总网络配置：使用Web UI的RV345P和思科企业无线

目标

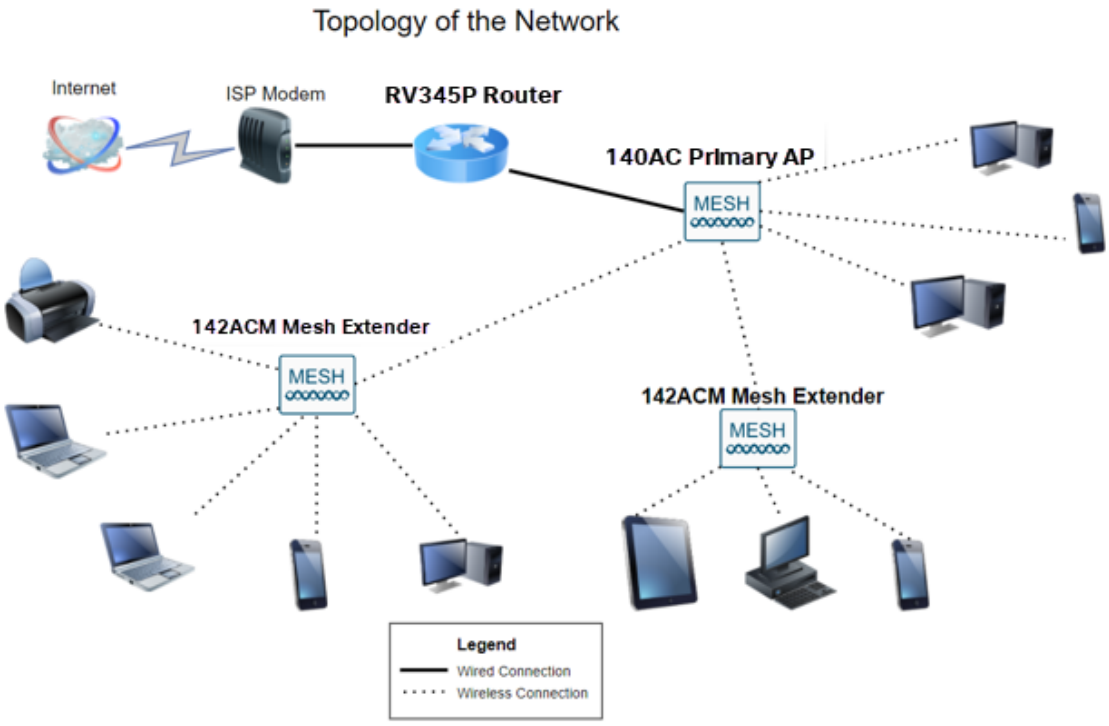
本指南将介绍如何使用RV345P路由器、CBW140AC接入点和两个CBW142ACM网状扩展器配置无线网状网络。

本文使用Web用户界面(UI)建立网状无线网络。如果您希望使用移动应用（推荐用于轻松无线设置），请单击跳至使用移动应用的文章。

目录

- 使用Web UI检查和更新软件
- 在Web UI上创建WLAN
- 可选无线配置
    - 使用Web UI创建访客WLAN（可选）
    - 使用Web UI进行应用程序分析（可选）
    - 使用Web UI进行客户端分析（可选）

拓扑



简介

您的所有研究都汇集在一起，您已购买了思科设备，这真令人兴奋！在本场景中，我们使用RV345P路由器。此路由器提供以太网供电(PoE)，允许您将CBW140AC插入路由器，而不是交换机。CBW140AC和CBW142ACM网状扩展器将用于创建无线网状网络。

此高级路由器还提供了附加功能的选项。

1. 应用控制允许您控制流量。此功能可配置为允许流量，但可记录流量、阻止流量并记录流量，或仅阻止流量。
2. Web过滤用于防止Web流量进入不安全或不适当的网站。此功能没有日志记录。
3. AnyConnect是思科提供的安全套接字层(SSL)虚拟专用网络(VPN)。VPN允许远程用户和站点通过互联网建立安全隧道连接到您的公司办公室或数据中心。

如果您想使用这些功能，则需要购买许可证。路由器和许可证在线注册，本指南将介绍这些内容。

如果您不熟悉本文档中使用的某些术语或想了解有关网状网络的更多详细信息，请查阅以下文章：

- 思科业务：新术语表
- 欢迎使用思科企业无线网状网络
- 思科企业无线网络常见问题(FAQ)

适用设备 |软件版本

- RV345P |1.0.03.21
- CBW140AC |10.4.1.0
- CBW142ACM | 10.4.1.0（网状网络至少需要一个网状扩展器）

先决条件

准备路由器

1. 确保您有当前的Internet连接进行设置。
2. 请联系您的Internet服务提供商(ISP)，了解使用RV345P路由器时他们拥有的任何特殊说明。某些ISP提供带内置路由器的网关。如果您有带集成路由器的网关，则可能必须禁用路由器并将广域网(WAN)IP地址（互联网提供商分配给您的帐户的唯一互联网协议地址）和所有网络流量传递给新路由器。
3. 确定路由器的放置位置。如果可能，您需要一个开放区域。这可能不容易，因为您必须将路由器连接到Internet服务提供商(ISP)的宽带网关（调制解调器）。

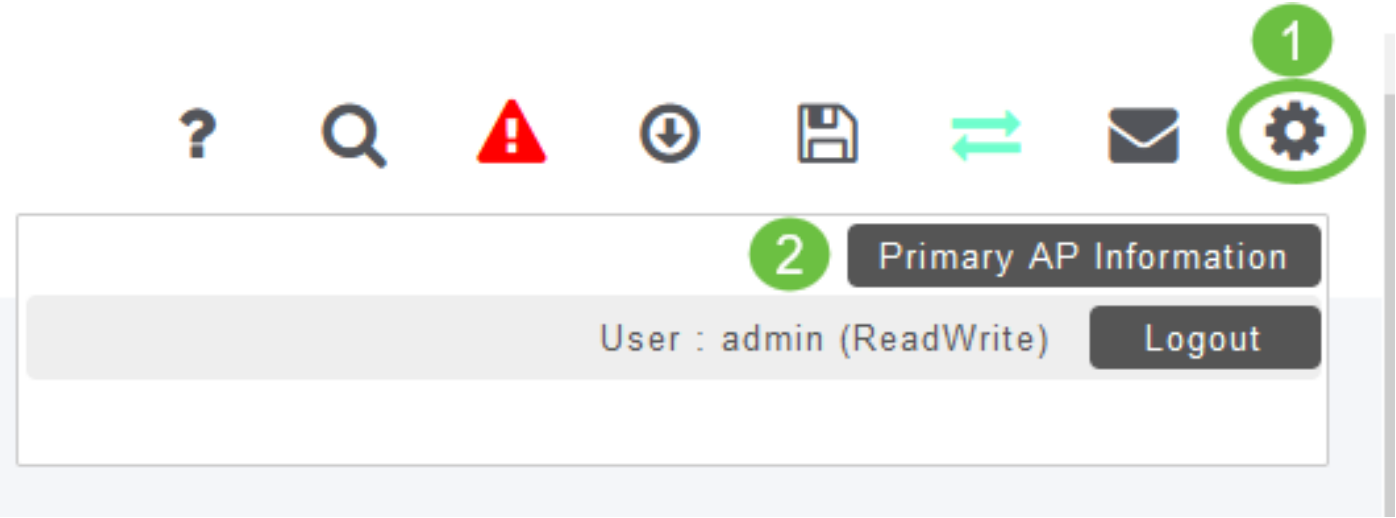
获取Cisco.com帐户

现在您拥有思科设备，您需要获得Cisco.com帐户，有时也称为思科连接在线标识(CCO ID)。 帐户不收费。

如果您已经有帐户，可以跳至本文的下一部分。

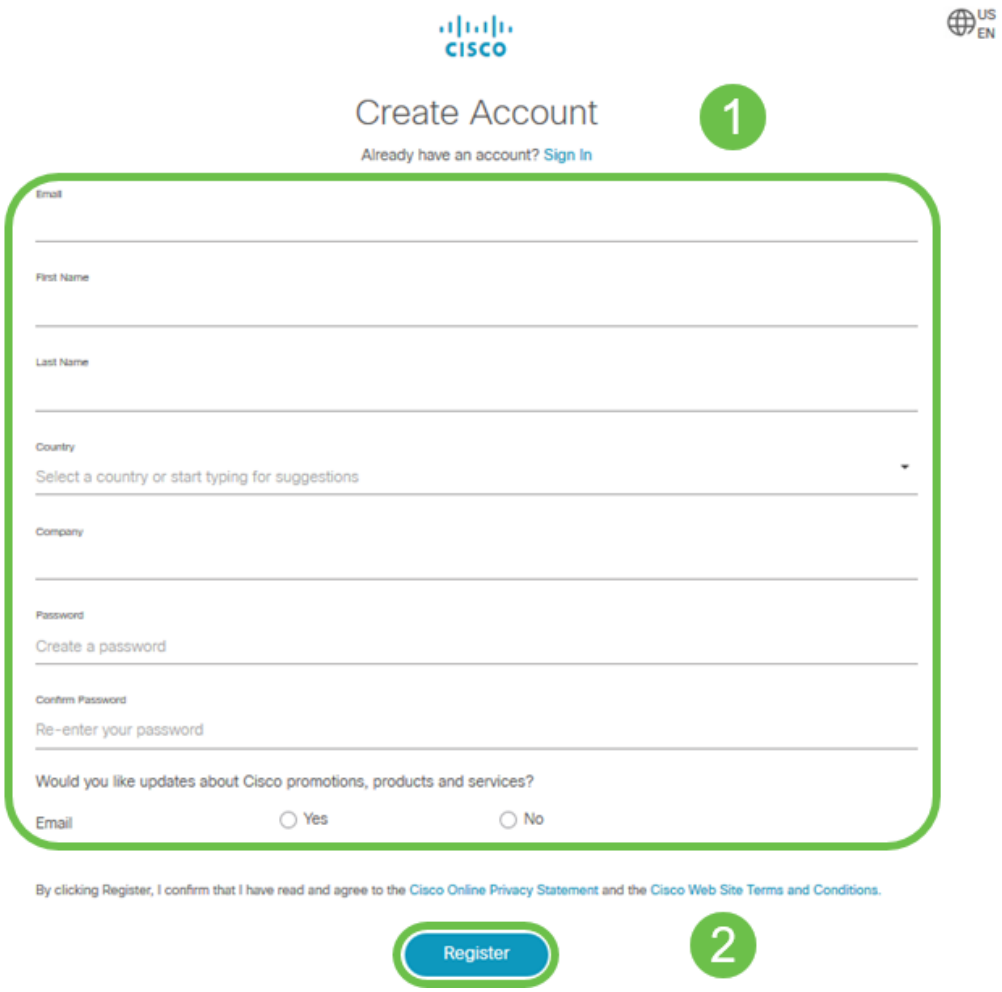
第 1 步

转到Cisco.com。单击“人**员”图**标，然**后单击“创建帐户”**。



步骤 2

输入创建帐户所需的详细信息，然后单击**注册**。按照说明完成注册过程。



如果您有任何问题，[请单击跳至Cisco.com帐户注册帮助页](#)。

配置RV345P路由器

路由器在网络中至关重要，因为它路由数据包。它使计算机能够与其他不在同一网络或子网中的计算机通信。路由器访问路由表以确定应将数据包发送到何处。路由表列出了目的地址。静态和动态配置都可以列在路由表中，以便将数据包发送到其特定目的地。

您的RV345P配有针对许多小型企业优化的默认设置。但是，您的网络需求或Internet服务提供商(ISP)可能要求您修改其中的一些设置。在联系您的ISP了解相关要求后，可以使用Web用户界面(UI)进行更改。

准备好了吗？我们开始吧！

RV345P开箱即用

第 1 步

将以太网电缆从RV345P LAN（以太网）端口之一连接到计算机的以太网端口。如果计算机没有以太网端口，则需要适配器。终端必须与RV345P处于同一有线子网中才能执行初始配置。

步骤 2

请务必使用RV345P随附的电源适配器。使用不同的电源适配器可能损坏RV345P或导致USB连接器故障。电源开关默认打开。

将电源适配器连接到RV345P的12VDC端口，但暂时不要将其插入电源。

步骤 3

确保调制解调器已关闭。

步骤 4

使用以太网电缆将电缆或DSL调制解调器连接到RV345P的WAN端口。

步骤 5

将RV345P适配器的另一端插入电源插座。这将打开RV345P电源。将调制解调器插回电源，以便也能通电。当电源适配器正确连接且RV345P完成启动时，前面板上的电源指示灯呈稳定绿色。

设置路由器

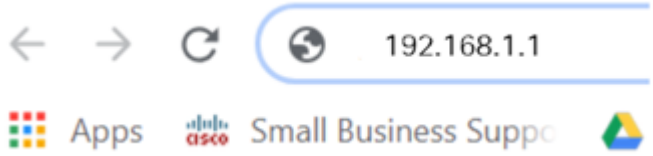
准备工作已完成，现在是时候进行一些配置了！要启动Web UI，请执行以下步骤。

第 1 步

如果将计算机配置为动态主机配置协议(DHCP)客户端，则192.168.1.x范围内的IP地址将分配给PC。DHCP可自动为计算机分配IP地址、子网掩码、默认网关和其他设置。必须将计算机设置为参与DHCP过程才能获取地址。这可以通过选择在计算机上TCP/IP的属性中自动获取IP地址来完成。

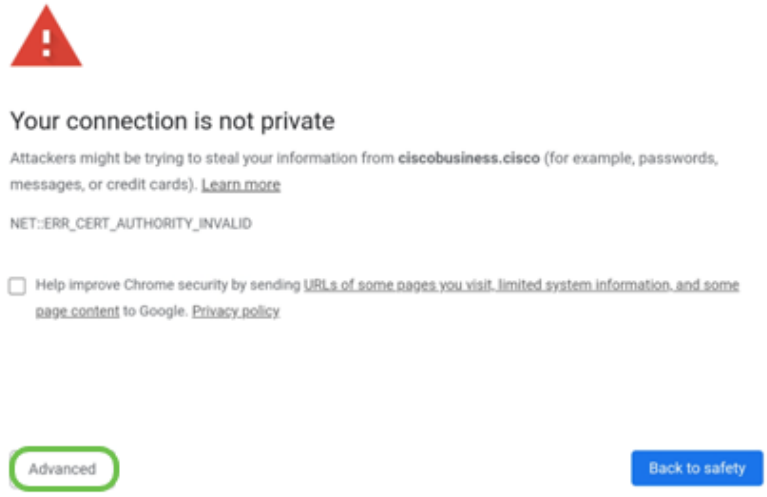
步骤 2

打开Safari、Internet Explorer或Firefox等Web浏览器。在地址栏中，输入RV345P的默认IP地址192.168.1.1。



步骤 3

浏览器可能会发出网站不受信任的警告。继续访问网站。如果您未连接，请跳至“Troubleshooting the Internet Connection(排除Internet连接故障)”。

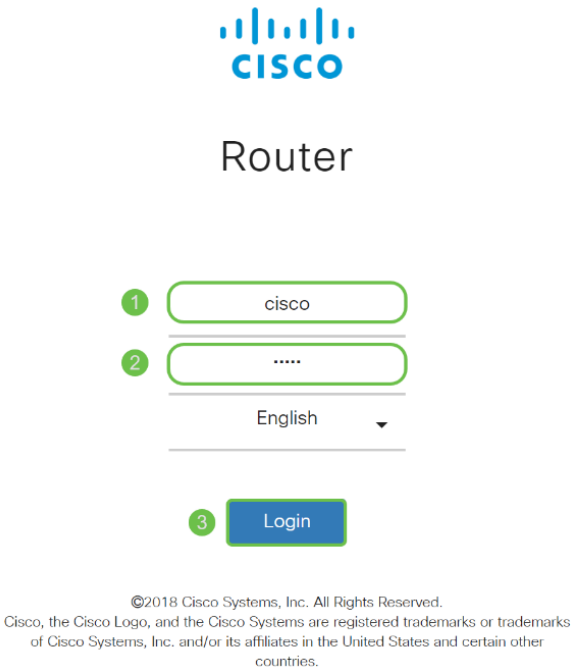


步骤 4

出现登录页时，输入默认用户名*cisco*和默认密*码cisco*。

单击 Login。

有关详细信息，请点击How to access the web-based setup page of Cisco RV340 series VPN routers。



步骤 5

单击 **Login**。系统将*显示*"入门"页。如果导航窗格未打开，可通过单击菜单图标将其**打开**。

现在，您已确认连接并登录到路由器，请跳至本文的初始配置部分。

排除Internet连接故障

当然，如果您正在阅读此内容，您可能无法连接到Internet或Web UI。其中一个解决方案应会有所帮助。

在已连接的Windows操作系统上，您可以通过打开命令提示符来测试网络连接。输入**ping 192.168.1.1**（路由器的默认IP地址）。 如果请求超时，您将无法与路由器通信。

如果连接不正常，可以查看此故障排除文章。

其他一些需要尝试的东西：

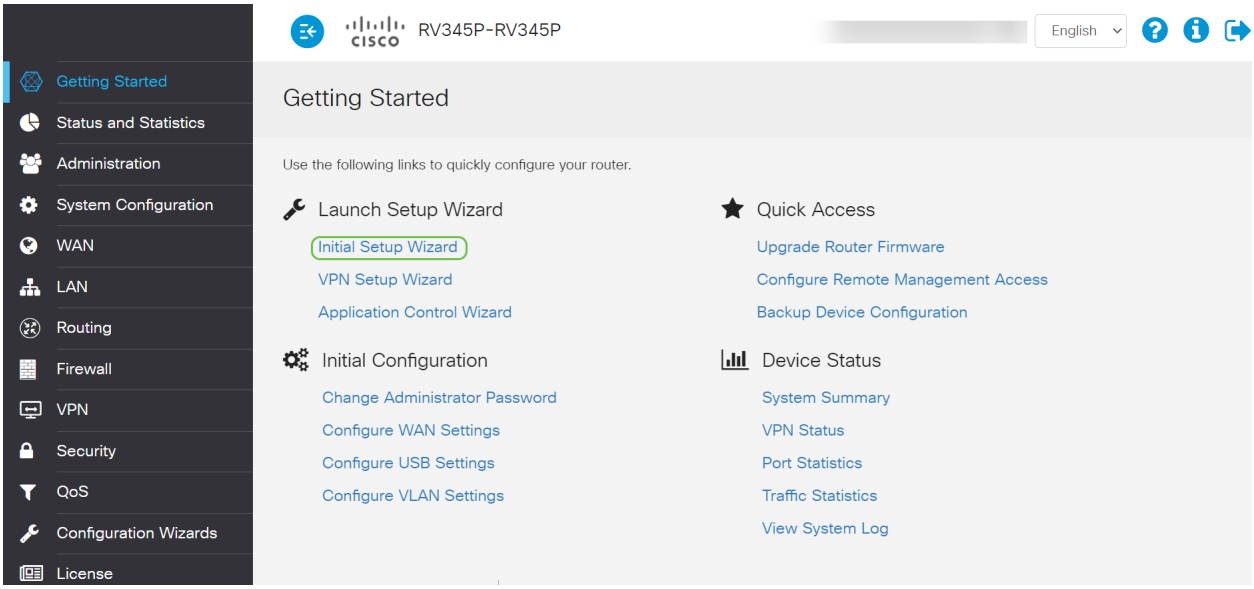
1. 验证您的Web浏览器是否未设置为“脱机工作”。
2. 检查以太网适配器的局域网连接设置。PC应通过DHCP获取IP地址。或者，PC可以在192.168.1.x范围内拥有静态IP地址，默认网关设置为192.168.1.1（RV345P的默认IP地址）。 要连接，您可能需要修改RV345P的网络设置。如果使用Windows 10，请查看Windows 10指示以修改网络设置。
3. 如果现有设备占用192.168.1.1 IP地址，则需要解决此冲突，网络才能运行。本部分末尾有关此内容的详细信息，或者单击此处直接转到此处。
4. 关闭两台设备，重置调制解调器和RV345P。接下来，打开调制解调器电源，让它空闲大约2分钟。然后打开RV345P电源。您现在应该会收到WAN IP地址。
5. 如果您有DSL调制解调器，请让您的ISP将DSL调制解调器置于网桥模式。

初始配置

我们建议您完成本节中*列出的*初始设置向导步骤。您可以随时更改这些设置。

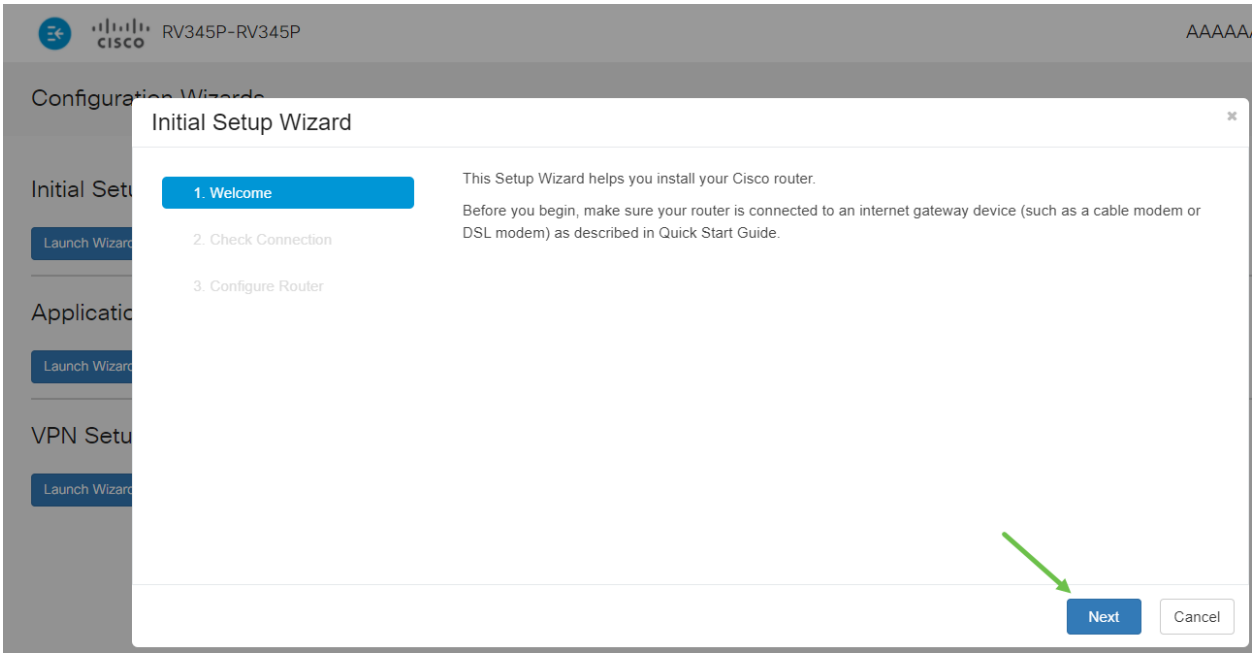
第 1 步

从“入**门”页单**击“初始*设置向*导”。



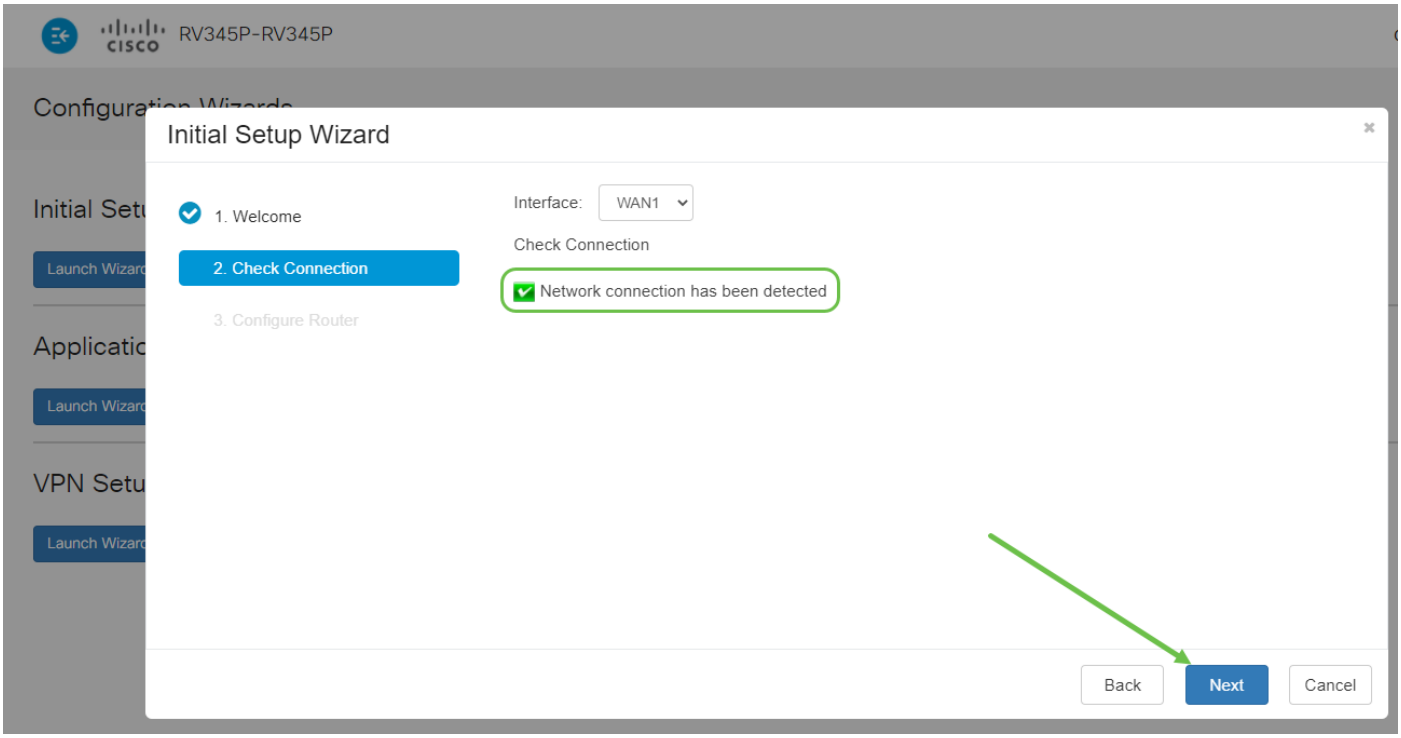
步骤 2

此步骤确认电缆已连接。由于您已确认此项，请单击“下**一步”**。



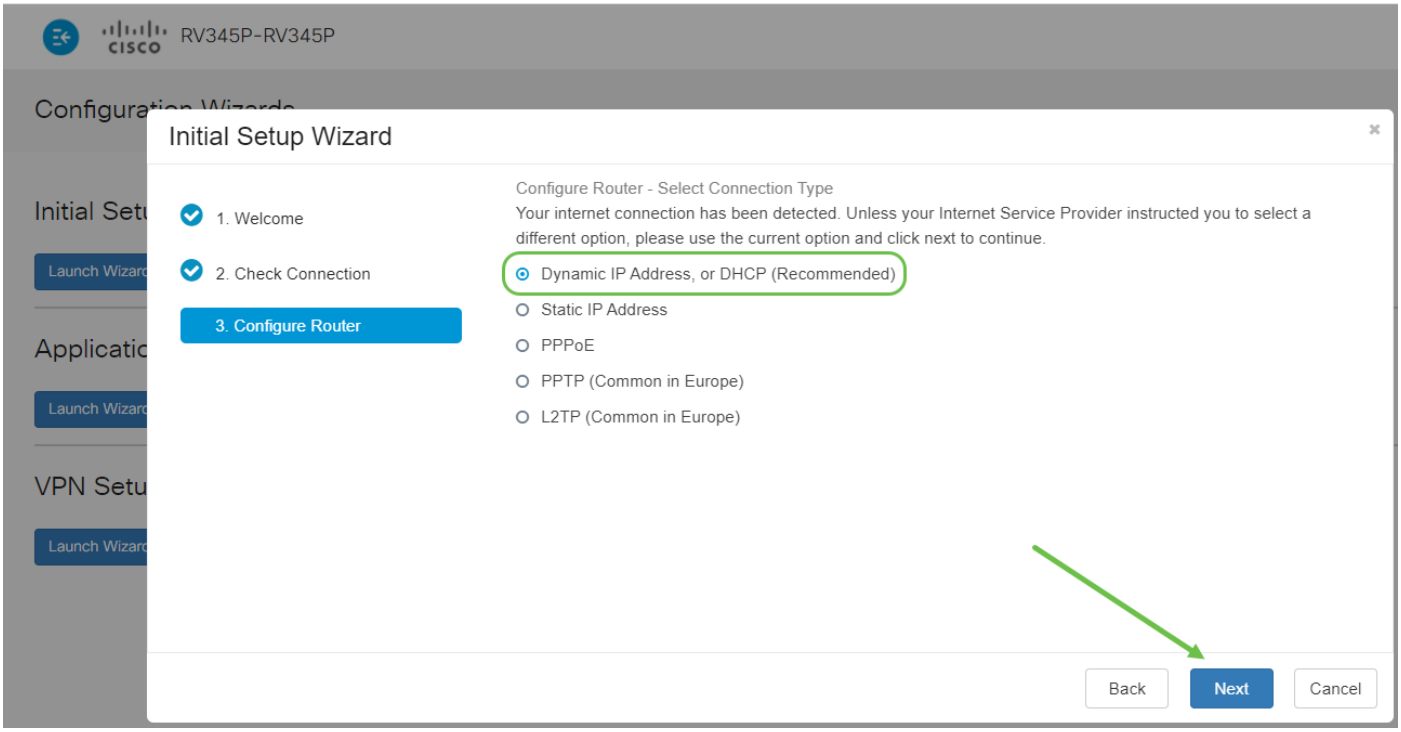
步骤 3

此步骤包括确保路由器已连接的基本步骤。由于您已确认此项，请单击“下一步”。



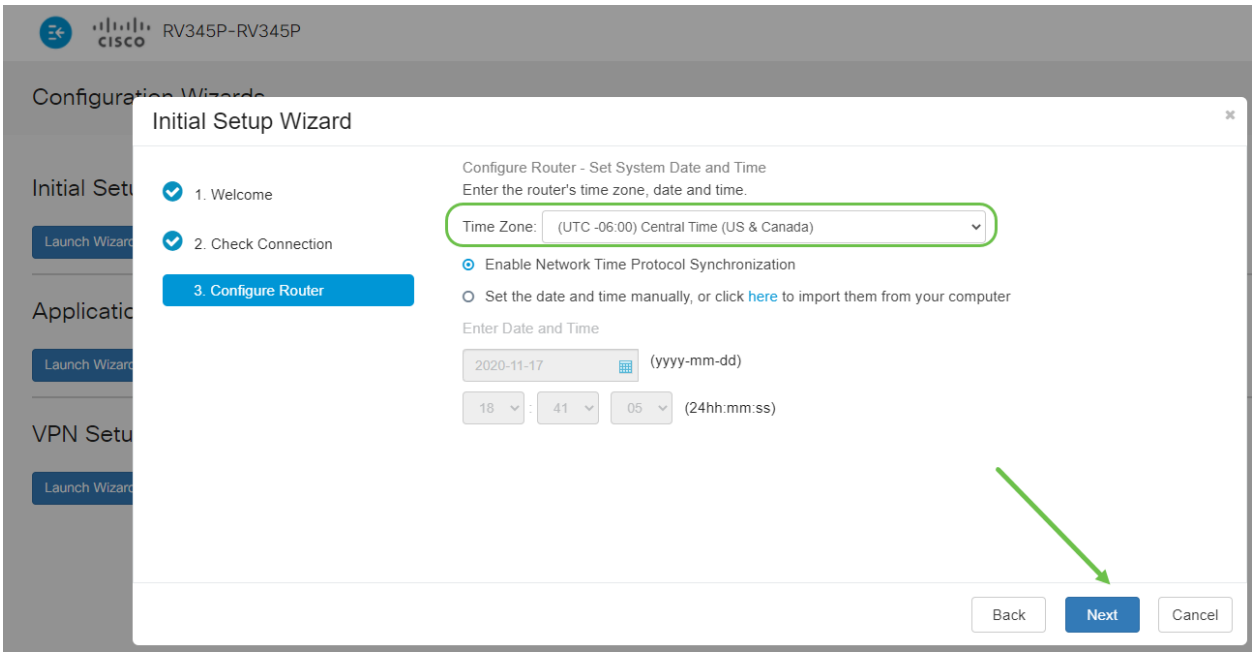
步骤 4

下一个屏幕显示您为路由器分配IP地址的选项。在此场景中，您需要选择DHCP。单击Next。



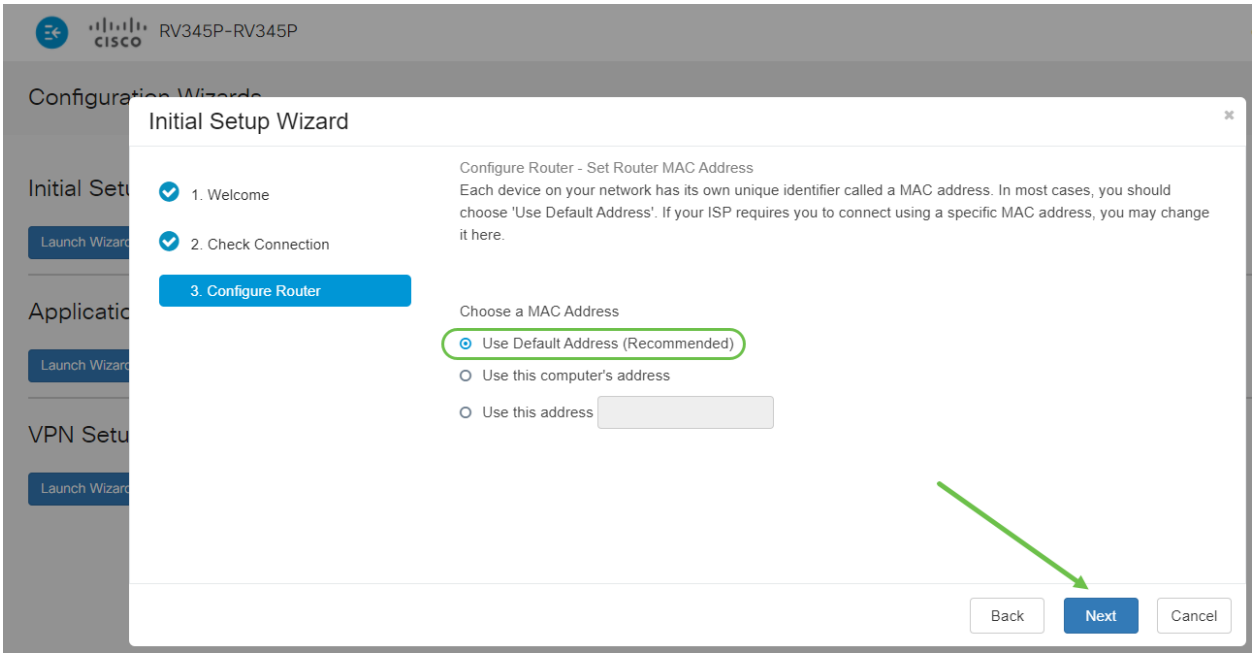
步骤 5

系统将提示您设置路由器时间设置。这一点很重要，因为它可在查看日志或排除事件故障时实现精确性。选择时**区，然**后单击**下一步**。



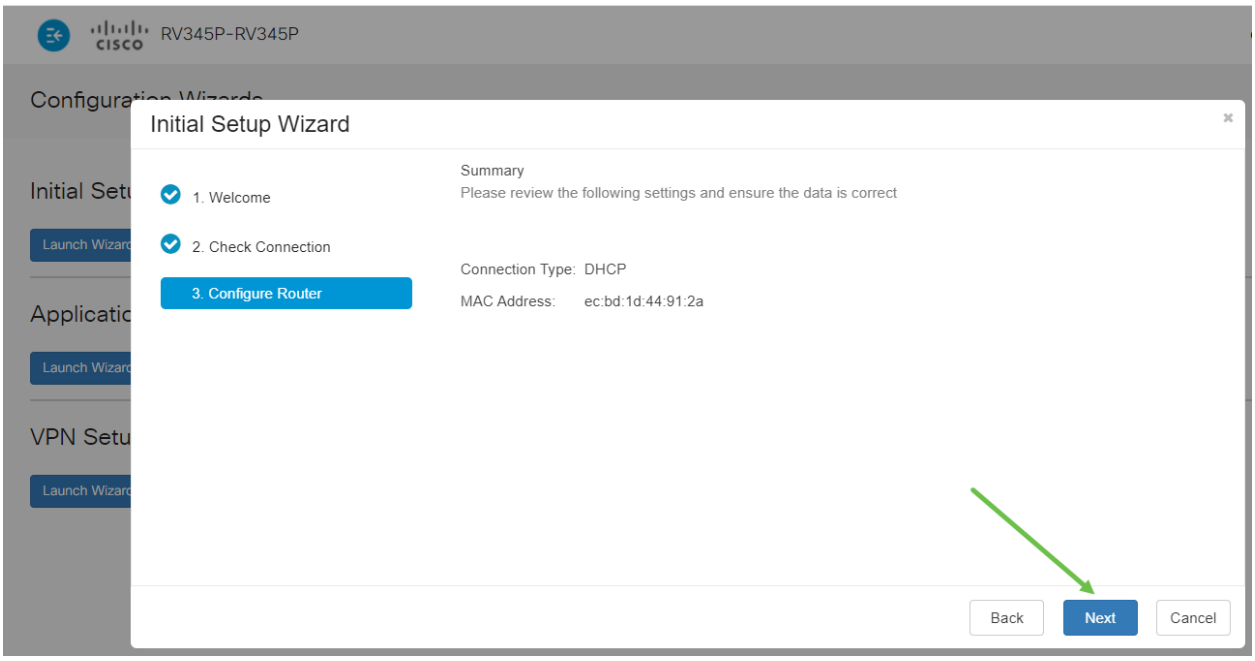
步骤 6

您将选择要分配给设备的MAC地址。通常，您将使用默认地址。单击 Next。



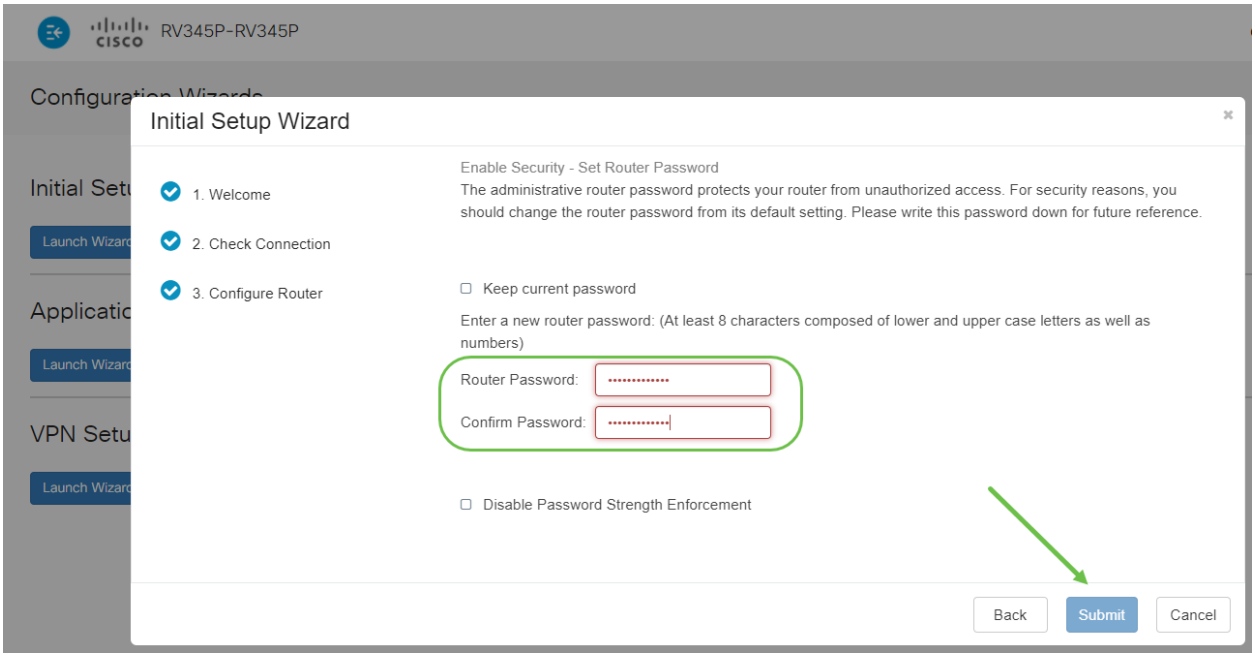
步骤 7

以下页面是所选选项的摘要。如果满意，请查看并**单击“下一步”**。



步骤 8

在下一步中，您将选择登录路由器时使用的密码。密码的标准是至少包含8个字符（大小写和小写）并包含数字。请**输入符**合强度要求的密码。单击 Next。记下您的密码以供将来登录。



建议不 *要选择禁用密码强 度实施*。此选项允许您选择简单到123的密码，该密码与恶意攻击者1-2-3一样容易破解。

步骤 9

单击“保**存”图标**。

如果需要有关这些设置的详细信息，可以阅读[在RV34x路由器上配置DHCP WAN设置]。

您的RV345P默认启用以太网供电(PoE)，但您可以对其进行一些调整。如果需要自定义设置，请选中[在RV345P路由器上配置以太网供电(PoE)设置]。

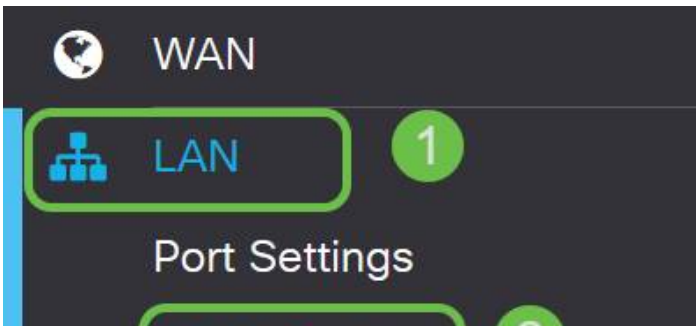
根据需要编辑IP地址（可选）

完成“初始 *设置向导*”后，可以通过编辑VLAN设置在路由器上设置静态IP地址。

只有在需要为现有网络中的路由器IP地址分配特定地址时，才需要执行此过程。如果不需要编辑IP地址，可以转到本文[的下]一部分。

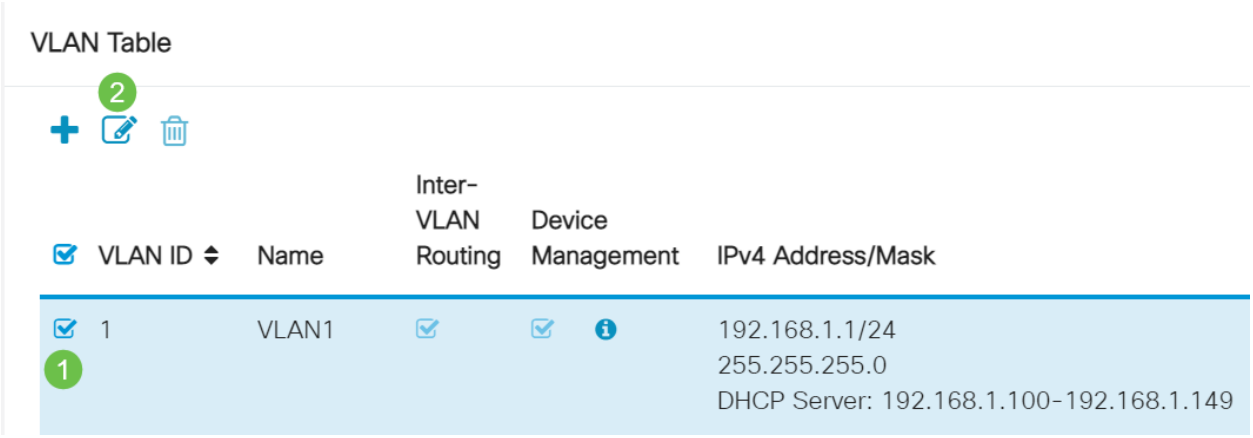
第 1 步

在左侧菜单中，单击“LAN”**>“VLAN设置”**。



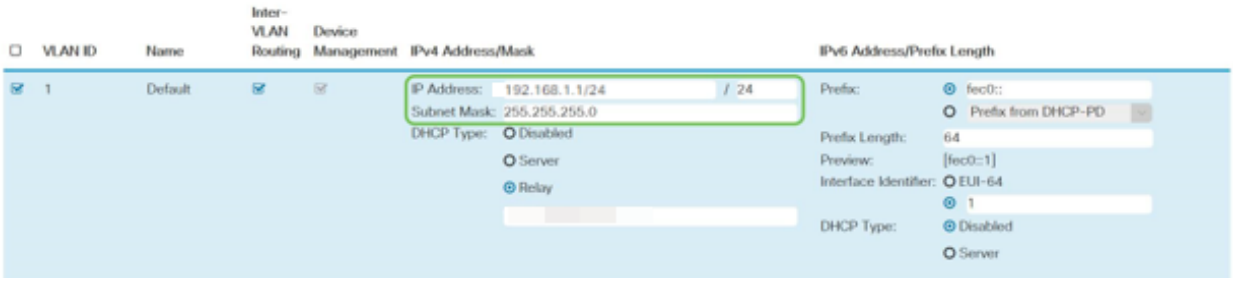
步骤 2

选择包**含路**由设备的VLAN，然后单击编**辑图标**。



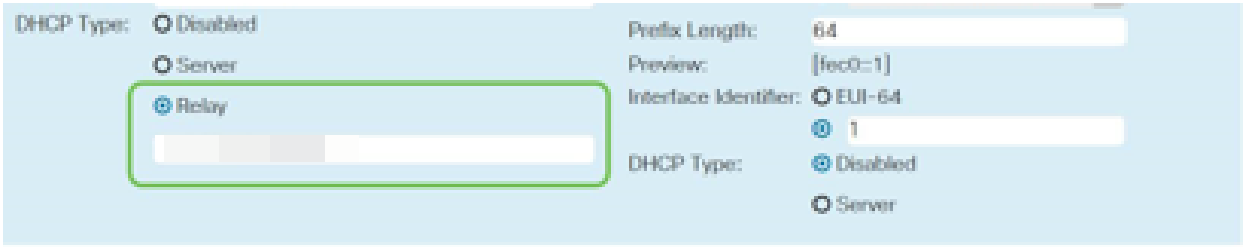
步骤 3

输入所需**的静态IP**地址，然**后单**击右上角的应用。



步骤 4（可选）

如果您的路由器不是分配IP地址的DHCP服务器/设备，则可以使用DHCP中继功能将DHCP请求定向到特定IP地址。IP地址可能是连接到WAN/Internet的路由器。

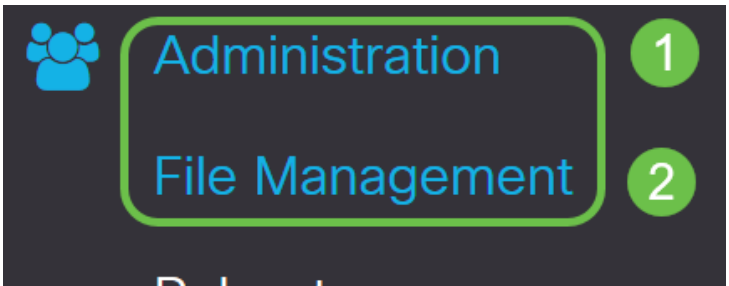


升级固件（如果需要）

这是一个重要步骤，不要跳过！

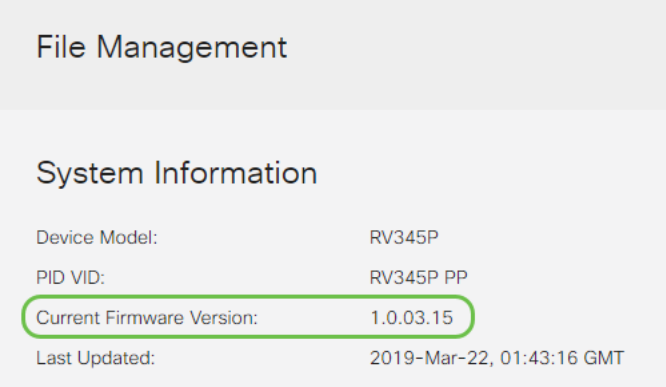
第 1 步

选择**管理>文件管理**。



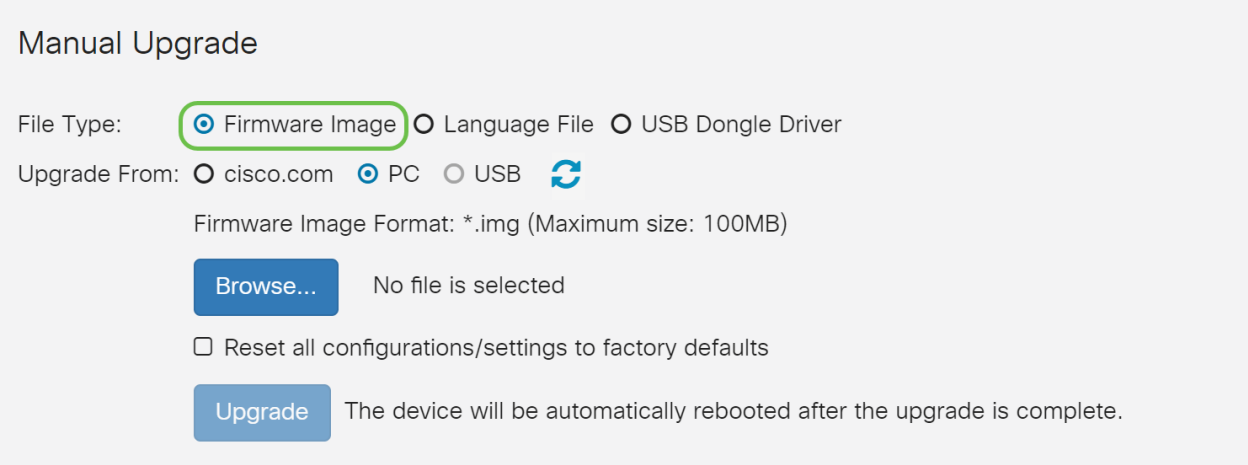
在“*系统信息*”区域中，以下子区域描述以下内容：

- 设备型号 — 显示设备型号。
- PID VID — 路由器的产品ID和供应商ID。
- 当前固件版本 — 设备上当前运行的固件。
- Cisco.com上提供的最新版本 — 思科网站上提供的软件的最新版本。
- 固件上次更新 — 路由器上上次固件更新的日期和时间。



步骤 2

在“Manual Upgrade(*手动升级*)”部分下，单击“File Type(文件类**型**)”的“Firmware Image(固件映*像*)”*单选按钮*。



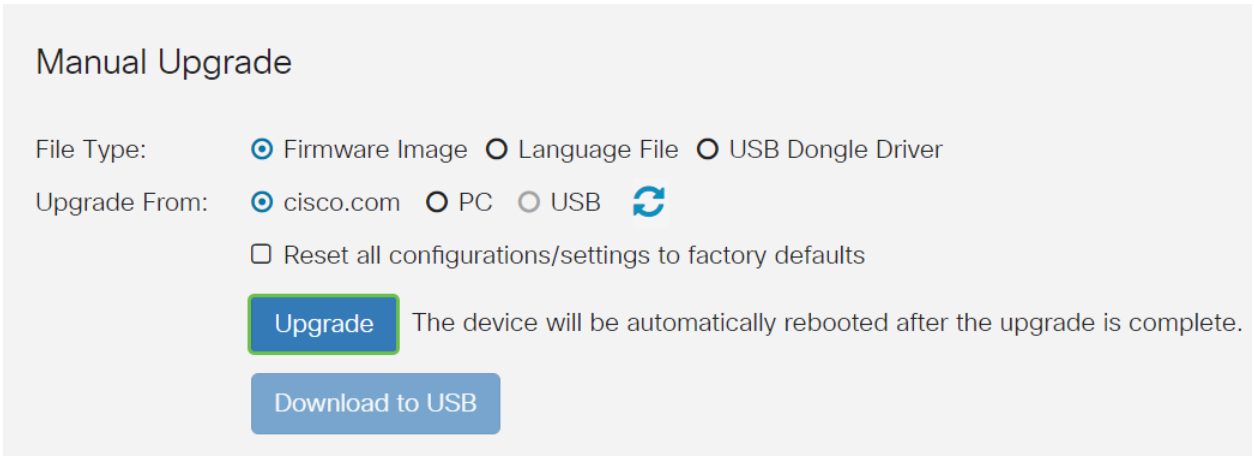
步骤 3

在“*手动升级*”页上，单击单选按钮以选*择cisco.com*。此功能还有其他一些选项，但这是执行升级的最简单方法。此过程直接从思科软件下载网页安装最新的升级文件。

