Understand FlexConnect on Catalyst 9800 Wireless Controller

Contents

Introduction

Background Information

Prerequisites

Requirements

Components Used

Network Diagram

Configurations

Create/Modify a WLAN Profile

Create/Modify a Policy Profile

Create/Modify a Policy Tag

Create/Modify a Flex Profile

Create/Modify a Site Tag

Policy Tag Assignment to AP

Policy Tag Assignment per AP

Policy Tag Assignment for Multiple APs

Flexconnect ACLs

Centrally switched WLAN

Locally switched WLAN

Verify if the ACL is applied

Verification

VLANs/Interfaces Configuration

WLAN Configuration

AP Configuration

Tag Configuration

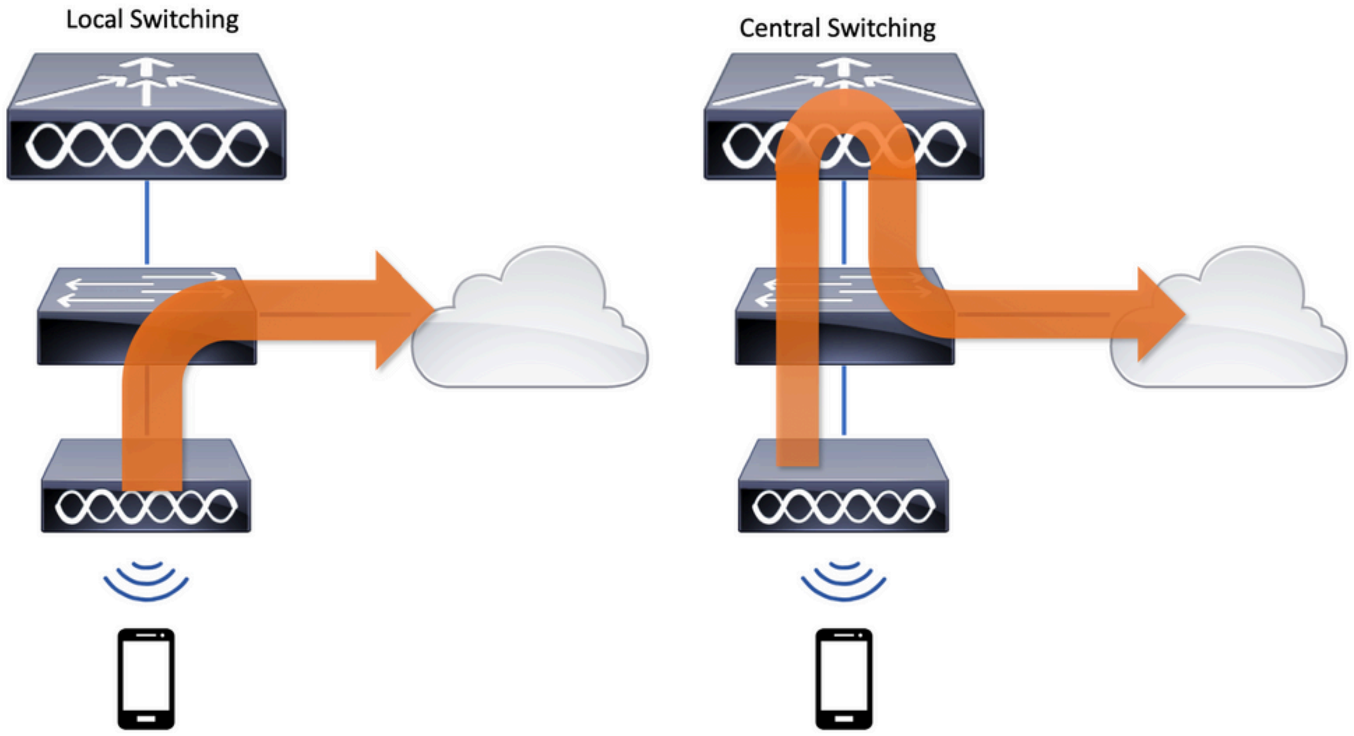
Profile Configuration

Introduction

This document describes the FlexConnect feature and its general configuration on 9800 Wireless Controllers.

Background Information

FlexConnect refers to the capability of an Access Point (AP) to determine if the traffic from the wireless clients is put directly on the network at the AP level (Local Switching) or if the traffic is centralized to the 9800 controller (Central Switching).



Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

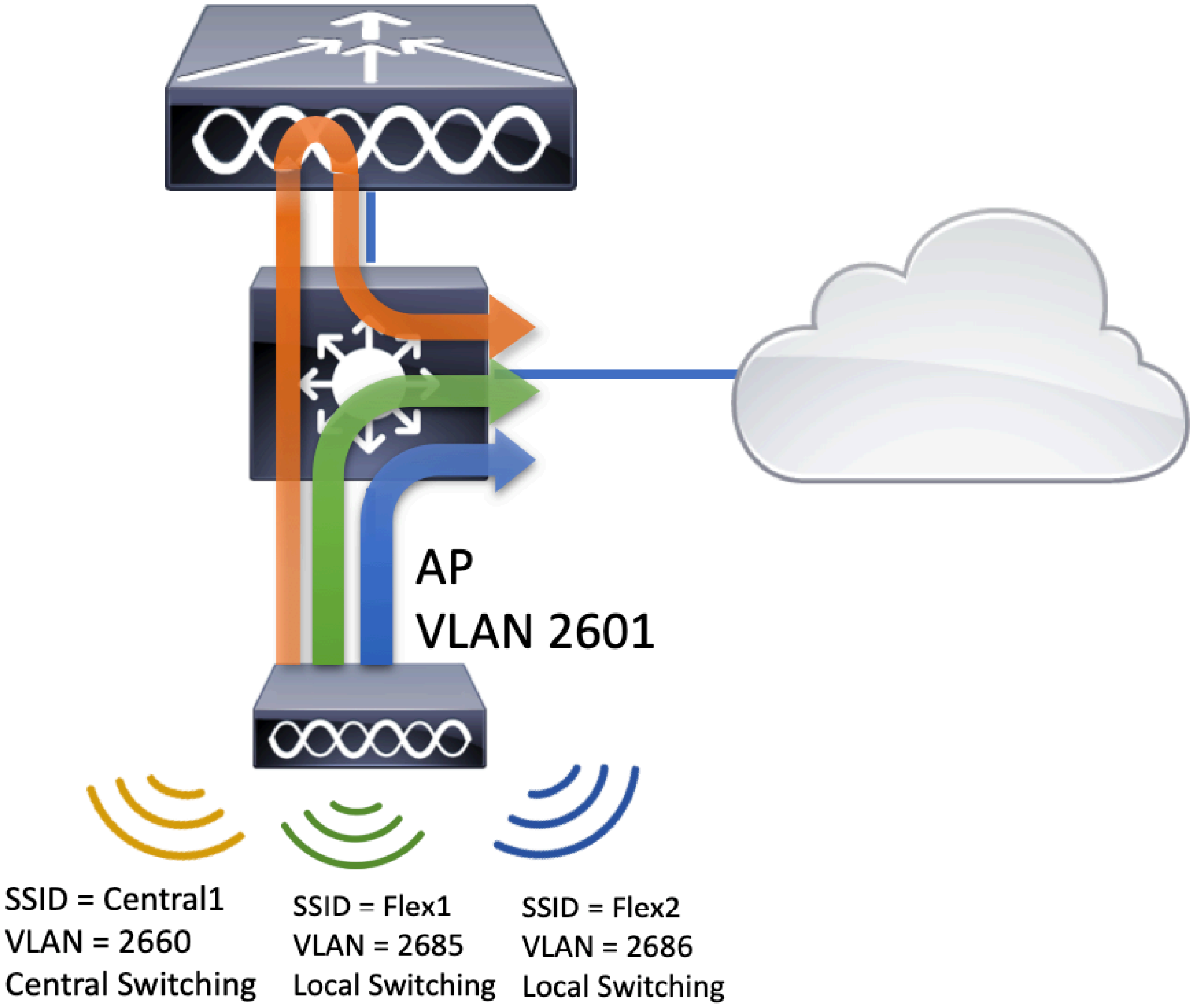
The information in this document is based on these software and hardware versions:

- Cisco Catalyst 9800 Wireless Controllers with Cisco IOS®-XE Gibraltar v17.3.x

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.

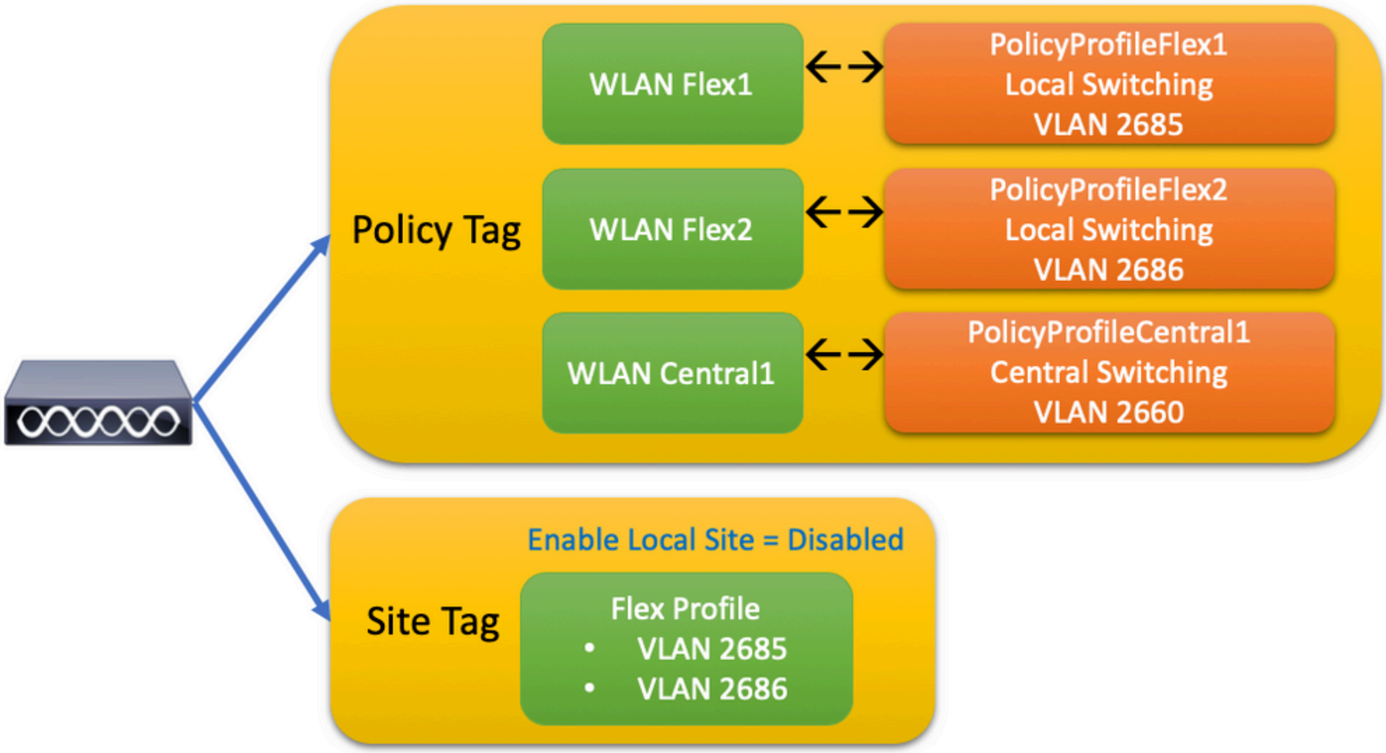
Network Diagram

This document is based on this topology:



Configurations

This is the visual scheme of the configuration that is needed to accomplish the scenario of this document:



To configure a FlexConnect Local Switching Service Set Identifier (SSID), here are the general steps to follow:

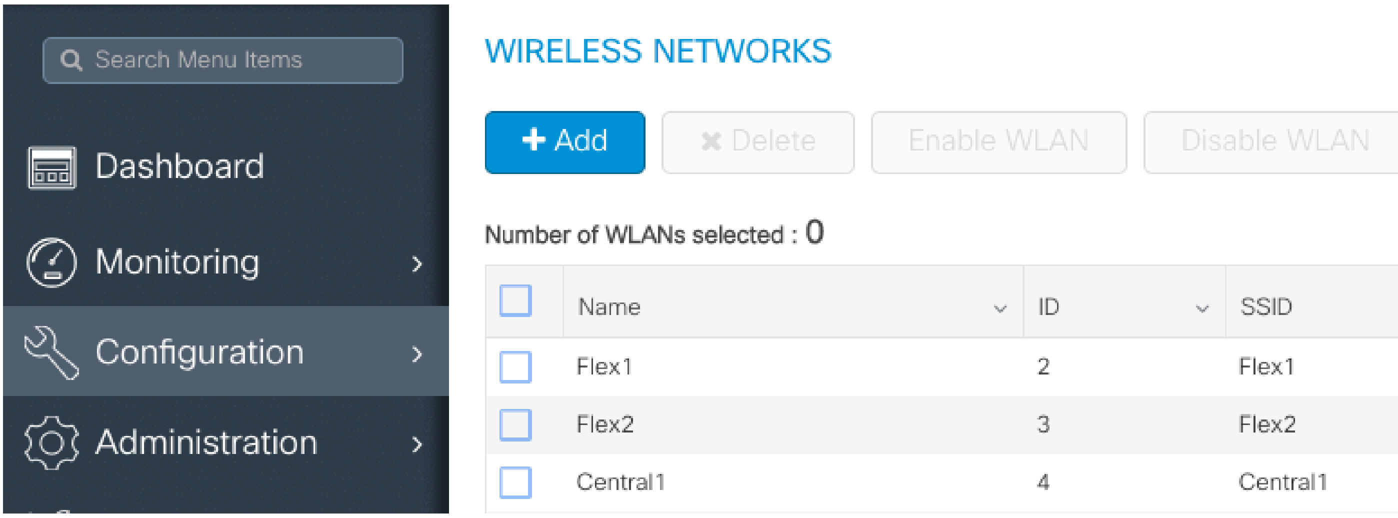
1. Create/Modify a WLAN profile
2. Create/Modify a Policy Profile
3. Create/Modify a Policy Tag
4. Create/Modify a Flex Profile
5. Create/Modify a Site Tag
6. Policy Tag Assignment to AP

These sections explain how to configure each them, step by step.

