在RV34x系列路由器上将默认自签名证书替换为第三方SSL证书

简介

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。

CA通过两种方式签署证书：

1. CA使用私钥对证书签名。

2. CA使用RV34x生成的证书签名请求(CSR)对证书进行签名。

大多数商业证书供应商使用中间证书。由于中间证书由受信任根CA颁发，因此由中间证书颁发的任何证书都继承受信任根的信任，如信任的证书链。

目标

本文旨在说明如何请求和上传由CA颁发的第三方安全套接字层(SSL)证书，以替换RV34x路由器上的自签名证书。

适用设备

- RV340
- RV340W
- RV345
- RV345P

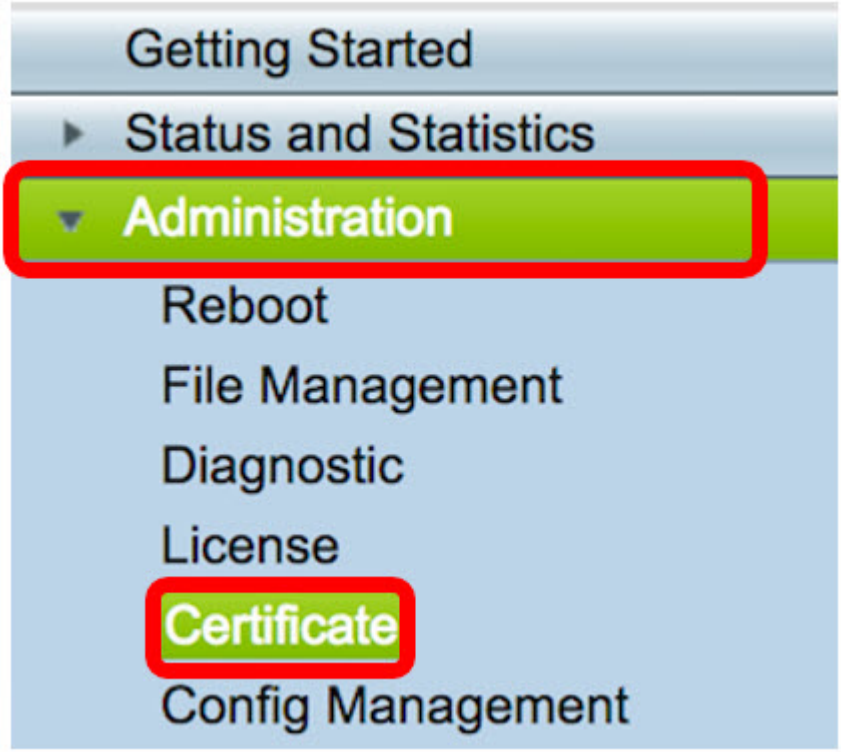
软件版本

- 1.0.01.17

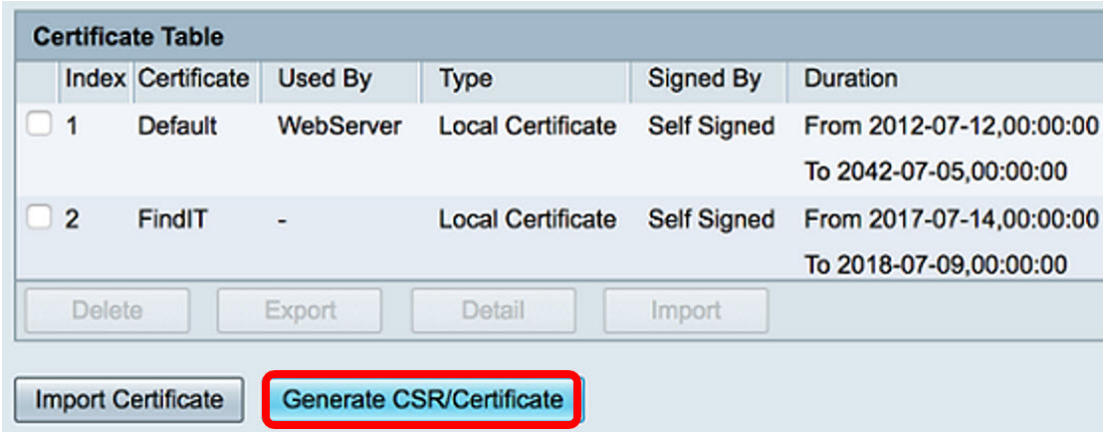
用第3方SSL证书替换默认自签名证书

生成 CSR

步骤1.登录到路由器的基于Web的实用程序，然后选择Administration > Certificate。



步骤2.在Certificate Table（证书表）下，单击**Generate CSR/Certificate(生成CSR/证书)**按钮。

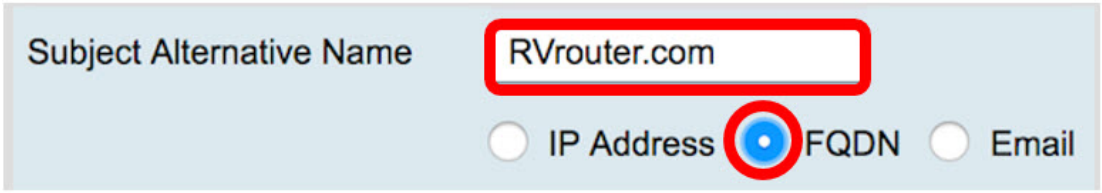


步骤3.在“生成*CSR/证书”窗*口中，单击*类型*下拉箭头并选择**证书签名请求**。

步骤4.在Certificate Name字段中输入证*书的名*称。

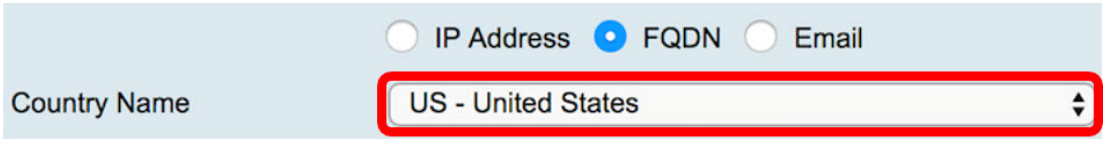
注意：在本例中，使用34xrouter。

步骤5.在Subject Alternative Name字段中输入备*用名称*，然后单击其下**方的**FQDN单选按钮进行匹配。备用名称是可用于访问路由器的域名。



