Configure 802.1X Authentication on Catalyst 9800 Wireless Controller Series

Contents

Introduction

This document describes how to set up a WLAN with 802.1X security on a Cisco Catalyst 9800 Series Wireless Controller.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- 802.1X

Components Used

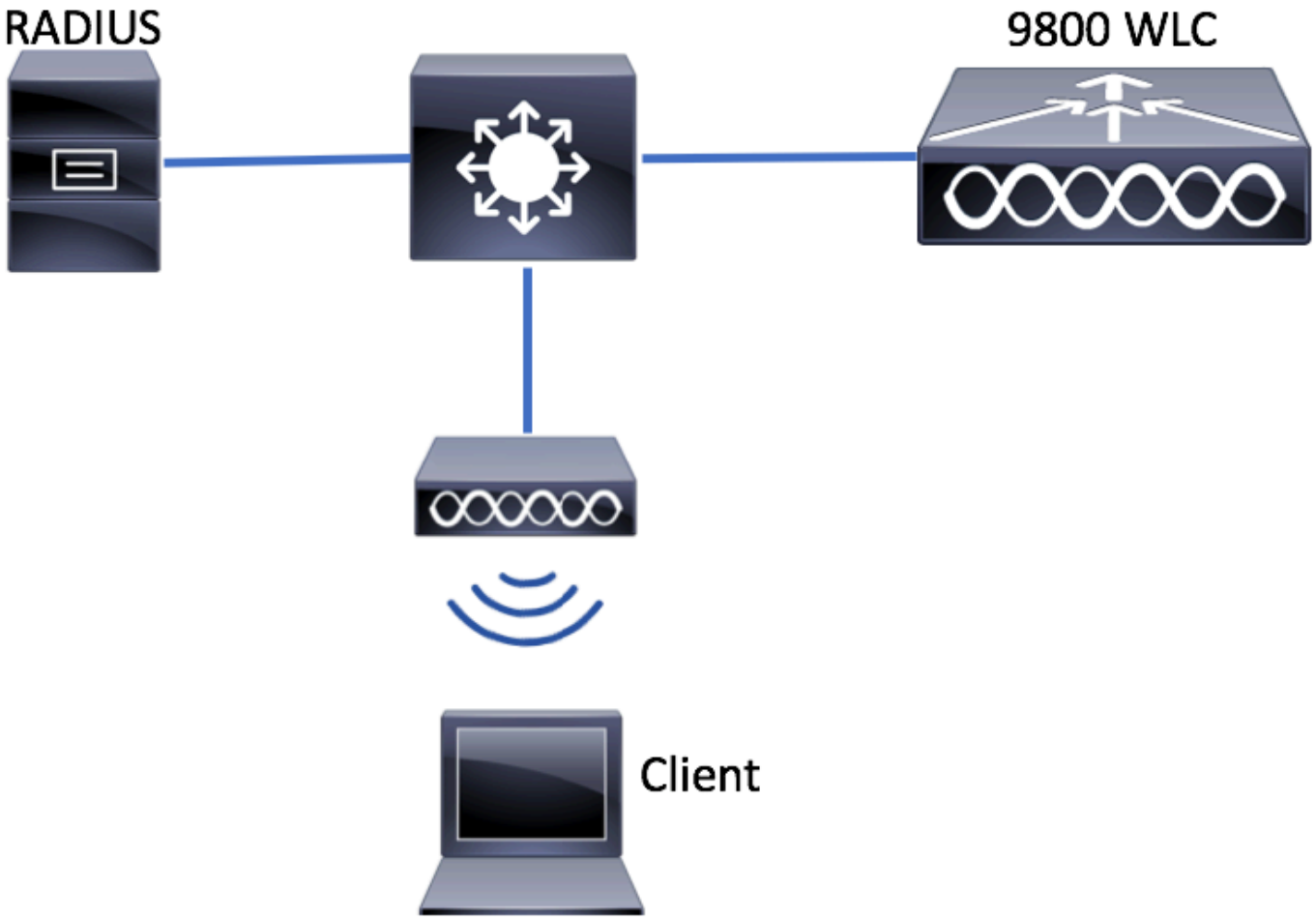
The information in this document is based on these software and hardware versions:

- Catalyst 9800 Wireless Controller Series (Catalyst 9800-CL)
- Cisco IOS® XE Gibraltar 17.3.x
- Cisco ISE 3.0

