在RV34x系列路由器上管理证书

目标

数字证书通过证书的指定主题对公钥的所有权进行认证。这允许依赖方依赖由私钥所作的签名或断言，该私钥对应于经认证的公钥。路由器可以生成自签名证书，即由网络管理员创建的证书。它还可以向证书颁发机构(CA)发出申请数字身份证书的请求。从第三方应用获得合法证书非常重要。

我们来谈一谈从证书颁发机构(CA)获取证书。CA用于身份验证。从任意数量的第三方站点购买证书。这是证明您的站点是安全的官方方式。本质上，CA是可信赖的来源，用于验证您是合法企业且可信。根据您的需求，以最低的成本获得证书。CA会签出您，一旦他们验证您的信息，他们会向您颁发证书。此证书可以作为文件下载到您的计算机上。然后，您可以进入路由器（或VPN服务器）并上传它。

本文旨在向您展示如何在RV34x系列路由器上生成、导出和导入证书。

适用设备 |软件版本

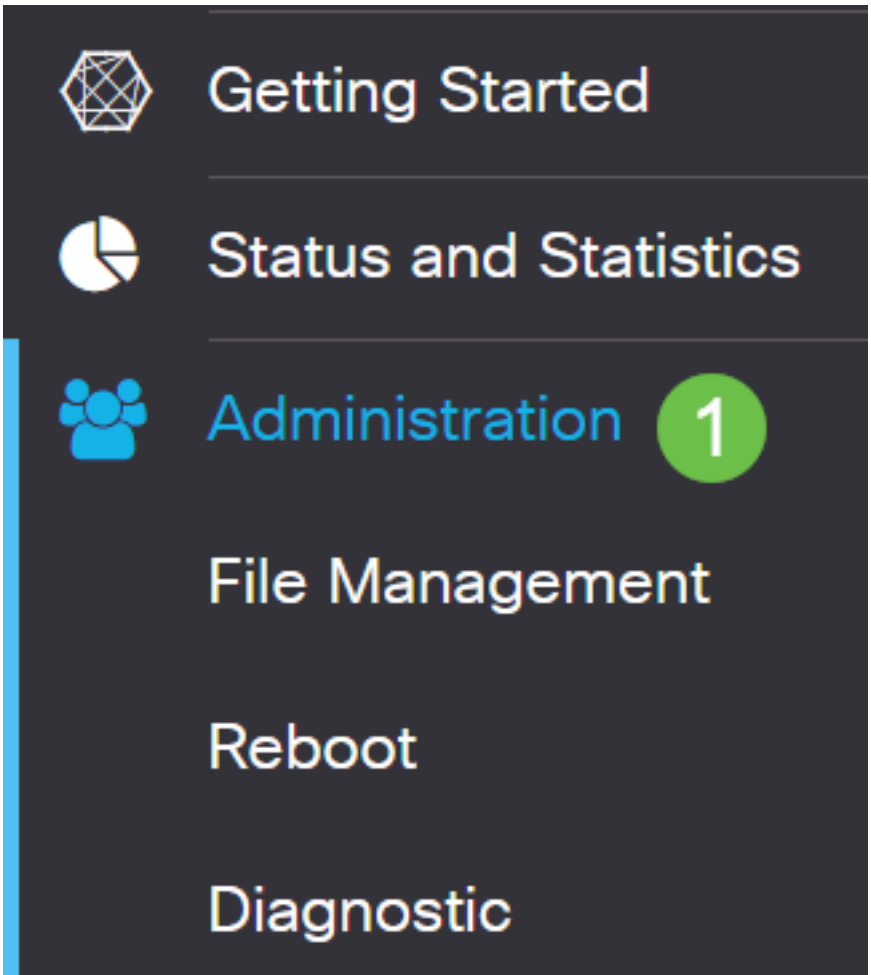
- RV34x系列 |1.0.03.20

在路由器上管理证书

生成CSR/证书

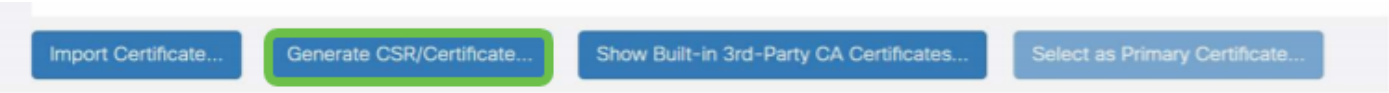
第 1 步

登录到路由器的基于Web的实用程序，然后选择**Administration > Certificate**。



步骤 2

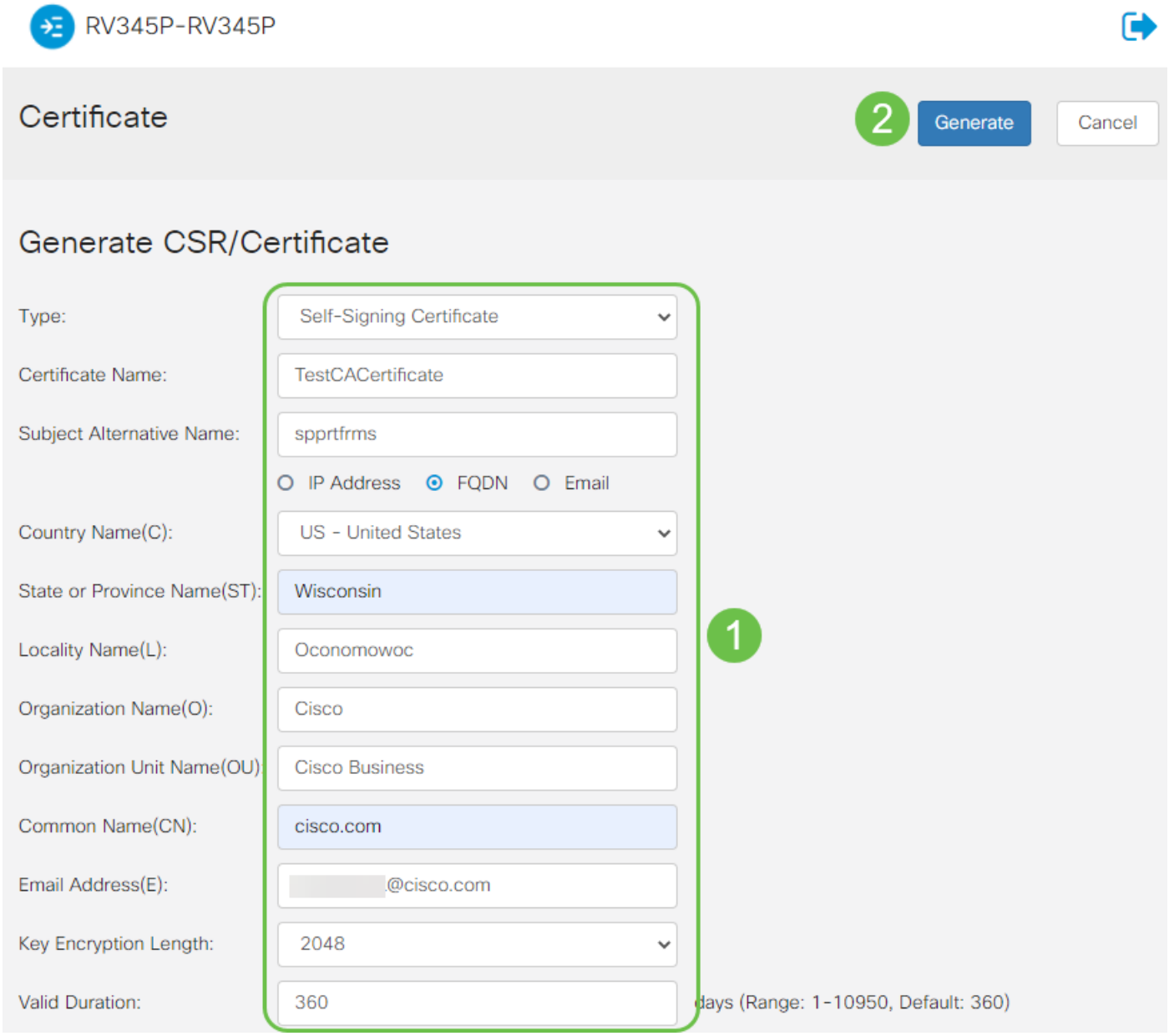
单击**Generate CSR/Certificate**。您将进入“生成CSR/证书”(Generate CSR/Certificate)页面。



