FlexConnect WLAN with 802.1x AAA override on Catalyst 9800 Wireless Controllers

Contents

Introduction

This document describes how to set up an elastic Wireless LAN controller (9800 WLC) with FlexConnect mode Access Points (APs) and an 802.1x Wireless Local Area Network (WLAN) locally switched with Virtual Local Area Network (VLAN) Authentication, Authorization and Accounting (AAA) override.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- 9800 WLC configuration mode
- FlexConnect

Components Used

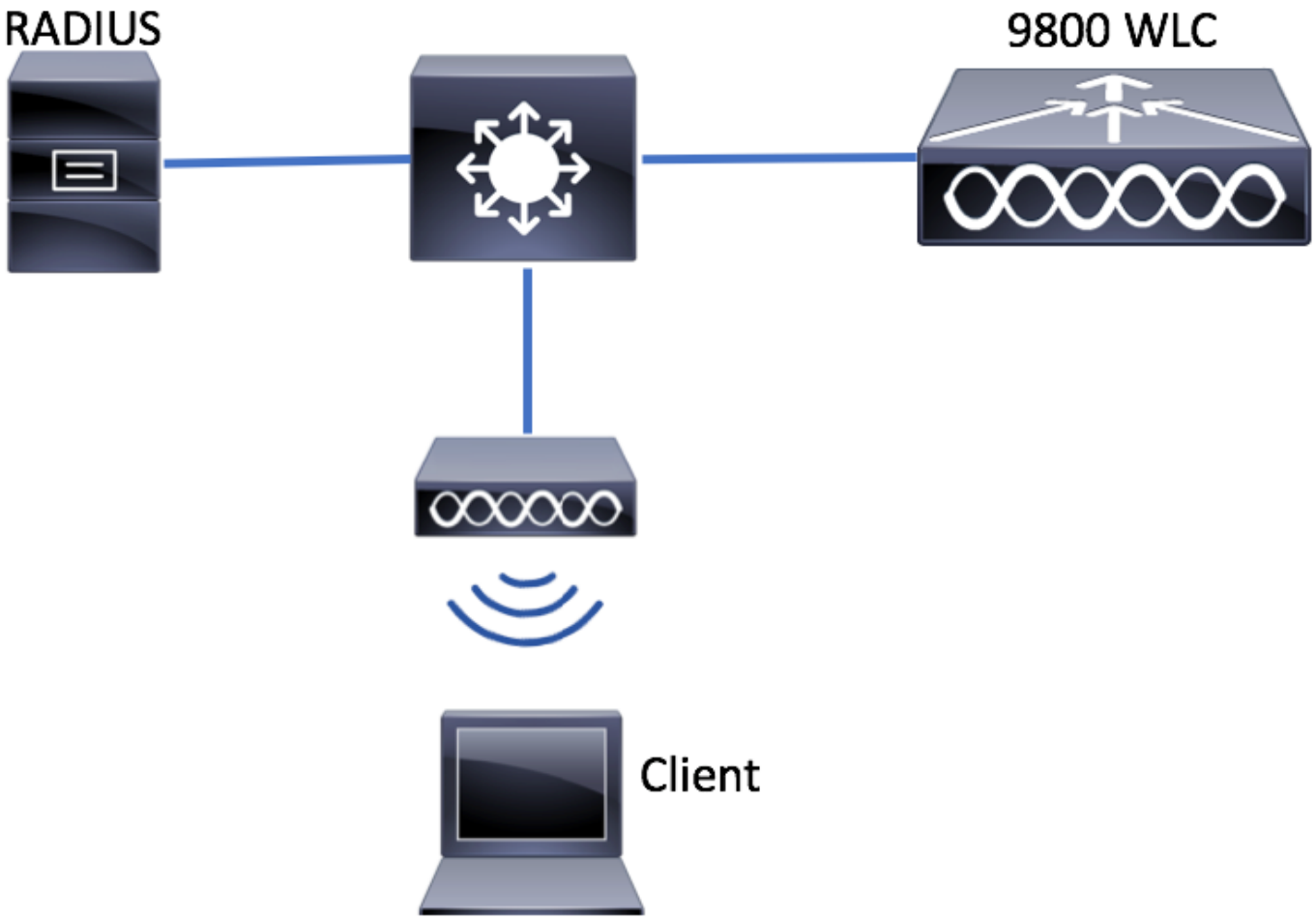
The information in this document is based on these software and hardware versions:

- 9800 WLC v16.10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram



Configuration

AAA Configuration on 9800 WLC

You can follow the instructions from this link:

AAA Configuration on 9800 WLC

WLAN Configuration

You can follow the instructions from this link:

WLAN Configuration

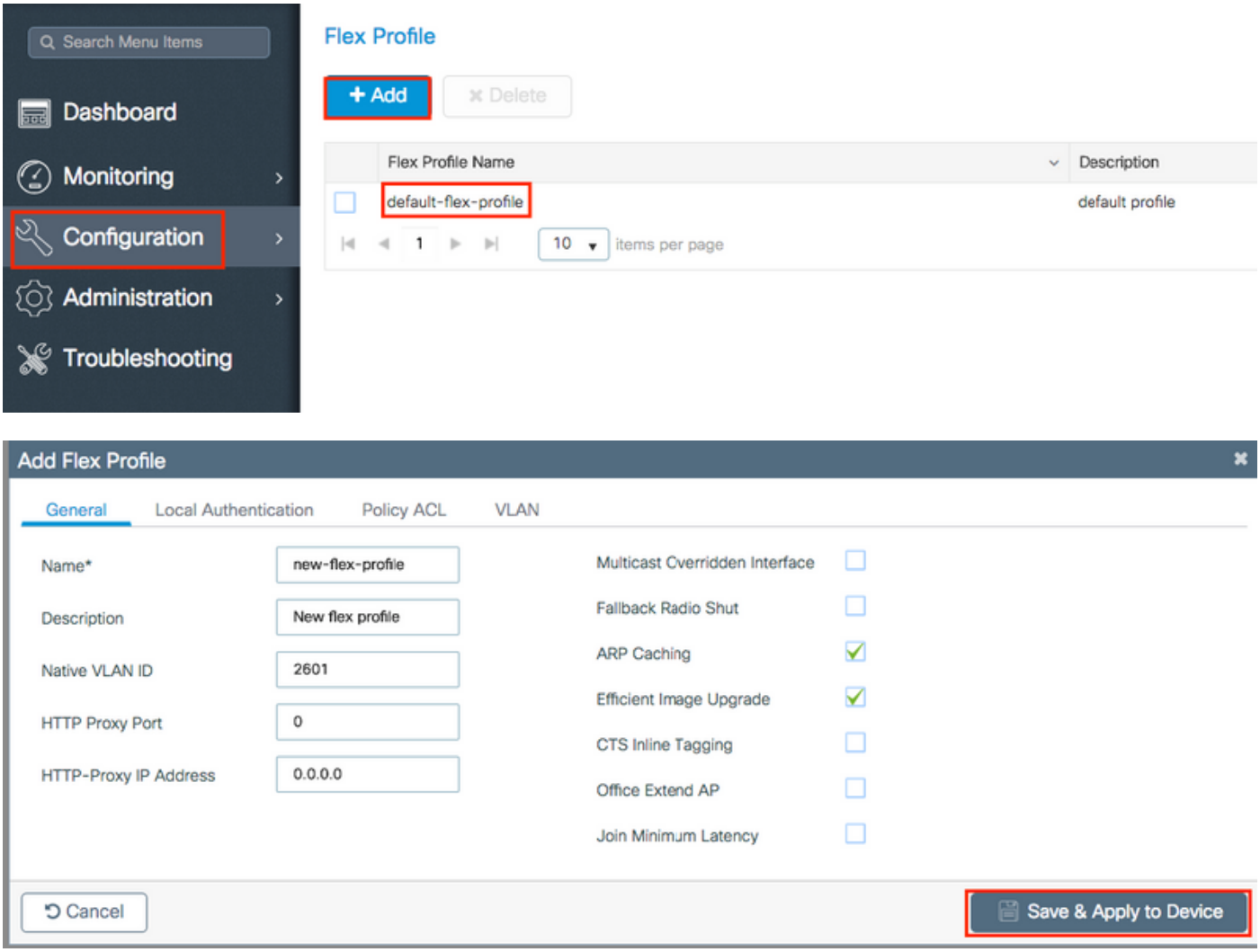
Set AP as FlexConnect mode

Unlike AireOS configuration, on 9800 WLC it is not possible to configure the AP local or flexconnect mode directly from the AP. Follow these steps to configure an AP in FlexConnect mode.

