WLANs

WLANs

A WLAN is a wireless network feature that

- enables control of wireless local area networks for lightweight access points
- supports up to 16 advertised WLANs per access point with up to 4096 total configurable WLANs, and
- allows selective advertisement using profiles and tags for better manageability.

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

WLAN configuration details

Each WLAN has a separate WLAN ID, a separate profile name, and a WLAN SSID.

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 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.

Wi-Fi multimedia (WMM) policy

Wi-Fi Multimedia (WMM) is used to prioritize different types of traffic. The WMM policy options include:

- **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 do not support WMM can join the WLAN but will not benefit from the 802.11n rates.

Note For 802.11ax APs and higher (Cisco Catalyst 9117, 9124, 913x, 916x, 917x APs), WMM can not be **Disabled**. Only **Required** or **Allowed** options are supported.

Band selection

A band selection is a wireless network feature that

- facilitates the movement of dual-band client radios from congested frequency bands
- enables clients to connect to less congested 5-GHz access points for improved network performance, and
- reduces interference from other devices by optimizing which frequency band clients use.

The 2.4-GHz band is often congested. Clients using this band may experience interference from Bluetooth devices, microwave ovens, cordless phones, and co-channel interference from other access points due to the 802.11b/g channel limit of 3 nonoverlapping channels. By configuring band selection on devices, administrators can steer dual-band clients toward the 5-GHz band, improving overall network performance.

Off-channel scanning deferral

Off-channel scanning deferral is a wireless network feature that

- temporarily postpones RRM off-channel scanning activities when important data transmission occurs
- prevents performance impact on critical traffic by avoiding the normal 70-millisecond off-channel periods, and
- can be configured on a per-WLAN basis with specific WMM UP class and time threshold parameters.

Off-channel scanning operations

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 millseconds. 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

A Delivery Traffic Indication Map (DTIM) period is a 802.11 network timing mechanism that

- allows power-saving clients to wake up at the appropriate time if they are expecting broadcast or multicast data
- determines when access points transmit buffered broadcast and multicast frames after beacon broadcasts, and
- coincides with the DTIM broadcast interval.

DTIM period characteristics

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.

Typical DTIM values and their transmission patterns:

- DTIM value 1: Transmits broadcast and multicast frames after every beacon
- DTIM value 2: Transmits 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 policies

A WLAN radio policy is a wireless network configuration feature that

- allows broadcasting the WLAN on the corresponding slot
- provides more granular control compared to existing WLAN features that broadcast on all applicable slots, and
- is supported only on 5 GHz band.

WLAN radio policy functionality

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.

Restrictions for WLAN radio policy

This topic lists the restrictions that apply to WLAN radio policy configuration.

- WLAN is pushed to all the radios only if these configurations are 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 a WLAN security feature that

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

A diagnostic channel is a troubleshooting feature that

- enables testing of client and AP communication to identify network difficulties
- allows corrective measures to be taken to make the client operational on the network, and
- provides GUI or CLI configuration options for enabling diagnostic tests.

Configuration options

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

AP names in beacon

AP names in beacon is a feature that

- extends the maximum length for AP name from 16 to 32 characters
- prevents AP name truncation in beacons, and
- uses a vendor specific (VS) Information Element (IE) instead of CCX IEs.

The extended length matches the maximum length supported in the controller. This enhancement resolves issues where AP names were truncated due to a 16-character limit imposed by CCX Information Elements (IEs).

Feature history

Table 1: Feature history for AP names in beacons

Feature name	Release information	Feature description
AP names in beacons	Cisco IOS XE 17.18.2	AP names in beacon is a feature that allows AP names to be extended from 16 to 32 characters, prevents truncation of AP names in beacon frames, and uses a vendor-specific Information Element (IE) instead of the older CCX IEs.

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

This reference provides restrictions and limitations that apply when configuring and managing WLANs on wireless controllers.

- Do not configure PSK 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 WLAN wizard is a simplified workflow that

- helps you quickly create a WLAN and setup some primary configurations for your specific deployment
- supports wireless deployment modes including Local mode, FlexConnect mode, and Guest CWA mode, and
- provides different authentication methods for each deployment mode.

Wireless deployment modes

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).

Important These steps help configure WLANs, otherwise an error might occur.