Create/Modify a WLAN Profile

You can use this guide to create the three SSIDs:

Create your SSID

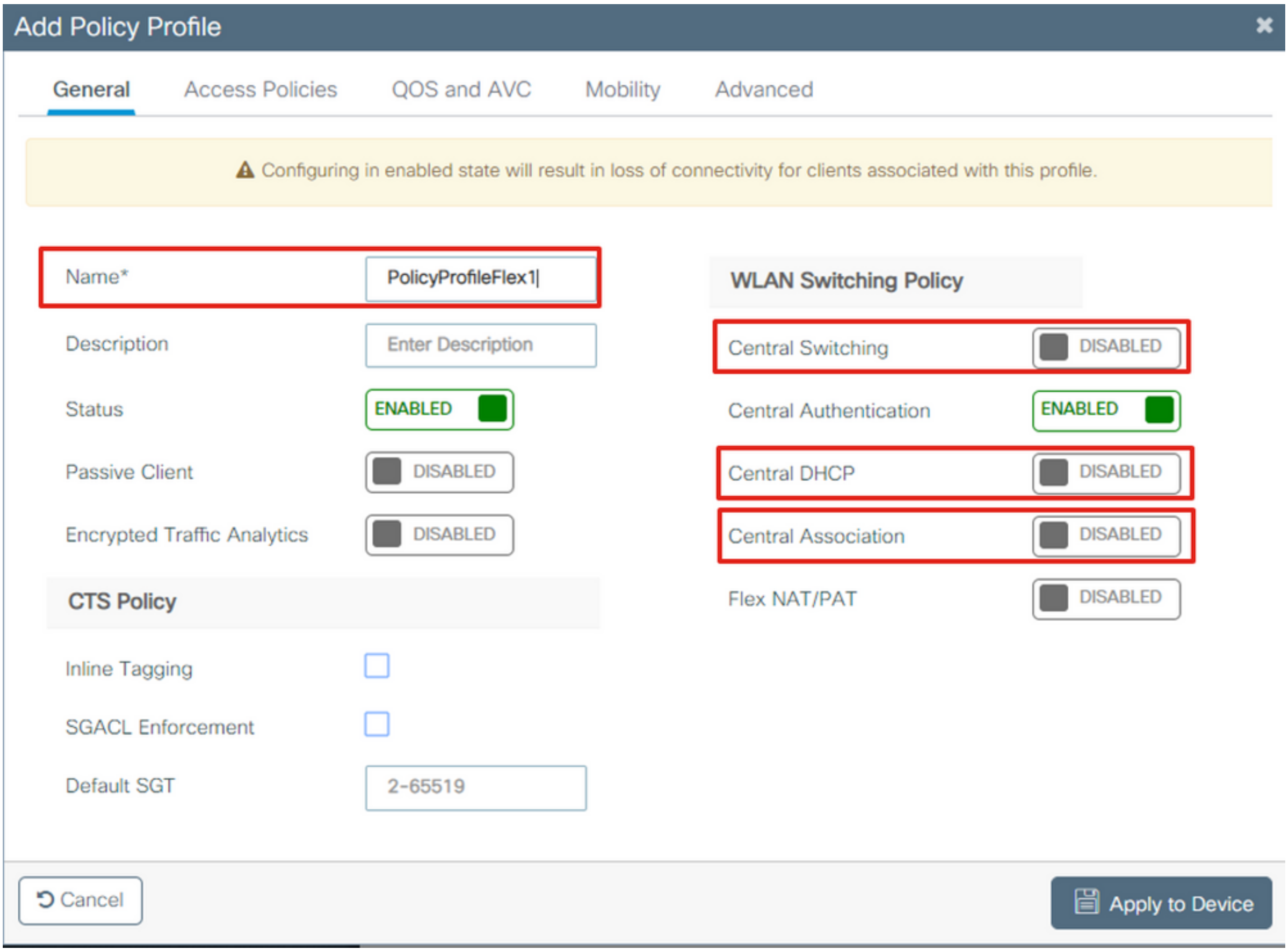


Number of WLANs selected : 0

□	Name	ID	SSID
□	Flex1	2	Flex1
□	Flex2	3	Flex2
□	Central1	4	Central1

Create/Modify a Policy Profile

Step 1. Navigate to Configuration > Tags & Profiles > Policy. Either select the name of one that already exists or click **+ Add** to add a new one.



⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name*	PolicyProfileFlex1
Description	Enter Description
Status	ENABLED
Passive Client	DISABLED
Encrypted Traffic Analytics	DISABLED

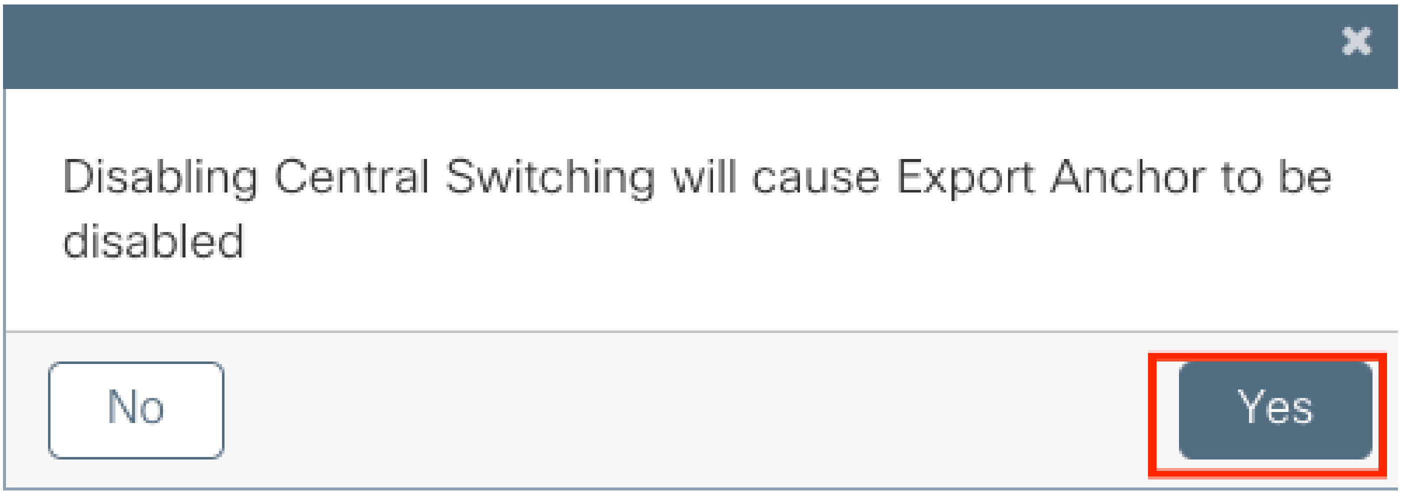
CTS Policy

Inline Tagging	□
SGACL Enforcement	□
Default SGT	2-65519

WLAN Switching Policy

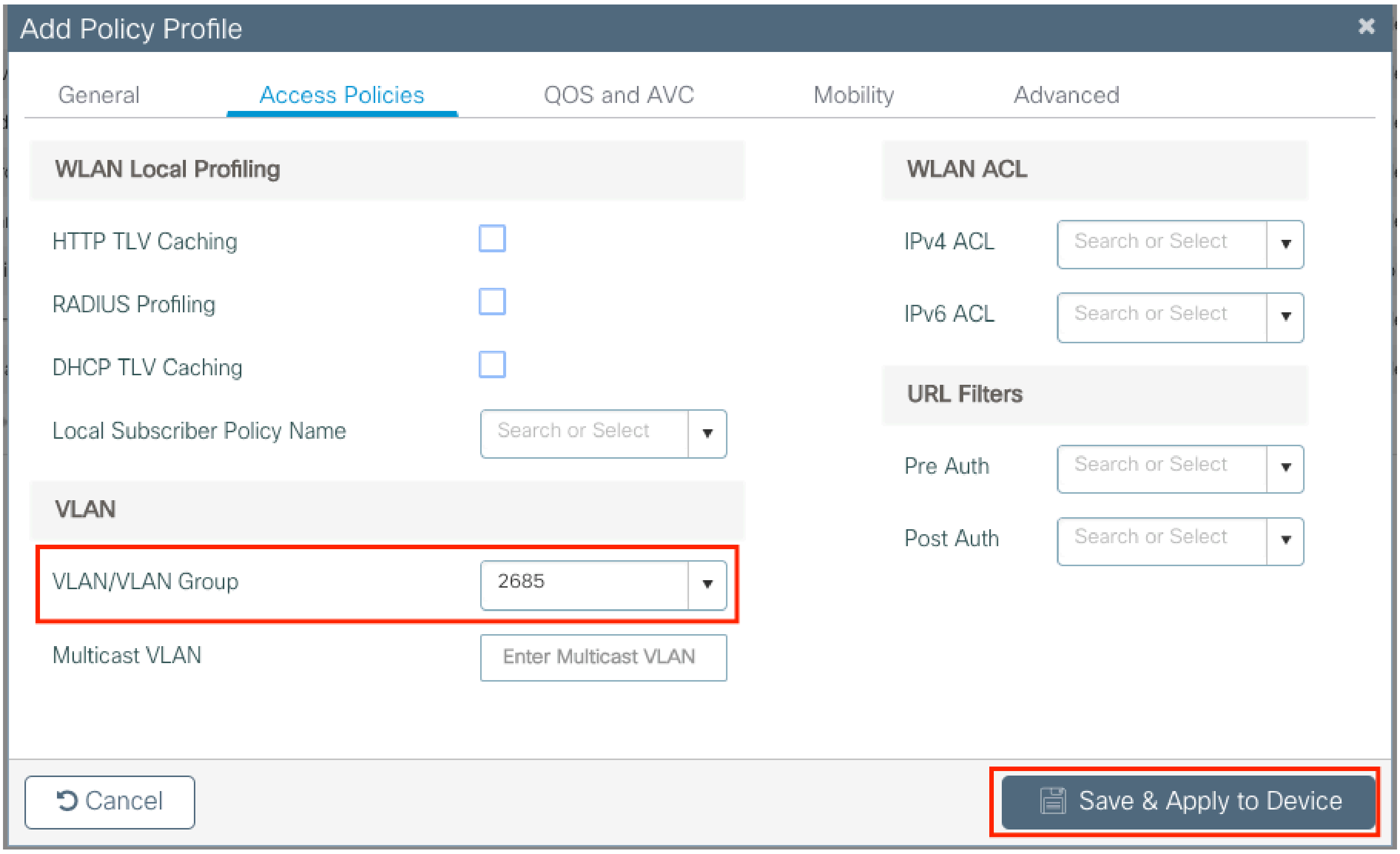
Central Switching	DISABLED
Central Authentication	ENABLED
Central DHCP	DISABLED
Central Association	DISABLED
Flex NAT/PAT	DISABLED

When you disable Central Switching this warning message appears, click Yes and continue with the configuration.



Disabling Central Switching will cause Export Anchor to be disabled

Step 2. Go to the Access Policies tab and type the VLAN (You do not see it in the drop-down list because this VLAN does not exists on the 9800 WLC). After that, click Save & Apply to Device.



Add Policy Profile

WLAN Local Profiling

HTTP TLV Caching □

RADIUS Profiling □

DHCP TLV Caching □

Local Subscriber Policy Name: Search or Select

VLAN

VLAN/VLAN Group: 2685

Multicast VLAN: Enter Multicast VLAN

WLAN ACL

IPv4 ACL: Search or Select

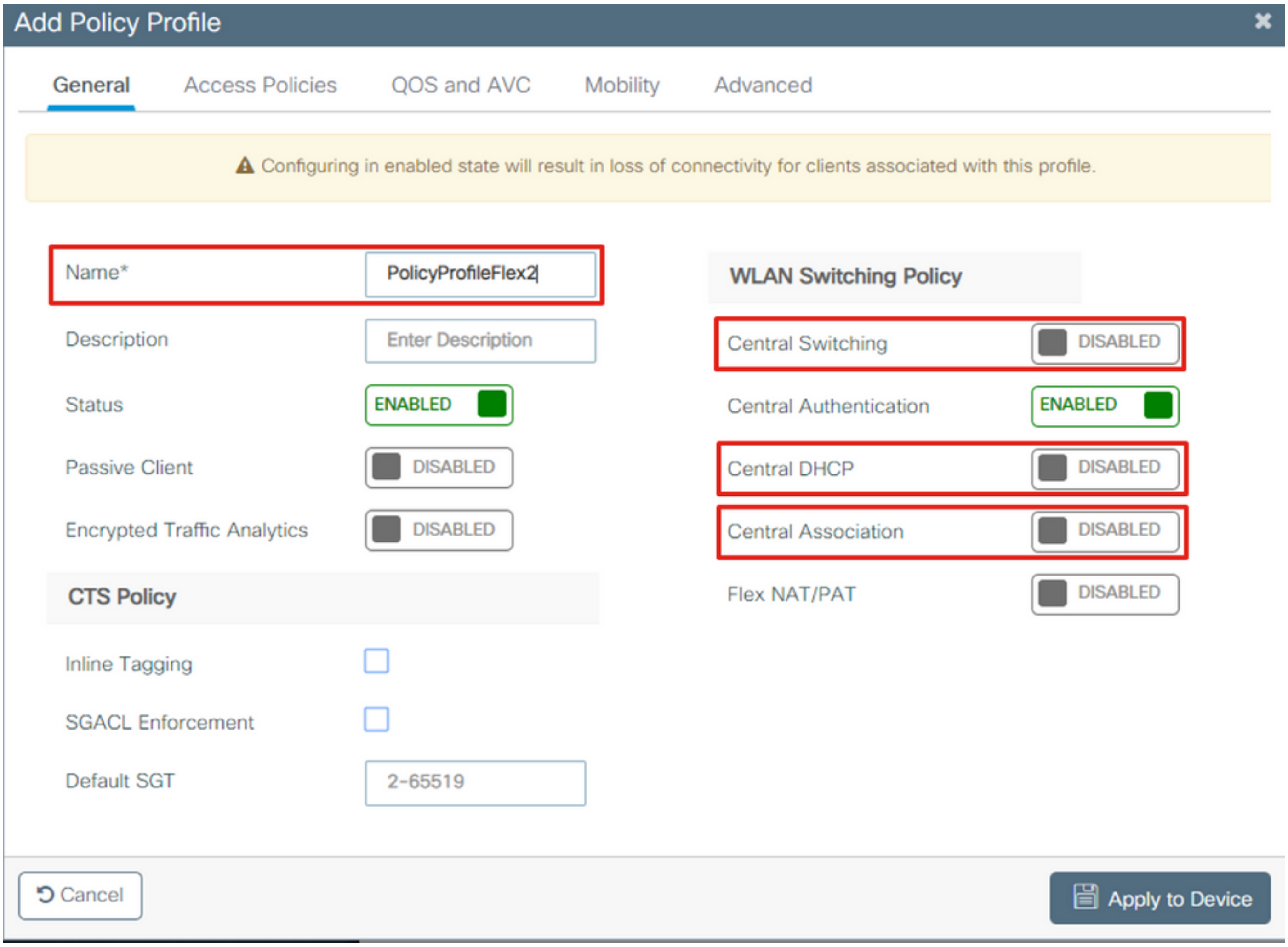
IPv6 ACL: Search or Select

URL Filters

Pre Auth: Search or Select

Post Auth: Search or Select

Step 3. Repeat the same for the PolicyProfileFlex2.



