

# RV320およびRV325 VPNルータでのマイ証明書の設定

## 目的

証明書は、個人またはデバイスのIDの確認、サービスの認証、またはファイルの暗号化に使用されます。RV320では、自己署名またはサードパーティ認証によって最大50個の証明書を追加できます。クライアントまたは管理者の証明書をエクスポートし、PCまたはUSBデバイスに保存してからインポートできます。

このドキュメントの目的は、プライマリ証明書の選択、証明書のエクスポート、およびRV32xシリーズVPNルータでの証明書のインポートの方法を説明することです。

## 該当するデバイス

- ・ RV320デュアルWAN VPNルータ
- ・ RV325ギガビットデュアルWAN VPNルータ

## [Software Version]

- ・ v1.1.0.09

## 自分の証明書

ステップ1: Web構成ユーティリティにログインし、[Certificate Management] > [My Certificate]を選択します。[My Certificate]ページが開きます。



My Certificate						
My Certificate Table						
Used	Type	Subject	Duration	Details	Export	
<input checked="" type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06			
<input type="radio"/>	Certificate Signing Request	CN=com OU=so				CSR
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29			

Buttons: Add, Delete, Select as Primary Certificate

証明書には2つのタイプがあります。

- ・ 自己署名：独自の作成者によって署名されたSecure Socket Layer(SSL)証明書。このタイプは、秘密鍵が攻撃者によって侵害された場合にキャンセルできないため、安全性が低くなります。
- ・ 証明書署名要求(CSR)：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)。秘密キーは秘密にされるため、自己署名よりも安全です。

ステップ2:[My Certificate Table]から目的のラジオボタンをクリックして、証明書を選択します。

ステップ3:[Select as Primary Certificate]をクリックして、選択した証明書をプライマリ証明書にします。

ステップ4: ( オプション ) 証明書に関する詳細情報を表示するには、[詳細]アイコンをクリックします。

My Certificate					
My Certificate Table					
Used	Type	Subject	Duration	Details	Export
<input checked="" type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input type="radio"/>	Certificate Signing Request	CN=com OU=so			
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		

[証明書の詳細]ウィンドウが開きます。

Certificate Details	
<b>Certificate Information</b>	
Version:	3
Serial Number:	D8 AF 62 26 26 36 5D D1
<b>Subject Information</b>	
Subject:	CN=6c:20:56:c6:16:52 OU=RV320 O=Cisco Systems, Inc. L=Irvine C=US ST=California
Public Key Algorithm:	rsaEncryption -
Subject Key Identifier:	2D E3 89 6D FC 43 76 2B AF 1D AC 2B F1 EB 11 D3 19 FE AD 63
<b>Issuer Information</b>	
Issuer:	CN=6c:20:56:c6:16:52 OU=RV320 O=Cisco Systems, Inc. L=Irvine C=US ST=California
Valid From:	Apr 8 19:12:48 2013 GMT
Valid Through:	Apr 6 19:12:48 2023 GMT
Signature Algorithm:	sha1WithRSAEncryption
Authority Key Identifier:	2D E3 89 6D FC 43 76 2B AF 1D AC 2B F1 EB 11 D3 19 FE AD 63
Fingerprint:	33 C4 E6 40 7D DD 1F 44 32 57 18 A9 AA D1 66 FB 5A B2 CD 36

ステップ5: ( オプション ) 証明書を削除するには、削除する証明書のオプションボタンをクリックし、[削除]をクリックします。

ステップ6:[Save]をクリックして設定を保存します。

## 自己署名証明書のエクスポート

ステップ1:[Export ( エクスポート ) ]列の目的のアイコンボタンをクリックして、自己署名証明書をエクスポートします。



My Certificate					
My Certificate Table					
Used	Type	Subject	Duration	Details	Export
<input checked="" type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input type="radio"/>	Certificate Signing Request	CN=com OU=so			
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		

