



Monitoring

This chapter contains the following sections:

- [About the Cisco Business Wireless AP Monitoring Service, on page 1](#)
- [Customizing the Network Summary View, on page 2](#)
- [Customizing Access Points Table View, on page 3](#)
- [Viewing Access Point Details, on page 4](#)
- [Viewing Client Details, on page 11](#)
- [Viewing Guest Client Details, on page 14](#)
- [Troubleshooting a Client, on page 15](#)
- [Viewing Mesh Extender, on page 16](#)
- [Viewing Applications, on page 17](#)
- [Viewing Rogue Access Points, on page 17](#)
- [Viewing Interferer Details, on page 19](#)
- [Wireless Dashboard, on page 19](#)
- [Customizing the Access Point Performance View, on page 21](#)
- [Customizing the Client Performance View, on page 22](#)

About the Cisco Business Wireless AP Monitoring Service

The Cisco Business Wireless AP Monitoring service enables the Primary AP to monitor the WLANs and all the connected devices on the network.

The **Monitoring** service offers the following capabilities through the **Network Summary** and **Wireless Dashboard** tabs:

- View details of configured WLANs.
- View list of top WLANs based on traffic and associated clients.
- View details of APs in the network.
- View details of clients operating actively at either 2.4 GHz or 5 GHz.
- View summary of client device, guest client device, operating systems and applications running on these devices.
- View a detailed list of rogue clients and APs.

- View details of various interferers in the network on the 2.4 GHz and 5 GHz radio frequencies.
- Monitor the performance of APs in the network.
- Monitor the performance of clients and guest clients in the network.

**Note**

- All the parameters on the **Network Summary** page are read-only parameters.
- This page is automatically refreshed every 30 seconds.

Customizing the Network Summary View

The **Network Summary** page lets you view data in a graphical format. You can customize the Network Summary view by adding or removing the widgets. The data displayed in various widgets can be viewed either in the doughnut view format or in the tabular view format by toggling the display icon on the top right of the individual widgets.

**Note**

Each of the action icons available within the widget is discussed in the [Using the Widgets](#) section.

The following widgets are displayed in the Network Summary page.

- **OPERATING SYSTEMS** (By clients)—Displays the OS information of the Clients (such as Linux clients, Android clients and so on) that are connected to the WLAN. For this feature, the user has to enable Local Profiling in the WLAN.
- **GUESTS** (By usage)—Displays the Top 10 guest clients in the network based on the throughput and usage.
- **ACCESS POINTS** (By usage)—Displays the Top 10 access points in the network based on the number of clients connected, usage and throughput.
- **APPLICATIONS** (By usage)—Displays the Top 10 applications such as gmail, youtube, facebook and so on based on usage level of the clients connected in the network. For this feature, the user has to enable the Application Visibility Control (AVC) option in the WLAN.
- **TOP WLANS** (By usage)—Displays the Top 10 WLANs in the network by usage and number of clients connected.
- **CLIENTS** (By usage)—Displays the Top 10 clients in the network based on throughput and usage.

Using the Widgets

This section details the various icons/options available within the widget to customize and view data as required.

- Use the **x** icon within a widget to remove the widget from the **Monitoring** page.
- Use the **+** icon on the top right to add the widget in the **Monitoring** page.

- Use the clear data (gear) icon to clear the usage data and reset to zero.
- Use the tabular (graphical) toggle icon and the tabulated list toggle icon to change the display of data between tabular view or doughnut view.
- Use the Save icon within a widget to export the top 10 entries locally in Excel format.



Note All entries will be exported for Guests widget.

Customizing Access Points Table View

Step 1 Navigate to **Monitoring > Network Summary > Access Points**.

Note You can also obtain high level details of the Access point by clicking on the count link in the **Access Points** summary section under **Monitoring > Network Summary** page.

Step 2 In the **Access Points** page, toggle between the **2.4GHz** and **5GHz** tabs to view a tabular listing of the access points operating at the respective radio frequencies. The following fields are displayed:

- AP Name**—Displays the name of the access point.
- Role**—Pictorial representation of the type of AP. A Primary AP is depicted with a (P) attached to the AP icon, a Mesh Extender is represented by an (E) attached to the AP icon and a Primary capable AP has no letter specified to the AP icon.
- Type**—Specifies if the AP is a Primary AP, Primary capable AP or a Mesh Extender.
- IP Address**—The IPv4 address of the device.
- Model**—Model of the CBW AP.
- Clients**—Number of client devices connected to the access point
- Usage**—The amount of data that has transferred between access point and the client device.
- Uptime**—Duration of how long the AP has been powered up.
- Admin Status**—Displays the configured status of 2.4GHz / 5GHz Radio is enabled or disabled.
- Operational Status**—Displays the running status of 2.4GHz / 5GHz Radio.
- Channel Utilization**—Level of traffic including data and interference over the channel that is assigned on the AP. Interference includes both Wi-Fi and non Wi-Fi signals. High utilization of channel, for example above 50%, suggests high level of interference including noise from nearby APs/clients/rogues on the same channel which results in poor client performance. The values are represented in % format.
- Throughput(Avg)**—This represents the amount of data that can be transferred from the access point to the client device.
- Channel**—Channel number at which the access point's radio is broadcasting the signal.
- Transmit Power (Avg)**—The logarithmic power level at which the access point is broadcasting the signal. The values are displayed in decibel-milliwatt (dBm) units.
- Coverage Hole**—Coverage holes are areas where clients cannot receive a signal from the wireless network. A coverage hole is considered to have occurred when client SNRs falls below -80dBm of data RSSI.
- Interference(Avg)**—RF interference involves unwanted, interference of RF signals that disrupt normal wireless operations, that creates potential network latency and poor client performance. Interfering RF signals includes both Wi-Fi and non-Wi-Fi signals. The values are represented in % format.

