# Configuration Model for Cisco Catalyst 9800 Series Wireless Controller

**First Published:** 2021-11-01

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

# CONTENTS

CHAPTER 17

CHAPTER 18

# Document Conventions

This document uses the following conventions:

| Convention | Description |
|---|---|
| ^ or Ctrl | Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.) |
| **bold** font | Commands and keywords and user-entered text appear in **bold** font. |
| *Italic* font | Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font. |
| `Courier` font | Terminal sessions and information the system displays appear in `courier` font. |
| **`Bold Courier`** font | **`Bold Courier`** font indicates text that the user must enter. |
| [x] | Elements in square brackets are optional. |
| ... | An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated. |
| \| | A vertical line, called a pipe, indicates a choice within a set of keywords or arguments. |
| [x \| y] | Optional alternative keywords are grouped in brackets and separated by vertical bars. |
| {x \| y} | Required alternative keywords are grouped in braces and separated by vertical bars. |
| [x {y \| z}] | Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element. |
| string | A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks. |
| < > | Nonprinting characters such as passwords are in angle brackets. |
| [ ] | Default responses to system prompts are in square brackets. |
| !, # | An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line. |

### Reader Alert Conventions

This document may use the following conventions for reader alerts:

**Note** Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

**Tip** Means *the following information will help you solve a problem.*

**Caution** Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

**Timesaver** Means *the described action saves time.* You can save time by performing the action described in the paragraph.

**Warning** IMPORTANT SAFETY INSTRUCTIONS

Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Read the installation instructions before using, installing, or connecting the system to the power source. Use the statement number provided at the end of each warning statement to locate its translation in the translated safety warnings for this device. Statement 1071

SAVE THESE INSTRUCTIONS

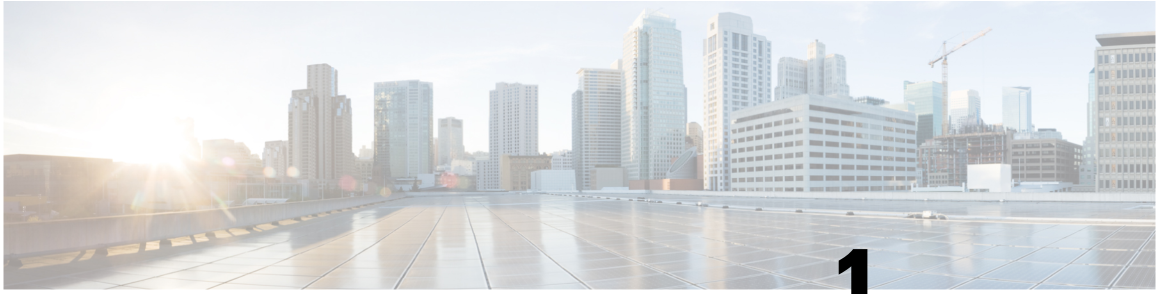
# Related Documentation

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



CHAPTER 1

# Overview of the Configuration Model

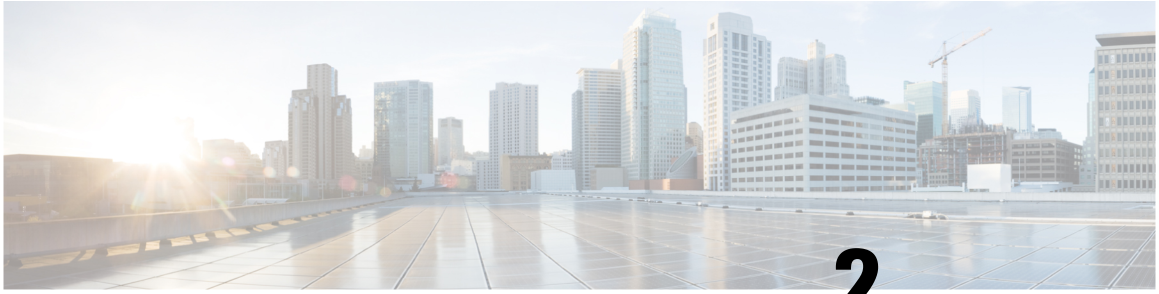
## Overview of Cisco 9800 Series Configuration Model

Cisco Catalyst 9800 Series Wireless Controllers are the next generation of wireless controllers built for intent-based networking.

These controllers can be deployed in physical and virtual (private and public cloud) form factors and can be managed through Cisco Digital Networking Architecture (DNA) Center, NETCONF-YANG, Cisco Prime Infrastructure, web-based GUI, or CLI.

The Cisco Catalyst 9800 Series configuration model is based on profiles and tags. Profiles group a set of features and functionalities, and tags allow you to assign these features and functionalities to access points (APs).

This model helps the client or AP devices to derive their configurations from the profiles that are contained within the tags. AP devices can be mapped to the tags either statically or as part of a rule engine that runs on the controller and comes into effect during the AP join process. Configuration objects are modularized as objects that help in the reuse of the configuration. In addition, a flat tag-based configuration model eliminates the complexities associated with inheritance and container-based grouping, leading to a simpler and flexible configuration that can ease change management.



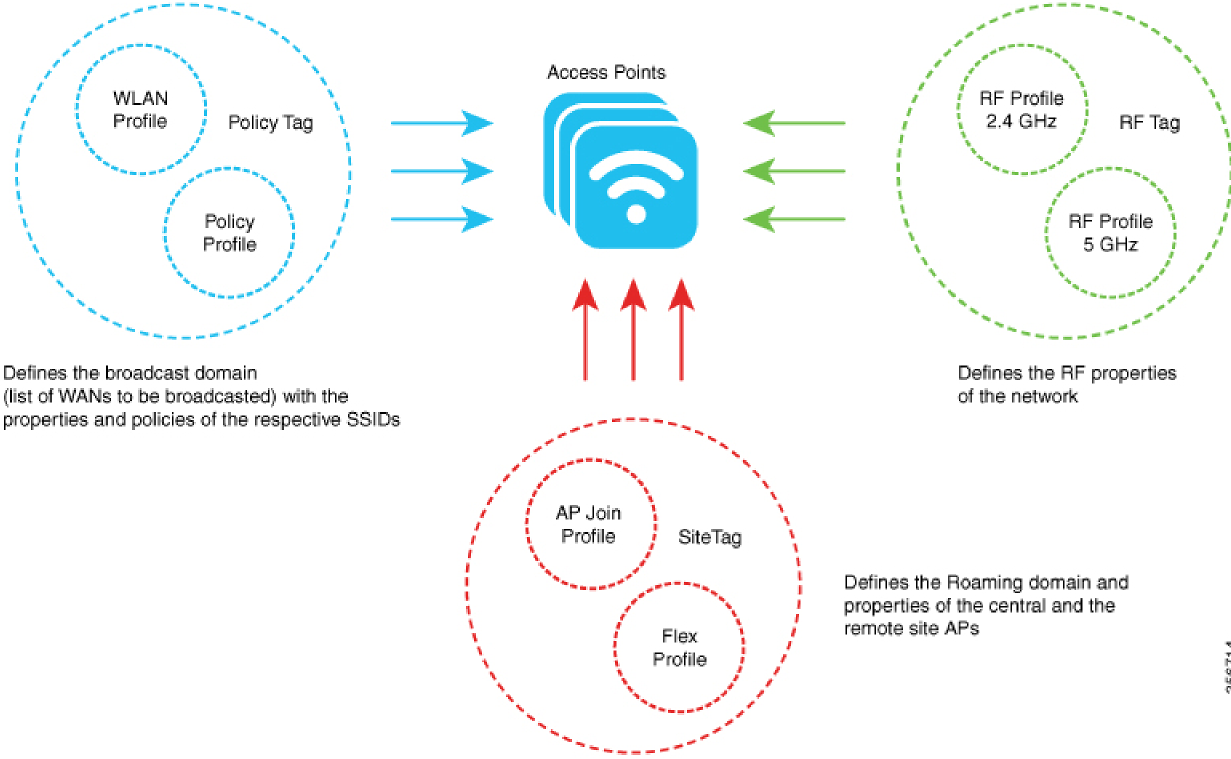
CHAPTER 2

# Elements of the Configuration Model

## Elements of the Configuration Model

This section describes profiles and tags that constitute the configuration model.

*Figure 1: Elements of the Configuration Model*


WLAN Profile
Policy Tag
Policy Profile
Defines the broadcast domain (list of WANs to be broadcasted) with the properties and policies of the respective SSIDs
Access Points
RF Profile 2.4 GHz
RF Tag
RF Profile 5 GHz
Defines the RF properties of the network
AP Join Profile
SiteTag
Flex Profile
Defines the Roaming domain and properties of the central and the remote site APs

### Profiles

Profiles define the properties of the AP or the associated clients. Profiles are reusable entities that can be used across tags. By default, WLAN profile, Policy profile, AP Join profile, Flex profile, and 2.4/5GHz RF profiles are available on the wireless controller during boot up.

Other kinds of profiles are also available, depending on the characteristic of the network they define. These profiles are part of a larger construct called a Tag.

There are five types of profiles:

- WLAN Profile: Defines the properties of a Wireless LAN (WLAN) such as the profile name, status, WLAN ID, layer 2 and layer 3 security parameters, Authentication, Authorization, and Accounting (AAA) server associated with the service set identifiers (SSIDs), and other parameters that are specific to a particular WLAN.

  An SSID identifies the specific wireless network for the controller to access. WLAN profiles are configured with same or different SSID. Creating WLANs with the same SSID allows the assignment of different layer 2 security policies within the same wireless LAN.

  To distinguish WLANs having the same SSID, create a unique profile name for each WLAN. WLANs with the same SSID must have unique layer 2 security policies so that clients can select a WLAN based on the information advertised in the beacon and probe responses. The switching and network policies are not part of the WLAN profile.

- Policy Profile: Defines the network policies and the switching policies for a client with the exception of quality of service (QoS), which constitute the AP policies. Policy profile is a reusable entity across tags. Anything that is a policy for the client that is applied on the AP or controller is moved to the policy profile. For example, VLAN, access control list (ACL), QoS, session timeout, idle timeout, Application Visibility and Control (AVC) profile, Bonjour profile, local profiling, device classification and so on. Switching policies define central switching or local switching attributes of a WLAN.

  The WLAN profile and Policy profile are both part a Policy Tag and define the characteristics and policy definitions of a set of WLANs.

- AP Join Profile: Consists of the following parameters, Control and Provisioning of Wireless Access Points (CAPWAP) IPv4 or IPv6 , UDP Lite, high availability, retransmit configuration parameters, global AP failover, hyperlocation configuration parameters, Telnet or SSH, 11u parameters, and so on. The default AP join profile values have the global AP parameters and the AP group parameters. Some AP join profile changes require the CAPWAP connection to be reset, because these parameters pertain to the characteristics of the AP.

- Flex Profile: Groups all settings to be assigned to a Flex AP, native VLAN, ACL mapping, and so on. It contains policy attributes and remote site-specific parameters. For example, the Extensible Authentication Protocol (EAP) profiles that can be used when the AP acts as an authentication server.

  The AP Join profile and Flex profile are both part of a Site Tag and define the characteristics of a local or remote site.

- Radio Frequency (RF) Profile: Contains the common radio configuration for APs. RF profiles are applied to all the APs that belong to an AP group, where all the APs in that group have the same profile settings. By default, there exists two default RF profiles, one for 802.11a and one for 802.11b.

### Tags

A tag is defined by the policies associated with it. The properties of the tag is in turn inherited by an associated client or AP. There are various types of tags, each associated with different profiles. No two types of tags include profiles having common properties. Each tag has a default that is created when the system boots up.

- Policy Tag: Defines network and switching policies for the client. QoS is an exception, which constitutes AP policies as well. Policy tag maps the WLAN profile to the policy profile.

  This tag contains the map of the WLAN policy profile. There are 16 entries per policy tag. Changes to the map entries are based on the status of the WLAN profile and policy profile. For example, if a map is added to the policy tag, and both the WLAN profile and the policy profile are enabled, the definitions are pushed to APs using the policy tag. However, if one of them is in the disabled state, the definition is not pushed to the AP. Similarly, if a WLAN profile is already being broadcast by an AP, it can be deleted through the CLI in the policy tag.

- Site Tag: Assigns the AP Join profile settings to the AP. The site tag defines the properties of a site, both central and remote (FlexConnect) site. The attributes of a site that are common across central and remote site are part of the AP Join profile. The attributes that are specific to flex or remote site are part of the Flex profile. The default Site Tag constitutes of the default AP Join profile. There is no default Flex profile.

  Apart from the Flex profile, the site tag also comprises of attributes that are specific to the physical site (and hence cannot be a part of the profile that is a reusable entity).

  If a Flex profile name or an AP profile name is changed in the site tag, the AP is forced to rejoin the controller by disconnecting the Datagram Transport Layer Security (DTLS) session. When a site tag is created, the AP and Flex profiles are set to the default values, default-ap-profile and default-flex-profile.

- RF Tag: Contains the 2.4 GHz and 5 GHz RF profiles. The default RF tag contains the global configuration. Both these profiles contain the same default values for global RF profiles for the respective radios.

An access point is always assigned three tags, one for each type. If a tag is not explicitly defined, the AP will get the default policy, site, or RF tag.

## Roaming Between Policy Tags

Policy tags are used to verify the SSID that is being broadcast by an AP, and the type of policy, so that policy tags define the broadcast domain for a group of APs.

Roaming across two different policy tags (the same SSID, but different policy profile name) or intra-controller roaming will force a client to go through the full authentication and DHCP process to renew its IP address. The process is to prevent clients from jumping from one policy to another without a full reauthentication.

**Note** If a policy profile associated to an SSID is the same (same name and content) in different policy tags, then roaming for that SSID is seamless. The slow roam happens if there is a change in the policy profile associated to the SSID.

## Assigning Tags to Access Points

You can assign tags from the following sources. The sources are listed in the order of priority.

- Static: You select an AP and assign tags. This configuration is saved on the controller based on the AP's Ethernet MAC address. When an AP joins the specific controller, it is always assigned the specified tags.
- Location: This is a configuration construct internal to the Cisco Catalyst 9800 Series Wireless Controller (It is not the AP location that you can configure on each AP.), and is used primarily in the basic setup flow. A location allows you to create a group of three tags (policy, site, and RF) and assign APs to it.
- Filter: You can use a regular expression to assign tags to APs as they join the controller. You can set a filter based only on the AP name, so that this method cannot be used for out-of-the-box APs.
- AP: The AP itself carries the tag information learned through Plug-and-Play (PnP) or pushed from the controller.
- Default: This is the default tag source.

The first two methods of assigning tags (static and location) are static mapping configurations, and hence have the highest priorities. Filter allow you to define a dynamic mapping of APs-to-tags based on regular expressions. When the source is an AP, it means that this information is saved on the AP itself and will be presented to the controller when the AP joins it. If there is no tag mapping configuration on the Cisco Catalyst 9800 Series Wireless Controller, and if APs do not carry any tag information, these APs are assigned default tags.

Access Points are tagged based on the broadcast domain, the site it belongs to, and the desired RF characteristics. Once tagged, the AP gets a list of WLANs to be broadcast along with the properties of the respective SSIDs, properties of the APs on the local or remote site, and the RF properties of the network. By default, an AP is tagged with the default policy, site, and RF tag unless changed. When a tag associated with an AP is changed, the AP resets its CAPWAP connection.

APs are identified by the Ethernet MAC address, and the association to AP and tag is stored in the controller configuration.

Each AP is assigned three unique tags: a policy, site, and RF tag. By default, when an AP joins the controller, it gets default tags; the default policy tag, default site tag, and default RF tag. You can change to the default tags or create custom tags. Use the WebUI to view the tags configured on each AP.

## Preserving Tags When Moving APs Between Controllers

The following conditions must be met when moving APs between controllers:

- If the AP does not have any tag information and there is no mapping configured for that AP on the controller to be joined, the AP is assigned default tags when moved to the controller.
- The AP retains the tag information when moving between the controllers, if both the controllers have the same mapping of AP to the tags. This can be done through static configuration, by assigning the AP to a location, or through filters.
- The AP retains its tag when moved between the two controllers if the tags are saved to the AP and the tags are defined on both controllers.
- If the AP has a saved tag assigned and joins a controller where these tags are not present, the AP is assigned default tags (assuming that no other mapping is configured on the controller that the AP is joining).
- If the AP retains its tag name assignment, but the settings within the tag are different on the two controllers, the AP is configured based on the settings present on the currently joined controller.

Note The above information also applies to N+1 redundancy.

## AP Filter

AP filters are similar to the ACLs used in the controller, and are applied at the global level. You can add AP names as filters, and other attributes can be added as required. You can also add the filter criteria as part of the discovery requests.

The AP Filter feature organizes tag sources with the right priority, based on the configuration.

You cannot disable the AP filter feature. However, the relative priority of a tag source can be configured using **ap filter-priority** *priority filter-name* command.

Note You can configure tag names at the Plug-n-Play (PnP) server (similar to the Flex group and AP group), and the AP stores and send the tag name as part of the discovery and join requests.

# Modifying Access Point Tags

Modifying an AP tag results in the DTLS connection being reset, forcing the AP to rejoin the controller. If only one tag is specified in the configuration, default tags are used for other types. For example, if only policy tag is specified, the default site tag, and default RF tag are used for the site and RF tags.

# RF Tag Profiles

RF Profiles allows you to group set of APs that share a common coverage zone together and selectively change how RRM operates the APs within that coverage zone. For example, a university might deploy a high density of APs in an area where a high number of users congregate or meet. This situation requires that you manipulate both data rates and power to address the cell density while managing the co-channel interference. In adjacent areas, normal coverage is provided and such manipulation would result in a loss of coverage.

Using RF profiles and RF tags allows you to optimize the RF settings for set of APs that operate in different environments or coverage zones. RF profiles are created for the IEEE 802.11 radios and are applied to all APs that are mapped to an RF tag, where all APs with that RF tag have the same profile settings.

CHAPTER 3

# Working with Profiles and Tags

## Assigning Tags to Access Points

You can assign tags from the following sources. The sources are listed in the order of priority.

- Static: You select an AP and assign tags. This configuration is saved on the controller based on the AP's Ethernet MAC address. When an AP joins the specific controller, it is always assigned the specified tags.
- Location: This is a configuration construct internal to the Cisco Catalyst 9800 Series Wireless Controller (It is not the AP location that you can configure on each AP.), and is used primarily in the basic setup flow. A location allows you to create a group of three tags (policy, site, and RF) and assign APs to it.
- Filter: You can use a regular expression to assign tags to APs as they join the controller. You can set a filter based only on the AP name, so that this method cannot be used for out-of-the-box APs.
- AP: The AP itself carries the tag information learned through Plug-and-Play (PnP) or pushed from the controller.
- Default: This is the default tag source.

The first two methods of assigning tags (static and location) are static mapping configurations, and hence have the highest priorities. Filter allow you to define a dynamic mapping of APs-to-tags based on regular expressions. When the source is an AP, it means that this information is saved on the AP itself and will be presented to the controller when the AP joins it. If there is no tag mapping configuration on the Cisco Catalyst 9800 Series Wireless Controller, and if APs do not carry any tag information, these APs are assigned default tags.

Access Points are tagged based on the broadcast domain, the site it belongs to, and the desired RF characteristics. Once tagged, the AP gets a list of WLANs to be broadcast along with the properties of the respective SSIDs, properties of the APs on the local or remote site, and the RF properties of the network. By default, an AP is tagged with the default policy, site, and RF tag unless changed. When a tag associated with an AP is changed, the AP resets its CAPWAP connection.

APs are identified by the Ethernet MAC address, and the association to AP and tag is stored in the controller configuration.

Each AP is assigned three unique tags: a policy, site, and RF tag. By default, when an AP joins the controller, it gets default tags; the default policy tag, default site tag, and default RF tag. You can change to the default tags or create custom tags. Use the WebUI to view the tags configured on each AP.

# Preserving Tags When Moving APs Between Controllers

The following conditions must be met when moving APs between controllers:

- If the AP does not have any tag information and there is no mapping configured for that AP on the controller to be joined, the AP is assigned default tags when moved to the controller.
- The AP retains the tag information when moving between the controllers, if both the controllers have the same mapping of AP to the tags. This can be done through static configuration, by assigning the AP to a location, or through filters.
- The AP retains its tag when moved between the two controllers if the tags are saved to the AP and the tags are defined on both controllers.
- If the AP has a saved tag assigned and joins a controller where these tags are not present, the AP is assigned default tags (assuming that no other mapping is configured on the controller that the AP is joining).
- If the AP retains its tag name assignment, but the settings within the tag are different on the two controllers, the AP is configured based on the settings present on the currently joined controller.

**Note** The above information also applies to N+1 redundancy.

# Modifying Access Point Tags

Modifying an AP tag results in the DTLS connection being reset, forcing the AP to rejoin the controller. If only one tag is specified in the configuration, default tags are used for other types. For example, if only policy tag is specified, the default site tag, and default RF tag are used for the site and RF tags.

# Roaming Between Policy Tags

Policy tags are used to verify the SSID that is being broadcast by an AP, and the type of policy, so that policy tags define the broadcast domain for a group of APs.

Roaming across two different policy tags (the same SSID, but different policy profile name) or intra-controller roaming will force a client to go through the full authentication and DHCP process to renew its IP address. The process is to prevent clients from jumping from one policy to another without a full reauthentication.

Note If a policy profile associated to an SSID is the same (same name and content) in different policy tags, then roaming for that SSID is seamless. The slow roam happens if there is a change in the policy profile associated to the SSID.

# RF Tag Profiles

RF Profiles allows you to group set of APs that share a common coverage zone together and selectively change how RRM operates the APs within that coverage zone. For example, a university might deploy a high density of APs in an area where a high number of users congregate or meet. This situation requires that you manipulate both data rates and power to address the cell density while managing the co-channel interference. In adjacent areas, normal coverage is provided and such manipulation would result in a loss of coverage.

Using RF profiles and RF tags allows you to optimize the RF settings for set of APs that operate in different environments or coverage zones. RF profiles are created for the IEEE 802.11 radios and are applied to all APs that are mapped to an RF tag, where all APs with that RF tag have the same profile settings.

# AP Filter

AP filters are similar to the ACLs used in the controller, and are applied at the global level. You can add AP names as filters, and other attributes can be added as required. You can also add the filter criteria as part of the discovery requests.

The AP Filter feature organizes tag sources with the right priority, based on the configuration.

You cannot disable the AP filter feature. However, the relative priority of a tag source can be configured using **ap filter-priority** *priority filter-name* command.

Note You can configure tag names at the Plug-n-Play (PnP) server (similar to the Flex group and AP group), and the AP stores and send the tag name as part of the discovery and join requests.

CHAPTER 4

# N+1 High Availability

## N+1 High Availability

N+1 mode of high availability in Cisco Catalyst 9800 Series Wireless Controllers allows a single wireless controller (WLC) to be used as a backup controller for 'N' primary controllers. This solution allows high availability to be configured on controllers that are geographically on separate Layer 3 networks or across WAN links.

A single backup controller can be used to provide backup for multiple primary WLCs. These WLCs are independent of each other and do not share configuration or IP addresses on any of their interfaces. Each of these controllers need to be managed separately, and can run a different hardware and a different software version.

**Note** If the software version is different between the primary and secondary controllers, the AP will download the software upon joining the secondary controller, which can result in a higher failover time.

N+1 high availability is stateless, no state information about APs and clients is shared between controllers. As a result, the AP CAPWAP state machine is restarted when the primary controller fails. If the fallback option is enabled, APs fall back from the backup WLC to the primary WLC automatically when the primary WLC resumes operation. APs with the highest priority on the primary connect first to the backup controller.

N+1 mode of high availability can be configured in combination with AP Stateful Switchover (SSO), where the primary and/or secondary controllers are their own SSO pair.

The WLAN security settings must be identical across the N+1 controllers; else, the clients may not be able to connect after a failover.

For more information, see the Cisco Catalyst 9800 Wireless Controller N+1 High Availability White Paper.

CHAPTER 5

# WLANs

## WLANs

The WLANs 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 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.

## 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 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.

## Band Selection

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 AP. 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 non-overlapping 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 are 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 AP 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 AP transmits buffered broadcast and multicast frames for 5 times every second. Either of these settings are suitable for applications, including 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 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.

