AnyConnect：将自签名证书安装为受信任源

目标

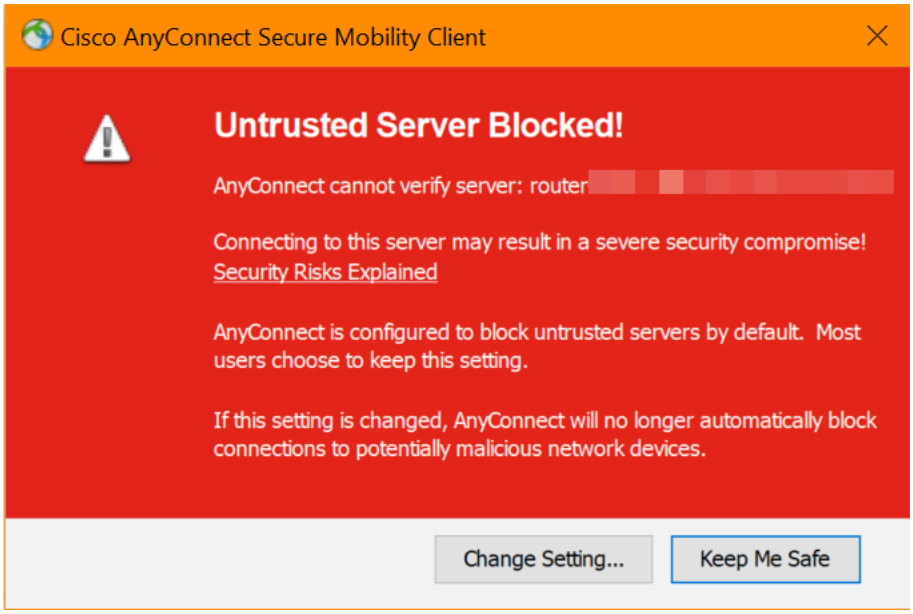
本文的目的是指导您在Windows计算机上创建和安装自签名证书作为受信任源。这将消除AnyConnect中的“不受信任的服务器”警告。

简介

Cisco AnyConnect虚拟专用网络(VPN)移动客户端为远程用户提供安全的VPN连接。它提供思科安全套接字层(SSL)VPN客户端的优势，并支持基于浏览器的SSL VPN连接不可用的应用和功能。AnyConnect VPN通常由远程员工使用，它使员工可以像在办公室一样连接到公司网络基础设施，即使他们不在办公室也是如此。这增加了员工的灵活性、移动性和工作效率。

证书在通信过程中非常重要，用于验证个人或设备的身份、验证服务或加密文件。自签名证书是由其自己的创建者签名的SSL证书。

首次连接到AnyConnect VPN移动客户端时，用户可能会遇到“不受信任的服务器”警告，如下图所示。



按照本文中的步骤在Windows计算机上安装自签名证书作为受信任源，以消除此问题。

应用导出的证书时，请确保将其放在安装了Anyconnect的客户端PC上。

AnyConnect软件版本

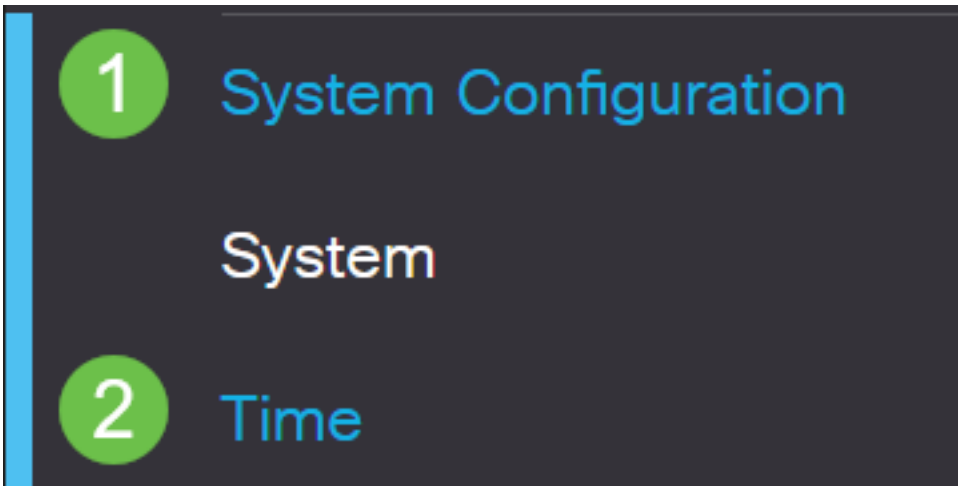
- AnyConnect - v4.9.x(下载最新版本)

