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** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
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	**no shutdown** **Example:** `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** **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 (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** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile* **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** **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 (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** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile xyz-ap-profile`	Configures an AP profile and enters AP profile configuration mode. **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* **Example:** `Device(config-ap-profile)# description "xyz ap profile"`	Adds a description for the AP profile.
Step 5	**accounting method-list***method-list-name* **Example:** `Device(config-ap-profile)# accounting method-list accounting-list1`	Configures an accounting method-list.
Step 6	**antenna monitoring** **Example:** `Device(config-ap-profile)# antenna monitoring`	Configures detection of broken AP antennas.
Step 7	**apphost** **Example:** `Device(config-ap-profile)# apphost`	Enables the application hosting framework on Cisco APs.
Step 8	**auxiliary-client interface vlan** *vlan-ID* **Example:** `Device(config-ap-profile)# auxiliary-client interface vlan vlan1`	Configures the auxiliary-client interface VLAN.
Step 9	**awips forensic** **Example:** `Device(config-ap-profile)# awips forensic`	Enables Adaptive Wireless Intrusion Prevention System (wIPS).
Step 10	**bssid-neighbor-stats interval** *interval* **Example:** `Device(config-ap-profile)# bssid-neighbor-stats interval 23`	Configures the interval at which BSSID neighbor statistics is sent from the AP. • BSSID is the MAC address of the wireless access point.
Step 11	**bssid-stats bssid-stats-frequency** *seconds* **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**} **Example:** `Device(config-ap-profile)# capwap fallback`	Sets the Control and Provisioning of Wireless Access Points Protocol (CAPWAP) parameters.
Step 13	**capwap-discovery** {**private** | **public**} **Example:** `Device(config-ap-profile)# capwap-discovery private`	Configures the CAPWAP discovery response. • Based on the configured parameters, either private IP addresses or public IP addresses are inclued in the discovery.
Step 14	**cdp** **Example:** `Device(config-ap-profile)# cdp`	Configures Cisco Discovery Protocol.
Step 15	**cisco-dna grpc** **Example:** `Device(config-ap-profile)# cisco-dna grpc`	Enables the GRPC channel to Cisco DNA.
Step 16	**client-rssi-stats interval** *interval* **Example:** `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**} **Example:** `Device(config-ap-profile)# core-dump tftp-server 2001:db8::2 filename file1 compress`	Enables core dump of the memory.
Step 18	**dhcp-server** **Example:** `Device(config-ap-profile)# dhcp-server`	Configures a DHCP server.
Step 19	**dot11** {**24ghz** | **5ghz**} **reporting-interval** *interval* **Example:** `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**} **Example:** `Device(config-ap-profile)# dot1x max-sessions 30`	Configures IEEE 802.1X credentials for all APs .

	Command or Action	Purpose
Step 21	**ext-module** **Example:** `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* **Example:** `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** **Example:** `Device(config-ap-profile)# hyperlocation`	Configures the hyperlocation feature on all supported APs.
Step 24	**icap subscription ap rf spectrum enable** **Example:** `Device(config-ap-profile)# icap subscription ap rf spectrum enable`	Configures the radio frequency spectrum subscription.
Step 25	**ip dhcp fallback** **Example:** `Device(config-ap-profile)# ip dhcp fallback`	Configures DHCP fallback. **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** **Example:** `Device(config-ap-profile)# jumbo-mtu`	Enables jumbo maximum transmission unit (MTU) status.
Step 27	**lag** **Example:** `Device(config-ap-profile)# lag`	Enables CAPWAP lag for Cisco APs.
Step 28	**ledflash** {**duration** *duration* | **indefinite**} **Example:** `Device(config-ap-profile)# ledflash indefinite`	Enables LED-state for all Cisco APs.
Step 29	**link-encryption** **Example:** `Device(config-ap-profile)# link-encryption`	Enables the link encryption state on all Cisco APs.
Step 30	**link-latency** **Example:**	Enables link latency on all Cisco APs.