如果您的设备未连接到Internet或者因Internet断开而受到影响，您将无法从cisco.com升级。如果这与您有关，可在此处找到其他 选项。

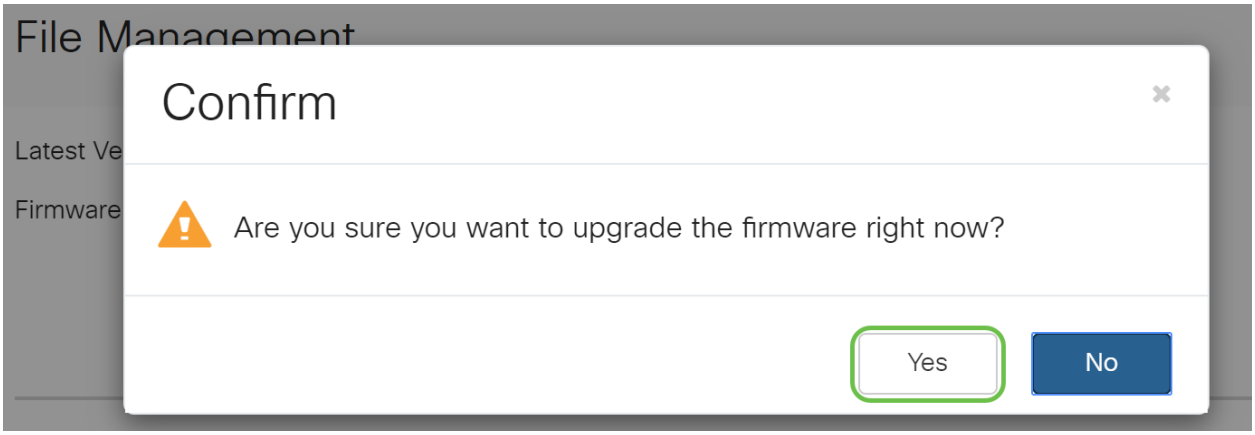
步骤 4

单击**Upgrade**。

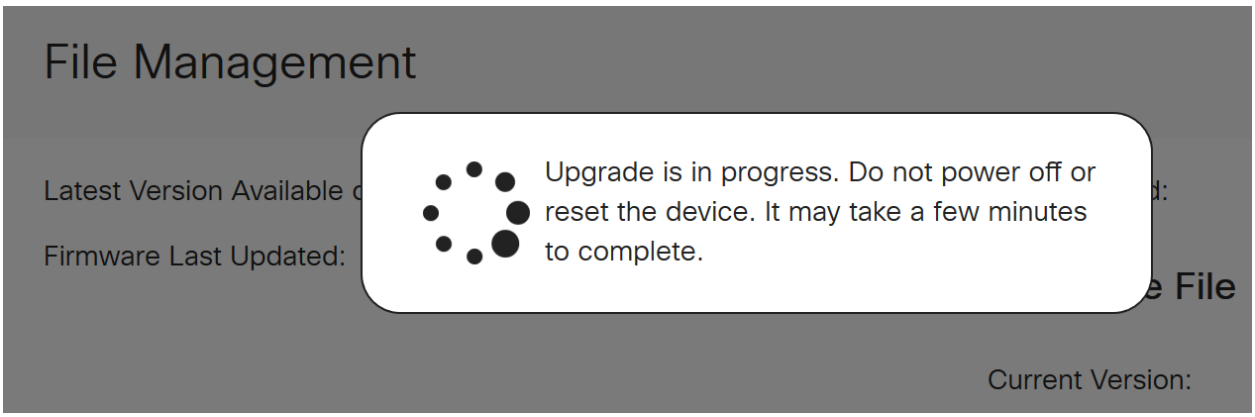


步骤 5

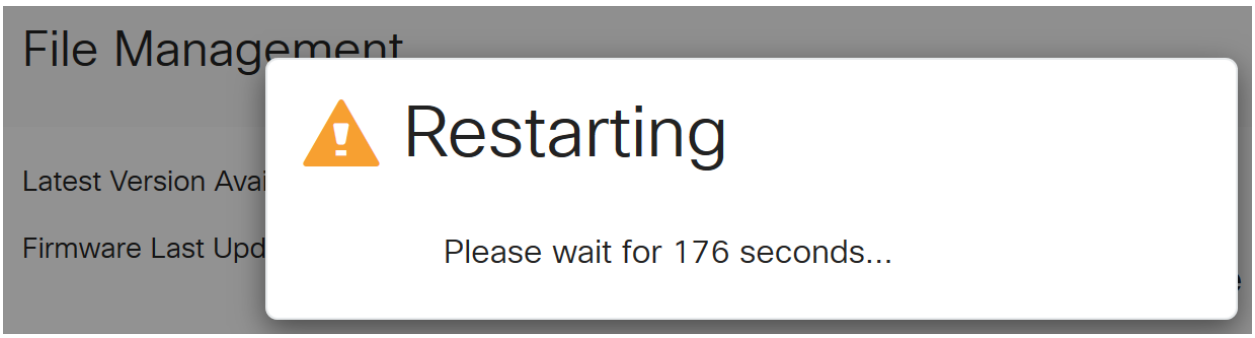
在确认窗口中单击是继续。



更新过程需要不中断地运行。升级过程中，屏幕上会显示以下消息。

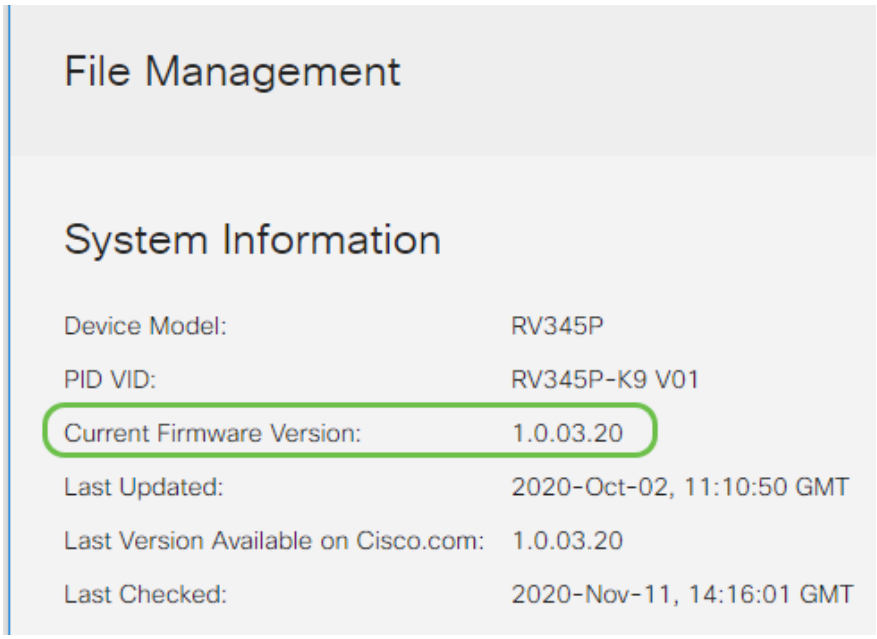


升级完成后，系统将弹出一个通知窗口，通知您路由器将*重新启动*，并倒数估计完成过程的时间。之后，您将注销。



步骤 6

重新登录基于Web的实用程序以验证路由器固件是否已升级，滚动到*System Information*。“当前*固件版本*”区域现在应显示已升级的固件版本。

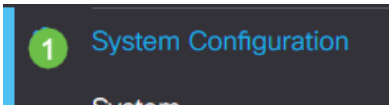


在RV345P系列路由器上配置自动更新

由于更新非常重要，而您是忙碌的人，因此从此处开始配置自动更新是明智之举！

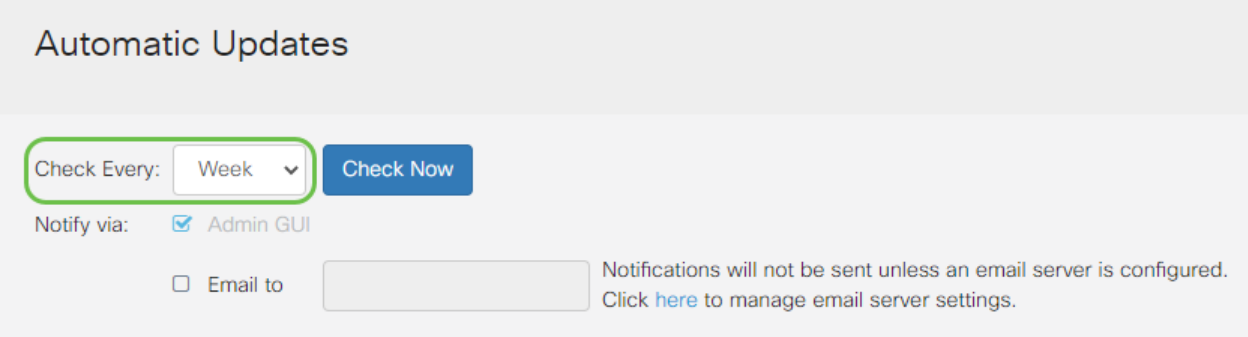
第 1 步

登录到基于Web的实用程序，然后选择**System Configuration > Automatic Updates**。



步骤 2

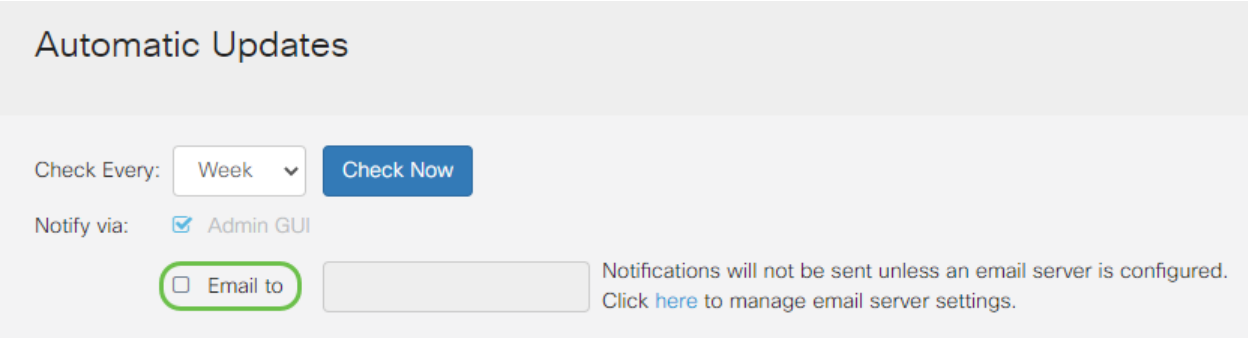
从*Check Every*下拉列表中，选择路由器应检查更新的频率。



步骤 3

在“通*知”区*域中，选中“通**过电**子邮件发送更新”复选框。默认*情况下*，“管理GUI”复选框已启用，无法禁用。更新可用后，基于Web的配置中将显示通知。

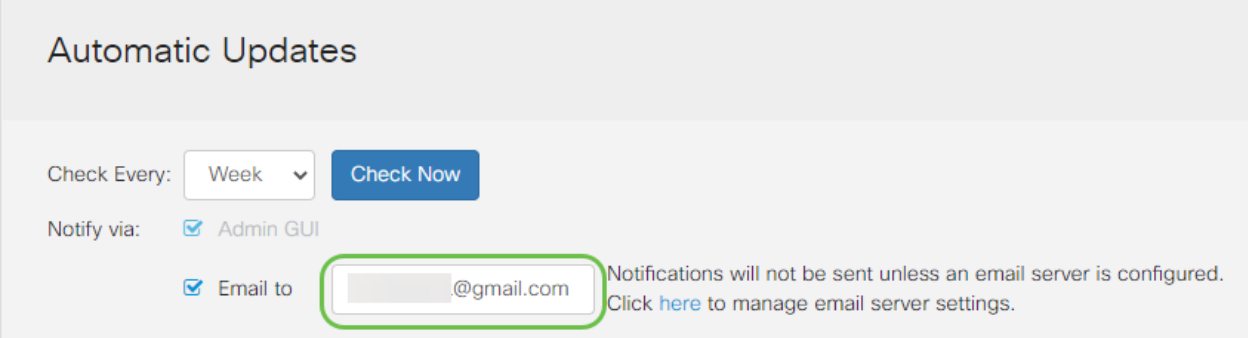
如果要设置电子邮件服务器设置，请单击此处了解如何。



步骤 4

在“电邮至地址”字*段中输*入电邮地址。

强烈建议使用单独的电子邮件帐户，而不是使用个人电子邮件来维护隐私。

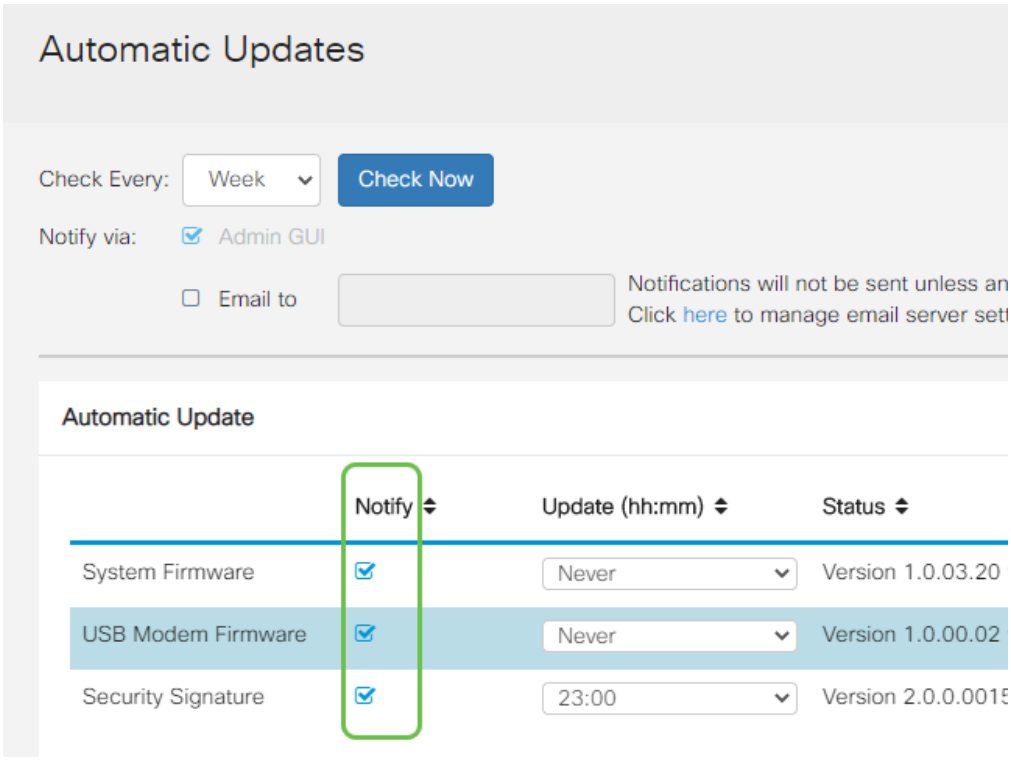


步骤 5

在“自*动更新*”区域下，选中**Notify** 复选框以显示要通知的更新类型。选项有：

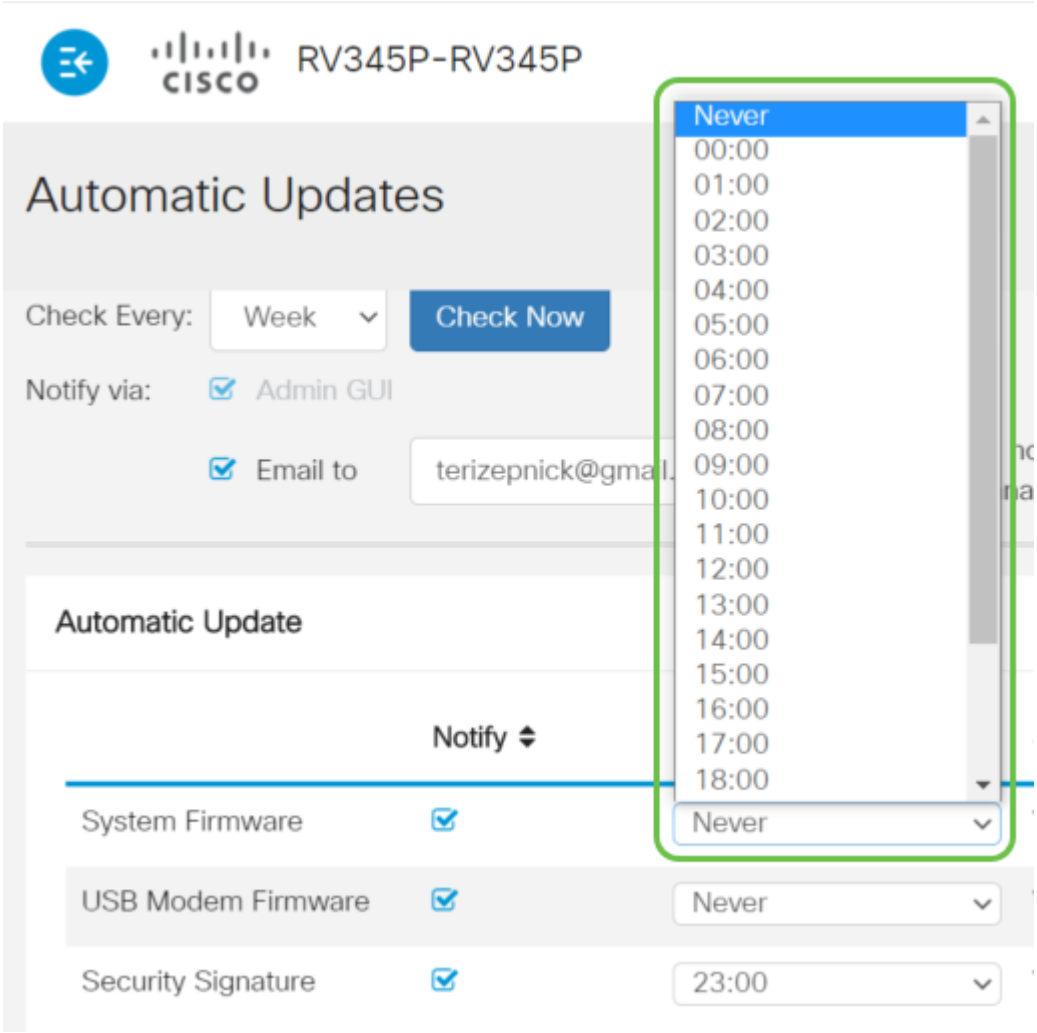
- 系统固件 — 设备的主控制程序。

- USB调制解调器固件 — USB端口的控制程序或驱动程序。
- 安全签名 — 此签名将包含应用控制的签名，用于识别应用、设备类型、操作系统等。



步骤 6

从*自动更新*下拉列表中，选择要完成自动更新的一天中的某个时间。某些选项可能因您选择的更新类型而异。安全签名是进行立即更新的唯一选项。建议您设置关闭办公室的时间，以便在不方便的时间不中断服务。



状态显示当前运行的固件版本或安全签名。

步骤 7

单击 Apply。

步骤 8

要永久保存配置，请转至“复制/保存配置”页，或单击**页面**上部的保存图标。

太棒了，您的路由器基本设置已完成！现在，您有一些配置选项可供探索。

安全选项

当然，您希望网络安全。有一些简单的选项，例如使用复杂的密码，但如果您想采取措施实现更安全的网络，请查看本节中有关安全性的内容。

RV安全许可证（可选）

此RV安全许可证功能可保护您的网络免受来自Internet的攻击：

- 入侵防御系统(IPS):检查网络数据包、日志和/或阻止各种网络攻击。它提供更高的网络可用性、更快的补救和全面的威胁防护。
- 防病毒：通过扫描应用程序以查找各种协议（如HTTP、FTP、SMTP电子邮件附件、POP3电子邮件附件和通过路由器的IMAP电子邮件附件）来防止病毒。
- 网络安全：在连接到互联网时实现业务效率和安全性，允许终端设备和互联网应用的互联网访问策略帮助确保性能和安全性。它基于云，包含80多个类别，分类的域超过4.5亿。
- 应用识别：确定策略并将其分配给Internet应用。500个独特应用会自动识别。
- 客户端标识：动态识别客户端并对其进行分类。能够根据终端设备类别和操作系统分配策略。

RV安全许可证提供网络过滤。Web过滤功能允许您管理对不适当网站的访问。它可以屏幕客户端的Web访问请求，以确定是允许还是拒绝该网站。

许可的安全功能可免费试用90天。如果您希望在评估期后继续使用路由器上的高级安全功能，则必须获取并激活许可证。

另一个安全选项是Cisco Umbrella。如果您想跳到Umbrella部分，请单击此处。

如果不需要任何一个安全许可证，请单击跳至本文档的VPN部分。

智能帐户简介

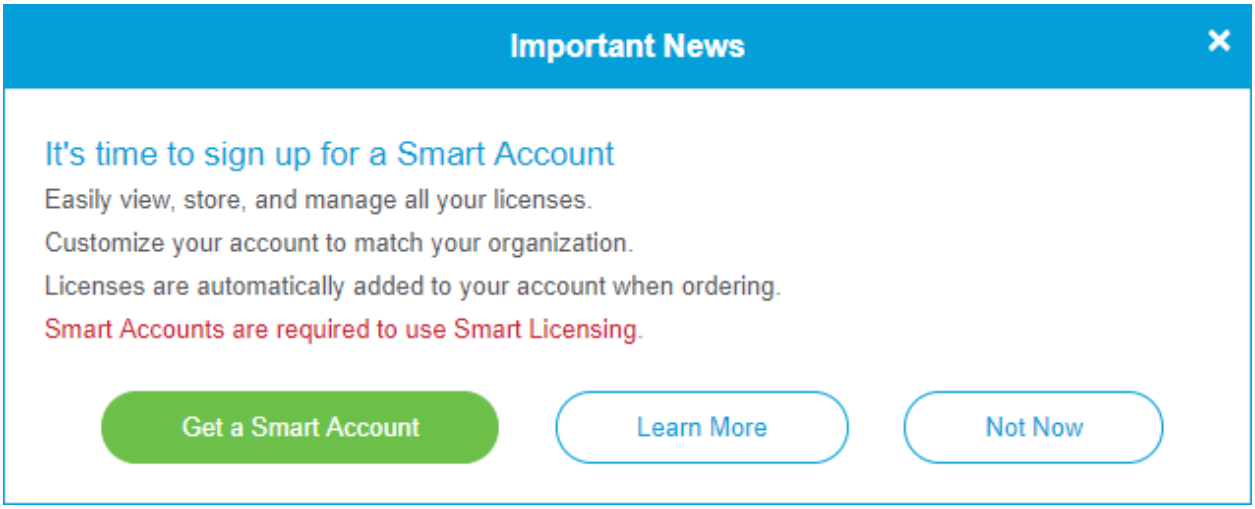
要购买RV安全许可证，您需要智能帐户。

通过授权激活此智能帐户，您同意您有权代表您的组织创建帐户并管理产品和服务授权、许可协议以及帐户的用户访问。思科合作伙伴不得代表客户授权创建帐户。

新智能帐户的创建是一次性事件，从那时起，通过工具提供管理。

创建智能帐户

当您使用您的Cisco.com帐户或CCO ID（您在本文档开头创建的ID）访问您的一般思科帐户时，您可能会收到创建智能帐户的消息。



如果您尚未看到此弹出窗口，可以单击进入“智能帐户**创建”页面**。您可能需要使用Cisco.com帐户凭证登录。

有关申请智能帐户涉及的步骤的其他详细信息，请单**击此处**。

请务必记下您的帐户名称以及其他注册详细信息。

快速提示：如果需要输入域，但您没有域，则可以以name@domain.com的形式输入您的电子邮*件地址*。常见域包括gmail、yahoo等，具体取决于您的公司或提供商。

在购买RV安全许可证之前，您必须拥有Cisco.com(CCO ID)帐户和思科智能帐户。

购买RV安全许可证

您必须从思科总代理商或思科合作伙伴处购买许可证。要查找思科合作伙伴，请点**击此处**。

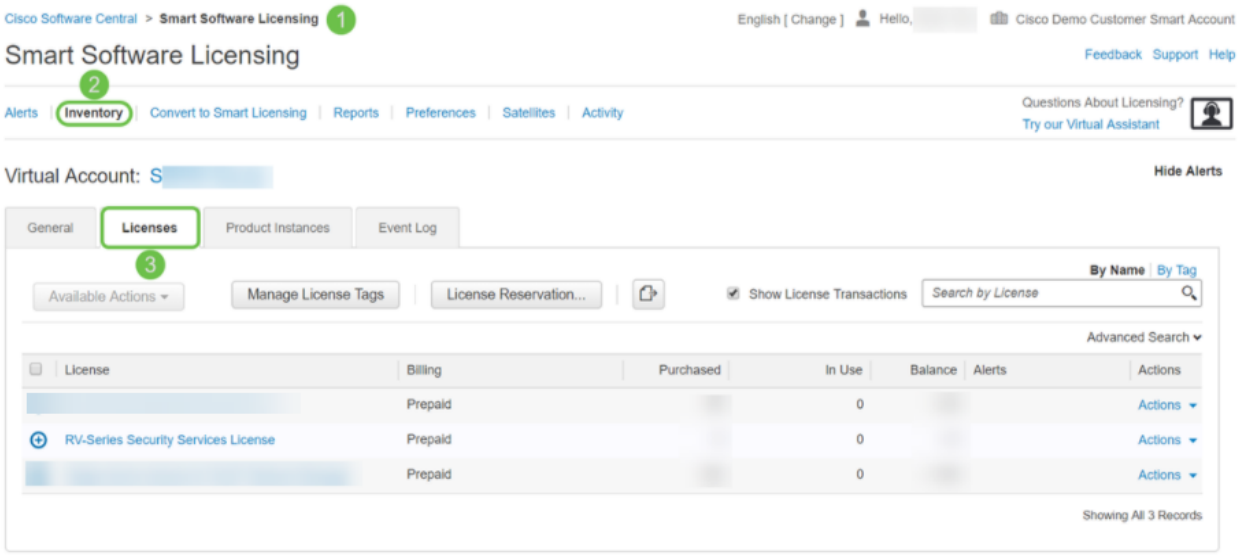
下表显示许可证的部件号。

类型	Product ID	描述
RV安全许可证	LS-RV34X-SEC-1YR=	RV安全：1 年:动态网络过滤器、应用可视性、客户端识别和统计、网御系统IPS。

许可证密钥不是直接输入到您的路由器中，但在您订购许可证后，将分配给您的思科智能帐户。许可证在您的帐户上显示所需的时间量取决于合作伙伴何时接受订单以及经销商将许可证链接到您的帐户的时间，通常为24-48小时。

确认许可证在智能帐户中

导航至您的智能许可证帐户页面，然后点击智**能软件许可证页面>资产>许可证**。

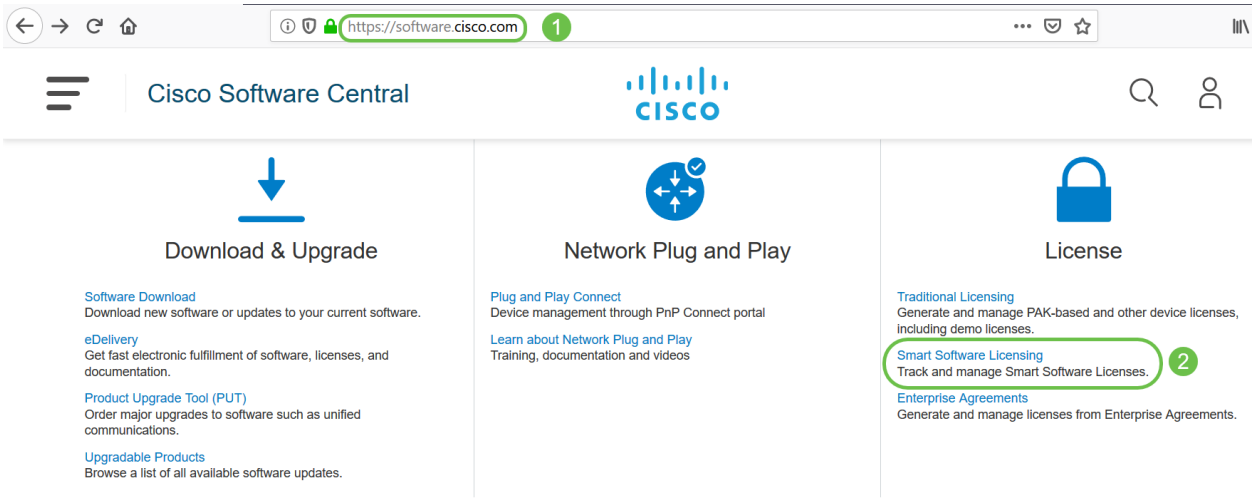


如果您在智能帐户中未看到许可证，请联系您的思科合作伙伴。

在RV345P系列路由器上配置RV安全许可证

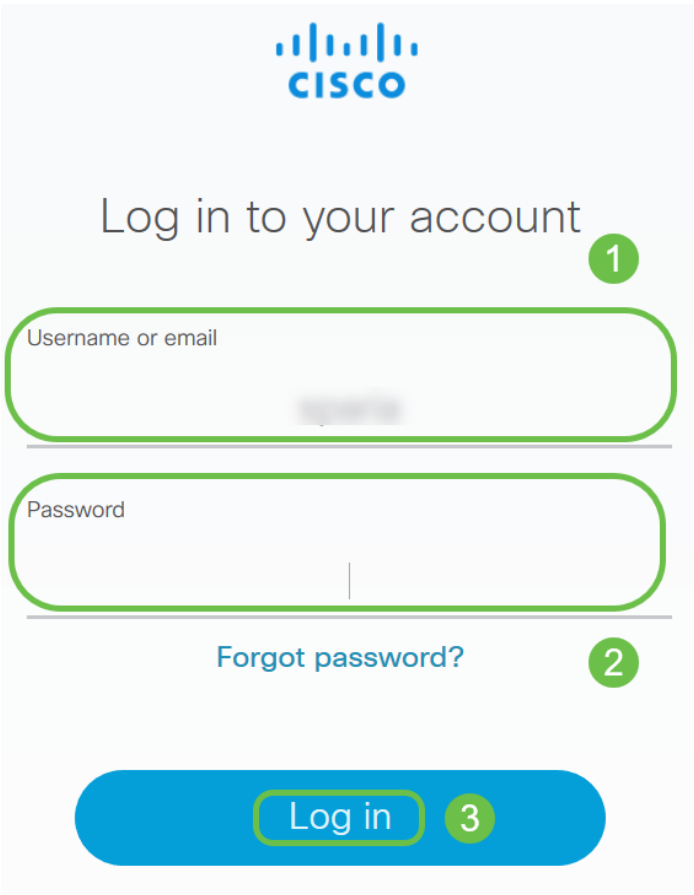
第 1 步

访问思科软件并导航至**智能软件许可**。



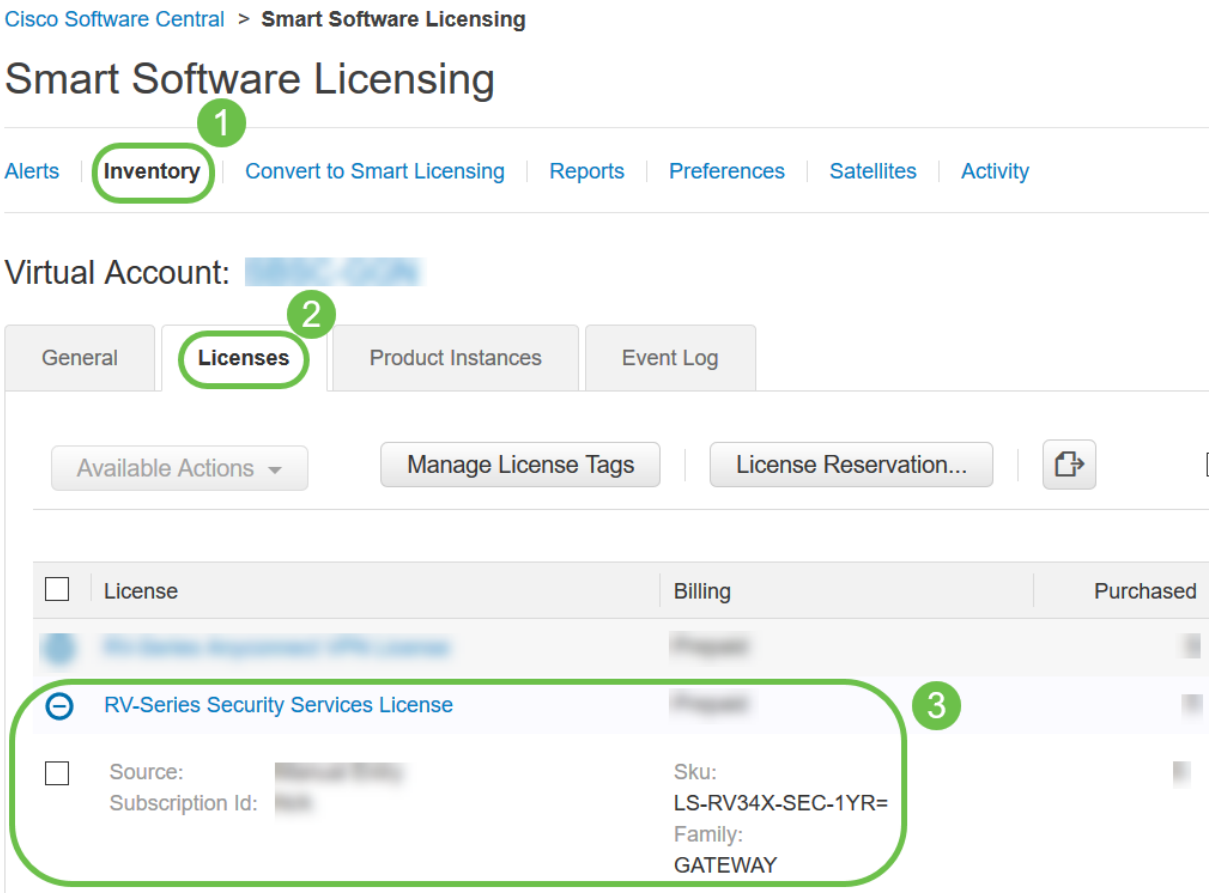
步骤 2

输入您*的用户名*或电*子邮*件和密码以登录智能帐户。单击**Log in**。



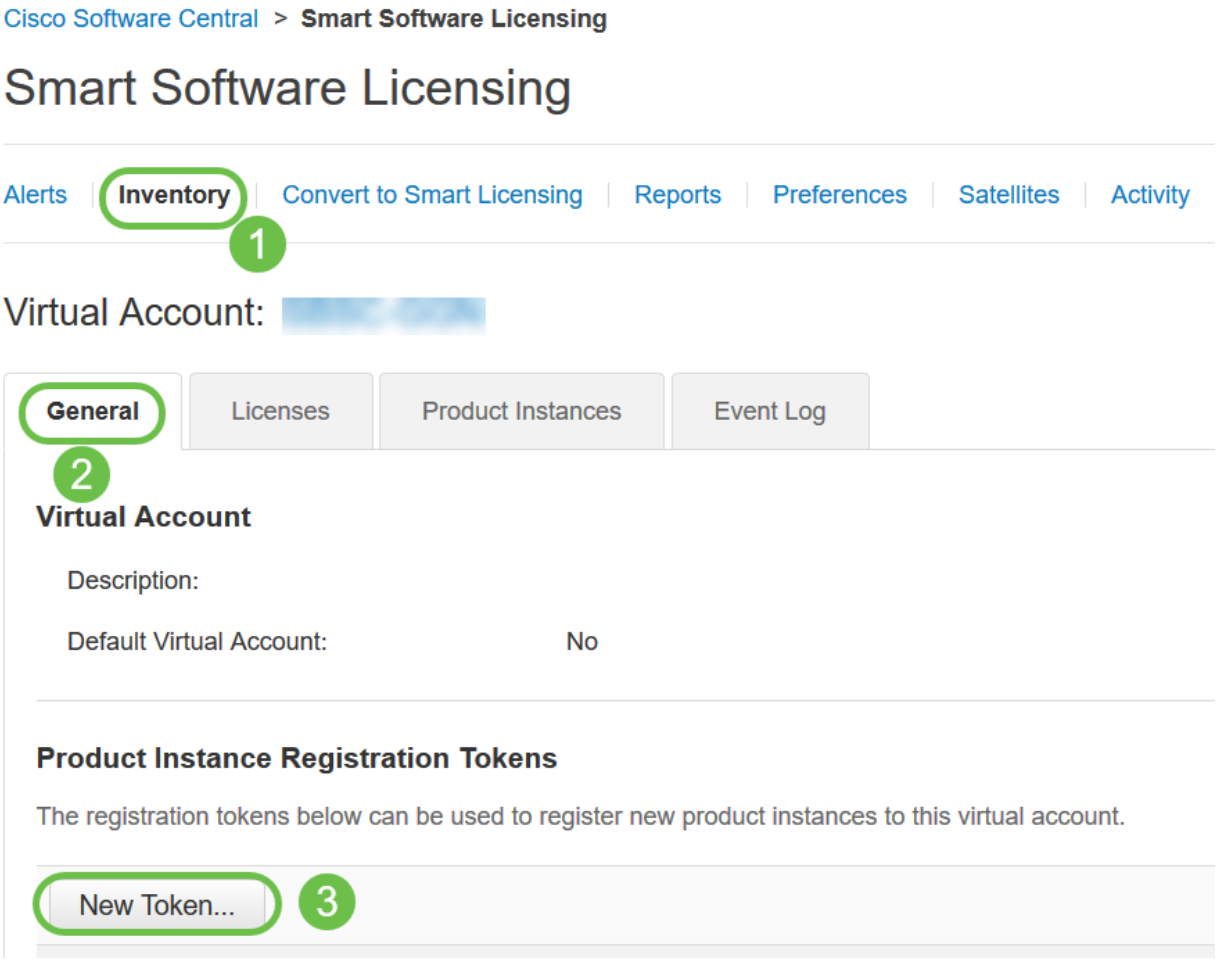
步骤 3

导航至**Inventory > Licenses**，并验证RV系*列安全服务许可证*是否列在您的智能帐户上。如果您未看到所列的许可证，请联系您的思科合作伙伴。



步骤 4

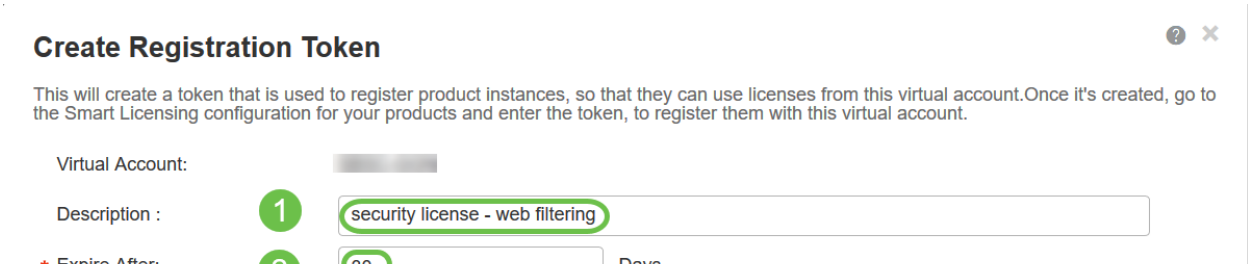
导航至“**库存**”>“**常规**”。在“*产品实例注册令牌*”下，单击“**新建令牌**”。



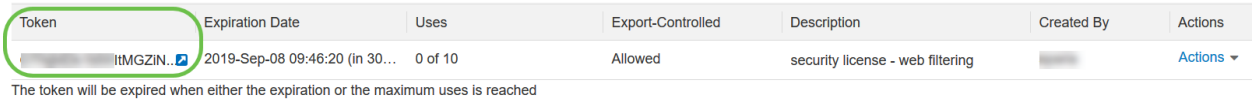
步骤 5

系统将显示“创建注册令牌”窗口。“*虚拟帐户*”区域显示将在其上创建注册令牌的虚拟帐户。在“创*建注册令*牌”页上，完成以下操作：

- 在“说明”字段中，输入令牌的唯一说明。在本例中，输入安全许可证 — 网络过滤。
- 在Expire After字段中，输入介于1至365天之间的值。思科建议此字段的值为30天；但是，您可以根据需要编辑值。
- 最大“使用次数”字段输入一个值以定义要使用该令牌的次数。当达到天数或最大使用次数时，令牌将过期。
- 选中Allow export-controlled fonuctionals on the products registered with this token复选框，以启用虚拟帐户中产品实例的令牌的导出控制功能。如果您不想允许导出控制功能可用于此令牌，请取消选中此复选框。仅当您符合导出控制功能时才使用此选项。某些出口控制功能受美国商务部限制。取消选中此复选框时，这些功能仅适用于使用此令牌注册的产品。违反规定的，应当给予处罚和行政处分。
- 单击**创建**令牌以生成令牌。

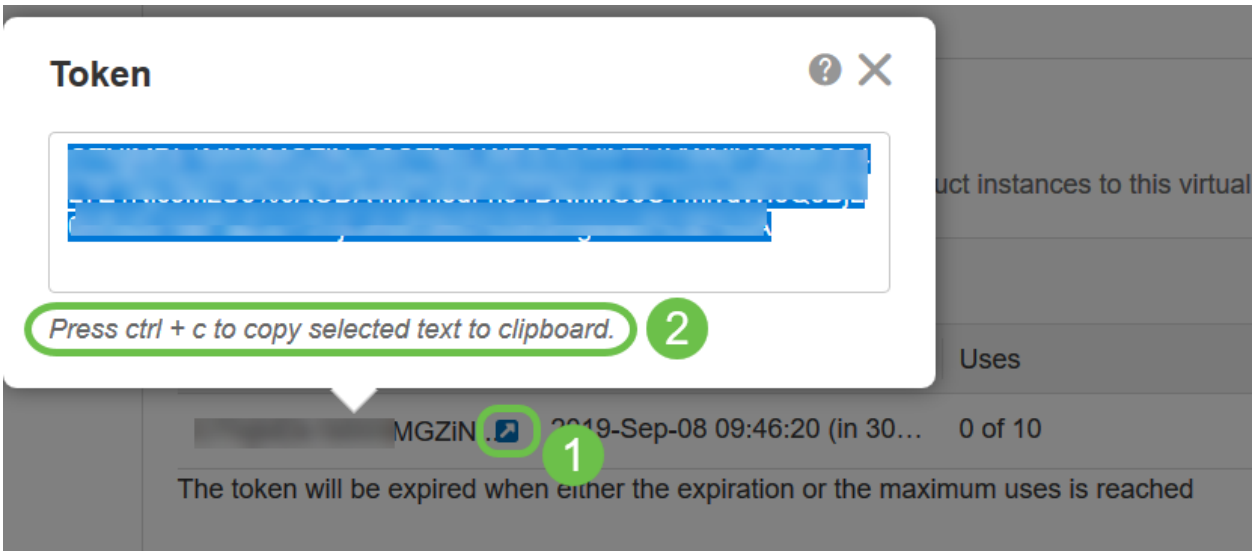


您现在已成功生成产品实例注册令牌。



步骤 6

单击“**令牌**”列中的箭*头图标*，将令牌复制到剪贴板，然后按键**盘上的ctrl** + c。

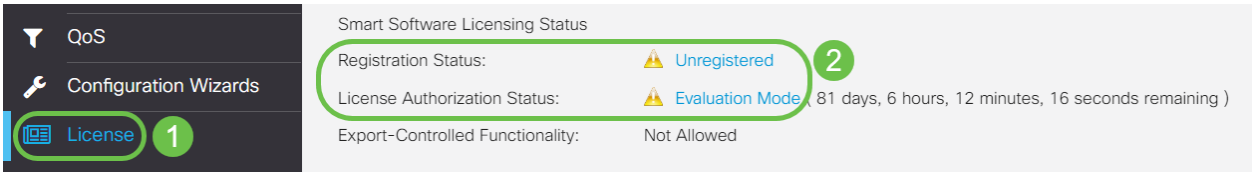


步骤 7（可选）

单击**Actions**下拉**菜单**，选择**Copy**将令牌复制到剪贴板，或选择**Download...**以下载可从中复制的令牌的文本文件副本。

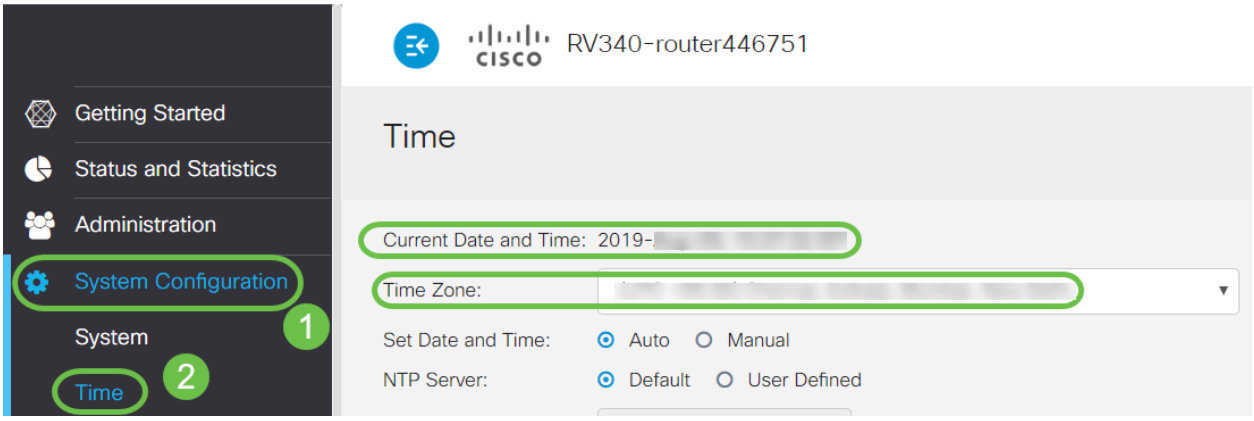
步骤 8

导航至“许可证”并*验证*“*注*册状态”是否显*示*为“未注册”，“许可证授权状态”是否显示为“评估模*式*”。



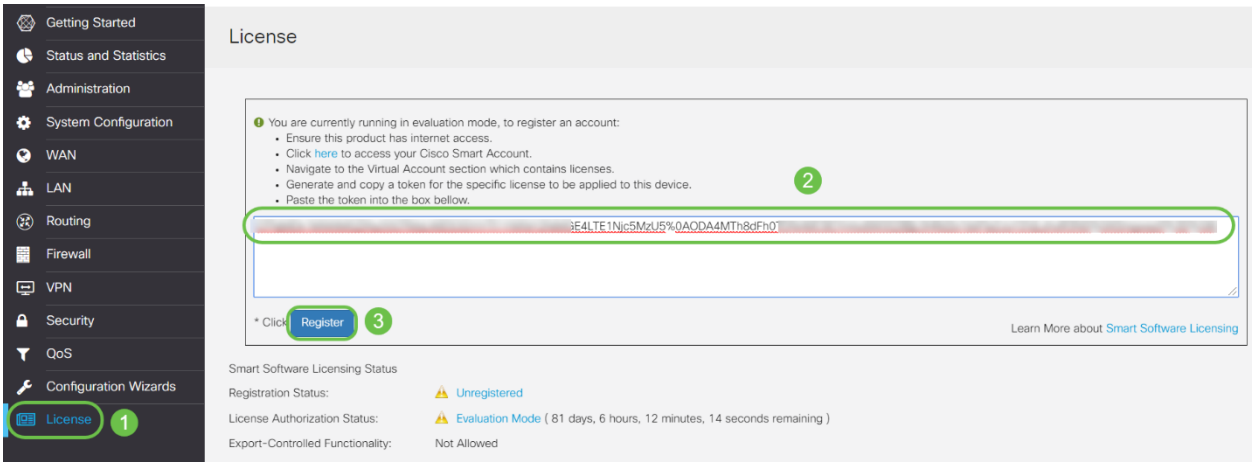
步骤 9

导航至**系统配置>时**间，并验证*当前日期和时*间*和时区*是否*正确反映*了您的时区。



步骤 10

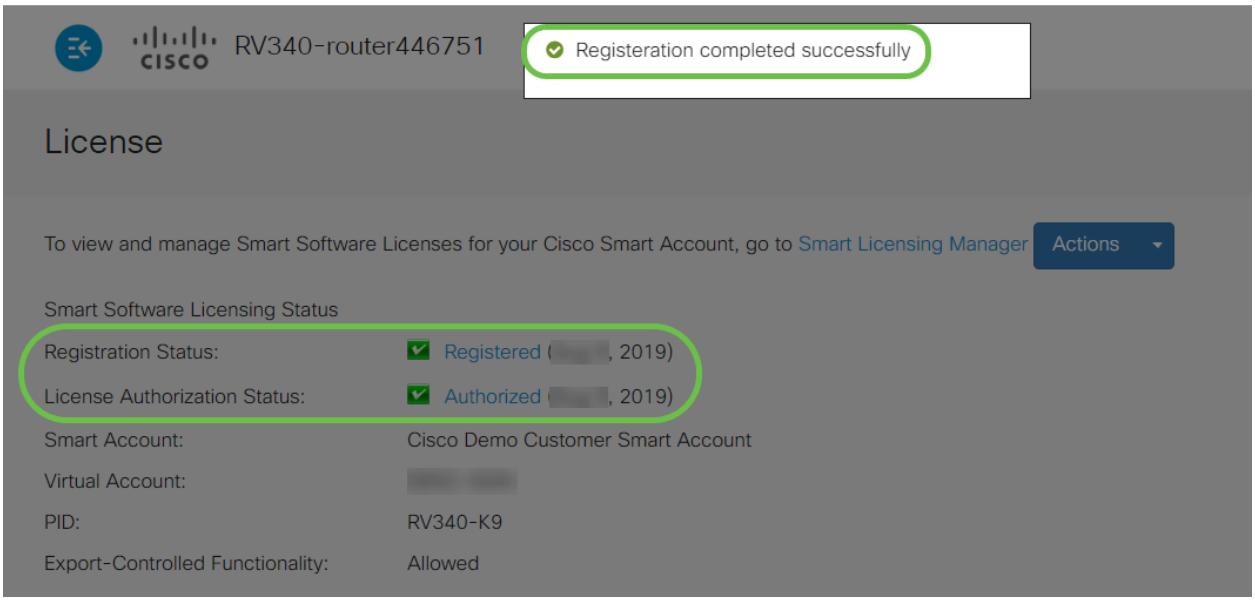
导航至**许可证**。在键盘上选择ctrl + v，将复制的令牌粘贴到"许*可证*"选项卡下**的文本**框中的步骤6。单击"**Register(注册)**"。



注册可能需要几分钟。请勿在路由器尝试联系许可证服务器时离开该页面。

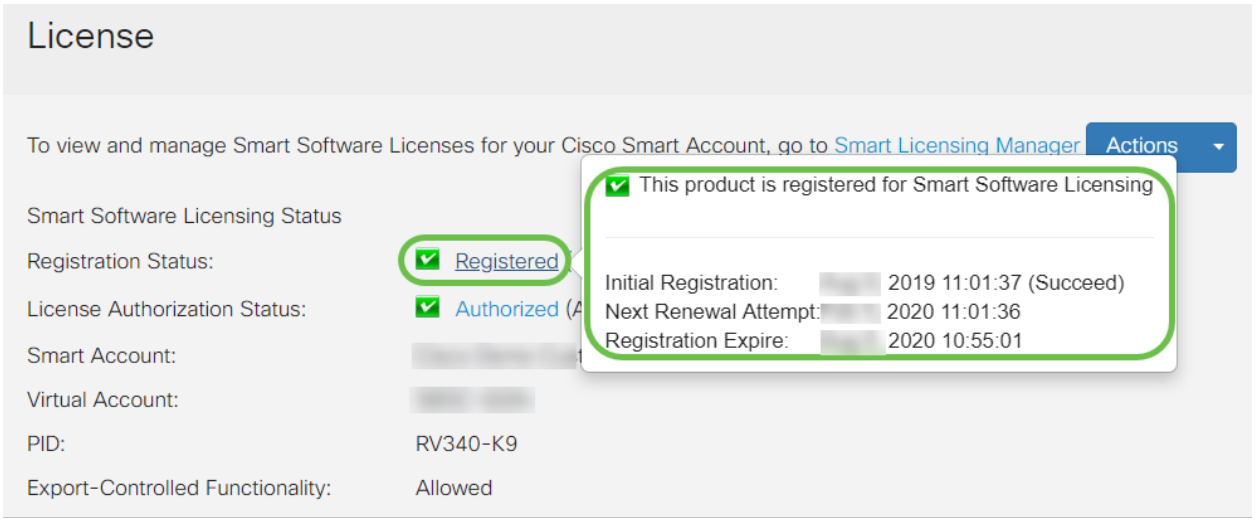
步骤 11

您现在应该已使用智能许可证成功注册并授权RV345P系列路由器。您将在屏幕上收到通知注册*成功完成*。此外，您还可以看到注册状*态显*示为*已注册*,*许可证授权状*态显示为*Authorized*。



步骤 12（可选）

要查看许可证的注册状*态的更*多详细信息，请将指针悬停在注册状*态上*方。系统将显示一条对话框消息，其中包含以下信息：

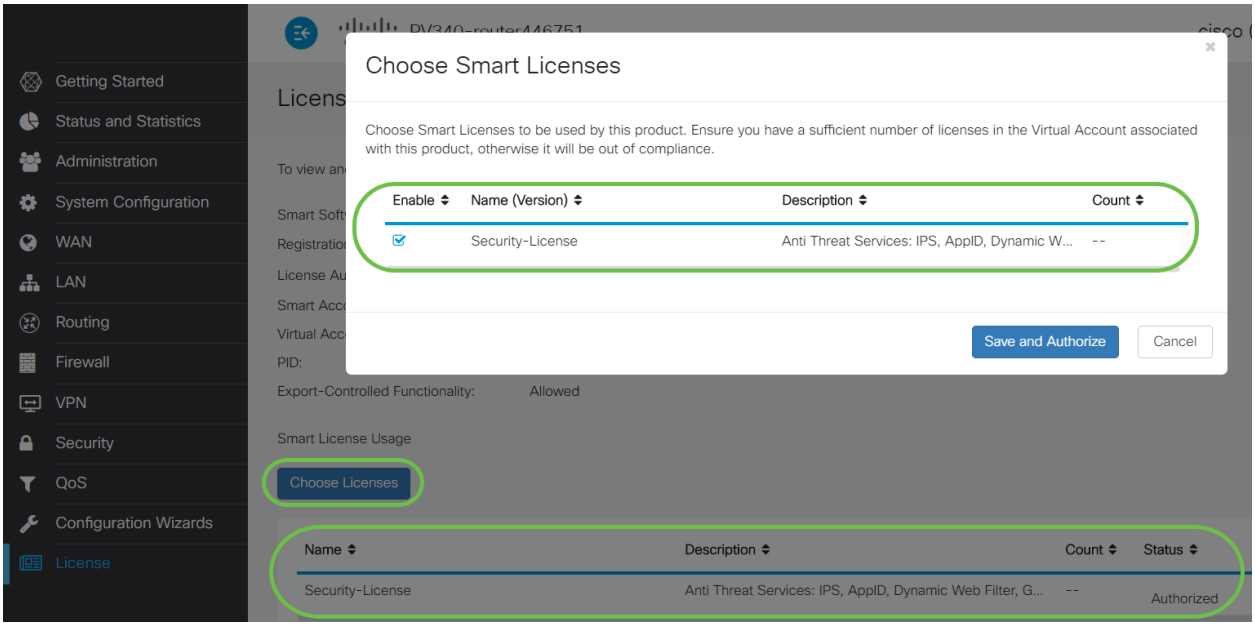


- 初始注册 — 此区域表示注册许可证的日期和时间。
- Next Renewal Attempt — 此区域指示路由器尝试续订许可证的日期和时间。
- Registration Expire — 此区域指示注册到期的日期和时间。

步骤 13

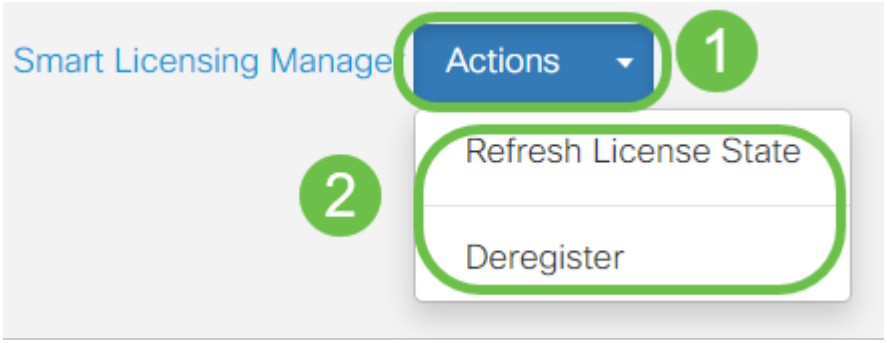
在“许*可证*”页面上，验*证“安全许*可证”状态是*“授权”*。您还可以单击“Choose License(选**择许可证)**”按钮以验*证“Security-License*（安全许可证）”是否已启用。

如果在此步骤中遇到任何问题，可能需要重新启动路由器。



步骤 14（可选）

要刷*新许可证状*态或*从路*由器注销许可证，请单击*智能许可管理器操作*下拉菜单，然后选择一个措施项。



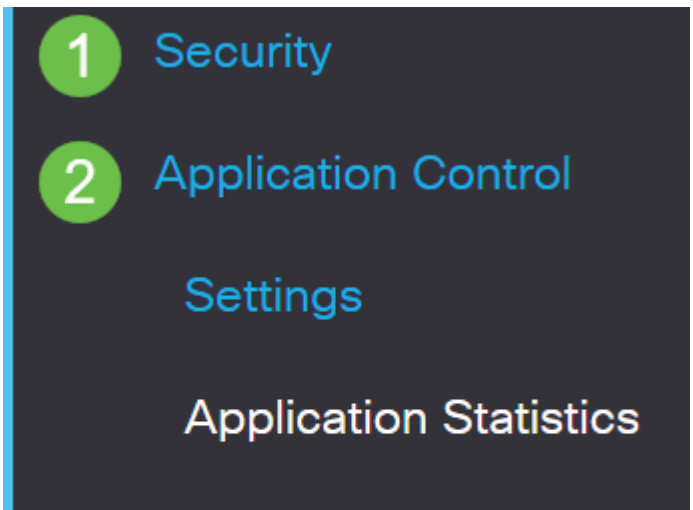
现在，您的许可证已在路由器上，您需要完成下一节中的步骤。

RV345P路由器上的Web过滤

激活后90天，您可以免费使用网络过滤。免费试用后，如果您想继续使用此功能，则需要购买许可证。[单击返回该部分。]