注意：在本例中，使用RVrouter.com。

步骤6.单击*Country Name*下拉箭头选择您所在国家/地区。

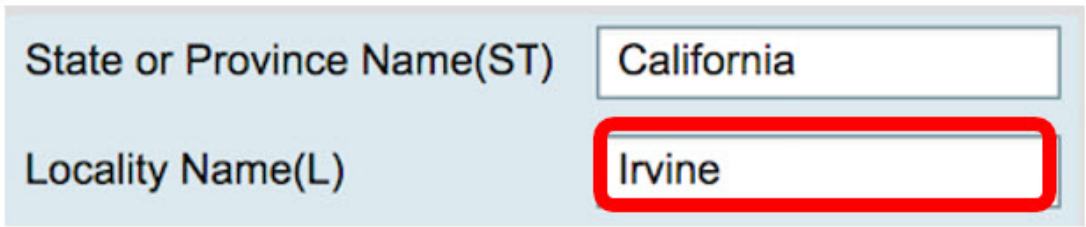


注意：在本例中，选择美国 — 美国。

步骤7.在省或省名称(ST)字*段中输入省或省的名*称。

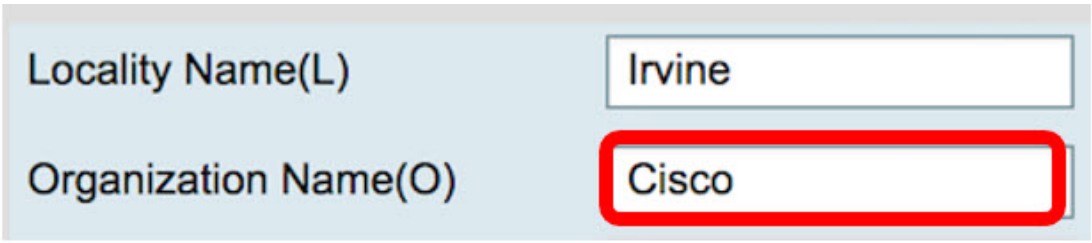
注意：在本例中，使用California。

步骤8.在Locality Name(L)字*段中输入位置*。



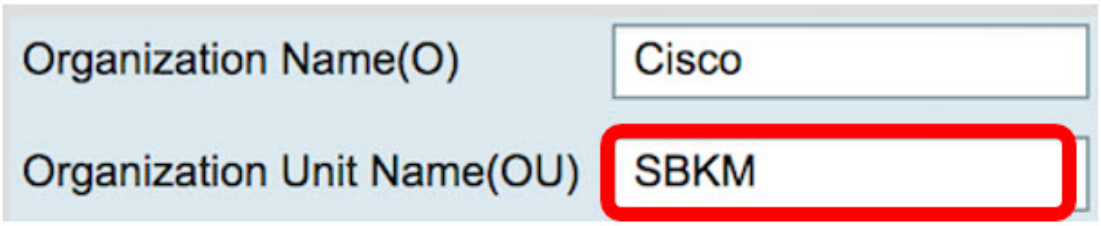
注意：在本例中，使用Irvine。

步骤9.在提供的字段中输入组织名称(O)。



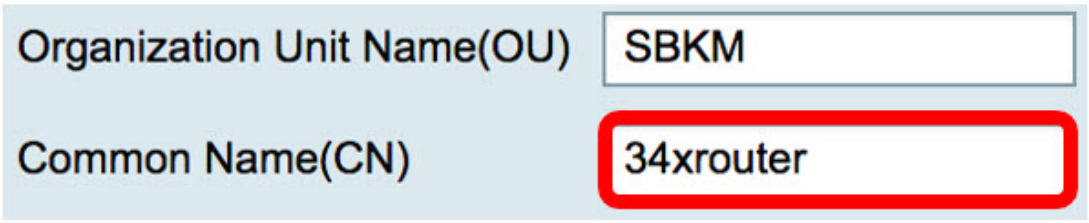
注意：在本例中，使用思科。

步骤10.在提供的字段中输入组织单位名称(OU)。



注意：在本例中，使用SBKM。

步骤11.在Common Name(CN)字*段中输入名*称。

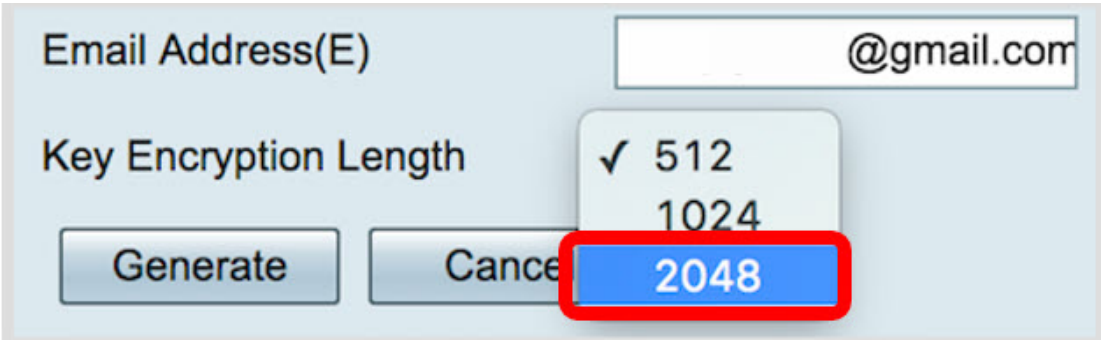


注意：在本例中，使用34xrouter。

步骤12.输入您的电子邮件地址或要将证书发送到的任何电子邮件地址。

注意：在本例中，使用gmail.com电子邮件地址。

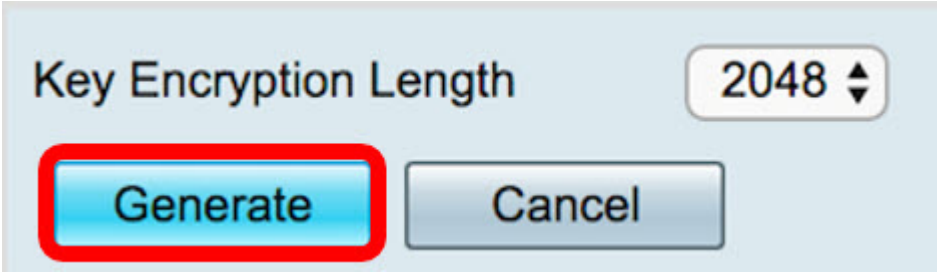
步骤13.从下拉*菜单中选择*Key Encryption Length，以设置密钥中的位数。默认长度为512。



