

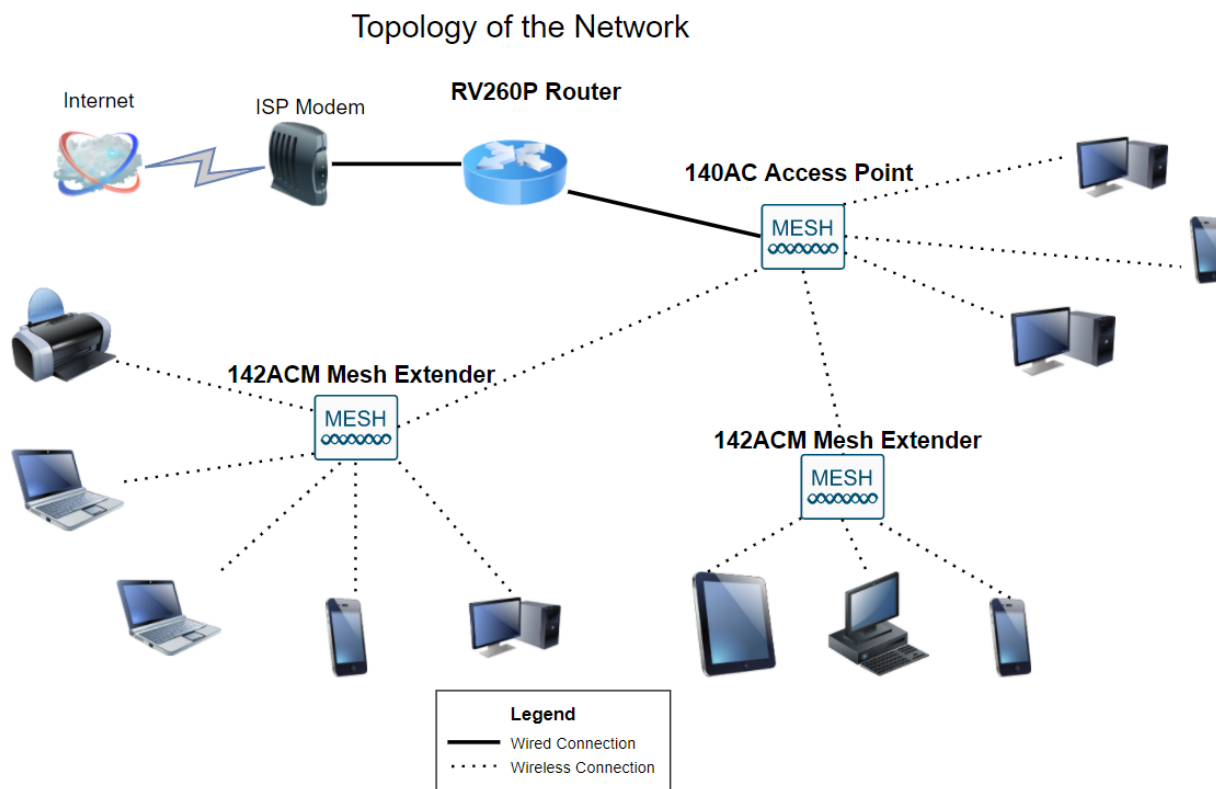
# Total Network Configuration: RV260P with Cisco Business Wireless and the Web UI

## Objective:

This guide will show you how to configure a wireless mesh network using an RV260P router, a CBW140AC access point, and two CBW142ACM mesh extenders.

This article uses the Web User Interface (UI) to set up the mesh wireless network. If you prefer to use the mobile application, which is recommended for easy wireless setup, [click to jump to the article that uses the mobile application](#). If you want to use the Web UI, keep reading!

## Topology:



## Introduction

Here you are, ready to set up your new network. It's an exciting day! In this scenario, we are using an RV260P router. This router provides Power over Ethernet (PoE) which allows you to plug the CBW140AC into the router instead of a switch. The CBW140AC and the CBW142ACM mesh extenders will be used to create a wireless mesh network.

If you are unfamiliar with some of the terms used in this document or want more details about Mesh Networking, check out the following articles:

- [Cisco Business: Glossary of New Terms](#)

- [Welcome to Cisco Business Wireless Mesh Networking](#)
- [Frequently Asked Questions \(FAQ\) for a Cisco Business Wireless Network](#)

Are you ready? Let's get to it!

## Applicable Devices | Software Version

- RV260P | 1.0.0.17
- CBW140AC | 10.3.1.0
- CBW142ACM | 10.3.1.0 (at least one mesh extender is needed for the mesh network)

## Table of Contents

- [Before you Get Started](#)
- [Configure the RV260P Router](#)
  - [RV260P Out of the Box](#)
  - [Set Up the Router](#)
  - [Troubleshooting the Internet Connection](#)
  - [Initial Configuration](#)
  - [Upgrade Firmware if Needed](#)
  - [Configure VLANs \(Optional\)](#)
  - [Edit an IP address \(Optional\)](#)
  - [Add a Static IP](#)
- [Configure the CBW140AC](#)
  - [CBW140AC Out of the Box](#)
  - [Set Up the 140AC Primary Wireless Access Point on the Web UI](#)
- [Wireless Troubleshooting Tips](#)
- [Configure the CBW142ACM Mesh Extenders Using the Web UI](#)
- [Check and Update Software Using the Web UI](#)
- [Create WLANs on the Web UI](#)
- [Create a Guest WLAN using the Web UI \(Optional\)](#)
- [Application Profiling using the Web UI \(Optional\)](#)
- [Client Profiling using the Web UI \(Optional\)](#)

## Before you Get Started

1. Make sure you have a current Internet connection for setup.
2. Contact your ISP to find out any special instructions they have when using your RV260 router. Some ISPs offer gateways with built-in routers. If you have a gateway with an integrated router, you may have to disable the router and pass the Wide Area Network (WAN) IP address (the unique Internet protocol address that the Internet provider assigns to your account) and all network traffic through to your new router.
3. Decide where to place the router. You will want an open area if possible. This may not be easy because you must connect the router to the broadband gateway (modem) from your Internet Service Provider (ISP).

# Configure the RV260P Router

A router is essential in a network because it routes packets. It enables a computer to communicate with other computers that are not on the same network or subnet. A router accesses a routing table to determine where packets should be sent. The routing table lists destination addresses. Static and dynamic configurations can both be listed on the routing table in order to get packets to their specific destination.

Your RV260P comes with default settings that are optimized for many small businesses. However, your network demands or Internet Service Provider (ISP) might require you to modify a few of these settings. After you contact your ISP for the requirements, you can make changes using the Web User Interface (UI).

## RV260P Out of the Box

### Step 1

Connect the Ethernet cable from one of the RV260P LAN (Ethernet) ports to the Ethernet port on the computer. You will need an adapter if your computer doesn't have an Ethernet port. The terminal must be in the same wired subnetwork as the RV260P to perform the initial configuration.

### Step 2

Be sure to use the power adapter that is supplied with the RV260P. Using a different power adapter could damage the RV260P or cause USB dongles to fail. The power switch is on by default.

Connect the power adapter to the 12VDC port of the RV260P, but don't plug it into power yet.

### Step 3

Make sure the modem is turned off.

### Step 4

Use an Ethernet cable to connect your cable or DSL modem to the WAN port on the RV260P.

### Step 5

Plug the other end of the RV260P adapter into an electrical outlet. This will power on the RV260. Plug the modem back in so it can power up as well. The power light on the front panel is solid green when the power adapter is connected properly, and the RV260P is finished booting.

## Set Up the Router

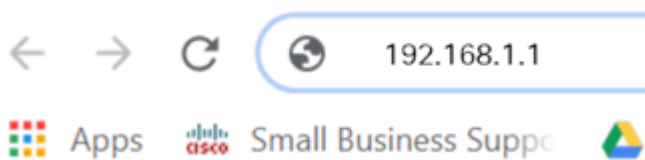
The prep work is done, now it's time to do some configurations! To launch the Web UI, follow these steps:

### Step 1

If your computer is configured to become a Dynamic Host Configuration Protocol (DHCP) client, an IP address in the 192.168.1.x range is assigned to the PC. DHCP automates the process of assigning IP addresses, subnet masks, default gateways, and other settings to computers. Computers must be set to participate in the DHCP process to obtain an address. This is done by selecting to obtain an IP address automatically in the properties of TCP/IP on the computer.

### Step 2

Open a web browser such as Safari, Internet Explorer, or Firefox. In the address bar, enter the default IP address of the RV260P which is 192.168.1.1.



### Step 3

The browser might issue a warning that the website is untrusted. Continue to the website. If you are not connected, jump down to [Troubleshooting the Internet Connection](#).



#### 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](#)



### Step 4

When the sign-in page appears, enter the default username *cisco* and the default password *cisco*. Both the username and password are case sensitive.



## 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.

### Step 5

Click **Login**. The *Getting Started* page appears. Now that you have confirmed the connection and logged in to the router, jump to the [Initial Configuration](#) section of this article.

## Troubleshooting the Internet Connection

Dang it, if you are reading this you are probably having trouble connecting to the Internet or the Web UI. One of these solutions should help.

On your connected Windows OS, you can test your network connection by opening the command prompt. Enter ping 192.168.1.1 (the default IP address of the router). If the request times out, you are not able to communicate with the router.

If connectivity is not happening, you can check out [Troubleshooting on RV160 and RV260 Routers](#).

Some other things to try:

1. Verify that your web browser is not set to Work Offline.
2. Check the local area network connection settings for your Ethernet adapter. The PC should obtain an IP address through DHCP. Alternatively, the PC can have a static IP address in the 192.168.1.x range with the default gateway set to 192.168.1.1 (the default IP address of the RV260P). To connect, you may need to modify the network settings of the RV260P. If you are using Windows 10, check out [Windows 10 directions to modify the network settings](#).
3. If you have existing equipment occupying the 192.168.1.1 IP address, you'll need to resolve this conflict for the network to operate. More on this at the end of this section, or [click here to be taken there directly](#).

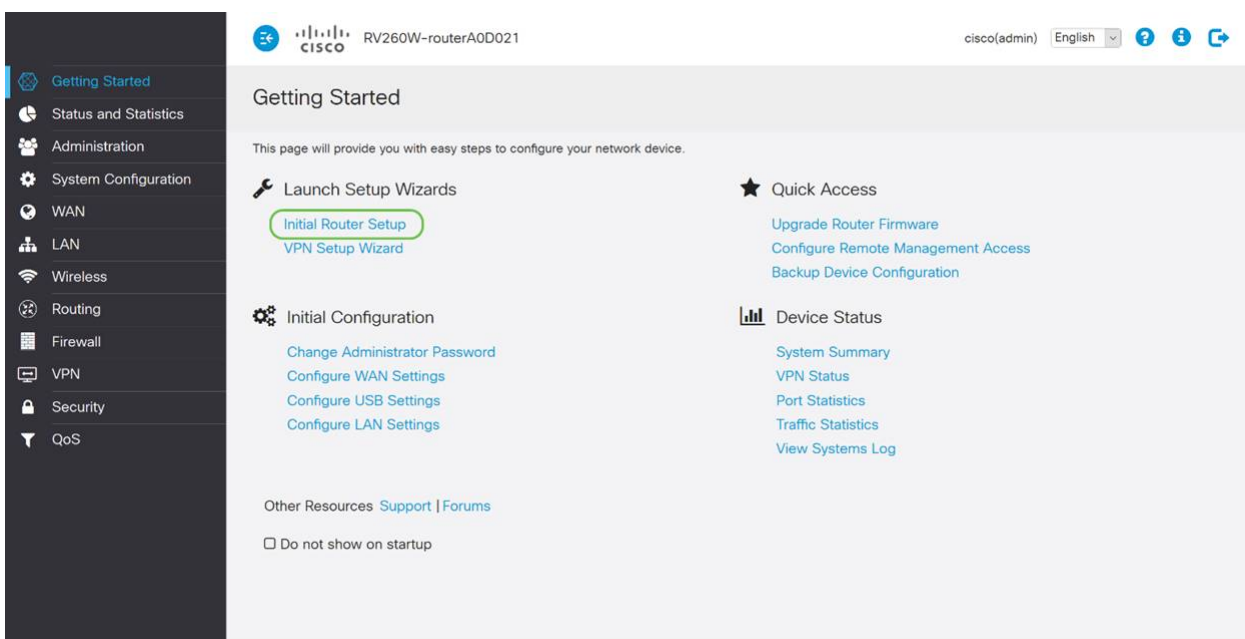
4. Reset the modem and the RV260P by powering off both devices. Next, power on the modem and let it sit idle for about 2 minutes. Then power on the RV260P. You should now receive a WAN IP address.
5. If you have a DSL modem, ask your ISP to put the DSL modem into bridge mode.

## Initial Configuration

We recommend that you go through the Initial Setup Wizard steps listed in this section. You can change these settings at any time.

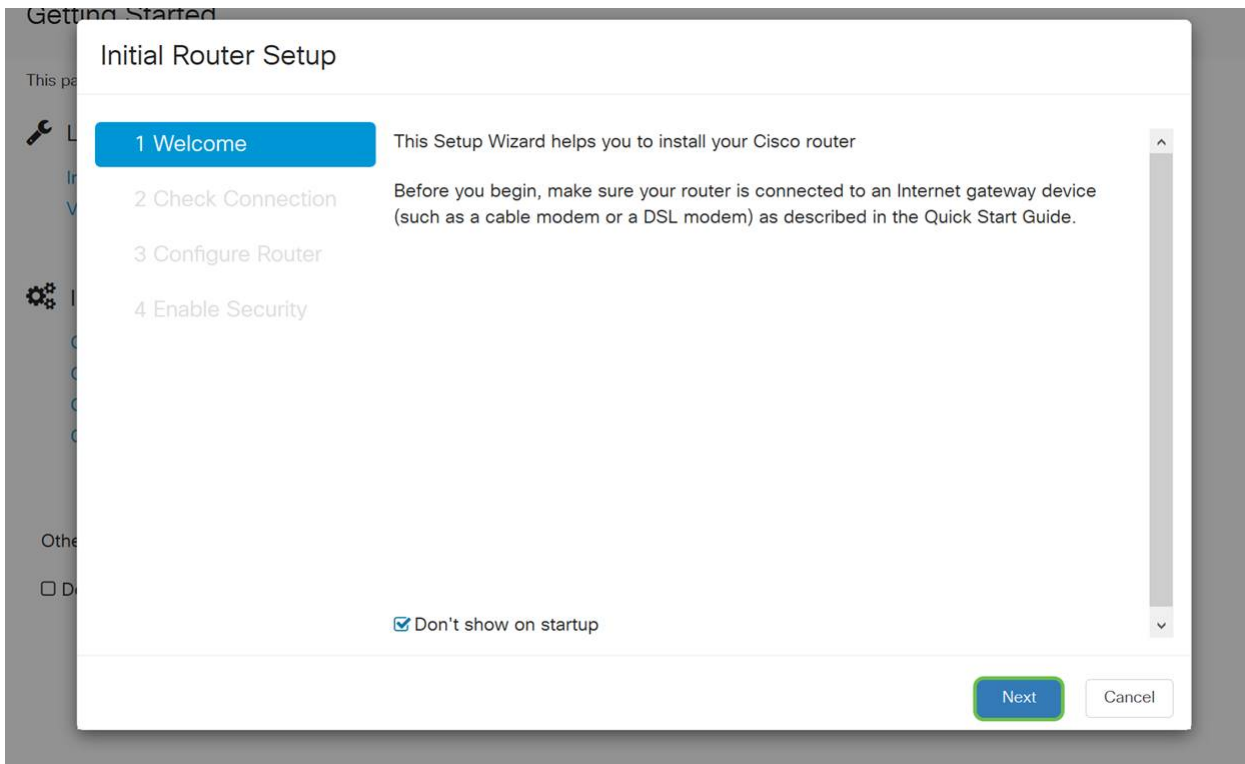
### Step 1

Click **Initial Setup Wizard** from the *Getting Started* Page.



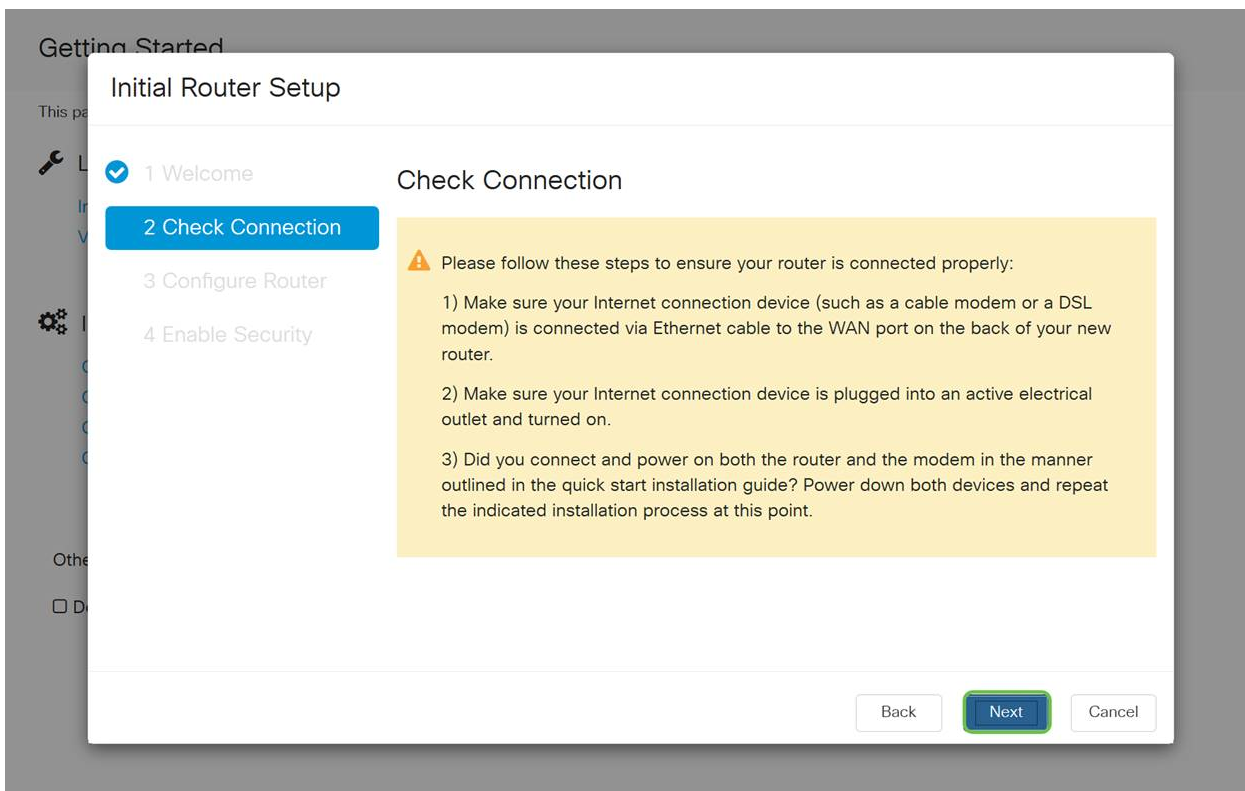
### Step 2

This step confirms the cables are connected. Since you confirmed this already, click **Next**.



