The bridge to possible

Cisco Catalyst 9800 FlexConnect Branch Deployment Guide

Contents

Introduction

This document describes how to deploy a Cisco FlexConnect® wireless branch solution on the Cisco Catalyst™ wireless platform. The Catalyst wireless platform is available in two flavors, the virtual form factor and a hardware appliance.

The virtual form factor can be deployed on any x86 server that supports hypervisor such as VMware ESXi, KVM, etc. To get the list of supported hypervisors and the versions, please refer to the deployment guide of the Catalyst wireless family. The virtual form factor can be deployed on-prem with an enterprise or can be installed on cloud providers such as AWS.

The Catalyst 9800 Wireless Controller is the hardware appliance for the Catalyst wireless family. The Catalyst 9800WC and virtual cloud controller run on the Cisco IOS® XE software base, utilizing the flexibility and modularity available with the platform.

Refer to the following documentation for how to get started on the Catalyst 9800 and cloud-based virtual wireless LAN controller.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_c9800_wireless_controller_virtual_dg.html

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_c9800_wireless_controller_series_web_dg.html

The documents covers the features that are supported on the following platforms and releases.

Supported platforms

Catalyst wireless platforms

11ac Wave 1 and Wave 2 Access Points - 18xx, 2802, 3802, 4800, 1540, 1560, 1700, 2700, 3700, 1570

11ax Access Points - 9105, 9115, 9117, 9120, 9130

Supported releases

IOS-XE 16.10 and higher.

FlexConnect architecture

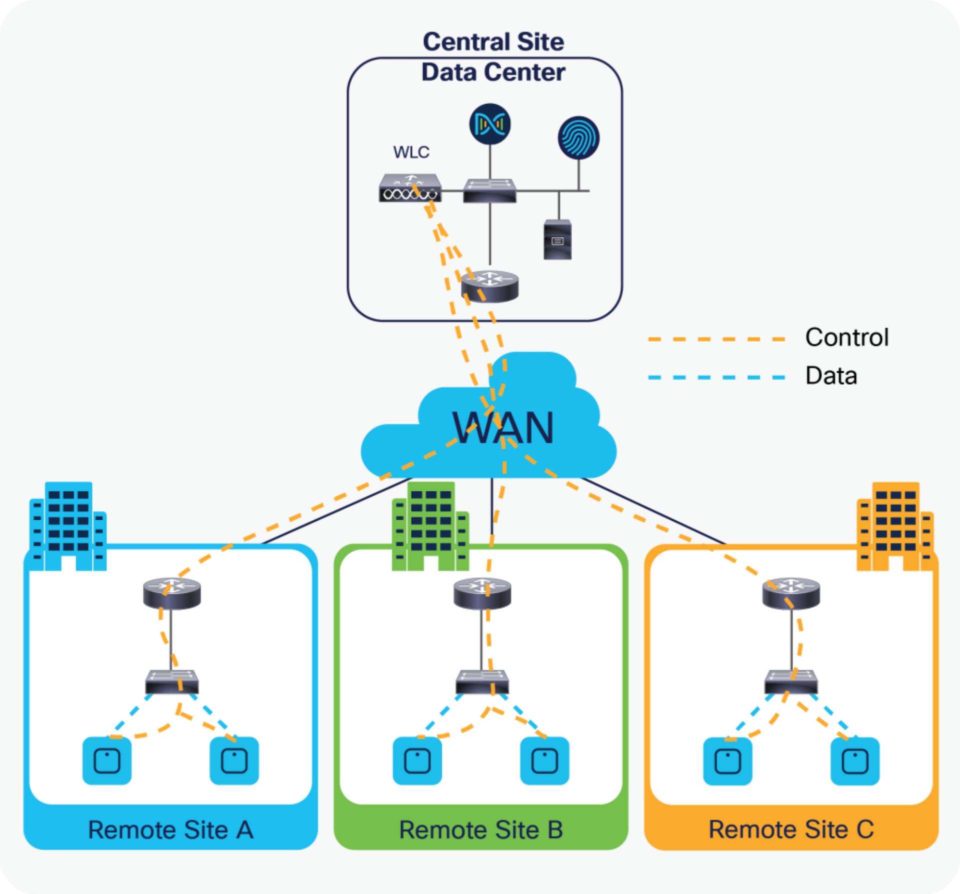


Figure 1.
FlexConnect Architecture and Traffic Flow

FlexConnect is a wireless solution for branch office and remote office deployments.

The FlexConnect solution enables the customer to:

- Centralize control and manage traffic of APs from the data center.
- Distribute the client data traffic at each branch office.

Advantages of centralizing access point control traffic

- Single pane of monitoring and troubleshooting
- Ease of management
- Secured and seamless mobile access to data center resources
- Reduction in branch footprint
- Increase in operational savings

Advantages of distributing client data traffic

- No operational downtime (survivability) against complete WAN link failures or controller unavailability
- Mobility resiliency within branch during WAN link failures
- Increase in branch scalability; supports branch sizes that can scale up to 100 APs and 250,000 square feet (5000 square feet per AP)

The Cisco FlexConnect solution also supports central client data traffic. The table below defines the supported Layer 2 and Layer 3 security types only for central-switched and local-switched users.

Table 1. L2 security support for centrally and locally switched users

WLAN L2 security	Type	Result
None	N/A	Allowed
WPA + WPA2	802.1x	Allowed
	CCKM	Allowed
	802.1x + CCKM	Allowed
	PSK	Allowed
802.1x	WEP	Allowed
Static WEP	WEP	Allowed
WEP + 802.1x	WEP	Allowed

Table 2. L3 security support for centrally and locally switched users

WLAN L3 security	Type	Result
Web authentication	Internal	Allowed
	External	Allowed
	Customized	Allowed
Web pass-through	Internal	Allowed
	External	Allowed
	Customized	Allowed
Conditional web redirect	WEP	Allowed
Splash page web redirect	WEP	Allowed

FlexConnect modes of operation

Table 3. Flexconnect modes of operation

FlexConnect mode	Description
Connected	FlexConnect is said to be in connected mode when its CAPWAP control plane back to the controller is up and operational, meaning the WAN link is not down.
Standalone	Standalone mode is specified as the operational state the FlexConnect enters when it no longer has the connectivity back to the controller. FlexConnect APs in standalone mode will continue to function with last known configuration, even in the event of power failure and WLC or WAN failure.

WAN requirements

FlexConnect APs are deployed at the branch site and managed from the data center over a WAN link. The maximum transmission unit (MTU) must be at least 500 bytes.

Table 4. FlexConnect WAN Bandwidth and latency requirements

Deployment type	WA bandwidth (min)	WAN RTT latency (max)	Max APs per branch	Max clients per branch
Data	64 Kbps	300 ms	5	25
Data	640 Kbps	300 ms	50	1000
Data	1.44 Mbps	1 sec	50	1000
Data + voice	128 Kbps	100 ms	5	25
Data + voice	1.44 Mbps	100 ms	50	1000
Monitor	64 Kbps	2 sec	5	N/A
Monitor	640 Kbps	2 sec	50	N/A

Note: It is highly recommended that the minimum bandwidth restriction remains 12.8 Kbps per AP, with the round-trip latency no greater than 300 ms for data deployments and 100 ms for data + voice deployments.

Feature Matrix

Refer to the FlexConnect matrix document in the link below to validate the list of supported features.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_flexConnect_feature_matrix.html

Wireless branch network design

The rest of this document highlights the guidelines and describes the best practices for implementing secured distributed branch networks. FlexConnect architecture is recommended for wireless branch networks that meet the following design requirements.

Primary design requirements

- Branch size that can scale up to 100 APs and 250,000 square feet (5000 square feet per AP)
- Central management and troubleshooting
- No operational downtime
- Client-based traffic segmentation
- Seamless and secured wireless connectivity to corporate resources
- PCI compliant
- Support for guests

Overview

Branch customers find it increasingly difficult and expensive to deliver full-featured scalable and secure network services across geographic locations. In order to support customers, Cisco is addressing these challenges by introducing the FlexConnect deployment mode.

The FlexConnect solution virtualizes the complex security, management, configuration, and troubleshooting operations within the data center and then transparently extends those services to each branch. Deployments using FlexConnect are easier for IT to set up, manage, and, most importantly, scale.

Advantages

- Increase scalability with 6000 AP support.
- Increased resiliency using FlexConnect fault tolerance
- Increase segmentation of traffic using FlexConnect (central and local switching)
- Ease of management by replicating store designs using different policy profiles and site tags per store while maintaining the same WLAN profile as seen in figure below

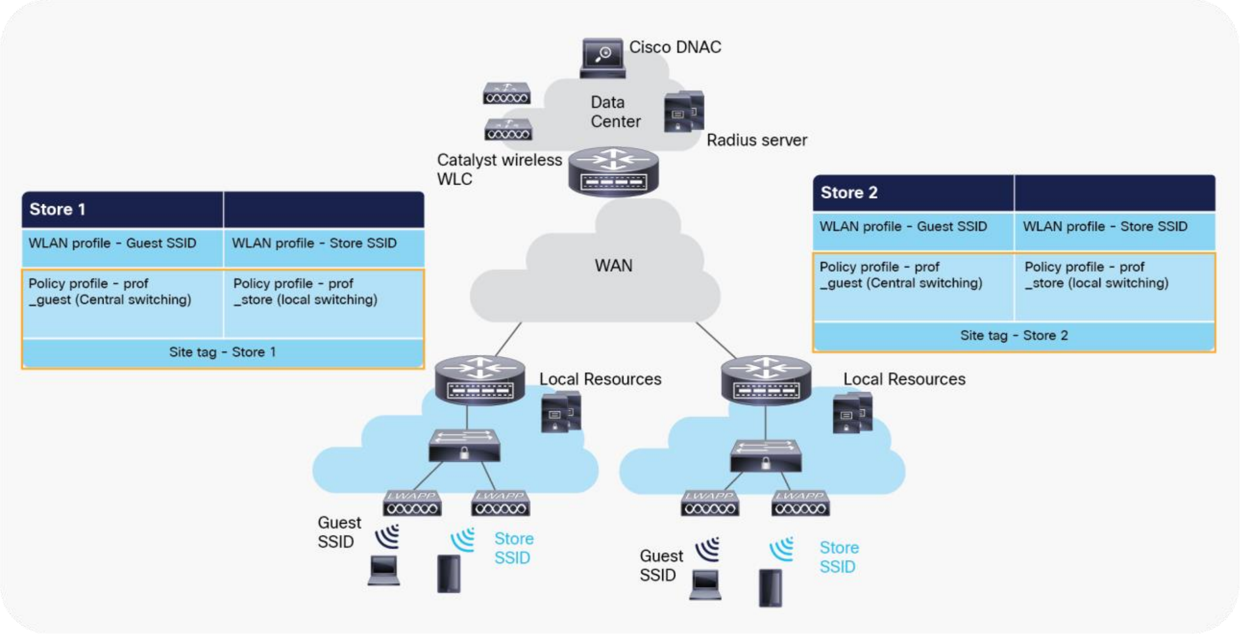

Cisco DNAC
Data Center
Radius server
Catalyst wireless WLC
Store 1
WLAN profile - Guest SSID
WLAN profile - Store SSID
Policy profile - prof _guest (Central switching)
Policy profile - prof _store (local switching)
Site tag - Store 1
Store 2
WLAN profile - Guest SSID
WLAN profile - Store SSID
Policy profile - prof _guest (Central switching)
Policy profile - prof _store (local switching)
Site tag - Store 2
WAN
Local Resources
Local Resources
Guest SSID
Store SSID
Guest SSID
Store SSID

Figure 2.
Design replication across stores by mapping different site tags and policy tags

Features addressing branch network design

The rest of the sections in this guide capture feature usage and recommendations to realize the typical branch network design.

Table 5. Features addressing branch network design

Features	Highlights
New config model on Catalyst wireless family	Ability to decouple and modularize the configuration entities. This enables you to have the same configuration across different stores by having the same profiles across stores and using a different tag for each store.
Fault tolerance	Improves the wireless branch resiliency and provides no operational downtime.
Client limit per WLAN	Limiting total guest clients on branch network.
Auto-convert APs in FlexConnect	Assigning a site tag that has a flex profile will auto-convert the AP to FlexConnect mode without user intervention.
Efficient AP image upgrade	Reduces downtime when upgrading your branch. Efficient AP upgrade saves WAN bandwidth and enables a branch AP to upgrade at a much faster pace.
Guest access	Continue existing Cisco's guest access architecture with FlexConnect by having a central switched SSID that is a tunnel to a controller in the DMZ zone.
URL ACL	Ability to support use cases of bring your own device (BYOD) at the branch
Backup radius server	Provides resiliency at the branch due to WAN outage
AAA override	Provides segmentation and polices per user

Cisco Catalyst wireless config model

This section describes the new config model introduced in the Catalyst wireless platforms.

The new config model goes towards the modularized and reusable model with logical decoupling of configuration entities.

The model introduces the uses of tags and profiles. The below table gives an overview of the tags and profile used within the new Catalyst wireless products.

Table 6. Tags on Profile on the Catalyst 9800 controller

Tags and profile	Highlights
WLAN profile	Creation of WLAN with the corresponding security. Addition of AAA entities and configuring the advanced capabilities of the WLAN.
Policy profile	Defines the policy of the WLAN such as central /local switching, ACL, VLAN mapping for the WLAN, QOS, AAA policy, and export anchor.
Policy tag	Defines the mapping of the WLAN to the policy profile.
Flex profile	Flex profile defines the WLAN to VLAN mapping for flex deployment, ACL mapping, and radius server configuration.

Tags and profile	Highlights
AP join profile	Defines the CAPWAP and AP parameters related to join procedures.
RF profile/RF tag	RF characteristics of the site mapped to an RF tag.
Site tag	Site tags maps the flex profile and the AP join profile.
AP tag	Maps the policy tag, site. and RF tag on to the AP.

The model follows the design and provision theme.

The design phase involves creating the elements necessary for the wireless networks such as wireless SSID, policy management, RF tagging flex profile, etc. The deployment phase is where the designed elements are provisioned on the AP.

Profiles and tags

Profiles represent a set of attributes that are applied to the clients associated to the APs. Profiles are reusable entities that can be used across tags. Profiles (used by tags) define the properties of the AP or associated clients.

There are different kinds of profiles depending on the characteristic of the entities they define. These profiles are in turn part of a larger construct called a tag.

A tag's property is defined by the property of the profiles associated to it. This property is in turn inherited by an associated client/AP. There are various types of tags, each associated to different profiles.

No two types of tags include profiles having common properties. This helps eliminate the precedence amongst the configuration entities to a large extent. Every tag has a default that is created when the system boots up.

WLAN profile

The WLAN profile defines the properties of a WLAN such as profile name, status, WLAN ID, L2 and L3 security parameters, AAA server associated with this SSID, and other parameters that are specific to a particular WLAN.

Policy profile

The policy profile is an entity that comprises of network and switching polices for a client, with the exception of QoS, which constitute the AP policies as well.

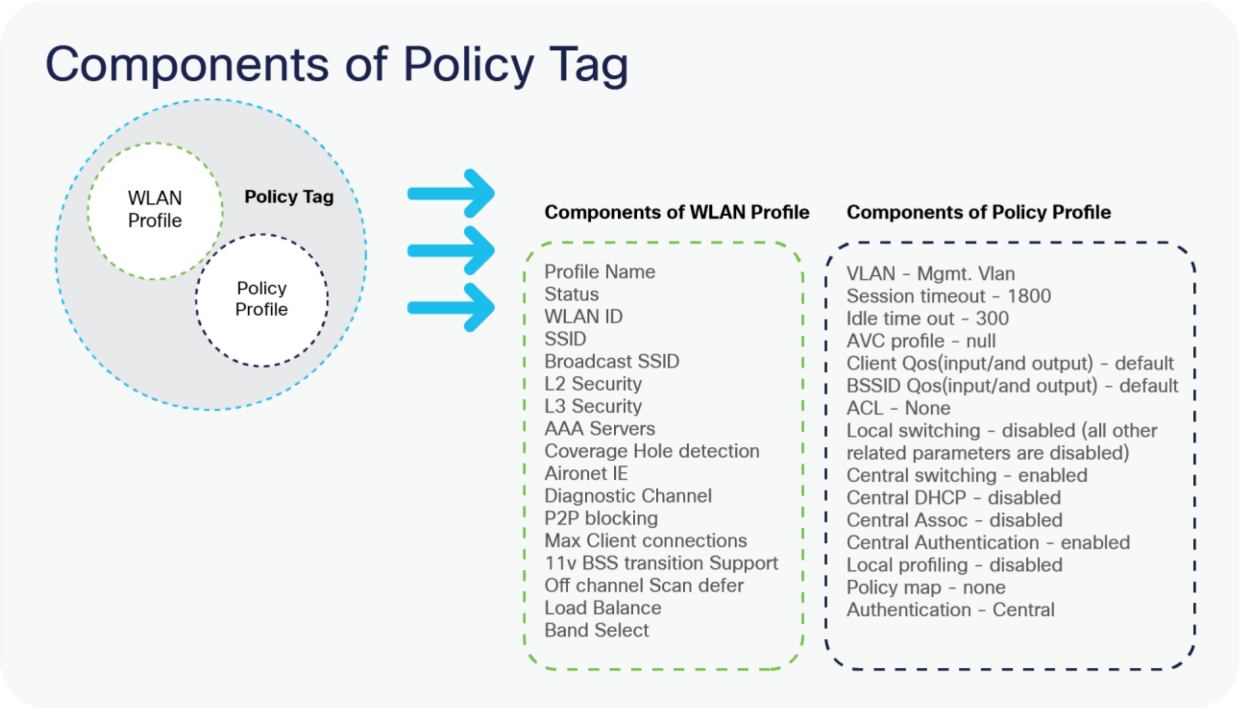
The policy profile is a reusable entity across tags. Anything that is a policy for the client applied on the AP/controller is moved to the policy profile – or example, VLAN, ACL, QOS, session timeout, idle timeout, AVC profile, bonjour profile, local profiling, device classification, etc.

The WLAN profile and policy profile are both part of a policy tag and define the characteristics and policy definitions of a set of WLANs. The intent of decoupling the policies from the SSID, even though it is a one-to-one mapping, is to give more flexibility to the admin in configuring site-based policies (local or remote) while keeping the WLAN definition common.

Policy tag

Policy tag constitutes the mapping of WLAN profiles to policy profiles. The policy profile defines the network policies and the switching policies for a client (with the exception of QoS, which constitutes the AP policy as well as the client policy).

A default policy tag with WLAN profiles with a WLAN ID <16 is mapped to a default policy profile.



Components of WLAN Profile

Profile Name
Status
WLAN ID
SSID
Broadcast SSID
L2 Security
L3 Security
AAA Servers
Coverage Hole detection
Aironet IE
Diagnostic Channel
P2P blocking
Max Client connections
11v BSS transition Support
Off channel Scan defer
Load Balance
Band Select

Components of Policy Profile

VLAN - Mgmt. Vlan
Session timeout - 1800
Idle time out - 300
AVC profile - null
Client Qos(input/and output) - default
BSSID Qos(input/and output) - default
ACL - None
Local switching - disabled (all other related parameters are disabled)
Central switching - enabled
Central DHCP - disabled
Central Assoc - disabled
Central Authentication - enabled
Local profiling - disabled
Policy map - none
Authentication - Central

Figure 3.
Components of Policy Tag

AP join profile

Following parameters will be part of the AP join profile - CAPWAP IPV4/IPV6, UDP lite, high availability, retransmit config parameters, global AP failover, hyper-location config parameters, Telnet/SSH, 11u parameters, etc. For AP join profile changes, a small subset requires the CAPWAP connection to be reset since these parameters pertain to the characteristic of the AP.

Flex profile

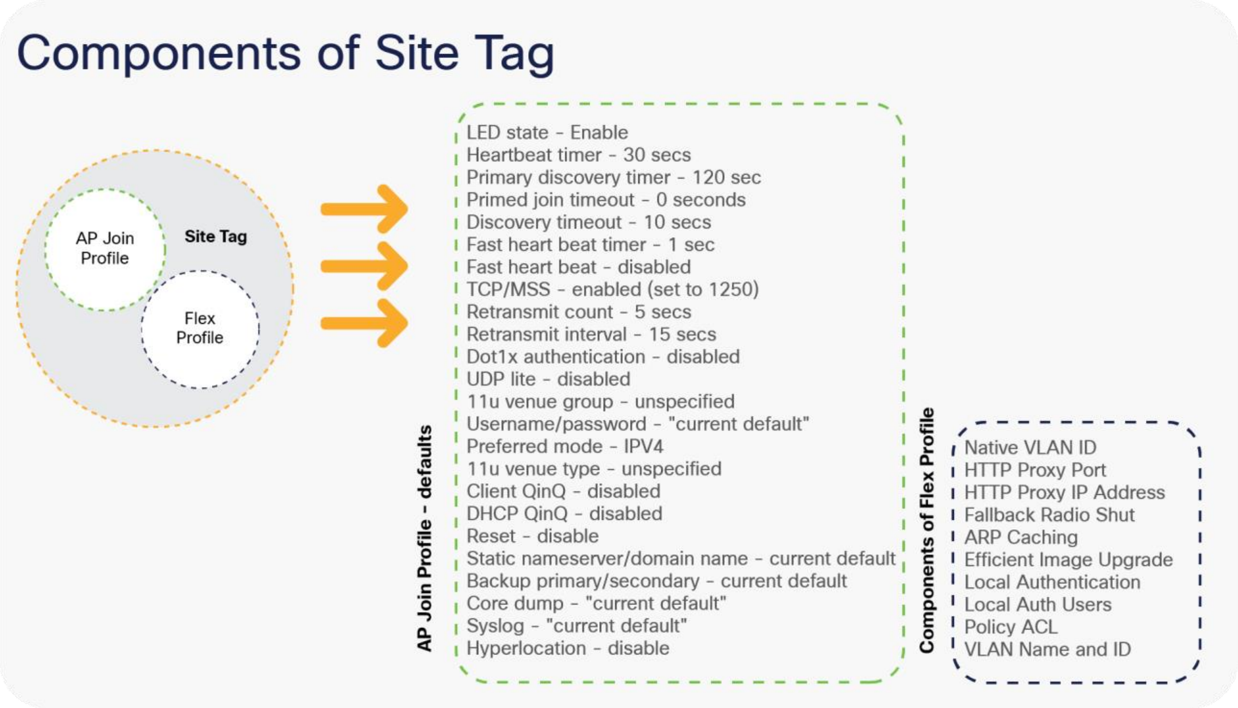
The flex profile contains the remote site-specific parameters – for example, the primary and secondary AP list, the EAP profiles that can be used for the case where AP acts as an authentication server, local radius server information, VLAN-ACL mapping, etc. There is no default flex profile; however, a custom flex-profile can be added to the default site tag.

The AP join profile and flex profile are both part of a site tag and define the characteristics of a local or remote site.

Site tag

The site tag constitutes two profiles, the flex profile and the AP join profile. The site tag defines the properties of a site, both central as well as remote (FlexConnect) site. The attributes of a site that are common across the central and remote site are part of the AP join profile. The attributes that are specific to the flex/remote site are part of the flex profile.

The default site tag constitutes the default AP join profile. There is no default flex profile. The default AP join profile values will be the same as that for the global AP parameters today plus a few parameters from the AP group in today’s configuration like “preferred mode,” 802.11u parameters, location, etc.



LED state - Enable
Heartbeat timer - 30 secs
Primary discovery timer - 120 sec
Primed join timeout - 0 seconds
Discovery timeout - 10 secs
Fast heart beat timer - 1 sec
Fast heart beat - disabled
TCP/MSS - enabled (set to 1250)
Retransmit count - 5 secs
Retransmit interval - 15 secs
Dot1x authentication - disabled
UDP lite - disabled
11u venue group - unspecified
Username/password - "current default"
Preferred mode - IPV4
11u venue type - unspecified
Client QinQ - disabled
DHCP QinQ - disabled
Reset - disable
Static nameserver/domain name - current default
Backup primary/secondary - current default
Core dump - "current default"
Syslog - "current default"
Hyperlocation - disable

Native VLAN ID
HTTP Proxy Port
HTTP Proxy IP Address
Fallback Radio Shut
ARP Caching
Efficient Image Upgrade
Local Authentication
Local Auth Users
Policy ACL
VLAN Name and ID

Figure 4.
Components of Site Tag

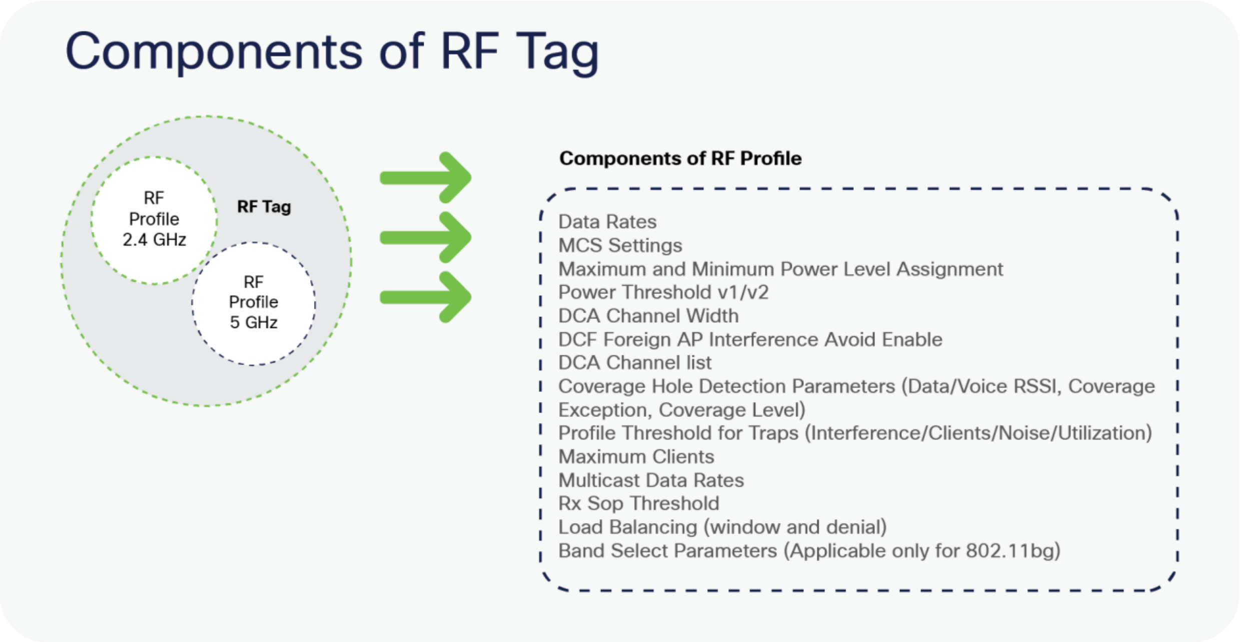
RF profile

By default, there exists two default RF profiles (one for 802.11a and one for 802.11b). RF profiles constitute the RF-specific configurations such as data rates, MCS settings, power assignment, DCA parameters, CHDM variables, and HDX features. One 802.11a RF profile and one 802.11b RF profile can be added to an RF tag.

RF tag

The RF tag constitutes the 11a and 11b RF profiles. The default RF Tag constitutes the default 802.11a RF profile and the default 802.11b RF profile.

The default 11a RF profile and 11b RF profile contain default values for global RF profiles for the respective radios.



Components of RF Tag

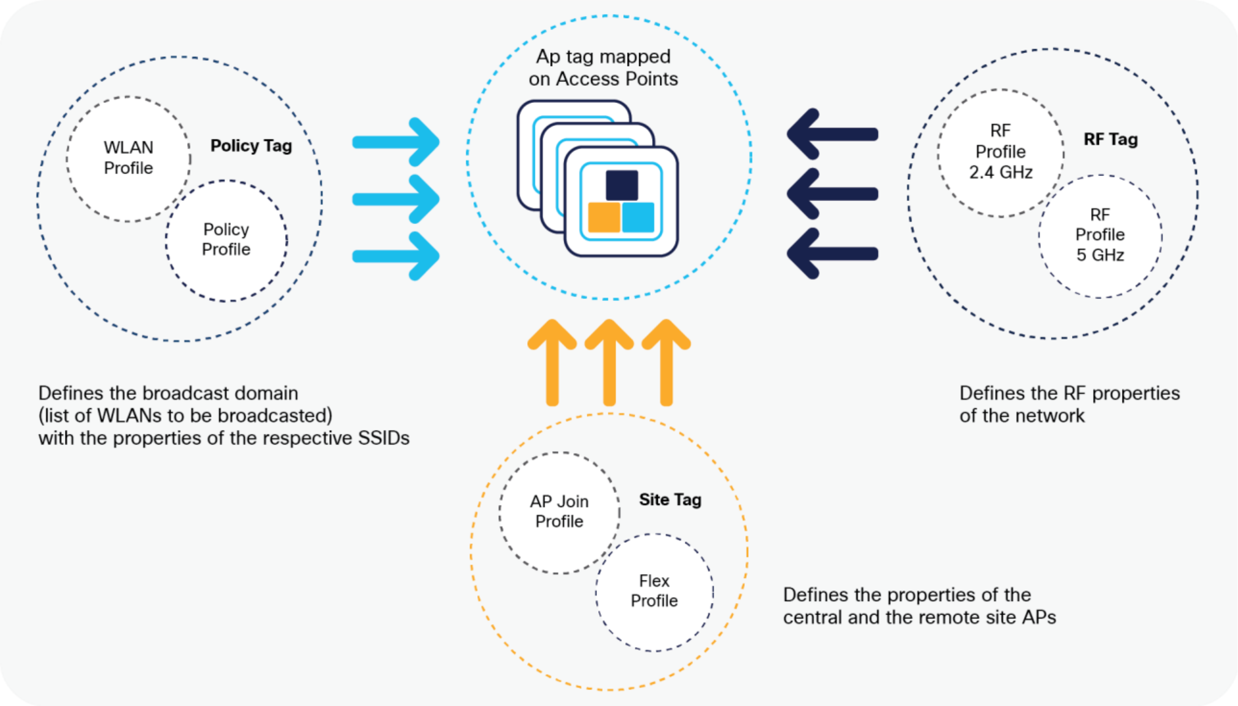
Components of RF Profile

- Data Rates
- MCS Settings
- Maximum and Minimum Power Level Assignment
- Power Threshold v1/v2
- DCA Channel Width
- DCF Foreign AP Interference Avoid Enable
- DCA Channel list
- Coverage Hole Detection Parameters (Data/Voice RSSI, Coverage Exception, Coverage Level)
- Profile Threshold for Traps (Interference/Clients/Noise/Utilization)
- Maximum Clients
- Multicast Data Rates
- Rx Sop Threshold
- Load Balancing (window and denial)
- Band Select Parameters (Applicable only for 802.11bg)

Figure 5.
Components of RF Tag

AP tag

Access points are tagged based on the SSIDs and the associated policies it broadcasts by associating a policy with the AP, the site it belongs to, and the RF characteristics desired for that access point by mapping the respective tags. Once tagged, the AP gets a list of WLANs to be broadcasted along with the properties of the respective SSIDs, properties of the local/remote site, and the RF properties of the network.



Defines the broadcast domain (list of WLANs to be broadcasted) with the properties of the respective SSIDs

Defines the RF properties of the network

Defines the properties of the central and the remote site APs

Figure 6.
Tags and Profiles association and mapping relationship

There are three different options for an administrator to accomplish the flow of creating profiles and tags:

- Use of the basic wireless setup wizard
- Use of advance wireless setup wizard
- Manual configuration

Please refer to the controller deployment guide for controller bring up, SVI creation, and management of GUI access.

The following sections will cover the method and ways a profile and tags can be configured on the Catalyst wireless platforms. An example of a store that has the following deployment model will be used to showcase the configuration model.

A store SSID that has a WPA-PSK security enabled to connect the handhelds used in a store – the SSID would be a locally switched SSID.

A guest SSID that is centrally switched.

An enterprise SSID for employees that has dot1x enabled and uses radius server for authentication.

Table 7. Deployment scenario examples

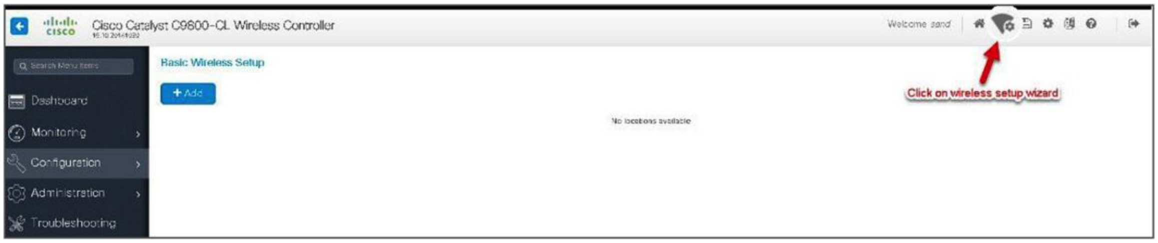
SSID	Security	Switching
Store-SSID	WPA-PSK	Local
Guest SSID	Web-auth	Central
Enterprise SSID	Wpa-2/dot1x	Local

Basic wireless setup wizard

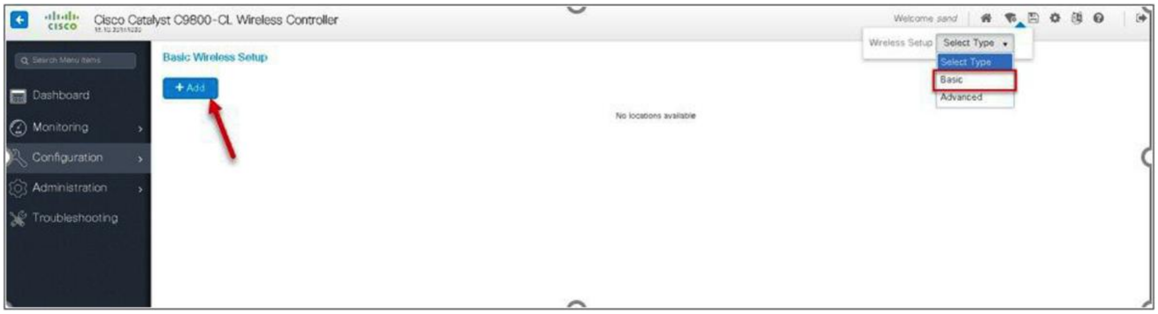
In the basic wireless setup wizard, we will cover the use of creating a store SSID with WP-PSK security.

Procedure

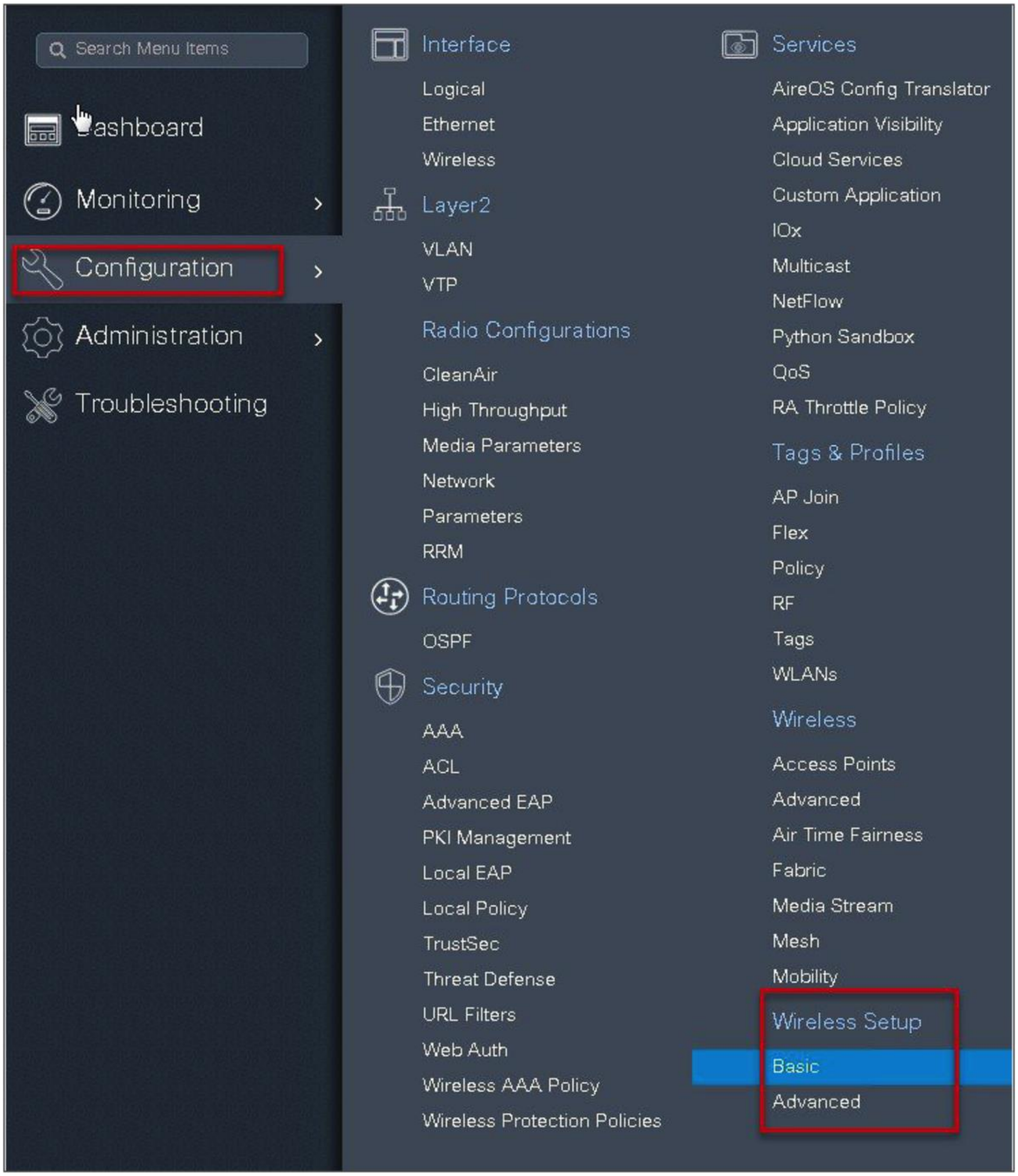
Step 1. Click on the wireless setup wizard.



Step 2. Select the basic setup wizard from the drop-down box and click on "Add."



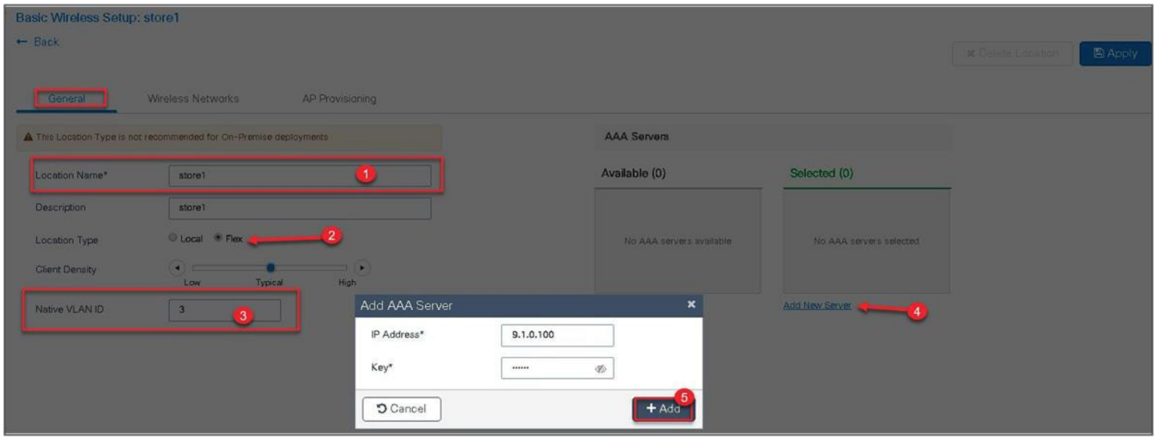
An administrator can also start the wizard by navigating to Configuration > Wireless Setup > Basic.



Step 3. Select a name for the remote site, and specify the location type as flex for branch deployments.

The native VLAN ID refers to the native VLAN ID pushed to the AP. The AAA server defines the radius server address pushed to the AP in the branch for local authentication.

To add a new server, click on “Add New server” and specify an IP address and a secret key.



Basic Wireless Setup: store1

This Location Type is not recommended for On-Premise deployments

Location Name* store1

Description store1

Location Type ○ Local ● Flex

Client Density: Typical

Native VLAN ID 3

AAA Servers

Available (0): No AAA servers available

Selected (0): No AAA servers selected

Add AAA Server

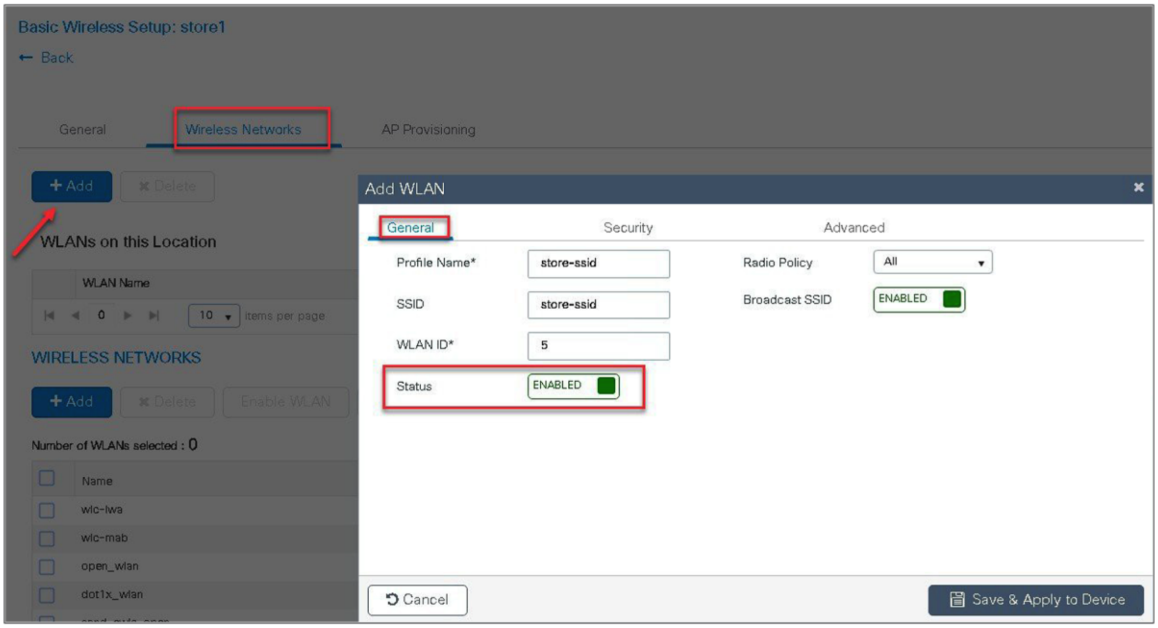
IP Address* 9.1.0.100

Key* ••••••

Step 4. Click on the wireless network to create an SSID along with the policy.

To create a new WLAN, click on “Define New.”

Define the security for the WLAN (for reference, an SSID with PSK is created here).



Basic Wireless Setup: store1

WLANs on this Location

WIRELESS NETWORKS

Number of WLANs selected : 0

Name: wlc-lwa, wlc-mab, open_wlan, dot1x_wlan

Add WLAN

Profile Name* store-ssid

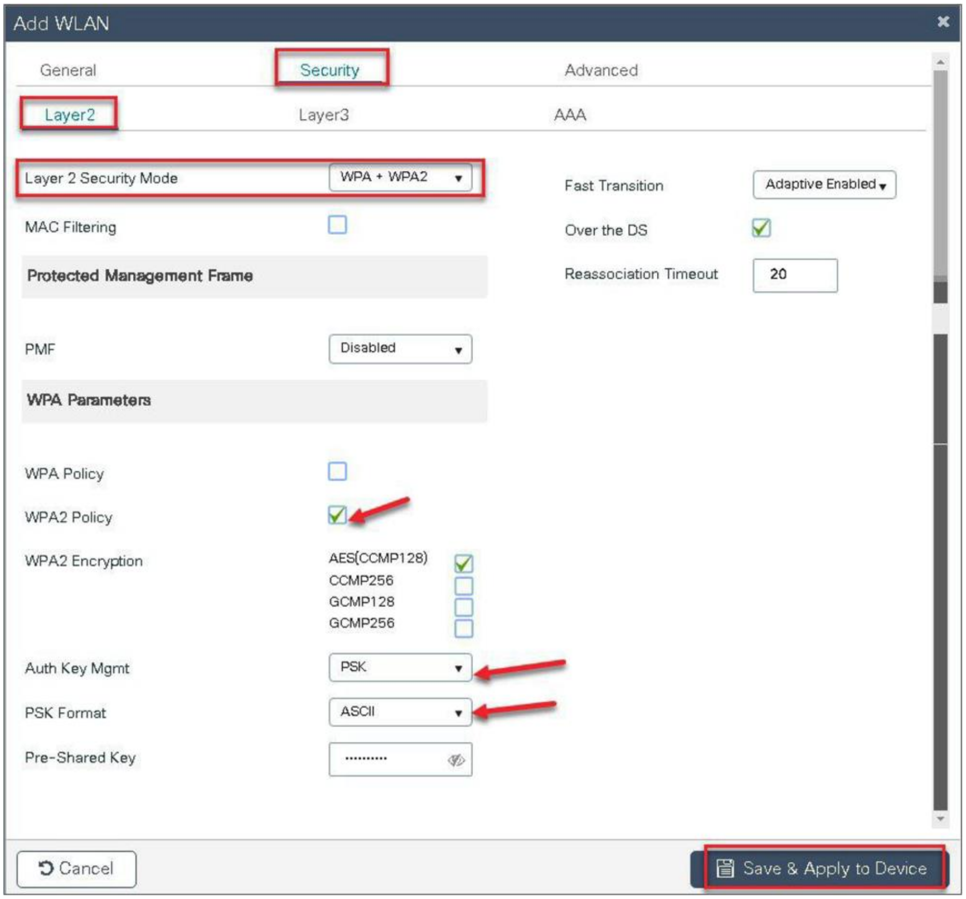
SSID store-ssid

WLAN ID* 5

Status ENABLED

Radio Policy All

Broadcast SSID ENABLED



Add WLAN

General | Security | Advanced

Layer2 | Layer3 | AAA

Layer 2 Security Mode: WPA + WPA2

MAC Filtering: □

Protected Management Frame

PMF: Disabled

WPA Parameters

WPA Policy: □

WPA2 Policy: ☑

WPA2 Encryption: AES(CCMP128) ☑, CCMP256 □, GCMP128 □, GCMP256 □

Auth Key Mgmt: PSK

PSK Format: ASCII

Pre-Shared Key: ··········

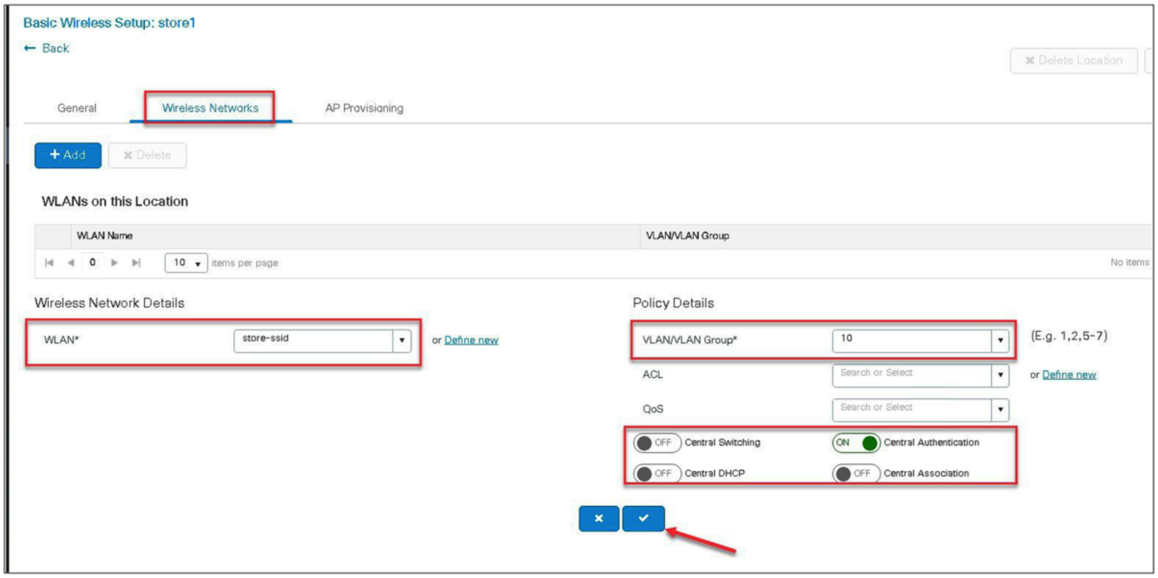
Fast Transition: Adaptive Enabled

Over the DS: ☑

Reassociation Timeout: 20

Step 5. Define the policy for the WLAN.

The VLAN/VLAN group defines the VLAN used by the SSID.



Basic Wireless Setup: store1

WLANs on this Location

WLAN Name	VLAN/VLAN Group

0 · 10 items per page · No items

Wireless Network Details

WLAN*: store-ssid or Define new

Policy Details

VLAN/VLAN Group*: 10 (E.g. 1,2,5-7)

ACL: Search or Select or Define new

QoS: Search or Select

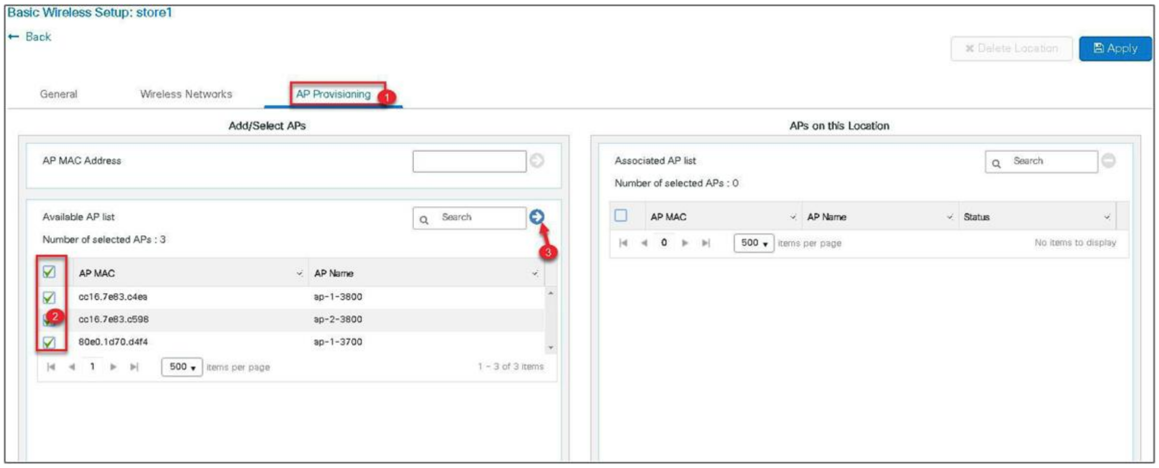
OFF Central Switching · ON Central Authentication

OFF Central DHCP · OFF Central Association

Step 6. Click on the AP provisioning to provision the SSID and policy profile on the selected AP.

Once the AP is provisioned, the AP gets converted to flex mode based on the site tag assigned to the AP.

If the AP is already in flex mode, there is no conversion. If the AP is in local mode, the AP would reboot to boot in FlexConnect mode.



Basic Wireless Setup: store1

Add/Select APs

AP MAC Address

Available AP list

Number of selected APs : 3

☑	AP MAC	AP Name
☑	cc16.7e83.c4ea	ap-1-3800
☑	cc16.7e83.c598	ap-2-3800
☑	80e0.1d70.d4f4	ap-1-3700

1 - 3 of 3 items

APs on this Location

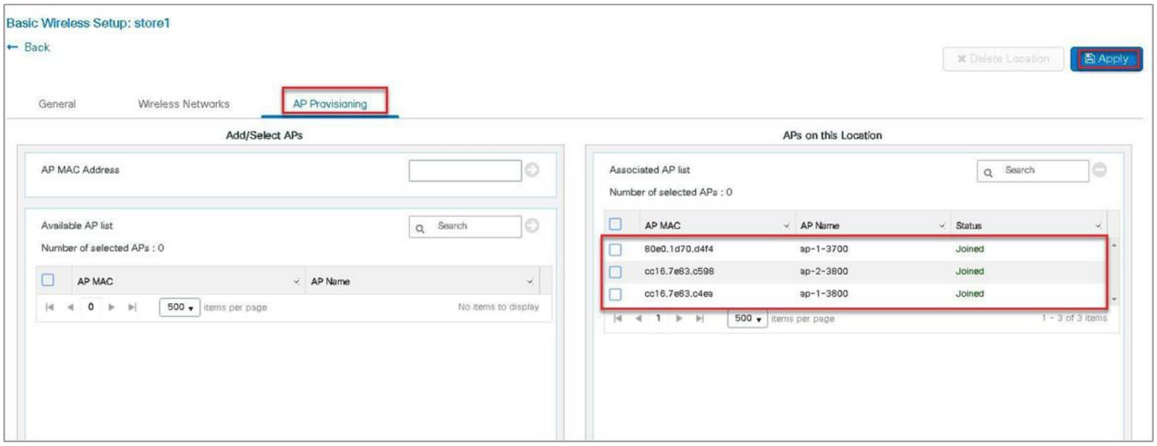
Associated AP list

Number of selected APs : 0

□	AP MAC	AP Name	Status

No items to display

Step 7. Click apply to complete the wizard.



Basic Wireless Setup: store1

Add/Select APs

AP MAC Address

Available AP list

Number of selected APs : 0

□	AP MAC	AP Name

No items to display

APs on this Location

Associated AP list

Number of selected APs : 0

□	AP MAC	AP Name	Status
□	80e0.1d70.d4f4	ap-1-3700	Joined
□	cc16.7e83.c598	ap-2-3800	Joined
□	cc16.7e83.c4ea	ap-1-3800	Joined

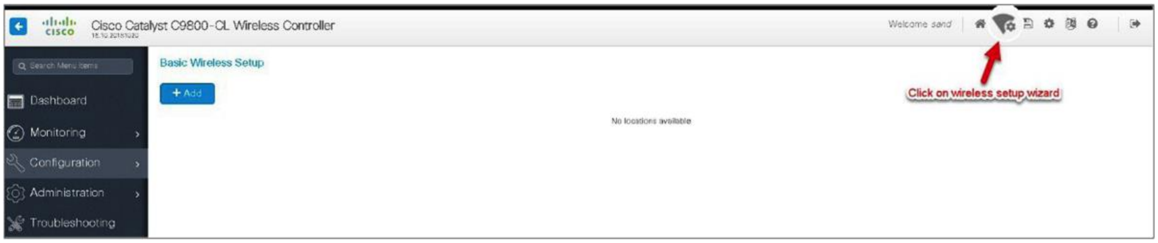
1 - 3 of 3 items

Advanced wireless setup wizard

In this section, the advance config wizard is used to create a guest SSID with web authentication, which would be centrally switched through a WLC at the data center.

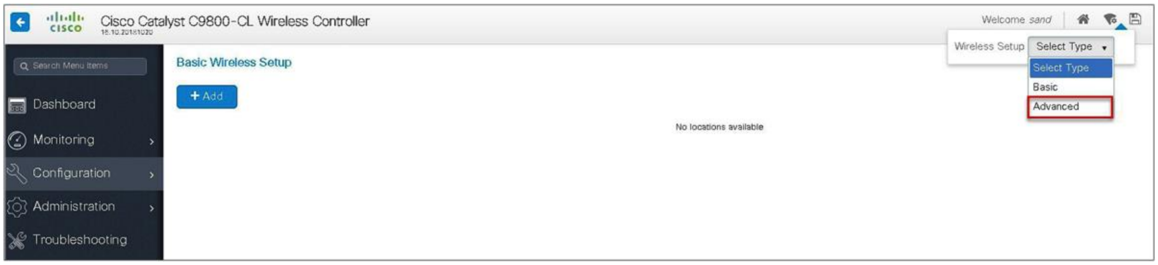
Procedure

Step 1. Click on the wireless setup wizard.

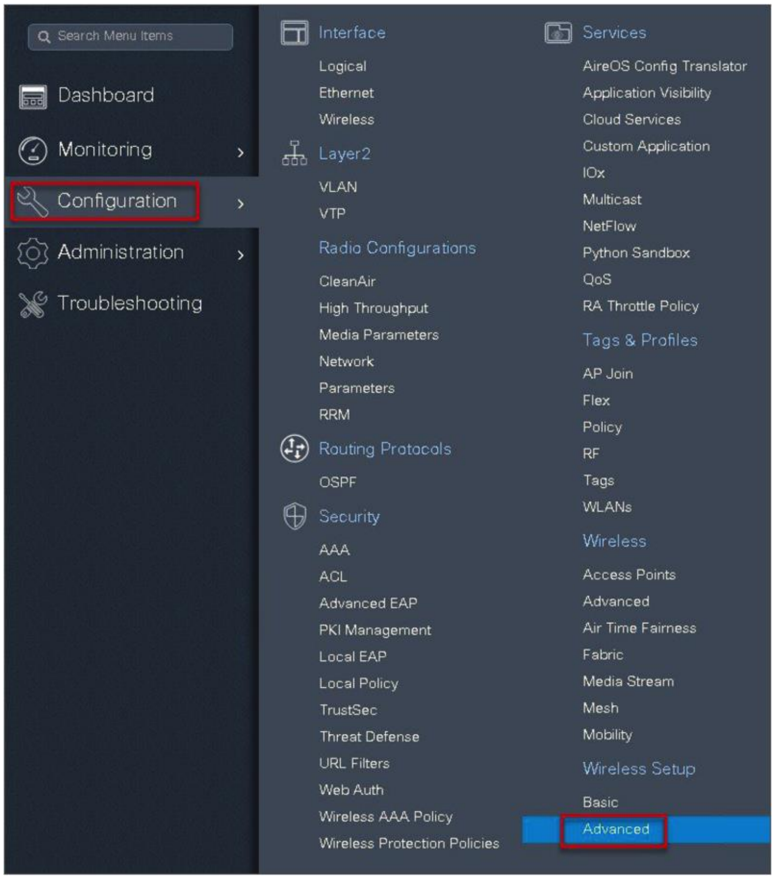


Click on wireless setup wizard

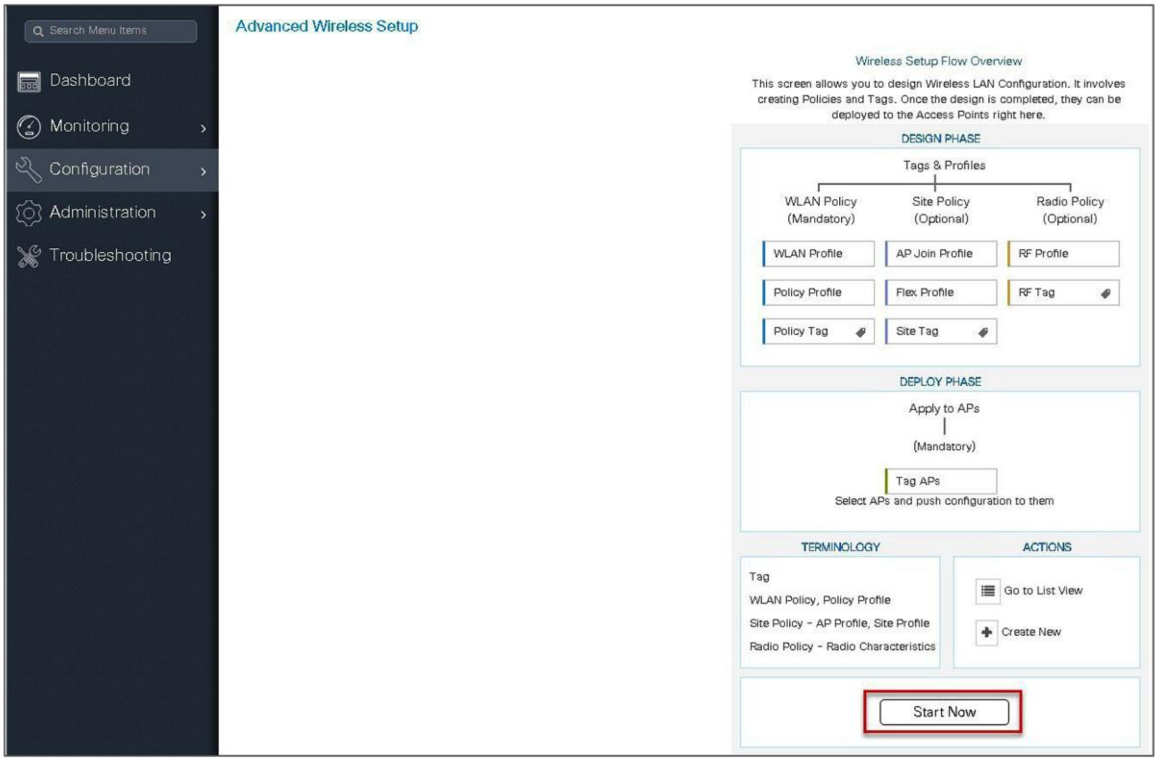
Step 2. Select the advanced option.



An administrator can also start the wizard by navigating to Configuration > Wireless Setup > Advanced.



Step 3. The advanced config wizard gives an overview of the flow of tags and policies. Click on the "Start Now" button to start the wizard.

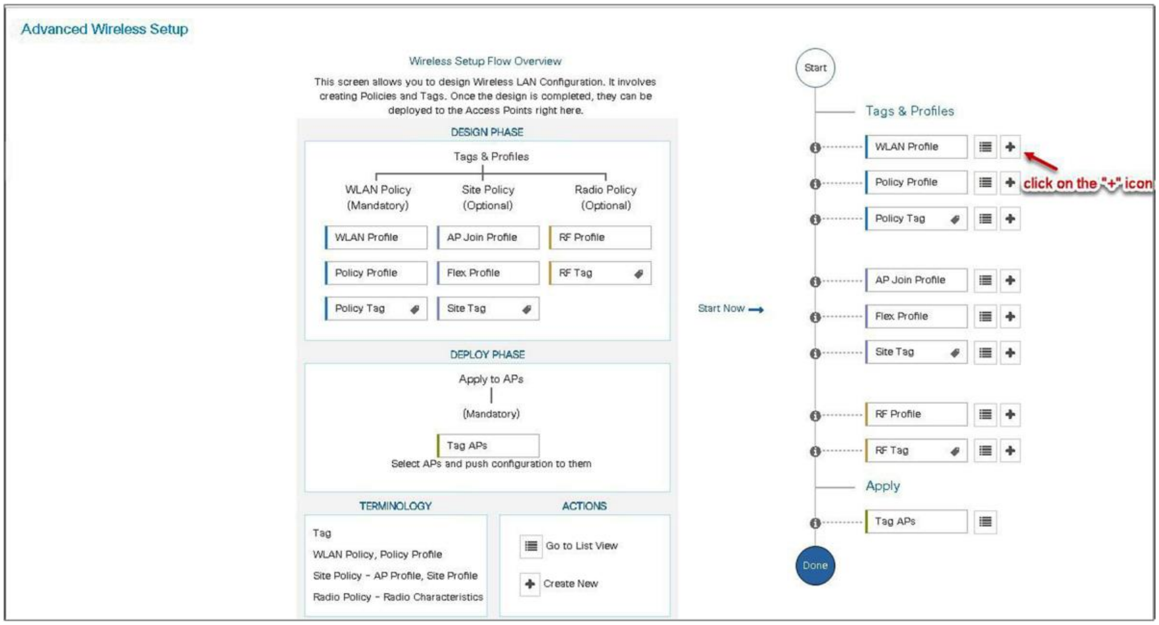


This screen allows you to design Wireless LAN Configuration. It involves creating Policies and Tags. Once the design is completed, they can be deployed to the Access Points right here.

Select APs and push configuration to them

Tag
WLAN Policy, Policy Profile
Site Policy - AP Profile, Site Profile
Radio Policy - Radio Characteristics

Step 4. Click on the "+" icon to start creating the WLAN.

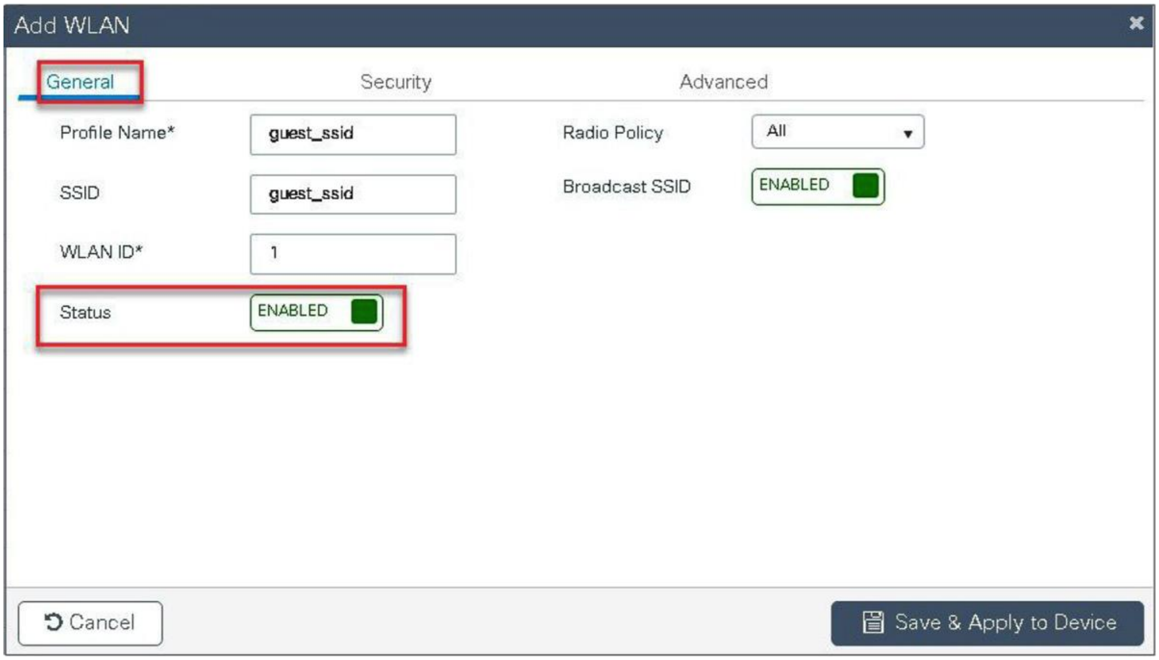


This screen allows you to design Wireless LAN Configuration. It involves creating Policies and Tags. Once the design is completed, they can be deployed to the Access Points right here.

Select APs and push configuration to them

Tag
WLAN Policy, Policy Profile
Site Policy - AP Profile, Site Profile
Radio Policy - Radio Characteristics

Step 5. Define the SSID name and security type for the WLAN.



Add WLAN

Profile Name* guest_ssid

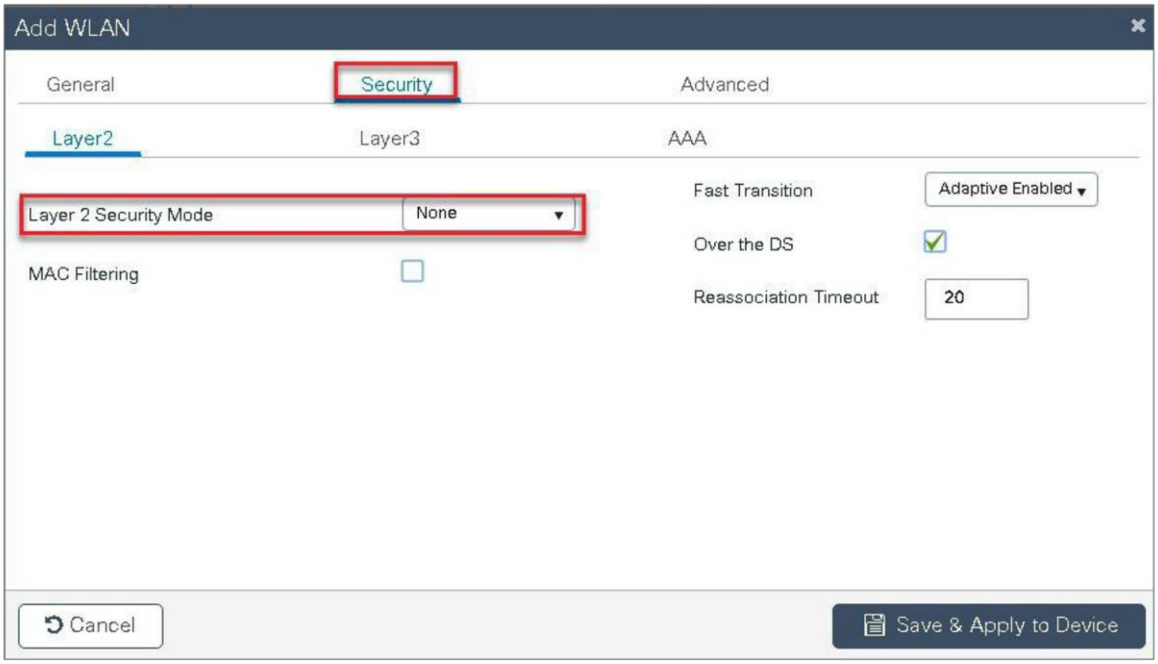
SSID guest_ssid

WLAN ID* 1

Status ENABLED

Radio Policy All

Broadcast SSID ENABLED



Add WLAN

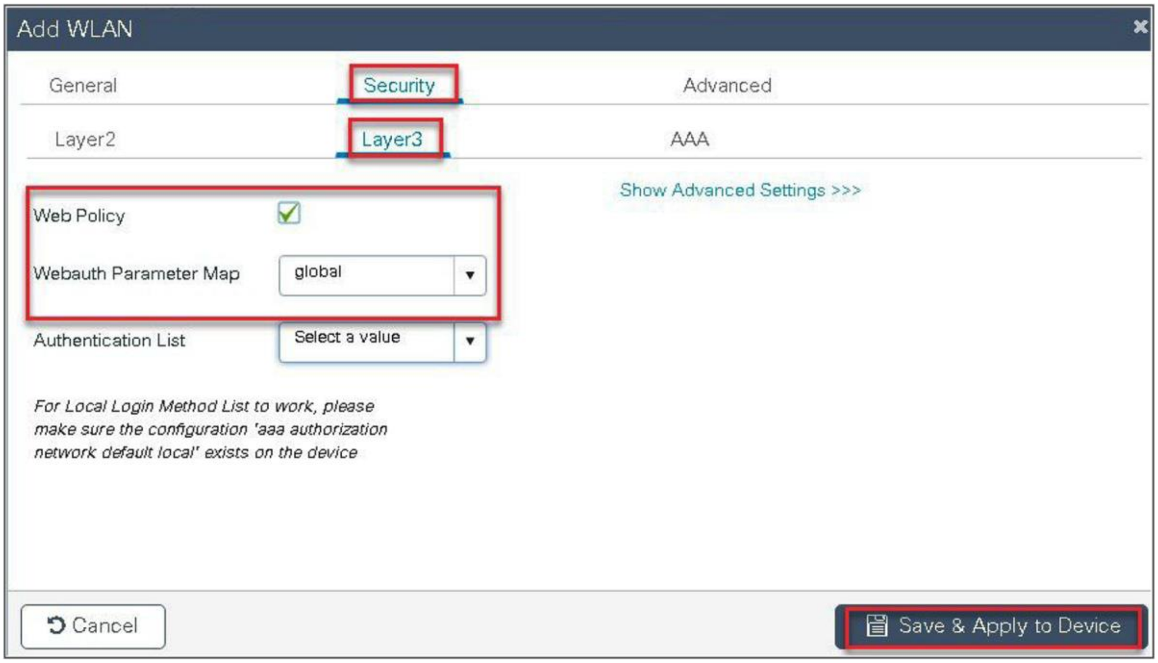
Layer 2 Security Mode None

MAC Filtering □

Fast Transition Adaptive Enabled

Over the DS ☑

Reassociation Timeout 20

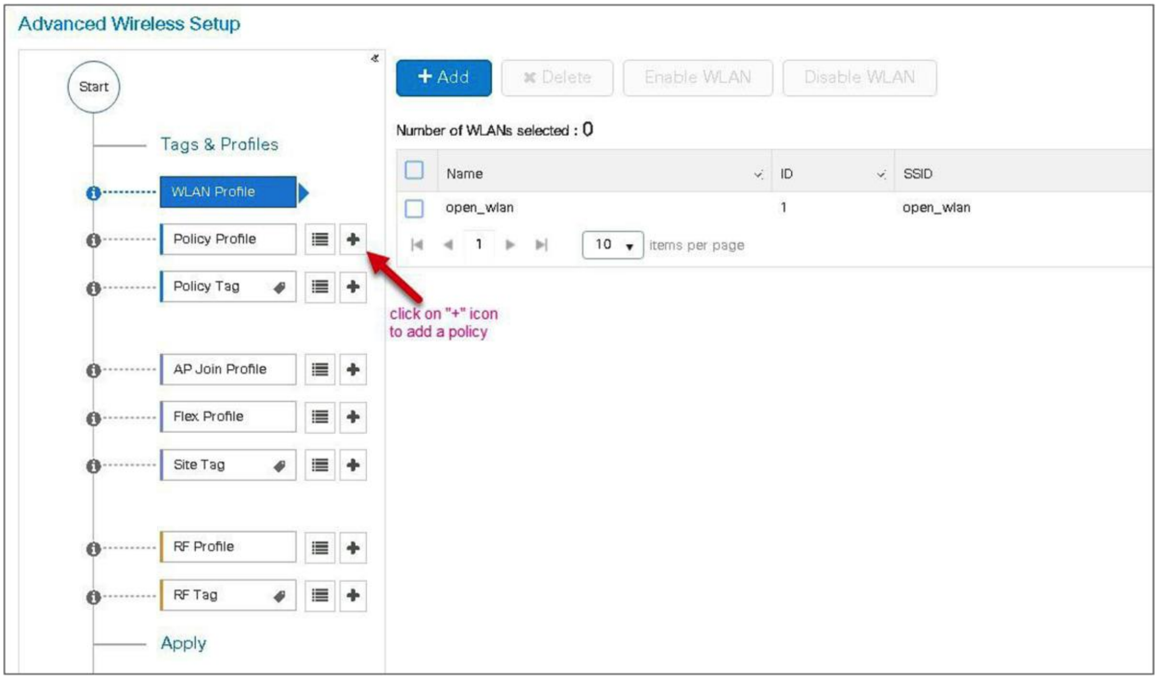


Web Policy	☑
Webauth Parameter Map	global
Authentication List	Select a value

For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device

Step 6. Create a policy profile for the SSID.

Define the policy profile to be central switched and central authentication.

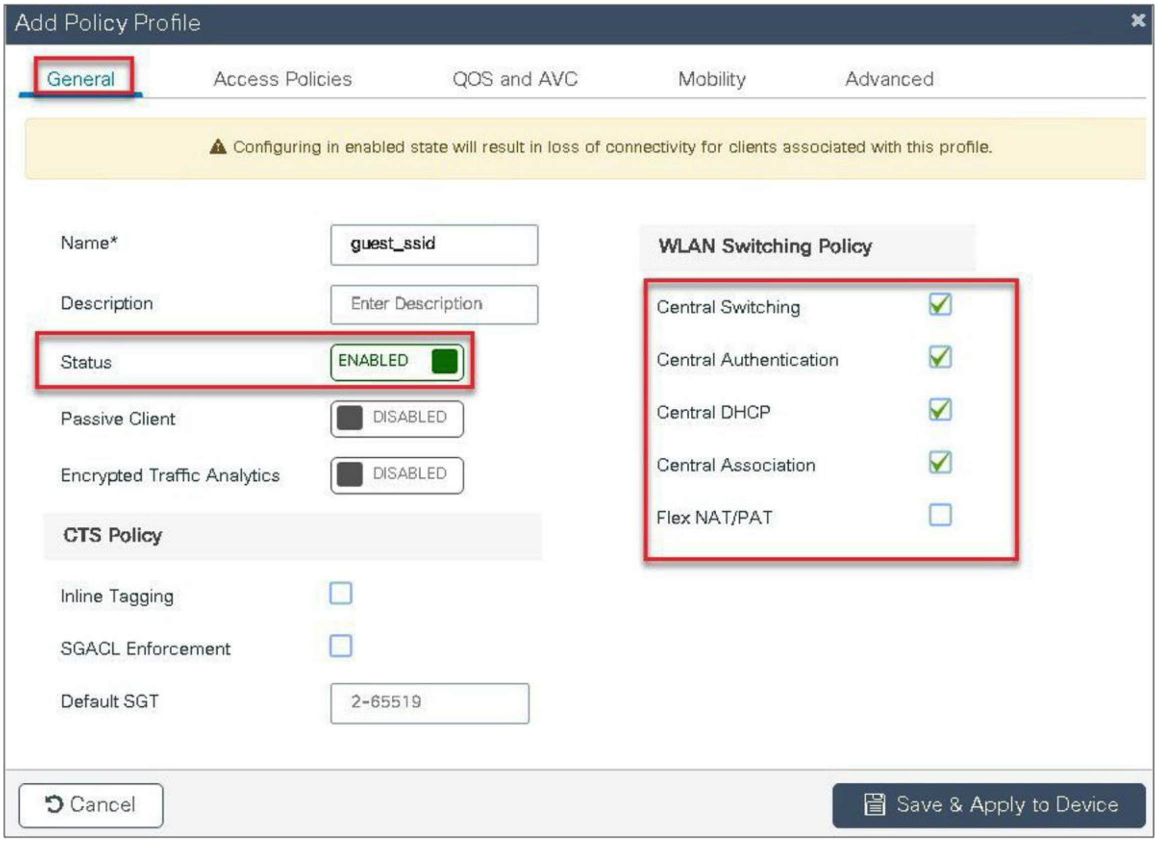


Number of WLANs selected : 0

□	Name	ID	SSID
□	open_wlan	1	open_wlan

1 | 10 items per page

click on "+" icon to add a policy



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

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

CTS Policy

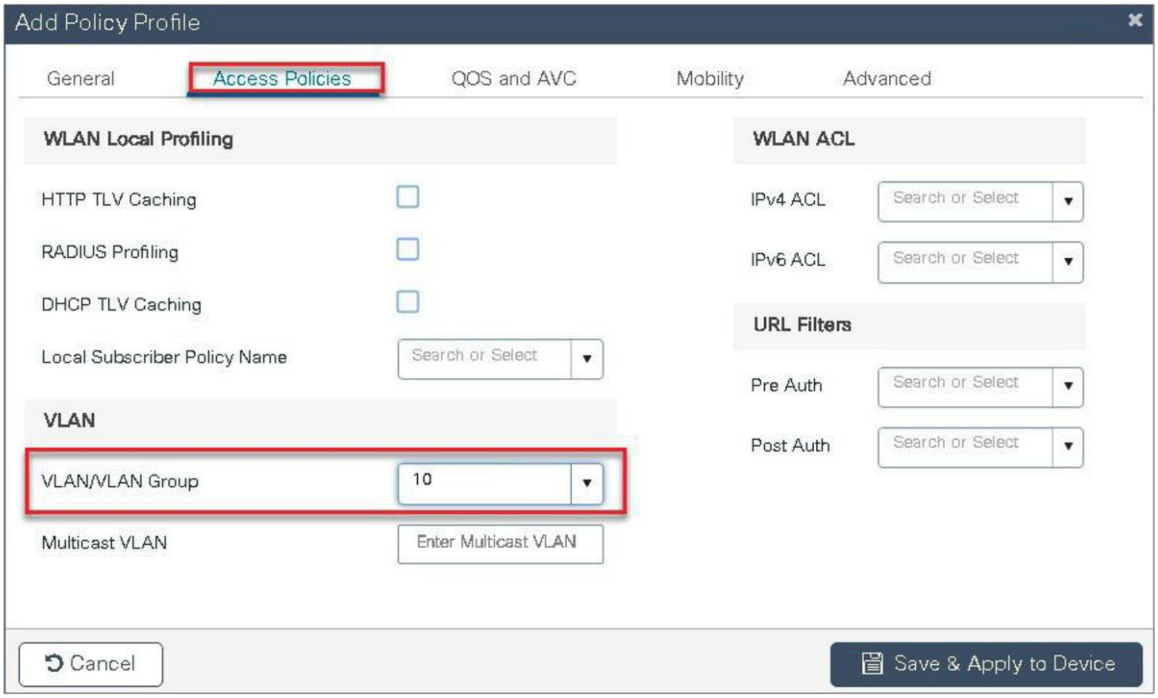
Inline Tagging	□
SGACL Enforcement	□
Default SGT	2-65519

WLAN Switching Policy

Central Switching	☑
Central Authentication	☑
Central DHCP	☑
Central Association	☑
Flex NAT/PAT	□

Step 7. Define a VLAN for the SSID under the access policies. In the example below, the VLAN 10 is mapped on the policy profile.

The controller also needs a Layer 2 VLAN or a Layer 3 SVI to be created to centrally switch the traffic from the controller.



WLAN Local Profiling

HTTP TLV Caching	□
RADIUS Profiling	□
DHCP TLV Caching	□
Local Subscriber Policy Name	Search or Select

VLAN

VLAN/VLAN Group	10
Multicast VLAN	Enter Multicast VLAN

WLAN ACL

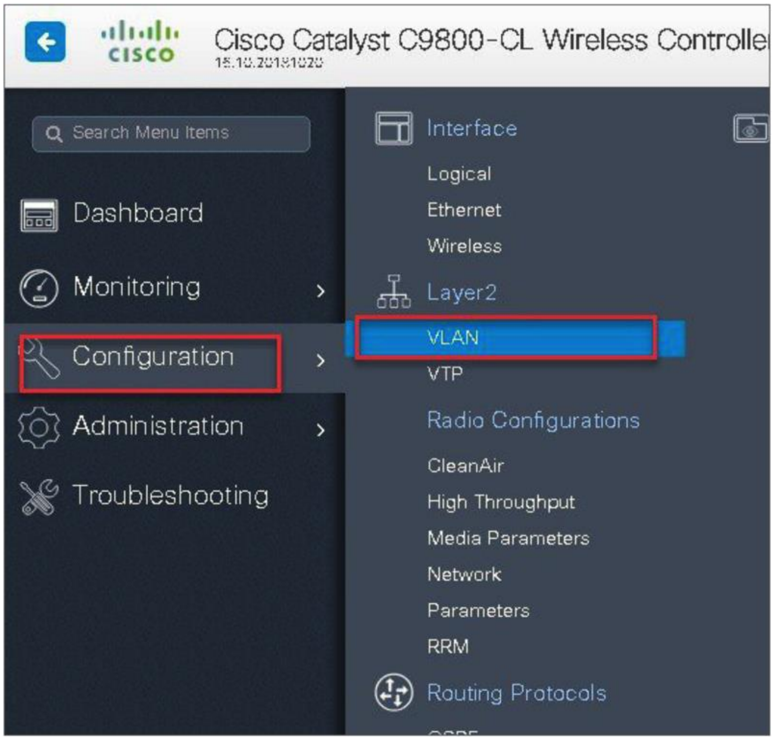
IPv4 ACL	Search or Select
IPv6 ACL	Search or Select

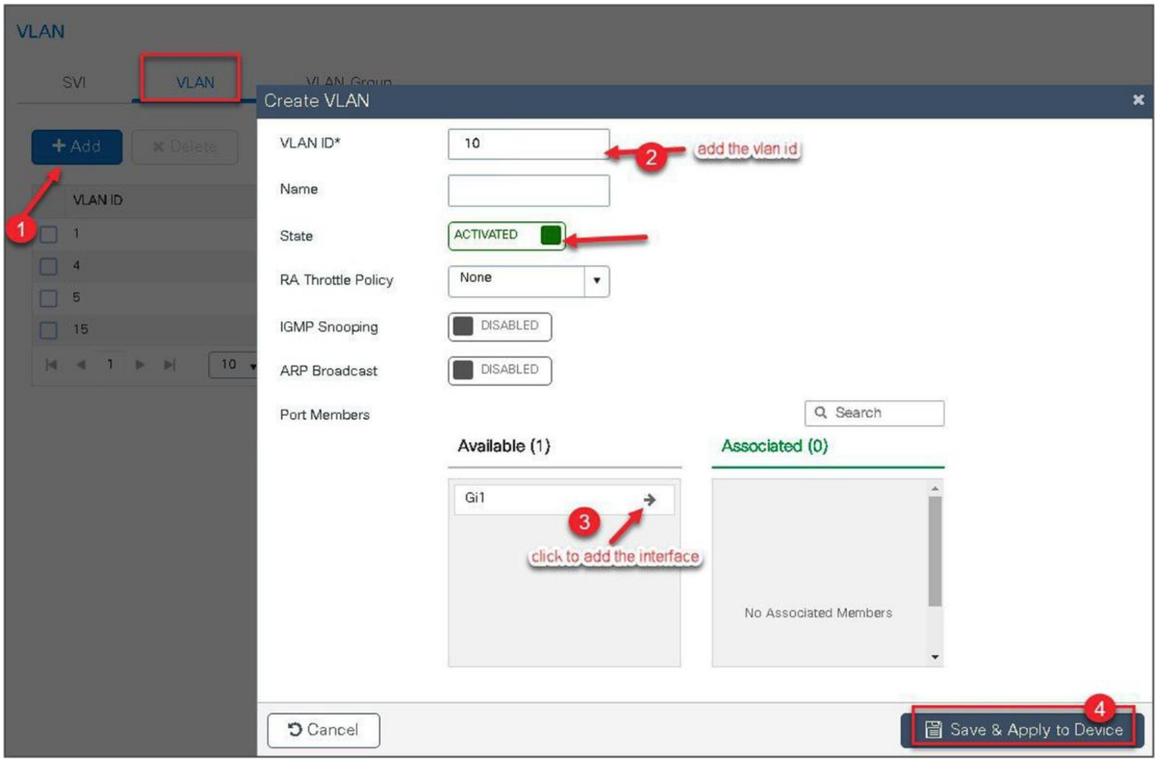
URL Filters

Pre Auth	Search or Select
Post Auth	Search or Select

In this example, we create a Layer 2 VLAN on the controller.

Navigate to Configuration > VLAN.





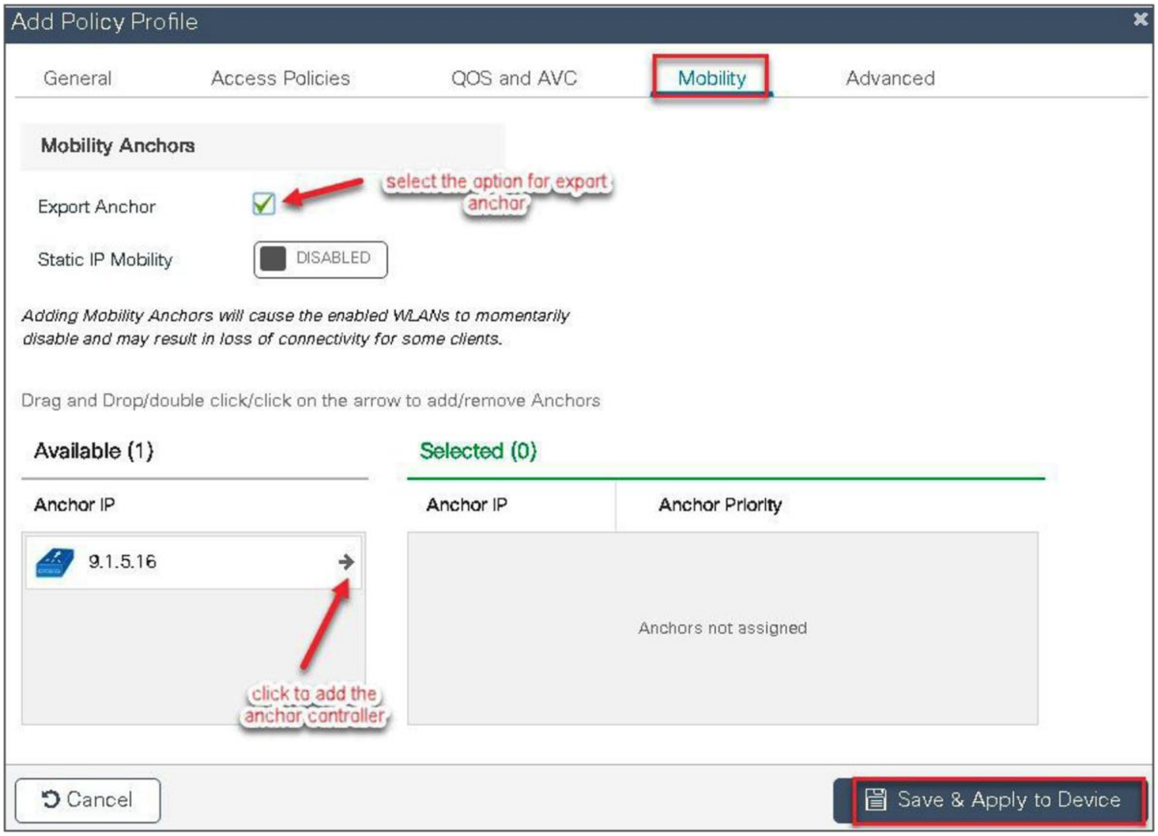
Create VLAN

VLAN ID*	10
Name	
State	ACTIVATED
RA Throttle Policy	None
IGMP Snooping	DISABLED
ARP Broadcast	DISABLED
Port Members	

add the vlan id

click to add the interface

Step 8. An optional attribute to set is the export anchor configuration. Please refer to the mobility deployment guide to set up mobility peers.