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

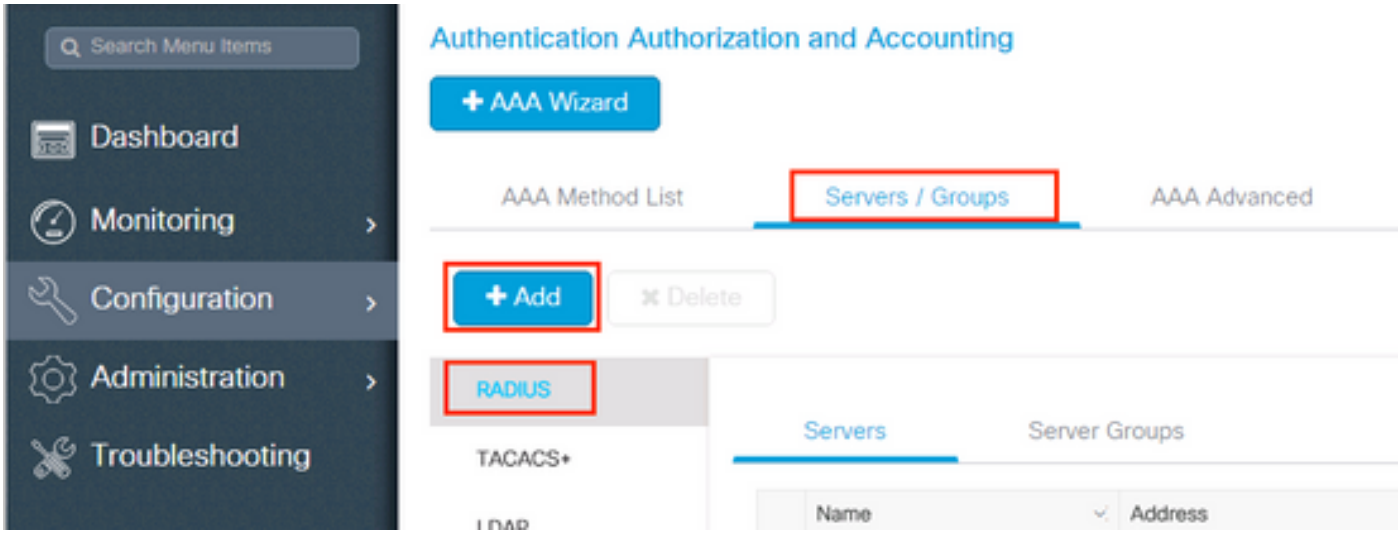


WLC Configuration

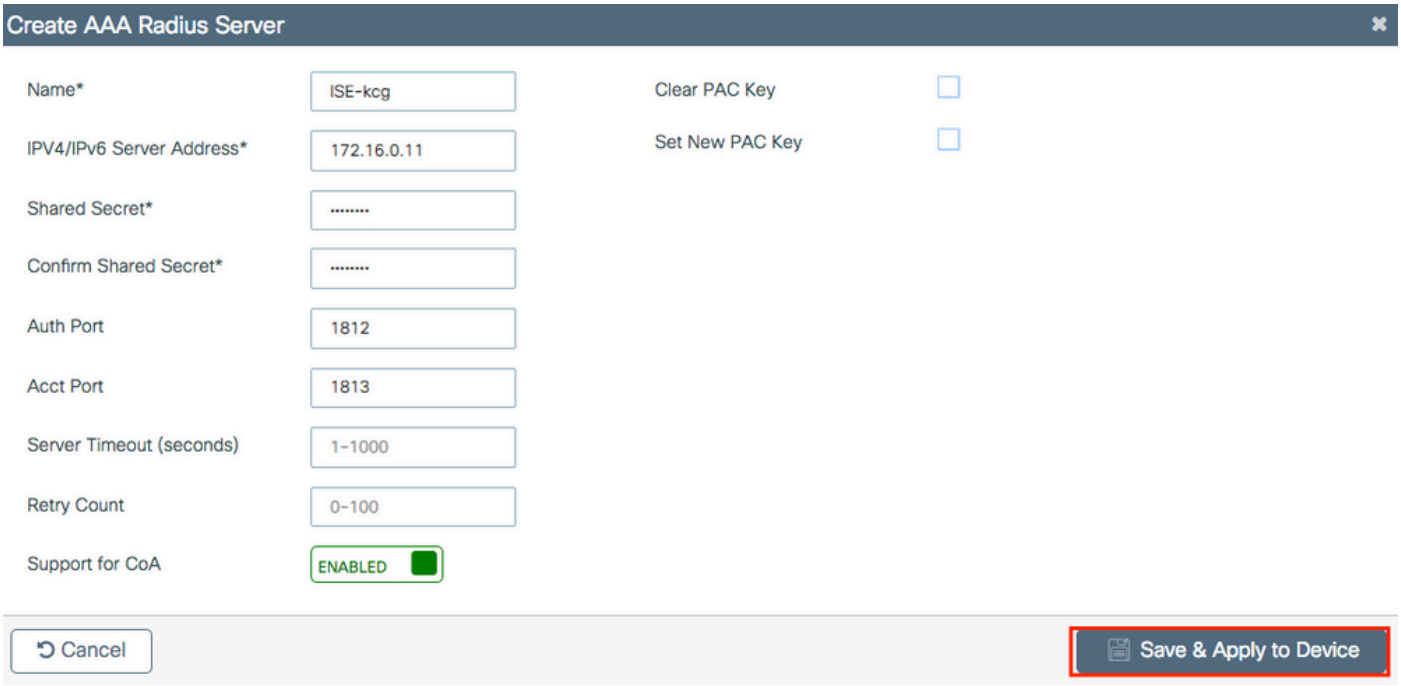
AAA Configuration on 9800 WLCs

GUI:

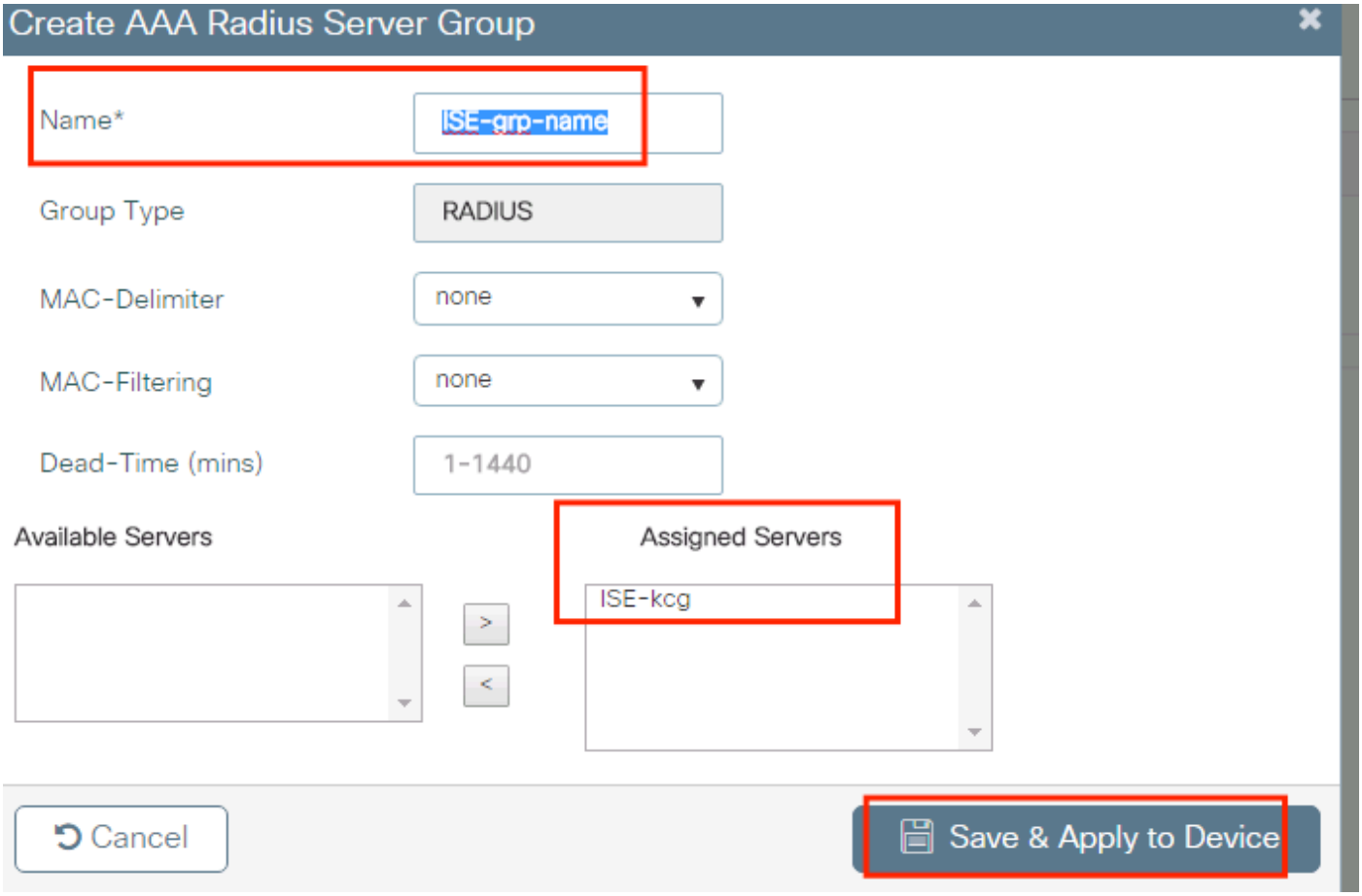
Step 1. Declare RADIUS server. Navigate to **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add** and enter the RADIUS server information.



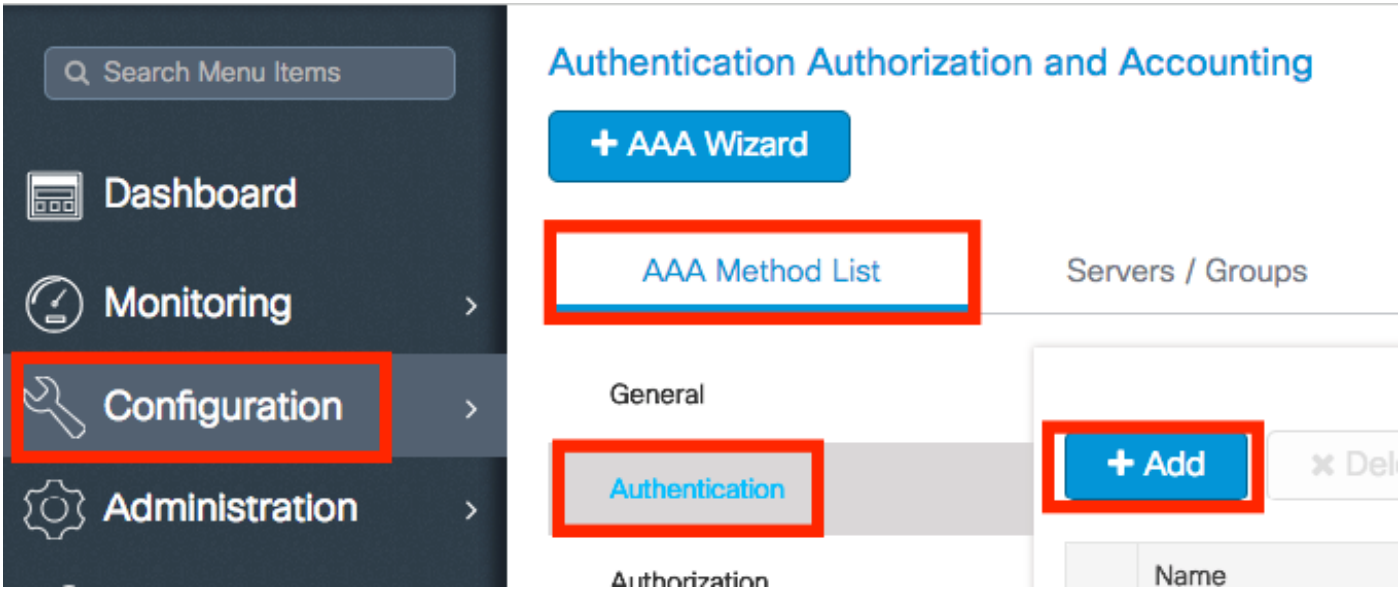
Ensure **Support for CoA** is enabled if you plan to use Central Web Authentication (or any kind of security that requires Change of Authorization [CoA]) in the future.