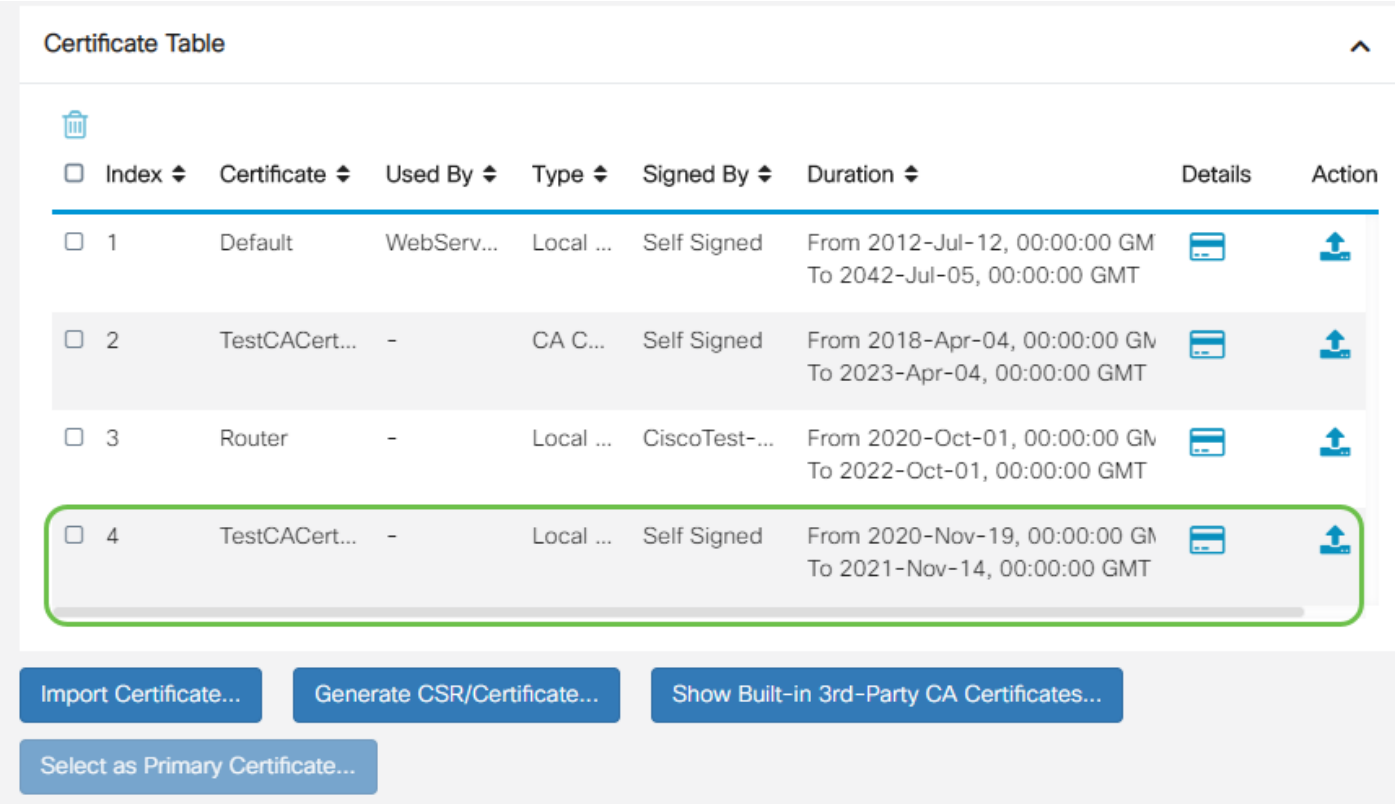
步骤 3

用以下内容填写框：

- 选择适当的证书类型
  - 自签名证书 — 这是由其自己的创建者签名的安全套接字层(SSL)证书。此证书不太可信，因为如果私钥被攻击者以某种方式入侵，则无法取消该证书。
  - 认证签名请求 — 这是公钥基础设施(PKI)，发送到证书颁发机构以申请数字身份证书。它比自签名更安全，因为私钥是保密的。
- 在Certificate Name字段中输入证书*的名称*以标识请求。此字段不能为空，也不能包含空格和特殊字符。
- （可选）在“主题备用名称”区域下，单击单选按钮。选项有：
  - IP地址 — 输入Internet协议(IP)地址
  - FQDN — 输入完全限定域名(FQDN)
  - 电子邮件 — 输入电子邮件地址
- 在“主*题备用名称*”字段中，输入FQDN。
- 从“国家/地区名称”下拉列表中选择贵组织合法注册的国家/地区名称。
- 在“省/自治区名称(ST)”字段中输入您的组织所在的省/自治区、*省/自治区或地区的名称*或缩写。
- 在Locality Name字段中输入您的组织注册或位于的地*区或城*市。
- 输入企业合法注册的名称。如果您注册为小型企业或独资企业主，请在“组织名称”字段中输入证书申*请者的*名称。不能使用特殊字符。
- 在“组织单位名称”*字段中输入*名称，以区分组织内的部门。
- 在“公用名”字*段中输*入名称。此名称必须是您为其使用证书的网站的完全限定域名。
- 输入要生成证书的人员的电子邮件地址。
- 从Key Encryption Length下拉列表中，选择密钥长度。选项为512、1024和2048。密钥长度越长，证书就越安全。
- 在有*效持续时间*字段中，输入证书的有效天数。默认值为 360。
- 单击生成。



