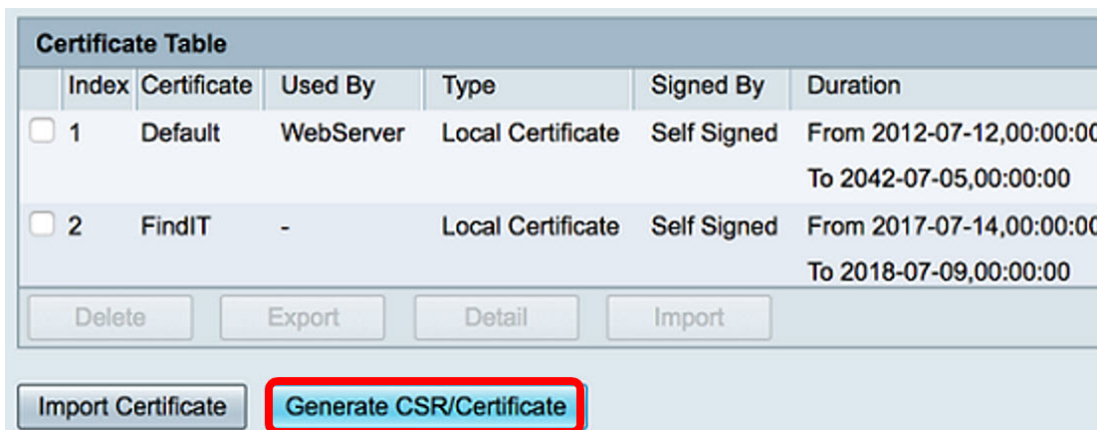
デフォルトの自己署名証明書を3rd Party SSL証明書に置き換え

CSR の生成

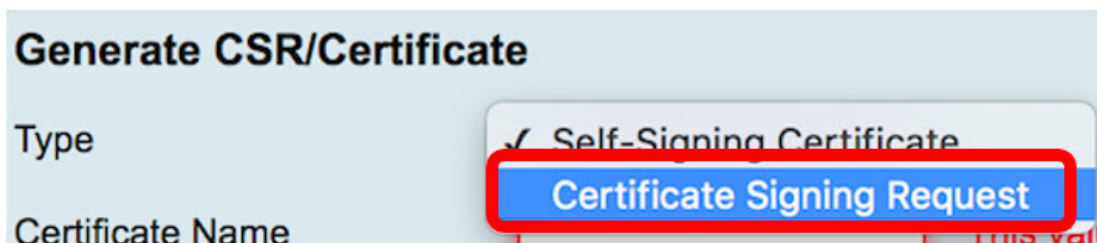
ステップ1：ルータのWebベースのユーティリティにログインし、[Administration] > [Certificate]を選択します。



ステップ2:[Certificate Table]で、[Generate CSR/Certificate]ボタンをクリックします。



ステップ3:[Generate CSR/Certificate]ウィンドウで、[Type]ドロップダウン矢印をクリックして、[Certificate Signing Request]を選択します。



ステップ4:[Certificate Name]フィールドに証明書の名前を入力します。

Generate CSR/Certificate

Type

Certificate Signing Request ▾

Certificate Name

34xrouter

注：この例では、34xrouterが使用されています。

ステップ5:[Subject Alternative Name]フィールドに代替名を入力し、その下の[FQDN]ラジオボタンをクリックして一致させます。代替名は、ルータへのアクセスに使用できるドメイン名です。

Subject Alternative Name

RVrouter.com

IP Address

FQDN

Email

注：この例では、RVrouter.comが使用されています。

ステップ6:[国名(Country Name)]ドロップダウン矢印をクリックして、所在地の国を選択します。

IP Address

FQDN

Email

Country Name

US - United States ▾

注：この例では、[US - United States]が選択されています。

ステップ7:[State or Province Name(ST)]フィールドに州または州の名前を入力します。

Country Name

US - United States ▾

State or Province Name(ST)