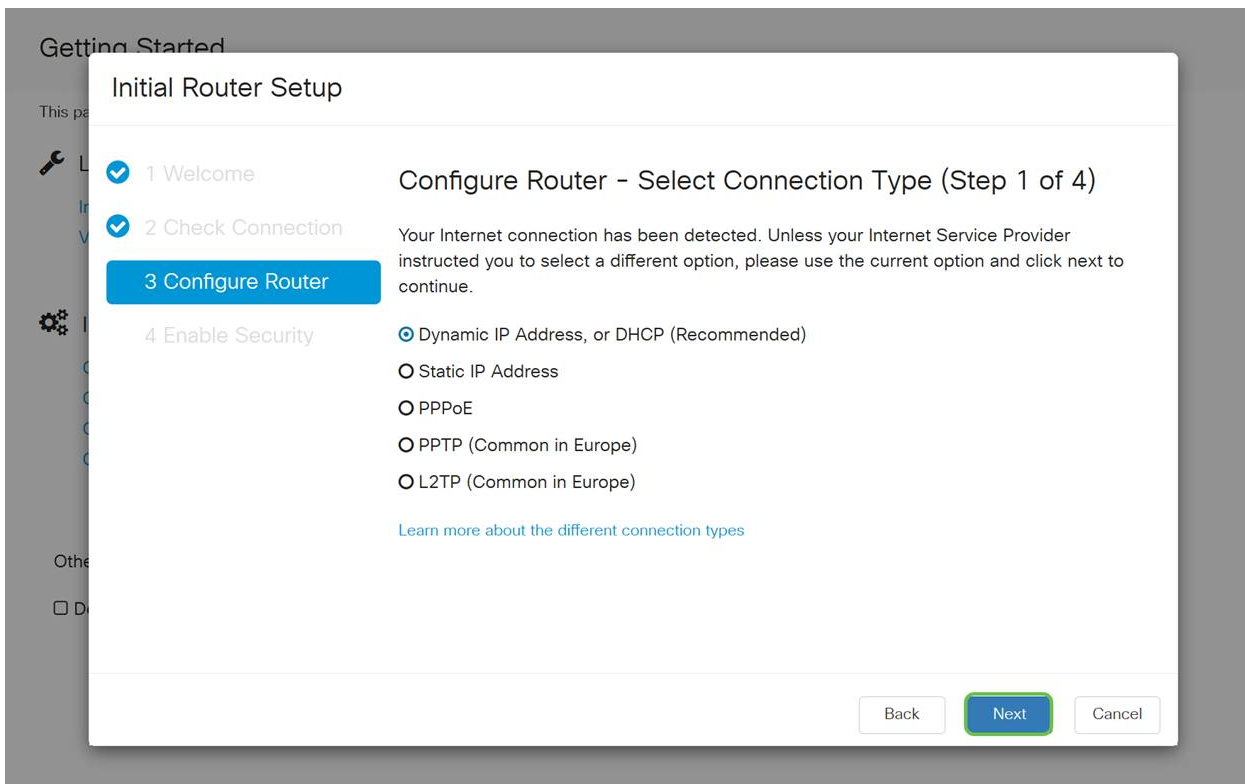
### Step 3

This step covers basic steps to make sure your router is connected. Since you have already confirmed this, click **Next**.



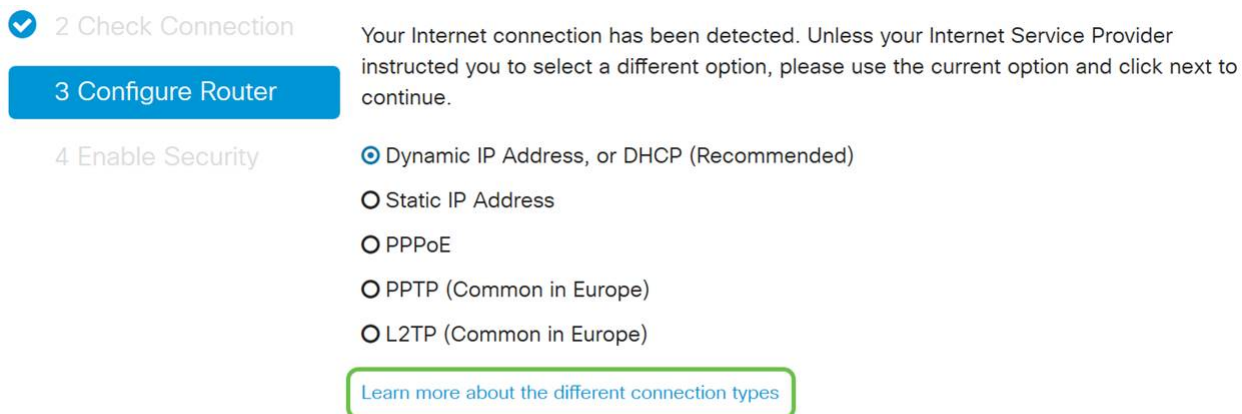
### Step 4

The next screen displays your options for assigning IP addresses to your router. You need to select DHCP in this scenario. Click **Next**.



Although you must use DHCP for this initial setup, you can select to *Learn more about the different connection types* toward the bottom of your screen the future reference. For more details on this, check out the following articles:

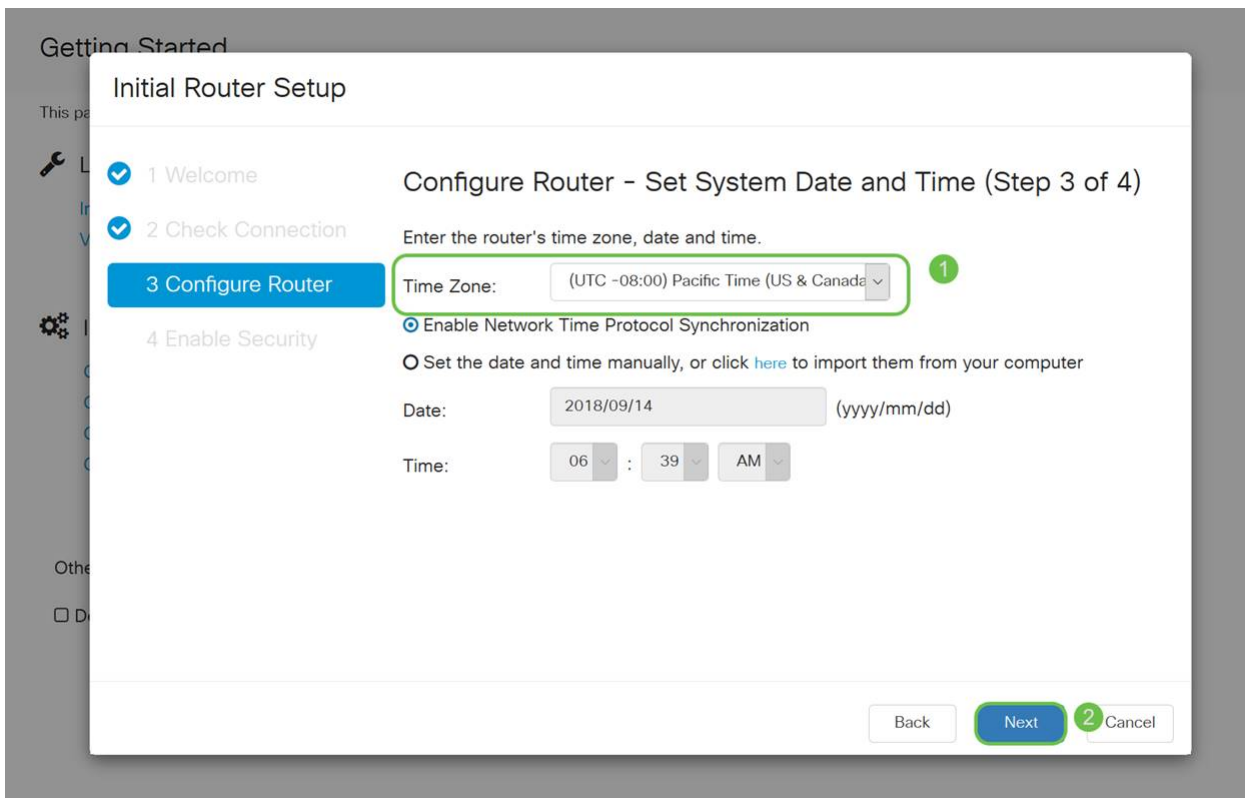
- [WAN Configuration on RV160x and RV260x Devices](#)
- [Configuring Static Routing on the RV160 and RV260](#)



## Step 5

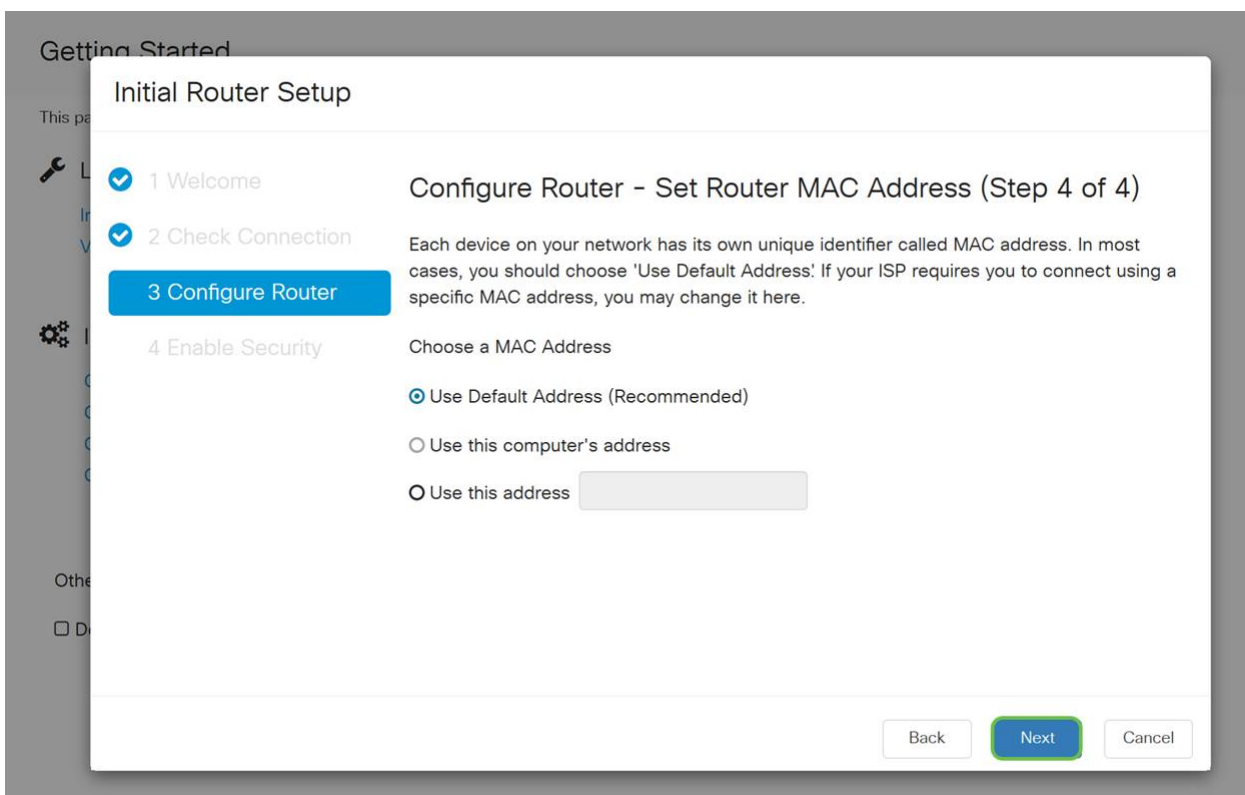
Here, you will be prompted to set your router time settings. This is important because it enables precision when reviewing logs or troubleshooting events. Select your **Time Zone** and then click **Next**.





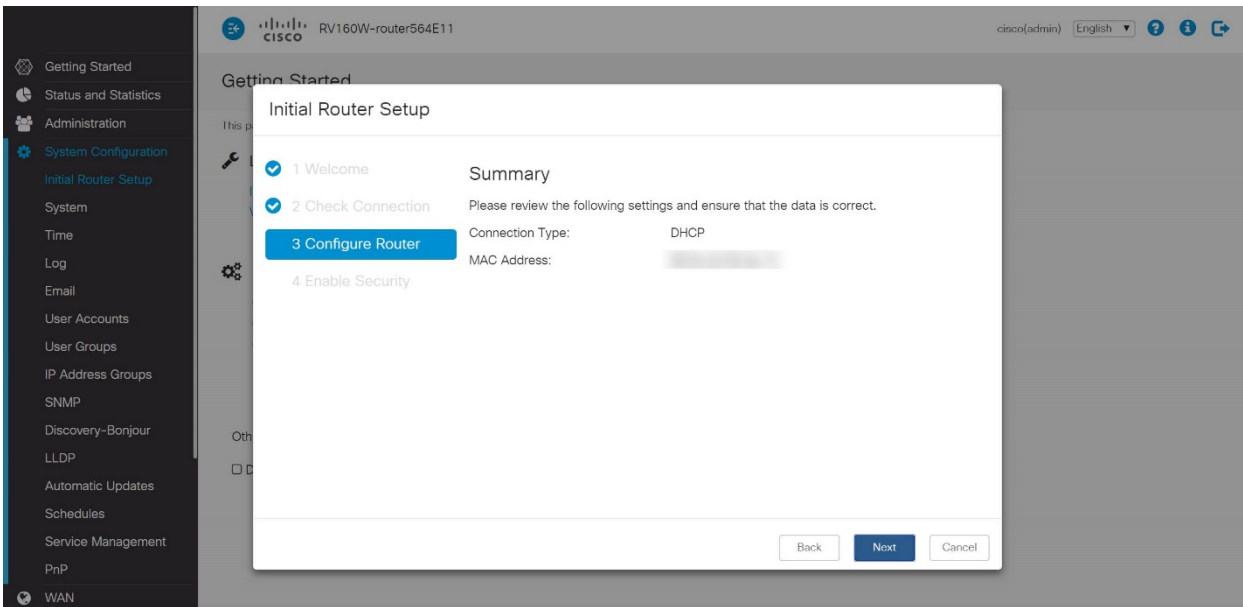
## Step 6

On this screen, you will select what MAC addresses to assign to devices. Most often, you will use the default address. Click **Next**.



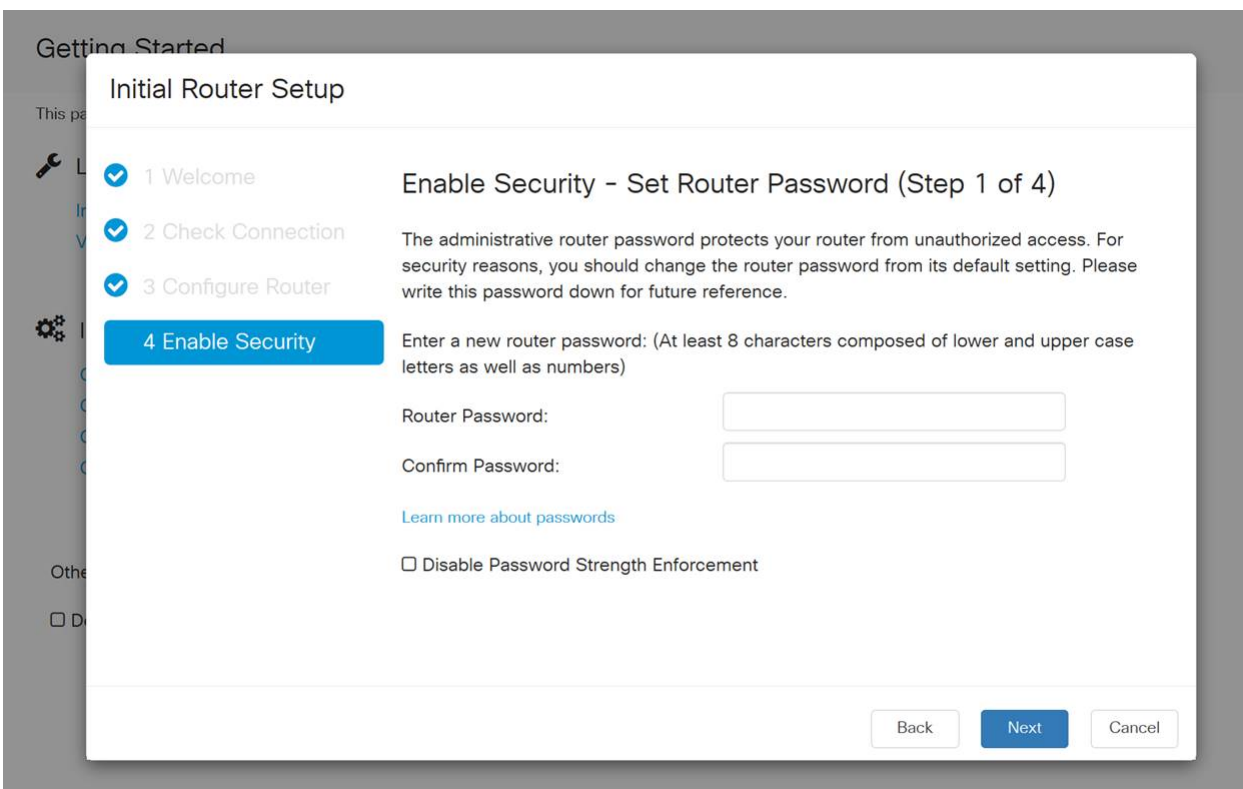
## Step 7

The following page is a summary of the selected options. Review and click **Next** if satisfied.



## Step 8

For the next step, you will select a password to use when logging into the router. The standard for passwords is to contain at least 8 characters (both upper and lower case) and includes numbers. **Enter a password** that conforms with the strength requirements. Click **Next**. Take note of your password for future logins.



It is *not* recommended that you select *Disable Password Strength Enforcement*. This option would let you select a password as simple as 123, which would be as easy as 1-2-3 for malicious actors to crack.

## Step 9

Click the **save icon**.

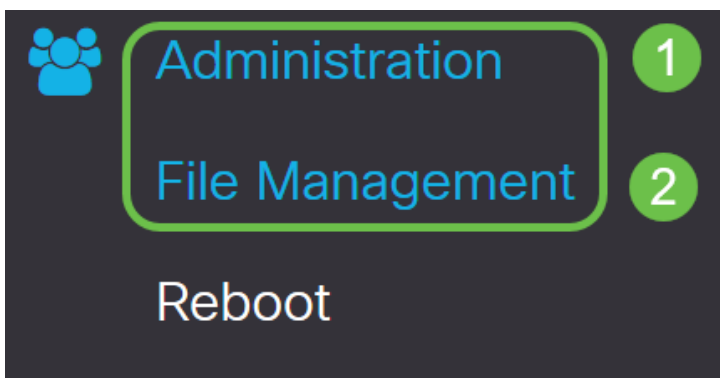


## Upgrade Firmware if Needed

This is an important section, don't skip it!

### Step 1

Choose **Administration > File Management**.



In the *System Information* area, the following sub-areas describe the following:

- Device Model - Displays the model of your device.
- PID VID - Product ID and Vendor ID of the router.
- Current Firmware Version - Firmware that is currently running on the device.
- Latest Version Available on Cisco.com - Latest version of the software available on the Cisco website.
- Firmware last updated - Date and time of the last firmware update made on the router.

# 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

## Step 2

Under the *Manual Upgrade* section, click on the **Firmware Image** radio button for *File Type*.

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.

## Step 3

On the *Manual Upgrade* page, click on a radio button to select *cisco.com*. There are a few other options for this, but this is the easiest way to do an upgrade. This process installs the latest upgrade file directly from the Cisco Software Downloads webpage.

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.

## Step 4

Click on **Upgrade**.

Manual Upgrade

File Type:  Firmware Image  Language File  USB Dongle Driver

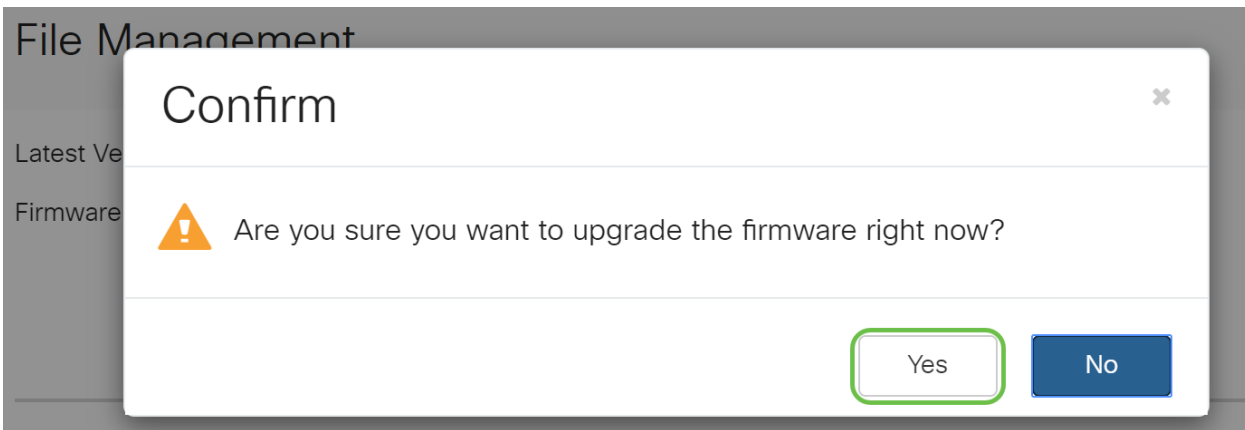
Upgrade From:  cisco.com  PC  USB 

Reset all configurations/settings to factory defaults

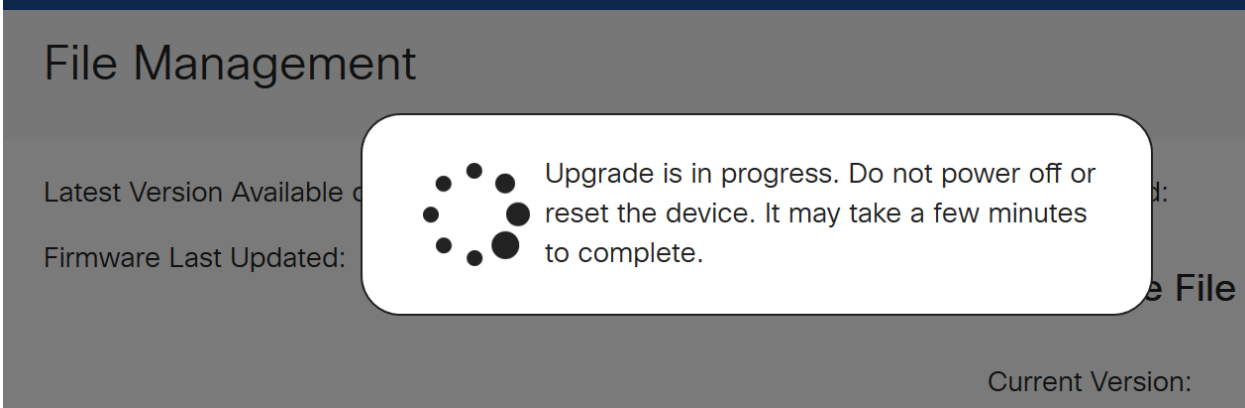
The device will be automatically rebooted after the upgrade is complete.

