



# AP Management

---

- [AP Crash File Upload, on page 2](#)
- [Configuring AP Crash File Upload \(CLI\), on page 3](#)
- [Information About LED States for Access Points, on page 3](#)
- [Configuring LED State in Access Points \(GUI\), on page 4](#)
- [Configuring LED State for Access Points in the Global Configuration Mode \(CLI\), on page 4](#)
- [Configuring LED State in the AP Profile, on page 5](#)
- [Verifying LED State for Access Points, on page 5](#)
- [Access Point Support Bundle, on page 6](#)
- [Exporting an AP Support Bundle \(GUI\), on page 6](#)
- [Exporting an AP Support Bundle \(CLI\), on page 7](#)
- [Monitoring the Status of Support Bundle Export, on page 7](#)
- [Information About Access Point Memory Information, on page 7](#)
- [Verifying Access Point Memory Information, on page 8](#)
- [Information About Access Point Tag Persistency, on page 8](#)
- [Configuring AP Tag Persistency \(GUI\), on page 8](#)
- [Configuring AP Tag Persistency \(CLI\), on page 9](#)
- [Verifying AP Tag Persistency, on page 10](#)
- [Feature History for AP Power Save, on page 11](#)
- [Information About AP Power Save, on page 11](#)
- [Wakeup Threshold for Access Point Power Save Mode, on page 19](#)
- [AP Power Save Scenarios, on page 19](#)
- [Configuring Power Policy Profile \(GUI\), on page 21](#)
- [Configuring a Power Policy Profile \(CLI\), on page 21](#)
- [Configuring a Calendar Profile \(GUI\), on page 24](#)
- [Configuring a Calendar Profile \(CLI\), on page 25](#)
- [Configuring a Power Policy in an AP Join Profile \(GUI\), on page 26](#)
- [Mapping a Power Profile Under an AP Profile \(CLI\), on page 26](#)
- [Configuring Client Wakeup Threshold \(CLI\), on page 27](#)
- [Configuring PoE-Out Interface in Power Profile \(GUI\), on page 27](#)
- [Configuring PoE-Out Interface in Power Profile \(CLI\), on page 28](#)
- [Configuration Example of Power Profile, on page 29](#)
- [Verifying Access Point Power Policy \(GUI\), on page 29](#)
- [Verifying the Access Point Power Profile, on page 30](#)

- [Verifying Radio Spatial Streams, on page 31](#)
- [Verifying Client Threshold, on page 31](#)
- [Verifying PoE-Out Details, on page 32](#)
- [Information About Access Point Real-Time Statistics, on page 32](#)
- [Feature History for Real Time Access Point Statistics, on page 32](#)
- [Restrictions for AP Radio Monitoring Statistics , on page 33](#)
- [Configuring Access Point Real Time Statistics \(GUI\), on page 33](#)
- [Configuring Real-Time Access Point Statistics \(CLI\), on page 34](#)
- [Configuring AP Radio Monitoring Statistics, on page 36](#)
- [Monitoring Access Point Real-Time Statistics \(GUI\), on page 37](#)
- [Verifying Access Point Real-Time Statistics, on page 38](#)
- [Feature History for Access Point Auto Location Support, on page 38](#)
- [Information About Access Point Auto Location Support, on page 39](#)
- [Configuring Access Point Geolocation Derivation Using Ranging \(GUI\) , on page 40](#)
- [Configuring Access Point Geolocation Derivation Using Ranging \(CLI\), on page 41](#)
- [Configuring Access Point Ranging Parameters \(GUI\), on page 41](#)
- [Configuring Access Point Ranging Parameters \(CLI\), on page 42](#)
- [Configuring Access Point Coordinates and Floor Information \(CLI\), on page 42](#)
- [Configuring On-Demand Access Point Ranging \(CLI\), on page 43](#)
- [Enabling Fine Time Measurement \(802.11mc\) Responder \(GUI\), on page 44](#)
- [Configuring Fine Time Measurement \(802.11mc\) Responder \(CLI\), on page 44](#)
- [Configuring Air Pressure Reporting \(CLI\), on page 45](#)
- [Verifying Access Point Geolocation Information, on page 45](#)

## AP Crash File Upload

When a converted access point unexpectedly reboots, the access point stores a crash file on its local flash memory at the time of the crash. After the unit reboots, it sends the reason for the reboot to the device. If the unit rebooted because of a crash, the device pulls up the crash file using the existing CAPWAP messages and stores it in the device flash memory. The crash information copy is removed from the access point's flash memory when the device pulls it from the access point:




---

**Note** The system does not generate reports in case of a reload.

---

During a process crash, the following are collected locally from the device:

- Full process core
- Trace logs
- Cisco IOS syslogs (not guaranteed in case of nonactive crashes)
- System process information
- Bootup logs
- Reload logs

- Certain types of proc information

All this information is stored in separate files, which are then archived and compressed into one bundle. This makes it convenient to get a crash snapshot in one place, and can be then moved off the box for analysis. This report is generated before the device goes down to ROMMON/bootloader.



**Note** Except for the full core and tracelogs, everything else is a text file.

## Configuring AP Crash File Upload (CLI)

### Procedure

- |               |  |
|---------------|--|
| <b>Step 1</b> | <b>enable</b><br>Enters privileged EXEC mode.  |
| <b>Step 2</b> | <b>ap name <i>ap-name</i> crash-file get-crash-data</b><br>Collects AP crash information. The crash file is uploaded automatically after the AP reloads to ready state. Therefore, this command does not have to be manually executed. |
| <b>Step 3</b> | <b>ap name <i>ap-name</i> crash-file get-radio-core-dump slot {0   1}</b><br>Collects the AP core dump file for slot 0 or slot 1.  |
| <b>Step 4</b> | <b>ap name <i>ap-name</i> core-dump <i>tftp-ip crash-file</i> uncompress</b><br>Uploads the AP crash coredump file to the given TFTP location.   |
| <b>Step 5</b> | <b>show ap crash-file</b><br>Displays the AP crash file, as well as the radio crash file.  |
| <b>Step 6</b> | <b>dir bootflash</b><br>Displays the crash file in bootflash with .crash extension.  |

## Information About LED States for Access Points

In a wireless LAN network where there are a large number of access points, it is difficult to locate a specific access point associated with the controller. You can configure the controller to set the LED state of an access point so that it blinks and the access point can be located. This configuration can be done in the wireless network on a global as well as per-AP level.

The LED state configuration at the global level takes precedence over the AP level.



**Note** For APs that have Ethernet LEDs in addition to the main system LED, the Ethernet LEDs are enabled or disabled (switched ON or OFF) as per the system LED. For example, if the system LED is ON, the Ethernet LED will also be ON.

## Configuring LED State in Access Points (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Wireless > Access Points**.
- Step 2** Click an AP from the AP list.  
The **Edit AP** window is displayed.
- Step 3** In the **General** tab, under the General section, go to **LED Settings**.
- Click the box adjacent to the **LED State** field to enable or disable the LED state.
  - From the **LED Brightness Level** drop-down list, choose a value from 1 to 8.
- Step 4** Under the **Flash Settings** section, perform the following steps:
- Click the box adjacent to the **Flash State** field to enable or disable the flash state.  
When the flash state is enabled, the current status of the flash and the flash duration fields are displayed.
  - From the **Flash Duration** drop-down list, choose either **Always ON** or **Timed**.  
If you choose the **Timed** option, the **Time Duration** field is displayed.
  - In the **Time Duration** field, specify the flash duration time, in seconds. The default value is one second.  
The valid range is between 1 second and 3600 seconds.
- Step 5** Click **Update & Apply to Device**.
- 

## Configuring LED State for Access Points in the Global Configuration Mode (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>ap name <i>Cisco-AP-name</i> led</b>  <b>Example:</b> Device# ap name <i>Cisco-AP-name</i> led	Enables the LED state for Cisco APs, globally.

	Command or Action	Purpose
<b>Step 3</b>	<b>ap name <i>Cisco-AP-name</i> led flash {start duration <i>duration</i>   stop}</b>  <b>Example:</b> <pre>Device# ap name Cisco-AP-name led flash start duration 20  Device# ap name Cisco-AP-name led flash stop</pre>	Configures the starting and the stopping of the AP LED flash. The valid start duration range is between 0 and 3600 seconds.
<b>Step 4</b>	<b>ap name <i>Cisco-AP-name</i> led-brightness-level 1-8</b>  <b>Example:</b> <pre>Device# ap name Cisco-AP-name led-brightness-level 4</pre>	Configures the LED brightness level. Value of the brightness is from 1 to 8.

## Configuring LED State in the AP Profile

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <pre>Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>ap profile <i>default-ap-profile</i></b>  <b>Example:</b> <pre>Device(config)#ap profile default-ap-profile</pre>	Enters the AP profile configuration mode.
<b>Step 3</b>	<b>led</b>  <b>Example:</b> <pre>Device(config-ap-profile)# led</pre>	Enables the LED-state for all Cisco APs.

## Verifying LED State for Access Points

To verify the LED state of the access points, use the following command:

**show ap name *AXXX-APXXXX.bdXX.f2XX* config general**

```
Device# show ap name XXXX-APXXXX.bdXX.f2XX config general
Cisco AP Name : XXXX-APXXXX.bdXX.f2XX
=====
Cisco AP Identifier : 0cXX.bdXX.65XX
Country Code : Multiple Countries : FR,IN,US
Regulatory Domain Allowed by Country : 802.11bg:-AE 802.11a:-ABDEN
AP Country Code : US - United States
```

```

AP Regulatory Domain
802.11bg : -A
802.11a : -B
.
.
.
CAPWAP Preferred mode : IPv4
CAPWAP UDP-Lite : Not Configured
AP Submode : WIPS
Office Extend Mode : Disabled
Dhcp Server : Disabled
Remote AP Debug : Disabled
Logging Trap Severity Level : information
Logging Syslog facility : kern
Software Version : 17.X.0.XXX
Boot Version : 1.1.X.X
Mini IOS Version : 0.0.0.0
Stats Reporting Period : 180
LED State : Enabled
MDNS Group Id : 0
.
.
.

```

## Access Point Support Bundle

An access point (AP) support bundle contains core files, crash files, **show run-configuration**, configuration commands, msglogs, and traplogs.

This topic describes how you can retrieve the support bundle information of an AP and export it to the controller or to an external server. (Until Cisco IOS XE, Release 17.2.1, you had to log in to the AP console to retrieve the AP support-bundle information.)

The Access Point Support Bundle feature is supported only on Cisco Wave2 APs and Cisco Catalyst APs.