检查时间设置

作为前提条件，您需要确保路由器设置了正确的时间，包括时区和夏时制设置。

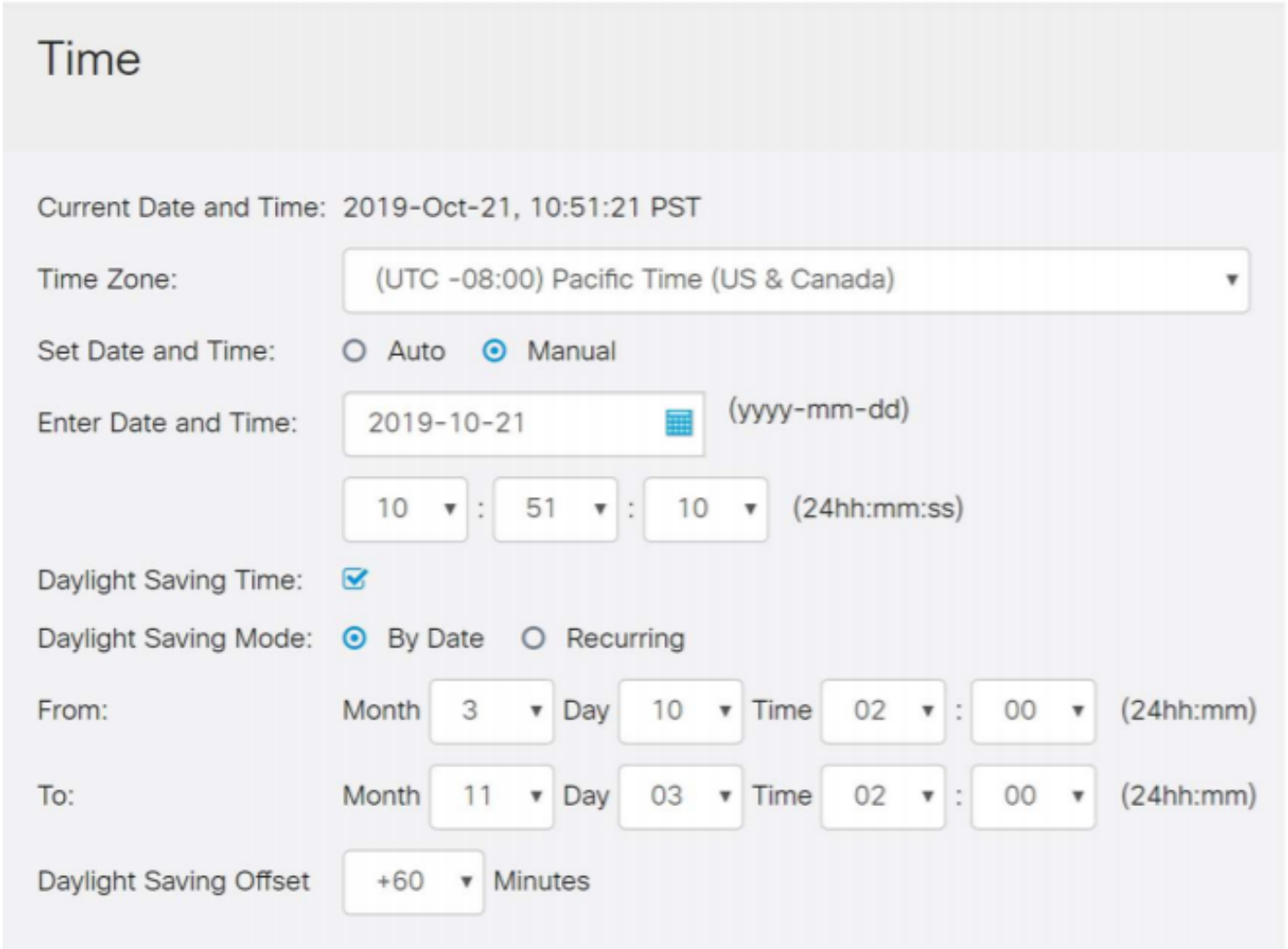
第 1 步

导航至**系统配置>时间**。



步骤 2

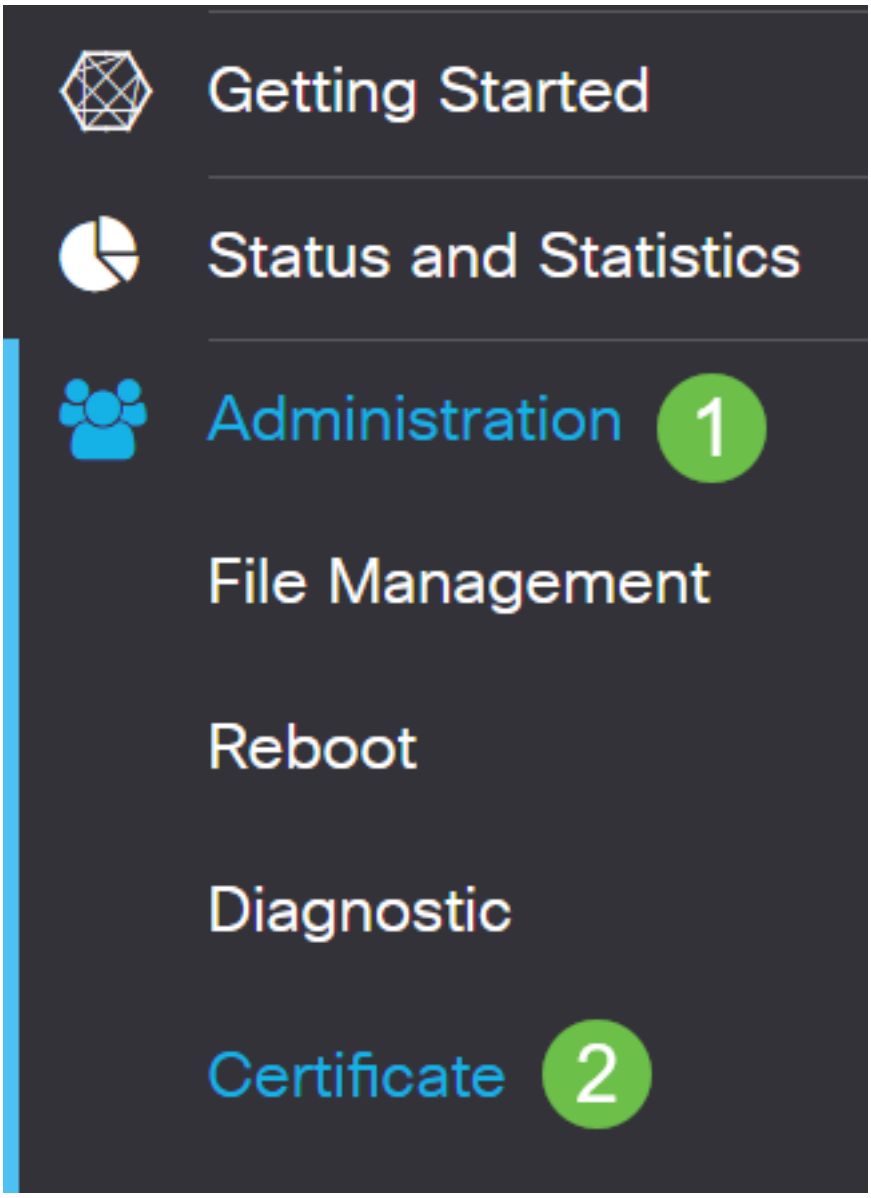
确保所有设置都正确。



创建自签名证书

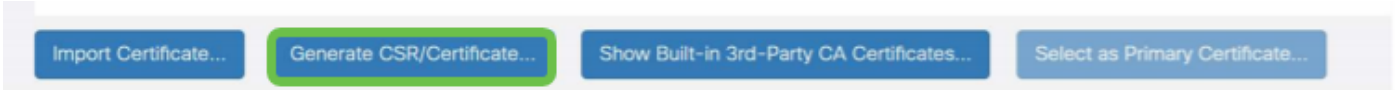
第 1 步

登录RV34x系列路由器并导航至**Administration > Certificate**。



步骤 2

单击“**Generate CSR/Certificate（生成CSR/证书）**”。



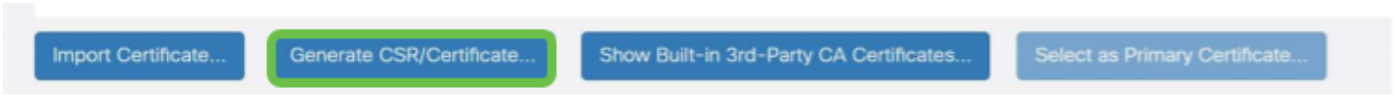
步骤 3

填写以下信息：

- type：自签名证书
- 证书名称：（您选择的任何名称）
- 主题备用名称：如果WAN端口上将使用IP地址，请选择框**下的IP**地址或**FQDN**（如果要使用完全限定域名）。在框中，输入WAN端口的IP地址或FQDN。
- 国家/地区名称(C):选择设备所在的国家/地区

