网络配置总数：使用Web UI的RV345P和Cisco Business Wireless

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。

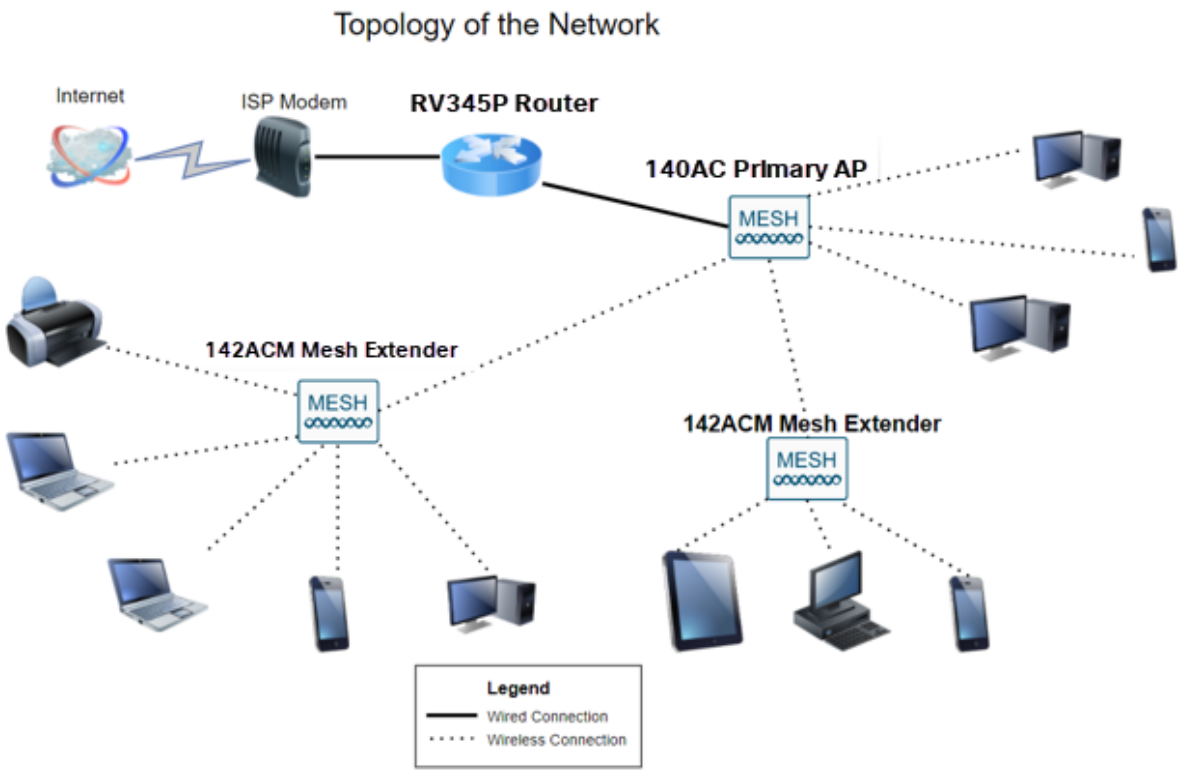
本文使用Web用户界面(UI)设置网状无线网络。如果您更喜欢使用移动应用（建议使用它来实现轻松的无线设置），请单击跳转到使用移动应用的文章。

目录

- 先决条件
  - 准备路由器
  - 获取Cisco.com帐户
- 配置RV345P路由器
  - RV345P开箱即用
  - 设置路由器
  - 排除Internet连接故障
  - 初始配置
  - 根据需要编辑IP地址（可选）
  - 升级固件（如果需要）
  - 在RV345P系列路由器上配置自动更新
- 安全选项
  - RV安全许可证（可选）
  - RV345P路由器上的Web过滤
  - Umbrella RV分支许可证（可选）
  - 其他安全选项
- VPN选项
  - VPN 传递
  - AnyConnect VPN
  - Shrew软件VPN
  - 其他VPN选项
- RV345P路由器的补充配置
  - 配置VLAN（可选）

        - 将VLAN分配到端口（可选）
        - 添加静态IP（可选）
        - 管理证书（可选）
        - 使用Dongle和RV345P系列路由器配置移动网络（可选）
    - 配置CBW140AC
        - CBW140AC开箱即用
        - 在Web UI上设置140AC主无线接入点
    - 无线故障排除提示
    - 使用Web UI配置CBW142ACM网状扩展器
    - 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进行应用分析（可选）
        - 使用Web UI的客户端分析（可选）

拓扑



简介

您的所有研究都齐聚一堂，并且您已购买思科设备，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插入路由器而非交换机。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其他功能的选项。

1. 应用控制允许您控制流量。可以将此功能配置为允许流量但记录流量、阻止流量并记录流量，或者仅阻止流量。
2. Web过滤用于防止网络流量流向不安全或不合适的网站。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来连接到您的公司办公室或数据中心。

如果要使用这些功能，您需要购买许可证。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，或者希望了解有关网状网络的更多详细信息，请查看以下文章：

- Cisco Business：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. 确保您当前有用于设置的互联网连接。

2 请联系您的Internet服务提供商(ISP)，了解他们在使用RV345P路由器时有何特殊说明。某些ISP提供带有内置路由器的网关。如果您有一个带集成路由器的网关，您可能需要禁用路由器并将广域网(WAN)IP地址（Internet提供商分配给您的帐户的唯一Internet协议地址）和所有网络流量传递到您的新路由器。

3 确定路由器的放置位置。如果可能的话，你需要一个开放区域。这可能并不容易，因为您必须将路由器从Internet服务提供商(ISP)连接到宽带网关（调制解调器）。

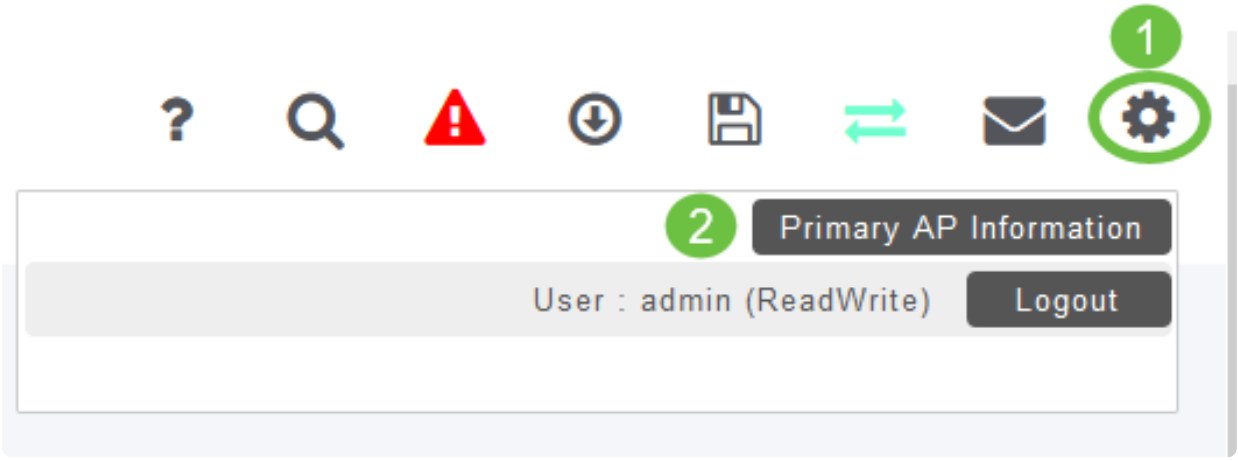
获取Cisco.com帐户

现在您拥有了思科设备，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。

如果您已经拥有帐户，可以跳至本文的下一部分。

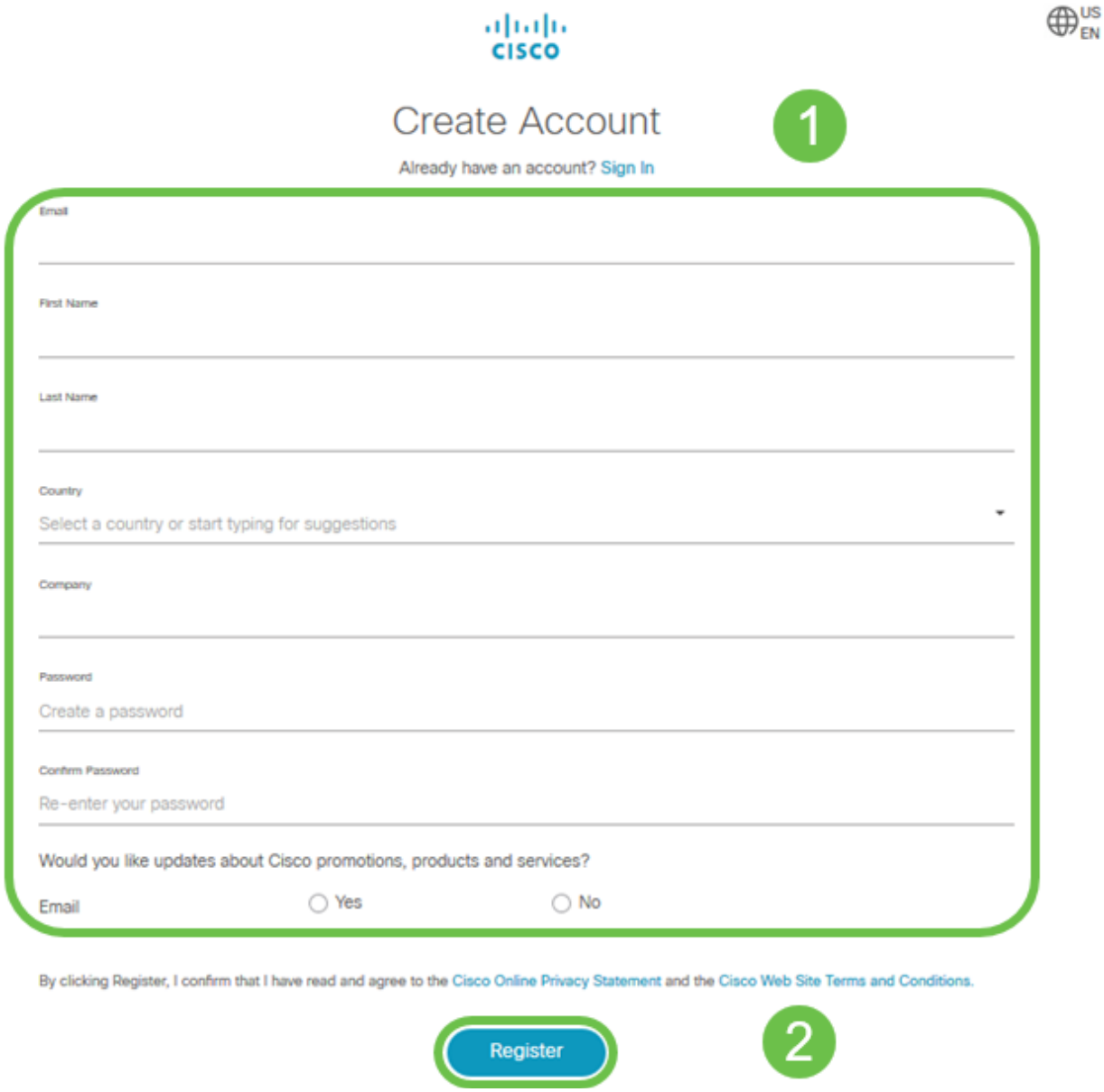
第 1 步

转到Cisco.com。单击person图标，然后单击Create an account。



第 2 步

输入创建帐户所需的详细信息，然后单击Register。按照说明完成注册过程。



如果有任何问题，请点击以跳至Cisco.com帐户注册帮助页面。

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。它使计算机能够与不在同一网络或子网中的其他计算机通信。路由器访问路由表以确定应发送数据包的位置。路由表列出了目的地址。静态和动态配置都可以在路由表中列出，以便将数据包发送到其特定目的地。

您的RV345P带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)可能会要求您修改其中一些设置。在联系您的ISP了解要求后，您可以使

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

将以太网电缆从其中一个RV345P　LAN（以太网）端口连接到计算机的以太网端口。如果您的计算机没有以太网端口，则需要适配器。终端必须与RV345P位于同一有线子网中才能执行初始配置。

第 2 步

确保使用RV345P随附的电源适配器。使用不同的电源适配器可能会损坏RV345P或导致USB转换器故障。默认情况下，电源开关处于打开状态。

将电源适配器连接到RV345P的12VDC端口，但不要将其插入电源。

第 3 步

确保调制解调器已关闭。

第 4 步

使用以太网电缆将电缆或DSL调制解调器连接到RV345P上的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的电源。重新插入调制解调器，使其也能通电。正确连接电源适配器和RV345P完成启动后，前面板上的电源指示

灯呈稳定绿色。

设置路由器

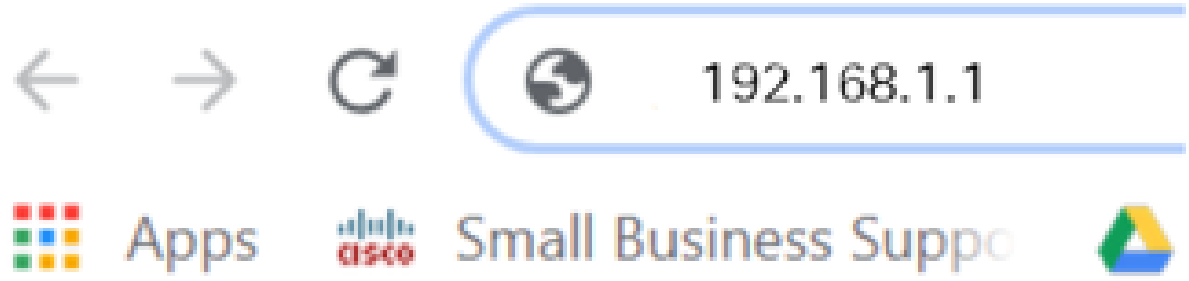
准备工作已经完成，现在需要了解一些配置！要启动Web UI，请执行以下步骤。

第 1 步

如果您的计算机配置为动态主机配置协议(DHCP)客户端，则会为PC分配192.168.1.x范围内的IP地址。DHCP自动将IP地址、子网掩码、默认网关和其他设置分配给计算机。必须将计算机设置为参与DHCP过程才能获取地址。这可以通过在计算机的TCP/IP属性中选择自动获取IP地址来实现。

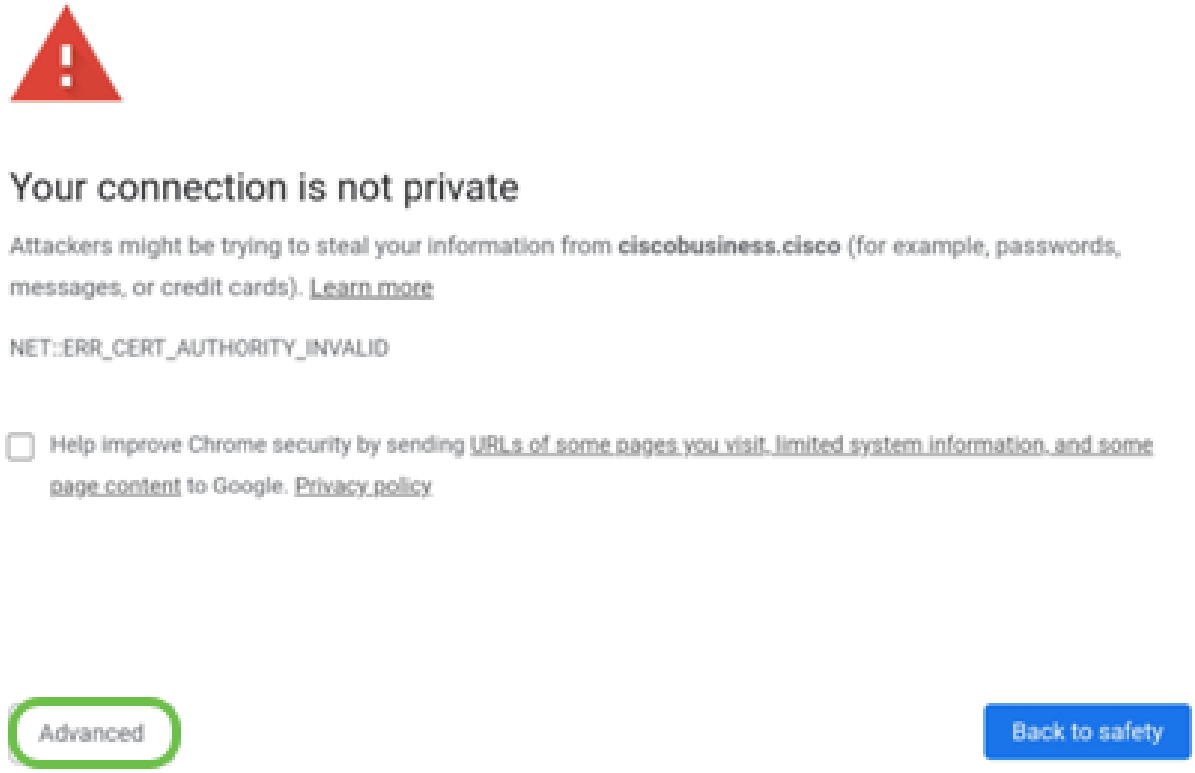
第 2 步

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。



第 3 步

浏览器可能会发出警告，指出该网站不受信任。继续浏览网站。如果您未连接，请跳至Internet连接故障排除。

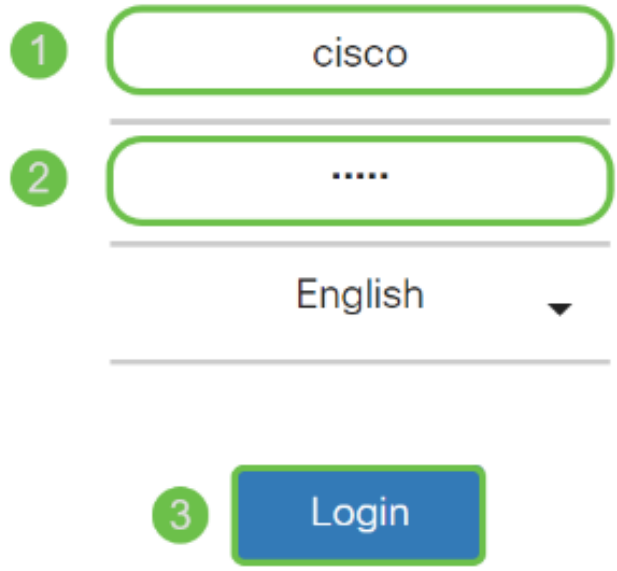


第 4 步

当登录页面显示时，输入默认用户名cisco和默认密码cisco。

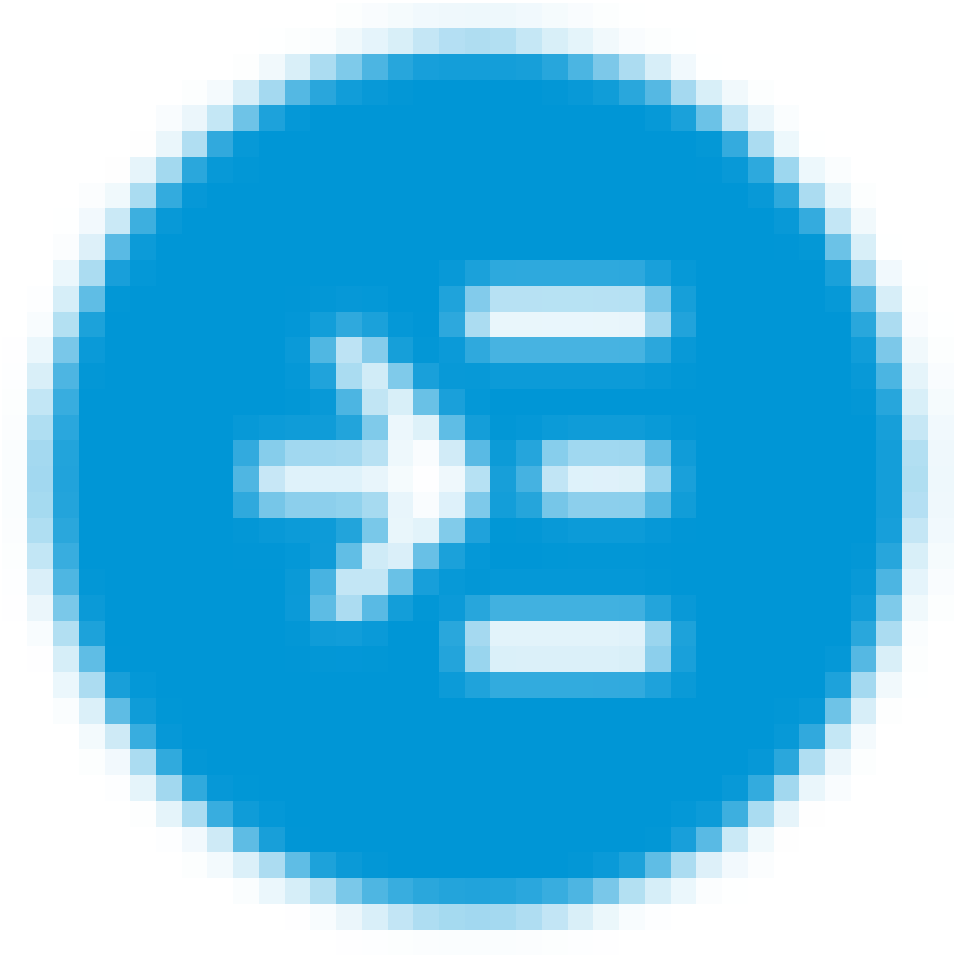
单击 Login。

有关详细信息，请单击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Getting Started页面。如果导航窗格未打开，可以通过单击菜单图标打开它。



确认连接并登录到路由器后，跳至本文的初始配置部分。

排除Internet连接故障

见鬼，如果您正在阅读此内容，则可能难以连接到Internet或Web　UI。其中一种解决方案应该会有所帮助。

在连接的Windows操作系统上，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。

如果连接没有发生，您可以查看此故障排除文章。

其他需要尝试的事情：

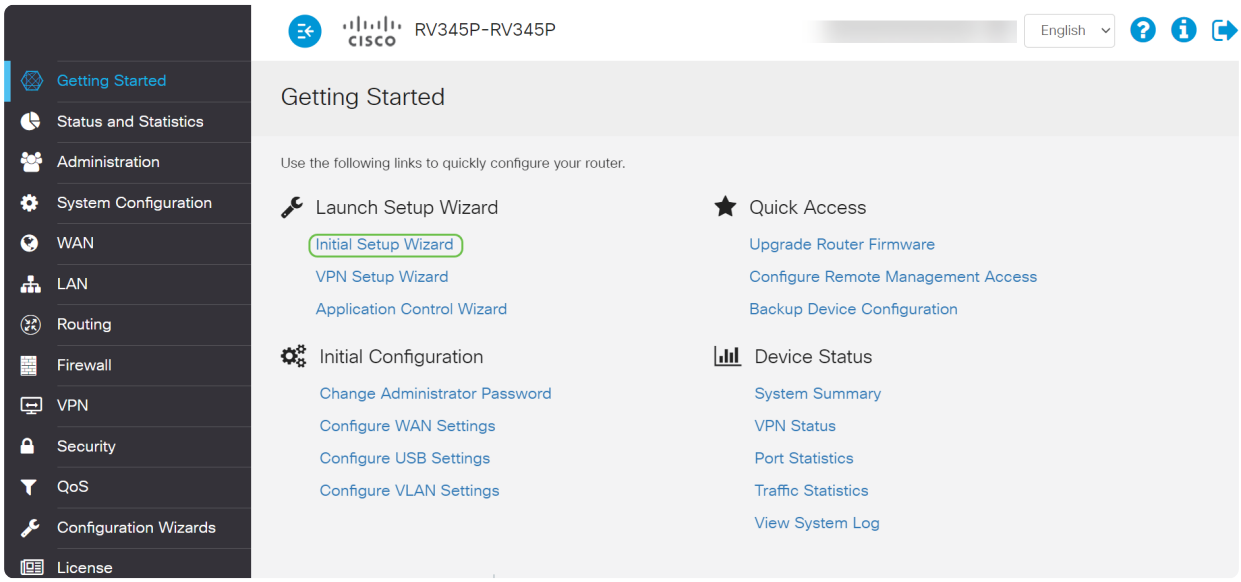
1. 验证您的Web浏览器未设置为“脱机工作”。
2. 检查以太网适配器的局域网连接设置。PC应通过DHCP获取IP地址。或者，PC可以拥有一个192.168.1.x范围内的静态IP地址，默认网关设置为192.168.1.1（RV345P的默认IP地址）。 若要连接，可能需要修改RV345P的网络设置。如果使用Windows 10，请查看Windows 10说明以修改网络设置。
3. 如果现有设备占用了192.168.1.1 IP地址，您需要解决此冲突才能使网络正常运行。在本部分末尾对此进行详细说明，或单击此处直接进行说明。
4. 通过关闭两台设备来重置调制解调器和RV345P。接下来，打开调制解调器的电源，使其处于空闲状态大约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ISP将DSL调制解调器置于网桥模式。

初始配置

建议您完成本部分中列出的初始设置向导步骤。您可以随时更改这些设置。

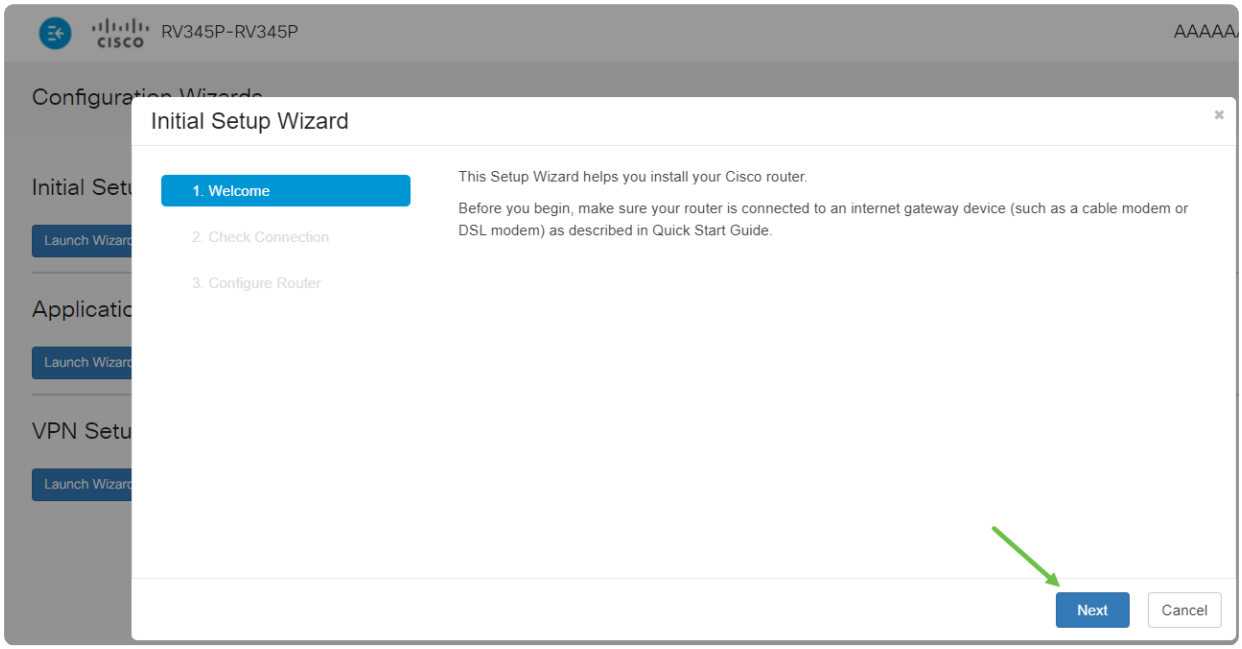
第 1 步

从Getting Started页单击Initial Setup Wizard。



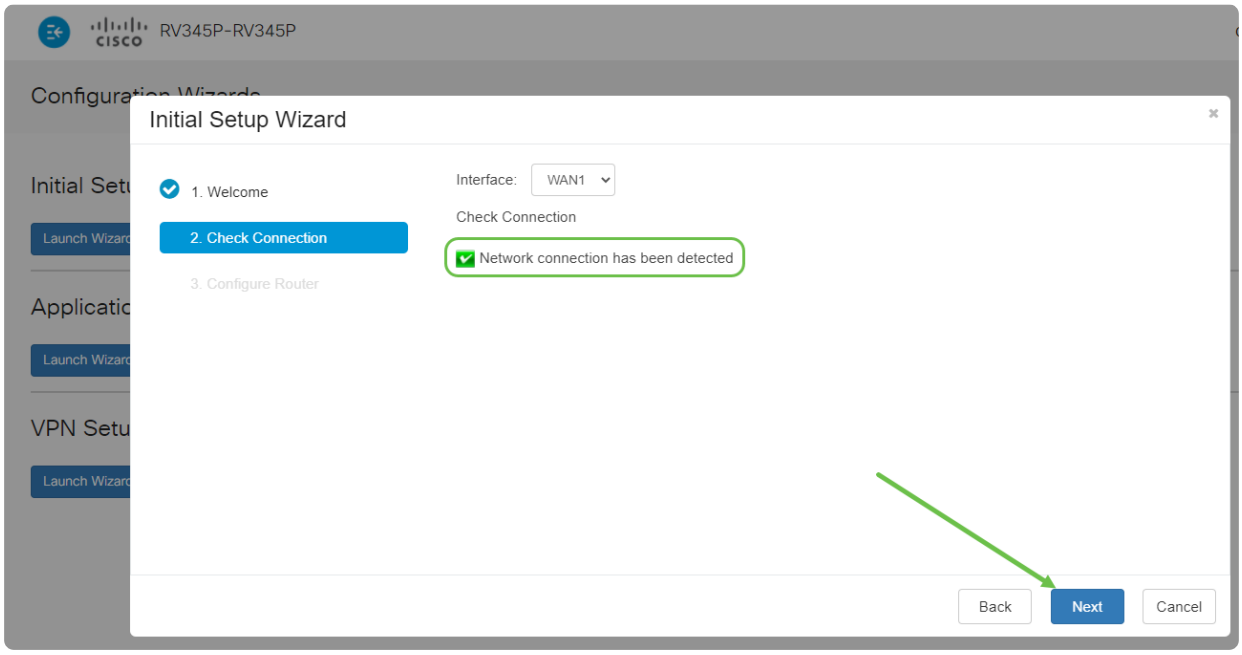
第 2 步

此步骤确认电缆已连接。由于您已经确认了这一点，请单击Next。



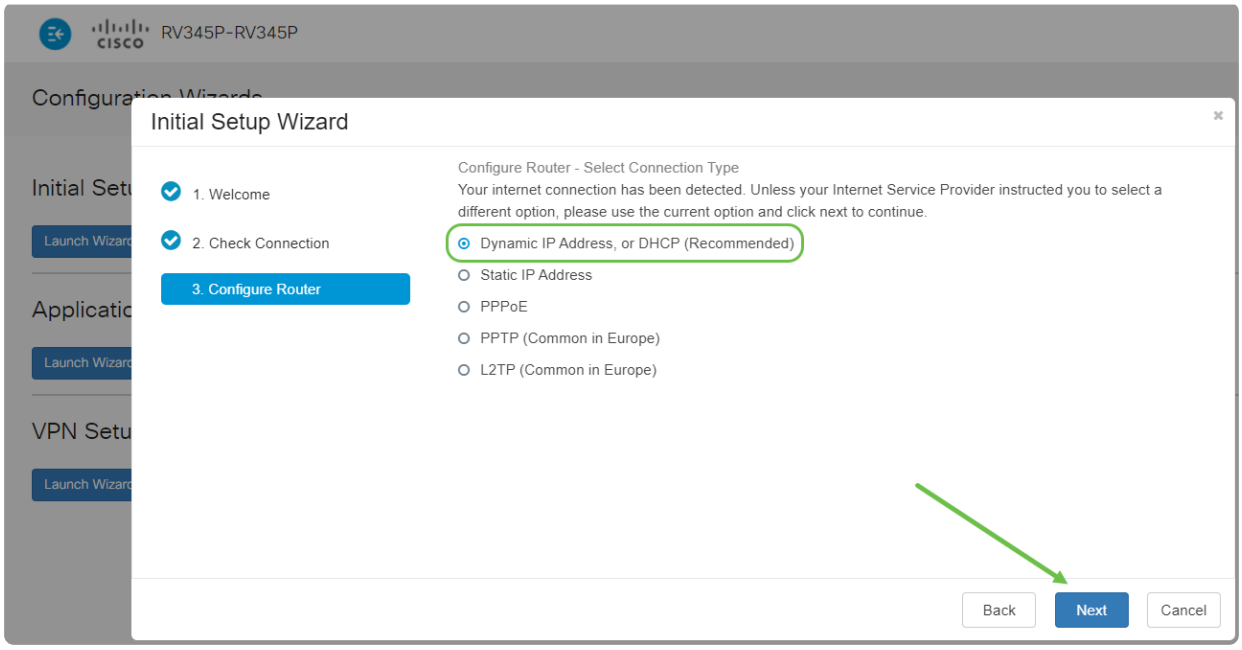
第 3 步

此步骤包含确保路由器连接的基本步骤。由于您已经确认了这一点，请单击Next。



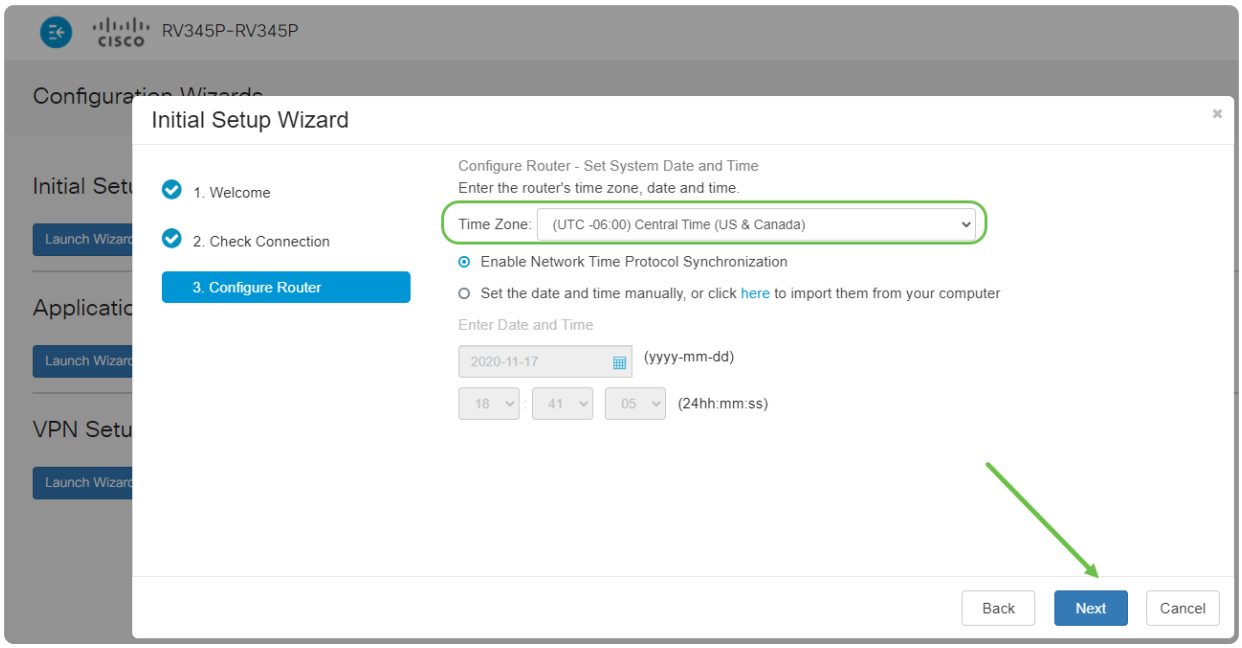
第 4 步

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



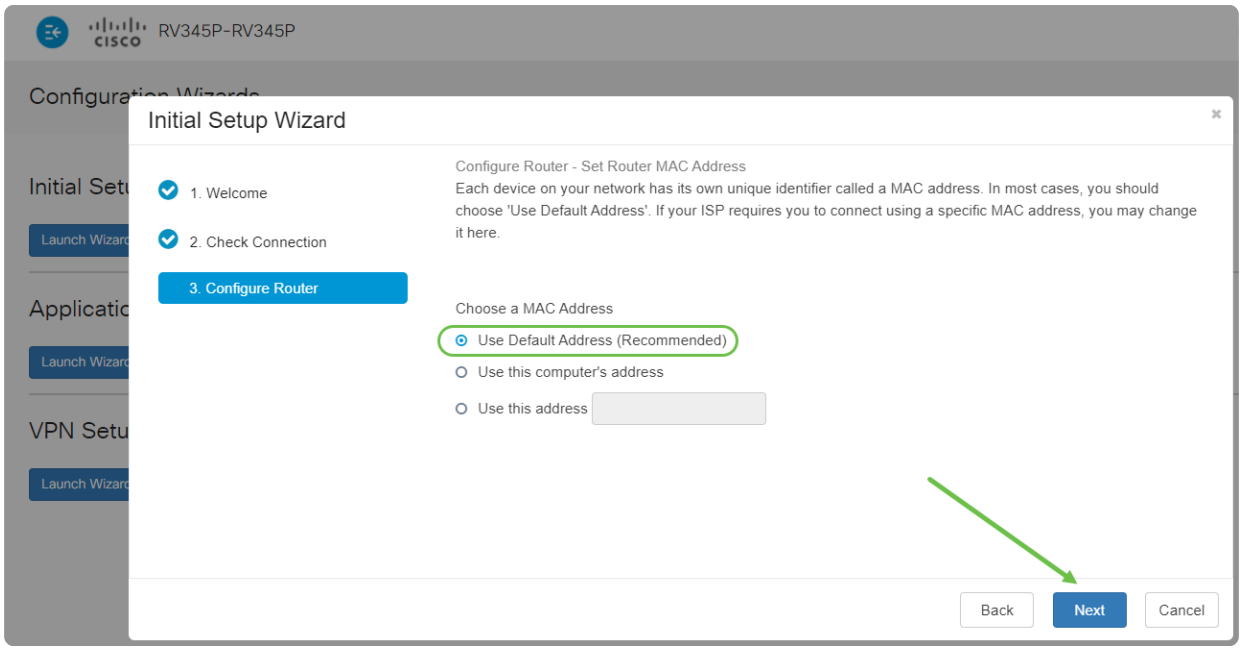
步骤 5

系统将提示您设置路由器时间设置。这一点非常重要，因为它可在查看日志或排除事件故障时确保准确性。选择Time Zone，然后单击Next。



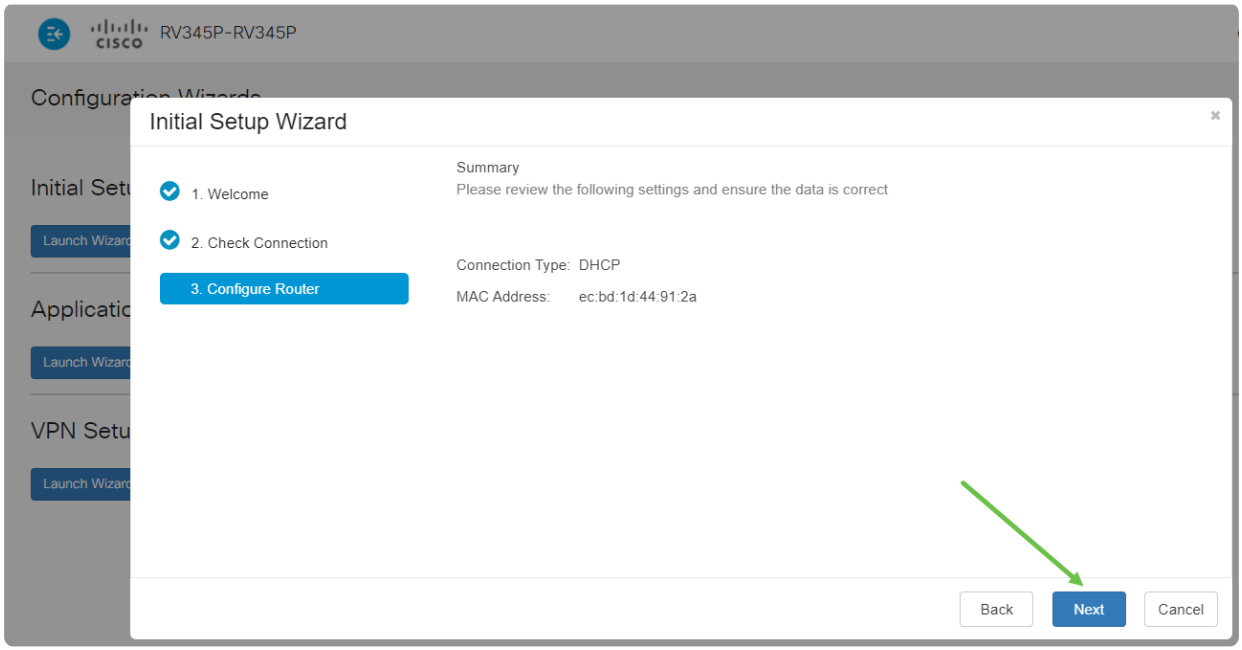
第 6 步

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。



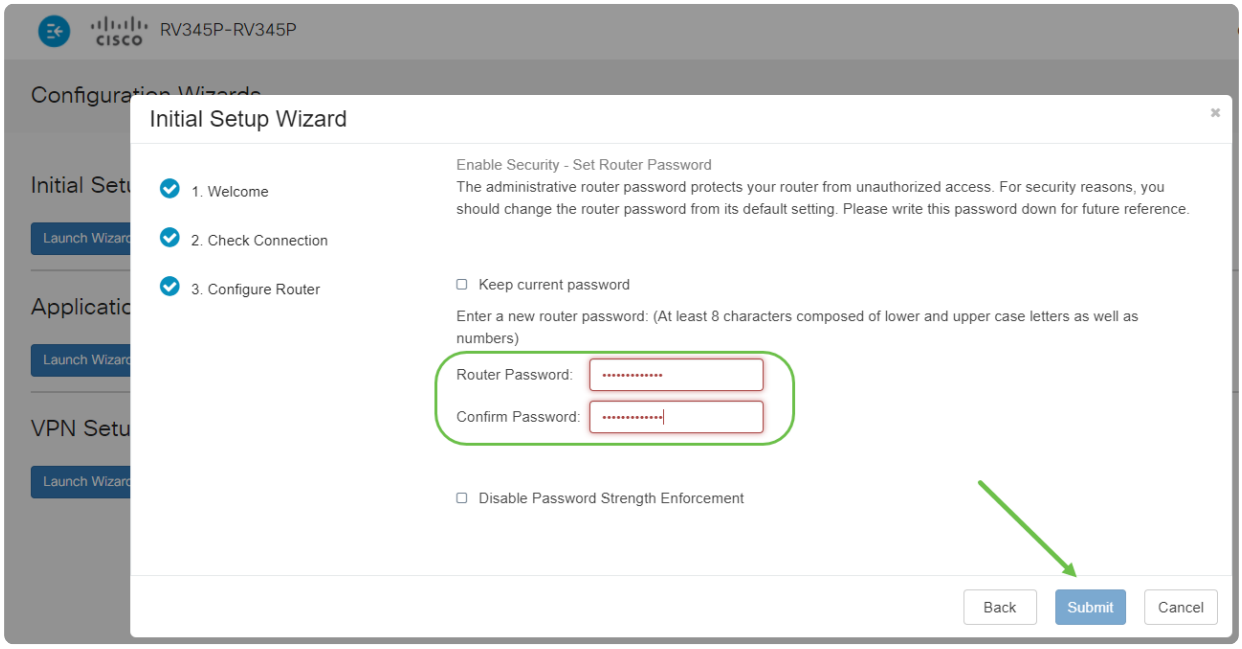
第 7 步

下一页是所选选项的摘要。查看并点击下一步（如果满意）。



步骤 8

在下一步中，您将选择登录路由器时使用的密码。密码的标准是包含至少8个字符（大写和小写）并包含数字。请输入一个符合强度要求的密码。单击 Next。记下密码以便将来登录。



ⓘ Note: 不建 议您选择Disable Password Strength Enforcement。此选项允许您选择简单到123的密码，该密码将简单到1-2-3，便于恶意攻击者破解。

步骤 9

单击save图标。



如果您需要有关这些设置的更多信息，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。如果您需要自定义设置，请查看RV345P路由器上的配置以太网供电(PoE)设置。

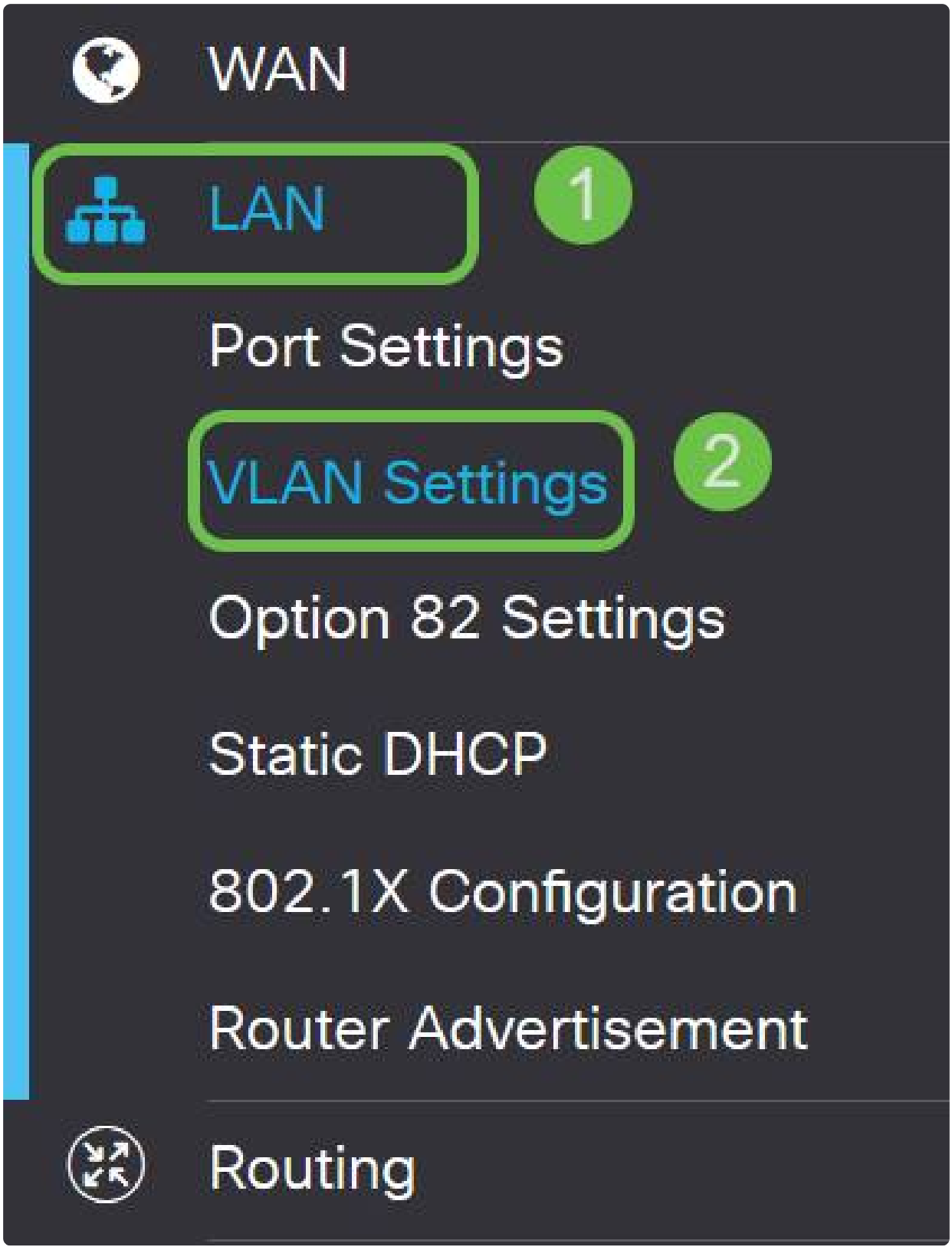
根据需要编辑IP地址（可选）

完成初始设置向导后，您可以通过编辑VLAN设置来设置路由器上的静态IP地址。

只有当您的路由器IP地址需要在现有网络中分配特定地址时，才需要执行此过程。如果您不需要编辑IP地址，可以转到本文的下一部分。

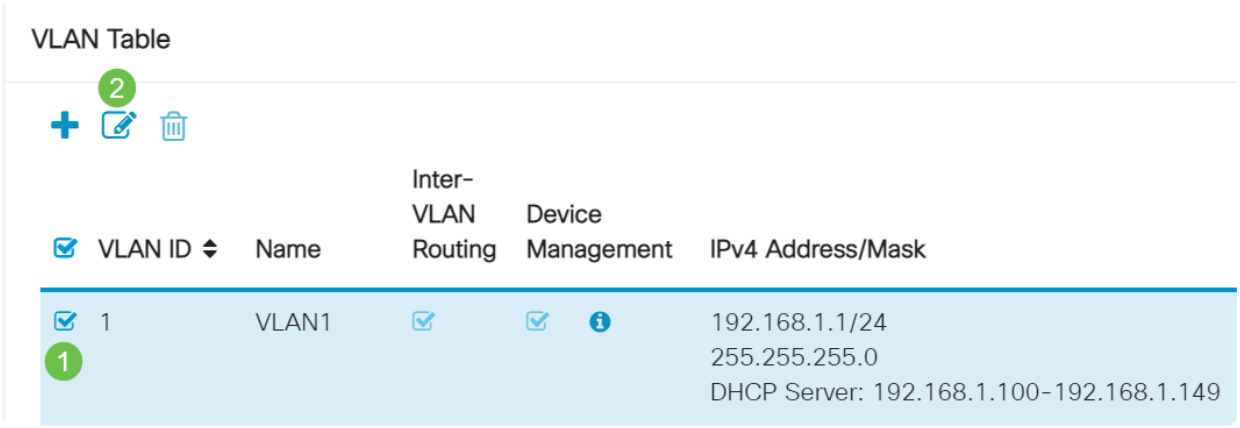
第 1 步

在左侧菜单中，单击LAN > VLAN Settings。



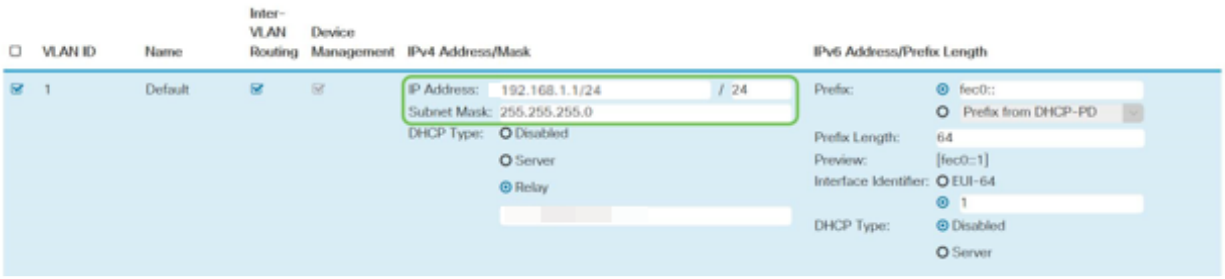
第 2 步

选择包含路由设备的VLAN，然后点击编辑图标。



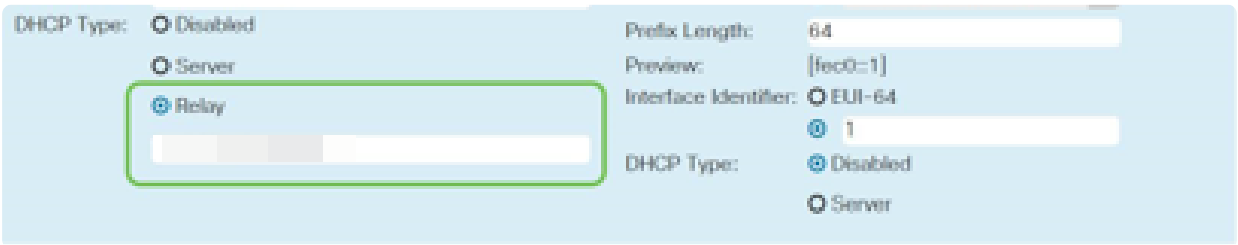
第 3 步

输入所需的静态IP地址，然后单击右上角的Apply。



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，您可以使用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。

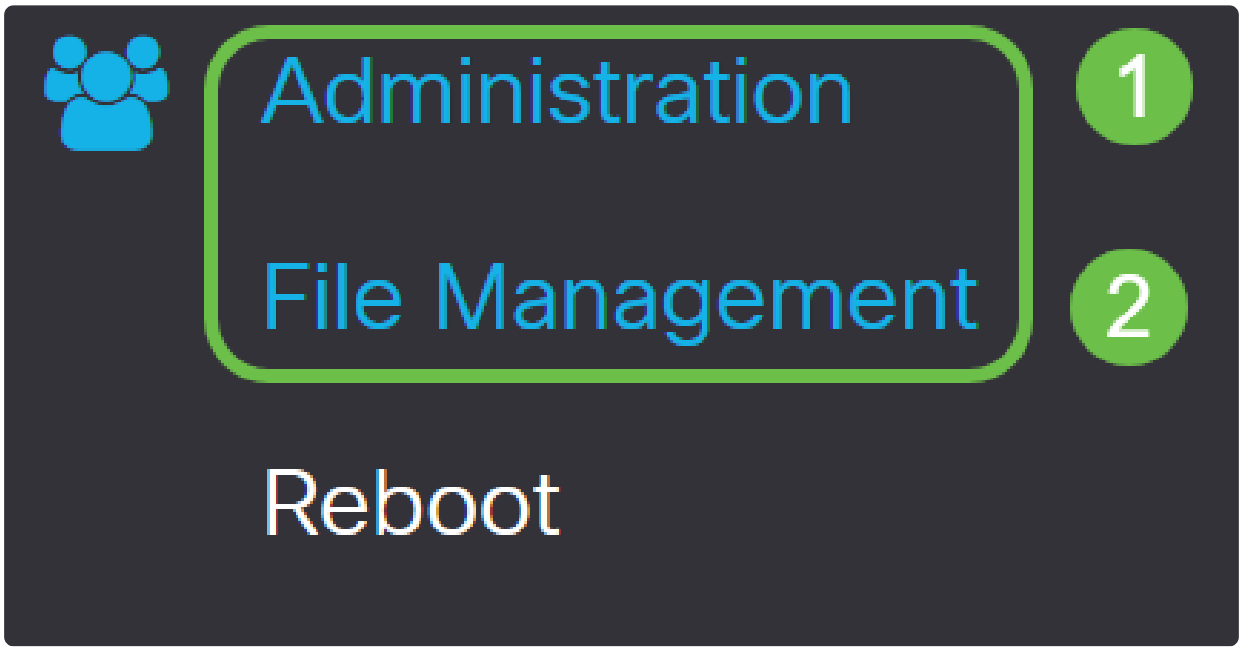


升级固件（如果需要）

这是很重要的一步，不要跳过！

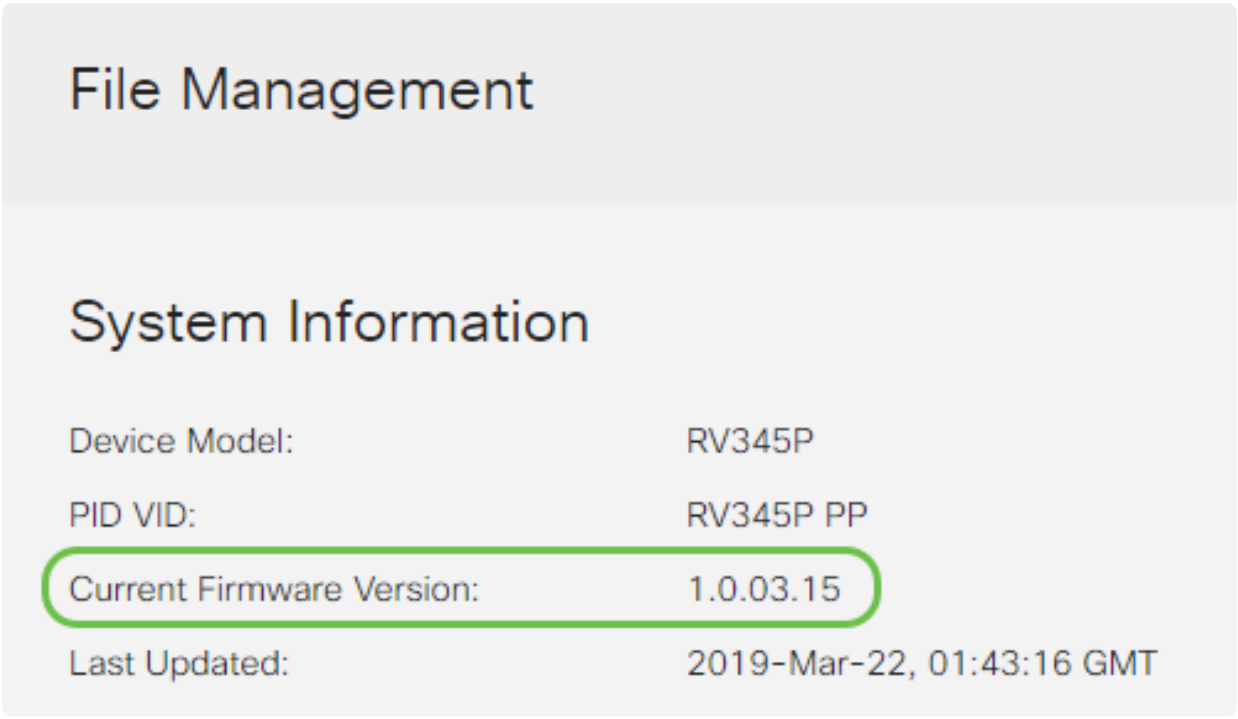
第 1 步

选择Administration > File Management。



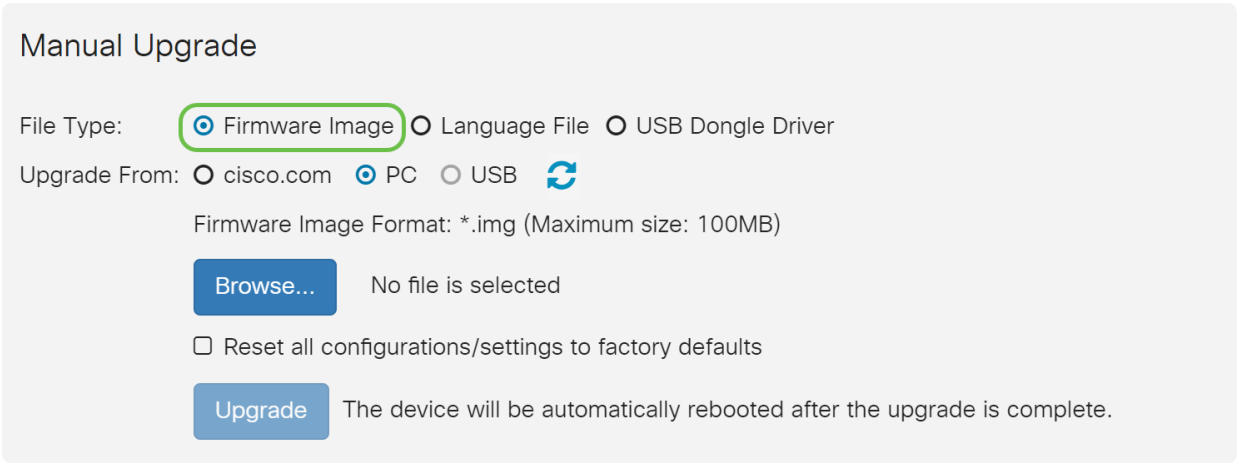
在System Information区域中，以下子区域描述以下内容：

- 设备型号 — 显示设备的型号。
- 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 — 思科网站上提供的最新软件版本。
- 固件上次更新 — 路由器上上次固件更新的日期和时间。



第 2 步

在Manual Upgrade部分下，单击Firmware Image单选按钮，然后选择File Type。



第 3 步

在Manual　Upgrade页面上，点击单选按钮选择cisco.com。有几种其他选项，但这是进行升级最简单的方法。此过程直接从思科软件下载网页安装最新的升级文件。

ⓘ Note: 如果您的设备未连接到Internet或正处于Internet断开状态，您将无法从cisco.com进行升级。如果这适用于您，您可以在此处找到替代 选项。



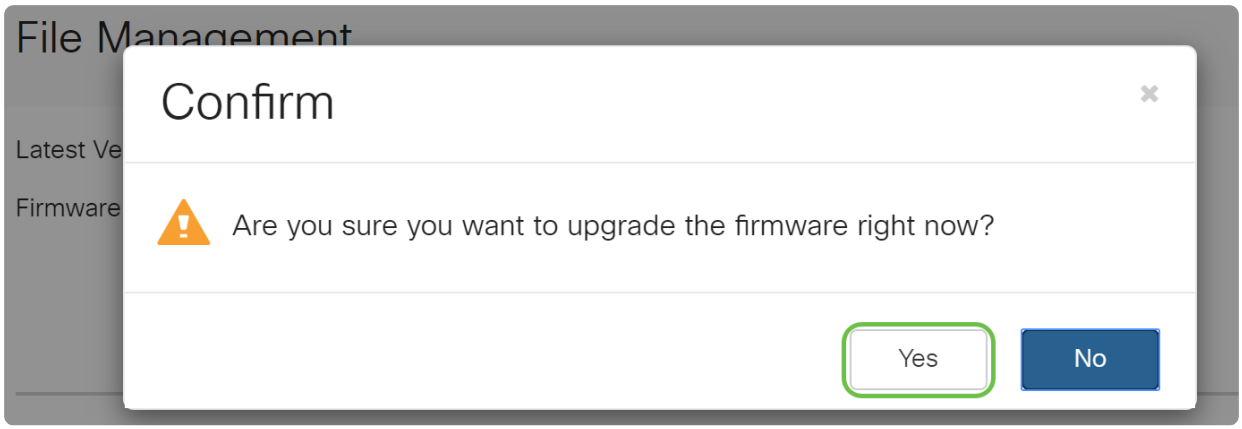
第 4 步

单击Upgrade。

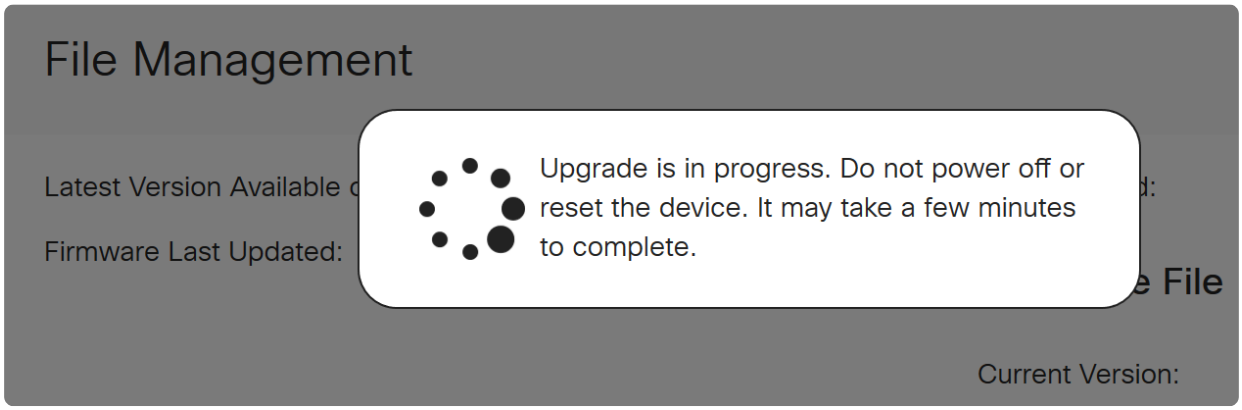


步骤 5

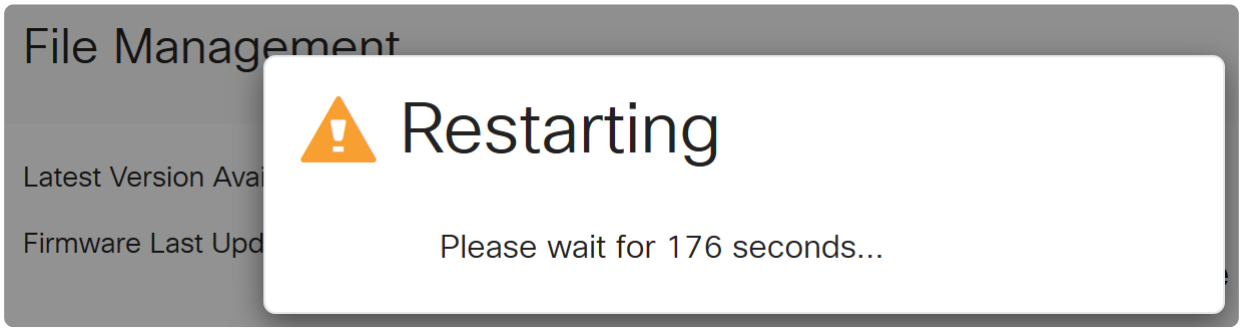
在确认窗口中单击Yes以继续。



ⓘ Note: 更新过程需要不间断地运行。升级过程中，屏幕上将显示以下消息。

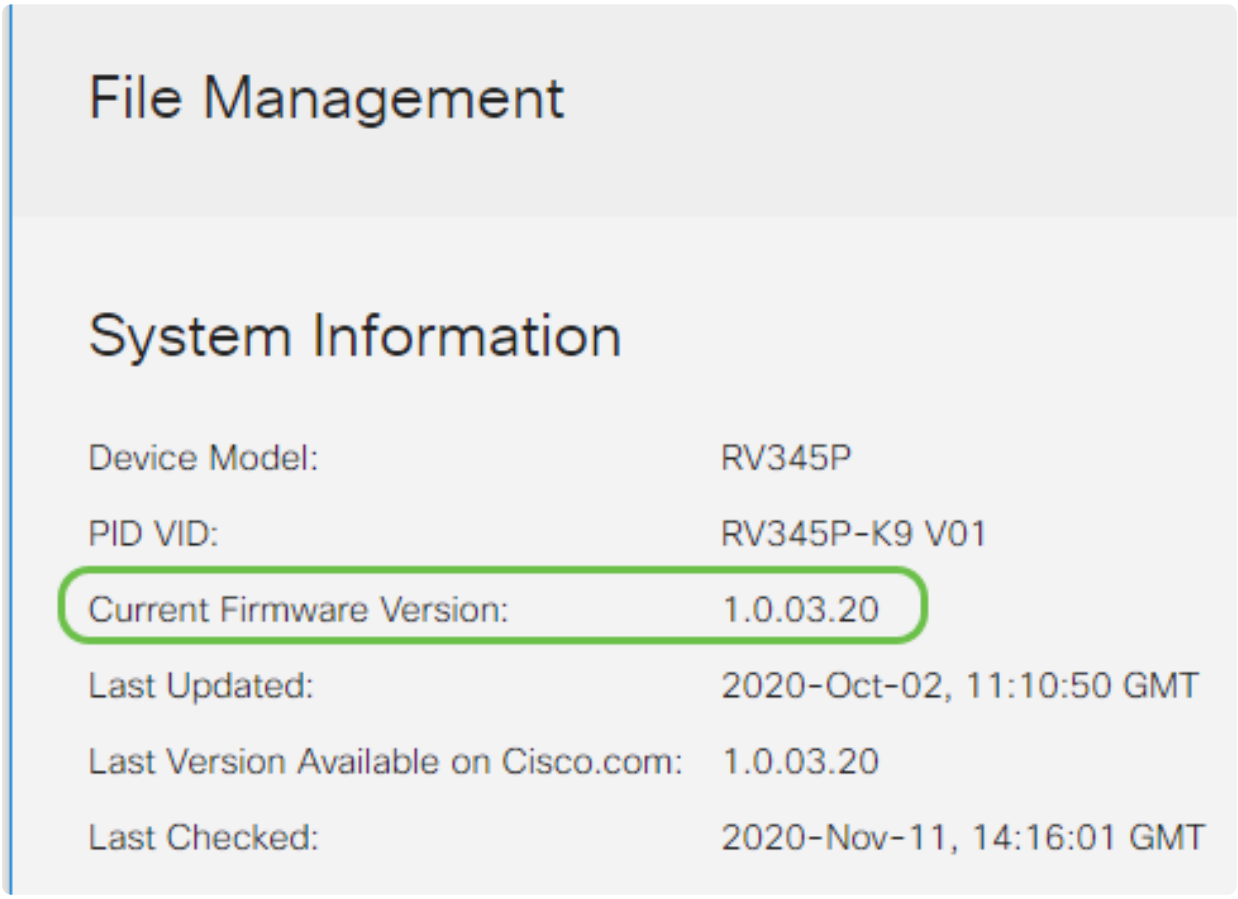


升级完成后，将弹出一个通知窗口，通知您路由器将重新启动Restarting，并注明预计完成此过程所需的时间。之后，您将注销。



第 6 步

重新登录到基于Web的实用程序以验证路由器固件是否已升级，然后滚动到系统信息。Current Firmware Version区域现在应显示升级后的固件版本。

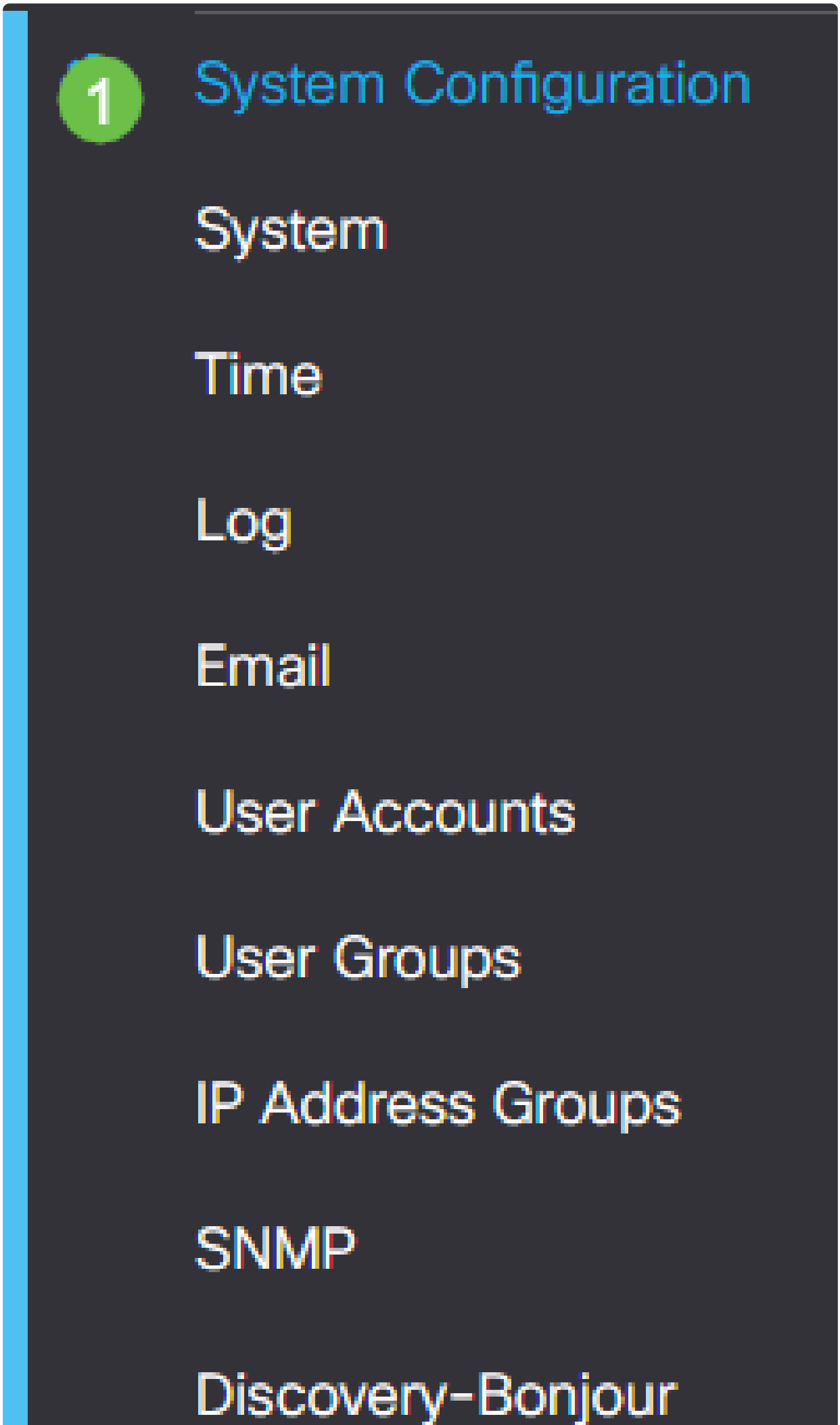


在RV345P系列路由器上配置自动更新

由于更新非常重要，而您又很忙，因此从这里向外配置自动更新是很有意义的！

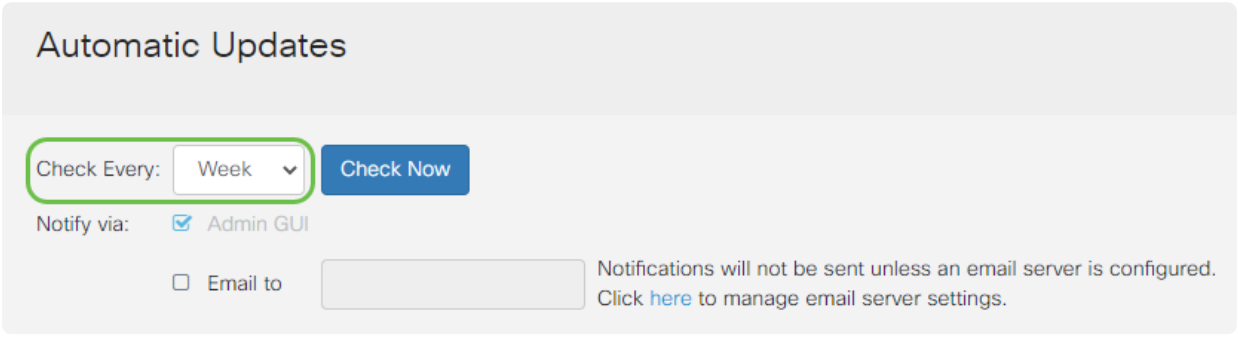
第 1 步

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


1
System Configuration
System
Time
Log
Email
User Accounts
User Groups
IP Address Groups
SNMP
Discovery-Bonjour

第 2 步

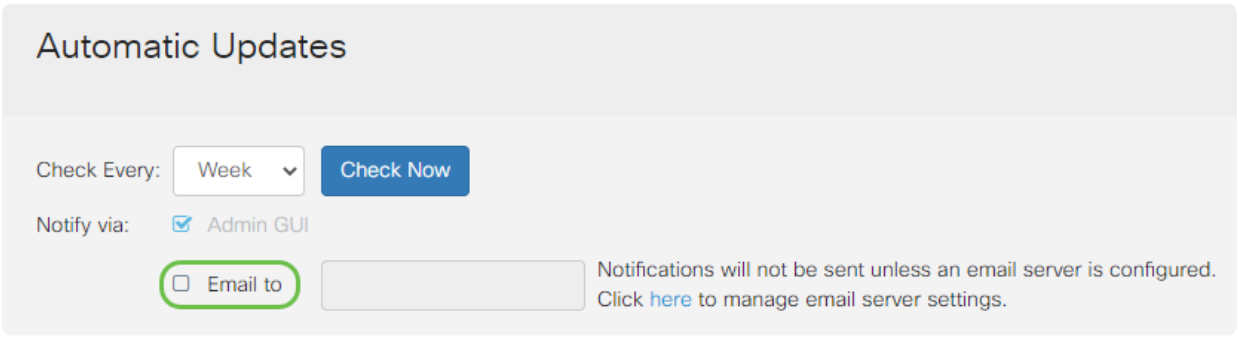
从Check Every下拉列表中，选择路由器检查更新的频率。



第 3 步

在Notify　via区域中，选中Email　to复选框以通过邮件接收更新。默认情况下，Admin GUI复选框处于启用状态，且无法禁用。更新可用后，通知将显示在基于Web的配置中。