California

注：この例では、Californiaが使用されています。

ステップ8:[Locality Name(L)]フィールドにローカリティを入力します。

State or Province Name(ST)

California

Locality Name(L)

Irvine

注：この例では、Irvineが使用されています。

ステップ9：表示されたフィールドに組織名(O)を入力します。

Locality Name(L)	Irvine
Organization Name(O)	Cisco

注：この例では、Ciscoが使用されています。

ステップ10：表示されたフィールドに組織単位名(OU)を入力します。

Organization Name(O)	Cisco
Organization Unit Name(OU)	SBKM

注：この例では、SBKMが使用されています。

ステップ11:[Common Name(CN)]フィールドに名前を入力します。

Organization Unit Name(OU)	SBKM
Common Name(CN)	34xrouter

注：この例では、34xrouterが使用されています。

ステップ12：証明書を送信する電子メールアドレスまたは電子メールアドレスを入力します。

Common Name(CN)	34xrouter
Email Address(E)	@gmail.com

注：この例では、gmail.comの電子メールアドレスが使用されています。

ステップ13：ドロップダウンメニューから[Key Encryption Length]を選択して、キーのビット数を設定します。デフォルトの長さは512です。

Email Address(E)

Key Encryption Length 512 1024 2048

注：この例では、2048 が使用されます。短いキーに比べて長い暗号化の方がデコードが困難なため、セキュリティが向上するため、この方法を強くお勧めします。

ステップ14:[Generate]をクリックします。

Key Encryption Length

作成した証明書要求が証明書テーブルに表示されます。

Certificate Table					
	Index	Certificate	Used By	Type	Signed By
<input type="checkbox"/>	1	Default	WebServer	Local Certificate	Self Signed
<input type="checkbox"/>	2	FindIT	-	Local Certificate	Self Signed
<input type="checkbox"/>	3	34xRouter	-	Certificate Signing Request	-

これで、CSRが正常に生成されました。

CSRのエクスポート

ステップ1：証明書テーブルの証明書要求の横にあるチェックボックスをオンにし、[Export]をクリックします。

Certificate Table					
	Index	Certificate	Used By	Type	
<input type="checkbox"/>	1	Default	WebServer	Local Certificate	
<input type="checkbox"/>	2	FindIT	-	Local Certificate	
<input checked="" type="checkbox"/>	3	34xRouter	-	Certificate Signing Request	

ステップ2:[証明書のエクスポート(Export Certificate)]ウィンドウで[ダウンロード(Download)]をクリックし、PEM形式でファイルをコンピュータにダウンロードします。



これで、CSRをコンピュータにエクスポートできました。

証明書プロバイダーへのCSRのアップロード

ステップ1：ダウンロードしたファイルをメモ帳を使用して開き、CSRをコピーして、サードパーティのSSL証明書プロバイダーサイトにあるフィールドに貼り付けます。

1. Copy and paste your CSR into this box:	<pre>STZJWoGLiyqRIPPHKREghzRfRh9WVW9KWdXzAgMI UzBRMAkGA1UdEwQCMAAwHQYDVR0OBBYEFB24F/ A1UdDwQEAwIF4DAYBgNVHREETAPgg0zNHhyb3VC CwUAA4IBAQAB8J/x6+BLOGr797UeHxBH8sCuBSwQ dYGbl7qzZVVO+b/TvJii7jG52ojYzNDGFWamfYnoCrhv x7+ooeOn9ihoOXxEFKhrn2ueaMZJKQAnFpCwapbsxf pVBnwK74cfF8NBVivtX08SK6qn9qgsvxJcGxmlyBiffV YZITBEWG2Q1TVIY0brOkNbir2VuGoqpsplRqMcq/yE 1WkB91P7hA6X4AB80cKZQEdDsCvrjtgI -----END CERTIFICATE REQUEST-----</pre>
2. Select the server software used to generate the CSR:	Select from list: <input type="button" value="v"/>

