# Configure WLAN Anchor Mobility Feature on Catalyst 9800

## Contents


**Introduction**

**Prerequisites**

- Requirements
- Components Used

**Configure**

- Foreign/Anchor Scenario Between 9800 WLCs
  - Network Diagram: Two Catalyst 9800 WLCs
  - Configure a 9800 Foreign with a 9800 Anchor
- Foreign 9800 WLC - Anchor AireOS
  - Catalyst 9800 Foreign - AireOS Anchor Network Diagram
  - Configure 9800 Foreign with AireOS Anchor
- Foreign AireOS - Anchor 9800 WLC
  - AireOS Foreign with 9800 Anchor Network Diagram
  - Configure a 9800 Foreign with an AireOS Anchor

**Verification**

- Verify on the 9800 WLC
- Verify on the AireOS WLC

**Troubleshoot**

- Conditional Debugging and Radio Active Tracing
- Verify the AireOS WLC


## Introduction

This document describes how to configure a Wireless Local Area Network (WLAN) on a foreign/anchor scenario with Catalyst 9800 Wireless Controllers.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Command Line Interface (CLI) or Graphic User Interface (GUI) access to the wireless controllers
- Mobility on Cisco Wireless LAN Controllers (WLCs)
- 9800 Wireless Controllers
- AireOS WLCs

### Components Used

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

- AireOS WLC version 8.8 MR2 (you can also use Inter Release Controller Mobility (IRCM) special 8.5 images)
- 9800 WLC v16.10 or later
- 9800 WLC Configuration Model

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.

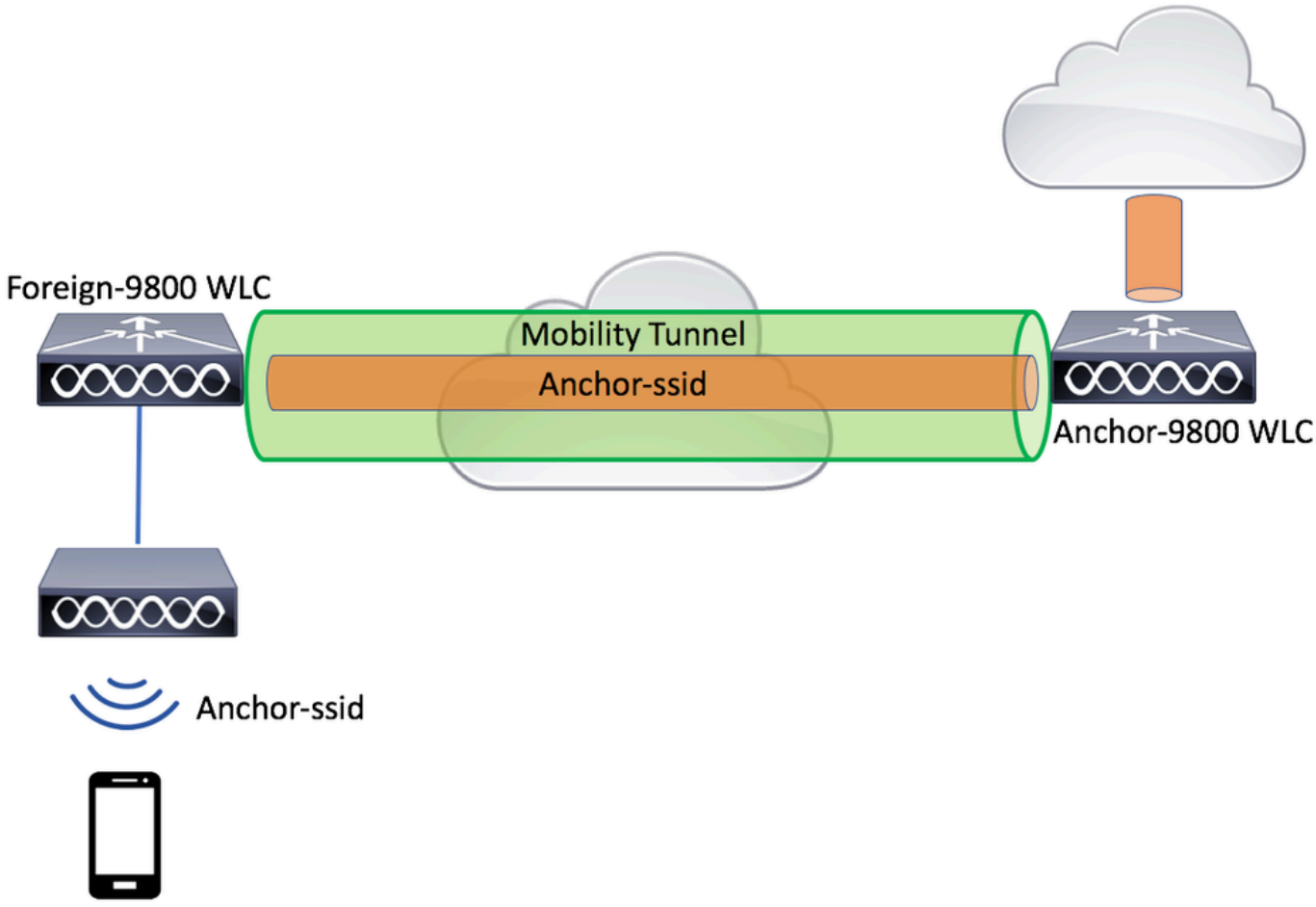
# Configure

This is a feature normally used for Guest access scenarios, to terminate all traffic from clients into a single L3 exit point, even if the clients come from different controllers and physical locations. The mobility tunnel provides a mechanism to keep the traffic isolated, as it transverses the network.

## Foreign/Anchor Scenario Between 9800 WLCs

This scenario depicts the two Catalyst 9800s used.

**Network Diagram: Two Catalyst 9800 WLCs**




For mobility guest scenarios, there are two main controller roles:

- Foreign controller: This WLC owns layer 2 or the wireless side. It has access points connected to it. All client traffic for the anchored WLANs is encapsulated into the mobility tunnel to be sent to the anchor. It does not exit locally.

- Anchor controller: This is the layer 3 exit point. It receives the mobility tunnels from the foreign controllers and decapsulates or terminates the client traffic into the exit point (VLAN). This is the point where the clients are seen in the network, thus the anchor name.

Access points on the foreign WLC broadcast the WLAN SSIDs and have a policy tag assigned that links the WLAN profile with the appropriate policy profile. When a wireless client connects to this SSID, the foreign controller sends both, the SSID name and Policy Profile as part of the client information to the anchor WLC. Upon receipt, the anchor WLC checks its own configuration to match the SSID name as well as the Policy Profile name. Once anchor WLC finds a match, it applies the configuration that corresponds to it and an exit point to the wireless client. Therefore, it is mandatory that WLAN and Policy Profile names and configurations match on both foreign 9800 WLC and anchor 9800 WLC with the exception of VLAN under the Policy Profile.

---

**Note**: WLAN Profile and Policy Profile names can match on both 9800 Anchor and 9800 Foreign WLC.

---

**Configure a 9800 Foreign with a 9800 Anchor**

Step 1. Build a mobility tunnel between the Foreign 9800 WLC and Anchor 9800 WLC.

You can refer to this document: Configuring Mobility topologies on Catalyst 9800

Step 2. Create the desired SSID on both 9800 WLCs.

Supported security methods:

- Open
- MAC filter
- PSK
- Dot1x
- Local/External Web Authentication (LWA)
- Central Web Authentication (CWA)