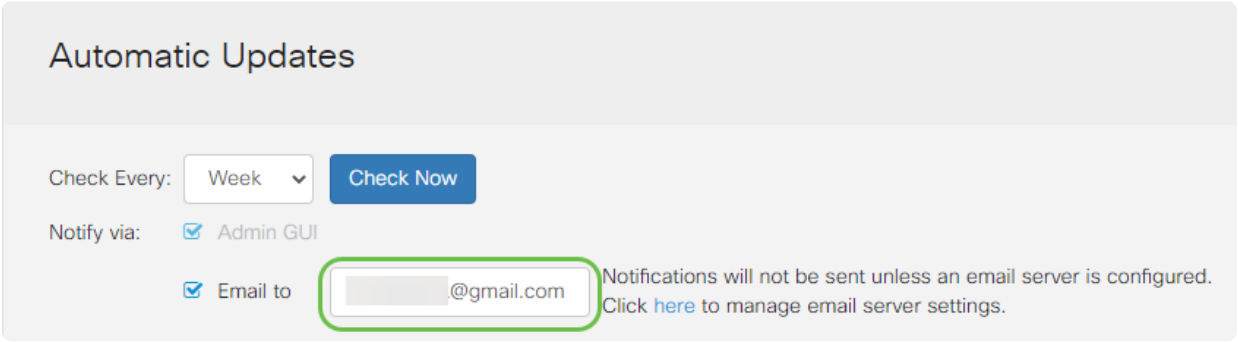
如果要设置电子邮件服务器设置，请单击此处了解方法。



第 4 步

在Email to address字段中输入电子邮件地址。

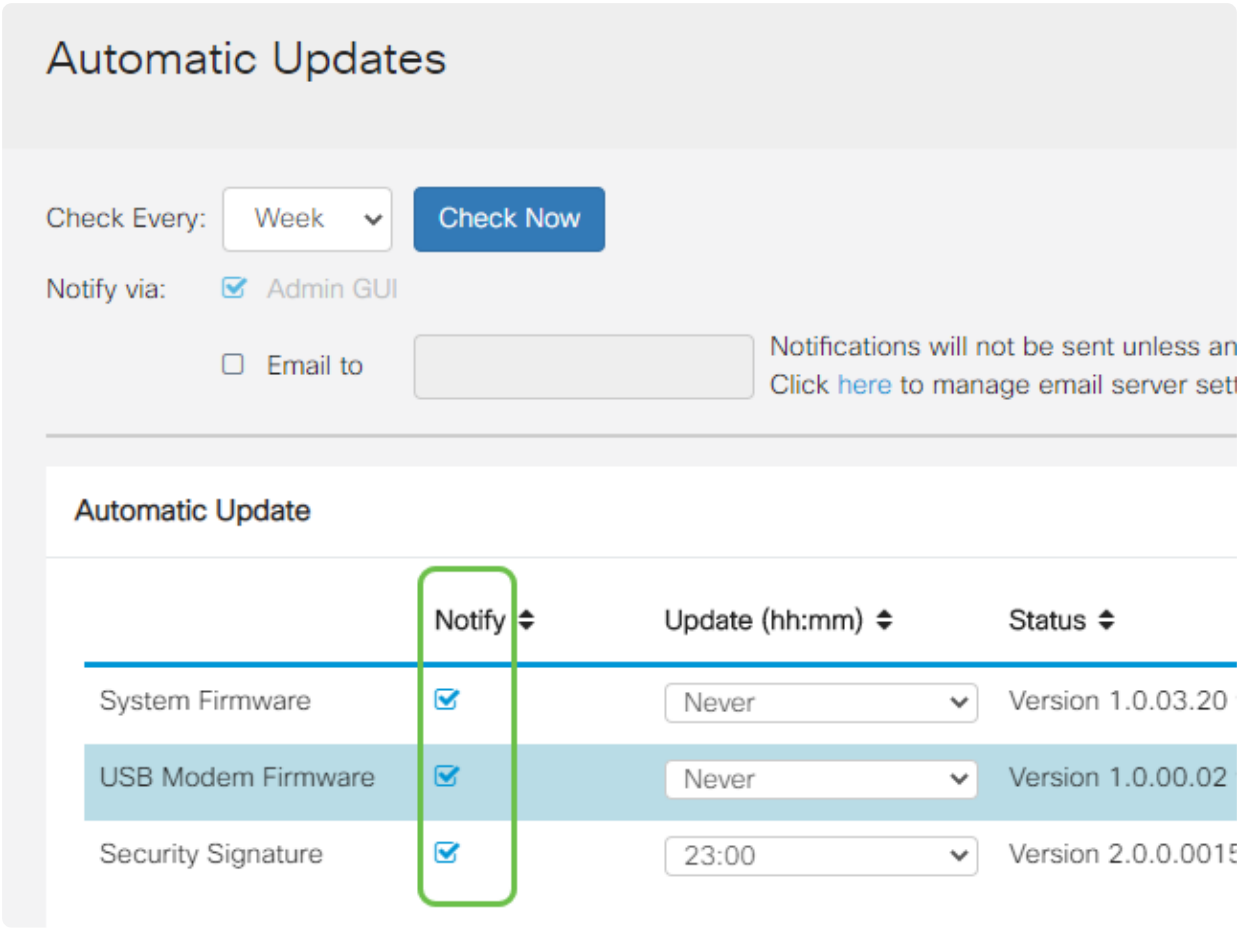
ⓘ Note: 强烈建议使用单独的电子邮件帐户，而不是使用个人电子邮件来维护隐私。



步骤 5

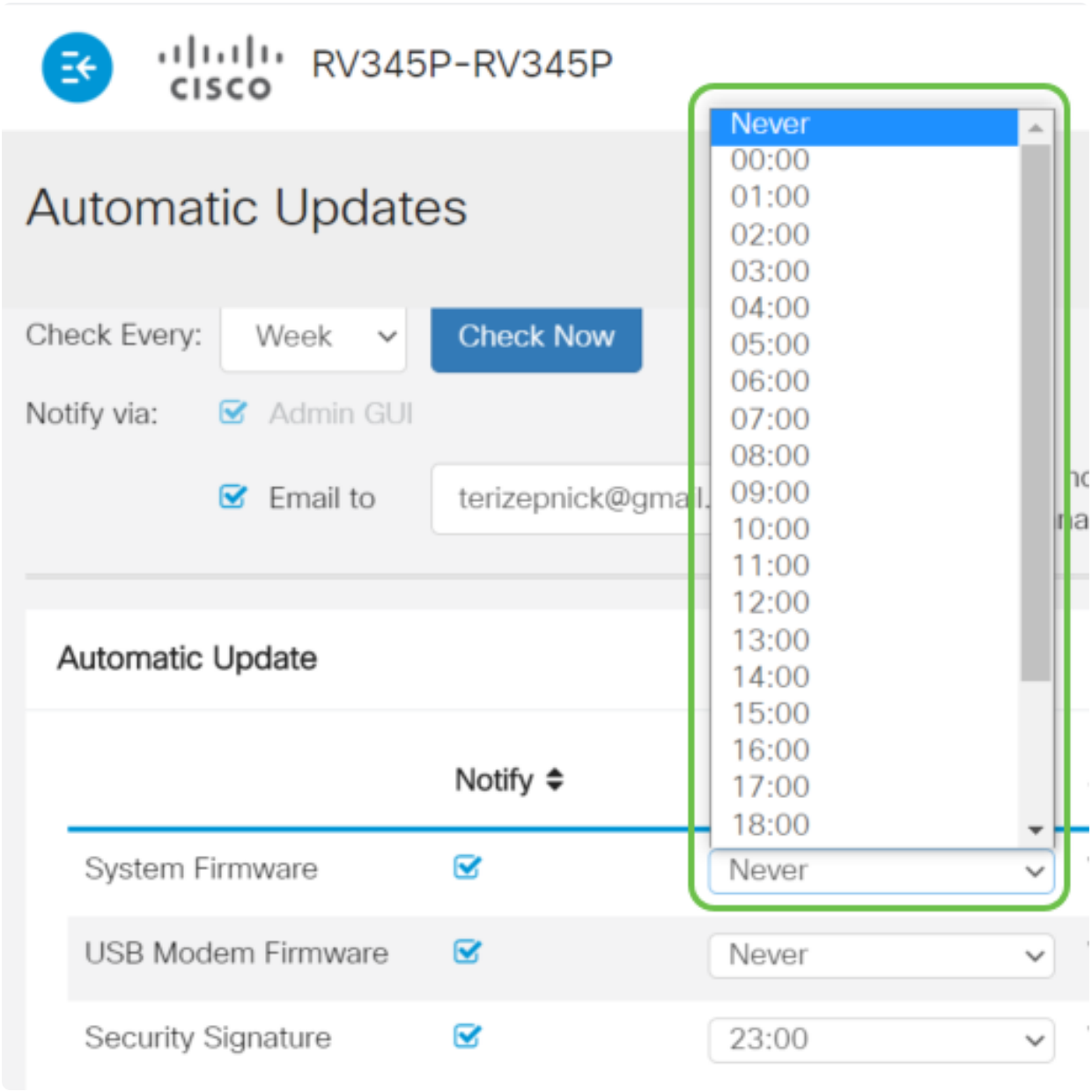
在Automatically Update区域下，选中要通知的更新类型的Notify复选框。选项有：

- 系统固件 — 设备的主要控制程序。
- 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 — 这将包含Application Control的签名，用于识别应用、设备类型、操作系统等。



第 6 步

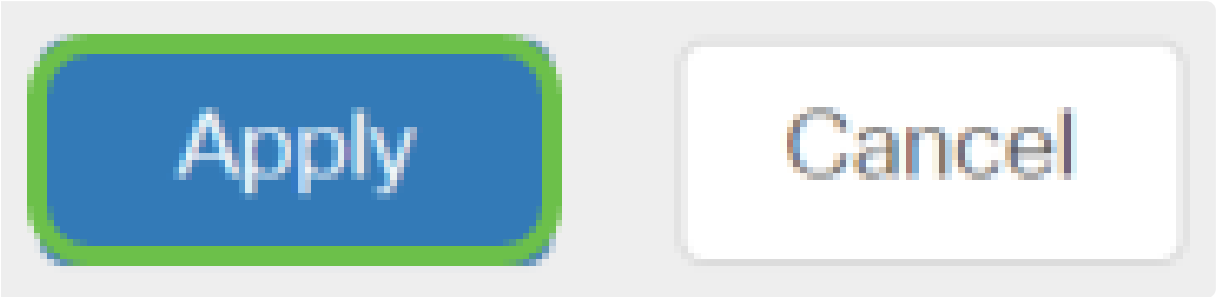
从Automatic　Update下拉列表中，选择要完成自动更新的当天时间。有些选项可能会因您选择的更新类型而异。安全签名是进行即时更新的唯一选项。建议您在办公室关闭时设置时间，以免服务在不方便的时间中断。



状态显示当前运行的固件版本或安全签名。

第 7 步

单击 Apply。



步骤 8

要永久保存配置，请转到“复制/保存配置”页或单击该页上方的保存图标。



太好了，您的路由器基本设置已完成！现在，您可以了解一些配置选项。

安全选项

当然，您希望您的网络是安全的。有一些简单的选项，例如设置复杂的密码，但如果您想采取更安全的网络措施，请查阅本部分的安全信息。

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。它可以提高网络可用性、加快补救速度，并提供全面的威胁防护。
- 防病毒软件：通过扫描各种协议（例如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）的应用来防御病毒。
- 网络安全：在连接到Internet的同时提高业务效率和安全性，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。它是基于云的，包含80多个类别，分类域超过4.5亿个。
- 应用识别：确定策略并将其分配给Internet应用程序。自动识别500个不同的应用。
- 客户端标识：动态地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Web过滤。Web过滤功能允许您管理对不当网站的访问。它可以屏蔽客户端的Web访问请求以确定是允许还是拒绝该网站。

> ⓘ Note: 许可的安全功能可免费试用90天。如果要在评估期后继续使用路由器的高级安全功能，则必须获取并激活许可证。

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

如果您不需要任何安全许可证，请单击以跳转至本文档的VPN部分。

智能帐户简介

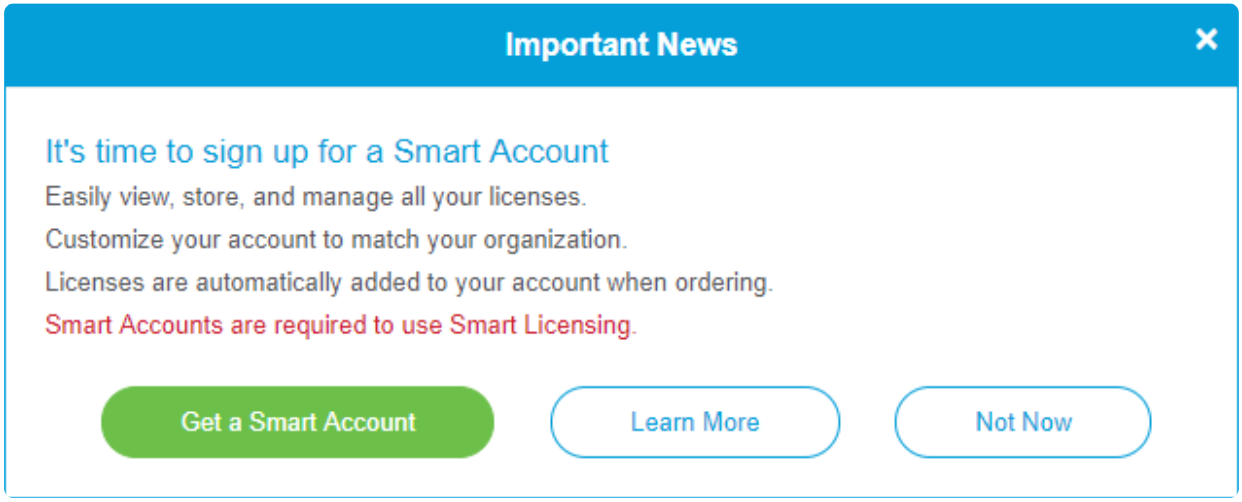
要购买RV安全许可证，您需要一个智能帐户。

授权激活此智能帐户即表示您同意授权您代表您的组织创建帐户、管理产品和服务授权、许可协议以及用户访问帐户。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的事件，从那时起，通过工具向前提供管理。

创建智能帐户

当您使用Cisco.com帐户或CCO ID（您在本文档开头创建的帐户）访问您的常规思科帐户时，可能会收到一条创建智能帐户的消息。



如果尚未看到此弹出窗口，您可以点击以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。

有关申请智能帐户所涉及步骤的更多详细信息，请点击此处。

请务必注意您的帐户名称以及其他注册详细信息。

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

> ⓘ Note: 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

您必须从您的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。

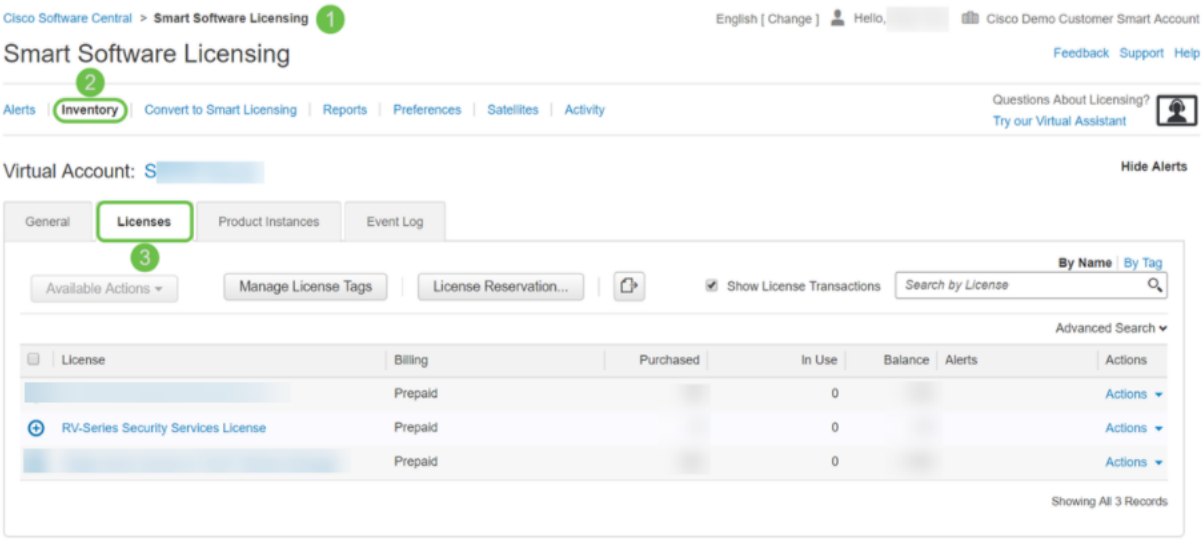
下表显示许可证的部件号。

类型	Product ID	描述
RV安全许可证	LS-RV34X-SEC-1YR=	RV安全：1年:动态Web过滤器、应用可视性、客户端识别和统计信息、网关防病毒和

许可证密钥不会直接输入您的路由器，但会在您订购许可证后分配给您的思科智能帐户。许可证显示在您的帐户上所需的时间取决于合作伙伴接受订单的时间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

导航到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。

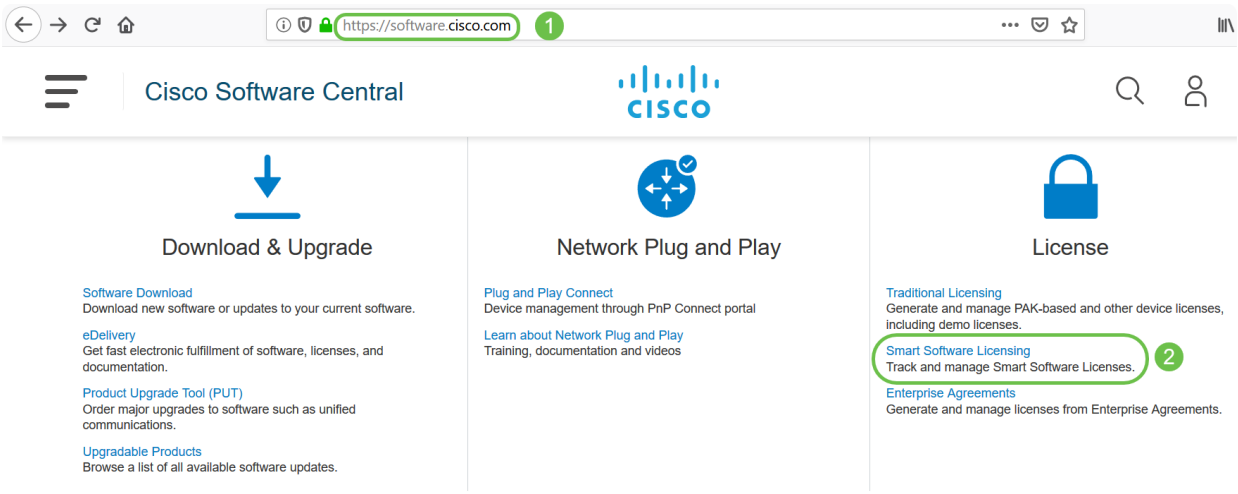


ⓘ Note: 如果您在智能帐户中看不到许可证，请联系您的思科合作伙伴。

在RV345P系列路由器上配置RV安全许可证

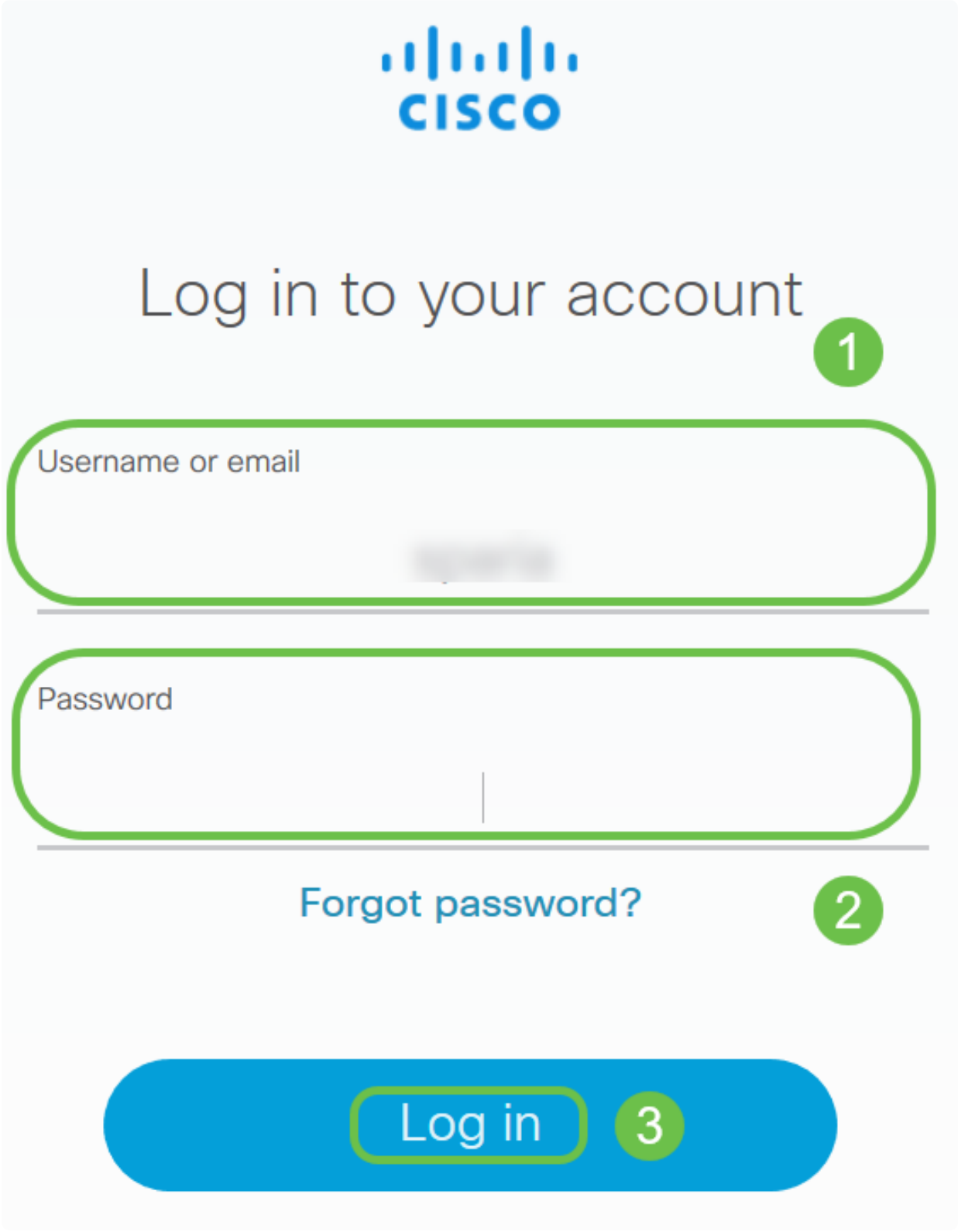
第 1 步

访问思科软件并导航到智能软件许可。



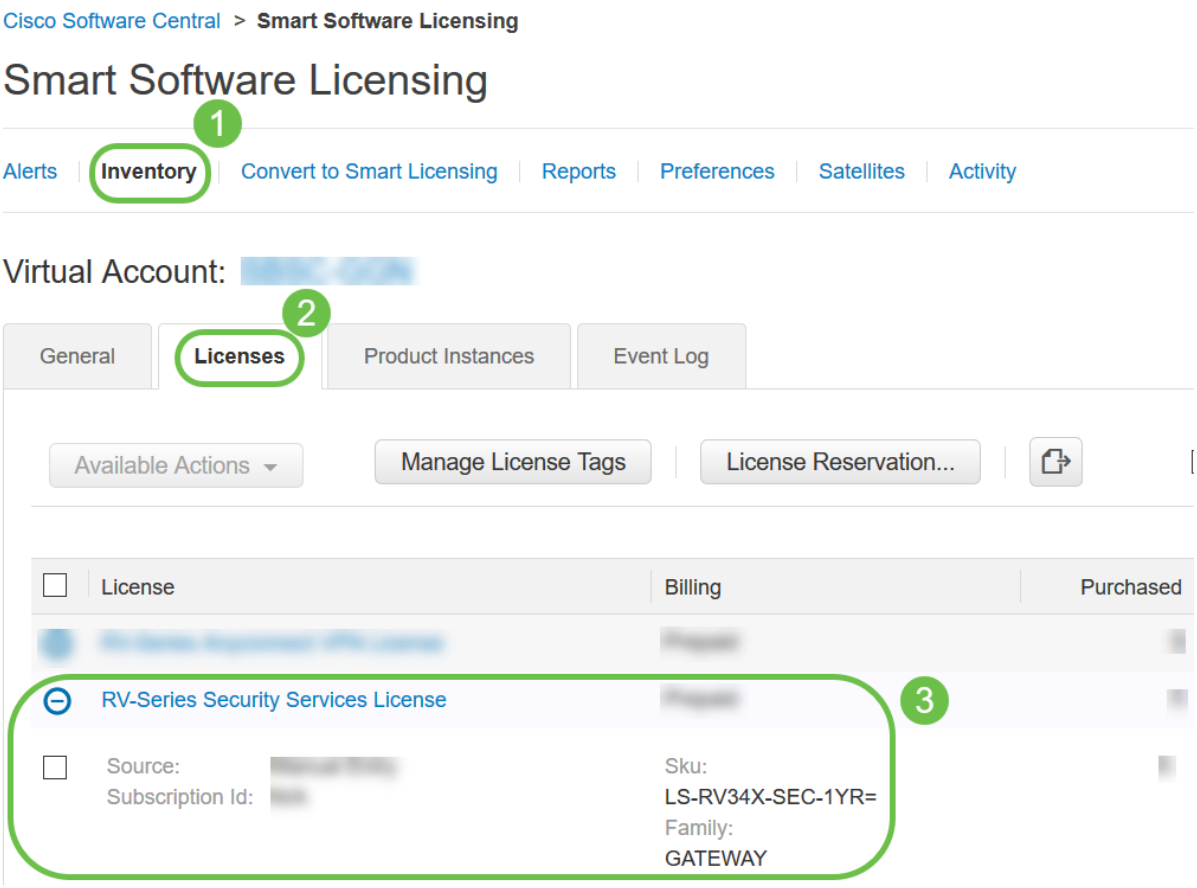
第 2 步

输入您的用户名或电邮和密码以登录您的智能帐户。单击Log in。



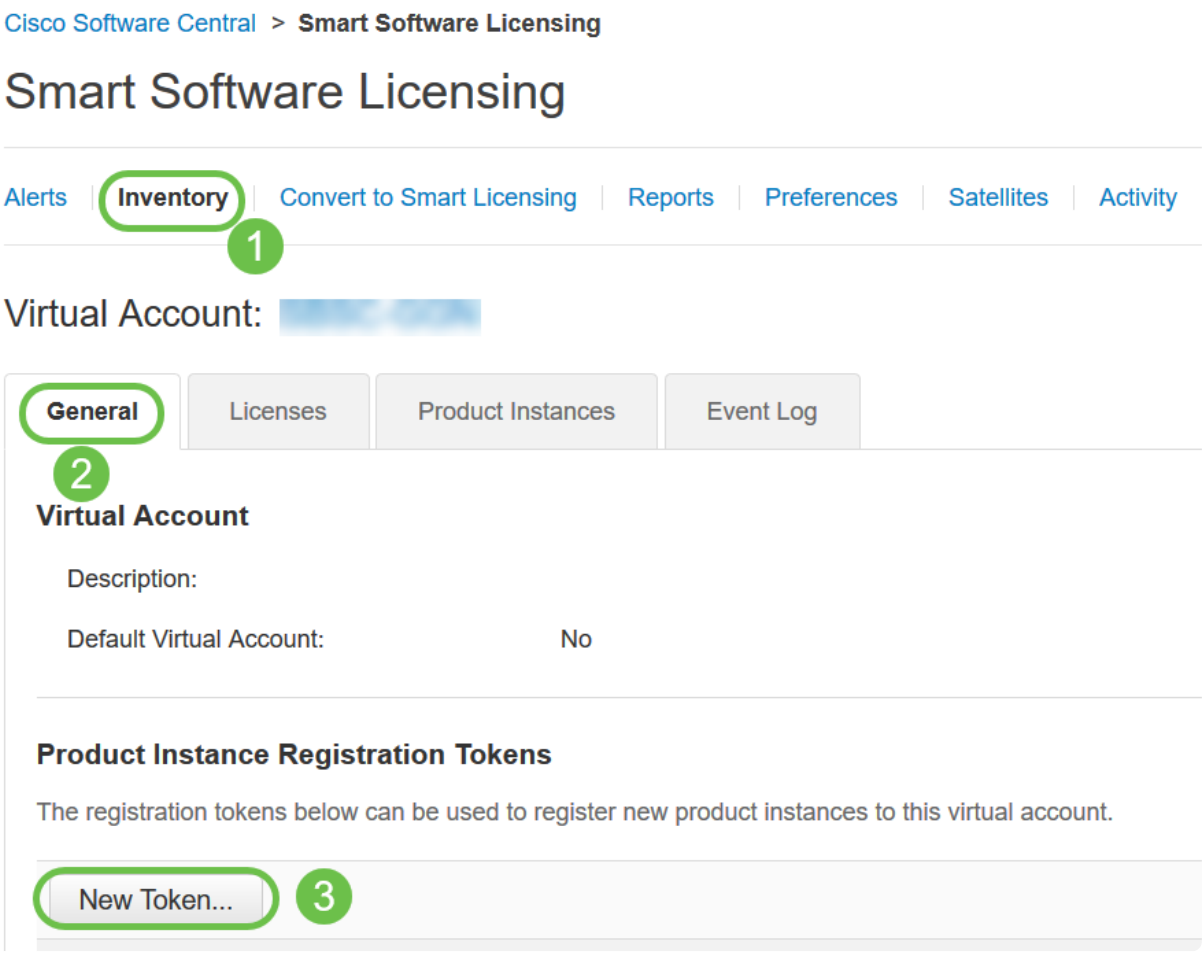
第 3 步

导航到资产>许可证，并验证您的智能帐户中是否列出了RV系列安全服务许可证。如果您未看到列出的许可证，请与您的思科合作伙伴联系。



第 4 步

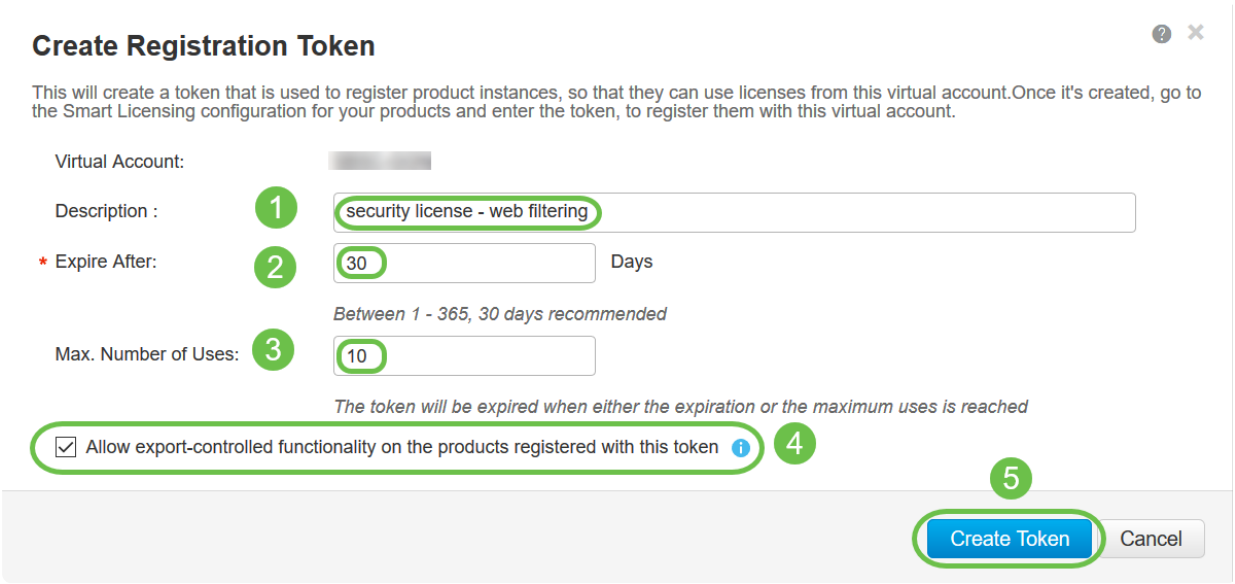
导航到资产>常规。在Product Instance Registration Tokens下，单击New Token。



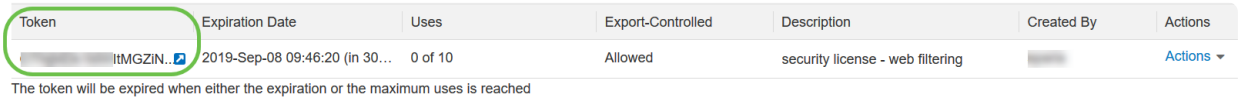
步骤 5

将显示“创建注册令牌”(Create Registration Token)窗口。Virtual Account区域显示将在其下创建注册令牌的虚拟帐户。在创建注册令牌页面上，完成以下操作：

- 在说明(Description)字段中，输入令牌的唯一说明。在本示例中，输入了安全许可证— Web过滤。
- 在Expire After字段中，输入介于1到365天之间的值。Cisco建议将此字段的值为30天；但是，您可以根据需要编辑该值。
- 在Max。使用次数字段输入一个值，以定义要使用该令牌的次数。令牌将在达到天数或最大使用次数时过期。
- 选中Allow export-controlled functionality on the products registered with this token复选框，以启用虚拟帐户中产品实例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。仅在符合导出控制功能时才使用此选项。一些出口控制功能受到美国商务部的限制。取消选中复选框时，对于使用此令牌注册的产品，这些功能受到限制。任何违反行为都将会受到处罚和行政收费。
- 单击Create Token生成令牌。

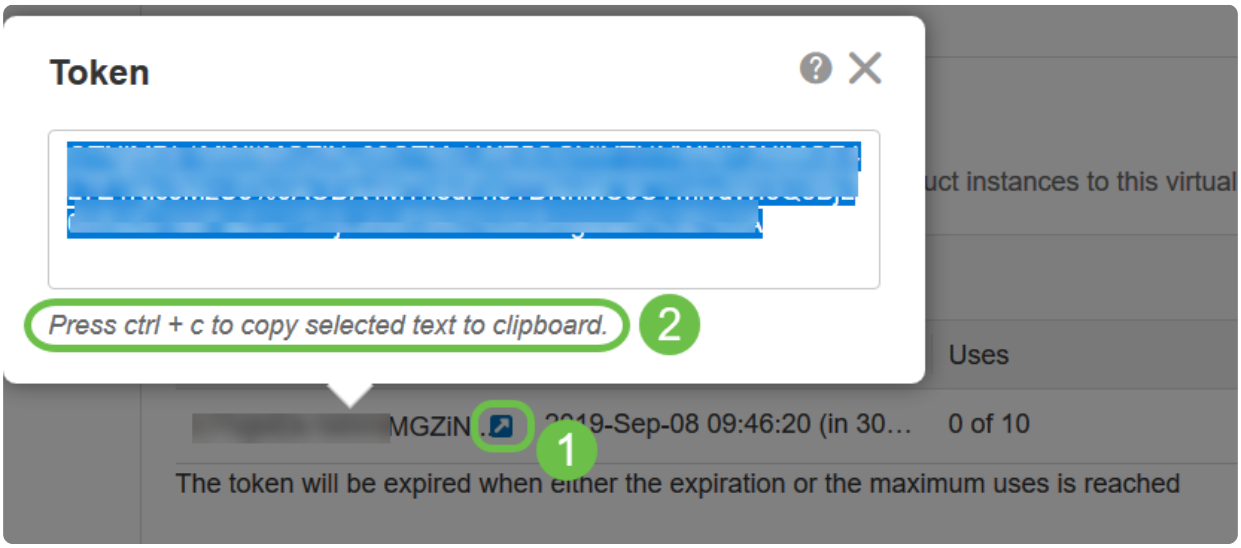


现在，您已成功生成产品实例注册令牌。



第 6 步

单击令牌列中的箭头图标，将令牌复制到剪贴板，请按键盘上的ctrl + c。



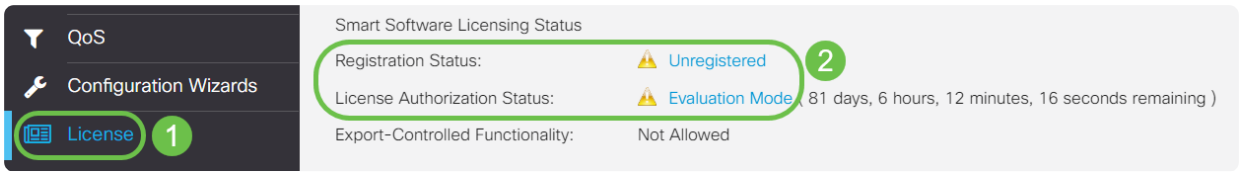
步骤 7（可选）

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



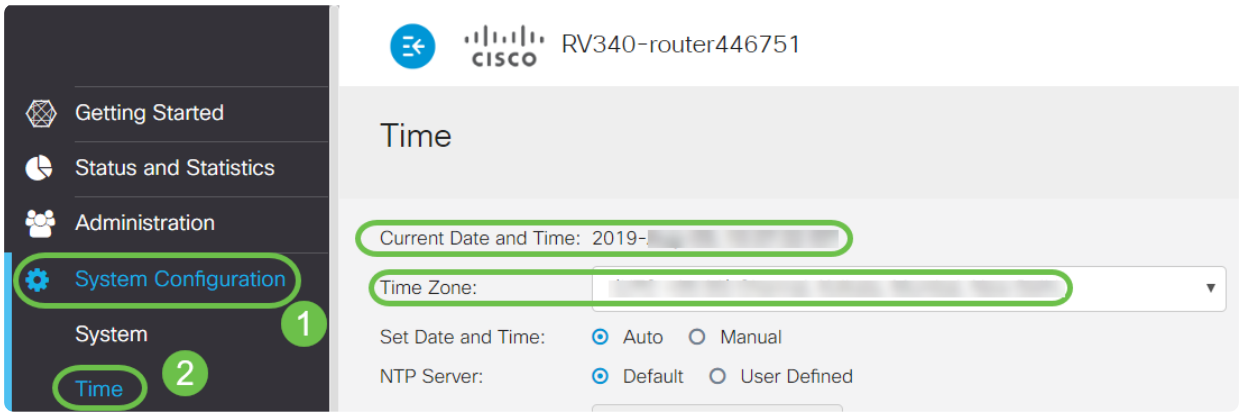
步骤 8

导航到License并验证Registration Status显示为Unregistered,License Authorization Status显示为Evaluation Mode。



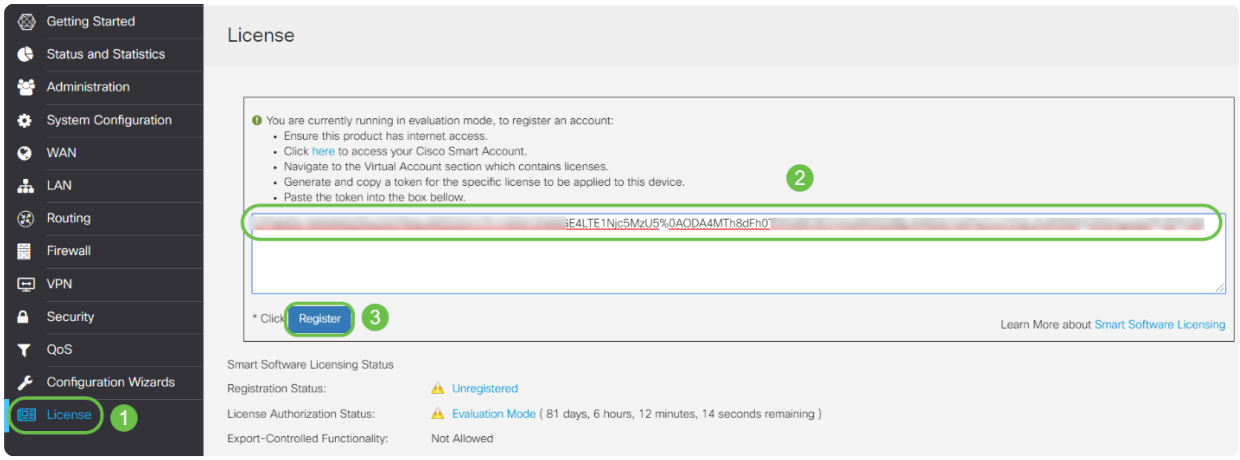
步骤 9

导航到System Configuration > Time，并验证Current Date and Time和Time和Time Zone是否按照您的时区正确反映。



步骤 10

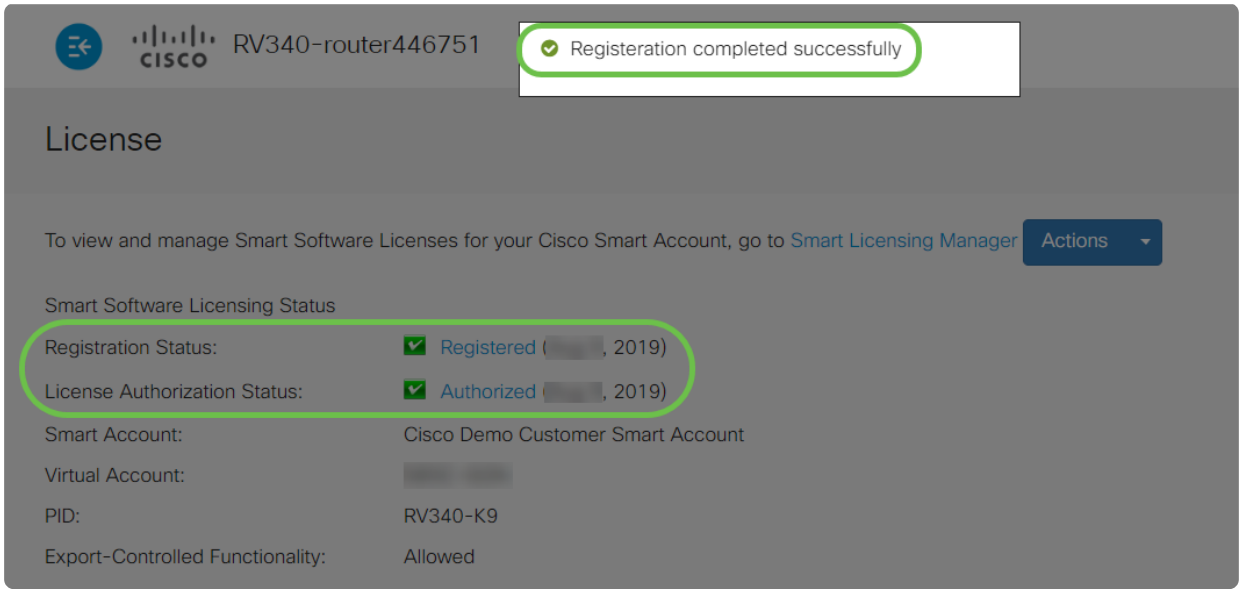
导航到License。通过在键盘上选择ctrl + v，将步骤6中复制的令牌粘贴到License选项卡下的文本框中。单击Register。



注册可能需要几分钟。当路由器尝试联系许可证服务器时，请勿离开该页面。

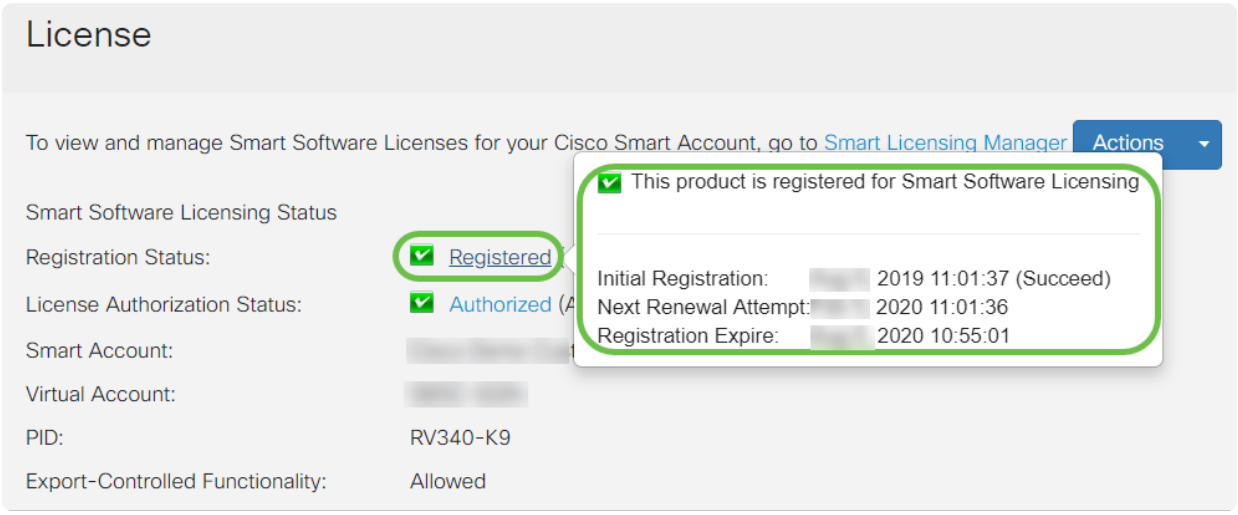
步骤 11

现在，您应该已经成功注册并授权使用智能许可证的RV345P系列路由器。您将在成功完成注册屏幕上收到通知。此外，您还可以看到Registration Status显示为Registered,License Authorization Status显示为Authorized。



步骤 12（可选）

要查看许可证Registration Status的更多详细信息，请将指针悬停在Registered状态上。系统将显示包含下列信息的对话框消息：

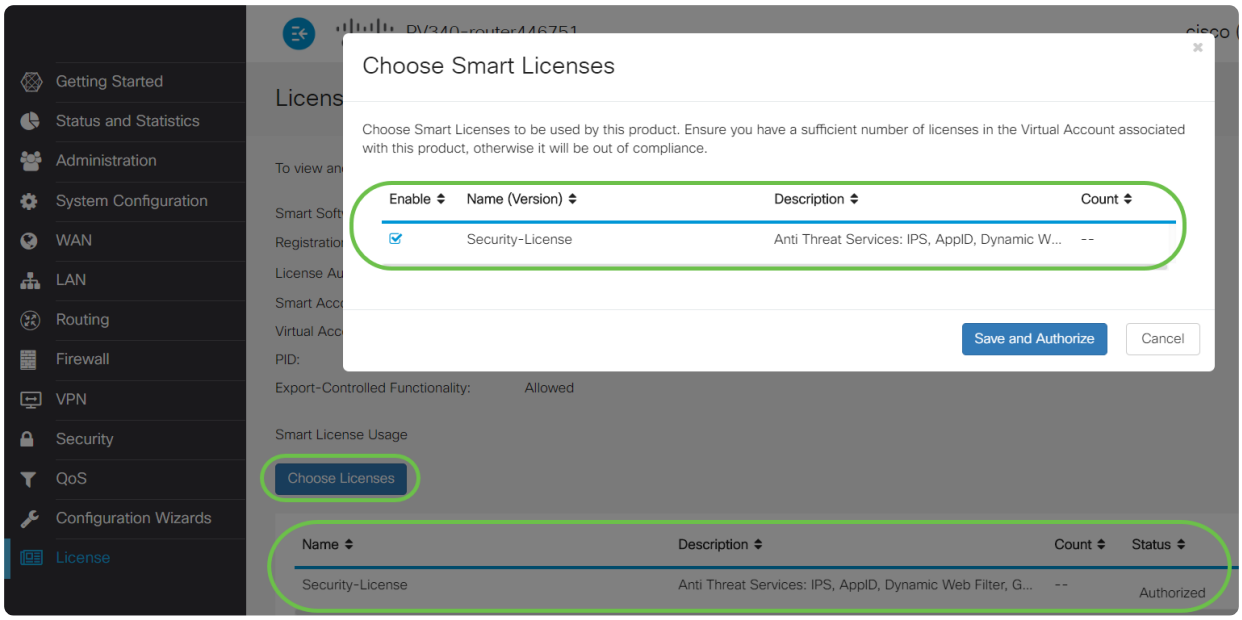


- 初始注册 — 此区域表示注册许可证的日期和时间。
- 下一次续订尝试 — 此区域指示路由器尝试续订许可证的日期和时间。
- 注册到期 — 此区域指示注册到期的日期和时间。

步骤 13

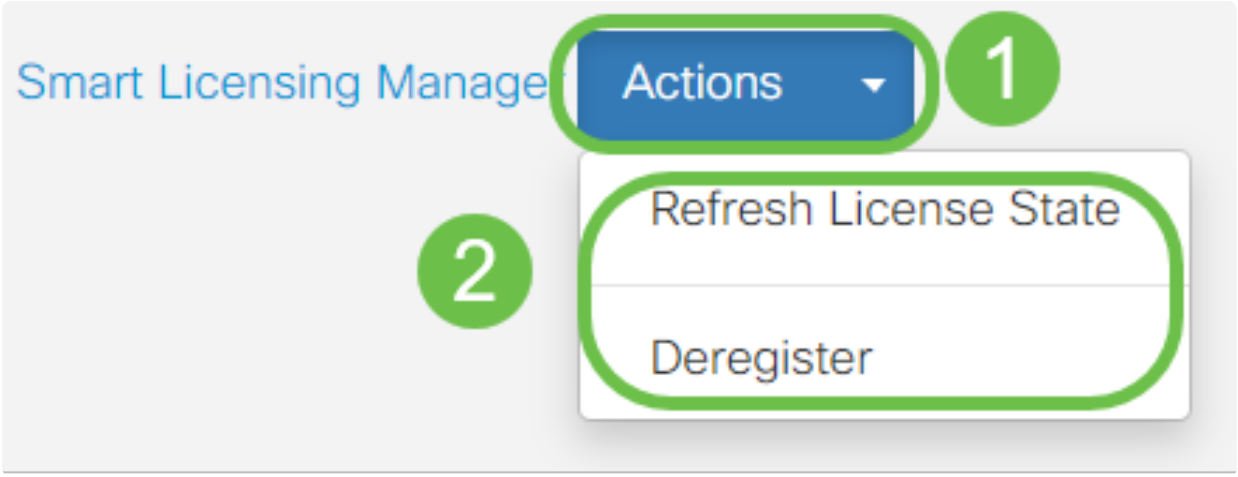
在License页面上，验证Security-License状态是否显示Authorized。您还可以点击Choose License按钮以验证Security-License是否已启用。

ⓘ Note: 如果您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取消注册许可证，请点击智能许可管理器操作下拉菜单并选择操作项。



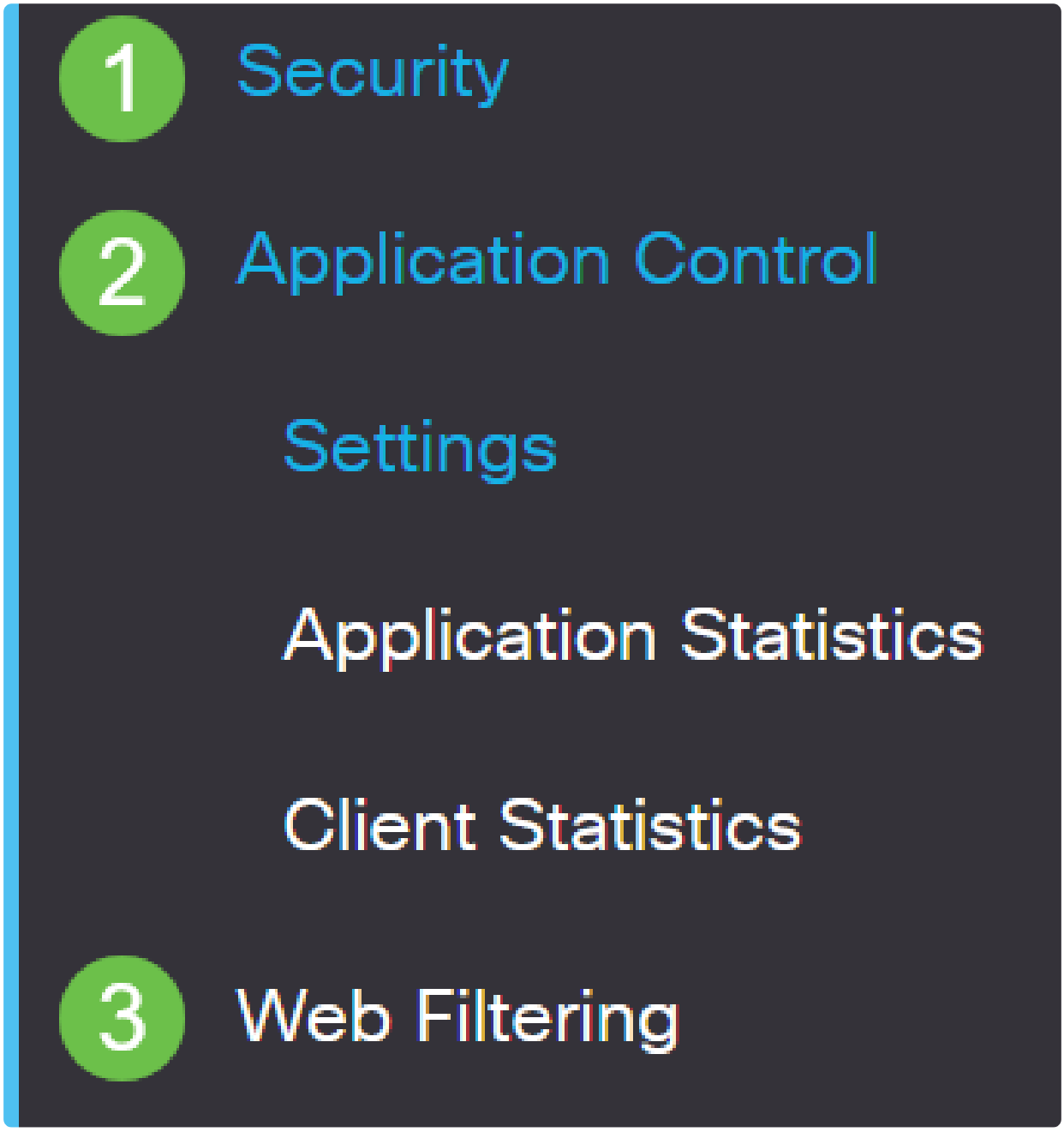
现在路由器上已经有了您的许可证，您需要完成下一部分中的步骤。

RV345P路由器上的Web过滤

激活后90天，您就可以免费使用Web过滤。免费试用后，如果要继续使用此功能，您需要购买许可证。单击可返回该部分。

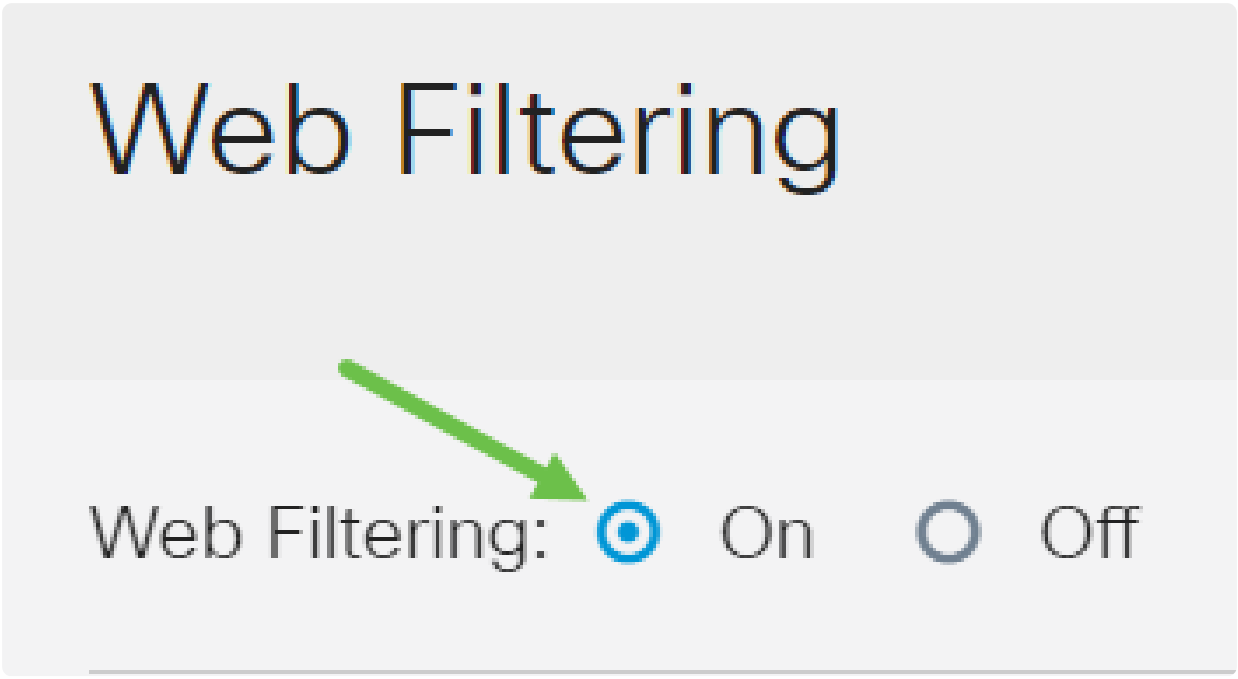
第 1 步

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



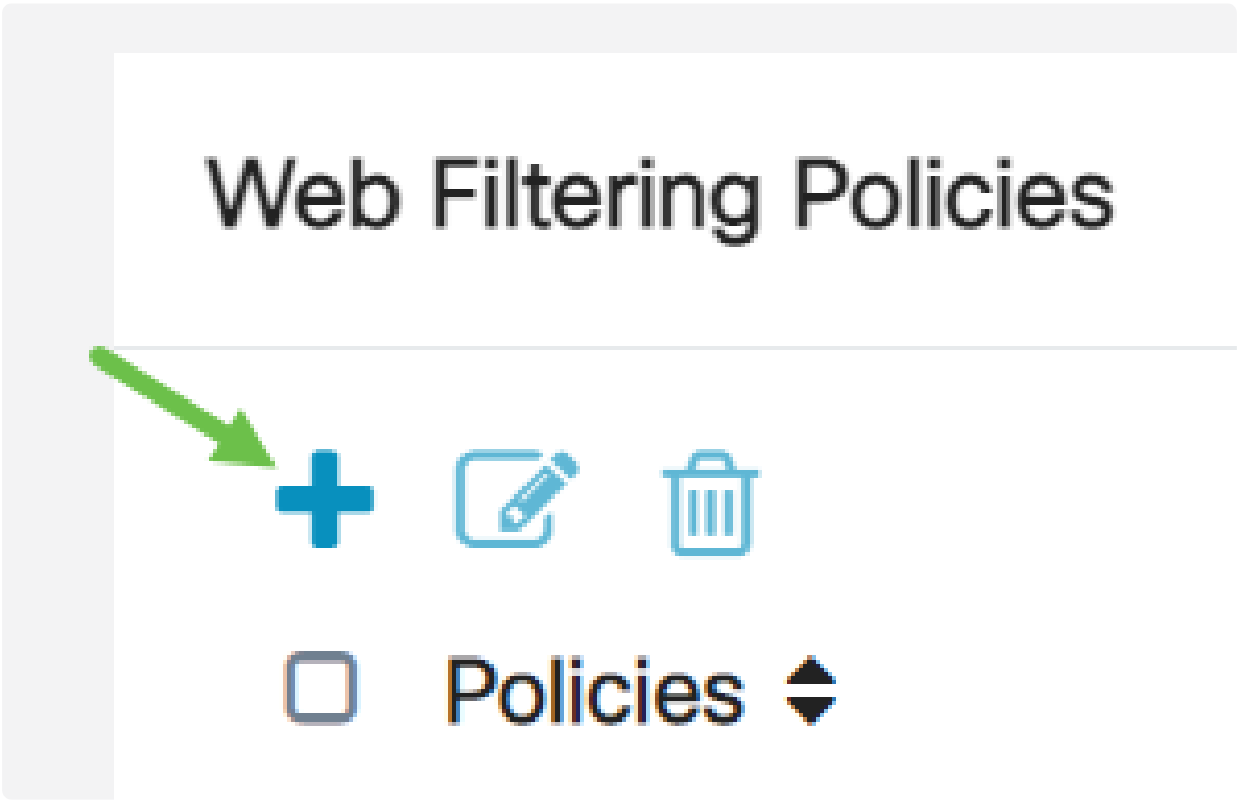
第 2 步

选择开单选按钮。


Web Filtering
Web Filtering: On Off

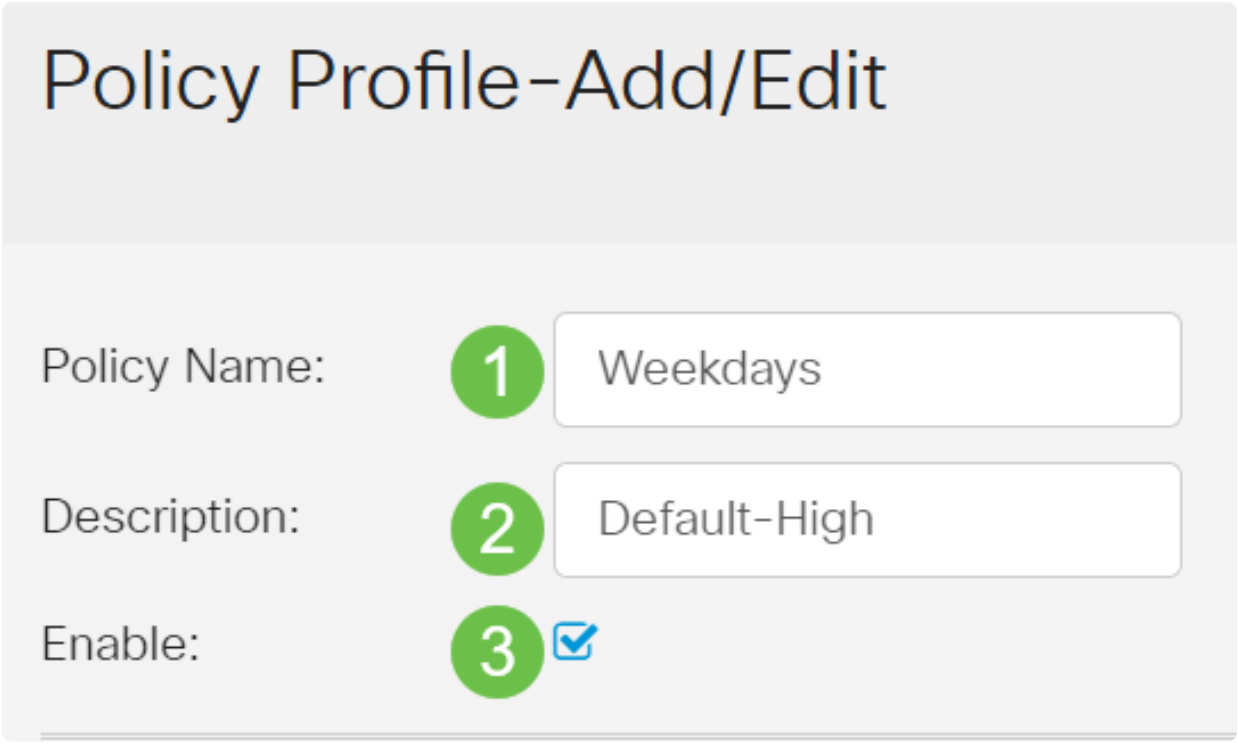
第 3 步

单击add图标。


Web Filtering Policies
Policies

第 4 步

输入Policy Name、Description和Enable 复选框。



ⓘ Note: 如果您的路由器上启用了内容过滤，则将显示一条通知，通知您内容过滤已被禁用，且不能同时启用这两个功能。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。

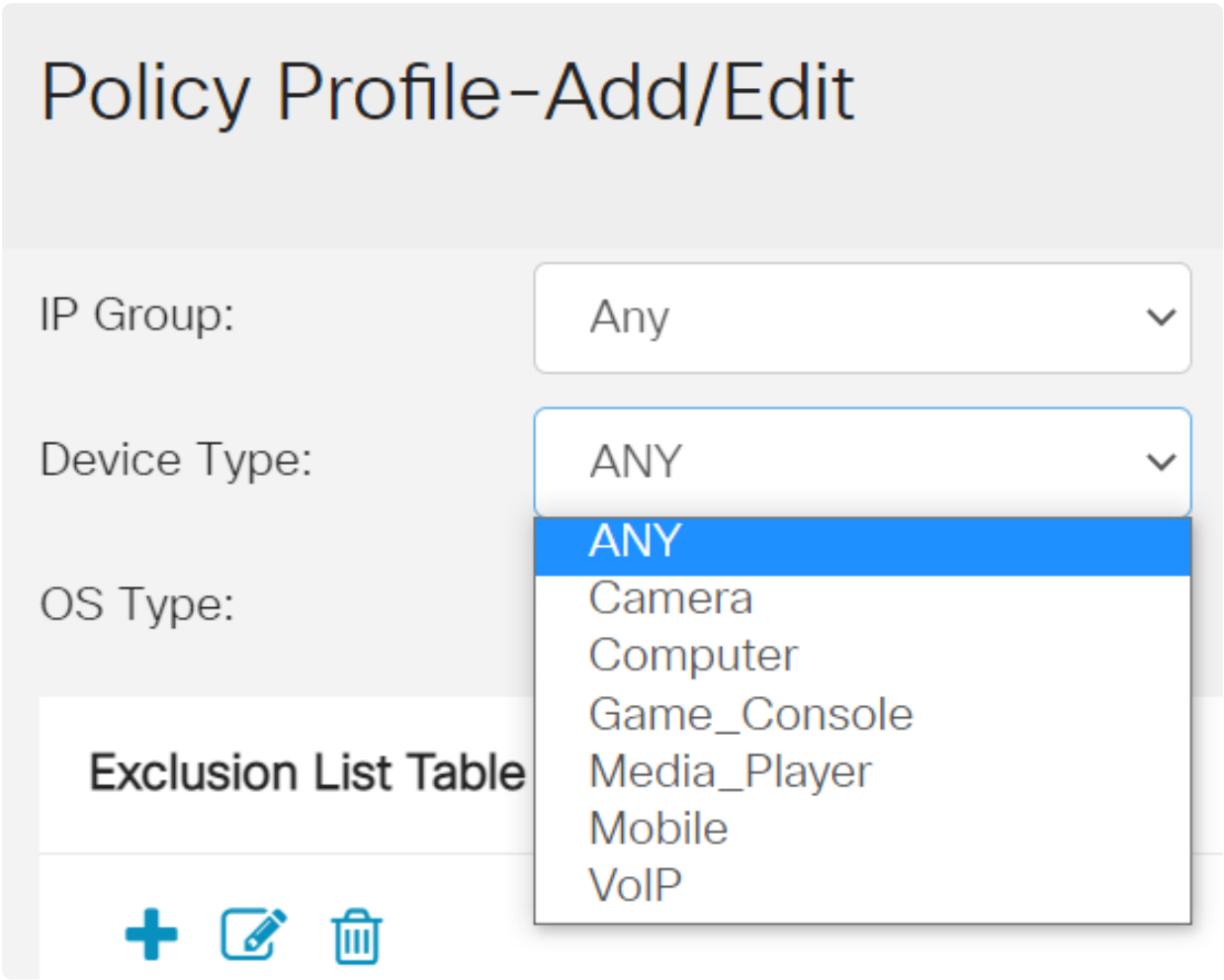


ⓘ Note: 内容将根据网站或URL的恶名基于Web信誉索引进行过滤。如果分数低于40，网站将被阻止。要了解有关Web信誉技术的更多信息，请单击 此处 了解详细信息。

第 6 步

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：

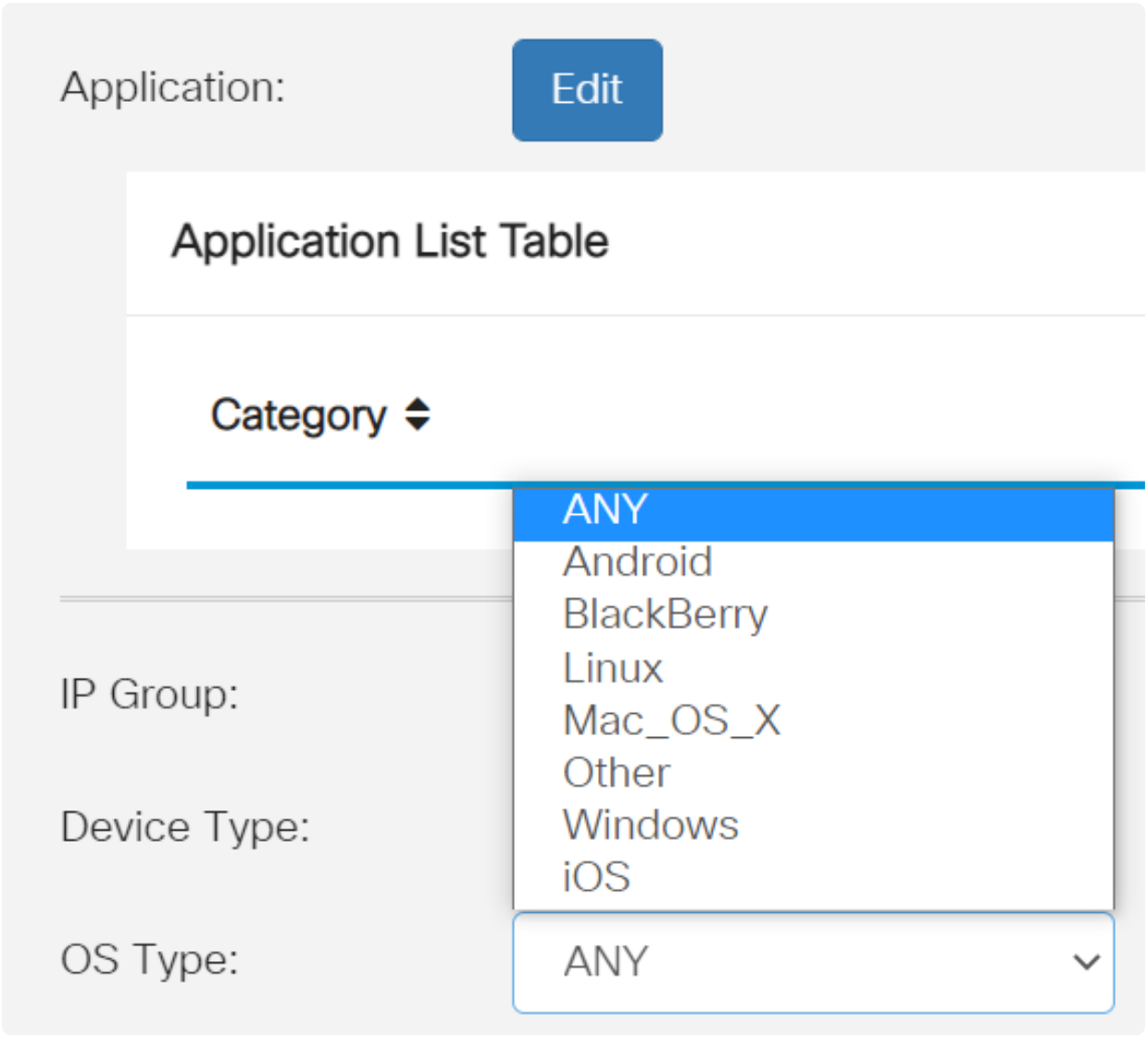
- ANY — 选择此项可将策略应用于任何设备。
- 摄像头 — 选择此项，将策略应用于摄像头（例如IP安全摄像头）。
- 计算机 — 选择此项可将策略应用于计算机。
- Game_Console — 选择此项可将策略应用于游戏控制台。
- Media_Player — 选择此项可将策略应用到Media Player。
- 移动 — 选择此项可将策略应用于移动设备。
- VoIP — 选择此项将策略应用于Internet协议语音设备。



第 7 步

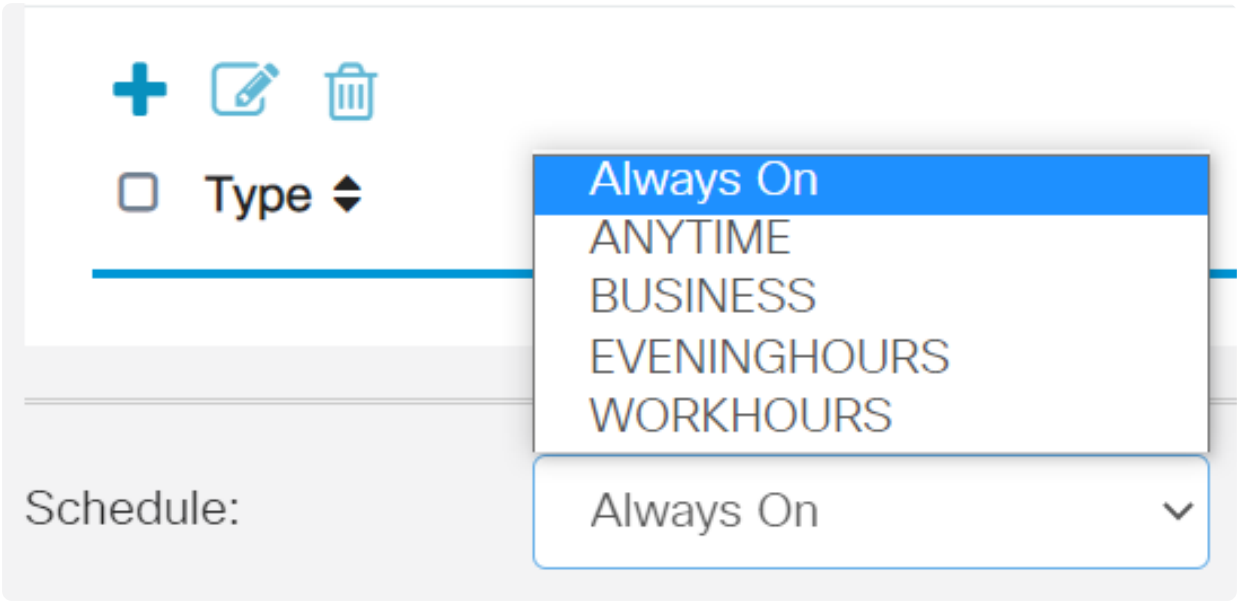
从OS Type下拉列表中，选择策略应适用的操作系统(Operating System， OS)。一次只能选择一个选项。选项有：