GUI

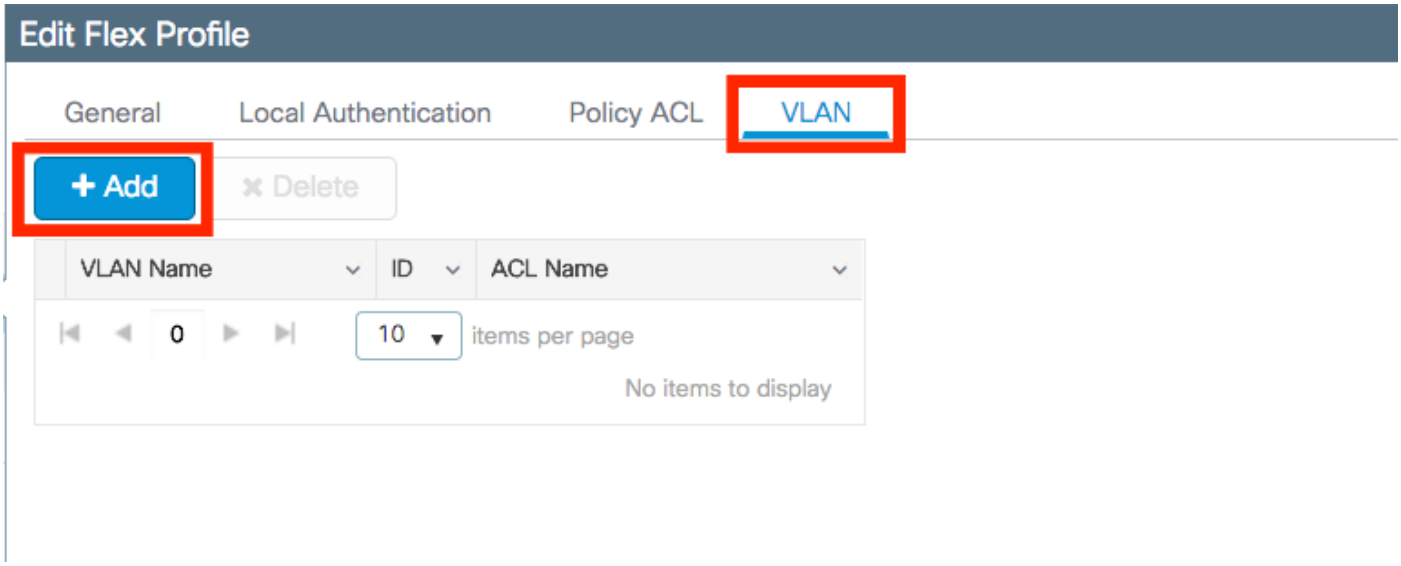
Step 1. Configure a Flex Profile.

Navigate to **Configuration > Tags & Profiles > Flex** and either modify the **default-flex-profile** or click **+Add** to create a new one.

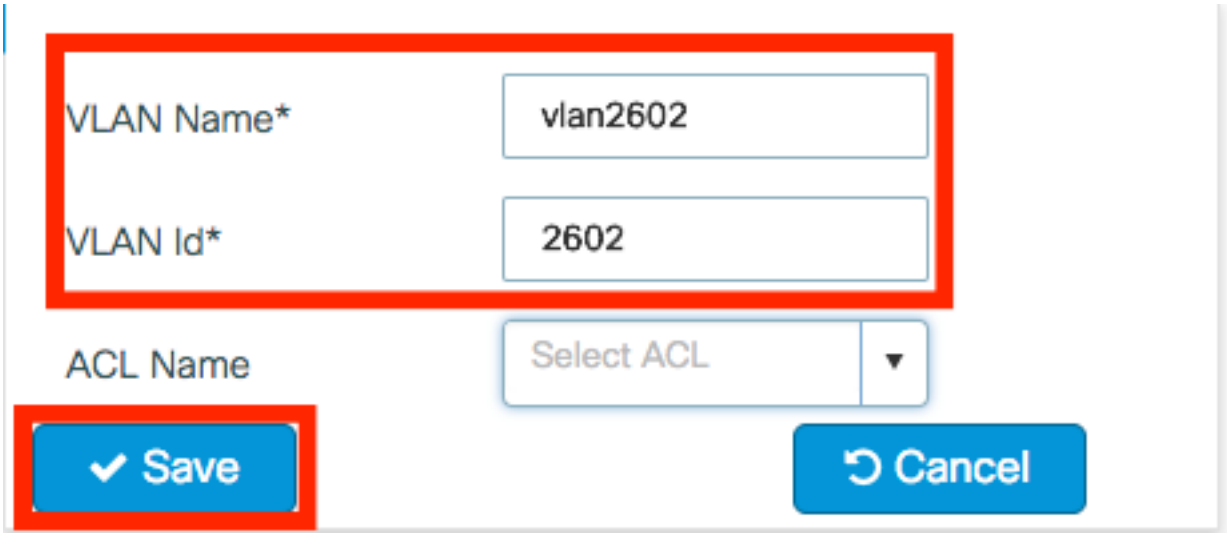


Step 2. Add the needed VLANs (both the default WLAN's VLANs or the VLANs pushed from ISE).

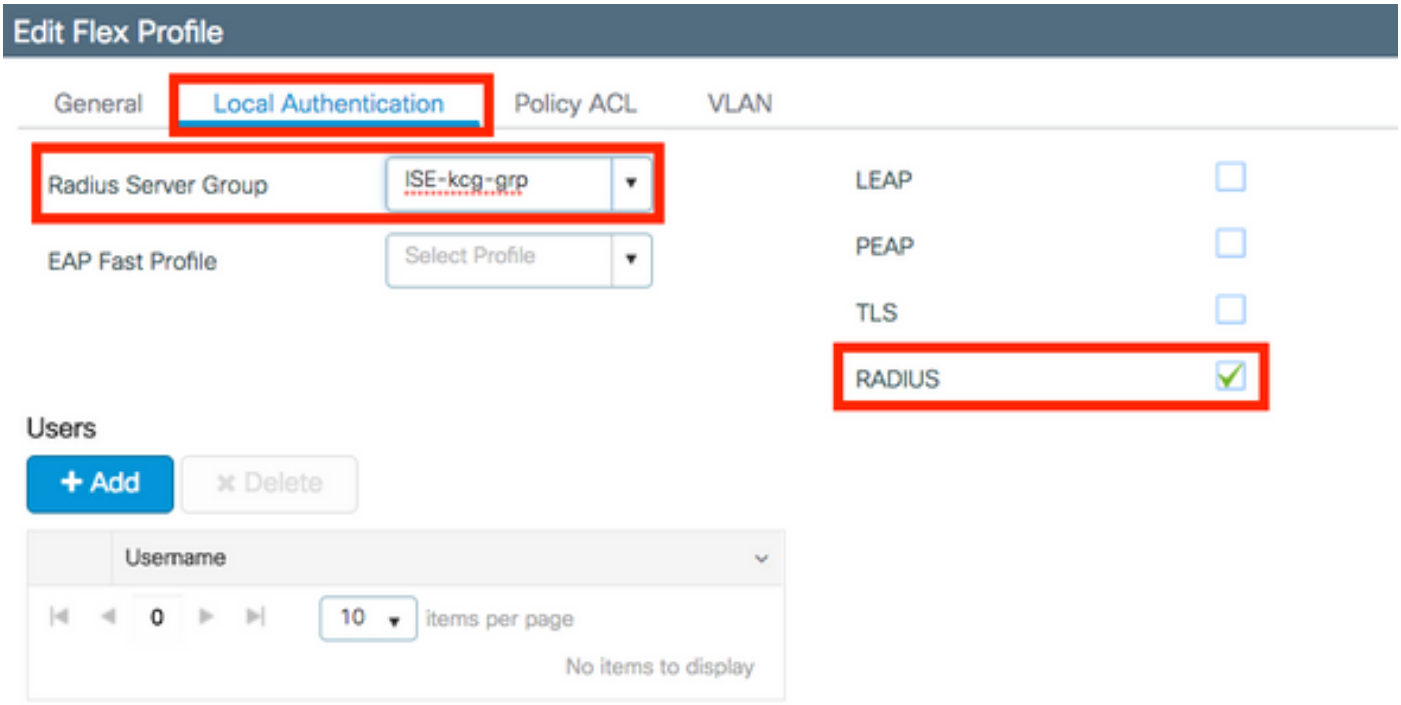
> **Note**: At step 3 of section **Policy Profile Configuration**, you select the default VLAN assigned to the SSID. If you use a VLAN name on that step, ensure that you use the same vlan name on the Flex Profile configuration, otherwise clients won't be able to connect to the WLAN.



You can optionally add specific ACLs per VLAN.