## Step 5

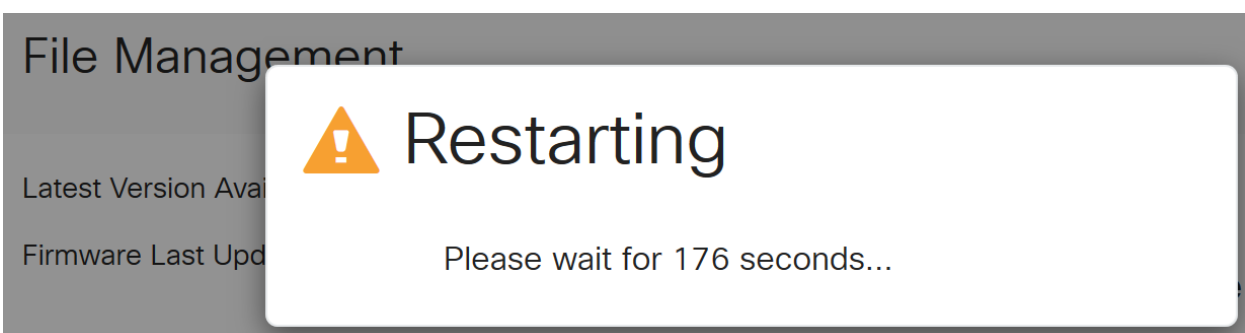
Click **Yes** in the confirmation window to continue.



The update process needs to run without interruption. You will get the following message on the screen while the upgrade is in progress.



Once the upgrade has been completed, a notification window will pop-up to inform you that the router will be *Restarting* with a countdown of the estimated time for the process to finish. Following this, you will be logged out.



## Step 6

Log back into the web-based utility to verify that the router firmware has been upgraded, scroll to the *System Information*. The *Current Firmware Version* area should now display the upgraded firmware version.

# 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

Congratulations, your basic settings on your router are complete! You have some configuration options moving forward.

I encourage you to keep scrolling through the article to learn more about these options and if they apply to you. If you prefer, you can click any of the hyperlinks to jump to a section instead.

- [Configure VLANs \(Optional\)](#)
- [Edit IP Address \(Optional\)](#)
- [Add static IP addresses \(Optional\)](#)
- [I'm ready to configure the Mesh Wireless portion of my network!](#)

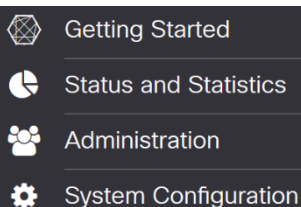
## Configure VLANs (Optional)

A Virtual Local Area Network (VLAN) allows you to logically segment a Local Area Network (LAN) into different broadcast domains. In scenarios where sensitive data may be broadcast on a network, VLANs can be created to enhance security by designating a broadcast to a specific VLAN. VLANs can also be used to enhance performance by reducing the need to send broadcasts and multicasts to unnecessary destinations. You can create a VLAN, but this has no effect until the VLAN is attached to at least one port, either manually or dynamically. Ports must always belong to one or more VLANs.

If you do not want to create VLANs, you can skip to the [next section](#).

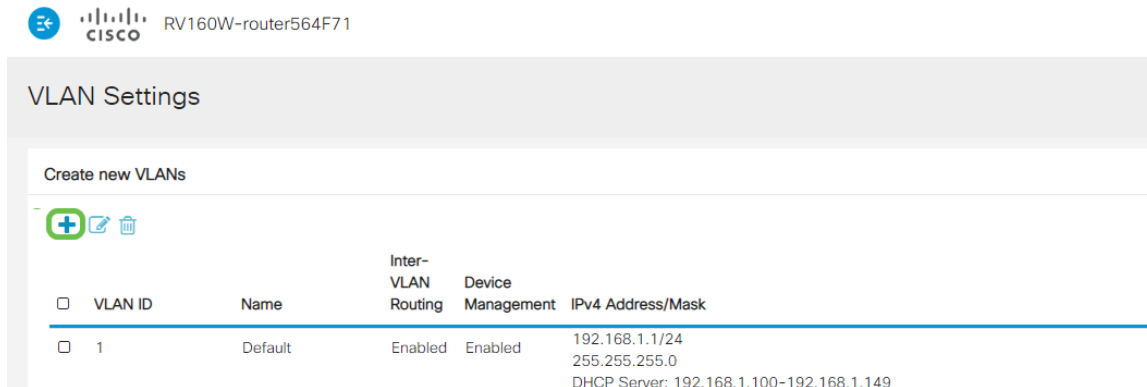
### Step 1

Navigate to **LAN > VLAN Settings**.



## Step 2

Click **Add** to create a new VLAN.



RV160W-router564F71

### VLAN Settings

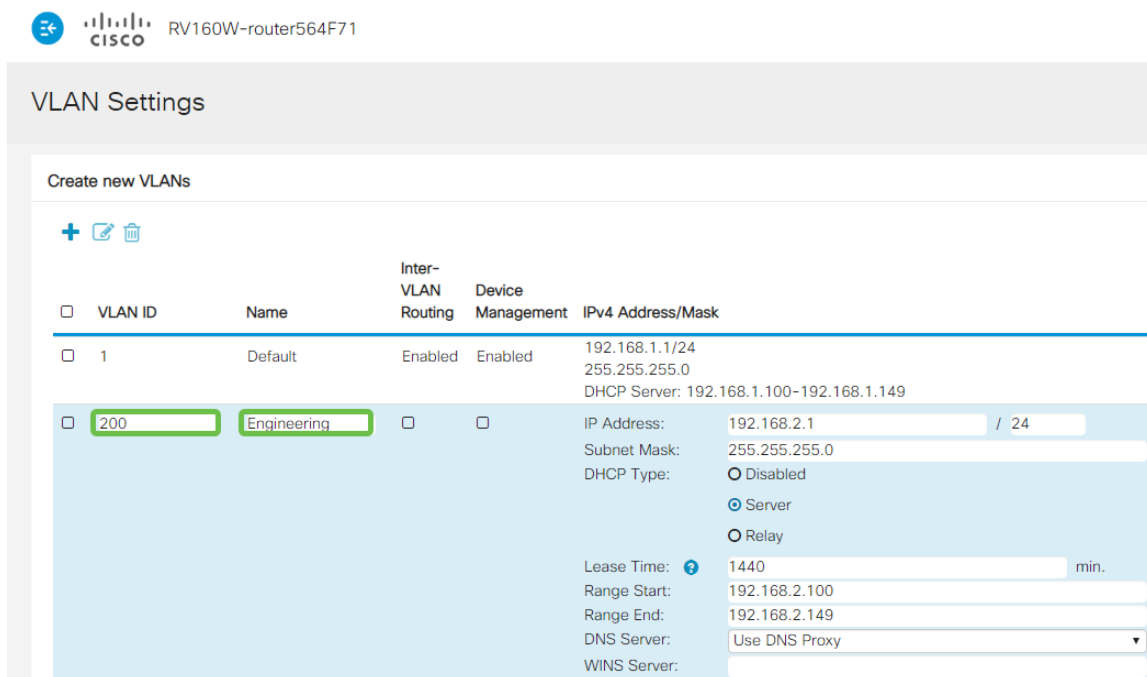
Create new VLANs

<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

## Step 3

Enter the *VLAN ID* that you want to create and a *Name* for it. The *VLAN ID* range is from 1-4093.

We entered **200** as our *VLAN ID* and **Engineering** as the *Name* for the 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
<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"/> Relay Lease Time: 1440 min. Range Start: 192.168.2.100 Range End: 192.168.2.149 DNS Server: Use DNS Proxy WINS Server:

## Step 4

Uncheck the *Enabled* box for both *Inter-VLAN Routing* and *Device Management* if desired.

Inter-VLAN routing is used to route packets from one VLAN to another VLAN. In general, this is not recommended for guest networks as you will want to isolate guest users it leaves VLANs less secure. There are times when it may be necessary for VLANs to route between each other. If this is the case, check out [Inter-VLAN Routing on an RV34x Router with Targeted ACL Restrictions](#) to configure specific traffic that you allow between VLANs.

Device Management is the software that allows you to use your browser to log into the Web UI of the RV260P, from the VLAN, and manage the RV260P. This should also be disabled on Guest networks.

In this example, we did not enable either the *Inter-VLAN Routing* or *Device Management* to keep the VLAN more secure.

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:

## Step 5

The private IPv4 address will auto-populate in the *IP Address* field. You can adjust this if you choose. In this example, the subnet has 192.168.2.100-192.168.2.149 IP addresses available for DHCP. 192.168.2.1-192.168.2.99, and 192.168.2.150-192.168.2.254 are available for static IP addresses.

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:

## Step 6



The subnet mask under *Subnet Mask* will auto-populate. If you make changes, this will automatically adjust the field.

For this demonstration, we will be leaving the *Subnet Mask* as **255.255.255.0** or **/24**.

The screenshot shows the 'VLAN Settings' page for a Cisco RV160W router. It features a table of existing VLANs and a configuration form for a new VLAN. The table has columns for 'VLAN ID', 'Name', 'Inter-VLAN Routing', 'Device Management', and 'IPv4 Address/Mask'. The configuration form for a new VLAN (ID 200, Name Engineering) includes fields for 'IP Address' (192.168.2.1), 'Subnet Mask' (255.255.255.0), 'DHCP Type' (Server), 'Lease Time' (1440 min), 'Range Start' (192.168.2.100), 'Range End' (192.168.2.149), 'DNS Server' (Use DNS Proxy), and 'WINS Server'. The Subnet Mask and the /24 suffix are highlighted with green boxes.

## Step 7

Select a *Dynamic Host Configuration Protocol (DHCP) Type*. The following options are:

*Disabled* – Disables the DHCP IPv4 server on VLAN. This is recommended in a test environment. In this scenario, all IP addresses would need to be manually configured and all communication would be internal.

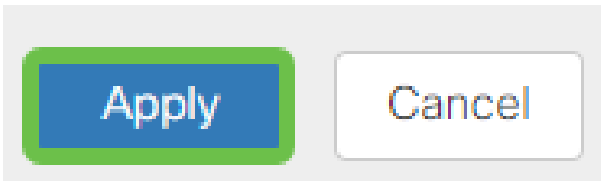
*Server* - This is the most often used option.

- Lease Time – Enter a time value of 5 to 43,200 minutes. The default is 1440 minutes (equal to 24 hours).
- Range Start and Range End – Enter the range start and end of IP addresses that can be assigned dynamically.
- DNS Server – Select to use the DNS server as a proxy, or from ISP from the drop-down list.
- WINS Server – Enter the WINS server name.
- DHCP Options:
  - Option 66 – Enter the IP address of the TFTP server.
  - Option 150 – Enter the IP address of a list of TFTP servers.
  - Option 67 – Enter the configuration filename.
- Relay – Enter the remote DHCP server IPv4 address to configure the DHCP relay agent. This is a more advanced configuration.

The screenshot shows the top portion of the 'VLAN Settings' page for a Cisco RV160W router. It includes the 'Create new VLANs' section with a plus icon, a minus icon, and a trash icon. The table of VLANs is partially visible, showing the 'VLAN ID' and 'Name' columns.

## Step 8

Click **Apply** to create the new VLAN.



## Assign VLANs to Ports

16 VLANs can be configured on the RV260, with one VLAN for the Wide Area Network (WAN). VLANs that are not on a port should be *Excluded*. This keeps the traffic on that port exclusively for the VLAN/VLANs the user specifically assigned. It is considered a best practice.

Ports can be set to be an Access Port or a Trunk Port:

- Access Port - Assigned one VLAN. Untagged frames are passed.
- Trunk Port - Can carry more than one VLAN. 802.1q. Trunking allows for a native VLAN to be Untagged. VLANs that you don't want on the Trunk should be Excluded.

One VLAN assigned its own port:

- Considered an Access port.
- The VLAN that is assigned this port should be labeled Untagged.
- All other VLANs should be labeled Excluded for that port.

Two or more VLANs that share one port:

- Considered a Trunk Port.
- One of the VLANs can be labeled Untagged.
- The rest of the VLANs that are part of the Trunk Port should be labeled Tagged.
- The VLANs that are not part of the Trunk Port should be labeled Excluded for that port.

**Note:** In this example, there are no trunks.

## Step 9

Select the *VLAN IDs* to edit. Click **Edit**.

In this example, we have selected *VLAN 1* and *VLAN 200*.

## Assign VLANs to ports

<input type="checkbox"/>	VLAN ID	LAN1	LAN2
<input checked="" type="checkbox"/>	1	Untagged	Excluded
<input checked="" type="checkbox"/>	200	Excluded	Untagged

### Step 10

Click **Edit** to assign a VLAN to a LAN port and specify each setting as *Tagged*, *Untagged*, or *Excluded*.

In this example, on LAN1 we assigned VLAN 1 as **Untagged** and VLAN 200 as **Excluded**. For LAN2 we assigned VLAN 1 as **Excluded** and VLAN 200 as **Untagged**.

## Assign VLANs to ports

<input type="checkbox"/>	VLAN ID	LAN1	LAN2
<input checked="" type="checkbox"/>	1	Untagged	Excluded
<input checked="" type="checkbox"/>	200	Excluded	Untagged

### Step 11

Click **Apply** to save the configuration.

**Apply**

You should now have successfully created a new VLAN and configured VLANs to ports on the RV260. Repeat the process to create the other VLANs. For example, VLAN300 would be created for Marketing with a subnet of 192.168.3.x and VLAN400 would be created for Accounting with a subnet of 192.168.4.x.

That's the basics of VLANs. Click on the hyperlink to learn more about [VLAN Best Practices and Security Tips for Cisco Business Routers](#).

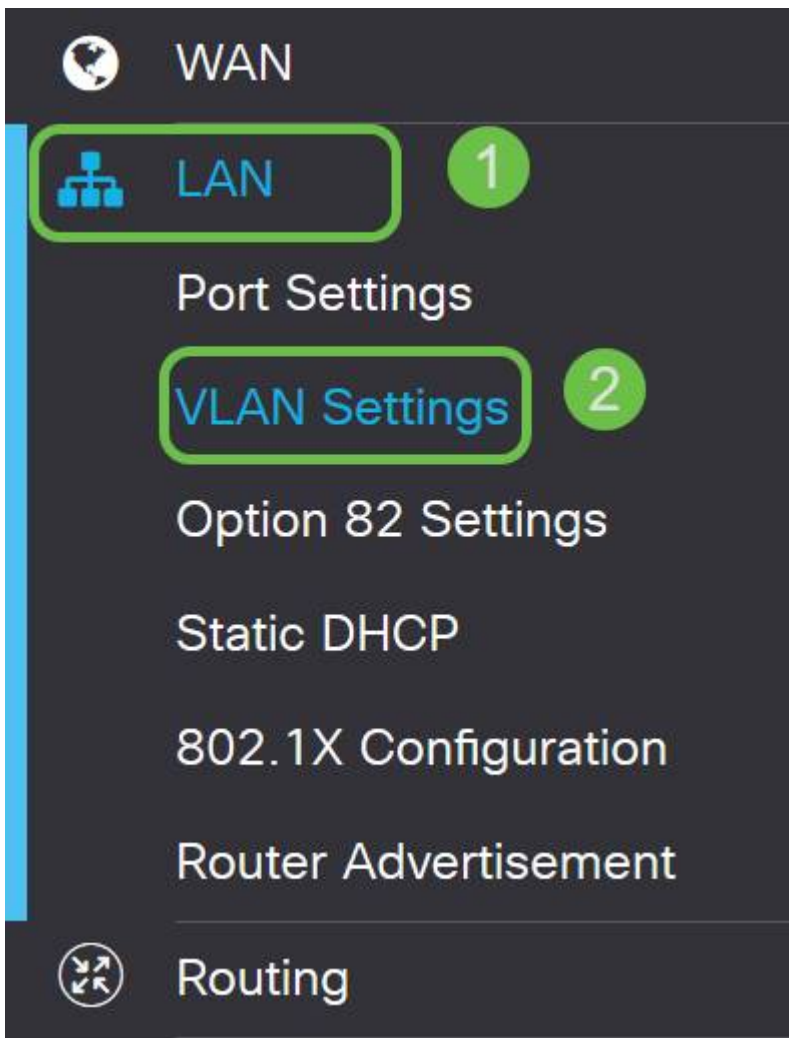
## Edit an IP address (Optional)

After completing the *Initial Setup Wizard*, you can set a static IP address on the router by editing the VLAN settings. Skip re-running the initial setup wizard, to perform this change follow the steps below.

If you don't need to edit an IP address, you can move to the [next section](#) of this article.

### Step 1

In the left-hand menu-bar click **LAN > VLAN Settings**.



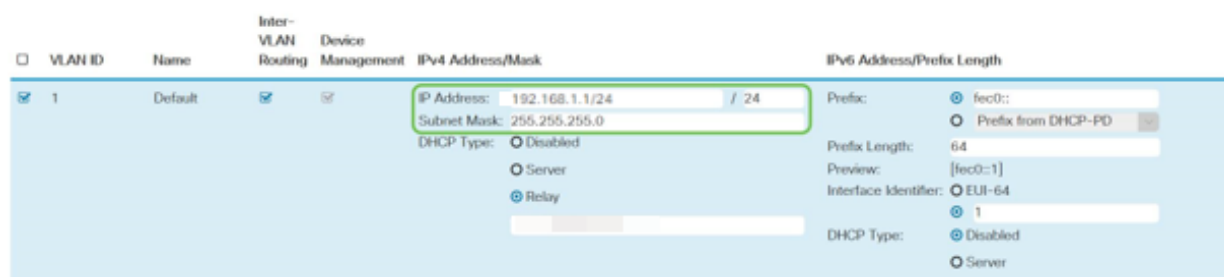
## Step 2

Then select the **VLAN** that contains your routing device, then click the **edit icon**.



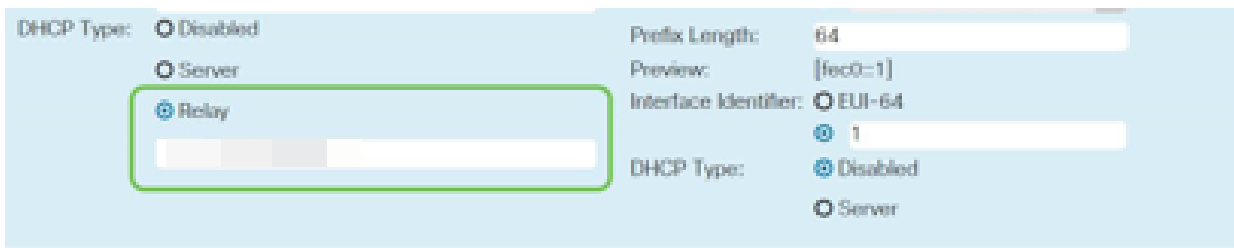
## Step 3

Enter your desired **static IP address** and click **Apply** in the upper-right hand corner.



## Step 4 (Optional)

If your router is not the DHCP server/device assigning IP addresses, you can use the DHCP Relay feature to direct DHCP requests to a specific IP address. The IP address is likely to be the router connected to the WAN/Internet.