- 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操作系统。
- 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 — 将策略应用到Windows操作系统。
- iOS — 仅将策略应用于iOS OS。



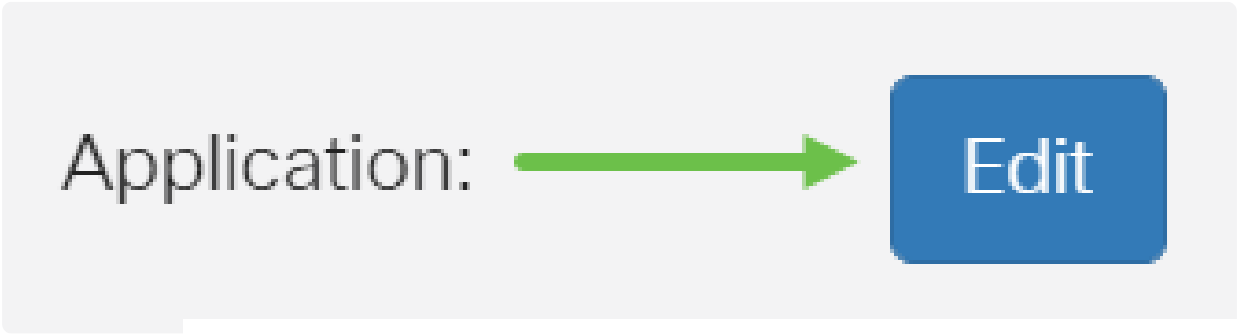
步骤 8

向下滚动到Schedule部分，然后选择最符合您需求的选项。



步骤 9

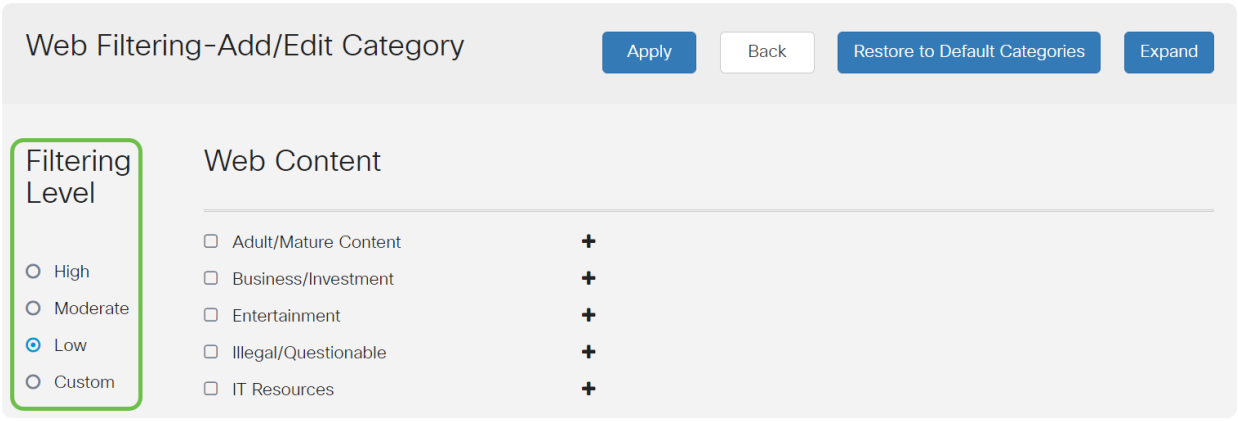
点击编辑图标。



步骤 10

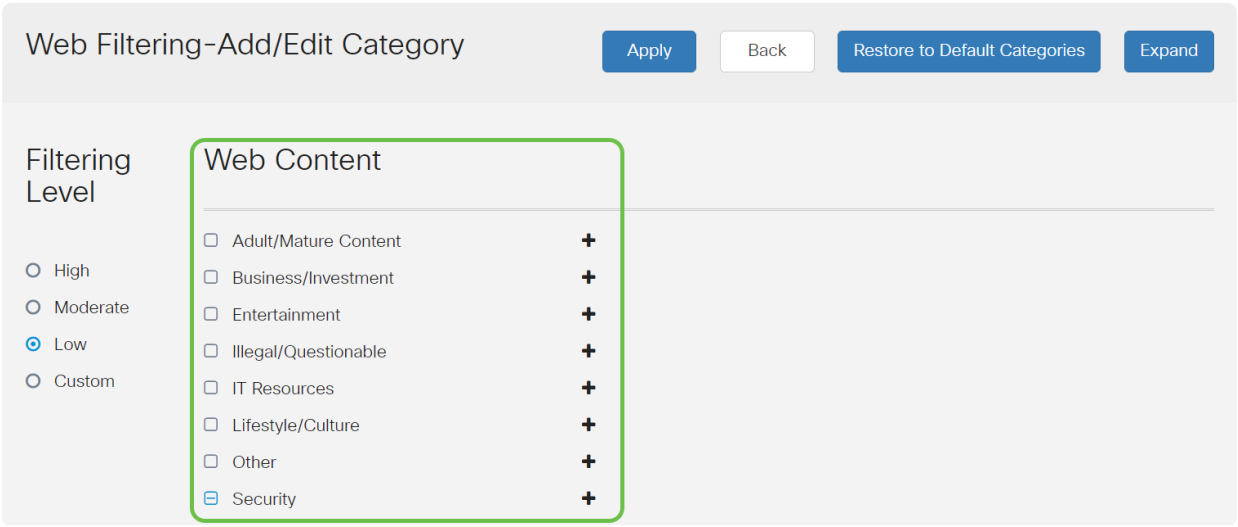
在Filtering Level列中，点击单选按钮快速定义最适合网络策略的过滤范围。选项包括“高”、“中等”、“低”和“自定义”。单击以下任何过滤级别，了解过滤到每个已启用网络内容类别的特定预定义子类别。预定义的过滤器无法再更改，因此呈灰色显示。

- 低 — 这是默认选项。此选项启用安全性。
- Moderate — 使用此选项可启用“成人/成人内容”、“非法/可疑”和“安全”。
- 高 — 通过此选项启用成人/成熟内容、业务/投资、非法/可疑、IT资源和安全。
- 自定义 — 未设置默认设置以允许用户定义的过滤器。



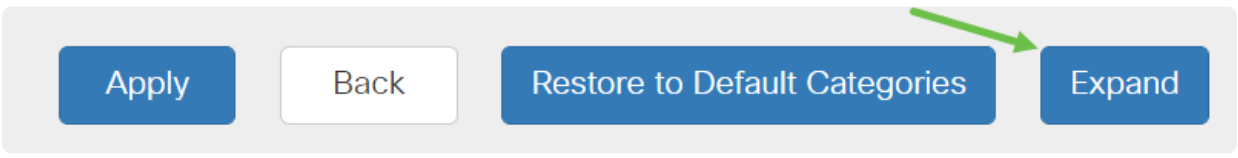
步骤 11

输入要过滤的网络内容。如果您想了解某一部分的更多详细信息，请点击加号图标。



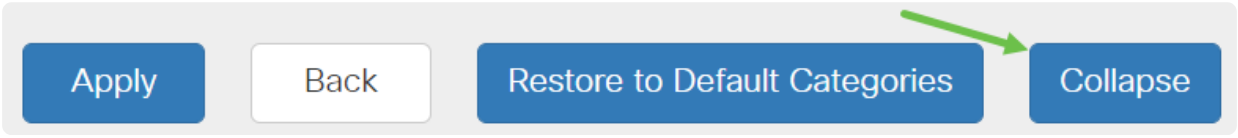
步骤 12（可选）

要查看所有Web内容子类别和说明，可以单击Expand按钮。



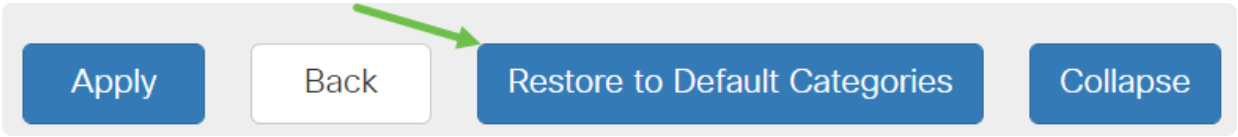
步骤 13（可选）

单击Collapse折叠子类别和说明。



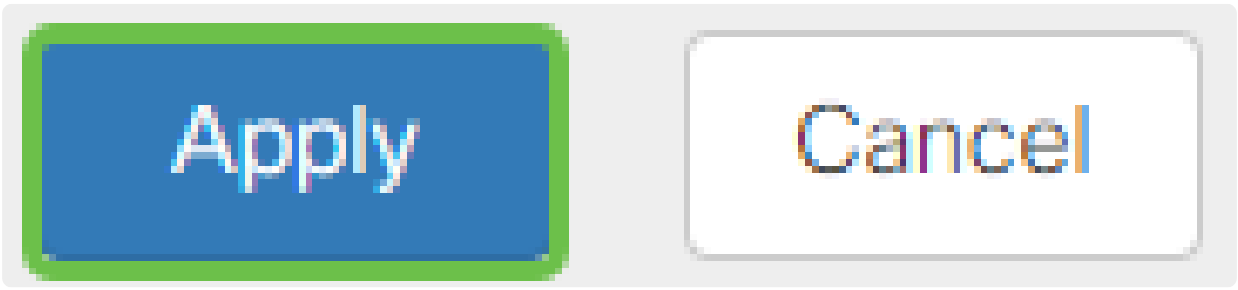
步骤 14（可选）

要恢复默认类别，请点击恢复默认类别。



步骤 15

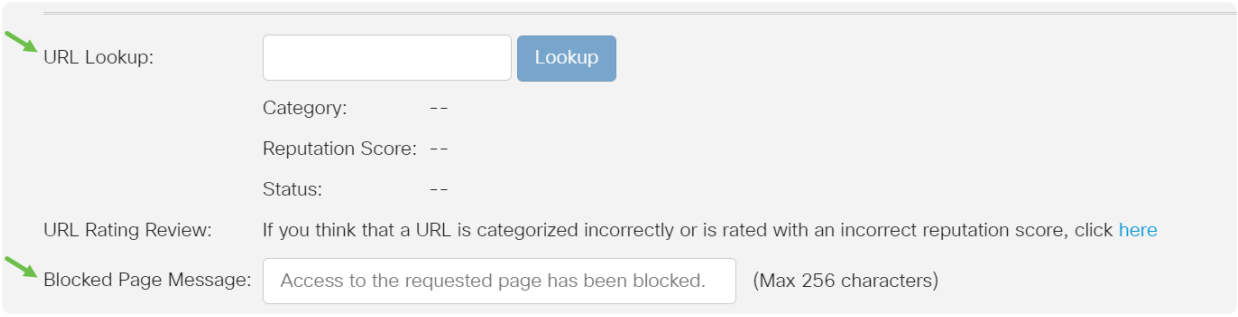
单击Apply以保存配置，并返回到Filter页面以继续设置。



ⓘ Note: 在“应用列表表”中，将根据所选过滤级别填写的相应子类别将填充该表。

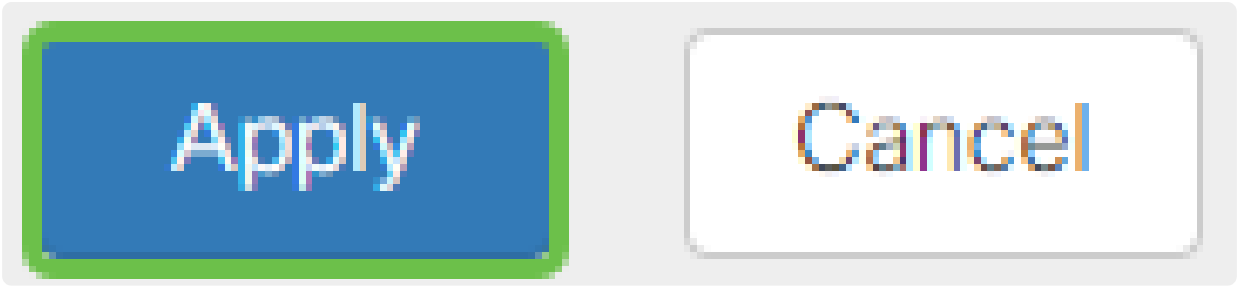
步骤 16（可选）

其他选项包括URL Lookup和显示请求的页面被阻止时间的消息。



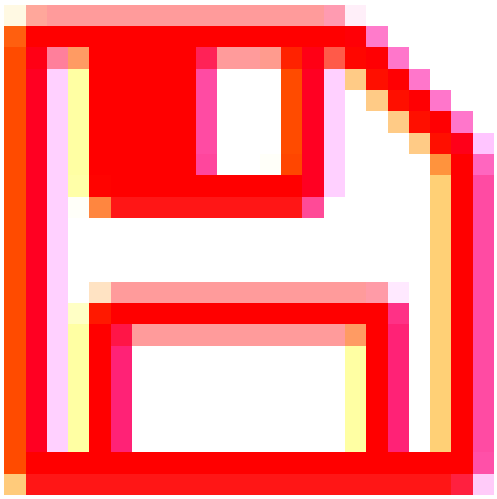
步骤 17（可选）

单击 Apply。



步骤 18

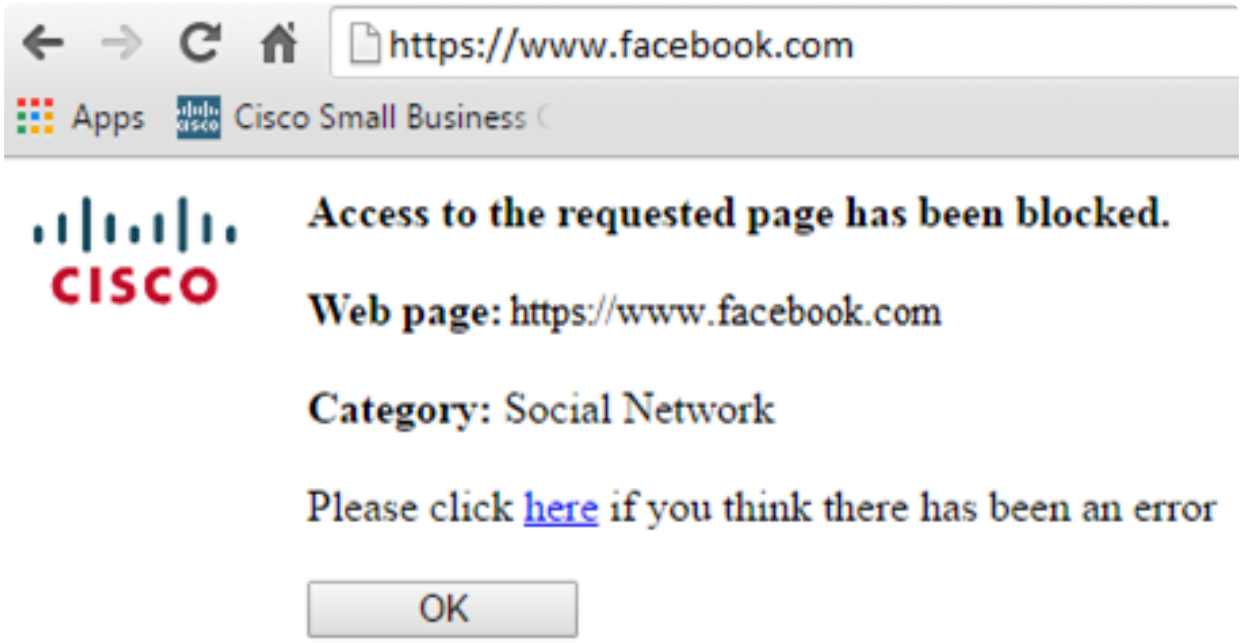
要永久保存配置，请转到复制/保存配置页或单击该页上方的保存图标。



步骤 19（可选）

要验证网站或URL是否已被过滤或阻止，请启动Web浏览器或在浏览器中打开一个新选项卡。输入已列出阻止或过滤为被阻止或拒绝的域名。

在本例中，我们使用了www.facebook.com。



现在，您应该已经在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，因此您可能不需要Umbrella。如果您还需要Umbrella，请点击此处。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，但它不会显示在虚拟帐户中，则有两个选项：

1. 跟进经销商，请求他们进行转接。
2. 联系我们，我们将与经销商取得联系。

理想情况下，您也不必这样做，但是如果您到达这个十字路口，我们乐意为您提供帮助！为了尽可能简化流程，您需要上表中以及下面概述的凭证。

所需信息	查找信息
许可证发票	完成许可证购买后，应通过电子邮件发送给您。
思科销售订单编号	您可能需要返回经销商处才能获得此服务。
智能帐户许可证页面的截图	截取屏幕截图可捕获您屏幕的内容，以便与我们的团队共享。如果您不熟

屏幕截图

一旦您拥有了令牌，或者要进行故障排除，建议您截取屏幕截图来捕获屏幕内容。

鉴于捕获屏幕截图所需的步骤不同，请参阅以下内容了解特定于您的操作系统的链接。

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

Umbrella RV分支许可证（可选）

Umbrella是思科提供的一个简单但非常有效的云安全平台。

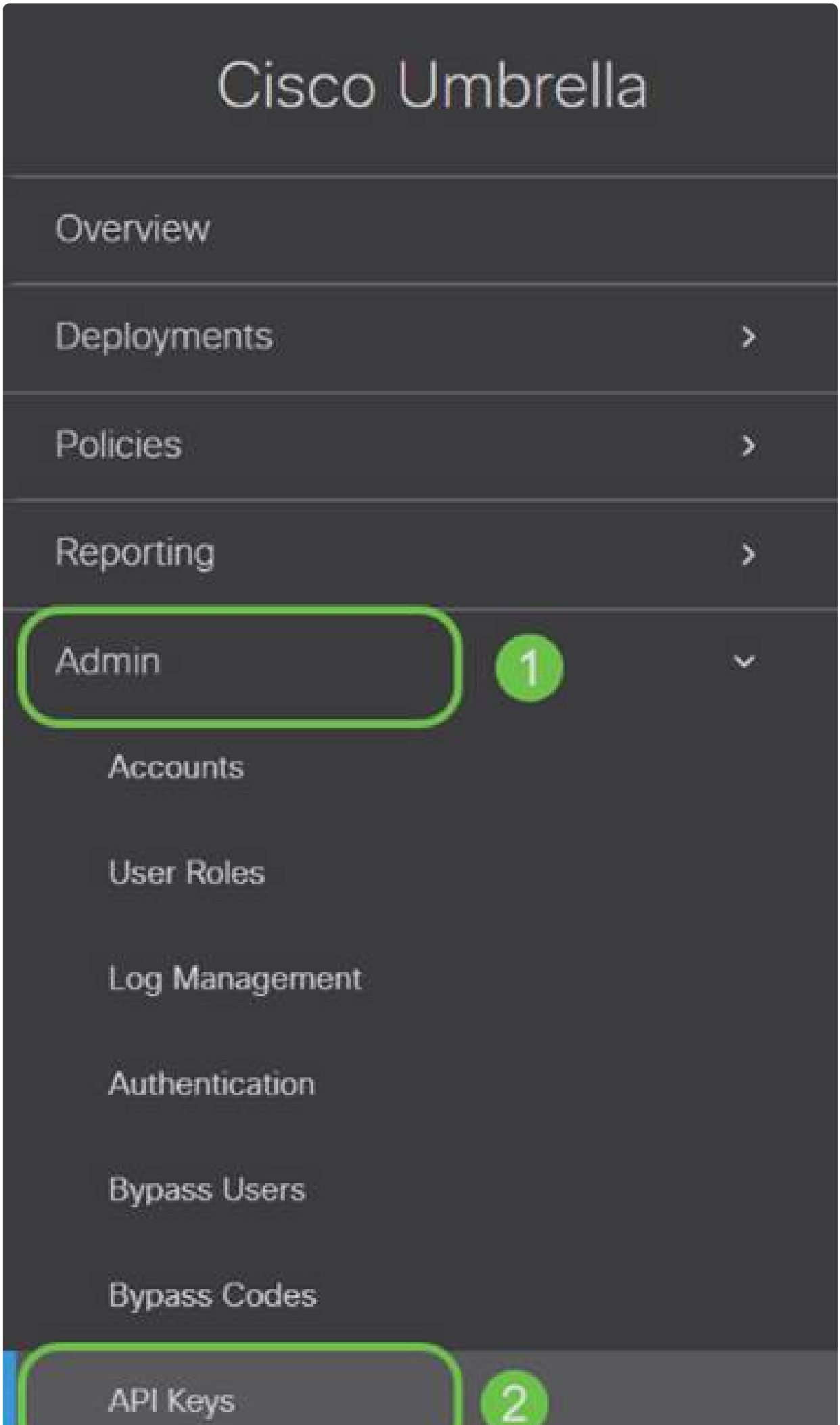
Umbrella在云中运行并执行许多与安全相关的服务。从突发性威胁到事后调查Umbrella可发现并阻止跨所有端口和协议的攻击。

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会传递到Umbrella的DNS解析器，如果安全警告与域关联，则请求会被阻止。此遥测数据传输和分析在微秒内完成，几乎不会增加延迟。遥测数据使用日志和仪器，跟踪全世界数十亿个DNS请求。当这些数据无处不在时，在全球范围内将其关联起来，可以在攻击开始时迅速做出响应。有关详细信息，请参阅思科的隐私政策：完整策略、摘要版本。将遥测数据视为源自工具和日志的数据。

请访问Cisco Umbrella了解详情并创建帐户。如果您遇到任何问题，请在此处查阅文档，并在此处查看Umbrella支持选项。

第 1 步

登录您的Umbrella帐户后，从Dashboard屏幕点击Admin > API Keys。

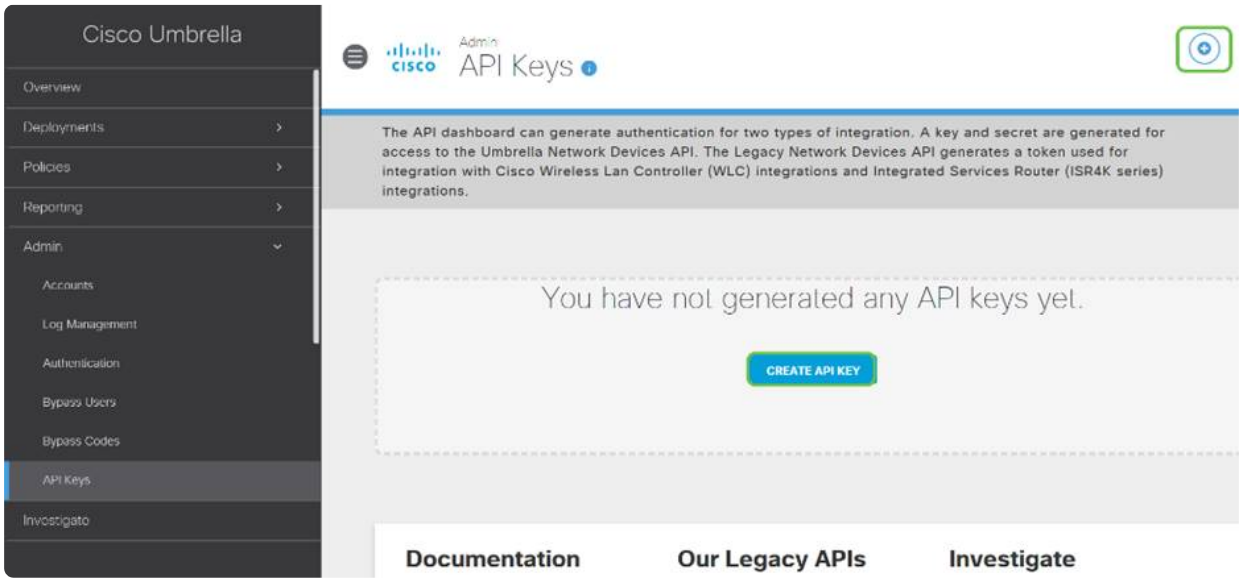

Cisco Umbrella
Overview
Deployments
Policies
Reporting
Admin
1
Accounts
User Roles
Log Management
Authentication
Bypass Users
Bypass Codes
API Keys
2

API密钥屏幕的剖析（使用预先存在的API密钥）

1. 添加API密钥 — 启动创建新密钥以与Umbrella API配合使用。
2. 附加信息 — 向下/向上滑动，并提供此屏幕的解释程序。
3. 令牌井 — 包含此帐户创建的所有密钥和令牌。（在创建密钥后填充）
4. 支持文档 — 链接至与每个部分中的主题相关的Umbrella站点文档。

第 2 步

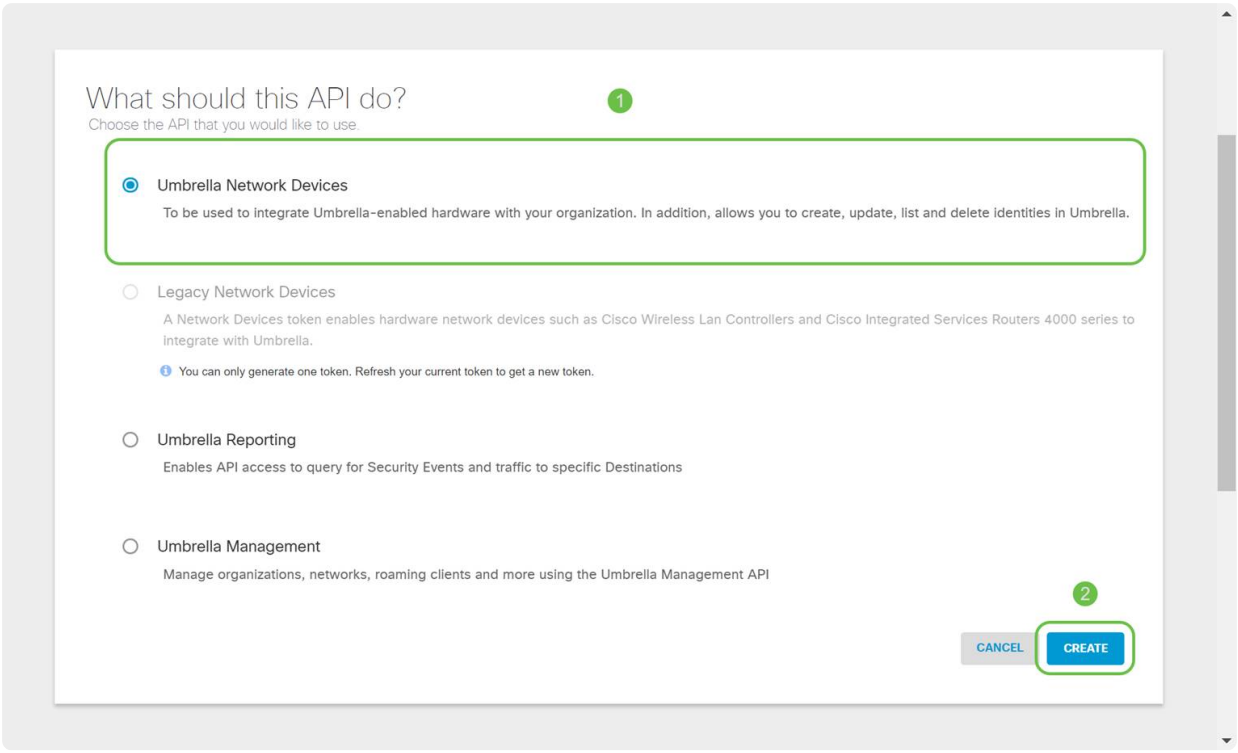
单击右上角的Add API Key按钮，或单击Create API Key按钮。两者功能相同。



ⓘ Note: 上面的屏幕截图与您第一次打开此菜单时看到的内容类似。

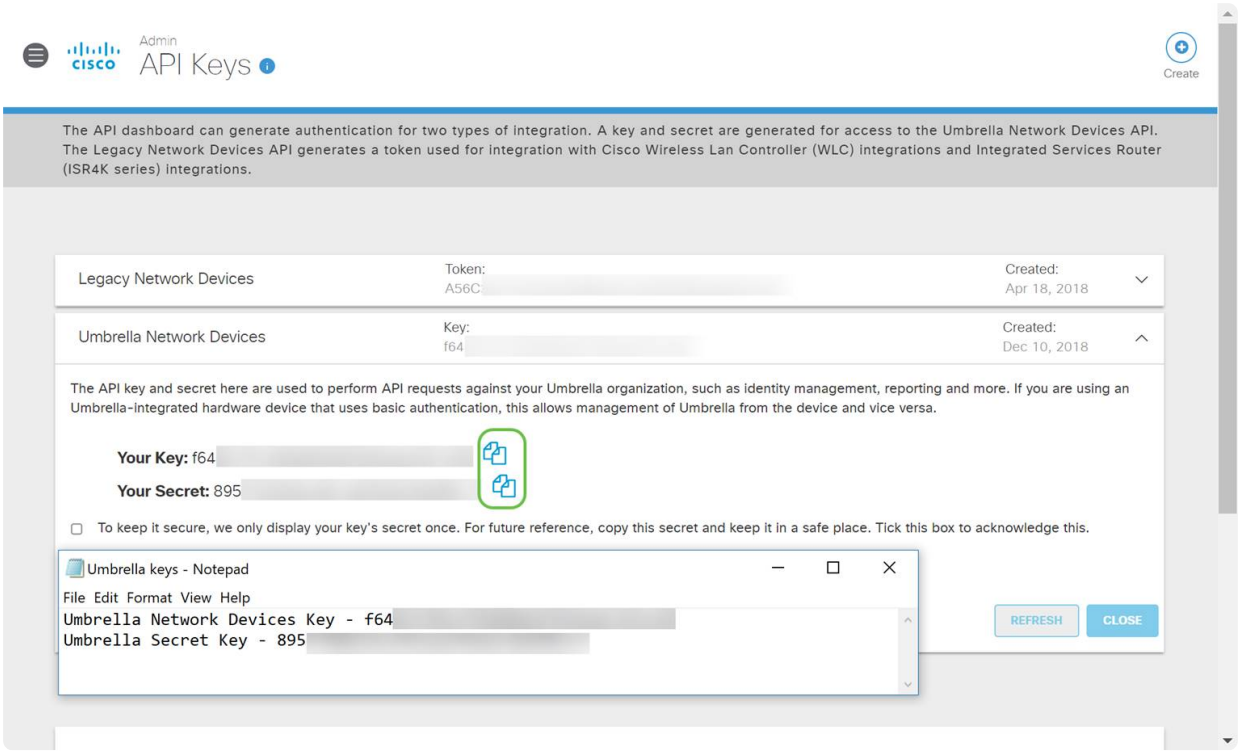
第 3 步

选择Umbrella Network Devices，然后单击Create按钮。



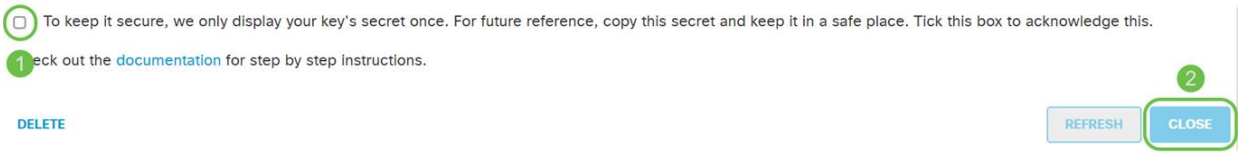
第 4 步

打开文本编辑器（如记事本），然后点击API和API Secret Key右侧的copy icon，弹出通知将确认密钥已复制到剪贴板。一次一个将您的密钥和API密钥粘贴到文档中，并标记它们以供将来参考。在本例中，其标签为“Umbrella network devices key”。然后，将文本文件保存到安全位置，以便以后轻松访问。



步骤 5

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临时查看密钥的确认，然后单击Close按钮。



ⓘ Note: 如果丢失或意外删除了密钥，则没有函数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，并对您希望使用Umbrella保护的每台设备重新授权新的API密钥。

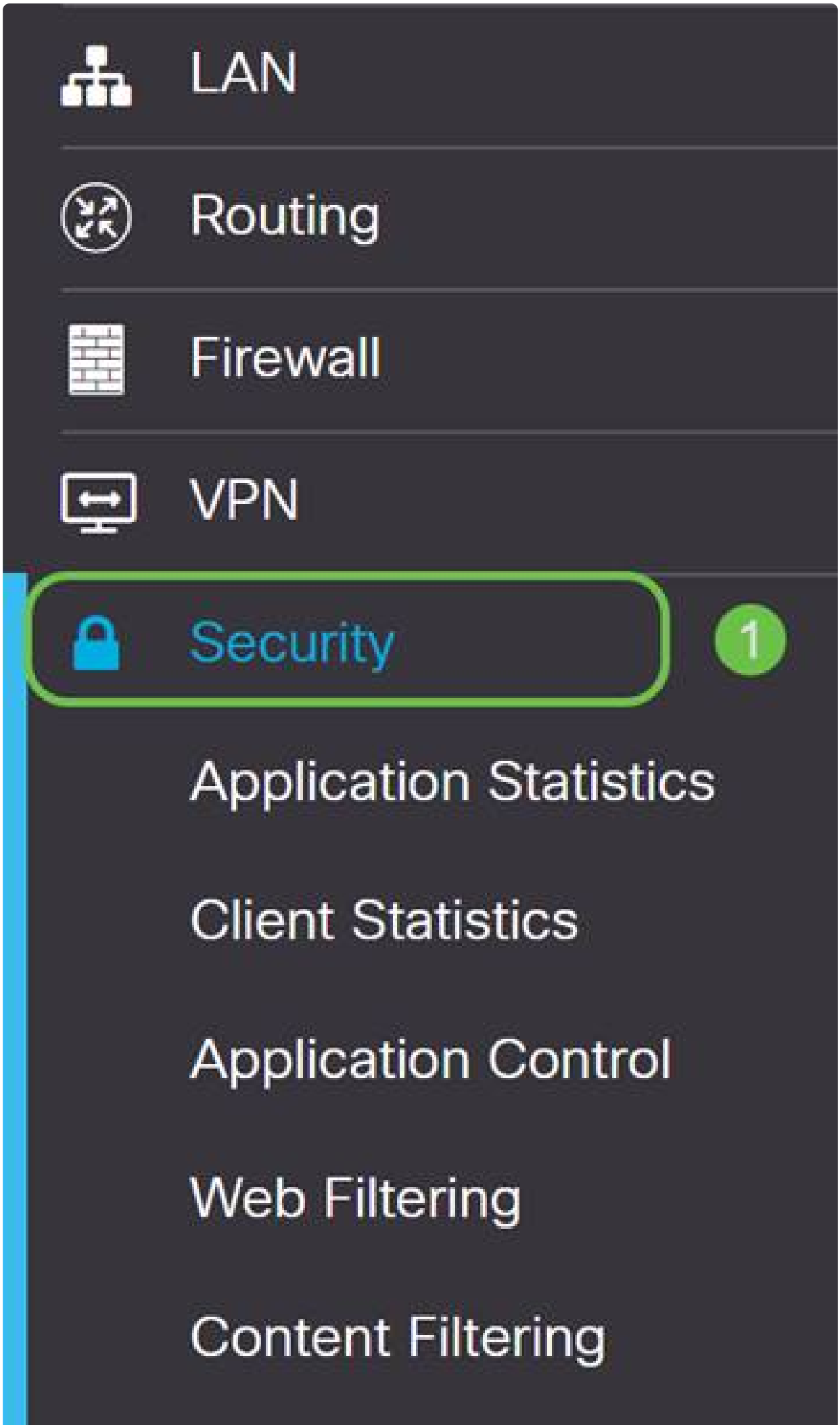
在RV345P上配置Umbrella

现在，我们已经在Umbrella内创建了API密钥，您可以将这些密钥安装到您的RV345P上

。

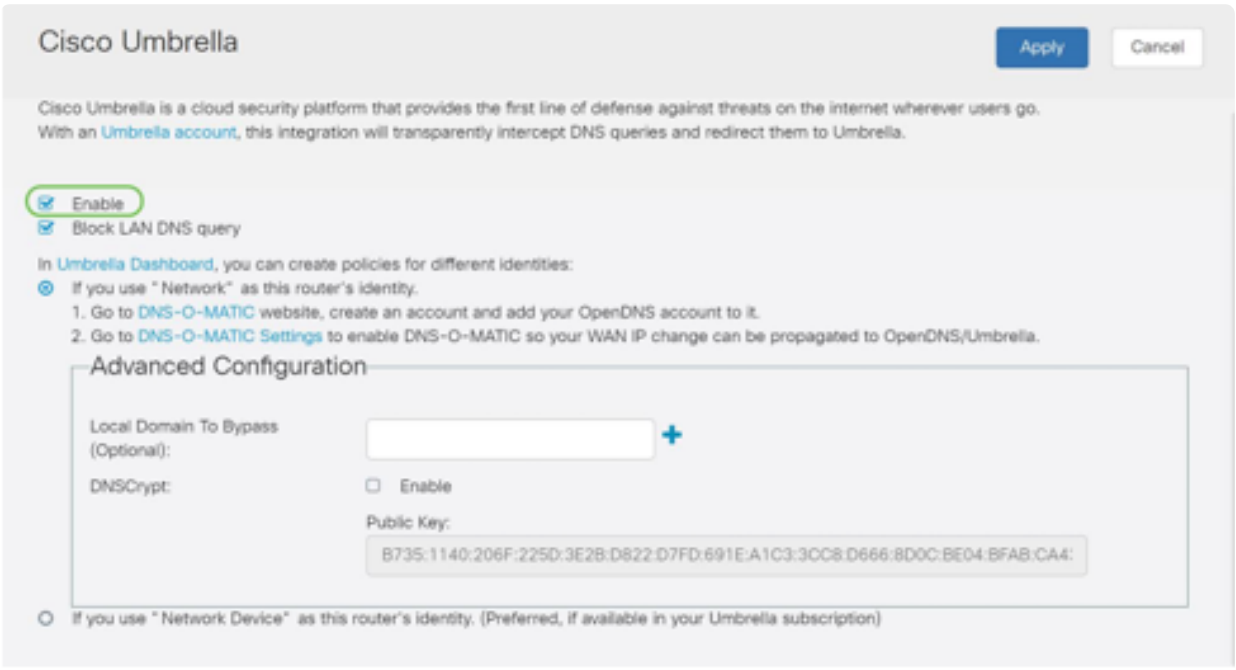
第 1 步

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


LAN
Routing
Firewall
VPN
Security
1
Application Statistics
Client Statistics
Application Control
Web Filtering
Content Filtering

第 2 步

Umbrella API屏幕包含一系列选项，通过点击Enable复选框开始启用Umbrella。

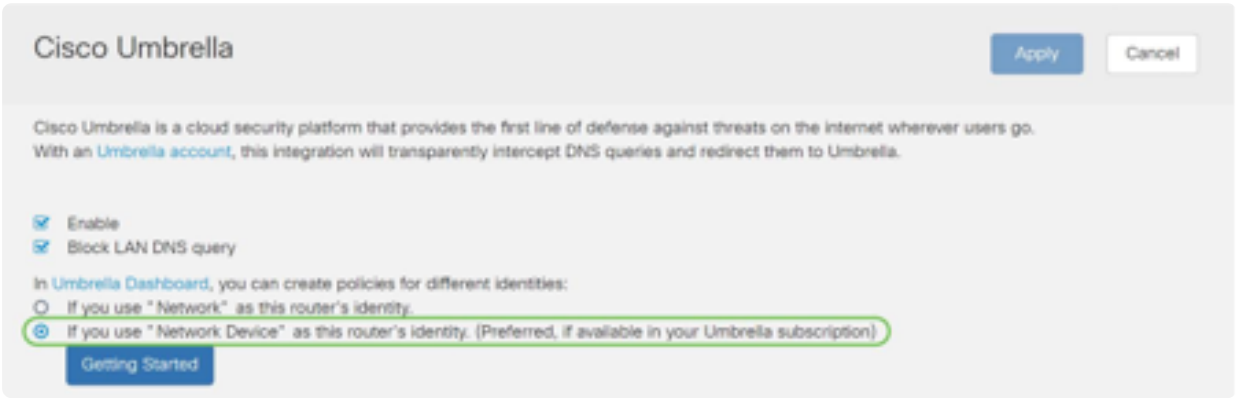


步骤 3（可选）

默认情况下，选中Block LAN DNS Queries框。此功能可以在您的路由器上自动创建访问控制列表，从而阻止DNS流量流出Internet。此功能强制所有域转换请求通过RV345P，对大多数用户来说是一个好主意。

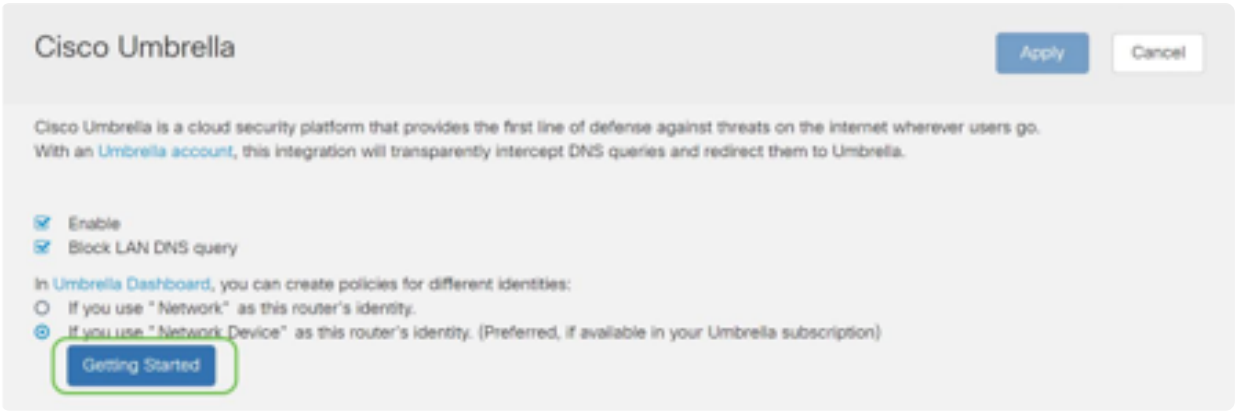
第 4 步

下一步有两种不同的方式。它们都取决于您的网络设置。如果您使用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交互。出于我们的目的，我们依赖于“网络设备”，因此我们点击底部单选按钮。



步骤 5

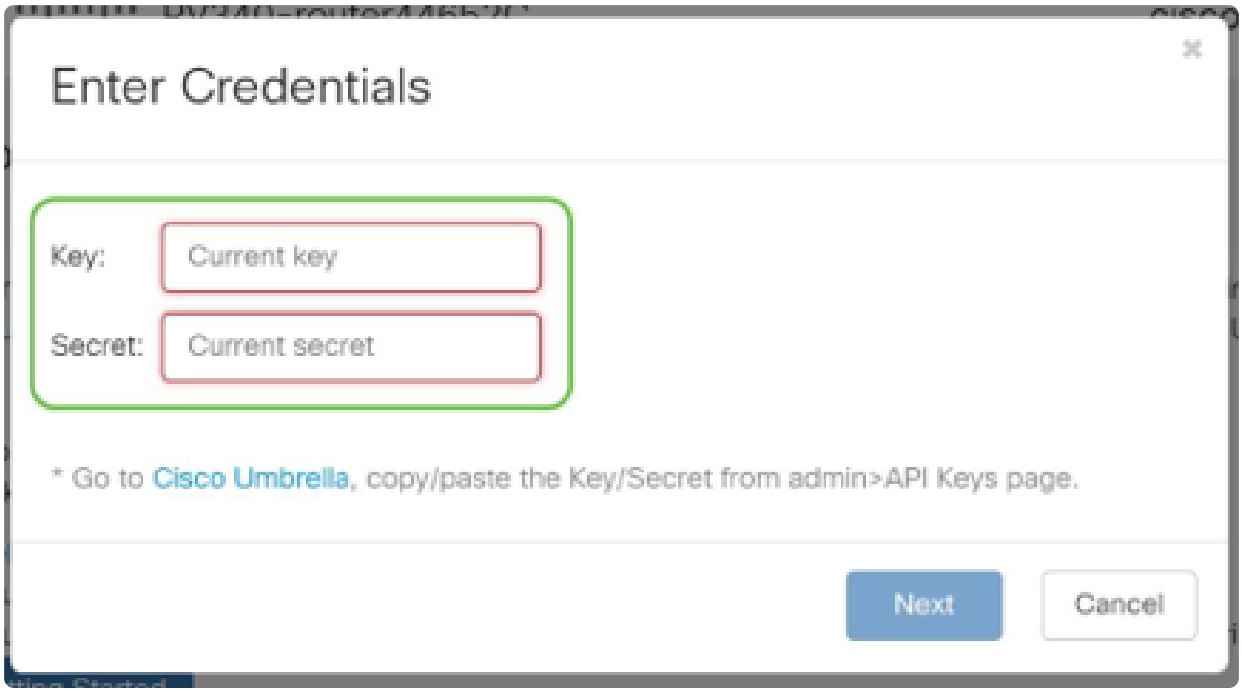
单击Getting Started。



第 6 步

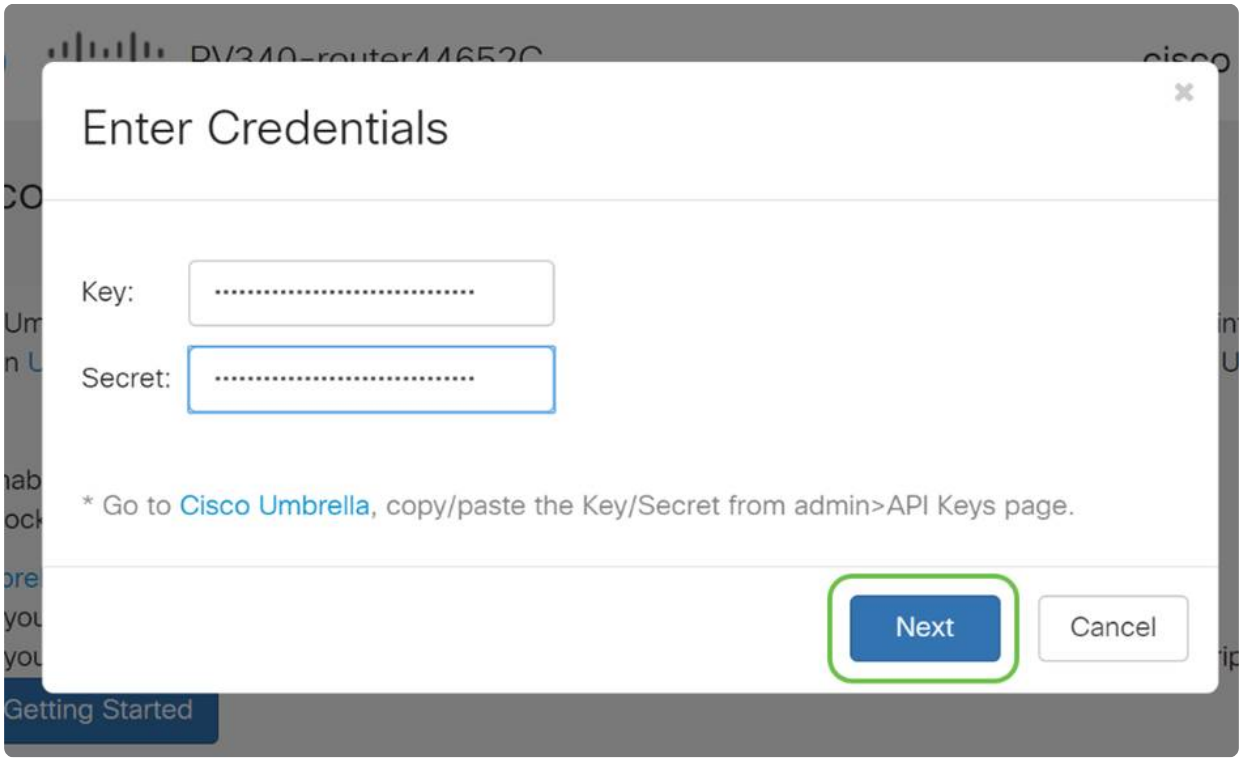
在文本框中输入API密钥和密钥。

> ⓘ Note: 说两遍才知道这很重要！如果丢失或意外删除了密钥，则没有函数或支持号码可供调用以检索此密钥。请妥善保管此密钥。如果丢失，您需要删除密钥，并对您希望使用Umbrella保护的每台设备重新授权新的API密钥。



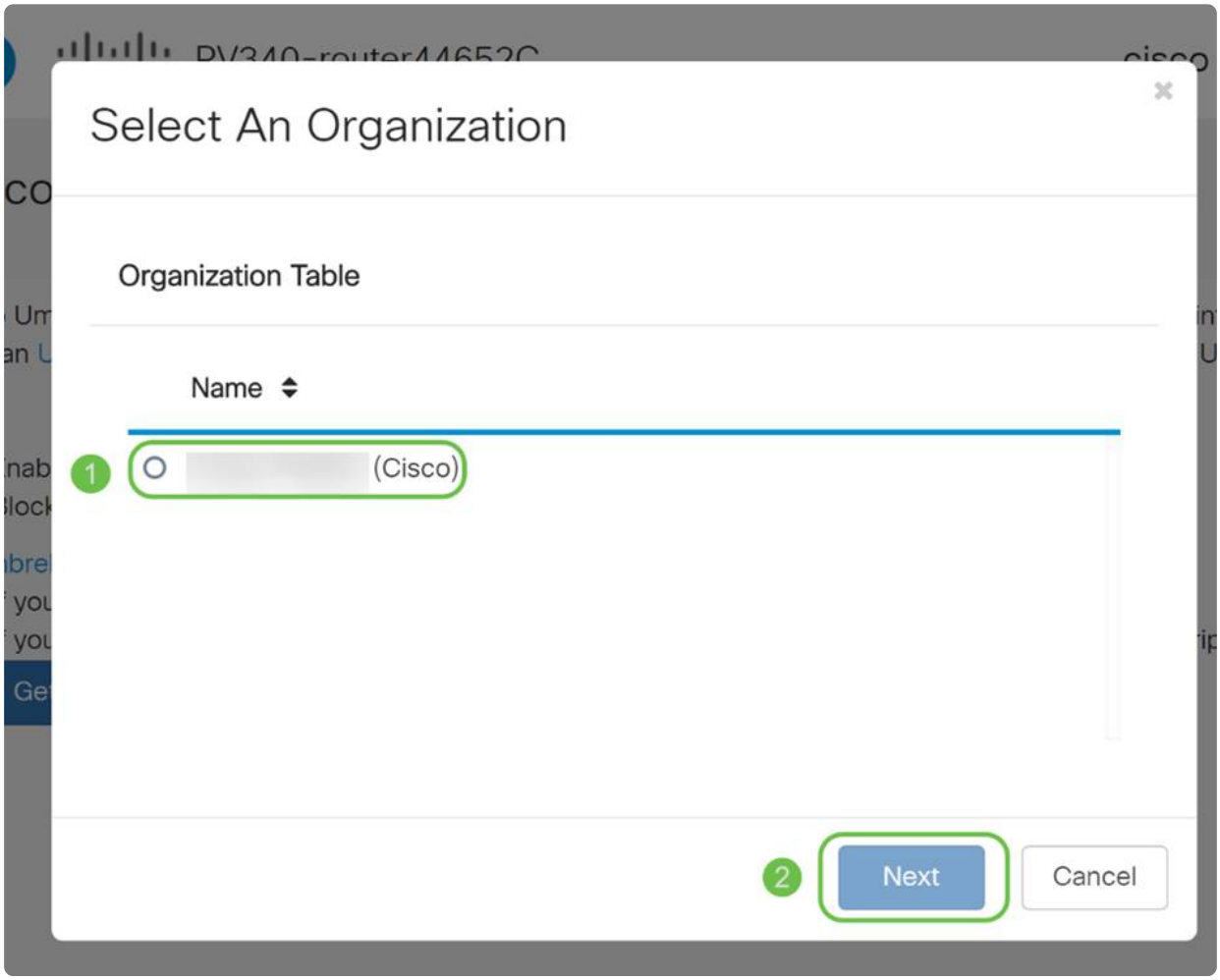
第 7 步

输入API和密钥后，单击Next按钮。



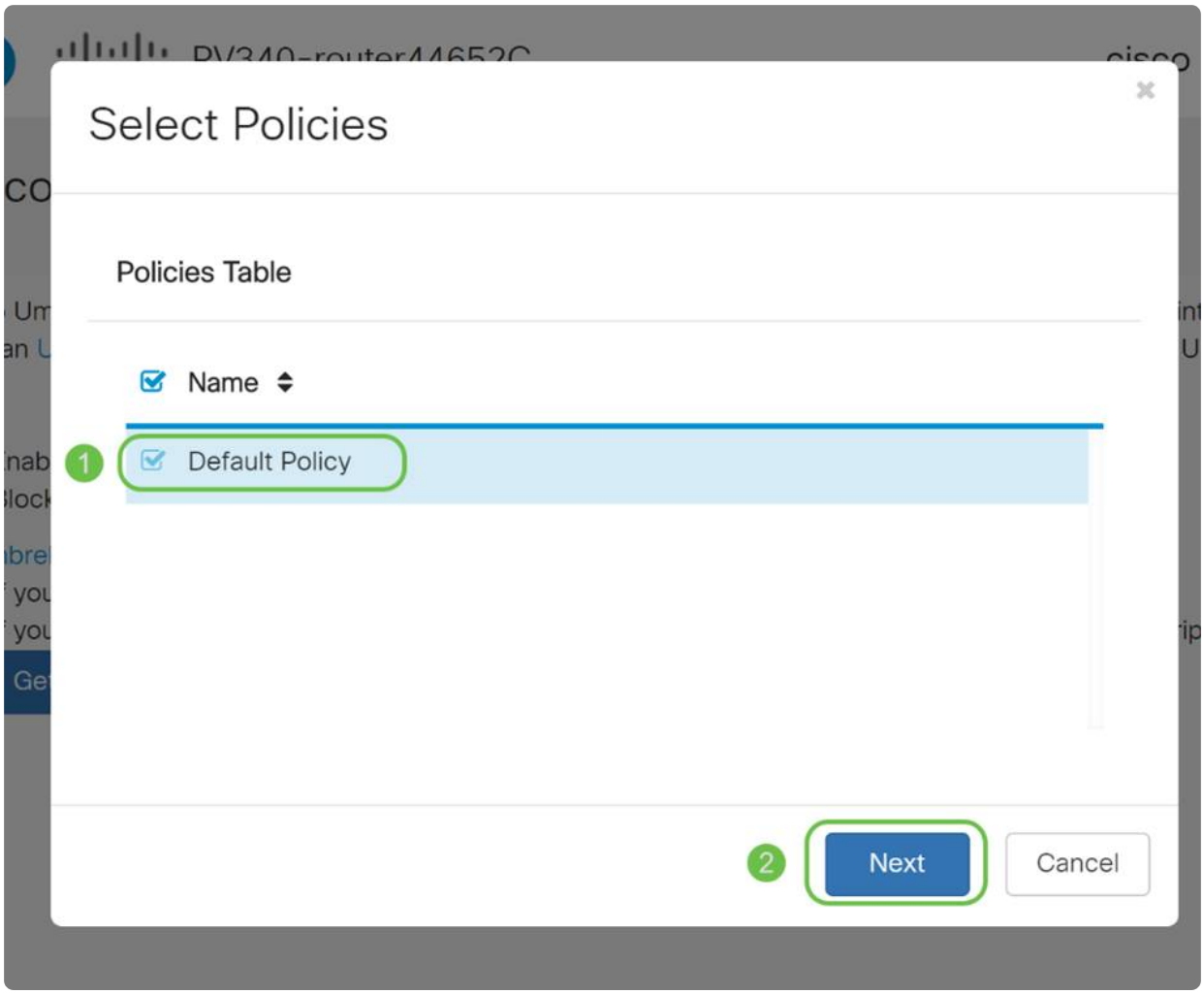
步骤 8

在下一个屏幕中，选择要与路由器关联的组织。单击 Next。



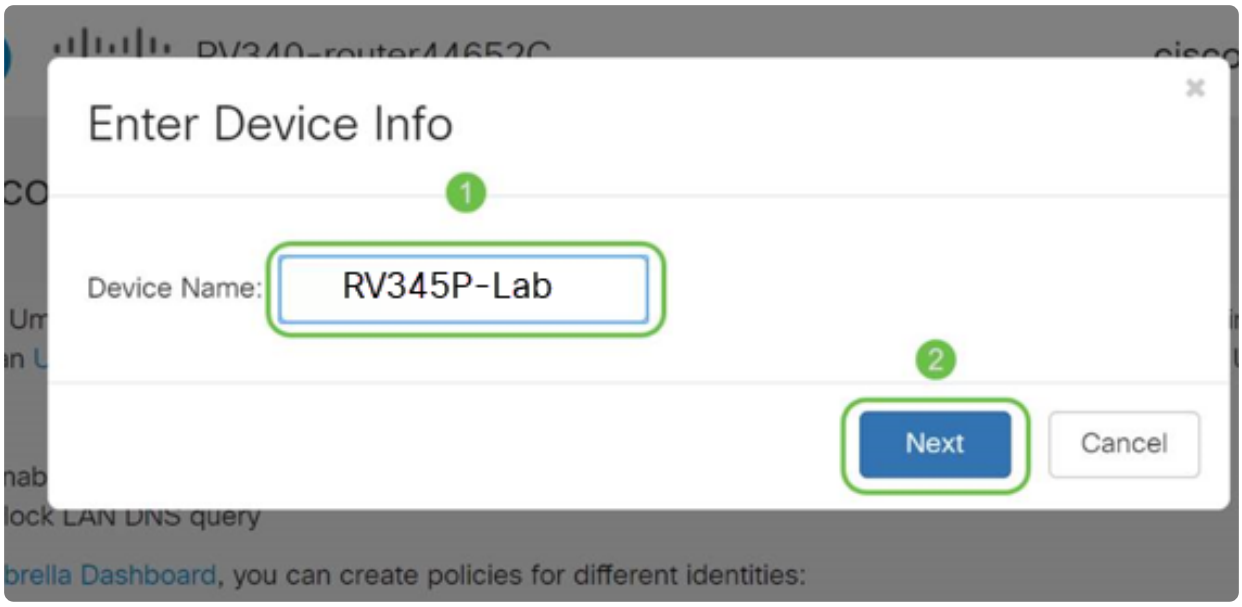
步骤 9

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。



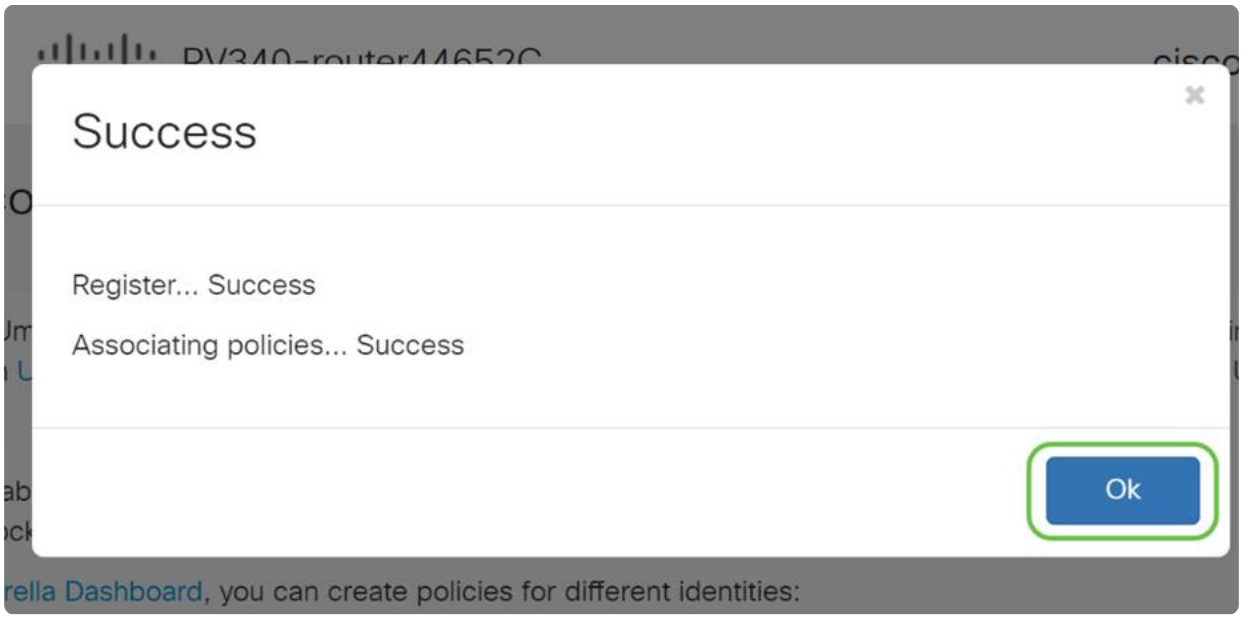
步骤 10

为设备指定名称，以便可以在Umbrella报告中指定该设备。在我们的设置中，我们将其命名为RV345P-Lab。



步骤 11

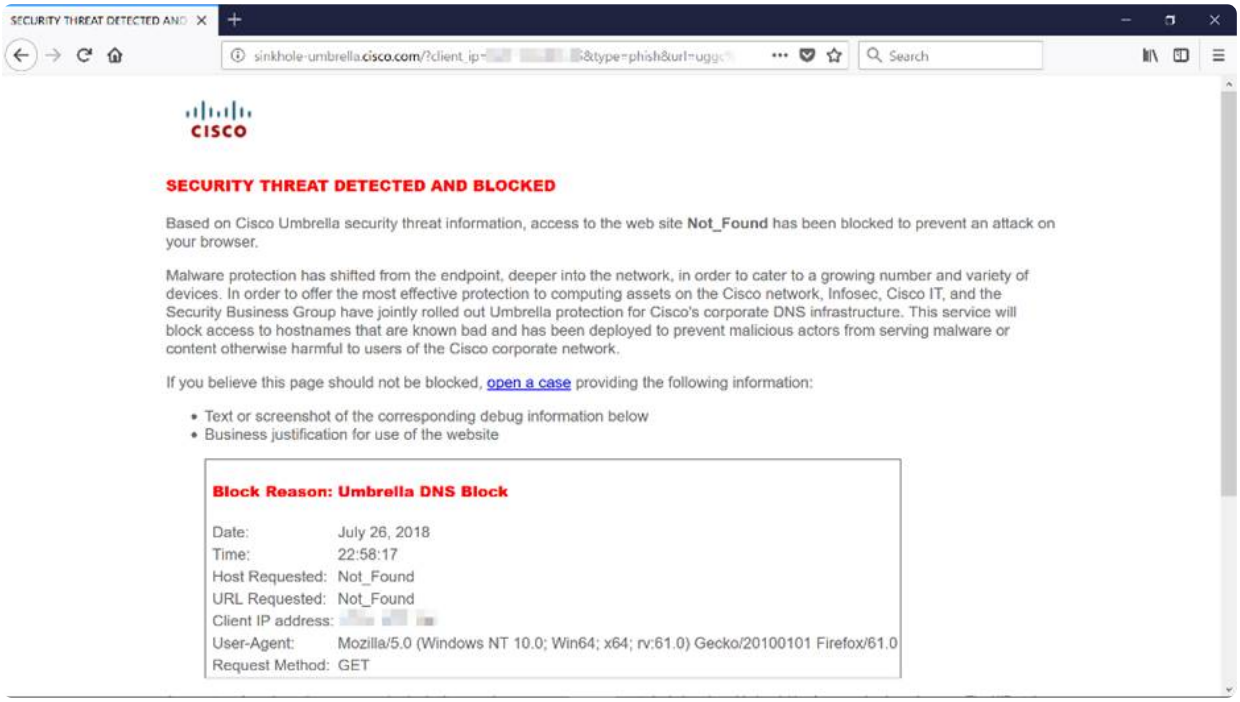
成功关联后，下一个屏幕将验证所选设置并提供更新。Click OK.