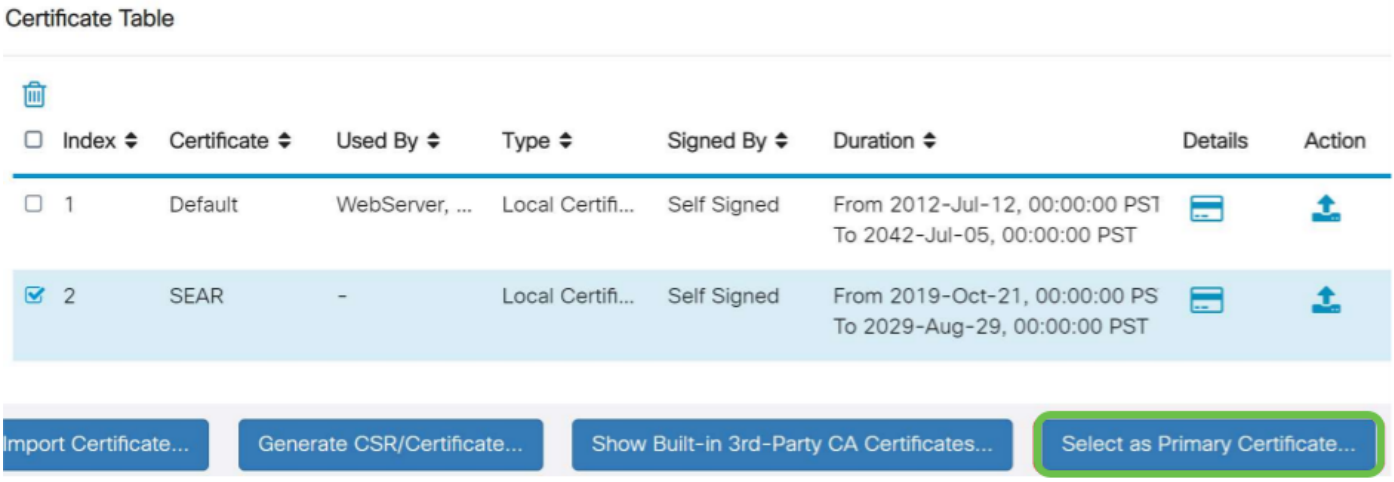
- 省/自治区名称(ST):选择设备所在的州或省
- 位置名称(L):（可选）选择设备所在的Locality。这可以是一个城镇，城市等。
- 组织名称(O):（可选）
- 组织单位名称(OU):公司名称
- 公用名称 (cn):此MUST与设置为“主题备用名称”的匹配
- 电子邮件地址(E):（可选）
- 密钥加密长度：2048
- 有效持续时间：这是证书的有效期。默认值为 360 天。您可以根据需要调整此值，最多10,950天或30年。

