# System Configuration


- Information About New Configuration Model, on page 1
- Configure a wireless profile policy (GUI), on page 3
- Configure a wireless policy profile (CLI), on page 4
- Configure a flex profile, on page 5
- Configure an AP profile (GUI), on page 6
- Configure an AP profile (CLI), on page 10
- Configure an RF profile (GUI), on page 11
- Configure an RF profile (CLI), on page 11
- Enhanced Site Tag-Based Load Balancing, on page 13
- Configure policy tag (GUI), on page 16
- Configure a policy tag (CLI), on page 17
- Configure wireless RF tag (GUI), on page 18
- Configure wireless RF tag (CLI), on page 18
- Attach a policy tag and site tag to an AP (GUI), on page 19
- Attach policy tag and site tag to an AP (CLI), on page 20
- Time Management, on page 21
- AP Filter, on page 21
- Configuring Access Point for Location Configuration, on page 27


# Information About New Configuration Model

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

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

### Policy Tag

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

The policy tag contains the map of WLAN policy profile. There can be a maximum of 16 such entries per policy tag. Changes to the map entries are effected based on the status of the WLAN profile and policy profile. For example, if a map (WLAN1 and Policy1) is added to the policy tag, and both the WLAN profile and the policy profile are enabled, the definitions are pushed to the APs using the policy tag. However, if one of them is in disabled state, the definition is not pushed to the AP. Similarly, if a WLAN profile is already being broadcast by an AP, it can be deleted using the no form of the command in the policy tag.

### Site Tag

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

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

### RF Tag

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

### Profiles

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

### WLAN Profile

WLAN profiles are configured with same or different service set identifiers (SSIDs). An SSID identifies the specific wireless network for the controller to access. Creating WLANs with the same SSID allows to assign different Layer 2 security policies within the same wireless LAN.

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

### Policy Profile

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

### Flex Profile

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

### AP Join Profile

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

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

### RF Profile

RF profile contains the common radio configuration for the APs. RF profiles are applied to all the APs that belong to an AP group, where all the APs in that group have the same profile settings.

### Association of APs

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

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

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

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

### Modifying AP Tags

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

# Configure a wireless profile policy (GUI)

Define and apply a wireless profile policy to manage network behavior and access for wireless clients.

Use this task to create or modify a policy profile, ensuring wireless network policies suit your organization's needs.

### Procedure

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

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

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

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

**Step 5** In the WLAN Switching Policy section, choose the following, as required:

- No 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.
- No 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 6** Click **Save & Apply to Device**.

The wireless profile policy is successfully created and applied. Devices use the updated policy settings for wireless client management.

# Configure a wireless policy profile (CLI)

Define and apply a wireless policy profile on your device using command-line interface commands.

Use this task to configure wireless profile policies on Cisco wireless controllers. Policy profiles specify settings such as VLAN mapping, idle timeouts, and accounting lists for wireless networks.

**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.

Follow the procedure given to configure a wireless profile policy:

**Before you begin**

- Ensure you have administrator privileges to access and configure the device.
- Have the required VLAN ID, idle timeout value, and accounting list details available, if applicable.

Follow these steps to configure a wireless profile policy:

### Procedure

**Step 1** Enter global configuration mode.

**Example:**

```
Device# configure terminal
```

**Step 2** Configure the WLAN policy profile and enters wireless policy configuration mode.

**Example:**

```
Device(config)# wireless profile policy rr-xyz-policy-1
```

**Step 3** (Optional) Configure the duration of idle timeout in seconds.

**Example:**

```
Device(config-wireless-policy)# idle-timeout 1000
```

**Step 4** Configure the VLAN name or VLAN ID.

**Example:**

```
Device(config-wireless-policy)# vlan 24
```

**Step 5** Save the configuration, exit configuration mode, and return to privileged EXEC mode.

**Example:**

```
Device(config-wireless-policy)# no shutdown
```

**Step 6** (Optional) View detailed information about a policy profile, using the **show wireless profile policy detailed** *policy-profile-name* command.

**Example:**

```
Device# show wireless profile policy summary
```

The wireless policy profile is configured and enabled on the device. All specified settings are applied to the selected policy.

### What to do next

- Associate the policy profile with a WLAN as needed.
- Review and validate the applied settings by connecting a client device and confirming expected behavior.

