

Troubleshooting a Cisco Business Wireless Mesh Network

Objective

This document will cover several areas to analyze when troubleshooting Cisco Business Wireless (CBW) mesh networks.

If you have a traditional wireless network, you should check out [Troubleshooting a Traditional Cisco Business Wireless Network](#).

Applicable Devices | Firmware Version

- 140AC ([Data Sheet](#)) | 10.1.1.0 ([Download latest](#))
- 141ACM ([Data Sheet](#)) | 10.1.1.0 ([Download latest](#))
- 142ACM ([Data Sheet](#)) | 10.1.1.0 ([Download latest](#))
- 143ACM ([Data Sheet](#)) | 10.1.1.0 ([Download latest](#))
- 145AC ([Data Sheet](#)) | 10.1.1.0 ([Download latest](#))
- 240AC ([Data Sheet](#)) | 10.1.1.0 ([Download latest](#))

Table of Contents

- [For optimum performance and reliability, keep these in mind!](#)
- [When troubleshooting, why not start with the basics?](#)
 - [Check Physical and Environmental Conditions](#)
 - [Other Items to Consider](#)
 - [Number of SSIDs](#)
- [Are you having trouble logging into the Primary AP?](#)
- [Do you have the latest version running on your APs?](#)
 - [Why It's Important](#)
 - [Upgrade Troubleshooting](#)
- [Do any of these situations apply to you?](#)
- [Check connectivity issues](#)
 - [Run Connectivity Tests from the Web User Interface \(UI\)](#)
 - [Could DHCP Problems be the Issue?](#)
 - [Windows Support](#)
- [Maybe the settings need to be adjusted](#)
 - [RF Optimization](#)
 - [Bridge Group Names](#)
 - [Allow Lists](#)
- [Interference and spacing considerations](#)
 - [Rogues, Interferers, and RF Channels...oh my!](#)
 - [Recommendations for Spacing and Deployment](#)
 - [Signal to Noise Ratio Between "Hops"](#)
- [Take a look behind the curtain](#)
 - [Syslogs](#)
 - [Support Bundle](#)

- [Access to the Primary AP Tech Support Bundle](#)
- [Adjust one of the CBW Mobile Phone Settings](#)
- [If all else fails, reset to factory default settings](#)

Introduction

Mesh wireless networks are awesome, but let's face it, things happen! Just like any wireless network, a number of things can cause problems. Sometimes there is a simple fix, while others might be more complicated.

If you are unfamiliar with terms in this document, check out [Cisco Business: Glossary of New Terms](#).

For optimum performance and reliability, keep these in mind!

1. Make sure the area has full coverage for the expected number of clients and their applications. Additional wireless access points may need to be added in order to smooth out the performance across your total wireless infrastructure.
2. Be aware of the types of applications they may be using (or as an administrator, the types of applications you may allow).
3. Clients running video streaming applications consume more bandwidth than those that may be streaming audio-only programs. Video applications rely on buffering to provide a decent experience.
4. Clients running voice-related applications require immediate service with no delays while not being as bandwidth-intensive. Since there is no buffering with a voice call, it is very important that packets are not dropped.


Ready for some troubleshooting? Let's dig in!

This toggled section highlights tips for beginners.

Logging In


Log into the Web User Interface (UI) of the Primary AP. To do this, open a web browser and enter <https://ciscobusiness.cisco.com> You may receive a warning before proceeding. Enter your credentials. You can also access the Primary AP by entering [https://\[ipaddress\]](https://[ipaddress]) (of the Primary AP) into a web browser.

Tool Tips

If you have questions about a field in the user interface, check for a tool tip that looks like the following: 

Trouble locating the Expand Main Menu icon?

Navigate to the menu on the left-hand side of the screen, if you don't see the menu button, click

this icon to open the side-bar menu. 

Cisco Business App

These devices have companion apps that share some management features with the web user interface. Not all features in the Web user interface will be available in the App.

[Download iOS App](#) [Download Android App](#)

Frequently Asked Questions

If you still have unanswered questions, you can check our frequently asked questions document. [FAQ](#)

When troubleshooting, why not start with the basics?

Check Physical and Environmental Conditions

This is the easiest way to troubleshoot but is often overlooked. Even though these may appear to be obvious, it is good to start with the basics.

1. Is all the equipment turned on?
2. Is there power to everything?
3. Do you have a link light on consistently? Green lights are a good sign!
4. Are the cables connected correctly?
5. Could it be a bad cable?
6. Is any of the equipment overheated?
7. Could there be environmental factors such as where it is located?
8. Are there metal or thick walls between the AP and the wireless device?
9. If the client is completely unable to connect, could the client be out of range?

Other Items to Consider

1. Restart the AP
2. For APs connecting to a switch, check the switch configuration and verify that the switch is running in good health. The CPU utilization, temperature, and memory utilization should be below the specified threshold levels.
3. On the Web UI, under *Monitoring*, check the *Wireless Dashboard* to gather information on performance and other issues.
4. Enable *Bonjour* and *Link Layer Discovery Protocol (LLDP)* on the router if it is available.
5. Enable *Wireless Multicast Forwarding* when available for gaming and streaming applications.
6. Make sure all Primary Capable APs are on the same VLAN.
7. If you've logged into the Primary AP via wireless, and you edit certain settings, such as the VLAN, you may be disconnected. Connecting to the Primary AP via wired allows that connection to remain more stable.

Number of SSIDs

Every SSID requires sending a beacon frame every 100 milliseconds (ms), which can eat up a lot of channel utilization.

It is best to limit the total number of SSIDs on the AP to 1-2 SSIDs per radio or per AP, even though the mesh network can support up to a physical limit of 16 SSIDs per radio.

Are you having trouble logging into the Primary AP?

Perhaps you have tried to log into *ciscobusiness.cisco*, and are encountering problems. Check out these simple suggestions:

- If you just completed Day Zero configurations, close the app and then re-launch it.
- Make sure the correct Service Set Identifier (SSID) is selected. This is the name that you created for the wireless network.
- Log into the Primary AP with *https://<IP address of the Primary AP>*. The Primary AP address is the assigned IP address you used in the initial set up procedure. If you opted out of assigning a manual address at that time, check your router for the DHCP IP address given to the Primary AP management page. The management address will be assigned on MAC address 00:00:5e:00:01:01.
- Once you do initial setup, be sure *https://* is being used whether you are logging into *ciscobusiness.cisco* or by entering the IP management address into your web browser. Depending on your settings, your browser may have auto-populated with *http://* since that is what you used the very first time you logged in.
- The problem might be your web browser. For example, in Firefox you would click on the menu at the top right of the screen. Select **Help > Troubleshooting Information** and click on **Refresh Firefox**.
- Disconnect any Virtual Private Network (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.
- If you have an Android phone, you may be using a private Domain Name Server (DNS) and may need to disable this feature for connectivity. To check this, you can typically find this under Settings > Network and Internet > Advanced > Private DNS.

Do you have the latest version running on your APs?

Why It's Important

Firmware, also referred to as software, comes embedded on your access point. Upgrading firmware improves the performance and stability of your AP. Upgrades may include new features or fix a vulnerability that was experienced in the previous version of the software. Is it really that important? Absolutely! It is so vital that all the links for upgrades were added in the [Firmware Version](#) section of this article. This could be a simple solution to try if you are having network problems. You may have issues when adding the first Mesh Extender to a network if there is a firmware version mismatch, so why not update them all right away!

It is extremely important to update all Mesh Extenders before updating the Primary Capable APs.

You can upgrade the firmware in a number of ways, but it is recommended that you use *Cisco.com* for the upgrade. If you would like assistance in upgrading firmware, check out [Update Software of a Cisco Business Wireless Access Point](#).

Upgrade Troubleshooting

Sometimes an upgrade doesn't go smoothly. There are some simple things you can try:

1. Refresh or close the web browser.
2. Clear the browser cache and re-log into the Primary AP. The process for this varies based on the web browser you use.
3. Click on an alternate page or tab in the Primary AP Web User Interface (UI) and then go back to the Software Update page and try the firmware image download again.
4. Try a new web browser. For example, if you were using Chrome and it isn't working, try Firefox.
5. On rare occasions, if the management page failed to start the firmware upgrade or is unresponsive (no status change after initiating upgrade), it may be necessary to power off/on all the access points and mesh extenders on the network and retry the firmware upgrade.

Do any of these situations apply to you?

