



FlexConnect Catalyst Wireless Branch Deployment Guide



Table of Contents

Introduction	3
Supported Platforms	3
Supported releases	3
FlexConnect Architecture	4
Wireless Branch Network Design	6
Cisco Catalyst Wireless Config Model	9
Flexconnect VLAN override	50
FlexConnect VLAN Based Central Switching	67
Local Authentication and Backup Radius server	89
CCKM/OKC and PMK Caching	107
Peer to Peer Blocking	107
FlexConnect ACL	109
AP Pre-Image Download	121
FlexConnect Smart AP Image Upgrade	123
Flexconnect Pre-auth ACL and URL filtering	126
Client Association Limit per WLAN/AP	151
Summary	151
Procedure	151
Limitations	152

[Fault Tolerance](#) **152**

[VideoStream for FlexConnect Local Switching](#) **153**

[Glossary](#) **161**

Introduction

This document describes how to deploy a Cisco FlexConnect wireless branch solution on the Catalyst wireless platform. The Catalyst wireless platform are 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 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. Catalyst 9800WC and virtual cloud controller runs on the IOS-XE software base, utilizing the flexibility and modularity available with the platform.

Refer the following documentation on bring up of 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 is supported on the following platforms and releases.

Supported Platforms

Catalyst wireless platforms

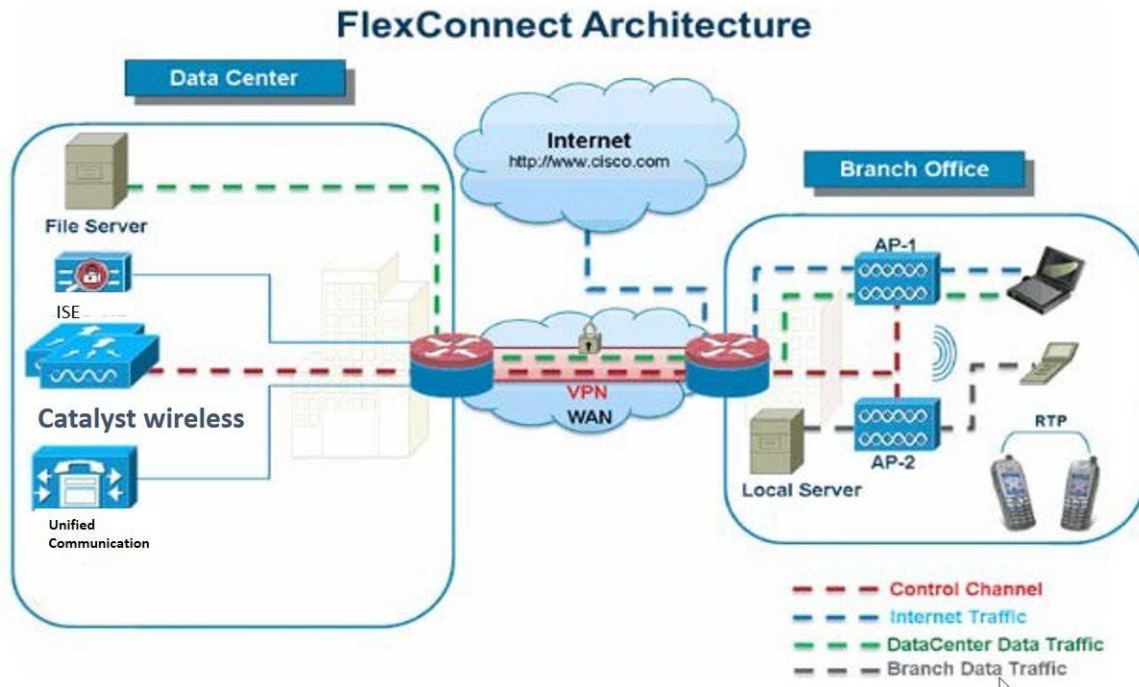
11ac Wave 1 and Wave 2 Access Points

AP18xx, 2802, 3802, 4800, 1540, 1560, 1700, 2700, 3700, 1570

Supported releases

IOS-XE -16.10

FlexConnect Architecture



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 size that can scale up to 100 APs and 250,000 square feet (5000 sq. 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

FlexConnect Mode	Description
Connected	A 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.

FlexConnect Mode	Description
Standalone	<p>Standalone mode is specified as the operational state the FlexConnect enters when it no longer has the connectivity back to the controller.</p> <p>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.</p>

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.

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	1.44Mbps	1 sec	50	1000
Data + Voice	128 Kbps	100 ms	5	25
Data + Voice	1.44Mbps	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 the flexconnect matrix document on the below link to validate the list of supported feature.

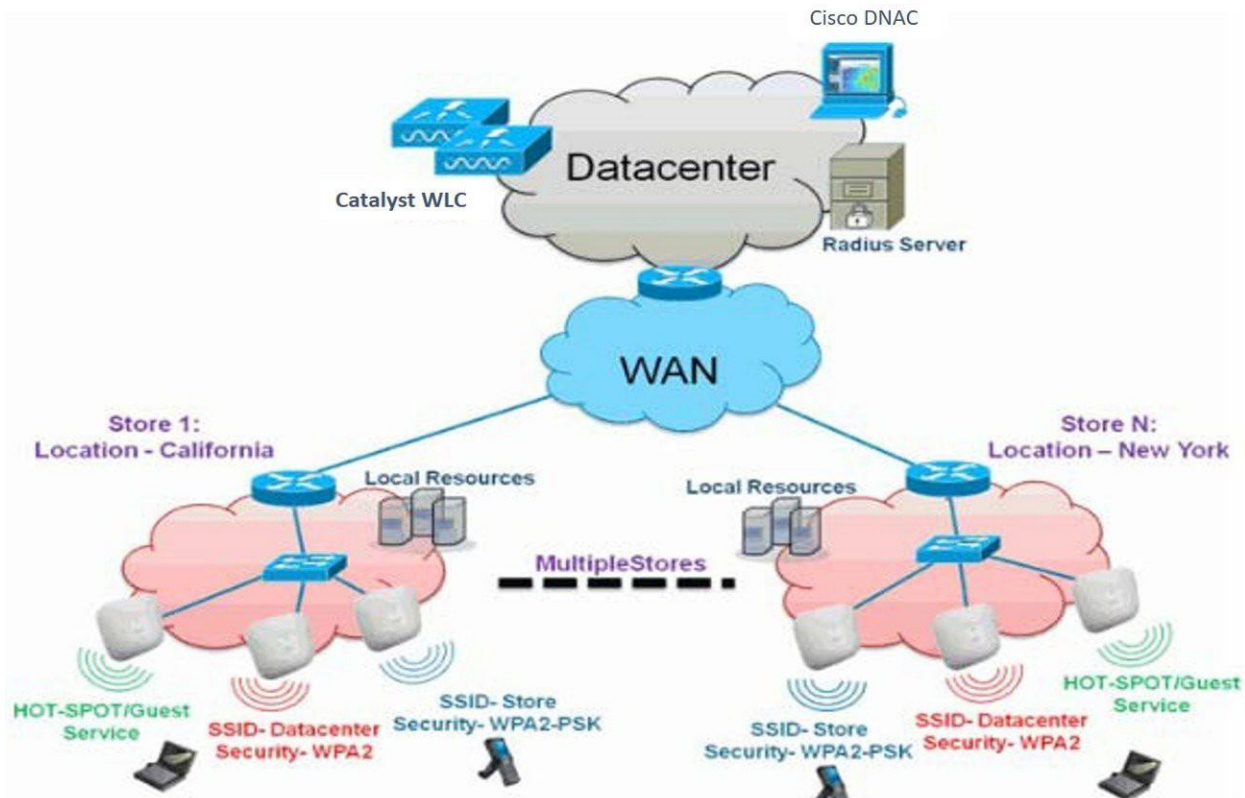
Wireless Branch Network Design

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 sq. 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.

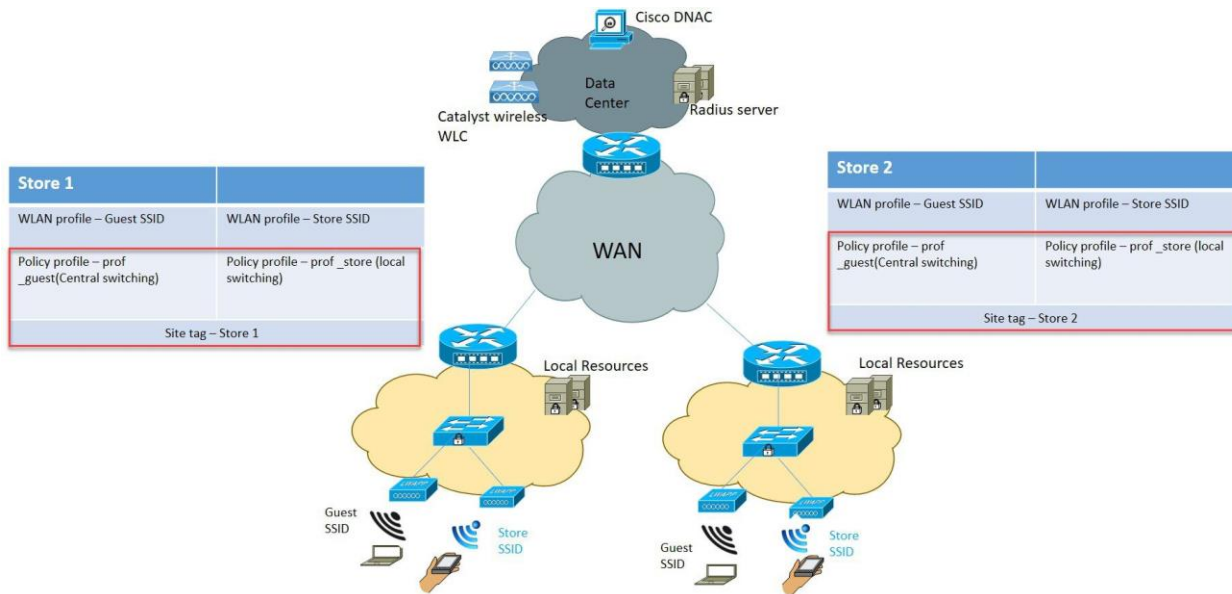
The FlexConnect solution virtualizes the complex security, management, configuration, and troubleshooting operations within the data center and then transparently extends those services to each branch. Deployments using FlexConnect are easier for IT to set up, manage and, most importantly, scale.

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:

Figure 1: Design replication across stores by mapping different site tags and policy tags



Features Addressing Branch Network Design

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

Features	Highlights
New config model on catalyst wireless family.	Ability to decouple and modularize the configuration entities .This enables to have the same configuration across different stores by having the same profiles across stores and using a different tags 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 which has a flex profile will autoconvert the AP to flexconnect mode without user intervention.
Efficient AP image upgrade	Reduces downtime when upgrading your branch and 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 which is tunnel to a controller in the DMZ zone.

Features	Highlights
URL ACL	Ability to support use cases of BYOD at the branch
Back up 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 Modularized and Reusable model with Logical decoupling of configuration entities

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

Table 3: Tags and Profiles

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.
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 which 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 type 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

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

Policy profile is an entity that constitutes of the all network and switching polices for a client with the exception of QoS which constitute the AP policies as well.

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. For example, VLAN, ACL, QOS, Session timeout, Idle timeout, AVC profile, Bonjour profile, Local profiling, Device classification etc.

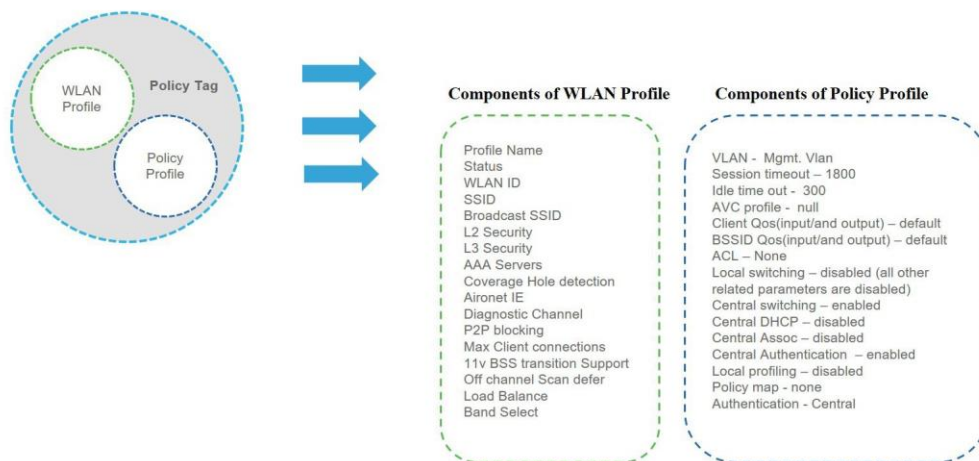
The WLAN Profile and Policy Profile are both part a Policy Tag and define the characteristics and policy definitions of a set of WLANs. The intent of decoupling the policies from the SSID even though it is a one-to-one mapping, is to give more flexibility to the admin in configuring site based policies(local 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 client policy)

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

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 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 master and slave AP list, the EAP profiles which 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.

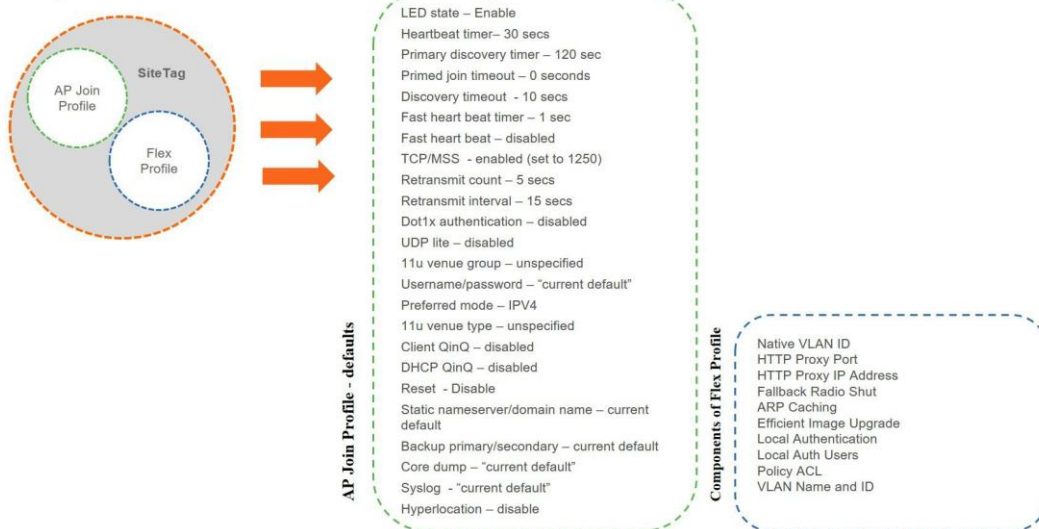
The AP Join Profile and Flex Profile are both part a Site Tag and define the characteristics of a local or remote site.

Site tag

Site tag constitutes of 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 central and remote site are part of the AP Join profile. The attributes that are specific to flex/remote site are part of the flex profile.

Default Site Tag constitutes of the default AP Join profile. There is no default flex profile. The default AP join profile values will be same as that for the global AP parameters today plus few parameters from the AP group in today’s configuration like “preferred mode”, 802.11u parameters, Location etc.

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.

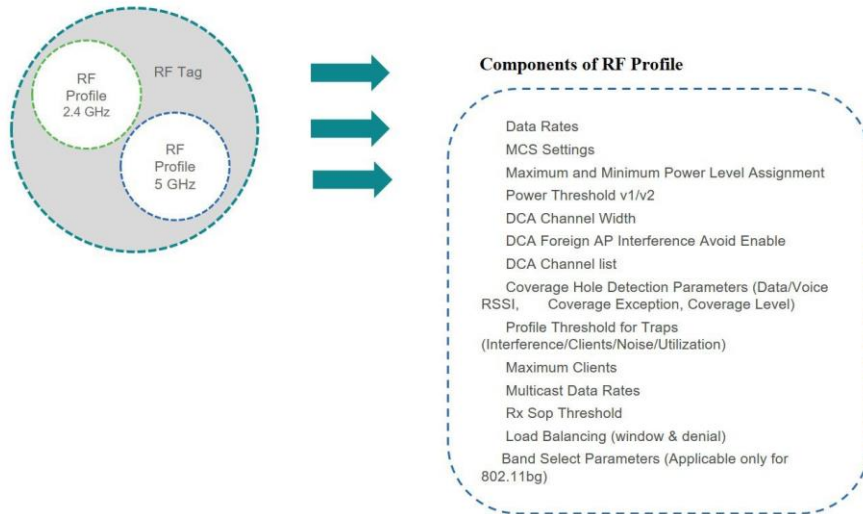
RF Tag

RF tag constitutes of the 11a and 11b RF profiles Default RF Tag constitutes of the default 802.11a RF profile and the default 802.11b RF Profile.

The default 11a RF profile and 11b RF profile contains default values for global RF Profiles for the respective radios.

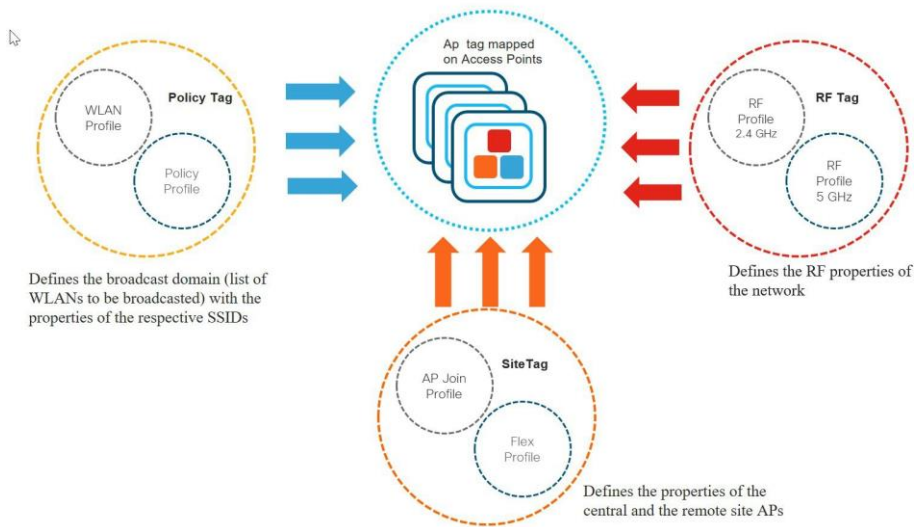


Components of RF Tag



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.



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 the controller deployment guide for controller bring up, SVI creation and management 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 which has the following deployment model will be used to show case the configuration model.