注意：生成的证书现在应显示在证书表中。

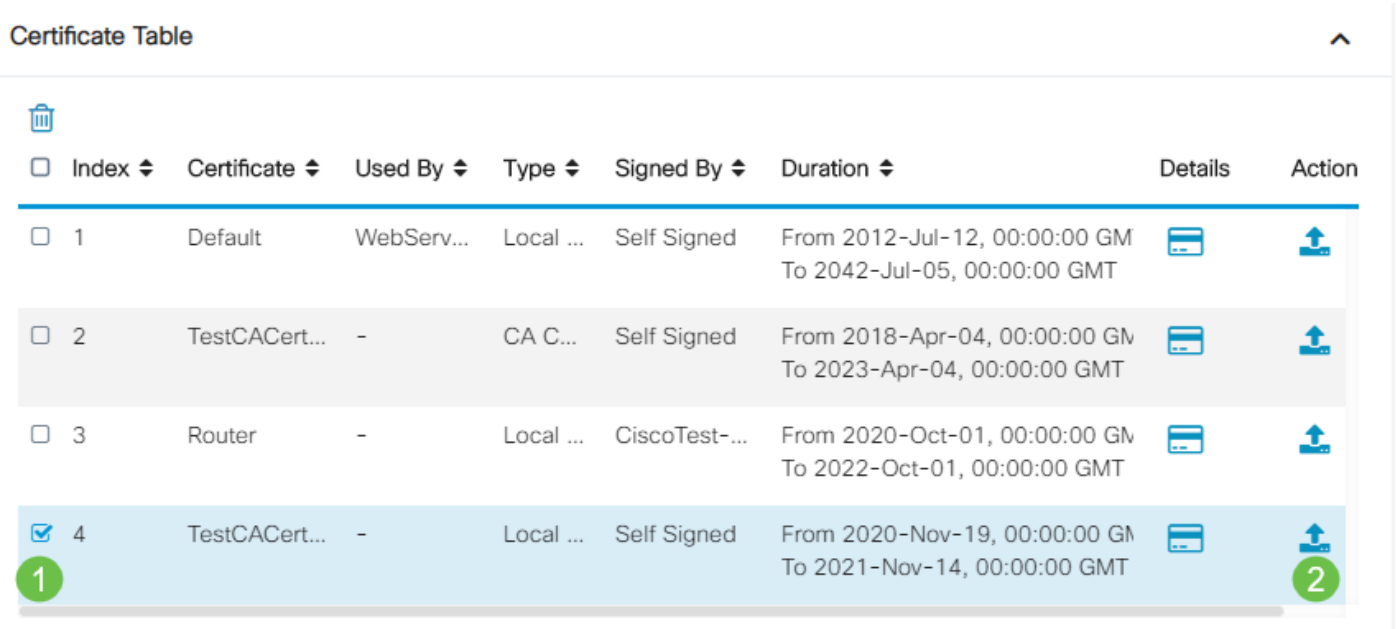


您现在应该已在RV345P路由器上成功创建证书。

导出证书

第 1 步

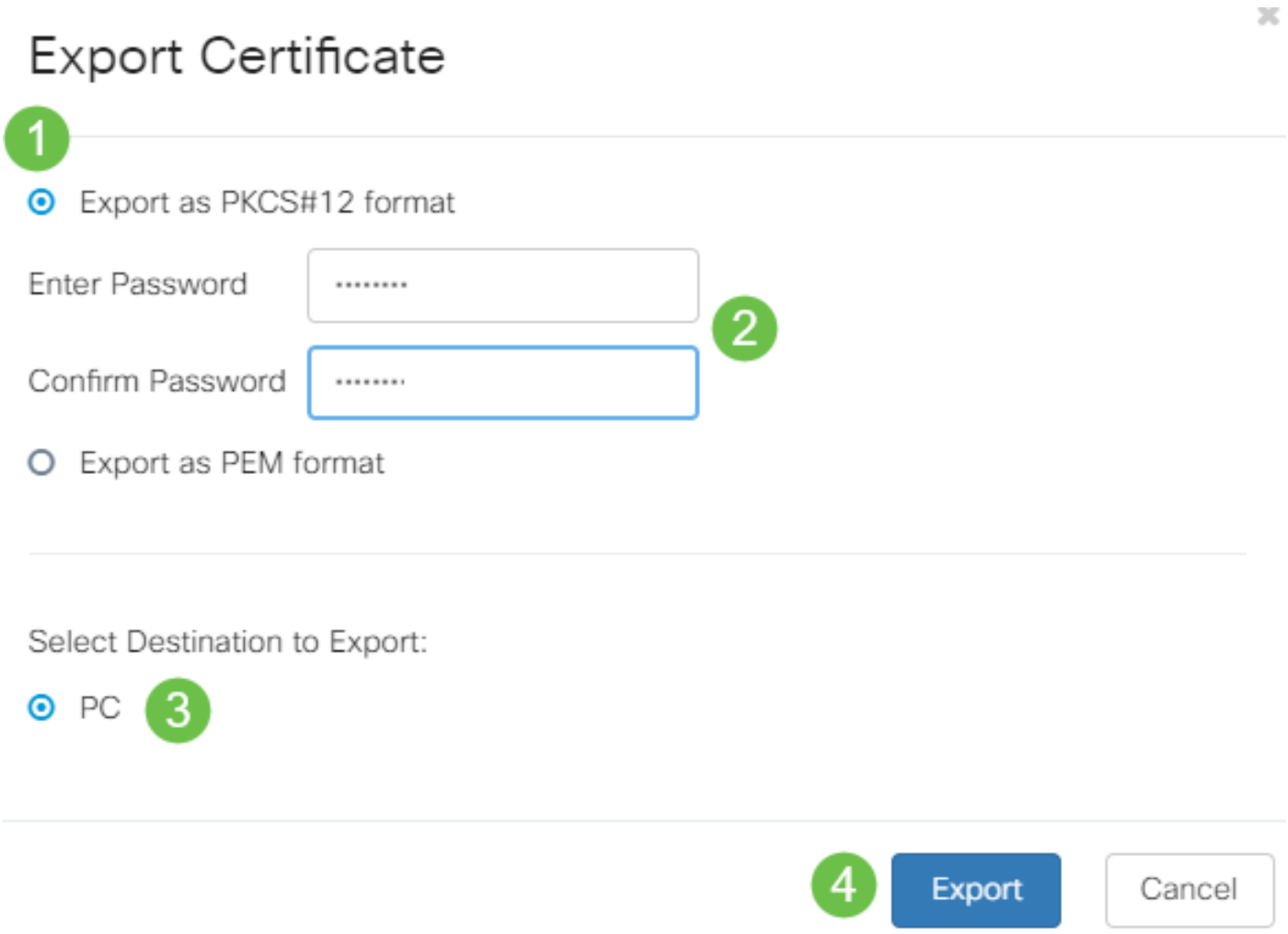
在证书表中，选中要导出的证书的复选框，然后单击导**出图标**。



步骤 2