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 these 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

Local mode is a WLAN deployment configuration that

- is used when the WLAN is present in an office setup with no branch offices

- creates two CAPWAP tunnels from an AP to the controller, one for management and the other for data traffic, and
- implements centrally switched behavior where data traffic is tunneled from the AP to the controller for routing.

Local mode traffic handling

In local mode, data traffic is tunneled (bridged) from the AP to the controller where it is then routed by some routing device. This behavior is known as "centrally switched" because the data traffic is processed at the controller level. Locally switched means the traffic is terminated at the local switch adjacent to the access point.

Authentication methods

An authentication method is a WLAN security configuration that

- sets the method by which a client can access the WLAN
- decides the level of security on the WLAN, and
- is selected from the left panel when configuring a WLAN for local mode.

Authentication method options

The authentication method 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 htttp(s) traffic and redirects the client to the internal web page for authentication.
- External Web Authentication: The controller intercepts htttp(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.

Configure WLAN profile and policy

Configure the WLAN profile and policy to define wireless network properties and network policies for client switching and AP management.

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.

The WLAN profile and policy are configured with the specified network name, SSID, WLAN ID, and associated policy parameters.

Configure authentication for WLAN

Set up authentication configurations to secure your WLAN and control client access based on your chosen authentication method.

Authentication configurations include keys, filters, ACLs, and parameter maps that correspond to your selected authentication method. Each authentication method requires specific configuration steps to establish secure client connections.

Follow these steps to configure authentication for your WLAN:

Procedure

Step 1 If you have selected **PSK** as the authentication method, configure these parameters:

a) In the **WLAN > Pre-Shared Key (PSK)** section, select the PSK format. Choose between ASCII and Hexadecimal formats.

b) From the **PSK type** drop-down list, choose if you want the key to be unencrypted or AES encrypted.

c) 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:

a) In the **WLAN > AAA** tab, configure the AAA server list for the WLAN.

b) Select any of the available AAA servers to add to the WLAN.

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 **Local Web Authentication** as the authentication method, configure these parameters:

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** tab, enter the username in the local database to establish a username-based authentication system.

1. Enter the user name to be saved.
2. From the **Password Encryption** drop-down list, choose if you want the password to be unencrypted or encrypted.
3. 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.
4. 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 these parameters:

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.

Configure tags on WLAN

Configure tags on WLAN to define properties through associated policies that are inherited by clients and access points.

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.

The tags are successfully configured on the WLAN. The properties defined by the policies associated with these tags will be inherited by the associated clients and access points.

AP Provision

This task allows you to add access points to the local site and associate them with appropriate tags for WLAN configuration.

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 **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.

The access points are successfully provisioned and associated with the configured tags, creating a WLAN in local mode with the specified authentication and configuration settings.

FlexConnect mode

FlexConnect mode is a wireless solution that

- enables configuration and control of 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
- allows FlexConnect APs to switch client data traffic and perform client authentication locally when their connection to the controller is lost, and
- offers network survivability in the event of a loss of connection to the centralized wireless controller.

FlexConnect mode deployment

This figure shows a FlexConnect mode deployment:

Authentication methods

An authentication method is a security mechanism that

- sets the method by which a client can access the WLAN
- decides the level of security on the WLAN, and
- determines how traffic is intercepted and redirected for client authentication.

Authentication method options

To configure a WLAN for FlexConnect mode, select the preferred authentication method from the left panel. The authentication method options are:

- Local Web Authentication: The controller intercepts htttp(s) traffic and redirects the client to the internal web page for authentication.
- External Web Authentication: The controller intercepts htttp(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.

Configure WLAN profile and policy

Configure WLAN profile and policy settings to establish wireless network connectivity with appropriate security parameters and client policies.

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.

The WLAN profile and policy are configured with the specified network name, SSID, WLAN ID, and associated VLAN settings for wireless network connectivity.

Configure authentication configurations

Configure authentication settings, keys, filters, ACLs, and parameter maps for your selected WLAN authentication method to enable secure wireless access for users.

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.

Follow these steps to configure authentication configurations:

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.

Configure tags on WLAN

Configure tags on WLAN to define properties through associated policies that are inherited by clients and access points.

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.

Follow these steps to configure tags on WLAN:

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.

The tags are configured on the WLAN with their associated policies and profiles.

AP Provision

Access point provisioning allows you to associate discovered or manually added APs with specific WLAN configurations by applying policy, site, and RF tags.

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.