注意：在本例中，使用2048。这是强烈建议的，因为较长的加密比较较短的密钥更难解码

，因此使其更安全。

步骤14.单击“生**成**”。

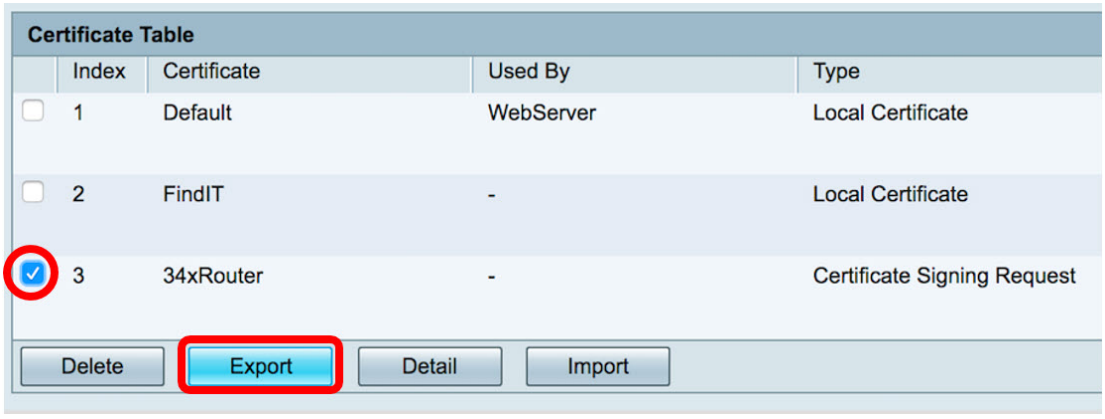


您创建的证书请求现在将显示在证书表中。

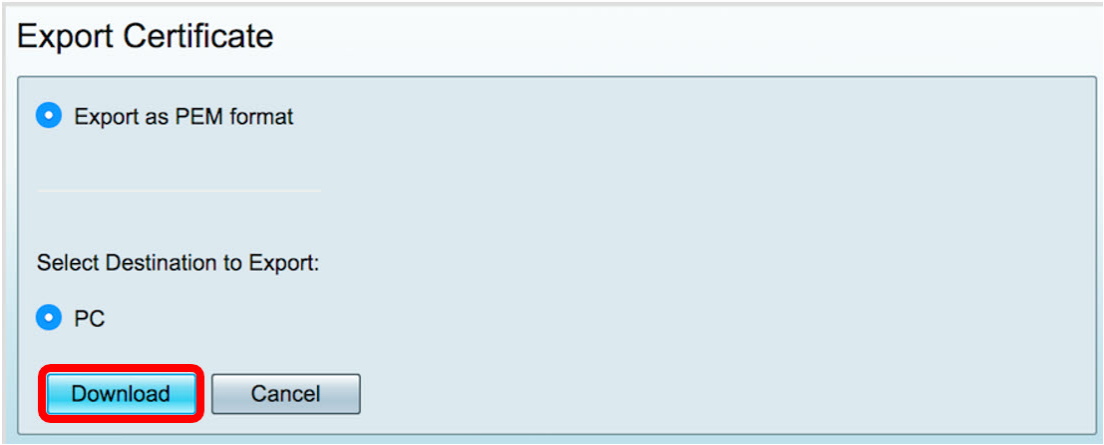
您现在已成功生成CSR。

导出CSR

步骤1.选中Certificate Table中证书请求旁的框，然后单击**Export**。



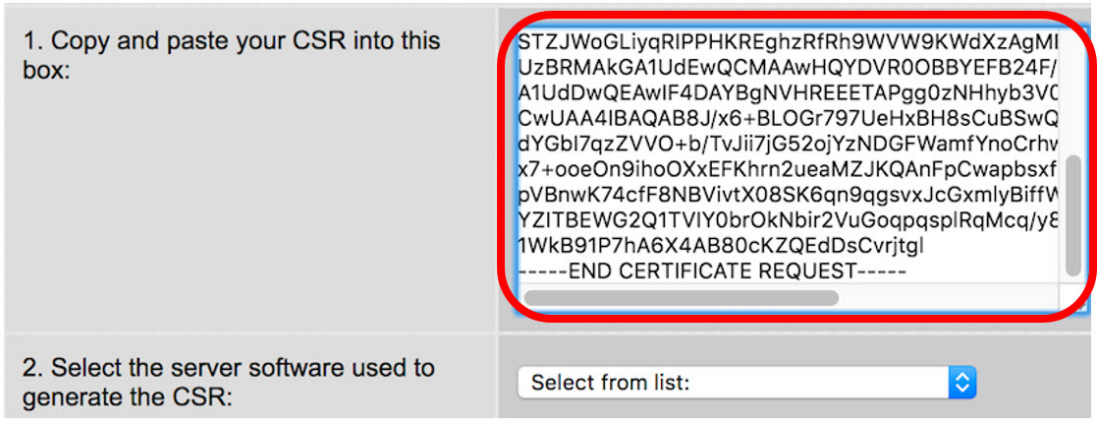
步骤2.在“导出证书”窗**口中**单击“*下载*”，以PEM格式将文件下载到计算机中。