- If you are using the downstream Ethernet port on the CBW240, switch to another port.
- If you are using captive portal, avoid using Chrome-based browsers, including Microsoft Edge. Sometimes you may not be able to join the network. It might be as simple as using Firefox as your browser.
- If a client is using a VPN connection without split tunneling/split DNS, the CBW management page may be inaccessible and the mobile app may not function. Try temporarily disabling the VPN on the client to access CBW management functions.
- If private DNS is enabled on the client, DNS queries are encrypted and CBW cannot intercept them. This will prevent the Cisco Business mobile app from working and will prevent `ciscobusiness.cisco` from resolving. It is recommended that you either manage CBW from a client joined to the network without private DNS, or manage CBW using the Web UI via the management IP address.
- Make sure CBW devices are not set up in the same VLAN as a Cisco Wireless LAN Controller.

Could it be a connectivity issue?

Run Connectivity Tests from the Web User Interface (UI)

The AP must be able to communicate with other devices to be effective. A simple way to check this is to perform a ping.

Ping the AP from at least two clients that are connected (associated) to that particular access point.

Ping from the router to the access point IP address to see if end-to-end connectivity is available. Ping from the router to the wireless clients associated with the AP to check if they can be reached from the main network.

Potential DHCP Problems

Even though you probably assigned a static IP address to your Primary AP, this AP still needs to have access to a DHCP server. This DHCP server must be operational and reachable from the LAN Ethernet port of the AP. This is necessary so the Primary AP can provide IP addresses for all

APs and clients that join the network. If you see a blinking red light on the Primary after a reboot, this could be your problem.

Even though a static IP address can be chosen for CBW management, it only applies to the management IP address. Every access point, including mesh extenders need a separate IP address for its access point functionality. The management MAC address is 00:00:5e:00:01:01.

Even if all CBW addresses are configured as static, adding a new AP or mesh extender still requires a DHCP server for the initial installation of the new device, even if you plan to change it to a static IP address later.

It's possible that there are more clients needing an IP address than are available in the DHCP pool. See the section *How to View or Change the Pool of IP Addresses for DHCP* section the article [Best Practices for Setting Static IP Addresses on Cisco Business Hardware](#) for more information.

There may be times where too many DHCP addresses are cached, which can also prevent clients from getting an IP address. To learn more about this, check out [Tips to Keep the ARP Table Available for DHCP IP Addressing](#). You may also reboot the router if this is more convenient.

Windows Support

If you use Windows, select your wireless connection from the Network Connections panel and verify that its status is *Enabled*.

Detailed guidance can be found at the Microsoft Support Forum for troubleshooting wireless network connectivity at the clicking on the following link: [Fix Wi-Fi connection issues in Windows](#).

Maybe the CBW settings need to be adjusted

There are some default settings that might cause connection issues in some older devices. You can try changing the following settings.

RF Optimization

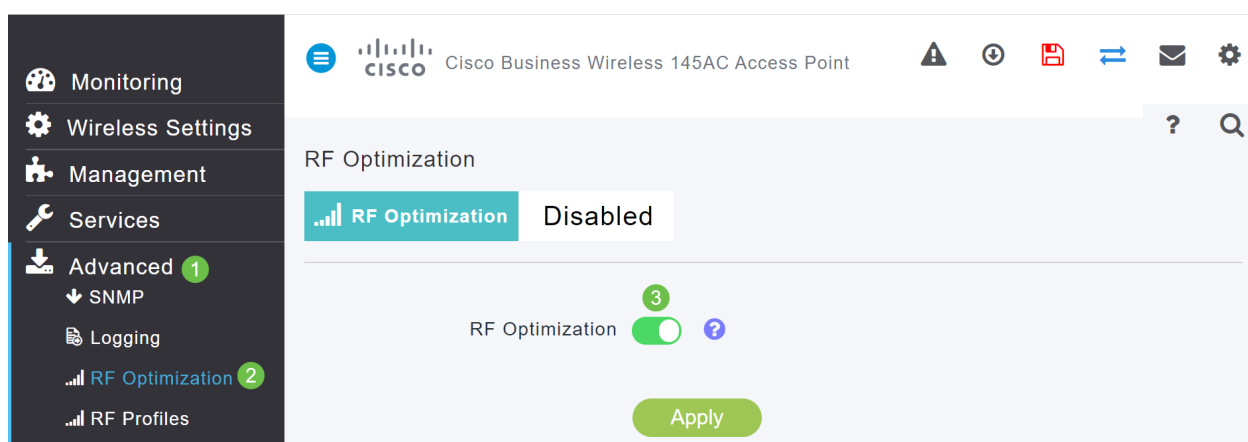
Step 1

Make sure you are in *Expert View* for these settings.



Step 2

Navigate to **Advanced > RF Optimization**. Toggle on *RF Optimization*.



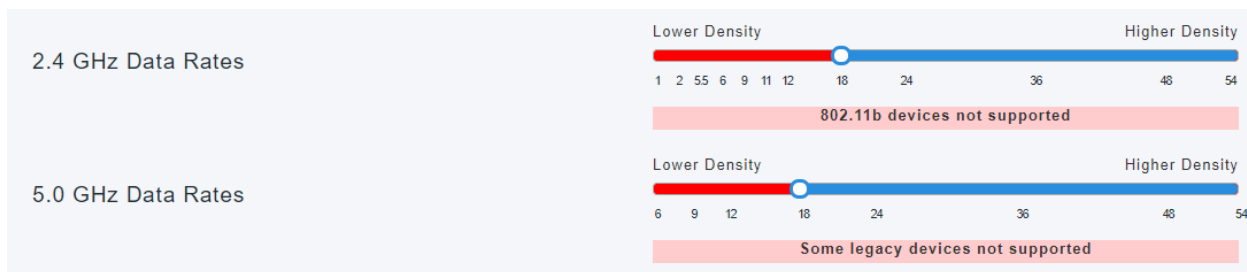
Step 3

Scroll down to the bottom of this screen. Within each radio Data Rates, remove support for lower control rates to remove older legacy wireless mode clients, such as 802.11b clients.



Step 4

A notification will come up that older devices are not supported. The further to the right you slide, the less that can connect.



Bridge Group Names

If you set up your network with all APs at factory default

When you conducted the Day Zero configurations for your mesh network, a BGN was automatically created. It is the same as the first Service Set Identifier (SSID) you entered, up to the first 10 characters. This BGN is used within APs to associate and make sure the APs are staying connected properly. If you set up your Primary AP and then join subordinate APs, the BGN should automatically match with no further configurations needed.

If you reset a Primary AP or moved a configured AP to a new network

If you perform a reset to factory default on the Primary AP, or move APs from one configured network to another, this can cause a mismatch of BGNs.

When an AP tries to join a network in a scenario where the BGN doesn't match any networks available, the subordinate AP will still attempt to temporarily join the network with the strongest signal. The AP will be able to join the network if it is [Allow Listed](#) and approved.

Once the AP has joined the network, since the BGN doesn't match, the subordinate AP will continue to look for a matching BGN every 10 to 15 minutes. This will cause the connection to drop and then join again if a matching BGN isn't found. This can cause a lot of problems with connectivity in the wireless network, especially when there might be a stronger wireless signal coming from another wireless network.

As a simple solution, for all APs to work together, you should make sure the BGN on all APs match exactly. To clear out the BGN on the other APs, you can do a factory reset on them, or you can manually change each one to match.

If you want to view or change a Bridge Group Name (BGN) on an AP

It is recommended that BGNs get assigned to the mesh extenders with the most hops be configured first, working up to the least number of hops. After that, the Primary Capable APs BGNs should be assigned. The Primary AP BGN should be configured last. You can view and change them one at a time by performing the following steps.

Step 1

Log into the AP and enter your credentials.



Cisco Business Wireless Access Point

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



© 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 2

Switch to *Expert View* by clicking on the **arrow icon**.



Step 3

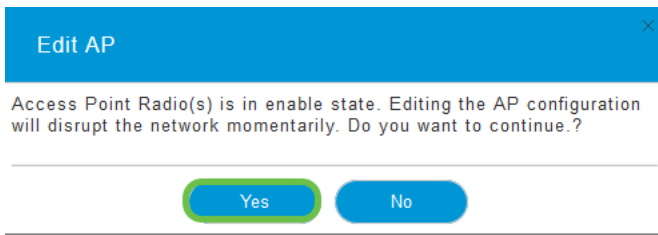
Navigate to **Wireless Settings > Access Points**. Click on the **edit icon** of the AP you want to edit or view.

The screenshot shows the Cisco Business Wireless 140AC Access Point configuration interface. The left sidebar has a navigation menu with 'Monitoring' (1), 'Wireless Settings' (2), 'WLANs', 'Access Points' (2), 'Access Points Groups', 'WLAN Users', 'Guest WLANs', 'Mesh', 'Management', 'Services', and 'Advanced'. The main content area is titled 'Access Points' and shows a table of two APs. The first AP is a 'Master Capable' AP with IP 192.168.1.127 and model CBW140AC-B. The second AP is a 'Mesh Extender' with IP 192.168.1.112 and model CBW142AC... The table has columns for Action, Manage, Type, Location, Name, IP Address, AP Mac, Up Time, and AP Model. There are also icons for Master AP, Primary Master AP and Preferred Master, Preferred Master, and Mesh Extender. A 'Global AP Configuration' button is visible in the top right of the table area.