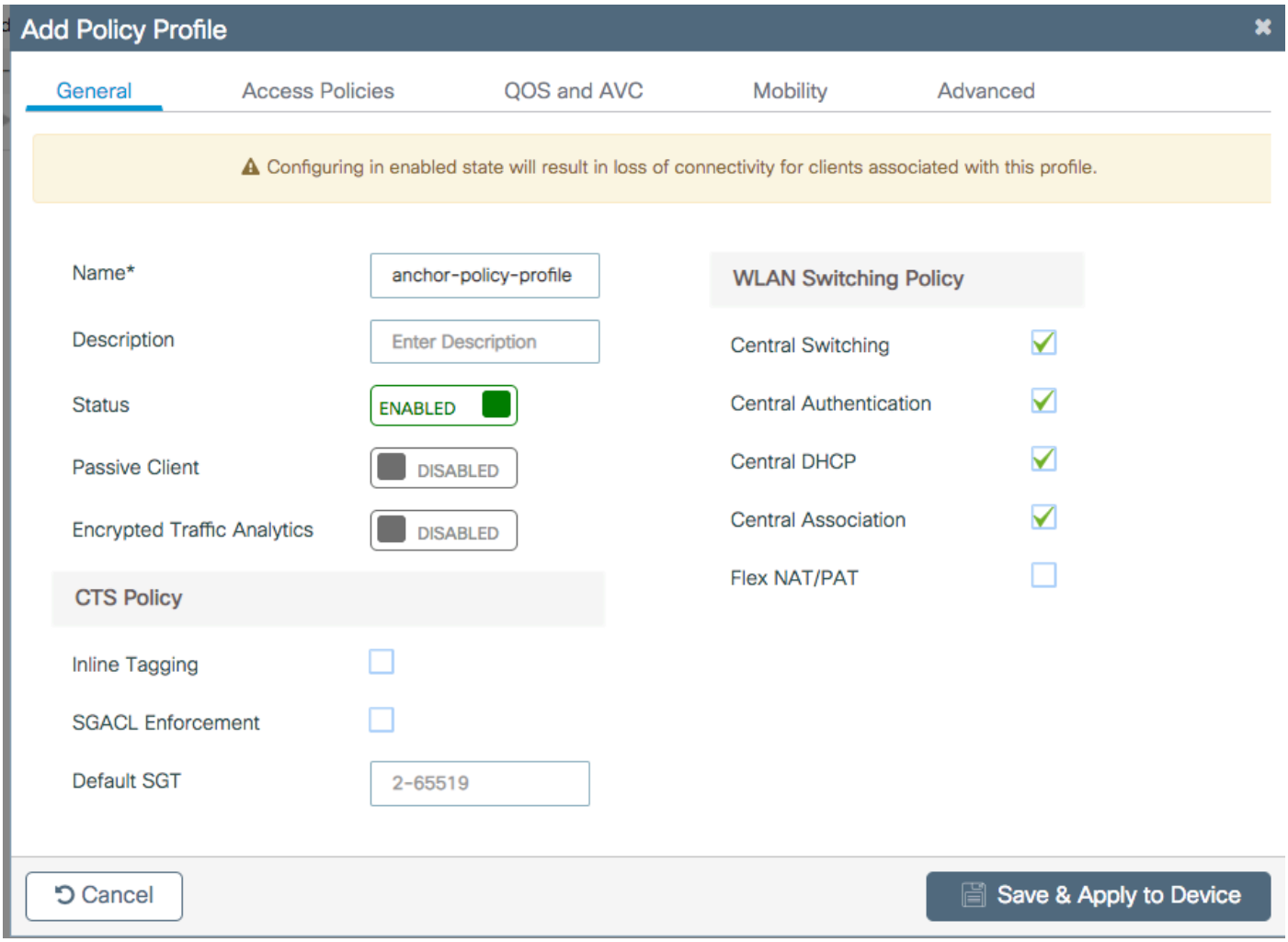
---

**Note**: Both 9800 WLCs must have the same kind of configuration, otherwise anchor does not work.

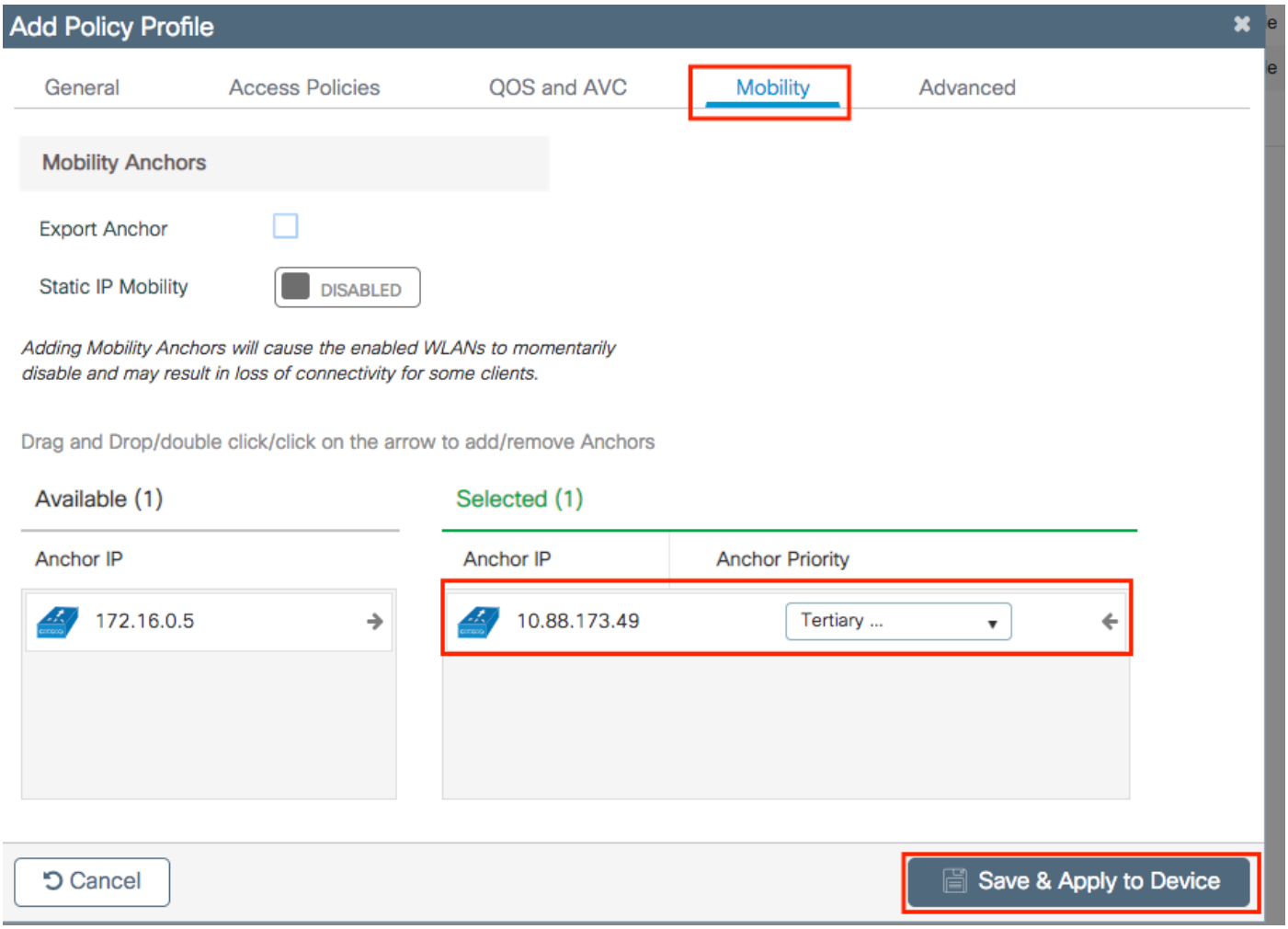
---

Step 3. Log in to the foreign 9800 WLC and define anchor 9800 WLC IP address under the policy profile.

Navigate to Configuration > Tags & Profiles > Policy > + Add.

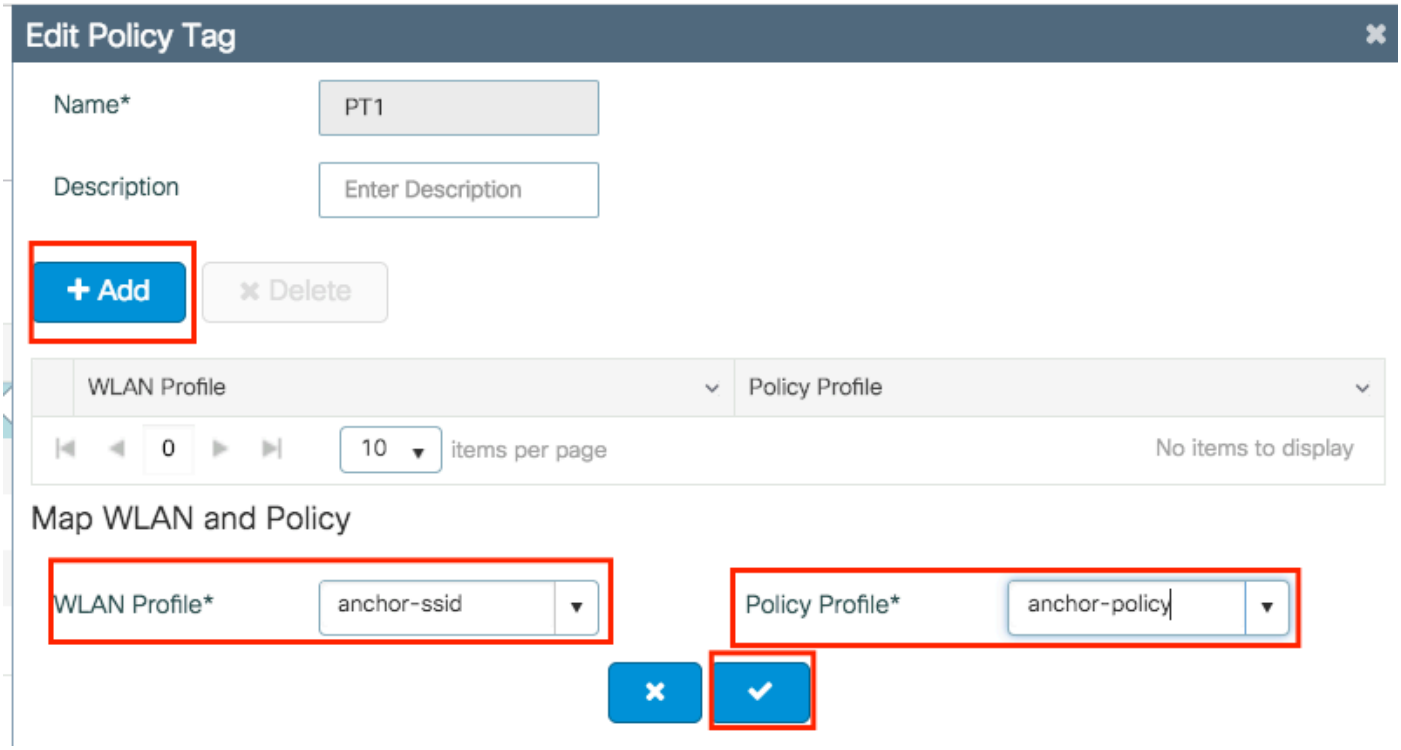



On the Mobility tab, choose the IP address of the anchor 9800 WLC.