A store SSID which has a WPA-PSK security enabled, to connect the handhels used in a store .The SSID would be locally switched SSID

A guest SSID which is centrally switched

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

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

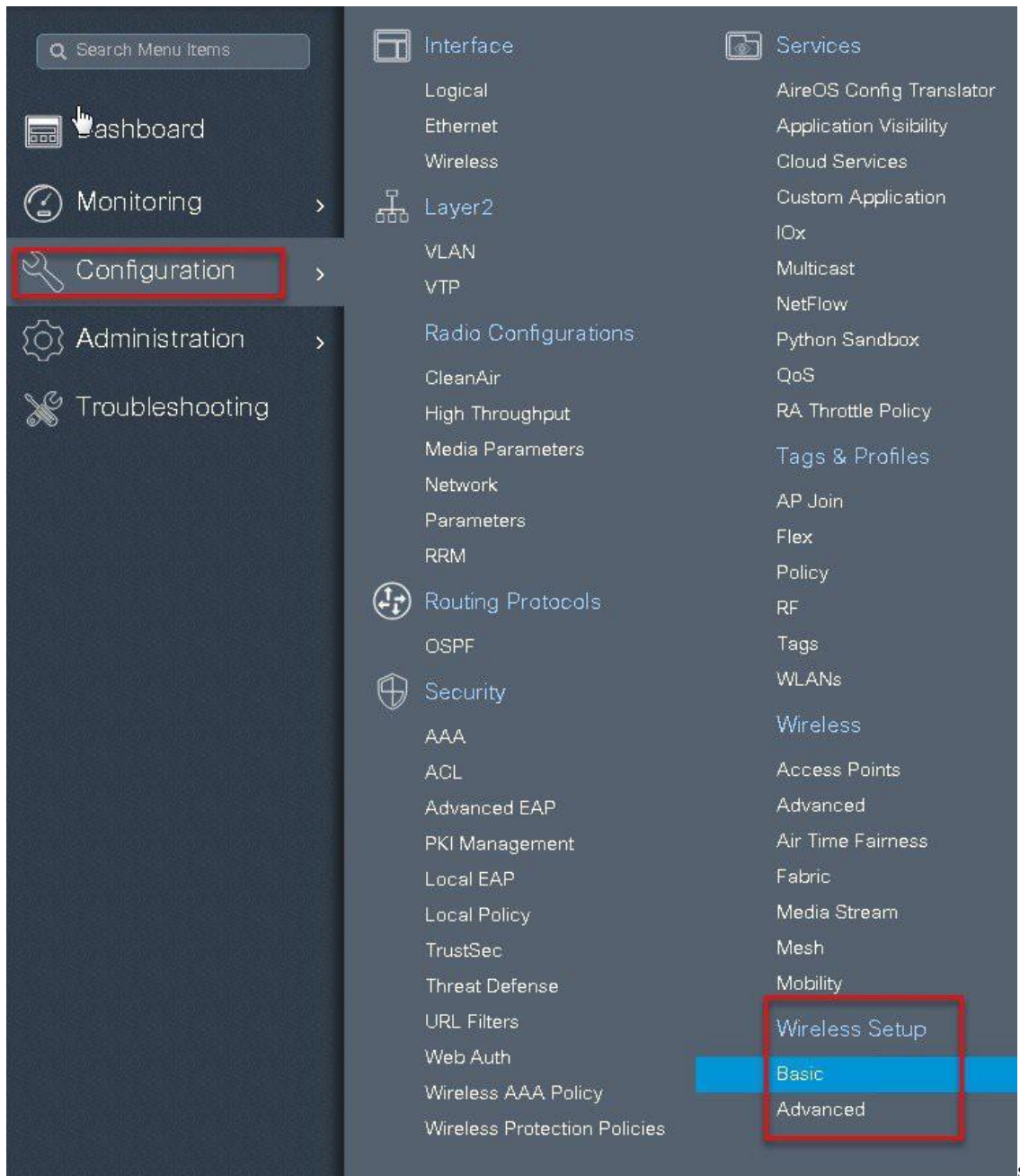
Step1 Click on the wireless setup wizard .



Step2 Select the basic setup wizard from the drop down box and click on “Add”.



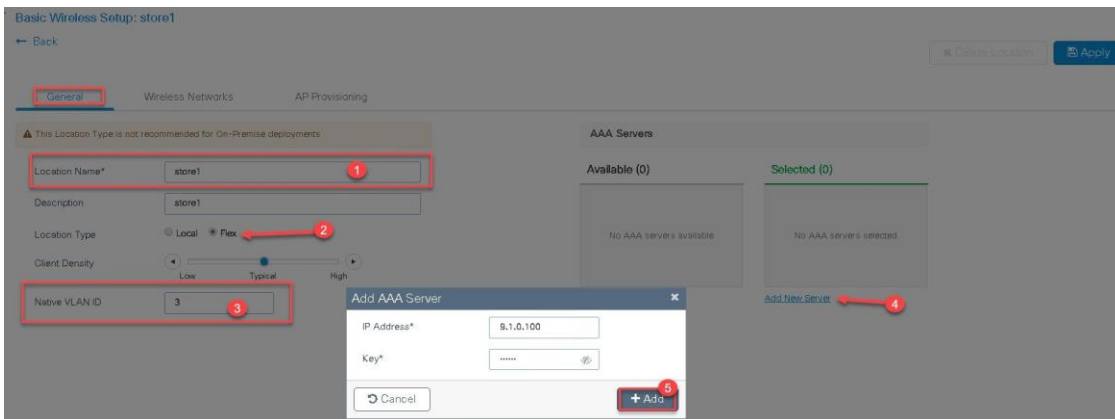
An Administrator can also start the wizard by navigating to Configuration>wireless setup >basic



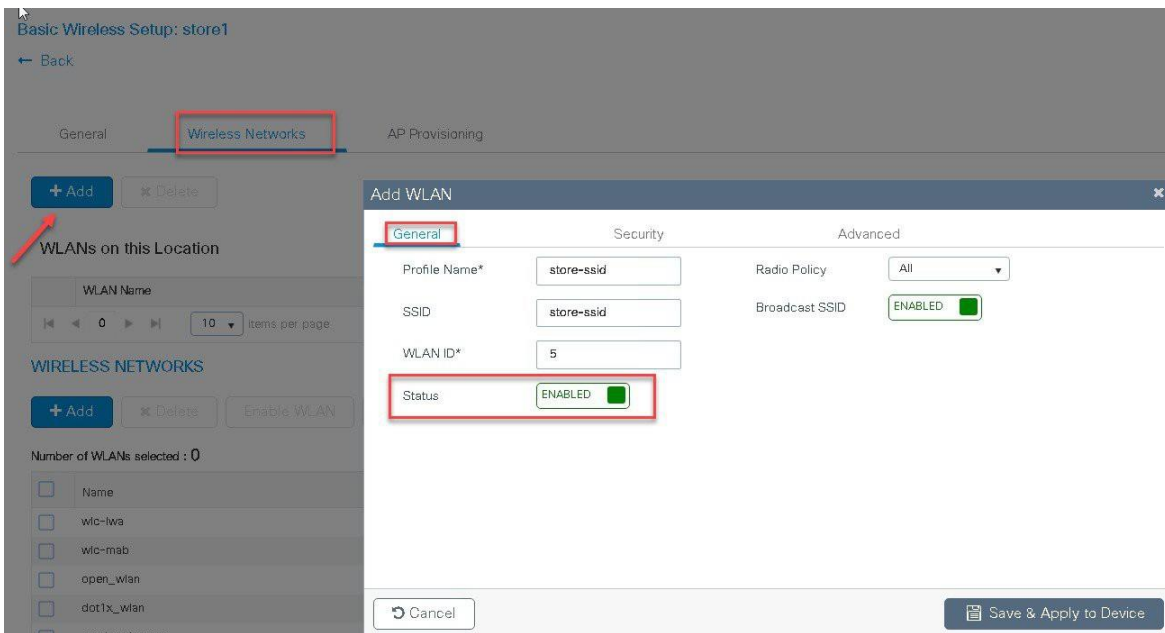
Step3 Select a name for the remote site, specify the location type as flex for branch deployments.

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



- Step4** 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.



Add WLAN

General Security Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode WPA + WPA2

Fast Transition Adaptive Enabled

MAC Filtering

Over the DS

Reassociation Timeout 20

Protected Management Frame

PMF Disabled

WPA Parameters

WPA Policy

WPA2 Policy

WPA2 Encryption

AES(CCMP128)

CCMP256

GCMP128

GCMP256

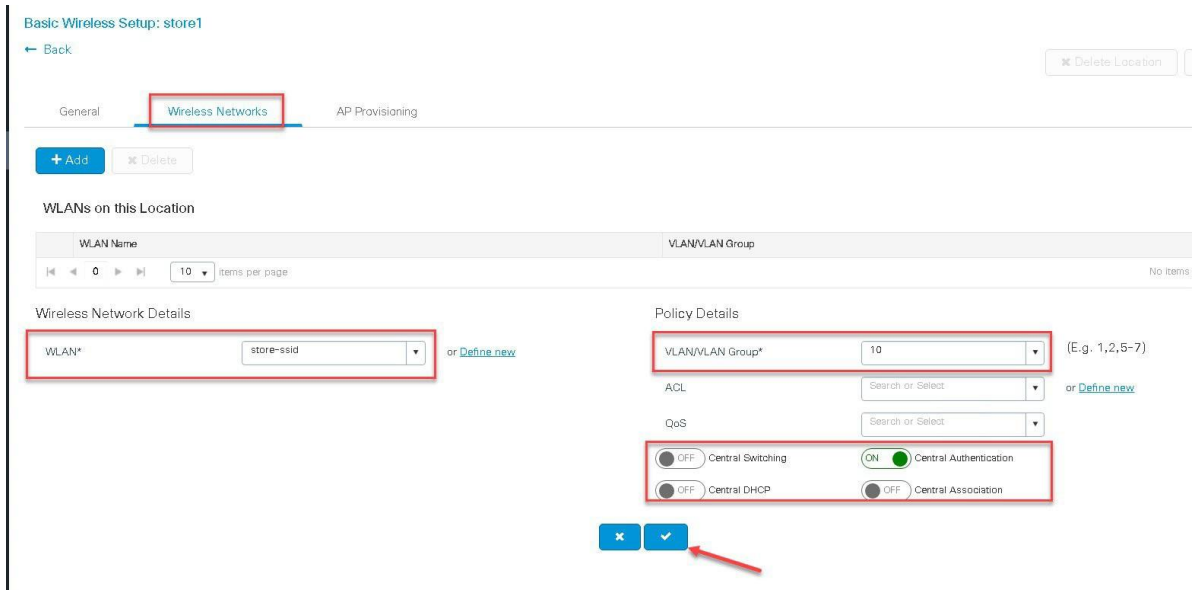
Auth Key Mgmt PSK

PSK Format ASCII

Pre-Shared Key

Cancel Save & Apply to Device

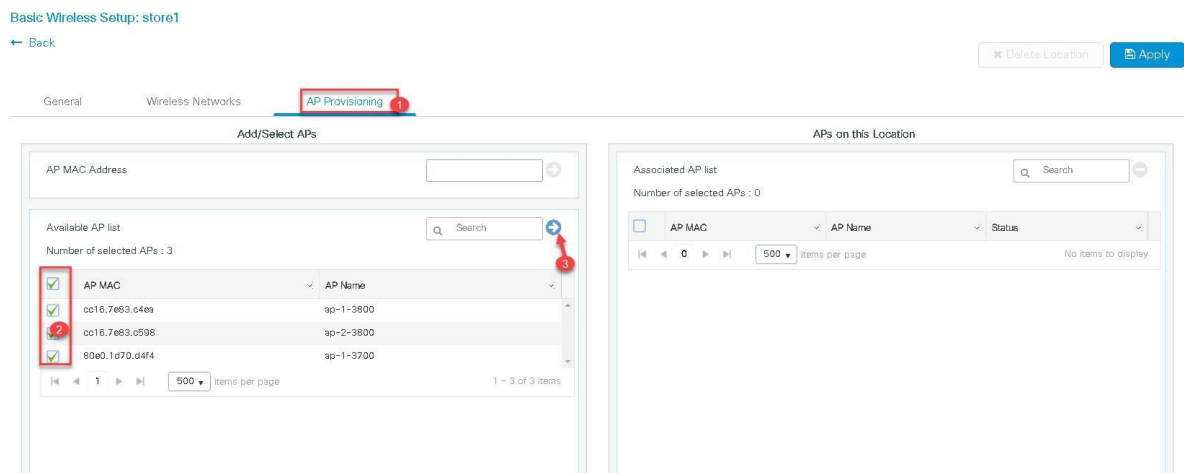
- Step5** Define the policy for the WLAN.
 The VLAN/VLAN group defines the VLAN used by the SSID.



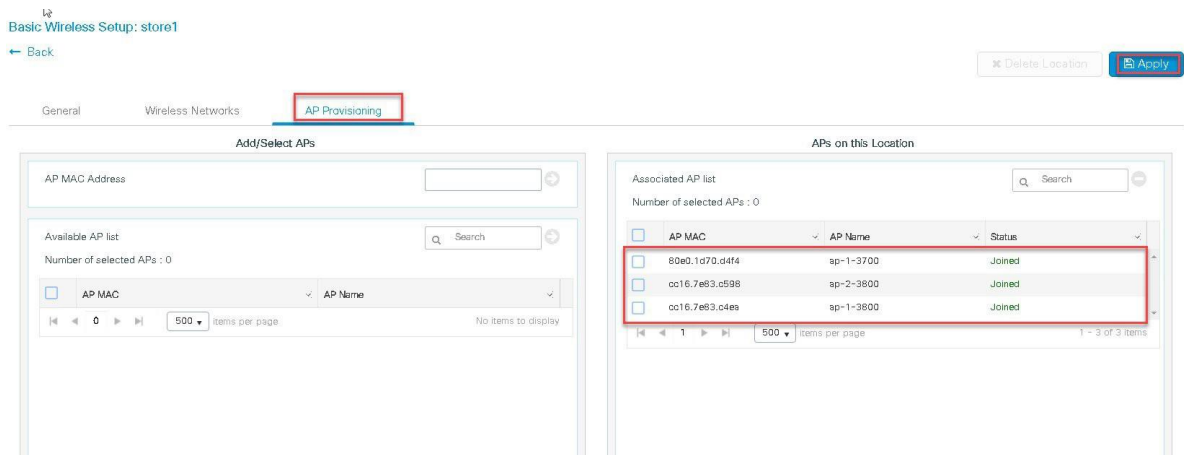
Step6 Click on the AP provisioning to provision the SSID and policy profile on the selected AP.

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, ap would reboot to boot in flex connect mode.



Step7 Click apply to complete the wizard.

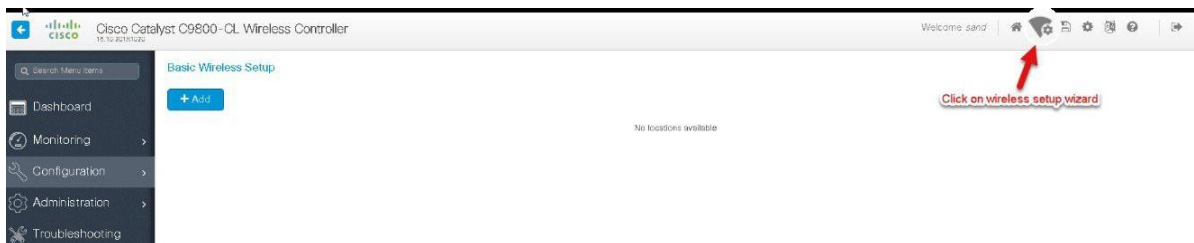


Advanced wireless setup wizard

In this section, the advance config wizard is used to create a Guest SSID with web-authentication which would be central switched through a WLC at the datacenter.

Procedure

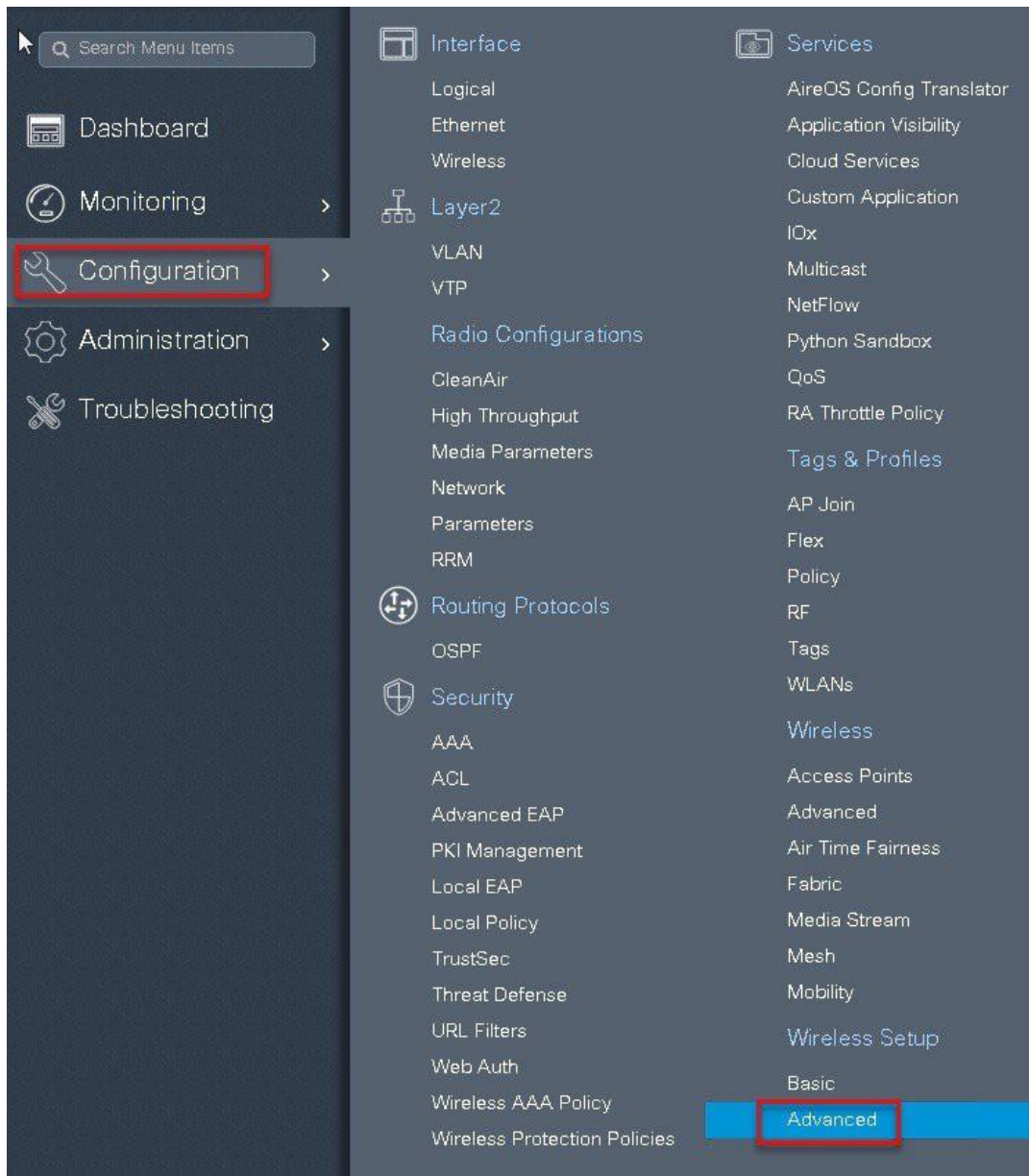
Step 1 Click on the wireless setup wizard.



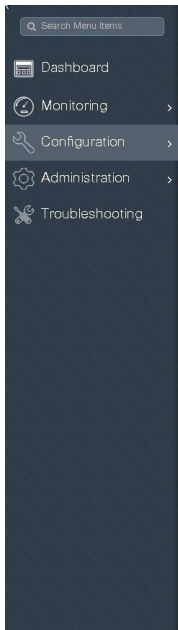
Step 2 Select the advanced option.



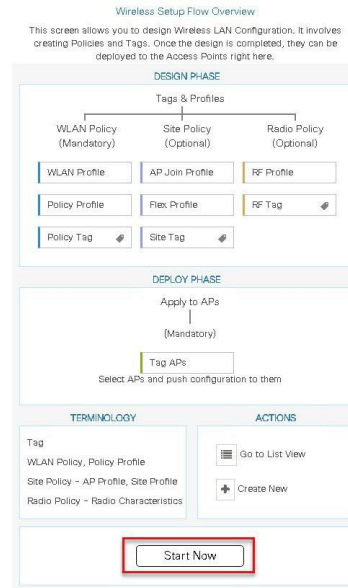
An Administrator can also start the wizard by navigating to Configuration > wireless setup > advanced.



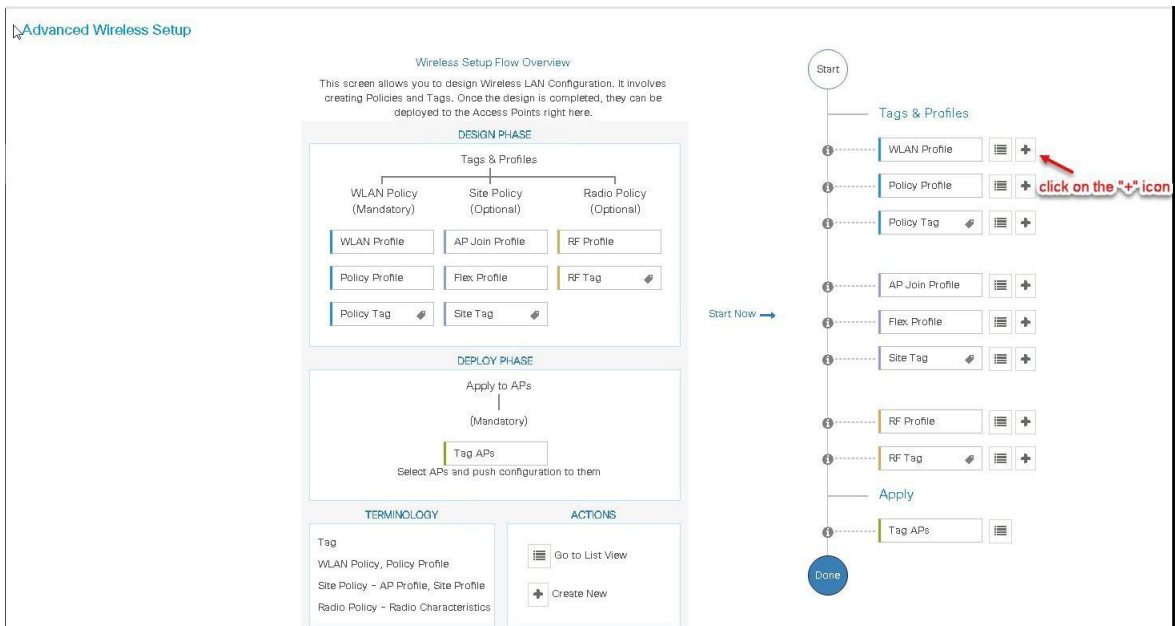
Step3 The Advanced config wizard gives an overview of the flow of tag and policies . Click on the “Start Now” button to start the wizard.