# Configure a flex profile

Create or modify a flex profile to customize wireless network behavior for specific sites or device groups.

Use flex profiles within your network management system to define site-specific configurations such as VLANs, SSIDs, or access policies.

**Before you begin**

Identify the devices or sites to apply the flex profile.

### Procedure

**Step 1** Enter global configuration mode.

**Example:**

```
Device# configure terminal
```

**Step 2** Configure a flex profile and enter flex profile configuration mode.

**Example:**

```
Device(config)# wireless profile flex rr-xyz-flex-profile
```

**Step 3** (Optional) Enable default parameters for the flex profile.

**Example:**

```
Device(config-wireless-flex-profile)# description xyz-default-flex-profile
```

**Step 4** (Optional) Enable ARP caching.

**Example:**

```
Device(config-wireless-flex-profile)# arp-caching
```

**Step 5** Save the configuration, exit configuration mode, and return to privileged EXEC mode.

**Example:**

```
Device(config-wireless-flex-profile)# end
```

**Step 6** (Optional) View detailed parameters about the flex profile, use the **show wireless profile flex detailed** *flex-profile-name* command.

**Example:**

```
Device# show wireless profile flex summary
```

The flex profile is created or updated and available for assignment to devices or sites.

### What to do next

Assign the flex profile to the relevant site, device, or group as needed.

# Configure an AP profile (GUI)

Configure and customize AP join profiles for your wireless deployment.

Use this task to define, modify, or apply AP profile parameters such as country code, LED state, timers, VLAN tagging, security settings, management options, and advanced features, using the device's graphical interface.

**Before you begin**

- Review the default AP join profile to update parameters for your environment (For example, Control and Provisioning of Wireless Access Points (CAPWAP), IPv4 or IPv6, UDP Lite, High Availability, retransmit configuration parameters, global AP failover, Hyperlocation configuration parameters, Telnet or SSH, 11u parameters, and so on.)
- Obtain required information, such as network-specific settings, controller addresses, credentials, and profile names.

### Procedure

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

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

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

**Step 3** In the **General** tab, enter a name and description for the AP join profile.

**Step 4** Check the **LED State** check box to set the LED state of all APs connected to the device to blink, making them easier to locate.

**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 AP 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 AP that allows the AP to join the device.

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

**Step 7** In the **AP** tab, you can configure various options:

- 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. Use power injectors to provide flexible powering options for APs, such as local power, multiport switches with inline power, or multiport power patch panels.
c) From the **Power Injector Type** drop-down list, choose power injector type from the following options:

- Installed: If you want the AP to examine and remember the MAC address of the currently connected switch port. (This selection assumes that a power injector is connected.)
- Override: To enable the AP to operate in high-power mode without first verifying a matching MAC address.

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 .
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 for 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 used for health monitoring, proximity detection, asset tracking, and in-store navigation. You can customize BLE beacon settings for each AP, even if they are configured globally.

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 one to 10, with a default value of one.
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**.

**Step 8** 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, SSH or both configurations, 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, 802.1x credentials, or both as required.
g) Click **Save & Apply to Device**.

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

**Step 9** In the **Rogue AP** tab, check the **Rogue Detection** check box to enable rogue detection.

**Step 10** 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 11** 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 12** 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 13** Check the **Rogue Containment Automatic Rate Selection** check box to enable rogue containment automatic rate selection.

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

**Step 14** Check the **Auto Containment on FlexConnect Standalone** check box to enable the feature.

The AP continues containment if it moves to FlexConnect standalone mode.

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

---

The AP join profile is created or updated. Devices assigned to this profile use its configuration for network operation and management.

### What to do next

- Verify that APs have successfully joined and received the new settings by reviewing AP status.
- Adjust profile settings as necessary for site-specific needs or to resolve configuration issues.

# Configure an AP profile (CLI)

Set up and customize an AP profile using CLI commands to apply network-wide AP configurations.

Use this procedure when you need to define or modify an AP profile for your wireless controller, typically to standardize AP settings or apply feature-specific options.

**Before you begin**

Identify the name and required settings for your AP profile.

**Procedure**

**Step 1** Enter global configuration mode.

**Example:**

```
Device# configure terminal
```

**Step 2** Configure an AP profile and enter AP profile configuration mode.

**Example:**

```
Device(config)# ap profile xyz-ap-profile
```

**Note**

- In an AP profile, the **EAP-FAST** is the default EAP type.
- When you delete a named profile, the APs associated with that profile does not revert to the default profile.

