

Identifying Rogue Clients in a Cisco Business Wireless Network

Objective

The objective of this article is to show you how to identify rogue Access Points (APs) and rogue wireless clients in a Cisco Business Wireless (CBW) traditional or mesh network.

Applicable Devices | Firmware Version

- 140AC ([Data Sheet](#)) | 10.0.1.0 ([Download latest](#))
- 141ACM ([Data Sheet](#)) | 10.0.1.0 ([Download latest](#)) - extenders are only used in a mesh network
- 142ACM ([Data Sheet](#)) | 10.0.1.0 ([Download latest](#)) - extenders are only used in a mesh network
- 143ACM ([Data Sheet](#)) | 10.0.1.0 ([Download latest](#)) - extenders are only used in a mesh network
- 145AC ([Data Sheet](#)) | 10.0.1.0 ([Download latest](#))
- 240AC ([Data Sheet](#)) | 10.0.1.0 ([Download latest](#))
- 150AX ([Data Sheet](#)) | 10.3.2.0 ([Download latest](#))
- 151AXM ([Data Sheet](#)) | 10.3.2.0 ([Download latest](#))

CBW 15x series devices are not compatible with CBW 14x/240 series devices and coexistence on the same LAN is not supported.

Introduction

CBW Access Points (APs) are 802.11 a/b/g/n/ac (Wave 2) based, with internal antennas. They can be used as traditional standalone devices or as part of a mesh network.

In a perfect world, everyone would be respectful and honest when using your wireless network. Unfortunately, we don't live in a perfect world. As an administrator, your job is to be aware of any potential problems.

Rogue APs are APs that have been installed on a network without your permission. Rogue clients are any other detected devices that do not belong to your company.

These connections could be totally innocent, but there is always a risk that these rogues will attempt to attack your network or steal sensitive information. To keep on top of this, you can view the rogue APs and rogue clients. Once detected, these rogues cannot be blocked through the AP, but it does give you information to investigate further.

The CBW APs will only detect rogues on channels you are currently using or channels that overlap.


View Rogue APs

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>. 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](#)

Step 1

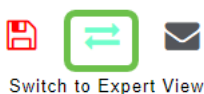
Log into the Web User Interface (UI) of the Primary AP. To do this, open a web browser and enter <https://ciscobusiness.cisco>. You may receive a warning before proceeding. Enter your credentials.

You can also access the Primary AP by entering <https://<ipaddress>> (of the Primary AP) into a web browser.

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

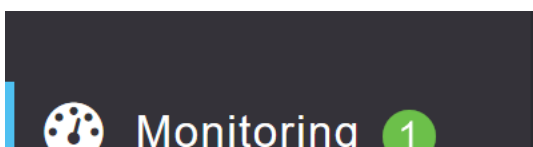
Step 2

To make these configurations, you need to be in *Expert View*. Click on the **arrow icon** on the top-right menu of the Web UI to switch to *Expert View*.



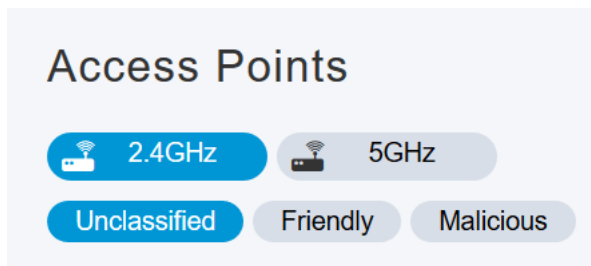
Step 3

Navigate to **Monitoring > Network Summary > Rogues > Access Points**.