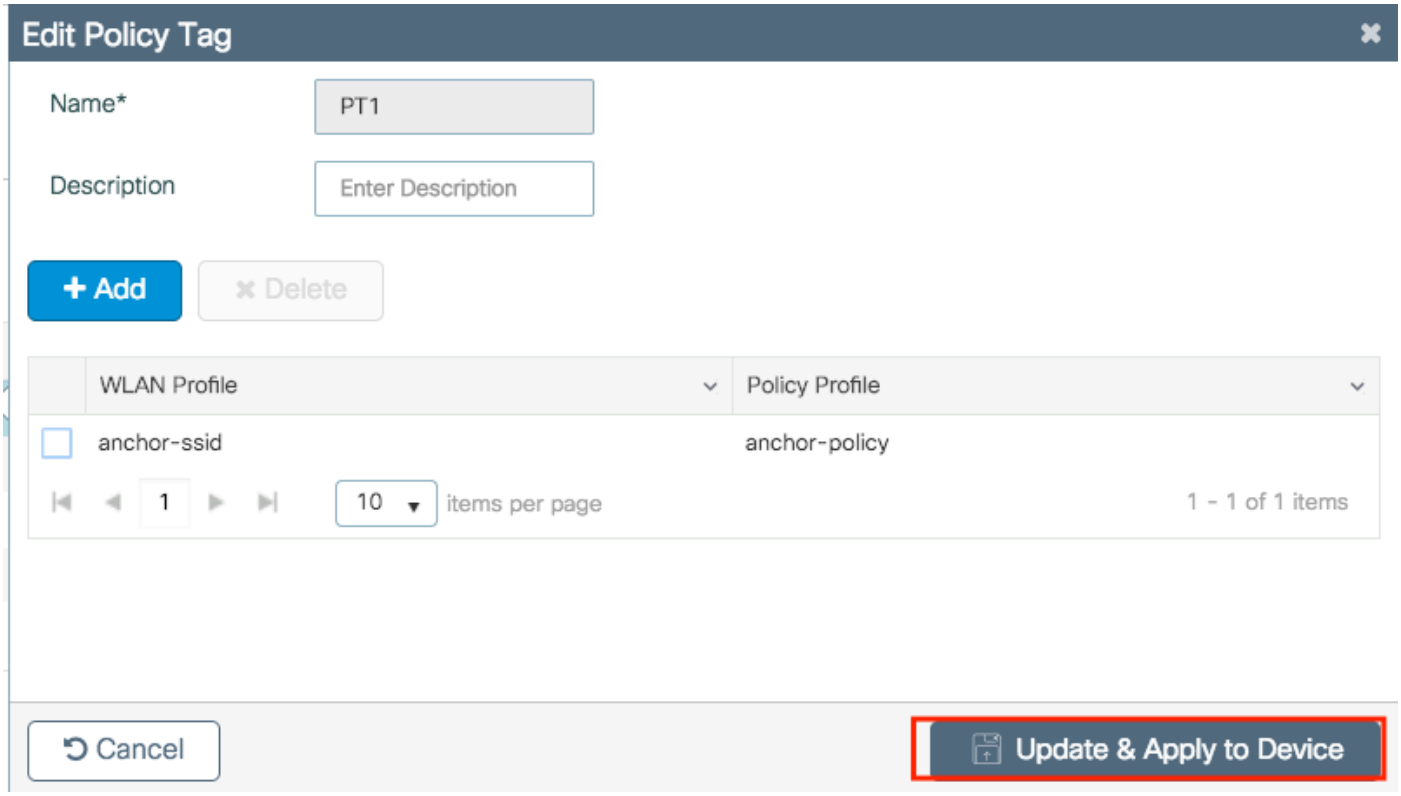



Step 4. Link the Policy Profile with the WLAN inside the Policy Tag assigned to the APs associated with the foreign controller that services this WLAN.

Navigate to Configuration > Tags & Profiles > Tags and either create a new one or use the one that exists.

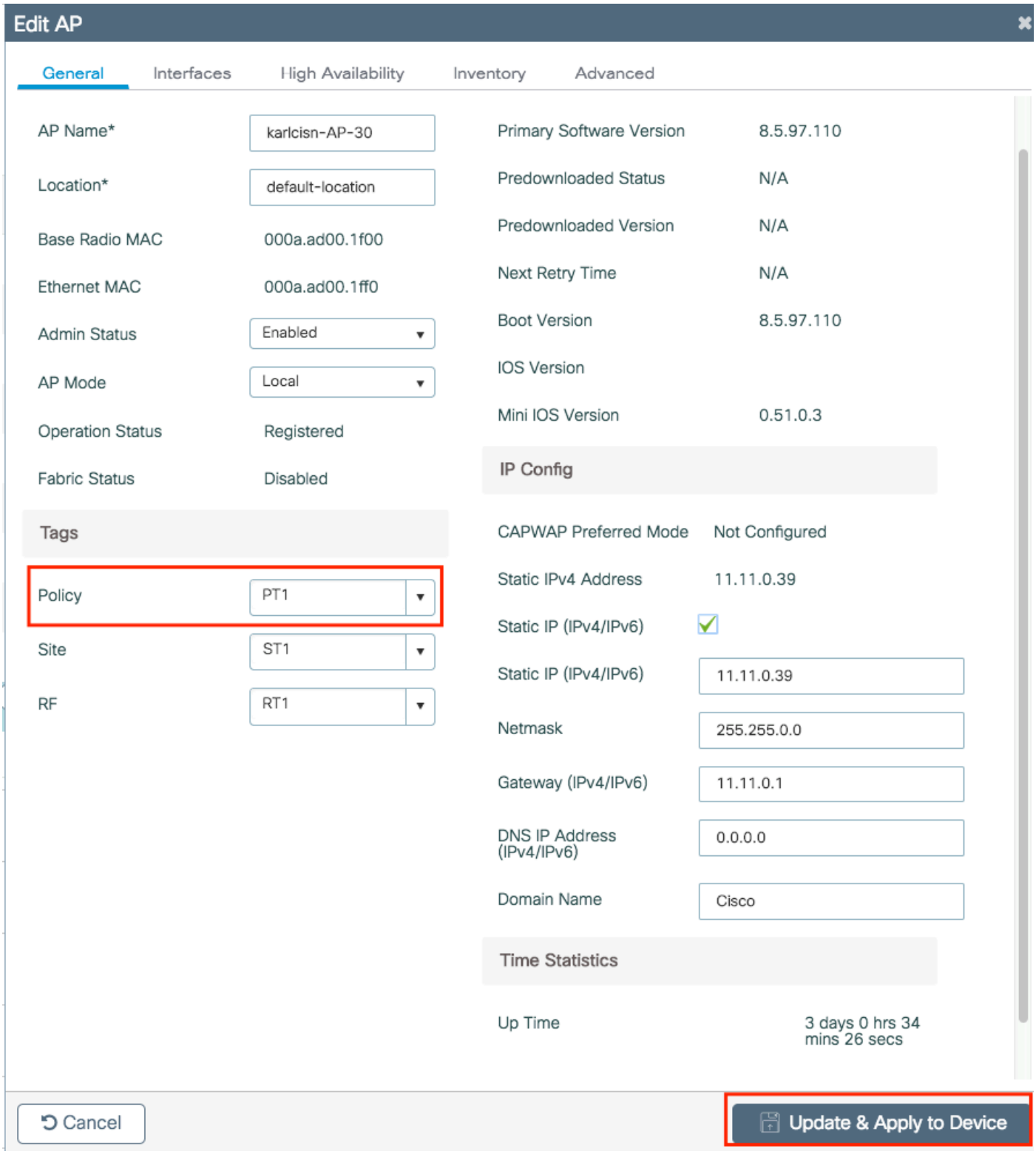


Ensure you choose Update & Apply to Device to apply the changes to the Policy Tag.




Step 5 (optional). Assign the Policy Tag to an AP or verify that it already has it.

Navigate to Configuration > Wireless > Access Points > AP name > General.




**Note**: Be aware that if you perform a change in the AP tag after you choose Update & Apply to Device, the AP restarts its tunnel CAPWAP, so it loses association with the 9800 WLC and then recovers it.

From the CLI:

```
Foreign 9800 WLC
```

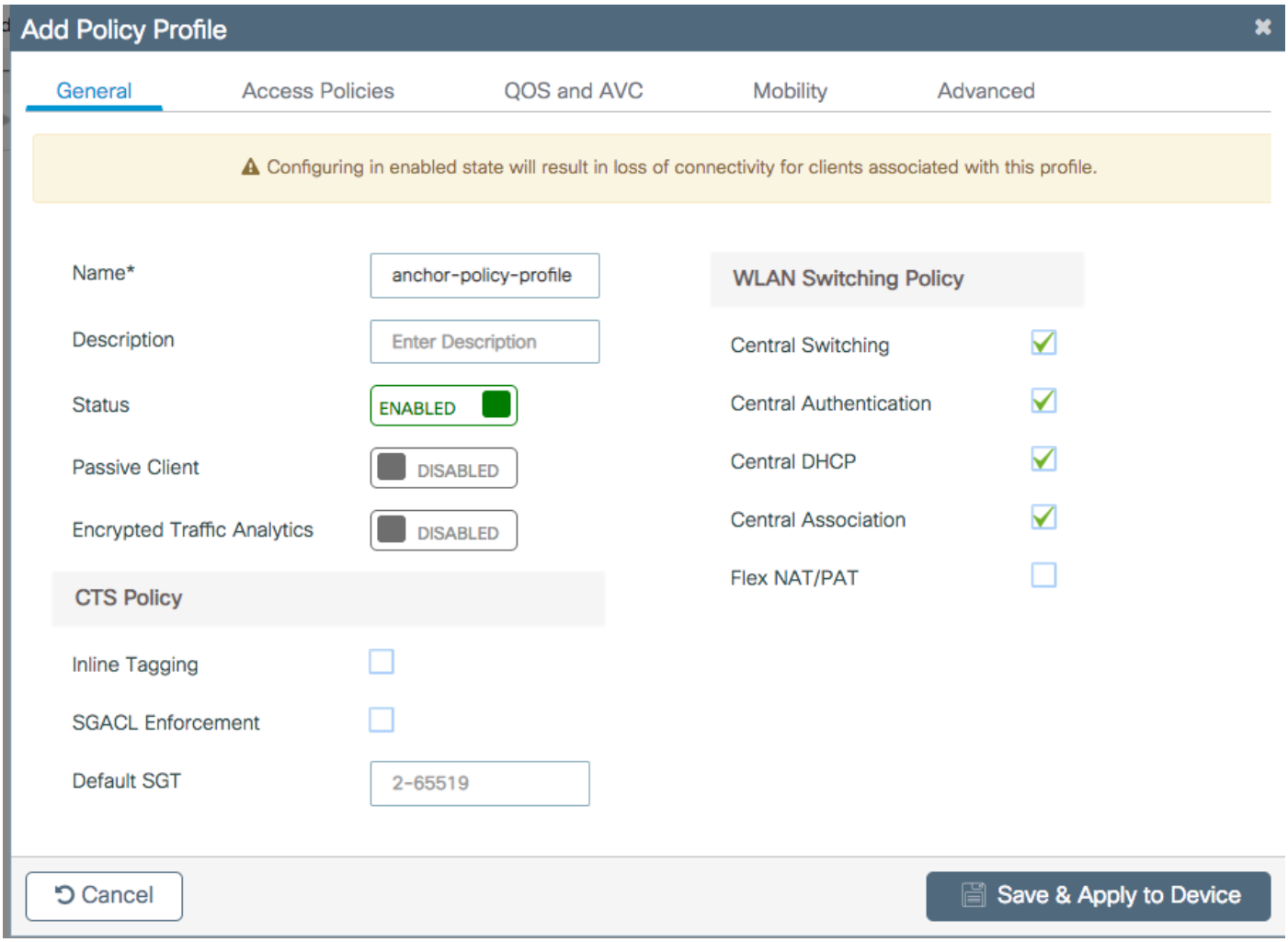
```
# config t
# wireless profile policy anchor-policy
# mobility anchor 10.88.173.105 priority 3
# no shutdown
# exit

# wireless tag policy PT1
# wlan anchor-ssid policy anchor-policy
# exit

# ap aaaa.bbbb.dddd
# site-tag PT1
# exit
```

Step 6. Log in to anchor 9800 WLC and create the anchor policy profile. Ensure it has the exact same name that you used on the foreign 9800 WLCs.