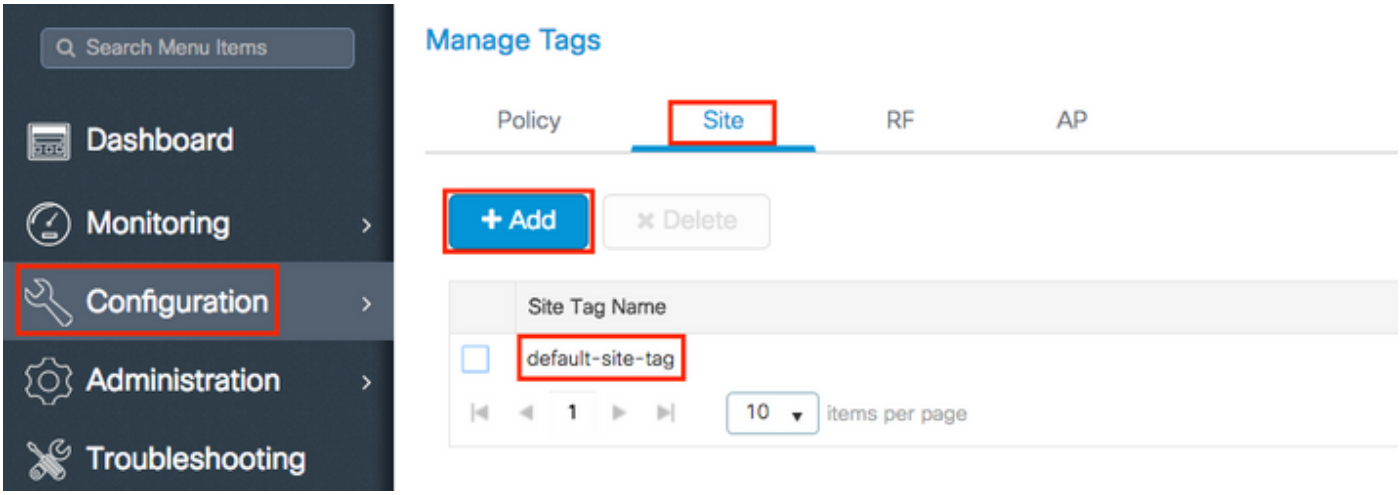


Optionally, assign a Radius server group to allow the FlexConnect APs perform local authentication.



Step 3. Configure a Site Tag.

Navigate to **Configuration > Tags & Profiles > Tags > Site.** Either modify the **default-site-tag** (which is the tag assigned by default to all the APs) or create a new one (Click **+Add** to create a new one).

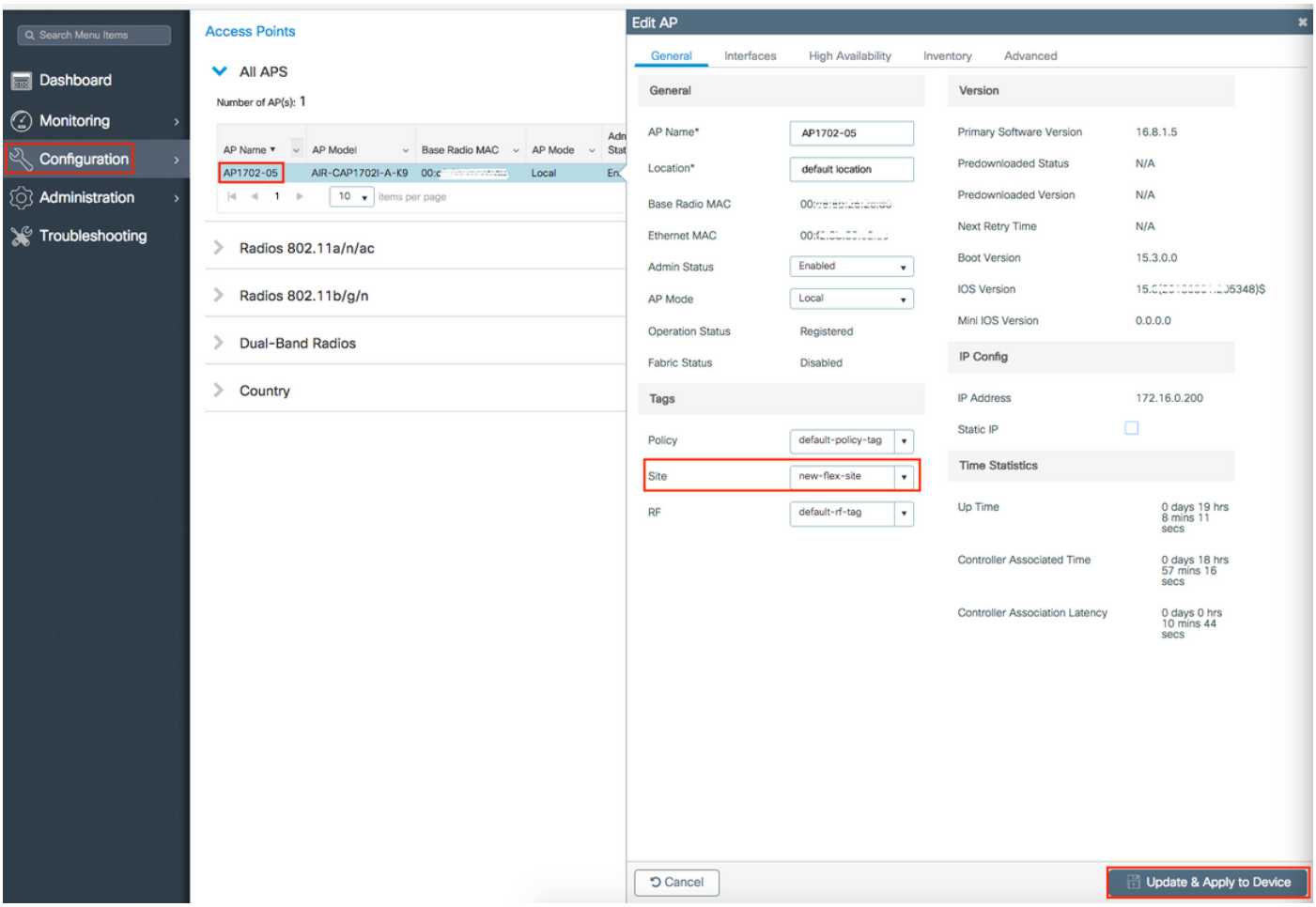


Ensure you disable **Enable Local Site** option, otherwise the **Flex Profile** option is not available.

Note: Any AP that gets a Site Tag with **Enable Local Site** enabled, is configured as local mode. Likewise, any AP that gets a Site Tag with **Enable Local Site** disabled, is configured as flexconnect mode.

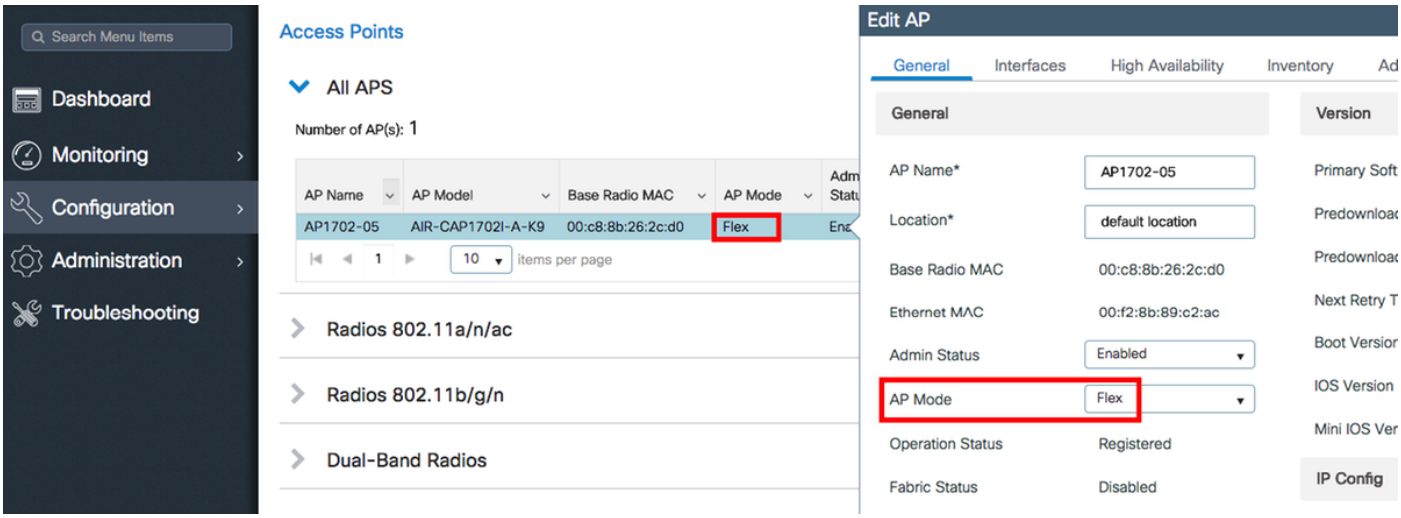
Step 4. Make an AP associate to the 9800 WLC and assign the Site tag configured on Step 2.

Navigate to **Configuration > Wireless > Access Points > AP name** and set the Site tag. Then click **Update & Apply to Device** to set the change.



Note: Be aware that after change the tag on an AP, it loses its association to the 9800 WLC and join back within about 1 minute.