Action	Manage	Type	Location	Name	IP Address	AP Mac	Up Time	AP Model
		Master Capable	default locat...	APA453.0E1...	192.168.1.127	a4:53:0e:1f...	44 days, 21 ...	CBW140AC-B
		Mesh Extender	default locat...	AP68CA.E46...	192.168.1.112	68:ca:e4:6e...	23 days, 16 ...	CBW142AC...

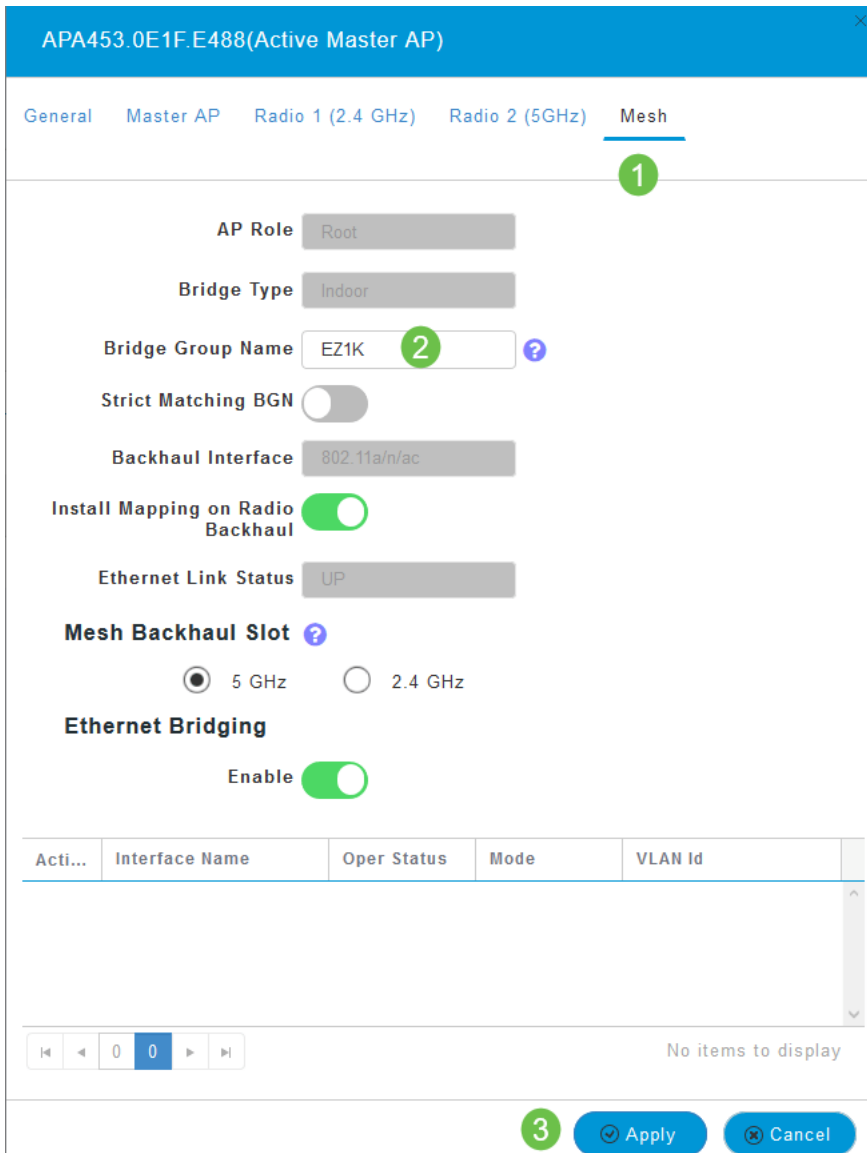
Step 4

A pop-up will ask for confirmation that you want to edit the AP configuration. Select **Yes**.



Step 5

Click the *Mesh* tab. Here you can view and change the *Bridge Group Name*. If you make changes, be sure you click **Apply**.



Step 6

Repeat the steps for each AP in the network you want to check. Click the **save icon** to permanently save any changes. Keep in mind that when a bridge group name is assigned, the device performs a reboot. Since a reboot interrupts Wi-Fi, it is not recommended during business hours.



Allow Lists

In order to connect other Primary-capable APs and mesh extenders, you need to create an Allow List on a Primary AP that includes the Media Access Control (MAC) address of all the APs.

In addition, subordinate APs need to be Allow Listed so that the Primary AP can access and upgrade the other APs, which is essential to keep the network up and running.

This Allow List, along with all APs having the same Bridge Group Name (BGN), helps the APs connect efficiently and consistently. To add a Media Access Control (MAC) address and label it as Allow List, complete the following steps.

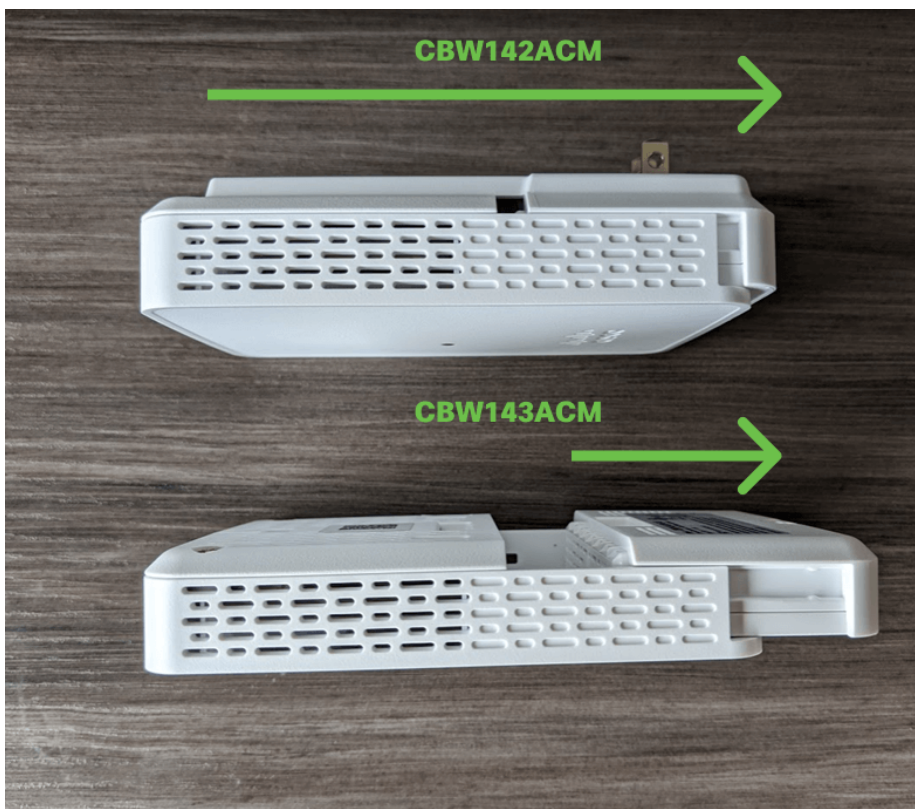
Step 1

You need to know the MAC address of the AP. If you know the MAC address of your AP, you can skip to [Step 4](#).

A MAC address includes numbers and letters in pairs, separated by colons.

Step 2

On most APs, the MAC address can be found on the outside of the actual AP. On the 142ACM and 143ACM you need to slide out the power apparatus to view the MAC address. To do this, apply light pressure on the AP where the arrows indicate. Slide and lift the power component out.



Step 3

On the 142ACM and 143ACM, you will see the MAC address in the locations pointed out below.



Step 4

1. Select **Wireless Settings**
2. Select **WLAN Users**
3. Select **Local MAC Addresses**
4. Select **Add MAC Address**

The screenshot shows the Cisco Business Wireless 140AC Access Point configuration interface. The left sidebar contains navigation options: Monitoring, Wireless Settings (1), WLANs, Access Points, Access Points Groups, WLAN Users (2), Guest WLANs, Mesh, Management, Services, and Advanced. The main content area is titled 'WLAN Users' and shows a 'Users' count of 0. Below this, there are tabs for 'WLAN Users' (3) and 'Local MAC Addresses' (3). A search bar is present. Below the search bar, there are buttons for 'Add MAC Address' (4), 'Refresh', and 'Number of Blacklist:0 Number of Whitelist:2'. A table displays the current MAC addresses:

Action	MAC Address	Type	Profile Name	Description
	68:ca: [redacted]	WhiteList	Any WLAN/RLAN	CBW142 Mesh Extender
	a4:53: [redacted]	WhiteList	Any WLAN/RLAN	CBW140AC-e488

At the bottom, there is a pagination control showing '10 items per page' and '1 - 2 of 2 items'.