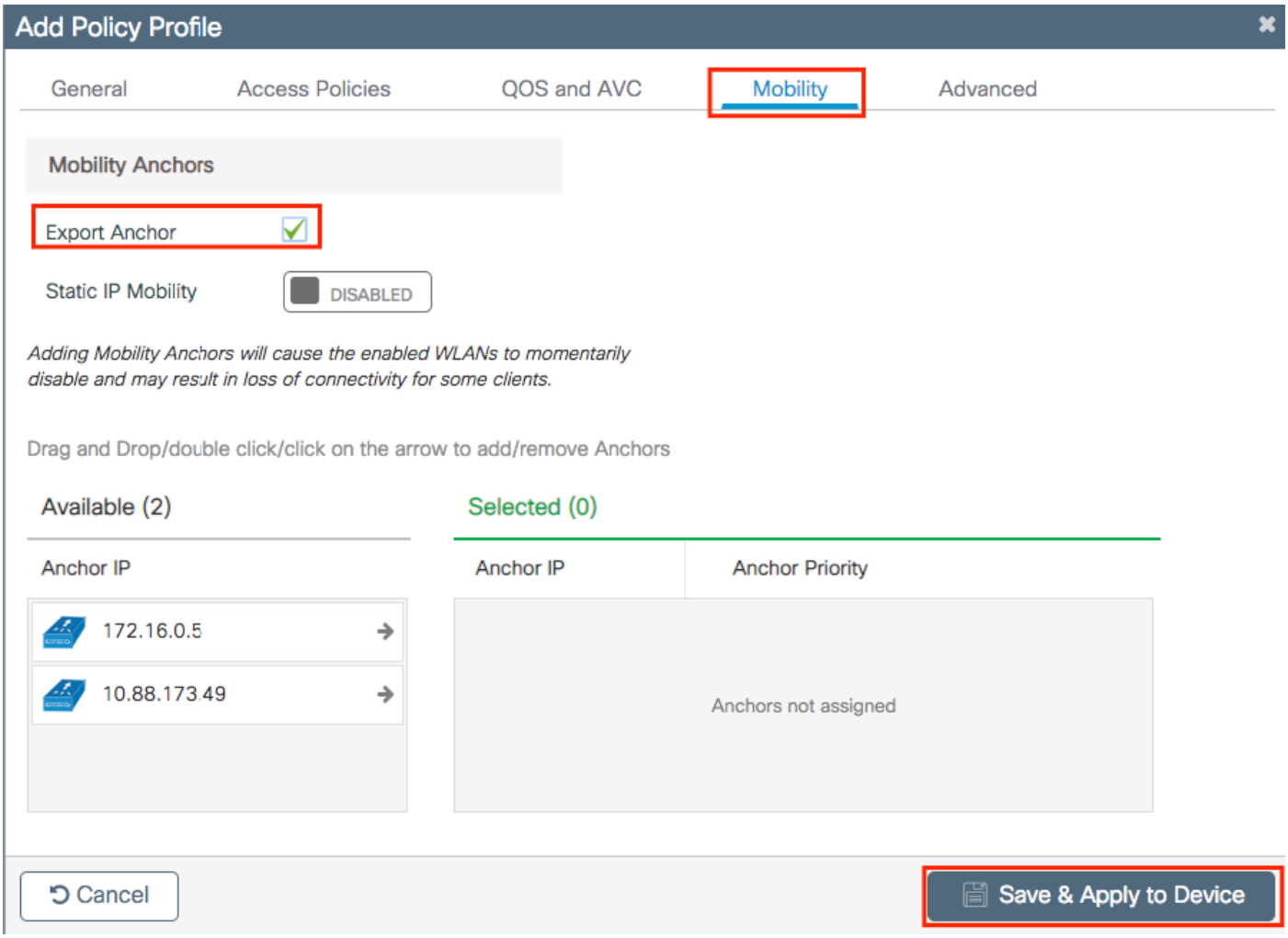
Navigate to Configuration > Tags & Profiles > Policy > + Add.




Navigate to Mobility tab and enable Export Anchor.This instructs the 9800 WLC that it is the anchor 9800 WLC for any WLAN that uses that Policy Profile. When the foreign 9800 WLC sends the clients to the anchor 9800 WLC, it informs about the WLAN and the Policy Profile that the client is assigned to, so the anchor 9800 WLC knows which local Policy Profile to use.

**Note**: You must not configure mobility peers and export anchor at the same time. That is an invalid configuration scenario.

**Note**: You must not use the Export Anchor setting, for any policy profile tied to a WLAN profile on a controller with access points. This prevents the SSID to be broadcasted, so this policy must be used exclusively for Anchor functionality.




From the CLI:

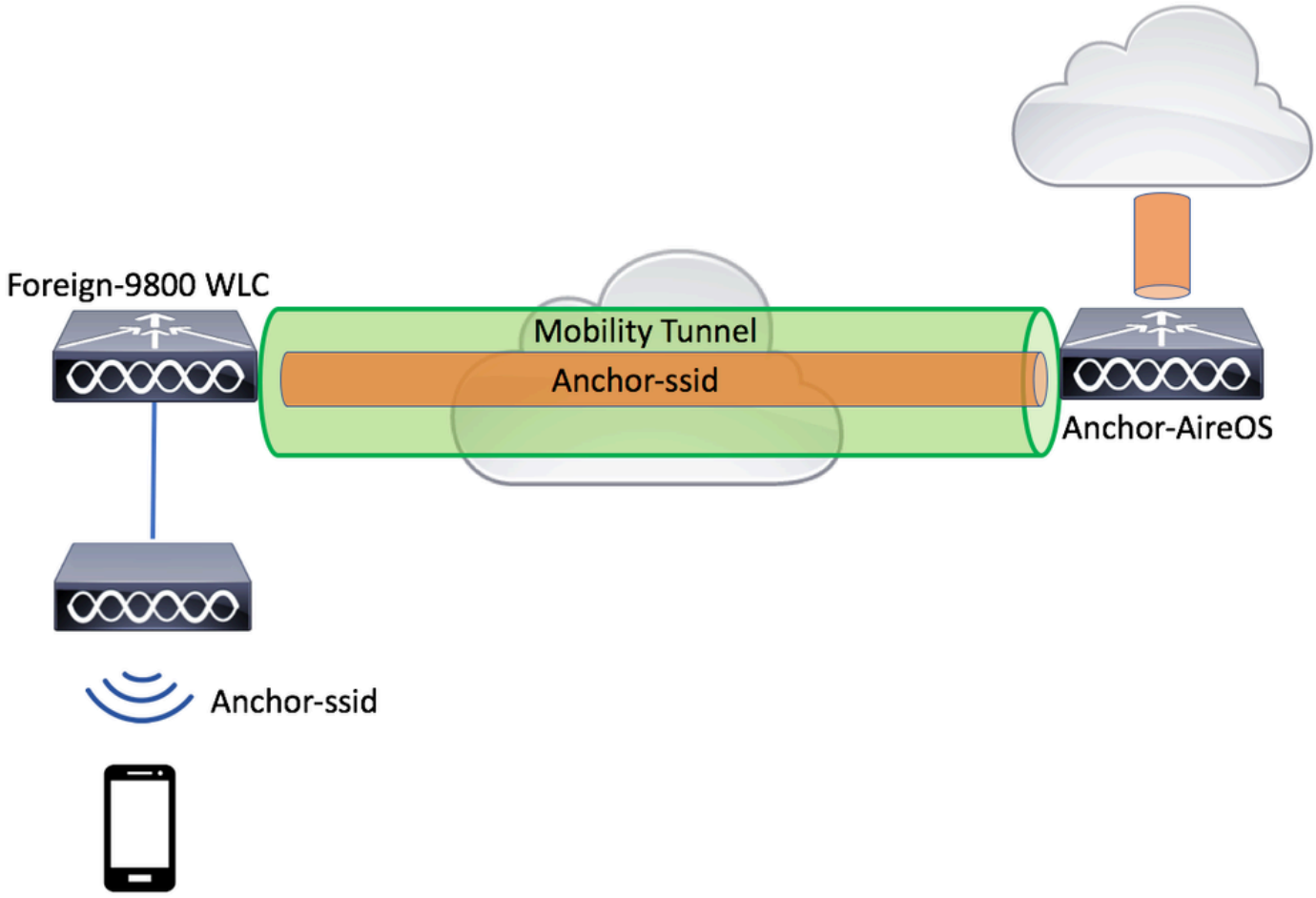
```
Anchor 9800 WLC

# config t
# wireless profile policy <anchor-policy>
# mobility anchor
# vlan <VLAN-id_VLAN-name>
# no shutdown
# exit
```

## Foreign 9800 WLC - Anchor AireOS

This setup depicts the scenario where a Catalyst 9800 WLC is used as Foreign with an AireOS Unified WLC used as the anchor.

**Catalyst 9800 Foreign - AireOS Anchor Network Diagram**




**Configure 9800 Foreign with AireOS Anchor**

Step 1. Build a mobility tunnel between the Foreign 9800 WLC and Anchor AireOS WLC.

Refer to this document: Configuring Mobility topologies on Catalyst 9800

Step 2. Create the desired WLANs on both WLCs.