Buttons: Add, Delete, Select as Primary Certificate

使用可能なアイコンボタンは次のように定義されます。

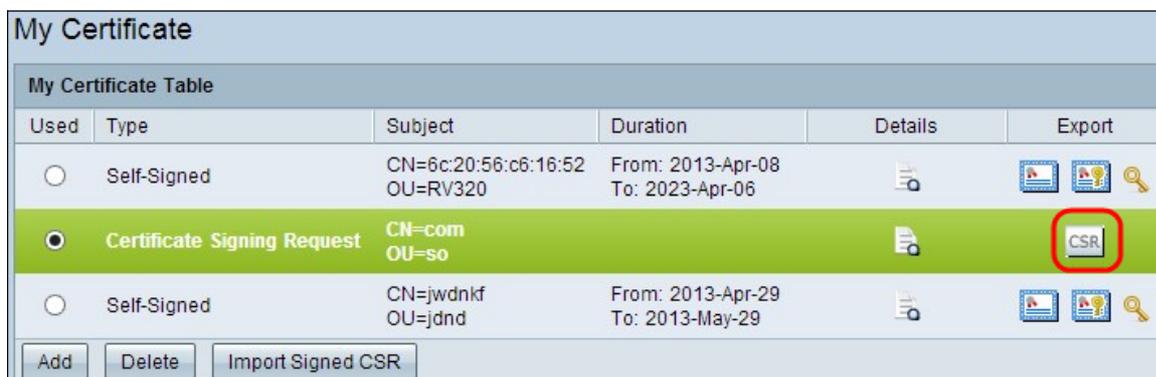
- ・ Export Certificate for Client : クライアントをバーチャルプライベートネットワーク (VPN)に接続するために使用されるクライアント証明書をエクスポートします。
- ・ Export Certificate for Administrator – 管理者証明書をエクスポートします。秘密キーが生成され、バックアップ用にコピーが保持されます。
- ・ Export Private Key:VPNクライアントソフトウェアの秘密キーをエクスポートします。VPN接続には別のクレデンシャルが必要です。

ステップ2:[開く]をクリックしてキーを表示します。

ステップ3:[Save]をクリックして、キーを保存します。

## 証明書署名要求のエクスポート

ステップ1:[CSR]をクリックします ( 証明書署名要求のエクスポート ) 。



My Certificate					
My Certificate Table					
Used	Type	Subject	Duration	Details	Export
<input type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input checked="" type="radio"/>	Certificate Signing Request	CN=com OU=so			
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		

Buttons: Add, Delete, Import Signed CSR

ステップ2:[Open]をクリックして表示します。

ステップ3:[Save]をクリックして、PCまたはUSBのキーを保存します。

## 証明書のインポート

ステップ1:[Add]をクリックして**証明書**をインポートします。

My Certificate					
My Certificate Table					
Used	Type	Subject	Duration	Details	Export
<input type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input checked="" type="radio"/>	Certificate Signing Request	CN=com OU=so			
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		

次のウィンドウが表示されます。

My Certificate	
<input checked="" type="radio"/>	3rd-Party Authorized
<input type="radio"/>	Self-Signed
<b>Import Full Certificate Set</b>	
<input checked="" type="radio"/>	Import from PC
CA Certificate:	<input type="button" value="Choose File"/> No file chosen ( PEM format )
Certificate + Private Key:	<input type="button" value="Choose File"/> No file chosen ( PEM format )
<input type="radio"/>	Import from USB Device
USB Device Status:	No Device Attached <input type="button" value="Refresh"/>
<input type="button" value="Save"/>	<input type="button" value="Cancel"/>

ステップ2：目的のオプションボタンをクリックして、インポートする証明書のタイプを定義します。

My Certificate	
<input checked="" type="radio"/>	3rd-Party Authorized
<input type="radio"/>	Self-Signed
<b>Import Full Certificate Set</b>	
<input checked="" type="radio"/>	Import from PC
CA Certificate:	<input type="button" value="Choose File"/> No file chosen ( PEM format )
Certificate + Private Key:	<input type="button" value="Choose File"/> No file chosen ( PEM format )
<input type="radio"/>	Import from USB Device
USB Device Status:	No Device Attached <input type="button" value="Refresh"/>
<input type="button" value="Save"/>	<input type="button" value="Cancel"/>

- ・ 3rd-Party Authorized：認証局がデジタル署名を提供する公開キーインフラストラクチャ

(PKI)。

- ・ 自己署名：独自の作成者によって署名されたSecure Socket Layer(SSL)証明書。

ステップ3：目的のオプションボタンをクリックして、証明書のインポート方法を選択します。

My Certificate

3rd-Party Authorized  
 Self-Signed

Import Full Certificate Set

Import from PC  
CA Certificate:  No file chosen ( PEM format )  
Certificate + Private Key:  No file chosen ( PEM format )

Import from USB Device

- ・ PCからインポート – 証明書は、保存したPCからインポートされます。
- ・ USBからインポート – 証明書がUSBドライブからインポートされます。

## PCからの証明書のインポート

ステップ1：サードパーティの承認済み証明書をインポートする場合は、[CA Certificate]の横にある[Choose File]をクリックし、ファイルの場所を参照して選択します。