现在，您已成功将CSR导出到计算机。

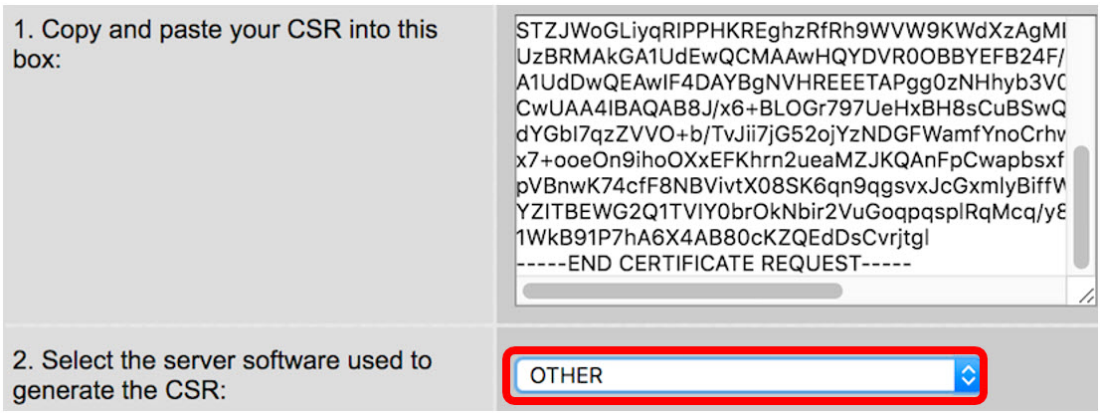
将CSR上传到证书提供程序

步骤1.使用记事本打开下载的文件，然后复制CSR，然后将其粘贴到第三方SSL证书提供程序站点中提供的字段。



注意：在本例中，Comodo.com用作证书提供程序。

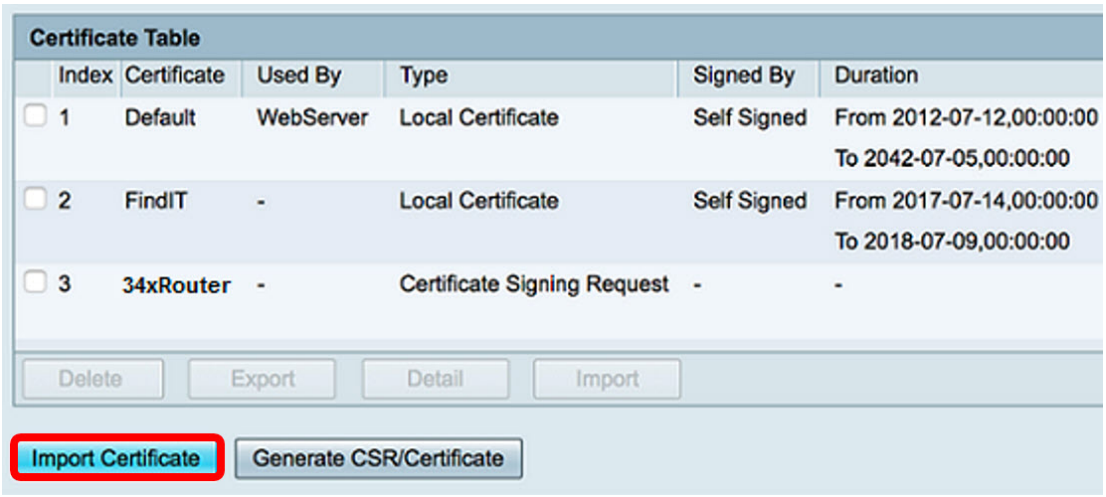
步骤2.选择用于生成CSR的服务器软件。在这种情况下，由于RV34x路由器不在列表中，因此选择OTHER。



