



## WLANs

---

- [Information About WLANs, on page 1](#)
- [Prerequisites for WLANs, on page 4](#)
- [Restrictions for WLANs, on page 4](#)
- [How to Configure WLANs, on page 6](#)
- [Verifying WLAN Properties \(CLI\), on page 28](#)
- [Verifying WLAN-VLAN Information for an AP, on page 28](#)
- [Verifying a WLAN Radio Policy, on page 29](#)

## Information About WLANs

This feature enables you to control WLANs for lightweight access points. Each WLAN has a separate WLAN ID, a separate profile name, and a WLAN SSID. All access points can advertise up to 16 WLANs. However, you can create up to 4096 WLANs and then selectively advertise these WLANs (using profiles and tags) to different access points for better manageability.

You can configure WLANs with different SSIDs or with the same SSID. An SSID identifies the specific wireless network that you want the device to access.



---

**Note** The **wireless client max-user-login concurrent** command will work as intended even if the **no configure max-user-identity response** command is configured.

---



---

**Note** We recommend that you configure the **password encryption aes** and the **key config-key password-encrypt key** commands to encrypt your password.

---



---

**Note** From Cisco IOS XE Cupertino 17.7.1 release onwards, only 8 WLANs are broadcasted on 6-GHz band.

---



---

**Note** For C9105, C9115, and C9120 APs, when a new WLAN is pushed from the controller and if the existing WLAN functional parameters are changed, the other WLAN clients will disconnect and reconnect.

---

## Band Selection

Band select enables client radios that are capable of dual-band (2.4 and 5-GHz) operations to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave ovens, and cordless phones as well as co-channel interference from other access points because of the 802.11b/g limit of 3 nonoverlapping channels. To prevent these sources of interference and improve overall network performance, configure band selection on the device.

## Off-Channel Scanning Deferral

A lightweight access point, in normal operational conditions, periodically goes off-channel and scans another channel. This is in order to perform RRM operations such as the following:

- Transmitting and receiving Neighbor Discovery Protocol (NDP) packets with other APs.
- Detecting rogue APs and clients.
- Measuring noise and interference.

During the off-channel period, which normally is about 70 milliseconds, the AP is unable to transmit or receive data on its serving channel. Therefore, there is a slight impact on its performance and some client transmissions might be dropped.

While the AP is sending and receiving important data, it is possible to configure off-channel scanning deferral so that the AP does not go off-channel and its normal operation is not impacted. You can configure off-channel scanning deferral on a per-WLAN basis, per WMM UP class basis, with a specified time threshold in milliseconds. If the AP sends or receives, on a particular WLAN, a data frame marked with the given UP class within the specified threshold, the AP defers its next RRM off-channel scan. For example, by default, off-channel scanning deferral is enabled for UP classes 4, 5, and 6, with a time threshold of 100 milliseconds. Therefore, when RRM is about to perform an off-channel scan, a data frame marked with UP 4, 5, or 6 is received within the last 100 milliseconds, RRM defers going off-channel. The AP radio does not go off-channel when a voice call sending and receiving audio samples is marked as UP class 6 for every active 20 milliseconds.

Off-channel scanning deferral does come with a tradeoff. Off-channel scanning can impact throughput by 2 percent or more, depending on the configuration, traffic patterns, and so on. Throughput can be slightly improved if you enable off-channel scanning deferral for all traffic classes and increase the time threshold. However, by not going off-channel, RRM can fail to identify AP neighbors and rogues, resulting in negative impact to security, DCA, TPC, and 802.11k messages.

## DTIM Period

In the 802.11 networks, lightweight access points broadcast a beacon at regular intervals, which coincides with the Delivery Traffic Indication Map (DTIM). After the access point broadcasts the beacon, it transmits any buffered broadcast and multicast frames based on the value set for the DTIM period. This feature allows power-saving clients to wake up at the appropriate time if they are expecting broadcast or multicast data.

Typically, the DTIM value is set to 1 (to transmit broadcast and multicast frames after every beacon) or 2 (to transmit broadcast and multicast frames after every other beacon). For instance, if the beacon period of the 802.11 network is 100 ms and the DTIM value is set to 1, the access point transmits buffered broadcast and multicast frames for 10 times every second. If the beacon period is 100 ms and the DTIM value is set to 2, the access point transmits buffered broadcast and multicast frames for 5 times every second. Either of these settings are suitable for applications, including Voice Over IP (VoIP), that expect frequent broadcast and multicast frames.

However, the DTIM value can be set as high as 255 (to transmit broadcast and multicast frames after every 255th beacon). The only recommended DTIM values are 1 and 2; higher DTIM values will likely cause communications problems.



---

**Note** A beacon period, which is specified in milliseconds on the device, is converted internally by the software to 802.11 Time Units (TUs), where 1 TU = 1.024 milliseconds. Depending on the AP model, the actual beacon period may vary slightly; for example, a beacon period of 100 ms may in practice equate to 104.448 ms.

---

## WLAN Radio Policy

The existing WLAN feature allows you to broadcast WLAN on a specified radio on all the applicable slots. With the WLAN Radio Policy feature, you can broadcast the WLAN on the corresponding slot. Note that this option is supported only on 5-GHz band.

## Restrictions for WLAN Radio Policy

- WLAN is pushed to all the radios only if the following configuration is used:
  - WPA3 + AES cipher + 802.1x-SHA256 AKM
  - WPA3 + AES cipher + OWE AKM
  - WPA3 + AES cipher + SAE AKM
  - WPA3 + CCMP256 cipher + SUITEB192-1X AKM
  - WPA3 + GCMP256 cipher + SUITEB-1X AKM
  - WPA3 + GCMP128 cipher + SUITEB192-1X AKM

## Prerequisites for Configuring Cisco Client Extensions

- The software supports CCX versions 1 through 5, which enables devices and their access points to communicate wirelessly with third-party client devices that support CCX. CCX support is enabled automatically for every WLAN on the device and cannot be disabled. However, you can configure Aironet information elements (IEs).
- If Aironet IE support is enabled, the access point sends an Aironet IE 0x85 (which contains the access point name, load, number of associated clients, and so on) in the beacon and probe responses of this WLAN, and the device sends Aironet IEs 0x85 and 0x95 (which contains the management IP address

of the device and the IP address of the access point) in the reassociation response if it receives Aironet IE 0x85 in the reassociation request.

## Peer-to-Peer Blocking

Peer-to-peer blocking is applied to individual WLANs, and each client inherits the peer-to-peer blocking setting of the WLAN to which it is associated. Peer-to-Peer enables you to have more control over how traffic is directed. For example, you can choose to have traffic bridged locally within the device, dropped by the device, or forwarded to the upstream VLAN.

Peer-to-peer blocking is supported for clients that are associated with local and central switching WLANs.



---

**Note** Peer-to-peer blocking feature is VLAN-based. WLANs using the same VLAN has an impact, if Peer-to-peer blocking feature is enabled.

---

## Diagnostic Channel

You can choose a diagnostic channel to troubleshoot why the client is having communication problems with a WLAN. You can test the client and access points to identify the difficulties that the client is experiencing and allow corrective measures to be taken to make the client operational on the network. You can use the device GUI or CLI to enable the diagnostic channel, and you can use the device **diag-channel** CLI to run the diagnostic tests.



