System Configuration

Information About New Configuration Model

The configuration of Cisco Catalyst 9800 Series Wireless Controllers is simplified using different tags, namely rf-tag, policy-tag, and site-tag. The access points would derive their configuration from the profiles that are contained within the tags.

Profiles are a collection of feature-specific attributes and parameters applied to tags. The rf-tag contains the radio profiles, the site-tag contains flex-profile and ap-join-profile, and the policy-tag contains the WLAN profile and policy profile.

The FlexConnect configuration helps the central controller to manage sites that are geo-distributed, for example, retail, campus, and so on.

Policy Tag

The policy tag constitutes mapping of the WLAN profile to the policy profile. The WLAN profile defines the wireless characteristics of the WLAN. The policy profile defines the network policies and the switching policies for the client (Quality of Service [QoS] is an exception which constitutes AP policies as well).

The policy tag contains the map of WLAN policy profile. There are 16 such entries per policy tag. Changes to the map entries are effected based on the status of the WLAN profile and policy profile. For example, if a map (WLAN1 and Policy1) is added to the policy tag, and both the WLAN profile and the policy profile are enabled, the definitions are pushed to the APs using the policy tag. However, if one of them is in 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 using the no form of the command in the policy tag.

Site Tag

The site tag defines the properties of a site and contains the flex profile and the AP join profile. The attributes that are specific to the corresponding flex or remote site are part of the flex profile. Apart from the flex profile, the site tag also comprises attributes that are specific to the physical site (and hence cannot be a part of the profile that is a reusable entity). For example, the list of primary APs for efficient upgrade is a part of a site tag rather than that of a flex profile.

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 default values (default-ap-profile and default-flex-profile).

RF Tag

The 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.

Profiles

Profiles are a collection of feature-specific attributes and parameters applied to tags. Profiles are reusable entities that can be used across tags. Profiles (used by tags) define the properties of the APs or its associated clients.

WLAN Profile

WLAN profiles are configured with same or different service set identifiers (SSIDs). An SSID identifies the specific wireless network for the controller to access. Creating WLANs with the same SSID allows to assign 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 definition.

Policy Profile

Policy profile broadly consists of network and switching policies. Policy profile is a reusable entity across tags. Anything that is a policy for a client that is applied on an AP or controller is moved to the policy profile, for example, VLAN, ACL, QoS, session timeout, idle timeout, AVC profile, bonjour profile, local profiling, device classification, BSSID QoS, and so on. However, all the wireless-related security attributes and features on the WLAN are grouped under the WLAN profile.

Flex Profile

Flex profile contains policy attributes and remote site-specific parameters. For example, the EAP profiles that can be used when the AP acts as an authentication server for local RADIUS server information, VLAN-ACL mapping, VLAN name-to-ID mapping, and so on.

AP Join Profile

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 and IPv6, UDP Lite, High Availability, Retransmit config parameters, Global AP failover, Hyperlocation config parameters, Telnet and SSH, 11u parameters, and so on.

Note Telnet is not supported for the following Cisco AP models: 1542D, 1542I, 1562D, 1562E, 1562I, 1562PS, 1800S, 1800T, 1810T, 1810W,1815M, 1815STAR, 1815TSN, 1815T, 1815W, 1832I, 1840I, 1852E, 1852I, 2802E, 2802I, 2802H, 3700C, 3800, 3802E, 3802I, 3802P, 4800, IW6300, ESW6300, 9105AXI, 9105AXW, 9115AXI, 9115AXE, 9117I, APVIRTUAL, 9120AXI, 9120AXE, 9124AXI, 9124AXD, 9130AXI, 9130AXE, 9136AXI, 9162I, 9164I, and 9166I.

RF Profile

RF profile contains the common radio configuration for the 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.

Association of APs

APs can be associated using different ways. The default option is by using Ethernet MAC address, where the MAC is associated with policy-tag, site tag, and RF tag.

In filter-based association, APs are mapped using regular expressions. A regular expression (regex) is a pattern to match against an input string. Any number of APs matching that regex will have policy-tag, site tag, and RF tag mapped to them, which is created as part of the AP filter.

In AP-based association, tag names are configured at the PnP server and the AP stores them and sends the tag name as part of discovery process.

In location-based association, tags are mapped as per location and are pushed to any AP Ethernet MAC address mapped to that location.

Modifying AP Tags

Modifying an AP tag results in DTLS connection 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 will be used for site tag and RF tag.