Add Policy Profile

Mobility Anchors

Export Anchor ☑

Static IP Mobility DISABLED

Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (1)

Anchor IP
9.1.5.16

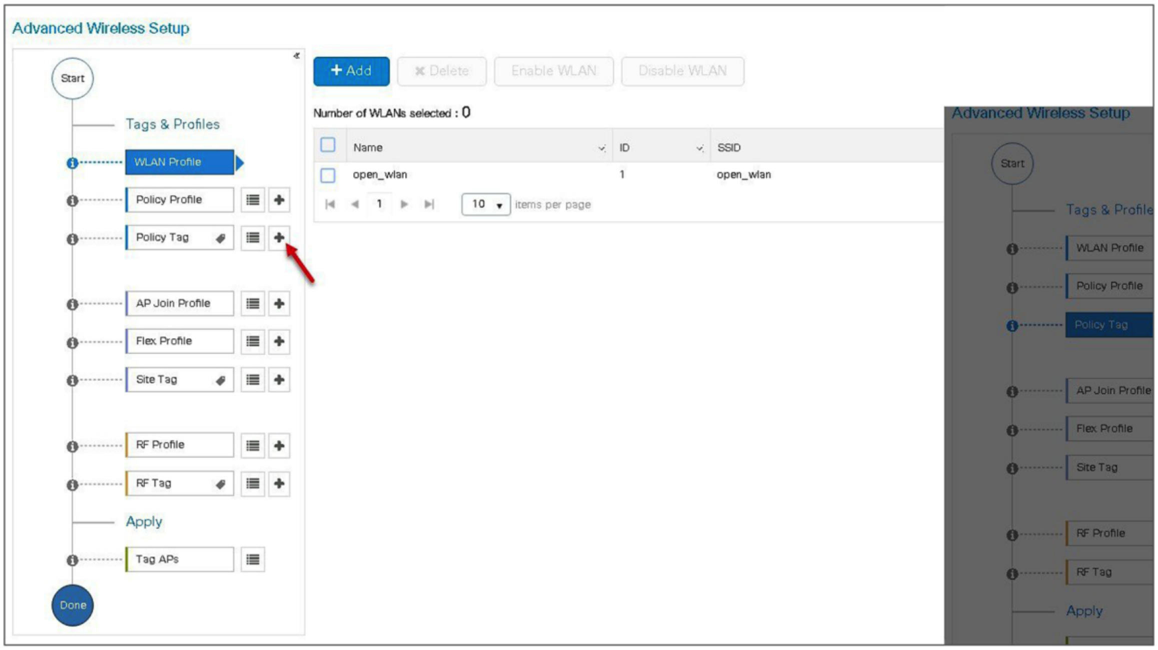
Selected (0)

Anchor IP	Anchor Priority
Anchors not assigned	

select the option for export anchor

click to add the anchor controller

Step 9. Create a policy tag that binds the SSID and policy profile together.



Advanced Wireless Setup

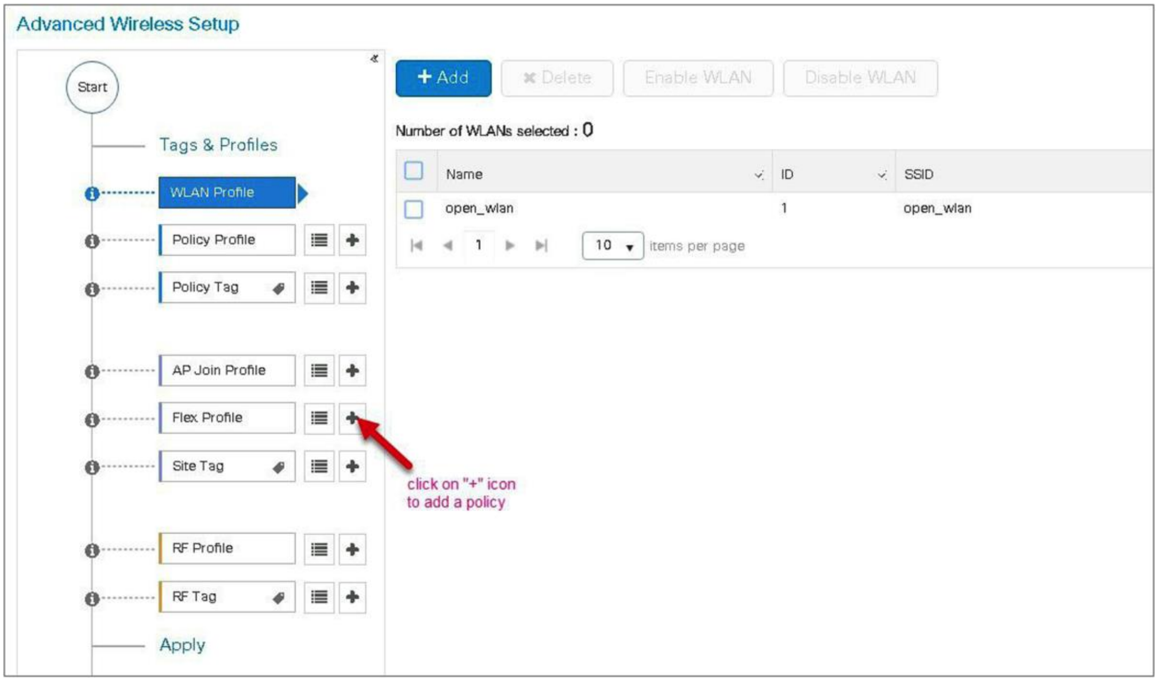
Number of WLANs selected : 0

□	Name	ID	SSID
□	open_wlan	1	open_wlan

1 10 items per page

Step 10. Define a flex profile. The flex profile is used for configuring the VLANs on the AP that is used for the local switched SSIDs.

In this example, the guest SSID is centrally switched. In cases where there is a mix of central-switched and local-switched SSIDs, an administrator can create a flex profile and define the VLANs to be used by the local-switched SSIDs.



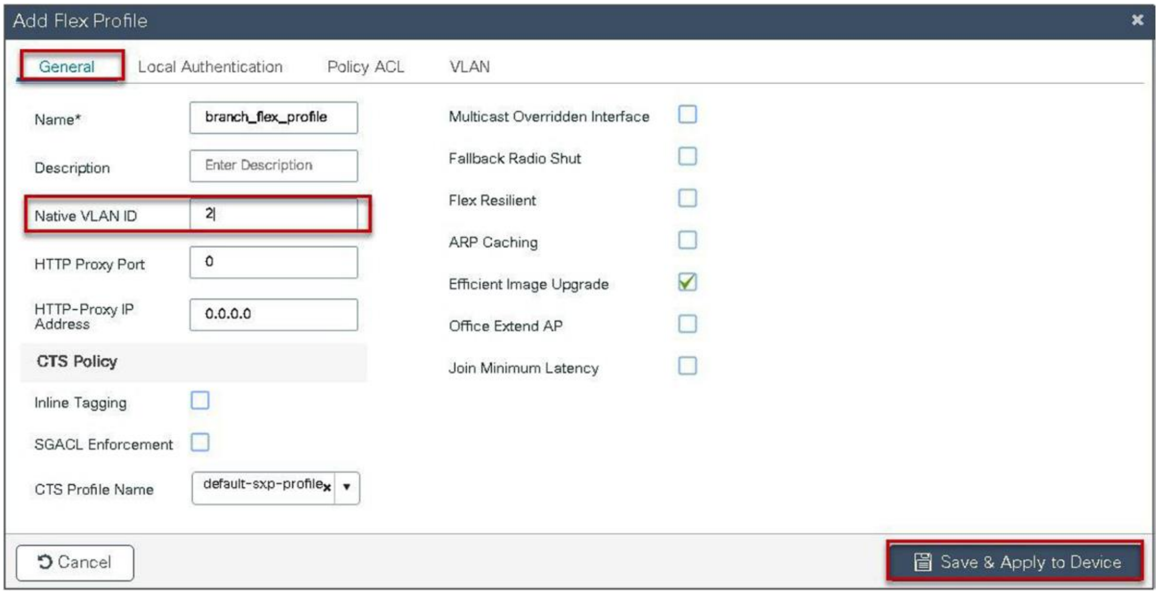
Number of WLANs selected : 0

□	Name	ID	SSID
□	open_wlan	1	open_wlan

1 | 10 items per page

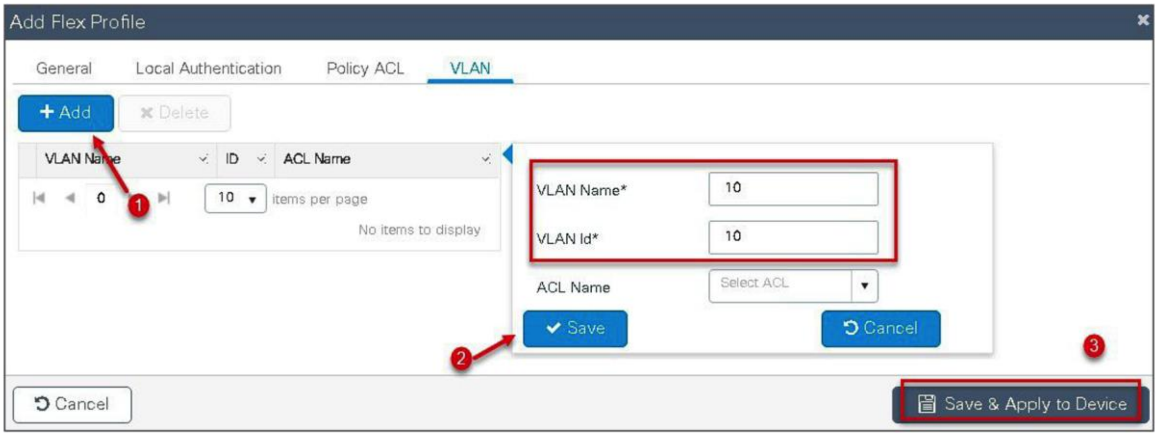
click on "+" icon to add a policy

Step 11. Define the native VLAN for the FlexConnect APs.



Name*	branch_flex_profile	Multicast Overridden Interface	□
Description	Enter Description	Fallback Radio Shut	□
Native VLAN ID	2	Flex Resilient	□
HTTP Proxy Port	0	ARP Caching	□
HTTP-Proxy IP Address	0.0.0.0	Efficient Image Upgrade	☑
CTS Policy		Office Extend AP	□
Inline Tagging	□	Join Minimum Latency	□
SGACL Enforcement	□		
CTS Profile Name	default-sxp-profile		

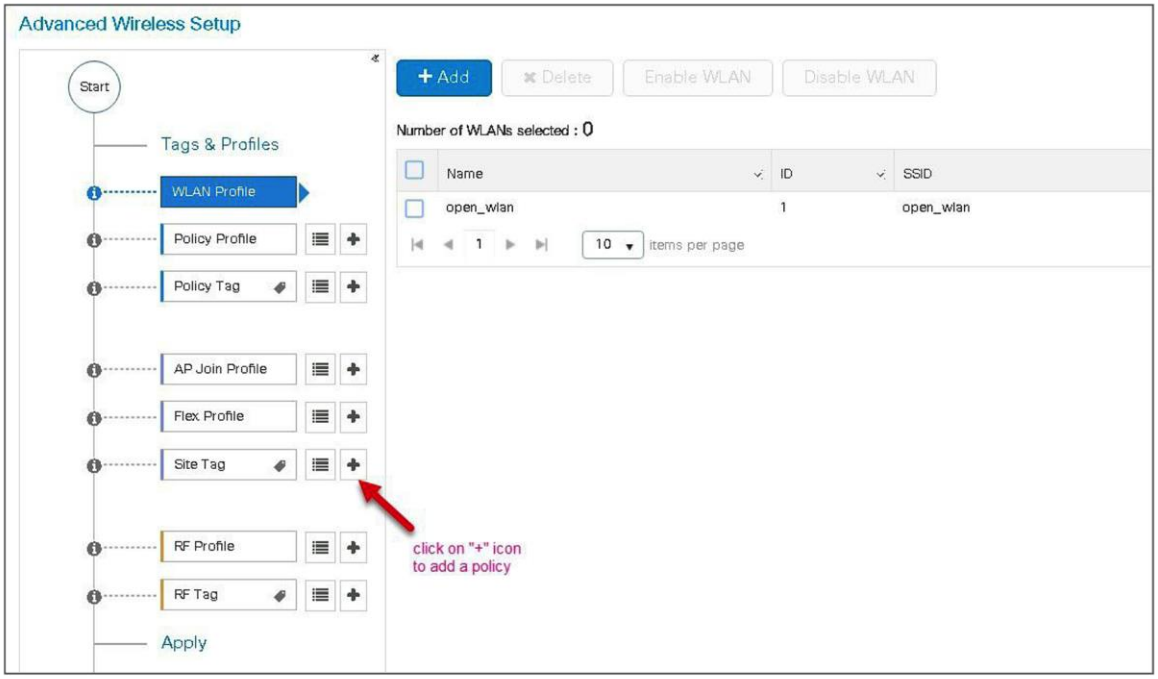
Step 12. Define the VLANS to be used for the local-switched SSID.



Add Flex Profile

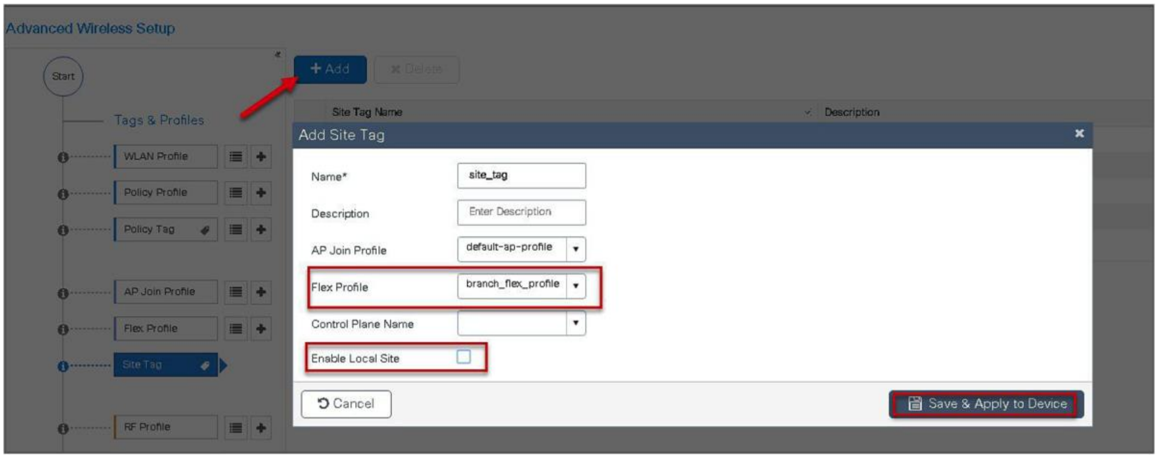
VLAN Name*	10
VLAN Id*	10
ACL Name	Select ACL ▾

Step 13. Define a site tag that binds the flex profile and a default AP join profile. To add a flex profile on a site tag, uncheck the "Enable Local Site" option.



Number of WLANs selected : 0

Name	ID	SSID
open_wlan	1	open_wlan



Add Site Tag

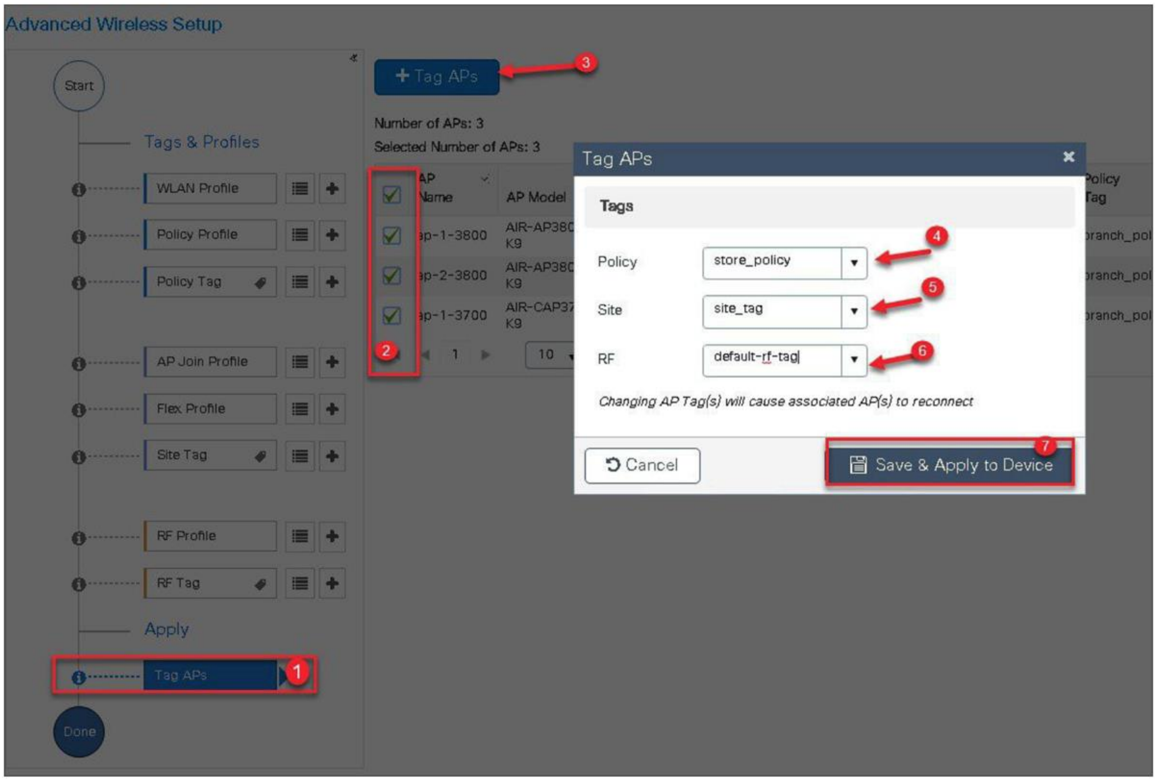
Name*	site_tag
Description	Enter Description
AP Join Profile	default-ap-profile ▾
Flex Profile	branch_flex_profile ▾
Control Plane Name	▾
Enable Local Site	☐

Step 14. The final stage is to provision the policy, site, and RF tag on the AP. Click on “Tag Aps” to select the profiles and have it configured for the AP. In this example, the AP is tagged using a default RF tag.

Once the AP is provisioned with the site tag, the AP gets converted to flex mode based on the site tag assigned to the AP.

If the AP is already in flex mode, there is no conversion. If the AP is in local mode, the AP would reboot to boot in FlexConnect mode.

The assigning of a tag does the auto-conversion of the AP mode based on properties of the tag.



Number of APs: 3
Selected Number of APs: 3

☑	AP Name	AP Model	Policy Tag
☑	ap-1-3800	AIR-AP380 K9	branch_pol
☑	ap-2-3800	AIR-AP380 K9	branch_pol
☑	ap-1-3700	AIR-CAP37 K9	branch_pol

Tag APs

Tags

Policy: store_policy

Site: site_tag

RF: default-rf-tag

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

Manual configuration

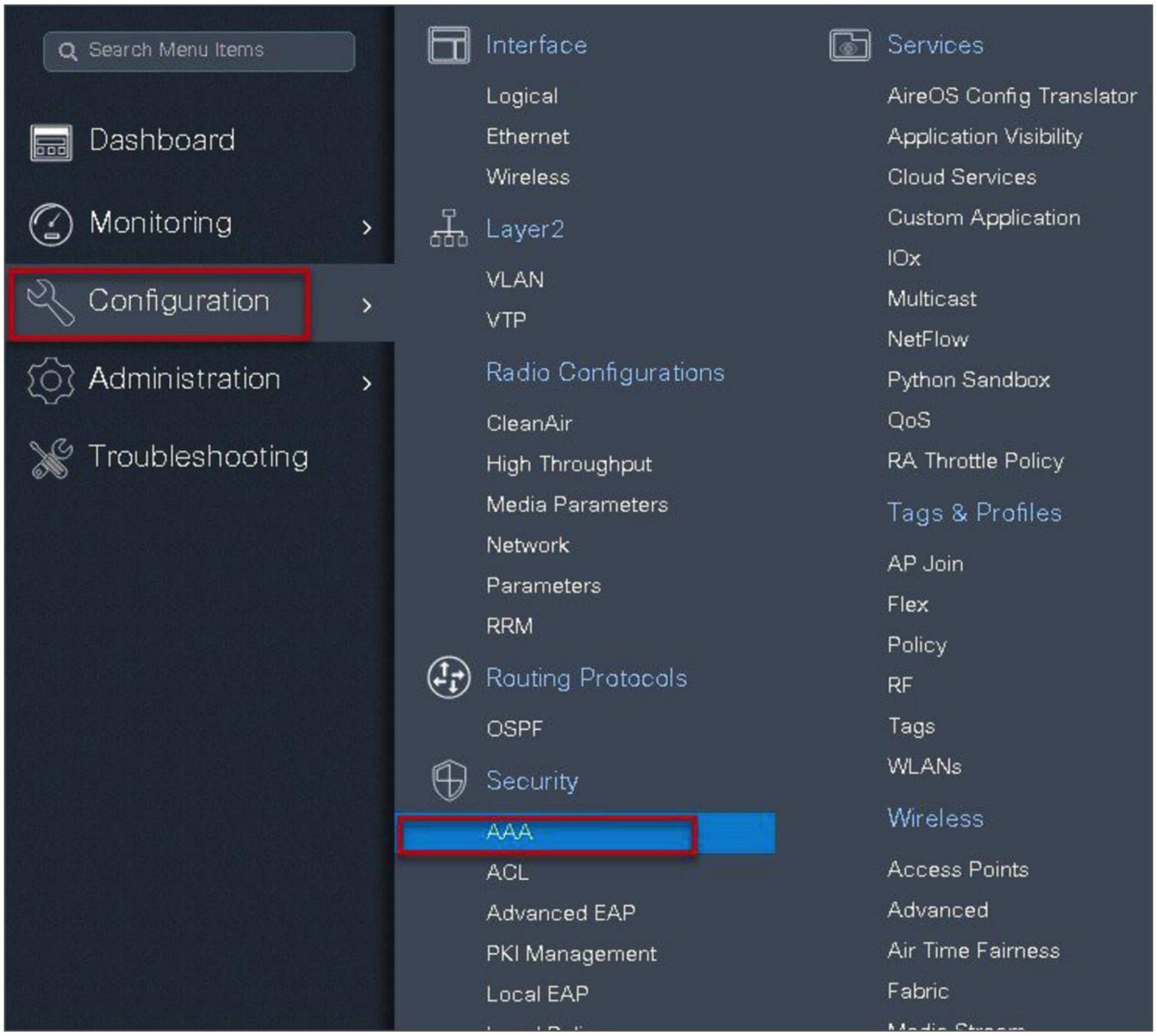
The manual configuration for creating the SSID/tags and profiles is done using the WLC GUI. In this section, we will cover creating an enterprise SSID with dot1x enabled.

The first step in creating an enterprise SSID with dot1x is to define the AAA server for authentication.

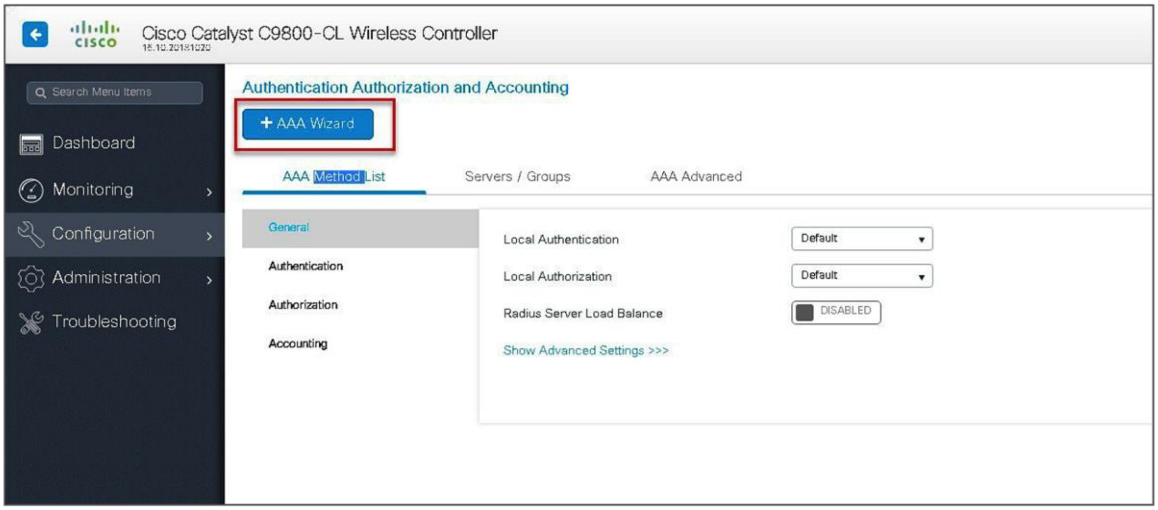
Procedure

Step 1. Define an AAA server and method list for dot1x, which is mapped to the WLAN. The AAA server is created by navigating to the following:

Configuration > Security > AAA



Step 2. Use the AAA wizard to create the server and server groups.



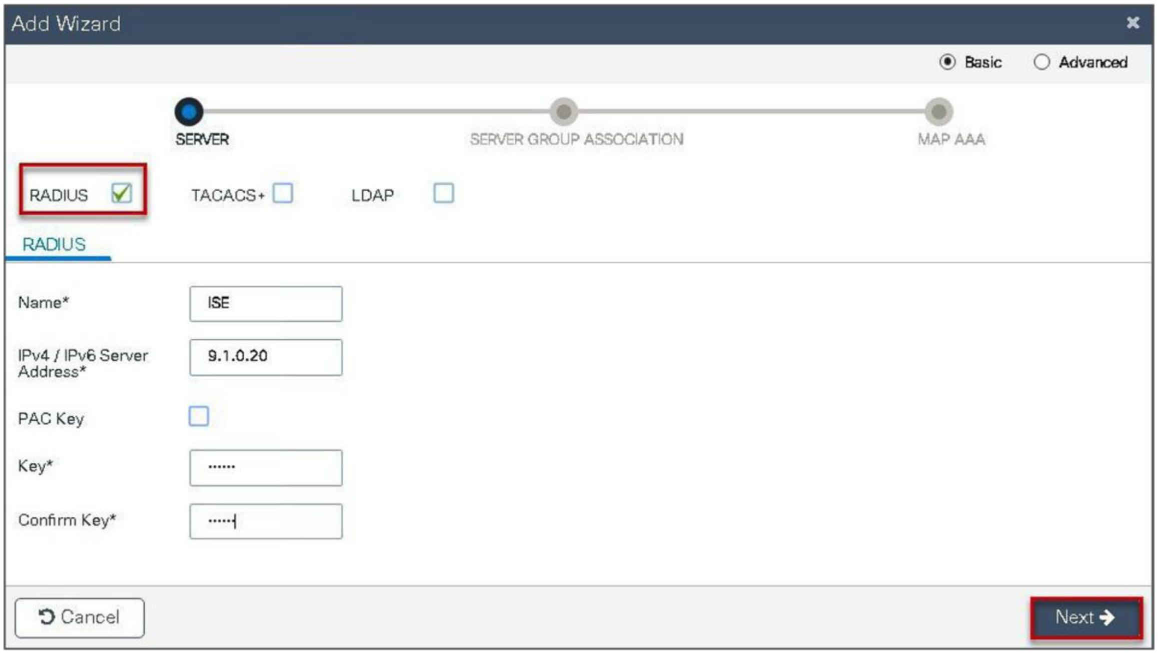
Authentication Authorization and Accounting

Local Authentication: Default

Local Authorization: Default

Radius Server Load Balance: DISABLED

Step 3. Define a name for the server and specify the IP address and shared secret.



Add Wizard

● Basic ○ Advanced

RADIUS ☑ TACACS+ □ LDAP □

Name*: ISE

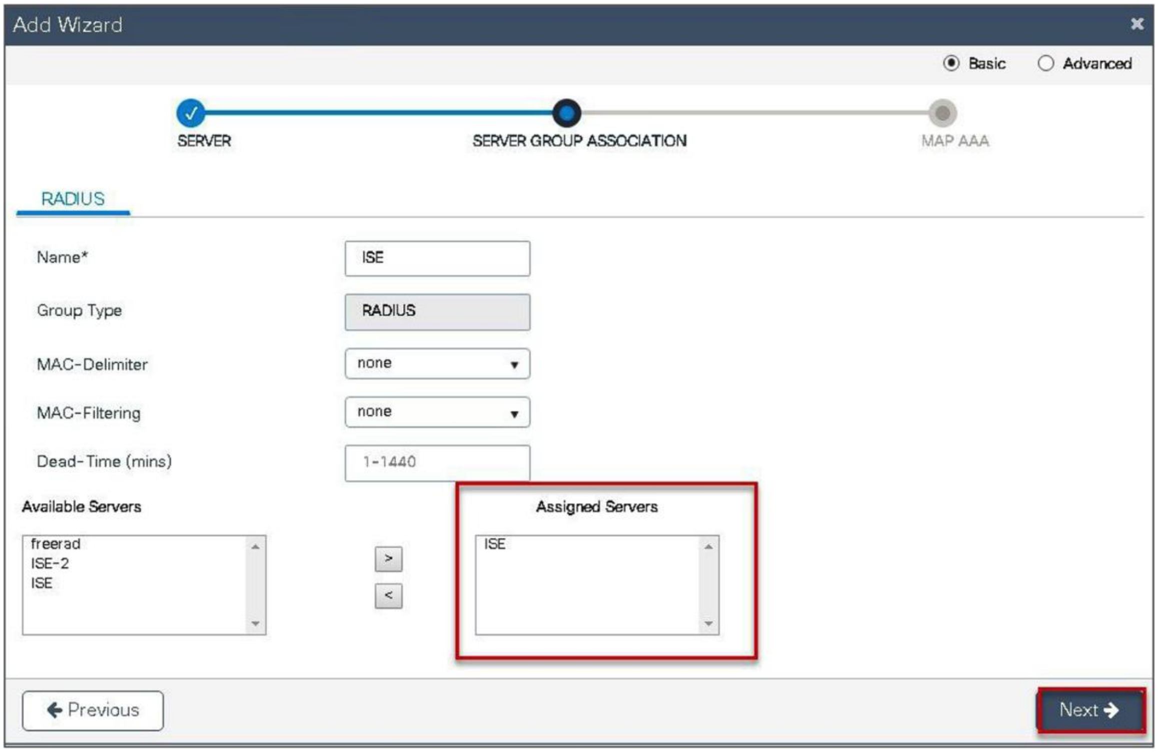
IPv4 / IPv6 Server Address*: 9.1.0.20

PAC Key: □

Key*: ••••••

Confirm Key*: ••••••

Step 4. Create a server group and map the server in the group.



Name*: ISE

Group Type: RADIUS

MAC-Delimiter: none

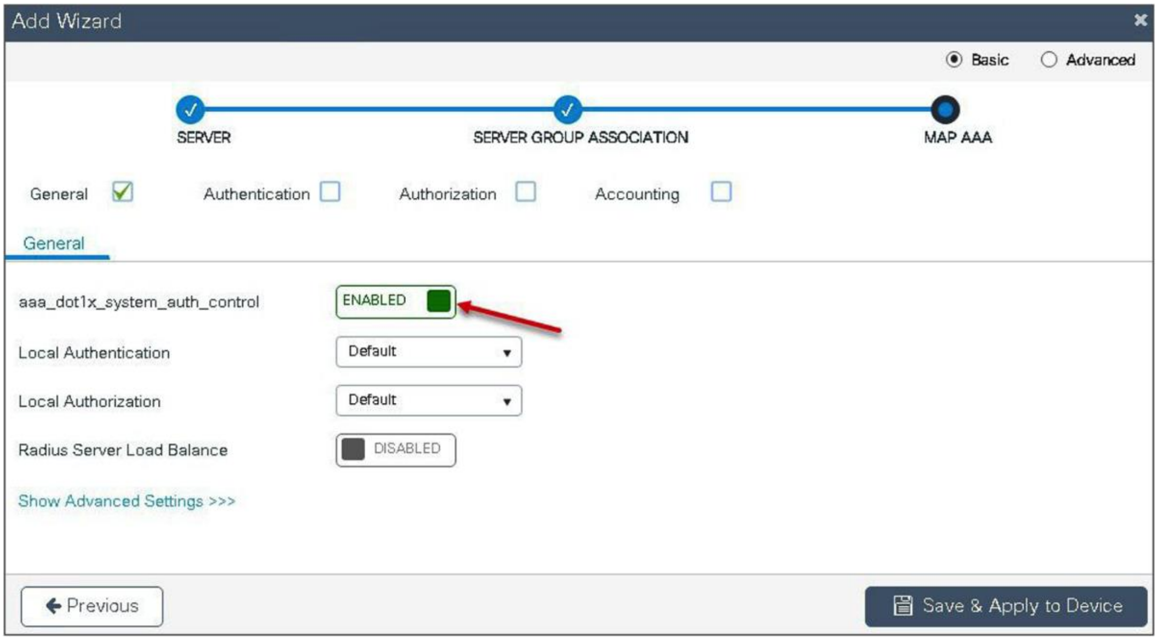
MAC-Filtering: none

Dead-Time (mins): 1-1440

Available Servers: freerad, ISE-2, ISE

Assigned Servers: ISE

Step 5. Enable dot1x system control and checkmark the authentication and authorization profile.



General ☑ Authentication □ Authorization □ Accounting □

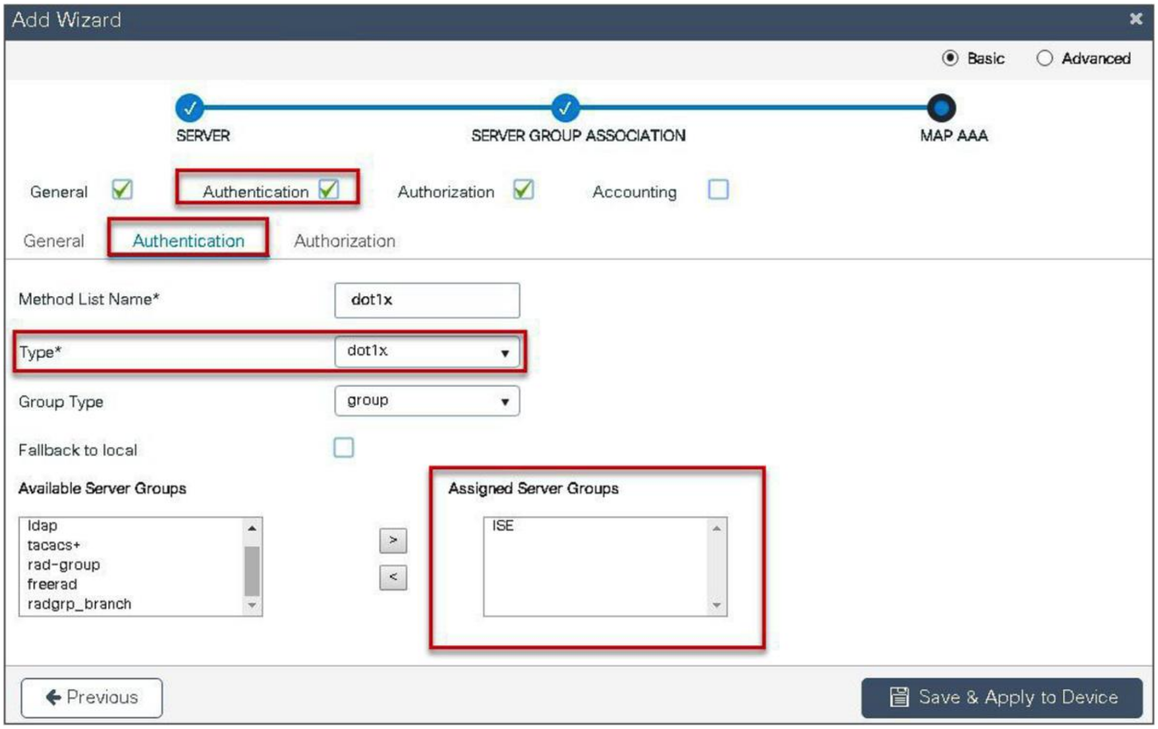
aaa_dot1x_system_auth_control: ENABLED

Local Authentication: Default

Local Authorization: Default

Radius Server Load Balance: DISABLED

Step 6. Checkmark the authentication list and define the method type as dot1x and map the server group.



Add Wizard

● Basic ○ Advanced

SERVER — SERVER GROUP ASSOCIATION — MAP AAA

General ☑ Authentication ☑ Authorization ☑ Accounting □

General | Authentication | Authorization

Method List Name*: dot1x

Type*: dot1x

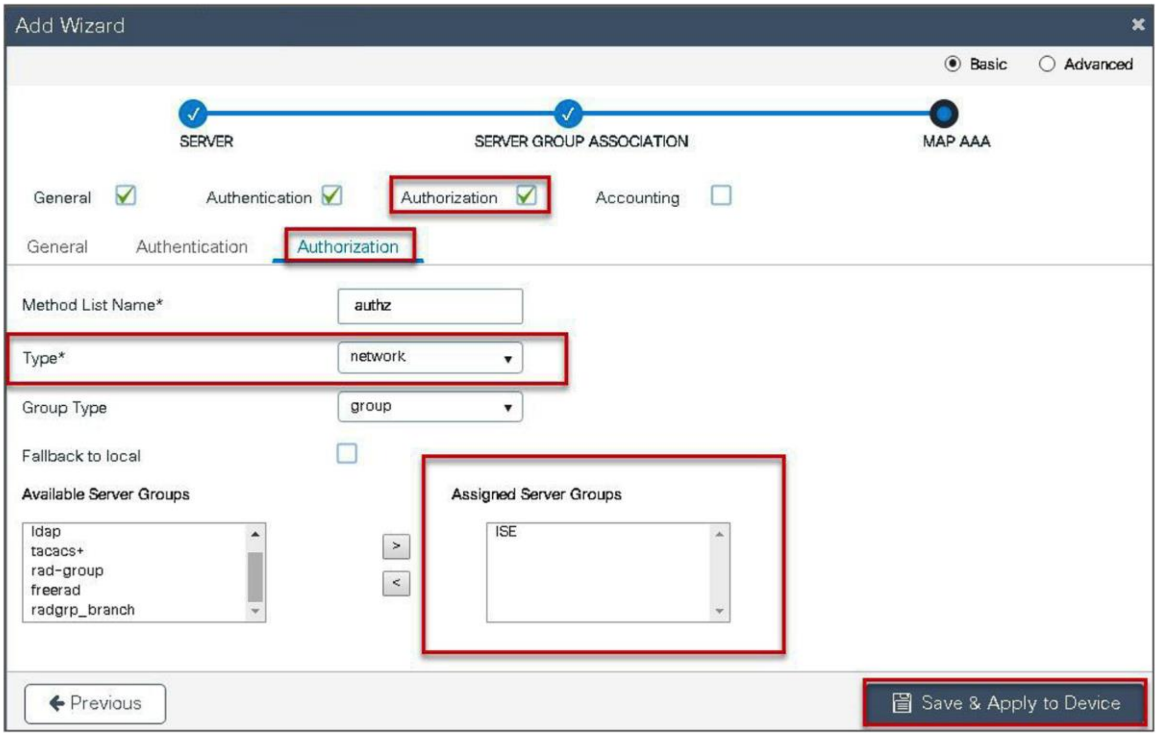
Group Type: group

Fallback to local: □

Available Server Groups: ldap, tacacs+, rad-group, freerad, radgrp_branch

Assigned Server Groups: ISE

Step 7. Checkmark the authorization list, define the method type as network, and map the server group.



Add Wizard

● Basic ○ Advanced

SERVER — SERVER GROUP ASSOCIATION — MAP AAA

General ☑ Authentication ☑ Authorization ☑ Accounting □

General | Authentication | Authorization

Method List Name*: authz

Type*: network

Group Type: group

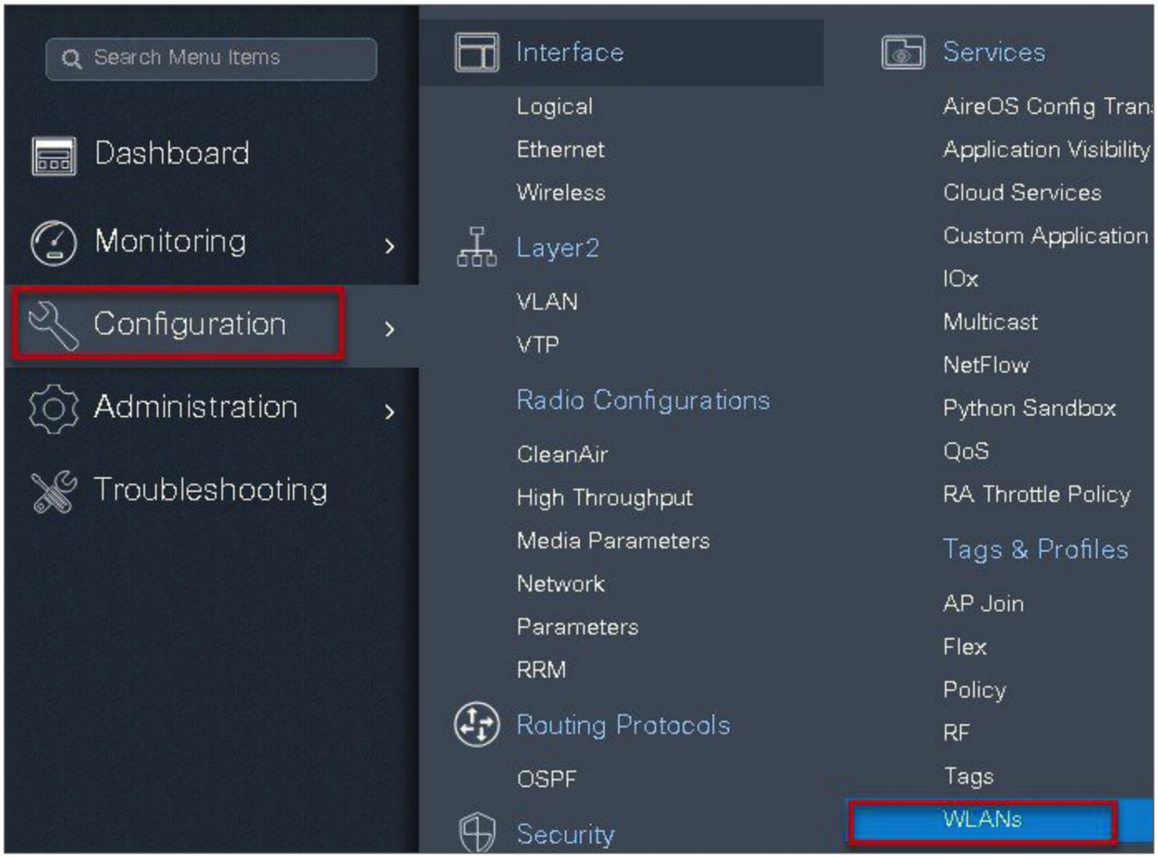
Fallback to local: □

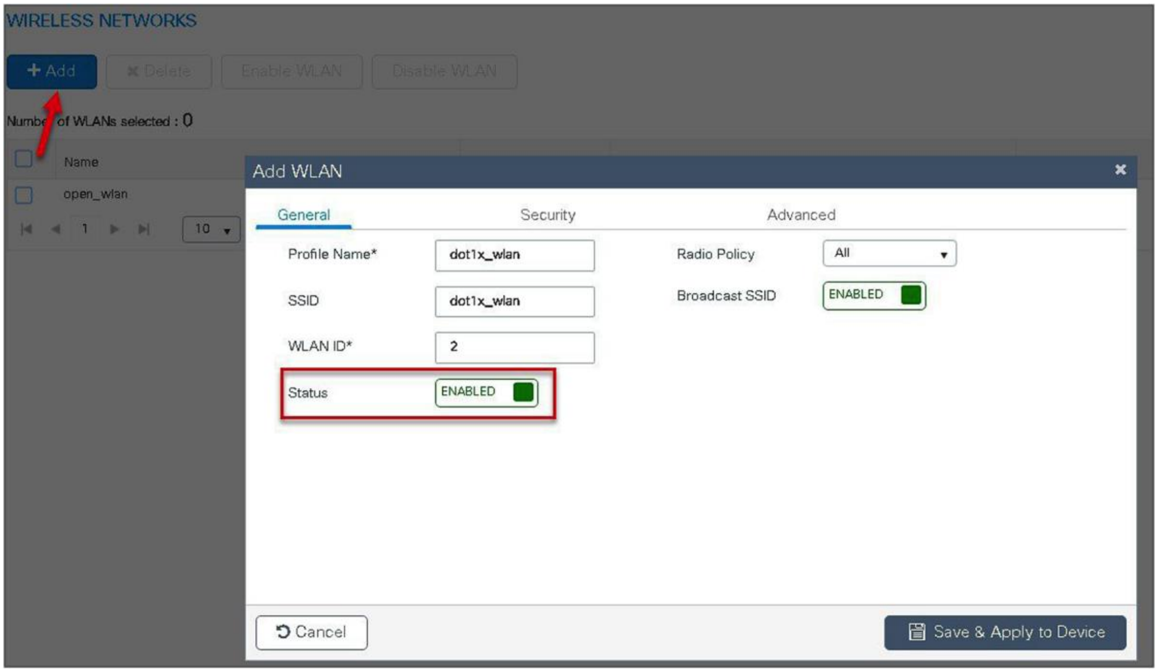
Available Server Groups: ldap, tacacs+, rad-group, freerad, radgrp_branch

Assigned Server Groups: ISE

Step 8. Create a dot1x WLAN and map the method list on the WLAN.

Navigate to Configuration > Tags & Profiles > WLAN to create the SSID.

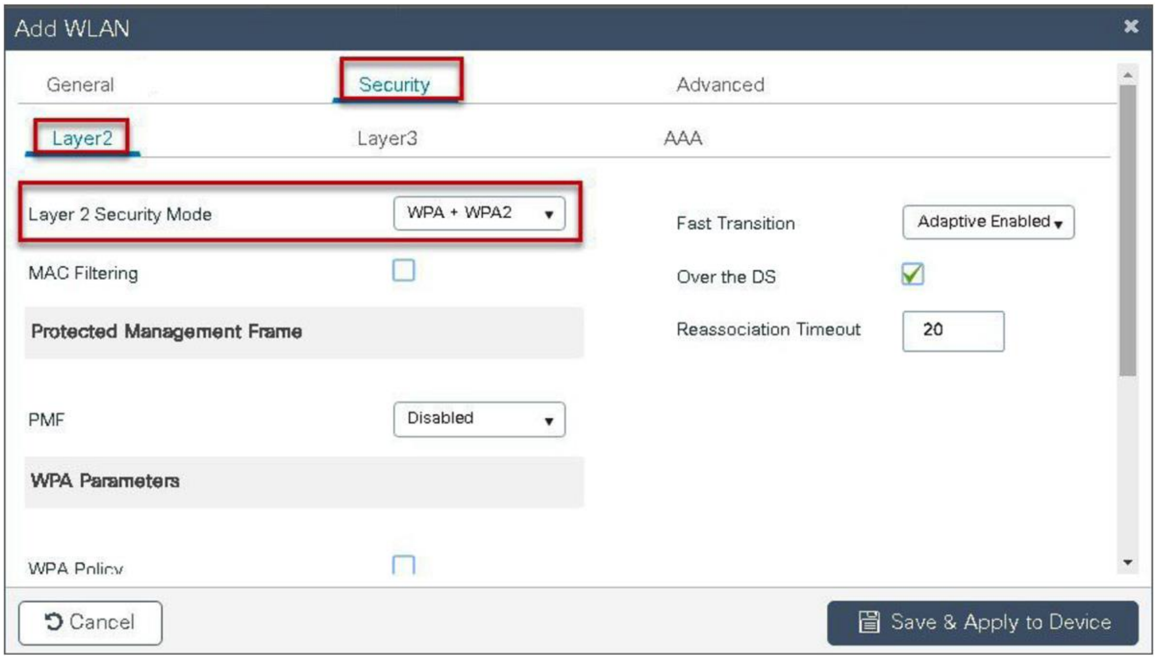




Number of WLANs selected : 0

Profile Name*	dot1x_wlan	Radio Policy	All
SSID	dot1x_wlan	Broadcast SSID	ENABLED
WLAN ID*	2		
Status	ENABLED		

Step 9. Define the security for the WLAN.



Layer 2 Security Mode: WPA + WPA2

MAC Filtering □

Protected Management Frame

PMF: Disabled

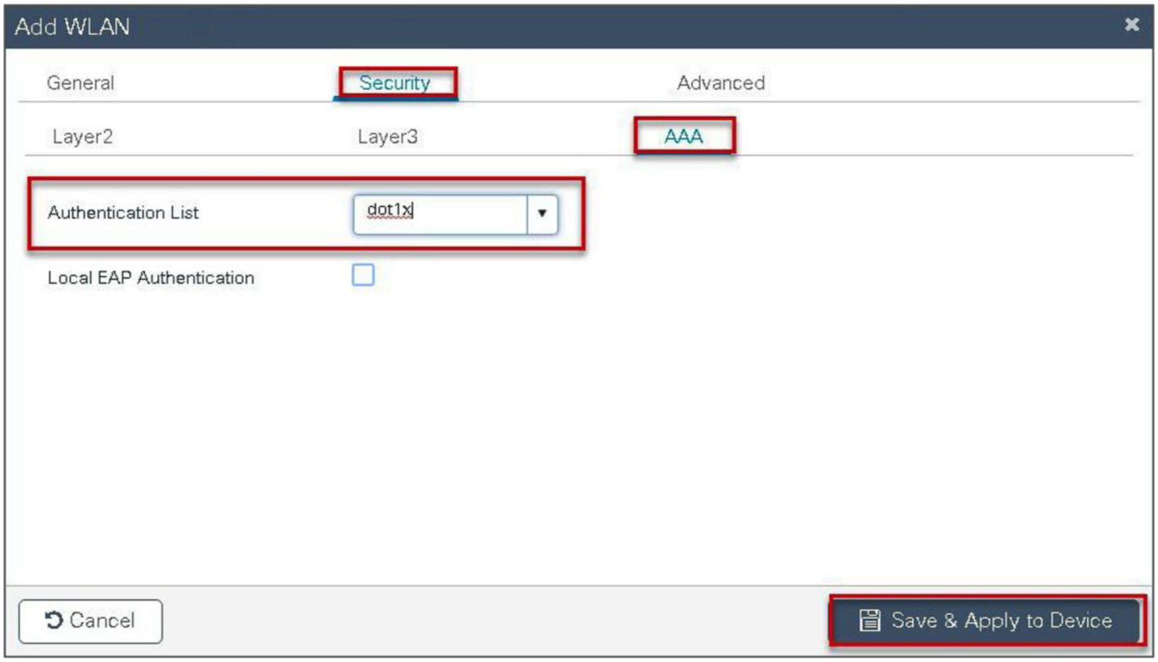
WPA Parameters

WPA Policy □

Fast Transition: Adaptive Enabled

Over the DS ☑

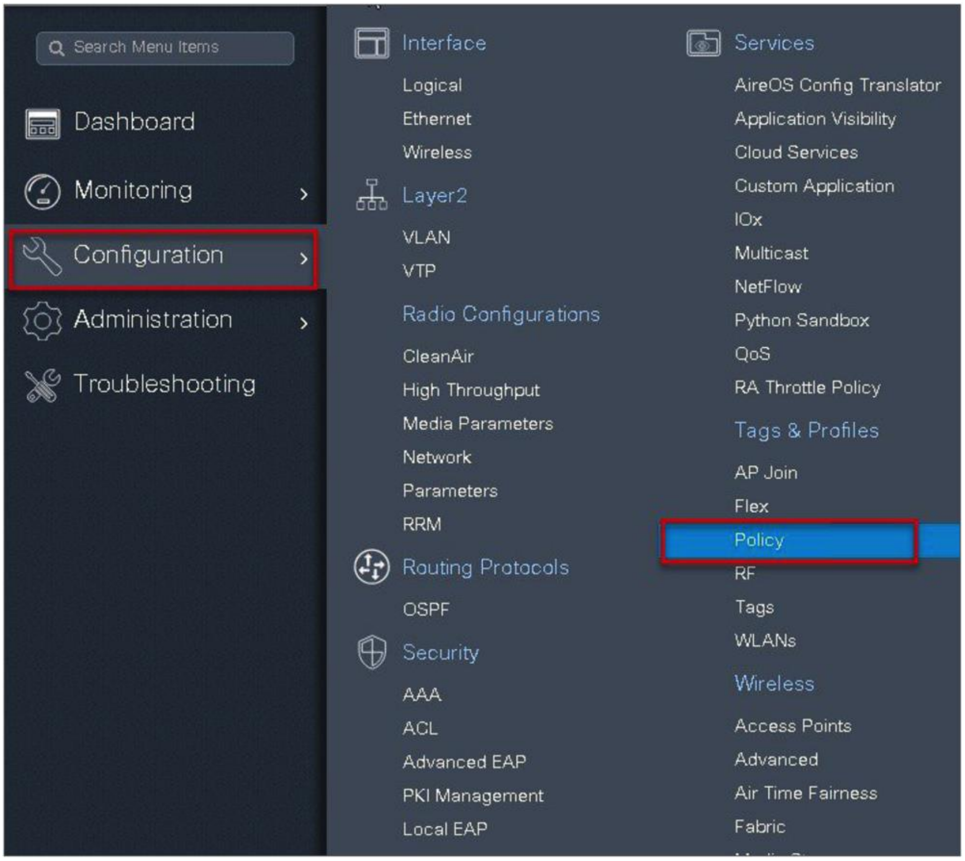
Reassociation Timeout: 20

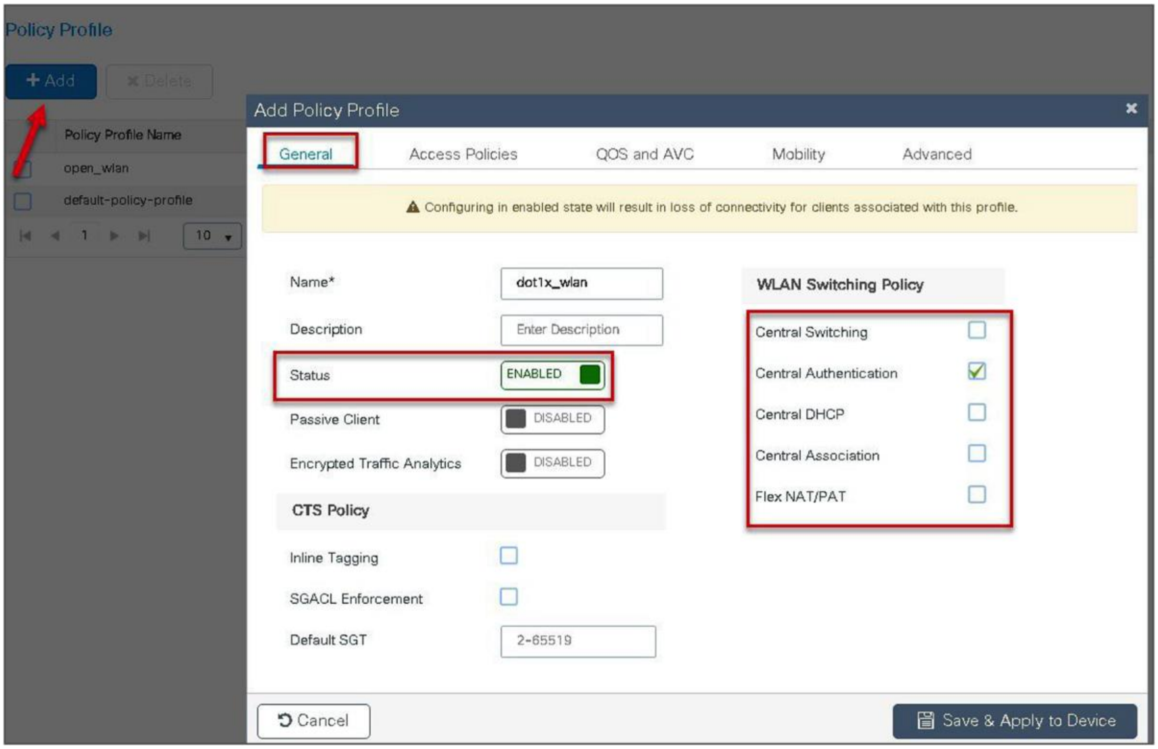


Authentication List: dot1x

Local EAP Authentication □

Step 10. Create a policy profile that defines the switching capability of the WLAN and the interface mapping to the WLAN.





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

Name*	dot1x_wlan
Description	Enter Description
Status	ENABLED
Passive Client	DISABLED
Encrypted Traffic Analytics	DISABLED

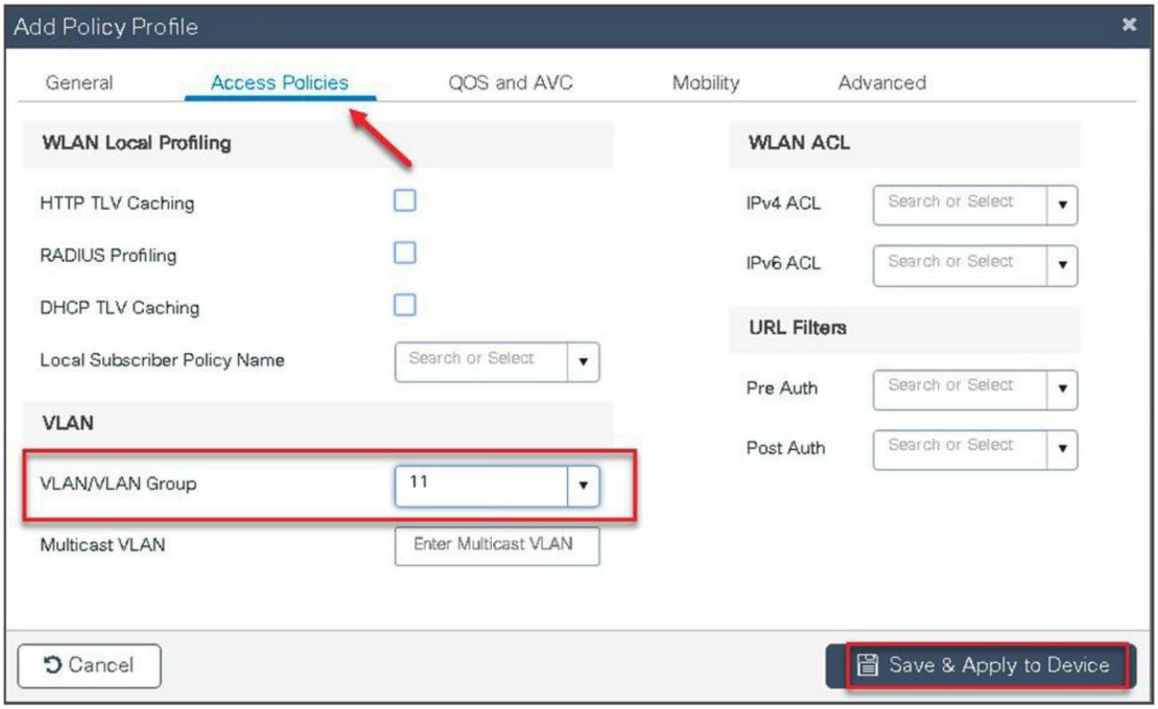
CTS Policy

Inline Tagging	□
SGACL Enforcement	□
Default SGT	2-65519

WLAN Switching Policy

Central Switching	□
Central Authentication	☑
Central DHCP	□
Central Association	□
Flex NAT/PAT	□

Step 11. Define the VLAN to be used by the SSID.



WLAN Local Profiling

HTTP TLV Caching ☐

RADIUS Profiling ☐

DHCP TLV Caching ☐

Local Subscriber Policy Name: Search or Select

VLAN

VLAN/VLAN Group: 11

Multicast VLAN: Enter Multicast VLAN

WLAN ACL

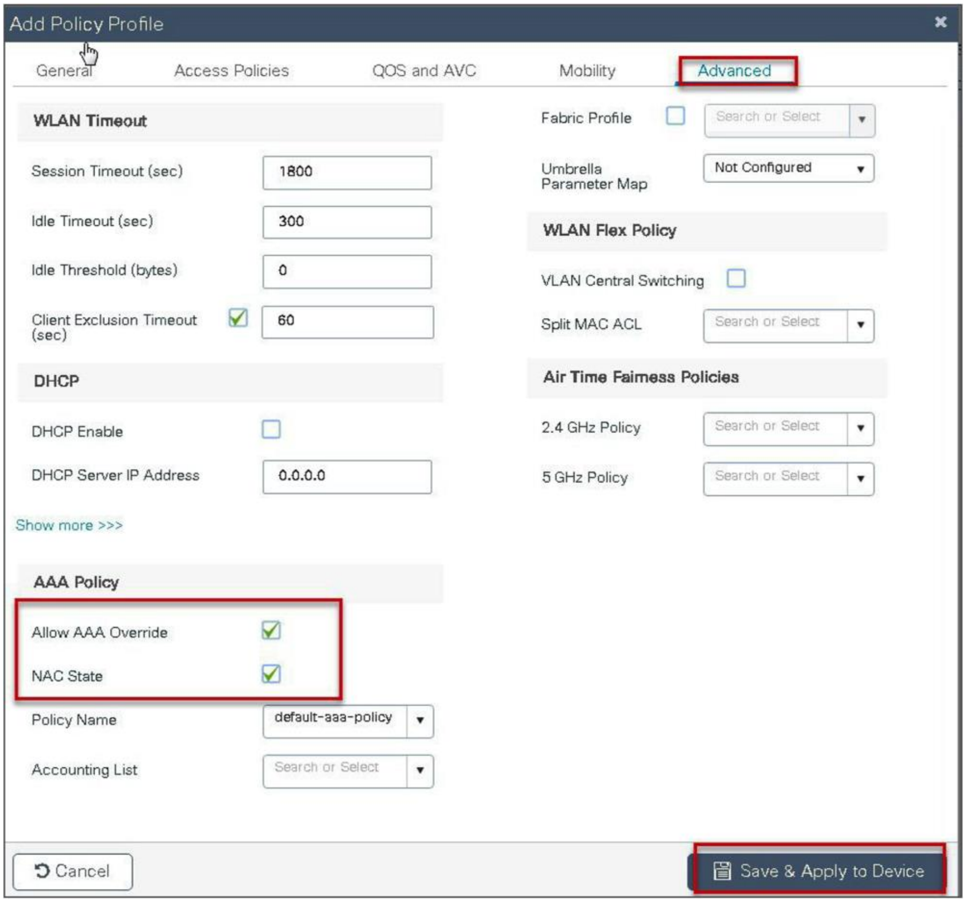
IPv4 ACL: Search or Select

IPv6 ACL: Search or Select

URL Filters

Pre Auth: Search or Select

Post Auth: Search or Select



WLAN Timeout

Session Timeout (sec): 1800

Idle Timeout (sec): 300

Idle Threshold (bytes): 0

Client Exclusion Timeout (sec): ☑ 60

DHCP

DHCP Enable ☐

DHCP Server IP Address: 0.0.0.0

AAA Policy

Allow AAA Override ☑

NAC State ☑

Policy Name: default-aaa-policy

Accounting List: Search or Select

Fabric Profile ☐ Search or Select

Umbrella Parameter Map: Not Configured

WLAN Flex Policy

VLAN Central Switching ☐

Split MAC ACL: Search or Select

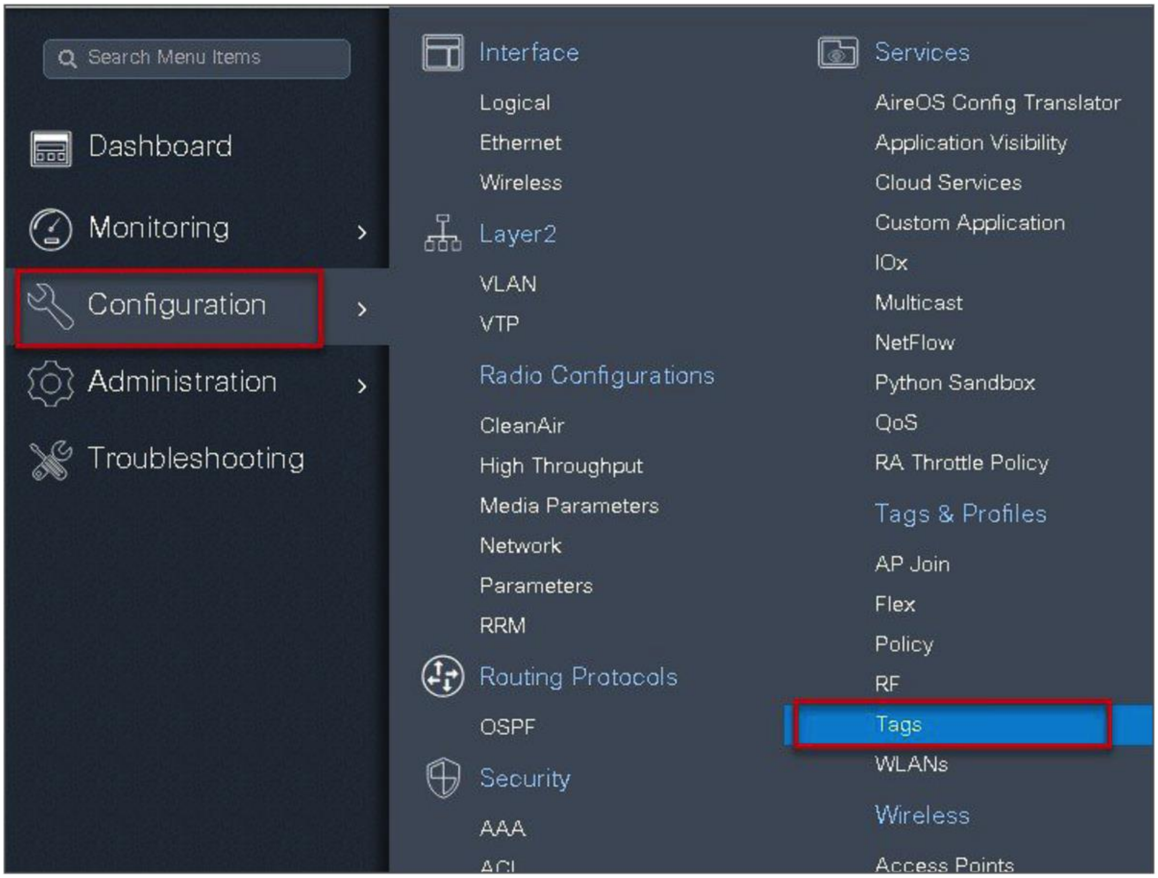
Air Time Fairness Policies

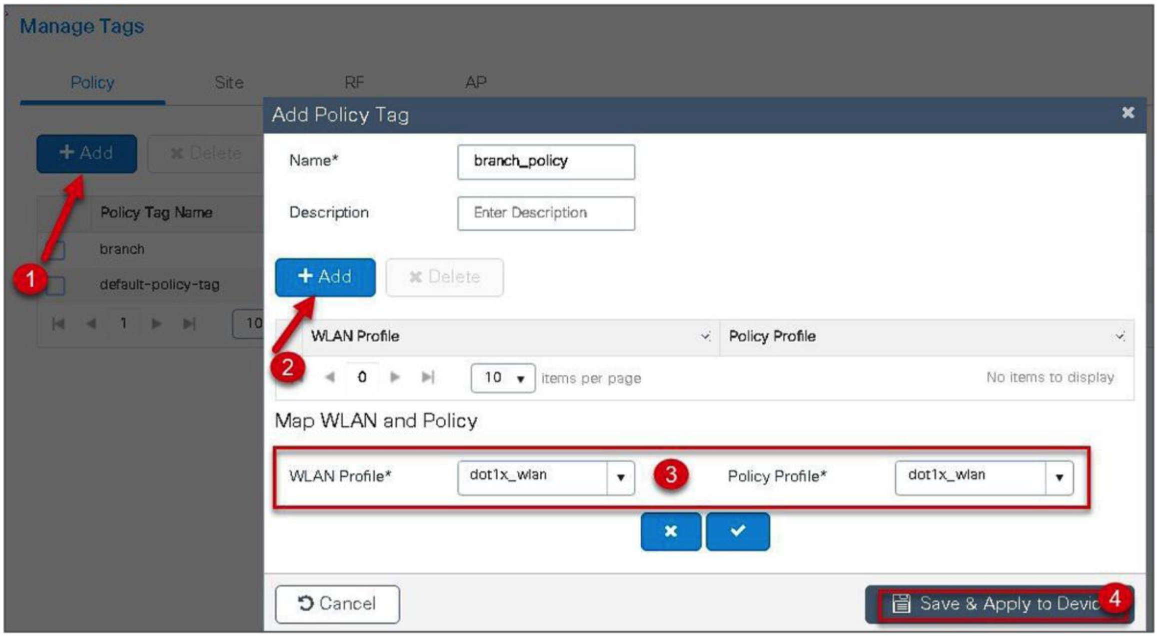
2.4 GHz Policy: Search or Select

5 GHz Policy: Search or Select

Step 12. Create a policy tag that bundles the policy profile and WLAN profile together.

Navigate to Configuration > Tag and create a policy tag mapping the WLAN and policy profile.





Add Policy Tag

Name* branch_policy

Description Enter Description

WLAN Profile	Policy Profile

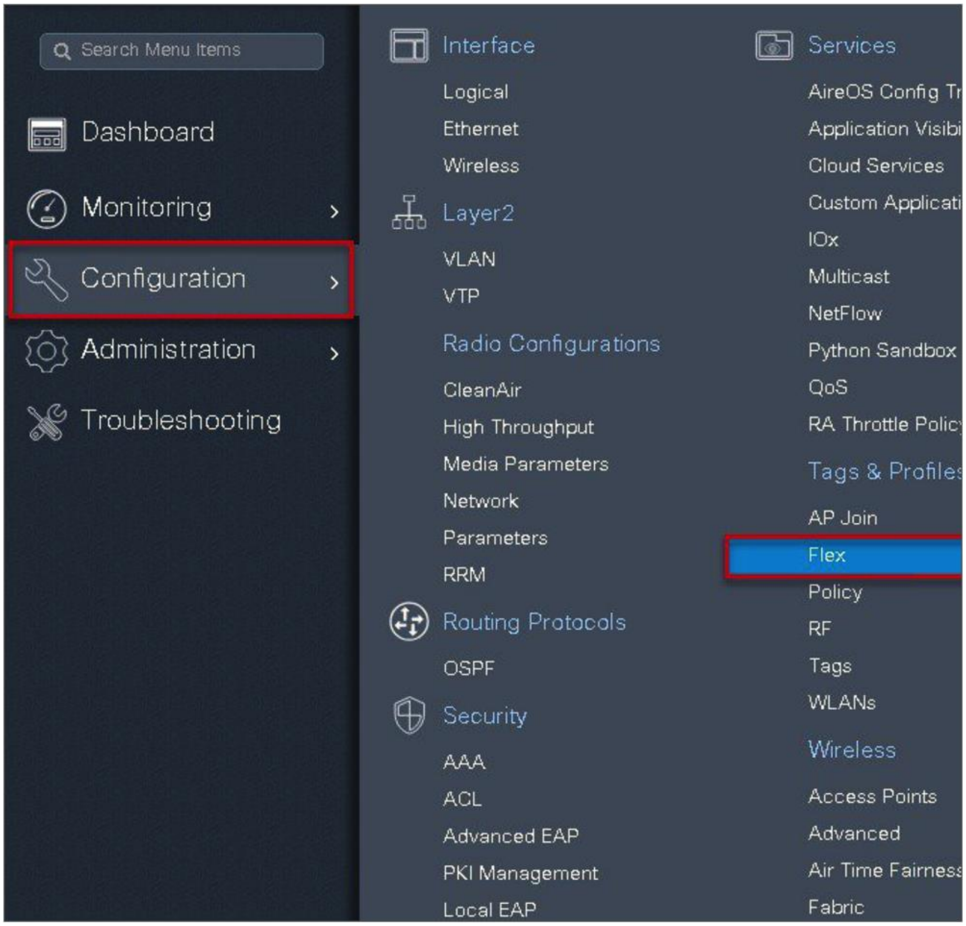
0 10 items per page No items to display

Map WLAN and Policy

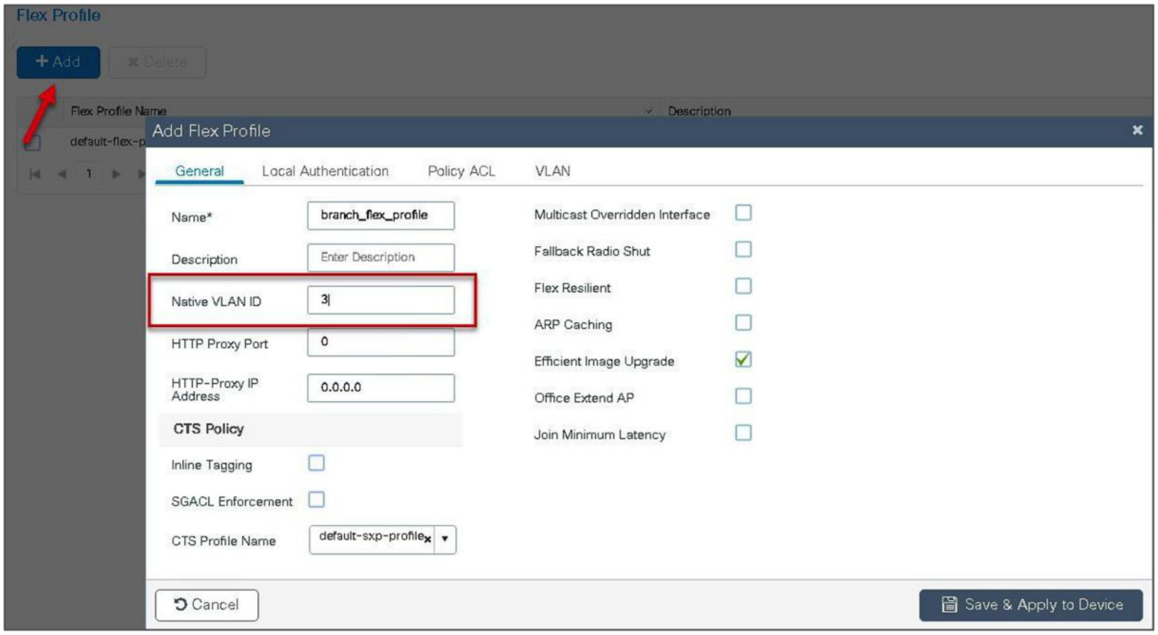
WLAN Profile* dot1x_wlan Policy Profile* dot1x_wlan

Step 13. Create a flex profile that defines the flex AP properties.

To create a flex profile, navigate to Configuration > Tags and Profile > Flex.



Step 14. Define the native VLAN for the FlexConnect AP.



Name*: branch_flex_profile

Description: Enter Description

Native VLAN ID: 3

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 ☐

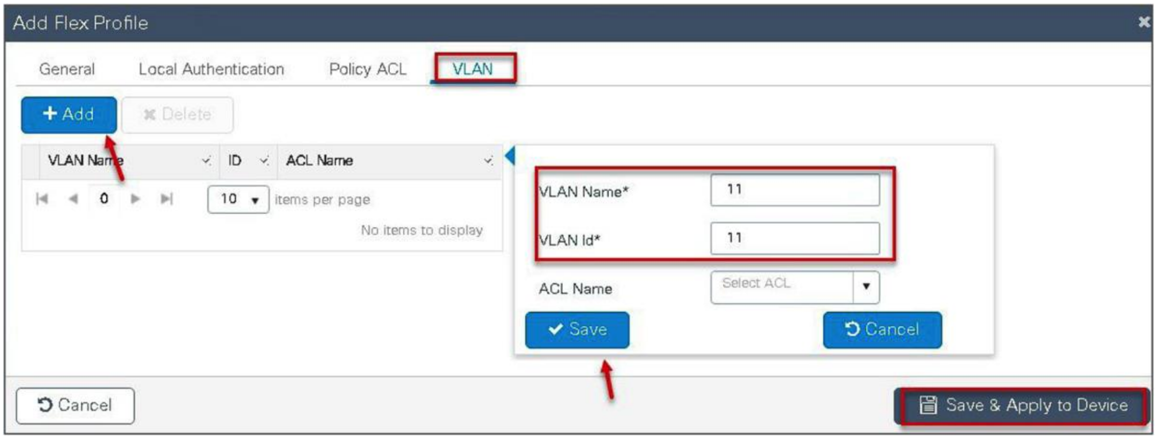
ARP Caching ☐

Efficient Image Upgrade ☑

Office Extend AP ☐

Join Minimum Latency ☐

Step 15. Define the VLANS to be used for local-switched SSID. In this example, we use VLAN 11, which is the local-switched VLAN from the AP.



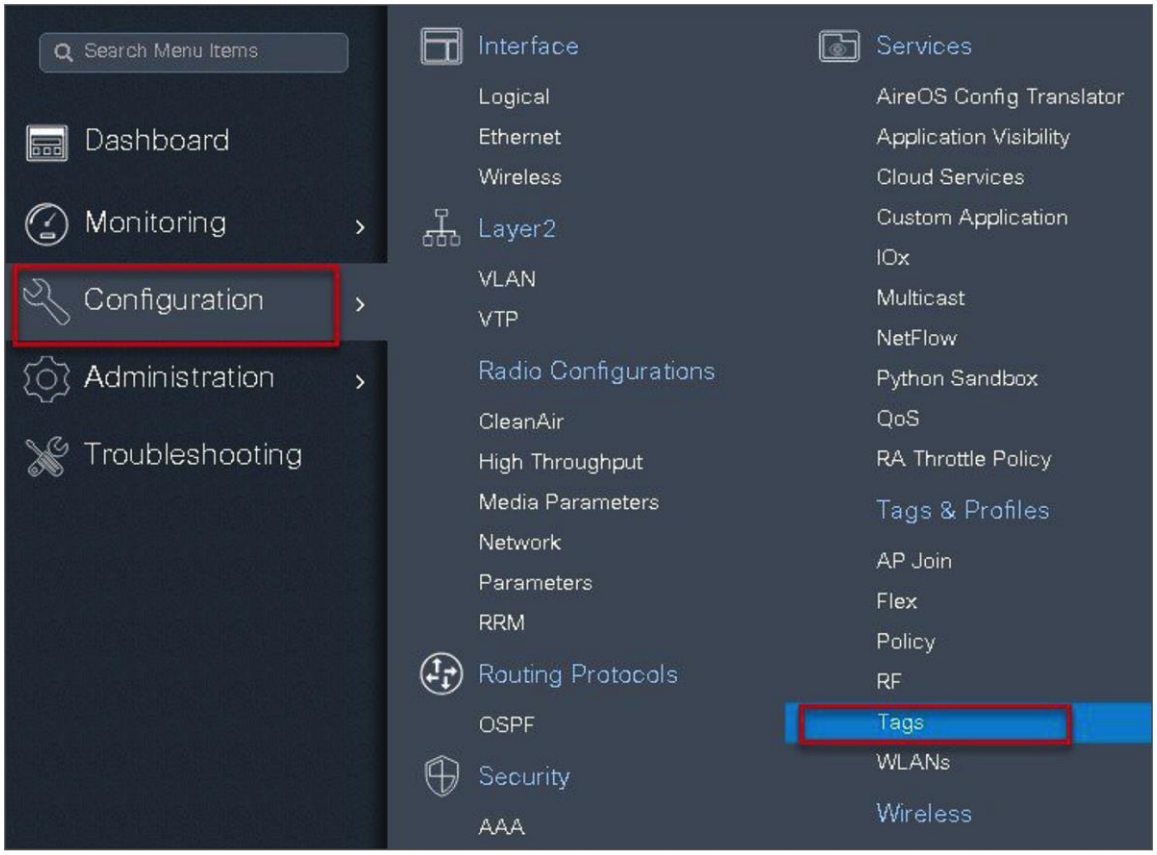
VLAN Name* 11

VLAN Id* 11

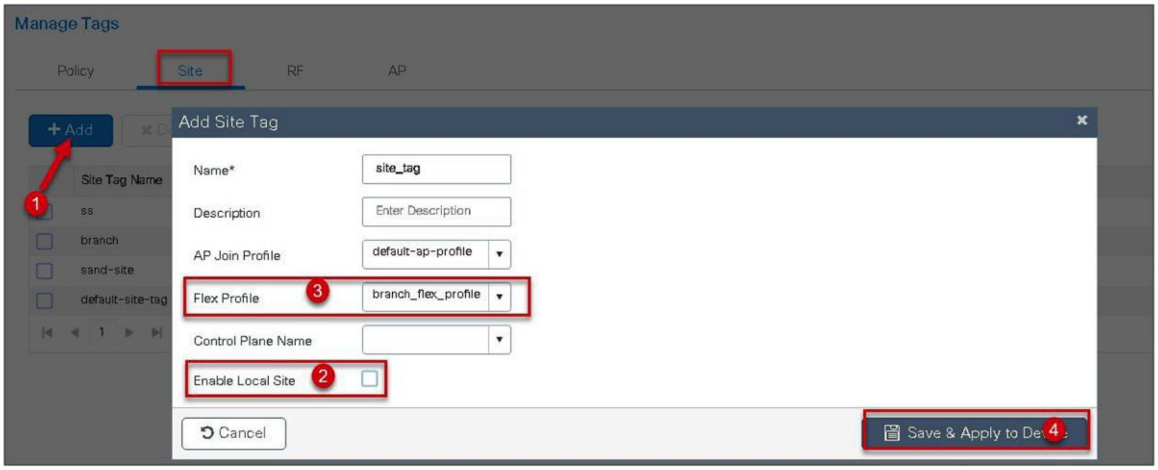
ACL Name Select ACL

Step 16. Create a site tag that maps the flex and RF profile.

To create a site tag, navigate to Configuration > Tags and Profile > Tags.



Step 17. Uncheck “Enable Local Site” to map the flex profile on the site tag.



Add Site Tag

Name* site_tag

Description Enter Description

AP Join Profile default-ap-profile

Flex Profile branch_flex_profile

Control Plane Name

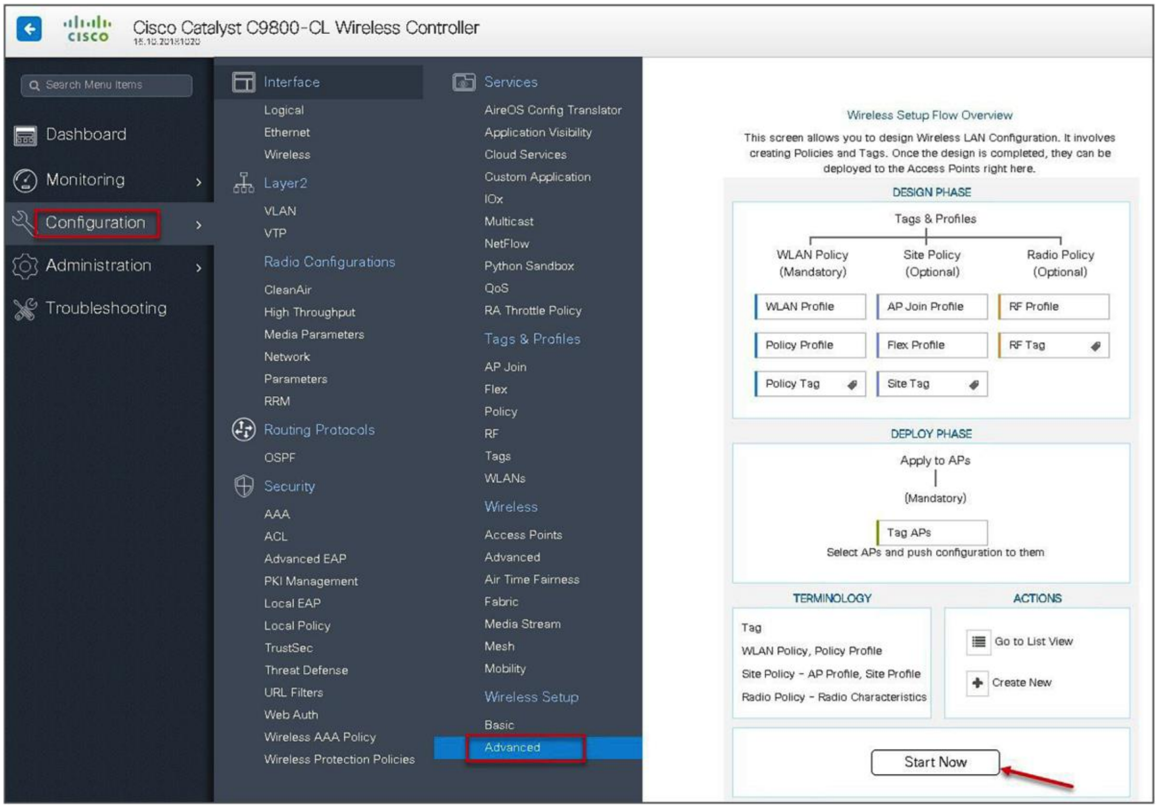
Enable Local Site □

Step 18. Map the policy site tag and RF tag on the AP. To tag the AP, an administrator can use the following options.

- Use the advanced config wizard
- Use a static mapping
- Use a filter

Using the advanced config wizard to tag the APs:

Navigate to Configuration > Wireless Setup > Advanced.



Wireless Setup Flow Overview

This screen allows you to design Wireless LAN Configuration. It involves creating Policies and Tags. Once the design is completed, they can be deployed to the Access Points right here.

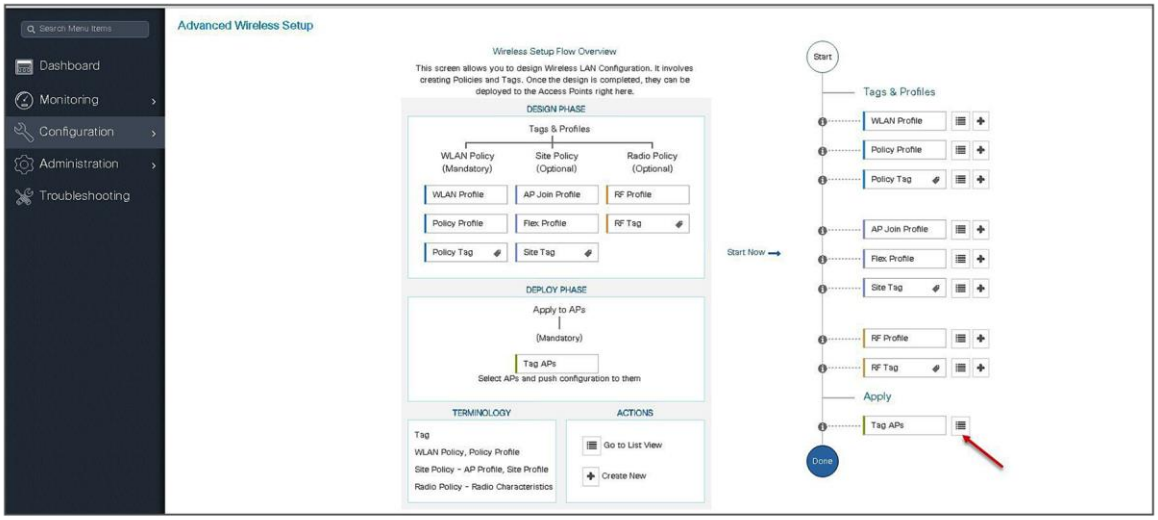
Select APs and push configuration to them

Tag

WLAN Policy, Policy Profile

Site Policy - AP Profile, Site Profile

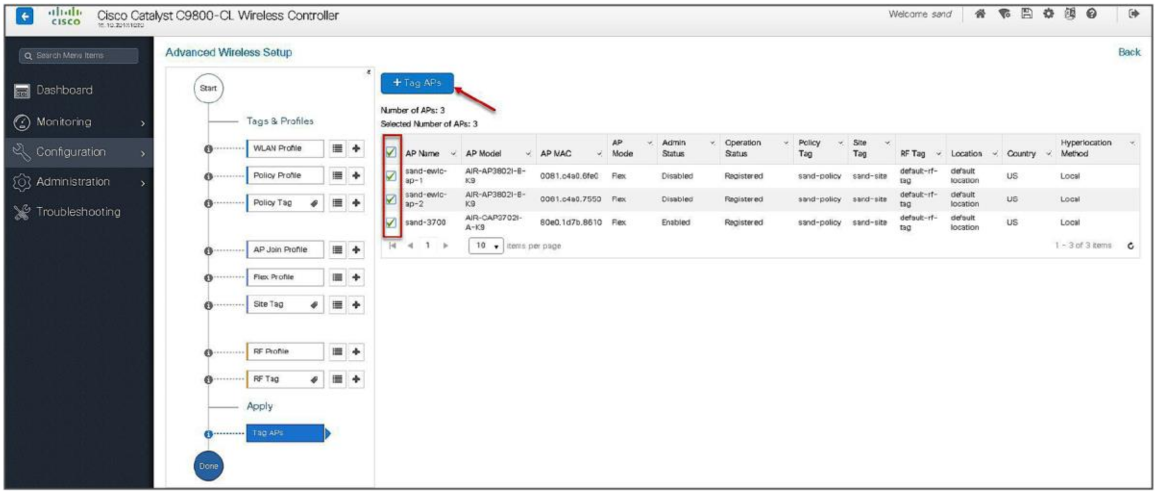
Radio Policy - Radio Characteristics



This screen allows you to design Wireless LAN Configuration. It involves creating Policies and Tags. Once the design is completed, they can be deployed to the Access Points right here.