Step 5

Enter the following information:

1. *MAC Address*
2. *Description* (up to 32 characters)
3. Select the *Allow List* radio button
4. Click **Apply**

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

- 1. **MAC Address**: a4:52:0f:1e:16:5a
- 2. **Description**: ACM141
- Type**: BlackList WhiteList (3)
- Profile Name**: Any WLAN/RLAN

At the bottom, there are buttons for **Apply** (4) and **Cancel**.

Interference and spacing considerations

Rogues, Interferers, and RF Channels...oh my!

Interference can cause issues on wireless networks and can come from more sources than ever before. Microwaves, security cameras, smartwatches, motion detectors, or even fluorescent bulbs can cause interference.

How much they affect the network can depend on many factors including the amount of power emitted if the object is constantly on, or if it is intermittent. The stronger the signal or the more frequently it is on the more problems that can arise.

Rogue APs and rogue clients can cause problems if there are too many on the same channel as well.

Interference can be a major inhibitor to wireless performance, creating security vulnerabilities and wireless network instability.

There are tools available to monitor **the channel(s) you are currently utilizing**. You have the ability to change channels as well. Check out the following articles for more information.

- [Identifying Rogue Clients](#)
- [Identifying Interferers](#)
- [Changing RF Channels](#)

Recommendations for Spacing and Deployment

1. Place Mesh Extenders in line-of-site of Primary-Capable APs.
2. Downstream Mesh Extenders in line-of-site of parent Mesh Extender.
3. Downstream Mesh Extenders require good/excellent on backhaul SSID signal strength from upstream Primary-Capable APs.
4. Mesh Extenders should have a minimum Signal to Noise Ratio (SNR) value of 30.
5. Avoid placing Mesh Extenders too close to other Mesh Extenders or other Primary-Capable APs.

The following chart lists the expected coverage areas in an open space. If you deploy your network in an area that is not open, reduce these values by 20-30%.

Model	Recommended Distance (Meters)	Recommended Distance (Feet)
CBW240AC	18 - 21	60 - 70
CBW140AC	15 - 18	50 - 60
CBW145AC	15 - 18	50 - 60
CBW141ACM	15 - 18	50 - 60
CBW142ACM	10 - 13	32 - 42
CBW143ACM	10 - 13	32 - 42

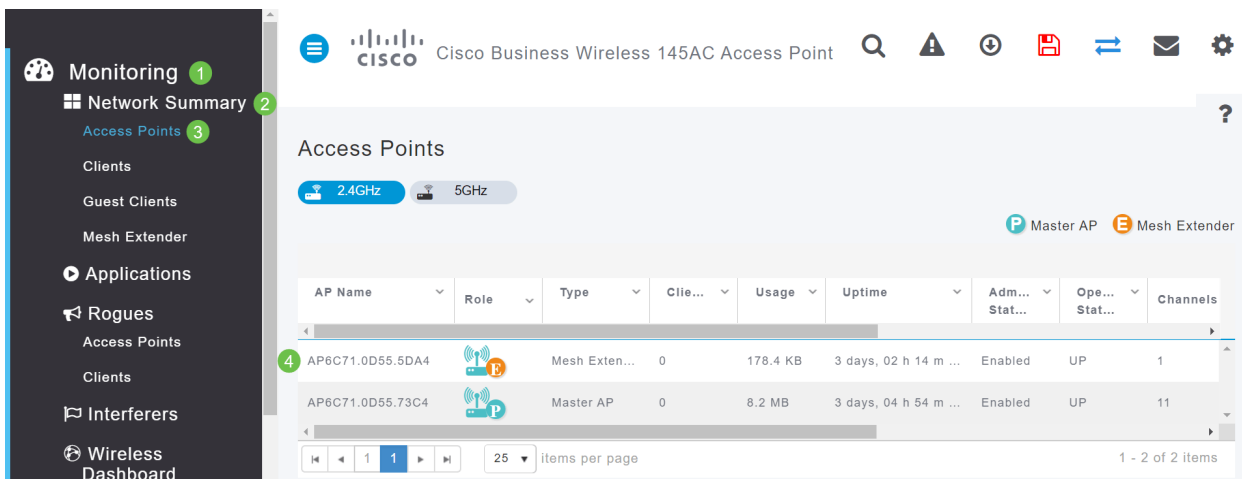
Signal to Noise Ratio Between “Hops”

In all networks, you need to work on a strong signal between clients and the APs. In a mesh network, you also need to make sure there is a strong signal between the various APs between each other. If one of the “hops” doesn’t have a great signal, a higher signal to noise ratio, you will need to troubleshoot that. You may need to adjust the location or check to see what is causing interference.

Step 1

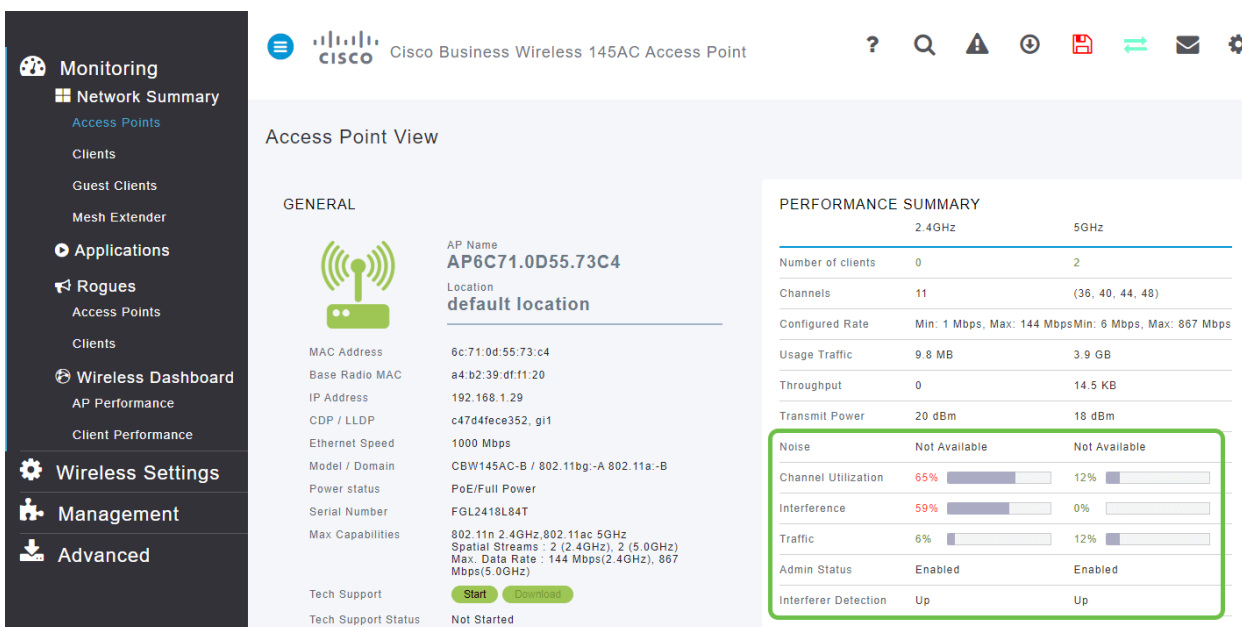
Navigate to **Monitoring > Network Summary > Access Points** and click on any access point in

the table to check the associated client signal strength.



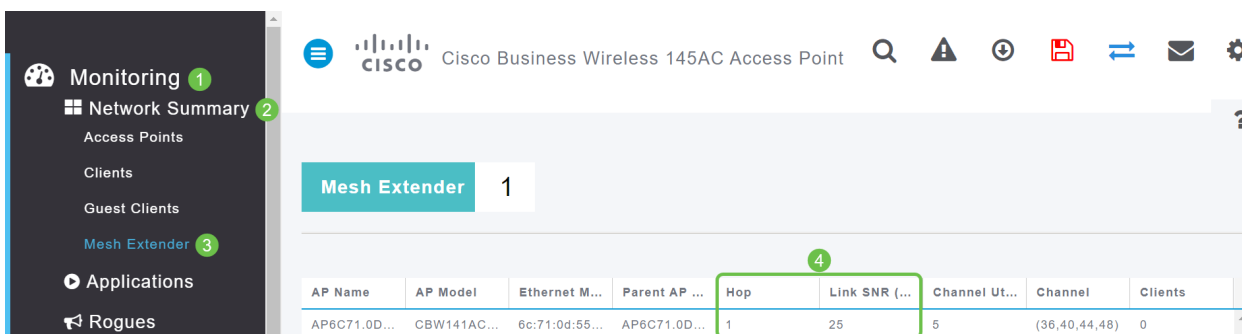
Step 2

Once the *Access Point View* opens, look over the information under *Performance Summary*.