Configuring a Wireless Profile Policy (GUI)

Procedure

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 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.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy rr-xyz-policy-1`	Configures WLAN policy profile and enters wireless policy configuration mode.
Step 3	**idle-timeout** *timeout* **Example:** `Device(config-wireless-policy)# idle-timeout 1000`	(Optional) Configures the duration of idle timeout, in seconds.
Step 4	**vlan** *vlan-id* **Example:** `Device(config-wireless-policy)# vlan 24`	Configures VLAN name or VLAN ID.
Step 5	**accounting-list** *list-name* **Example:** `Device(config-wireless-policy)# accounting-list user1-list`	Sets the accounting list for IEEE 802.1x.
Step 6	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.
Step 7	**show wireless profile policy summary** **Example:** `Device# show wireless profile policy summary`	Displays the configured policy profiles. **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 (GUI)

Procedure

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 a Flex Profile

Follow the procedure given below to set a flex profile:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex rr-xyz-flex-profile`	Configures a Flex profile and enters Flex profile configuration mode.
Step 3	**description** **Example:** `Device(config-wireless-flex-profile)# description xyz-default-flex-profile`	(Optional) Enables default parameters for the flex profile.
Step 4	**arp-caching** **Example:** `Device(config-wireless-flex-profile)# arp-caching`	(Optional) Enables ARP caching.
Step 5	**end** **Example:** `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** **Example:** `Device# show wireless profile flex summary`	(Optional) Displays the flex-profile parameters. **Note** To view detailed parameters about the flex profile, use the **show wireless profile flex detailed** *flex-profile-name* command.

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.

Procedure

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 AP Profile (CLI)

Follow the procedure given below to configure and AP profile:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile xyz-ap-profile`	Configures an AP profile and enters AP profile configuration mode. **Note** In an AP profile, the **EAP-FAST** is the default EAP type.

	Command or Action	Purpose
		Note When you delete a named profile, the APs associated with that profile will not revert to the default profile.
Step 3	**description** *ap-profile-name* **Example:** `Device(config-ap-profile)# description "xyz ap profile"`	Adds a description for the ap profile.
Step 4	**cdp** **Example:** `Device(config-ap-profile)# cdp`	Enables CDP for all Cisco APs.
Step 5	**end** **Example:** `Device(config-ap-profile)# end`	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.
Step 6	**show ap profile name***profile-name* **detailed** **Example:** `Device# show ap profile name xyz-ap-profile detailed`	(Optional) Displays detailed information about an AP join profile.

Configuring User for AP Management (CLI)

Follow the procedure given below to configure a user for the AP management:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile default-ap-profile`	Configures an AP profile and enters AP profile configuration mode.
Step 3	**mgmtuser username <username> password {0 | 8}** *<password>* **Example:** `Device(config-ap-profile)# mgmtuser username myusername password 0 12345678`	Specifies the AP management username and password for managing all of the access points configured to the controller. • **0**: Specifies an UNENCRYPTED password. • **8**: Specifies an AES encrypted password.

	Command or Action	Purpose
		Note While configuring an username, ensure that special characters are not used as it results in error with bad configuration.
Step 4	**end** **Example:** `Device(configure-ap-profile)# end`	Returns to privileged EXEC mode.

Setting a Private Configuration Key for Password Encryption

Follow the procedure given below to set a private configuration key for password encryption:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**key config-key password encrypt** key *<config-key>* **Example:** `Device(config)# key config-key password-encrypt 12345678`	Sets the password encryption keyword. Here, *config-key* refers to any key value with minimum 8 characters. **Note** The *config-key* value must not begin with the following special characters: !, #, and ;
Step 3	**password encryption aes** **Example:** `Device(config)# password encryption aes`	Enables the encrypted preshared key.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring an RF Profile (GUI)

Procedure

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**.

Configuring an RF Profile (CLI)

Follow the procedure given below to configure an RF profile:

Before you begin

Ensure that you use the same RF profile name that you create here, when configuring the wireless RF tag too. 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.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz rf-profile** *rf-profile* **Example:** `Device(config)# ap dot11 24ghz rf-profile rfprof24_1`	Configures an RF profile and enters RF profile configuration mode. **Note** Use the **24ghz** command to configure the 802.11b parameters. Use the **5ghz** command to configure the 802.11a parameters.
Step 3	**default** **Example:** `Device(config-rf-profile)# default`	(Optional) Enables default parameters for the RF profile.

	Command or Action	Purpose
Step 4	**no shutdown** **Example:** `Device(config-rf-profile)# no shutdown`	Enables the RF profile on the device.
Step 5	**end** **Example:** `Device(config-rf-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.
Step 6	**show ap rf-profile summary** **Example:** `Device# show ap rf-profile summary`	(Optional) Displays the summary of the available RF profiles.
Step 7	**show ap rf-profile name** *rf-profile* **detail** **Example:** `Device# show ap rf-profile name rfprof24_1 detail`	(Optional) Displays detailed information about a particular RF profile.