确认

祝贺您，您现在受到Cisco　Umbrella的保护。还是你？我们通过一个实时示例进行仔细检查，确保思科已创建一个网站，该网站专用于在加载页面时迅速确定问题。请单击此处，或在浏览器栏中键入https://InternetBadGuys.com。

如果Umbrella配置正确，您会看到类似于此的屏幕。



其他安全选项

您是否担心有人从网络设备拔下以太网电缆并连接到该电缆，从而试图未经授权访问网络？在这种情况下，注册一个允许主机列表非常重要，该列表会允许主机使用各自的IP和MAC地址直接连接到路由器。有关说明，请参阅在RV34x系列路由器上配置IP源保护。

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（例如Internet）访问、发送和接收来自专用网络的数据，但仍能确保安全连接到底层网络基础设施，以保护专用网络及其资源。

VPN隧道可建立一个私有网络，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，也有必要允许他们访问其专用网络。

VPN允许远程主机像位于同一本地网络一样运行。路由器最多支持50个隧道。在路由器

配置用于Internet连接后，可以在路由器和终端之间建立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，请查看思科企业VPN概述和最佳实践。

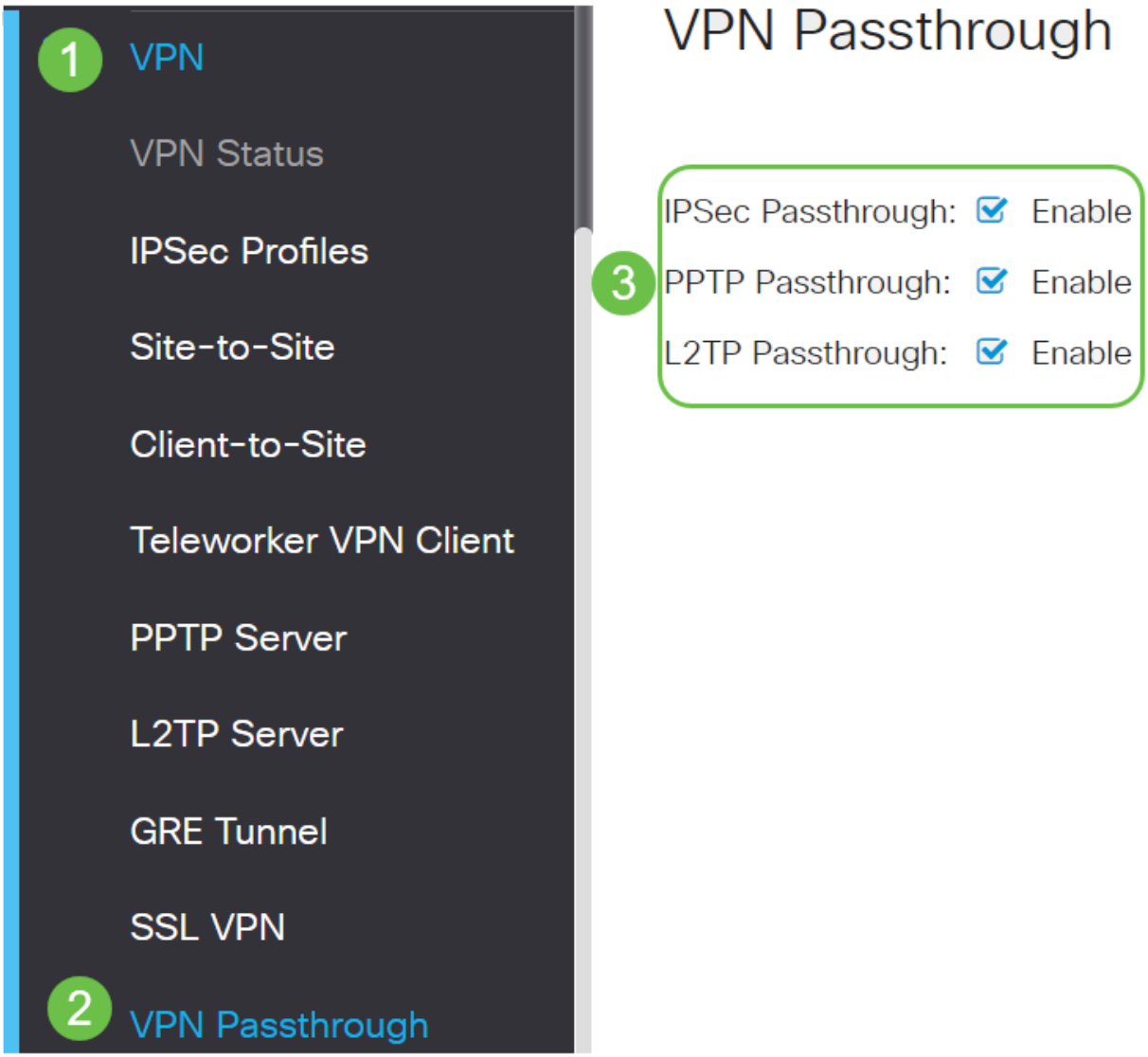
> ⓘ Note: AnyConnect VPN是本配置指南中列出的唯一支持Cisco VPN的产品。
>
> 思科不支持第三方非思科产品，包括GreenBow和Shrew Soft。它们严格出于指导目的被包括在内。如果您在文章之外需要这些方面的支持，您应该联系第三方以获得支持。

如果您不打算设置VPN，可以单击跳至下一部分。

VPN 传递

通常，当您要支持多个具有相同Internet连接的客户端时，每台路由器都支持网络地址转换(NAT)以节省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。这就是VPN穿透功能进入的地方。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直通仅允许PPTP和IPsec VPN通过Internet（从VPN客户端发起），然后到达远程VPN网关。此功能常见于支持NAT的家庭路由器上。

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



AnyConnect VPN

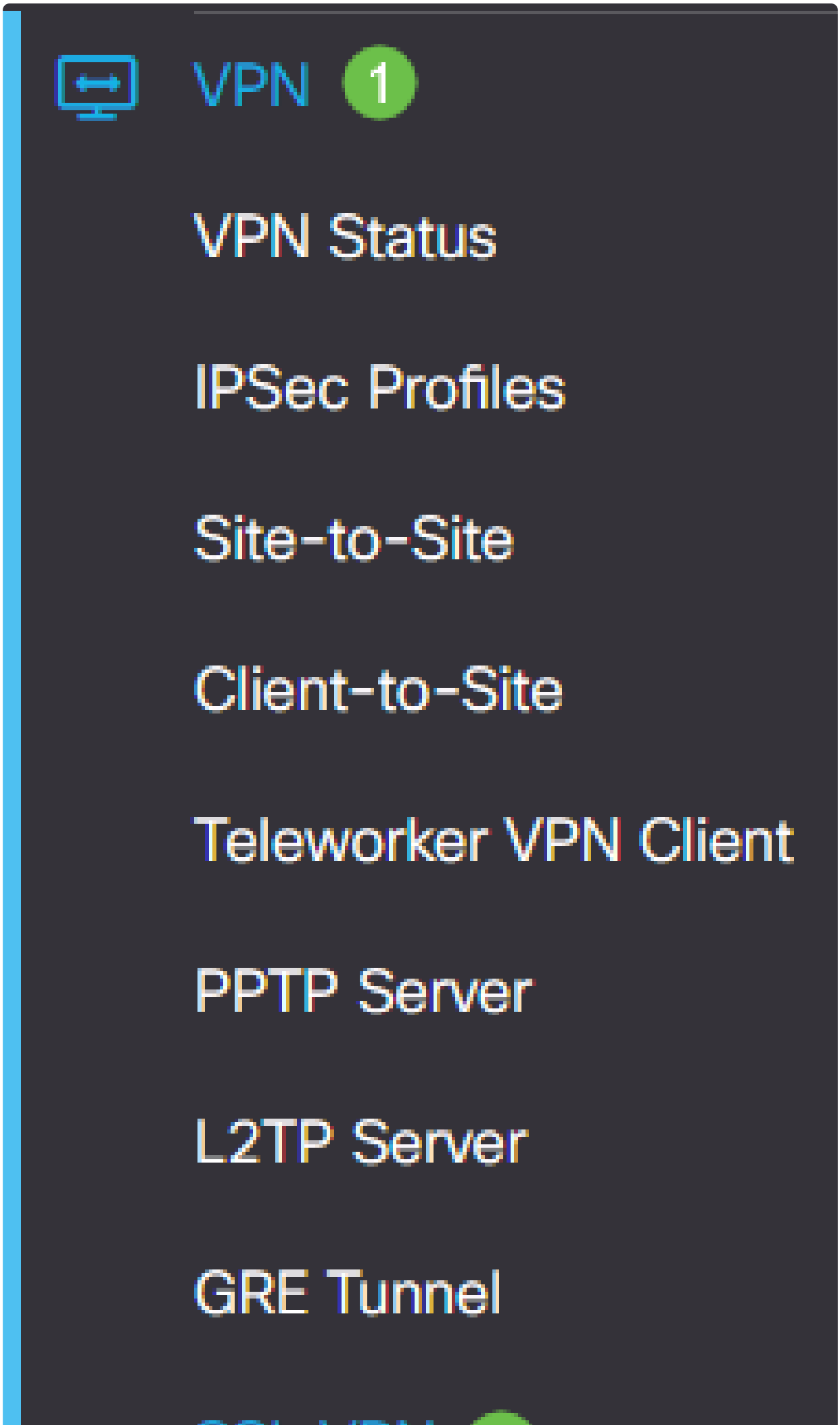
使用Cisco AnyConnect有几个优点：

1. 安全且持续的连接
2. 持久的安全性和策略实施
3. 可从自适应安全设备(ASA)或企业软件部署系统部署
4. 可定制和可翻译的
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Internet密钥交换版本2.0(IKEv2.0)协议

在RV345P上配置AnyConnect SSL VPN

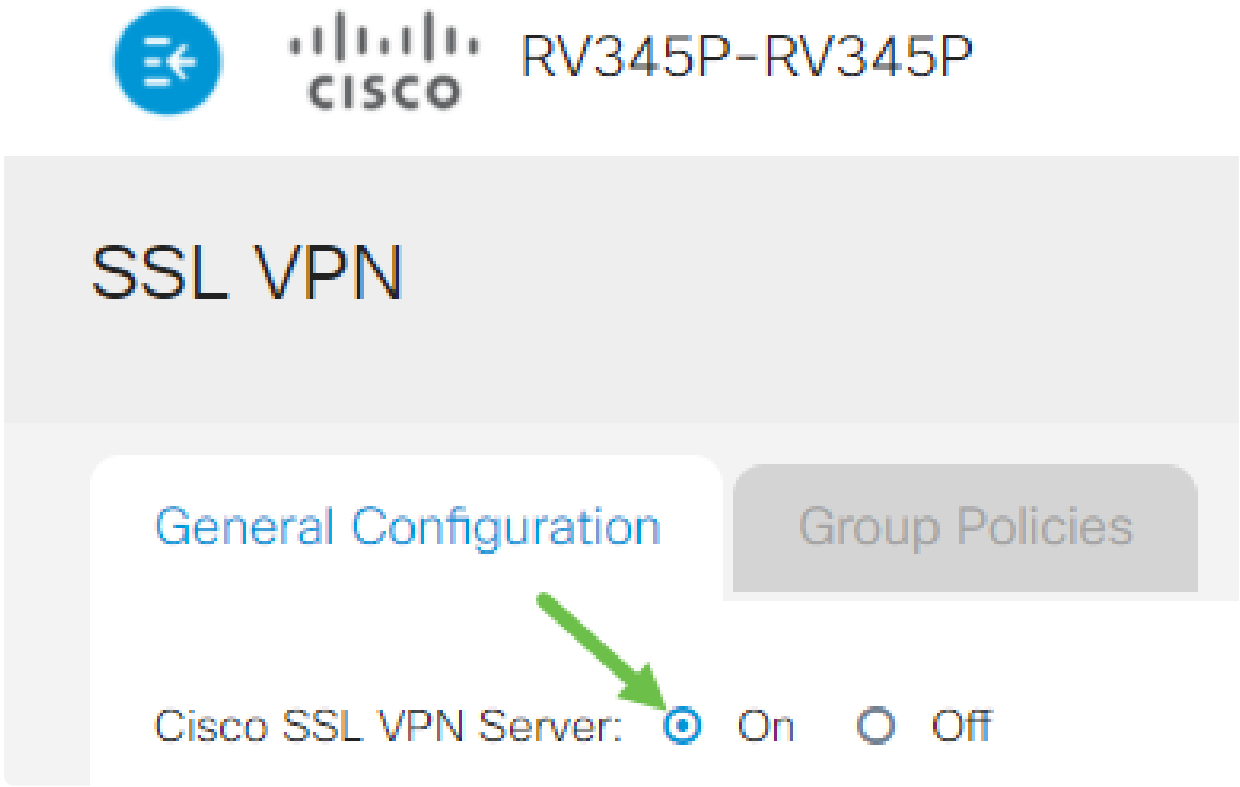
第 1 步

访问路由器基于Web的实用程序并选择VPN > SSL VPN。


VPN
1
VPN Status
IPSec Profiles
Site-to-Site
Client-to-Site
Teleworker VPN Client
PPTP Server
L2TP Server
GRE Tunnel

第 2 步

单击On单选按钮以启用Cisco SSL VPN服务器。



强制网关设置

第 1 步

以下配置设置是必需的：

1 从下拉列表中选择网关接口。此端口将用于通过SSL VPN隧道传递流量。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至65535。

3 从下拉列表中选择证书文件(Certificate File)。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。

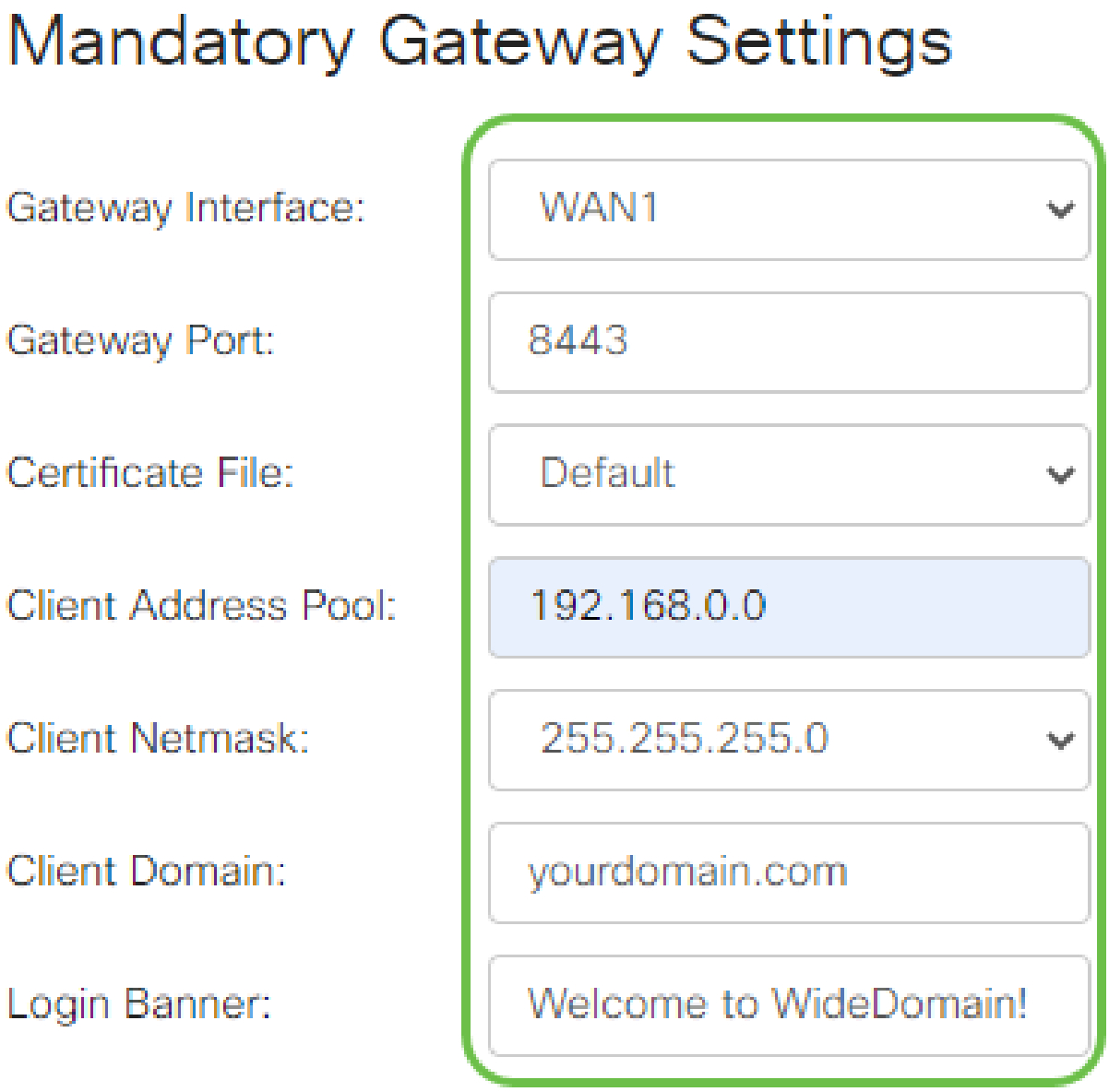
4 在客户端地址池字段中输入客户端地址池的IP地址。此池将是分配给远程VPN客户端的IP地址范围。

确保IP地址范围不与本地网络中的任何IP地址重叠。

5 从下拉列表中选择Client Netmask。

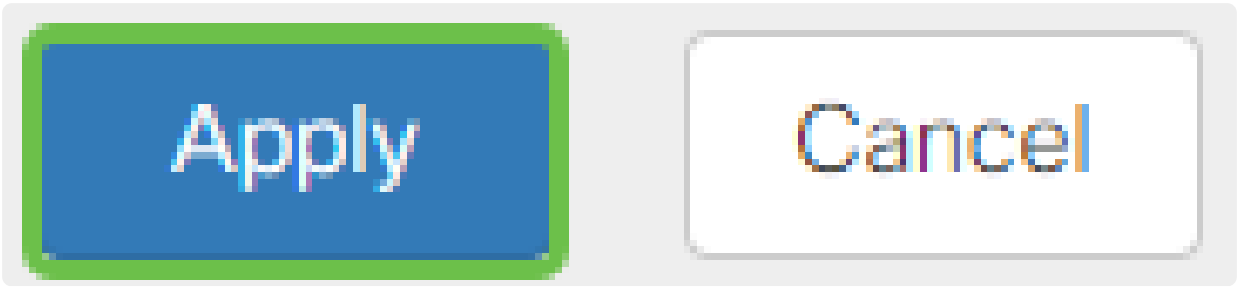
6 在Client Domain字段中输入客户端域名。这是应推送到SSL VPN客户端的域名。

7 在Login Banner字段中输入显示为登录标语的文本。这是客户端每次登录时显示的标语。



第 2 步

单击 Apply。

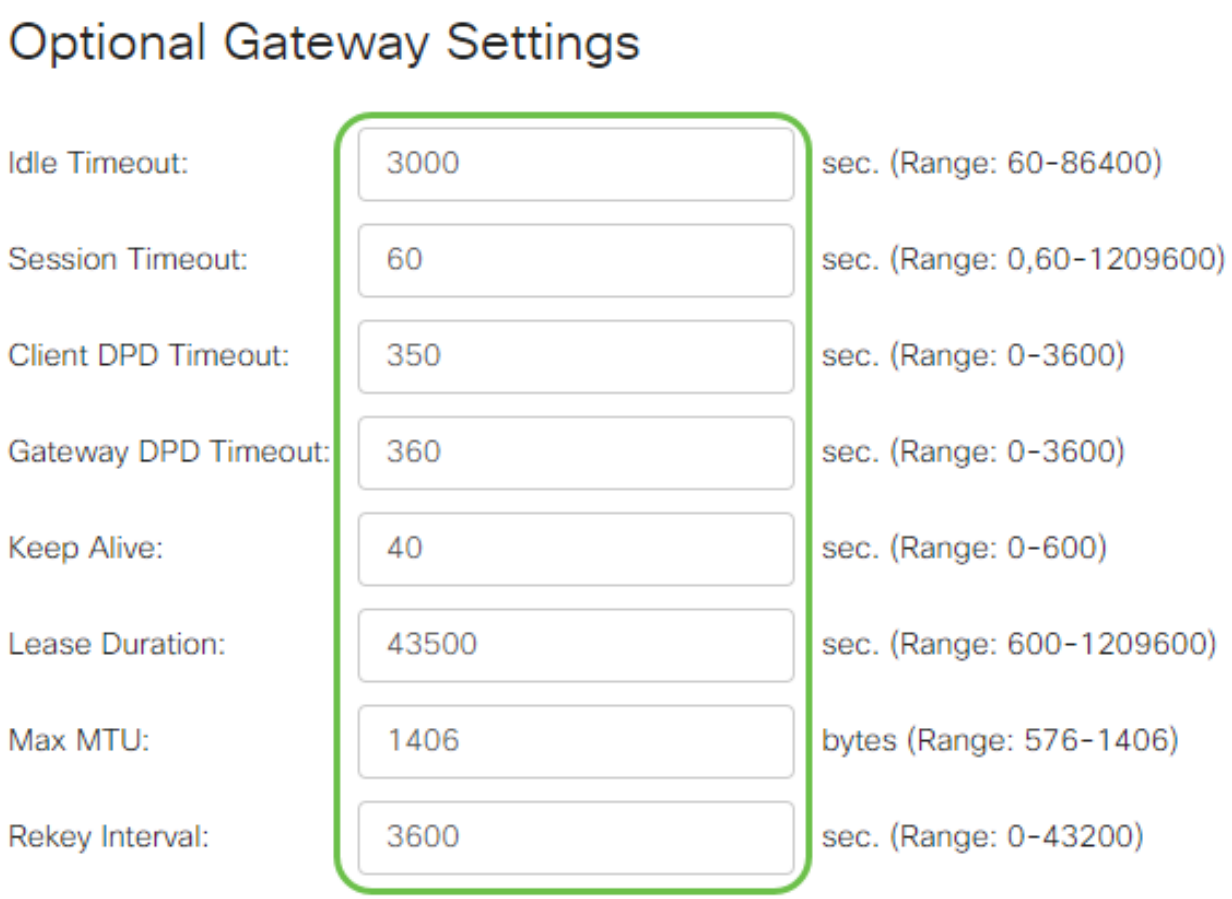


可选网关设置

第 1 步

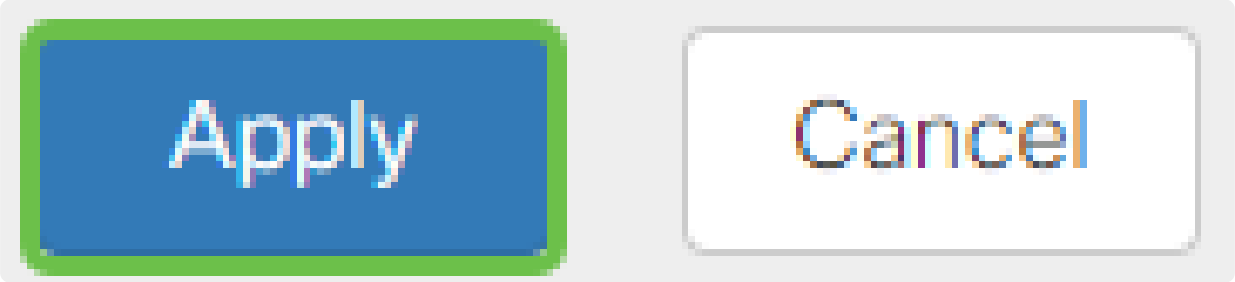
以下配置设置是可选的：

1. 输入介于60到86400之间的空闲超时值（以秒为单位）。该值将是SSL VPN会话可以保持空闲的持续时间。
2. 在Session Timeout（会话超时）字段中，输入一个以秒为单位的值。这是传输控制协议(TCP)或用户数据报协议(UDP)会话在指定的空闲时间之后超时的时间。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一个值（以秒为单位），范围为0到600。此功能可确保您的路由器始终连接到Internet。如果它被丢弃，它将尝试重新建立VPN连接。
6. 在Lease Duration字段中输入要连接的隧道的持续时间值（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。



第 2 步

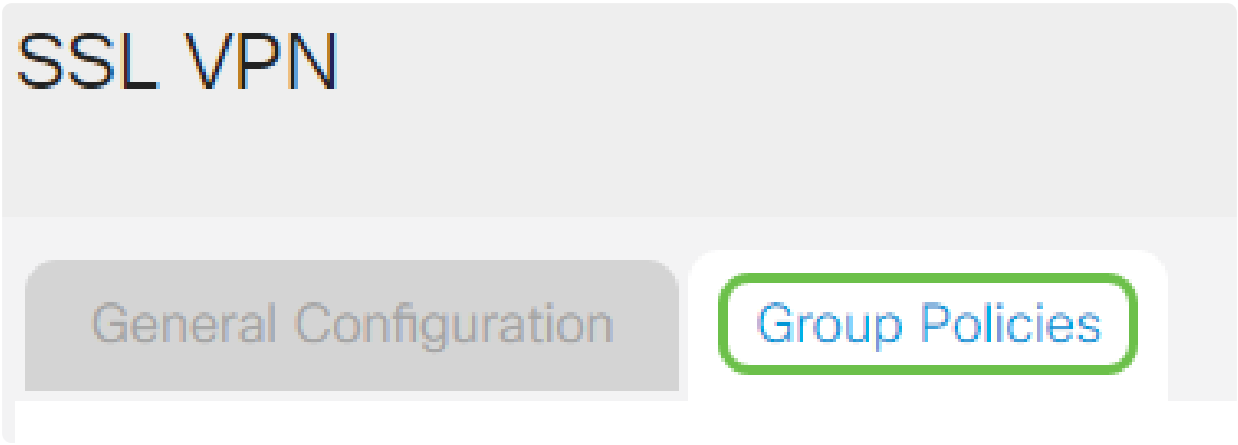
单击 Apply。



配置组策略

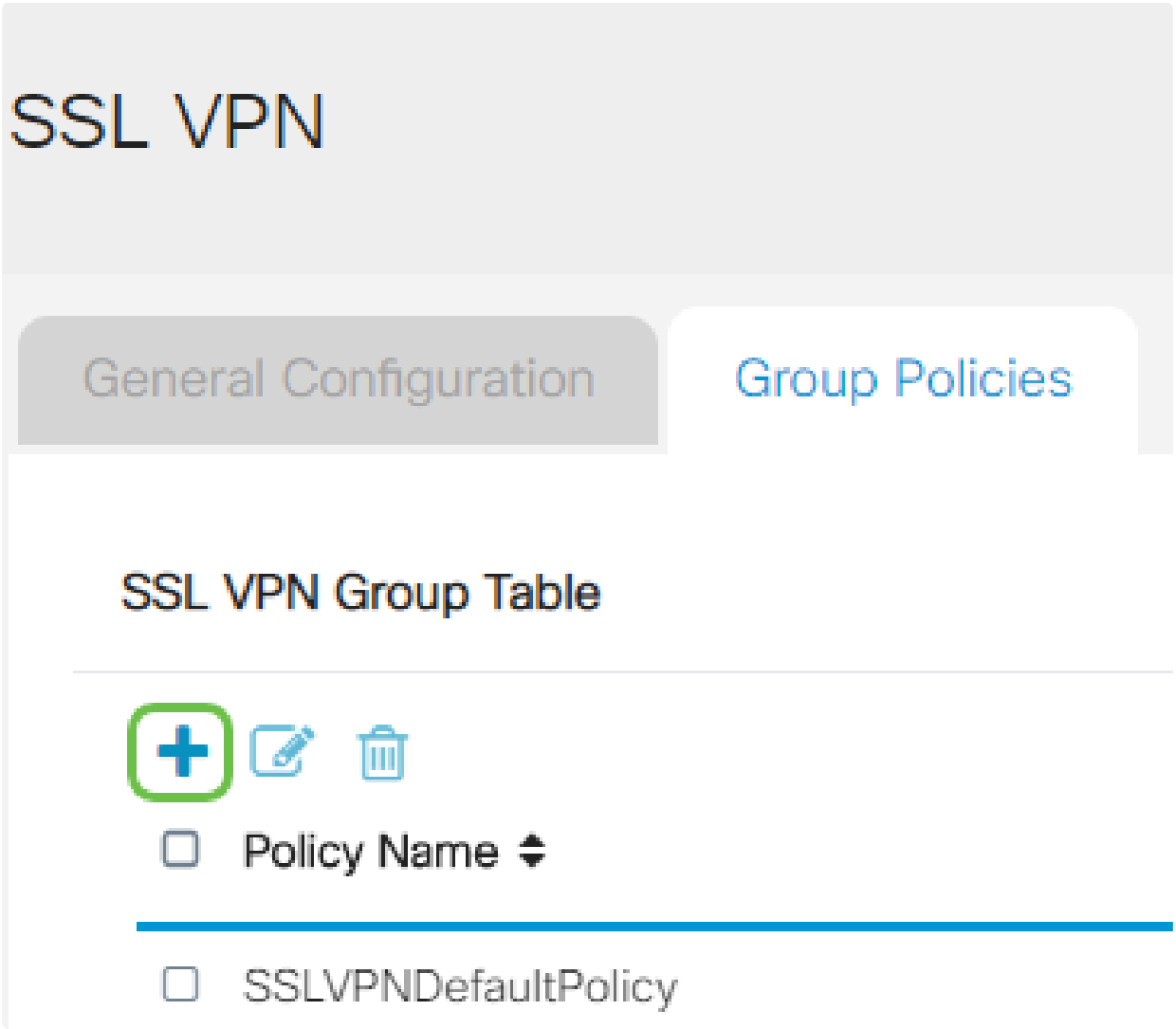
第 1 步

点击Group Policies选项卡。



第 2 步

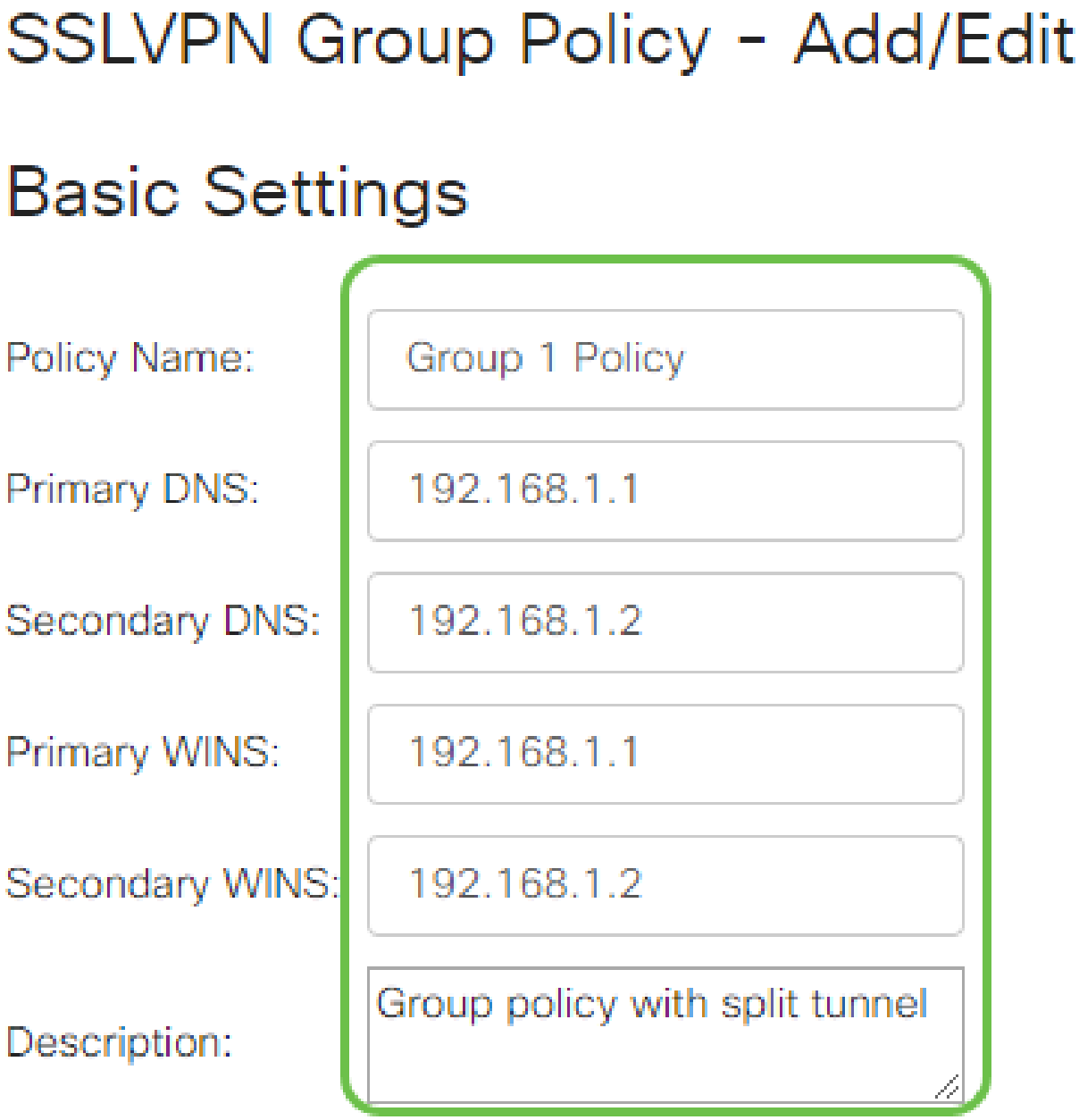
点击SSL VPN Group Table下的add图标以添加组策略。



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

第 3 步

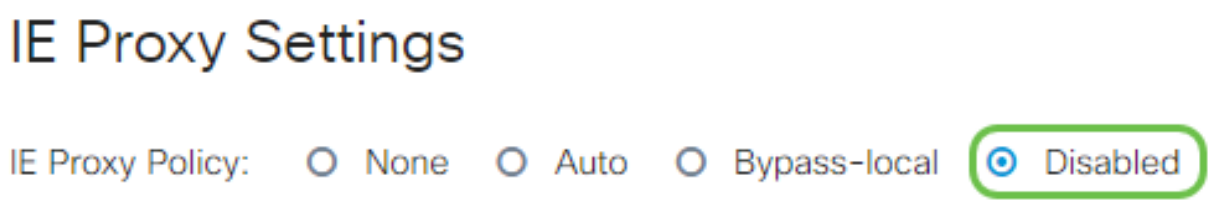
1. 在Policy Name字段中输入您的首选策略名称。
2. 在提供的字段中输入主要DNS的IP地址。默认情况下，已提供此IP地址。
3. （可选）在提供的字段中输入辅助DNS的IP地址。这将在主DNS发生故障时用作备份。
4. （可选）在提供的字段中输入主WINS的IP地址。
5. （可选）在提供的字段中输入辅助WINS的IP地址。
6. （可选）在说明字段中输入策略的说明。



步骤 4（可选）

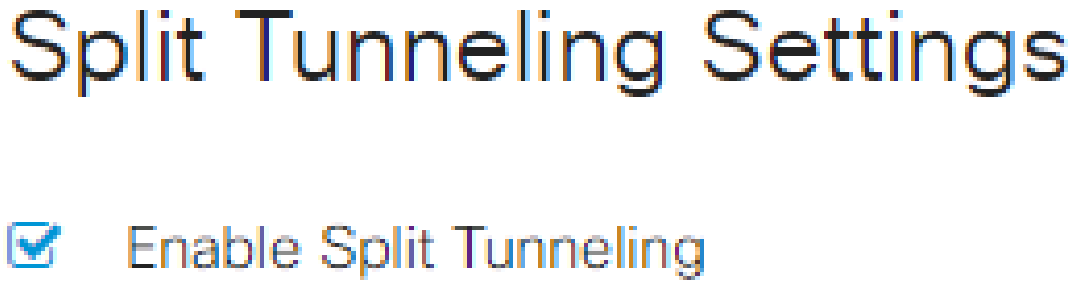
点击单选按钮选择IE Proxy Policy（IE代理策略），以启用Microsoft Internet Explorer(MSIE)代理设置来建立VPN隧道。选项有：

- 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区域中，选中Enable Split Tunneling复选框，以允许以未加密方式将发往Internet的流量直接发送到Internet。完全隧道会将所有流量发送到终端设备，然后将其路由到目标资源，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。



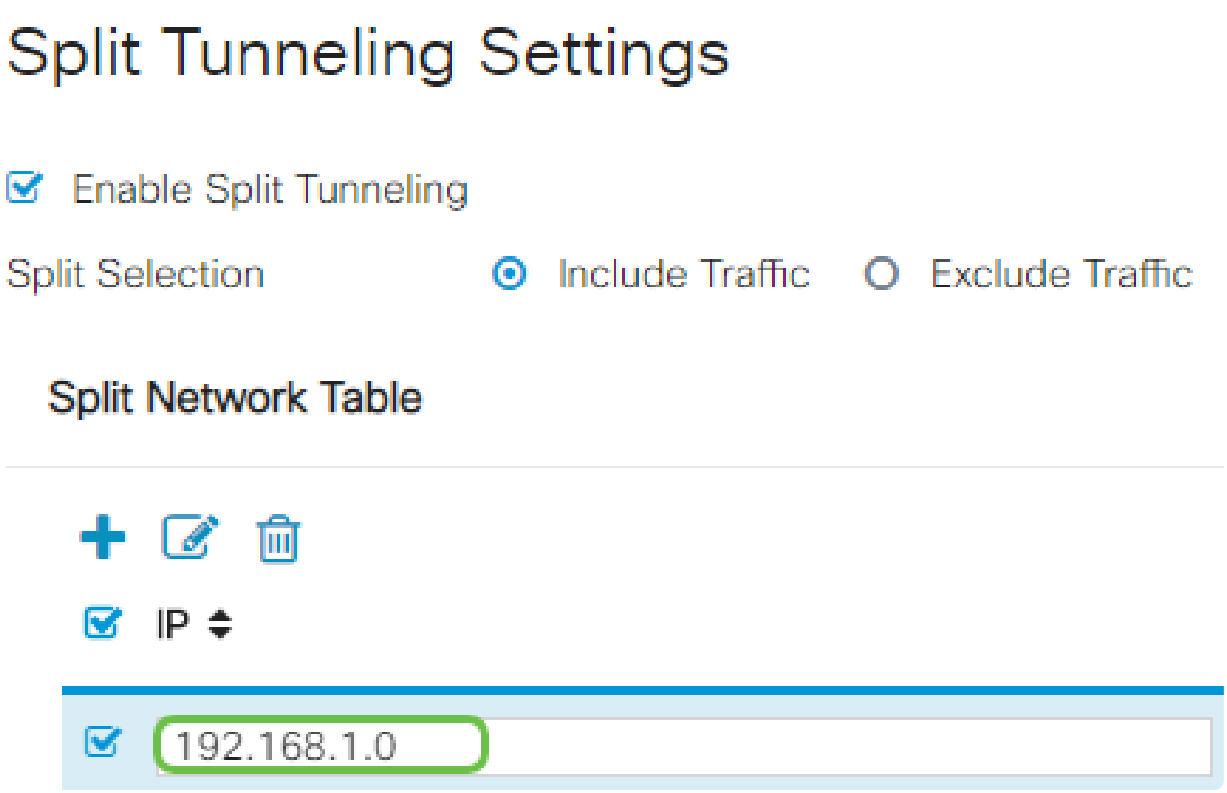
第 7 步

在Split Network Table中，点击add icon以添加拆分网络例外。



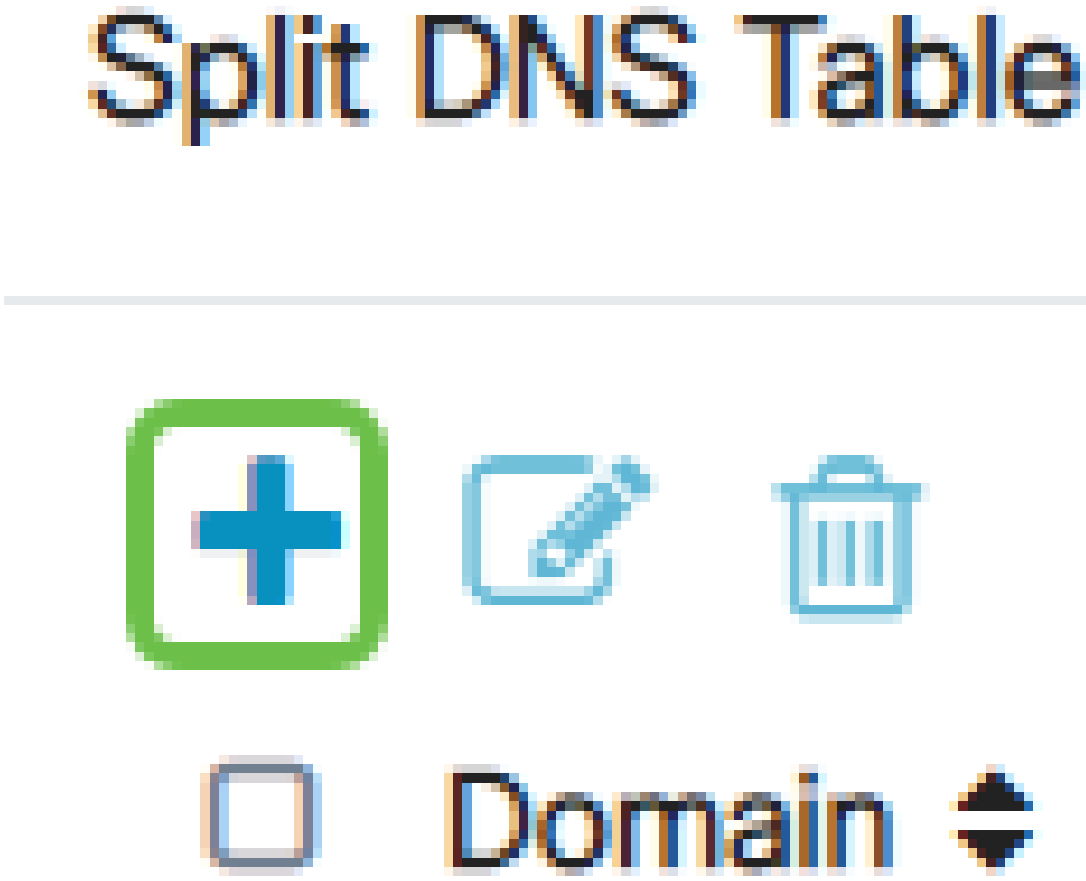
步骤 8

在提供的字段中输入网络的IP地址。



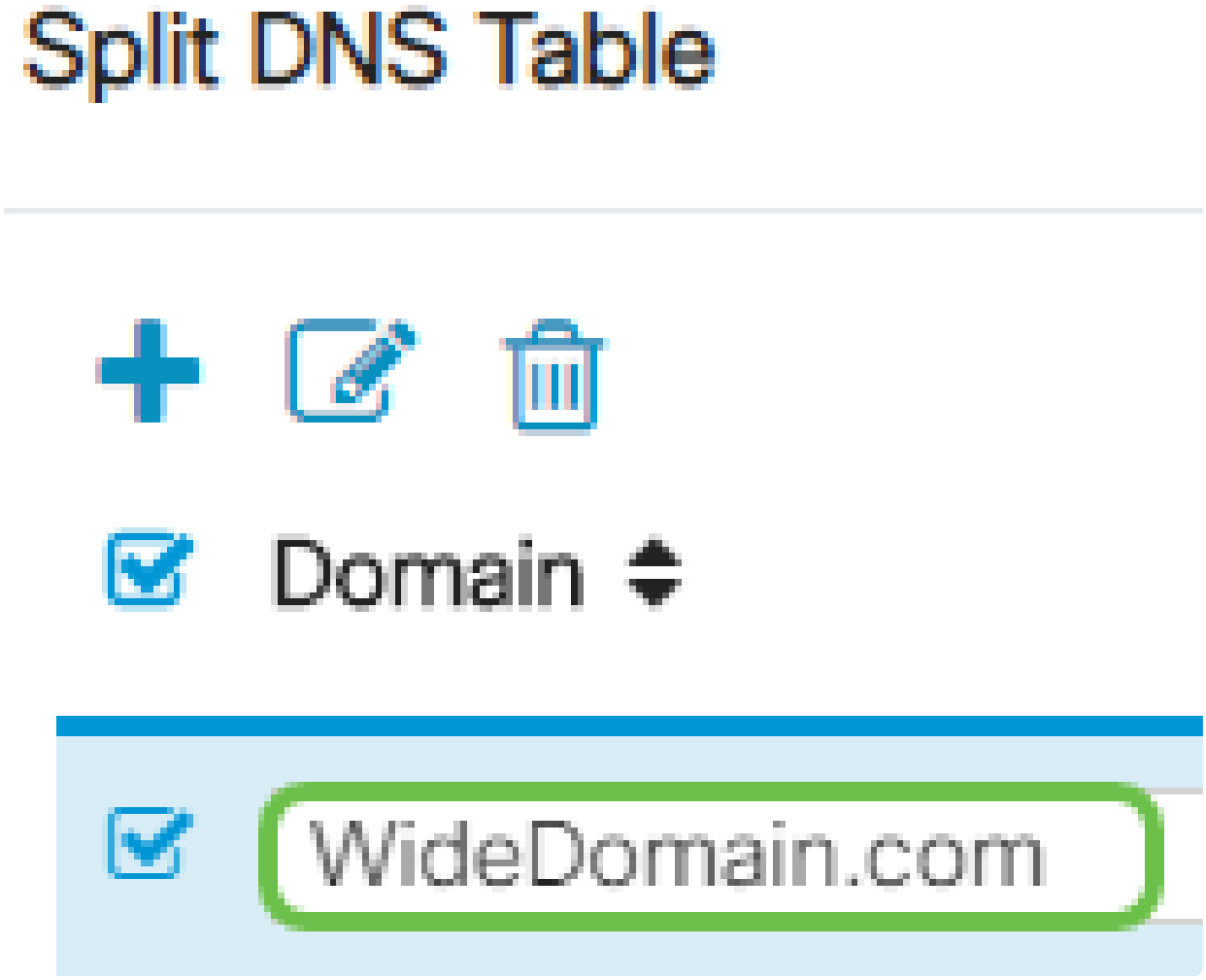
步骤 9

在拆分DNS表中，点击add图标以添加拆分DNS例外。



步骤 10

在提供的字段中输入域名，然后单击Apply。



默认情况下，路由器附带2个AnyConnect服务器许可证。这意味着，一旦拥有AnyConnect客户端许可证，您就可以与任何其他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。

下一部分详细介绍如何获取客户端许可证。

AnyConnect移动客户端

VPN客户端是在要连接到远程网络的计算机上安装并运行的软件。此客户端软件的设置配置必须与VPN服务器的配置相同，例如IP地址和身份验证信息。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。根据要连接的网络的物理位置，VPN客户端也可以是硬件设备。如果使用VPN连接连接位于不同位置的两个网络，通常会发生这种情况。

Cisco AnyConnect安全移动客户端是一种软件应用程序，用于连接到在各种操作系统和硬件配置下工作的VPN。此软件应用程序使用户可以安全访问另一个网络的远程资源，就像直接连接到其网络一样。

路由器注册并配置了AnyConnect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，下一部分将详细介绍该过程。

购买许可证

您必须从您的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可用于购买包含25个捆绑包的额外许可证。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，列出的产品ID将是完整功能的最低要求。

请注意，首先列出的AnyConnect客户端许可证产品SKU提供期限为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也具有不同的订用级别，如下所示：

- LS-AC-PLS-1Y-S1 - 1年期Cisco AnyConnect Plus客户端许可证
- LS-AC-PLS-3Y-S1 — 3年Cisco AnyConnect Plus客户端许可证
- LS-AC-PLS-5Y-S1 — 5年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，您应向其发送以下链接：

- Windows 窗口版本:Windows计算机上的AnyConnect
- Mac：在Mac上安装AnyConnect。
- Ubuntu桌面：在 Ubuntu 桌面版上安装和使用 AnyConnect
- 如果您遇到问题，可以转至Gather Information for Basic Troubleshooting on Cisco AnyConnect Secure Mobility Client Errors。

检验AnyConnect VPN连接

第 1 步

单击AnyConnect Secure Mobility Client图标。

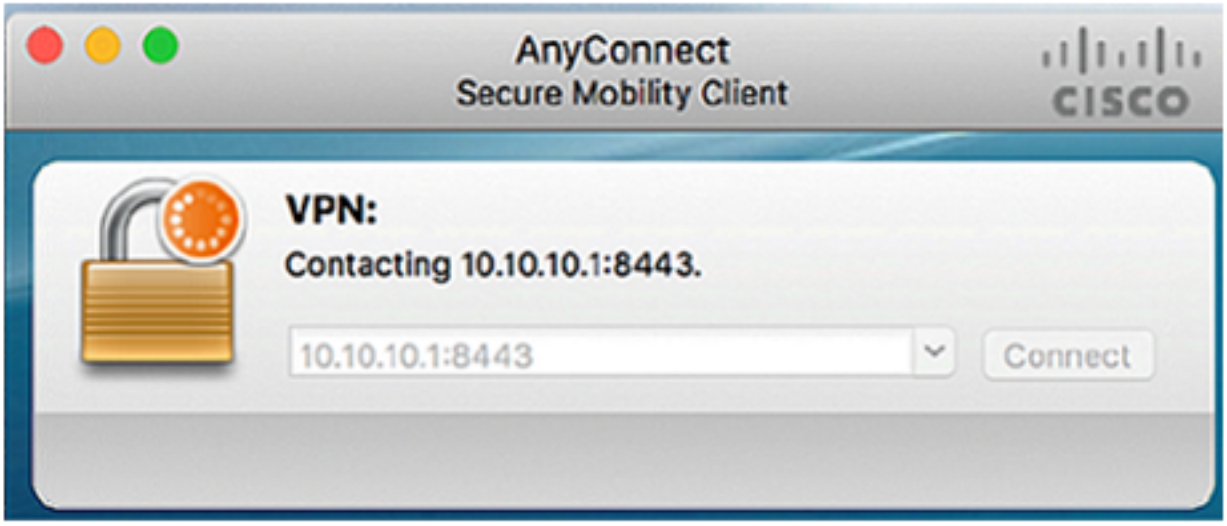


第 2 步

在AnyConnect Secure Mobility Client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Connect。

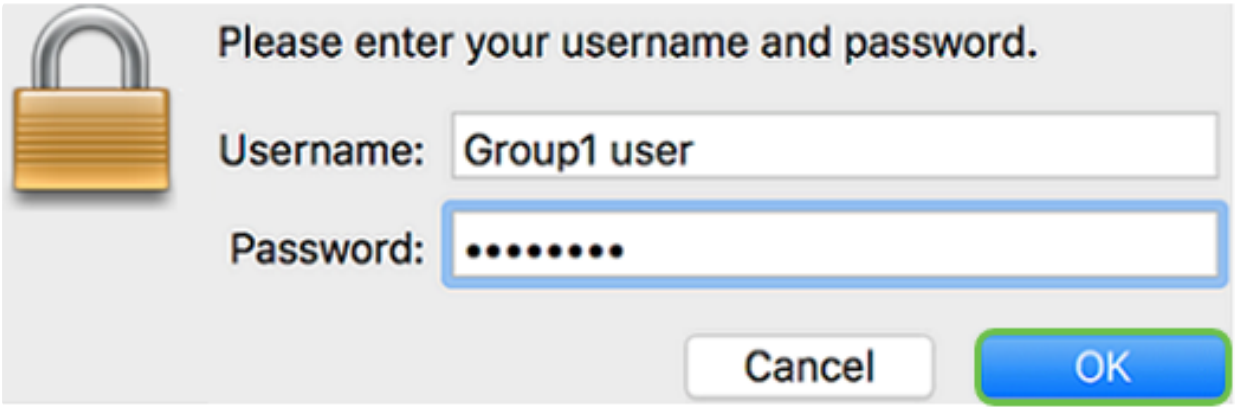


软件现在将显示它正在联系远程网络。



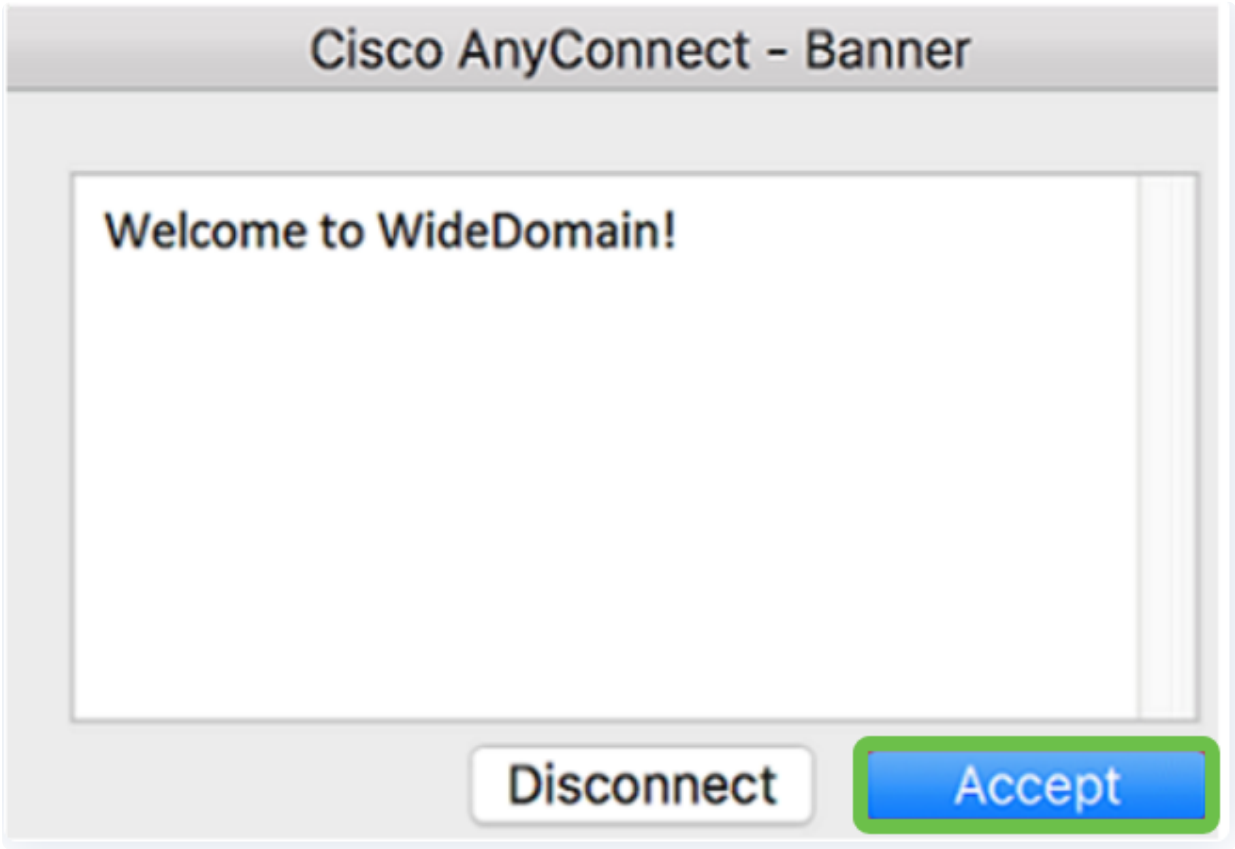
第 3 步

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。

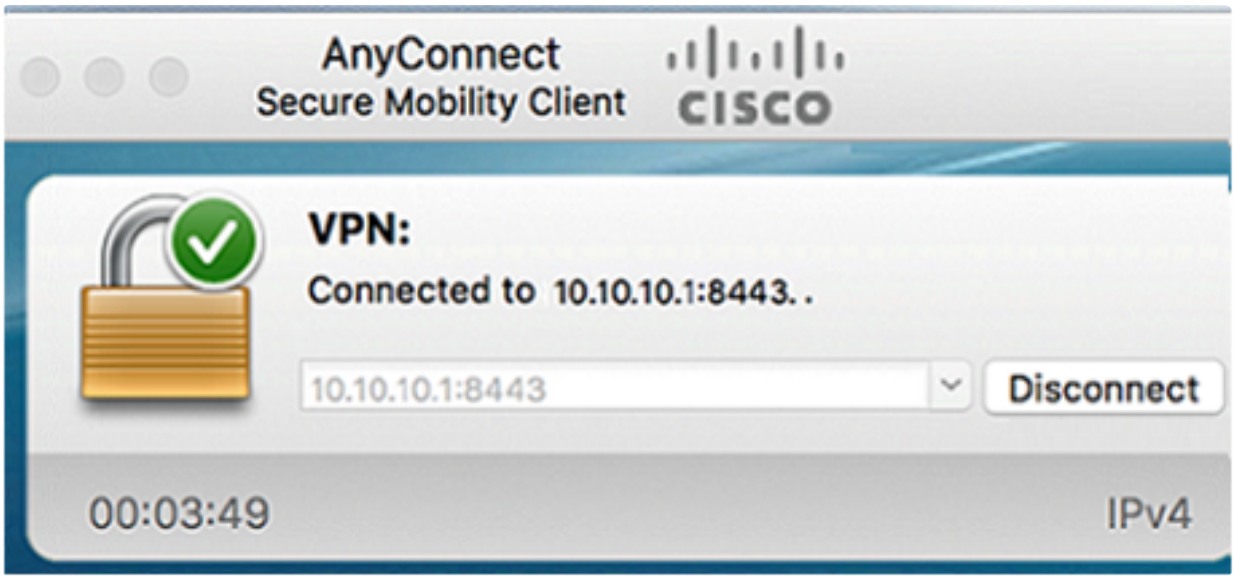


第 4 步

一旦建立连接，系统就会显示登录横幅。单击 Accept。



AnyConnect窗口现在应指示与网络的VPN连接是否成功。



如果现在使用AnyConnect VPN，可以跳过其他VPN选项并转到下一节。

Shrew软件VPN

IPsec VPN允许您通过建立互联网上的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，支持Shrew Soft VPN客户端。本节将介绍如何配置路由器和智能软客户端，以保护与VPN的连接。

> ⓘ Note: 思科不支持Shrew Soft。本示例仅用于演示目的。如果您在使用Shrew Soft时遇到问题，请与他们联系以获得支持。

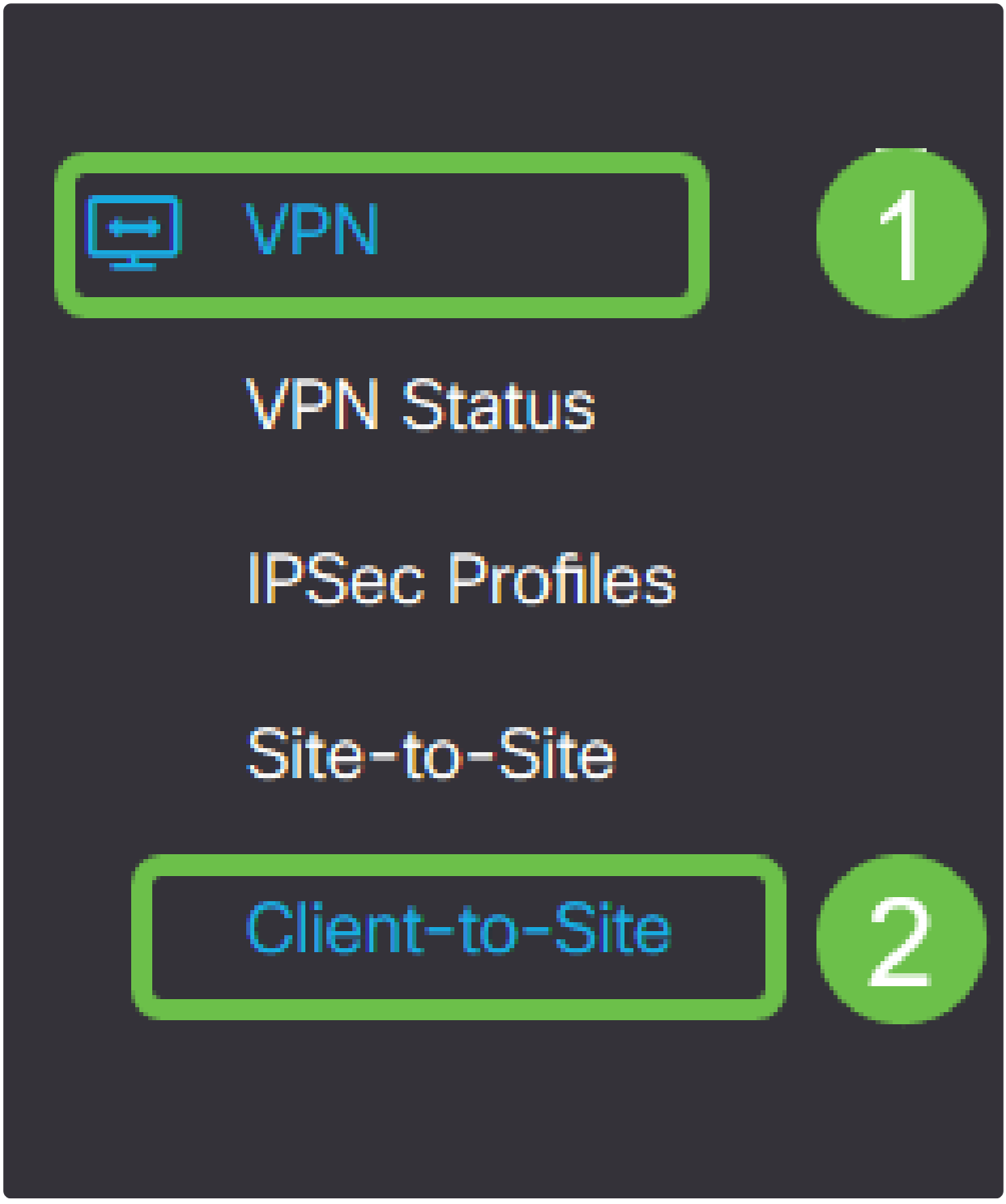
您可以在以下位置下载最新版本的Shrew Soft VPN客户端软件：https://www.shrew.net/download/vpn

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。

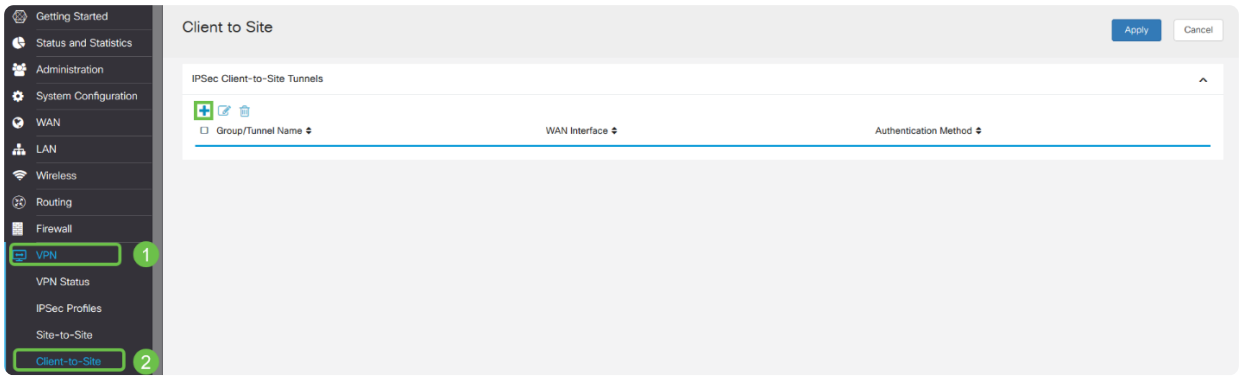
第 1 步

导航到VPN > Client-to-Site。



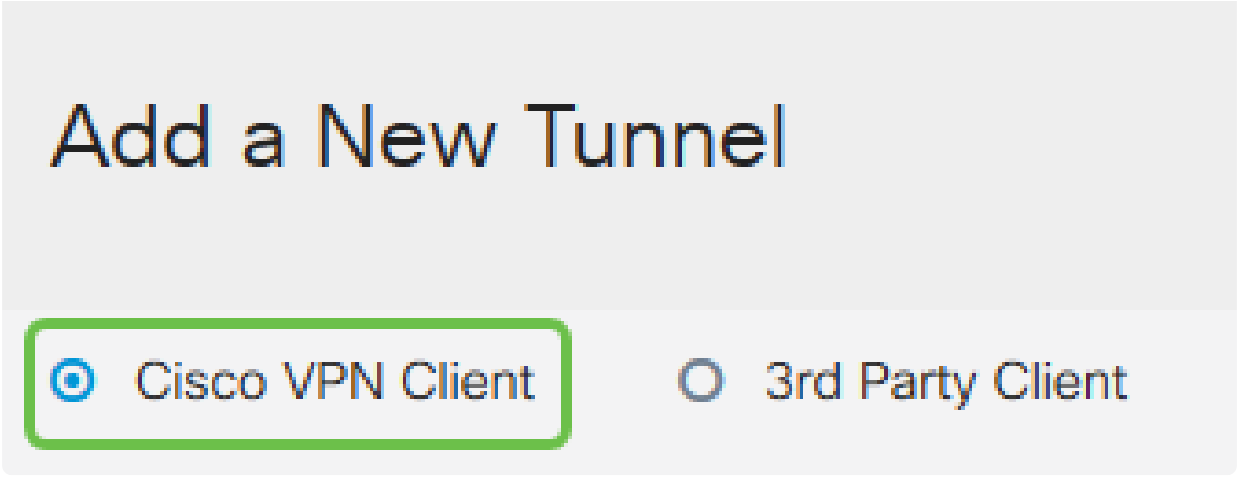
第 2 步

添加客户端到站点VPN配置文件。



第 3 步

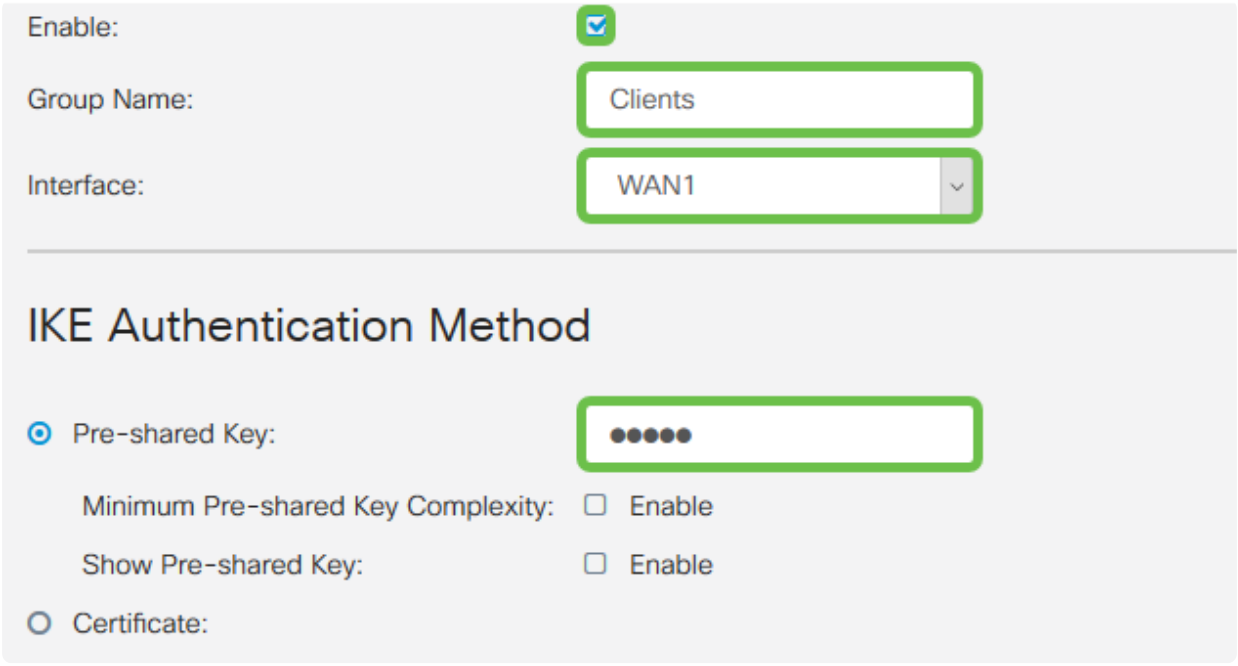
选择Cisco VPN Client选项。



第 4 步

选中Enable框以激活VPN客户端配置文件。我们还将配置Group Name，选择WAN接口，然后输入Pre-shared Key。

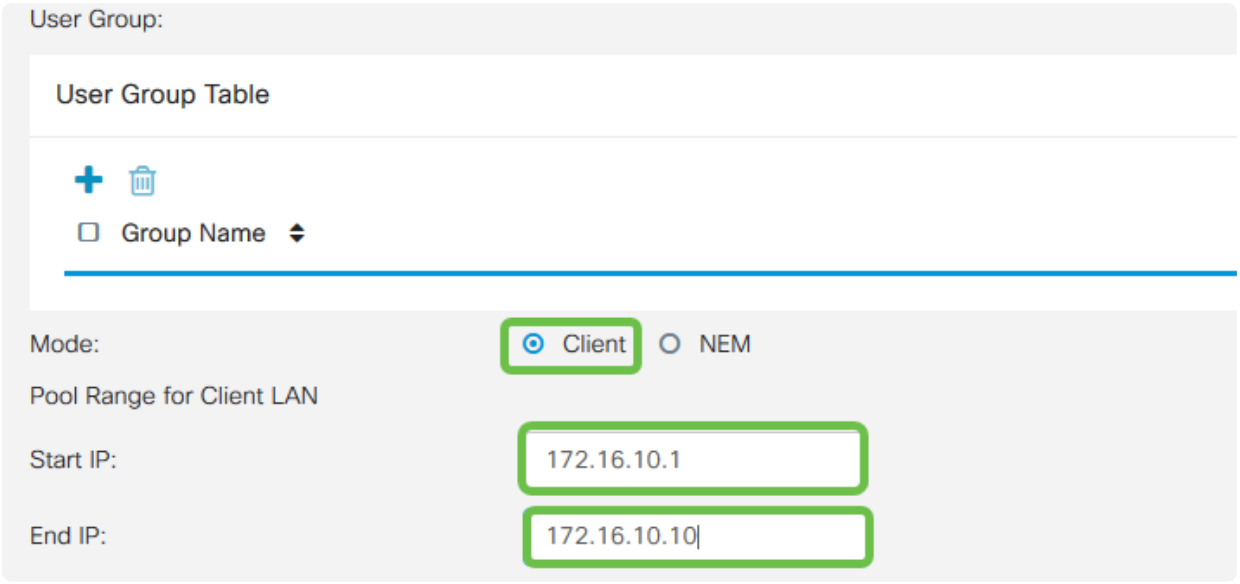
ⓘ Note: 请注意 Group Name和 Pre-shared Key，它们将在以后配置客户端时使用。



步骤 5

暂时将用户组表留空。这是用于路由器上的User Group，但我们尚未对其进行配置。确保Mode设置为Client。输入客户端LAN的池范围。我们将使用172.16.10.1到172.16.10.10。

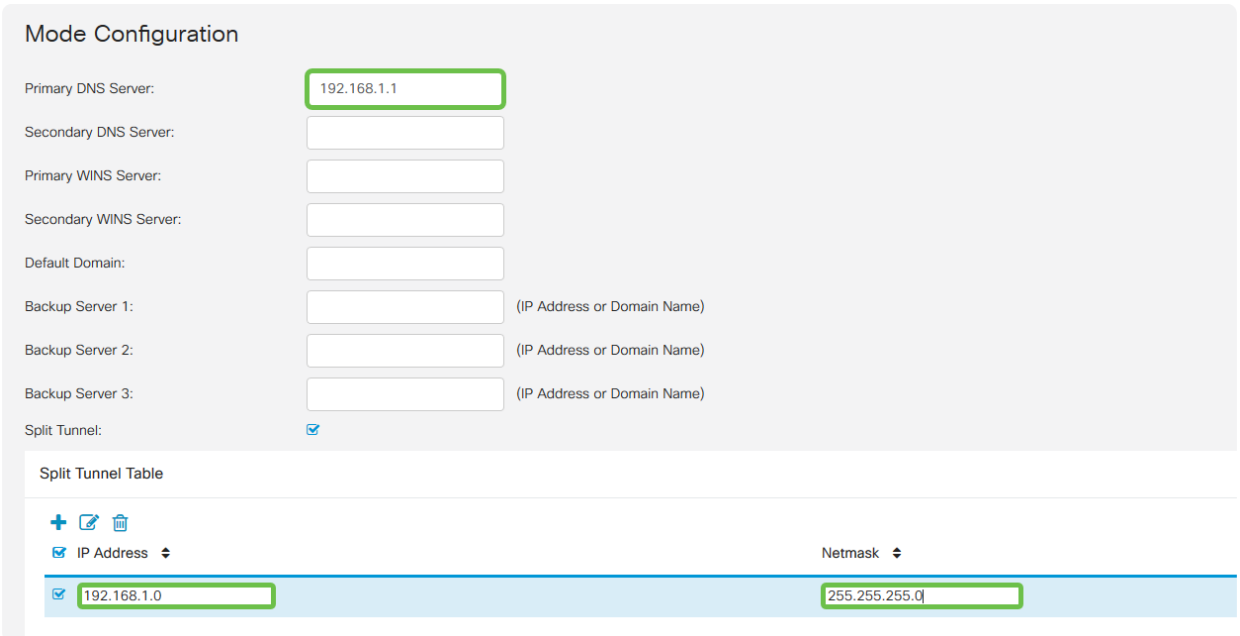
ⓘ Note: 池范围应使用网络中其它位置未使用的唯一子网。



第 6 步

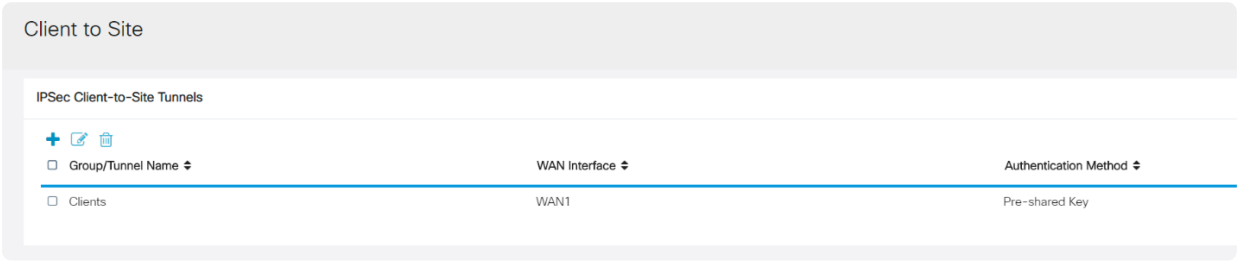
此处我们配置模式配置设置。以下是我们将使用的设置：

- 主 DNS 服务器：如果您有内部DNS服务器或想要使用外部DNS服务器，可在此处输入。否则，默认设置为RV345P LAN IP地址。在本例中，我们将使用默认值。
- 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。在本例中，我们将使用分割隧道。
- 拆分隧道表：输入VPN客户端通过VPN应有权访问的网络。本示例使用RV345P LAN网络。



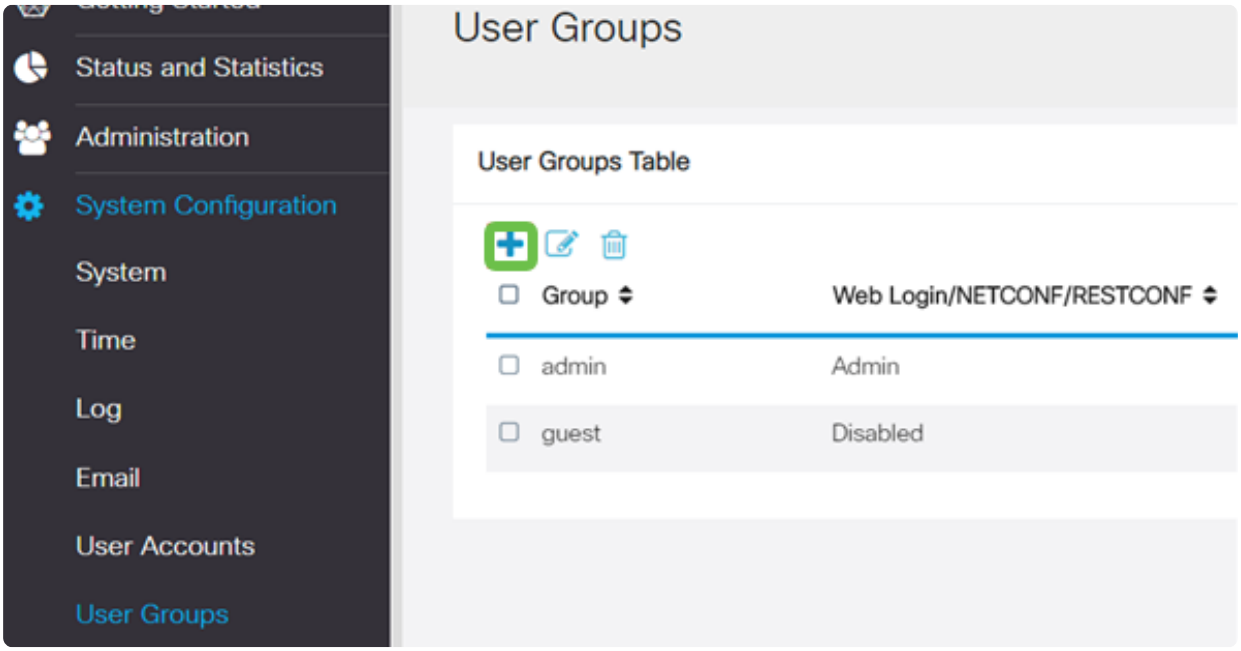
第 7 步

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



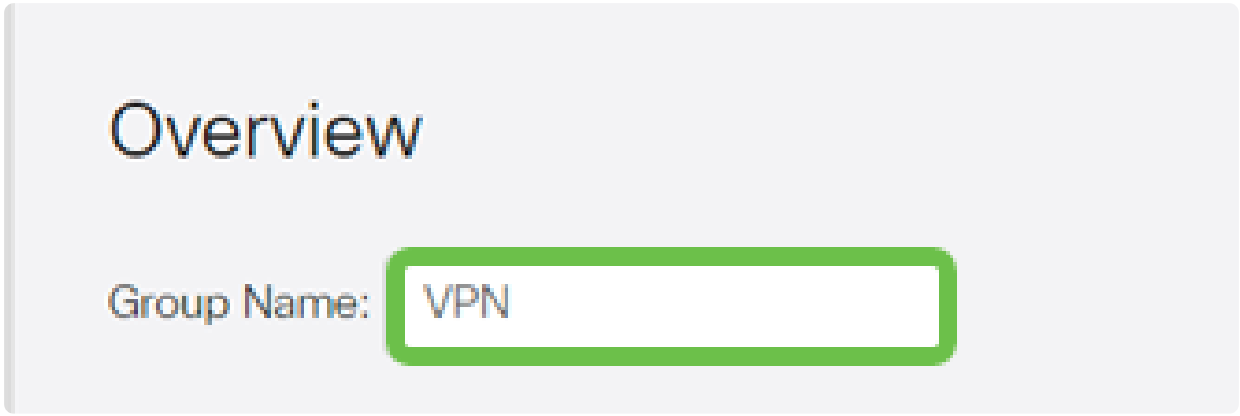
步骤 8

配置User Group以用于对VPN客户端用户进行身份验证。在System Configuration > User Groups下，点击加号图标以添加用户组。