Select APs and push configuration to them

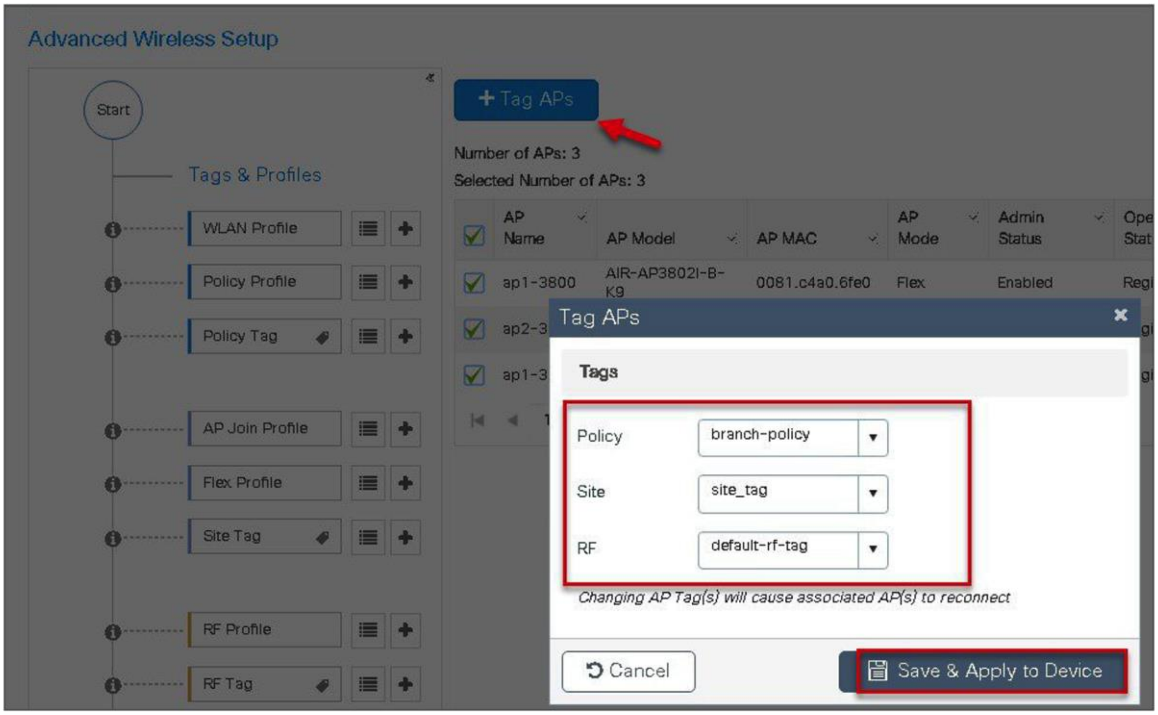
Tag
WLAN Policy, Policy Profile
Site Policy - AP Profile, Site Profile
Radio Policy - Radio Characteristics



Number of APs: 3
Selected Number of APs: 3

☑	AP Name	AP Model	AP MAC	AP Mode	Admin Status	Operation Status	Policy Tag	Site Tag	RF Tag	Location	Country	Hyperlocation Method
☑	sand-ewlc-ap-1	AIR-AP3802I-B-K9	0081.c4a0.6fe0	Flex	Disabled	Registered	sand-policy	sand-site	default-rf-tag	default location	US	Local
☑	sand-ewlc-ap-2	AIR-AP3802I-B-K9	0081.c4a0.7550	Flex	Disabled	Registered	sand-policy	sand-site	default-rf-tag	default location	US	Local
☑	sand-3700	AIR-CAP3702I-A-K9	80e0.1d7b.8610	Flex	Enabled	Registered	sand-policy	sand-site	default-rf-tag	default location	US	Local

1 · 10 items per page · 1 - 3 of 3 items



Advanced Wireless Setup

Number of APs: 3

Selected Number of APs: 3

☑	AP Name	AP Model	AP MAC	AP Mode	Admin Status	Ope Stat
☑	ap1-3800	AIR-AP3802I-B-K9	0081.c4a0.6fe0	Flex	Enabled	Regi
☑	ap2-3					
☑	ap1-3					

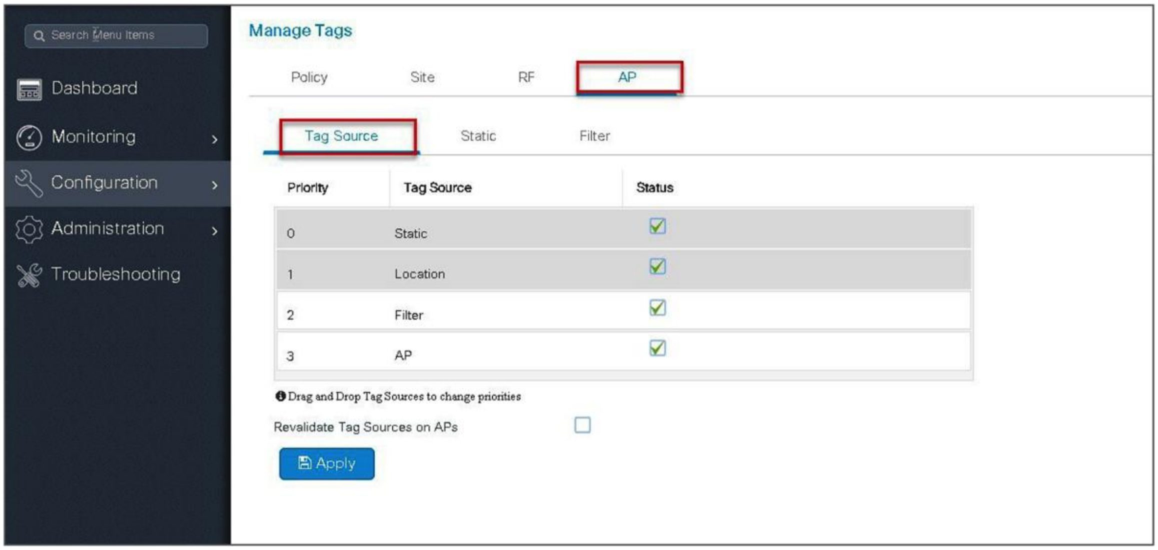
Tag APs

Tags

Policy	branch-policy
Site	site_tag
RF	default-rf-tag

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

Using a static mapping to tag the APs.



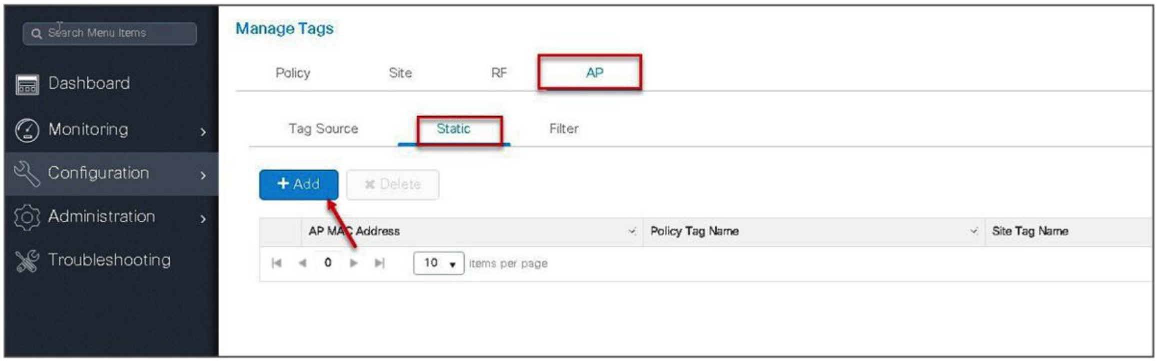
Manage Tags

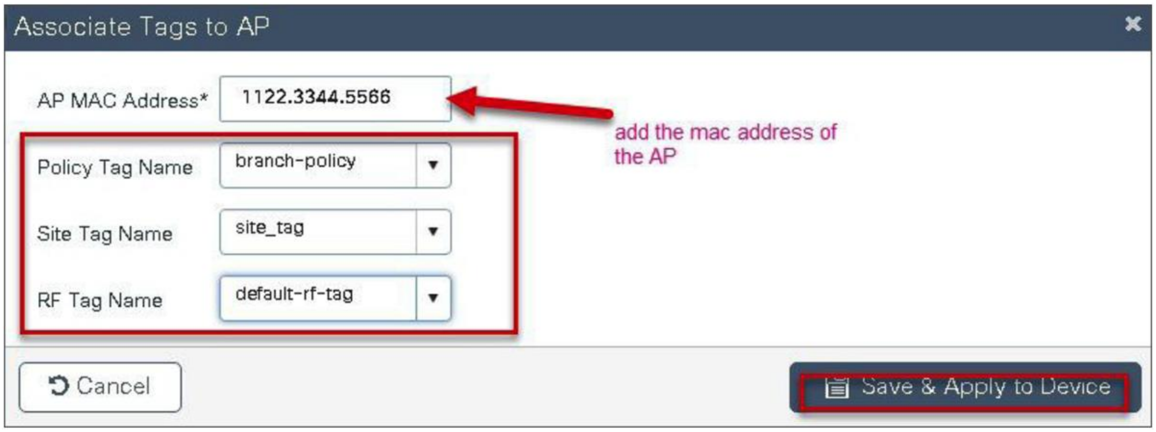
Priority	Tag Source	Status
0	Static	☑
1	Location	☑
2	Filter	☑
3	AP	☑

Drag and Drop Tag Sources to change priorities

Revalidate Tag Sources on APs ☐

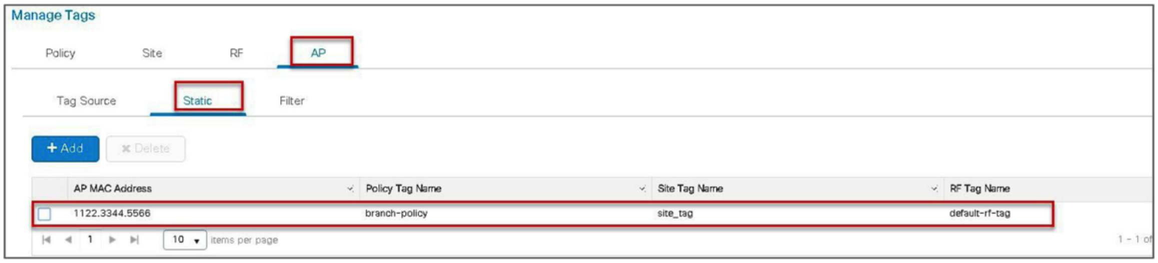
Static mapping – In the static mapping, the administrator needs to specify the MAC address of the AP along with the site, policy, and RF tag.





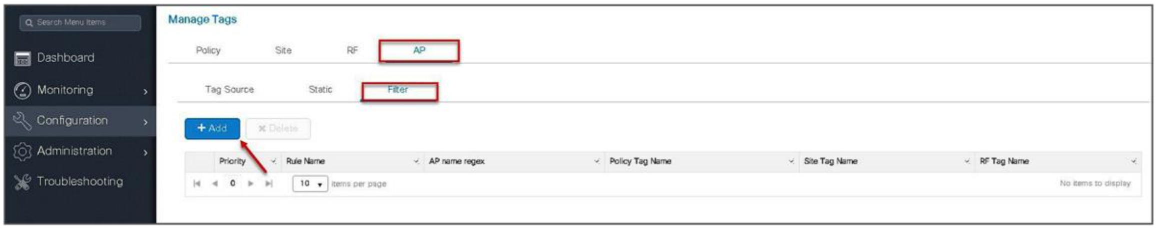
AP MAC Address*	1122.3344.5566
Policy Tag Name	branch-policy
Site Tag Name	site_tag
RF Tag Name	default-rf-tag

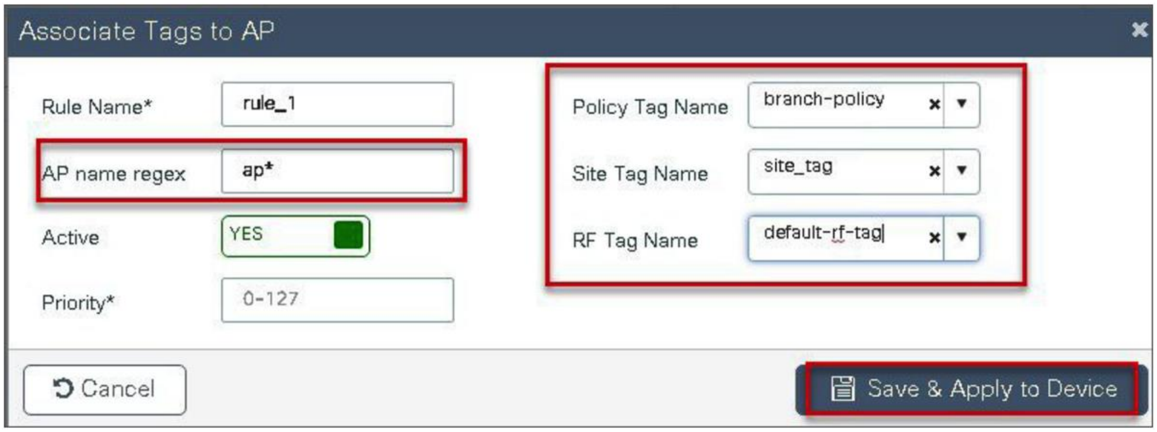
add the mac address of the AP



AP MAC Address	Policy Tag Name	Site Tag Name	RF Tag Name
□ 1122.3344.5566	branch-policy	site_tag	default-rf-tag

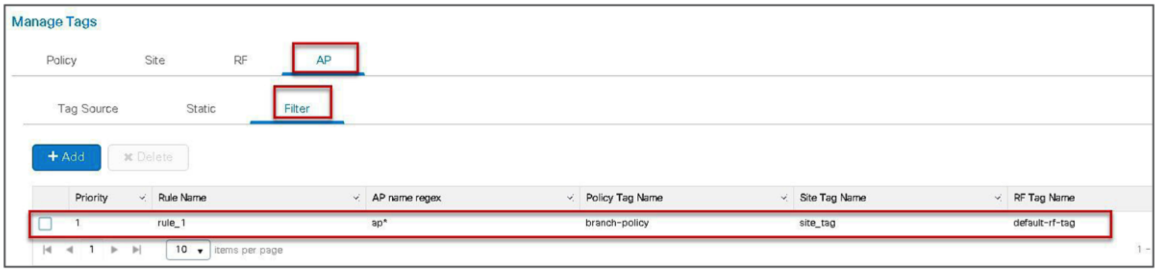
Using a filter to tag the AP:





Associate Tags to AP

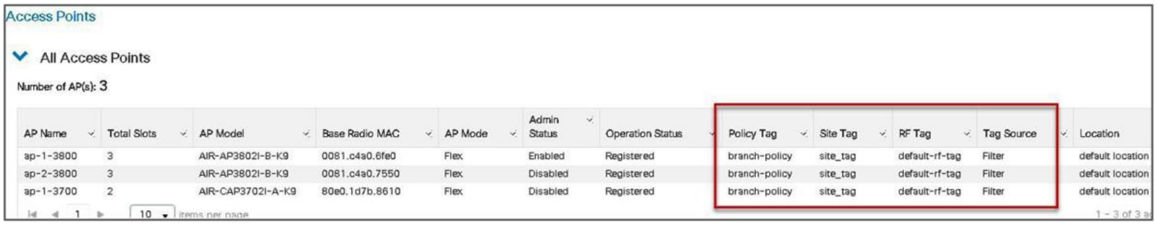
Rule Name*	rule_1	Policy Tag Name	branch-policy
AP name regex	ap*	Site Tag Name	site_tag
Active	YES	RF Tag Name	default-rf-tag
Priority*	0-127		



Manage Tags

	Priority	Rule Name	AP name regex	Policy Tag Name	Site Tag Name	RF Tag Name
□	1	rule_1	ap*	branch-policy	site_tag	default-rf-tag

The access point summary page shows the source based on which tags were assigned to an AP.



Access Points

All Access Points

Number of AP(s): 3

AP Name	Total Slots	AP Model	Base Radio MAC	AP Mode	Admin Status	Operation Status	Policy Tag	Site Tag	RF Tag	Tag Source	Location
ap-1-3800	3	AIR-AP3802I-B-K9	0081.c4a0.6fe0	Flex	Enabled	Registered	branch-policy	site_tag	default-rf-tag	Filter	default location
ap-2-3800	3	AIR-AP3802I-B-K9	0081.c4a0.7550	Flex	Disabled	Registered	branch-policy	site_tag	default-rf-tag	Filter	default location
ap-1-3700	2	AIR-CAP3702I-A-K9	80e0.1d7b.8610	Flex	Disabled	Registered	branch-policy	site_tag	default-rf-tag	Filter	default location

Once the AP is provisioned with the site tag, the AP gets converted to flex mode based on the site tag assigned to the AP.

If the AP is already in flex mode, there is no conversion. If the AP is in local mode, AP would reboot to boot in FlexConnect mode.

The assigning of the tag does the auto-conversion of the AP mode based on properties of the tag.

FlexConnect VLAN override

AAA override of VLAN on individual WLAN is supported for local switching. In order to have a dynamic VLAN assignment, the AP would have the VLAN pre-created based on a configuration using the flex profile mapped to the site tag. The VLANs used in the flex profile are pushed to the AP, and overriding of the WLAN is done using the VLAN the AP is programmed to.

Summary

- AAA VLAN override is supported on WLANs configured for local switching in central and local authentication mode.
- AAA override should be enabled on the policy profile mapped to the WLAN.
- The FlexConnect AP should have VLAN pre-created from WLC. This is done in the flex profile mapped to the site tag.
- If VLANs returned by the AAA override are not present on the AP, the client will be excluded and not allowed access to the network.
- Multicast traffic on an AAA-overridden VLAN is not supported.

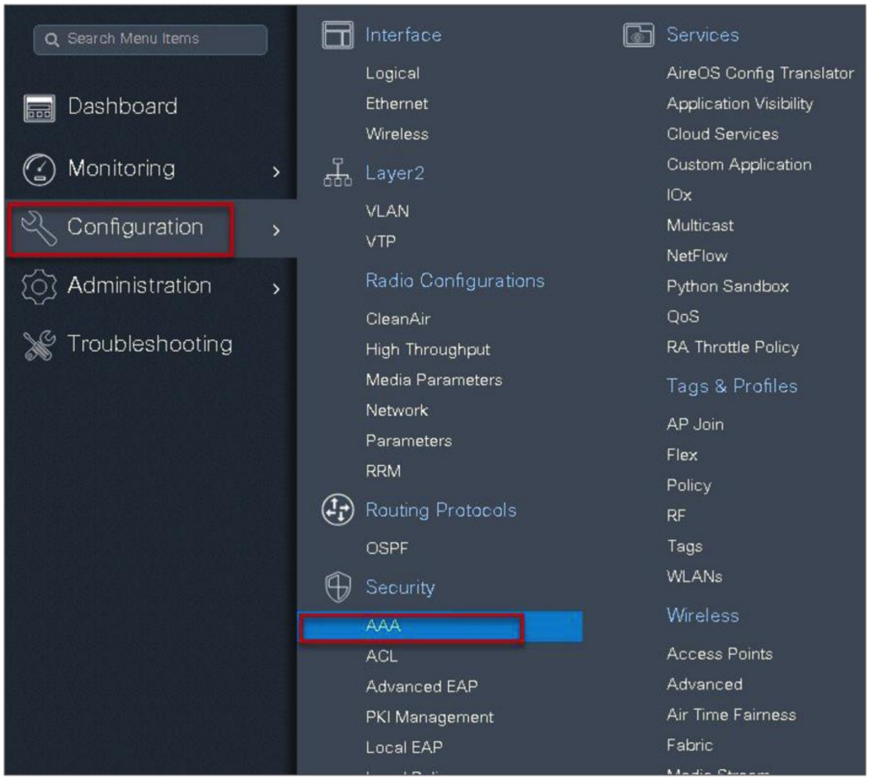
Procedure to enable VLAN

The procedure to enable VLAN override is outlined below along with the GUI configuration. The WLAN here is enabled for dot1x-based authentication.

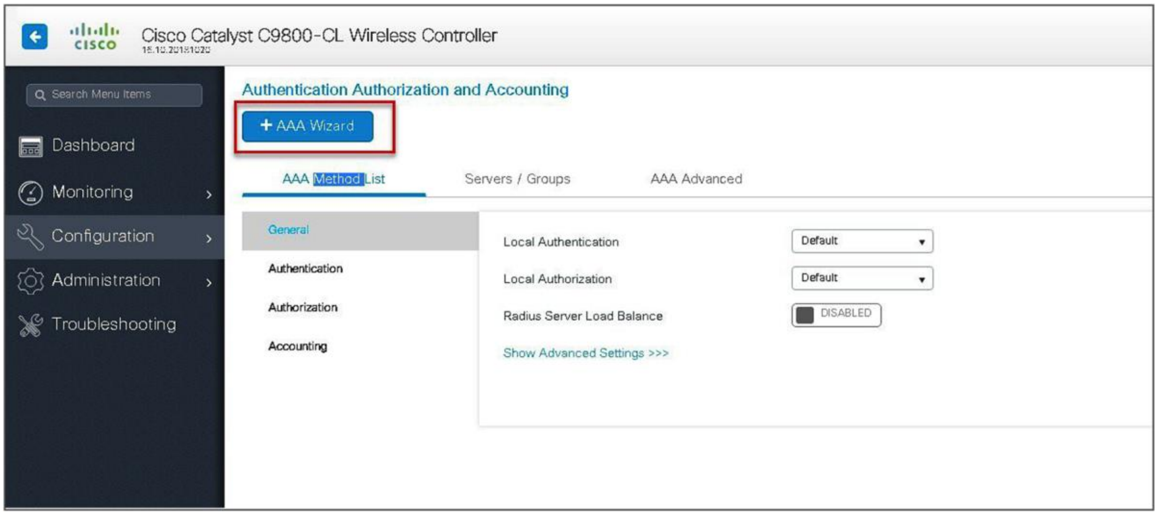
Procedure

Step 1. Define an AAA server and method list for dot1x, which is mapped to the WLAN. The AAA server is created by navigating to the following:

Configuration > Security > AAA

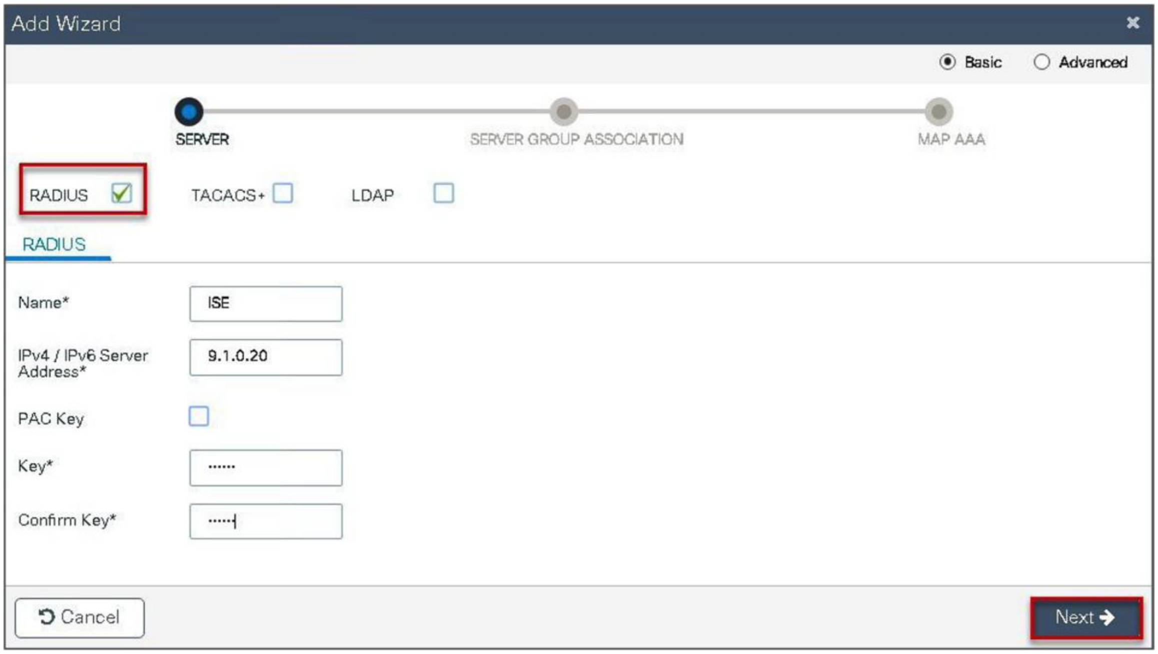


Step 2. Use the AAA wizard to create the server and server groups.



Local Authentication	Default
Local Authorization	Default
Radius Server Load Balance	DISABLED

Step 3. Define a name for the server and specify the IP address and shared secret.

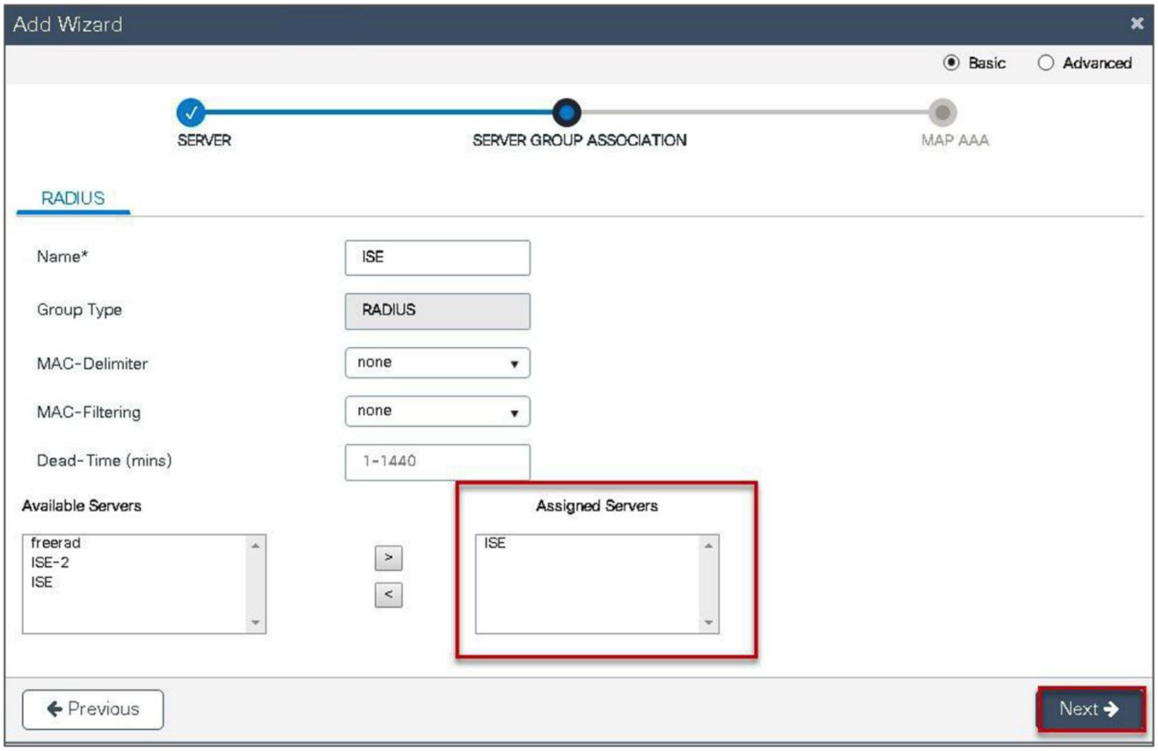


● Basic ○ Advanced

RADIUS ☑ TACACS+ □ LDAP □

Name*	ISE
IPv4 / IPv6 Server Address*	9.1.0.20
PAC Key	□
Key*	••••••
Confirm Key*	••••••

Step 4. Create a server group and map the server in the group.



Name* ISE

Group Type RADIUS

MAC-Delimiter none

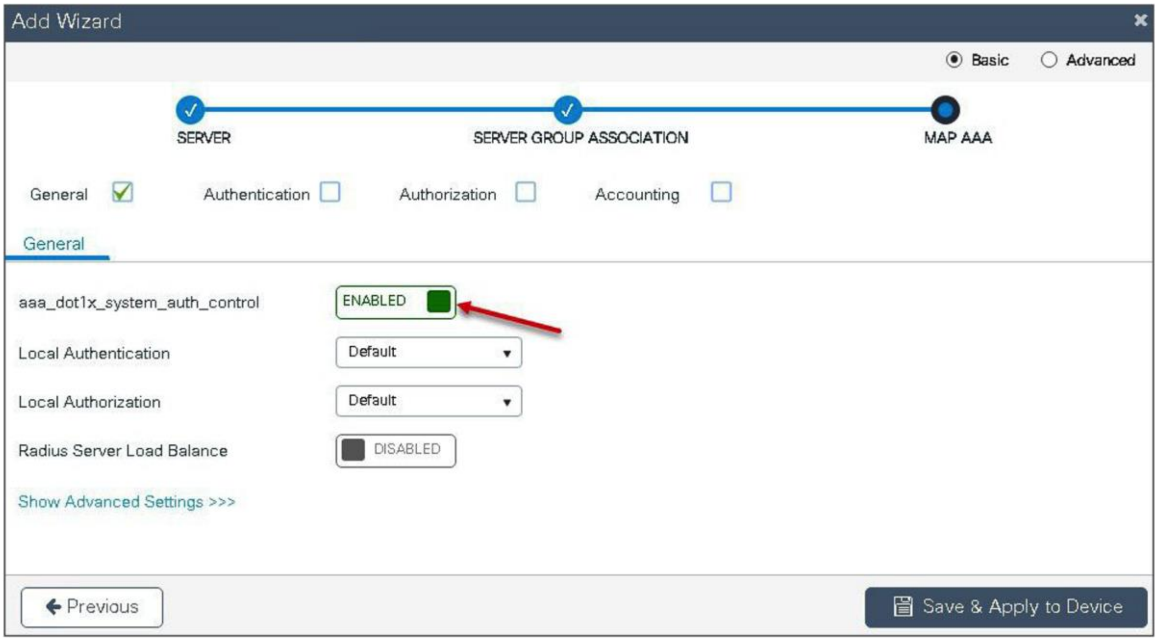
MAC-Filtering none

Dead-Time (mins) 1-1440

Available Servers: freerad, ISE-2, ISE

Assigned Servers: ISE

Step 5. Enable dot1x system control and checkmark the authentication and authorization profile.



General ☑ Authentication □ Authorization □ Accounting □

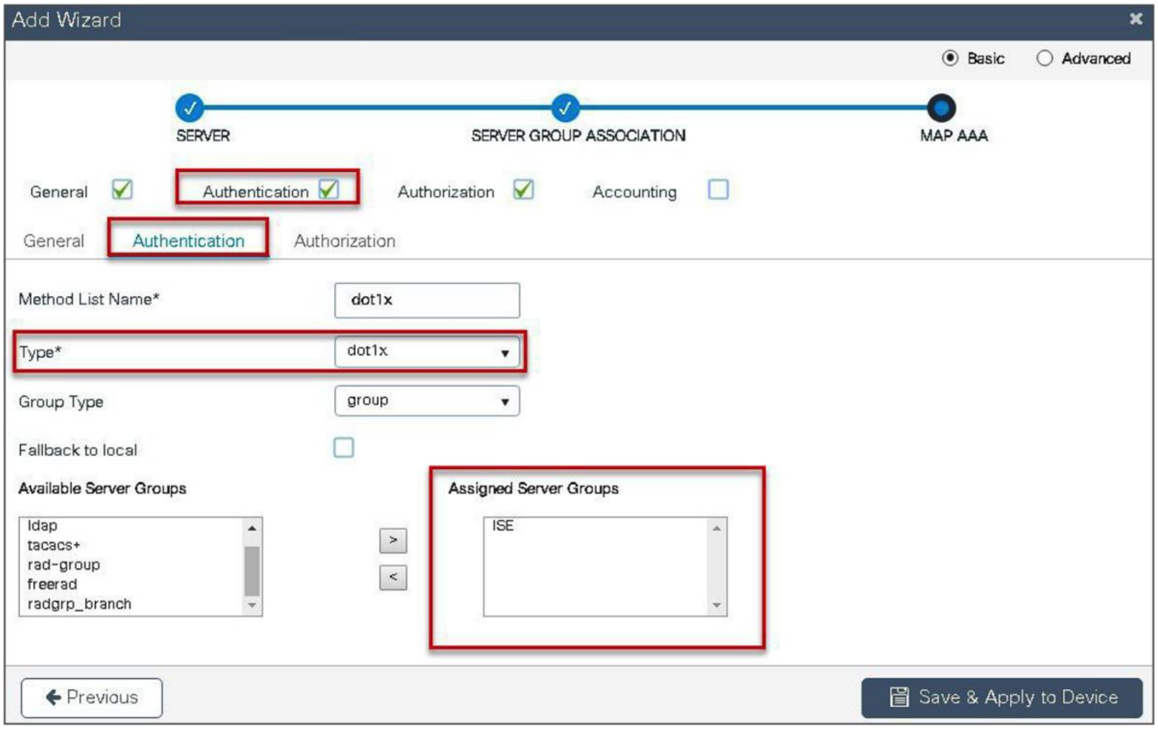
aaa_dot1x_system_auth_control ENABLED

Local Authentication Default

Local Authorization Default

Radius Server Load Balance DISABLED

Step 6. Define the method type as dot1x and map the server group.



Add Wizard

● Basic ○ Advanced

SERVER — SERVER GROUP ASSOCIATION — MAP AAA

General ☑ Authentication ☑ Authorization ☑ Accounting □

General | Authentication | Authorization

Method List Name*: dot1x

Type*: dot1x

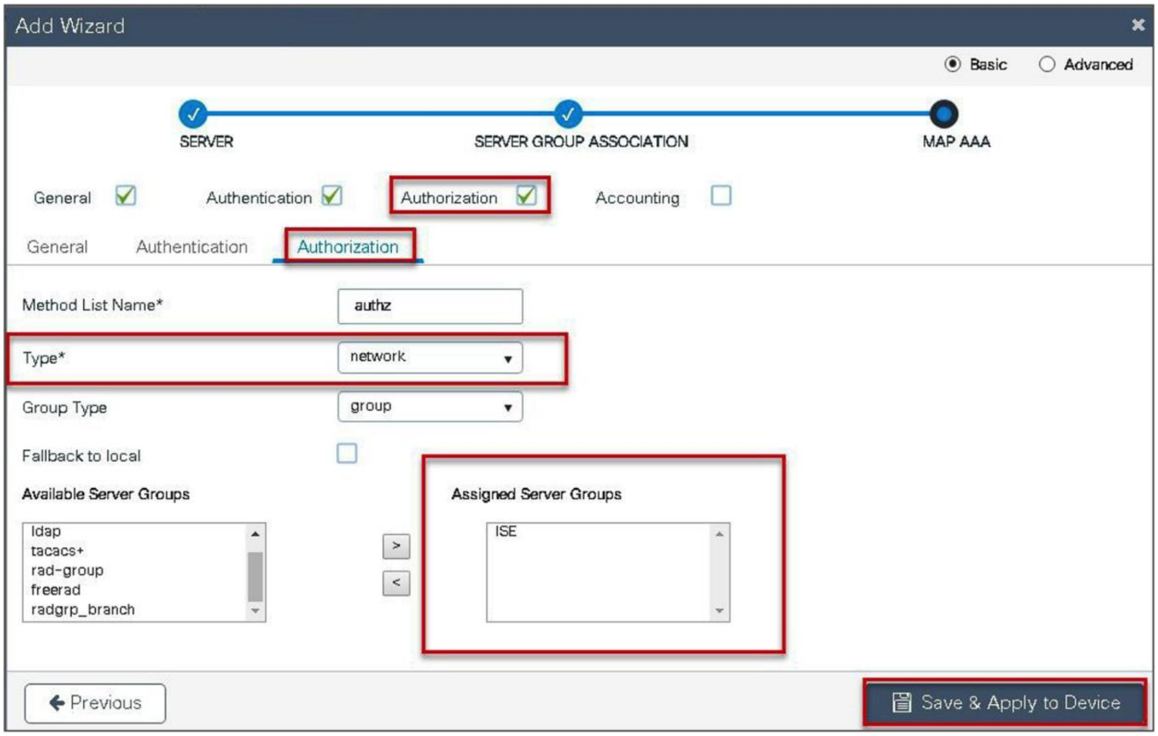
Group Type: group

Fallback to local: □

Available Server Groups: ldap, tacacs+, rad-group, freerad, radgrp_branch

Assigned Server Groups: ISE

Step 7. Define the method type as network and map the server group.



Add Wizard

● Basic ○ Advanced

SERVER — SERVER GROUP ASSOCIATION — MAP AAA

General ☑ Authentication ☑ Authorization ☑ Accounting □

General | Authentication | Authorization

Method List Name*: authz

Type*: network

Group Type: group

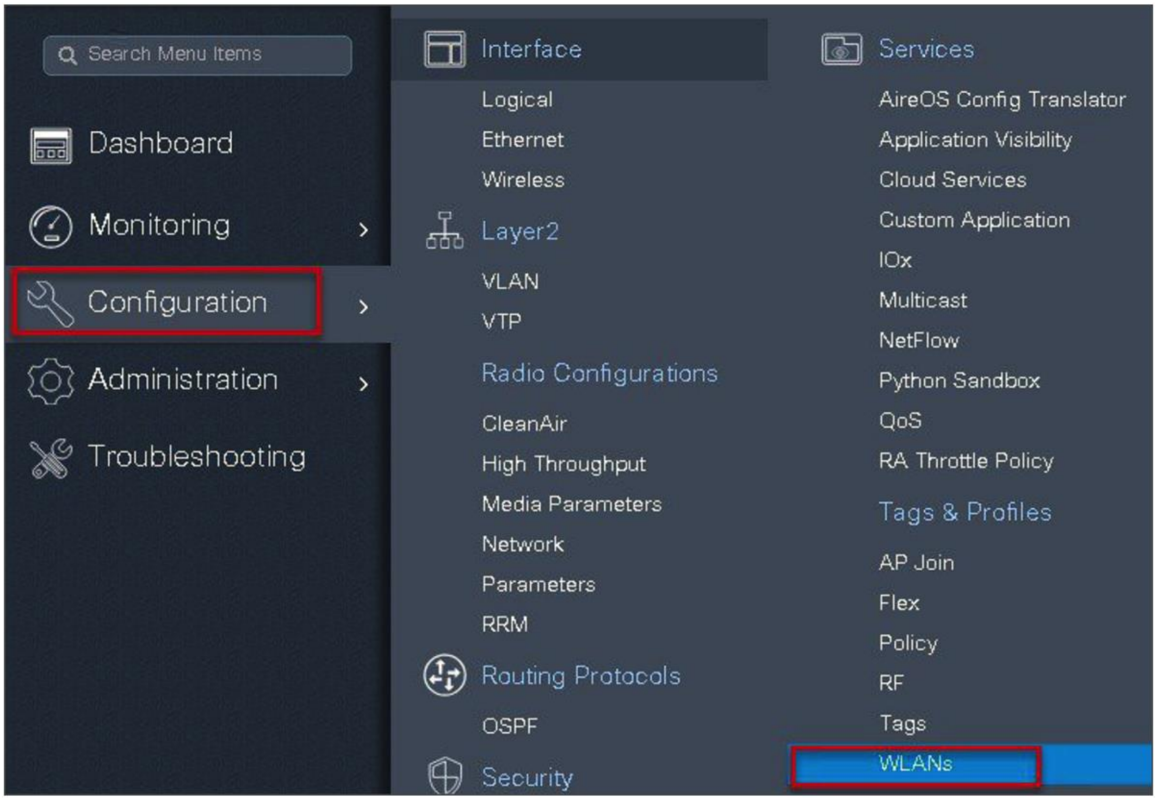
Fallback to local: □

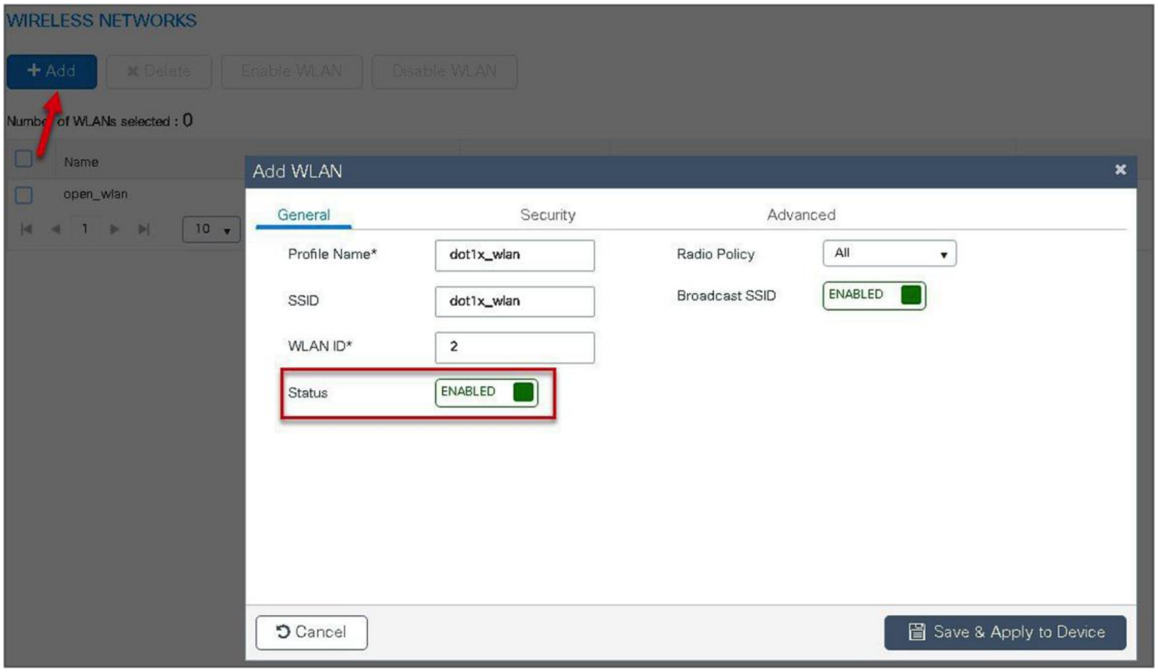
Available Server Groups: ldap, tacacs+, rad-group, freerad, radgrp_branch

Assigned Server Groups: ISE

Step 8. Create a dot1x WLAN and map the method list on the WLAN.

Navigate to Configuration > Tags & Profiles > WLAN to create the SSID.





Profile Name*: dot1x_wlan

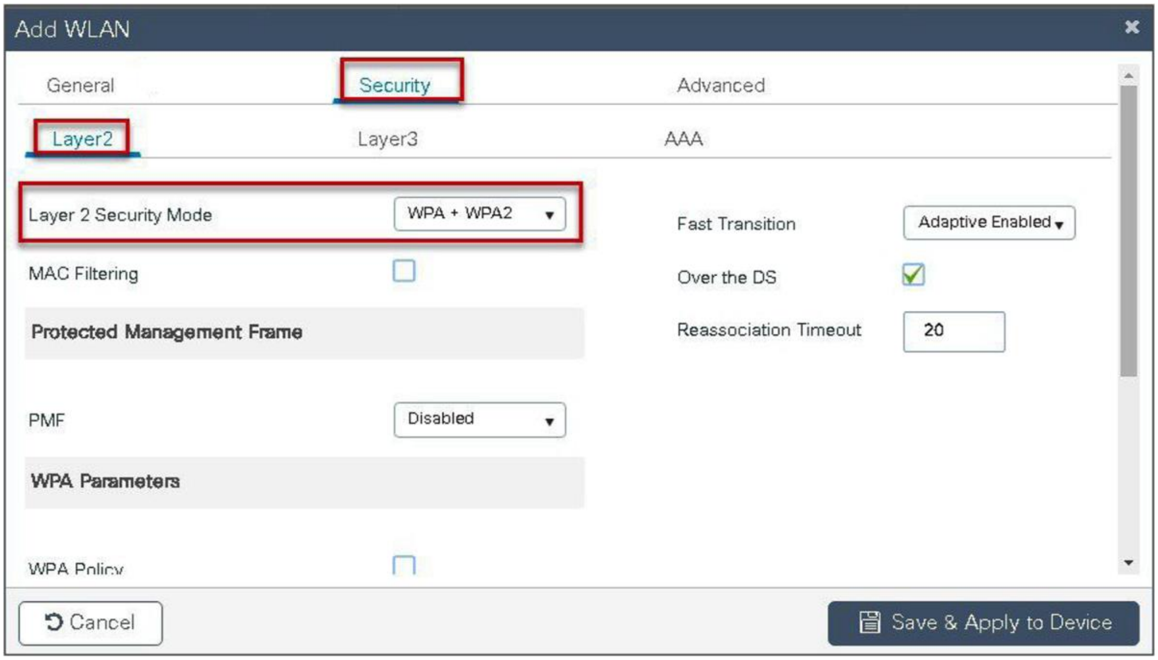
SSID: dot1x_wlan

WLAN ID*: 2

Status: ENABLED

Radio Policy: All

Broadcast SSID: ENABLED



Layer 2 Security Mode: WPA + WPA2

MAC Filtering: □

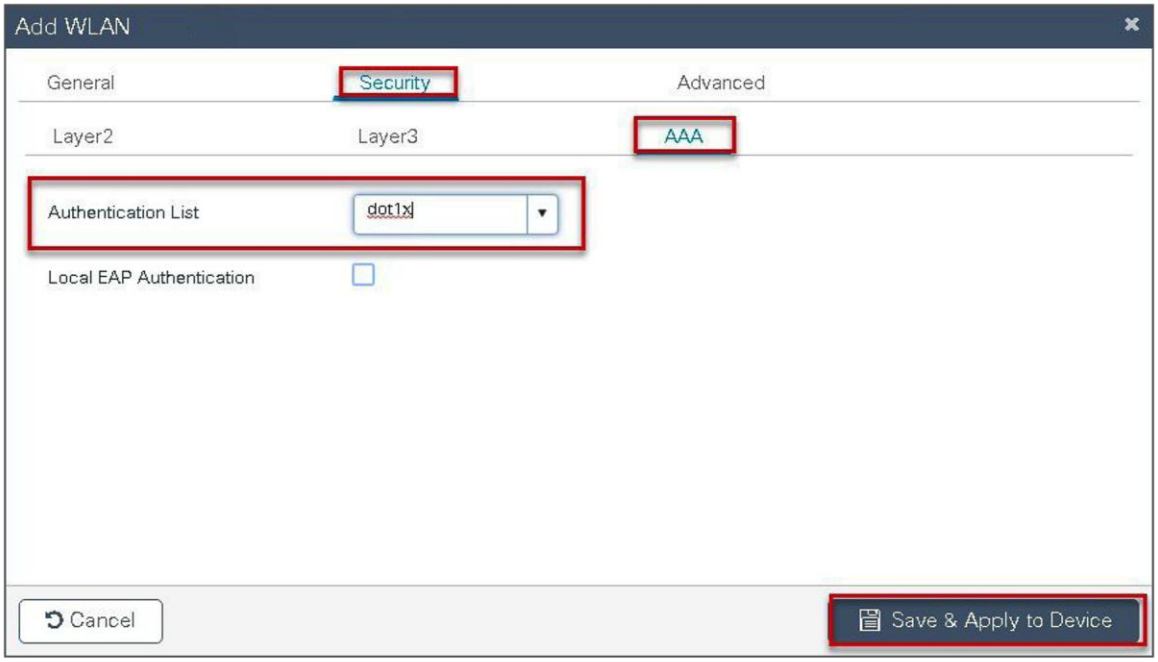
PMF: Disabled

WPA Policy: □

Fast Transition: Adaptive Enabled

Over the DS: ☑

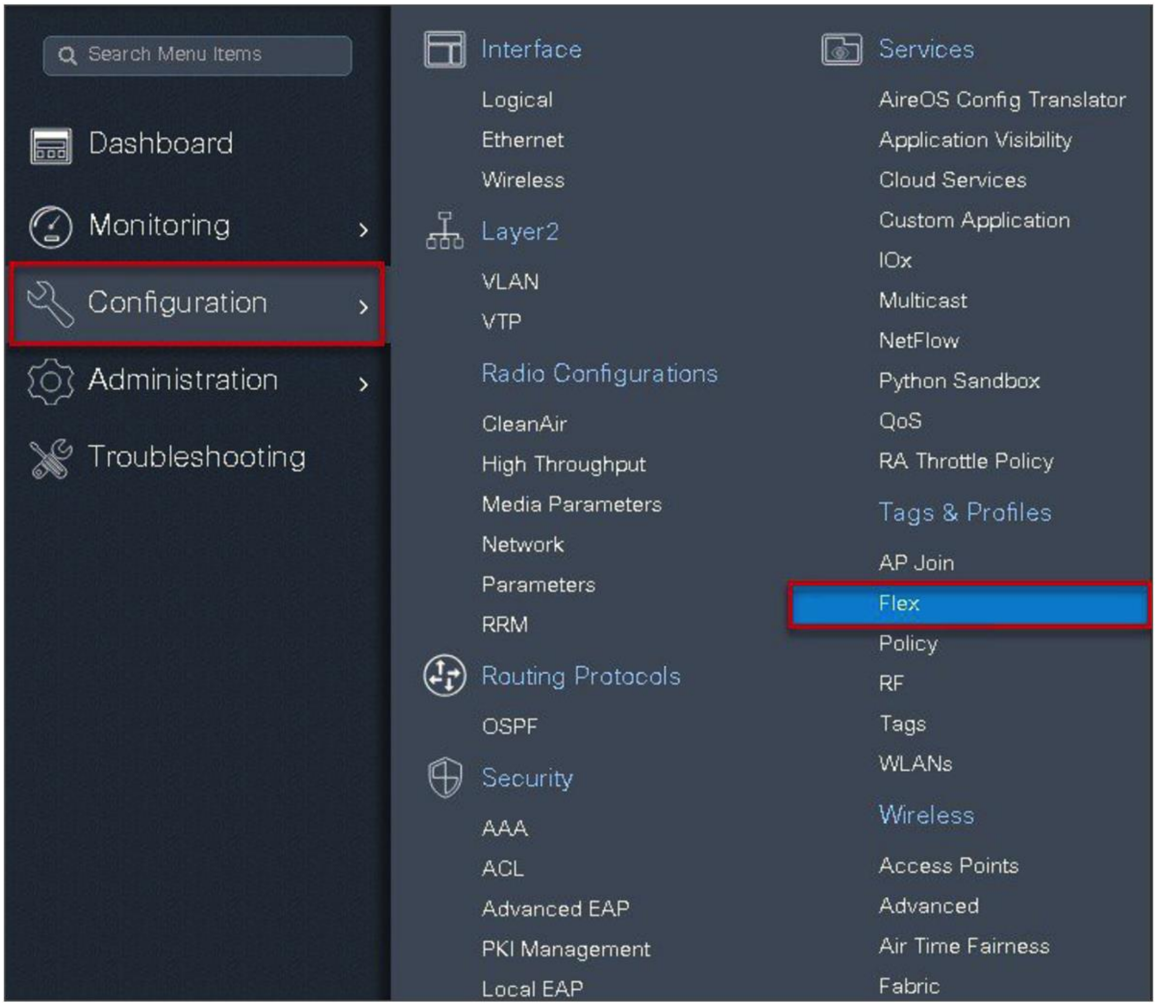
Reassociation Timeout: 20

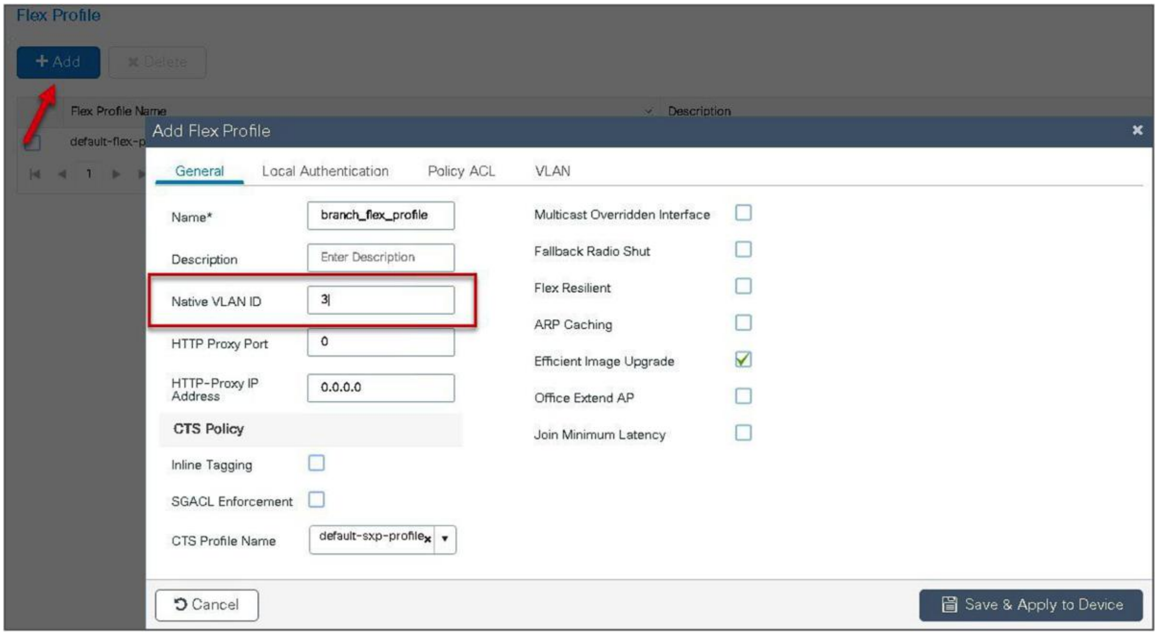


Authentication List: dot1x

Local EAP Authentication: □

Step 9. Create a flex profile. Create a VLAN on the flex profile, which is the VLAN returned by the AAA.



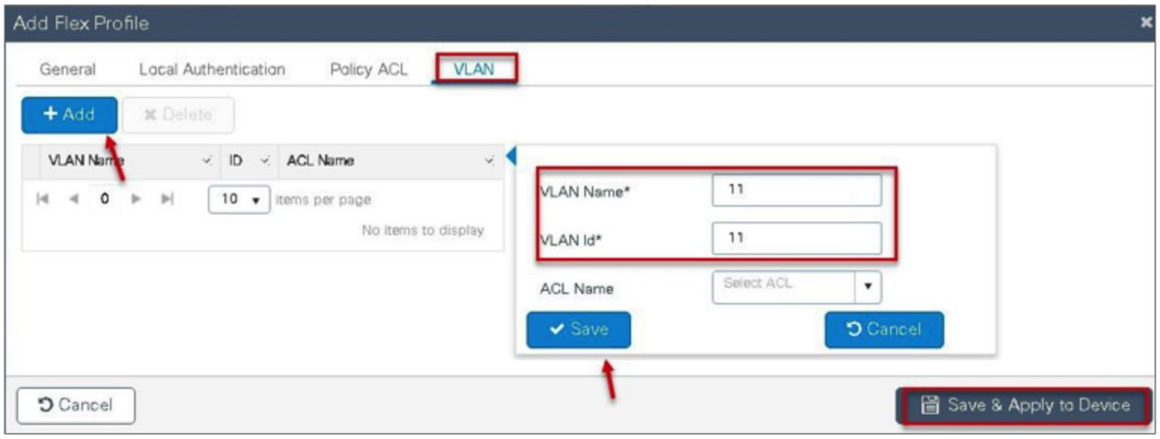


Name*	branch_flex_profile
Description	Enter Description
Native VLAN ID	3
HTTP Proxy Port	0
HTTP-Proxy IP Address	0.0.0.0

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	□

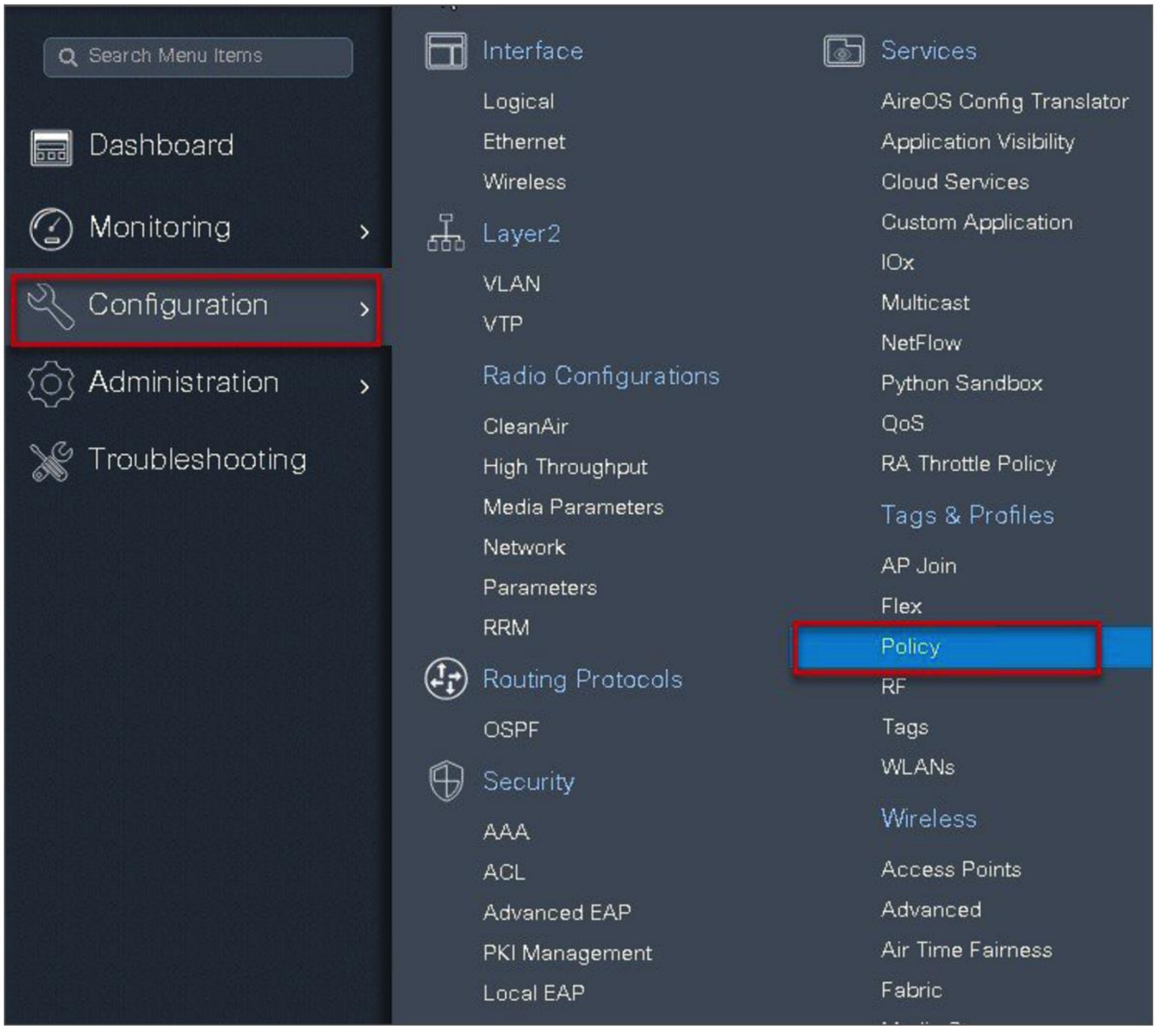


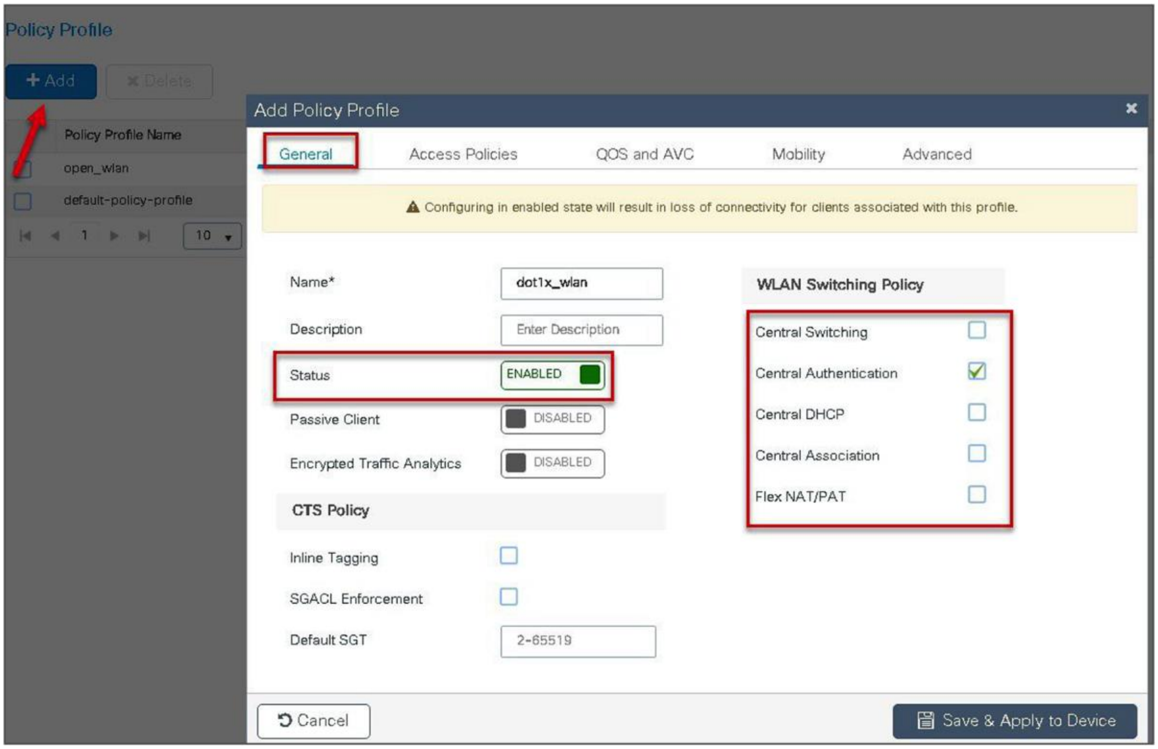
VLAN Name* 11

VLAN Id* 11

ACL Name Select ACL

Step 10. Create a policy profile, enable local switching and central authentication on the profile, map the default VLAN for the WLAN, and enable AAA override.





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

Name* dot1x_wlan

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

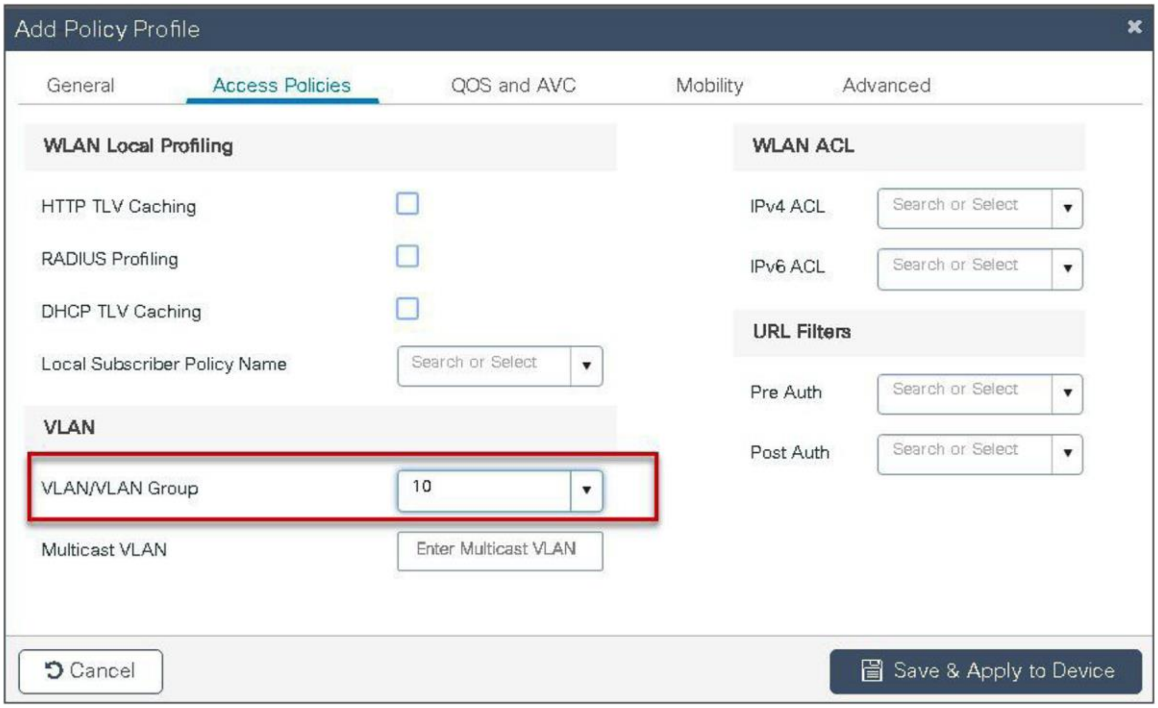
Central Switching □

Central Authentication ☑

Central DHCP □

Central Association □

Flex NAT/PAT □



WLAN Local Profiling

HTTP TLV Caching □

RADIUS Profiling □

DHCP TLV Caching □

Local Subscriber Policy Name Search or Select

VLAN

VLAN/VLAN Group 10

Multicast VLAN Enter Multicast VLAN

WLAN ACL

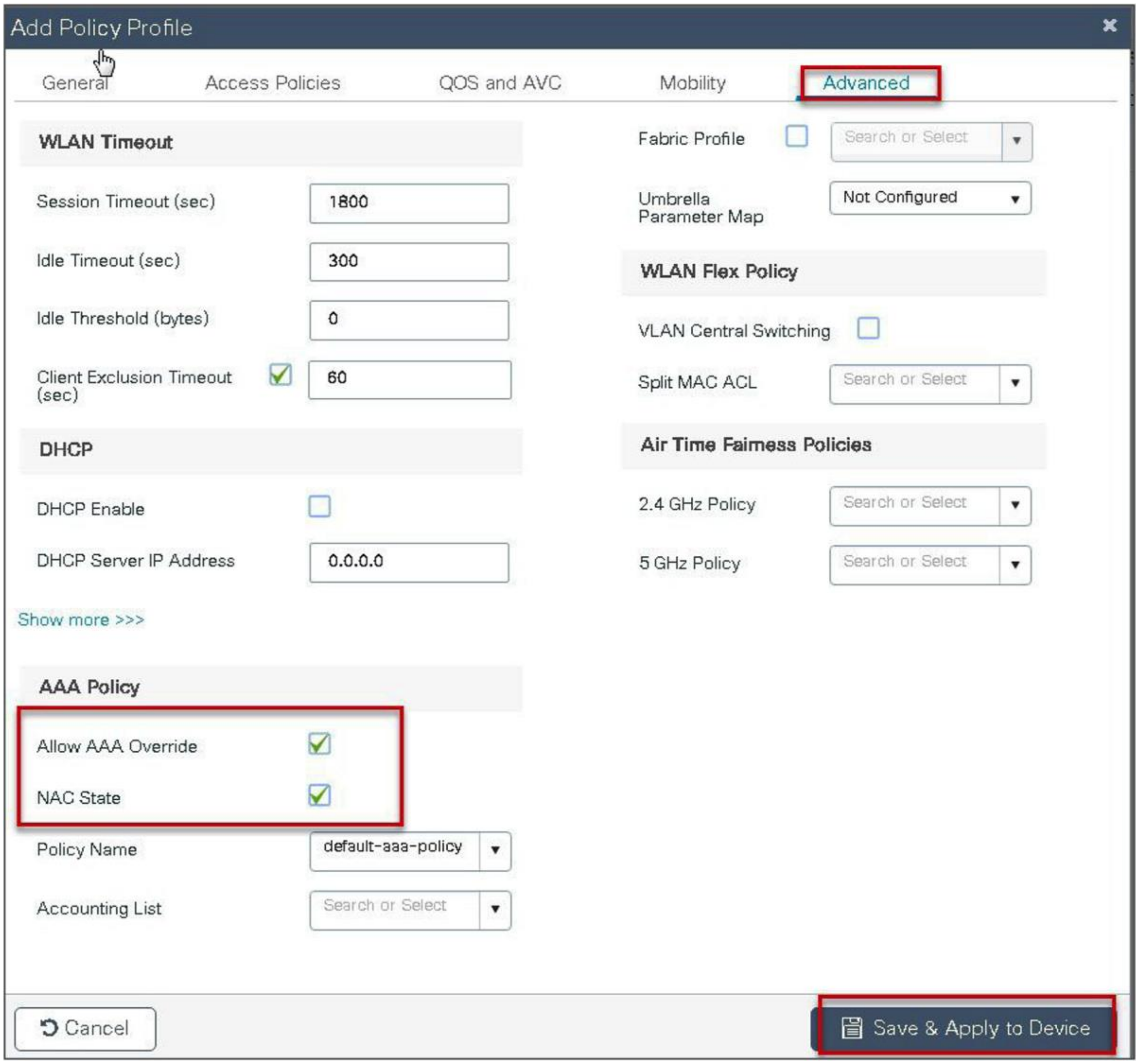
IPv4 ACL Search or Select

IPv6 ACL Search or Select

URL Filters

Pre Auth Search or Select

Post Auth Search or Select



Add Policy Profile

WLAN Timeout

Session Timeout (sec)	1800
Idle Timeout (sec)	300
Idle Threshold (bytes)	0
Client Exclusion Timeout (sec) ☑	60

DHCP

DHCP Enable	□
DHCP Server IP Address	0.0.0.0

Show more >>>

AAA Policy

Allow AAA Override	☑
NAC State	☑
Policy Name	default-aaa-policy
Accounting List	Search or Select

Fabric Profile □	Search or Select
Umbrella Parameter Map	Not Configured

WLAN Flex Policy

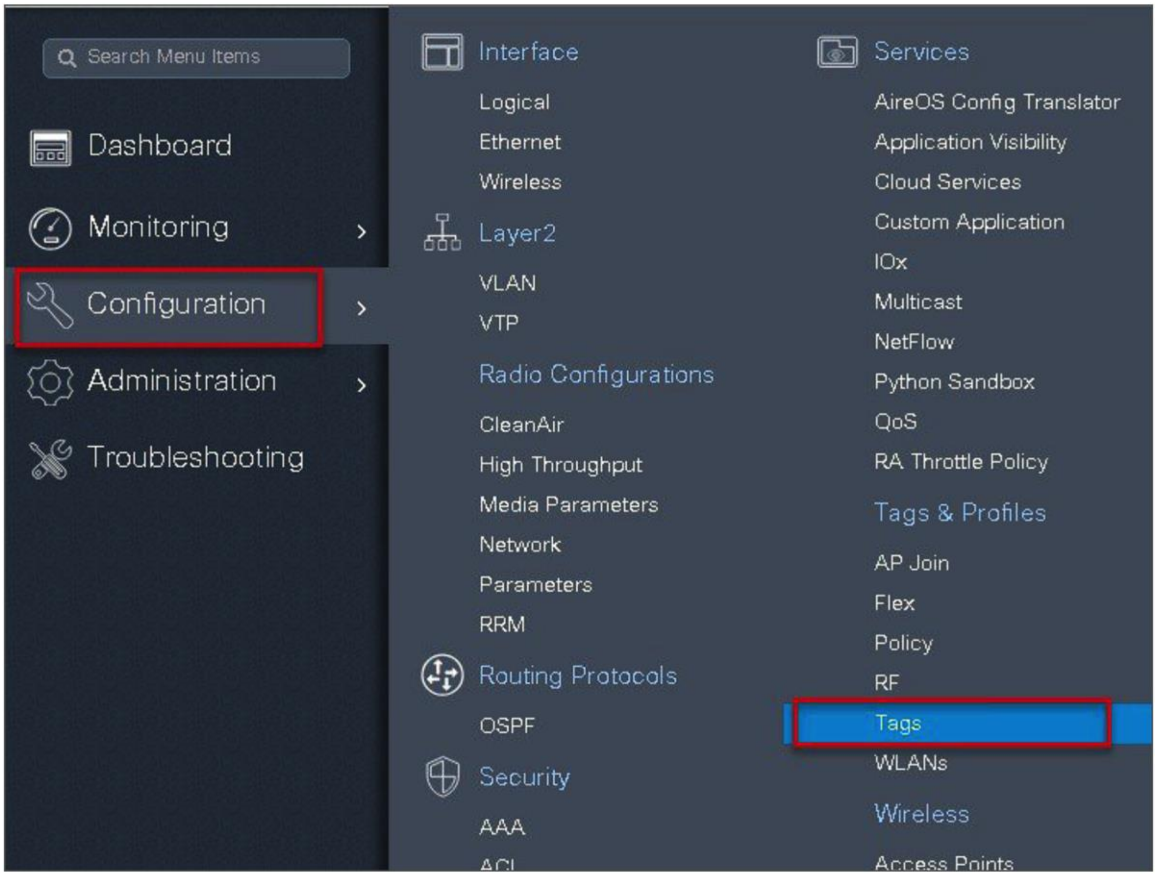
VLAN Central Switching	□
Split MAC ACL	Search or Select

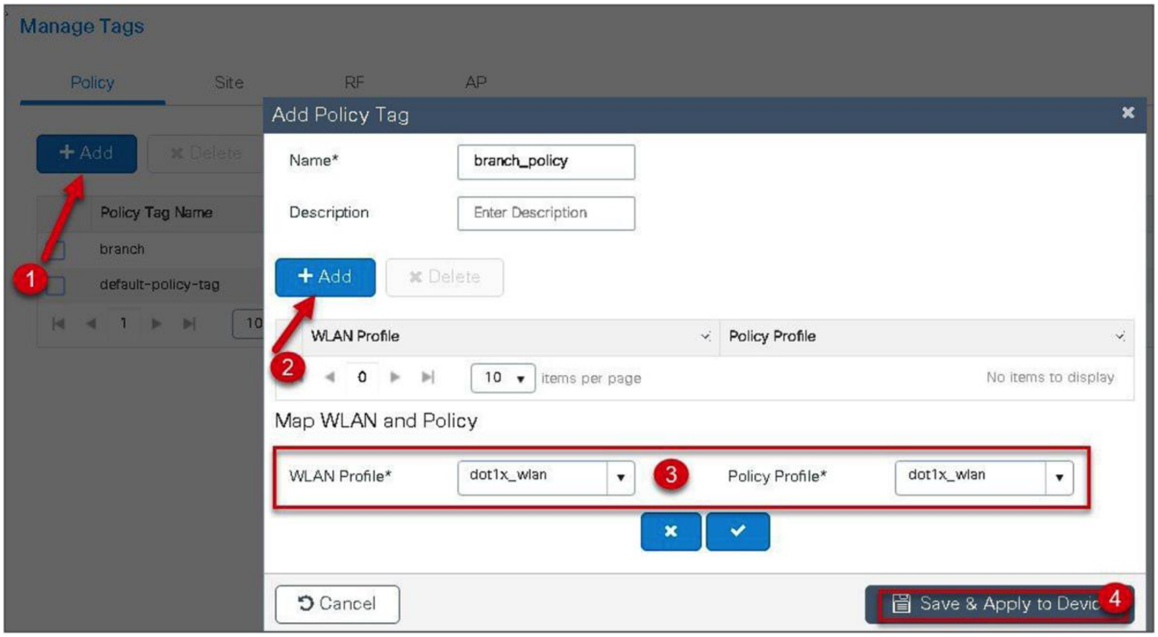
Air Time Fairness Policies

2.4 GHz Policy	Search or Select
5 GHz Policy	Search or Select

Step 11. Map the WLAN to the policy profile.

Navigate to Configuration > Tags and create a policy tag mapping the WLAN and policy profile.





Add Policy Tag

Name*	branch_policy
Description	Enter Description

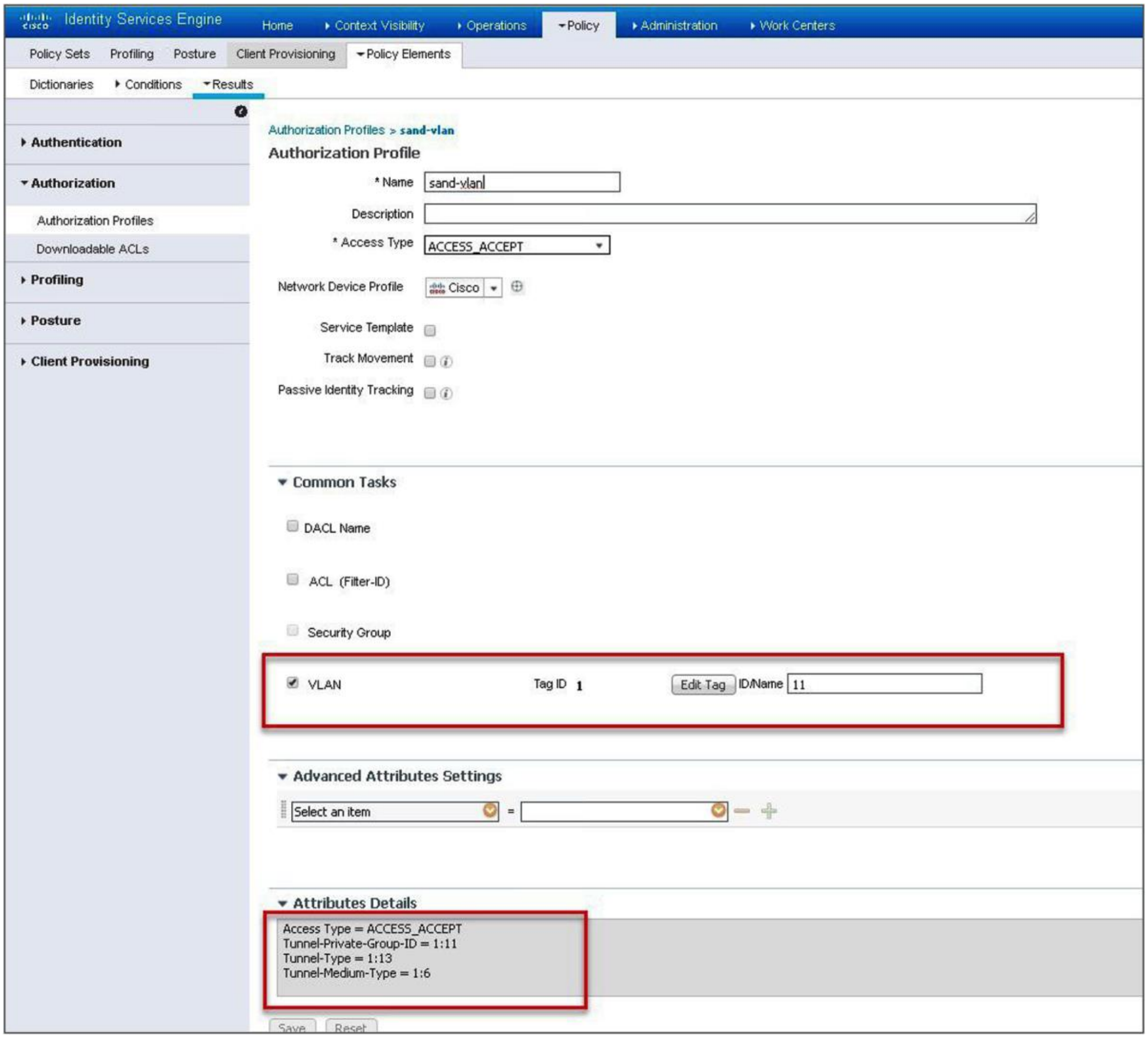
Map WLAN and Policy

WLAN Profile*	dot1x_wlan	Policy Profile*	dot1x_wlan

Step 12. Create an authorization profile on the ISE to override the VLAN from AAA.

Create the respective authorization rules to return the authorization profile as part of access accept.

The screenshot below is for the authorization profile. The authorization rules should refer to the profile created.



Authorization Profile

* Name: sand-vlan

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

Common Tasks

□ DACL Name

□ ACL (Filter-ID)

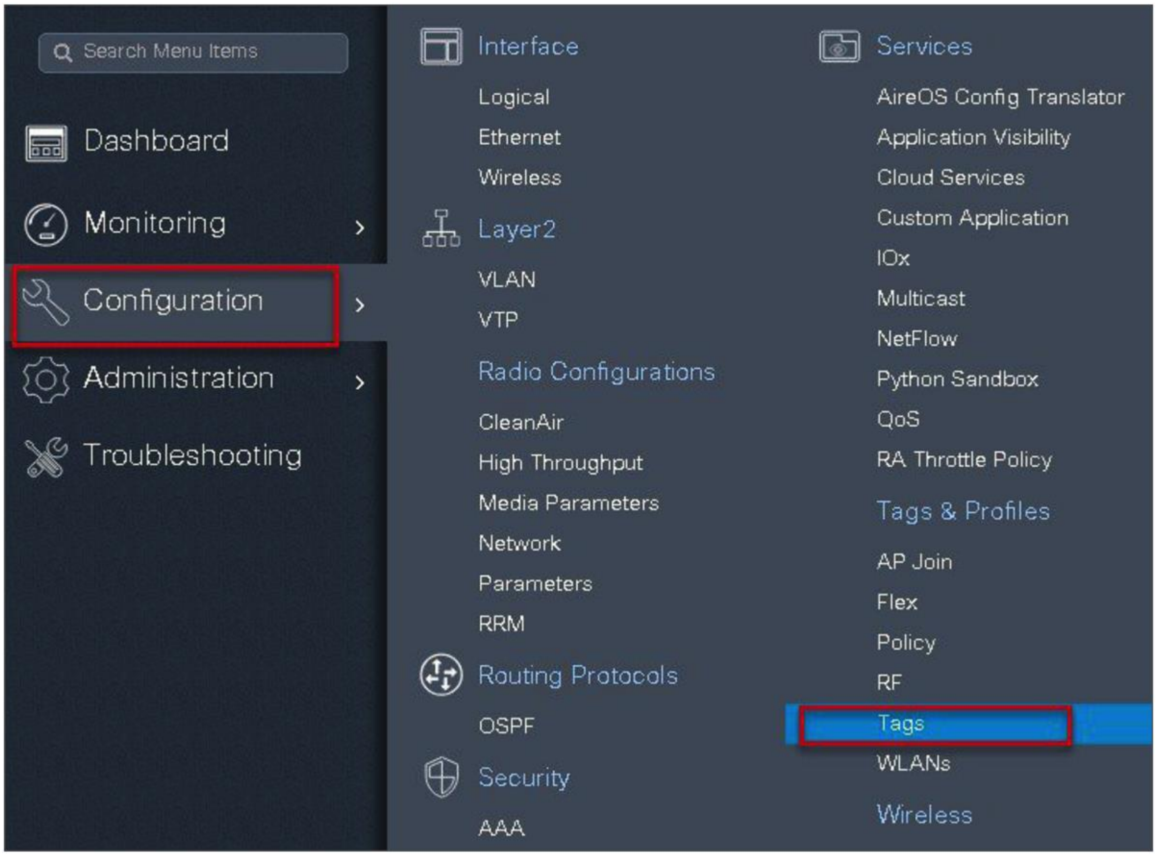
□ Security Group

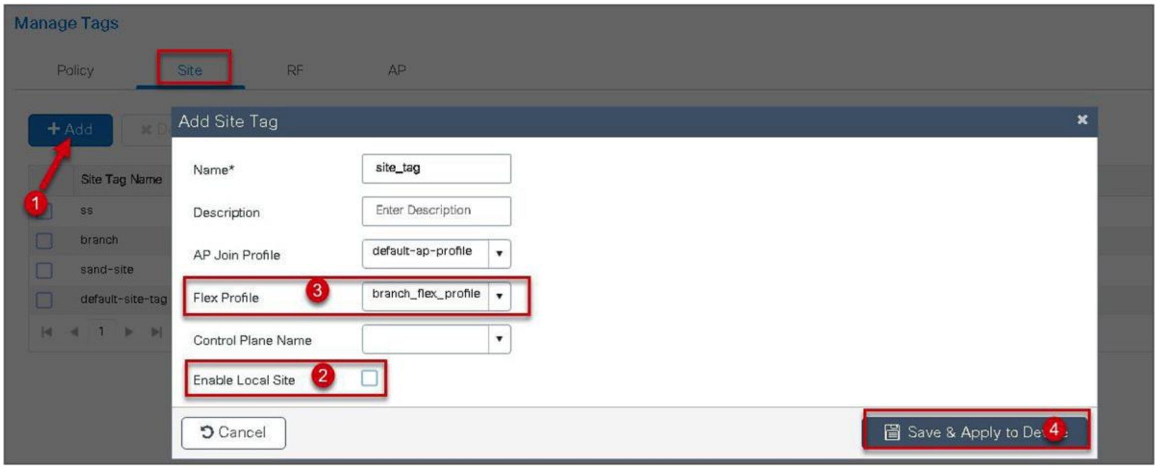
☑ VLAN Tag ID 1 Edit Tag ID/Name 11

Attributes Details

```
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:11
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6
```

Step 13. Create a site tag and map the flex profile on the site tag.



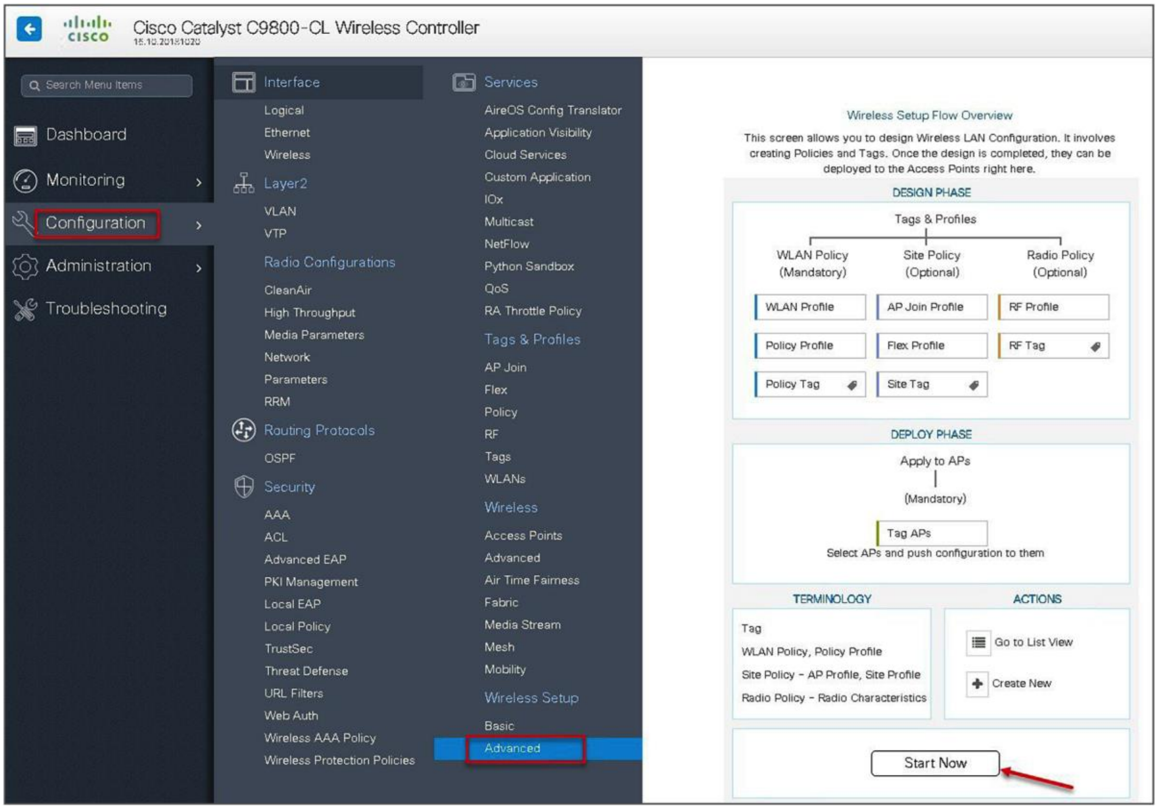


Add Site Tag

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

Step 14. Map the policy site tag and RF tag on the AP using the advanced config wizard.

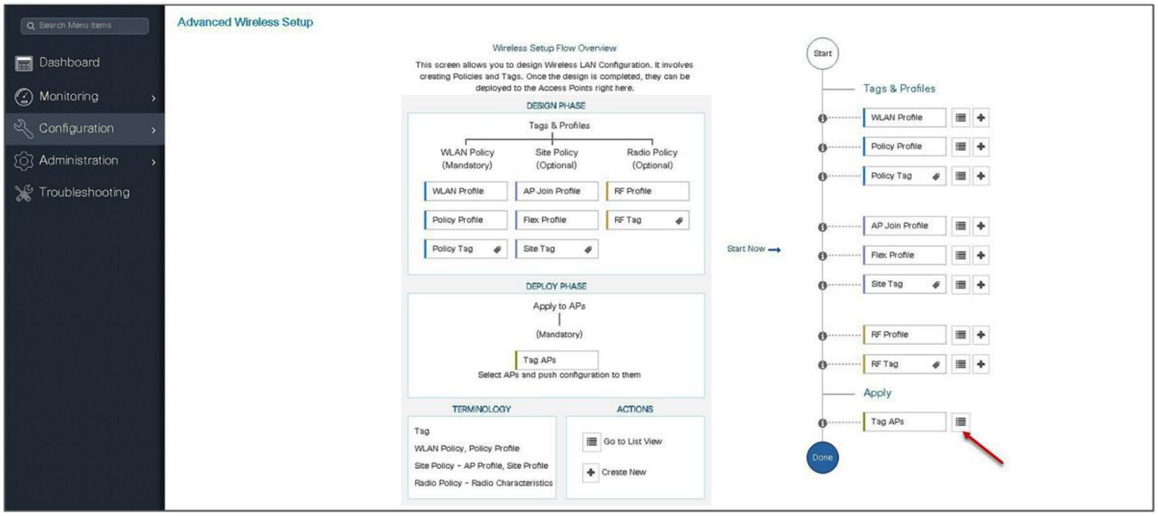
Navigate to Configuration > Wireless Setup > Advanced.