Step 5. Once the AP joins back, notice the AP mode is Flex



CLI

```
# config t
# wireless profile flex new-flex-profile
# arp-caching
# description "New flex profile"
# native-vlan-id 2601

# config t
# wireless tag site new-flex-site
# flex-profile new-flex-profile
# no local-site
# site-tag new-flex-site

# config t
# ap <eth-mac-address>
# site-tag new-flex-site
Associating site-tag will cause associated AP to reconnect
# exit

#show ap name <ap-name> config general | inc AP Mode
AP Mode                                         : FlexConnect
```

Switch Configuration

Configure the switch's interface to which the AP is connected to.

```
# config t
# interface <int-id>
# switchport trunk native vlan 2601
# switchport mode trunk
# spanning-tree portfast trunk
# end
```

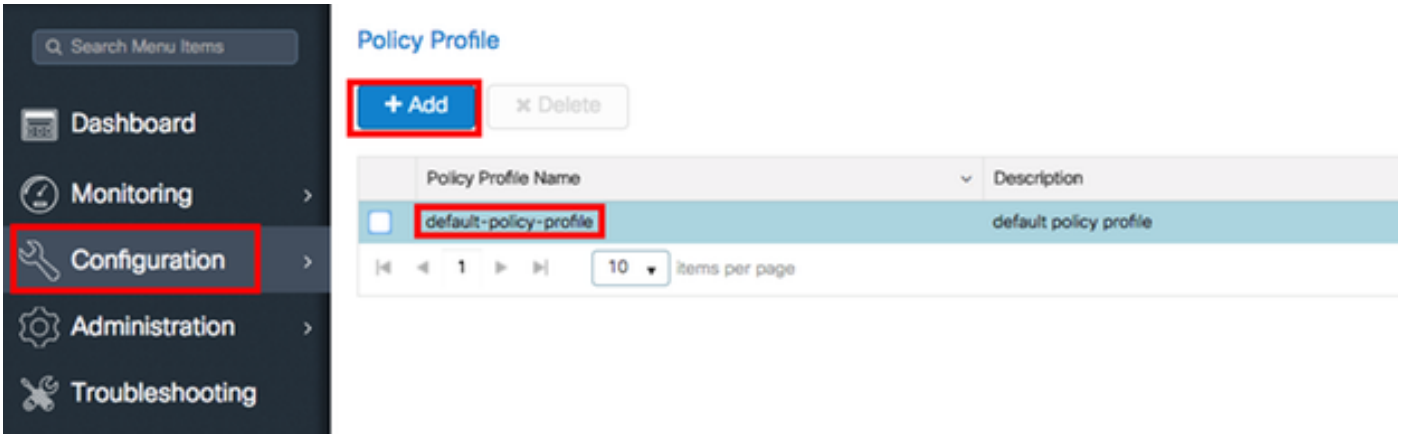
Policy Profile Configuration

Inside a Policy Profile you can decide to which VLAN assign the clients, among other settings (like Access Controls List [ACLs], Quality of Service [QoS], Mobility Anchor, Timers and so on).

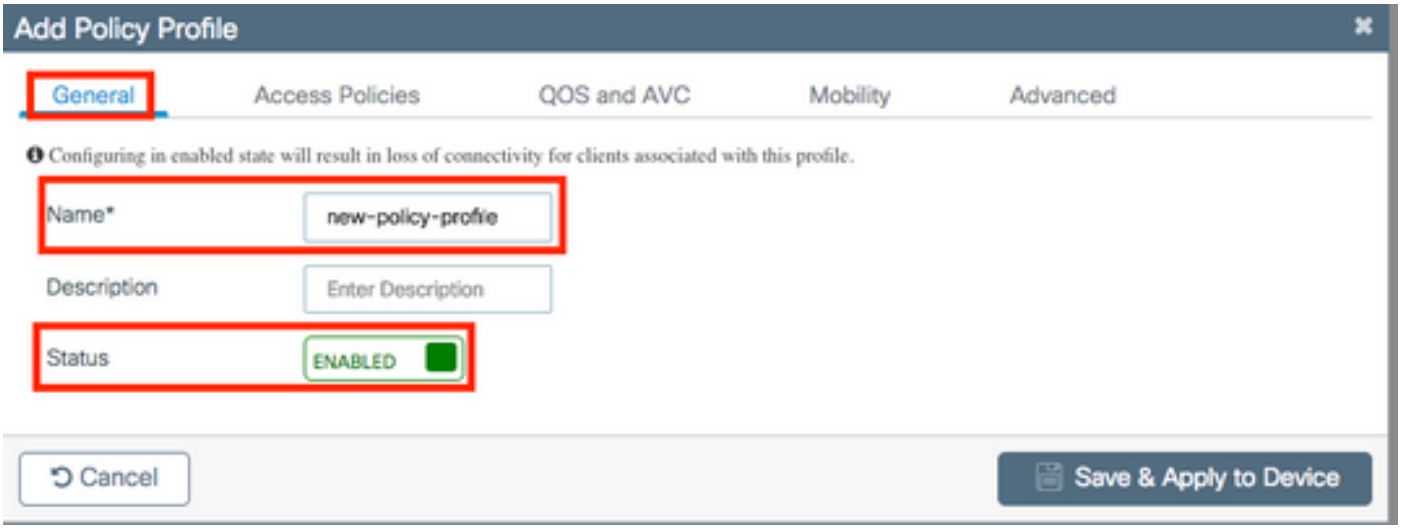
GUI

Step 1. Configure the Policy Profile to be assigned to the WLAN.

Navigate to **Configuration > Tags & Profiles > Policy** and either create a new one or modify the **default-policy-profile.**



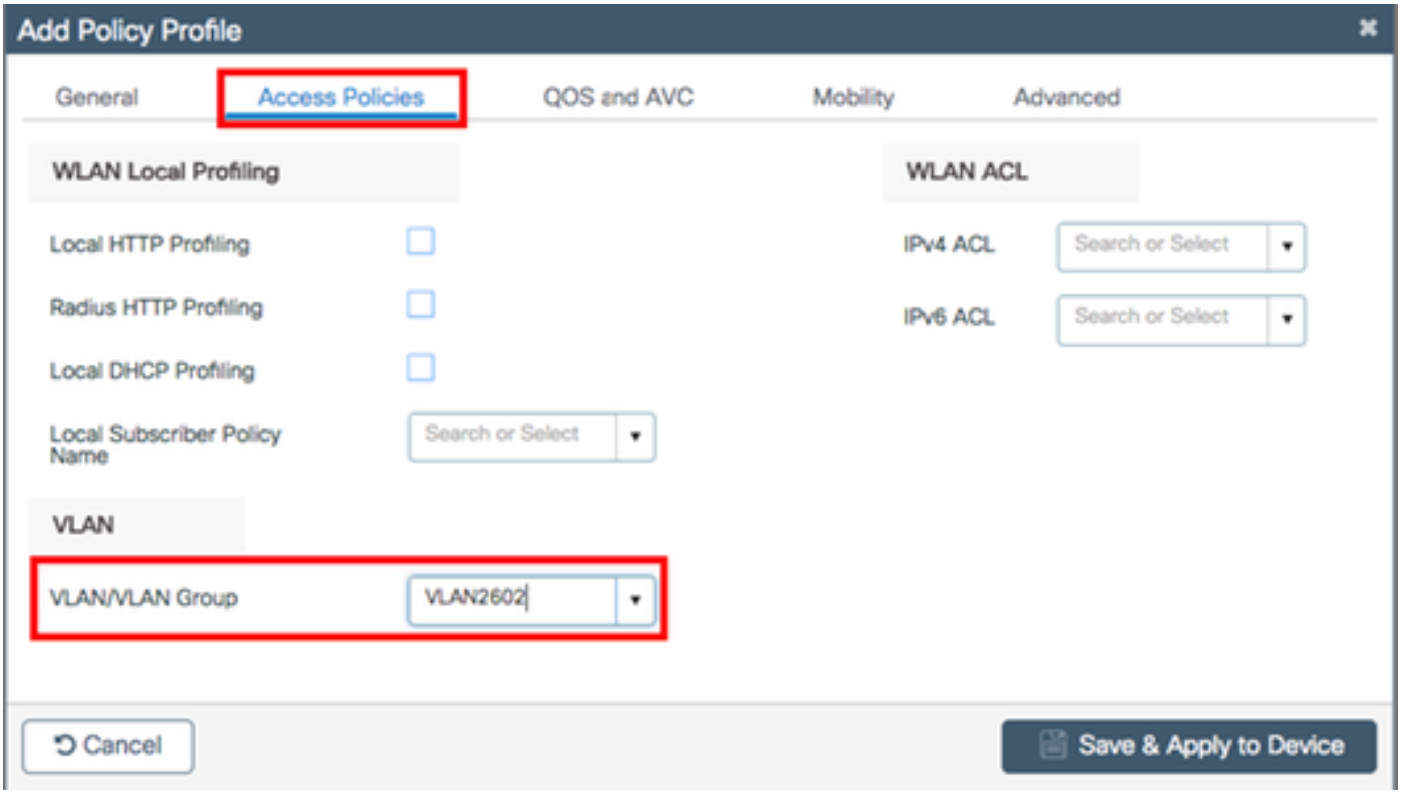
Step 2. From the **General tab,** assign a name to the Policy Profile and change its status to **ENABLED.**