Step 3

You can also gather information on all mesh extender *Hop* counts and *Signal to Noise Ratio*. Navigate to **Monitoring > Network Summary > Mesh Extender**.



Take a look behind the curtain

Syslogs

Being aware of events can help ensure the network runs smoothly and prevent failures. Syslogs are useful for network troubleshooting, debugging packet flow, and to monitor events.

These logs can be viewed on the Web User Interface (UI) of the Primary AP and if configured, on remote log servers. Events are typically erased from the system when rebooted if they are not saved on a remote server.

If you would like more information, check out [Setting Up System Message Logs \(Syslogs\) on a CBW Network](#).

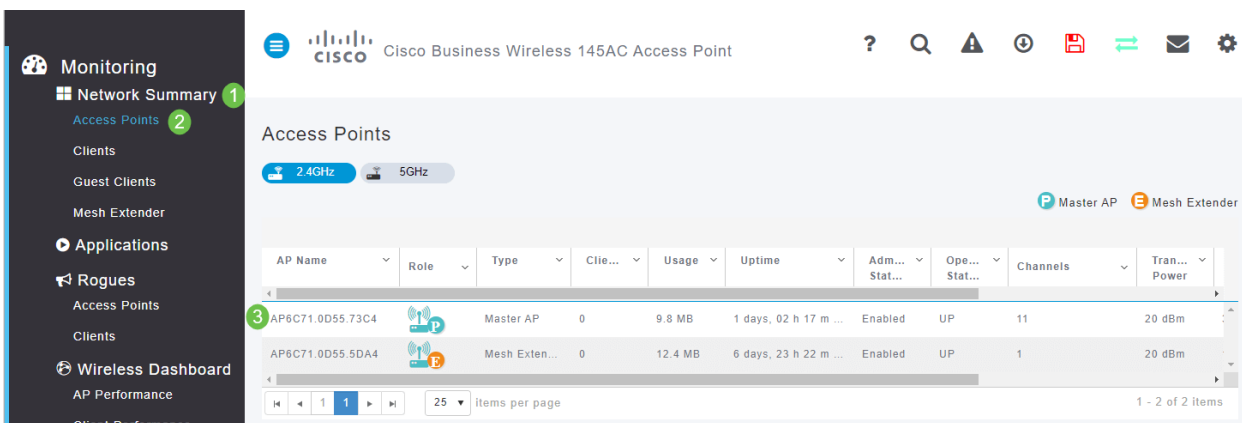
Support Bundle

A feature that is available on this CBW equipment is to download a support bundle. A support bundle is a tool that can be helpful in troubleshooting. It provides the AP boot-up logs and specifies the configurations applied. To get a complete picture, this might need to be done on every AP.

Before downloading the support bundle on the Primary AP, make sure you are running the most current release of firmware. To update firmware, select the correct link under [Applicable Devices | Firmware Version](#). If you would like assistance in upgrading firmware, check out [Update Software of a Cisco Business Wireless Access Point](#).

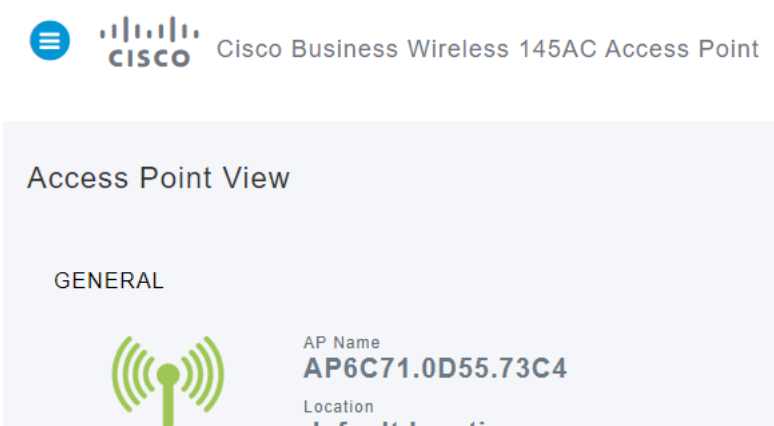
Step 1

To download the tech support bundle specific to access point functionality, select **Monitoring > Access Points**. Select the AP you would like to access.



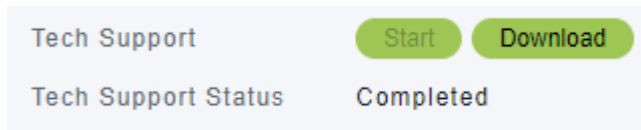
Step 2

Under the *Tech Support* section, select **Start**.



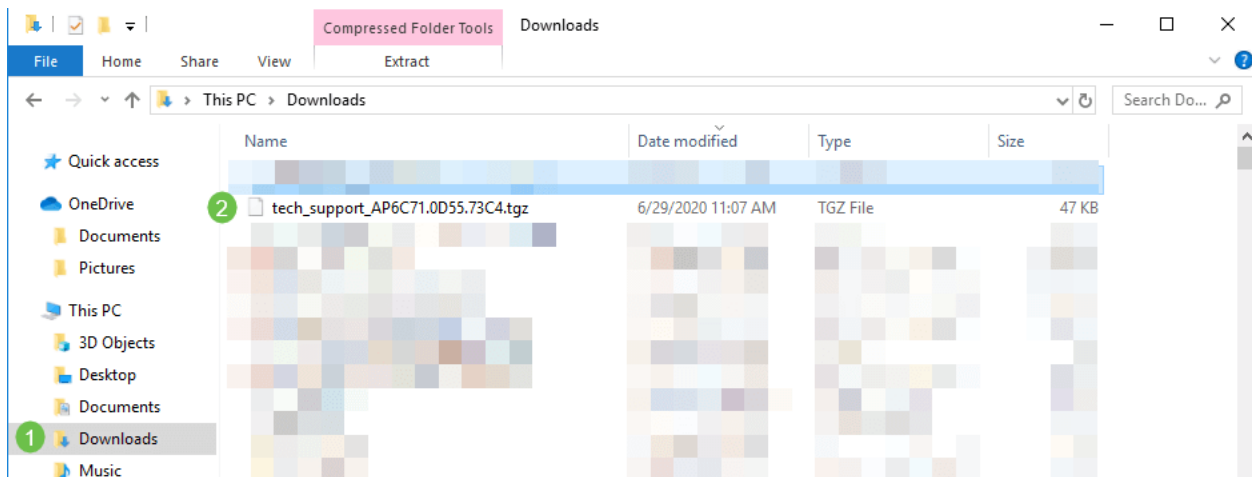
Step 3

When the download is complete, you will see the *Tech Support Status* is *Completed*. Select the **Download** button to download the files. At this point, even if the download happens to fail, it is deleted from the memory of the AP. This would happen if you don't allow pop-ups.