## Exporting an AP Support Bundle (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Wireless > Access Points**.
- Step 2** Click the corresponding AP name.  
The **Edit AP** window is displayed.
- Step 3** Click the **Support Bundle** tab.
- Step 4** From the **Destination** drop-down list, choose one of the following:
- **This Device**: If you choose this, enter the values for the **Server IP**, **Destination File Path**, **Username**, and **Password** fields.
- Note** When you choose **This Device**, a bundle is sent through Secure Copy (SCP) to the controller (if you have configured the **ip scp server enable** command globally on the controller). You can easily retrieve the bundle later from your browser, using the controller file manager.

- **External Server:** If you choose this, from the **Transfer Mode** drop-down list, choose either **scp** or **tftp**.

If you choose the **scp** transfer mode, enter the values for the **Server IP**, **Destination File Path**, **Username**, and **Password** fields.

If you choose the **tftp** transfer mode, enter the values for the **Server IP**, and **Destination File Path** fields.

**Note** Information about the **Last Export Status**, such as **State**, **Transfer Mode**, **Server IP**, **File Path**, and **Time of Export**, is displayed on the right-hand side of the window.

**Step 5** Click **Start Transfer**.

## Exporting an AP Support Bundle (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. Enter your password, if prompted.
<b>Step 2</b>	<b>ap name</b> <i>Cisco-AP-name</i> <b>export</b> <b>support-bundle mode</b> { <b>scp</b>   <b>tftp</b> } <b>target</b> <b>ip-address</b> { <i>A.B.C.D</i>   <i>X:X:X:X::X</i> } <b>path</b> <i>file-path</i>  <b>Example:</b> Device> ap name <i>Cisco-AP-name</i> export support-bundle mode scp target ip-address 10.1.1.1 path <i>file-path</i>	Exports the AP support bundle through the SCP or TFTP transfer modes.  If you select the <b>scp</b> , you will be prompted to provide your username and password.  For <b>tftp</b> , username and password is not required.

## Monitoring the Status of Support Bundle Export

To monitor the status of a support bundle export, run the following command:

```
Device# show ap support-bundle summary
```

AP Name	Server-IP	Status	Last Successful Time	Path	File-name
---------	-----------	--------	----------------------	------	-----------

AP_28XXX	81.1.1.10	Copy Success	04/24/2020 07:27:38 UTC		
AP_28XXX_support.17.4.0.2.2020.07XXXX.tgz					

## Information About Access Point Memory Information

With the introduction of the Access Point Memory Information feature, you can view the access point (AP) memory type, the CPU type, and the memory size per AP, after single sign-on authentication. APs share the memory information with the controller during the join phase.

To view the memory information of a specific AP, use the **show ap name AP-NAME config general** command.

## Verifying Access Point Memory Information

To verify the memory information of a specified AP, including the CPU type, memory type and memory size, use the following command:

```
Device# show ap name AP-NAME config general
Cisco AP Name      : AP-NAME
=====
Cisco AP Identifier                : 00XX.f1XX.e0XX
Country Code                     : Multiple Countries : FR,IN,US
Regulatory Domain Allowed by Country : 802.11bg:-AE 802.11a:-ABDEN
AP Country Code                  : US - United States
AP Regulatory Domain
    802.11bg                      : -A
    802.11a                      : -B
.
.
.
CPU Type                         : ARMv7 Processor rev 1 (v7l)
Memory Type                     : DDR4
Memory Size                     : 1028096 KB
.
.
.
```

## Information About Access Point Tag Persistency

From Cisco IOS XE Bengaluru 17.6.1 onwards, AP tag persistency is enabled globally on the controller. When APs join a controller with tag persistency enabled, the mapped tags are saved on the APs without having to write the tag configurations on each AP, individually.

## Configuring AP Tag Persistency (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > Tags**.
  - Step 2** Click the **AP** tab.
  - Step 3** In the **Tag Source** tab, check the **Enable AP Tag Persistency** check box to configure AP Tag persistency globally.  
  
When APs join a controller with the tag persistency enabled, the mapped tags are saved on the AP without having to write the tag configurations on each AP individually.
  - Step 4** Click **Apply to Device**.
-



**What to do next**

Save tags on an AP.

## Saving Tags on an Access Point (GUI)

**Procedure**

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Choose <b>Configuration &gt; Wireless &gt; Access Points</b> .   |
| <b>Step 2</b> | Click an AP from the list.<br>The <b>Edit AP</b> page is displayed.  |
| <b>Step 3</b> | Click the <b>General</b> tab.  |
| <b>Step 4</b> | In the <b>Tags</b> section, specify the appropriate policy, site, and RF tags that you created in the <b>Configuration &gt; Tags &amp; Profiles &gt; Tags</b> page.                          |
| <b>Step 5</b> | From the <b>Policy</b> drop-down list, select a value.   |
| <b>Step 6</b> | From the <b>Site</b> drop-down list, select a value.   |
| <b>Step 7</b> | From the <b>RF</b> drop-down list, select a value.   |
| <b>Step 8</b> | Check the <b>Write Tag Config to AP</b> check box to push the tags to the AP so that the AP can save and remember this information even when the AP is moved from one controller to another. |
| <b>Step 9</b> | Click <b>Update &amp; Apply to Device</b> .  |
- 

## Deleting Saved Tags on the Access Point

**Procedure**

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Choose <b>Configuration &gt; Wireless &gt; Access Points</b> .   |
| <b>Step 2</b> | Click an AP from the list of APs.<br>The <b>Edit AP</b> window is displayed.   |
| <b>Step 3</b> | In the <b>Edit AP</b> window, choose the <b>Advanced</b> tab.  |
| <b>Step 4</b> | In the <b>Set to Factory Default</b> section, check the <b>Clear Resolved Tag Config</b> check box to clear the saved tags on an AP. |
| <b>Step 5</b> | Click <b>Update &amp; Apply to Device</b> .  |
- 

## Configuring AP Tag Persistency (CLI)

**Before you begin**

For an AP to preserve its policy tag, site tag, and RF tag configured from the primary controller, these tags must also exist on the other controllers that the AP connect to. If all the three tags do not exist, the AP applies

the default policy tag, site tag, and RF tag. Similarly, the tag policy is applicable even if one or two tags exist. AP tag persistency helps in priming an AP in N+1 redundancy scenarios. For more information about configuring tags, see [https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-6/config-guide/b\\_wl\\_17\\_6\\_cg/m\\_config\\_model.html](https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-6/config-guide/b_wl_17_6_cg/m_config_model.html).



**Note** After being enabled, AP tag persistency is performed during AP join. Therefore, if there are any APs that are already joined to the controller, those APs must rejoin the controller.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>ap tag persistency enable</b>  <b>Example:</b> Device(config)# ap tag persistency enable	Configures AP tag persistency.
<b>Step 3</b>	<b>end</b>  <b>Example:</b> Device(config)# end	Exits configuration mode and returns to privileged EXEC mode.

## Verifying AP Tag Persistency

To verify AP tag persistency in the primary controller, use the following command:

```
Device# show ap tag summary
Number of APs: 1
```

AP Name	AP Mac	Site Tag Name	Policy Tag Name	RF Tag Name
	Misconfigured	Tag Source		
Cisco01_AP	xxxx.xxxx.xxxx	default-site-tag	OpenRoaming	default-rf-tag
No		Static		



**Note** If the Tag Source displays **Static** or **Filter**, it means that the AP tag mappings were configured on the primary controller. If the source displays **Default**, it means that the AP received the default tags when joining the controller.

To verify the AP tag persistency in the secondary controller, use the following command:

```
Device# show ap tag summary
Number of APs: 1
```

AP Name	AP Mac	Site Tag Name	Policy Tag Name	RF Tag Name
---------	--------	---------------	-----------------	-------------

Misconfigured      Tag Source

Cisco01\_AP      xxxx.xxxx.xxxx      default-site-tag      OpenRoaming      default-rf-tag  
No                      AP



**Note** If the Tag Source displays **AP**, it means that the policy tag, site tag, and RF tag match what was configured on the primary controller, indicating that the AP tags have persisted across controllers.

## Feature History for AP Power Save

This table provides release and related information for the feature explained in this module.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

**Table 1: Feature History for AP Power Save**

Release	Feature Information
Cisco IOS XE Cupertino 17.8.1	This feature allows a network administrator to force APs to operate in low-power mode to reduce power consumption.
Cisco IOS XE Cupertino 17.9.1	Feature support for the following APs: <ul style="list-style-type: none"> <li>• Cisco Catalyst 9164 Series Access Points</li> <li>• Cisco Catalyst 9166 Series Access Points</li> </ul>
Cisco IOS XE Dublin 17.10.1	The following features are supported: <ul style="list-style-type: none"> <li>• Radio spatial streams</li> <li>• Flexible PoE profiles</li> </ul>
Cisco IOS XE 17.13.1	AP Power Distribution support in Cisco Catalyst 9124 Series APs.

## Information About AP Power Save

The power-save mode in APs allows a network administrator to force APs to operate in low-power mode to reduce power consumption.

The AP Power Save feature is supported in the following APs:

- Cisco Catalyst 9115 Series Access Points
- Cisco Catalyst 9120 Series Access Points
- Cisco Catalyst 9124 Series Access Points
- Cisco Catalyst 9130 Series Access Points

- Cisco Catalyst 9136 Series Access Points
- Cisco Catalyst 9164 Series Access Points
- Cisco Catalyst 9166 Series Access Points
- Cisco Catalyst 9162 Series Access Points

## Access Point Power Policy

The access point power policy allows you to define the power budget utilization available for an AP, wherein, you can define a set of policies for different interfaces on an AP. You can manage interfaces such as Wi-Fi radios, USB, and so on, as required.

Cisco Catalyst 9124 AXI/D APs support up to two radio interfaces (single 5 GHz), and Cisco Catalyst 9124 AXE APs support up to three (dual 5 GHz) radio interfaces. When Cisco Catalyst 9124 Series APs operate under 802.3at/PoE+/30W insufficient power condition, the new operating modes support both dual or Tri-Radio mode.

### Use Case for AP Power Policy

The following is the use case of an AP power policy:

- You can define a power policy for the available power inputs, such as, 802.3af, 802.3at, 802.3bt (for multiple levels), DC power, and so on. With tri-radio and quad-radio APs, the power requirement has gone beyond the capability of the 802.3at Power over Ethernet (PoE) mode. Therefore, with the AP power policy, for example, we statically predefine an AP operation when provided with non-802.3bt power (such, as TX power, radio chains, USB port, SFP, and so on).

## Power-Save Mode

The power-save mode enables an AP to switch to a low-power mode when no clients are associated with the AP. For example, when this mode is enabled in workspaces, the AP falls asleep during after hours, thereby saving power consumption of the AP throughout the night.

From Cisco IOS-XE Cupertino 17.10.1 onwards, you can shut down AP radios or lower the radio spatial streams, to reduce usage of power. You can enforce radio speed by configuring the number of spatial streams on the radios. The combinations for radio spatial stream policies are: 1X1, 2X2, 3X3 (only for Cisco Catalyst 9130 Series Access Points), 4X4, and 8X8.