**Step 3** Add a description for the AP profile.

**Example:**

```
Device(config-ap-profile)# description "xyz ap profile"
```

**Step 4** Enable CDP for all Cisco APs.

**Example:**

```
Device(config-ap-profile)# cdp
```

**Step 5** Save the configuration, exit configuration mode, and return to privileged EXEC mode.

**Example:**

```
Device(config-ap-profile)# end
```

**Step 6** (Optional) Display detailed information about an AP join profile.

**Example:**

```
Device# show ap profile name xyz-ap-profile detailed
```

The AP profile is created or updated with specified settings, and changes are active on the controller.

### What to do next

Assign APs to the new profile as required, and verify AP behavior matches the intended configuration.

# Configure an RF profile (GUI)

Create and enable an RF profile to optimize radio frequency settings for your wireless network.

Use this task to define an RF profile that sets parameters for radio bands and device operation. This ensures consistent performance across your wireless deployment.

### Before you begin

Use the same RF profile name when configuring the wireless RF tag. If the RF tag contains an RF profile that does not exist, the radios do not operate.

### Procedure

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

**Step 2** On the **RF Profile** window, 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**.

The new RF profile is created, enabled, and applied to the device.

### What to do next

- Verify that the RF profile settings are visible and active on your device.
- Assign the profile to RF tags or APs, if required, to complete your configuration.

# Configure an RF profile (CLI)

Create and enable an RF profile to optimize radio frequency settings for your wireless network.

Use this task to define an RF profile that sets parameters for radio bands and device operation. This ensures consistent performance across your wireless deployment.

### Before you begin

Use the same RF profile name when configuring the wireless RF tag. If the RF tag contains an RF profile that does not exist, the radios do not operate.

### Procedure

**Step 1** Enter global configuration mode.

**Example:**

```
Device# configure terminal
```

**Step 2** Configure an RF profile, and enter RF profile configuration mode.

**Example:**

```
Device(config)# ap dot11 24ghz rf-profile rfprof24_1
```

**Note**
Use the **24ghz** command to configure the 802.11b parameters. Use the **5ghz** command to configure the 802.11a parameters.

**Step 3** (Optional) Enable default parameters for the RF profile.

**Example:**

```
Device(config-rf-profile)# default
```

**Step 4** Enable the RF profile on the device.

**Example:**

```
Device(config-rf-profile)# no shutdown
```

**Step 5** Exit configuration mode and return to privileged EXEC mode.

**Example:**

```
Device(config-rf-profile)# end
```

**Step 6** (Optional) Display a summary of available RF profiles.

**Example:**

```
Device# show ap rf-profile summary
```

**Step 7** (Optional) Display detailed information about a particular RF profile.

**Example:**

```
Device# show ap rf-profile name rfprof24_1 detail
```

You have created and enabled a new RF profile, and applied it to the device.

### What to do next

- Verify that the RF profile settings are visible and active on your device.
- Assign the profile to RF tags or APs as required to complete your configuration.

# Enhanced Site Tag-Based Load Balancing

## Feature History for Enhanced Site Tag-Based Load Balancing

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 Enhanced Site Tag-Based Load Balancing***

| Release | Feature | Feature Information |
|---|---|---|
| Cisco IOS XE Dublin 17.10.1 | Enhanced Site Tag-Based Load Balancing | The Site Tag-based load balancing is available from Cisco IOS-XE Gibraltar 16.10.1 release.<br>When the first AP from a site joins the controller, it takes the decision to load balance the entire site. However, this is done without knowing the site load.<br>The enhancement to load balancing feature introduced in Cisco IOS-XE 17.10.1 specifies a site load to help with better load balancing. |

## Enhanced site tag-based load balancing

A site tag-based load balancing is a controller mechanism that

- distributes APs across Wireless Network Control Daemon (WNCD) processes based on site tags,
- allows configuration of a site load for each site tag to optimize AP assignment considering site size, and
- automatically retains site tags in persistent memory and balances them during controller bootup in descending order of the configured site load.

The controller takes the load balancing decision for a site tag when the first AP from that site tag joins.

