

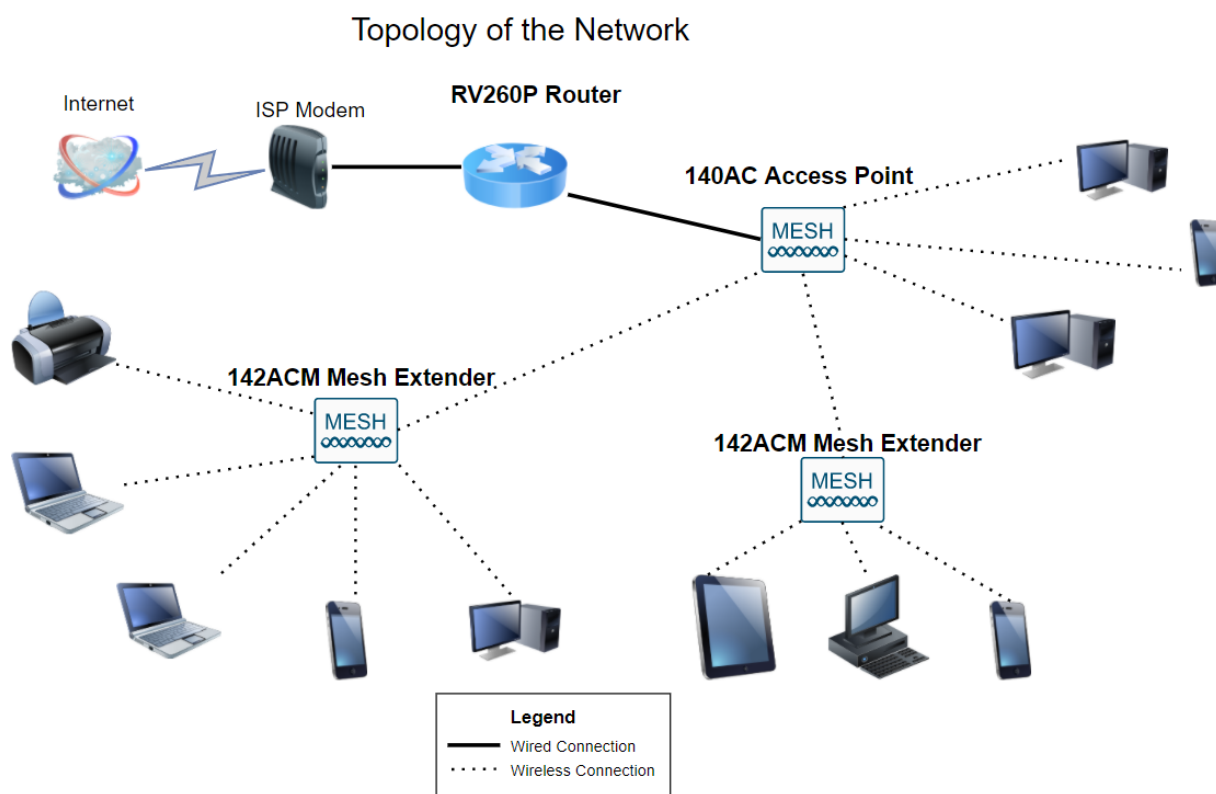
# 总网络配置：RV260P，搭配Cisco Business Wireless和Web UI

## 目标：

本指南将介绍如何使用RV260P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](#)。如果要使用Web UI，请继续阅读！

## 拓扑：



## 简介

您已准备好设置新网络。这是令人兴奋的一天！在此场景中，我们使用RV260P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。

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\(FAQ\)](#)

准备好了吗？我们开始吧！

## 适用设备 | 软件版本

- RV260P | 1.0.0.17
- CBW140AC | 10.3.1.0
- CBW142ACM | 10.3.1.0 ( 网状网络至少需要一个网状扩展器 )

## 目录

- [开始之前](#)
- [配置RV260P路由器](#)
  - [RV260P开箱即用](#)
  - [设置路由器](#)
  - [排除Internet连接故障](#)
  - [初始配置](#)
  - [升级固件 \( 如果需要 \)](#)
  - [配置VLAN \( 可选 \)](#)
  - [编辑IP地址 \( 可选 \)](#)
  - [添加静态IP](#)
- [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](#)
- [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 \( 可选 \)](#)

## 开始之前

1. 确保您有当前的Internet连接进行设置。
2. 联系您的ISP，了解使用RV260路由器时ISP有哪些特殊说明。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 ) 。

## 配置RV260P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RV260P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。

## RV260P开箱即用

### 第 1 步

将以太网电缆从RV260P 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RV260P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RV260P随附的电源适配器。使用不同的电源适配器可能损坏RV260P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RV260P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RV260P的WAN端口。

### 步骤 5

将RV260P适配器的另一端插入电源插座。这将打开RV260的电源。将调制解调器重新插入，以便也能通电。当电源适配器正确连接且RV260P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，现在该做一些配置了！要启动Web UI，请执行以下步骤：

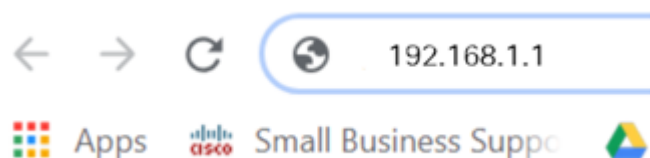
### 第 1 步

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RV260P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)”。



#### Your connection is not private

Attackers might be trying to steal your information from [ciscobusiness.cisco](#) (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR\_CERT\_AUTHORITY\_INVALID

Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. [Privacy policy](#)

Advanced

Back to safety

### 步骤 4

出现登录页时，输入默认用户名cisco和默认密码cisco。用户名和口令都区分大小写。



## Router

1

2

English ▾

3

©2018 Cisco Systems, Inc. All Rights Reserved.

Cisco, the Cisco Logo, and the Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

### 步骤 5

单击 **Login**。系统将显示“入门”页。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，您可以选中[RV160和RV260路由器上的故障排除](#)。

其他一些需要尝试的东西：

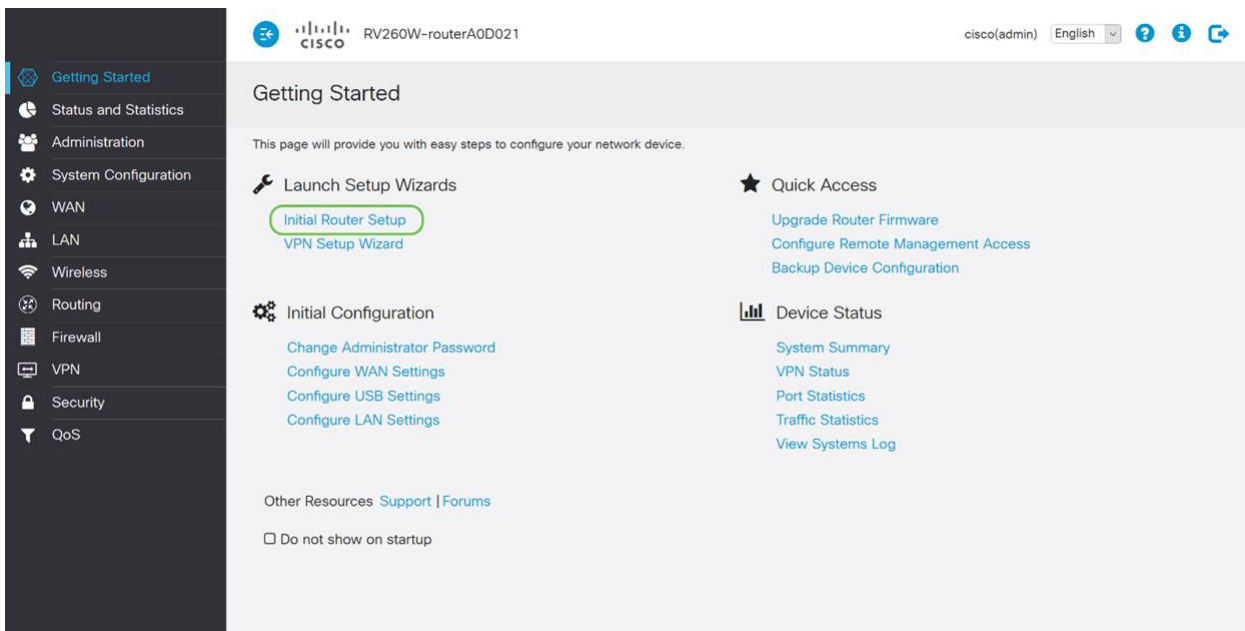
1. 验证您的Web浏览器是否未设置为“脱机工作”。
2. 检查以太网适配器的局域网连接设置。PC应通过DHCP获取IP地址。或者，PC可以在192.168.1.x范围内拥有静态IP地址，默认网关设置为192.168.1.1 (RV260P的默认IP地址)。要连接，您可能需要修改RV260P的网络设置。如果使用Windows 10，请检查[Windows 10方向以修改网络设置](#)。
3. 如果现有设备占用192.168.1.1 IP地址，则需要解决此冲突，网络才能运行。本部分末尾有关此内容的详细信息，或[单击此处直接转到此处](#)。
4. 关闭两台设备，重置调制解调器和RV260P。接下来，打开调制解调器电源，让它空闲大约2分钟。然后打开RV260P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。