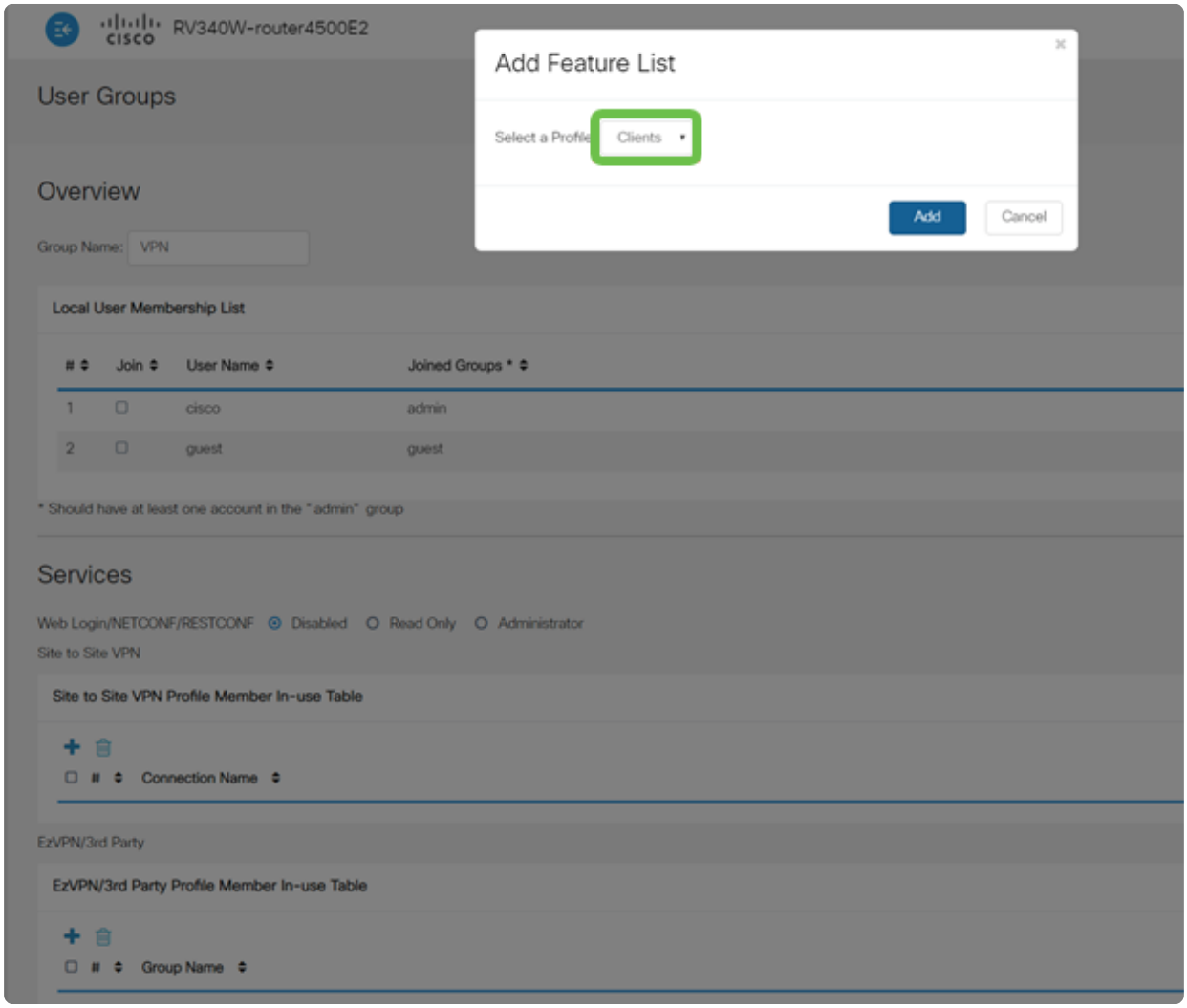
步骤 9

输入组名称。



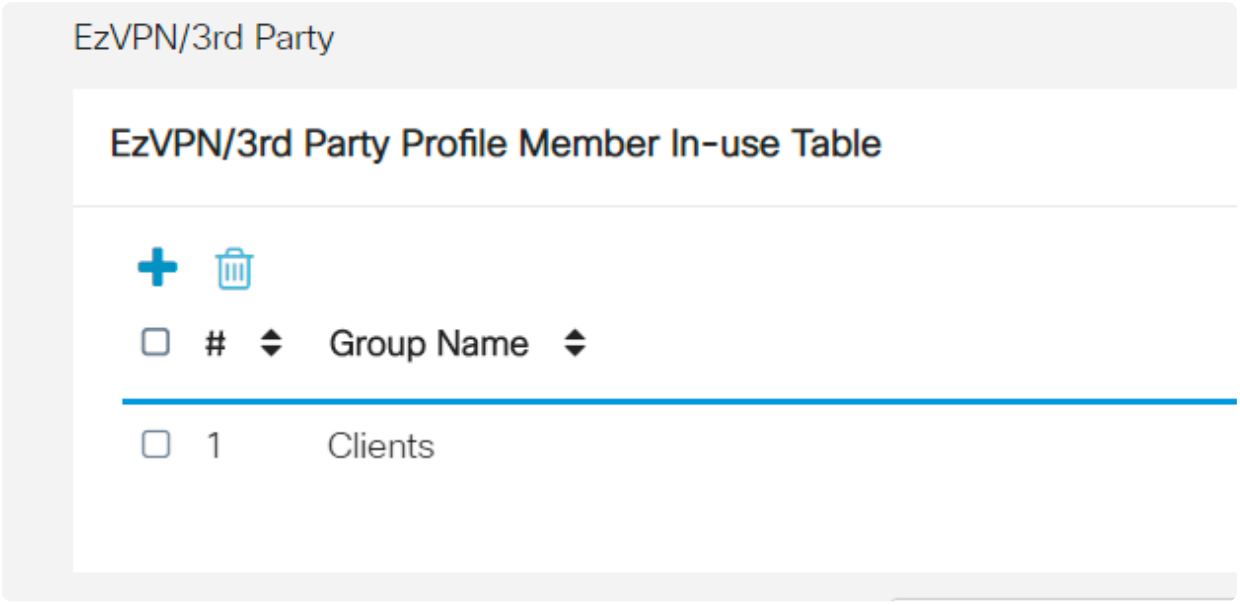
步骤 10

在Services > EzVPN/third Party下，单击Add将此用户组链接到之前配置的Client-to-Site Profile。



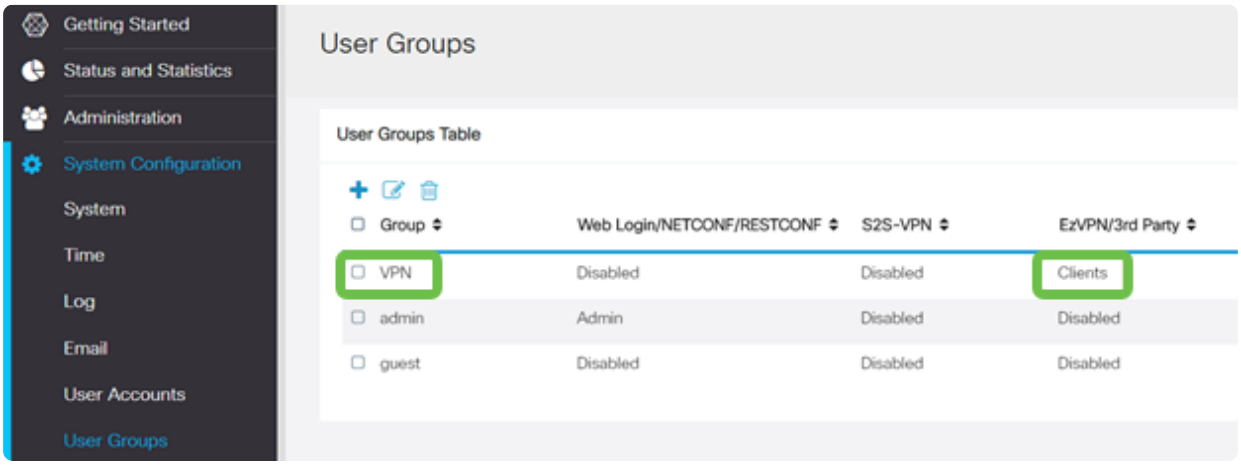
步骤 11

您现在应该会在EzVPN/第3方的列表中看到Client-to-Site Group Name。



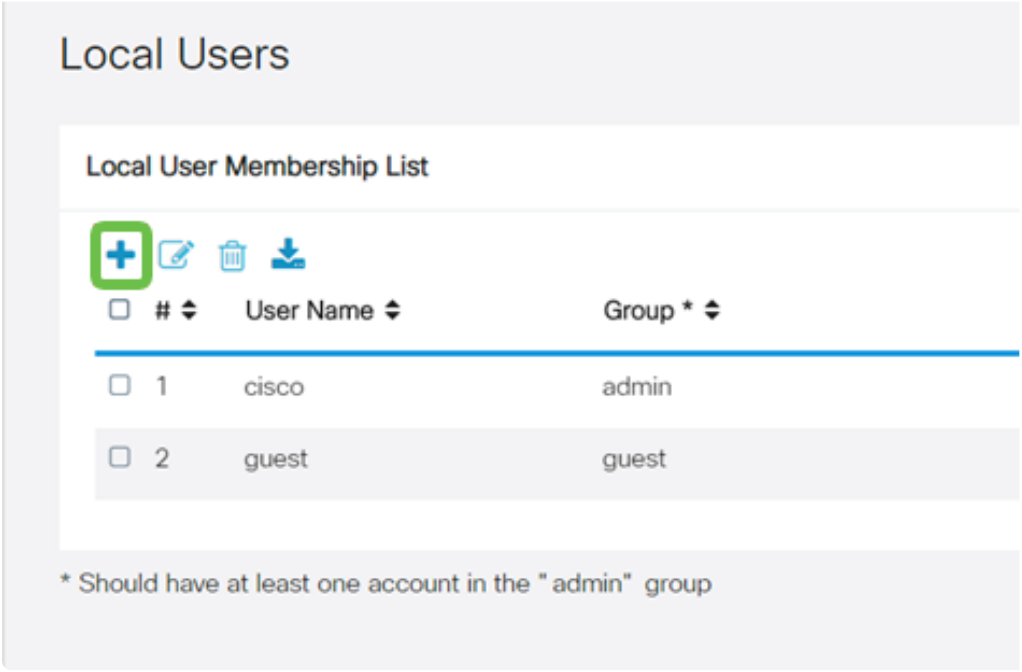
步骤 12

在Apply用户组配置后，您将在User Groups列表中看到该用户组，并显示新用户组将与之前创建的客户端到站点配置文件一起使用。



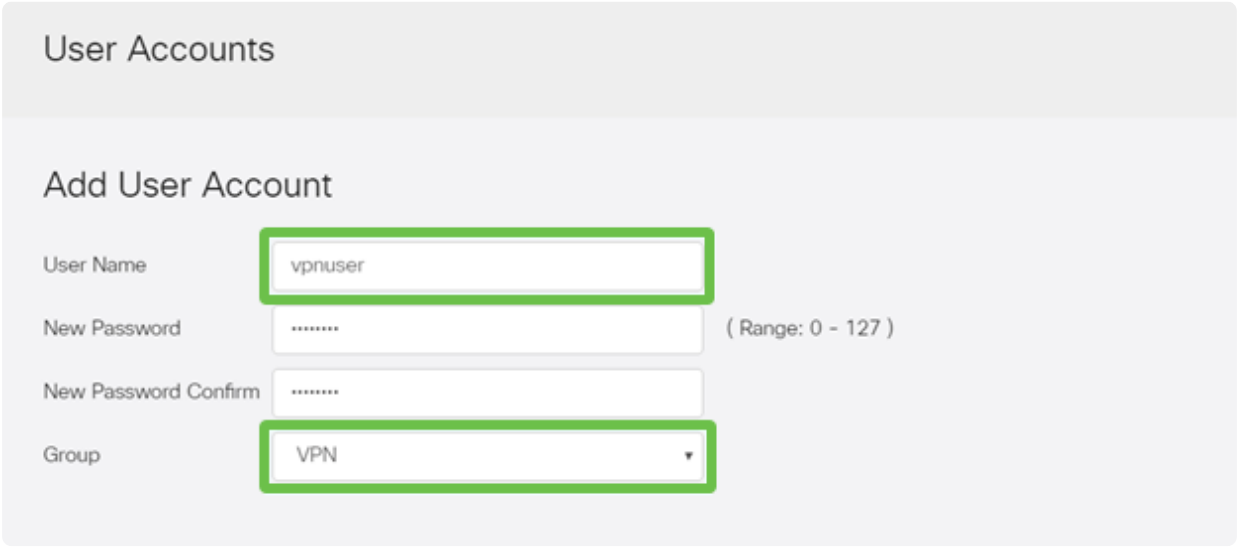
步骤 13

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



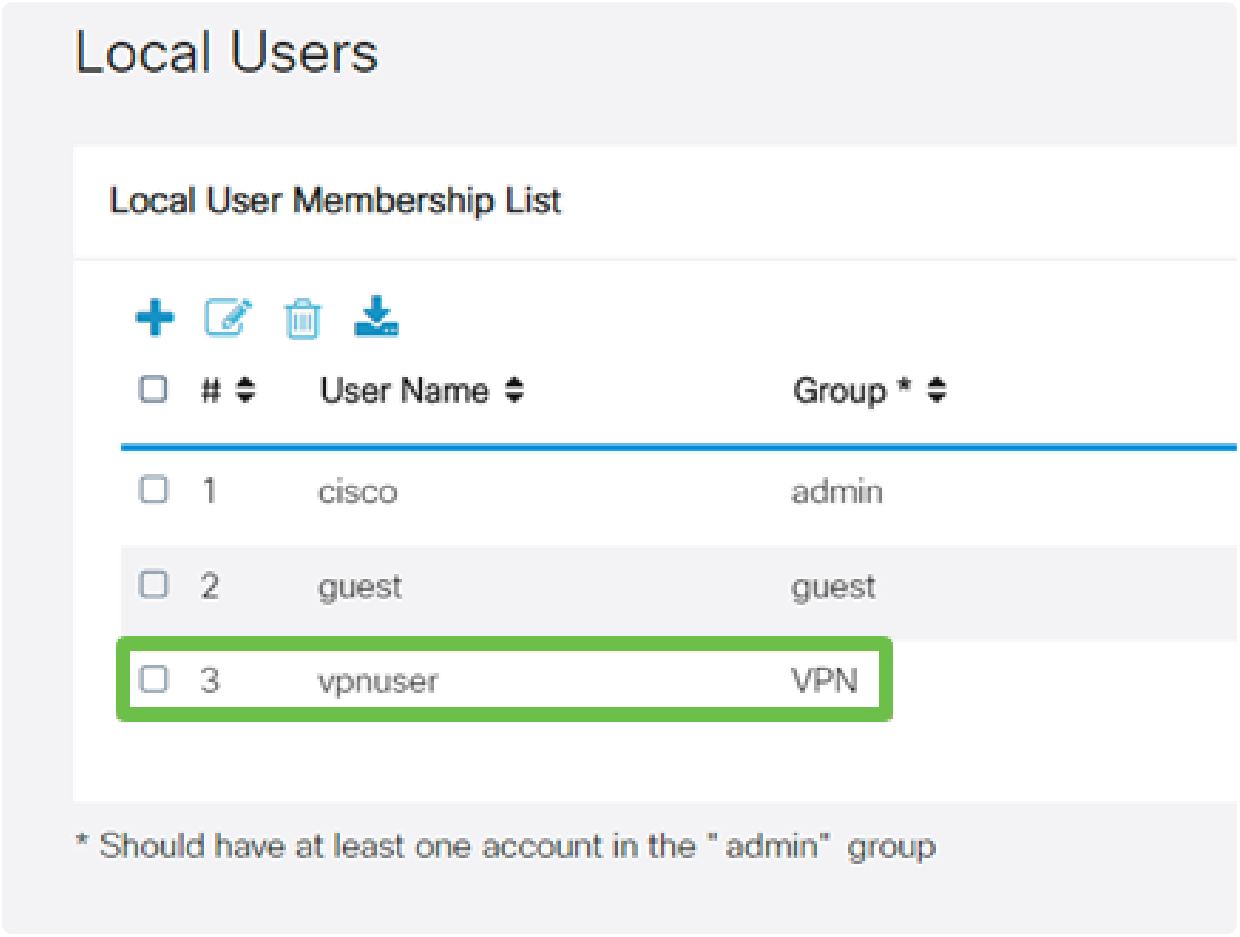
步骤 14

输入新的用户名和新密码。验证Group已设置为您刚才配置的新用户组。完成后单击Apply。



步骤 15

新用户将显示在本地用户列表中。



RV345P系列路由器的配置到此结束。接下来，您将配置Shrew Soft VPN客户端。

配置Shrew Soft VPN客户端

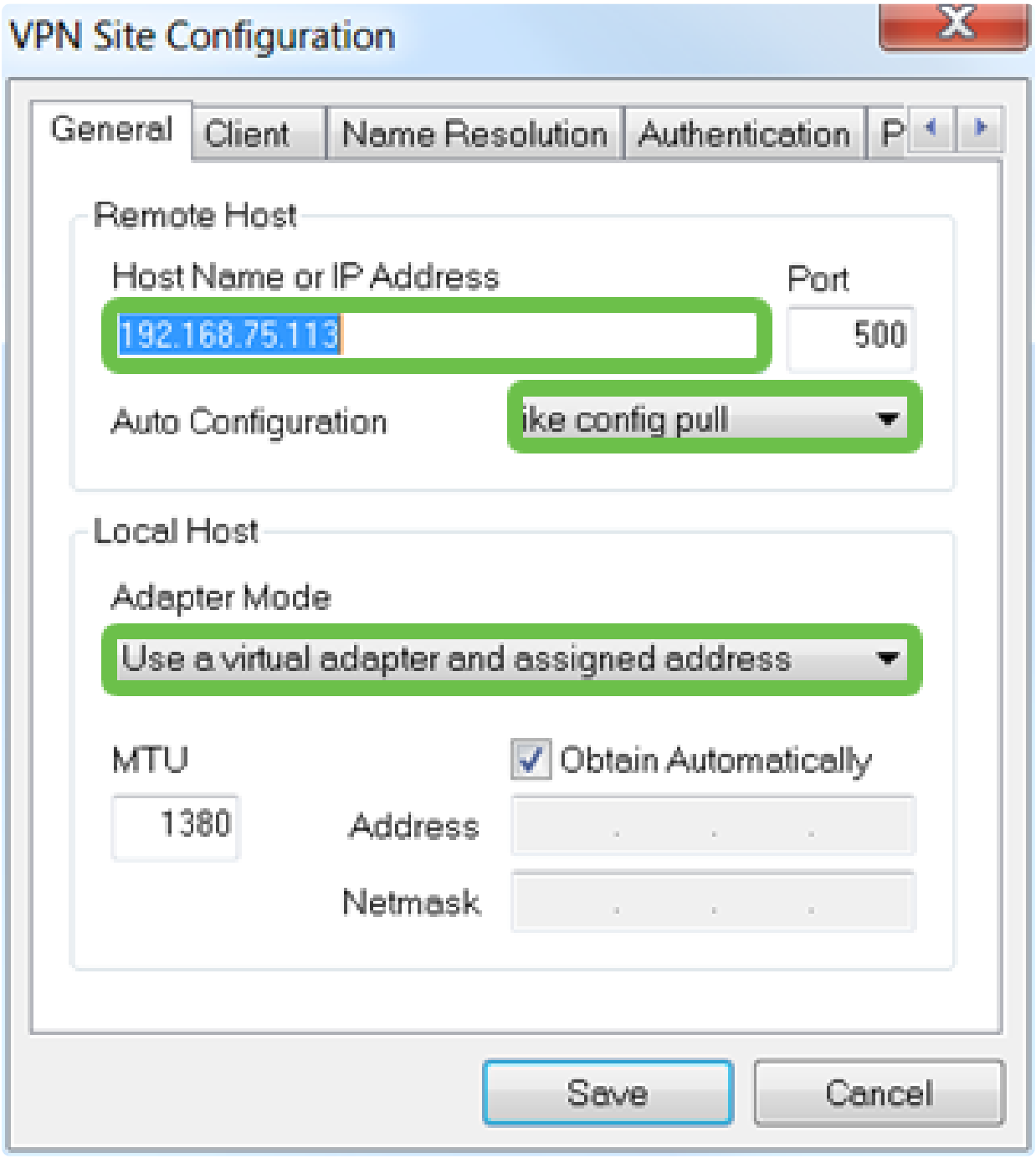
请执行以下步骤。

第 1 步

打开Shrew Soft VPN Access Manager，然后单击Add以添加配置文件。在出现的VPN Site Configuration窗口中，配置General选项卡：

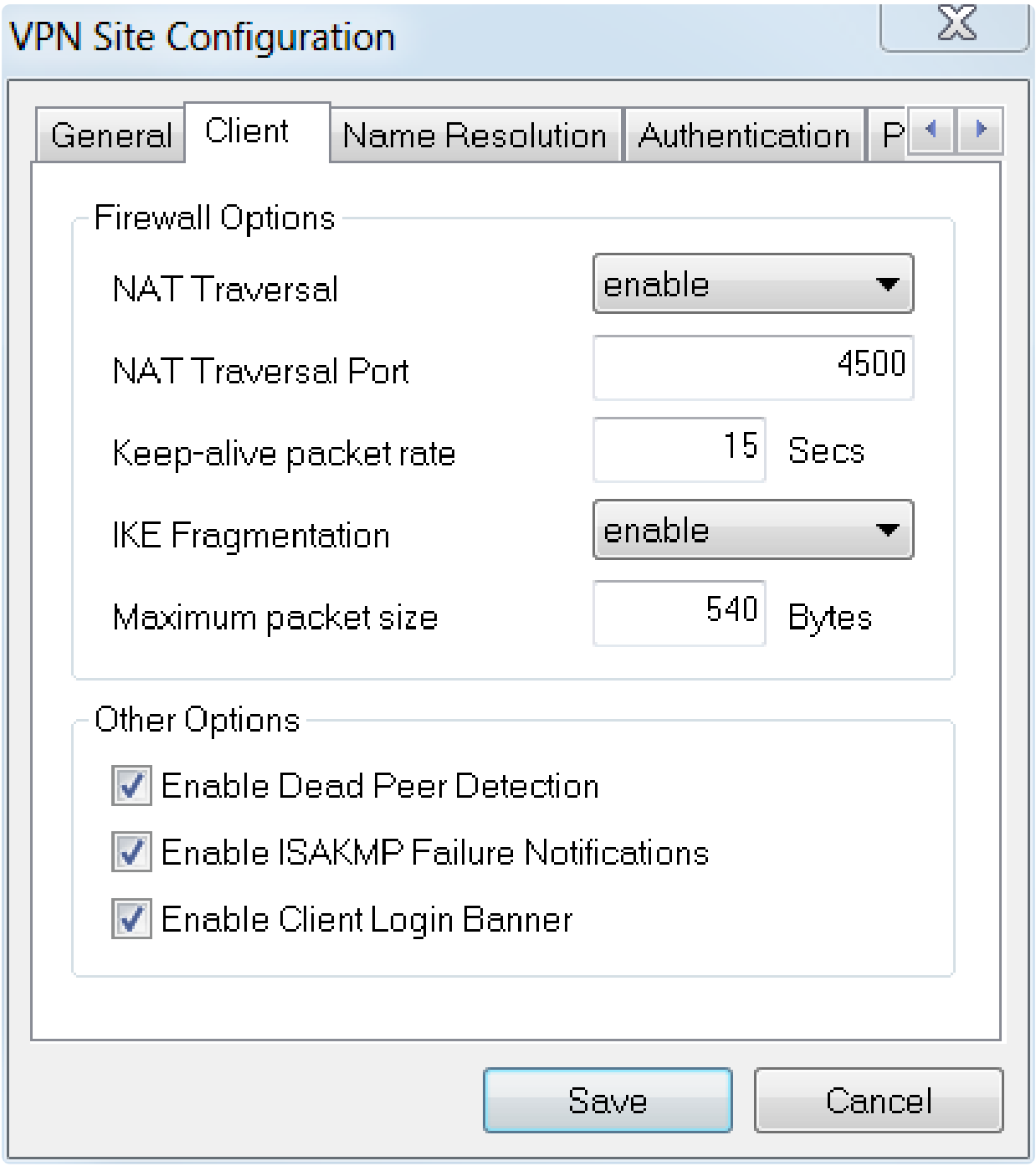
- 主机名或 IP 地址:使用WAN IP地址（或RV345P的主机名）
- 自动配置:选择ike config pull

- 适配器模式：选择使用虚拟适配器和分配的地址



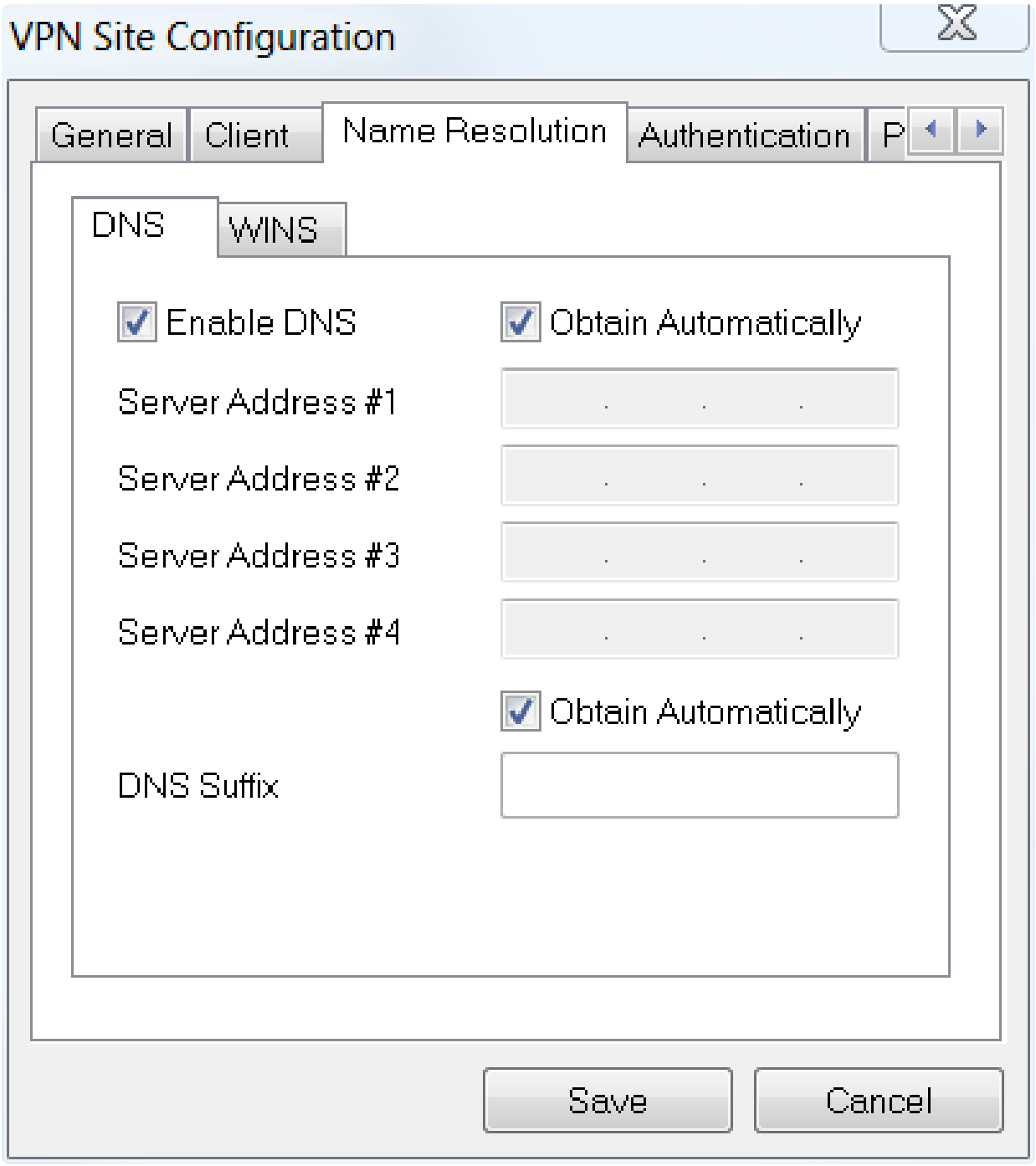
第 2 步

配置Client选项卡。在本例中，我们保留了默认设置。



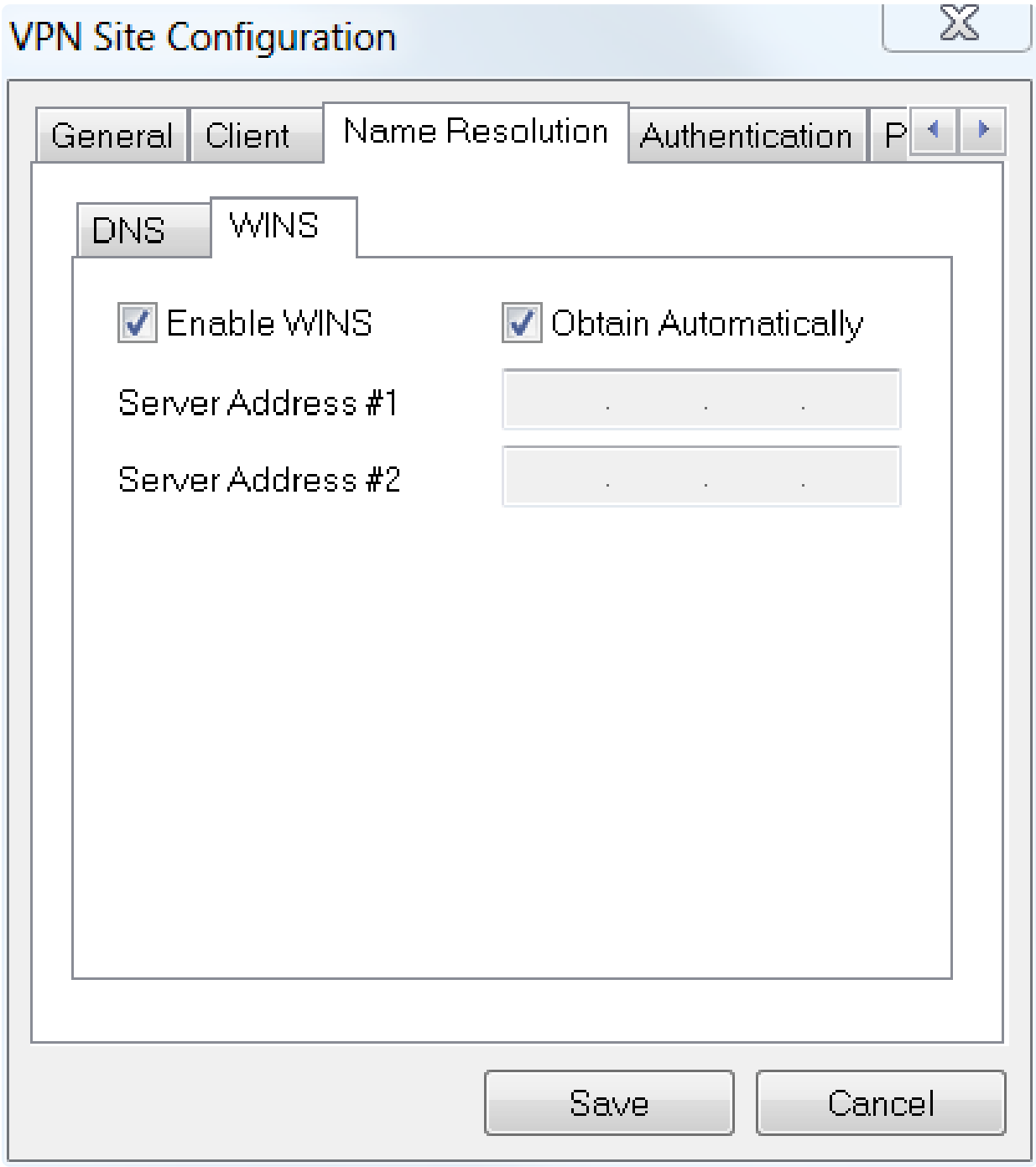
第 3 步

在Name Resolution > DNS下，选中Enable DNS框，并选中Obtain Automatically框。



第 4 步

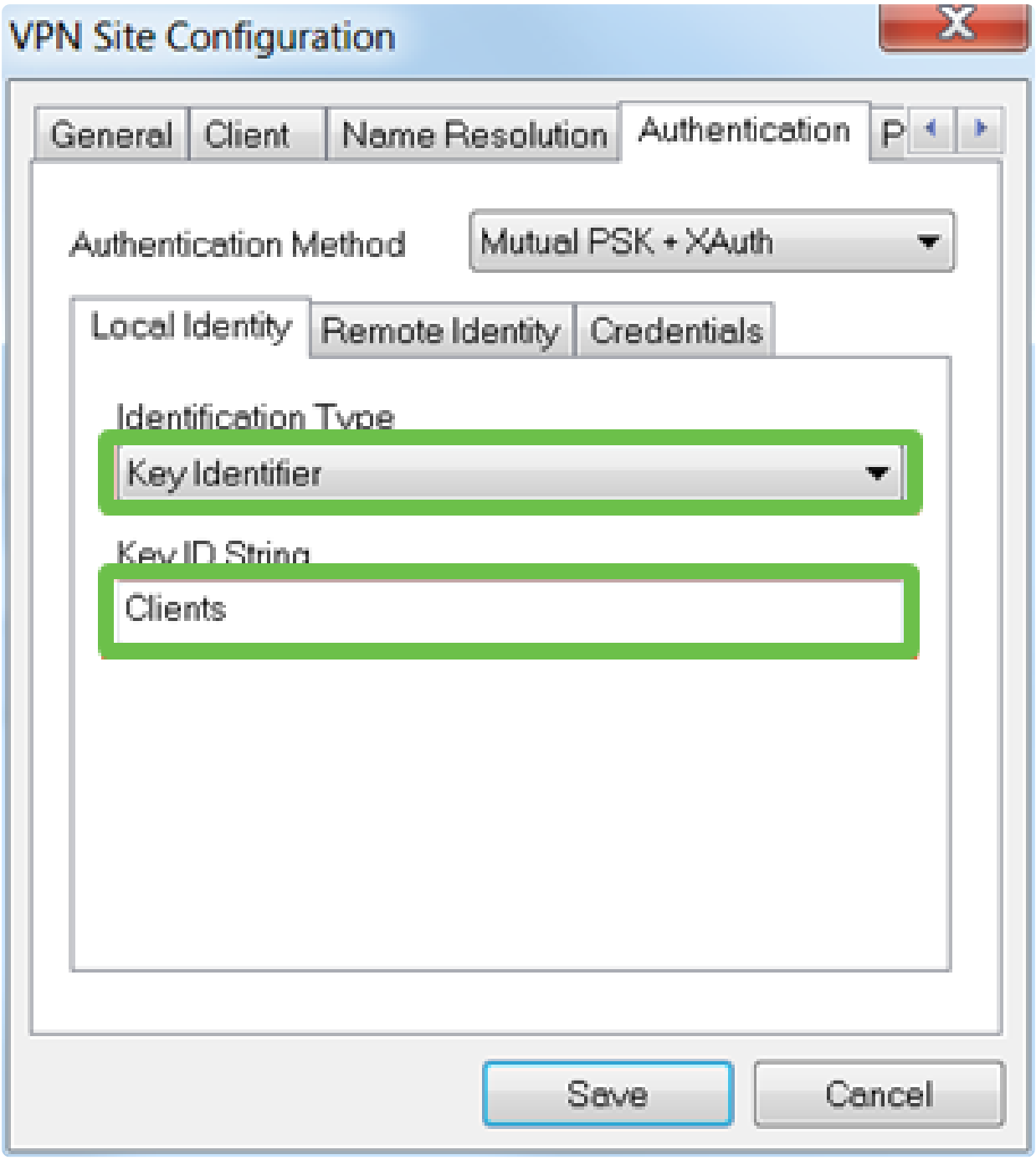
在Name Resolution > WINS选项卡下，选中Enable WINS框，并使Obtain Automatically框保持选中状态。



步骤 5

单击Authentication > Local Identity。

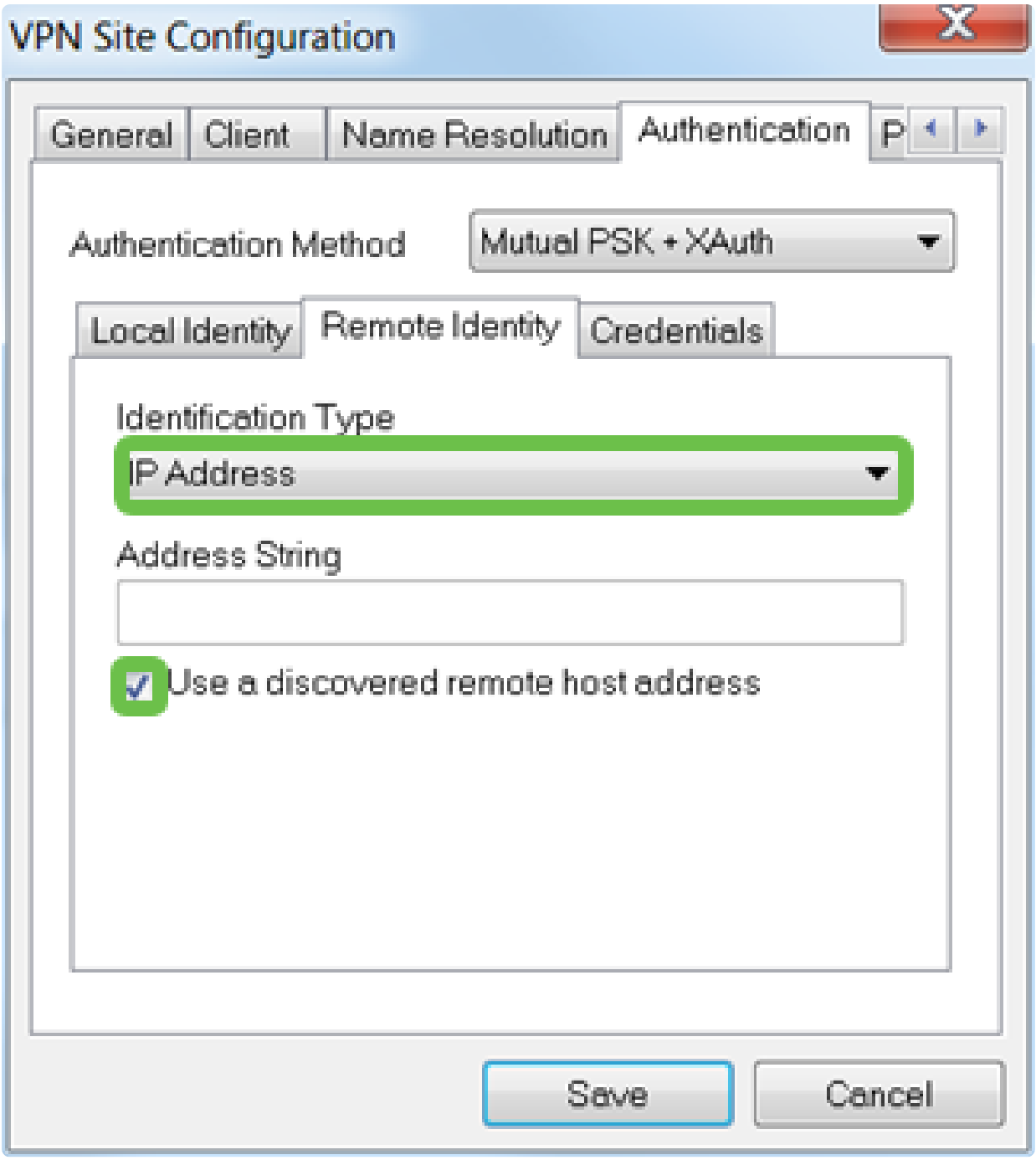
- 标识类型:选择密钥标识符
- 密钥ID字符串:输入在RV345P上配置的Group Name



第 6 步

在身份验证>远程身份下。在本例中，我们保留了默认设置。

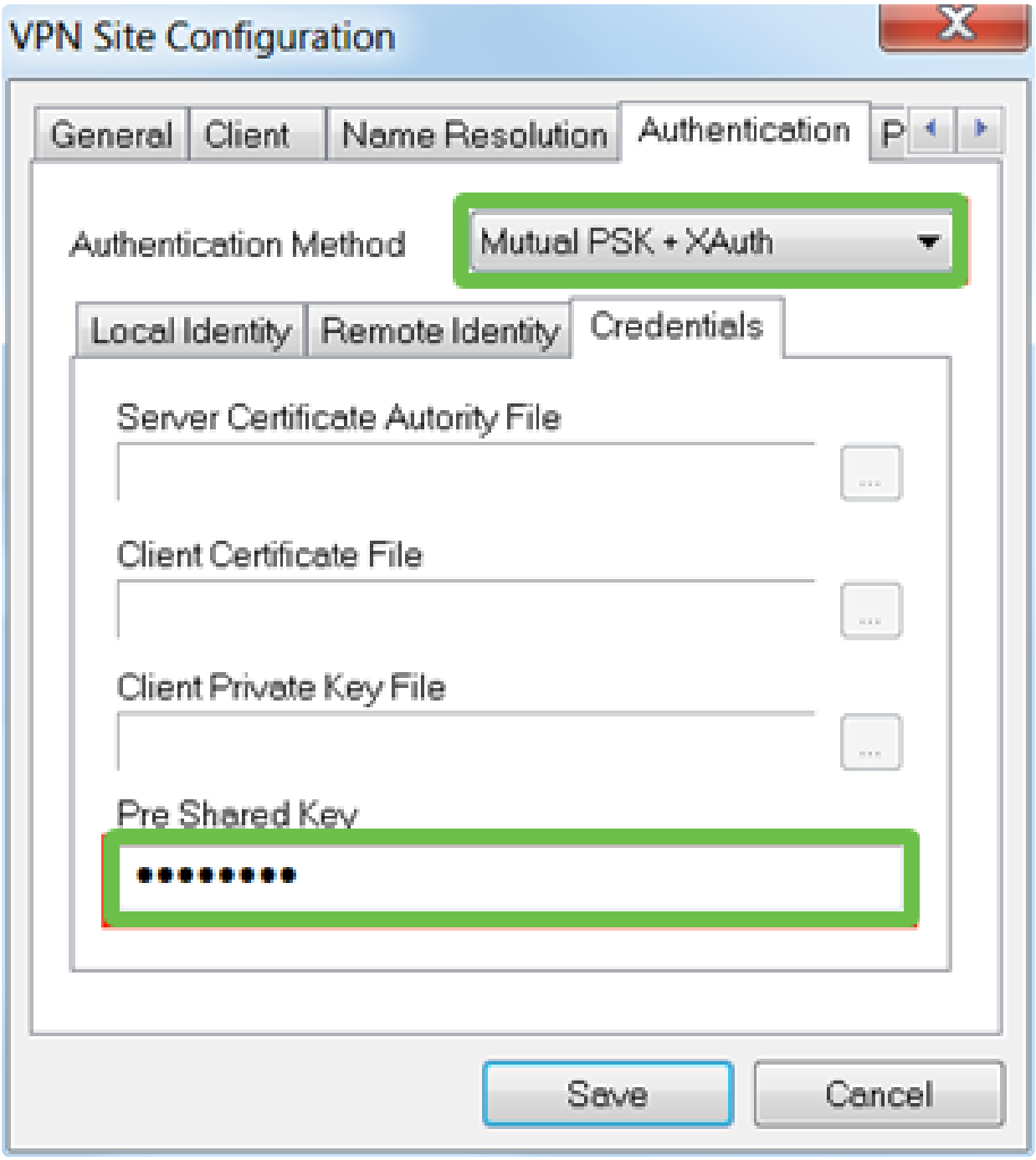
- 标识类型:IP Address
- 地址字符串:<blank>
- 使用发现的远程主机地址框：已选中



第 7 步

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

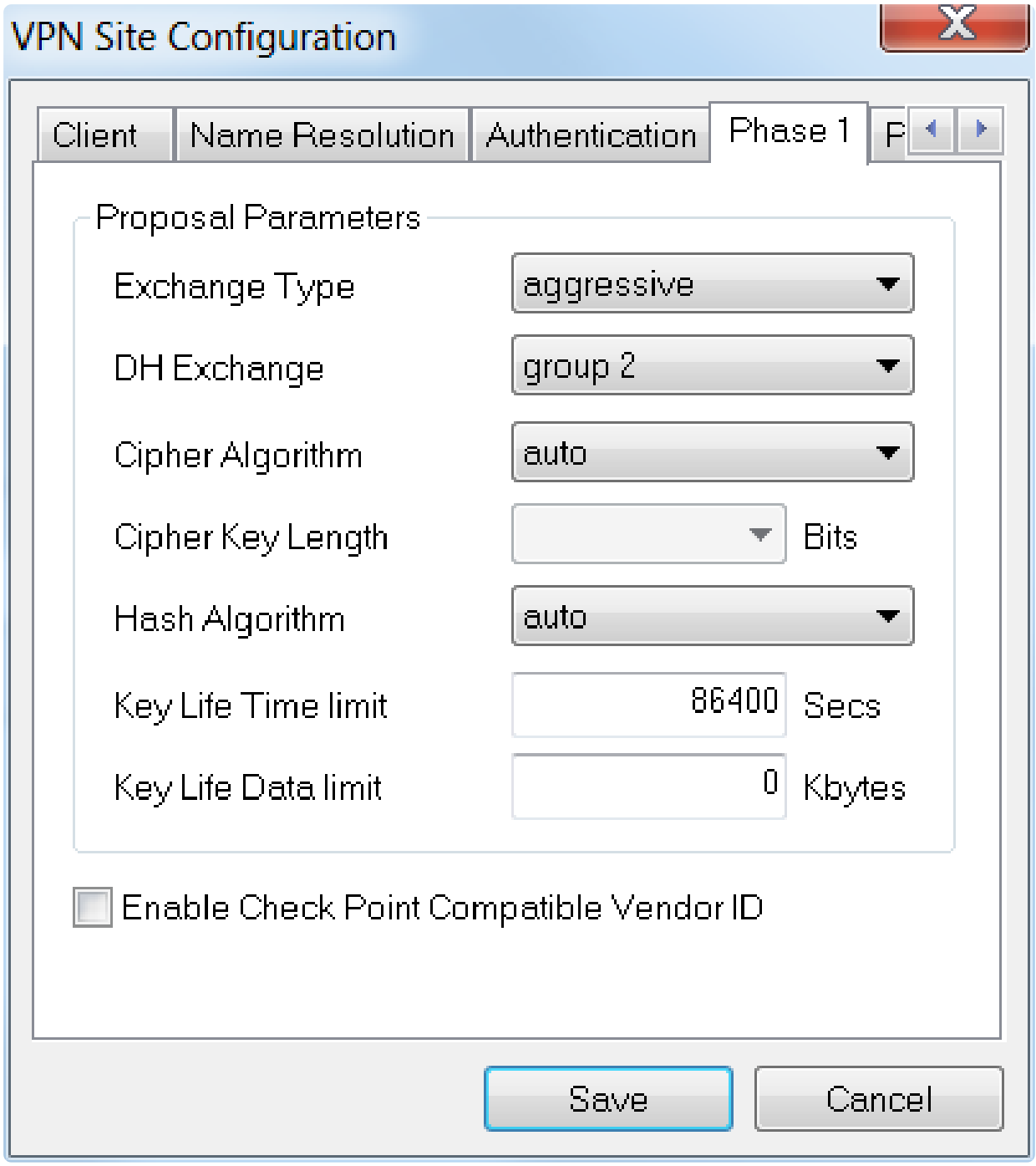
- 认证方法:选择Mutual PSK + XAuth
- 预共享密钥:输入在RV345P客户端配置文件中配置的预共享密钥



步骤 8

用于Phase 1选项卡。在本示例中，保留了默认设置：

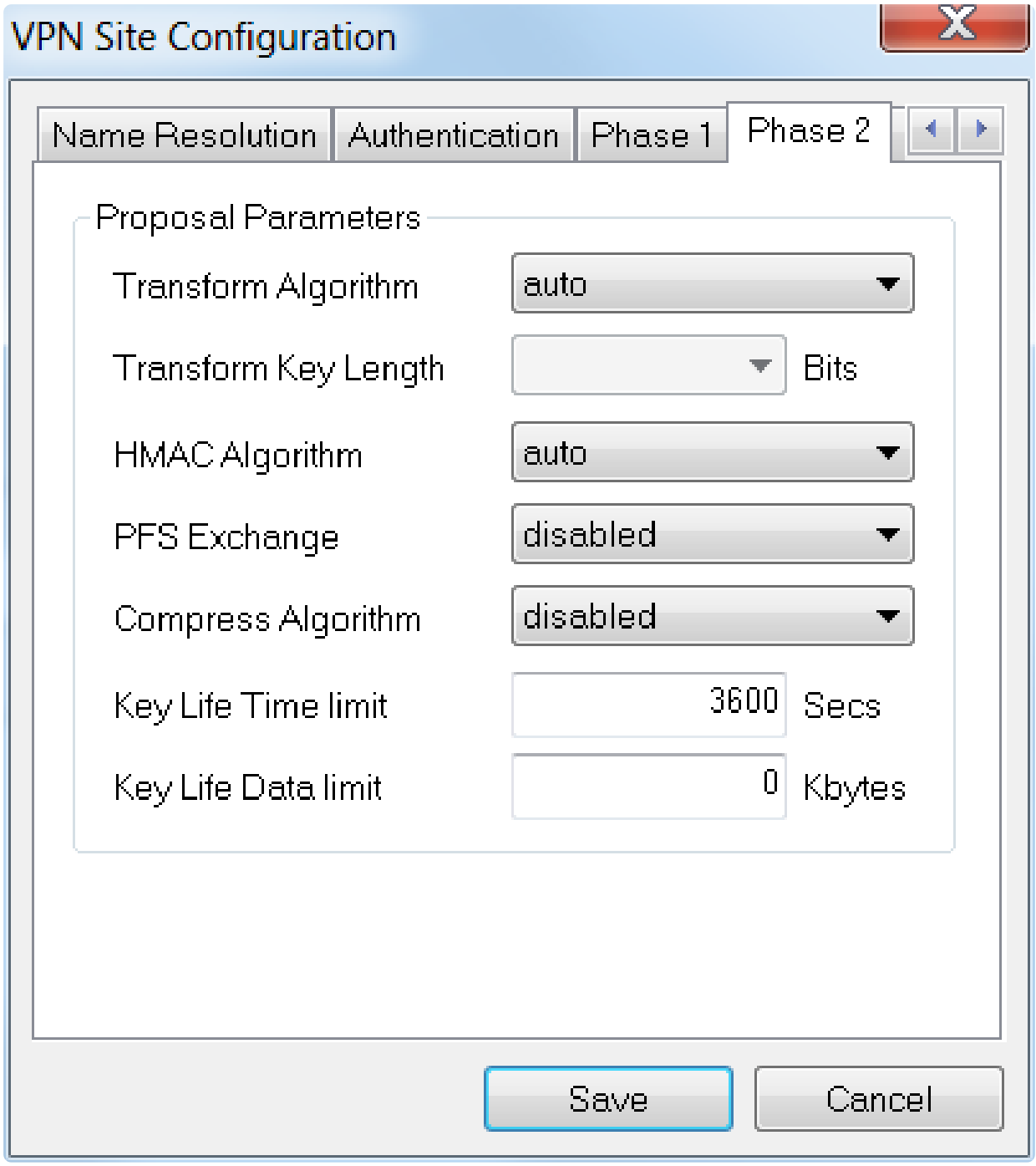
- Exchange类型：激进
- DH交换：组2
- 密码算法：自动
- 散列算法：自动



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 Exchange：已禁用
- 压缩算法：已禁用

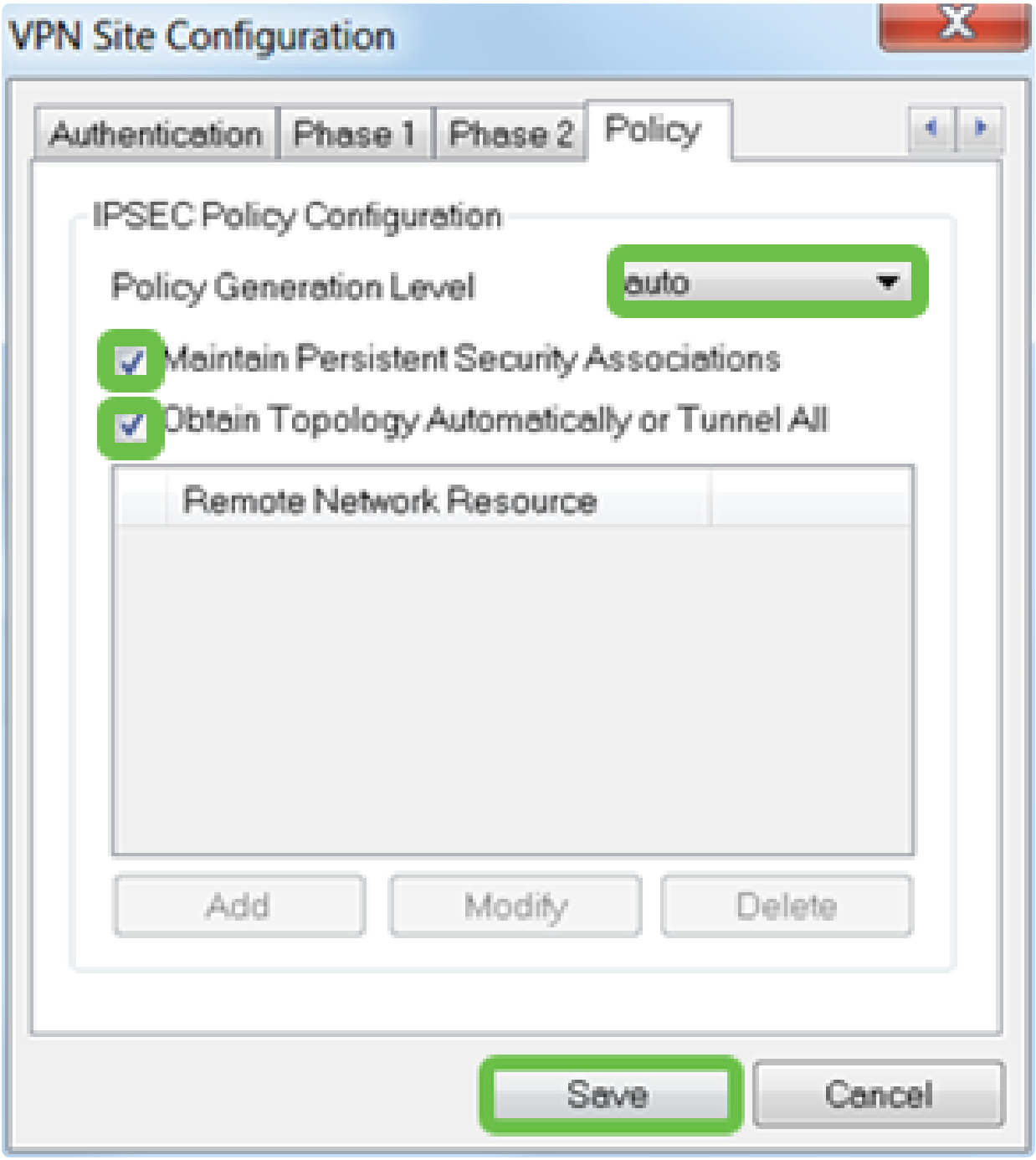


步骤 10

对于Policy选项卡示例，我们使用以下设置：

- 策略生成级别：自动
- 维护持久安全关联：已选中
- 自动获取拓扑或全部建立隧道：已选中

由于我们在RV345P上配置了Split-Tunneling，因此不需要在此处进行配置。

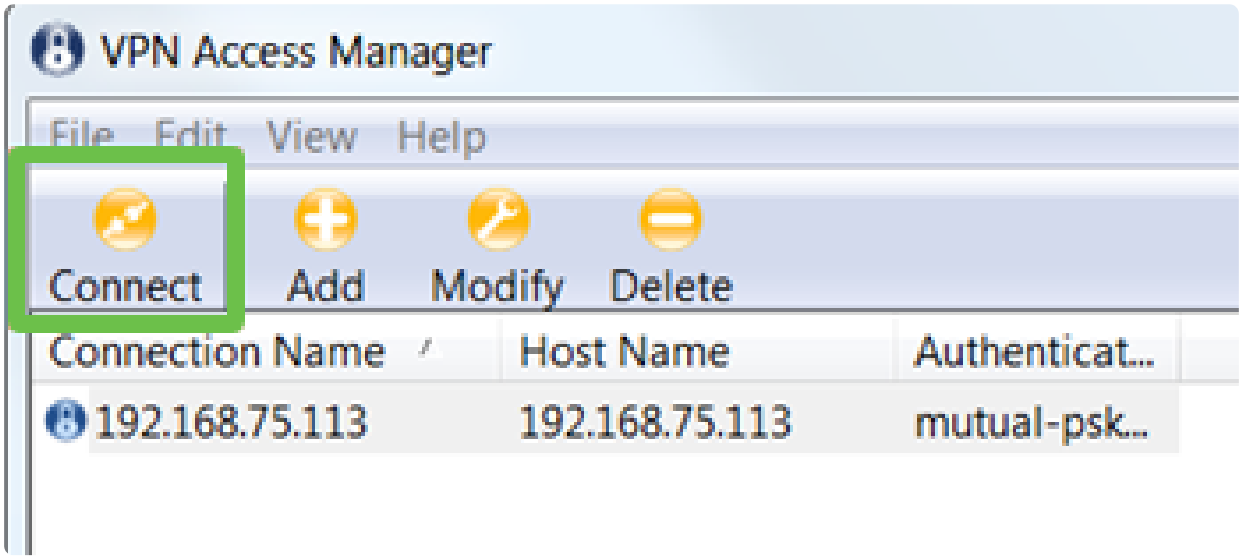


完成后，单击 Save（保存）。

步骤 11

现在已准备好测试连接。在VPN Access Manager中，突出显示连接配置文件，然后单

击Connect按钮。



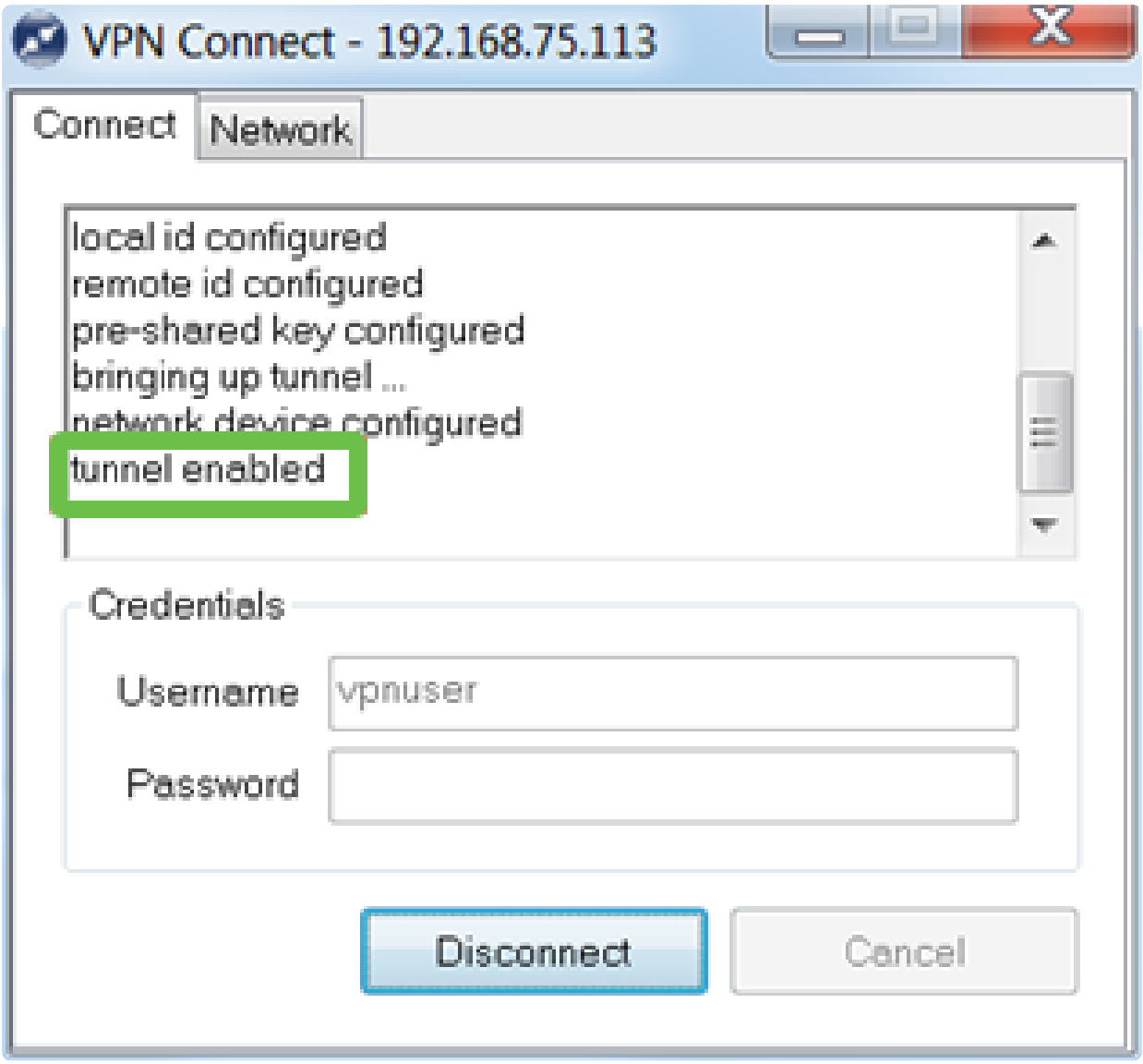
步骤 12

在出现的VPN　Connect窗口中，使用您在RV345P上创建的User　Account的凭证输入Username和Password（步骤13和14）。 完成后，单击Connect。



步骤 13

检验隧道是否已连接。您应该看到隧道已启用。



ⓘ Note: 在此配置中以Shrew Soft为例。由于Shrew Soft不是思科产品，如果您需要技术支持，请联系此第三方。

其他VPN选项

也可选择使用VPN。有关详细信息，请点击以下链接：

- 使用GreenBow VPN客户端与RV34x系列路由器连接
- 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系列路由器上配置互联网协议安全(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）

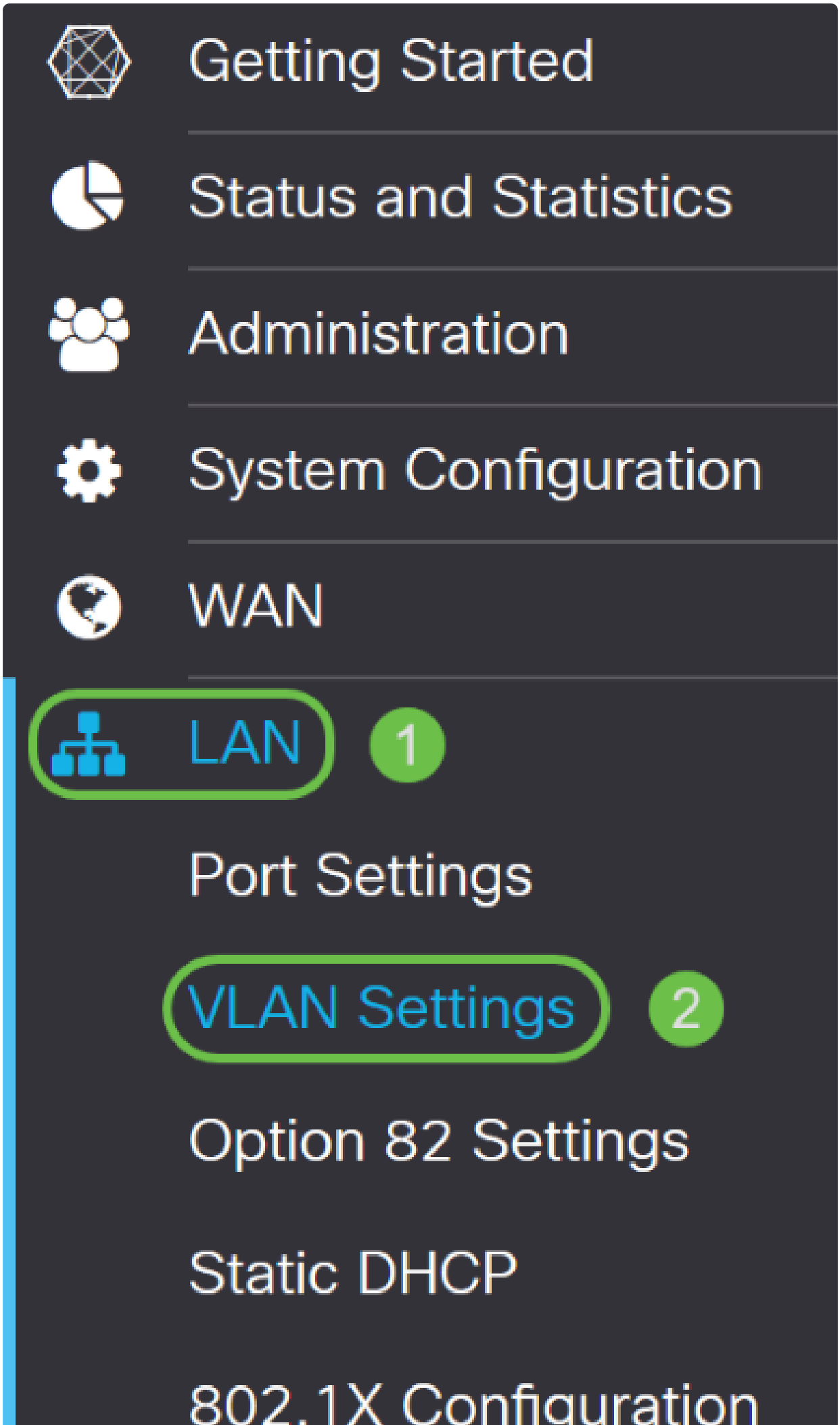
利用虚拟局域网（VLAN），您可以将局域网（LAN）逻辑划分为不同的广播域。在敏感数据可能会在网络中广播的情况下，可以创建 VLAN 以通过指定广播到特定 VLAN 来增强安全性。利用 VLAN，还可在一定程度上免于将广播和组播发送到不必要的目标，从而提高性能。您可以创建VLAN，但只有将VLAN手动或动态地连接到至少一个端口后，此操作才有效。端口必须始终属于一个或多个VLAN。

您可能希望参考VLAN最佳实践和安全提示以获取其他指导。

如果您不想创建VLAN，可以跳到下一节。

第 1 步

导航到LAN > VLAN Settings。


Getting Started
Status and Statistics
Administration
System Configuration
WAN
LAN
1
Port Settings
VLAN Settings
2
Option 82 Settings
Static DHCP
802.1X Configuration

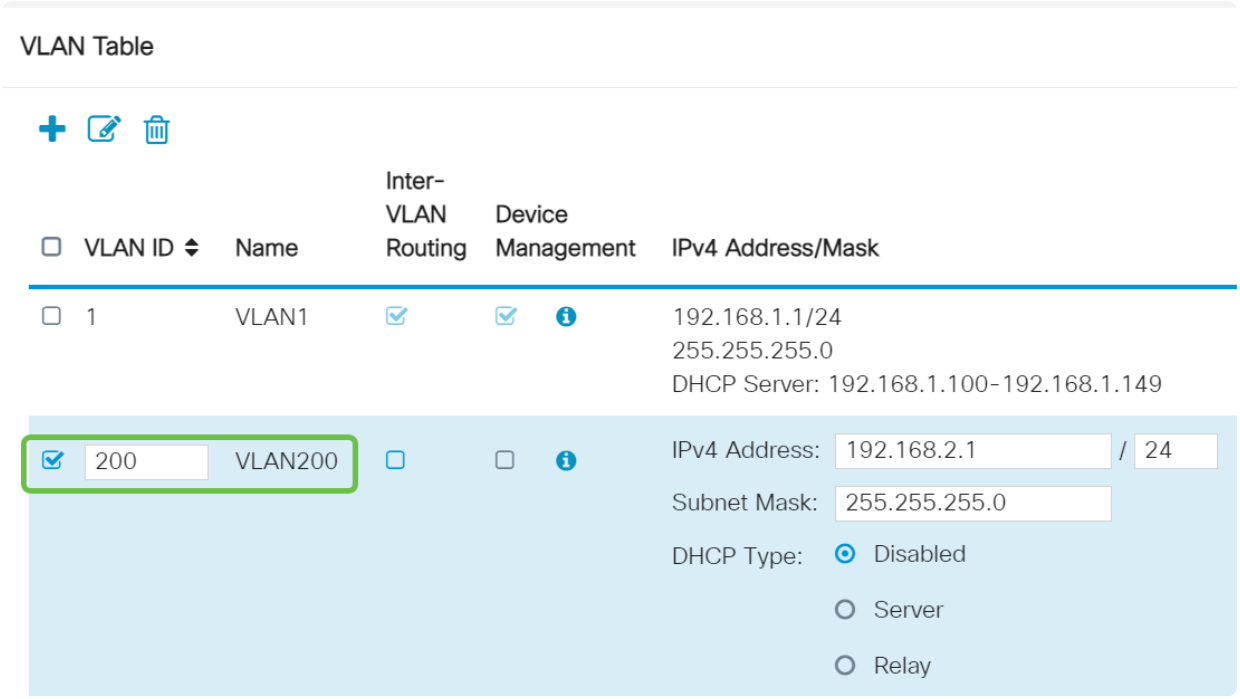
第 2 步

单击add图标以创建新的VLAN。



第 3 步

输入您要创建的VLAN ID和名称。VLAN ID的范围为1-4093。



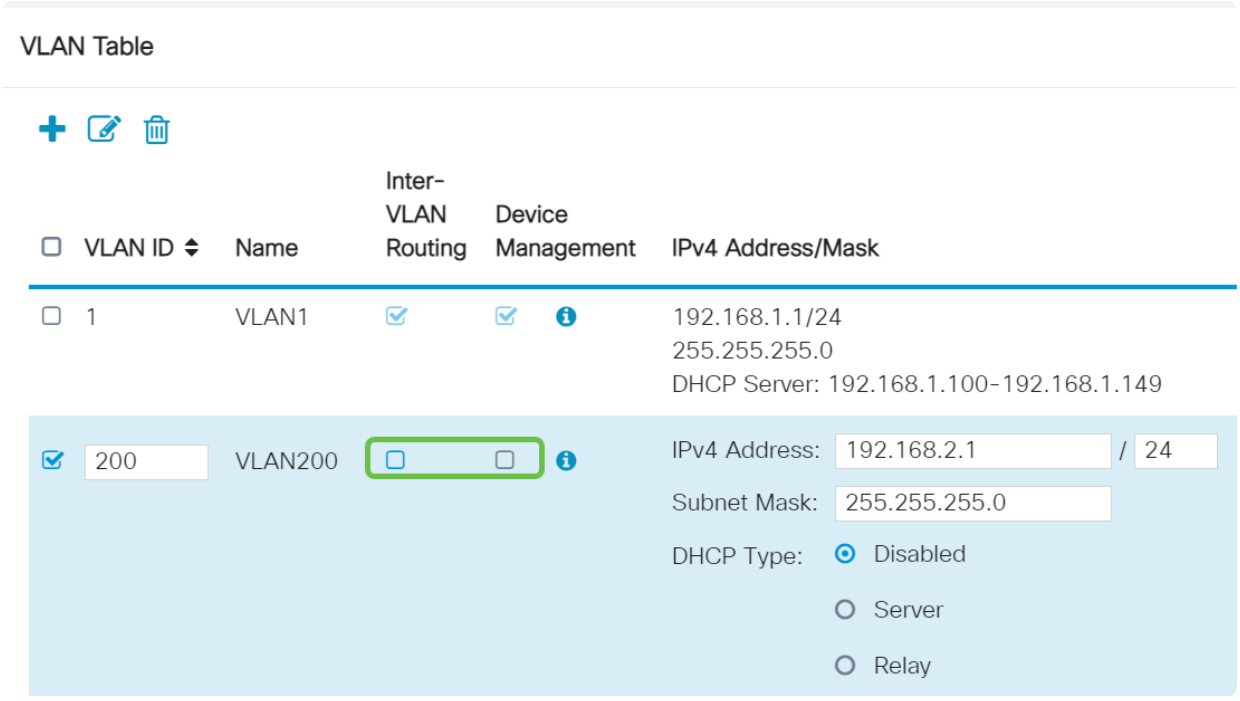
第 4 步

如果需要，请取消选中Inter-VLAN　Routing和Device　Management的Enabled复选框。VLAN间路由用于将数据包从一个VLAN路由到另一个VLAN。

通常，不建议对访客网络执行此操作，因为您将要隔离访客用户，这会导致VLAN安全性降低。有时VLAN可能需要在彼此之间路由。如果出现这种情况，请在具有目标ACL限制的RV34x路由器上查看VLAN间路由，以配置您允许的VLAN之间的特定流量。

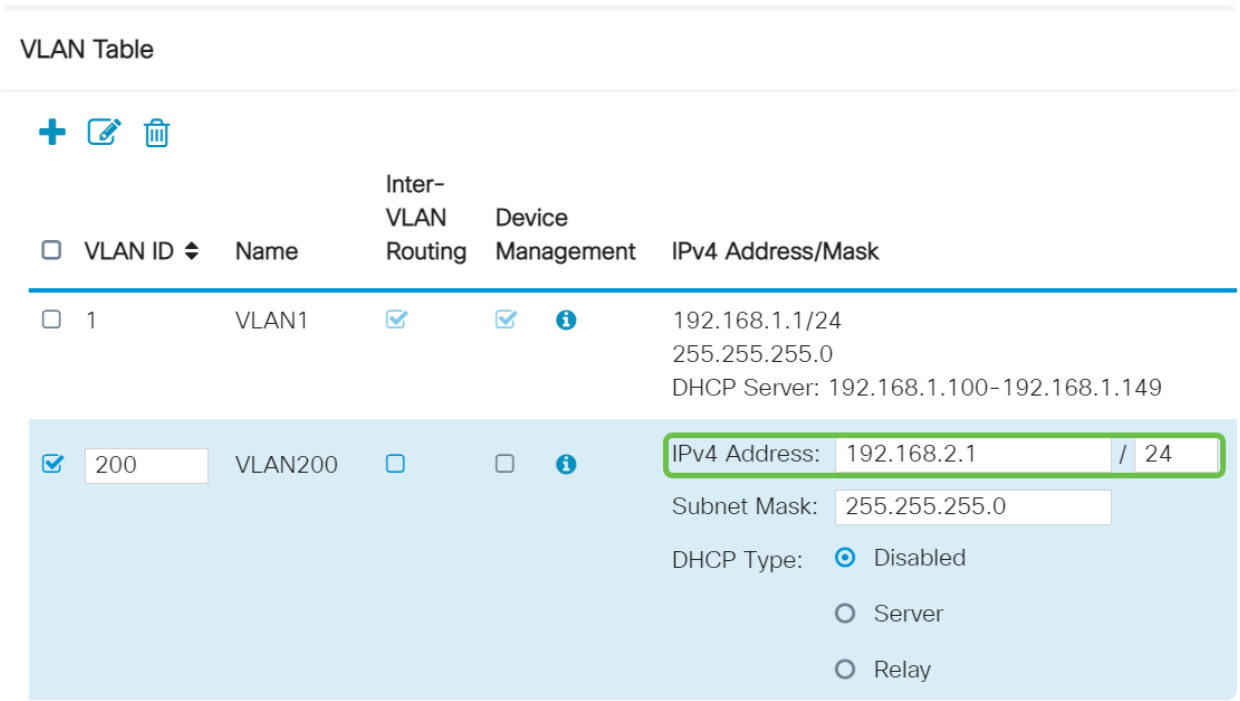
Device　Management软件允许您使用浏览器从VLAN登录到RV345P的Web　UI并管理RV345P。这也应在访客网络上禁用。

在本例中，我们未启用VLAN间路由或设备管理以确保VLAN更安全。



步骤 5

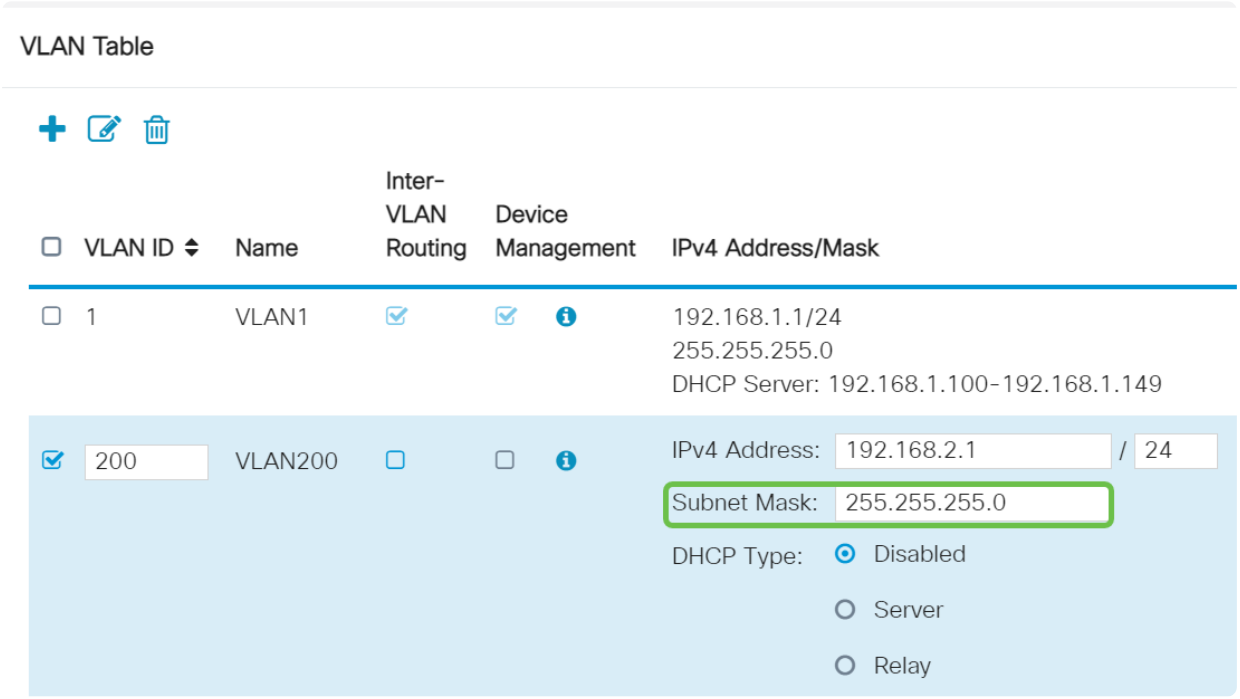
私有IPv4地址将自动填入IP Address字段。如果您选择，可以调整此值。在本示例中，子网有192.168.2.100-192.168.2.149可用于DHCP的IP地址。192.168.2.1-192.168.2.99和192.168.2.150-192.168.2.254可用于静态IP地址。



第 6 步

Subnet Mask下的子网掩码将自动填充。如果您进行更改，将自动调整该字段。

在本演示中，我们将保留子网掩码为255.255.255.0或/24。



第 7 步

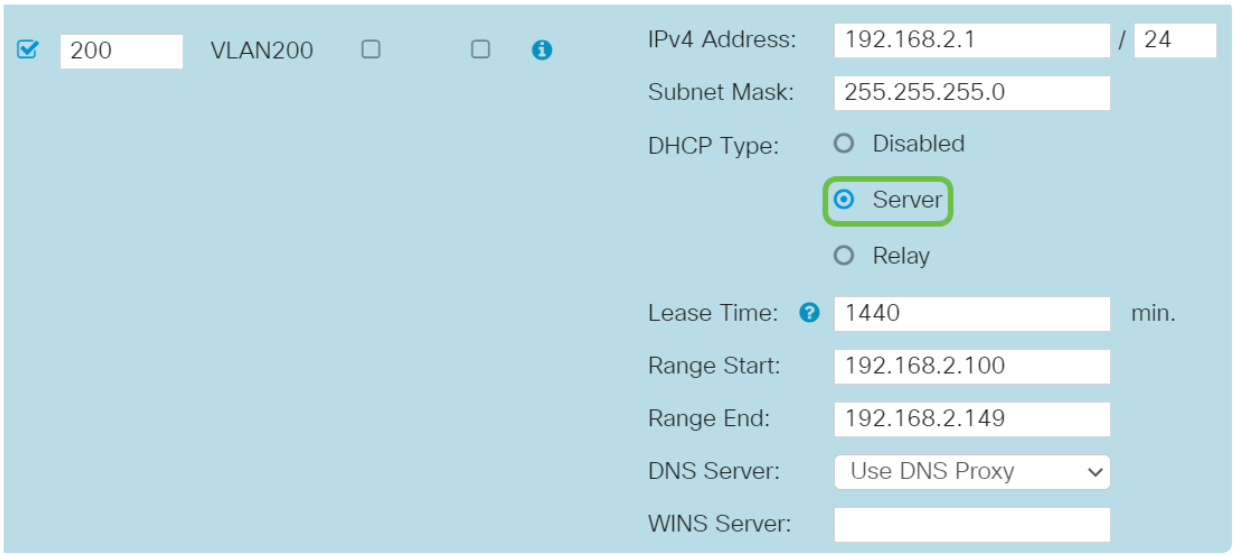
选择动态主机配置协议(DHCP)类型。以下选项是：

Disabled — 禁用VLAN上的DHCP IPv4服务器。建议在测试环境中执行此操作。在这种情况下，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。