Follow these steps to provision access points and apply tags to associate them with the WLAN:

Procedure

Step 1 To add tags and associate APs to the WLAN, click on **AP Provisioning** from the left panel.

Step 2 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 3 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 4 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 5 Select the APs to be associated to the WLAN from this table.

Step 6 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 7 Click **Apply**.

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

The access points are successfully provisioned and associated with the WLAN configuration. A WLAN in FlexConnect mode is created with the specified authentication method, authentication filters, tags, and APs.

Guest CWA mode

Guest CWA mode is a wireless network security implementation that

- provides secure and accountable internet access to visitors using Central Web Authentication
- uses the enterprise's existing wireless and wired infrastructure to the maximum extent, and
- comprises two controllers - a Guest Foreign and a Guest Anchor.

Guest CWA mode implementation

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.

Controller types

A controller type is a WLAN configuration category that

- determines how controllers manage guest client connections and traffic
- defines the role each controller plays in the guest access network, and
- enables proper traffic flow and security implementation for guest WLAN services.

Controller type options

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 controller type 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.

Configure WLAN profile and policy

Configure WLAN profile and policy settings to establish wireless network connectivity and define network switching policies for clients.

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.

The WLAN profile and policy are configured with the specified network name, SSID, WLAN ID, and policy settings. The wireless network is ready for client connections with the defined switching policies.

Configure authentication for guest access

Configure AAA server settings and access control lists to enable guest authentication through Central Web Authentication for WLAN access.

For the Guest access mode, the authentication method is Central Web Authentication. This configuration allows guest users to authenticate through a centralized web portal before gaining network access.

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.

The WLAN is now configured with AAA authentication settings for guest access, allowing clients to authenticate through the specified AAA servers and apply the configured access control rules.

Configure tags on WLAN

Configure tags to define properties that are inherited by associated clients and access points through various policy profiles.

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.

Tags are configured on the WLAN with site configuration, policy, and RF tags that define the properties inherited by associated clients and access points.

AP provision

This task enables you to add access points to the local site and associate them with the wireless LAN configuration by applying appropriate tags.

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.

The access points are successfully provisioned and associated with the WLAN configuration. A WLAN in Guest CWA mode is created with the specified authentication method, mobility anchors, authentication filters, tags, and APs.

Create WLANs (GUI)

Create wireless local area networks (WLANs) to enable network connectivity and manage wireless access configurations through the GUI interface.

Use the GUI interface to create and configure WLANs when you need to establish wireless network connectivity. This method provides a visual interface for WLAN configuration and management.

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**.

The WLAN is created and applied to the device. The new WLAN appears in the WLANs list and is ready for use.

Create WLANs (CLI)

Create wireless local area networks (WLANs) to provide wireless network access for clients.

You can create SSID using GUI or CLI. However, we recommend that you use CLI to create SSID. By default, the WLAN is disabled after creation.

Follow these steps to create WLANs using CLI commands:

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Specify the WLAN name and ID.

Example:

```
Device(config)# wlan profile-name wlan-id [ssid]
```

Example:

```
Device(config)# wlan profile-name wlan-id [ssid] mywlan 34 mywlan-SSID
```

- For the *profile-name*, enter the profile name. The range is from 1 to 32 alphanumeric characters.
- For the *wlan-id*, enter the WLAN ID. The range is from 1 to 512.
- For the *ssid*, enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID.

Note

- You can create SSID using GUI or CLI. However, we recommend that you use CLI to create SSID.

- By default, the WLAN is disabled.

Step 3 Return to privileged EXEC mode.

Example:

```
Device# end
```

Alternatively, you can also press Ctrl-Z to exit global configuration mode.

The WLAN is created with the specified profile name, WLAN ID, and SSID. The WLAN is disabled by default and must be enabled separately for use.

Delete WLANs (GUI)

Remove unwanted or obsolete WLANs from your network configuration to maintain optimal performance and security.

Use this procedure when you need to remove WLANs that are no longer required or need to be replaced with new configurations. This task can be performed on single or multiple WLANs simultaneously.

Procedure

Step 1 In the **Configuration** > **Tags & Profiles** > **WLANs** page, check the check box adjacent to the WLAN you want to delete.

To delete multiple WLANs, select multiple WLANs check boxes.

Step 2 Click **Delete**.

Step 3 Click **Yes** on the confirmation window to delete the WLAN.