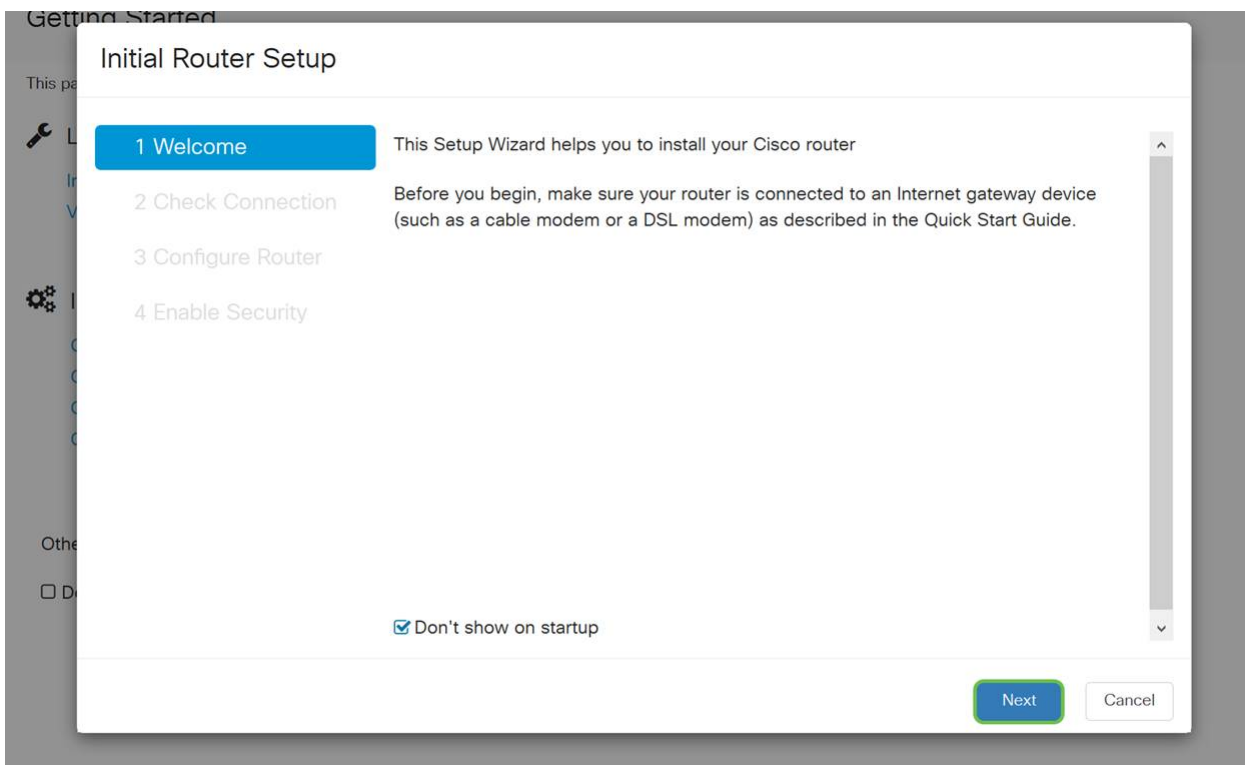
### 第 1 步

从“入门”页单击“初始设置向导”。



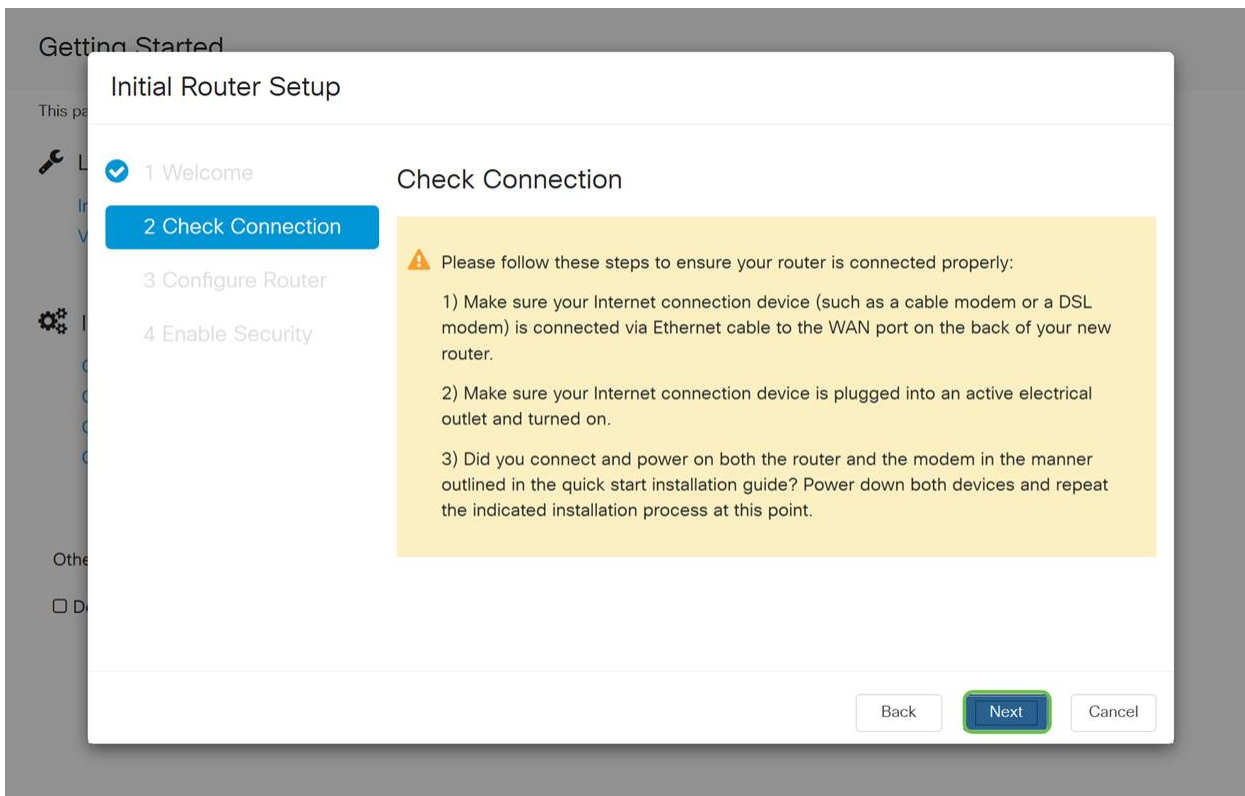
## 步骤 2

此步骤确认电缆已连接。由于您已确认此项，请单击“下一步”。



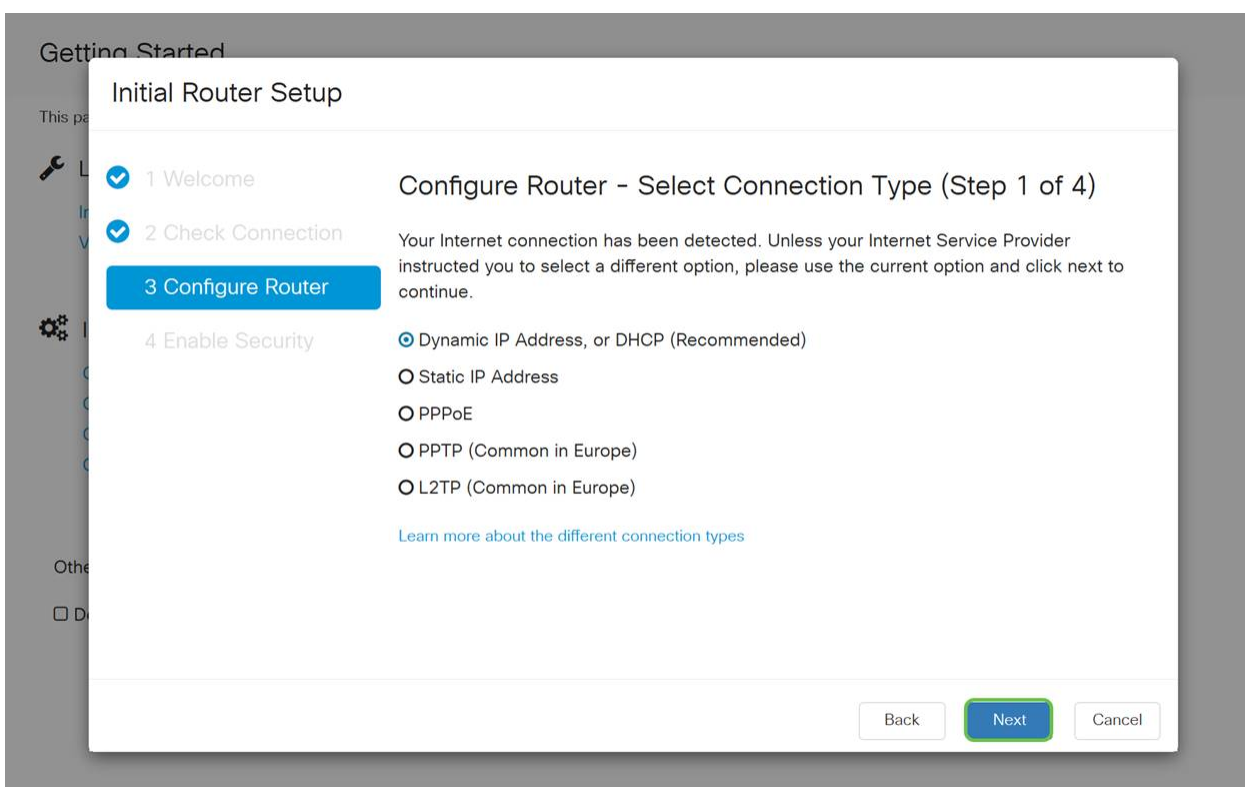
## 步骤 3

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”。



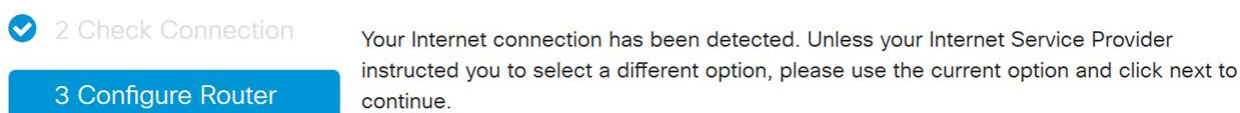
#### 步骤 4

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。



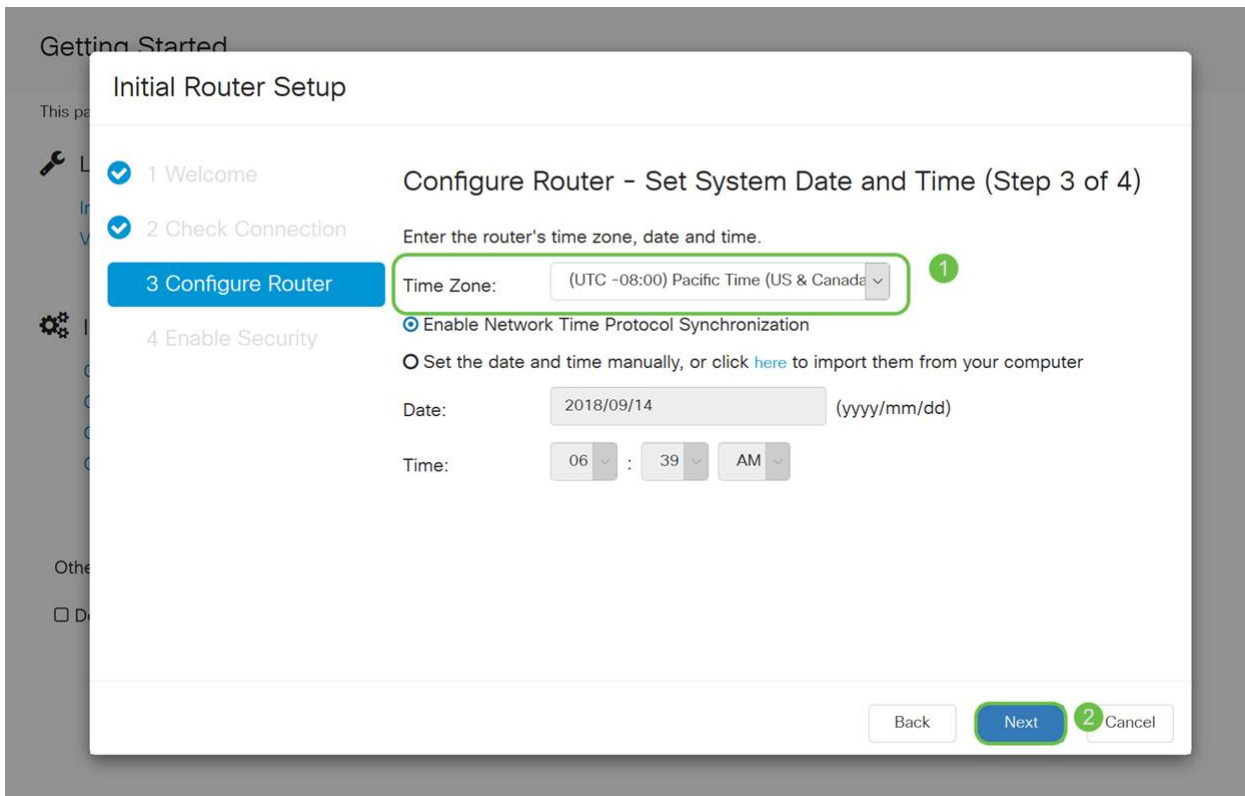
虽然您必须使用DHCP进行此初始设置，但您可以选择在屏幕底部了解有关不同连接类型的详细信息，以供将来参考。有关此方面的详细信息，请参阅以下文章：

- [RV160x和RV260x设备上的WAN配置](#)
- [在RV160和RV260上配置静态路由](#)



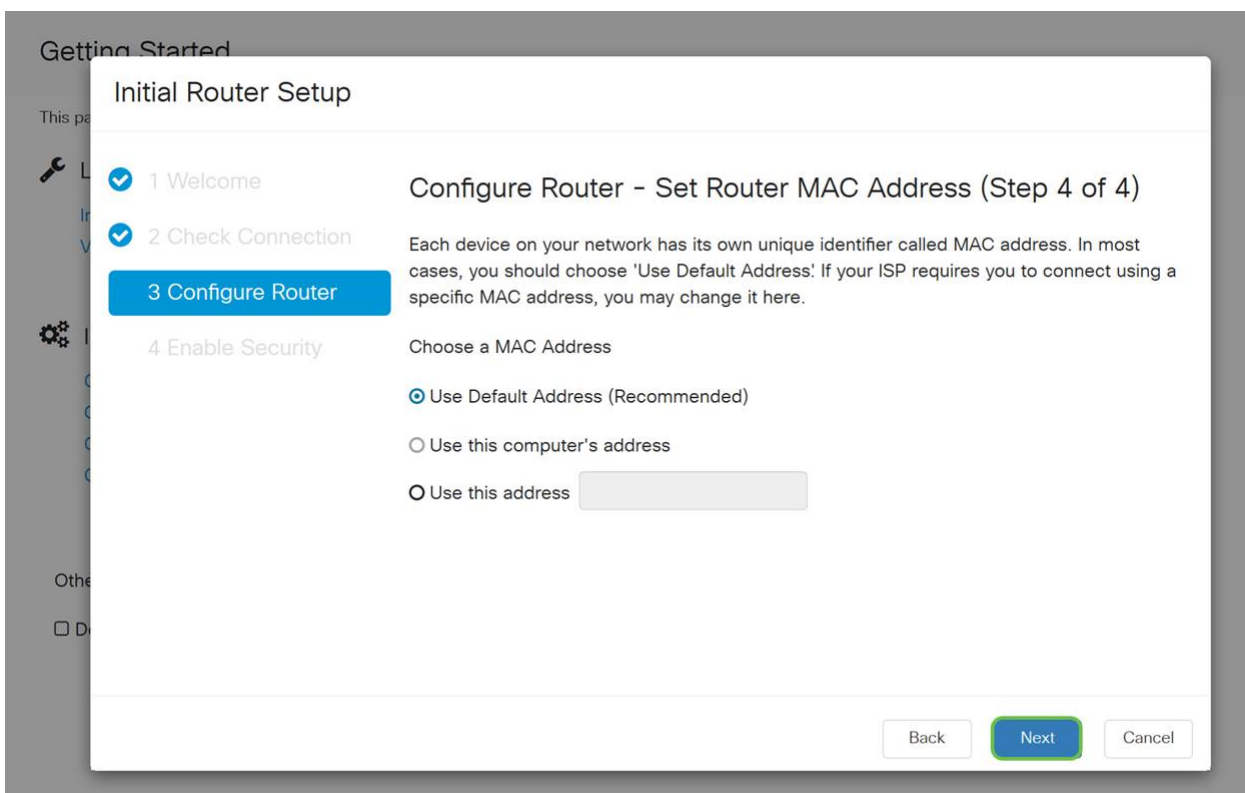
## 步骤 5

此时，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

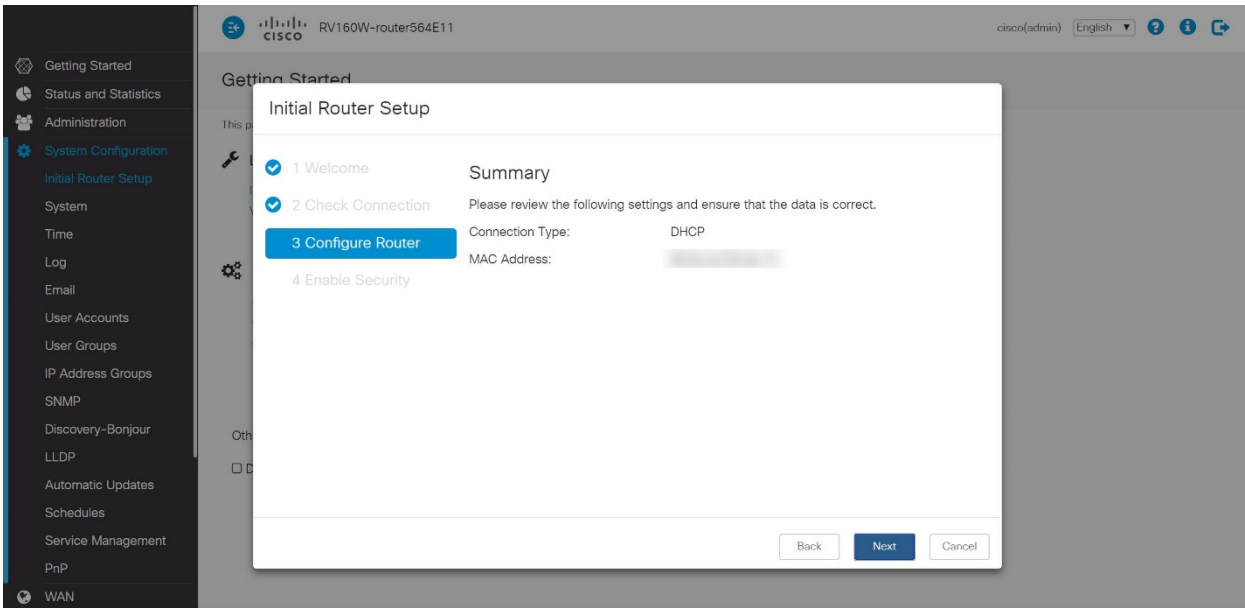
在此屏幕上，您将选择要分配给设备的MAC地址。通常，您将使用默认地址。单击Next。



## 步骤 7

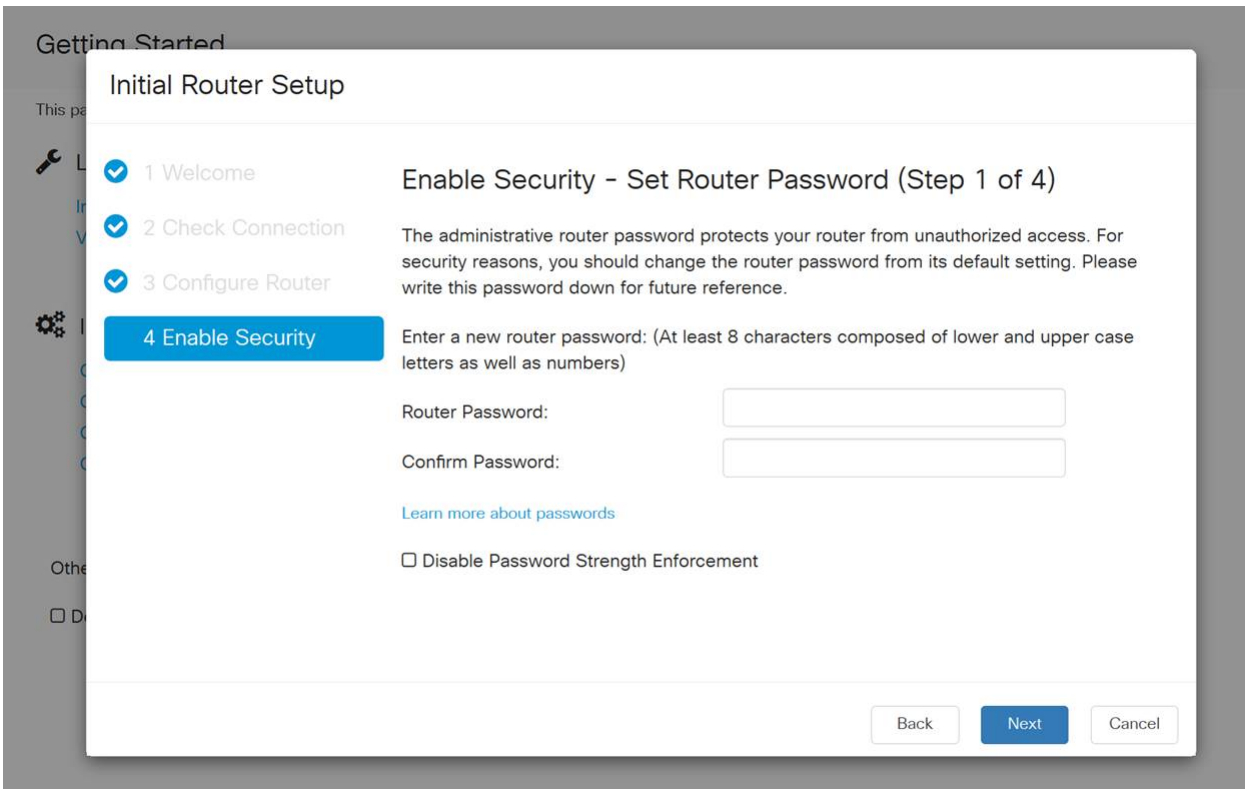


以下页面是所选选项的摘要。如果满意，请查看并单击“下一步”。



## 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

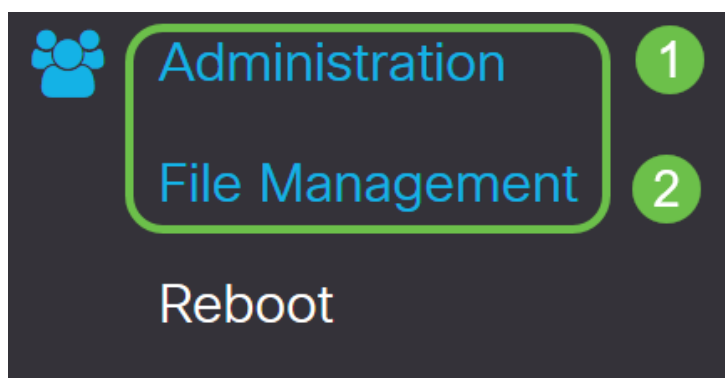
单击“保存”图标。



这是一个重要部分，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。

# File Management

## System Information

Device Model: RV260P

PID VID: RV260P-K9 V01

Current Firmware Version: 1.0.00.15

Latest Version Available on Cisco.com: -


Firmware Last Updated: 2019-Apr-17, 18:28:12

## 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。

### Manual Upgrade

File Type:  Firmware Image  Language File  USB Dongle Driver

Upgrade From:  cisco.com  PC  USB 

Firmware Image Format: \*.img (Maximum size: 100MB)

No file is selected

Reset all configurations/settings to factory defaults


The device will be automatically rebooted after the upgrade is complete.

## 步骤 3

在“手动升级”页上，单击单选按钮选择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。

### Manual Upgrade

File Type:  Firmware Image  Language File  USB Dongle Driver

Upgrade From:  cisco.com  PC  USB 

Reset all configurations/settings to factory defaults


The device will be automatically rebooted after the upgrade is complete.

## 步骤 4

单击Upgrade。

### Manual Upgrade

File Type:  Firmware Image  Language File  USB Dongle Driver

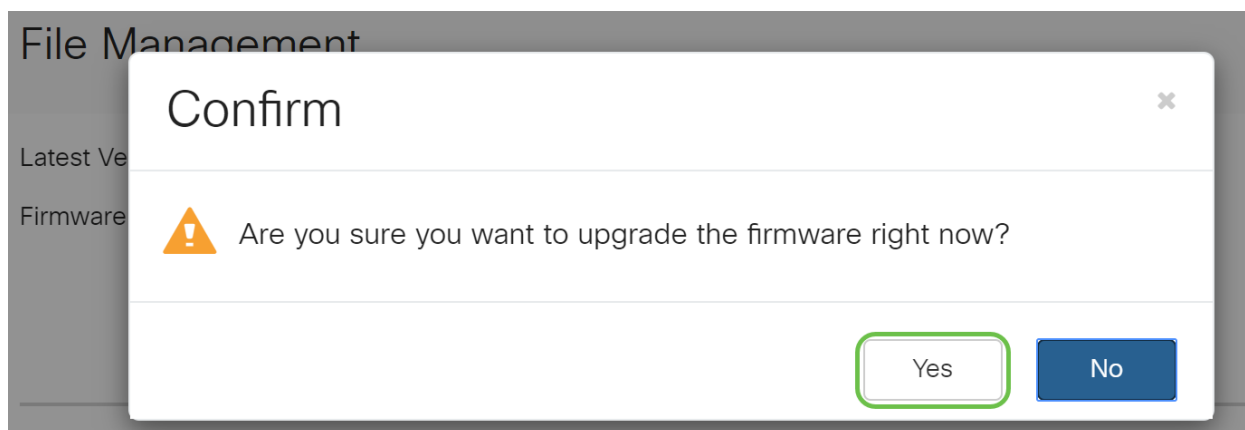
Upgrade From:  cisco.com  PC  USB 

Reset all configurations/settings to factory defaults

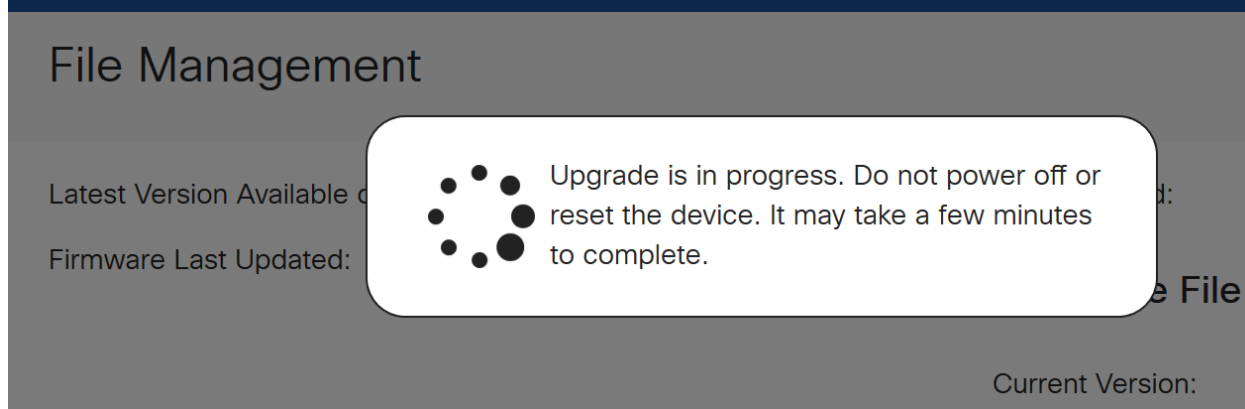
The device will be automatically rebooted after the upgrade is complete.