# 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.

You can also block the peer-to-peer traffic if any two clients do not share the same pre-shared key (PSK). This is supported on local and flex-connect modes.

Peer-to-peer blocking can be configured at three levels: allow, drop, and pre-shared key.

- Allow-private-group: Enables the blocking of peer-to-peer traffic with the same tag value. If allow-private-group is disabled, then all peer-to-peer traffic with different tag values are dropped.
- Drop: Drops all peer-to-peer traffic.
- Forward-upstream: Blocks all peer-to-peer traffic and forwards the traffic to the next-hop device.

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

# 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 APs 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 use the **diag-channel** CLI to run the diagnostic tests.

Note We recommend that you enable the diagnostic channel feature only for nonanchored SSIDs that use the management interface.

# SSIDs

The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple APs or bridges on a network or subnet can use the same SSID. SSIDs are case sensitive, and can contain up to 32 alphanumeric characters. Do not include spaces in your SSID.

When configuring an SSID, assign these following configuration settings to the SSID:

- VLAN
- RADIUS accounting for traffic using the SSID
- APs or bridge authentication method

**Note** VLAN and RADIUS accounting can only be configured for policy profiles. AP or bridge authentication can only be configured for WLANs.

You can assign an username and password to the SSID to allow the AP or bridge to authenticate to your network using LEAP authentication.

If your network uses VLANs, you should assign the access point or bridge SSID to your network's native VLAN.

# WLAN Security

This section describes the WLAN security methods.

## WPA1 and WPA2

Wi-Fi Protected Access (WPA or WPA1) and WPA2 are standards-based security solutions from the Wi-Fi Alliance that provide data protection and access control for wireless LAN systems. WPA1 is compatible with the IEEE 802.11i standard but was implemented prior to the standard's ratification; WPA2 is the Wi-Fi Alliance's implementation of the ratified IEEE 802.11i standard.

By default, WPA1 uses Temporal Key Integrity Protocol (TKIP) and Message Integrity Check (MIC) for data protection while WPA2 uses the stronger Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). By default, both WPA1 and WPA2 use the 802.1X for authenticated key management. However, the following options are also available:

- PSK: When you choose PSK (also known as WPA preshared key or WPA passphrase), you need to configure a preshared key (or a passphrase). This key is used as the Pairwise Master Key (PMK) between clients and the authentication server.
- Cisco Centralized Key Management: uses a fast rekeying technique that enables clients to roam from one AP to another without going through the controller, typically in under 150 milliseconds (ms). Cisco Centralized Key Management reduces the time required by the client to mutually authenticate with the new AP and derive a new session key during re-association. Cisco Centralized Key Management fast secure roaming ensures that there is no perceptible delay in time-sensitive applications, such as wireless VoIP, Enterprise Resource Planning (ERP), or Citrix-based solutions. Cisco Centralized Key Management is a Cisco Compatible Extensions v4-compliant feature. If Cisco Centralized Key Management is selected, only Cisco Centralized Key Management clients are supported.

  When Cisco Centralized Key Management is enabled, the behavior of APS differ from that of the controller for fast roaming in the following ways:

  - If an association request sent by a client has Cisco Centralized Key Management enabled in a Robust Secure Network Information Element (RSN IE), but Cisco Centralized Key Management IE is not encoded and only PMKID is encoded in RSN IE, then the controller does not do a full authentication. Instead, the controller validates the PMKID and does a four-way handshake.
  - If an association request sent by a client has Cisco Centralized Key Management enabled in RSN IE and Cisco Centralized Key Management IE is encoded and only PMKID is present in the RSN IE, then the AP does a full authentication. The AP does not use PMKID sent with the association request when Cisco Centralized Key Management is enabled in RSN IE.

- 802.1X+Cisco Centralized Key Management: During normal operation, 802.1X-enabled clients mutually authenticate with a new access point by performing a complete 802.1X authentication, including communication with the main RADIUS server. However, when you configure your WLAN for 802.1X and Cisco Centralized Key Management fast secure roaming, Cisco Centralized Key Management-enabled clients securely roam from one AP to another without the need to reauthenticate to the RADIUS server. 802.1X+Cisco Centralized Key Management is considered as an optional Cisco Centralized Key Management because both Cisco Centralized Key Management and non-Cisco Centralized Key Management clients are supported when this option is selected.

On a single WLAN, you can allow WPA1, WPA2, and 802.1X/PSK/Cisco Centralized Key Management/802.1X+Cisco Centralized Key Management clients to join. All the APs on such a WLAN advertise WPA1, WPA2, and 802.1X/PSK/Cisco Centralized Key Management/802.1X+Cisco Centralized Key Management information elements in their beacons and probe responses. When you enable WPA1 and/or WPA2, you can also enable one or two ciphers, or cryptographic algorithms, designed to protect data traffic. Specifically, you can enable AES and/or TKIP data encryption for WPA1 and/or WPA2. TKIP is the default value for WPA1, and AES is the default value for WPA2.

## WPA3

WPA3 is a replacement to WPA2, as announced by the Wi-Fi Alliance. The new standard has two modes:

- WPA3-Personal with 128-bit encryption: The WPA3 standard provides a replacement to the WPA2 preshared key (PSK) with Simultaneous Authentication of Equals (SAE), as defined in the IEEE 802.11-2016 standard. With SAE, the user experience is the same (choose a passphrase to connect), but SAE automatically adds a step to the *handshake*, which makes brute force attacks ineffective. With SAE, the passphrase is not exposed, making it impossible for attackers to find the passphrase through brute force dictionary attacks.

  The Protected Management Frames (PMF) should be used for all WPA3-Personal connections. Previously, PMF was an optional capability, which you could configure. With WPA3, PMF must be negotiated for all WPA3 connections that provide an additional layer of protection from de-authentication and dissociation attacks.

- WPA3-Enterprise with 192-bit encryption: This WPA3 standards is aligned with the recommendations from the Commercial National Security Algorithm (CNSA) Suite, which is commonly in place in high-security Wi-Fi networks in verticals such as government, defense, finance, and so on.

## WLAN Layer 2 Security

WLAN supports Layer 2 and Layer 3 security methods. WLANs with the same SSID must have unique Layer 2 security policies so that clients can make a WLAN selection based on the information advertised in beacon and probe responses.

The available Layer 2 security policies are as follows:

- None (open WLAN)
- WPA+WPA2

**Note** Although WPA and WPA2 cannot be used by multiple WLANs with the same SSID, you can configure two WLANs with the same SSID with WPA/TKIP with PSK and Wi-Fi Protected Access (WPA)/Temporal Key Integrity Protocol (TKIP) with 802.1X, or with WPA/TKIP with 802.1X or WPA/AES with 802.1X.

A WLAN configured with TKIP support will not be enabled on an RM3000AC module.

- Static Wired Equivalent Privacy (WEP) (not supported on Wave 2 APs)
- WPA2+WPA3
- Enhanced Open

CHAPTER 6

# Remote LANs

## Remote LAN

A Remote LAN (RLAN) is used for authenticating wired clients using the controller. Once the wired client successfully joins the controller, the LAN ports switch the traffic between central or local switching modes. The traffic from wired client is treated as wireless client traffic.

The RLAN in an AP sends the authentication request to authenticate the wired client. The authentication of wired client in RLAN is similar to the central authenticated wireless client.

**Note** RLAN is supported in APs that have more than one Ethernet port.

CHAPTER 7

# Scale Information

## Scale Information

For scale information, see the FlexConnect Catalyst Wireless Branch Deployment Guide.

CHAPTER 8

# Supported Releases

## Supported Releases

- Cisco IOS XE Gibraltar 16.10.1 and later releases

CHAPTER 9

# Recommendations and Limitations

-

## Recommendations

This section provides some recommendations that you can keep in mind while using the Cisco Catalyst 9800 Series Wireless Controller configuration model.

- When you design your Cisco Catalyst wireless network, it is important to consider site tags and the way these are mapped to APs. For the best performance of your Cisco Catalyst 9800 Series Wireless Controller, it is recommended that you:
  - Use custom site tags and not the default site tag.
  - Assign the same site tag to all the APs in the same roaming domain.
  - Limit the number of APs to 500 per site tag whenever possible.
  - Do not exceed the following maximum number of APs per site tag:

*Table 1: Maximum Number of APs per Site Tag*

| Platform | Maximum Number of APs per Site Tag |
|---|---|
| • Cisco Catalyst 9800-80 Series Wireless Controller (medium and large)<br>• Cisco Catalyst 9800-CL Wireless Controller for Cloud (medium and large) | 1600 |
| Cisco Catalyst 9800-40 Series Wireless Controller | 800 |
| Any other Cisco Catalyst 9800 platform | Equal to the maximum number of APs supported. |

- When designing your policy tag assignment, ensure that all APs in the same roaming domain should have the same policy profile. In case you need to assign different policies, then we recommend that you use Cisco IOS XE Amsterdam 17.3.x and later releases.
- We recommend that you limit the number of SSIDs configured on the controller. You can configure 16 simultaneous WLANs or SSIDs (per radio on each AP). Because each WLAN or SSID needs separate probe responses and beacons transmitted at the lowest mandatory rate, the RF pollution increases as more SSIDs are added.

  Also, some smaller wireless stations such as PDAs, Wi-Fi phones, and barcode scanners cannot cope with a high number of Basic SSIDs (BSSIDs) over the air. This results in lockups, reloads, or association failures. It is recommended that you have one to three SSIDs for an enterprise, and one SSID for high-density designs. By using the AAA override feature, you can reduce the number of WLANs or SSIDs while assigning individual per-user VLAN/settings in a single-SSID scenario.
- Because you can modify the existing tags, create new ones, and attach these tags to APs in different ways, we recommend that you validate the tag configuration using the following command:

  ```
  Device# wireless config validate
  ```
- Do not mix clients with DHCP and static IP address on the same SSID when associating with a VLAN group.
- To enhance security, ensure that all clients obtain their IP addresses from the DHCP server. The DHCP-Required option in the Policy profile settings forces clients to request or renew a DHCP address every time they associate with a WLAN, before they are allowed to send or receive other traffic in the network. The DHCP-Required option allows for strict control over the IP addresses in use.
- Set the per-WLAN user idle timeout to 3600 seconds (60 minutes) to reduce the likelihood of client getting deleted when moving out of coverage areas or when the client is battery-operated and may go to sleep frequently.
- If you have devices that are still using Cisco Centralized Key Management, ensure that you change Cisco Centralized Key Management validation to 5 seconds to avoid roaming issues when using Cisco-based clients.

# Restrictions for WLANs

- Do not configure pre-shared key (PSK) and Cisco Centralized Key Management in a WLAN, because this configuration is not supported.
- Ensure that the Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES) ciphers are enabled with Wi-Fi Protected Access (WPA1) configuration, else In-Service Software Upgrade (ISSU) may break during the upgrade process.
- When you change the WLAN profile name, the 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, because the 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 the shutting down of 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 are not supported.
- In a dual-stack (with IPv4 and IPv6 configured) Cisco Catalyst 9800 Series Wireless Controller, if an AP tries to join the controller with the IPv6 tunnel before the IPv4 tunnel gets cleared, you will see a traceback, and the 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 is assigned to the same AP radio, you must have a unique Layer 2 security policy so that clients can safely select between these WLANs.
- The SSID that is sent as part of the user profile works only if the **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 not supported in FlexConnect mode or local mode.
- You cannot mix open configuration models with CLI-based, GUI-based, or DNA Center-based configurations. However, if you decide to use multiple model types, these 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.

⚠

**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.

# Restrictions for Peer-to-Peer Blocking

- Peer-to-peer blocking does not apply to multicast traffic.
- Peer-to-peer blocking is not enabled by default.
- 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.
- Unified solution for central switching clients supports peer-to-peer upstream-forward. However, this is not supported in the FlexConnect solution; it is treated as peer-to-peer drop, and client packets are dropped.

# Restrictions for DHCP for WLANs

- If you override the DHCP server in a WLAN, you must ensure that you configure the underlying Cisco IOS configuration in such a way that the DHCP server is reachable.
- WLAN DHCP override works only if DHCP service is enabled on the device.

  You can configure DHCP service in either of the following ways:

  - Configuring the DHCP pool on the device.
  - Configuring a DHCP relay agent on the SVI. Note that the VLAN of the SVI must be mapped to the WLAN where DHCP override is configured.

## Topic 2.1

# Restrictions for FlexConnect DHCP-Required

The following are the restrictions and limitations for the FlexConnect DHCP-Required feature:

- The DHCP-Required feature is applicable for IPv4 addresses only.
- The IP-MAC binding can be pushed to other APs only through the custom policy profile. IP-MAC binding is not available in the default policy. The mapping is propagated to all the APs in the same custom policy profile.
- The DHCP-Required feature works on IP-MAC binding basis and is not supported with the third-party work group bridge (WGB), where WGB wired client information is not shared to AP by the WGB.

CHAPTER 10

# Configuration Workflow

## Configuration Workflow

The following set of steps defines the logical order of configuration. Apart from the WLAN profile, all the profiles and tags have a default object associated with it.

You can configure an AP to operate in either the FlexConnect mode or local mode.

- FlexConnect: To operate in FlexConnect mode, assign the AP to a site tag that is configured to be the remote site, and Cisco Catalyst 9800 Series Wireless Controllers will automatically move to FlexConnect mode. The AP will not reboot but will go for a CAPWAP restart and rejoin in less than 30 seconds. The default flex profile is selected. For more information, see the *FlexConnect* chapter.
- Local: Local switching on the WLAN provides resiliency against WAN failures and reduces the amount of data going over the WAN, thus reducing the WAN bandwidth usage. Local switching is useful in deployments where resources are local to the branch site and data traffic does not need to be sent back to the controller over the WAN link.

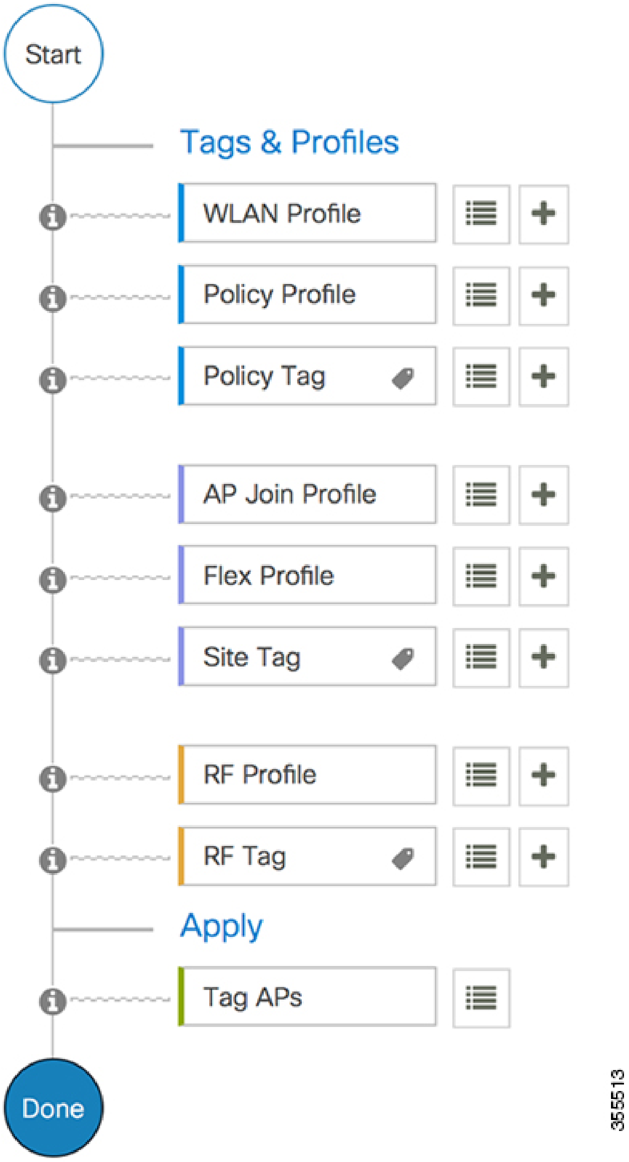
**Note** FlexConnect is not supported in local mode.

1. Create the following profiles:
    - WLAN
    - Policy
    - AP Join
    - Flex: Not supported in local mode.
    - RF
2. Create the following tags:
    - Policy
    - Site

- RF

3. Associate tags to an AP.

*Figure 2: Configuration Workflow*



CHAPTER 11

# Configuring Profiles

# Configuring Profiles Through the CLI

## Configuring a Wireless Profile Policy (CLI)

Follow the procedure given below to configure a wireless profile policy:

**Note** When a client moves from an old controller to a new controller (managed by Cisco Prime Infrastructure), the old IP address of the client is retained, if the IP address is learned by ARP or data gleaning. To avoid this scenario, ensure that you enable **ipv4 dhcp required** command in the policy profile. Otherwise, the IP address gets refreshed only after a period of 24 hours.

### SUMMARY STEPS

1. **configure terminal**
2. **wireless profile policy** *profile-policy*
3. **idle-timeout** *timeout*
4. **vlan** *vlan-id*
5. **no shutdown**
6. **show wireless profile policy summary**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **wireless profile policy** *profile-policy*<br>**Example:**<br>`Device(config)# wireless profile policy rr-xyz-policy-1` | Configures WLAN policy profile and enters wireless policy configuration mode. |
| **Step 3** | **idle-timeout** *timeout*<br>**Example:**<br>`Device(config-wireless-policy)# idle-timeout 1000` | (Optional) Configures the duration of idle timeout, in seconds. |
| **Step 4** | **vlan** *vlan-id*<br>**Example:**<br>`Device(config-wireless-policy)# vlan 24` | Configures VLAN name or VLAN ID. |
| **Step 5** | **no shutdown**<br>**Example:**<br>`Device(config-wireless-policy)# no shutdown` | Saves the configuration and exits configuration mode and returns to privileged EXEC mode. |
| **Step 6** | **show wireless profile policy summary**<br>**Example:**<br>`Device# show wireless profile policy summary` | Displays the configured policy profiles.<br>**Note** (Optional) To view detailed information about a policy profile, use the **show wireless profile policy detailed** *policy-profile-name* command. |

# Configuring a Flex Profile (CLI)

Follow the procedure given below to set a flex profile:

## SUMMARY STEPS

1. **configure terminal**
2. **wireless profile flex** *flex-profile*
3. **description**
4. **arp-caching**
5. **end**
6. **show wireless profile flex summary**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 2** | **wireless profile flex** *flex-profile*<br>**Example:** | Configures a Flex profile and enters Flex profile configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config)# wireless profile flex rr-xyz-flex-profile` | |
| **Step 3** | **description**<br>**Example:**<br>`Device(config-wireless-flex-profile)# description xyz-default-flex-profile` | (Optional) Enables default parameters for the flex profile. |
| **Step 4** | **arp-caching**<br>**Example:**<br>`Device(config-wireless-flex-profile)# arp-caching` | (Optional) Enables ARP caching. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config-wireless-flex-profile)# end` | Saves the configuration and exits configuration mode and returns to privileged EXEC mode. |
| **Step 6** | **show wireless profile flex summary**<br>**Example:**<br>`Device# show wireless profile flex summary` | (Optional) Displays the flex-profile parameters.<br>**Note** To view detailed parameters about the flex profile, use the **show wireless profile flex detailed** *flex-profile-name* command. |

# Configuring an AP Profile (CLI)

When you modify an AP join profile in the controller, the Network Time Protocol (NTP) server IP is not pushed to the AP. This is because, the AP profile-specific NTP server IP is introduced to address the time sensitivity of the Hyperlocation feature and is pushed to the AP only when the operational status of Hyperlocation is Up. This behavior is applicable to all Hyperlocation-related TLVs (trigger threshold, reset threshold, and detection threshold) as well.

Configure the options that are required. Not all options are mandatorily required.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap profile** *ap-profile*
4. **description** *ap-profile-name*
5. **accounting method-list***method-list-name*
6. **antenna monitoring**
7. **apphost**
8. **auxiliary-client interface vlan** *vlan-ID*
9. **awips forensic**
10. **bssid-neighbor-stats interval** *interval*
11. **bssid-stats bssid-stats-frequency** *seconds*
12. **capwap** {**backup** | **fallback** | **retransmit** | **timers** | **udplite** | **window**}
13. **capwap-discovery** {**private** | **public**}

14. **cdp**
15. **cisco-dna grpc**
16. **client-rssi-stats interval** *interval*
17. **core-dump tftp-server** *ipv4/ipv6* **filename** *filename* {**compress** | **uncompress**}
18. **dhcp-server**
19. **dot11** {**24ghz** | **5ghz**} **reporting-interval** *interval*
20. **dot1x** {**eap-type** | **5ghz** | **lsc-ap-auth-state** | **max-sessions** *sessions* | **username**}
21. **ext-module**
22. **gas-ap-rate-limit** *maximum-requests-allowed request-limit-interval*
23. **hyper-location**
24. **icap subscription ap rf spectrum enable**
25. **ip dhcp fallback**
26. **jumbo-mtu**
27. **lag**
28. **ledflash** {**duration** *duration* | **indefinite**}
29. **link-encryption**
30. **link-latency**
31. **mesh-profile** *name*
32. **mgmtuser username** *username* **password** {**0** | **8**} _password_**secret** {**0** | **8** } *secret*
33. **ntp ip**{*ipv4-address* | *ipv6-address* }
34. **oeap** {**link-encryption** | **local-access** | **provisioning-ssid** | **rogue-detection**}
35. **packet-capture** *profile-name*
36. **pakseq-jump-delba**
37. **power** {**injector** {**installed** | **override** | **switch-mac-address**} | **pre-standard**}
38. **preferred-mode** {**disable** | **ipv4** | **ipv6**}
39. **qos-map action-frame**
40. **rogue detection report-interval** *interval*
41. **ssh**
42. **ssid broadcast persistent**
43. **statistics traffic-distribution interval** *interval*
44. **stats-timer** *duration*
45. **syslog level** {**alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings** }
46. **tcp-adjust-mss** {**enable** | **size** *mss-value*
47. **telnet**
48. **trace** *profile-name*
49. **usb-enable**
50. **end**
51. **show ap profile name**_profile-name_ **detailed**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:** | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device> enable` | |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ap profile** *ap-profile*<br>**Example:**<br>`Device(config)# ap profile xyz-ap-profile` | Configures an AP profile and enters AP profile configuration mode.<br>**Note** When you delete a named profile, the APs associated with that profile will not revert to the default profile. |
| **Step 4** | **description** *ap-profile-name*<br>**Example:**<br>`Device(config-ap-profile)# description "xyz ap profile"` | Adds a description for the AP profile. |
| **Step 5** | **accounting method-list***method-list-name*<br>**Example:**<br>`Device(config-ap-profile)# accounting method-list accounting-list1` | Configures an accounting method-list. |
| **Step 6** | **antenna monitoring**<br>**Example:**<br>`Device(config-ap-profile)# antenna monitoring` | Configures detection of broken AP antennas. |
| **Step 7** | **apphost**<br>**Example:**<br>`Device(config-ap-profile)# apphost` | Enables the application hosting framework on Cisco APs. |
| **Step 8** | **auxiliary-client interface vlan** *vlan-ID*<br>**Example:**<br>`Device(config-ap-profile)# auxiliary-client interface vlan vlan1` | Configures the auxiliary-client interface VLAN. |
| **Step 9** | **awips forensic**<br>**Example:**<br>`Device(config-ap-profile)# awips forensic` | Enables Adaptive Wireless Intrusion Prevention System (wIPS). |
| **Step 10** | **bssid-neighbor-stats interval** *interval*<br>**Example:**<br>`Device(config-ap-profile)# bssid-neighbor-stats interval 23` | Configures the interval at which BSSID neighbor statistics is sent from the AP.<br>• BSSID is the MAC address of the wireless access point. |
| **Step 11** | **bssid-stats bssid-stats-frequency** *seconds*<br>**Example:** | Sets the frequency timer for BSSID statistics. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-ap-profile)# bssid-stats bssid-stats-frequency 100` | |
| **Step 12** | **capwap** {**backup** \| **fallback** \| **retransmit** \| **timers** \| **udplite** \| **window**}<br>**Example:**<br>`Device(config-ap-profile)# capwap fallback` | Sets the Control and Provisioning of Wireless Access Points Protocol (CAPWAP) parameters. |
| **Step 13** | **capwap-discovery** {**private** \| **public**}<br>**Example:**<br>`Device(config-ap-profile)# capwap-discovery private` | Configures the CAPWAP discovery response.<br>• Based on the configured parameters, either private IP addresses or public IP addresses are inclued in the discovery. |
| **Step 14** | **cdp**<br>**Example:**<br>`Device(config-ap-profile)# cdp` | Configures Cisco Discovery Protocol. |
| **Step 15** | **cisco-dna grpc**<br>**Example:**<br>`Device(config-ap-profile)# cisco-dna grpc` | Enables the GRPC channel to Cisco DNA. |
| **Step 16** | **client-rssi-stats interval** *interval*<br>**Example:**<br>`Device(config-ap-profile)# client-rssi-stats interval 34` | Configures the client Received Signal Strength Indicator (RSSI) statistics reporting interval. |
| **Step 17** | **core-dump tftp-server** *ipv4/ipv6* **filename** *filename* {**compress** \| **uncompress**}<br>**Example:**<br>`Device(config-ap-profile)# core-dump tftp-server 2001:db8::2 filename file1 compress` | Enables core dump of the memory. |
| **Step 18** | **dhcp-server**<br>**Example:**<br>`Device(config-ap-profile)# dhcp-server` | Configures a DHCP server. |
| **Step 19** | **dot11** {**24ghz** \| **5ghz**} **reporting-interval** *interval*<br>**Example:**<br>`Device(config-ap-profile)# dot11 24ghz reporting-interval 78` | Configures a interval at which client report needs to be sent from AP to clients on the specified radio frequency. |
| **Step 20** | **dot1x** {**eap-type** \| **5ghz** \| **lsc-ap-auth-state** \| **max-sessions** *sessions* \| **username**}<br>**Example:**<br>`Device(config-ap-profile)# dot1x max-sessions 30` | Configures IEEE 802.1X credentials for all APs . |