The following are the advantages of the power-save mode:

- Increases the energy saving per AP: In the power save mode you can reduce AP functions during off-peak hours and save an additional 20% in energy costs compared to the regular idle mode.
- Enables environmentally conscious purchases: Large enterprises and companies track environmental performance as one of their key indices. They have a centralized energy team to monitor their energy efficiency, which magnifies the importance of the power-save feature.

## PoE Profiles

- **Fixed PoE Profile:** The APs negotiate the power that is required, from the switches they are connected to. The power required varies from one AP model to another AP model. If an AP is not granted the power it requested, it operates under the power budget. In such conditions, some of the interfaces operate under *degraded conditions*.

For example, some radios may operate at 2SS instead of at 4SS, which they are capable of. The operating conditions for each of the AP interfaces differs from one power level to another. These are referred to as fixed PoE profiles. Fixed PoE profiles are applied when the AP is operating in normal mode, that is, nonpower-save mode. When the AP operates in power-save mode, the configured PoE power policies are applied.

- **PoE Power Policy:** With power policies or profiles, you can configure interfaces that you want to set at certain speeds. With this policy, you can configure a profile of your choice that will be pushed to the AP based on your calendar or timing. For example, on a group of APs in the second floor, push a profile where you want to turn off all APs, except 2.4-GHz radio, from 7 p.m. to 7 a.m.
- **Flexible PoE Profile:** With flexible PoE profiles, you can configure different interfaces and set specific parameter values and states for each interface, instead of following fixed PoE profile rules. If an AP does not get the power it requires, it operates under the power budget by using the flexible PoE profile.

In Cisco IOS XE 17.13.1, PoE-out is a new interface introduced in Cisco Catalyst 9124 Series APs, in addition to the USB, Ethernet, and LAN interfaces. The PoE-out for Cisco Catalyst 9124 Series AP RLAN works only if you have enabled the RLAN port.

The operational parameter values for each interface of the AP may be adjusted based on the AP's hardware specifications as the following Table 2 to 7.

**Table 2: AP Power Draw Specifications: Cisco Catalyst 9115, 9120, 9130 Series APs**

Access Points	PoE-In-Mode/DC Mode	Consumption @ Power Device	Consumption @ Power Source Equipment	Feature Mode						
		AP	Worst-Case Cable	Radio 1	Radio 2	Radio 3	Ethernet	USB	Module	PoEOut
Cisco Catalyst 9115AXI Access Points	.3af	13.0	15.4	2X2	2X2	—	1G	N	—	—
	.3at	16.0	18.9	4X4	4X4	—	2.5G	N	—	—
	.3at	20.4	24.1	4X4	4X4	—	2.5G	Y(3.75W)	—	—
Cisco Catalyst 9115AXE Access Points	.3af	13.0	15.4	2X2	2X2	—	1G	N	—	—
	.3at	17.0	20.1	4X4	4X4	—	2.5G	N	—	—
	.3at	21.4	25.3	4X4	4X4	—	2.5G	Y(3.75W)	—	—

Access Points	PoE-In-Mode/DC Mode	Consumption @ Power Device	Consumption @ Power Source Equipment	Feature Mode						
		AP	Worst-Case Cable	Radio 1	Radio 2	Radio 3	Ethernet	USB	Module	PoEOut
Cisco Catalyst 9200XIE Access Points	.3af	13.8	15.4	1X1	1X1	Enabled	1G	N	—	—
	.3at	20.5	23.2	4X4	4X4	Enabled	2.5G	N	—	—
	.3at	25.5	30.0	4X4	4X4	Enabled	2.5G	Y(4.5W)	—	—
Cisco Catalyst 9300XIE Access Points	.3af	13.8	15.4	1X1	1X1	Enabled	1G	N	—	—
	.3at	25.5	30.0	8X8	4X4	Enabled	5G	N	—	—
	.3at	25.5	30.0	Primary 4X4 Secondary Off	4X4	Enabled	5G	Y(4.5W)	—	—
	.3at	25.5	30.0	Primary 4X4 Secondary 4X4	Disabled	Enabled	5G	Y(4.5W)	—	—
	.3bt	30.5	33.3	8X8	4X4	Enabled	5G	Y(4.5W)	—	—

Table 3: AP Power Draw Specifications: Cisco Catalyst 9136 Series APs

Access Points	Power Mode	Consumption @Power Device	Consumption @Power Source Equipment	Feature Mode								
		at AP	Worst-Case Cable	5G Radio	2G Radio	6G Radio	AUX Radio	Mgig0	Mgig1	USB	Module	PoE Out
Cisco Catalyst 9136 Series Access Points	.3af - Fixed	13.9	15.4	Disabled	Disabled	Disabled	Enabled	1G	Disabled	Disabled	—	—
	.3at - Fixed	24.0	27.90	Primary - 4X4 Secondary - Disabled	2X2	2X2	Enabled	2.5G	2.5G (hitless failover standby)	Disabled	—	—
	.3bt - Fixed	43.4	54.81	8X8 or Dual 4X4	4X4	4X4	Enabled	5G	5G	Y(9W)	—	—
	.3bt - PoE Policy 1	37.3	41.63	8X8 or Dual 4X4	4X4	4X4	Enabled	5G	5G	Disabled	—	—

Table 4: AP Power Draw Specifications: Cisco Catalyst 9166 Series APs

Access Points	Profile	Consumption @Power Device	Consumption @Power Source Equipment	Feature Mode								
		at AP	Worst-Case Cable	5G Radio	2G Radio	6G Radio	AUX Radio	Mgig0	Mgig1	USB	Module	PoEOut
Cisco Catalyst 9166 Series Access Points	.3af - Fixed	13.9	15.4	Disabled	Disabled	Disabled	Enabled	1G	—	Disabled	—	—
	.3at - Fixed Policy	25.5	30.0	4X4	4X4	4X4	Enabled	5G	—	Disabled	—	—
	.3bt - Fixed	30.5	32.8	4X4	4X4	4X4	Enabled	5G	—	Y (4.5 W)	—	—
	DC Jack - Fixed	30.5	—	4X4	4X4	4X4	Enabled	5G	—	Y (4.5 W)	—	—

Table 5: AP Power Draw Specifications: Cisco Catalyst 9164 Series APs

Access Points	Profile	Consumption @Power Device	Consumption @Power Source Equipment	Feature Mode								
		at AP	Worst-Case Cable	5G Radio	2G Radio	6G Radio	AUX Radio	Mgig0	Mgig1	USB	Module	PoEOut
Cisco Catalyst 9164 Series Access Points	.3af - Fixed	13.9	15.4	Disabled	Disabled	Disabled	Enabled	1G	—	Disabled	—	—
	.3at - Fixed	25.5	30.0	4X4	2X2	4X4	Enabled	2.5G	—	Disabled	—	—
	.3bt - Fixed	30.1	32.8	4X4	2X2	4X4	Enabled	2.5G	—	Y (4.5 W)	—	—
	DC Jack - Fixed	30.1	—	4X4	2X2	4X4	Enabled	2.5G	—	Y (4.5 W)	—	—



Table 6: AP Power Draw Specifications: Cisco Catalyst 9162 Series APs

Access Points	Radio Mode	Consumption @Power Device	Consumption @Power Source Equipment	Feature Mode								
		at AP	Worst-Case Cable	5G Radio	2G Radio	6G Radio	AUX Radio	Mgig0	Mgig1	USB	Module	PoE Out
Cisco Catalyst 9162 Series Access Points	.3af	13.3	14.32	1X1	Disabled	1X1	Enabled	1G	—	Disabled	—	—
	.3at	20.1	22.67	2X2	2X2	2X2	Enabled	2.5G	—	Disabled	—	—
	.3at	25.5	30	2X2	2X2	2X2	Enabled	2.5G	—	Y (4.5W)	—	—

Table 7: AP Power Draw Specifications: Cisco Catalyst 9124 Series APs

Access Points	Radio Mode	Consumption @Power Device	Consumption @Power Source Equipment	Feature Mode										
		at AP	Worst-Case Cable	Radio 0	R0 dBm Per Path	Radio 1	R1 dBm Per Path	Radio 2	R02 dBm Per Path	AUX Radio	Port Mgig	SFP Module	GbE PHY	PoE Out
				2.4 GHz Radio		5 GHz Primary Radio		5 GHz Secondary Radio		Other				
Cisco Catalyst 9124 AXI	.3af	13.8	15.4	Disabled	—	Disabled	—	NA	NA	Enabled	1G	N	N	N
	.3at	25.5	30	2X2	23	2X2	23	NA	NA	Enabled	1G	N	Y	N
	.3bt	33.6	39.5	4X4	24	4X4	24	NA	NA	Enabled	2.5G	Y	Y	N
Cisco Catalyst 9124 AXD	UPE / DC													
Cisco Catalyst 9124 AXE Dual Radio Mode	.3bt	51	60	4X4	24	4X4	24	NA	NA	Enabled	2.5G	Y	Y	Y
	UPE / DC													

Access Points	RME	Consumption @Power Device	Consumption @Power Source Equipment	Feature Mode										
		at AP	Worst-Case Cable	Radio 0	R0 dBm Per Path	Radio 1	R1 dBm Per Path	Radio 2	R02 dBm Per Path	AUX Radio	Band Mgmt	SFP Module	GbE PHY	REQt
				2.4 GHz Radio		5 GHz Primary Radio		5 GHz Secondary Radio		Channe				
Cisco Catalyst 9124 AXI	.3at	25.5	30	Shutdn	—	4X4	24	Shutdn	—	Enbld	2.5G	Y	N	N
Cisco Catalyst 9124 AXD														
Single 5G Radio														
Cisco Catalyst 9124 AXE Tri-Band Mode	.3af	13.8	15.4	Disbld	—	Disbld	—	Disbld	—	Enbld	1G	N	N	N
	.3at	25.5	30	Disbld	—	Disbld	—	Disbld	—	Enbld	1G	N	N	N
	.3bt / UCE / DC	33.6	39.5	2X2	24	2X2	24	2X2	24	Enbld	2.5G	Y	Y	N
	.3bt / UCE / DC	51	60	2X2	24	2X2	24	2X2	24	Enbld	2.5G	Y	Y	Y
Cisco Catalyst 9124 AXE Dual 5G Radio	.3at	25.5	30	Shutdn	—	2X2	23	2X2	23	Enbld	1G	N	Y	N

## Wakeup Threshold for Access Point Power Save Mode

The Wakeup Threshold feature enables you to define the client threshold in the AP power profile configuration to determine when the AP wakes up from the power save mode or enter into the power save mode.