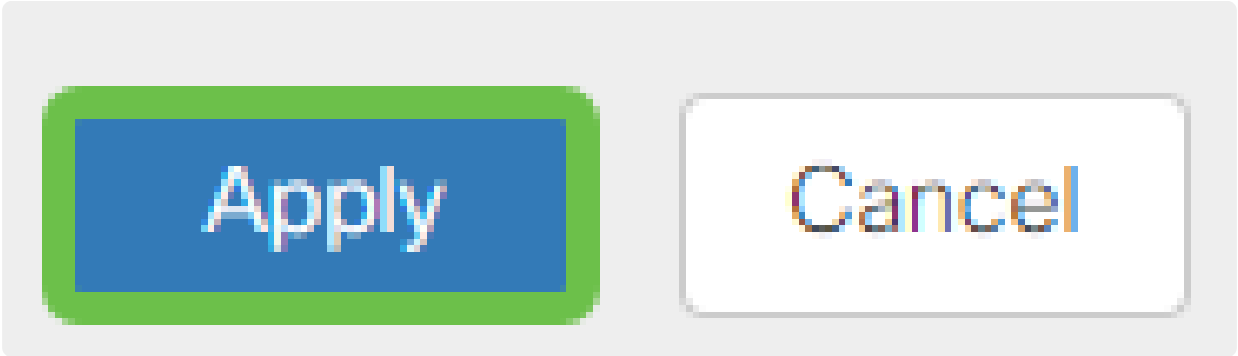
- 租用时间 — 输入时间值5到43,200分钟。默认值为1440分钟（等于24小时）。
- Range Start和Range End — 输入可以动态分配的IP地址的范围开始和结束。
- DNS Server — 选择将DNS服务器用作代理，或从下拉列表的ISP中选择。
- WINS服务器 — 输入WINS服务器名称。

- DHCP Options（DHCP 选项）：
  - 选项66 — 输入TFTP服务器的IP地址。
  - 选项150 — 输入TFTP服务器的IP地址。
  - 选项67 — 输入配置文件。
- 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以创建新的VLAN。



将VLAN分配到端口（可选）

在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应排除Excluded。这会将该端口上的流量专用于用户专门分配的VLAN/VLAN。这被认为是一种最佳做法。

端口可以设置为接入端口或中继端口：

- 接入端口 — 分配了一个VLAN。未标记的帧将被通过。
- 中继端口 — 可以承载多个VLAN。802.1q。中继允许本征VLAN无标记。您不希望在中继上使用的VLAN应排除在Excluded中。

一个VLAN分配了自己的端口：

- 被视为接入端口。
- 分配给此端口的VLAN应标记为未标记。
- 对于该端口，所有其他VLAN都应标记为Excluded。

共享一个端口的两个或多个VLAN:

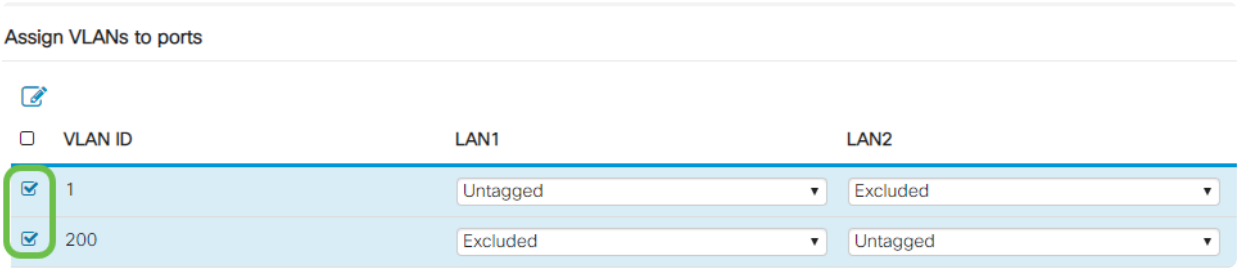
- 被视为中继端口。
- 其中一个VLAN可以标记为“无标记”。
- 属于Trunk端口的其他VLAN应标记为Tagged。
- 不属于中继端口的VLAN应标记为已排除。

> ⓘ Note: 在本示例中，没有中继。

第 1 步

选择要编辑的VLAN ID。

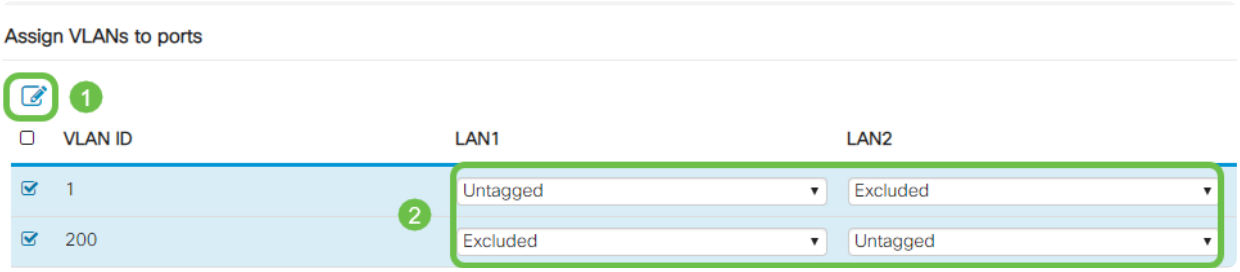
在本例中，我们选择了VLAN 1和VLAN 200。



第 2 步

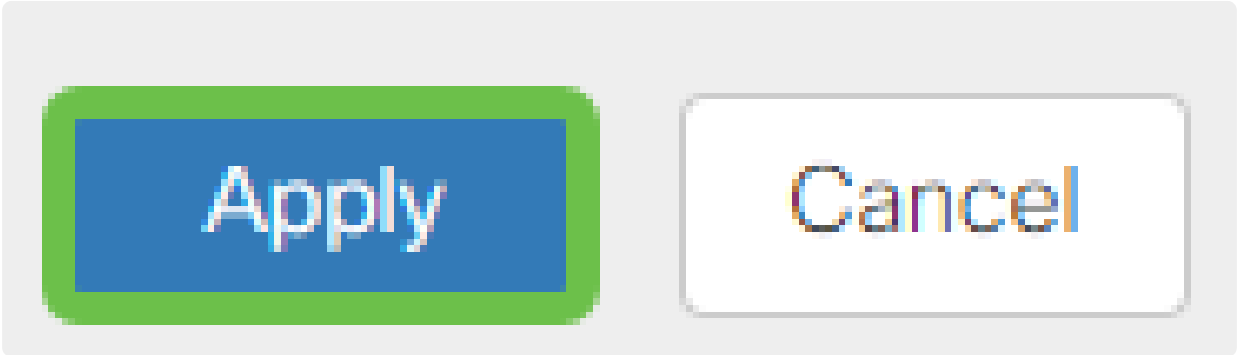
单击Edit将VLAN分配给LAN端口，并将每个设置指定为Tagged、Untagged或Excluded。

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。



第 3 步

单击Apply保存配置。



现在，您应该已经成功创建了一个新的VLAN并为RV345P上的端口配置了VLAN。重复此过程以创建其他VLAN。例如，VLAN300将为Marketing创建，子网为192.168.3.x，VLAN400将为Accounting创建，子网为192.168.4.x。

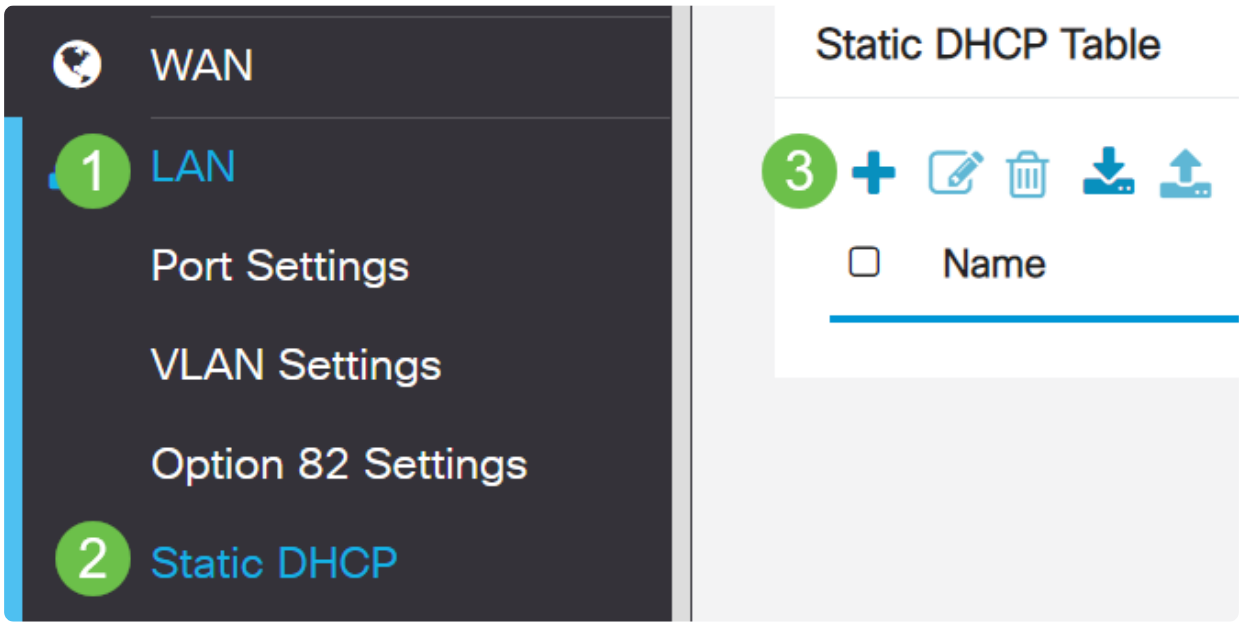
添加静态IP（可选）

如果希望某台设备可以访问其他VLAN，您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。这仅在启用VLAN间路由时有效。在其他情况下，静态IP可能很有用。有关设置静态IP地址的详细信息，请查看在思科业务硬件上设置静态IP地址的最佳实践。

如果您不需要添加静态IP地址，您可以转到本文的下一节。

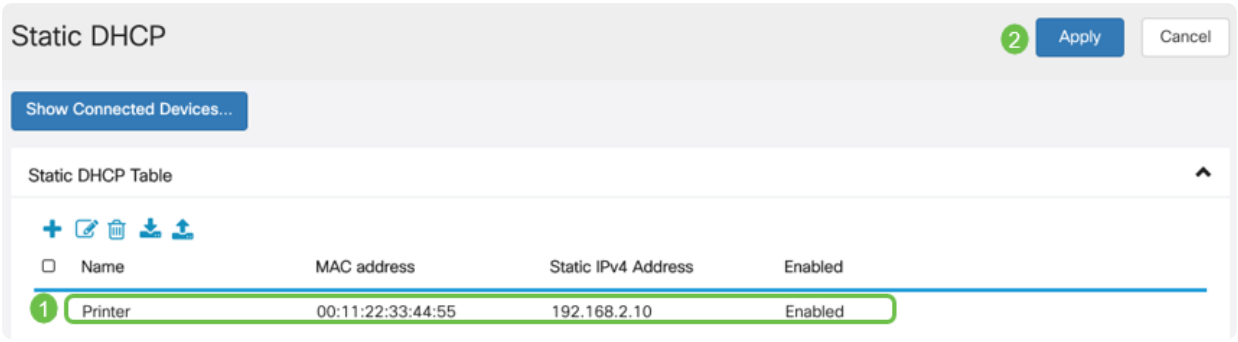
第 1 步

导航到LAN > Static DHCP。点击加号图标。



第 2 步

添加设备的静态DHCP信息。在本示例中，设备是打印机。



管理证书（可选）

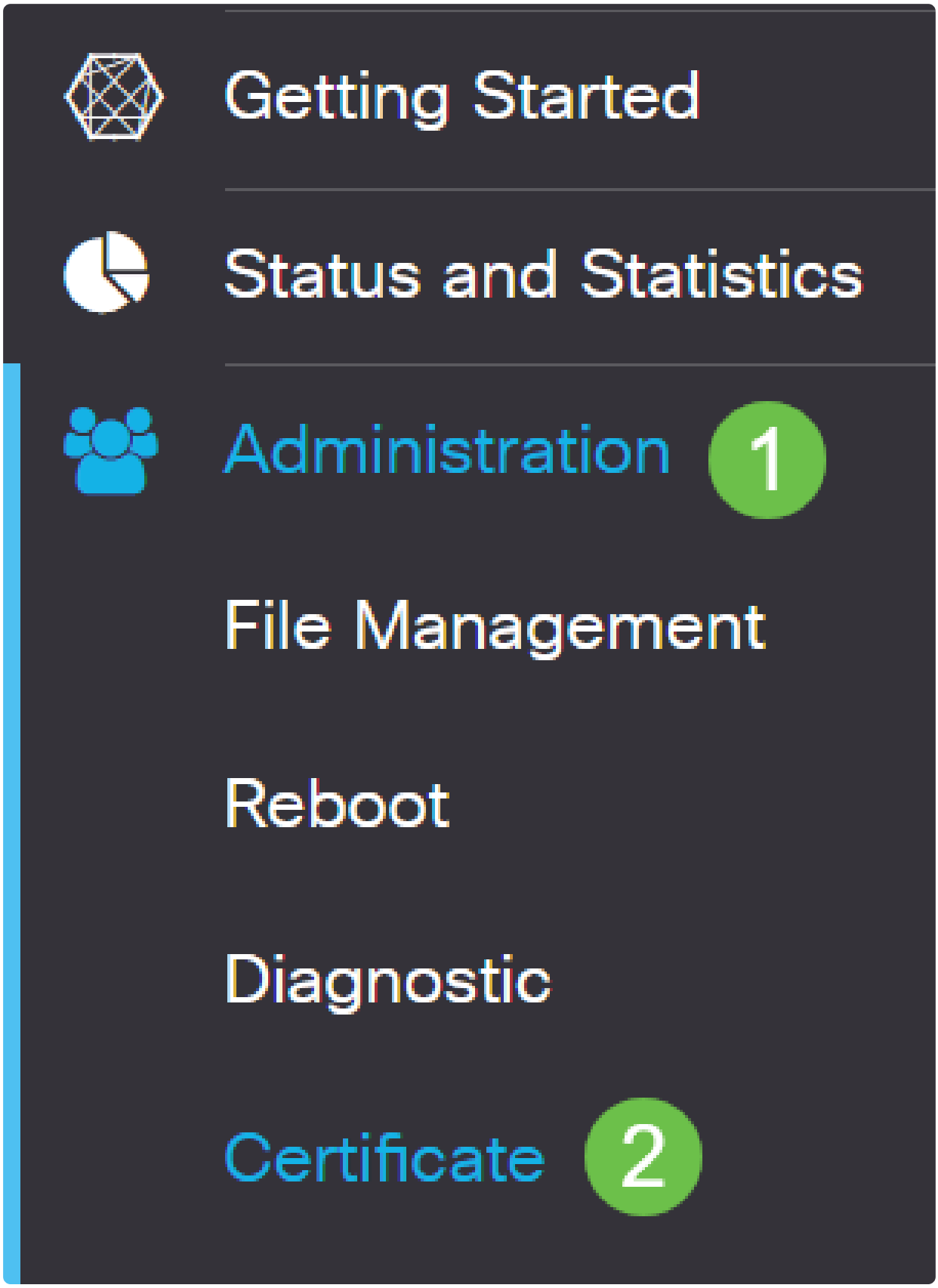
数字证书通过证书的指定主题来证明公共密钥的所有权。这允许依赖方依赖于由私钥执行的签名或声明，该私钥对应于经过认证的公钥。路由器可以生成自签名证书，即由网络管理员创建的证书。它还可以向证书颁发机构(CA)发送请求以申请数字身份证书。必须拥有来自第三方应用的合法证书。

证书颁发机构(CA)用于身份验证。可以从任意数量的第三方站点购买证书。这是证明您的站点安全的官方方式。实质上，CA是可信来源，用于验证您是否为合法企业并且可以受到信任。根据您的需要，以最低成本提供证书。CA会签出您的帐户，他们验证您的信息后，会向您颁发证书。此证书可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）并将其上传到那里。

生成CSR/证书

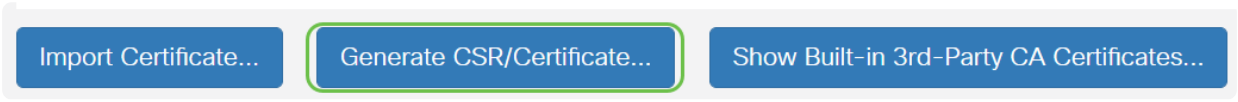
第 1 步

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


Getting Started
Status and Statistics
Administration
1
File Management
Reboot
Diagnostic
Certificate
2

第 2 步

点击生成CSR/证书。您将进入“生成CSR/证书”(Generate CSR/Certificate)页面。

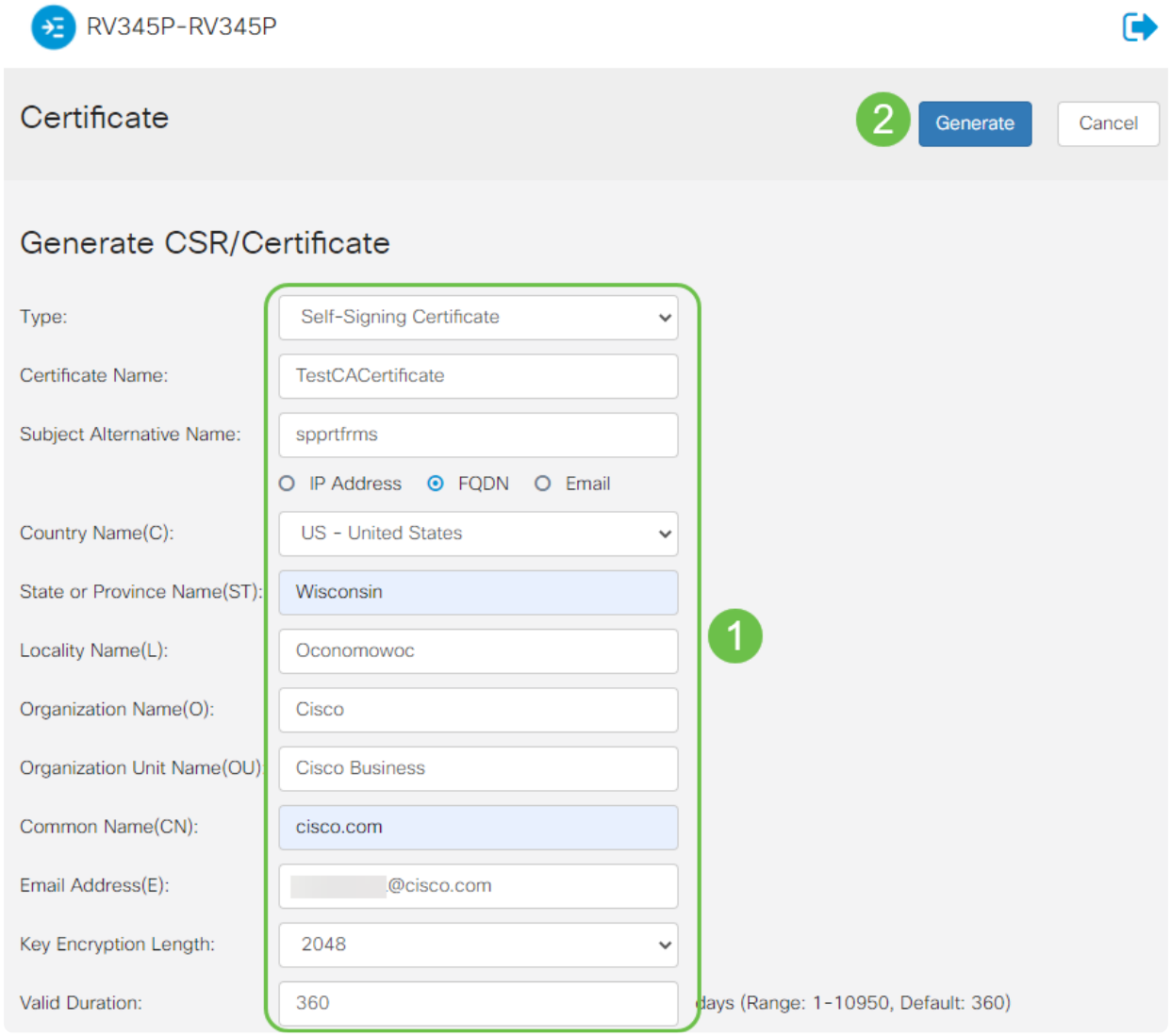


第 3 步

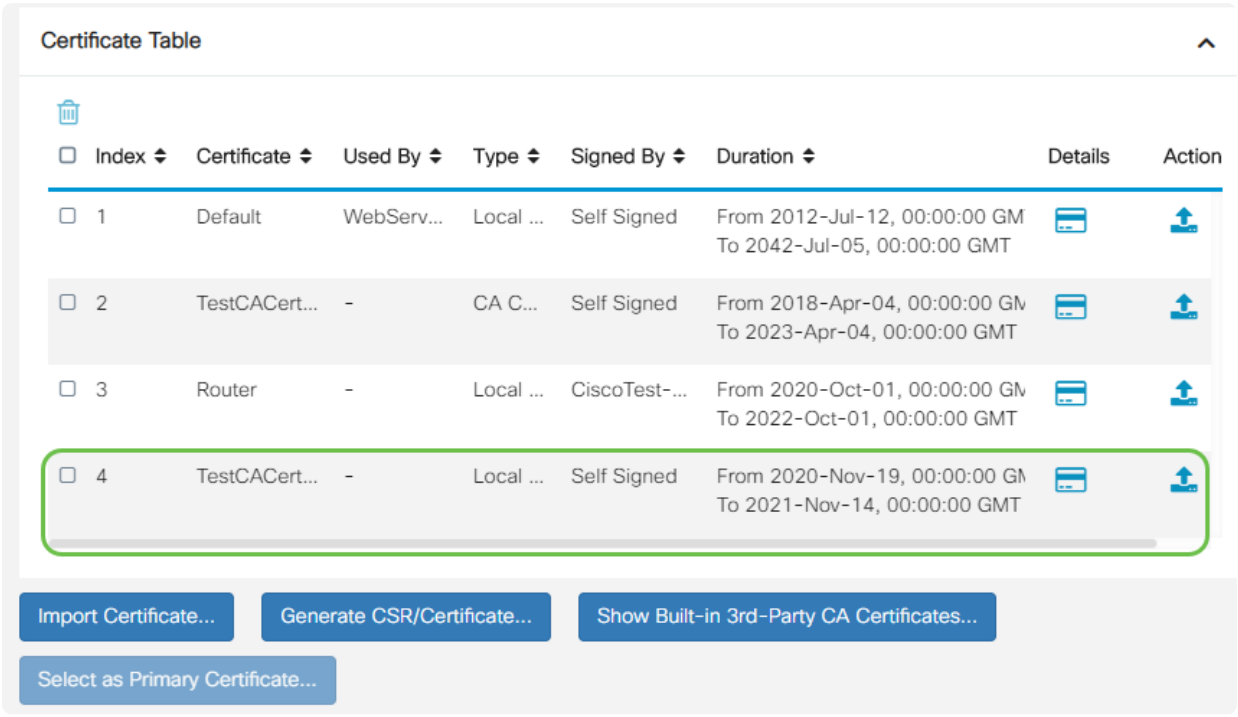
用以下内容填写这些框：

- 选择适当的证书类型
  - 自签名证书 — 这是由自己的创建者签署的安全套接字层(SSL)证书。此证书不受信任，因为如果攻击者以某种方式入侵私钥，则无法取消此证书。
  - 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Subject Alternative Name区域下，点击单选按钮。选项有：
  - IP Address — 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Country Name下拉列表中选择组织合法注册的国家/地区名称。
- 在State or Province Name(ST)字段中输入组织所在的州、省、区域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方或城市的名称。
- 输入企业合法注册时使用的名称。如果您注册为小型企业或独资企业，请在Organization Name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，以区分组织内的各个部门。
- 在Common Name字段中输入名称。此名称必须是您对其使用证书的网站的完全限定域名。
- 输入想要生成证书的人的电邮地址。
- 从Key Encryption Length下拉列表中，选择密钥长度。选项为512、1024和2048。密钥长度越大，证书就越安全。
- 在Valid Duration字段中，输入证书有效的天数。默认值为 360。
- 单击生成。



ⓘ Note: 生成的证书现在应显示在证书表中。

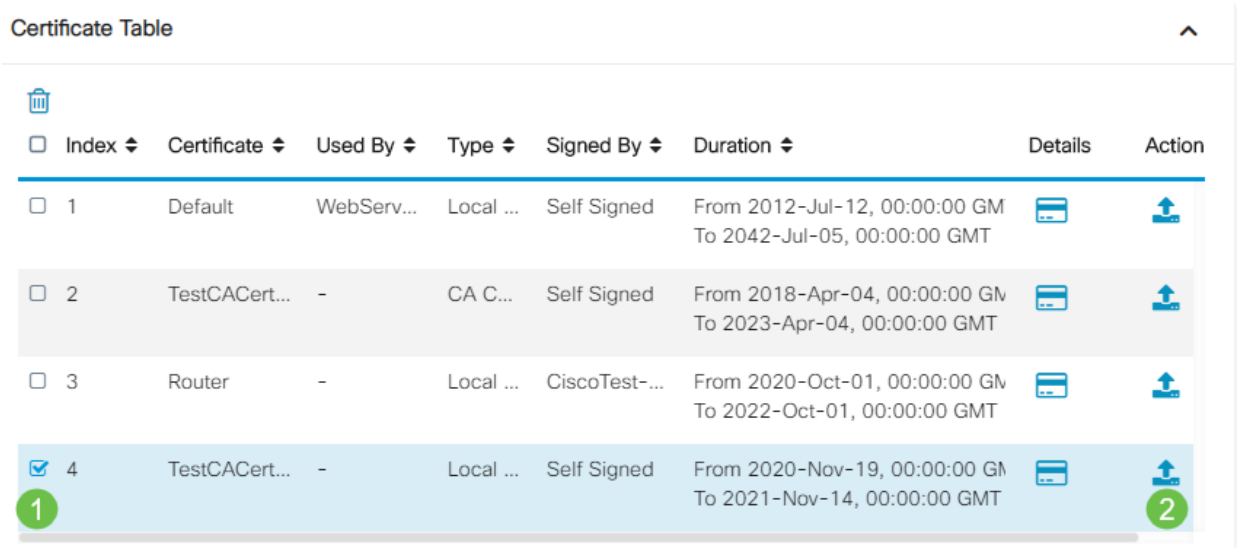


您现在应该已经在RV345P路由器上成功创建证书。

导出证书

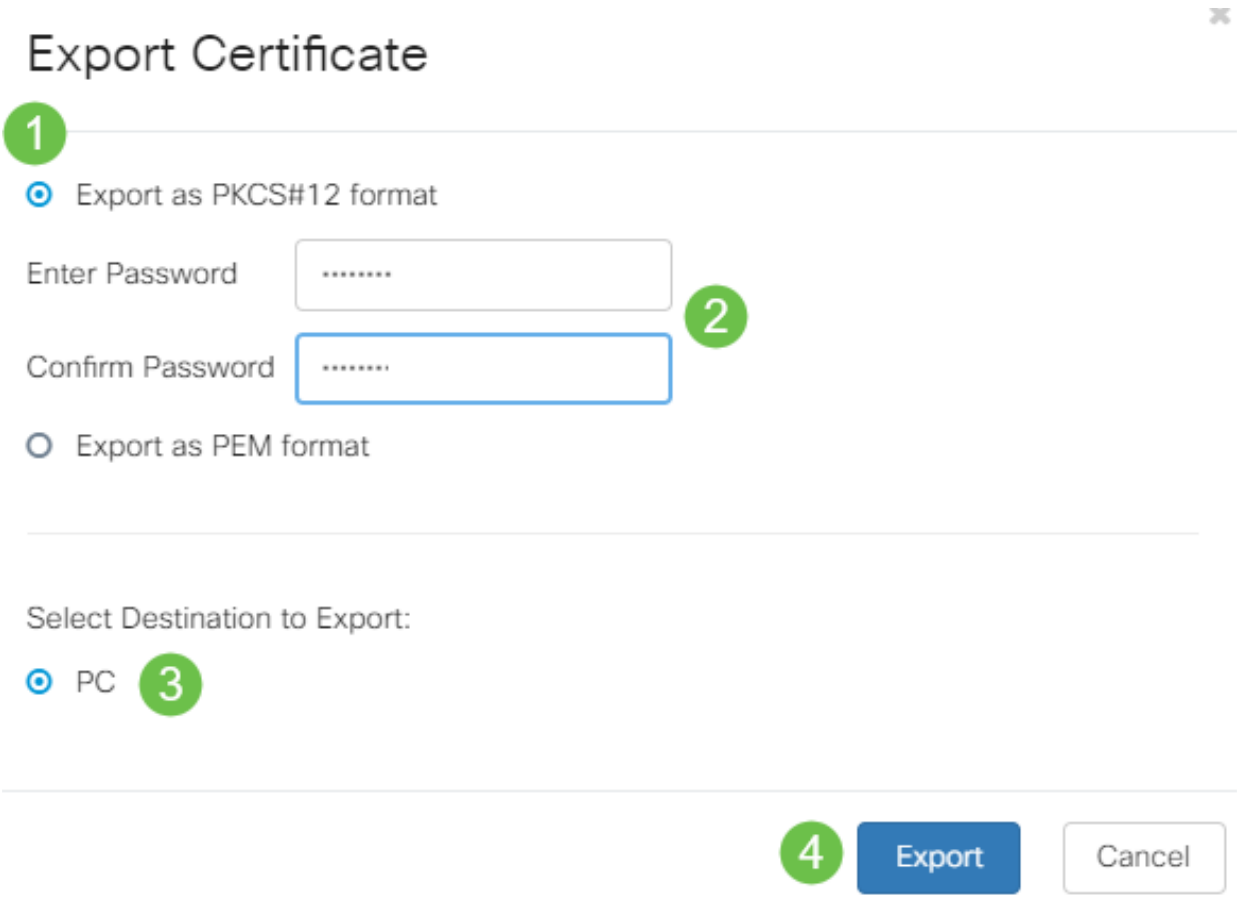
第 1 步

在证书表中，选中要导出的证书的复选框，然后点击export图标。



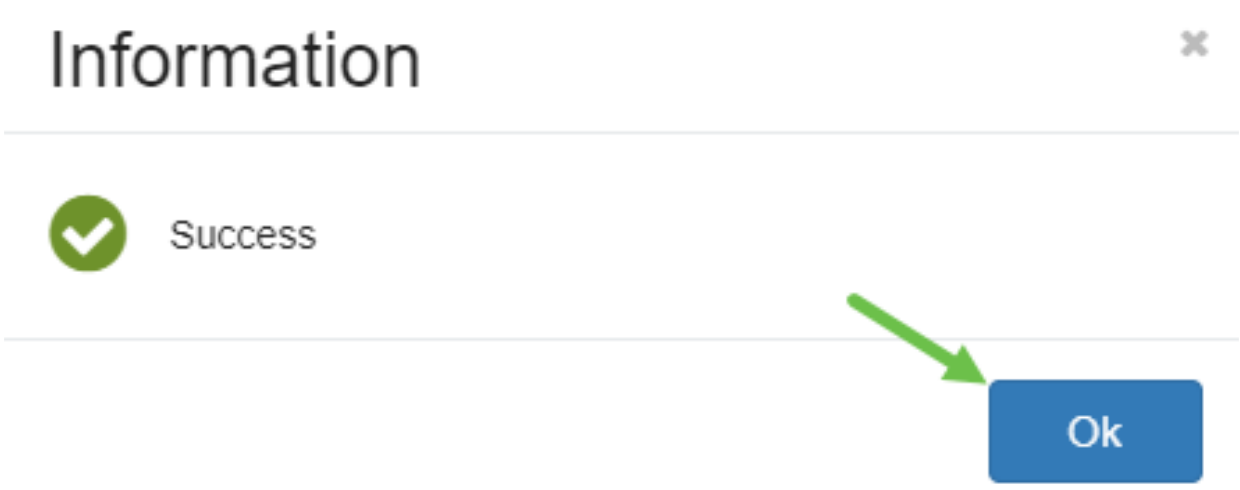
第 2 步

- 点击格式以导出证书。选项有：
  - PKCS #12 — 公钥加密标准(PKCS)#12是以.p12扩展名提供的导出证书。需要对文件进行加密，以便在导出、导入和删除文件时对其进行保护。
  - PEM — 隐私增强型邮件(PEM)通常用于Web服务器，因为它可以使用记事本等简单文本编辑器轻松转换为可读数据。
- 如果选择PEM，只需单击Export。
- 在Enter Password字段中输入密码以保护要导出的文件。
- 在Confirm Password字段中重新输入密码。
- 在Select Destination区域，已选择PC，它是当前唯一可用的选项。
- 单击Export。



第 3 步

Download按钮下方会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.

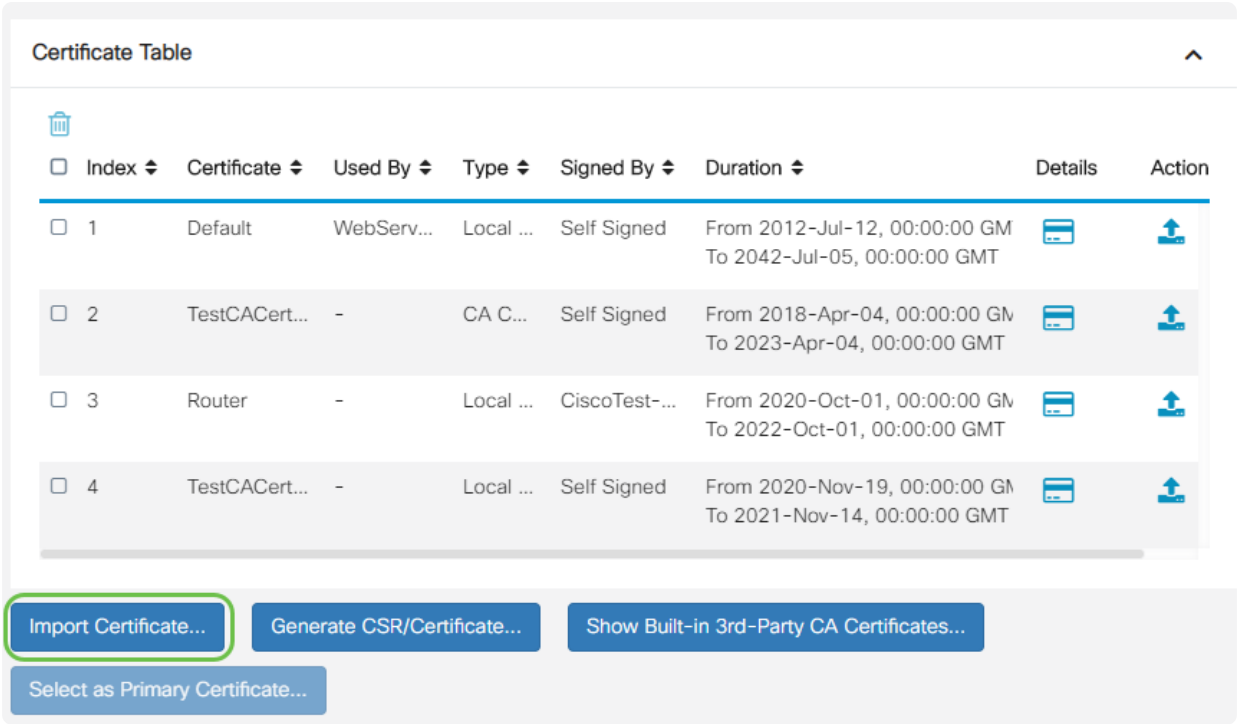


您现在应该已经成功在RV345P系列路由器上导出证书。

导入证书

第 1 步

单击Import Certificate....

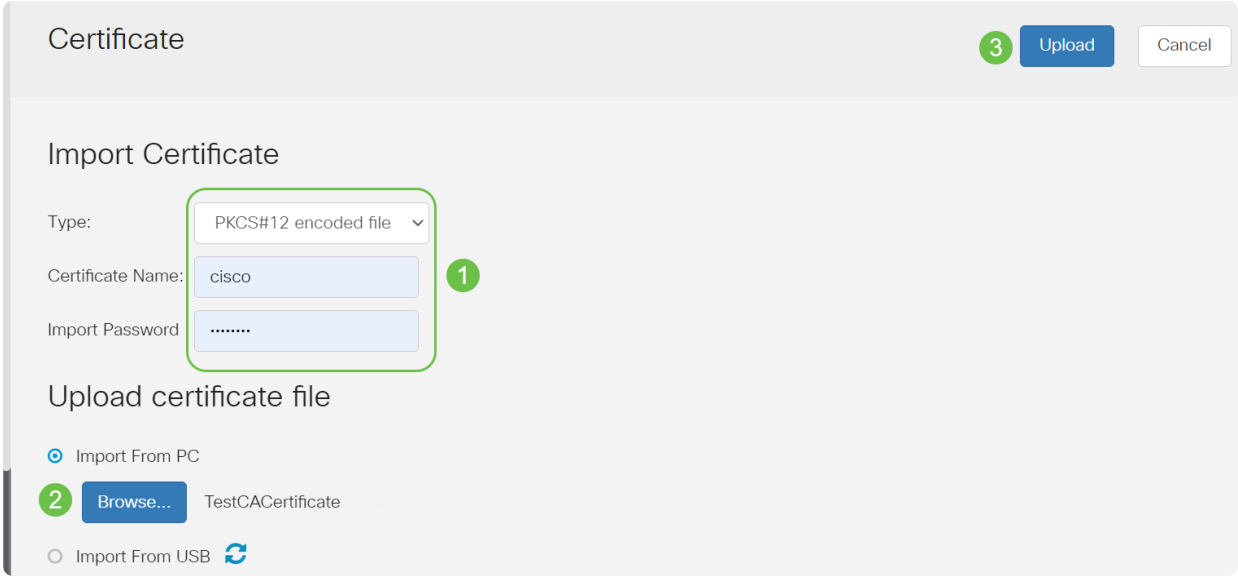


第 2 步

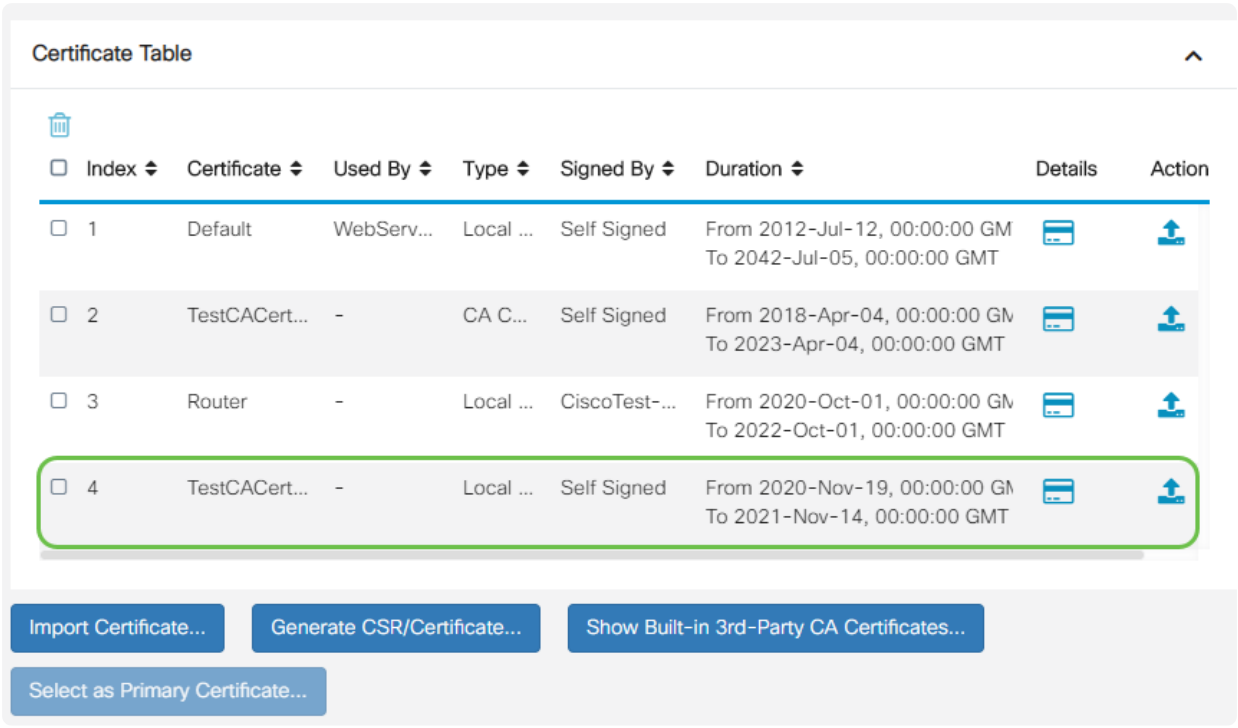
- 从下拉列表中选择要导入的证书类型。选项有：
  - 本地证书 — 路由器上生成的证书。
  - CA证书 — 由受信任的第三方机构认证的证书，该机构已确认证书中包含的信息是准确的。
  - PKCS #12 Encoded file — 公钥加密标准(PKCS)#12是存储服务器证书的格式。

- 在Certificate Name字段中输入证书的名称。
- 如果选#12了PKCS密码，请在Import Password字段中输入文件的密码。否则，请跳至步骤3。
- 点击源以导入证书。选项有：
  - 从PC
  - 从USB导入

- 如果路由器未检测到USB驱动器，“从USB导入”选项将灰显。
- 如果选择Import From USB（从USB导入），并且路由器无法识别您的USB，请单击Refresh（刷新）。
- 点击“选择文件”按钮并选择适当的文件。
- 单击Upload。



成功后，您将自动进入证书主页。证书表将填充最近导入的证书。



现在，您应该已经成功地在RV345P路由器上导入了证书。

使用Dongle和RV345P系列路由器配置移动网络（可选）

您可能想要使用加密狗和RV345P路由器配置备用移动网络。如果出现这种情况，应阅读使用转换器和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上的PoE端口插入RV345P上的PoE端口。RV345P的前4个端口可提供PoE，因此可以使用其中任意一个。

检查指示灯的状态。接入点将需要大约10分钟时间启动。LED将以多个模式呈绿色闪烁

，依次经过绿色、红色和琥珀色，然后再次变为绿色。LED的颜色强度和色调在单位之间可能有细微的变化。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，而不能连接到任何其他支持主或网状网扩展器设备。

如果您的接入点不是新的、开箱即用的，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。有关此问题的帮助，请查看如何重新启动RV345x路由器并重置为出厂默认设置。

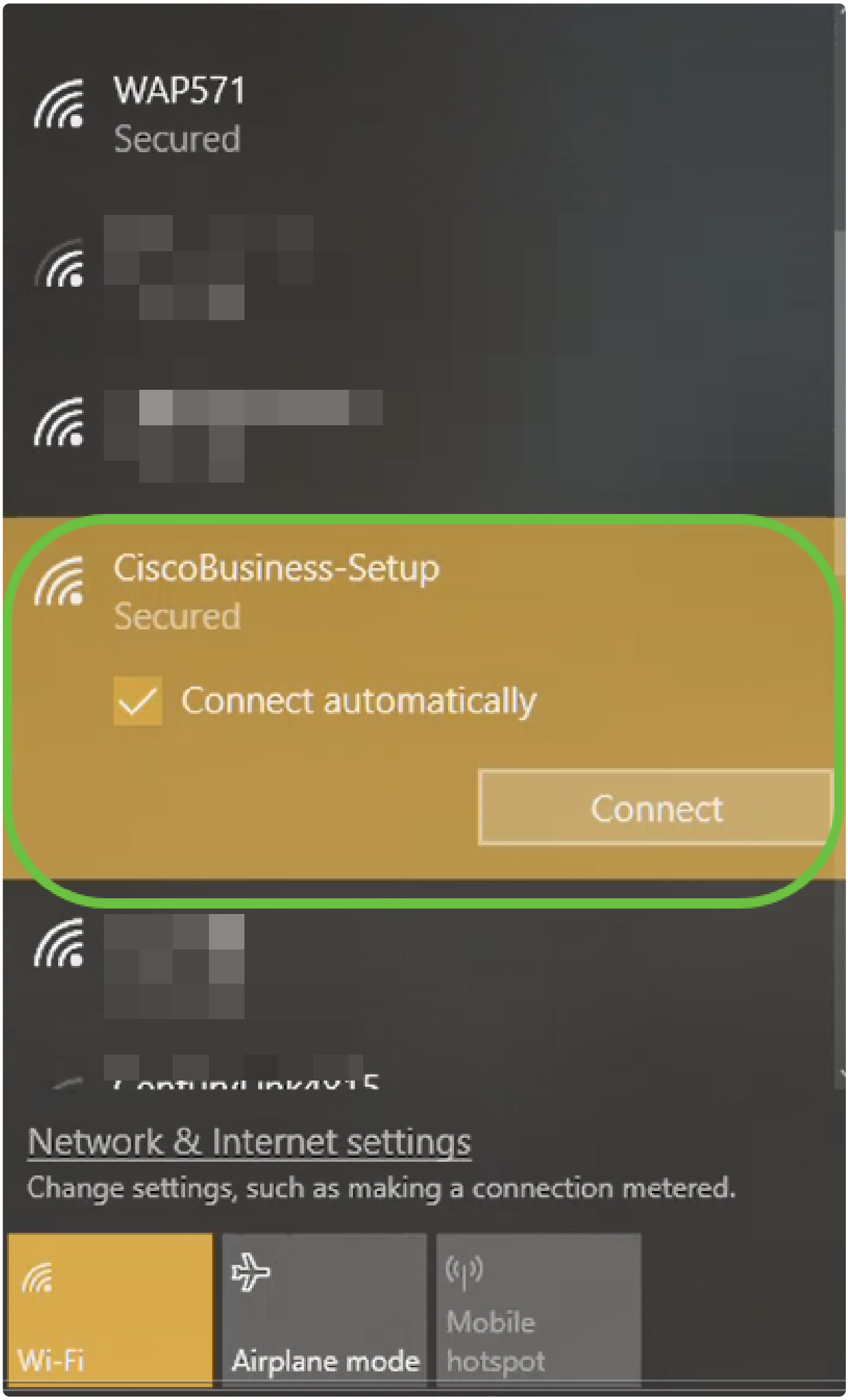
在Web UI上设置140AC主无线接入点

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，它提供了更多的配置选项，但稍微复杂一些。如果您想在下一节中使用移动应用，请单击访问移动应用说明。

如果无法连接，请参阅本文的无线故障排除提示部分。

第 1 步

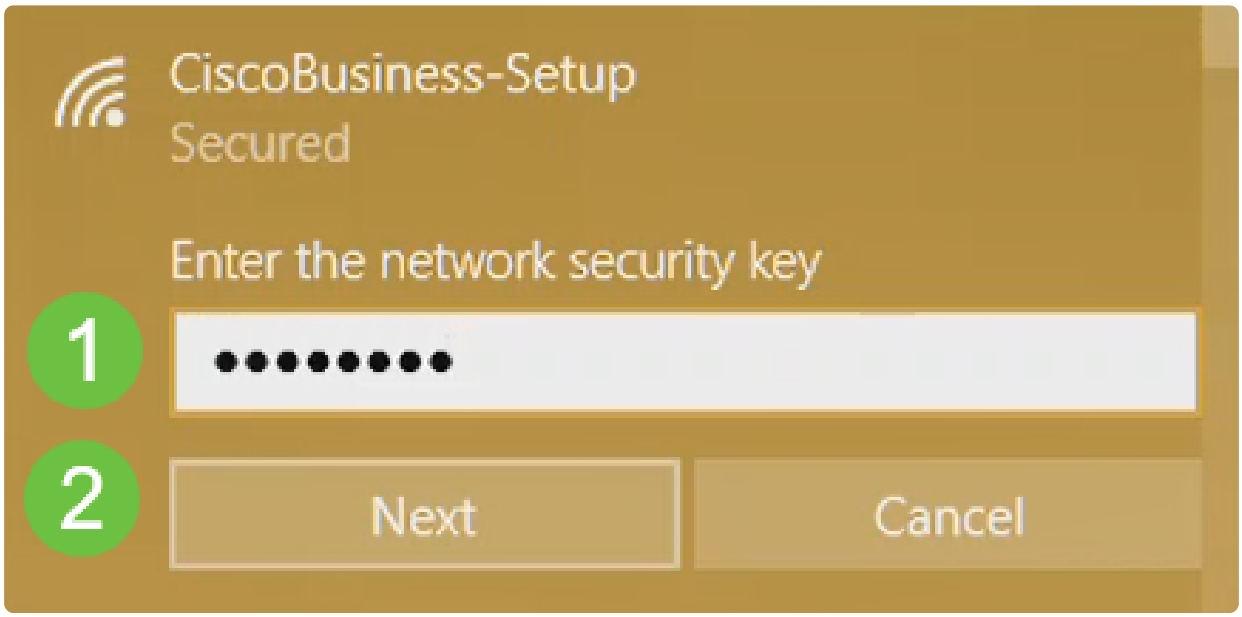
在PC上，单击Wi-Fi图标并选择CiscoBusiness-Setup无线网络。单击 Connect。


WAP571
Secured
CiscoBusiness-Setup
Secured
Connect automatically
Connect
Network & Internet settings
Change settings, such as making a connection metered.
Wi-Fi
Airplane mode
Mobile hotspot

如果您的接入点不是新的、开箱即用的，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。

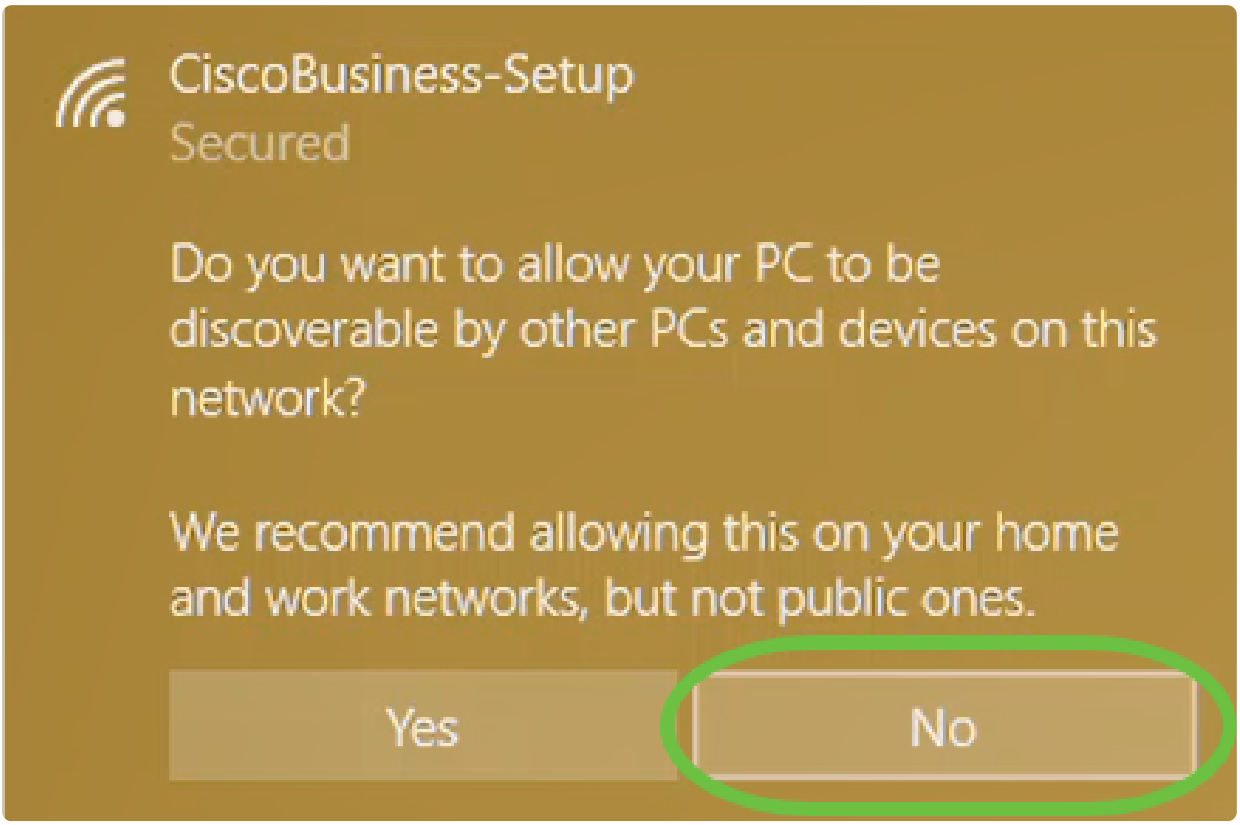
第 2 步

输入口令cisco123，然后单击Next。



第 3 步

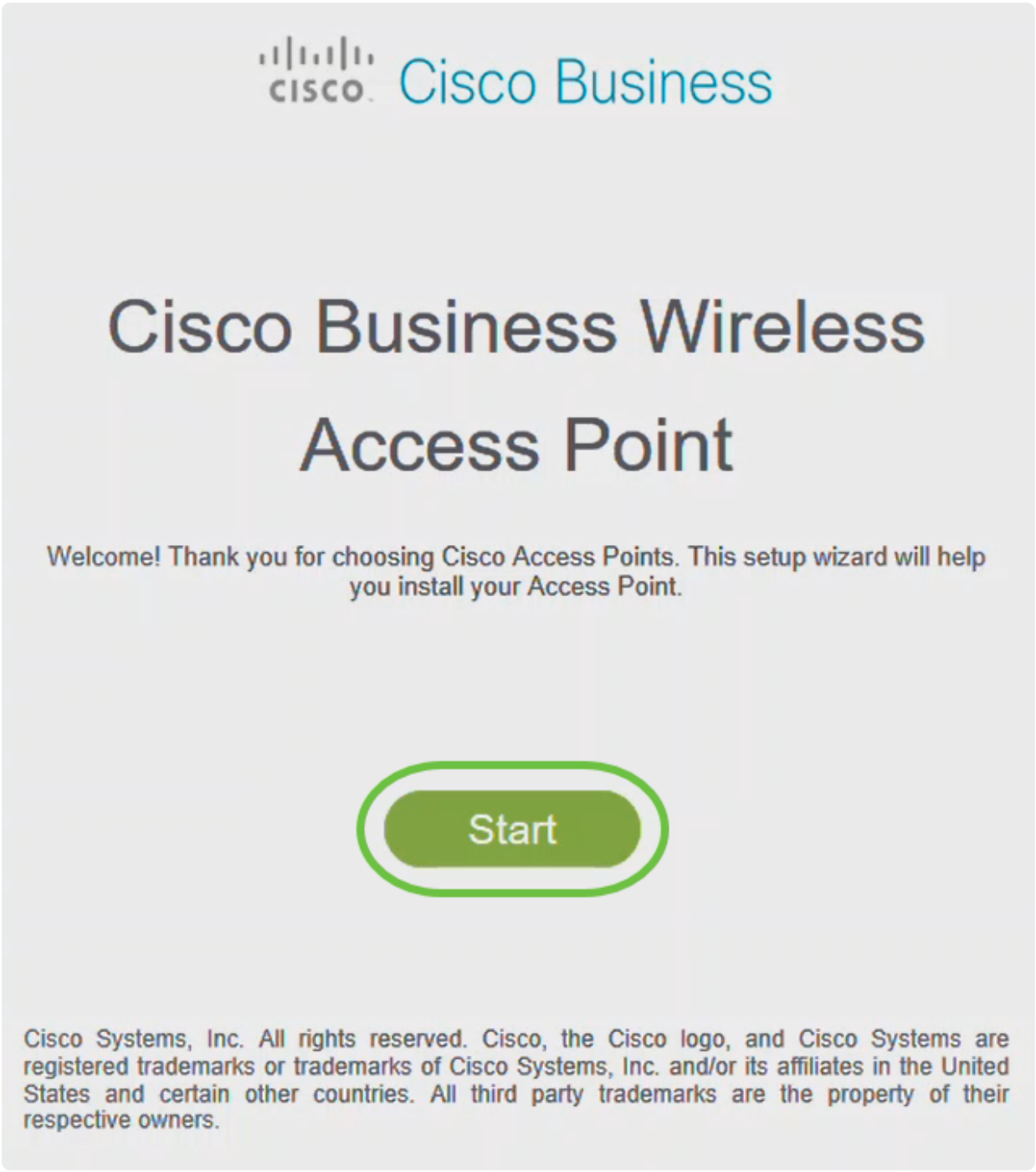
您将看到以下屏幕。由于您一次只能配置一台设备，请单击No。



只能将一个设备连接到CiscoBusiness-Setup SSID。如果另一台设备尝试连接，则无法连接。如果您无法连接到SSID并已验证密码，则可能是某些其他设备建立了连接。重新启动AP并重试。

第 4 步

连接后，Web浏览器应自动重定向至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，然后按Enter。在网页上单击Start。



ⓘ Note: 如果您看不到该网页，请再等待几分钟，或重新加载该页面。完成此初始设置后，您将使用https://ciscobusiness.cisco登录。如果您的Web浏览器自动填充 http://，则需要手动键入 https://才能获得访问权限。

步骤 5

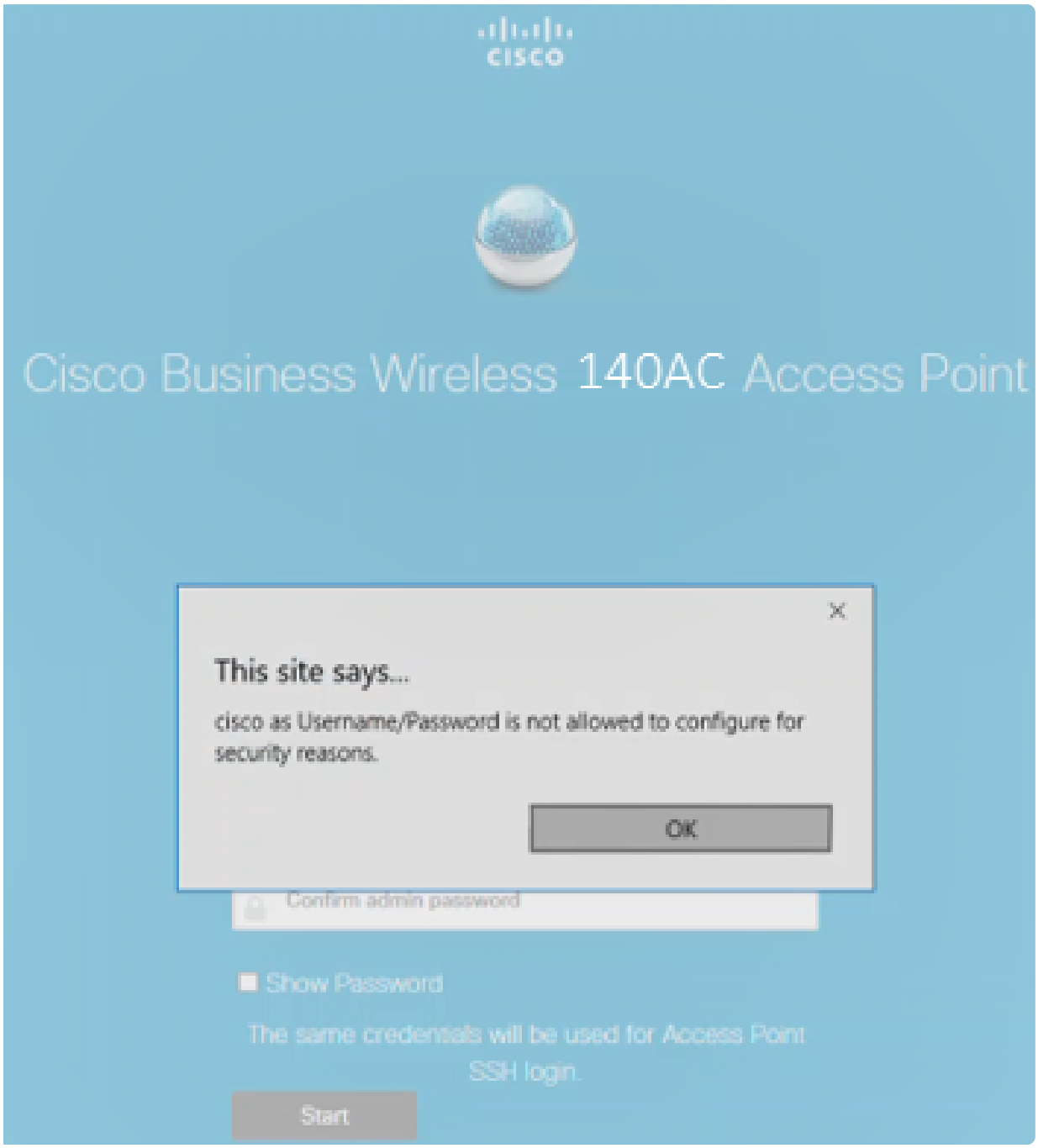
通过输入以下内容创建管理员帐户：

- 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Show Password旁边的复选框来选择显示密码。单击开始。



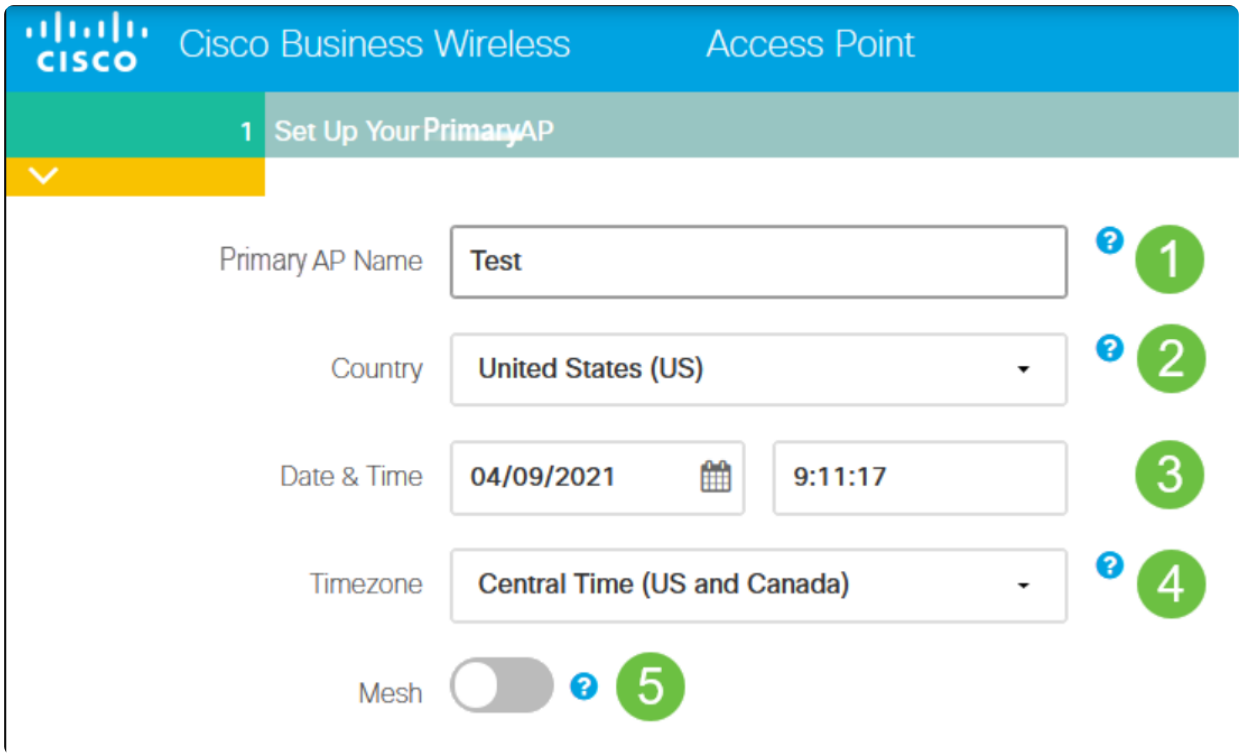
请勿在用户名或密码字段中使用cisco或其变体。如果这样做，您将收到如下所示的错误消息。



第 6 步

通过输入以下内容设置您的主AP:

- 主AP名称
- 国家/地区
- 日期和时间
- 时区
- 网状



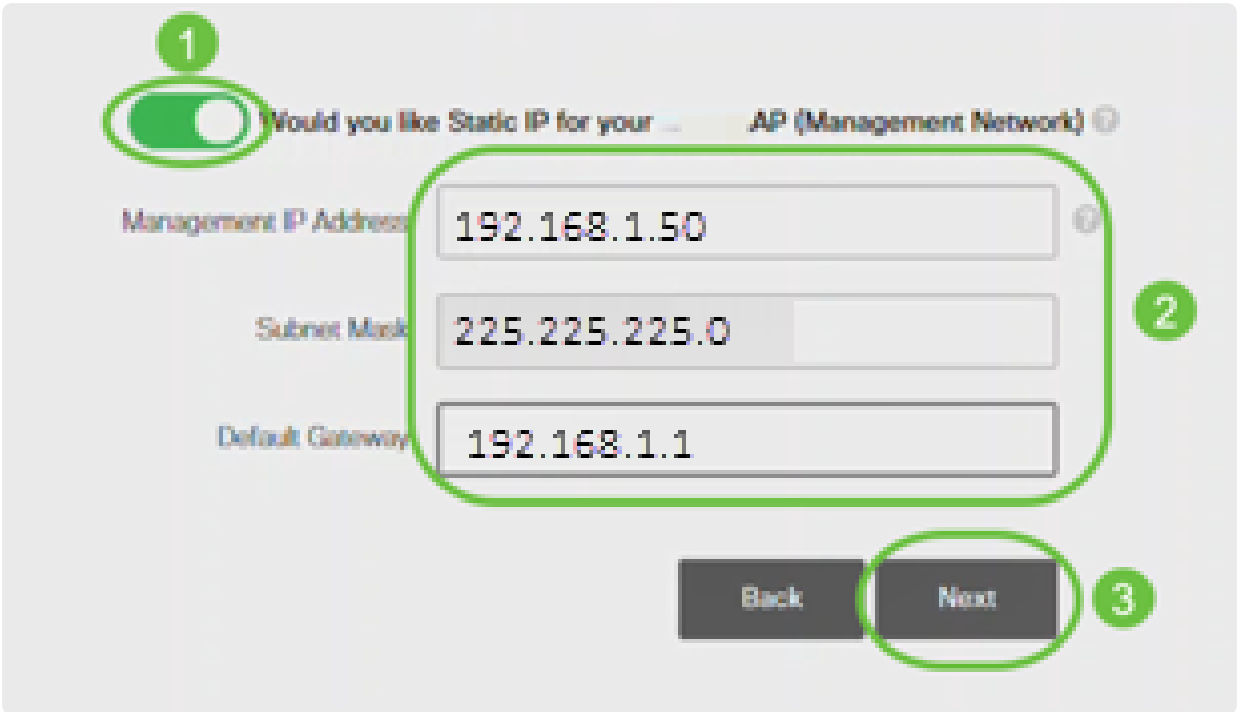
只要计划创建网状网络，才应启用网状。默认情况下，该选项处于禁用状态。

第 7 步

（可选）您可以为CBW140AC启用静态IP以用于管理目的。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。



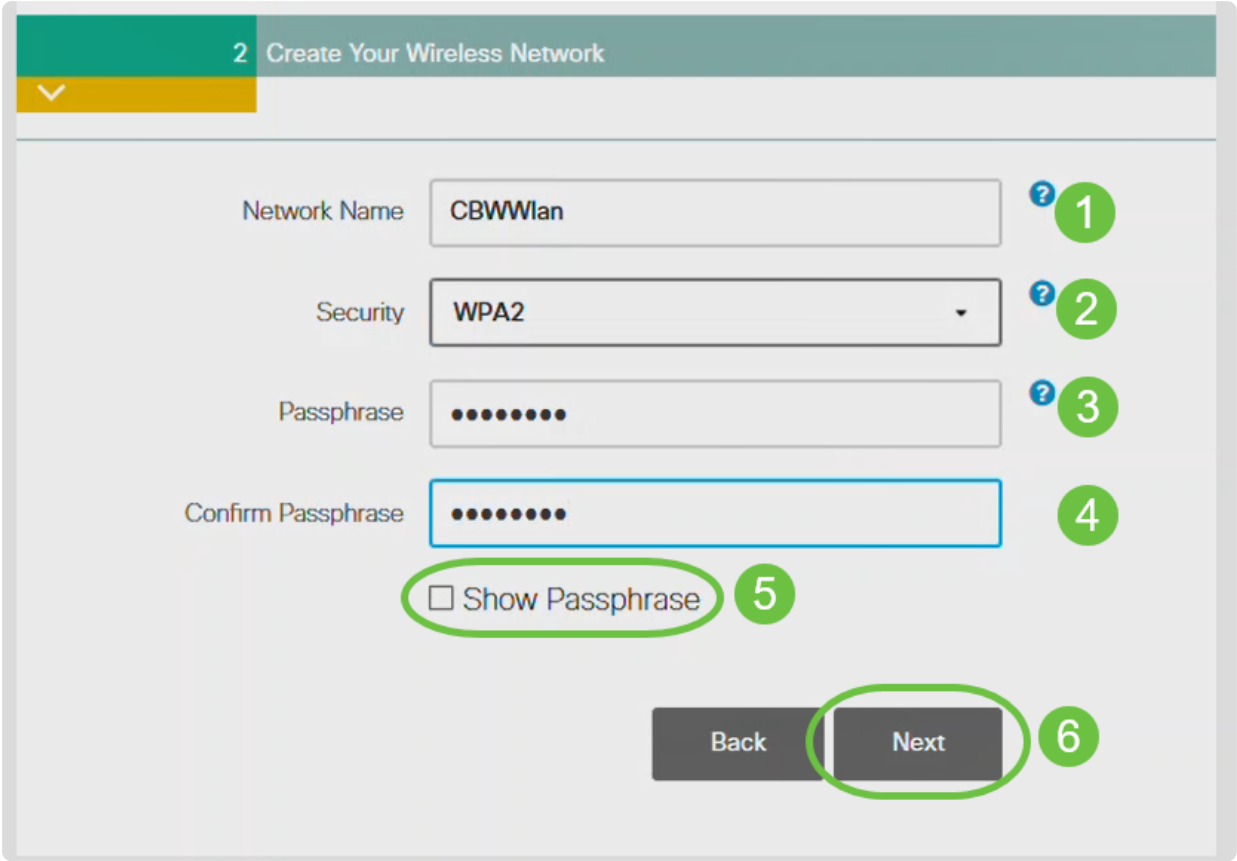
默认情况下，此选项处于禁用状态。

步骤 8

通过输入以下内容创建您的无线网络：

- 网络名称
- 选择安全
- 口令
- 确认口令
- （可选）勾选复选框以显示口令。

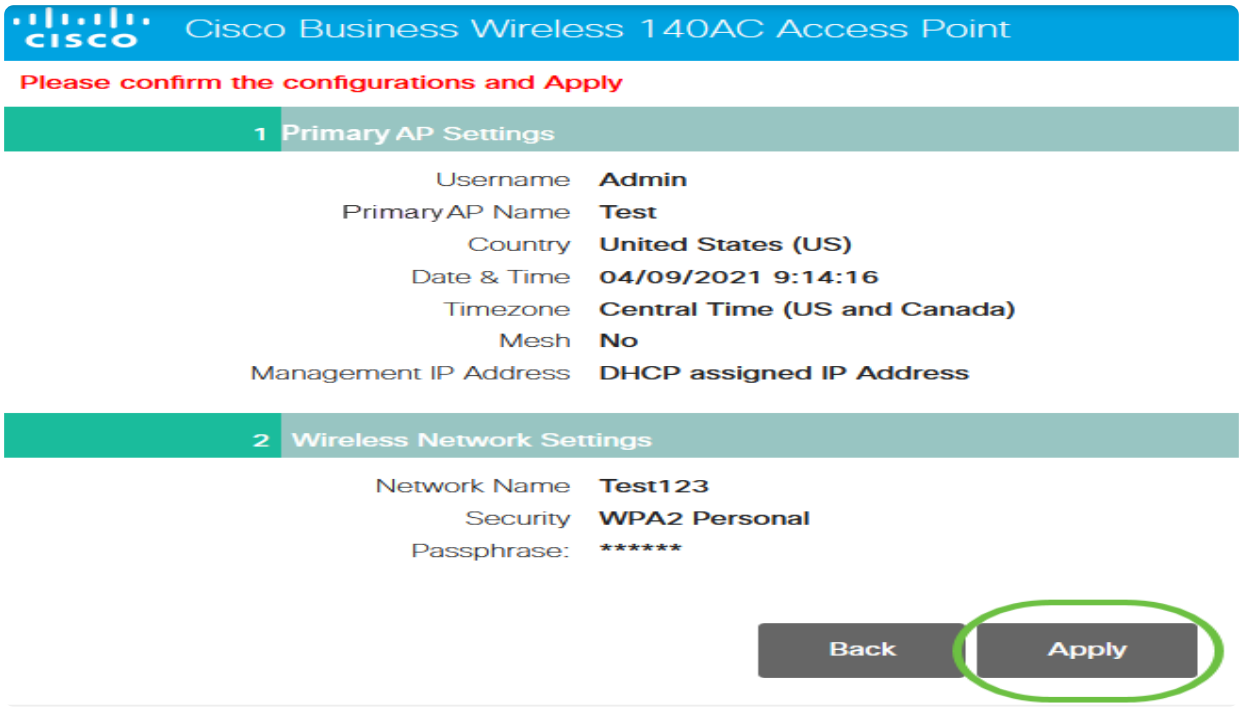
单击 Next。



Wi-Fi保护访问(WPA)第2版(WPA2)是Wi-Fi安全的当前标准。

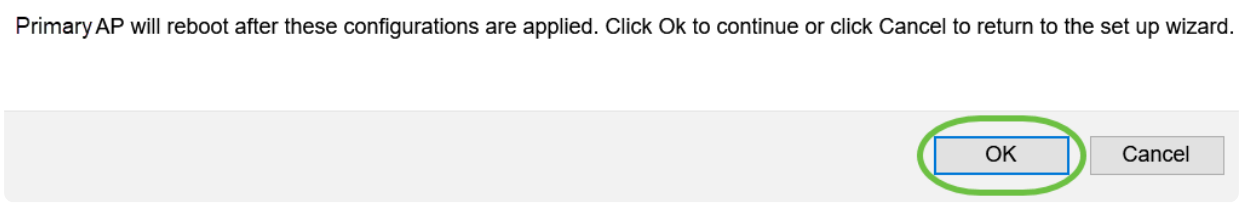
步骤 9

确认设置并单击Apply。

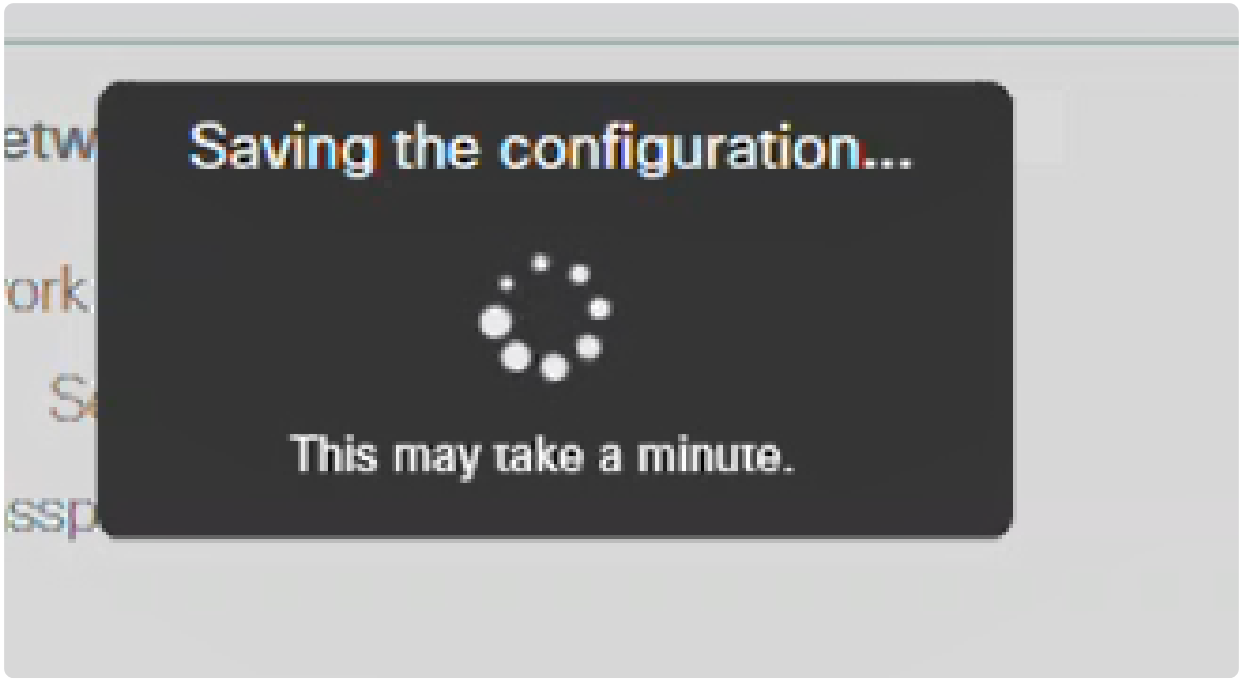


步骤 10

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。

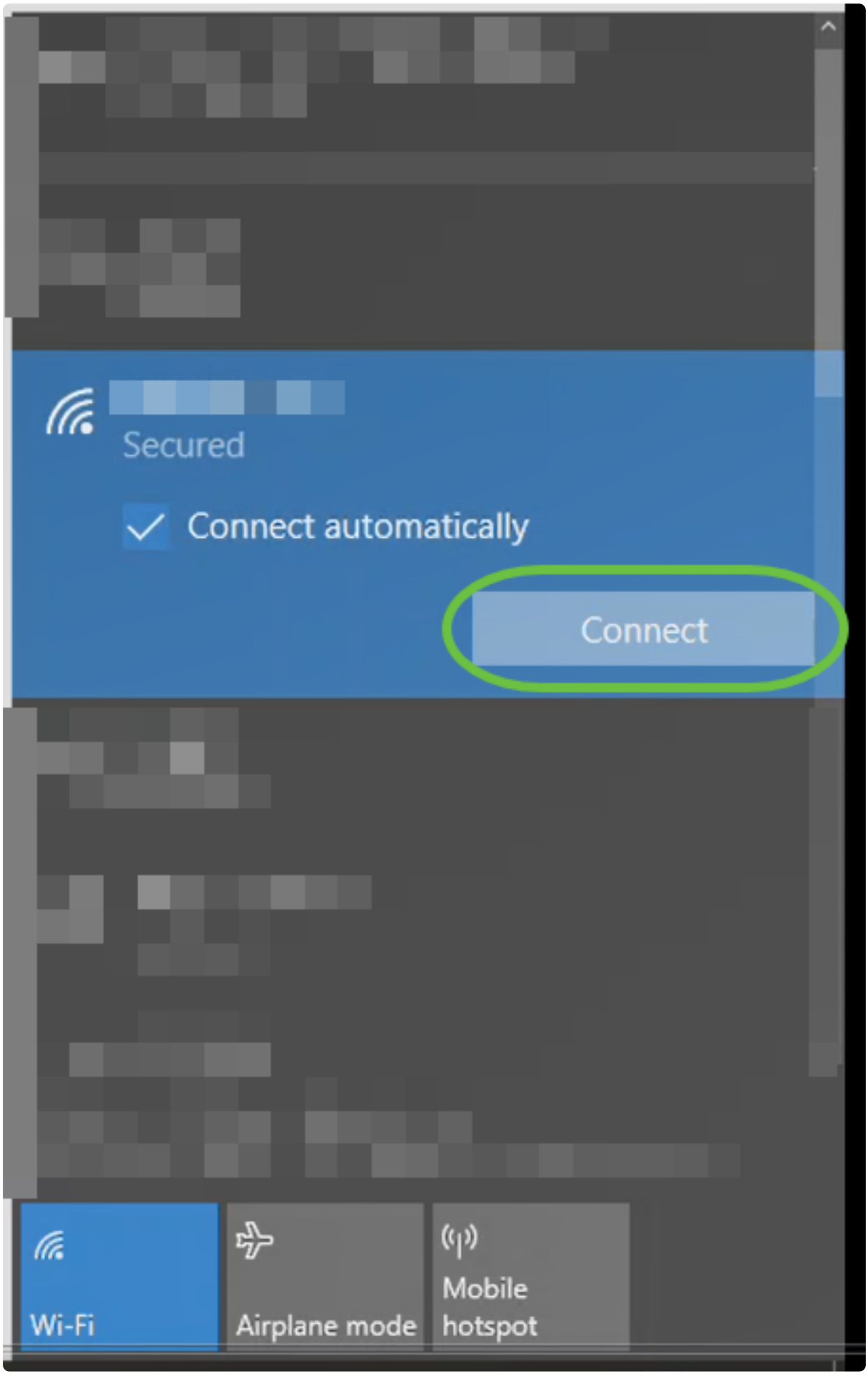


在重新启动期间，接入点中的LED将经历多种颜色模式。当LED呈绿色闪烁时，继续下一步。如果LED没有超过红色闪烁模式，则表明您的网络中没有DHCP服务器。确保AP连接到交换机或带DHCP服务器的路由器。