| | Command or Action | Purpose |
|---|---|---|
| **Step 21** | **ext-module**<br>**Example:**<br>`Device(config-ap-profile)# ext-module` | Enables the extended module on all APs. |
| **Step 22** | **gas-ap-rate-limit** *maximum-requests-allowed request-limit-interval*<br>**Example:**<br>`Device(config-ap-profile)# gas-ap-rate-limit 35 900` | Limits the number of Generic Advertisement Services (GAS) request action frames to be sent to the controller by an AP in a given interval. |
| **Step 23** | **hyper-location**<br>**Example:**<br>`Device(config-ap-profile)# hyperlocation` | Configures the hyperlocation feature on all supported APs. |
| **Step 24** | **icap subscription ap rf spectrum enable**<br>**Example:**<br>`Device(config-ap-profile)# icap subscription ap rf spectrum enable` | Configures the radio frequency spectrum subscription. |
| **Step 25** | **ip dhcp fallback**<br>**Example:**<br>`Device(config-ap-profile)# ip dhcp fallback` | Configures DHCP fallback.<br>**Note** DHCP fallback is enabled by default. So, if an AP is assigned a static IP address and unable to reach the controller, the AP falls back to the DHCP. To stop an AP from moving the static IP to DHCP, you must disable the DHCP fallback configuration in an AP join profile. |
| **Step 26** | **jumbo-mtu**<br>**Example:**<br>`Device(config-ap-profile)# jumbo-mtu` | Enables jumbo maximum transmission unit (MTU) status. |
| **Step 27** | **lag**<br>**Example:**<br>`Device(config-ap-profile)# lag` | Enables CAPWAP lag for Cisco APs. |
| **Step 28** | **ledflash** {**duration** *duration* \| **indefinite**}<br>**Example:**<br>`Device(config-ap-profile)# ledflash indefinite` | Enables LED-state for all Cisco APs. |
| **Step 29** | **link-encryption**<br>**Example:**<br>`Device(config-ap-profile)# link-encryption` | Enables the link encryption state on all Cisco APs. |
| **Step 30** | **link-latency**<br>**Example:** | Enables link latency on all Cisco APs. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-ap-profile)# link-latency` | |
| **Step 31** | **mesh-profile** *name*<br>**Example:**<br>`Device(config-ap-profile)# mesh-profile mesh1` | Configures the mesh profile. |
| **Step 32** | **mgmtuser username** *username* **password** {**0** \| **8**} *password***secret** {**0** \| **8** } *secret*<br>**Example:**<br>`Device(config-ap-profile)# mgmtuser username mgmtuser1 password 8 password1 secret 8 secret8` | Configures an username, password and a secret for privileged AP management. |
| **Step 33** | **ntp ip**{*ipv4-address* \| *ipv6-address* }<br>**Example:**<br>`Device(config-ap-profile)# ntp ip 2001:db8::1` | Configures the NTP server IP/IPv6 address. |
| **Step 34** | **oeap** {**link-encryption** \| **local-access** \| **provisioning-ssid** \| **rogue-detection**}<br>**Example:**<br>`Device(config-ap-profile)# oeap link-encryption` | Enables link encryption for Cisco OfficeExtend access points (OEAPs). |
| **Step 35** | **packet-capture** *profile-name*<br>**Example:**<br>`Device(config-ap-profile)# packet-capture pcap1` | Configures a profile for packet capturing. |
| **Step 36** | **pakseq-jump-delba**<br>**Example:**<br>`Device(config-ap-profile)# pakseq-jump-delba` | Configures the AP radio to send DELBA on packet sequence. |
| **Step 37** | **power** {**injector** {**installed** \| **override** \| **switch-mac-address**} \| **pre-standard**}<br>**Example:**<br>`Device(config-ap-profile)# power pre-standard` | Enables the power over Ethernet (PoE) switch state. |
| **Step 38** | **preferred-mode** {**disable** \| **ipv4** \| **ipv6**}<br>**Example:**<br>`Device(config-ap-profile)# preferred-mode disable` | Disables preferred-mode. |
| **Step 39** | **qos-map action-frame**<br>**Example:**<br>`Device(config-ap-profile)# qos-map action-frame` | Sends 802.11 QoS map-action frame when the QoS map-configuration changes. |
| **Step 40** | **rogue detection report-interval** *interval*<br>**Example:**<br>`Device(config-ap-profile)# rogue detection report-interval 100` | Configures rogue-detection report-interval for monitor mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 41** | **ssh**<br>**Example:**<br>`Device(config-ap-profile)# ssh` | Enables SSH, if the AP user management credentials are nondefault. |
| **Step 42** | **ssid broadcast persistent**<br>**Example:**<br>`Device(config-ap-profile)# ssid broadcast persistent` | Enables persistent Service Set Identifier (SSID) broadcast on the profile. |
| **Step 43** | **statistics traffic-distribution interval** *interval*<br>**Example:**<br>`Device(config-ap-profile)# statistics traffic-distribution interval 90` | Enables traffic distribution statistics. |
| **Step 44** | **stats-timer** *duration*<br>**Example:**<br>`Device(config-ap-profile)# stats-timer 8` | Configures the duration of the statistics timer. |
| **Step 45** | **syslog level** {**alerts** \| **critical** \| **debugging** \| **emergencies** \| **errors** \| **informational** \| **notifications** \| **warnings** }<br>**Example:**<br>`Device(config-ap-profile)# syslog level critical` | Configures the system error message logging settings. |
| **Step 46** | **tcp-adjust-mss** {**enable** \| **size** *mss-value*<br>**Example:**<br>`Device(config-ap-profile)# tcp-adjust-mss enable` | Enables the TCP maximum segment size configuration for all Cisco APs. |
| **Step 47** | **telnet**<br>**Example:**<br>`Device(config-ap-profile)# telnet` | Enables Telnet, if the AP user management credentials are nondefault. |
| **Step 48** | **trace** *profile-name*<br>**Example:**<br>`Device(config-ap-profile)# trace trace-profile` | Configures the AP trace profile. |
| **Step 49** | **usb-enable**<br>**Example:**<br>`Device(config-ap-profile)# usb-enable` | Enables USBs for Cisco APs. |
| **Step 50** | **end**<br>**Example:**<br>`Device(config-ap-profile)# end` | Exits AP profile configuration mode and returns to privileged EXEC mode. |
| **Step 51** | **show ap profile name***profile-name* **detailed**<br>**Example:** | (Optional) Displays detailed information about an AP join profile. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device# show ap profile name xyz-ap-profile detailed` | |

## Configuring an RF Profile (CLI)

All steps given in this task may not be required for your configuration, use the ones that are required.

### Before you begin

Ensure that you use the same RF profile name that you create here, when you configure the wireless RF tag. If there is a mismatch in the RF profile name (for example, if the RF tag contains an RF profile that does not exist), the corresponding radios will not come up.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap dot11 24ghz rf-profile** *rf-profile*
4. **default**
5. **airtime** {**bridge-client-access airtime-allocation** *allocation-percentage* | **mode** {**enforce-policy** | **monitor**} | **optimization**}
6. **band-select cycle** {**count** *cycles-not-responding* | **threshold** *threshold-value*}
7. **channel** {**add** *channel-number* | **foreign** | **remove** *channel-number*}
8. **client-network-preference** {**connectivity** | **default** | **throughput**}
9. **coverage** {**data rssi threshold** *threshold-value* | **exception** *exception-level* | **level** *exception-level* | **voice rssi threshold** *threshold-value*}
10. **description** *description*
11. **dot11ax spatial-reuse obss-pd** [**non-srg-max** *tnon-SRG-value*]
12. **high-density** {**clients count** *maximum-client-connections* | **multicast data-rate** *options*| **rx-sop threshold** {**auto** | **custom** *RX-SOP-value* | **high** | **low** | **medium**}
13. **hsr-mode** [**neighbor-timeout** *neighbor-timeout*]
14. **load-balancing** {**denial** *denial-count* | **window** *number-of-clients* }
15. **ndp-mode** {**auto** | **off-channel**}
16. **rate** {*options* {**disable** | **mandatory** | **supported** } | **mcs** *index-number*}
17. **trap threshold** {**clients** | **interference** | **noise** | **utilization** } *threshold*
18. **tx-power** {**max** | **min** | **v1 threshold** } *threshold*
19. **no shutdown**
20. **end**
21. **show ap rf-profile summary**
22. **show ap rf-profile name** *rf-profile* **detail**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable** | Enables privieged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device> enable` | • Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ap dot11 24ghz rf-profile** *rf-profile*<br>**Example:**<br>`Device(config)# ap dot11 24ghz rf-profile rfprof24_1` | Configures an RF profile and enters RF profile configuration mode. |
| **Step 4** | **default**<br>**Example:**<br>`Device(config-rf-profile)# default` | (Optional) Enables default parameters for the RF profile. |
| **Step 5** | **airtime** {**bridge-client-access airtime-allocation** *allocation-percentage* \| **mode** {**enforce-policy** \| **monitor**} \| **optimization**}<br>**Example:**<br>`Device(config-rf-profile)# airtime mode enforce-policy` | Configures airtime-fairness in enforce-policy mode. |
| **Step 6** | **band-select cycle** {**count** *cycles-not-responding* \| **threshold** *threshold-value*}<br>**Example:**<br>`Device(config-rf-profile)# band-select cycle threshold 90` | Sets the time threshold for a new scanning cycle. |
| **Step 7** | **channel** {**add** *channel-number* \| **foreign** \| **remove** *channel-number*}<br>**Example:**<br>`Device(config-rf-profile)# channel add 9` | Specifies the channel number to be added to the DCA allowed channel list. |
| **Step 8** | **client-network-preference** {**connectivity** \| **default** \| **throughput**}<br>**Example:**<br>`Device(config-rf-profile)# client-network-preference connectivity` | Applies connectivity preference for the client network. |
| **Step 9** | **coverage** {**data rssi threshold** *threshold-value* \| **exception** *exception-level* \| **level** *exception-level* \| **voice rssi threshold** *threshold-value*}<br>**Example:**<br>`Device(config-rf-profile)# coverage exception 90` | Sets the Cisco AP coverage exception level. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 10** | **description** *description*<br>**Example:**<br>`Device(config-rf-profile)# description rfprof24_1` | (Optional) Adds a description to the RF profile. |
| **Step 11** | **dot11ax spatial-reuse obss-pd** [**non-srg-max** *tnon-SRG-value*]<br>**Example:**<br>`Device(config-rf-profile)# dot11ax spatial-reuse obss-pd non-srg-max -78` | Configures the maximum 802.11ax non-SRG OBSS PD value. |
| **Step 12** | **high-density** {**clients count** *maximum-client-connections* \| **multicast data-rate** *options*\| **rx-sop threshold** {**auto** \| **custom** *RX-SOP-value* \| **high** \| **low** \| **medium**}<br>**Example:**<br>`Device(config-rf-profile)# high-density client count 90` | Configures the maximum client connections per AP radio. |
| **Step 13** | **hsr-mode** [**neighbor-timeout** *neighbor-timeout*]<br>**Example:**<br>`Device(config-rf-profile)# hsr-mode` | Enables High-Speed Roam (HSR) mode for the RF profile. |
| **Step 14** | **load-balancing** {**denial** *denial-count* \| **window** *number-of-clients* }<br>**Example:**<br>`Device(config-rf-profile)# load-balancing window 12` | Sets the aggressive load-balancing client window. |
| **Step 15** | **ndp-mode** {**auto** \| **off-channel**}<br>**Example:**<br>`Device(config-rf-profile)# ndp-mode auto` | Enables Neighbor Discovery Protocol (NDP) auto mode. |
| **Step 16** | **rate** {*options* {**disable** \| **mandatory** \| **supported** } \| **mcs** *index-number*}<br>**Example:**<br>`Device(config-rf-profile)# rate mcs 20` | Configures modulation and coding scheme (MCS) data rates for the RF profile. |
| **Step 17** | **trap threshold** {**clients** \| **interference** \| **noise** \| **utilization** } *threshold*<br>**Example:**<br>`Device(config-rf-profile)# trap theshold noise -90` | Configures the trap threshold for noise. |
| **Step 18** | **tx-power** {**max** \| **min** \| **v1 threshold** } *threshold*<br>**Example:**<br>`Device(config-rf-profile)# tx-power min 12` | Configures the minimum auto-RF transmit power. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 19** | **no shutdown**<br>**Example:**<br>`Device(config-rf-profile)# no shutdown` | Enables the RF profile on the device. |
| **Step 20** | **end**<br>**Example:**<br>`Device(config-rf-profile)# end` | Exits RF profile configuration mode and returns to privileged EXEC mode. |
| **Step 21** | **show ap rf-profile summary**<br>**Example:**<br>`Device# show ap rf-profile summary` | (Optional) Displays the summary of the available RF profiles. |
| **Step 22** | **show ap rf-profile name** *rf-profile* **detail**<br>**Example:**<br>`Device# show ap rf-profile name rfprof24_1 detail` | (Optional) Displays detailed information about a particular RF profile. |

# Configuring Profiles through the GUI

-

## Configuring a Wireless Profile Policy (GUI)

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

**Step 2** On the **Policy Profile** page, click **Add**.

**Step 3** In the **Add Policy Profile** window, in **General** tab, enter a name and description for the policy profile. The name can be ASCII characters from 32 to 126, without leading and trailing spaces. Do not use spaces as it causes system instability.

**Step 4** To enable the policy profile, set **Status** as **Enabled**.

**Step 5** Use the slider to enable or disable **Passive Client** and **Encrypted Traffic Analytics**.

**Step 6** In the **CTS Policy** section, choose the appropriate status for the following:

- Inline Tagging—a transport mechanism using which a controller or access point understands the source SGT.
- SGACL Enforcement

**Step 7** Specify a default **SGT**. The valid range is from 2 to 65519.

**Step 8** In the WLAN Switching Policy section, choose the following, as required:

- Central Switching: Tunnels both the wireless user traffic and all control traffic via CAPWAP to the centralized controller where the user traffic is mapped to a dynamic interface/VLAN on the controller. This is the normal CAPWAP mode of operation.
- Central Authentication: Tunnels client data to the controller, as the controller handles client authentication.

- Central DHCP: The DHCP packets received from AP are centrally switched to the controller and then forwarded to the corresponding VLAN based on the AP and the SSID.
- Central Association Enable: When central association is enabled, all switching is done on the controller.
- Flex NAT/PAT: Enables Network Address Translation(NAT) and Port Address Translation (PAT) mode.

**Step 9** Click **Save & Apply to Device**.

# Configuring a Flex Profile (GUI)

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

**Step 2** Click **Add**.

**Step 3** Enter the **Name** of the Flex Profile. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

**Step 4** In the **Description** field, enter a description for the Flex Profile.

**Step 5** Click **Apply to Device**.

# Configuring an AP Profile (GUI)

### Before you begin

The default AP join profile values will have the global AP parameters and the AP group parameters. The AP join profile contains attributes that are specific to AP, such as CAPWAP, IPv4/IPv6, UDP Lite, High Availability, retransmit configuration parameters, global AP failover, Hyperlocation configuration parameters, Telnet/SSH, 11u parameters, and so on.

**Step 1** Choose **Configuration** > **Tags & Profiles** > **AP Join**.

**Step 2** On the **AP Join Profile** page, click **Add**.

The **Add AP Join Profile** page is displayed.

**Step 3** In the **General** tab, enter a name and description for the AP join profile. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

**Step 4** Check the **LED State** check box to set the LED state of all APs connected to the device to blink so that the APs are easily located.

**Step 5** In the **Client** tab and **Statistics Timer** section, enter the time in seconds that the AP sends its 802.11 statistics to the controller.

**Step 6** In the **TCP MSS Configuration** section, check the **Adjust MSS Enable** check box to enter value for Adjust MSS. You can enter or update the maximum segment size (MSS) for transient packets that traverse a router. TCP MSS adjustment enables the configuration of the maximum segment size (MSS) for transient packets that traverse a router, specifically TCP segments with the SYN bit set.

In a CAPWAP environment, a lightweight access point discovers a device by using CAPWAP discovery mechanisms, and then sends a CAPWAP join request to the device. The device sends a CAPWAP join response to the access point that allows the access point to join the device.

When the access point joins the device, the device manages its configuration, firmware, control transactions, and data transactions.

**Step 7** In the **CAPWAP** tab, you can configure the following:

- High Availability

  You can configure primary and secondary backup controllers for all access points (which are used if primary, secondary, or tertiary controllers are not responsive) in this order: primary, secondary, tertiary, primary backup, and secondary backup. In addition, you can configure various timers, including heartbeat timers and discovery request timers. To reduce the controller failure detection time, you can configure the fast heartbeat interval (between the controller and the access point) with a smaller timeout value. When the fast heartbeat timer expires (at every heartbeat interval), the access point determines if any data packets have been received from the controller within the last interval. If no packets have been received, the access point sends a fast echo request to the controller.

a) In the **High Availability** tab, enter the time (in seconds) in the **Fast Heartbeat Timeout** field to configure the heartbeat timer for all access points. Specifying a small heartbeat interval reduces the amount of time it takes to detect device failure.
b) In the **Heartbeat Timeout** field, enter the time (in seconds) to configure the heartbeat timer for all access points. Specifying a small heartbeat interval reduces the amount of time it takes to detect device failure.
c) In the **Discovery Timeout** field, enter a value between 1 and 10 seconds (inclusive) to configure the AP discovery request timer.
d) In the **Primary Discovery Timeout** field, enter a value between 30 and 3000 seconds (inclusive) to configure the access point primary discovery request timer.
e) In the **Primed Join Timeout** field, enter a value between 120 and 43200 seconds (inclusive) to configure the access point primed join timeout.
f) In the **Retransmit Timers Count** field, enter the number of times that you want the AP to retransmit the request to the device and vice-versa. Valid range is between 3 and 8.
g) In the **Retransmit Timers Interval** field, enter the time duration between retransmission of requests. Valid range is between 2 and 5.
h) Check the **Enable Fallback** check box to enable fallback.
i) Enter the **Primary Controller** name and IP address.
j) Enter the **Secondary Controller** name and IP address.
k) Click **Save & Apply to Device**.

**Note** The primary and secondary settings in the AP join profile are not used for AP fallback. This means that the AP will not actively probe for those controllers (which are a part of the AP join profile), when it has joined one of them.

This setting is used only when the AP loses its connection with the controller, and then prioritizes which other controller it should join. These controllers have a priority of 4 and 5, following APs in the **High Availability** tab of the AP page.

The APs that are added as the primary, secondary, and tertiary APs in the **High Availability** tab of the AP configuration page, are actively probed and are used for the AP fallback option.

- Advanced

a) In the **Advanced** tab, check the **Enable VLAN Tagging** check box to enable VLAN tagging.

b) Check the **Enable Data Encryption** check box to enable Datagram Transport Layer Security (DTLS) data encryption.

c) Check the **Enable Jumbo MTU** to enable big maximum transmission unit (MTU). MTU is the largest physical packet size, measured in bytes, that a network can transmit. Any messages larger than the MTU are divided into smaller packets before transmission. Jumbo frames are frames that are bigger than the standard Ethernet frame size, which is 1518 bytes (including Layer 2 (L2) header and FCS). The definition of frame size is vendor-dependent, as these are not part of the IEEE standard.

d) Use the **Link Latency** drop-down list to select the link latency. Link latency monitors the round-trip time of the CAPWAP heartbeat packets (echo request and response) from the AP to the controller and back.

e) From the **Preferred Mode** drop-down list, choose the mode.

f) Click **Save & Apply to Device**.

**Step 8** In the **AP** tab, you can configure the following:

- General

a) In the **General** tab, check the **Switch Flag** check box to enable switches.

b) Check the **Power Injector State** check box if power injector is being used. Power Injector increases wireless LAN deployment flexibility of APs by providing an alternative powering option to local power, inline power-capable multiport switches, and multiport power patch panels.

Power Injector Selection parameter enables you to protect your switch port from an accidental overload if the power injector is inadvertently bypassed.

c) From the **Power Injector Type** drop-down list, choose power injector type from the following options:

- Installed—This option examines and remembers the MAC address of the currently connected switch port and assumes that a power injector is connected. Choose this option if your network contains older Cisco 6-Watt switches and you want to avoid possible overloads by forcing a double-check of any relocated access points.

  If you want to configure the switch MAC address, enter the MAC address in the Injector Switch MAC Address text box. If you want the access point to find the switch MAC address, leave the Injector Switch MAC Address text box blank.

  **Note** Each time an access point is relocated, the MAC address of the new switch port fails to match the remembered MAC address, and the access point remains in low-power mode. You must then physically verify the existence of a power injector and reselect this option to cause the new MAC address to be remembered.

- Override—This option allows the access point to operate in high-power mode without first verifying a matching MAC address. You can use this option if your network does not contain any older Cisco 6-W switches that could be overloaded if connected directly to a 12-W access point. The advantage of this option is that if you relocate the access point, it continues to operate in high-power mode without any further configuration. The disadvantage of this option is that if the access point is connected directly to a 6-W switch, an overload occurs.

d) In the **Injector Switch MAC** field, enter the MAC address of the switch .

e) From the **EAP Type** drop-down list, choose the EAP type as *EAP-FAST*, *EAP-TLS*, or *EAP-PEAP*.

f) From the **AP Authorization Type** drop-down list, choose the type as either *CAPWAP DTLS +* or *CAPWAP DTLS*.

g) In the **Client Statistics Reporting Interval** section, enter the interval for 5 GHz and 2.4 GHz radios in seconds.

h) Check the **Enable** check box to enable extended module.

i) From the **Profile Name** drop-down list, choose a profile name for mesh.

j) Click **Save & Apply to Device**.

- Hyperlocation: Cisco Hyperlocation is a location solution that allows to track the location of wireless clients with the accuracy of one meter. Selecting this option disables all other fields in the screen, except NTP Server.

a) In the **Hyperlocation** tab, check the **Enable Hyperlocation** check box.
b) Enter the **Detection Threshold** value to filter out packets with low RSSI. The valid range is –100 dBm to –50 dBm.
c) Enter the **Trigger Threshold** value to set the number of scan cycles before sending a BAR to clients. The valid range is 0 to 99.
d) Enter the **Reset Threshold** value to reset value in scan cycles after trigger. The valid range is 0 to 99.
e) Enter the **NTP Server** IP address.
f) Click **Save & Apply to Device**.