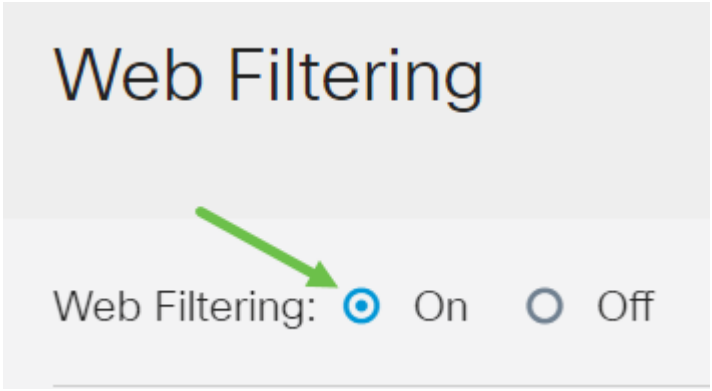
第 1 步

登录到基于Web的实用程序，然后选择**Security > Application Control > Web Filtering**。



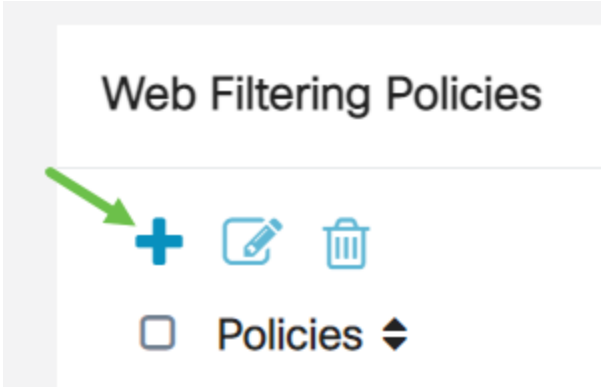
步骤 2

选择“On”单选按钮。



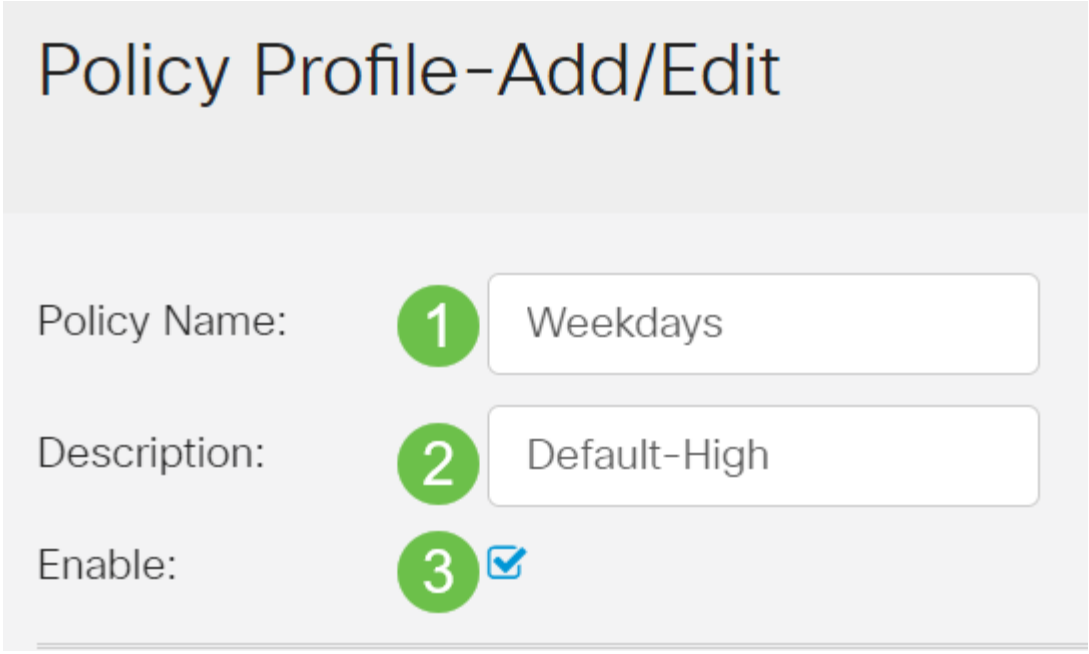
步骤 3

单击“添**加”图标**。



步骤 4

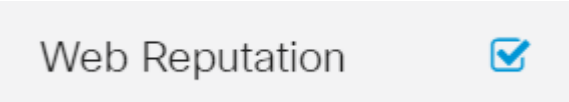
输入策*略名称*、*说明*和*启用*复选框。



如果您的路由器上启用了内容过滤，则会显示一条通知，通知您内容过滤已禁用，并且无法同时启用这两项功能。单击 **Apply**继续配置。

步骤 5

选中Web Reputation复选框以启用基于Web信誉索引的过滤。

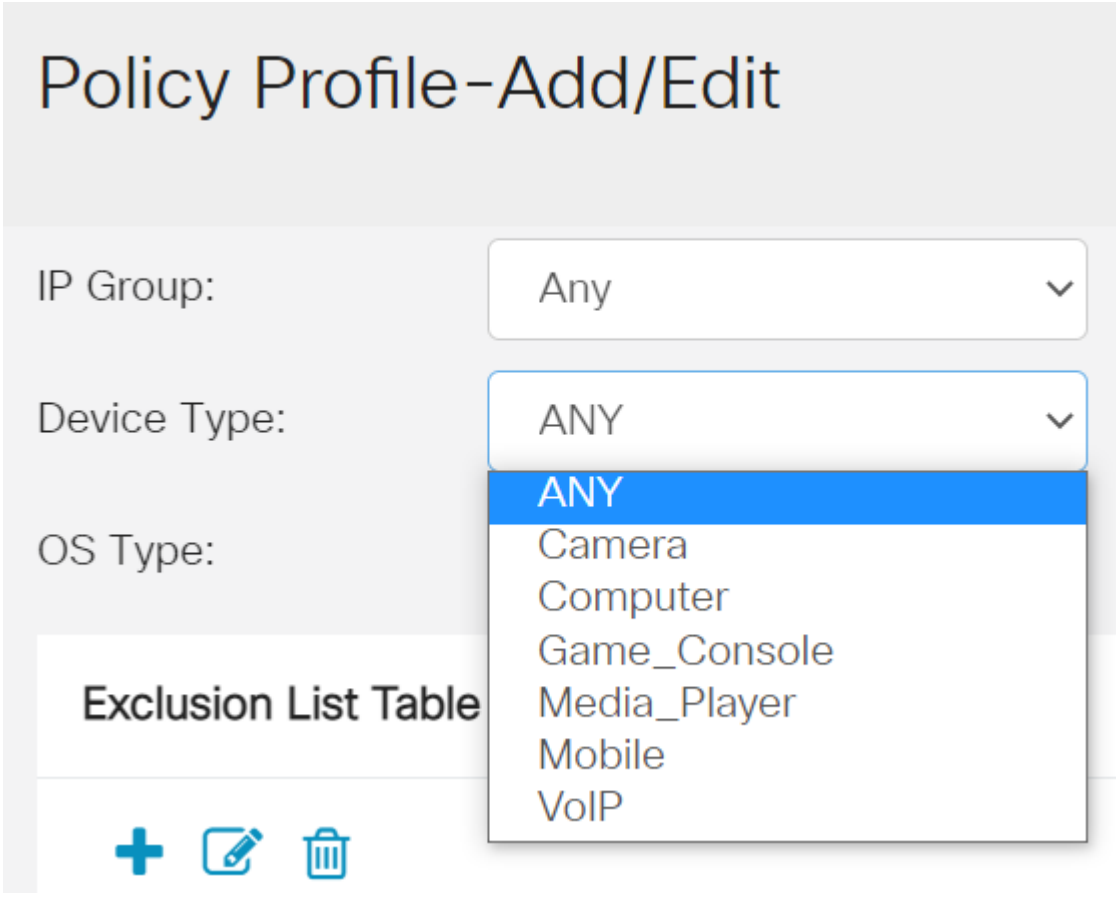


内容将根据网站或URL的恶名根据Web信誉索引进行过滤。如果分数低于40分，网站将被屏蔽。要了解有关Web信誉技术的详细信息，请 单击此处了解详细信息。

步骤 6

从*Device Type*下拉列表中，选择要过滤的数据包的源/目标。一次只能选择一个选项。选项有：

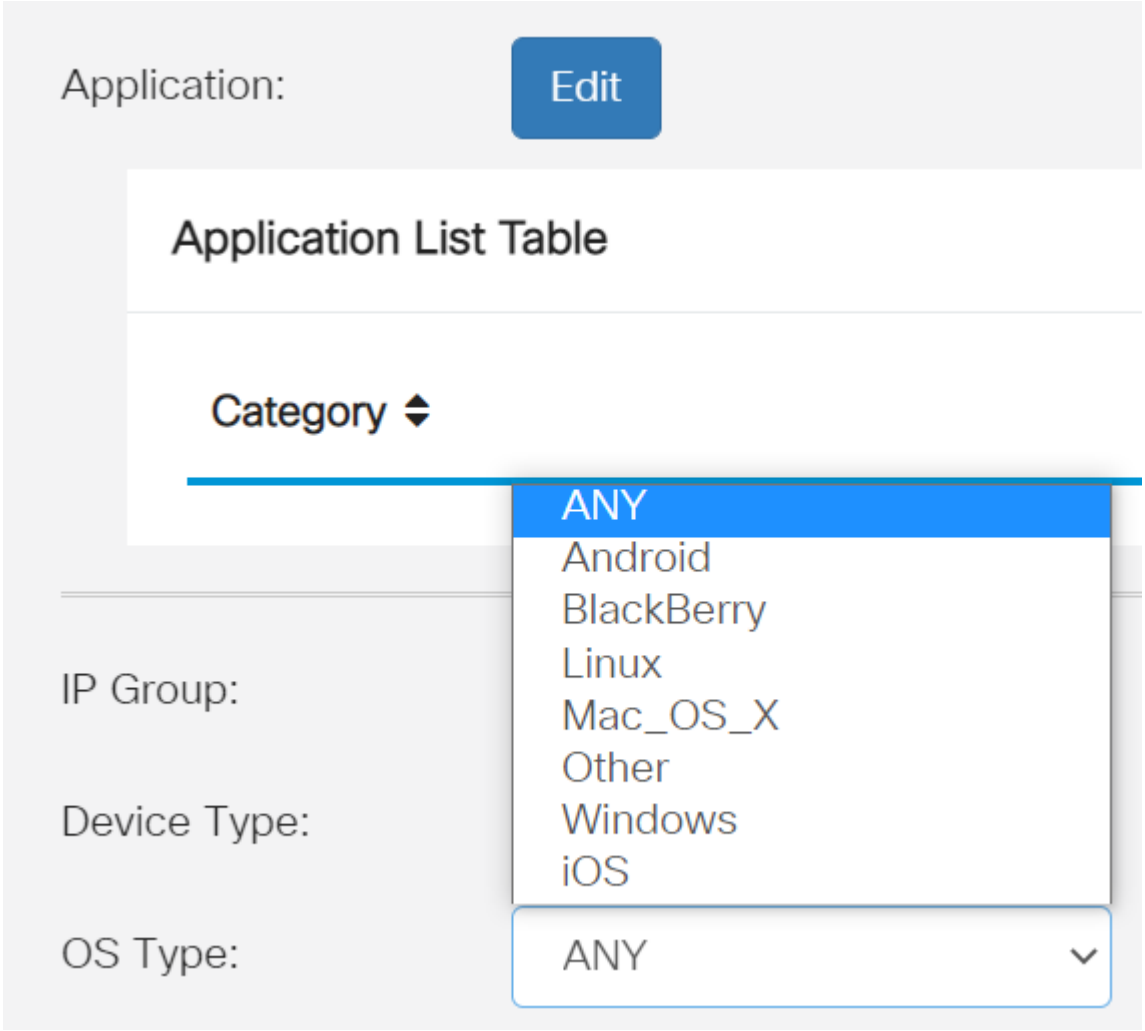
- ANY — 选择此选项可将策略应用于任何设备。
- 摄像头 — 选择此选项可将策略应用于摄像头（例如IP安全摄像头）。
- 计算机 — 选择此选项可将策略应用于计算机。
- Game_Console — 选择此选项可将策略应用于游戏机。
- Media_Player — 选择此选项可将策略应用于媒体播放器。
- 移动 — 选择此选项可将策略应用于移动设备。
- VoIP — 选择此选项可将策略应用于Voice over Internet Protocol设备。



步骤 7

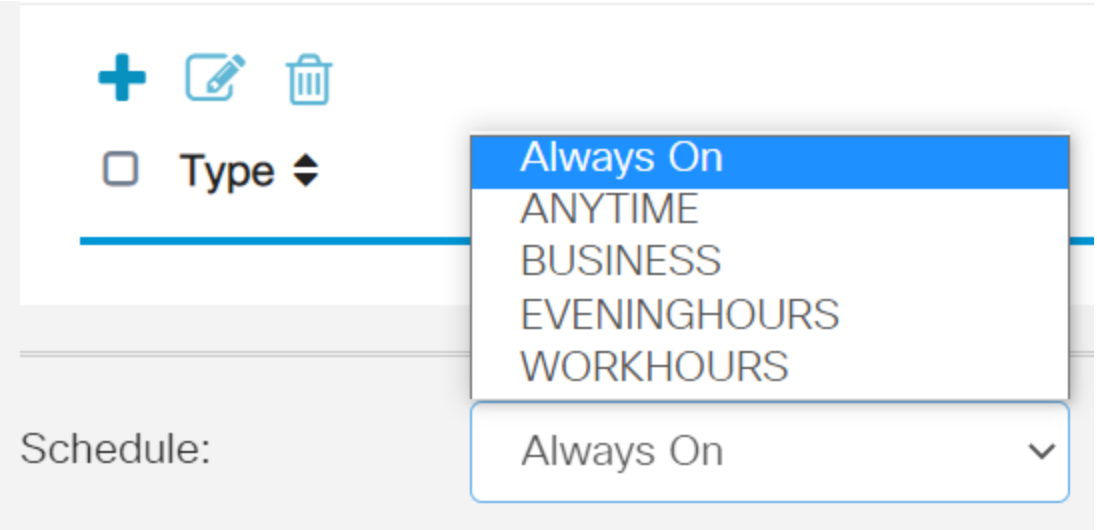
从OS *Type*下拉列表中，*选择策略应适用的操作系统(OS)*。一次只能选择一个选项。选项有：

- ANY — 将策略应用于任何类型的操作系统。这是默认设置。
- Android — 仅将策略应用于Android操作系统。
- BlackBerry — 仅将策略应用于Blackberry OS。
- Linux — 仅将策略应用于Linux操作系统。
- Mac_OS_X — 仅将策略应用于Mac OS。
- 其他 — 将策略应用于未列出的操作系统。
- Windows — 将策略应用于Windows操作系统。
- iOS — 仅将策略应用于iOS OS。



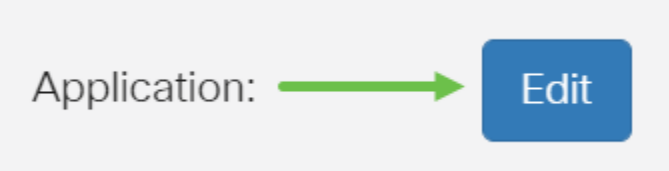
步骤 8

向下滚动到“计*划*”部分，并选择最符合您需求的选项。



步骤 9

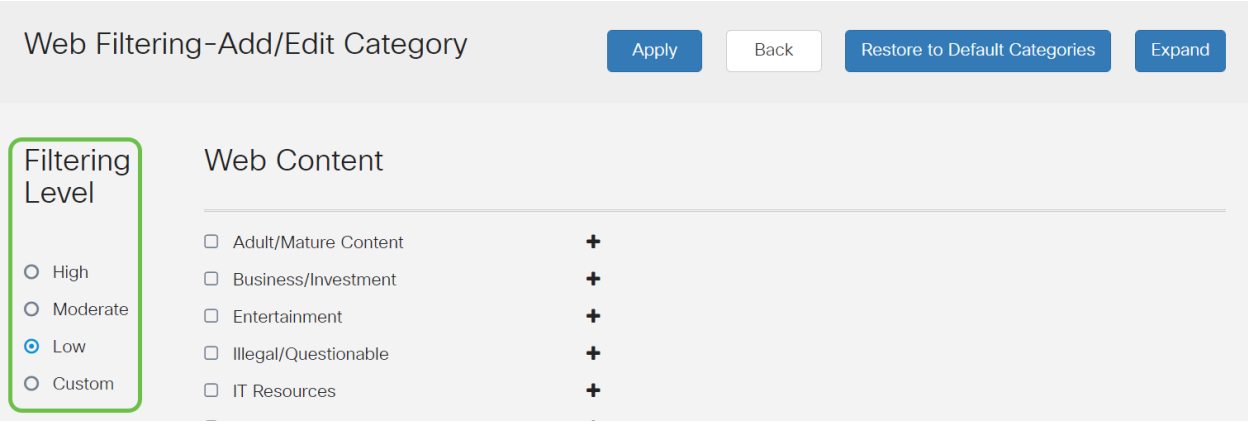
单击编辑图标。



步骤 10

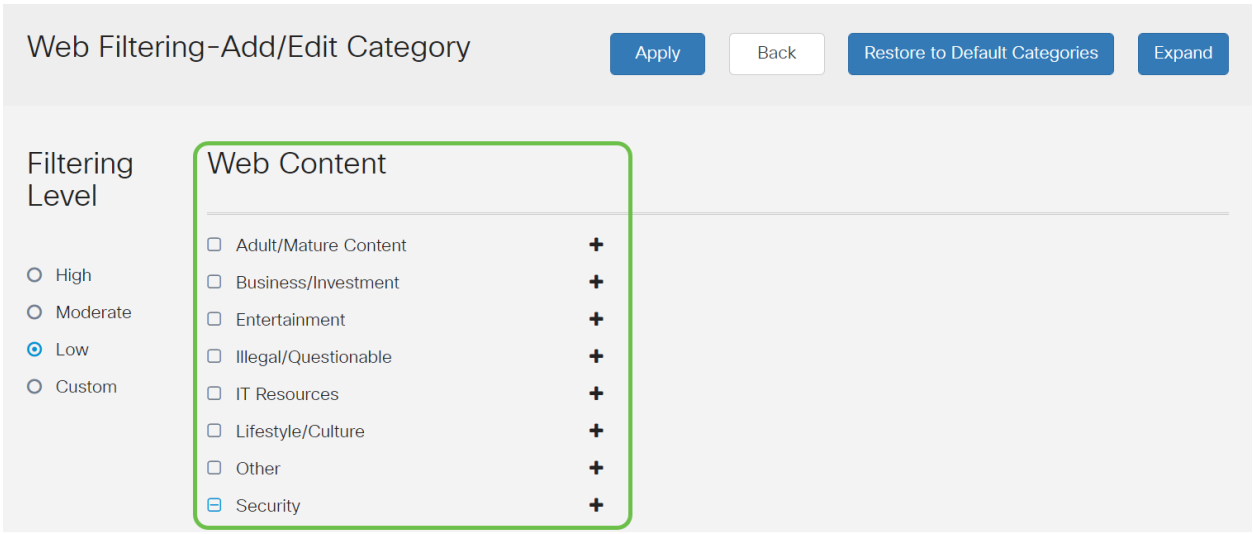
在过滤级别(Filtering Level)列中，点击单选按钮以快速定义最适合网络策略的过滤范围。选项有High、Medore、Low和Custom。点击以下任何过滤级别，了解已过滤到其每个已启用的Web内容类别的特定预定义子类别。预定义的过滤器不能再被更改，并且灰显。

- 低 — 这是默认选项。此选项启用了安全性。
- 中度 — 使用此选项启用成人/成熟内容、非法/可疑和安全。
- 高 — 使用此选项可启用成人/成熟内容、业务/投资、非法/可疑、IT资源和安全。
- 自定义 — 未设置任何默认值以允许用户定义的过滤器。



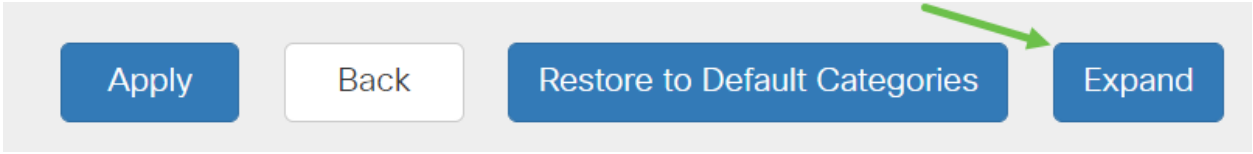
步骤 11

输入要过滤的Web内容。如果要详细了解一个部分，请单击加号图标。



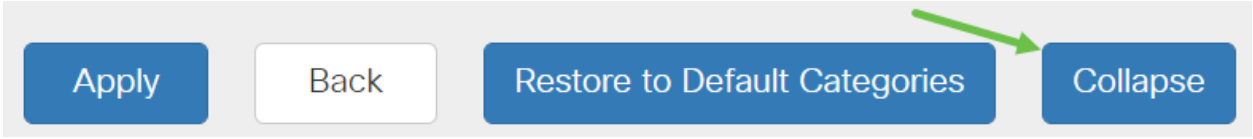
步骤 12（可选）

要查看所有Web内容子类别和说明，可单击“展开”**按钮**。



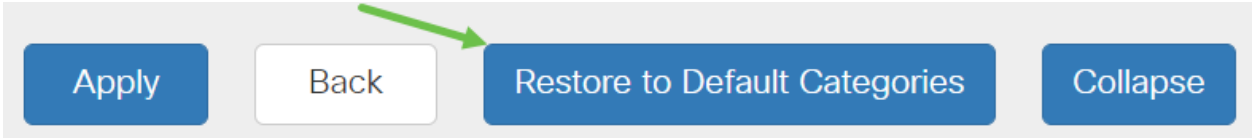
步骤 13（可选）

单击**折叠**可折叠子类别和说明。



步骤 14（可选）

要返回默认类别，请单击“恢**复为默认类别**”。



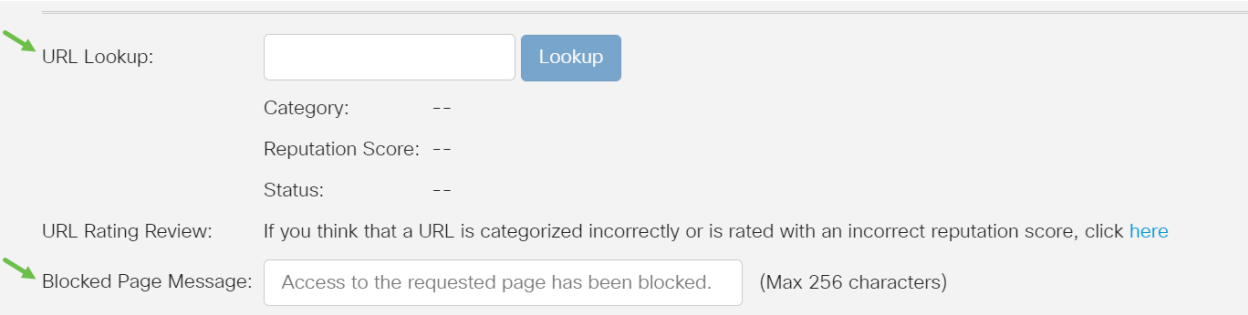
步骤 15

单击**Apply**保存配置并返回到Filter页以继续设置。

在应用列表表中，基于所选过滤级别的相应子类别将填充该表。

步骤 16（可选）

其他选项包括URL查找和当请求的页面被阻止时显示的消息。



步骤 17（可选）

单击 Apply。

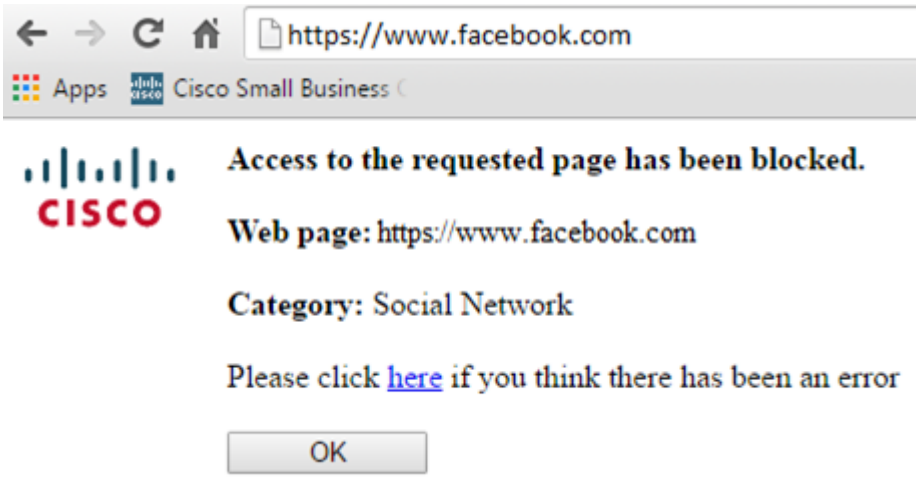
步骤 18

要永久保存配置，请转至“*复制/保存配*置”页，或**单击**页面上部的保存图标。

步骤 19（可选）

要验证网站或URL是否已过滤或阻止，请启动Web浏览器或在浏览器中打开新选项卡。输入已列出阻止或已过滤为阻止或拒绝的域名。

在本例中，我们使用www.facebook.com。



现在，您应该已在RV345P路由器上成功配置了Web过滤。由于您使用RV安全许可证进行网络过滤，因此可能不需要Umbrella。如果还需要Umbrella，请单击此处。如果您有足够的安全性，请单击跳至下一节。

故障排除

如果您购买了许可证，但该许可证未显示在虚拟帐户中，则您有两个选项：

1. 跟进经销商，要求他们进行转让。
2. 联系我们，我们将与经销商联系。

理想情况下，您也不必这样做，但如果您到达这条十字路口，我们很乐意提供帮助！要使流程尽可能方便，您需要上表中的凭证以及下面列出的凭证。

所需信息	查找信息
许可证发票	在完成许可证购买后，应通过电子邮件将此信息发送给您。
思科销售订单编号	您可能需要返回经销商获取此信息。
智能帐户许可证页面的截图	截图将捕获屏幕内容，以便与我们的团队共享。如果您不熟悉屏幕截图，可以使

屏幕截图

一旦您有了令牌，或者您正在进行故障排除，建议您截取屏幕内容。

鉴于捕获屏幕截图所需过程的不同，请参阅下文，了解特定于您的操作系统的链接。

- Windows 窗口版本
- MAC
- iPhone/iPad
- Android

Umbrella RV分支机构许可证（可选）

Umbrella是思科简单而高效的云安全平台。

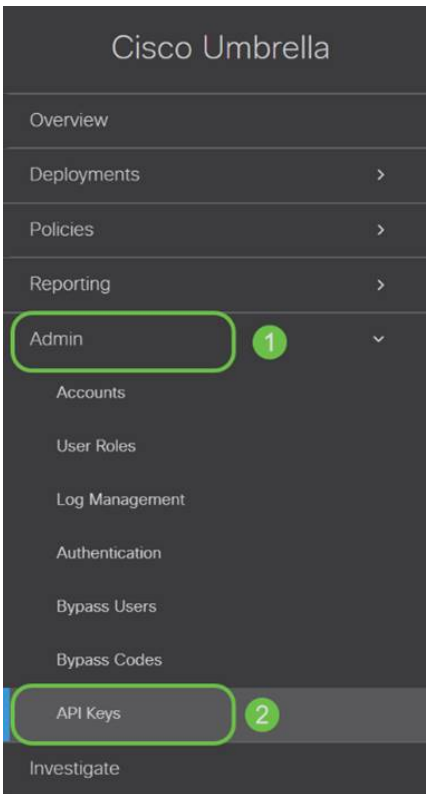
Umbrella在云中运行，并执行许多与安全相关的服务。从紧急威胁到事后调查。Umbrella发现并防止所有端口和协议上的攻击。

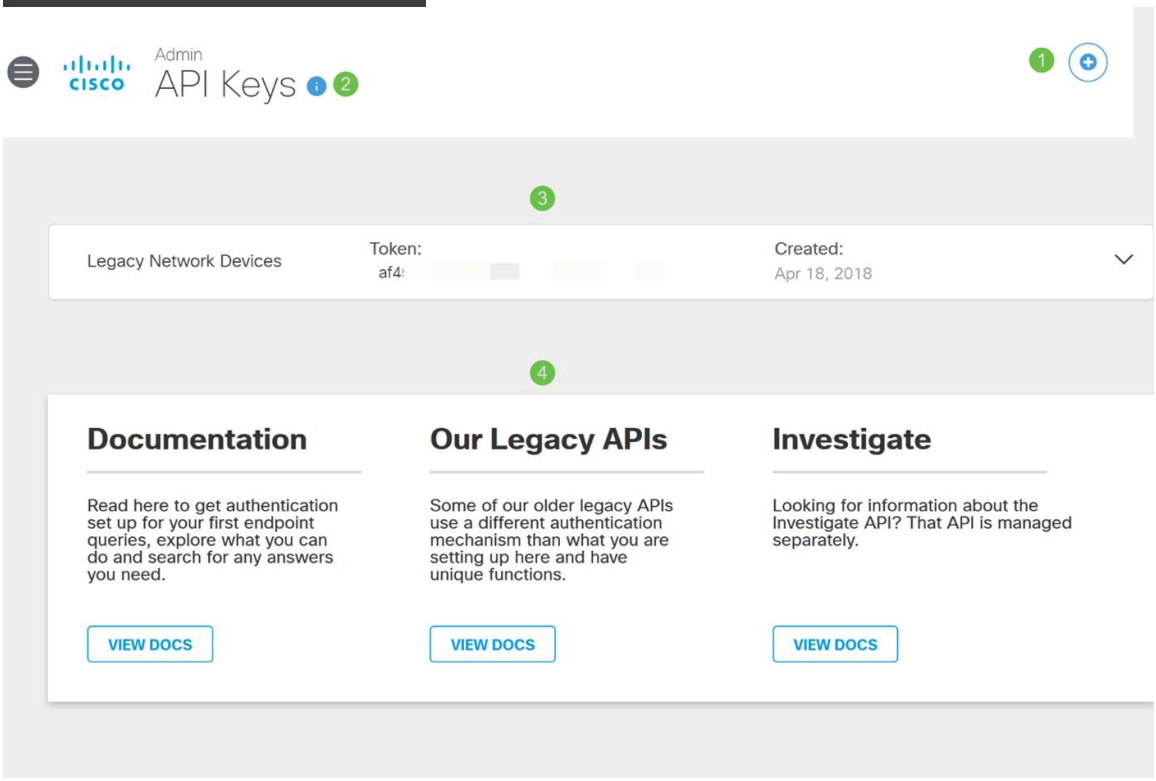
Umbrella使用DNS作为防御的主要媒介。当用户在其浏览器栏中输入URL并按*Enter*时，Umbrella将参与传输。该URL将传递到Umbrella的DNS解析器，如果安全警告与域关联，则会阻止请求。此遥测数据传输并以微秒为单位进行分析，几乎不会增加延迟。遥测数据使用日志和仪器跟踪全球数十亿个DNS请求。当此数据无处不在时，将其关联到全球，可在攻击开始时快速响应。有关详细信息，请参阅思科的隐私政策：完整策略、摘要版本。将遥测数据视为从工具和日志派生的数据。

请访问Cisco Umbrella了解详情并创建帐户。如果遇到任何问题，请查看此处获取文档，并查看此处获取Umbrella Support选项。

第 1 步

登录Umbrella帐户后，从Dashboard屏幕*单击*Admin > **API Keys**。



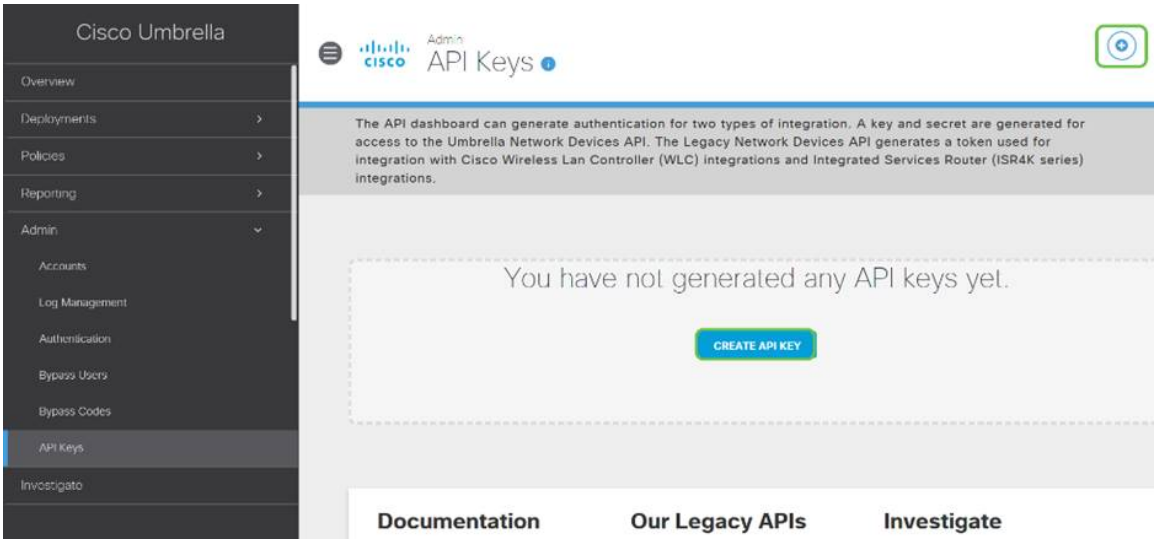


API密钥屏幕剖析（使用预先存在的API密钥）

1. 添加API密钥 — 启动新密钥的创建，以便与Umbrella API一起使用。
2. 其他信息 — 向下/向上滑动，其中包含此屏幕的说明者。
3. 令牌好 — 包含此帐户创建的所有密钥和令牌。（创建密钥后填充）
4. 支持文档 — 指向Umbrella站点上与每个部分的主题相关的文档的链接。

步骤 2

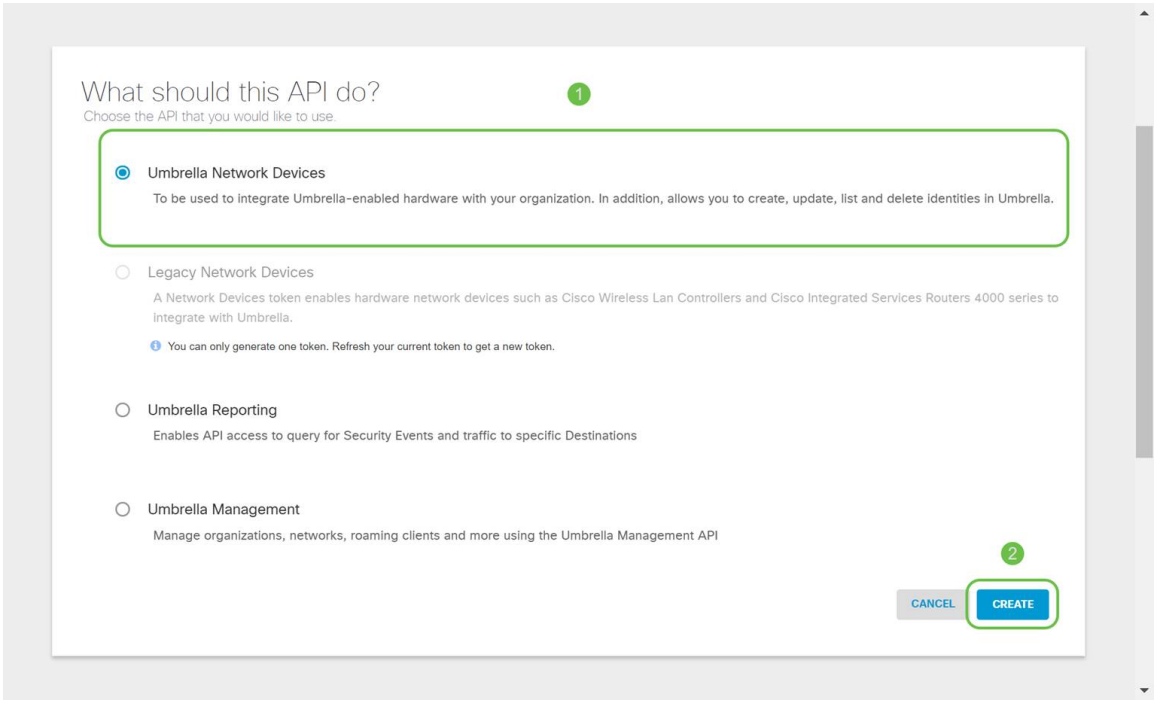
单击右上角**的Add API Key**（添加API密钥）按钮，或单击Create API Key(创**建API密钥)**按钮。它们的功能相同。



上面的屏幕截图类似于您第一次打开此菜单时看到的内容。

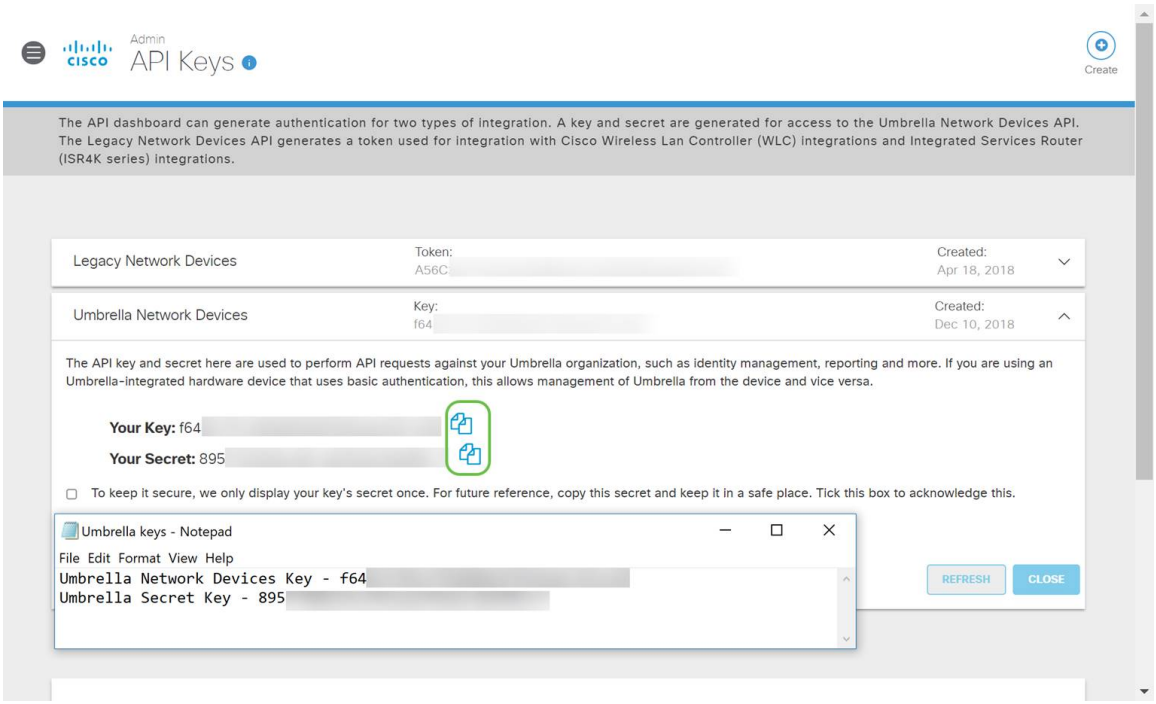
步骤 3

选择“**Umbrella Network Devices”**，然后单击“**Create**”按钮。



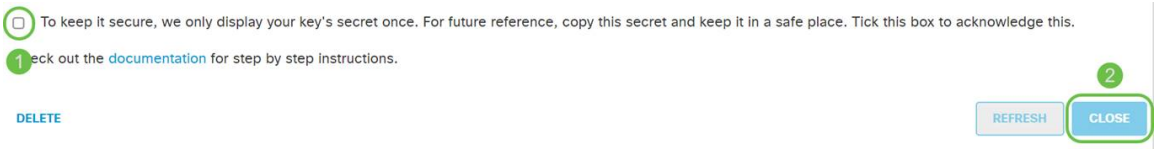
步骤 4

打开文本编辑器（如记事本），然**后单**击API和API密钥右侧的*复制图*标，弹出通知将确认密钥已复制到剪贴板。一次一个地将您的密钥和API密钥粘贴到文档中，标记它们以供将来参考。在本例中，其标签为“Umbrella网络设备密钥”。然后将文本文件保存到安全位置，以便稍后访问。



步骤 5

在将密钥和密钥复制到安全位置后，从*Umbrella API屏幕*单击**复选框**以确认完成对临时查看密钥的确认，然后单击**关闭**按钮。



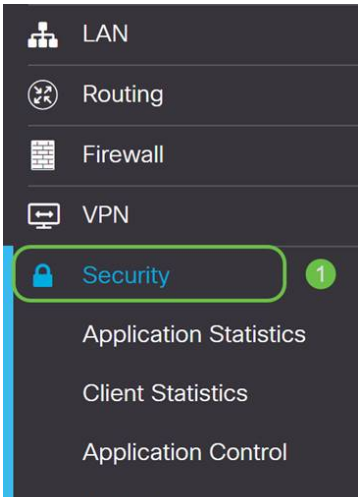
如果丢失或意外删除密钥，则没有功能或支持号码可供调用以检索此密钥。如果丢失，您需要删除密钥，并重新授权要使用Umbrella保护的每台设备的新API密钥。

在RV345P上配置Umbrella

现在，我们已在Umbrella中创建了API密钥，您可以获取这些密钥并将其安装到RV345P上。

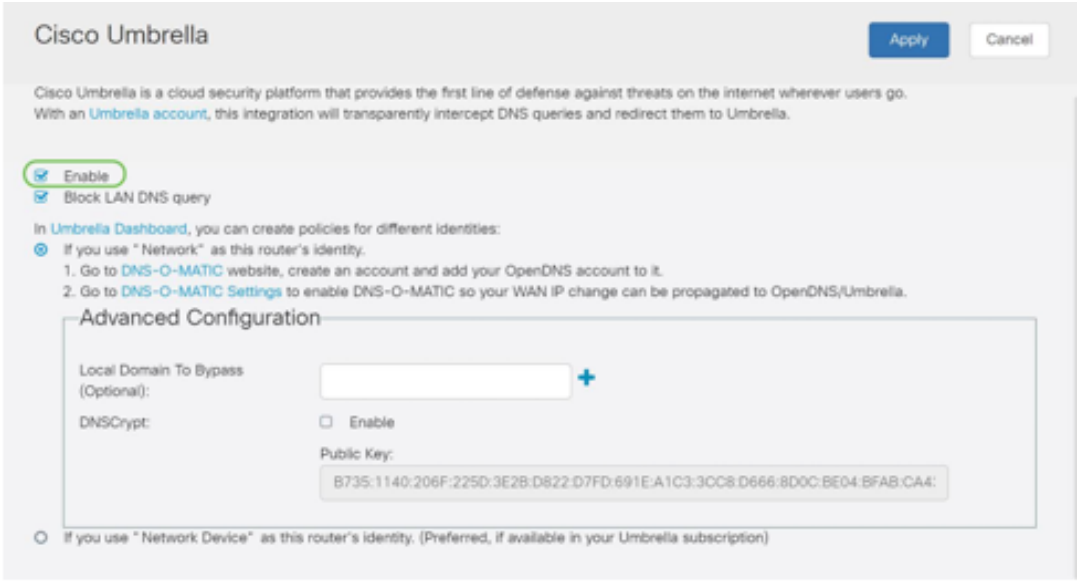
第 1 步

登录到RV345P路由器后，单击侧栏菜**单中的Security** > Umbrella。



步骤 2

Umbrella API屏幕有一系列选项，通过单击“启用”复选框开始启用Umbrella。

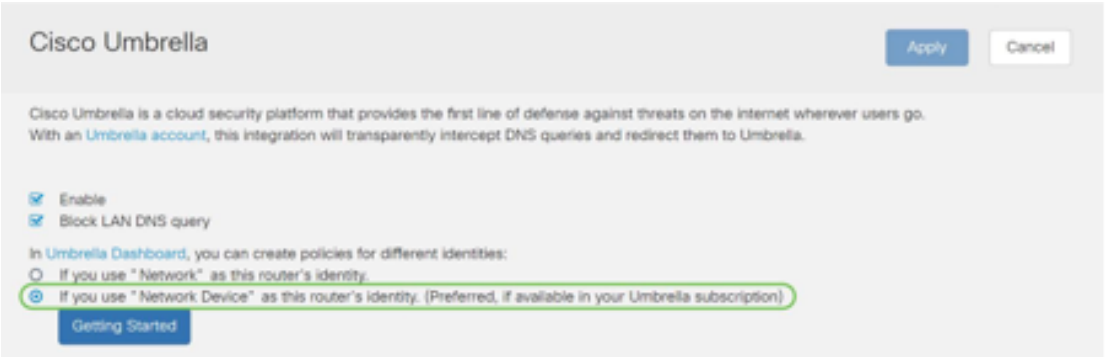


步骤 3（可选）

默认情况下，选中Block LAN *DNS Queries(阻止LAN DNS查*询)框。此简洁的功能会自动在您的路由器上创建访问控制列表，从而防止DNS流量流出互联网。此功能强制所有域转换请求通过RV345P进行定向，对大多数用户来说都是一个好主意。

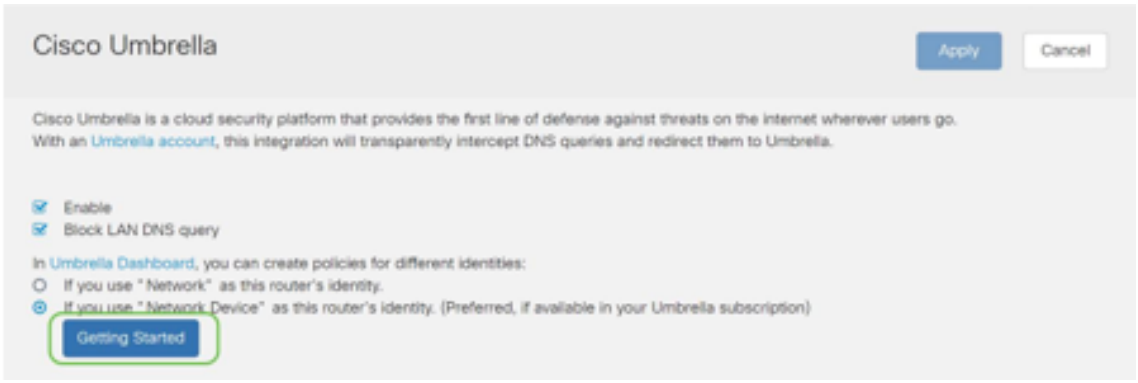
步骤 4

下一步将以两种不同的方式进行。它们都取决于您的网络设置。如果使用DynDNS或NoIP等服务，则保留默认命名方案“Network”。您需要登录这些帐户，以确保Umbrella在提供保护时与这些服务进行接口。出于我们的目的，我们依赖“网络设备”，因此我们单击底部单选按钮。



步骤 5

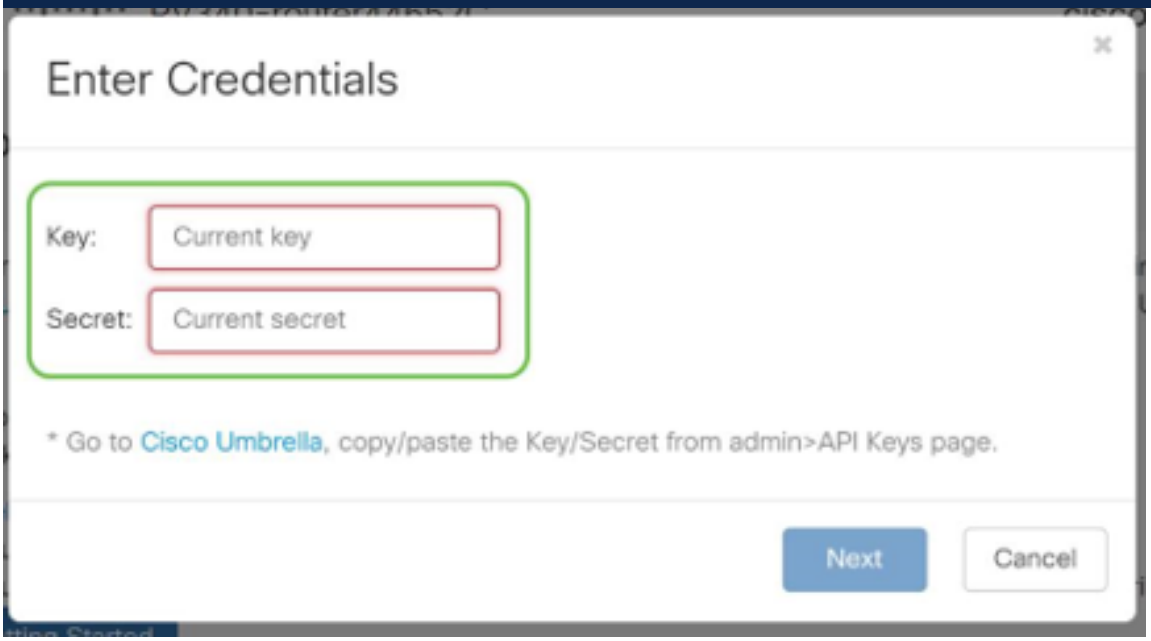
单击“**入门**”。



步骤 6

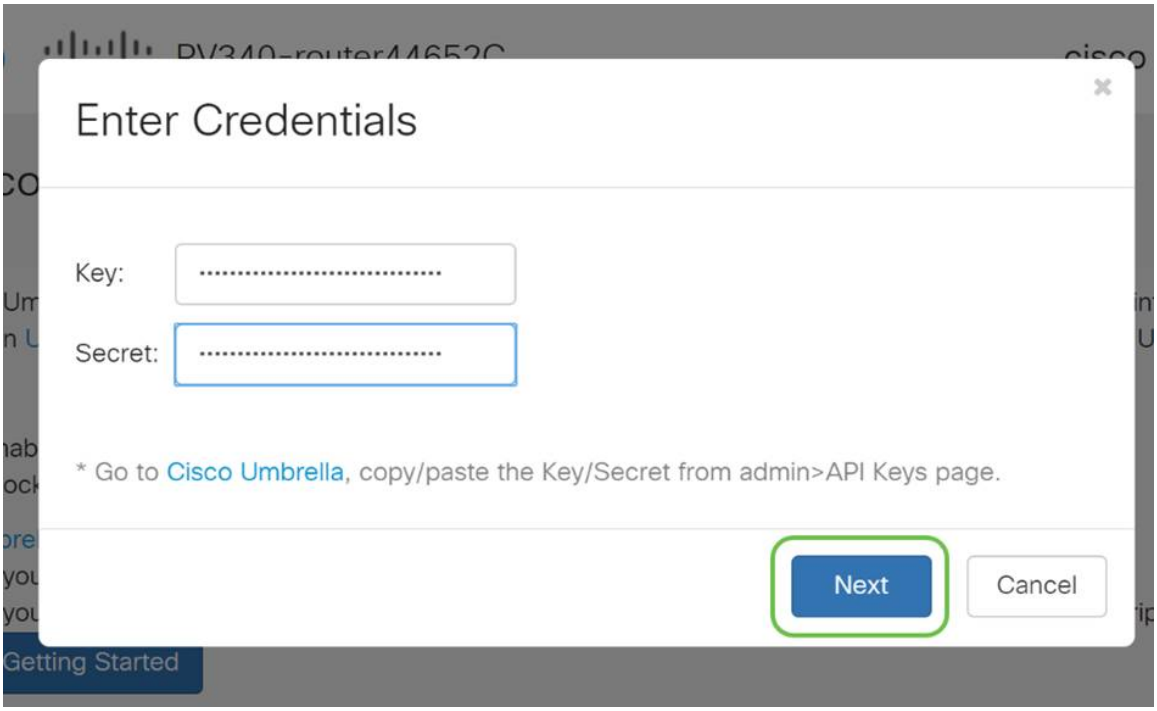
在文**本框中输入API**密钥和密钥。

两次叫出来，这样你就知道这很重要！如果丢失或意外删除密钥，则没有功能或支持号码可供调用以检索此密钥。请保密并保护其安全。如果丢失，您需要删除密钥，并重新授权要使用Umbrella保护的每台设备的新API密钥。



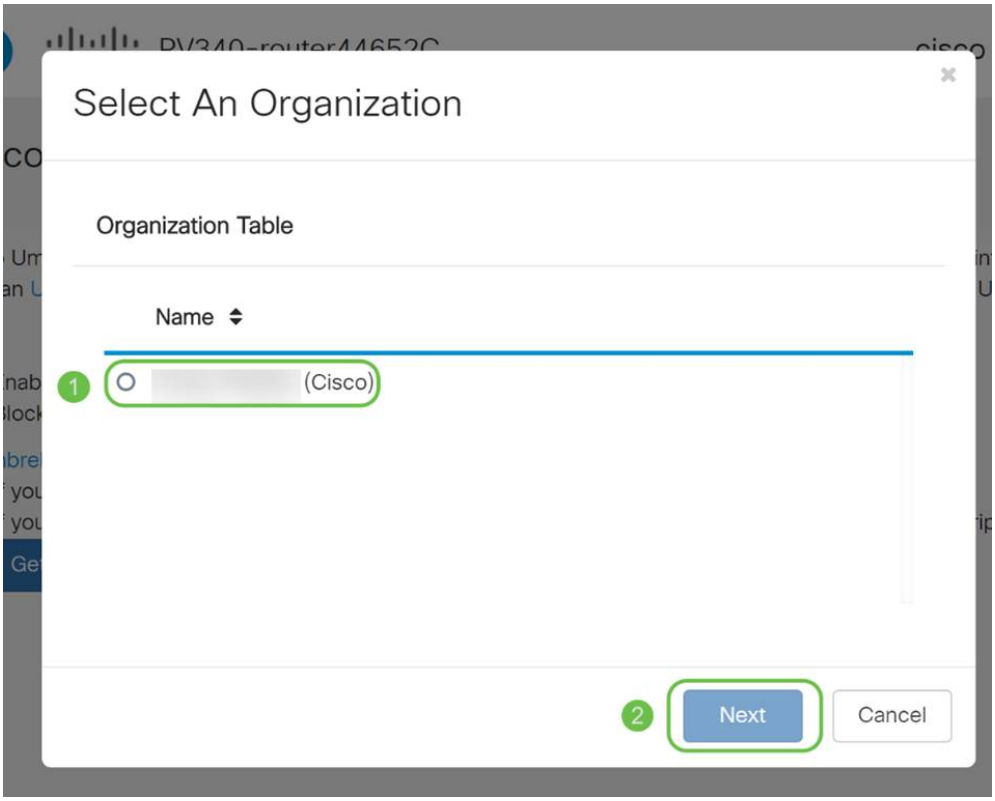
步骤 7

输入API和密钥后，单击“Next”**按钮**。



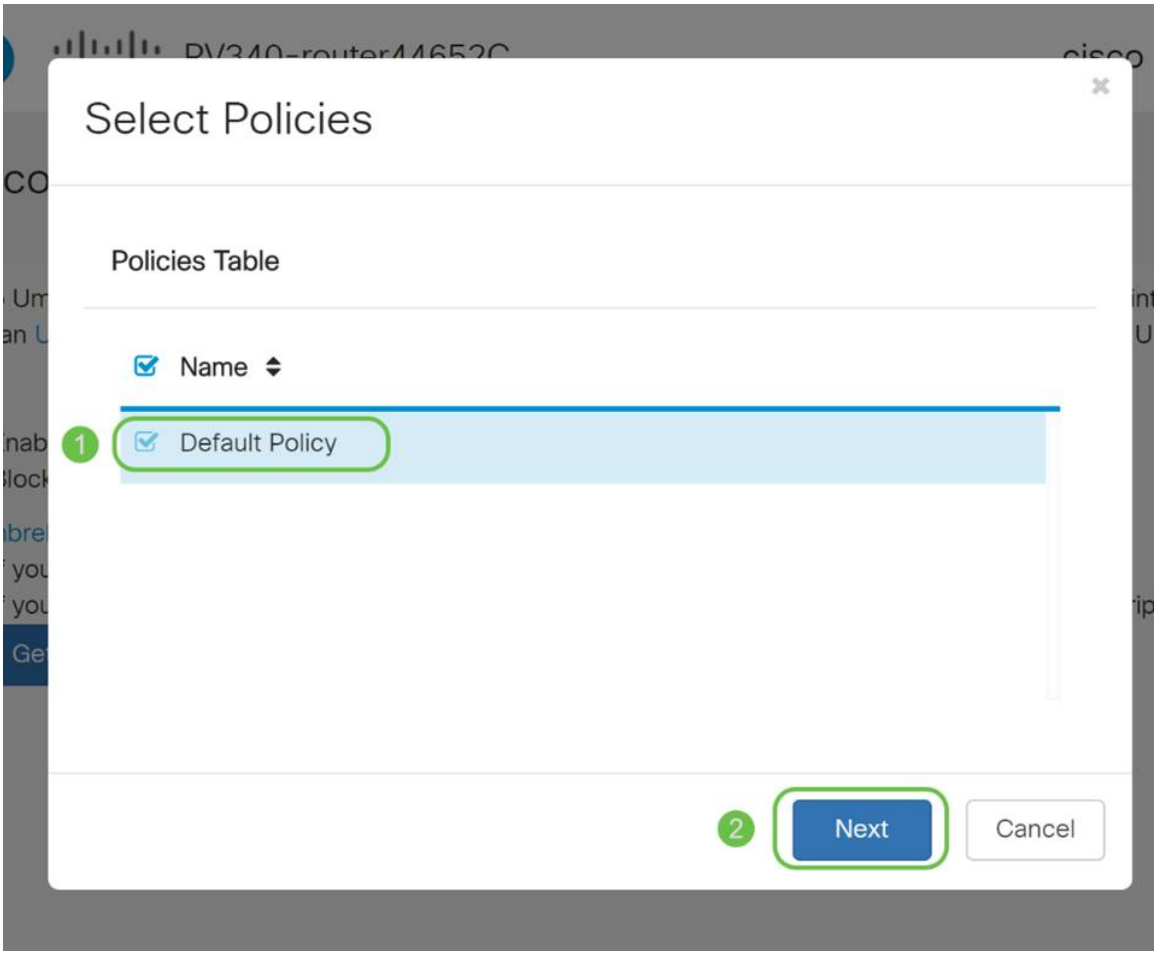
步骤 8

在下一个屏幕中，选择要与路由器关联的组织。单击 Next。



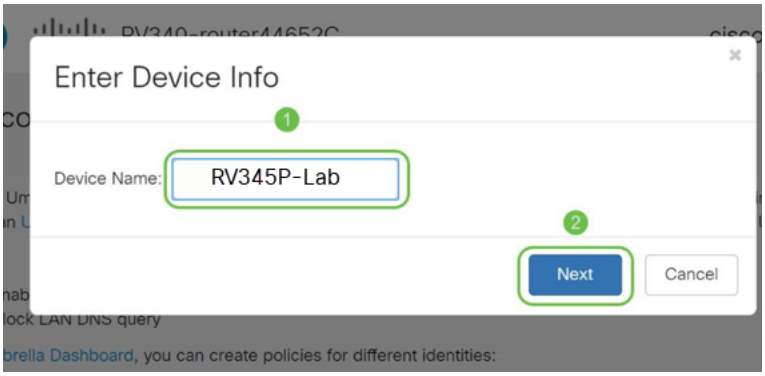
步骤 9

选择要应用于RV345P路由的流量的策略。对于大多数用户，默认策略将提供足够的覆盖范围。



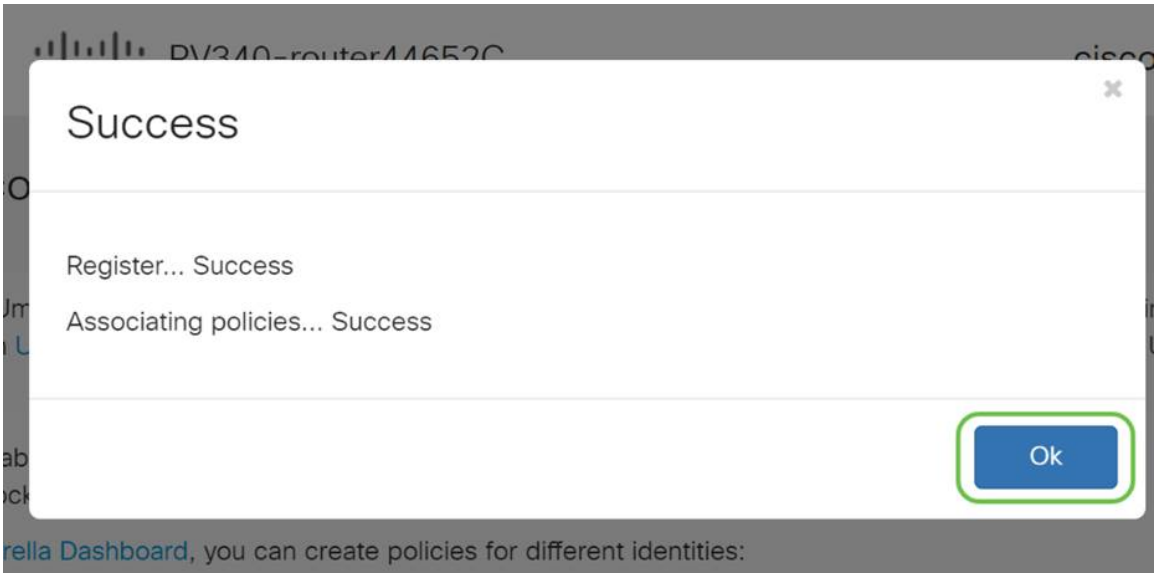
步骤 10

为设备指定名称，以便在Umbrella报告中指定。在我们的设置中，我们将其命名为*RV345P-Lab*。



步骤 11

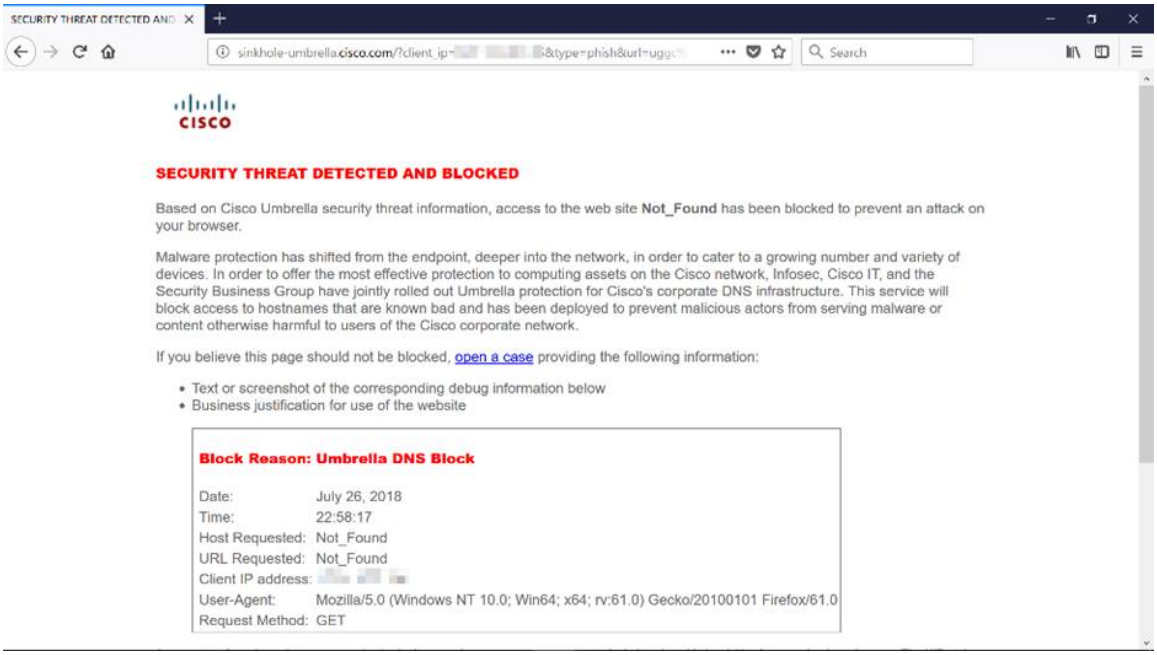
下一个屏幕将验证您选择的设置，并在成功关联时提供更新。Click OK.