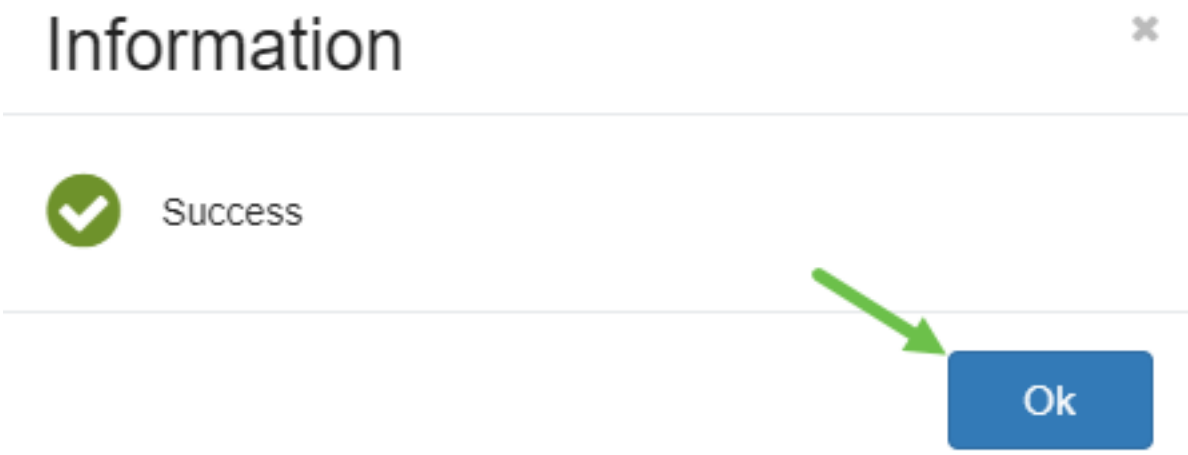
- 单击格式以导出证书。选项有：
  - PKCS #12 — 公钥加密标准(PKCS)#12是带有.p12扩展的导出证书。要加密文件以在文件导出、导入和删除时对其进行保护，需要密码。
  - PEM - Privacy Enhanced Mail(PEM)常用于Web服务器，因为它们能够通过使用简单文本编辑器（如记事本）轻松转换为可读数据。

- 如果选择PEM，只需单击**Export**。
- 在“输入密码”字段中输入密码以保护要导*出的*文件。
- 在“确认密码”字*段中重新输*入密码。
- 在Select Destination（选择目标）区域，PC已选择，是当前唯一可用的选项。
- 单击**Export**。



步骤 3

“Download”（下载）按钮下方将显示一条指示下载成功的消息。文件将开始在浏览器中下载。Click **OK**.