The selected WLAN(s) are permanently removed from the system and will no longer appear in the WLANs list.

Delete WLANs (CLI)

Delete WLAN profiles that are no longer needed or require reconfiguration in the wireless network environment.

Use this procedure when you need to remove WLAN profiles from the wireless controller configuration. Deleting a WLAN removes the profile and associated settings from the system.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Delete the WLAN.

Example:

```
Device(config)# no wlan wlan-profile-name wlan-id  [ssid]
```

```
Device(config)# no wlan test2
```

The arguments are:

- The *wlan-name* is the WLAN profile name.
- The *wlan-id* is the WLAN ID.
- The *ssid* is the WLAN SSID name configured for the WLAN.

Note
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.

Step 3 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

The WLAN profile is deleted from the wireless controller configuration. If the WLAN was associated with an AP group, it is automatically removed from the group and the AP's radio interface.

WLAN search methods (CLI)

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

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

Enable WLANs (GUI)

Enable wireless local area networks (WLANs) to allow wireless client connections and network access through the graphical user interface.

Use this task when you need to activate WLANs that have been configured but are currently disabled, allowing wireless devices to connect to your network.

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**.

The WLAN is ENABLED and wireless clients can now connect to the network through this WLAN.

Enable WLANs (CLI)

Enable previously configured WLANs to make them operational and available for client connections.

WLANs must be explicitly enabled after configuration to allow wireless clients to connect. This procedure activates a specific WLAN profile.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 2 Enter WLAN configuration submode.

Example:

```
Device(config)# WLAN profile-name
```

Example:

```
Device(config)# WLAN test4
```

The *profile-name* is the profile name of the configured WLAN.

Step 3 Enable the WLAN.

Example:

```
Device(config-wlan)# no shutdown
```

Step 4 Return to privileged EXEC mode.

Example:

```
Device(config-wlan)# end
```

The WLAN is now enabled and operational, allowing wireless clients to connect to the network.

Disable WLANs (GUI)

Disable WLANs to prevent wireless network access when maintenance is required or to temporarily suspend wireless services.

Use this procedure when you need to temporarily disable wireless networks without deleting the WLAN configuration. The WLAN settings remain intact and can be re-enabled later.

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**.

The WLAN is DISABLED and wireless clients can no longer connect to this network. The WLAN configuration is preserved and can be re-enabled when needed.

Disable WLANs (CLI)

Disable specific WLANs to prevent wireless client access when needed for maintenance or security purposes.

You may need to disable WLANs temporarily for maintenance, troubleshooting, or security reasons. This procedure shows how to disable a WLAN using the CLI and verify the change.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enter WLAN configuration submode.

Example:

```
Device(config)# wlan profile-name
```

Example:

```
Device(config)# wlan test4
```

The *profile-name* is the profile name of the configured WLAN.

Step 3 Disable the WLAN.

Example:

```
Device(config-wlan)# shutdown
```

Step 4 Return to privileged EXEC mode.

Example:

```
Device(config-wlan)# end
```

Step 5 Display the list of all WLANs configured on the device.

Example:

```
Device# show wlan summary
```

You can search for the WLAN in the output to verify it has been disabled.

The specified WLAN is now disabled and will not accept wireless client connections until re-enabled.

Configure general WLAN properties (CLI)

Configure media stream, broadcast SSID, and radio properties for a WLAN.

You can configure these properties: Media stream, Broadcast SSID, and Radio settings for optimal WLAN performance and visibility.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enter WLAN configuration submode.

Example:

```
Device(config)# wlan profile-name
```

Example:

```
Device(config)# wlan test4
```

The *profile-name* is the profile name of the configured WLAN.

Step 3 Disable the WLAN.

Example:

```
Device(config-wlan)# shutdown
```

Step 4 Broadcast the SSID for this WLAN.

Example:

```
Device(config-wlan)# broadcast-SSID
```

Step 5 Configure the WLAN radio policy for dot11 radios.

Example:

```
Device(config-wlan)# dot11bg 11g
```

Also see the section: Configuring a WLAN Radio Policy.

Step 6 Enable multicast VLANs on this WLAN.

Example:

```
Device(config-WLAN)# media-stream multicast-direct
```

Step 7 Enable the WLAN.

Example:

```
Device(config-wlan)# no shutdown
```

Step 8 Return to privileged EXEC mode.

Example:

```
Device(config-wlan)# end
```

The WLAN is now configured with the specified general properties including media stream, broadcast SSID, and radio settings.