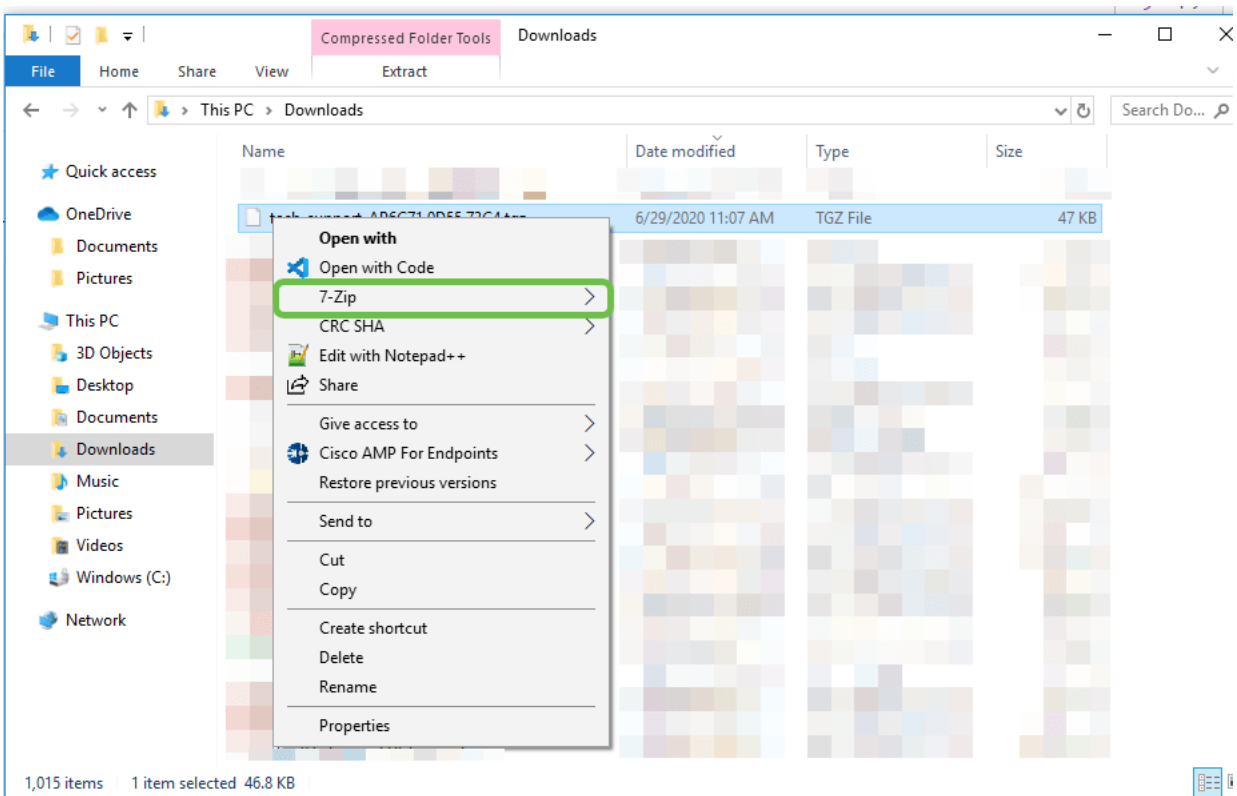
Step 4

In the *Download* folder of your computer files, you will see a tech support *.tgz* file. The files inside this folder need to be extracted.

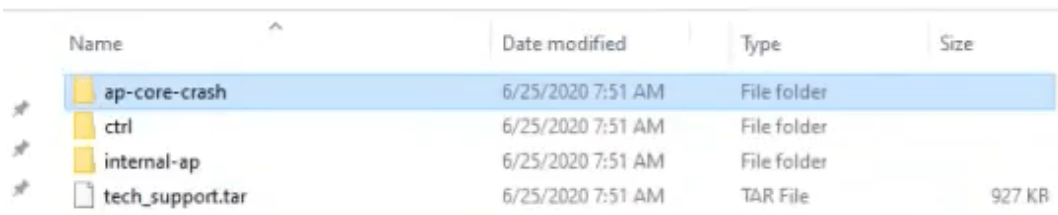


Step 5

Right-click and select the unzip application that you would like to use. In this example, *7-Zip* was used. Select to extract the files to the location you select. By default, the files are sent to the *Downloads* folder.

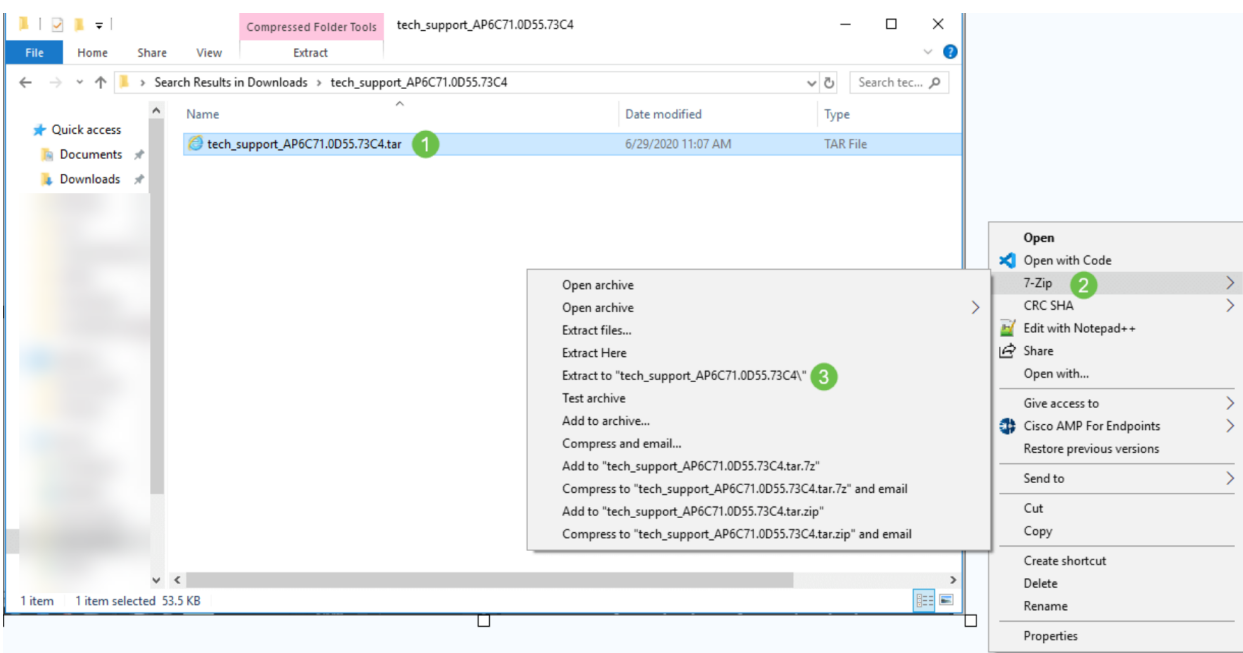


(Alternative View) If you have a core crash, you might see these folders instead.



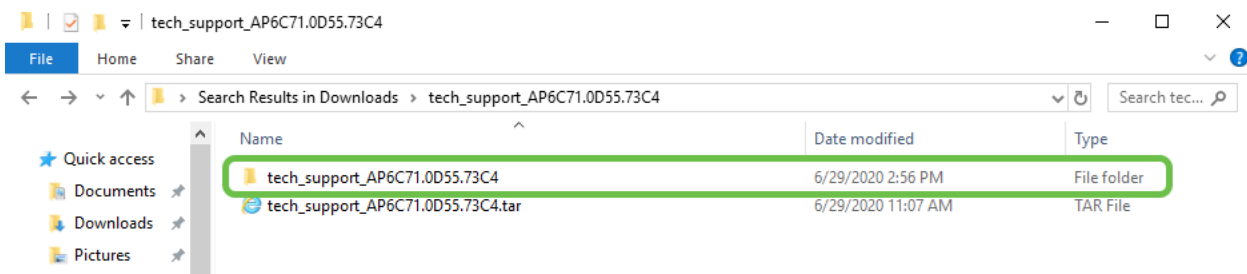
Step 6

Once the files have been extracted from the `.tgz` file, they will be in a `.tar` file. This file will need to be extracted again.



Step 7

You will see the `tech_support` folder. Double-click on the folder to open the files.



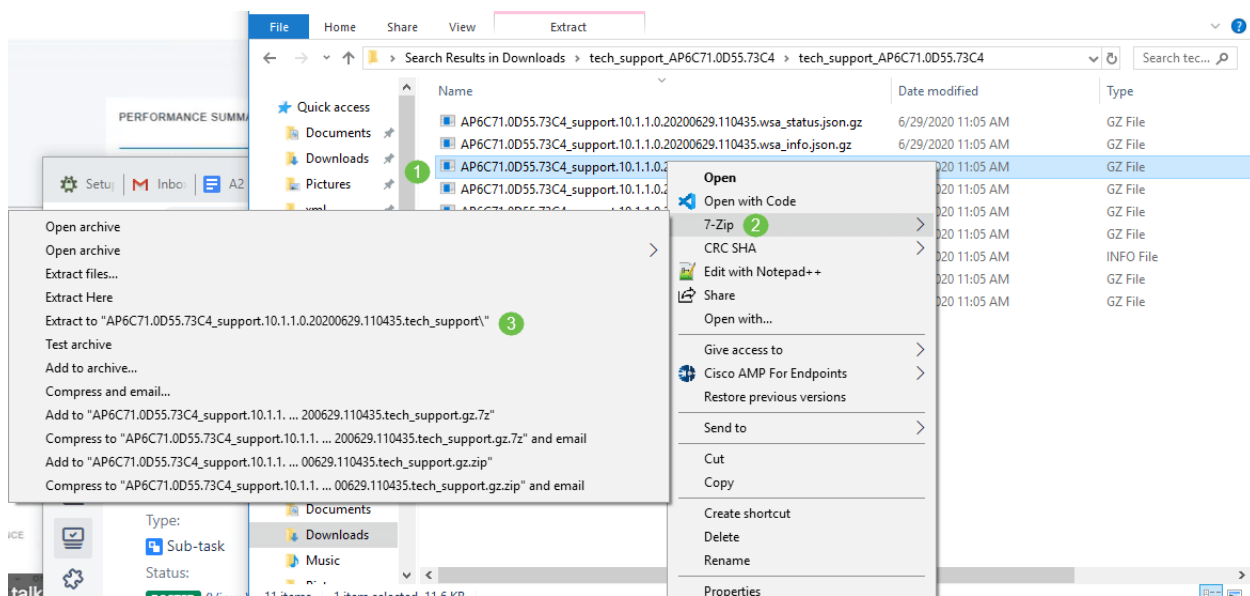
Step 8

Within the support bundle, the *cli_file* (configuration file), *msg/syslogs* (event logs), and *startlog* provide the most relevant information. The files you see may vary. An example is shown here.