Advanced Wireless Setup



Step4 click on the “+” icon to start creating the WLAN.



Step5 Define the SSID name and security type for the WLAN.

Add WLAN

General Security Advanced

Profile Name* Radio Policy

SSID Broadcast SSID

WLAN ID*

Status

Add WLAN

General Security Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode Fast Transition

MAC Filtering Over the DS

Reassociation Timeout

Add WLAN

General **Security** Advanced

Layer2 **Layer3** AAA

Web Policy

Webauth Parameter Map global

Authentication List Select a value

Show Advanced Settings >>>

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

Cancel Save & Apply to Device

Step6 Create a policy profile for the SSID.
 Define the policy profile to be central switched and central authentication.

Advanced Wireless Setup

+ Add Delete Enable WLAN Disable WLAN

Number of WLANs selected : 0

<input type="checkbox"/>	Name	ID	SSID
<input type="checkbox"/>	open_wlan	1	open_wlan

10 Items per page

Start

Tags & Profiles

- WLAN Profile
- Policy Profile
- Policy Tag
- AP Join Profile
- Flex Profile
- Site Tag
- RF Profile
- RF Tag

Apply

click on "+" icon to add a 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.

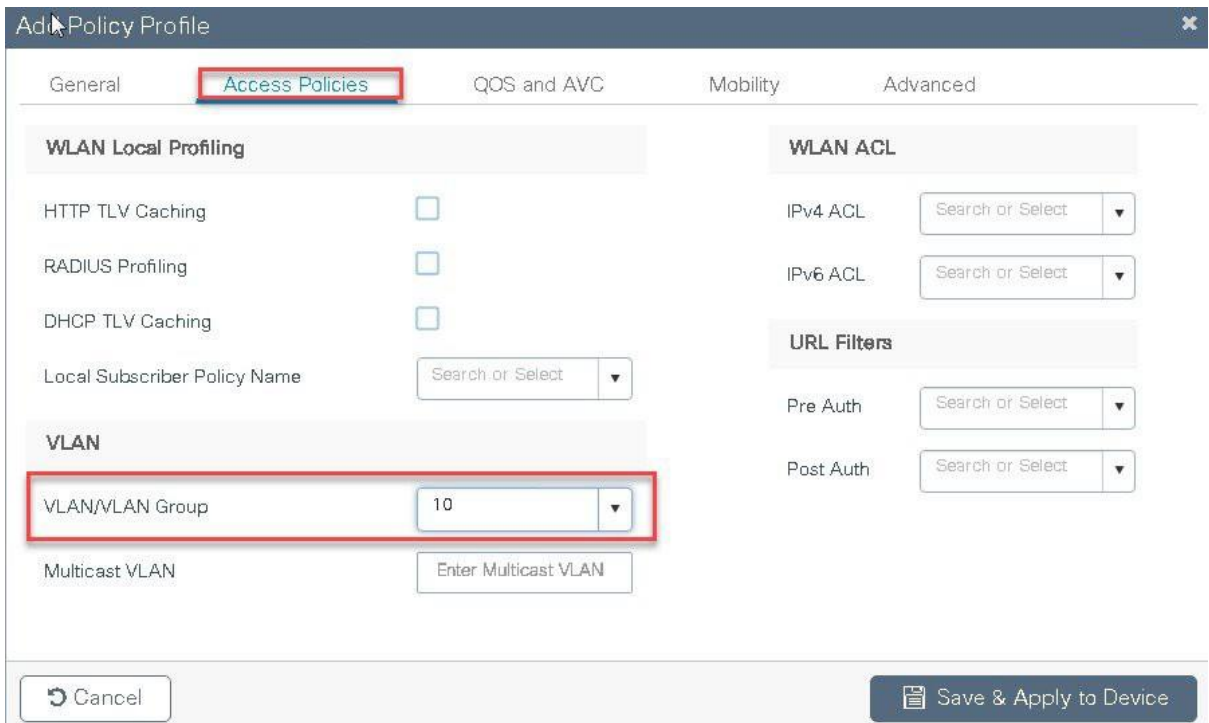
Name*	guest_ssid	WLAN Switching Policy	
Description	Enter Description	Central Switching	<input checked="" type="checkbox"/>
Status	ENABLED ■	Central Authentication	<input checked="" type="checkbox"/>
Passive Client	<input type="checkbox"/> DISABLED	Central DHCP	<input checked="" type="checkbox"/>
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED	Central Association	<input checked="" type="checkbox"/>
CTS Policy		Flex NAT/PAT	<input type="checkbox"/>
Inline Tagging	<input type="checkbox"/>		
SGACL Enforcement	<input type="checkbox"/>		
Default SGT	2-65519		

↶ Cancel
📄 Save & Apply to Device

Step 7

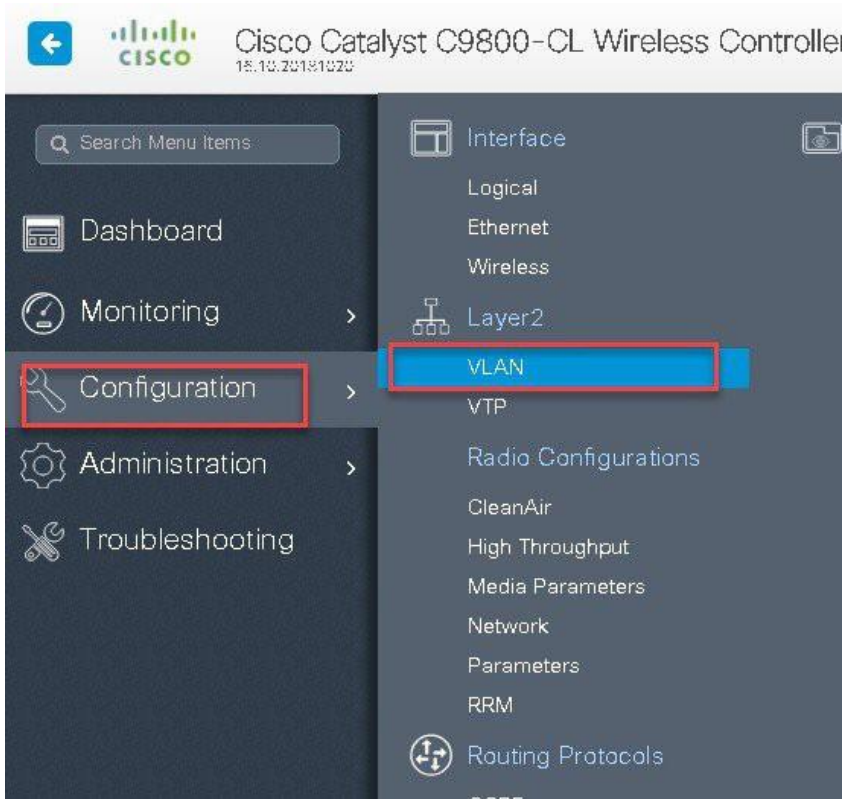
Define a VLAN for the SSID under the access policies , in the example below the VLAN 10 is mapped on the policy profile.

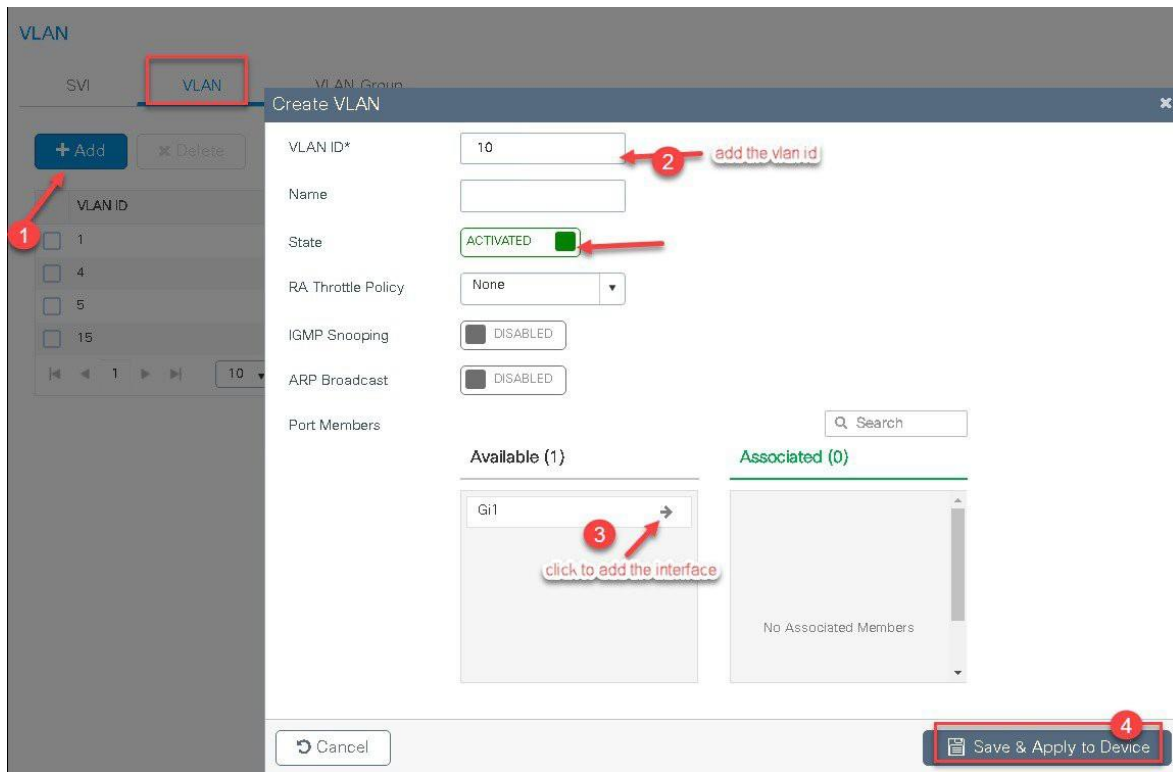
The Controller also needs a layer 2 VLAN or a layer 3 SVI to be created to centrally switch the traffic from the controller.



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

Navigate to Configuration > VLAN





Step8 An optional attribute to set is the export anchor configuration, please refer the mobility deployment guide to set up mobility peers.

Add Policy Profile ✕

General Access Policies QoS and AVC **Mobility** Advanced


Mobility Anchors

Export Anchor *select the option for export anchor*

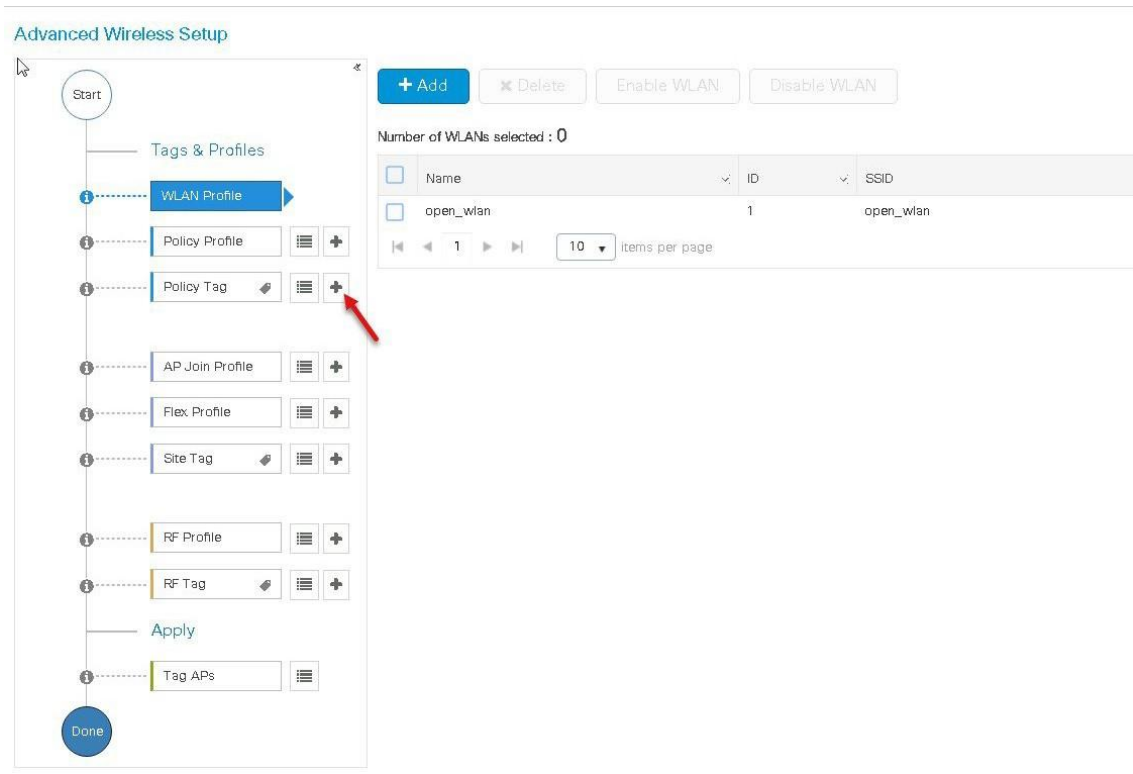
Static IP Mobility DISABLED

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)	Selected (0)	
Anchor IP	Anchor IP	Anchor Priority
<div style="border: 1px solid #ccc; padding: 5px; display: flex; align-items: center;"> 9.1.5.16 →</div> <i>click to add the anchor controller</i>	Anchors not assigned	

Step9 Create a policy tag which binds the SSID and policy profile together.



Step 10 Define a flex profile, the flex profile is used for configuring the VLANs on the AP which is used for the local switched SSID's.

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

Advanced Wireless Setup

Start

Tags & Profiles

- WLAN Profile
- Policy Profile
- Policy Tag
- AP Join Profile
- Flex Profile
- Site Tag
- RF Profile
- RF Tag

Apply

+ Add x Delets Enable WLAN Disable WLAN

Number of WLANs selected : 0

<input type="checkbox"/>	Name	ID	SSID
<input type="checkbox"/>	open_wlan	1	open_wlan

10 Items per page

click on "+" icon to add a policy

Step11 Define the native VLAN for the flexconnect AP's.

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

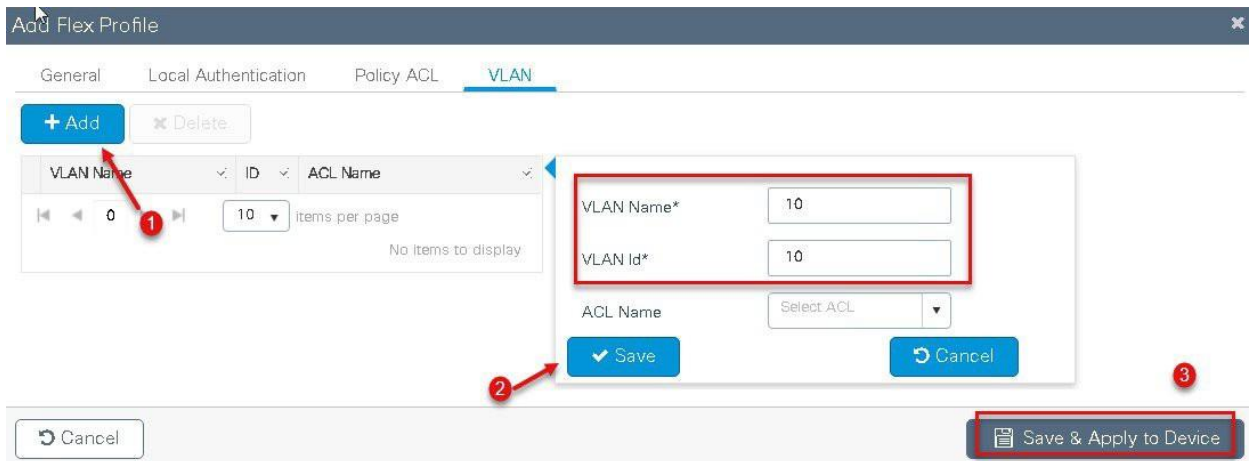
Efficient Image Upgrade

Office Extend AP

Join Minimum Latency

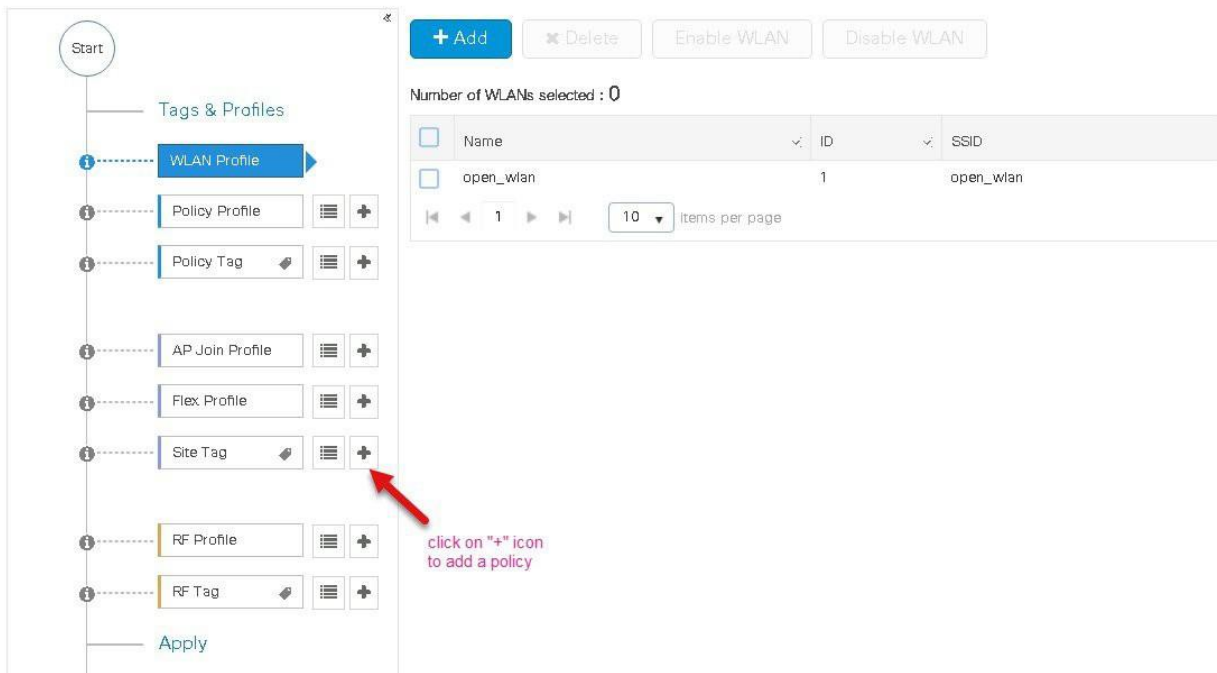
Cancel Save & Apply to Device

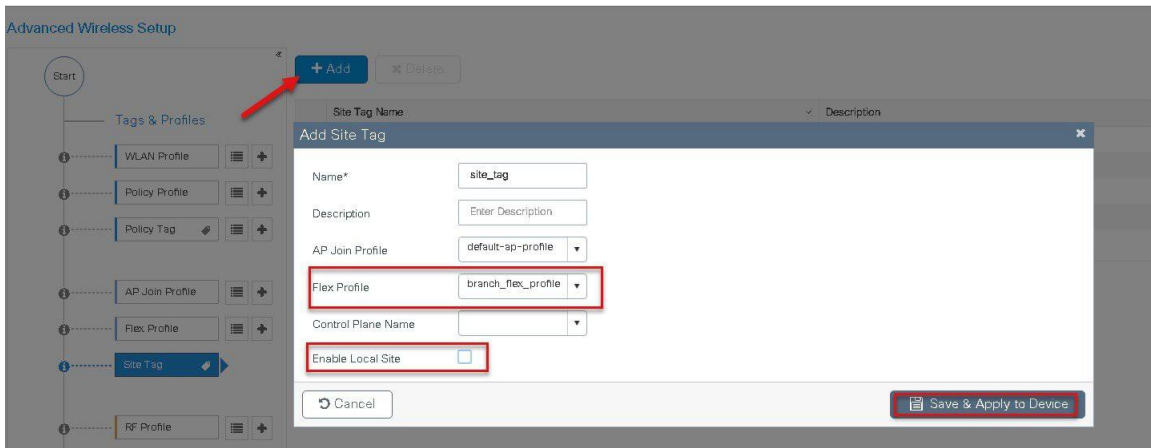
Step12 Define the VLANS to be used for the local switched SSID.