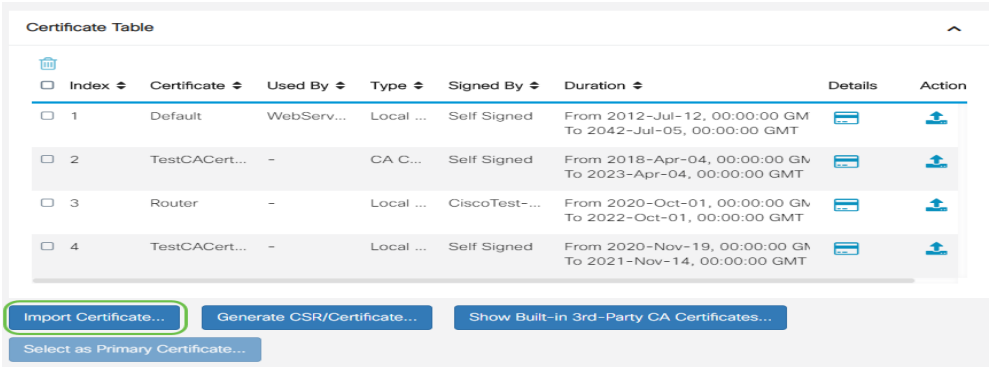


现在，您应该已成功导出Rv34x系列路由器上的证书。

导入证书

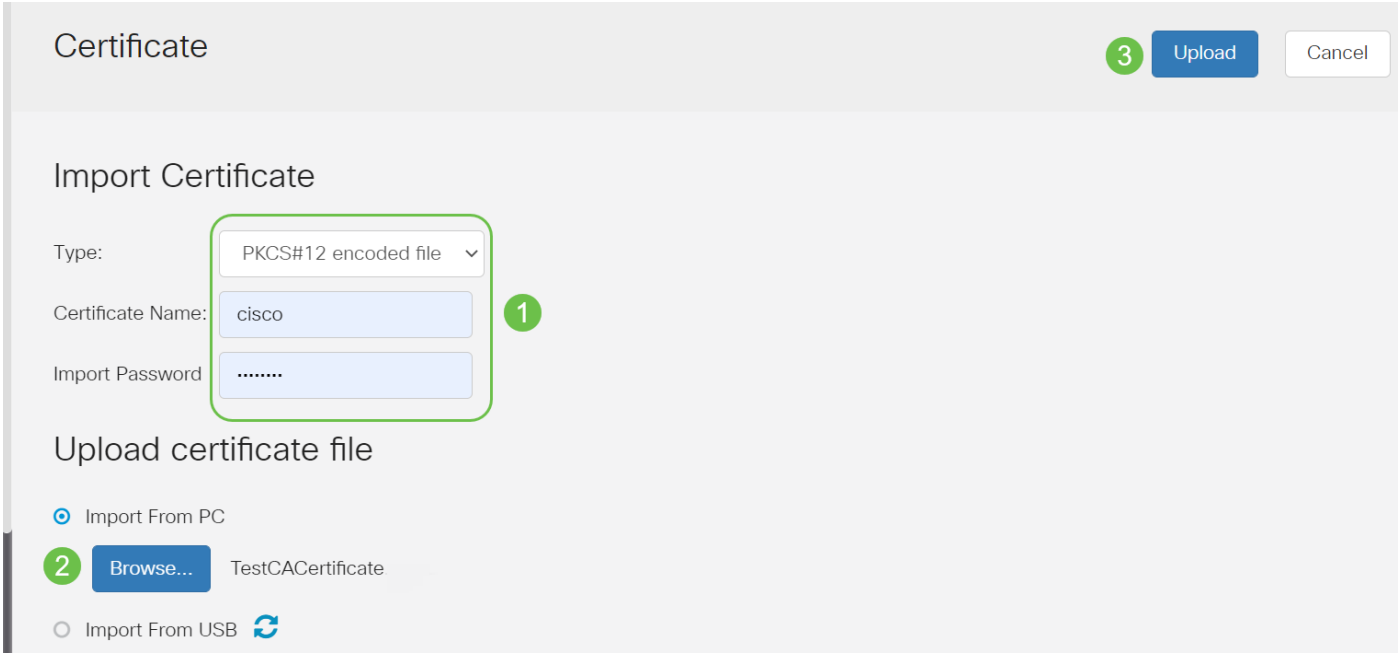
第 1 步

单击“**Import Certificate...**”。

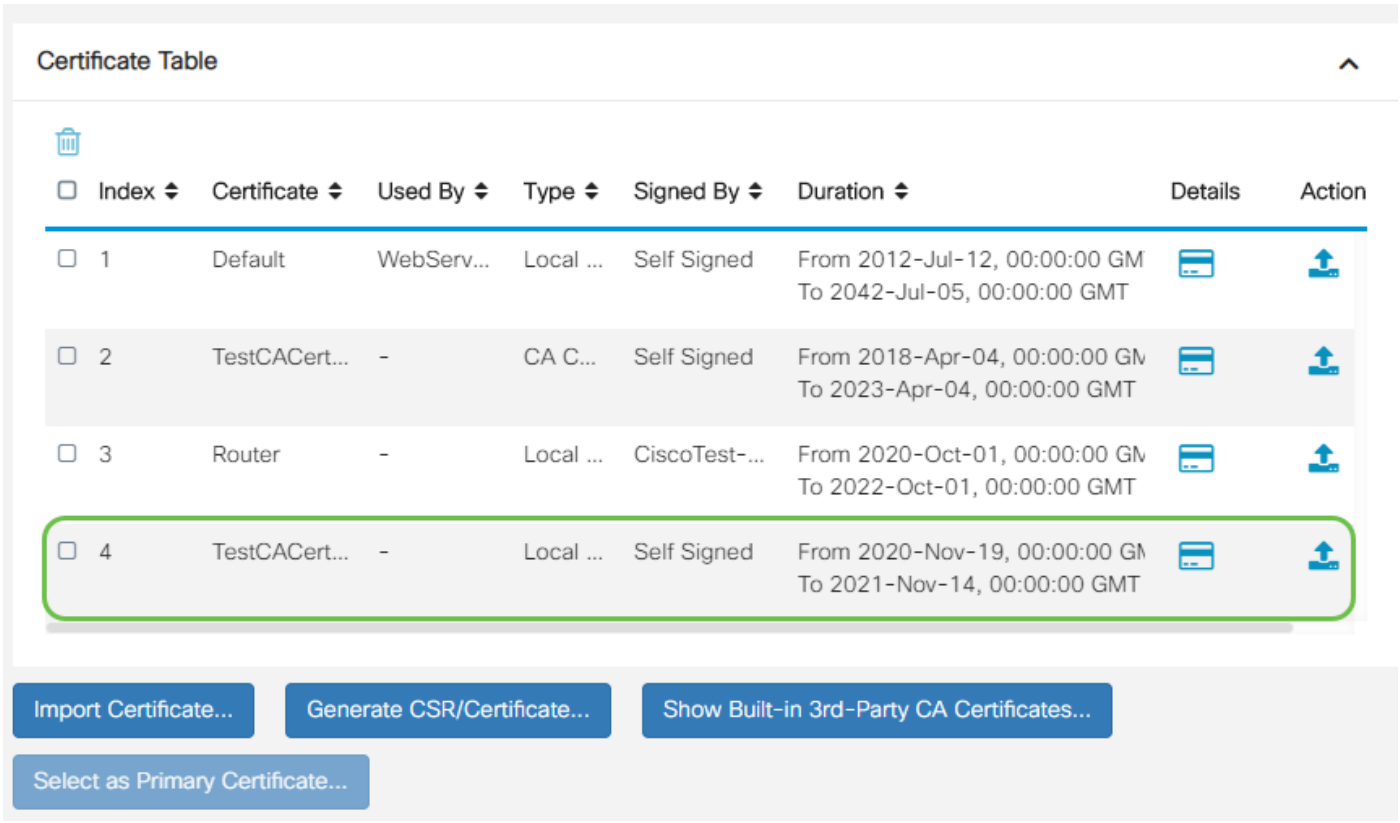


步骤 2

- 从下拉列表中选择要导入的证书类型。选项有：
  - 本地证书 — 路由器上生成的证书。
  - CA证书 — 由受信任的第三方机构认证的证书，它确认证书中包含的信息准确。
  - PKCS #12编码文件 — 公钥加密标准(PKCS)#12是存储服务器证书的格式。
- 在Certificate Name字段中输入证*书的名*称。
- 如果选择了PKCS #12，请在Import Password字段中输入文*件的密*码。否则，请跳至步骤3。
- 单击源导入证书。选项有：
  - 从PC导入
  - 从USB导入
- 如果路由器未检测到USB驱动器，“从USB导入”选项将呈灰色显示。
- 如果选择“从USB导入”，且路由器无法识别您的USB，请单击“刷新”。
- 单击“选择文件”按钮并选择适当的文件。
- 单击**Upload**。



成功后，您将自动进入主Certificate页面。证书表将填充最近导入的证书。



现在，您应该已成功在RV34x系列路由器上导入证书。