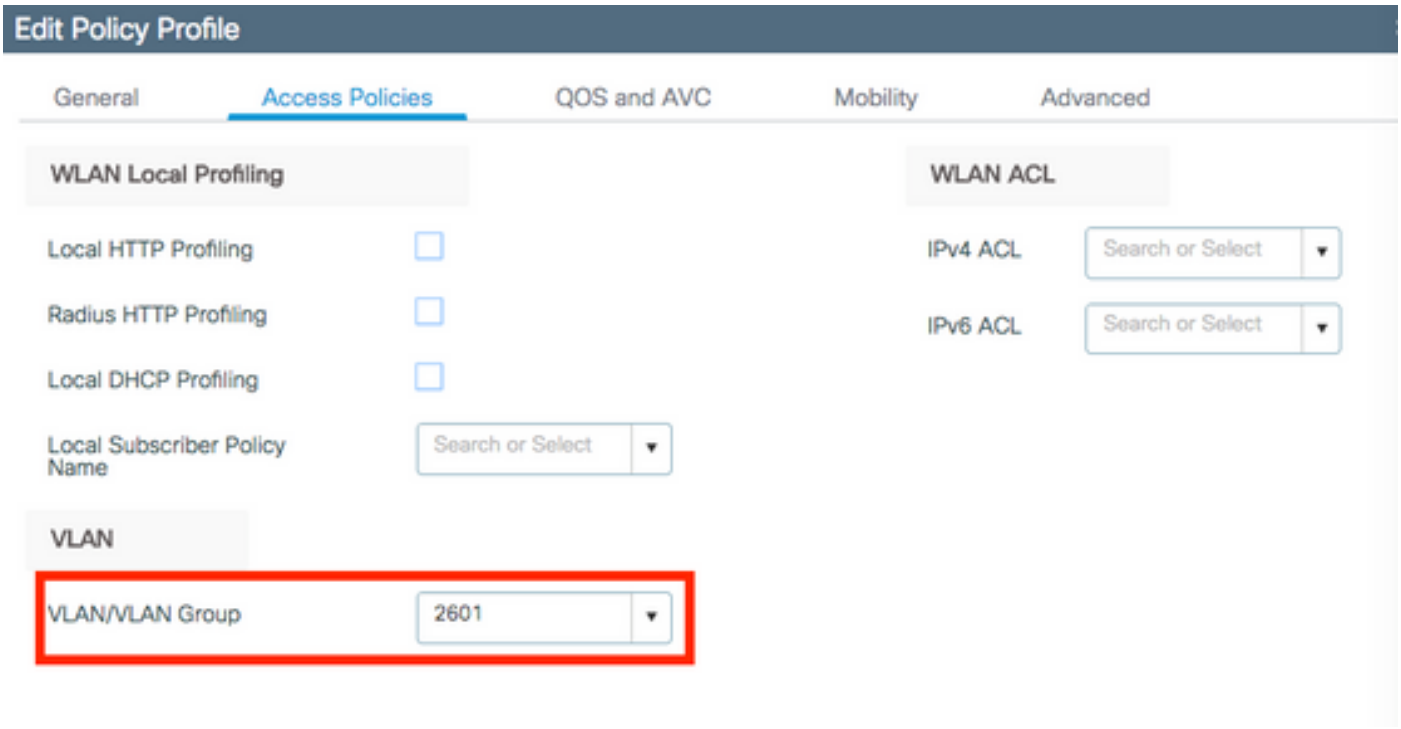
Step 3. From the **Access Policies** tab assign the VLAN to which the wireless clients are assigned when they connect to this WLAN by default.

You can either select one VLAN name from the drop down or manually type a vlan id.

> **Note**: If you select a vlan name from the dropdown, ensure it matches the vlan name used on the step 2 from section **Set AP as FlexConnect mode.**

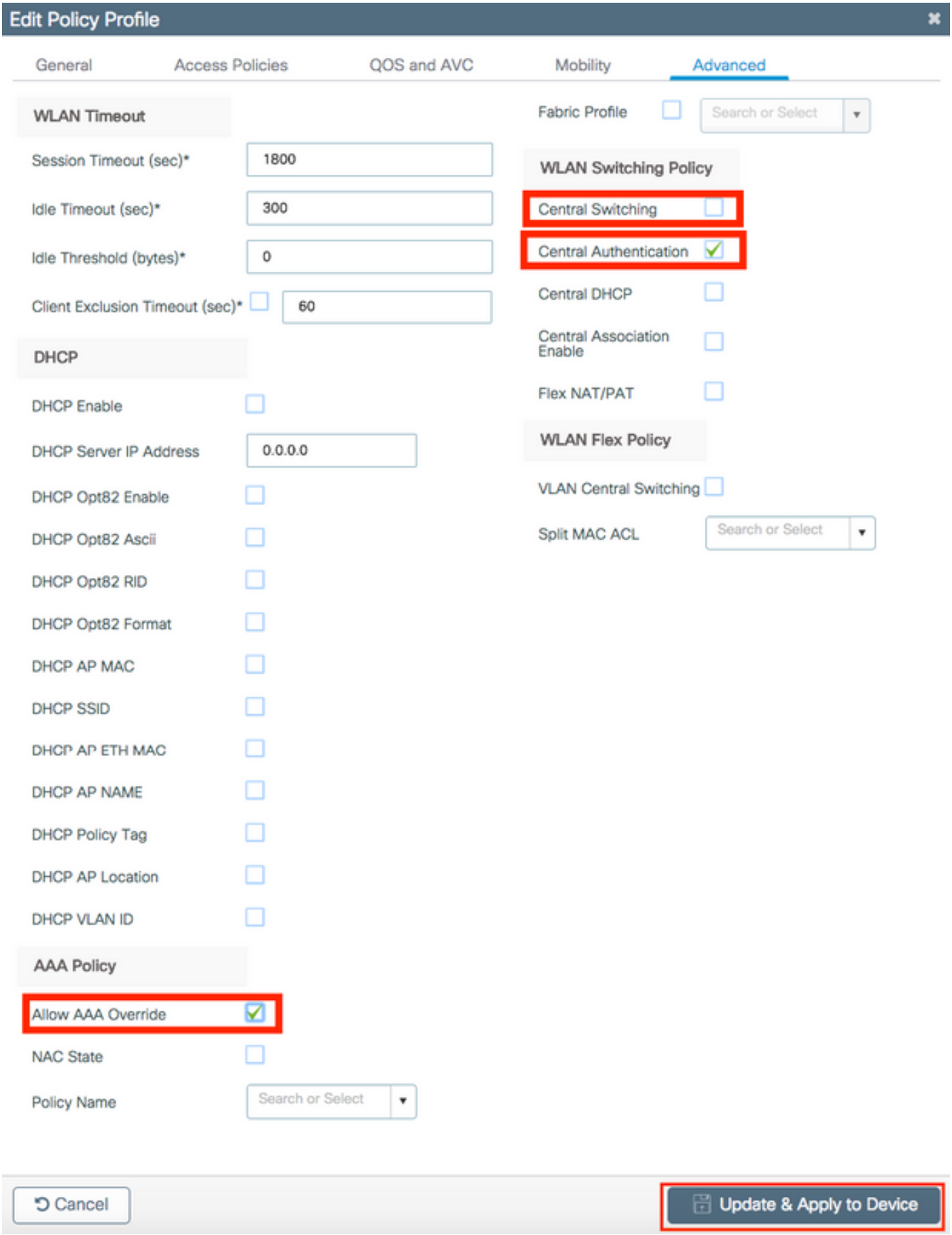


or



Step 4. Navigate to the **Advanced tab** and enable **Central Authentication Enable** and **Allow AAA Override**options**. Central Switching** must be disabled.

Central Authentication must be enabled if you want the authentication process to be performed centrally by the 9800 WLC. Disable it if you want the FlexConnect APs authenticate the wireless clients.