Add Policy Profile

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name*: PolicyProfileFlex2

Description: Enter Description

Status: ENABLED

Passive Client: DISABLED

Encrypted Traffic Analytics: DISABLED

CTS Policy

Inline Tagging □

SGACL Enforcement □

Default SGT: 2-65519

WLAN Switching Policy

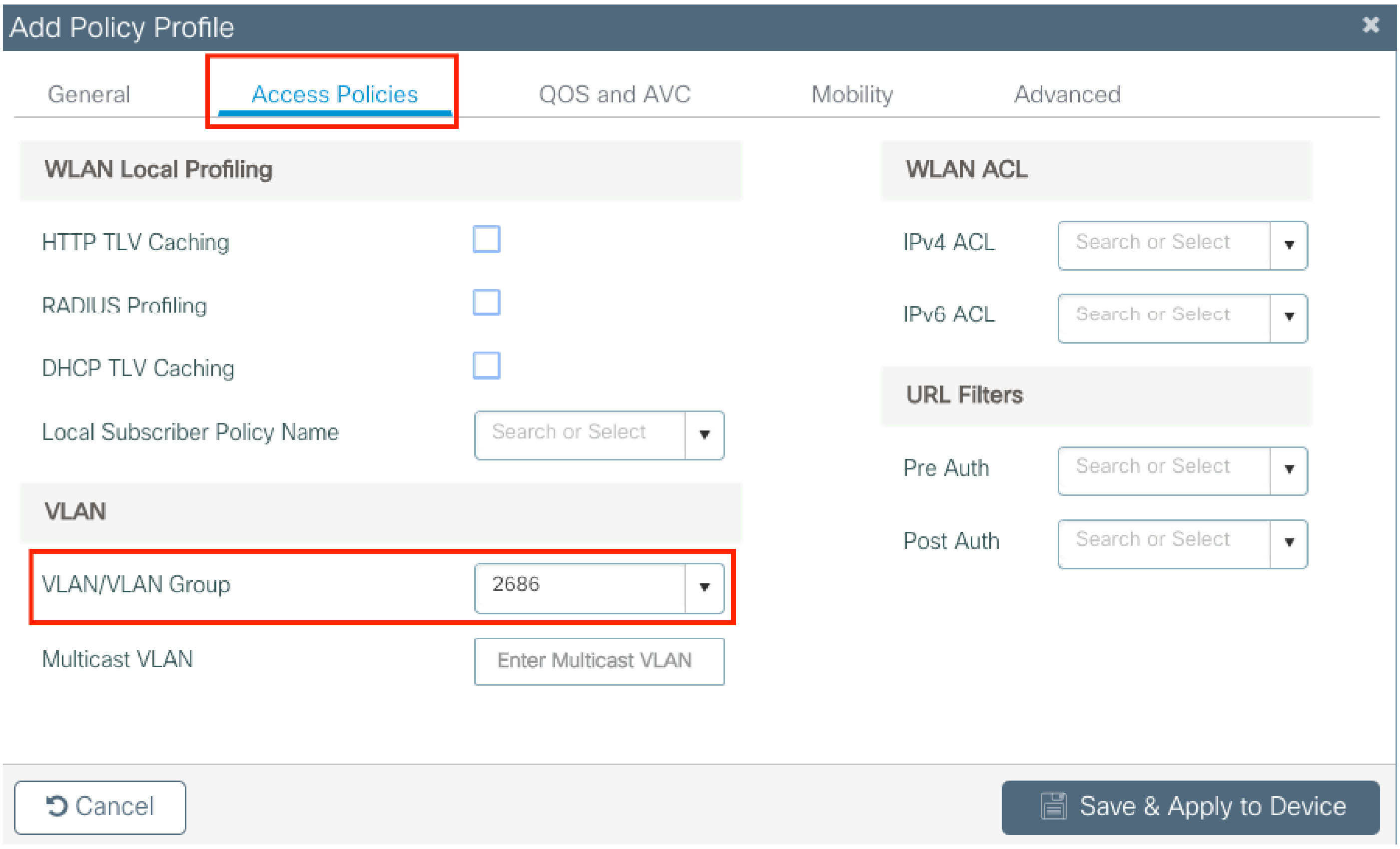
Central Switching: DISABLED

Central Authentication: ENABLED

Central DHCP: DISABLED

Central Association: DISABLED

Flex NAT/PAT: DISABLED



Add Policy Profile

WLAN Local Profiling

HTTP TLV Caching □

RADIUS Profiling □

DHCP TLV Caching □

Local Subscriber Policy Name: Search or Select

VLAN

VLAN/VLAN Group: 2686

Multicast VLAN: Enter Multicast VLAN

WLAN ACL

IPv4 ACL: Search or Select

IPv6 ACL: Search or Select

URL Filters

Pre Auth: Search or Select

Post Auth: Search or Select

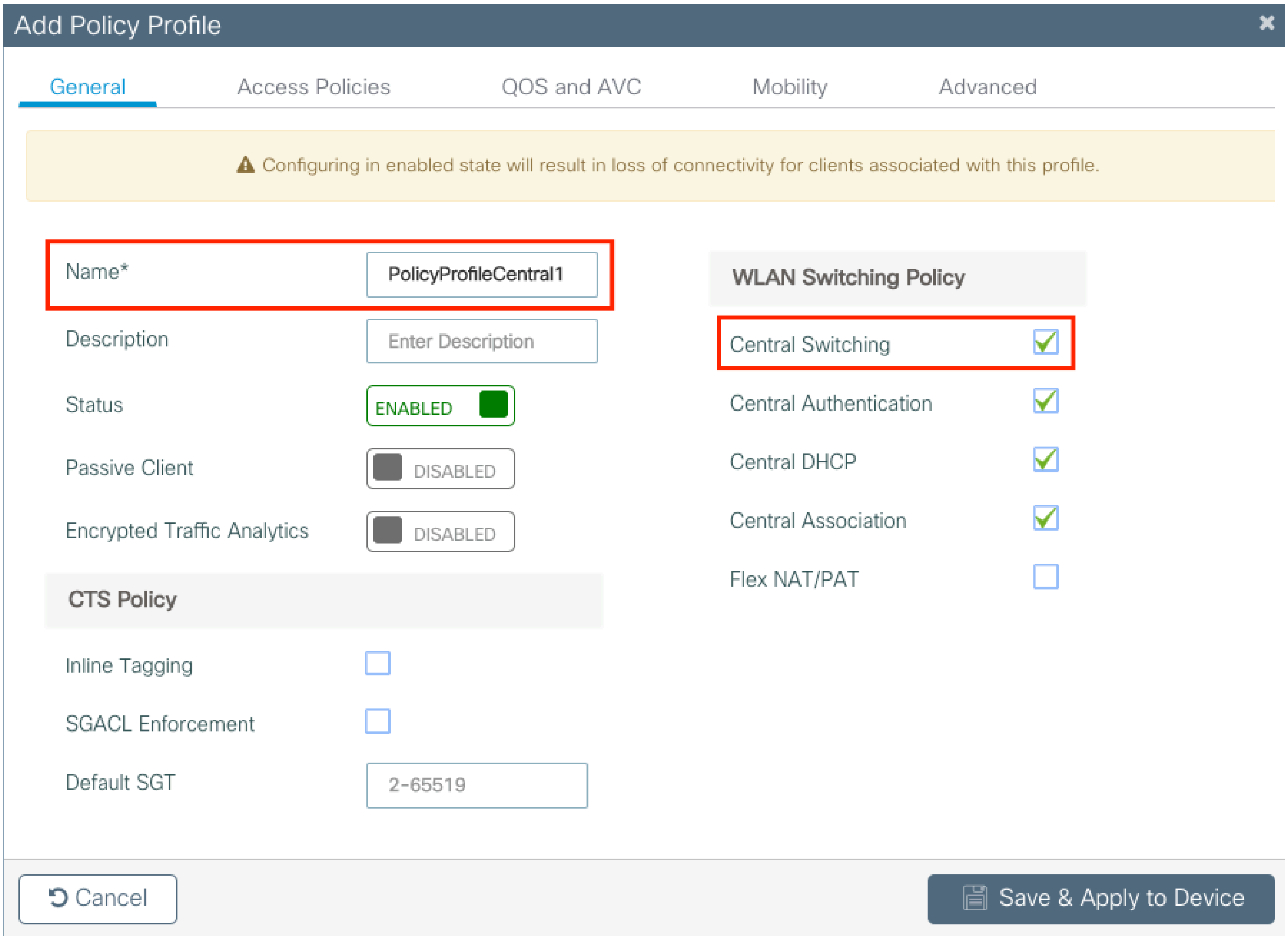
Step 4. For the centrally switched SSID, ensure its needed VLAN exists on the 9800 WLC and if not, create it.

Note: In FlexConnect APs with locally switched WLANs, the traffic is switched at the AP and the DHCP requests from the client goes into the wired network by the AP interface directly. The AP does not have any SVI in the client subnet, so it is not able to do DHCP proxy; and thus, the DHCP relay configuration (DHCP Server IP Address), in the Policy Profile > Advanced tab, has no meaning for locally switched WLANs. In these scenarios, the switchport needs to allow the client VLAN and then, if the DHCP server is in a different VLAN, configure the IP helper in the client SVI/default gateway so it knows where to send the DHCP request from the client.

Declare Client VLANs

Step 5. Create a Policy Profile for the Central SSID.

Navigate to Configuration > Tags & Profiles > Policy. Either select the name of one that already exists or click **+ Add** to add a new one.



⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name* PolicyProfileCentral1