确认

祝贺您，您现在受到Cisco Umbrella的保护。还是你？让我们用一个实例进行双重检查，以确保Cisco已创建一个网站，专门用来确定该网站的加载速度。单击此处或在浏览器栏中键入https://InternetBadGuys.com。

如果Umbrella配置正确，屏幕将类似此处显示。



其他安全选项

您是否担心有人会尝试通过从网络设备拔下以太网电缆并将其连接到网络来未经授权访问网络？在这种情况下，必须注册一列允许直接连接到路由器的主机，其IP地址和MAC地址各自。有关说明，请参阅“Configure IP Source Guard on the RV34x Series Router（在RV34x系列路由器上配置IP源防护）”一文。

VPN选项

虚拟专用网络(VPN)连接允许用户通过公共或共享网络（如Internet）访问、发送和接收

数据到专用网络和从专用网络接收数据，但仍确保与底层网络基础设施的安全连接以保护专用网络及其资源。

VPN隧道建立一个专用网络，该专用网络可以使用加密和身份验证安全地发送数据。公司办公室大多使用VPN连接，因为即使员工不在办公室，也允许其访问其专用网络既有用也是必要的。

VPN允许远程主机像位于同一本地网络一样工作。该路由器最多支持50个隧道。在路由器配置了Internet连接后，可以在路由器和终端之间设置VPN连接。VPN客户端完全依赖于VPN路由器的设置才能建立连接。

如果您不确定哪个VPN最符合您的需求，请查看Cisco Business VPN概述和最佳实践。

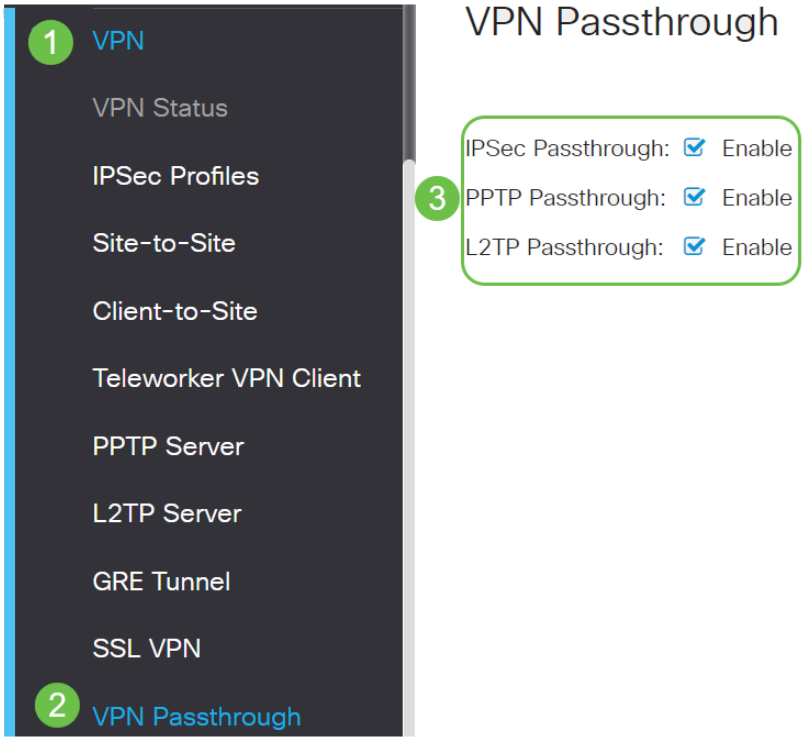
AnyConnect VPN是本配置指南中列出的唯一受思科VPN支持的产品。思科不支持第三方非思科产品，包括TheGreenBow和Shrew Soft。严格以指导为目的。如果您需要在文章之外的这些方面获得支持，应联系该第三方寻求支持。

如果您不计划设置VPN，可以单击跳至下一节。

VPN 传递

通常，每台路由器都支持网络地址转换(NAT)，以便在您希望支持具有相同Internet连接的多个客户端时节省IP地址。但是，点对点隧道协议(PPTP)和互联网协议安全(IPsec)VPN不支持NAT。VPN直通就是在这里出现的。VPN直通功能允许从连接到此路由器的VPN客户端生成的VPN流量通过此路由器并连接到VPN终端。VPN直通允许PPTP和IPsec VPN仅通过从VPN客户端发起的Internet，然后到达远程VPN网关。此功能通常在支持NAT的家用路由器上使用。

默认情况下，IPsec、PPTP和L2TP直通已启用。如果要查看或调整这些设置，请选择**VPN > VPN Passthrough**。根据需要查看或调整。



AnyConnect VPN

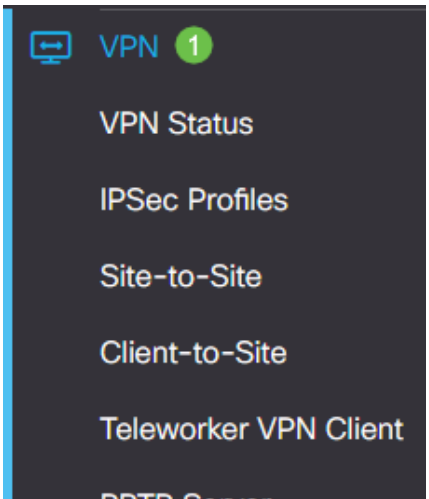
使用Cisco AnyConnect有以下几个优点：

1. 安全且持久的连接
2. 持续的安全和策略实施
3. 可从自适应安全设备(ASA)或企业软件部署系统部署
4. 可定制和可翻译
5. 易于配置
6. 支持互联网协议安全(IPsec)和安全套接字层(SSL)
7. 支持互联网密钥交换版本2.0(IKEv2.0)协议

在RV345P上配置AnyConnect SSL VPN

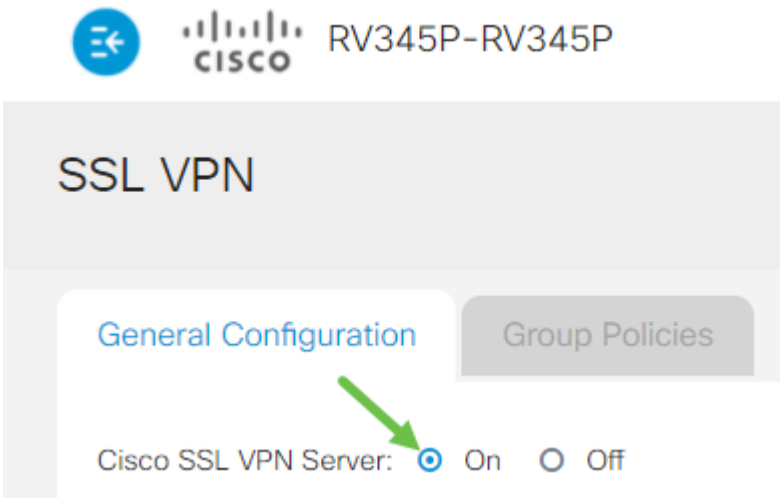
第 1 步

访问路由器基于Web的实用程序，然后选**择VPN > SSL VPN**。



步骤 2

单击**On**单选按钮以启用Cisco SSL VPN Server。



强制网关设置

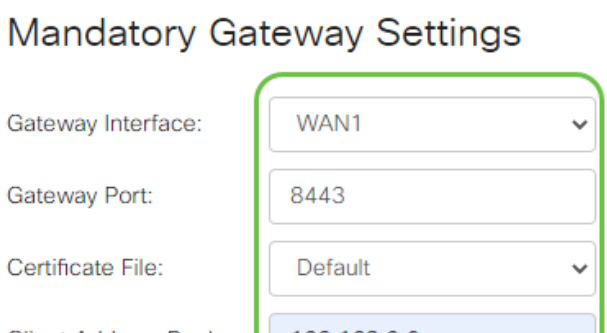
第 1 步

以下配置设置为必填项：

1. 从下拉列表中选择网关接口。这将是用于通过SSL VPN隧道传递流量的端口。选项包括：WAN1、WAN2、USB1、USB2
2. 在Gateway Port字段中输入用于SSL VPN网关的端口号，范围为1到65535。
3. 从下拉列表中选择证书文件。此证书对尝试通过SSL VPN隧道访问网络资源的用户进行身份验证。下拉列表包含默认证书和导入的证书。
4. 在Client Address Pool字段中输入客户端地址池*的IP地*址。此池是将分配给远程VPN客户端的IP地址范围。

确保IP地址范围不与本地网络上的任何IP地址重叠。

6. 从下拉列表中选择客户端网络掩码。
7. 在Client Domain（客户端域）字段中*输入客户端*域名。这将是应推送到SSL VPN客户端的域名。
8. 在Login Banner字段中输入显示为登录标语*的*文本。这将是每次客户端登录时显示的标语。



步骤 2

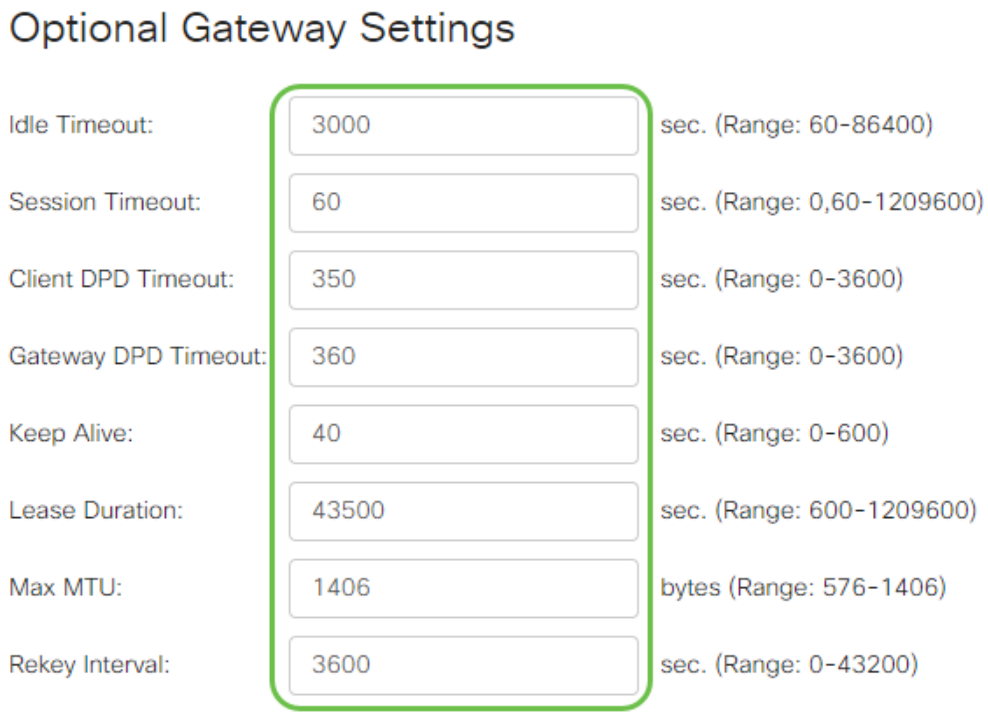
单击 Apply。

可选网关设置

第 1 步

以下配置设置是可选的：

1. 为空闲超时(Idle Timeout)输入一个介于60到86400之间的值（以秒为单位）。这将是SSL VPN会话可以保持空闲的持续时间。
2. 在Session Timeout字段中输入以秒*为单位的*值。这是*传*输控制协议(TCP)或用户数据报协议(UDP)会话在指定空闲时间后超时所需的时间。范围从 60 至 1209600。
3. 在ClientDPD Timeout字段中输入介*于0到*3600之间的值（以秒为单位）。此值指定定期发送HELLO/ACK消息以检查VPN隧道的状态。*必*须在VPN隧道的两端启用此功能。
4. 在GatewayDPD Timeout字段中输入介*于0到*3600之间的值（以秒为单位）。此值指定定期发送HELLO/ACK消息以检查VPN隧道的状态。*必*须在VPN隧道的两端启用此功能。
5. 在“保持连接”字*段中*输入介于0和600之间的值（以秒为单位）。此功能可确保路由器始终连接到Internet。如果VPN连接被丢弃，它将尝试重新建立该连接。
6. 在Lease Duration字段中，为要连接的隧道的持续时间输入*以秒为*单位。范围从 600 至 1209600。
7. 输入可通过网络发送的数据包大小（以字节为单位）。范围从 576 至 1406。
8. 在Rekey Interval字段中输入中*继间隔*时间。Rekey功能允许SSL密钥在会话建立后重新协商。范围从 0 至 43200。



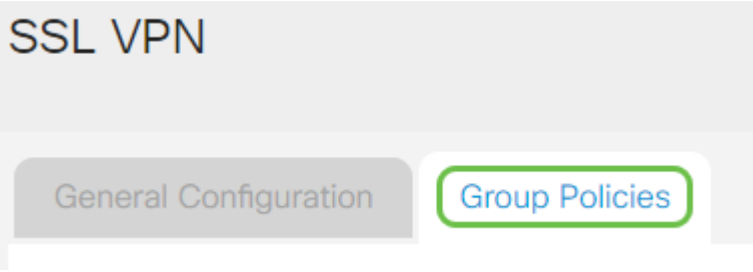
步骤 2

单击 Apply。

配置组策略

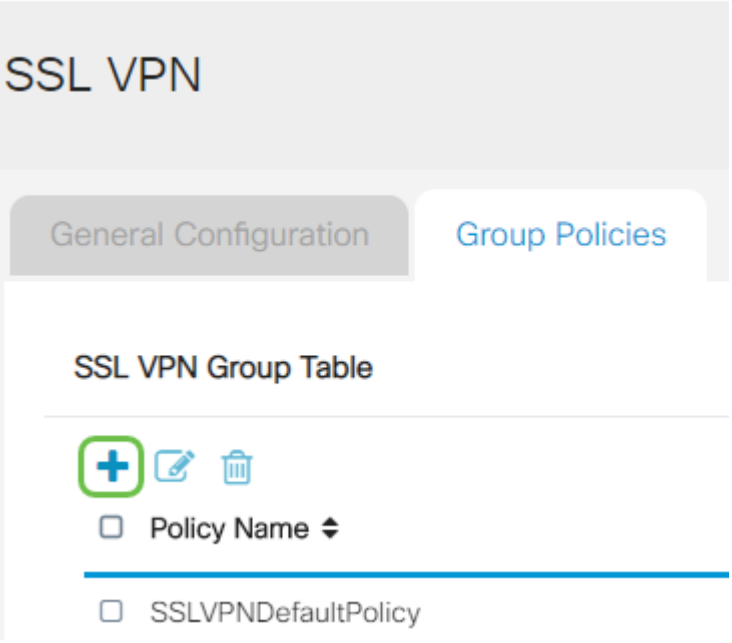
第 1 步

单击“组**策略**”选项卡。



步骤 2

单击SSL **VPN组**表下的添加图标以添加组策略。

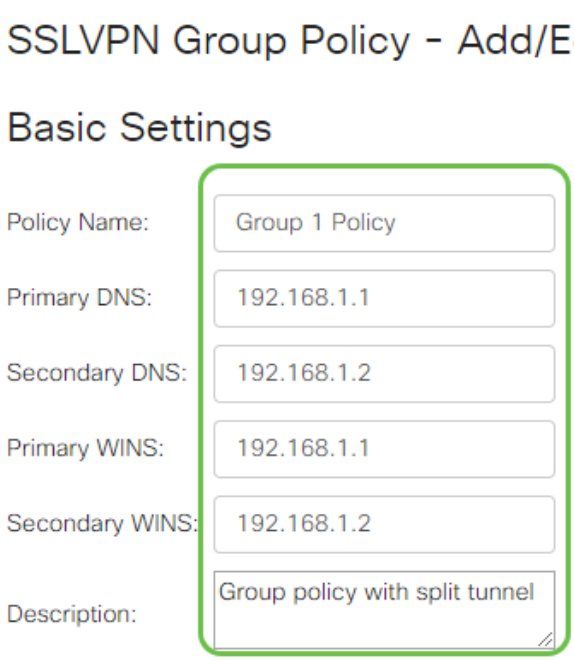


SSL VPN Group表将显示设备上的组策略列表。您还可以编辑列表中名为SSLVPNDefaultPolicy的第一个组策略。这是设备提供的默认策略。

步骤 3

1. 在Policy Name字段中输入首选*策略*名称。
2. 在提供的字段中输入主DNS的IP地址。默认情况下，已提供此IP地址。

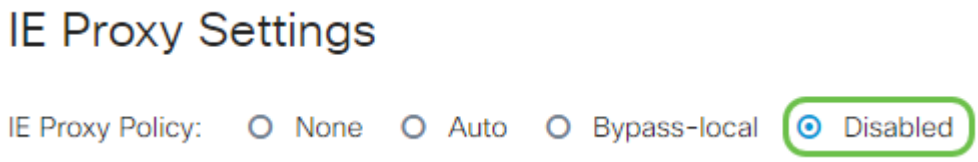
3. *（可选）在提供的字段中输入辅助DNS的IP地址。当主DNS发生故障时，这将用作备份。*
4. （可选）在提供的字段中输入主WINS的IP地址。
5. （可选）在提供的字段中输入辅助WINS的IP地址。
6. （可选）在“说明”字段中输入策略*的说*明。



步骤 4（可选）

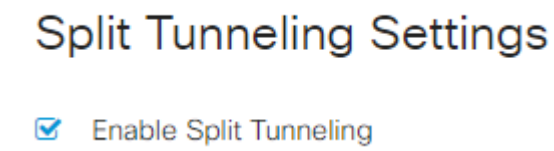
点击单选按钮以选择IE代理策略，以启用Microsoft Internet Explorer(MSIE)代理设置以建立VPN隧道。选项有：

- 无 — 允许浏览器不使用代理设置。
- 自动 — 允许浏览器自动检测代理设置。
- Bypass-local — 允许浏览器绕过在远程用户上配置的代理设置。
- 已禁用 — 禁用MSIE代理设置。



步骤 5（可选）

在Split Tunneling Settings区域，选中**Enable Split Tunneling**复选框，以允许将发往互联网的流量不加密地直接发送到互联网。全隧道将所有流量发送到终端设备，然后将其路由到目的资源，从而消除企业网络的Web访问路径。

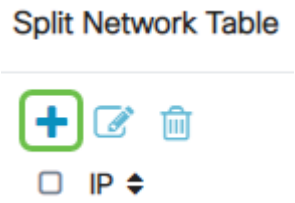


步骤 6（可选）

点击单选按钮以选择应用分割隧道时是包括还是排除流量。

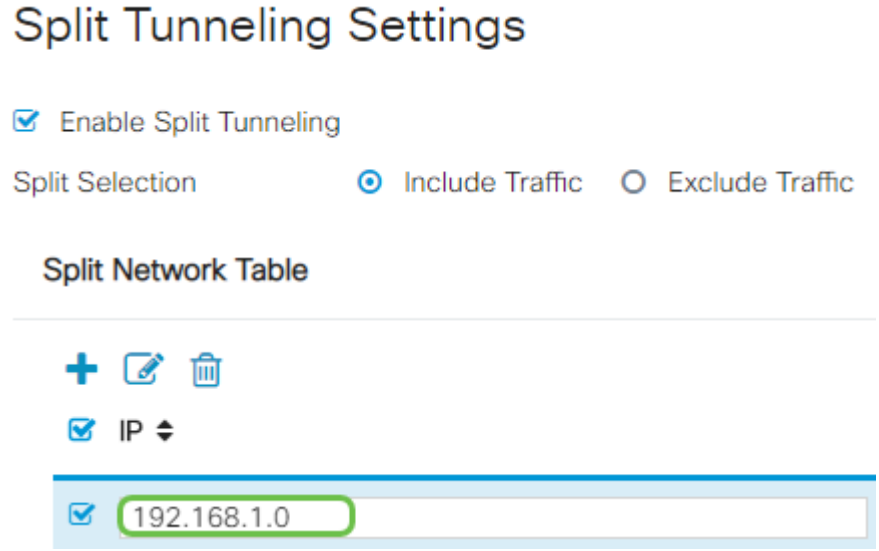
步骤 7

在拆分网络表中，单击添**加图**标以添加拆分网络异常。



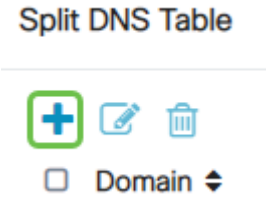
步骤 8

在提供的字段中输入网络的IP地址。



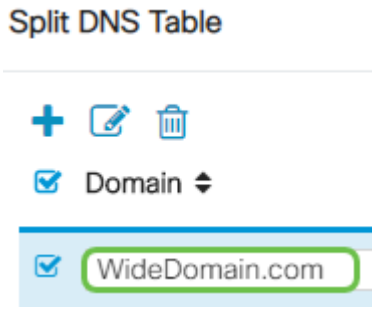
步骤 9

在拆分DNS表中，单击添**加图**标以添加拆分DNS异常。



步骤 10

在提供的字段中输入域名，然后单击**应用**。



默认情况下，该路由器带有2个AnyConnect服务器许可证。这意味着，一旦您拥有AnyConnect客户端许可证，就可以与任何其他RV340系列路由器同时建立2个VPN隧道。

简而言之，RV345P路由器不需要许可证，但所有客户端都需要许可证。AnyConnect客户端许可证允许桌面和移动客户端远程访问VPN网络。

下一节详细介绍如何获取客户端的许可证。

AnyConnect移动客户端

VPN客户端是在希望连接到远程网络的计算机上安装并运行的软件。必须使用与VPN服务器相同的配置（如IP地址和身份验证信息）设置此客户端软件。此身份验证信息包括用于加密数据的用户名和预共享密钥。VPN客户端也可以是硬件设备，具体取决于要连接的网络的物理位置。如果VPN连接用于连接位于不同位置的两个网络，则通常会发生这种情况。

Cisco AnyConnect安全移动客户端是用于连接到在各种操作系统和硬件配置上运行的VPN的软件应用。此软件应用程序使另一个网络的远程资源能够以安全的方式被访问，就像用户直接连接到他的网络一样。

使用AnyConnect注册和配置路由器后，客户端可以从您购买的可用许可证池在路由器上安装许可证，详见下一节。

购买许可证

您必须从思科总代理商或思科合作伙伴处购买许可证。订购许可证时，您必须以name@domain.com的形式提供您的思科智能帐户ID或域*ID*。

如果您没有思科总代理商或合作伙伴，您可以在此处找到一个。

在撰写本文时，以下产品SKU可用于购买25个捆绑包中的其他许可证。请注意，Cisco AnyConnect订购指南中概述的AnyConnect客户端许可证还有其他选项，但是，所列产品ID是完整功能的最低要求。

请注意，AnyConnect客户端许可证产品SKU首先列出，提供1年的许可证，并且至少需要购买25个许可证。适用于RV340系列路由器的其他产品SKU也提供不同订用级别，如下所示：

- LS-AC-PLS-1Y-S1 — 1年Cisco AnyConnect Plus客户端许可证
- LS-AC-PLS-3Y-S1 - 3年期Cisco AnyConnect Plus客户端许可证
- LS-AC-PLS-5Y-S1 - 5年期Cisco AnyConnect Plus客户端许可证
- LS-AC-PLS-P-25-S — 25件装Cisco AnyConnect Plus永久客户端许可证
- LS-AC-PLS-P-50-S - 50件装Cisco AnyConnect Plus永久客户端许可证

客户端信息

当您的客户端设置以下其中一项时，您应将以下链接发送给他们：

- Windows 窗口版本:Windows计算机上的AnyConnect
- Mac：在Mac上安装AnyConnect。
- Ubuntu桌面：在Ubuntu桌面上安装和使用AnyConnect
- 如果您有问题，可以转至“收集信息以进行Cisco AnyConnect安全移动客户端错误的基本故障排除”。

验证AnyConnect VPN连接

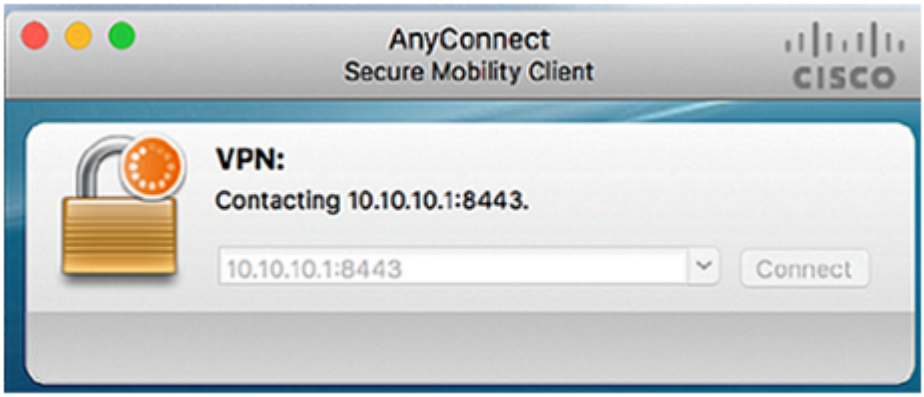
第 1 步

单击AnyConnect安全移动客户端图标。

步骤 2

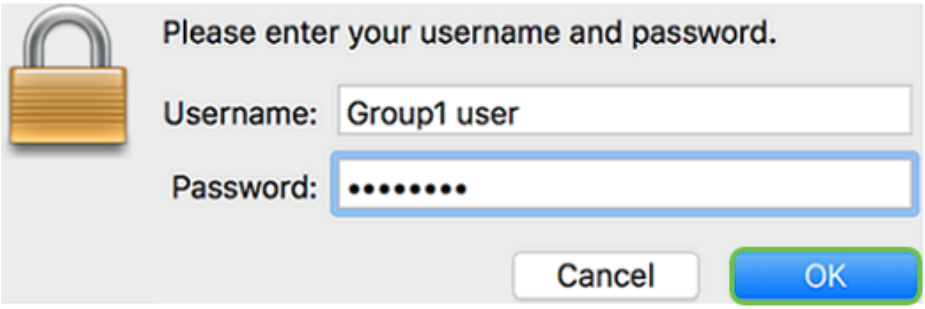
在AnyConnect安全移动客户端窗口中，输入网关IP地址和网关端口号，用冒号(:)分隔，然后单击**连接**。

软件现在将显示它正在与远程网络联系。



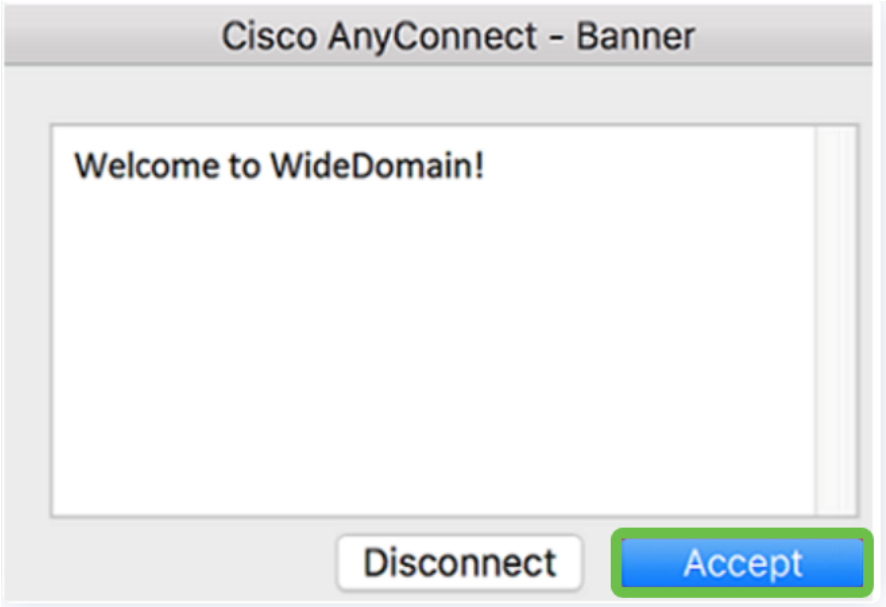
步骤 3

在各自的字段中输入您的服务器用户名和密码，然后单击**OK**。

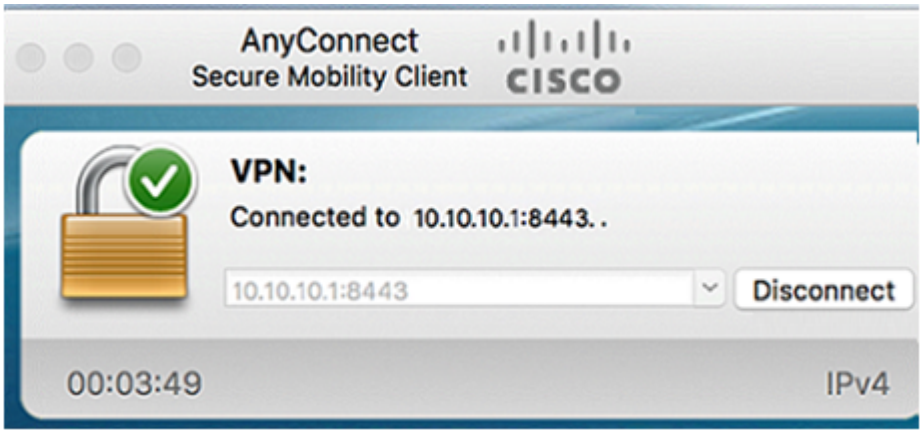


步骤 4

一旦建立连接，就会出现登录横幅。单击 Accept。



现在，AnyConnect窗口应指示与网络的VPN连接成功。



如果现在使用AnyConnect VPN，可以跳过其他VPN选项，转到下[一部分](#)。

史鲁软VPN

IPsec VPN允许您通过在Internet上建立加密隧道来安全地获取远程资源。RV34X系列路由器用作IPsec VPN服务器，并支持Shrew Soft VPN客户端。本节将介绍如何配置路由器和Shrew软客户端以保护与VPN的连接。

思科不支持Shrew Soft。本示例仅用于演示目的。如果您对史鲁软有问题，请联系他们寻求支持。

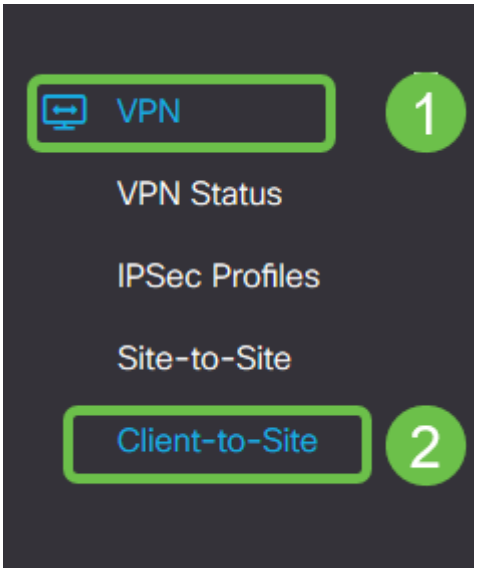
您可以从以下位置下载最新版本的Shrew Soft VPN客户端软件：https://www.shrew.net/download/vpn

在RV345P系列路由器上配置Shrew Soft

首先，我们将在RV345P上配置客户端到站点VPN。

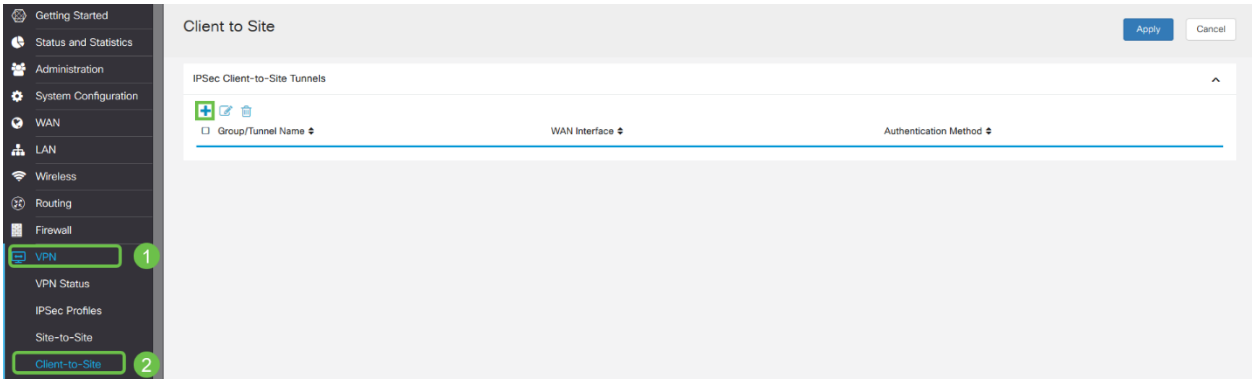
第 1 步

导航至**VPN > Client-to-Site。**



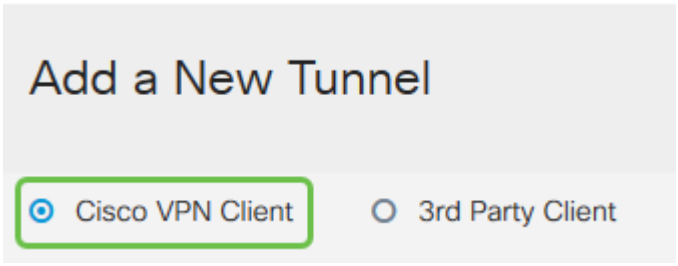
步骤 2

添加客**户端到站点VPN配置**文件。



步骤 3

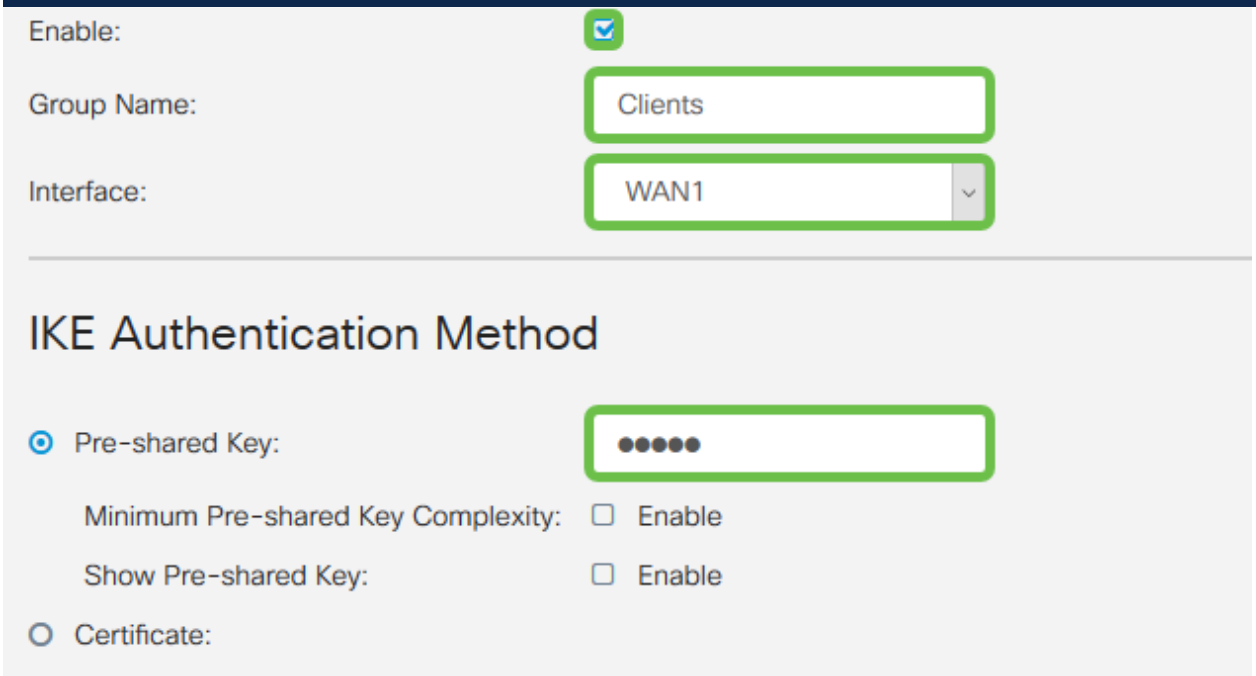
选择**Cisco VPN Client**选项。



步骤 4

选中**Enable**框，使VPN客户端配置文件处于活动状态。我们还将配置*组名*称，选**择WAN接**口，并输**入预共享密钥**。

请注意 *组名*和 *预共享密*钥，它们稍后将在配置客户端时使用。

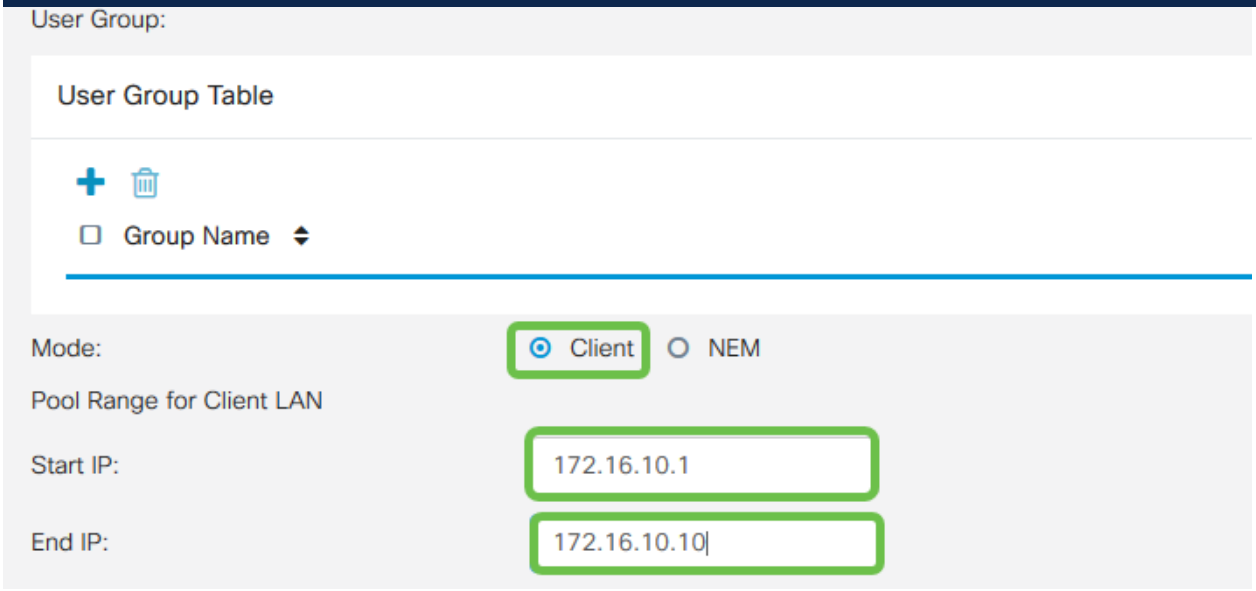


步骤 5

暂时将**用户组表**留空。这是用于路*由器*上的用户组，但我们尚未对其进行配置。确保模

式设置为**客户端**。输入客**户端LAN的池范围**。我们将使用172.16.10.1到172.16.10.10。

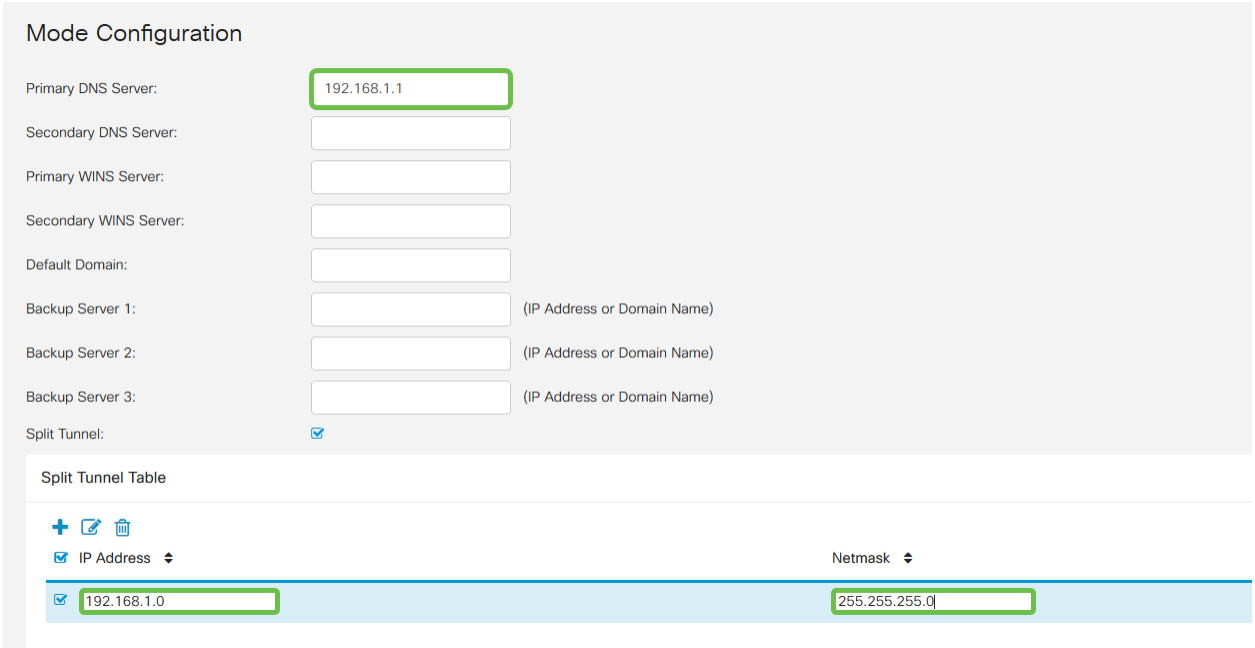
池范围应使用网络中其他位置未使用的唯一子网。



步骤 6

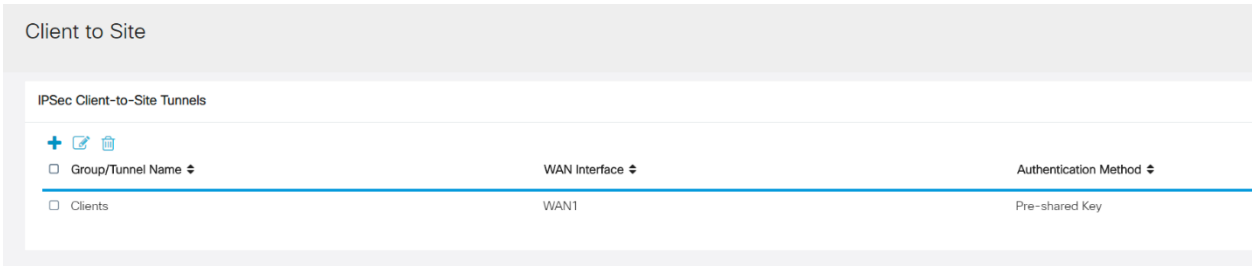
此处是配置模式配**置设置**的位置。我们将使用以下设置：

- **主 DNS 服务器**：如果您有内部DNS服务器或想使用外部DNS服务器，可以在此处输入。否则，默认设置为RV345P LAN IP地址。我们将在示例中使用默认值。
- **分割隧道：选**中以启用分割隧道。这用于指定哪些流量将通过VPN隧道。我们将在示例中使用分割隧道。
- **拆分隧道表**：输入VPN客户端应通过VPN访问的网络。本示例使用RV345P LAN网络。



