# Wireless Settings

This chapter contains the following sections:



## About WLANs and RLANs in CBW Access Point Network

Wireless LAN (WLAN) is a network that allows devices to connect and communicate on wireless mode. Remote-LAN (RLAN) is similar to a WLAN. The only difference being that a WLAN is used for wireless connection, and a Remote-LAN is used for wired connection.

On connecting a wired client to the CBW240AC/CBW145AC ports in a non-mesh deployment, the client will be able to access the internet.

**Note** RLAN is not supported in Mesh deployments. To support wired devices in Mesh deployment, refer to List item..

In a non-mesh deployment, when the Primary AP boots up, the **Default_RLAN** is automatically created.

You may also refer LAN port functionality for different models to understand the LAN port functionality supported for different AP models.

You can create and manage Wireless Local Area Networks (WLANs) and Remote LANs (RLANs) using the **WLANs** screen. This is discussed in the following sections.

## Setting Up WLANs RLANs and WLAN Users

Choose **Wireless Settings** > **WLANs**.

The total number of active WLANs and RLANs (in non-mesh deployments) is displayed at the top of the **WLANs/RLANs** window which includes a list of WLANs currently configured on the Primary AP. The following details are displayed for each WLAN/RLAN:

- Status of the WLAN. It can be enabled or disabled
- Displays if it is a WLAN or RLAN.
- Name of the WLAN
- Security Policy on WLAN
- Radio Policy on WLAN

### Guidelines and Limitations for Setting Up WLANs

- You can associate up to 16 WLANs/RLANs (inclusive of DEFAULT_RLAN in non-mesh deployments) with the CBW Primary AP and create a total of 16 WLANs/RLANs. Cisco recommends a maximum of 4 WLANs. The Primary AP assigns all the configured WLANs to all the connected APs.
- Each WLAN has a unique WLAN ID, a unique profile name, and an SSID.
- The Profile name and SSID can have up to 31 characters.
- Each connected AP advertises only the WLANs that are in an **Enabled** state. The APs do not broadcast disabled WLANs.
- Peer-to-peer blocking does not apply to multicast traffic.
- You cannot map a WLAN to VLAN0, and you cannot map VLANs 1002 to 1006.
- Dual-stack clients with static IPv4 addresses are not supported.
- Profile name and security type must be unique for each WLAN.

# Viewing WLANs

The **WLANs** window lists all the WLANs/RLANs that are currently configured on the Primary AP, along with the following details for each WLAN/RLAN:

- **Action**—Provides option to **Edit** or **Delete** the WLAN.
- **Active**—Status of the WLAN. It can be enabled or disabled.
- **Type**—Displays the type as WLAN or RLAN
- **Name**—Profile Name of the WLAN. Several WLANs can be configured with the same SSID name but with unique policy name and security mechanisms.
- **SSID**—SSID name of the WLAN.
- **Security Policy**—Denotes the Security Type of the WLAN. It can be an Open network, WPA2 Personal, WPA2+WPA3(Personal), WPA3 Personal, WPA2 Enterprise, Central Web Auth (CWA) or guest network.
- **MAC filtering**—This option is displayed when you configure a Security Type with MAC Filtering enabled in the previous field. For example, when you configure a Open WLAN with the MAC Filtering enabled, then it displays Open+Macfilter.
- **Radio Policy**—Displays the Radio in which the WLAN is broadcasting. By default, it is **All**.

**Note** See About WLANs and RLANs in CBW Access Point Network, on page 1 section for a brief explanation on WLANs.

**Tip** The total number of active WLANs/RLANs is displayed at the top of the page. If the list of WLAN/RLAN spans multiple pages, you can browse these pages by clicking the page number links or the forward and backward icons.

To view details of configured WLANs, go to **Wireless Settings** > **WLANs**.

# Adding and Modifying a WLAN

To add a WLAN, do the following:

1. Choose **Wireless Settings** > **WLANs**.
2. In the **WLANs** window, click **Add new WLAN/RLAN**. The **Add new WLAN/RLAN** window is displayed.

   To edit a WLAN/RLAN, do the following:

   Click the **Edit** icon adjacent to the WLAN/RLAN you want to modify.

   **Note** Editing the WLAN/RLAN will disrupt the network momentarily.

   For example, to change the Security Type for a WLAN that has been created, do the following:

   a. Click the **Edit** icon.
   b. Click **Yes** in the pop-up message.
   c. Go to **WLAN security** tab and select the required security type from the drop down-list.
   d. Click **Apply** to save the configurations or **Cancel** to discard the changes.

   Each of the tabs in this window is explained in the following sections.

To delete a WLAN/RLAN, click the **Delete** icon adjacent to the WLAN/RLAN you want to delete and follow the instructions.

## Configuring General Details

Navigate to **Wireless Settings** > **WLANs** > **Add new WLAN/RLAN** > **General**.

Under the **General** tab, set the following parameters:

1. **WLAN ID**—From the drop-down list, choose an ID number for the WLAN.
2. **Type**—Indicates if the type of network is WLAN or RLAN. Choose WLAN option.
3. **Profile Name**— The profile name must be unique and should not exceed 31 characters.

4. **SSID**—The profile name also acts as the SSID. You can choose to specify an SSID that is different from the WLAN profile name. The SSID must be unique and should not exceed 31 characters.
5. **Enable**—Click this tab to enable/disable the WLAN.
6. **Radio Policy**—Click the drop-down list and choose from the following options:
   a. **All**—Configures the WLAN to support dual-band (2.4 GHz and 5 GHz) capable clients
   b. **2.4 GHz only**—Configures the WLAN to support 802.11b/g/n capable clients only
   c. **5 GHz only**—Configures the WLAN to support 802.11a/n/ac capable clients only
7. **Broadcast SSID**—The default is **Enabled** for the SSID to be discovered. Use the toggle button to hide the SSID.
8. **Local Profiling**—By default, this option is **disabled**. Enable this option to view the Operating System that is running on the Client or to see the User name.

## Configuring WLAN Security

Navigate to **Wireless Settings** > **WLANs** > **Add new WLAN/RLAN** > **WLAN Security**.

Under the **WLAN Security** tab, set the following parameters.

- **Guest Network**—Guest user access can be provided on WLANs which are specifically designated for use by guest users. If the Guest Network is enabled, then the WLAN is considered as Guest WLAN. By default, this field is disabled.

  The following fields are displayed when you **Enable** the **Guest Network** option. These are applicable for WLANs and Guest WLANs.

  For details on creating a Guest Network, refer to Creating a Guest Network.

- **Captive Network Assistant**—This feature detects the presence of a captive portal by sending a web request on connecting to a wireless network. This request is directed to a URL for iPhone models and if a response is received, then the internet access is assumed available and no further interaction is required. If no response is received, then the Internet access is assumed to be blocked by the captive portal and Apple's Captive Network Assistant (CNA) auto-launches the pseudo-browser to request portal login in a controlled window.

- **MAC Filtering**— You can also restrict or permit a particular client joining your network by enabling the MAC Filtering feature. For details, refer to Blocking and Unblocking Clients, on page 16.

**Note** When MAC Filtering is enabled on the WLAN, the client MAC address must be added to the Local MAC Addresses list by navigating to **Wireless Settings** > **WLAN Users** > **Local MAC Addresses** with the **Type** as **Allowlist** for enabling the client to join the network via that SSID.

- **Captive Portal**—This field is visible only when the **Guest Network** option is enabled. This is used to specify the type of web portal that can be used for authentication purposes. Following are the types of web portals that you can choose.
  - **Internal Splash Page**—Choose this option to have a default Cisco web portal based authentication.

- **External Splash Page**—Choose this option to have external captive portal authentication, using a web server outside your network. Also, specify the URL of the server in the **Captive Portal URL** field.

**Note** Ensure to add this URL rule in the configuring ACL name under **Advanced >Security Settings** page.

- **Access Type**—This field is visible only when the **Guest Network** option is enabled.
  - **Local User Account**—This is the default option. Choose this option to authenticate guests using the username and password which you can specify for guest users of this WLAN, under **Wireless Settings > WLAN Users**. For more information, see Viewing and Managing WLAN Users, on page 15
  - **Web Consent**—Choose this option to allow guests access to the WLAN upon acceptance of displayed terms and conditions. This option allows guest users to access the WLAN without entering a username and password.
  - **Email Address**—Choose this option, if you want guest users to be prompted for their e-mail address when attempting to access the WLAN. Upon entering a valid email address, the access to the internet is provided. This option allows guest users to access the WLAN without entering a username and password.