This screen allows you to design Wireless LAN Configuration. It involves creating Policies and Tags. Once the design is completed, they can be deployed to the Access Points right here.

Select APs and push configuration to them

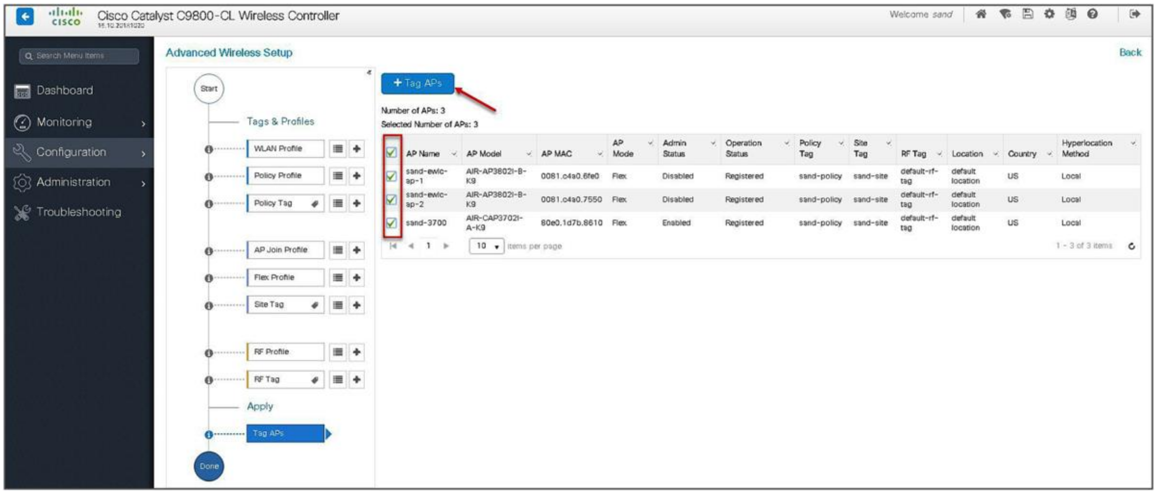
Tag
WLAN Policy, Policy Profile
Site Policy - AP Profile, Site Profile
Radio Policy - Radio Characteristics



This screen allows you to design Wireless LAN Configuration. It involves creating Policies and Tags. Once the design is completed, they can be deployed to the Access Points right here.

Select APs and push configuration to them

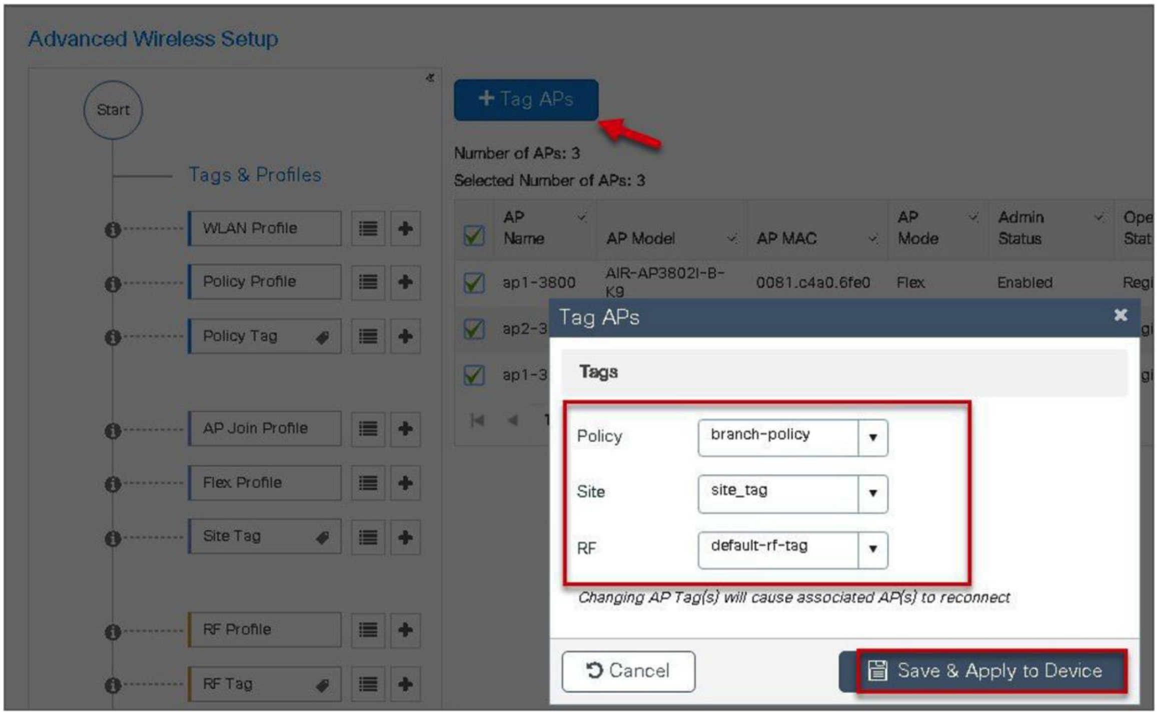
Tag
WLAN Policy, Policy Profile
Site Policy - AP Profile, Site Profile
Radio Policy - Radio Characteristics



Number of APs: 3
Selected Number of APs: 3

☑	AP Name	AP Model	AP MAC	AP Mode	Admin Status	Operation Status	Policy Tag	Site Tag	RF Tag	Location	Country	Hyperlocation Method
☑	sand-ewlc-ap-1	AIR-AP3802I-B-K9	0081.c4a0.6fe0	Flex	Disabled	Registered	sand-policy	sand-site	default-rf-tag	default location	US	Local
☑	sand-ewlc-ap-2	AIR-AP3802I-B-K9	0081.c4a0.7550	Flex	Disabled	Registered	sand-policy	sand-site	default-rf-tag	default location	US	Local
☑	sand-3700	AIR-CAP3702I-A-K9	80e0.1d7b.8610	Flex	Enabled	Registered	sand-policy	sand-site	default-rf-tag	default location	US	Local

1 - 3 of 3 items



Number of APs: 3
Selected Number of APs: 3

☑	AP Name	AP Model	AP MAC	AP Mode	Admin Status	Ope Stat
☑	ap1-3800	AIR-AP3802I-B-K9	0081.c4a0.6fe0	Flex	Enabled	Regi
☑	ap2-3					
☑	ap1-3					

Tag APs

Tags

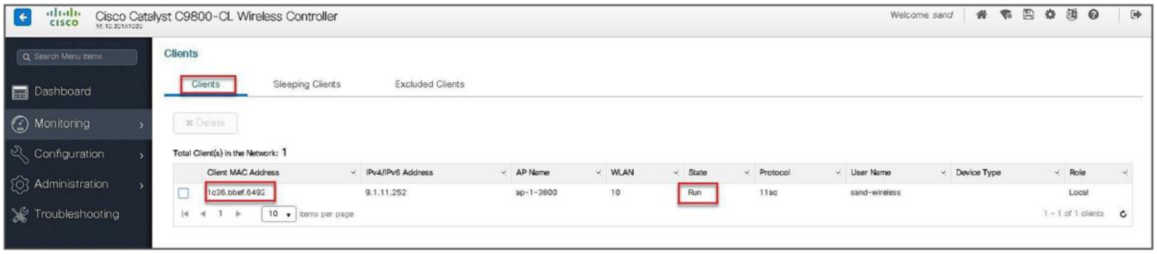
Policy	branch-policy
Site	site_tag
RF	default-rf-tag

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

Step 15. Associate a client on the WLAN and authenticate using the username configured in the AAA server in order to return the AAA VLAN as the attribute.

Verify the client connectivity by navigating to monitoring wireless clients and verify the access VLAN that the client is mapped to.

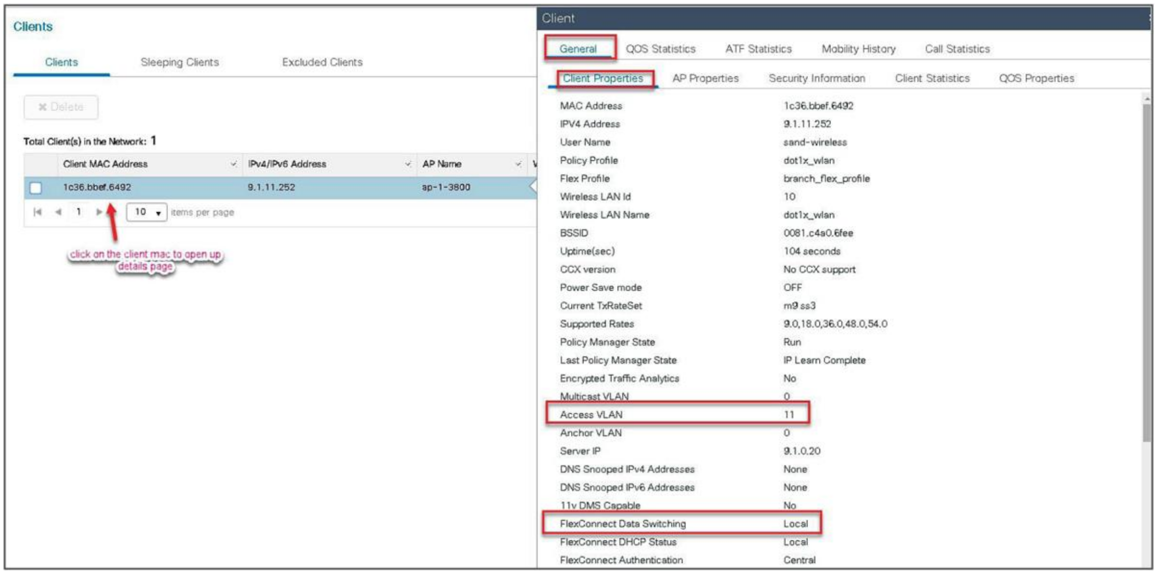
Double-click on the client MAC to open up the details of the client session.



Total Client(s) in the Network: 1

□	Client MAC Address	IPv4/IPv6 Address	AP Name	WLAN	State	Protocol	User Name	Device Type	Role
□	1c36.bbef.6492	9.1.11.252	ap-1-3800	10	Run	11ac	sand-wireless		Local

1 - 1 of 1 clients

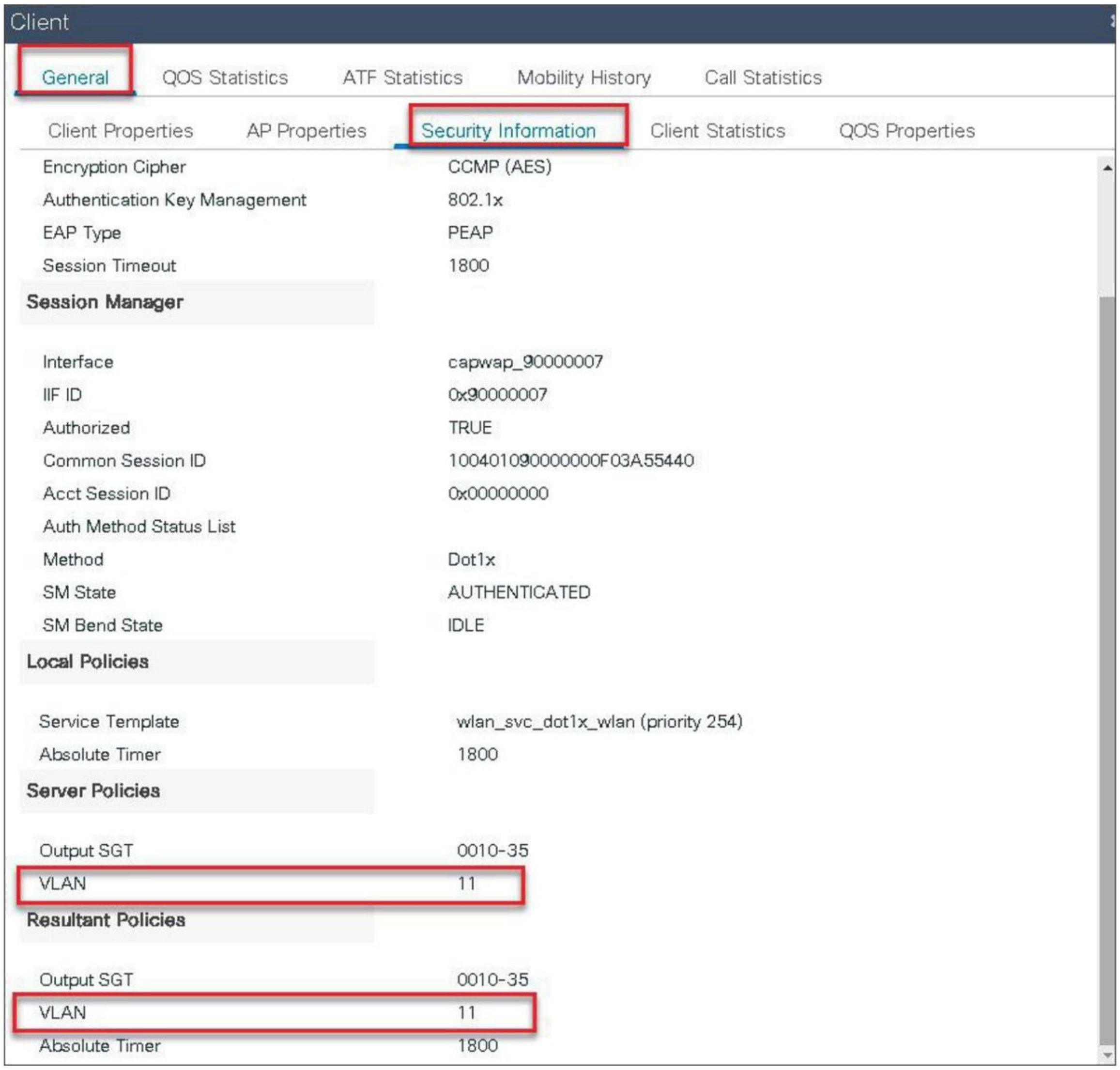


Total Client(s) in the Network: 1

	Client MAC Address	IPv4/IPv6 Address	AP Name
□	1c36.bbef.6492	9.1.11.252	ap-1-3800

click on the client mac to open up details page

MAC Address	1c36.bbef.6492
IPV4 Address	9.1.11.252
User Name	sand-wireless
Policy Profile	dot1x_wlan
Flex Profile	branch_flex_profile
Wireless LAN Id	10
Wireless LAN Name	dot1x_wlan
BSSID	0081.c4a0.6fee
Uptime(sec)	104 seconds
CCX version	No CCX support
Power Save mode	OFF
Current TxRateSet	m9 ss3
Supported Rates	9.0,18.0,36.0,48.0,54.0
Policy Manager State	Run
Last Policy Manager State	IP Learn Complete
Encrypted Traffic Analytics	No
Multicast VLAN	0
Access VLAN	11
Anchor VLAN	0
Server IP	9.1.0.20
DNS Snooped IPv4 Addresses	None
DNS Snooped IPv6 Addresses	None
11v DMS Capable	No
FlexConnect Data Switching	Local
FlexConnect DHCP Status	Local
FlexConnect Authentication	Central



Encryption Cipher	CCMP (AES)
Authentication Key Management	802.1x
EAP Type	PEAP
Session Timeout	1800
Session Manager	
Interface	capwap_90000007
IIF ID	0x90000007
Authorized	TRUE
Common Session ID	100401090000000F03A55440
Acct Session ID	0x00000000
Auth Method Status List	
Method	Dot1x
SM State	AUTHENTICATED
SM Bend State	IDLE
Local Policies	
Service Template	wlan_svc_dot1x_wlan (priority 254)
Absolute Timer	1800
Server Policies	
Output SGT	0010-35
VLAN	11
Resultant Policies	
Output SGT	0010-35
VLAN	11
Absolute Timer	1800

FlexConnect VLAN-based central switching

VLAN-based central switching is a feature that will enable central or local switching based on the VLAN returned as part of the AAA override. If the VLAN provided by the AAA is part of the VLAN present on the AP, the client would be locally switched, and if the VLAN returned by the AAA is not present in the AP and is available at the WLC, the client would be centrally switched.

Summary

Traffic flow on WLANs configured for local switching when flex APs are in connected mode:

- If the VLAN is returned as one of the AAA attributes and that VLAN is not present in the flex AP database, traffic will switch centrally and the client will be assigned this VLAN/interface returned from the AAA server provided that the VLAN exists on the WLC.
- If the VLAN is returned as one of the AAA attributes and that VLAN is not present in the flex AP database, traffic will switch centrally. If that VLAN is also not present on the WLC, the client will be excluded with the reason being VLAN failure.
- If the VLAN is returned as one of the AAA attributes and that VLAN is present in the FlexConnect AP database, traffic will switch locally.
- If the VLAN is not returned from the AAA server, the client will be assigned a VLAN mapped on the policy profile that is attached to the policy tag on that FlexConnect AP and traffic will switch locally.
- If the VLAN returned as part of the AAA attribute is present on both the AP and WLC, the client will be locally switched. The VLAN on the AP takes precedence over the one on the WLC.

Traffic flow on WLANs configured for local switching when flex APs are in standalone mode:

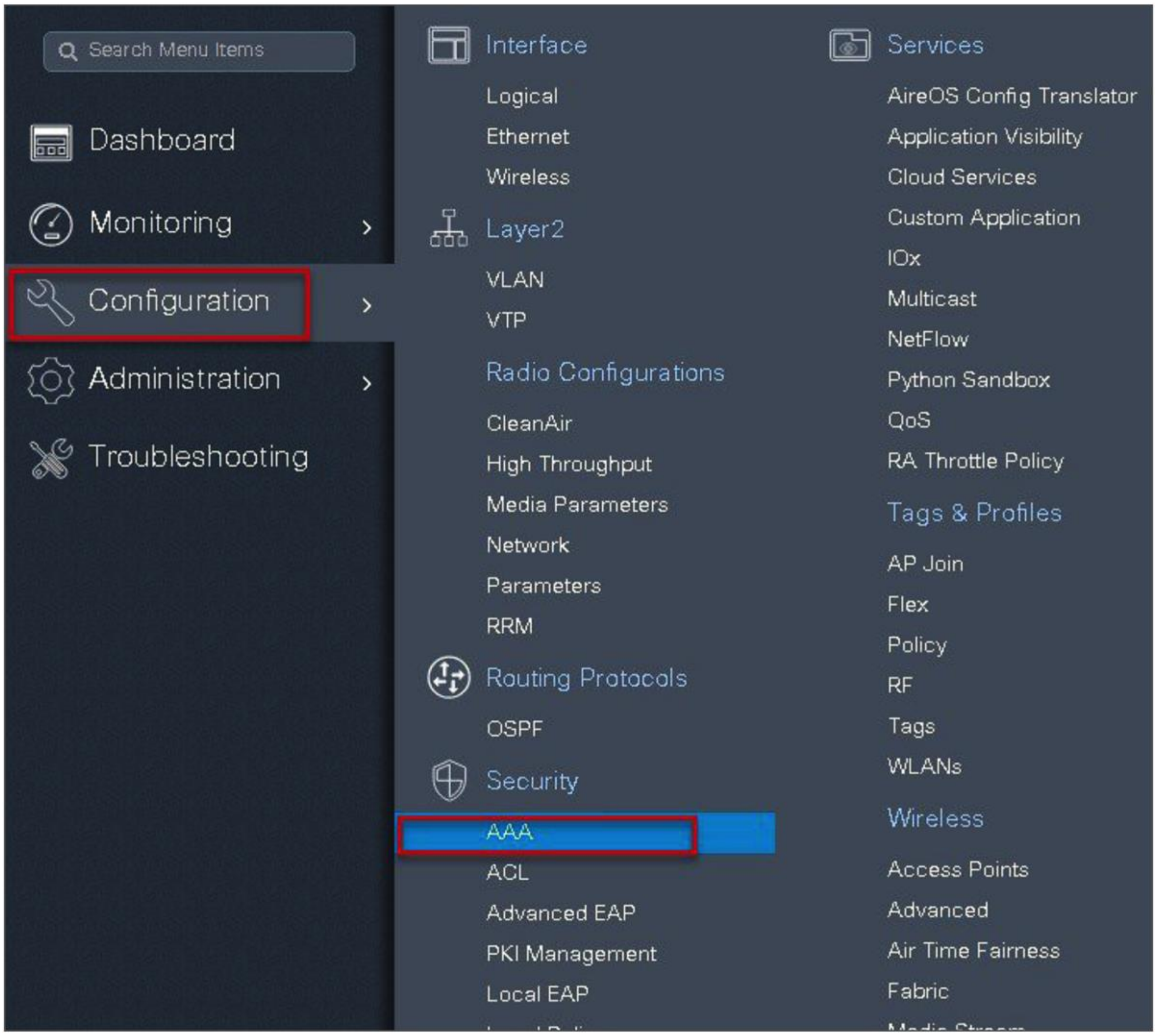
- If the VLAN returned by an AAA server is not present in the flex AP database, the client will be put to default VLAN (that is the VLAN mapped on the policy profile, which is linked to the WLAN). When the AP connects back, this client will be de-authenticated and will switch traffic centrally.
- If the VLAN returned by an AAA server is present in the flex AP database, the client will be put into a returned VLAN, and traffic will switch locally.
- If the VLAN is not returned from an AAA server, the client will be assigned a WLAN mapped VLAN on that FlexConnect AP, and traffic will switch locally.

Steps to configure FlexConnect VLAN-based central switching

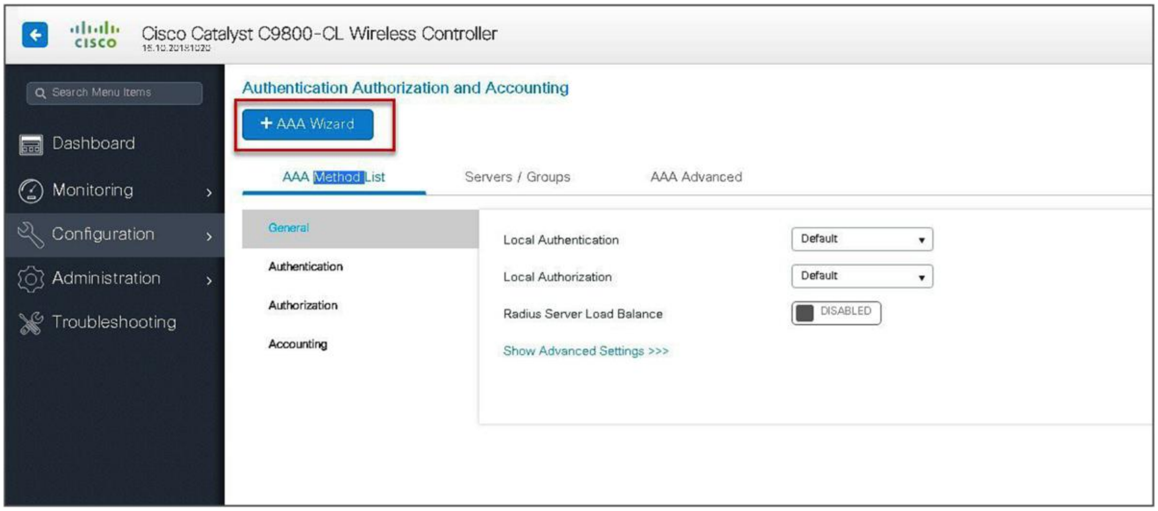
Procedure

Step 1. Define an AAA server and method list for dot1x, which is mapped to the WLAN. The AAA server is created by navigating to the following:

Configuration > Security > AAA.

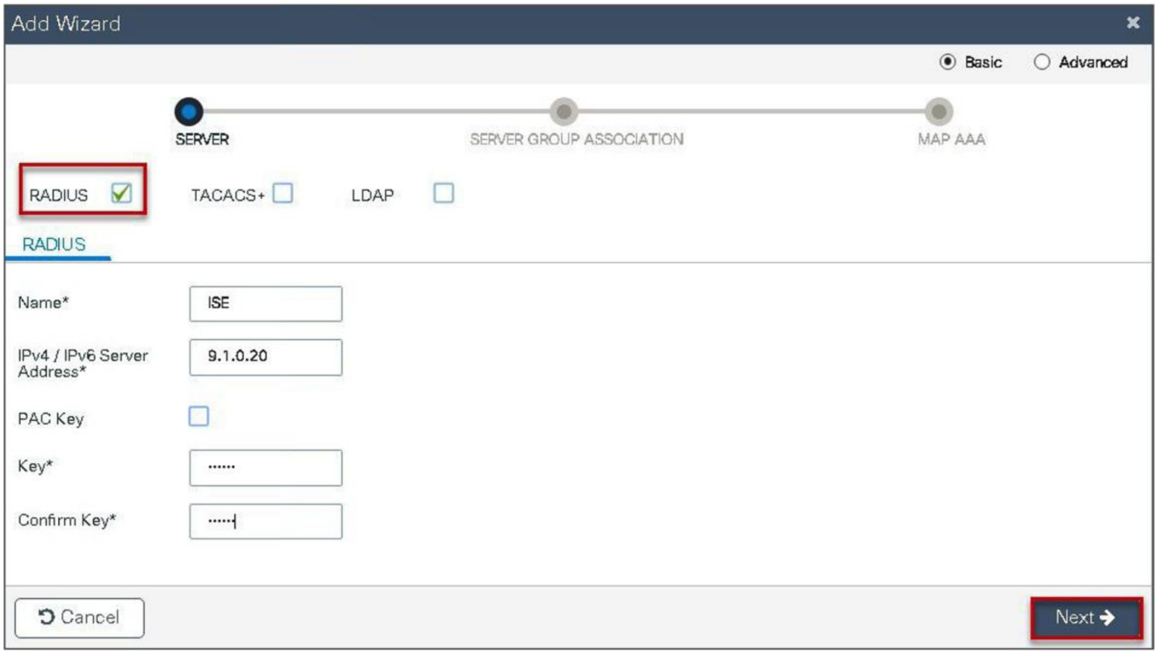


Step 2. Use the AAA wizard to create the server and server groups.



Local Authentication: Default
Local Authorization: Default
Radius Server Load Balance: DISABLED

Step 3. Define a name for the server and specify the IP address and shared secret.

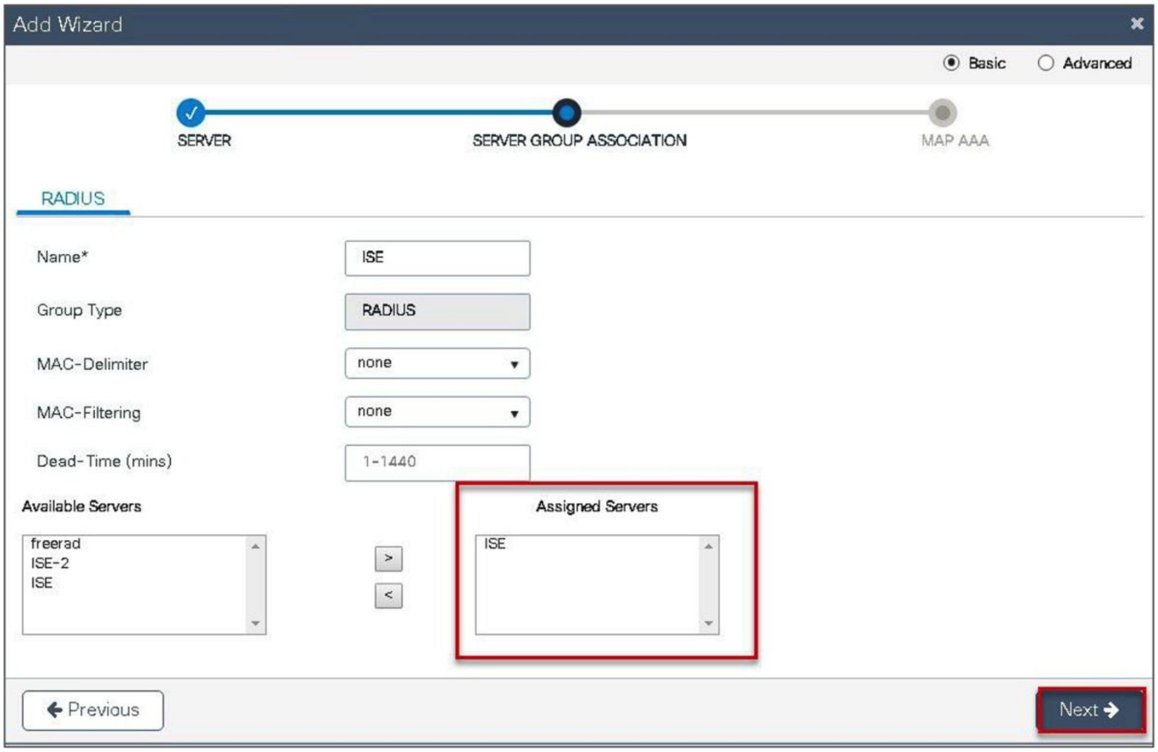


● Basic ○ Advanced

RADIUS ☑ TACACS+ □ LDAP □

Name*: ISE
IPv4 / IPv6 Server Address*: 9.1.0.20
PAC Key: □
Key*: ••••••
Confirm Key*: ••••••

Step 4. Create a server group and map the server in the group.



Name* ISE

Group Type RADIUS

MAC-Delimiter none

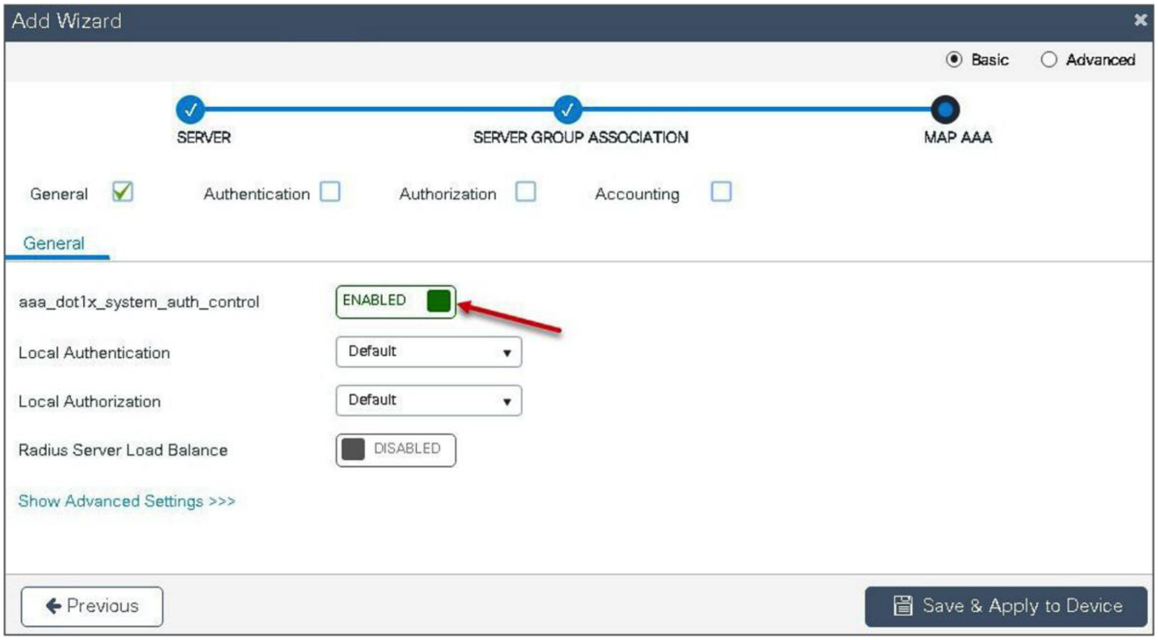
MAC-Filtering none

Dead-Time (mins) 1-1440

Available Servers: freerad, ISE-2, ISE

Assigned Servers: ISE

Step 5. Enable dot1x system control and checkmark the authentication and authorization profile.



General ☑ Authentication □ Authorization □ Accounting □

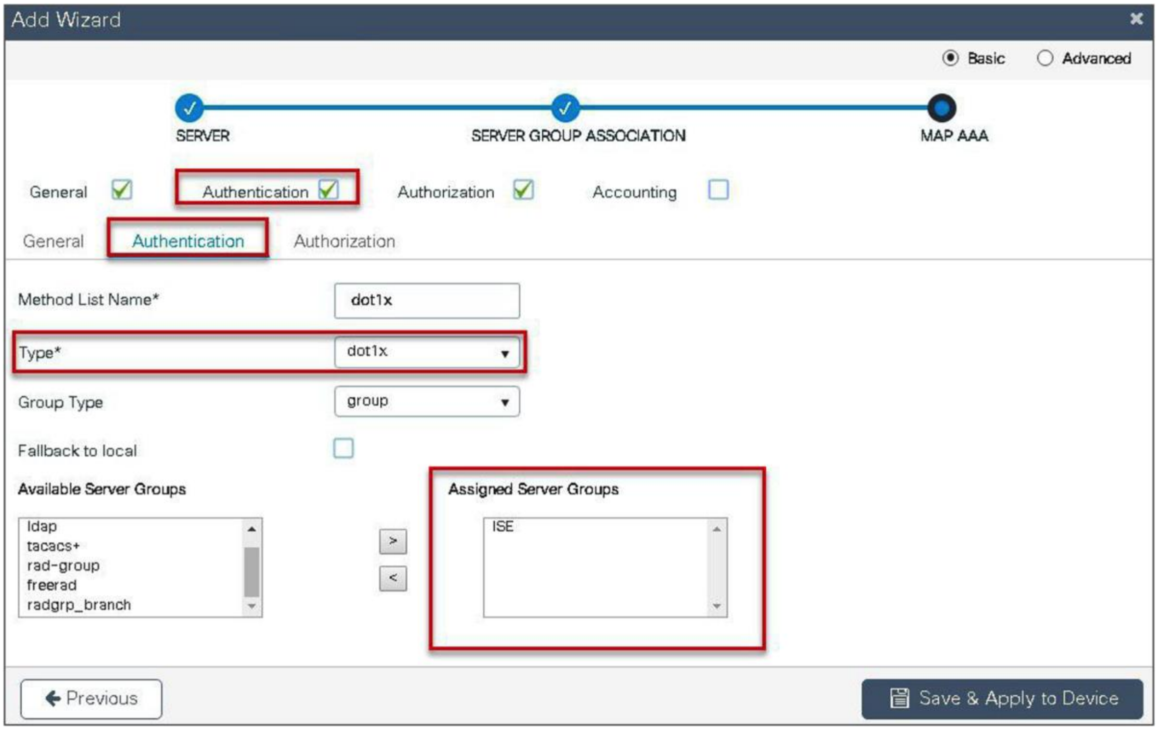
aaa_dot1x_system_auth_control ENABLED

Local Authentication Default

Local Authorization Default

Radius Server Load Balance DISABLED

Step 6. Define the method type as dot1x and map the server group.



● Basic ○ Advanced

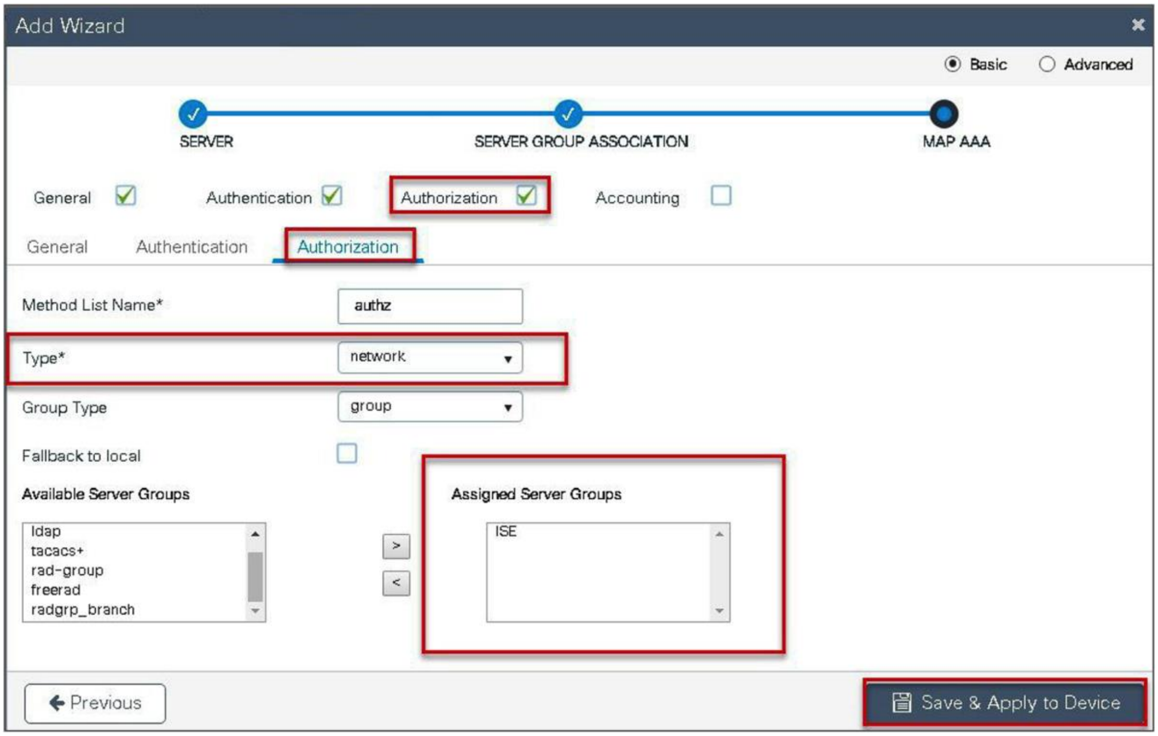
General ☑ Authentication ☑ Authorization ☑ Accounting □

Method List Name*	dot1x
Type*	dot1x
Group Type	group
Fallback to local	□

Available Server Groups: ldap, tacacs+, rad-group, freerad, radgrp_branch

Assigned Server Groups: ISE

Step 7. Define the method type as network and map the server group.



● Basic ○ Advanced

General ☑ Authentication ☑ Authorization ☑ Accounting □

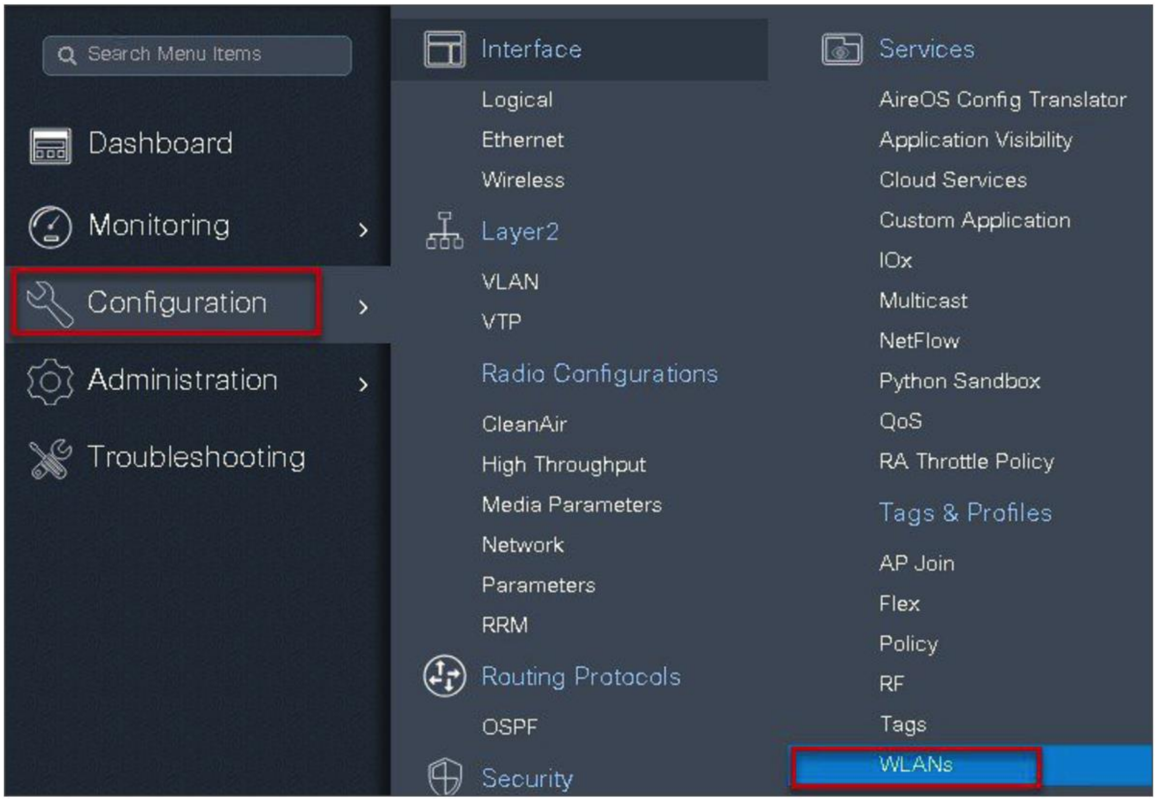
Method List Name*	authz
Type*	network
Group Type	group
Fallback to local	□

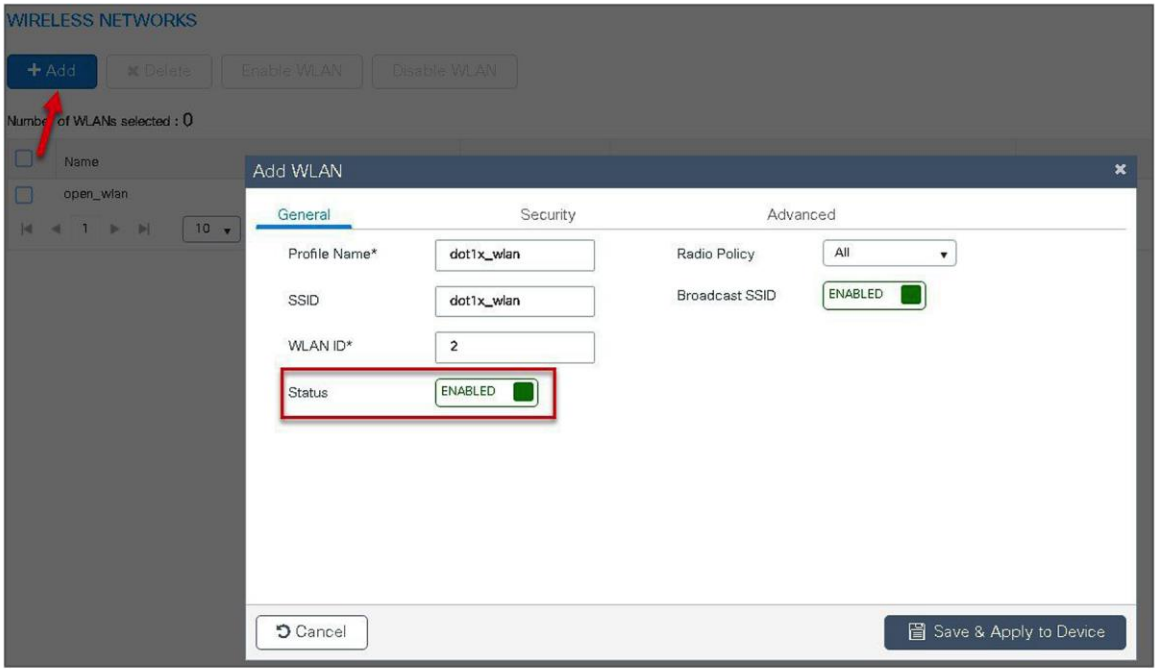
Available Server Groups: ldap, tacacs+, rad-group, freerad, radgrp_branch

Assigned Server Groups: ISE

Step 8. Create a dot1x WLAN and map the method list on the WLAN.

To create an SSID, navigate to Configuration > Tags & Profiles > WLANs.





Profile Name* dot1x_wlan

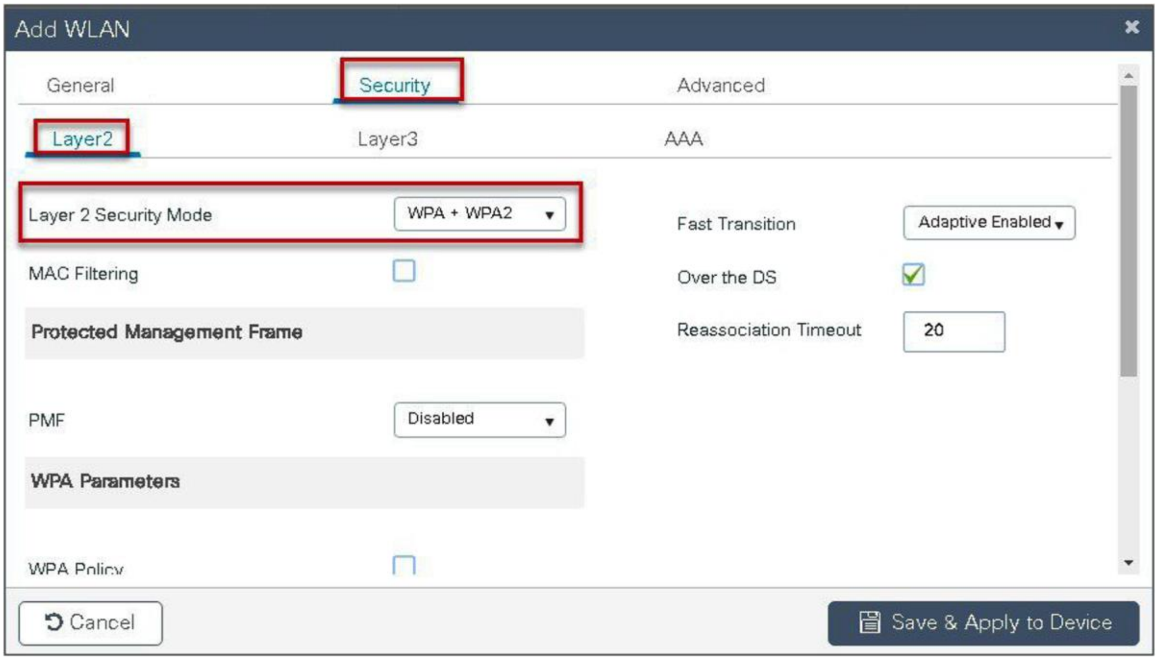
SSID dot1x_wlan

WLAN ID* 2

Status ENABLED

Radio Policy All

Broadcast SSID ENABLED



Layer 2 Security Mode: WPA + WPA2

MAC Filtering: □

Protected Management Frame

PMF: Disabled

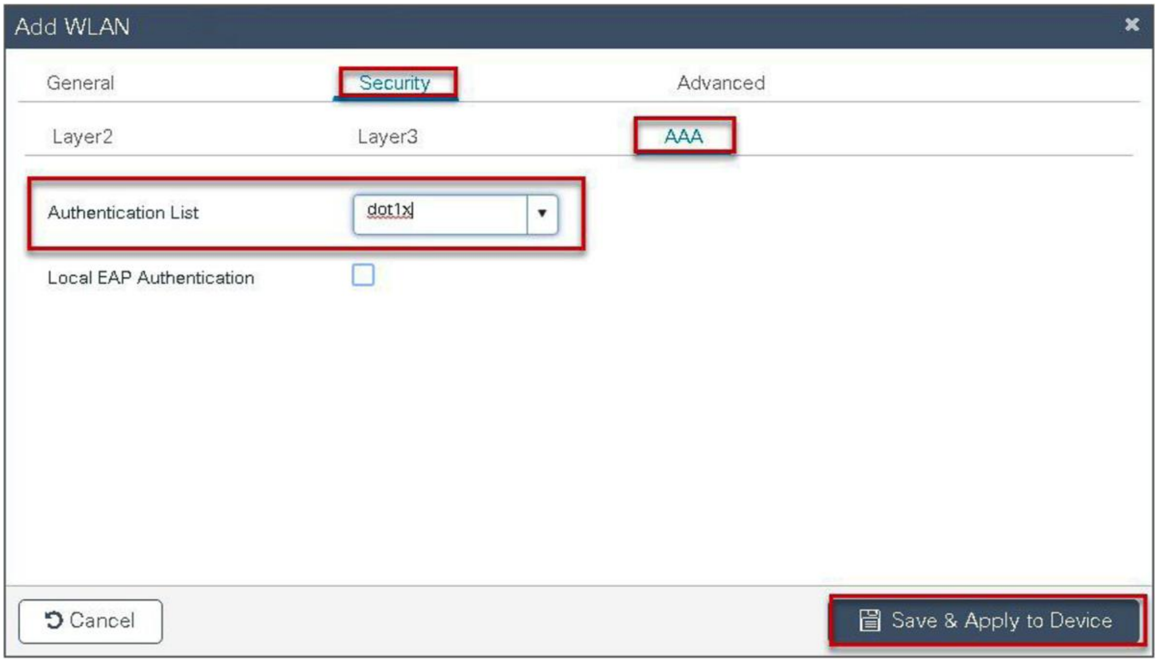
WPA Parameters

WPA Policy: □

Fast Transition: Adaptive Enabled

Over the DS: ☑

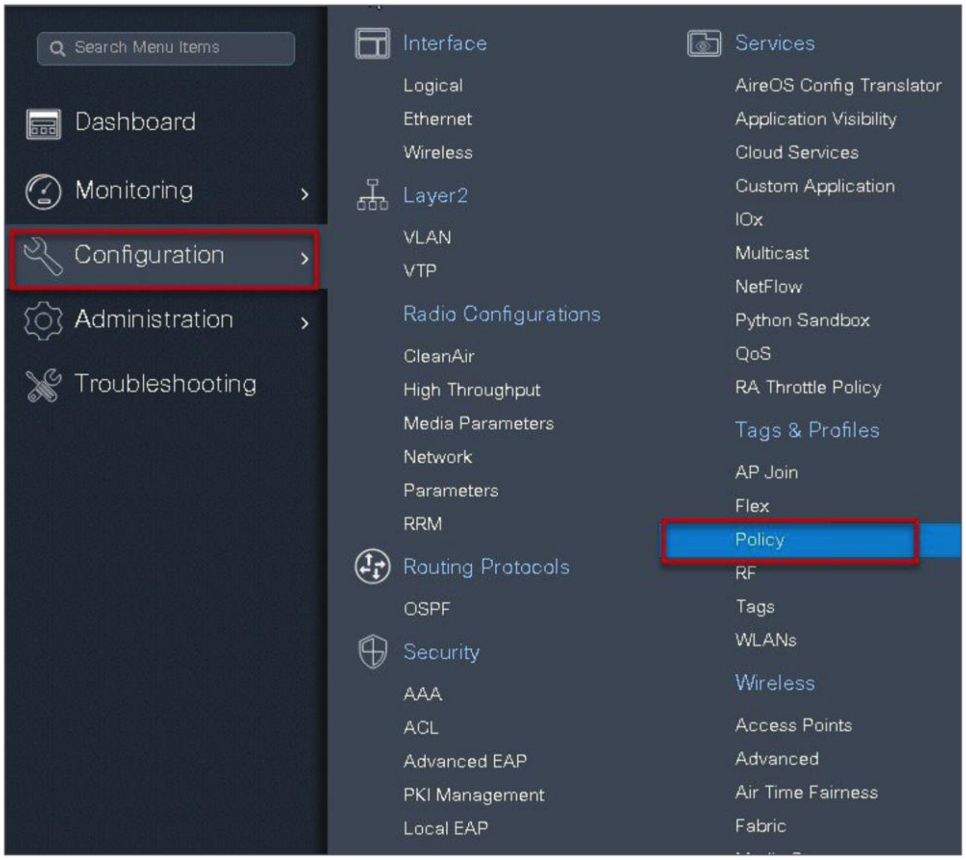
Reassociation Timeout: 20

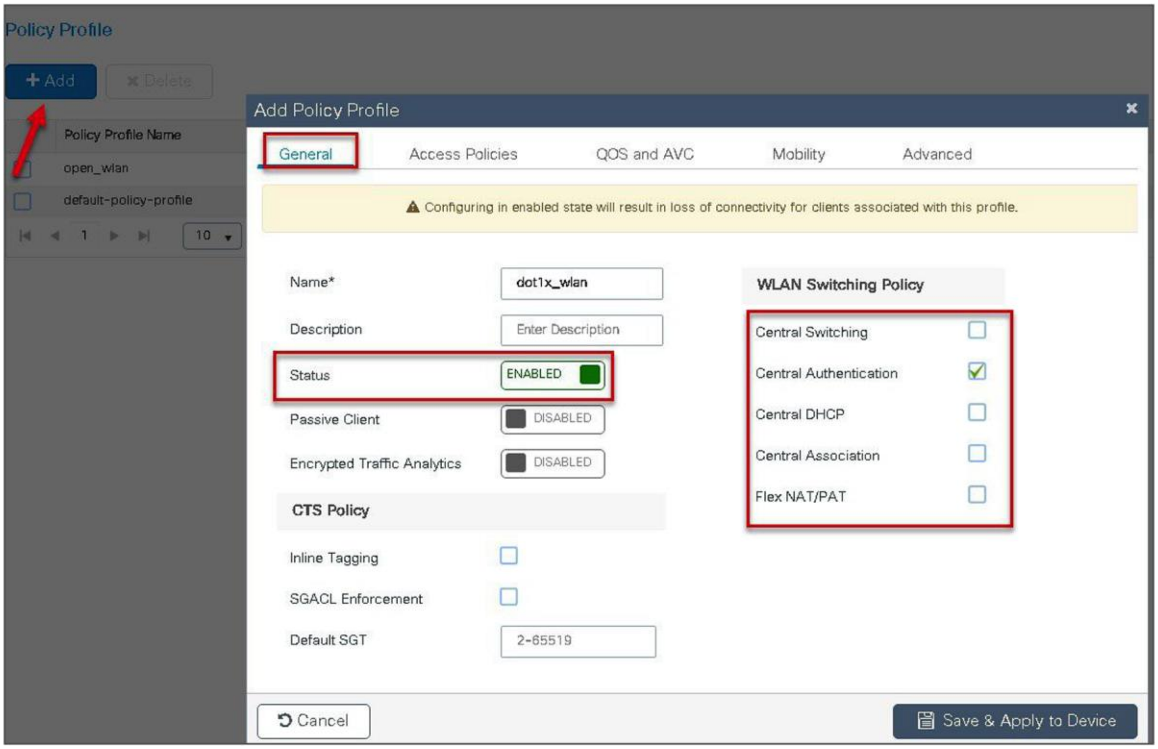


Authentication List: dot1x

Local EAP Authentication: □

Step 9. Create a policy profile, enable local switching and central authentication on the profile, map the default VLAN for the WLAN, and enable AAA override.





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

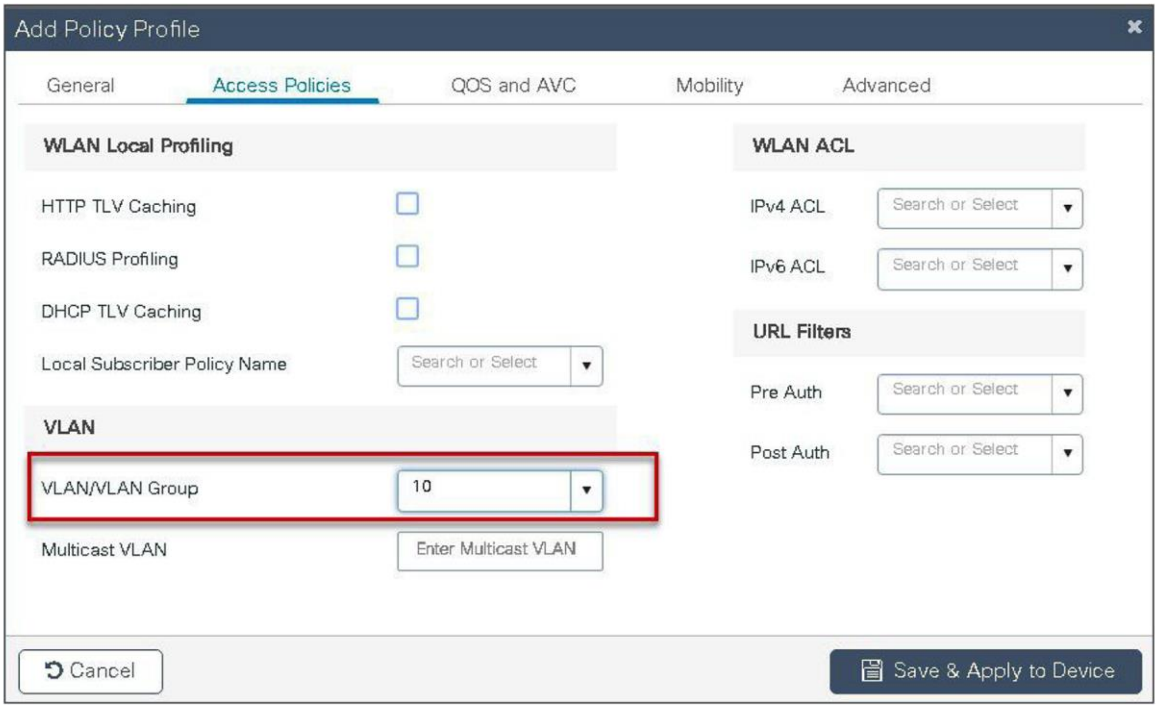
Name*	dot1x_wlan
Description	Enter Description
Status	ENABLED
Passive Client	DISABLED
Encrypted Traffic Analytics	DISABLED

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

WLAN Local Profiling

HTTP TLV Caching □

RADIUS Profiling □

DHCP TLV Caching □

Local Subscriber Policy Name: Search or Select ▾

VLAN

VLAN/VLAN Group: 10 ▾

Multicast VLAN: Enter Multicast VLAN

WLAN ACL

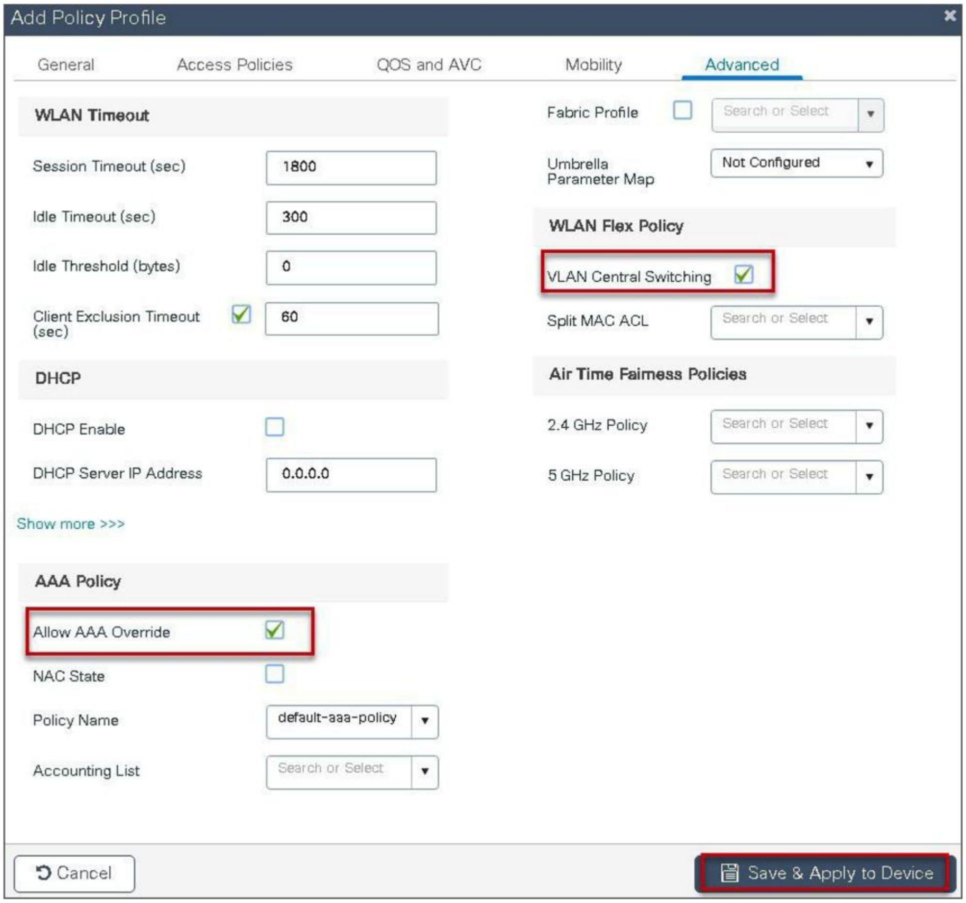
IPv4 ACL: Search or Select ▾

IPv6 ACL: Search or Select ▾

URL Filters

Pre Auth: Search or Select ▾

Post Auth: Search or Select ▾



Add Policy Profile

WLAN Timeout

Session Timeout (sec): 1800

Idle Timeout (sec): 300

Idle Threshold (bytes): 0

Client Exclusion Timeout (sec) ☑ 60

DHCP

DHCP Enable □

DHCP Server IP Address: 0.0.0.0

Show more >>>

AAA Policy

Allow AAA Override ☑

NAC State □

Policy Name: default-aaa-policy ▾

Accounting List: Search or Select ▾

Fabric Profile □ Search or Select ▾

Umbrella Parameter Map: Not Configured ▾

WLAN Flex Policy

VLAN Central Switching ☑

Split MAC ACL: Search or Select ▾

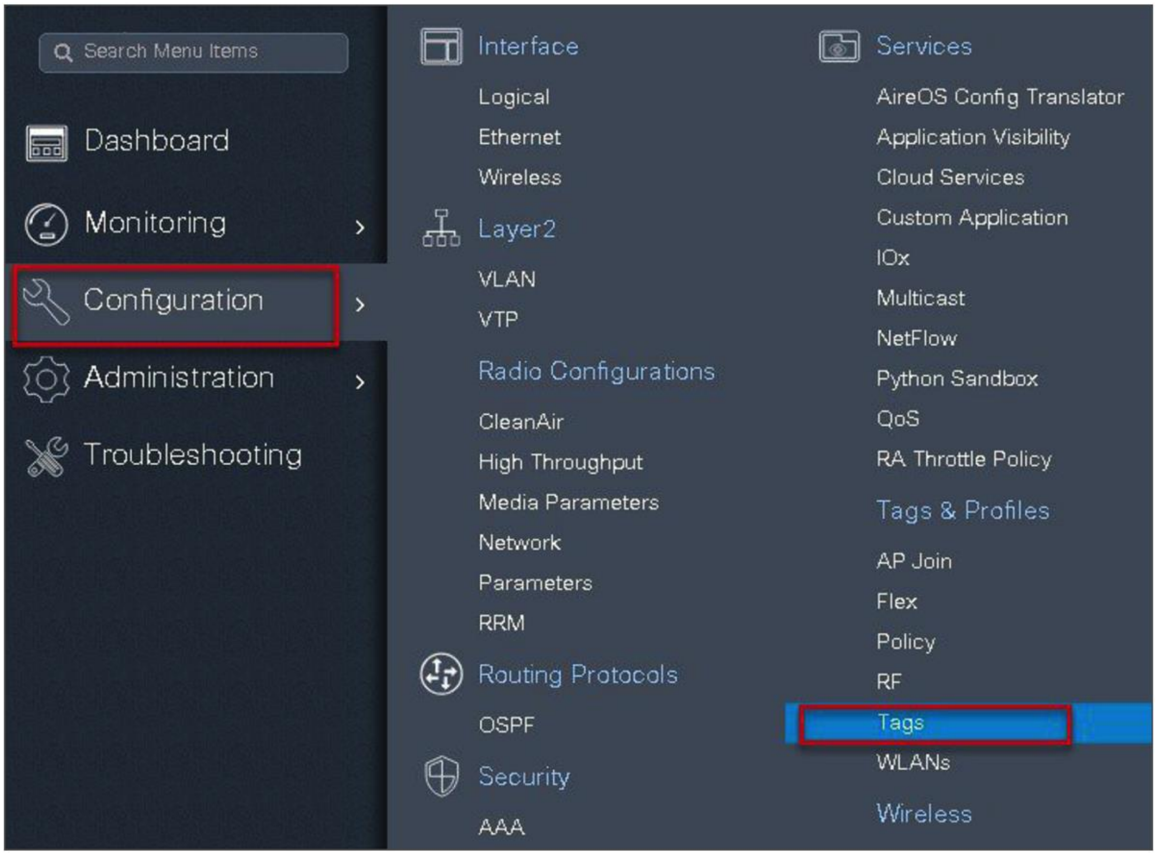
Air Time Fairness Policies

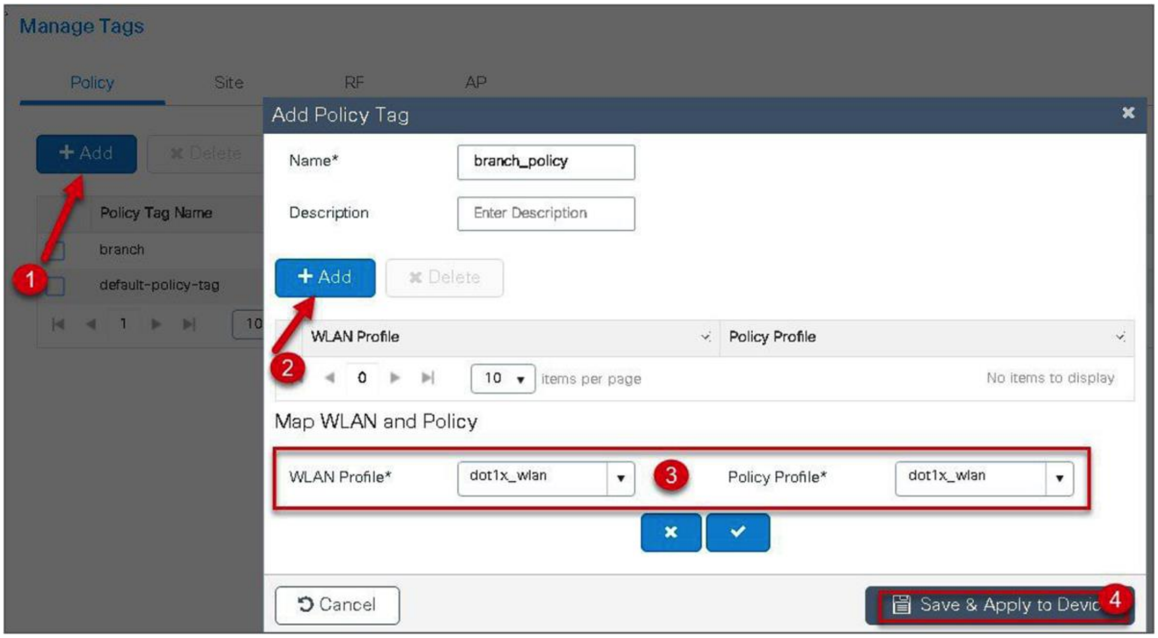
2.4 GHz Policy: Search or Select ▾

5 GHz Policy: Search or Select ▾

Step 10. Map the WLAN to the policy profile.

Navigate to Configuration > Tag and create a policy tag mapping the WLAN and policy profile.





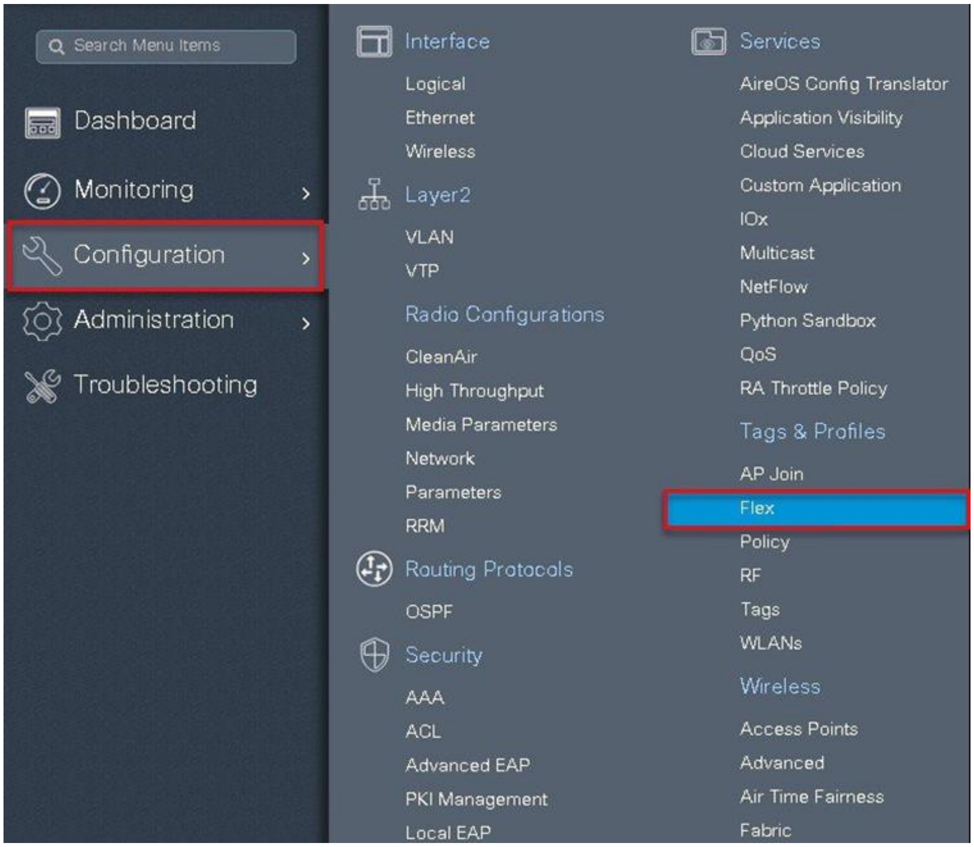
Name* branch_policy

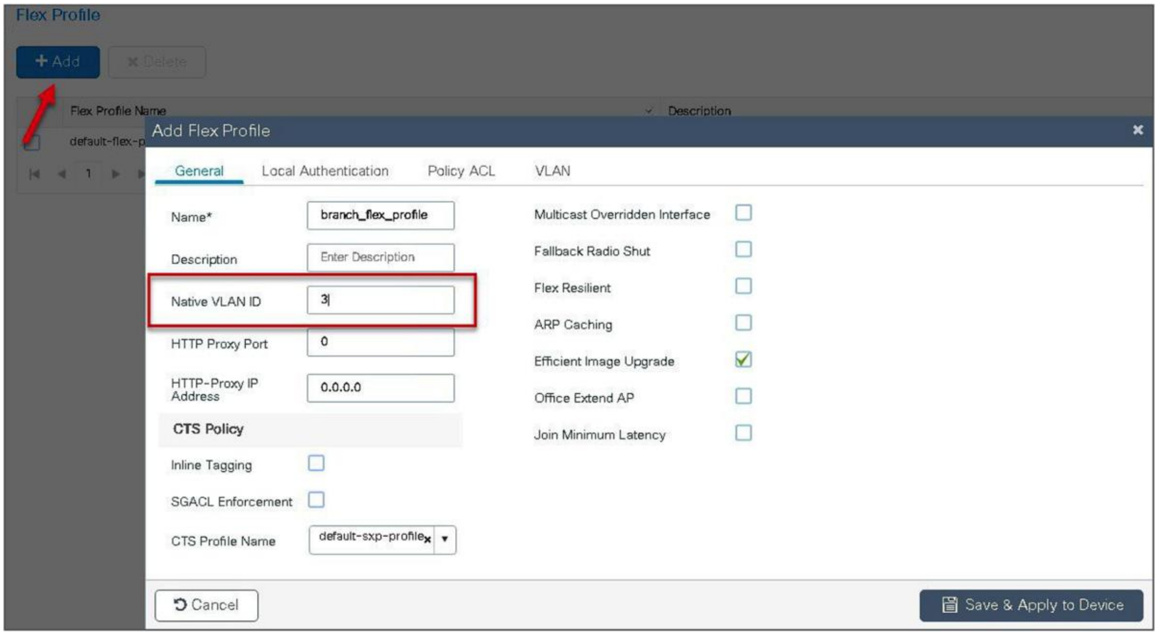
Description Enter Description

WLAN Profile* dot1x_wlan

Policy Profile* dot1x_wlan

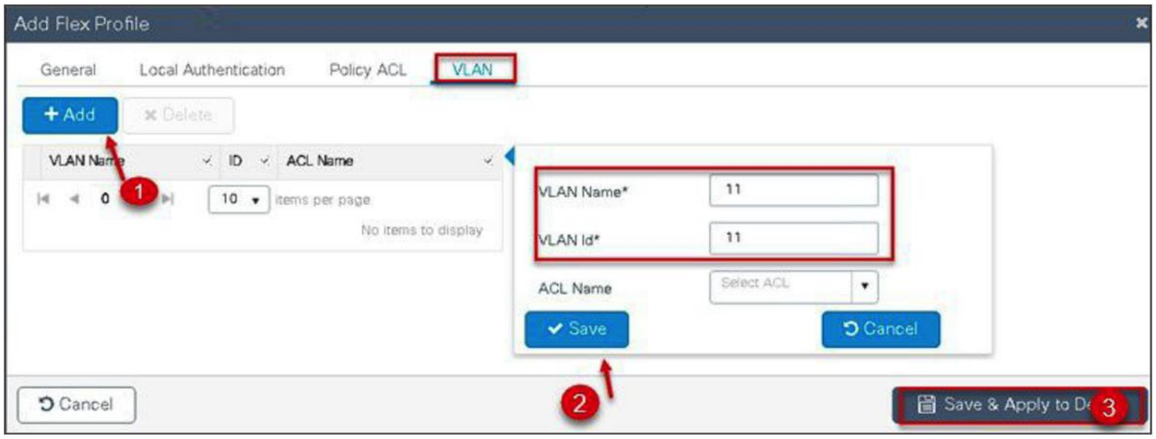
Step 11. Create a flex profile and define a VLAN on the flex profile returned by the AAA radius server.





Add Flex Profile

Name*	branch_flex_profile	Multicast Overridden Interface	□
Description	Enter Description	Fallback Radio Shut	□
Native VLAN ID	3	Flex Resilient	□
HTTP Proxy Port	0	ARP Caching	□
HTTP-Proxy IP Address	0.0.0.0	Efficient Image Upgrade	☑
CTS Policy		Office Extend AP	□
Inline Tagging	□	Join Minimum Latency	□
SGACL Enforcement	□		
CTS Profile Name	default-sxp-profile		



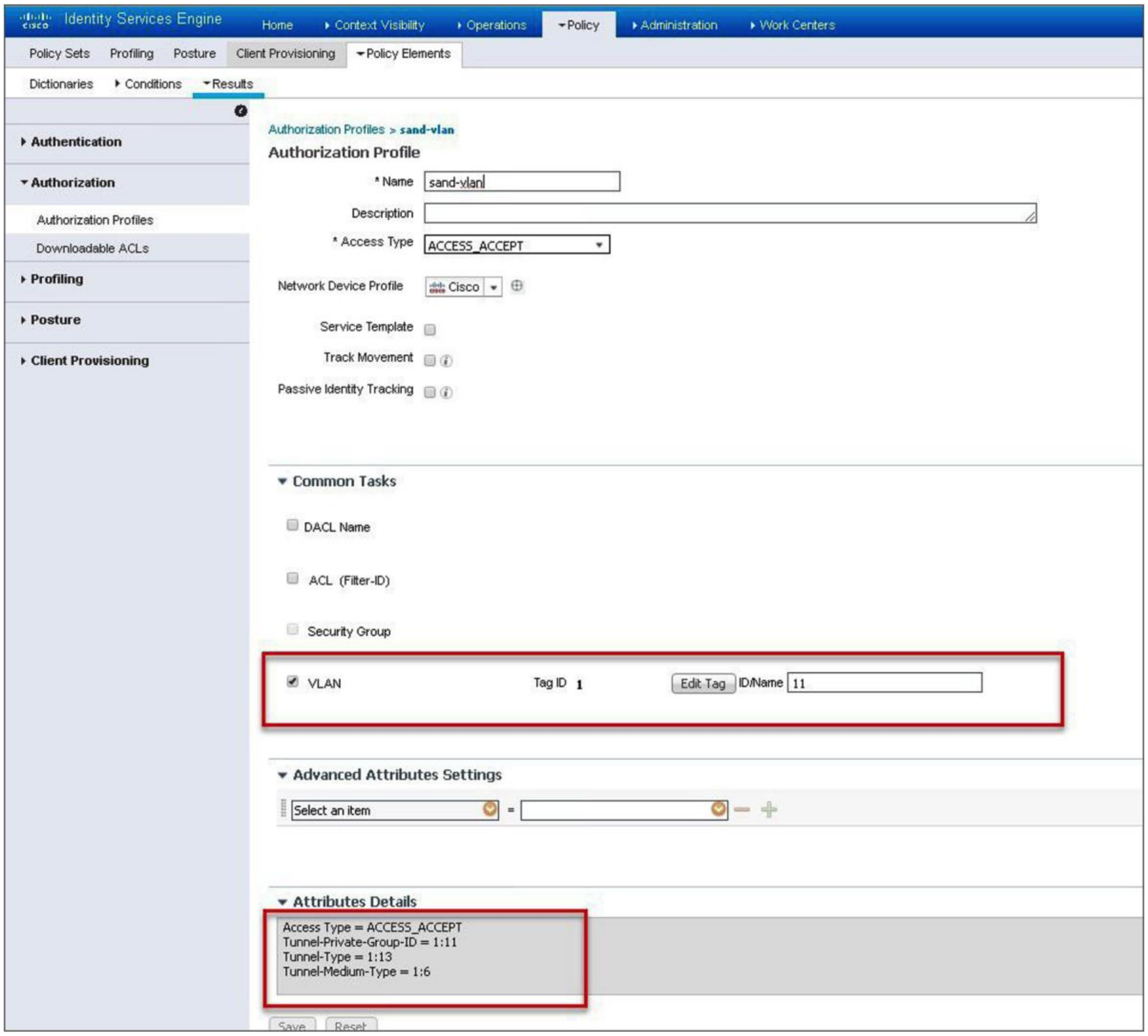
VLAN Name* 11

VLAN Id* 11

ACL Name Select ACL

Step 12. Create an authorization profile on the ISE to override the VLAN.

Create the respective authorization rules to return the authorization profile as part of access accept.



Authorization Profiles > sand-vlan

Authorization Profile

* Name sand-vlan

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

Common Tasks

□ DACL Name

□ ACL (Filter-ID)

□ Security Group

☑ VLAN Tag ID 1 ID/Name 11

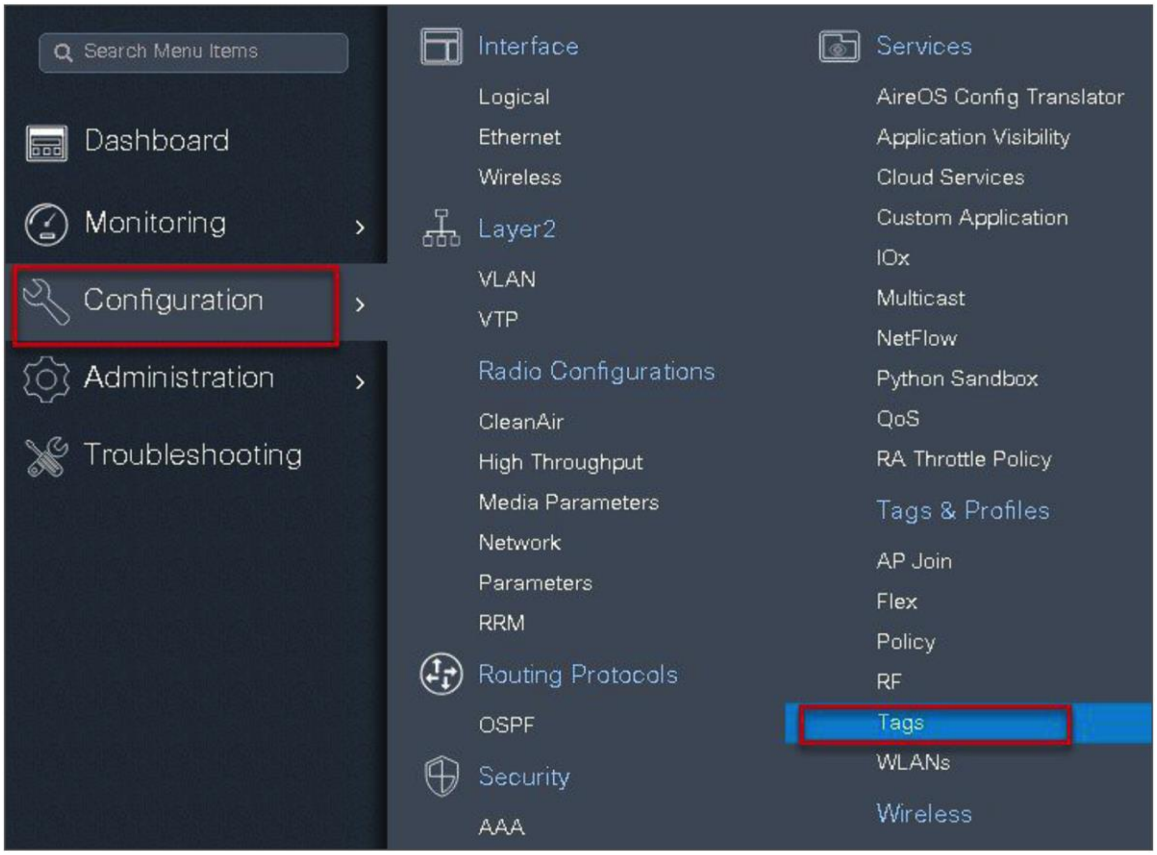
Advanced Attributes Settings

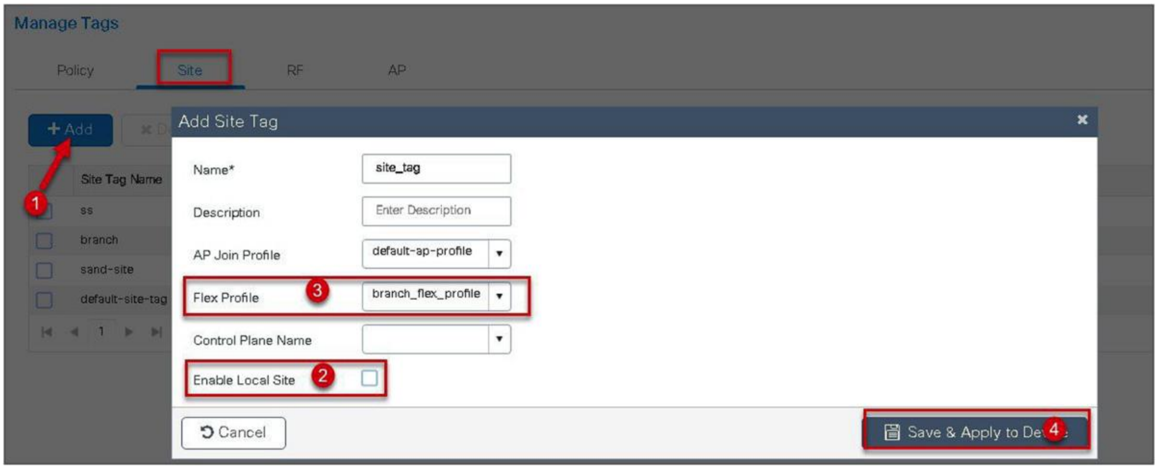
Select an item =

Attributes Details

```
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:11
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6
```

Step 13. Create a site tag and map the flex profile on the site tag.



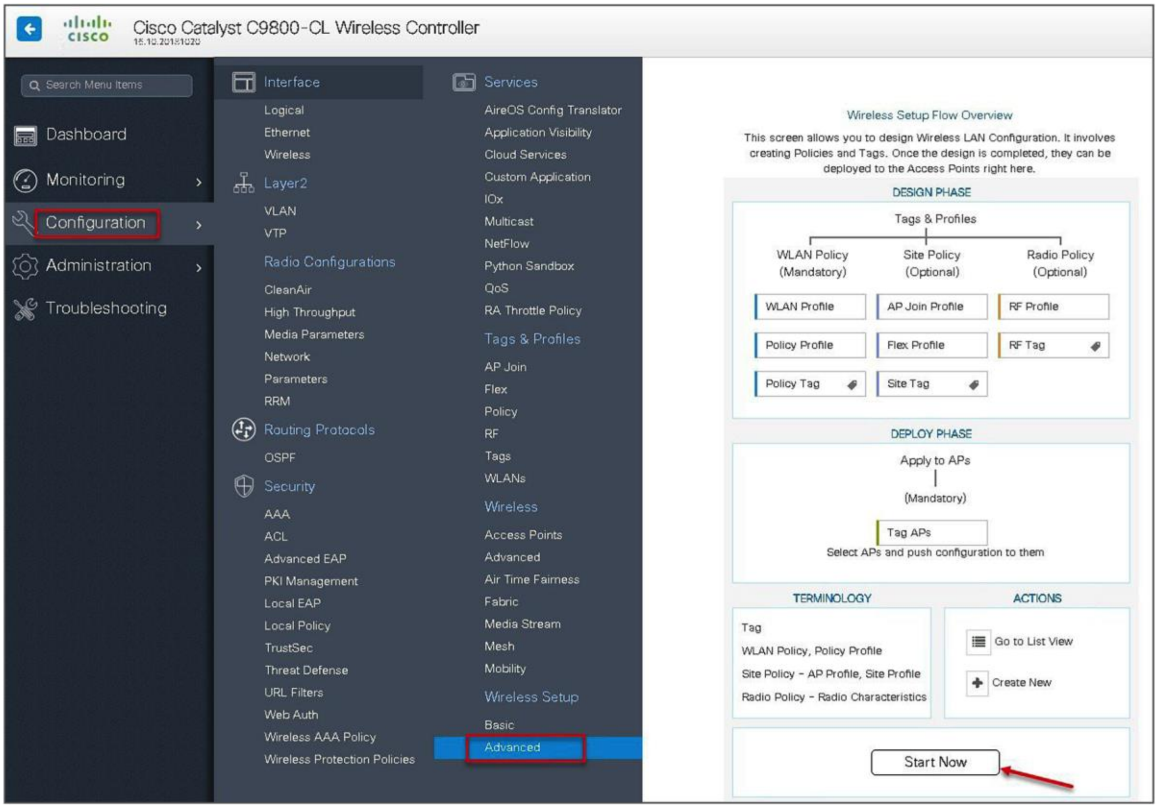


Name*	site_tag
Description	Enter Description
AP Join Profile	default-ap-profile ▾
Flex Profile	branch_flex_profile ▾
Control Plane Name	▾
Enable Local Site	□

Step 14. Map the policy site tag and RF tag on the AP using the advanced config wizard.

Assigning a site tag on an AP would result in AP reboot due to conversion to FlexConnect mode. The reboot is avoided if the AP is already in FlexConnect mode.

Navigate to Configuration > Wireless Setup > Advanced.



Wireless Setup Flow Overview

This screen allows you to design Wireless LAN Configuration. It involves creating Policies and Tags. Once the design is completed, they can be deployed to the Access Points right here.

Select APs and push configuration to them

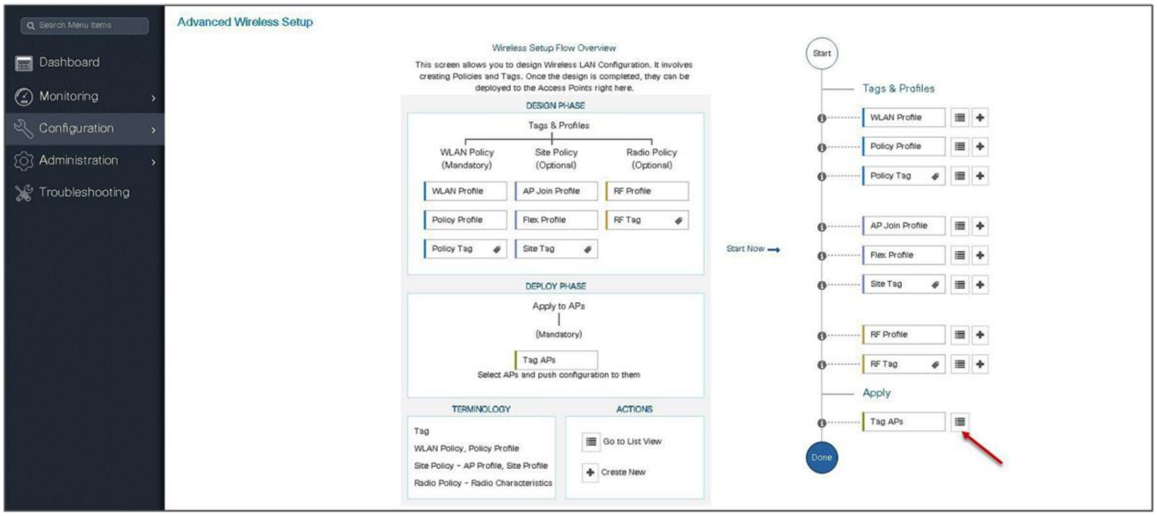
TERMINOLOGY

Tag

WLAN Policy, Policy Profile

Site Policy - AP Profile, Site Profile

Radio Policy - Radio Characteristics



Wireless Setup Flow Overview

This screen allows you to design Wireless LAN Configuration. It involves creating Policies and Tags. Once the design is completed, they can be deployed to the Access Points right here.