## 步骤 5

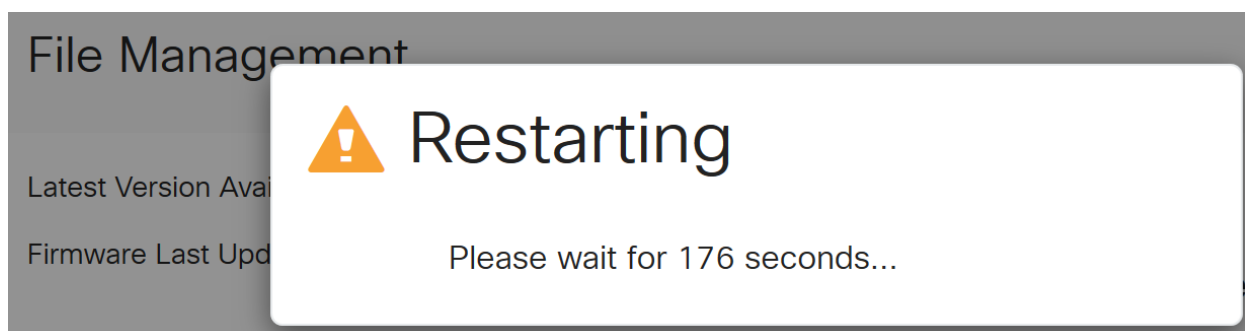
在确认窗口中单击是继续。



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 (系统信息)”。“当前固件版本”区域现在应显示已升级的固件版本。

# File Management

## System Information

Device Model:	RV260P
PID VID:	RV260P-K9 V01
Current Firmware Version:	1.0.01.01
Latest Version Available on Cisco.com:	-
Firmware Last Updated:	2020-Oct-26, 20:23:32

## Language File

Current Version: 1.0.0.0

祝贺您，您的路由器基本设置已完成！您有一些配置选项在继续。

我建议您继续滚动浏览文章，以了解有关这些选项以及这些选项是否适用于您的详细信息。如果您愿意，可以点击任何超链接跳至章节。

- [配置VLAN \( 可选 \)](#)
- [编辑IP地址 \( 可选 \)](#)
- [添加静态IP地址 \( 可选 \)](#)
- [我已准备好配置网络的网状无线部分!](#)

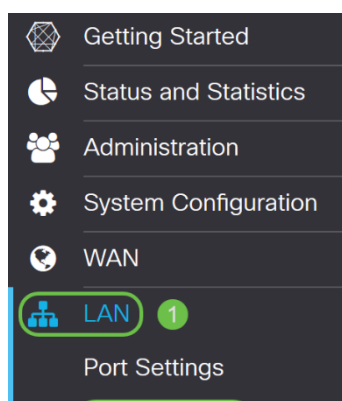
## 配置VLAN ( 可选 )

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。

如果不想创建VLAN，可跳至下一[节](#)。

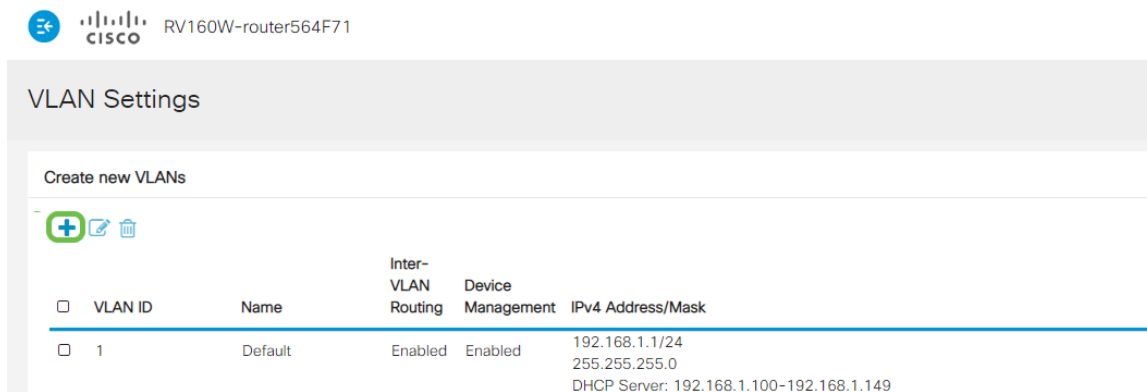
### 第 1 步

导航至LAN > VLAN Settings。



## 步骤 2

单击Add创建新的VLAN。



RV160W-router564F71

### VLAN Settings

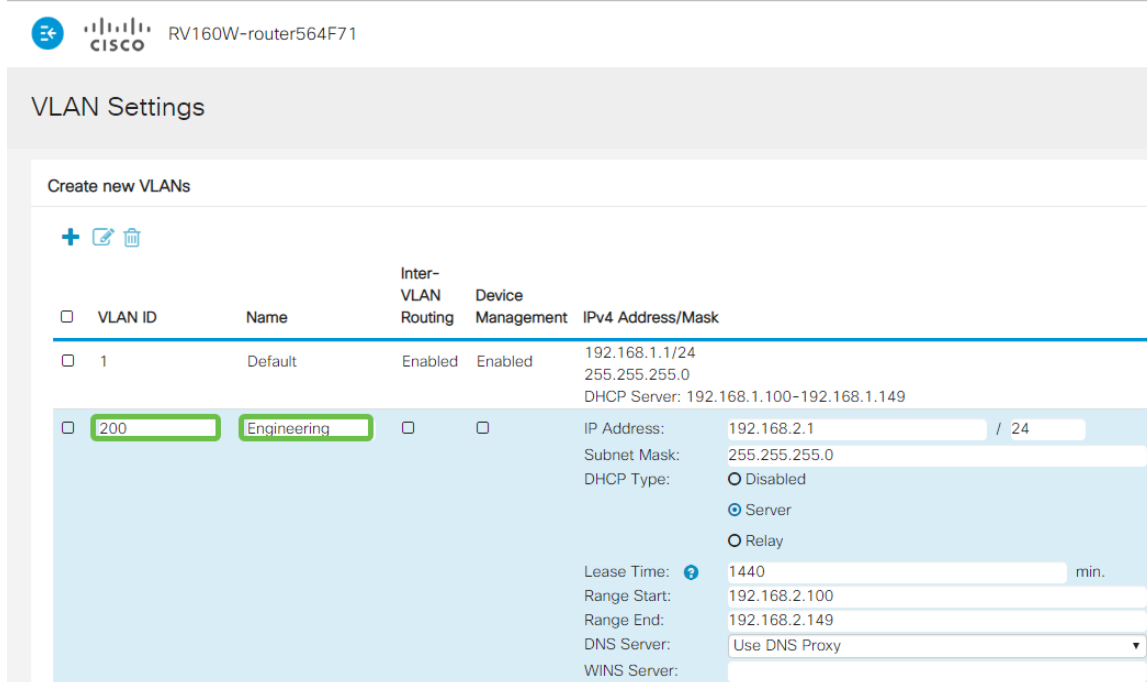
Create new VLANs

<input type="checkbox"/>	VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
<input type="checkbox"/>	1	Default	Enabled	Enabled	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149

## 步骤 3

输入要创建的VLAN ID，并输入名称。VLAN ID范围为1-4093。

我们输入200作为VLAN ID，Engineering作为VLAN的名称。



RV160W-router564F71

### VLAN Settings

Create new VLANs

<input type="checkbox"/>	VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
<input type="checkbox"/>	1	Default	Enabled	Enabled	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149
<input type="checkbox"/>	200	Engineering	<input type="checkbox"/>	<input type="checkbox"/>	IP Address: 192.168.2.1 / 24 Subnet Mask: 255.255.255.0 DHCP Type: <input type="radio"/> Disabled <input checked="" type="radio"/> Server <input type="radio"/> Relay Lease Time: 1440 min. Range Start: 192.168.2.100 Range End: 192.168.2.149 DNS Server: Use DNS Proxy WINS Server:

## 步骤 4

如果需要，取消选中Inter-VLAN Routing和Device Management的Enabled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RV260P的Web UI并管理RV260P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。

RV160W-router564F71

### VLAN Settings

Create new VLANs

VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
1	Default	Enabled	Enabled	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149
200	Engineering	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	IP Address: 192.168.2.1 / 24 Subnet Mask: 255.255.255.0 DHCP Type: <input type="radio"/> Disabled <input checked="" type="radio"/> Server <input type="radio"/> Relay Lease Time: 1440 min. Range Start: 192.168.2.100 Range End: 192.168.2.149 DNS Server: Use DNS Proxy WINS Server:

## 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。

RV160W-router564F71

### VLAN Settings

Create new VLANs

VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
1	Default	Enabled	Enabled	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149
200	Engineering	<input type="checkbox"/>	<input type="checkbox"/>	IP Address: 192.168.2.1 / 24 Subnet Mask: 255.255.255.0 DHCP Type: <input type="radio"/> Disabled <input checked="" type="radio"/> Server <input type="radio"/> Relay Lease Time: 1440 min. Range Start: 192.168.2.100 Range End: 192.168.2.149 DNS Server: Use DNS Proxy WINS Server:

## 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。

## VLAN Settings

Create new VLANs



<input type="checkbox"/>	VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
<input type="checkbox"/>	1	Default	Enabled	Enabled	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149
<input type="checkbox"/>	200	Engineering	<input type="checkbox"/>	<input type="checkbox"/>	IP Address: 192.168.2.1 / 24 Subnet Mask: 255.255.255.0 DHCP Type: <input checked="" type="radio"/> Server <input type="radio"/> Disabled <input type="radio"/> Relay Lease Time: 1440 min. Range Start: 192.168.2.100 Range End: 192.168.2.149 DNS Server: Use DNS Proxy WINS Server:

### 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。

## VLAN Settings

Create new VLANs

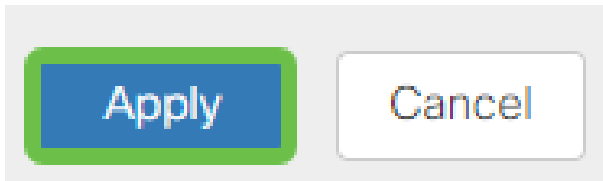


<input type="checkbox"/>	VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
<input type="checkbox"/>	1	Default	Enabled	Enabled	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149
<input type="checkbox"/>	200	Engineering	<input type="checkbox"/>	<input type="checkbox"/>	IP Address: 192.168.2.1 / 24 Subnet Mask: 255.255.255.0 DHCP Type: <input checked="" type="radio"/> Server <input type="radio"/> Disabled <input type="radio"/> Relay Lease Time: 1440 min. Range Start: 192.168.2.100 Range End: 192.168.2.149 DNS Server: Use DNS Proxy WINS Server:



## 步骤 8

单击**Apply**以创建新VLAN。



### 为 VLAN 分配端口

在RV260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。

**注意：**在本示例中，没有中继。

## 步骤 9

选择要编辑的VLAN ID。单击 Edit。

在本例中，我们选择了VLAN 1和VLAN 200。

#### Assign VLANs to ports

VLAN ID	LAN1	LAN2
1	Untagged	Excluded
200	Excluded	Untagged

### 步骤 10

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**。

#### Assign VLANs to ports

VLAN ID	LAN1	LAN2
1	Untagged	Excluded
200	Excluded	Untagged

### 步骤 11

单击**Apply**保存配置。

Apply Cancel

您现在应该已成功创建新VLAN，并将VLAN配置到RV260上的端口。重复此过程以创建其他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。

这是VLAN的基础。单击超链接，详细了解《思科企业路由器的VLAN最佳实践和安全提示》。

## 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。跳过重新运行初始设置向导，按照以下步骤执行此更改。

如果不需要编辑IP地址，可以转到本文的下一部分。

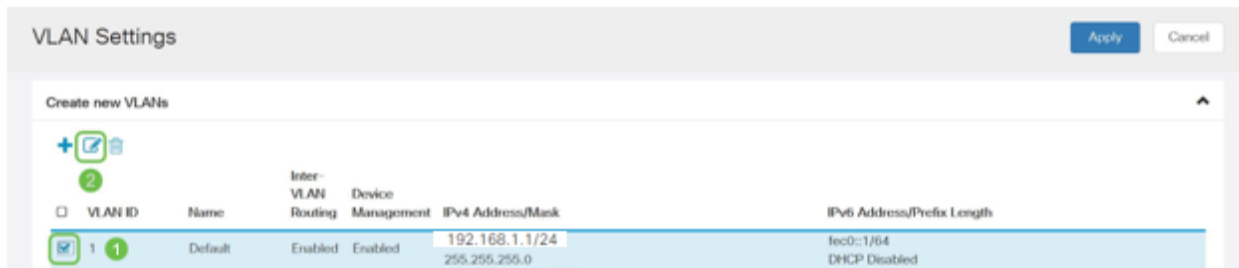
### 第 1 步

在左侧菜单栏中，单击LAN > VLAN Settings。



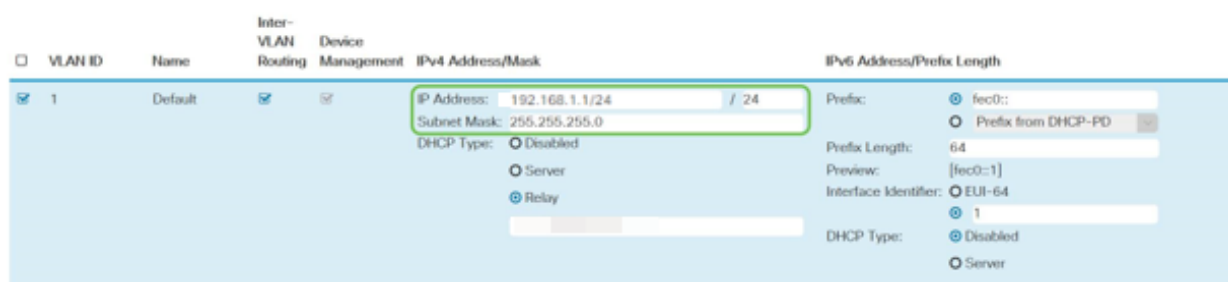
## 步骤 2

然后选择包含路由设备的VLAN，然后单击编辑图标。



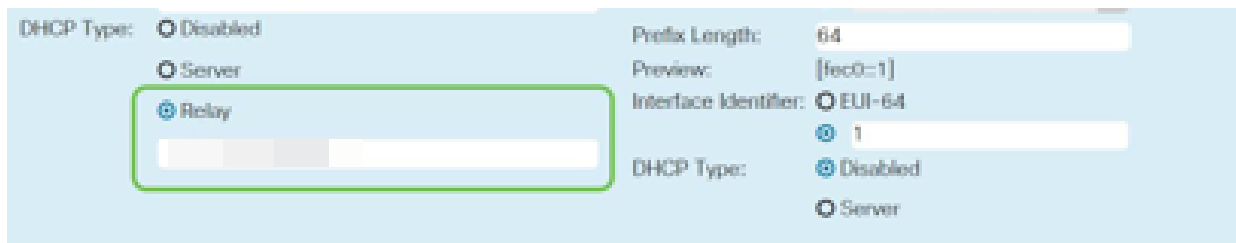
## 步骤 3

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。



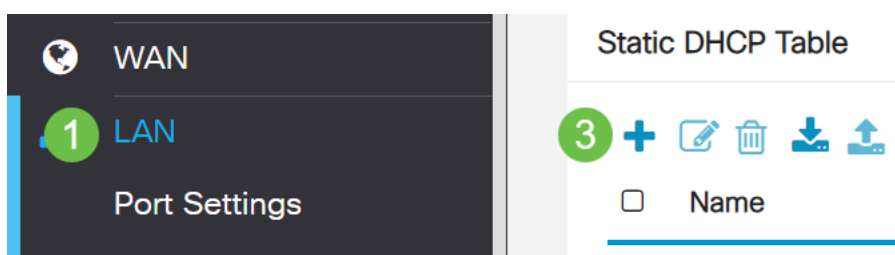
## 添加静态IP

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](#)。

如果您不需要添加静态IP地址，可以转到本文的[下一节](#)来配置接入点。

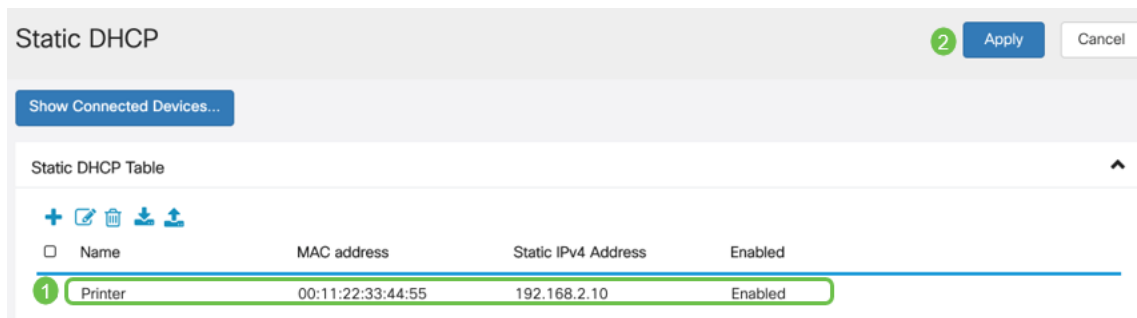
## 第 1 步

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。



祝贺您，您已完成RV260P路由器的配置。我们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RV260P的PoE端口。RV260P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 RV260 Routers](#)。