---

**Note** We recommend that you enable the diagnostic channel feature only for non-anchored SSIDs that use the management interface. CCX Diagnostic feature has been tested only with clients having Cisco ADU card

---

## Prerequisites for WLANs

- You can associate up to 16 WLANs with each access point group and assign specific access points to each group. Each access point advertises only the enabled WLANs that belong to its access point group. The access point (AP) does not advertise disabled WLANs in its access point group or WLANs that belong to another group.
- We recommend that you assign one set of VLANs for WLANs and a different set of VLANs for management interfaces to ensure that devices properly route VLAN traffic.

## Restrictions for WLANs

- Do not configure PSK and CCKM in a WLAN, as this configuration is not supported and impacts client join flow.
- Ensure that TKIP or AES ciphers are enabled with WPA1 configuration, else ISSU may break during upgrade process.

- When you change the WLAN profile name, then FlexConnect APs (using AP-specific VLAN mapping) will become WLAN-specific. If FlexConnect Groups are configured, the VLAN mapping will become Group-specific.
- Do not enable IEEE 802.1X Fast Transition on Flex Local Authentication enabled WLAN, as client association is not supported with Fast Transition 802.1X key management.
- Peer-to-peer blocking does not apply to multicast traffic.
- In FlexConnect, peer-to-peer blocking configuration cannot be applied only to a particular FlexConnect AP or a subset of APs. It is applied to all the FlexConnect APs that broadcast the SSID.
- The WLAN name and SSID can have up to 32 characters.
- WLAN and SSID names support only the following ASCII characters:
  - Numerals: 48 through 57 hex (0 to 9)
  - Alphabets (uppercase): 65 through 90 hex (A to Z)
  - Alphabets (lowercase): 97 through 122 hex (a to z)
  - ASCII space: 20 hex
  - Printable special characters: 21 through 2F, 3A through 40, and 5B through 60 hex, that is: ! " # \$ % & ' ( ) \* + , - . / : ; < = > ? @ [ \ ] ^ \_ ` { | } ~
- WLAN name cannot be a keyword; for example, if you try to create a WLAN with the name as 's' by entering the **wlan s** command, it results in shutting down all WLANs because 's' is used as a keyword for shutdown.
- You cannot map a WLAN to VLAN 0. Similarly, you cannot map a WLAN to VLANs 1002 to 1006.
- Dual stack clients with a static-IPv4 address is not supported.
- In a dual-stack with IPv4 and IPv6 configured in the Cisco 9800 controller, if an AP tries to join controller with IPv6 tunnel before its IPv4 tunnel gets cleaned, you would see a traceback and AP join will fail.
- When creating a WLAN with the same SSID, you must create a unique profile name for each WLAN.
- When multiple WLANs with the same SSID get assigned to the same AP radio, you must have a unique Layer 2 security policy so that clients can safely select between them.
- The SSID that is sent as part of the user profile will work only if **aaa override** command is configured.
- RADIUS server overwrite is not configured on a per WLAN basis, but rather on a per AAA server group basis.
- Downloadable ACL (DACL) is supported only on the central switching mode. It is not supported for Flex Local switching or on the Cisco Embedded Wireless Controller.
- You cannot mix open configuration models with CLI-based, GUI-based, or Catalyst Center-based configurations. However, if you decide to use multiple model types, they must remain independent of each other. For example, in open configuration models, you can only manage configurations that have been created using an open configuration model, not a CLI-based or GUI-based model. Configurations that are created using open configuration models cannot be modified using a GUI-based model, or CLI-based model, or any other model.

- When you are configuring **dot11bg 11g** command and **radio dot11bg** or **radio dot11g** command, the clients can still connect in 5GHz radio. In this scenario, the client association needs to be blocked. This option is only available on a 2.4-GHz radio.

**Caution**

Some clients might not be able to connect to WLANs properly if they detect the same SSID with multiple security policies. Use this WLAN feature with care.

## How to Configure WLANs

### WLAN Wizard

A wireless local-area network (WLAN) is a group of devices that form a network based on radio transmissions rather than wired connections. The WLAN Wizard on the WebUI is a simplified workflow designed to help you quickly create a WLAN and setup some primary configurations for your specific deployment.

The Wizard supports the following wireless deployment modes:

- **Local mode:** In Local mode, the WLAN is broadcast in the campus locally.
- **Flex Connect mode:** In FlexConnect mode, the WLAN is broadcast remotely across the WAN in a branch.
- **Guest CWA mode:** In Guest CWA mode, the WLAN is created for guest access with Central Web Authentication (CWA).

There are different authentication methods supported for each deployment mode.

To configure a WLAN for your preferred wireless deployment mode using the WLAN wizard on the WebUI, go to **Configuration > Wireless Setup > WLAN Wizard**.

You can also navigate to the WLAN Wizard by the following paths:

- On the Toolbar, click on the **Wireless Setup** icon and select **WLAN Wizard** from the drop-down list.
- On the left navigation pane, go to **Configuration > Tags & Profiles > WLANs** and click on **WLAN Wizard** on the top-right corner.

On the **WLAN Wizard** page, select a wireless deployment mode for the WLAN to initiate steps for setting up the WLAN with profiles, authentication methods, tags, and APs and other configurations.

### Local Mode

The WLAN is deployed in Local mode when the WLAN is present in an office setup with no branch offices. In local mode, an AP creates two CAPWAP tunnels to the controller. One is for management, the other is data traffic. This behavior is known as "centrally switched" because the data traffic is tunneled (bridged) from the AP to the controller where it is then routed by some routing device. Locally switched means the traffic is terminated at the local switch adjacent to the access point.



## Authentication Method

To configure a WLAN for local mode, select the preferred authentication method from the left panel. The authentication method sets the method by which a client can access the WLAN and decides the level of security on the WLAN. The options are:

- **PSK:** A Pre-Shared Key (PSK) is a unique key created for individuals or groups of users on the same SSID. A client will have to enter the PSK to be authenticated and allowed to access the WLAN.
- **Dot1x:** The client must go through relevant EAP authentication model to start exchanging traffic in the WLAN.
- **Local Web Authentication:** The controller intercepts http(s) traffic and redirects the client to the internal web page for authentication.
- **External Web Authentication:** The controller intercepts http(s) traffic and redirects the client to the login page hosted on the external web server for authentication.
- **Central Web Authentication:** The controller redirects all web traffic from the client to the ISE login page for authentication.

## WLAN Profile and Policy

After selecting the Authentication method, click on **WLAN** on the left panel to enter the WLAN profile and policy details.

The WLAN profile defines the properties of a WLAN such as Profile Name, Status, WLAN ID, L2 and L3 Security parameters, AAA Server associated with this SSID and other parameters that are specific to a particular WLAN. The policy profile defines the network policies and the switching policies for a client (with the exception of QoS), which constitute the AP policies as well.

