

在RV320和RV325 VPN路由器上配置我的证书

目标

证书用于验证个人或设备的身份、验证服务或加密文件。在RV320上，您可以通过自签名或第三方授权最多添加50个证书。您可以导出客户端或管理员的证书并将其保存在PC或USB设备上，然后导入。

本文档旨在向您展示如何在RV32x系列VPN路由器上选择主证书、导出证书和导入证书。

适用设备

- RV320双WAN VPN路由器
- RV325千兆双WAN VPN路由器

软件版本

- v1.1.0.09

我的证书

步骤1.登录Web配置实用程序，然后选择Certificate Management > **My Certificate**。“我的证书”页打开：



The screenshot shows the 'My Certificate' management page. It features a table with columns for 'Used', 'Type', 'Subject', 'Duration', 'Details', and 'Export'. Three certificates are listed: a selected 'Self-Signed' certificate (CN=6c:20:56:c6:16:52, OU=RV320, valid from 2013-Apr-08 to 2023-Apr-06), a 'Certificate Signing Request' (CN=com, OU=so), and another 'Self-Signed' certificate (CN=jwdnkf, OU=jdnd, valid from 2013-Apr-29 to 2013-May-29). Below the table are buttons for 'Add', 'Delete', and 'Select as Primary Certificate'.

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		

证书分为两种类型：

- 自签名 — 由其自己的创建者签名的安全套接字层(SSL)证书。此类型的安全性较低，因为如果私钥被攻击者破坏，则无法取消它。
- 证书签名请求 — 发送到证书颁发机构以申请数字身份证书的公钥基础设施(PKI)。它比自签名更安全，因为私钥是保密的。

步骤2.从My Certificate Table中单击所需的单选按钮以选择证书。

步骤3.单击**Select as Primary Certificate**，使所选证书成为主证书。

步骤4. (可选) 要查看有关证书的详细信息，请点击**详细信息**图标。

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		

“证书详细信息”窗口打开：

Certificate Details	
Certificate Information	
Version:	3
Serial Number:	D8 AF 62 26 26 36 5D D1
Subject Information	
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
Issuer Information	
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

步骤5. (可选) 要删除证书，请点击要删除的证书的单选按钮，然后点击删除。

步骤6.单击“保存”以保存设置。

导出自签名证书

步骤1.单击“导出”列中的所需图标按钮以导出自签名证书。

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		

可用图标按钮定义如下：

- Export Certificate for Client — 导出用于将客户端连接到虚拟专用网络(VPN)的客户端证书。
- 导出管理员证书 — 导出管理员证书。生成私钥并保留副本以备份。
- 导出私钥 — 导出VPN客户端软件的私钥，该软件需要单独的凭据才能连接VPN。