注：この例では、証明書プロバイダーとしてComodo.comが使用されています。

ステップ2:CSRの生成に使用するサーバソフトウェアを選択します。この場合、RV34xルータがリストにないので、OTHERが選択されます。

1. Copy and paste your CSR into this box:	<pre>STZJWoGLiyqRIPPHKREghzRfRh9WVW9KWdXzAgMI UzBRMAkGA1UdEwQCMAAwHQYDVR0OBBYEFB24F/ A1UdDwQEAwIF4DAYBgNVHREETAPgg0zNHhyb3VC CwUAA4IBAQAB8J/x6+BLOGr797UeHxBH8sCuBSwQ dYGbl7qzZVVO+b/TvJii7jG52ojYzNDGFWamfYnoCrhv x7+ooeOn9ihoOXxEFKhrn2ueaMZJKQAnFpCwapbsxf pVBnwK74cfF8NBVivtX08SK6qn9qgsvxJcGxmlyBiffV YZITBEWG2Q1TVIY0brOkNbir2VuGoqpsplRqMcq/yE 1WkB91P7hA6X4AB80cKZQEdDsCvrjtgI -----END CERTIFICATE REQUEST-----</pre>
2. Select the server software used to generate the CSR:	<input type="button" value="v"/> OTHER

ステップ3：証明書をコンピュータにダウンロードします。

3rd SSLパーティ証明書のアップロード

ステップ1：ルータのWebベースのユーティリティで、[Certificate Table]の下の[Import

Certificate]ボタンをクリックします。

Certificate Table						
	Index	Certificate	Used By	Type	Signed By	Duration
<input type="checkbox"/>	1	Default	WebServer	Local Certificate	Self Signed	From 2012-07-12,00:00:00 To 2042-07-05,00:00:00
<input type="checkbox"/>	2	FindIT	-	Local Certificate	Self Signed	From 2017-07-14,00:00:00 To 2018-07-09,00:00:00
<input type="checkbox"/>	3	34xRouter	-	Certificate Signing Request	-	-