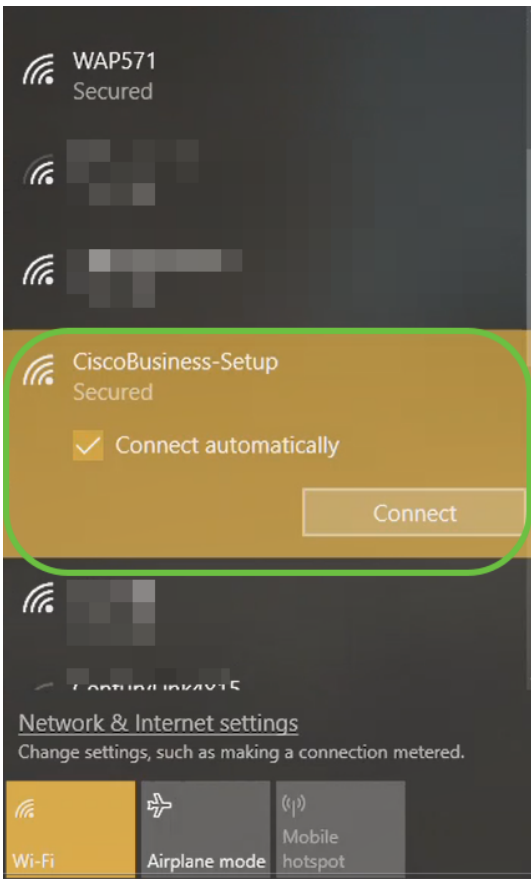
### 在Web UI上设置140AC主无线接入点

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

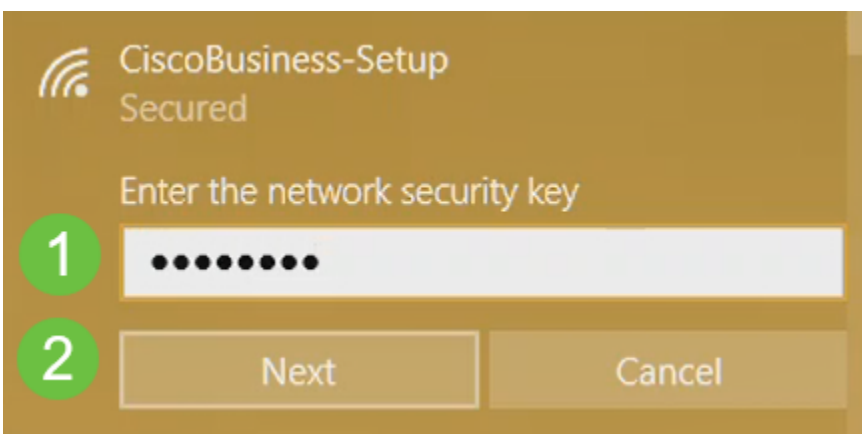
在PC上，单击Wi-Fi图标，然后选择*CiscoBusiness-Setup*无线网络。单击 Connect。



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。

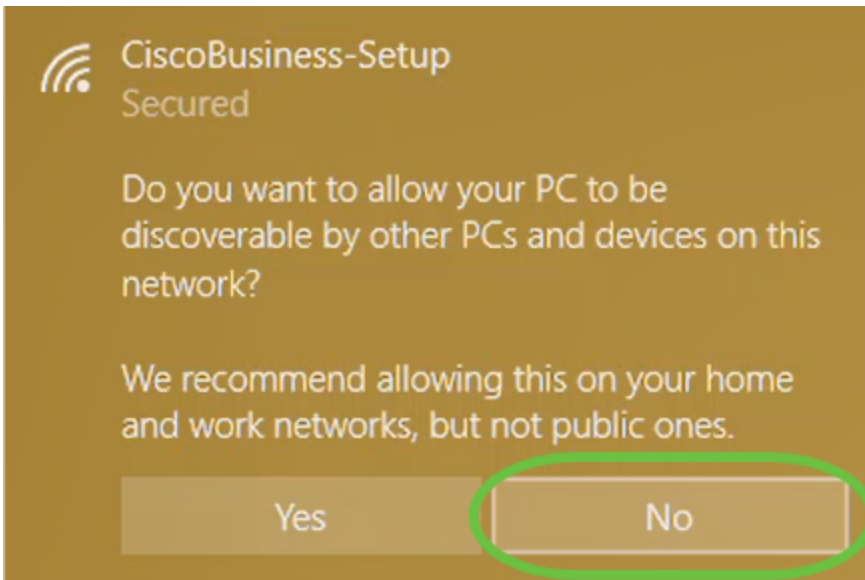
## 步骤 2

输入口令 `cisco123`，然后单击 **Next**。



## 步骤 3

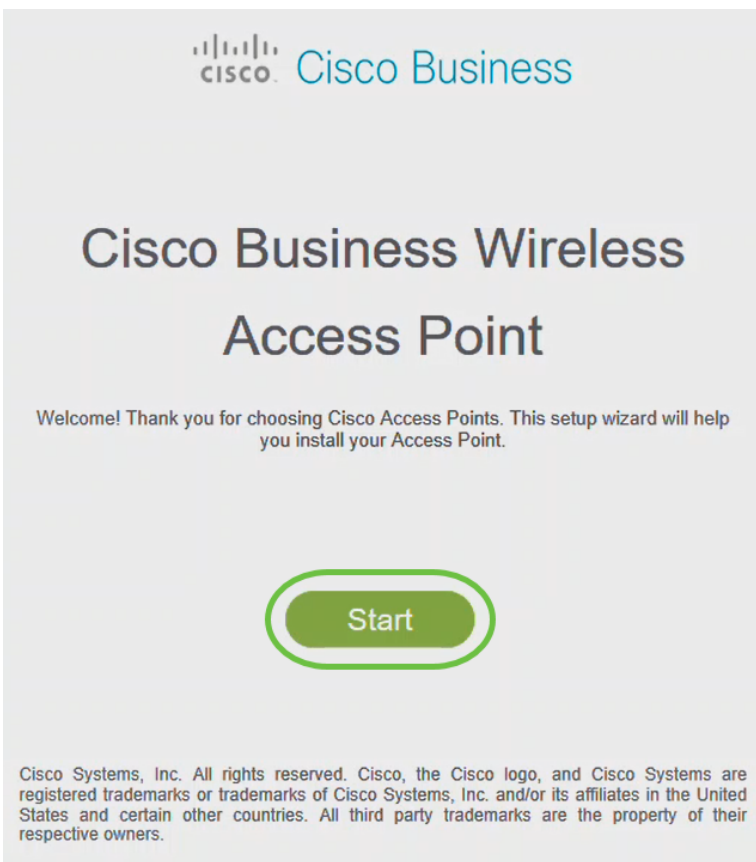
您将看到以下屏幕。由于一次只能配置一台设备，请单击**否**。



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

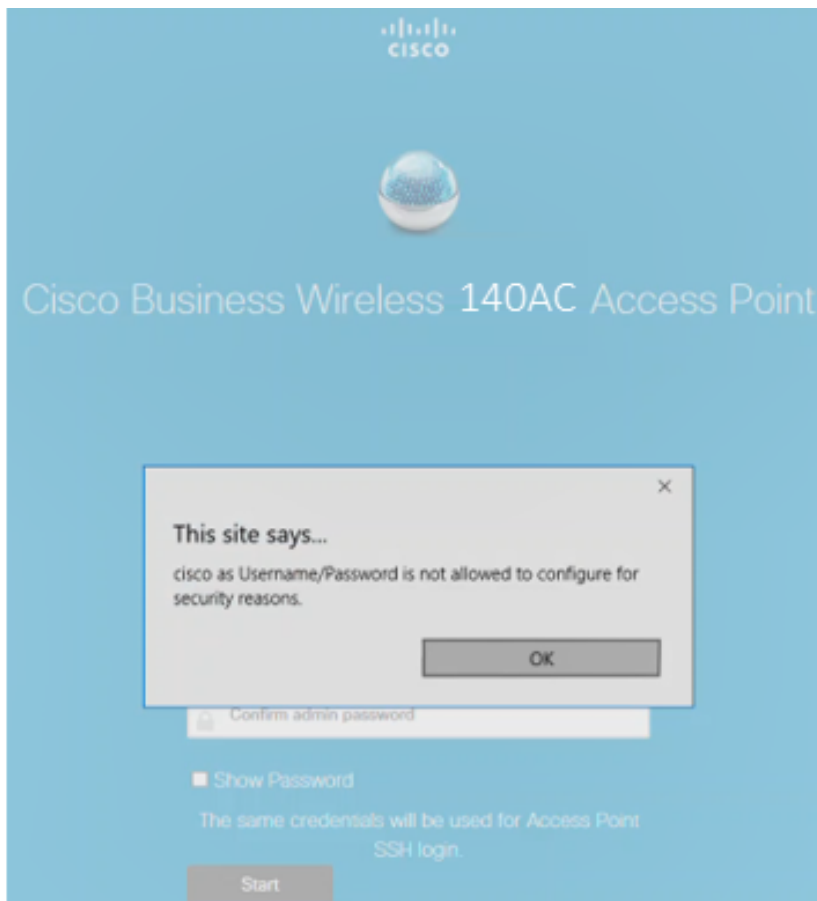
通过输入以下内容创建管理员帐户：

- 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。

The screenshot shows the Cisco Business Wireless 140AC Access Point setup interface. At the top, the Cisco logo is displayed. Below it, the text reads "Cisco Business Wireless 140AC Access Point". A message says "Welcome! Please start by creating an admin account." There are three input fields: the first contains "admin", the second and third are for passwords. A "Show Password" checkbox is checked. A "Start" button is at the bottom. Five green circles with numbers 1 through 5 highlight the input fields, the "Show Password" checkbox, and the "Start" button.

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



## 1 Set Up Your Primary AP

Primary AP Name  ? **1**

Country  ? **2**

Date & Time   ? **3**

Timezone  ? **4**

Mesh  ? **5**

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。

1 Would you like Static IP for your ... AP (Management Network)

Management IP Address

Subnet Mask  **2**

Default Gateway

Back Next **3**

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。

2 Create Your Wireless Network

Network Name: CBWWlan

Security: WPA2

Passphrase: .....

Confirm Passphrase: .....

Show Passphrase

Back 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”。



Please confirm the configurations and Apply

## 1 Primary AP Settings

Username **Admin**  
Primary AP Name **Test**  
Country **United States (US)**  
Date & Time **04/09/2021 9:14:16**  
Timezone **Central Time (US and Canada)**  
Mesh **No**  
Management IP Address **DHCP assigned IP Address**

## 2 Wireless Network Settings

Network Name **Test123**  
Security **WPA2 Personal**  
Passphrase: **\*\*\*\*\***

Back

Apply

### 步骤 10

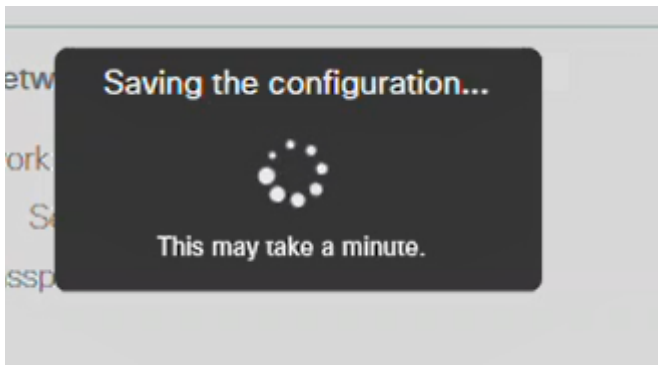
单击OK以应用设置。

Primary AP will reboot after these configurations are applied. Click Ok to continue or click Cancel to return to the set up wizard.

OK

Cancel

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。

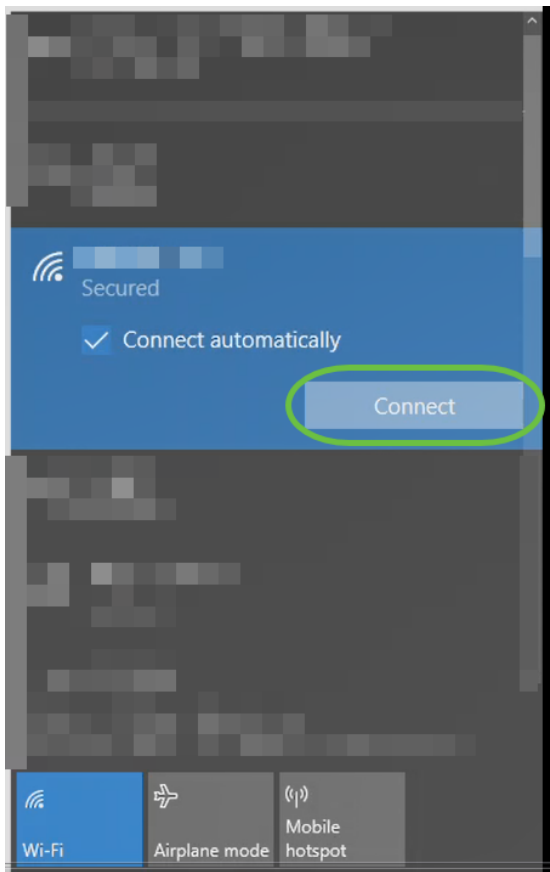


在重新启动期间，接入点中的LED将经过多种颜色模式。当LED呈绿色闪烁时，请继续下一步。如果LED未通过红色闪烁模式，则表明您的网络中没有DHCP服务器。确保AP连接到交换机或具有DHCP服务器的路由器。

## 步骤 11

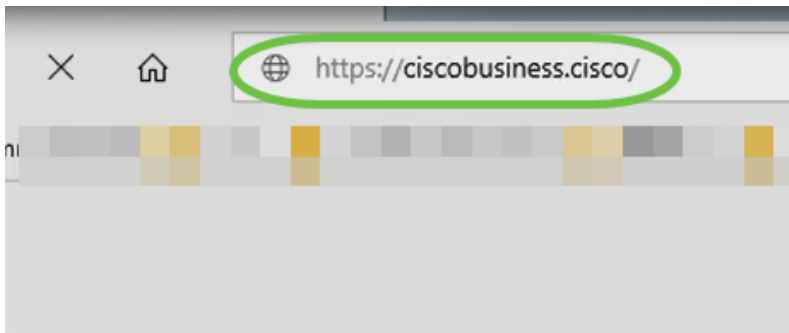
转到PC上的无线选项，选择您配置的网络。单击 Connect。

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。

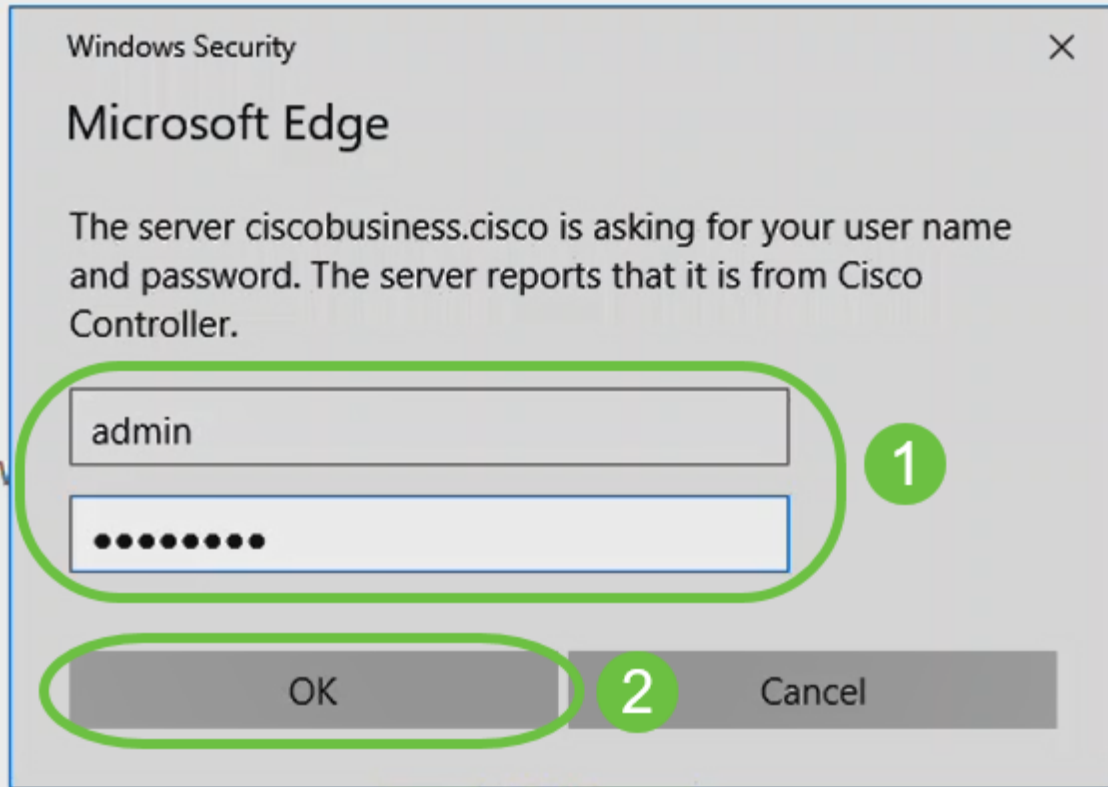
### 步骤 13

单击 Login。



### 步骤 14

使用已配置的凭证登录。Click OK.



© 2015 - 2020 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All third party trademarks are the property of their respective owners.