- q) **Noise**—Noise refers to any energy interference that degrades the quality of a wireless signal. Noise can affect everything from radio transmissions to network speeds. The values are displayed in decibel-milliwatt (dBm) units.
- r) **Rogues**—Any device that shares your channel and is not managed by your CBW network can be considered as a Rogue.
- s) **MAC Address**—The Unique physical address of the device.
- t) **Mode**—Displays if the device is in AP Only mode or Mesh mode.

Step 3 You can click the downward arrow on the top right of the column headers to customize the details displayed in the table. You may choose to hide, show or rearrange the desired columns, sort them in the order you wish or filter the table contents based on the desired parameters.

Viewing Access Point Details

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

Click on one of the Access Point to display the **Access Point View** page. This page consists of the following AP parameter details:

GENERAL

- **AP Name**—Displays the name of the access point.
- **Location**—The physical location of the access point.
- **MAC Address**—The Unique physical address of the device.
- **Base Radio MAC**—The Hardware (HW) address of 2.4 and 5GHz radios. (The address is same for both the radios).
- **IP Address**—The IPv4 address is a 32-bit number that uniquely identifies an access point.
- **CDP / LLDP**—The name and the port of the switch to which the access point is connected.



Note This field is applicable only for Primary capable APs. (Wired uplink APs).

- **Ethernet Speed**—Link speed capability of the switch port.
- **Model / Domain**—Model number of the access point / Radio domains.
- **Power Status**— Indicates the power level and mode of power.
- **Parent MAC Address**—Displays the Parent MAC address (AP to which it is connected wirelessly) This option is available only for Mesh Extenders.
- **Nearest APs**—Displays the top 3 neighbor APs with high link SNR value. For more information see **Link SNR (dBm)** in [Viewing Mesh Extender, on page 16](#).

This field is helpful for determining best location APs and Mesh extenders during installation. It would also help to troubleshoot connectivity issues.



Note The nearest AP field also displays Wireless Mesh Extenders.

- **Serial Number**— The unique number provided at the time of manufacturing.
- **Max Capabilities**—The radio domains, Spatial streams and maximum data rates of the access point.

TECH SUPPORT

You can download the support bundle for individual Access Points, which provides the AP boot-up logs and specifies the configurations applied.

To generate and download the bundle, use **Start** and **Download** in the Primary AP UI.

- **Start**—Click **Start** to start the bundle generation. By default, this button is enabled.
- **Download**—Click **Download** to save the bundle locally. This button will be enabled only after the bundle is generated.



Note The Pop-up blocker should be disabled in your Browser settings to download the tech support bundle for the AP.

The status of the bundle generation can be tracked by using the **Tech Support Status**.



Note Tech Support bundle can be generated for only one AP at a time.

Tech Support Status—The support bundle generation status can be viewed in this field. The status values can be one of the following:

- **Not started**—The bundle generation has not been triggered. This is the default status.
- **In Progress**—Bundle generation is in progress.
- **Completed**—The bundle generation is complete and can be downloaded using **Download**.

PERFORMANCE SUMMARY

This table provides the following details specific to the radios:

- **Number of clients**—The number of client devices connected to a specific Access Point.
- **Channel**—Channel number at which the access point's radio is broadcasting the signal.



Note Number of channels will be 1, 2 and 4 for 20MHz, 40MHz and 80 MHz respectively.

- **Configured Rate**—The default minimum and maximum data rates of the access point.

- **Usage Traffic**—The amount of data that has transferred between access point and the client device.
- **Throughput**—This represents the amount of data that can be transferred from the access point to the client device.
- **Transmit Power**—The logarithmic power level at which the access point is broadcasting the signal.
- **Noise**—Noise refers to any energy interference that degrades the quality of a wireless signal. Noise can affect everything from radio transmissions to network speeds.
- **Channel Utilization**—Level of traffic including data and interference over the channel that is assigned on the AP. Interference includes both Wi-Fi and non Wi-Fi signals. High utilization of channel, for example above 50%, suggests high level of interference including noise from nearby APs/clients/rogues on the same channel which results in poor client performance.
- **Interference**—RF interference involves unwanted, interference of RF signals that disrupt normal wireless operations, that creates potential network latency and poor client performance. Interfering RF signals includes both Wi-Fi and non-Wi-Fi signals.
- **Traffic**—Shows the data traffic in 2.4GHz and 5GHz radio.
- **Admin Status**—Status of the Radios for 2.4 GHz and 5 GHz.
- **Interferer Detection**—Status of Interferer detection for 2.4GHz and 5GHz radios.

{AP Name} DETAILS

This table provides the following details specific to the Access Point:

- **CLIENTS**—This table shows the client details that are connected to it. For per field details, refer to [Viewing Client Details, on page 11](#).
- **RF TROUBLESHOOT**—Displays a visual graphical representation of parameters that can affect the radio performance of the access points, such as:
 - **NEIGHBOR AND ROGUE APs**—Displays the Neighbor and Rogue APs on the current and adjacent channels for a given radio and the signal strength they are heard at. This visualization allows you to quickly identify Neighbor and Rogue APs that are causing interference and reducing the overall RF performance for the cell.
 - **CLEAN AIR INTERFERERS**—Displays the sources of non Wi-Fi interferers and their severity on the current and adjacent channels for a given radio. This visualization allows you to quickly identify non Wi-Fi sources of interference that are reducing the overall RF performance for the cell.
 - **CLIENT DISTRIBUTION ON TOP NEIGHBOR APs**—Displays the top 5 neighbor AP with signal strength greater than -70 dBm on the APs current client serving channel (2.4 GHz and 5GHz). Tx power and number of clients associated to this AP and its neighbor APs are shown. Number of clients is not available for neighbor APs on different Primary AP.
 - **CLIENT DISTRIBUTION BY DATA RATES**—Each client's throughput varies depending on the data rate it is using (802.11 a/b/n/ac) at any given point in time, and this data rate may vary every second. Various factors such as RSSI values, RF interference, etc. may affect a client device's instantaneous data rate.
- **SPECTRUM INTELLIGENCE**



Note By default Spectrum Intelligence (SI) is disabled in order to reduce the CPU cycles and increase the performance.