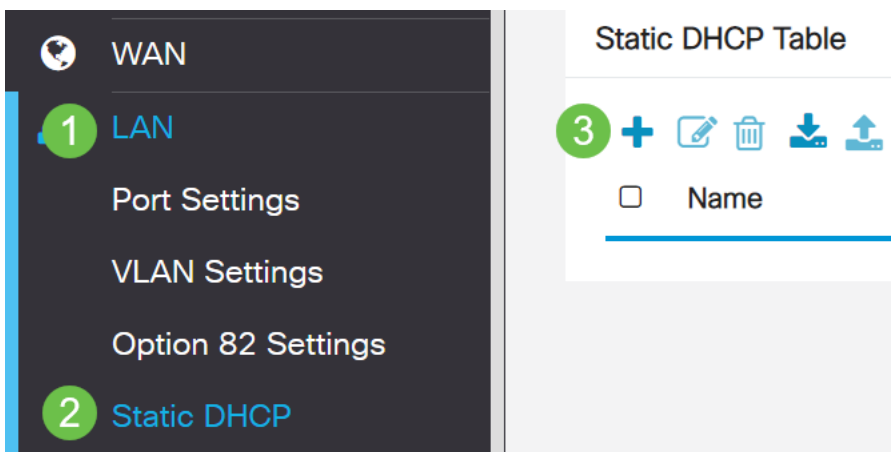
## Add a Static IP

If you would like a certain device to be reachable to other VLANs, you can give that device a static local IP address and create an access rule to make it accessible. This only works if Inter-VLAN routing is enabled. There are other situations where a static IP may be useful. For more information on setting static IP addresses, check out [Best Practices for Setting Static IP Addresses on Cisco Business Hardware](#).

If you don't need to add a static IP address, you can move to the [next section](#) of this article to configure the Access Points.

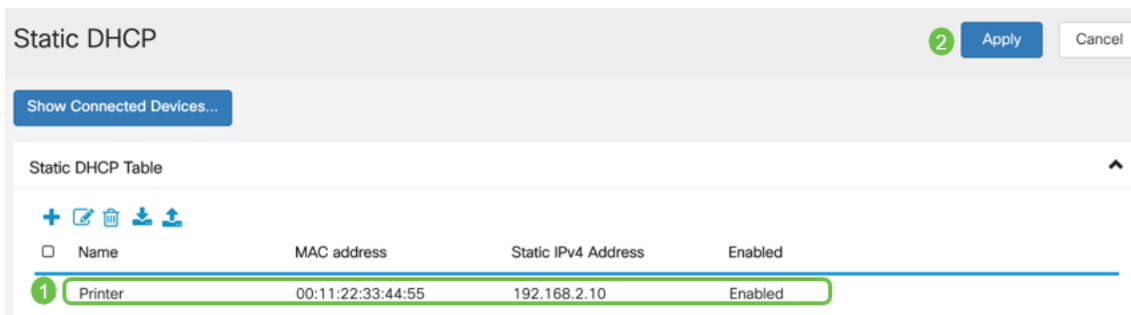
### Step 1

Navigate to **LAN > Static DHCP**. Click on the **plus icon**.



### Step 2

Add the **Static DHCP** information for the device. In this example, the device is a printer.



Congratulations, you have completed the configuration of your RV260P router. We will now configure your Cisco Business Wireless devices.

## Configure the CBW140AC

### CBW140AC Out of the Box

Start by plugging an Ethernet cable from the PoE port on your CBW140AC to a PoE port on the RV260P. The first 4 ports on the RV260P can supply PoE, so any of them can be used.

Check the status of the indicator lights. The access point will take about 10 minutes to boot. The LED will blink green in multiple patterns, alternating rapidly through green, red, and amber before turning green again. There may be small variations in the LED color intensity and hue from unit to unit. When the LED light is blinking green, proceed to the next step.

The PoE Ethernet uplink port on the Primary AP can ONLY be used to provide an uplink to the LAN, and NOT to connect to any other Primary capable or mesh extender devices.

If your access point isn't new, out of the box, make sure it is reset to factory default settings for the *CiscoBusiness-Setup* SSID to show up in your Wi-Fi options. For assistance with this, check out [How to Reboot and Reset to Factory Default Settings on RV260 Routers](#).

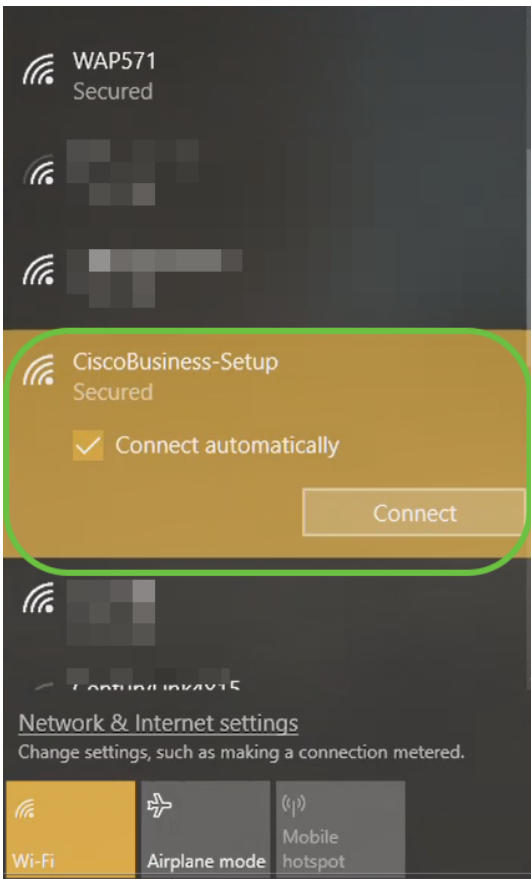
### Set Up the 140AC Primary Wireless Access Point on the Web UI

You can set up the Access Point using the mobile application or the Web UI. This article uses the Web UI for setup, which gives more options for configuration but is a little more complicated. If you would like to use the mobile application for the next sections, click to access the [mobile application instructions](#).

If you have trouble connecting, refer to the [Wireless Troubleshooting Tips](#) section of this article.

#### Step 1

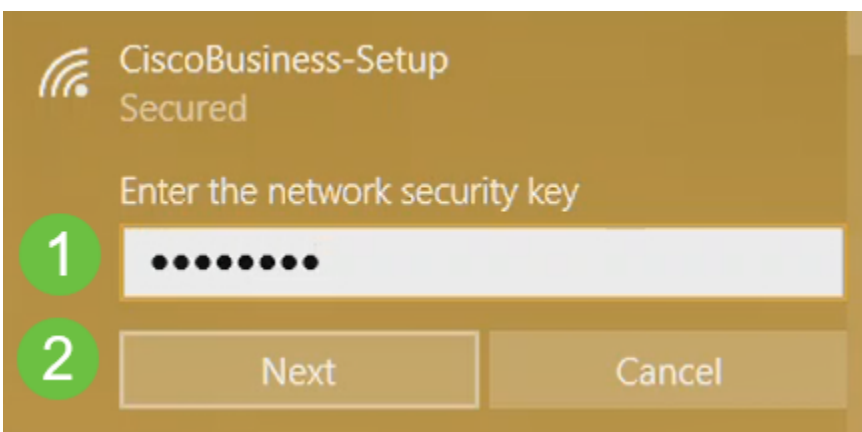
On your PC, click the **Wi-Fi icon** and choose *CiscoBusiness-Setup* wireless network. Click Connect.



If your access point isn't new, out of the box, make sure it is reset to factory default settings for the *CiscoBusiness-Setup* SSID to show up in your Wi-Fi options.

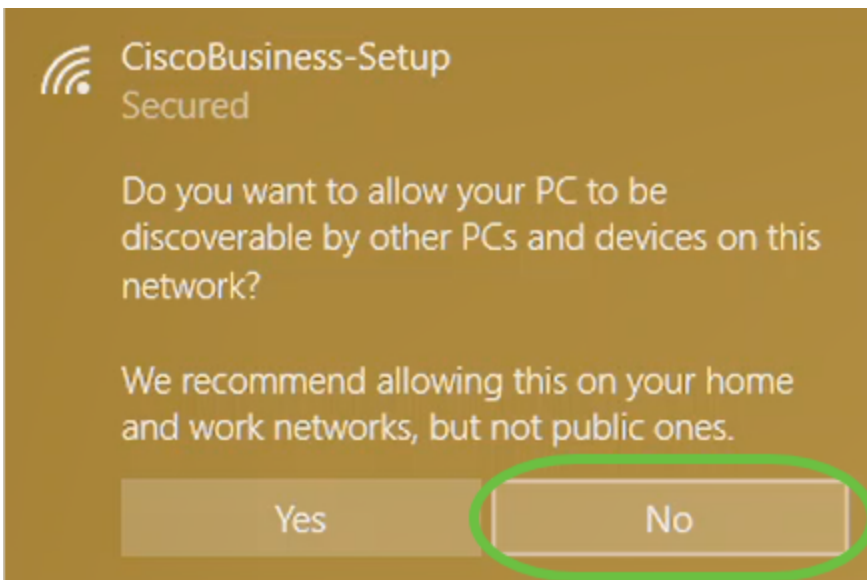
## Step 2

Enter the passphrase **cisco123** and click **Next**.



## Step 3

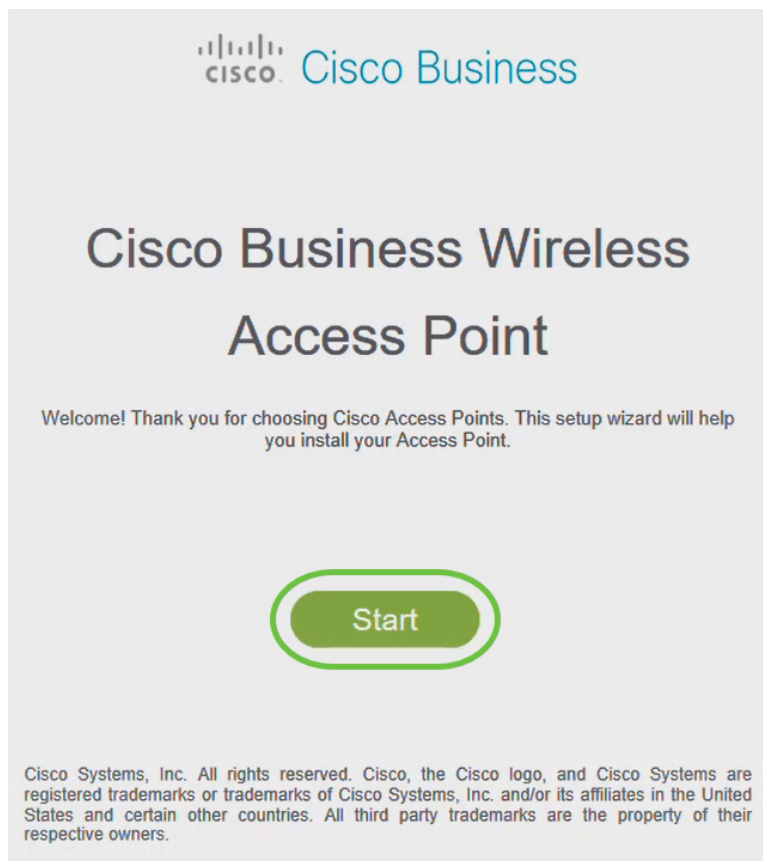
You will get the following screen. Since you can configure only one device at a time, click **No**.



Only one device can be connected to the *CiscoBusiness-Setup* SSID. If a second device attempts to connect, it will not be able to. If you are unable to connect to the SSID and have validated the password, some other device may have made the connection. Restart the AP and try again.

#### Step 4

Once connected, the web browser should auto-redirect to the CBW AP setup wizard. If not, open a web browser, such as Internet Explorer, Firefox, Chrome, or Safari. In the address bar, type **http://ciscobusiness.cisco** and press **Enter**. Click **Start** on the webpage.





If you do not see the webpage, wait for a few more minutes or reload the page. After this initial setup, you will use `https://ciscobusiness.cisco` to log in. If your web browser auto-populates with `http://`, you need to manually type in the `https://` to gain access.

## Step 5

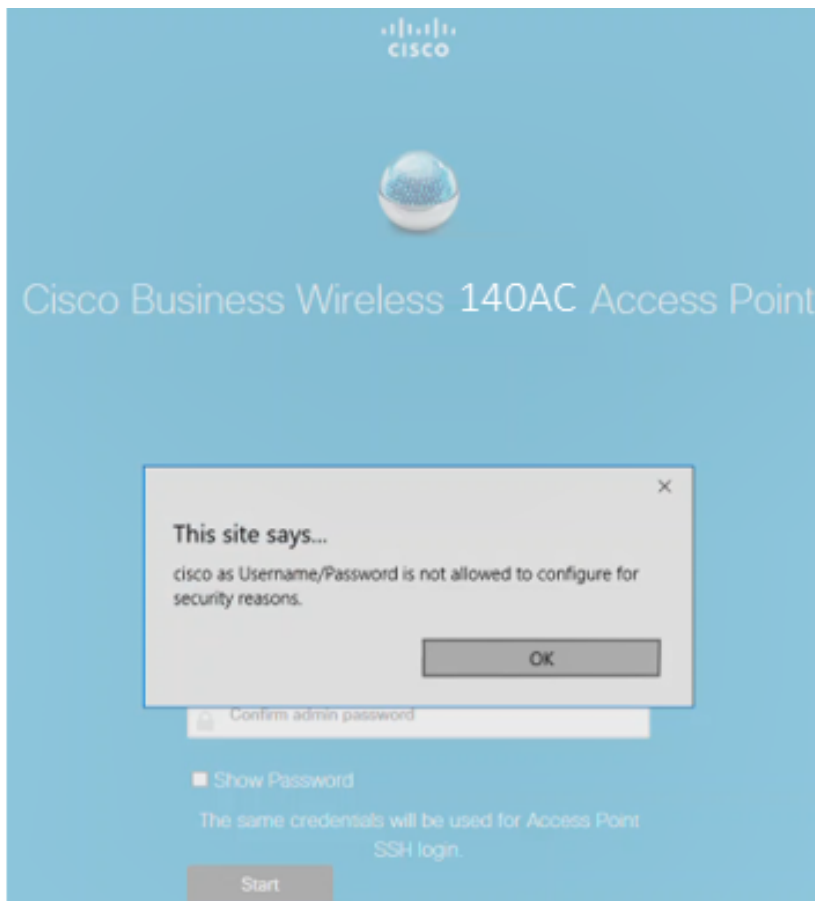
Create an *admin account* by entering the following:

- Admin username (Maximum of 24 characters)
- Admin password
- Confirm admin password

You can choose to show the password by checking the checkbox next to *Show Password*. Click **Start**.

The screenshot shows the Cisco Business Wireless 140AC Access Point setup interface. It features a blue background with the Cisco logo at the top. The main heading is "Cisco Business Wireless 140AC Access Point". Below this, a message reads "Welcome! Please start by creating an admin account." There are three input fields: the first contains the username "admin", the second and third are masked with "P". To the right of each field is a green circle with a number (1, 2, 3). Below the fields is a checkbox labeled "Show Password" with a green circle containing the number 4. Below that is a "Start" button with a green circle containing the number 5. A note at the bottom says "Credentials will be used to manage the Access Point".

Do not use *cisco*, or variations of it in the username or password fields. If you do, you will get an error message as shown below.



## Step 6

*Set Up Your Primary AP* by entering the following:

- Primary AP Name
- Country
- Date & Time
- Timezone
- Mesh

## 1 Set Up Your Primary AP

Primary AP Name  ? **1**

Country  ? **2**

Date & Time   **3**

Timezone  ? **4**

Mesh  ? **5**

*Mesh* should be enabled only if you plan to create a mesh network. By default, it is disabled.

### Step 7

(Optional) You can enable *Static IP* for your CBW140AC for management purposes. If not, the interface gets an IP address from your DHCP server. To configure static IP, enter the following:

- Management IP Address
- Subnet Mask
- Default Gateway

Click **Next**.

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

Management IP Address  ?

Subnet Mask  **2**

Default Gateway

**3**

By default, this option is disabled.

## Step 8

Create Your Wireless Networks by entering the following:

- Network Name
- Choose Security
- Passphrase
- Confirm Passphrase
- (Optional) Check the checkbox to Show Passphrase.

Click **Next**.

2 Create Your Wireless Network

Network Name: CBWWlan

Security: WPA2

Passphrase: .....

Confirm Passphrase: .....

Show Passphrase

Back Next

Wi-Fi protected Access (WPA) version 2 (WPA2), is the current standard for Wi-Fi security.

## Step 9

Confirm the settings and click **Apply**.



Please confirm the configurations and Apply

## 1 Primary AP Settings

Username **Admin**  
PrimaryAP 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

### Step 10

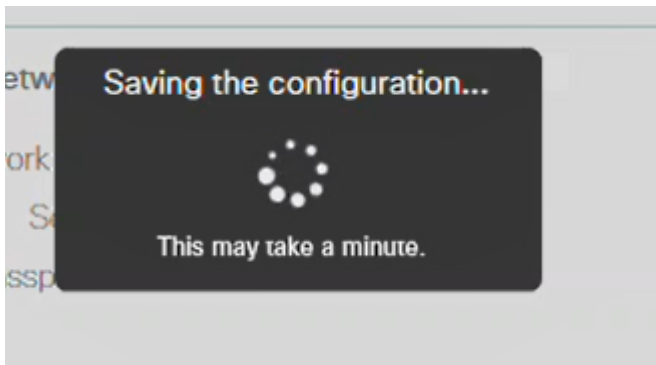
Click **OK** to apply the settings.

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

You will see the following screen while the configurations are being saved and the system reboots. This might take 10 minutes.

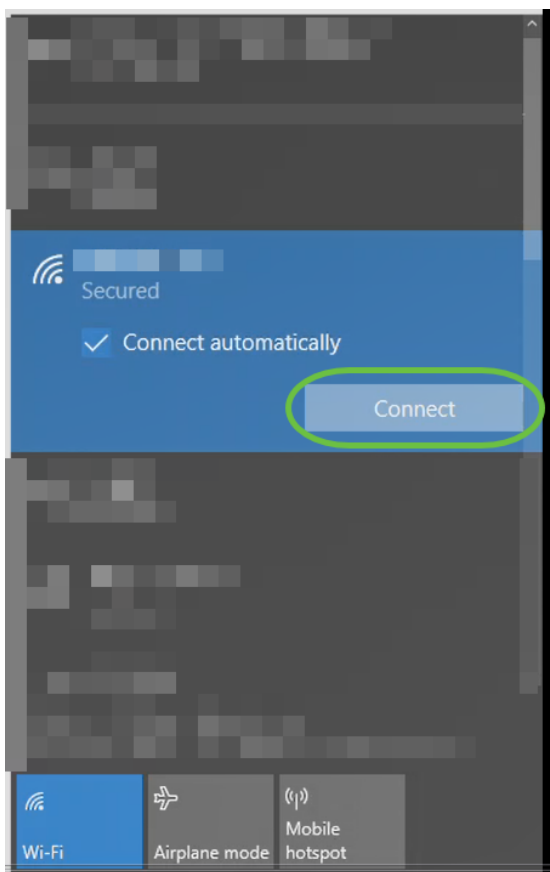


During the reboot, the LED in the access point will go through multiple color patterns. When the LED is blinking green, proceed to the next step. If the LED does not get past the red flashing pattern, it indicates that there is no DHCP server in your network. Ensure that the AP is connected to a switch or a router with a DHCP server.

### Step 11

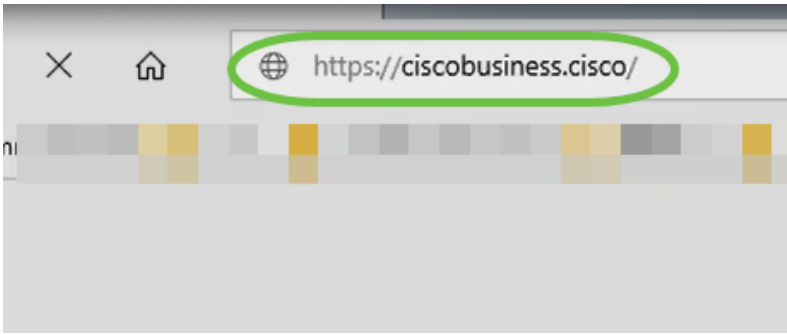
Go to the wireless options on your PC and choose the network that you configured. Click **Connect**.