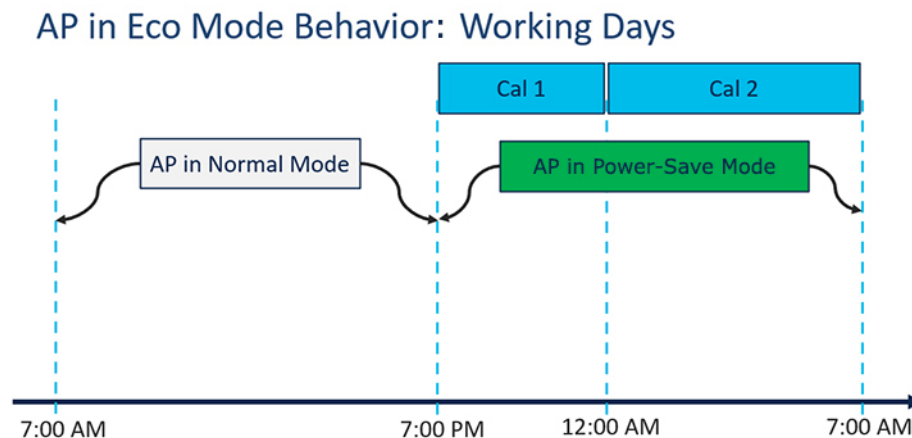
When the AP applies the calendar associated power profile (for an active calendar), and the number of connected clients reach the wakeup threshold, the AP wakes up from power save mode and goes into the Fixed power profile mode or the Regular power profile (insufficient power) mode.

When the AP applies the calendar associated power profile (for an active calendar), and the number of connected clients is less than the wakeup threshold, the AP applies the calendar associated power profile to shut down the interface or to lower the interface speed to save power.

## AP Power Save Scenarios

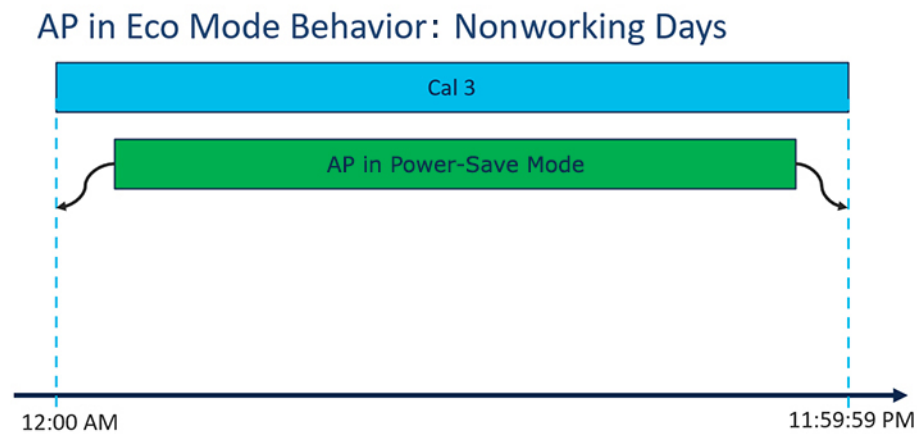
The AP Power Save feature helps APs to enter into a power-save mode or low-power mode by applying a calendar, for example, for after hours, associated with the corresponding power profile. The AP profile is enhanced to associate a PoE power policy with calendar profiles. The following are the scenarios for Eco mode APs:

- **Figure 1: AP in Eco Mode Behavior: Working Days**



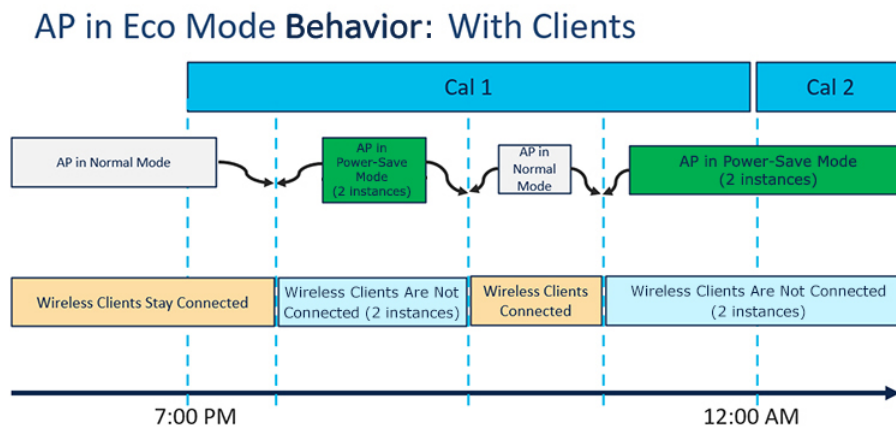
On working days, from 7:00 a.m. to 7:00 p.m., the AP functions in normal mode or fixed mode, when the maximum number of clients are connected to the AP. From 7:00 p.m. to 12:00 a.m., the **Cal1** calendar profile timer starts to put the AP in the power-save mode. Likewise, the **Cal2** calendar profile timer starts, and extends the power-save mode from 12:00 a.m. to 7:00 a.m. Again, at 7:00 a.m., the AP goes into normal mode.

• **Figure 2: AP in Eco Mode Behavior: Nonworking Days**



On nonworking days, the AP goes into power-saving mode from 12:00 a.m. to 11:59:59 p.m. The **Cal3** calendar profile is applied here. This profile defines the timer for the power-save mode. This means that there are no clients connected to the AP, and that the AP is asleep.

• **Figure 3: AP in Eco Mode Behavior: With Clients**



When clients are connected to the AP, the AP automatically switches to the normal mode. For example, in the calendar profile **Cal1**, the AP is in normal mode, because wireless clients are connected to the AP. At 8:00 p.m., clients get dissociated from the AP, and the AP goes into power-save mode. When clients enter the AP coverage area at 9:30 p.m., the AP automatically switches from power-save mode to normal mode of operation.

# Configuring Power Policy Profile (GUI)

## Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > Power Profile**.
- Step 2** Click **Add**.  
The **Add Power Profile** window is displayed.
- Step 3** Enter a name and description for the power profile. The name must be ASCII characters of up to 128 characters, without leading or trailing spaces.
- Step 4** Click **Add** to add rules for the power profile.
- Step 5** In the **Sequence number** field, enter a unique sequence number to designate the priority in which power should be disabled for the component. The sequence number of 0 indicates that the component should be disabled first.
- Step 6** From the **Interface** and **Interface ID** drop-down list, choose interface and interface ID to designate to the component for which the power derating rule applies.
- Step 7** From the **Parameter** and **Parameter value** drop-down list, choose the values depending on the interface you chose in step 6.  
  
For example, if you chose **Ethernet** as an interface, you can further customize the rule for the interface by choosing the associated speed. This rule ensures that the AP disables power for the Ethernet interface that is operating at a higher speed, and thereby consuming more power.
- Step 8** Click the check mark to save and then click **Apply to Device**.
- 

# Configuring a Power Policy Profile (CLI)

## Before you begin

You must keep at least one radio interface up and running before you configure a power policy profile.

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile power</b> <i>power-profile-name</i>  <b>Example:</b> Device(config)# <b>wireless profile power</b> <i>power-profile-name</i>	Configures the power policy profile.

	Command or Action	Purpose
<b>Step 3</b>	<p><i>sequence-number</i> <b>ethernet</b> {<b>GigabitEthernet0</b>   <b>GigabitEthernet1</b> <b>speed</b> {<b>1000mbps</b>   <b>100mbps</b>   <b>2500mbps</b>   <b>5000mbps</b>}   <b>LAN1</b>   <b>LAN2</b>   <b>LAN3</b> <b>state disable</b>}</p> <p><b>Example:</b></p> <pre>Device(config-wireless-power-profile)# 10 ethernet gigabitethernet1 speed 1000mbps</pre>	<p>Configures the power policy for Ethernet.</p> <p><i>sequence-number</i>: The power profile settings are ordered by sequence numbers. AP derating takes place as per the sequence number entered. The same combination of interface identifiers and parameter values does not appear in another sequence number. The same interface with the same parameter can appear multiple times with different parameter values, however, the parameter value that yields the lowest power consumption is the one that gets selected, irrespective of the sequence number if there is active calendar.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• The Ethernet interface is used to join the controller. The uplink interface is not disabled even if it is defined in the power policy.</li> <li>• Ethernet speed configuration is not operational in Cisco IOS XE 17.8.1 and later releases.</li> </ul>
<b>Step 4</b>	<p><i>sequence-number</i> <b>radio 24ghz</b> {<b>spatial-stream</b> {<b>1</b>   <b>2</b>   <b>3</b>   <b>4</b>}   <b>state shutdown</b>}</p> <p><b>Example:</b></p> <pre>Device(config-wireless-power-profile)# 20 radio 24ghz spatial stream 2</pre>	<p>Configures spatial stream for the 2.4-GHz band radio.</p> <p>Here:</p> <p><i>sequence-number</i>: The power profile settings are ordered by sequence numbers. AP derating takes place as per the sequence number entered. The same combination of interface identifiers and parameter values does not appear in another sequence number. The same interface with the same parameter can appear multiple times with different parameter values.</p> <ul style="list-style-type: none"> <li>• 1: Specifies a 1X1 radio spatial stream.</li> <li>• 2 : Specifies a 2X2 radio spatial stream.</li> <li>• 3 : Specifies a 3X3 radio spatial stream.</li> <li>• 4 : Specifies a 4X4 radio spatial stream.</li> </ul> <p><b>state shutdown</b>: Indicates that the radio state is down.</p>
<b>Step 5</b>	<p><i>sequence-number</i> <b>radio 5ghz</b> {<b>spatial-stream</b> {<b>1</b>   <b>2</b>   <b>3</b>   <b>4</b>   <b>8</b>}   <b>state shutdown</b>}</p> <p><b>Example:</b></p>	<p>Configures spatial stream for the 5-GHz band radio.</p> <p>Here:</p>