You can enable the SI for the radio using the following instructions:

Ensure that you enable the **Interferer detection** globally under **Advanced > RF Optimization**(in Expert View).

Navigate to **Wireless Settings > Access Points** and select an AP. Click **Edit** and choose either 2.4GHz or 5GHz radio.

- **ACTIVE INTERFERERS**—Displays the Active Interferers for Access point for the selected radio. For further details of the table refer Viewing Details of Interferers under Viewing Interferers.
- **NON WI-FI CHANNEL UTILIZATION**—Displays the Non Wi-fi Channel Utilization for the Access point of the selected radio.
- **INTERFERENCE POWER**—Shows the Interference Power for the Access point on the selected radio.

• TOOLS

This section in the UI consists of options to configure the LED states of the access points and also provides details of the image in the description table:

- **AP LED DISABLE**—To configure LED, refer to the [LED Display Settings](#).
- **BLINK AP LED**— The Blink AP LED function causes the LED to blink Red/Amber/Green for 60 seconds. This is used to identify the AP. To configure LED, refer to the [LED Display Settings](#).
- **RESTART AP**—You can reload AP if needed. The AP which acts as a Primary AP does not have this option.
- **INTERCHANGE IMAGE**—You can swap the primary version and backup version of the image. This will take effect only after the AP reloads.
- **FACTORY DEFAULT**—You can reset the AP to factory default settings if required. The AP which acts as a Primary AP does not have this option. To reset Primary AP to factory defaults refer to [Clearing the Primary AP Configuration and Resetting to Factory Defaults](#).
- **EXPORT CONFIG**—You can download the running configuration of the AP to .TXT file format. The configuration file is saved on the device in which the Primary AP UI is being viewed. By default the file is saved as AP<macaddress>_config.txt in your downloads folder. This option is available for the Primary AP and all the APs associated with the Primary AP.

The following mandatory configurations of an AP are exported, using which the AP can be restored even after a factory reset.

- **Information in AP Config File**

Table 1:

File Contents	Parameters
AP General Details	APModel, APLocation, APMODE, APRole, IPConfigMode (either DHCP or static), IsBridgeAP, NextPrimaryAP, IsPreferredPrimary
Radio Details	AdminStatus, ChannelWidth, Channel, TransmitPower, InterfererDetection
Mesh Mode detail	MeshRole (RAP or MAP), MeshBackhaulSlot, InstallMapping, BridgeType, BridgeGroupName, BackhaulInterface, StrictMatchBGN, PreferredParent, EthernetBridge, EthernetLinkStatus
Ethernet bridging VLANs	Name, Status, VlanTagging, NativeVlanId

Following is a sample of an AP Config file:

```

APModel: CBW240AC-H
APLocation: default location
APMode: 7
APRole: Root
IPConfigMode: 0
IsBridgeAP: 1
NextPrimaryAP: 00:00:00:00:00:00
IsPreferredPrimary 0
RogueDetectionStatus: 0
Radio0_AdminStatus: 1
Radio0_ChannelWidth: 20 MHz
Radio0_Channel: Automatic
Radio0_TransmitPower: Automatic
Radio0_InterfererDetection: 0
Radio1_AdminStatus: 1
Radio1_ChannelWidth: 80 MHz
Radio1_Channel: Automatic
Radio1_TransmitPower: Automatic
Radio1_InterfererDetection: 0
MeshRole: 1
MeshBackhaulSlot: 1
InstallMapping: 1
BridgeType: Indoor
BridgeGroupName: 00sasi
BackhaulInterface: 802.11a/n/ac
StrictMatchBGN: 0
EthernetBridge: 1
EthernetLinkStatus: UpDn
MeshInterfacel_Name: GigabitEthernet1
MeshInterfacel_Status: 0
MeshInterfacel_VlanTagging 1
MeshInterfacel_NativeVlanId 0

```

- **IMPORT CONFIG**—Using this option, you can upload the configuration file (in .TXT file format) of the AP. The configuration should match the AP model. This option is available for the Primary AP and all the APs associated with the Primary AP.

You can also track the status of the configuration file uploaded in the [TOOLS](#) section.



- Note**
1. Non Mesh Configuration file should not be imported to Mesh deployment APs.
 2. After uploading the configurations to the AP, it normally takes 1-2 minutes to take effect. You can also see the LED of the AP change from Solid/Blinking Green to Blinking Amber while applying the configurations and back to Blinking Green once the upload is complete.



Note The above **Export/Import Config** options added in the **Access Points** page is specific to a particular AP. If you want to change the configuration for the entire CBW network, refer to [Export and Import Primary AP Configuration](#).

• Description Table Details

Description Item	Status Meaning
Primary AP Primary Image	The default active image version of the Primary AP.
Primary AP Backup Image	The backup image version of the Primary AP.
AP Primary Image	The active image version of the access point.
AP Backup image	The backup image version of the access point.
Predownload status	If the access point is going for an software update the corresponding predownload status is displayed.
Predownloaded version	Version of the predownloaded image during software upgrade process.