Supported security methods:

- Open
- MAC filter
- PSK
- Dot1x
- Local/External Web Authentication (LWA)
- Central Web Authentication (CWA)

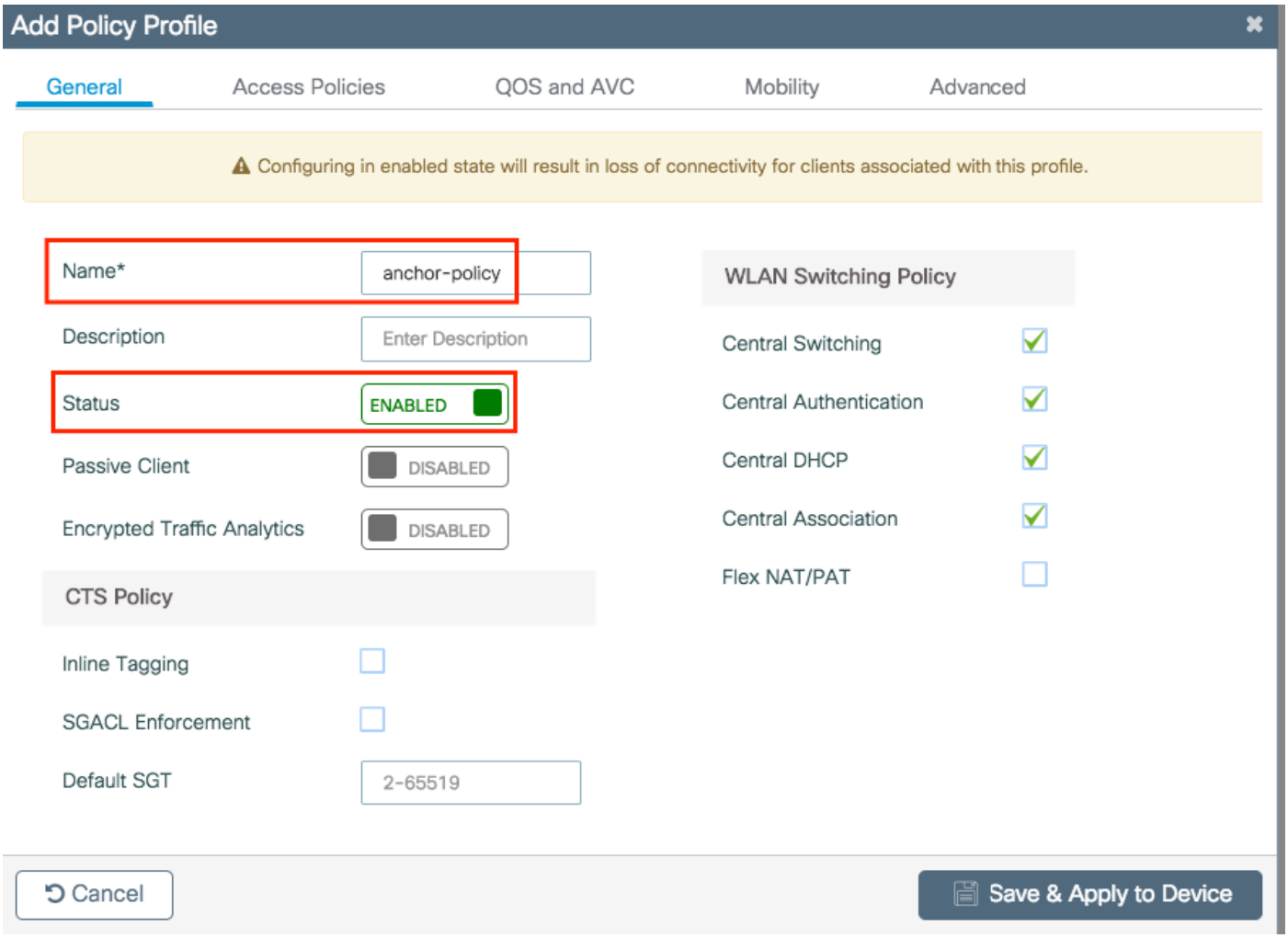
---

**Note**: Both AireOS WLC and 9800 WLC must have the same kind of configuration, otherwise anchor does not work.

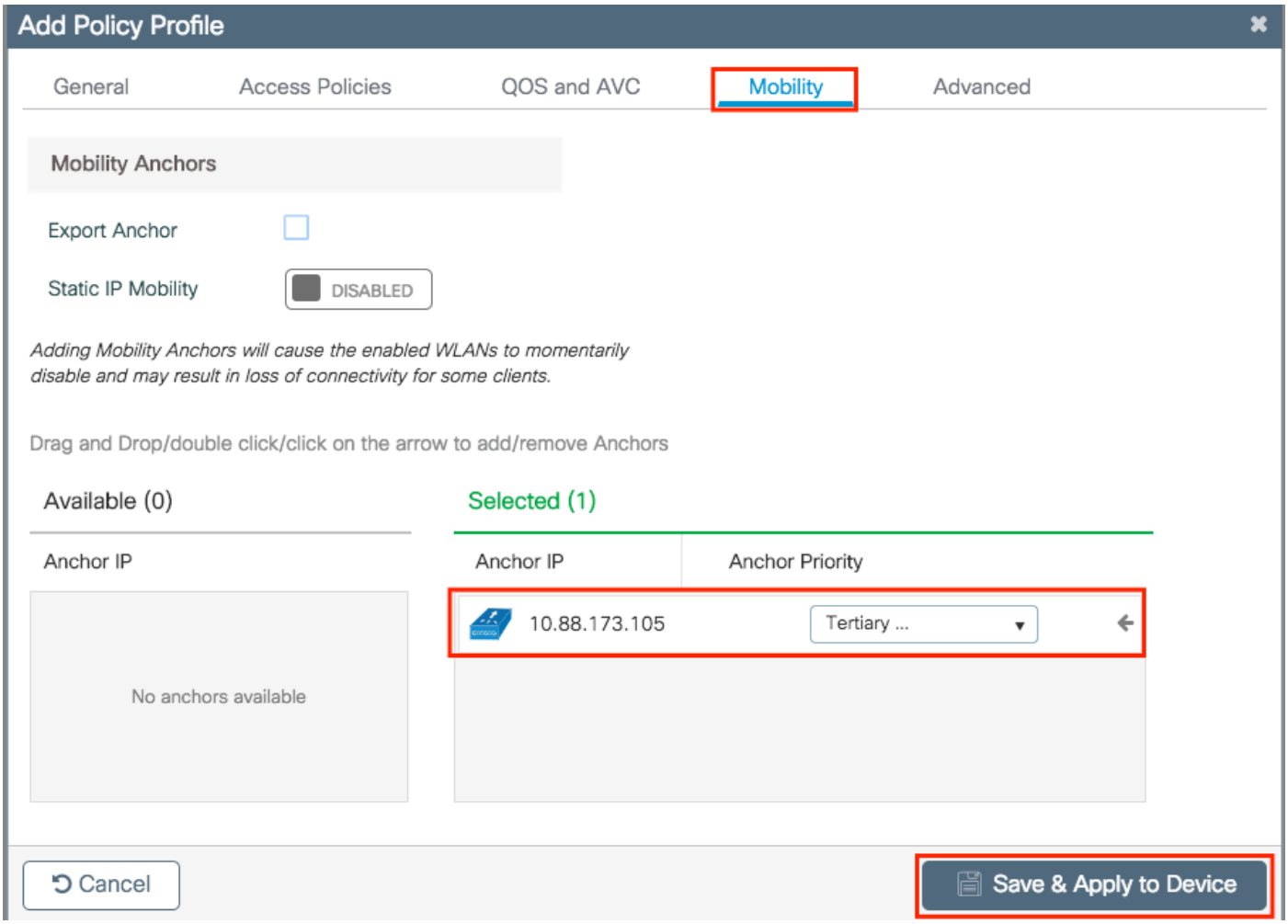
---

Step 3. Log in to the 9800 WLC (that acts as foreign) and create the anchor policy profile.

Navigate to Configuration > Tags & Profiles > Policy > + Add .

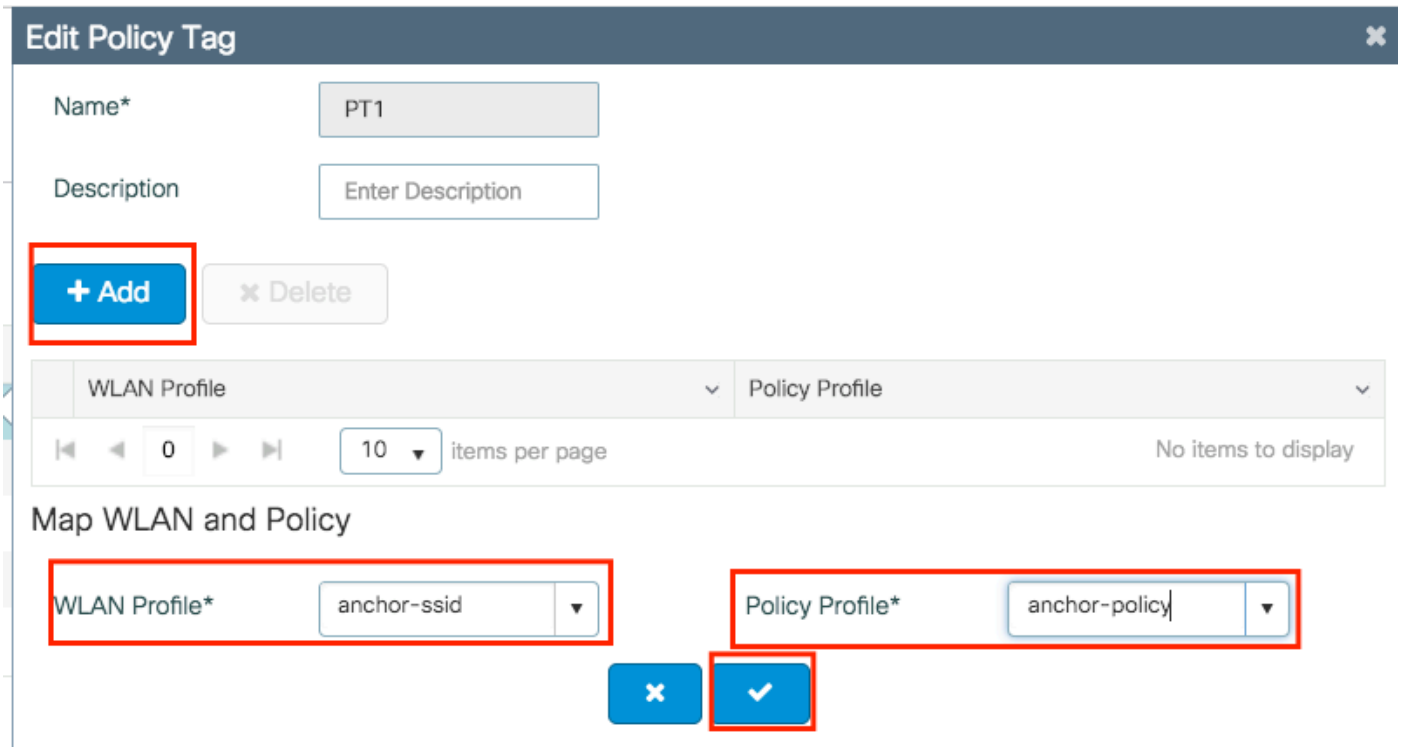



Navigate to Mobility tab and choose the anchor AireOS WLC. The 9800 WLC forwards the traffic of the SSID associated with this Policy Profile to the chosen anchor.