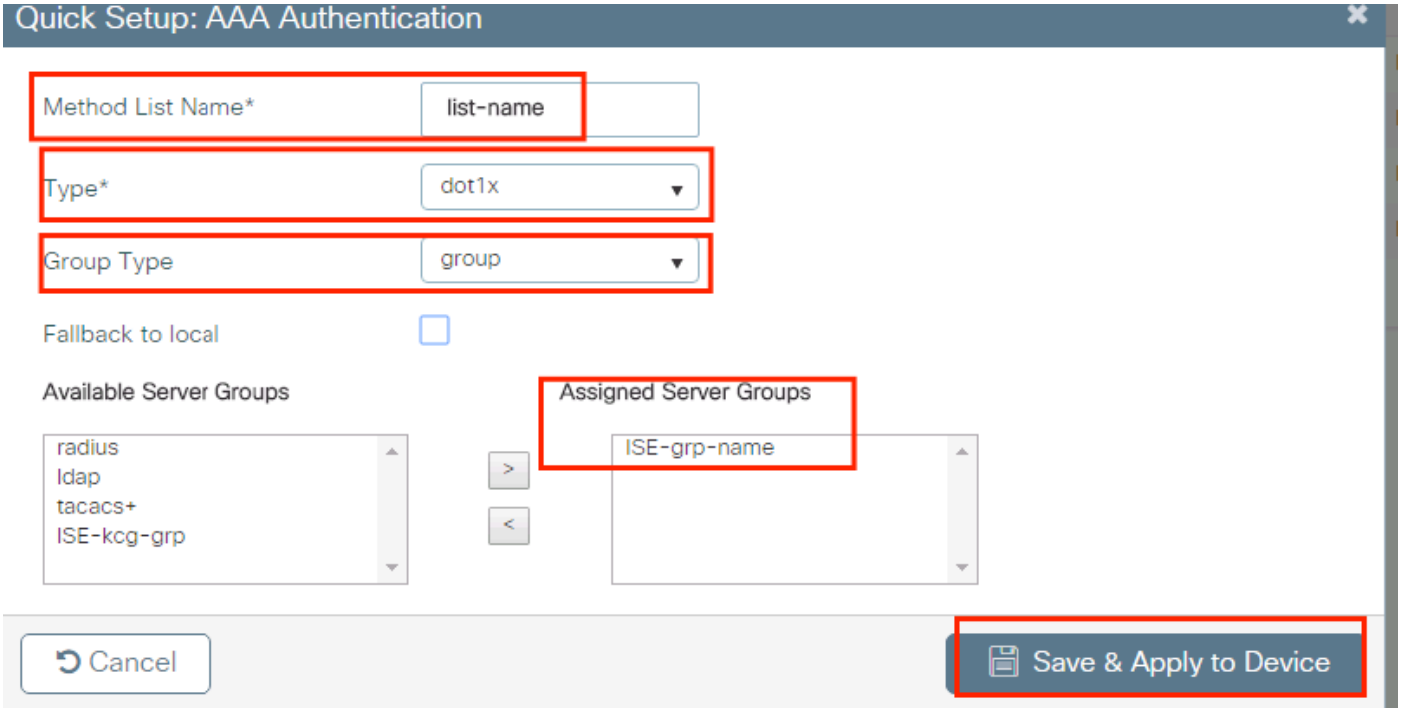
Step 2. Add the RADIUS server to a RADIUS group. Navigate to **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add.** Give a name to your group and move the server you created earlier in the list of **Assigned Servers**.



Step 3. Create an Authentication Method List. Navigate to **Configuration > Security > AAA > AAA Method List > Authentication > + Add**.



Enter the information:



CLI:

```
# config t
# aaa new-model

# radius server <radius-server-name>
# address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813
# timeout 300
# retransmit 3
# key <shared-key>
# exit

# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>
# aaa authentication dot1x <dot1x-list-name> group <radius-grp-name>
```

Note on the AAA Dead-Server Detection

After you have configured your RADIUS server, you can check if it is considered as "ALIVE":

```
#show aaa servers | s WNCD Platform State from WNCD (1) : current UP Platform State from WNCD (2) : current UP Platform State from WNCD (3) : current UP Platform State from WNCD (4) : current UP ...
```

You can configure the **dead criteria**, as well as the **deadtime** on your WLC, especially if you use multiple RADIUS servers.

```
#radius-server dead-criteria time 5 tries 3 #radius-server deadtime 5
```

> **Note**: The **dead criteria** is the criteria used to mark a RADIUS server as dead. It consists of: 1. A timeout (in seconds) which represents the amount of time that must elapse from the time the controller last received a valid packet from the RADIUS server to the time the server is

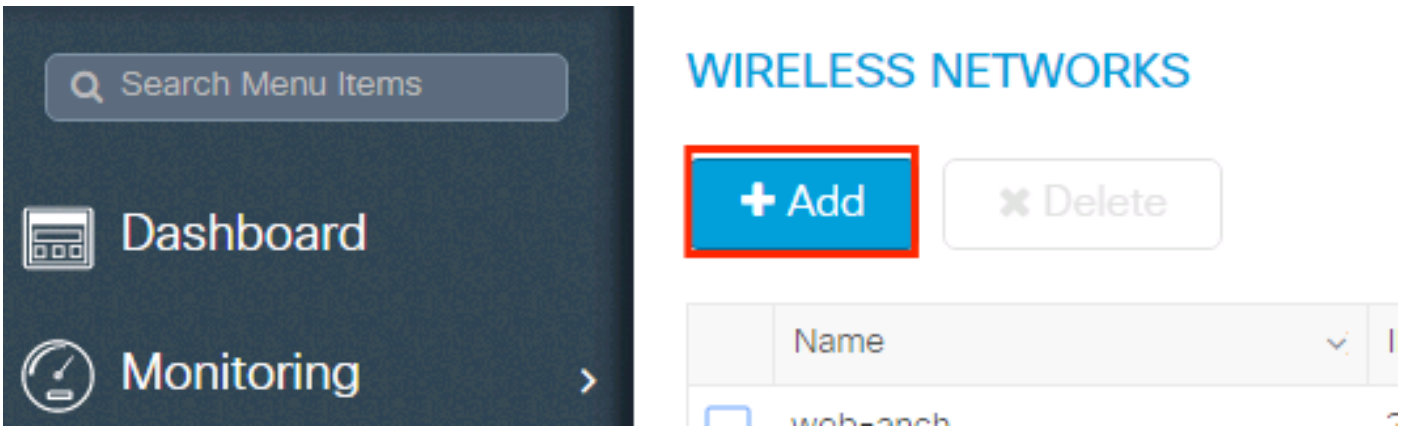
marked as dead. 2. A counter, which represents the number of consecutive timeouts that must occur on the controller before the RADIUS server is marked as dead.

Note: The **deadtime** specifies the amount of time (in minutes) the server remains in dead status after dead-criteria marks it as dead. Once the deadtime expires, the controller marks the server as UP (ALIVE) and notifies the registered clients about the state change. If the server is still unreachable after the state is marked as UP and if the dead criteria is met, then server is marked as dead again for the deadtime interval.