Configure advanced WLAN properties (CLI)

Configure advanced WLAN properties to customize wireless network behavior and security settings.

Advanced WLAN properties provide additional configuration options for wireless networks, including coverage hole detection, client association limits, access control, and peer-to-peer blocking settings. These configurations help optimize wireless performance and security based on specific network requirements.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enter WLAN configuration submode.

Example:

```
Device(config)# wlan profile-name
```

Example:

```
Device(config)# wlan test4
```

The *profile-name* is the profile name of the configured WLAN.

Step 3 Enable coverage hole detection for this WLAN.

Example:

```
Device(config-wlan)# chd
```

Step 4 Enable support for Aironet IEs for this WLAN.

Example:

```
Device(config-wlan)# ccx aironet-iesupport
```

Step 5 Set the maximum number of clients that can be configured on a WLAN. Configure limits for clients per WLAN, clients per AP, or clients per AP radio.

Example:

```
Device(config-wlan)# client association limit {clients-per-WLAN | ap clients-per-AP-per-WLAN
 | radio clients-per-AP-radio-per-WLAN}
```

Example:

```
Device(config-wlan)# client association limit AP 400
```

Step 6 Configure the IPv4 WLAN web ACL.

Example:

```
Device(config-wlan)# ip access-group web ACL-name
```

Example:

```
Device(config-wlan)# ip access-group web test-ACL-name
```

The *ACL-name* specifies the user-defined IPv4 ACL name.

Step 7 Configure peer-to-peer blocking parameters.

Example:

```
Device(config-wlan)# peer-blocking [allow-private-group | drop | forward-upstream]
```

Example:

```
Device(config-WLAN)# peer-blocking drop
```

The keywords are:

- **allow-private-group**: Enables peer-to-peer blocking on the Allow Private Group action.
- **drop**: Enables peer-to-peer blocking on the drop action.
- **forward-upstream**: No action is taken and forwards packets to the upstream.

  Note
  The **forward-upstream** 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.

Step 8 Set the channel scan defer priority and defer time.

Example:

```
Device(config-WLAN)# channel-scan {defer-priority {0-7} | defer-time {0-6000}}
```

Example:

```
Device(config-WLAN)# channel-scan defer-priority 6
```

The arguments are:

- **defer-priority**: Specifies the priority markings for packets that can defer off-channel scanning. The range is from 0 to 7. The default is 3.
- **defer-time**: Deferral time in milliseconds. The range is from 0 to 6000. The default is 100.

Step 9 Return to privileged EXEC mode.

Example:

```
Device(config-wlan)# end
```

The advanced WLAN properties are now configured with the specified settings for coverage hole detection, client limits, access control, peer-to-peer blocking,broadcast filtering, AAA override, session timeout, exclusion list management, and diagnostic channel support.

Configure advanced WLAN properties (GUI)

Configure advanced WLAN properties to enable enhanced wireless network features including coverage optimization, client connection limits, BSS transition support, and 802.11ax capabilities.

Advanced WLAN properties provide additional configuration options to optimize wireless network performance and enable specific features for client management and network diagnostics.

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 diabled.

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:

- 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 these configuration tasks:

a) Select the check box to enable these parameters:

- 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:

- 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**.

The WLAN profile is updated with advanced properties, and features such as coverage optimization, client connection limits, enhanced roaming, and diagnostics are enabled for improved network performance.

Configure WLAN radio policy (GUI)

Configure a WLAN radio policy to define the radio bands and settings for wireless network operation through the graphical user interface.

Use this procedure when you need to set up radio policies for WLANs to control which radio bands (2.4 GHz or 5 GHz) are used and configure related settings for optimal wireless network performance.

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 5 Ghz 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 these options:

- 802.11g only
- 802.11b/g

Step 10 Click **Apply to Device**.

The WLAN radio policy is configured and applied to the device with the specified radio bands and settings.

Configure a WLAN radio policy (CLI)

Configure WLAN radio policy to control which radio bands and slots the WLAN operates on.

Use this procedure to configure WLAN radio policy settings when you need to specify which radio bands (2.4 GHz, 5 GHz, or 6 GHz) and which radio slots the WLAN should use for wireless communication.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enter WLAN configuration submode.

Example:

```
Device(config)# wlan profile-name
```

Example:

```
Device(config)# wlan test4
```

The *profile-name* is the profile name of the configured WLAN.