Name	Date modified	Type
AP6C71.0D55.73C4_support.10.1.1.0.20200629.110435.wsa_status.json.gz	6/29/2020 11:05 AM	GZ File
AP6C71.0D55.73C4_support.10.1.1.0.20200629.110435.wsa_info.json.gz	6/29/2020 11:05 AM	GZ File
AP6C71.0D55.73C4_support.10.1.1.0.20200629.110435.tech_support.gz	6/29/2020 11:05 AM	GZ File
AP6C71.0D55.73C4_support.10.1.1.0.20200629.110435.syslogs.gz	6/29/2020 11:05 AM	GZ File
AP6C71.0D55.73C4_support.10.1.1.0.20200629.110435.startlog.gz	6/29/2020 11:05 AM	GZ File
AP6C71.0D55.73C4_support.10.1.1.0.20200629.110435.messages.gz	6/29/2020 11:05 AM	GZ File
AP6C71.0D55.73C4_support.10.1.1.0.20200629.110435.info	6/29/2020 11:05 AM	INFO File
AP6C71.0D55.73C4_support.10.1.1.0.20200629.110435.brain.log.gz	6/29/2020 11:05 AM	GZ File
AP6C71.0D55.73C4_support.10.1.1.0.20200629.110435.brain.error.log.gz	6/29/2020 11:05 AM	GZ File

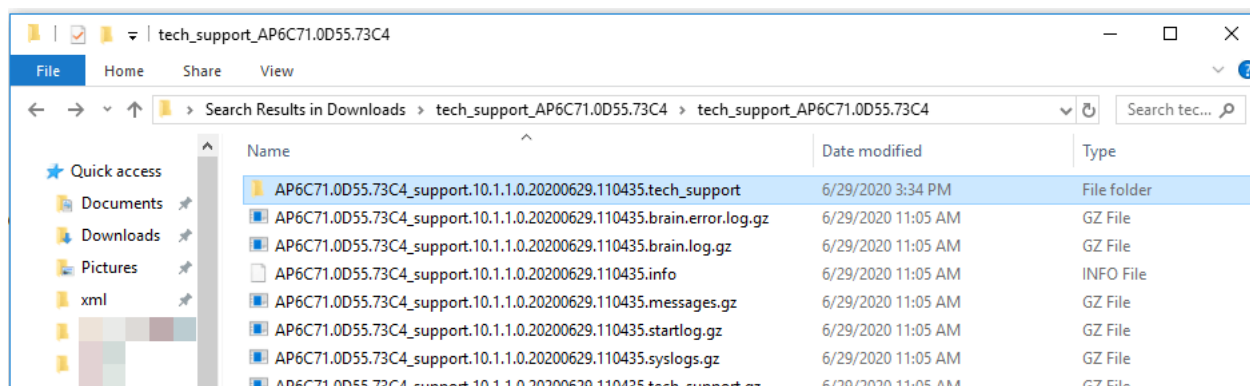
Step 9

Right-click on the file you would like to unzip. In this example, the file will be unzipped into a folder for *tech_support*.



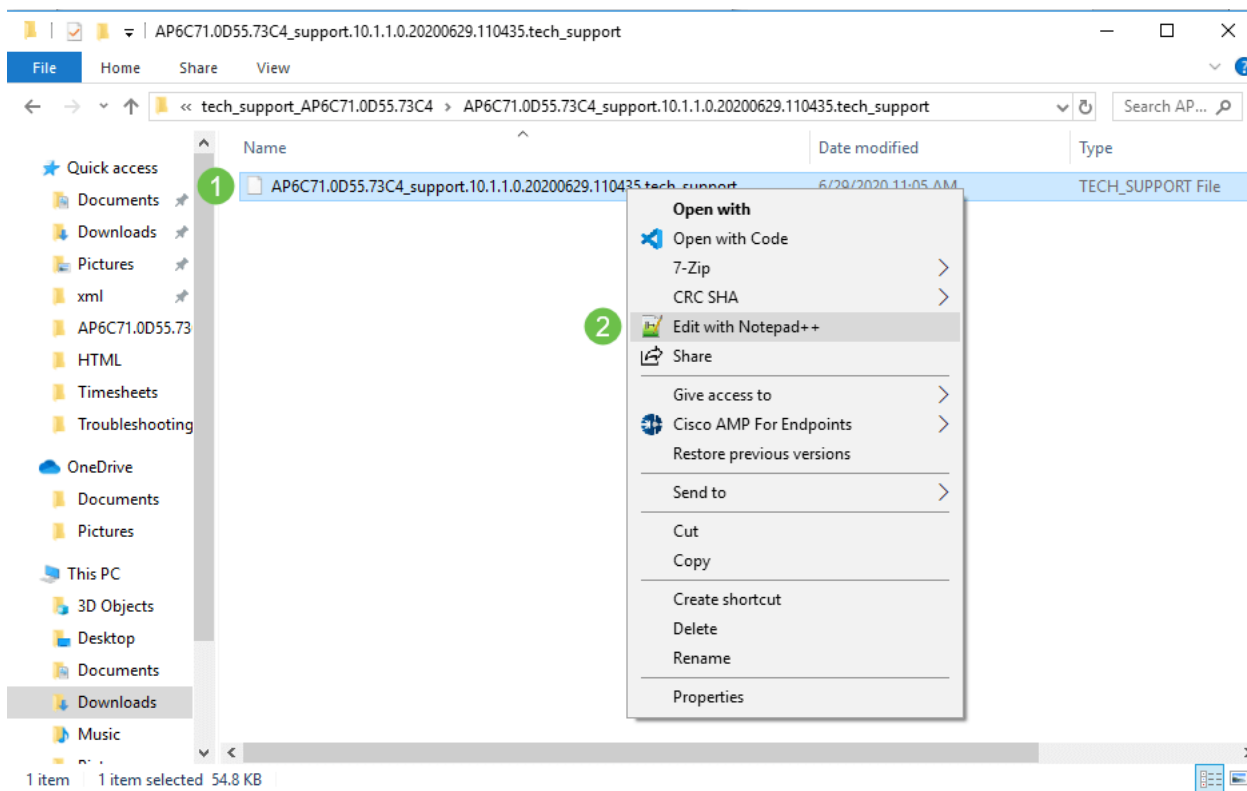
Step 10

The *tech_support* folder will appear. Double-click to open the folder.



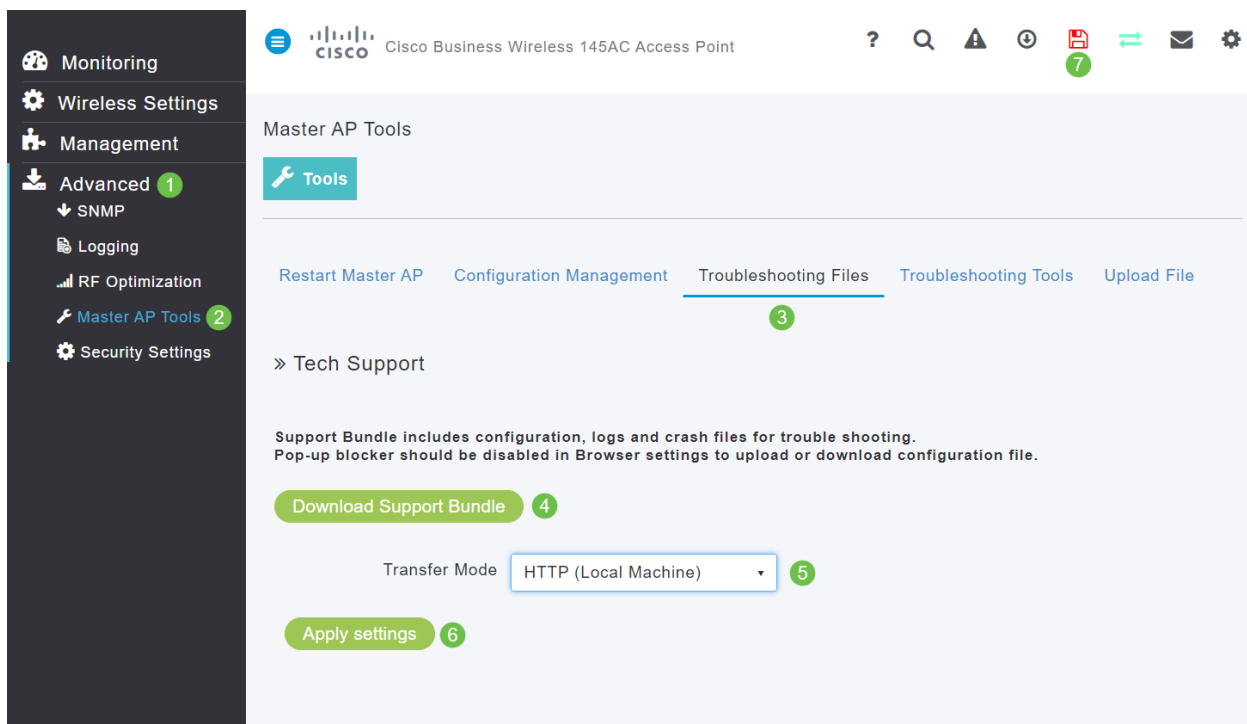
Step 11

Right-click on the file and select a text file reader. In this example, we used **Edit with Notepad++**.