**Note** You can also collect the email address information by configuring **Accounting Radius Server** under **Management** > **Admin Accounts** > **Radius** in **Expert View**. By default, the email address will be sent to the first Radius server configured.

  - **RADIUS**—Refer to details on RADIUS in the Security Type-WPA2 Enterprise section.
  - **WPA2 Personal**—Refer to Security Type Personal, on page 7in the following section.
  - **Social Login**—Choose this option to allow guest access to WLAN upon authentication by Google/Facebook using their personal credentials. Once the user connects to this guest WLAN they will be redirected to the default login page where they can find the login buttons for Google or Facebook, or both depending on which toggle buttons are enabled. Log in using the respective account, and get the specific Internet access.

    If **Social Login** Access type is selected, the two toggle options will be displayed:
    - **Facebook** —Turn on this option when you want to allow a guest user access only using Facebook accounts.
    - **Google**—Turn on this option when you want to allow a guest user access only using Google accounts.

    By default both toggles are enabled, so guest users can use Facebook or Google accounts for authentication.

**Note** Apple devices will not be able to sign-in via Google, if **Captive Network Assistant** (CNA) is enabled with **Social Login** as **Access Type**. You will need to disable CNA and sign-in via Google for Guest access.

- **ACL Name(IPv4)**—This field is visible only when the **Guest Network** option is enabled.

**Note** For a detailed explanation on this feature refer to Configuring Access Control Lists (ACL). This description is applicable for WLAN and Guest WLAN.

Any ACL created through **Advanced** > **Security Settings** > **Add new ACL** is also displayed here.

- **None**— No ACL is applied
- **Enable Facebook Login**— The user can map to this when required to configure a Guest WLAN with Social Login as **Access type** and the Facebook toggle is enabled.
- **Enable Google Login**— The user can map to this when required to configure a Guest WLAN with Social Login as **Access type** and the Google toggle is enabled.
- **Enable Social Login**— This is a default setting. The user can map this when required to configure a Guest WLAN with Social Login as Access type.
- **ACL Name(IPv6)**—This field is visible only when the **Guest Network** option is enabled.

**Note** For a detailed explanation on this feature refer to Configuring Access Control Lists (ACL). This description is applicable for WLAN and Guest WLAN.

Any ACL created through **Advanced** > **Security Settings** > **Add new ACL** is also displayed here.

- **Security Type**—For details on this option, refer to the following section:

**Note** Security Type is only displayed when Guest Network option is disabled.

Each of the options available in the **Security Type** drop-down is explained in detail below:

### Security Type-Open

This option stands for Open authentication, which allows any device to authenticate and then attempt to communicate with an AP. Using open authentication, any wireless device can authenticate with the AP.

### Security Type Personal

- **WPA2**—This option stands for Wi-Fi Protected Access 2 with Pre-Shared Key (PSK). WPA2 Personal is a method used for securing your network with the use of a PSK authentication. The PSK is configured separately both on the Primary AP, under the WLAN security policy, and on the client. WPA2 Personal does not rely on an authentication server on your network. By default, it is **enabled**.
- **WPA3**—This option stands for Wi-Fi Protected Access 3 (WPA3), the latest version of Wi-Fi Protected Access (WPA), which is a suite of protocols and technologies that provide authentication and encryption for Wi-Fi networks. WPA3 leverages Simultaneous Authentication of Equals (SAE) to provide stronger protections for users against password guessing attempts by third parties. When the client connects to the Access Point, they perform an SAE exchange. If successful, they will each create a cryptographically strong key, from which the session key will be derived. Typically, a client and Access Point goes into phases of commit and then confirm. Once there is a commitment, the client and Access Point can then go into the confirm states each time there is a session key to be generated.

  For advanced security, enable WPA3 in addition to WPA2. By default, the value is disabled.

**Note** You can also enable WPA3 individually, provided the client is WPA3 compatible.

- **Passphrase Format**—Choose **ASCII** or **HEX** (hexadecimal range) from the PSK Format drop-down list and then enter a pre-shared key in the text box. WPA pre-shared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.
- **Passphrase**—Specify the password.

**Note** The PSK you enter is hidden under dots for security purposes.

- **Confirm Passphrase**—Confirm the password.
- **Show Passphrase**—Check the checkbox, if you would like to display the password that was entered for verification.
- **Password Expiry**—This option helps to enable password expiry for WLANs with WPA-PSK. By default, the password expiry is **disabled**.
- **Expiry (Days)**—Set Value for expiry in days. Range: 1 - 180 days. By default, 180 days will be set as expiry value. This field is displayed when you enable the **Password Expiry** toggle switch.

**Note** Once the expiry value is exceeded, the WLAN will be disabled. If required, re-enable the WLAN and set the expiry value.

### Security Type-WPA2 Enterprise

This option stands for Wi-Fi Protected Access 2, with a local authentication server or a RADIUS server. When you choose this option, you will see the following fields:

- **Authentication Server**—You can choose **External Radius** or **AP**. The default option is **External Radius**.

  To have a local authentication method, choose **AP** in the **Authentication Server** drop-down list. This option is a Local EAP authentication method that allows users and wireless clients to be authenticated locally. The Primary AP serves as the authentication server and the local user database, which removes dependency on an external authentication server.

**Note** You will see note specifying whether the Radius Server is configured for Authentication and Accounting. Radius Server can be configured by navigating to **Admin Accounts** > **RADIUS** in Expert view.

- To have a RADIUS server-based authentication method, choose **External Radius** in the **Authentication Server** drop-down list. RADIUS is a client/server protocol that enables communication with a central server to authenticate users and authorize their access to the WLAN.
- **Radius Profiling**—The Primary AP acts as the collector of the information and sends the RADIUS server with the required data in an optimal form. Clients on the WLANS will be profiled as soon as profiling is enabled.

  Profiling can be based on the following:

  - Role defining the user type or the user group to which the user belongs.
  - Device type, such as Windows machine, Smart Phone, iPad, iPhone and Android.
  - Username / password.
  - Location, based on the AP group to which the client is connected.
  - Time of the day based on what time of the day the client is allowed on the network.

- **BYOD**—This is a **Bring Your Own Device** (BYOD) solution architecture, combining elements across the network for a unified approach to secure device access. It is enabled when a user wants to connect their personal devices in a more secure manner.

### Security Type-Central Web Auth

It is a method of authentication in which the host's Web browser is redirected to a RADIUS server. The RADIUS server provides a web portal where the user can enter a username and password. If these credentials are validated by the RADIUS server, the user is authenticated and is allowed access to the network. When you choose this option, you will see the following fields:

**Radius Profiling**—Refer to Radius Profiling in the earlier section.

### RADIUS Server

RADIUS is a client/server protocol that enables communication with a central server to authenticate users and authorize their access to the WLAN/RLAN. To have a RADIUS server-based authentication method, choose **External Radius** in the **Authentication Server** drop-down list.

**Note** This section appears in UI, when you do the following:

- Set the WLAN security to **WPA2 Enterprise with Authentication Server** and choose **External Radius**.
- Set the WLAN security to **Central Web Auth**.
- Set the WLAN security to **WPA2/WPA3 Personal**, and enable the **MAC filtering** toggle button.

The following fields are visible for the Security Types: **WPA2 Enterprise**, **Central Web Auth**, and **WPA2 Personal** with the MAC filter option turned on.

- **Radius Server**—Provided for external authentication when you connect to a WLAN.
- **Authentication Caching**—This feature helps store the client information essential for authentication locally in the cache on the CBW. This happens when the authentication with the RADIUS Server is successful. If the connectivity to the RADIUS server is lost, the information stored in the cache is used for authenticating the clients. You can also configure cache when the RADIUS Server is up and running. If the client details are not available locally, the request for authentication is sent through the RADIUS Server disabled.

**Note** This is field is not visible for the security type **Central Web Auth**.

When you enable this option, the following fields are displayed.