## 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。

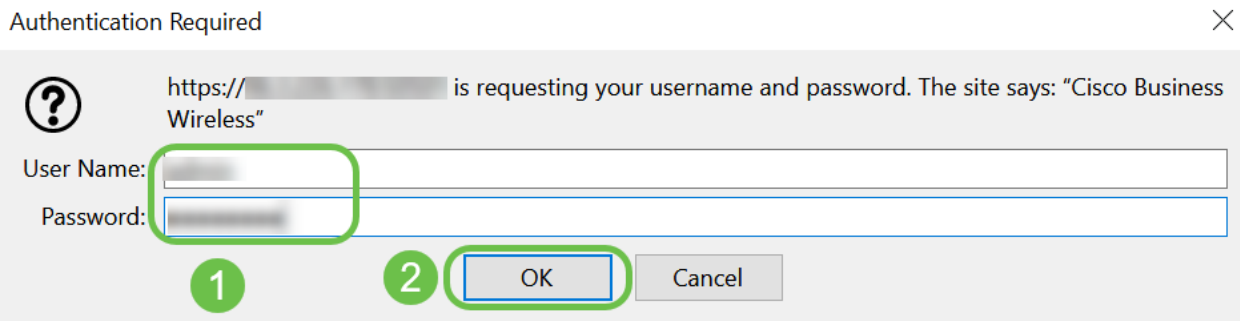
# Cisco Business Wireless Access Point

Welcome! Please click the login button to enter your user name and password



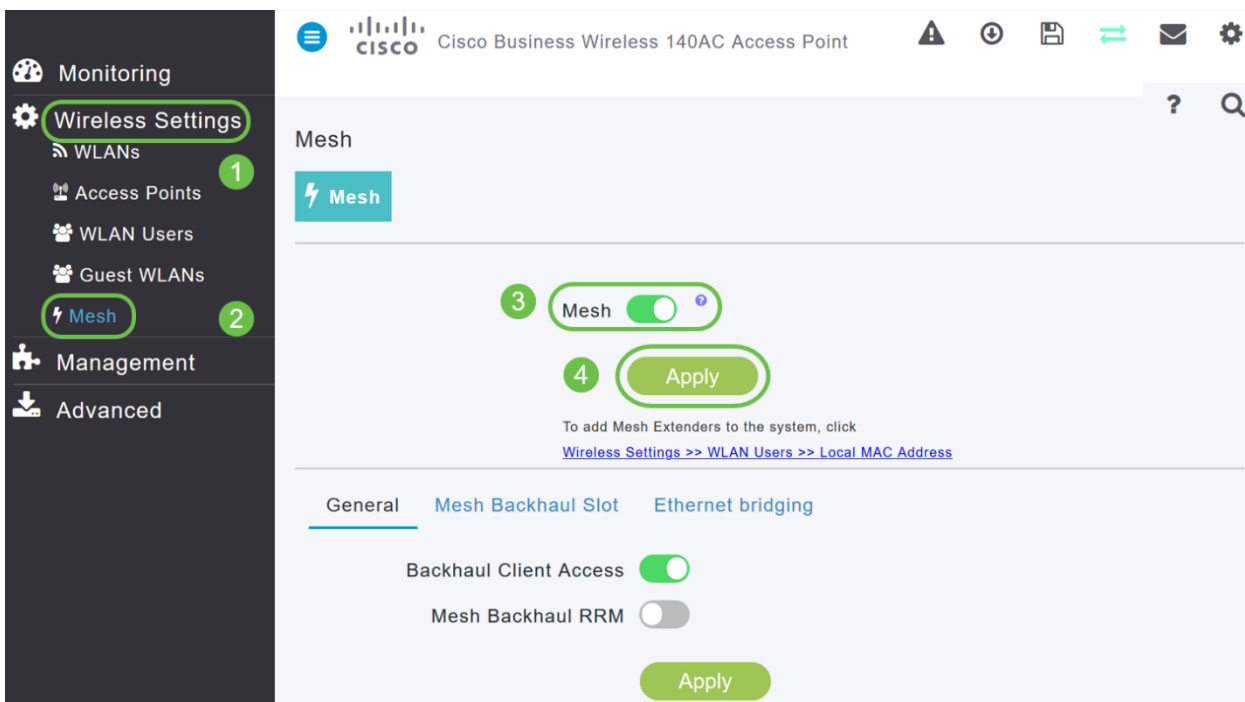
## 步骤 4

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。

The screenshot shows the configuration page for 'Local MAC Addresses' under 'WLAN Users'. The interface includes a sidebar with 'Wireless Settings' and 'WLAN Users' highlighted. The main content area shows a table of MAC addresses and an 'Add MAC Address' button. The table has the following data:

Action	MAC Address	Type	Profile Name	Description
<input type="checkbox"/> ✕	68:ca:e4:6e:15:58	AllowList	Any WLAN/RLAN	CBW142 Mesh Extender
<input type="checkbox"/> ✕	a4:53:0e:1f:e4:88	AllowList	Any WLAN/RLAN	CBW140AC-e488

## 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。

The 'Add MAC Address' dialog box contains the following fields and options:

- MAC Address: 68:ca:e4:6e:15:38
- Description: CBW142 Mesh Extender
- Type:  Block list  Allow list
- Profile Name: Any WLAN/RLAN
- Buttons: Apply, Cancel

## 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)”。

Primary AP Information	
Primary AP Name	Cisco Buisness Wireless
Model	CBW-145AC
Serial Number	ABC1415DEF1
Software Version	10.4.1.0
Up Time	2 days, 17 hours, 45 minutes
Primary AP Time	Sat Feb 27 10:05:15 2021
Timezone	San jose
Country	Multiple Countries : US
Management IP Address	10.10.10.7
Memory Usage	63%
Max Access Points Supported	50

### 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。

## AP Information

Primary AP Name	
Model	CBW140AC-B
Serial Number	
Software Version	10.0.251.24
Up Time	5 days, 1 hour, 57 minutes
Primary AP Time	Sun Mar 29 16:50:26 2020
Timezone	Central Time (US and Canada)
Country	US - United States
Management IP Address	192.168.1.125
Memory Usage	55%
Max Access Points Supported	50

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。

Software Update

Version 10.0.251.24

Transfer Mode TFTP

IP Address(IPv4)/Name \* 172.16.1.35

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**。

Transfer Mode

Cisco.com

HTTP

TFTP

SFTP

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。

Transfer Mode

Automatically Check For Updates

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。

Cisco Business Wireless 140AC Access Point

Software Update

Version 10.0.251.24

Transfer Mode

Automatically Check For Updates

Last Software Check  [Check Now](#)

Latest Software Release  ?

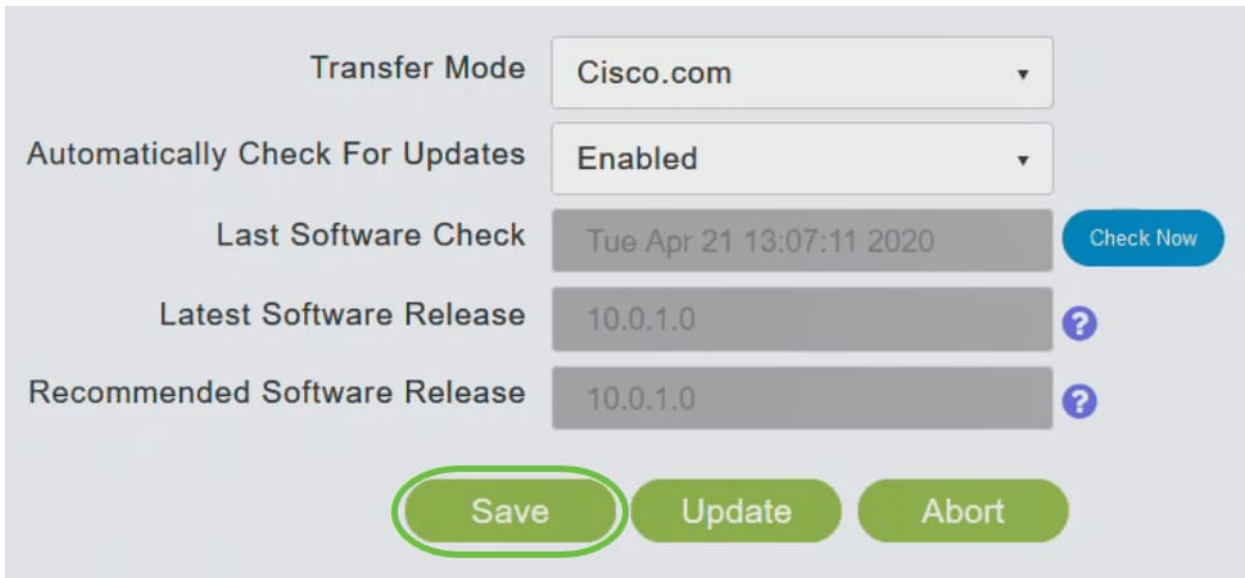
Recommended Software Release  ?

[Save](#) [Update](#) [Abort](#)

Software update is available for your Cisco Business Wireless AP/APs on cisco.com

### 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。

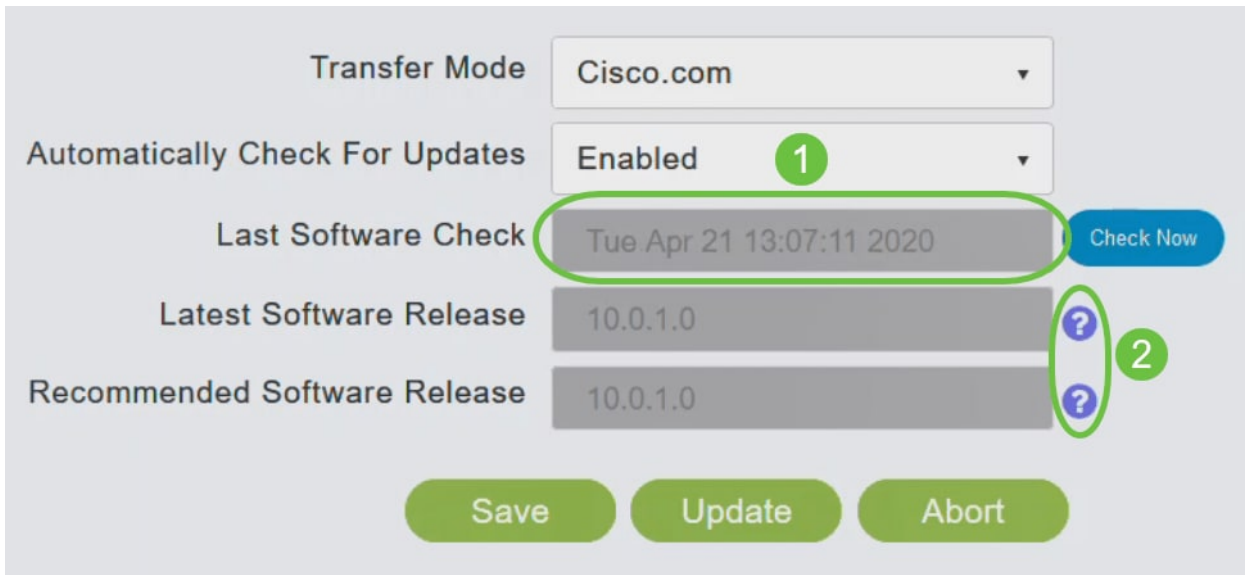


The image shows a software update configuration interface. It includes a 'Transfer Mode' dropdown set to 'Cisco.com', an 'Automatically Check For Updates' dropdown set to 'Enabled', and a 'Last Software Check' field showing 'Tue Apr 21 13:07:11 2020'. There are also fields for 'Latest Software Release' and 'Recommended Software Release', both showing '10.0.1.0'. A 'Check Now' button is located to the right of the 'Last Software Check' field. At the bottom, there are three buttons: 'Save', 'Update', and 'Abort'. The 'Save' button is highlighted with a green oval.

Transfer Mode	Cisco.com
Automatically Check For Updates	Enabled
Last Software Check	Tue Apr 21 13:07:11 2020
Latest Software Release	10.0.1.0
Recommended Software Release	10.0.1.0

Buttons: Save, Update, Abort

“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。



The image shows the same software update configuration interface as above, but with annotations. A green circle with the number '1' is placed next to the 'Automatically Check For Updates' dropdown. A green oval highlights the 'Last Software Check' field. A green circle with the number '2' is placed next to the question mark icons in the 'Latest Software Release' and 'Recommended Software Release' fields. The 'Check Now' button is also visible.

Transfer Mode	Cisco.com
Automatically Check For Updates	Enabled
Last Software Check	Tue Apr 21 13:07:11 2020
Latest Software Release	10.0.1.0
Recommended Software Release	10.0.1.0

Buttons: Save, Update, Abort

## 步骤 6

您可以随时通过单击“立即检查”手动运行软件检查。

Transfer Mode	Cisco.com	▼
Automatically Check For Updates	Enabled	▼
Last Software Check	Tue Apr 21 13:07:11 2020	<a href="#">Check Now</a>
Latest Software Release	10.0.1.0	?
Recommended Software Release	10.0.1.0	?

[Save](#) [Update](#) [Abort](#)

## 步骤 7

要继续软件更新，请单击**Update**。

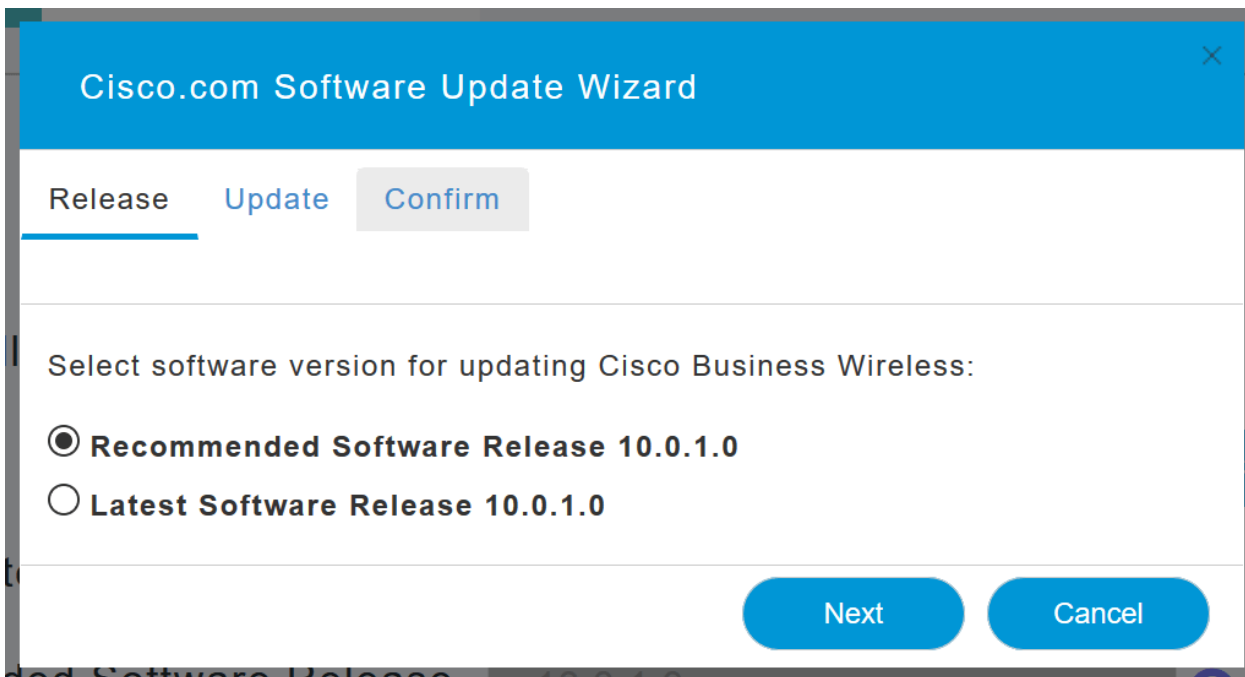
Transfer Mode	Cisco.com	▼
Automatically Check For Updates	Enabled	▼
Last Software Check	Tue Apr 21 13:07:11 2020	<a href="#">Check Now</a>
Latest Software Release	10.0.1.0	?
Recommended Software Release	10.0.1.0	?

[Save](#) [Update](#) [Abort](#)

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：

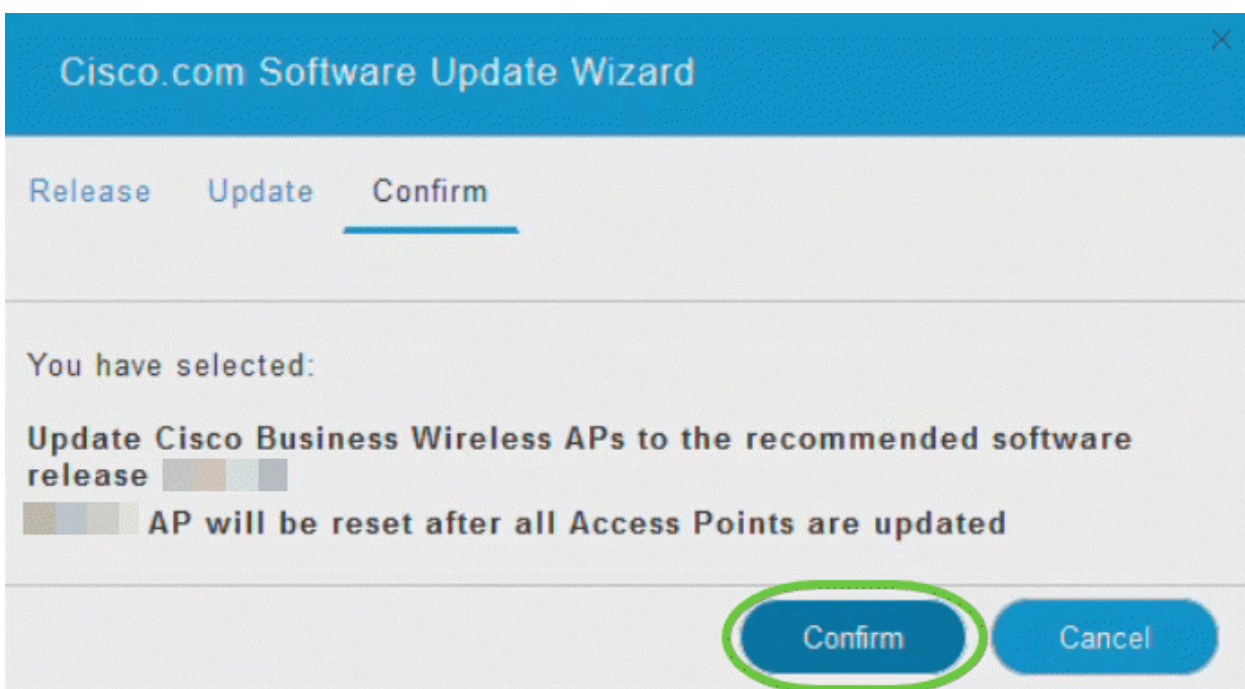
- 版本选项卡 — 指定是要更新到推荐的软件版本还是最新软件版本。
- Update选项卡 — 指定何时应重置AP。您可以选择立即完成，或安排以后的时间。要将主AP设置为在映像预下载完成后自动重新启动，请选中自动重新启动复选框。
- “确认”选项卡 — 确认您的选择。

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 )”。

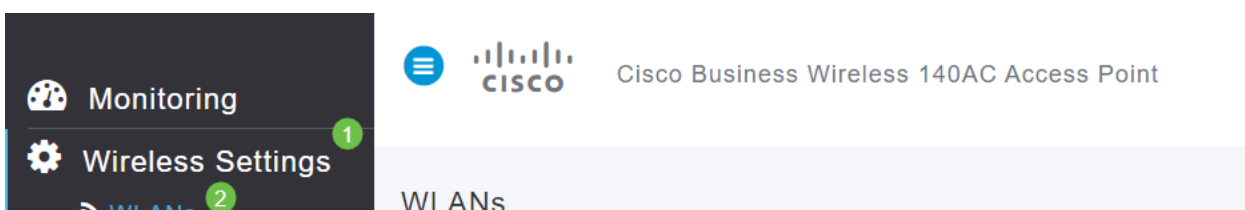


## 在Web UI上创建WLAN

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。

Add new WLAN/RLAN

General | WLAN Security | VLAN & Firewall | Traffic Shaping | Scheduling

WLAN ID: 2 **1**

Type: WLAN **2**

Profile Name \*: Engineering **3**

SSID \*: Engineering **3**

WLANs with same SSID can be configured, unless layer-2 security settings are different.