- BLE: If your APs are Bluetooth Low Energy (BLE) enabled, they can transmit beacon messages that are packets of data or attributes transmitted over a low energy link. These BLE beacons are frequently used for health monitoring, proximity detection, asset tracking, and in-store navigation. For each AP, you can customize BLE Beacon settings configured globally for all APs.

a) In the **BLE** tab, enter a value in the **Beacon Interval** field to indicate how often you want your APs to send out beacon advertisements to nearby devices. The range is from 1 to 10, with a default of 1.
b) In the **Advertised Attenuation Level** field, enter the attenuation level. The range is from 40 to 100, with a default of 59.
c) Click **Save & Apply to Device**.

- Packet Capture: Packet Capture feature allows to capture the packets on the AP for the wireless client troubleshooting. The packet capture operation is performed on the AP by the radio drivers on the current channel on which it is operational, based on the specified packet capture filter.

a) In the **Packet Capture** tab, choose an **AP Packet Capture Profile** from the drop-down list.
b) You can also create a new profile by clicking the **+** sign.
c) Enter a name and description for the AP packet capture profile.
d) Enter the **Buffer Size**.
e) Enter the **Duration**.
f) Enter the **Truncate Length** information.
g) In the **Server IP** field, enter the IP address of the TFTP server.
h) In the **File Path** field, enter the directory path.
i) Enter the username and password details.
j) From the **Password Type** drop-down list, choose the type.
k) In the **Packet Classifiers** section, use the option to select or enter the packets to be captured.
l) Click **Save**.
m) Click **Save & Apply to Device**.

**Step 9** In the **Management** tab, you can configure the following:

- Device

a) In the **Device** tab, enter the **IPv4/IPv6 Address** of the TFTP server, **TFTP Downgrade** section.
b) In the **Image File Name** field, enter the name of the software image file.
c) From the **Facility Value** drop-down list, choose the appropriate facility.
d) Enter the IPv4 or IPv6 address of the host.
e) Choose the appropriate **Log Trap Value**.
f) Enable Telnet and/or SSH configuration, if required.
g) Enable core dump, if required.
h) Click **Save & Apply to Device**.

- User

a) In the **User** tab, enter username and password details.
b) Choose the appropriate password type.
c) In the **Secret** field, enter a custom secret code.
d) Choose the appropriate secret type.
e) Choose the appropriate encryption type.
f) Click **Save & Apply to Device**.

- Credentials

a) In the **Credentials** tab, enter local username and password details.
b) Choose the appropriate local password type.
c) Enter 802.1x username and password details.
d) Choose the appropriate 802.1x password type.
e) Enter the time in seconds after which the session should expire.
f) Enable local credentials and/or 802.1x credentials as required.
g) Click **Save & Apply to Device**.

- CDP Interface

a) In the **CDP Interface** tab, enable the CDP state, if required.
b) Click **Save & Apply to Device**.

**Step 10** In the **Rogue AP** tab, check the **Rogue Detection** check box to enable rogue detection.

**Step 11** In the **Rogue Detection Minimum RSSI** field, enter the RSSI value.

This field specifies the minimum RSSI value for which a Rogue AP should be reported. All Rogue APs with RSSI lower than what is configured will not be reported to controller.

**Step 12** In the **Rogue Detection Transient Interval** field, enter the transient interval value.

This field indicates how long the Rogue AP should be seen before reporting the controller.

**Step 13** In the **Rogue Detection Report Interval** field, enter the report interval value.

This field indicates the frequency (in seconds) of Rogue reports sent from AP to controller.

**Step 14** Check the **Rogue Containment Automatic Rate Selection** check box to enable rogue containment automatic rate selection.

Here, the AP selects the best rate for the target Rogue, based on its RSSI.

**Step 15** Check the **Auto Containment on FlexConnect Standalone** check box to enable the feature.

Here, the AP will continue containment in case it moves to FlexConnect standalone mode.

**Step 16** Click **Save & Apply to Device**.

# Configuring an RF Profile (GUI)

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

**Step 2** On the **RF Profile** page, click **Add**.

**Step 3** In the **General** tab, enter a name for the RF profile. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

**Step 4** Choose the appropriate **Radio Band**.

**Step 5** To enable the profile, set the status as **Enable**.

**Step 6** Enter a **Description** for the RF profile.

**Step 7** Click **Save & Apply to Device**.

CHAPTER 12

# Configuring Tags

# Configuring Tags Through the CLI

## Configuring a Site Tag (CLI)

Follow the procedure given below to configure a site tag:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **wireless tag site** *site-name*
4. **flex-profile** *flex-profile-name*
5. **description** *site-tag-name*
6. **end**
7. **show wireless tag site summary**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **wireless tag site** *site-name*<br>**Example:** | Configures a site tag and enters site tag configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config)# wireless tag site rr-xyz-site` | |
| **Step 4** | **flex-profile** *flex-profile-name*<br>**Example:**<br>`Device(config-site-tag)# flex-profile rr-xyz-flex-profile` | Configures a flex profile.<br>**Note** You cannot remove the flex profile configuration from a site tag if local site is configured on the site tag.<br>**Note** The **no local-site** command needs to be used to configure the Site Tag as Flexconnect, otherwise the Flex profile configuration does not take effect. |
| **Step 5** | **description** *site-tag-name*<br>**Example:**<br>`Device(config-site-tag)# description "default site tag"` | Adds a description for the site tag. |
| **Step 6** | **end**<br>**Example:**<br>`Device(config-site-tag)# end` | Exits site tag configuration mode and returns to privileged EXEC mode. |
| **Step 7** | **show wireless tag site summary**<br>**Example:**<br>`Device# show wireless tag site summary` | (Optional) Displays the number of site tags.<br>**Note** To view detailed information about a site, use the **show wireless tag site detailed** *site-tag-name* command.<br>**Note** The output of the **show wireless loadbalance tag affinity wncd** *wncd-instance-number* command displays default tag (site-tag) type, if both site tag and policy tag are not configured. |

# Configuring a Policy Tag (CLI)

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **wireless tag policy** *policy-tag-name*
4. **description** *description*
5. **remote-lan** *name* **policy** *profile-policy-name* {**ext-module** | **port-id** *name*}
6. **wlan** *wlan-name* **policy** *profile-policy-name*
7. **end**
8. **show wireless tag policy summary**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>- Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **wireless tag policy** *policy-tag-name*<br>**Example:**<br>`Device(config-policy-tag)# wireless tag policy default-policy-tag` | Configures a policy tag, and enters policy tag configuration mode.<br>**Note** When performing LWA, the clients connected to a controller gets disconnected intermittently before session timeout.<br>As a workaround it is recommended to include all policy profiles with central association or no central association under a given policy tag. |
| **Step 4** | **description** *description*<br>**Example:**<br>`Device(config-policy-tag)# description default-policy-tag` | Adds a description to the policy tag. |
| **Step 5** | **remote-lan** *name* **policy** *profile-policy-name* {**ext-module** \| **port-id** *name*}<br>**Example:**<br>`Device(config-policy-tag)# remote-lan rr-xyz-rlan-aa policy rr-zyz-rlan1 port-id 2` | Maps a remote-LAN profile to a policy profile. |
| **Step 6** | **wlan** *wlan-name* **policy** *profile-policy-name*<br>**Example:**<br>`Device(config-policy-tag)# wlan rr-xyz-wlan-aa policy rr-xyz-policy-1` | Maps a policy profile to a WLAN profile. |
| **Step 7** | **end**<br>**Example:**<br>`Device(config-policy-tag)# end` | Saves the configuration, exits configuration mode, and returns to privileged EXEC mode. |
| **Step 8** | **show wireless tag policy summary**<br>**Example:**<br>`Device# show wireless tag policy summary` | (Optional) Displays the configured policy tags.<br>**Note** To view detailed information about a policy tag, use the **show wireless tag policy detailed** *policy-tag-name* command. |

# Configuring Wireless RF Tag (CLI)

Follow the procedure given below to configure a wireless RF tag:

### Before you begin

- You can use only two profiles (IEEE 802.11a and IEEE 802.11b) in an RF tag .
- Ensure that you use the same AP tag name that you created when configuring the AP tag task too.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **wireless tag rf** *rf-tag*
4. **24ghz-rf-policy** *rf-policy*
5. **5ghz-rf-policy** *rf-policy*
6. **description** *policy-description*
7. **end**
8. **show wireless tag rf summary**
9. **show wireless tag rf detailed** *rf-tag*

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **wireless tag rf** *rf-tag*<br>**Example:**<br>`Device(config)# wireless tag rf rftag1` | Creates an RF tag and enters wireless RF tag configuration mode. |
| **Step 4** | **24ghz-rf-policy** *rf-policy*<br>**Example:**<br>`Device(config-wireless-rf-tag)# 24ghz-rf-policy rfprof24_1` | Attaches an IEEE 802.11b RF policy to the RF tag. |
| **Step 5** | **5ghz-rf-policy** *rf-policy*<br>**Example:**<br>`Device(config-wireless-rf-tag)# 5ghz-rf-policy rfprof5_1` | Attaches an IEEE 802.11a RF policy to the RF tag. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **description** *policy-description*<br>**Example:**<br>`Device(config-wireless-rf-tag)# description Test` | Adds a description for the RF tag. |
| **Step 7** | **end**<br>**Example:**<br>`Device(config-wireless-rf-tag)# end` | Exits configuration mode and returns to privileged EXEC mode. |
| **Step 8** | **show wireless tag rf summary**<br>**Example:**<br>`Device# show wireless tag rf summary` | Displays the available RF tags. |
| **Step 9** | **show wireless tag rf detailed** *rf-tag*<br>**Example:**<br>`Device# show wireless tag rf detailed rftag1` | Displays detailed information of a particular RF tag. |

# Configuring an AP Tag (CLI)

### Before you begin

Ensure that you use the same AP tag that is configured here in the Wireless RF tag.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap** *mac-address*
4. **policy-tag** *policy-tag*
5. **rf-tag** *rf-tag*
6. **site-tag** *site-tag*
7. **end**
8. **show ap tag summary**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters the global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **ap** *mac-address*<br>**Example:**<br>`Device(config)# ap 188b.9dbe.6eac` | Enters the AP tag configuration mode.<br>**Important** Use the AP MAC address. Do not use the Ethernet MAC address. |
| **Step 4** | **policy-tag** *policy-tag*<br>**Example:**<br>`Device(config-ap-tag)# policy-tag policytag1` | Maps a policy tag to the AP. |
| **Step 5** | **rf-tag** *rf-tag*<br>**Example:**<br>`Device(config-ap-tag)# rf-tag rftag1` | Configures a named RF tag and adds the AP mac-address to the tag. |
| **Step 6** | **site-tag** *site-tag*<br>**Example:**<br>`Device(config-ap-tag)# site-tag sitetag1` | Maps a site tag to the AP. |
| **Step 7** | **end**<br>**Example:**<br>`Device(config-ap-tag)# end` | Exits AP tag configuration mode and returns to privileged EXEC mode. |
| **Step 8** | **show ap tag summary**<br>**Example:**<br>`Device# show ap tag summary` | Displays the tag summary of available APs. |

### What to do next

Configure Wireless RF tag.

## Configuring Wireless RF Tag (CLI)

Follow the procedure given below to configure a wireless RF tag:

### Before you begin

- You can use only two profiles (IEEE 802.11a and IEEE 802.11b) in an RF tag .
- Ensure that you use the same AP tag name that you created when configuring the AP tag task too.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **wireless tag rf** *rf-tag*
4. **24ghz-rf-policy** *rf-policy*
5. **5ghz-rf-policy** *rf-policy*

6. **description** *policy-description*
7. **end**
8. **show wireless tag rf summary**
9. **show wireless tag rf detailed** *rf-tag*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **wireless tag rf** *rf-tag*<br>**Example:**<br>`Device(config)# wireless tag rf rftag1` | Creates an RF tag and enters wireless RF tag configuration mode. |
| **Step 4** | **24ghz-rf-policy** *rf-policy*<br>**Example:**<br>`Device(config-wireless-rf-tag)# 24ghz-rf-policy rfprof24_1` | Attaches an IEEE 802.11b RF policy to the RF tag. |
| **Step 5** | **5ghz-rf-policy** *rf-policy*<br>**Example:**<br>`Device(config-wireless-rf-tag)# 5ghz-rf-policy rfprof5_1` | Attaches an IEEE 802.11a RF policy to the RF tag. |
| **Step 6** | **description** *policy-description*<br>**Example:**<br>`Device(config-wireless-rf-tag)# description Test` | Adds a description for the RF tag. |
| **Step 7** | **end**<br>**Example:**<br>`Device(config-wireless-rf-tag)# end` | Exits configuration mode and returns to privileged EXEC mode. |
| **Step 8** | **show wireless tag rf summary**<br>**Example:**<br>`Device# show wireless tag rf summary` | Displays the available RF tags. |
| **Step 9** | **show wireless tag rf detailed** *rf-tag*<br>**Example:**<br>`Device# show wireless tag rf detailed rftag1` | Displays detailed information of a particular RF tag. |

# Attaching Policy Tag and Site Tag to an AP (CLI)

Follow the procedure given below to attach a policy tag and a site tag to an AP:

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap** *mac-address*
4. **policy-tag** *policy-tag-name*
5. **site-tag** *site-tag-name*
6. **rf-tag** *rf-tag-name*
7. **end**
8. **show ap tag summary**
9. **show ap name** *ap-name* **tag info**
10. **show ap name** *ap-name* **tag detail**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ap** *mac-address*<br>**Example:**<br>`Device(config)# ap F866.F267.7DFB` | Configures a Cisco AP and enters AP profile configuration mode.<br>**Note** The *mac-address* should be a wired MAC address. |
| **Step 4** | **policy-tag** *policy-tag-name*<br>**Example:**<br>`Device(config-ap-tag)# policy-tag rr-xyz-policy-tag` | Maps a policy tag to the AP. |
| **Step 5** | **site-tag** *site-tag-name*<br>**Example:**<br>`Device(config-ap-tag)# site-tag rr-xyz-site` | Maps a site tag to the AP. |
| **Step 6** | **rf-tag** *rf-tag-name*<br>**Example:**<br>`Device(config-ap-tag)# rf-tag rf-tag1` | Associates the RF tag. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | **end**<br>**Example:**<br>`Device(config-ap-tag)# end` | Exits AP profile configuration mode and returns to privileged EXEC mode. |
| **Step 8** | **show ap tag summary**<br>**Example:**<br>`Device# show ap tag summary` | (Optional) Displays AP details and the tags associated to it. |
| **Step 9** | **show ap name** *ap-name* **tag info**<br>**Example:**<br>`Device# show ap name ap-name tag info` | (Optional) Displays the AP name with tag information. |
| **Step 10** | **show ap name** *ap-name* **tag detail**<br>**Example:**<br>`Device# show ap name ap-name tag detail` | (Optional) Displays the AP name with tag details. |

# Setting the Tag Priority (CLI)

Multiple tag sources might result in ambiguity for network administrators. To address this, you can define priority for tags. When an AP joins the controller, the tags are selected based on the priority. If precedence is not set, the default is used.

Use the following procedure to set the tag priority:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap tag-source-priority** *source-priority* **source** {**ap** | **filter**}
4. **ap tag-source-priority** *source-priority* **source** {**ap** | **filter**}
5. **end**
6. **ap tag-sources revalidate**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **ap tag-source-priority** *source-priority* **source** {**ap** \| **filter**}<br>**Example:**<br>`Device(config)# ap tag-source-priority 2 source ap` | Configures AP tag source priority. |
| **Step 4** | **ap tag-source-priority** *source-priority* **source** {**ap** \| **filter**}<br>**Example:**<br>`Device(config)# ap tag-source-priority 1 source filter` | Configures source priority for the filter.<br>• Use the filter that was configured by using the **ap filter name** command.<br>**Note** It is not mandatory to configure an AP filter, it comes with default priorities. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config)# end` | Exits global configuration mode and returns to privileged EXEC mode. |
| **Step 6** | **ap tag-sources revalidate**<br>**Example:**<br>`Device# ap tag-sources revalidate` | Revalidates the AP tag sources. The AP tag priority become active only after this command is configured.<br>**Note** When you change the priority for the AP and filter, run the **ap tag-sources revalidate** command to evaluate the priority. |

# Configuring Tags Through the GUI

## Configuring a Site Tag (GUI)

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

**Step 2** On the **Manage Tags** page, click the **Site** tab.

**Step 3** Click **Add** to view the **Add Site Tag** window.

**Step 4** Enter a name and description for the site tag. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

**Step 5** Choose the required **AP Join Profile** to be attached to the site tag.

**Step 6** Choose the required **Control Plane Name**.

**Step 7** If required, enable the **Local Site**.

Disabling Local Site means that the site is remote and the deployment is FlexConnect mode.

**Step 8** Click **Save & Apply to Device**.

# Configuring Policy Tag (GUI)

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

**Step 2** Click **Add** to view the **Add Policy Tag** window.

**Step 3** Enter a name and description for the policy tag. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

**Step 4** Click **Add** to map WLAN and policy.

**Step 5** Choose the WLAN profile to map with the appropriate policy profile, and click the tick icon.

**Step 6** Click **Save & Apply to Device**.

# Configuring Wireless RF Tag (GUI)

**Step 1** a) Choose **Configuration** > **Tags & Profiles** > **Tags** > **RF**.

**Step 2** Click **Add** to view the **Add RF Tag** window.

**Step 3** Enter a name and description for the RF tag. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

**Step 4** Choose the required **5 GHz Band RF Profile** and **2.4 GHz Band RF Profile** to be associated with the RF tag.

**Step 5** Click **Update & Apply to Device**.

# Configuring an AP Tag (GUI)

### Before you begin

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

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

**Step 2** On the **Manage Tags** page, click the AP tab.

**Step 3** In the **Tag Source** tab, drag and drop the tag sources to change priorities.

**Step 4** Check the **Revalidate Tag Sources on APs** check box, if required.

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

**Step 6** In the **Static** tab, click **Add**.

**Step 7** In the **Associate Tags to AP** window, enter a MAC address.

**Step 8** Choose the appropriate **Policy Tag Name**, **Site Tag Name**, and **RF Tag Name**.

**Step 9** Click **Save & Apply to Device**.

**Step 10** In the **Filter** tab, click **Add**.

**Step 11** In the **Associate Tags to AP** window, enter a rule and AP name regex.

**Step 12** Use the slider to enable **Active**.

**Step 13** Enter the **Priority**. The valid range is from 0 to 127.

**Step 14** Choose the appropriate **Policy Tag Name**, **Site Tag Name**, and **RF Tag Name.**

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

# Configuring RF Profile (GUI)

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

**Step 2** On the**RF Profile** page, click **Add** to configure the following:

- General
- 802.11
- RRM
- Advanced

**Step 3** In the **General** tab, proceed as follows:

a) Enter a name and description for the RF profile.
b) Choose the appropriate radio band.
c) To enable the profile, set the status as *Enable*.
d) Click **Save & Apply to Device**.

**Step 4** In the **802.11** tab, proceed as follows:

a) Choose the required operational rates.
b) Select the required 802.11n MCS Rates by checking the corresponding check boxes.
c) Click **Save & Apply to Device**.

**Step 5** In the **RRM > General** tab, proceed as follows:

a) Enter the foreign interference threshold between 0 and 100 percent in the Interference field. The default is 10.
b) In the **Clients** field, enter the client threshold between 1 and 75 clients. The default is 12.
c) In the **Noise** field, enter the foreign noise threshold between –127 and 0 dBm. The default is –70.
d) In the **Utilization** percentage field, enter the RF utilization threshold between 0 and 100 percent. The default is 80.

**Step 6** In the **RRM > Coverage** tab, proceed as follows:

a) Enter the client level in the Minimum Client Level field.
b) In the **Data RSSI Threshold** field, enter the actual value in dBm. Value ranges from -60 to -90 dBm and the default value is –80 dBm.
c) In the **Voice RSSI Threshold** field, enter the actual value in dBm. Value ranges from -60 to -90 dBm and the default value is –75.
d) In the **Exception Level** field, enter the maximum desired percentage of clients on an AP's radio operating below the desired coverage threshold. Value ranges from 0 to 100% and the default value is 25%.

**Step 7** In the **RRM > TPC** tab, proceed as follows:

a) Enter the power level assignment on this radio in the **Maximum Power Level** field. If you configure maximum transmit power, RRM does not allow any access point attached to the device to exceed this transmit power level (whether the power is set by RRM TPC or by coverage hole detection).
b) In the **Minimum Power Level** field, enter the minimum power level assignment on this radio.

c) In the **Power Threshold V1** field, enter the cutoff signal level used by RRM when determining whether to reduce an access point's power.

**Step 8** In the **RRM > DCA** tab, proceed as follows:

a) Check the **Avoid AP Foreign AP Interference** check box to cause the controller's RRM algorithms to consider 802.11 traffic from foreign access points (those not included in your wireless network) when assigning channels to lightweight access points, or unselect it to disable this feature. For example, RRM may adjust the channel assignment to have access points avoid channels close to foreign access points. The default value is selected.
b) Choose the appropriate channel width.
c) In the **DCA Channels** section, the DCA Channels field shows the channels that are currently selected. To choose a channel, select the appropriate check box. Extended UNII-2 channels in the 802.11a/n/ac band do not appear in the channel list: 100, 104, 108, 112, 116, 132, 136, and 140. To include these channels in the channel list, select the Extended UNII-2 Channels check box.
d) Click **Save & Apply to Device**.

**Step 9** In the **Advanced** tab, enter the following information in the **High Density Parameters** section:

a) In the **Max Clients** field, set the maximum number of clients allowed globally.
b) Use the **Multicast Data Rate** drop-down to choose the data rate for multicast traffic.

Choose auto to configure the device to use the radio's default data rate.

c) Use the **Rx SOP Threshold** drop-down to set the Receiver Start of Packet Detection Threshold (Rx SOP) to determine the Wi-Fi signal level in dBm at which AP radios will demodulate and decode a packet. The higher the RXSOP level, the less sensitive the radio is and the smaller the receiver cell size will be. Reducing the cell size ensures that clients connect to the nearest access point using highest possible data rates. Choose auto to configure the device to use the radio's default threshold.

**Step 10** In the **Client Distribution** section, enter the following:

- **Load Balancing Window**—Enter a value between 1 and 20 to specify the load-balancing window and the number of client associations on the AP with the lightest load.

- **Load Balancing Denial Count**—Enter a value between 0 and 10 to specify the number of times the client associations will be rejected for a particular AP.

**Step 11** In the **High Speed Roam** section, check the **Mode Enable** check box to enable the mode.

**Step 12** In the **Neighbor Timeout** field, enter the neighbor timeout value.

**Step 13** From the **Client Network Preference** drop-down list, choose the client network preference.

**Step 14** In the **ATF Configuration** section, use the slider to enable or disable **Status** and **Bridge Client Access**.

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

# Configuring Wireless RF Tag (GUI)

**Step 1** a) Choose **Configuration** > **Tags & Profiles** > **Tags** > **RF**.

**Step 2** Click **Add** to view the **Add RF Tag** window.

**Step 3** Enter a name and description for the RF tag. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

**Step 4** Choose the required **5 GHz Band RF Profile** and **2.4 GHz Band RF Profile** to be associated with the RF tag.