The *CiscoBusiness-Setup* SSID will disappear after reboot.



### Step 12

Open a web browser and type in *https://[IP address of the CBW AP]*. Alternatively, you can type *https://ciscobusiness.cisco* in the address bar and press enter.



Make sure that you type *https* and not *http* at this step.

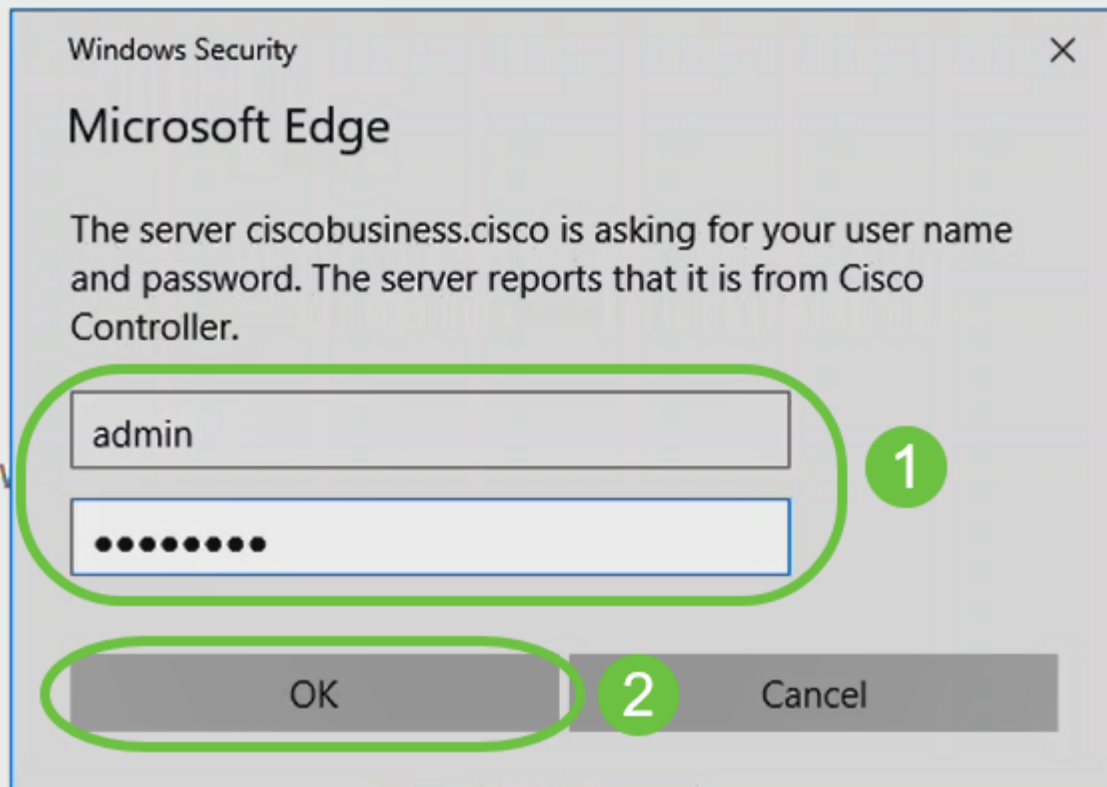
### Step 13

Click **Login**.



### Step 14

Log in using the credentials that were configured. 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.

## Step 15

You will be able to access the Web UI page of the AP.





# Wireless Troubleshooting Tips

If you have any issues, check out the following tips:

- Make sure the correct Service Set Identifier (SSID) is selected. This is the name that you created for the wireless network.
- Disconnect any VPN for either the mobile app or on a laptop. You might even be connected to a VPN that your mobile service provider uses that you might not even know. For example, an Android (Pixel 3) phone with Google Fi as a service provider there is a built-in VPN that auto-connects without notification. This would need to be disabled to find the Primary AP.
- Log into the Primary AP with `https://<IP address of the Primary AP>`.
- Once you do the initial setup, be sure `https://` is being used whether you are logging into `ciscobusiness.cisco` or by entering the IP address into your web browser. Depending on your settings, your computer may have auto-populated with `http://` since that is what you used the very first time you logged in.
- To help with problems related to accessing the Web UI or browser issues during the use of the AP, in the web browser (Firefox in this case) click on the Open menu, go to Help > Troubleshooting Information and click on Refresh Firefox.

## Configure the CBW142ACM Mesh Extenders Using the Web UI

You are in the home stretch of setting up this network, you just need to add your mesh extenders!

### Step 1

Plug the two Mesh Extenders into the wall in the locations you have selected. Write down the MAC Address of each mesh extender.

### Step 2

Wait about 10 minutes for the Mesh Extenders to boot up.

### Step 3

Enter the Primary Access Points (APs) IP address on the web browser. Click **Login** to access the Primary AP.

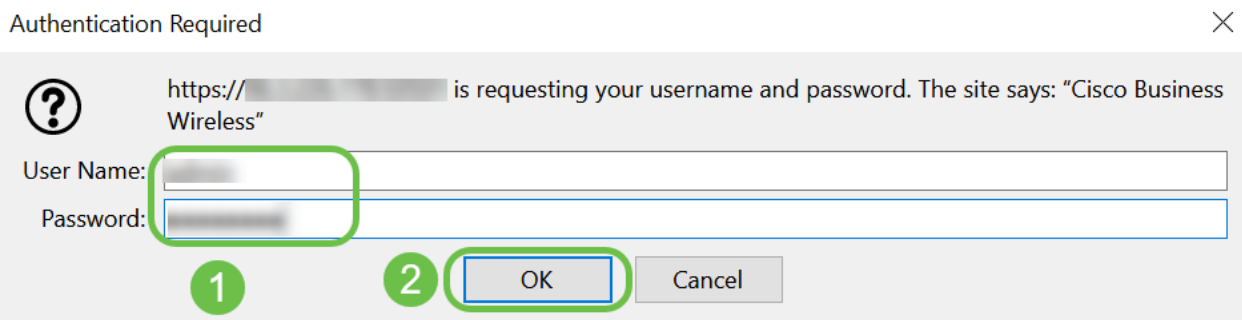
# Cisco Business Wireless Access Point

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



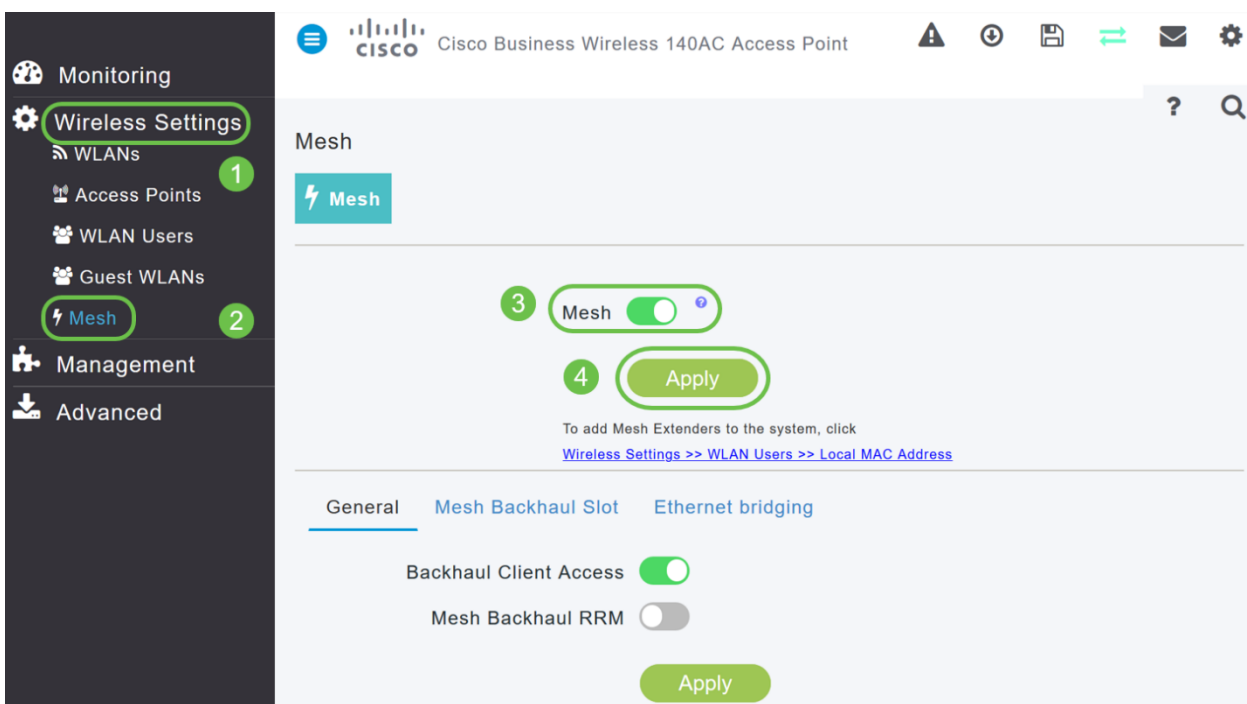
## Step 4

Enter your *User Name* and *Password* credentials to access the Primary AP. Click **OK**.



## Step 5

Navigate to **Wireless Settings > Mesh** . Make sure the *Mesh* is Enabled. Click **Apply**.



## Step 6

If Mesh was not already enabled, the WAP may need to perform a reboot. A pop-up will appear to do a reboot. Confirm. This will take about 10 minutes. During a reboot, the LED will blink green in multiple patterns, alternating rapidly through green, red, and amber before turning green again. There may be small variations in the LED color intensity and hue from unit to unit.

## Step 7

Navigate to **Wireless Settings > WLAN Users > Local MAC Addresses**. Click **Add MAC Address**.

The screenshot shows the Cisco Business Wireless 140AC Access Point configuration interface. The left sidebar is dark grey with a navigation menu. The main content area is light grey and displays the 'WLAN Users' configuration page. The 'Local MAC Addresses' tab is selected. A table lists existing MAC addresses with columns for Action, MAC Address, Type, Profile Name, and Description. The 'Add MAC Address' button is highlighted with a green circle.

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

## Step 8

Enter the MAC address and Description of the Mesh Extender. Select the *Type* as Allow list. Select the *Profile Name* from the drop-down menu. Click **Apply**.

The 'Add MAC Address' dialog box is shown with 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

## Step 9

Be sure to save all your configurations by pressing the **save icon** on the top-right pane of the screen.



Repeat for each mesh extender.

## Check and Update Software Using the Web UI

Don't skip this important step! There are a few ways to update software, but the steps listed below are recommended as the easiest to execute when you use the Web UI.

To view and update the current software version of your Primary AP, perform the following steps.

### Step 1

Click the **gear icon** at the top-right corner of the web interface, and then click **Primary AP Information**.

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

### Step 2

Compare the version that is running to the latest software version. Close the window once you know if you need to update the software.

## 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

If you are running the latest version of software, you can jump to the [Create WLANs](#) section.

### Step 3

Choose **Management > Software Update** from the menu.

The *Software Update* window is displayed with the current software version number listed at the top.

The screenshot shows the 'Software Update' configuration page. On the left is a dark sidebar menu with the following items: 'Management' (1), 'Access', 'Admin Accounts', 'Time', 'Software Update' (2), and 'Advanced'. The main content area is titled 'Software Update' and features a teal 'Version' button with a downward arrow and a green circle containing the number '3'. To the right of this button is a text input field containing '10.0.251.24'. Below this, there is a 'Transfer Mode' dropdown menu set to 'TFTP' and an 'IP Address(IPv4)/Name \*' text input field containing '172.16.1.35'.

You can update the CBW AP software and the Current configurations on the Primary AP will not be deleted.

From the *Transfer Mode* drop-down list, choose **Cisco.com**.

Transfer Mode	Cisco.com
Automatically Check For Updates	HTTP
	TFTP
Last Software Check	SFTP
Latest Software Release	Cisco.com


**Step 4**






To set the Primary AP to automatically check for software updates, choose **Enabled** in the *Automatically Check for Updates* drop-down list. This is enabled by default.

Transfer Mode	Cisco.com
Automatically Check For Updates	Enabled


When a software check is done and if a newer latest or recommended software update is available on Cisco.com, then:

- The **Software Update Alert icon** at the top right corner of the Web UI will be green in color (or gray). Clicking the icon will bring you to the Software Update page.
- The Update button at the bottom of the *Software Update* page is enabled.

 Cisco Business Wireless 140AC Access Point
 

**Software Update**

 Version

10.0.251.24

Transfer Mode	Cisco.com
Automatically Check For Updates	Enabled
Last Software Check	Fri Mar 27 10:44:29 2020
	<a href="#" style="background-color: #0070c0; color: white; padding: 5px 10px; border-radius: 3px;">Check Now</a>
Latest Software Release	10.0.1.0
	<a href="#" style="color: #0070c0;">?</a>
Recommended Software Release	10.0.1.0
	<a href="#" style="color: #0070c0;">?</a>

Save

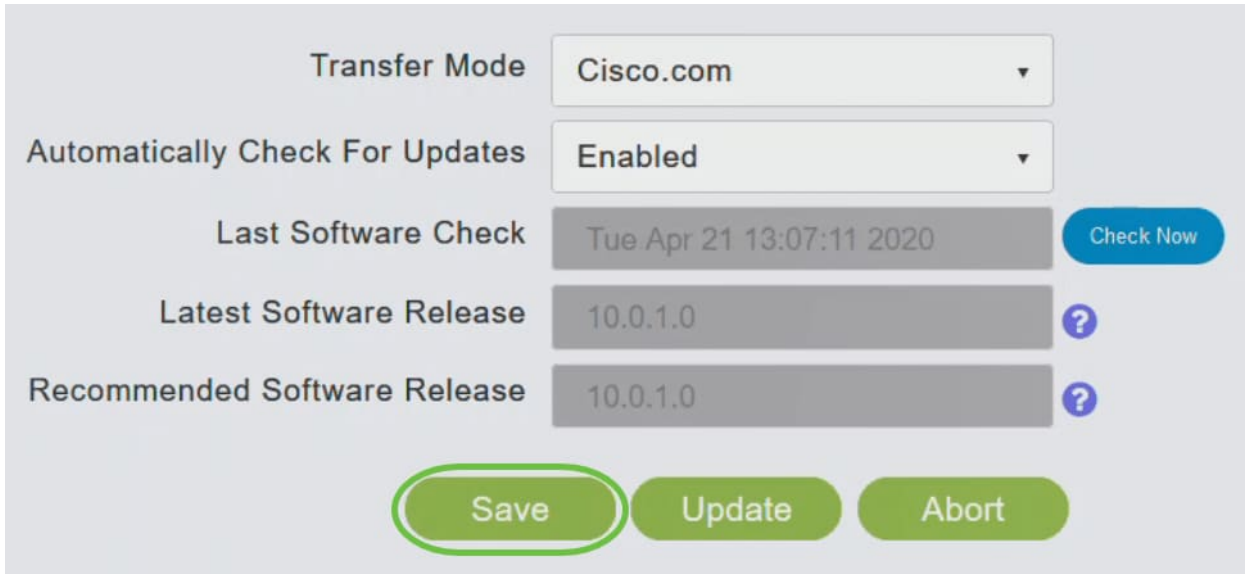
Update

Abort

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

**Step 5**

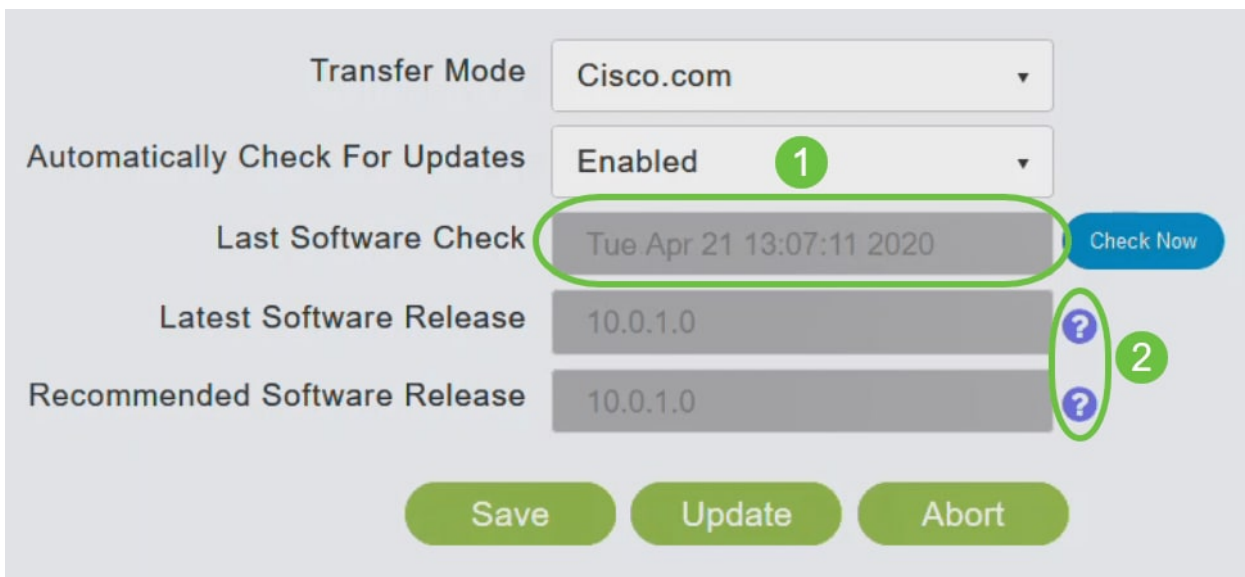
Click **Save**. This saves the entries or changes you have made in both *Transfer Mode* and *Automatically Check For Updates*.



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

Save Update Abort

The *Last Software Check* field displays the timestamp of the last automatic or manual software check. You can view the notes of displayed releases by clicking the **question mark icon** next to it.



Transfer Mode	Cisco.com	
Automatically Check For Updates	Enabled	1
Last Software Check	Tue Apr 21 13:07:11 2020	Check Now
Latest Software Release	10.0.1.0	?
Recommended Software Release	10.0.1.0	?

Save Update Abort

## Step 6

You can manually run a software check anytime by clicking *Check Now*.

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](#)

### Step 7

To proceed with the software update, click **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	?

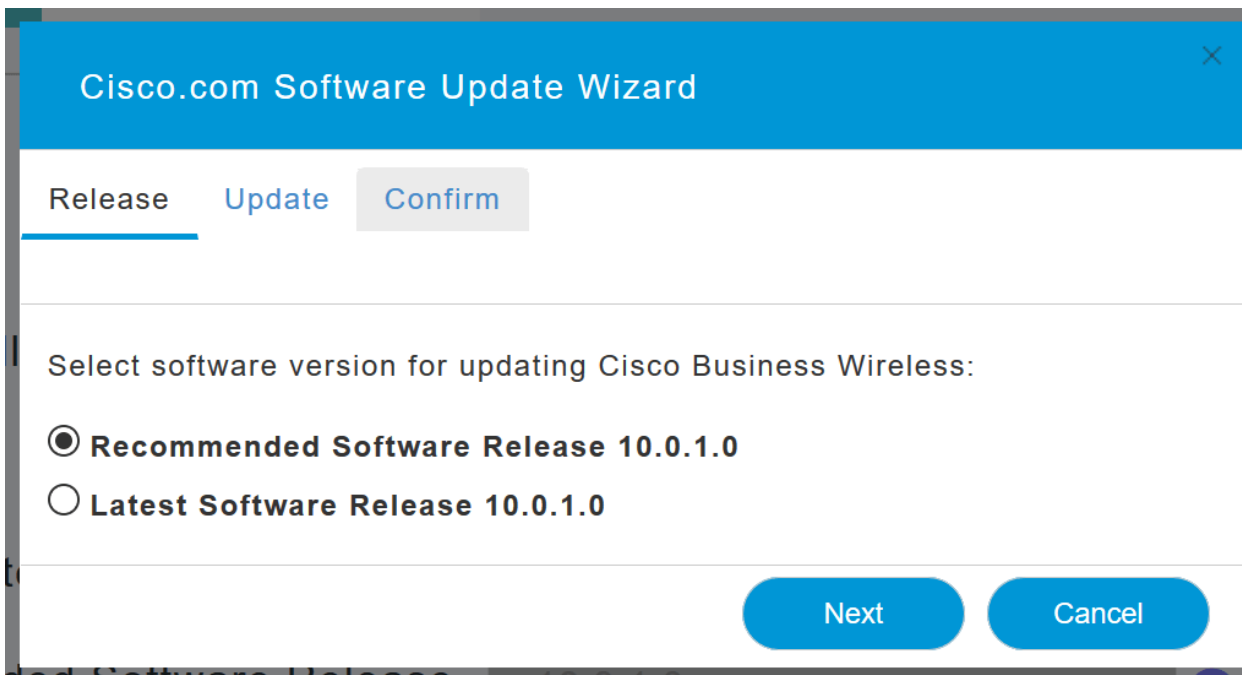
[Save](#) [Update](#) [Abort](#)

The *Software Update Wizard* appears. The wizard takes you through the following three tabs in sequence:

- Release tab - Specify whether you want to update to the recommended software release or the latest software release.
- Update tab - Specify when the APs should be reset. You can opt to have it done right away or schedule it for a later time. To set the Primary AP to automatically reboot after the image pre-download is complete, check the Auto Restart checkbox.
- Confirm tab - Confirm your selections.