- **User Cache Timeout**—Specifies the time period at which the authenticated credential in the cache expires.

  If the client's cache that expires is associated to the controller, then it would get deauthenticated,

**Note** Any change in cache timeout value on the WLAN will affect only new client associations and the existing clients won’t get impacted.

- **User Cache Reuse**—Use the credentials cache information before cache timeout. By default this is disabled.

**Note** Local cache client entries are deleted in the following scenarios:

- The CBW Primary AP reboots
- The cache time expires
- The security of the WLAN changes
- A WLAN is deleted
- Authentication Caching is disabled on the WLAN

- **Add RADIUS Authentication Server**—Click this tab to add the following RADIUS Authentication Server details:
  - **Server IP Address**—Select the IP address of the RADIUS server from the drop down list.
  - **State**—Shows the state of the RADIUS server.
  - **Port Number**—Provided for communication with the RADIUS server. By default, it is 1812.

**Note** To map RADIUS server to WLAN, first configure the RADIUS server details under **Management** > **Admin Accounts** > **RADIUS** in Expert View.

- **Add RADIUS Accounting Sever**—Click this tab to add the following RADIUS Accounting Server details:
  - **Server IP Address**—Select the IP address of the RADIUS server from the drop down list.
  - **State**—Displays if the accounting server is in an enabled or disabled state.
  - **Port Number**—It is used for communication with the RADIUS server. By default, the value is 1813.

**Note** You can only add/delete the Radius server entries.

To map RADIUS server to WLAN, first configure the RADIUS server details under **Management** > **Admin Accounts** > **RADIUS** in Expert View.

## Configuring VLAN and Firewall

Navigate to **Wireless Settings** > **WLANs** > **Add new WLAN/RLAN** > **VLAN & Firewall**.

Specify the following parameters:

1. **Client IP Management**—To assign an IP address to the client through external DHCP server.
2. **Peer to Peer Block**—It disables communication between clients that are connected in the same WLAN. By default this is **disabled**.

   For example, when you connect two clients (say A and B) on the same WLAN with Peer to Peer Blocking enabled, then the client (A) will not be able to reach client (B) and vice versa.
3. **Use VLAN Tagging**—From the drop-down list, choose **Yes** to enable VLAN tagging of packets. By default this field is set to **No**.

   If you choose to enable **VLAN Tagging**, choose the VLAN ID in the **VLAN ID** field. By default, the Native VLAN ID set to **1** will be mapped.

   You can configure Native VLAN ID, under **Wireless Settings > Access Points > Global AP configuration > VLAN Tagging**.
4. **Enable Firewall**—To enable a firewall for the WLAN based on Access Control Lists (ACLs), choose **Yes** from the drop-down list. By default, this field is set to **No**. To create an ACL, refer to Configuring

Access Control Lists (ACL) later in this section. When you enable the **Enable Firewall** option, the following fields are displayed:

**a.** In the **WLAN Post-auth ACL** section, choose **IPv4/IPv6 ACLs** in the **ACL Name(IPv4) / ACL Name(IPv6)** fields. These ACL rules are applied to the clients connected to the WLAN after successful authentication.

**b.** In the **VLAN ACL** section, choose **IPv4/IPv6 ACLs** in the **ACL Name(IPv4)** and specify the **ACL Direction**. The ingress (inbound) and egress (outbound) ACL specifies the types of network traffic that are allowed in or out of the device in the network. Choose **Both** to allow ingres and egress traffic.

## Configuring Traffic Shaping

Navigate to **Wireless Settings** > **WLANs** > **Add new WLAN/RLAN** > **Traffic Shaping**. Configure the following parameters:

- **Quality of service (QoS)** —Qos refers to the capability of a network to provide better service to selected network traffic over various technologies. The primary goal of QoS is to provide priority, including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics.

  The CBW Primary AP supports the following four QoS levels. Under the **QoS** tab, from the **QoS** drop-down list, choose one of the following QoS levels:

  - **Platinum (Voice)**—Ensures a high quality of service for voice over wireless.
  - **Gold (Video)**—Supports high-quality video applications.
  - **Silver (Best Effort)**—Supports normal bandwidth for clients.
  - **Bronze (Background)**—Provides the lowest bandwidth for guest services.

- Specify the **Rate limits per client** and **Rate limits per BSSID** (in Kbps) using the following criteria:
  - **Average downstream bandwidth limit**—Define the average data rate for downstream TCP traffic by entering the rate in Kbps in the Average Data Rate text boxes.
  - **Average real-time downstream bandwidth limit**—Define the average real-time rate for downstream UDP traffic by entering the rate in Kbps in the Average Real-Time Rate text boxes.
  - **Average upstream bandwidth limit**—Define the average data rate for upstream TCP traffic by entering the rate in Kbps in the Average Data Rate text boxes.
  - **Average real-time upstream bandwidth limit**—Define the average real-time rate for upstream UDP traffic by entering the rate in Kbps in the Average Real-Time Rate text boxes.

**Note** Average Data Rate is used to measure TCP traffic while Average Real-time rate is used for UDP traffic. They are measured in kbps for all the entries. The values for Average Data Rate and Average Real-time rate can be different because they are applied to different upper layer protocols such as TCP and UDP. These different values for the rates do not impact the bandwidth.

- **Fastlane**—Wireless application traffic in real-time environments often needs to be prioritized by its type. For example, due to real time application constraints, voice over Wi-Fi traffic needs a higher priority than Safari web traffic.

  Various standards exist to help network devices agree on how different types of traffic are marked to make sure they are prioritized. QoS Fastlane greatly simplifies this agreement process so that network congestion is minimized and time sensitive traffic (like voice or video) is delivered on time.

  On enabling the fastlane, the QoS is set to platinum such that voice traffic has higher priority than any other traffic.

- **Application Visibility Control** classifies applications using the Network-Based Application Recognition (NBAR2) engine, and provides application-level visibility in wireless networks. Application Visibility enables the Primary AP to detect and recognize more than 1000 applications and perform real-time analysis, and monitor network congestion and network link usage. This feature contributes to the **Applications By Usage** statistic in the **Monitoring** > **Network Summary**.

  To enable **Application Visibility Control**, choose **Enabled** from the **Application Visibility** drop-down list. Otherwise, choose **Disabled** which is the default option.

- **AVC Profile**—Displays the WLAN name.

- **Add Rule**—To allow/deny specific applications when the clients get connected to the specific WLAN.

  - **Application**—List the applications that can be allowed/denied.

  - **Action**— Choose **Mark** to allow the application process with priority, **Drop** to deny the application and **Rate limit** to limit the rate (includes the Average Rate and Burst Rate) at which the application runs.

## Configuring Advanced Options

Switch to Expert View in the CBW Web-UI by clicking the bi-directional arrows toggle button on the top-right.

Navigate to **Wireless Settings** > **WLANs** > **Add new WLAN/RLAN** > **Advanced**:

- **Allow AAA Override**—AAA Override option of a WLAN enables you to configure the WLAN for identity networking. It enables you to apply VLAN, Access Control Lists (ACLs) and Quality of Service (QoS) to individual WLANs on the returned RADIUS attributes from the AAA server.

- **802.11r**—802.11r enabled WLAN provides faster roaming for wireless client devices. It is desired that 11r capable devices will be able to join a WLAN with 11r enabled for better roaming experience. However, if 11r is enabled on a WLAN, the legacy devices (i.e. is non-11r clients) will not be able to join the WLAN.

  This feature help clients roam better by telling them when to roam and providing them with information about neighboring APs so that no time is wasted scanning when roaming is needed.

  This option is available only for WPA2/WPA3 Personal WLAN with the WPA2 toggle button alone enabled, or WPA2 Enterprise enabled WLANs. By default, this option is **Disabled**.