Step 13 Define a site tag which 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.

Advanced Wireless Setup





Step 14

The final stage is to provision the policy, site and RF tag on the AP.

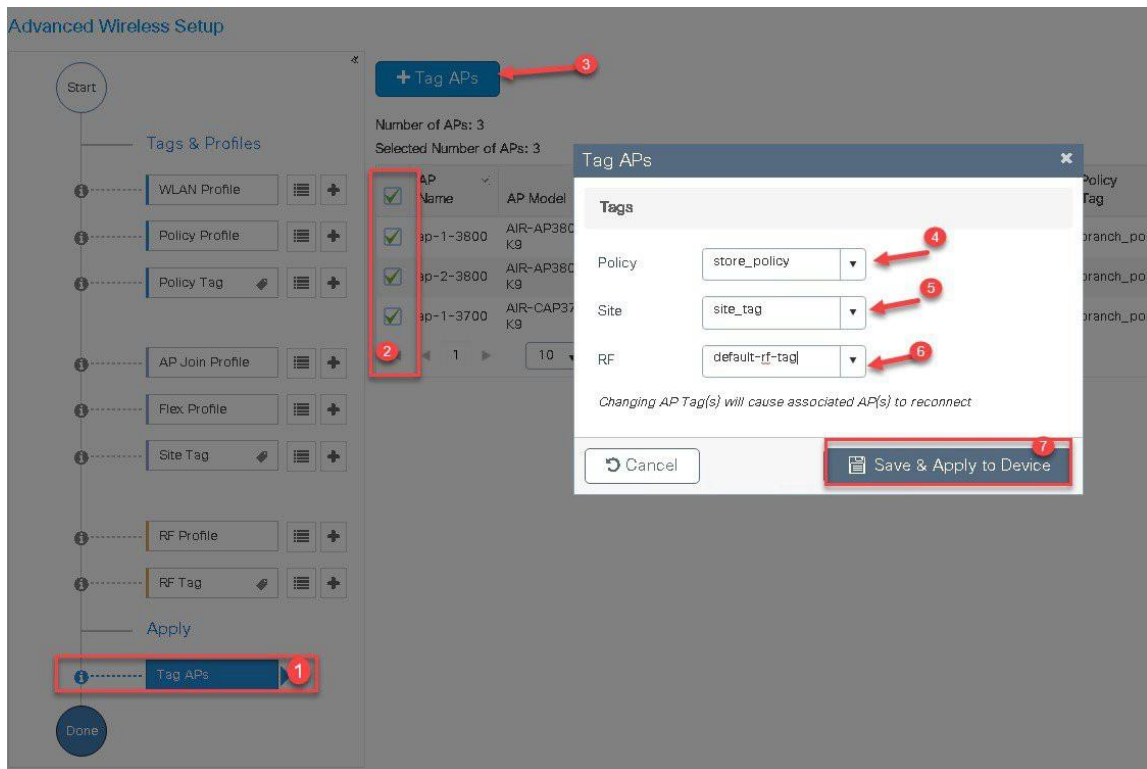
Click on Tag APs to select the profiles and have it configured for the AP.

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, AP would reboot to boot in flex connect mode.

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



Manual Configuration

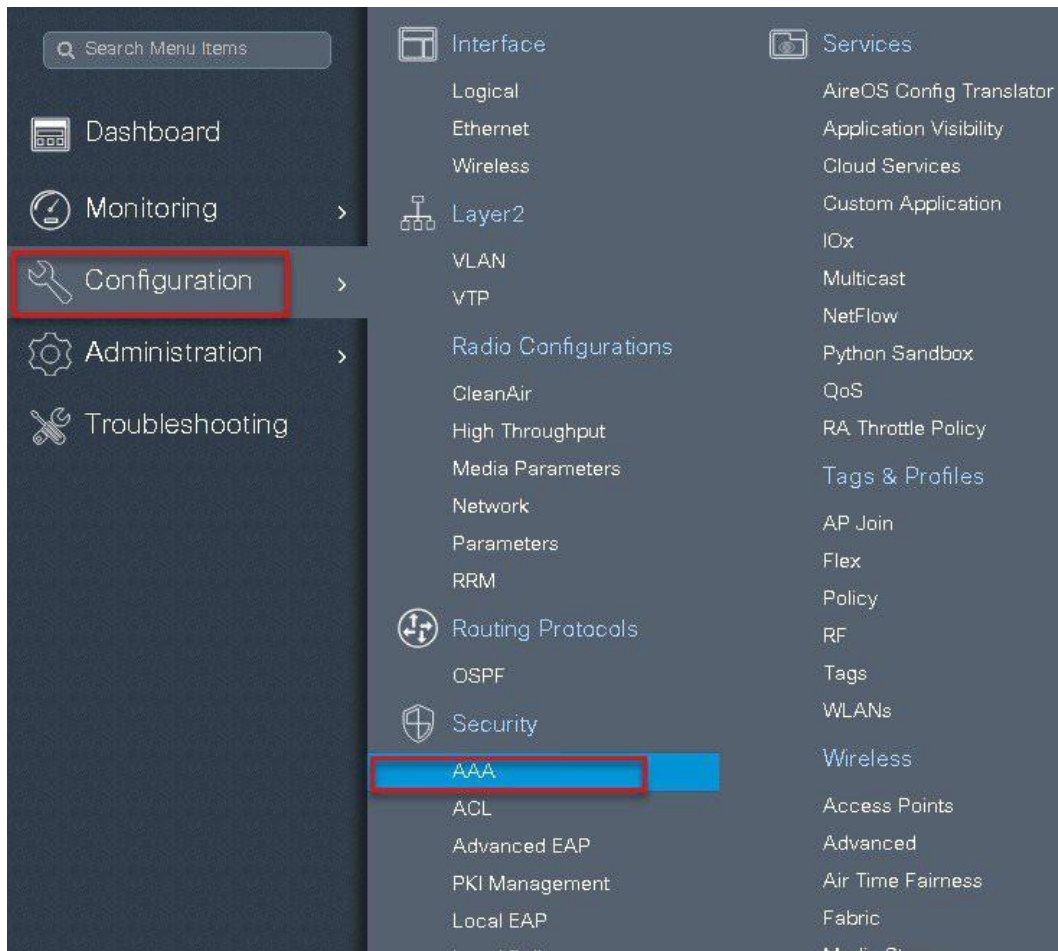
The manual configuration for creating the SSID /tags and profiles is done using the WLC GUI, in this section we will cover creating an enterprise SSID with dot1x enabled.

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

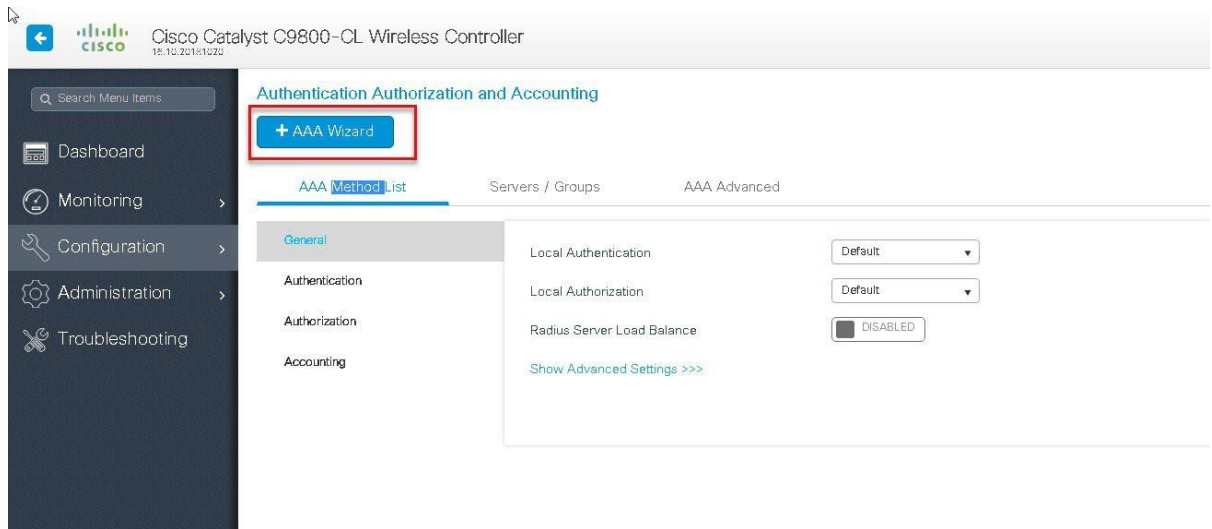
Procedure

Step1 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:

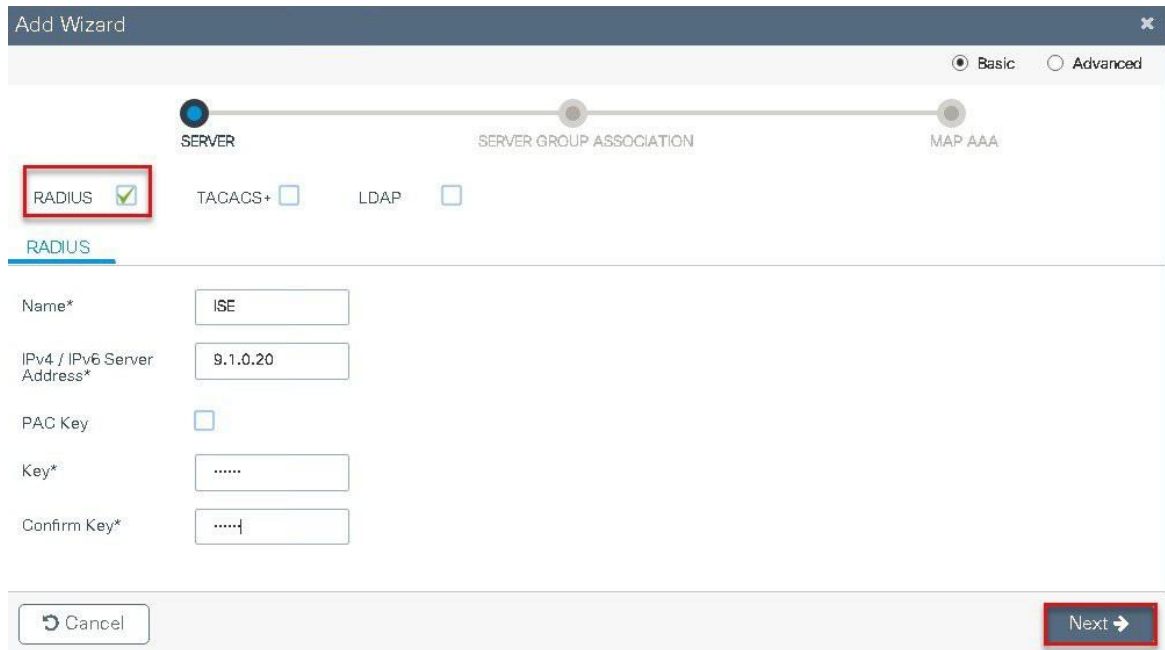
Configuration > security > AAA



Step2 Use the AAA wizard to create the server and server groups.



Step3 Define a name for the server and specify the IP address and shared secret.



Step4 Create a server group and map the server in the group.

Add Wizard Basic Advanced

SERVER SERVER GROUP ASSOCIATION MAP AAA

RADIUS

Name*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Available Servers

- freerad
- ISE-2
- ISE

Assigned Servers

- ISE

← Previous Next →


Step5 Enable dot1x system control and check mark 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 

Local Authentication

Local Authorization

Radius Server Load Balance

[Show Advanced Settings >>>](#)

← Previous Save & Apply to Device

Step6 Check mark 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*

Type*

Group Type

Fallback to local

Available Server Groups

- Idap
- tacacs+
- rad-group
- freerad
- radgrp_branch

> <

Assigned Server Groups

- ISE

> <

[← Previous](#)

[Save & Apply to Device](#)

Step7 Check mark the authorization list and 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*

Type*

Group Type

Fallback to local

Available Server Groups

- Idap
- tacacs+
- rad-group
- freerad
- radgrp_branch

> <

Assigned Server Groups

- ISE

> <

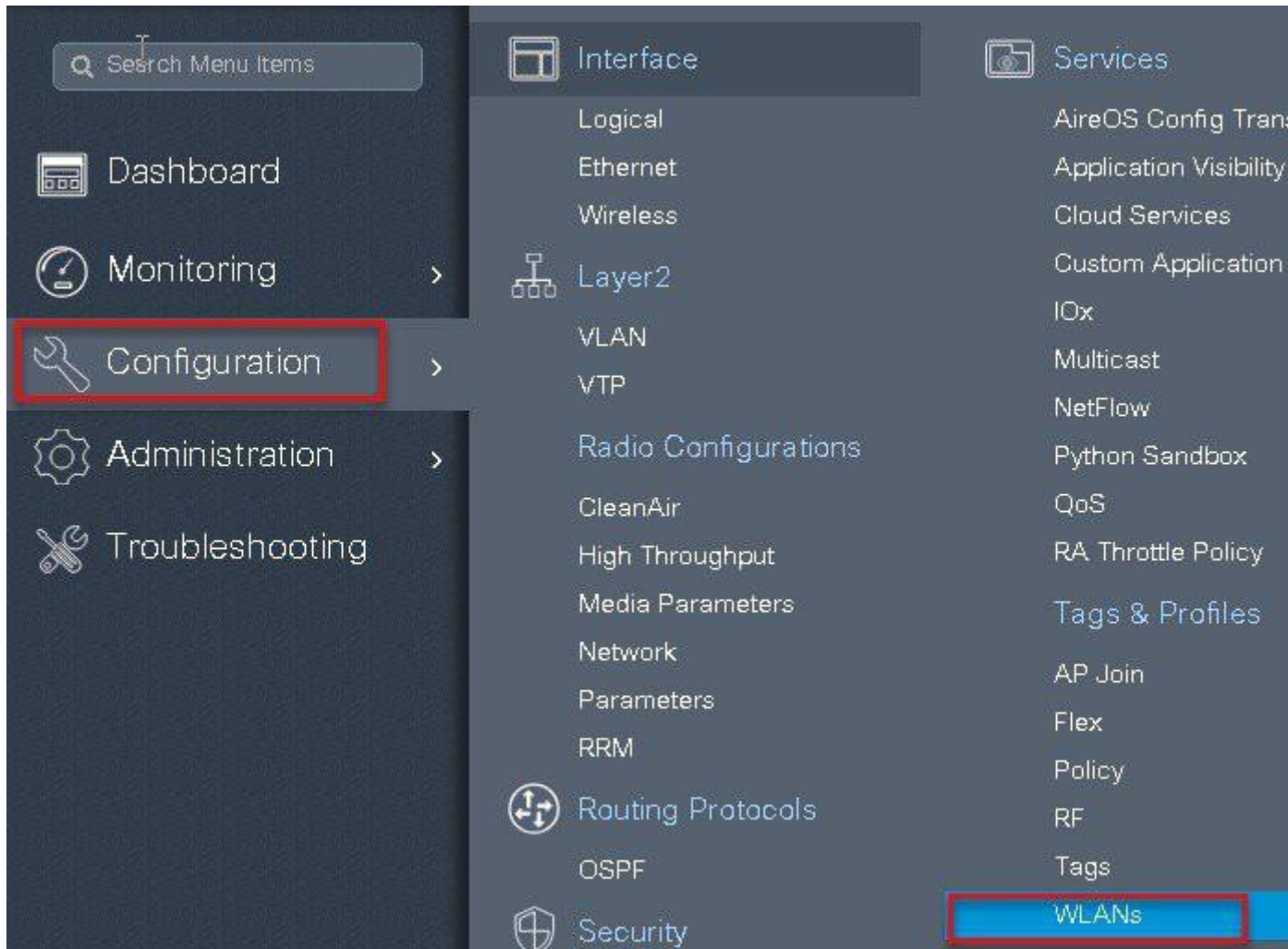
[← Previous](#)

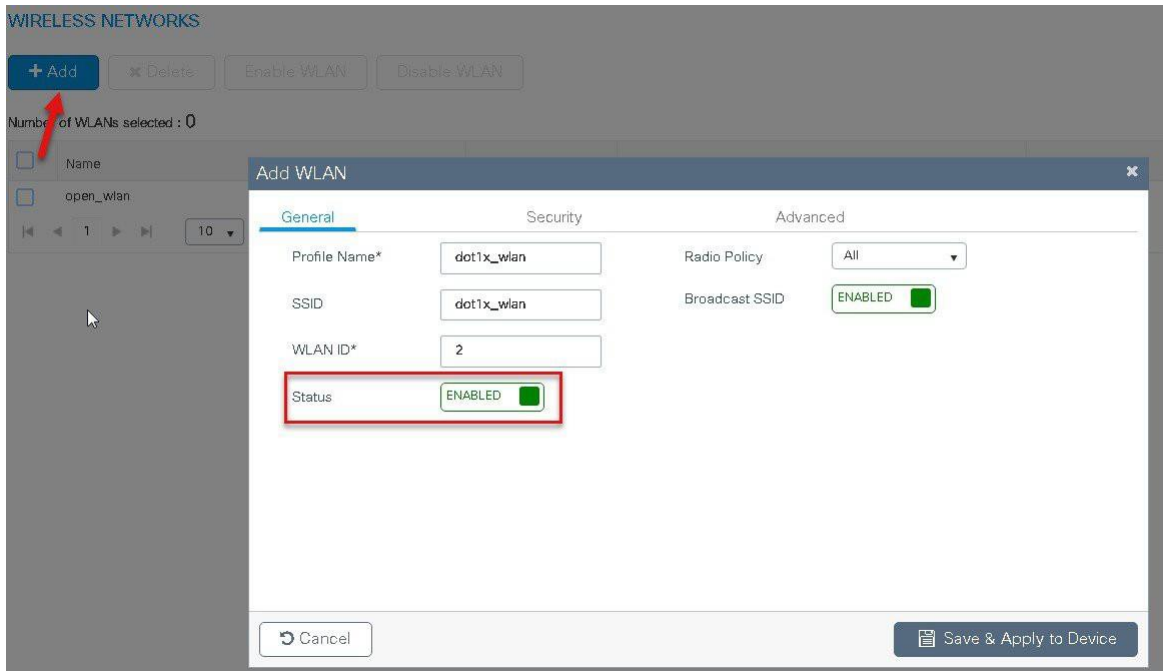
[Save & Apply to Device](#)

Step8

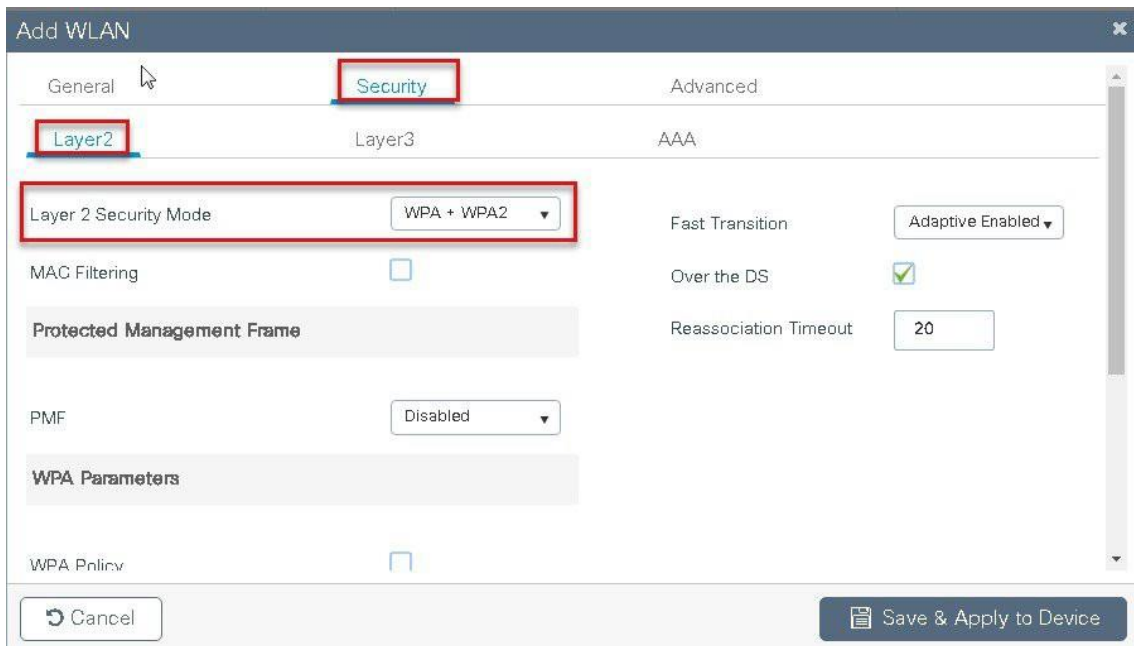
Create a Dot1x WLAN and map the method list on the WLAN.