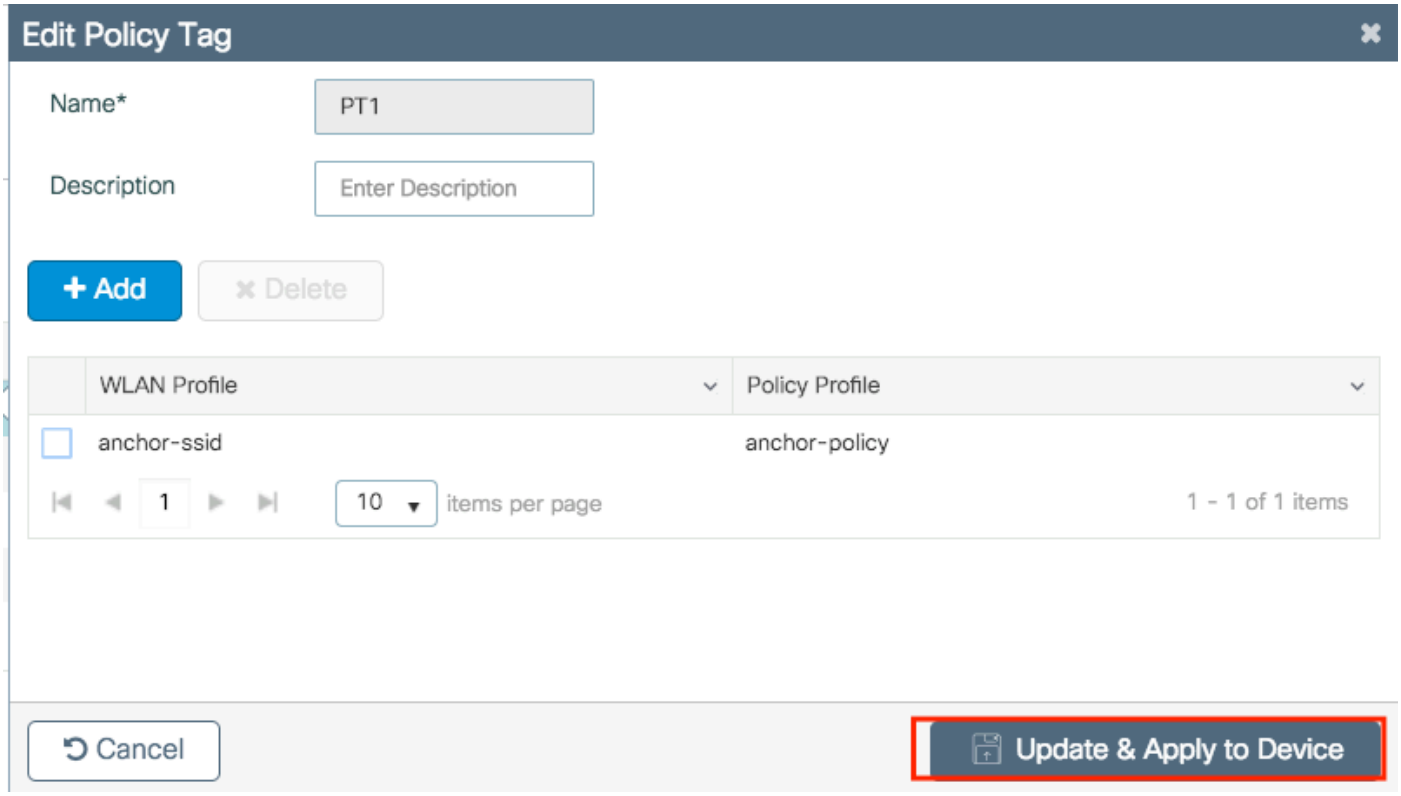



Step 4. Link the Policy Profile with the WLAN inside the Policy Tag assigned to the APs associated with the foreign controller that services this WLAN.

Navigate to Configuration > Tags & Profiles > Tags and either create a new one or use the one that exists.

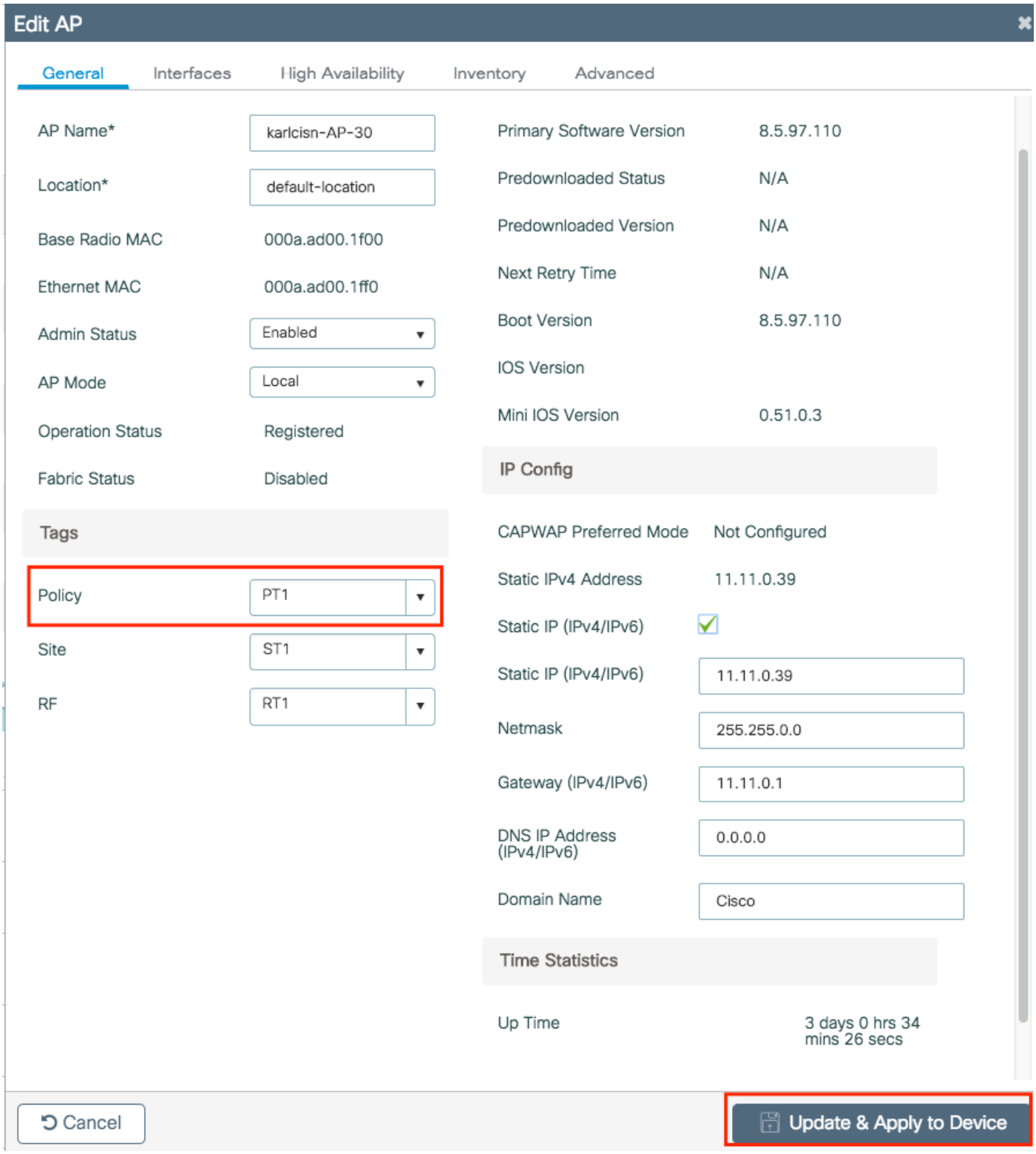


Ensure you choose Update & Apply to Device to apply the changes to the Policy Tag.




Step 5 (optional). Assign the Site to an AP or verify that it already has it.

Navigate to Configuration > Wireless > Access Points > AP name > General.




**Note**: Be aware that if you perform a change in the AP tag after you choose Update & Apply to Device, the AP restarts its tunnel CAPWAP, so it loses association with the 9800 WLC and then recovers it.