	Command or Action	Purpose
	<pre>Device(config-wireless-power-profile)# 30 radio 5ghz spatial stream 4</pre>	<p><i>sequence-number</i>: The power profile settings are ordered by sequence numbers. AP derating takes place as per the sequence number entered. The same combination of interface identifiers and parameter values does not appear in another sequence number. The same interface with the same parameter can appear multiple times with different parameter values.</p> <ul style="list-style-type: none"> <li>• 1: Specifies a 1X1 radio spatial stream.</li> <li>• 2 : Specifies a 2X2 radio spatial stream.</li> <li>• 3 : Specifies a 3X3 radio spatial stream.</li> <li>• 4 : Specifies a 4X4 radio spatial stream.</li> <li>• 8 : Specifies a 8X8 radio spatial stream.</li> </ul> <p><b>state shutdown</b>: Indicates that the radio state is down.</p>
<b>Step 6</b>	<p><i>sequence-number</i> <b>radio secondary-5ghz</b> {<b>spatial-stream</b> {1   2   3   4   8}   <b>state shutdown</b>}</p> <p><b>Example:</b></p> <pre>Device(config-wireless-power-profile)# 40 radio 5ghz spatial stream 4</pre>	<p>Configures spatail stream for a secondary 5-GHz band radio.</p> <p>Here:</p> <p><i>sequence-number</i>: The power profile settings are ordered by sequence numbers. AP derating takes place as per the sequence number entered. The same combination of interface identifiers and parameter values does not appear in another sequence number. The same interface with the same parameter can appear multiple times with different parameter values.</p> <ul style="list-style-type: none"> <li>• 1: Specifies a 1X1 radio spatial stream.</li> <li>• 2 : Specifies a 2X2 radio spatial stream.</li> <li>• 3 : Specifies a 3X3 radio spatial stream.</li> <li>• 4 : Specifies a 4X4 radio spatial stream.</li> <li>• 8 : Specifies a 8X8 radio spatial stream.</li> </ul> <p><b>state shutdown</b>: Indicates that the radio state is down.</p>
<b>Step 7</b>	<p><i>sequence-number</i> <b>radio 6ghz</b> {<b>spatial-stream</b> {1   2   3   4   8}   <b>state shutdown</b>}</p> <p><b>Example:</b></p> <pre>Device(config-wireless-power-profile)# 50 radio 6ghz spatial stream 2</pre>	<p>Configures spatail stream for the 6-GHz band radio.</p> <p>Here:</p> <p><i>sequence-number</i>: The power profile settings are ordered by sequence numbers. AP derating</p>

	Command or Action	Purpose
		<p>takes place as per the sequence number entered. The same combination of interface identifiers and parameter values does not appear in another sequence number. The same interface with the same parameter can appear multiple times with different parameter values.</p> <ul style="list-style-type: none"> <li>• 1 : Specifies a 1X1 radio spatial stream.</li> <li>• 2 : Specifies a 2X2 radio spatial stream.</li> <li>• 3 : Specifies a 3X3 radio spatial stream.</li> <li>• 4 : Specifies a 4X4 radio spatial stream.</li> <li>• 8 : Specifies a 8X8 radio spatial stream.</li> </ul> <p><b>state shutdown:</b> Indicates that the radio state is down.</p>
<b>Step 8</b>	<p><i>sequence-number</i> <b>usb 0 state disable</b></p> <p><b>Example:</b></p> <pre>Device(config-wireless-power-profile)# 60 usb 0 state disable</pre>	Configures the power policy for USB.

## Configuring a Calendar Profile (GUI)

Configure calendar profiles to set up a daily, weekly, or monthly recurrence schedule.

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > Calendar**.
- Step 2** Click **Add**.  
The **Add Calendar Profile** window is displayed.
- Step 3** Enter a name for the calendar profile. The name must be ASCII characters of up to 32 characters, without leading or trailing spaces.
- Step 4** From the **Recurrence** drop-down list, choose the schedule for which you want to create a profile.
- Step 5** Select the **Start Time** and the **End Time** for the recurrence schedule.



**Note**

- For daily recurrences, you can select the start time and end time. For example, if you want the AP to derate the power on certain interfaces between 7 p.m. to 7 a.m. daily, or if you want the controller to not allow any clients to be associated during this period, you can set up this daily recurrence schedule.

To cover this timespan, you must create two calendar profiles, one for 7 p.m. till 23:59:59, and another one from midnight to 7 a.m. of the next calendar day, and map it to the same power profile. After this, assign it to the AP Join profile.

- For weekly recurrences, select the specific days of the week along with the start and end time.
- For monthly recurrence, select the specific days of the month along with the start and end time.

**Step 6** Click **Apply** to save the configuration.

## Configuring a Calendar Profile (CLI)

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile calendar-profile name</b> <i>calendar_profile_ap_power</i>  <b>Example:</b> Device# wireless profile calendar-profile name ap_power_calendar	Configures a calendar profile. Enters the calendar profile configuration mode.  Here, <b>name</b> refers to the name of the calendar profile.
<b>Step 3</b>	<b>recurrence daily</b>  <b>Example:</b> Device(config-calendar-profile)# recurrence daily	Configures daily recurrence for daily profile.
<b>Step 4</b>	<b>start start-time end end-time</b>  <b>Example:</b> Device(config-calendar-profile)# start 16:00:00 end 20:00:00	Configures the start time and end time for calendar profile.
<b>Step 5</b>	<b>end</b>  <b>Example:</b> Device(config-calendar-profile)# end	Returns to privileged EXEC mode.

## Configuring a Power Policy in an AP Join Profile (GUI)

Power policy supports the use of a power profile or a mapped configuration of a power profile and a calendar profile that are pushed to an AP during an AP join session. You can map a maximum of five combination profiles (calendar and power) per AP profile.

### Before you begin

Ensure that the power profile and calendar profile are created and displayed in the respective drop-down lists in the GUI.

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > AP Join**.  
The **Add AP Join Profile** window is displayed.
- Step 2** Click the **AP** tab.
- Step 3** Under the AP tab, click the **Power Management** tab.
- Step 4** From the **Regular Power Profile** drop-down list, choose the power profile.  
The AP applies these settings to derate the power based on the configured priority list.
- Note** If you want the AP to apply the power profile configuration during a specific time period, choose the **Calendar Profile** and map it to the power profile from the drop-down list.
- Step 5** Click the check mark to associate the mapping.
- Step 6** Click **Apply to Device** to save the configuration.
- 

## Mapping a Power Profile Under an AP Profile (CLI)

### Before you begin

Ensure that you have defined a calendar profile in the wireless profile, before you map the calendar profile to an AP join profile.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>ap profile</b> <i>ap-profile-name</i>  <b>Example:</b> Device(config)# <b>ap profile</b> <i>ap-profile-name</i>	Configures an AP profile and enters AP profile configuration mode.

	Command or Action	Purpose
<b>Step 3</b>	<b>power-profile</b> <i>power-profile-name</i> <b>Example:</b> Device(config-ap-profile)# <b>power-profile</b> <i>power-profile-name</i>	Configures the AP power profile. This power profile is used during non-calendar hours to meet the power budget provided by the switch connected to the AP.
<b>Step 4</b>	<b>calendar-profile</b> <i>calendar-profile-name</i> <b>Example:</b> Device(config-ap-profile)# <b>calendar-profile</b> <i>ap-calendar-profile</i>	Maps a calendar profile to the AP profile. Enters the AP profile calendar configuration mode.
<b>Step 5</b>	<b>[no] action power-saving-mode power-profile</b> <i>power-profile-name</i> <b>Example:</b> Device(config-ap-profile-calendar)# <b>action power-saving-mode</b> <b>power-profile</b> <i>power-profile1</i>	Maps a specific power profile to a specific calendar profile. Maps the power-saving mode action for the calendar profile. Use the <b>no</b> form of this command to disable the command. <b>Note</b> You can have more than one mapping of calendar profile to power profile.

## Configuring Client Wakeup Threshold (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile power</b> <i>power-profile-name</i> <b>Example:</b> Device(config)# <b>wireless profile power</b> <i>power-profile1</i>	Configures the power policy profile.
<b>Step 3</b>	<b>power-save-client-threshold</b> <i>client-threshold</i> <b>Example:</b> Device(config-wireless-power-profile)# <b>power-save-client-threshold</b> 5	Configures the client threshold up to which the AP can stay in the power save mode. The valid range is between 1 and 32 clients. The default value is 1.

## Configuring PoE-Out Interface in Power Profile (GUI)

### Before you begin

Enable the RLAN port for the AP.

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > Power Profile**.
- Step 2** Click **Add**.  
The **Add Power Profile** window is displayed.
- Step 3** Enter a name and description for the power profile. The name can contain up to 128 ASCII characters, without leading or trailing spaces.
- Step 4** (Optional) From the **Power Save Client Threshold** counter, select a value to set a limit to the number of client associations with the AP. The default value is 1. The valid range is between 1 to 32.
- Step 5** Click **Add** to create a rule for the PoE-Out interface.  
The **Rule** section is displayed in the window.
- Step 6** In the **Rule** section, complete the following steps:
- In the **Sequence number** field, enter a unique sequence number to assign the priority in which power should be disabled for the component. A sequence number of 0 indicates that the component should be disabled first.
  - From the **Interface** drop-down list, choose **Ethernet** as the interface.
  - From the **Interface ID** drop-down list, choose one of the following interfaces: **LAN1**, **LAN2**, or **LAN3**.
  - From the **Parameter** drop-down list, choose **POE-out**.  
  
A POE-out port on an AP is used to provide power to the another device, for example, a camera. This selection ensures that the power usage of the port is reduced or shut down at the specified sequence.
- Step 7** Click the check mark button to save.
- Step 8** Click **Apply to Device**.
- 

## Configuring PoE-Out Interface in Power Profile (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wireless profile power <i>power-profile-name</i></b>  <b>Example:</b> Device(config)# wireless profile power poe-out-power-profile	Configures the power policy profile. Enters the wireless power profile configuration mode.
<b>Step 3</b>	<b><i>sequence-number</i> ethernet LAN1 poe-out disable</b>  <b>Example:</b>	Disables the PoE-out state.