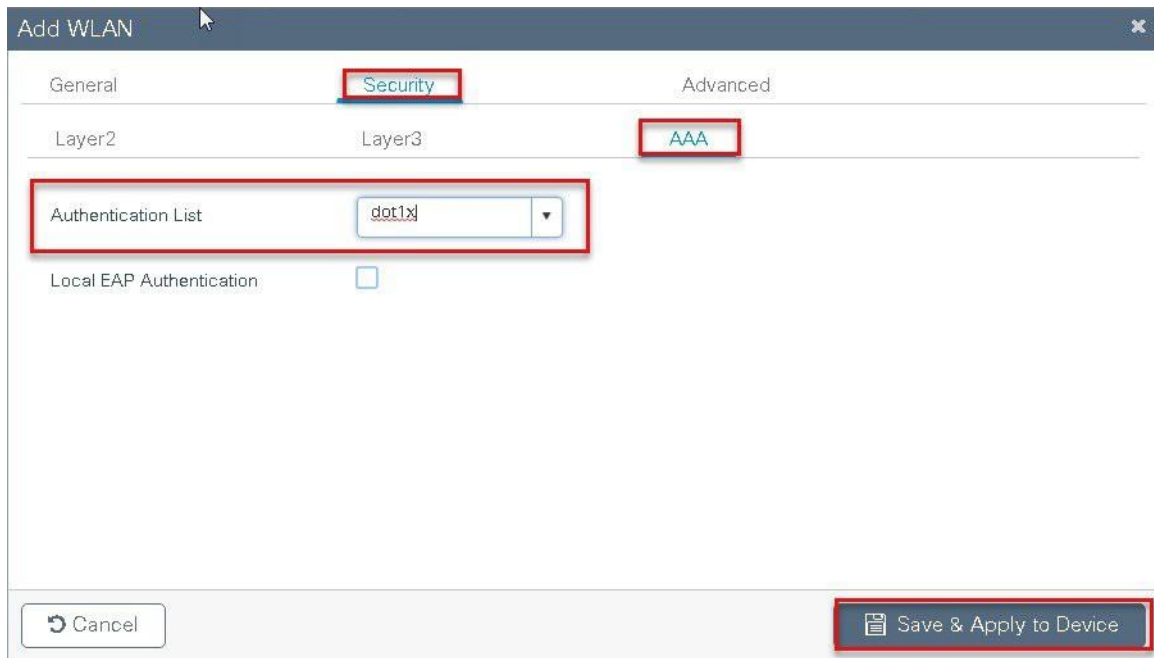
Navigate to the ConfigurationTags & profiles > WLAN to create the SSID.



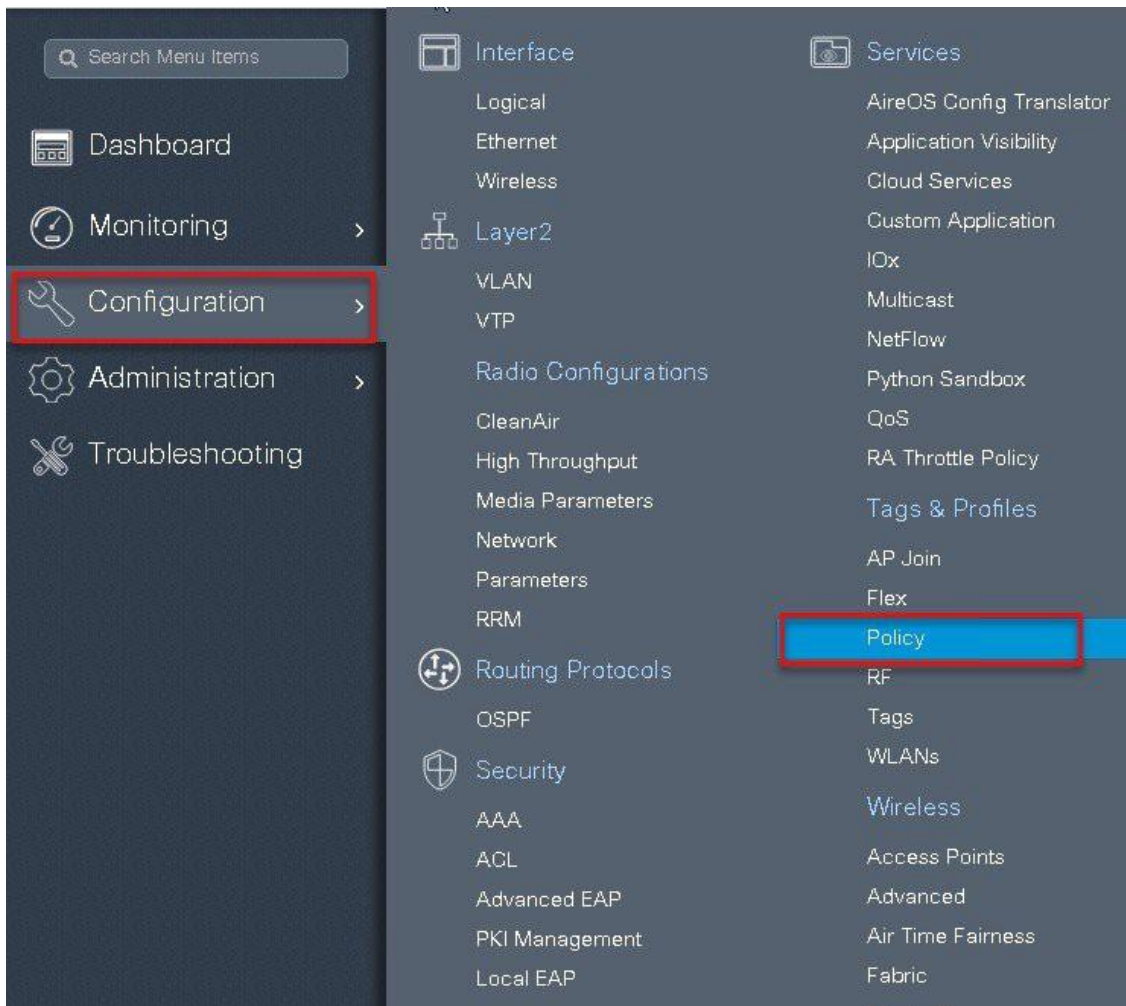


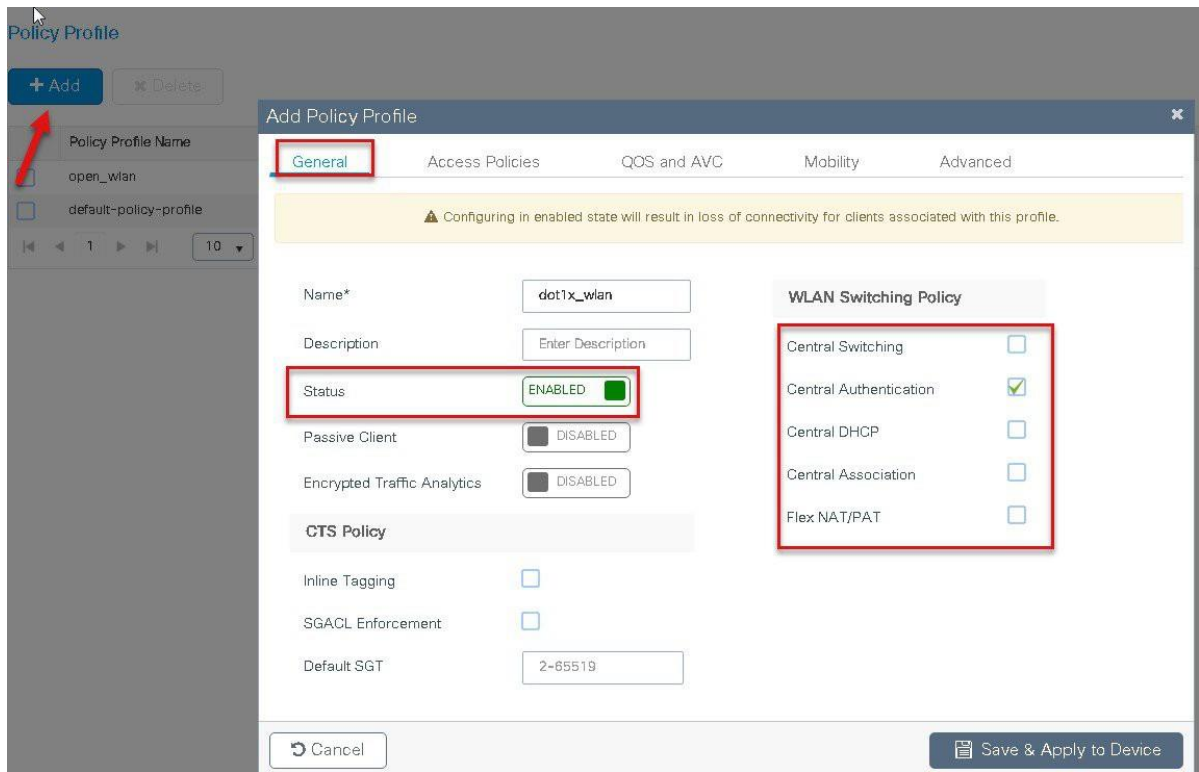
Step9 Define the security for the WLAN.



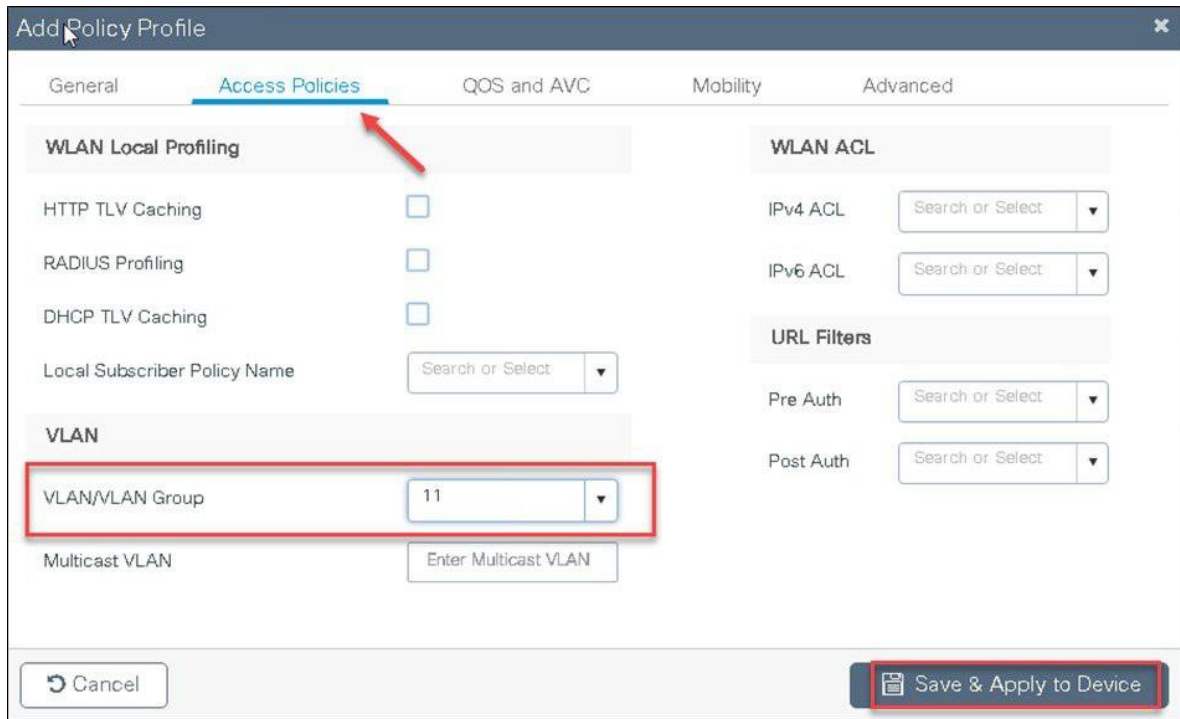


Step 10 Create a policy profile which defines switching capability of the WLAN and the interface mapping to the WLAN.





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



Add Policy Profile

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

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

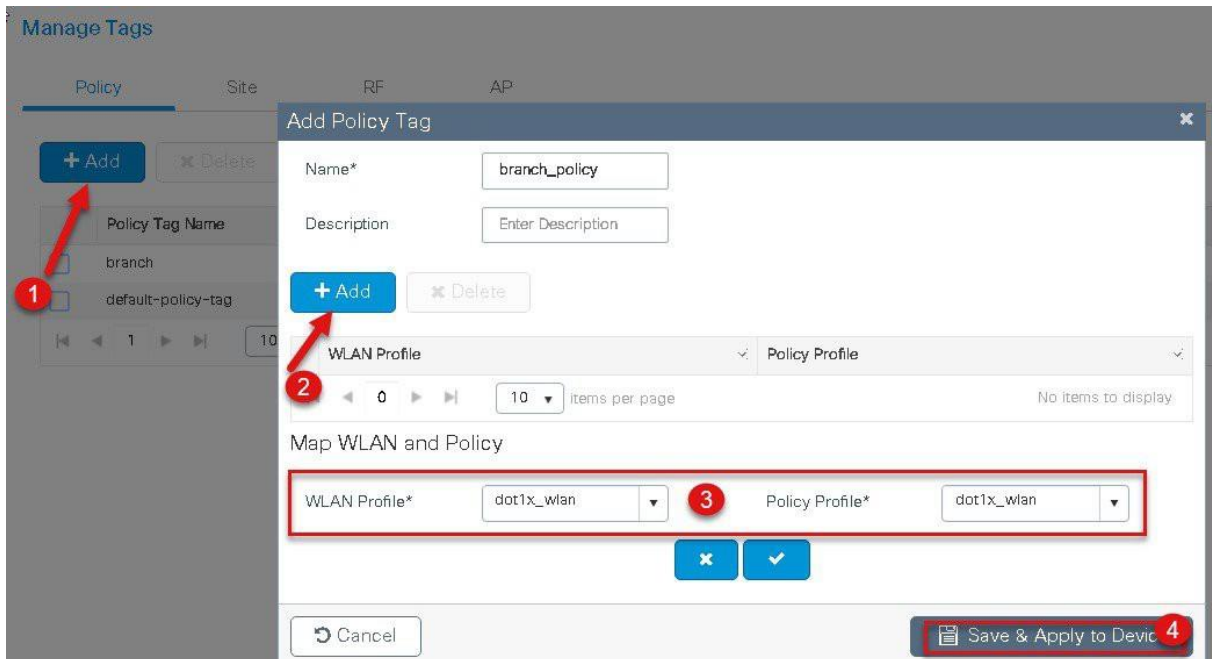
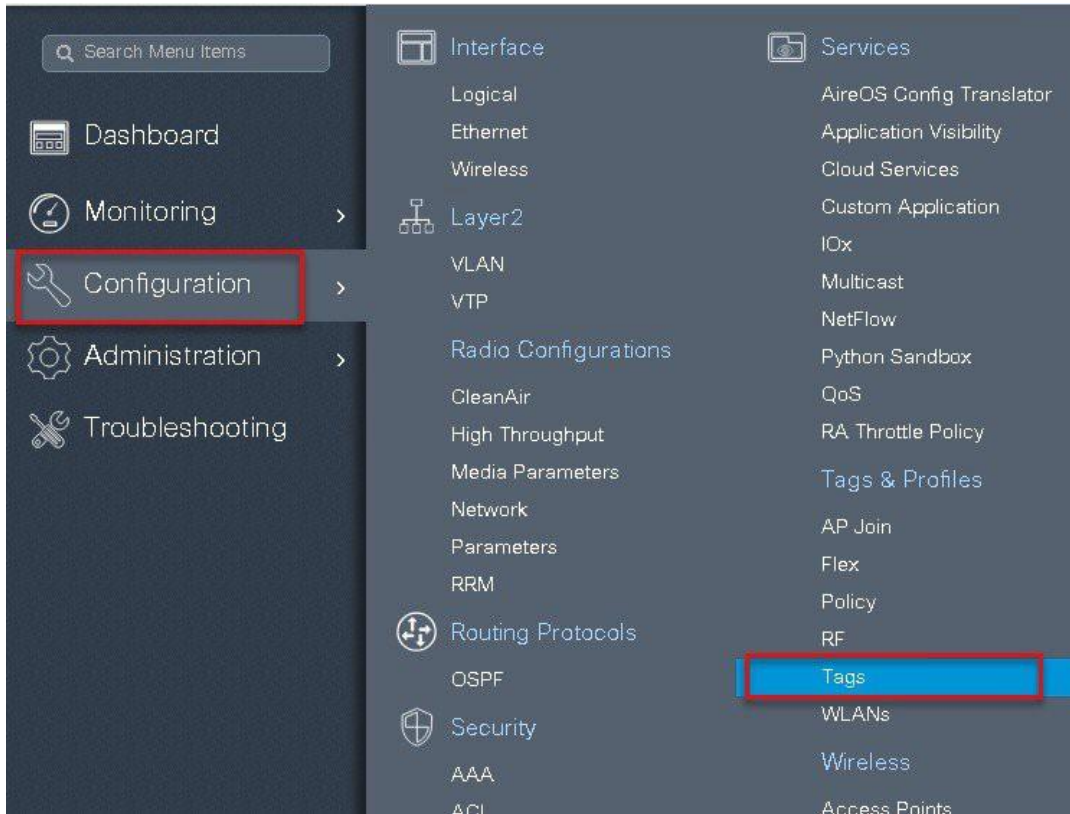
Air Time Fairness Policies