步骤 11

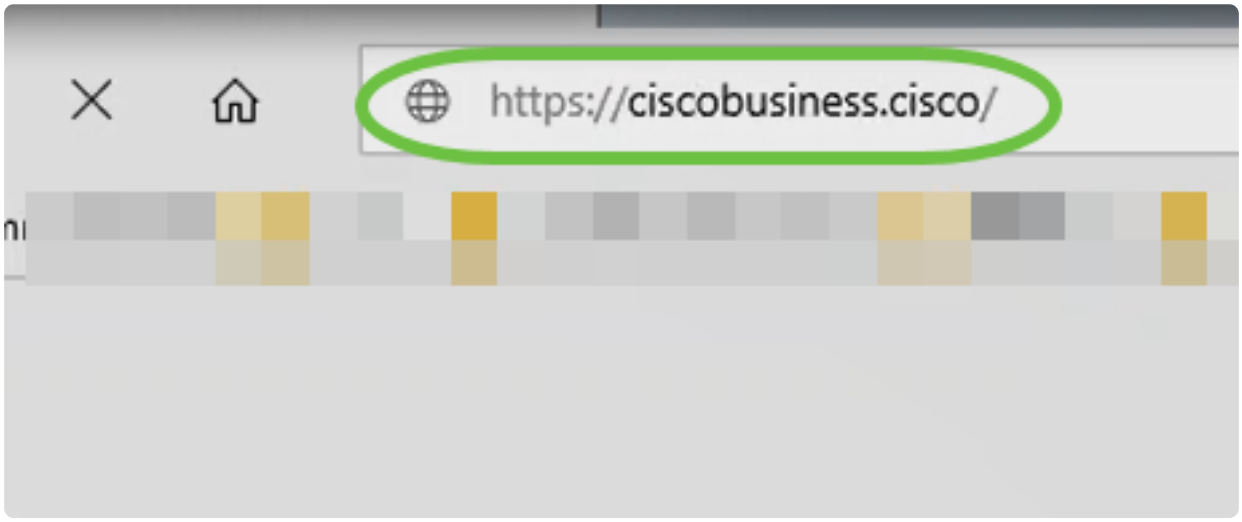
转到PC上的无线选项，然后选择您配置的网络。单击 Connect。

CiscoBusiness-Setup SSID将在重新启动后消失。


Secured
Connect automatically
Connect
Wi-Fi
Airplane mode
Mobile hotspot

步骤 12

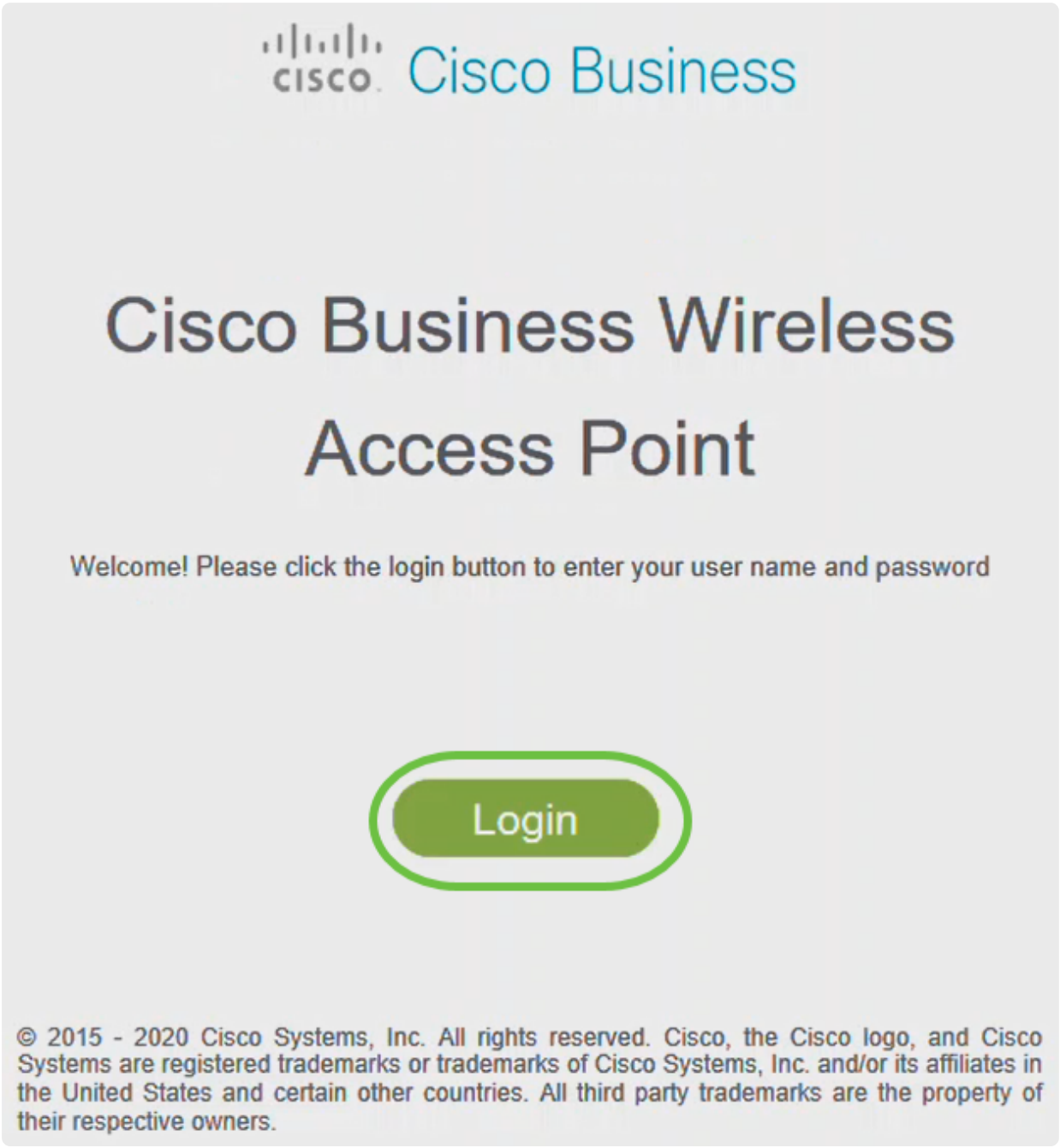
打开Web浏览器并键入https://[CBW AP的IP地址]。或者，您可以在地址栏中键入https://ciscobusiness.cisco，然后按Enter。



ⓘ Note: 确保在此步骤中键入 https，而不是 http。

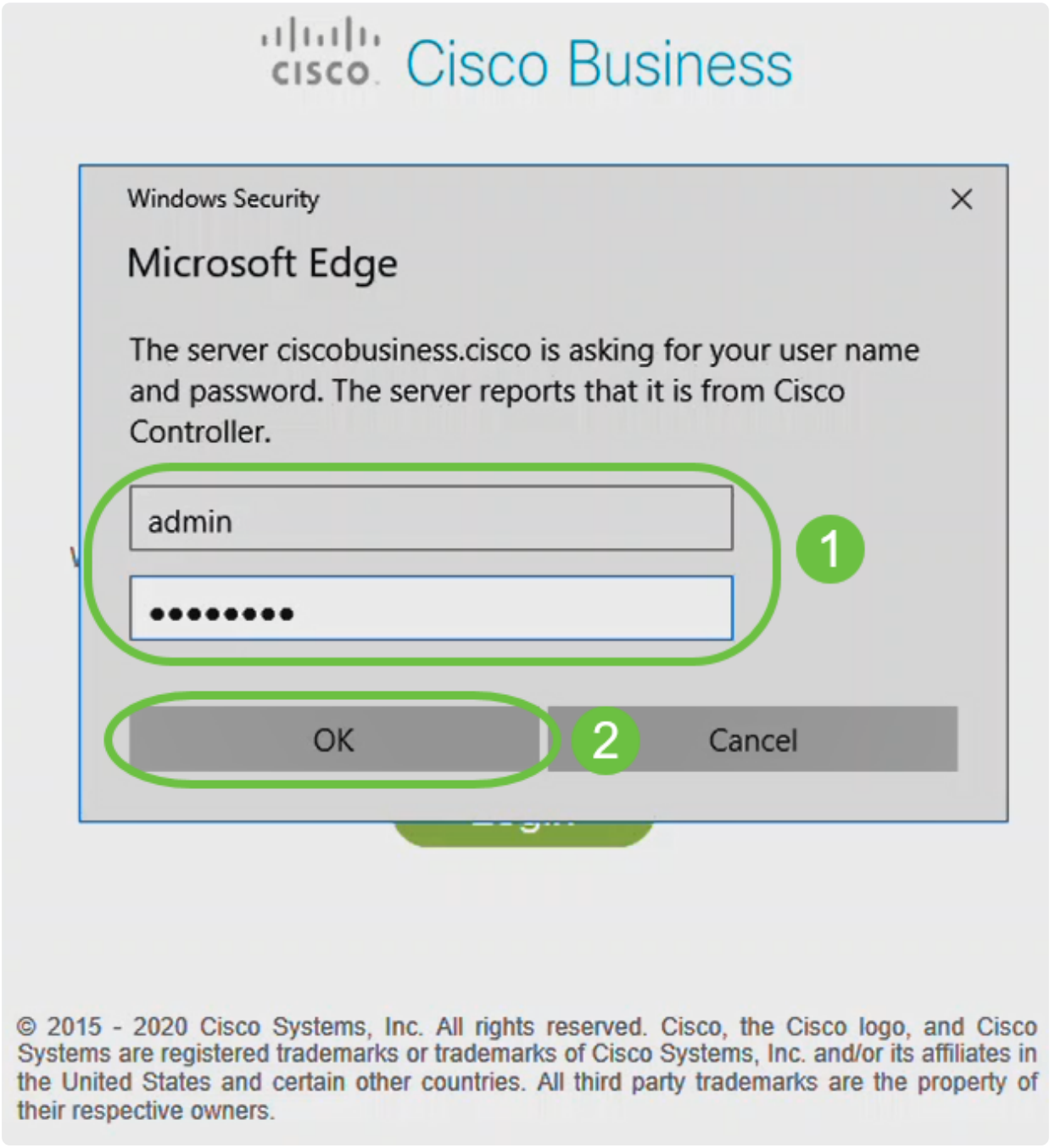
步骤 13

单击 Login。



步骤 14

使用配置的凭证登录。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上的任何VPN。您甚至可能连接到您的移动服务提供商使用的VPN，而您甚至可能不知道。例如，Android(Pixel 3)手机以Google Fi作为服务提供商，有一个内置VPN，可在不通知的情况下自动连接。要查找主AP，需要禁用此功能。
- 使用https://<主AP的IP地址>登录到主AP。
- 完成初始设置后，无论您是登录ciscobusiness.cisco，还是在Web浏览器中输入IP地址，请确保使用https:// is。根据您的设置，您的计算机可能已自动填充了http:// since，这是您首次登录时所用的内容。
- 要帮助解决在使用AP期间与访问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”(Open)菜单，转到“帮助”(Help)>“故障排除信息”(Troubleshooting Information)并单击“刷新Firefox”(Refresh Firefox)。

使用Web UI配置CBW142ACM网状扩展器

您处于设置此网络的主体阶段，只需添加网状扩展器即可！

第 1 步

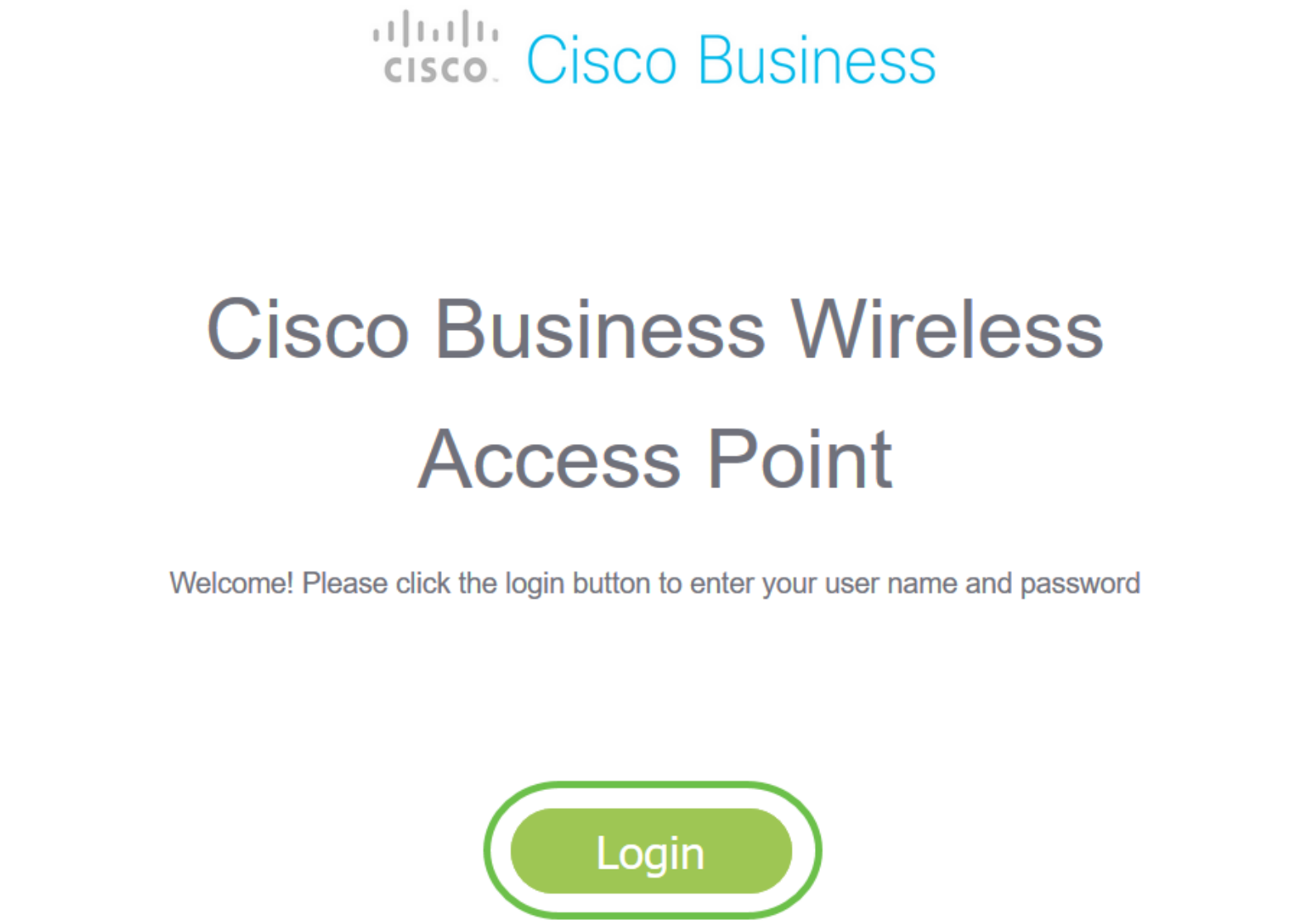
将两个网状扩展器插入所选位置的墙中。记下每个网状网扩展器的MAC地址。

第 2 步

等待约10分钟，以便网状扩展器启动。

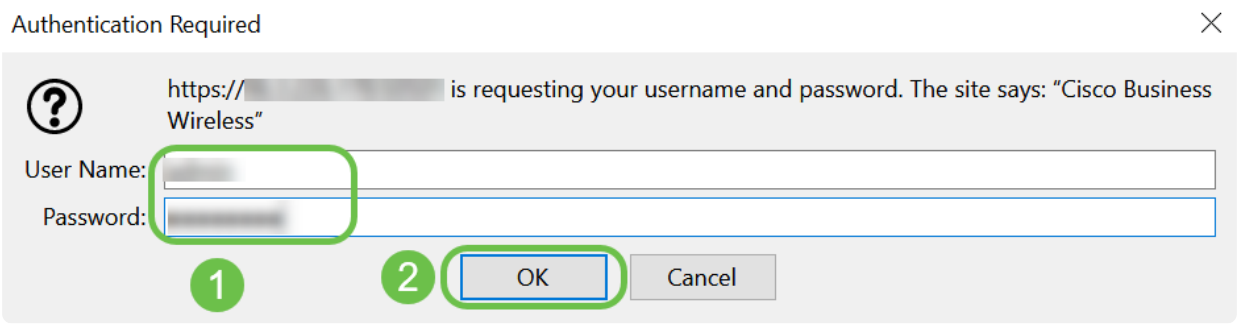
第 3 步

在Web浏览器上输入主接入点(AP)IP地址。单击Login访问主AP。



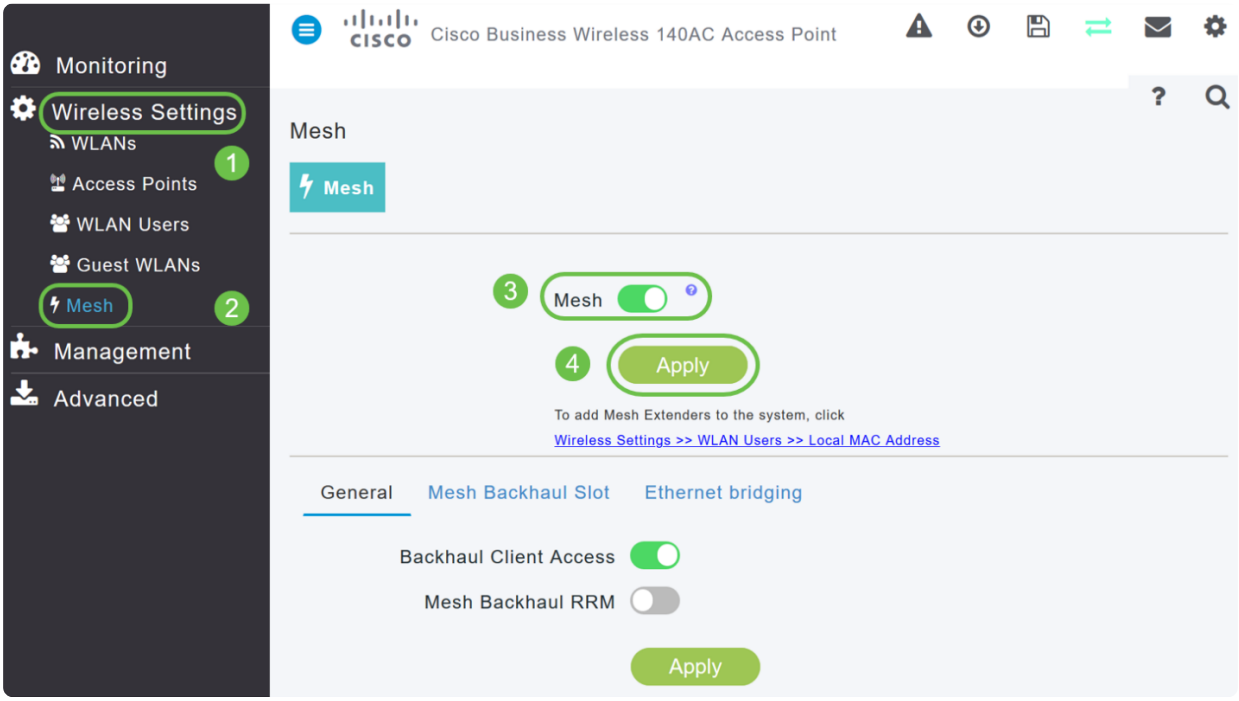
第 4 步

输入您的用户名和密码凭证以访问主AP。Click OK.



步骤 5

导航到无线设置>网状。确保Mesh已启用。单击 Apply。



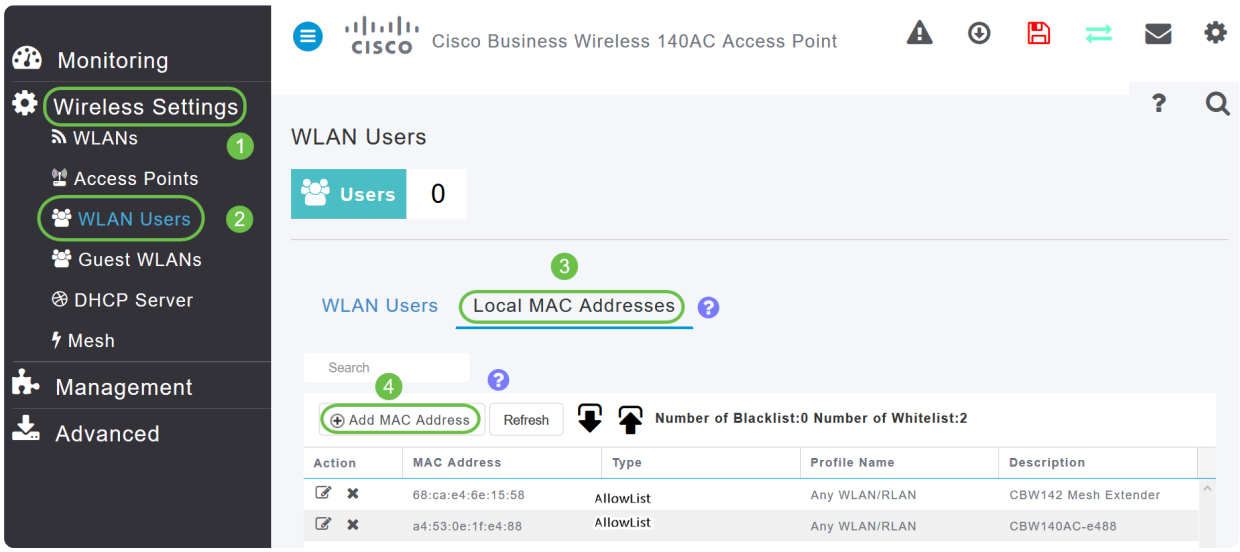
第 6 步

如果网状网络尚未启用，WAP可能需要重新启动。系统将显示一个弹出窗口，用于重新

启动。确认。这大约需要10分钟。在重新启动期间，LED将以多个模式呈绿色闪烁，在再次变为绿色之前，会快速交替显示绿色、红色和琥珀色。LED的颜色强度和色调在单位之间可能有细微的变化。

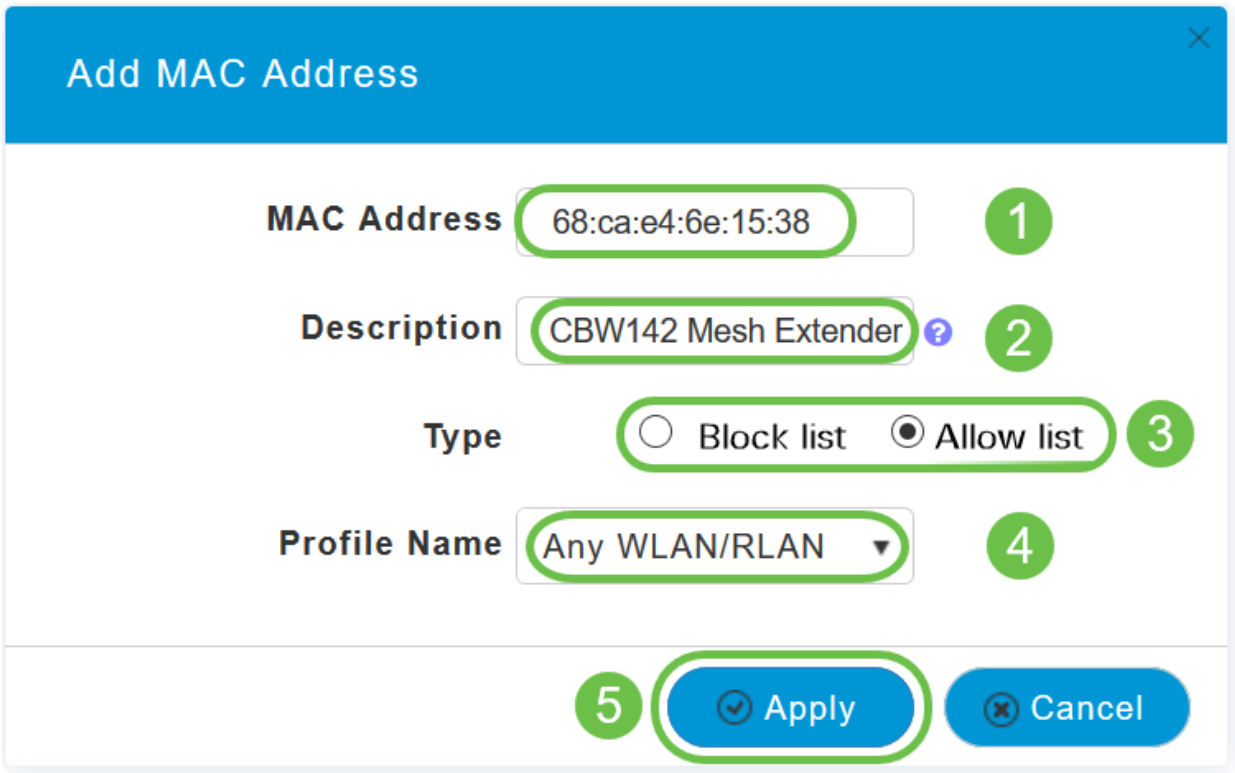
第 7 步

导航到无线设置> WLAN用户>本地MAC地址。单击Add MAC Address。



步骤 8

输入网状网扩展器的MAC地址和说明。选择Type作为Allow列表。从下拉菜单中选择配置文件名称。单击 Apply。



步骤 9

请务必按屏幕右上角窗格上的save图标保存所有配置。



对每个网状扩展器重复上述步骤。

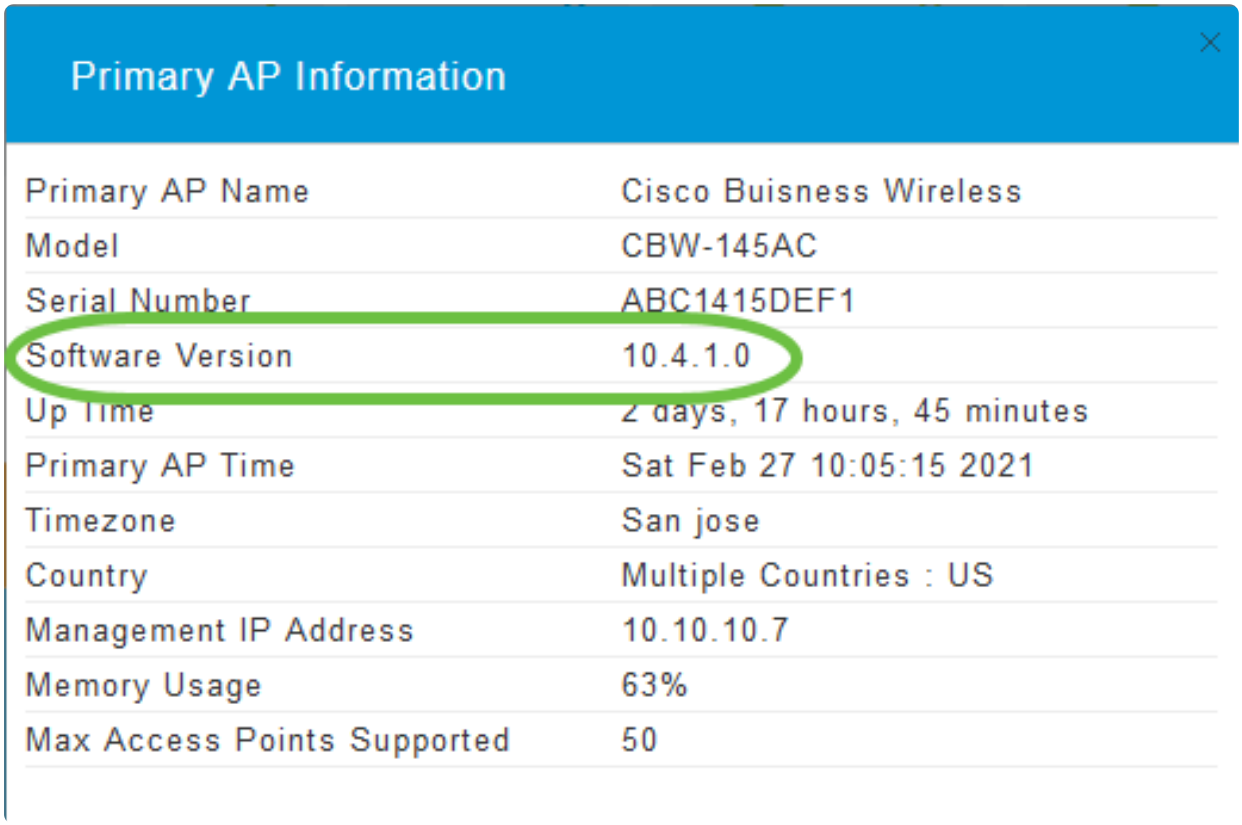
使用Web UI检查和更新软件

不要跳过这一重要步骤！更新软件的方法有很多，但建议您在使用Web UI时最容易执行下面列出的步骤。

要查看和更新您的主AP的当前软件版本，请执行以下步骤。

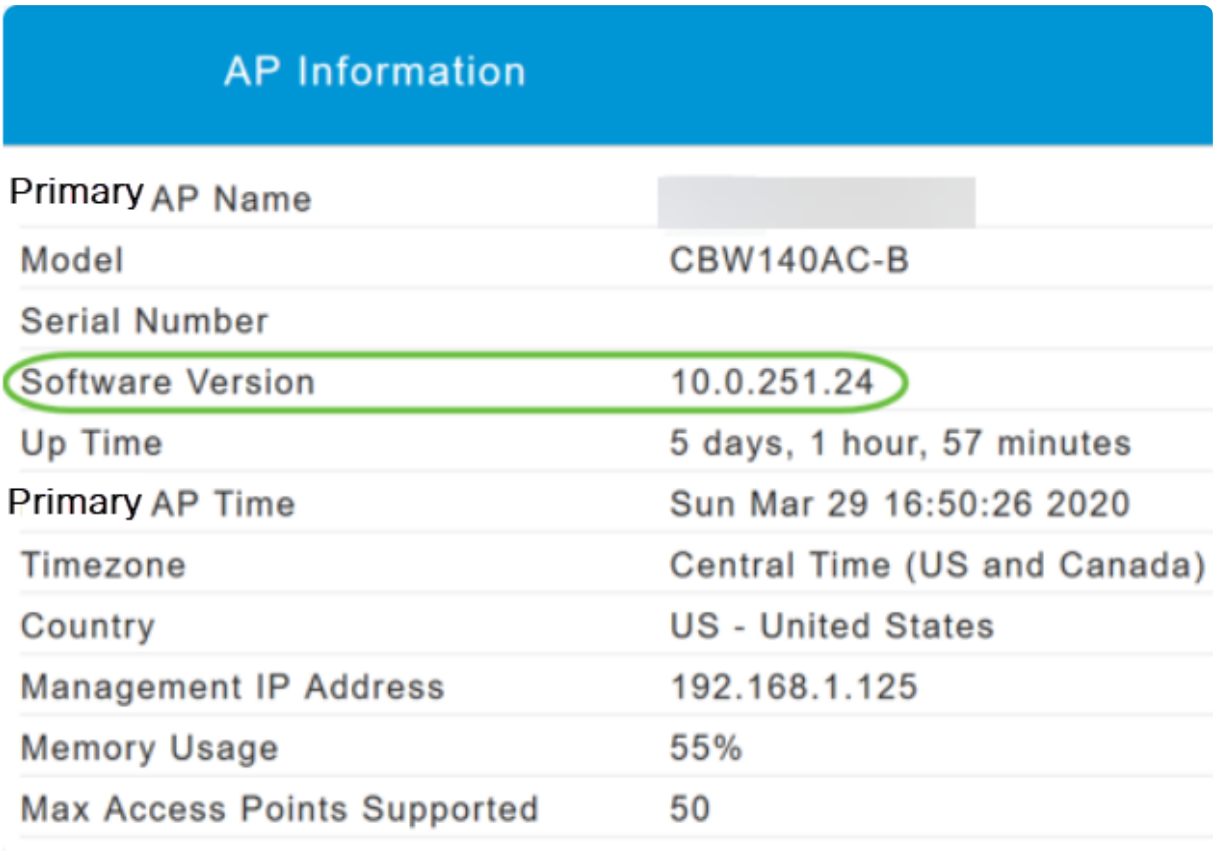
第 1 步

单击Web界面右上角的齿轮图标，然后单击主AP信息。



第 2 步

将运行的版本与最新的软件版本进行比较。如果您知道是否需要更新软件，请关闭窗口。

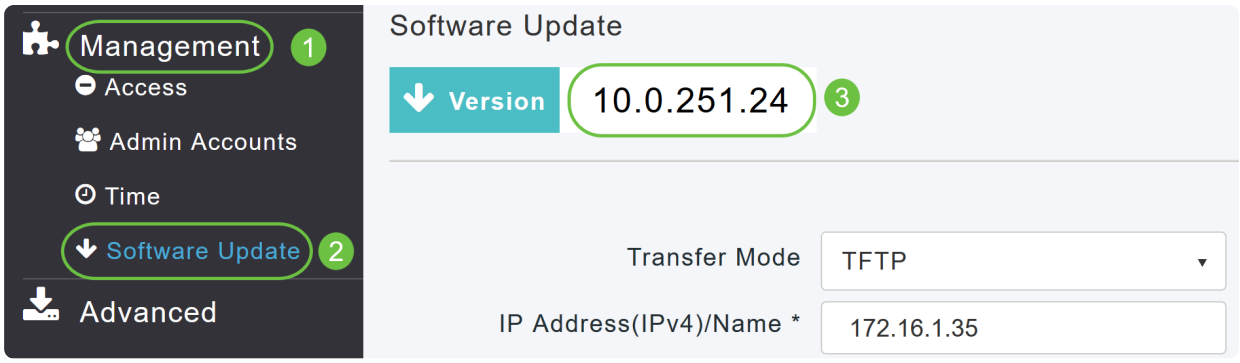


如果您运行的是最新版本的软件，则可以跳至创建WLANs部分。

第 3 步

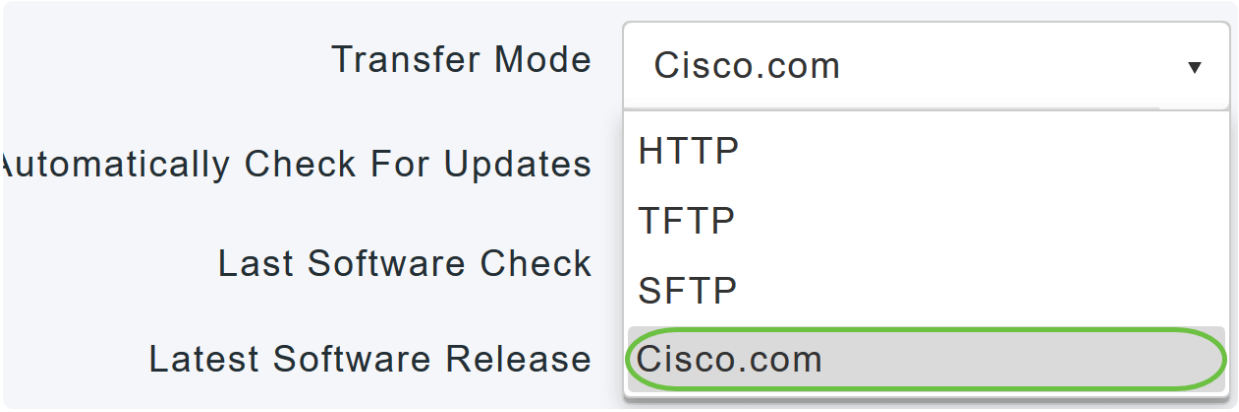
从菜单中选择管理>软件更新。

将显示Software Update窗口，其中当前软件版本号列在顶部。



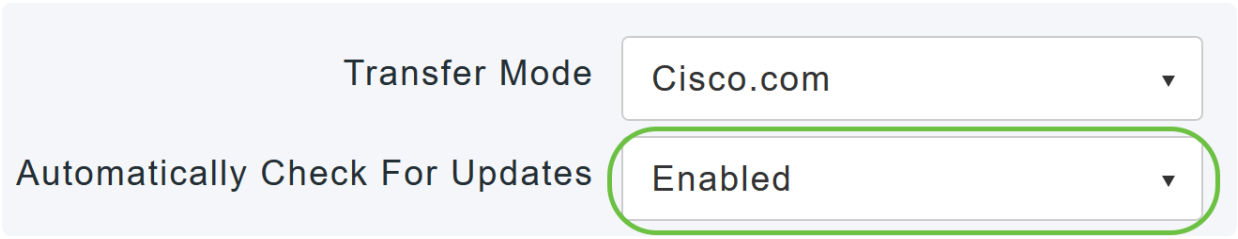
您可以更新CBW AP软件，并且不会删除主AP上的当前配置。

从Transfer Mode下拉列表中，选择Cisco.com。



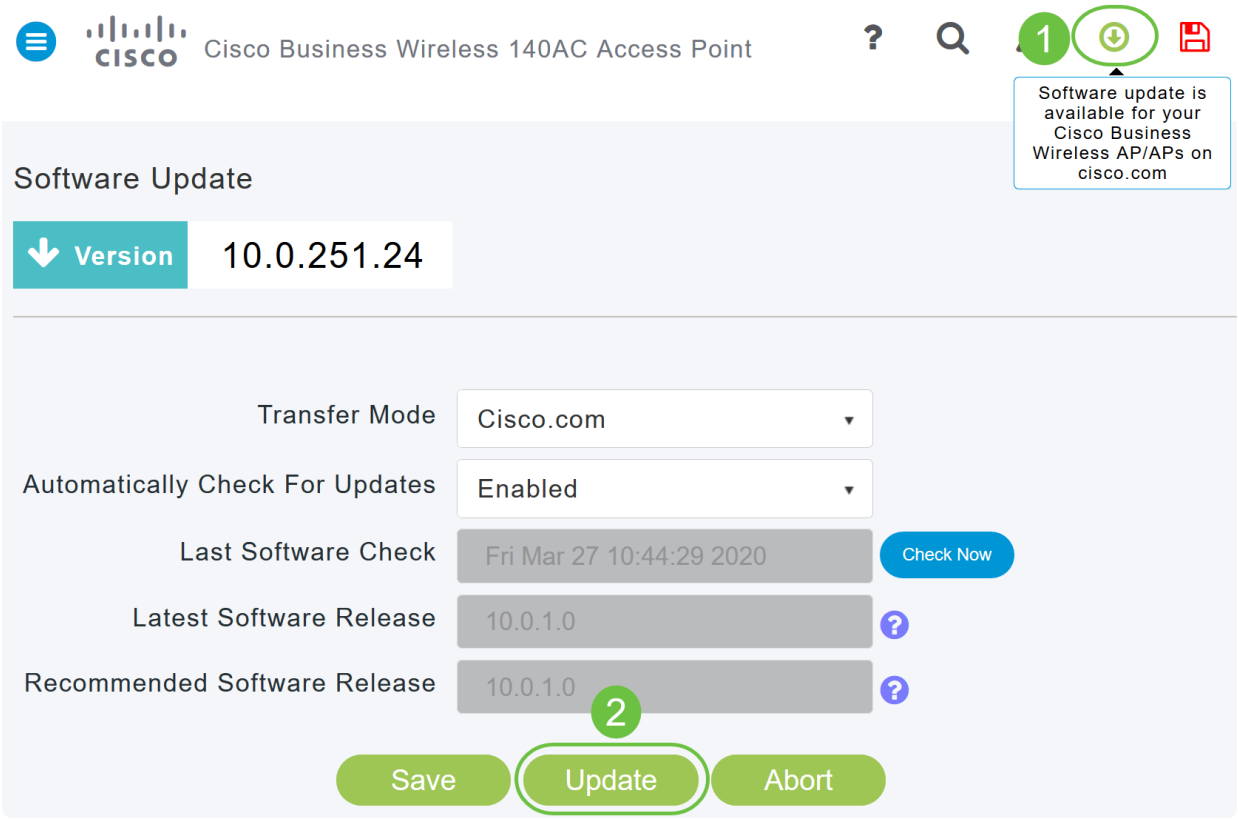
第 4 步

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。



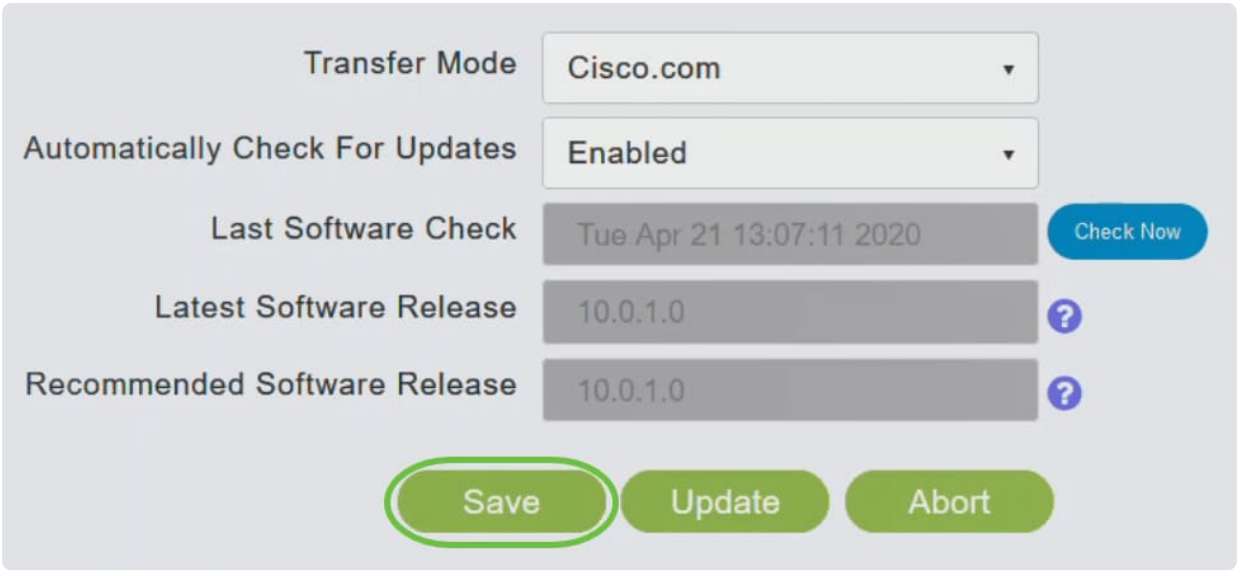
完成软件检查后，如果Cisco.com上提供了更新的最新或推荐的软件更新，则：

- Web UI右上角的Software Update Alert图标为绿色（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Update（更新）按钮处于启用状态。

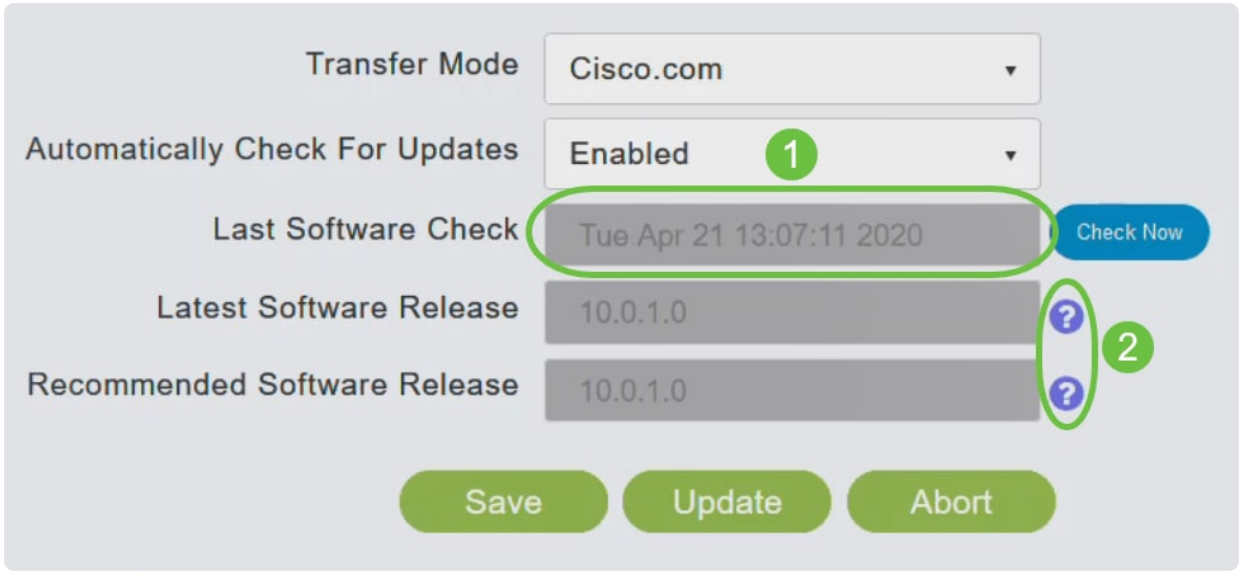


步骤 5

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。

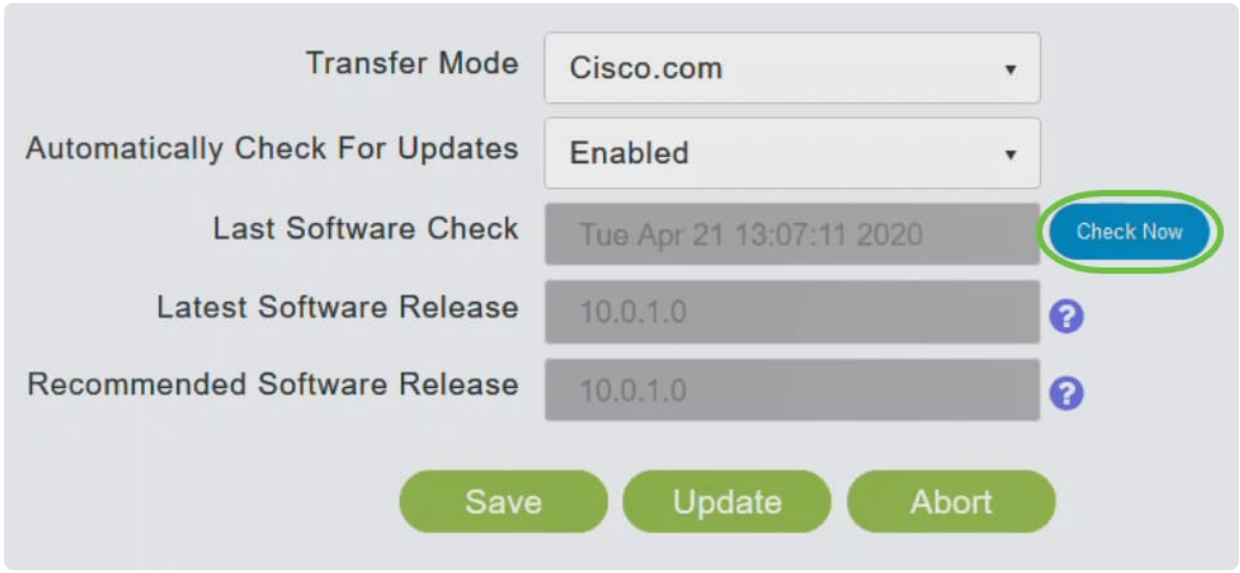


Last Software Check字段显示上次自动或手动软件检查的时间戳。您可以点击显示的版本旁的问号图标查看版本注释。



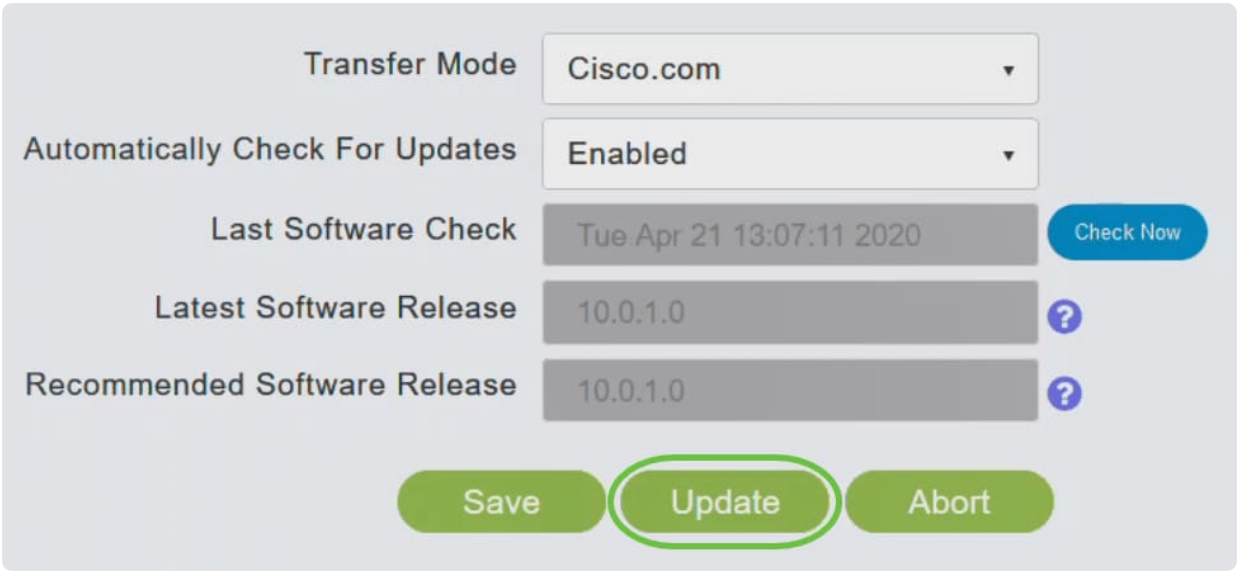
第 6 步

您可以随时单击Check Now手动运行软件检查。



第 7 步

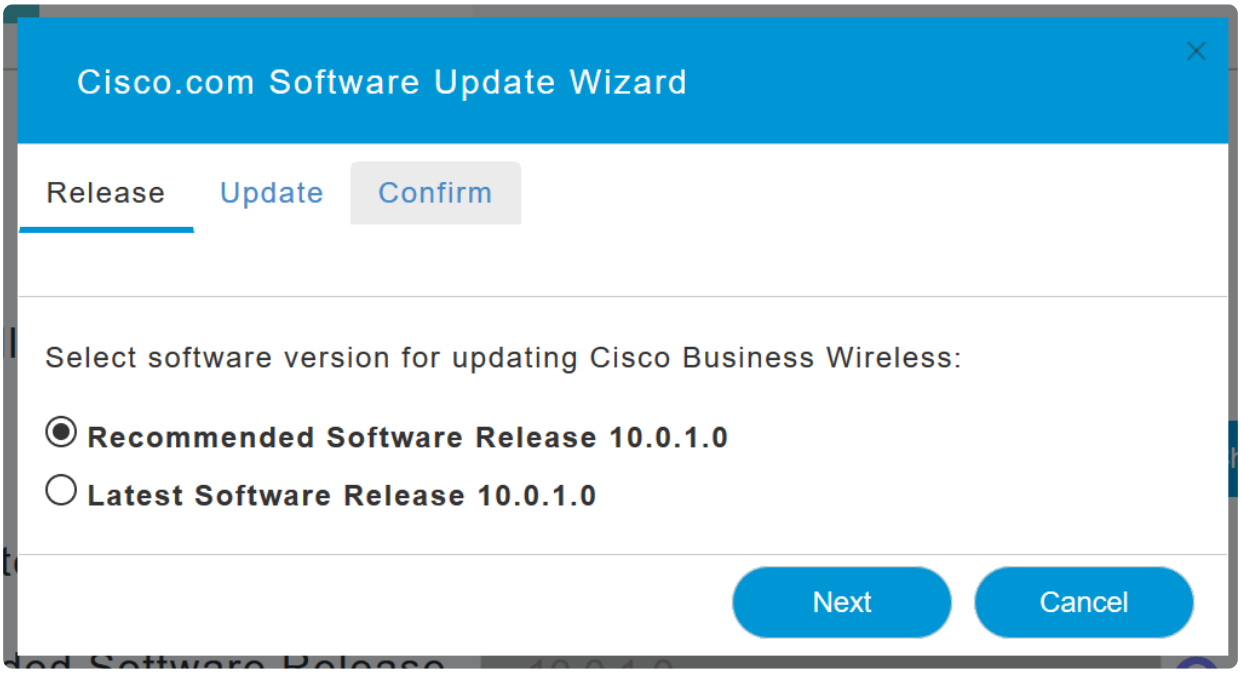
要继续软件更新，请单击Update。



系统将显示软件更新向导。向导会按顺序引导您完成以下三个选项卡：

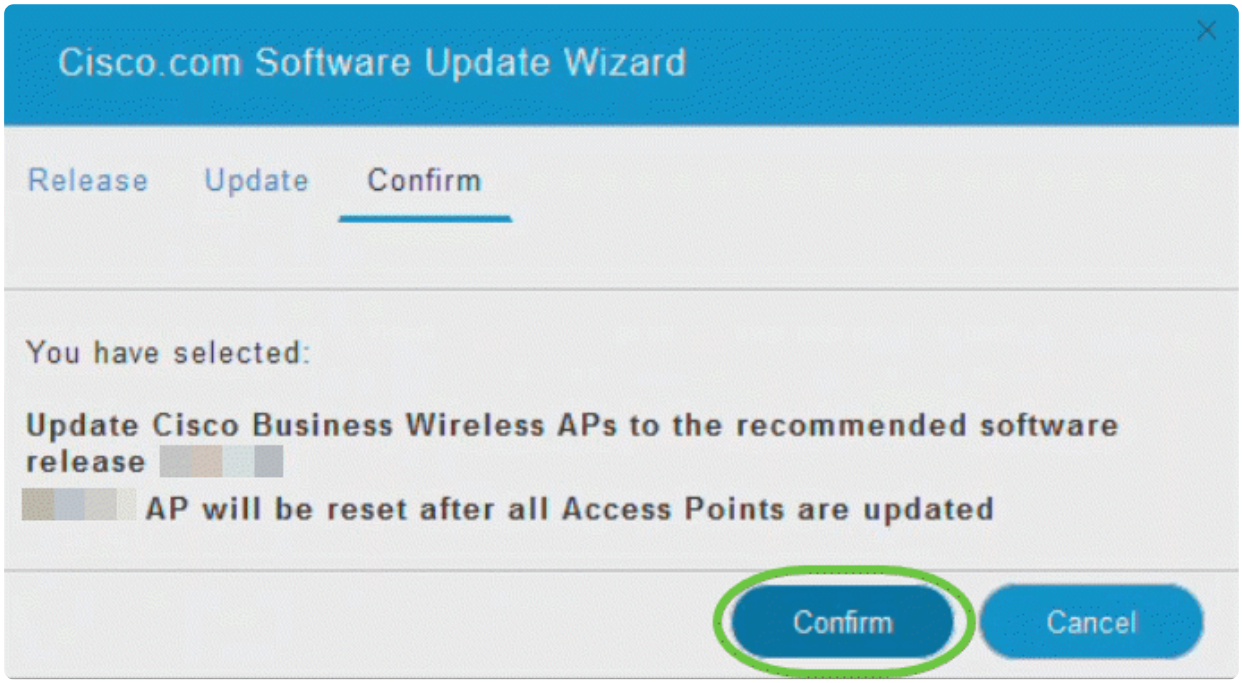
- Release（版本）选项卡 — 指定是要更新到推荐的软件版本还是最新软件版本。
- Update选项卡 — 指定应重置AP的时间。您可以选择立即完成，也可以将其安排在以后进行。要将主AP设置为在映像预下载完成后自动重新启动，请选中Auto Restart复选框。
- “确认”选项卡 — 确认您的选择。

按照向导中的说明进行操作。在单击Confirm之前，您可以随时返回至任何选项卡。



步骤 8

单击Confirm。



在Web UI上创建WLAN

此部分允许您创建无线局域网(WLAN)。

第 1 步

通过导航到无线设置> WLANs可以创建WLAN。然后选择Add new WLAN/RLAN。



第 2 步

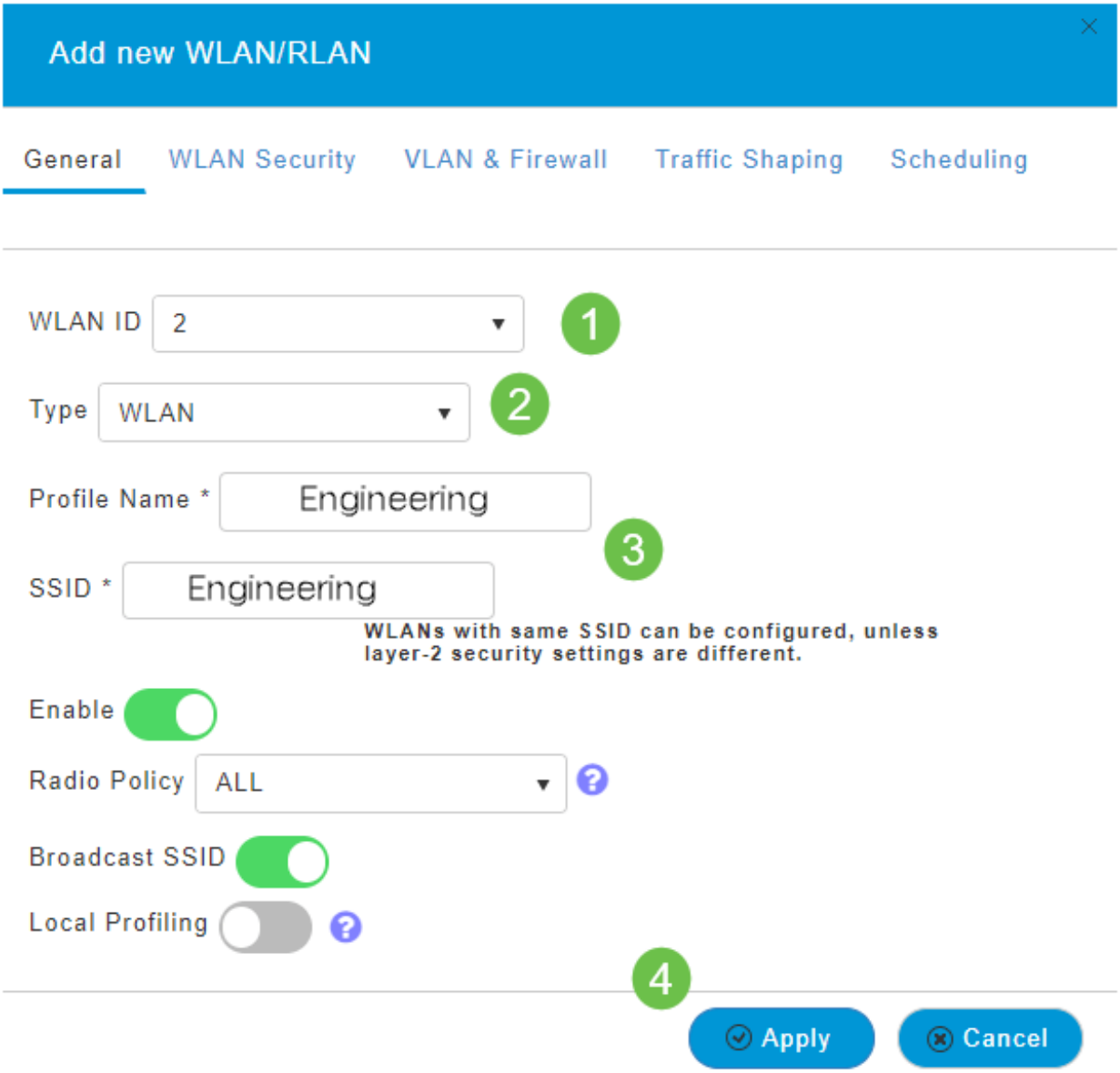
在General选项卡下，输入以下信息：

- WLAN ID — 为WLAN选择一个数字
- 类型 — 选择WLAN
- 配置文件名称 — 当您输入名称时，SSID将自动填充相同的名称。名称必须唯一，且不能超过31个字符。

以下字段在本示例中保留为默认值，但会列出说明，以便您以不同方式配置它们。

- SSID — 配置文件名称也用作SSID。如果需要，您可以更改此项。名称必须唯一，且不能超过31个字符。
- Enable — 应保持启用状态以使WLAN正常工作。
- Radio Policy（无线电策略）— 通常希望将此选项保留为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。
- Local Profiling — 您只需要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。



第 3 步

您将进入WLAN安全选项卡。

在本示例中，以下选项保留为默认值：

- 访客网络、强制网络助理和MAC过滤处于禁用状态。有关设置访客网络的详细信息将在下一部分中详细介绍。
- WPA2 Personal - Wi-Fi Protected Access 2 with Pre-shared Key(PSK)Passphrase Format - ASCII。此选项表示使用预共享密钥(PSK)的Wi-Fi保护访问2。

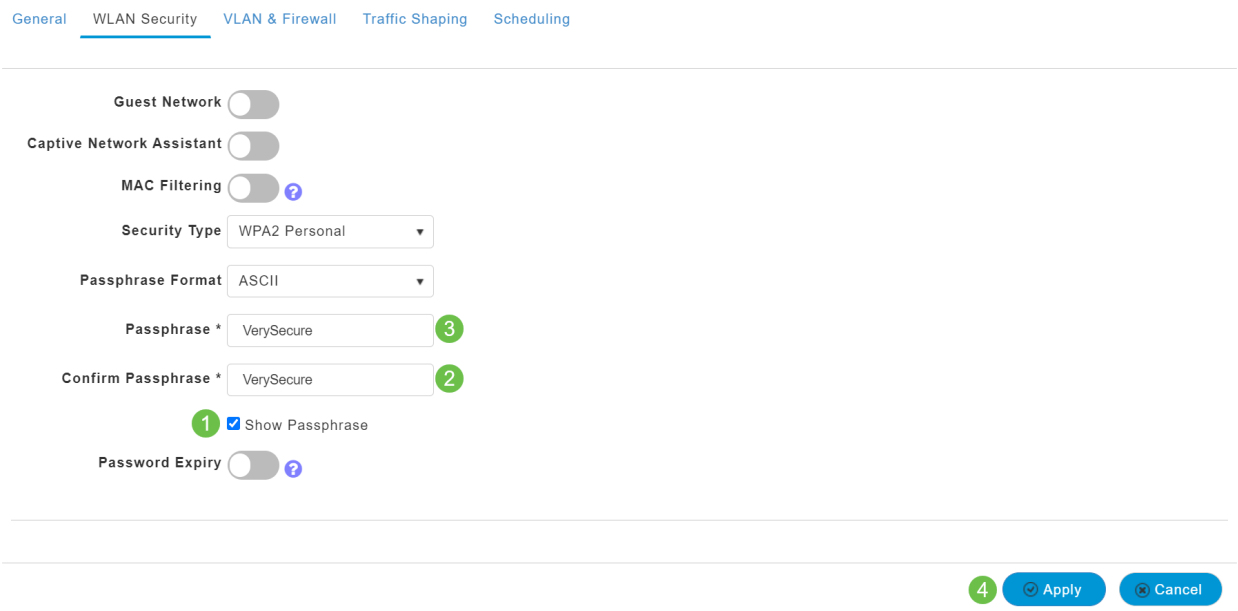
WPA2 Personal是使用PSK身份验证来保护网络的方法。PSK在主AP、WLAN安全策略下和客户端上分别配置。WPA2 Personal不依赖于网络上的身份验证服务器。

- 口令格式- ASCII保留为默认值。

在此场景中输入了以下字段：

- 显示口令 — 单击复选框可查看您输入的口令。
- 密码短语 — 输入密码短语的名称（密码）。
- 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。



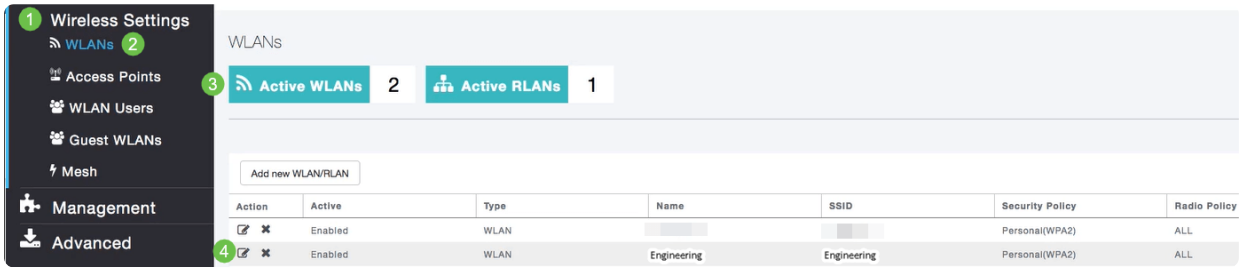
第 4 步

请务必通过单击Web UI屏幕右上角面板上的save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数增加到2，并显示新的WLAN。



对要创建的其他WLAN重复这些步骤。

可选无线配置

现在已设置所有基本配置，可以开始滚动了。您有一些选项，因此您可以跳至以下任何部分：

- 使用Web UI创建访客WLAN（可选）
- 应用分析（可选）
- 客户端分析（可选）
- 我准备就绪，可以开始使用我的网络了！

使用Web UI创建访客WLAN（可选）

访客WLAN允许访客访问您的思科企业无线网络。

第 1 步

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

第 2 步

通过导航到无线设置> WLAN可以创建无线局域网(WLAN)。然后选择Add new WLAN/RLAN。



第 3 步

在General选项卡下，输入以下信息：

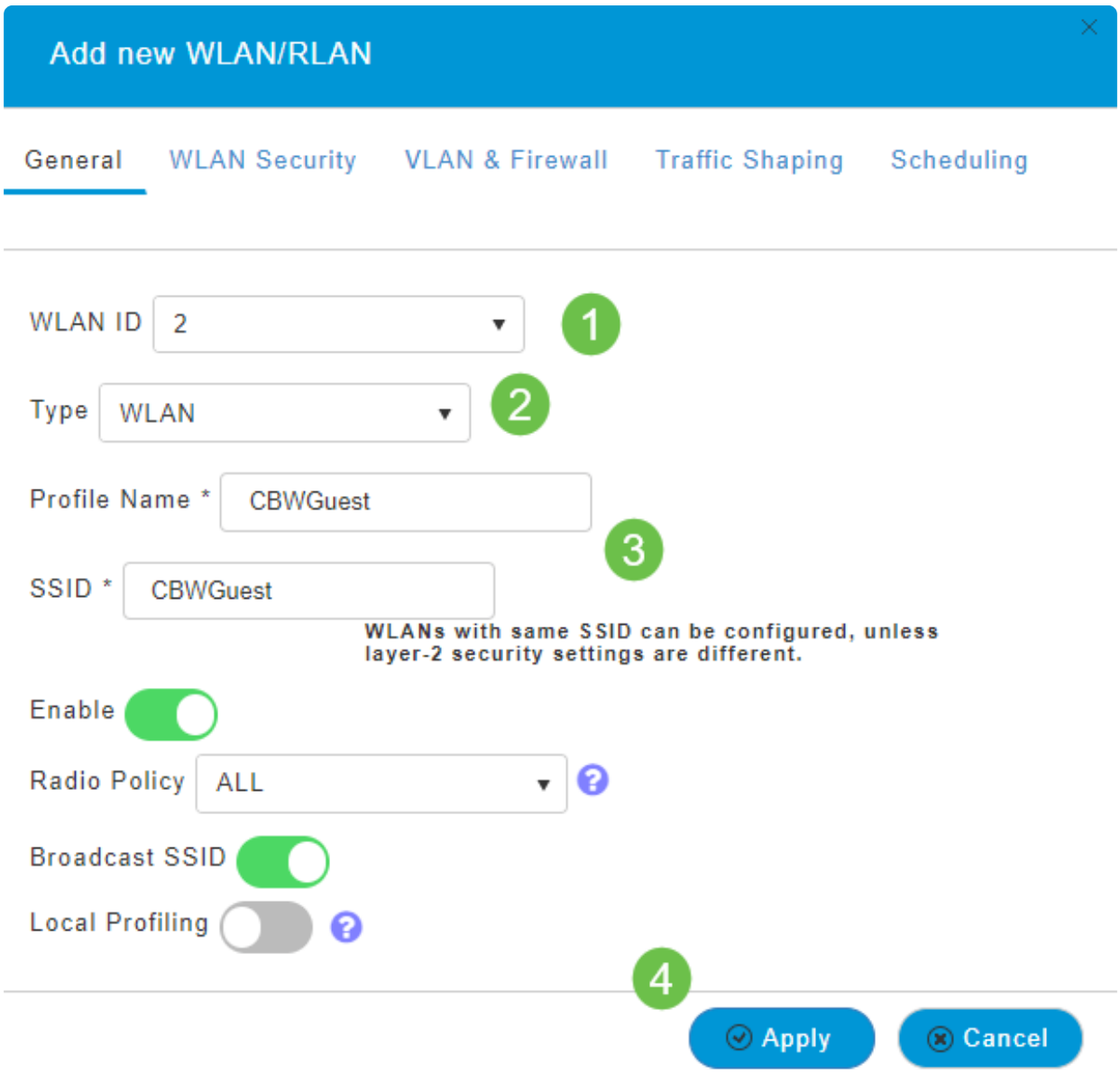
- WLAN ID — 为WLAN选择一个数字
- 类型 — 选择WLAN
- 配置文件名称 — 当您输入名称时，SSID将自动填充相同的名称。名称必须唯一，且不能超过31个字符。