***Table 2: Feature History***

| Feature | Release | Feature Information |
|---|---|---|
| Enhanced Site Tag-Based Load Balancing | Cisco IOS XE Dublin 17.10.1 | When the first AP from a site joins the controller, it takes the decision to load balance the entire site. However, this is done without knowing the site load. |

### How controllers functioned before load balancing

Previously, controllers did not consider the actual size of sites when making load balancing decisions. The system functioned optimally only when all sites were of approximately equal size. Unequal distribution caused some WNCDs to be overloaded while others remained underused.

The enhanced feature enables administrators to specify a site load for each site tag, ensuring the controller takes site size into account when distributing APs and thus resulting in improved load distribution among WNCDs.

#### Behavior during controller reboot

- After you configure site load balancing in one or more site tags and reboot the controller, The feature retains actively used site tags and balances them at bootup by prioritizing those with higher configured site load before any APs join.
- If load balancing is configured for a site tag with APs already joined, load balancing assignments remain unchanged unless all APs, including those not in the site tag, disconnect or the controller is rebooted.

#### assigning a higher site load to one site over the other

Suppose Site Tag X is assigned a higher site load than Site Tag Y. Upon controller bootup, APs from Site Tag X are distributed among WNCDs before those from Site Tag Y, helping prevent excessive load on any single WNCD even if Site Tag X contains many more APs than Site Tag Y.

#### Analogy: assigning classes to school buses

Think of enhanced site tag-based load balancing like assigning students from different-sized classes (site tags) to school buses (WNCDs). If you ignore class size, you might put all students from the largest class on a single bus, overloading it while leaving other buses half empty. By taking class sizes into account when assigning students, you distribute them more evenly and efficiently among the buses, preventing overcrowding and making better use of all resources. Similarly, by setting site load values, the controller assigns APs more fairly to WNCDs, balancing the work and avoiding overload.

## Prerequisites for Enhanced Site Tag-Based Load Balancing

- Ensure that you configure the site load.
- We recommended that you configure all the named sites with a load value.

**Note** The configured load is only an estimate. It will only be used for site load balancing. Specifically, it does not prevent APs, or clients from joining or associating.

## Use cases

The site load configuration uses a load factor instead of an absolute number to address different use cases. Although the load factor does not have to match the number of APs in a site, using the AP count often provides a practical approximation of the site load.

Here are the use cases:

- Sites with normal client density and roaming load can use AP count as a good approximation of site load. Examples include cubicle areas in offices and hospitals.

- For sites with high client density and roaming load, configure a load factor greater than the number of APs. For example, when a site has 200 APs, use a load factor of 300 or 400 to accommodate the increased client load. Examples include stadiums, cafeterias, and conference floors.

# Configure site load (CLI)

Assign a relative load value to a site tag using CLI. This helps the system optimize resource allocation and network performance for wireless deployments.

Use this task when you need to set or adjust the load recommendation for a specific site on your wireless controller. The load value influences how resources are distributed across sites.

**Before you begin**

Identify the name of the site tag you want to configure.

### Procedure

**Step 1** Enter global configuration mode.

**Example:**

```
Device# configure terminal
```

**Step 2** Configure site tag and enter site tag configuration mode.

**Example:**

```
Device(config)# wireless tag site area1
```

**Step 3** Configure the site load.

**Example:**

```
Device(config-site-tag)# load 200
```

The *load* is the estimate of the relative load reserved for the site. Values range between zero to 1000. The default value zero means no load recommendation for the site.

**Step 4** Return to privileged EXEC mode.

**Example:**

```
Device(config-site-tag)# end
```

The controller uses the configured load value for the specified site tag to optimize network resource allocation for that site

### What to do next

Optionally, verify your changes by displaying the site tag configuration and confirming the new load value.

# Verify enhanced site tag-based load balancing configuration

To view detailed information about a site, use the command:

```
Device# show wireless tag site detailed area1
Site Tag Name        : area1
Description          :
-------------------------------------
AP Profile           : default-ap-profile
Local-site           : Yes
Image Download Profile: default
Fabric AP DHCP Broadcast : Disabled
Fabric Multicast Group IPv4 Address : 239.1.1.1
Site Load            : 200
```

To view the default site tag type for Wireless Network Controller daemon (WNCD) instances, use the command:

```
Device# show wireless loadbalance tag affinity
Tag           Tag type    No of AP's Joined   Wncd Instance
-----------------------------------------------------------------------
area1         SITE TAG                  50         0
area2         SITE TAG                  50         0
area3         SITE TAG                  100        1
area4         SITE TAG                  150        2
```

# Configure policy tag (GUI)

Create and apply a policy tag to group wireless local area network (WLAN) and policy profiles for your network configuration.