	Command or Action	Purpose
	Device(config-wireless-power-profile)# 1 ethernet LAN1 poe-out disable	

## Configuration Example of Power Profile

The following example shows how to define a power save policy:

```
wireless profile power power-save
    10 radio 5ghz state shutdown
    20 radio secondary-5ghz state shutdown
    30 radio 6ghz state shutdown
    40 usb 0 state disable
```

The following example shows how to define a calendar profile:

```
wireless profile calender-profile name eve-to-midnight
    recurrence daily
    start 19:00:00 end 23:59:59
wireless profile calender-profile name midnight-to-morning
    recurrence daily
    start 00:00:00 end 07:00:00
wireless profile calender-profile name weekends
    recurrence weekly
    day Saturday
    day Sunday
    start 00:00:00 end 23:59:59
```

The following example shows how to define an AP join profile and map a calendar profile to a power profile:

```
ap profile wireless-prof-sitel
    calendar-profile eve-to-midnight
    action power-saving-mode power-profile power-save
    calendar-profile midnight-to-morning
    action power-saving-mode power-profile power-save
    calendar-profile weekends
    action power-saving-mode power-profile power-save
```

## Verifying Access Point Power Policy (GUI)

To verify the applied configuration on the GUI, follow these steps:

### Procedure

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Choose <b>Monitoring &gt; AP Statistics</b> .  |
| <b>Step 2</b> | Click a Cisco Catalyst 9136 series AP from the list of APs.<br>The <b>General</b> window is displayed.                         |
| <b>Step 3</b> | Click the <b>Power</b> tab.<br>The <b>Power Operational Status</b> and the <b>AP Fixed Power Policy</b> details are displayed. |
| <b>Step 4</b> | Click <b>OK</b> .  |
-

To verify the AP fixed power policy details from the list of configured APs, follow these steps:

### Procedure

- 
- Step 1** Choose **Configuration > Access Points**.
  - Step 2** Click a Cisco Catalyst 9136 series AP from the list of APs.  
The **Edit AP** window is displayed.
  - Step 3** Click the **Interfaces** tab.  
The **AP Fixed Power Policy** details are displayed.
  - Step 4** Click **Update & Apply**.
- 

## Verifying the Access Point Power Profile

To view the calendar profile and its mapping, run the following command:

```
Device# show ap profile name default-ap-profile detailed
AP Profile Name           : default-ap-profile
Description               : default ap profile
Power profile name        : power_prof_day
AP packet capture profile : Not Configured
AP trace profile          : Not Configured
Mesh profile name         : default-mesh-profile
Power profile name        : Not Configured
Calendar Profile
  Profile Name             : cal47
  Power saving mode profile name : pow_da
  -----
  Profile Name             : cal48
  Power saving mode profile name : pow23
  -----
```

To view the operational details of the AP, run the following command:

```
Device# show ap name cisco-ap power-profile summary
AP power derate Capability : Capable
```

```
Power saving mode
Power saving mode profile : pow2
Associated calendar profile : cal1
```

```
AP power profile status : Insufficient De-rating
```

Interface	Interface-ID	Parameter	Parameter value	Status
Radio	5 GHz	State	DISABLED	Success
Radio	6 GHz	State	DISABLED	Not Applicable
Ethernet	LAN1	State	DISABLED	Not Applicable
Radio	2.4 GHz	State	DISABLED	Success
Ethernet	Gig0	Speed	5000 MBPS	Fixed Policy

**AP power derate capability** is displayed in the output as **Capable** only for those APs that support power policy. For the other APs, it is displayed as **Not Capable**.

In the **show ap name cisco-ap power-profile summary** output, in the power saving mode, the status of the interface configured in the power profile (for example, **pow2**) is applied on the AP, and the AP sends the

details (that are displayed in the show command) such as, the name of the power saving profile and the associated calendar profile.

The table that is displayed shows the interfaces and the parameter status of the power saving profile. The AP sends the information as to which of the interfaces are disabled. For example, if the AP does not have a 6-GHz radio interface, the **Status** is displayed as **Not Applicable**. If the interfaces are applied without any errors, then **Success** is displayed.



**Note** When the AP uses the fixed power policy, due to inactive calendar or client connectivity, the interfaces are not displayed in the power profile summary if their status is UP on the AP.

## Verifying Radio Spatial Streams

To view the configuration and operational details of radio spatial stream rules in the power profile, run the following commands:

```
Device# show wireless profile power detailed wireless_pow_profile_name
Power profile name          : wireless_pow_profile_name
```

```
-----
Description                  :
.
Seq No      Interface      Interface-id      Parameter      Parameter value
-----
100         Radio         6 GHz           Spatial Stream  2 x 2
200         Radio         5 GHz           Spatial Stream  8 x 8
400         USB           USB0            State           DISABLED
500         Ethernet      Gig0            Speed           100 MBPS
600         Radio         6 GHz           State           DISABLED
700         Radio         2.4 GHz         State           DISABLED
900         Radio         5 GHz           State           DISABLED
```

```
Device# show ap name cisco-ap-name power-profile summary
AP power derate Capability   : Capable
```

```
AP fixed power policy
-----
```

Interface	Interface-ID	Parameter	Parameter value	Status
Ethernet	Gig0	Speed	5000 MBPS	Fixed Policy
Radio	2.4 GHz	Spatial Stream	4 x 4	Fixed Policy
Radio	5 GHz	Spatial Stream	8 x 8	Fixed Policy
Radio	Sec 5 GHz	Spatial Stream	4 x 4	Fixed Policy
USB	USB0	State	DISABLED	Fixed Policy

## Verifying Client Threshold

To view the client threshold details, run the following command:

```
Device# show wireless profile power detailed profile1
Power profile name          : profile1
-----
Description                  : Power profile 1
Power save client threshold : 5
```

Seq No	Interface	Interface-id	Parameter	Parameter value
0	Radio	6 GHz	State	DISABLED
1	Radio	5 GHz	Spatial Stream	1 x 1
2	Radio	2.4 GHz	Spatial Stream	2 x 2
3	USB	USB0	State	DISABLED

## Verifying PoE-Out Details

To view the PoE-out details in the wireless power profile, run the following commands:

```
Device# show wireless profile power detailed poe-out_profile_name
Power profile name          : poe-out_profile_name
```

```
Description                : profile-description
```

Seq No	Interface	Interface-id	Parameter	Parameter value
10 ...				
20	Ethernet	LAN 1	POE_OUT	DISABLED
30 ...				

```
Device# show ap name Cisco-Ap1 power-profile summary
AP power derate Capability  : Capable
```

```
AP fixed power policy
```

Interface	Interface-ID	Parameter	Parameter value	Status
...				
Ethernet	LAN 1	POE_OUT	DISABLED	Fixed Policy
...				

## Information About Access Point Real-Time Statistics

From Cisco IOS XE Bengaluru 17.5.1 onwards, you can track the CPU utilization and memory usage of an AP, and monitor the health of an AP, by generating real-time statistics for an AP.

SNMP traps are defined for CPU and memory utilization of APs and the controller. An SNMP trap is sent out when the threshold is crossed. The sampling period and statistics interval can be configured using SNMP, YANG, and CLI.

Statistics interval is used to process the data coming from an AP, and the average CPU utilization and memory utilization is computed over time. You can also configure an upper threshold for these statistics. When a statistic value surpasses the upper threshold, an alarm is enabled, and an SNMP trap is triggered.

From Cisco IOS XE Cupertino 17.7.1 release onwards, for radio monitoring, you can reset the radios based on the statistics sent by the AP for a sampling period. When you configure the radios in the controller, if there is no increment in the Tx or Rx statistics when the radio is up, then the radio reset is triggered.

## Feature History for Real Time Access Point Statistics

This table provides release and related information for the feature explained in this module.



Table 8: Feature History for Real Time Access Point Statistics

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.7.1	Real Time Access Point Statistics	This feature is enhanced with the implementation of AP threshold values between 0 and 50 to trigger an alarm.

## Restrictions for AP Radio Monitoring Statistics

You cannot reset the radio firmware from the controller. The controller will shut and unshut the radio if the Rx or Tx count is not incremented for a radio slot in a specified period.

## Configuring Access Point Real Time Statistics (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > AP Join**.
- Step 2** Click **Add**. The **Add AP Join Profile** page is displayed.
- Step 3** Under the **AP** tab, click the **AP Statistics** tab.
- Step 4** In the **System Monitoring** section:
- Enable **Monitor Real Time Statistics** to get calculated statistics and alarms of the AP.
  - To receive an alarm when the upper threshold is surpassed for parameters such as CPU utilization and memory, enable **Trigger Alarm for AP**.
  - Enter the threshold percentage for CPU and memory usage in the **CPU Threshold to Trigger Alarm** field and **Memory Threshold to Trigger Alarm** fields, respectively. The valid range is between 0 to 50. An SNMP trap is sent out when this threshold is crossed.
  - In the **Interval to Hold Alarm** field, enter the time for which the alarm is held before it gets triggered. The valid range is between 0 and 3600 seconds.
  - In the **Trap Retransmission Time** field, enter the time between retransmissions of the alarm. The valid range is between 0 and 65535 seconds.
  - To define how often data should be collected from the AP, enter a value in the **Sampling Interval** field. The valid range is between 720 and 3600 seconds.
  - To define the interval at which AP statistics are to be calculated, enter a value in the **Statistics Interval** field. The valid range is between 2 and 900 seconds.
  - To automatically reload the AP when there is high CPU and memory usage in the defined sampling interval, select the **Reload the AP** check box.
- Step 5** Under the **Radio Monitoring** section:
- Select the **Monitoring of AP Radio stuck** check box to verify that the Tx and Rx statistics of the AP are updated each time the payloads are coming in from the AP to the controller.
  - To generate an alarm for the radio of the AP when there is no increment in the Tx and RX statistics for the payloads, select the **Alarms for AP Radio stuck** check box.

- c) Select the **Reset the stuck AP Radio** check box to recover the radio from the bad state. A radio admin state payload will be sent from the controller to toggle the radio and the radio will be shut when there is no increment in the Tx and Rx statistics.
- d) To define how often data should be collected from the radio, enter a value in the **Sampling Interval** field. The valid range is between 720 and 3600 seconds.

**Step 6** Click **Apply to Device** to save the configuration.

## Configuring Real-Time Access Point Statistics (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>ap profile</b> <i>ap-profile-name</i>  <b>Example:</b> Device(config)# ap profile doc-test	Configures the AP profile. The default AP join profile name is <i>default-ap-profile</i> .
<b>Step 3</b>	<b>stats-timer</b> <i>frequency</i>  <b>Example:</b> Device(config-ap-profile)# stats-timer 60	(Optional) Configures the statistics timer. This command is used to change the frequency of the statistics reports coming from the AP. The valid values range between 0 and 65535 seconds.
<b>Step 4</b>	<b>statistics ap-system-monitoring enable</b>  <b>Example:</b> Device(config-ap-profile)# statistics ap-system-monitoring enable	(Optional) Enables monitoring of AP real-time statistics (CPU and memory).
<b>Step 5</b>	<b>statistics ap-system-monitoring alarm-enable</b>  <b>Example:</b> Device(config-ap-profile)# statistics ap-system-monitoring alarm-enable	Enables alarms for AP real-time statistics (CPU and memory).
<b>Step 6</b>	<b>statistics ap-system-monitoring alarm-hold-time</b> <i>duration</i>  <b>Example:</b> Device(config-ap-profile)# statistics ap-system-monitoring alarm-hold-time 400	Defines the alarms for AP real-time statistics (CPU and Memory). The valid values range between 0 and 3600 seconds.