Configuring a Site Tag (GUI)

Procedure

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 a Site Tag (CLI)

Follow the procedure given below to configure a site tag:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag site** *site-name* **Example:** `Device(config)# wireless tag site rr-xyz-site`	Configures a site tag and enters site tag configuration mode.
Step 3	**flex-profile** *flex-profile-name* **Example:** `Device(config-site-tag)# flex-profile rr-xyz-flex-profile`	Configures a flex profile. **Note** You cannot remove the flex profile configuration from a site tag if local site is configured on the site tag. **Note** The **no local-site** command needs to be used to configure the Site Tag as Flexconnect, otherwise the Flex profile config does not take effect.
Step 4	**description** *site-tag-name* **Example:** `Device(config-site-tag)# description "default site tag"`	Adds a description for the site tag.
Step 5	**end** **Example:** `Device(config-site-tag)# end`	Saves the configuration and exits configuration mode and returns to privileged EXEC mode.
Step 6	**show wireless tag site summary** **Example:** `Device# show wireless tag site summary`	(Optional) Displays the number of site tags. **Note** To view detailed information about a site, use the **show wireless tag site detailed** *site-tag-name* command. **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 Policy Tag (GUI)

Procedure

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 a Policy Tag (CLI)

Follow the procedure given below to configure a policy tag:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**wireless tag policy** *policy-tag-name* **Example:** `Device(config-policy-tag)# wireless tag policy default-policy-tag`	Configures policy tag and enters policy tag configuration mode. **Note** When performing LWA, the clients connected to a controller gets disconnected intermittently before session timeout.
Step 4	**description** *description* **Example:** `Device(config-policy-tag)# description "default-policy-tag"`	Adds a description to a policy tag.
Step 5	**remote-lan** *name* **policy** *profile-policy-name* {**ext-module**| **port-id** }	Maps a remote-LAN profile to a policy profile.

	Command or Action	Purpose
	Example: `Device(config-policy-tag)# remote-lan rr-xyz-rlan-aa policy rr-xyz-rlan-policy1 port-id 2`	
Step 6	**wlan** *wlan-name* **policy** *profile-policy-name* **Example:** `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** **Example:** `Device(config-policy-tag)# end`	Exits policy tag configuration mode, and returns to privileged EXEC mode.
Step 8	**show wireless tag policy summary** **Example:** `Device# show wireless tag policy summary`	(Optional) Displays the configured policy tags. **Note** To view detailed information about a policy tag, use the **show wireless tag policy detailed** *policy-tag-name* command.

Configuring Wireless RF Tag (GUI)

Procedure

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 Wireless RF Tag (CLI)

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

Before you begin

- You can use only two profiles (2.4-GHz and 5-GHz band RF profiles) in an RF tag.
- Ensure that you use the same AP tag name that you created when configuring the AP tag task too.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag rf** *rf-tag* **Example:** `Device(config)# wireless tag rf rftag1`	Creates an RF tag and enters wireless RF tag configuration mode.
Step 3	**24ghz-rf-policy** *rf-policy* **Example:** `Device(config-wireless-rf-tag)# 24ghz-rf-policy rfprof24_1`	Attaches an IEEE 802.11b RF policy to the RF tag. To configure a dot11a policy, use the **5ghz-rf-policy** command.
Step 4	**description** *policy-description* **Example:** `Device(config-wireless-rf-tag)# description Test`	Adds a description for the RF tag.
Step 5	**end** **Example:** `Device(config-wireless-rf-tag)# end`	Exits configuration mode and returns to privileged EXEC mode.
Step 6	**show wireless tag rf summary** **Example:** `Device# show wireless tag rf summary`	Displays the available RF tags.
Step 7	**show wireless tag rf detailed** *rf-tag* **Example:** `Device# show wireless tag rf detailed rftag1`	Displays detailed information of a particular RF tag.

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

Procedure

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**.

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:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap** *mac-address* **Example:** `Device(config)# ap F866.F267.7DFB`	Configures a Cisco AP and enters AP profile configuration mode. **Note** The *mac-address* should be a wired mac address.
Step 3	**policy-tag** *policy-tag-name* **Example:** `Device(config-ap-tag)# policy-tag rr-xyz-policy-tag`	Maps a policy tag to the AP.
Step 4	**site-tag** *site-tag-name* **Example:** `Device(config-ap-tag)# site-tag rr-xyz-site`	Maps a site tag to the AP.
Step 5	**rf-tag** *rf-tag-name* **Example:** `Device(config-ap-tag)# rf-tag rf-tag1`	Associates the RF tag.
Step 6	**end** **Example:** `Device(config-ap-tag)# end`	Saves the configuration, exits configuration mode, and returns to privileged EXEC mode.
Step 7	**show ap tag summary** **Example:** `Device# show ap tag summary`	(Optional) Displays AP details and the tags associated to it.
Step 8	**show ap name** <*ap-name*> **tag info** **Example:**	(Optional) Displays the AP name with tag information.