单击“**Generate(生成)**”。



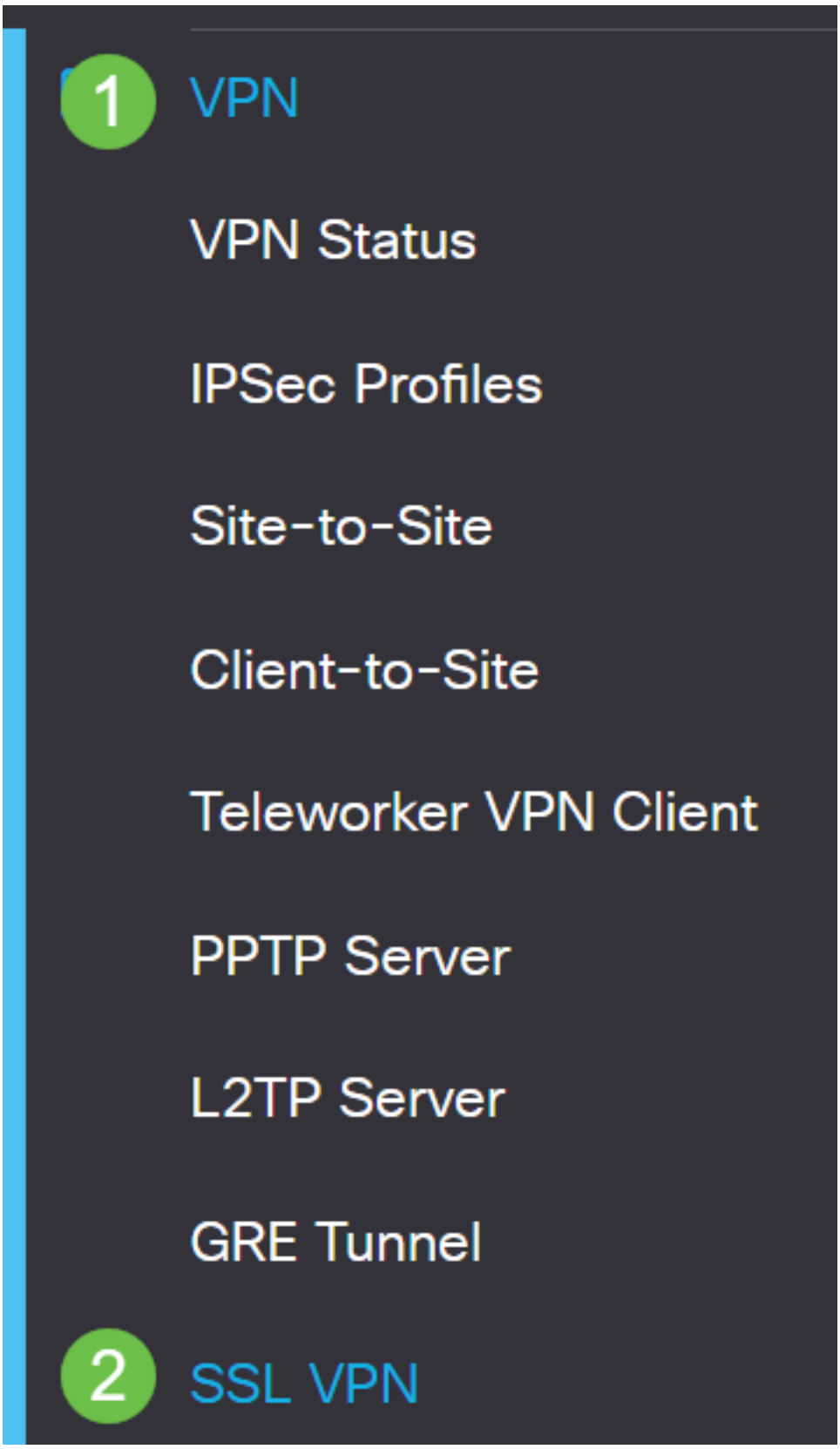
步骤 4

选择刚创建的证书，然后点击选择**为主证书。**



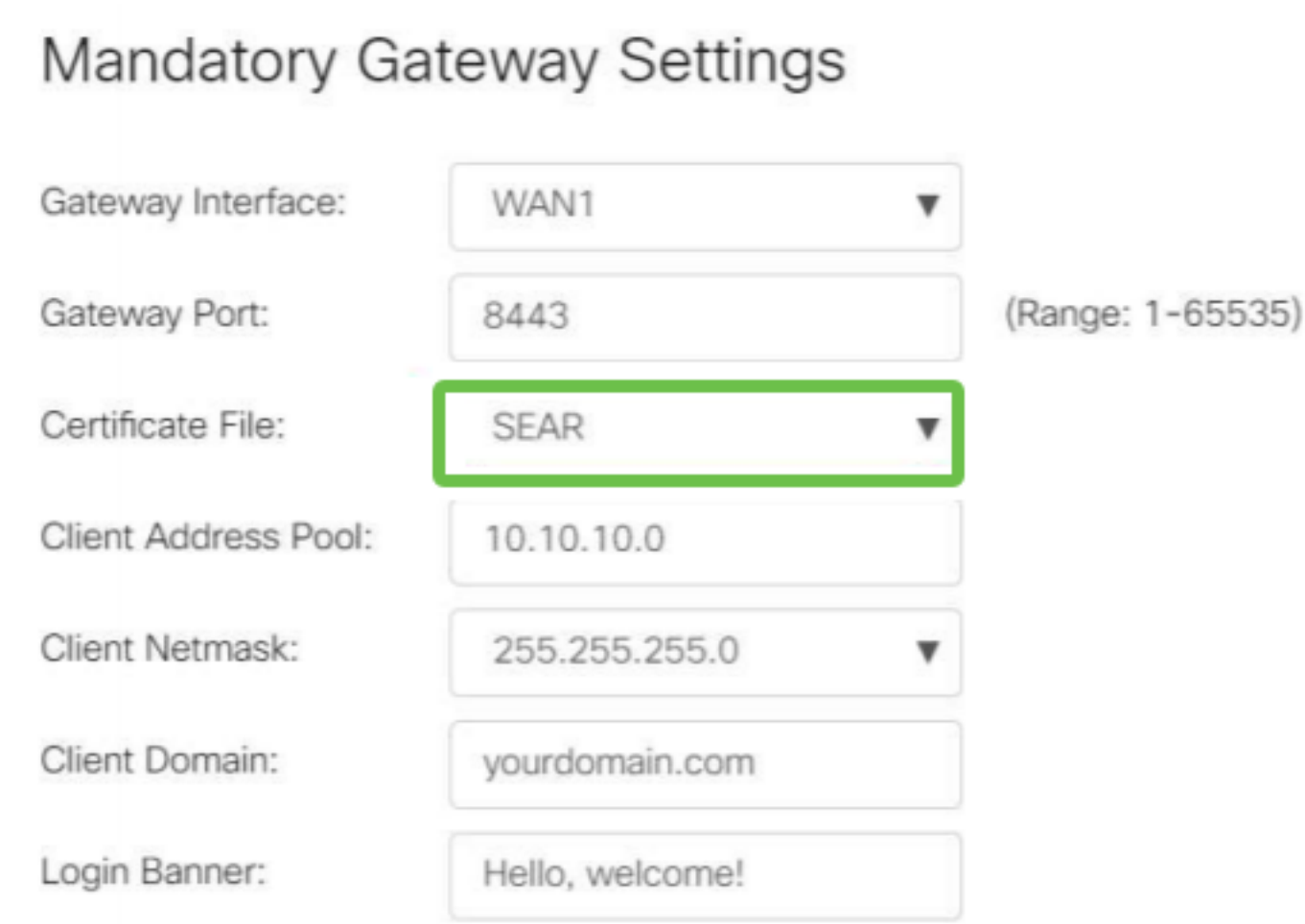
步骤 5

刷新Web用户界面(UI)。 由于是新证书，因此您需要重新登录。登录后，转到**VPN > SSL VPN**。



步骤 6

将证**书文件**更改为新创建的证书。



步骤 7

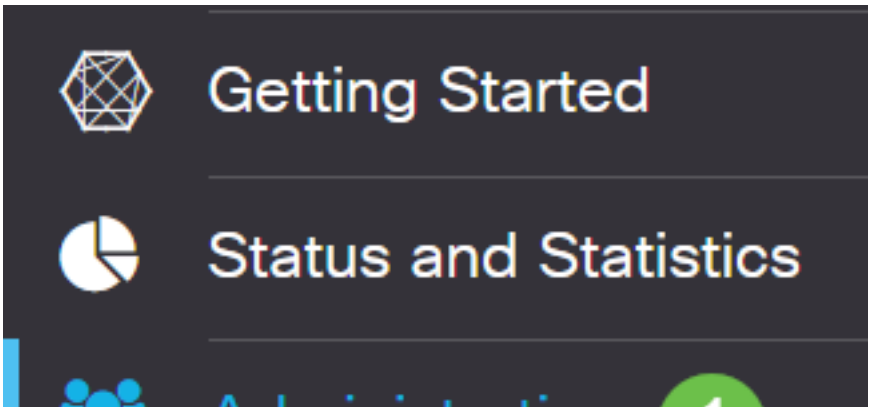
单击 **Apply**。

安装自签名证书

要在Windows计算机上安装自签名证书作为受信任源，以消除AnyConnect中的“不受信任服务器”警告，请执行以下步骤：