Use this task when you need to define or update policy tags for your wireless network devices using the GUI.

**Before you begin**

- Prepare unique names for policy tags using ASCII characters (32 to 126, no leading or trailing spaces).
- Identify the WLAN and policy profiles you plan to map.

## Procedure

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

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

**Step 3** Enter a name and description for the policy tag. You can use ASCII characters from 32 to 126, but do not include any leading or trailing spaces.

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

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

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

Your device has the new policy tag applied. The mapped WLAN and policy profiles are now active based on your configuration.

### What to do next

Verify that connected devices use the updated policy tag and that expected network policies are enforced.

# Configure a policy tag (CLI)

Create and apply a policy tag to group wireless local area network (WLAN) and policy profiles for your network configuration.

Use this task when you need to define or update policy tags for your wireless network devices using the CLI.

**Before you begin**

- Prepare unique names for policy tags using ASCII characters (32 to 126, no leading or trailing spaces).
- Identify the WLAN and policy profiles you plan to map.

## Procedure

**Step 1** Enter global configuration mode.

**Example:**

```
Device# configure terminal
```

**Step 2** Configure policy tag and enter policy tag configuration mode.

**Example:**

```
Device(config-policy-tag)# wireless tag policy default-policy-tag
```

**Note**
When performing local web authentication, the clients connected to a controller get disconnected intermittently before session timeout.

**Step 3** Add a description to a policy tag.

**Example:**

```
Device(config-policy-tag)# description "default-policy-tag"
```

**Step 4** Map a remote-LAN profile to a policy profile.

**Example:**

```
Device(config-policy-tag)# remote-lan remote-lan-name policy profile-policy-name port-id
port-id-number
```

**Step 5** Map a policy profile to a WLAN profile.

**Example:**

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

**Step 6** Exit policy tag configuration mode, and return to privileged EXEC mode.

**Example:**

```
Device(config-policy-tag)# end
```

**Step 7** (Optional) Display the configured policy tags.

**Example:**

```
Device# show wireless tag policy summary
```

**Note**
To view detailed information about a policy tag, use the **show wireless tag policy detailed** *policy-tag-name* command.

Your device has the new policy tag applied. The mapped WLAN and policy profiles are now active based on your configuration.

### What to do next

Verify that connected devices use the updated policy tag and the expected network policies are applied.

# Configure wireless RF tag (GUI)

Create and apply an RF tag that defines radio frequency profiles for device groups.

### Procedure

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

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

**Step 3** Enter a name and description for the RF tag. The name can be ASCII characters from 32 to 126 and must not include leading or trailing spaces.

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

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

The RF tag is created with the specified RF profiles and applied to the device.

# Configure wireless RF tag (CLI)

Assign and configure an radio frequency (RF) tag on your wireless device using the CLI, to manage radio profile settings per tag.

Perform this task to create or modify a wireless RF tag. This allows you to apply specific 2.4 GHz, 5 GHz, or 6 GHz RF profiles to associated APs.

**Before you begin**

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

### Procedure

**Step 1** Enter global configuration mode.

**Example:**

```
Device# configure terminal
```

**Step 2** Create an RF tag to enter wireless RF tag configuration mode.

**Example:**

```
Device(config)# wireless tag rf rftag1
```

**Step 3** Attach an IEEE 802.11b RF policy to the RF tag.

**Example:**

```
Device(config-wireless-rf-tag)# 24ghz-rf-policy rfprof24_1
```

To configure a dot11a policy, use the **5ghz-rf-policy** command.

**Step 4** Add a description for the RF tag.

**Example:**

```
Device(config-wireless-rf-tag)# description Test
```

**Step 5** Exit configuration mode to return to privileged EXEC mode.

**Example:**

```
Device(config-wireless-rf-tag)# end
```

**Step 6** Display the available RF tags.

**Example:**

```
Device# show wireless tag rf summary
```

**Step 7** Display detailed information of a particular RF tag.

**Example:**

```
Device# show wireless tag rf detailed rftag1
```

You have configured the RF tag and it is now available for assignment.

#### What to do next

Assign the RF tag to the appropriate AP tag or APs if you have not already done so.