From the CLI:

```
# config t
# wireless profile policy anchor-policy
```

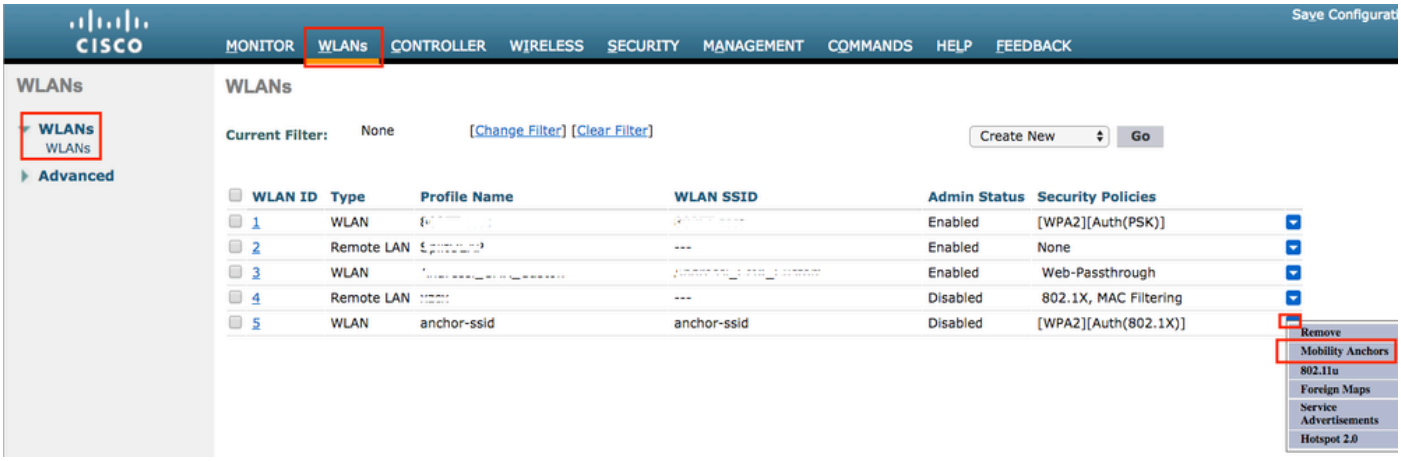
```
# mobility anchor 10.88.173.105 priority 3
# no shutdown
# exit

# wireless tag policy PT1
# wlan anchor-ssid policy anchor-policy
# exit

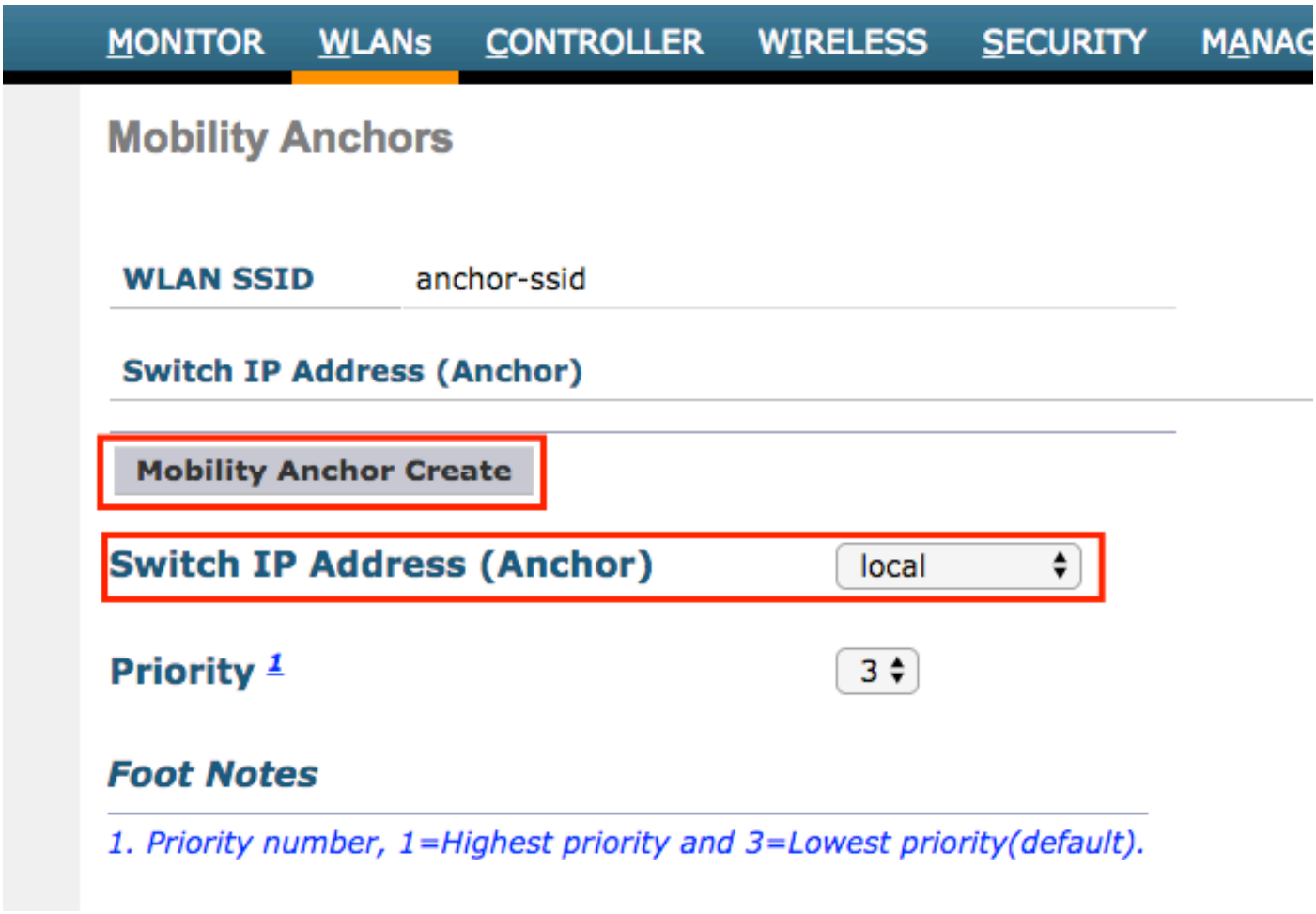
# ap aaaa.bbbb.dddd
# site-tag PT1
# exit
```

Step 6. Configure the AireOS WLC as the anchor.

Log in to AireOS and navigate to WLANs > WLANs. Choose the arrow to the right end of the WLAN row in order to navigate to the drop-down menu and choose Mobility Anchors.




Set it as the local anchor.

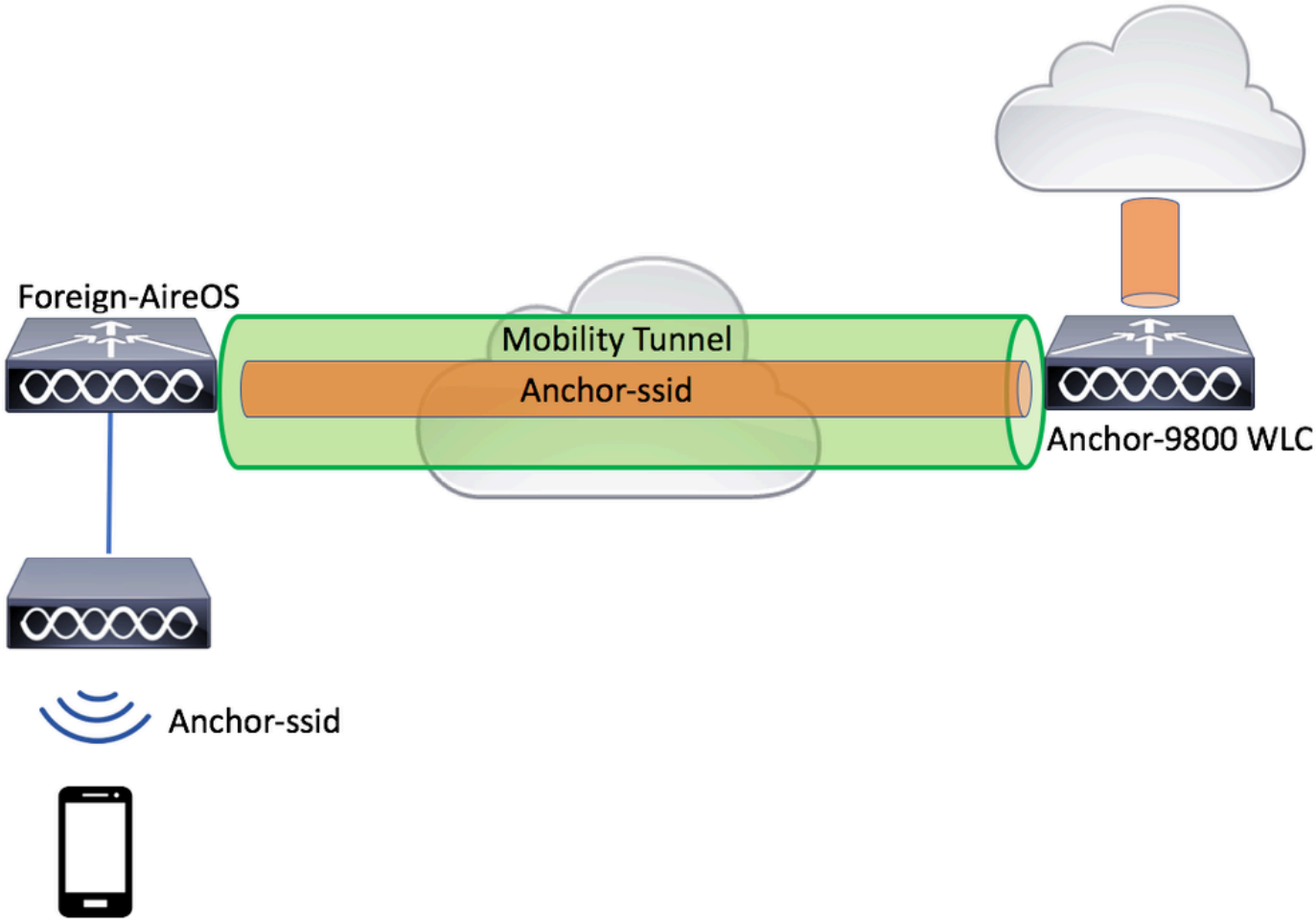



From the CLI:

```
> config wlan disable <wlan-id>
> config wlan mobility anchor add <wlan-id> <AireOS-WLC's-mgmt-interface>
> config wlan enable <wlan-id>
```

## Foreign AireOS - Anchor 9800 WLC

### AireOS Foreign with 9800 Anchor Network Diagram




**Configure a 9800 Foreign with an AireOS Anchor**

Step 1. Build a mobility tunnel between the Foreign 9800 WLC and Anchor AireOS WLC.

You can refer to this document: Configuring Mobility topologies on Catalyst 9800

Step 2. Create the desired SSID on both WLCs.

Supported security methods:

- Open
- MAC filter
- PSK
- Dot1x
- Local/External Web Authentication (LWA)
- Central Web Authentication (CWA)