**Step 5** Click **Update & Apply to Device**.

## Set Tag Priority (GUI)

**Step 1** Choose **Configuration** > **Tags & Profiles** > **Tags** > **AP** > **Tag Source**.

**Step 2** Drag and Drop the Tag Sources to change priorities.

CHAPTER 13

# Attaching Tags to an AP

## Attaching Policy Tag and Site Tag to an AP (CLI)

Follow the procedure given below to attach a policy tag and a site tag to an AP:

### SUMMARY STEPS

1. **configure terminal**
2. **ap** *mac-address*
3. **policy-tag** *policy-tag-name*
4. **site-tag** *site-tag-name*
5. **rf-tag** *rf-tag-name*
6. **end**
7. **show ap tag summary**
8. **show ap name** <*ap-name*> **tag info**
9. **show ap name** <*ap-name*> **tag detail**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 2** | **ap** *mac-address*<br>**Example:**<br>`Device(config)# ap F866.F267.7DFB` | Configures a Cisco AP and enters AP profile configuration mode.<br>**Note** The *mac-address* should be a wired mac address. |
| **Step 3** | **policy-tag** *policy-tag-name*<br>**Example:**<br>`Device(config-ap-tag)# policy-tag rr-xyz-policy-tag` | Maps a policy tag to the AP. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **site-tag** *site-tag-name*<br>**Example:**<br>`Device(config-ap-tag)# site-tag rr-xyz-site` | Maps a site tag to the AP. |
| **Step 5** | **rf-tag** *rf-tag-name*<br>**Example:**<br>`Device(config-ap-tag)# rf tag rf-tag1` | Associates the RF tag. |
| **Step 6** | **end**<br>**Example:**<br>`Device(config-ap-tag)# end` | Saves the configuration, exits configuration mode, and returns to privileged EXEC mode. |
| **Step 7** | **show ap tag summary**<br>**Example:**<br>`Device# show ap tag summary` | (Optional) Displays AP details and the tags associated to it. |
| **Step 8** | **show ap name** <*ap-name*> **tag info**<br>**Example:**<br>`Device# show ap name ap-name tag info` | (Optional) Displays the AP name with tag information. |
| **Step 9** | **show ap name** <*ap-name*> **tag detail**<br>**Example:**<br>`Device# show ap name ap-name tag detail` | (Optional) Displays the AP name with tag detals. |

# Attaching a Policy Tag and Site Tag to an AP (GUI)

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

The **All Access Points** section displays details of all the APs on your network.

**Step 2** To edit the configuration details of an AP, select the row for that AP.

The **Edit AP** window is displayed.

**Step 3** In the **General** tab and **Tags** section, specify the appropriate policy, site, and RF tags, that you created on the **Configuration** > **Tags & Profiles** > **Tags** page.

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

CHAPTER 14

# Creating an AP Filter

# Creating and Setting Up an AP Filter (CLI)

## Creating an AP Filter (CLI)

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap filter name** *filter-name*
4. **ap name-regex** *regular-expression*
5. **tag policy** *policy-tag*
6. **tag rf** *rf-tag*
7. **tag site** *site-tag*
8. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters the global configuration mode. |
| **Step 3** | **ap filter name** *filter-name*<br>**Example:**<br>`Device(config)# ap filter filter-1` | Configures an AP filter and enters AP filter configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **ap name-regex** *regular-expression*<br>**Example:**<br>`Device(config-ap-filter)# ap name-regex testany` | Configures the AP filter based on regular expression. |
| **Step 5** | **tag policy** *policy-tag*<br>**Example:**<br>`Device(config-ap-filter)# tag policy pol-tag1` | Configures a policy tag for this filter. |
| **Step 6** | **tag rf** *rf-tag*<br>**Example:**<br>`Device(config-ap-filter)# tag rf rf-tag1` | Configures an RF tag for this filter. |
| **Step 7** | **tag site** *site-tag*<br>**Example:**<br>`Device(config-ap-filter)# tag site site1` | Configures a site tag for this filter. |
| **Step 8** | **end**<br>**Example:**<br>`Device(config-ap-filter)# end` | Exits AP filter configuration mode and returns to privileged EXEC mode. |

# Set Up and Update Filter Priority

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap filter priority** *priority* **filter-name** *filter-name*
4. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ap filter priority** *priority* **filter-name** *filter-name*<br>**Example:** | Configures priority for an AP filter.<br>**Note** A filter without a priority is not active. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config)# ap filter priority 10 filter-name filter-1` | • Configure the priority for an filter that is configured using the **ap filter name** command.<br>• Priority cannot be assigned to a filter without any regular expression. |
| **Step 4** | **end**<br>**Example:**<br>`Device(config)# end` | Exits global configuration mode and returns to privileged EXEC mode. |

# Creating and Setting Up an AP Filter (GUI)

## Create an AP Filter (GUI)

**Step 1** Choose **Configuration** > **Tags & Profiles** > **Tags** > **AP** > **Filter**.

**Step 2** Click **Add**.

**Step 3** In the **Associate Tags to AP** dialog box which is displayed, enter the **Rule Name**, the **AP name regex** and the **Priority**. Optionally, you can also choose the policy tag from the **Policy Tag Name** drop-down list, the site tag from the **Site Tag Name** drop-down list and the RF tag from the **RF Tag Name** drop-down list.

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

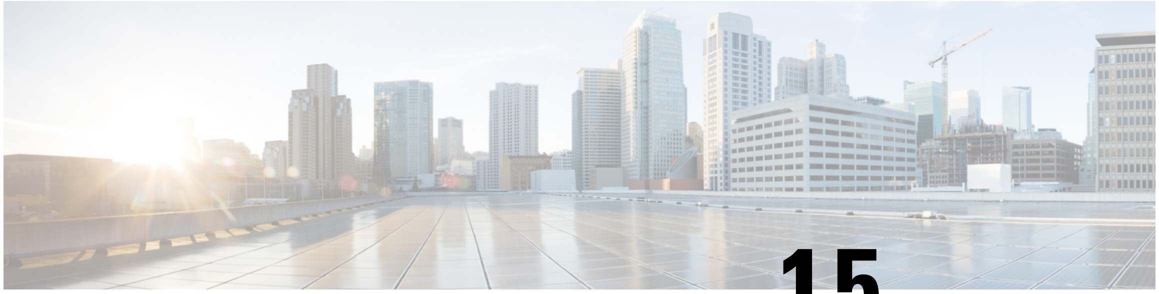
## Set Up and Update Filter Priority (GUI)

**Step 1** Choose **Configuration** > **Tags & Profiles** > **Tags** > **AP** > **Filter**.

**Step 2**

a) If you want to setup a new AP filter, then click **Add**. In the **Associate Tags to AP** dialog box which is displayed, enter the **Rule Name**, the **AP name regex** and the **Priority**. Optionally, you can also select the **Policy Tag Name**, the **Site Tag Name** and the **RF Tag Name**. Click **Apply to Device**.

b) If you want to update the priority of an existing AP filter, click on the Filter and in the **Edit Tags** dialog box and change the **Priority**. In case the Filter is Inactive, no priority can be set to it. Click **Update and Apply to Device**.



CHAPTER 15

# Configuring WLANs

## Configuring WLANs Through the CLI

### Creating and Enabling WLANs (CLI)

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **wlan** *profile-name wlan-id* [*ssid*]
4. **no shutdown**
5. **end**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters the global configuration mode. |
| **Step 3** | **wlan** *profile-name wlan-id* [*ssid*]<br>**Example:**<br>`Device(config)# wlan mywlan 34 mywlan-ssid` | Specifies the WLAN name and ID:<br>• For the *profile-name* argument, enter the profile name. The range is from 1 to 32 alphanumeric characters.<br>• For the *wlan-id*argument, enter the WLAN ID. The range is from 1 to 512. |

| | Command or Action | Purpose |
|---|---|---|
| | | • For the *ssid*argument, enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID.<br>**Note** • You can create an SSID using the GUI or CLI. However, we recommend that you use CLI to create SSID.<br>• The configured WLAN is disabled by default. |
| **Step 4** | **no shutdown**<br>**Example:**<br>`Device(config-wlan)# no shutdown` | Enables the WLAN. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config)# end` | Exits global configuration mode and returns to privileged EXEC mode. |

# Disabling and Deleting WLANs (CLI)

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **wlan** *profile-name*
4. **shutdown**
5. **exit**
6. **no wlan** *wlan-name wlan-id ssid*
7. **show wlan summary**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **wlan** *profile-name*<br>**Example:**<br>`Device(config)# wlan mywlan-ssid` | Enters WLAN configuration mode.<br>• The *profile-name* argument is the profile name of the configured WLAN. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **shutdown**<br>**Example:**<br>`Device(config-wlan)# shutdown` | Disables the WLAN. |
| **Step 5** | **exit**<br>**Example:**<br>`Device(config-wlan)# exit` | Exits WLAN configuration mode and returns to global configuration mode. |
| **Step 6** | **no wlan** *wlan-name wlan-id ssid*<br>**Example:**<br>`Device(config)# no wlan mywlan-ssid` | Deletes the WLAN. |
| **Step 7** | **show wlan summary**<br>**Example:**<br>`Device# show wlan summary` | Displays the list of all WLANs configured on the device. |

# Configuring General WLAN Properties (CLI)

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **wlan** *profile-name*
4. **shutdown**
5. **broadcast-ssid**
6. **radio** {**dot11a** | **dot11ag** | **dot11bg** | **dot11ag**}
7. **media-stream multicast-direct**
8. **assisted-roaming** {**dual-list** | **neighbor-list** | **prediction**}
9. **band-select**
10. **bss-transition**
11. **bssmaxidle** [**protected-mode**]
12. **device-analytics** [**export**]
13. **dms**
14. **dot11ax**
15. **dtim dot11** {**24ghs** | **5ghz** } *DTIM-period*
16. **ignore-rsn-ie-len**
17. **ipv6 traffic-filter web** *ipv6-acl-name*
18. **load-balance**
19. **local-auth** *EAP-profile*
20. **no shutdown**
21. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **wlan** *profile-name*<br>**Example:**<br>`Device(config)# wlan test4` | Enters WLAN configuration mode. The *profile-name* is the profile name of the configured WLAN. |
| **Step 4** | **shutdown**<br>**Example:**<br>`Device(config-wlan)# shutdown` | Disables the WLAN. |
| **Step 5** | **broadcast-ssid**<br>**Example:**<br>`Device(config-wlan)# broadcast-ssid` | Broadcasts the SSID for this WLAN. |
| **Step 6** | **radio** {**dot11a** \| **dot11ag** \| **dot11bg** \| **dot11ag**}<br>**Example:**<br>`Device(config-wlan)# radio dot11g` | Configures the WLAN on all radio bands.<br>• **dot11a**: Configures the WLAN on only 802.11a radio bands.<br>• **dot11g**: Configures the WLAN on 802.11ag radio bands.<br>• **dot11bg**: Configures the WLAN on only 802.11b/g radio bands (only 802.11b if 802.11g is disabled).<br>• **dot11ag**: Configures the wireless LAN on 802.11g radio bands only. |
| **Step 7** | **media-stream multicast-direct**<br>**Example:**<br>`Device(config-wlan)# media-stream multicast-direct` | Enables multicast VLANs on the WLAN. |
| **Step 8** | **assisted-roaming** {**dual-list** \| **neighbor-list** \| **prediction**}<br>**Example:**<br>`Device(config-wlan)# assisted-roaming neighbor-list` | Configures the 802.11k neighbor-list support on the WLAN. |
| **Step 9** | **band-select**<br>**Example:**<br>`Device(config-wlan)# band-select` | Allows band selection on the WLAN. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 10** | **bss-transition**<br>**Example:**<br>`Device(config-wlan)# bss-transition` | Configures 802.11v Basic Service Set (BSS) transition per WLAN. |
| **Step 11** | **bssmaxidle** [**protected-mode**]<br>**Example:**<br>`Device(config-wlan)# bssmaxidle protected-mode` | Configures protected mode for BSS maximum idle processing per WLAN. |
| **Step 12** | **device-analytics** [**export**]<br>**Example:**<br>`Device(config-wlan)# device-analytics export` | Configures device-analytics export on the WLAN. |
| **Step 13** | **dms**<br>**Example:**<br>`Device(config-wlan)# dms` | Configures Directed Multicast Service (DMS) processing per WLAN. |
| **Step 14** | **dot11ax**<br>**Example:**<br>`Device(config-wlan)# dot11ax` | Configures 802.11ax on the WLAN. |
| **Step 15** | **dtim dot11** {**24ghs** \| **5ghz** } *DTIM-period*<br>**Example:**<br>`Device(config-wlan)# bssmaxidle protected-mode` | Sets the Delivery Traffic Indication Map (DTIM) period for the 802.11a radio for the WLAN. |
| **Step 16** | **ignore-rsn-ie-len**<br>**Example:**<br>`Device(config-wlan)# ignore-rsn-ie-len` | Skips the Robust Security Network (RSN) Information Element (IE) length validation during key exchange. |
| **Step 17** | **ipv6 traffic-filter web** *ipv6-acl-name*<br>**Example:**<br>`Device(config-wlan)# ipv6 traffic-filter web ipv6-acl-1` | Specifies the IPv6 WLAN web access list. |
| **Step 18** | **load-balance**<br>**Example:**<br>`Device(config-wlan)# load-balance` | Allows load balancing on the WLAN. |
| **Step 19** | **local-auth** *EAP-profile*<br>**Example:**<br>`Device(config-wlan)# local-auth eap-profile1` | Sets the Extensible Authentication Protocol (EAP) profile on the WLAN. |
| **Step 20** | **no shutdown**<br>**Example:**<br>`Device(config-wlan)# no shutdown` | Enables the WLAN. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 21** | **end**<br>**Example:**<br>`Device(config-wlan)# end` | Exits WLAN configuration mode and returns to privileged EXEC mode. |

# Configuring Advanced WLAN Properties (CLI)

## SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **chd**
4. **ccx aironet-iesupport**
5. **client association limit** {*clients-per-wlan* | **ap** *clients-per-ap-per-wlan* | **radio***clients-per-ap-radio--per-wlan*}
6. **ip access-group web** *acl-name*
7. **peer-blocking** [**allow-private-groupdrop** | **forward-upstream**]
8. **channel-scan** {**defer-priority 0-7** | **defer-time 0 - 6000**}
9. **mac-filtering** [*authorization-list* **authorization-override**]
10. **mbo**
11. **mdns-sd-interface** {**drop** | **gateway**}
12. **mu-mimo**
13. **multicast buffer** *multicast-buffers*
14. **roamed-voice-client re-anchor**
15. **scan-report** {**association** | **roam**}
16. **scheduler asr**
17. **static-ip tunneling**
18. **tfs**
19. **uapsd compliant-client**
20. **universal-ap-admin**
21. **wifi-direct policy** {**allow** | **not-allow** | **xconnect-not-allow**}
22. **wifi-to-cellular**
23. **wmm** {**allowed** | **require**}
24. **wnm-sleep-mode**
25. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **wlan** *profile-name*<br>**Example:**<br>`Device(config)# wlan test4` | Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN. |
| **Step 3** | **chd**<br>**Example:**<br>`Device(config-wlan)# chd` | Enables coverage hole detection for this WLAN. |
| **Step 4** | **ccx aironet-iesupport**<br>**Example:**<br>`Device(config-wlan)# ccx aironet-iesupport` | Enables support for Aironet IEs for this WLAN. |
| **Step 5** | **client association limit** {*clients-per-wlan* \|**ap** *clients-per-ap-per-wlan* \|**radio***clients-per-ap-radio--per-wlan*}<br>**Example:**<br>`Device(config-wlan)# client association limit ap 400` | Sets the maximum number of clients, clients per AP, or clients per AP radio that can be configured on a WLAN. |
| **Step 6** | **ip access-group web** *acl-name*<br>**Example:**<br>`Device(config-wlan)# ip access-group web test-acl-name` | Configures the IPv4 WLAN web ACL. The variable *acl-name* specifies the user-defined IPv4 ACL name. |
| **Step 7** | **peer-blocking** [**allow-private-groupdrop** \| **forward-upstream**]<br>**Example:**<br>`Device(config-wlan)# peer-blocking drop` | Configures peer to peer blocking parameters. The keywords are as follows:<br>• **allow-private-group**: Enables peer-to-peer blocking on the Allow Private Group action.<br>• **drop**: Enables peer-to-peer blocking on the drop action.<br>• **forward-upstream**: No action is taken and forwards packets to the upstream.<br>**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** | **channel-scan** {**defer-priority 0-7** \| **defer-time 0 - 6000**}<br>**Example:**<br>`Device(config-wlan)# channel-scan defer-priority 6` | Sets the channel scan defer priority and defer time.<br>• **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. |

| | Command or Action | Purpose |
|---|---|---|
| | | • **defer-time**: Deferral time in milliseconds. The range is from 0 to 6000. The default is 100. |
| **Step 9** | **mac-filtering** [*authorization-list* **authorization-override**]<br>**Example:**<br>`Device(config-wlan)# mac-flitering mac-list1 authorization-override` | Sets the override-authorization list for MAC filtering. |
| **Step 10** | **mbo**<br>**Example:**<br>`Device(config-wlan)# mbo` | Configures Wi-Fi Alliance Agile Multiband (MBO) support on the WLAN. |
| **Step 11** | **mdns-sd-interface** {**drop** \| **gateway**}<br>**Example:**<br>`Device(config-wlan)# mdns-sd-interface gateway` | Enables multicast Domain Name System (mDNS) gateway for the WLAN. |
| **Step 12** | **mu-mimo**<br>**Example:**<br>`Device(config-wlan)# mu-mimo` | Configures 802.11ac Multi-User Multiple Input Multiple Output (MU-MIMO) on the WLAN. |
| **Step 13** | **multicast buffer** *multicast-buffers*<br>**Example:**<br>`Device(config-wlan)# multicast buffer 56` | Configures multicast buffer tuning for 802.11a radio for the WLAN. |
| **Step 14** | **roamed-voice-client re-anchor**<br>**Example:**<br>`Device(config-wlan)# multicast buffer 56` | Configures the re-anchor policy for roaming voice clients. |
| **Step 15** | **scan-report** {**association** \| **roam**}<br>**Example:**<br>`Device(config-wlan)# scan-report association` | Enables scan report (beacon measurement) requests when clients get associated. |
| **Step 16** | **scheduler asr**<br>**Example:**<br>`Device(config-wlan)# scheduler asr` | Configures advanced scheduling-request handling on the WLAN. |
| **Step 17** | **static-ip tunneling**<br>**Example:**<br>`Device(config-wlan)# static-ip tunneling` | Configures static IP client-tunneling support on the WLAN. |
| **Step 18** | **tfs**<br>**Example:**<br>`Device(config-wlan)# tfs` | Configure TFS processing on the WLAN. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 19** | **uapsd compliant-client**<br>**Example:**<br>`Device(config-wlan)# uapsd compliant-client` | Configures Wi-Fi MultiMedia (WMM) Unscheduled automatic power save delivery (U-APSD) compliant-client support for the WLAN. |
| **Step 20** | **universal-ap-admin**<br>**Example:**<br>`Device(config-wlan)# universal-ap-admin` | Enables universal AP on the WLAN. |
| **Step 21** | **wifi-direct policy** {**allow** \| **not-allow** \| **xconnect-not-allow**}<br>**Example:**<br>`Device(config-wlan)# wifi-direct policy allow` | Allows Wi-Fi direct clients to associate unconditionally with the WLAN. |
| **Step 22** | **wifi-to-cellular**<br>**Example:**<br>`Device(config-wlan)# wifi-to-cellular` | Configures Wi-Fi-to-cellular steering on the WLAN. |
| **Step 23** | **wmm** {**allowed** \| **require**}<br>**Example:**<br>`Device(config-wlan)# wmm allowed` | Allows WMM on the WLAN. |
| **Step 24** | **wnm-sleep-mode**<br>**Example:**<br>`Device(config-wlan)# wnm-sleep-mode` | Configures Wireless Network Management (WNM) sleep mode on the WLAN. |
| **Step 25** | **end**<br>**Example:**<br>`Device(config-wlan)# end` | Exits WLAN configuration mode and 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
```

# Configuring WLANs Through the GUI

## Creating WLANs (GUI)

**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**.

## Deleting WLANs (GUI)

**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.

## Disabling WLANs (GUI)

**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**.

## 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.

**Step 1** Choose **Configuration** > **Wireless** > **WLANs** > **Wireless Networks**.

**Step 2** In the **Wireless Networks** window, 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 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** From the **WMM Policy** drop-down list, choose the policy as Allowed, Disabled, or Required. By default, the WMM policy is Allowed.

**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 **Save & Apply to Device**.

CHAPTER 16

# Configuring WLAN Security

# Configuring WLAN Security (CLI)

## Configuring Static WEP Layer 2 Security Parameters (CLI)

### Before you begin

You must have administrator privileges.

### SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **security static-wep-key** [**authentication** {**open** | **shared**} | **encryption** {**104** | **40**} {**ascii** | **hex**} [**0** | **8**]]
4. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 2** | **wlan** *profile-name*<br>**Example:**<br>`# wlan test4` | Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN. |
| **Step 3** | **security static-wep-key** [**authentication** {**open** \| **shared**} \| **encryption** {**104** \| **40**} {**ascii** \| **hex**} [**0** \| **8**]] | The keywords are as follows: |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`(config-wlan)# security static-wep-key authentication open` | • **static-wep-key**—Configures Static WEP Key authentication.<br>• **authentication**—Specifies the authentication type you can set. The values are open and shared.<br>• **encryption**—Specifies the encryption type that you can set. The valid values are 104 and 40. 40-bit keys must contain 5 ASCII text characters or 10 hexadecimal characters. 104-bit keys must contain 13 ASCII text characters or 26 hexadecimal characters.<br>• **ascii**—Specifies the key format as ASCII.<br>• **hex**—Specifies the key format as HEX. |
| **Step 4** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode. |

# Configuring WPA + WPA2 Layer 2 Security Parameters (CLI)

**Note** The default security policy is WPA2.

### Before you begin

You must have administrator privileges.

## SUMMARY STEPS

1. **configure terminal**
2. **wlan** *profile-name*
3. **security wpa**
4. **security wpa wpa1**
5. **security wpa wpa1 ciphers** [**aes** | **tkip**]
6. **security wpa wpa2**
7. **security wpa wpa2 ciphers** [**aes** | **tkip**]

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **wlan** *profile-name*<br>**Example:**<br>`# wlan test4` | Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN. |
| **Step 3** | **security wpa**<br>**Example:**<br>`(config-wlan)# security wpa` | Enables WPA. |
| **Step 4** | **security wpa wpa1**<br>**Example:**<br>`(config-wlan)# security wpa wpa1` | Enables WPA1. |
| **Step 5** | **security wpa wpa1 ciphers** [**aes** \| **tkip**]<br>**Example:**<br>`(config-wlan)# security wpa wpa1 ciphers aes` | Specifies the WPA1 cipher. Choose one of the following encryption types:<br>• **aes**—Specifies WPA/AES support.<br>• **tkip**—Specifies WPA/TKIP support. |
| **Step 6** | **security wpa wpa2**<br>**Example:**<br>`(config-wlan)# security wpa wpa2` | Enables WPA2. |
| **Step 7** | **security wpa wpa2 ciphers** [**aes** \| **tkip**]<br>**Example:**<br>`(config-wlan)# security wpa wpa2`<br>**Example:**<br>`(config-wlan)# security wpa wpa2 ciphers tkip` | Configure WPA2 cipher. Choose one of the following encryption types:<br>• **aes**—Specifies WPA/AES support.<br>• **tkip**—Specifies WPA/TKIP support. |

# Configuring WLAN Security (GUI)

## Configuring Static WEP Layer 2 Security Parameters (GUI)

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

**Step 2** On the **WLANs** page, click the name of the WLAN.

**Step 3** In the **Edit WLAN** window, click the **Security** tab.

**Step 4** From the **Layer 2 Security Mode** drop-down list, select the **Static WEP** option.

**Step 5** (Optional) Check the **Shared Key Authentication** check box to set the authentication type as shared. By leaving the check box unchecked, the authentication type is set to open.

**Step 6** Set the **Key Size** as either **40 bits** or **104 bits**.

- 40 bits: The keys with 40-bit encryption must contain 5 ASCII text characters or 10 hexadecimal characters.

- 104 bits: The keys with 104-bit encryption must contain 13 ASCII text characters or 26 hexadecimal characters.

**Step 7** Set the appropriate **Key Index**; you can choose between 1 to 4.

**Step 8** Set the **Key Format** as either **ASCII** or **Hex**.

**Step 9** Enter a valid **Encryption Key**.

- 40 bits: The keys with 40-bit encryption must contain 5 ASCII text characters or 10 hexadecimal characters.
- 104 bits: The keys with 104-bit encryption must contain 13 ASCII text characters or 26 hexadecimal characters.

**Step 10** Click **Update & Apply to Device**.

## Configuring WPA + WPA2 Layer 2 Security Parameters (GUI)

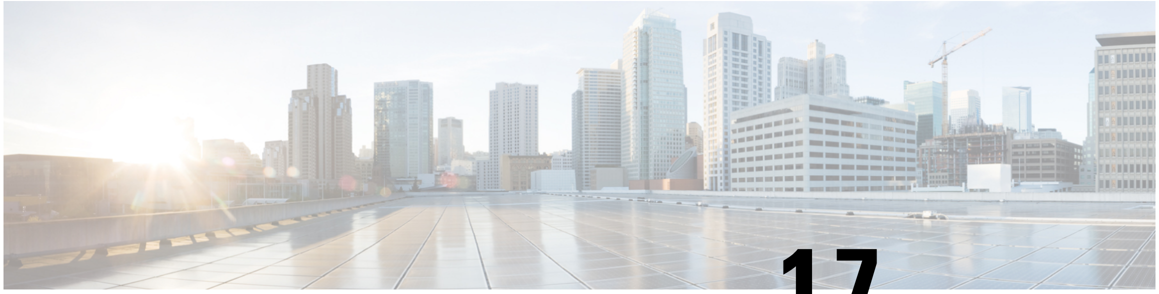
**Step 1** Click **Configuration** > **Tags and Profiles** > **WLANs**.

**Step 2** Click **Add** to add a new WLAN Profile or click the one you want to edit.

**Step 3** In the **Edit WLAN** window, click **Security** > **Layer2**.

**Step 4** From **Layer 2 Security Mode** drop-down menu, select **WPA + WPA2**.

**Step 5** Configure the security parameters and then click **Save and Apply to Device**.



CHAPTER 17

# Configuring Policy Profile Features

## Configuring AAA Override

### SUMMARY STEPS

1. **configure terminal**
2. **wireless profile policy** *profile-policy*
3. **aaa-override**
4. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 2** | **wireless profile policy** *profile-policy*<br>**Example:**<br>`Device(config)# wireless profile policy test-wgb` | Configures WLAN policy profile and enters the wireless policy configuration mode. |
| **Step 3** | **aaa-override**<br>**Example:**<br>`Device(config-wireless-policy)# aaa-override` | Configures AAA policy override.<br>**Note** If VLAN is not pushed from the RADIUS server, the VLAN Override feature can be disabled from the RADIUS server. |
| **Step 4** | **end** | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device(config-wireless-policy)# end` | Alternatively, you can also press **Ctrl-Z** to exit global configuration mode. |

# Configuring Override VLAN for Central Switching

### SUMMARY STEPS

1. **configure terminal**
2. **vlan** *vlan-id*
3. **name** *vlan-name*
4. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 2** | **vlan** *vlan-id*<br>**Example:**<br>`Device(config)# vlan 20` | Defines VLANs that can be pushed from the RADIUS server.<br>**Note** The valid VLAN ID ranges from 1 to 4094. |
| **Step 3** | **name** *vlan-name*<br>**Example:**<br>`Device(config-vlan)# name vlan_ascii` | (Optional) Changes the default name of the VLAN. |
| **Step 4** | **end**<br>**Example:**<br>`Device(config-vlan)# end` | Returns to privileged EXEC mode.<br>Alternatively, you can also press **Ctrl-Z** to exit global configuration mode. |

# Configuring Override VLAN for Local Switching

### SUMMARY STEPS

1. **configure terminal**
2. **wireless profile flex** *flex_profile_name*
3. **vlan-name** *vlan_name*
4. **vlan-id** *vlan_id*
5. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 2** | **wireless profile flex** *flex_profile_name*<br>**Example:**<br>`Device(config)# wireless profile flex rr-xyz-flex-profile` | Configures a Flex profile. |
| **Step 3** | **vlan-name** *vlan_name*<br>**Example:**<br>`Device(config-wireless-flex-profile)# vlan-name vlan_123` | Defines VLANs that can be pushed from the RADIUS server. |
| **Step 4** | **vlan-id** *vlan_id*<br>**Example:**<br>`Device(config-wireless-flex-profile-vlan)# vlan-id 23` | Configures VLAN ID.<br>The valid VLAN ID ranges from 1 to 4096. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config-wireless-flex-profile-vlan)# end` | Returns to privileged EXEC mode.<br>Alternatively, you can also press **Ctrl-Z** to exit global configuration mode. |

# Verifying VLAN Override on Layer 3 Web Authentication

To display the VLAN override after L3 authentication, use the following command:

```
Device# show wireless client mac <mac> detail
[…]
        Vlan Override after L3 Auth: True
```

To display the statistics about client, use the following command:

```
Device# show wireless stats client detail
[…]
      Total L3 VLAN Override vlan change received      : 1
      Total L3 VLAN Override disassociations sent      : 1
      Total L3 VLAN Override re-associations received  : 1
      Total L3 VLAN Override successful VLAN change    : 1
      […]
      L3 VLAN Override connection timeout                             : 0
```

# Configuring DHCP for WLANS (CLI)

## Configuring DHCP Scopes (CLI)

### SUMMARY STEPS

1. **configure terminal**
2. **ip dhcp pool** *pool-name*
3. **network** *network-name mask-address*
4. **dns-server** *hostname*
5. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 2** | **ip dhcp pool** *pool-name*<br>**Example:**<br>`(config)#ip dhcp pool test-pool` | Configures the DHCP pool address. |
| **Step 3** | **network** *network-name mask-address*<br>**Example:**<br>`(dhcp-config)#network 209.165.200.224 255.255.255.0` | Specifies the network number in dotted-decimal notation and the mask address. |
| **Step 4** | **dns-server** *hostname*<br>**Example:**<br>`(dhcp-config)#dns-server example.com` | Specifies the DNS name server. You can specify an IP address or a hostname. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode. |

## Configuring the Internal DHCP Server Under Client VLAN SVI (CLI)

### Before you begin

- For wireless clients, only two DHCP servers are supported.
- To use the internal DHCP server for both wireless and wired client VLAN, an IP address must be configured under the client VLAN SVI.

- For wireless clients, the IP address of the internal DHCP server must be different from the address of the wireless client VLAN SVI (in the DHCP helper address configuration).
- For wireless clients, the internal DHCP server can be configured under the client VLAN SVI or under the wireless policy profile.

## SUMMARY STEPS

1. **configure terminal**
2. **interface loopback** *interface-number*
3. **ip address** *ip-address*
4. **exit**
5. **interface vlan** *vlan-id*
6. **ip address** *ip-address*
7. **ip helper-address** *ip-address*
8. **no mop enabled**
9. **no mop sysid**
10. **exit**
11. **ip dhcp excluded-address** *ip-address*
12. **ip dhcp excluded-address** *ip-address*
13. **ip dhcp pool** *pool-name*
14. **network** *network-name mask-address*
15. **default-router** *ip-address*
16. **exit**
17. **wireless profile policy** *profile-policy*
18. **central association**
19. **central dhcp**
20. **central switching**
21. **description** *policy-proile-name*
22. **vlan** *vlan-name*
23. **no shutdown**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 2** | **interface loopback** *interface-number*<br>**Example:**<br>`Device(config)# interface Loopback0` | Creates a loopback interface and enters interface configuration mode. |
| **Step 3** | **ip address** *ip-address*<br>**Example:** | Configures the IP address for the interface. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-if)# ip address 10.10.10.1 255.255.255.255` | |
| **Step 4** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode. |
| **Step 5** | **interface vlan** *vlan-id*<br>**Example:**<br>`Device(config)# interface vlan 32` | Configures the VLAN ID. |
| **Step 6** | **ip address** *ip-address*<br>**Example:**<br>`Device(config-if)# ip address 192.168.32.100 255.255.255.0` | Configures the IP address for the interface. |
| **Step 7** | **ip helper-address** *ip-address*<br>**Example:**<br>`Device(config-if)# ip helper-address 10.10.10.1` | Configures the destination address for UDP broadcasts.<br>**Note** If the IP address used in the **ip helper-address** command is an internal address of the controller an internal DHCP server is used. Otherwise, the external DHCP server is used. |
| **Step 8** | **no mop enabled**<br>**Example:**<br>`Device(config-if)# no mop enabled` | Disables the Maintenance Operation Protocol (MOP) for an interface. |
| **Step 9** | **no mop sysid**<br>**Example:**<br>`Device(config-if)# no mop sysid` | Disables the task of sending MOP periodic system ID messages. |
| **Step 10** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode. |
| **Step 11** | **ip dhcp excluded-address** *ip-address*<br>**Example:**<br>`Device(config)# ip dhcp excluded-address 192.168.32.1` | Specifies the IP address that the DHCP server should not assign to DHCP clients. |
| **Step 12** | **ip dhcp excluded-address** *ip-address*<br>**Example:**<br>`Device(config)# ip dhcp excluded-address 192.168.32.100` | Specifies the IP addresses that the DHCP server should not assign to DHCP clients. |
| **Step 13** | **ip dhcp pool** *pool-name*<br>**Example:** | Configures the DHCP pool address. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config)# ip dhcp pool pool-vlan32` | |
| **Step 14** | **network** *network-name mask-address*<br>**Example:**<br>`Device(dhcp-config)# network 192.168.32.0 255.255.255.0` | Specifies the network number in dotted-decimal notation, along with the mask address. |
| **Step 15** | **default-router** *ip-address*<br>**Example:**<br>`Device(dhcp-config)# default-router 192.168.32.1` | Specifies the IP address of the default router for a DHCP client. |
| **Step 16** | **exit**<br>**Example:**<br>`Device(dhcp-config)# exit` | Exits DHCP configuration mode. |
| **Step 17** | **wireless profile policy** *profile-policy*<br>**Example:**<br>`Device(config)# wireless profile policy default-policy-profile` | Configures the WLAN policy profile and enters wireless policy configuration mode. |
| **Step 18** | **central association**<br>**Example:**<br>`Device(config-wireless-policy)# central association` | Configures central association for locally switched clients. |
| **Step 19** | **central dhcp**<br>**Example:**<br>`Device(config-wireless-policy)# central dhcp` | Configures the central DHCP for locally switched clients. |
| **Step 20** | **central switching**<br>**Example:**<br>`Device(config-wireless-policy)# central switching` | Configures WLAN for central switching. |
| **Step 21** | **description** *policy-proile-name*<br>**Example:**<br>`Device(config-wireless-policy)# description "default policy profile"` | Adds a description for the policy profile |
| **Step 22** | **vlan** *vlan-name*<br>**Example:**<br>`Device(config-wireless-policy)# vlan 32` | Assigns the profile policy to the VLAN. |
| **Step 23** | **no shutdown**<br>**Example:**<br>`Device(config-wireless-policy)# no shutdown` | Enables the wireless profile policy. |

# Configuring the Internal DHCP Server Under a Wireless Policy Profile

## SUMMARY STEPS

1. **configure terminal**
2. **interface loopback** *interface-number*
3. **ip address** *ip-address*
4. **exit**
5. **interface vlan** *vlan-id*
6. **ip address** *ip-address*
7. **no mop enabled**
8. **no mop sysid**
9. **exit**
10. **ip dhcp excluded-address** *ip-address*
11. **ip dhcp pool** *pool-name*
12. **network** *network-name mask-address*
13. **default-router** *ip-address*
14. **exit**
15. **wireless profile policy** *profile-policy*
16. **central association**
17. **central switching**
18. **description** *policy-proile-name*
19. **ipv4 dhcp opt82**
20. **ipv4 dhcp opt82 ascii**
21. **ipv4 dhcp opt82 format vlan_id**
22. **ipv4 dhcp opt82 rid** *vlan_id*
23. **ipv4 dhcp server** *ip-address*
24. **vlan** *vlan-name*
25. **no shutdown**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 2** | **interface loopback** *interface-number*<br>**Example:**<br>`Device(config)# interface Loopback0` | Creates a loopback interface and enters interface configuration mode. |
| **Step 3** | **ip address** *ip-address*<br>**Example:**<br>`Device(config-if)# ip address 10.10.10.1 255.255.255.255` | Configures the IP address for the interface. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode. |
| **Step 5** | **interface vlan** *vlan-id*<br>**Example:**<br>`Device(config)# interface vlan 32` | Configures the VLAN ID. |
| **Step 6** | **ip address** *ip-address*<br>**Example:**<br>`Device(config-if)# ip address 192.168.32.100 255.255.255.0` | Configures the IP address for the interface. |
| **Step 7** | **no mop enabled**<br>**Example:**<br>`Device(config-if)# no mop enabled` | Disables the Maintenance Operation Protocol (MOP) for an interface. |
| **Step 8** | **no mop sysid**<br>**Example:**<br>`Device(config-if)# no mop sysid` | Disables the task of sending MOP periodic system ID messages. |
| **Step 9** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode. |
| **Step 10** | **ip dhcp excluded-address** *ip-address*<br>**Example:**<br>`Device(config)# ip dhcp excluded-address 192.168.32.100` | Specifies the IP address that the DHCP server should not assign to DHCP clients. |
| **Step 11** | **ip dhcp pool** *pool-name*<br>**Example:**<br>`Device(config)# ip dhcp pool pool-vlan32` | Configures the DHCP pool address. |
| **Step 12** | **network** *network-name mask-address*<br>**Example:**<br>`Device(dhcp-config)# network 192.168.32.0 255.255.255.0` | Specifies the network number in dotted-decimal notation along with the mask address. |
| **Step 13** | **default-router** *ip-address*<br>**Example:**<br>`Device(dhcp-config)# default-router 192.168.32.1` | Specifies the IP address of the default router for a DHCP client. |
| **Step 14** | **exit**<br>**Example:** | Exits DHCP configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(dhcp-config)# exit` | |
| **Step 15** | **wireless profile policy** *profile-policy*<br>**Example:**<br>`Device(config)# wireless profile policy default-policy-profile` | Configures a WLAN policy profile and enters wireless policy configuration mode. |
| **Step 16** | **central association**<br>**Example:**<br>`Device(config-wireless-policy)# central association` | Configures central association for locally switched clients. |
| **Step 17** | **central switching**<br>**Example:**<br>`Device(config-wireless-policy)# central switching` | Configures local switching. |
| **Step 18** | **description** *policy-proile-name*<br>**Example:**<br>`Device(config-wireless-policy)# description "default policy profile"` | Adds a description for the policy profile. |
| **Step 19** | **ipv4 dhcp opt82**<br>**Example:**<br>`Device(config-wireless-policy)# ipv4 dhcp opt82` | Enables DHCP Option 82 for the wireless clients. |
| **Step 20** | **ipv4 dhcp opt82 ascii**<br>**Example:**<br>`Device(config-wireless-policy)# ipv4 dhcp opt82 ascii` | Enables ASCII on DHCP Option 82. |
| **Step 21** | **ipv4 dhcp opt82 format vlan_id**<br>**Example:**<br>`Device(config-wireless-policy)# ipv4 dhcp opt82 format vlan32` | Enables VLAN ID. |
| **Step 22** | **ipv4 dhcp opt82 rid** *vlan_id*<br>**Example:**<br>`Device(config-wireless-policy)# ipv4 dhcp opt82 rid` | Supports the addition of Cisco 2-byte Remote ID (RID) for DHCP Option 82. |
| **Step 23** | **ipv4 dhcp server** *ip-address*<br>**Example:**<br>`Device(config-wireless-policy)#  ipv4 dhcp server 10.10.10.1` | Configures the WLAN's IPv4 DHCP server. |
| **Step 24** | **vlan** *vlan-name*<br>**Example:** | Assigns the profile policy to the VLAN. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-wireless-policy)# vlan 32` | |
| **Step 25** | **no shutdown**<br>**Example:**<br>`Device(config-wireless-policy)# no shutdown` | Enables the wireless profile policy. |

# Configuring the Internal DHCP Server Globally (CLI)

## SUMMARY STEPS

1. **configure terminal**
2. **interface loopback** *interface-num*
3. **ip address** *ip-address*
4. **exit**
5. **interface vlan***vlan-id*
6. **ip address** *ip-address*
7. **no mop enabled**
8. **no mop sysid**
9. **exit**
10. **ip dhcp-server** *ip-address*
11. **ip dhcp excluded-address** *ip-address*
12. **ip dhcp pool** *pool-name*
13. **network** *network-name mask-address*
14. **default-router** *ip-address*
15. **exit**
16. **wireless profile policy** *profile-policy*
17. **central association**
18. **central dhcp**
19. **central switching**
20. **description** *policy-proile-name*
21. **vlan** *vlan-name*
22. **no shutdown**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 2** | **interface loopback** *interface-num*<br>**Example:**<br>`Device(config)# interface Loopback0` | Creates a loopback interface and enters interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **ip address** *ip-address*<br>**Example:**<br>`Device(config-if)# ip address 10.10.10.1 255.255.255.255` | Configures the IP address for the interface. |
| **Step 4** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode. |
| **Step 5** | **interface vlan***vlan-id*<br>**Example:**<br>`Device(config)# interface vlan 32` | Configures the VLAN ID. |
| **Step 6** | **ip address** *ip-address*<br>**Example:**<br>`Device(config-if)# ip address 192.168.32.100 255.255.255.0` | Configures the IP address for the interface. |
| **Step 7** | **no mop enabled**<br>**Example:**<br>`Device(config-if)# no mop enabled` | Disables the Maintenance Operation Protocol (MOP) for an interface. |
| **Step 8** | **no mop sysid**<br>**Example:**<br>`Device(config-if)# no mop sysid` | Disables the task of sending the MOP periodic system ID messages. |
| **Step 9** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits the interface configuration mode. |
| **Step 10** | **ip dhcp-server** *ip-address*<br>**Example:**<br>`Device(config)# ip dhcp-server 10.10.10.1` | Specifies the target DHCP server parameters. |
| **Step 11** | **ip dhcp excluded-address** *ip-address*<br>**Example:**<br>`Device(config)# ip dhcp excluded-address 192.168.32.100` | Specifies the IP address that the DHCP server should not assign to DHCP clients. |
| **Step 12** | **ip dhcp pool** *pool-name*<br>**Example:**<br>`Device(config)# ip dhcp pool pool-vlan32` | Configures the DHCP pool address. |
| **Step 13** | **network** *network-name mask-address*<br>**Example:** | Specifies the network number in dotted-decimal notation along with the mask address. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(dhcp-config)# network 192.168.32.0 255.255.255.0` | |
| **Step 14** | **default-router** *ip-address*<br>**Example:**<br>`Device(dhcp-config)# default-router 192.168.32.1` | Specifies the IP address of the default router for a DHCP client. |
| **Step 15** | **exit**<br>**Example:**<br>`Device(dhcp-config)# exit` | Exits DHCP configuration mode. |
| **Step 16** | **wireless profile policy** *profile-policy*<br>**Example:**<br>`Device(config)# wireless profile policy default-policy-profile` | Configures a WLAN policy profile and enters wireless policy configuration mode. |
| **Step 17** | **central association**<br>**Example:**<br>`Device(config-wireless-policy)# central association` | Configures central association for locally switched clients. |
| **Step 18** | **central dhcp**<br>**Example:**<br>`Device(config-wireless-policy)# central dhcp` | Configures central DHCP for locally switched clients. |
| **Step 19** | **central switching**<br>**Example:**<br>`Device(config-wireless-policy)# central switching` | Configures local switching. |
| **Step 20** | **description** *policy-proile-name*<br>**Example:**<br>`Device(config-wireless-policy)# description "default policy profile"` | Adds a description for the policy profile. |
| **Step 21** | **vlan** *vlan-name*<br>**Example:**<br>`Device(config-wireless-policy)# vlan 32` | Assigns the profile policy to the VLAN. |
| **Step 22** | **no shutdown**<br>**Example:**<br>`Device(config-wireless-policy)# no shutdown` | Enables the profile policy. |

# Verifying Internal DHCP Configuration

To verify client binding, use the following command:

```
Device# show ip dhcp binding

Bindings from all pools not associated with VRF:
IP address      Client-ID/              Lease expiration        Type       State
Interface
                Hardware address/
                User name
192.168.32.3    0130.b49e.491a.53       Mar 23 2018 06:42 PM    Automatic  Active
Loopback0
```

To verify the DHCP relay statistics for a wireless client, use the following command:

```
Device# show wireless dhcp relay statistics

DHCP Relay Statistics
---------------------

DHCP Server IP :   10.10.10.1

Message              Count
--------------------------
DHCPDISCOVER      :  1
BOOTP FORWARD     :  137
BOOTP REPLY       :  0
DHCPOFFER         :  0
DHCPREQUEST       :  54
DHCPACK           :  0
DHCPNAK           :  0
DHCPDECLINE       :  0
DHCPRELEASE       :  0
DHCPINFORM        :  82

Tx/Rx Time :
------------
LastTxTime : 18:42:18
LastRxTime : 00:00:00

Drop Counter :
-------------
TxDropCount : 0
```

To verify the DHCP packet punt statistics in CPP, use the following command:

```
Device# show platform hardware chassis active qfp feature wireless punt statistics

CPP Wireless Punt stats:

                                 App Tag     Packet Count
                                 -------     ------------
         CAPWAP_PKT_TYPE_DOT11_PROBE_REQ            14442
              CAPWAP_PKT_TYPE_DOT11_MGMT               50
              CAPWAP_PKT_TYPE_DOT11_IAPP             9447
              CAPWAP_PKT_TYPE_DOT11_RFID                0
               CAPWAP_PKT_TYPE_DOT11_RRM                0
             CAPWAP_PKT_TYPE_DOT11_DOT1X                0
        CAPWAP_PKT_TYPE_CAPWAP_KEEPALIVE             2191
      CAPWAP_PKT_TYPE_MOBILITY_KEEPALIVE                0
            CAPWAP_PKT_TYPE_CAPWAP_CNTRL             7034
             CAPWAP_PKT_TYPE_CAPWAP_DATA                0
          CAPWAP_PKT_TYPE_MOBILITY_CNTRL                0
                         WLS_SMD_WEBAUTH                0
                       SISF_PKT_TYPE_ARP             5292
                      SISF_PKT_TYPE_DHCP              140
```

```
                              SISF_PKT_TYPE_DHCP6             1213
                            SISF_PKT_TYPE_IPV6_ND              350
                         SISF_PKT_TYPE_DATA_GLEAN               44
                      SISF_PKT_TYPE_DATA_GLEAN_V6               51
                         SISF_PKT_TYPE_DHCP_RELAY              122
                  CAPWAP_PKT_TYPE_CAPWAP_RESERVED                0
```

# Configuring FlexConnect DHCP-Required (CLI)

Perform the procedure given below to configure FlexConnect DHCP-Required through the CLI:

### SUMMARY STEPS

1. **configure terminal**
2. **wireless profile policy** *profile-policy*
3. **ipv4 dhcp required**
4. **no shutdown**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device#configure terminal` | Enters global configuration mode. |
| **Step 2** | **wireless profile policy** *profile-policy*<br>**Example:**<br>`Device#wireless profile policy` *`rr-xyz-policy-1`* | Configures WLAN policy profile and enters the wireless policy configuration mode. |
| **Step 3** | **ipv4 dhcp required**<br>**Example:**<br>`Device(config-wireless-policy)#ipv4 dhcp required` | Enables the FlexConnect DHCP-Required feature. |
| **Step 4** | **no shutdown**<br>**Example:**<br>`Device(config-wireless-policy)#no shutdown` | Saves the configuration. |

# Verifying FlexConnect DHCP-Required

- To verify the IP address learnt for a client on an IP DHCP-Required policy-enabled WLAN, use the **show wireless client summary** command:

**Note** The controller or AP does not learn the IP address through other means such as ARP or data gleaning, when IPv4 DHCP-Required is enabled.