Description Enter Description

Status ENABLED

Passive Client DISABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

Inline Tagging □

SGACL Enforcement □

Default SGT 2-65519

WLAN Switching Policy

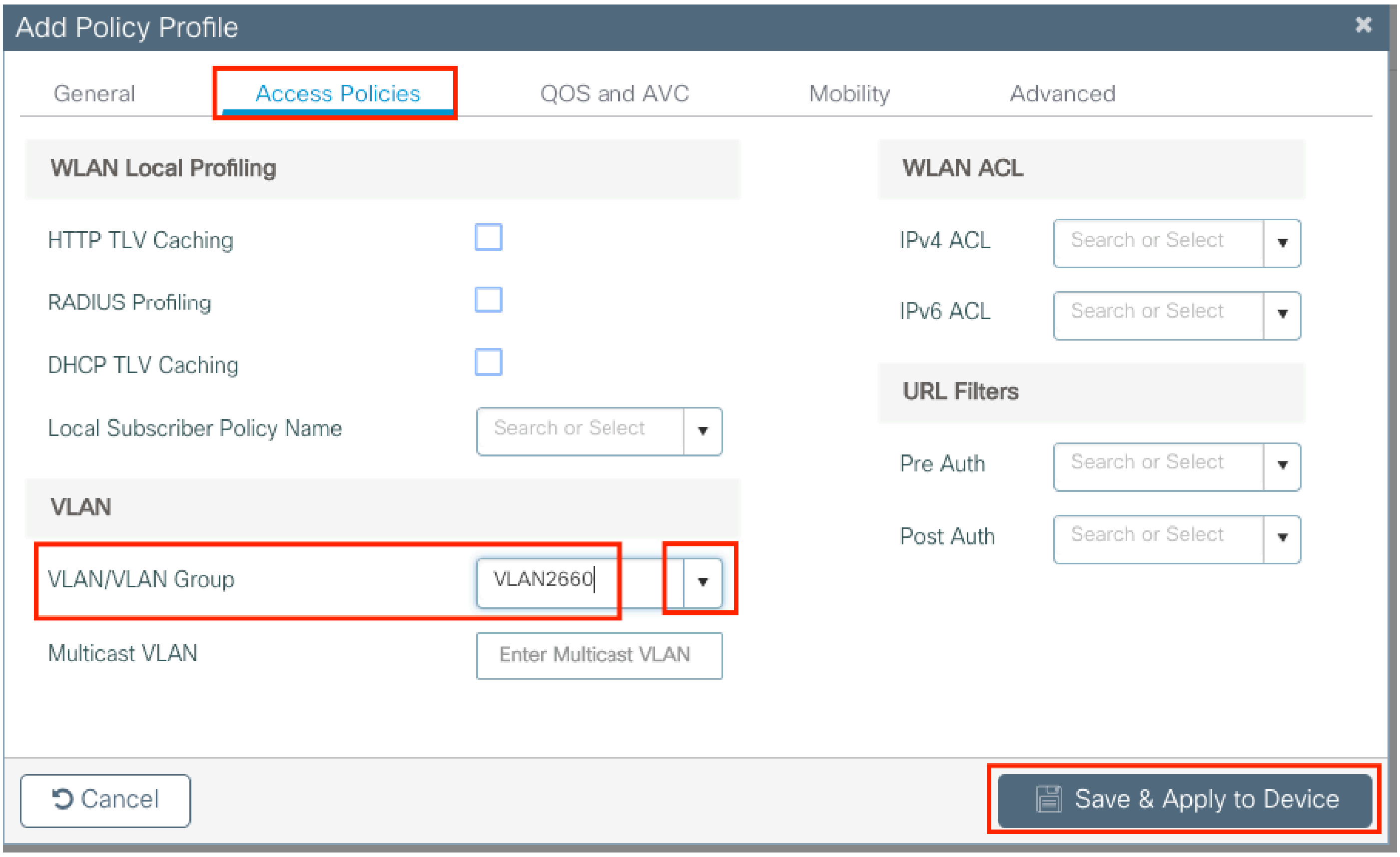
Central Switching ☑

Central Authentication ☑

Central DHCP ☑

Central Association ☑

Flex NAT/PAT □



Add Policy Profile

General | Access Policies | QOS and AVC | Mobility | Advanced

WLAN Local Profiling

HTTP TLV Caching □

RADIUS Profiling □

DHCP TLV Caching □

Local Subscriber Policy Name: Search or Select ▾

VLAN

VLAN/VLAN Group: VLAN2660 ▾

Multicast VLAN: Enter Multicast VLAN

WLAN ACL

IPv4 ACL: Search or Select ▾

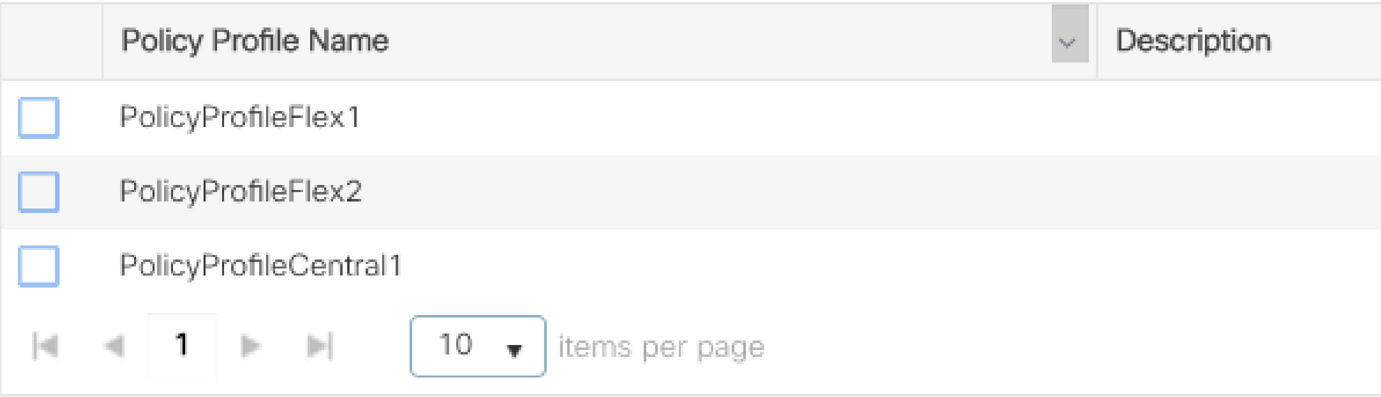
IPv6 ACL: Search or Select ▾

URL Filters

Pre Auth: Search or Select ▾

Post Auth: Search or Select ▾

As a result, there are three Policy Profiles.



	Policy Profile Name	Description
□	PolicyProfileFlex1	
□	PolicyProfileFlex2	
□	PolicyProfileCentral1	

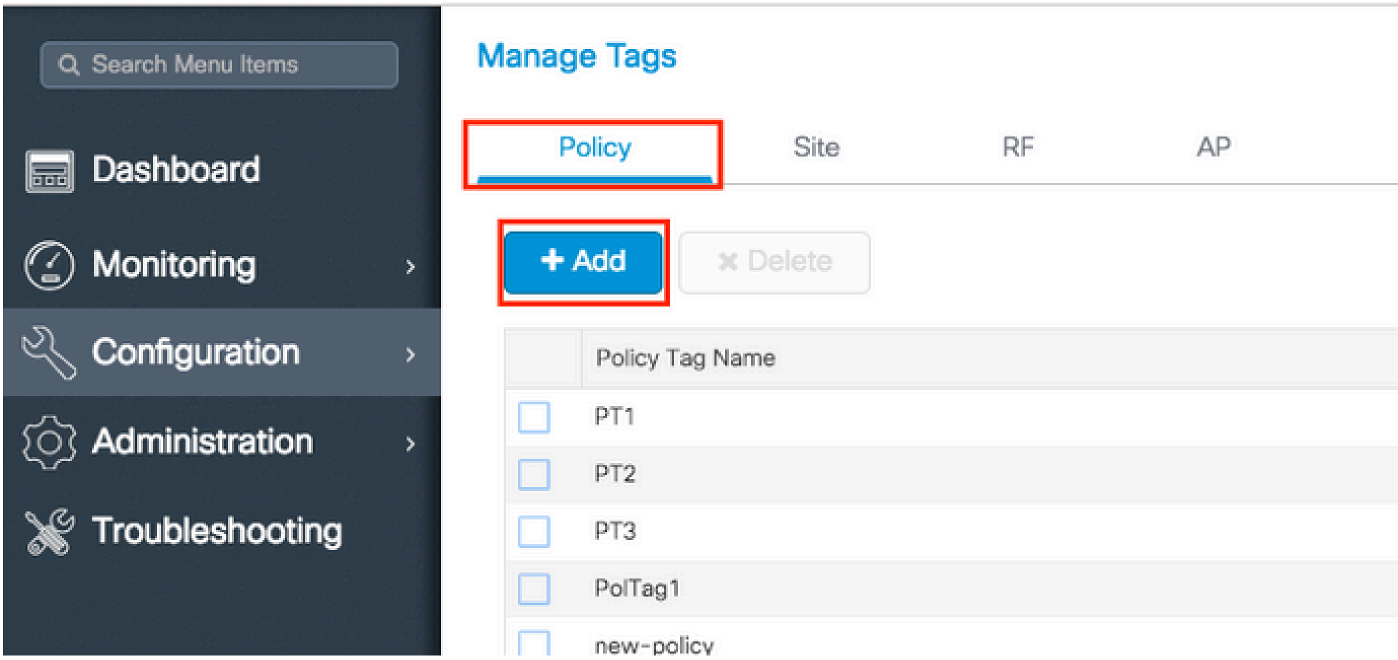
CLI:

```
# config t

# vlan 2660
# exit

# wireless profile policy PolicyProfileFlex1
# no central switching
# vlan 2685
# no shutdown
# exit

# wireless profile policy PolicyProfileFlex2
# no central switching
# vlan 2686
# no shutdown
# exit

# wireless profile policy PolicyProfileCentral1
# vlan VLAN2660
# no shutdown
# end
```

Create/Modify a Policy Tag

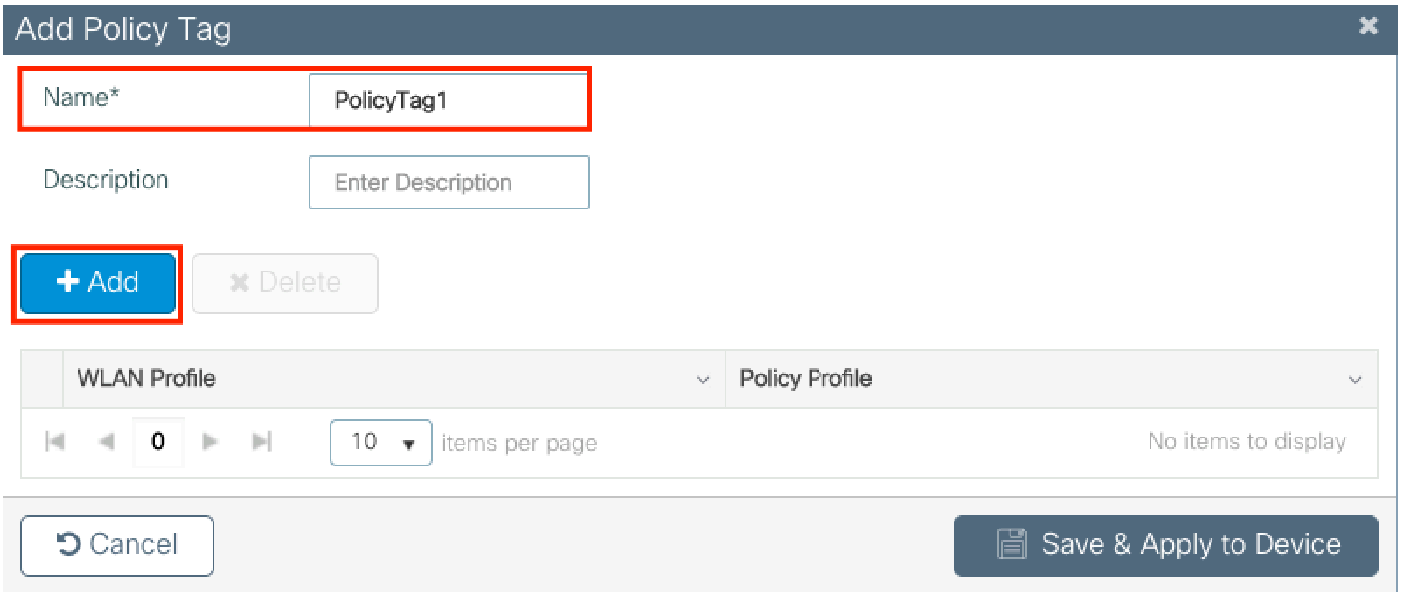
The Policy Tag is the element that allows you to specify which SSID is linked to which Policy Profile.

Step 1. Navigate to Configuration > Tags & Profiles > Tags > Policy. Either select the name of one that already exists or click + **Add** to add a new one.



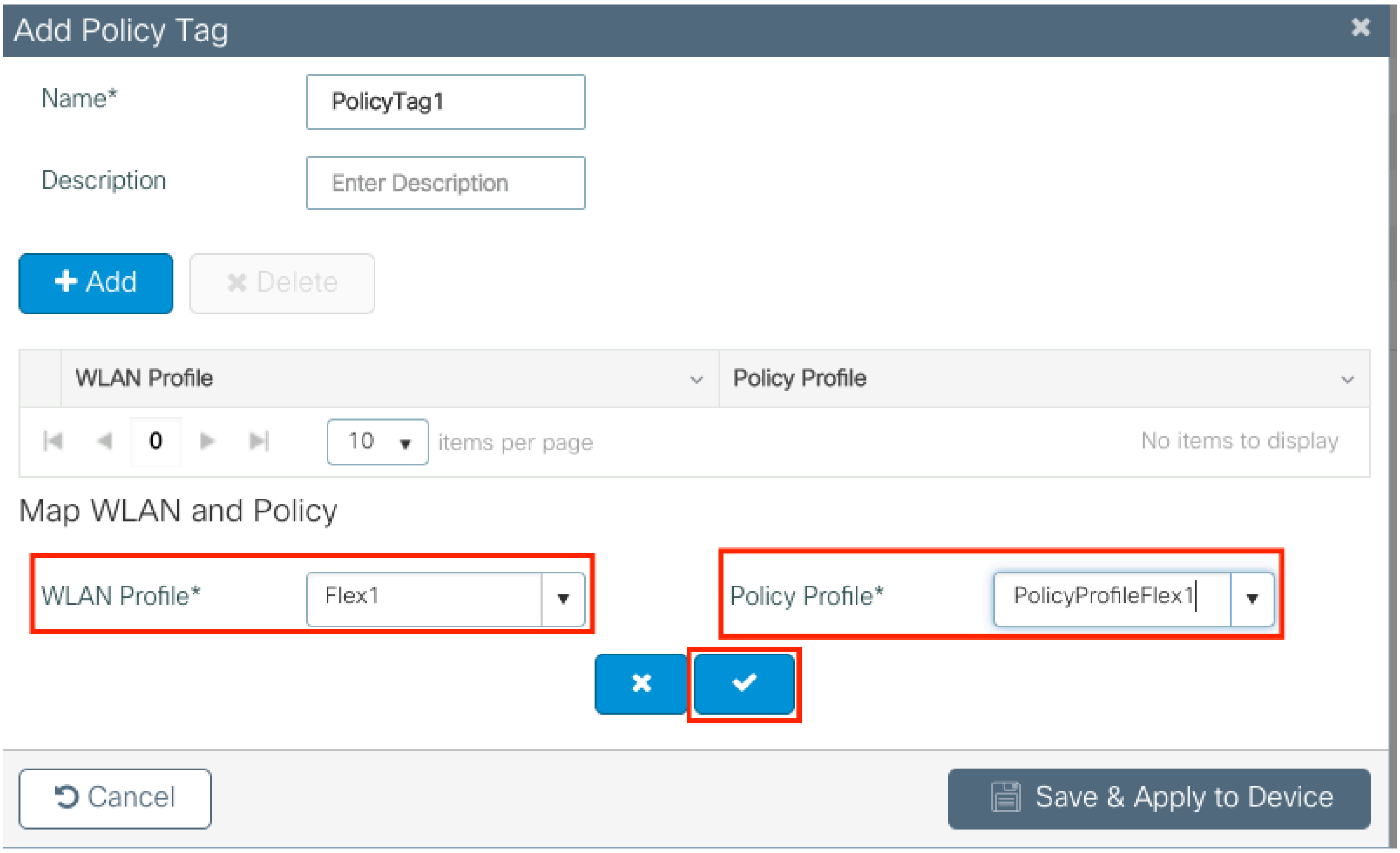
	Policy Tag Name
□	PT1
□	PT2
□	PT3
□	PolTag1
□	new-policy

Step 2. Inside the Policy Tag, click **+Add**, from the drop-down list select the **WLAN Profile** name to add to the Policy Tag and Policy Profile to which you want to link it. After that click the checkmark.