**Note** The 802.11r and WPA3 are not compatible with each other.

- **Over The DS**—Use **Over The DS** (Distributed System) button to enable or disable the fast roaming facility. By default, this is **Disabled**.
- **Reassociation Timeout(secs)**—Enter the number of seconds after which the re-association attempt of a client to an AP should time out. The valid range is 1 to 100 seconds. Default is 20 seconds.
- **DTIM Period 802.11a/n(beacon intervals)**—Depending on the timing set for your AP, it "buffers" broadcast and multicast data and let your mobile devices or clients know when to "wake up" to receive those data.
- **DTIM Period 802.11b/g/n(beacon intervals)**—Depending on the timing set for your AP, it "buffers" broadcast and multicast data and let your mobile devices or clients know when to "wake up" to receive those data.
- **Client Band Select**—Band selection enables client radios that are capable of dual-band (2.4 and 5 GHz) operation to move to a less congested band.
- **Client Load Balancing**— This feature can be used in order to load-balance clients across access points. Enabling this will improve client distribution on the wireless network.

**Note** You cannot configure the number of clients per AP.

- **Umbrella Profile**, **Umbrella Mode**, **Umbrella DHCP Override**—For details on these options, refer to Configuring Cisco Umbrella on Primary AP
- **mDNS**, **mDNS Profile**—For details on these options, refer to Mapping mDNS Profile to WLAN
- **Multicast IP**— Enter the Multicast IP group address. By default, the field will be null.
- **Multicast Direct** — Enable the Multicast Direct toggle button to enhance the video streaming for wireless clients by converting multicast packets to unicast at CBW AP. By default, this is **Disabled**.

  To enable this toggle, change the **QoS** value under the **Traffic Shaping** section to **Gold** or **Platinum**.

  For details, see Media Steam.

## Configuring Scheduling

CBW supports an option to schedule availability for every WLAN. By default, all WLANs are available 24/7 when they are initially created. To schedule the WLAN availability, do the following:

1. Navigate to **Wireless Settings** > **WLANs** > **Add new WLAN/RLAN** > **Scheduling**.
2. **Schedule WLAN**—You may choose one of the following options from the drop-down.
   - **Enable**—This enables scheduling for a chosen WLAN.
   - **Disable**—This disables scheduling for all the WLANs except the WLAN that is enabled.
   - **No Schedule**—Scheduling is not applied to the WLAN.

**Note** You can also schedule the day/time for the WLAN to be broadcasted by enabling the corresponding Day and mention the start and end time using the slider.

Enable the option **Apply to all Weekdays** to make changes for all the weekdays. By default, it is **disabled**.

3. Click **Apply** to save the changes.

# Enabling and Disabling WLANs RLANs

**Step 1** Choose **Wireless Settings** > **WLANs/RLANs**.

**Step 2** In the **WLANs** window, click the **Edit** icon adjacent to the WLAN you want to enable or disable.

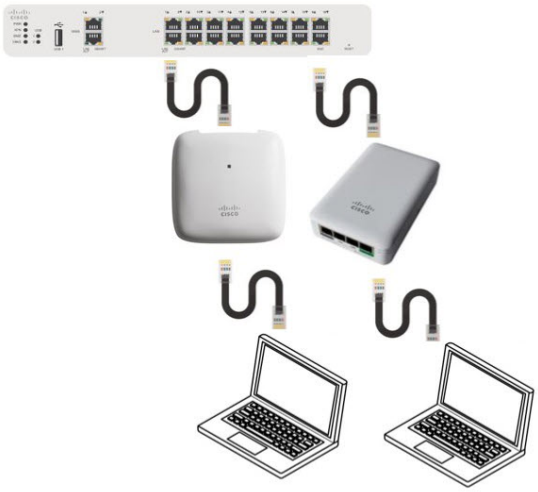
**Step 3** In the **Edit WLAN/RLAN** window, under **General**, select **Enabled** or **Disabled** to enable/disable WLAN/RLAN.

**Step 4** Click **Apply**.

**Note** Clicking **Apply** after creating a new WLAN or editing an existing one always enables the WLAN irrespective of whether it was previously enabled or disabled.

# Configuring RLAN in AP

In order to configure RLAN in Primary capable APs (CBW140AC, CBW240AC and CBW145AC), execute the following steps to map the RLAN to your AP ports:



1. Create RLANs with 802.1x Authentication or Open access type
2. Create AP Groups, associate RLAN to AP Group, add APs to AP Group and finally associate Wired Ports to RLANs.

To create RLAN, follow the procedure below:

**Step 1** Navigate to **Wireless Settings** > **WLANs** and click **Add new WLAN/RLAN**.

**Step 2** Under the **General** tab, select **RLAN** from the **Type** drop-down list box.

**Step 3** Enter the Profile name.

**Step 4** Under the RLAN Security, select **802.1x** or **Open** for authentication type.

**Step 5** When you enable the **802.1x**, the following options are displayed:

a) MAB (MAC Authentication Bypass)—MAB enables port-based access control using the MAC address of the client. A MAB-enabled port can be dynamically enabled or disabled based on the MAC address of the device that connects to it. Add the client MAC in the Local MAC Address table. Refer to Blocking and Unblocking Clients, on page 16 clients. By default, it is **enabled**.

b) Authentication Server—Please refer to Security Type - WPA2 Enterprise.

**Step 6** Use the parameters available on the **General**, **RLAN Security**, and **Advanced** tabs for configuring the remote LAN.

**Note** For descriptions of parameters available under **RLAN Security**, **VLAN & Firewall**, **Traffic Shaping** and **Advanced** tabs, refer to Configuring WLAN Security, on page 4.

**Step 7** Click **Apply** to save the changes.

You can monitor the number of clients connected to the network by navigating to **Monitoring > Network Summary** and view the wired clients in the **Wired Networks** block.

# Editing and Deleting WLANs RLANs

**Step 1** Choose **Wireless Settings** > **WLANs/RLANs**.

**Step 2** In the table of WLANs listed, perform one of the following actions as required:

- To edit a WLAN/RLAN, click the **Edit** icon adjacent to the WLAN/RLAN you want to modify.
- To delete a WLAN/RLAN, click the **Delete** icon adjacent to the WLAN/RLAN you want to delete.

# Viewing and Managing WLAN Users

You can view and manage WLAN users only for WPA2 Enterprise and Guest WLAN with Local User Accounts as access types. To use your Cisco Business Wireless network, a wireless client should connect to a WLAN in the network. To connect to a WLAN, the wireless client will have to use the user credentials set for that WLAN. If this WLAN uses WPA2-Personal as a Security Policy, then the user must provide the appropriate WPA2-PSK set for that WLAN on the Primary AP. If the Security Policy is set to WPA2-Enterprise/Local User Account, the user must provide a valid user identity and the corresponding password

In the **WLAN Users** window, you can set up different users and their respective user credentials for the different WLANs in the CBW AP wireless network. These are local users authenticated by the Primary AP using WPA2-PSK.

To view and manage WLAN users, choose **Wireless Settings** > **WLAN Users**.

The **WLAN Users** window is displayed along with the total number of WLAN users configured on the Primary AP. It also lists all the WLAN users in the network along with the following details:

- **User name**—Name of the WLAN user.
- **Guest user**— Indicates a guest user account if the toggle button is enabled. This user account is provided with a limited validity of 86400 seconds (or 24 hours) from the time of its creation.
- **WLAN Profile**—The WLANs that the user can connect to.
- **Password**—The password to connect to a WLAN.
- **Description**—Additional details or comments about the user.

### Adding a WLAN User

To add a WLAN user, click **Add WLAN User** and specify the following details:

- **User name**—Specify a name for the WLAN user account.
- **Guest user**—Enable the slider button if this is meant to be a guest WLAN user account. You can also specify the validity of this account from the time of its creation, in seconds, in the **Lifetime** field. The default value is 86400 seconds (that is, 24 hours). You can specify a lifetime value from 60 to 31536000 seconds (that is, 1 minute to 1 year).
- **WLAN Profile**—Select the WLAN that this user can connect to. From the drop-down list, choose a particular WLAN, or choose **Any WLAN** to apply this account for all WLANs set up on the Primary AP.

  This drop-down list is populated with the WLANs which have been configured under **Wireless Settings** > **WLANs**.

  For information on adding WLANs, see Adding and Modifying a WLAN, on page 3.
- **Password**—The password to be used when connecting to a WLAN.
- **Description**—Additional details or comments for the user.

### Editing a WLAN User

To edit a WLAN user, click the **Edit** icon adjacent to the WLAN user whose details you want to modify and make the necessary changes.