Select APs and push configuration to them

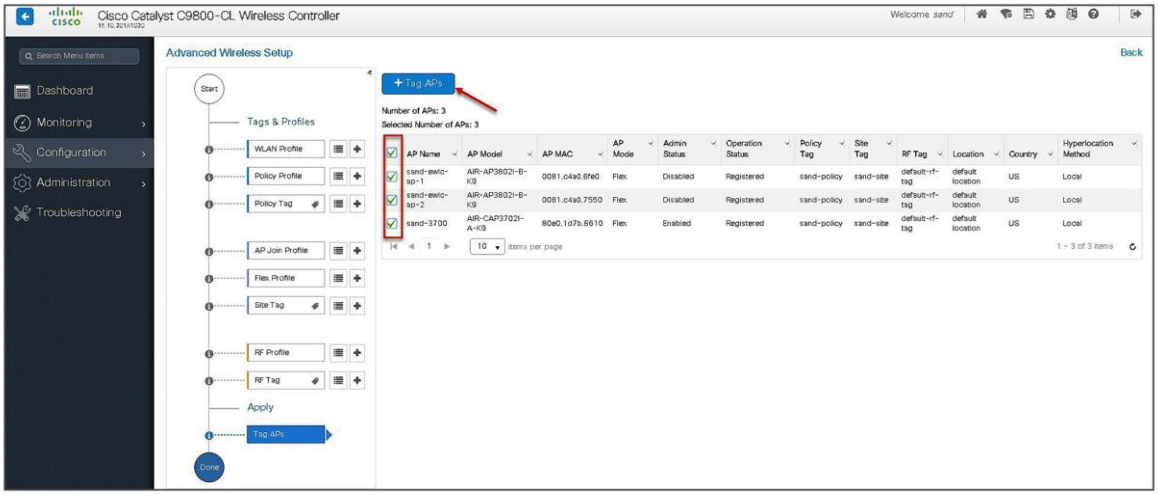
TERMINOLOGY

Tag

WLAN Policy, Policy Profile

Site Policy - AP Profile, Site Profile

Radio Policy - Radio Characteristics

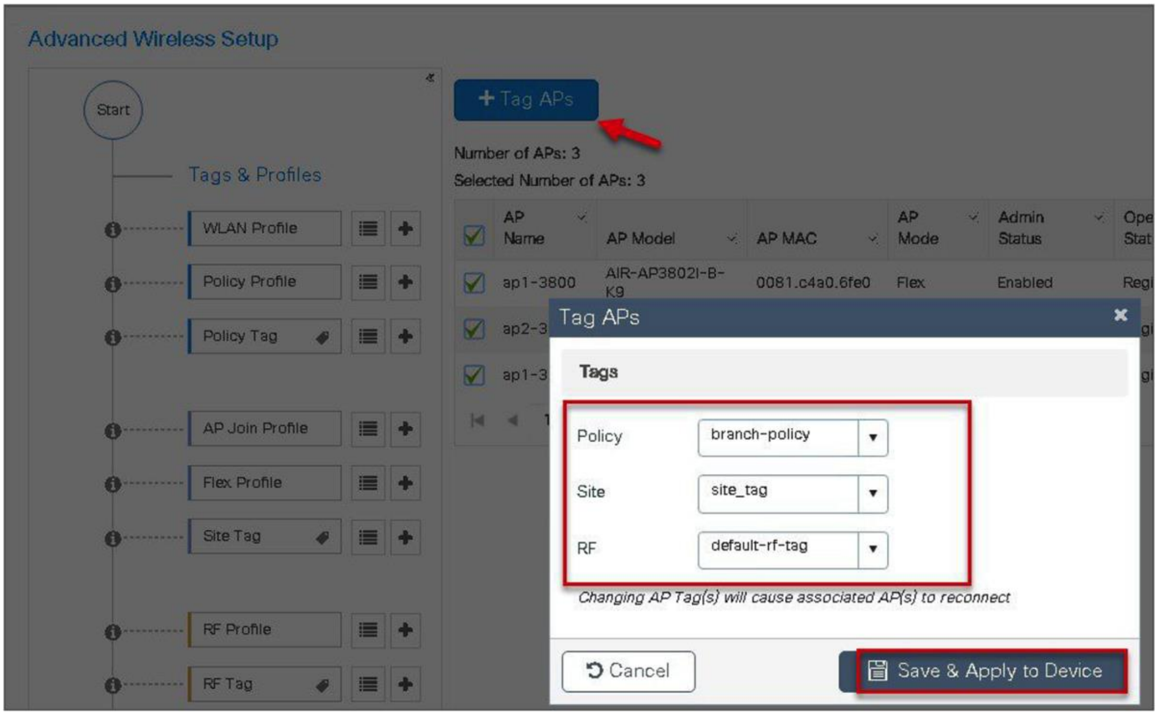


Number of APs: 3

Selected Number of APs: 3

☑	AP Name	AP Model	AP MAC	AP Mode	Admin Status	Operation Status	Policy Tag	Site Tag	RF Tag	Location	Country	Hyperlocation Method
☑	sand-ewlc-ap-1	AIR-AP3802I-B-K9	0081.c4a0.6fe0	Flex	Disabled	Registered	sand-policy	sand-site	default-rf-tag	default location	US	Local
☑	sand-ewlc-ap-2	AIR-AP3802I-B-K9	0081.c4a0.7550	Flex	Disabled	Registered	sand-policy	sand-site	default-rf-tag	default location	US	Local
☑	sand-3700	AIR-CAP3702I-A-K9	80e0.1d7b.8610	Flex	Enabled	Registered	sand-policy	sand-site	default-rf-tag	default location	US	Local

10 items per page 1 - 3 of 3 items



Number of APs: 3

Selected Number of APs: 3

☑	AP Name	AP Model	AP MAC	AP Mode	Admin Status	Ope Stat
☑	ap1-3800	AIR-AP3802I-B-K9	0081.c4a0.6fe0	Flex	Enabled	Regi
☑	ap2-3					gi
☑	ap1-3					gi

Tag APs

Tags

Policy: branch-policy

Site: site_tag

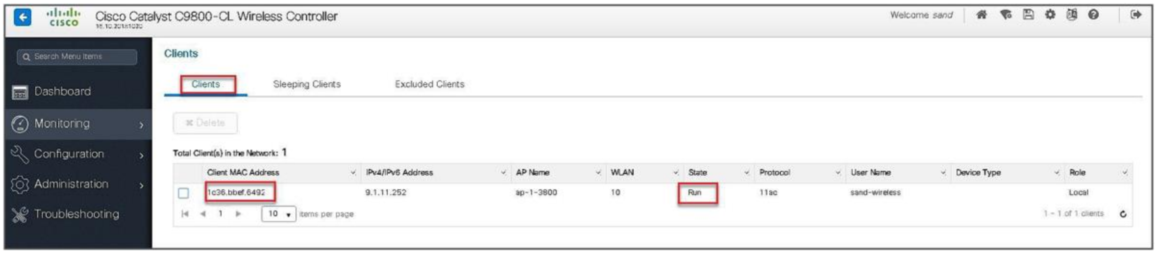
RF: default-rf-tag

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

Step 15. Associate a client on the WLAN and authenticate using the username configured in the AAA server in order to return the AAA VLAN as an attribute.

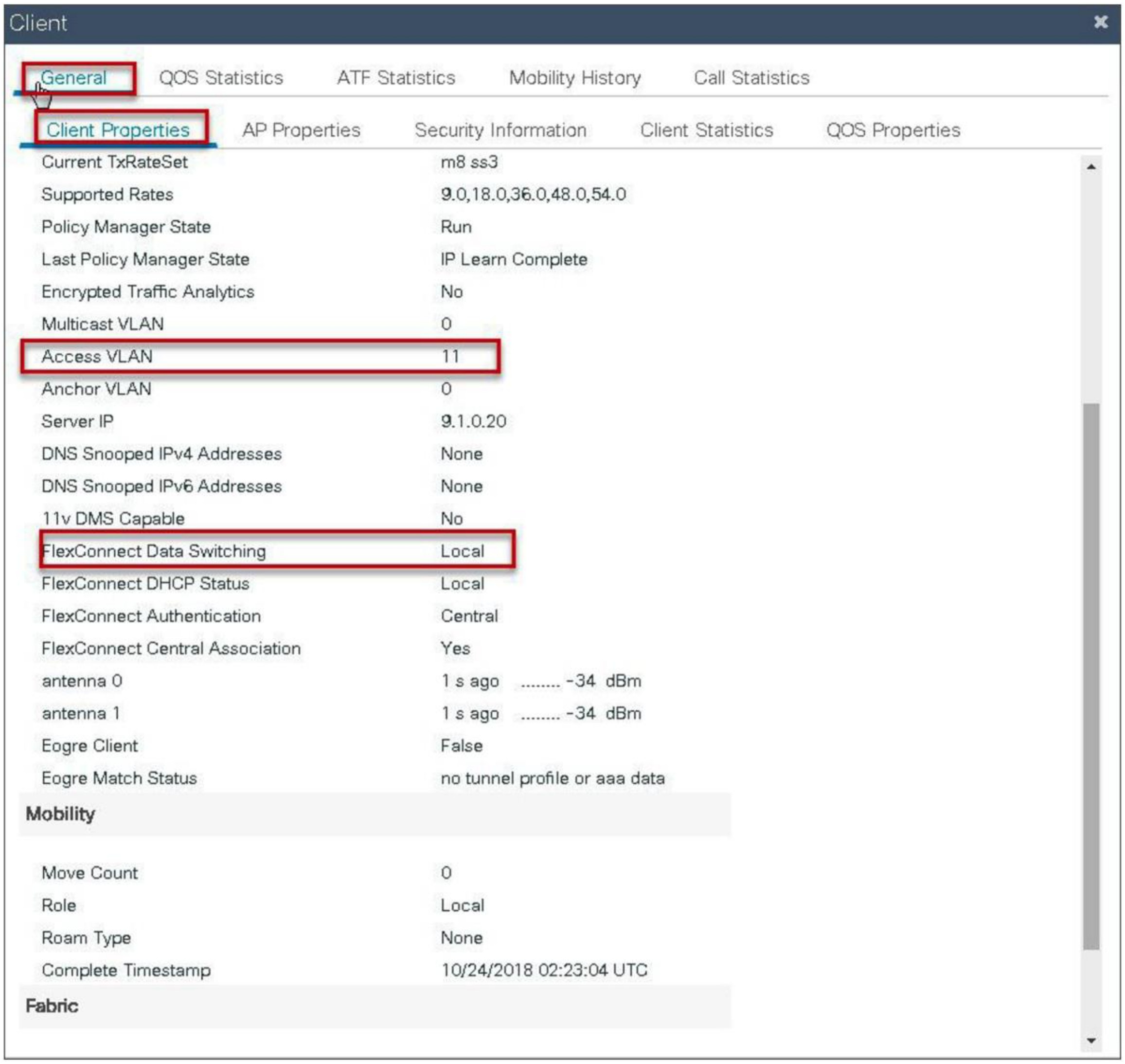
Verify the client connectivity by navigating to Monitoring > Wireless > Clients and verify the access VLAN the client is mapped to.

In this step, the AAA returns VLAN 11, which is present in the AP database results in the local-switched WLAN. Double-click on the client MAC to open the details of the client session.



Total Client(s) in the Network: 1

	Client MAC Address	IPv4/IPv6 Address	AP Name	WLAN	State	Protocol	User Name	Device Type	Role
□	1c36.bbef.6492	9.1.11.252	ap-1-3800	10	Run	11ac	sand-wireless		Local

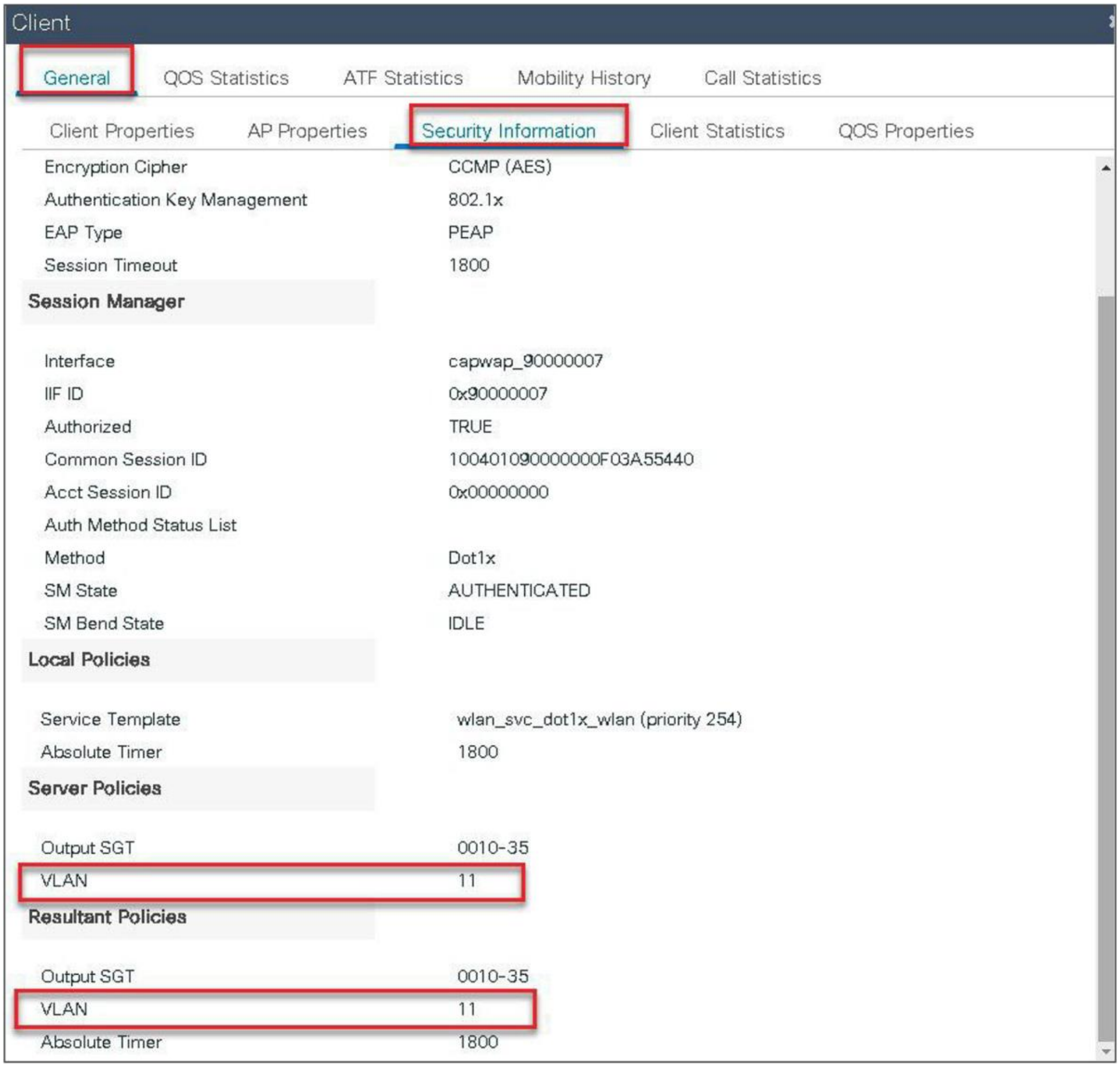


Current TxRateSet	m8 ss3
Supported Rates	9.0,18.0,36.0,48.0,54.0
Policy Manager State	Run
Last Policy Manager State	IP Learn Complete
Encrypted Traffic Analytics	No
Multicast VLAN	0
Access VLAN	11
Anchor VLAN	0
Server IP	9.1.0.20
DNS Snooped IPv4 Addresses	None
DNS Snooped IPv6 Addresses	None
11v DMS Capable	No
FlexConnect Data Switching	Local
FlexConnect DHCP Status	Local
FlexConnect Authentication	Central
FlexConnect Central Association	Yes
antenna 0	1 s ago .... -34 dBm
antenna 1	1 s ago .... -34 dBm
Eogre Client	False
Eogre Match Status	no tunnel profile or aaa data

Mobility

Move Count	0
Role	Local
Roam Type	None
Complete Timestamp	10/24/2018 02:23:04 UTC

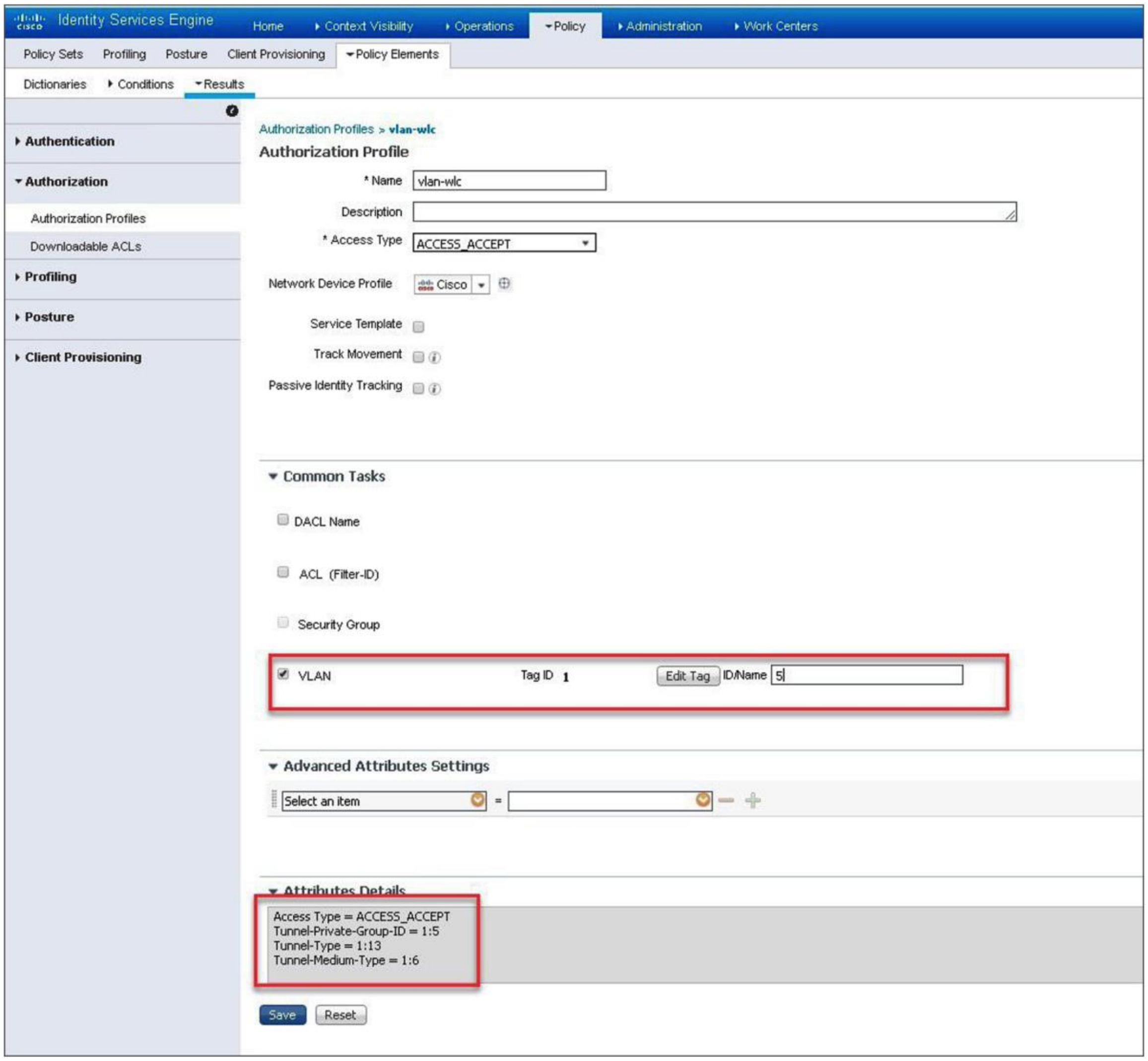
Fabric



Encryption Cipher	CCMP (AES)
Authentication Key Management	802.1x
EAP Type	PEAP
Session Timeout	1800
Session Manager	
Interface	capwap_90000007
IIF ID	0x90000007
Authorized	TRUE
Common Session ID	100401090000000F03A55440
Acct Session ID	0x00000000
Auth Method Status List	
Method	Dot1x
SM State	AUTHENTICATED
SM Bend State	IDLE
Local Policies	
Service Template	wlan_svc_dot1x_wlan (priority 254)
Absolute Timer	1800
Server Policies	
Output SGT	0010-35
VLAN	11
Resultant Policies	
Output SGT	0010-35
VLAN	11
Absolute Timer	1800

Step 16. Create an authorization profile to return a VLAN that is not present on the AP database but on the WLC.

In this example, VLAN 5 is present on the WLC and not on the AP database, which results in the WLAN being central switched.



Authorization Profile

* Name: vlan-wlc

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

□ DACL Name

□ ACL (Filter-ID)

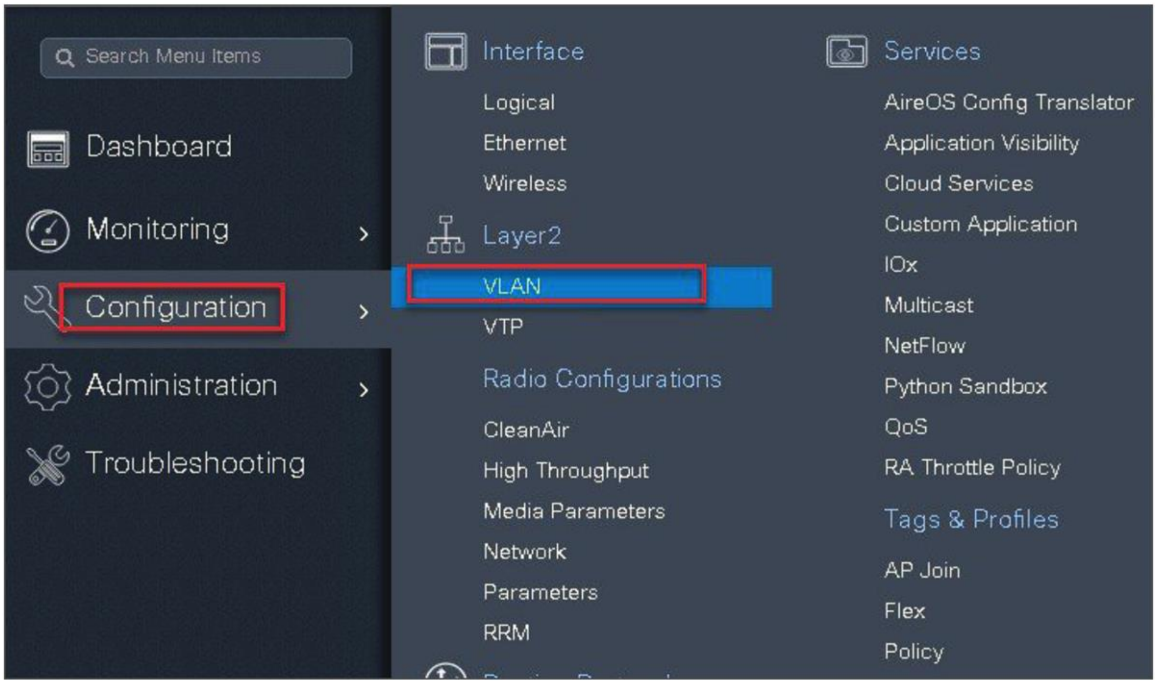
□ Security Group

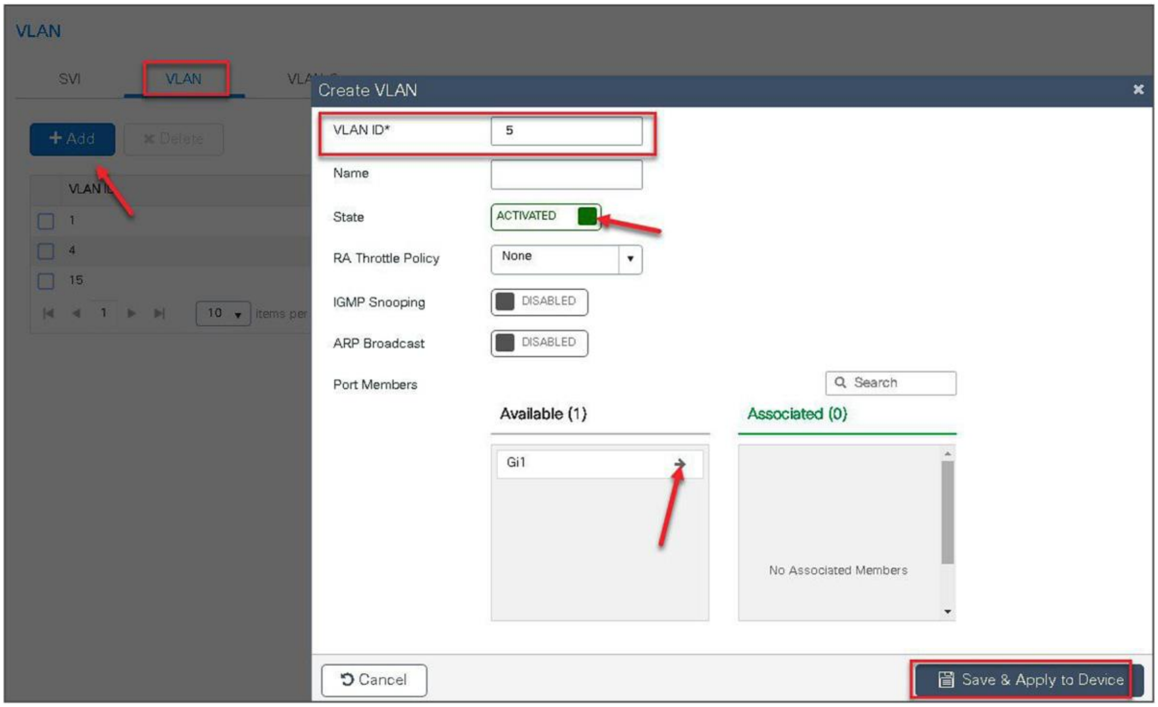
☑ VLAN Tag ID 1 Edit Tag ID/Name 5

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:5
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6

Step 17. Validation on the presence of VLAN 5 on the WLC.

Navigate to Configuration > VLAN.





Create VLAN

VLAN ID* 5

Name

State ACTIVATED

RA Throttle Policy None

IGMP Snooping DISABLED

ARP Broadcast DISABLED

Port Members

Available (1)

Gi1

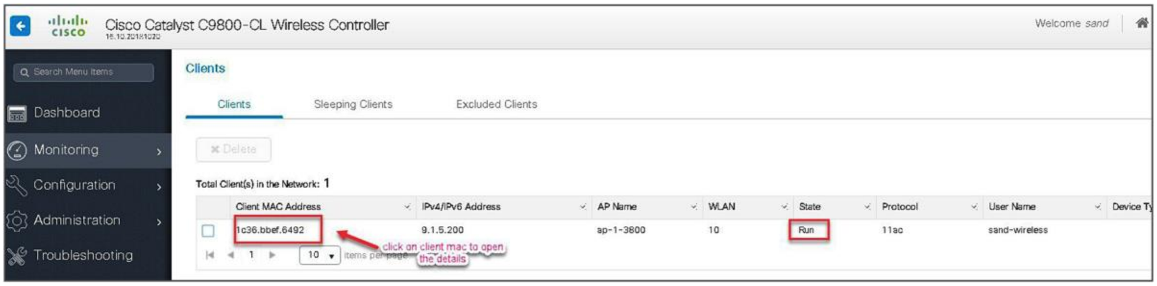
Associated (0)

No Associated Members

Step 18. Associate a client on the WLAN and authenticate using the username configured in the AAA server in order to return the AAA VLAN (VLAN5) as the return attribute.

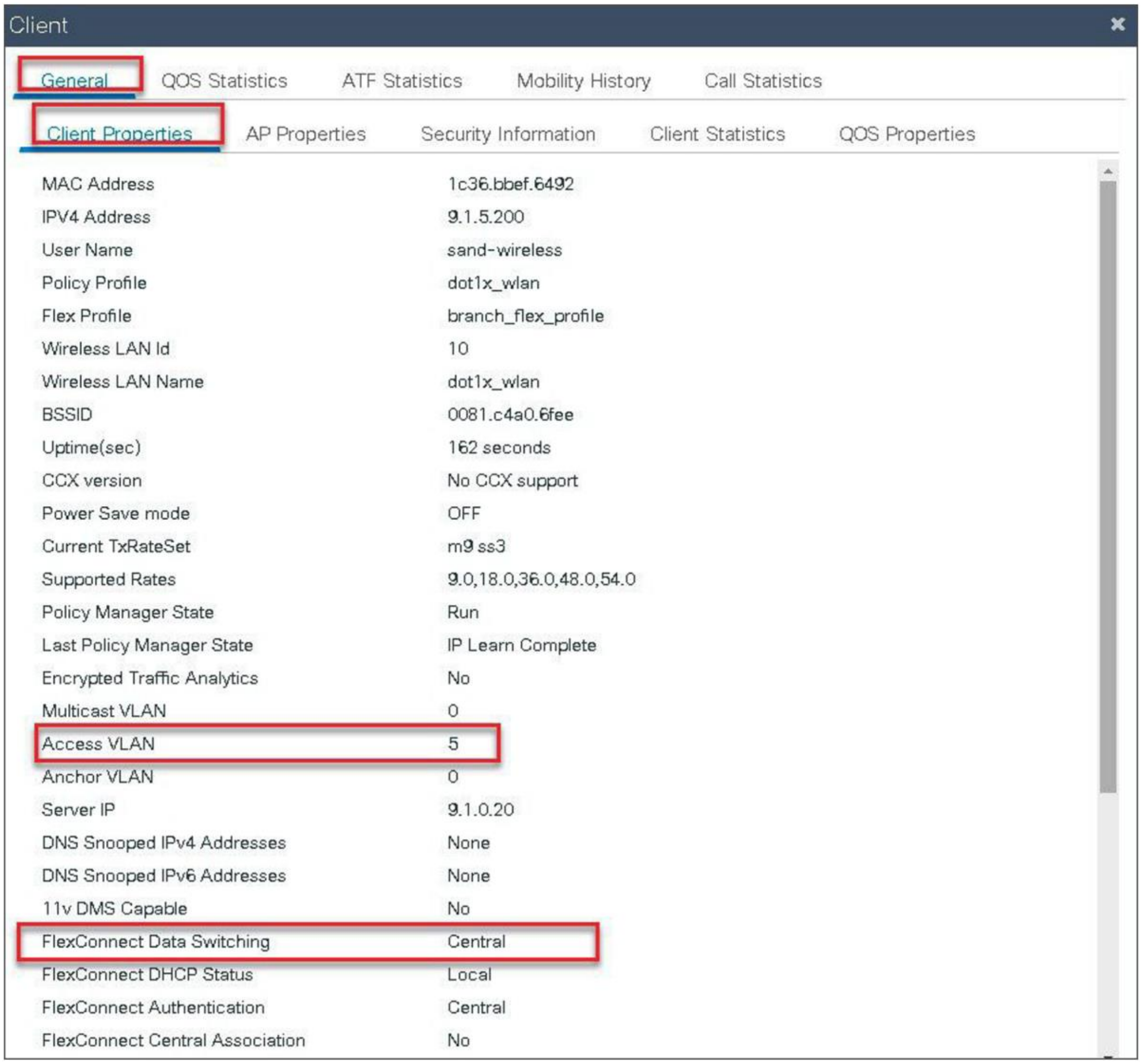
Verify the client connectivity by navigating to Monitoring > Wireless > Clients and verify the access VLAN the client is mapped to and the switching properties for the client.

Double-click on the client MAC to open the details of the client session.

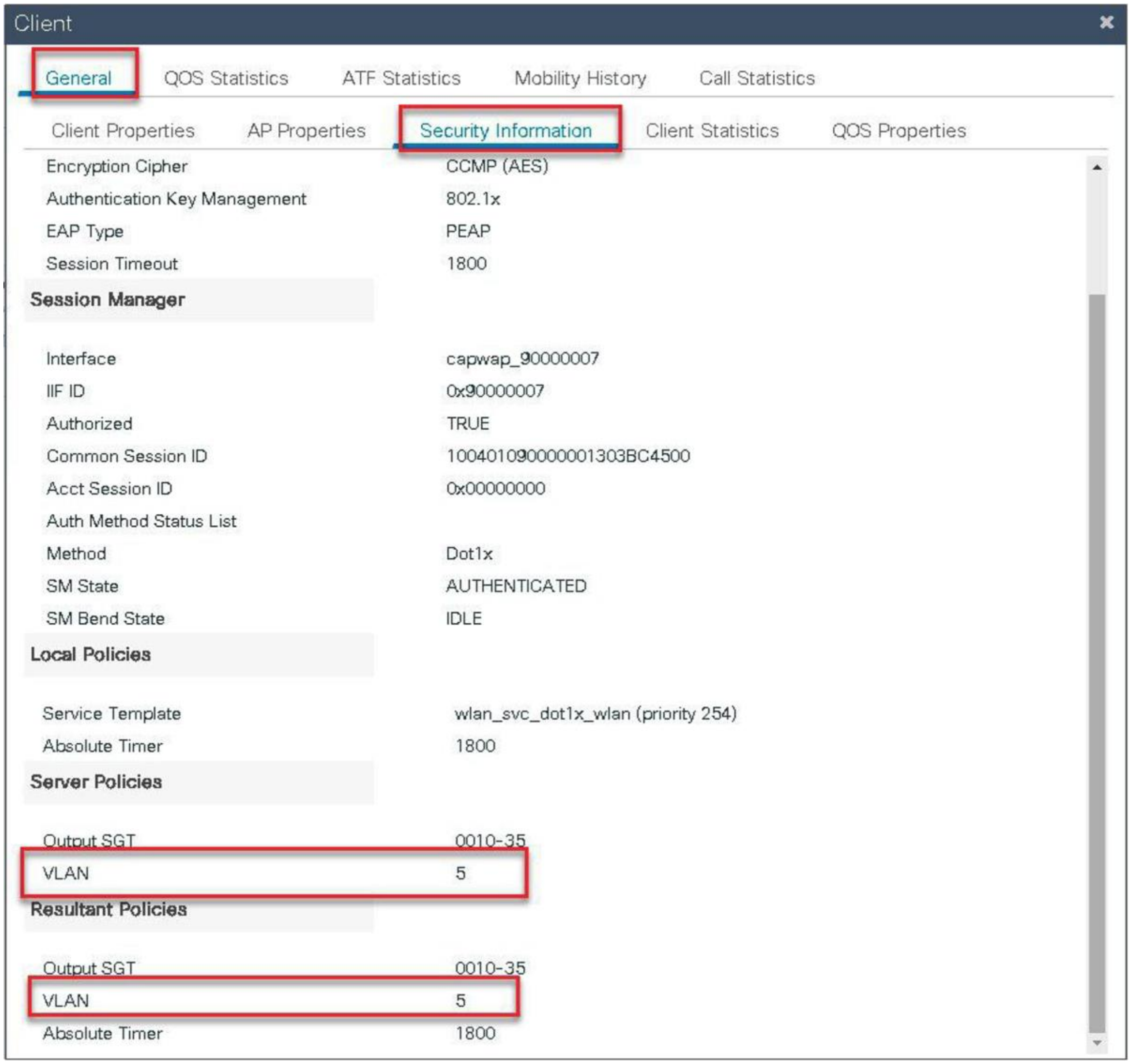


Total Client(s) in the Network: 1

	Client MAC Address	IPv4/IPv6 Address	AP Name	WLAN	State	Protocol	User Name	Device Ty
□	1c36.bbef.6492	9.1.5.200	ap-1-3800	10	Run	11ac	sand-wireless	



MAC Address	1c36.bbef.6492
IPV4 Address	9.1.5.200
User Name	sand-wireless
Policy Profile	dot1x_wlan
Flex Profile	branch_flex_profile
Wireless LAN Id	10
Wireless LAN Name	dot1x_wlan
BSSID	0081.c4a0.6fee
Uptime(sec)	162 seconds
CCX version	No CCX support
Power Save mode	OFF
Current TxRateSet	m9 ss3
Supported Rates	9.0,18.0,36.0,48.0,54.0
Policy Manager State	Run
Last Policy Manager State	IP Learn Complete
Encrypted Traffic Analytics	No
Multicast VLAN	0
Access VLAN	5
Anchor VLAN	0
Server IP	9.1.0.20
DNS Snooped IPv4 Addresses	None
DNS Snooped IPv6 Addresses	None
11v DMS Capable	No
FlexConnect Data Switching	Central
FlexConnect DHCP Status	Local
FlexConnect Authentication	Central
FlexConnect Central Association	No



Encryption Cipher	CCMP (AES)
Authentication Key Management	802.1x
EAP Type	PEAP
Session Timeout	1800
Session Manager	
Interface	capwap_90000007
IIF ID	0x90000007
Authorized	TRUE
Common Session ID	1004010900000001303BC4500
Acct Session ID	0x00000000
Auth Method Status List	
Method	Dot1x
SM State	AUTHENTICATED
SM Bend State	IDLE
Local Policies	
Service Template	wlan_svc_dot1x_wlan (priority 254)
Absolute Timer	1800
Server Policies	
Output SGT	0010-35
VLAN	5
Resultant Policies	
Output SGT	0010-35
VLAN	5
Absolute Timer	1800

Local authentication and backup radius server

In most typical branch deployments, it is easy to foresee that client 802.1X authentication takes place centrally at the WLC located at the data center; however, there arises certain concerns with central authentication at the WLC.

How can wireless clients perform 802.1X authentication and access data center services if the WLC fails?

How can wireless clients perform 802.1X authentication if the WAN link between the branch and data center fails? Is there any impact on branch mobility during WAN failures?

Does the FlexConnect solution provide no operational branch downtime?

FlexConnect local authentication and backup/local radius can address the above concerns by enabling the branch to operate independently in case of a WAN outage or connectivity issue with the controller.

Summary

- The use of local authentication in branch enables resiliency at the branch location by providing wireless access in scenarios where the WAN connectivity is lost with the data center. The AP moves to standalone mode and provides wireless access with authentication for dot1x directed to a radius server available at the branch side.
- The AP can act as a radius server, and this feature is only supported on the Wave 1 APs.
- This feature can be used with central authentication or local authentication. In the central authentication case, the WLC will authenticate the wireless clients as long as the AP is in connected mode.
- Once the AP loses connectivity with the WLC, the AP will move to standalone and authenticate the client locally.
- This feature can be used with local authentication and local switching. In cases where there is a local radius server at the branch, the AP can forward the radius request to the radius server at the branch, thereby avoiding the latency variation caused by the WAN links.
- EAP-LEAP is the only method supported for AP as radius server.

Local authentication with external radius server

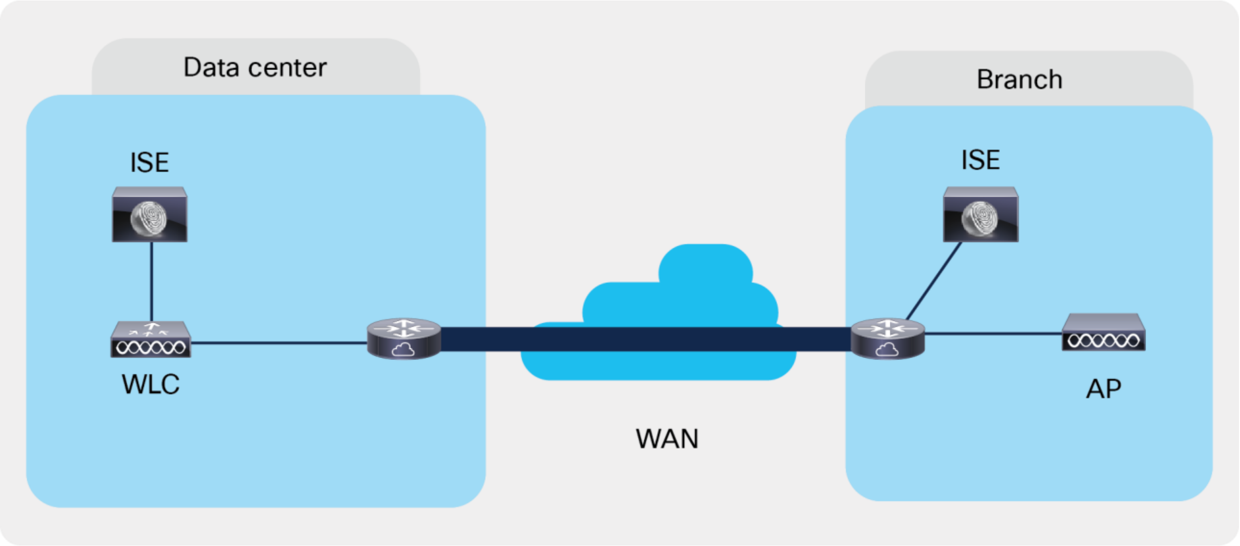


Figure 7.
Local Authentication with External RADIUS server at the Branch

Steps for local authentication and backup radius server

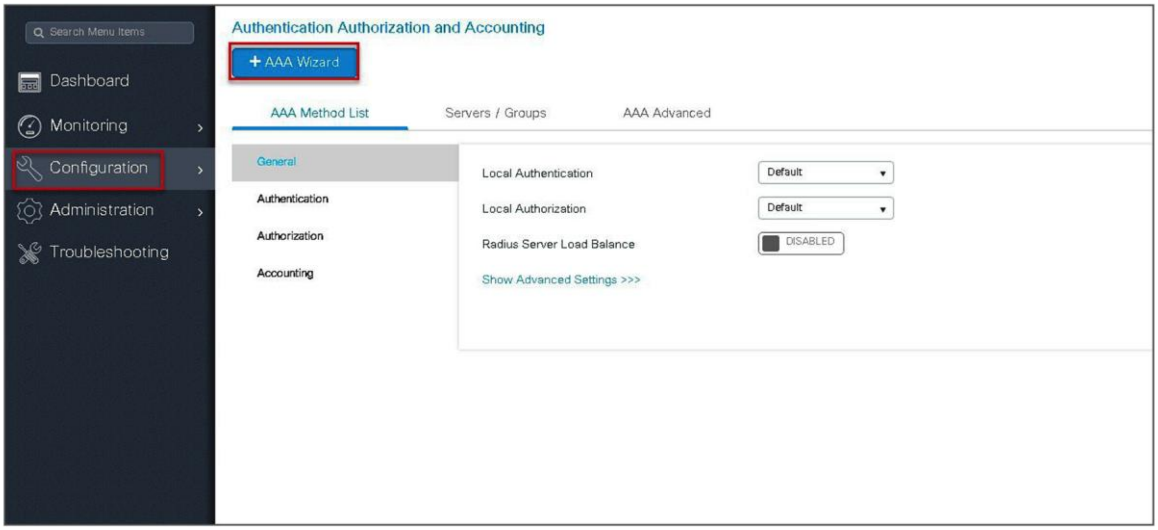
Procedure

Step 1. Define an AAA server. For branch deployment, specify the AAA server used at the branch side.

Navigate to Configuration > Security > AAA and start the AAA wizard.

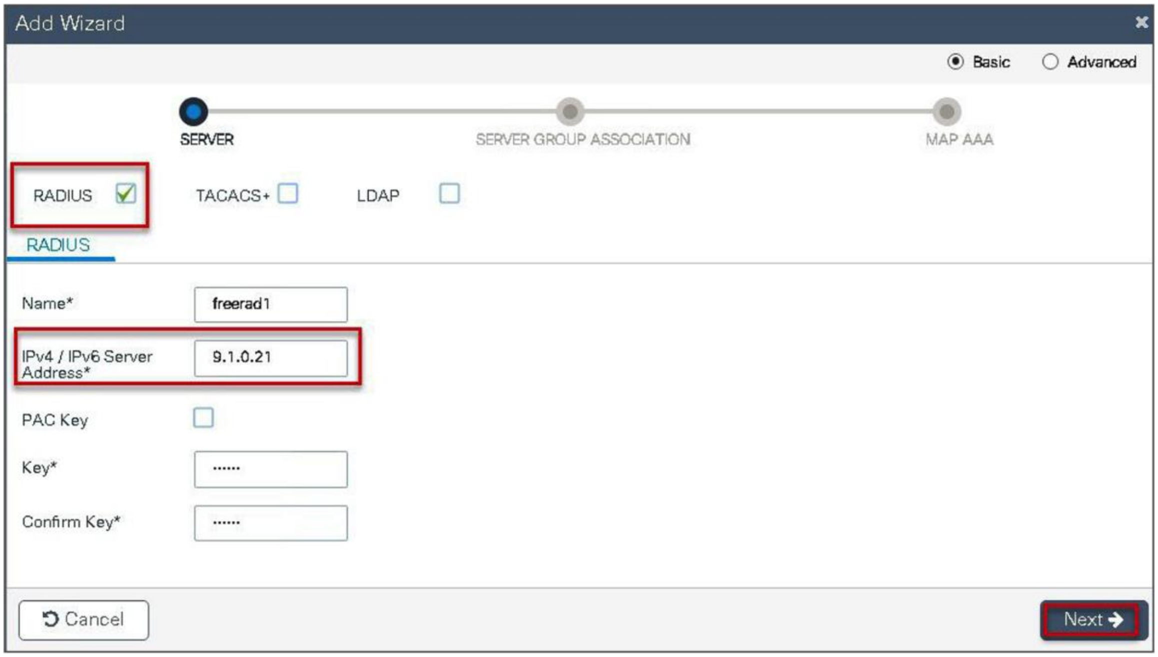
The wizard helps in creating the following flow.

- Create a radius server.
- Create a server group and map the radius server on the server group.
- Map the server for dot1x authentication.



Authentication Authorization and Accounting

Local Authentication	Default
Local Authorization	Default
Radius Server Load Balance	DISABLED

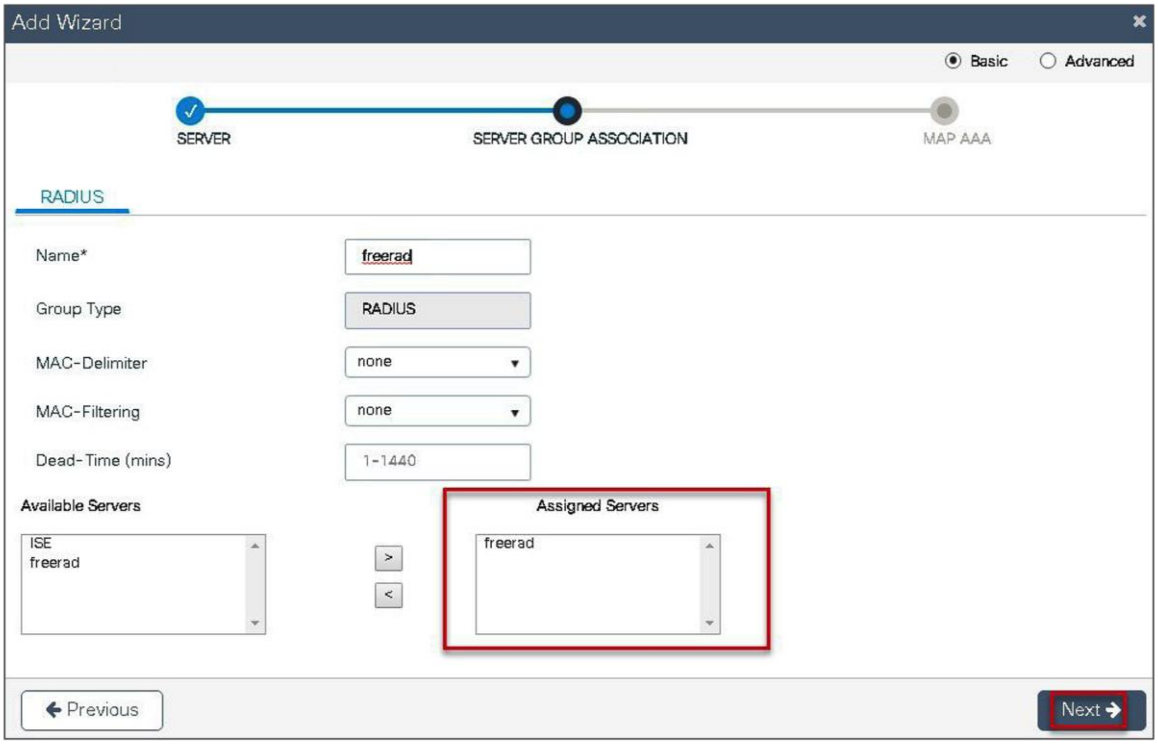


Add Wizard

● Basic ○ Advanced

RADIUS ☑ TACACS+ □ LDAP □

Name*	freerad1
IPv4 / IPv6 Server Address*	9.1.0.21
PAC Key	□
Key*	······
Confirm Key*	······



Add Wizard

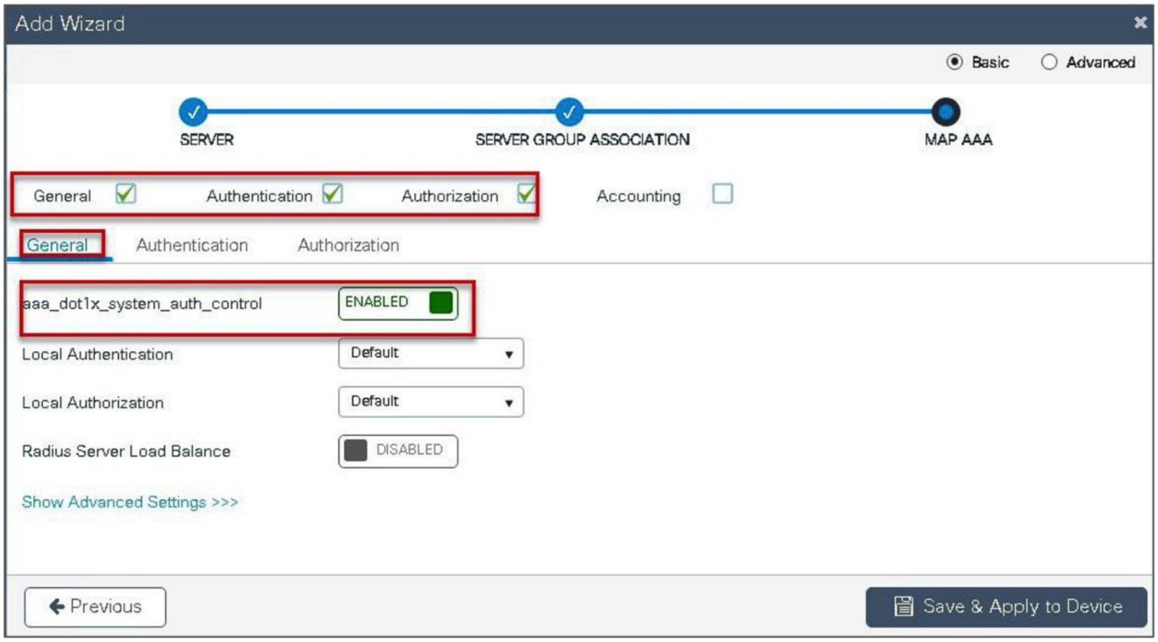
● Basic ○ Advanced

SERVER — SERVER GROUP ASSOCIATION — MAP AAA

RADIUS

Name*	freerad
Group Type	RADIUS
MAC-Delimiter	none
MAC-Filtering	none
Dead-Time (mins)	1-1440

Available Servers	Assigned Servers
ISE freerad	freerad



Add Wizard

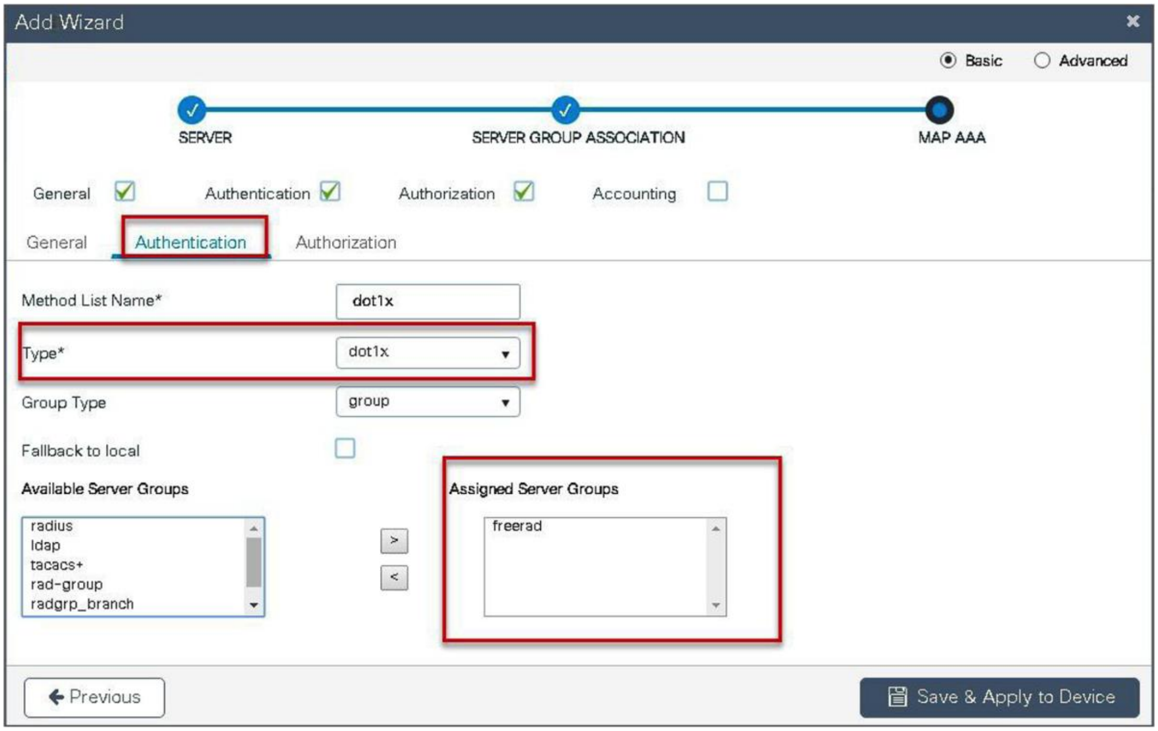
● Basic ○ Advanced

SERVER — SERVER GROUP ASSOCIATION — MAP AAA

General ☑ Authentication ☑ Authorization ☑ Accounting □

General | Authentication | Authorization

aaa_dot1x_system_auth_control	ENABLED
Local Authentication	Default
Local Authorization	Default
Radius Server Load Balance	DISABLED



Method List Name*: dot1x

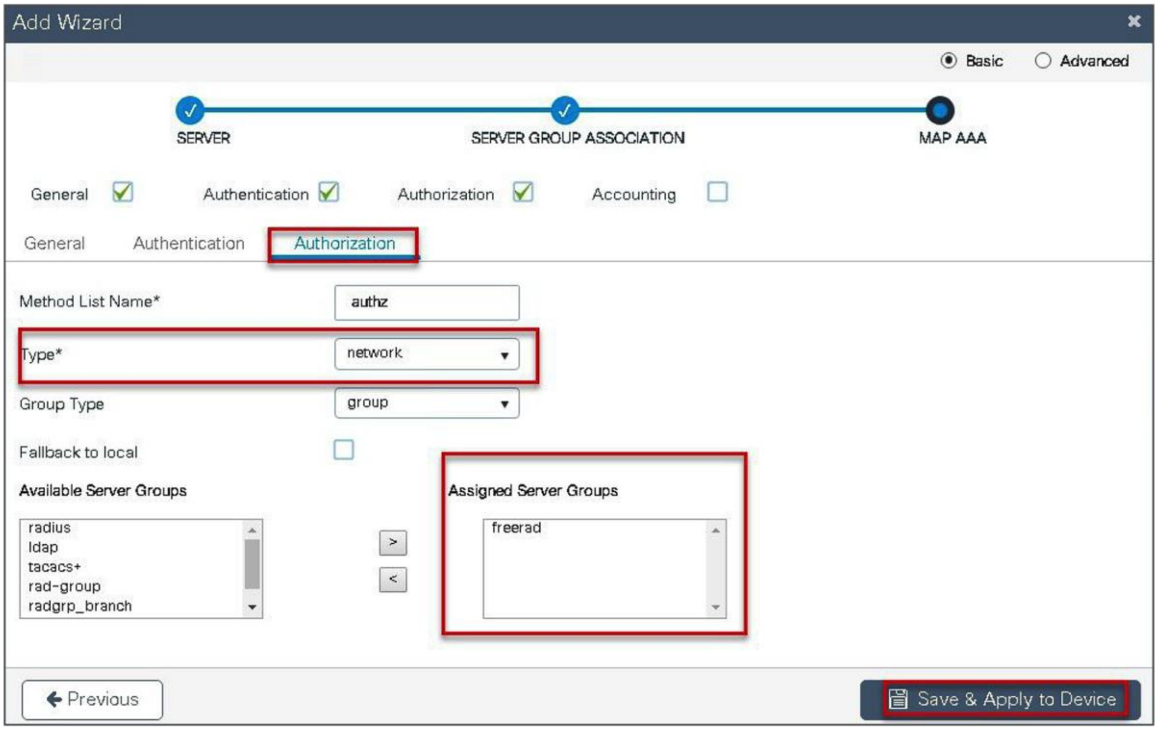
Type*: dot1x

Group Type: group

Fallback to local □

Available Server Groups: radius, ldap, tacacs+, rad-group, radgrp_branch

Assigned Server Groups: freerad



Method List Name*: authz

Type*: network

Group Type: group

Fallback to local □

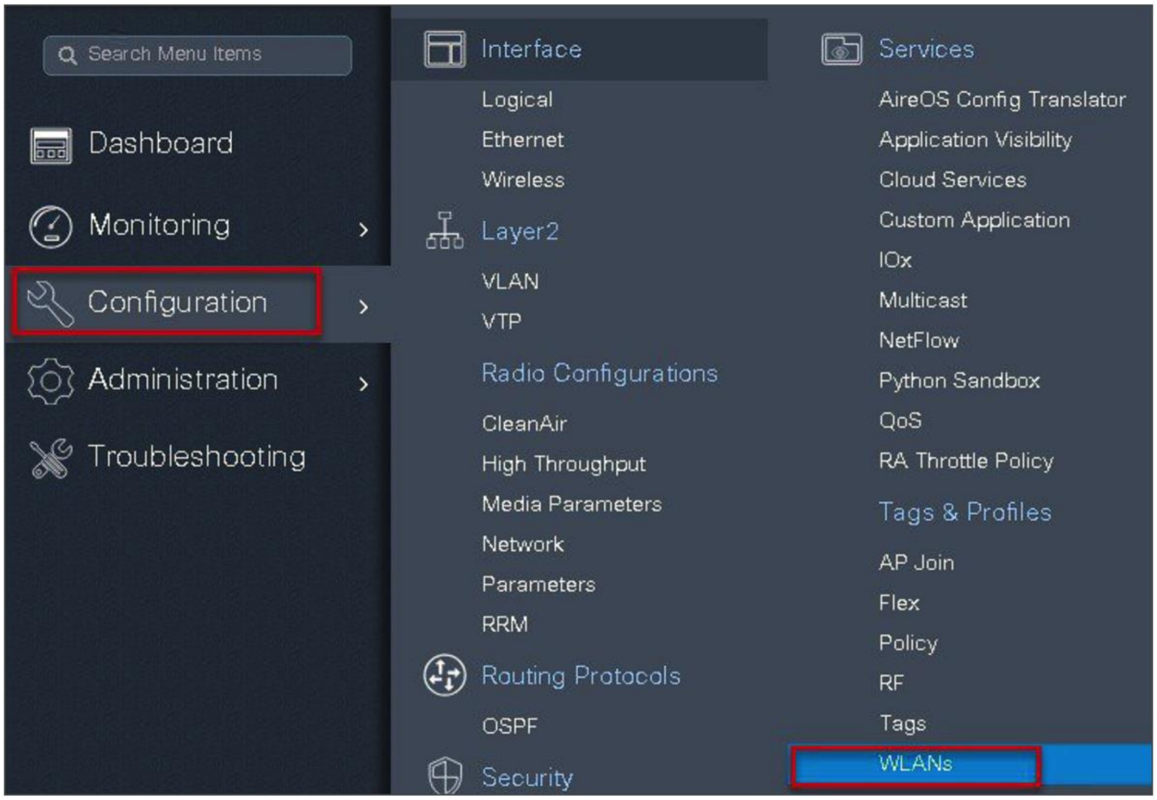
Available Server Groups: radius, ldap, tacacs+, rad-group, radgrp_branch

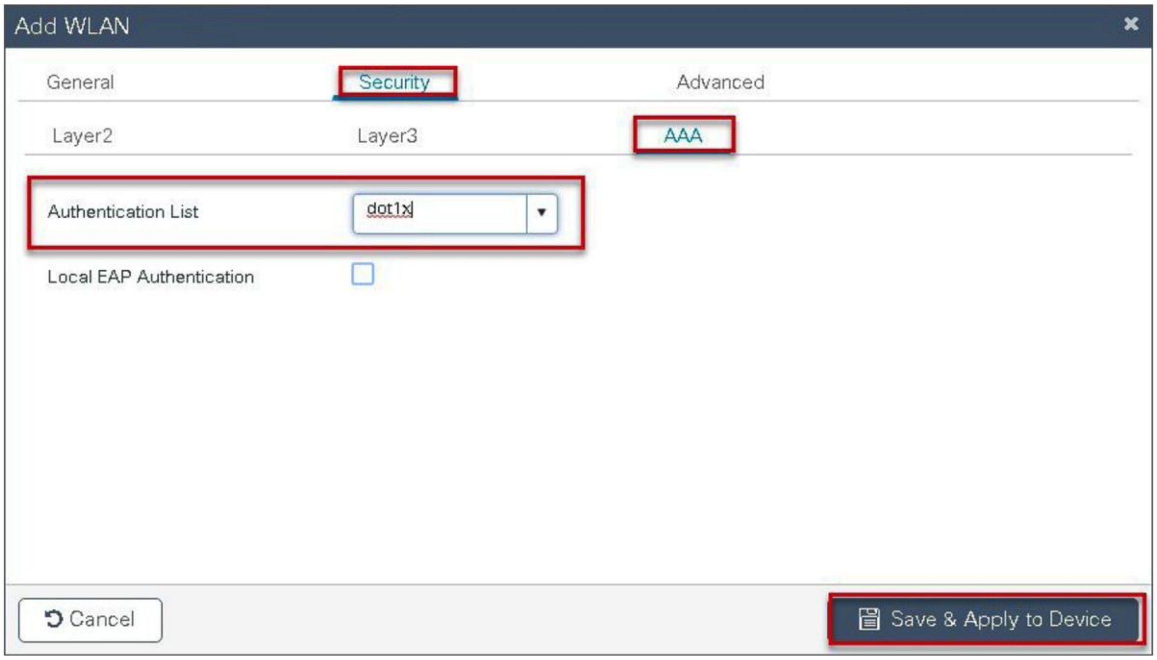
Assigned Server Groups: freerad

Step 2. Create an SSID on the controller for dot1x authentication.

To create an SSID, navigate to Configuration > Tags & Profiles > WLANs.

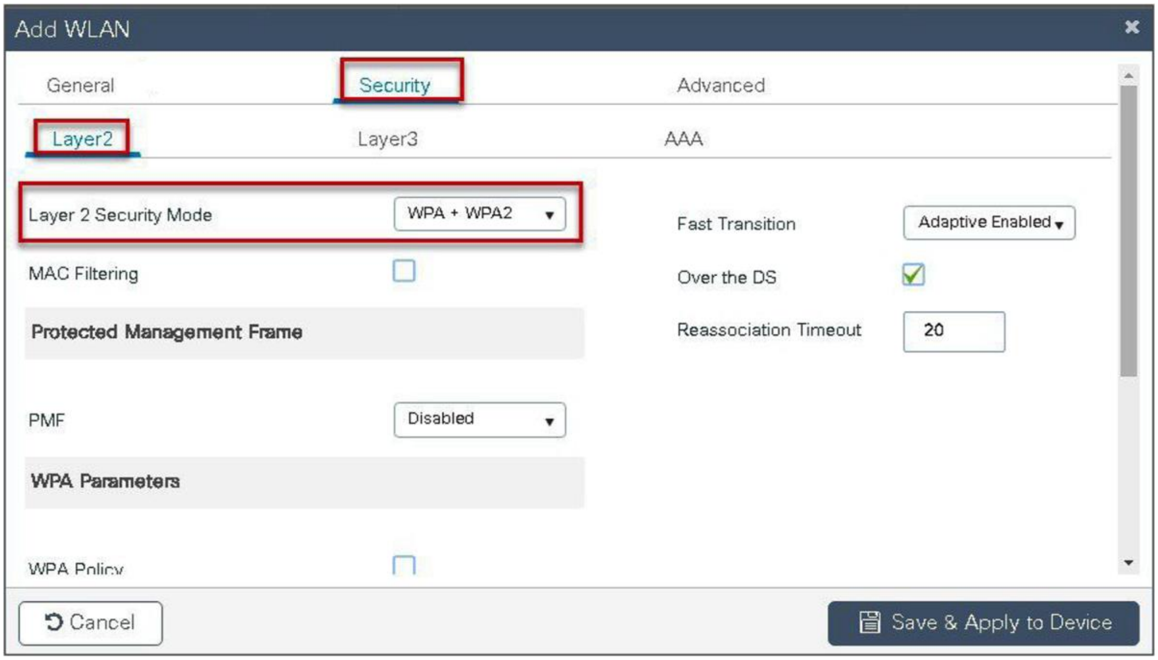
Defines the method list created for dot1x on the WLAN AAA settings.





Authentication List: dot1x

Local EAP Authentication □



Layer 2 Security Mode: WPA + WPA2

MAC Filtering: □

Protected Management Frame

PMF: Disabled

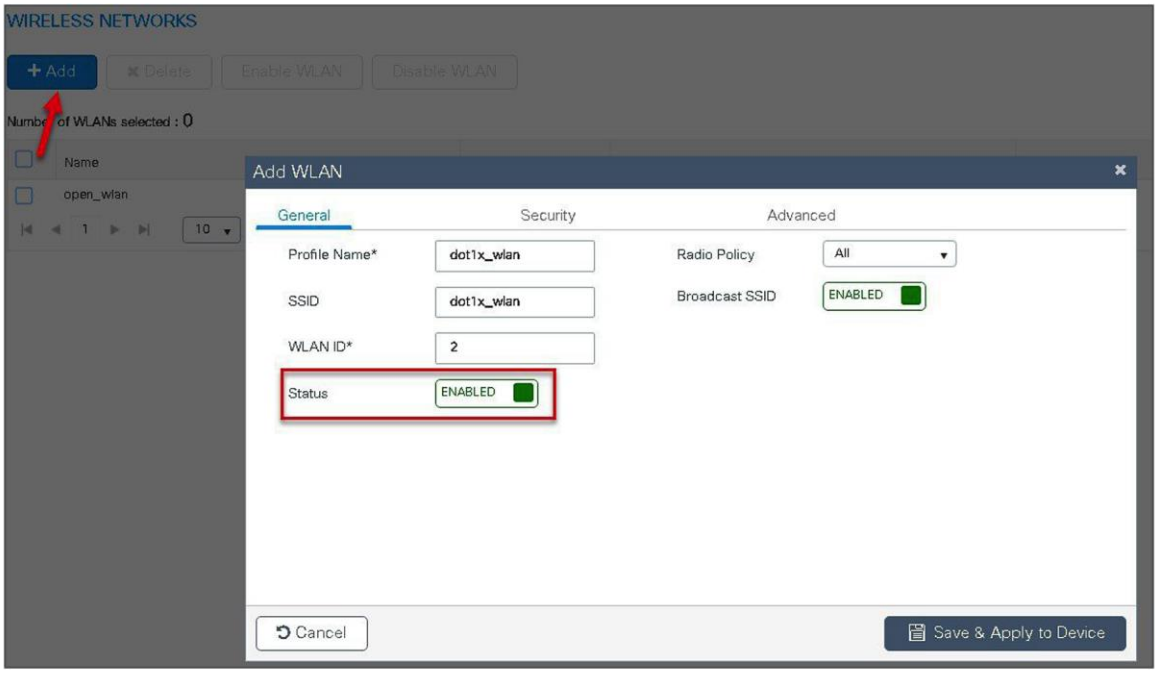
WPA Parameters

WPA Policy: □

Fast Transition: Adaptive Enabled

Over the DS: ☑

Reassociation Timeout: 20



Numbe of WLANs selected : 0

□	Name
□	open_wlan

Profile Name*: dot1x_wlan

SSID: dot1x_wlan

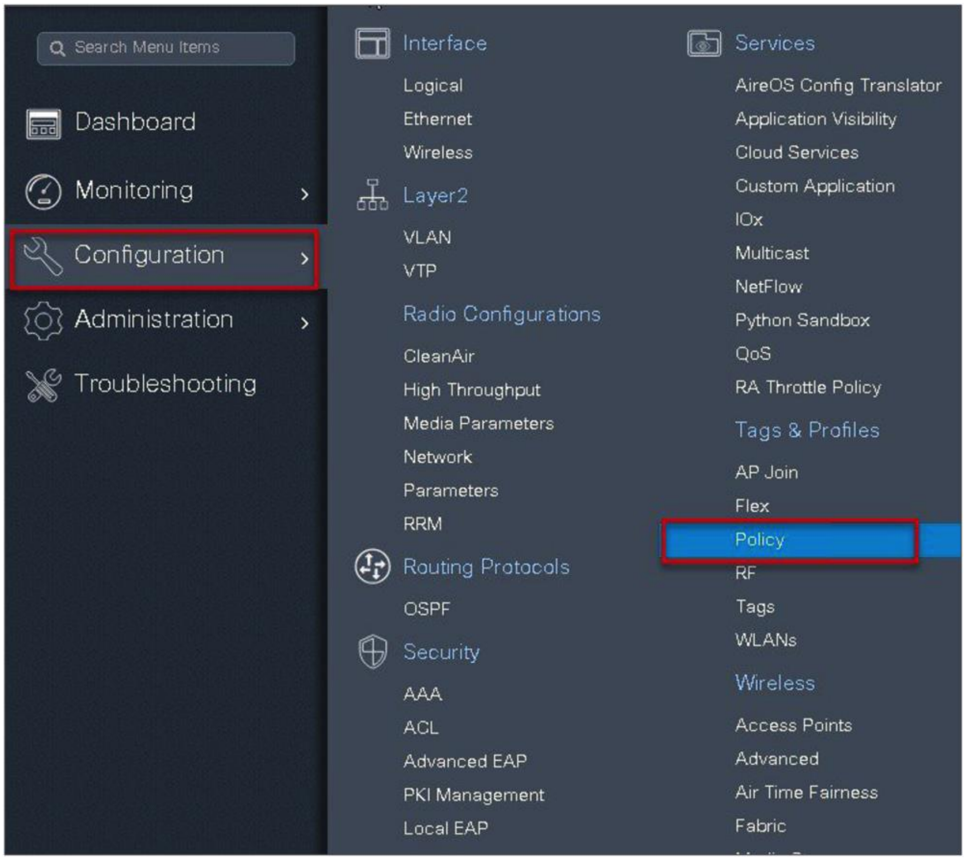
WLAN ID*: 2

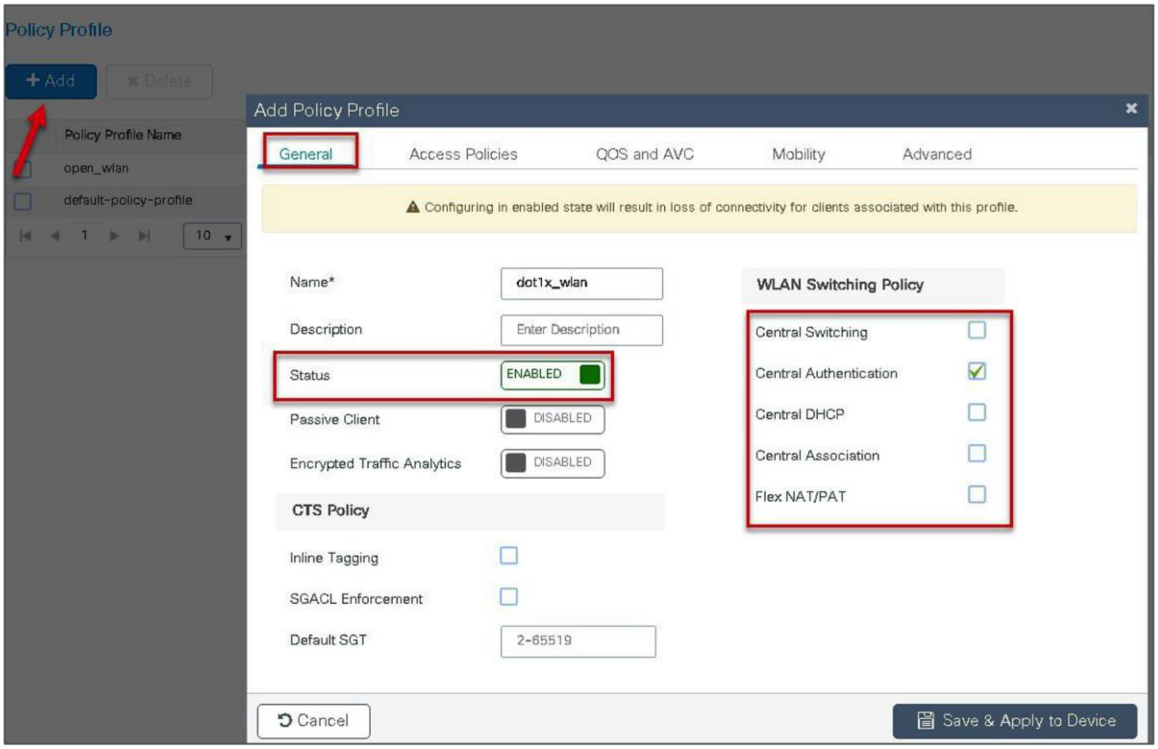
Status: ENABLED

Radio Policy: All

Broadcast SSID: ENABLED

Step 3. Create a policy profile and enable local switching and central authentication on the profile.





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

Name*	dot1x_wlan
Description	Enter Description
Status	ENABLED
Passive Client	DISABLED
Encrypted Traffic Analytics	DISABLED

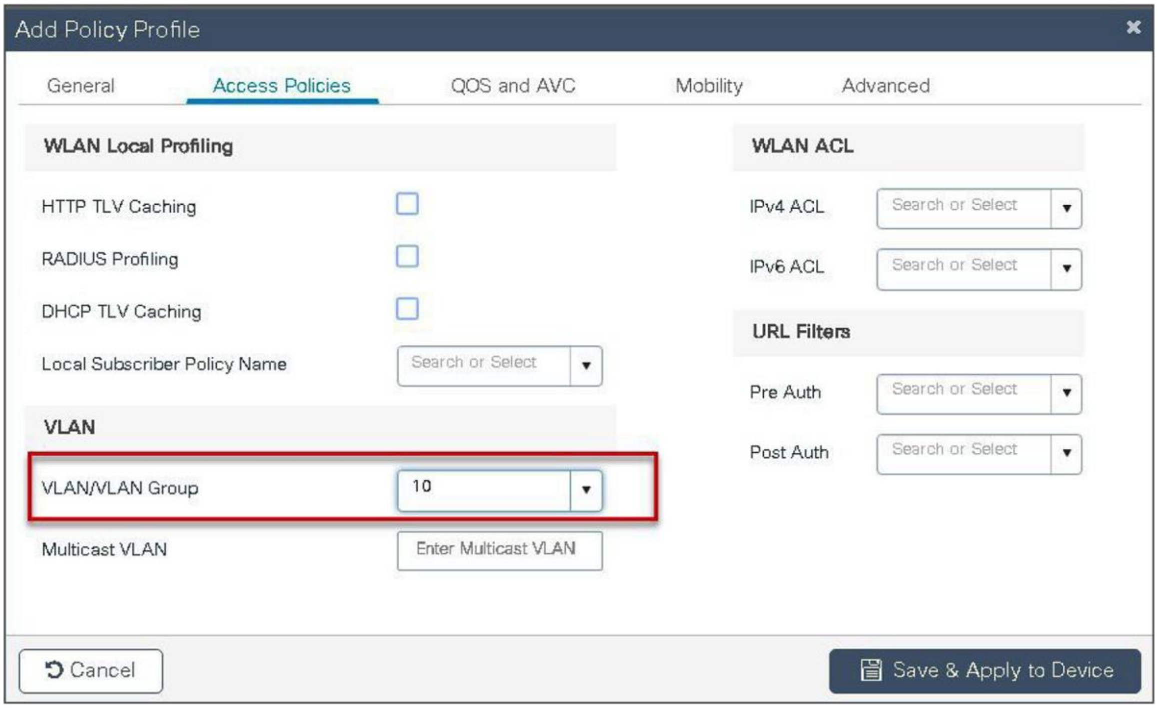
CTS Policy

Inline Tagging	□
SGACL Enforcement	□
Default SGT	2-65519

WLAN Switching Policy

Central Switching	□
Central Authentication	☑
Central DHCP	□
Central Association	□
Flex NAT/PAT	□

Step 4. Map the default VLAN for the WLAN.



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: 10

Multicast VLAN: Enter Multicast VLAN

WLAN ACL

IPv4 ACL: Search or Select

IPv6 ACL: Search or Select

URL Filters

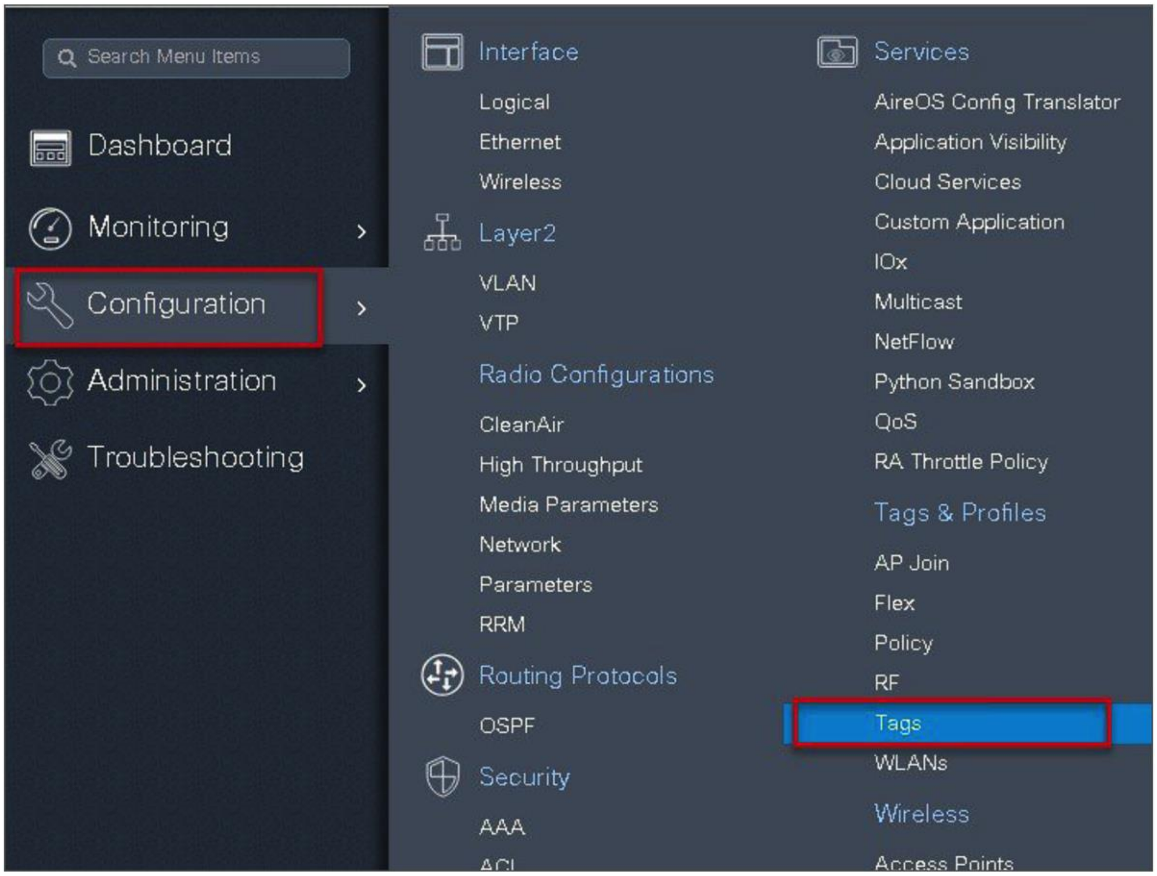
Pre Auth: Search or Select

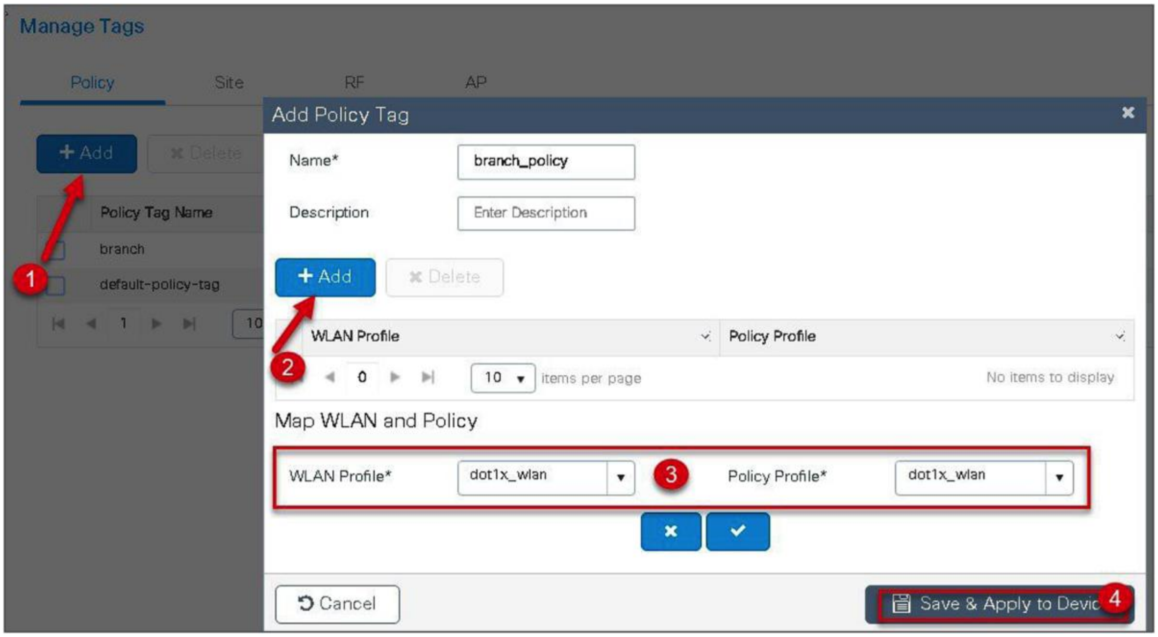
Post Auth: Search or Select

Cancel | Save & Apply to Device

Step 5. Map the WLAN to policy profile.

Navigate to Configuration > Tag and create a policy tag mapping the WLAN and policy profile.





Add Policy Tag

Name*: branch_policy

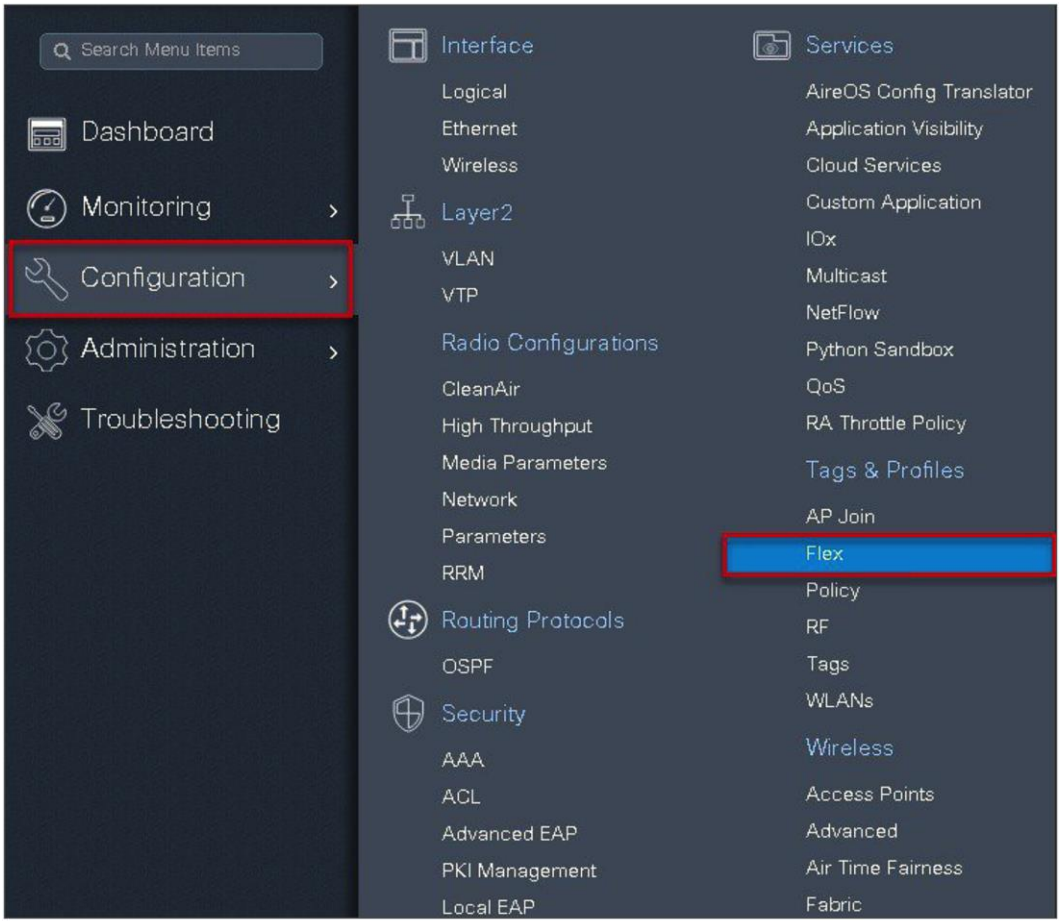
Description: Enter Description

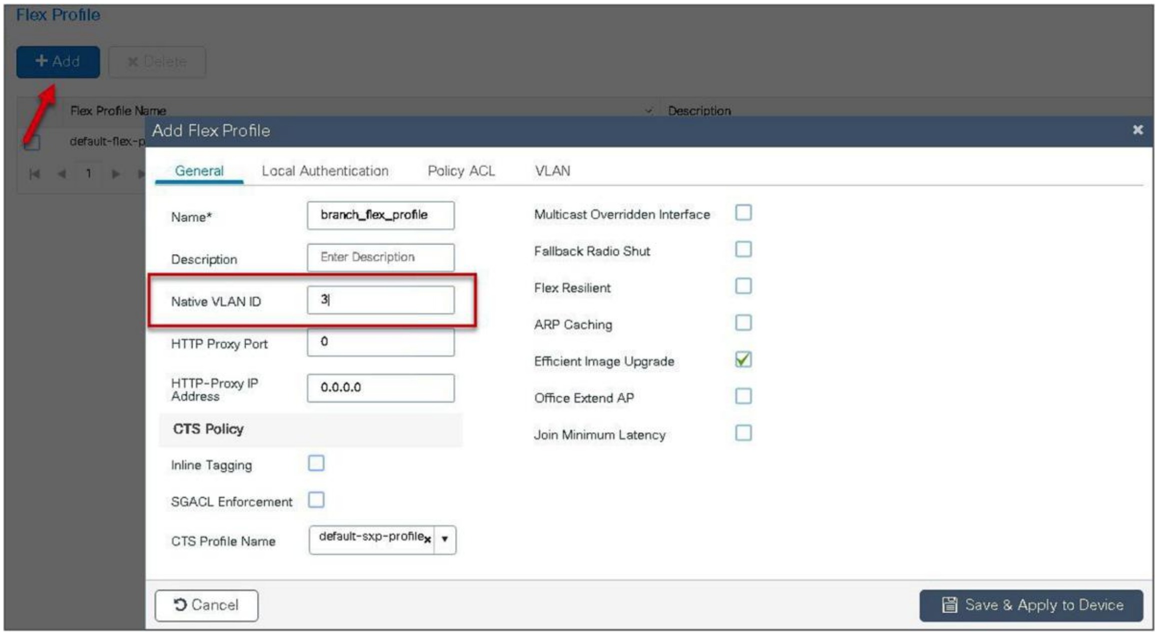
Map WLAN and Policy

WLAN Profile*: dot1x_wlan

Policy Profile*: dot1x_wlan

Step 6. Create a flex profile to create the VLAN on the profile to be used by the SSID.