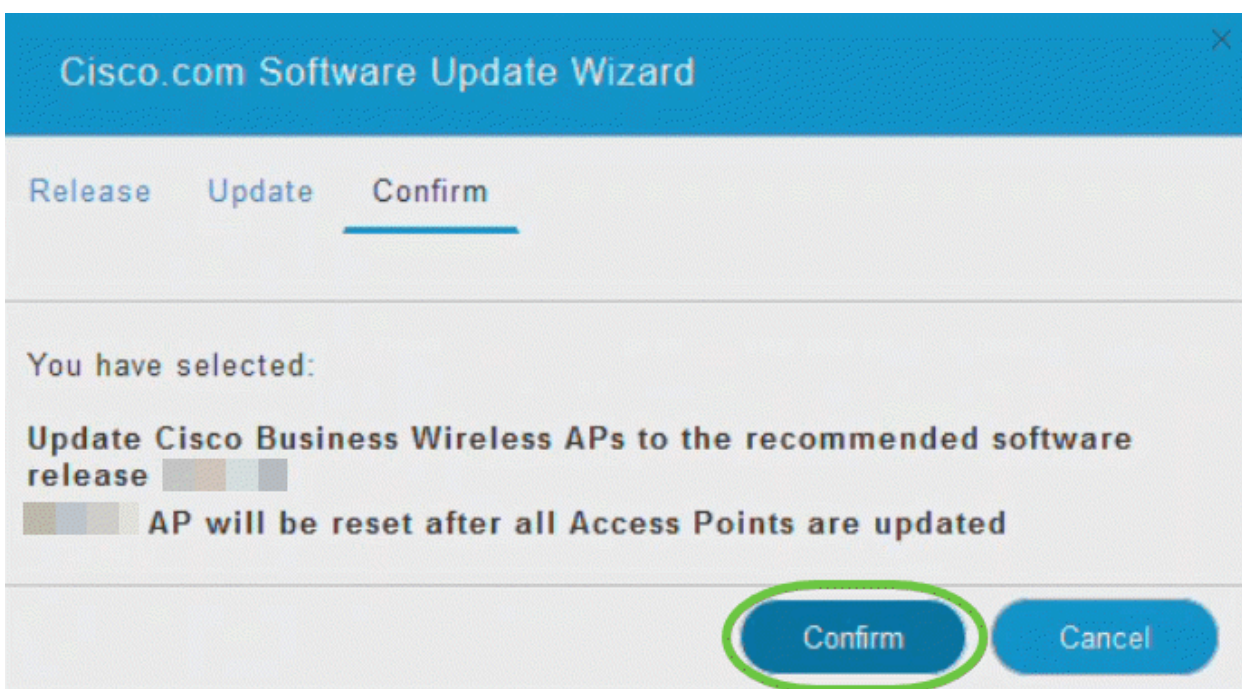
Follow the instructions in the wizard. You can go back to any tab at any time before you click *Confirm*.





### Step 8

Click **Confirm**.

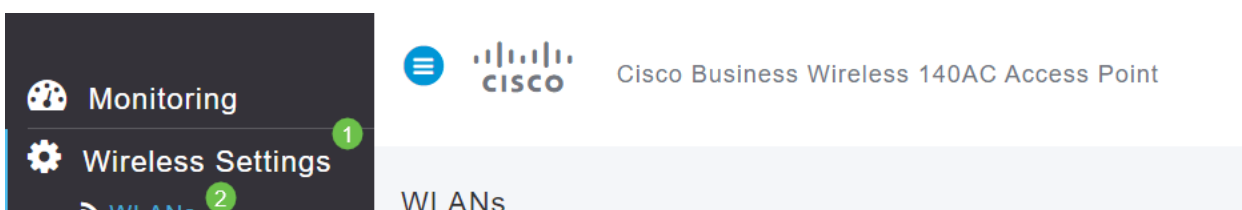


## Create WLANs on the Web UI

This section allows you to create Wireless Local Area Networks (WLANs).

### Step 1

A WLAN can be created by navigating to **Wireless Settings > WLANs**. Then select **Add new WLAN/RLAN**.



## Step 2

Under the *General* tab, enter the following information:

- WLAN ID – Select a number for the WLAN
- Type – Select **WLAN**
- Profile Name – When you enter a name, the SSID will auto-populate with the same name. The name must be unique and should not exceed 31 characters.

The following fields were left as default in this example, but explanations are listed in case you would like to configure them differently.

- SSID – The profile name also acts as the SSID. You can change this if you would like. The name must be unique and should not exceed 31 characters.
- Enable – This should be left enabled for the WLAN to work.
- Radio Policy – Typically you would want to leave this as **All** so that 2.4GHz and 5GHz clients can access the network.
- Broadcast SSID – Usually you would want the SSID to be discovered so you would want to leave this as Enabled.
- Local Profiling – You would only want to enable this option to view the Operating System that is running on the Client or to see the User name.

Click **Apply**.

The screenshot shows the 'Add new WLAN/RLAN' configuration window with the following settings:

- WLAN ID: 2 (marked with a green circle 1)
- Type: WLAN (marked with a green circle 2)
- Profile Name: Engineering (marked with a green circle 3)
- SSID: Engineering (marked with a green circle 3)
- Enable:
- Radio Policy: ALL (marked with a green circle 4)
- Broadcast SSID:
- Local Profiling:

Buttons:

## Step 3

You will be taken to the *WLAN Security* tab.

In this example, the following options were left as the default:

- Guest Network, Captive Network Assistant, and MAC Filtering were left disabled. Details for setting up a guest network are detailed in the next section.
- WPA2 Personal – Wi-Fi Protected Access 2 with Pre-shared Key (PSK) Passphrase Format – ASCII. This option stands for Wi-Fi Protected Access 2 with Pre-Shared Key (PSK).

WPA2 Personal is a method used for securing your network with the use of a PSK authentication. The PSK is configured separately both on the Primary AP, under the WLAN security policy, and on the client. WPA2 Personal does not rely on an authentication server on your network.

- Passphrase Format - **ASCII is left as default.**

The following fields were entered in this scenario:

- Show Passphrase – click the checkbox to be able to see the Passphrase you enter.
- Passphrase – Enter a name for the Passphrase (password).
- Confirm Passphrase – Enter the password again to confirm.

Click **Apply**. This will automatically activate the new 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

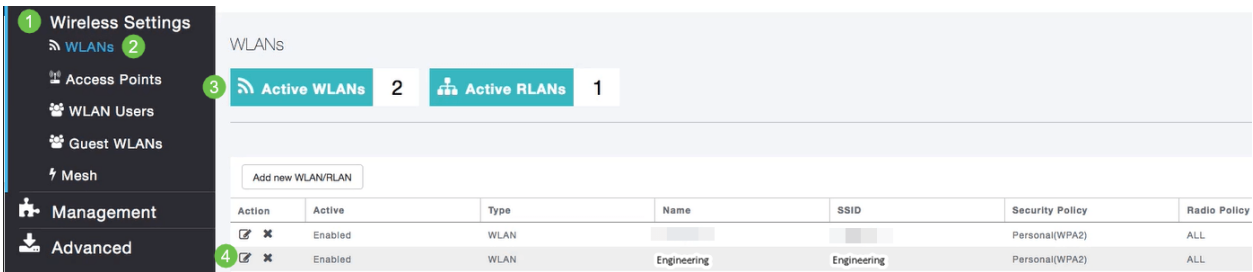
#### Step 4

Be sure to save your configurations by clicking the **save icon** on the top right panel of the Web UI screen.



#### Step 5

To view the WLAN you created, select **Wireless Settings > WLANs**. You will see the number of Active WLANs raised to 2, and the new WLAN is displayed.



Repeat these steps for other WLANs you want to create.

## Optional Wireless Configurations

You now have all basic configurations set and are ready to roll. You have some options, so feel free to jump to any of the following sections:

- [Create a Guest WLAN using the Web UI \(Optional\)](#)
- [Application Profiling \(Optional\)](#)
- [Client Profiling \(Optional\)](#)
- [I'm ready to wrap this up and start using my network!](#)

### Create a Guest WLAN using the Web UI (Optional)

A guest WLAN gives guest access to your Cisco Business Wireless network.

#### Step 1

Log into the Web UI of the Primary AP. Open a web browser and enter [www.https://ciscobusiness.cisco](https://ciscobusiness.cisco). You may receive a warning before proceeding. Enter your credentials. You can also access it by entering the IP address of the Primary AP.

#### Step 2

A Wireless Local Area Network (WLAN) can be created by navigating to **Wireless Settings > WLANs**. Then select **Add new WLAN/RLAN**.



### Step 3

Under the *General* tab, enter the following information:

*WLAN ID* – Select a number for the WLAN

*Type* – Select **WLAN**

*Profile Name* – When you enter a name, the SSID will auto-populate with the same name. The name must be unique and should not exceed 31 characters.

The following fields were left as default in this example, but explanations are listed in case you would like to configure them differently.

*SSID* – The profile name also acts as the SSID. You can change this if you would like. The name must be unique and should not exceed 31 characters.

*Enable* – This should be left enabled for the WLAN to work.

*Radio Policy* – Typically you would want to leave this as **All** so that 2.4GHz and 5GHz clients can access the network.

*Broadcast SSID* – Usually you would want the SSID to be discovered so you would want to leave this as Enabled.

*Local Profiling* – You would only want to enable this option to view the Operating System that is running on the Client or to see the User name.

Click **Apply**.

## Add new WLAN/RLAN

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

WLAN ID

1

Type

2

Profile Name \*

3

SSID \*

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

Enable

Radio Policy

?

Broadcast SSID

Local Profiling

?

4

Apply

Cancel

### Step 4

You will be taken to the *WLAN Security* tab. In this example, the following options were selected.

- Guest Network – Enable
- Captive Network Assistant – If you use Mac or IOS, you will probably want to enable this. This feature detects the presence of a captive portal by sending a web request on connecting to a wireless network. This request is directed to a Uniform Resource Locator (URL) for iPhone models and if a response is received, then the Internet access is assumed available and no further interaction is required. If no response is received, then the Internet access is assumed to be blocked by the captive portal and Apple's Captive Network Assistant (CNA) auto-launches the pseudo-browser to request portal login in a controlled window. The CNA may break when redirecting to an Identity Services Engine (ISE) captive portal. The Primary AP prevents this pseudo-browser from popping up.
- Captive Portal – This field is visible only when the Guest Network option is enabled. This is used to specify the type of web portal that can be used for authentication purposes. Select Internal Splash Page to use the default Cisco web-portal-based authentication. Choose External Splash Page if you will have captive portal authentication, using a web

server outside your network. Also, specify the URL of the server in the Site URL field.

## 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 ▼ ?

In this example, the Guest WLAN with an enabled Social login access type will be created. Once the user connects to this guest WLAN, they will be redirected to the Cisco default login page where they can find the login buttons for Google and Facebook. The user can log in using their Google or Facebook account to obtain Internet access.

### Step 5

On this same tab, select an *Access Type* from the drop-down menu. In this example, *Social Login* was selected. This is the option that allows guests to use their Google or Facebook credentials to authenticate and get access to the network.

Other options for *Access Type* include:

*Local User Account* – The default option. Choose this option to authenticate guests using the username and password which you can specify for guest users of this WLAN, under **Wireless Settings > WLAN Users**. This is an example of the default Internal Splash Page.



#### Welcome to the Cisco Business Wireless

Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your unified wireless solution to work.

User Name

Password

You can customize this by navigating to **Wireless Settings > Guest WLANs**. From here you can enter a *Page Headline* and *Page Message*. Click **Apply**. Click **Preview**.

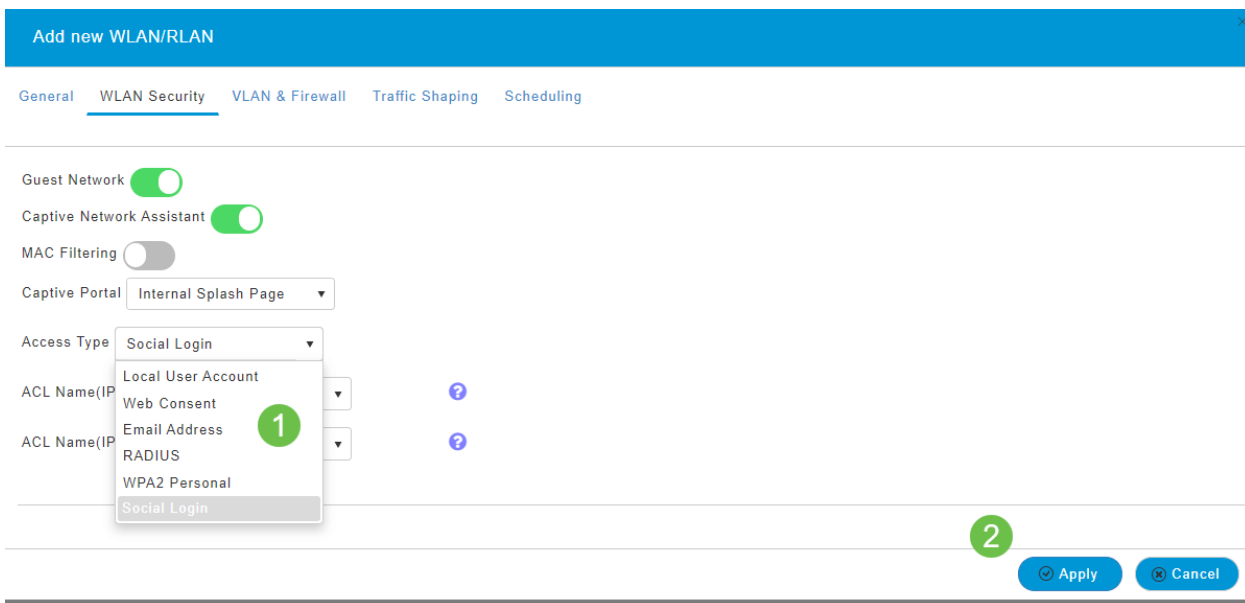
*Web Consent* – Allows guests access to the WLAN upon acceptance of displayed terms and conditions. Guest users can access the WLAN without entering a username and password.

*Email Address* – Guest users will need to enter their email address to access the network.

*RADIUS* – Use this with an external authentication server.

*WPA2 Personal* – Wi-Fi Protected Access 2 with Pre-shared Key (PSK)

Click **Apply**.



## Step 6

Be sure to save your configurations by clicking the **save icon** on the top right panel of the Web UI screen.



You have now created a guest network that is available on your CBW network. Your guests will appreciate the convenience.

## Application Profiling using the Web UI (Optional)

Profiling is a subset of features that enable enacting organizational policy. It allows you to match and prioritize traffic types. Like rules make decisions about how to rank or drop the traffic. The Cisco Business Mesh Wireless system features client and application profiling. The act of accessing a network as a user begins with many exchanges of information, among that information is the type of traffic. Policy interrupts traffic flow to direct the path, much like a flow-chart. Other types of policy features include - guest access, access control lists, and QoS.

## Step 1

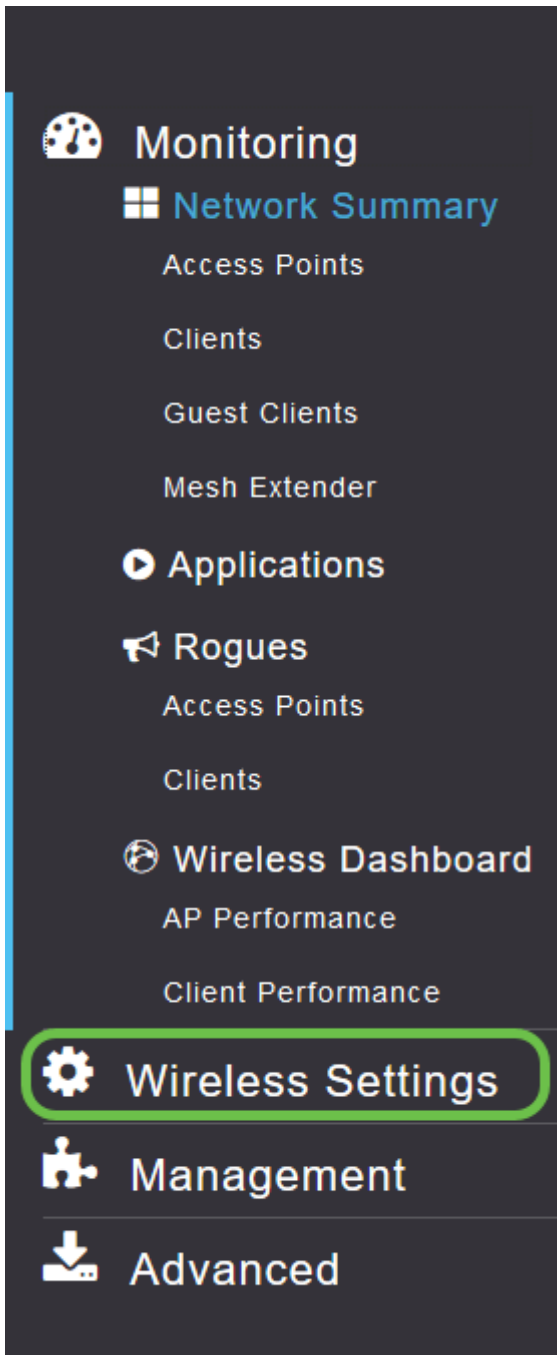


Navigate to the menu on the left-hand side of the screen if you don't see the left-hand menu bar.



## Step 2

The Monitoring menu loads by default when signing into the device. You will need to click **Wireless Settings**.

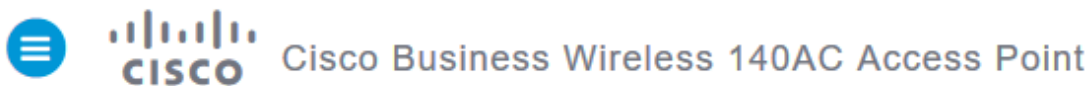


The image below is similar to what you will see when you click the Wireless Settings link.

The screenshot shows the Cisco Business Wireless 140AC Access Point management interface. The left sidebar contains navigation options: Monitoring, Wireless Settings (with sub-options: WLANs, Access Points, WLAN Users, Guest WLANs, Mesh), Management, and Advanced. The main content area is titled 'WLANs' and features a teal button labeled 'Active WLANs' with a count of '1'. Below this is a table with columns: Action, Active, Type, Name, SSID, Security Policy, and Radio Policy. The table contains one row with the following data: Action (checkbox checked), Active (Enabled), Type (WLAN), Name (EZ1K), SSID (EZ1K), Security Policy (Personal(WPA2)), and Radio Policy (ALL).