### Procedure

- 
- Step 1** In the **Network Name** section, enter a **WLAN profile name**, which is a unique name for your wireless network. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.
  - Step 2** Enter a valid **SSID** for the WLAN. A valid SSID can be up to 32 characters and can contain spaces. A valid SSID can be ASCII characters from 0 to 31, with leading and trailing spaces. This is the broadcast name for your WLAN.
  - Step 3** Enter the **WLAN ID**.
  - Step 4** In the **WLAN Policy** section, enter the **Policy Profile name**. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.
  - Step 5** Select the **VLAN** to be associated with the Policy Profile from the drop-down list..

- Step 6** To select an existing Policy Profile for the WLAN, click on **Select Existing** and choose a **Policy Profile** from the drop-down list..
- 

## Authentication Configurations

Set up the authentication configurations and filters for the WLAN depending on the method you have chosen. These include the keys, filters, ACLs, and parameter maps as applicable to the selected authentication method.

### Procedure

---

- Step 1** If you have selected **PSK** as the authentication method, configure the following:
- In the **WLAN > Pre-Shared Key (PSK)** section, select the PSK format. Choose between ASCII and Hexadecimal formats.
  - From the **PSK type** drop-down list, choose if you want the key to be unencrypted or AES encrypted.
  - In the **Pre-Shared Key** field, enter the pass key for the WLAN.
- Step 2** If you have selected **Dot1x** as the authentication method, configure the following:
- In the **WLAN > AAA** tab, configure the AAA server list for the WLAN.
  - Select any of the available AAA servers to add to the WLAN.
  - To add a new AAA server to the list, click on Add New Server and enter the IP address and server-key.
  - To use an already configured AAA server list, click on **Use Existing** and select the appropriate list from the drop-down.
- Step 3** If you have selected **Local Web Authentication** as the authentication method, configure the following:
- In the **WLAN > Parameter Map** tab, configure the parameter map for the WLAN. A parameter map sets parameters that can be applied to subscriber sessions during authentication.
    - In the **Global Configuration** section, configure the global parameter map.
    - Enter an IPv4 or IPv6 address to configure a virtual IP address for redirecting the clients to the login page of the controller.
    - From the Trustpoint drop-down list, select the trustpoint for HTTPS login page. The trustpoint corresponds to the device certificate the controller will use in conjunction with the virtual IP and hostname.
    - In the **WLAN Specific Configuration** section, either create a new parameter map for the WLAN, or select an existing parameter map from the drop-down list.
  - In the **WLAN > Local Users** tab, enter the username in the local database to establish a username-based authentication system.
    - Enter the user name to be saved.
    - From the **Password Encryption** drop-down list, choose if you want the password to be unencrypted or encrypted.
    - In the **Password** field, specify the password the user must enter to gain access to the switch. The password must be from 1 to 25 characters and can contain embedded spaces.
    - Click on the + sign to add the credentials to the database. Add as many user credentials as required.



- Step 4** If you have selected **External Web Authentication** as the authentication method, configure the following:
- a) In the **WLAN > Parameter Map** tab, configure the parameter map for the WLAN.
    1. In the **Global Configuration** section, configure the global parameter map.
    2. Enter an IPv4 or IPv6 address to configure the virtual IP address of the external web authentication login page to which the guest users are redirected.
    3. From the **Trustpoint** drop-down list, select the trustpoint for HTTPS login page. The trustpoint corresponds to the device certificate the controller will use in conjunction with the virtual IP and hostname.
    4. In the **WLAN Specific Configuration** section, either create a new parameter map for the WLAN, or select an existing parameter map from the drop-down list.
    5. To create a new parameter map, enter the parameter-map name.
    6. In the **Redirect URL for login** field, enter the URL of the external server that will host the authentication page for login.
    7. In the **Portal IPV4 Address** field, enter the IPv4 address of the external server to send redirects. If the external server uses an IPv6 address, in the **Portal IPV6 Address** field, enter the IPv6 address of the portal to send redirects.
  - b) In the **WLAN > ACL / URL Filter** tab, configure the ACL rules and the URL filter list.
    1. In the **Pre Auth ACL** section, enter the name of the ACL.
    2. In the **IP address** field, enter the source IP address and the destination IP address. This will configure the ACL to permit packet transfer from and to the specified IP address. You can add as many IP addresses as required.
    3. In the **URL Filter** section, enter a name for the URL Filter list that you are creating.
    4. Use the slider to set the list action to **Permit** or **Deny** the URLs.
    5. Specify the URLs in the **URLs** box. Enter every URL on a new line.
- Step 5** If you have selected Central Web Authentication as the authentication method, configure the following:
- a) In the **WLAN > AAA/ACL** tab, configure the AAA server list and ACL for the WLAN.
  - b) In the **AAA Configuration** section, select any of the available AAA servers to add to the WLAN. This will be the server where the clients will get authenticated.
  - c) To add a new AAA server to the list, click on **Add New Server** and enter the IP address and server-key.
  - d) To use an already configured AAA server list, click on **Use Existing** and select the appropriate list from the drop-down.
  - e) In the **ACL List** section, enter the name of the ACL. This ACL will contain the rules regarding URLs that can be accessed by the client and should match the name configured on the RADIUS server.

## Tags

To configure tags on the WLAN, click on **Tags** from the left panel.

A Tag's property is defined by the policies associated to it. This property is in turn inherited by an associated client/AP. There are various type of tags, each associated to different profiles.

### Procedure

---

- Step 1** In the **Site Configuration** section, either enter a site tag to be added, or select an existing site tag from the drop-down list. You can add as many tags as required. In the local mode, the site tag contains the AP join profile only.
- Step 2** In the **Policy Tag** section, either enter a policy tag to be added, or select an existing policy tag from the drop-down list. You can add as many tags as required. The policy tag constitutes mapping of the WLAN profile to the policy profile. The WLAN profile defines the wireless characteristics of the WLAN. The policy profile defines the network policies and the switching policies for the client.
- Step 3** In the **RF Tag** section, either enter an RF tag to be added, or select an existing RF tag from the drop-down list. You can add as many tags as required. The RF tag contains the 2.4 GHz and 5 GHz RF profiles.
- 

## AP Provisioning

Once the Wireless network and RF characteristics are set up, access points can be added to the local site either using static AP MAC address assignment or by assigning already joined APs to a specific location.

To add tags and associate APs to the WLAN, click on **AP Provisioning** from the left panel.

### Procedure

---

- Step 1** The APs already discovered by the controller are listed in the **Provision Joined APs** tab. You can select the APs to be associated to the WLAN from this table.
- Step 2** To add tags to the selected APs, select the appropriate Policy Tag, Site Tag, and RF Tag from the respective drop-down lists. Click on **Add** to apply the tags.
- Step 3** To add APs manually, click on the **Pre-provision APs** tab. You can either add individual MAC addresses of the APs or upload a CSV file with the AP MAC addresses listed. The added APs will be listed in the table below.
- Step 4** Select the APs to be associated to the WLAN from this table.
- Step 5** To add tags to the selected APs, select the appropriate Policy Tag, Site Tag, and RF Tag from the respective drop-down lists. Click on **Add** to apply the tags.

A table of all the APs and the tags added to them is displayed in the **Selected APs** tab.