	Command or Action	Purpose
	`Device# show ap name ap-name tag info`	
Step 9	**show ap name** <*ap-name*> **tag detail** **Example:** `Device# show ap name ap-name tag detail`	(Optional) Displays the AP name with tag details.

AP Filter

Introduction to AP Filter

The introduction of tags in the new configuration model in the Cisco Catalyst 9800 Series Wireless Controller has created multiple sources for tags to be associated with access points (APs). Tag sources can be static configuration, AP filter engine, per-AP PNP, or default tag sources. In addition to this, the precedence of the tags also plays an important role. The AP filter feature addresses these challenges in a seamless and intuitive manner.

AP filters are similar to the access control lists (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. 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 PnP server (similar to the Flex group and AP group) and the AP stores and send the tag name as part of discovery and join requests.

Set Tag Priority (GUI)

Procedure

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

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

Set Tag Priority

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 picked based on priority. If precedence is not set, the defaults are used.

Use the following procedure to set tag priority:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**ap tag-source-priority** *source-priority* **source {filter | pnp}** **Example:** `Device(config)# ap tag-source-priority 2 source pnp`	Configures AP tag source priority. **Note** It is not mandatory to configure AP filter. It comes with default priorities for Static, Filter, and PnP.
Step 3	**end** **Example:** `Device(config)# end`	Exits configuration mode and returns to privileged EXEC mode.
Step 4	**ap tag-sources revalidate** **Example:** `Device# ap tag-sources revalidate`	Revalidates AP tag sources. The priorities become active only after this command is run. **Note** If you change the priorities for Filter and PnP, and want to evaluate them, run the **revalidate** command.

Create an AP Filter (GUI)

Procedure

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**.

Create an AP Filter (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**ap filter name** *filter_name* **Example:** `Device(config)# ap filter filter-1`	Configures an AP filter.
Step 3	**ap name-regex** *regular-expression* **Example:** `Device(config-ap-filter)# ap name-regex testany`	Configures the AP filter based on regular expression. For example, if you have named an AP as **`ap-lab-12`**, then you can configure the filter with a regular expression, such as **`ap-lab-\d+`** , to match the AP name.
Step 4	**tag policy** *policy-tag* **Example:** `Device(config-ap-filter)# tag policy pol-tag1`	Configures a policy tag for this filter.
Step 5	**tag rf** *rf-tag* **Example:** `Device(config-ap-filter)# tag rf rf-tag1`	Configures an RF tag for this filter.
Step 6	**tag site** *site-tag* **Example:** `Device(config-ap-filter)# tag site site1`	Configures a site tag for this filter.
Step 7	**end** **Example:** `Device(config-ap-filter)# end`	Exits configuration mode and returns to privileged EXEC mode.

Set Up and Update Filter Priority (GUI)

Procedure

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**.

Set Up and Update Filter Priority

Follow the procedure given below to set and update filter priority:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap filter priority** *priority* **filter-name** *filter-name* **Example:** `Device(config)# ap filter priority 10 filter-name test1`	Configure AP filter priority. Valid values range from 0 to 1023; 0 is the highest priority. **Note** A filter without a priority is not active. Similarly, you cannot set a filter priority without a filter.
Step 3	**end** **Example:** `Device(config-ap)# end`	Exits configuration mode and returns to privileged EXEC mode.