Name* PolicyTag1

Description Enter Description



Add Policy Tag

Name*: PolicyTag1

Description: Enter Description

	WLAN Profile	Policy Profile

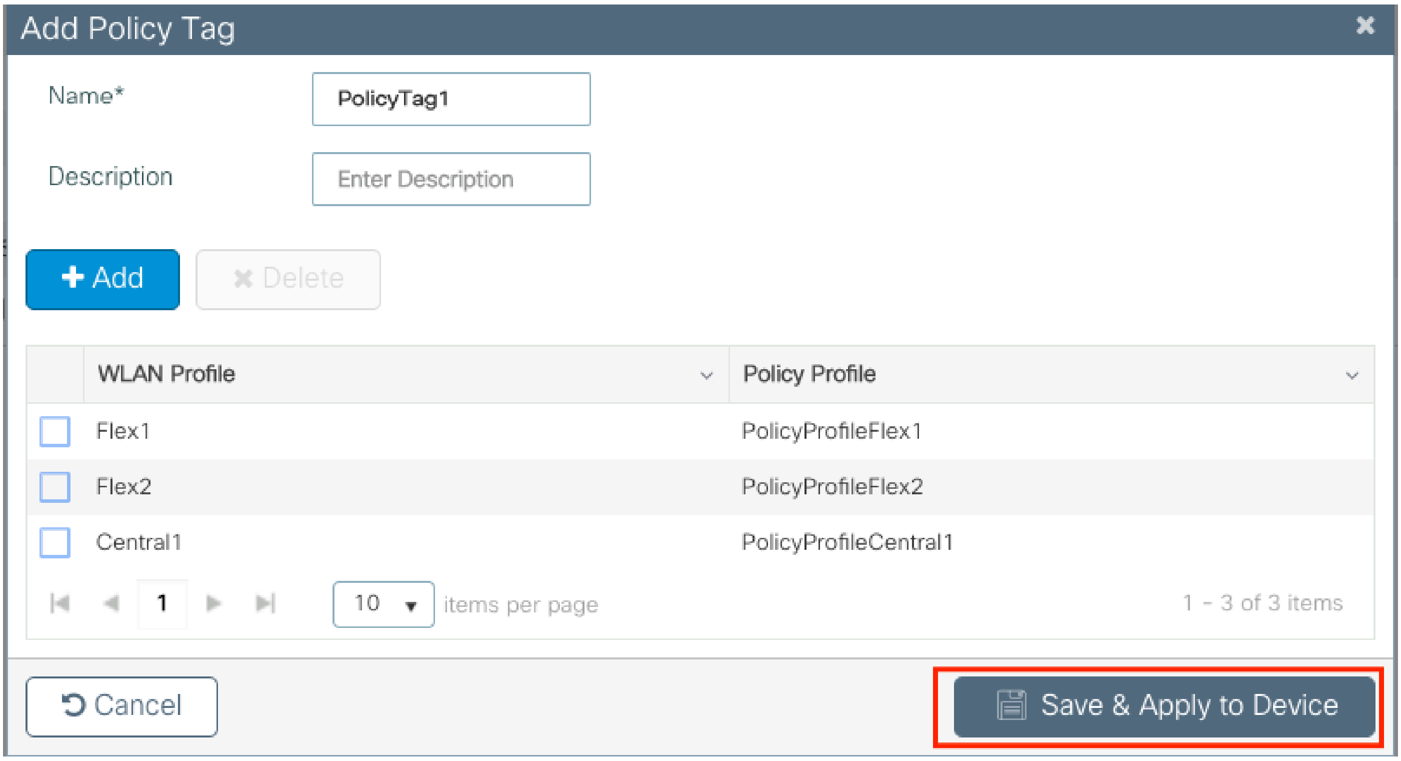
0 | 10 items per page | No items to display

Map WLAN and Policy

WLAN Profile*: Flex1

Policy Profile*: PolicyProfileFlex1

Repeat for the three SSIDs, and after that click Save & Apply to Device.



Add Policy Tag

Name*: PolicyTag1

Description: Enter Description

	WLAN Profile	Policy Profile
□	Flex1	PolicyProfileFlex1
□	Flex2	PolicyProfileFlex2
□	Central1	PolicyProfileCentral1

1 | 10 items per page | 1 – 3 of 3 items

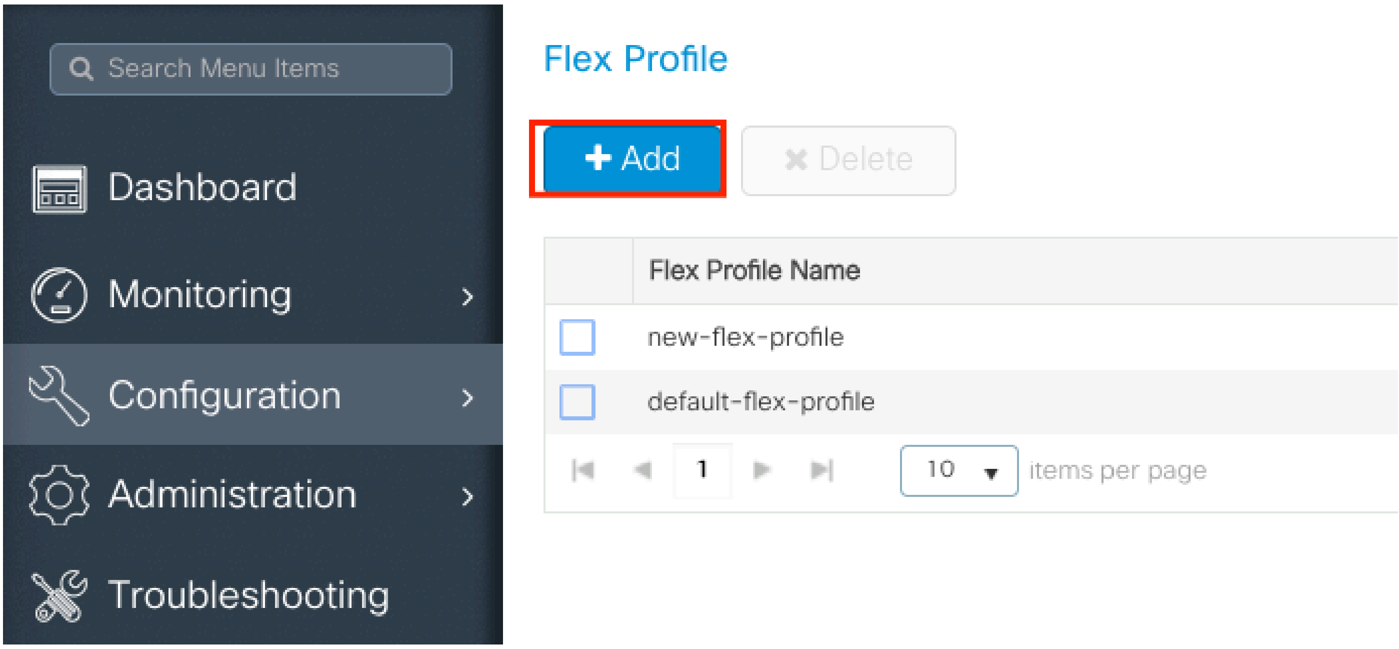
CLI:

```
# config t

# wireless tag policy PolicyTag1
# wlan Flex1 policy PolicyProfileFlex1
# wlan Flex2 policy PolicyProfileFlex2
# wlan Central1 policy PolicyProfileCentral1
# end
```

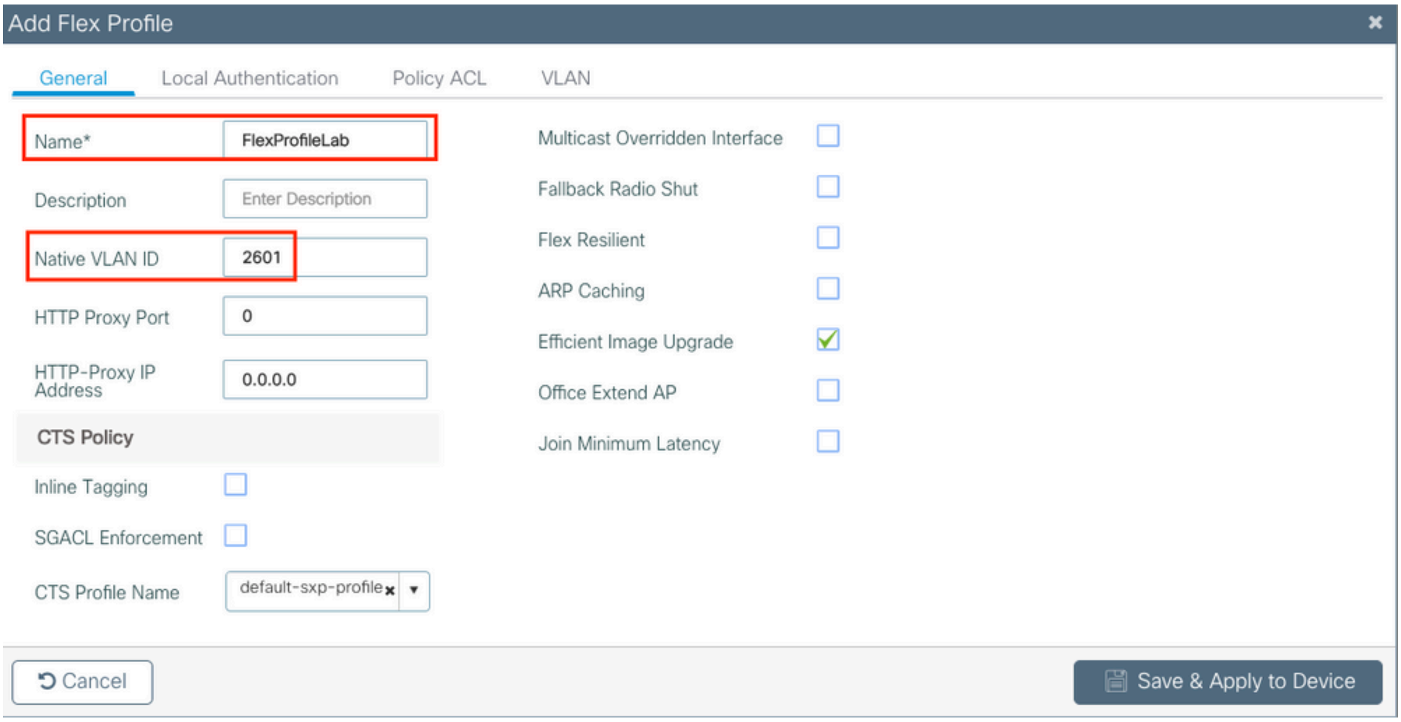
Create/Modify a Flex Profile

In the topology used for this document, notice that there are two SSIDs in Local Switching with two different VLANs. Inside the Flex Profile is where you specify the APs VLAN (Native VLAN) and any other VLAN that the AP needs to be aware of, in this case, the VLANs used by the SSIDs.

Step 1. Navigate to Configuration > Tags & Profiles > Flex and either create a new one or modify one that already exists.



Step 2. Define a name for the Flex Profile and specify the APs VLAN (Native VLAN ID).



Name*	FlexProfileLab
Description	Enter Description
Native VLAN ID	2601
HTTP Proxy Port	0
HTTP-Proxy IP Address	0.0.0.0

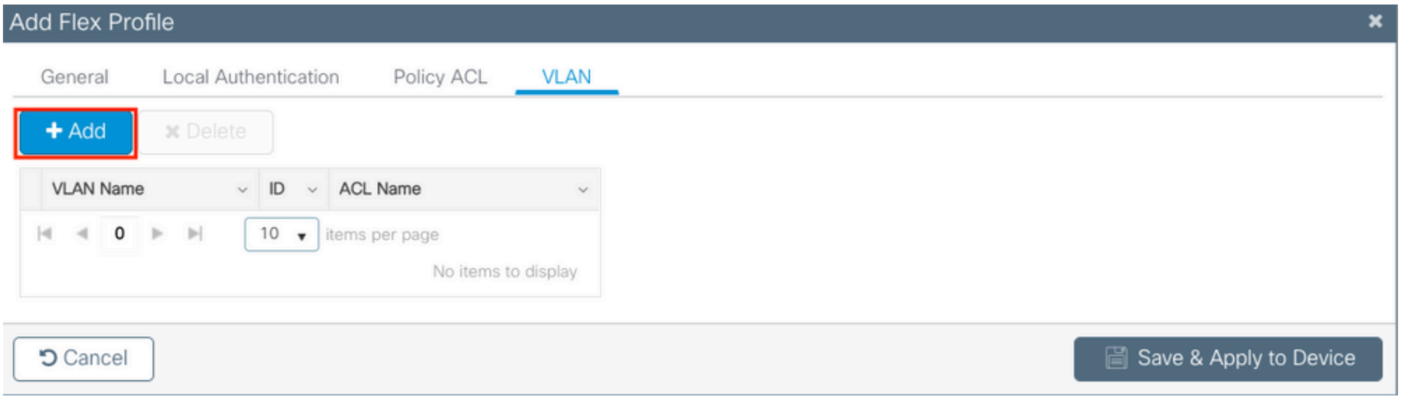
CTS Policy

Inline Tagging	□
SGACL Enforcement	□
CTS Profile Name	default-sxp-profile

Multicast Overridden Interface	□
Fallback Radio Shut	□
Flex Resilient	□
ARP Caching	□
Efficient Image Upgrade	☑
Office Extend AP	□
Join Minimum Latency	□

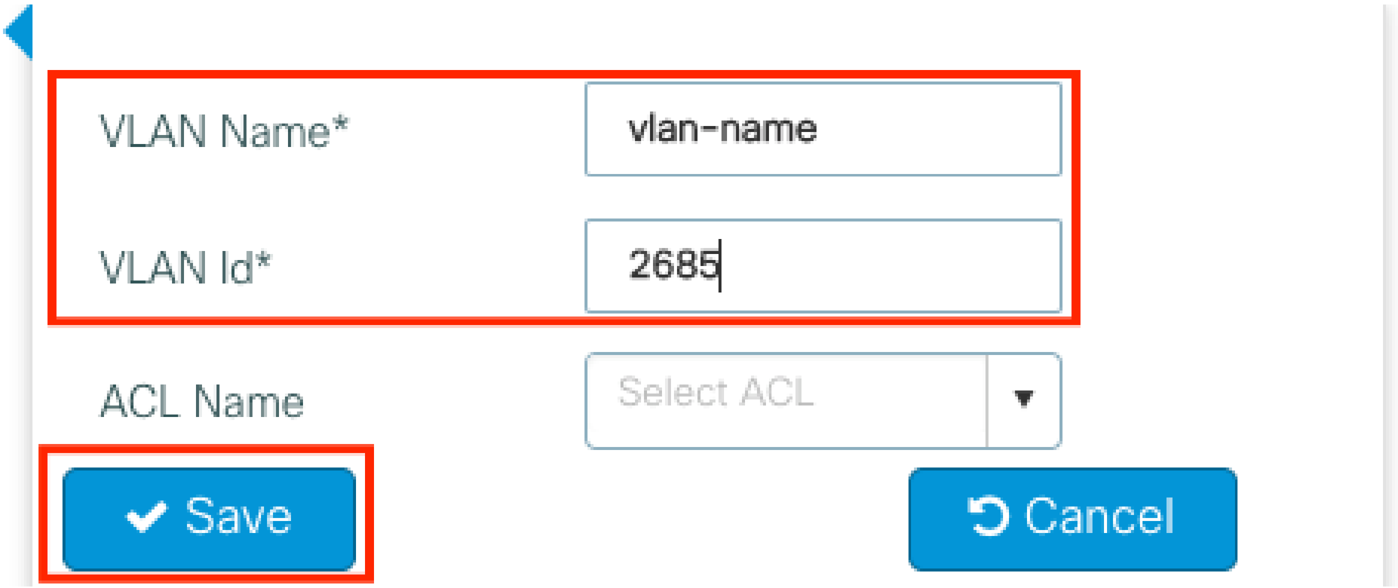
Step 3. Navigate to the VLAN tab and specify the needed VLAN.