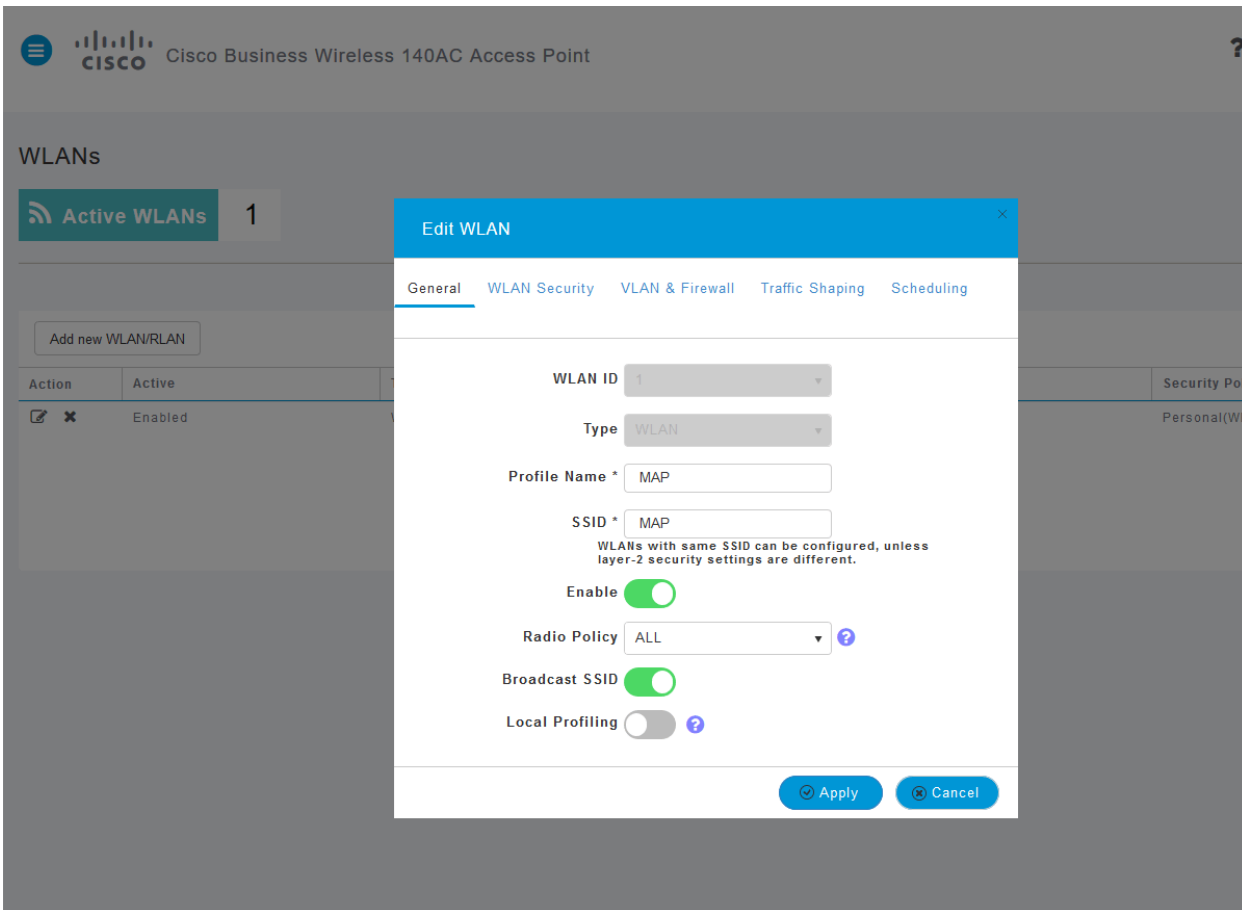
### Step 3

Click the **edit icon** to the left of the Wireless Local Area Network you want to enable the application on.



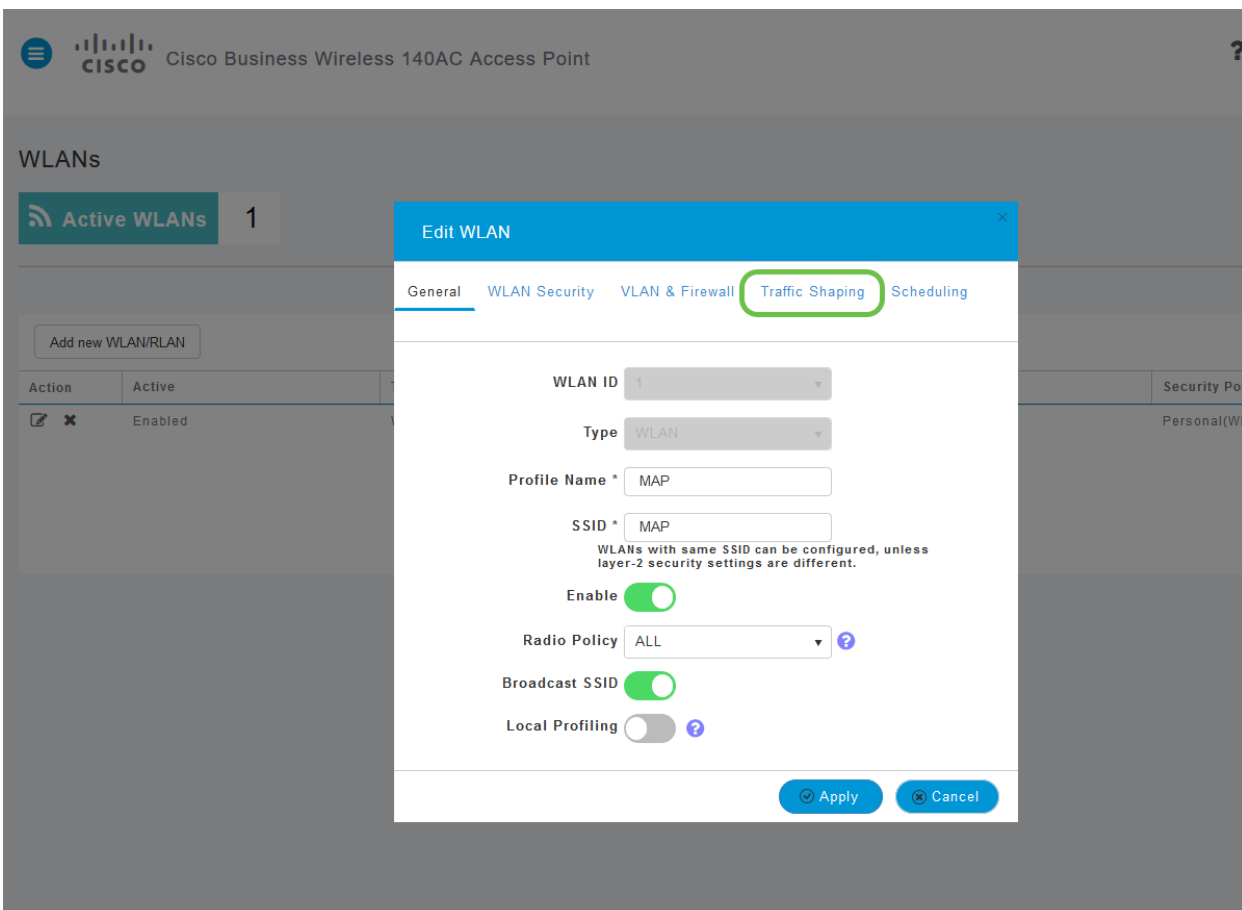
This screenshot is similar to the one above but highlights the 'Active WLANs' button and the 'Edit' icon in the table. The 'Active WLANs' button is highlighted with a teal background. The 'Edit' icon (a pencil) in the 'Action' column of the table is circled in green.

Since you recently added the WLAN, your *Edit WLAN* page may appear similar to the below:

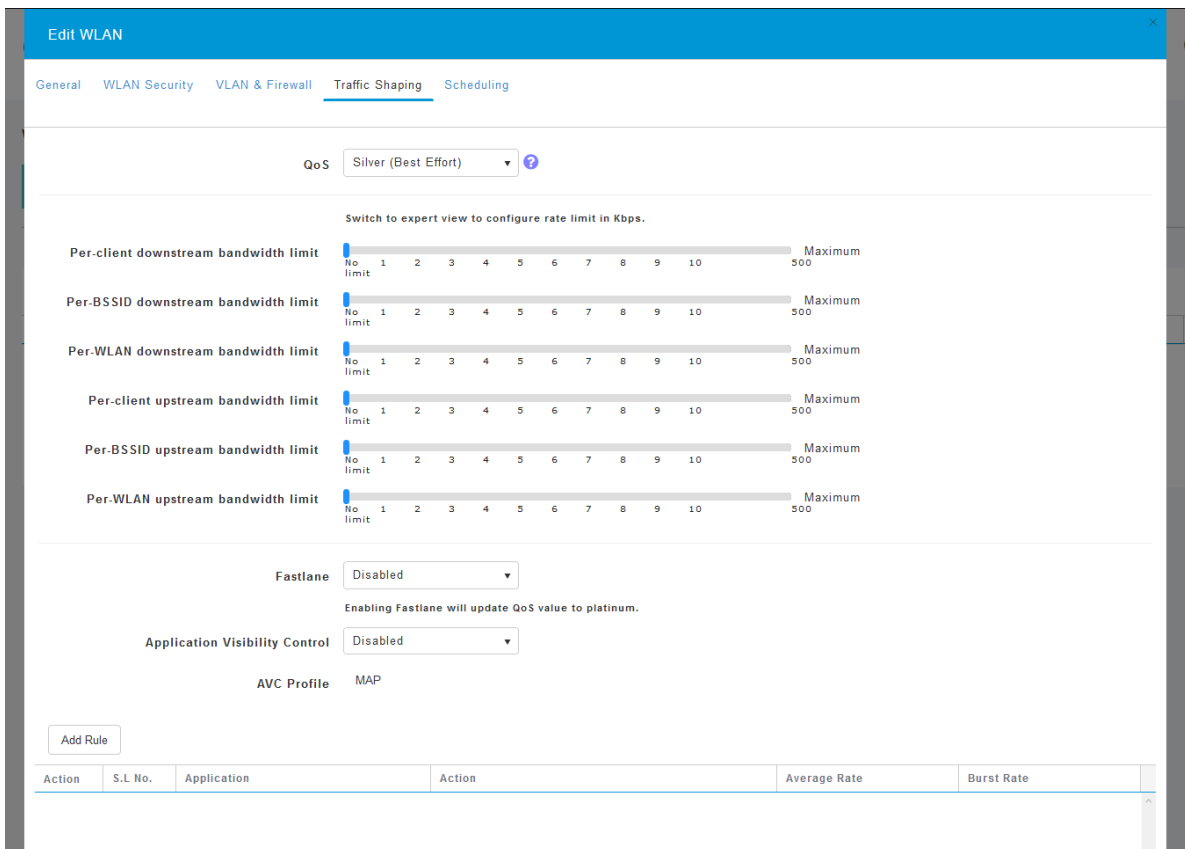


#### Step 4

Navigate to the **Traffic Shaping** tab by clicking on it.

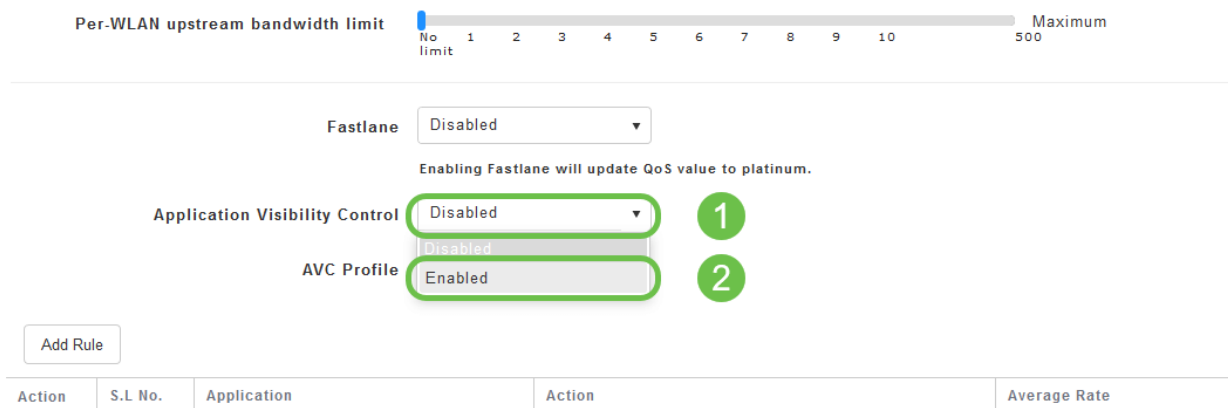


Your screen may appear as follows:



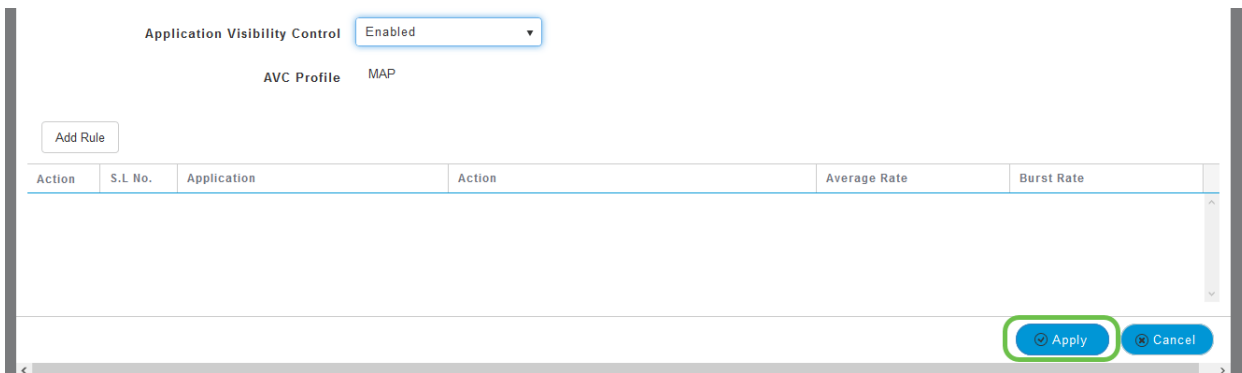
## Step 5

Toward the bottom of the page, you will find the *Application Visibility Control* feature. This is disabled by default. Click the dropdown and select **Enabled**.



## Step 6

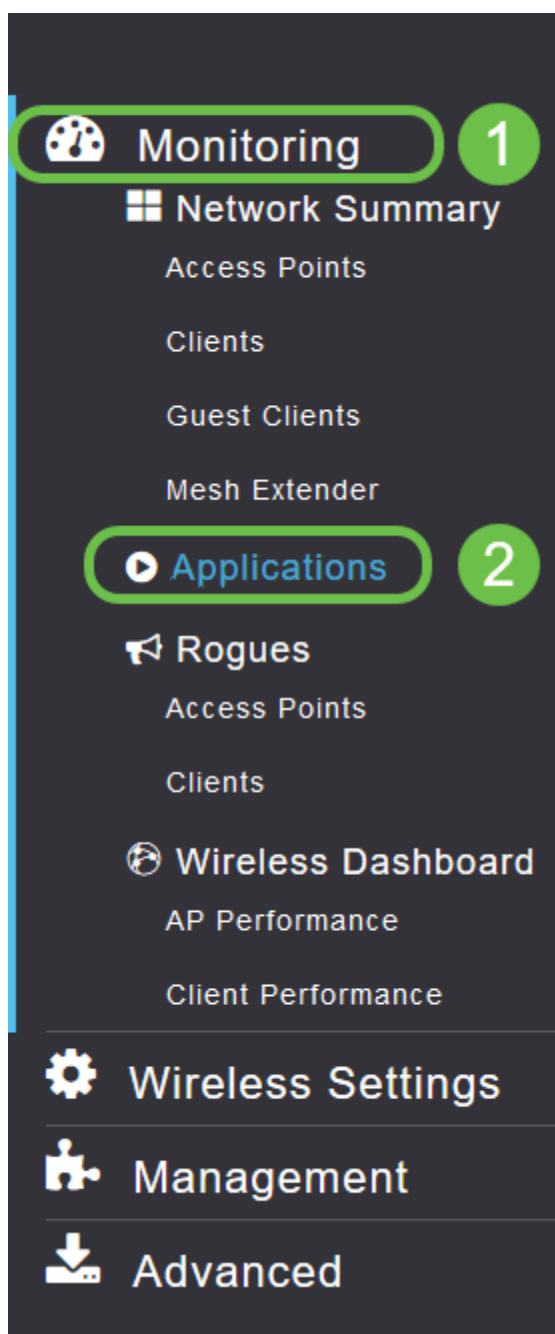
Click the **Apply** button.



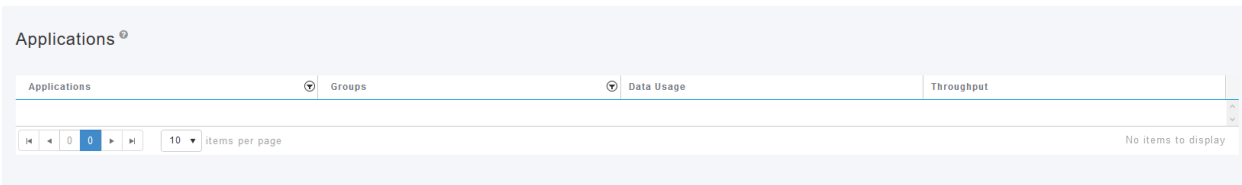
This setting must be enabled, otherwise the feature will not function.

## Step 7

Click the cancel button to close the WLAN sub-menu. Then click the **Monitoring** menu on the left-hand menu bar. Once you are able, click the **Applications** menu item.



If you've had no traffic to any source, your page will be blank as shown below.



This page will display the following information:

- Application – includes many different types
- Groups – Indicates the type of application group for easier sorting
- Data Usage – The amount of data used by this service overall
- Throughput – The amount of bandwidth used by the application

You can click on the tabs to sort from largest to smallest, which can help identify the largest consumers of network resources.

This feature is very powerful for managing your WLAN resources on a granular level. Below are some of the more common groups and application types. Your list is likely to include many more, including the following groups and examples:

- Browsing
  - EX: Client-specific, SSL
- Email
  - EX: Outlook, Secure-pop3
- Voice-and-video
  - EX: WebEx, Cisco Spark,
- Business-and-Productivity-tools
  - EX: Microsoft Office 365,
- Backup-and-storage
  - EX: Windows-Azure,
- Consumer-Internet
  - iCloud, Google Drive
- Social Networking
  - EX: Twitter, Facebook
- Software Updates
  - EX: Google-Play, IOS
- Instant Messaging
  - EX: Hangouts, Messages

Shown here is an example of what the page will look like when populated.

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

Each table heading is clickable for sorting which is especially useful for *Data Usage* and *Throughput* fields.

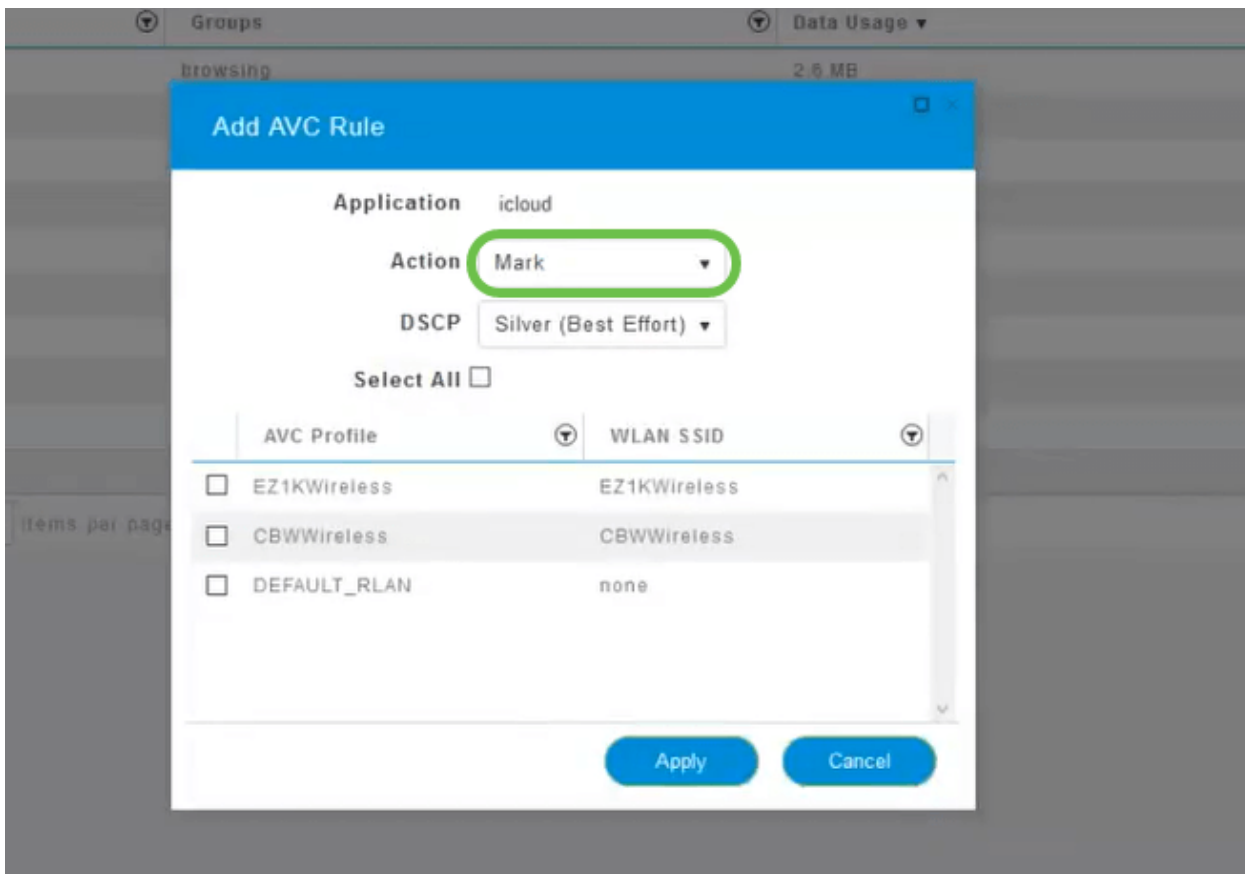
## Step 8

Click the row for the type of traffic you would like to manage.