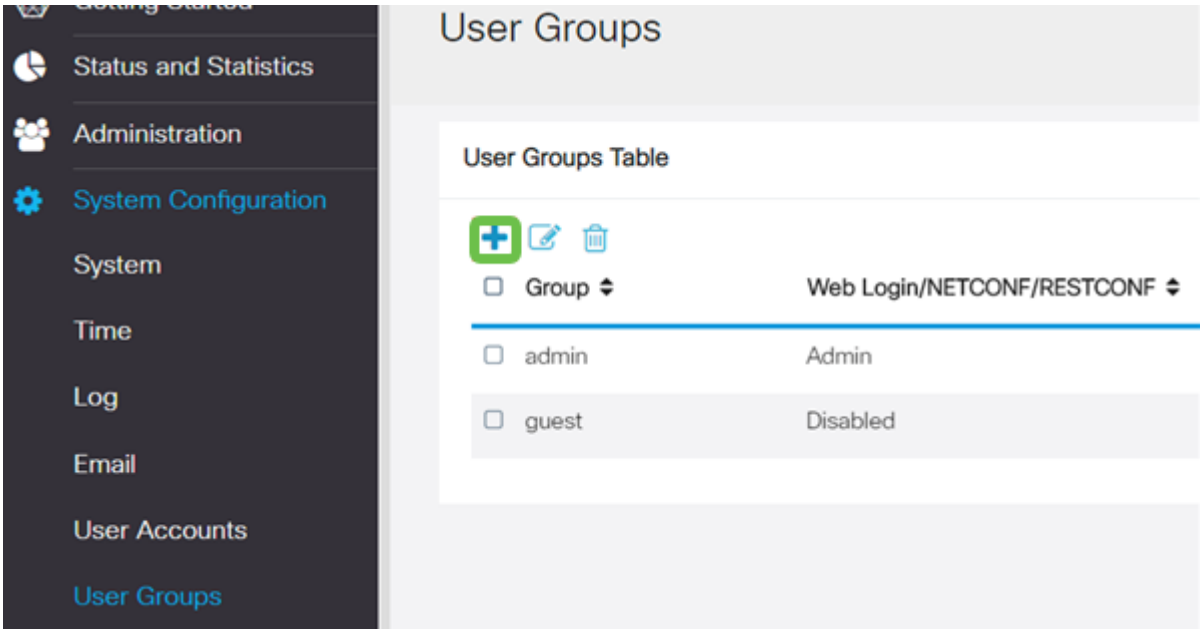
步骤 7

单击Save后，我们可以在IPsec Client-to-Site Groups列表中看到配置文件。



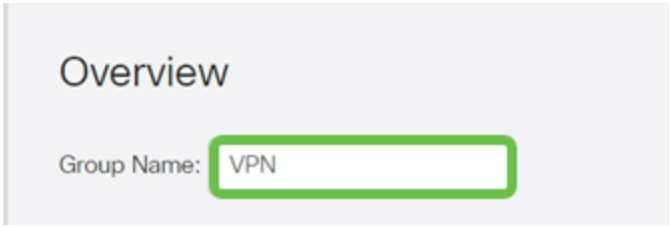
步骤 8

配置用**于验证**VPN客户端用户的用户组。在“**系统配置**”>“**用**户组”下，单**击加**号图标添加用户组。



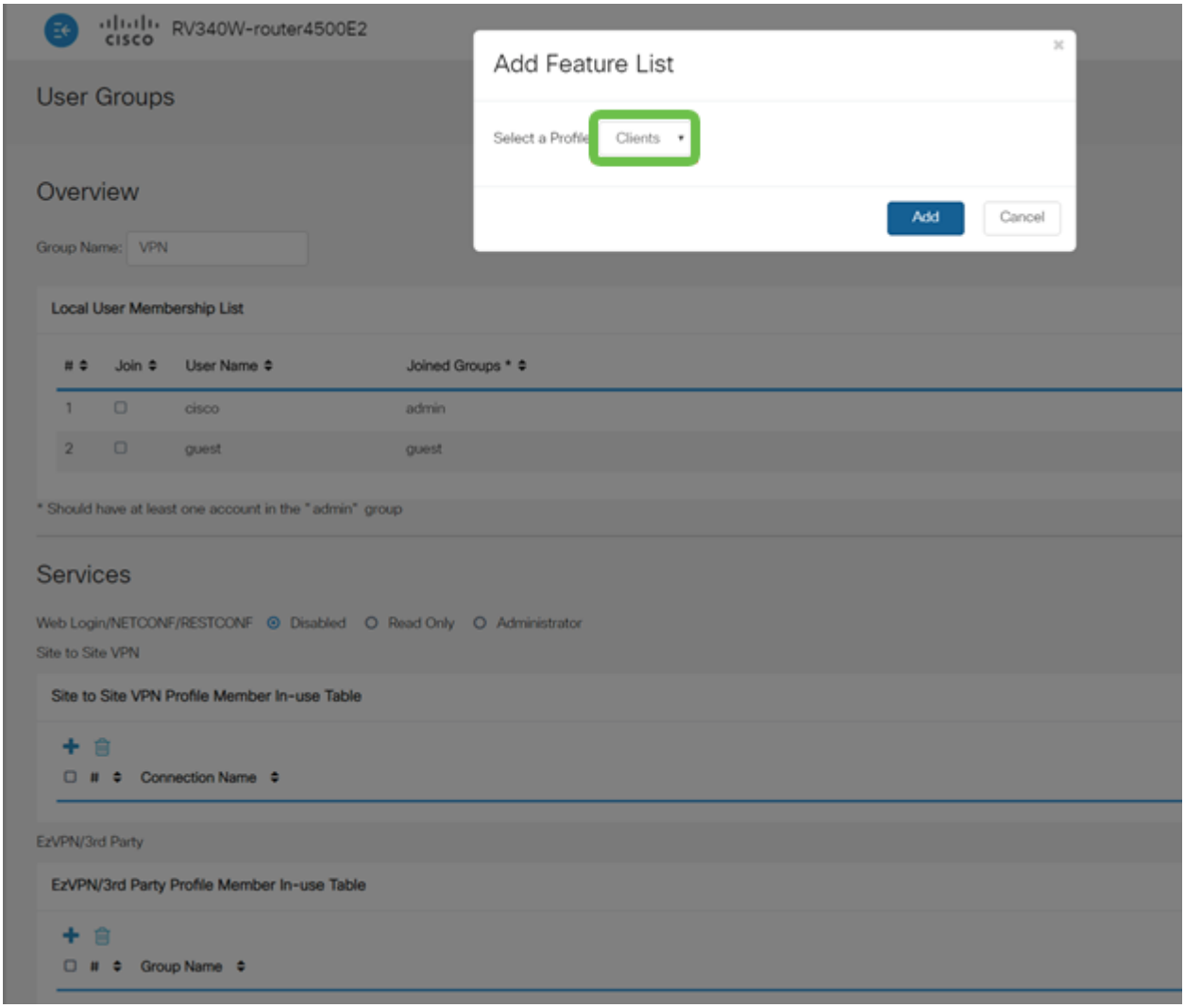
步骤 9

输入组名称。



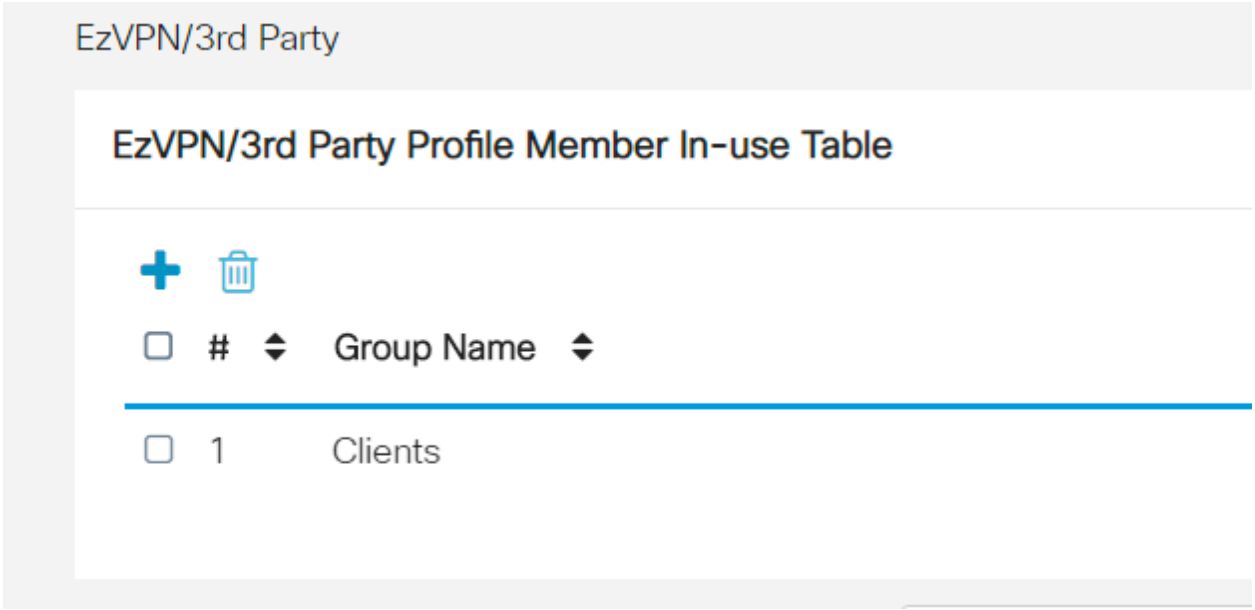
步骤 10

在**Services > EzVPN/第3方**下，单击**Add** 将此用户组链接到先前配置的Client-to-Site Profile。



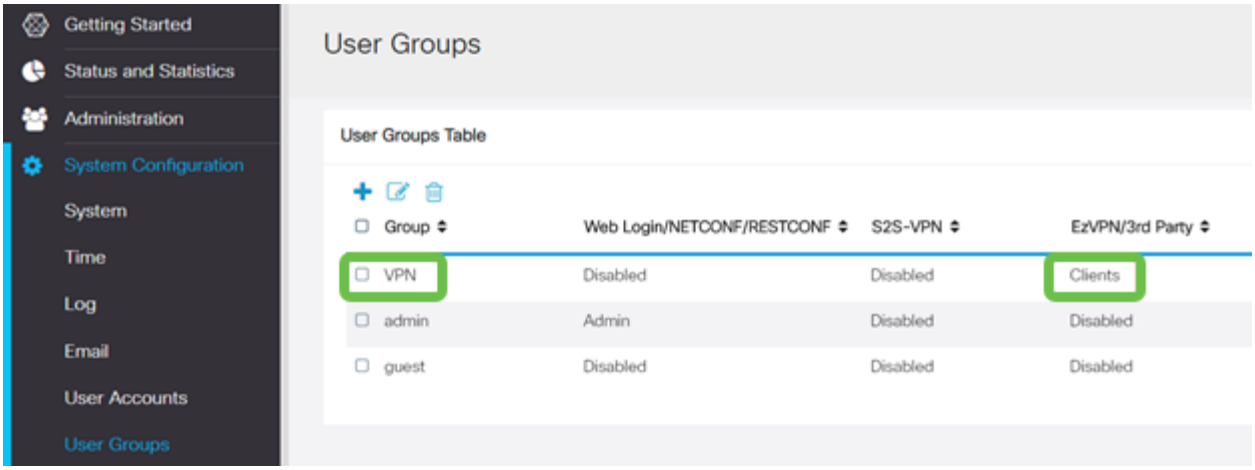
步骤 11

现在，您应该**在EzVPN/第**三方的列表中看**到"客户端到站点组名"。**



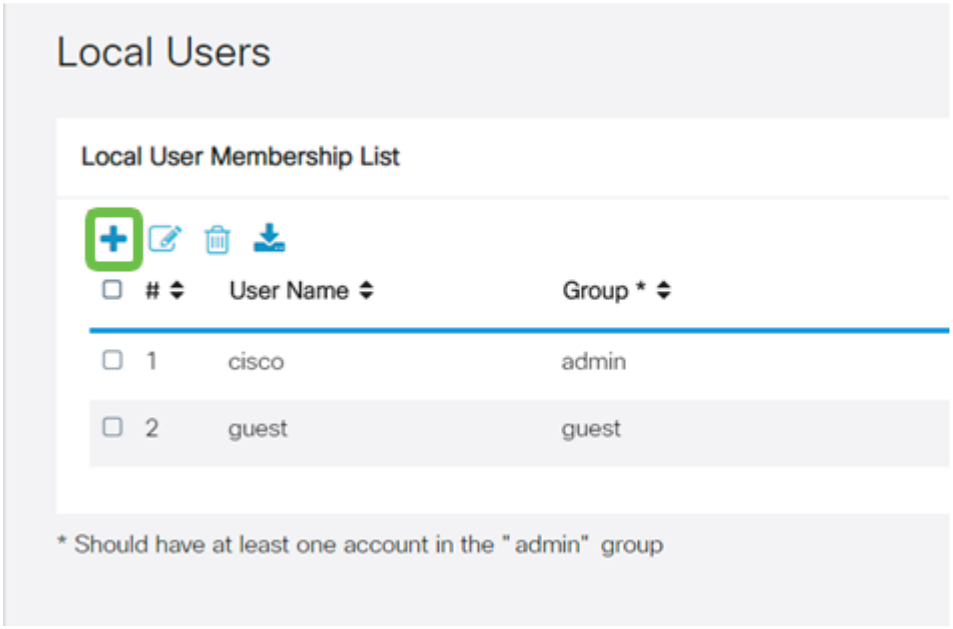
步骤 12

应用用**户**组配置后，您将在**用户组**列表中看到该配置，并显示新用户组将与您之前创建的客户端到站点配置文件一起使用。



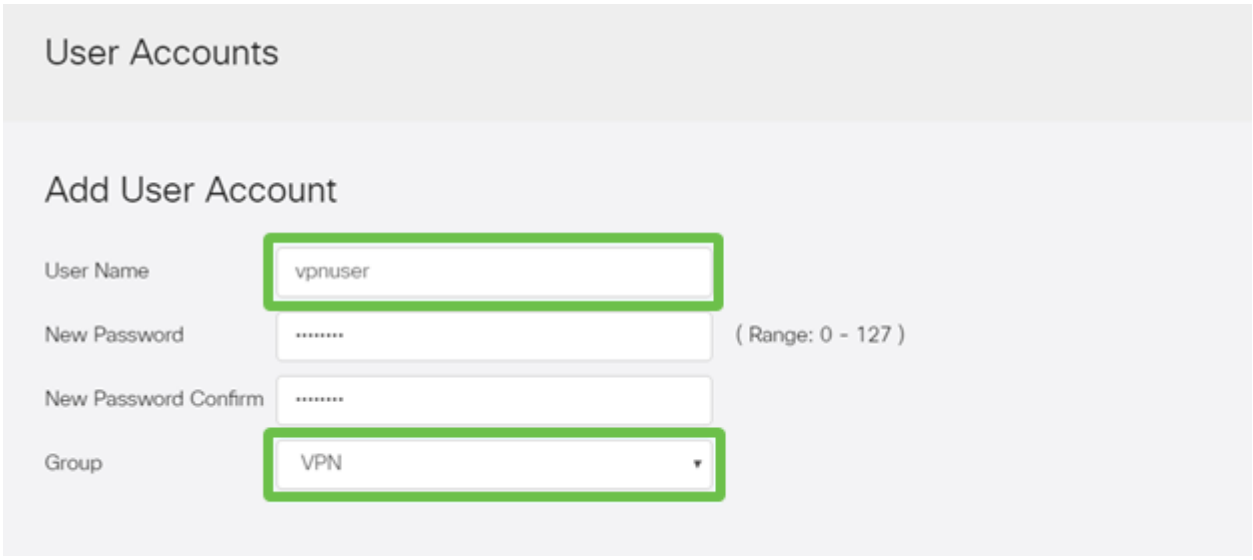
步骤 13

在System Configuration > User Accounts**中配置新用户**。单击加号**图标**创建新用户。



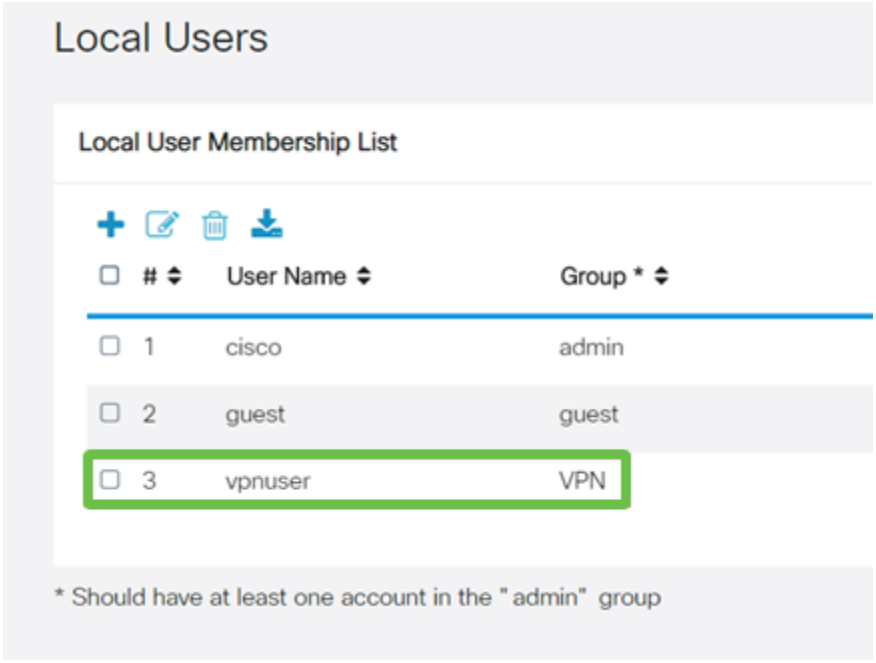
步骤 14

输入新**用户名**和新**密码**。验证组**是否**已设置为刚**配置**的新用户组。完成后**单击**“应用”。



步骤 15

新用**户**将显示在本地用户**列表中**。



RV345P系列路由器的配置完成。接下来，您将配置Shrew Soft VPN客户端。

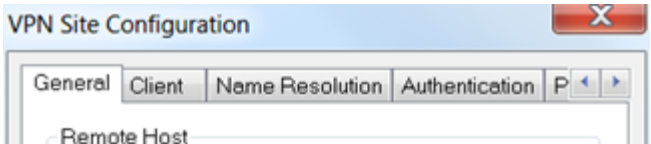
配置Shrew Soft VPN客户端

执行以下步骤。

第 1 步

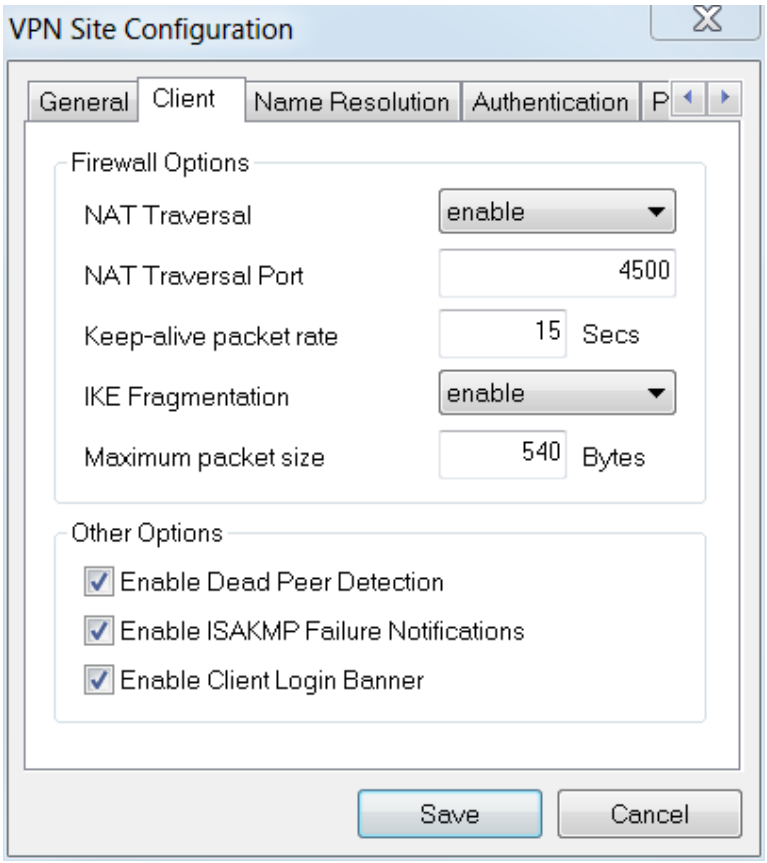
打开Shrew Soft VPN Access Manager，*然后单*击“添**加”**添加配置文件。在显示*的VPN Site Configuration*窗口中，配置General**选**项卡：

- **主机名或 IP 地址:**使用WAN IP地址（或RV345P的主机名）
- **自动配置**:选择ike config pull
- **适配器模式**:选择**使用虚拟适配器和分配的地址**



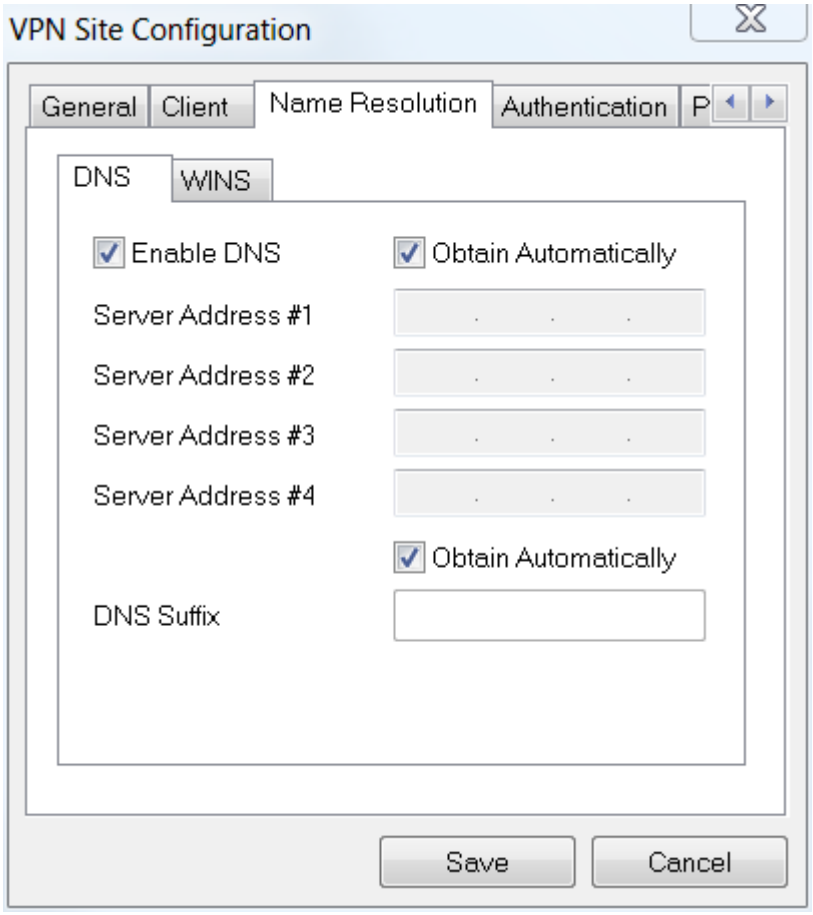
步骤 2

配置“客户端”选项卡。在本例中，我们保留了默认设置。



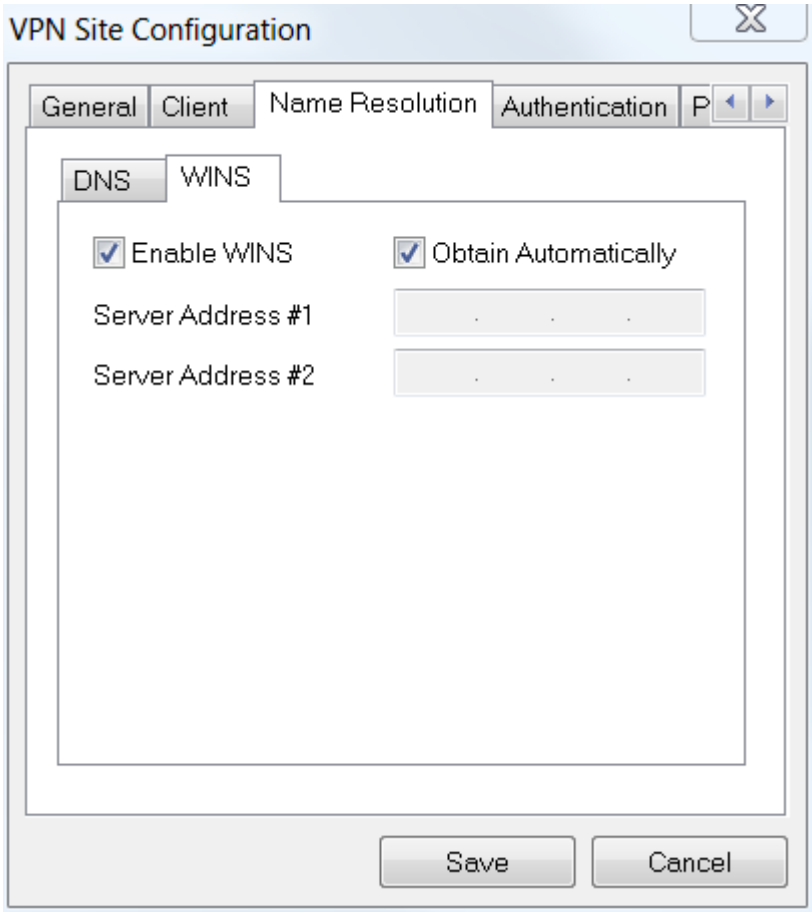
步骤 3

在“名称解析> DNS”下，选中“启用DNS”框，并选中“自动获取”框。



步骤 4

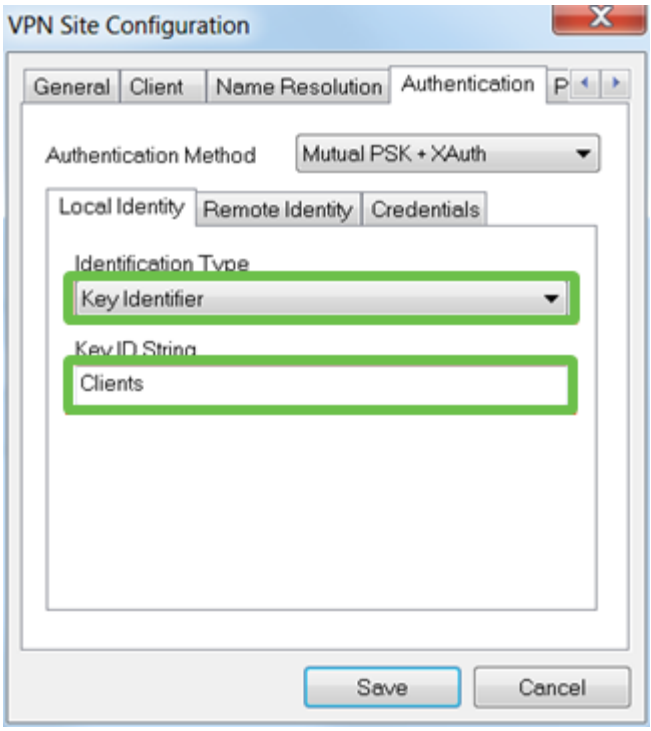
在**Name Resolution > WINS**选项卡下，选中**Enable WINS** 框，并保持选中**Obtain Automatically**框。



步骤 5

单击**Authentication > Local Identity**。

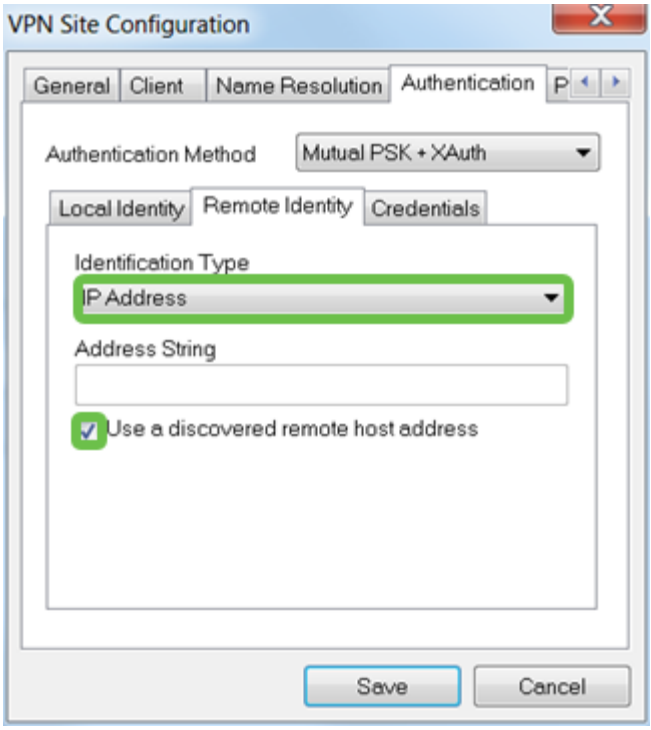
- **标识类型**:选择**密钥标识符**
- **密钥ID字符串**:输入**在RV345P**上配置的组名



步骤 6

在**Authentication > Remote Identity**下。在本例中，我们保留了默认设置。

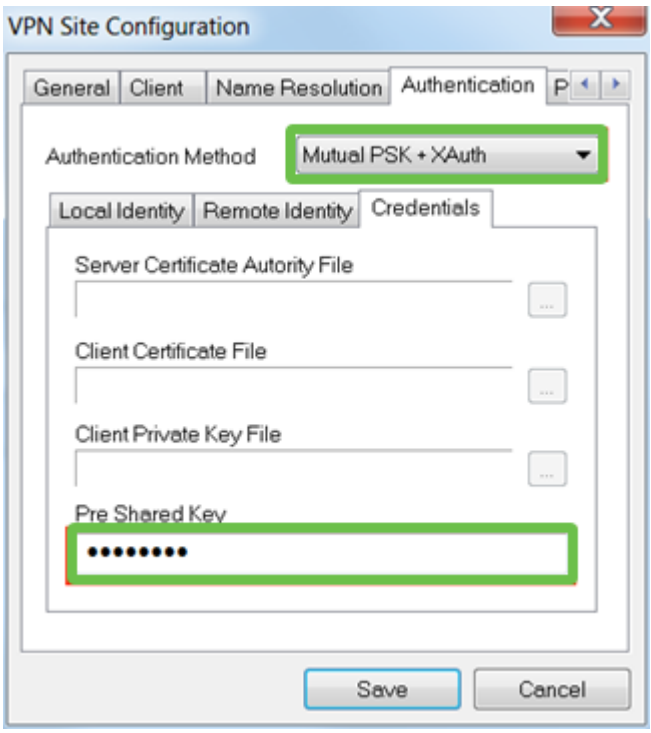
- **标识类型**:IP Address
- **地址字符串**:<blank>
- **使用已发现的远程主机地址**框：已选中



步骤 7

在**Authentication > Credentials**下，配置以下内容：

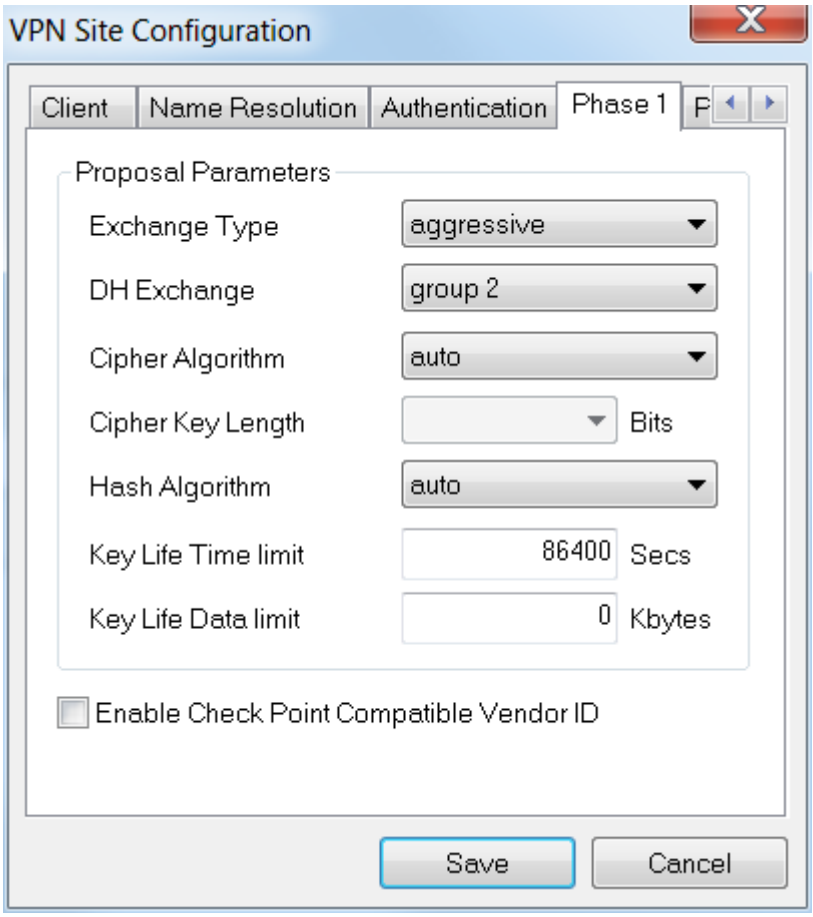
- **认证方法**:选择**Mutual PSK +扩展验证**
- **预共享密钥**:输入在**RV345P客户端配**置文件中配置的预共享密钥



步骤 8

用于“阶**段1**”选项卡。在本例中，保留了默认设置：

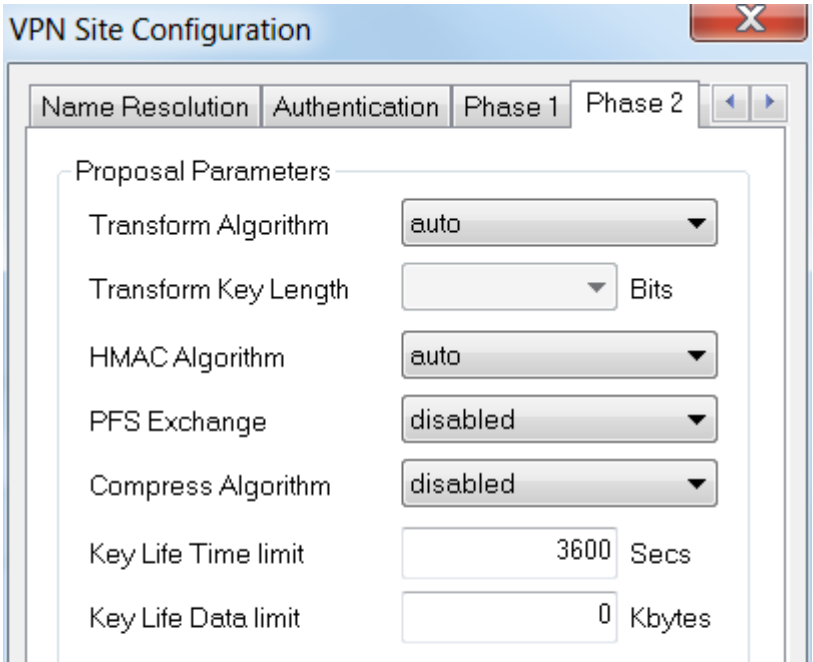
- **Exchange类型：主动**性
- **DH交换**：组2
- **密码算法**：自动
- **散列算法**：自动



步骤 9

在本例中，Phase 2选项卡**的默**认值保持不变。

- **转换算法**：自动
- **HMAC算法**：自动
- **PFS交换**：已禁用
- **压缩算法**：已禁用

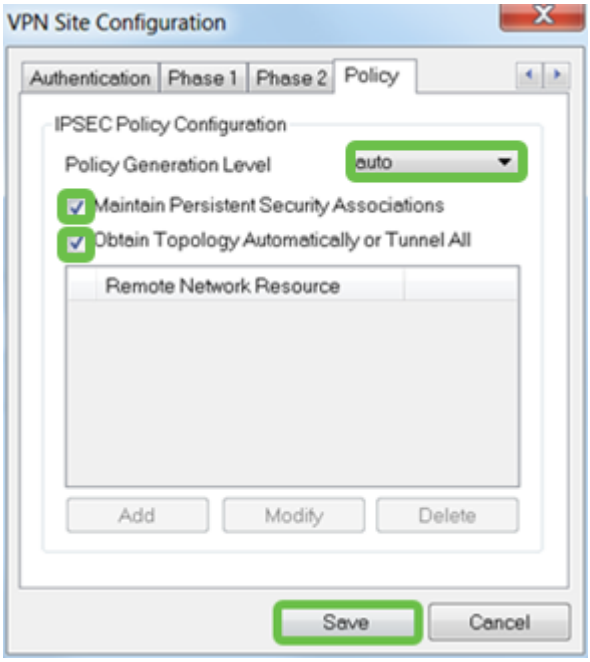


步骤 10

对于**Policy**选项卡示例，我们使用了以下设置：

- **策略生成级别：自动**
- **维护持续安全关联：已选中**
- **自动获取拓扑或全部隧道：已选中**

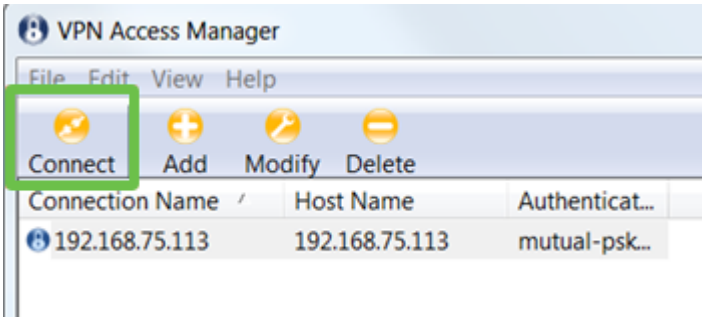
由于我们在**RV345P**上配置了分割隧道，因此我们无需在此处进行配置。



完成后，单击 Save（保存）。

步骤 11

您现在已准备好测试连接。在“VPN *Access Manager(VPN访问管*理器)”中，突出显示连接配置文件并单击“**Connect(连**接)”按钮。

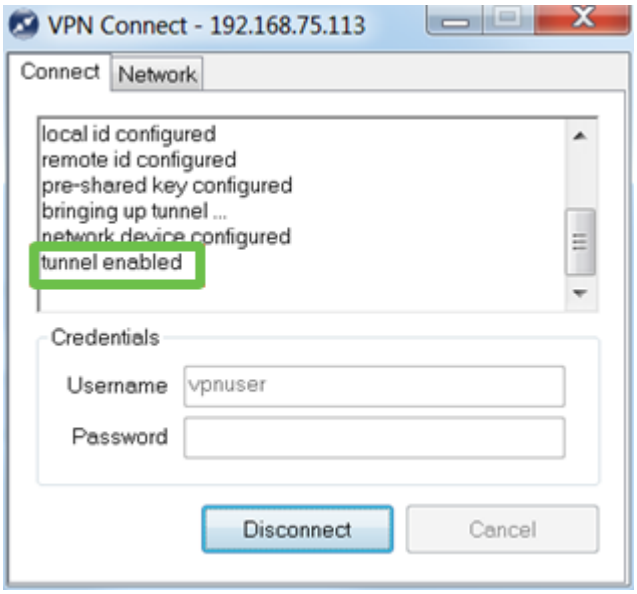


步骤 12

在出现**的VPN Connect**窗口中，使用您在RV345P上创建的**用户帐户**的凭证输入**用户名**和**密码**（步骤13和14）。 完成后，单击**Connect**。

步骤 13

验证隧道是否已连接。您应该看到隧**道已启用**。



Shrew Soft用作此配置的示例。由于Shrew Soft不是思科产品，如果您需要技术帮助，请联系此第三方。

其他VPN选项

还有一些其他使用VPN的选项。有关详细信息，请点击以下链接：

- 使用GreenBow VPN客户端连接RV34x系列路由器
- 在RV34x系列路由器上配置远程工作人员VPN客户端
- 在Rv34x系列路由器上配置点对点隧道协议(PPTP)服务器
- 在RV34x系列路由器上配置Internet协议安全(IPsec)配置文件
- 在RV34x路由器上配置L2TP WAN设置
- 在RV34x上配置站点到站点VPN

RV345P路由器的补充配置

配置VLAN（可选）

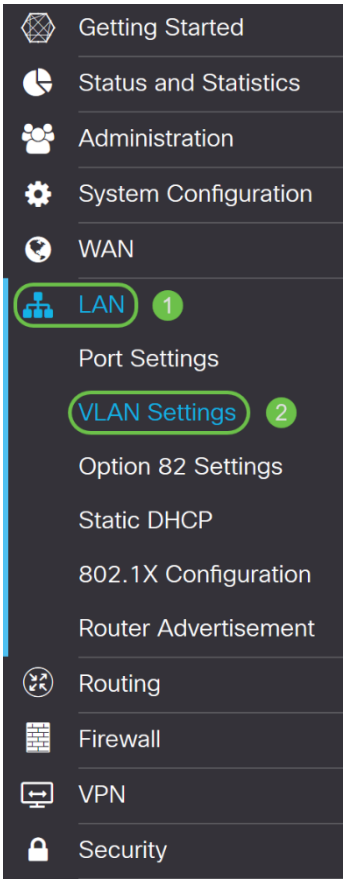
虚拟局域网(VLAN)允许您将局域网(LAN)逻辑分段到不同的广播域。在敏感数据可以在网络上广播的情况下，可以创建VLAN来通过将广播指定给特定VLAN来增强安全性。VLAN还可以通过减少向不必要目的地发送广播和组播的需求来增强性能。您可以创建VLAN，但这在VLAN至少手动或动态连接到一个端口之前不起作用。端口必须始终属于一个或多个VLAN。

您可能想要参阅VLAN最佳实践和安全提示以获得更多指导。

如果不想创建VLAN，可跳至下一节。

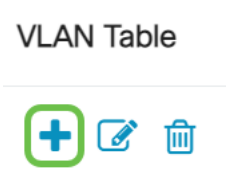
第 1 步

导航至**LAN > VLAN Settings**。



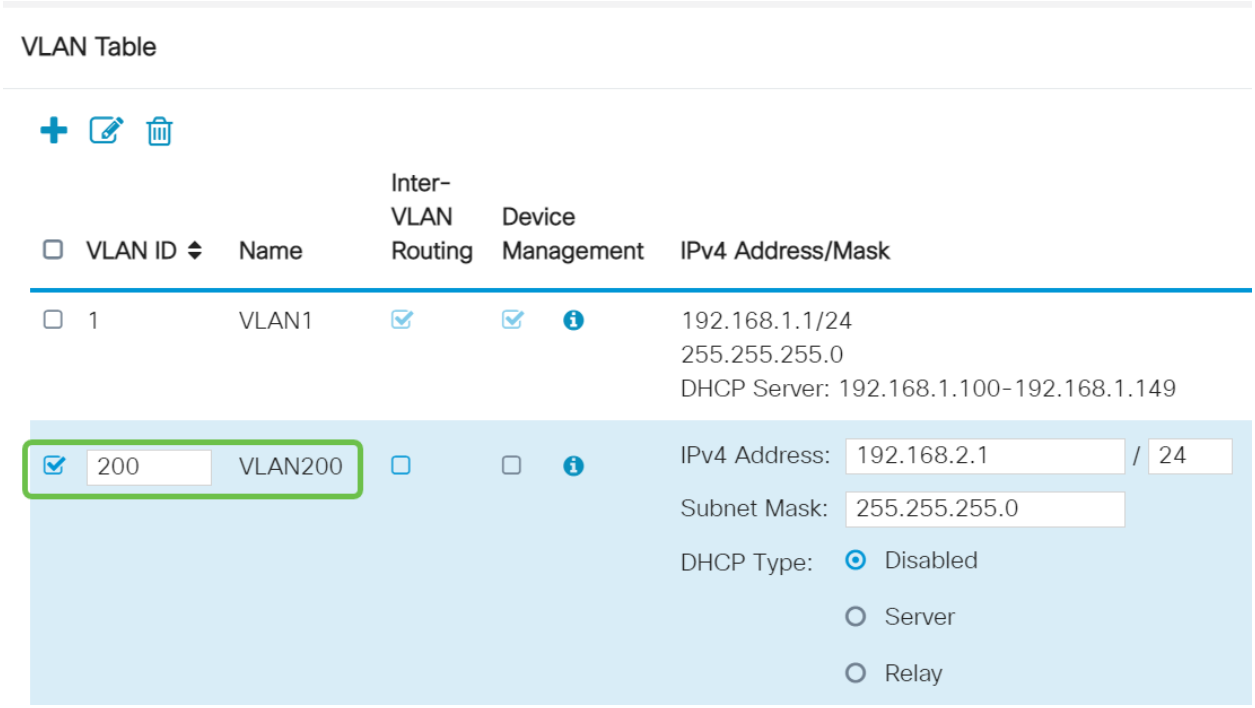
步骤 2

单击添**加图**标创建新的VLAN。



步骤 3

输入*要创*建的VLAN ID，并*输入*名称。VLAN *ID范*围为1-4093。



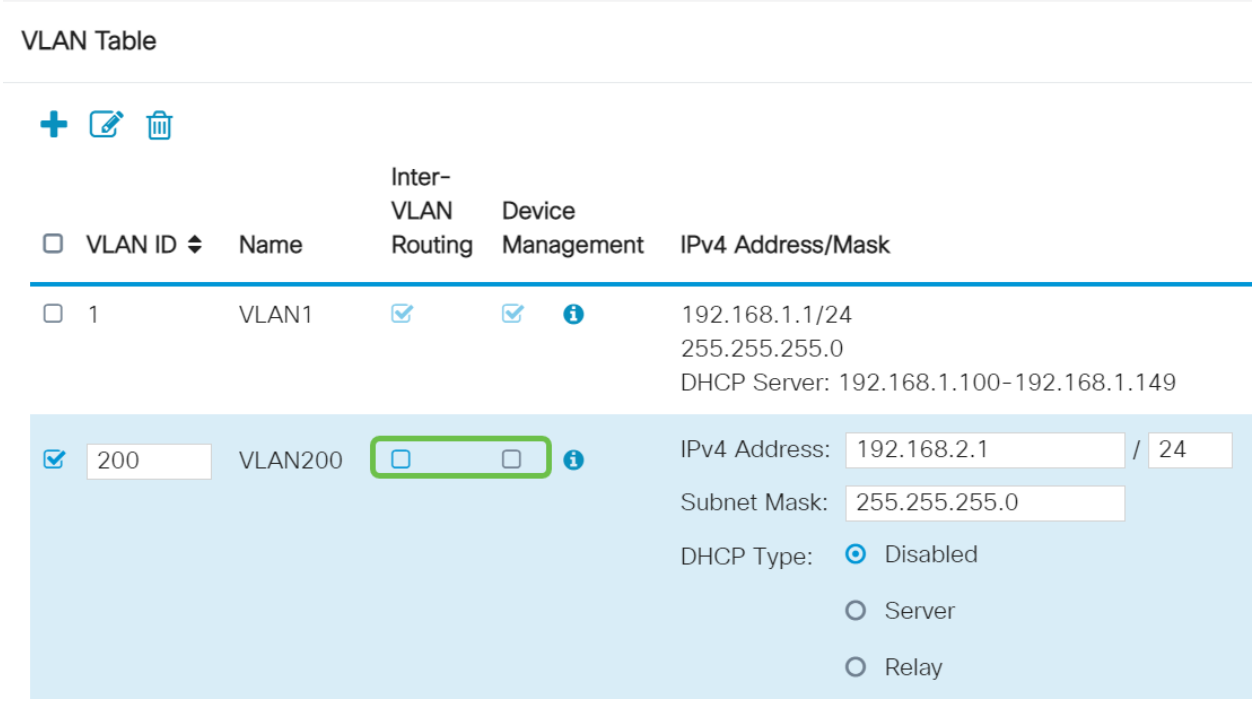
步骤 4

如果需要,*取消选*中“VLAN间路由”和“设备管理”**的“已启用”框。**VLAN间路由用于将数据包从一个VLAN路由到另一个VLAN。

通常，不建议对访客网络使用此功能，因为您希望隔离访客用户，使VLAN更不安全。有时，VLAN之间可能需要相互路由。如果出现这种情况，请选中Inter-VLAN Routing on an RV34x Router with Targeted ACL Restrictions，以配置您允许在VLAN之间传输的特定流量。

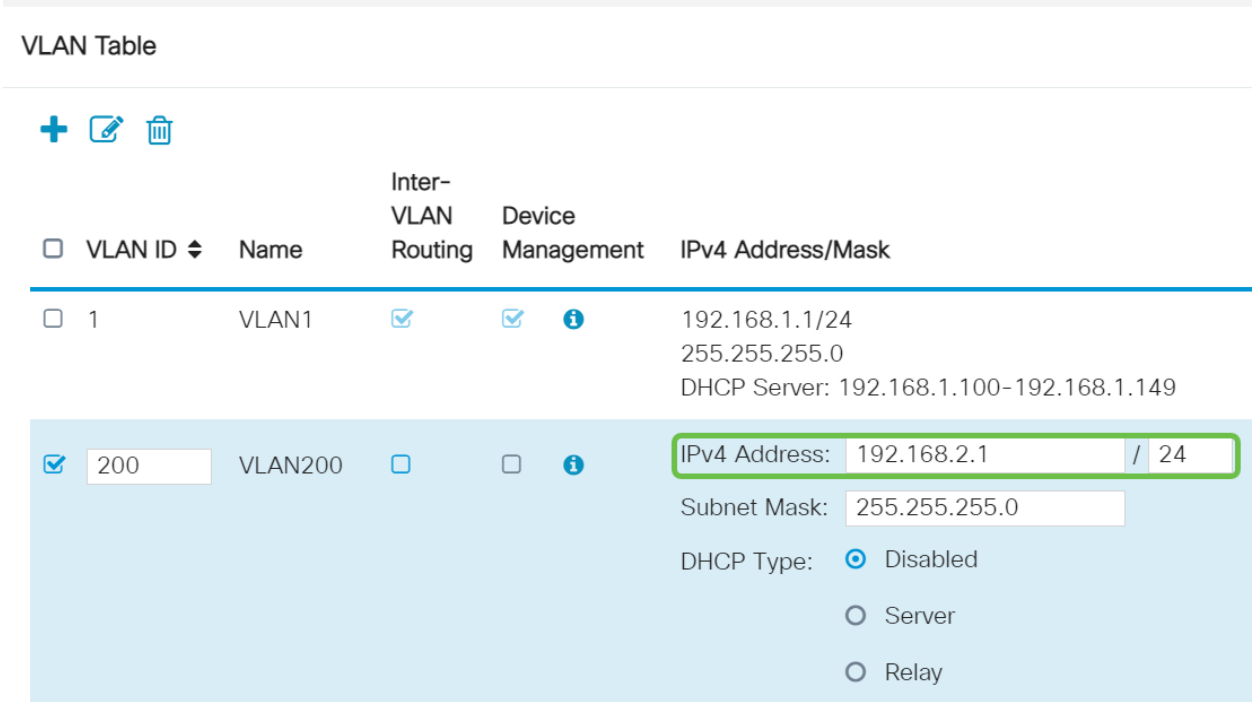
设备管理是允许您使用浏览器从VLAN登录RV345P的Web UI并管理RV345P的软件。此功能也应在访客网络上禁用。

在本示例中，我们未启用VLAN间*路由或*设备*管理*来保证VLAN的安全性。



步骤 5

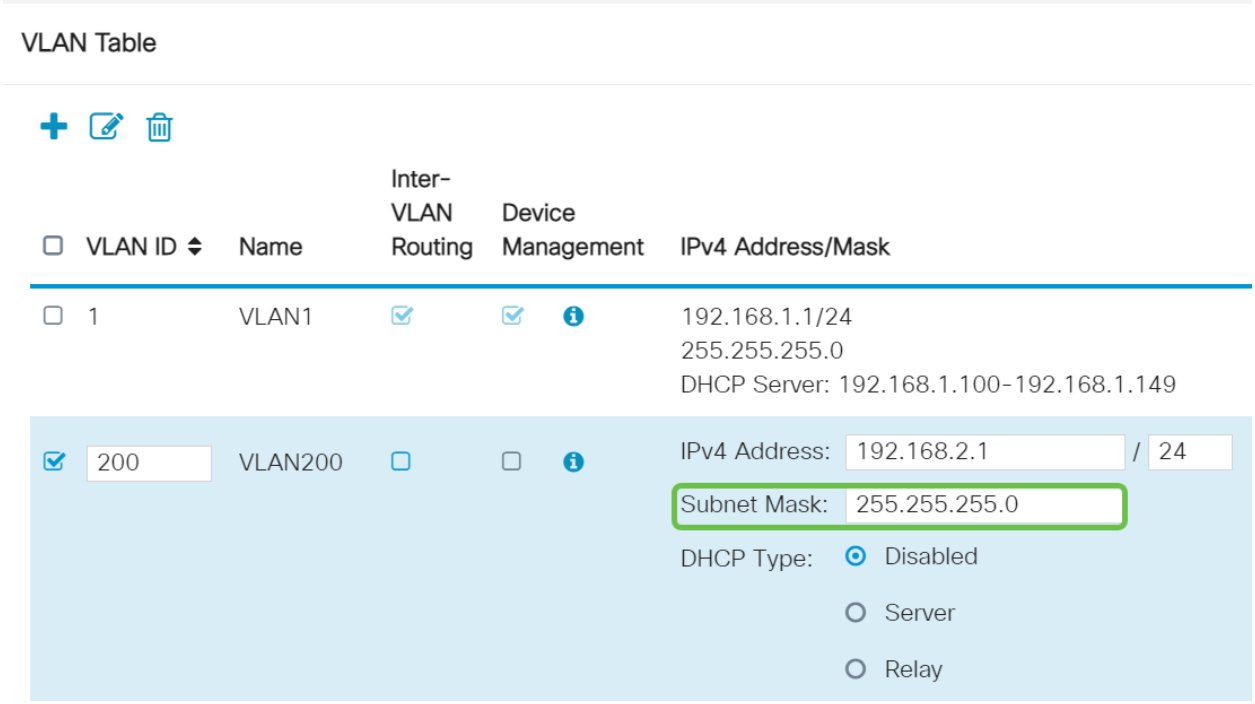
专用IPv4地址将自动填充在“IP地*址*”字段中。如果您选择，可以调整此值。在本例中，子网有192.168.2.100-192.168.2.149个IP地址可供DHCP使用。192.168.2.1-192.168.2.99和192.168.2.150-192.168.2.254可用于静态IP地址。



步骤 6

“子网掩码”下*的子网*掩码将自动填充。如果您进行更改，这将自动调整字段。

在本演示中，我们将保留*子网掩码*255.255.255.0或/24。



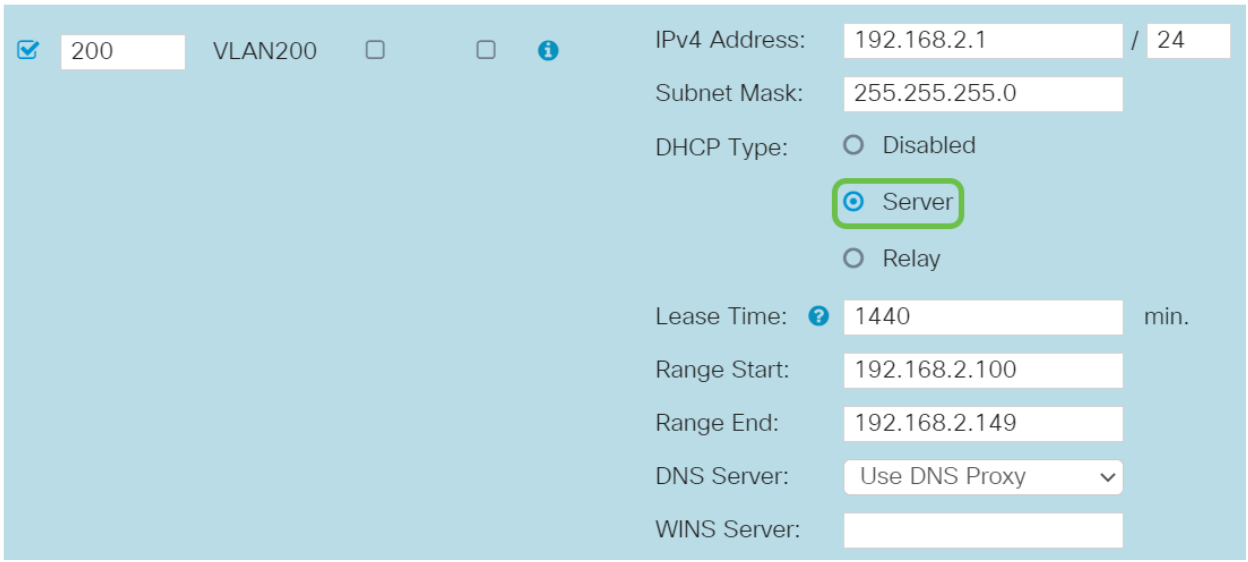
步骤 7

选择动*态主机配置协议(DHCP)类型*。以下选项为：

禁用 — 禁用VLAN上的DHCP IPv4服务器。建议在测试环境中使用。在此场景中，需要手动配置所有IP地址，并且所有通信都是内部通信。

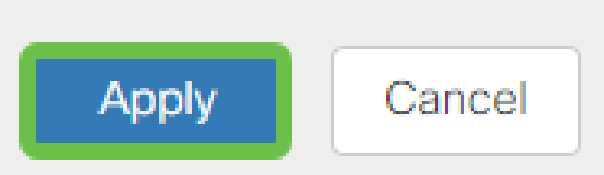
服务器 — 这是最常使用的选项。

- 租用时间 — 输入时间值5到43,200分钟。默认值为1440分钟（等于24小时）。
- 范围开始和范围结束 — 输入可动态分配的IP地址的范围开始和结束。
- DNS Server — 从下拉列表中选择将DNS服务器用作代理或从ISP使用。
- WINS服务器 — 输入WINS服务器名称。
- DHCP Options（DHCP 选项）：
  - 选项66 — 输入TFTP服务器的IP地址。
  - 选项150 — 输入TFTP服务器列表的IP地址。
  - 选项67 — 输入配置文件名。
- 中继 — 输入远程DHCP服务器IPv4地址以配置DHCP中继代理。这是更高级的配置。



步骤 8

单击**Apply**以创建新VLAN。



将VLAN分配到端口（可选）

RV345P上可以配置16个VLAN，其中一个VLAN用于广域网(WAN)。不在端口上的VLAN应被*排除*。这会将该端口上的流量保留给用户指定的VLAN/VLAN。它被视为最佳实践。

端口可以设置为接入端口或中继端口：

- 接入端口 — 分配一个VLAN。传递无标记帧。
- 中继端口 — 可以传输多个VLAN。802.1q。中继允许本征VLAN无标记。您不想在中继上使用的VLAN应排除。

一个VLAN分配了自己的端口：

- 视为接入端口。
- 分配给此端口的VLAN应标记为“未标记”。
- 对于该端口，所有其它VLAN应标记为Excluded。

共享一个端口的两个或多个VLAN:

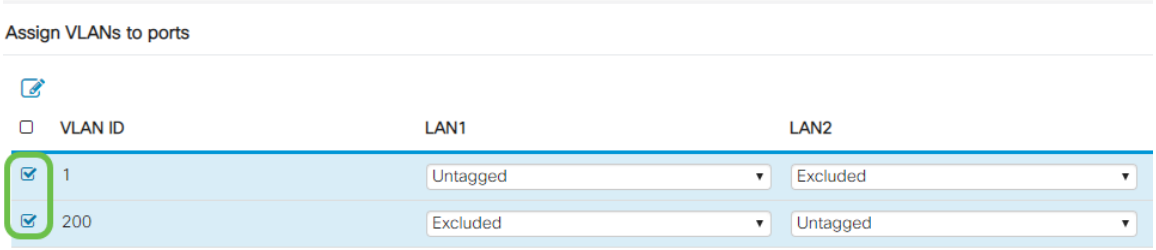
- 被视为中继端口。
- 其中一个VLAN可以标记为“未标记”。
- 属于中继端口的其余VLAN应标记为“标记”。
- 不属于中继端口的VLAN应标记为该端口的Excluded。

在本例中，没有中继。

第 1 步

选择要*编辑的*VLAN ID。

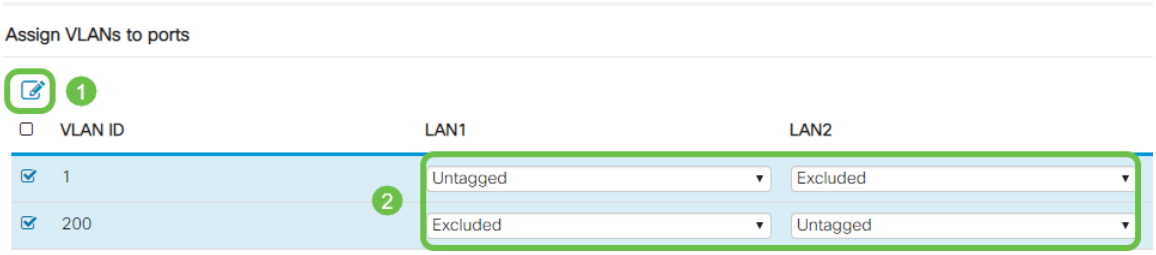
在本例中，我们选*择了*VLAN *1和VLAN 200*。



步骤 2

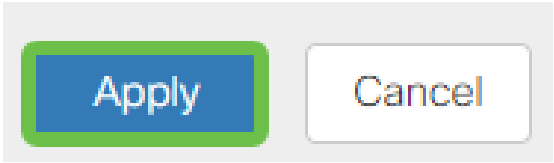
单击**Edit**将VLAN分配给LAN端口，并将每个设置指定为*Tagged*、*Untagged*或*Excluded*。

在本示例中，在LAN1上，我们将VLAN 1分配为**Untagged**，将VLAN 200分配为**Excluded**。对于LAN2，我们将VLAN 1分配为**Excluded**，将VLAN 200分配为**Untagged**。



步骤 3

单击**Apply**保存配置。



您现在应该已成功创建新VLAN，并将VLAN配置到RV345P上的端口。重复该过程以创建其他VLAN。例如，VLAN300将创建用于营销，子网为192.168.3.x，而VLAN400将创建用于子网为192.168.4.x的记帐。

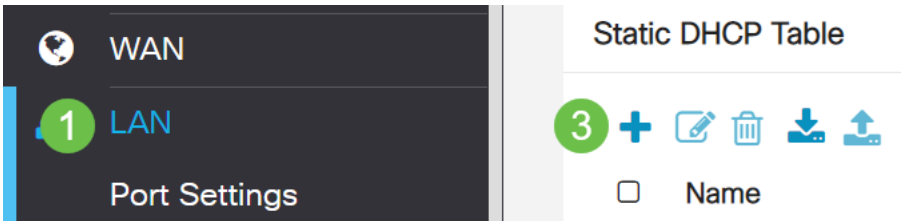
添加静态IP（可选）

如果希望某台设备可以访问其他VLAN，可以为该设备提供静态本地IP地址并创建访问规则使其可访问。仅当启用VLAN间路由时，此功能才起作用。有些情况下，静态IP可能有用。有关设置静态IP地址的详细信息，请参阅[在思科业务硬件上设置静态IP地址的最佳实践]。

如果不需要添加静态IP地址，可转到本文[的下]一部分。

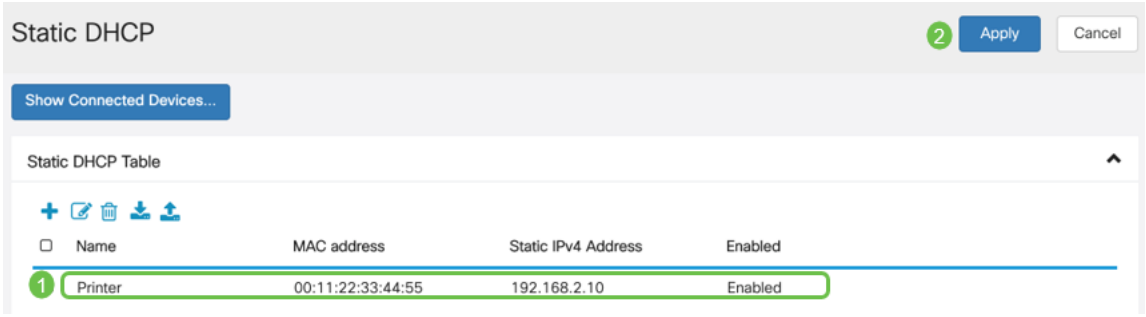
第 1 步

导航至**LAN > Static DHCP**。单击加号**图标**。



步骤 2

添加设**备的静**态DHCP信息。在本例中，设备是打印机。



管理证书（可选）

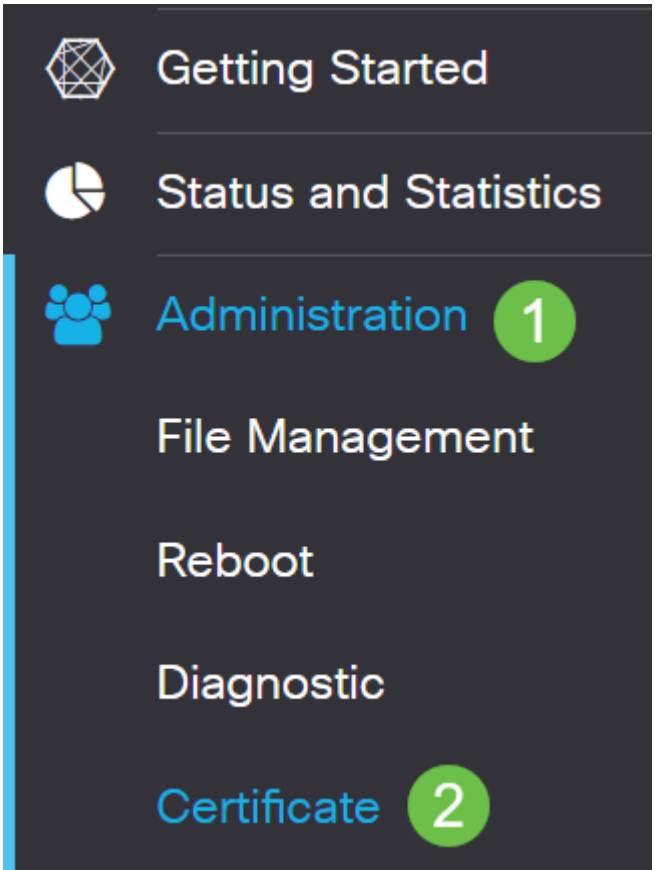
数字证书通过证书的指定主题对公钥的所有权进行认证。这允许依赖方依赖由私钥所作的签名或断言，该私钥对应于经认证的公钥。路由器可以生成自签名证书，即由网络管理员创建的证书。它还可以向证书颁发机构(CA)发出申请数字身份证书的请求。从第三方应用获得合法证书非常重要。