2.4 GHz Policy Search or Select

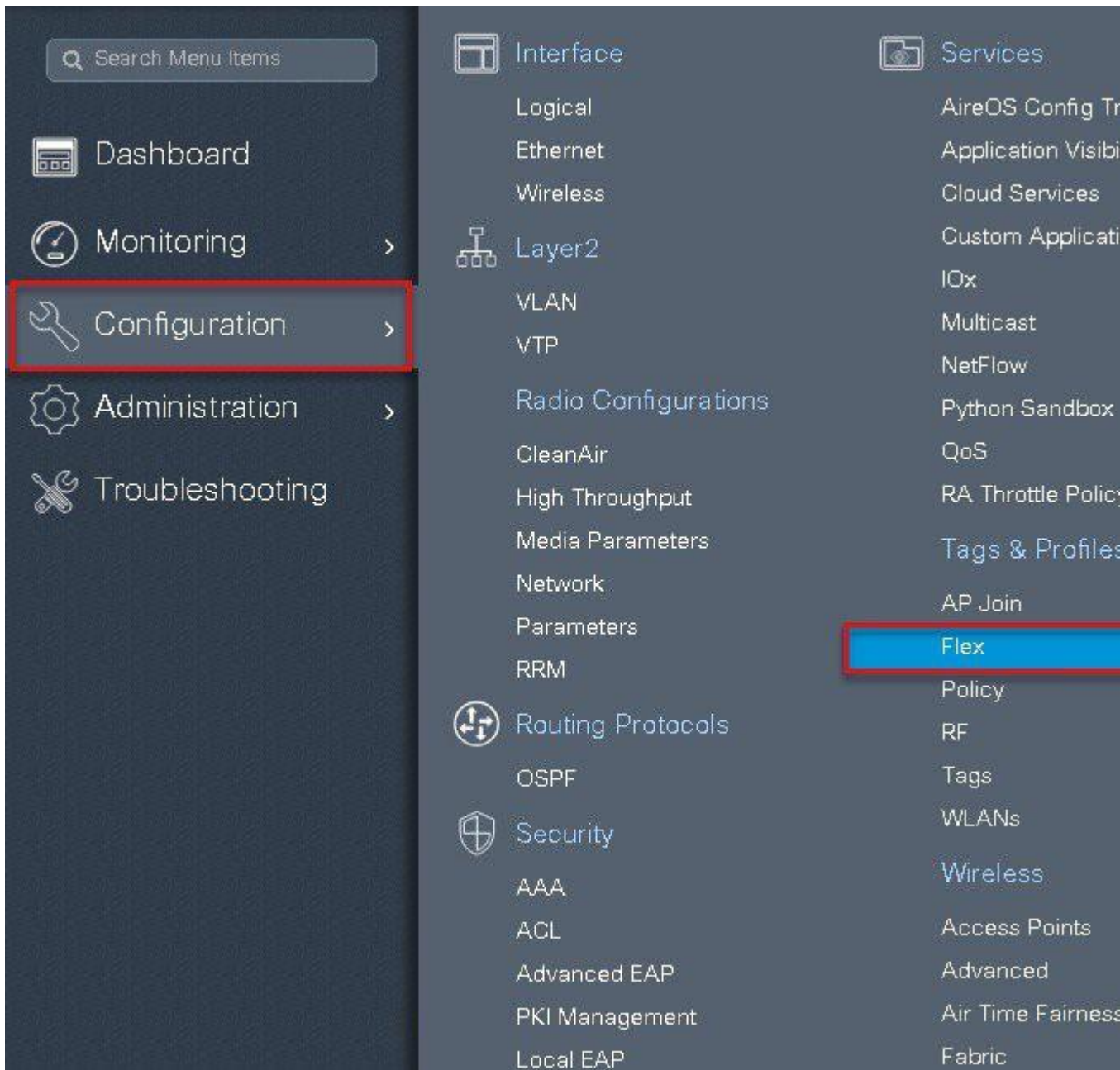
5 GHz Policy Search or Select

Cancel Save & Apply to Device

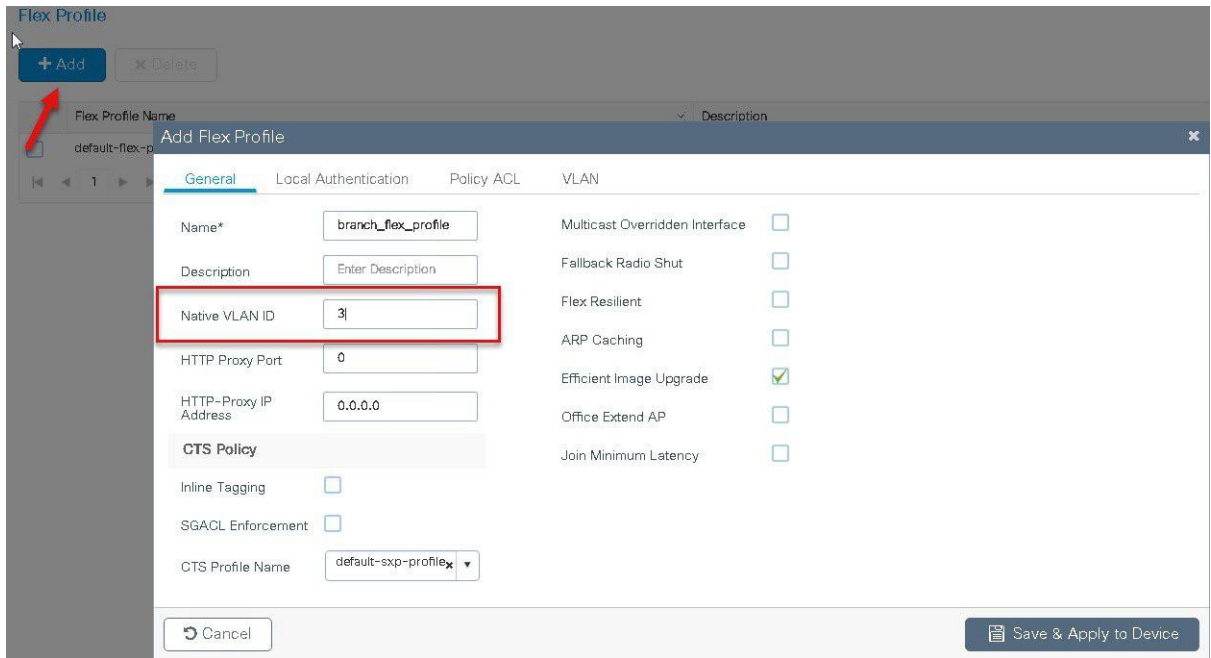
- Step 12** Create a policy tag which bundles the policy profile and WLAN profile together.
 Navigate to configuration > Tag and create a policy tag mapping the WLAN and policy profile.



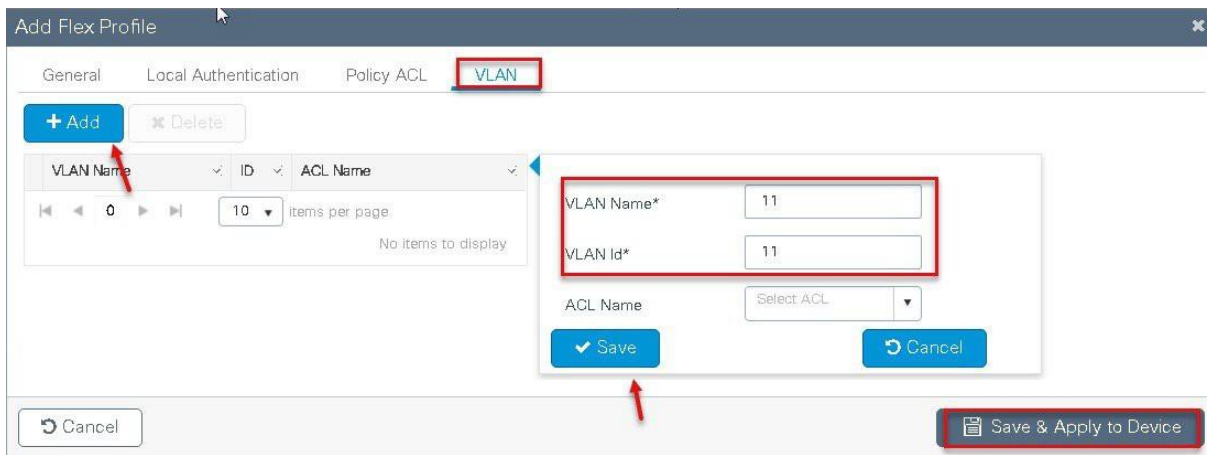
Step 13 Create a flex profile that defines the flex AP properties.
To create a flex profile navigate to Configuration > Tags and Profile > flex.



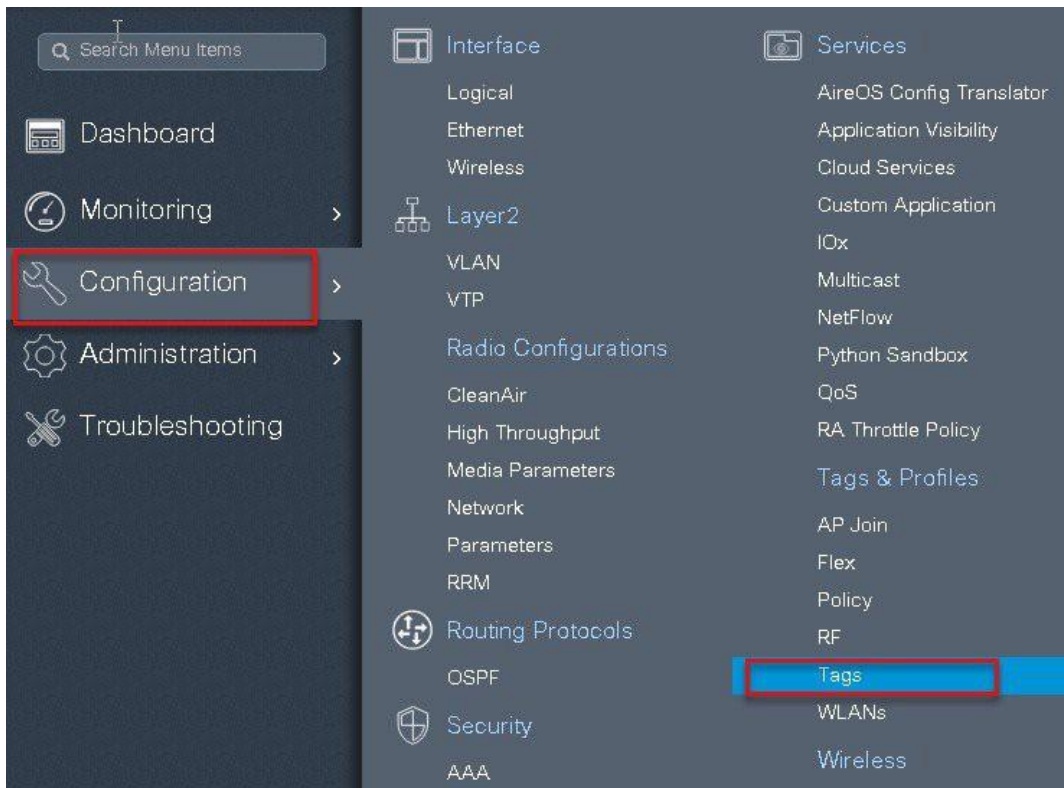
Step 14 Define the native VLAN for the Flexconnect AP.



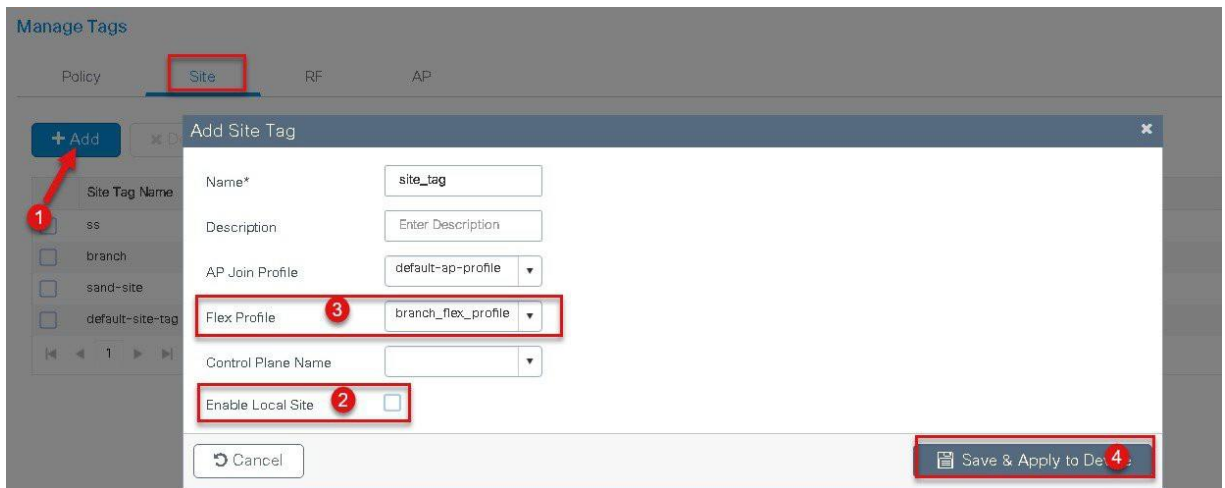
Step 15 Define the VLANs to be used for local switched SSID, in this example we use VLAN 11 which is local switched VLAN from the AP.



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.



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 AP's

Navigate to Configuration > wireless setup > Advanced

The screenshot shows the Cisco Catalyst C9800-CL Wireless Controller interface. The left sidebar contains a navigation menu with the following items: Dashboard, Monitoring, Configuration (highlighted with a red box), Administration, and Troubleshooting. The main content area is divided into three sections: Interface, Services, and a central list of configuration options. The 'Advanced' option under the 'Wireless Setup' section is highlighted with a red box. The right side of the interface displays the 'Wireless Setup Flow Overview' screen, which includes a 'DESIGN PHASE' section with 'Tags & Profiles' (WLAN Policy, Site Policy, Radio Policy) and 'DEPLOY PHASE' (Apply to APs, Tag APs). A 'Start Now' button is highlighted with a red arrow.

The screenshot shows the 'Advanced Wireless Setup' wizard. The left sidebar is the same as in the previous screenshot. The main content area displays the 'Advanced Wireless Setup' screen, which includes the 'Wireless Setup Flow Overview' and a detailed 'Start Now' flow. The flow starts with 'Start' and proceeds through the following steps: Tags & Profiles, WLAN Profile, Policy Profile, Policy Tag, AP Join Profile, Flex Profile, Site Tag, RF Profile, RF Tag, and Tag APs. The 'Tag APs' step is highlighted with a red arrow. The flow ends with 'Done'.

Cisco Catalyst C9600-CL Wireless Controller

Advanced Wireless Setup

+ Tag APs

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.c4a0.7560	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

Start

Tags & Profiles

- WLAN Profile
- Policy Profile
- Policy Tag
- AP Join Profile
- Flex Profile
- Site Tag
- RF Profile
- RF Tag

Apply

Tag APs

Done

Advanced Wireless Setup

+ Tag APs

Number of APs: 3
Selected Number of APs: 3

AP Name	AP Model	AP MAC	AP Mode	Admin Status	Operation Status
✓ ap1-3800	AIR-AP3802I-B-K9	0081.c4a0.6fe0	Flex	Enabled	Registered
✓ ap2-3800	AIR-AP3802I-B-K9	0081.c4a0.7560	Flex	Disabled	Registered
✓ ap1-3700	AIR-CAP3702I-A-K9	80e0.1d7b.8610	Flex	Enabled	Registered

Tag APs

Tags

Policy: branch-policy

Site: site_tag

RF: default-rf-tag

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

Cancel Save & Apply to Device

Start

Tags & Profiles

- WLAN Profile
- Policy Profile
- Policy Tag
- AP Join Profile
- Flex Profile
- Site Tag
- RF Profile
- RF Tag

Using a static mapping to tag the AP's.

Manage Tags

Policy Site RF **AP**

Tag Source Static Filter

Priority	Tag Source	Status
0	Static	<input checked="" type="checkbox"/>
1	Location	<input checked="" type="checkbox"/>
2	Filter	<input checked="" type="checkbox"/>
3	AP	<input checked="" type="checkbox"/>

ⓘ Drag and Drop Tag Sources to change priorities

Revalidate Tag Sources on APs

Apply

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

Manage Tags

Policy Site RF **AP**

Tag Source **Static** Filter

+ Add

AP MAC Address	Policy Tag Name	Site Tag Name
----------------	-----------------	---------------

10 items per page

Associate Tags to AP

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

Cancel **Save & Apply to Device**

Manage Tags

Policy Site RF **AP**

Tag Source **Static** Filter

+ Add *** Delete**

AP MAC Address	Policy Tag Name	Site Tag Name	RF Tag Name
<input type="checkbox"/> 1122.3344.5566	branch-policy	site_tag	default-rf-tag

1 - 1 of

Using a Filter to tag the AP

Search Menu Items

- Dashboard
- Monitoring
- Configuration
- Administration
- Troubleshooting

Manage Tags

Policy Site RF **AP**

Tag Source Static **Filter**

+ Add *** Delete**

Priority	Rule Name	AP name regex	Policy Tag Name	Site Tag Name	RF Tag Name
0					

No items to display

Associate Tags to AP

Rule Name*

AP name regex

Active YES

Priority*

Policy Tag Name

Site Tag Name

RF Tag Name

Manage Tags

Policy Site RF **AP**

Tag Source Static **Filter**

+ Add *** Delete**

Priority	Rule Name	AP name regex	Policy Tag Name	Site Tag Name	RF Tag Name
<input type="checkbox"/> 1	rule_1	ap*	branch-policy	site_tag	default-rf-tag

1 -

The Access point summary page show the source based on which the tags was 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 flex connect mode.

The assigning of 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 dynamic VLAN assignment, AP would have the VLAN pre-created based on a configuration using the flex profile mapped to the site tag. The VLAN's used in the flex profile is 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 AAA override are not present on AP, client will be excluded and not allowed access to the network.
- Multicast traffic on a AAA overridden VLAN is not supported

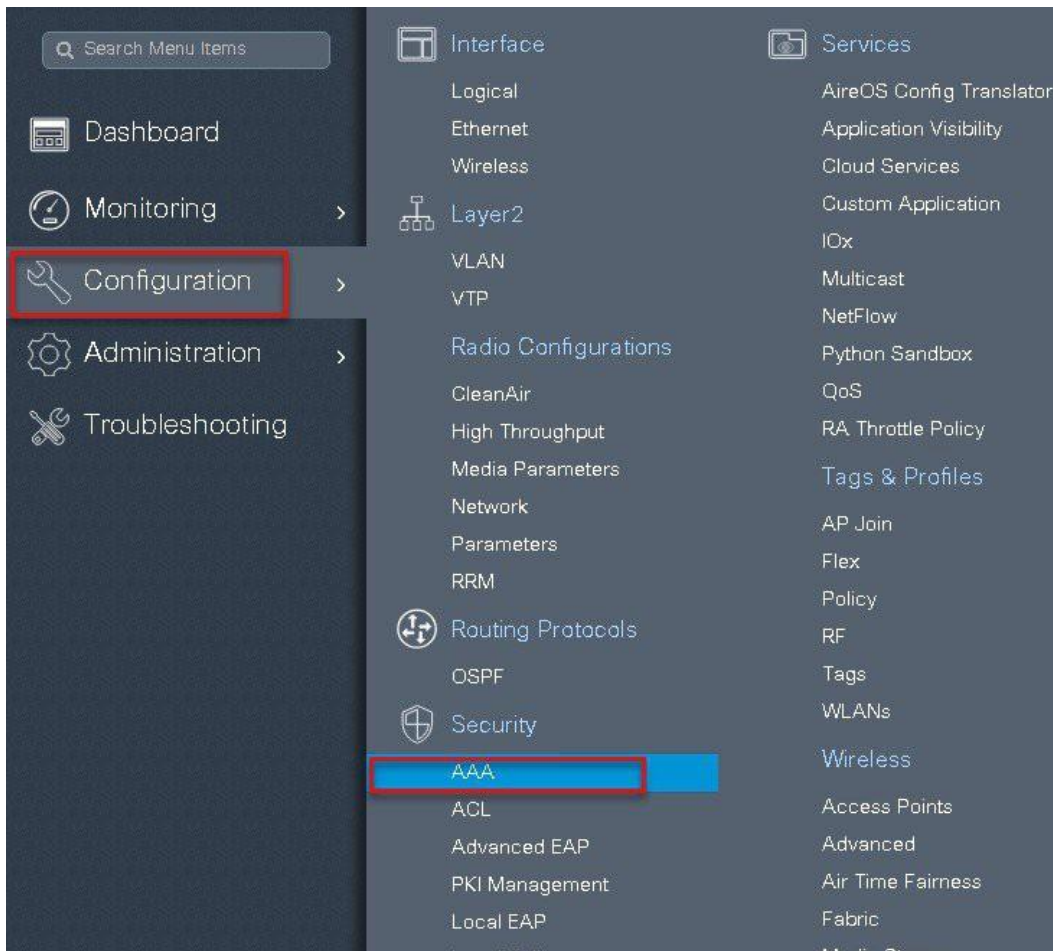
Procedure to Enable VLAN

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

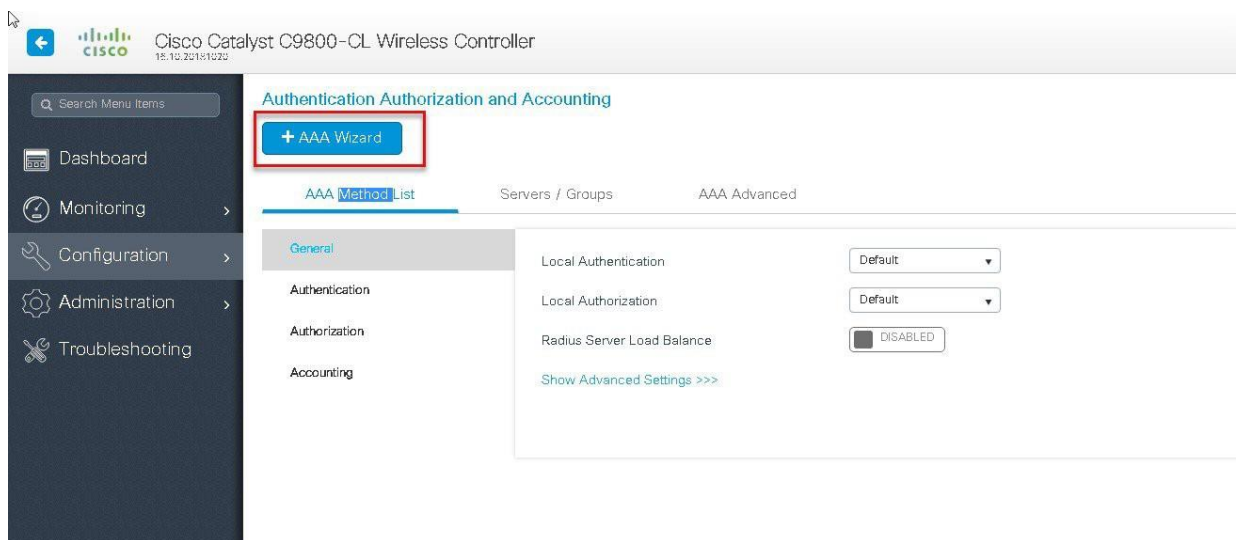
Procedure

Step 1 Define a 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



Step2 Use the AAA wizard to create the server and server groups.