• PACKET CAPTURE

Using this option, you can capture the packets in the specified interface and for the specified protocol. Packet capture is supported on Wired Interfaces as well as the internal Primary AP interface responsible for communication between management functions and access points. Supported protocols are IP, TCP, and UDP. This option is available only in **Expert View**.

The following are the configurations required for starting the capture,

- **INTERFACE** – Choose whether the capture should be taken in Wired interface or Primary AP interface



Note Primary AP interface is available only for the AP acting as Primary AP.

- **WIRED INTERFACE** – Select the required Ethernet port. Based on the AP model, supported wired interfaces will be populated automatically.

CBW Model	No. of Ethernet Ports
CBW140AC	1
CBW240AC	2
CBW145AC	4
CBW141ACM	4
CBW142ACM	0
CBW143ACM	1

- **PROTOCOL** – Select the required protocol for starting the capture. Supported protocols are IP, UDP, and TCP.
- **START/STOP** – Button to Start/Stop the capture for the configured Interface and protocol.
- **DOWNLOAD** – Once the capture is stopped, the pcap file will be ready for download. By clicking on the Download button, the PCAP file will be saved to the local machine. By default, the PCAP file is saved as *AP<macaddress>_capture.pcap*.
You can also view the status of capture on top of the pane.



Note

- CBW142ACM does not support packet capture feature as it does not have Ethernet ports
 - The “Primary AP” capture will be visible only for AP which is currently acting as the Primary AP
 - The Wired0 interface of CBW141ACM is mapped to LAN4 Port
-

• Limitations:

- The maximum allowed pcap size is 5MB, after which the ongoing capture automatically stops and the pcap file can be downloaded locally by clicking on the Download button.
- Only one capture is allowed to run in single point of time. If the user is attempting to start the capture in one AP while the capture is in progress on other AP, a warning message will be displayed in CBW UI.

• SYSLOG

Using this option, you can collect per AP logs by configuring the Syslog server IP, and logging level for individual APs.

- **SYSLOG SERVER IP** – IP Address of the Syslog Server running in the network.
- **LOG SYSLOG LEVEL** – Sets the Logging level up to which the logs would be sent to the Syslog Server. By default, the log syslog level is set to **Notifications (5)**.

The available logging levels:

- **Emergencies (0)**
- **Alerts (1)**
- **Critical (2)**
- **Errors (3)**
- **Warnings (4)**
- **Notifications (5) (Default)**
- **Informational (6)**
- **Debugging (7)**

Messages with a severity equal to or less than the set level are sent to the syslog server.

- **LOGGING** – Option to Enable/disable the Logging for individual AP. By default, the logging is **Disabled**. If the logging is enabled, the syslog messages will be sent to the configured Syslog server else the messages will not be sent to the Syslog Server.



Note

- This configuration is available for all APs (Mesh Extenders, Primary AP, Primary Capable APs).
 - Syslog Server IP configured for each AP can be same/different.
 - By default, Syslog Server IP would be configured as broadcast (255.255.255.255). The Level will be set to Notifications.
 - To capture the Primary AP logs:
 - Configure the Syslog Server details under **Advanced > Logging > Add Syslog Server**.
 - Set the Logging level under **Advanced > Logging > Log Syslog Level**.
-

Viewing Client Details

Step 1 Click **Monitoring>Network Summary**.

A summary of all active clients is displayed in the **Active Clients** summary section. These clients are either 802.11b/g/n clients operating at 2.4 GHz or 802.11a/n/ac clients operating at 5 GHz.

Note You can also view this page by navigating via **Monitoring>Network SummaryClients**.

Step 2 In the **Active Clients** summary section, click the count display icon to view high-level details of the client device or navigate to **Monitoring>Network SummaryClients**. This section will give you an overview of the connected clients and its parameters as explained below:

In the **Clients** page, there are three upper blocks that list the following details:

- **Clients**—This tile displays the total number of clients connected.
- **Wireless**—This tile displays the number of clients specific to 2.4 GHz and 5 GHz radio.
- **Apple**—This tile is specific to the Apple Clients. Specifies the number of clients.
 - **Fastlane**—This tile displays the number of fastlane using clients. Fastlane allows iOS apps connected to CBW access points to be prioritized. This means your voice, video and real-time data gets to be first in line. To enable Fastlane go to **Wireless Settings>WLANs>Add/edit WLAN>Traffic Shaping>Fastlane**.
 - **Analytics**—This tile displays the number of Analytics capable clients.

Click on the required client from the list in the table displayed to view the per client details. The following details are displayed:

Client Details Table

You can click the downward arrow on the top right of the column headers to customize the details displayed in the table. You may choose to hide, show or rearrange the desired columns, sort them in the order you wish or filter the table contents based on the desired parameters.

- **User Name**—The user name of the client connected to the Primary AP (Default: Unknown).
- **IPv4 Address**— The IPv4 address is a 32-bit number that uniquely identifies the client device.
- **AP Name**—The configured AP name to which the client associated will be displayed in this column.
- **Protocol**—The WiFi standard through which the client is connected. It can be 802.11a/b/g/n/ac.
- **Hostname**—The MAC address of the client is displayed by default. Enable **Wireless Settings>Add/Edit WLAN>Local Profiling** to view the hostname of the clients supported.
- **Client Type**—The Capable Client's operating systems will be displayed in this column as Android, Apple-Device etc.
- **Connection Speed**—The maximum data rate strength of the client connected to the access point. The values are displayed in units of Mbps.
- **Status**—The active status of the client.
- **Signal Quality**—Signal quality is a value ranging from 0 to 100 dB. This includes, the noise generated by interference sources and the signal strength.
- **Signal Strength**—Signal strength is the wireless signal power level received by the wireless client. Strong signal strength results in more reliable connections and higher speeds. Signal strength is represented in -dBm format, ranges from 0 to -100dBm. The closer the value to 0, the stronger the signal.
- **Usage**—The amount of data consumed by the client.
- **WLAN SSID**—Shows to which SSID the client has connected.
- **Uptime**—The duration of how long the client is connected to the access point.
- **Mac Address**—The MAC(Hardware) address of the client connected.
- **Frequency Bandwidth**—The radio on which the client is connected 2.4 GHz or 5 GHz.
- **WLAN Profile**—The profile name of the configured WLAN to which the client is connected.