证书颁发机构(CA)用于身份验证。可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。

生成CSR/证书

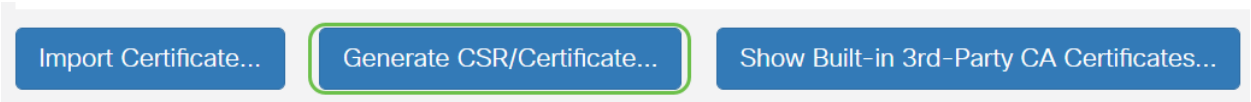
第 1 步

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。

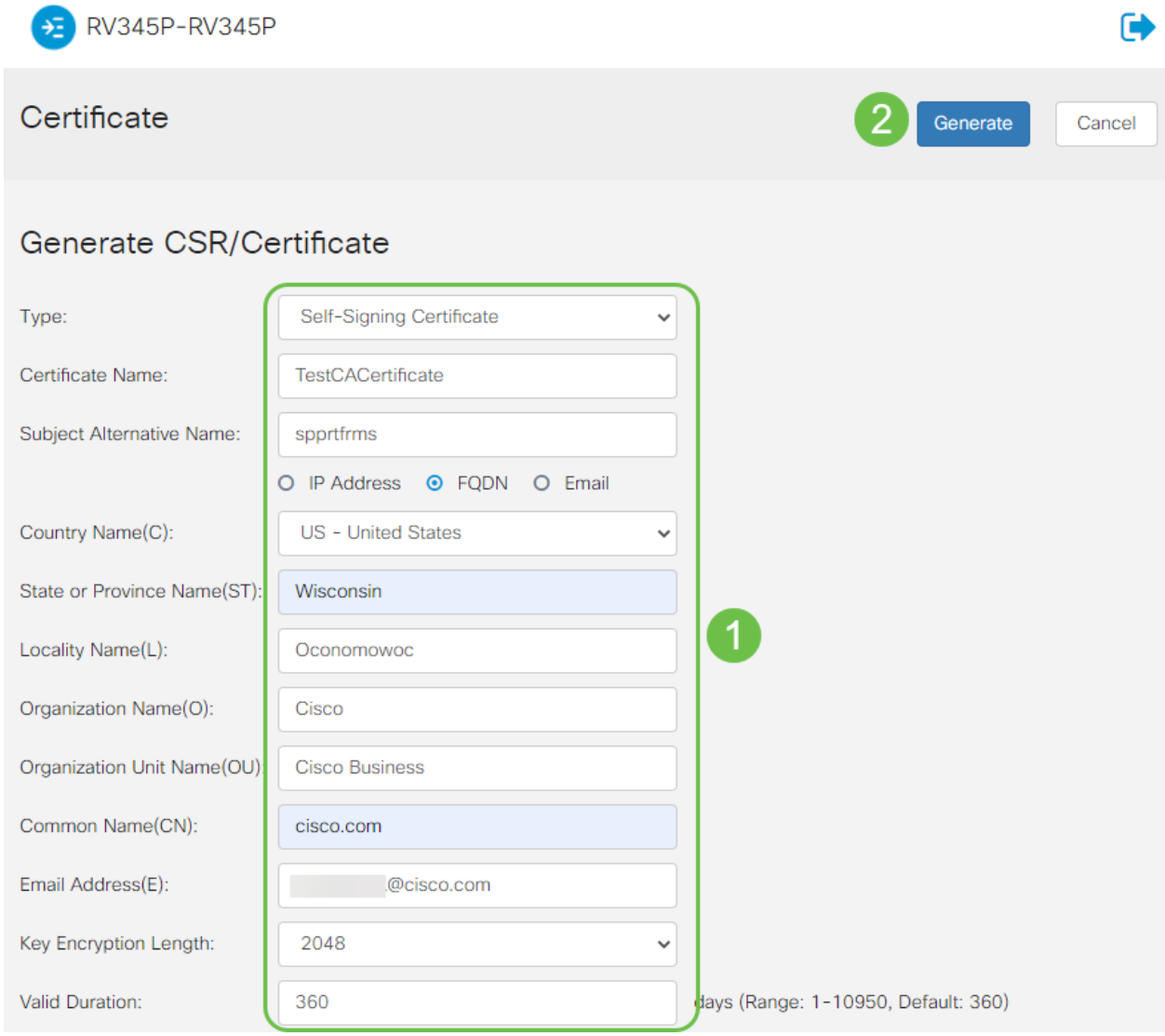


步骤 3

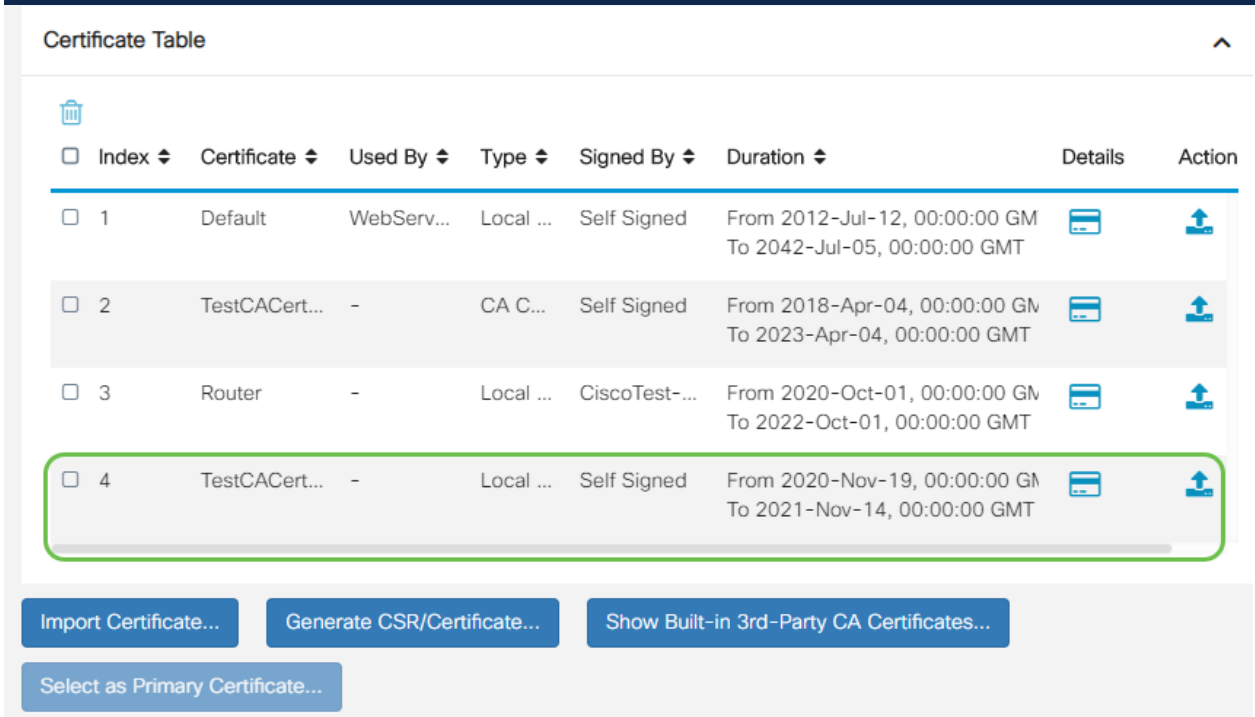
用以下内容填写框：

- 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Subject Alternative Name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。
- 在省或省名称(ST)字段中输入贵组织所在州、省、地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所在的地区或城市的名称。
- 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，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(Valid Duration)字段中，输入证书的有效天数。默认值为 360。
- 单击生成。



生成的证书现在应显示在证书表中。

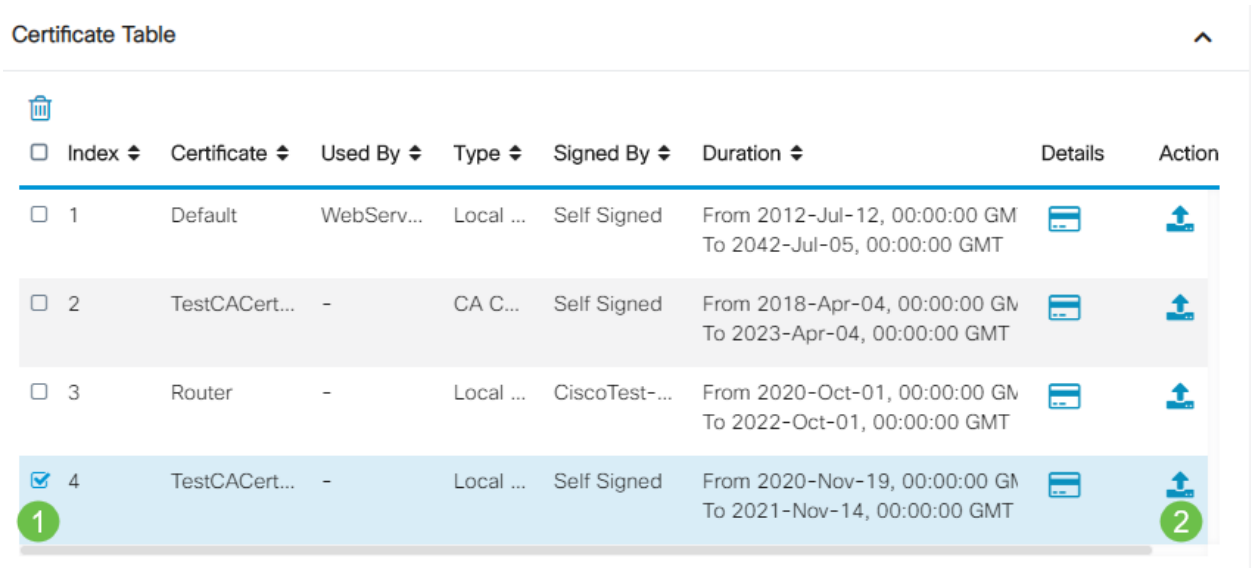


您现在应该已在RV345P路由器上成功创建证书。

导出证书

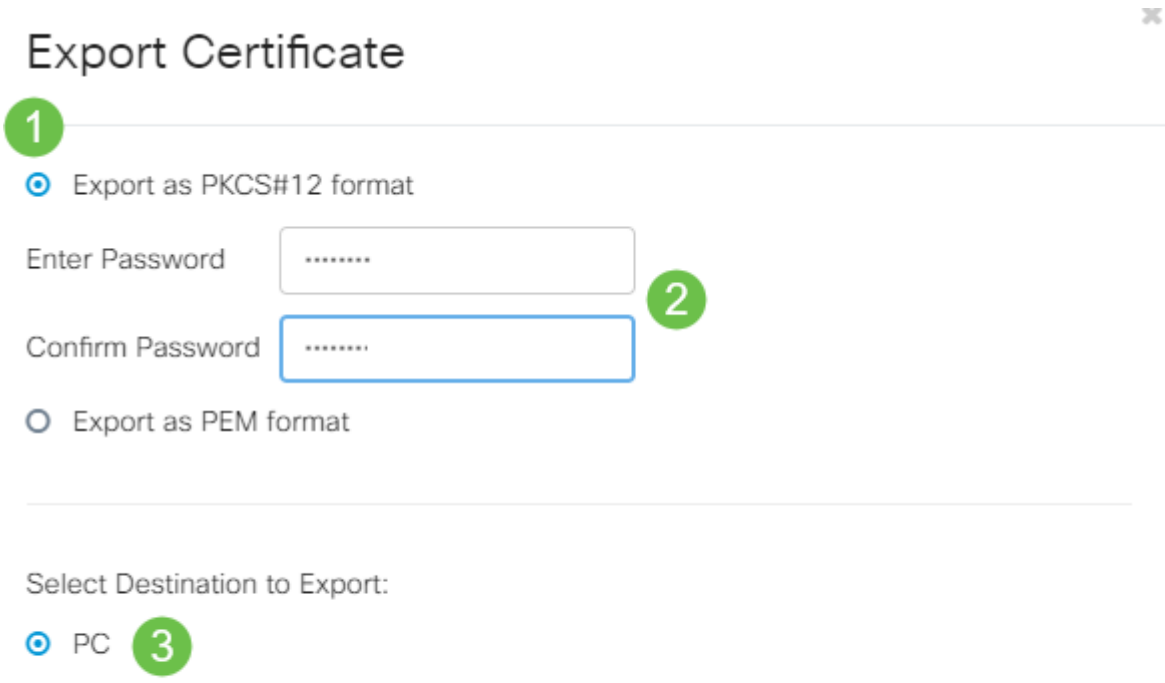
第 1 步

在证书表中，勾选要导出的证书的复选框，然后单击导**出图标**。



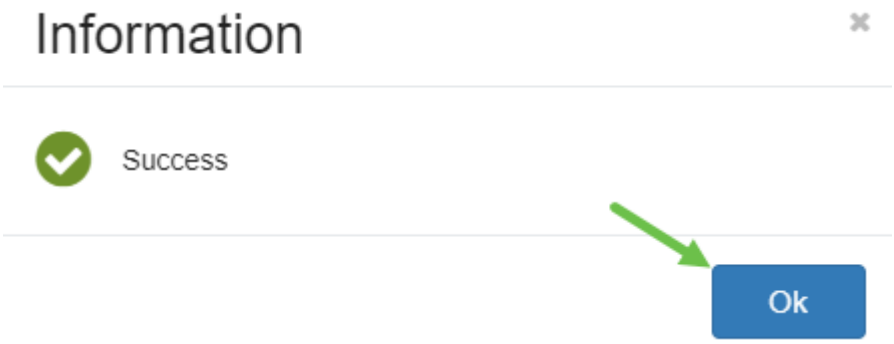
步骤 2

- 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.

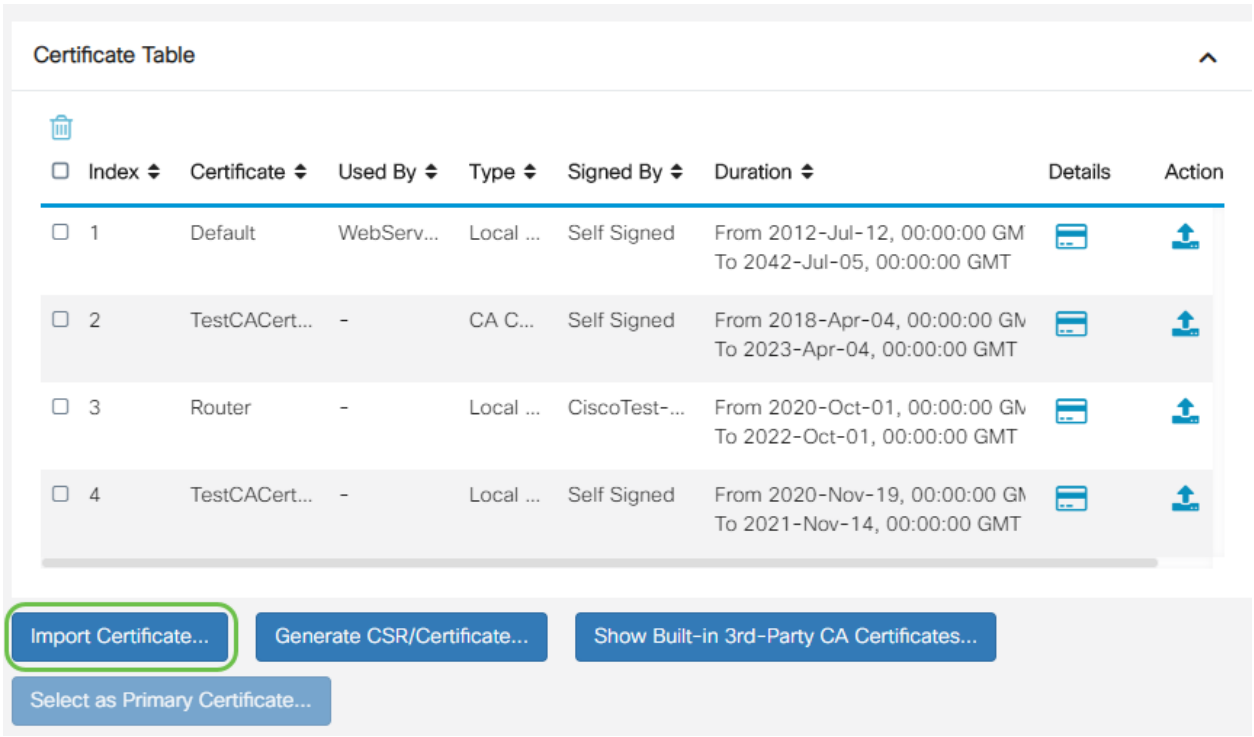


您现在应该已成功导出RV345P系列路由器上的证书。

导入证书

第 1 步

单击“**Import Certificate...**”。



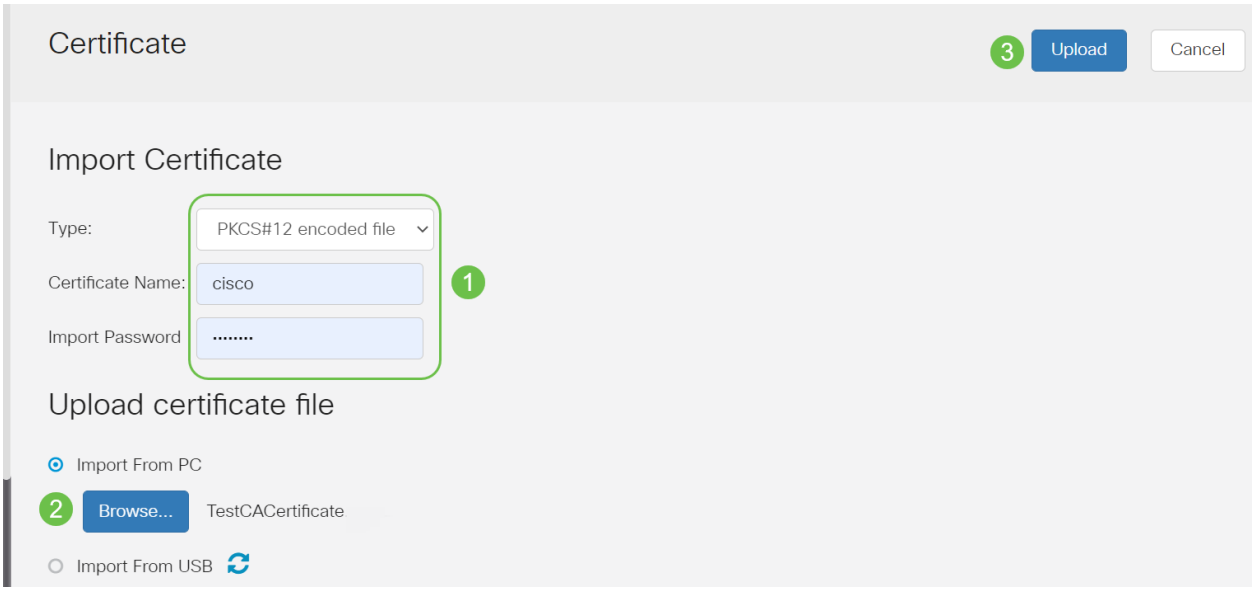
步骤 2

- 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字段中为文件输入密码。否则，请跳至步骤

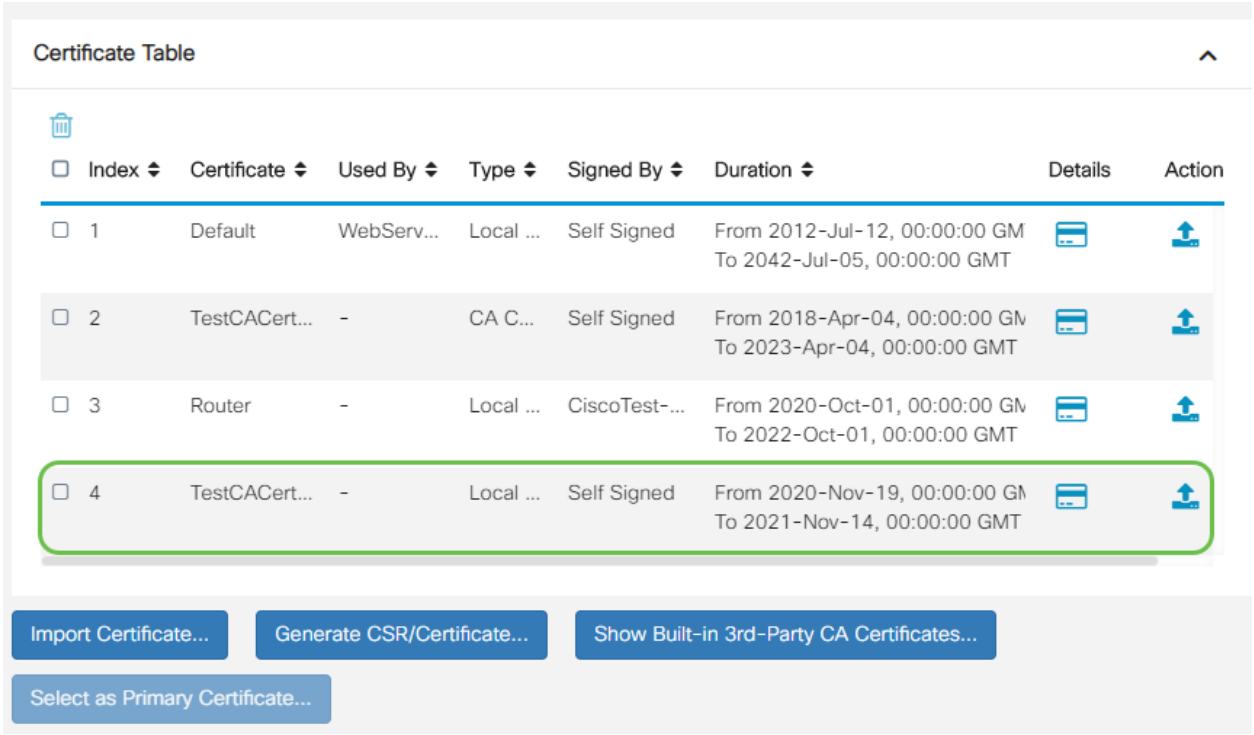
3。

- 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RV345P路由器上导入证书。

使用Dongle和RV345P系列路由器配置移动网络（可选）

您可能希望使用转换器和RV345P路由器配置备份移动网络。如果是这种情况，您应阅

读“Configure a Mobile Network Using a Dongle an RV34x Series Router（使用Dongle和RV34x系列路由器配置移动网络）”。

祝贺您，您已完成RV345P路由器的配置！您现在将配置您的思科企业无线设备。

配置CBW140AC

CBW140AC开箱即用

首先将以太网电缆从CBW140AC的PoE端口插入RV345P的PoE端口。RV345P的前4个端口可以提供PoE，因此可以使用其中任何一个端口。

检查指示灯的状态。接入点启动大约需要10分钟。LED会以多种模式闪烁绿色，快速交替通过绿色、红色和琥珀色，然后再次变为绿色。LED颜色强度和色相在单元之间可能有小的变化。当LED指示灯呈绿色闪烁时，请继续下一步。

主AP上的PoE以太网上行链路端口只能用于提供到LAN的上行链路，不能连接到任何其他支持主AP或网状扩展器的设备。

如果您的接入点不是新的，开箱即用，请确保将其重置为出厂默认设置，以便*CiscoBusiness-Setup* SSID显示在您的Wi-Fi选项中。有关此方面的帮助，请选中How to Reboot and Reset to Factory Default Settings on RV345x Routers。

在Web UI上设置140AC主无线接入点

您可以使用移动应用或Web UI设置接入点。本文使用Web UI进行设置，这为配置提供了更多选项，但稍为复杂。如果您想在下一部分使用移动应用，请单击以访问移动应用说明。

如果连接时出现问题，请参阅本文的无线故障排除提示部分。

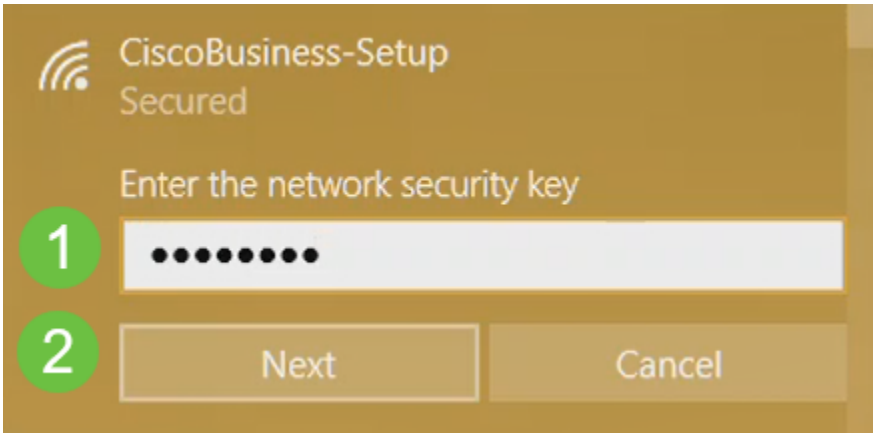
第 1 步

在PC上，单击Wi-Fi**图标，然**后选*择CiscoBusiness-Setup*无线网络。单击 Connect。

如果您的接入点不是新的，开箱即用，请确保将其重置为出厂默认设置，以便*CiscoBusiness-Setup* SSID显示在您的Wi-Fi选项中。

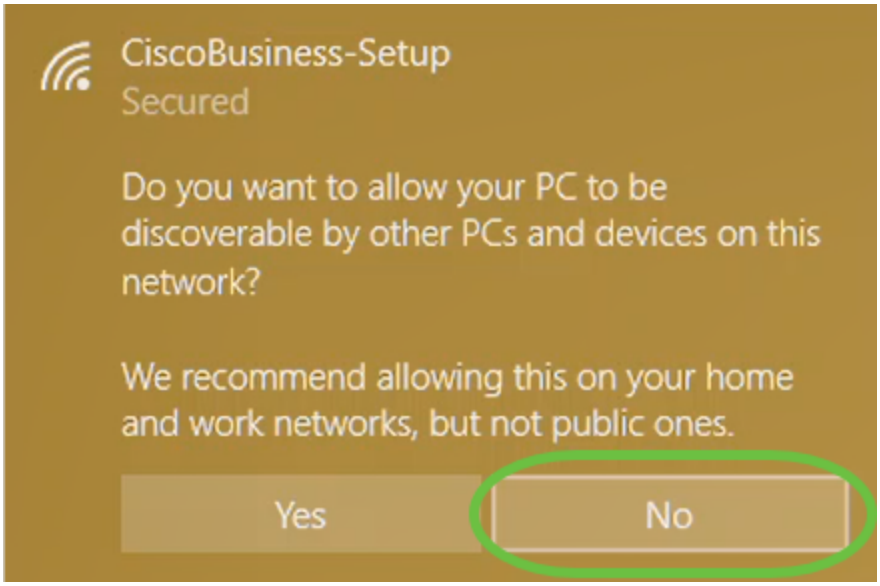
步骤 2

输入口令**cisco123**,然后单**击Next**。



步骤 3

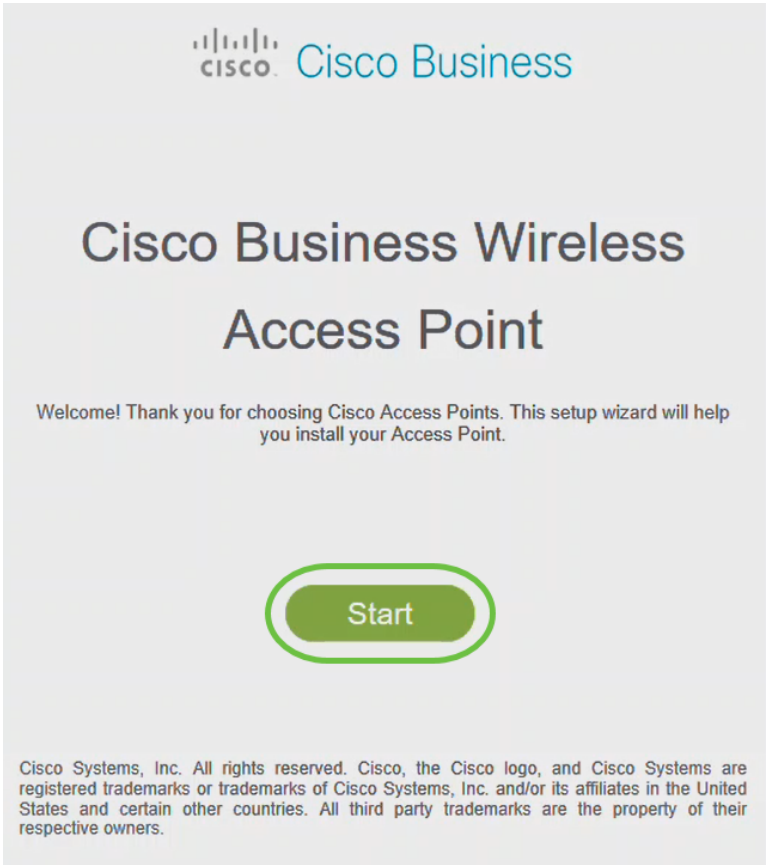
您将看到以下屏幕。由于一次只能配置一台设备，请单击**否**。



只能将一台设备连接到*CiscoBusiness-Setup* SSID。如果另一台设备尝试连接，则无法连接。如果无法连接到SSID并且已验证了密码，则可能是其他某台设备进行了连接。重新启动AP并重试。

步骤 4

连接后，Web浏览器应自动重定向到CBW AP设置向导。否则，请打开Web浏览器，例如Internet Explorer、Firefox、Chrome或Safari。在地址栏中，键入**http://ciscobusiness.cisco**并按**Enter**。单击**Start**在网页上。



如果您未看到网页，请再等几分钟或重新加载页面。完成初始设置后，您将使用

https://ciscobusiness.cisco登录。如果Web浏览器自动填充 *http://*，则需要手动键入 *https://*以获取访问权限。

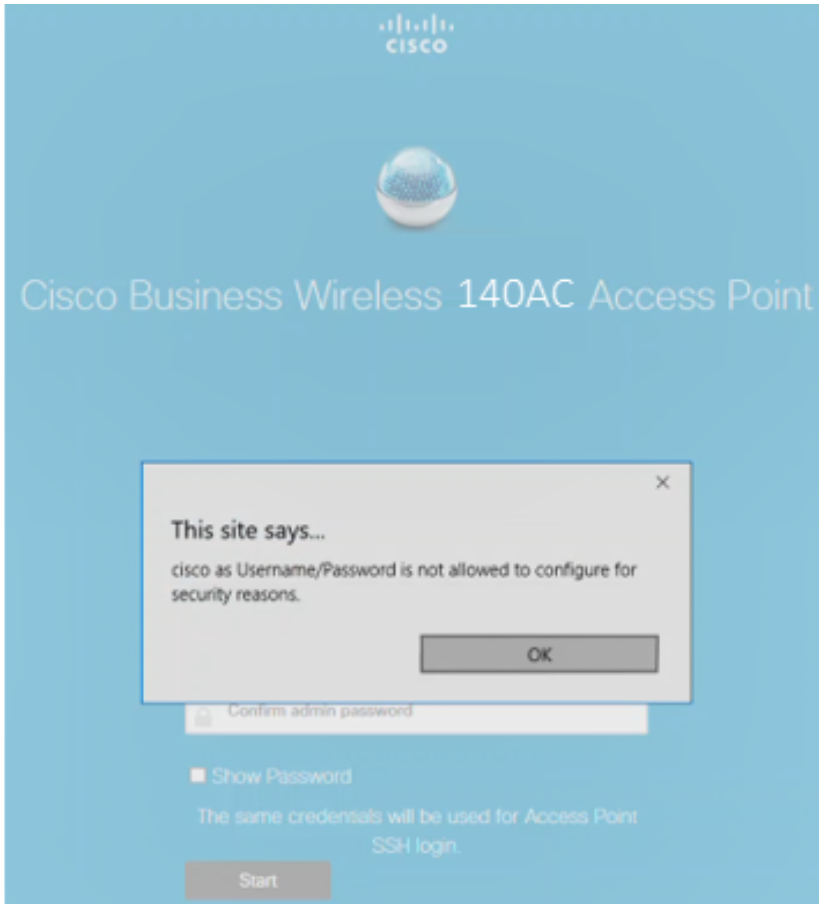
步骤 5

通过输入以下内容创建管理员帐户：

- 管理员用户名（最多24个字符）
- Admin 密码
- 确认 Admin 密码

您可以通过选中“显示密码”旁的复选框来选择显示密码。单击开始。

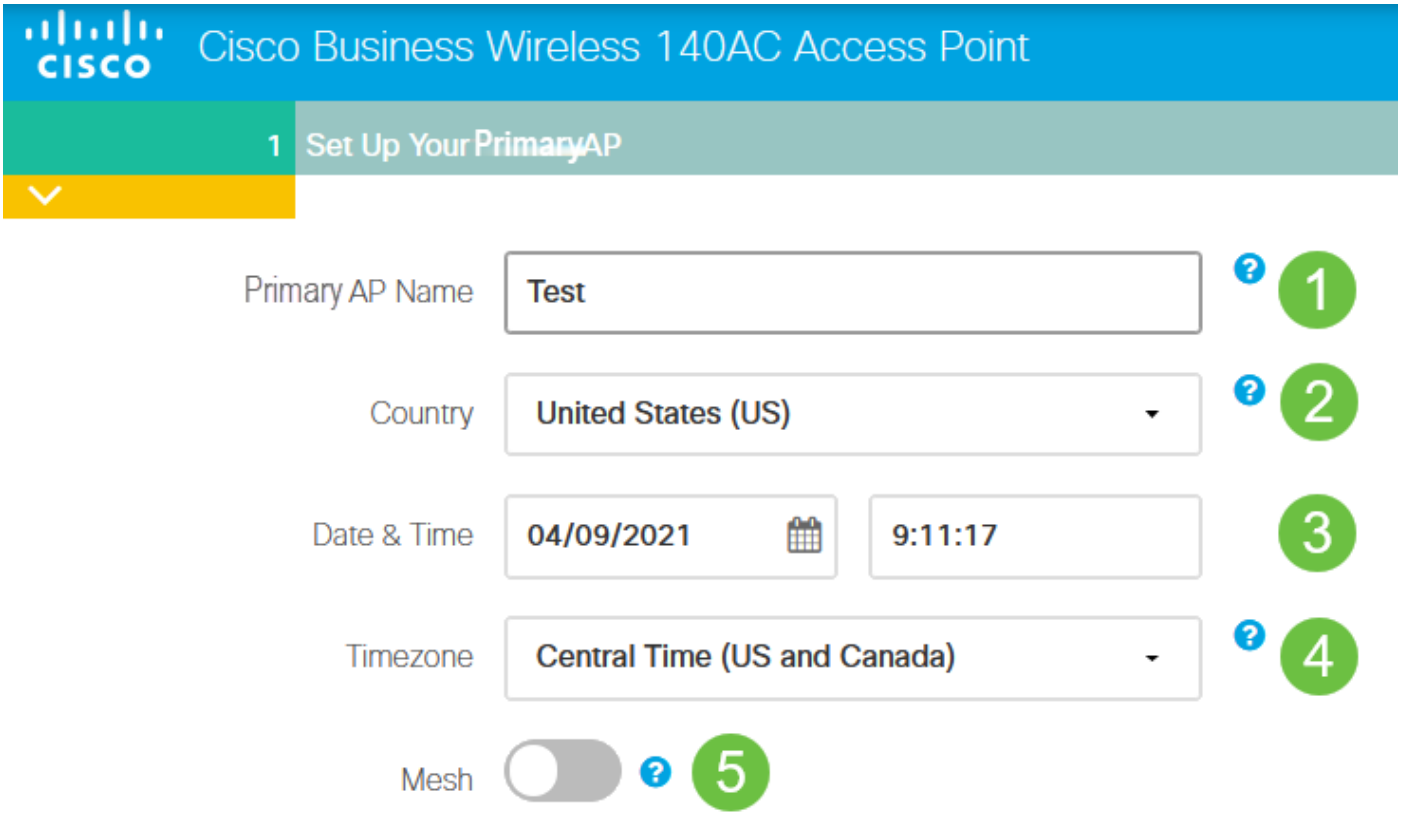
请勿在用户名或密码字段中使用*cisco*或其变体。如果您这样做，您将收到错误消息，如下所示。



步骤 6

*通过输入以下命令*设置主AP:

- 主AP名称
- 国家/地区
- 日期和时间
- 时区
- 网状



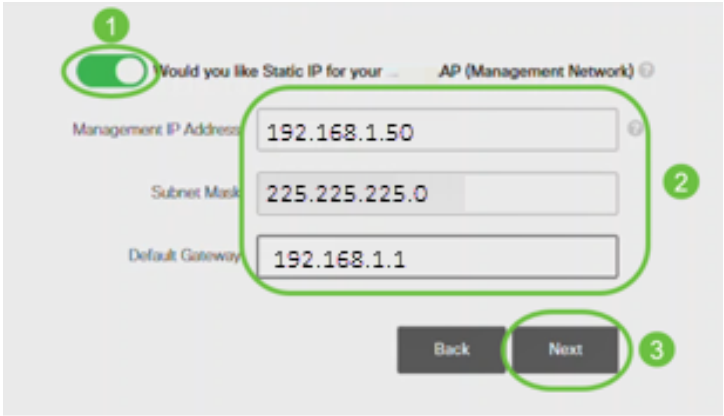
*仅当*您计划创建网状网络时，才应启用网状网。默认情况下，它处于禁用状态。

步骤 7

（可选）您可以为*CBW140AC启用*静态IP以用于管理。否则，接口将从DHCP服务器获取IP地址。要配置静态IP，请输入以下命令：

- 管理 IP 地址
- 子网掩码
- 默认网关

单击 Next。



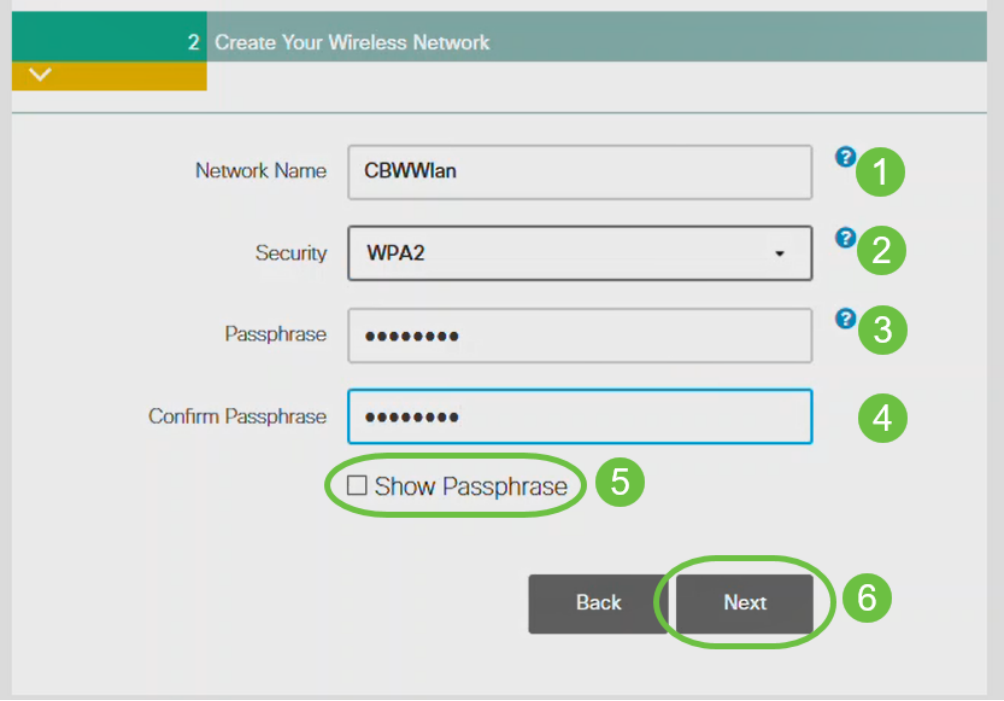
默认情况下，此选项处于禁用状态。

步骤 8

通过输入以下命令创建您的无线网络：

- 网络名称
- 选择安全
- 密码
- 确认密码
- （可选）选中复选框以显示密码短语。

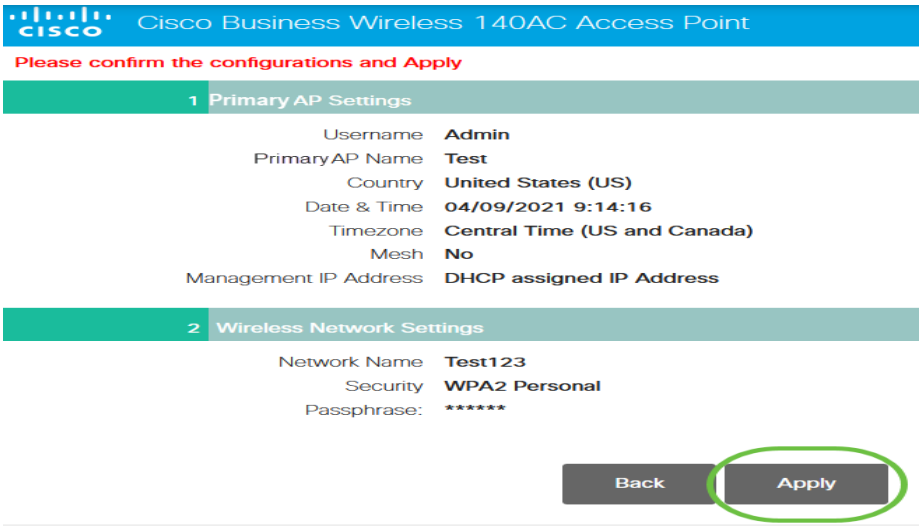
单击 Next。



Wi-Fi保护访问(WPA)第2版(WPA2)是Wi-Fi安全的当前标准。

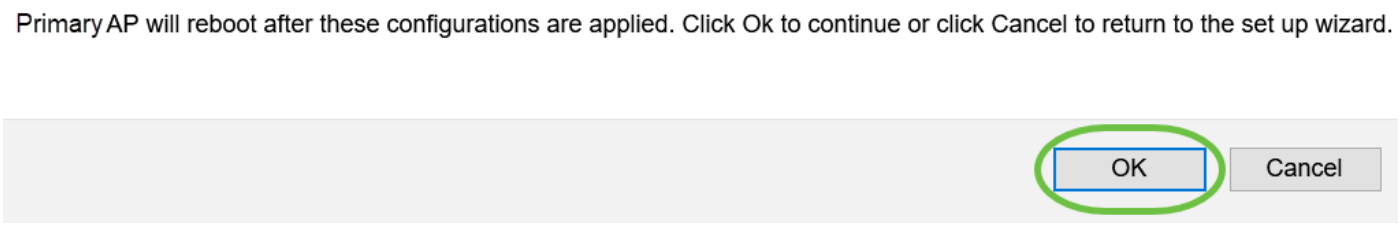
步骤 9

确认设置并单击“**Apply**”。

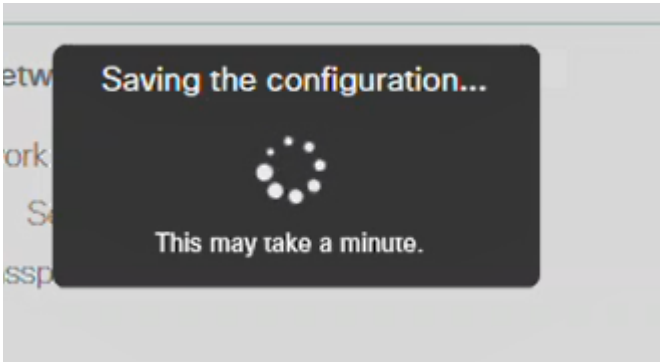


步骤 10

单击**OK**以应用设置。



保存配置并重新启动系统时，您将看到以下屏幕。这可能需要10分钟。

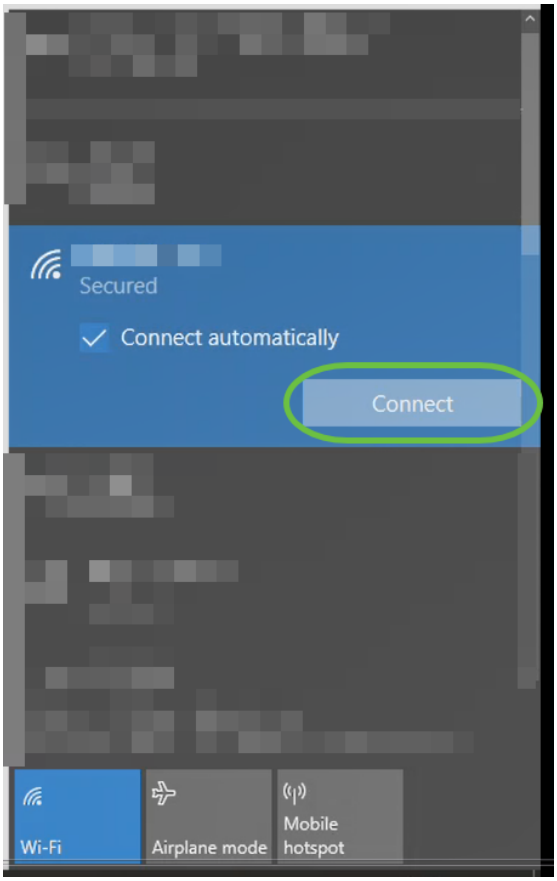


在重新启动期间，接入点中的LED将经过多种颜色模式。当LED呈绿色闪烁时，请继续下一步。如果LED未通过红色闪烁模式，则表明您的网络中没有DHCP服务器。确保AP连接到交换机或具有DHCP服务器的路由器。

步骤 11

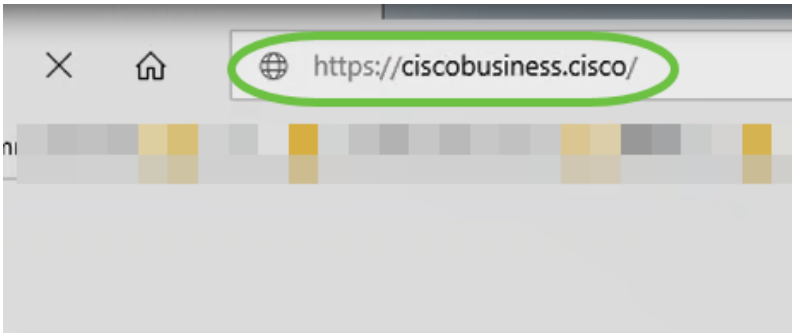
转到PC上的无线选项，选择您配置的网络。单击 Connect。

重新*启动后*，CiscoBusiness-Setup SSID将消失。



步骤 12

打开Web浏览器并键入*https:///[CBW AP的IP地址]*。或者，您可以在地址栏中键入https://ciscobusiness.cisco并按Enter键。



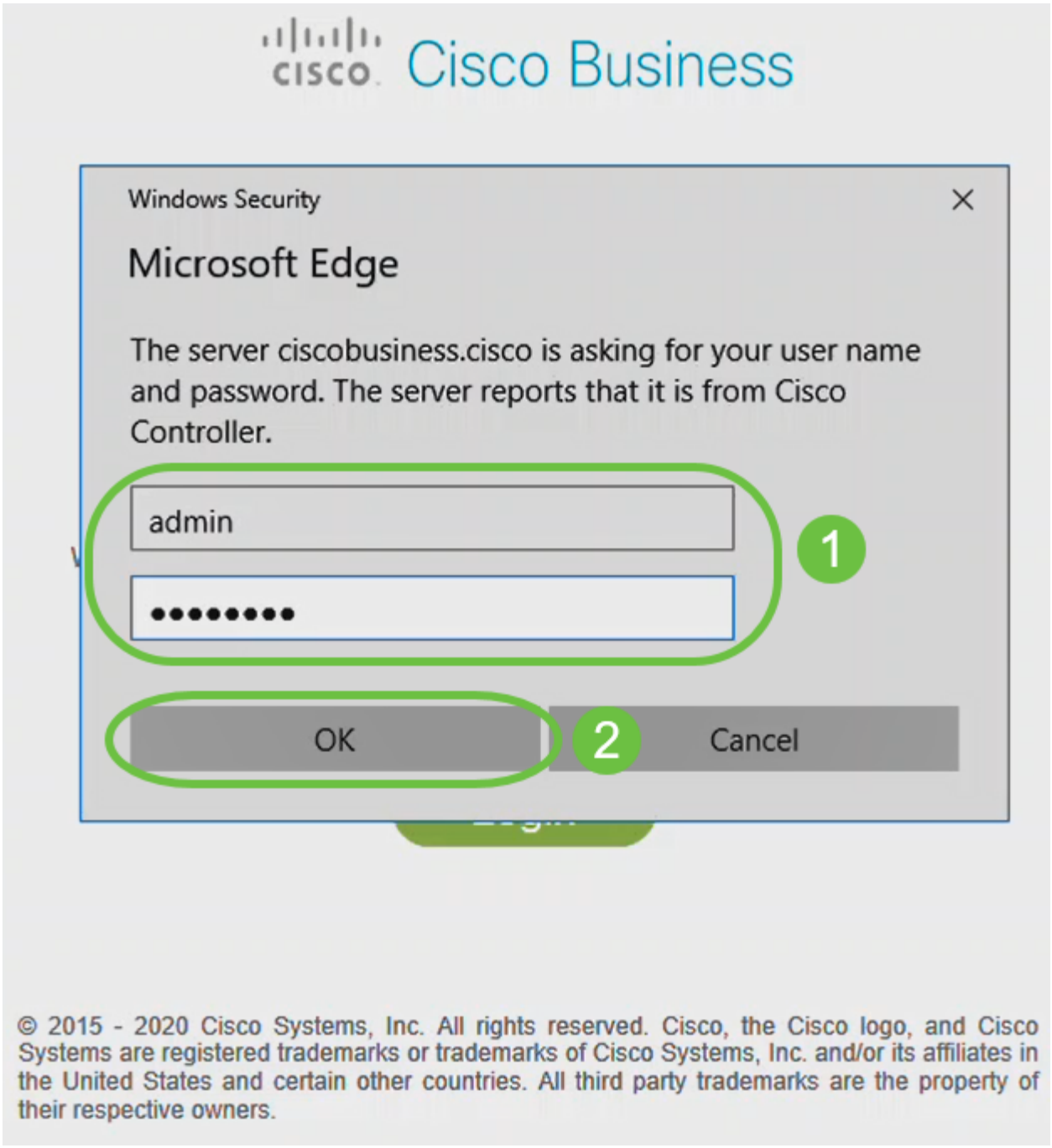
确保在此步骤中 *键入*https， *而*不键入http。

步骤 13

单击 Login。

步骤 14

使用已配置的凭证登录。Click OK.



步骤 15

您将能够访问AP的Web UI页面。

无线故障排除提示

如果您有任何问题，请查看以下提示：

- 确保选择了正确的服务集标识符(SSID)。这是您为无线网络创建的名称。
- 断开移动应用或笔记本电脑的任何VPN连接。您甚至可能连接到移动服务提供商使用的VPN，而您甚至可能不知道该VPN。例如，Android(Pixel 3)手机（Google Fi作为服务提供商）有一个内置VPN，可自动连接，无需通知。要查找主AP，需要禁用此功能。
- 使用https://<主AP的IP地址>登录主AP。
- 完成初始设置后，无论您是登录到*ciscobusiness.cisco*，还是在Web浏览器中输入IP地址，都确保使用https://。根据您的设置，您的计算机可能已自动填充http://，因为这是您首次登录时使用的。
- 要帮助解决在使用AP期间访问Web UI或浏览器问题相关的问题，请在Web浏览器（本例中为Firefox）中单击“打开”菜单，转到“帮助”>“故障排除信息”，然后单击“刷新Firefox”。

使用Web UI配置CBW142ACM网状扩展器

您正处于设置此网络的起点，只需添加网状扩展器！

第 1 步

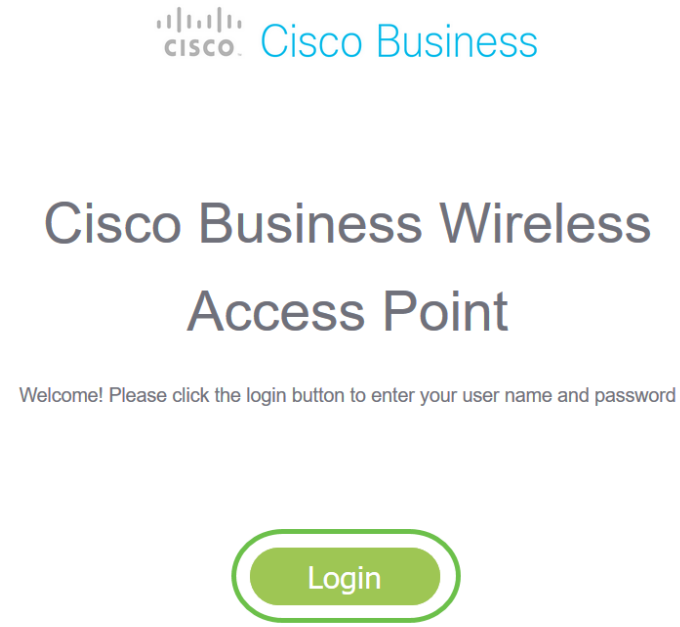
将两个网状扩展器插入选定位置的壁中。写下每个网状扩展器的MAC地址。

步骤 2

等待约10分钟，使网状扩展器启动。

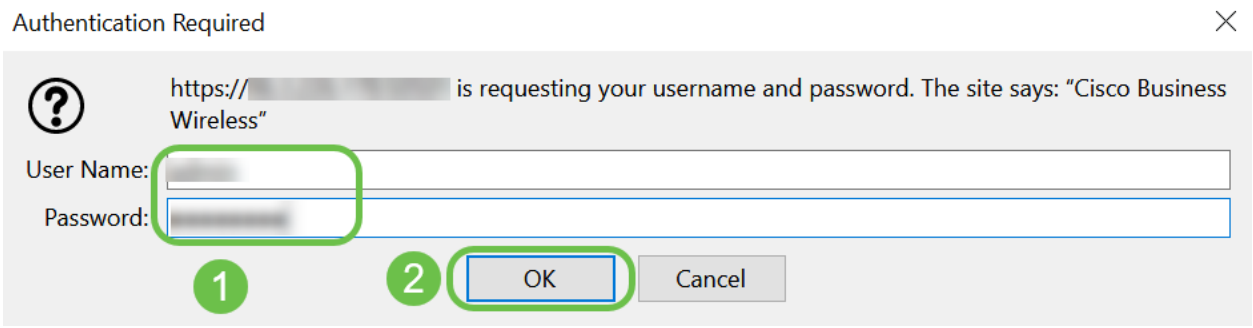
步骤 3

在Web浏览器上输入主接入点(AP)IP地址。单击**Login**访问主AP。



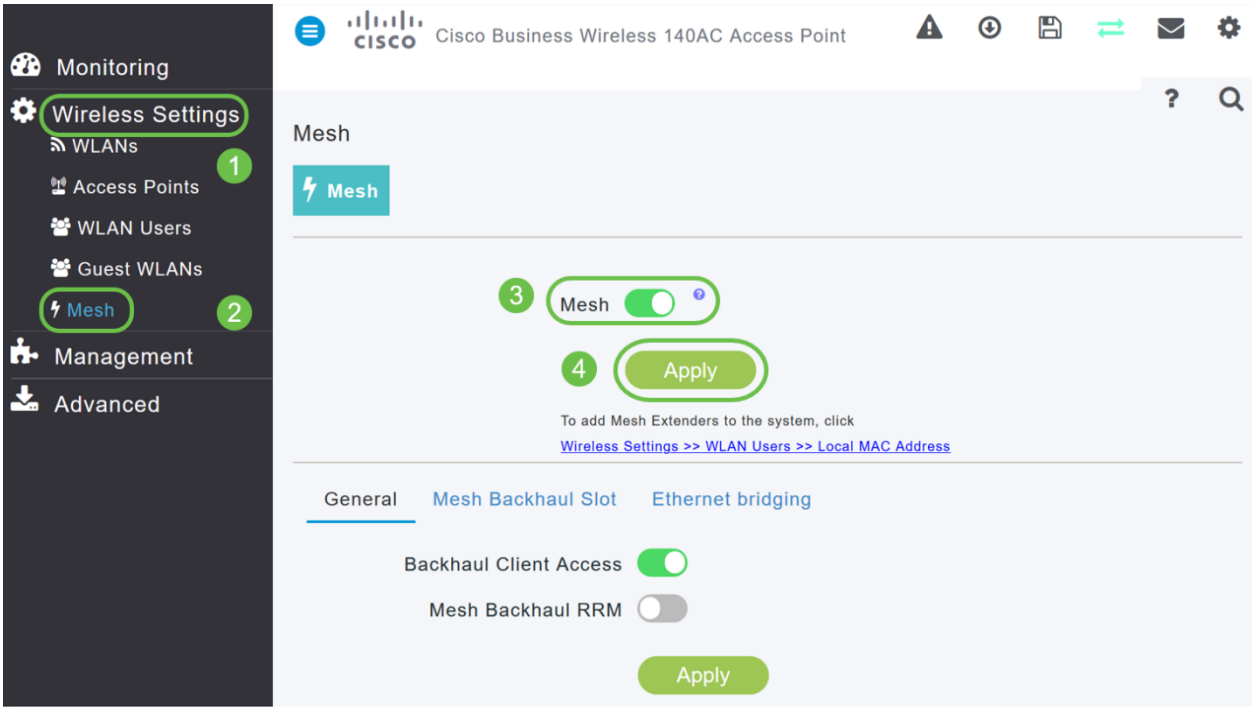
步骤 4

输入您*的用户*名和*密*码凭据以访问主AP。Click OK.