Step3 Define a name for the server and specify the IP address and shared secret.

Add Wizard Basic Advanced

SERVER
SERVER GROUP ASSOCIATION
MAP AAA

RADIUS
 TACACS+
 LDAP

RADIUS

Name*

IPv4 / IPv6 Server Address*

PAC Key

Key*

Confirm Key*

Step4 Create a server group and map the server in the group.

Add Wizard Basic Advanced

SERVER
SERVER GROUP ASSOCIATION
MAP AAA

RADIUS

Name*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Available Servers

freerad	<input type="button" value=">"/> <input type="button" value="<"/>	Assigned Servers
ISE-2		ISE
ISE		


Step5 Enable dot1x system control and check mark 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 

Local Authentication ▼

Local Authorization ▼

Radius Server Load Balance

[Show Advanced Settings >>>](#)

← Previous Save & Apply to Device

Step6 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*

Type* ▼

Group Type ▼

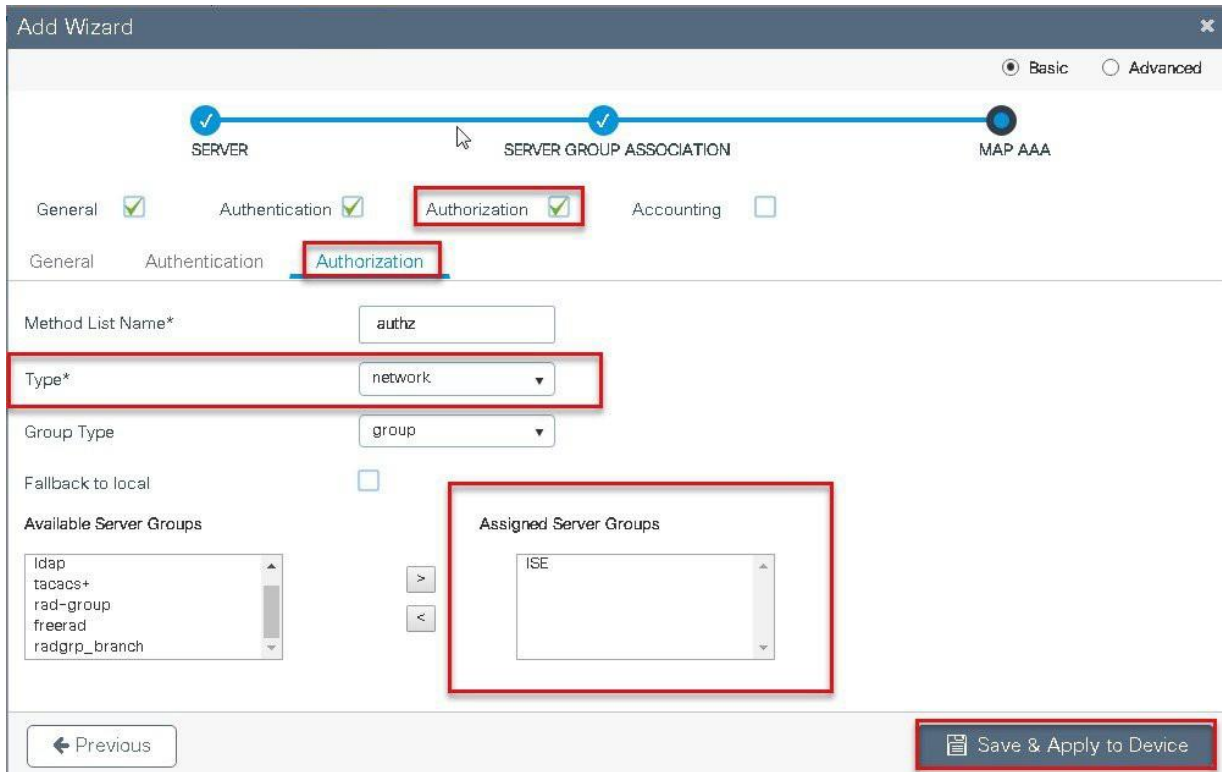
Fallback to local

Available Server Groups

ldap tacacs+ rad-group freerad radgrp_branch	<input type="button" value=">"/> <input type="button" value="<"/>	Assigned Server Groups <input type="text" value="ISE"/>
--	---	---

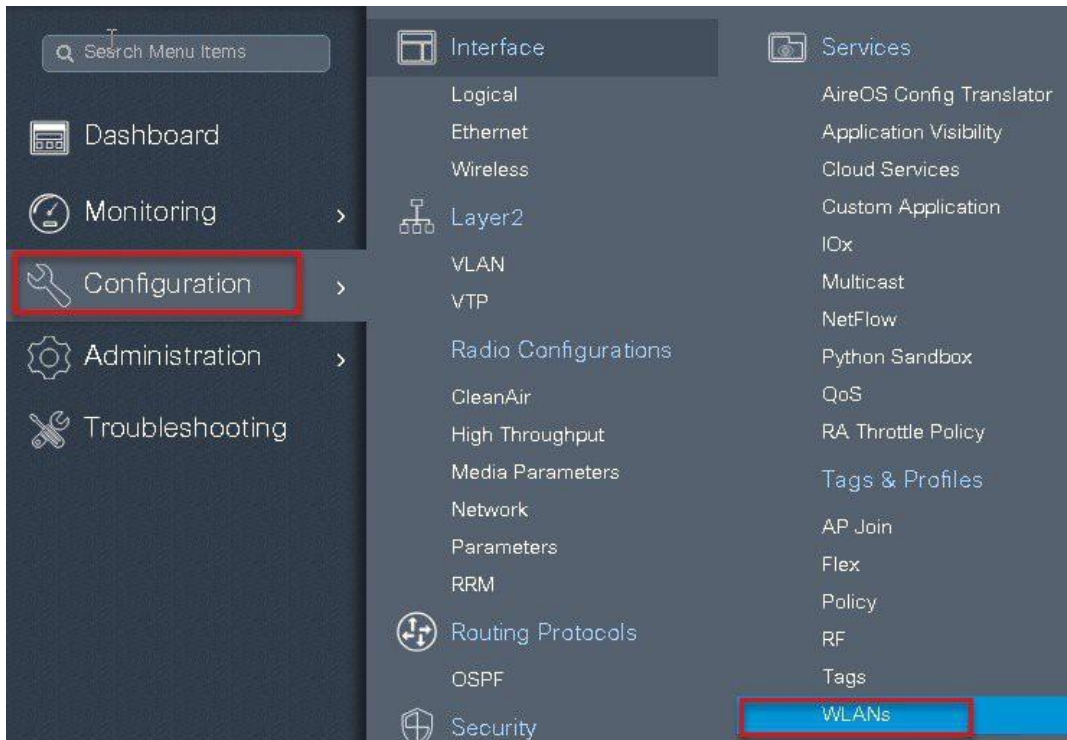
← Previous Save & Apply to Device

Step7 Define the method type as network and map the server group.



Step8 Create a Dot1x WLAN and map the method list on the WLAN.

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



WIRELESS NETWORKS

+ Add * Delete Enable WLAN Disable WLAN

Number of WLANs selected : 0

open_wlan

1 10

Add WLAN

General Security Advanced

Profile Name* dot1x_wlan Radio Policy All

SSID dot1x_wlan Broadcast SSID ENABLED

WLAN ID* 2

Status ENABLED

Cancel Save & Apply to Device

Add WLAN

General Security Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode WPA + WPA2

MAC Filtering

Protected Management Frame

PMF Disabled

WPA Parameters

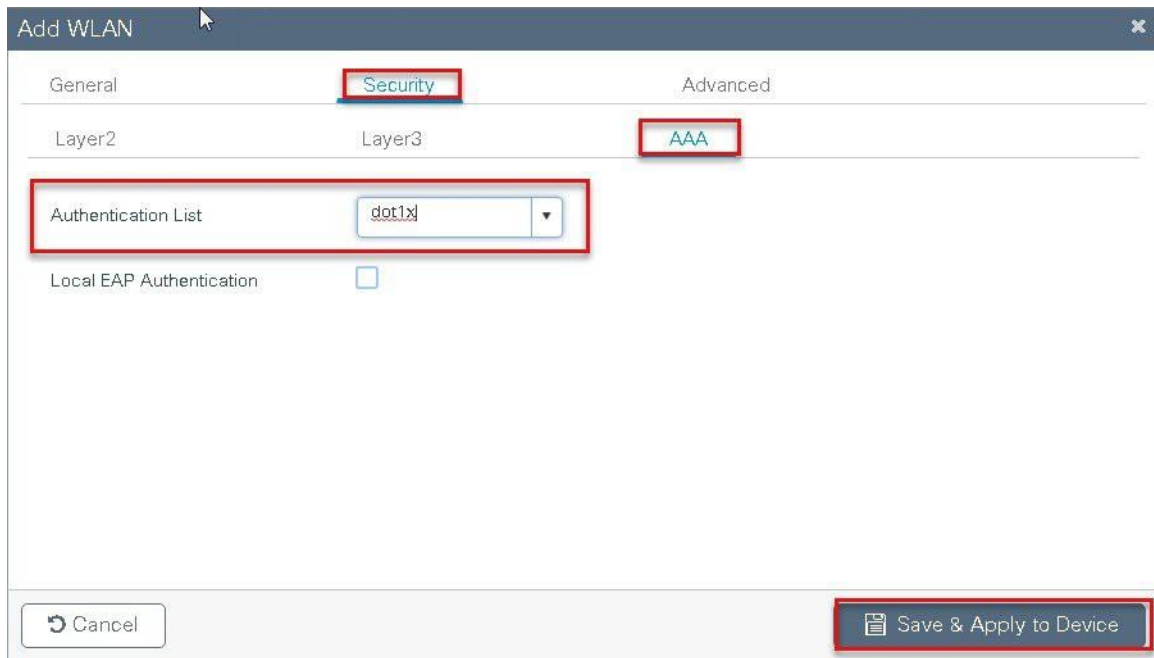
WPA Policy

Fast Transition Adaptive Enabled

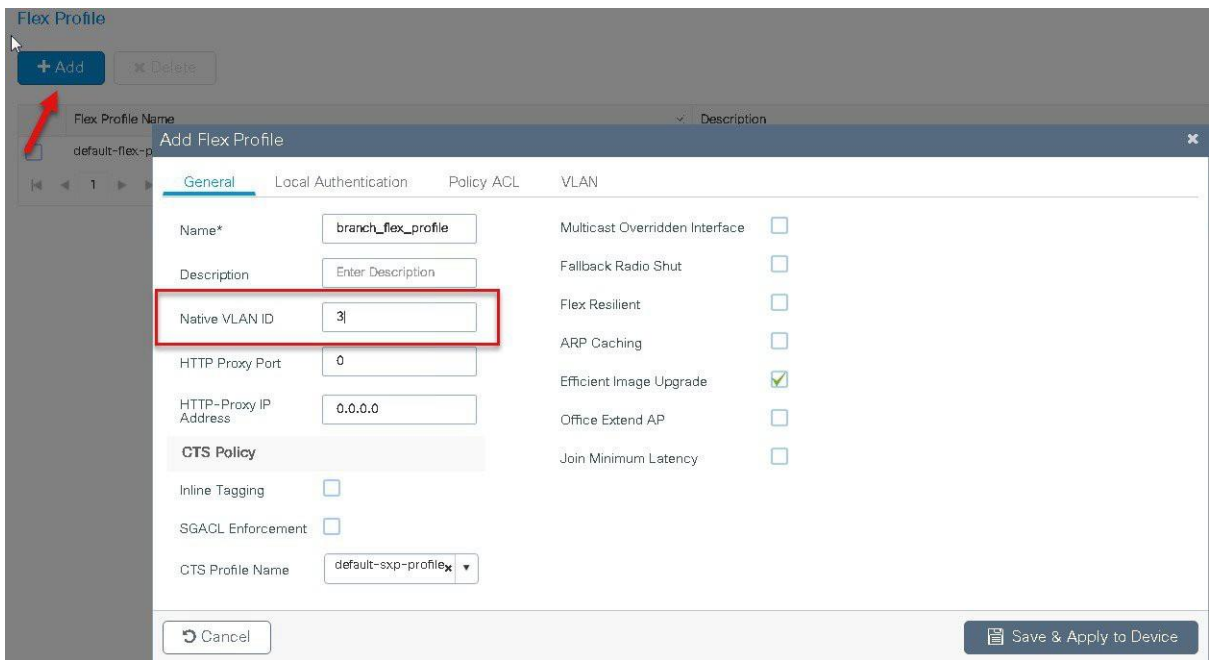
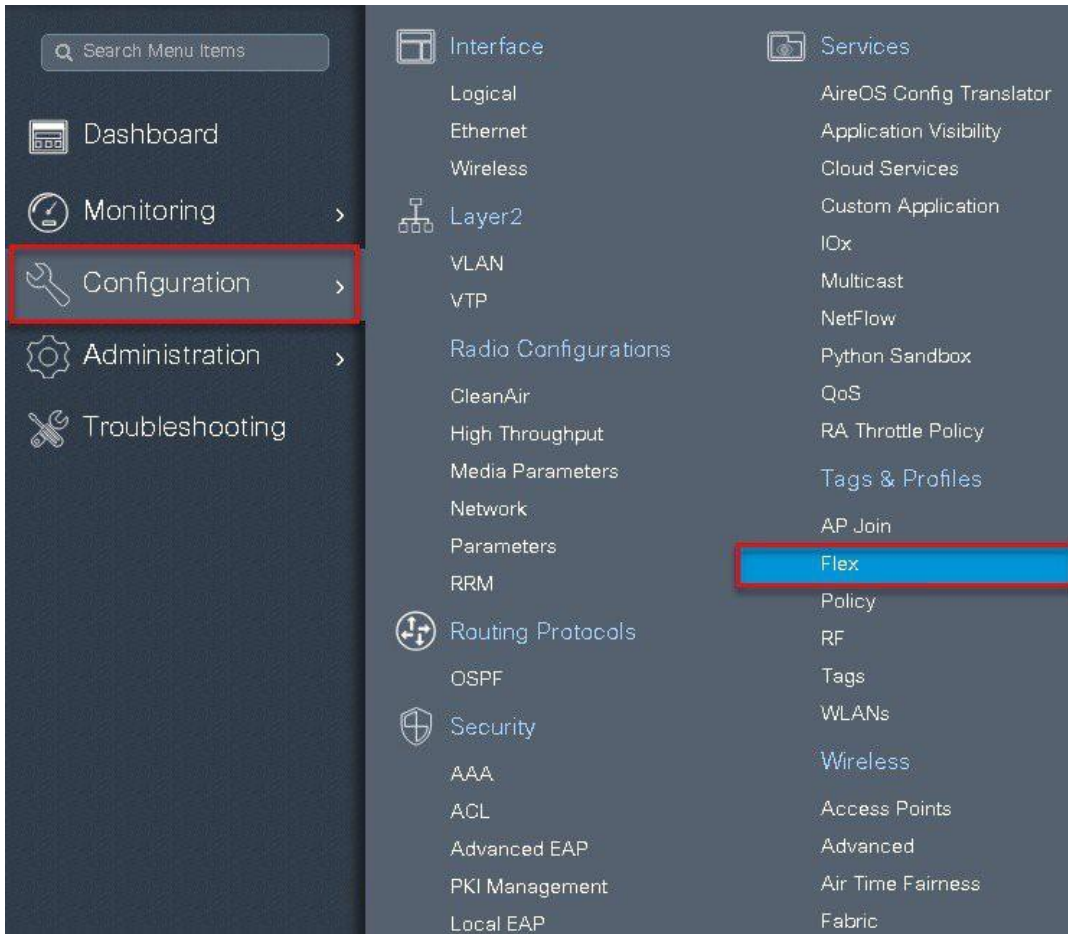
Over the DS

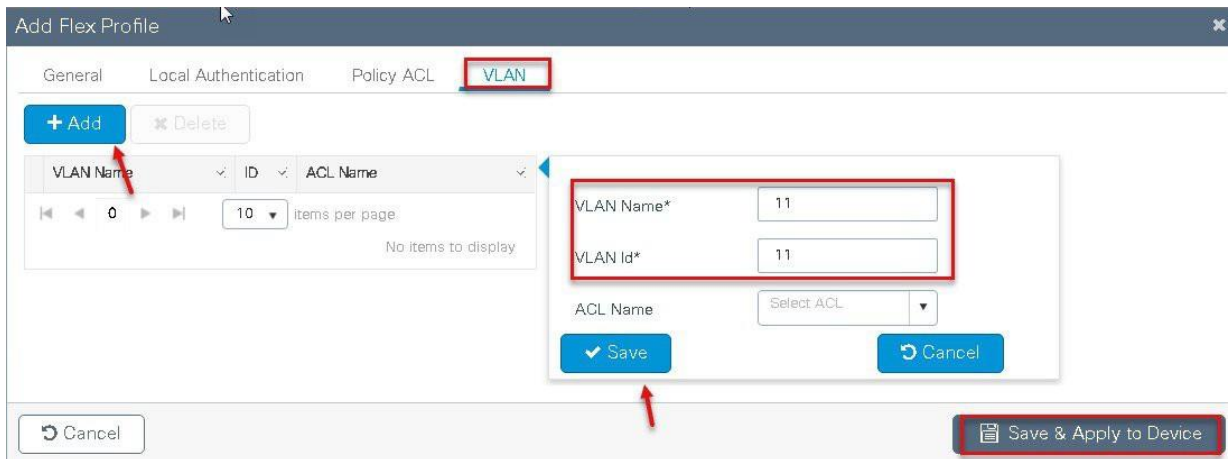
Reassociation Timeout 20

Cancel Save & Apply to Device

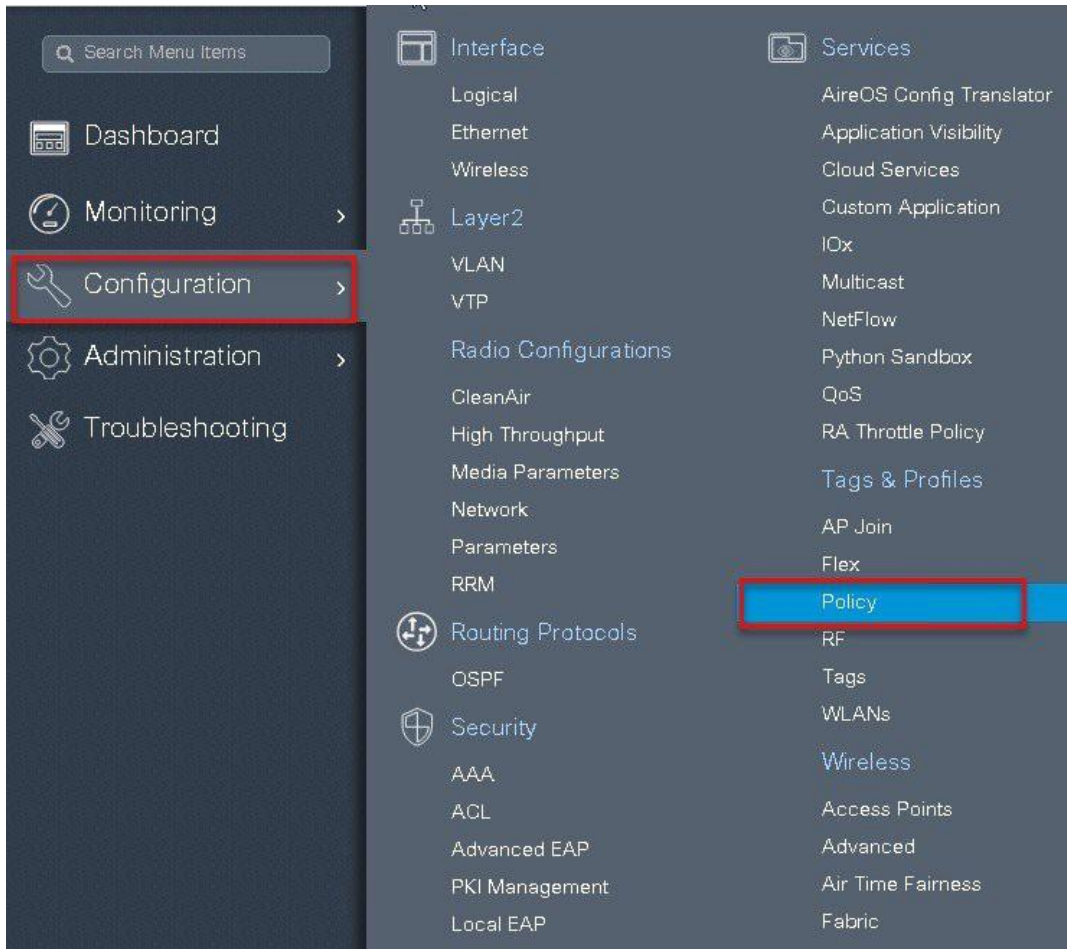


Step9 Create a flex profile, Create a Vlan on the Flex profile which is the VLAN returned by the AAA.