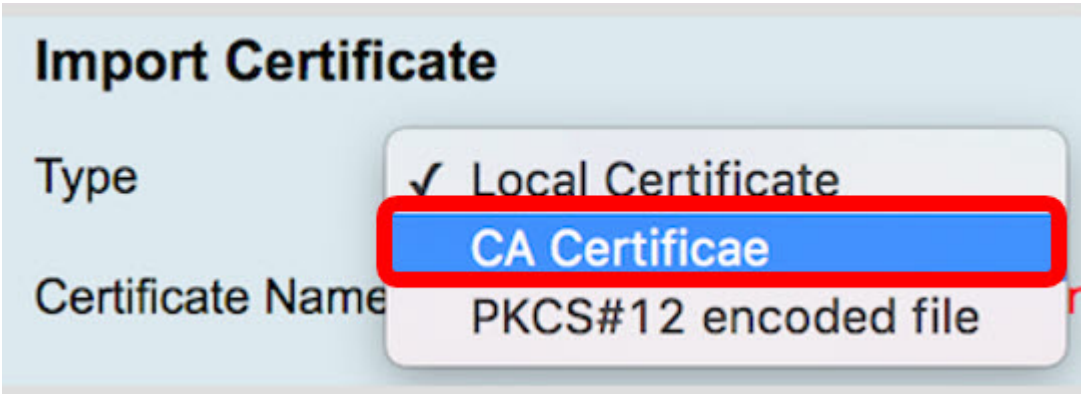
步骤3.将证书下载到计算机中。

上传第3个SSL方证书

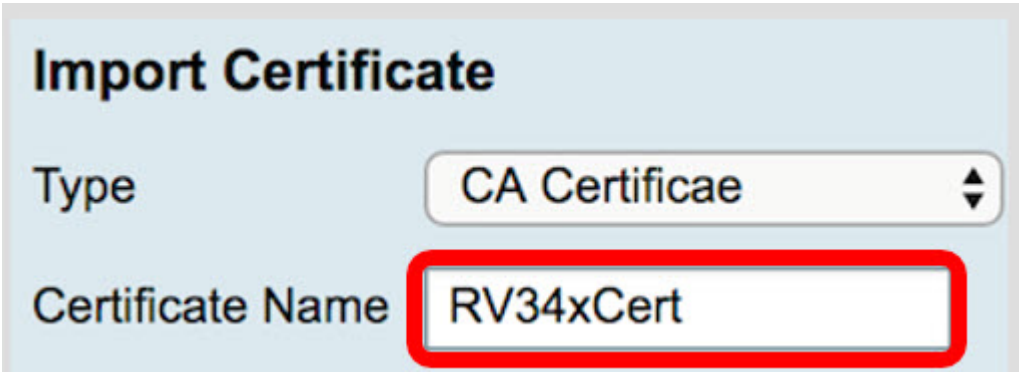
步骤1.在路由器的基于Web的实用程序中，单击Certificate Table下的**Import Certificate**按钮。