	Command or Action	Purpose
<b>Step 7</b>	<b>ap-system-monitoring alarm-retransmit-time <i>duration</i></b>  <b>Example:</b> <pre>Device(config-ap-profile)# ap-system-monitoring alarm-retransmit-time 100</pre>	Defines the interval between retransmissions of the trap alarm. The valid values range between 0 and 65535 seconds.
<b>Step 8</b>	<b>statistics ap-system-monitoring cpu-threshold <i>percentage</i></b>  <b>Example:</b> <pre>Device(config-ap-profile)# statistics ap-system-monitoring cpu-threshold 30</pre>	<p>Defines the threshold for CPU usage on the AP (percentage) to trigger alarms.</p> <p><b>Note</b> From Cisco IOS XE Cupertino 17.7.1 release onwards, the valid threshold value for CPU on the AP to trigger the alarms is between 0 and 50.</p>
<b>Step 9</b>	<b>ap-system-monitoring mem-threshold <i>percentage</i></b>  <b>Example:</b> <pre>Device(config-ap-profile)# ap-system-monitoring mem-threshold 40</pre>	<p>Defines the threshold for memory usage on AP to trigger alarms. The percentage of threshold for memory usage on the AP to trigger is between 0 and 100.</p> <p><b>Note</b> From Cisco IOS XE Cupertino 17.7.1 release onwards, the valid threshold value for memory usage on the AP to trigger the alarms is between 0 and 50.</p>
<b>Step 10</b>	<b>ap-system-monitoring sampling-interval <i>duration</i></b>  <b>Example:</b> <pre>Device(config-ap-profile)# statistics ap-system-monitoring sampling-interval 600</pre>	(Optional) Defines the sampling interval. The valid values range between 2 and 900 seconds.
<b>Step 11</b>	<b>exit</b>  <b>Example:</b> <pre>Device(config-ap-profile)# exit</pre>	Exits from AP profile configuration mode and returns to global configuration mode.
<b>Step 12</b>	<b>trapflags ap ap-stats</b>  <b>Example:</b> <pre>Device(config)# trapflags ap ap-stats</pre>	Enables sending AP-related traps. Traps are sent when statistics exceed the configured threshold.

### Example

```
Device(config)# ap profile default-policy-profile
Device(config-ap-profile)# statistics ap-system-monitoring enable
Device(config-ap-profile)#statistics ap-system-monitoring sampling-interval 90
Device(config-ap-profile)#statistics ap-system-monitoring stats-interval 120
Device(config-ap-profile)#statistics ap-system-monitoring alarm-enable
Device(config-ap-profile)#statistics ap-system-monitoring alarm-hold-time 3
```

```

Device(config-ap-profile)#statistics ap-system-monitoring alarm-retransmit-time 10
Device(config-ap-profile)#statistics ap-system-monitoring cpu-threshold 90
Device(config-ap-profile)#statistics ap-system-monitoring mem-threshold 90
Device(config)# trapflags ap ap-stats

```

## Configuring AP Radio Monitoring Statistics

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>ap profile <i>profile-name</i></b>  <b>Example:</b> Device(config)# ap profile test1	Configures an AP profile and enters the AP profile configuration mode.
<b>Step 3</b>	<b>statistic ap-radio-monitoring enable</b>  <b>Example:</b> (config-ap-profile)#statistic ap-radio-monitoring enable	Enables the monitoring of AP radio stuck statistics.
<b>Step 4</b>	<b>statistic ap-radio-monitoring alarm-enable</b>  <b>Example:</b> (config-ap-profile)#statistic ap-radio-monitoring alarm-enable	(Optional) Enables the alarm for AP radio stuck statistics.
<b>Step 5</b>	<b>statistic ap-system-monitoring action reload-ap interval <i>duration</i></b>  <b>Example:</b> (config-ap-profile)# statistic ap-radio-monitoring action reload-ap interval850	(Optional) Specifies the sampling interval in seconds. The valid values range between 720 and 3600 seconds.
<b>Step 6</b>	<b>statistic ap-radio-monitoring action radio-reset</b>  <b>Example:</b> (config-ap-profile)# statistic ap-radio-monitoring action radio-reset	(Optional) Generates an alarm and resets the radio if the radio is stuck.
<b>Step 7</b>	<b>statistic ap-system-monitoring action reload-ap</b>  <b>Example:</b> (config-ap-profile)# statistic ap-system-monitoring action reload-ap	Reloads the AP.

### Example

```
Device(config)# ap profile test1
Device(config-ap-profile)# statistics ap-radio-monitoring enable
Device(config-ap-profile)# statistic ap-radio-monitoring alarm-enable
Device(config-ap-profile)# statistic ap-radio-monitoring sampling-interval 750
Device(config-ap-profile)# statistic ap-radio-monitoring action radio-reset
Device(config-ap-profile)# statistic ap-system-monitoring action reload-ap
```

## Monitoring Access Point Real-Time Statistics (GUI)

### Procedure

- Step 1** Choose **Monitoring > Wireless > AP Statistics**.
- Step 2** Click the **General** tab.
- Step 3** Click an AP name. The **General** window is displayed.
- Step 4** To view the AP Statistics data, click the **AP Statistics** tab.

The following information is displayed:

- **Memory alarm last send time:** Displays the time of the last memory trap sent.
- **Memory Alarm Status:** Displays the state of the memory alarm. An alarm can be **ACTIVE**, **INACTIVE**, **INACTIVE\_SOAKING**, **ACTIVE\_SOAKING**. An alarm is soaked until the configured hold time has passed.
- **Memory alarm raise time:** Displays the last time the memory alarm was active.
- **Memory alarm clear time:** Displays the last time the memory alarm was inactive.
- **Last statistics received:** Displays the time of the last statistics report received from the AP.
- **Current CPU Usage:** Displays the latest percentage of CPU usage reported.
- **Average CPU Usage:** Displays the average CPU usage calculated.
- **Current Memory Usage:** Displays the latest percentage of memory usage reported.
- **Average Memory Usage:** Displays the average memory usage calculated.
- **Current window size:** Displays the window size. The window size is calculated by dividing the statistics interval by the sampling interval. The average CPU and memory usage is calculated by the window size.
- **CPU alarm last send time:** Displays the time of the last CPU trap sent.
- **CPU Alarm Status:** Displays the state of the CPU alarm. An alarm can be **ACTIVE**, **INACTIVE**, **INACTIVE\_SOAKING**, **ACTIVE\_SOAKING**. An alarm is soaked until the configured hold time has passed.
- **CPU alarm raise time:** Displays the last time the CPU alarm was active.

- **CPU alarm clear time:** Displays the last time the CPU alarm was inactive.

**Step 5** Click OK.

## Verifying Access Point Real-Time Statistics

To verify AP real-time statistics, run the **show ap config general | section AP statistics** command:

```
Device# show ap config general | section AP statistics
!Last Statistics
AP statistics : Enabled
Current CPU usage : 4
Average CPU usage : 49
Current memory usage : 35
Average memory usage : 35
Last statistics received : 03/09/2021 15:25:08
!Statistics Configuration
Current window size : 1
Sampling interval : 30
Statistics interval : 300
AP statistics alarms : Enabled
!Alarm State - Active, Inactive, Inactive_Soaking, Inactive_Soaking
Memory alarm status : Active
Memory alarm raise time : 03/09/2021 15:24:29
Memory alarm clear time : NA
Memory alarm last send time : 03/09/2021 15:24:59
CPU alarm status : Inactive
CPU alarm raise time : 03/09/2021 15:24:25
CPU alarm clear time : 03/09/2021 15:25:05
CPU alarm last send time : 03/09/2021 15:25:05
!Alarm Configuration
Alarm hold time : 6
Alarm retransmission time : 30
Alarm threshold cpu : 30
Alarm threshold memory : 32
```

To verify the statistics reporting period, run the **show ap config general | i Stats Reporting Period** command:

```
Device# show ap config general | i Stats Reporting Period
Stats Reporting Period : 10
```

## Feature History for Access Point Auto Location Support

This table provides release and related information about the feature explained in this section.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

**Table 9: Feature History for Access Point Auto Location Support**

Release	Feature Information
Cisco IOS XE Dublin 17.12.1	The Access Point Auto Location Support feature helps to effectively self-locate APs in a global coordinate by combining various ranging technologies and algorithms.

Release	Feature Information
Cisco IOS XE Dublin 17.13.1	The improvized Access Point Auto Location Support feature helps wireless clients to leverage Fine Timing Measurement (FTM) and AP GNSS for indoor navigation.

## Information About Access Point Auto Location Support

In all enterprise wireless deployments, AP location is manually entered. In many cases, the AP location is not entered because it is a tedious process to identify the location manually and enter it in the system, or, the AP location is entered only to provide a reference for client location. A Global Positioning System (GPS) or a Global Navigation Satellite System (GNSS) solution is not feasible because of the indoor nature of the deployments.

From Cisco IOS XE Dublin 17.12.1 onwards, a solution to effectively self-locate the APs in a global coordinate by combining various ranging technologies and algorithms, is introduced through the AP Location feature.

Location of an object, by definition, is dependent on a reference point. Here, reference points are based as a few subsets of sparse nodes from a group of nodes serving a continuous RF domain. These are the ones that have visibility to the open sky, namely, the ones located near the windows, or the ones at the periphery of the building or floor.

The AP Auto Location solution delivers accurate, automated, up-to-date AP location leveraging Fine Timing Measurement (FTM) and GNSS when available. If GNSS is not accessible, a few manual anchors need to be provided per floor. This feature requires an AP density such that neighboring APs can hear each other at maximum power. The accuracy of the feature depends on the building type and the distances between APs.

The process includes:

- Segmentation of a large number of APs into smaller segments with floor-level labels and the calculation of the geolocations of all the APs at the end of the process.
- Geolocation of an AP is determined at the controller, Cisco Spaces, or both the controller and Cisco Spaces.
- Highly accurate GNSS positioning of the APs that have good GNSS signal reception and, geolocating the APs with no GNSS reception by running the locationing algorithm to determine the geolocation based on inter-APs ranging data (FTM) to GNSS-enabled APs.

From Cisco IOS XE 17.13.1 onwards, the AP Auto Location Support feature has been improvized to help wireless clients to leverage FTM and AP GNSS for indoor navigation.

- Client FTM: You can enable the FTM responder in the designated WLANs for indoor navigation. The APs support ranging from unassociated clients through the FTM responders in the 5-GHz and 6-GHz bands.
- Air Pressure Reporting Updates: APs send air pressure report to the controller. As an enhancement to this feature, in Cisco IOS XE 17.13.1, remote procedure calls (RPC) and the Privileged EXEC mode commands enable the collection of air pressure details for a specific duration. For example, if you set the duration as 10 minutes, then the AP will send samples every 30 seconds, for 10 minutes.
- AP Band Filters: In Cisco IOS XE Dublin 17.12.1, the area optimization for AP-to-AP ranging was triggered on a per site-tag basis. From Cisco IOS XE Dublin 17.13.1 onwards, band filters such as 5 GHz or 6 GHz are enhanced for effective ranging.

- **AP Ranging Completion Notification:** The controller monitors all APs in a given site for ranging completion. Ranging is considered as complete only after the AP sends the ranging report back to the controller, in response to the ranging requests made by the controller.

The controller notifies the APs and Cisco Spaces when ranging is complete for a given site.

- **AP Movement Alarm:** When an AP gets disconnected and later reconnects in a different location, the AP sends an alarm to the controller. The controller prints a syslog and sends an event to Cisco Spaces, to notify the user about the AP movement.