### Deleting a WLAN User

To delete a WLAN user, click the **Delete** icon adjacent to the WLAN user you want to delete. and then click **Ok** in the confirmation dialog box.

# Blocking and Unblocking Clients

**Step 1** Go to **Wireless Settings** > **WLAN Users** > **Local MAC Address**.

**Step 2** Click **Add MAC Address** and add the client MAC address.

**Step 3** You can choose to **Allowlist/Blocklist** the client by selecting it from the **Type** option and then click **Apply**.

Choose the type as **Blocklist** to deny the client joining your network.

**Note** Blocklisting a client or Mesh Extender that is currently joined to the network will not take effect until it attempts to rejoin the network after a disconnect or reboot.

Choose the type **Allowlist** to add the client to your network. The **MAC Filtering** should be enabled on the WLAN to add your client MAC to the Local MAC address with Type as **Allowlist**. This helps the client to join the network.

You can also import/export the Local MAC address list.

The status of Import is displayed under **Local MAC Address** section. Select **Click Here** to see the list of MAC IDs which failed to be imported.

# Social Login for Guest Users

This feature provides social login privileges for guest users that are connected using Google or Facebook accounts. To enable this option, execute the following on the Primary AP:

**Step 1** On the left navigation pane, choose **Wireless Settings > WLANs > Add new WLAN/RLAN**

**Step 2** Under the **General tab**, fill in the basic information for your WLAN. For details, see Adding and Modifying a WLAN, on page 3.

**Step 3** Click the **WLAN Security** tab. Specify the following details:

a) Enable the **Guest Network** toggle button.

b) Under **Access Type** drop down list, select **Social Login**.

c) Enable **Facebook** or **Google**, or both.

- If the **Facebook** toggle alone is enabled, guest users are authenticated using Facebook accounts.
- If the **Google** toggle alone is enabled, guest users are authenticated using Google accounts.
- If **both** toggles are enabled, guest users are authenticated using Facebook or Google accounts.

  By default, both toggles are **enabled**.

d) Click **Apply** to save the configuration.

e) Once the WLAN is created with the **Social Login**access type, the respective **Pre-auth ACL** is automatically mapped to the WLAN.

**Note** Note You can also add and edit your URLs by navigating to Enable_Social_Login in **Advanced > Security settings**.

The Guest WLAN with an enabled Social login access type will be created. Once you connect to this guest WLAN you will be redirected to the default login page where you will find the login buttons for Google, or Facebook, or both depending on the toggle buttons enabled. Log in using the respective account and obtain the Internet access.

# Personal PSK for Clients

This feature provides the flexibility of configuring a different PSK passphrase for clients connecting to the same WPA2 Personal WLAN with WPA2 policy enabled. CBW AP uses an AAA server to authenticate the client.

**Note** This feature is not supported for WPA3 enabled WLANs.

To enable this feature, switch to Expert View and configure the following on the Primary AP:

**Step 1** Navigate to **Wireless Settings** > **WLANs** > **Add new WLAN/RLAN**.

**Step 2** Under the **General** tab, fill in the basic information for your WLAN. For more information see Adding and Modifying a WLAN, on page 3.

**Step 3** Click the **WLAN Security** tab and specify the following details:

**a.** Enable **MAC Filtering** toggle button.

**b.** Under the **Security Type** drop-down list, select **WPA2/WPA3 Personal**.

**c.** Click the **WPA2** toggle button to turn it on.

**d.** Select the **Passphrase Format** as either HEX or ASCII.

**e.** Enter the **Passphrase**.

**f.** Confirm the **Passphrase**. For more information see Adding and Modifying a WLAN, on page 3.

**Step 4** Under the **Radius Server** tab, map the radius server detail using the following steps.

a) Click **Add RADIUS Authentication Server**.
b) Click **Add RADIUS Accounting Server** .
c) Select the Radius Server IP address from the drop-down list.
d) Click **Apply**.

After a successful MAC authentication, RADIUS Server will display the following Cisco AVPair attributes:

- **psk-mode** – This contains the format of the Passphrase, it could be either ASCII, HEX, asciiEnc, or hexEnc.
- **psk** – This contains the Passphrase configured for the client on the RADIUS Server

**Note** The psk value could be a simple ASCII or HEX value or encrypted bytes in case of asciiEnc orhexEnc. The algorithm used for encryption or decryption is as per RFC2865 (user-password section – 16 bytes authenticator followed by encrypted key).

To configure radius server, navigate to **Management** > **Admin Accounts** > **Radius (Expert View)**. For details, refer to Managing TACACS+ and RADIUS Servers

**Step 5** Click the **Authentication Caching** toggle button.

a) Enter the **User Cache Timeout** in minutes
b) Enter the**User Cache Reuse** if required.

By default, the **User Cache Reuse** is disabled. For more information see RADIUS Server, on page 8

If **Authentication caching** is enabled, the PSK key is stored in the local cache along with the MAC Address and is used for subsequent authentications. The CBW AP first checks if any local DB is available for authenticating the client otherwise the request will be sent to Radius server for Authentication.

View the Auth cached clients at **Management** > **Admin Accounts** > **Auth Cached Users (Expert View)**. For more information see Viewing Auth Cached Users

**Step 6** Under the **Advanced**tab, click the **AAA Override** toggle button.

**Step 7** Click **Apply** to save the WLAN updates.

**Note**
- Devices with MAC addresses configured on Radius server will be able to connect to WLAN only with PSK passphrase configured on Radius server.
- Devices with MAC addresses configured on Radius server will not be able to connect to WLAN with PSK configured on WLAN.
- Devices with no MAC addresses configured on Radius server will be able to connect to WLAN with PSK configured on WLAN only. Navigate to **Wireless Settings** > **WLAN Users** > **Local MAC Addresses** and add the Client MAC in the **Allowlist** field. For more information see Blocking and Unblocking Clients, on page 16.

# Managing Associated Access Points

**Step 1** Choose **Wireless Settings** > **Access Points**.

**Step 2** In the **Access Points Administration** window, the number of APs associated with the CBW is displayed at the top of the window, along with the following details:

- **Manage**—The following icons indicate whether the AP is acting as a Primary AP or Primary capable AP or Mesh Extender.

***Figure 1: Primary AP icon***

***Figure 2: Mesh Extender icon***

***Figure 3: Subordinate AP icon***

- **Type**—Specifies if the AP is Primary capable or a Mesh Extender.
- **Location**—Location of the AP.

- **AP Role**—Operating role of the AP. It can be either Root or Mesh. The AP Role is only accessible on APs and only when in Expert mode.
- **Name**—Name of the AP.
- **IP Address**—IP address of the AP.
- **AP MAC**—The MAC address of the AP.
- **Up Time**—Duration of how long the AP has been powered up.
- **AP Model**—The model number of the access point.

**Note** When an AP joins an AP group; or the RF profile of the AP group is changed, the AP rejoins the Primary AP. The AP will receive new configuration specific to the new AP group or RF profile.

# Global AP Configuration

This allows you to configure a Native VLAN ID.

**Step 1** Navigate to **Wireless Settings > Access Points**.

**Step 2** Click **Global AP Configuration** and configure the **Native VLAN ID** under the **VLAN Tagging** tab.

**Step 3** Click **Apply**.

# Administering Access Points

**Step 1** Choose **Wireless Settings**>**Access Points**.

**Step 2** In the **Access Points** window, click the **Edit** icon adjacent to the AP you want to manage.

**Note** You can only administer those APs that are associated to the Primary AP.

**Step 3** In the **Edit**, under the **General** tab, you can edit the following AP parameters:

- The **Make me Primary AP** button is available only for subordinate APs that are capable of participating in the Primary Election process. Click this button, to make the AP, the Primary AP.
- **IP Configuration**—Choose **Obtain from DHCP** to let the IP address of the AP be assigned by a DHCP server on the network, or choose to have a **Static IP** address. If you choose to have a static IP address, then you can edit the IP Address, Subnet Mask, and Gateway fields.
- **AP Name**—Edit the name of the AP. This is a free text field.
- **Location**—Edit a location for the AP. This is a free text field.
- **Set as Preferred Primary**—Enable this to make the AP as the preferred Primary.

**Note** Setting as Preferred Primary will not change the current network status. In other words, it will not force the AP to take over as Primary, but it will take effect next time the network reboots.