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

## Step 9

Click the **Action** drop-down box to select how you will treat that traffic type.



For this example, we're leaving this option at *Mark*.

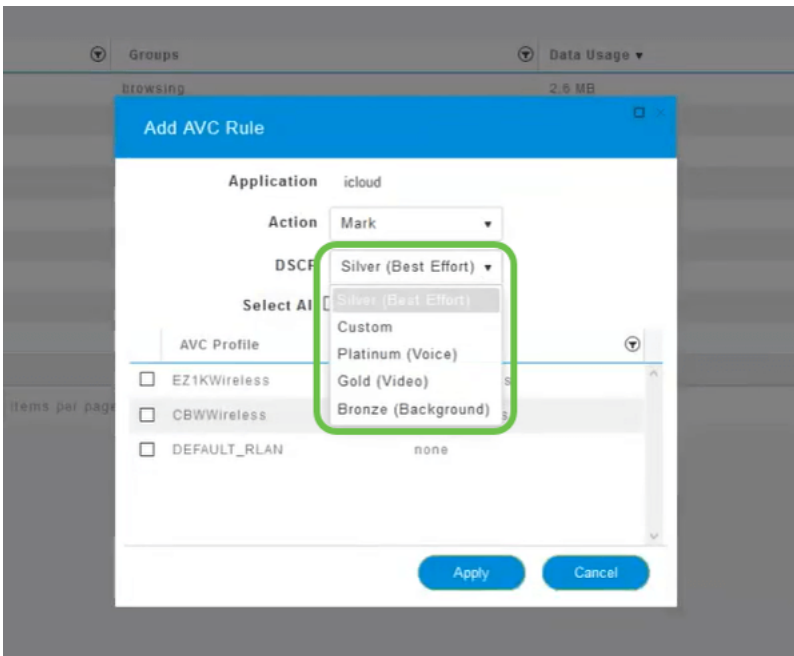
Action to take on traffic

- Mark – Places the traffic type into one of Differentiated Services Code Point (DSCP) 3 tiers -governing how many resources are available to the application type
- Drop – Do not do anything but discard the traffic
- Rate Limit – Enables you to set the Average Rate, Burst Rate in Kbps

## Step 10

Click the drop-down box in the **DSCP** field to select from the following options.





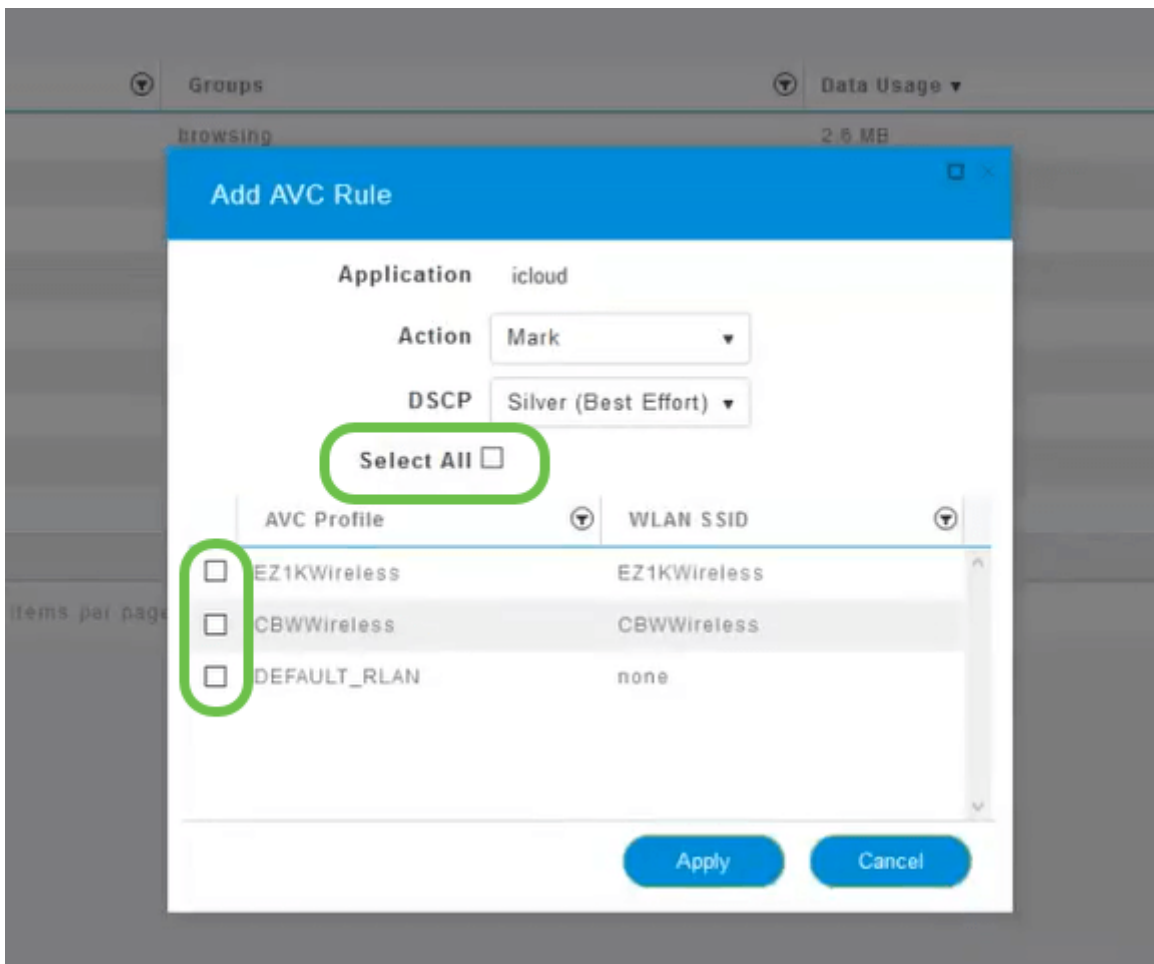
Below are the DSCP options for the traffic to be marked. These options progress from fewer resources to more resources available to the traffic type you are editing.

- Bronze (Background) – Less
- Silver (Best Effort)
- Gold (Video)
- Platinum (Voice) More
- Custom – User set

As a web convention, traffic has migrated toward SSL browsing, which prevents you from seeing what's inside the packets as they move from your network into the WAN. As such, a large majority of web traffic will be using SSL. Setting SSL traffic for a lower priority may affect your browsing experience.

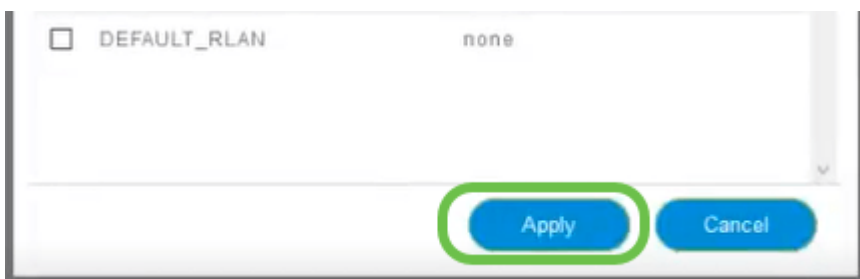
## Step 11

Now select the individual SSID you would like this policy to run or click **Select All**.



## Step 12

Now click **Apply** to begin this policy.



Two cases where this could apply:

- Guests/Users streaming a large amount of traffic preventing mission-critical traffic from getting through. You can either raise the priority for Voice, lower the priority of Netflix traffic to improve things.
- Large software updates downloading during office hours can be deprioritized or rate limited.

You did it! Application profiling is a very powerful tool that can be further enabled by also enabling Client Profiling, as is detailed in the next section.

## Client Profiling using the Web UI (Optional)

Upon connecting to a network, devices exchange client profiling information. By

default, *Client Profiling* is disabled. This information may include:

- Host Name – or the name of the device
- Operating System – the core software of the device
- OS Version – The iteration of the applicable software

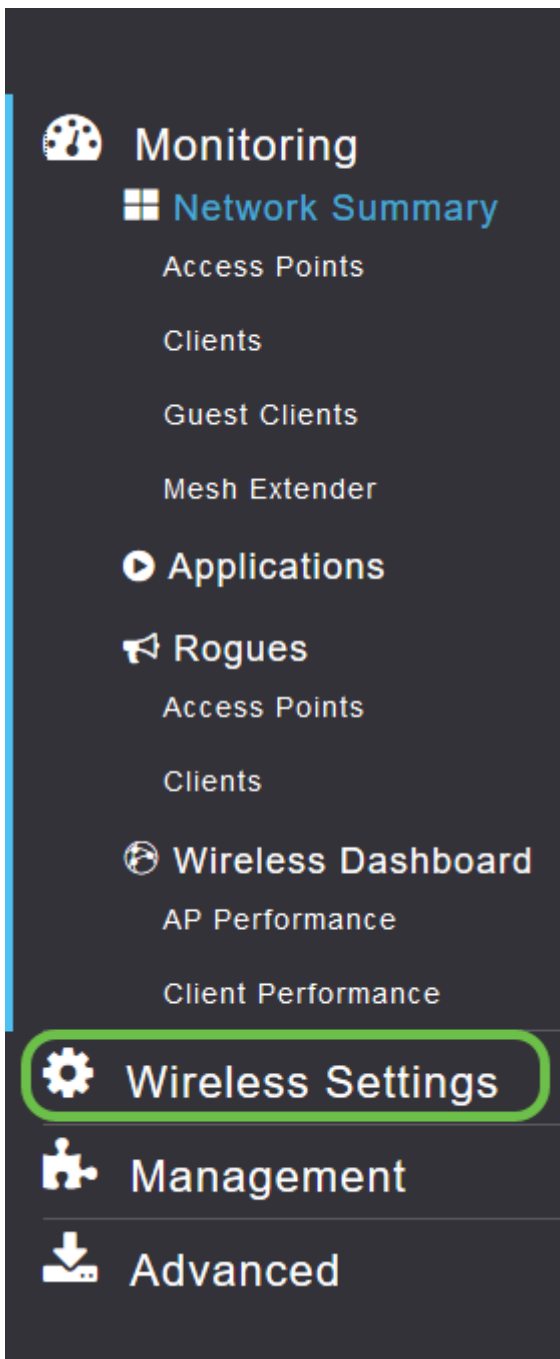
Statistics about these clients include the amount of data used and throughput.

Tracking client profiles enables greater control over the wireless local area network. Or you could use it as a function of another feature. Such as using application throttling device types that don't carry mission-critical data for your business.

Once enabled, client details for your network can be found on the Monitoring section of the Web UI.

## **Step 1**

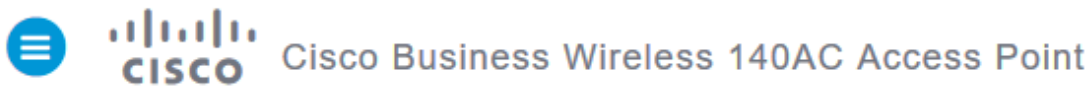
Click **Wireless Settings**.



The below is similar to what you will see when your click the Wireless Settings link:

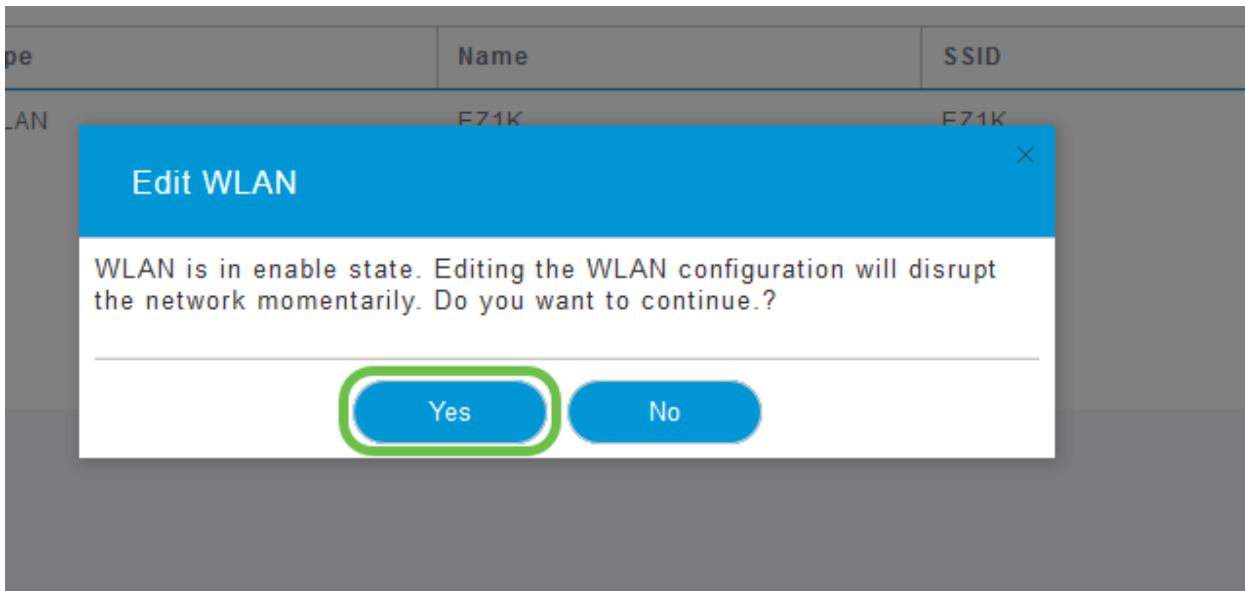
## Step 2

Decide which WLAN you want to use for the application and click the **edit icon** to the left of it.



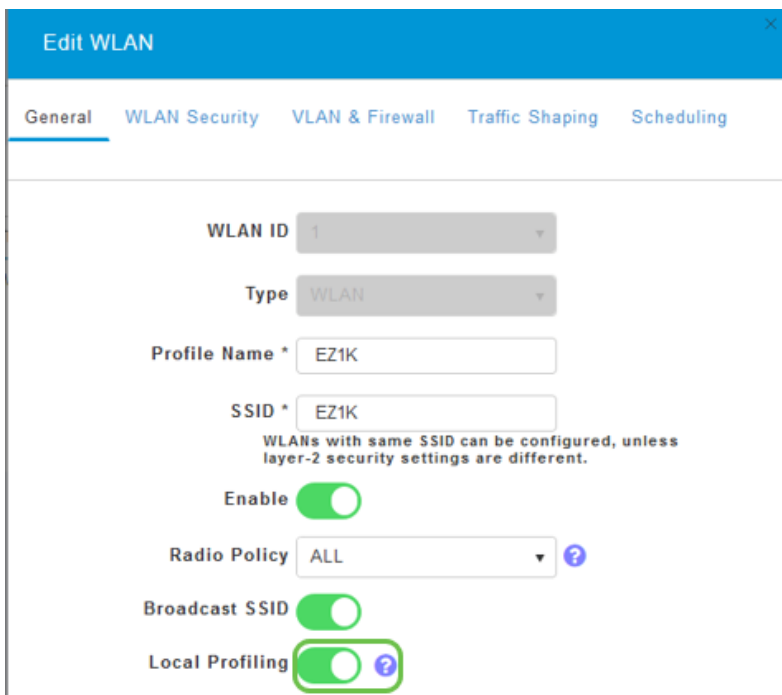
## Step 3

A pop-up menu may appear similar to the below. This important message may temporarily affect service on your network. Click **Yes** to move forward.



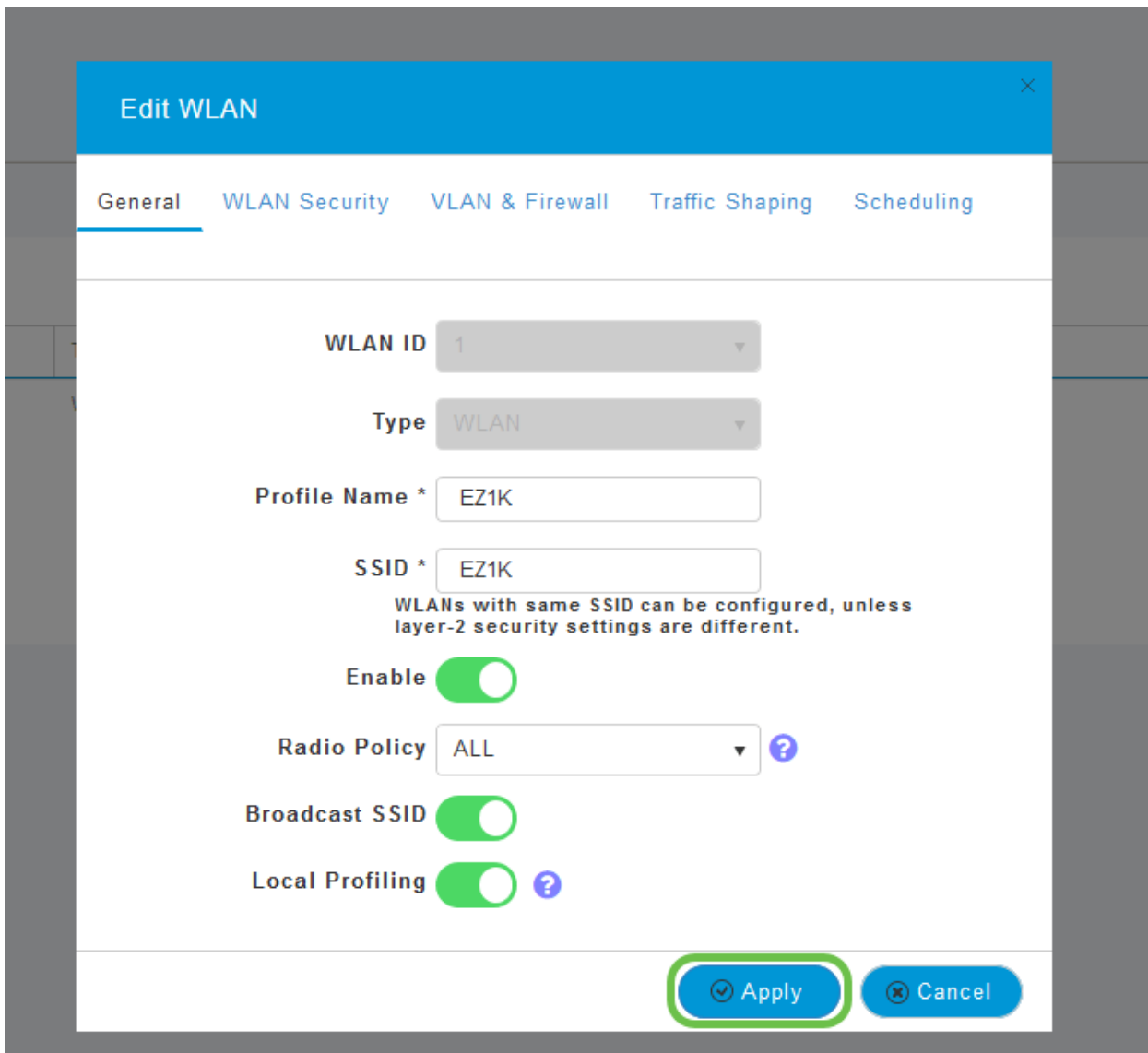
#### Step 4

Toggle client profiling by clicking the **Local Profiling** toggle button.



#### Step 5

Click **Apply**.



## Step 6

Click the **Monitoring** section menu item on the left-hand side. You will see the client data begin to appear in the Dashboard of the *Monitoring* tab.

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

## Conclusion

You now have now completed the setup of your secure network. What a great feeling, now ake a minute to celebrate and then get to work!

We want the best for our customers, so you have any comments or suggestions regarding this topic, please send us an email to the [Cisco Content Team](#).

If you would like to read other articles and documentation, check out the support pages for your hardware:

- [Cisco RV260P VPN Router with PoE](#)
- [Cisco Business 140AC Access Point](#)
- [Cisco Business 142ACM Mesh Extender](#)