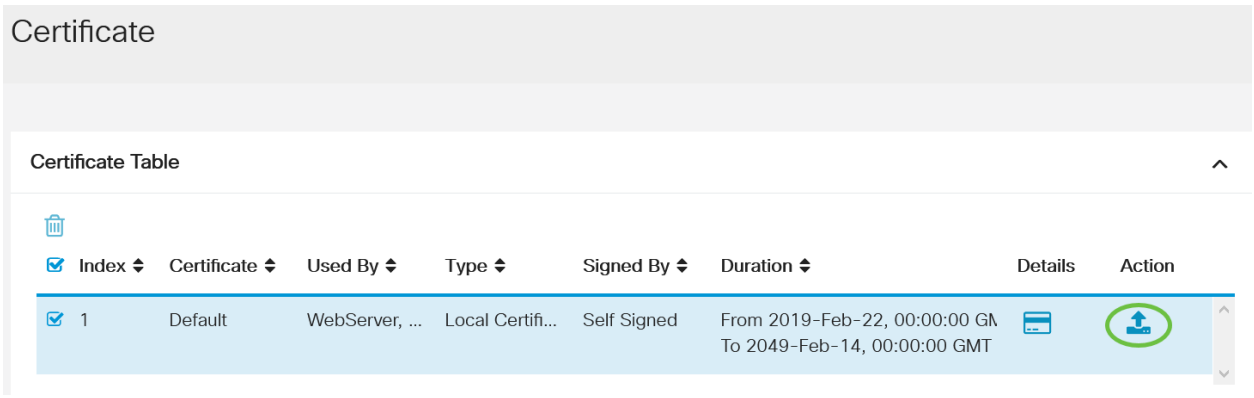
第 1 步

登录RV34x系列路由器并导航至**Administration > Certificate**。



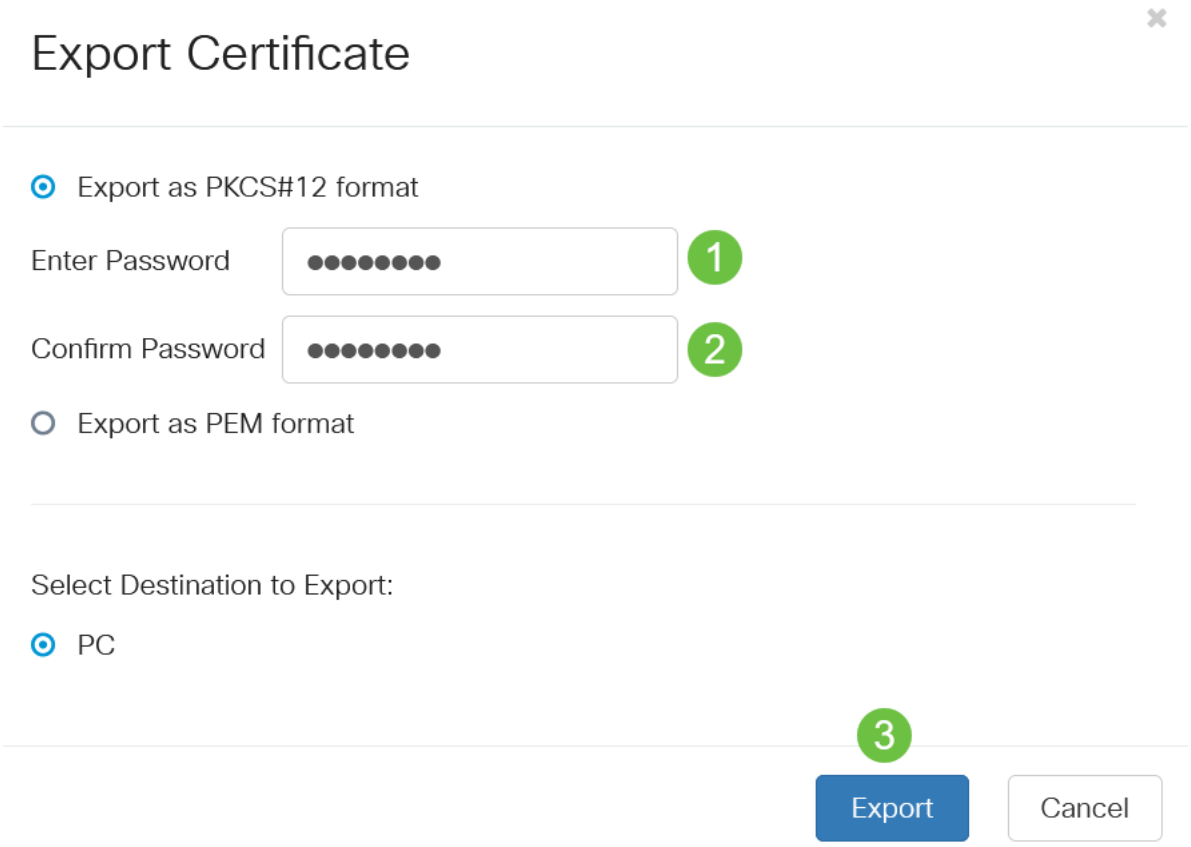
步骤 2

选择默认的自签名证书，然后单击“导出”**按钮**下载证书。



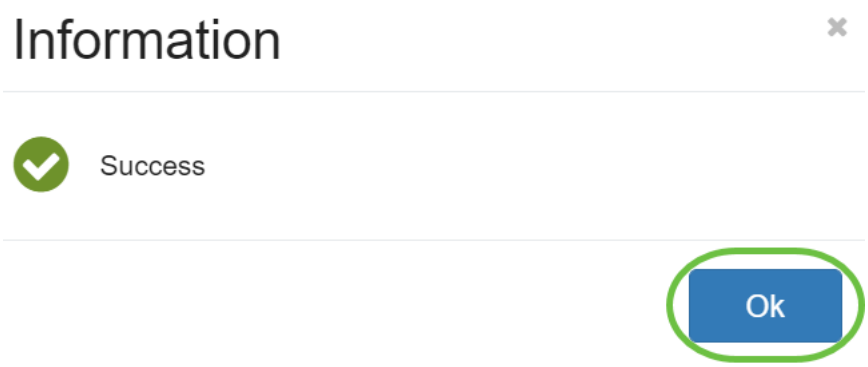
步骤 3

在“导*出证书*”窗口中，输入证书的密码。在“确认密码”字段中重新*输入密*码，然后单击**导出。**



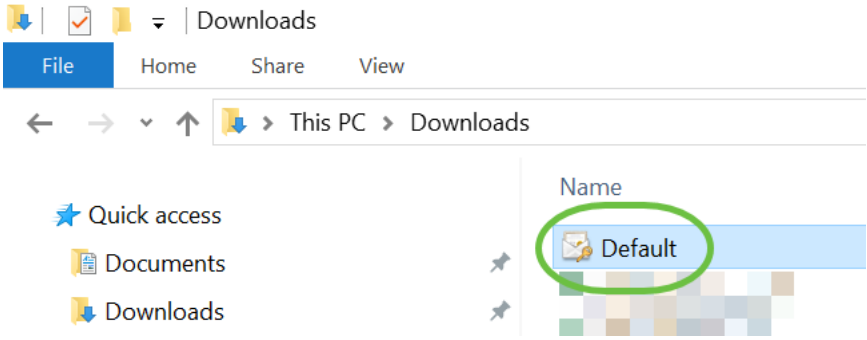
步骤 4

您将看到一个弹出窗口，通知证书已成功下载。Click **OK**.