ステップ2:[Certificate + Private Key]の横にある[Choose File]をクリックし、ファイルの場所を参照して選択します。

ステップ3:[Save]をクリックして設定を保存します。インポートされた証明書が[マイ証明書テーブル]に表示されます。

My Certificate

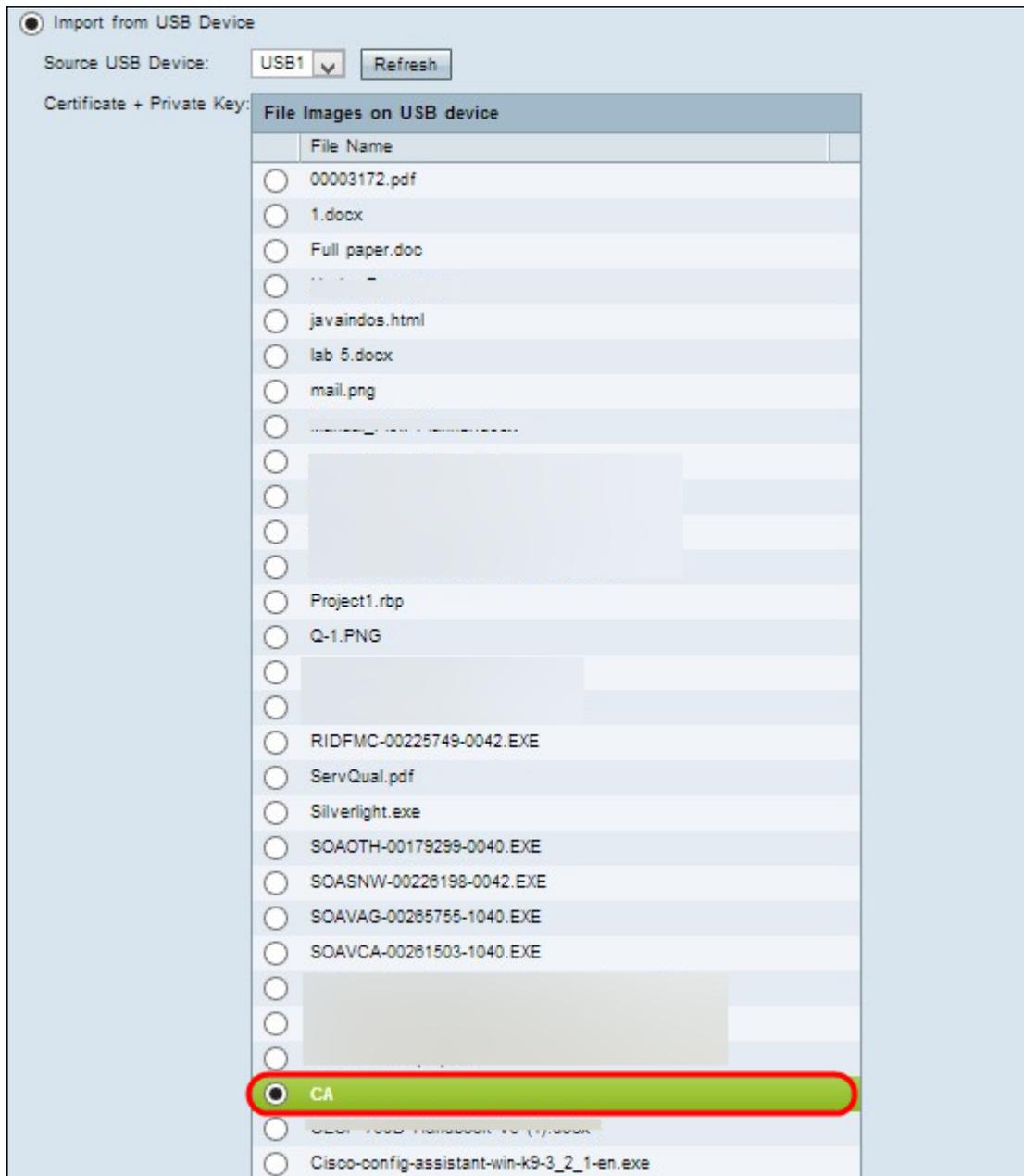
My Certificate Table

Used	Type	Subject	Duration	Details	Export
<input checked="" type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input type="radio"/>	Certificate Signing Request	CN=com OU=so			
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		
<input type="radio"/>	Self-Signed	CN= OU=			

## USBからの証明書のインポート

ステップ1:[Source USB Device]ドロップダウンリストから適切なUSBデバイスを選択しま

す。



ステップ2：サードパーティ認証証明書をインポートする場合は、該当するオプションボタンをクリックして、USBに保存したCA証明書をインポートします。

ステップ3：適切なオプションボタンを選択して、USBに保存した証明書+秘密キーをインポートします。

ステップ4:[Save]をクリックして設定を保存します。インポートされた証明書が[マイ証明書テーブル]に表示されます。

## My Certificate

My Certificate Table					
Used	Type	Subject	Duration	Details	Export
<input checked="" type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		  
<input type="radio"/>	Certificate Signing Request	CN=com OU=so			
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		  
<input type="radio"/>	Self-Signed	CN= OU=			  