Enable:

Radio Policy: ALL **?**

Broadcast SSID:

Local Profiling:  **?**

**4**

Apply Cancel

## 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。

General **WLAN Security** VLAN & Firewall Traffic Shaping Scheduling

Guest Network

Captive Network Assistant

MAC Filtering

Security Type WPA2 Personal

Passphrase Format ASCII

Passphrase \* VerySecure 3

Confirm Passphrase \* VerySecure 2

1  Show Passphrase

Password Expiry

4

## 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。

Action	Active	Type	Name	SSID	Security Policy	Radio Policy
<input checked="" type="checkbox"/>	Enabled	WLAN			Personal(WPA2)	ALL
<input checked="" type="checkbox"/>	Enabled	WLAN	Engineering	Engineering	Personal(WPA2)	ALL

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](https://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 )。



The screenshot displays the Cisco Business Wireless 140AC Access Point Web UI. The left sidebar is dark grey with white text and icons. The main content area is light grey. The 'WLANs' section shows two active items: 'Active WLANs' and 'Active RLANS', both with a count of 1. Below this is a table with the following data:

Action	Active	Type	Name	SSID	Security Policy	Radio Policy	
	Enabled	WLAN	EZ1K	EZ1K	Personal(WPA2)	ALL	
	Enabled	RLAN	DEFAULT_RLAN	DEFAULT_RLAN	Open	N/A	

#### 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。

**Add new WLAN/RLAN**

General | WLAN Security | VLAN & Firewall | Traffic Shaping | Scheduling

WLAN ID: 2

Type: WLAN

Profile Name \*: CBWGuest

SSID \*: CBWGuest

WLANs with same SSID can be configured, unless layer-2 security settings are different.

Enable:

Radio Policy: ALL

Broadcast SSID:

Local Profiling:

Apply | Cancel

#### 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。

## Add new WLAN/RLAN

General WLAN Security VLAN & Firewall Traffic Shaping Scheduling

Guest Network  1

Captive Network Assistant  2

MAC Filtering

Captive Portal Internal Splash Page ▼ 3

Access Type Social Login ▼

ACL Name(IPv4) None ▼ ?

ACL Name(IPv6) None ▼ ?

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。

The screenshot shows the 'Add new WLAN/RLAN' configuration page. The 'WLAN Security' tab is active. The 'Access Type' dropdown menu is open, showing options: Local User Account, Web Consent, Email Address (marked with a green circle '1'), RADIUS, WPA2 Personal, and Social Login. The 'Apply' button is marked with a green circle '2'.

## 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。

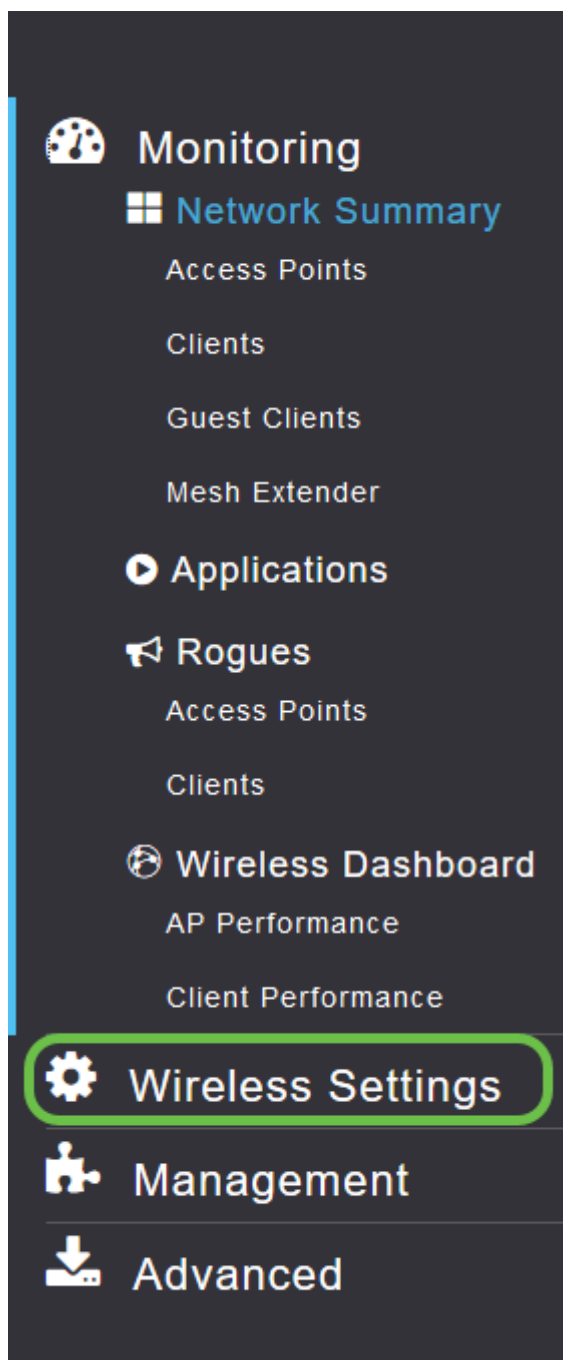
## 第 1 步

如果未看到左侧菜单栏，请导航到屏幕左侧的菜单。

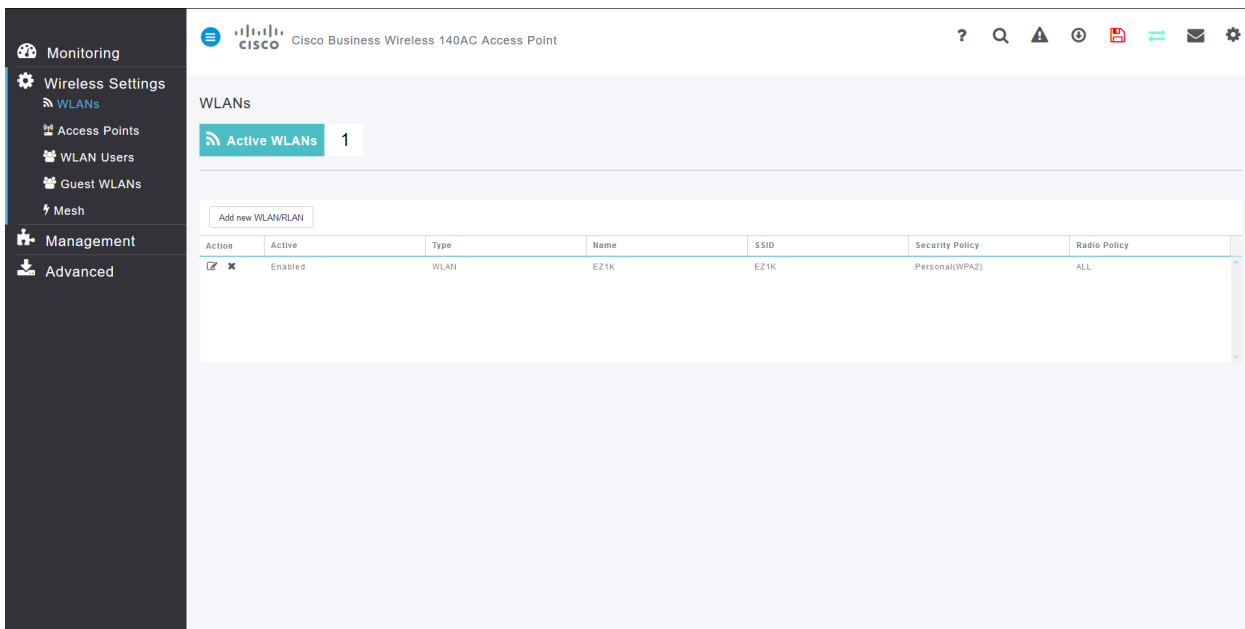


## 步骤 2

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)”。

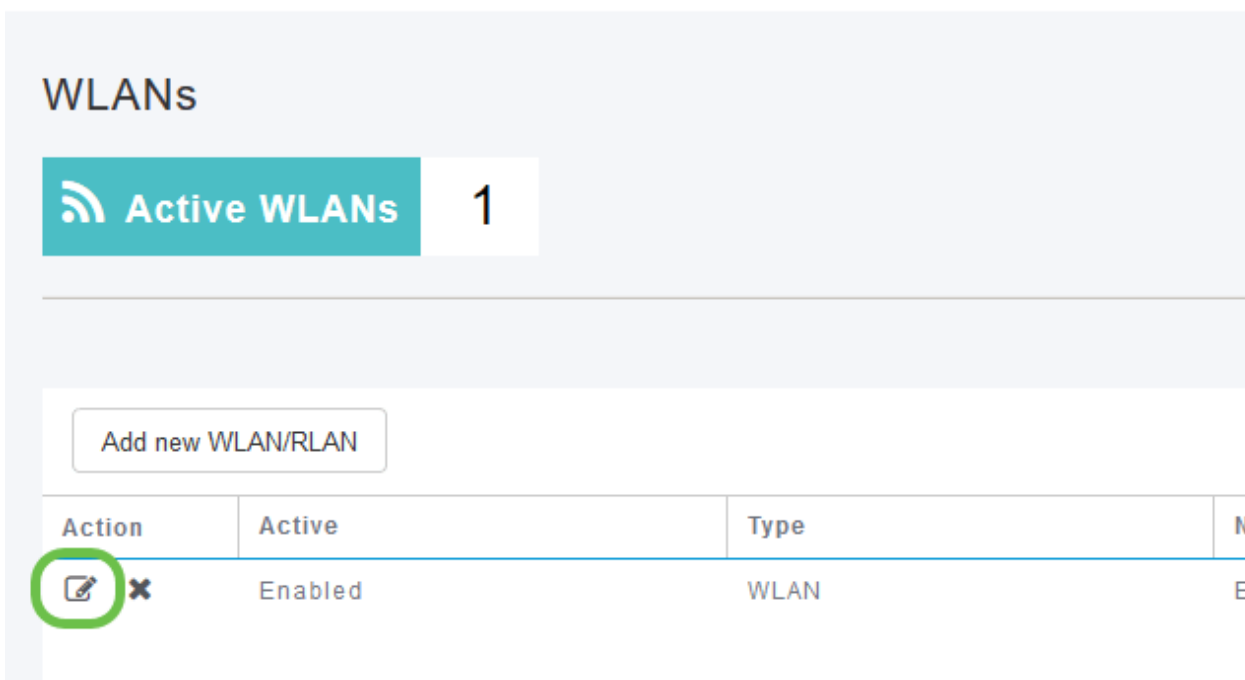
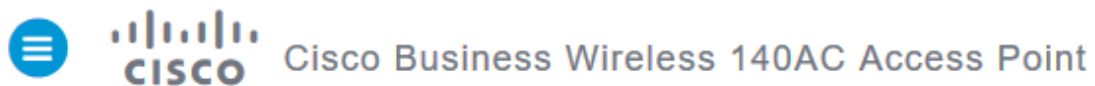