```
Device# show wireless client summary
Number of Clients: 1
MAC Address         AP Name            Type  ID  State          Protocol     Method
Role
-------------------------------------------------------------------------------------
1cXX.bXXX.59XX      APXXXX.7XXX.4XXX   WLAN  3   IP Learn       11ac         Dot1x
Local
```

- This example shows that the client IP is in the **Run** state, indicating that the client has received the IP address from DHCP:

```
Device# show wireless client summary
Number of Clients: 1
MAC Address       AP Name             Type       ID       State         Protocol
Method      Role
-------------------------------------------------------------------------------------
5XXX.37XX.c3XX    APXXXX.4XXX.4XXX    WLAN        3        Run          11n(5)
None        Local
```

# Configuring DHCP for WLANs (GUI)

## Configuring DHCP Scopes (GUI)

**Step 1** Choose **Administration** > **DHCP Pools**.

**Step 2** In the **Pools** section, click **Add** to add a new DHCP pool.

The **Create DHCP Pool** dialog box is displayed.

**Step 3** In the **DHCP Pool Name** field, enter a name for the new DHCP pool.

**Step 4** From the **IP Type** drop-down list, choose the IP address type.

**Step 5** In the **Network** field, enter the network served by this DHCP scope. This IP address is used by the management interface with netmask applied, as configured in the **Interfaces** window.

**Step 6** In the **Subnet Mask** field, enter the subnet mask assigned to all the wireless clients.

**Step 7** In the **Starting ip** field, enter the starting IP address.

**Step 8** In the **Ending ip** field, enter the trailing IP address.

**Step 9** In the **Reserved Only** field, enable or disable it.

**Step 10** From the **Lease** drop-down list, choose the lease type as either **User Defined** or **Never Expires**. If you choose User Defined, you can enter the amount of time that an IP address is granted to a client.

**Step 11** To perform advanced configuration for DHCP scope, click **Advanced**.

**Step 12** Check the **Enable DNS Proxy** check box to enable DNS proxy.

**Step 13** In the **Default Router(s)** field, enter the IP address of the optional router or routers that connect to the device and click the + icon to add them to the list. Each router must include a DHCP forwarding agent that enables a single device to serve the clients of multiple devices.

**Step 14** In the **DNS Server(s)** field, enter the IP address of the optional DNS server or servers and click the + icon to add them to the list. Each DNS server must be able to update a client's DNS entry to match the IP address assigned by the DHCP scope.

**Step 15** In the **NetBios Name Server(s)** field, enter the IP address of the optional Microsoft NetBIOS name server or servers, such as Microsoft Windows Internet Naming Service (WINS) server, and click the **+** icon to add them to the list.

**Step 16** In the **Domain** field, enter the optional domain name of the DHCP scope for use with one or more DNS servers.

**Step 17** To add **DHCP** options, click **Add** in the **DHCP Options List** section. DHCP provides an internal framework for passing configuration parameters and other control information, such as DHCP options, to the clients on your network. DHCP options carry parameters as tagged data stored within protocol messages exchanged between the DHCP server and its clients.

**Step 18** Enter the **DHCP** option that you want to add.

**Step 19** Click **Save & Apply to Device**.

## Configuring the Internal DHCP Server Under Client VLAN SVI (GUI)

**Step 1** Choose **Configuration** > **Layer2** > **VLAN** > **SVI**.

**Step 2** Click an SVI.

**Step 3** Click the **Advanced** tab.

**Step 4** Under **DHCP Relay** settings, enter the **IPV4 Helper Address**.

**Step 5** Click **Update & Apply to Device**.

## Configuring the Internal DHCP Server Under a Wireless Policy Profile (GUI)

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

**Step 2** Click a policy name.

**Step 3** Click the **Advanced** tab.

**Step 4** Under **DHCP** settings, check or uncheck the **IPv4 DHCP Required** check box and enter the **DHCP Server IP Address**.

**Step 5** Click **Update & Apply to Device**.

## Configuring the Internal DHCP Server Globally (GUI)

**Step 1** Choose **Administration** > **DHCP Pools** > **Pools**.

**Step 2** Click **Add**.

The **Create DHCP Pool** window is displayed.

**Step 3** Enter the **DHCP Pool Name**, **Network**, **Starting ip**, and **Ending ip**.

**Step 4** From the **IP Type**, **Subnet Mask**, and **Lease** drop-down lists, choose a value.

**Step 5** Click the **Reserved Only** toggle button.

**Step 6** Click **Apply to Device**.

# Configuring FlexConnect DHCP-Required (GUI)

Perform the steps given below to configure the FlexConnect DHCP-Required feature through the GUI:

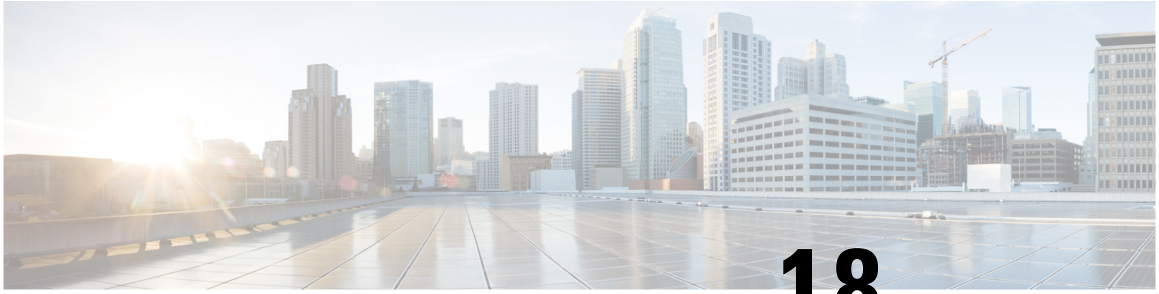
**Step 1** Choose **Configuration** > **Tags & Profiles** > **Policy**.

**Step 2** On the **Policy** window, click the name of the corresponding Policy Profile.
The **Edit Policy Profile** window is displayed.

**Step 3** Click the **Advanced** tab.

**Step 4** In the **DHCP** section, check the **IPv4 DHCP Required** check box to enable the feature.

**Step 5** Click **Update & Apply to Device**.



CHAPTER 18

# Configuring Remote LANs

# Configuring Remote LANs (CLI)

## Creating an RLAN Profile (CLI)

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap remote-lan profile-name** *remote-lan-profile-name rlan-id*
4. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ap remote-lan profile-name** *remote-lan-profile-name rlan-id*<br>**Example:**<br>`Device(config)# ap remote-lan profile-name rlan_profile_name 3` | Configures remote LAN profile and enters RLAN configuration mode.<br>• *remote-lan-profile*: The remote LAN profile name. Range is from 1 to 32 alphanumeric characters.<br>• *rlan-id*: The remote LAN identifier. Range is from 1 to 128. |

| | Command or Action | Purpose |
|---|---|---|
| | | **Note** You can create a maximum of 128 RLANs. You cannot use the *rlan-id* of an existing RLAN while creating another RLAN.<br>Both RLAN and WLAN profiles cannot have the same names. Similarly, RLAN and WLAN policy profile cannot have the same names. |
| **Step 4** | **end**<br>**Example:**<br>`Device(config-remote-lan)# end` | Exits RLAN configuration mode and returns to privileged EXEC mode. |

# Configuring RLAN Profile Parameters (CLI)

### Before you begin

**Note** The configurations in this section are not mandatory for an RLAN profile.

In case of central switching mode, you need to configure both central switching and central DHCP.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap remote-lan profile-name** *remote-lan-profile-name rlan-id*
4. **client association limit** *client-connections*
5. **ip access-group web** *IPv4-acl-name*
6. **ipv6 traffic-filter web** *IPv6-acl-name*
7. **local-auth** *profile name*
8. **mac-filtering** *mac-filter-name*
9. **mdns-sd-interface** {**drop** | **gateway**}
10. **security dot1x authentication-list** *list-name*
11. **security web-auth authentication-list** *list-name*
12. **no shutdown**
13. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ap remote-lan profile-name** *remote-lan-profile-name rlan-id*<br>**Example:**<br>`Device(config)# ap remote-lan profile-name rlan_profile_name 3` | Configures remote LAN profile and enters RLAN configuration mode. |
| **Step 4** | **client association limit** *client-connections*<br>**Example:**<br>`Device(config-remote-lan)# client association limit 1` | Configures client connections per RLAN.<br>*client-connections*: The maximum client connections per RLAN. Range is from 0 to 10000. 0 refers to unlimited client connections. |
| **Step 5** | **ip access-group web** *IPv4-acl-name*<br>**Example:**<br>`Device(config-remote-lan)# ip access-group web acl_name` | Configures RLAN IP configuration commands.<br>*IPv4-acl-name*: The IPv4 ACL name or ID. |
| **Step 6** | **ipv6 traffic-filter web** *IPv6-acl-name*<br>**Example:**<br>`Device(config-remote-lan)# ipv6 traffic-filter web ipv6-acl` | Configures RLAN IP configuration commands.<br>*IPv6-acl-name*: The IPv6 ACL name or ID. |
| **Step 7** | **local-auth** *profile name*<br>**Example:**<br>`Device(config-remote-lan)# local-auth profile_name` | Sets EAP profile on an RLAN. |
| **Step 8** | **mac-filtering** *mac-filter-name*<br>**Example:**<br>`Device(config-remote-lan)# mac-filtering mac_filter` | Sets MAC filtering support on an RLAN. |
| **Step 9** | **mdns-sd-interface** {**drop** \| **gateway**}<br>**Example:**<br>`Device(config-remote-lan)# mdns-sd-interface gateway` | Enables MDNS gateway for the RLAN. |
| **Step 10** | **security dot1x authentication-list** *list-name*<br>**Example:**<br>`Device(config-remote-lan)# security dot1x authentication-list dot1_auth_list` | Configures 802.1X for an RLAN. |
| **Step 11** | **security web-auth authentication-list** *list-name*<br>**Example:** | Configures web authentication for an RLAN. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-remote-lan)# security web-auth authentication-list web_auth_list` | **Note** You can activate either web authentication or dot1x authentication at a time. |
| **Step 12** | **no shutdown**<br>**Example:**<br>`Device(config-remote-lan)# no shutdown` | Enables RLAN profile. |
| **Step 13** | **end**<br>**Example:**<br>`Device(config-remote-lan)# end` | Exits RLAN configuration mode and returns to privileged EXEC mode. |

# Creating an RLAN Policy Profile (CLI)

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap remote-lan-policy policy-name** *profile name*
4. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ap remote-lan-policy policy-name** *profile name*<br>**Example:**<br>`Device(config)# ap remote-lan-policy policy-name rlan_policy_prof_name` | Configures RLAN policy profile and enters RLAN policy configuration mode. |
| **Step 4** | **end**<br>**Example:**<br>`Device(config)# ap remote-lan-policy policy-name rlan_policy_prof_name` | Exits RLAN policy configuration mode and returns to privileged EXEC mode. |

# Configuring RLAN Policy Profile Parameters (CLI)

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap remote-lan-policy policy-name** *profile name*
4. **central switching**
5. **central dhcp**
6. **exclusionlist timeout** *timeout*
7. **ipv4** {**acl** *ipv6_acl* | **dhcp** {**required** | **server** *ip-address*}}
8. **ipv6 acl** *ipv6-acl*
9. **aaa-policy** *policy-name*
10. **aaa-override**
11. **accounting-list** *list-name*
12. **mdns-sd service-policy** *service-policy-name*
13. **session-timeout** *timeout in seconds*
14. **host-mode** {**multidomain** *voice domain* | **multihost** |**singlehost**}
15. **violation-mode** {**protect** | **replace** | **shutdown**}
16. **poe**
17. **power-level** *level*
18. **pre-auth**
19. **user-defined-network** [**drop-unicast**]
20. **shutdown**
21. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ap remote-lan-policy policy-name** *profile name*<br>**Example:**<br>`Device(config)# ap remote-lan-policy policy-name rlan_policy_prof_name` | Configures RLAN policy profile and enters RLAN policy configuration mode. |
| **Step 4** | **central switching**<br>**Example:**<br>`Device(config-remote-lan-policy)# central switching` | Configures central switching. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **central dhcp**<br>**Example:**<br>`Device(config-remote-lan-policy)# central dhcp` | Configures central DHCP. |
| **Step 6** | **exclusionlist timeout** *timeout*<br>**Example:**<br>`Device(config-remote-lan-policy)# exclusionlist timeout 200` | Sets exclusion-listing on RLAN.<br>*timeout*: Sets the time, up to which the client will be in excluded state. Range is from 0 to 2147483647 seconds. 0 refers to no timeout. |
| **Step 7** | **ipv4** {**acl** *ipv6_acl* \| **dhcp** {**required** \| **server** *ip-address*}}<br>**Example:**<br>`Device(config-remote-lan-policy)# ipv4 dhcp server 10.1.1.1` | Configures an IPv4 DHCP server for the RLAN. |
| **Step 8** | **ipv6 acl** *ipv6-acl*<br>**Example:**<br>`Device(config-remote-lan-policy)# ipv6 acl ipv6_acl` | Configures an IPv6 ACL. |
| **Step 9** | **aaa-policy** *policy-name*<br>**Example:**<br>`Device(config-remote-lan-policy)# aaa-policy aaa_policy1` | Configures AAA policy. |
| **Step 10** | **aaa-override**<br>**Example:**<br>`Device(config-remote-lan-policy)# aaa-override` | Configures AAA policy override. |
| **Step 11** | **accounting-list** *list-name*<br>**Example:**<br>`Device(config-remote-lan-policy)# accounting-list rlan_acct_list1` | Sets the accounting list for IEEE 802.1x. |
| **Step 12** | **mdns-sd service-policy** *service-policy-name*<br>**Example:**<br>`Device(config-remote-lan-policy)# mdns-sd service-policy mdns-service-policy` | Configures an MDNS service policy. |
| **Step 13** | **session-timeout** *timeout in seconds*<br>**Example:**<br>`Device(config-remote-lan-policy)# session-timeout 21` | Configures client session timeout.<br>*timeout in seconds*: Defines the duration of a session. Range is from 20 to 86400 seconds. |
| **Step 14** | **host-mode** {**multidomain** *voice domain* \| **multihost** \|**singlehost**}<br>**Example:** | Configures host mode for remote-LAN 802.1x.<br>*voice domain*: The RLAN voice domain VLAN ID. Range is from 0 to 65535. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-remote-lan-policy)# host-mode multidomain` | You can configure the following IEEE 802.1X authentication modes:<br>• Multi-Domain Mode: The authenticator allows one host from the data domain and another from the voice domain. This is a typical configuration on switch ports with IP phones connected.<br>• Multi-Host Mode: The first device to authenticate opens up to the switch port, so that all other devices can use the port. You need not authenticate other devices independently, if the authenticated device becomes authorized the switch port is closed.<br>• Single-Host Mode: The default host mode. In this mode, the switch port allows only a single host to be authenticated and passes traffic one by one. |
| **Step 15** | **violation-mode** {**protect** \| **replace** \| **shutdown**}<br>**Example:**<br>`Device(config-remote-lan-policy)# violation-mode protect` | Configures violation mode for Remote-LAN 802.1x.<br>When a security violation occurs, a port is protected based on the following configured violation actions:<br>• Shutdown: Disables the port.<br>• Replace: Removes the current session and initiates authentication for the new host. This is the default behavior.<br>• Protect: Drops packets with unexpected MAC addresses without generating a system message. In single-host authentication mode, a violation is triggered when more than one device is detected in data VLAN. In multi-host authentication mode, a violation is triggered when more than one device is detected in data VLAN or voice VLAN. |
| **Step 16** | **poe**<br>**Example:**<br>`Device(config-remote-lan-policy)# poe` | Enables Power over Ethernet (PoE). |
| **Step 17** | **power-level** *level*<br>**Example:**<br>`Device(config-remote-lan-policy)# power-level 1` | Configures the power level to be supported on the LAN port. |
| **Step 18** | **pre-auth**<br>**Example:**<br>`Device(config-remote-lan-policy)# pre-auth` | Configures pre-authentication for the RLAN. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 19** | **user-defined-network** [**drop-unicast**]<br>**Example:**<br>`Device(config-remote-lan-policy)# user-defined network` | Configures an user-defined network. |
| **Step 20** | **shutdown**<br>**Example:**<br>`Device(config-remote-lan-policy)# shutdown` | Enables RLAN policy profile. |
| **Step 21** | **end**<br>**Example:**<br>`Device(config-remote-lan-policy)# end` | Exits RLAN policy configuration mode and returns to privileged EXEC mode. |

# Configuring a Policy Tag and Mapping an RLAN Policy Profile to an RLAN Profile (CLI)

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **wireless tag policy** *policy-tag-name*
4. **remote-lan** *remote-lan-profile-name* **policy** *rlan-policy-profile-name* **port-id** *port-id*
5. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **wireless tag policy** *policy-tag-name*<br>**Example:**<br>`Device(config)# wireless tag policy remote-lan-policy-tag` | Configures policy tag and enters policy tag configuration mode. |
| **Step 4** | **remote-lan** *remote-lan-profile-name* **policy** *rlan-policy-profile-name* **port-id** *port-id*<br>**Example:** | Maps an RLAN policy profile to an RLAN profile. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-policy-tag)# remote-lan rlan_profile_name policy rlan_policy_profile port-id 2` | |
| **Step 5** | **end**<br>**Example:**<br>`Device(config-policy-tag)# end` | Exit policy tag configuration mode and returns to privileged EXEC mode. |

# Attaching an RLAN Policy Tag to an Access Point (CLI)

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap** *ap-ethernet-mac*
4. **policy-tag** *policy-tag-name*
5. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ap** *ap-ethernet-mac*<br>**Example:**<br>`Device(config)# ap 00a2.891c.21e0` | Configures MAP address for an AP and enters AP configuration mode. |
| **Step 4** | **policy-tag** *policy-tag-name*<br>**Example:**<br>`Device(config-ap-tag)# policy-tag remote-lan-policy-tag` | Attaches a policy tag to the access point.<br>*policy-tag-name*: Name of the policy tag defined earlier. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config-ap-tag)# end` | Exits AP configuration mode and returns to privileged EXEC mode. |

# Configuring Remote LANs (GUI)

## Creating RLAN Profile (GUI)

**Step 1** Choose **Configuration** > **Tags & Profiles** > **Remote LAN**.

**Step 2** Click **Add**.

**Step 3** Enter the **Profile Name**, **RLAN ID** and enable or disable the **Status** toggle button. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

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

## Configuring RLAN Profile Parameters (GUI)

**Step 1** Choose **Configuration** > **Tags & Profiles** > **Remote LAN**.

**Step 2** On the **RLAN Profile** tab, click **Add**.

The **Add RLAN Profile** window is displayed.

**Step 3** In the **General** tab:

a) Enter a **Name** and **RLAN ID** for the RLAN profile. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

b) Set the number of client connections per RLAN in the **Client Association Limit** field.

The range depends on the maximum number of clients supported by the platform.

c) To enable the profile, set the status as **Enable**.

**Step 4** In the **Security** > **Layer2** tab

a) To enable 802.1x for an RLAN, set the **802.1x** status as **Enabled**.

**Note** You can activate either web or 802.1x authentication list at a time.

b) Choose the authorization list name from the **MAC Filtering** drop-down list.

c) Choose the 802.1x for an RLAN authentication list name from the **Authentication List** drop-down list.

**Step 5** In the **Security** > **Layer3** tab

a) To enable web authentication for an RLAN, set the **Web Auth** status as **Enabled**.

**Note** You can activate either web or 802.1x authentication list at a time.

b) Choose the web authentication parameter map from the **Webauth Parameter Map** drop-down list.

c) Choose the web authentication list name from the **Authentication List** drop-down list.

**Step 6** In the **Security** > **AAA** tab

a) Set the **Local EAP Authentication** to enabled. Also, choose the required **EAP Profile Name** from the drop-down list.

**Step 7** Save the configuration.

## Creating RLAN Policy Profile (GUI)

**Step 1** Choose **Configuration** > **Wireless** > **Remote LAN** > **RLAN Policy**

**Step 2** Click **Add**.

**Step 3** In the **General** tab, enter the **Policy Name**.

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

## Configuring RLAN Policy Profile Parameters (GUI)

**Step 1** Choose **Configuration** > **Wireless** > **Remote LAN**.

**Step 2** On the **Remote LAN** page, click **RLAN Policy** tab.

**Step 3** On the **RLAN Policy** page, click the name of the **Policy** or click **Add** to create a new one.

The **Add/Edit RLAN Policy** window is displayed.

**Step 4** In the **General** tab:

a) Enter a **Name** and **Description** for the policy profile.
b) Set **Central Authentication** to **Enabled** state.
c) Set **Central DHCP** to **Enabled** state.
d) Set the **PoE** check box to enable or disable state.
e) To enable the policy, set the status as **Enable**.

**Step 5** In the **Access Policies** Tab, choose the VLAN name or number from the **VLAN** drop-down list.

**Note** When central switching is disabled, the VLAN in the RLAN policy cannot be configured as the AP's native VLAN. To use the AP's native VLAN for client IP, the VLAN should be configured as either **no vlan** or **vlan 1** in the RLAN policy profile.

**Step 6** From the **Host Mode** drop-down list, choose the **Host Mode** for the remote-LAN802.1x from the following options:

- Single-Host Mode—Is the default host mode. In this mode, the switch port allows only a single host to be authenticated and passes traffic one by one.

- Multi-Host Mode—The first device to authenticate opens up to the switch port, so that all other devices can use the port. You need not authenticate other devices independently, if the authenticated device becomes authorized the switch port is closed.

- Multi-Domain Mode—The authenticator allows one host from the data domain and another from the voice domain. This is a typical configuration on switch ports with IP phones connected.

**Note**
- For an RLAN profile with open-auth configuration, you must map the RLAN-policy with single host mode. Mapping RLAN-policy with multi-host or multi-domain mode is not supported.
- The controller does not assign data versus voice VLAN, based on traffic. RLAN only supports multiple VLAN assignments through 802.1x AAA override. You must create data and voice VLANs and then assign these VLANs to respective clients, based on their authentication through the 802.1x AAA override.

**Step 7** Configure IPv6 ACL or Flexible NetFlow.

- Under the **Access Policies** > **Remote LAN ACL** section, choose the **IPv6 ACL** from the drop-down list.
- Under the **Access Policies** > **AVC** > **Flow Monitor IPv6** section, check the **Egress Status** and **Ingress Status** check boxes and choose the policies from the drop-down lists.

**Step 8** Click the **Advanced** tab.

a) Configure the violation mode for Remote-LAN 802.1x from the **Violation Mode** drop-down list, choose the violation mode type from the following options:

   - Shutdown—Disables the port
   - Replace—Removes the current session and initiates authentication for the new host. This is the default behavior.
   - Protect—Drops packets with unexpected MAC addresses without generating a system message.

b) Enter the **Session Timeout (sec)** value to define the client's duration of a session.

   The range is between 20 and 86400 seconds.

c) Under **AAA Policy Params** section, check the **AAA Override** check box to enable AAA override.

d) Under the **Exclusionlist Params** section, check the **Exclusionlist** check box and enter the **Exclusionlist Timeout** value.

   This sets the exclusion time for a client. The range is between 0 and 2147483647 seconds. 0 refers to no timeout.

**Step 9** Save the configuration.

# Attaching Policy Tag to an Access Point (GUI)

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

**Step 2** Select the AP to attach the Policy Tag.

**Step 3** Under the **Tags** section, use the **Policy** drop-down to select a policy tag.

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

CHAPTER 19

# Verifying the Configuration

This chapter provides the output of **show** commands that help you verify the configuration.

## Verifying the AP Filter Configuration

The following **show** commands are used to display tag sources and filters, and their priorities.

To view the tag source priorities, use the following command:

```
Device# show ap tag sources

Priority Tag source
--------------------------------
0 Static
1 Filter
2 AP
3 Default
```

To view the available filters, use the following command:

```
Device# show ap filter all

Filter Name             regex             Policy Tag              RF Tag              Site
 Tag
------------------------------------------------------------------------------------------
first                   abcd              pol-tag1                 rf-tag1
site-tag1
test1                   testany                                                      site1

filter1                 testany
```

To view the list of active filters, use the following command:

```
Device# show ap filters active

Priority   Filter Name       regex          Policy Tag              RF Tag
Site Tag
------------------------------------------------------------------------------------------
10         test1             testany
```

```
site1
```

To view the source of an AP tag, use the following command:

```
Device# show ap tag summary

Number of APs: 4

AP Name          AP Mac         Site Tag Name    Policy Tag Name    RF Tag Name
Misconfigured Tag Source
-----------------------------------------------------------------------------------------
AP002A.1034.CA78 002a.1034.ca78 named-site-tag   named-policy-tag   named-rf-tag   No Filter

AP00A2.891C.2480 00a2.891c.2480 named-site-tag   named-policy-tag   named-rf-tag   No Filter