- **Rogue Detection**— Enable this option to make the AP detect Rogue AP and client on both 2.4GHz and 5GHz radios.

  **Note**
  - Imported AP configuration would take precedence. Refer to the *Tools* section in Viewing Access Point Details.
  - When upgrading from earlier versions (where rogue detection was enabled), even after upgrade rogue detection would remain enabled.
  - If rogue detection is disabled, no new rogues would be detected. Rogues that are already detected, would be removed after 5 minutes, based on the default expiry time of rogue APs and clients.

The following non-editable AP parameters are also displayed under the **General** tab:

- **Operating Mode**—Displays the operating Mode of the AP.
- **AP MAC address** —Displays the AP MAC address.
- **AP Model number** —Displays the AP Model number.
- IP Address of the access point (non-editable only if **Obtain from DHCP** has been selected).
- Subnet mask (non-editable only if **Obtain from DHCP** has been selected).
- Gateway (non-editable only if **Obtain from DHCP** has been selected).

**Step 4** For the Primary AP, under the **Primary** tab, you can manually edit the following Primary AP parameters:

- **Primary AP Name**—You can edit the Primary AP Name set during Initial configuration using Setup Wizard.
- **IP configuration**—You can configure either Static IP or obtain from DHCP.
- **IP Address**—This IP address can be used in the Login URL to access the Primary AP's web interface. The URL is in the format *http://<ip addr>* or *https://<ip addr>*. If you change this IP address, the login URL also changes.
- **Subnet Mask**—Subnet mask of the network.

  **Note** **IP Address**, **Subnet Mask** and **Gateway** fields are editable only if **Static IP Address** is selected.

- **VRID**—Virtual Router Identifier, is a unique number used to identify a virtual router. By default, the value of VRID is 1 and the configurable range is between 1-255. This option is available only in **Expert View**.

  **Note** Change the VRID only if a VRID conflict is detected in the network. To check if there are any VRID conflicts, go to **Advanced** > **Logging**. In the **Logs** window, the following message will be logged in Errors (3) level: `"%CNFGR-3-VRRP_CONFLICT_DETECTED: cnfgr.c:4856 VRRP group conflict detected with VRID <vrid number>! Configure new VRID value under Wireless Settings > Access Points > Edit AP > Primary AP in Expert View"`

- **Country Code**—Select the country for your Primary AP. It is not advisable to change the country code unless you have not configured the correct country in the initial setup wizard.

**Step 5** Under the **Radio 1** and **Radio 2** tabs you can set the following parameters.

**Note** The **Radio 1** tab corresponds to the 2.4 GHz (802.11 b/g/n) radio on all APs. The **Radio 2** tab corresponds to only the 5 GHz (802.11a/n/ac) radio on all APs.

The radio tab name also indicates the operational radio band within brackets.

| Parameter | Description | |
|---|---|---|
| **Status** | Enable or Disable the corresponding radio on the AP. | |
| **Channel** | For 2.4 GHz, you can set this to Automatic, or set a value from 1 to 11.<br>Selecting **Automatic** enables Dynamic Channel Assignment. This means that channels are dynamically assigned to each AP, under the control of the Primary AP. This prevents neighboring APs from broadcasting over the same channel and prevents interference and other communication problems. For the 2.4 GHz radio, 11 channels are offered in the U.S. and up to 14 in other parts of the world. However, only 1-6-11 can be considered non-overlapping if they are used by neighboring APs.<br>Assigning a specific value statically assigns a channel to that AP. | For 5 GHz, you can set this to Automatic,36,40,44,48,52 (DFS),56 (DFS),60 (DFS),64 (DFS),100 (DFS),104 (DFS),108 (DFS),112 (DFS),116 (DFS),120 (DFS),124 (DFS),128 (DFS),132 (DFS),136 (DFS),140 (DFS),144 (DFS),149,153,157,161 or 165.<br>For the 5 GHz radio, up to 23 non-overlapping channels are offered.<br>Assigning a specific value statically assigns a channel to that AP.<br>**Note** The channels in both the radios will change according to the country configured in the Primary AP.<br>For **Mesh backhaul Radio**, the **Automatic** option is not supported in **Mesh** mode. |
| **Channel Width** | The channel width for 2.4 GHz can only be 20 MHz. | The channel width for 5 GHz can be set to Automatic, or to 20, 40, or 80 MHz, if channel bonding is used. By default, it is set to 80 MHz.<br>Channel bonding groups the channels by 2 or 4 for a single radio stream. This increases the speed and the throughput. Because the number of channels is insufficient in 2.4 GHz, channel bonding cannot be used to enable multiple non-overlapping channels. |

| Parameter | Description |
|---|---|
| **Transmit Power** | You can set it to Automatic, or provide a value ranging from 100, 75, 50, 25, 12 (in terms of percentages).<br>By default, it is set to 100% (maximum power).<br>Selecting **Automatic** adjusts the radio transmitter output power based on the varying signal level at the receiver. This allows the transmitter to operate at less than maximum power for most of the time; when fading conditions occur, transmit power will be increased as required until the maximum is reached.<br>For **Mesh backhaul Radio**, the **Automatic** option is not supported in **Mesh** mode.<br>*Nations apply their own RF emission regulations to the allowable channels, allowed users and maximum power levels within these frequency ranges. As per the regulatory rules, the DFS channels (52 – 144) have low TX power levels compared to non-DFS channels (36-48, 149-165).*<br>Please choose the non DFS channel for maximizing the coverage.<br>In Mesh Mode navigate to: **Wireless Settings** > **Access Points** and click the edit icon at the left end of the row, then select **Radio 2** and **Channel**.<br>In Non-mesh mode: (in Expert view) navigate to: **Advanced** > **RF Optimization** > **Select DCA channels** > **5Ghz** then unselect the DFS channel numbers. |
| **Interferer Detection** | Enable this option to identify the non Wi-Fi devices.<br>**Note** Ensure that you enable the Interferer detection globally under **Advanced > RF Optimization** (in **Expert View**). |

**Step 6** Click **Apply** to save your changes and exit.

**Note** For details on the **Mesh** tab, refer to Mesh Network Components, on page 28.

# Access Point Groups

By creating Access Point Groups you can control which SSIDs or RLANs can be pushed to each AP group. Each access point advertises the enabled WLANs/RLANs that belong to its access point group. The access point does not advertise disabled WLANs/RLANs in its access point group or WLANs/RLANs that belong to another group.

By default, there is a AP Group called **default-group** created on your Primary AP and all the WLANs/RLANs are mapped to this default group. All the access points are also mapped to this default-group. This means, WLAN/RLAN (ID 1-16) will be available in any of the APs belonging to the default group.

**Note** Any AP or Mesh extender added to the network is mapped to the **default-group**. If required, you can create your own AP group and map the AP to the same.

For Mesh deployments, ensure both the Root AP and Mesh AP are mapped to the same Access Point Group.

To configure this, do the following:

1. Switch to **Expert View** by clicking the bi-directional icon on the top right of the Primary AP UI.
2. Go to **Wireless Settings** > **Access Points Groups** > **Add New Group**.
3. In the **General** tab, provide an AP Group Name and a description for your reference.
4. In the **WLANs** tab, select the WLAN or RLAN that you want to push to the group.
5. In the **Access Points** tab, push the access point to the group that you created such that the WLANs/RLANs is advertised in only those particular APs.

**Note** RLANs are supported in non-mesh deployment only.

6. Select the **RF profile** in 2.4 GHz and 5 GHz, if needed. Else, you can create a custom RF Profile. For details, refer to RF Profiles.
7. In the **Ports** tab, enable the LAN ports to which you want to map the RLAN. Thereby, select a particular RLAN from the Remote LAN drop-down list box. This is applicable only in non-mesh deployments.

   By default, LAN1 and PoE is enabled.

**Note** Power over Ethernet- PoE enables Power and Data to be combined onto a single Ethernet cable. For example, IP cameras can be powered up through this port.

8. Click **Apply**.

# Setting a Login Page for WLAN Guest Users

Before you begin, follow these steps to provide guest users with access to your network:

**Step 1** Set up a new WLAN or decide on an existing WLAN, to which you will provide access for guest users. You can also specifically set up a WLAN exclusively for guest access. This is done by setting the **WLAN Security** as **Guest** for that WLAN. For more information, see Adding and Modifying a WLAN, on page 3.