Delete Export Detail Import

Import Certificate Generate CSR/Certificate

ステップ2:[Import Certificate]ウィンドウで[Type]ドロップダウンメニューをクリックし、[CA Certificate]を選択します。

Import Certificate

Type

✓ Local Certificate

CA Certificate

Certificate Name

PKCS#12 encoded file

ステップ3：表示されたフィールドに証明書名を入力します。

Import Certificate

Type

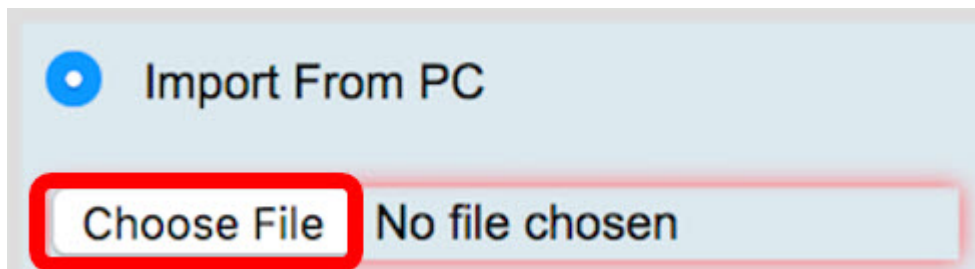
CA Certificate

Certificate Name

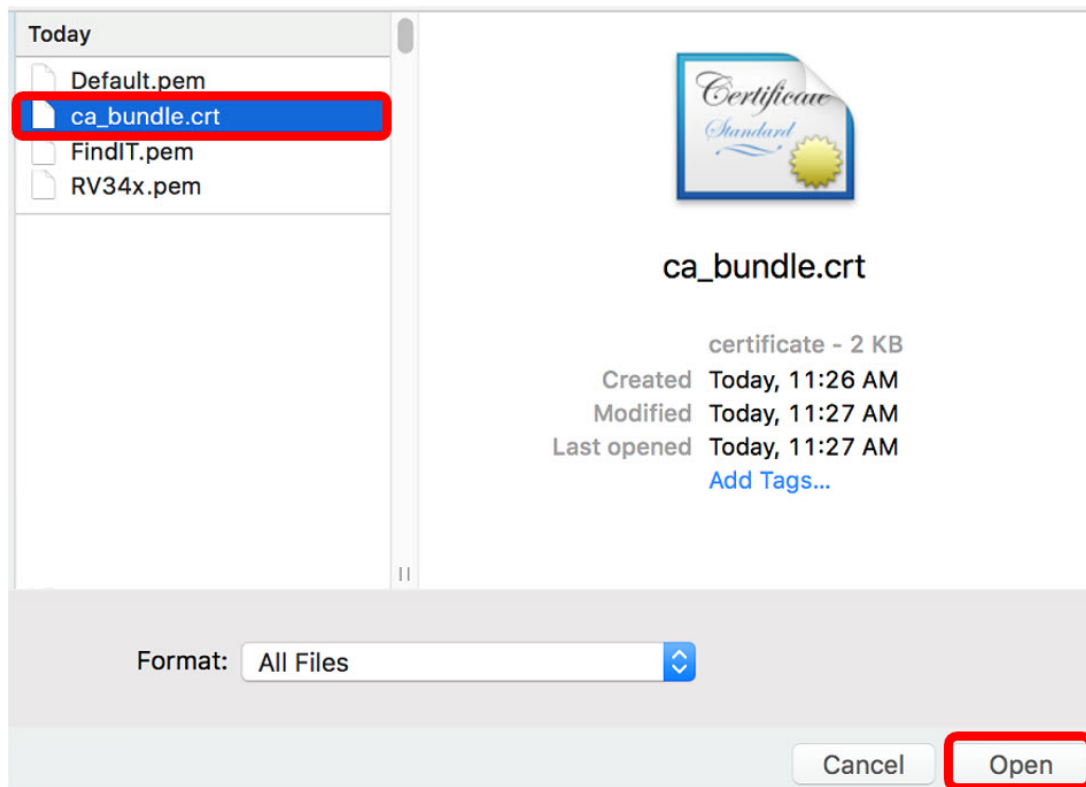
RV34xCert

注：この例では、RV34xCertが使用されています。

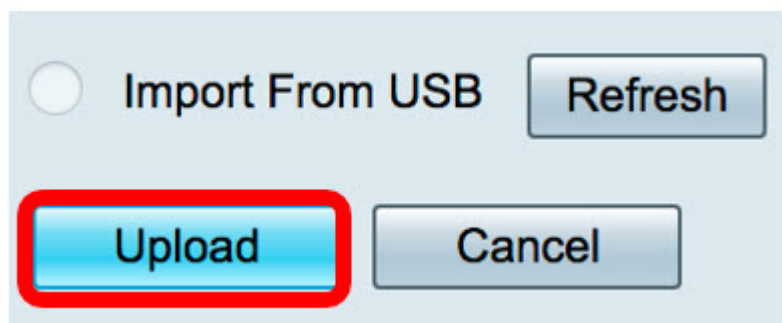
ステップ4:[Choose File]ボタンをクリックし、CAからダウンロードした証明書ファイルを探します。