In this scenario, there are clients on VLANs 2685 and 2686. These VLANs do not exist on the 9800 WLC, add them to the Flex Profile so they exist on the AP.



VLAN Name	ID	ACL Name

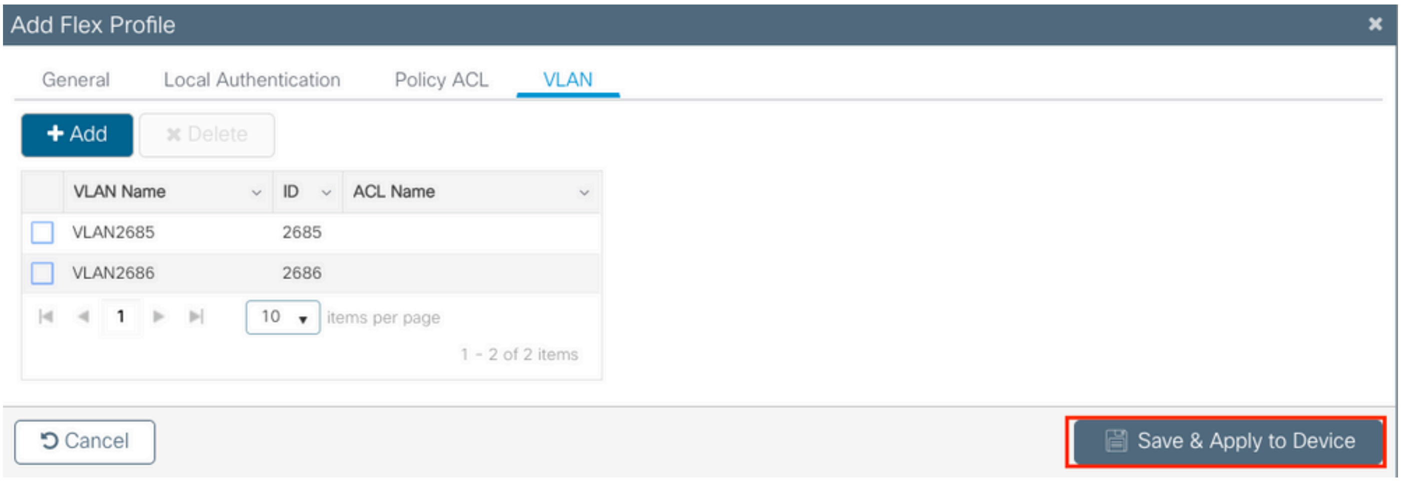
No items to display



VLAN Name*	vlan-name
VLAN Id*	2685
ACL Name	Select ACL

Note: When you created the Policy Profile, If you selected a VLAN name instead of VLAN ID, ensure the VLAN name here in the Flex Profile is the exact same one.

Repeat for the needed VLANs.



	VLAN Name	ID	ACL Name
□	VLAN2685	2685	
□	VLAN2686	2686	

Notice that the VLAN used for Central switching was not added, as the AP does not need to be aware about it.

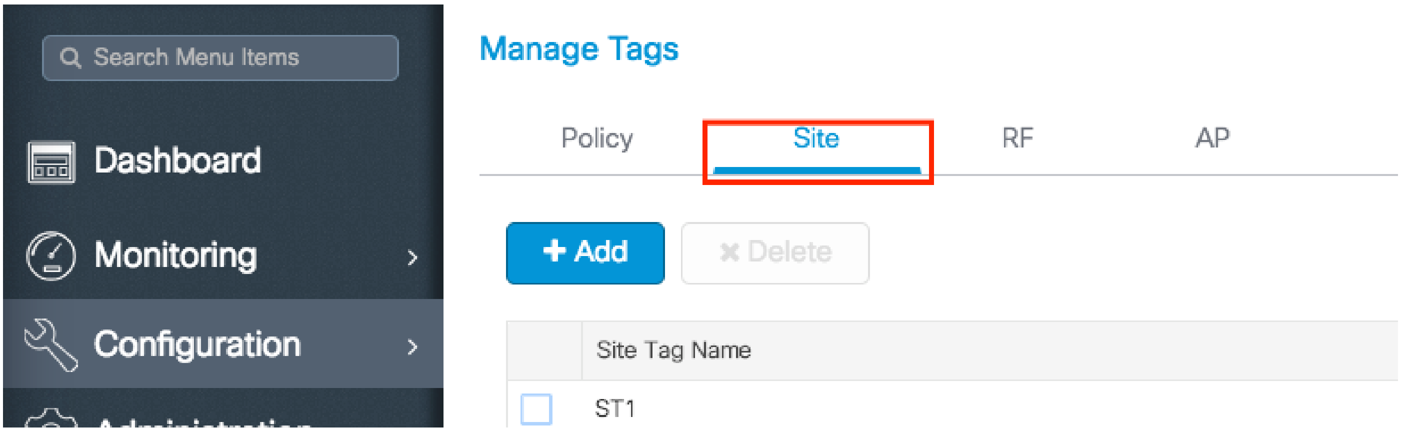
CLI:

```
# config t

# wireless profile flex FlexProfileLab
# native-vlan-id 2601
# vlan-name VLAN2685
# vlan-id 2685
# vlan-name VLAN2686
# vlan-id 2686
# end
```

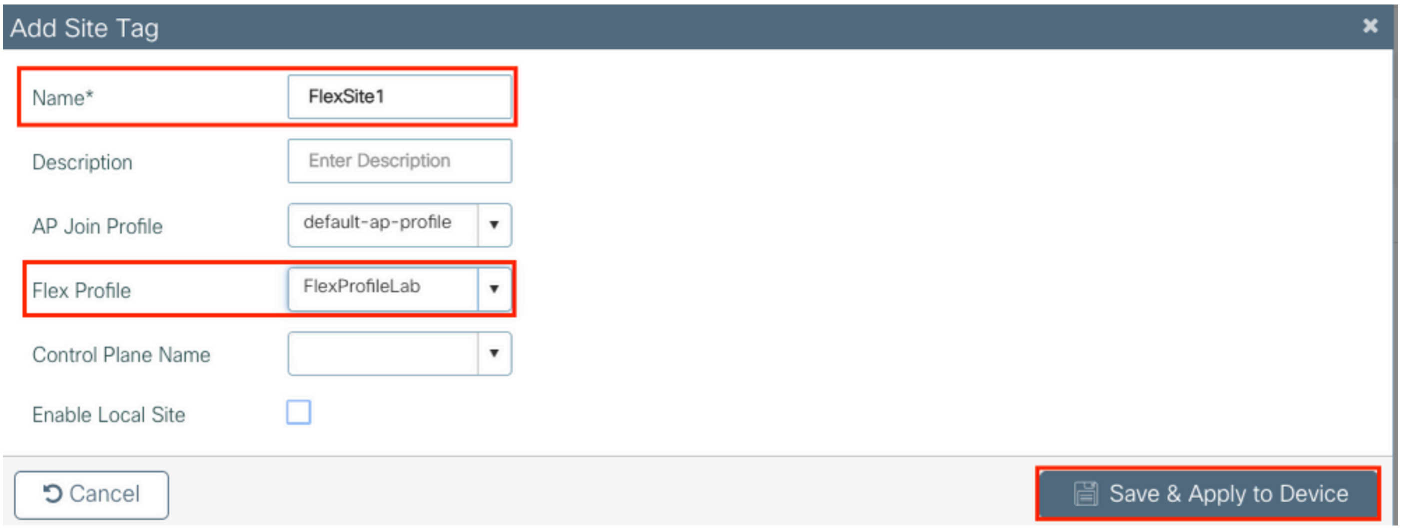
Create/Modify a Site Tag

The Site Tag is the element that allows you to specify which AP join and/or Flex Profile is assigned to the APs.

Step 1. Navigate to **Configuration** > **Tags & Profiles** > **Tags** > **Site.** Either select the name of one that already exists or click **+ Add** to add a new one.



Step 2. Inside the Site Tag, disable the **Enable Local Site** option (Any AP that receives a Site Tag with the Enable Local Site option disabled is converted into FlexConnect mode). Once it is disabled you can also select the Flex Profile. After that click Save & Apply to Device.


Add Site Tag

Name*	FlexSite1
Description	Enter Description
AP Join Profile	default-ap-profile
Flex Profile	FlexProfileLab
Control Plane Name	
Enable Local Site	□

CLI:

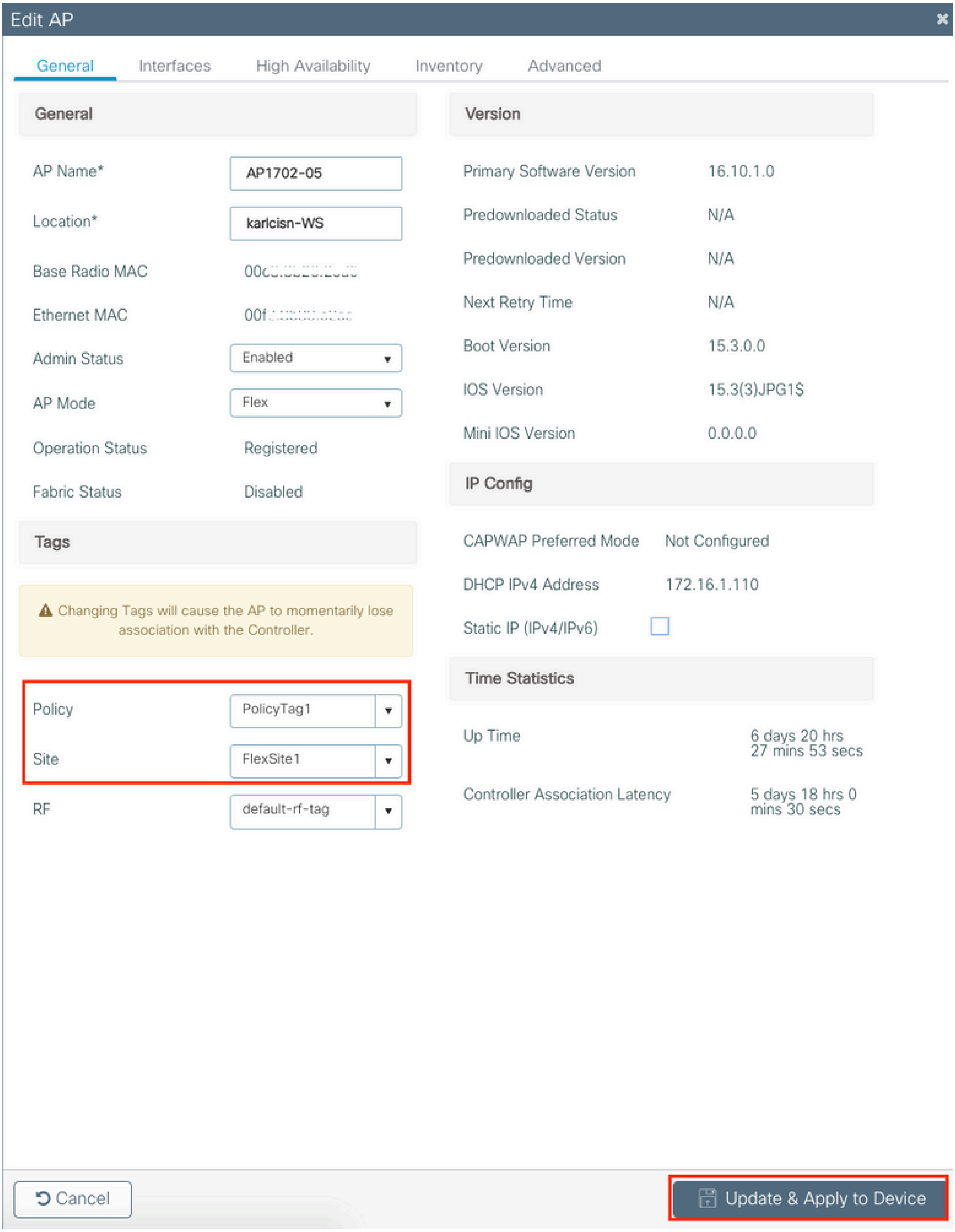
```
# config t
# wireless tag site FlexSite1
# flex-profile FlexProfileLab
# no local-site
```

Policy Tag Assignment to AP

You can assign a Policy Tag directly to an AP or assign the same Policy Tag to a group of APs at the same time. Choose the one that fits you.

Policy Tag Assignment per AP

Navigate to Configuration > Wireless > Access Points > AP name > General > Tags. From the **Site** drop-down list, select the desired Tags and click Update & Apply to Device.