CLI

```
# config t
# wireless profile policy new-policy-profile # central association # vlan <vlan-id or vlan-name>
```

```
# no shutdown
```

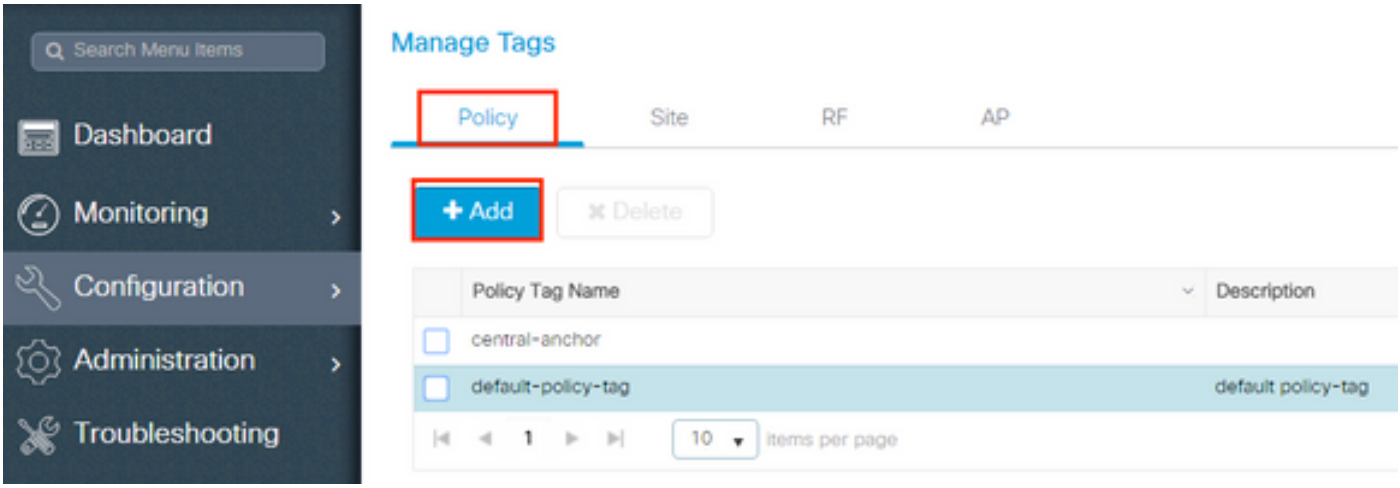
Policy Tag Configuration

Policy Tag is used to link the SSID with the Policy Profile. You can either create a new Policy Tag or use the default-policy tag.

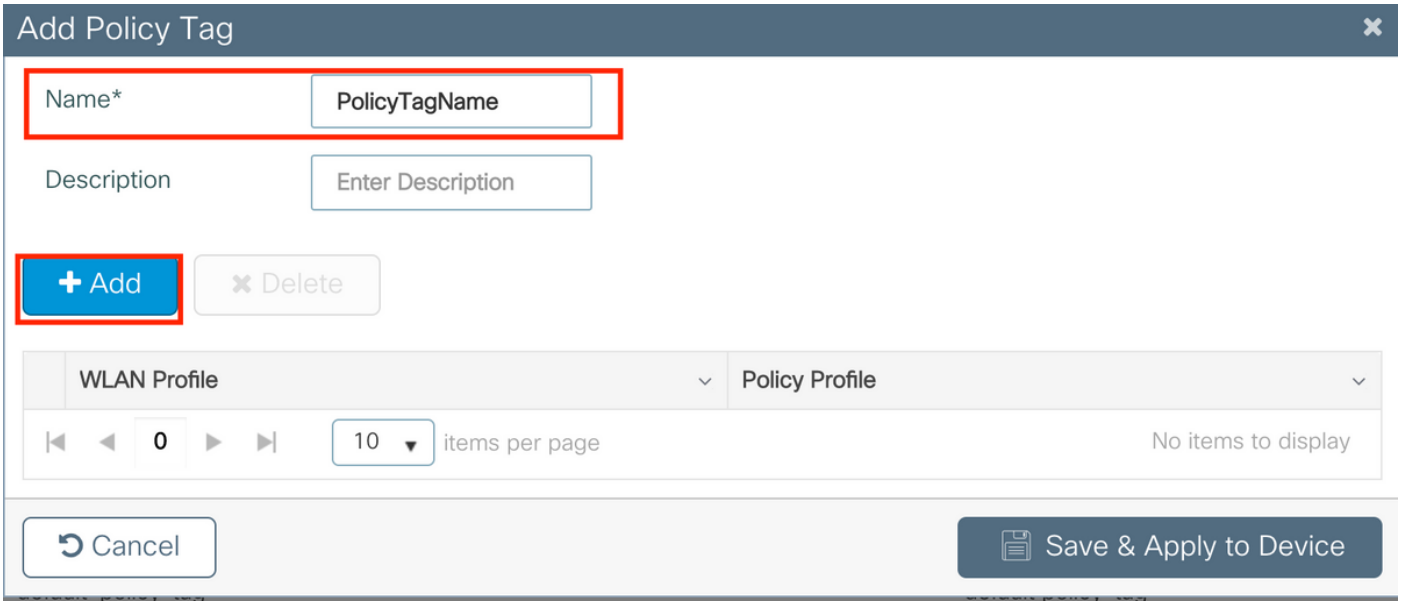
> **Note**: The default-policy-tag automatically maps any SSID with a WLAN ID between 1 to 16 to the default-policy-profile. It cannot be modified nor deleted. If you have a WLAN with ID 17 or higher, the default-policy-tag cannot be used.

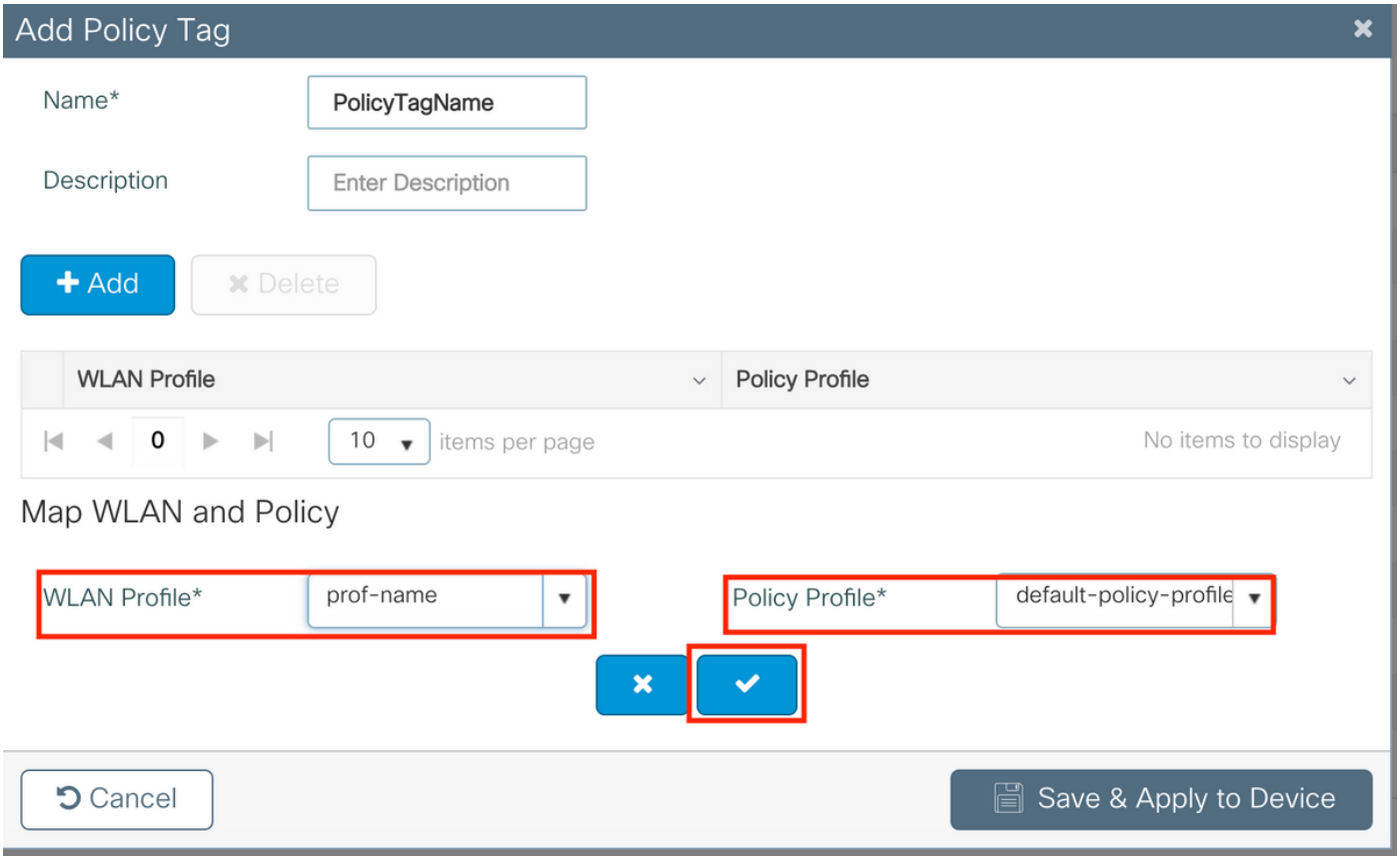
GUI:

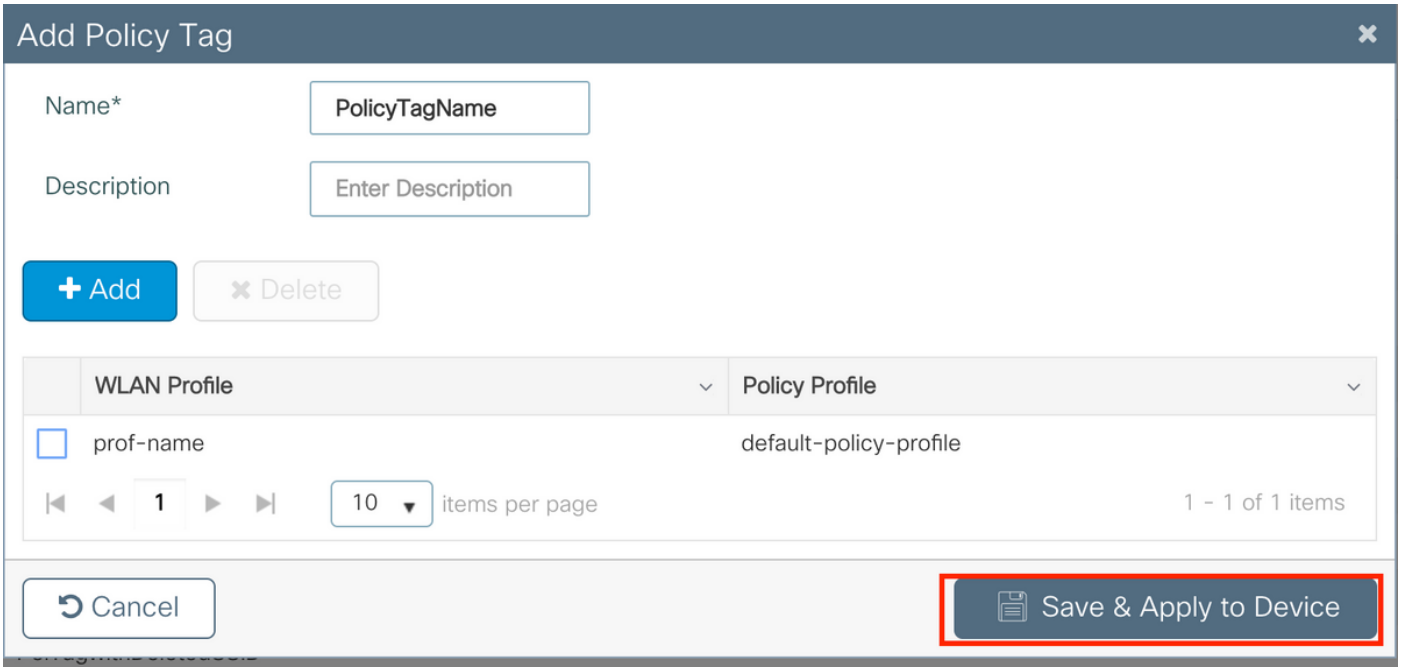
Navigate to **Configuration > Tags & Profiles > Tags > Policy** and add a new one if needed.



Link your WLAN Profile to the desired Policy Profile.







CLI:

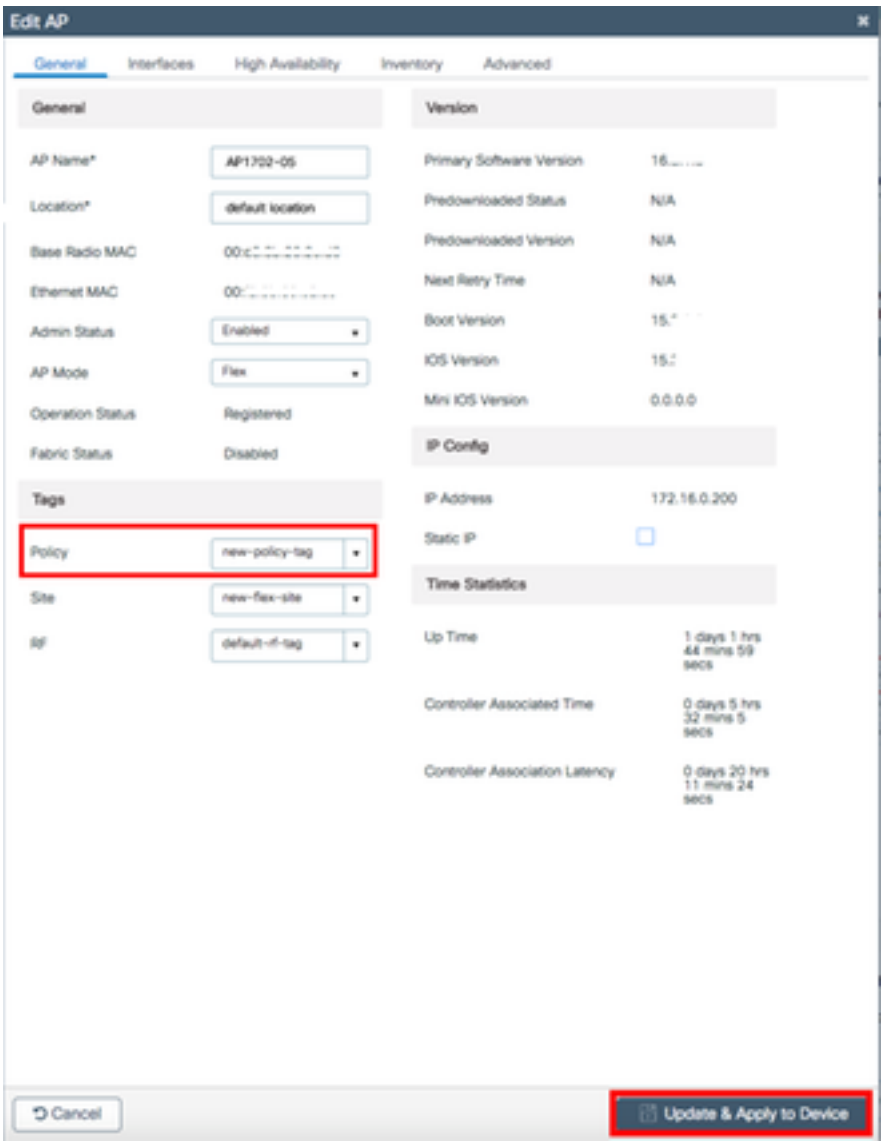
```
# config t
# wireless tag policy <policy-tag-name>
# wlan <profile-name> policy <policy-profile-name>
```

Policy Tag Assignation

Assign the Policy tag to the AP

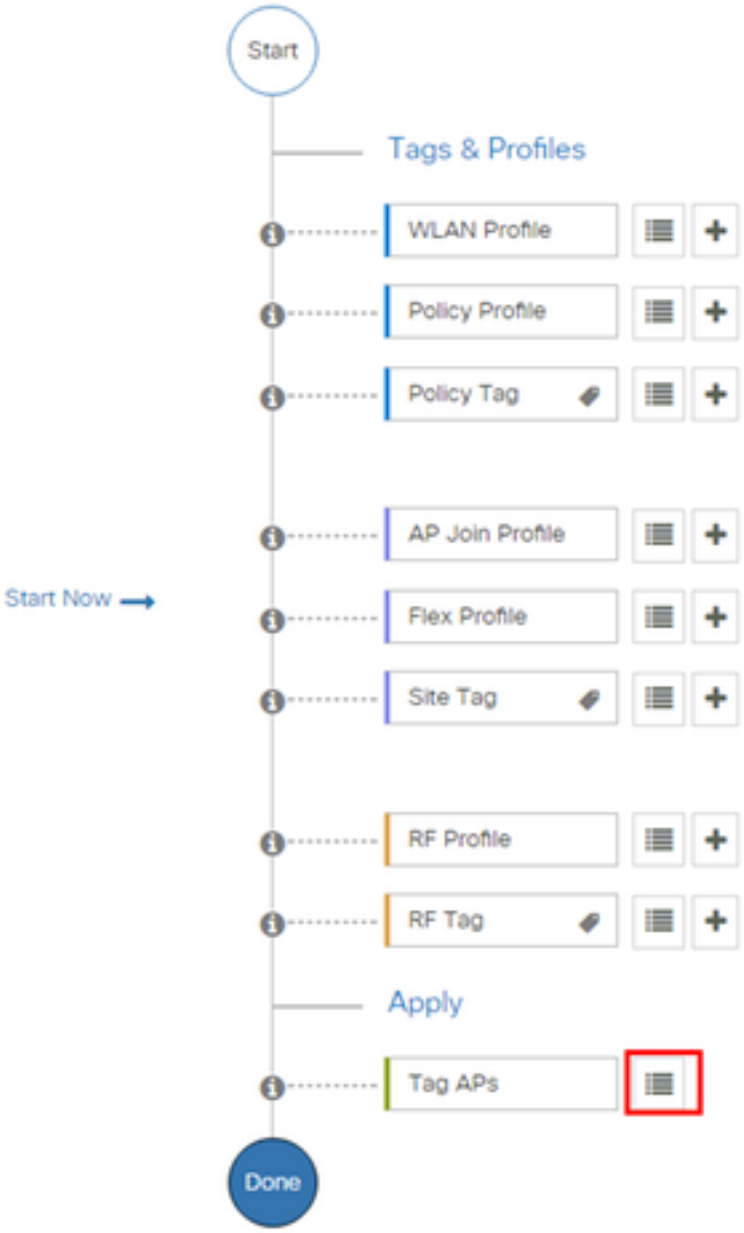
GUI

To assign the tag to one AP navigate to **Configuration > Wireless > Access Points > AP Name > General Tags,** make the needed assignment and then click **Update & Apply to Device.**