ステップ5: ファイルをクリックし、[開く]をクリックします。



ステップ6:[Upload]をクリックします。



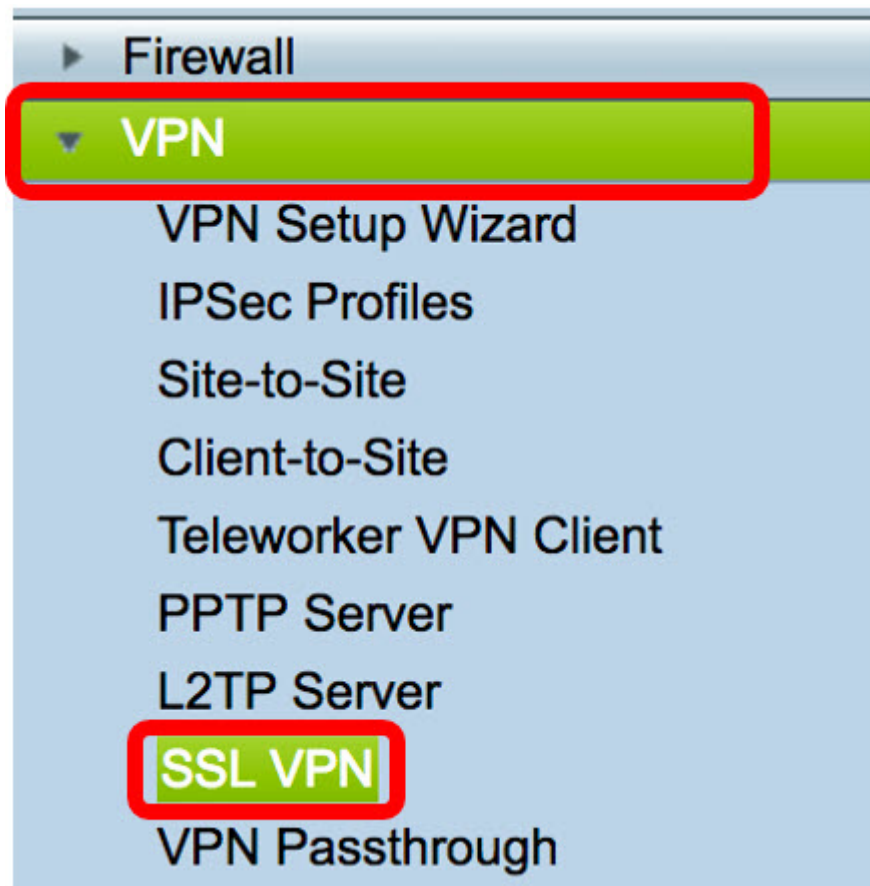
証明書テーブルに新しい証明書名が表示され、タイプがCA証明書に置き換えられ、そのラベルが3rd party CAによって署名された。

Certificate Table						
Index	Certificate	Used By	Type	Signed By	Duration	
<input type="checkbox"/> 1	Default	WebServer	Local Certificate	Self Signed	From 2012-07-12,00:00:00 To 2042-07-05,00:00:00	
<input type="checkbox"/> 2	FindIT	-	Local Certificate	Self Signed	From 2017-07-14,00:00:00 To 2018-07-09,00:00:00	
<input type="checkbox"/> 3	RV34xCert	-	CA Certificate	DST Root CA X3	From 2016-03-17,00:00:00 To 2021-03-17,00:00:00	

これで、RV34xルータに3rd party SSL証明書が正常にアップロードされました。

デフォルトの自己署名証明書の置き換え

ステップ1: Webベースのユーティリティで、[VPN] > [SSL VPN]を選択します。



ステップ2: [On] オプションボタンをクリックして、Cisco SSL VPNサーバを有効にします。

SSL VPN

General Configuration

Group Policies

Cisco SSL VPN Server On Off

ステップ3:[Mandatory Gateway Settings]で、[Certificate File]ドロップダウンメニューをクリックし、新しくアップロードしたSSL証明書を選択してデフォルトの証明書を置き換えます。

Mandatory Gateway Settings

Gateway Interface

Gateway Port (Range: 1-65535)

Certificate File
 Default
 FindIT

Client Address Pool

ステップ4：表示されたフィールドに必要なクライアントドメインを入力します。

Certificate File

Client Address Pool

Client Netmask

Client Domain

注：この例では、RVrouter.comが使用されています。

ステップ5:[Apply]をクリックします。



これで、デフォルトの自己署名証明書が3rd party SSL証明書に正しく置き換えられました。

次の記事も参考になります。[RV34xシリーズルータに関するFAQ](#)

このサイトには、興味深い記事へのリンクが掲載されています。[RV34xシリーズルータ製品ページ](#)