步骤2.在“导入证书”窗口中，单击“类型”下拉菜单并选择**CA证书**。

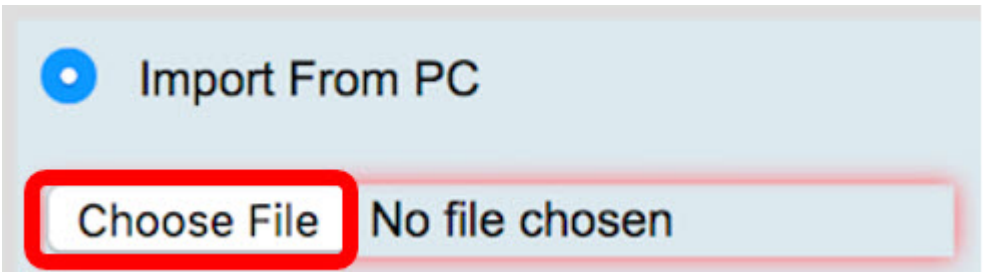


步骤3.在提供的字段中输入证书名称。

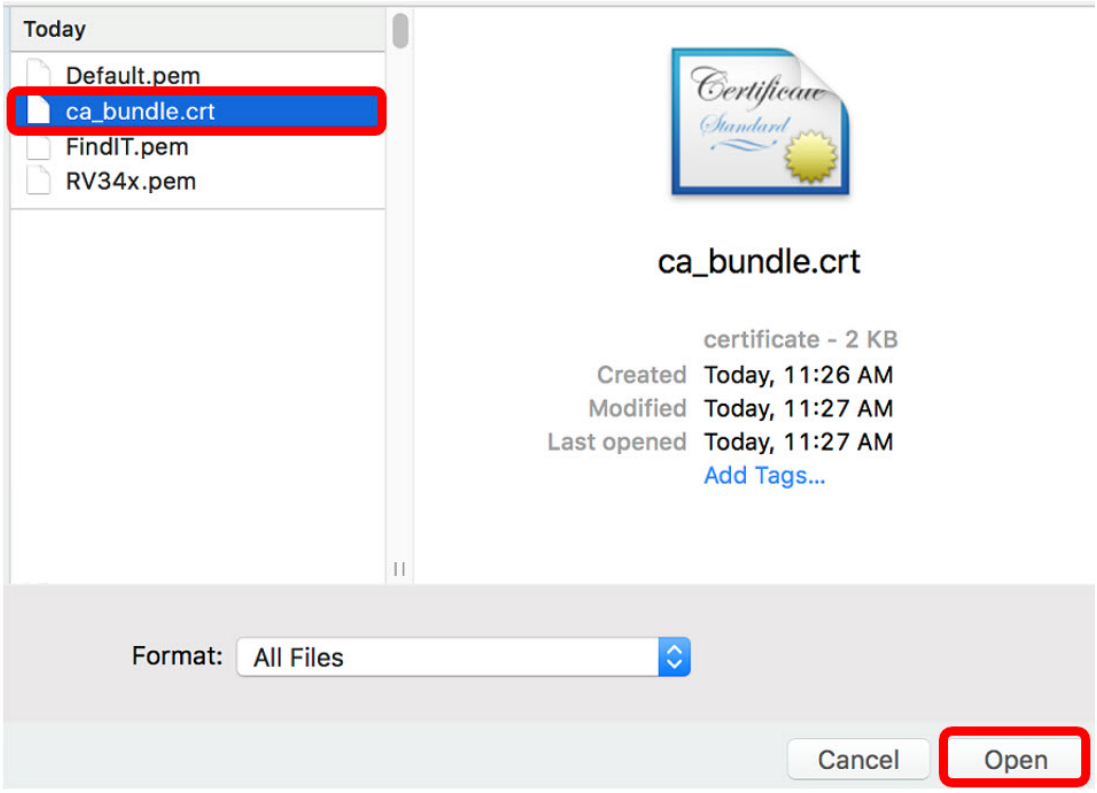


注意：在本例中，使用RV34xCert。

步骤4.单击Choose File**按钮**，找到您从CA下载的证书文件。

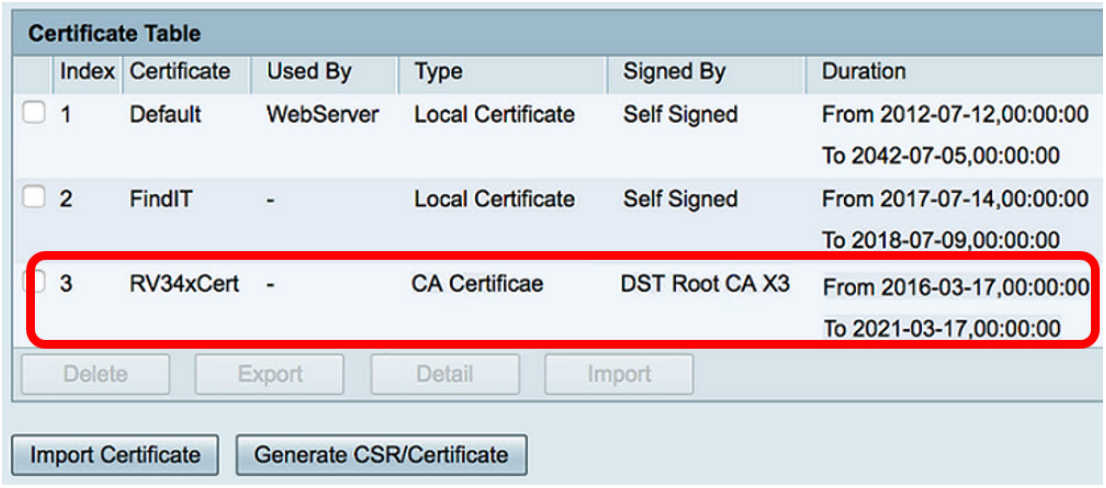


步骤5.单击文件，然后单击“打**开**”。



步骤6.单击**Upload**。