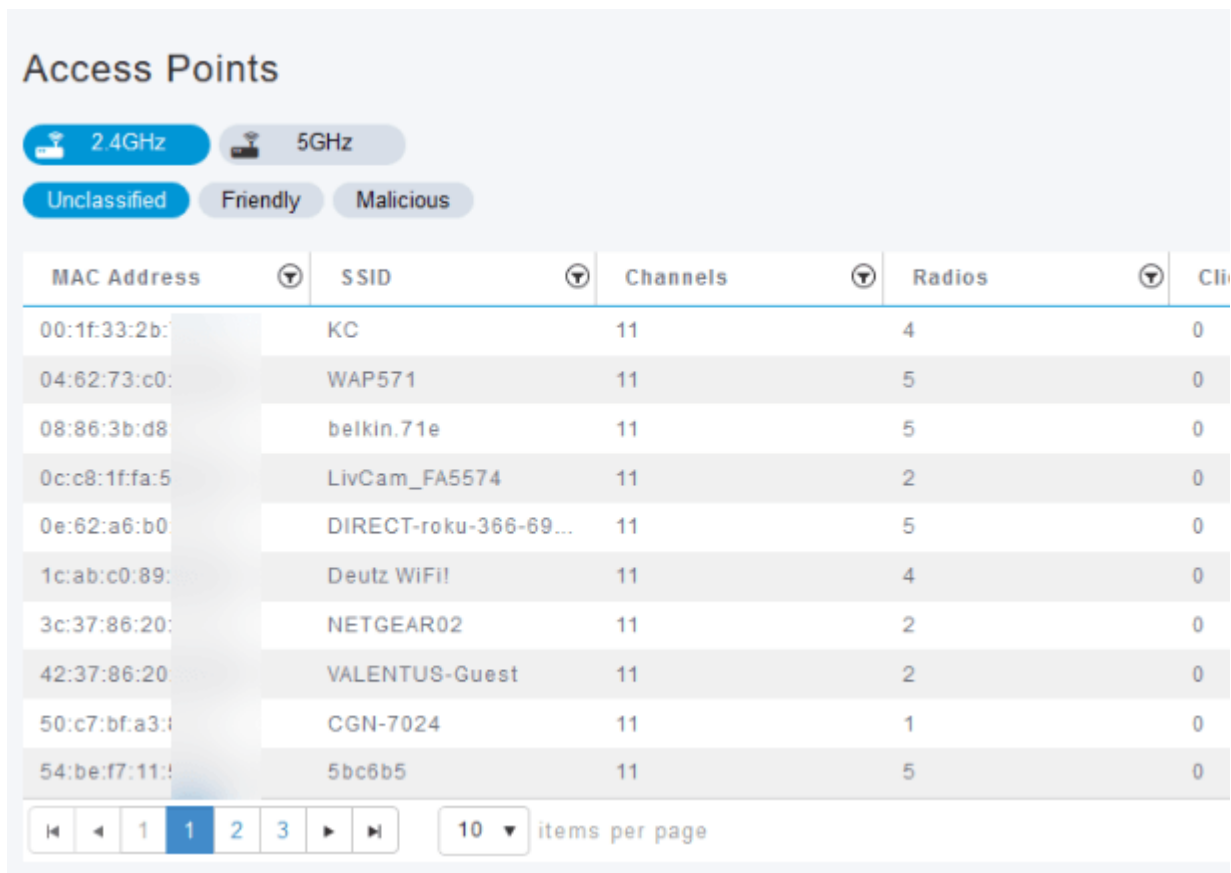
Step 4

Once this page opens, you can select to see 2.4 GHz or 5 GHz by clicking on the tab. By default, all rogue APs are labeled Unclassified. The AP does not change the labels for the rogue APs, that is something you would manually do.



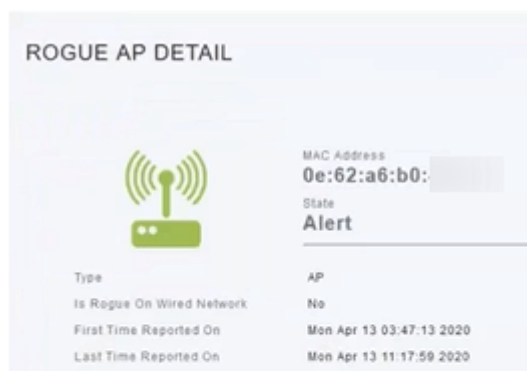
Step 5

The rogue APs are listed, you can click on any of them to investigate further.