- Step 6** Click **Apply**.

This will create a WLAN in local mode with the authentication method, authentication filters, tags, and APs configured on it.

---

## FlexConnect Mode

FlexConnect is a wireless solution for branch office and remote office deployments. It enables you to configure and control access points (AP) in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office. The FlexConnect access points can switch client data traffic and perform client authentication locally when their connection to the controller is lost. An

AP in Flex mode offers network survivability in the event of a loss of connection to the centralized wireless controller.



## Authentication Method

To configure a WLAN for FlexConnect mode, select the preferred authentication method from the left panel. The authentication method sets the method by which a client can access the WLAN and decides the level of security on the WLAN.

The options are:

- **Local Web Authentication:** The controller intercepts http(s) traffic and redirects the client to the internal web page for authentication.
- **External Web Authentication:** The controller intercepts http(s) traffic and redirects the client to the login page hosted on the external web server for authentication.
- **Central Web Authentication:** The controller redirects all web traffic from the client to the ISE login page for authentication.

## WLAN Profile and Policy

After selecting the Authentication method, click on **WLAN** on the left panel to enter the WLAN profile and policy details.

The WLAN profile defines the properties of a WLAN such as Profile Name, Status, WLAN ID, L2 and L3 Security parameters, AAA Server associated with this SSID and other parameters that are specific to a particular WLAN. The policy profile defines the network policies and the switching policies for a client (with the exception of QoS), which constitute the AP policies as well.

### Procedure

- 
- Step 1** In the **Network Name** section, enter a **WLAN profile name**, which is a unique name for your wireless network. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.
  - Step 2** Enter a valid **SSID** for the WLAN. A valid SSID can be up to 32 characters and can contain spaces. A valid SSID can be ASCII characters from 0 to 31, with leading and trailing spaces. This is the broadcast name for your WLAN.
  - Step 3** Enter the **WLAN ID**.
  - Step 4** In the **WLAN Policy** section, enter the **Policy Profile name**. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.
  - Step 5** Select the **VLAN** to be associated with the Policy Profile from the drop-down list..
  - Step 6** To select an existing Policy Profile for the WLAN, click on **Select Existing** and choose a **Policy Profile** from the drop-down list..
-

## Authentication Configurations

Set up the authentication configurations and filters for the WLAN depending on the method you have chosen. These include the keys, filters, ACLs, and parameter maps as applicable to the selected authentication method.

### Procedure

#### Step 1

If you have selected **Local Web Authentication** as the authentication method, configure the following:

- a) In the **WLAN > Parameter Map** tab, configure the parameter map for the WLAN. A parameter map sets parameters that can be applied to subscriber sessions during authentication.
  1. In the **Global Configuration** section, configure the global parameter map.
  2. Enter an IPv4 or IPv6 address to configure a virtual IP address for redirecting the clients to the login page of the controller.
  3. From the **Trustpoint** drop-down list, select the trustpoint for HTTPS login page. The trustpoint corresponds to the device certificate the controller will use in conjunction with the virtual IP and hostname.
  4. In the **WLAN Specific Configuration** section, either create a new parameter map for the WLAN, or select an existing parameter map from the drop-down list.
- b) In the **WLAN > Local Users / Flex** tab, configure a Flex profile and enter the username in the local database to establish a username-based authentication system.
  1. In the **Flex Profile** section, enter the name of the new flex profile and the native VLAN ID.
  2. To use an already existing Flex profile, click on **Select Existing** to choose a profile from the drop-down list and enter the native VLAN ID.
  3. In the **Local Users** section, enter the user name to be saved.
  4. From the **Password Encryption** drop-down list, choose if you want the password to be unencrypted or encrypted.
  5. In the **Password** field, specify the password the user must enter to gain access to the switch. The password must be from 1 to 25 characters and can contain embedded spaces.
  6. Click on the + sign to add the credentials to the database. Add as many user credentials as required.

#### Step 2

If you have selected **External Web Authentication** as the authentication method, configure the following:

- a) In the **WLAN > Parameter Map** tab, configure the parameter map for the WLAN.
  1. In the **Global Configuration** section, configure the global parameter map.
  2. Enter an IPv4 or IPv6 address to configure the virtual IP address of the external web authentication login page to which the guest users are redirected.
  3. From the **Trustpoint** drop-down list, select the trustpoint for HTTPS login page. The trustpoint corresponds to the device certificate the controller will use in conjunction with the virtual IP and hostname.
  4. In the **WLAN Specific Configuration** section, either create a new parameter map for the WLAN, or select an existing parameter map from the drop-down list.

5. To create a new parameter map, enter the parameter-map name.
  6. In the **Redirect URL for login** field, enter the URL of the external server that will host the authentication page for login.
  7. In the **Portal IPv4 Address** field, enter the IPv4 address of the external server to send redirects. If the external server uses an IPv6 address, in the **Portal IPv6 Address** field, enter the IPv6 address of the portal to send redirects.
- b) In the **WLAN > ACL / URL Filter** tab, configure the ACL rules and the URL filter list.
1. In the **Flex Profile** section, enter the name of the new flex profile and the native VLAN ID.
  2. To use an already existing Flex profile, click on **Select Existing** to choose a profile from the drop-down list and enter the native VLAN ID.
  3. In the **Pre Auth ACL** section, enter the name of the ACL.
  4. In the **IP address** field, enter the source IP address and the destination IP address. This will configure the ACL to permit packet transfer from and to the specified IP address. You can add as many IP addresses as required.
  5. In the **URL Filter** section, enter a name for the URL Filter list that you are creating.
  6. Click on **Add** to add the URLs.
  7. Specify the URL to be added to the list and its preference.
  8. Use the slider to set the list action to **Permit** or **Deny** the URLs.
  9. Click **Save**.
- You can add as many URLs to the list as required.
- c) To add a new AAA server to the list, click on Add New Server and enter the IP address and server-key.
- d) To use an already configured AAA server list, click on **Use Existing** and select the appropriate list from the drop-down.

**Step 3**

If you have selected **Central Web Authentication** as the authentication method, configure the following:

- a) In the **WLAN > AAA/ACL** tab, configure the AAA server list and ACL for the WLAN.
- b) In the **AAA Configuration** section, select any of the available AAA servers to add to the WLAN. This will be the server where the clients will get authenticated.
- c) To add a new AAA server to the list, click on **Add New Server** and enter the IP address and server-key.
- d) To use an already configured AAA server list, click on **Use Existing** and select the appropriate list from the drop-down.
- e) In the **Flex Profile** section, enter the name of the new flex profile and the native VLAN ID.
- f) To use an already existing Flex profile, click on **Select Existing** to choose a profile from the drop-down list and enter the native VLAN ID.
- g) In the **ACL List** section, enter the name of the ACL. This ACL will contain the rules regarding URLs that can be accessed by the client and should match the name configured on the RADIUS server.

**Tags**

To configure tags on the WLAN, click on **Tags** from the left panel.

A Tag's property is defined by the policies associated to it. This property is in turn inherited by an associated client/AP. There are various type of tags, each associated to different profiles.