以下字段在本示例中保留为默认值，但会列出说明，以便您以不同方式配置它们。

- SSID — 配置文件名称也用作SSID。如果需要，您可以更改此项。名称必须唯一，且不能超过31个字符。
- Enable — 应保持启用状态以使WLAN正常工作。

- Radio Policy — 通常，您可能希望将其保留为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“启用”。
- Local Profiling — 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。

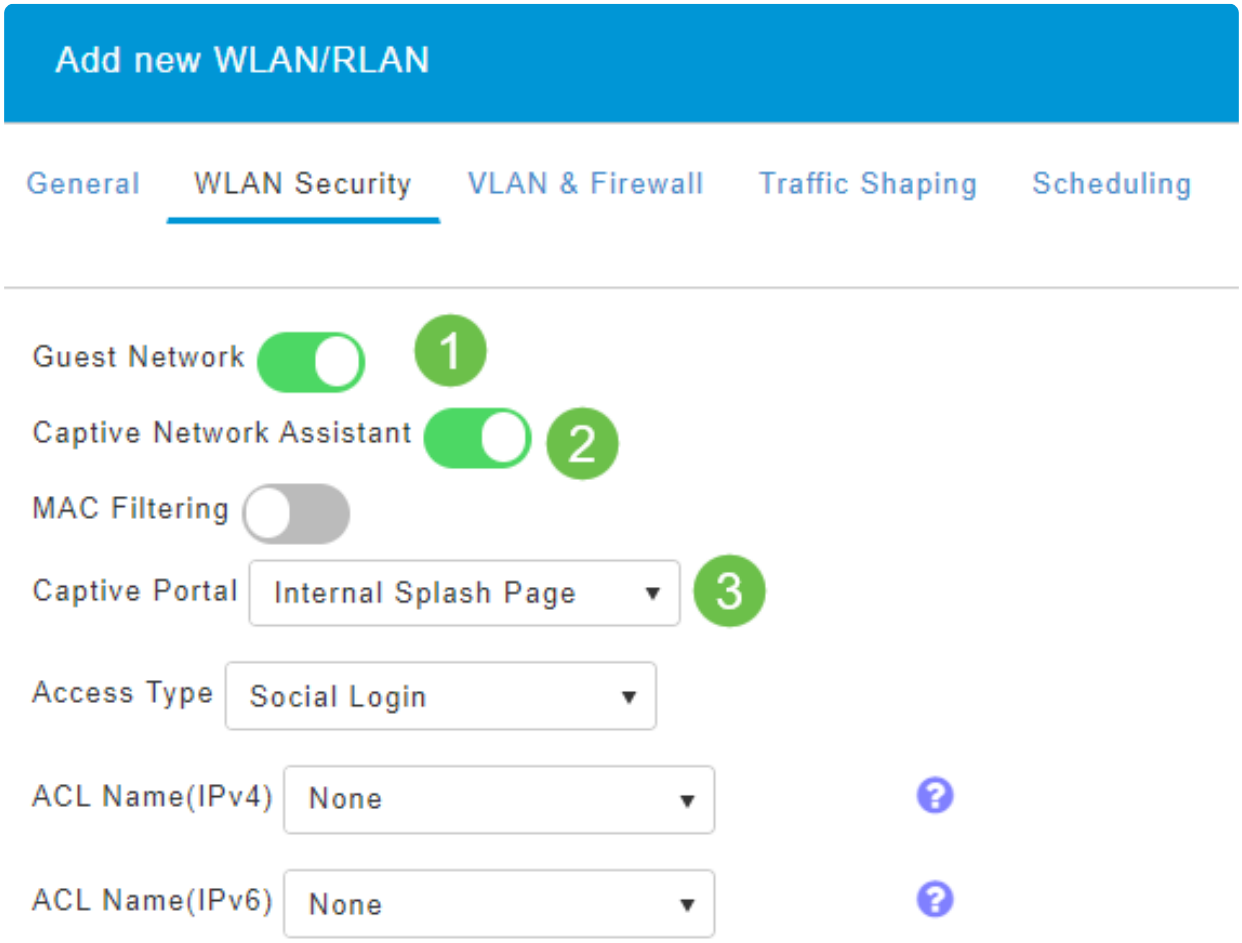
单击 Apply。



第 4 步

您将进入WLAN安全选项卡。在本示例中，选择了以下选项。

- 访客网络 — 启用
- Captive Network Assistant — 如果您使用Mac或IOS，您可能要启用它。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的存在。此请求被定向到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)自动启动伪浏览器以请求在受控窗口中登录门户。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阻止此伪浏览器弹出。
- 强制网络门户 — 此字段仅在启用“访客网络”(Guest Network)选项时可见。这用于指定可用于身份验证目的的Web门户的类型。选择Internal Splash Page以使用默认基于Cisco Web门户的身份验证。如果您要使用网络外部的Web服务器进行强制网络门户身份验证，请选择External Splash Page。此外，在Site URL字段中指定服务器的URL。



在本示例中，将创建已启用社交登录访问类型的访客WLAN。用户连接到此访客WLAN后，将被重定向到Cisco默认登录页面，在该页面上可以找到Google和Facebook的登录按钮。用户可以使用其Google或Facebook帐户登录以访问Internet。

步骤 5

在此选项卡上，从下拉菜单中选择Access Type。在本示例中，选择了Social Login。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。

Access Type的其他选项包括：

- 本地用户帐户 — 默认选项。选择此选项可使用您在Wireless Settings > WLAN Users下为此WLAN的访客用户指定的用户名和密码对访客进行身份验证。这是默认内部启动页的示例。



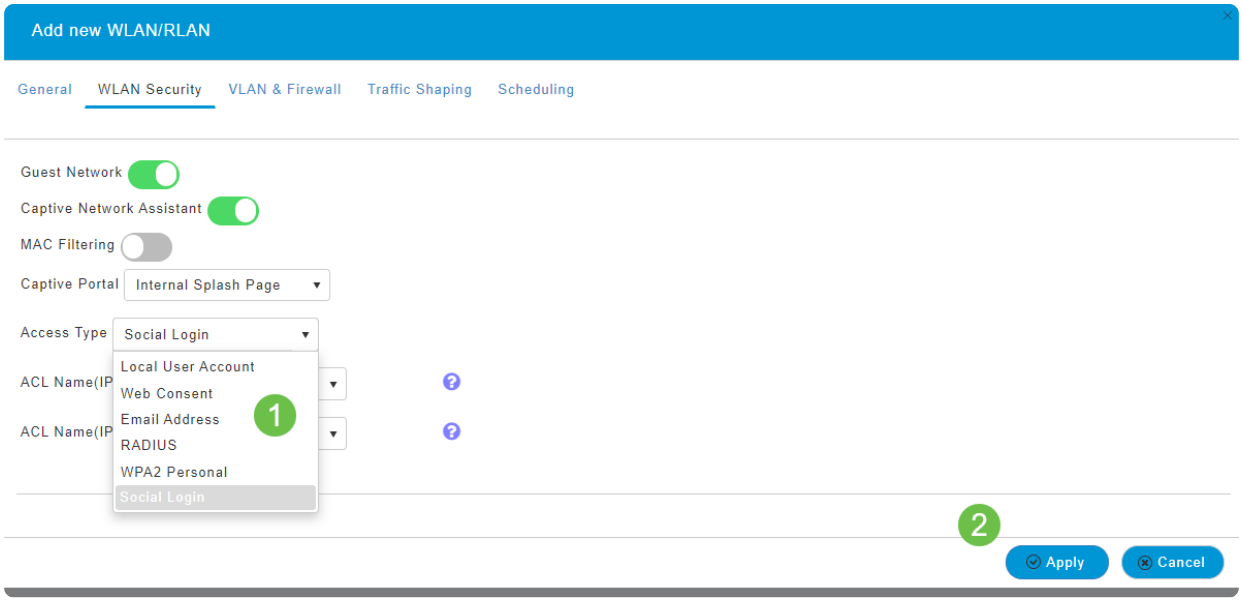
您可以通过导航到Wireless Settings > Guest WLANs来自定义此设置。在此处可输入页面标题和页面消息。单击 Apply。单击Preview。

- Web Consent — 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。

- 电邮地址 — 访客用户需要输入其电邮地址才能访问网络。
- RADIUS -将其用于外部身份验证服务器。
- WPA2个人 — 使用预共享密钥(PSK)的Wi-Fi保护访问2

单击 Apply。



第 6 步

请务必通过单击Web UI屏幕右上角面板上的save图标来保存配置。



现在，您已经创建了一个访客网络，该网络在CBW网络上可用。客人将非常享受便利。

使用Web UI进行应用分析（可选）

分析是启用组织策略功能的子集。它允许您匹配流量类型并确定其优先级。就像规则决定如何排列或丢弃流量一样。Cisco Business Mesh Wireless系统具有客户端和应用分析功能。用户访问网络的行为始于许多信息交换，其中信息是流量的类型。策略会中断流量来指导路径，就像流程图一样。其他类型的策略功能包括 — 访客接入、访问控制列表和QoS。

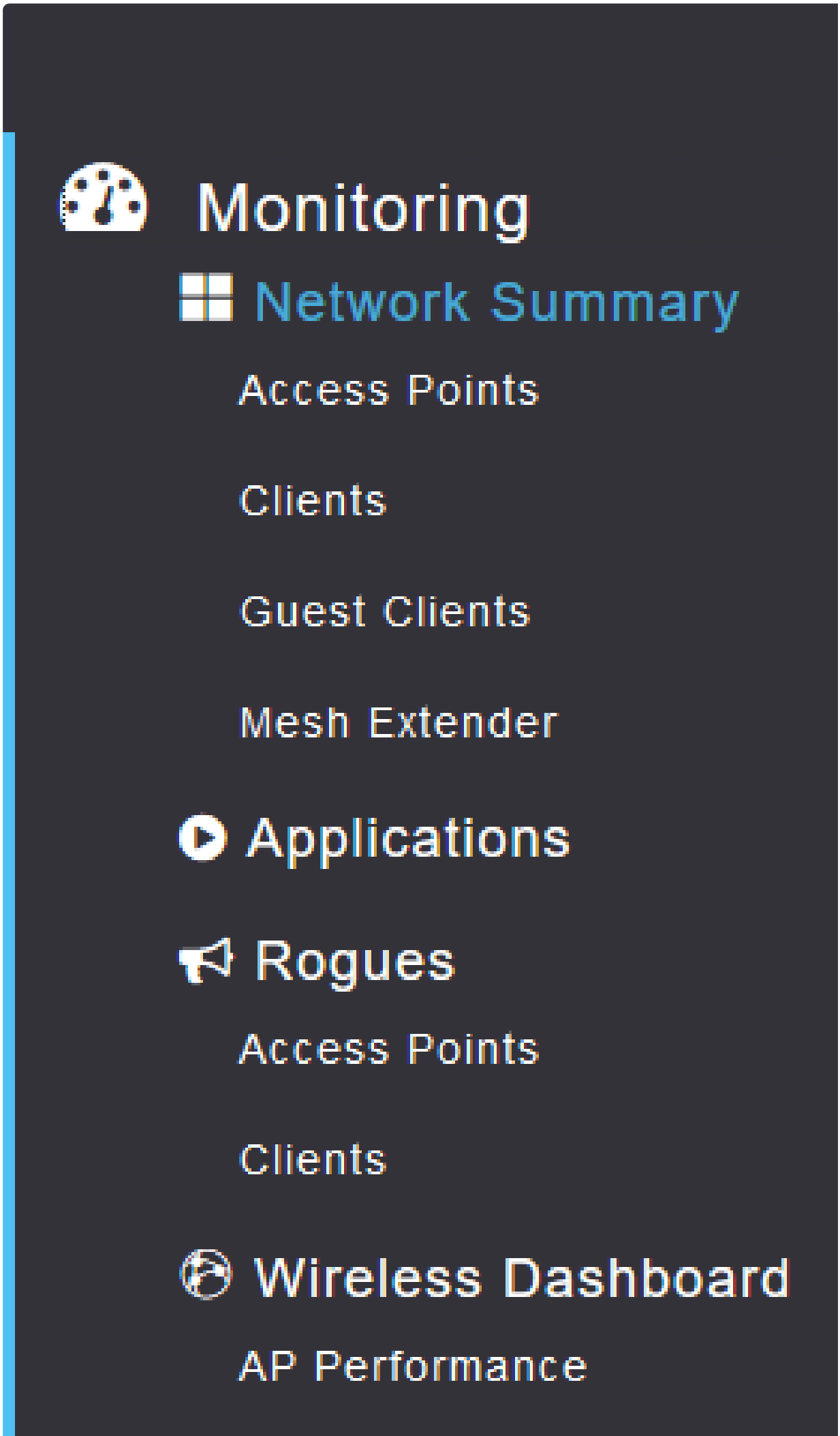
第 1 步

如果未看到左侧菜单栏，请导航到屏幕左侧的菜单。

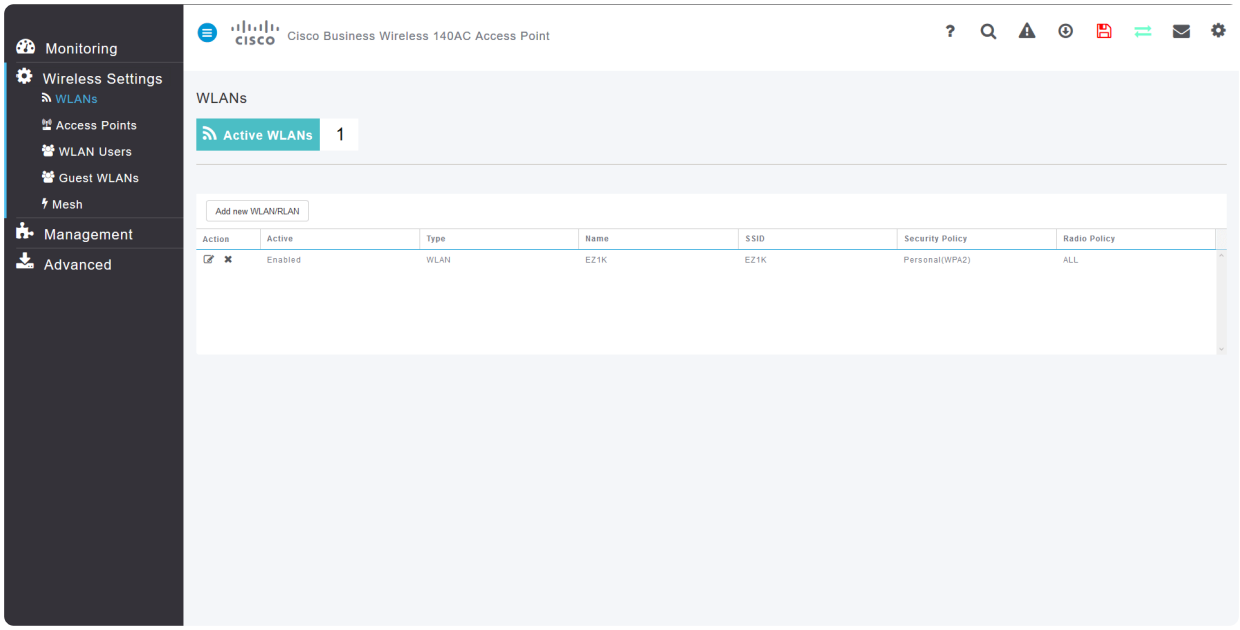


第 2 步

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

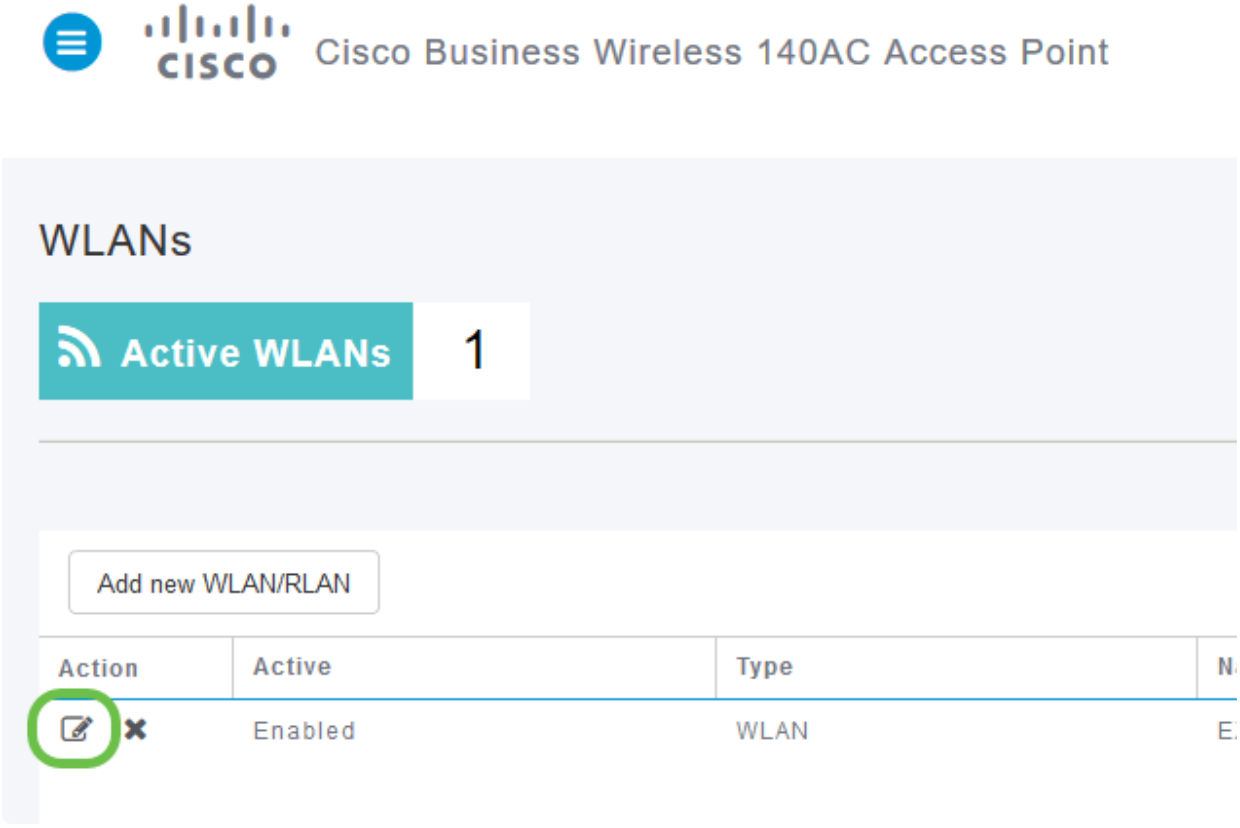

Monitoring
Network Summary
Access Points
Clients
Guest Clients
Mesh Extender
Applications
Rogues
Access Points
Clients
Wireless Dashboard
AP Performance

下图与您点击Wireless Settings（无线设置）链接时看到的内容相似。

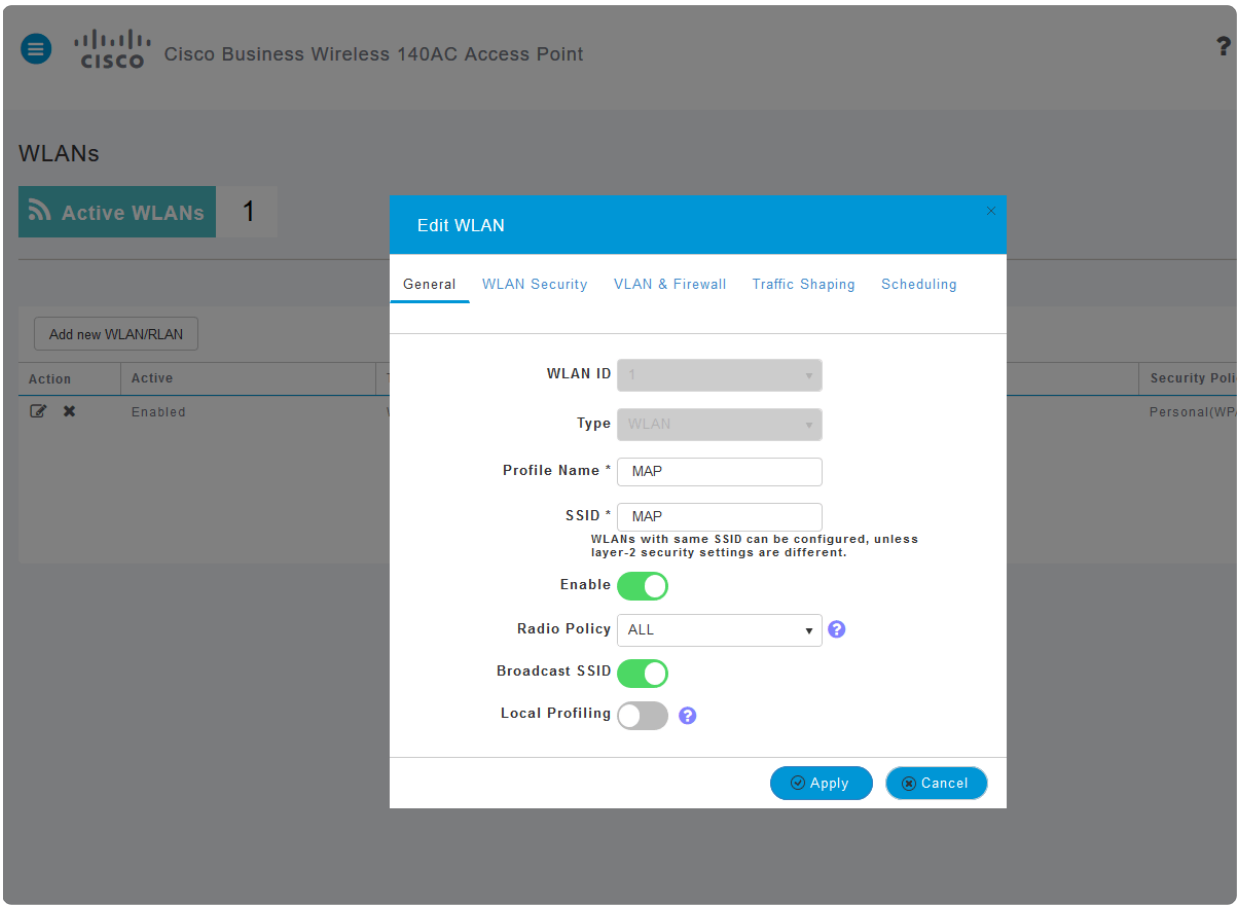


第 3 步

点击要启用应用的无线局域网左侧的编辑图标。

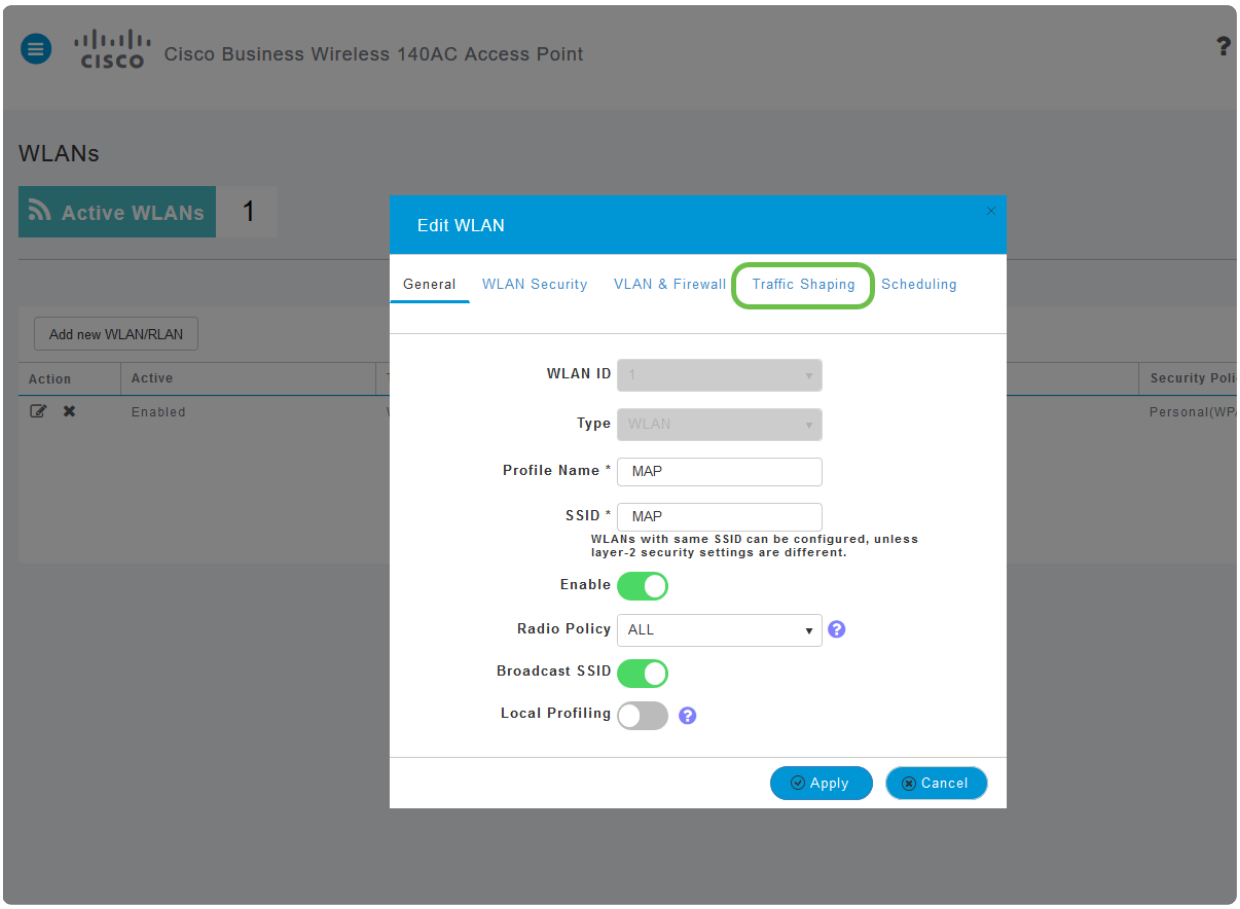


由于您最近添加了WLAN，您的Edit WLAN页面可能如下所示：

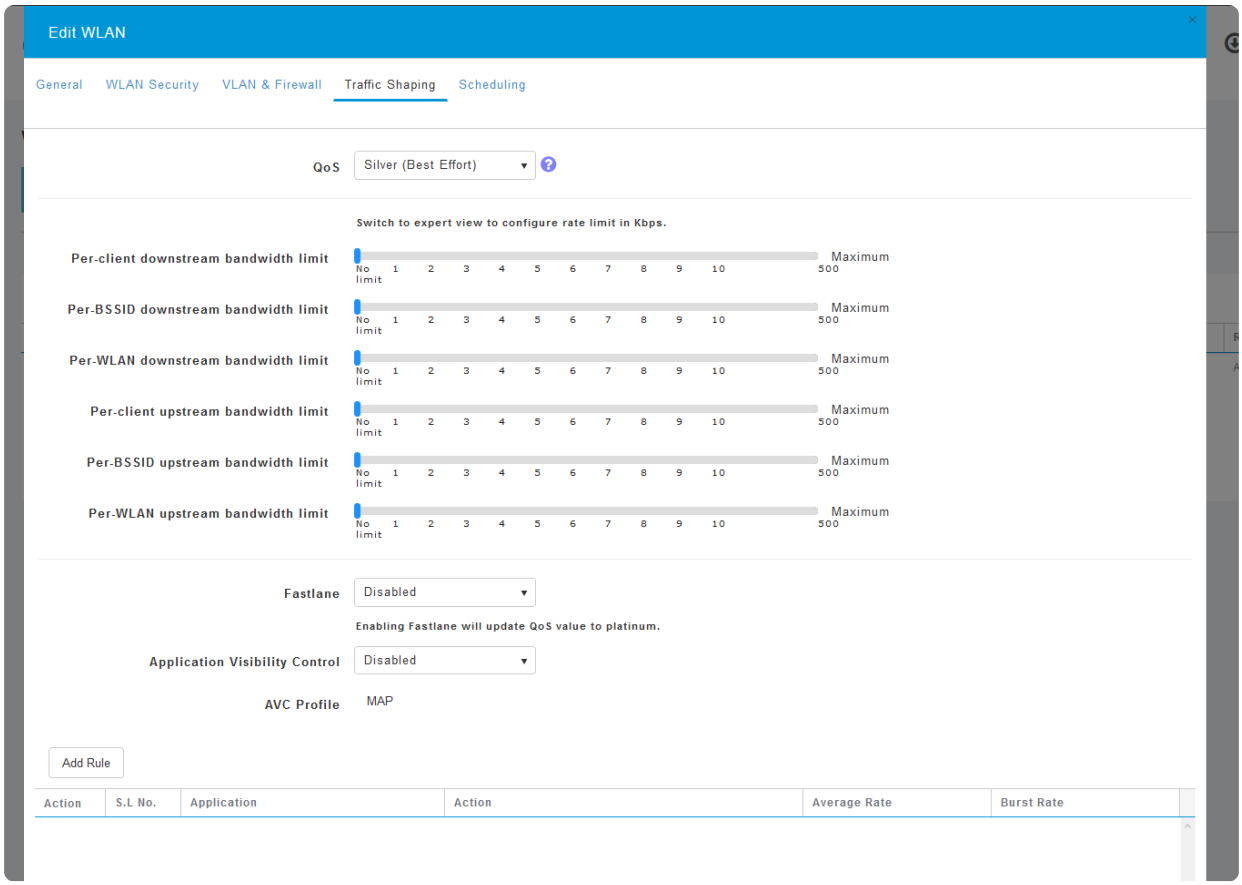


第 4 步

单击导航到流量整形(Traffic Shaping)选项卡。

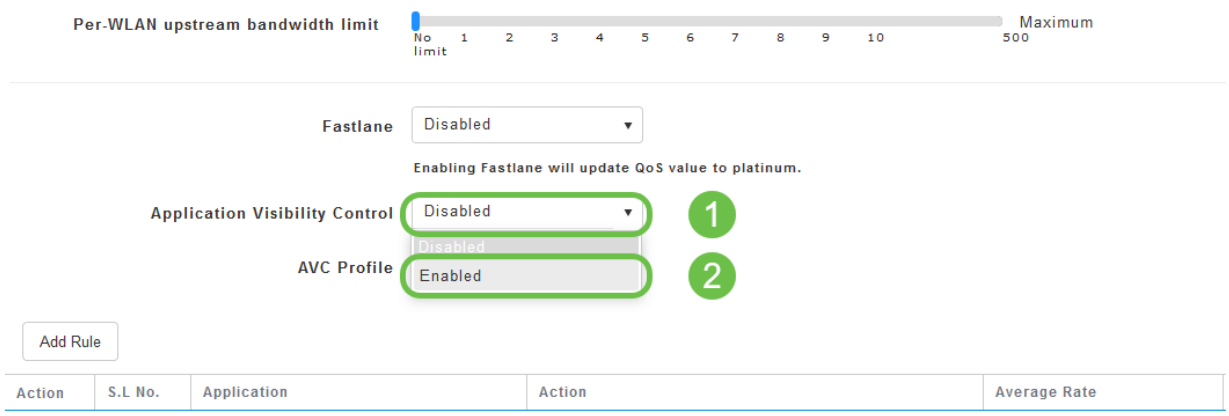

Cisco Business Wireless 140AC Access Point
WLANs
Active WLANs 1
Add new WLAN/RLAN
Action
Active
Enabled
Edit WLAN
General
WLAN Security
VLAN & Firewall
Traffic Shaping
Scheduling
WLAN ID 1
Type WLAN
Profile Name * MAP
SSID * MAP
WLANs with same SSID can be configured, unless layer-2 security settings are different.
Enable
Radio Policy ALL
Broadcast SSID
Local Profiling
Apply
Cancel

屏幕可能显示如下：



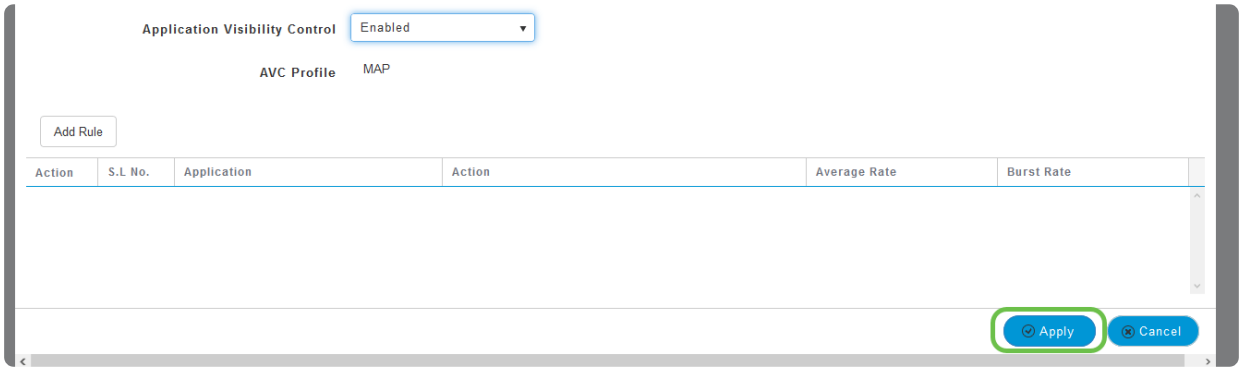
步骤 5

在页面底部，您可以找到应用可视性控制功能。默认情况下，此选项处于禁用状态。单击下拉列表并选择启用。



第 6 步

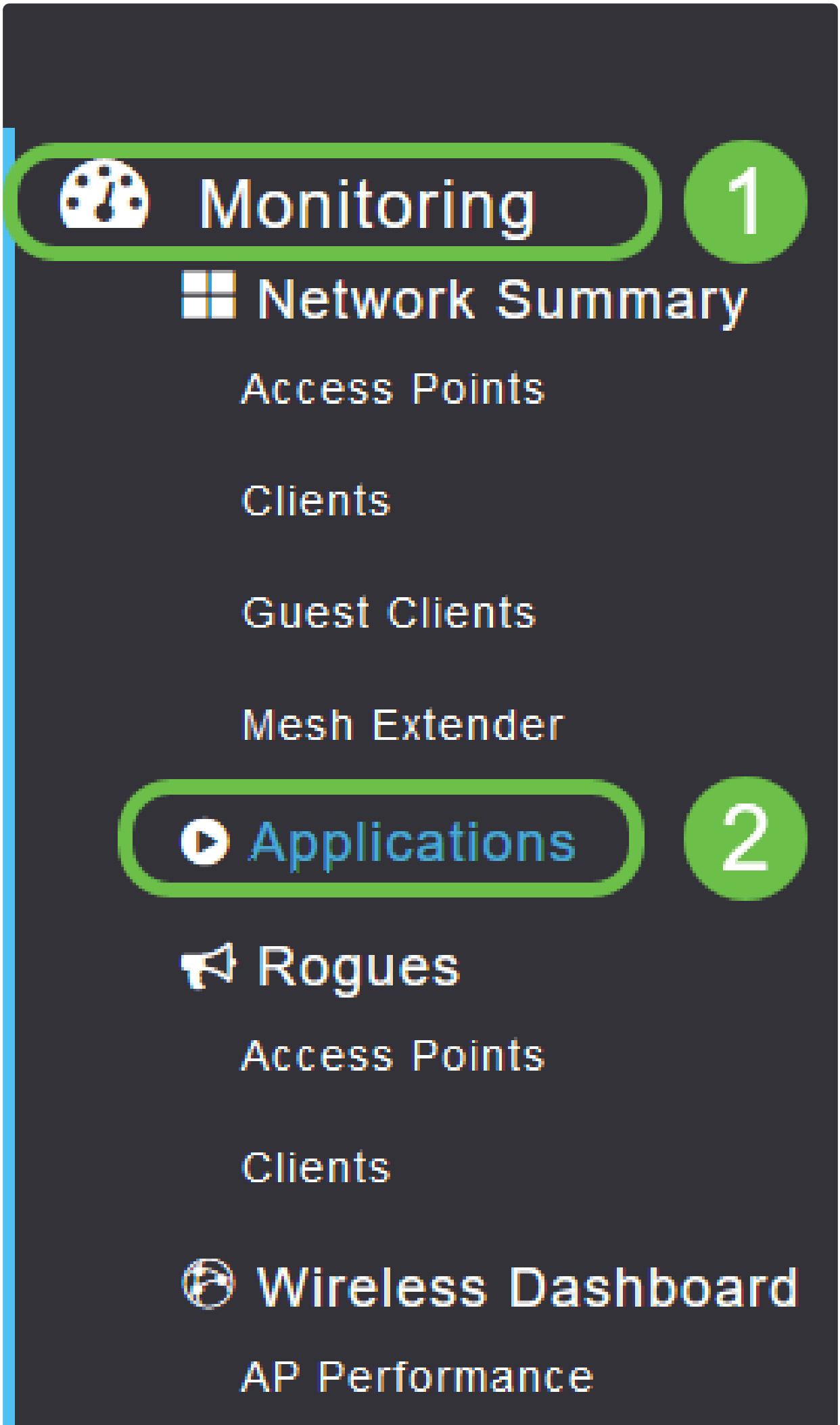
单击应用按钮.



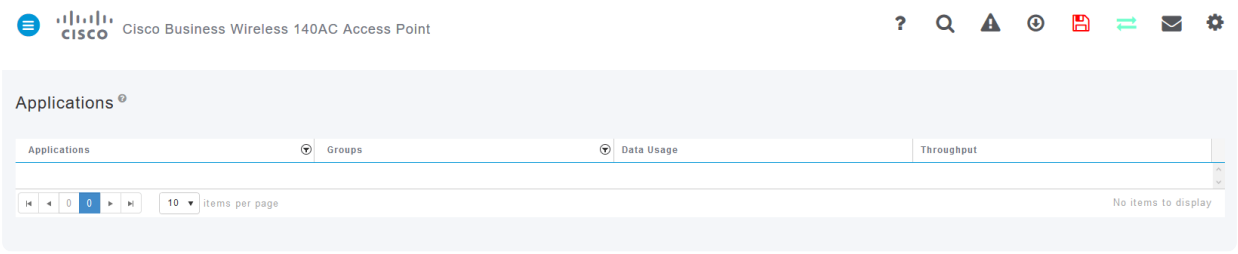
必须启用此设置，否则功能将无法运行。

第 7 步

单击取消按钮关闭WLAN子菜单。然后点击左侧菜单栏上的Monitoring菜单。一旦您能够访问，请点击Applications菜单项。


Monitoring
1
Network Summary
Access Points
Clients
Guest Clients
Mesh Extender
Applications
2
Rogues
Access Points
Clients
Wireless Dashboard
AP Performance

如果您没有流向任何源的流量，您的页面将为空白，如下所示。



此页面将显示以下信息：

- 应用 — 包括许多不同类型
- Groups — 指示应用组的类型，以便更轻松地排序
- Data Usage — 此服务整体使用的数据量
- 吞吐量 — 应用程序使用的带宽量

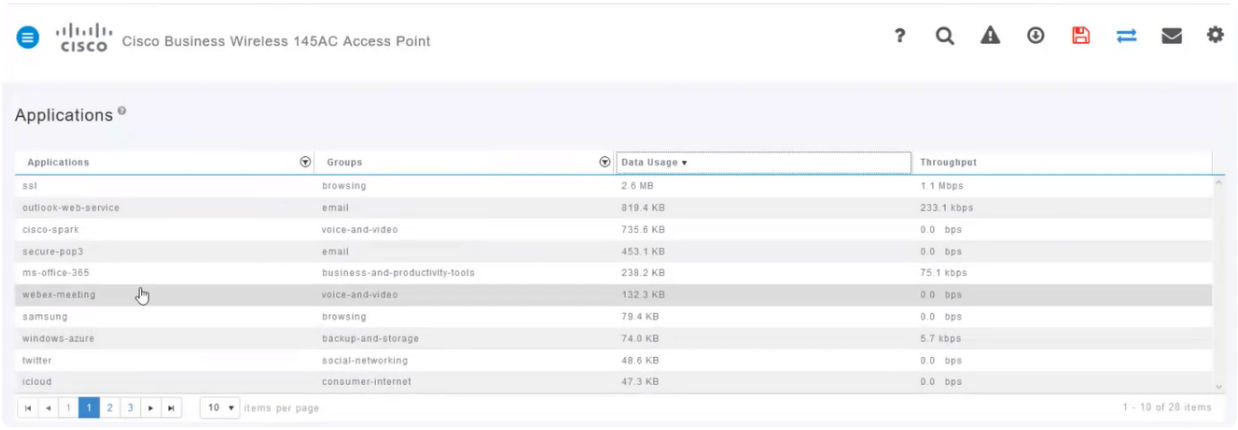
您可以点击选项卡，从大到小进行排序，这有助于确定网络资源的最大消费者。

此功能非常强大，可用于在精细级别管理您的WLAN资源。下面是一些比较常见的组和应用程序类型。您的列表可能包括更多内容，包括以下组和示例：

- 浏览
    - 例如：客户端特定的，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
- Software Updates

- 例如：Google-Play、IOS
- 即时消息
  - 例如：环聊、留言

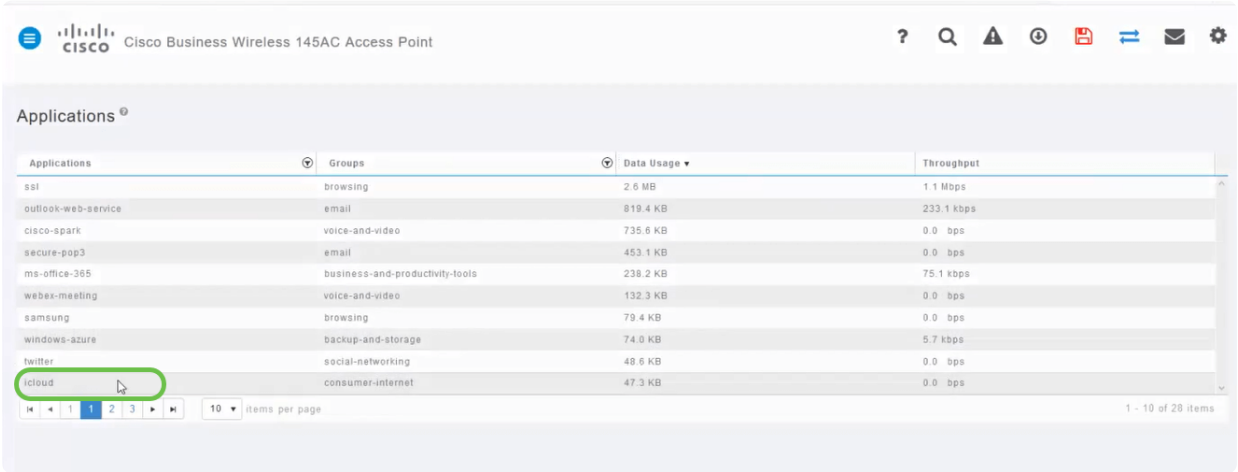
此处显示的是填充页面时的页面外观示例。



每个表标题都可以点击进行排序，这对于数据使用和吞吐量字段尤其有用。

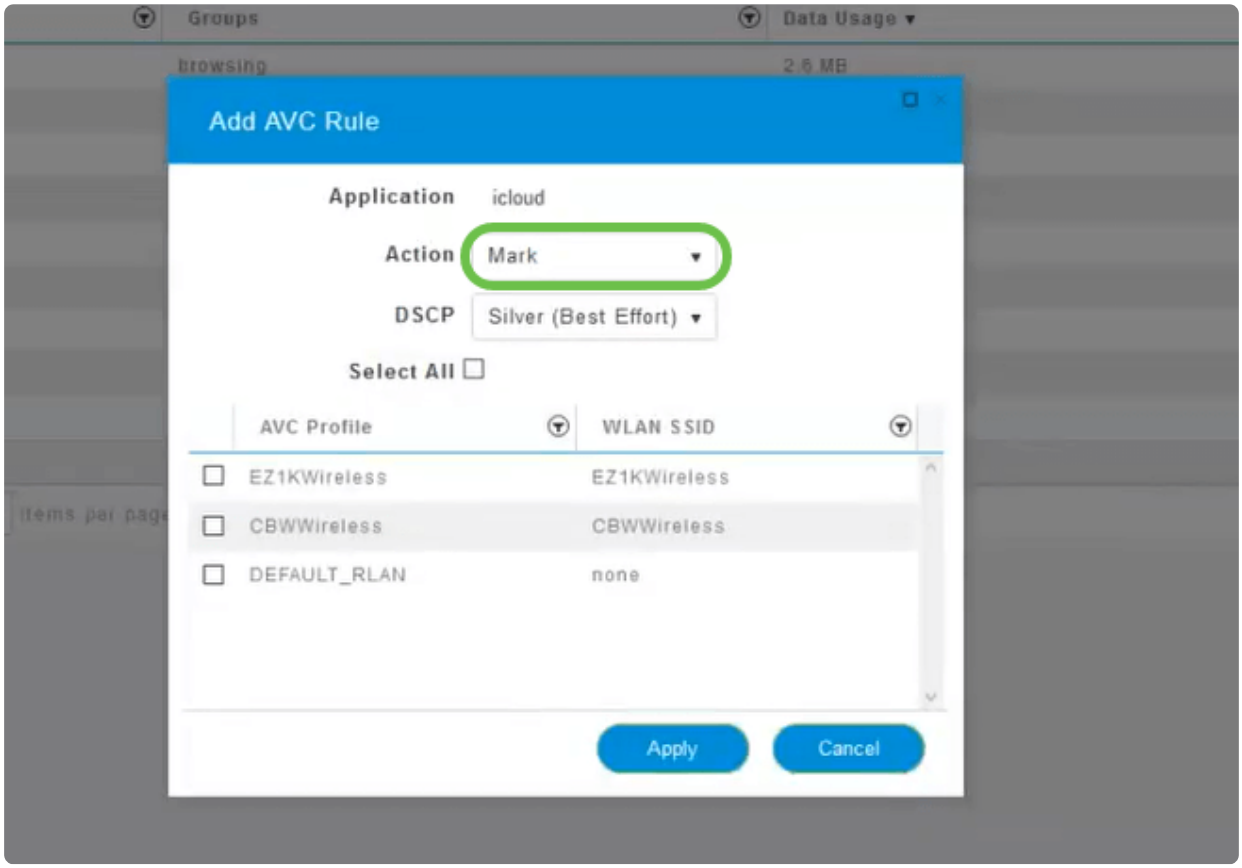
步骤 8

点击要管理的流量类型的行。



步骤 9

单击Action下拉框以选择如何处理该流量类型。



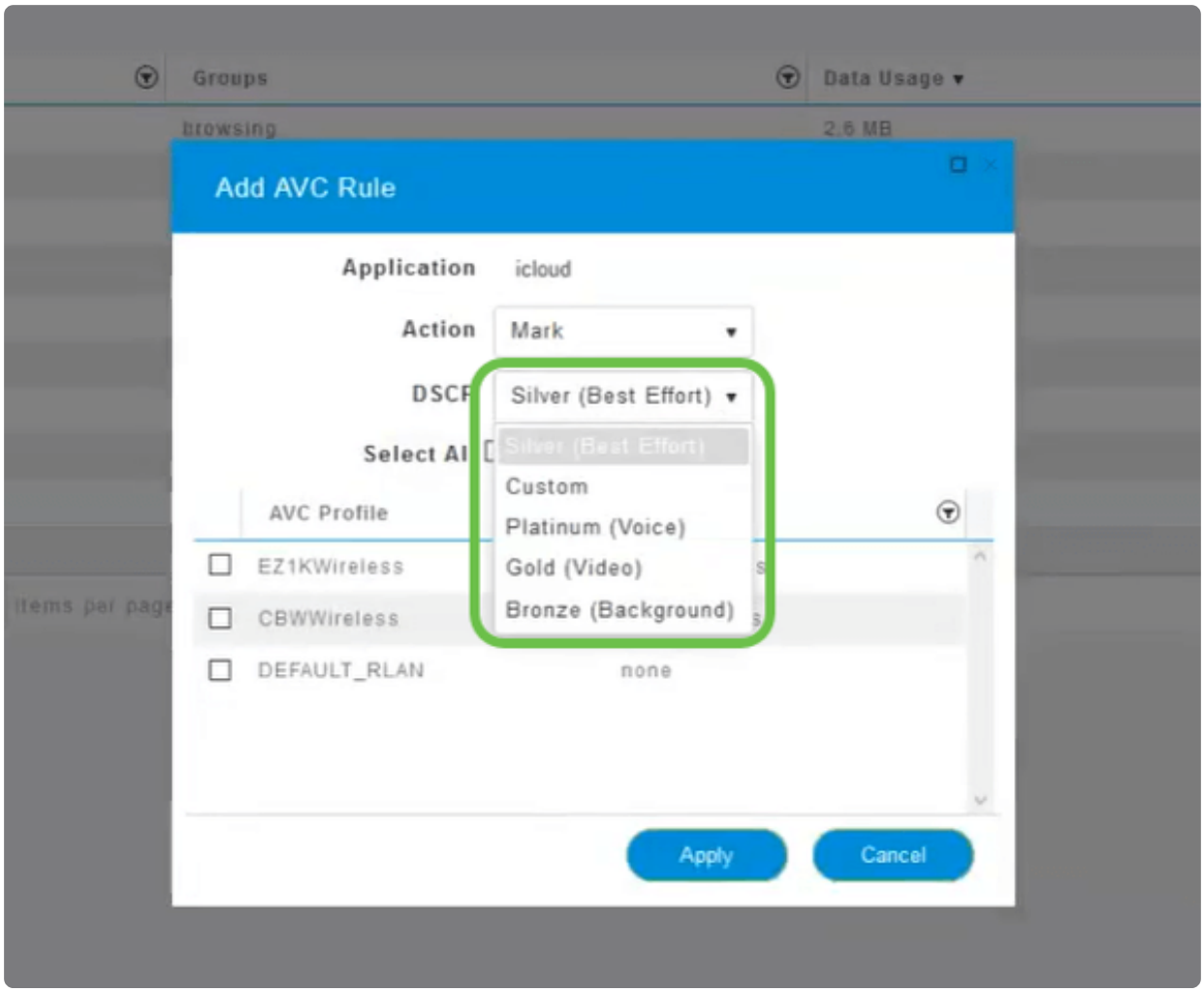
在本例中，我们将在Mark处保留此选项。

要对流量执行的操作

- 标记 — 将流量类型置于差分服务代码点(DSCP)3层之一 — 控制可供应用类型使用的资源数量
- 丢弃 — 不执行任何操作，但丢弃流量
- 速率限制 — 用于设置平均速率、突发速率（以Kbps为单位）

步骤 10

点击DSCP字段中的下拉框以从以下选项中进行选择。



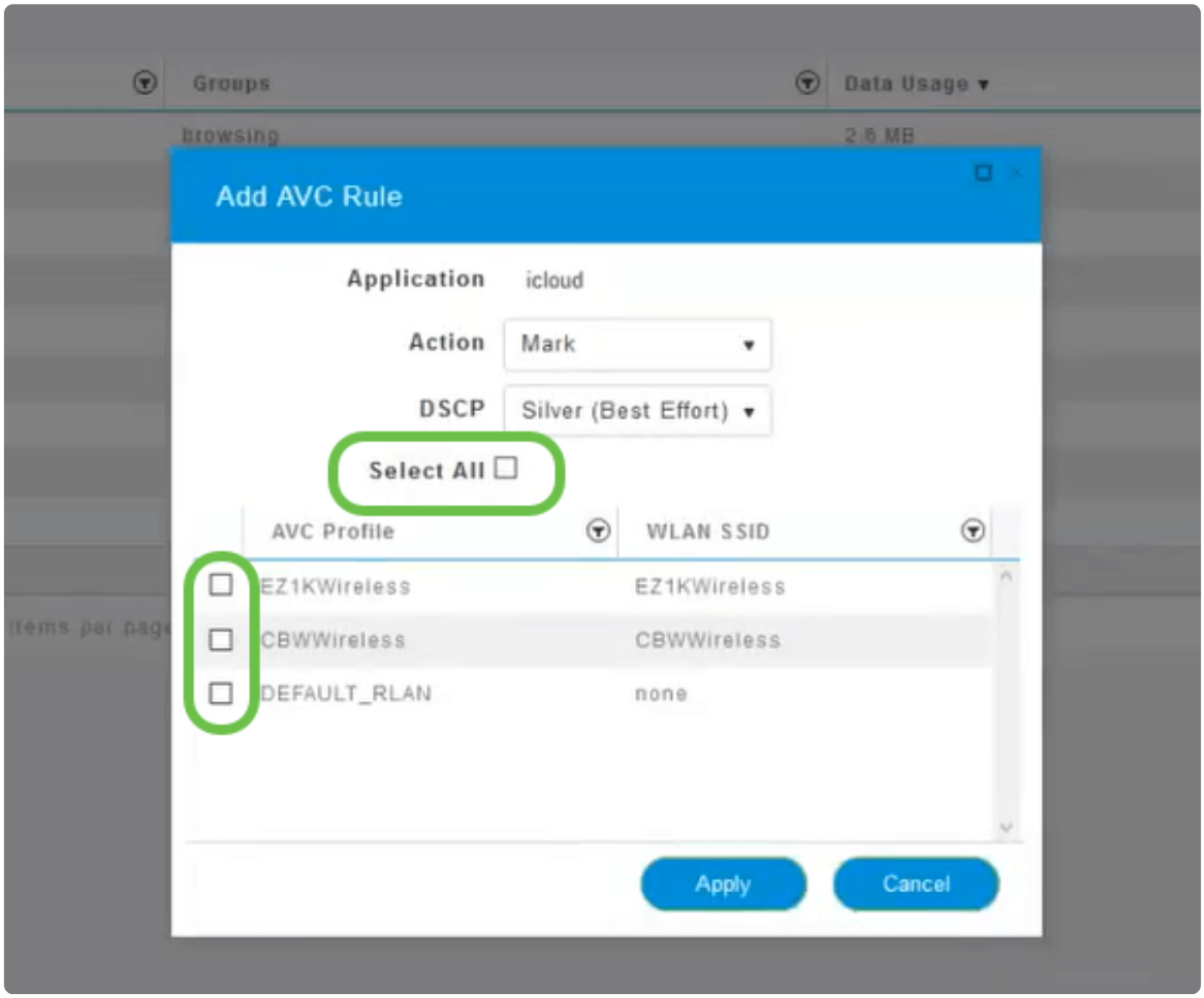
以下是待标记流量的DSCP选项。这些选项从更少的资源演变为更多可用于您正在编辑的流量类型的资源。

- 铜级（背景）— 更少
- 银牌（尽力）
- 金牌（视频）
- 白金级（语音）更多
- 自定义 — 用户设置

根据Web惯例，流量已迁移至SSL浏览，这会阻止您查看数据包从您的网络进入WAN时的内容。因此，大部分网络流量将使用SSL。将SSL流量设置为较低优先级可能会影响您的浏览体验。

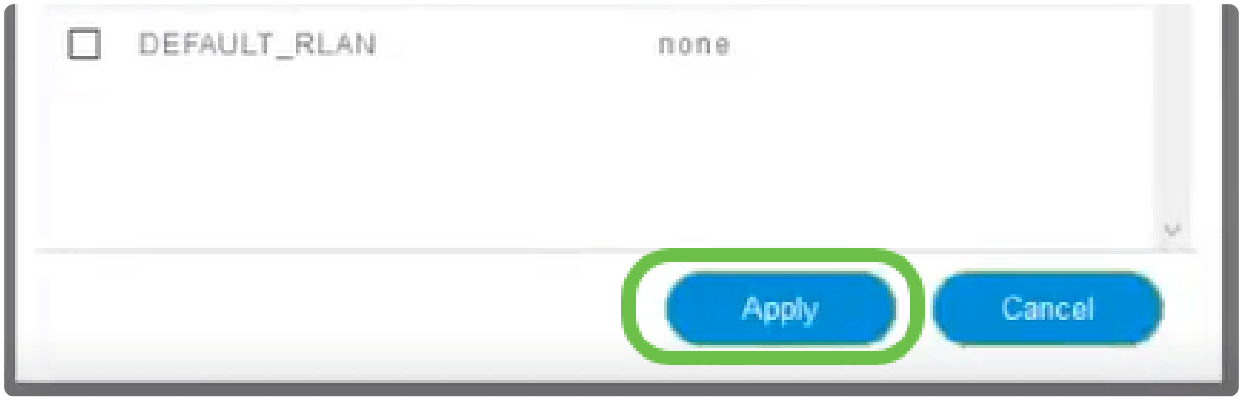
步骤 11

现在请选择您希望此策略运行的单个SSID，或者单击Select All。



步骤 12

现在单击Apply开始此策略。



以下两个情况可能适用：

- 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。
- 在办公时间内下载的大型软件更新可以取消优先级或进行速率限制。

你成功了！应用分析是一个非常强大的工具，也可以通过启用客户端分析来进一步启用，如下一节所述。

使用Web UI的客户端分析（可选）

连接到网络后，设备会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。这些信息可能包括：

- Host Name — 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

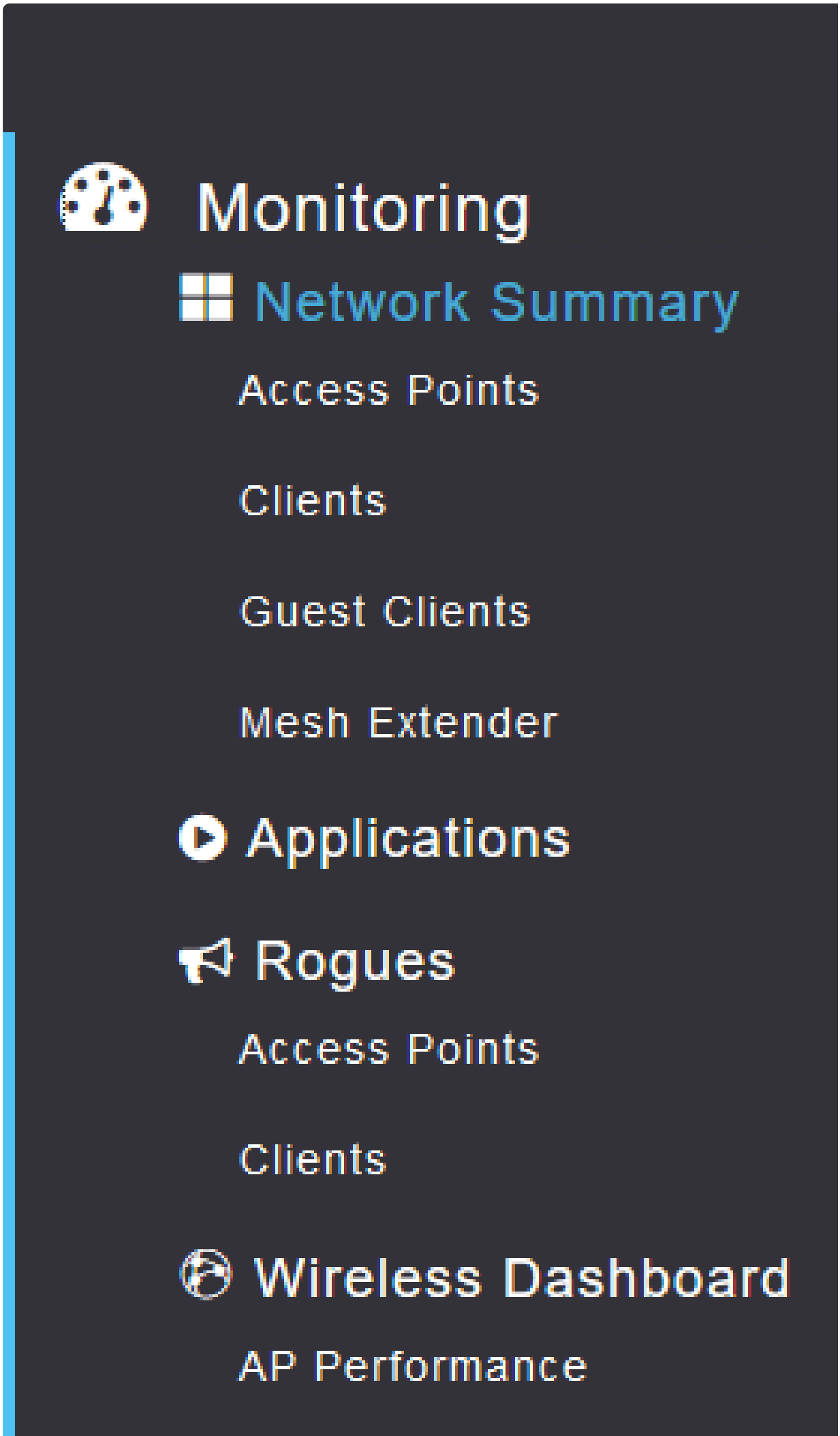
有关这些客户端的统计数据包括使用的数据量和吞吐量。

跟踪客户端配置文件可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。例如使用不传输您的业务任务关键型数据的应用限制设备类型。

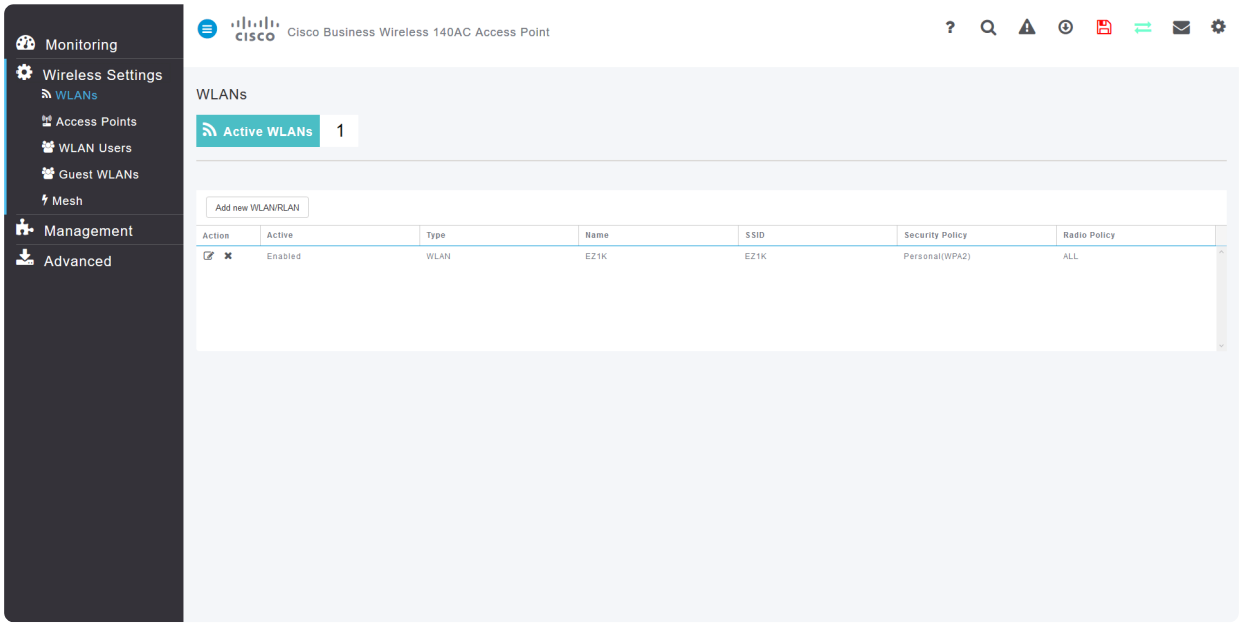
启用后，可以在Web UI的“Monitoring”（监控）部分找到您网络的客户端详细信息。

第 1 步

单击Wireless Settings。

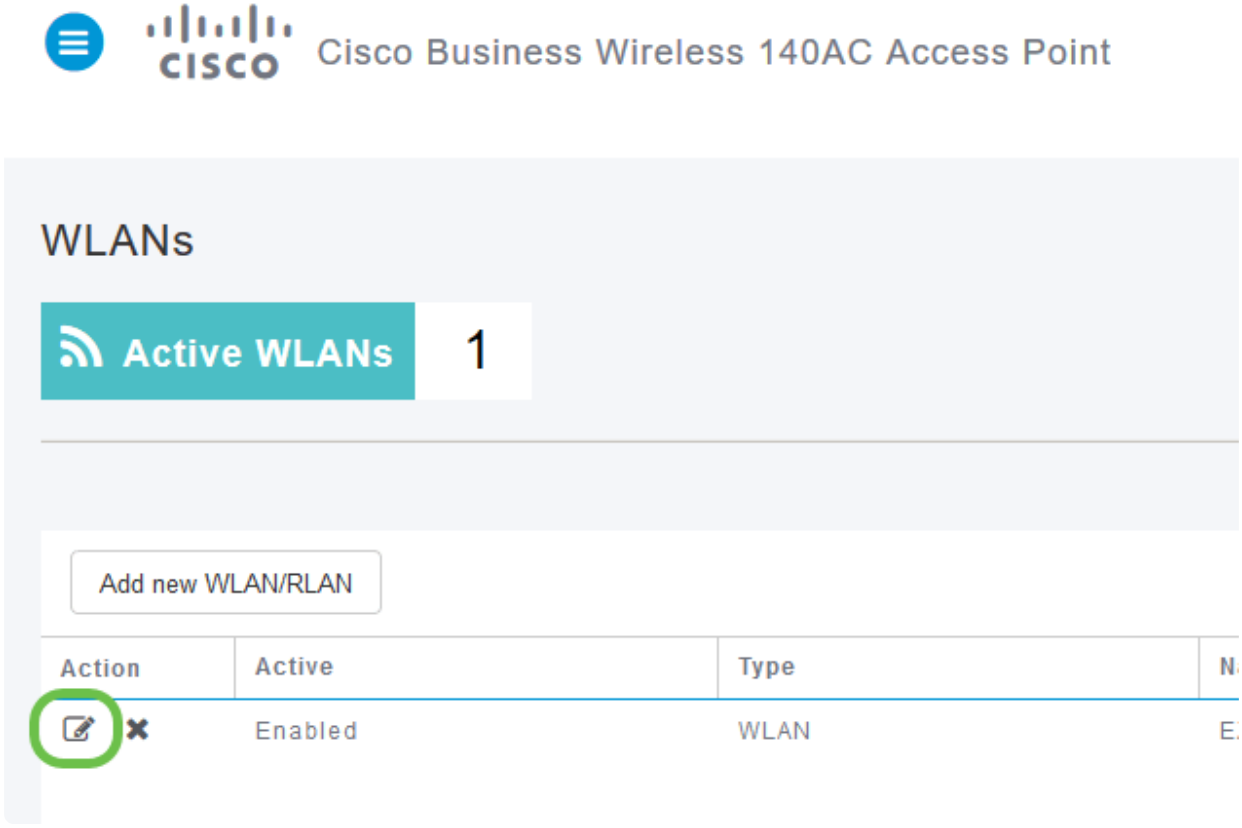

Monitoring
Network Summary
Access Points
Clients
Guest Clients
Mesh Extender
Applications
Rogues
Access Points
Clients
Wireless Dashboard
AP Performance

下面类似于您点击Wireless Settings（无线设置）链接时看到的内容：



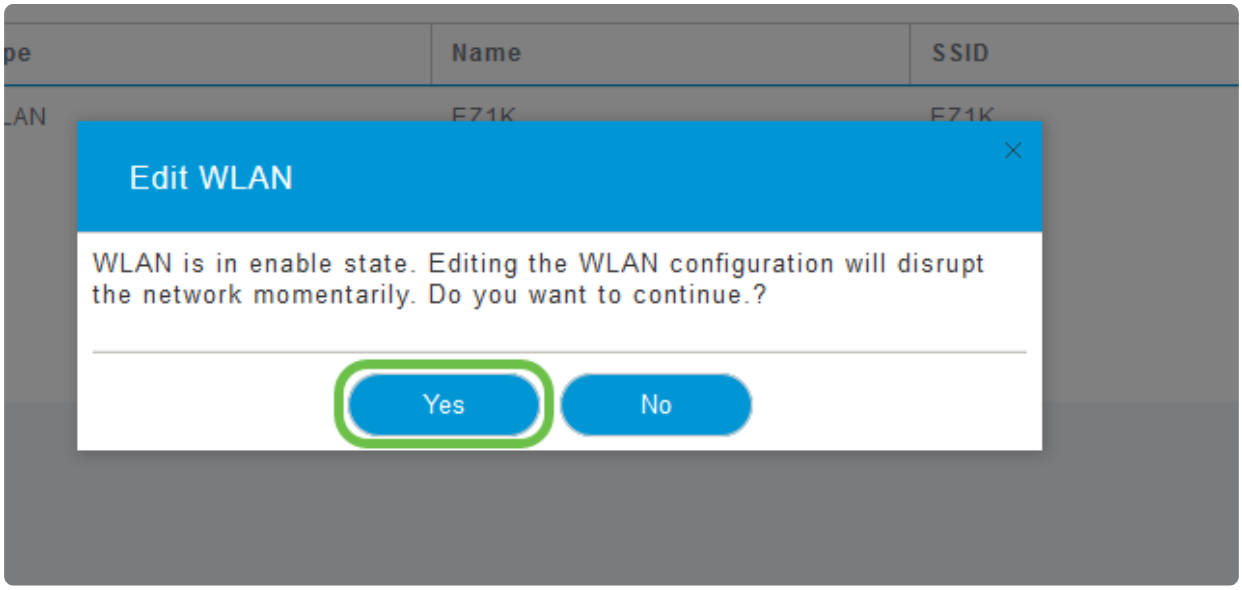
第 2 步

确定要用于应用的WLAN，然后点击其左侧的edit图标。



第 3 步

弹出菜单可能如下图所示。此重要消息可能会暂时影响网络上的服务。单击Yes向前移动。



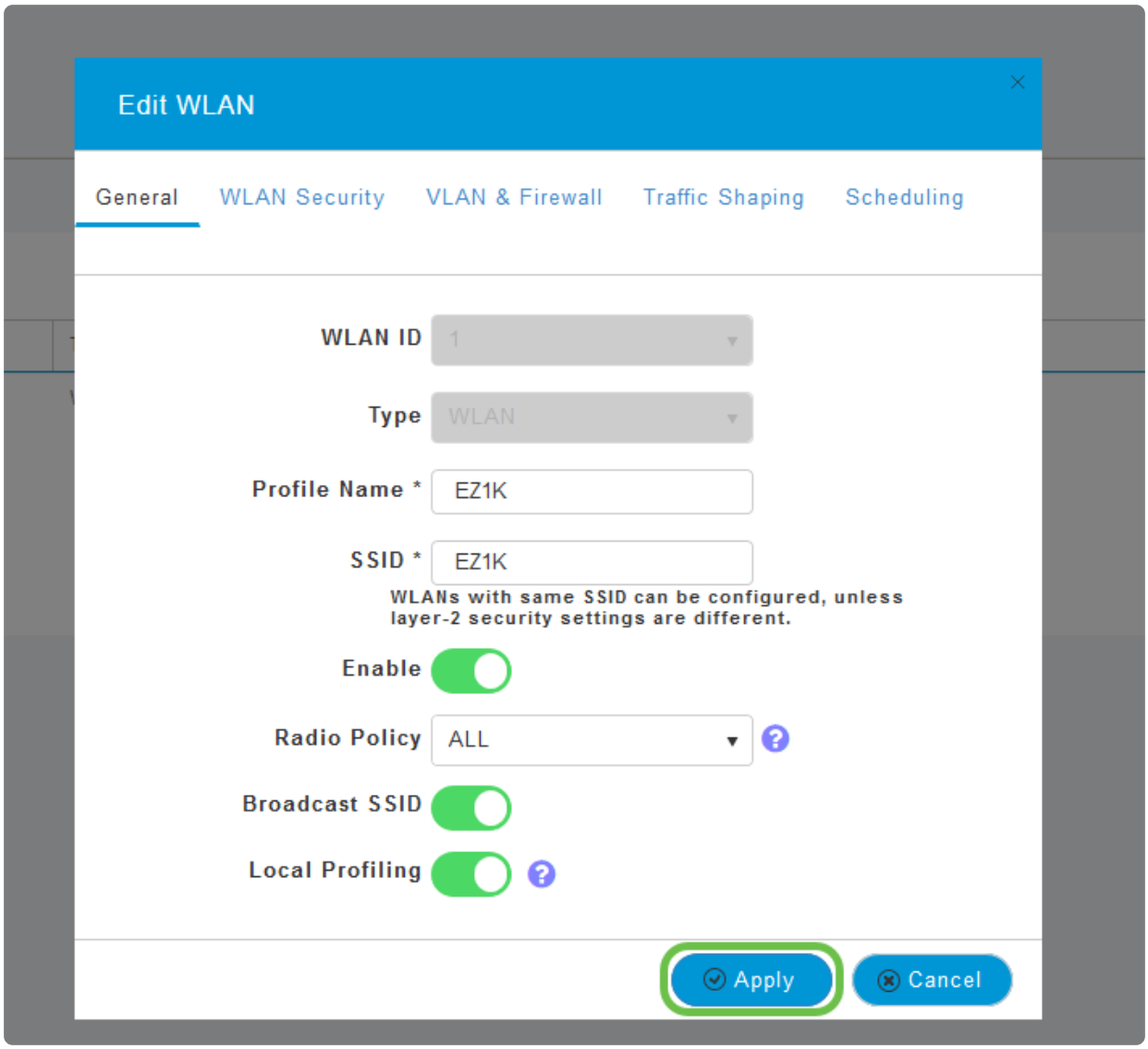
第 4 步

单击Local Profiling（本地分析）切换按钮切换客户端分析。



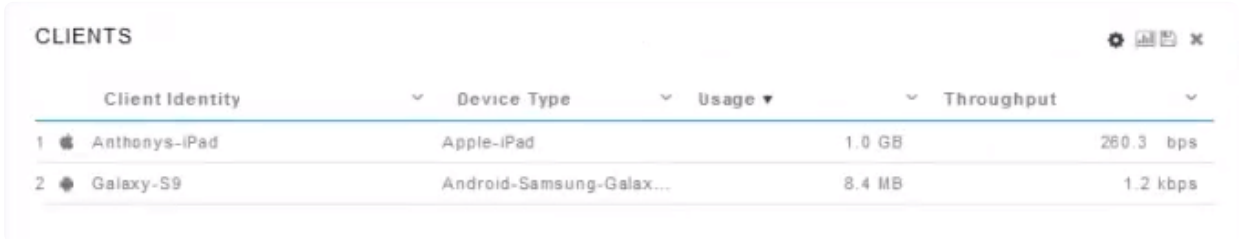
步骤 5

单击 Apply。



第 6 步

单击左侧的Monitoring部分菜单项。您将看到客户端数据开始显示在Monitoring选项卡的Dashboard中。



结论

现在，您已完成安全网络的设置。多么美好的感受，现在花一分钟庆祝一下，然后开始工作！

我们希望为客户提供最好的服务。如果您对此主题有任何意见或建议，请发送电子邮件至思科内容团队。

如果您想阅读其他文章和文档，请查看您的硬件的支持页面：

- 带PoE的思科RV345P VPN路由器
- 思科企业140AC接入点
- 思科Business 142ACM网状扩展器

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。