Edit AP

General | Interfaces | High Availability | Inventory | Advanced

General

AP Name*	AP1702-05
Location*	karlcisn-WS
Base Radio MAC	00c[redacted]
Ethernet MAC	00f[redacted]
Admin Status	Enabled
AP Mode	Flex
Operation Status	Registered
Fabric Status	Disabled

Tags

⚠ Changing Tags will cause the AP to momentarily lose association with the Controller.

Policy	PolicyTag1
Site	FlexSite1
RF	default-rf-tag

Version

Primary Software Version	16.10.1.0
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	15.3.0.0
IOS Version	15.3(3)JPG1$
Mini IOS Version	0.0.0.0

IP Config

CAPWAP Preferred Mode	Not Configured
DHCP IPv4 Address	172.16.1.110
Static IP (IPv4/IPv6)	□

Time Statistics

Up Time	6 days 20 hrs 27 mins 53 secs
Controller Association Latency	5 days 18 hrs 0 mins 30 secs

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

Note: If the AP is configured in Local mode (or any other mode) and then it gets a Site Tag with Enable Local Site option disabled, the AP reboots and comes back in FlexConnect mode.

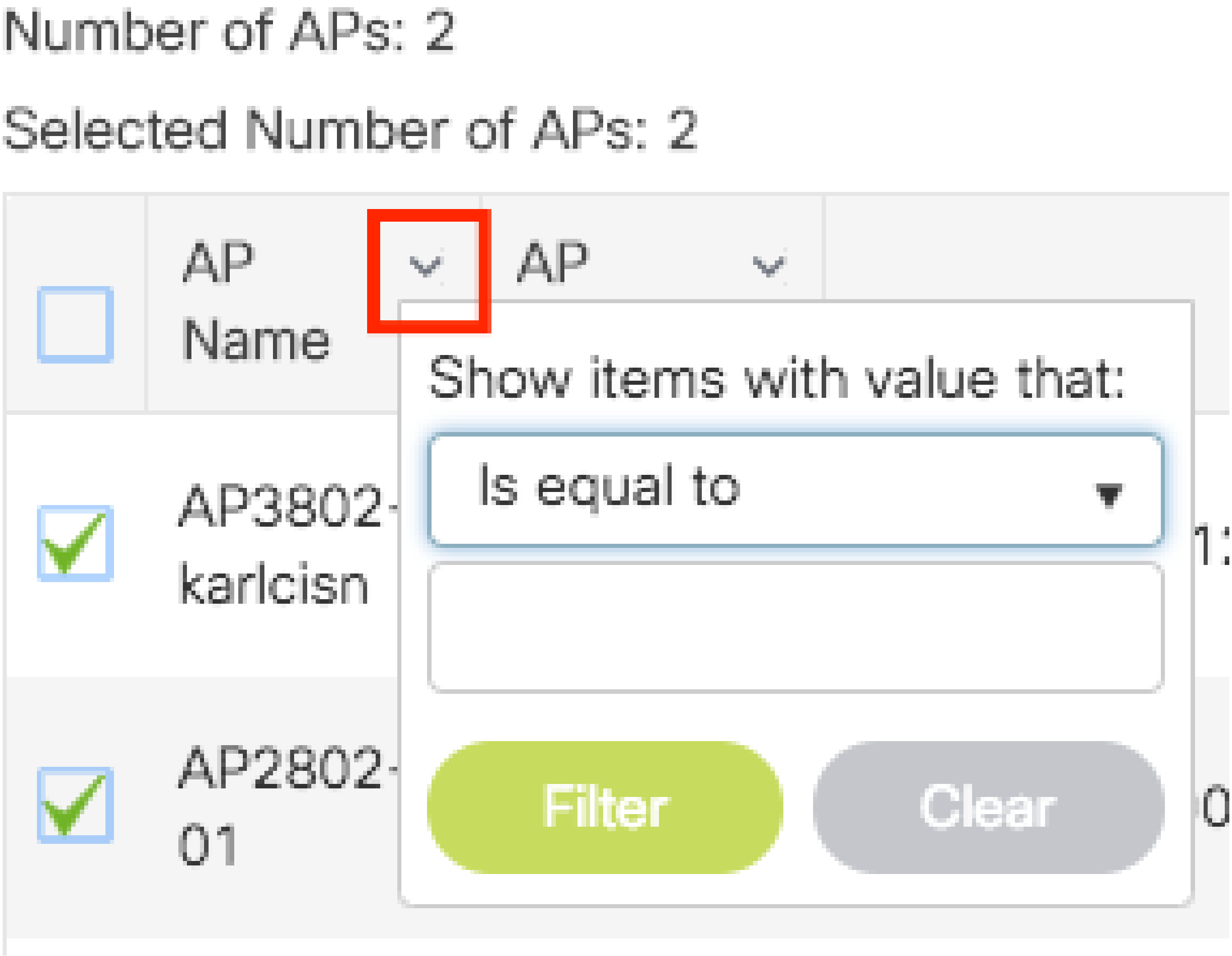
CLI:

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

Policy Tag Assignment for Multiple APs

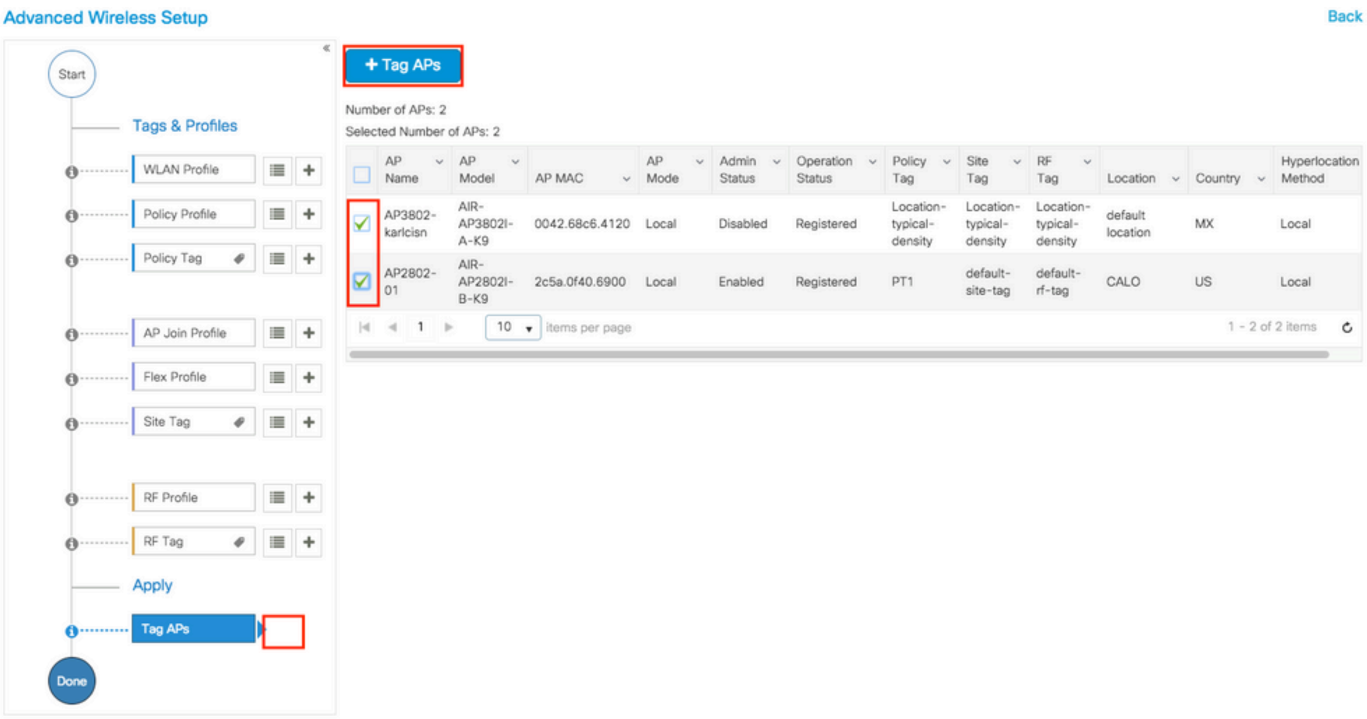
Navigate to **Configuration** > **Wireless Setup** > **Advanced** > **Start Now.**

Click on the Tag APs :≡ icon, after that select the list of APs you want to assign the tags to (You can click on the point down arrow next to AP name [or any other field] to filter the list of APs).


Number of APs: 2

Selected Number of APs: 2

Once you have selected the desired APs, click on **+ Tag APs**.



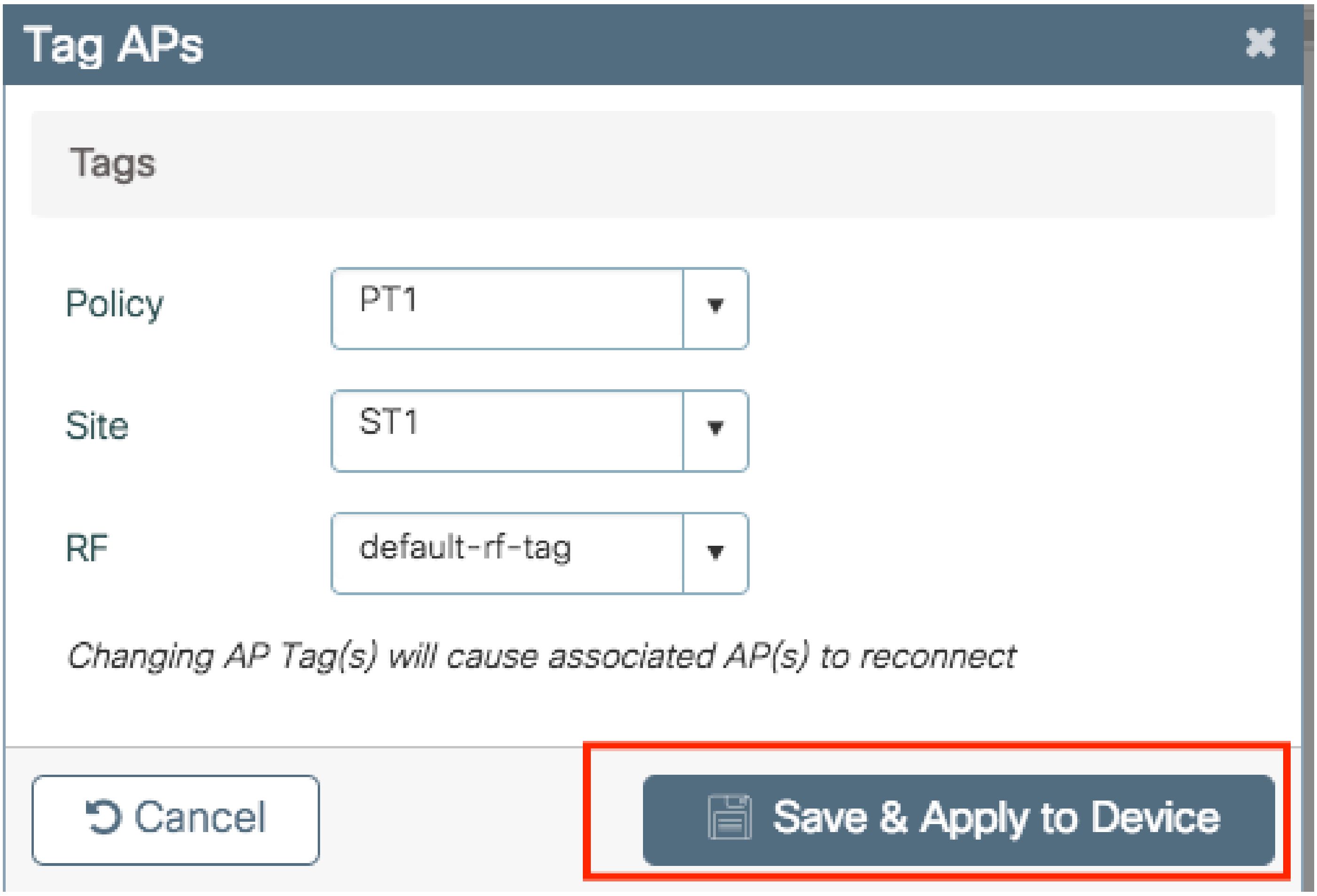
Number of APs: 2

Selected Number of APs: 2

□	AP Name	AP Model	AP MAC	AP Mode	Admin Status	Operation Status	Policy Tag	Site Tag	RF Tag	Location	Country	Hyperlocation Method
☑	AP3802-karlcisn	AIR-AP3802I-A-K9	0042.68c6.4120	Local	Disabled	Registered	Location-typical-density	Location-typical-density	Location-typical-density	default location	MX	Local
☑	AP2802-01	AIR-AP2802I-B-K9	2c5a.0f40.6900	Local	Enabled	Registered	PT1	default-site-tag	default-rf-tag	CALO	US	Local

1 · 10 items per page · 1 - 2 of 2 items

Select the tags you want to assign to the APs and click Save & Apply to Device.



Tag APs

Tags

Policy: PT1

Site: ST1

RF: default-rf-tag

Changing AP Tag(s) will cause associated AP(s) to reconnect

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

Note:If the AP is configured in Local mode (or any other mode) and then it gets a Site Tag with Enable Local Site option disabled, the AP reboots and comes back in FlexConnect mode.

CLI:

There is no CLI option to assign the same Tag to multiple APs.