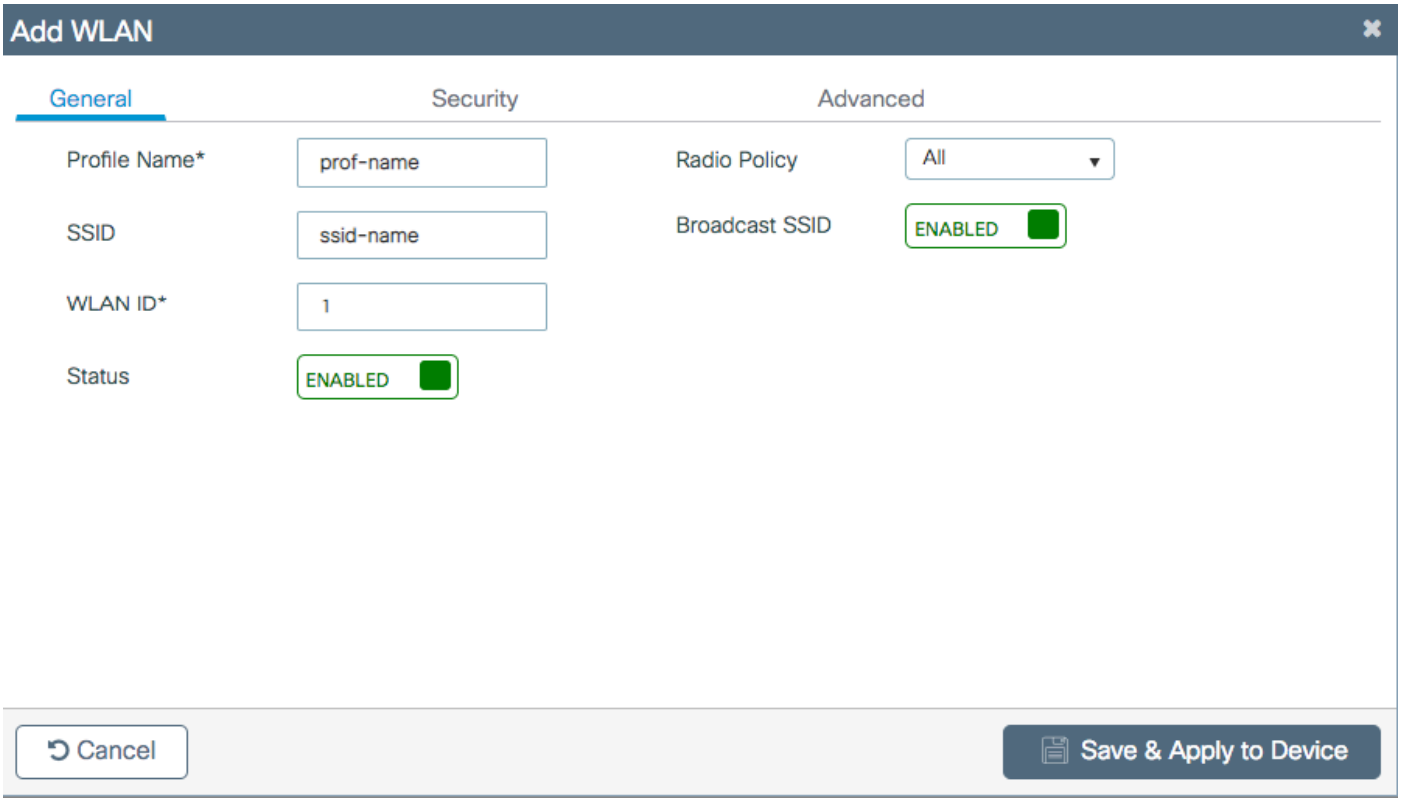
WLAN Profile Configuration

GUI:

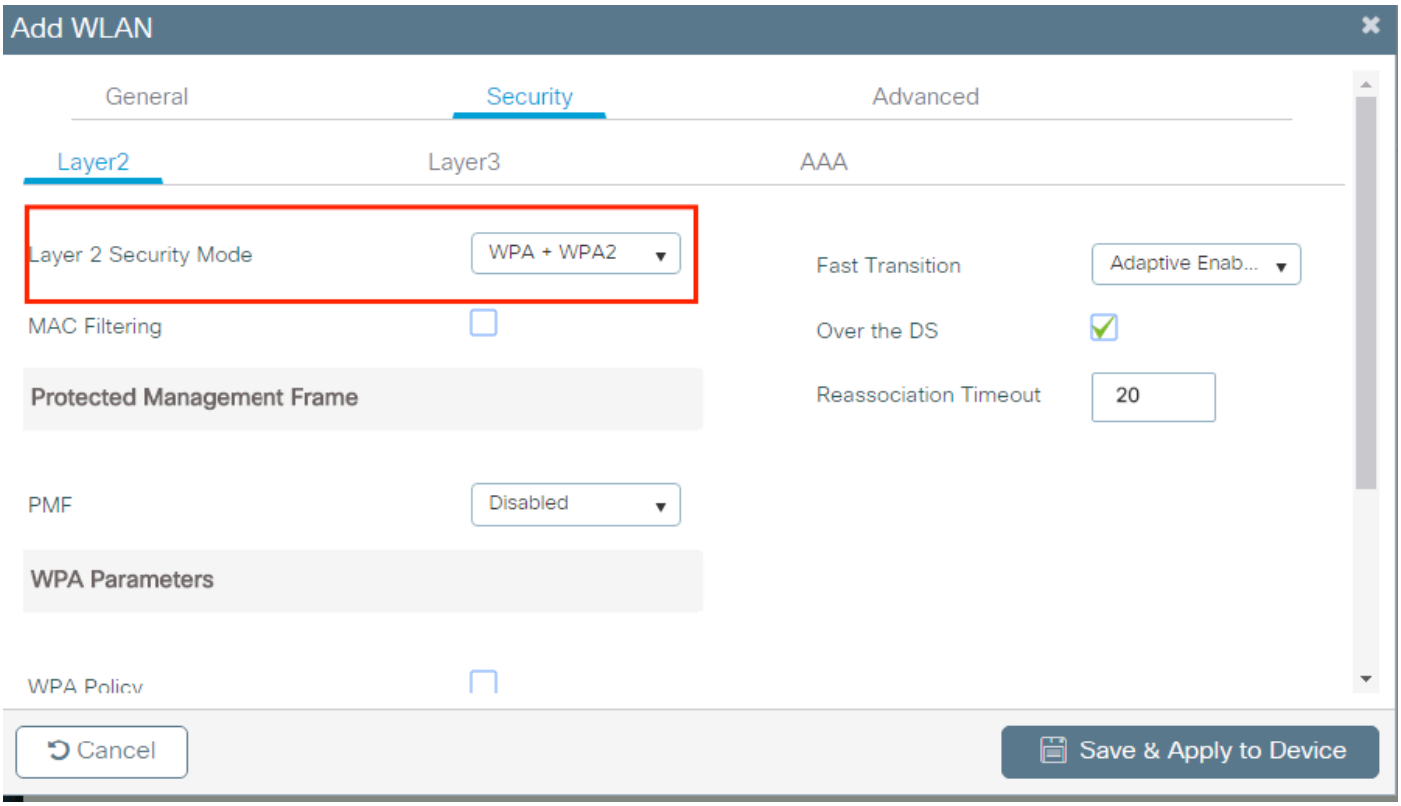
Step 1. Create the WLAN. Navigate to **Configuration > Wireless > WLANs > + Add** and configure the network as needed.