步骤2.单击“打开”查看密钥。

步骤3.单击Save保存密钥。

导出证书签名请求

步骤1.单击CSR (导出证书签名请求)。

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		

步骤2.单击“打开”查看。

步骤3.单击Save将密钥保存在PC或USB上。

导入证书

步骤1.单击Add导入证书。

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		

系统将显示以下窗口：

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

USB Device Status: No Device Attached

步骤2. 点击所需的单选按钮以定义要导入的证书类型。

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

USB Device Status: No Device Attached

- 第三方授权 — 证书颁发机构提供数字签名的公钥基础设施(PKI)。
- 自签名 — 由其自己的创建者签名的安全套接字层(SSL)证书。

步骤3.点击所需的单选按钮以选择要如何导入证书。

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

·从PC导入 — 证书是从您保存的PC导入。

·从USB导入 — 证书从USB驱动器导入。

从PC导入证书

步骤1.如果要导入第三方授权证书，请点击CA证书旁边的**选择文件**，以浏览文件的位置并选择它。

步骤2.单击**Certificate + Private Key**旁的**Choose File(选择文件)**，浏览文件的位置并选择它。

步骤3.单击“**保存**”保存设置。导入的证书将显示在“我的证书表”中。

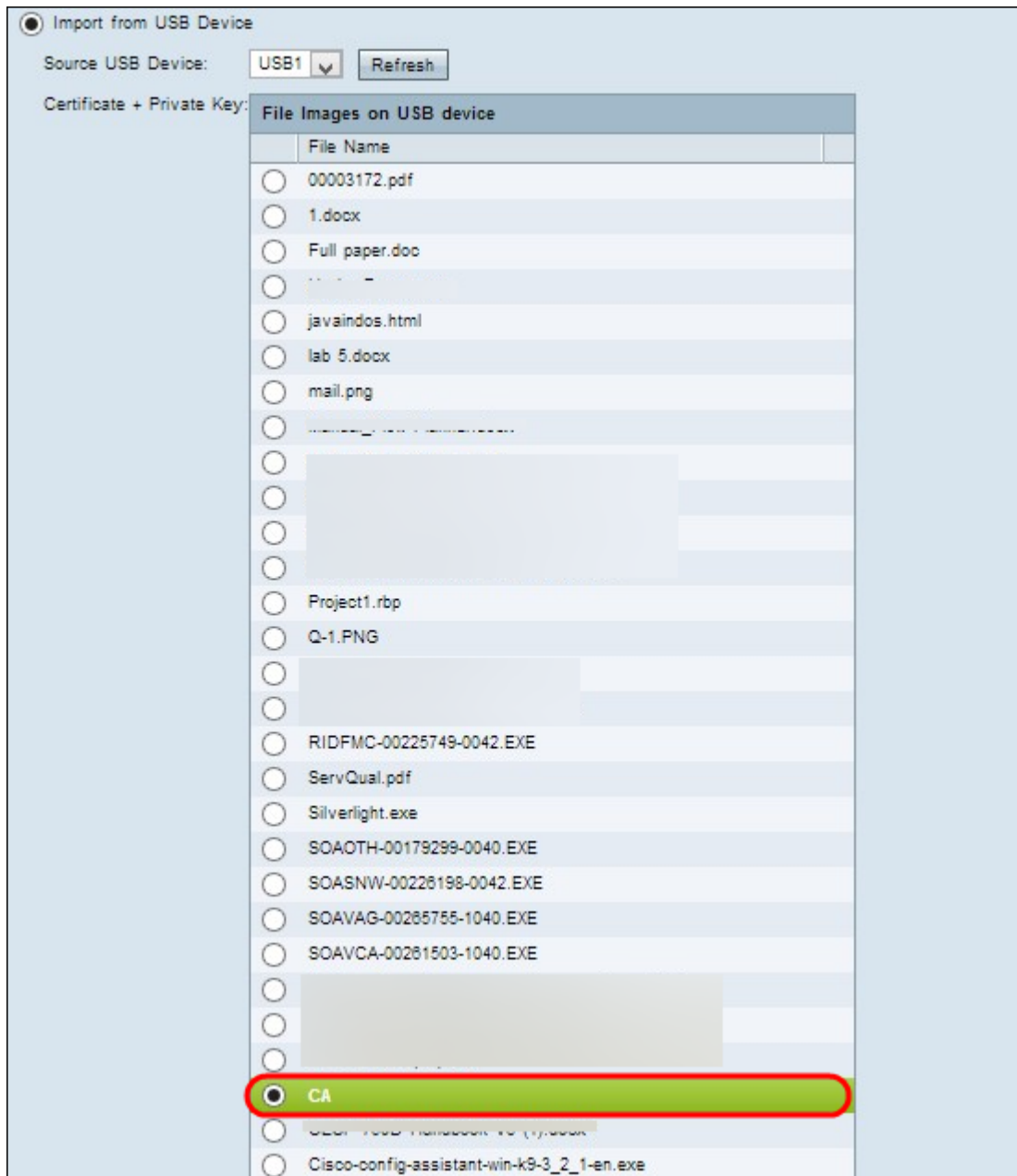
My Certificate

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		
<input type="radio"/>	Self-Signed	CN= OU=			

从USB导入证书

步骤1.从“源USB设备”下拉列表中选择适当的USB设备。













步骤2.如果要导入第3方授权证书，请点击相应的单选按钮以导入您在USB上保存的CA证书。

步骤3.选择适当的单选按钮以导入您在USB上保存的证书+私钥。

步骤4.单击“保存”以保存设置。导入的证书将显示在“我的证书表”中。

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		  
<input type="radio"/>	Self-Signed	CN= OU=		