### Procedure

---

- Step 1** In the **Site Configuration** section, either enter a site tag to be added, or select an existing site tag from the drop-down list. You can add as many tags as required. In FlexConnect mode, the site tag contains the AP join profile and the Flex profile.
  - Step 2** In the **Policy Tag** section, either enter a policy tag to be added, or select an existing policy tag from the drop-down list. You can add as many tags as required. The policy tag constitutes mapping of the WLAN profile to the policy profile. The WLAN profile defines the wireless characteristics of the WLAN. The policy profile defines the network policies and the switching policies for the client.
  - Step 3** In the **RF Tag** section, either enter an RF tag to be added, or select an existing RF tag from the drop-down list. You can add as many tags as required. The RF tag contains the 2.4 GHz and 5 GHz RF profiles.
- 

## AP Provisioning

Once the Wireless network and RF characteristics are set up, access points can be added to the local site either using static AP MAC address assignment or by assigning already joined APs to a specific location.

To add tags and associate APs to the WLAN, click on **AP Provisioning** from the left panel.

### Procedure

---

- Step 1** The APs already discovered by the controller are listed in the **Provision Joined APs** tab. You can select the APs to be associated to the WLAN from this table.
  - Step 2** To add tags to the selected APs, select the appropriate Policy Tag, Site Tag, and RF Tag from the respective drop-down lists. Click on **Add** to apply the tags.
  - Step 3** To add APs manually, click on the **Pre-provision APs** tab. You can either add individual MAC addresses of the APs or upload a CSV file with the AP MAC addresses listed. The added APs will be listed in the table below.
  - Step 4** Select the APs to be associated to the WLAN from this table.
  - Step 5** To add tags to the selected APs, select the appropriate Policy Tag, Site Tag, and RF Tag from the respective drop-down lists. Click on **Add** to apply the tags.  
A table of all the APs and the tags added to them is displayed in the **Selected APs** tab.
  - Step 6** Click **Apply**.  
This will create a WLAN in FlexConnect mode with the authentication method, authentication filters, tags, and APs configured on it.
- 

## Guest CWA Mode

The Guest mode addresses the need to provide internet access to guests in a secure and accountable manner with Central Web Authentication as the security method. The implementation of a wireless guest network

uses the enterprise's existing wireless and wired infrastructure to the maximum extent. This solution comprises of two controllers - a Guest Foreign and a Guest Anchor.



## Controller Type

To configure a WLAN for Guest CWA mode, select the type of controller configuration you want to set up on the device from the left panel.

The options are:

- **Foreign:** A Foreign is a controller in the WLAN that exists in the enterprise. A client sends a connection request to a Foreign controller to join the WLAN. It is a dedicated guest WLAN or SSID and is implemented throughout the campus wireless network wherever guest access is required. The Foreign controller manages the anchor controllers.
- **Anchor:** An Anchor is a controller or group of controllers in a WLAN that manage traffic within the network for a guest client. It provides internal security by forwarding the traffic from a guest client to a Cisco Wireless Controller in the demilitarized zone (DMZ) network.

## WLAN Profile and Policy

After selecting the Authentication method, click on **WLAN** on the left panel to enter the WLAN profile and policy details.

The WLAN profile defines the properties of a WLAN such as Profile Name, Status, WLAN ID, L2 and L3 Security parameters, AAA Server associated with this SSID and other parameters that are specific to a particular WLAN. The policy profile defines the network policies and the switching policies for a client (with the exception of QoS), which constitute the AP policies as well.

### Procedure

- 
- Step 1** In the **Network Name** section, enter a **WLAN profile name**, which is a unique name for your wireless network. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.
  - Step 2** Enter a valid **SSID** for the WLAN. A valid SSID can be up to 32 characters and can contain spaces. A valid SSID can be ASCII characters from 0 to 31, with leading and trailing spaces. This is the broadcast name for your WLAN.
  - Step 3** Enter the **WLAN ID**.
  - Step 4** In the **WLAN Policy** section, enter the **Policy Profile name**. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.
  - Step 5** Select the **VLAN** to be associated with the Policy Profile from the drop-down list..
  - Step 6** To select an existing Policy Profile for the WLAN, click on **Select Existing** and choose a **Policy Profile** from the drop-down list..

- Step 7** If you have selected **Foreign**, in the **Mobility Anchors** section, select the IP address of an available controller to assign it as the mobility anchor for the WLAN. This will extend the configurations on the Foreign controller onto the anchor controllers as well.
- 

## Authentication Configurations

For the Guest access mode, the authentication method is Central Web Authentication.

### Procedure

---

- Step 1** In the **WLAN > AAA/ACL** tab, configure the AAA server list and ACL for the WLAN.
- Step 2** In the **AAA Configuration** section, select any of the available AAA servers to add to the WLAN. This will be the server where the clients will get authenticated.
- Step 3** To add a new AAA server to the list, click on **Add New Server** and enter the IP address and server-key.
- Step 4** To use an already configured AAA server list, click on **Use Existing** and select the appropriate list from the drop-down.
- Step 5** In the **ACL List** section, enter the name of the ACL. This ACL will contain the rules regarding URLs that can be accessed by the client and should match the name configured on the RADIUS server.
- 

## Tags

To configure tags on the WLAN, click on **Tags** from the left panel.

A Tag's property is defined by the policies associated to it. This property is in turn inherited by an associated client/AP. There are various type of tags, each associated to different profiles.

### Procedure

---

- Step 1** In the **Site Configuration** section, either enter a site tag to be added, or select an existing site tag from the drop-down list. You can add as many tags as required.
- Step 2** In the **Policy Tag** section, either enter a policy tag to be added, or select an existing policy tag from the drop-down list. You can add as many tags as required. The policy tag constitutes mapping of the WLAN profile to the policy profile. The WLAN profile defines the wireless characteristics of the WLAN. The policy profile defines the network policies and the switching policies for the client.
- Step 3** In the **RF Tag** section, either enter an RF tag to be added, or select an existing RF tag from the drop-down list. You can add as many tags as required. The RF tag contains the 2.4 GHz and 5 GHz RF profiles.
- 

## AP Provisioning

Once the Wireless network and RF characteristics are set up, access points can be added to the local site either using static AP MAC address assignment or by assigning already joined APs to a specific location.

If you have selected **Foreign**, click on **AP Provisioning** from the left panel to add tags and associate APs to the WLAN.