### Use Case

A typical use case of the solution in the controller is either self-locating APs in one building or APs in one floor of a building.

### Supported Access Points

This feature is supported in the following APs:

- Cisco Catalyst 9130 Series Access Points
- Cisco Catalyst 9136 Series Access Points
- Cisco Catalyst 9164 Series Access Points
- Cisco Catalyst 9166 Series Access Points

## Configuring Access Point Geolocation Derivation Using Ranging (GUI)

### Procedure

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Choose <b>Configuration &gt; Wireless &gt; Wireless Global</b> .   |
| <b>Step 2</b> | In the <b>AP Geolocation</b> section, click the <b>Geolocation Derivation Using Ranging</b> toggle button to enable geolocation derivation.<br>When you enable <b>Geolocation Derivation Using Ranging</b> , it allows the corresponding AP to be a part of the location services that use ranging to determine the geolocation of the AP. |
| <b>Step 3</b> | Click <b>Apply</b> .   |
-



## Configuring Access Point Geolocation Derivation Using Ranging (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>[no] ap geolocation derivation ranging</b>  <b>Example:</b> Device(config)# ap geolocation derivation ranging	Enables geolocation derivation using ranging. Use the <b>no</b> form of this command to disable the feature.

## Configuring Access Point Ranging Parameters (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > AP Join**.
- Step 2** Click **Add**.
- Step 3** In the **General** tab, enter the name and description of the corresponding AP join profile.
- Step 4** Click the **Geolocation** tab.
- Step 5** In the **Fine Time Management (FTM)** section, complete the following:
- Click the **FTM** toggle button to allow APs to use FTM for inter AP ranging.
  - In the **FTM Initiator Burst Size** field, specify the burst size value. The burst size determines the size of the transmitted frames. The valid range is between 2 and 31 frames. The default value is 16 frames per burst.
  - From the **FTM Initiator Burst Duration** drop-down list, choose a value. The burst duration determines the interval of the transmitted frames. The default value is 32 microseconds.
- Step 6** Click **Apply to Device**.
-

## Configuring Access Point Ranging Parameters (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>ap profile <i>ap-profile-name</i></b>  <b>Example:</b> Device(config)# ap profile ap-profile1	Configures an AP profile and enters AP profile configuration mode.
<b>Step 3</b>	<b>[no] geolocation ftm</b>  <b>Example:</b> Device(config-ap-profile)# geolocation ftm	Enables geolocation Fine Timing Measurement (FTM).
<b>Step 4</b>	<b>[no] geolocation ftm initiator burst-size <i>burst-size</i></b>  <b>Example:</b> Device(config-ap-profile)# geolocation ftm initiator burst-size 8	Configures the geolocation FTM burst size. The burst size values are 4, 8, 16, 32, and 64 frames. The default value is 8 frames per burst.
<b>Step 5</b>	<b>[no] geolocation ftm initiator burst-duration {128ms   16ms   1ms   250us   2ms   32ms   4ms   500us   64ms   8ms}</b>  <b>Example:</b> Device(config-ap-profile)# geolocation ftm initiator burst-duration 32ms	Configures the geolocation FTM burst duration. The default value is 32 microseconds.

## Configuring Access Point Coordinates and Floor Information (CLI)

The following steps help you to configure the AP coordinates and the corresponding floor information.



**Note** There are no corresponding GUI steps for this configuration.

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> enable	Enables privileged EXEC mode. Enter your password, if prompted.
<b>Step 2</b>	<b>ap name</b> <i>ap-name</i> <b>geolocation coordinates</b> <i>longitude latitude</i> <b>Example:</b> Device# ap name cisco-ap1 geolocation coordinates 90 45	Configures the longitude and latitude of the AP. The value range for longitude is between -180 and 180 degrees. The value range for latitude is between -90 to 90 degrees.
<b>Step 3</b>	<b>ap name</b> <i>ap-name</i> <b>floor</b> <i>floor-id</i> <b>Example:</b> Device# ap name cisco-ap1 floor 2147483647	Configures the floor ID for the AP. The floor ID range is between -2147483648 and 2147483647.

## Configuring On-Demand Access Point Ranging (CLI)

The following steps help you to configure on-demand AP ranging.



**Note** There are no corresponding GUI steps for this configuration.

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> enable	Enables privileged EXEC mode. Enter your password, if prompted.
<b>Step 2</b>	<b>ap geolocation ranging site</b> <i>ap-site-tag</i> <b>accurate</b> [5ghz   6ghz] <b>Example:</b> Device# ap geolocation ranging site ap-site-tag accurate 5ghz	Enables accurate ranging using the 5-GHz or 6-GHz bands on APs under the configured site tag.  <b>Note</b> Client connections may be disrupted.
<b>Step 3</b>	<b>ap geolocation ranging all accurate</b> [5ghz   6ghz] <b>Example:</b> Device# ap geolocation ranging all accurate 5ghz	Enables accurate ranging using the 5-GHz or 6-GHz bands on all APs.  <b>Caution</b> Client connections may be disrupted.

## Enabling Fine Time Measurement (802.11mc) Responder (GUI)

### Procedure

- 
- Step 1** Choose **Configuration > Tags & Profiles > WLANs**.
- Step 2** Click **Add**.  
The **Add WLAN** page is displayed.
- Step 3** In the **General** tab, enter the **Profile Name**, the **SSID**, and the **WLAN ID**.
- Step 4** In the **Advanced** tab, under the **Geolocation** section, click the **Fine Time Measurement (FTM) Responder** toggle button to enable the AP to respond to time measurement queries sent from a client. The client sends time measurement queries to measure its distance to the AP and determine their indoor location.  
The **Advertise AP Location** field is displayed.
- Step 5** Click the **Advertise AP Location** toggle button to enable the AP to advertise its geolocation coordinates.
- Step 6** Click **Apply to Device** to save the configuration.
- 

## Configuring Fine Time Measurement (802.11mc) Responder (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>wlan profile-name wlan-id ssid-name</b> <i>profile-name wlan-id ssid-name</i>  <b>Example:</b> Device(config)# wlan wlan-profile 36 ssid1	Specifies the WLAN name and ID. <ul style="list-style-type: none"> <li>• <i>profile-name</i> is the WLAN name. Valid WLAN names can contain upto 32 alphanumeric characters</li> <li>• <i>wlan-id</i> is the wireless LAN identifier. The valid range is from 1 to 4096.</li> <li>• <i>ssid-name</i> is the SSID which can contain 32 alphanumeric characters.</li> </ul>
<b>Step 3</b>	<b>[no] geolocation ftm-responder</b>  <b>Example:</b> Device(config-wlan)# geolocation ftm-responder	Configures the FTM responder.

	Command or Action	Purpose
<b>Step 4</b>	<b>[no] geolocation ftm-responder advertise-ap-location</b>  <b>Example:</b> Device(config-wlan)# geolocation ftm-responder advertise-ap-location	Configures the advertisement of AP location to clients.
<b>Step 5</b>	<b>(Optional) clear ap geolocation ranging</b>  <b>Example:</b> Device# clear ap geolocation ranging	Clears the AP geolocation best known FTM report.

## Configuring Air Pressure Reporting (CLI)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  Enter your password, if prompted.
<b>Step 2</b>	<b>ap sensor air-pressure {all   site site-tag-name} [duration duration-time]</b>  <b>Example:</b> Device# ap sensor air-pressure site sitetag1 duration 10	Configures the sensor air pressure data collection for all APs or for APs in a specific site tag. The value range of the duration of the air pressure reporting is between 1 minute and 1440 minutes. The default is 10 minutes.

## Verifying Access Point Geolocation Information

To view the AP geolocation ranging report, run the following command:

```
Device# show ap geolocation ranging report
```

AP RadioMAC	NeighbourMAC	Type	Method	Dist(cm)	Channel	Band	Width	
Duration(ms)	RSSIAvg	Frames	Time					
10f9.20fd.b6e0-60	10f9.20fd.f640	BEST	FTM	122	213	6 GHz	20 MHz	32
	1/0		02/16/2023 15:25:04 UTC					
10f9.20fd.b6e0-60	10f9.20fd.f640	LATEST	FTM	122	213	6 GHz	20 MHz	32
	1/0		02/16/2023 15:25:04 UTC					
10f9.20fd.f640-71	10f9.20fd.b6e0	BEST	FTM	118	1	6 GHz	20 MHz	11
	1/0		01/25/1970 20:31:23 UTC					
10f9.20fd.f640-60	10f9.20fd.b6e0	LATEST	FTM	124	1	6 GHz	20 MHz	12
	1/0		02/16/2023 14:36:44 UTC					

To view an AP geolocation ranging request, run the following command:

```
Device# show ap geolocation ranging request
```

Request ID	SiteTag/All APs	Mode	Band	Requests	Responses	Reports
Start Time		End Time				

```

3          ALL APs          Accurate    All      2        2        4
09/22/2023 16:29:28 IST    09/22/2023 16:29:36 IST
2          ALL APs          Normal      All      2        0        0
09/22/2023 16:21:13 IST    09/22/2023 16:21:35 IST
1          ALL APs          Accurate    All      2        2        6
09/22/2023 16:18:39 IST    09/22/2023 16:18:49 IST

```

To view the AP geolocation summary, run the following command:

```

Device# show ap geolocation summary
AP Name          Radio MAC          Location Location Longitude  Latitude
Major-axis Minor-axis Orientation Height Height  Height  Height
              (meters) (degrees) Type (meters) Uncertainty Source (degrees) (degrees) (meters)
                                   (meters)

```

```

APCC9C.3EF1.0F30    10f9.20fd.f640    Ellipse    Manual    90.000000    90.000000    0
                   0          0.000000    NA      NA      NA      NA

```

To view the AP geolocation statistics, run the following command:

```

Device# show ap geolocation statistics
Num APs with GNSS          : 1
Num APs with manual height : 0
Num APs with derived geolocation : 0
Last geolocation derivation run : 07/21/2023 08:54:21

```

To view the AP geolocation GNSS-capable summary, run the following command:

```

Device# show ap geolocation gnss-capable summary
-----
AP Name          Radio MAC          GPS Coverage    Antenna Type    Last GPS fix
-----
APCC9C.3EF4.CF00    10f9.20fd.b6e0    No              Internal         NA

```

To view the AP geolocation ranging status, run the following commands:

```

Device# show ap geolocation ranging status
Device# show ap name geolocation ranging status

```

To view the ranging capability of APs, run the following command:

```

Device# show ap geolocation ranging capability
AP Name          FTM Responder    FTM Initiator
-----
AP0001.Cisco.CF00    Yes              Yes
AP0002.Cisco.0F30    Yes              Yes
AP-2800           No               No
AP0003.Cisco.82a0    No               No

```