**Step 2** Set up a guest user account. Go to **Wireless Settings > WLAN Users**, and set up an account with the **Guest User** check box selected. For more information, see Viewing and Managing WLAN Users, on page 15.

You can provide the Guest Users of your WLAN with one of the following login page options:

- A simple minimalist default login page with a few modification options. To configure this, see Setting the Default Login Page, on page 25.
- A customized login page uploaded into the Primary AP. To configure this, see Setting a Customized Login Page, on page 25.

# Setting the Default Login Page

Right out of the box, the default login page contains a Cisco logo and Cisco-specific text. You can choose to modify this default login page as described here.

**Step 1** Choose **Wireless Settings** > **Guest WLAN**.

**Step 2** In the **Guest WLANs** page, the number of Guest WLANs currently set up in the network is displayed at the top of the page.

**Step 3** Choose the **Internal (Default)** login page in the **Page Type** drop-down list.

**Step 4** Set the following parameters to modify the default internal login page:

- **Display Cisco Logo**—This field is set to **Yes** by default. To hide the Cisco logo that appears at the top-right corner of the default window, choose **No**. However, you do not have an option to display any other logo.

  **Note** You can preview the changes by clicking **Apply** > **Preview**.

- **Redirect URL After Login**— To have guest users redirected to a particular URL (such as the URL for your company) after login, enter the URL in this field. You can enter up to 254 characters.
- **Page Headline**—The default headline is *Welcome to the Cisco Business Wireless*. To create your own headline on the login page, enter the desired text in this field. You can enter up to 127 characters.
- **Page Message**— The default message is displayed: *Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your unified wireless solution to work.*. To create your own message on the login page, enter the desired text in this field, You can enter up to 2047 characters.

**Step 5** Click **Apply**.

# Setting a Customized Login Page

You can create a custom login page on a computer, compress the page and image files into a .TAR file, and then upload it to the Primary AP. The upload is done via HTTP.

**Note** When you save the Primary AP's configuration, it does not include extra files or components, such as the web authentication bundle, that you download and store on your Primary AP. Hence, manually save external backup copies of such files.

**Note** Cisco TAC is not responsible for creating a custom web authentication bundle.

### Before you begin

Create a custom login page on a computer while ensuring the following:

- Name the login page **`login.html`**. The Primary AP prepares the web authentication URL based on this name. If the server does not find this file after the web authentication bundle has been untarred, the bundle is discarded, and an error message appears.
- The page should not contain more than 5 elements (including HTML, CSS, and Images). This is because the internal Primary AP web server implements a DoS protection mechanism that limits each client to open a maximum of 5 (five) concurrent TCP connections depending on the load. Some browsers may try to open more than 5 TCP sessions at the same time if the page contains more elements and this may result in the page loading slowly depending on how the browser handles the DoS protection.
- Include input text boxes for the username and the password.
- Extract and set the action URL in the page from the original URL.
- Include scripts to decode the return status code.
- All paths used in the main page (to refer to images, for example) are of relative type.
- No filenames within the bundle are longer than 30 characters.

Compress the page and image files into a ,TAR file. The maximum allowed size of the files in their uncompressed state is 1 MB.

Cisco recommends that you use an application that complies with GNU standards to compress the .TAR file (also referred to as the web authentication bundle.). If you load a web authentication bundle with a .TAR compression application that is not GNU compliant, the Primary AP will not be able to extract the files in the bundle.

The .TAR file enters the Primary AP's file system as an untarred file.

**Note** If you have a complex customized web authentication bundle which does not comply with the aforementioned prerequisites, then Cisco recommends that you host it on an external web server.

**Step 1** Choose **Wireless Settings** > **Guest WLAN**.

The **Guest WLANs** page is displayed. The number of Guest WLANs currently set up in the network is displayed at the top of the page.

**Step 2** To upload a customized login page into the Primary AP, in the **Page Type** drop-down list, choose **Customized**.

**Step 3** Click **Upload** and browse to upload the `.TAR` file of the customized web authentication bundle. While uploading the `.TAR` file, the status of file upload is displayed on the same page.

**Step 4** If you want the user to be directed to a particular URL (such as the URL for your company) after login, enter that URL in the **Redirect URL After Login** text box. You can enter up to 254 characters.

**Step 5** Click **Apply**.

Click **Preview** to view your customized web authentication login page.

# About Cisco Mesh

Cisco Mesh introduces a new paradigm of wireless internet access by providing high data rate service and reliability. It is also a solution to reduce the complexity of wiring between each devices in a network. For a stable network establishment, there must be a wireless interacting medium between each APs.

CBW indoor mesh brings these values to you:

- Not having to run Ethernet wiring to each AP.
- Network connectivity where wires cannot provide connectivity.
- Easy to deploy and provide flexibility in deployment.

This chapter summarizes the design details for deploying a Cisco Mesh Extender for indoor environments. The indoor wireless access takes advantage of the growing popularity of inexpensive Wi-Fi clients, enabling new service opportunities and applications that improve user productivity and responsiveness.

### Adding a Mesh Extender

For details refer to Adding Mesh Extenders.

# Convert Non-Mesh to Mesh Deployment

For maintaining, the mesh state between the AP's there must be a communication establishment between them and this takes place through the backhaul radio (2.4GHz or 5GHz – user configurable). To configure the mesh mode in the Primary AP, do the following:

**Step 1** Go to **Wireless Settings**>**Mesh**.

**Step 2** Enable the **Mesh** toggle button and click **Apply**.

**Step 3** The entire network will operate in the **Mesh** mode after the Primary AP reboots.

**Step 4** Add the MAC address of the Mesh Extenders in the auth-list that you wish to join the network.

**Note** For details refer, Adding Mesh Extenders.

For the wired access points (CBW140AC, CBW240AC, CBW145AC) the MAC address will be added automatically in the Local MAC Address table, provided they exist in the same network.

**Step 5** The automatic entry of the physical address of the wired AP can be verified by knowing its last few digits in the MAC address.

For example, when a CBW140AC has joined the Primary AP, its MAC address will be displayed in the Local MAC Address table with its corresponding description as (CBW140AC-f898). Here, **f898** is the ending digits of its MAC address *A4:53:39:0E:F8:98*.

**Step 6** Wait for few minutes and navigate to **Wireless Settings>Access Points**.

**Step 7** Check if the access point has joined the Primary AP.

# Mesh Network Components

Navigate to **Wireless Settings** > **Access Points**. Click **Edit Access point**. The following options are available under the **Mesh** tab.

- **AP Role**—By default, the Primary/Primary Capable AP role is set to **Root** and the mesh extenders role is set to **Mesh**. You can configure the AP Role for Primary Capable APs from Root/Mesh to Mesh/Root. This option is configurable in **Expert View**. After changing the AP Role, the Primary Capable AP will reload and join the Primary AP.

  To check the AP role and type, navigate to **Wireless Settings** > **Access Points**.

  If the Primary Capable AP role is changed from **Root** to **Mesh**, the type will be displayed as **Mesh Extender**. The AP will join as a **Wired Mesh Extender** if a wired uplink is present. If not present, the AP will join as **Wireless Mesh Extender**. In either case, the functionality of Mesh Extender remains the same.

  If the Primary Capable AP role is changed from **Mesh** to **Root**, the Type will be displayed as **Primary Capable**.

**Note**

- Only Primary Capable APs (CBW140AC, CBW145AC, CBW240AC) are allowed to change the AP role.
- Primary Capable APs that are operating with AP Role as **Mesh**, will not be considered for Primary AP selection.

- **Bridge Type**—By default, it is set as **indoor**
- **Bridge Group Name**—Bridge group names (BGNs) control the association of mesh access points. BGNs can logically group radios to avoid two networks on the same channel from communicating with each other. The setting is also useful if you have more than one Primary capable AP in your network in the same sector (area). Default BGN is set with first 10 characters of the configured SSID during initial setup wizard. This option is available in **Expert View**.

**Caution** Exercise caution when you configure a BGN on a live network. Always start a BGN assignment from the farthest-most node (last node, bottom of mesh tree) and move up toward the RAP to ensure that no mesh access points are dropped due to old and new BGNs mixed within the same network.