### Procedure

- 
- Step 1** The APs already discovered by the controller are listed in the **Provision Joined APs** tab. You can select the APs to be associated to the WLAN from this table.
- Step 2** To add tags to the selected APs, select the appropriate Policy Tag, Site Tag, and RF Tag from the respective drop-down lists. Click on **Add** to apply the tags.
- Step 3** To add APs manually, click on the **Pre-provision APs** tab. You can either add individual MAC addresses of the APs or upload a CSV file with the AP MAC addresses listed. The added APs will be listed in the table below.
- Step 4** Select the APs to be associated to the WLAN from this table.
- Step 5** To add tags to the selected APs, select the appropriate Policy Tag, Site Tag, and RF Tag from the respective drop-down lists. Click on **Add** to apply the tags.
- A table of all the APs and the tags added to them is displayed in the **Selected APs** tab.
- Step 6** Click **Apply**.
- This will create a WLAN in Guest CWA mode with the authentication method, mobility anchors, authentication filters, tags, and APs configured on it.
- 

## Creating WLANs (GUI)

### Procedure

- 
- Step 1** In the **Configuration > Tags & Profiles > WLANs** page, click **Add**.
- The **Add WLAN** window is displayed.
- Step 2** Under the **General** tab and **Profile Name** field, enter the name of the WLAN. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.
- Step 3** Click **Save & Apply to Device**.
- 

## Creating WLANs (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<code>wlan profile-name wlan-id [ssid]</code>	Specifies the WLAN name and ID:

	Command or Action	Purpose
	<b>Example:</b> <pre>Device(config)# wlan mywlan 34 mywlan-ssid</pre>	<ul style="list-style-type: none"> <li>For the <i>profile-name</i>, enter the profile name. The range is from 1 to 32 alphanumeric characters.</li> <li>For the <i>wlan-id</i>, enter the WLAN ID. The range is from 1 to 512.</li> <li>For the <i>ssid</i>, enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID.</li> </ul> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>You can create SSID using GUI or CLI. However, we recommend that you use CLI to create SSID.</li> <li>By default, the WLAN is disabled.</li> </ul>
<b>Step 3</b>	<pre>end</pre> <b>Example:</b> <pre>Device(config)# end</pre>	Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.

## Deleting WLANs (GUI)

### Procedure

- 
- Step 1** In the **Configuration > Tags & Profiles > WLANs** page, check the checkbox adjacent to the WLAN you want to delete.
- To delete multiple WLANs, select multiple WLANs checkboxes.
- Step 2** Click **Delete**.
- Step 3** Click **Yes** on the confirmation window to delete the WLAN.
- 

## Deleting WLANs

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<pre>configure terminal</pre> <b>Example:</b>	Enters global configuration mode.

	Command or Action	Purpose
	Device# <code>configure terminal</code>	
<b>Step 2</b>	<p><code>no wlan wlan-name wlan-id ssid</code></p> <p><b>Example:</b></p> <p>Device(config)# <code>no wlan test2</code></p>	<p>Deletes the WLAN. The arguments are as follows:</p> <ul style="list-style-type: none"> <li>• The <i>wlan-name</i> is the WLAN profile name.</li> <li>• The <i>wlan-id</i> is the WLAN ID.</li> <li>• The <i>ssid</i> is the WLAN SSID name configured for the WLAN.</li> </ul> <p><b>Note</b> If you delete a WLAN that is part of an AP group, the WLAN is removed from the AP group and from the AP's radio.</p>
<b>Step 3</b>	<p><code>end</code></p> <p><b>Example:</b></p> <p>Device(config)# <code>end</code></p>	<p>Returns to privileged EXEC mode. Alternatively, you can also press <b>Ctrl-Z</b> to exit global configuration mode.</p>

## Searching WLANs (CLI)

To verify the list of all WLANs configured on the controller, use the following show command:

```
Device# show wlan summary
Number of WLANs: 4
```

WLAN Profile Name	SSID	VLAN	Status
1 test1	test1-ssid	137	UP
3 test2	test2-ssid	136	UP
2 test3	test3-ssid	1	UP
45 test4	test4-ssid	1	DOWN

To use wild cards and search for WLANs, use the following show command:

```
Device# show wlan summary | include test-wlan-ssid
1 test-wlan test-wlan-ssid 137 UP
```

## Enabling WLANs (GUI)

### Procedure

- Step 1** Choose **Configuration > Tags & Profiles > WLANs**.
- Step 2** On the **WLANs** page, click the WLAN name.
- Step 3** In the **Edit WLAN** window, toggle the **Status** button to **ENABLED**.

**Step 4** Click **Update & Apply to Device**.

## Enabling WLANs (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>wlan <i>profile-name</i></b> <b>Example:</b> Device(config)# <code>wlan test4</code>	Enters WLAN configuration submode. The <i>profile-name</i> is the profile name of the configured WLAN.
<b>Step 3</b>	<b>no shutdown</b> <b>Example:</b> Device(config-wlan)# <code>no shutdown</code>	Enables the WLAN.
<b>Step 4</b>	<b>end</b> <b>Example:</b> Device(config-wlan)# <code>end</code>	Returns to privileged EXEC mode.

## Disabling WLANs (GUI)

### Procedure

- Step 1** Choose **Configuration > Tags & Profiles > WLANs**.
- Step 2** In the **WLANs** window, click the WLAN name.
- Step 3** In the **Edit WLAN** window, set the **Status** toggle button as **DISABLED**.
- Step 4** Click **Update & Apply to Device**.

## Disabling WLANs (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b>	Enters global configuration mode.

	Command or Action	Purpose
	Device# <code>configure terminal</code>	
<b>Step 2</b>	<b>wlan</b> <i>profile-name</i> <b>Example:</b> Device(config)# <code>wlan test4</code>	Enters WLAN configuration submode. The <i>profile-name</i> is the profile name of the configured WLAN.
<b>Step 3</b>	<b>shutdown</b> <b>Example:</b> Device(config-wlan)# <code>shutdown</code>	Disables the WLAN.
<b>Step 4</b>	<b>end</b> <b>Example:</b> Device(config-wlan)# <code>end</code>	Returns to privileged EXEC mode.
<b>Step 5</b>	<b>show wlan summary</b> <b>Example:</b> Device# <code>show wlan summary</code>	Displays the list of all WLANs configured on the device. You can search for the WLAN in the output.

## Configuring General WLAN Properties (CLI)

You can configure the following properties:

- Media stream
- Broadcast SSID
- Radio

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>wlan</b> <i>profile-name</i> <b>Example:</b> Device(config)# <code>wlan test4</code>	Enters WLAN configuration submode. The <i>profile-name</i> is the profile name of the configured WLAN.
<b>Step 3</b>	<b>shutdown</b> <b>Example:</b> Device(config-wlan)# <code>shutdown</code>	Disables the WLAN.
<b>Step 4</b>	<b>broadcast-ssid</b> <b>Example:</b>	Broadcasts the SSID for this WLAN.

	Command or Action	Purpose
	Device(config-wlan)# <b>broadcast-ssid</b>	
<b>Step 5</b>	<b>dot11bg 11g</b> <b>Example:</b> Device(config-wlan)# <b>dot11bg 11g</b>	Configures the WLAN radio policy for dot11 radios.  Also see the section: Configuring a WLAN Radio Policy.
<b>Step 6</b>	<b>media-stream multicast-direct</b> <b>Example:</b> Device(config-wlan)# <b>media-stream multicast-direct</b>	Enables multicast VLANs on this WLAN.
<b>Step 7</b>	<b>no shutdown</b> <b>Example:</b> Device(config-wlan)# <b>no shutdown</b>	Enables the WLAN.
<b>Step 8</b>	<b>end</b> <b>Example:</b> Device(config-wlan)# <b>end</b>	Returns to privileged EXEC mode.