- AP MAC—Radio MAC address of the corresponding access point to which the client is connected.
- AP Group—This column shows the access points groups to which it is configured.
- IPv6 Address—This is the IPv6 address of the client device.

Client View

Select a required client from the list displayed to view the following details:

• GENERAL

- User Name—The user name of the client connected to the Primary AP (Default: Unknown).
 - Hostname—The MAC address of the client is displayed by default. Enable **Wireless Settings > Add/Edit WLAN > Local Profiling** to view the hostname of the clients supported.
 - MAC Address—The MAC(Hardware) address of the client connected.
 - Deauthenticate—Click this option to disconnect the client.

Note Deauthenticating the client removes a client from the WLAN, but that client will be able to rejoin unless their MAC address is added to the Blocklist.

To block the client permanently, navigate to **Wireless Settings > WLAN Users > Local MAC Addresses**, click **Add MAC address**, select **Blocklist** as the type and hit **Apply & Save**.
 - Uptime—The duration of how long the client is connected to the access point.
 - SSID—Shows to which SSID the client has connected.
 - AP Name—The configured AP name to which the client is associated. The AP name along with the location can be configured by navigating to **Wireless Settings > Access Points**.
 - Nearest APs—List of AP names nearer to the client based on signal strength.
 - Device Type—The Capable Client's operating systems will be displayed in this column as Android, Apple-Device etc,
 - Performance—This shows the Signal Strength, Signal Quality, Connection Speed, Channel Width.
 - Capabilities—This gives information on which domain the client is associated to the AP and its Spatial Stream.
 - Cisco Compatible—Cisco Compatible state changes only when a Cisco client (which supports CCX extensions of the IEEE standards) get associated to your access point.
 - Client connection score—Connection score is the percentage based connection quality between client and the access point. It denotes the current client data transfer speed. Higher the percentage, the faster and higher the data transferred. This value is based on the Client Actual Rate divided by either the Client Max Capability or Max AP Configured (whichever is lower).
- CONNECTIVITY GRAPHIC—This line graph represents the stages and current status of the associated client as Start, Association, Authentication, DHCP, and Online.
 - TOP APPLICATIONS—The top applications that are being used by the client device is presented in a graphical or tabular format. To utilize this, the user must enable AVC in **Wireless Settings > WLANs > Add/Edit WLAN > Traffic Shaping > Application Visibility Control**.

Note Ensure that the Application Visibility Control (AVC) is active under WLAN settings to view this data.

- **MOBILITY STATE**—This shows the graphical flowchart of stages on how the client is connected to the Primary AP.
 - Name of the Primary AP, with its IP address and the model number of the AP on which it is running.
 - Name of the AP with which the client is connected to the Primary AP, the AP's IP address, and the AP's model number.
 - Nature of connection between the AP and the client. For example, wireless 802.11n 5 GHz connection.
 - Name of the client, type of client (such as Microsoft Workstation), VLAN ID of the client, and the client's IP address.
- **NETWORK & QOS** —This shows client capability of some IEEE standards and user configured parameters such as IP address, VLAN, Source Group Tag, Fastlan Client, Mobility Role, WMM, U-APSD and QoS Level.
- **SECURITY & POLICY**—This table shows the encryption type and security policies on which the client is associated to the access point such as Policy (WPA2 or WPA3), Cipher, Key Management, EAP Type, ACL, mDNS, and AAA Role.

Viewing Guest Client Details

The clients that are connected to the **Guest WLANs** are known as **Guest Clients**. To obtain Guest WLANs the Primary AP provides guest user access on WLANs which are specifically designated for use by guest users. The concept of creating Guest WLANs is discussed in the later chapters.

Step 1 Click **Monitoring > Network Summary > Guest Clients**.

A summary of all active guest clients is displayed in the **Guest Clients** summary section. These clients are either 802.11b/g/n clients operating at 2.4 GHz or 802.11a/n/ac clients operating at 5 GHz.

Step 2 In the **Guest Client** page, the summary blocks display the number of guest clients and recently connected clients to the Primary AP. Each guest client detail can be viewed by clicking the specific client record.

In the **Guest Clients** page, there are two upper blocks that list the following details:

- **Guest Clients / Recent Clients**—Specifies the total number of guest clients and recent clients connected.
- **Wireless**—Specifies the number of 802.11b/g/n guest clients connected and operating either at 2.4 GHz or 5 GHz.

Click on the required guest client from the list in the table displayed to view the per guest client details. For a description of the parameters displayed for a specific guest client, refer to [Viewing Client Details](#):

Step 3 You can click the downward arrow on the top right of the column headers to customize the details displayed in the table. You may choose to hide, show or rearrange the desired columns, sort them in the order you wish or filter the table contents based on the desired parameters.

- Note** The clients connected to Guest WLANs are considered to be Guest Clients.
- You can export details of all the guest clients connected to the CBW network and download in Excel format using the **save** icon in the **Guest Widget**.
-

Troubleshooting a Client

This section describes in detail how to perform a client ping test and a connection test. These help to effectively investigate and troubleshoot connection issues.