Flexconnect ACLs

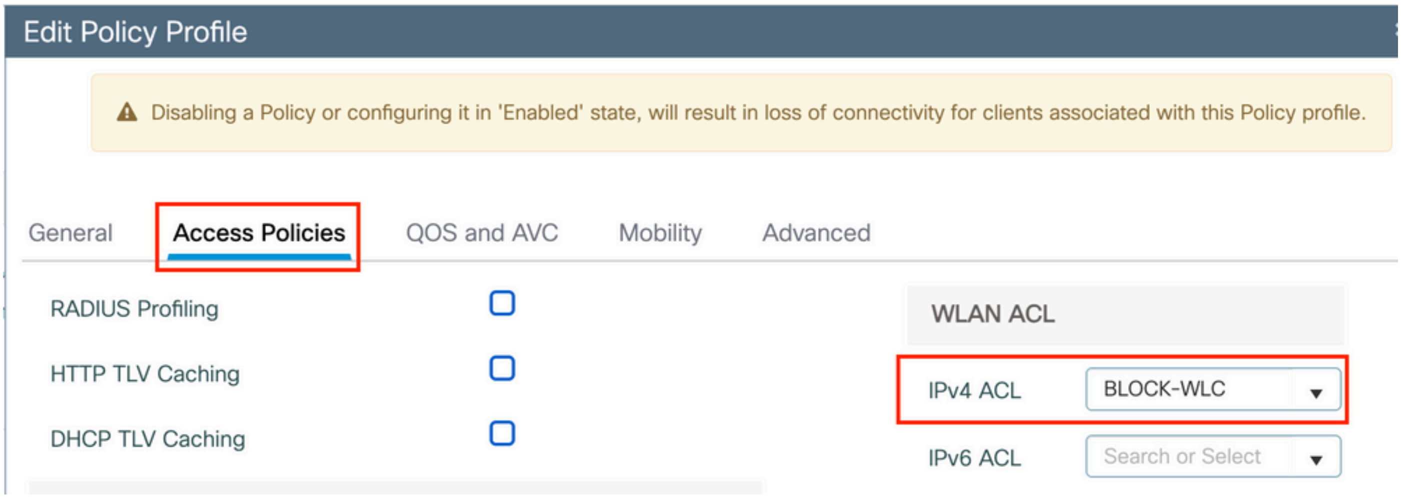
One thing to consider when you have a locally switched WLAN is how to apply an ACL to the clients.

In case of a centrally switched WLAN, all the traffic is released at the WLC, so the ACL does not need to be pushed to the AP. However, when the traffic is locally switched (flex connect - local switching), the ACL (defined on the controller) must be pushed to the AP, since the traffic is released at the AP. This is done when you add the ACL to the flex profile.

Centrally switched WLAN

To apply an ACL to the clients connected to a centrally switched WLAN :

Step 1 - Apply the ACL to the policy profile. Go to **Configuration** > **Tags & Profiles** > **Policy,** select the policy profile associated with the centrally switched WLAN. Under the **"Access Policies"** > **"WLAN ACL"** section, select the ACL that you want to apply to the clients.


Edit Policy Profile

Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

RADIUS Profiling ☐
HTTP TLV Caching ☐
DHCP TLV Caching ☐

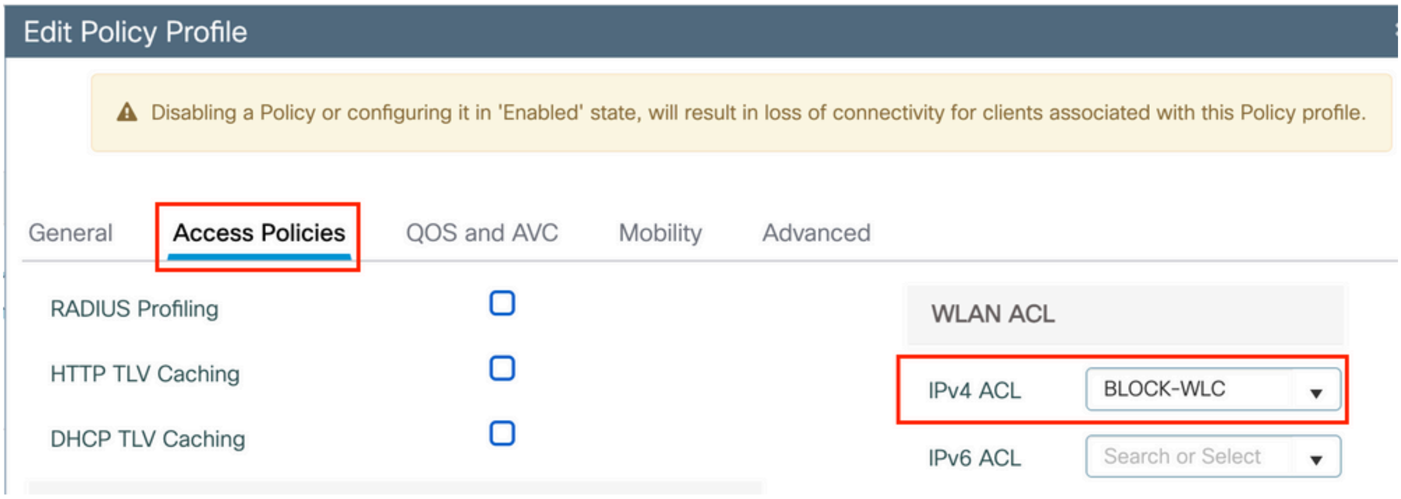
WLAN ACL
IPv4 ACL: BLOCK-WLC
IPv6 ACL: Search or Select

If you are configuring Central Web Authentication on a centrally switched WLAN, you can create a redirect ACL on the 9800, just like as if the AP was in local mode, since everything is centrally handled on the WLC in that case.

Locally switched WLAN

To apply an ACL to the clients connected to a locally switched WLAN :

Step 1 - Apply the ACL to the policy profile. Go to **Configuration** > **Tags & Profiles** > **Policy**, select the policy profile associated with the centrally switched WLAN. Under the **"Access Policies"** > **"WLAN ACL"** section, select the ACL that you want to apply to the clients.



Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

RADIUS Profiling □

HTTP TLV Caching □

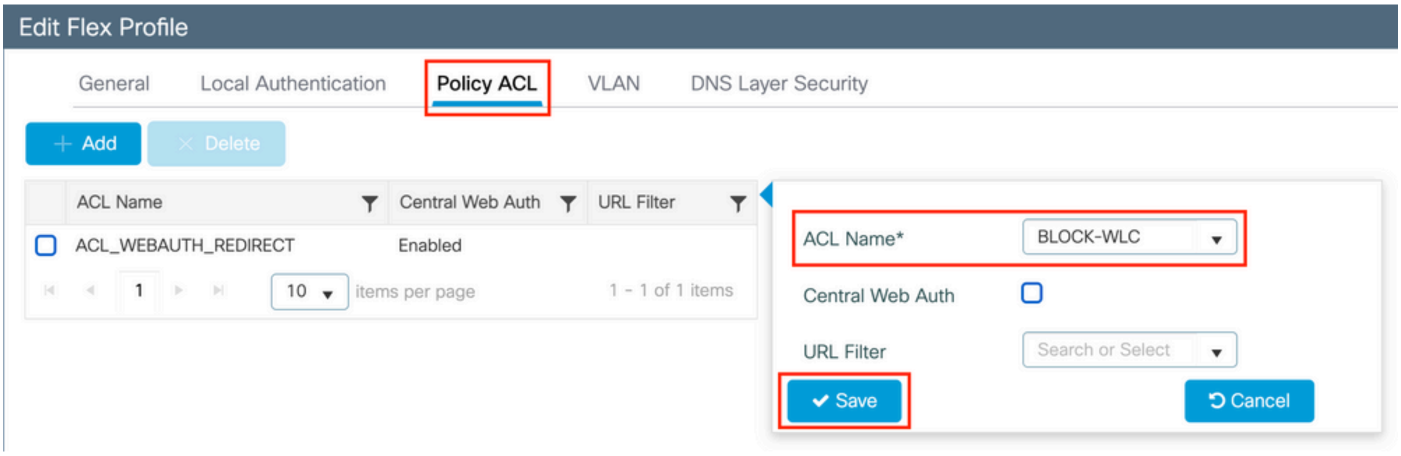
DHCP TLV Caching □

WLAN ACL

IPv4 ACL: BLOCK-WLC ▾

IPv6 ACL: Search or Select ▾

Step 2 - Apply the ACL to the flex profile. Go to **Configuration** > **Tags & Profiles** > **Flex**, select the flex profile assigned to the flex connect APs. Under the **"Policy ACL"** section, add the ACL and click "Save"



Edit Flex Profile

	ACL Name	Central Web Auth	URL Filter
□	ACL_WEBAUTH_REDIRECT	Enabled	

1 — 10 ▾ items per page — 1 - 1 of 1 items

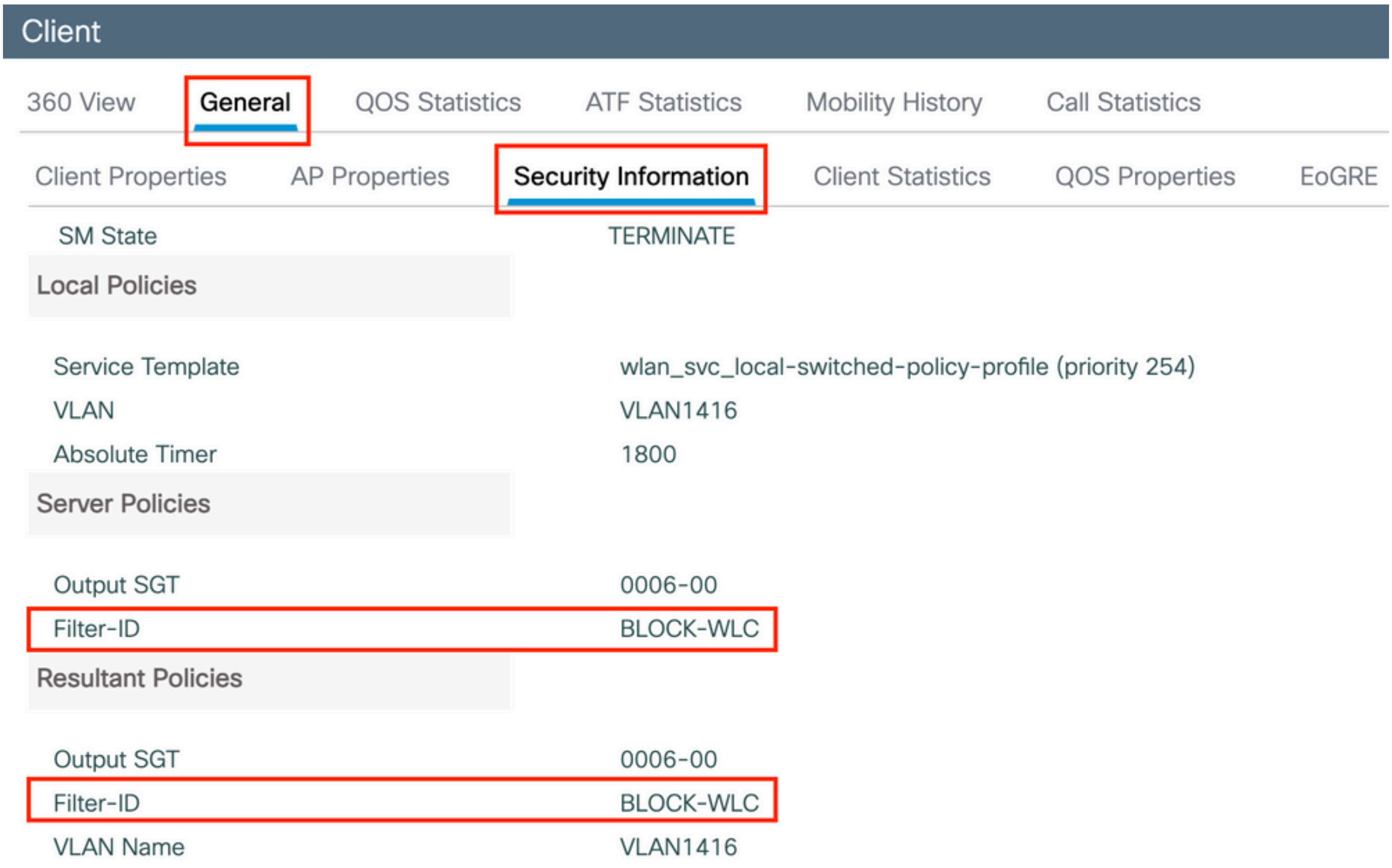
ACL Name*: BLOCK-WLC ▾

Central Web Auth □

URL Filter: Search or Select ▾

Verify if the ACL is applied

You can verify if the ACL is applied to a client when you go to **Monitoring** > **Wireless** > **Clients**, select the client you want to verify. In the section **General** > **Security Information**, check in the **"Server Policies"** section the name of the "Filter-ID" : it must correspond to the ACL applied.



SM State TERMINATE

Local Policies

Service Template wlan_svc_local-switched-policy-profile (priority 254)
VLAN VLAN1416
Absolute Timer 1800

Server Policies

Output SGT 0006-00
Filter-ID BLOCK-WLC

Resultant Policies

Output SGT 0006-00
Filter-ID BLOCK-WLC
VLAN Name VLAN1416

In case of Flex Connect (local switching) APs, you can verify if the ACL is pused to the AP by typing the command "#show ip access-lists" on the AP itself.

Verification

You can use these commands to verify the configuration.

VLANs/Interfaces Configuration

```
# show vlan brief
# show interfaces trunk
# show run interface <interface-id>
```

WLAN Configuration

```
# show wlan summary
# show run wlan [wlan-name]
# show wlan { id <wlan-id> | name <wlan-name> | all }
```

AP Configuration

```
# show ap summary
# show ap tag summary
# show ap name <ap-name> tag { info | detail }
```

```
# show ap name <ap-name> tag detail

AP Name            : AP2802-01
AP Mac             : 0896.ad9d.143e

Tag Type             Tag Name
-----------------------------
Policy Tag           PT1
RF Tag               default-rf-tag
Site Tag             default-site-tag

Policy tag mapping
------------------
WLAN Profile Name                Policy Name                      VLAN                             Cent
-------------------------------------------------------------------------------------------------------
psk-pbl-ewlc                     ctrl-vl2602                      VLAN0210                         ENAB

Site tag mapping
----------------
Flex Profile         : default-flex-profile
AP Profile           : default-ap-profile
Local-site           : Yes

RF tag mapping
--------------
5ghz RF Policy       : Global Config
2.4ghz RF Policy     : Global Config
```

Tag Configuration

```
# show wireless tag { policy | rf | site } summary
# show wireless tag { policy | rf | site } detailed <tag-name>
```

Profile Configuration

```
# show wireless profile { flex | policy } summary
# show wireless profile { flex | policy } detailed <profile-name>
# show ap profile <AP-join-profile-name> detailed
```