下图与您单击“无线设置”链接时看到的图像类似。

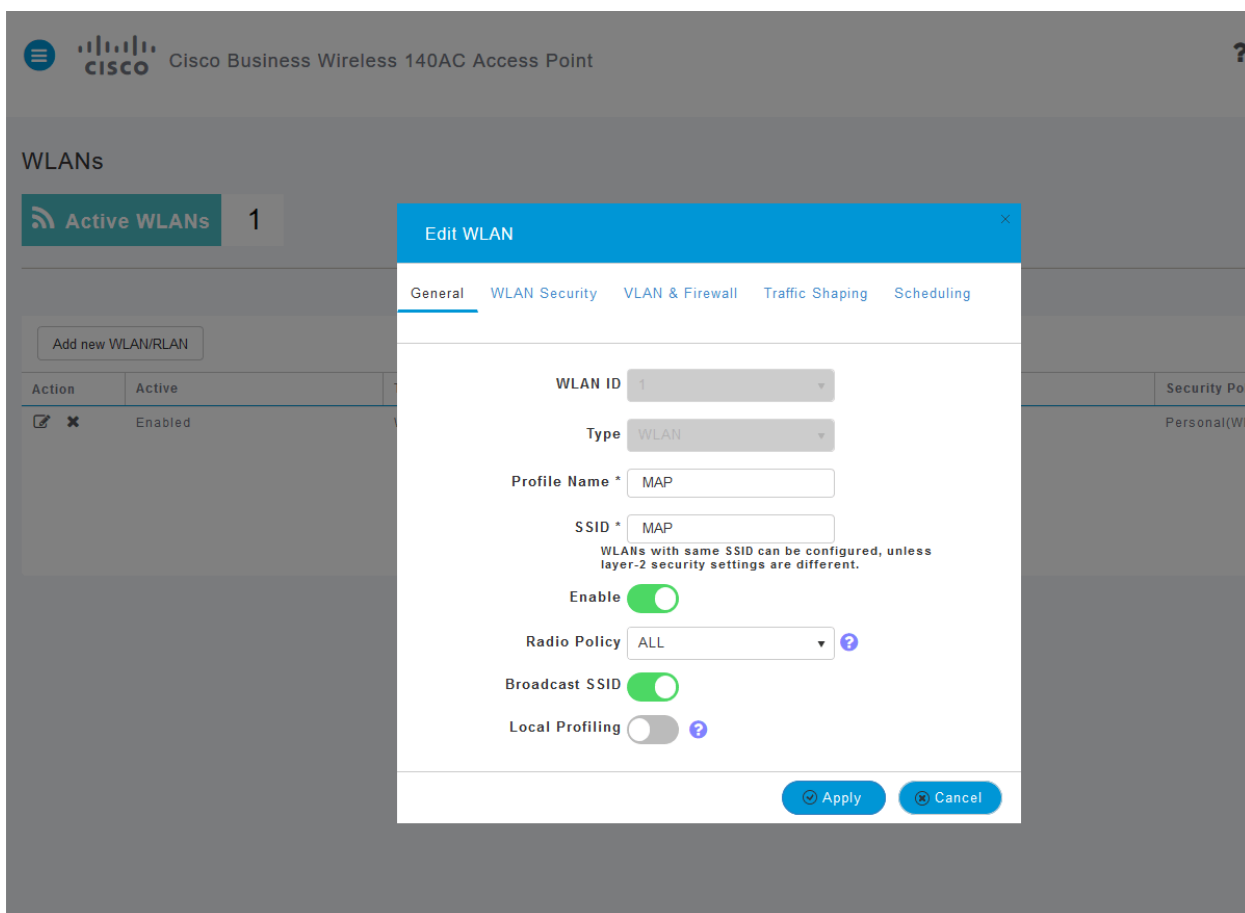


### 步骤 3

单击要启用应用的无线局域网左侧的**编辑图标**。

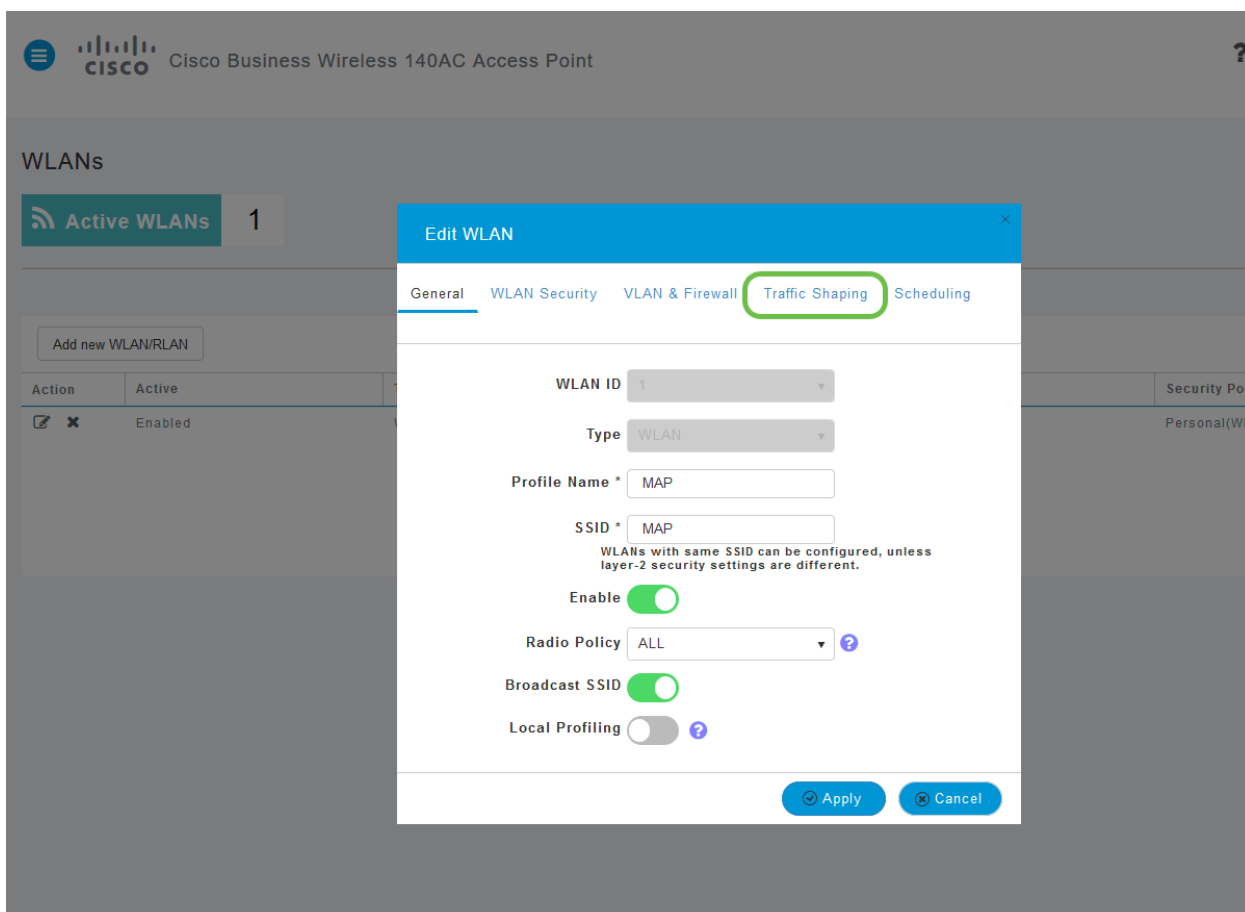


由于您最近添加了WLAN，因此您的“**编辑WLAN**”页面可能显示类似于以下内容：



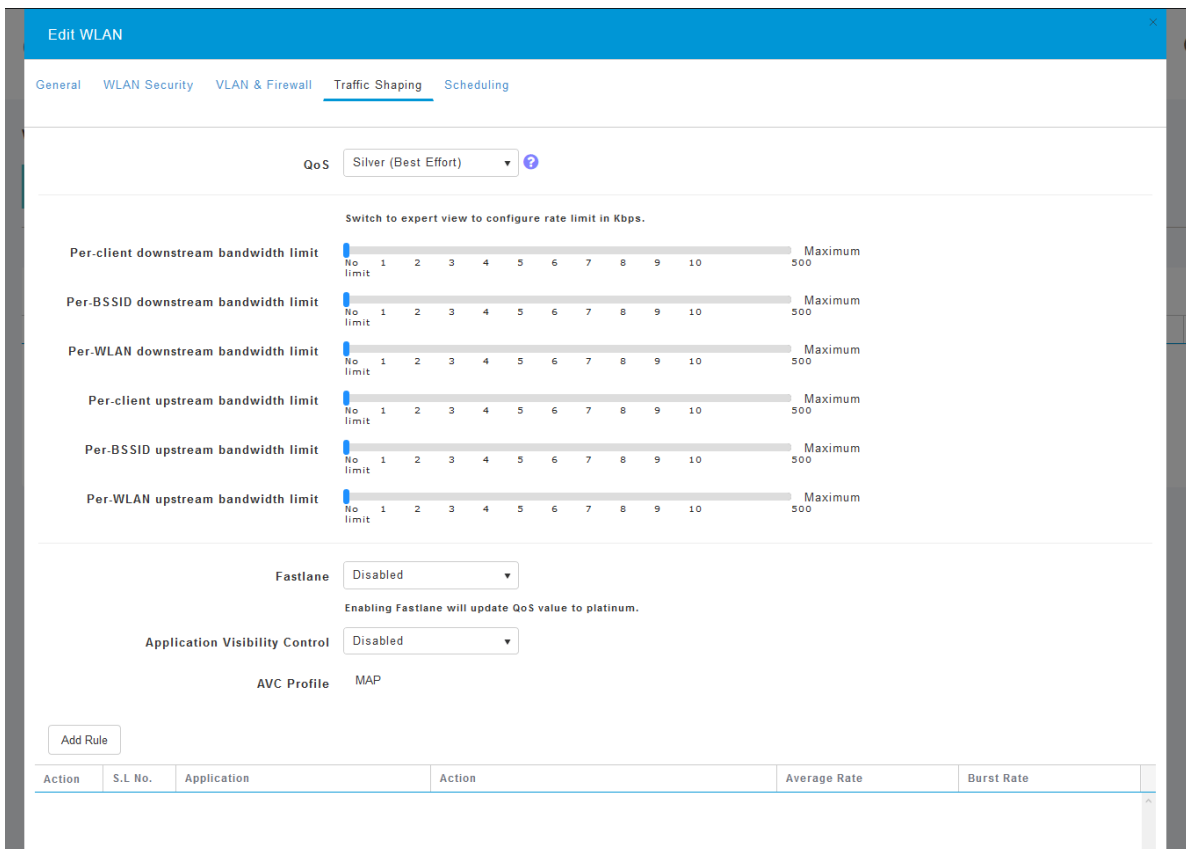
#### 步骤 4

单击“流量整形”选项卡。



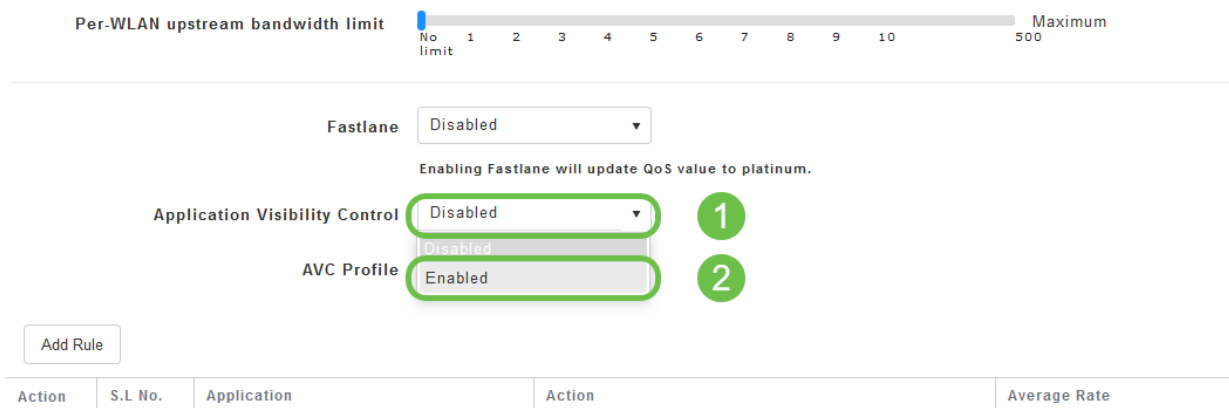
您的屏幕可能显示如下：





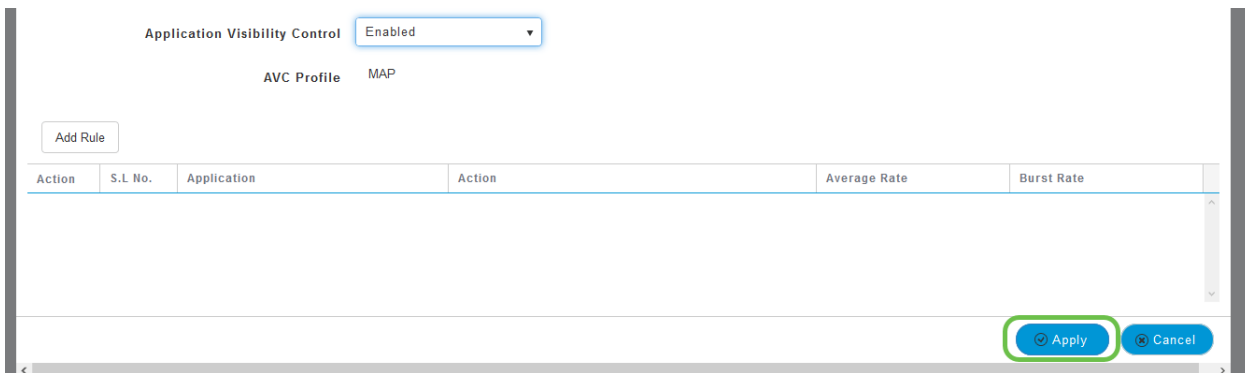
## 步骤 5

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

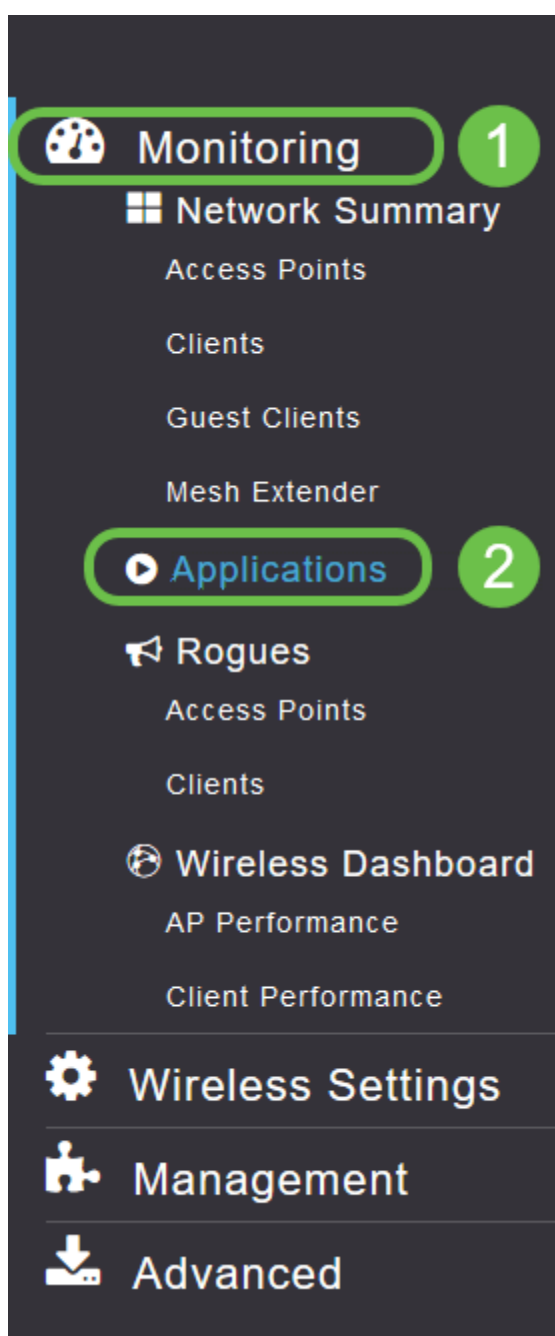
单击应用按钮。



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。



Applications	Groups	Data Usage	Throughput
ssl	browsing	2.6 MB	1.1 Mbps
outlook-web-service	email	819.4 KB	233.1 kbps
cisco-spark	voice-and-video	735.6 KB	0.0 bps
secure-pop3	email	453.1 KB	0.0 bps
ms-office-365	business-and-productivity-tools	238.2 KB	75.1 kbps
webex-meeting	voice-and-video	132.3 KB	0.0 bps
samsung	browsing	79.4 KB	0.0 bps
windows-azure	backup-and-storage	74.0 KB	5.7 kbps
twitter	social-networking	48.6 KB	0.0 bps
icloud	consumer-internet	47.3 KB	0.0 bps

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。

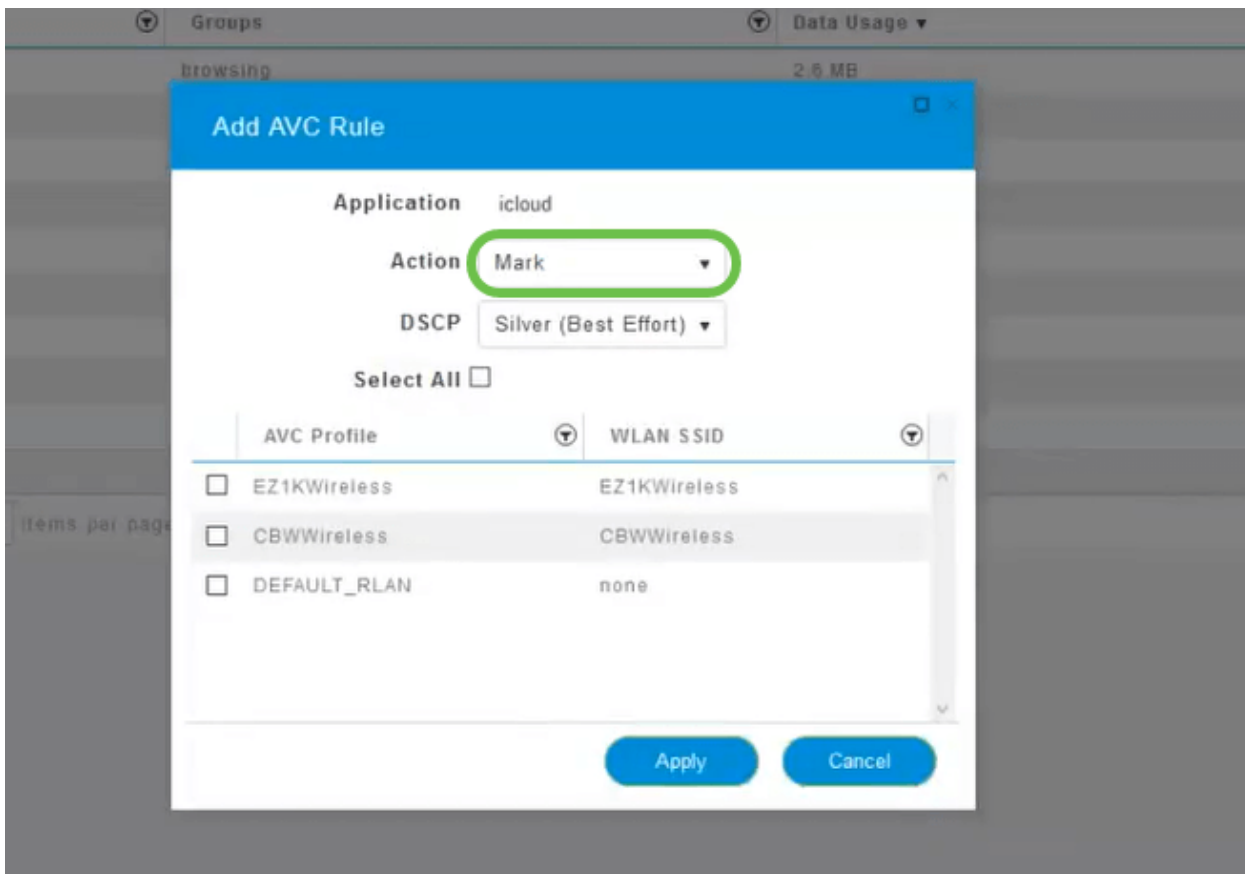
## 步骤 8

点击要管理的流量类型的行。

Applications	Groups	Data Usage	Throughput
ssl	browsing	2.6 MB	1.1 Mbps
outlook-web-service	email	819.4 KB	233.1 kbps
cisco-spark	voice-and-video	735.6 KB	0.0 bps
secure-pop3	email	453.1 KB	0.0 bps
ms-office-365	business-and-productivity-tools	238.2 KB	75.1 kbps
webex-meeting	voice-and-video	132.3 KB	0.0 bps
samsung	browsing	79.4 KB	0.0 bps
windows-azure	backup-and-storage	74.0 KB	5.7 kbps
twitter	social-networking	48.6 KB	0.0 bps
icloud	consumer-internet	47.3 KB	0.0 bps

## 步骤 9

单击Action下拉框，选择如何处理该流量类型。



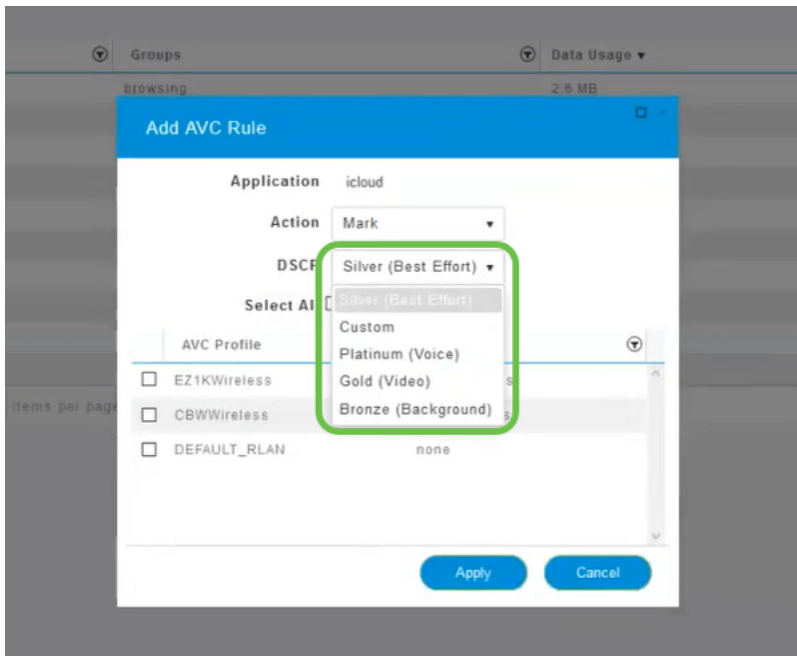
在本例中，我们将此选项留在*Mark*。

#### 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。



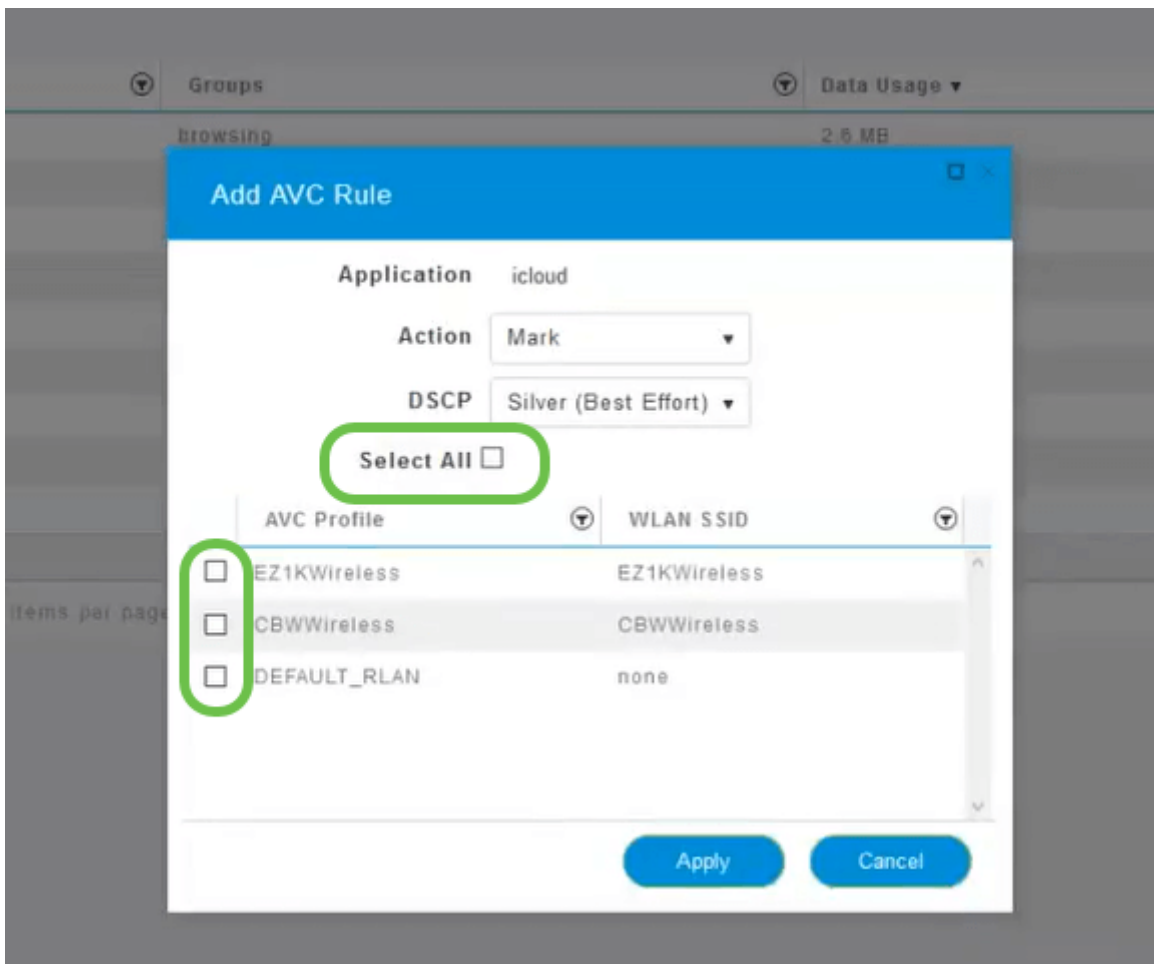
以下是要标记的流量的DSCP选项。这些选项从更少的资源进入您编辑的流量类型可用的更多资源。