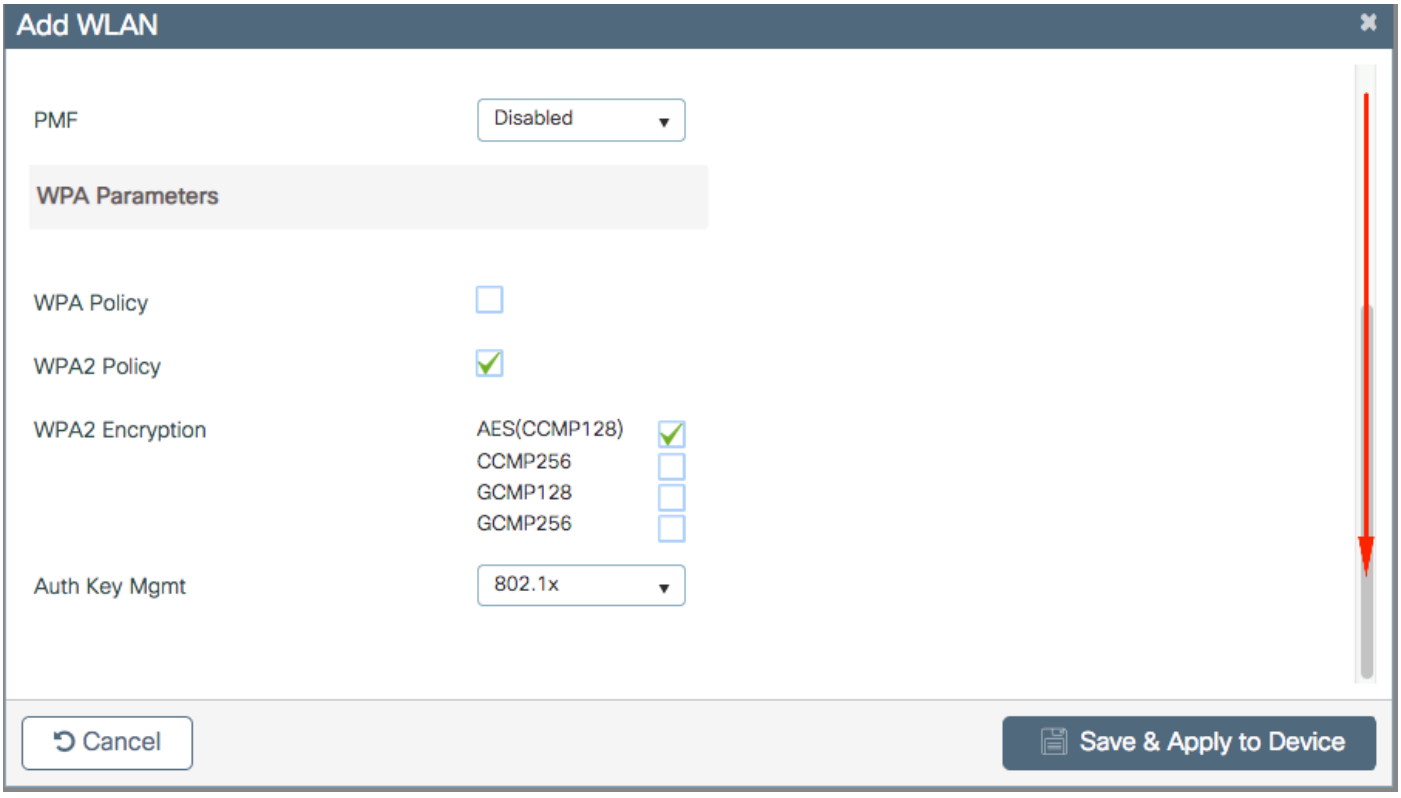


Step 2. Enter the WLAN information

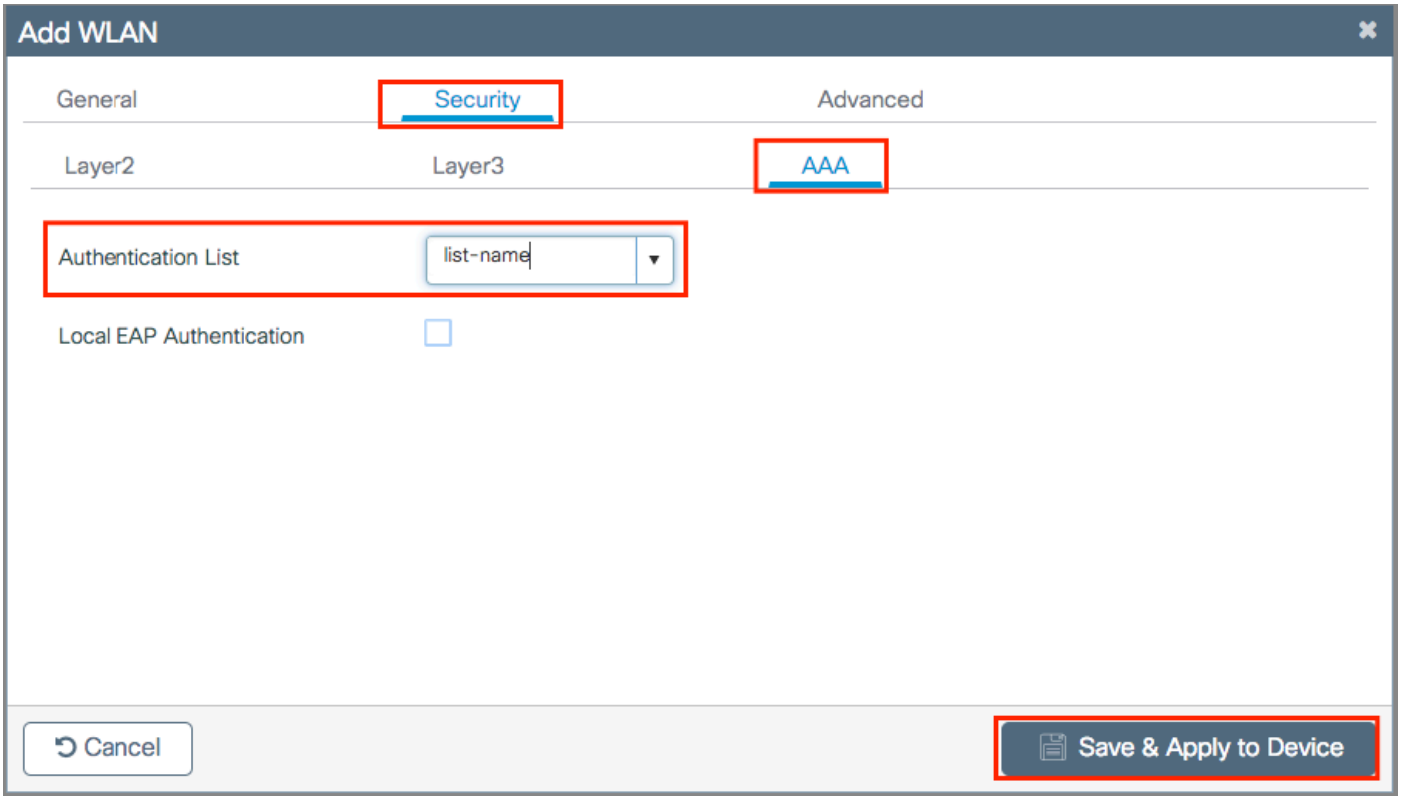


Step 3. Navigate to the **Security** tab and select the needed security method. In this case **WPA2 + 802.1x**.





Step 4. From the **Security > AAA** tab, select the authentication method created on Step 3 from AAA Configuration on 9800 WLC section.



CLI:

```
# config t
# wlan <profile-name> <wlan-id> <ssid-name>
# security dot1x authentication-list <dot1x-list-name>
# no shutdown
```

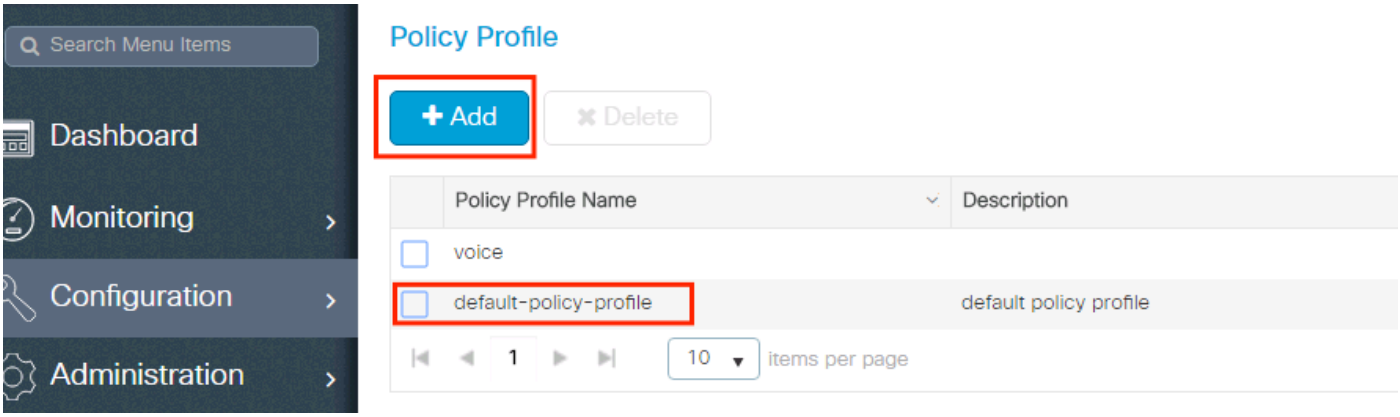
Policy Profile Configuration

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

You can either use your default policy profile or you can create a new profile.

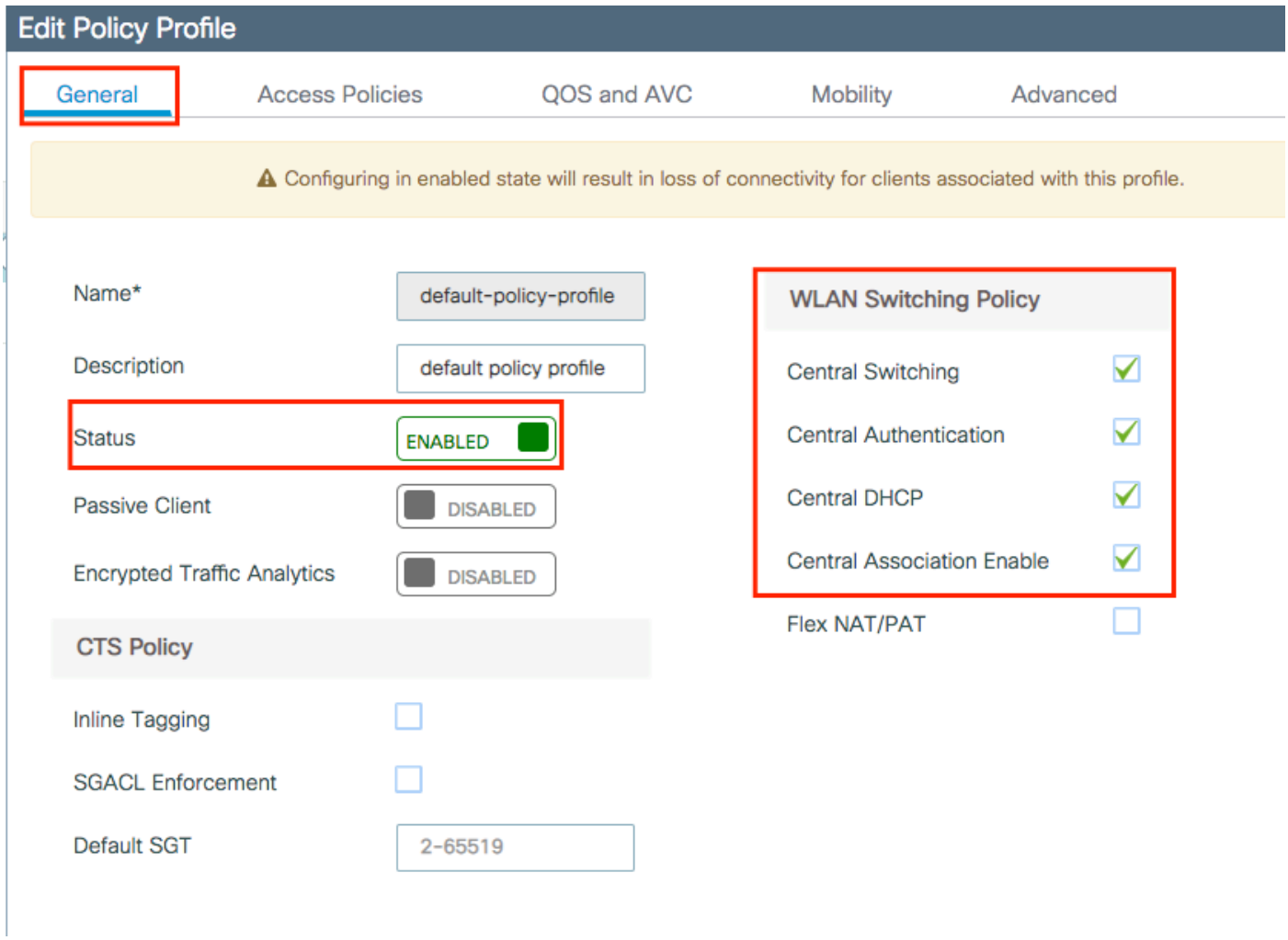
GUI:

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

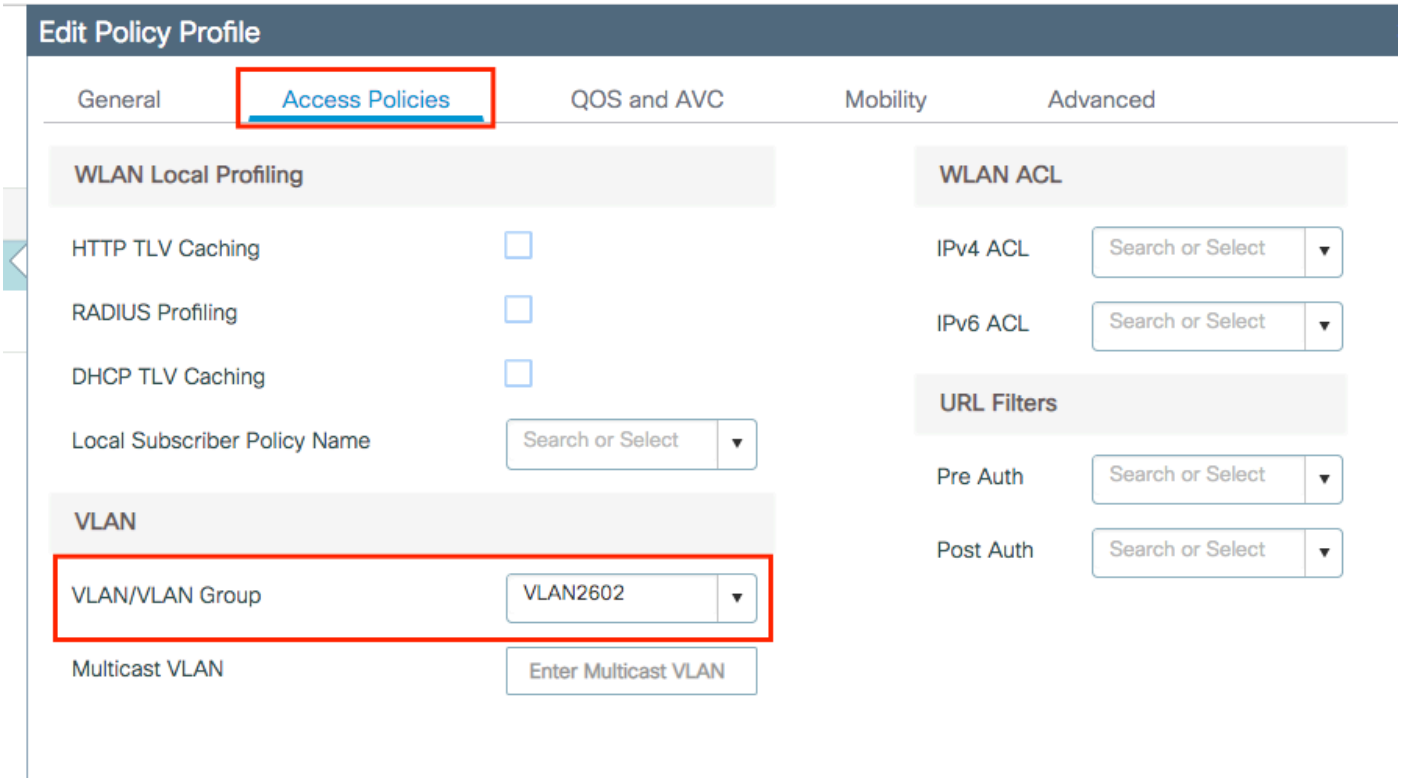


Ensure the profile is enabled.

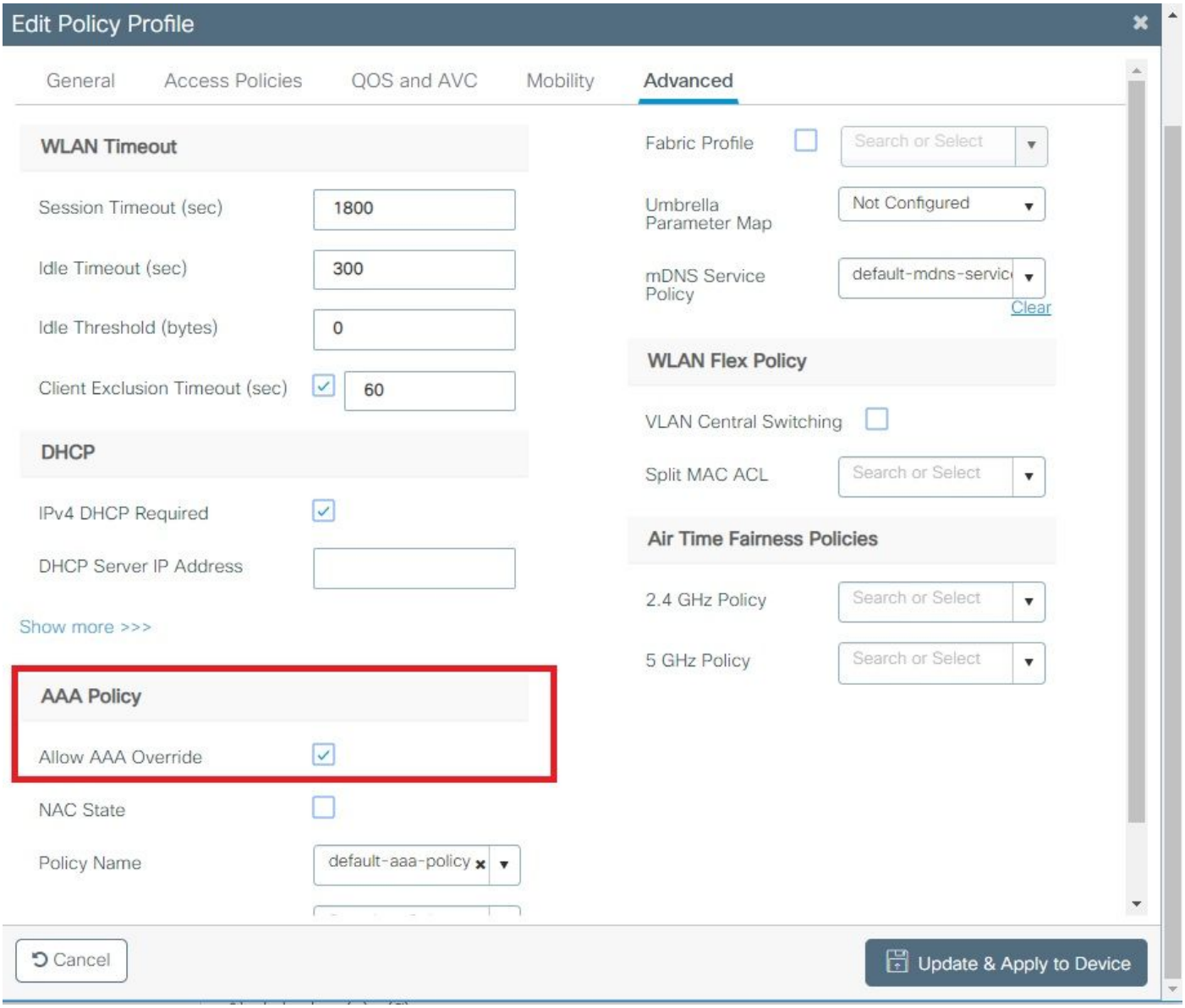
Also, if your Access Point (AP) is in local mode, ensure the policy profile have **Central Switching** and **Central Authentication** enabled.