步骤 5

导航至**无线设置>网状**。确保网状*网已*启用。单击 Apply。

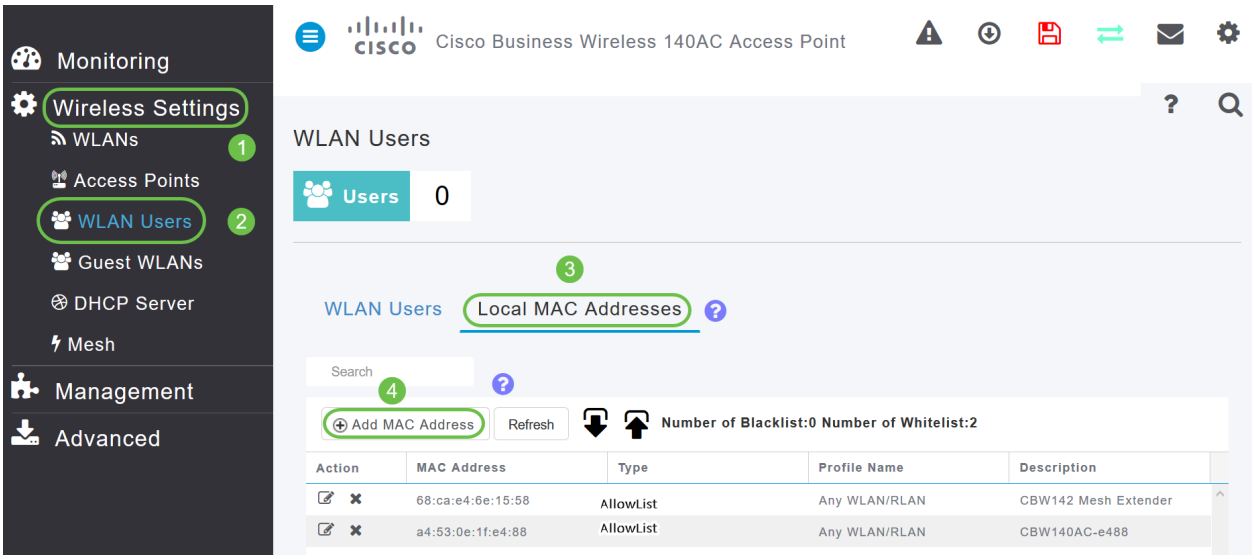


步骤 6

如果网状网尚未启用，则WAP可能需要执行重新启动。弹出窗口将显示为重新启动。确认。这大约需要10分钟。在重新启动期间，LED会以多种模式闪烁绿色，快速交替通过绿色、红色和琥珀色，然后再次变为绿色。LED颜色强度和色相在单元之间可能有小的变化。

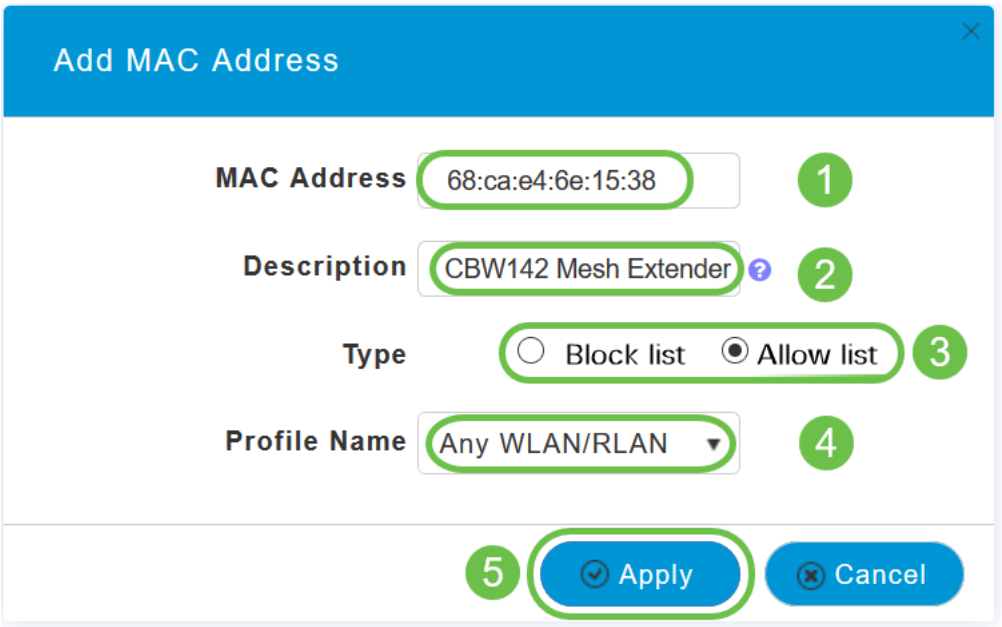
步骤 7

导航至**Wireless Settings > WLAN Users > Local MAC Addresses**。单击**Add MAC Address**。



步骤 8

输入网状扩展器的MAC地址和说明。选择“*Type as* Allow”列表。从下拉菜*单中选*择配置文件名称。单击 Apply。



步骤 9

请务必按屏幕右上窗格**上的**“保存”图标保存所有配置。

对每个网状扩展器重复此步骤。

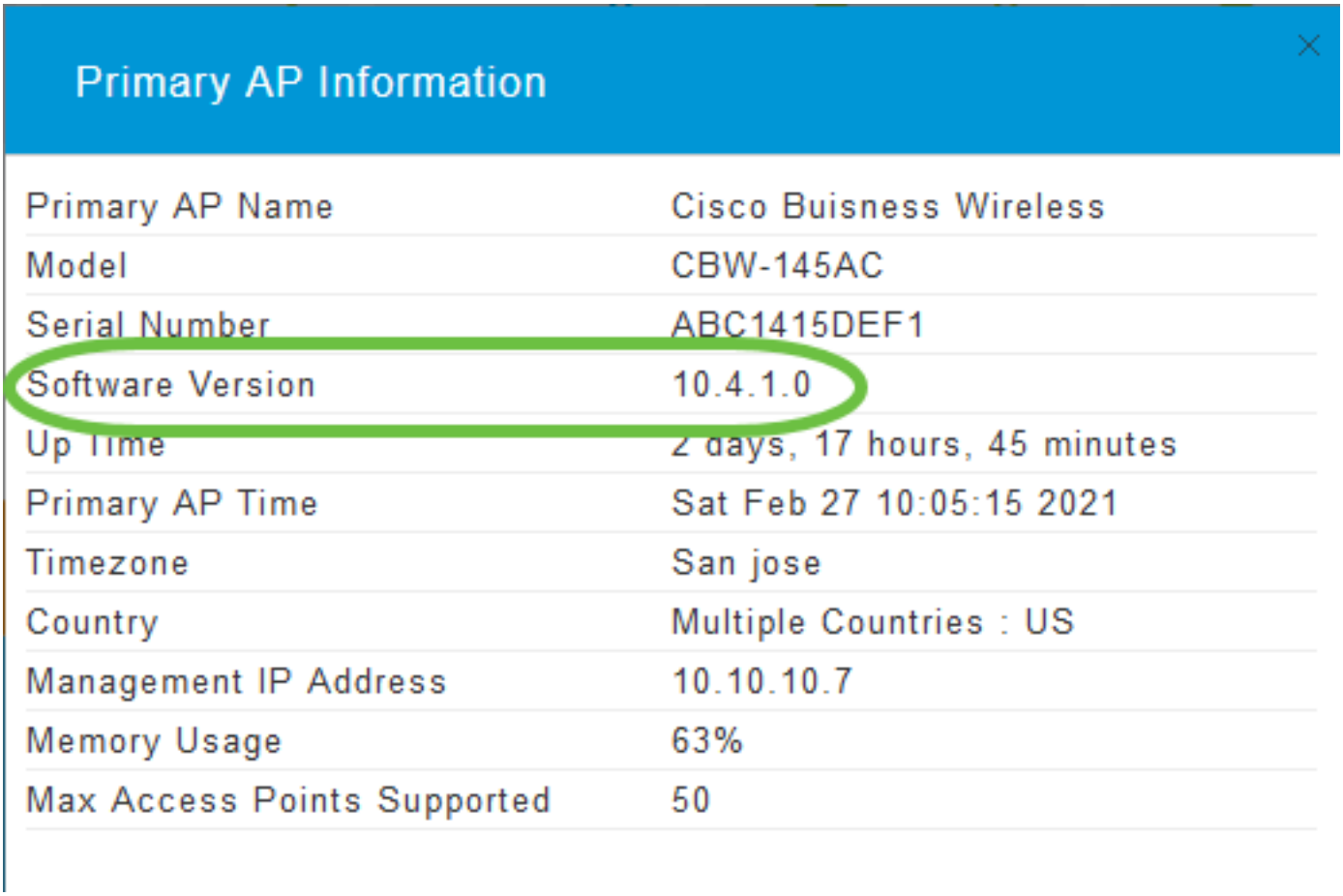
使用Web UI检查和更新软件

不要跳过这个重要步骤！有几种方法可以更新软件，但建议使用以下步骤作为使用Web UI时最容易执行的步骤。

要查看和更新主AP的当前软件版本，请执行以下步骤。

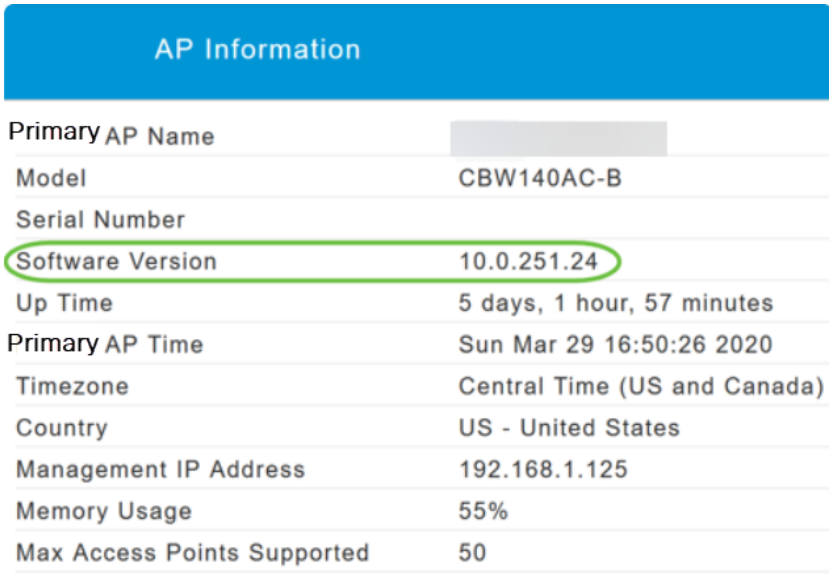
第 1 步

单击Web**界面**右上角的齿轮图标，然后单击“Primary AP Information(主要AP信**息)”**。



步骤 2

将运行的版本与最新软件版本进行比较。一旦知道是否需要更新软件，请关闭窗口。

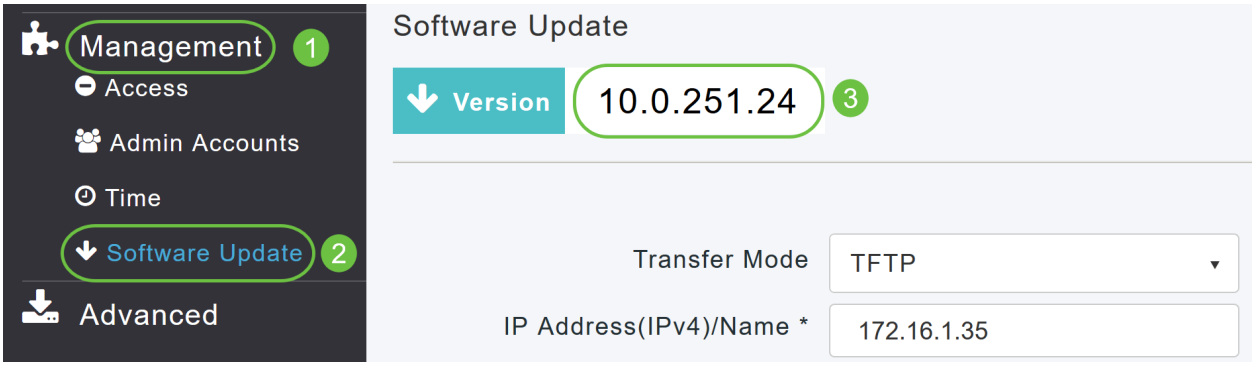


如果运行的是最新版本的软件，可以跳至“创建WLAN”部分。

步骤 3

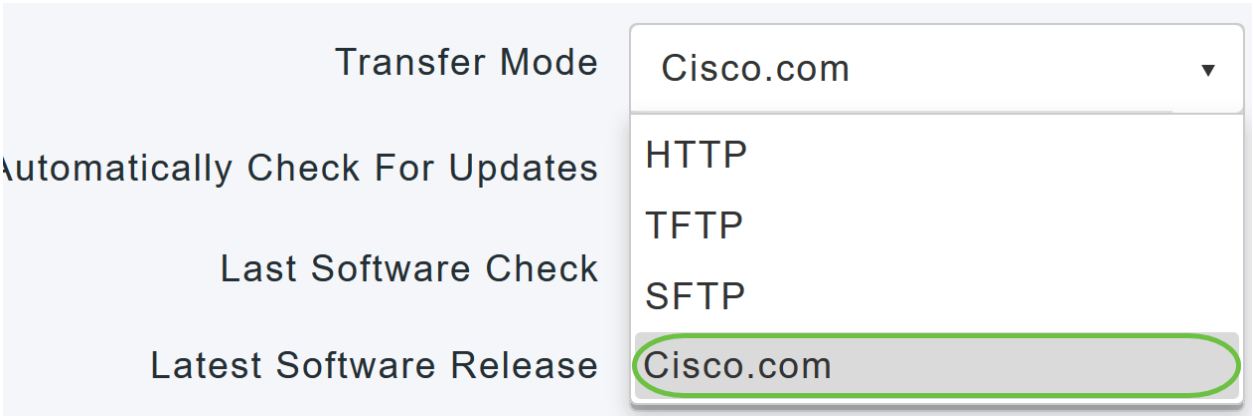
从菜单中选择**Management >** Software Update。

此时*将显示“软件更新”*窗口，其顶部列出了当前软件版本号。



您可以更新CBW AP软件，并且主AP上的当前配置不会被删除。

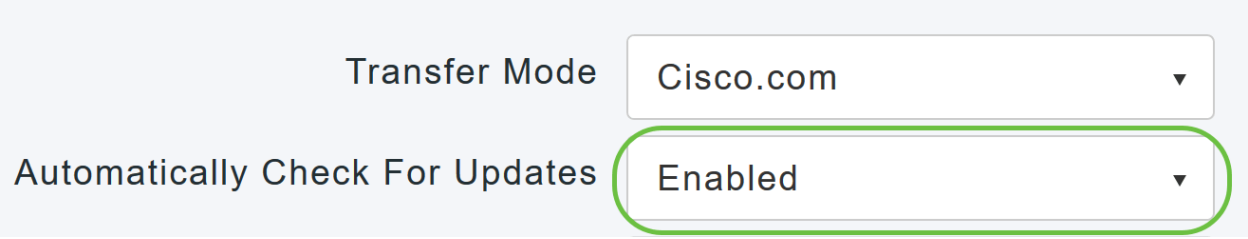
从“*传输模式*”下拉列表中，**选择Cisco.com**。



步骤 4

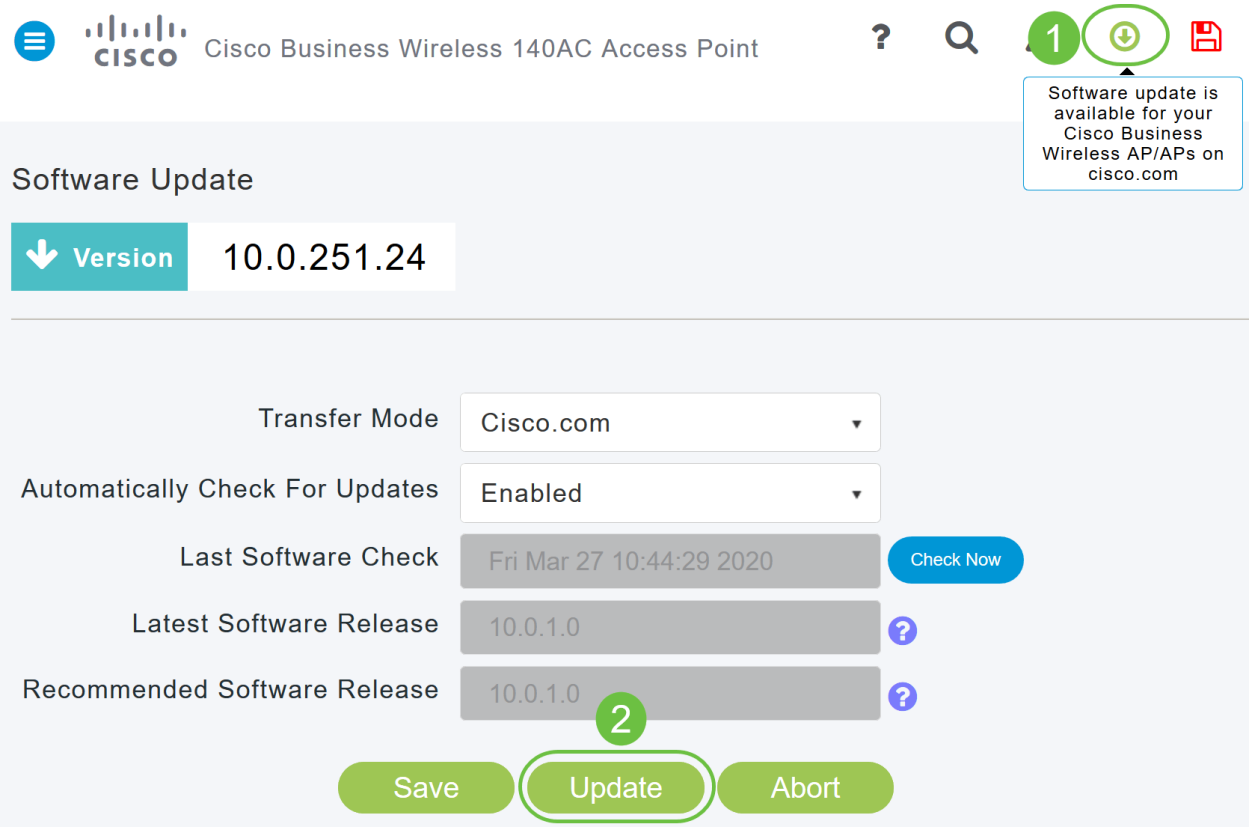
要将主AP设置为自动检查软件更新，请在*自动检查更新*下拉列**表中**选择启用。默认情况

下启用该接口。



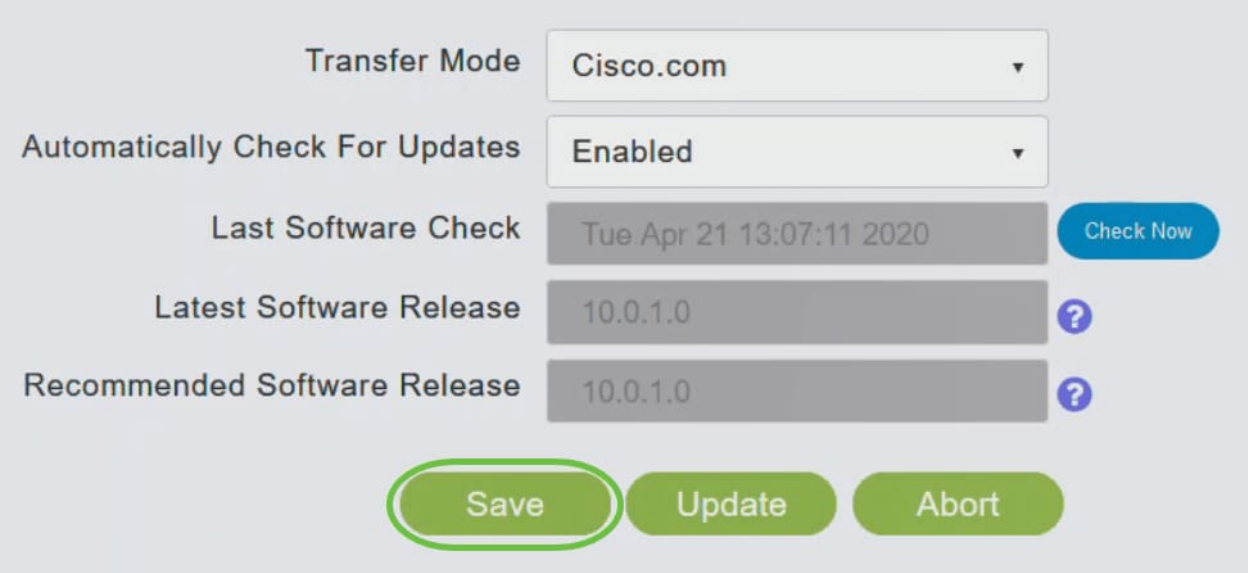
当软件检查完成且Cisco.com上提供更新的最新或推荐的软件更新时，则：

- Web **UI右上角**的“软件更新警报”图标将呈绿色（或灰色）。 点击该图标将进入软件更新页面。
- “软件更新”(Software Update)页面底部的“*更新”(Update*)按钮已启用。

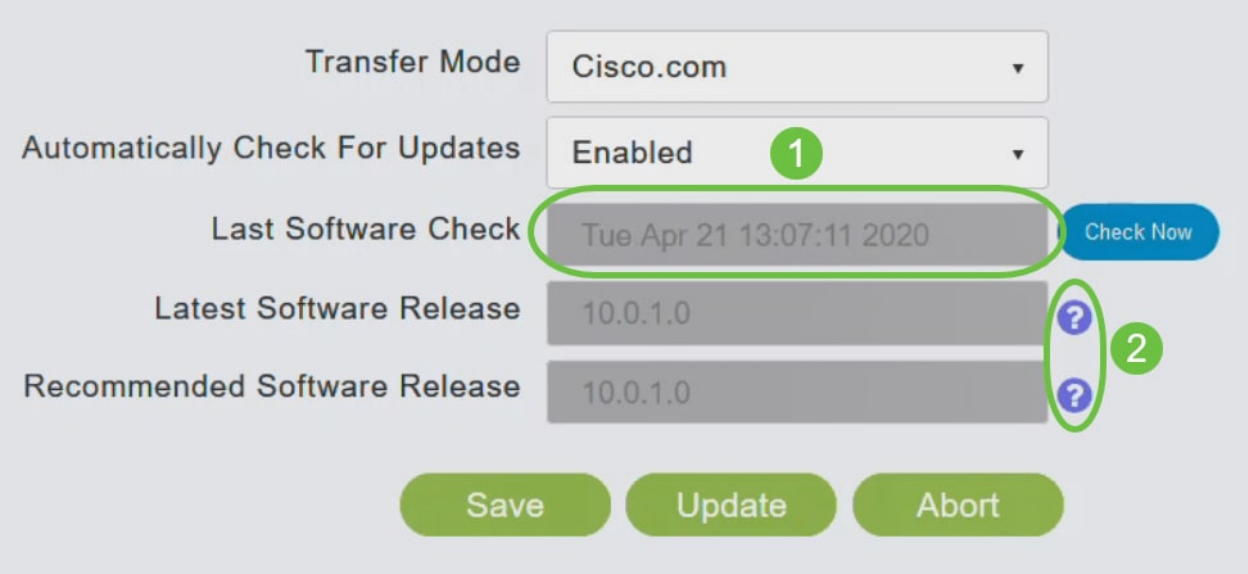


步骤 5

Click Save.这将保存您在传输模式和自动检查更*新中所*做的*条目或更改*。

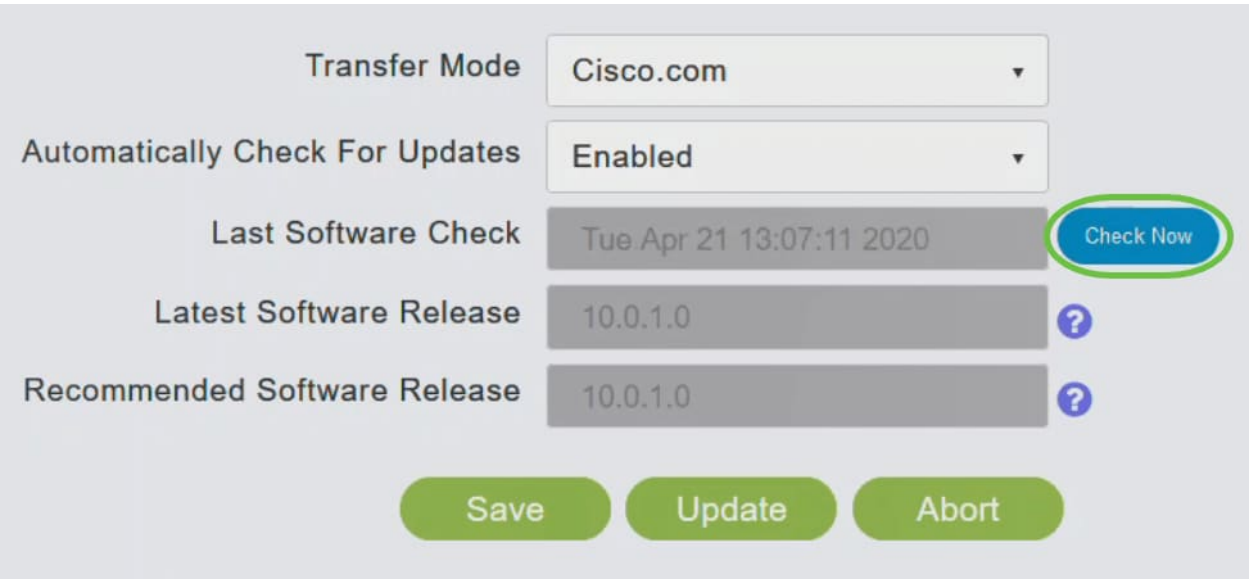


“上*次软件检查*”字段显示上次自动或手动软件检查的时间戳。单击显示的版本旁边的问号图**标可查看**其注释。



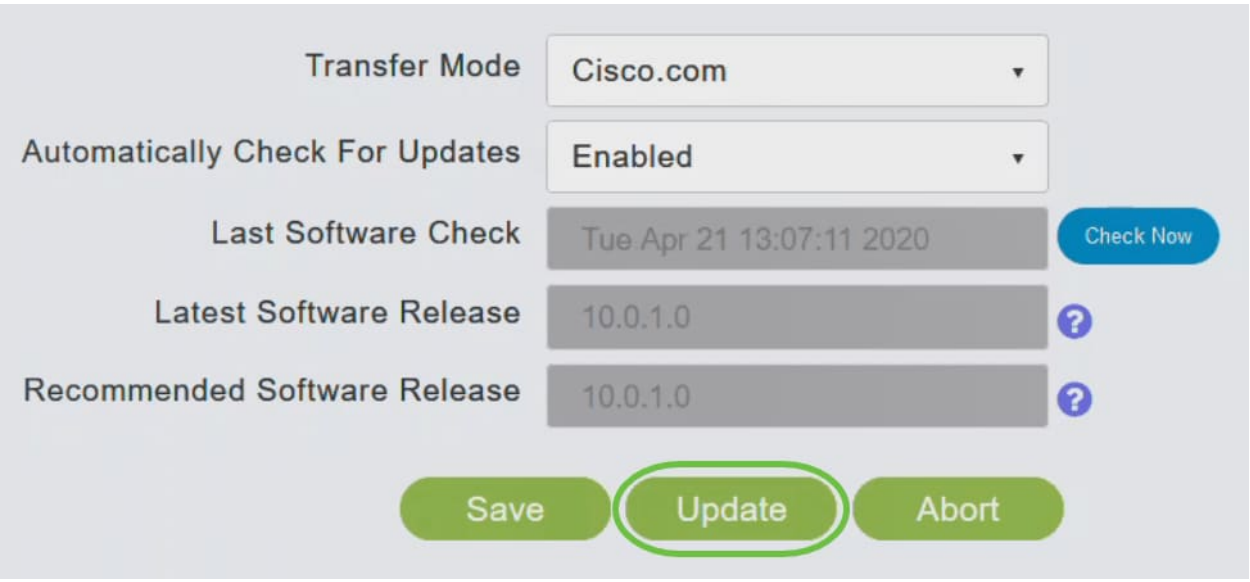
步骤 6

您可以随时通过单击“立即检查”手动*运行软件检查*。



步骤 7

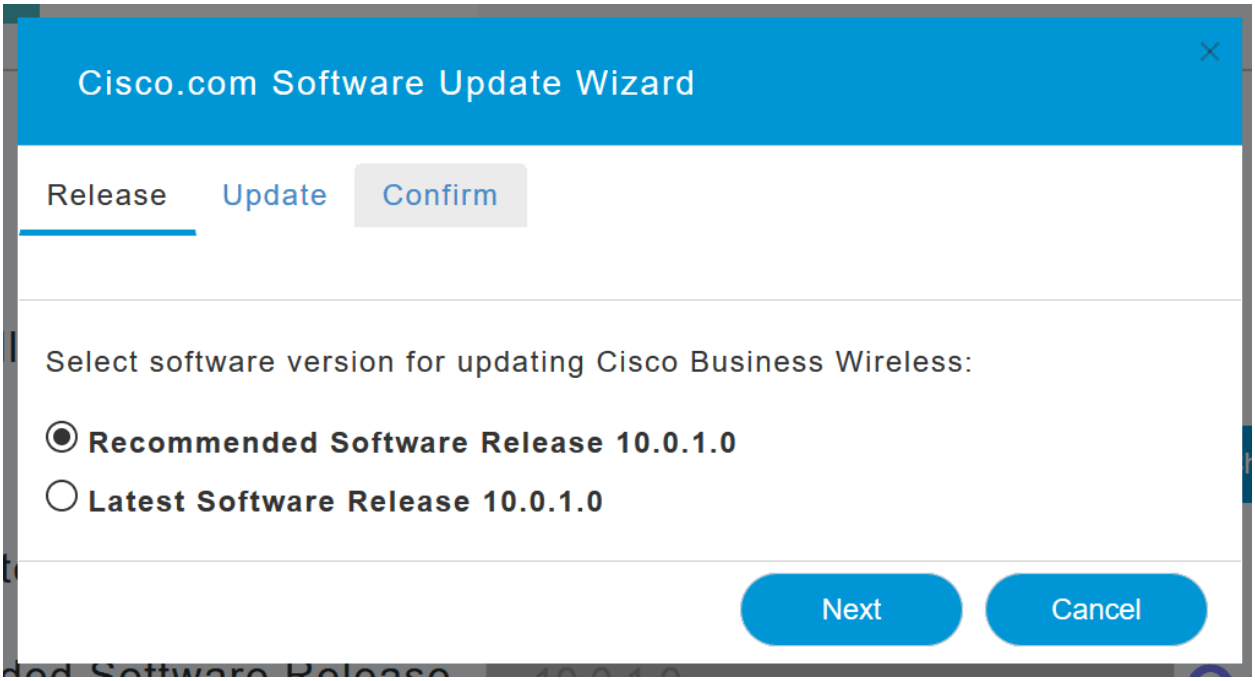
要继续软件更新，请单击**Update**。



系统将*显示“软件更新*向导”。此向导将引导您依次浏览以下三个选项卡：

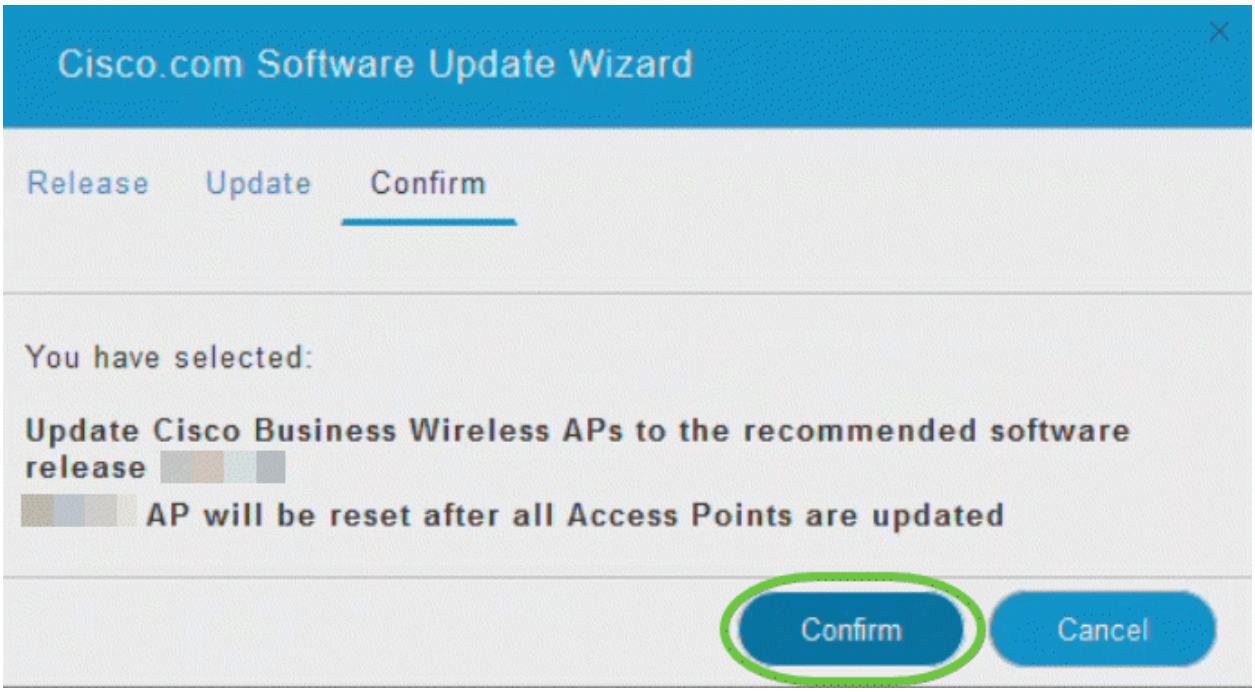
- 版本选项卡 — 指定是要更新到推荐的软件版本还是最新软件版本。
- Update选项卡 — 指定何时应重置AP。您可以选择立即完成，或安排以后的时间。要将主AP设置为在映像预下载完成后自动重新启动，请选中自动重新启动复选框。
- “确认”选项卡 — 确认您的选择。

按照向导中的说明操作。在单击“确认”之前，可以随时返回任何*选项卡*。



步骤 8

单击“**Confirm（确认）**”。

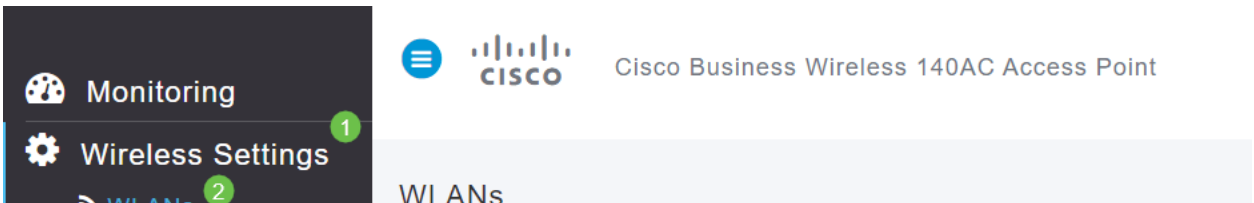


在Web UI上创建WLAN

此部分允许您创建无线局域网(WLAN)。

第 1 步

可以通过导航至Wireless Settings > WLANs**来创建WLAN**。然后选择**Add new WLAN/RLAN（添加新WLAN/RLAN）**。



步骤 2

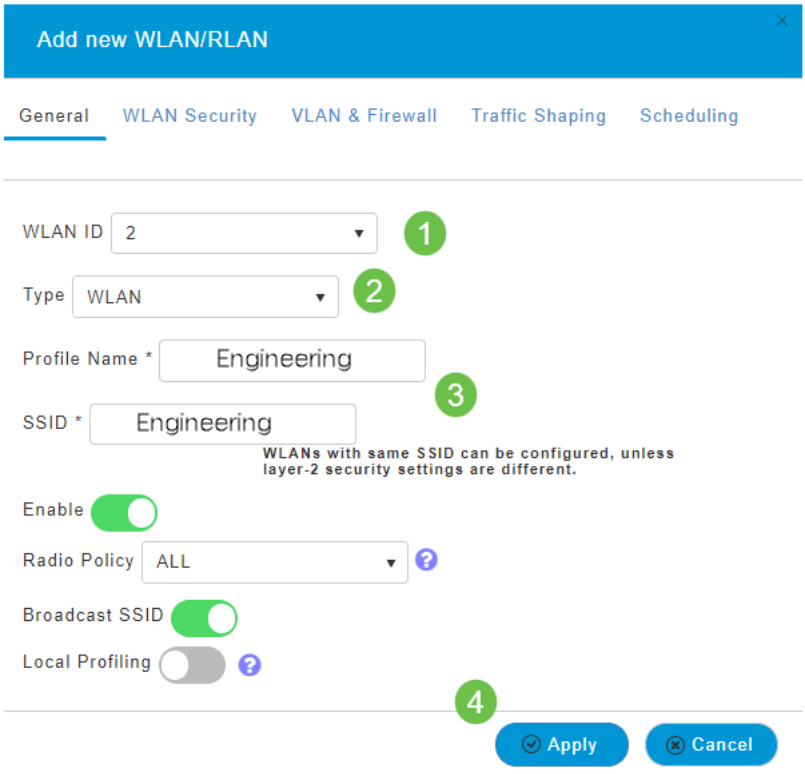
在“常规”*选项卡*下，输入以下信息：

- WLAN ID — 为WLAN选择一个编号
- 类型 — 选择**WLAN**
- 配置文件名称 — 输入名称时，SSID将自动填充相同的名称。名称必须唯一，且不应超过31个字符。

以下字段在本示例中保留为默认值，但是，如果您想以不同方式配置它们，则会列出说明。

- SSID — 配置文件名称也用作SSID。如果您愿意，可以更改此项。名称必须唯一，且不应超过31个字符。
- 启用 — 应保持启用状态，WLAN才能正常工作。
- 无线电策略 — 通常，您会希望将其保留为**All**，以便2.4GHz和5GHz客户端可以访问网络。
- 广播SSID — 通常，您希望发现SSID，以便将其保留为Enabled。
- 本地分析 — 您只希望启用此选项以查看客户端上运行的操作系统或查看用户名。

单击 Apply。



步骤 3

您将进入WLAN安全*选项*卡。

在本例中，以下选项保留为默认值：

- 访客网络、强制网络助理和MAC过滤保持禁用状态。有关设置访客网络的详细信息，请

参阅下一节。

- WPA2个人 — 带预共享密钥(PSK)密码短语格式的Wi-Fi保护访问2 - ASCII。此选项表示带预共享密钥(PSK)的Wi-Fi保护访问2。

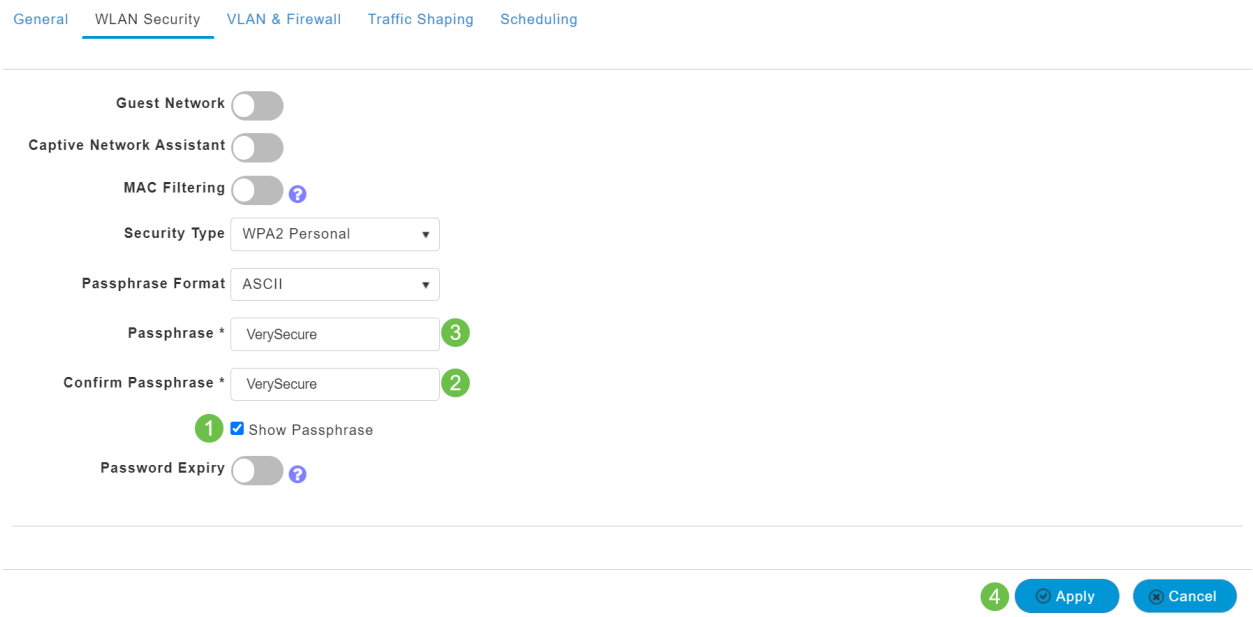
WPA2个人版是一种使用PSK身份验证保护网络的方法。PSK在主AP、WLAN安全策略下和客户端上分别配置。WPA2个人版不依赖于网络上的身份验证服务器。

- 密码短语格式- **ASCII保留为默认值。**

在此场景中输入了以下字段：

- Show Passphrase — 点击复选框可查看您输入的密码。
- 密码短语 — 输入密码短语（密码）的名称。
- 确认密码 — 再次输入密码进行确认。

单击 Apply。这将自动激活新的WLAN。

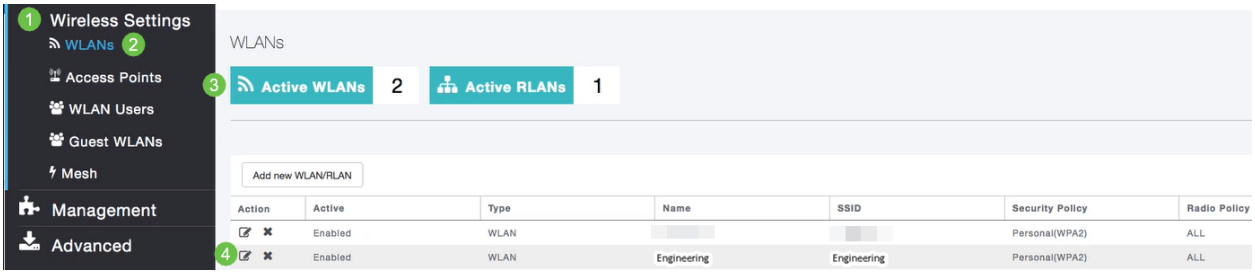


步骤 4

请务必单击Web UI屏幕右上面板上的保存图标来保存配置。

步骤 5

要查看您创建的WLAN，请选择**Wireless Settings > WLANs**。您将看到活动WLAN的数量增加到2，并显示新的WLAN。



对要创建的其他WLAN重复上述步骤。

可选无线配置

您现在已设置所有基本配置，并已准备就绪。您有一些选项，因此您可以跳到以下任何部分：

- 使用Web UI创建访客WLAN（可选）
- 应用程序分析（可选）
- 客户端分析（可选）
- 我已准备好总结并开始使用我的网络！

使用Web UI创建访客WLAN（可选）

访客WLAN为访客提供对思科企业无线网络的访问。

第 1 步

登录主AP的Web UI。打开Web浏览器并输入www.https://ciscobusiness.cisco。在继续之前，您可能会收到警告。输入您的凭证。您还可以通过输入主AP的IP地址来访问它。

步骤 2

通过导航至Wireless Settings > WLANs，可以创建无线**局域网(WLAN)**。然后选择**Add new WLAN/RLAN（添加新WLAN/RLAN）**。

步骤 3

在"常规"*选项卡*下，输入以下信息：

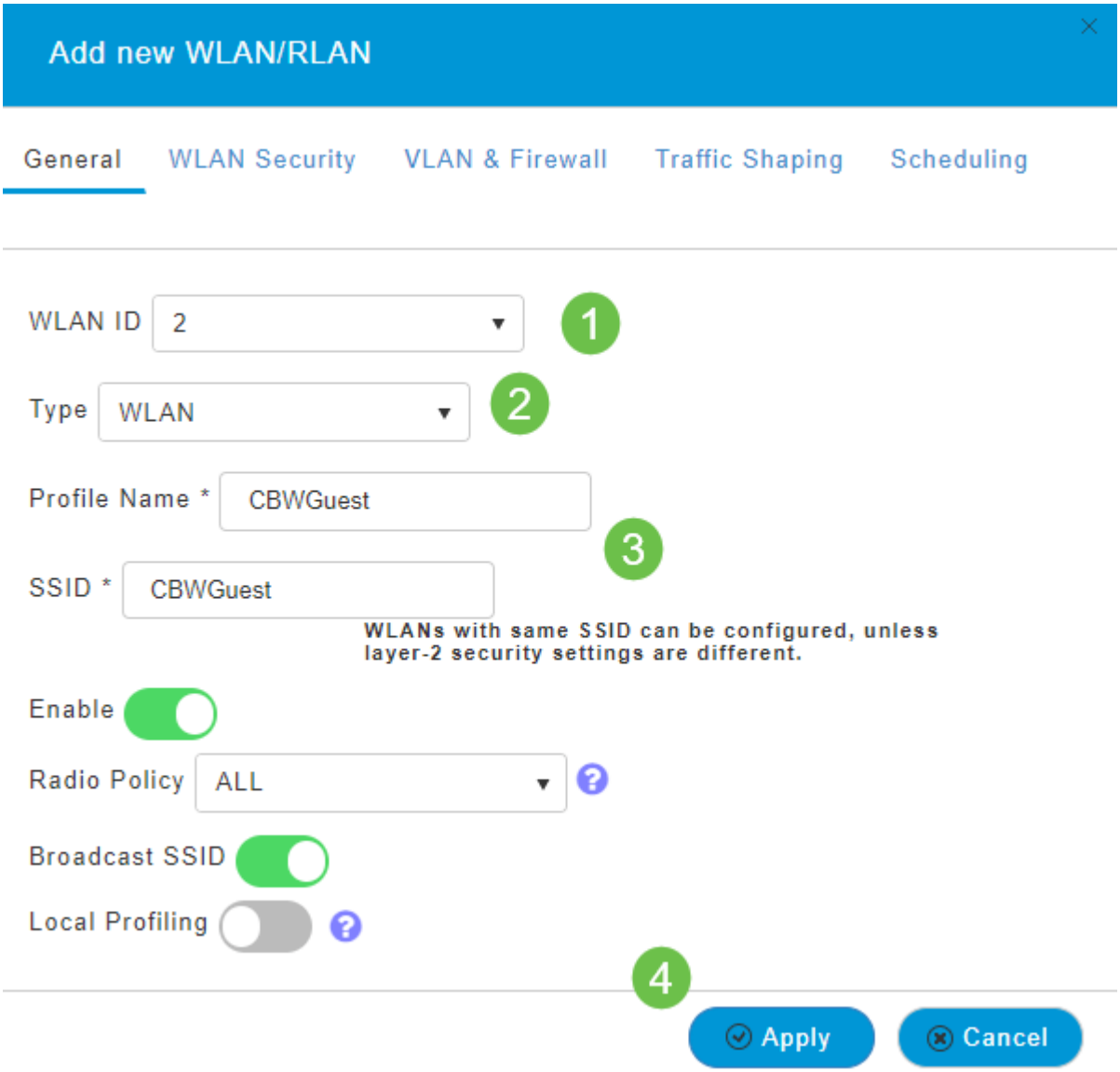
WLAN ID — 为WLAN选择一个编号
类型 — 选择**WLAN**

*配置*文件名称 — 输入名称时，SSID将自动填充相同的名称。名称必须唯一，且不应超过31个字符。

以下字段在本示例中保留为默认值，但是，如果您想以不同方式配置它们，则会列出说明。

SSID — 配置文件名称也用作SSID。如果您愿意，可以更改此项。名称必须唯一，且不应超过31个字符。
启用 — 应保持启用状态，WLAN才能正常工作。
无线电策略 — 通常，您希望将此设置保留为All，以便2.4GHz和5GHz客户端可以访问网络。
广播SSID — 通常，您希望发现SSID，以便将其保留为“已启用”。
本地分析 — 您只希望启用此选项以查看客户端上运行的操作系统或查看用户名。

单击 Apply。

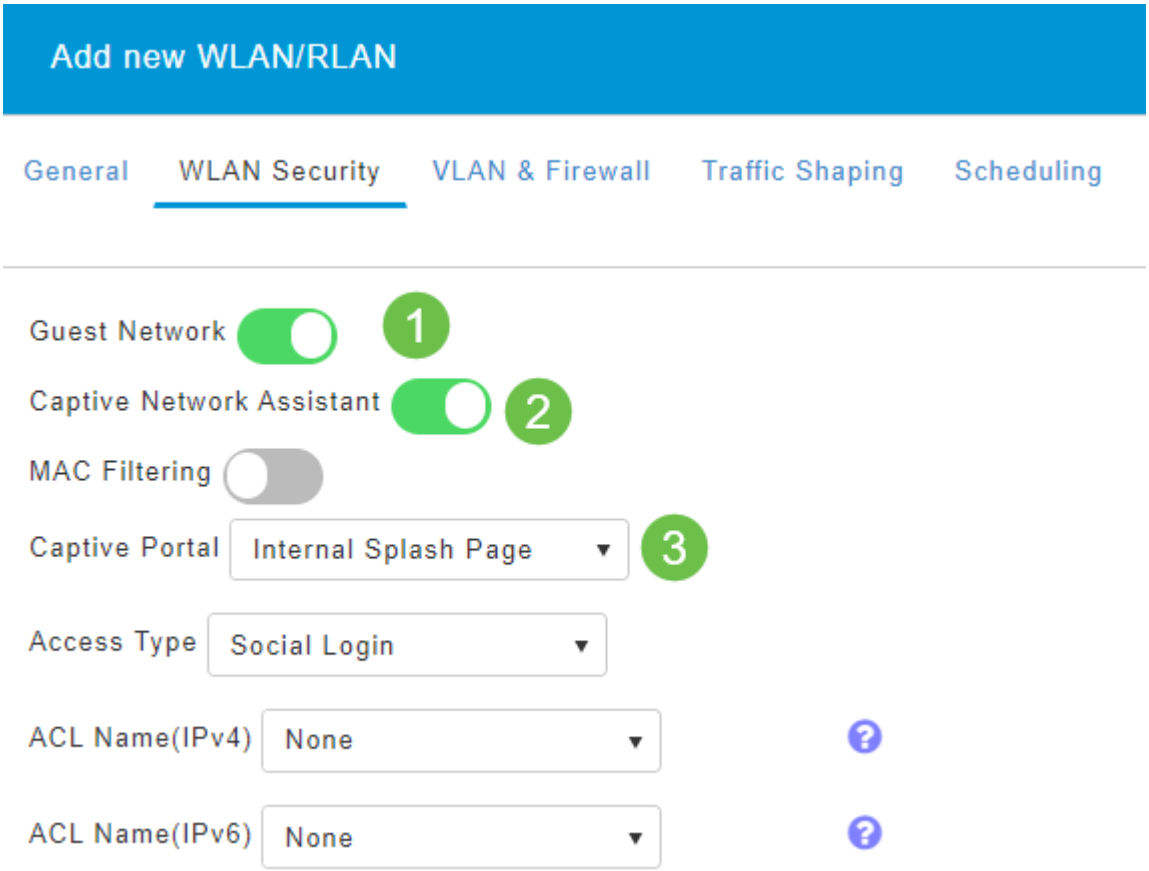


步骤 4

您将进入WLAN安全*选项*卡。在本例中，选择了以下选项。

- 访客网络 — 启用

- 强制网络助理 — 如果您使用Mac或IOS，您可能希望启用此功能。此功能通过在连接到无线网络时发送Web请求来检测强制网络门户是否存在。此请求指向iPhone型号的统一资源定位器(URL)，如果收到响应，则假设互联网访问可用，无需进一步交互。如果未收到响应，则假设强制网络门户阻止互联网访问，并且Apple的强制网络助理(CNA)会自动启动伪浏览器，在受控窗口中请求门户登录。当重定向到身份服务引擎(ISE)强制网络门户时，CNA可能会中断。主AP可防止此伪浏览器弹出。
- 强制网络门户 — 仅当启用访客网络选项时，此字段才可见。这用于指定可用于身份验证的Web门户类型。选择内部启动页面以使用默认的基于思科Web门户的身份验证。如果要使用网络外部的Web服务器进行强制网络门户身份验证，请选择外部启动页。此外，在Site URL字段中指定服务器的URL。



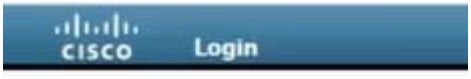
在本示例中，将创建启用了社交登录访问类型的访客WLAN。用户连接到此访客WLAN后，将重定向到思科默认登录页面，在该页面中，他们可以找到Google和Facebook的登录按钮。用户可以使用其Google或Facebook帐户登录以获取Internet访问。

步骤 5

在同一选项卡上，从下*拉菜单中选择*访问类型。在本例中，*选择了社*交登录。这是允许访客使用其Google或Facebook凭证进行身份验证和访问网络的选项。

“访问类型”的*其他选项*包括：

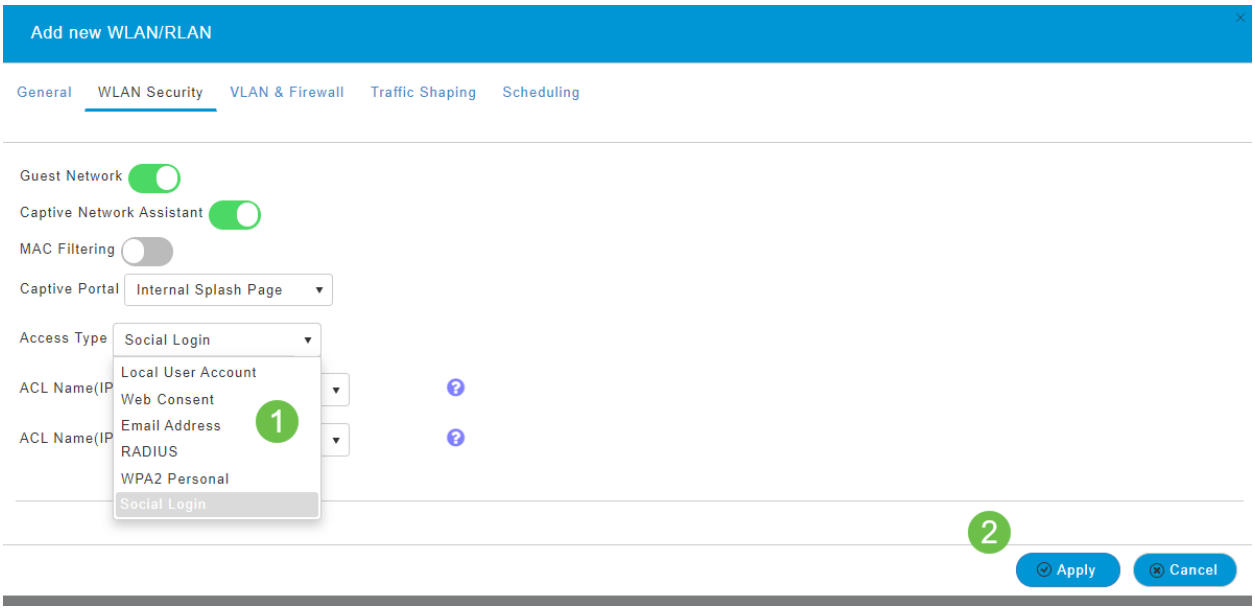
本地用户帐户 — 默认选项。选择此选项以使用用户名和密码对访客进行身份验证，您可以在“无线设置”>“WLAN用户”下为此WLAN的访**客用户指定用户名和密码**。这是默认内部启动页的示例。



您可以通过导航到Wireless Settings > Guest WLANs**来自定义此设置**。您可以在此处输入页*面标题*和页*面消息*。单击 Apply。单击“**预览**”。

Web同意 — 允许访客在接受显示的条款和条件后访问WLAN。访客用户无需输入用户名和密码即可访问WLAN。
Email Address — 访客用户需要输入其电子邮件地址才能访问网络。
RADIUS — 将其用于外部身份验证服务器。
WPA2个人 — 带预共享密钥(PSK)的Wi-Fi保护访问2

单击 Apply。



步骤 6

请务必单击Web UI屏幕右上面板上的保存图标来保存配置。

您现在已经创建了CBW网络上可用的访客网络。客人将非常感谢您的便利。

使用Web UI进行应用程序分析（可选）

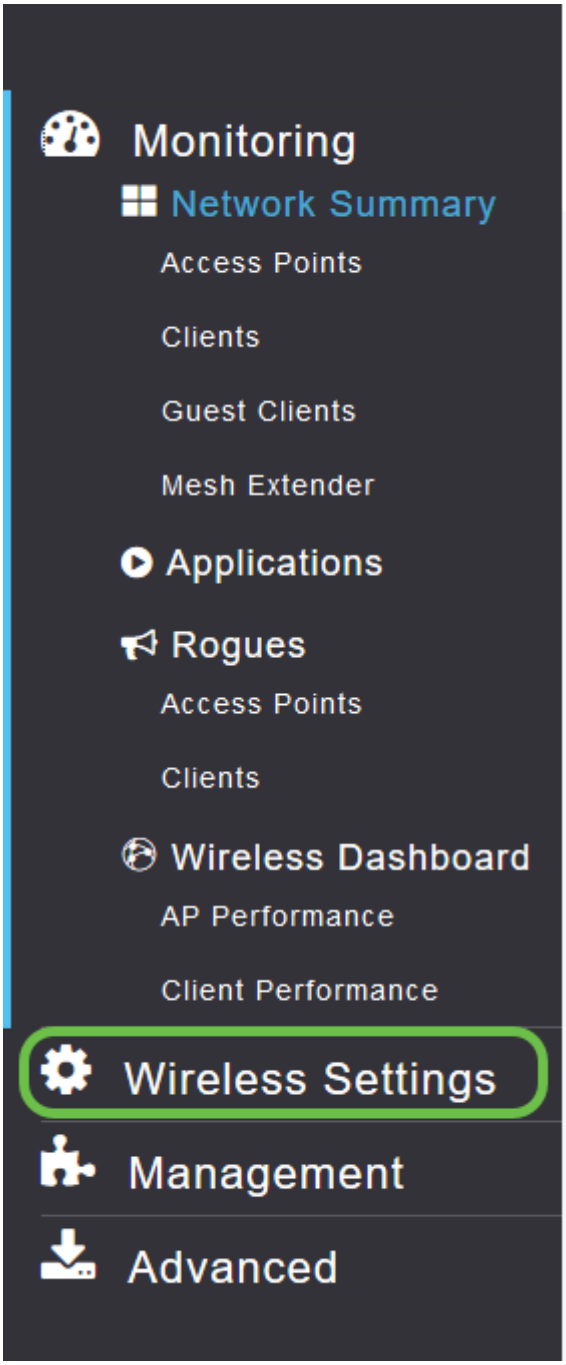
分析是支持实施组织策略的功能的子集。它允许您匹配流量类型并确定其优先级。与规则一样，规则也会决定如何对流量进行排名或丢弃。思科业务网状无线系统采用客户端和应用分析。作为用户访问网络的行为首先是进行许多信息交换，其中信息是流量类型。策略中断流量以引导路径，就像流图一样。其他类型的策略功能包括：访客访问、访问控制列表和QoS。