To troubleshoot wireless client joining issues, set the **Logging level** as **Notifications (5)** and check the logs in the Primary AP UI under **Management > Logging**.

Performing a Client Ping Test

You can perform a ping test on the client to determine the latency or delay between the Primary AP and the client. This is an Internet Control Message Protocol (ICMP) based test. Using the ping test you can know the connectivity as well as the latency between the Primary AP and the client.

Click **Start** to begin the test. The latency in milliseconds is represented graphically.

Performing a Connection Test

You may choose to perform a Connection test when the client fails to connect to a particular WLAN. This test takes about three minutes. Attempting to connect during the three minute test period will generate diagnostic information to aid in troubleshooting connection issues.

-
- Step 1** Go to **Monitoring > Network Summary > Clients**.
 - Step 2** Click on the client MAC address that you want to debug from the list of clients that are available.
 - Step 3** Scroll down to the **Client Test** and in the **Connection** tab click **Start**.
 - Step 4** Now disconnect the client from the WLAN and try re-connecting.
 - Step 5** The result at each stage of client connection establishment with the WLAN is displayed.
-

Generating an Event Log

The user may choose to perform a complete debug session by enabling the **Event Log** feature that is available in the per client view tab. The Event Log testing contains the time-stamp and message details that are exchanged between the client and the access point. The message type helps to analyze and conclude if a client is able to successfully join a WLAN or a reason for its failure in joining a particular WLAN.

-
- Step 1** Go to **Monitoring > Network Summary > Clients**.
 - Step 2** Click on the client MAC that you want to debug.

Step 3 Scroll down to the **Client Test** and in the **Event Log** tab, click on the **Start** option.

Step 4 Now, disconnect the client from the WLAN and try to re-connect it again.

Step 5 You can also save the results, by selecting the **Save to Disk** option in the Primary AP UI. Following is a sample output displayed when you generate an event log:

The screenshot shows the 'EVENT LOG' tab in a monitoring interface. At the top, there are three buttons: 'Start', 'Stop', and 'Save To Disk'. Below the buttons is a table with the following columns: Time Stamp, Module, Severity, Message Type, Message Subtype, and Details. The table contains 18 rows of event data.

Time Stamp	Module	Severity	Message Type	Message Subtype	Details
Mon Dec 09 201...	Dot11	INFO	ASSOC_REQ	MESSAGE_RECEIVED	None
Mon Dec 09 201...	Dot11	INFO	ASSOC_REQ	INVALID_RSN_IE	None
Mon Dec 09 201...	PEM	INFO	PEM_EVENT_MSG	WLAN_SUPPORTS_STATIC_DYNAMIC_W...	None
Mon Dec 09 201...	PEM	INFO	PEM_EVENT_MSG	IP_ACQUIRED_AND_AUTH_NOT_REQ_O...	None
Mon Dec 09 201...	Dot11	INFO	ASSOC_REQ	CLIENT_MOVED_TO_ASSOCIATED_STATE	None
Mon Dec 09 201...	Dot11	ERROR	AUTH_DOT1X	WLAN_REQUIRES_802_1X_AUTH	None
Mon Dec 09 201...	PEM	INFO	PEM_EVENT_MSG	WEB_AUTH_MAX_RETRY_EXCEEDED	None
Mon Dec 09 201...	PEM	INFO	PEM_EVENT_MSG	WEB_AUTH_SUCCESS	None
Mon Dec 09 201...	Dot11	INFO	ASSOC_REQ	MESSAGE_RECEIVED	None
Mon Dec 09 201...	Dot11	INFO	ASSOC_REQ	INVALID_RSN_IE	None
Mon Dec 09 201...	PEM	INFO	PEM_EVENT_MSG	WLAN_SUPPORTS_STATIC_DYNAMIC_W...	None
Mon Dec 09 201...	PEM	INFO	PEM_EVENT_MSG	IP_ACQUIRED_AND_AUTH_NOT_REQ_O...	None
Mon Dec 09 201...	Dot11	INFO	ASSOC_REQ	CLIENT_MOVED_TO_ASSOCIATED_STATE	None
Mon Dec 09 201...	Dot11	ERROR	AUTH_DOT1X	WLAN_REQUIRES_802_1X_AUTH	None
Mon Dec 09 201...	PEM	INFO	PEM_EVENT_MSG	WEB_AUTH_MAX_RETRY_EXCEEDED	None

Viewing Mesh Extender

Step 1 Navigate to **Monitoring > Network Summary > Mesh Extender**.

Step 2 In the **Mesh Extender** page, you can view the following details of the Mesh Extenders:

- **AP name**—Displays name of the Mesh Extender.
- **AP Model**—Displays the model of Mesh Extender.
- **Ethernet MAC**—Displays the Hardware MAC of the Mesh Extender.
- **Parent AP Name**—Displays the AP name to which the Mesh Extender has joined wirelessly.
- **Hop**—Displays the count of how far the Mesh Extender is operating from the Primary AP.
- **Link SNR (dBm)**— It's the signal to noise ratio calculated between the Mesh Extender and the Parent AP (to which the Mesh has joined).
- **Channel Utilization (%)**—Level of traffic including data and interference over the channel that is assigned on the AP. The values are represented in % format.
- **Channel**—Channel number at which the Mesh Extender's radio is operating.
- **Clients**—Total number of clients connected to this Mesh Extender.

Note Only devices operating in Mesh Extender Mode are displayed in the table.

Viewing Applications

Click the **Applications** menu to view the Top 10 application usage in the client traffic. This can be seen when you enable the Application Visibility Control (AVC) option in at least one WLAN. Navigate to **Wireless Settings > WLANs > Add/Edit WLAN > Traffic Shaping > Application visibility Control** to view.