Verify 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
```

Configuring Access Point for Location Configuration

Information About Location Configuration

During location configuration, you can perform the following:

- Configure a site or location for an AP.
- Configure a set of tags for this location.
- Add APs to this location.

Any location comprises of the following components:

- A set of unique tags, one for each kind, namely: Policy, RF and Site.
- A set of ethernet MAC addresses that applies to the tags.

This feature works in conjunction with the existing tag resolution scheme. The location is considered as a new tag source to the existing system. Similar, to the static tag source.

Prerequisite for Location Configuration

If you configure an access point in one location, you cannot configure the same access point in another location.

Configuring a Location for an Access Point (GUI)

Before you begin

Note When you create local and remote sites in the Basic Setup workflow, corresponding policies and tags are created in the backend. These tags and policies that are created in the Basic Setup cannot be modified using the Advanced workflow, and vice versa.

Procedure

Step 1 Choose **Configuration** > **Wireless Setup** > **Basic**.

Step 2 On the **Basic Wireless Setup** page, click **Add**.

Step 3 In the **General** tab, enter a name and description for the location.

Step 4 Set the **Location Type** as either *Local* or *Flex*.

Step 5 Use the slider to set **Client Density** as *Low*, *Typical* or *High*.

Step 6 Click **Apply**.

Configuring a Location for an Access Point (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap location name** *location_name* **Example:** `Device(config)# ap location name location1`	Configures a location for an access point. Run the **no** form of this command to remove location for an access point.
Step 3	**tag** {**policy** *policy_name*| **rf** *rf_name* | **site** **site_name**} **Example:** `Device(config-ap-location)# tag policy policy_tag`	Configures tags for the location.

	Command or Action	Purpose
	`Device(config-ap-location)# tag rf rf_tag` `Device(config-ap-location)# tag site site_tag`	
Step 4	**location** *description* **Example:** `Device(config-ap-location)# location description`	Adds description to the location.
Step 5	**end** **Example:** `Device(config-ap-location)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Adding an Access Point to the Location (GUI)

Note When the tag source is not set to location, the AP count and AP location tagging will not be correctly reflected on the web UI. To change static tag source on the AP, run the **no ap** *ap-mac* command on the controller to change AP tag source to default (which is location).

Procedure

Step 1 Choose **Configuration** > **Wireless Setup** > **Basic**.

Step 2 On the **Basic Wireless Setup** page, click **Add** to configure the following:

- General
- Wireless Networks
- AP Provisioning

Step 3 In the **AP Provisioning** tab and **Add/Select APs** section, enter the AP MAC address and click the right arrow to add the AP to the associated list.

You can also add a CSV file from your system. Ensure that the CSV has the MAC Address column.

Step 4 Use the search option in the **Available AP List** to select the APs from the Selected AP list and click the right arrow to add the AP to the associated list.

Step 5 Click **Apply**.

Adding an Access Point to the Location (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap location name** *location_name* **Example:** `Device(config)# ap location name location1`	Configures a location for an access point.
Step 3	**ap-eth-mac** *ap_ethernet_mac* **Example:** `Device(config-ap-location)# ap-eth-mac 188b.9dbe.6eac`	Adds an access point to the location.
Step 4	**end** **Example:** `Device(config-ap-location)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode. **Note** After adding an AP to a location, the AP may reset automatically to get the new configuration

Configuring SNMP in Location Configuration

SNMP MIB

The SNMP MIB provides information on a set of managed objects that represent logical and physical entities, and relationships between them.

Table 1: MIB Objects and Notes

MIB Objects	Notes
cLApLocationName	Provides the name of the AP location.
cLApLocationPolicyTag	Provides the policy tag configured on the location.
cLApLocationSitetag	Provides the site tag configured on the location.
cLApLocationRfTag	Provides the RF tag configured on the location.
cLAssociatedApsApMac	Provides the configured APs on the location.

Verifying Location Configuration

To view the summary of AP location configuration, use the following command:

```
Device# show ap location summary

Location Name    Description     Policy Tag           RF Tag           Site Tag
-------------------------------------------------------------------------------------------
first            first floor     default-policy-tag   default-rf-tag   default-site-tag
second           second floor    default-policy-tag   default-rf-tag   default-site-tag
```

To view the AP location configuration details for a specific location, use the following command:

```
Device# show ap location details first

Location Name.....................: first
Location description..............: first floor
Policy tag........................: default-policy-tag
Site tag..........................: default-site-tag
RF tag............................: default-rf-tag

Configured list of APs
005b.3400.0af0
005b.3400.0bf0
```

To view the AP tag summary, 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
-------------------------------------------------------------------------------------------------------
Asim_5-1     005b.3400.02f0   default-site-tag   default-policy-tag   default-rf-tag   Yes
             Filter
Asim_5-2     005b.3400.03f0   default-site-tag   default-policy-tag   default-rf-tag   No
             Default
Asim_5-9     005b.3400.0af0   default-site-tag   default-policy-tag   default-rf-tag   No
             Location
Asim_5-10    005b.3400.0bf0   default-site-tag   default-policy-tag   default-rf-tag   No
             Location
```

Verifying Location Statistics

To view the AP location statistics, use the following command:

```
Device# show ap location stats

Location name    APs joined     Clients joined     Clients on 11a     Clients on 11b
-------------------------------------------------------------------------------------------
first             2             0                   3                  4
second            0             0                   0                  0
```