第 1 步

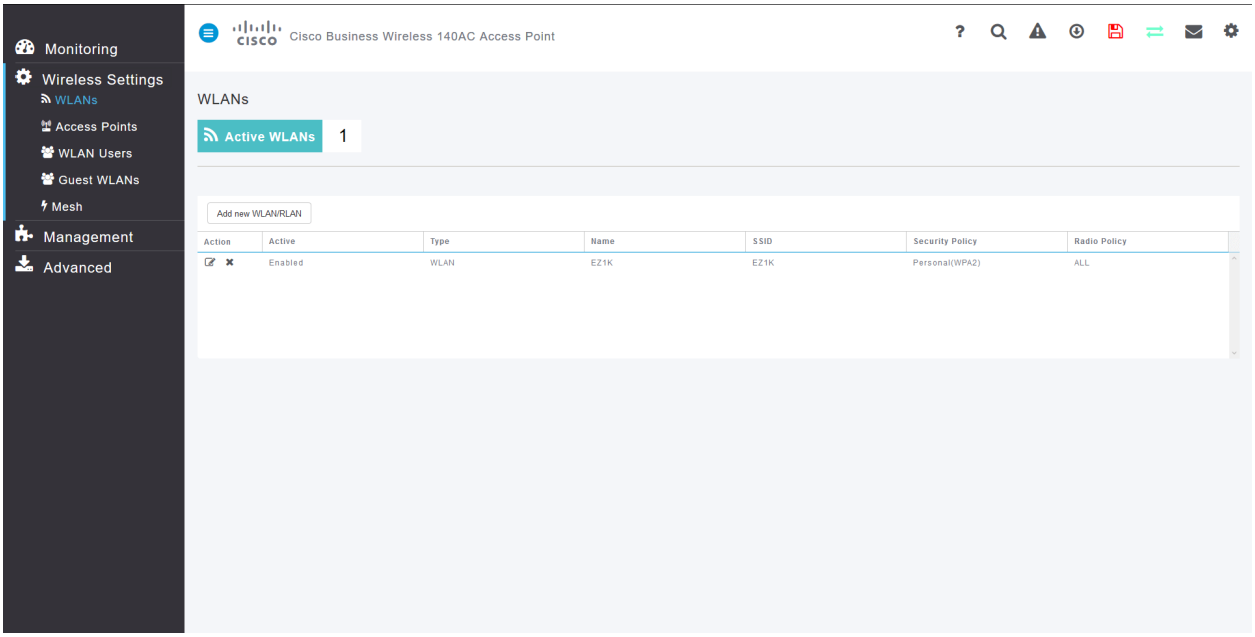
如果未看到左侧菜单栏，请导航到屏幕左侧的菜单。

步骤 2

默认情况下，登录设备时会加载“监控”菜单。您需要单击“Wireless Settings(无**线设置)**”。

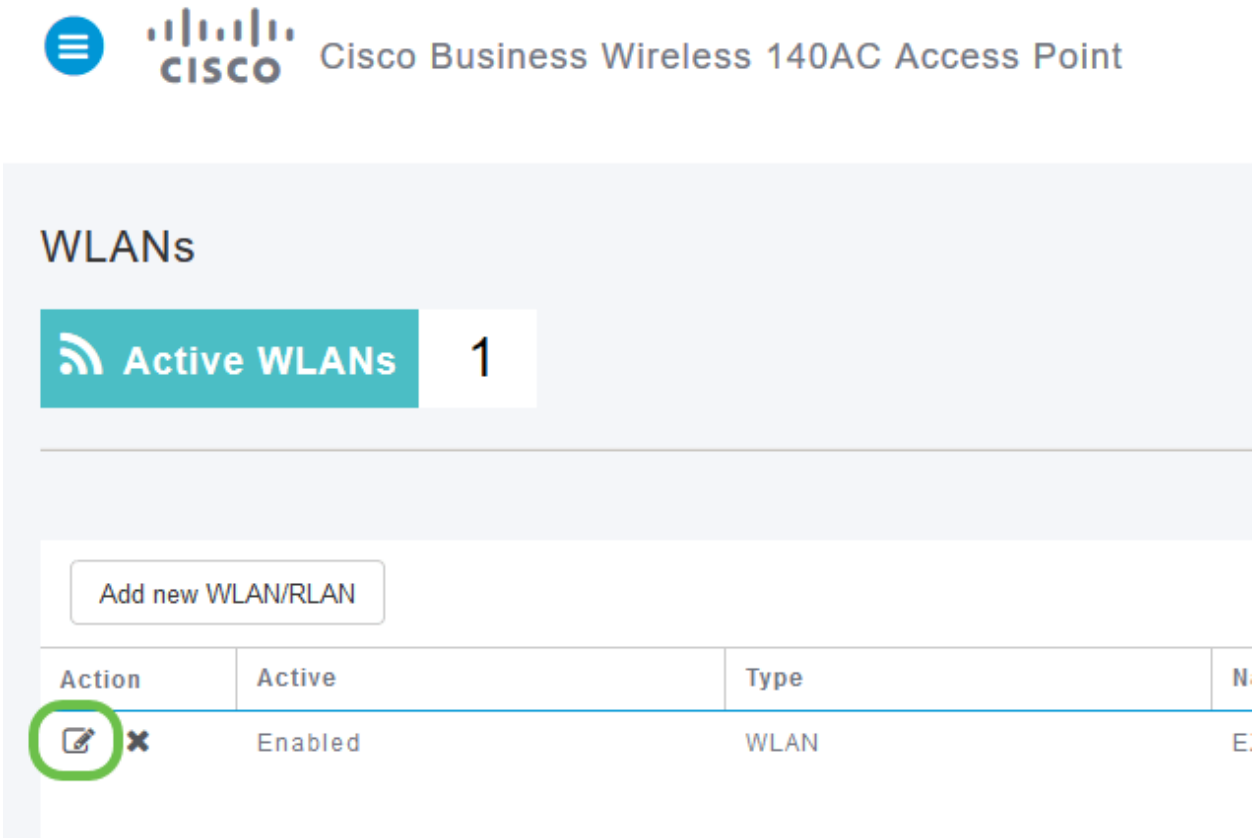


下图与您单击“无线设置”链接时看到的图像类似。

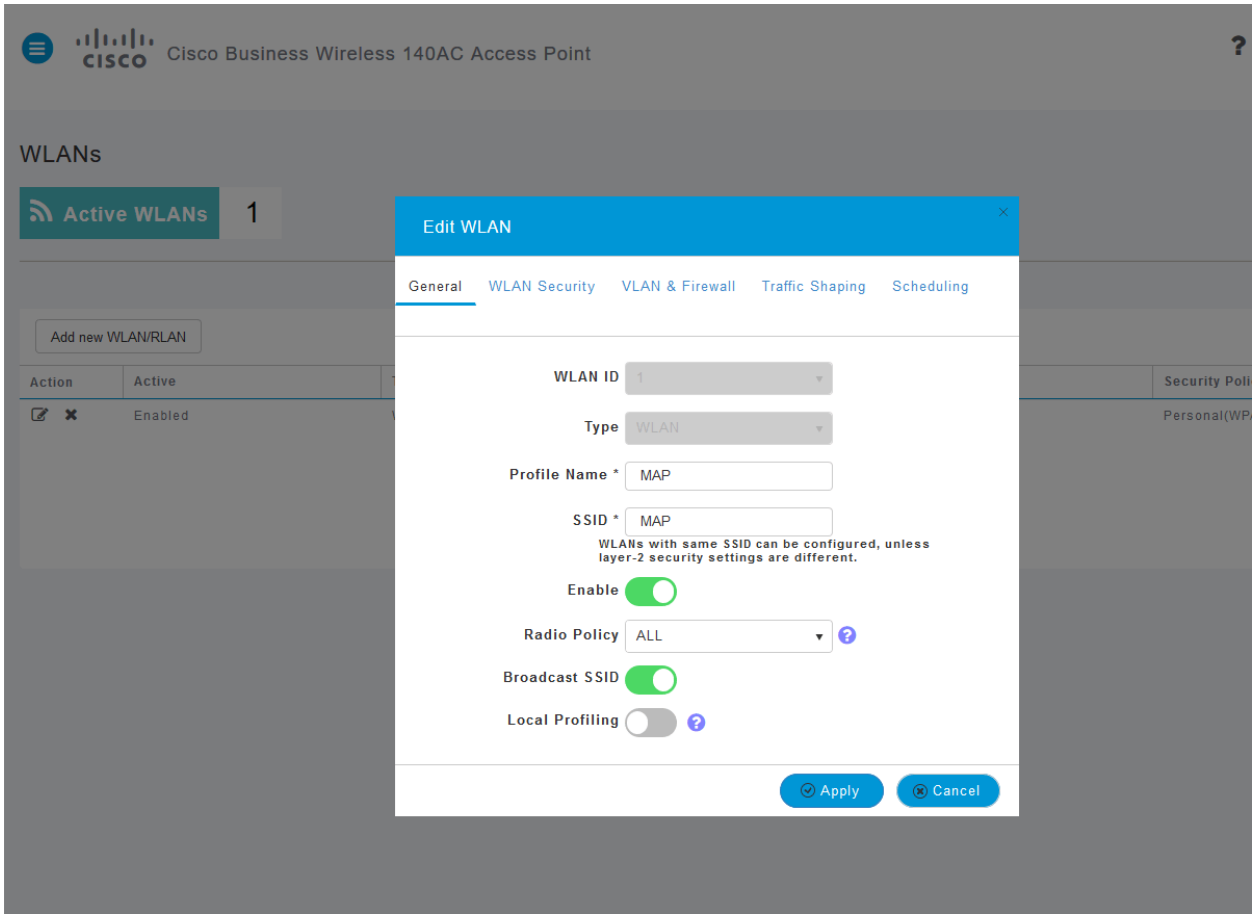


步骤 3

单击要启用应用的无线局域网左侧的**编辑图标**。

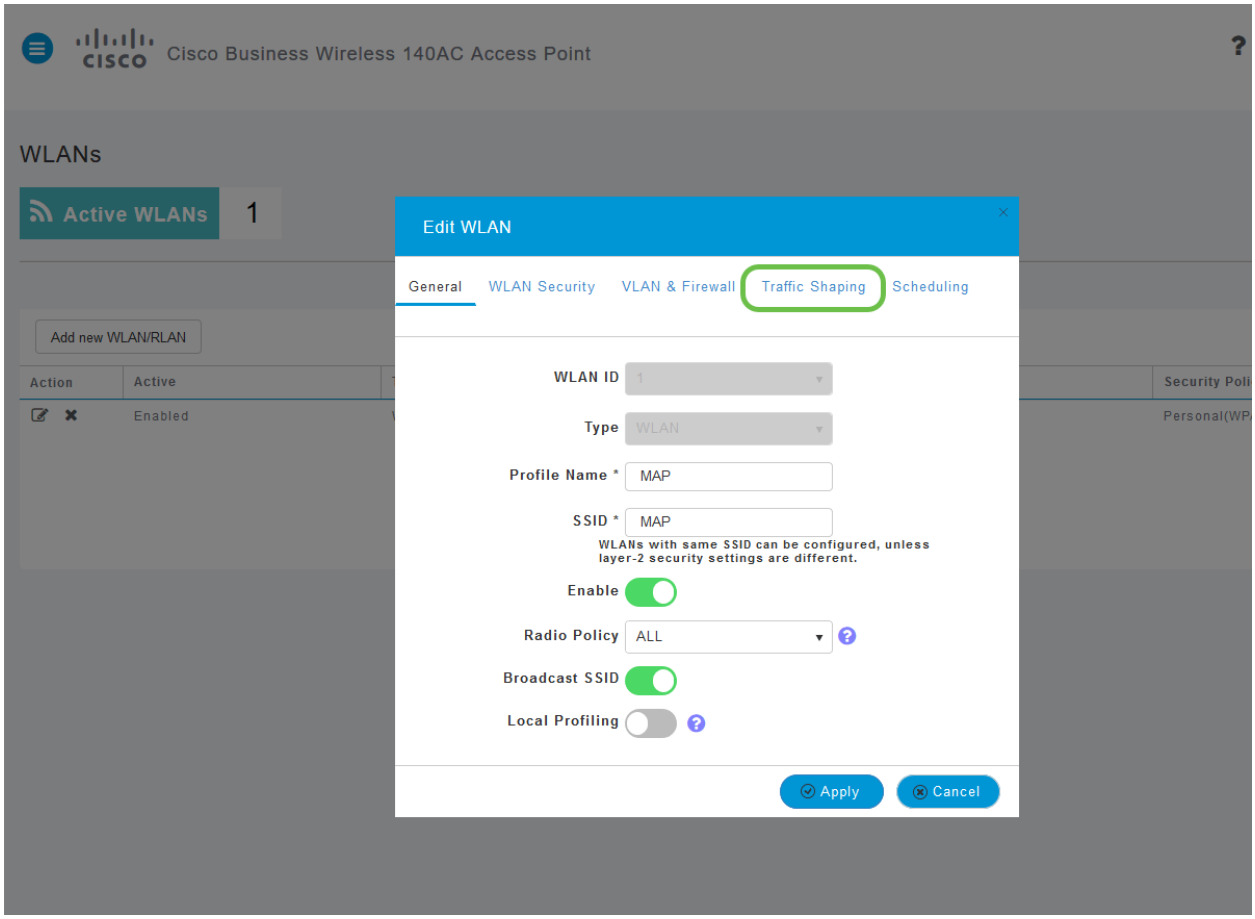


由于您最近添加了WLAN，因此您的“*编辑WLAN*”页面可能显示类似于以下内容：

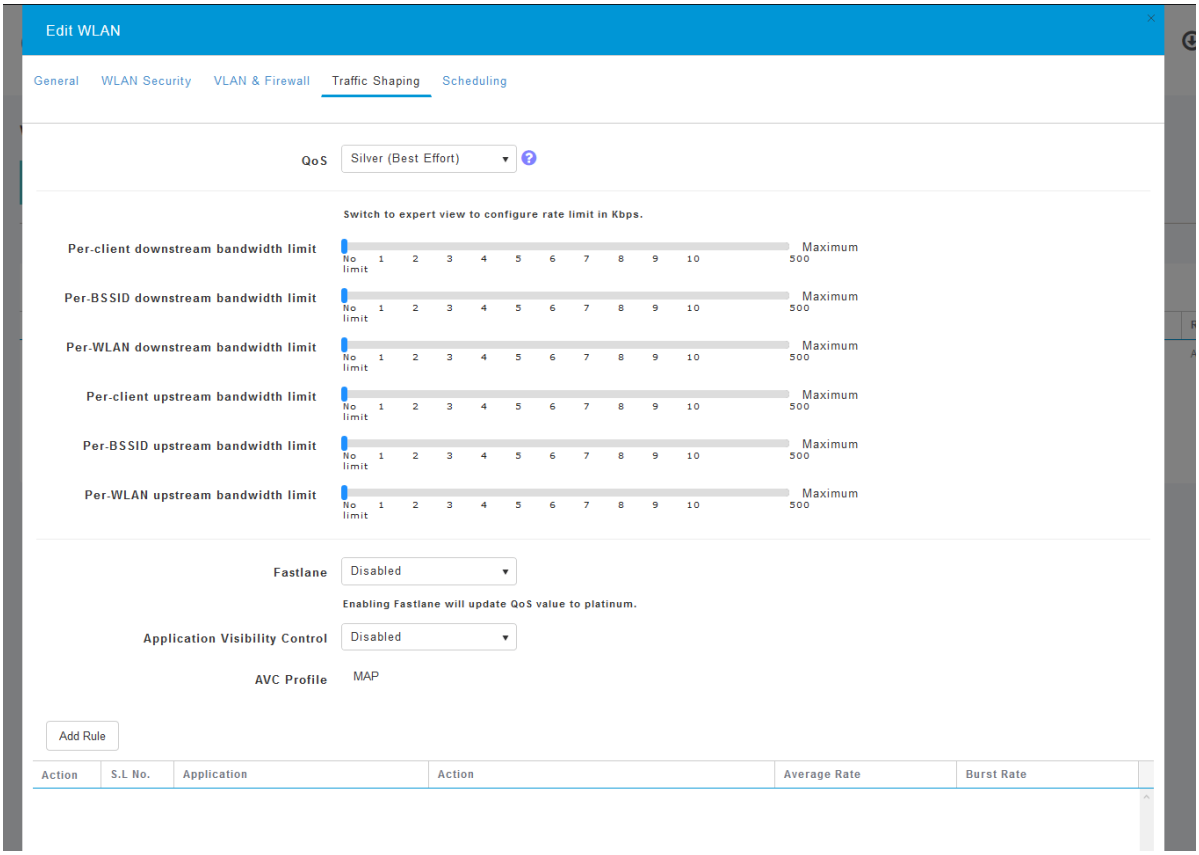


步骤 4

单击“流量整形”选项卡。

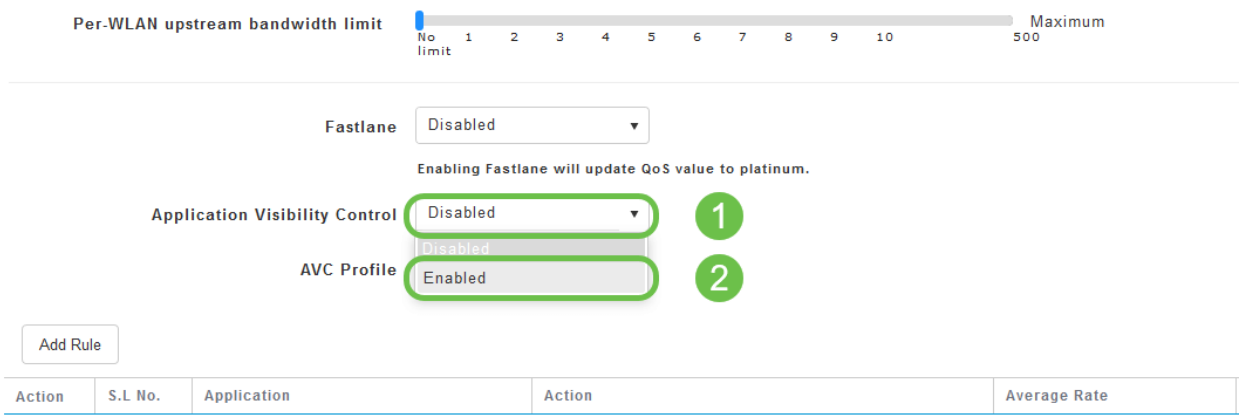


您的屏幕可能显示如下：



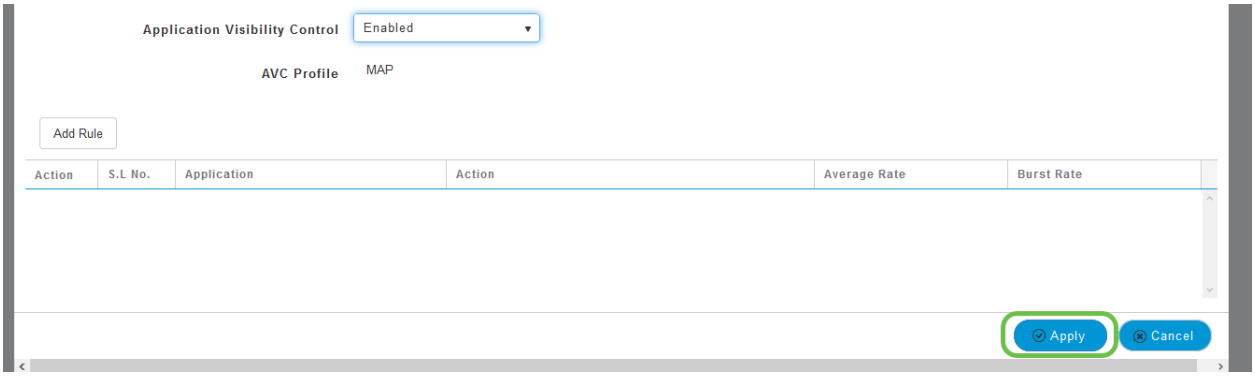
步骤 5

在页面底部，您将找到应用可视*性控制*功能。默认情况下禁用此功能。单击下拉列表，然后选择“**启用**”。



步骤 6

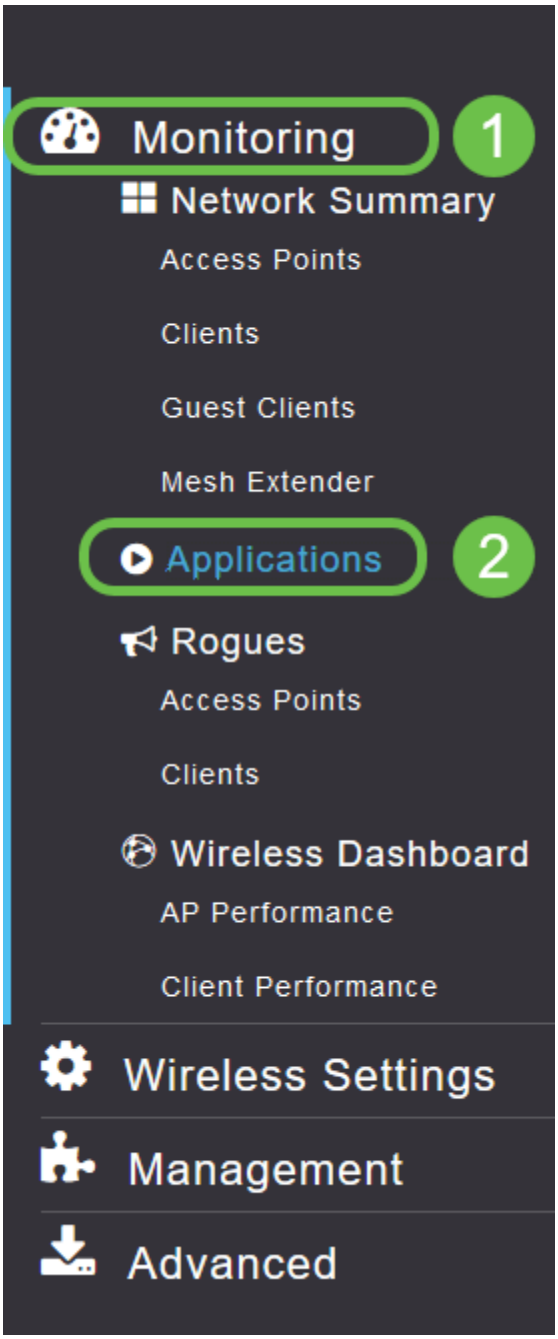
单击应用按钮.



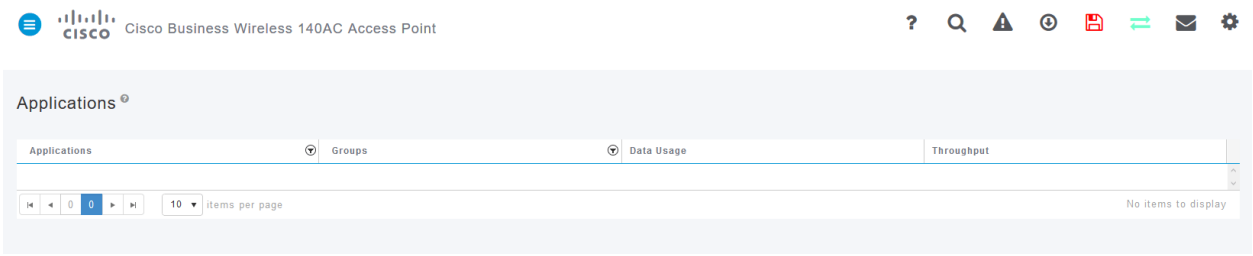
必须启用此设置，否则该功能将无法运行。

步骤 7

单击取消按钮关闭WLAN子菜单。然后单击左**侧菜**单栏上的“监控”菜单。一旦您能够，单击“应用**程序**”菜单项。



如果没有流向任何源的流量，页面将为空，如下所示。



此页面将显示以下信息：

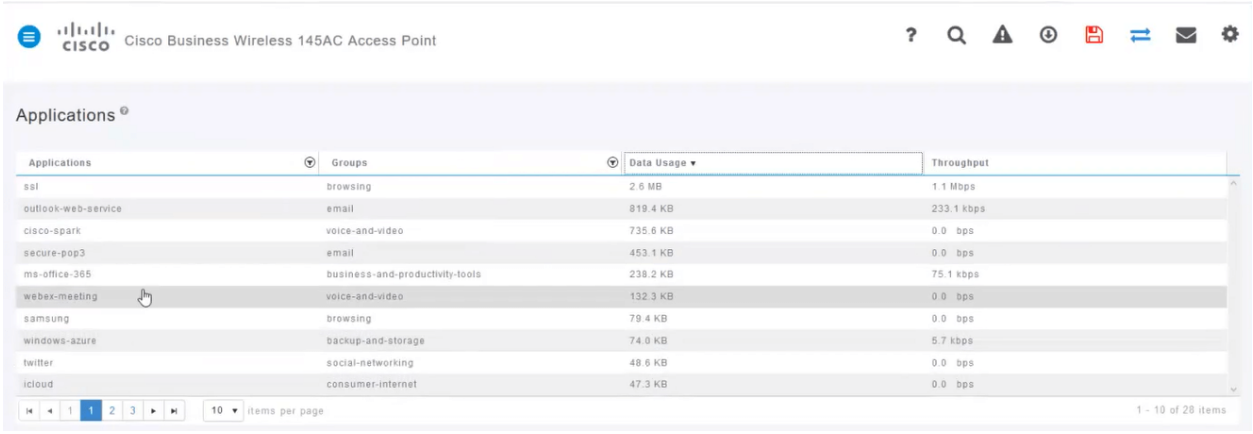
- 应用 — 包括许多不同类型
- 组 — 指示应用程序组的类型，以便更轻松地排序
- 数据使用情况 — 此服务整体使用的数据量
- 吞吐量 — 应用使用的带宽量

您可以点击选项卡，从大到小排序，这有助于确定网络资源的最大消费者。

此功能非常强大，可以在精细级别管理WLAN资源。以下是一些较为常见的组和应用类型。您的列表可能会包括更多内容，包括以下组和示例：

- 浏览
  - 例如：客户端特定，SSL
- 发送邮件
  - 例如：Outlook、Secure-pop3
- 语音和视频
  - 例如：WebEx、Cisco Spark、
- 业务和工作效率工具
  - 例如：Microsoft Office 365、
- 备份和存储
  - 例如：Windows-Azure、
- 消费者 — 互联网
  - iCloud、Google Drive
- 社交网络
  - 例如：Twitter、Facebook
- 软件更新
  - 例如：Google-Play、IOS
- 即时消息
  - 例如：挂断、消息

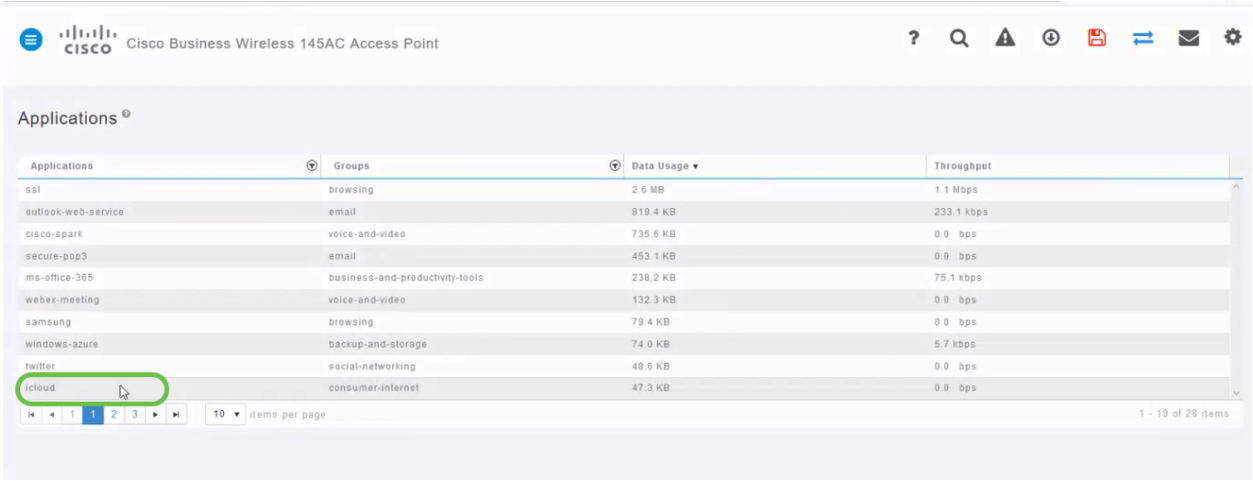
此处显示的是填充页面时的样例。



每个表标题都可单击以进行排序，这对数据使用和吞吐*量字段尤为有*用。

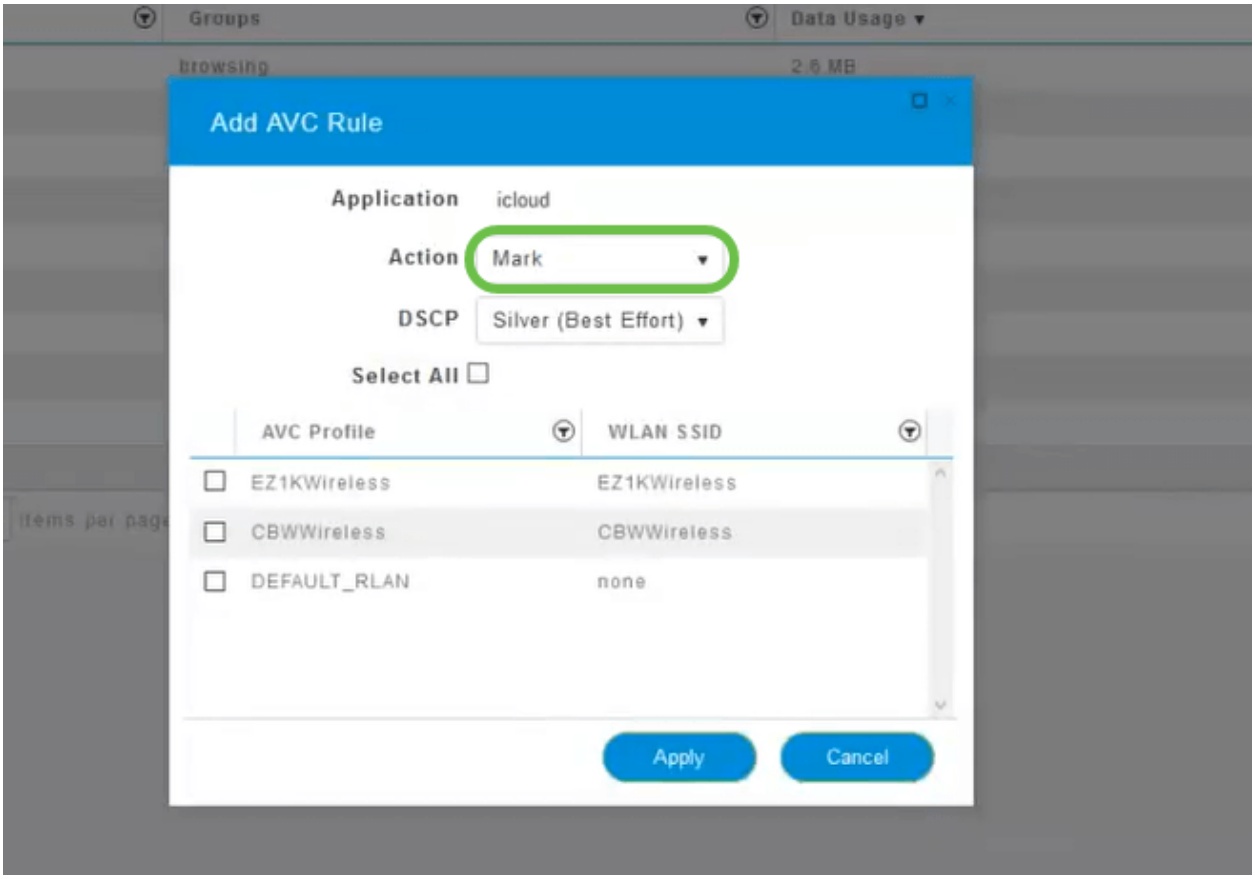
步骤 8

点击要管理的流量类型的行。



步骤 9

单击**Action**下拉框，选择如何处理该流量类型。



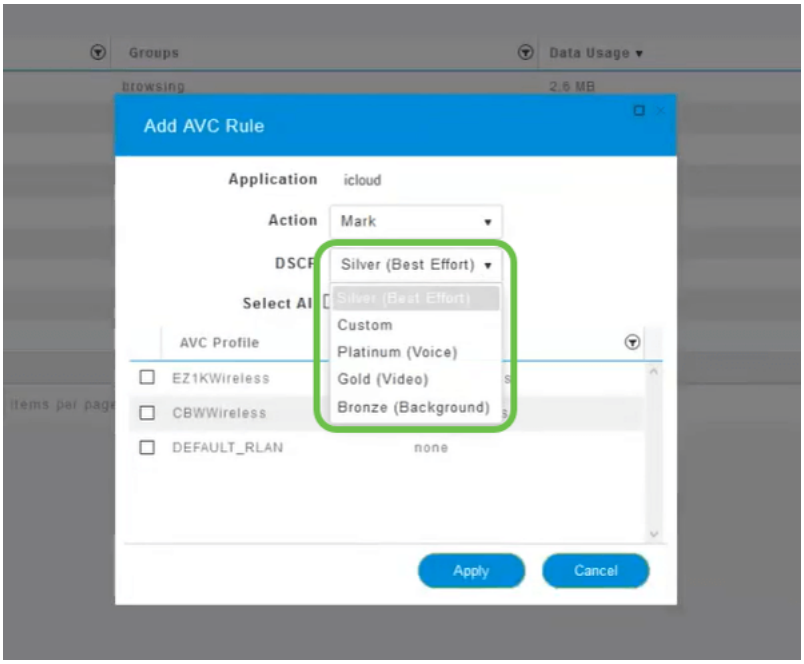
在本例中，我们将此选项留在*Mark*。

对流量采取的操作

- 标记 — 将流量类型放入差分服务代码点(DSCP)3层中的一个 — 管理应用类型可用的资源数量
- 丢弃 — 除丢弃流量外不执行任何操作
- 速率限制 — 用于设置平均速率、突发速率（以Kbps为单位）

步骤 10

单击DSCP字段中的下**拉框**以从以下选项中进行选择。



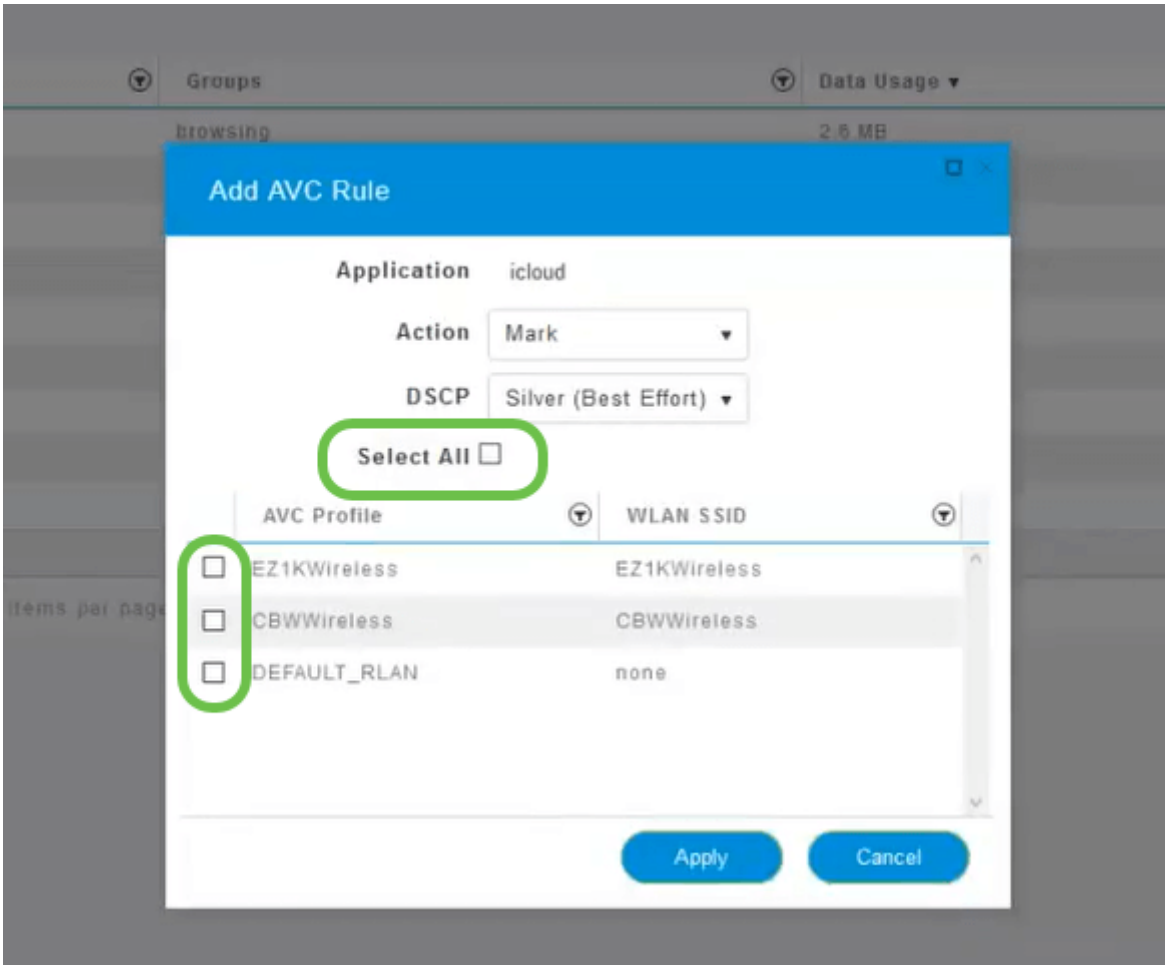
以下是要标记的流量的DSCP选项。这些选项从更少的资源进入您编辑的流量类型可用的更多资源。

- 铜级（背景）— 较少
- 银牌（尽力）
- 金牌（视频）
- 白金级（语音）更多
- 自定义 — 用户集

作为Web惯例，流量已迁移到SSL浏览，这会阻止您在数据包从网络移动到WAN时看到其内部内容。因此，大部分Web流量将使用SSL。为较低优先级设置SSL流量可能会影响浏览体验。

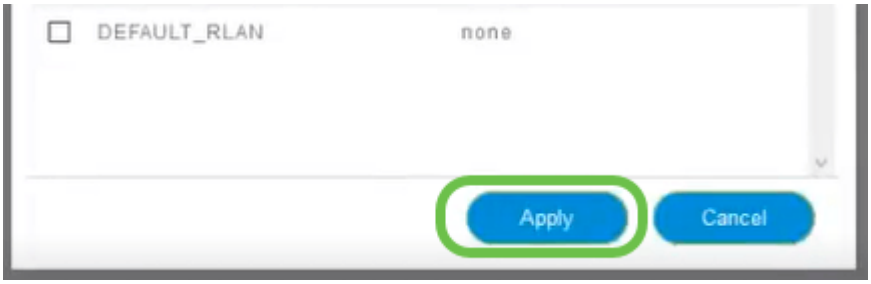
步骤 11

现在，选择要运行此策略的单个SSID，或单击“全**选**”。



步骤 12

现在单击**Apply**开始此策略。



这可能适用的两种情况：

- 访客/用户流传输大量流量，阻止任务关键型流量通过。您可以提高语音的优先级，降低Netflix流量的优先级，以改善情况。
- 可在办公时间下载大型软件更新时取消优先级或限制速率。

你成功了！应用程序分析是一种非常强大的工具，通过启用客户端分析可以进一步启用，如下一节所详述。

使用Web UI进行客户端分析（可选）

连接到网络后，设备交换客户端分析信息。默认情况下，*客户端分*析处于禁用状态。此信息可能包括：

- 主机名 — 或设备的名称
- 操作系统 — 设备的核心软件
- 操作系统版本 — 适用软件的小版本

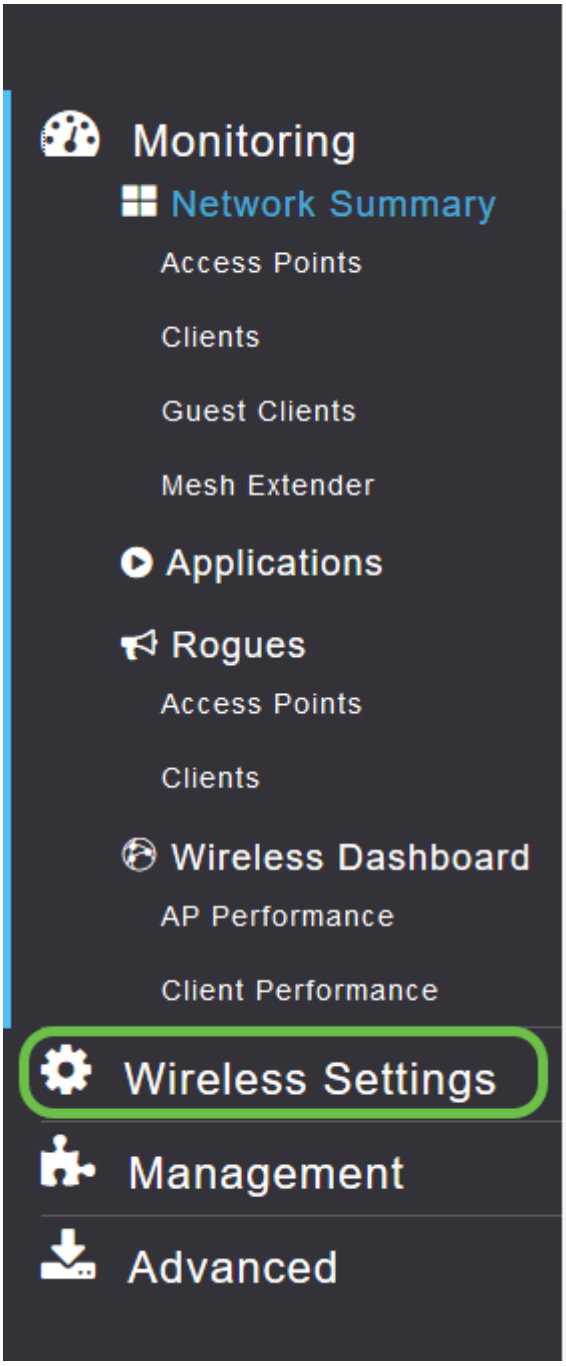
有关这些客户端的统计信息包括使用的数据量和吞吐量。

跟踪客户端配置文件可以更好地控制无线局域网。或者，您可以将其用作其他功能的功能。例如，使用不为您的业务传输任务关键型数据的应用限制设备类型。

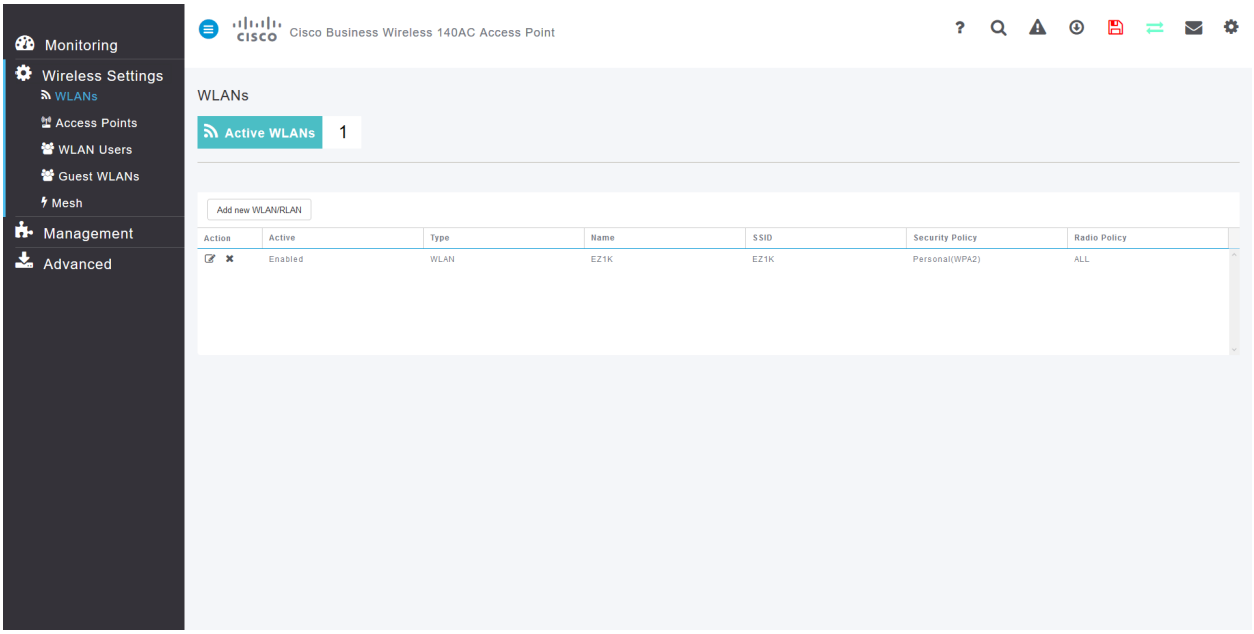
启用后，网络的客户端详细信息可在Web UI的Monitoring部分找到。

第 1 步

单击**Wireless Settings**。

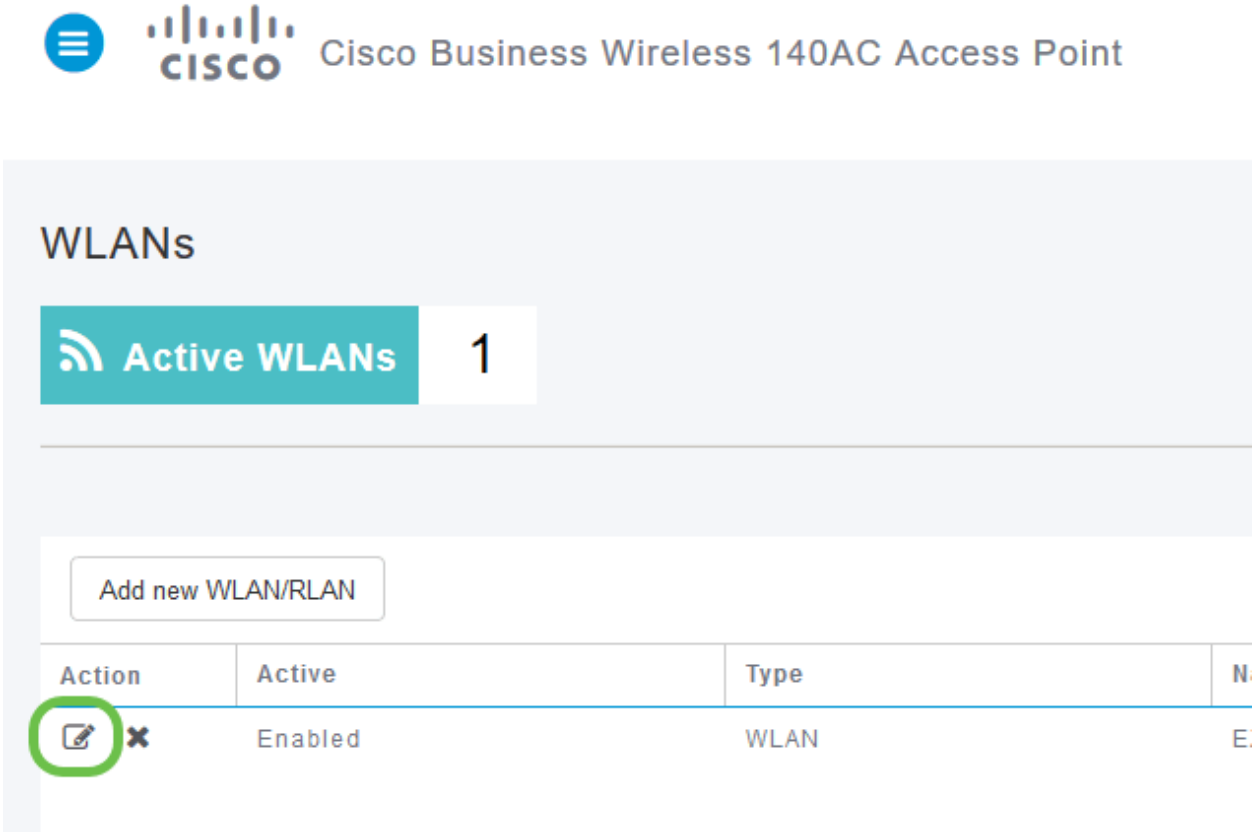


以下内容类似于您单击“无线设置”链接时看到的内容：



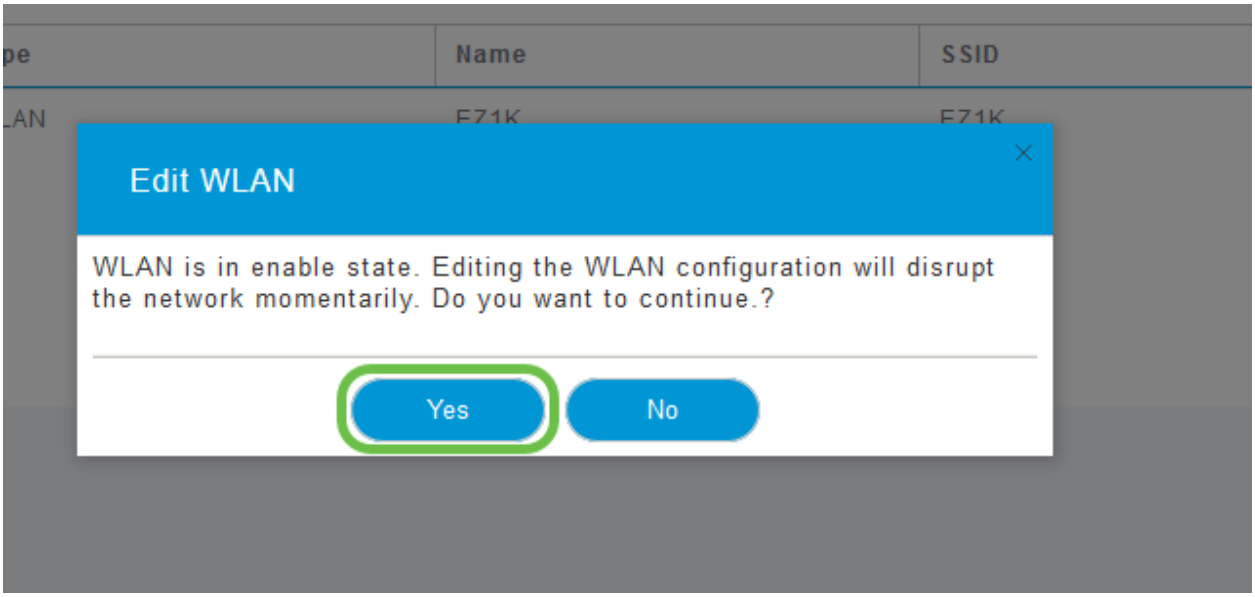
步骤 2

确定要用于应用的WLAN，然后单击**左**侧的编辑图标。



步骤 3

弹出菜单可能如下所示。此重要消息可能会暂时影响您网络上的服务。单击**是**继续。

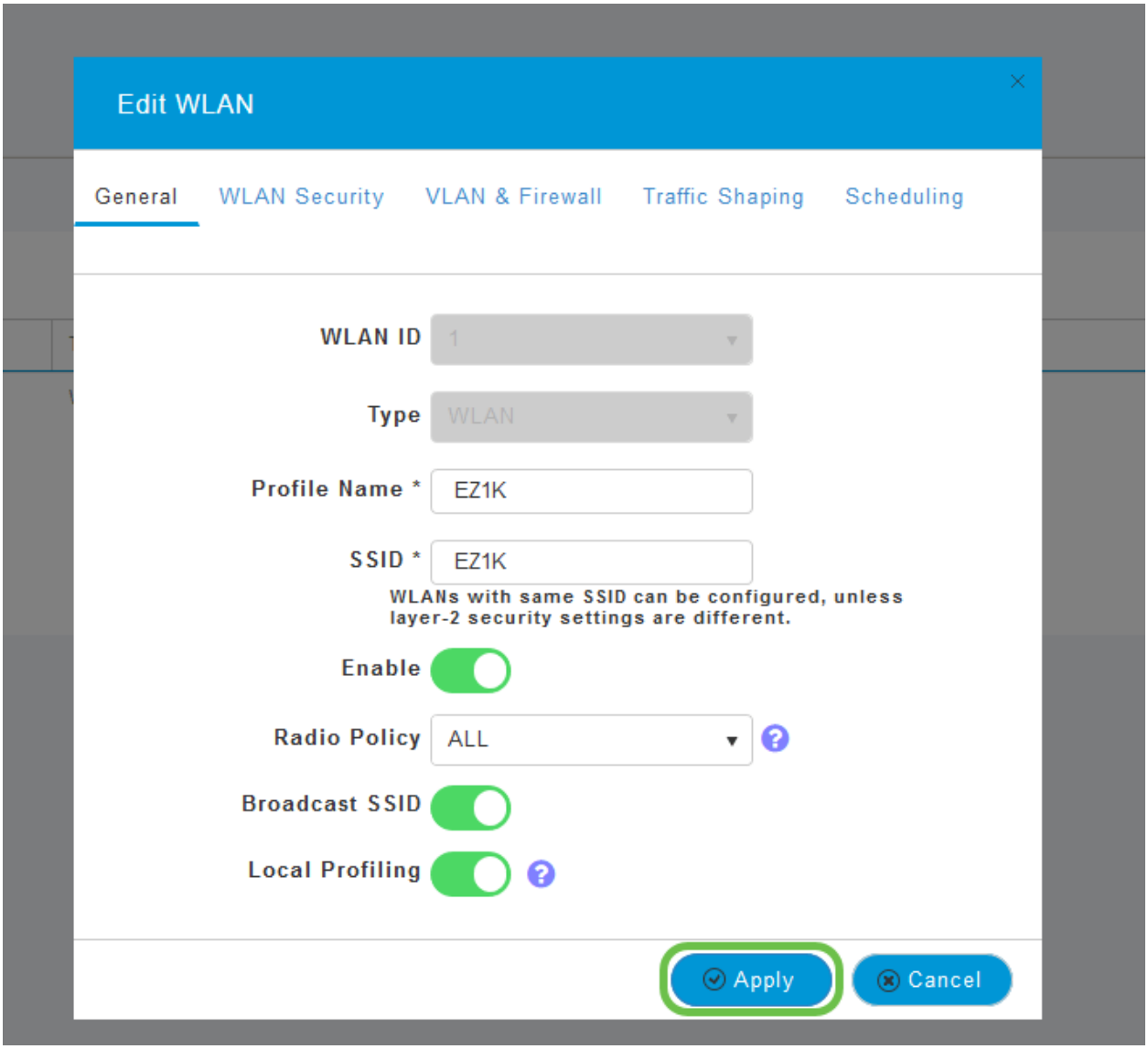


步骤 4

单击Local Profiling切换按钮**切换客**户端分析。

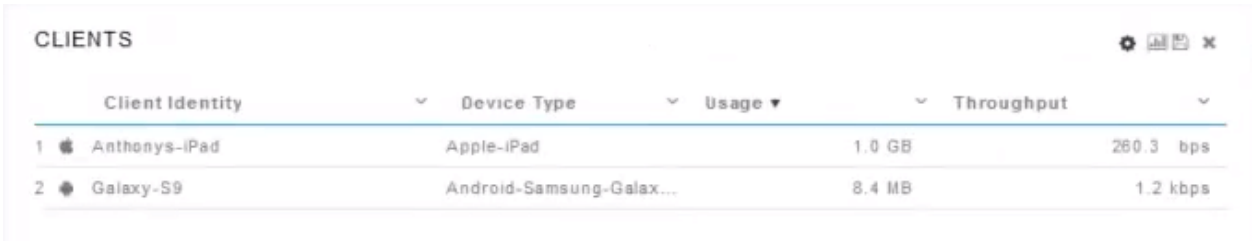
步骤 5

单击 Apply。



步骤 6

单击左侧的**Monitoring**部分菜单项。您将看到客户端数据开始出现在“监控”选项卡的“控*制面板*”中。



结论

您现在已完成安全网络的设置。多么美好的感觉，现在花一分钟庆祝，然后开始工作！

我们希望为客户提供最佳服务，因此您对此主题有任何意见或建议，请向思科内容团队发送一封电子邮件。

如果您想阅读其他文章和文档，请查看硬件的支持页面：

- 带PoE的思科RV345P VPN路由器

- 思科企业140AC接入点
- 思科企业142ACM网状扩展器