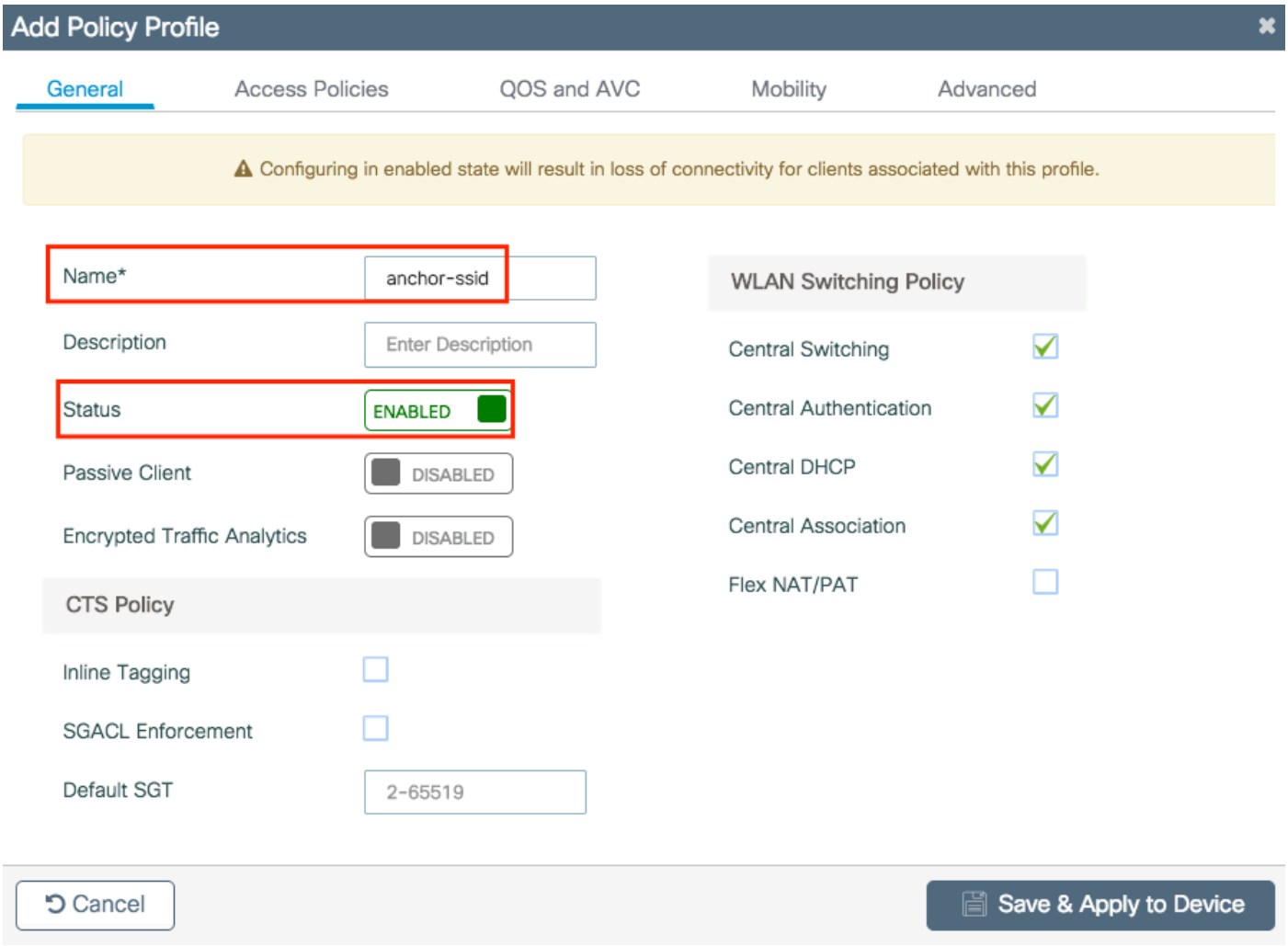
---

**Note**: Both AireOS WLC and 9800 WLC must have the same kind of configuration, otherwise anchor does not work.

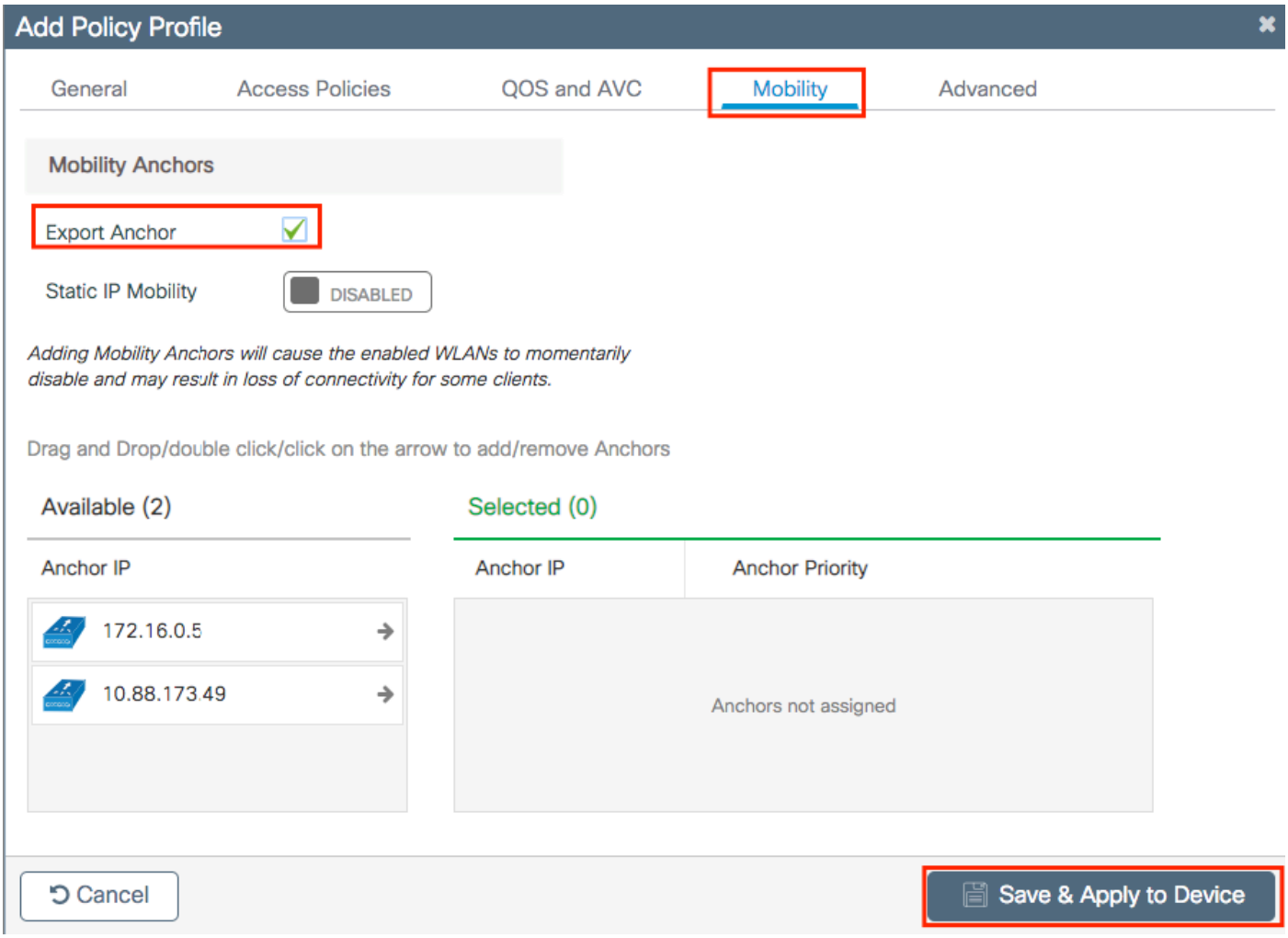
---

Step 3. Log in to the 9800 WLC (that acts as an anchor) and create the anchor policy profile.

Navigate to Configuration > Tags & Profiles > Policy > + Add.Ensure that the name of the Policy Profile on 9800 is the exact same name as the Profile name on the AireOS WLC, otherwise, it does not work.




Navigate to Mobility tab and enable Export Anchor.This instructs the 9800 WLC that it is the anchor 9800 WLC for any WLAN that uses that Policy Profile. When the foreign AireOS WLC sends the clients to the anchor 9800 WLC, it informs about the WLAN name that the client is assigned to, so the anchor 9800 WLC knows which local WLAN configuration to use and it also uses this name to know which local Policy Profile to use.




**Note**: Ensure you use this policy profile exclusively to receive traffic from foreign controllers.

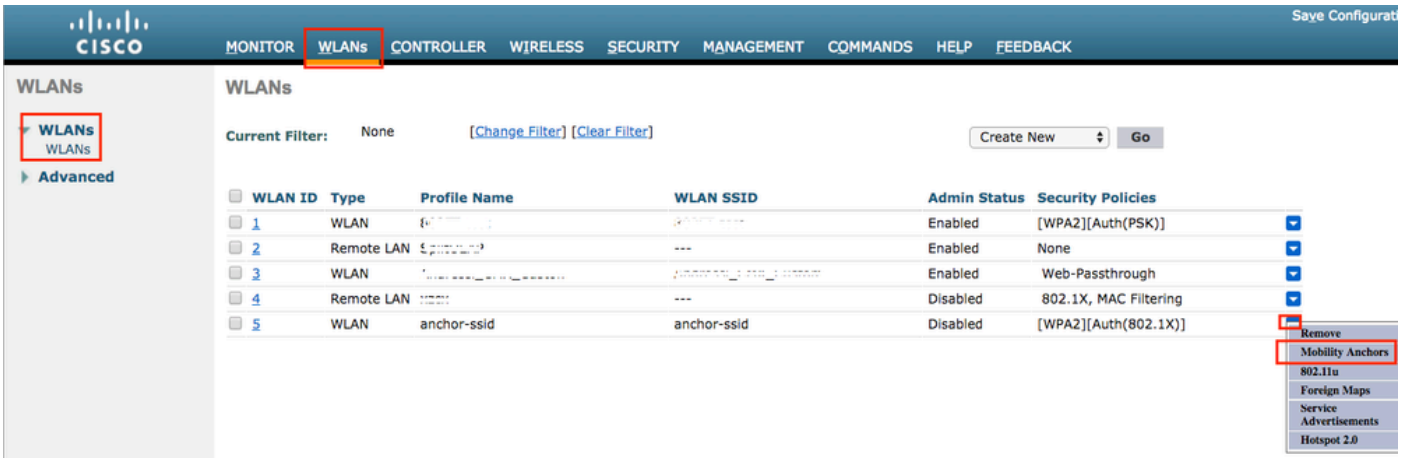
From the CLI:

```
Anchor 9800 WLC

# config t
# wireless profile policy <anchor-policy>
# mobility anchor
# vlan <VLAN-id_VLAN-name>
# no shutdown
# exit
```

Step 4. Configure the AireOS WLC as foreign.

Log in to AireOS and navigate to WLANs > WLANs.Navigate to the blow arrow at the end of the WLAN row and choose Mobility Anchor**s** .




Set the 9800 WLC as an anchor for this SSID.




From the CLI:

```
> config wlan disable <wlan-id>
> config wlan mobility anchor add <wlan-id> <9800 WLC's-mgmt-interface>
> config wlan enable <wlan-id>
```

# Verification

You can use these commands to verify the configuration and the state of the wireless clients with the use of a foreign/anchor SSID.

### Verify on the 9800 WLC

```
# show run wlan
# show wlan summary
# show wireless client summary
# show wireless mobility summary
# show ap tag summary
# show ap <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>
```

### Verify on the AireOS WLC

```
> show client summary
> show client detail <client-mac-addr>
> show wlan summary
> show wlan <wlan-id>
```

# Troubleshoot

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

---

 **Note**: Depending on the volume of logs generated, you can go back a 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 refer to these steps. (Ensure you log the session to a text file)

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

```
# show clock
```

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

```
# show logging
```

Step 3. Collect the always-on notice level traces for the specific mac or IP address. Remote mobility peer can filter this, if you suspect a mobility tunnel issue, or by wireless client mac address.

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

Step 4. 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) traces, which provides debug-level traces for all processes that interact with the specified condition (client mac address in this case). In order to enable conditional debugging, refer to these steps.

Step 5. Ensure there are no debug conditions enabled.

```
# clear platform condition all
```

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

These 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 the 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.
```

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 the logs were already written in the controller memory and you only need to populate a more verbose view of them.

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

**Note**: This command output returns traces for all logging levels for all processes and is quite voluminous. 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.

## Verify the AireOS WLC

You can run this command to monitor the activity of a wireless client on an AireOS WLC.

```
> debug client <client-mac-add>
```