现在，证书表将显示新证书名称，并且该类型现在替换为CA证书，并带有由第三方CA签名的标签。

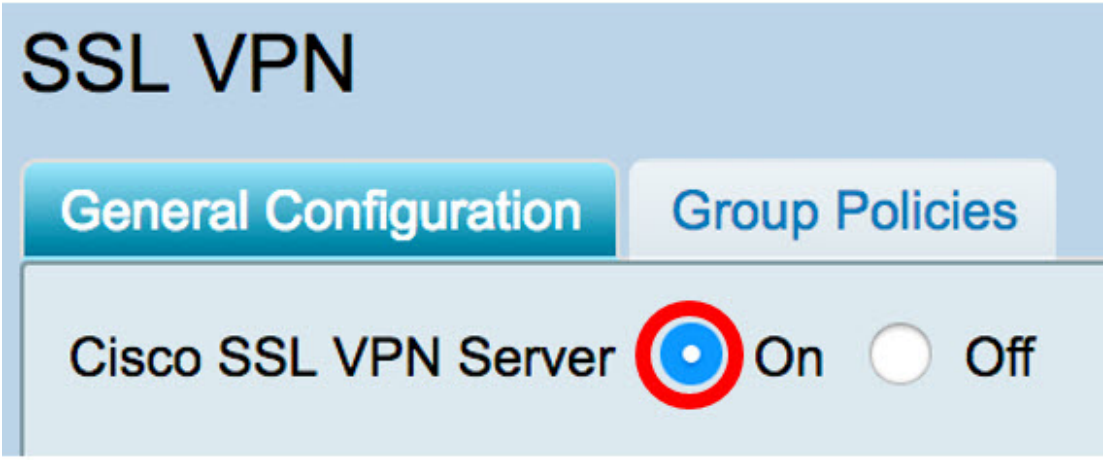


您现在已成功在RV34x路由器上上载第3方SSL证书。

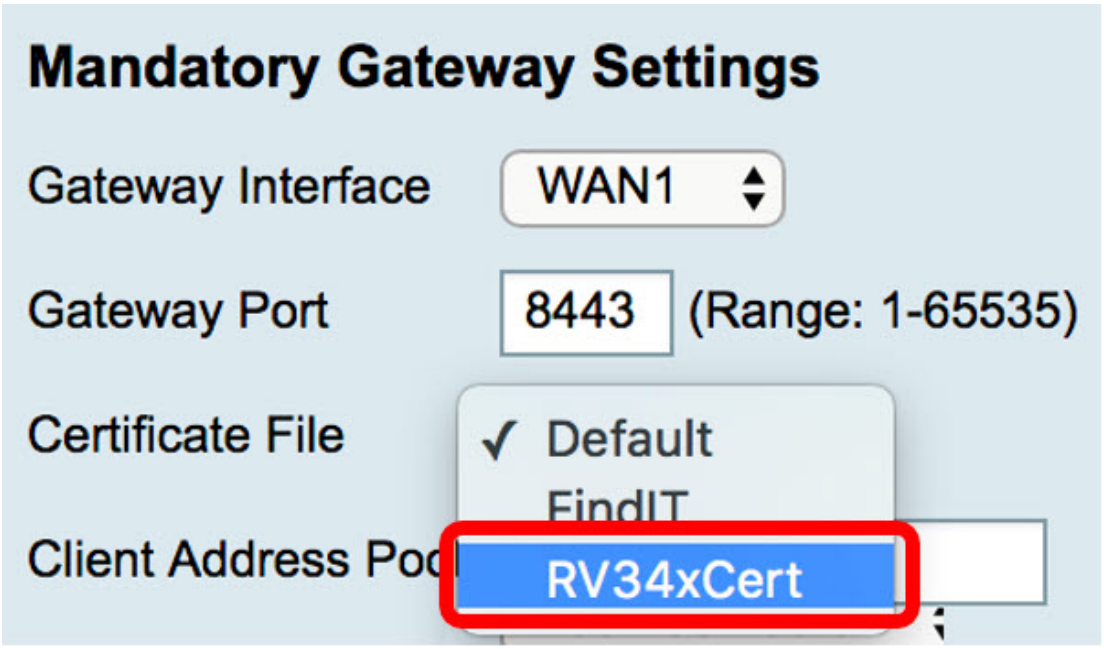
替换默认自签名证书

步骤1.在基于Web的实用程序中，选择**VPN > SSL VPN**。

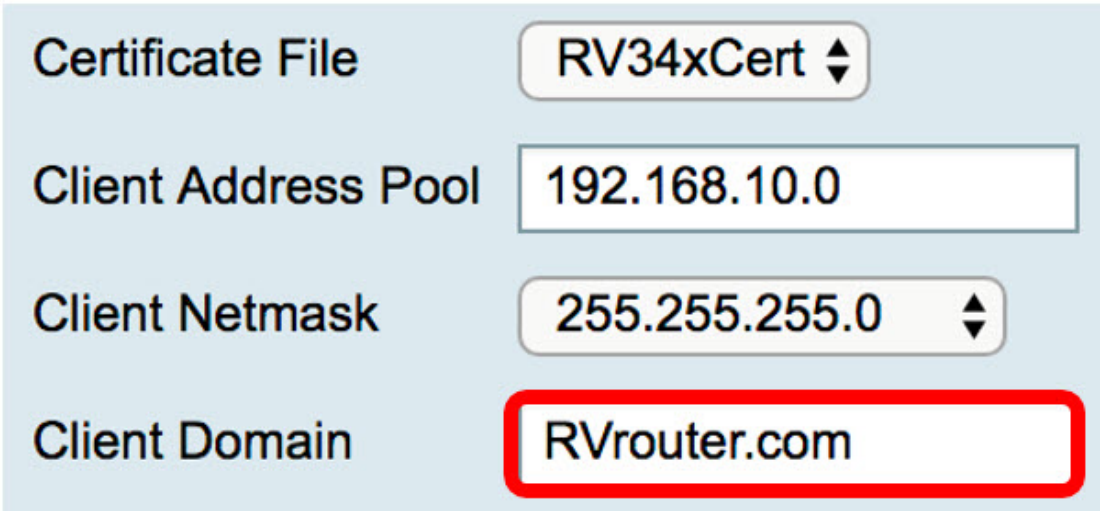
步骤2.单击**On**单选按钮以启用Cisco SSL VPN服务器。



步骤3.在Mandatory Gateway Settings（强制网关设置）下，单击*Certificate File*（证书文件）下拉菜单，通过选择新上传的SSL证书来替换默认证书。

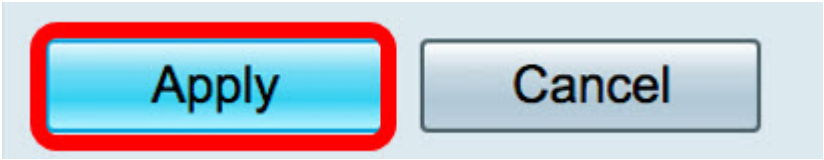


步骤4.在提供的字段中输入所需的客户端域。



注意：在本例中，使用RVrouter.com。

步骤5.单击“**应用**”。



现在，您已成功将默认自签名证书替换为第3方SSL证书。

您可能还会发现本文内容丰富：RV34x系列路由器常见问题(FAQ)

此网站提供了一些链接，指向您可能感兴趣的其他文章：RV34x系列路由器产品页