# Attach a policy tag and site tag to an AP (GUI)

Assign a policy tag and site tag to an AP using the GUI.

Use this procedure to associate specific network policies and locations with an AP in your Cisco wireless deployment.

**Before you begin**

Make sure you have the wired MAC address of the AP.

**Procedure**

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

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

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

The **Edit AP** window is displayed.

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

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

The AP is now associated with the specified policy, site, and optionally RF tags you selected.

# Attach policy tag and site tag to an AP (CLI)

Assign a policy tag and site tag to an AP using the CLI.

Use this procedure to associate specific network policies and locations with an AP in your Cisco wireless deployment.

**Before you begin**

Make sure you have the wired MAC address of the AP.

**Procedure**

**Step 1** Enter global configuration mode.

**Example:**

```
Device# configure terminal
```

**Step 2** Configure a Cisco AP and enters AP profile configuration mode.

**Example:**

```
Device(config)# ap F866.F267.7DFB
```

**Note**
The *mac-address* should be a wired mac address.

**Step 3** Map a policy tag to the AP.

**Example:**

```
Device(config-ap-tag)# policy-tag rr-xyz-policy-tag
```

**Step 4** Map a site tag to the AP.

**Example:**

```
Device(config-ap-tag)# site-tag rr-xyz-site
```

**Step 5** Associate the RF tag.

**Example:**

**Step 6** Save the configuration, exit configuration mode, and return to privileged EXEC mode.

**Example:**

```
Device(config-ap-tag)# end
```

**Step 7** (Optional) Display AP details and the tags associated to it.

**Example:**

```
Device# show ap tag summary
```

**Step 8** Display the AP name with tag information.

**Example:**

```
Device# show ap name "ap-name" tag info
```

**Step 9** (Optional) Display the AP name with tag details.

**Example:**

```
Device# show ap name ap-name tag detail
```

The AP is now associated with the specified policy, site, and optionally, RF tags you selected

# Time Management

The date and time of the system on EWC is configured when you run the initial wireless express setup wizard. You can change or configure the time from the GUI menu by choosing **Administration** > **Time**.

You can configure a Network Time Protocol (NTP) server to synchronize date and time, if it was not configured during the wireless express setup. Greenwich Mean Time (GMT) is used as the standard for setting the time zone on the controller. You can also update or add the specific NTP server to EWC.

**Note** EWC APs do not track time when powered off. Therefore, we recommned you to configure NTP to keep a proper time across reboots on the EWC.

# AP Filter

## AP filters

An AP filter is a global tagging mechanism that

- associates APs with specific tag sources based on defined filter criteria
- organizes and applies tag sources in priority order according to configuration, and
- enables flexible control over which tags are assigned to each AP throughout the device discovery and onboarding process.

### Additional reference information

AP filters function similarly to access control lists (ACLs) on the controller and operate at the global level. You can create AP filters based on AP names or other attributes, and incorporate filter criteria into discovery requests. Tag sources for APs can originate from static configuration, the AP filter engine, per-AP Plug and Play (PnP), or default configuration. The AP filter feature determines tag precedence, ensuring the correct tags are assigned according to organizational policies.

You cannot disable the AP filter feature. However, you can configure the priority of tag sources using the **ap filter-priority <priority> <filter-name>** command.

You can specify tag names at the PnP server (similarly to Flex groups or AP groups). During AP discovery and join requests, the AP stores and sends the allocated tag name as part of the request, allowing for automated and dynamic tag assignment.

### Analogy: ticket sorting gate

An AP filter is like a ticket sorting gate at an event venue. Each attendee (AP) presents information at the entrance, and the sorting gate (filter) checks their details to assign them to the right group or area (tag source) based on predefined criteria and priorities. Just as event organizers use sorting gates to efficiently direct attendees, network administrators use AP filters to efficiently assign tags and manage APs in large wireless environments.

# Set tag priority (GUI)

Set the order of priority for tag sources in AP configuration using the GUI

Use this task whenever you want to control which tag source is applied first to your AP configurations in the system. This helps ensure the desired tag assignment behavior.

### Procedure

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

**Step 2** Drag and drop the tag sources to change priorities.

The system saves and applies the new tag source priority for AP configuration.

# Set tag priority

Resolve ambiguity in tag assignment by defining the priority of tag sources for access points.