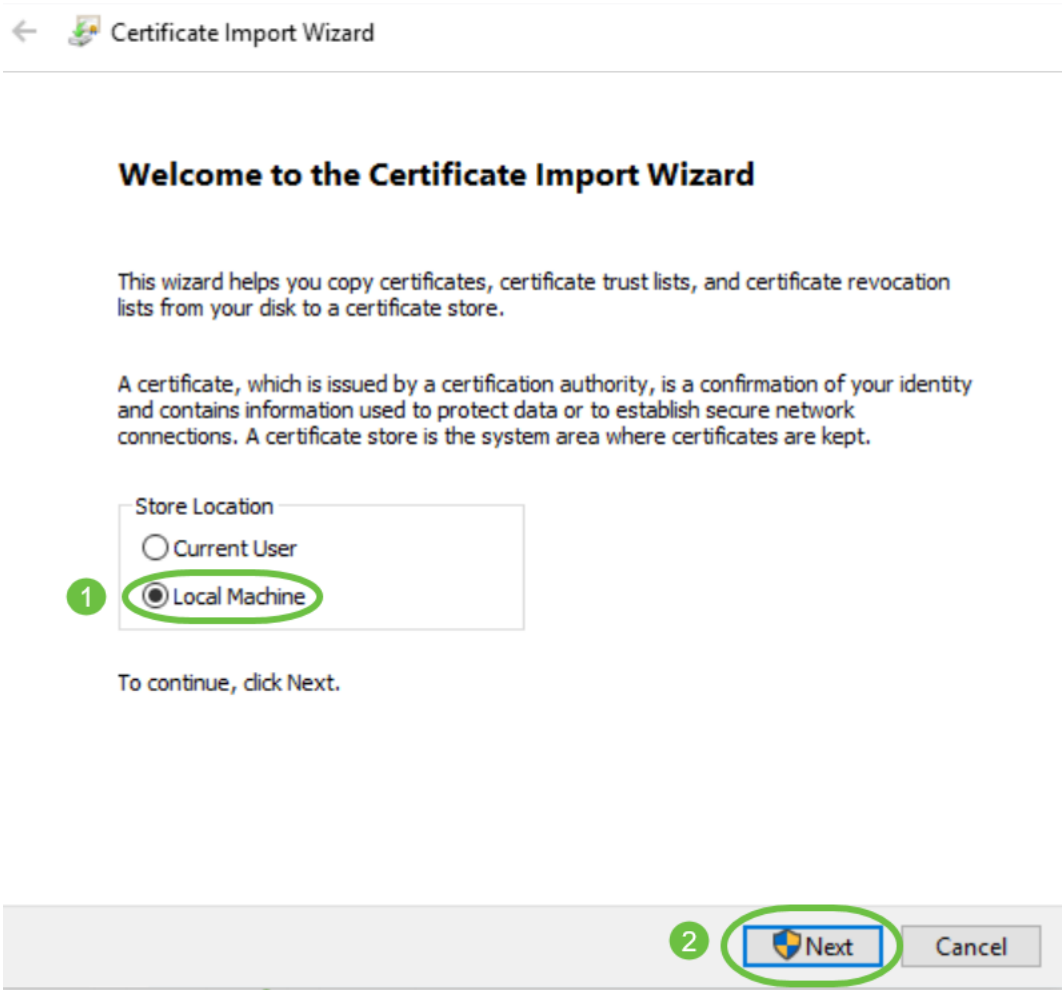
步骤 5

证书下载到您的PC后，找到文件，然后双击它。



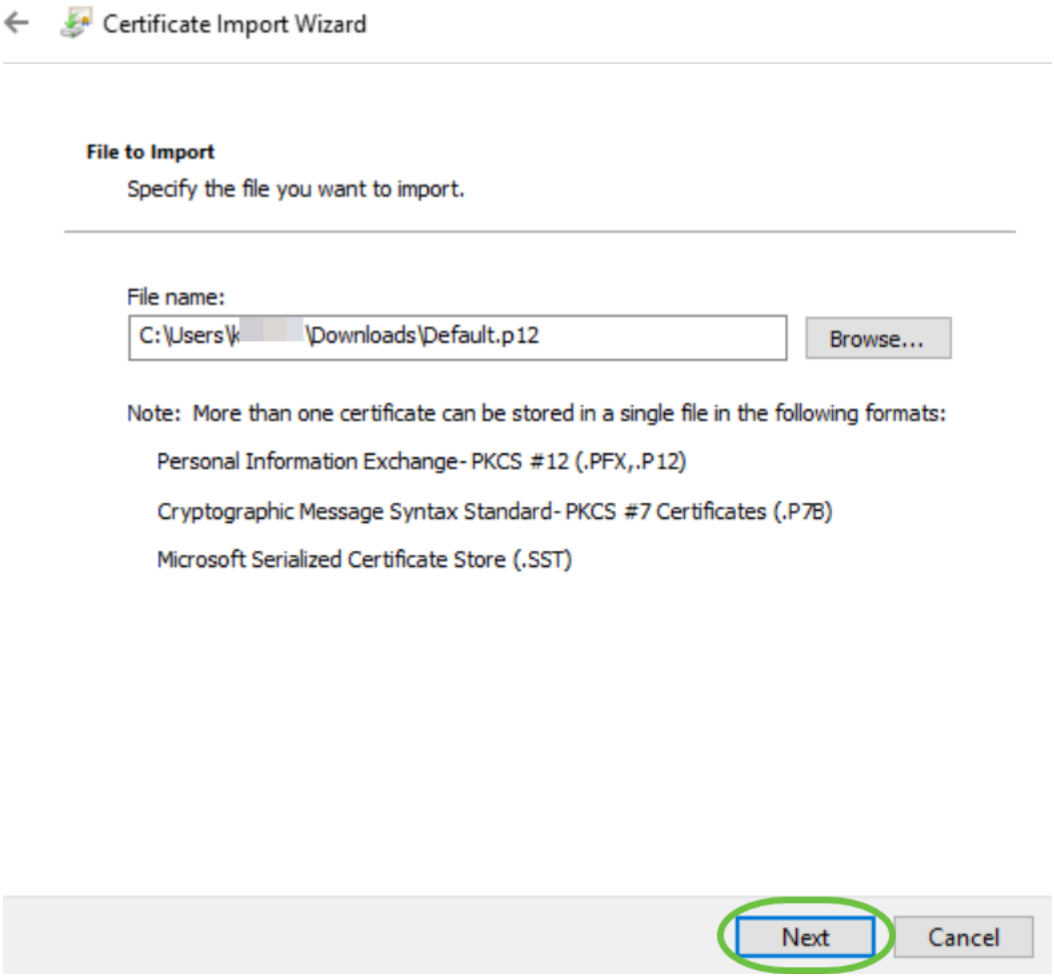
步骤 6

系统将显示“证书导入向导”窗口。对于“存储位置”，选择“**本地计算机**”。单击 **Next**。



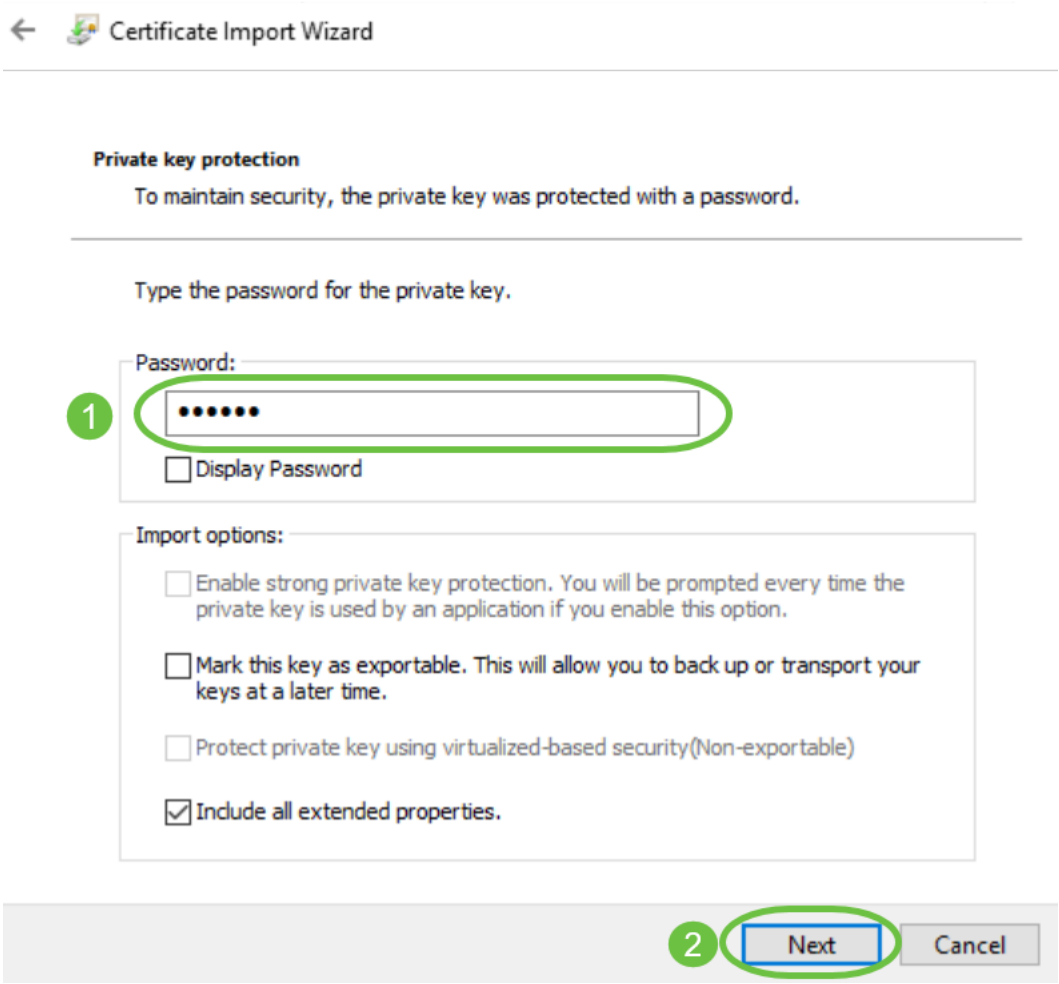
步骤 7

将在以下屏幕上显示“Certificate location and information（证书位置和信息）”。单击 **Next**。



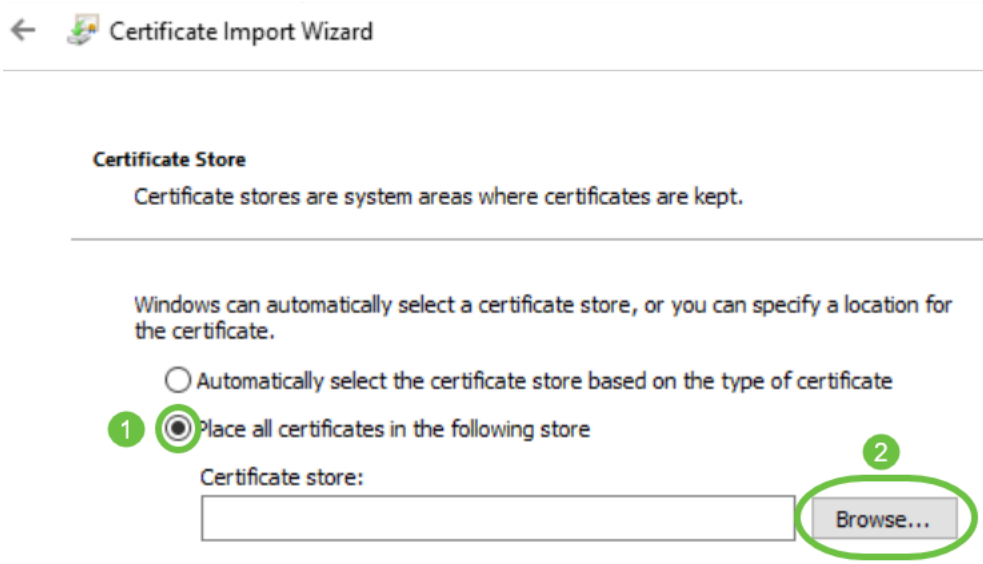