Select the VLAN where the clients need to be assigned in the **Access Policies** tab.



If you plan to have ISE return attributes in the Access-Accept like VLAN Assignment, please enable AAA override in the **Advanced** tab:



CLI:

```
# config
# wireless profile policy <policy-profile-name>
# aaa-override # central switching # description "<description>" # vlan <vlanID-or-VLAN_name> #
no shutdown
```

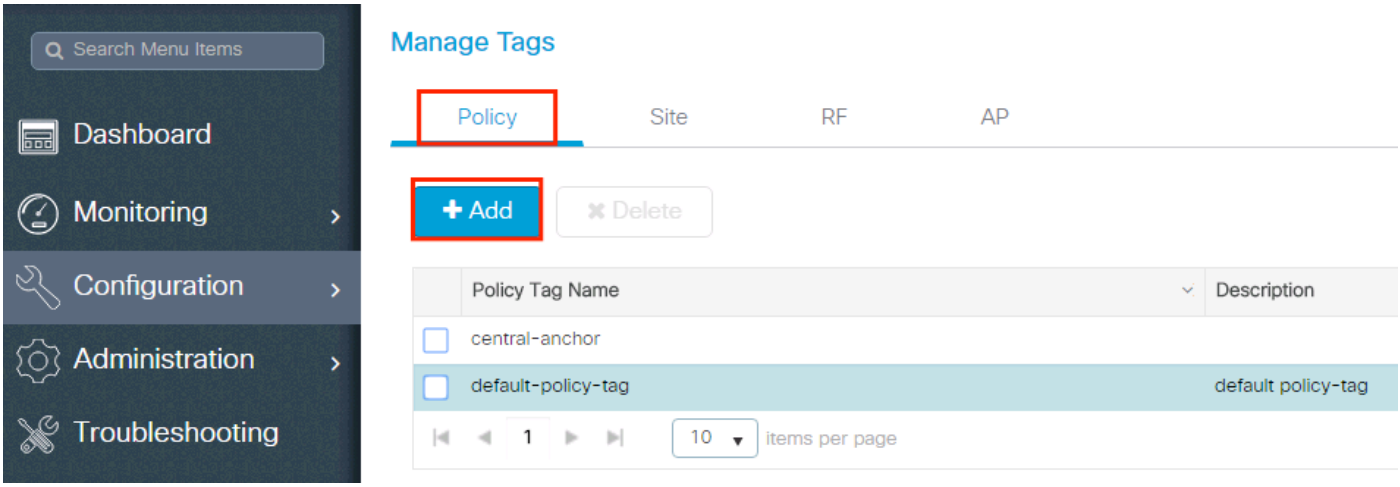
Policy Tag Configuration

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.

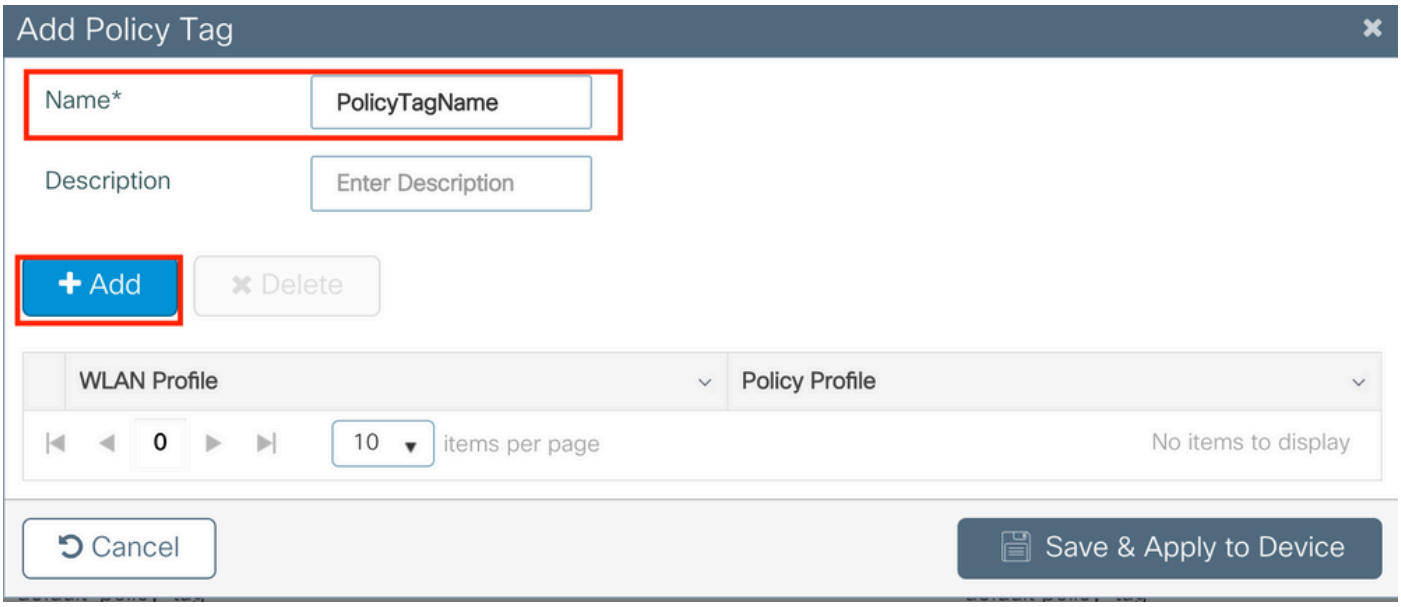
> **Note**: The default-policy-tag automatically maps any SSID with a WLAN ID between 1 and 16 to the default-policy-profile. It cannot be modified nor deleted. If you have a WLAN with ID 17 or higher, the default-policy-tag cannot be used.

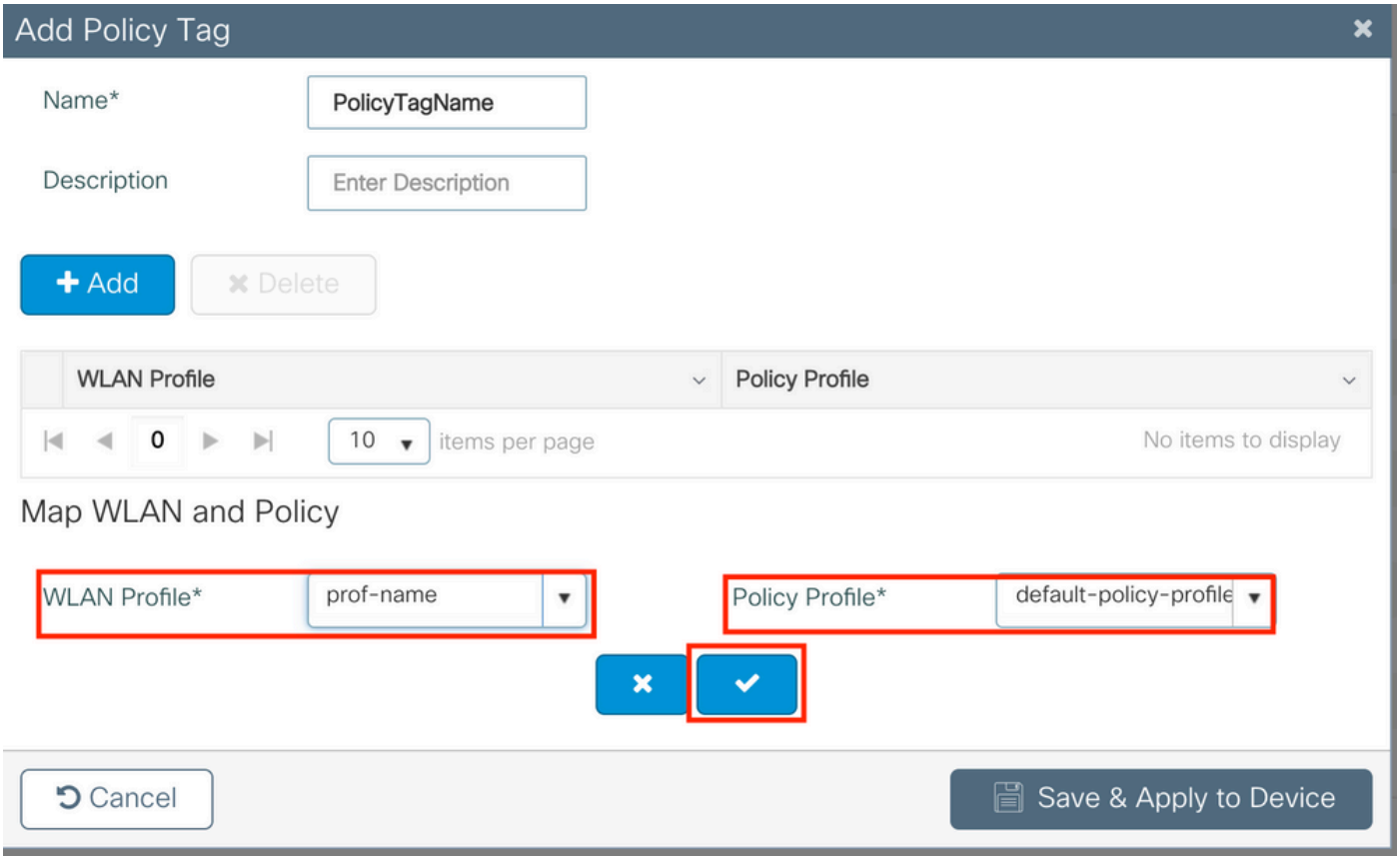
GUI:

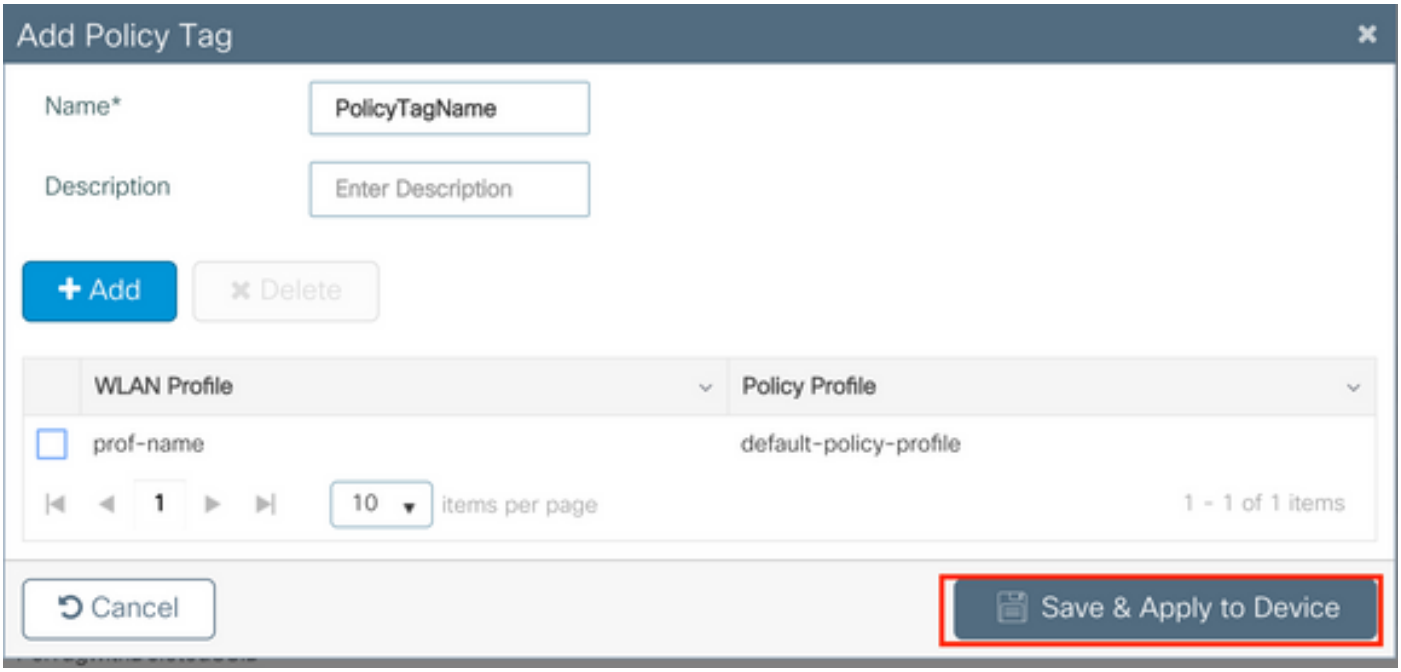
Navigate to **Configugation > Tags & Profiles > Tags > Policy** and add a new one if needed.



Link your WLAN Profile to the desired Policy Profile.







CLI:

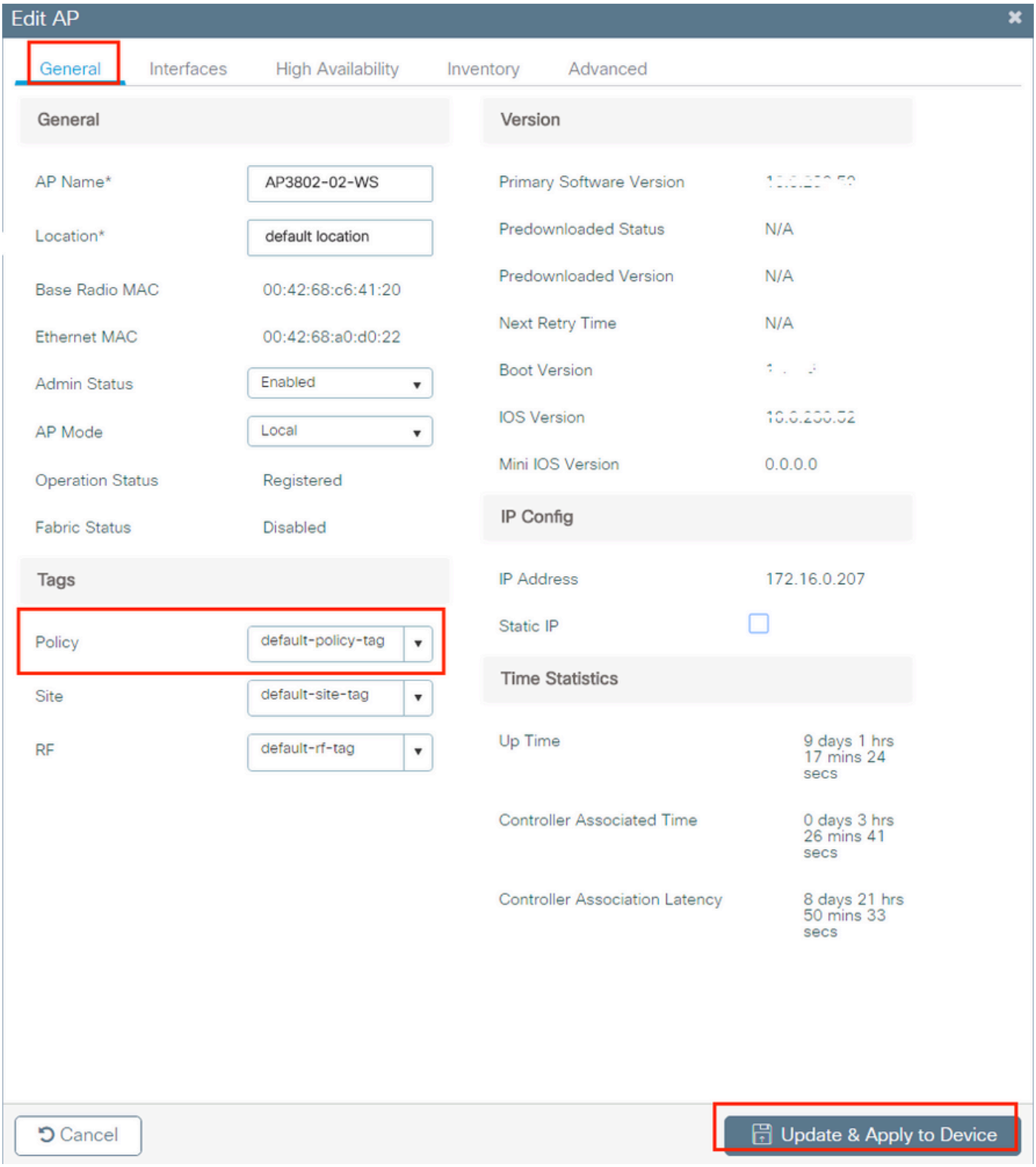
```
# config t
# wireless tag policy <policy-tag-name>
# wlan <profile-name> policy <policy-profile-name>
```

Policy Tag Assignation

Assign the Policy Tag to the needed APs.

GUI:

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



Note: Be aware that when the policy tag on an AP is changed, it drops its association to the 9800 WLC and joins back a few moments later.

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