Viewing Rogue Access Points

Any device that shares your channel and is not managed by you can be considered as a **Rogue**. This includes Rogue Access Points, Wireless Routers and Rogue clients. CBW APs have the in-built intelligence to detect rogue devices in both 2.4GHz and 5GHz radios.

The Rogue AP and Rogue Client Detection is **Disabled** on CBW APs by default. To enable Rogue Client Detection:

1. Navigate to **Wireless Settings > Access Points**.
2. Click the edit icon next to the AP you want change.
3. Click the **Rogue Detection** toggle button in the **General** tab.
4. Click **Apply** to save and exit.

After applying the changes, the Rogue detection will be enabled, and the Rogue APs will be reported to Primary AP.

You can view the following details of rogue devices which includes unmanaged neighboring Clients and Access Points.

- **MAC Address**—Rogue AP MAC address.
- **SSID**—The name of the SSID, which the Rogue AP is broadcasting.
- **Channels**—The channel in which the Rogue AP is operating.
- **Detecting AP Counts**—Displays the number of APs in which the Rogue AP is detected.
- **Clients**—Number of clients connected to the Rogue AP.
- **Class**—The class of the Rogue AP. By default, all the Rogue APs are unclassified. You can change the class of Rogue APs as **Friendly**, or **Malicious**.

Following are the classes that are supported by the CBW:

Class	Description
Unclassified	The CBW AP discovers all the Rogue APs and marks them under the Unclassified class by default. Also, the status of the Rogue AP remains as Alert since it remains unknown to the CBW network.

Class	Description
Friendly	<p>You can move the Rogue AP to a Friendly state if you know the Rogue APs MAC.</p> <p>Following are the options that are configurable:</p> <ul style="list-style-type: none"> • Internal—If the unknown access point is inside the network and poses no threat to WLAN security, you would manually configure it as Friendly, Internal. Example: An access point that exists within your premises. • External—If the unknown access point is outside the network and poses no threat to WLAN security, you would manually configure it as Friendly, External. Example: An access point that belongs to a neighboring coffee shop.
Malicious	<p>You can move the Rogue AP to Malicious class when you do not know the particulars of the AP. By default, the status remains as Alert since it remains unknown to the CBW network.</p>

- **State**—Displays the state of the Rogue AP. If the Rogue AP class is **friendly**, the state will be **Internal** or **External**, else the state will be **Alert**.

Configuring the Rogue AP States

-
- Step 1** Click **Monitoring > Network Summary**
 - Step 2** In the **Rogues** tab, click on the **Access Points**.
 - Step 3** Click on one of the available Rogue APs that is detected by the CBW.
 - Step 4** In the **Update class** drop-down list box, select the appropriate class.
 - Step 5** Select the class as **Friendly** to configure the status as **Internal** or **External**.
 - Step 6** If you specify the AP as **Malicious** class, then the status of the AP remains as **Alert**.
 - Step 7** You can also move an AP from one state (such as **Friendly**) to another (such as **Malicious**) by selecting the AP from the specific tabs.
 - Step 8** Click **Apply** to save the changes.
-

Viewing Rogue Client Details

-
- Step 1** Navigate to **Monitoring > Rogues > Clients** in **Expert View**.
 - Step 2** Clients that are associated to Rogue APs are displayed along with the following details:
 - **MAC address**—Rogue client's MAC address.
 - **AP MAC**—MAC address of the AP to which the Rogue client is connected.

- **SSID**—Displays to which SSID the client is connected.
 - **Detecting AP Counts**—Displays the number of APs in which the Rogue Client is detected.
 - **Last Seen**—Shows the time at which the Rogue client is detected.
 - **State**—Displays the state of the Rogue client.
 - **Wired**—Specifies if the detected Rogue client is Wired or Wireless.
-

Viewing Interferer Details

Interferers are non-Wi-Fi devices that cause disruption to your Wireless network. They may either be operating at 2.4 GHz or at 5 GHz. To view these devices, do the following:

Step 1 Click **Monitoring > Network Summary > Interferers**.

A summary of all non-Wi-Fi interfering devices is displayed in the **Interferers** summary window. These interferers may either be operating at 2.4 GHz or at 5 GHz.

Step 2 In the **Interferers** summary window, click the count display icon. The following details are displayed.

- **AP Name**—The name of the access point where the interference device is detected.
 - **Radio Slot**—Slot where the radio is installed.
 - **Interferer Type**—Type of the interferers such as Microwave Oven, Jammer, WiMax Mobile, and so on
 - **Affected Channel**—Channel that the device affects.
 - **Detected Time**—Time at which the interference was detected.
 - **Severity**—Severity index of the interfering device.
 - **Duty Cycle (%)**—Proportion of time during which the interfering device was active.
 - **RSSI**—Receive signal strength indicator (RSSI) of the access point.
 - **Dev ID**—Device identification number that uniquely identified the interfering device.
 - **Cluster ID**—Cluster identification number that is unique which identifies the type of the device.
-

Wireless Dashboard

This page displays the capabilities of AP and the Client for 2.4 GHz and 5 GHz. You can click the **Close Widget (X)** icon on the top right of the following widgets that you want to remove. You may add the closed widget again by clicking the + icon if you wish.

AP CAPABILITY

Displays the capability details for the APs managed by the Primary AP:

- **Max Configured Connection Rates:** Displays the graph and table for maximum configured connection rate in Mbps, mapped to different ranges, for each of the radios (2.4 GHz and 5GHz) for all the APs configured by the Primary AP.
- **AP Distribution by Channel Width:** Displays the graph and table for the maximum configured Channel Width for all the APs configured by the Primary AP.