## Configuring Advanced WLAN Properties (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>wlan <i>profile-name</i></b> <b>Example:</b> Device(config)# <b>wlan test4</b>	Enters WLAN configuration submenu. The <i>profile-name</i> is the profile name of the configured WLAN.
<b>Step 3</b>	<b>chd</b> <b>Example:</b> Device(config-wlan)# <b>chd</b>	Enables coverage hole detection for this WLAN.
<b>Step 4</b>	<b>ccx aironet-iesupport</b> <b>Example:</b> Device(config-wlan)# <b>ccx aironet-iesupport</b>	Enables support for Aironet IEs for this WLAN.

	Command or Action	Purpose
Step 5	<b>client association limit</b> { <i>clients-per-wlan</i>   <b>ap</b> <i>clients-per-ap-per-wlan</i>   <b>radioclients-per-ap-radio--per-wlan</b> }  <b>Example:</b> Device(config-wlan)# <b>client association limit ap 400</b>	Sets the maximum number of clients, clients per AP, or clients per AP radio that can be configured on a WLAN.
Step 6	<b>ip access-group web</b> <i>acl-name</i>  <b>Example:</b> Device(config-wlan)# <b>ip access-group web test-acl-name</b>	Configures the IPv4 WLAN web ACL. The variable <i>acl-name</i> specifies the user-defined IPv4 ACL name.
Step 7	<b>peer-blocking</b> [ <b>allow-private-group</b>   <b>drop</b>   <b>forward-upstream</b> ]  <b>Example:</b> Device(config-wlan)# <b>peer-blocking drop</b>	Configures peer to peer blocking parameters. The keywords are as follows: <ul style="list-style-type: none"> <li>• <b>allow-private-group</b>—Enables peer-to-peer blocking on the Allow Private Group action.</li> <li>• <b>drop</b>—Enables peer-to-peer blocking on the drop action.</li> <li>• <b>forward-upstream</b>—No action is taken and forwards packets to the upstream.</li> </ul> <p><b>Note</b> The <b>forward-upstream</b> option is not supported for Flex local switching. Traffic is dropped even if this option is configured. Also, peer to peer blocking for local switching SSIDs are available only for the clients on the same AP.</p>
Step 8	<b>channel-scan</b> { <b>defer-priority</b> { <b>0-7</b> }   <b>defer-time</b> { <b>0 - 6000</b> } }  <b>Example:</b> Device(config-wlan)# <b>channel-scan defer-priority 6</b>	Sets the channel scan defer priority and defer time. The arguments are as follows: <ul style="list-style-type: none"> <li>• <b>defer-priority</b>—Specifies the priority markings for packets that can defer off-channel scanning. The range is from 0 to 7. The default is 3.</li> <li>• <b>defer-time</b>—Deferral time in milliseconds. The range is from 0 to 6000. The default is 100.</li> </ul>
Step 9	<b>end</b>  <b>Example:</b> Device(config-wlan)# <b>end</b>	Returns to privileged EXEC mode.

## Configuring Advanced WLAN Properties (GUI)

### Before you begin

Ensure that you have configured an AP Join Profile prior to configuring the primary and backup controllers.

### Procedure

---

- Step 1** Choose **Configuration > Tags & Profiles > WLANs** .
- Step 2** Click **Add**.
- Step 3** Under the **Advanced** tab, check the **Coverage Hole Detection** check box.
- Step 4** Check the **Aironet IE** check box to enable Aironet IE on the WLAN.
- Step 5** Check the **Diagnostic Channel** check box to enable diagnostic channel on the WLAN.
- Step 6** From the **P2P Blocking Action** drop-down list, choose the required value.
- Step 7** Set the **Multicast Buffer** toggle button as enabled or disabled.
- Step 8** Check the **Media Stream Multicast-Direct** check box to enable the feature.
- Step 9** In the **Max Client Connections** section, specify the maximum number of client connections for the following:
- In the **Per WLAN** field, enter a value. The valid range is between 0 and 10000.
  - In the **Per AP Per WLAN** field, enter a value. The valid range is between 0 and 400.
  - In the **Per AP Radio Per WLAN** field, enter a value. The valid range is between 0 and 200.
- Step 10** In the **11v BSS Transition Support** section, perform the following configuration tasks:
- a) Check the **BSS Transition** check box to enable 802.11v BSS Transition support.
  - b) In the **Disassociation Imminent** field, enter a value. The valid range is between 0 and 3000.
  - c) In the **Optimized Roaming Disassociation Timer** field, enter a value. The valid range is between 0 and 40.
  - d) Select the check box to enable the following:
    - BSS Max Idle Service
    - BSS Max Idle Protected
    - Disassociation Imminent Service
    - Directed Multicast Service
    - Universal Admin
    - Load Balance
    - Band Select
    - IP Source Guard
- Step 11** In the **11ax** section, perform the following configuration tasks:
- a) Select the check box to enable the following:
    - Check the **Enable 11ax** checkbox to enable 802.11ax operation status on the WLAN.



- Check the **Downlink OFDMA** and **Uplink OFDMA** check boxes to enable downlink and uplink connections that use OFDMA.

Orthogonal Frequency Division Multiple Access (OFDMA) is a channel access mechanism that assures contention-free transmission to multiple clients in both the downlink (DL) and uplink (UL) within a respective single transmit opportunity.

- Check the **Downlink MU-MIMO** and **Uplink MU-MIMO** check boxes to enable downlink and uplink connections that use MU-MIMO.

With Multiuser MIMO (MU-MIMO), an AP can use its antenna resources to transmit multiple frames to different clients, all at the same time and over the same frequency spectrum.

- Enable the target wake up time configuration on the WLAN by checking the **BSS Target Wake Up Time** checkbox.

Target wake up time allows an AP to manage activity in the Wi-Fi network to minimize medium contention between stations, and to reduce the required amount of time that a station in the power-save mode needs to be awake. This is achieved by allocating stations to operate at non-overlapping times, and/or frequencies, and concentrate the frame exchanges in predefined service periods.

- Check the **Universal Admin** check box to enable Universal Admin support for the WLAN.
- Enable OKC on the WLAN by checking the **OKC** check box. Opportunistic Key Caching (OKC) allows the wireless client and the WLAN infrastructure to cache only one Pairwise Master Key (PMK) for the lifetime of the client association with this WLAN, even when roaming between multiple APs. This is enabled by default.
- Check the **Load Balance** check box to enable Aggressive Client Load Balancing. This allows lightweight access points to load balance wireless clients across access points.
- Check the **Band Select** check box to enable band selection for the WLAN. Band selection enables client radios that are capable of dual-band (2.4 and 5-GHz) operations to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested with interference from other electronic devices as well as co-channel interference from other access points. Band selection helps prevent these sources of interference and improve overall network performance.
- Enable IP Source Guard on the WLAN by checking the **IP Source Guard** check box. IP Source Guard (IPSG) is a Layer 2 security feature that prevents the wireless controller from forwarding the packets with source IP addresses that are not known to it.

- b) From the **WMM Policy** drop-down list, choose the policy as **Allowed**, **Disabled**, or **Required**. By default, the WMM policy is **Allowed**. Wi-Fi Multimedia (WMM) is used to prioritize different types of traffic.