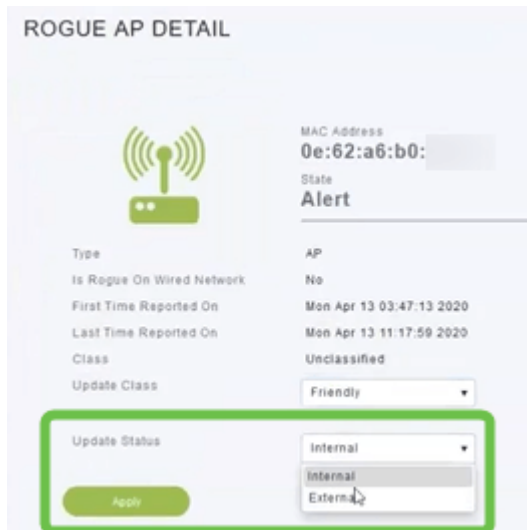
Step 6 (Optional)

If you want to classify any of the APs as *Friendly* or *Malicious*, you can select either option from the drop-down menu under *Update Class*. You might want to do this so that when you look at Unclassified Access Points in the future, you won't have to sort through an entire list. Be sure to click **Apply** when done.



Step 7 (Optional)

If you want to label an AP as *Internal* (in network) or *External* (possibly a neighboring company) you can do that under the *Update Status* section. Click **Apply** when done.



View Rogue Clients

Step 1

Log into the Web UI of the Primary AP. To do this, open a web browser and enter <https://ciscobusiness.cisco>. You may receive a warning before proceeding. Enter your credentials.

You can also access the Primary AP by entering <https://<ipaddress>> (of the Primary AP) into a web browser. For some actions, you can go us the Cisco Business Mobile app.

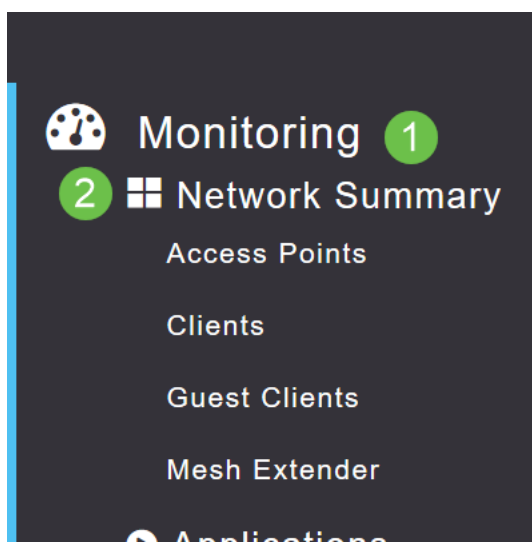
Step 2

To make these configurations, you need to be in *Expert View*. Click on the **arrow icon** on the top-right menu of the Web UI to switch to *Expert View*. For details on setting up a RADIUS server, check out [Radius](#)



Step 3

Navigate to **Monitoring > Network Summary > Rogues > Clients**.



Step 4

If there are any rogue clients, they will be listed. In this example, no rogue clients have been detected.

MAC Address	AP Mac	SSID	Radios	Last Seen	State	Wired
No items to display						

Conclusion

Now you have the ability to see rogues in your network. If you see a lot of rogues on a channel you are using, you can change the channel. There are considerations to keep in mind, so check out the change RF channel article (link when available).

[Frequently Asked Questions](#) [Radius](#) [Firmware Upgrade](#) [RLANs](#) [Application Profiling](#) [Client Profiling](#) [Primary AP Tools](#) [Umbrella](#) [WLAN Users](#) [Logging](#) [Traffic Shaping](#) [Rogues](#) [Interferers](#) [Configuration Management](#) [Port Configuration](#) [Mesh Mode](#) [Welcome to CBW Mesh Networking](#) [Guest Network using Email Authentication and RADIUS Accounting](#) [Troubleshooting Using a Draytek Router with CBW](#)