AP58AC.78DE.9946 58ac.78de.9946 default-site-tag default-policy-tag default-rf-tag No AP
AP0081.C4F4.1F34 0081.c4f4.1f34 default-site-tag default-policy-tag default-rf-tag No Default
```

# Verifying the WLAN configuration

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

```
Device# show wlan summary | include test-wlan-ssid

1    test-wlan                       test-wlan-ssid                    137   UP
```

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

```
Device# show wlan id  2

WLAN Profile Name     : name
================================================
Identifier                                       : 2
Description                                      :
Network Name (SSID)                              : name
Status                                           : Disabled
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
OKC                                              : Enabled
Number of Active Clients                         : 0
CHD per WLAN                                     : Enabled
```

```
WMM                                            : Allowed
WiFi Direct Policy                             : Disabled
Channel Scan Defer Priority:
  Priority (default)                           : 5
  Priority (default)                           : 6
Scan Defer Time (msecs)                        : 100
Media Stream Multicast-direct                  : Disabled
CCX - AironetIe Support                        : Disabled
Peer-to-Peer Blocking Action                   : Disabled
Configured Radio Bands                         : All
Operational State of Radio Bands             : All Bands Operational
DTIM period for 802.11a radio                  :
DTIM period for 802.11b radio                  :
Local EAP Authentication                       : Disabled
Mac Filter Authorization list name             : Disabled
Mac Filter Override Authorization list name    : Disabled
Accounting list name                           :
802.1x authentication list name                : default
802.1x authorization list name                 : Disabled
Security
    802.11 Authentication                      : Open System
    Static WEP Keys                            : Disabled
    Wi-Fi Protected Access (WPA/WPA2/WPA3)     : Enabled
        WPA (SSN IE)                           : Disabled
        WPA2 (RSN IE)                          : Enabled
            MPSK                               : Disabled
            EasyPSK                            : Disabled
            AES Cipher                         : Enabled
            CCMP256 Cipher                     : Disabled
            GCMP128 Cipher                     : Disabled
            GCMP256 Cipher                     : Disabled
            Randomized GTK                     : Disabled
        WPA3 (WPA3 IE)                         : Disabled
        Auth Key Management
            802.1x                             : Disabled
            PSK                                : Disabled
            CCKM                               : Disabled
            FT dot1x                           : Disabled
            FT PSK                             : Disabled
            Dot1x-SHA256                       : Disabled
            PSK-SHA256                         : Disabled
            SAE                                : Disabled
            OWE                                : Disabled
            SUITEB-1X                          : Disabled
            SUITEB192-1X                       : Disabled
    CCKM TSF Tolerance (msecs)                 : 1000
    OWE Transition Mode                        : Disabled
    OSEN                                       : Disabled
    FT Support                                 : Adaptive
        FT Reassociation Timeout (secs)        : 20
        FT Over-The-DS mode                    : Disabled
    PMF Support                                : Disabled
        PMF Association Comeback Timeout (secs): 1
        PMF SA Query Time (msecs)              : 200
    Web Based Authentication                   : Disabled
    Conditional Web Redirect                   : Disabled
    Splash-Page Web Redirect                   : Disabled
    Webauth On-mac-filter Failure              : Disabled
    Webauth Authentication List Name           : default
    Webauth Authorization List Name            : Disabled
    Webauth Parameter Map                      : WLAN1_MAP
Band Select                                    : Disabled
Load Balancing                                 : Disabled
Multicast Buffer                               : Disabled
Multicast Buffers (frames)                     : 0
IP Source Guard                                : Disabled
Assisted-Roaming
    Neighbor List                              : Enabled
    Prediction List                            : Disabled
    Dual Band Support                          : Disabled
IEEE 802.11v parameters
    Directed Multicast Service                 : Enabled
    BSS Max Idle                               : Enabled
        Protected Mode                         : Disabled
    Traffic Filtering Service                  : Disabled
    BSS Transition                             : Enabled
        Disassociation Imminent                : Disabled
            Optimised Roaming Timer (TBTTS)    : 40
            Timer (TBTTS)                      : 200
        Dual Neighbor List                     : Disabled
    WNM Sleep Mode                             : Disabled
802.11ac MU-MIMO                               : Enabled
802.11ax parameters
    802.11ax Operation Status                  : Enabled
    OFDMA Downlink                             : Enabled
    OFDMA Uplink                               : Enabled
    MU-MIMO Downlink                           : Enabled
    MU-MIMO Uplink                             : Enabled
    BSS Target Wake Up Time                    : Enabled
    BSS Target Wake Up Time Broadcast Support  : Enabled
802.11 protocols in 2.4ghz band
    Protocol                                   : dot11bg
Advanced Scheduling Requests Handling          : Enabled
mDNS Gateway Status                            : Bridge
WIFI Alliance Agile Multiband                  : Disabled
Device Analytics
    Advertise Support                          : Enabled
    Advertise Support for PC analytics         : Enabled
    Share Data with Client                     : Disabled
Client Scan Report (11k Beacon Radio Measurement)
    Request on Association                     : Disabled
    Request on Roam                            : Disabled
WiFi to Cellular Steering                      : Disabled
Advanced Scheduling Requests Handling          : Enabled
Locally Administered Address Configuration
    Deny LAA clients                           : Disabled
```

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

```
Device# show wlan name test

WLAN Profile Name     : test
================================================
Identifier                                     : 24
Description                                    :
Network Name (SSID)                            : test
Status                                         : Disabled
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
OKC                                            : Enabled
Number of Active Clients                       : 0
CHD per WLAN                                   : Enabled
WMM                                            : Allowed
WiFi Direct Policy                             : Disabled
```

```
Channel Scan Defer Priority:
  Priority (default)                           : 5
  Priority (default)                           : 6
Scan Defer Time (msecs)                        : 100
Media Stream Multicast-direct                  : Disabled
CCX - AironetIe Support                        : Disabled
Peer-to-Peer Blocking Action                   : Disabled
Configured Radio Bands
      2.4ghz                                   : Enabled
      5ghz                                     : Enabled
           Slot                                : Enabled on all slots
Operational State of Radio Bands
      2.4ghz                                   : UP
      5ghz                                     : UP
           Slot                                : Enabled on all slots
DTIM period for 802.11a radio                  :
DTIM period for 802.11b radio                  :
Local EAP Authentication                       : Disabled
Mac Filter Authorization list name             : Disabled
Mac Filter Override Authorization list name    : Disabled
Accounting list name                           :
802.1x authentication list name                : Disabled
802.1x authorization list name                 : Disabled
Security
    802.11 Authentication                      : Open System
    Static WEP Keys                            : Disabled
    Wi-Fi Protected Access (WPA/WPA2/WPA3)     : Enabled
        WPA (SSN IE)                           : Disabled
        WPA2 (RSN IE)                          : Enabled
            MPSK                               : Disabled
            EasyPSK                            : Disabled
            AES Cipher                         : Enabled
            CCMP256 Cipher                     : Disabled
            GCMP128 Cipher                     : Disabled
            GCMP256 Cipher                     : Disabled
            Randomized GTK                     : Disabled
        WPA3 (WPA3 IE)                         : Disabled
        Auth Key Management
            802.1x                             : Enabled
            PSK                                : Disabled
            CCKM                               : Disabled
            FT dot1x                           : Disabled
            FT PSK                             : Disabled
            Dot1x-SHA256                       : Disabled
            PSK-SHA256                         : Disabled
            SAE                                : Disabled
            OWE                                : Disabled
            SUITEB-1X                          : Disabled
            SUITEB192-1X                       : Disabled
    CCKM TSF Tolerance (msecs)                 : 1000
    OWE Transition Mode                        : Disabled
    OSEN                                       : Disabled
    FT Support                                 : Adaptive
        FT Reassociation Timeout (secs)        : 20
        FT Over-The-DS mode                    : Disabled
    PMF Support                                : Disabled
        PMF Association Comeback Timeout (secs): 1
        PMF SA Query Time (msecs)              : 200
    Web Based Authentication                   : Disabled
    Conditional Web Redirect                   : Disabled
    Splash-Page Web Redirect                   : Disabled
    Webauth On-mac-filter Failure              : Disabled
    Webauth Authentication List Name           : Disabled
    Webauth Authorization List Name            : Disabled
    Webauth Parameter Map                      : Disabled
Band Select                                    : Disabled
Load Balancing                                 : Disabled
Multicast Buffer                               : Disabled
Multicast Buffers (frames)                     : 0
IP Source Guard                                : Disabled
Assisted-Roaming
    Neighbor List                              : Enabled
    Prediction List                            : Disabled
    Dual Band Support                          : Disabled
IEEE 802.11v parameters
    Directed Multicast Service                 : Enabled
    BSS Max Idle                               : Enabled
        Protected Mode                         : Disabled
    Traffic Filtering Service                  : Disabled
    BSS Transition                             : Enabled
        Disassociation Imminent                : Disabled
            Optimised Roaming Timer (TBTTS)    : 40
            Timer (TBTTS)                      : 200
        Dual Neighbor List                     : Disabled
    WNM Sleep Mode                             : Disabled
802.11ac MU-MIMO                               : Enabled
802.11ax parameters
    802.11ax Operation Status                  : Enabled
    OFDMA Downlink                             : Enabled
    OFDMA Uplink                               : Enabled
    MU-MIMO Downlink                           : Enabled
    MU-MIMO Uplink                             : Enabled
    BSS Target Wake Up Time                    : Enabled
    BSS Target Wake Up Time Broadcast Support  : Enabled
802.11 protocols in 2.4ghz band
    Protocol                                   : dot11bg
Advanced Scheduling Requests Handling          : Enabled
mDNS Gateway Status                            : Bridge
WIFI Alliance Agile Multiband                  : Disabled
Device Analytics
    Advertise Support                          : Enabled
    Advertise Support for PC analytics         : Enabled
    Share Data with Client                     : Disabled
Client Scan Report (11k Beacon Radio Measurement)
    Request on Association                     : Disabled
    Request on Roam                            : Disabled
WiFi to Cellular Steering                      : Disabled
Advanced Scheduling Requests Handling          : Enabled
Locally Administered Address Configuration
    Deny LAA clients                           : Disabled
```

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

```
Device# show wlan all
```

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

```
Device# show wlan summary
```

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

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

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

```
Device# show runnning-config wlan

wlan name 2 name
 no security wpa akm dot1x
 security dot1x authentication-list default
 security web-auth authentication-list default
 security web-auth parameter-map WLAN1_MAP
wlan test 24 test
 ip access-group web user_v4_acl
 radio policy dot11 24ghz
 radio policy dot11 5ghz
wlan test2 15 test2
wlan test4 12 testssid
 radio policy dot11 5ghz
  slot 1
  slot 2
wlan wlan1 234 wlan1
wlan wlan2 14 wlan-aaa
 security dot1x authentication-list realm
wlan wlan7 27 wlan7
wlan test23 17 test23
wlan wlan_1 4 ssid_name
 security dot1x authentication-list authenticate_list_name
wlan wlan_3 5 ssid_3
 security wpa wpa1
 security wpa wpa1 ciphers aes
wlan wlan_8 9 ssid_name
 no security wpa wpa2 ciphers aes
 no security wpa akm dot1x
 security web-auth
wlan test400 18 test_ssid
wlan testtest 45 ssid-test
wlan wlan-new 3 ssid-new
wlan local_ewa 67 local_ewa
 ip access-group web EWA_ACL
wlan test-wlan 23 test-wlan
wlan wlan-test 1 wlan2
 mac-filtering default
wlan wlan-test2 25 ssid-test3
wlan WLAN_LWA_LOCAL 35 WLAN_LWA_LOCAL
wlan wlan_lwa_local 34 wlan_lwa_local
 security web-auth authentication-list WIRELESS_LWA_AUTHENTICATION
```

# Verifying the RLAN Configuration

To view the summary of all RLANs, use the following command:

```
Device# show remote-lan summary

Number of RLANs: 1

RLAN        Profile Name                          Status
----------------------------------------------------------------
1            rlan_test_1                           Enabled
```

To view the RLAN configuration by ID, use the following command:

```
Device# show remote-lan id <id>

Remote-LAN Profile Name              : rlan_test_1
====================================================
Identifier                                 : 1
Status                                     : Enabled
Mac-filtering                              : Not Configured
Number of Active Clients                   : 1
Security_8021X                             : Disabled
8021.x Authentication list name            : Not Configured
Local Auth eap Profile Name                : Not Configured
Web Auth Security                          : Disabled
Webauth Authentication list name           : Not Configured
Web Auth Parameter Map                     : Not Configured
Client association limit                   : 0
Ipv4 Web Pre Auth Acl                      : Not Configured
Ipv6 Web Pre Auth Acl                      : Not Configured
```

To view the RLAN configuration by profile name, use the following command:

```
Device# show remote-lan name <profile-name>

Remote-LAN Profile Name                    : rlan_test_1
========================================================
Identifier                                 : 1
Status                                     : Enabled
Mac-filtering                              : Not Configured
Number of Active Clients                   : 1
Security_8021X                             : Disabled
8021.x Authentication list name            : Not Configured
Local Auth eap Profile Name                : Not Configured
Web Auth Security                          : Disabled
Webauth Authentication list name           : Not Configured
Web Auth Parameter Map                     : Not Configured
Client association limit                   : 0
Ipv4 Web Pre Auth Acl                      : Not Configured
Ipv6 Web Pre Auth Acl                      : Not Configured
```

To view the detailed output of all RLANs, use the following command:

```
Device# show remote-lan all

Remote-LAN Profile Name            : rlan_test_1
==================================================
Identifier                         : 1
Status                             : Enabled
Mac-filtering                      : Not Configured
Number of Active Clients           : 1
Security_8021X                     : Disabled
8021.x Authentication list name    : Not Configured
Local Auth eap Profile Name        : Not Configured
Web Auth Security                  : Disabled
Webauth Authentication list name   : Not Configured
Web Auth Parameter Map             : Not Configured
Client association limit           : 0
Ipv4 Web Pre Auth Acl              : Not Configured
Ipv6 Web Pre Auth Acl              : Not Configured

Remote-LAN Profile Name            : rlan_test_2
==================================================
Identifier                         : 2
Status                             : Enabled
Mac-filtering                      : Not Configured
Number of Active Clients           : 1
Security_8021X                     : Disabled
8021.x Authentication list name    : Not Configured
Local Auth eap Profile Name        : Not Configured
Web Auth Security                  : Disabled
Webauth Authentication list name   : Not Configured
```

```
Web Auth Parameter Map             : Not Configured
Client association limit           : 0
Ipv4 Web Pre Auth Acl              : Not Configured
Ipv6 Web Pre Auth Acl              : Not Configured
```

To view the summary of policy profile for all RLANs, use the following command:

```
Device# show remote-lan policy summary

Number of Policy Profiles: 1

Profile Name                      Description                           Status
------------------------------------------------------------------------------------------
rlan_named_pp1                 Testing RLAN policy profile              Enabled
```

To view the LAN port configuration of a Cisco AP, use the following command:

```
Device# show ap name <ap_name> lan port summary

LAN Port status for AP L2_1815w_1
Port ID      status       vlanId        poe
---------------------------------------------
LAN1         Enabled       20          Disabled
LAN2         Enabled       20          NA
LAN3         Disabled      0           NA
```

To view the summary of all clients, use the following command:

```
Device# show wireless client summary

Number of Local Clients: 1

MAC Address       AP Name        WLAN         State    Protocol    Method     Role
---------------------------------------------------------------------------------------
d8eb.97b6.fcc6    L2_1815w_1      1           * Run     Ethernet    None      Local
```

To view the client details with the specified username, use the following command:

```
Device# show wireless client username cisco

MAC Address        AP Name          Status      WLAN      Auth Protocol
------------------------------------------------------------------------------------------
0014.d1da.a977    L2_1815w_1        Run 1 *      Yes        Ethernet
d8eb.97b6.fcc6    L2_1815w_1        Run 1 *      Yes        Ethernet
```

To view the detailed information for a client by MAC address, use the following command:

```
Device# show wireless client mac-address <mac_address> detail

Client MAC Address : d8eb.97b6.fcc6
Client IPv4 Address : 10.2.20.78
Client IPv6 Addresses : 2001:DB8::1
Client Username: N/A
AP MAC Address : 707d.b99e.c2e0
AP Name: L2_1815w_1
AP slot : 2
Client State : Associated
Policy Profile : rlan_named_pp1
Flex Profile : rlan-flex-profile
Remote LAN Id : 1
Remote LAN Name: rlan_test_1
BSSID : 707d.b99e.c2e1
Connected For : 1159 seconds
```

```
Protocol : Ethernet
Channel : 0
Port ID: 2
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Client CCX version : No CCX support
Session Timeout : 1800 sec (Remaining time: 641 sec)
Input Policy Name  : None
Input Policy State : None
Input Policy Source : None
Output Policy Name  : None
Output Policy State : None
Output Policy Source : None
WMM Support : Disabled
Fastlane Support : Disabled
Power Save : OFF
Current Rate : 0.0
Mobility:
  Move Count                  : 0
  Mobility Role               : Local
  Mobility Roam Type          : None
  Mobility Complete Timestamp : 07/06/2018 11:25:26 IST
Policy Manager State: Run
NPU Fast Fast Notified : No
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 1159 seconds
Policy Type : N/A
Encryption Cipher : None
Encrypted Traffic Analytics : No
Management Frame Protection : No
Protected Management Frame - 802.11w : No
EAP Type : Not Applicable
VLAN : 20
Access VLAN : 20
Anchor VLAN : 0
WFD capable : No
Managed WFD capable : No
Cross Connection capable : No
Support Concurrent Operation : No
Session Manager:
  Interface        : capwap_90000008
  IIF ID           : 0x90000008
  Authorized       : TRUE
  Session timeout  : 1800
  Common Session ID: 32130209000000136C48A29D
  Acct Session ID  : 0x00000000
  Aaa Server Details
  Server IP        :
  Auth Method Status List
   Method : None
  Local Policies:
   Service Template : wlan_svc_rlan_named_pp1_local (priority 254)
    Absolute-Timer   : 1800
    VLAN             : 20
  Server Policies:
  Resultant Policies:
    VLAN             : 20
    Absolute-Timer   : 1800
DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 0
11v BSS Transition : Not implemented
FlexConnect Data Switching : Central
FlexConnect Dhcp Status : Central
FlexConnect Authentication : Central
FlexConnect Central Association : No
Client Statistics:
  Number of Bytes Received : 6855
  Number of Bytes Sent : 1640
  Number of Packets Received : 105
  Number of Packets Sent : 27
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : 0 dBm
  Signal to Noise Ratio : 0 dB
Fabric status : Disabled
Client Scan Reports
Assisted Roaming Neighbor List
```

To view the summary of all AP tags, use the following command:

```
Device# show ap tag summary

Number of APs: 2

AP Name             AP Mac              Site Tag Name         Policy Tag Name         RF
Tag Name           Misconfigured    Tag Source
------------------------------------------------------------------------------------------
L2_1810d_1        0008.3296.24c0       default-site-tag       default-policy-tag
default-rf-tag        No               Default
L2_1810w_2        00b0.e18c.5880       rlan-site-tag             rlan_pt_1
default-rf-tag        No               Static
```

To view the summary of all policy tags, use the following command:

```
Device# show wireless tag policy summary

Number of Policy Tags: 2

Policy Tag Name                 Description
------------------------------------------------------------------------
rlan_pt_1
default-policy-tag              default policy-tag
```

To view details of a specific policy tag, use the following command:

```
Device# show wireless tag policy detailed <rlan_policy_tag_name>

Policy Tag Name : rlan_pt_1
Description     :

Number of WLAN-POLICY maps: 0

Number of RLAN-POLICY maps: 2
REMOTE-LAN Profile Name           Policy Name                             Port Id

------------------------------------------------------------------------------------------
rlan_test_1                       rlan_named_pp1                              1
```

```
rlan_test_1                          rlan_named_pp1                                  2
```

CHAPTER 20

# Troubleshooting Common Issues

## Troubleshooting Common Issues

**Problem Client cannot connect because there is no valid VLAN defined in the Policy profile.**

**Possible Cause** There is no valid VLAN defined on the Policy profile assigned to the WLAN.

1. **Solution** Verify the Policy profile used by the client.

   - **Solution** CLI:

     ```
     Device # show wireless client mac-address <aaaa.bbbb.cccc> detail | inc Policy Profile

     Policy Profile : default-policy-profile
     ```

     **Solution** Optionally search for a specific client by using its MAC address.

   - **Solution** GUI: Navigate to **Monitoring** > **Wireless** > **Clients** > **Client row** > **Client Properties**.

     **Solution** Optionally search for a specific client by using its MAC address.

2. **Solution** Verify the VLAN that is assigned to the Policy profile.

   - **Solution** CLI:

     ```
     Device # show wireless profile policy detailed default-policy-profile | inc VLAN


     VLAN                          : VLAN2686
     ```

   - **Solution** GUI: Navigate to **Configuration** > **Tags & Profiles** > **Policy** > **Policy Profile row** > **Access Policies**.

3. **Solution** Ensure that the VLAN parameter has a VLAN name or VLAN ID that is valid and active.

   - **Solution** CLI:

     ```
     Device# show vlan brief

     VLAN Name                             Status    Ports
     ---- -------------------------------- --------- -------------------------------
     1    default                          active    Te0/0/2, Te0/0/3
     210  VLAN0210                         active
     ```

```
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
2600 VLAN2600                         active
2601 VLAN2601                         active
2602 VLAN2602                         active
2686 VLAN2686                         active
```

**Note** VLAN names are case sensitive, so ensure that the name is exactly the same as seen in the output of the **show vlan brief** command.

- **Solution** GUI: Navigate to **Configuration** > **Layer2** > **VLAN** > **VLAN**.

4. **Solution** Fix the VLAN as required.

    - **Solution** CLI:

    ```
    Device> enable
    Device# configure terminal
    Device(config)# wireless profile policy default-policy-profile
    Device(config)# shutdown
    Device(config)# vlan <vlan-# or vlan-name>
    Device(config)# no shutdown
    Device(config)# end
    Device#
    ```

    - **Solution** GUI: Navigate back to**Configuration** > **Tags & Profiles** > **Policy** > **Policy Profile row** > **Access Policies** and fix the VLAN.

**Problem Client gets disconnected due to changes in the WLAN or Policy profile**.

**Possible Cause** Changes were made in the GUI or the SSID, or the Policy profile was manually disabled.

**Solution** Normal behavior. Avoid making changes to the SSIDs or Policy profiles during production hours.

**Problem Client disconnected due to session timeout**.

**Possible Cause** Client reached its session timeout.

**Solution** Normal behavior. Increase the Policy-profile session timeout associated with the SSID.

- **Solution** CLI:

```
Device> enable
Device# configure terminal
Device(config)# wireless profile policy <policy-profile-name>
Device(config)# shutdown
Device(config)# session-timeout <20-86400 seconds>
Device(config)# no shutdown
Device(config)# end
Device#
```

- **Solution** GUI: Navigate to **Configuration > Tags & Profiles > Policy > Policy Profile Name > Advanced > WLAN Timeout**, and customize timers as needed.

**Problem Client disconnected due to Idle Timeout**.

**Possible Cause** Client did not send traffic (or enough traffic) within the configured idle timeout interval.

**Solution** Normal behavior. Customize the Policy profile idle settings associated with the SSID.

- **Solution** CLI:

```
Device> enable
Device# configure terminal
Device(config)# wireless profile policy <policy-profile-name>
Device(config)# shutdown
Device(config)# idle-timeout <15-100000 seconds>
Device(config)# idle-threshold  <0-4294967295 bytes>
Device(config)# no shutdown
Device(config)# end
Device#
```

- **Solution** GUI: Navigate to **Configuration > Tags & Profiles > Policy > Policy Profile Name > Advanced > WLAN Timeout** , and customize idle setting as needed.

**Problem Client moved between SSIDs**.

**Possible Cause** Client was connected to one SSID and moved to a different one.

**Solution** Normal behavior. Remove the second SSID from the client.

CHAPTER 21

# Additional References

## Additional References

| Related Topic | Document Title |
|---|---|
| Best Practices | Cisco Catalyst 9800 Series Configuration Best Practices |
| Day-zero deployment | FlexConnect Catalyst Wireless Branch Deployment Guide |
| Web UI deployment | Cisco Catalyst 9800 Wireless Controller Series Web UI Deployment Guide |