- **Disabled**: Disables WMM on the WLAN.
- **Required**: Requires client devices to use WMM. Devices that do not support WMM cannot join the WLAN.
- **Allowed**: Devices that cannot support WMM can join the WLAN but will not benefit from the 802.11n rates.

- c) From the **mDNS** drop-down list, choose **Bridging**, **Gateway**, or **Drop**. Multicast DNS (mDNS) provides the ability to perform DNS-like operations on the local link in the absence of any conventional Unicast DNS server.

- **Bridging:** Packets with mDNS multicast IP and multicast mac will be sent on multicast CAPWAP tunnel.
- **Gateway:** All ingress mDNS packets received from the wired network on a L3 interface (SVI or physical) would be intercepted by the Controller software and processed.
- **Drop:** All ingress mDNS packets will be dropped.

**Step 12** In the **Off Channel Scanning Defer** section, choose the appropriate **Defer Priority** values and then specify the required Scan Defer Time value in milliseconds.

**Step 13** In the **Assisted Roaming (11k)** section, choose the appropriate status for the following:

- Prediction Optimization
- Neighbor List
- Dual-Band Neighbor List

**Step 14** In the **DTIM Period (in beacon intervals)** section, specify a value for 802.11a/n and 802.11b/g/n radios. The valid range is from 1 to 255.

**Step 15** Click **Apply to Device**.

## Configuring WLAN Radio Policy (GUI)

### Procedure

**Step 1** On the **Configuration > Tags & Profiles > WLANs** page, click **Add** to create WLANs.

**Step 2** In the **General** tab, enter a **Profile Name**, which is a unique name of the your wireless network.

The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

**Step 3** Enter a valid **SSID** for the WLAN.

A valid SSID can be up to 32 characters and can contain spaces. A valid SSID can be ASCII characters from 0 to 31, with leading and trailing spaces. This is the broadcast name for your WLAN.

**Step 4** Enter the **WLAN ID**. The valid range for the different models are listed below:

Model	WLAN ID Range
Cisco Catalyst 9800-80 Wireless Controller	1-4096
Cisco Catalyst 9800-CL Wireless Controller	1-4096
Cisco Catalyst 9800-40 Wireless Controller	1-4096
Cisco Catalyst 9800-L Wireless Controller	1-4096
Cisco Embedded Wireless Controller for an AP	1-16

- Step 5** Set the **WLAN Status** to Enabled.
- Step 6** To broadcast the SSID of the WLAN, set the status of Broadcast SSID to enabled. By default, this is disabled.
- Step 7** In the **Radio Policy** section, enable the desired radio band for the WLAN.
- 2.4ghz – Configures the policy on the 2.4-GHz radio.
  - 5ghz – Configures the policy on the 5-GHz radio.
- Step 8** If you enable the 5ghz radio band, select the radio slot to broadcast the WLAN on. The options are slot 0, slot 1, and slot 2. You can select multiple slots for the WLAN.
- Step 9** From the 802.11b/g Policy drop-down list, choose the radio policy from the following options:
- 802.11g only
  - 802.11b/g

Click **Apply to Device**.

## Configuring a WLAN Radio Policy (CLI)

Configure WLAN radio policy using commands.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wlan <i>profile-name</i></b>  <b>Example:</b> Device(config)# wlan test4	Enters WLAN configuration submode. The <i>profile-name</i> is the profile name of the configured WLAN.
<b>Step 3</b>	<b>shutdown</b>  <b>Example:</b> Device(config-wlan)# shutdown	Disables the WLAN.
<b>Step 4</b>	<b>radio policy dot11{5ghz   24ghz   6ghz }</b>  <b>Example:</b> Device(config-wlan)# radio policy dot11 5ghz	Enables the corresponding radio policy on the WLAN. The options are: <ul style="list-style-type: none"> <li>• <b>2.4ghz</b>: Configures the WLAN on 2.4-GHz radio only.</li> <li>• <b>5ghz</b>: Configures the WLAN on 5-GHz radio only.</li> <li>• <b>6ghz</b>: Configures the WLAN on 6-GHz radio only.</li> </ul>

	Command or Action	Purpose
<b>Step 5</b>	<b>slot {0  1   2}</b> <b>Example:</b> Device(config-wlan-radio-5ghz)# slot 1	Configures the WLAN radio policy on the slot that you choose. The options are: <ul style="list-style-type: none"> <li>• <b>0</b>: Configures the WLAN on the 5GHz radio with radio slot 0 (if using 5GHz).</li> <li>• <b>1</b>: Configures the WLAN on the 5GHz radio with radio slot 1.</li> <li>• <b>2</b>: Configures the WLAN on the 5GHz radio with radio slot 2 (if present).</li> </ul>
<b>Step 6</b>	<b>no shutdown</b> <b>Example:</b> Device(config-wlan)# no shutdown	Enables the WLAN.
<b>Step 7</b>	<b>end</b> <b>Example:</b> Device(config-wlan)# end	Returns to privileged EXEC mode.

## Verifying WLAN Properties (CLI)

To verify the WLAN properties based on the WLAN ID, use the following `show` command:

```
Device# show wlan id wlan-id
```

To verify the WLAN properties based on the WLAN name, use the following `show` command:

```
Device# show wlan name wlan-name
```

To verify the WLAN properties of all the configured WLANs, use the following `show` command:

```
Device# show wlan all
```

To verify the summary of all WLANs, use the following `show` command:

```
Device# show wlan summary
```

To verify the running configuration of a WLAN based on the WLAN name, use the following `show` command:

```
Device# show running-config wlan wlan-name
```

To verify the running configuration of all WLANs, use the following `show` command:

```
Device# show running-config wlan
```

## Verifying WLAN-VLAN Information for an AP

To verify the operational WLAN-VLAN mappings per AP, use the following command:

```
Device# show ap name test wlan vlan
```

```
Policy tag mapping
```

```

-----
WLAN Profile Name Name Policy      VLAN   Flex Central Switching  IPv4 ACL   IPv6 ACL
-----
jey_cwa           pp-local-1    46     Enabled                  jey_acl1   Not Configured
swaguest         pp-local-1    46     Enabled                  jey_acl1   Not Configured

```

## Verifying a WLAN Radio Policy

To verify the WLAN radio policy configuration status, use the following command:

```

Device# show wlan id 6 | sec Radio Bands
wpa3 enabled wlan:
Configured Radio Bands: All
Operational State of Radio Bands : All Bands Operational

Configured Radio Bands : All
Operational State of Radio Bands
  2.4ghz                : UP
  5ghz                  : UP
  6ghz                  : DOWN (Required config: Disable WPA2 and Enable WPA3 &
dot11ax)

wpa3 not enabled wlan :
Configured Radio Bands : All
Operational State of Radio Bands
2.4ghz : UP
5ghz   : UP

5ghz specify slot is enabled :
Configured Radio Bands
5ghz   : Enabled
Slot 0 : Enabled
Slot 1 : Disabled
Slot 2 : Disabled

Operational State of Radio Bands
5ghz   : UP
Slot 0 : Enabled
Slot 1 : Disabled
Slot 2 : Disabled

```