Step 3 Disable the WLAN.

Example:

```
Device(config-wlan)# shutdown
```

Step 4 Enable the corresponding radio policy on the WLAN.

Example:

```
Device(config-wlan)# radio policy dot11 {5ghz | 24ghz | 6ghz }
```

Example:

```
Device(config-wlan)# radio policy dot11 5ghz
```

The options are:

- **2.4ghz**: Configures the WLAN on 2.4-GHz radio only.
- **5ghz**: Configures the WLAN on 5-GHz radio only.
- **6ghz**: Configures the WLAN on 6-GHz radio only.

Step 5 Configure the WLAN radio policy on the slot that you choose.

Example:

```
Device(config-wlan-radio-5ghz)# slot slot-number
```

Example:

```
Device(config-wlan-radio-5ghz)# slot 1
```

The options are:

- **0**: Configures the WLAN on the 5GHz radio with radio slot 0 (if using 5GHz).
- **1**: Configures the WLAN on the 5GHz radio with radio slot 1.
- **2**: Configures the WLAN on the 5GHz radio with radio slot 2 (if present).

Step 6 Enable the WLAN.

Example:

```
Device(config-wlan)# no shutdown
```

Step 7 Return to privileged EXEC mode.

Example:

```
Device(config-wlan)# end
```

The WLAN is now configured with the specified radio policy and will operate on the designated radio band and slot.

Configure AP name advertisement in beacons (GUI)

To enable the inclusion of the AP hostname in beacon and probe responses, preventing truncation.

This feature allows the AP name to be extended to 32 characters, matching the maximum length in the controller. The configuration is available through CLI, NETCONF-YANG, and WebUI. By default, this feature is disabled.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.
The Add WLAN page is displayed.

Step 3 Click the **Advanced** tab.

Step 4 Check the **Advertise AP Name** check box to include the AP hostname in beacon and probe responses. This feature is disabled by default.

Step 5 Click **Apply to Device**.

The AP includes its hostname in beacon and probe responses.

Configure AP name advertisement in beacons

To enable the inclusion of the AP hostname in beacon and probe responses, preventing truncation.

This feature allows the AP name to be extended to 32 characters, matching the maximum length in the controller. The configuration is available via CLI, NETCONF-YANG, and WebUI. By default, this feature is disabled.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enter WLAN profile configuration mode for the desired WLAN.

Example:

```
Device(config)# wlan wlan-prof-name wlan-id ssid-name
```

Step 3 Disable the WLAN to allow configuration changes.

Example:

```
Device(config-wlan)# shutdown
```

Step 4 Enable AP name advertisement.

Example:

```
Device(config-wlan)# advertise ap-name
```

Step 5 Enable WLAN.

Example:

```
Device(config-wlan)# no shutdown
```

The AP now includes its hostname in beacon and probe responses.

```
Device# configure terminal
Device(config)# wlan wlan-profile1 25 ssid1
Device(config-wlan)# shutdown
Device(config-wlan)# advertise ap-name
Device(config-wlan)# no shutdown
```

WLAN properties verification (CLI)

To verify the WLAN properties based on the WLAN ID, use this command:

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

To verify the WLAN properties based on the WLAN name, use this command:

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

To verify the WLAN properties of all the configured WLANs, use this command:

```
Device# show wlan all
```

To verify the summary of all WLANs, use this command:

```
Device# show wlan summary
```

To verify the running configuration of a WLAN based on the WLAN name, use this command:

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

To verify the running configuration of all WLANs, use this command:

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

Verify WLAN-VLAN information of an AP

To verify the operational WLAN-VLAN mappings per AP, use this 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
```

WLAN radio policy verification

To verify the WLAN radio policy configuration status, use this 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
```

Verify AP name advertisement

To verify the AP name advertisement, use this command:

```
Device# show wlan id 1
WLAN Profile Name     : wlan-prof-name
================================================
Identifier                                       : 1
Description                                      :
Network Name (SSID)                              : cm71
```

```
Status                                          : Enabled
Broadcast SSID                                  : Enabled
Advertise-Apname                                : Disabled
Universal AP Admin                              : Disabled
Max Associated Clients per WLAN                 : 0
Max Associated Clients per AP per WLAN          : 0
Max Associated Clients per AP Radio per WLAN    : 200
.
.
.
```