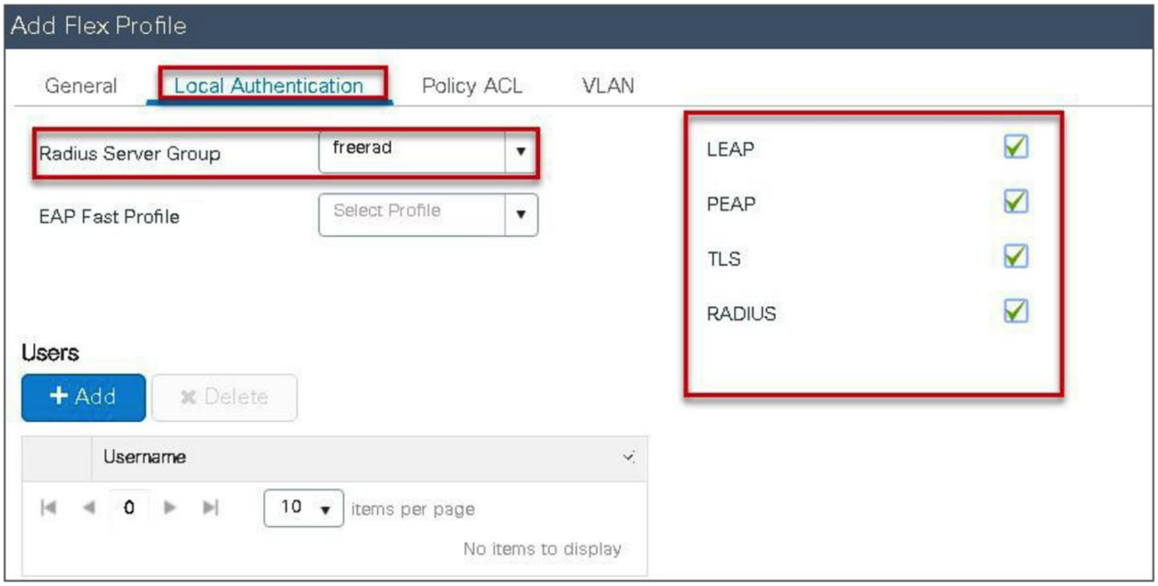
Add Flex Profile

Name*	branch_flex_profile
Description	Enter Description
Native VLAN ID	3
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	□



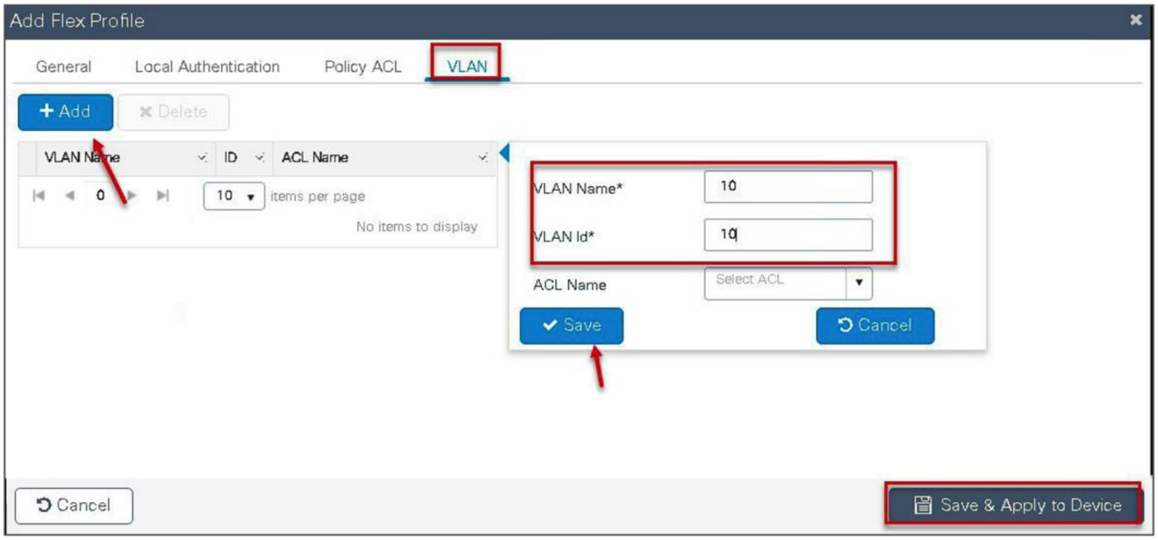
Add Flex Profile

Radius Server Group	freerad
EAP Fast Profile	Select Profile

LEAP	☑
PEAP	☑
TLS	☑
RADIUS	☑

Users

No items to display



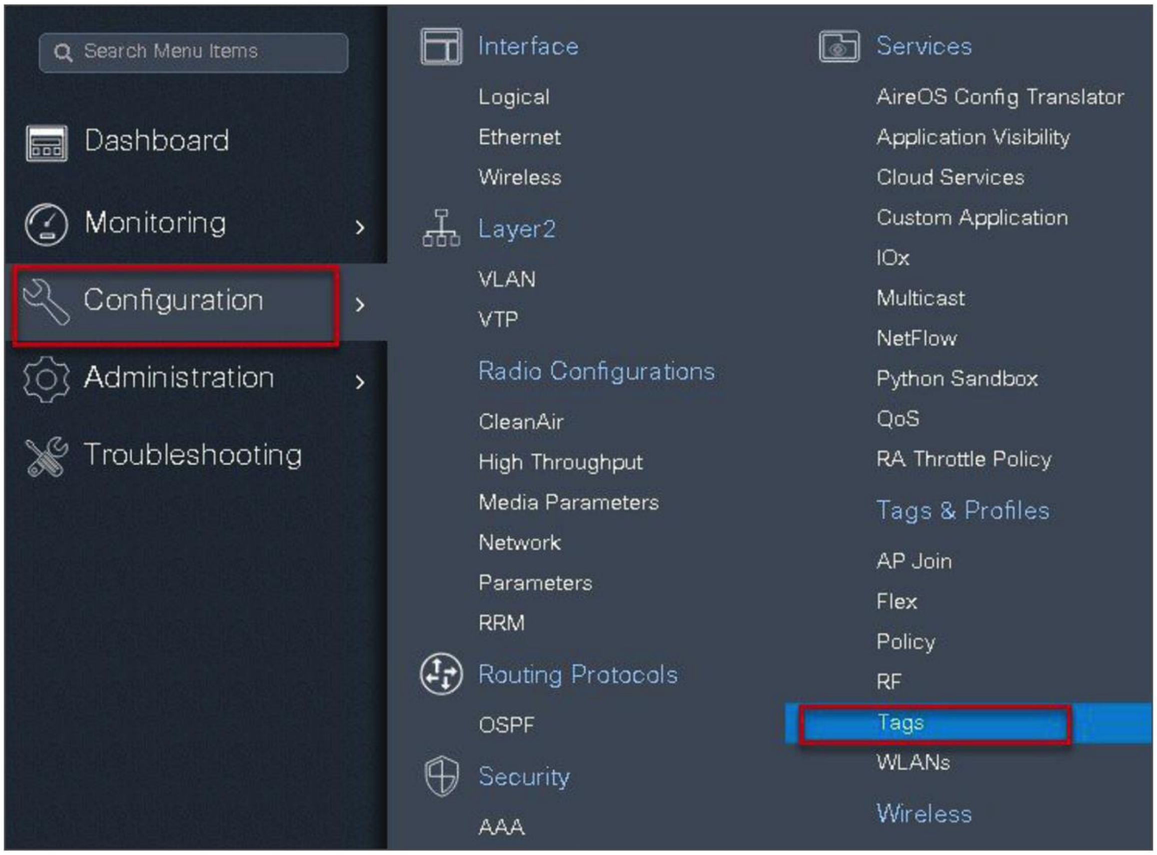
VLAN Name* 10

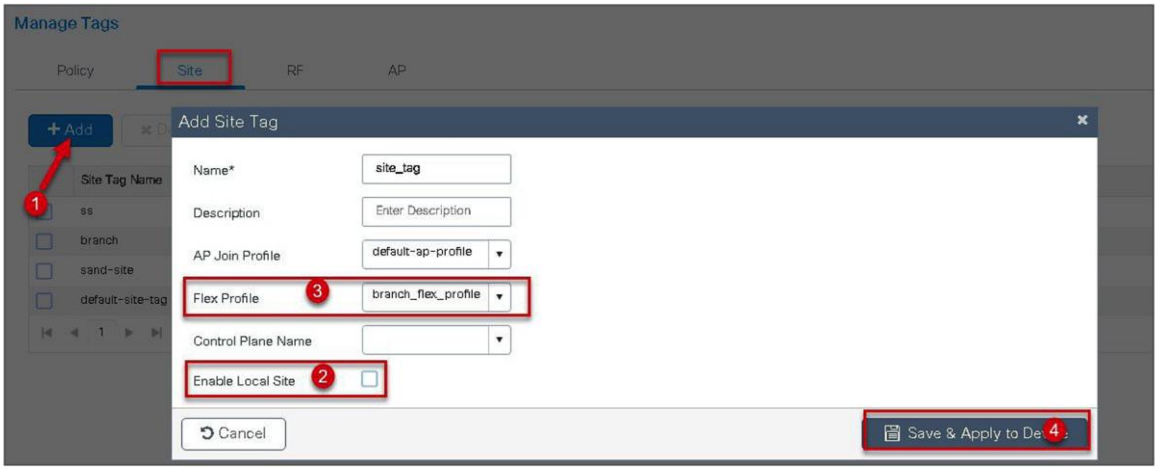
VLAN Id* 10

ACL Name

Step 7. Create a site tag and map the flex profile on the site tag.

Uncheck “Enable Local Site” to add the flex profile on the site tag.





Site Tag Name
ss
branch
sand-site
default-site-tag

Name*: site_tag

Description: Enter Description

AP Join Profile: default-ap-profile

Flex Profile: branch_flex_profile

Control Plane Name:

Enable Local Site: □

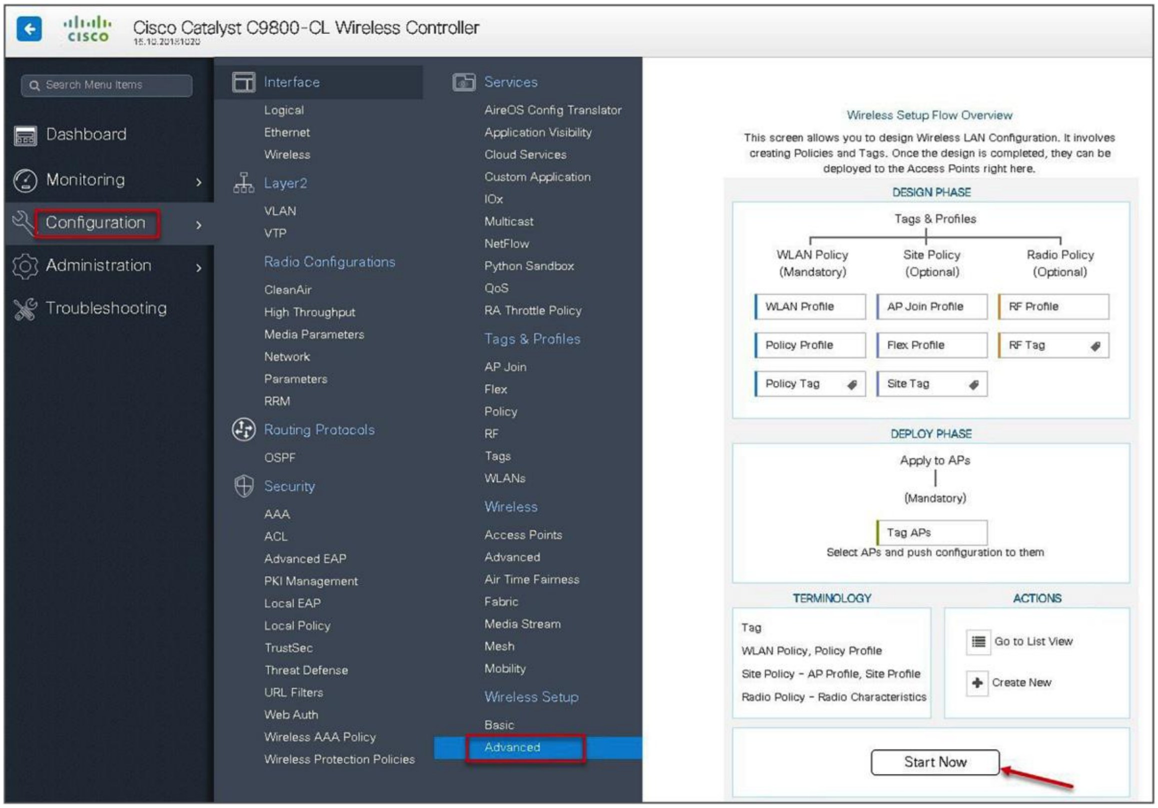
Step 8. Map the policy profile and site tag on the AP. To tag the AP, open the advanced config wizard and tag the AP with corresponding tags.

The mapping can be provisioned by creating a filter list based on the AP name.

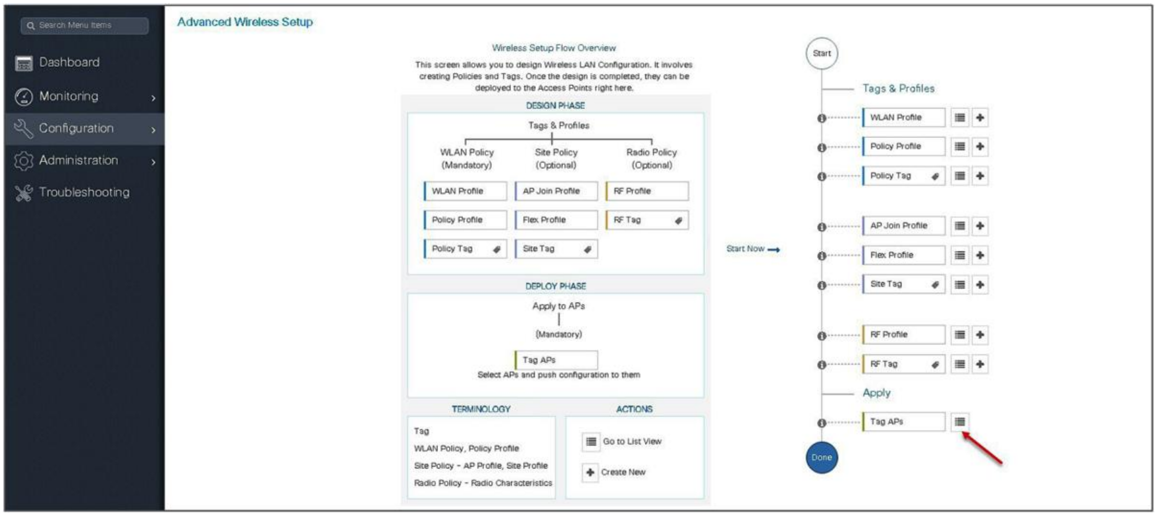
Assigning a site tag on an AP might result in AP reboot due to conversion to FlexConnect mode.

The reboot is avoided if the AP is already in FlexConnect mode.

Navigate to Configuration > Wireless Setup > Advanced.

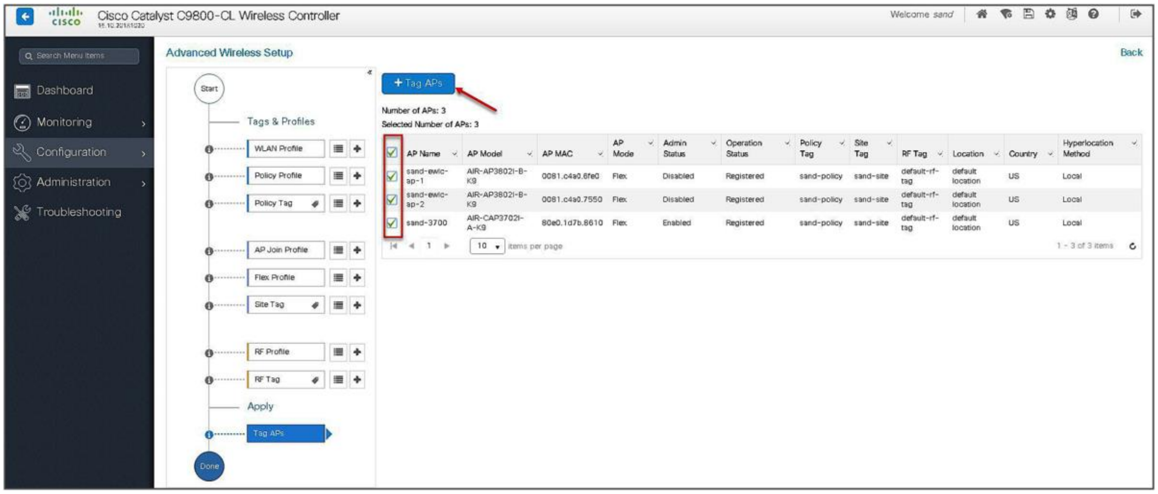


This screen allows you to design Wireless LAN Configuration. It involves creating Policies and Tags. Once the design is completed, they can be deployed to the Access Points right here.



Wireless Setup Flow Overview

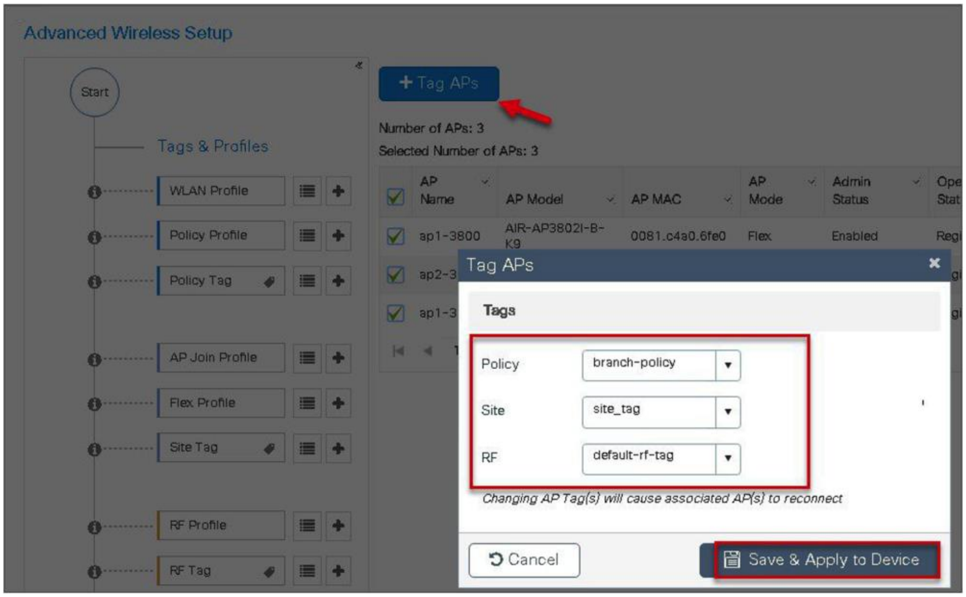
This screen allows you to design Wireless LAN Configuration. It involves creating Policies and Tags. Once the design is completed, they can be deployed to the Access Points right here.



Number of APs: 3
Selected Number of APs: 3

☑	AP Name	AP Model	AP MAC	AP Mode	Admin Status	Operation Status	Policy Tag	Site Tag	RF Tag	Location	Country	Hyperlocation Method
☑	sand-ewlc-ap-1	AIR-AP3802I-B-K9	0081.c4a0.6fe0	Flex	Disabled	Registered	sand-policy	sand-site	default-rf-tag	default location	US	Local
☑	sand-ewlc-ap-2	AIR-AP3802I-B-K9	0081.c4a0.7550	Flex	Disabled	Registered	sand-policy	sand-site	default-rf-tag	default location	US	Local
☑	sand-3700	AIR-CAP3702I-A-K9	80e0.1d7b.8610	Flex	Enabled	Registered	sand-policy	sand-site	default-rf-tag	default location	US	Local

1 · 10 items per page · 1 - 3 of 3 items



Number of APs: 3
Selected Number of APs: 3

☑	AP Name	AP Model	AP MAC	AP Mode	Admin Status	Ope Stat
☑	ap1-3800	AIR-AP3802I-B-K9	0081.c4a0.6fe0	Flex	Enabled	Regi
☑	ap2-3					
☑	ap1-3					

Tag APs

Tags

Policy	branch-policy
Site	site_tag
RF	default-rf-tag

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

AP as radius server

FlexConnect AP can be configured as a RADIUS server for LEAP client authentication. In standalone mode and also when local authentication feature is enabled on the WLANs, FlexConnect AP will perform dot1x authentication on the AP itself using the local radius facility.

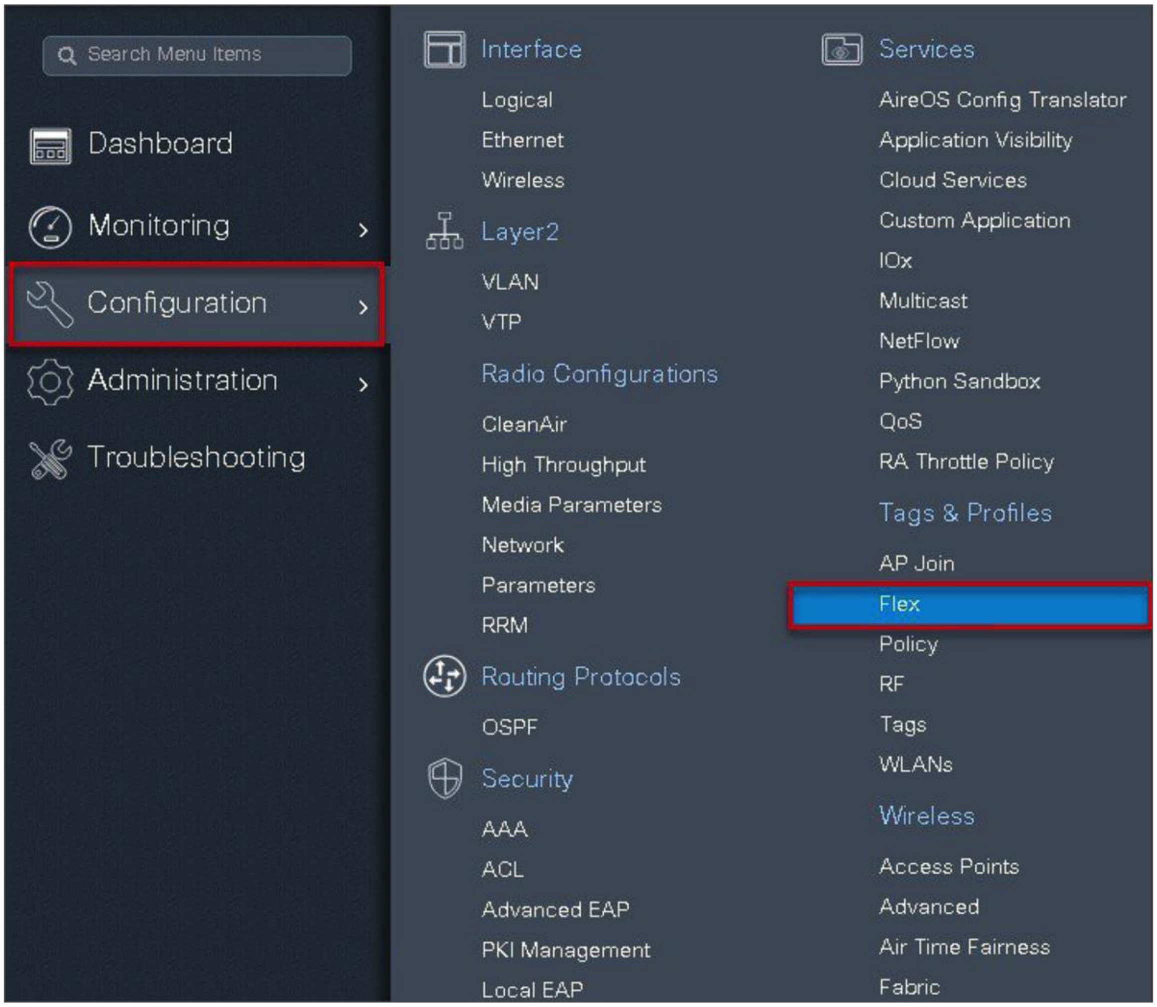
Procedure

To have the FlexConnect AP configured as the radius server, repeat steps 2, 3, 4, 5, 7, and 8 in the procedure section of configuring local authentication with external radius server.

The flex profile needs to be reconfigured to enable local radius server functionality.

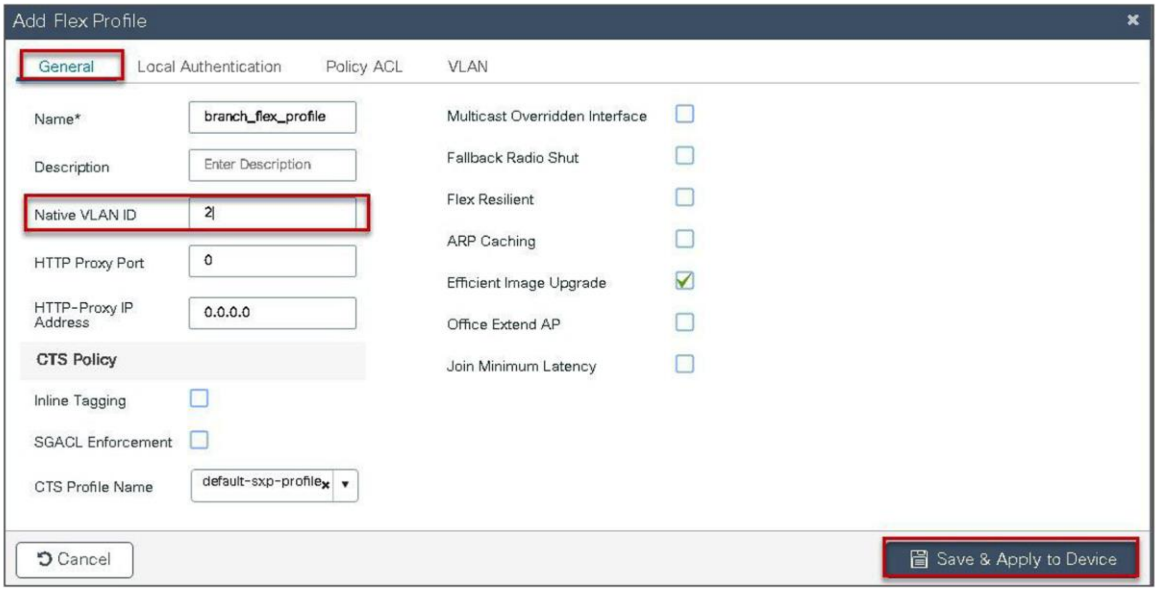
Procedure

Step 1. Create a flex profile. Navigate to Configuration > Flex.



Step 2. Specify the native VLAN ID for the AP. On the local authentication, specify the EAP methods to be used.

Add local users for authentication on the AP. The local users reside on the AP.



Add Flex Profile

General | Local Authentication | Policy ACL | VLAN

Name*: branch_flex_profile

Description: Enter Description

Native VLAN ID: 2

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 □

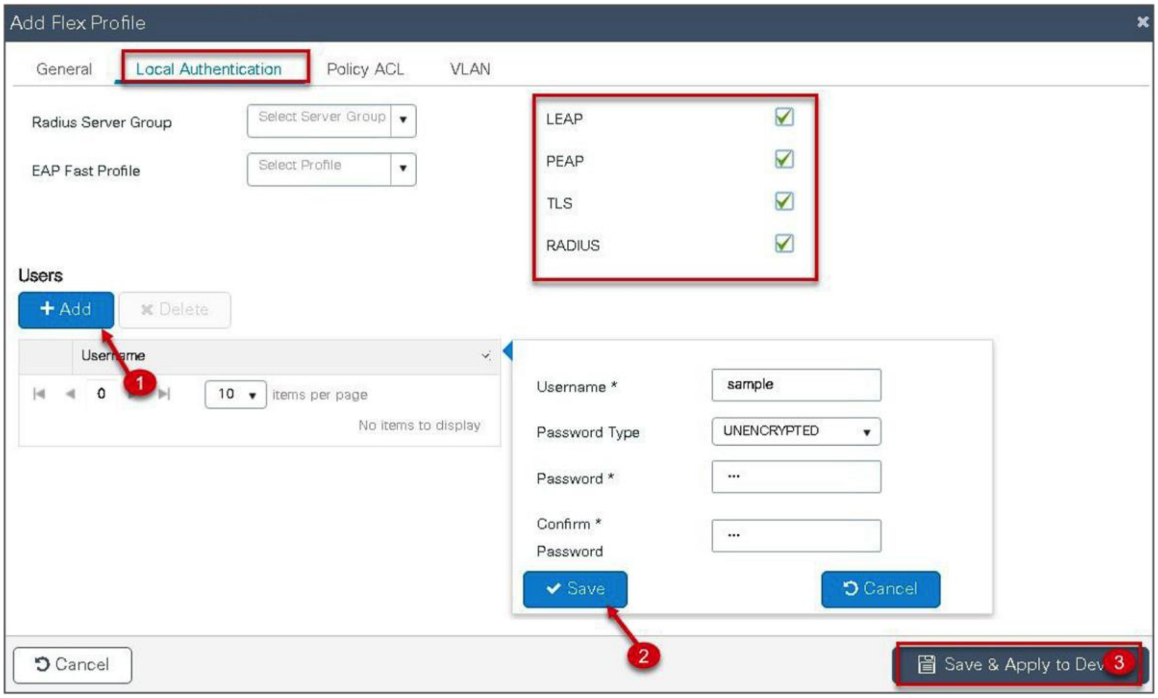
Flex Resilient □

ARP Caching □

Efficient Image Upgrade ☑

Office Extend AP □

Join Minimum Latency □



Add Flex Profile

General | Local Authentication | Policy ACL | VLAN

Radius Server Group: Select Server Group

EAP Fast Profile: Select Profile

LEAP ☑

PEAP ☑

TLS ☑

RADIUS ☑

Users

Username

0 | 10 items per page

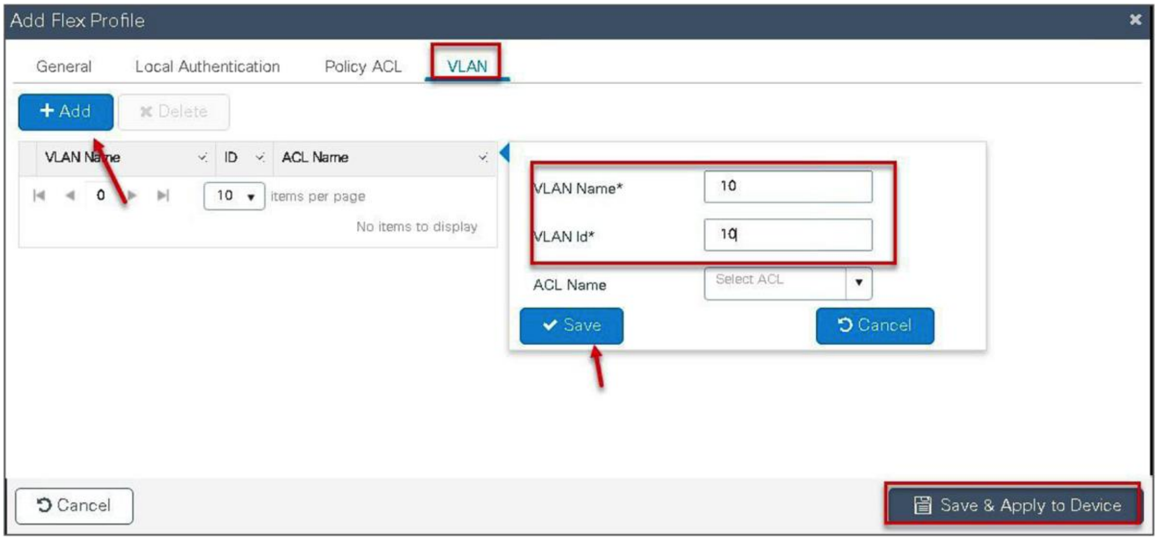
No items to display

Username *: sample

Password Type: UNENCRYPTED

Password *: ...

Confirm Password *: ...



VLAN Name* 10

VLAN Id* 10

ACL Name Select ACL

CCKM/OKC and PMK caching

CCKM/OKC and PMK caching enables fast roaming for wireless clients. Fast roaming is achieved by caching a derivative of the primary key from a full EAP authentication so that a simple and secure key exchange can occur when a wireless client roams to a different access point. This feature prevents the need to perform a full RADIUS EAP authentication as the client roams from one access point to another.

The controller supports CCKM/OKC and PMK caching, and the controller takes care of distributing the primary key to the APs. The controller distributes the primary key to all the APs whose site tag and policy tag are the same. This results in the ability to do fast roaming across the AP within the same site. The distribution of the primary key is done based on the site tag of the AP site the client initially associates, and the controller now finds all the APs that have a similar site tag and policy tag and pushes the primary key on those APs, thus enabling fast roaming among the APs.

Limitation

- The AP in standalone mode can support a maximum of two radius servers. The first server added in the server group acts as the primary. The second radius server acts as a backup for the primary.
- The AP as radius server is supported only on Wave 1 APs. On 16.10, the EAP method supported for the AP as the radius server is EAP-LEAP.
- Fast roaming is not supported with the default site tag. If the APs are mapped to a default site tag, the primary key for caching is not shared among those APs.

Peer-to-peer blocking

The controller supports peer-to-peer blocking in local switching mode. The configuration for the peer-to-peer blocking is available while creating the WLAN.

Peer-to-peer blocking can be configured with any of the following three actions.

- Disabled – Disables peer-to-peer blocking and bridged traffic locally within the controller for clients in the same subnet. This is the default value.
- Drop – Causes the controller to discard packets for clients in the same subnet.
- Forward upstream – Causes the packet to be forwarded on the upstream VLAN. The devices above the controller decide what action to take regarding the packet.

Summary

- Peer-to-peer blocking is configured per WLAN.
- Per WLAN, peer-to-peer blocking configuration is pushed by the WLC to FlexConnect APs.
- Peer-to-peer blocking action configured as drop or forward-upstream on WLAN is treated as peer-to-peer blocking enabled on the FlexConnect AP.

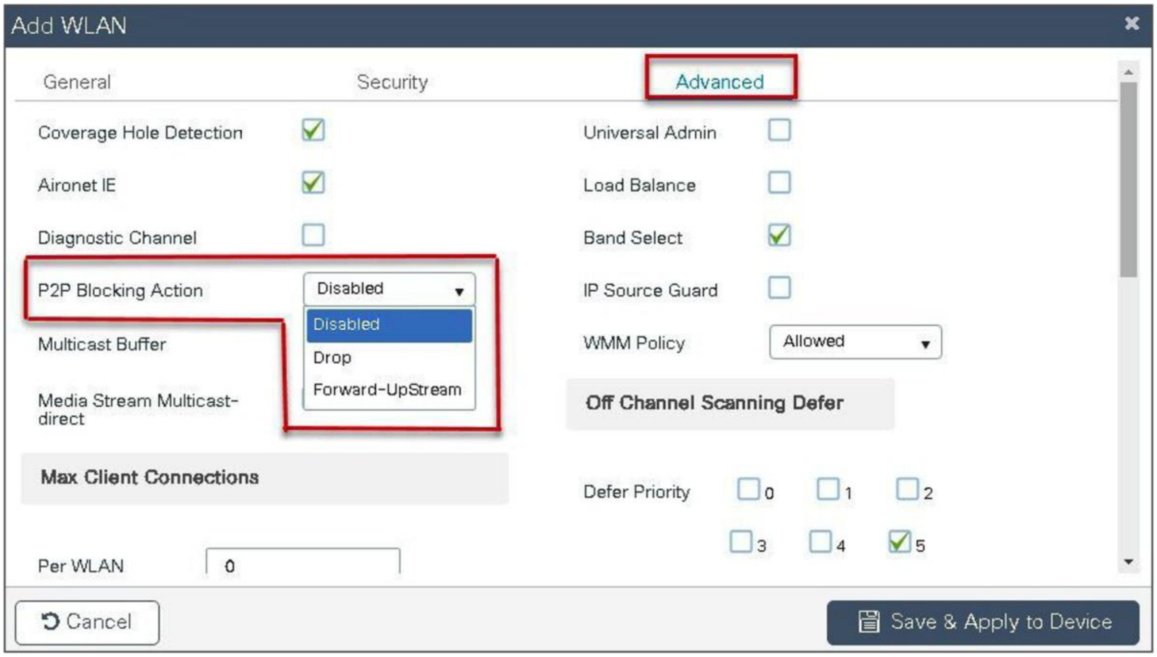
Steps

Procedure

Refer to the steps defined in the advanced config wizard of this document to create an SSID, policies, and tags on the controller.

Advanced wireless setup wizard

Select the peer-to-peer blocking action in the advanced tab of the WLAN creation to have the feature configured.



Coverage Hole Detection ☑
Aironet IE ☑
Diagnostic Channel □
P2P Blocking Action: Disabled
Multicast Buffer
Media Stream Multicast-direct

Max Client Connections

Per WLAN: 0

Universal Admin □
Load Balance □
Band Select ☑
IP Source Guard □
WMM Policy: Allowed

Off Channel Scanning Defer

Defer Priority: □ 0 □ 1 □ 2 □ 3 □ 4 ☑ 5

Once the P2P blocking action is configured on the WLAN, it is pushed from the WLC to the FlexConnect APs. The config will be retained by the AP when it moves from connected mode to standalone mode.

FlexConnect ACL

ACL usage on FlexConnect deployment provides a way to cater the need to provide access control at the FlexConnect AP for protection and integrity of locally switched data traffic from the AP. FlexConnect ACLs are created on the WLC and should then be configured with the VLAN on a flex profile that is mapped to a site tag. The site tag gets assigned to an AP. The ACL name can also be returned as part of an attribute from AAA.

Summary

The ACL implementation for branch deployments can be done through the following methods:

- WLAN ACL - The ACL is applied on the WLAN dot11 interface and is enforced to all the clients connecting on that SSID.
- WLAN ACL - The ACL is applied on the WLAN dot11 interface and is enforced to all the clients connecting on that SSID.
- Client ACL- The ACL is returned as part of the AAA attribute and is enforced for the specific client.

The ACL for the enforcement needs to be created on the WLC and also needs to be pushed to the Flex AP. The way to push the ACL to the flex AP is using the flex profiles. An administrator can create a policy ACL on the flex profile to push the ACL on the AP or use a dummy VLAN to ACL mapping on the flex profile. When a wireless client joins an SSID and an ACL is enforced either through WLAN/VLAN or AAA, the WLC checks if the ACL is also pushed to the AP. If the ACL is not present on the AP, the client is moved to the exclusion list.

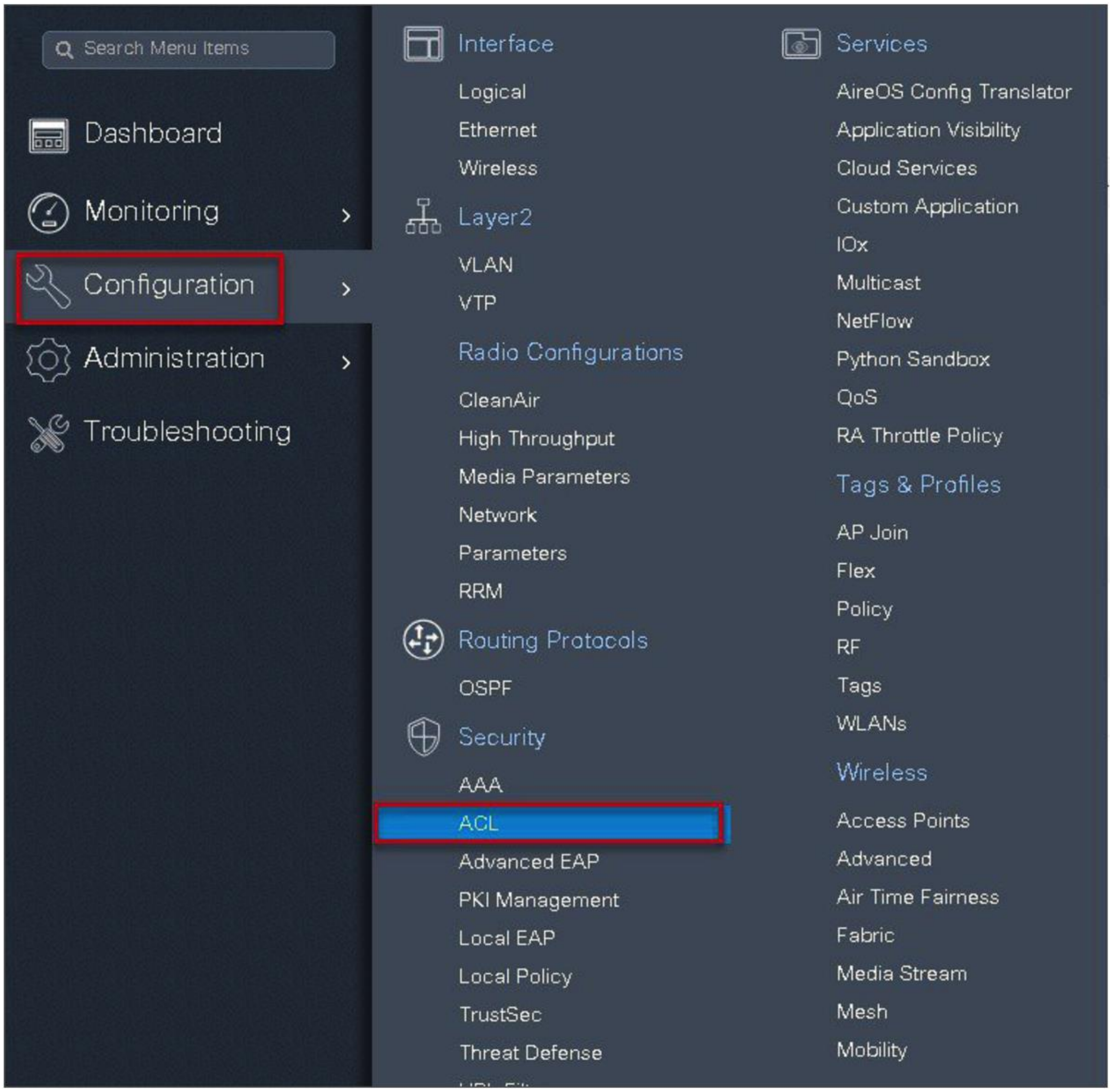
Procedure for WLAN ACL

Procedure for WLAN ACL:

- Create an ACL on the controller.
- Apply the ACL on the respective policy profile for the WLAN.
- Now create a flex profile, add a policy ACL, and map the corresponding ACL on the flex profile.
- Also add the ACL as part of the policy profile.
- Connect the client and validate that the ACL works.

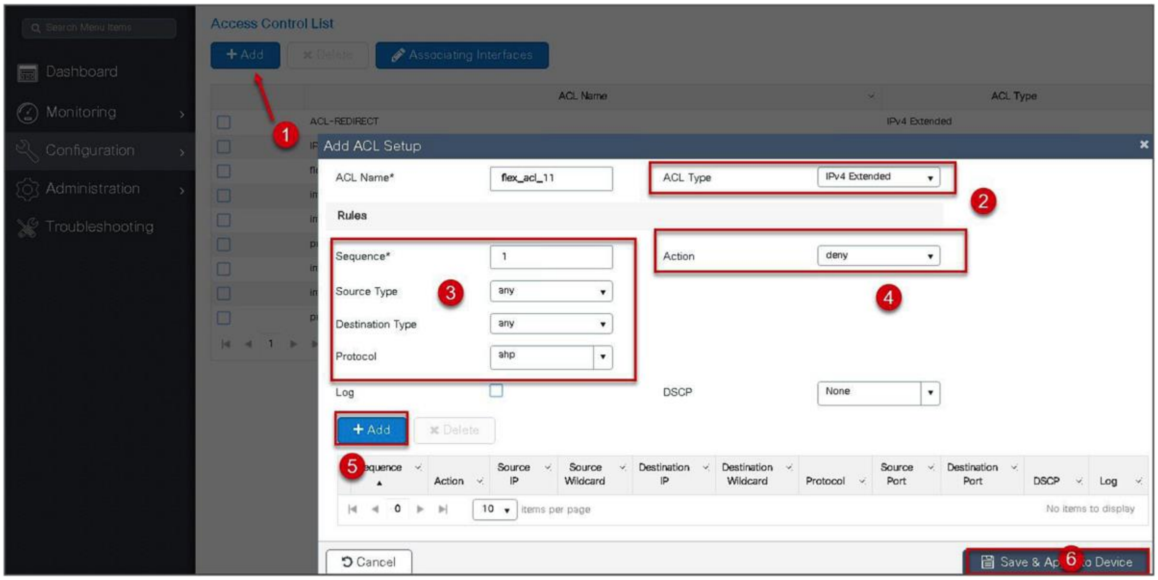
Procedure

Step 1. Create an ACL on the WLC by navigating to Configuration > Security > ACL.



Step 2. Perform the following steps:

- Click on “Add” to create an ACL, and define an ACL name.
- Specify the type of ACL: standard or extended.
- Define the rules for the ACL.
- Specify the action as permit or deny.
- Add the ACL rules and save the ACL.



ACL Name* flex_acl_11

ACL Type IPv4 Extended

Sequence* 1

Source Type any

Destination Type any

Protocol ahp

Action deny

Log □

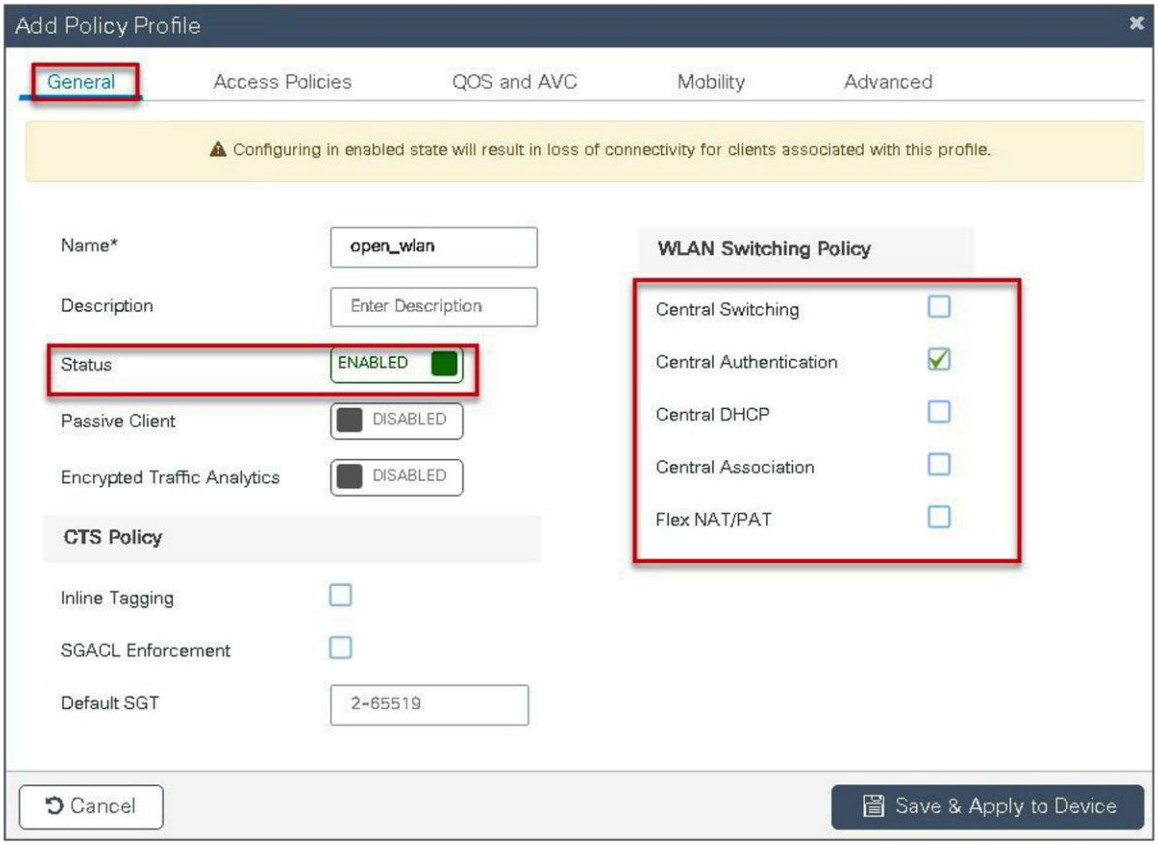
DSCP None

Step 3. Refer to the steps in the procedure of the advanced configuration wizard for the following:

- Create a WLAN
- Creation of policy profile (refer to the screenshot below to add the ACL)
- Policy tag mapping
- Flex profile (refer to the screenshot below to map the ACL using the policy ACL)
- Creation of the site tag
- Tagging the AP

Advanced wireless setup wizard:

The ACL is attached to the WLAN through the policy profile.



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

Name* open_wlan

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

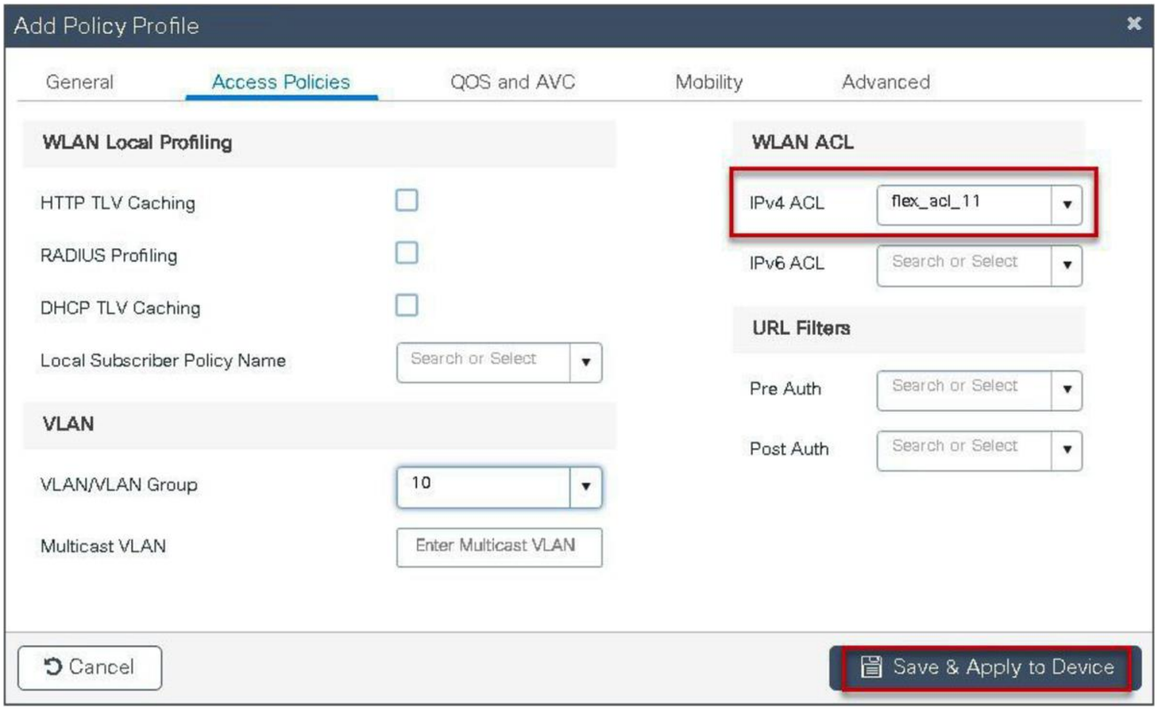
Central Switching □

Central Authentication ☑

Central DHCP □

Central Association □

Flex NAT/PAT □



WLAN Local Profiling

HTTP TLV Caching □

RADIUS Profiling □

DHCP TLV Caching □

Local Subscriber Policy Name Search or Select

VLAN

VLAN/VLAN Group 10

Multicast VLAN Enter Multicast VLAN

WLAN ACL

IPv4 ACL flex_acl_11

IPv6 ACL Search or Select

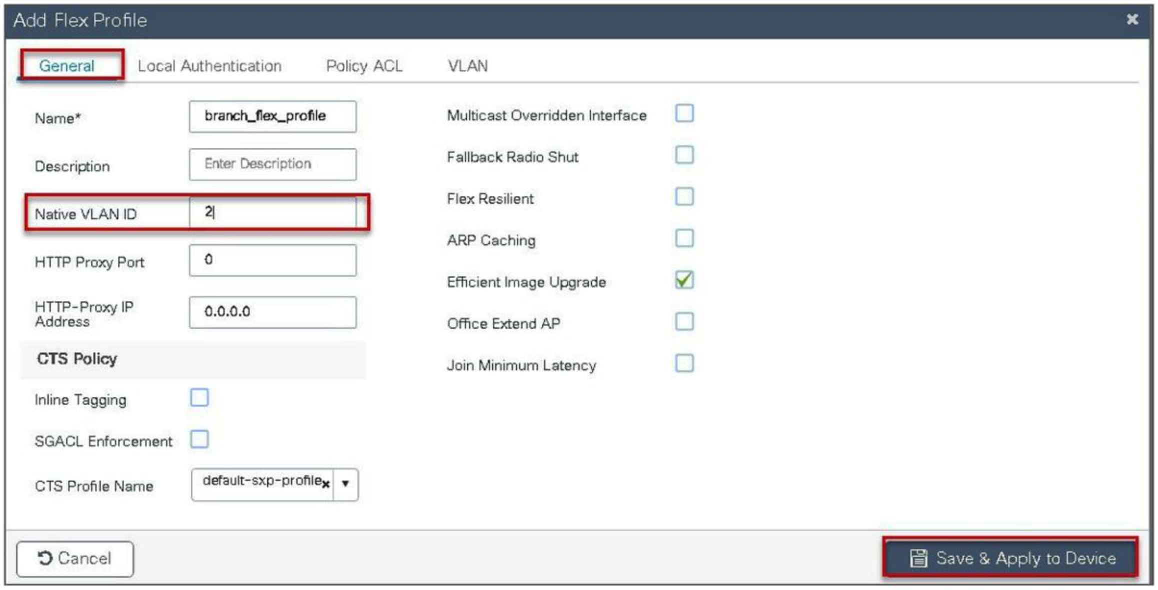
URL Filters

Pre Auth Search or Select

Post Auth Search or Select

Step 4. Assign the ACL on the flex profile by mapping the VLAN and ACL.

Define the native VLAN for the FlexConnect APs.



Name*: branch_flex_profile

Description: Enter Description

Native VLAN ID: 2

HTTP Proxy Port: 0

HTTP-Proxy IP Address: 0.0.0.0

Inline Tagging □

SGACL Enforcement □

CTS Profile Name: default-sxp-profile

Multicast Overridden Interface □

Fallback Radio Shut □

Flex Resilient □

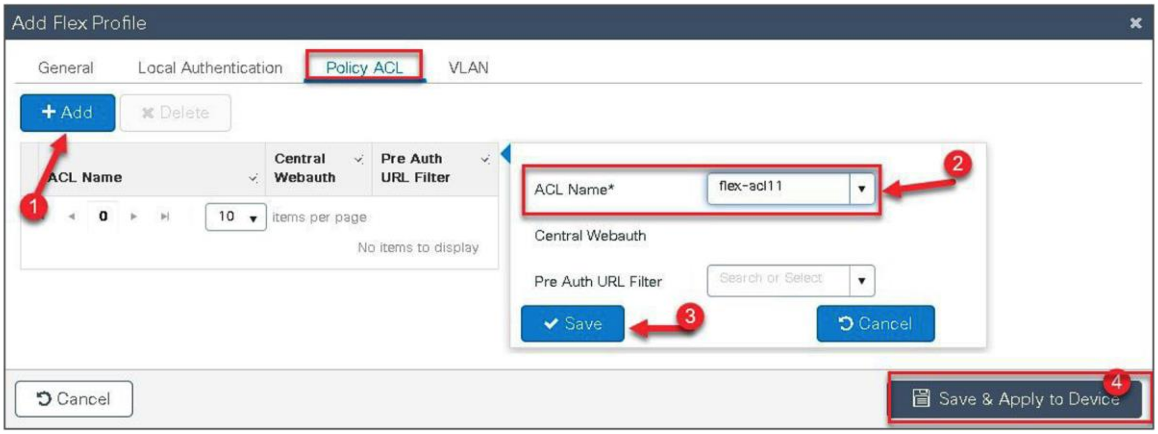
ARP Caching □

Efficient Image Upgrade ☑

Office Extend AP □

Join Minimum Latency □

Step 5. Push the ACL to AP by using the policy ACL configuration on the flex profile.



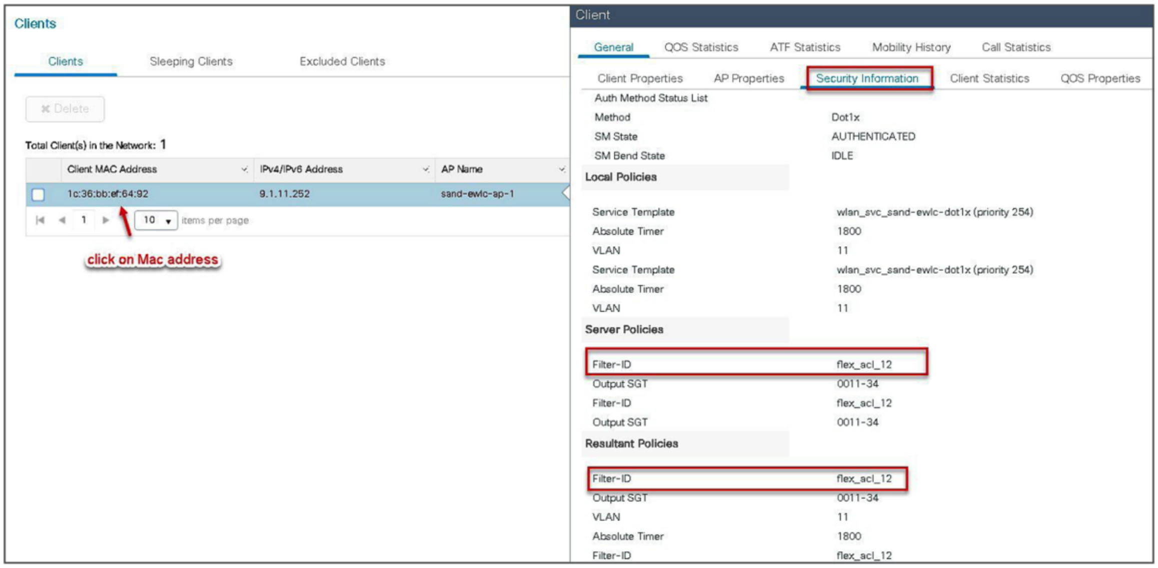
ACL Name*: flex-acl11

Central Webauth

Pre Auth URL Filter: Search or Select

Step 6. Verification on the controller.

Navigate to Monitoring > Wireless > Clients.



Total Client(s) in the Network: 1

	Client MAC Address	IPv4/IPv6 Address	AP Name
□	1c:36:bb:ef:64:92	9.1.11.252	sand-ewlc-ap-1

click on Mac address

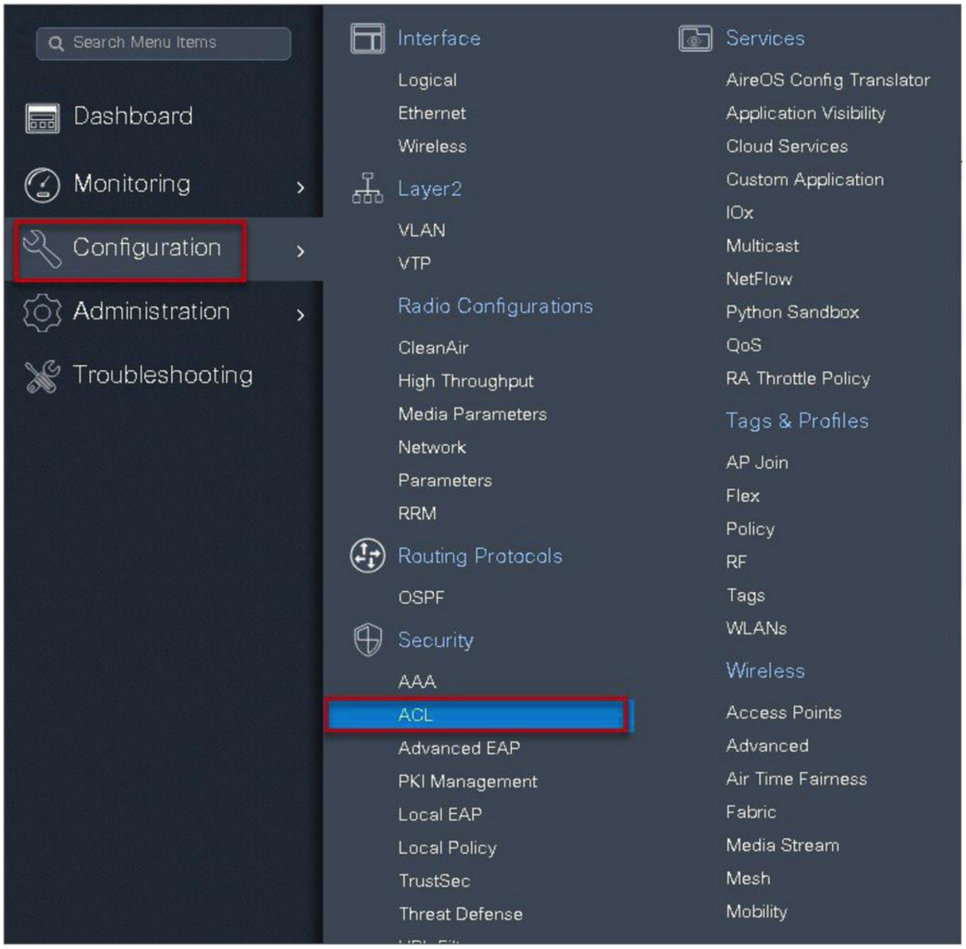
Auth Method Status List	
Method	Dot1x
SM State	AUTHENTICATED
SM Bend State	IDLE
Local Policies	
Service Template	wlan_svc_sand-ewlc-dot1x (priority 254)
Absolute Timer	1800
VLAN	11
Service Template	wlan_svc_sand-ewlc-dot1x (priority 254)
Absolute Timer	1800
VLAN	11
Server Policies	
Filter-ID	flex_acl_12
Output SGT	0011-34
Filter-ID	flex_acl_12
Output SGT	0011-34
Resultant Policies	
Filter-ID	flex_acl_12
Output SGT	0011-34
VLAN	11
Absolute Timer	1800
Filter-ID	flex_acl_12

Procedure for VLAN ACL

- Create an ACL on the controller.
- Create a flex profile and add a VLAN mapped to the WLAN.
- Map the ACL on the VLAN interface.
- Connect the client and validate that the ACL works.

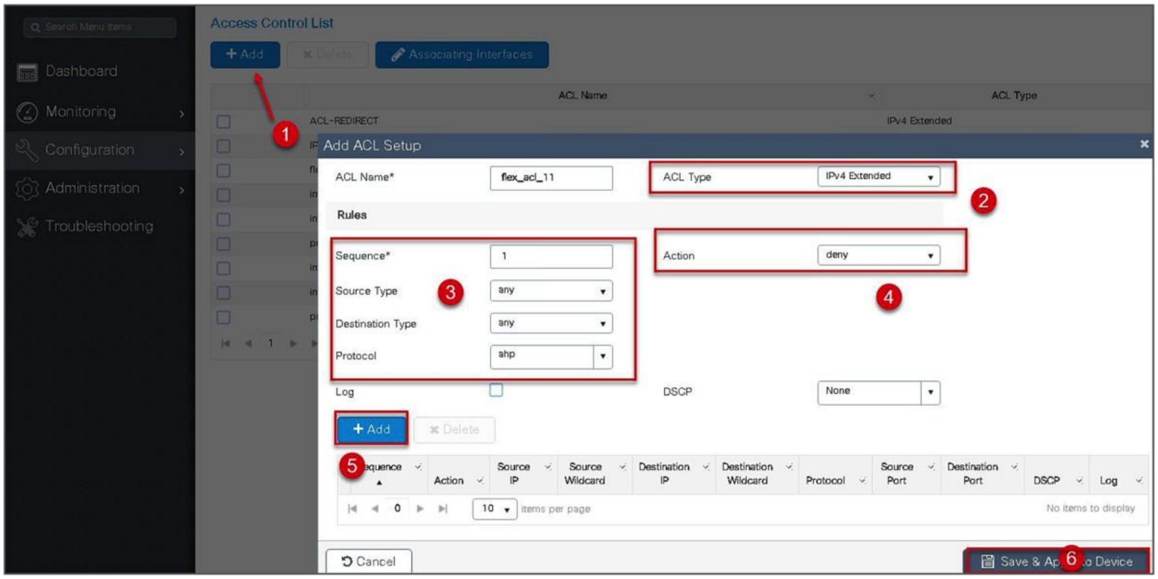
Procedure

Step 1. Create an ACL on the WLC by navigating to Configuration > Security > ACL.



Step 2. Perform the steps below:

- Click on "Add" to create an ACL and define an ACL name.
- Specify the type of ACL: standard or extended.
- Define the rules for the ACL.
- Specify the action as permit or deny.
- Add the ACL rules and save the ACL.



Add ACL Setup

ACL Name*: flex_acl_11

ACL Type: IPv4 Extended

Rules

Sequence*: 1

Source Type: any

Destination Type: any

Protocol: ahp

Log: ☐

Action: deny

DSCP: None

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log

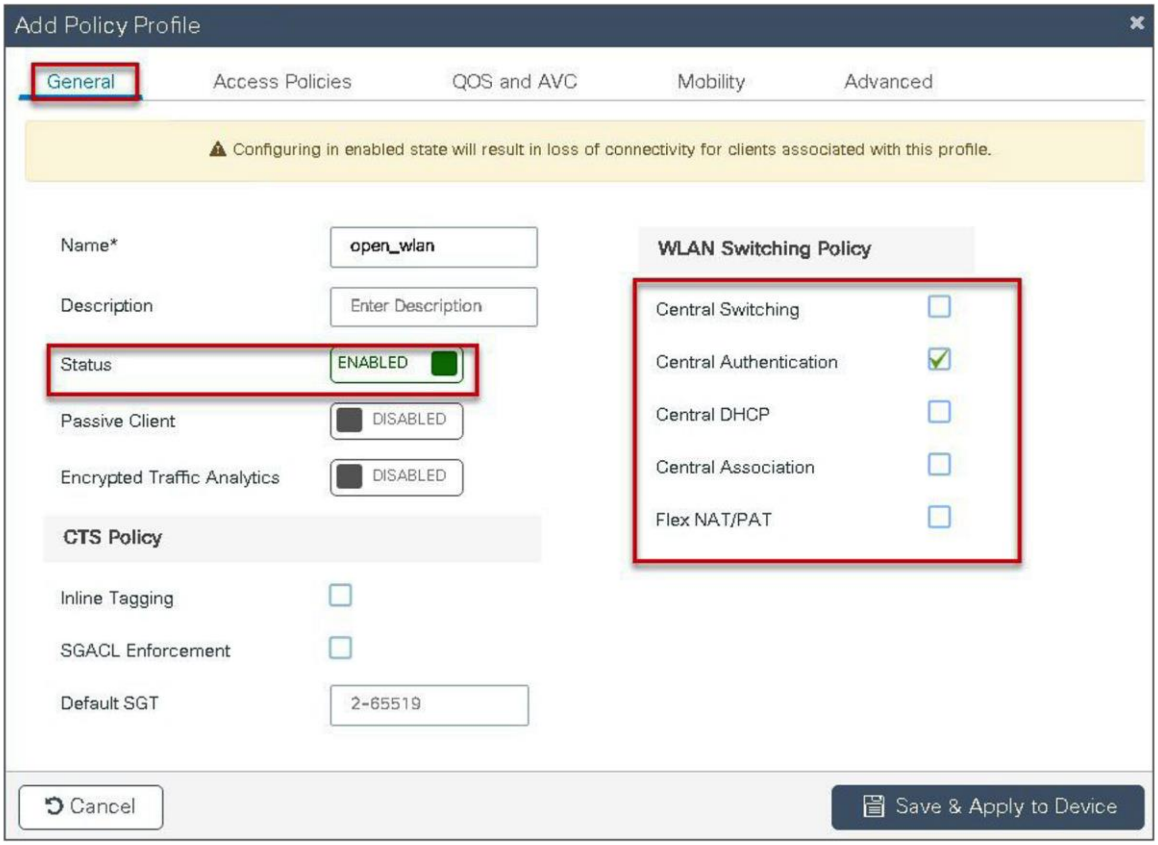
0 · 10 items per page · No items to display

Step 3. Refer to the steps in the procedure of the advanced configuration wizard for the following:

- Create a WLAN
- Creation of policy profile
- Policy tag mapping
- Flex profile creation
- Creation of site tag
- Tagging the AP

Advanced wireless setup wizard:

The ACL is attached to the WLAN through the policy profile.



Add Policy Profile

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

Name* open_wlan

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

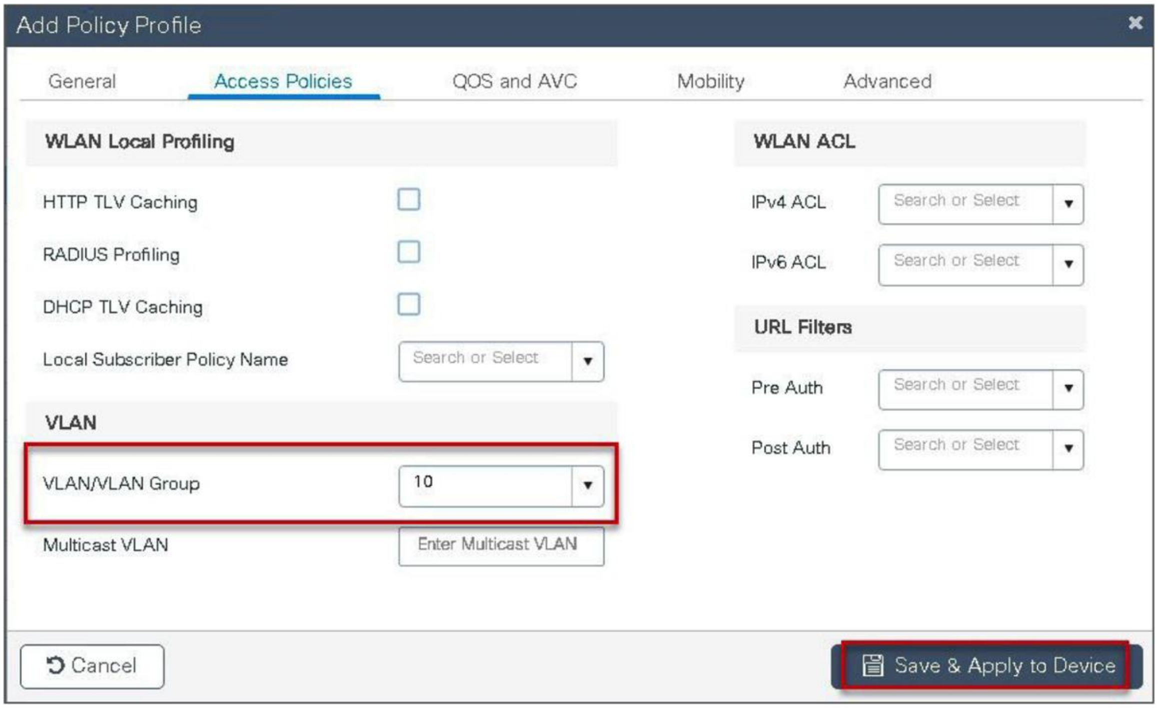
Central Switching □

Central Authentication ☑

Central DHCP □

Central Association □

Flex NAT/PAT □



Add Policy Profile

WLAN Local Profiling

HTTP TLV Caching □

RADIUS Profiling □

DHCP TLV Caching □

Local Subscriber Policy Name Search or Select

VLAN

VLAN/VLAN Group 10

Multicast VLAN Enter Multicast VLAN

WLAN ACL

IPv4 ACL Search or Select

IPv6 ACL Search or Select

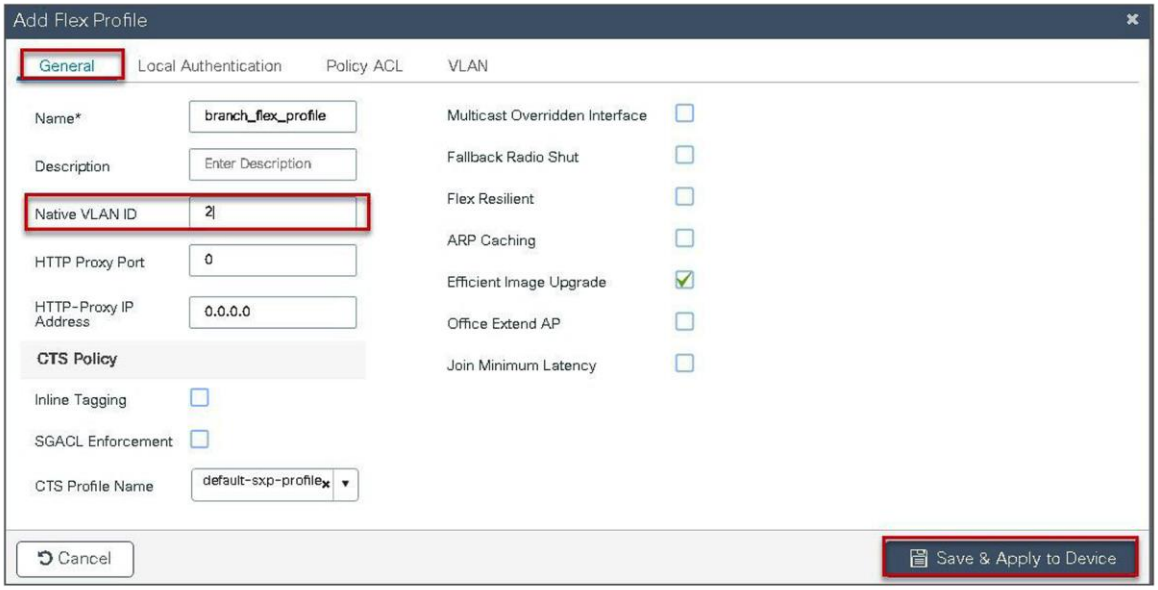
URL Filters

Pre Auth Search or Select

Post Auth Search or Select

Step 4. Assign the ACL on the flex profile by mapping the VLAN and ACL.

Define the native VLAN for the FlexConnect APs.



Name* branch_flex_profile

Description Enter Description

Native VLAN ID 2

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 □

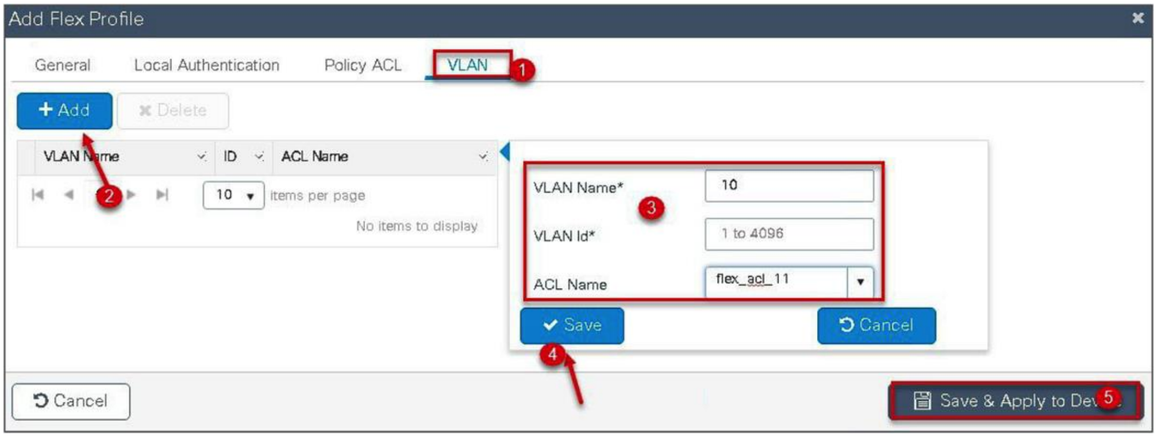
ARP Caching □

Efficient Image Upgrade ☑

Office Extend AP □

Join Minimum Latency □

Step 5. Define the VLAN and ACL mapping on the flex profile.



VLAN Name	ID	ACL Name

VLAN Name* 10

VLAN Id* 1 to 4096

ACL Name flex_acl_11

Client ACL overview

- This feature allows application of the per-client ACL for locally switching WLANs.
- Client ACL is returned from the AAA server on successful client authentication.
- The AP needs to be provisioned with the ACL by using the policy ACL or dummy VLAN ACL mapping on the flex profile.
- The ACL will be pushed to all the APs that have the same site tag and policy tag mapped.
- In the case of central authentication, when the controller receives the ACL from the AAA server, it will send the ACL name to the AP for the client. For locally authenticated clients, the ACL name will be sent from the AP to the controller as part of CCKM/PMK cache, which will then be distributed to all APs belonging to the same site tag and policy tag.

Procedure for client ACL

- Create an ACL on the controller.
- Create a dot1x-based SSID.
- Enable AAA override on the policy profile.
- Return the ACL name as part of the AAA access-accept from the AAA.

For the creation of the ACL, refer to the steps in the WLAN ACL use case. Refer to step 5 in the WLAN ACL section to push the ACL on to the AP.

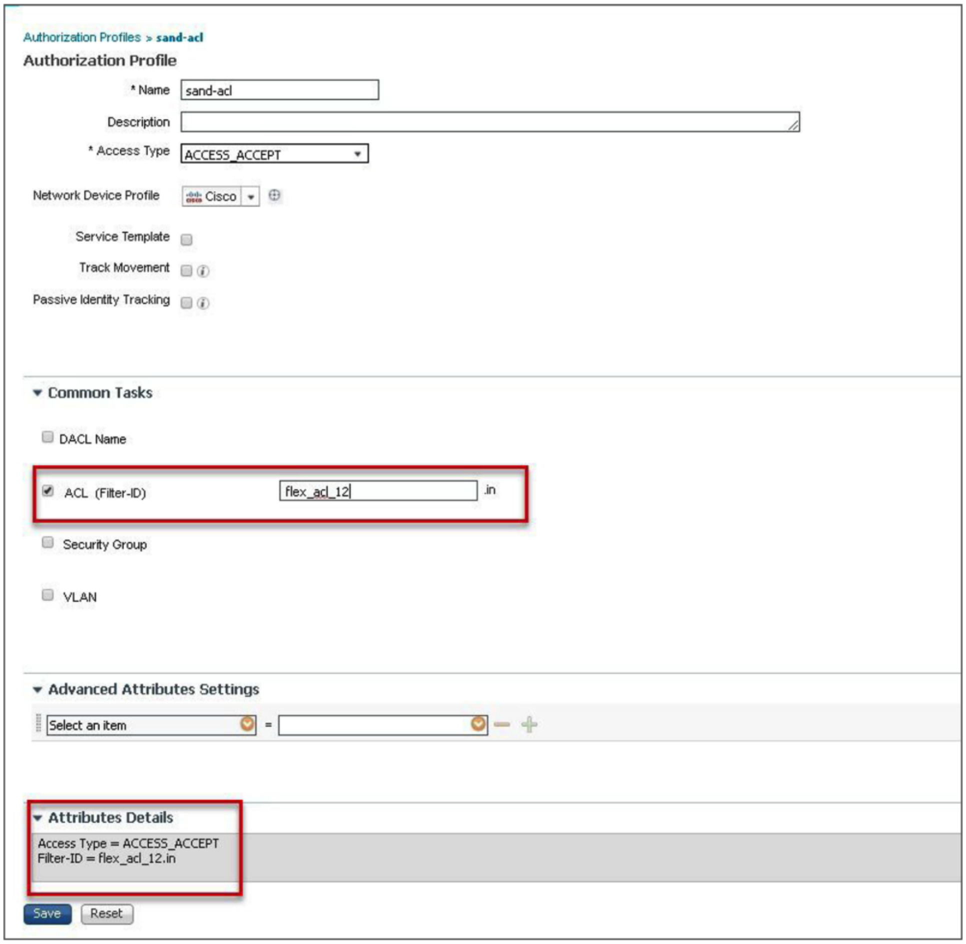
Procedure for WLAN ACL:

For creating a dot1x WLAN and enabling AAA override, refer to the procedure section of the VLAN override use case.

FlexConnect VLAN override

Procedure

Step 1. Authorization profile on ISE for returning ACL as an AAA attribute.



Authorization Profiles > sand-acl

Authorization Profile

* Name: sand-acl

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

Common Tasks

□ DACL Name

☑ ACL (Filter-ID) flex_acl_12 .in

□ Security Group

□ VLAN

Advanced Attributes Settings

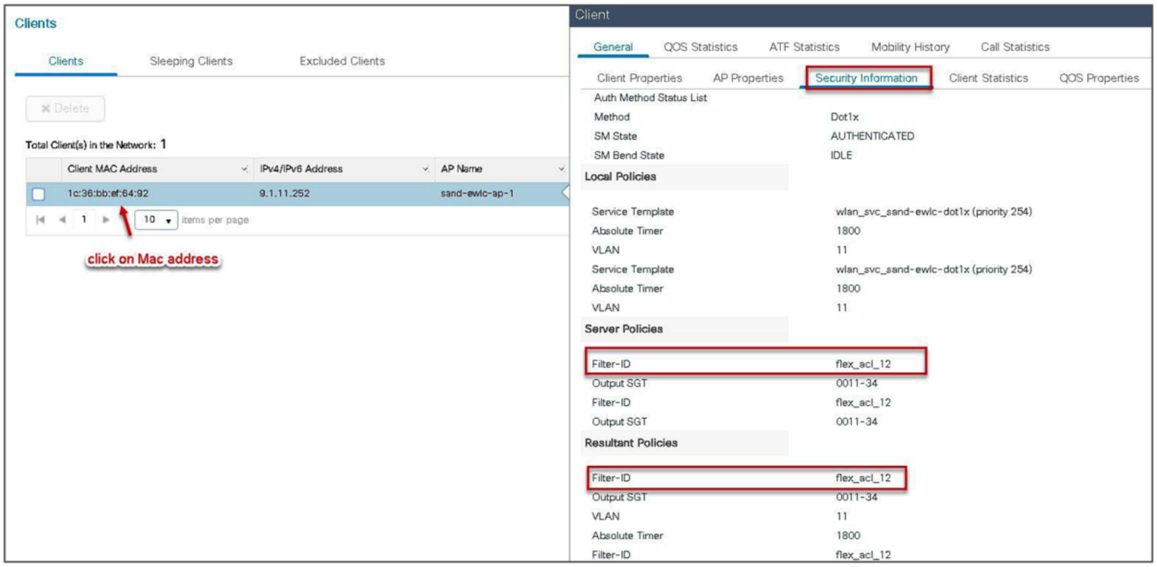
Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
Filter-ID = flex_acl_12.in

Step 2. Verification of ACL getting enforced on the AP and WLC.

Navigate to Monitor > Wireless > Clients.



Total Client(s) in the Network: 1

	Client MAC Address	IPv4/IPv6 Address	AP Name
□	1c:36:bb:ef:64:92	9.1.11.252	sand-ewlc-ap-1

Auth Method Status List

Method	Dot1x
SM State	AUTHENTICATED
SM Bend State	IDLE
Local Policies	
Service Template	wlan_svc_sand-ewlc-dot1x (priority 254)
Absolute Timer	1800
VLAN	11
Service Template	wlan_svc_sand-ewlc-dot1x (priority 254)
Absolute Timer	1800
VLAN	11
Server Policies	
Filter-ID	flex_acl_12
Output SGT	0011-34
Filter-ID	flex_acl_12
Output SGT	0011-34
Resultant Policies	
Filter-ID	flex_acl_12
Output SGT	0011-34
VLAN	11
Absolute Timer	1800
Filter-ID	flex_acl_12

Limitations

- The use of downloadable ACL is not supported on FlexConnect local switching. The downloadable ACLs are only supported for central switching.
- In case of central authentication if an ACL is returned from the AAA server but the corresponding ACL is not present on the AP, the client will be excluded with the reason being ACL failure.
- In the case of local authentication, the client will be de-authenticated continuously.

AP pre-image download

This feature allows the AP to download code while it is operational. The AP pre-image download is extremely useful in reducing the network downtime during software maintenance or upgrades. For the AP pre-image download to work, the controller should be in install mode of operation. If the controller is running in bundle mode, first have it converted to install mode before proceeding to AP pre-image download.

Summary

- Ease of software management
- Schedule per branch updates: NCS or Cisco Prime® is needed to accomplish this.
- Reduces downtime

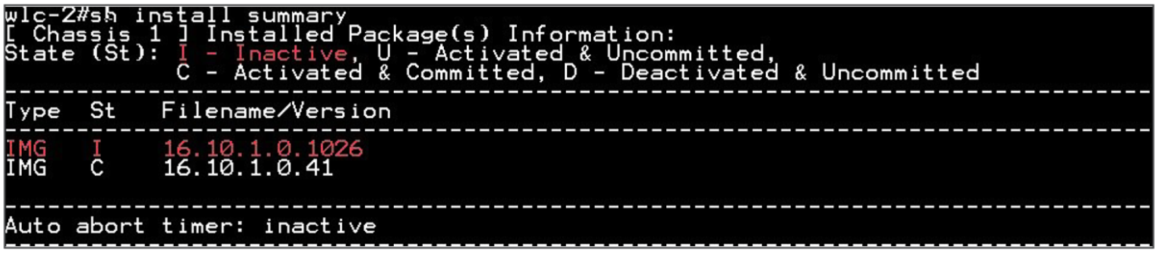
Procedure

Procedure

Step 1. Copy the image on the controller flash and the add the file using the install command:

```
wlc-2#install add file bootflash:wlc9500C-universalk9.BLD_V1610_THROTTLE_
010435.SSA.bin
```

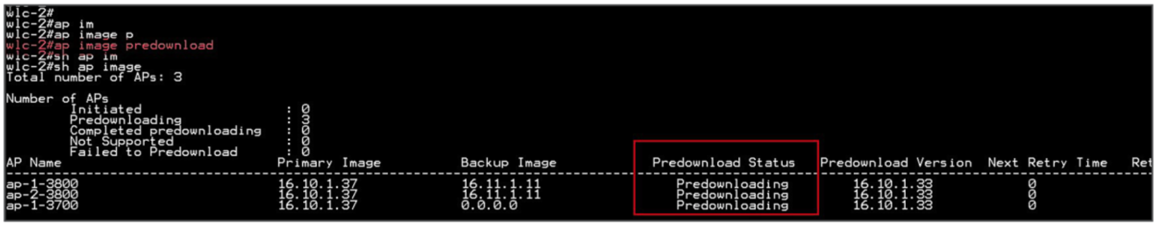
The install file command runs base compatibility checks on a file to ensure that the package is supported on the platform. It also adds an entry in the package, so that its status can be monitored and maintained.



```
wlc-2#sh install summary
[ Chassis 1 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   I    16.10.1.0.1026
IMG   C    16.10.1.0.41

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

Step 2. Once the file is added, the image can be pushed to the AP using the following CLI:

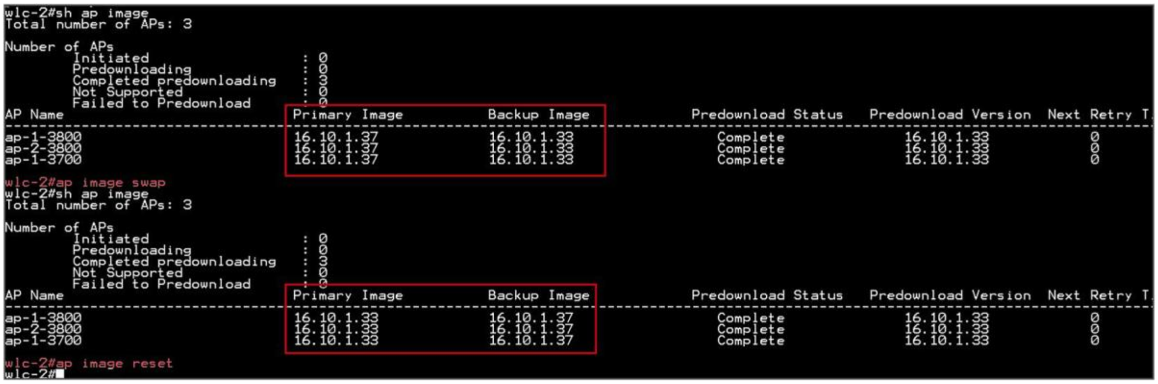
```
"ap image predownload"
```



```
wlc-2#
wlc-2#ap im
wlc-2#ap image p
wlc-2#ap image predownload
wlc-2#sh ap im
wlc-2#sh ap image
Total number of APs: 3

Number of APs
        Initiated                        : 0
        Predownloading                   : 3
        Completed predownloading         : 0
        Not Supported                    : 0
        Failed to Predownload            : 0
AP Name                          Primary Image          Backup Image          Predownload Status   Predownload Version   Next Retry Time   Ret
--------------------------------------------------------------------------------------------------------------------------------------------
ap-1-3800                        16.10.1.37             16.11.1.11              Predownloading       16.10.1.33            0
ap-2-3800                        16.10.1.37             16.11.1.11              Predownloading       16.10.1.33            0
ap-1-3700                        16.10.1.37             0.0.0.0                 Predownloading       16.10.1.33            0
```

Once the download is completed on the AP, issue the following CLI to swap the image and reset the AP:

- ap image swap
- ap image reset



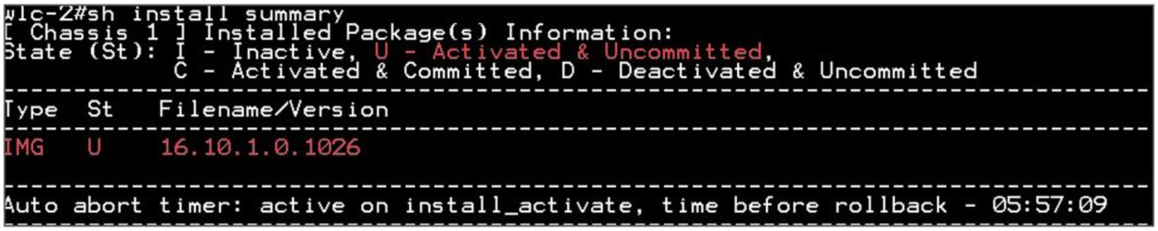
```
wlc-2#sh ap image
Total number of APs: 3

Number of APs
        Initiated                        : 0
        Predownloading                   : 0
        Completed predownloading         : 3
        Not Supported                    : 0
        Failed to Predownload            : 0
AP Name                           Primary Image          Backup Image           Predownload Status   Predownload Version   Next Retry T
-------------------------------------------------------------------------------------------------------------------------------------
ap-1-3800                         16.10.1.37             16.10.1.33                Complete             16.10.1.33            0
ap-2-3800                         16.10.1.37             16.10.1.33                Complete             16.10.1.33            0
ap-1-3700                         16.10.1.37             16.10.1.33                Complete             16.10.1.33            0
wlc-2#ap image swap
wlc-2#sh ap image
Total number of APs: 3

Number of APs
        Initiated                        : 0
        Predownloading                   : 0
        Completed predownloading         : 3
        Not Supported                    : 0
        Failed to Predownload            : 0
AP Name                           Primary Image          Backup Image           Predownload Status   Predownload Version   Next Retry T
-------------------------------------------------------------------------------------------------------------------------------------
ap-1-3800                         16.10.1.33             16.10.1.37                Complete             16.10.1.33            0
ap-2-3800                         16.10.1.33             16.10.1.37                Complete             16.10.1.33            0
ap-1-3700                         16.10.1.33             16.10.1.37                Complete             16.10.1.33            0
wlc-2#ap image reset
wlc-2#
```

Step 3. After the AP has been reset, use the following CLI to activate the image on the controller:

"Install Activate"

The Install Activate runs compatibility checks, installs the package, and updates the package status details. For a non-restartable package, it triggers a reload. The systems will prompt for saving the config and a reboot during the process.

Please input the response to save the config and reboot the WLC.

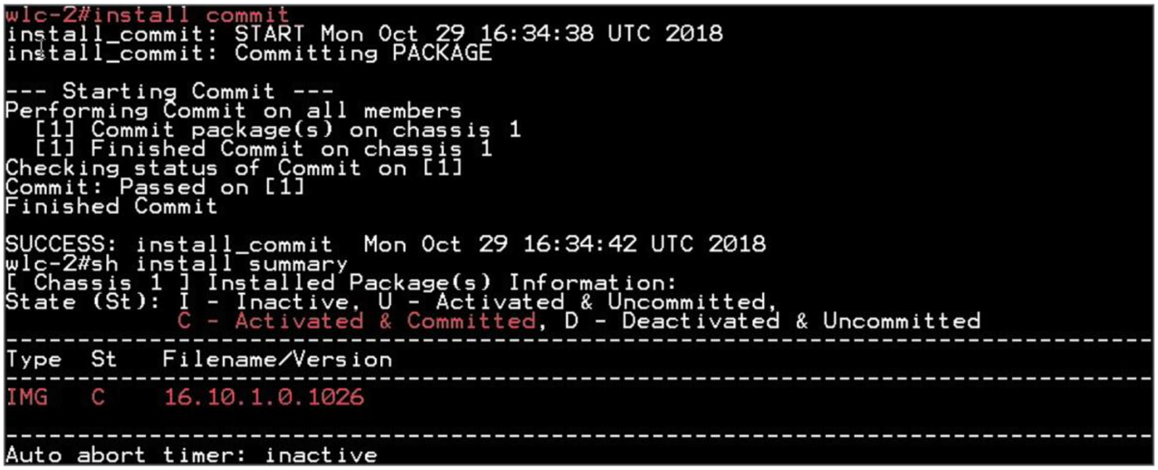


```
wlc-2#sh install summary
[ Chassis 1 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   U    16.10.1.0.1026

--------------------------------------------------------------------------------
Auto abort timer: active on install_activate, time before rollback - 05:57:09
--------------------------------------------------------------------------------
```

Step 4. Once the system is rebooted, use the following CLI to have the changes persist across reboot.

"Install Commit"

This commits the activation changes to be persistent across reloads The commit can be done after activation while the system is up, or after the first reload. If a package is activated but not committed, it remains active after the first reload, but not after the second reload.