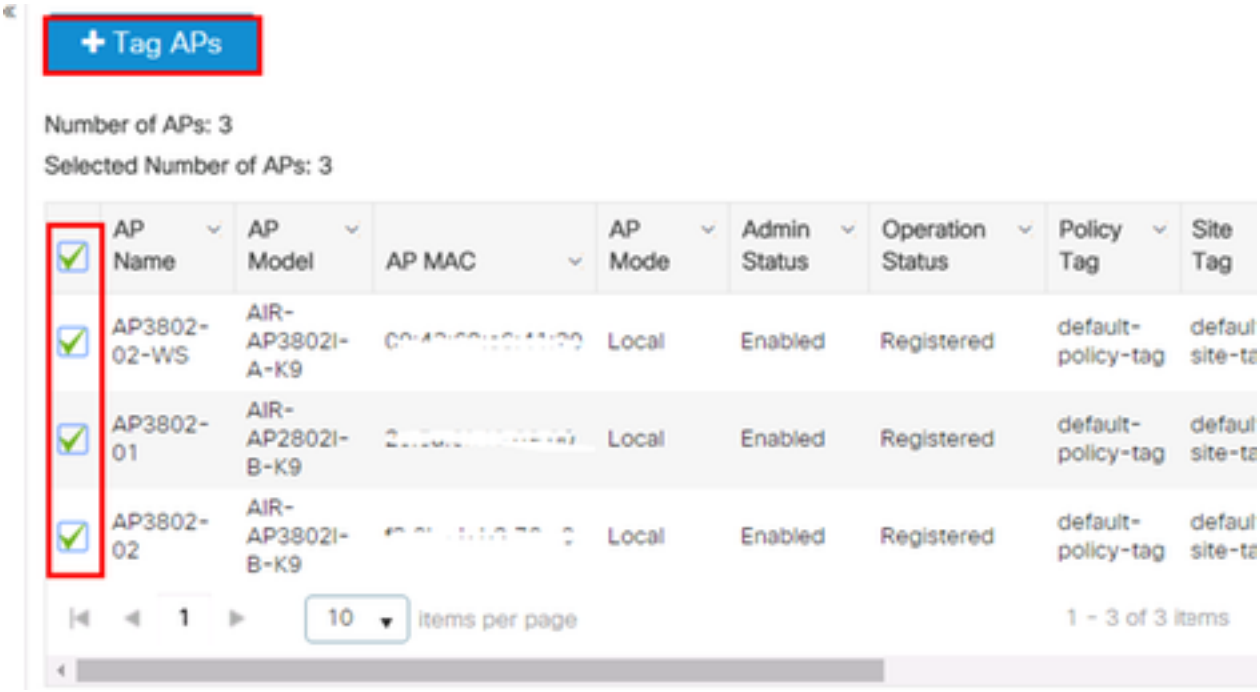


> **Note**: Be aware that after change the policy tag on an AP, it loses its association to the 9800 WLC and join back within about 1 minute.

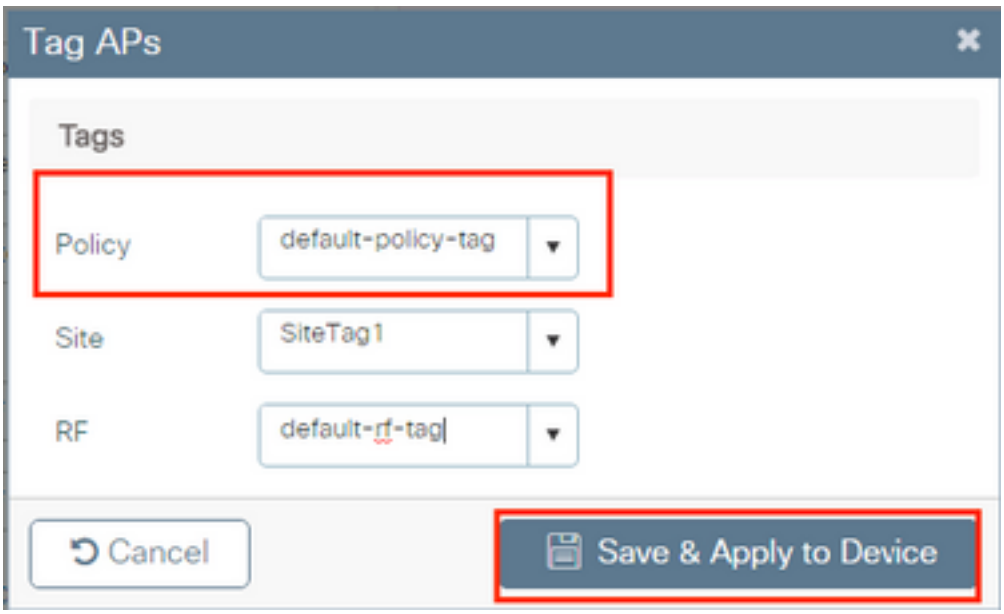
To assign the same Policy Tag to several APs navigate to **Configuration > Wireless > Wireless Setup > Start Now > Apply.**



Select the APs to which you want to assign the tag and click **+ Tag APs**



Select the whished Tag and click **Save & Apply to Device**



CLI

```
# config t
# ap <ethernet-mac-addr>
# policy-tag <policy-tag-name>
# end
```

ISE Configuration

For ISE v1.2 configuration check this link:

ISE Configuration

Verify

You can use these commands to verify current configuration

```
# show run wlan
# show run aaa
# show aaa servers
# show ap config general
# show ap name <ap-name> config general
# show ap tag summary
# show ap name <AP-name> tag detail
# show wlan { summary | id | name | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```

Troubleshoot

WLC 9800 provides ALWAYS-ON tracing capabilities. This ensures all client connectivity related errors, wanring and notice level messages are constantly logged and you can view logs for an incident or failure condition after it has occurred.

> **Note**: Depending on volume of logs being generated, you can go back few hours to several days.

In order to view the traces that 9800 WLC collected by default, you can connect via SSH/Telnet to the 9800 WLC and follow these steps (Ensure you are logging the session to a text file).

Step 1. Check controller's current time so you can track the logs in the time back to when the issue happened.

```
# show clock
```

Step 2. Collect syslogs from the controller's buffer or the external syslog as dictated by the system configuration. This provides a quick view into the system health and errors, if any.

```
# show logging
```

Step 3. Verify if any debug conditions are enabled.

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Tracing Configs:


Packet Infra debugs:

Ip Address                                              Port
------------------------------------------------------|----------
```

> **Note**: If you see any condition listed, it means the traces are being logged up to debug level for all the processes that encounter the enabled conditions (mac address, ip address etc).

This would increase the volume of logs. Therefore, it is recommended to clear all conditions when not actively debugging

Step 4. Assuming mac address under test was not listed as a condition in Step 3, collect the always-on notice level traces for the specific mac address.

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file
always-on-<FILENAME.txt>
```

You can either display the content on the session or you can copy the file to an external TFTP server.

```
# more bootflash:always-on-<FILENAME.txt>
or
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

Conditional Debugging and Radio Active Tracing

If the always-on traces do not give you enough information to determine the trigger for the problem under investigation, you can enable conditional debugging and capture Radio Active (RA) trace, which will provide debug level traces for all processes that interact with the specified condition (client mac address in this case). In order to enable conditional debugging, follow these steps.

Step 5. Ensure there are no debug conditions are enabled.

```
# clear platform condition all
```

Step 6. Enable the debug condition for the wireless client mac address that you want to monitor.

This commands start to monitor the provided mac address for 30 minutes (1800 seconds). You can optionally increase this time to up to 2085978494 seconds.

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

Note: In order to monitor more than one client at a time, run debug wireless mac <aaaa.bbbb.cccc> command per mac address.

Note: You do not see the output of the client activity on terminal session, as everything is buffered internally to be viewed later.

Step 7. Reproduce the issue or behavior that you want to monitor.

Step 8. Stop the debugs if the issue is reproduced before the default or configured monitor time is up.

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

Once the monitor-time has elapsed or the debug wireless has been stopped, the 9800 WLC generates a local file with the name:

ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Step 9. Collect the file of the mac address activity. You can either copy the ra trace .log to an external server or display the output directly on the screen.

Check the name of the RA traces file

```
# dir bootflash: | inc ra_trace
```

Copy the file to an external server:

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
tftp://a.b.c.d/ra-FILENAME.txt
```

Display the content:

```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Step 10. If the root cause is still not obvious, collect the internal logs which are a more verbose view of debug level logs. You do not need to debug the client again as we are only taking a futher detailed look at debug logs that have been already colllected and internally stored.

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> }
to-file ra-internal-<FILENAME>.txt
```

> **Note**: This command output returns traces for all logging levels for all processes and is quite voluminous. Please engage Cisco TAC to help parse through these traces.

You can either copy the ra-internal-FILENAME.txt to an external server or display the output directly on the screen.

Copy the file to an external server:

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

Display the content:

```
# more bootflash:ra-internal-<FILENAME>.txt
```

Step 11. Remove the debug conditions.

```
# clear platform condition all
```

> **Note**: Ensure that you always remove the debug conditions after a troubleshooting session.