- 

When an AP joins the wireless controller, it picks up tags from multiple sources. Setting tag source priorities ensures APs use tags from the preferred source. If you do not configure precedence, default priorities are used.

**Procedure**

**Step 1** Enter the global configuration mode.

**Example:**

```
Device# configure terminal
```

**Step 2** (Optional) Configure AP tag source priority. Default priorities for Static, Filter, and PnP.

**Example:**

```
Device(config)# ap tag-source-priority 2 source pnp
```

**Step 3** Exit configuration mode and return to privileged EXEC mode.

**Example:**

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

**Step 4** Revalidate AP tag sources. The priorities become active only after this command is run.

**Example:**

```
Device# ap tag-sources revalidate
```

**Note**
If you change the priorities for Filter and PnP, and need to verify the changes, run the **revalidate** command.

The controller applies the new tag source priorities, and APs assign tags based on your configured precedence.

# Create an AP filter (GUI)

Define an AP filter to automatically apply tags to APs that match specific naming patterns.

Use this task to organize and manage access points by creating filter rules based on AP names and assigning tags for policy, site, or RF profiles.

**Procedure**

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

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

**Step 3** In the **Associate Tags to AP** dialog box that is displayed, enter the **Rule Name** , the **AP name regex** , and the **Priority** .

**Step 4** (Optional) You can also choose the policy tag from the **Policy Tag Name** drop-down list, the site tag from the **Site Tag Name** drop-down list and the RF tag from the **RF Tag Name** drop-down list.

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

The AP filter is created. Any AP that matches the specified pattern is automatically assigned the designated tags.

# Create an AP filter (CLI)

Configure an AP filter using the CLI to apply specific policy, RF, and site tags to APs matching a name pattern.

- Identify the regular expression pattern for the AP names you want to filter.
- Determine the appropriate policy, RF, and site tag names to use.

### Procedure

**Step 1** Enter the global configuration mode.

**Example:**

```
Device# configure terminal
```

**Step 2** Configure an AP filter.

**Example:**

```
Device(config)# ap filter filter-1
```

**Step 3** Configure the AP filter based on regular expression.

**Example:**

```
Device(config-ap-filter)# ap name-regex testany
```

For example, if you have named an AP as **ap-lab-12**, then you can configure the filter with a regular expression, such as **ap-lab-\d+** , to match the AP name.

**Step 4** Configure a policy tag for this filter.

**Example:**

```
Device(config-ap-filter)# tag policy pol-tag1
```

**Step 5** Configure an RF tag for this filter.

**Example:**

```
Device(config-ap-filter)# tag rf rf-tag1
```

**Step 6** Configure a site tag for this filter.

**Example:**

```
Device(config-ap-filter)# tag site site1
```

**Step 7** Exit configuration mode to return to privileged EXEC mode.

**Example:**

```
Device(config-ap-filter)# end
```

The AP filter is configured with the specified criteria and tag associations. APs with names matching your pattern will have the corresponding tags applied.

# Configure filter priority (GUI)

Configure and manage the priority of AP filters to control tag associations on APs.

Perform this task when you need to add a new AP filter or change the priority of an existing AP filter using the GUI.

### Procedure

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

**Step 2** Choose:

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

b) To update the priority of an existing AP filter, click on the filter and in the **Edit Tags** dialog box and change the **Priority**. In case the filter is inactive, you cannot configure a priority. Click **Update and Apply to Device**.

The AP filter priority is configured or updated and applied to the specified devices.

# Configure filter priority (CLI)

Configure and manage the priority of AP filters to control tag associations on APs.

Perform this task when you need to add a new AP filter or change the priority of an existing AP filter using the GUI.

### Procedure

**Step 1** Enter global configuration mode.

**Example:**

```
Device# configure terminal
```

**Step 2** Configure AP filter priority. Valid values range from zero to 1023. The value zero represents the highest priority.

**Example:**

```
Device(config)# ap filter priority 10 filter-name test1
```

This step is necessary to activate the filter.

**Step 3** Exit configuration mode and return to privileged EXEC mode.

**Example:**

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

The AP filter priority is configured or updated and applied to the specified devices.