```
wlc-2#install commit
install_commit: START Mon Oct 29 16:34:38 UTC 2018
install_commit: Committing PACKAGE

--- Starting Commit ---
Performing Commit on all members
  [1] Commit package(s) on chassis 1
  [1] Finished Commit on chassis 1
Checking status of Commit on [1]
Commit: Passed on [1]
Finished Commit

SUCCESS: install_commit  Mon Oct 29 16:34:42 UTC 2018
wlc-2#sh install summary
[ Chassis 1 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    16.10.1.0.1026

--------------------------------------------------------------------------------
Auto abort timer: inactive
```

Limitation

The controller needs to be in install mode for the AP pre-image to work. If a controller works in bundle mode, it needs to be converted to install mode. Please refer to Cisco.com for the conversion for bundle mode to install mode.

FlexConnect smart AP image upgrade

The pre-image download feature reduces the downtime duration to a certain extent, but still all the FlexConnect APs have to pre-download the respective AP images over the WAN link with higher latency.

Efficient AP image upgrade will reduce the downtime for each FlexConnect AP. The basic idea is only one AP of each AP model will download the image from the controller and will act as Primary/Server, and the rest of the APs of the same model will work as Secondary/Client and will pre-download the AP image from the primary. The distribution of AP image from the server to the client will be on a local network and will not experience the latency of the WAN link. As a result, the process will be faster.

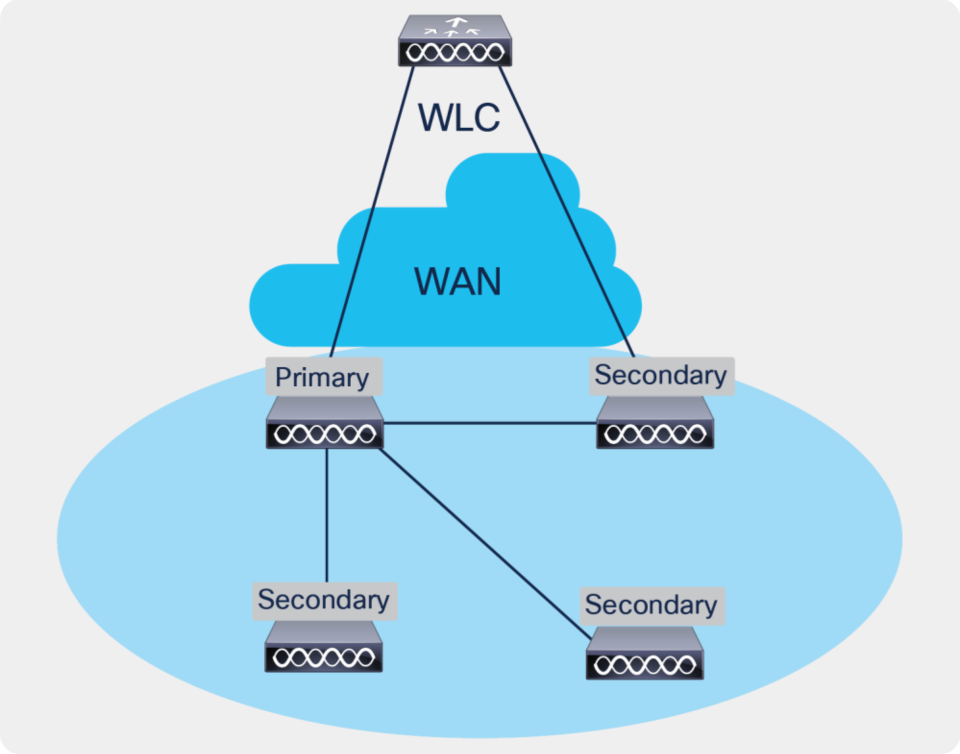


Figure 8.
FlexConnect Smart AP Image Upgrade Mechanism

Summary

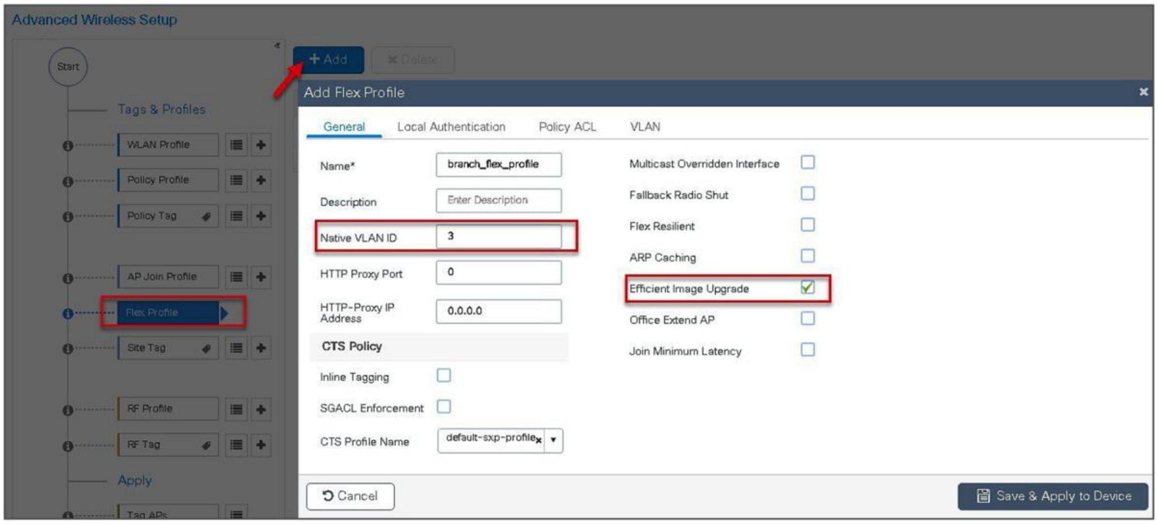
- Primary and secondary APs are selected for each AP model per site tag.
- Primary downloads image from WLC.
- Secondary downloads image from primary AP using TFTP.
- Reduces downtime and saves WAN bandwidth.
- The primary is chosen by the system. The AP with the lowest MAC among the same type and model is to become a primary.

Procedure

Procedure

Step 1. For steps to create a flex profile and to have it applied on the AP, refer to the steps in the advanced config wizard section of the document.

Enable smart AP image upgrade on the flex profile.



Add Flex Profile

Name* branch_flex_profile

Description Enter Description

Native VLAN ID 3

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 □

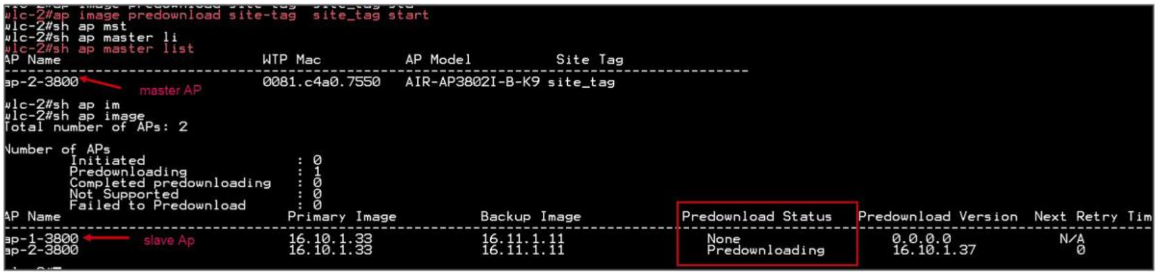
Join Minimum Latency □

Step 2. Download the image on the controller as outlined in step 1 of the AP image pre-download process. Issue the CLI below to initiate the smart AP image upgrade and also to see the primary AP elected for a given type of AP and the primary downloading image from the controller.

AP Pre-Image Download

```
ap image predownload site-tag <site_name> start
```

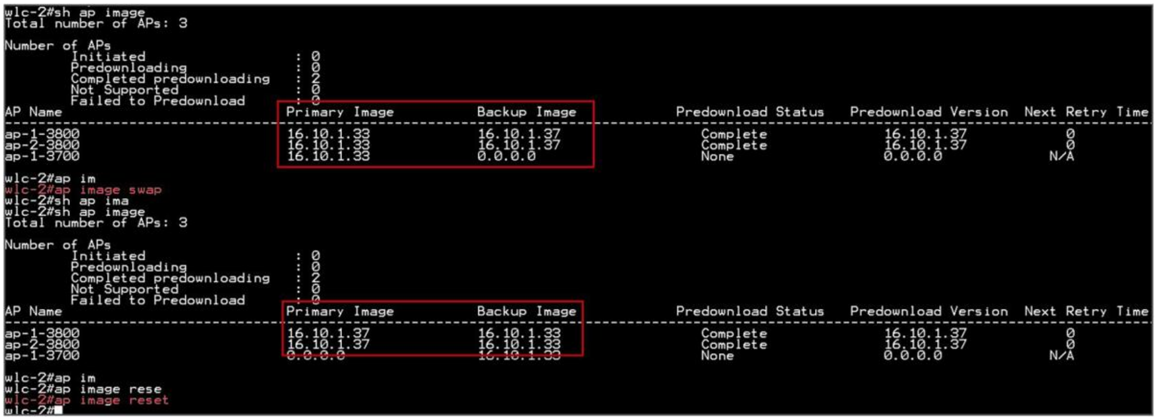
It is important to give the site tag and start the pre-image download process, as this would initiate the smart AP image upgrade process. If the site tag is not specified, the download falls back to the normal pre-image download process.



```
wlc-2#ap image predownload site-tag  site_tag start
wlc-2#sh ap mst
wlc-2#sh ap master li
wlc-2#sh ap master list
AP Name                         WTP Mac          AP Model          Site Tag
------------------------------------------------------------------------------------
ap-2-3800                       0081.c4a0.7550   AIR-AP3802I-B-K9 site_tag

wlc-2#sh ap im
wlc-2#sh ap image
Total number of APs: 2

Number of APs
        Initiated                      : 0
        Predownloading                 : 1
        Completed predownloading       : 0
        Not Supported                  : 0
        Failed to Predownload          : 0
AP Name                            Primary Image          Backup Image          Predownload Status    Predownload Version   Next Retry Tim
------------------------------------------------------------------------------------------------------------------------------------------
ap-1-3800                          16.10.1.33             16.11.1.11              None                  0.0.0.0              N/A
ap-2-3800                          16.10.1.33             16.11.1.11              Predownloading        16.10.1.37           0
```

Step 3. After the image pre-download on the AP is completed, follow the sequence below:

- Swap the AP image and reset the AP using the CLI “ap image swap” and “ap image reset.”
- Activate the image using the “Install Activate” CLI.
- During the activation, the WLC will go for a reboot. Use the CLI “Install Commit” to persist the changes across the reboot.



```
wlc-2#sh ap image
Total number of APs: 3

Number of APs
        Initiated                  : 0
        Predownloading             : 0
        Completed predownloading   : 2
        Not Supported              : 0
        Failed to Predownload      : 0
AP Name                           Primary Image          Backup Image               Predownload Status    Predownload Version   Next Retry Time
--------------------------------------------------------------------------------------------------------------------------------------------
ap-1-3800                         16.10.1.33             16.10.1.37                    Complete              16.10.1.37              0
ap-2-3800                         16.10.1.33             16.10.1.37                    Complete              16.10.1.37              0
ap-1-3700                         16.10.1.33             0.0.0.0                       None                  0.0.0.0               N/A

wlc-2#ap im
wlc-2#ap image swap
wlc-2#sh ap ima
wlc-2#sh ap image
Total number of APs: 3

Number of APs
        Initiated                  : 0
        Predownloading             : 0
        Completed predownloading   : 2
        Not Supported              : 0
        Failed to Predownload      : 0
AP Name                           Primary Image          Backup Image               Predownload Status    Predownload Version   Next Retry Time
--------------------------------------------------------------------------------------------------------------------------------------------
ap-1-3800                         16.10.1.37             16.10.1.33                    Complete              16.10.1.37              0
ap-2-3800                         16.10.1.37             16.10.1.33                    Complete              16.10.1.37              0
ap-1-3700                         0.0.0.0                16.10.1.33                    None                  0.0.0.0               N/A

wlc-2#ap im
wlc-2#ap image rese
wlc-2#ap image reset
wlc-2#
```

Limitation

The system decides on the election of a primary AP, and the decision on who the primary is decided when the smart AP image download process is initiated. Once the decision is made, any AP that joins after and which has a lower MAC will not alter or change the primary AP already elected.

FlexConnect pre-auth ACL and URL filtering

The URL filtering is an extension to the ACL deployments current in place. With the addition of URL filtering, the ACL can accept internet domain names in addition to the existing IP address rules. The FlexConnect deployments support the LWA, CWA, and BYOD flow. The LWA refers to the local web authentication done on the WLC while the CWA refers to the guest authentication done on the Identity Service Engine. The BYOD flow requires access to the app store for downloading the supplicant for which URL filters can be used. The use for URL filter can also be extended to CMX connect social login where the authentication happens on the social network site.

Summary

Pre-auth ACL refers to a state when a wireless client would require access to resources prior to getting authenticated. In the case of LWA/CWA or BYOD, the client might require access to resources before getting full access into the network. The URL filtering for flex is supported only on the Wave 2 platforms. The URL filtering follows a permit list and block list model of working. The administrator can specify up to 20 URLS within a URL filter. The URL filter supports wild-card matching to support sub-URL matching.

For e.g.:

URL type	Definition
cisco*	match any URL that starts with Cisco
***cisco.com**	match any URL that ends in cisco.com
www.cisco.com	match the exact string

The URL-filtering ACL works along with a regular ACL to have the URL ACL pushed to a flex AP. It needs to be linked with a regular ACL in the flex profile. The URL ACL works by snooping the DNS transaction between the DNS client and a DNS server. For flex deployment, the DNS snooping is performed on the AP for each client. With snooping in place, the AP learns the IP address of the resolved domain name in the DNS response.

If the domain name matches the configured URL, then the DNS response is parsed for the IP address, and the IP address is mapped in the ACL for locally switched traffic. The rules created from DNS parsing has a permit or deny based on the URL filtering rules, which is either permit listing or block listing. When a packet from or to a client traverses through the AP, the DNS rules are processed first before proceeding with the regular ACL processing. The URL filtering is optional configuration on the LWA and CWA flow.

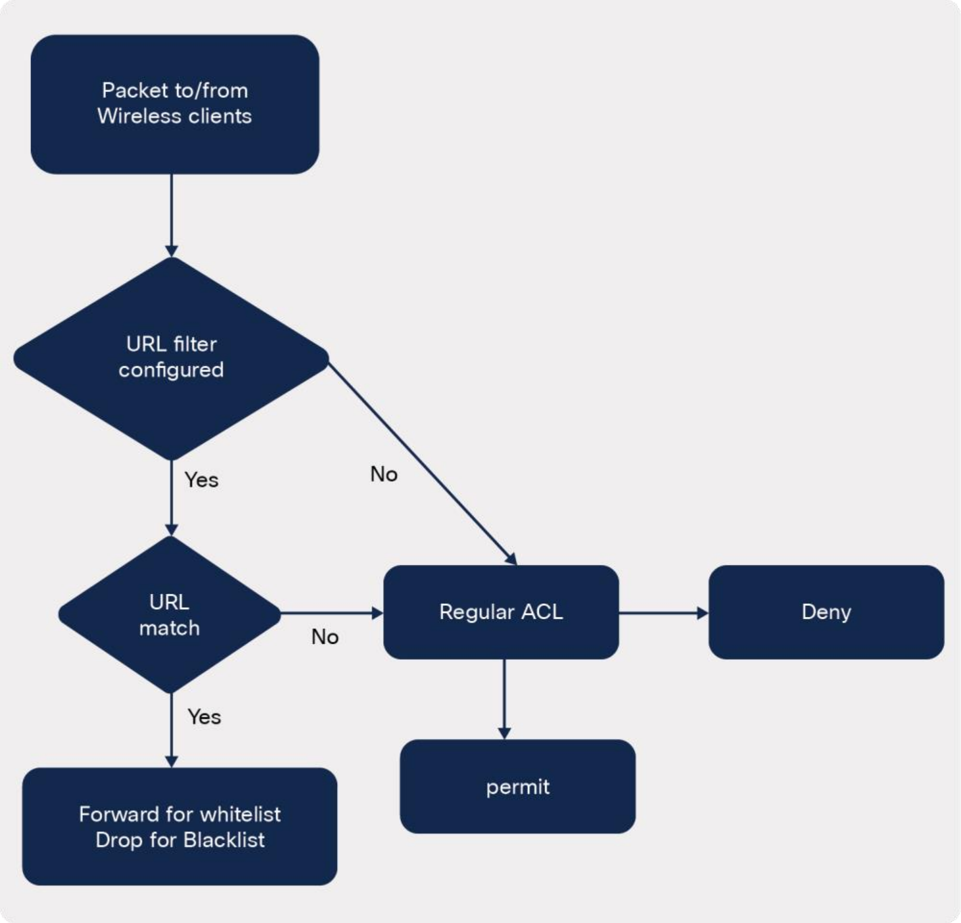

Packet to/from Wireless clients
URL filter configured
Yes
No
URL match
No
Regular ACL
Deny
Yes
permit
Forward for whitelist Drop for Blacklist

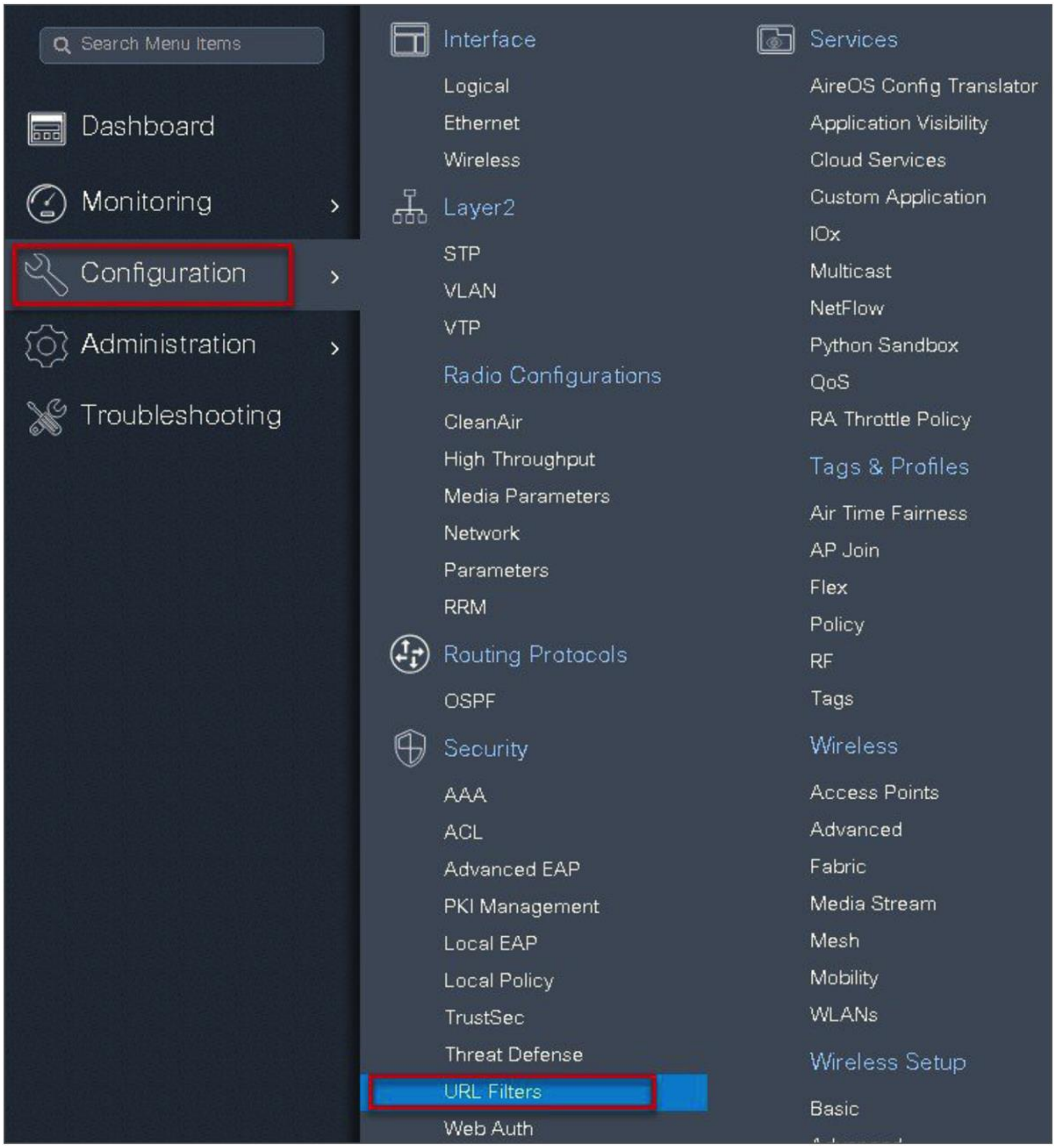
Figure 9.
URL-filtering ACL logic

LWA flow with URL filter

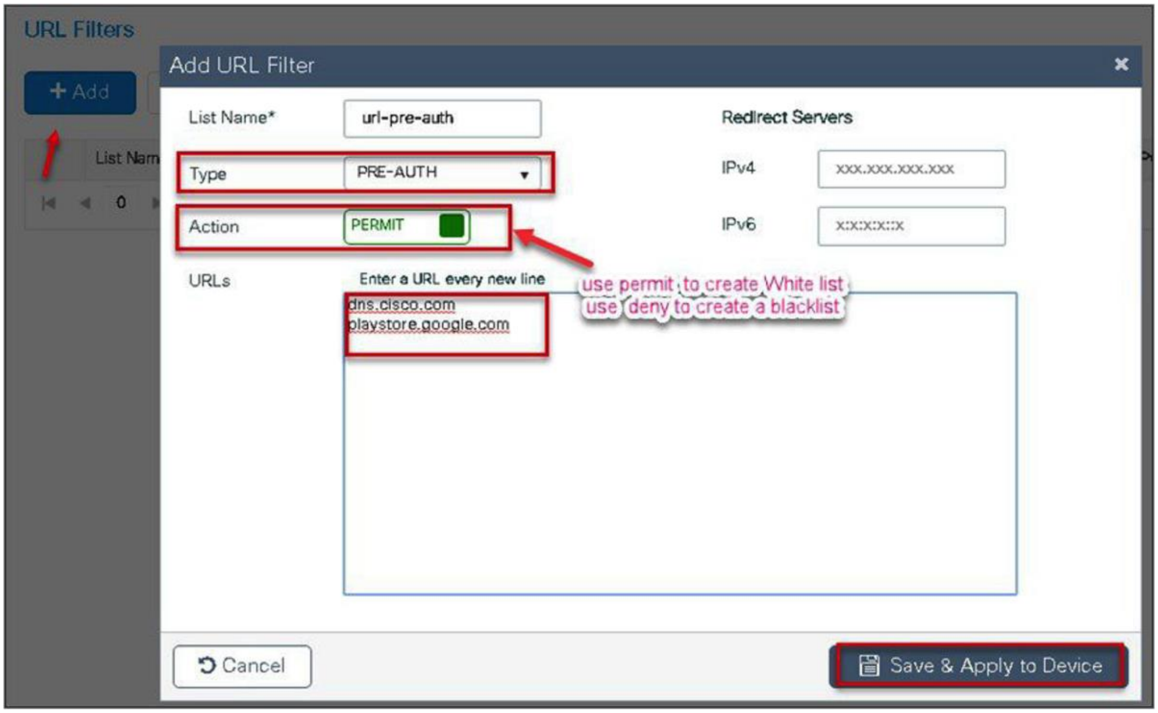
This section describes the steps to set up LWA with pre-auth ACL and URL filter. For the local web authentication, the pre-auth ACL and URL filtering is optional.

Procedure

Step 1. To create a URL filter, navigate to Configuration > Security > URL Filters.



Step 2. Create a URL filter.



List Name*: url-pre-auth

Type: PRE-AUTH

Action: PERMIT

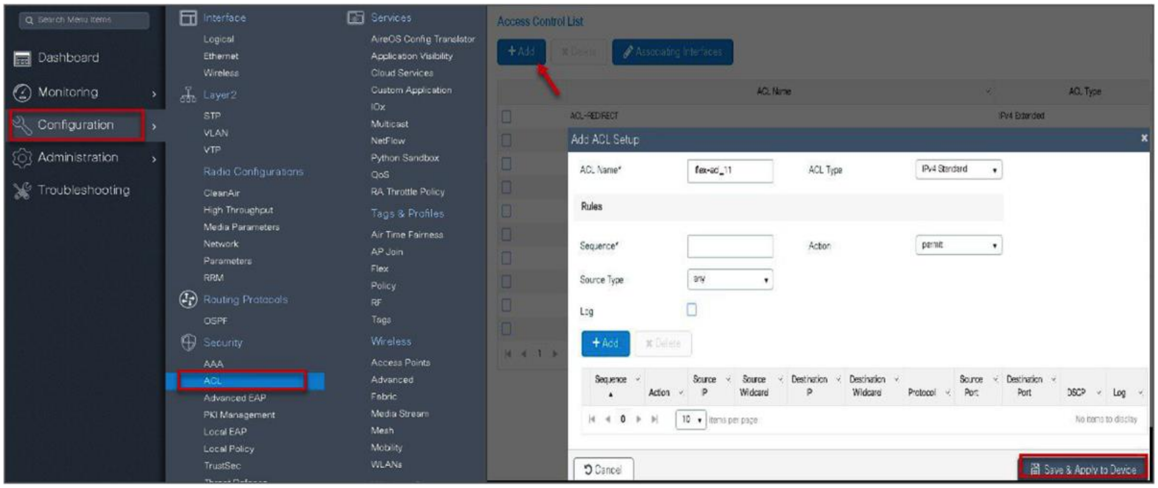
URLs: Enter a URL every new line

```
dns.cisco.com
playstore.google.com
```

IPv4: xxx.xxx.xxx.xxx

IPv6: x:x:x:x::x

Step 3. Create an ACL on the WLC to link with the URL ACL.



ACL Name	ACL Type
ACL-REDIRECT	IPv4 Extended

ACL Name*: flex-acl_11

ACL Type: IPv4 Standard

Sequence*:

Action: permit

Source Type: any

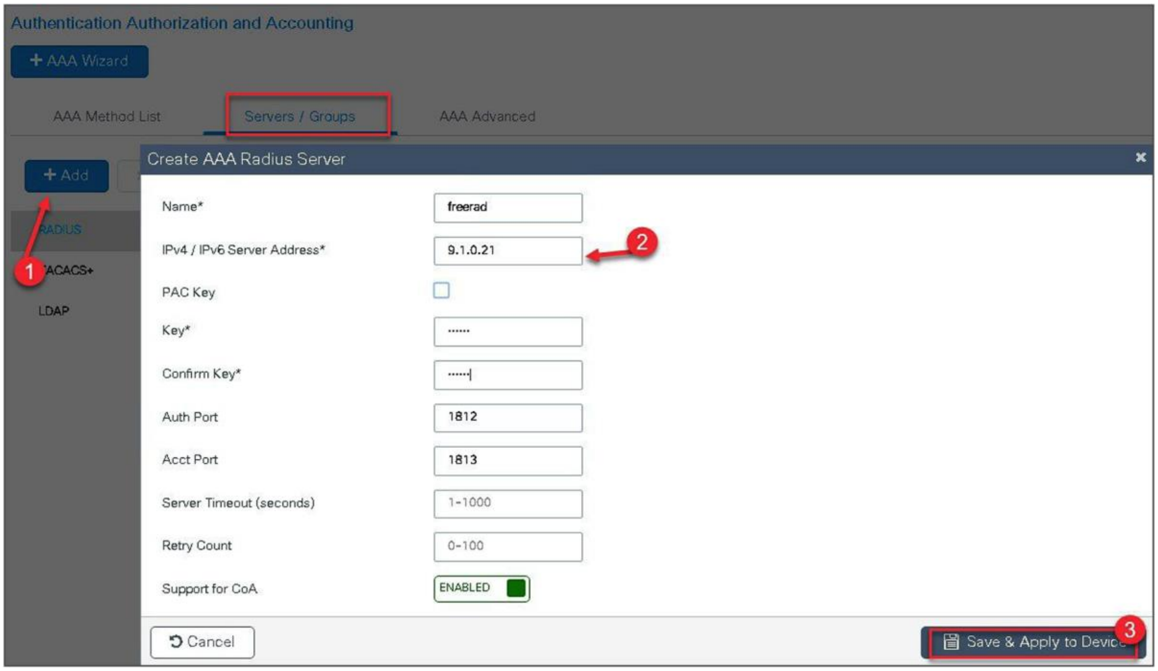
Log: □

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log

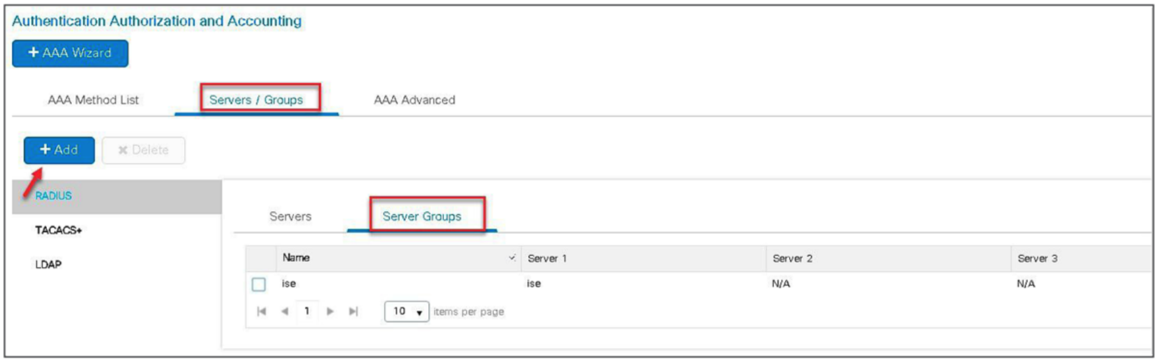
0 | 10 items per page | No items to display

Step 4. Create an authentication list on the WLC to be used on the LWA WLAN. The authentication list can point to a radius server or can do a local lookup.

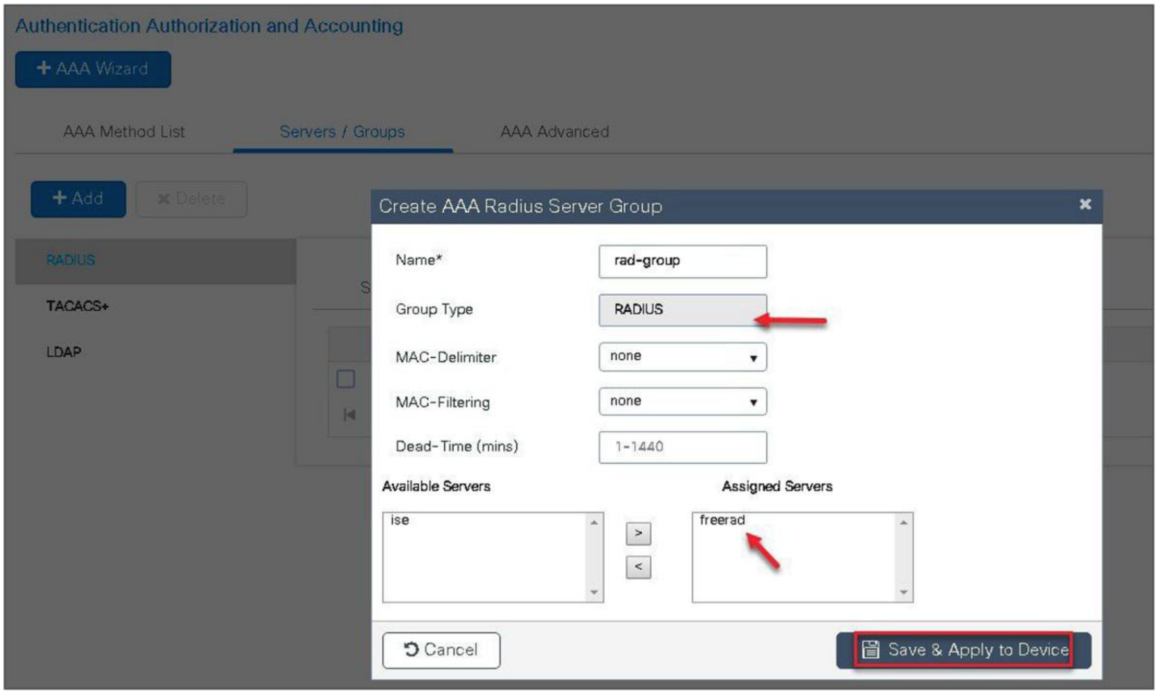
Navigate to Configuration > Security > AAA.



Name*	freerad
IPv4 / IPv6 Server Address*	9.1.0.21
PAC Key	□
Key*	••••••
Confirm Key*	••••••
Auth Port	1812
Acct Port	1813
Server Timeout (seconds)	1-1000
Retry Count	0-100
Support for CoA	ENABLED



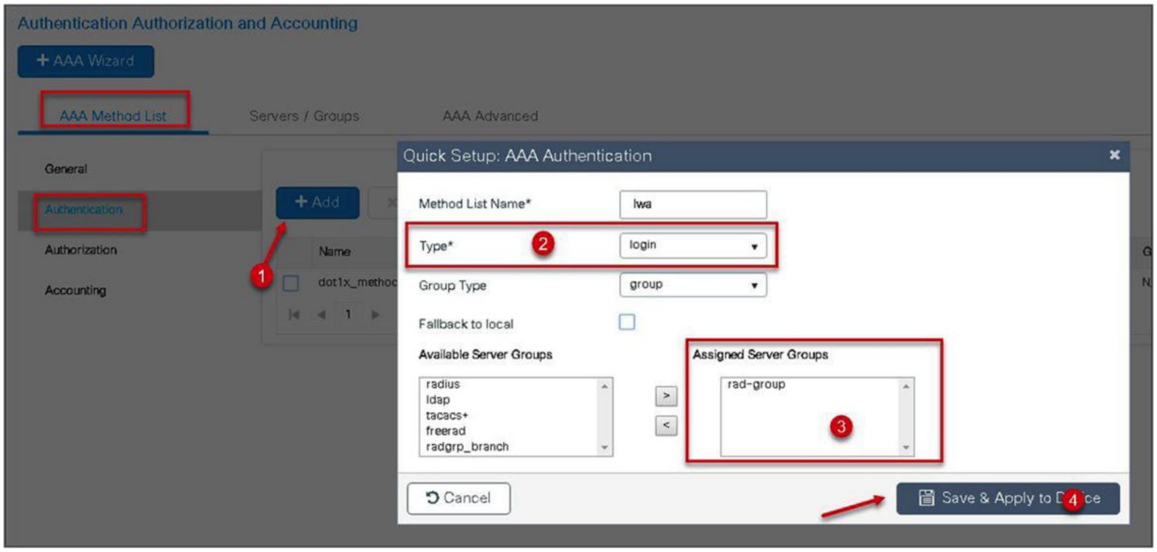
	Name	Server 1	Server 2	Server 3
□	ise	ise	N/A	N/A



Create AAA Radius Server Group

Name*	rad-group
Group Type	RADIUS
MAC-Delimiter	none
MAC-Filtering	none
Dead-Time (mins)	1-1440

Available Servers	Assigned Servers
ise	freerad



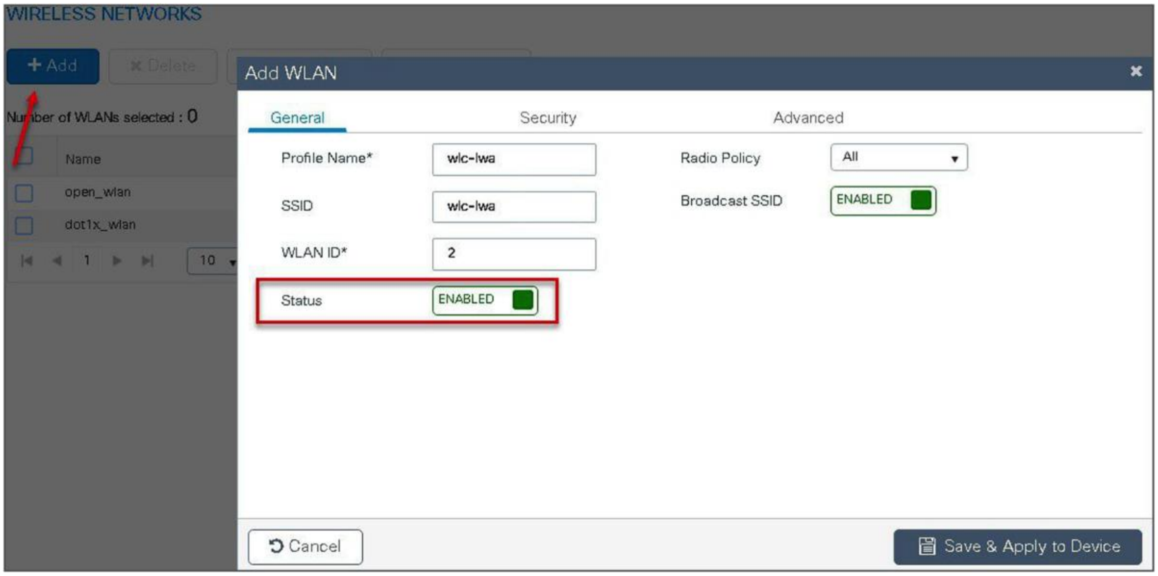
Quick Setup: AAA Authentication

Method List Name*	lwa
Type*	login
Group Type	group
Fallback to local	□

Available Server Groups	Assigned Server Groups
radius ldap tacacs+ freerad radgrp_branch	rad-group

Step 5. Create a WLAN to local web-authentication flow.

Navigate to Configuration > Tags & Profiles > WLAN.



Profile Name* wlc-lwa

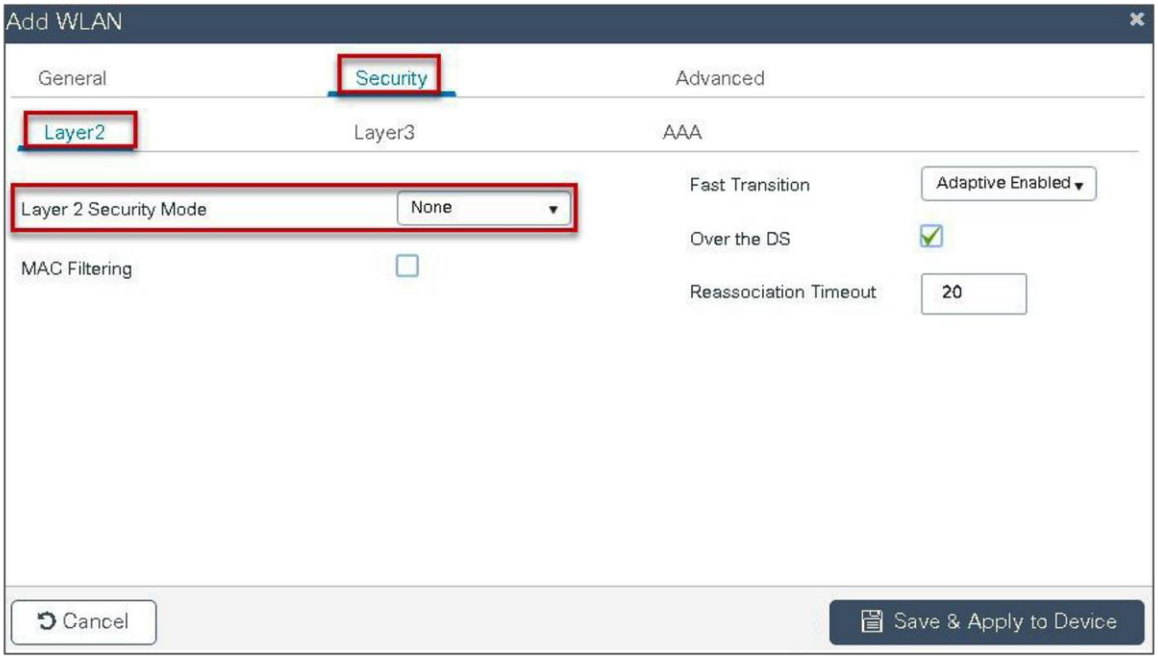
SSID wlc-lwa

WLAN ID* 2

Status ENABLED

Radio Policy All

Broadcast SSID ENABLED



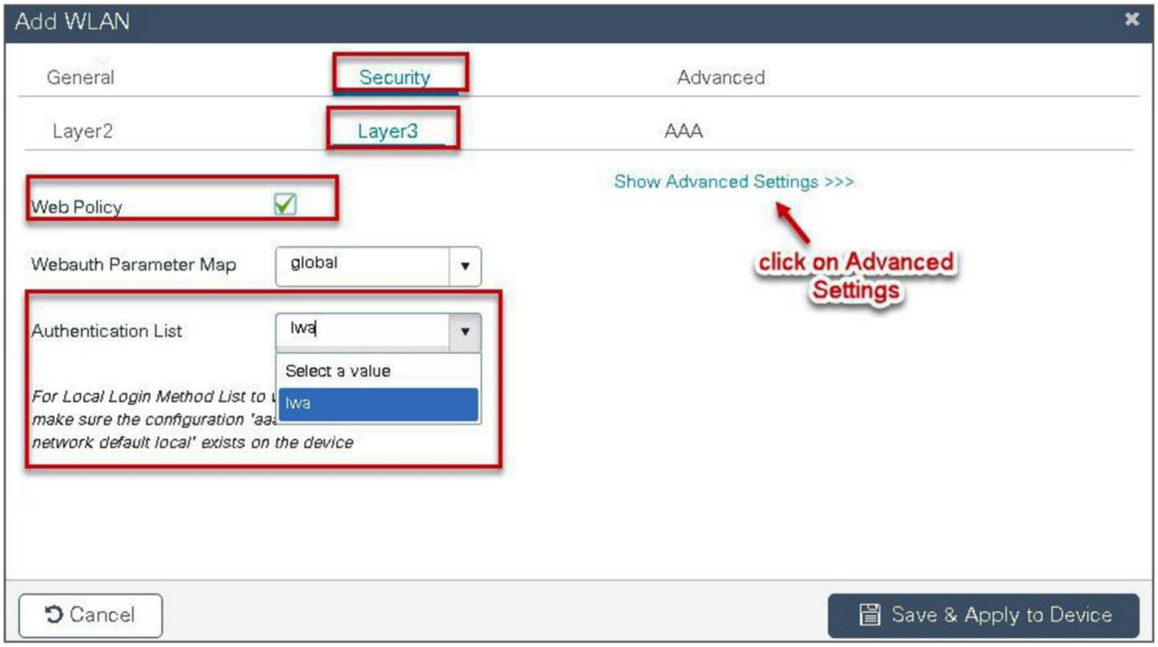
Layer 2 Security Mode None

MAC Filtering ☐

Fast Transition Adaptive Enabled

Over the DS ☑

Reassociation Timeout 20



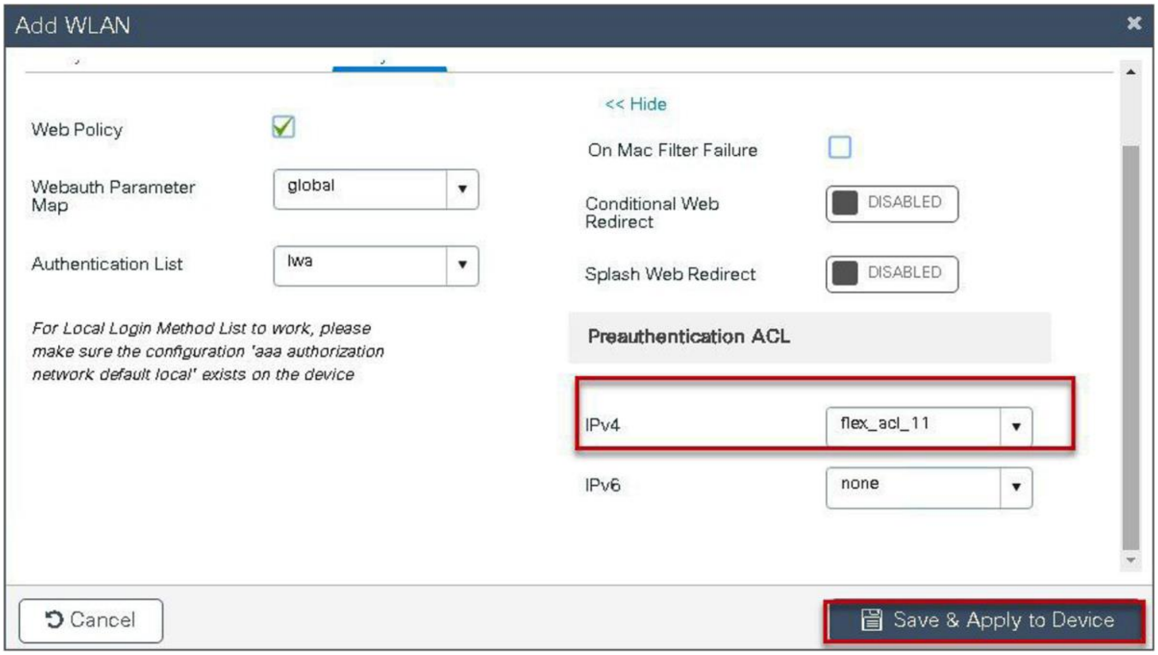
Web Policy ☑

Webauth Parameter Map: global

Authentication List: lwa

For Local Login Method List to w… make sure the configuration 'aa… network default local' exists on the device

click on Advanced Settings



Web Policy ☑

Webauth Parameter Map: global

Authentication List: lwa

For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device

On Mac Filter Failure □

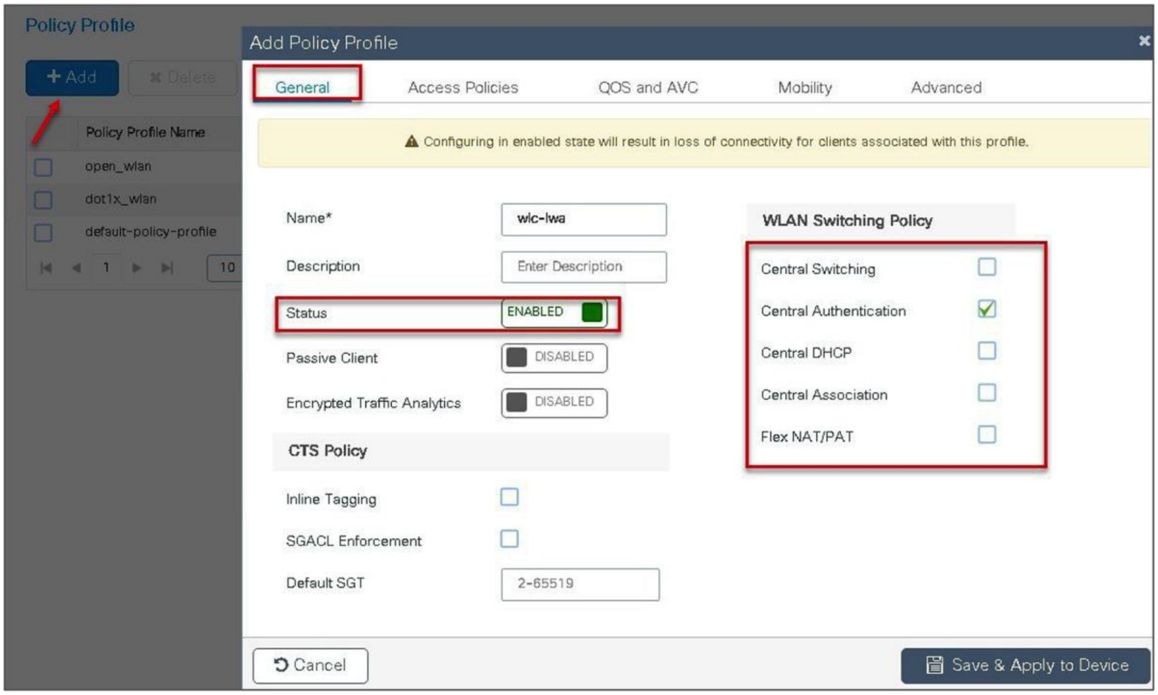
Conditional Web Redirect: DISABLED

Splash Web Redirect: DISABLED

IPv4: flex_acl_11

IPv6: none

Step 6. Create a policy profile.



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

Name*: wlc-lwa

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

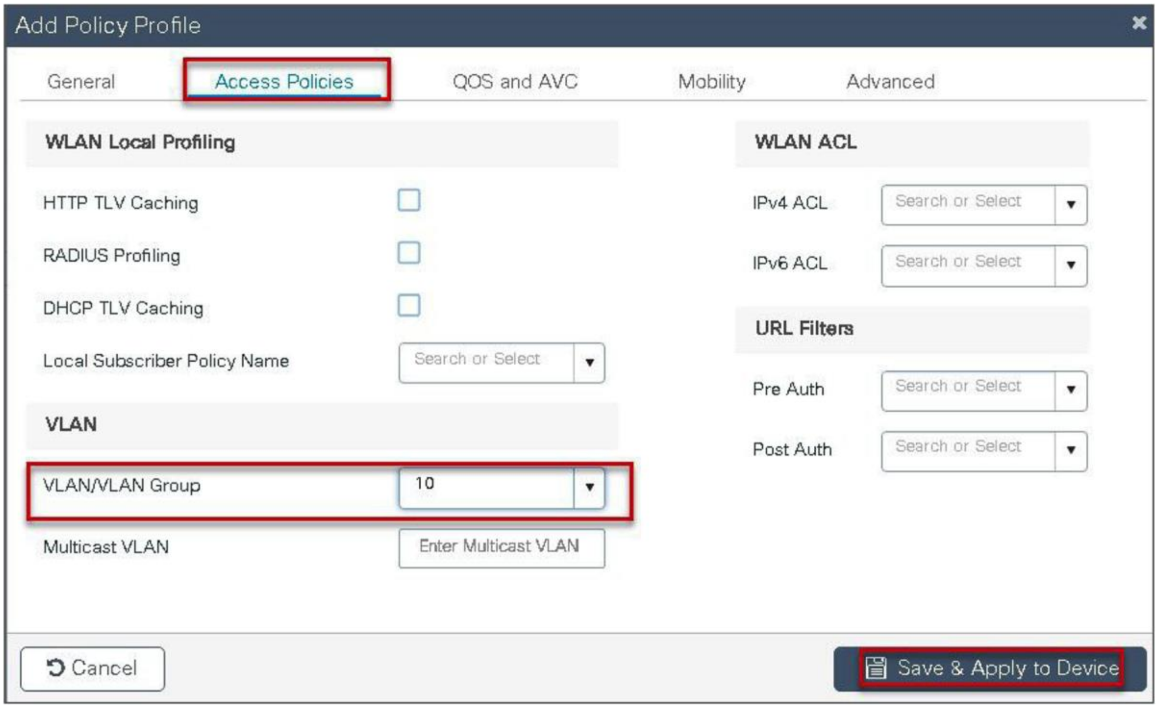
Central Switching □

Central Authentication ☑

Central DHCP □

Central Association □

Flex NAT/PAT □



WLAN Local Profiling

HTTP TLV Caching □

RADIUS Profiling □

DHCP TLV Caching □

Local Subscriber Policy Name: Search or Select

VLAN

VLAN/VLAN Group: 10

Multicast VLAN: Enter Multicast VLAN

WLAN ACL

IPv4 ACL: Search or Select

IPv6 ACL: Search or Select

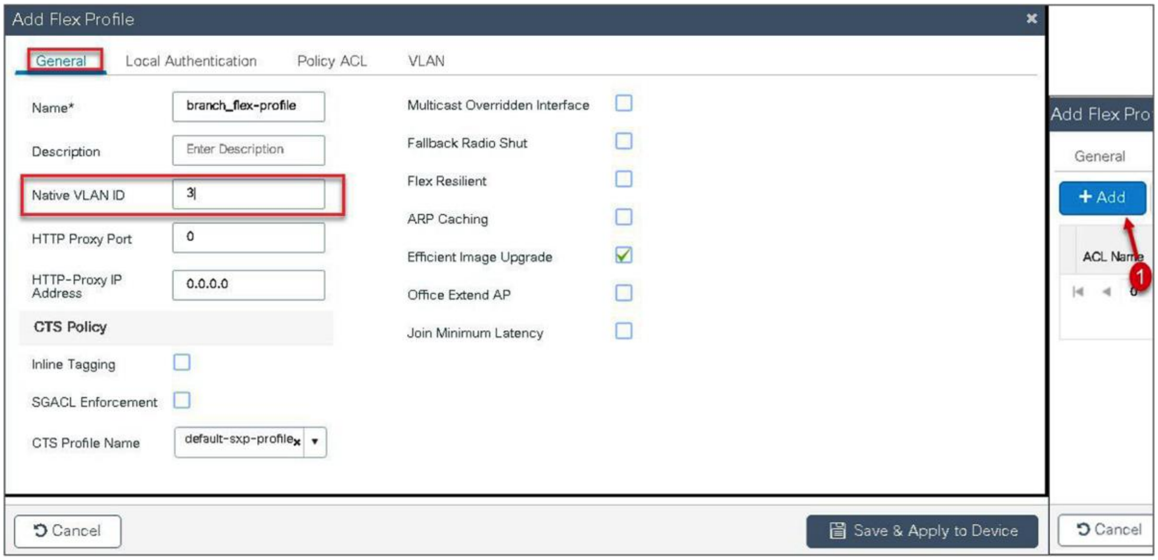
URL Filters

Pre Auth: Search or Select

Post Auth: Search or Select

Step 7. Create a flex profile.

Navigate to Configuration > Tags & Profiles > Flex.



Add Flex Profile

General | Local Authentication | Policy ACL | VLAN

Name*	branch_flex-profile
Description	Enter Description
Native VLAN ID	3
HTTP Proxy Port	0
HTTP-Proxy IP Address	0.0.0.0

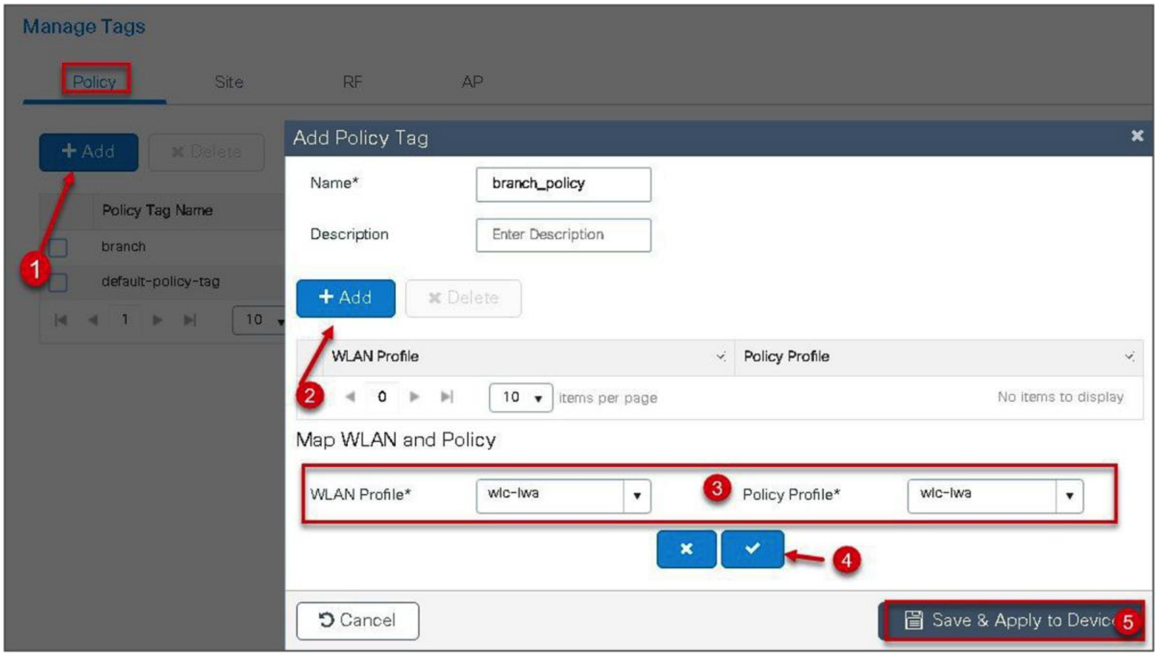
CTS Policy

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 8. Create a site tag mapping the policy tag and flex profile.

Navigate to Configuration > Tags & Profiles > Tags.



Manage Tags

Policy | Site | RF | AP

Policy Tag Name
branch
default-policy-tag

Add Policy Tag

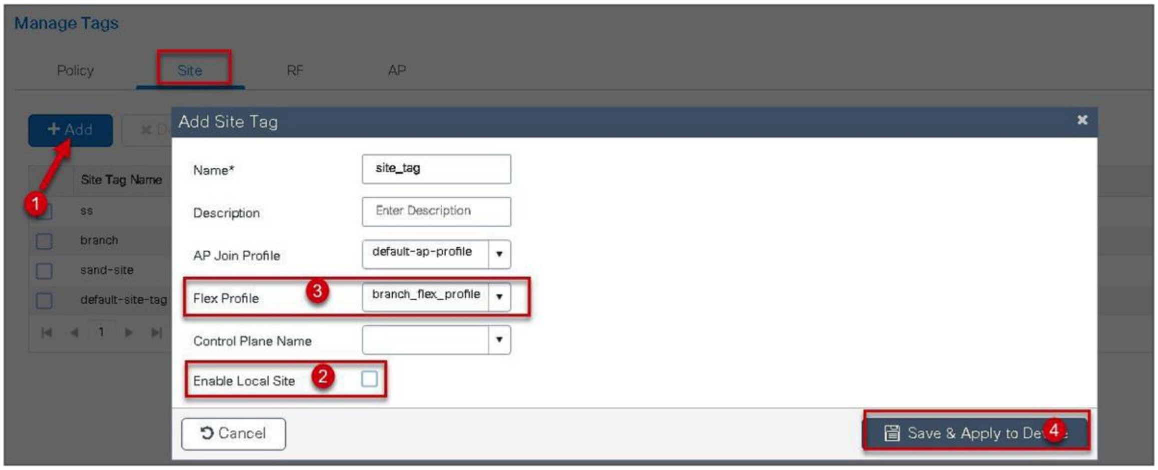
Name*	branch_policy
Description	Enter Description

WLAN Profile	Policy Profile

No items to display

Map WLAN and Policy

WLAN Profile*	wlc-lwa	Policy Profile*	wlc-lwa



Add Site Tag

Name* site_tag

Description Enter Description

AP Join Profile default-ap-profile

Flex Profile branch_flex_profile

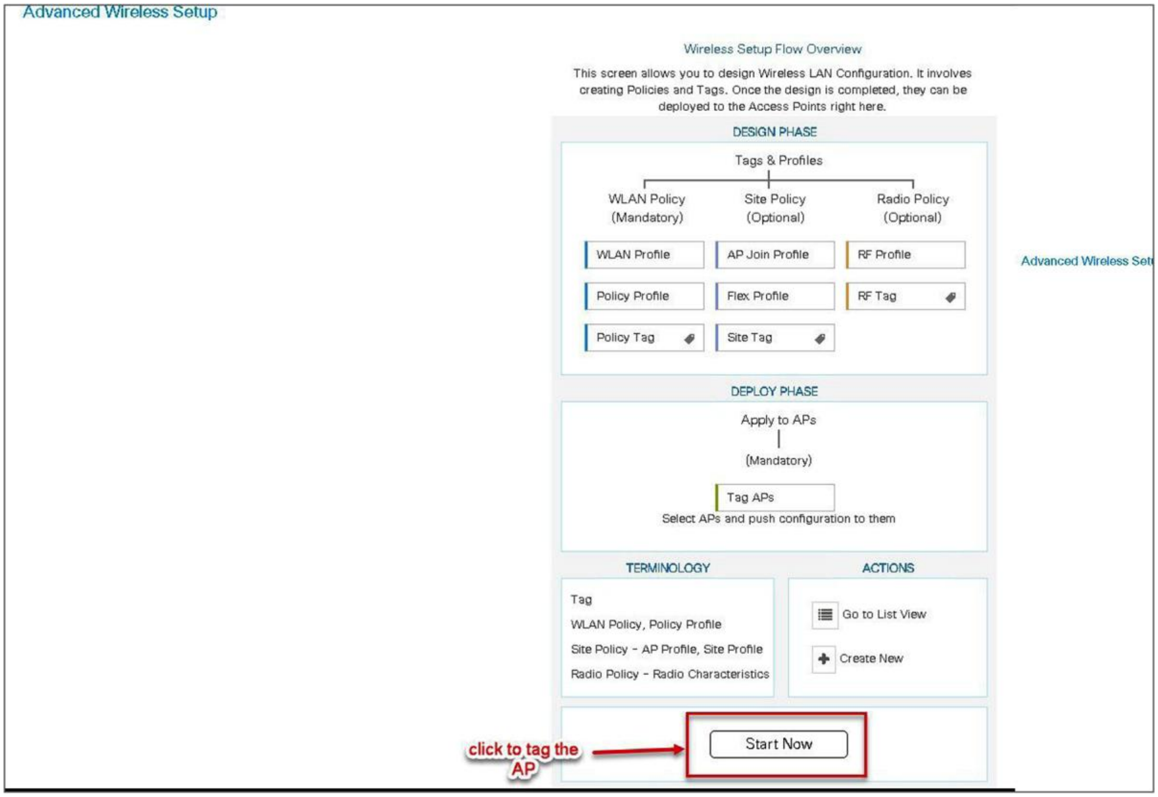
Control Plane Name

Enable Local Site □

Step 9. Map the tags on the AP. Once the APs are tagged with a policy profile, the APs will reboot due to conversion from local mode to FlexConnect mode.

If the APs are already in flex mode, the reboot wouldn't be triggered.

Navigate to Configuration > Wireless Setup > Advanced.



Advanced Wireless Setup

Wireless Setup Flow Overview

This screen allows you to design Wireless LAN Configuration. It involves creating Policies and Tags. Once the design is completed, they can be deployed to the Access Points right here.

Select APs and push configuration to them

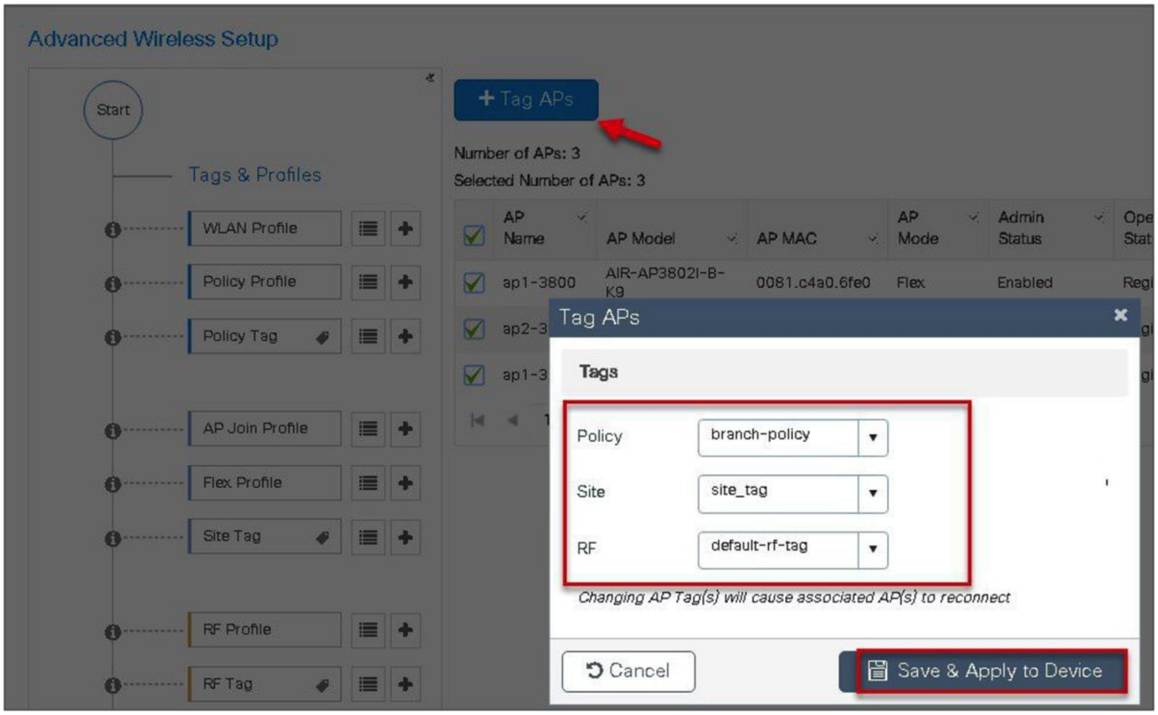
TERMINOLOGY

Tag

WLAN Policy, Policy Profile

Site Policy - AP Profile, Site Profile

Radio Policy - Radio Characteristics



Number of APs: 3

Selected Number of APs: 3

☑	AP Name	AP Model	AP MAC	AP Mode	Admin Status	Ope Stat
☑	ap1-3800	AIR-AP3802I-B-K9	0081.c4a0.6fe0	Flex	Enabled	Regi
☑	ap2-3					gi
☑	ap1-3					gi

Tag APs

Tags

Policy: branch-policy

Site: site_tag

RF: default-rf-tag

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

CWA flow on flex

This section describes the steps to set up CWA with the URL filter. For CWA flow, the URL filter is optional.

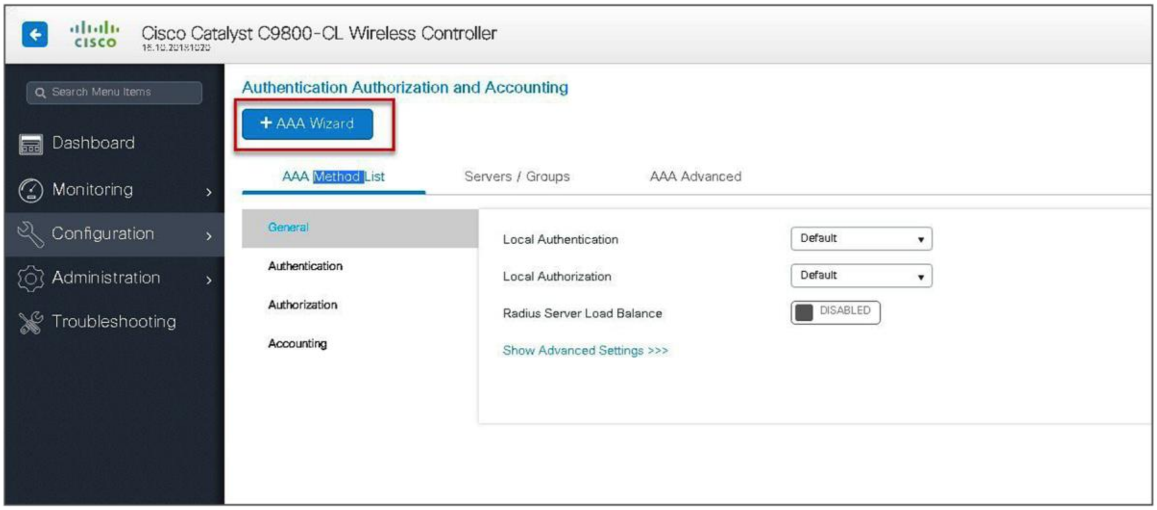
- Create a server and server group for MAC auth and AAA attributes.
- Create an authorization list on the controller.
- Create a MAB SSID and map the authorization list on the SSID.
- Create a redirect ACL and a URL filter (optional) on the controller.
- Bind the URL filter and ACL on the flex profile.
- Create an authorization profile on ISE to return the url-redirect and url-redirect-acl Cisco AV pair.

Procedure

Step 1. Create an authentication and authorization list on the WLC.

Navigate to Configuration > Security > AAA.

Use the AAA wizard to create the server and server groups.

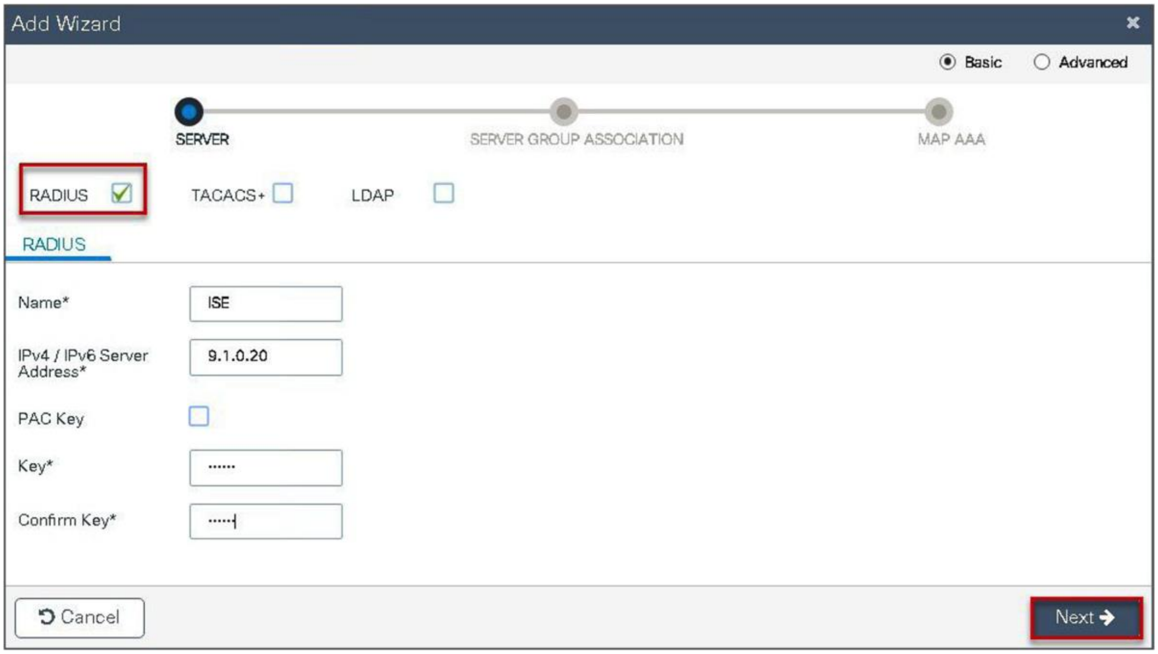


Local Authentication: Default

Local Authorization: Default

Radius Server Load Balance: DISABLED

Step 2. Define a name for the server and specify the IP address and shared secret.



● Basic ○ Advanced

RADIUS ☑ TACACS+ □ LDAP □

Name*: ISE

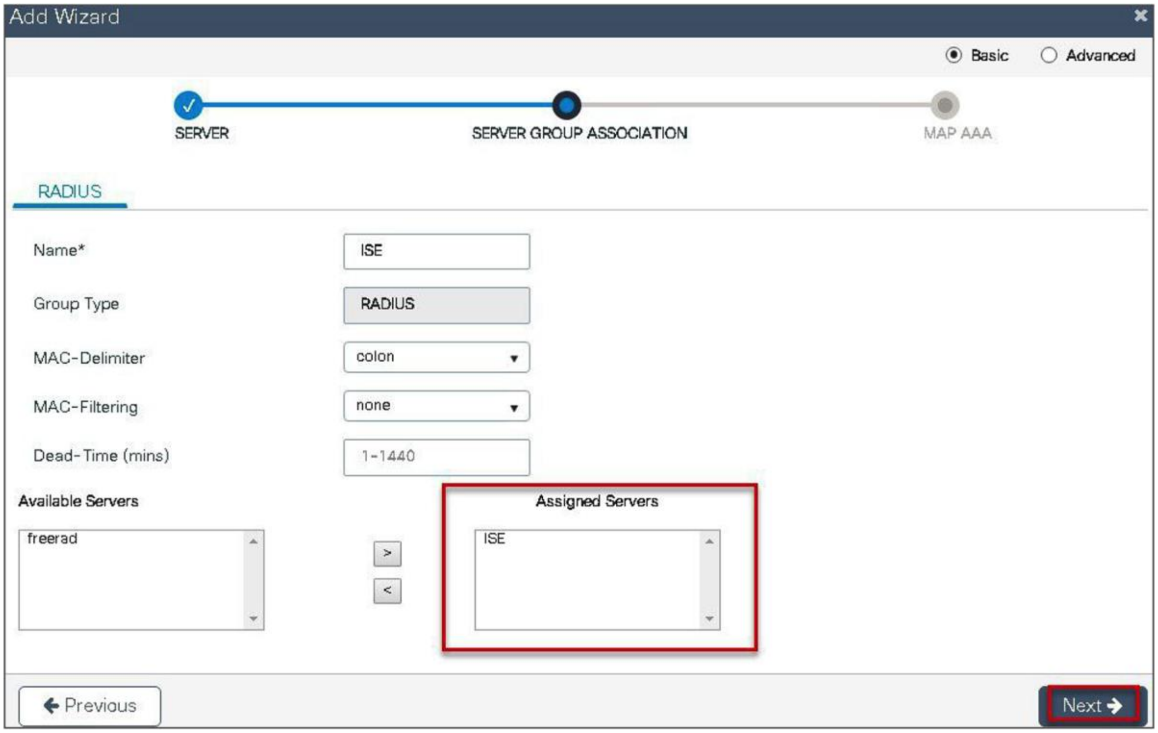
IPv4 / IPv6 Server Address*: 9.1.0.20

PAC Key □

Key*: ······

Confirm Key*: ······

Step 3. Create a server group and map the server in the group.



Add Wizard

● Basic ○ Advanced

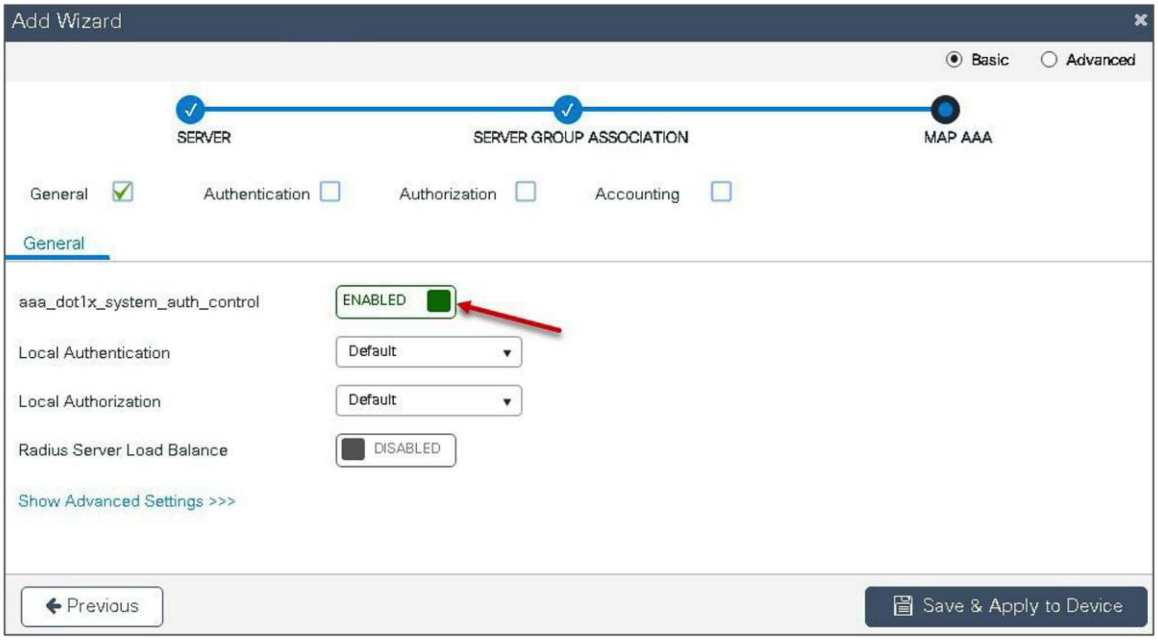
SERVER — SERVER GROUP ASSOCIATION — MAP AAA

RADIUS

Name*	ISE
Group Type	RADIUS
MAC-Delimiter	colon
MAC-Filtering	none
Dead-Time (mins)	1-1440

Available Servers		Assigned Servers
freerad	> <	ISE

Step 4. Enable dot1x system control and checkmark the authentication and authorization profile.



Add Wizard

● Basic ○ Advanced

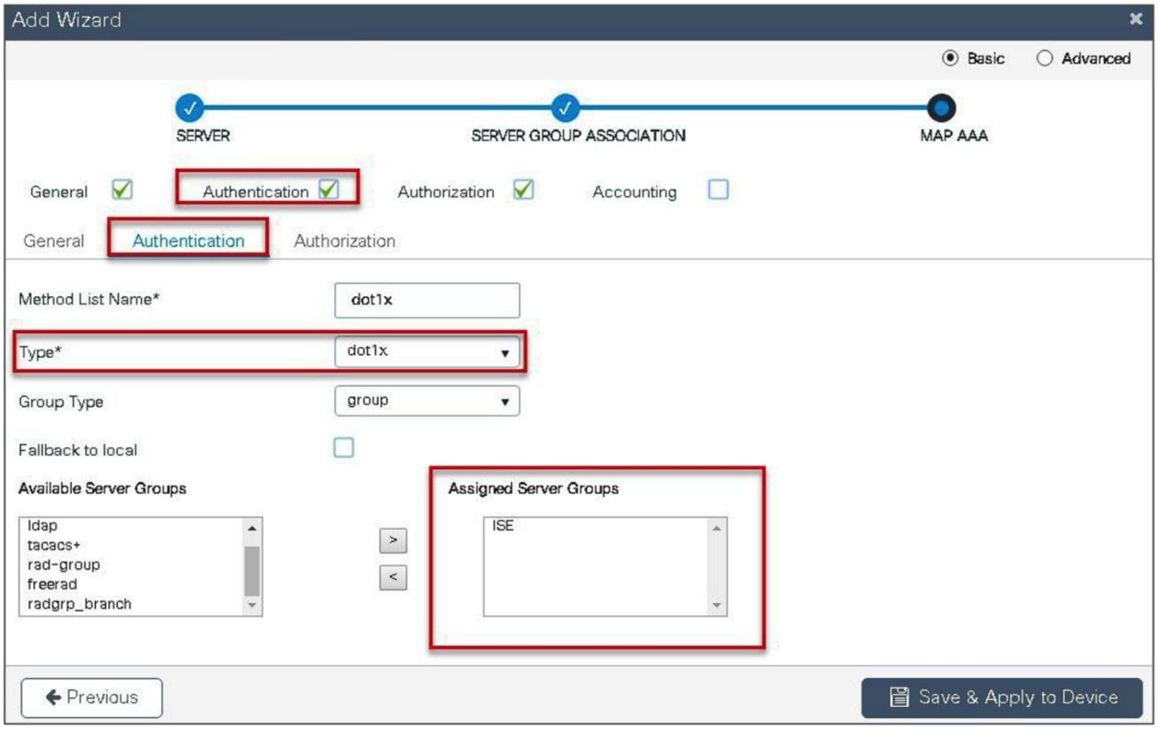
SERVER — SERVER GROUP ASSOCIATION — MAP AAA

General ☑ Authentication □ Authorization □ Accounting □

General

aaa_dot1x_system_auth_control	ENABLED
Local Authentication	Default
Local Authorization	Default
Radius Server Load Balance	DISABLED

Step 5. Define the method type as dot1x and map the server group.



Method List Name*: dot1x

Type*: dot1x

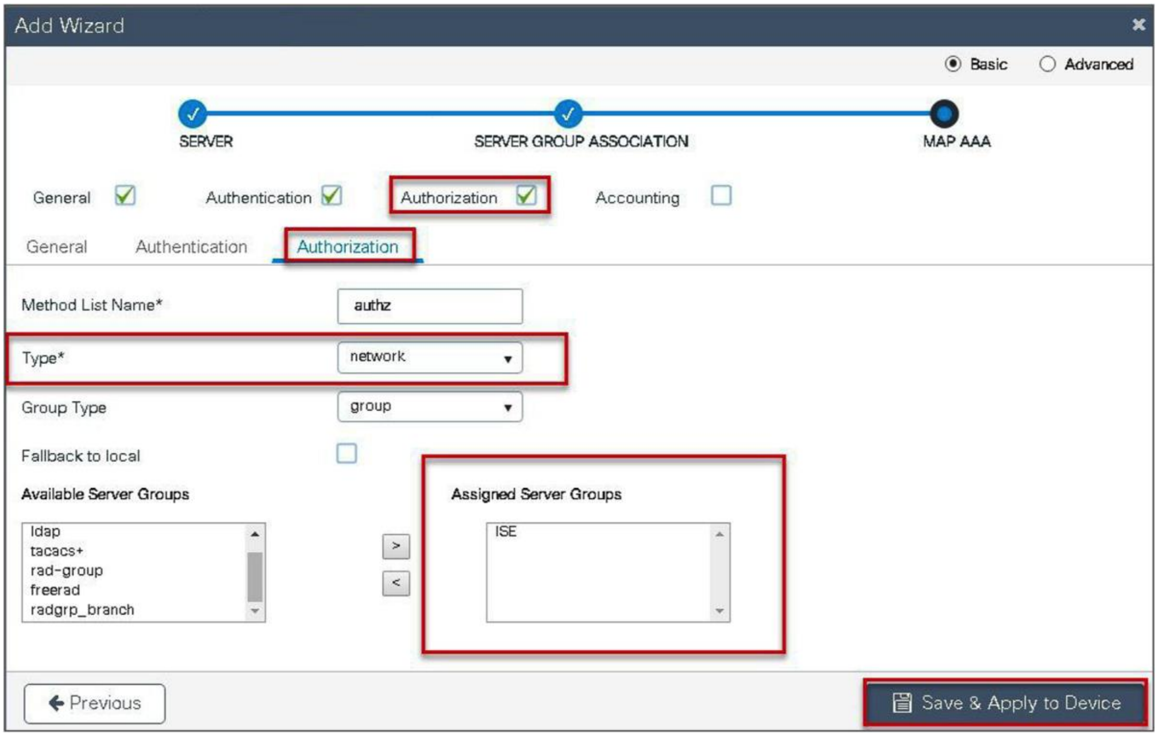
Group Type: group

Fallback to local: □

Available Server Groups: ldap, tacacs+, rad-group, freerad, radgrp_branch

Assigned Server Groups: ISE

Step 6. Define the method type as “network” and map the server group.



Method List Name*: authz

Type*: network

Group Type: group

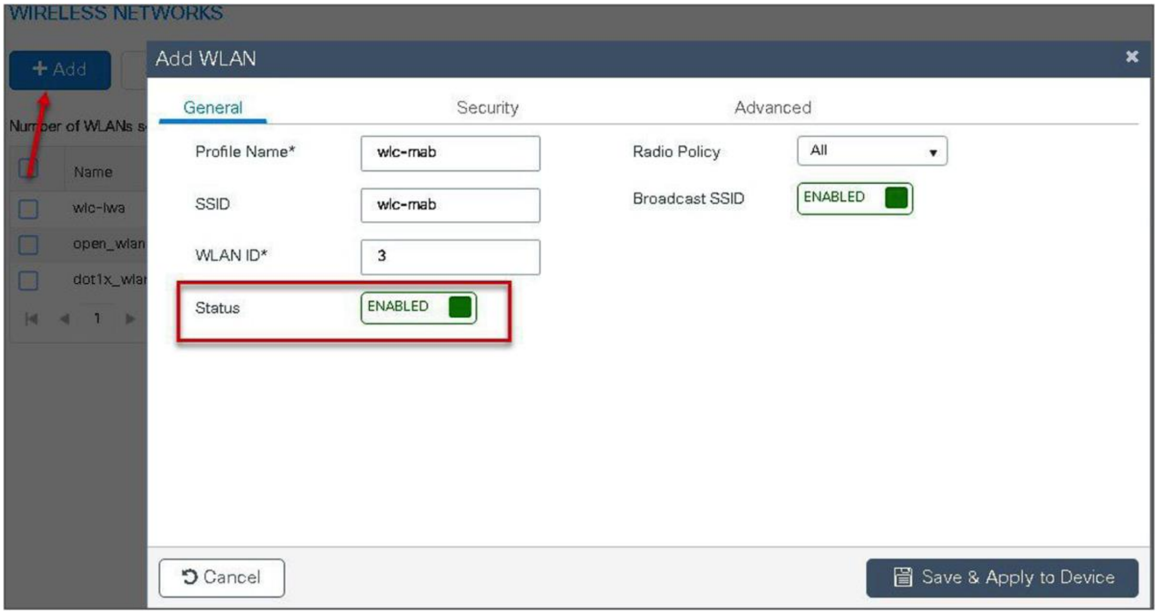
Fallback to local: □

Available Server Groups: ldap, tacacs+, rad-group, freerad, radgrp_branch

Assigned Server Groups: ISE

Step 7. Create a MAB SSID and map the authorization method list.

Navigate to Configuration > Tags & Profiles > WLAN.



Profile Name* wlc-mab

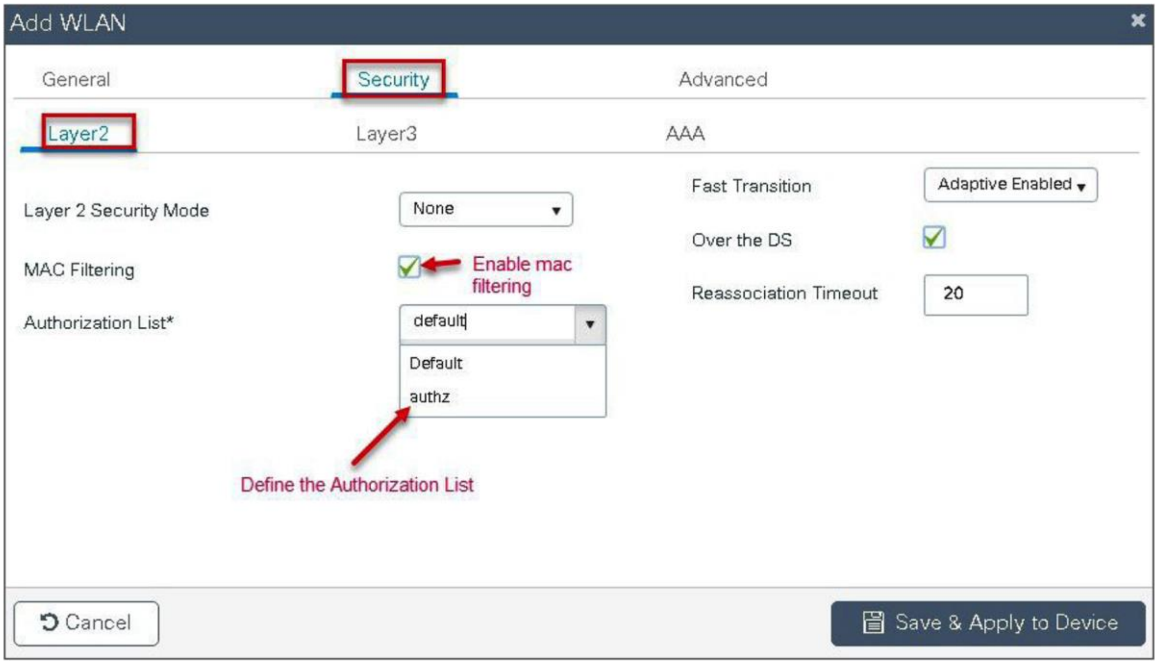
SSID wlc-mab

WLAN ID* 3

Status ENABLED

Radio Policy All

Broadcast SSID ENABLED



Layer 2 Security Mode None

MAC Filtering ☑

Enable mac filtering

Authorization List* default

Define the Authorization List

Fast Transition Adaptive Enabled

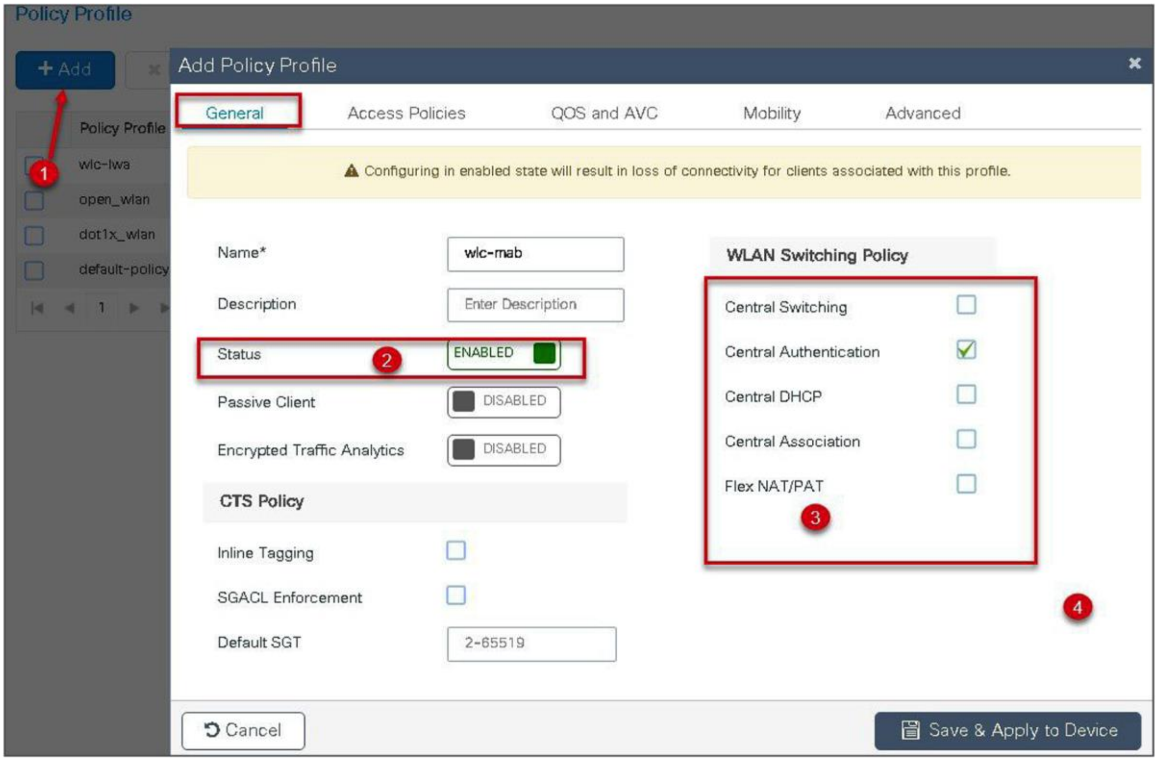
Over the DS ☑

Reassociation Timeout 20

Step 8. Enable the following on the policy profile:

- Local VLAN present on the AP (mapped in the flex profile)
- AAA override
- NAC

Navigate to Configuration > Tags & Profiles > Policy.



Policy Profile

+ Add

	Policy Profile
□	wlc-lwa
□	open_wlan
□	dot1x_wlan
□	default-policy

Add Policy Profile

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

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

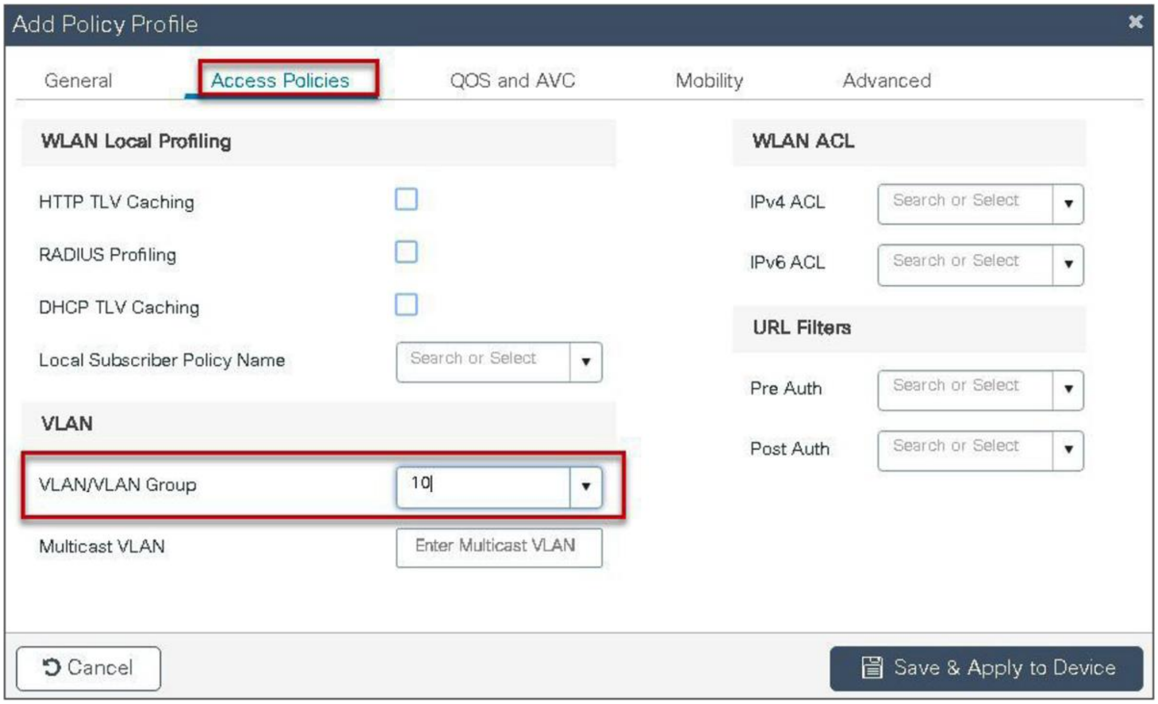
Name*	wlc-mab
Description	Enter Description
Status	ENABLED
Passive Client	DISABLED
Encrypted Traffic Analytics	DISABLED

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

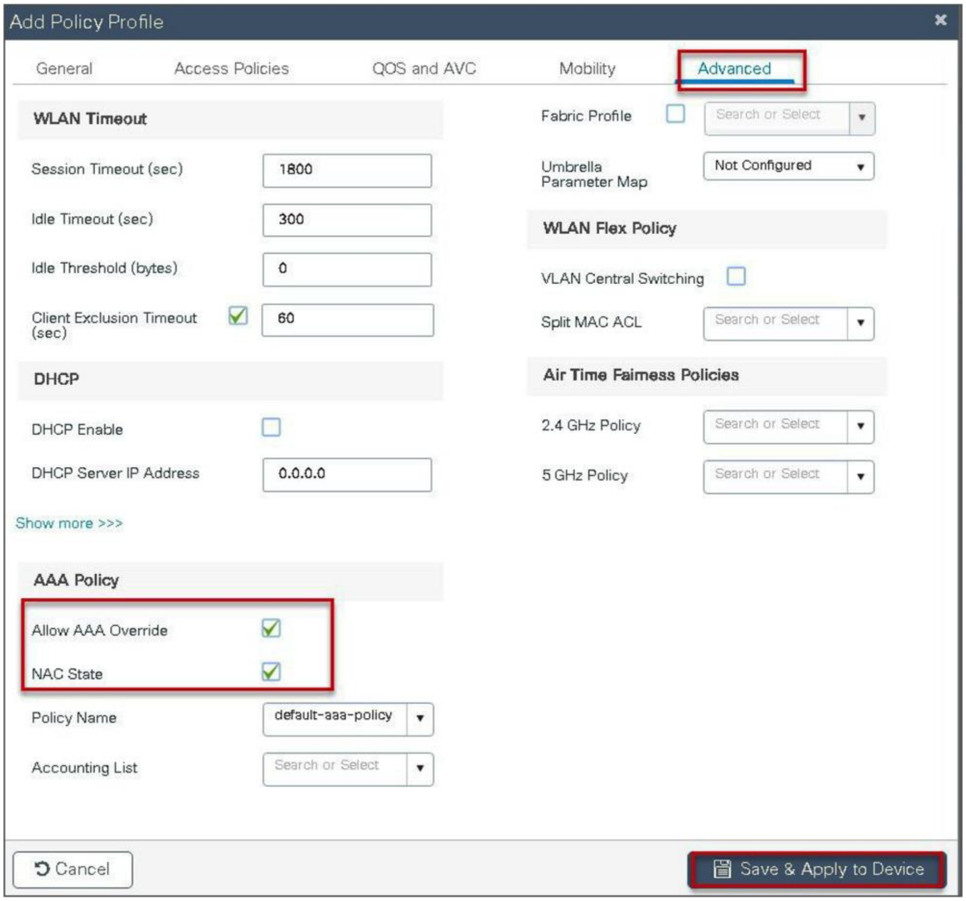
VLAN/VLAN Group	10
Multicast VLAN	Enter Multicast VLAN

WLAN ACL

IPv4 ACL	Search or Select
IPv6 ACL	Search or Select

URL Filters

Pre Auth	Search or Select
Post Auth	Search or Select



Add Policy Profile

WLAN Timeout

Session Timeout (sec): 1800

Idle Timeout (sec): 300

Idle Threshold (bytes): 0

Client Exclusion Timeout (sec): ☑ 60

DHCP

DHCP Enable: □

DHCP Server IP Address: 0.0.0.0

Show more >>>

AAA Policy

Allow AAA Override: ☑

NAC State: ☑

Policy Name: default-aaa-policy

Accounting List: Search or Select

Fabric Profile: □ Search or Select

Umbrella Parameter Map: Not Configured

WLAN Flex Policy

VLAN Central Switching: □

Split MAC ACL: Search or Select

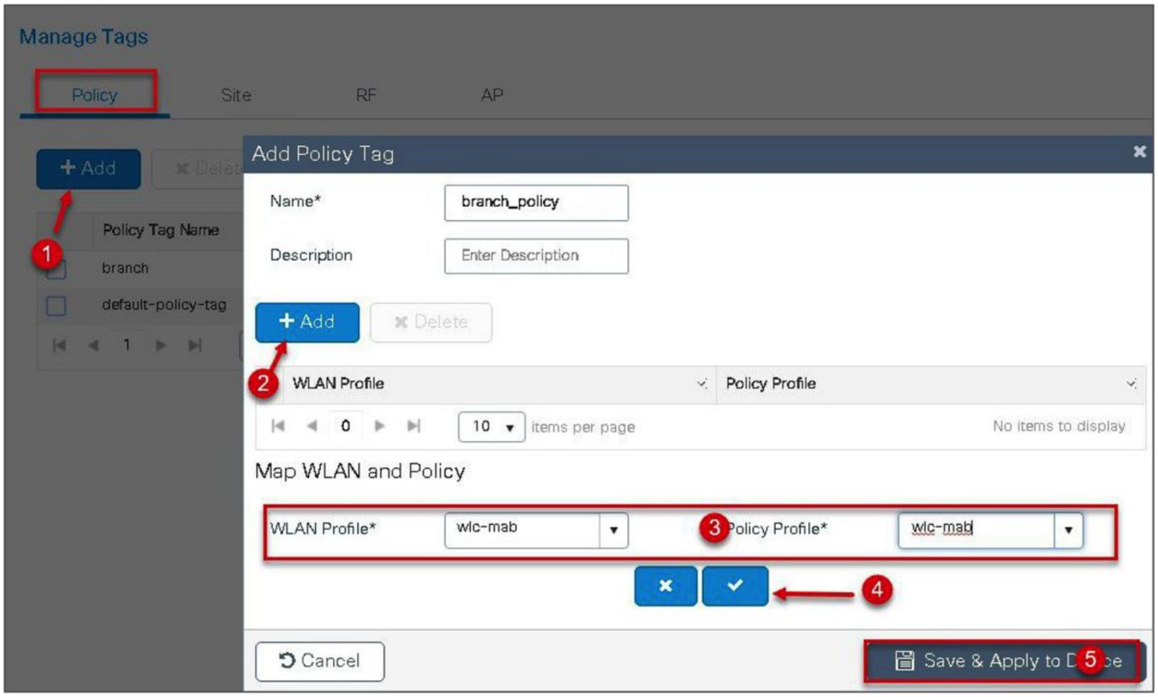
Air Time Fairness Policies

2.4 GHz Policy: Search or Select

5 GHz Policy: Search or Select

Step 9. Map the policy profile to the WLAN in the policy tag.

Navigate to Configuration > Tags and Profiles > Tags.



Manage Tags

Add Policy Tag

Name*: branch_policy

Description: Enter Description

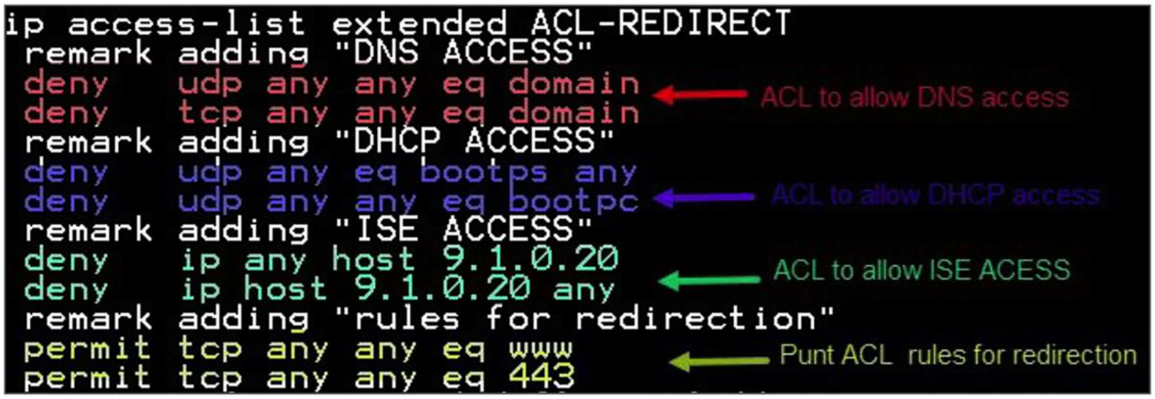
Map WLAN and Policy

WLAN Profile*: wlc-mab

Policy Profile*: wlc-mab

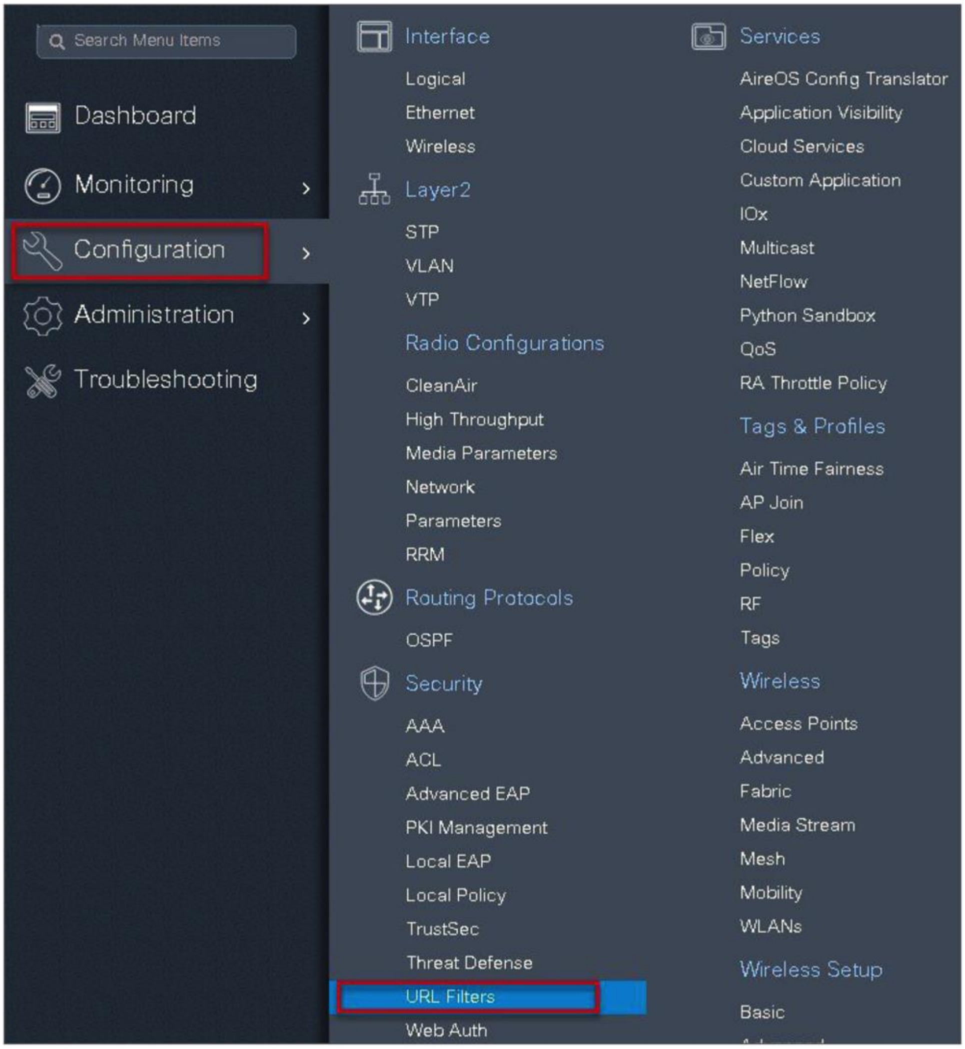
Step 10. Create a redirect ACL and an optional URL filter. The option to create a URL filter depends on access to resources during the pre-auth phase.

To create a redirect ACL, use the CLI on the controller. Have the rules created as shown below:



```
ip access-list extended ACL-REDIRECT
 remark adding "DNS ACCESS"
 deny    udp any any eq domain
 deny    tcp any any eq domain
 remark adding "DHCP ACCESS"
 deny    udp any eq bootps any
 deny    udp any any eq bootpc
 remark adding "ISE ACCESS"
 deny    ip any host 9.1.0.20
 deny    ip host 9.1.0.20 any
 remark adding "rules for redirection"
 permit tcp any any eq www
 permit tcp any any eq 443
```

To create a URL filter, navigate to Configuration > Security > URL Filters.



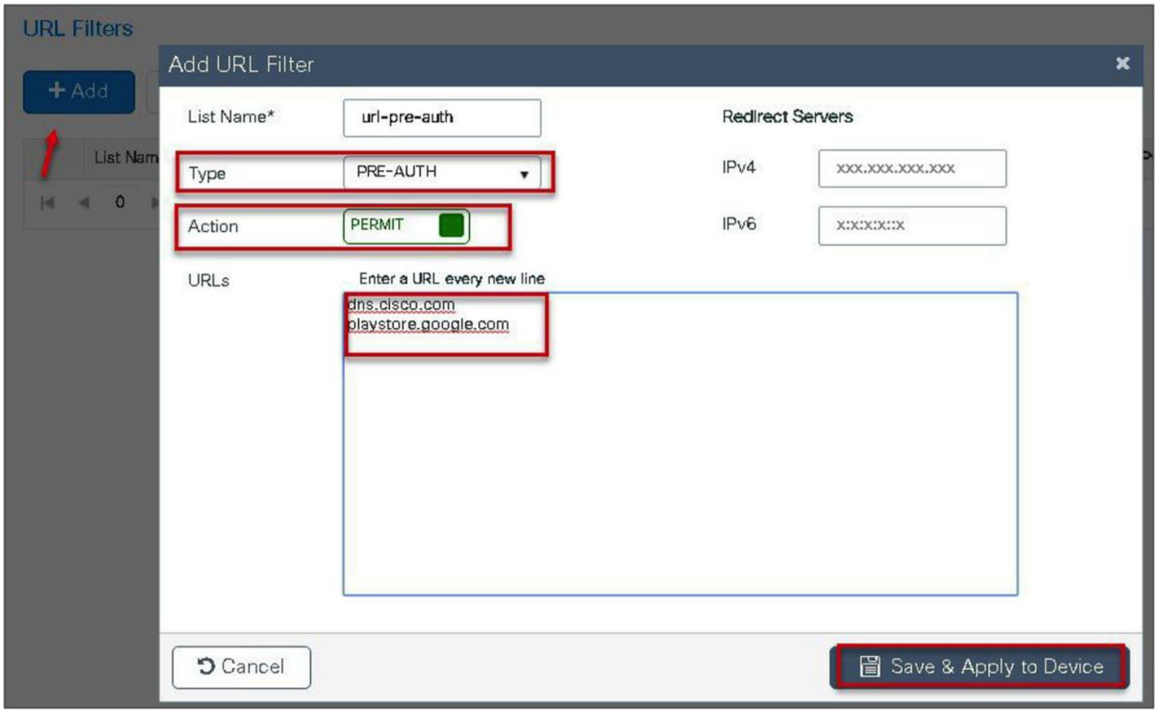
Step 11. Create a URL filter.

Permit action creates a permit list, while the deny action creates a blacklist.

Step 12. Enable the following on the flex profile.

Navigate to Configuration > Tags and Profiles > Flex.

- Local VLAN needs to be configured
- ACL and URL filter needs to be mapped



List Name* url-pre-auth

Type PRE-AUTH ▾

Action PERMIT 🟩

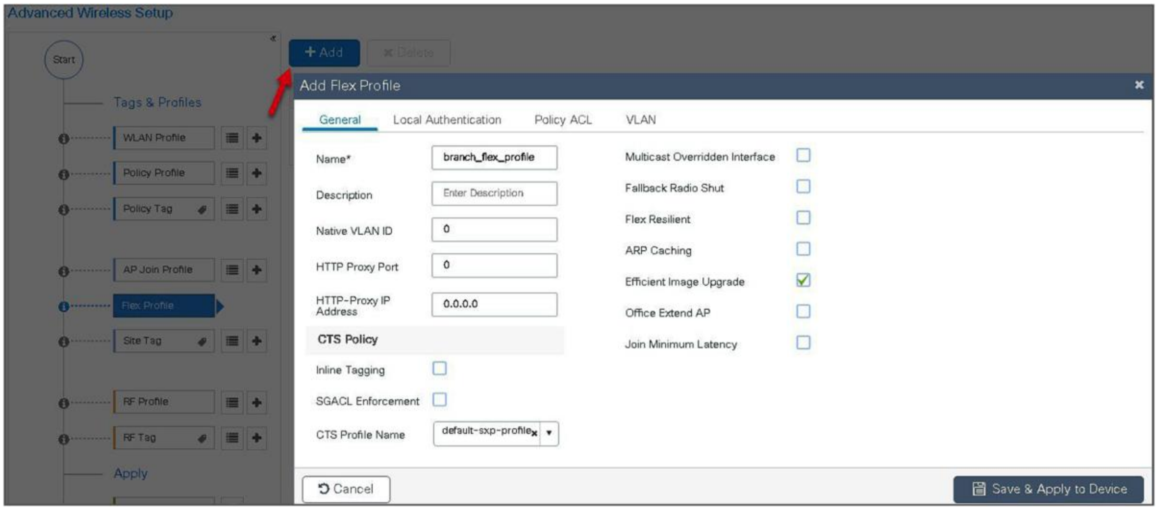
Redirect Servers

IPv4 xxx.xxx.xxx.xxx

IPv6 x:x:x:x::x

URLs Enter a URL every new line

dns.cisco.com
playstore.google.com



Name* branch_flex_profile

Description Enter Description

Native VLAN ID 0

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 □

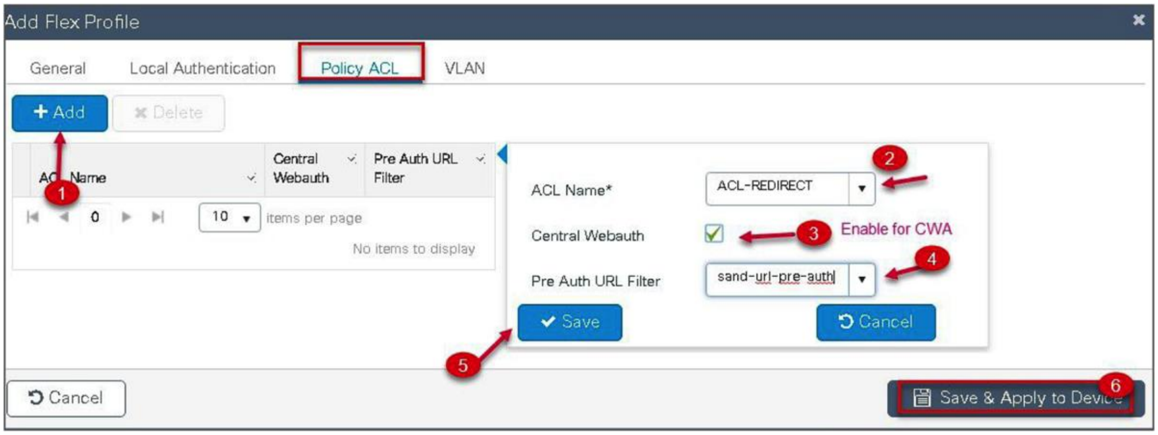
Flex Resilient □

ARP Caching □

Efficient Image Upgrade ☑

Office Extend AP □

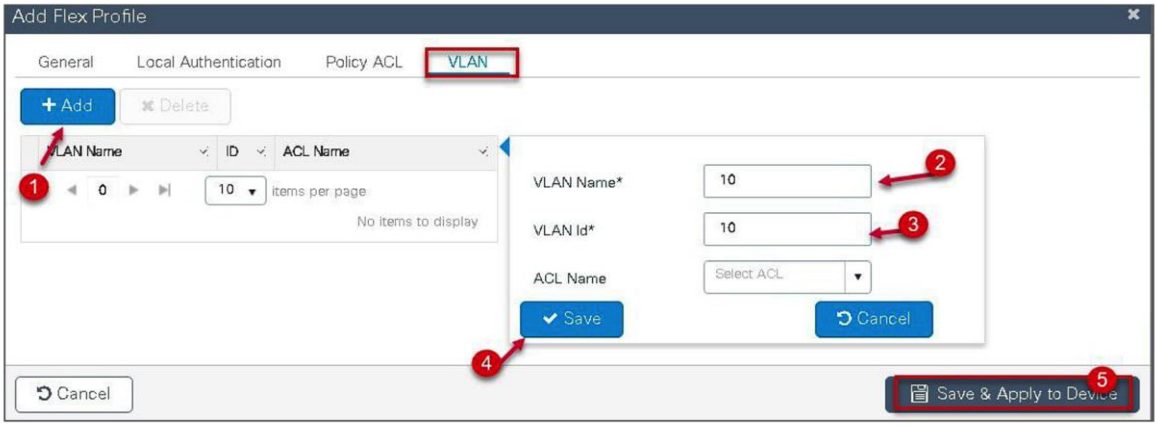
Join Minimum Latency □



ACL Name* ACL-REDIRECT

Central Webauth ☑ Enable for CWA

Pre Auth URL Filter sand-url-pre-auth



VLAN Name* 10

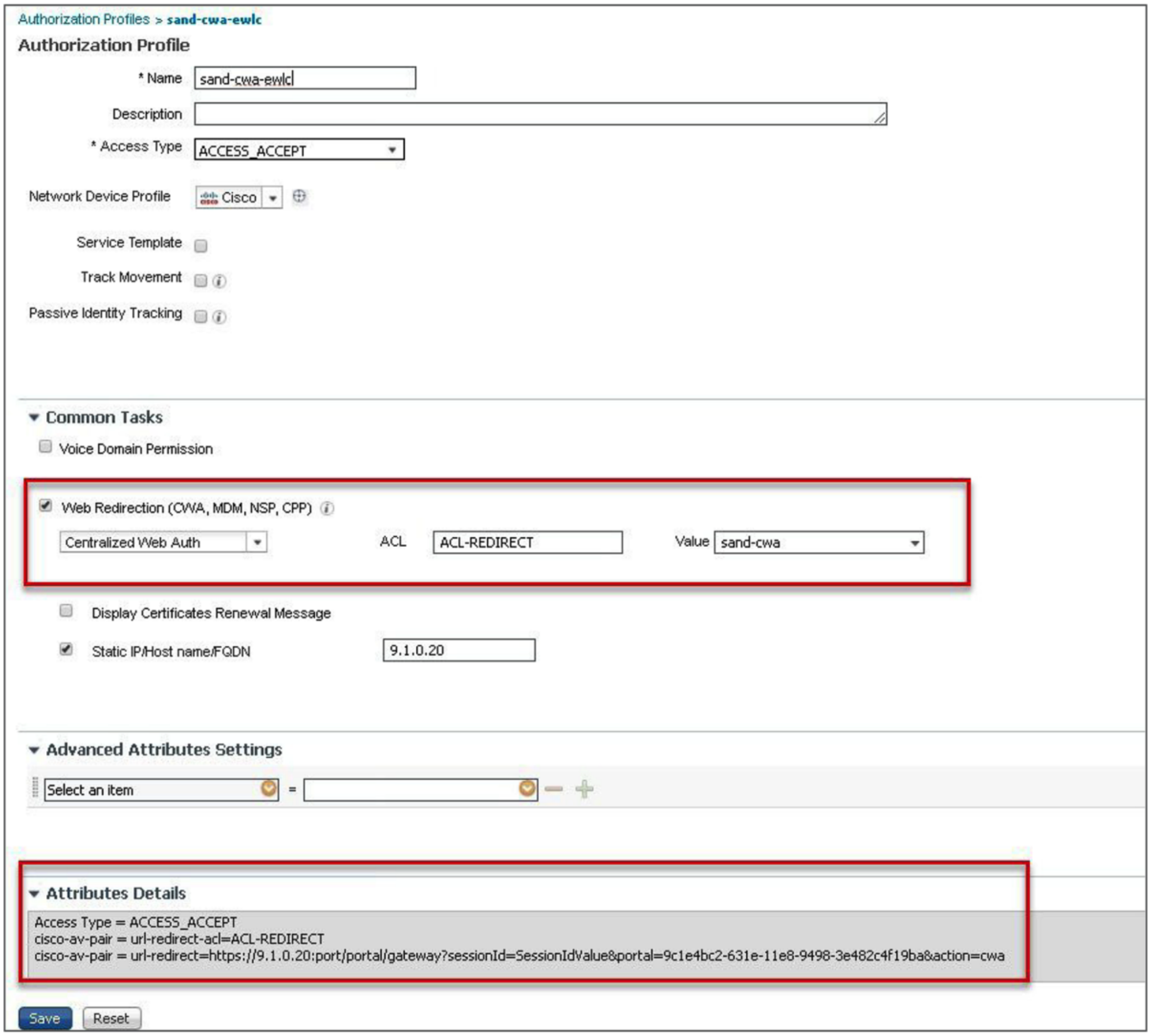
VLAN Id* 10

ACL Name Select ACL

Step 13. For assigning the flex profile on the site tag and mapping it on the AP, refer to the steps in the advanced configuration wizard of this document.

Step 14. Create an authorization profile and rule on ISE to return the CWA attributes.

For more details on ISE rules and configuration, please refer to the deployment guide:



Authorization Profiles > **sand-cwa-ewlc**

Authorization Profile

* Name: sand-cwa-ewlc

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

Common Tasks

□ Voice Domain Permission

☑ Web Redirection (CWA, MDM, NSP, CPP)

Centralized Web Auth ACL: ACL-REDIRECT Value: sand-cwa

□ Display Certificates Renewal Message

☑ Static IP/Host name/FQDN: 9.1.0.20

Advanced Attributes Settings

Select an item =

Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=ACL-REDIRECT
cisco-av-pair = url-redirect=https://9.1.0.20:port/portal/gateway?sessionId=SessionIdValue&portal=9c1e4bc2-631e-11e8-9498-3e482c4f19ba&action=cwa
```

www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html#anc6

Limitation

- The URL filter is only supported on Wave 2 APs and is not supported on Wave 1 APs.
- Post-auth support for URL filter is not supported for local switched clients.

Client association limit per WLAN/AP

The client limit per WLAN features addresses the requirement when an administrator would want to restrict the number of the clients accessing the wireless service – for example, limiting total guest clients from branch tunneling back to the data center.

Summary

The controller supports limiting the number of client associations in the following ways:

Per-WLAN basis - here the client association is limited on a per-WLAN basis

Per-AP per-WLAN - here the client association is limited on a per-WLAN per-AP basis

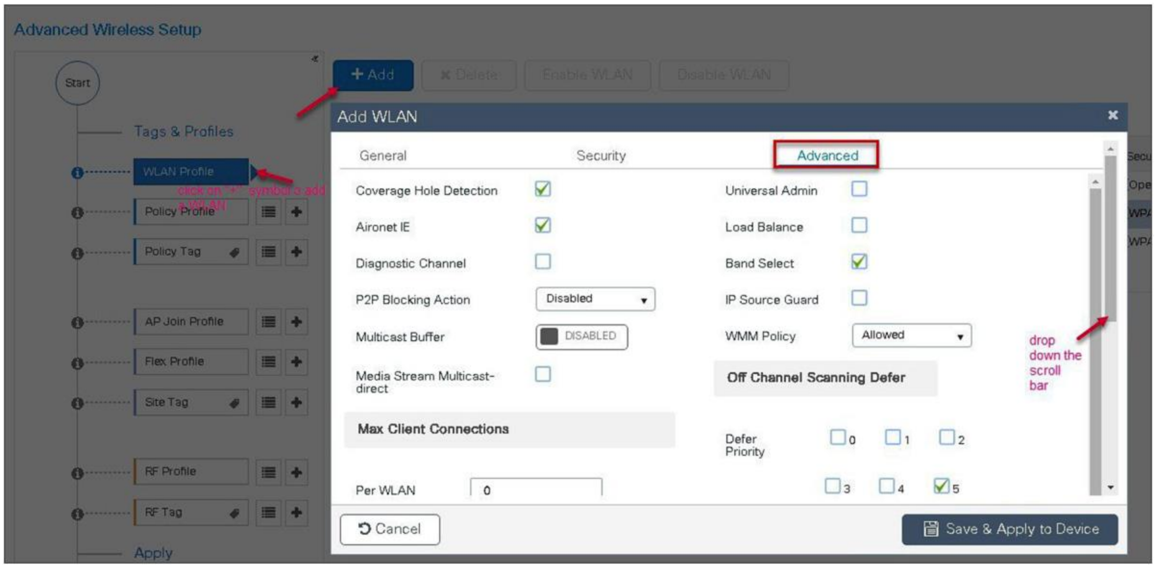
Per-AP radio per-WLAN - client association limited on a per-radio per-WLAN basis

Procedure

To enable a WLAN, please refer to the section of setting up the WLAN in the advanced wireless setup wizard of this document.

Procedure

During the WLAN configuration phase, enable the feature.



Coverage Hole Detection ☑

Aironet IE ☑

Diagnostic Channel □

P2P Blocking Action: Disabled

Multicast Buffer: DISABLED

Media Stream Multicast-direct □

Max Client Connections

Per WLAN: 0

Universal Admin □

Load Balance □

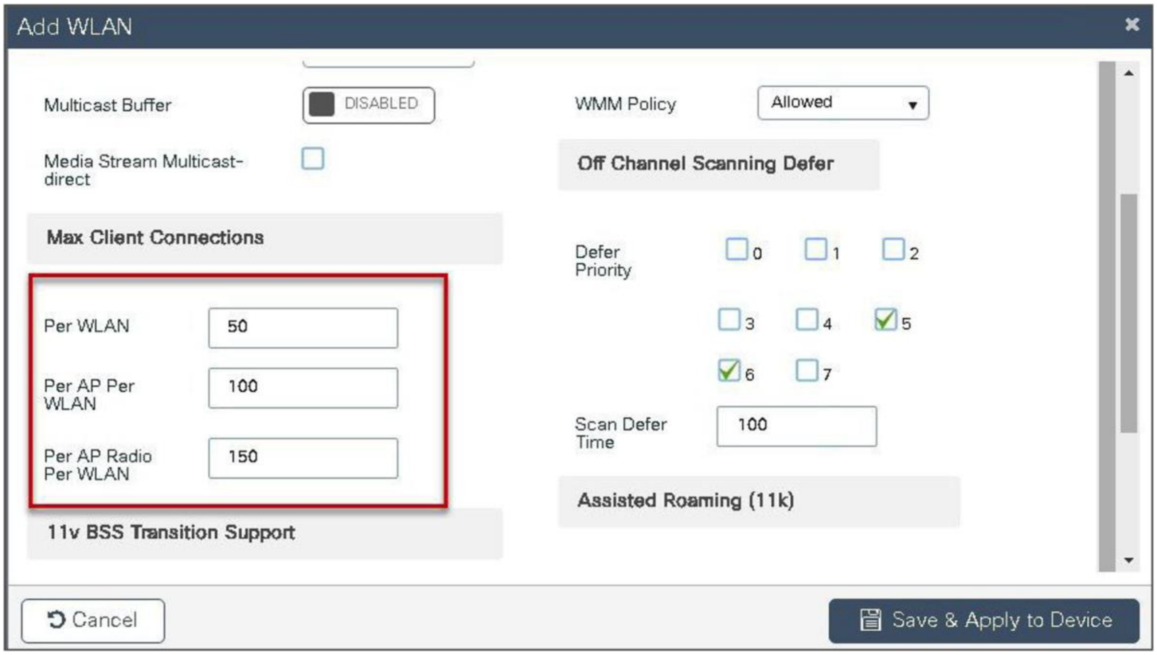
Band Select ☑

IP Source Guard □

WMM Policy: Allowed

Off Channel Scanning Defer

Defer Priority: □ 0 □ 1 □ 2 □ 3 □ 4 ☑ 5



Add WLAN

Multicast Buffer: DISABLED

Media Stream Multicast-direct □

Max Client Connections

Per WLAN	50
Per AP Per WLAN	100
Per AP Radio Per WLAN	150

11v BSS Transition Support

WMM Policy: Allowed

Off Channel Scanning Defer

Defer Priority: □ 0 □ 1 □ 2 □ 3 □ 4 ☑ 5 ☑ 6 □ 7

Scan Defer Time: 100

Assisted Roaming (11k)

Limitations

This feature does not enforce client limit when the FlexConnect is in the standalone state of operation.

Fault tolerance

FlexConnect fault tolerance allows wireless access and services to branch clients when:

- FlexConnect branch APs lose connectivity with the primary controller.
- FlexConnect branch APs are switching to the secondary controller.
- FlexConnect branch APs are re-establishing connection to the primary controller.

FlexConnect fault tolerance along with local authentication on the FlexConnect AP provide zero branch downtime during a network outage. This feature is enabled by default and cannot be disabled. It requires no configuration on the controller or AP. To ensure fault tolerance works smoothly, both the controllers need to have identical config such as:

- WLANM config and policy profile
- AP join profile/flex profile
- RF profile and RF tag
- Site tag

The management IP address of the controller can be different. An administrator can take a backup config of the primary controller and have it installed on the secondary controller to maintain config consistency.

Summary

- FlexConnect will not disconnect clients when the AP is connecting back to the same controller provided there is no change in configuration on the controller.
- FlexConnect will not disconnect clients when connecting to the backup controller provided there is no change in configuration and the backup controller is identical to the primary controller.
- FlexConnect will not reset its radios on connecting back to the primary controller provided there is no change in configuration on the controller.
- Supported on both Wave 1 and Wave 2 APs.

Limitations

- Supported only for FlexConnect with central/local authentication with local switching.
- Centrally authenticated clients require full re-authentication if the client session timer expires before the FlexConnect AP switches from standalone to connected mode.
- FlexConnect primary and backup controllers must be in the same mobility domain.

VideoStream for FlexConnect local switching

Introduction

This feature enables the wireless architecture to deploy multicast video streaming across the branches, just like it is currently possible for enterprise deployments. This feature recompenses the drawbacks that degrade the video delivery as the video streams and clients scale in a branch network. VideoStream makes video multicast to wireless clients more reliable and facilitates better usage of wireless bandwidth in the branch.

On a traditional WLAN network, multicast and broadcast are sent out over the wireless medium at the lowest data rate with no acknowledgement and the packet delivery for such streams are on a best-effort basis. This makes the usage of multicast unreliable on a WLAN network. The usage of multicast for delivering critical applications has become a demand and need of the hour. There is also a need to differentiate multiple streams and assign priority and weightage based on the applications supported. With the adoption of 802.11ac and the data rates supported, it is possible to deliver multicast streams using the data rates available on 11ac with reliability and priority built in.

Summary

- VideoStream provides efficient bandwidth utilization by removing the need to broadcast multicast packets to all WLANs on the AP
- Supported on Wave 1 and Wave 2 APs
- Supported for FlexConnect local switching and central authentication
- With VideoStream in FlexConnect local switching, the multicast to unicast conversion happens on the AP
- The branch infrastructure should have multicast enabled
- Admission control is currently not supported
- IPv6 support for media stream is not supported

The section below details the procedure for configuring media stream from the controller. It is expected that the branch network will be enabled for multicast.

Please ensure the following multicast features are enabled on the network.

- Multicast routing protocol – PIM sparse/dense mode
- IGMP version 2 or 3
- IGMP snooping

This section doesn't cover enabling multicast on the infrastructure other than on the wireless controller.

Procedure for enabling VideoStream

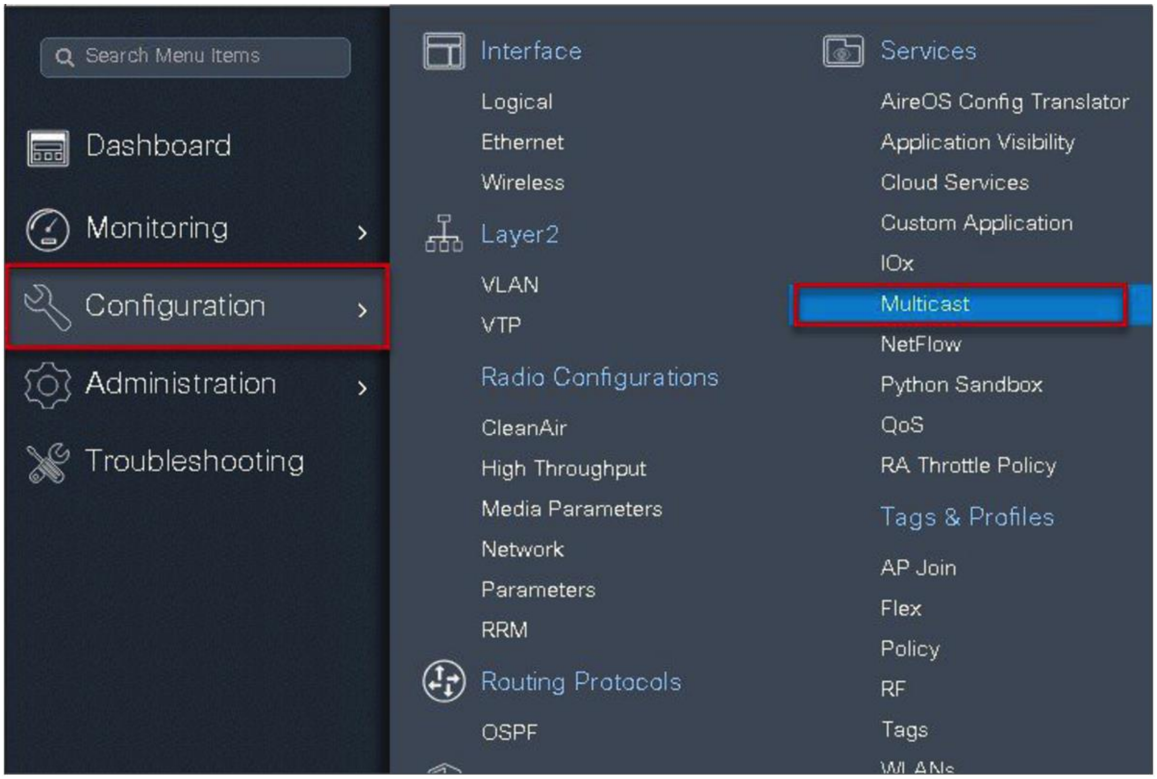
The steps here include only the changes to enable VideoStream.

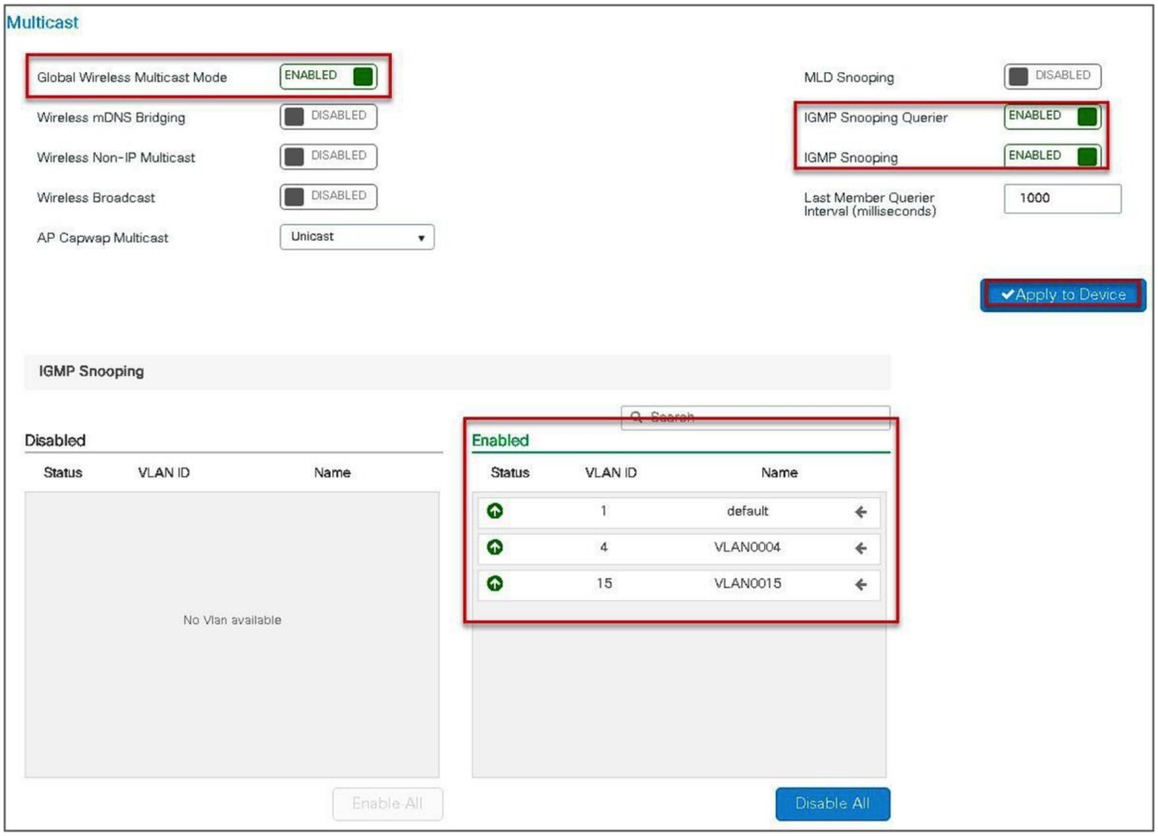
The advanced configuration section can be used to set up the SSID, profiles, and tags. The section below details the configuration of the media stream on the 5 GHz radio.

Procedure

Step 1. Enable multicast globally on the controller.

Navigate to Configuration > Services > Multicast.





Multicast

Global Wireless Multicast Mode: ENABLED

Wireless mDNS Bridging: DISABLED

Wireless Non-IP Multicast: DISABLED

Wireless Broadcast: DISABLED

AP Capwap Multicast: Unicast

MLD Snooping: DISABLED

IGMP Snooping Querier: ENABLED

IGMP Snooping: ENABLED

Last Member Querier Interval (milliseconds): 1000

✔Apply to Device

IGMP Snooping

Disabled

Status	VLAN ID	Name

No Vlan available

Enabled

Status	VLAN ID	Name	
●	1	default	←
●	4	VLAN0004	←
●	15	VLAN0015	←

Enable All

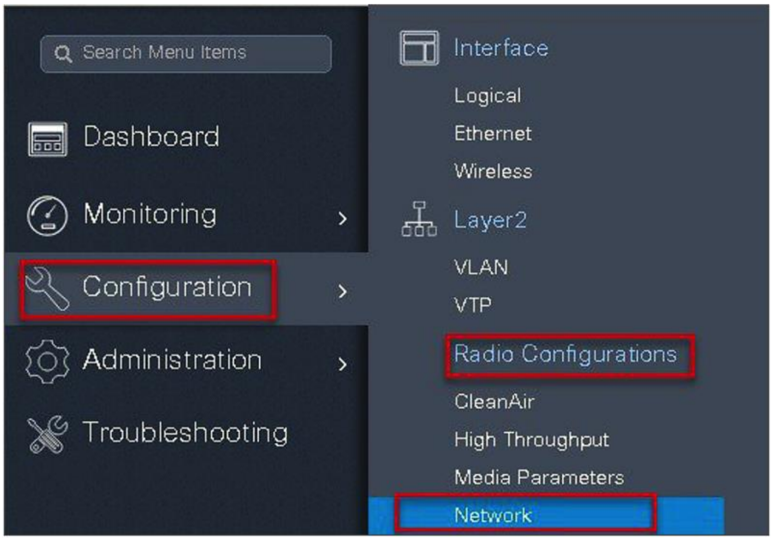
Disable All

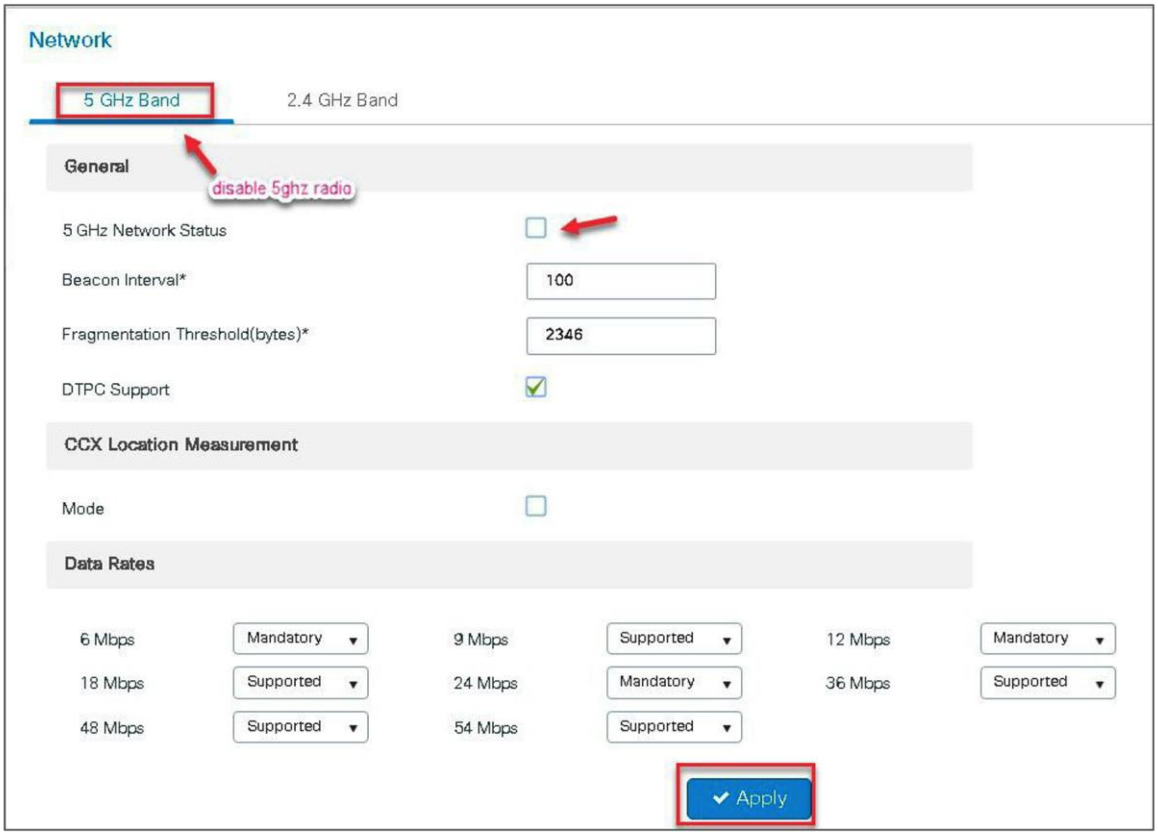
Step 2. Enable media stream on the dot11 interface.

Disable the appropriate radio interface before enabling the media stream.

Navigate to Configuration > Radio Configurations > Network.

Disable 5 or 2.4 GHz radio. In this example, we are enabling media stream on 5 GHz radio.





Network

5 GHz Band | 2.4 GHz Band

disable 5ghz radio

General

5 GHz Network Status □

Beacon Interval* 100

Fragmentation Threshold(bytes)* 2346

DTPC Support ☑

CCX Location Measurement

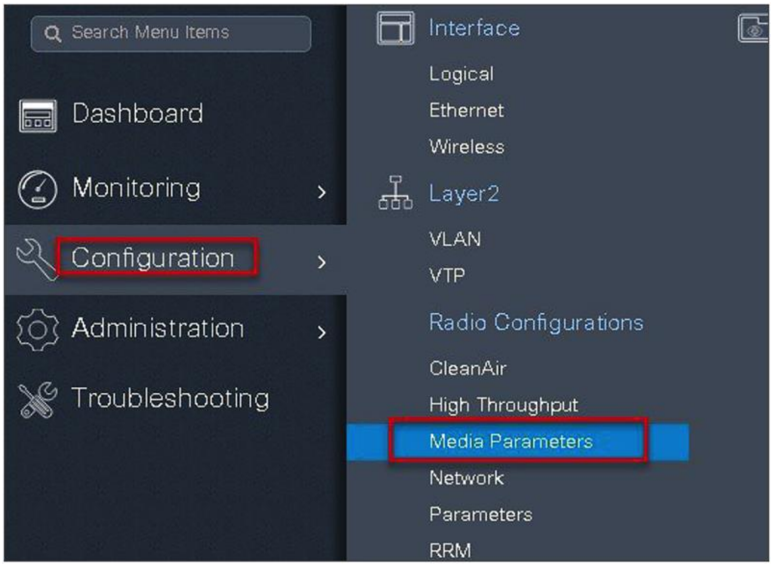
Mode □

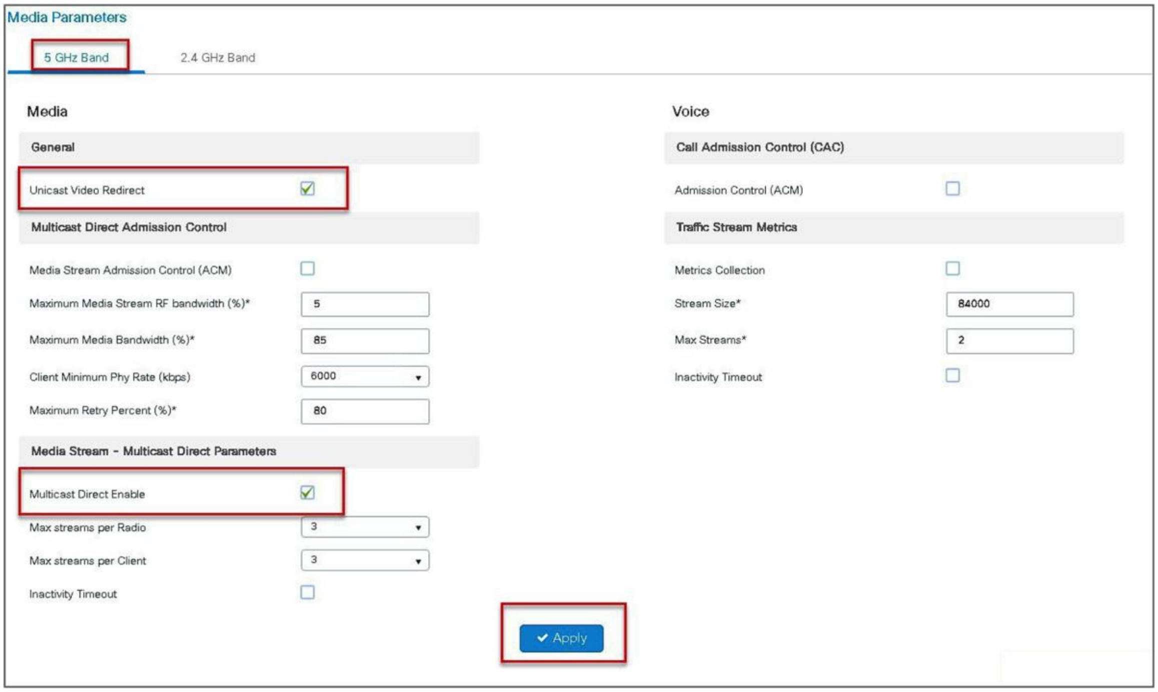
Data Rates

6 Mbps	Mandatory	9 Mbps	Supported	12 Mbps	Mandatory
18 Mbps	Supported	24 Mbps	Mandatory	36 Mbps	Supported
48 Mbps	Supported	54 Mbps	Supported		

✔ Apply

Step 3. Navigate to Configuration > Radio Configurations > Media Parameters.





Media Parameters

5 GHz Band | 2.4 GHz Band

Media

General

Unicast Video Redirect ☑

Multicast Direct Admission Control

Media Stream Admission Control (ACM)	☐
Maximum Media Stream RF bandwidth (%)*	5
Maximum Media Bandwidth (%)*	85
Client Minimum Phy Rate (kbps)	6000
Maximum Retry Percent (%)*	80

Media Stream - Multicast Direct Parameters

Multicast Direct Enable	☑
Max streams per Radio	3
Max streams per Client	3
Inactivity Timeout	☐

Voice

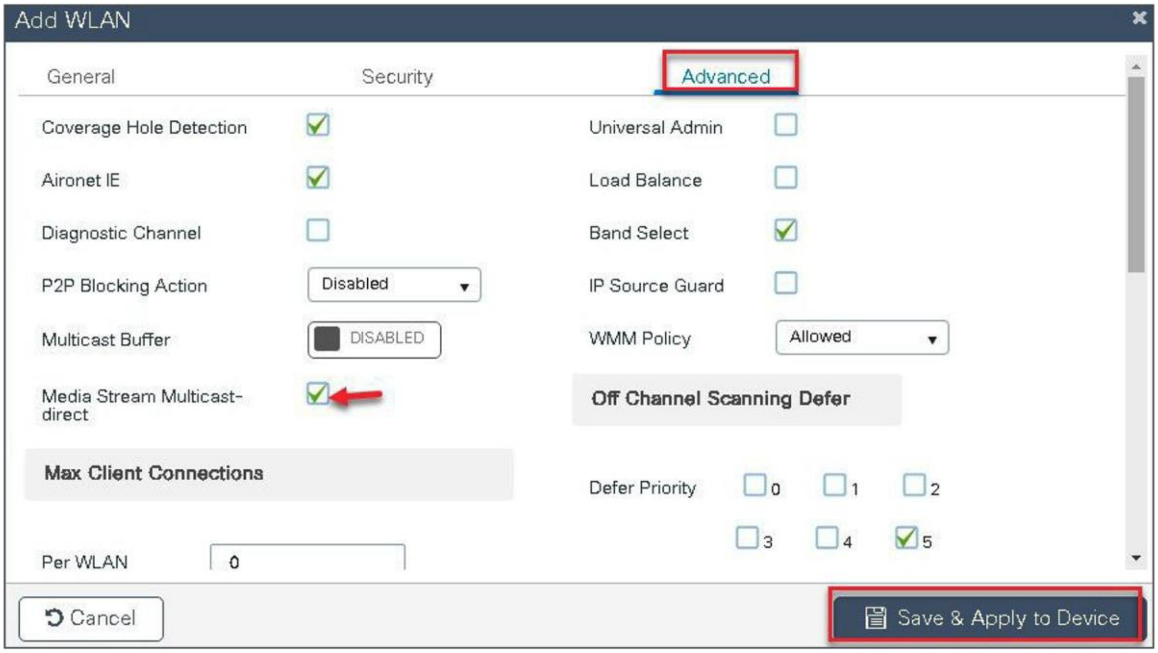
Call Admission Control (CAC)

Admission Control (ACM) ☐

Traffic Stream Metrics

Metrics Collection	☐
Stream Size*	84000
Max Streams*	2
Inactivity Timeout	☐

Step 4. Enable the media stream on the WLAN creation page on the advanced tab. Refer to the advanced configuration wizard section for WLAN creation.



Add WLAN

General | Security | Advanced

Coverage Hole Detection	☑	Universal Admin	☐
Aironet IE	☑	Load Balance	☐
Diagnostic Channel	☐	Band Select	☑
P2P Blocking Action	Disabled	IP Source Guard	☐
Multicast Buffer	DISABLED	WMM Policy	Allowed
Media Stream Multicast-direct	☑		

Max Client Connections

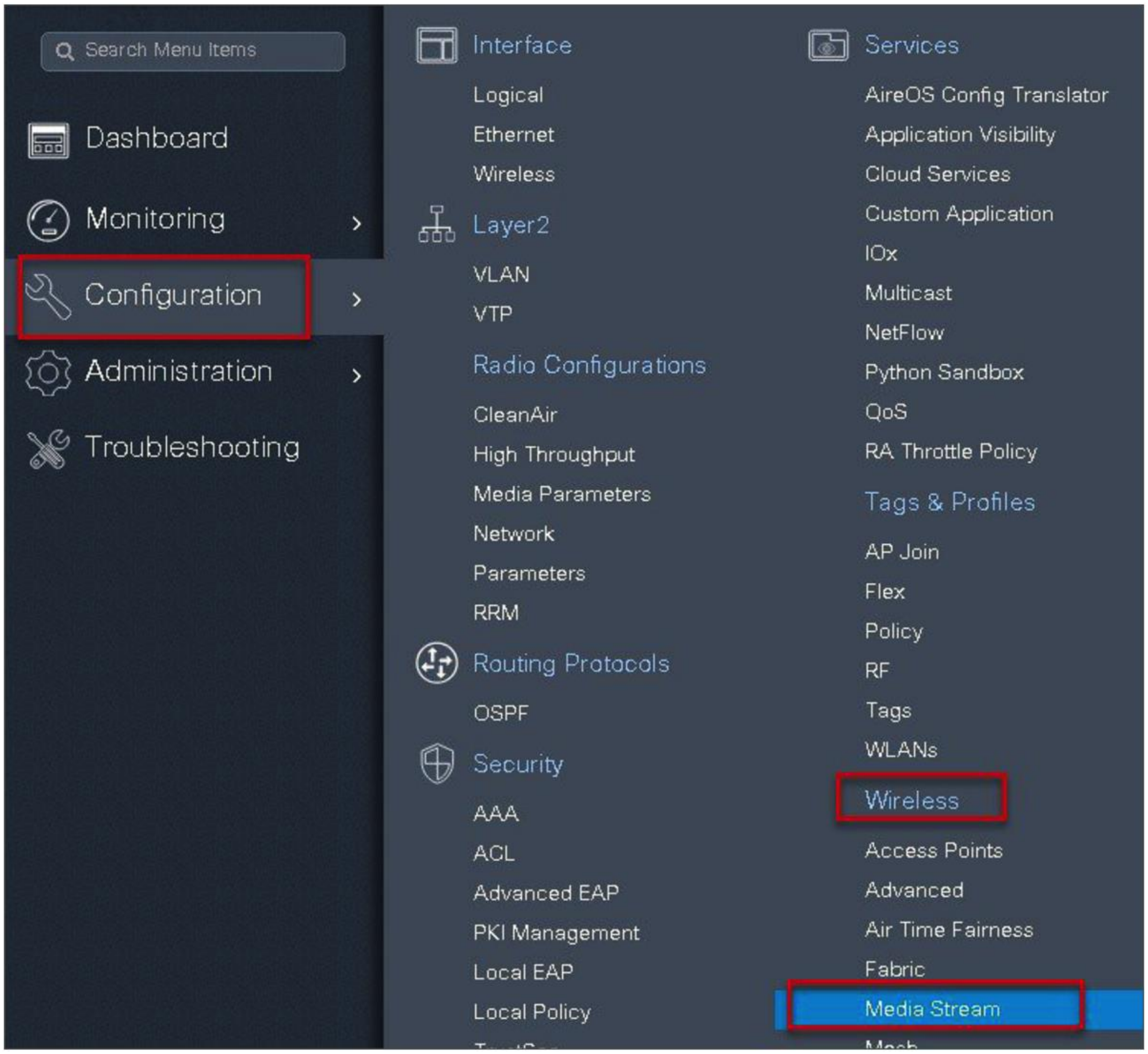
Per WLAN 0

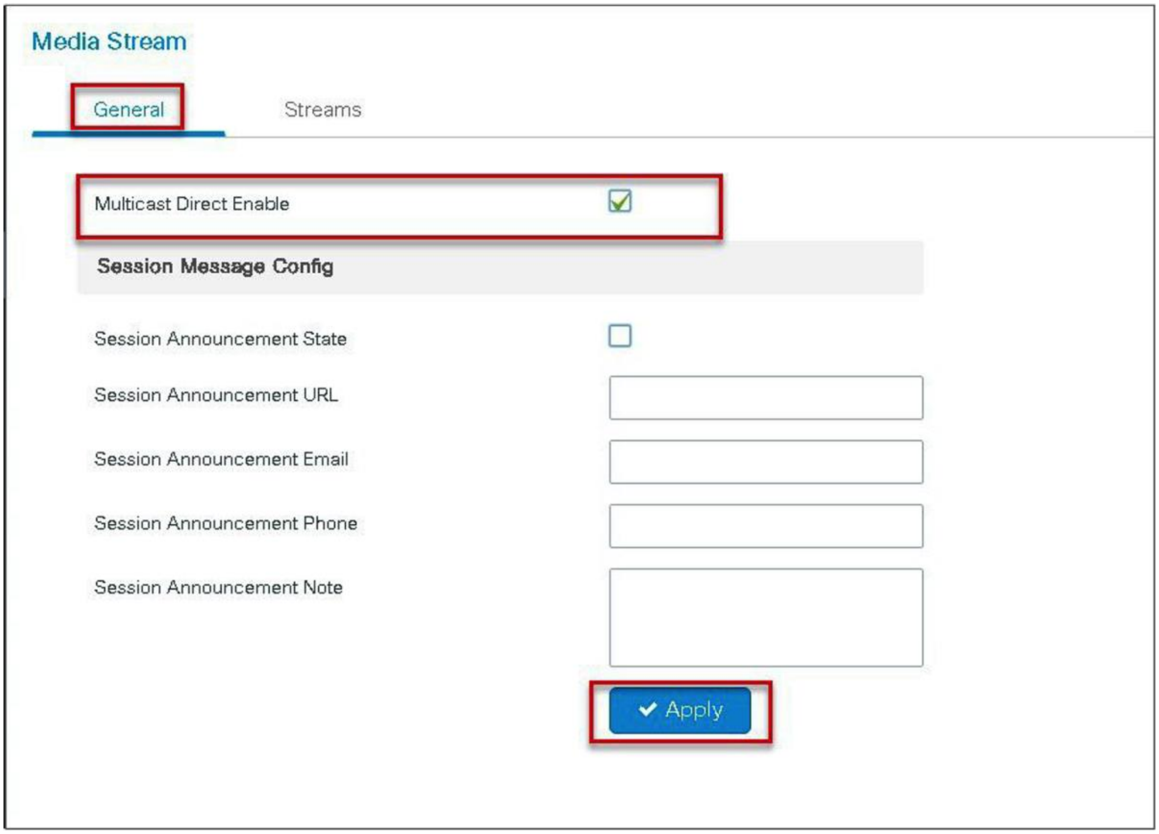
Off Channel Scanning Defer

Defer Priority ☐0 ☐1 ☐2 ☐3 ☐4 ☑5

Step 5. Define the media stream multicast address configuration.

Navigate to Wireless > Media Stream.





Media Stream

Multicast Direct Enable ☑

Session Message Config

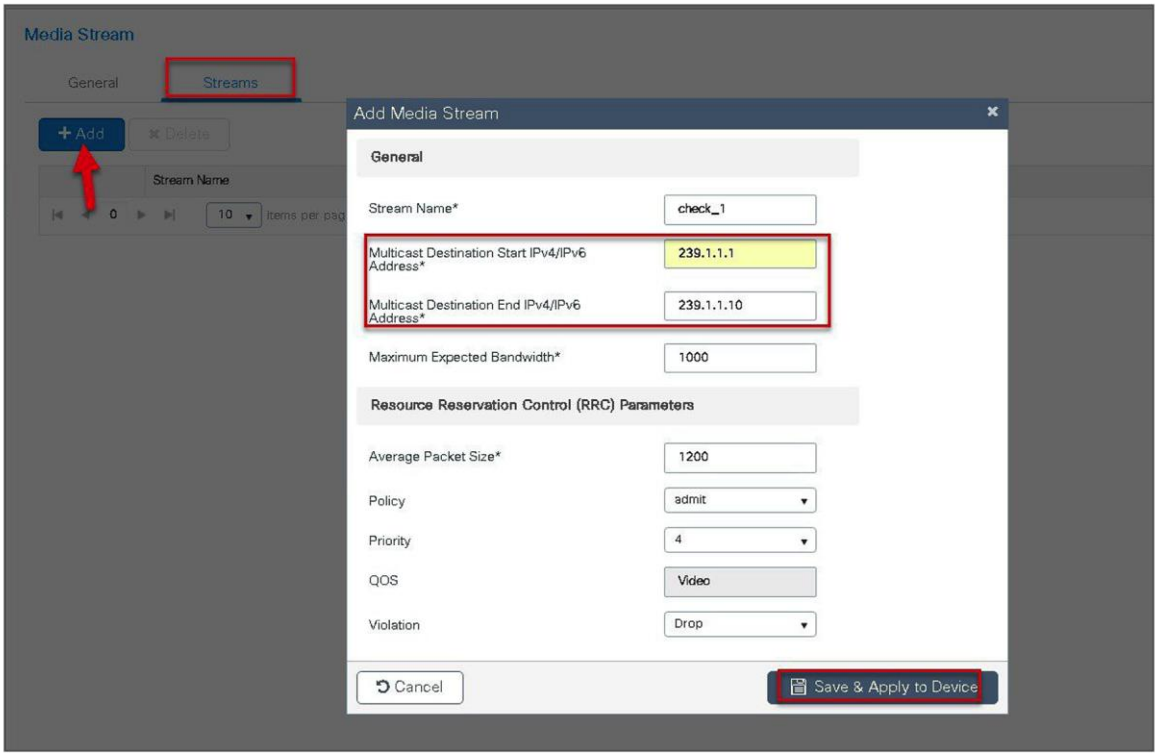
Session Announcement State □

Session Announcement URL

Session Announcement Email

Session Announcement Phone

Session Announcement Note



Media Stream

Add Media Stream

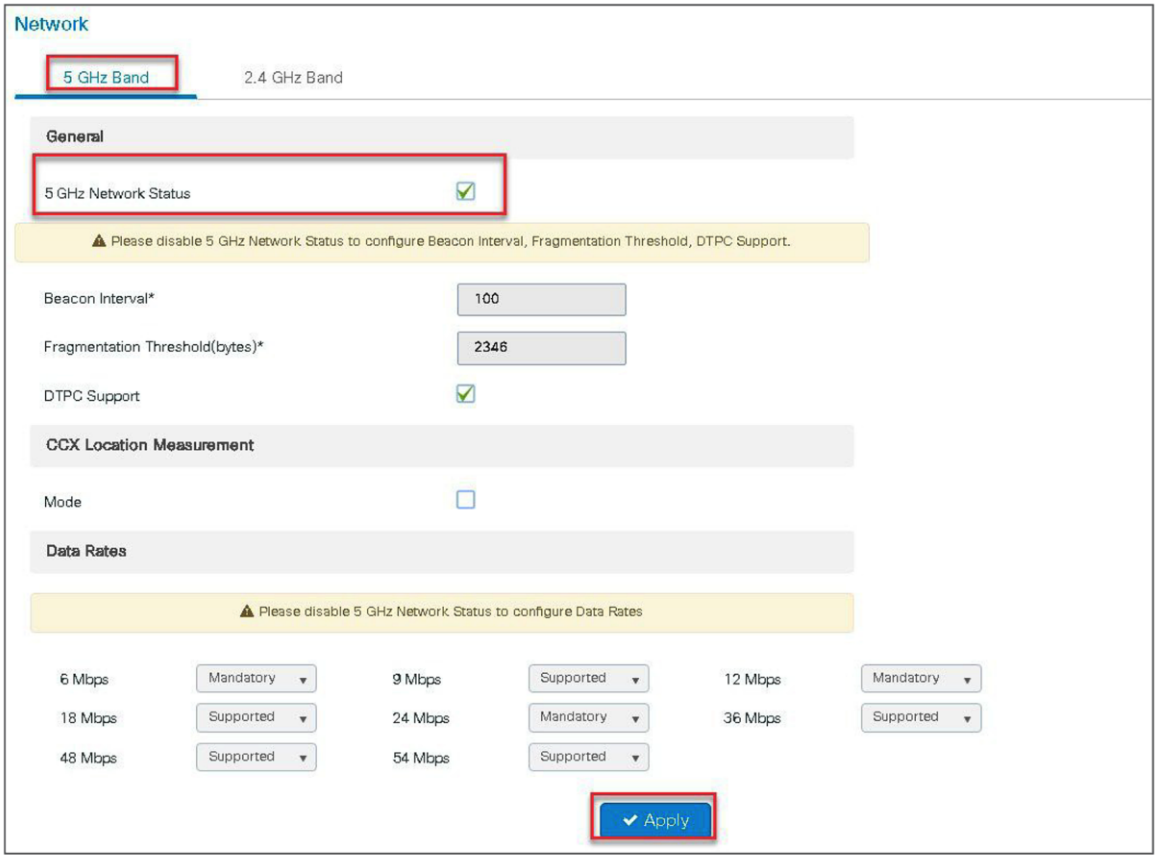
General

Stream Name*	check_1
Multicast Destination Start IPv4/IPv6 Address*	239.1.1.1
Multicast Destination End IPv4/IPv6 Address*	239.1.1.10
Maximum Expected Bandwidth*	1000

Resource Reservation Control (RRC) Parameters

Average Packet Size*	1200
Policy	admit
Priority	4
QOS	Video
Violation	Drop

Step 6. Enable the dot11 interface on which the media stream was enabled.



Network

5 GHz Band | 2.4 GHz Band

General

5 GHz Network Status ☑

Please disable 5 GHz Network Status to configure Beacon Interval, Fragmentation Threshold, DTPC Support.

Beacon Interval* 100

Fragmentation Threshold(bytes)* 2346

DTPC Support ☑

CCX Location Measurement

Mode □

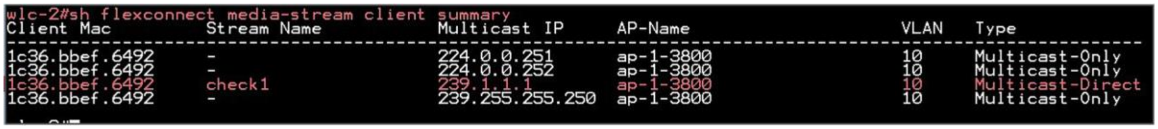
Data Rates

Please disable 5 GHz Network Status to configure Data Rates

6 Mbps	Mandatory	9 Mbps	Supported	12 Mbps	Mandatory
18 Mbps	Supported	24 Mbps	Mandatory	36 Mbps	Supported
48 Mbps	Supported	54 Mbps	Supported		

Connect the wireless client and subscribe to the respective multicast video stream.

Issue the CLI “show flexconnect media client summary” to see the multicast transmission being classified as multicast direct/video stream.



```
wlc-2#sh flexconnect media-stream client summary
Client Mac            Stream Name        Multicast IP     AP-Name                   VLAN    Type
--------------------------------------------------------------------------------------------------------
1c36.bbef.6492        -                  224.0.0.251      ap-1-3800                 10      Multicast-Only
1c36.bbef.6492        -                  224.0.0.252      ap-1-3800                 10      Multicast-Only
1c36.bbef.6492        check1             239.1.1.1        ap-1-3800                 10      Multicast-Direct
1c36.bbef.6492        -                  239.255.255.250  ap-1-3800                 10      Multicast-Only
```

Flex IP Overlap Support

Introduction

Multiple customers tend to use cookie cutter configuration across the sites and branches. This includes local or DHCP servers configured with the same subnet. Prior to 17.4, controller detected this is IP THEFT and clients would be blacklisted.

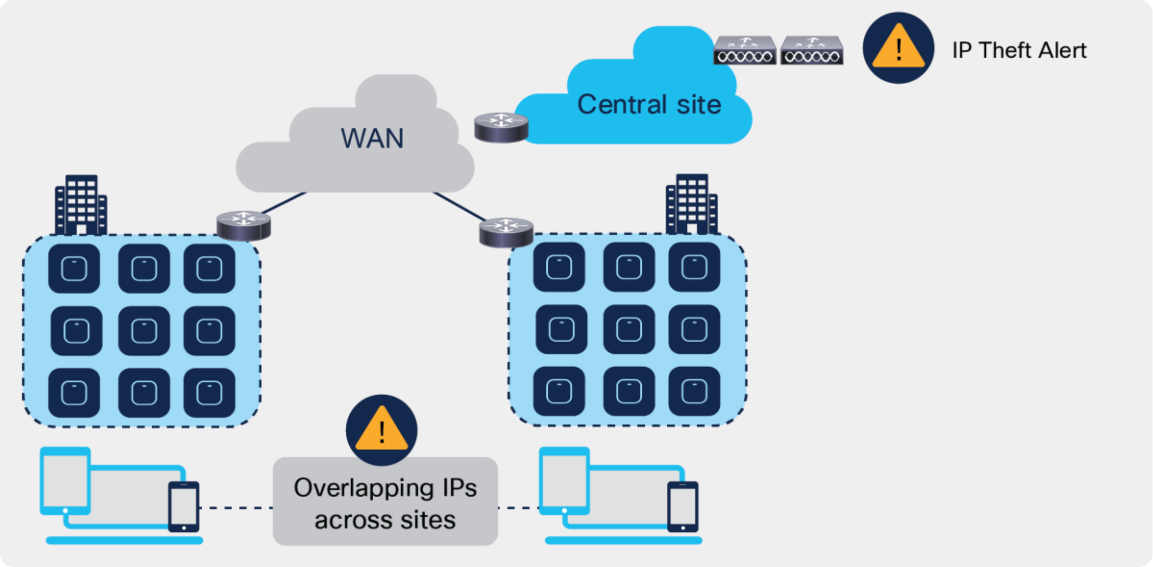


Figure 10.
Behavior of overlapping IPs across sites prior to Release 17.4

Release 17.4 adds support for overlapping IP addresses across different flex sites.

For this to work, every site needs to be assigned to a unique site-tag > C9800 uses the combination of site-tag + IP address as a unique ID for the client (called zone-id).

It is important to note that this is only available for Flex local DHCP/ local switching; for all other deployments (local mode, central switching, central DHCP, etc.), overlapping IPs are still not supported.

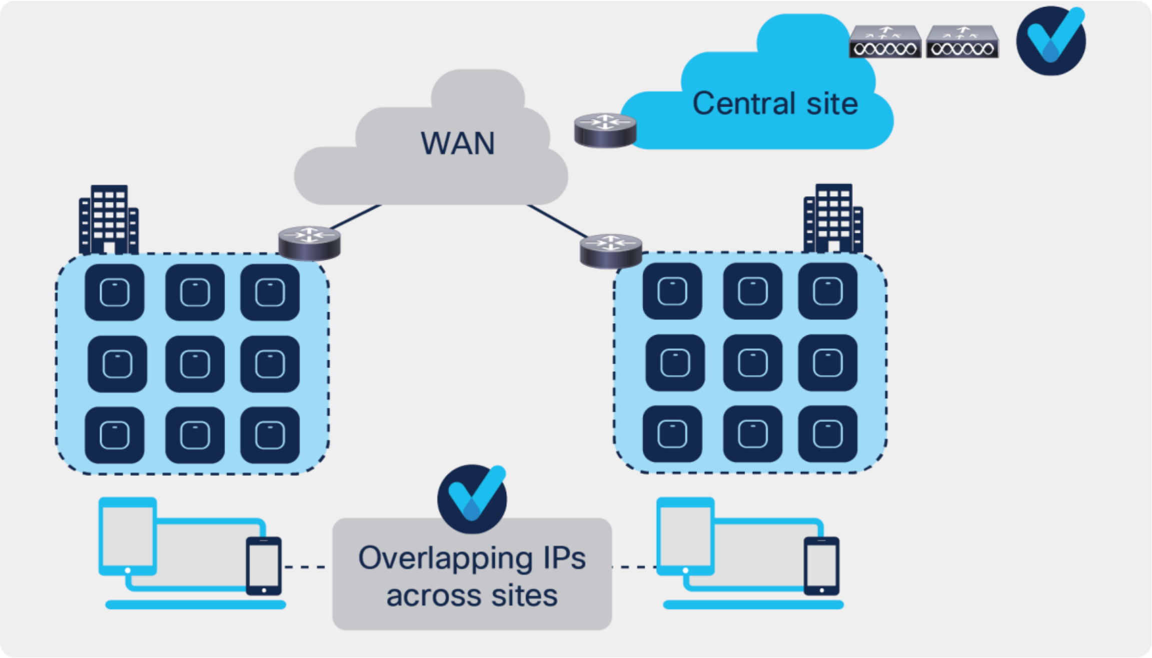
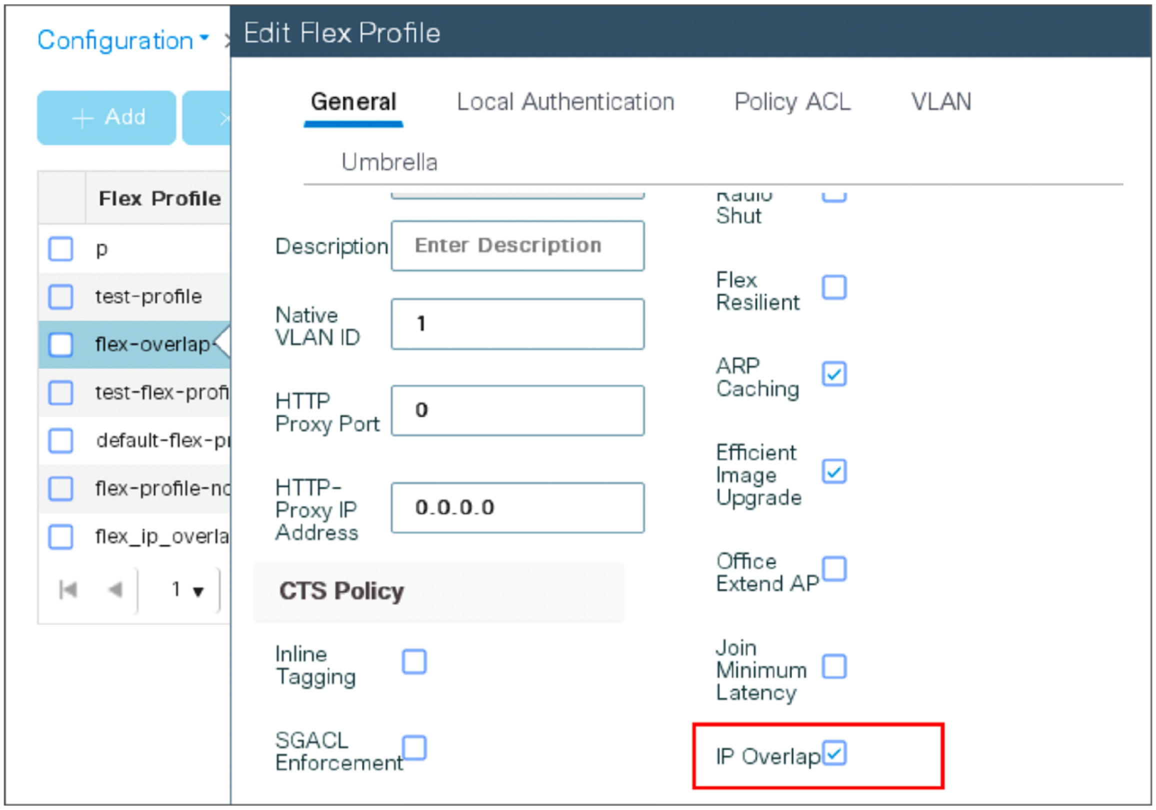


Figure 11.
Behavior of overlapping IPs across sites starting Release 17.4

This feature is supported on all C9800 appliances (physical and virtual). It is not supported on EWC on Catalyst AP and Catalyst 9k switch because these are meant for single site deployments.

Procedure for enabling Flex IP Overlap

Enable and disabling the feature is controlled via the config knob under the Flex Profile.



Flex Profile
- □ p
- □ test-profile
- □ flex-overlap
- □ test-flex-profi
- □ default-flex-p
- □ flex-profile-nc
- □ flex_ip_overla

Description: Enter Description

Native VLAN ID: 1

HTTP Proxy Port: 0

HTTP-Proxy IP Address: 0.0.0.0

CTS Policy

Inline Tagging □

SGACL Enforcement □

Radio Shut □

Flex Resilient □

ARP Caching ☑

Efficient Image Upgrade ☑

Office Extend AP □

Join Minimum Latency □

IP Overlap ☑

```
The equivalent CLI command is:
(config)#wireless profile flex flex1
(config-wireless-flex-profile)#ip overlap

To verify execute the following command:

9800-wlc#show wireless profile flex detailed flex1
Fallback Radio shut            : DISABLED
ARP caching                    : ENABLED
Efficient Image Upgrade        : ENABLED
OfficeExtend AP                : DISABLED
Join min latency               : DISABLED
IP overlap status              : ENABLED
```

“Show wireless device-tracking database ip <ip>” CLI will not be supported when IP overlap feature is enabled. Any filtering based on IP or Zone should be performed only on “Show wireless device-tracking database ip”.

```
9800-wlc#show wireless device-tracking database ip
ZONE-ID     IP                                    STATE       DISCOVERY      MAC
  ----------------------------------------------------------------------------------------
  0x00000004  21.21.0.1                             Reachable   IPv4 Packet   74da.3864.2a83
  0x0000000c  21.21.0.1                             Reachable   IPv4 DHCP     74da.3873.2a8b
  0x8000400a  fe80::76da:38ff:fe64:2a83             Reachable   IPv6 Packet   74da.3864.2a83
  0x8000c00a  fe80::76da:38ff:fe73:2a8b             Reachable   IPv6 Packet   74da.3873.2a8b
```

In order to enable or disable the Overlap IP Support which are part of the flex profile, following NETCONF RPC is defined

```
<nc:rpc xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="urn:uuid:a90868eb-
1b78-43b4-a949-2dca79687a69">
  <nc:edit-config>
    <nc:target>
      <nc:running/>
    </nc:target>
    <nc:config>
      <flex-cfg-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-flex-cfg">
        <flex-policy-entries>
          <flex-policy-entry>
            <policy-name>Flex_profile</policy-name>
            <description/>
            <ip-overlap-cfg>
              <flex-overlapping-ip-enable>true</flex-overlapping-ip-enable>
            </ip-overlap-cfg>
          </flex-policy-entry>
        </flex-policy-entries>
      </flex-cfg-data>
    </nc:config>
  </nc:edit-config>
</nc:rpc>
```

Glossary

- VLAN: virtual LAN
- RF: radio frequency
- FT: fault tolerance
- WAVE 1 AP: AP which supports WAVE 1 802.11ac (Cisco 3700)
- WAVE 2 AP: AP which supports WAVE f2 802.11ac (Cisco 1800/2800/3800/4800)
- WLC: wireless LAN controller

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C07-744990-00 09/21