	Command or Action	Purpose
	`Device(config-ap-profile)# link-latency`	
Step 31	**mesh-profile** *name* **Example:** `Device(config-ap-profile)# mesh-profile mesh1`	Configures the mesh profile.
Step 32	**mgmtuser username** *username* **password** {**0** | **8**} *password***secret** {**0** | **8** } *secret* **Example:** `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* } **Example:** `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**} **Example:** `Device(config-ap-profile)# oeap link-encryption`	Enables link encryption for Cisco OfficeExtend access points (OEAPs).
Step 35	**packet-capture** *profile-name* **Example:** `Device(config-ap-profile)# packet-capture pcap1`	Configures a profile for packet capturing.
Step 36	**pakseq-jump-delba** **Example:** `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**} **Example:** `Device(config-ap-profile)# power pre-standard`	Enables the power over Ethernet (PoE) switch state.
Step 38	**preferred-mode** {**disable** | **ipv4** | **ipv6**} **Example:** `Device(config-ap-profile)# preferred-mode disable`	Disables preferred-mode.
Step 39	**qos-map action-frame** **Example:** `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* **Example:** `Device(config-ap-profile)# rogue detection report-interval 100`	Configures rogue-detection report-interval for monitor mode.

	Command or Action	Purpose
Step 41	**ssh** **Example:** `Device(config-ap-profile)# ssh`	Enables SSH, if the AP user management credentials are nondefault.
Step 42	**ssid broadcast persistent** **Example:** `Device(config-ap-profile)# ssid broadcast persistent`	Enables persistent Service Set Identifier (SSID) broadcast on the profile.
Step 43	**statistics traffic-distribution interval** *interval* **Example:** `Device(config-ap-profile)# statistics traffic-distribution interval 90`	Enables traffic distribution statistics.
Step 44	**stats-timer** *duration* **Example:** `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** } **Example:** `Device(config-ap-profile)# syslog level critical`	Configures the system error message logging settings.
Step 46	**tcp-adjust-mss** {**enable** | **size** *mss-value* **Example:** `Device(config-ap-profile)# tcp-adjust-mss enable`	Enables the TCP maximum segment size configuration for all Cisco APs.
Step 47	**telnet** **Example:** `Device(config-ap-profile)# telnet`	Enables Telnet, if the AP user management credentials are nondefault.
Step 48	**trace** *profile-name* **Example:** `Device(config-ap-profile)# trace trace-profile`	Configures the AP trace profile.
Step 49	**usb-enable** **Example:** `Device(config-ap-profile)# usb-enable`	Enables USBs for Cisco APs.
Step 50	**end** **Example:** `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** **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: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**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.
Step 4	**default** **Example:** `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**} **Example:** `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*} **Example:** `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*} **Example:** `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**} **Example:** `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*} **Example:** `Device(config-rf-profile)# coverage exception 90`	Sets the Cisco AP coverage exception level.

	Command or Action	Purpose
Step 10	**description** *description* **Example:** `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*] **Example:** `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**} **Example:** `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*] **Example:** `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* } **Example:** `Device(config-rf-profile)# load-balancing window 12`	Sets the aggressive load-balancing client window.
Step 15	**ndp-mode** {**auto** | **off-channel**} **Example:** `Device(config-rf-profile)# ndp-mode auto`	Enables Neighbor Discovery Protocol (NDP) auto mode.
Step 16	**rate** {*options* {**disable** | **mandatory** | **supported** } | **mcs** *index-number*} **Example:** `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* **Example:** `Device(config-rf-profile)# trap theshold noise -90`	Configures the trap threshold for noise.
Step 18	**tx-power** {**max** | **min** | **v1 threshold** } *threshold* **Example:** `Device(config-rf-profile)# tx-power min 12`	Configures the minimum auto-RF transmit power.

	Command or Action	Purpose
Step 19	**no shutdown** **Example:** `Device(config-rf-profile)# no shutdown`	Enables the RF profile on the device.
Step 20	**end** **Example:** `Device(config-rf-profile)# end`	Exits RF profile configuration mode and returns to privileged EXEC mode.
Step 21	**show ap rf-profile summary** **Example:** `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** **Example:** `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**.