- **Strict Matching BGN**—When Strict Match BGN is enabled on the mesh AP, it will scan ten times to find the matched BGN parent. After ten scans, if the AP does not find the parent with matched BGN, it will connect to the non-matched BGN and maintain the connection for 15 minutes. After 15 minutes, the AP will again scan ten times and this cycle continues. The default BGN functionalities remain the same when Strict Match BGN is enabled. By default, it is **disabled**. This option is available in **Expert View**.
- **Preferred Parent**—This has to be computed from the Radio MAC of the Primary capable AP which you would like to set as preferred parent your Mesh AP. We need to add 11 in hex to last two bytes of the Preferred Parent's radio MAC. To obtain the Radio MAC of the Primary capable AP, go to **Monitoring** > **Access Points**, and the view the AP details by selecting the AP you want. Note down the Radio MAC

(xx:xx:xx:xx:xx:yy) and compute the value to be set in **Preferred Parent** field. Refer the table for sample computation.

**Note** This field is present only in Mesh Extender's **Mesh** tab.

| Before (yy) | After adding (+11) (yy') |
|---|---|
| 20 | 31 |
| 40 | 51 |
| 60 | 71 |
| 80 | 91 |
| A0 | B1 |
| C0 | D1 |
| E0 | F1 |

- **Backhaul Interface**—This displays the type of interface. It can be either 802.11a/n/ac if Mesh Backhaul Slot is 5GHz and 802.11b/g, if Mesh Backhaul Slot is 2.4GHz.
- **Install Mapping on Radio Backhaul**—This option helps to broadcast the SSIDs in backhaul radio such that the client can join the AP using the backhaul radio. By default it is **Enabled**. If you experience Mesh performance or stability issues, you can disable this option to avoid wireless clients joining the backhaul radio.
- **Mesh Backhaul Slot**—The communication between each APs are carried over a particular radio and you can configure it in either 5GHz or 2.4GHz. By default, it is in **5GHz** mode.

**Note** The Backhaul interface configuration done under **Wireless Settings** > **Mesh** > **Mesh Backhaul Slot** is the global configuration. If you want to override it for selected Access Points, you can change the Backhaul interface configuration by navigating to **Wireless Settings** > **Access Points (Edit)** > **Mesh** > **Mesh Backhaul Slot**.

- **Ethernet Bridging**—By using this feature, you can access internet by connecting a wired client to the LAN ports of the APs in the Mesh network. By default, it is **Enabled**.

  Primary APs **(CBW240AC, CBW145AC)** and Mesh Extender **(CBW141AC or CBW143AC with PoE adapter module)** support the Ethernet Bridging functionality.

  Refer LAN port functionality for different models to know the LAN port functionalities for different model APs.

  Ethernet bridging is **enabled** by default in Mesh mode.

  1. Connect a client to the **Ethernet port of CBW240AC or CBW145AC or CBW141ACM or CBW143ACM**.

**Note** The wired client connected to the LAN port of the AP will obtain the IP address in the AP's VLAN network.

2. Check if you are able to access the internet.

**Note** The Primary AP Web UI can be accessed only through the Management IP and not through the URL: *https://ciscobusiness.cisco*.

3. In the **Mesh** mode, the wired client connected to LAN ports will not be displayed in the Primary AP UI.
4. On connecting a client to the Ethernet port, the **Operational Status** changes to **UP**. You can change the VLAN and mode of that LAN port using the following steps. (By Default the Mode is **Access**).

   To configure VLANs, enable VLAN Transparency in **Mesh** Tab under **Wireless Settings > Mesh > VLAN Transparent**. Click on the **Edit** icon to change the configuration of the particular port. The **VLAN Mapping** window is displayed:

   a. Set the **Mode** to **Access** or **Trunk**.

   b. When you select the mode as **Access**, the VLAN Id is 0 by default. This enables the Wired client to obtain the IP in AP's VLAN.

   c. When you select the mode as **Trunk**, you can configure the Native VLAN on that port and other allowable VLANs for incoming or outgoing traffic.

**Note** You can configure the Native VLAN under **Wireless Settings > Access Points > Global AP Configuration > VLAN Tagging**.

# Changing Mesh Parameters

Following are the several mesh configurations that are available in the Primary AP UI under **Wireless Settings > Mesh**.

## Backhaul Client Access

When Backhaul Client Access is enabled, it allows wireless client association over the backhaul radio. The backhaul radio is a 5-GHz radio for most of the Cisco Access Points. This means that a backhaul radio can carry both backhaul traffic and client traffic.

When Backhaul Client Access is disabled, only backhaul traffic is sent over the backhaul radio and client association is over the second radio(s). By default, this option is **Enabled**.

## Mesh Backhaul Radio Resource Management

The Radio Resource Management (RRM) software embedded in the Primary AP acts as a built-in RF engineer to consistently provide real-time RF management of your wireless network. RRM enables the Primary AP to continually monitor their associated lightweight access points for information on traffic load, interference, noise, coverage and other nearby APs.

The RRM measurement in the mesh AP backhaul is enabled, if the wired Root AP has Ethernet uplink and there is no Mesh Extender joined to it.

## Mesh Backhaul Slot

**Note** The Backhaul interface configuration done under **Wireless Settings** > **Mesh** > **Mesh Backhaul Slot** is the global configuration. If you want to override it for selected Access Points, you can change the Backhaul interface configuration by navigating to **Wireless Settings** > **Access Points > (Edit)** > **Mesh** > **Mesh Backhaul Slot**.

In certain countries, Mesh Network with 5 GHz backhaul network is not allowed to use. Even in countries which is permitted with 5 GHz, customers may prefer to use 2.4 GHz radio frequencies to achieve much larger Mesh or Bridge distances.

When a Primary AP downlink backhaul is changed from 5 to 2.4 GHz or from 2.4GHz to 5 GHz, that selection gets propagated from Primary AP to all the Subordinate APs and they will disconnect from the previously configured channel to get reconnected to another channel. To do this, follow the instructions below:

**Step 1** Go to **Wireless Settings>Mesh>Mesh Backhaul Slot**.

**Step 2** Select the **backhaul radio** (either 5 GHz or 2.4GHz) in the Primary AP such that the configuration gets pushed to its subordinate APs to have a better mesh coverage.

**Note** Only Primary capable APs are configured with the backhaul frequency of 5 or 2.4GHz. Once the AP is configured, the same frequency selection will propagate down the branch to all the Subordinate APs.

## Modifying AP Port Configuration to Access/Trunk Mode

**Note** AP port configuration is applicable only to CBW240AC, CBW145AC, and CBW143ACM APs.

**Step 1** Go to **Wireless Settings** > **Access Points**.

**Step 2** Click **Edit AP**.

**Step 3** In the **Mesh** tab, ensure that the **Ethernet Bridging** is enabled.

**Step 4** Click **Edit** in the Port table. This is available when **Ethernet Bridging** is enabled.

**Step 5** In the **Mode** tab, select **Access** or **Trunk**.

**Step 6** In the **VLAN Id**, specify the VLAN.

The Operational Status changes to UP when an ethernet port is connected to a client.

## VLAN Transparent

This feature determines how a mesh access point handles VLAN tags for Ethernet bridged traffic. If **VLAN Transparent** is enabled, then VLAN tags are not handled and packets are bridged as untagged packets. To configure, go to **Wireless Settings** > **Mesh** > **Ethernet Bridging**.

**Note** No configuration of Ethernet ports is required when VLAN transparent is enabled. The Ethernet port passes both tagged and untagged frames without interpreting the frames.

If **VLAN Transparent** is disabled, then all packets are handled according to the VLAN configuration on the port (trunk, access mode). For details, see Modifying AP Port Configuration to Access/Trunk Mode, on page 31.

**Note**

- If the Ethernet port is set to Trunk mode, then Ethernet VLAN tagging must be configured.
- To use VLAN tagging, you must uncheck the VLAN Transparent check box. By default, it is enabled.

To enable the VLAN Transparent, do the following:

**Step 1** Navigate to **Wireless Settings>Mesh>Ethernet bridging**.

**Step 2** Enable **VLAN Transparent**.