CLIENT CAPABILITY

Displays the capability data for the clients managed by the Primary AP:

- **Client Capability by Spatial Stream:** Displays the graph and table for the number of clients capable of a particular spatial stream for all the clients connected to the Primary AP.
- **Client Capability by Max Protocol:** Displays the graph and table for the number of client based on the maximum data rate protocol supported for all the clients connected to the Primary AP.

AP PERFORMANCE-CHANNEL UTILISATION

Display the Performance details for the APs managed by the Primary AP:

- **Channel Utilization :** Displays the graph and table for the channel utilization as a percentage, mapped to different ranges, for each of the radios(2.4 GHz and 5GHz) for all the APs configured by the Primary AP.

CLIENT PERFORMANCE

Displays the connected characteristic for the clients managed by the Primary AP:

- **Client by Connection Score:** Displays the connection score percentages ranges for all the clients connected to the Primary AP. The Connection Score is calculated as a percentage value based on the Client Actual Rate divided by either Client Max Capability or Max AP Configured (whichever is lower). This ensures the Connection Score is always calculated based on the maximum possible rate based on each devices maximum rate capability.
- **Client by Connected Protocol:** Displays the graph and table for the number of client based on the connected protocol for all the clients connected to the Primary AP.

AP DISTRIBUTION

Displays the distribution of APs managed by the Primary AP:

- **AP distribution by Model:** Displays the graph and table for all APs configured by the Primary AP. Based on the Model name of the AP to the radios (2.4 GHz and 5GHz) the graph and table gets updated.
- **AP distribution by SpatialStream:** Displays the graph and table for all APs configured by Primary AP. Based on the SpatialStream to which it is connected for each of the radios (2.4 GHz and 5GHz) the graph and table get updated. The centre of the donut displays the maximum number of APs with the particular SpatialStream.

Customizing the Access Point Performance View

You can customize the AP Performance view by adding or removing the widgets.

Table 2: Wireless Dashboard - AP Performance

Widgets	Description
CHANNEL UTILIZATION -TOP APS	Level of traffic including data and interference over the channel that is assigned on the AP. Interference includes both Wi-Fi and non Wi-Fi signals. High utilization of channel, for example above 50%, suggests high level of interference including noise from nearby APs/clients/rogues on the same channel which results in poor client performance. Click to view the AP detail.
INTERFERENCE -TOP APS	RF interference involves unwanted, interference of RF signals that disrupt normal wireless operations, that creates potential network latency and poor client performance. Interfering RF signals includes both Wi-Fi and non Wi-Fi signals. Click to view the AP detail.
CLIENT LOAD -TOP APS	Load indicator displays current number of connected clients on each access point. Higher load may impact performance, using client load balancing you can improve client distribution on the wireless network. Click to view the AP detail.
COVERAGE-BOTTOM APS	Coverage holes are areas where clients cannot receive a signal from the wireless network. A coverage hole is considered to have occurred when client SNRs falls below a predetermined level. A coverage hole event is when several clients are stuck in the same coverage hole.
AP Join Failure Status	This widget shows the number of APs that failed to join the Primary AP and the associated error types during a specific day, week or month. Click a specific join error to see the APs that have failed to join the Primary AP with the associated error type. Click the setting to clear the AP Join statistics.

You can view the above statistics in both 2.4GHz and 5 GHz type of radios by clicking on them respectively.

Adding Widgets

-
- Step 1** Choose **Monitoring > Wireless Dashboard > AP Performance**.
- Step 2** Click the + (plus) icon on the top right of the AP Performance window.
- Step 3** Select the widgets you want to add from the following:
- **Channel Utilization**—Top APs
 - **Interference**—Top APs
 - **Client Load**—Top APs
 - **Coverage**—Bottom APs

- **AP Join Failure Status**—Bottom APs

- Note**
- Top APs—AP with the maximum client load.
 - Bottom APs—AP with low SNR values for the client.

Step 4 Click **Close**. The **AP Performance** window is refreshed with the new widgets.

Removing Widgets

Step 1 Choose **Monitoring > Wireless Dashboard > AP Performance**.

Step 2 Click the **Close Widget (X)** icon on the top right of the widgets that you want to remove. You may add the closed widget again by clicking the + icon if you wish.

Customizing the Client Performance View

You can customize the **Client Performance** view by adding or removing the widgets.

Table 3: Client Performance

Numbers & Labels	Description
Signal Strength	Strong signal strength results in more reliable connections and higher speeds. Signal strength is represented in -dBm format, ranges from 0 to -100dBm. The closer the value to 0, the stronger the signal. Click to get a summary of clients.
Connection Rate	Each client's throughput varies depending on the data rate used (802.11 a/b/n/ac) at any time, and this data rate may vary every second. Various factors such as RSSI values, RF interference, and so on, may affect a client device's instantaneous data rate.
Signal Quality	Signal quality is a value ranging from 0 to 100 dB. This includes the noise generated by interference sources and the signal strength.
Client Connections	Displays clients associated with the access points of any connectivity types.

Adding a Widget

Step 1 Choose **Monitoring > Wireless Dashboard > Client Performance**.

Step 2 Click the **Add Widget** icon on the top right of the **Client Performance** window.

Step 3 Select the widgets you want to add from the following:

- **Signal Strength**

- **Signal Quality**
- **Connection Rate**
- **Client Connections**

Step 4 Click **Close**. The **Client Performance** window is refreshed with the new widgets.

Removing a Widget

Step 1 Choose **Monitoring > Wireless Dashboard > Client Performance**.

Step 2 Click the **Close Widget(X)** icon on the top right of the widgets and select the ones you want to remove. You may add the closed widget again by clicking the + icon if you wish.