# Verify AP filter configuration

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

To view the tag source priorities, use the command:

```
Device# show ap tag sources

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

To view the available filters, use the command:

```
Device# show ap filter all

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

filter1                  testany
```

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

```
Device# show ap filters active

Priority   Filter Name       regex          Policy Tag              RF Tag
Site Tag
-------------------------------------------------------------------------------------------------------------
10         test1             testany
site1
```

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

```
Device# show ap tag summary

Number of APs: 4

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

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

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

# Configuring Access Point for Location Configuration

## Location configuration

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

A location is a network entity that

- represents a site or physical area where one or more APs are deployed
- associates a specific set of tags—policy, RF, and site tags—with those APs, and
- links each tag set to a collection of Ethernet MAC addresses corresponding to APs at that location.

### Location features and usage

Locations serve as a new tag source within the tag resolution scheme, functioning similarly to static tag sources. During location configuration, you can

- configure a site or location for an AP
- assign a set of tags for the location, and
- add APs to the location.

The combination of unique tags and associated MAC addresses distinguishes each location and enables organized network management.

## Restriction for location configuration

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

## Configure a location for an AP (GUI)

Create and classify a new location for an AP. Apply the appropriate type and client density settings.

Use this task when you need to add a location for AP deployment and associate location-specific policies or tags.

**Before you begin**

When you create local and remote sites in the basic setup workflow, the corresponding policies and tags are created automatically. Tags and policies created in the basic setup cannot be modified using the advanced workflow. Similarly, items created with the advanced workflow cannot be changed in the basic setup.

**Procedure**

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

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

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

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

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

**Step 6** Click **Apply**.

The new location is saved and ready for assignment and policy application.

# Configure a location for an AP (CLI)

Assign and configure a location for an AP using CLI commands.

Use this task to logically organize APs by location for better device management and policy assignment.
**Before you begin**

Confirm the AP is registered and operational.

**Procedure**

**Step 1** Enter global configuration mode.

**Example:**

```
Device# configure terminal
```

**Step 2** Configure a location for an AP.

**Example:**

```
Device(config)# ap location name location1
```

Run the **no** form of this command to remove location for an AP.

**Step 3** Configure tags for the location.

**Example:**

```
Device(config-ap-location)# tag policy policy_tag

Device(config-ap-location)# tag rf rf_tag

Device(config-ap-location)# tag site site_tag
```

**Step 4** Add description to the location.

**Example:**

```
Device(config-ap-location)# location description
```

**Step 5** Return to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

**Example:**

```
Device(config-ap-location)# end
```

The AP location is set and the associated tags and a description are configured.

# Add an AP to location (GUI)

Add an AP to a specific location using the GUI.

Use this task to associate APs with a defined location, which enables accurate AP count and location tagging in the GUI. Ensure the AP tag source is set to **location** for correct display—if needed, run the **no ap** *ap-mac* command on the controller to reset the AP tag source to default.

**Before you begin**

- Confirm you have the MAC address of the APs to be added.
- Optionally, prepare a CSV file with AP MAC addresses for bulk upload.

**Procedure**

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

**Step 2** In the **Basic Wireless Setup** window, click **Add** to configure these options:

- General
- Wireless Networks
- AP Provisioning

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

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

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

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

The selected APs are added to the specified location, and location tagging is updated in the GUI.

# Adding an Access Point to the Location (CLI)

**Procedure**

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

# Configuring SNMP in Location Configuration

# SNMP

EWC does not support SNMP and does not implement the SNMP MIBs of Cisco Catalyst 9800 Series Wireless Controllers, although EWC might respond to some of the object identifiers (OIDs).

# Verify location configuration

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

```
Device# show ap location summary

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

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

```
Device# show ap location details first
```

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

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

To view the AP tag summary, use the command:

```
Device# show ap tag summary

Number of APs: 4
AP Name      AP Mac           Site Tag Name      Policy Tag Name      RF Tag Name
Misconfigured  Tag Source
-----------------------------------------------------------------------------------------------------
Asim_5-1     005b.3400.02f0   default-site-tag   default-policy-tag   default-rf-tag   Yes
            Filter
Asim_5-2     005b.3400.03f0   default-site-tag   default-policy-tag   default-rf-tag   No
            Default
Asim_5-9     005b.3400.0af0   default-site-tag   default-policy-tag   default-rf-tag   No
            Location
Asim_5-10    005b.3400.0bf0   default-site-tag   default-policy-tag   default-rf-tag   No
            Location
```

# Verify location statistics

To view the AP location statistics, use the command:

```
Device# show ap location stats

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