- 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。

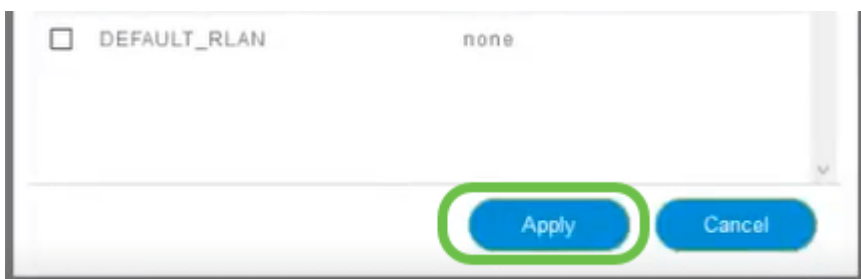
## 步骤 11

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

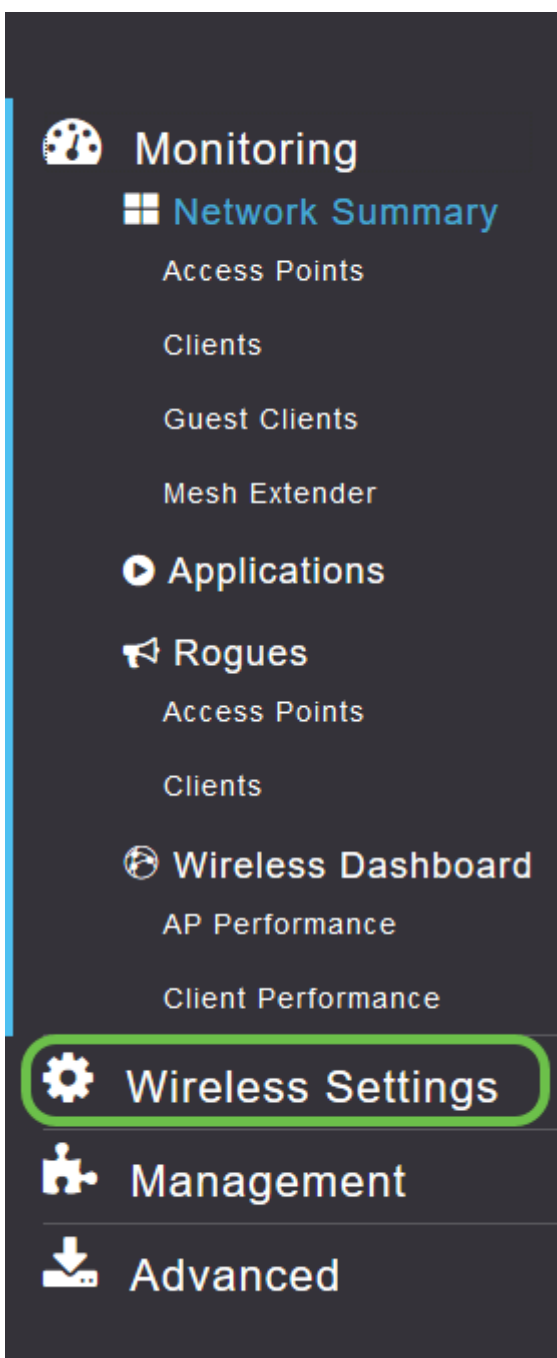
有关这些客户端的统计信息包括使用的数据量和吞吐量。

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。

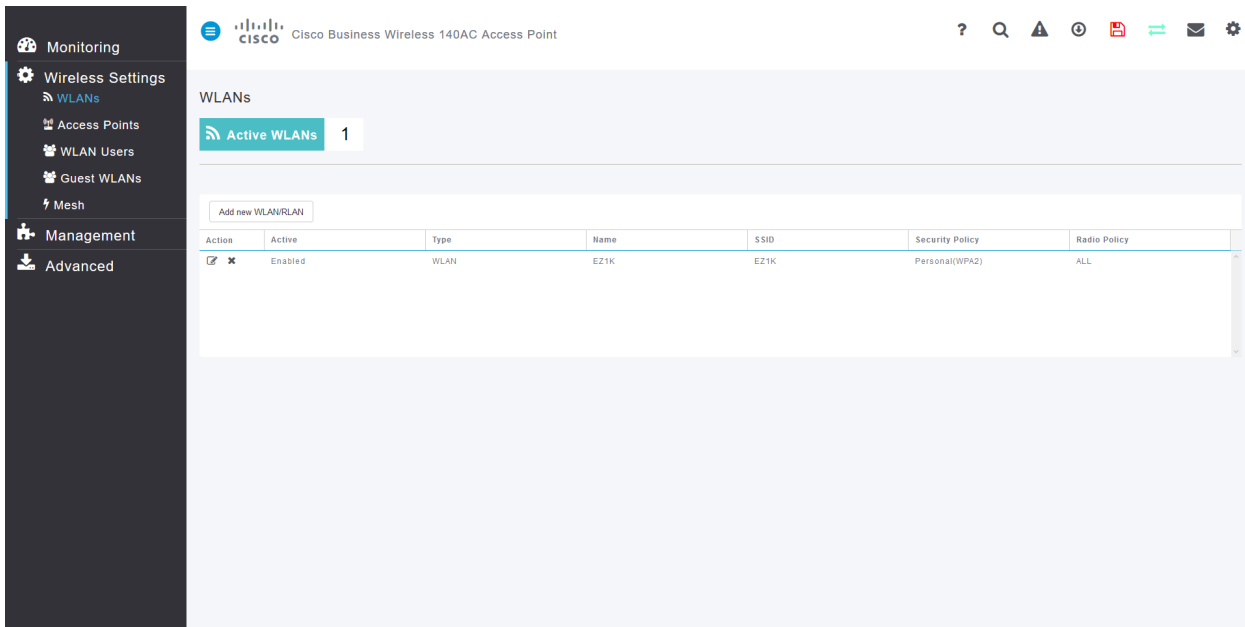
## 第 1 步

单击**Wireless Settings**。



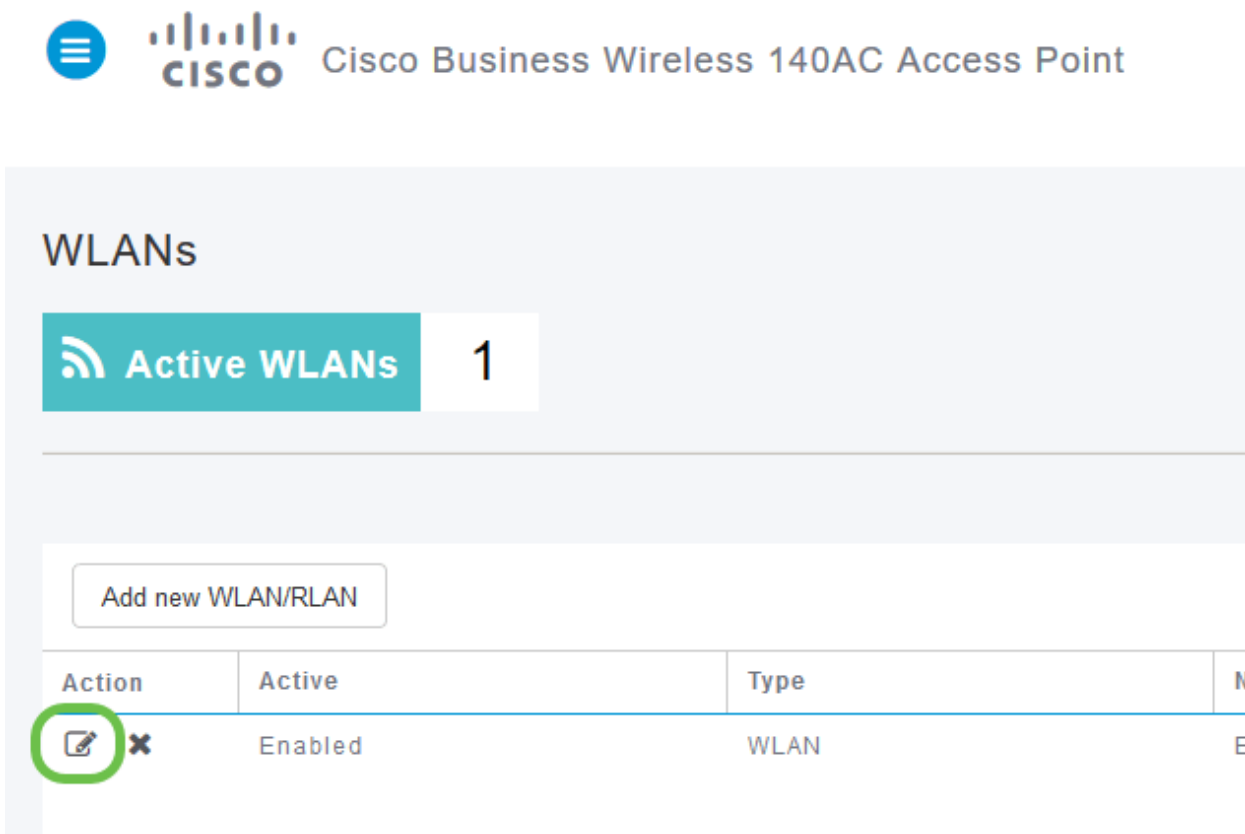
以下内容类似于您单击“无线设置”链接时看到的内容：





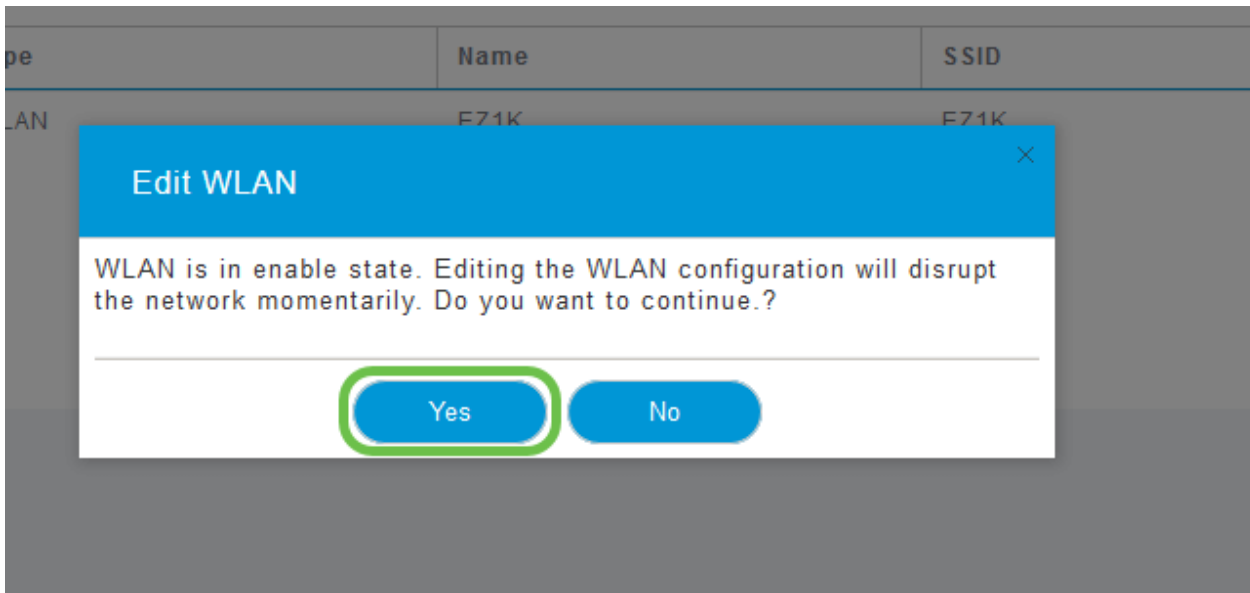
## 步骤 2

确定要用于应用的WLAN，然后单击左侧的编辑图标。



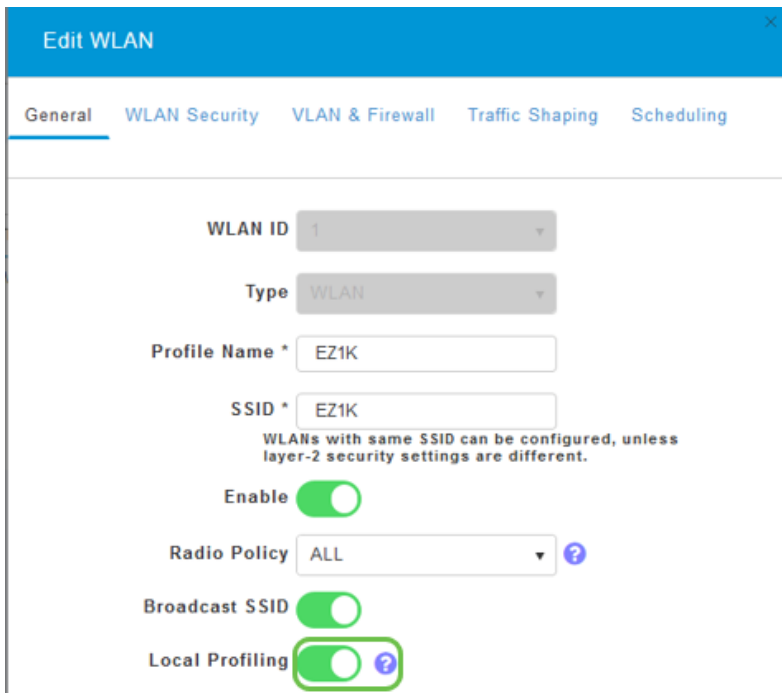
## 步骤 3

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。



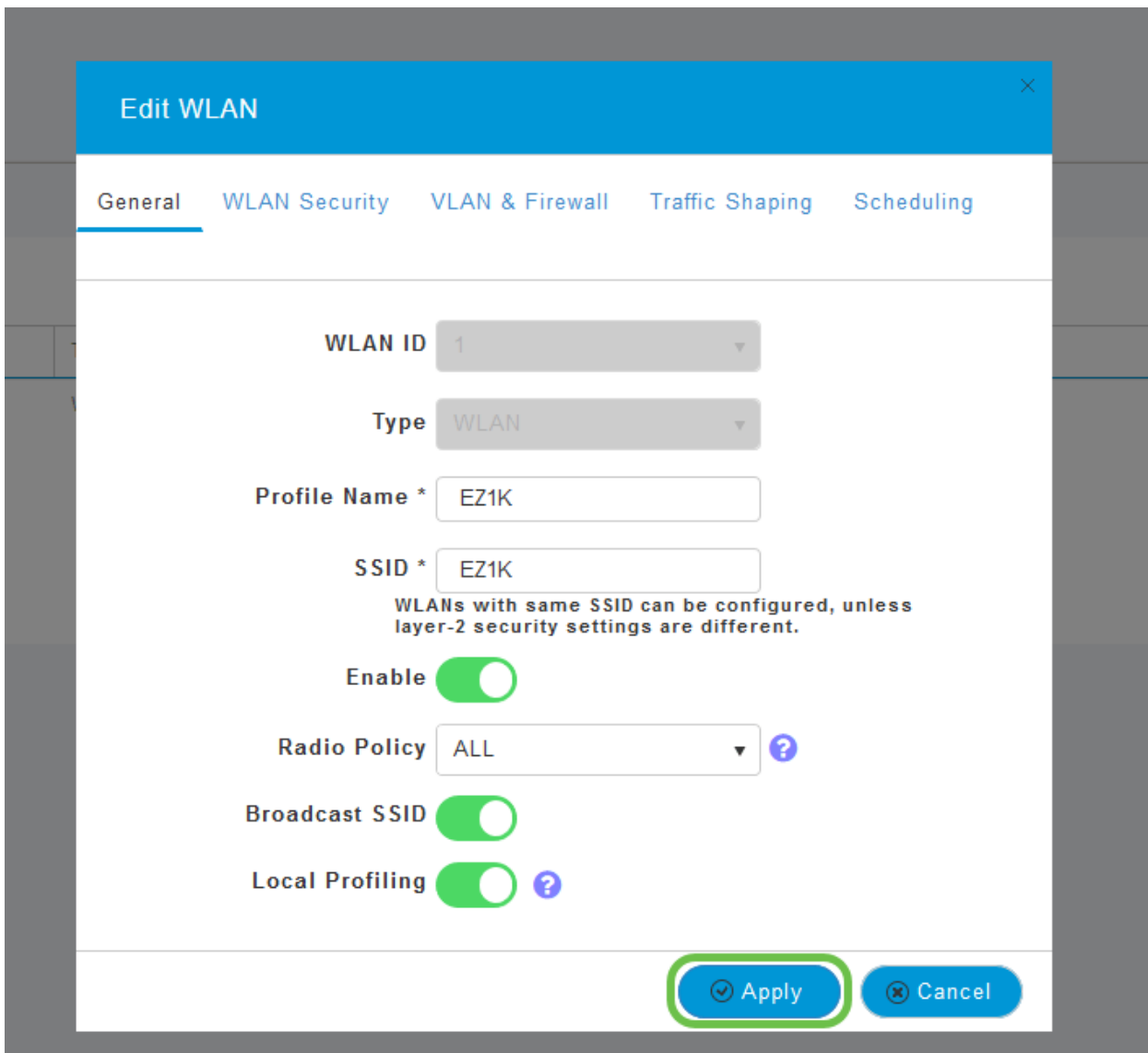
#### 步骤 4

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。

Client Identity	Device Type	Usage	Throughput
1 Anthony's-iPad	Apple-iPad	1.0 GB	260.3 bps
2 Galaxy-S9	Android-Samsung-Galax...	8.4 MB	1.2 kbps

## 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RV260P VPN路由器](#)

- [思科企业140AC接入点](#)
- [思科企业142ACM网状扩展器](#)