Access to the Primary AP Tech Support Bundle

The Primary AP tech support bundle is the main source of diagnostics. To download the tech support bundle that is built into the Primary AP or the virtual controller bundle, navigate to **Advanced > Primary AP Tools**. Select the *Troubleshooting Files* tab. Select **Download Support Bundle**. For *Transfer Mode*, select *HTTP* or *FTP*. Click **Apply settings**. Click on the **Save** icon.



Adjust one of the CBW Mobile Phone Settings

Change the 802.11r settings on the CBW Network

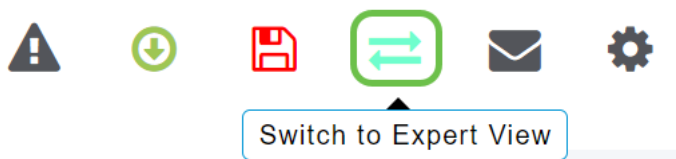
Step 1

Access the Web User Interface (UI) by entering the IP address of the Primary Access Point into a web browser. Make sure you are not on a Virtual Private Network (VPN) or this will not work. If you encounter security warnings, select the prompts to proceed.



Step 2

In the upper right-hand of the Web UI, click on the opposing arrows to switch to expert view.



Step 3

A pop-up window will appear, asking if you want to select expert view. Click **OK**.

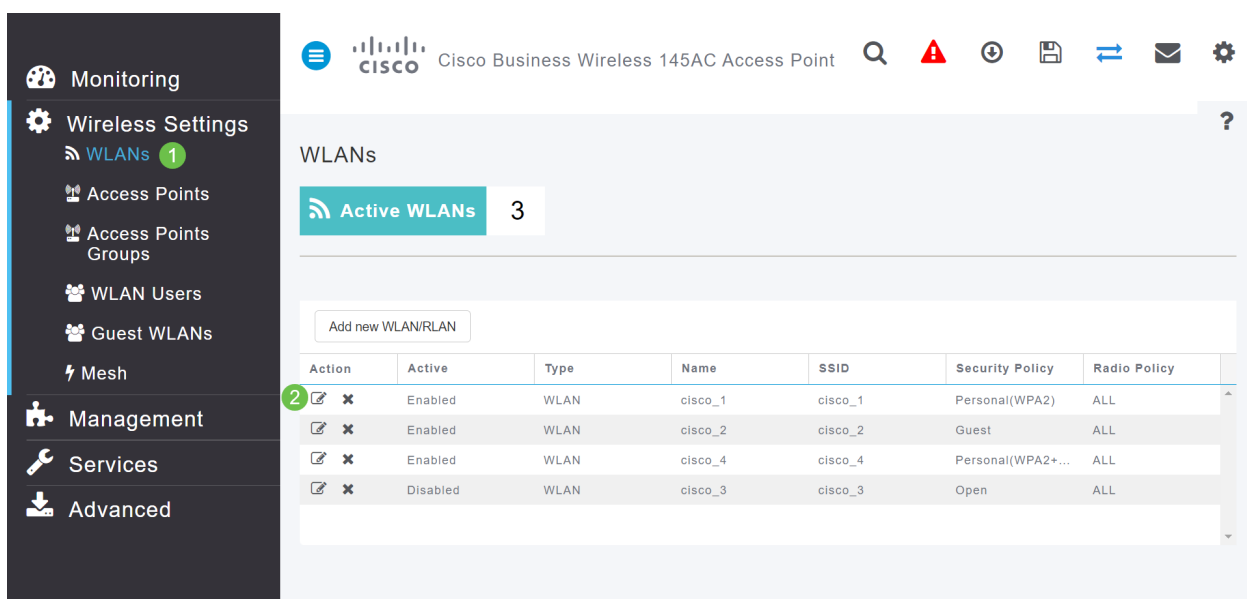
192.168.1.124 says

Do you want to select Expert View?



Step 4

Select **WLANs** and the **edit icon** for the WLAN you want to edit.



Monitoring

Wireless Settings

- WLANs 1
- Access Points
- Access Points Groups
- WLAN Users
- Guest WLANs
- Mesh

Management

Services









Advanced

Cisco Business Wireless 145AC Access Point

WLANs

Active WLANs 3

Add new WLAN/RLAN

Action	Active	Type	Name	SSID	Security Policy	Radio Policy
 	Enabled	WLAN	cisco_1	cisco_1	Personal(WPA2)	ALL
 	Enabled	WLAN	cisco_2	cisco_2	Guest	ALL
 	Enabled	WLAN	cisco_4	cisco_4	Personal(WPA2+...	ALL
 	Disabled	WLAN	cisco_3	cisco_3	Open	ALL

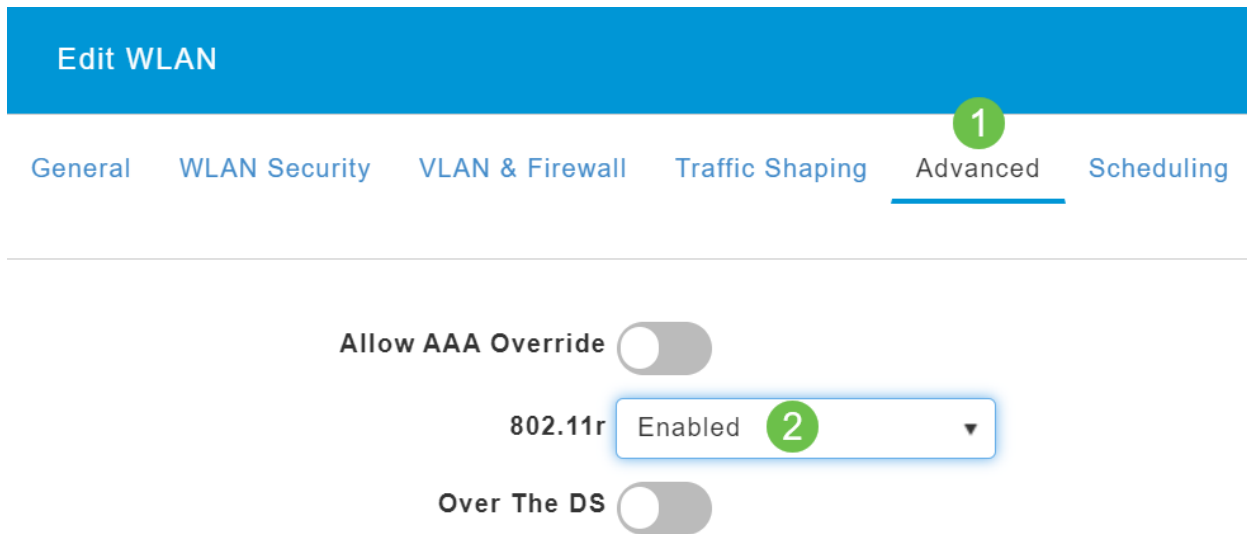
Step 5

A pop-up window will appear, asking if you want to continue. Click **Yes**.



Step 6

Click on the **Advanced** tab. Click on the drop-down menu for 802.11r and select **Enabled**.



Edit WLAN

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

Allow AAA Override

802.11r Enabled **2**

Over The DS

Step 7

Click **Apply**.



Step 8

To permanently save these settings, click the **save icon** on the top right of your screen.



If all else fails, reset to factory default settings

An option of last resort, that should only be done to remedy the most severe issues such as losing the ability to gain access to the management portal, is to perform a hardware reset on the router.

When you reset to factory default settings you lose all configurations. You will need to set up the router again from scratch so make sure you have the connection details.

The process on the new CBW APs is a little different than you may have experienced on other APs. For details on the reset, check out the article [Reset a CBW AP back to Factory Default Settings](#).

Conclusion

It was our intention to give you several different options for troubleshooting your mesh network. Mission accomplished! You should now have connectivity and can move on with your day.

[View a video related to this article...](#)

[Click here to view other Tech Talks from Cisco](#)