步骤 8

输入为证书选择的密码，然后单击“下一步”。



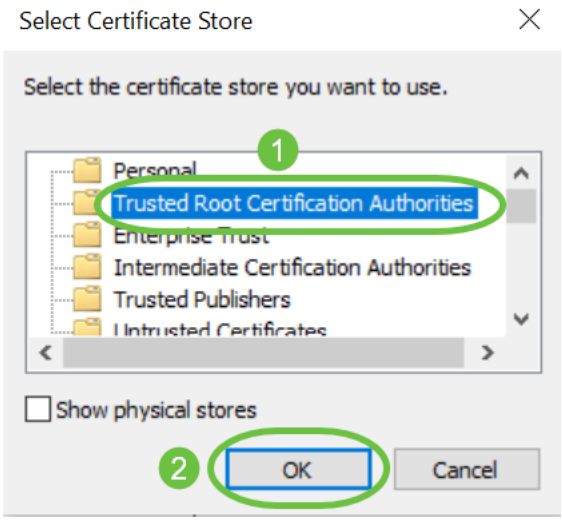
步骤 9

在下一个屏幕上，选择“Place all certificates in the following store”，然后单击“Browse”。



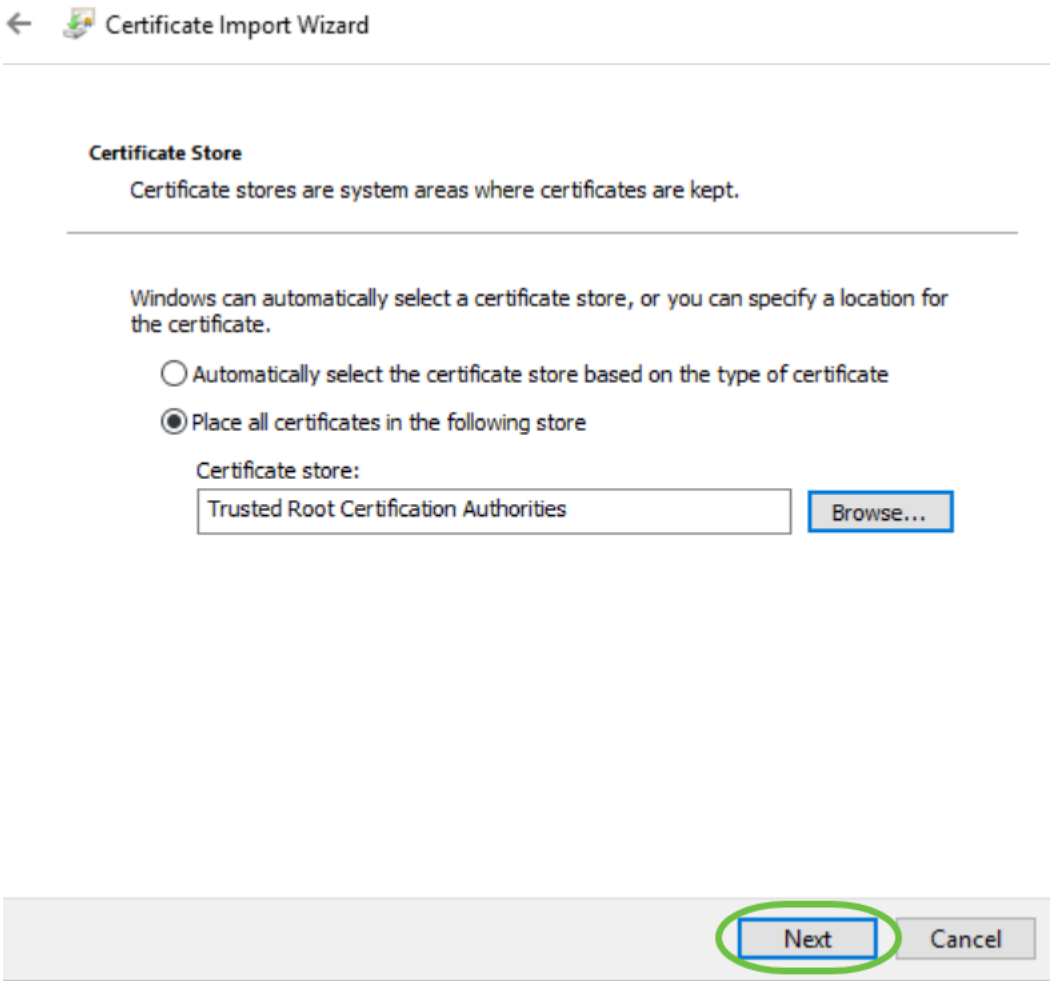
步骤 10

选择“**受信任的根证书颁发**机构”并**单击“确定**”。



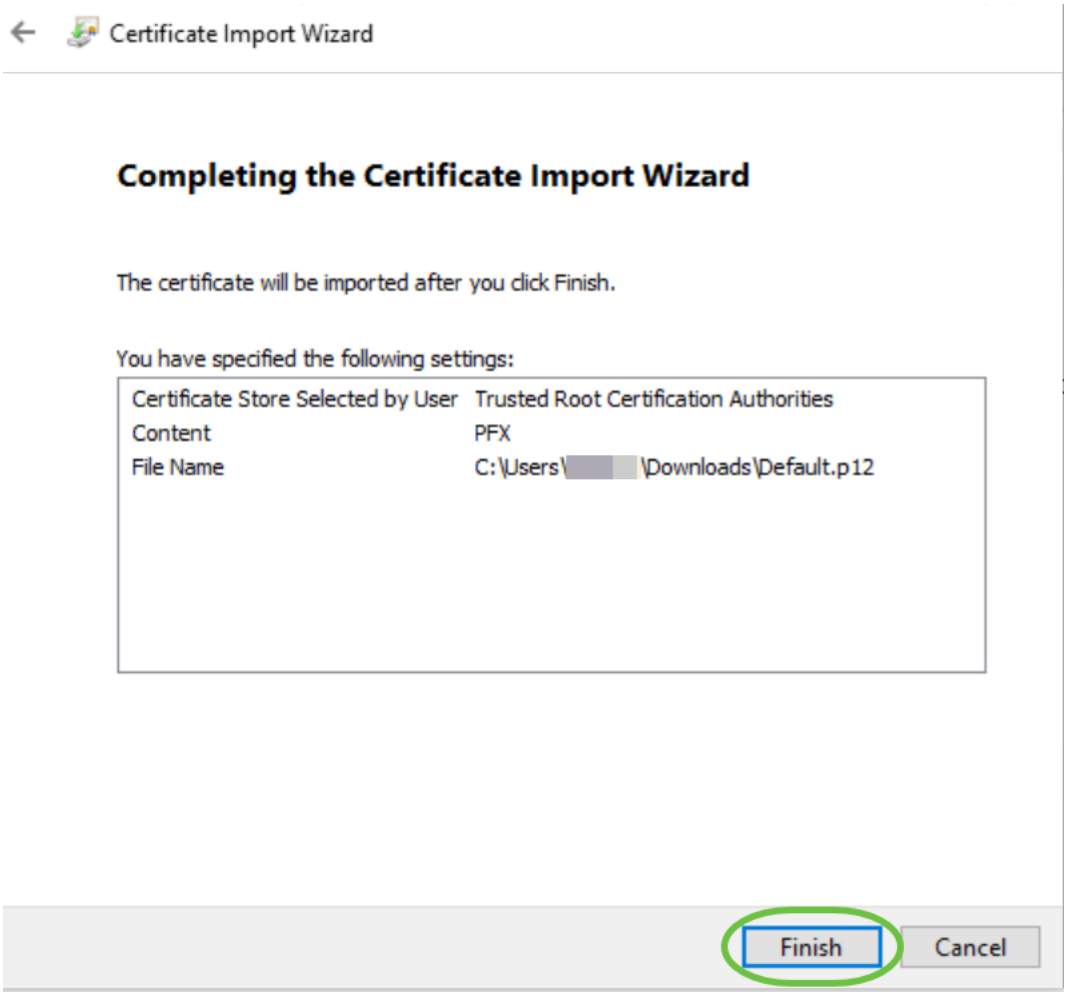
步骤 11

单击 **Next**。



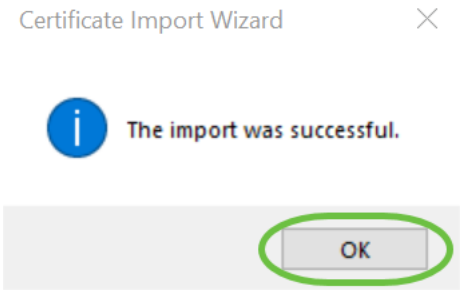
步骤 12

将显示设置摘要。单击**Finish**以导入证书。



步骤 13

您将看到证书已成功导入的确认。Click **OK**.



步骤 14

打开Cisco AnyConnect并尝试重新连接。您不应再看到Untrusted Server警告。

结论

给你！您现在已成功学习了在Windows计算机上将自签名证书作为受信任源安装的步骤，以消除AnyConnect中的“不受信任服务器”警告。

其它资源

[基本故障排除](#) [AnyConnect管理员指南版本4.9](#) [AnyConnect版本说明 — 4.9](#) [思科业务VPN概述和最佳实践](#)