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



Policy Profile

+ Add *** Delete**

Policy Profile Name

- open_wlan
- default-policy-profile

1 10

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*

Description

Status **ENABLED**

Passive Client DISABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

WLAN Switching Policy

Central Switching

Central Authentication

Central DHCP

Central Association

Flex NAT/PAT

Cancel **Save & Apply to Device**

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

VLAN

VLAN/VLAN Group

Multicast VLAN

WLAN ACL

IPv4 ACL

IPv6 ACL

URL Filters

Pre Auth

Post Auth

Cancel **Save & Apply to Device**

Add Policy Profile

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

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

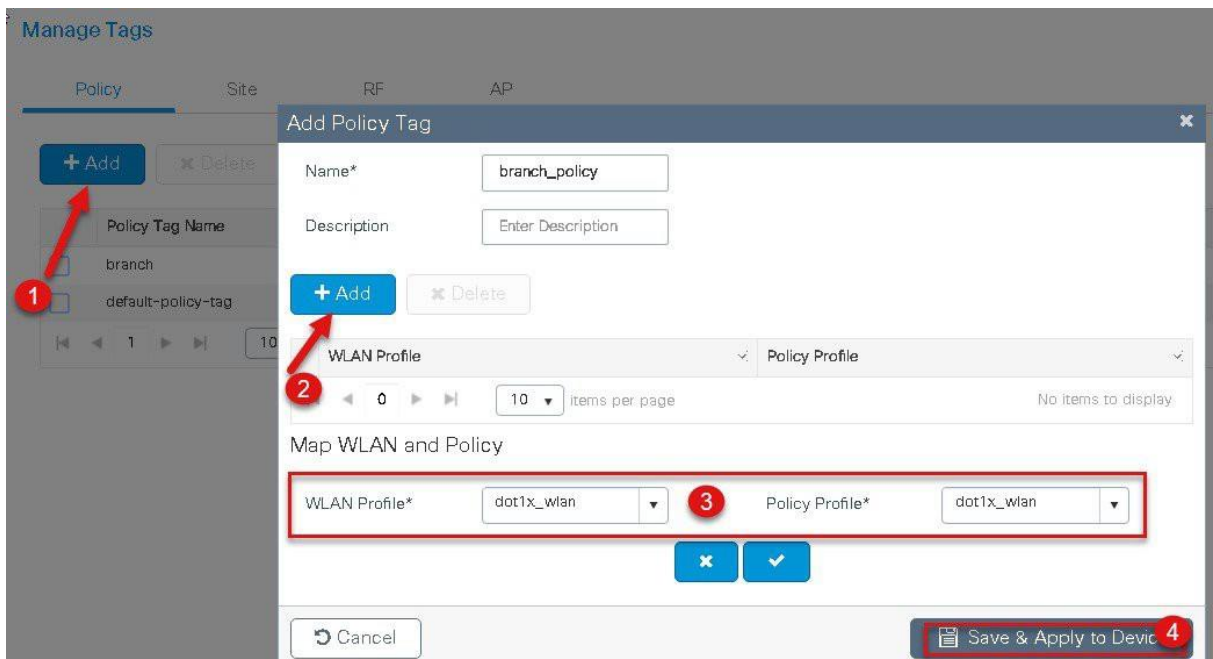
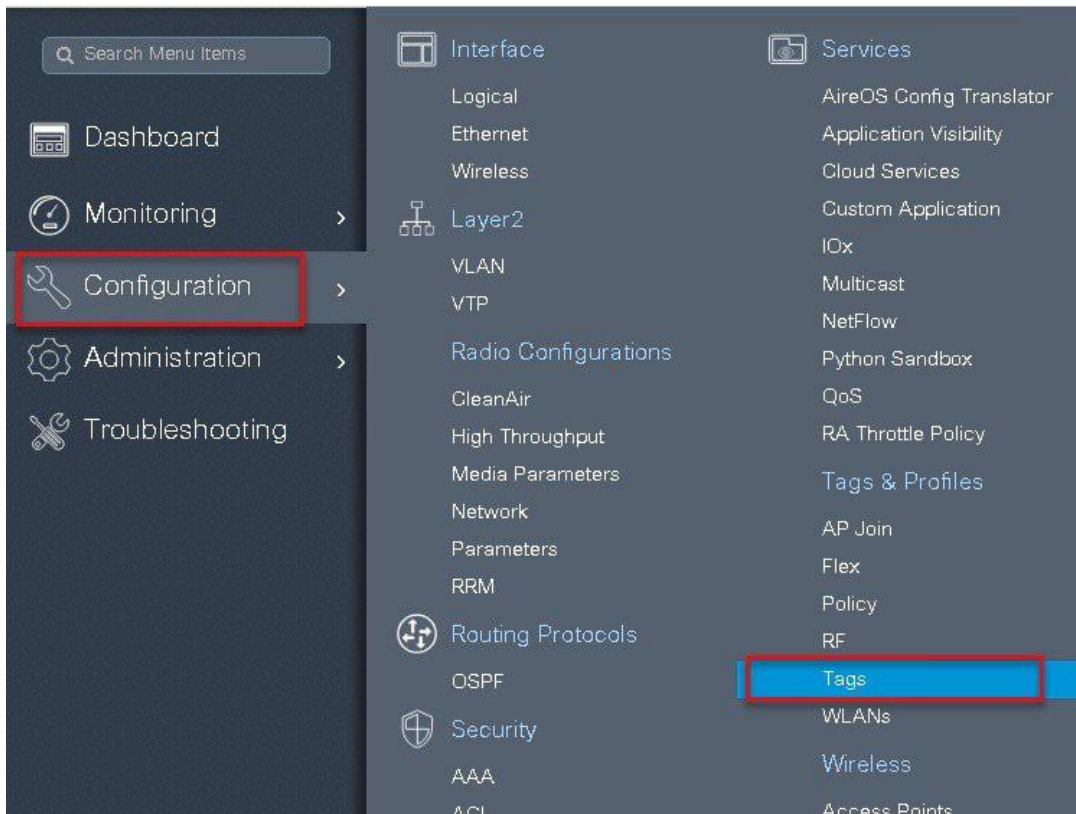
Split MAC ACL Search or Select

Air Time Fairness Policies

2.4 GHz Policy Search or Select

5 GHz Policy Search or Select

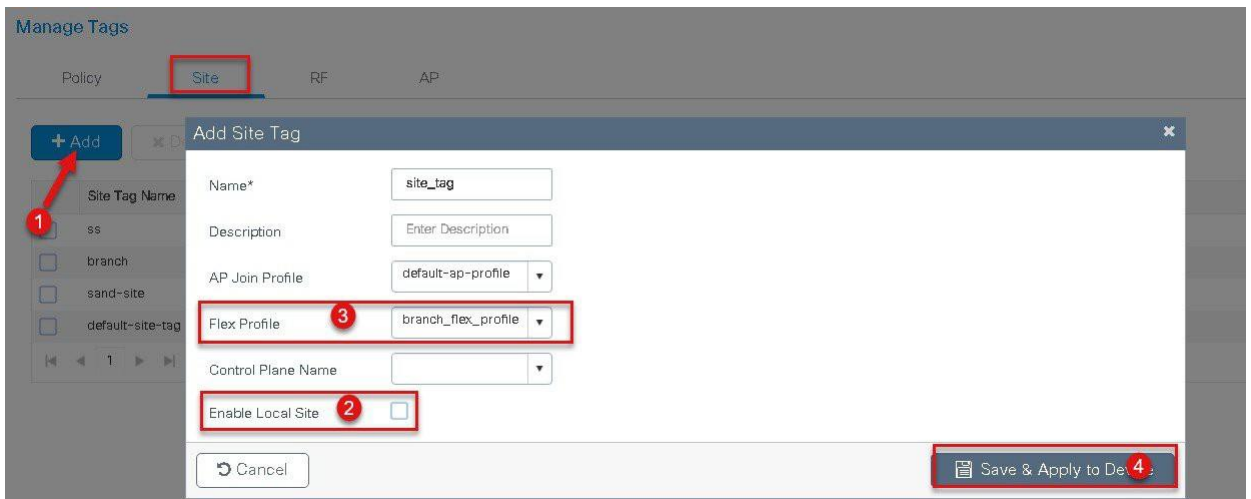
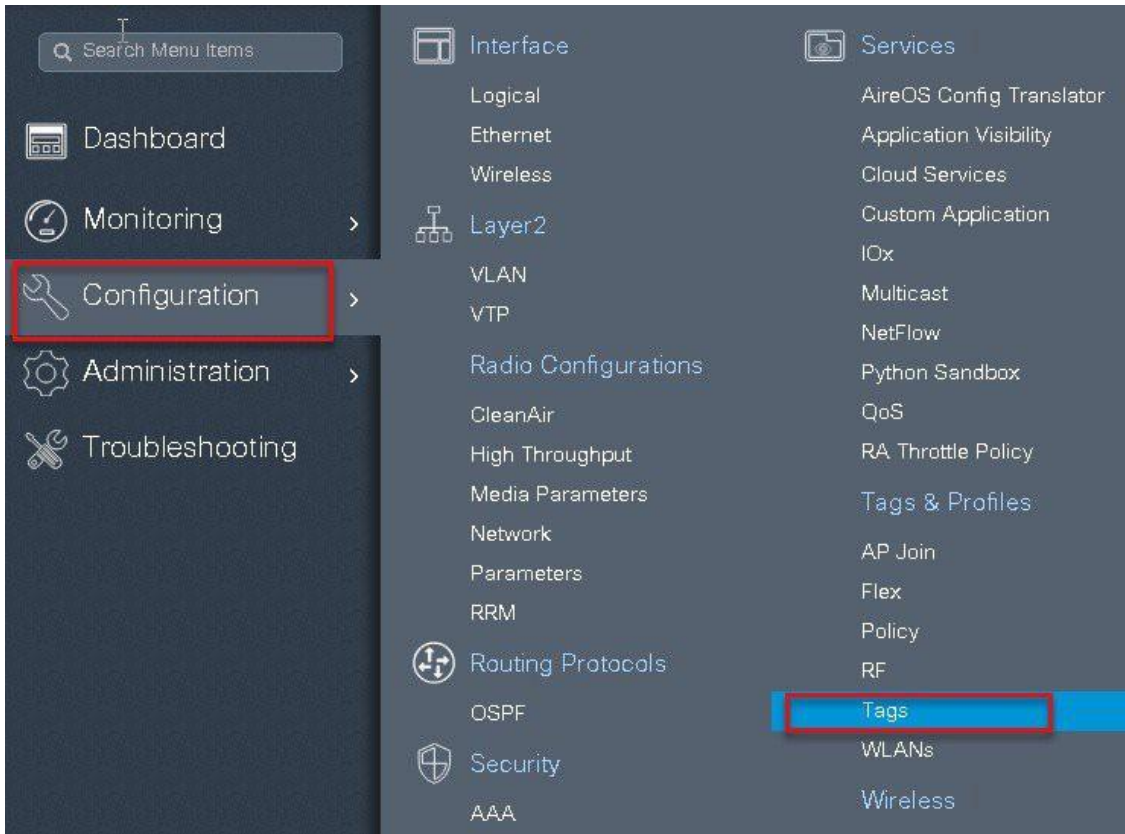
- Step 11** Map the WLAN to policy profile.
 Navigate to configurationTag and create a policy tag mapping the WLAN and policy profile.



- 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 the profile created.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation at the top reads: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The left sidebar contains a tree view with categories: Authentication, Authorization, Profiling, Posture, and Client Provisioning. The main content area is titled 'Authorization Profiles > sand-vlan' and 'Authorization Profile'. It includes fields for Name (sand-vlan), Description, Access Type (ACCESS_ACCEPT), and Network Device Profile (Cisco). There are checkboxes for Service Template, Track Movement, and Passive Identity Tracking. Under the 'Common Tasks' section, the 'VLAN' checkbox is checked, with 'Tag ID 1' and 'IDName 11' displayed. Below this is the 'Advanced Attributes Settings' section with a dropdown menu. The 'Attributes Details' section at the bottom shows the following values: Access Type = ACCESS_ACCEPT, Tunnel-Private-Group-ID = 1:11, Tunnel-Type = 1:13, and Tunnel-Medium-Type = 1:6. At the bottom of the page are 'Save' and 'Reset' buttons.

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



Step 14 Map the policy site tag and RF tag on the AP using the advanced config wizard .
 Navigate to Configuration wireless setup Advanced

Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Troubleshooting

Interface

- Logical
- Ethernet
- Wireless
- Layer2
- VLAN
- VTP
- Radio Configurations
- CleanAir
- High Throughput
- Media Parameters
- Network
- Parameters
- RRM
- Routing Protocols
- OSPF
- Security
- AAA
- ACL
- Advanced EAP
- PKI Management
- Local EAP
- Local Policy
- TrustSec
- Threat Defense
- URL Filters
- Web Auth
- Wireless AAA Policy
- Wireless Protection Policies

Services

- AireOS Config Translator
- Application Visibility
- Cloud Services
- Custom Application
- IOx
- Multicast
- NetFlow
- Python Sandbox
- QoS
- RA Throttle Policy
- Tags & Profiles
- AP Join
- Flex
- Policy
- RF
- Tags
- WLANs
- Wireless
- Access Points
- Advanced
- Air Time Fairness
- Fabric
- Media Stream
- Mesh
- Mobility
- Wireless Setup
- Basic
- 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.

DESIGN PHASE

Tags & Profiles

- WLAN Policy (Mandatory)
- Site Policy (Optional)
- Radio Policy (Optional)

WLAN Profile | AP Join Profile | RF Profile

Policy Profile | Flex Profile | RF Tag

Policy Tag | Site Tag

DEPLOY PHASE

Apply to APs (Mandatory)

Tag APs

Select APs and push configuration to them

TERMINOLOGY

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

ACTIONS

Go to List View
Create New

Start Now

Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Troubleshooting

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.

DESIGN PHASE

Tags & Profiles

- WLAN Policy (Mandatory)
- Site Policy (Optional)
- Radio Policy (Optional)

WLAN Profile | AP Join Profile | RF Profile

Policy Profile | Flex Profile | RF Tag

Policy Tag | Site Tag

DEPLOY PHASE

Apply to APs (Mandatory)

Tag APs

Select APs and push configuration to them

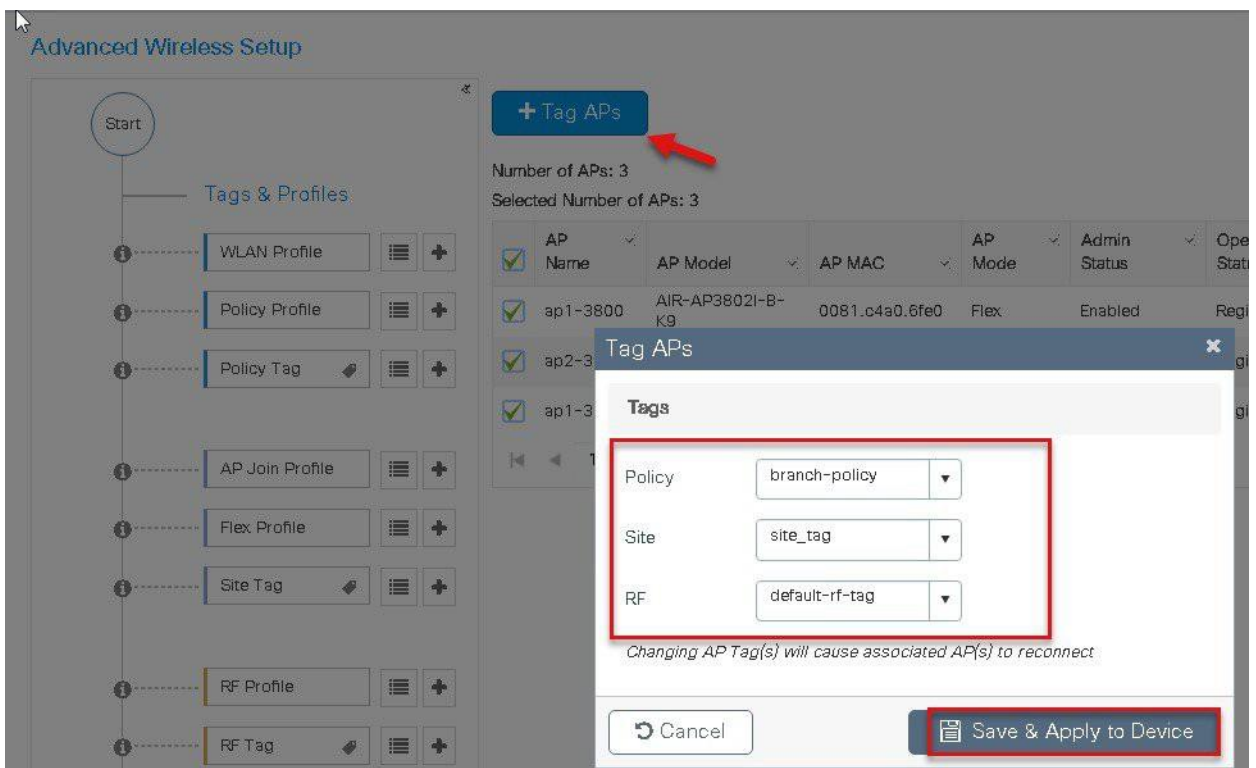
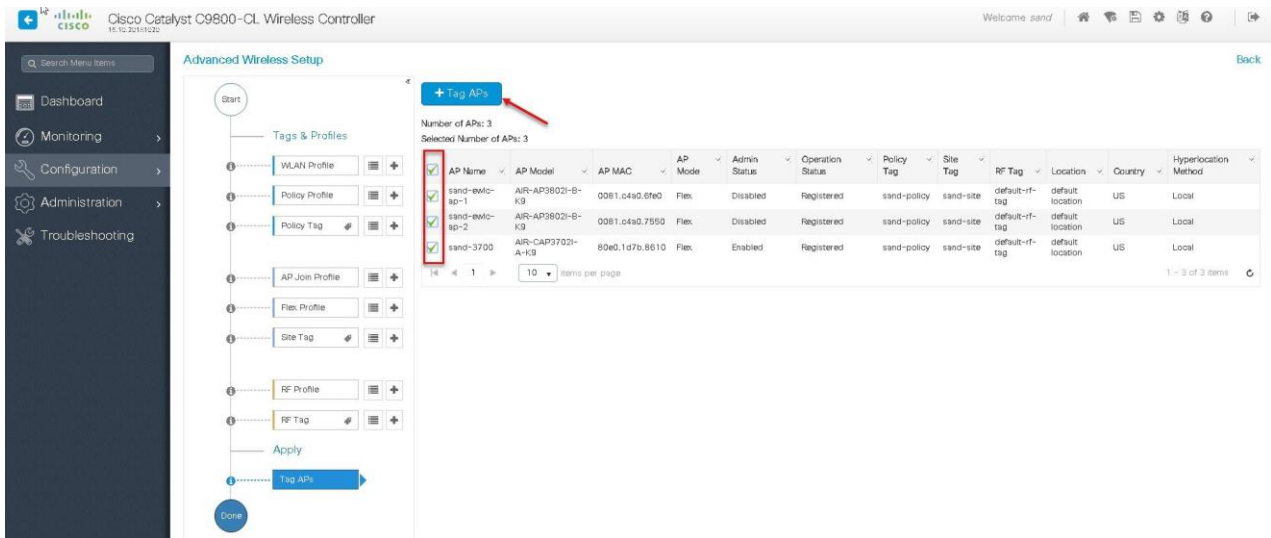
TERMINOLOGY

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

ACTIONS

Go to List View
Create New





Step 15

Associate a client on the WLAN and authenticate using the user name 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 the client is mapped to

Double click on the client mac to open up the details of the Client session

Cisco Catalyst C9800-CL Wireless Controller

Welcome sand

Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Troubleshooting

Clients

Client Properties

Client MAC Address: 1c36.bbef.6492

IPv4/Pv6 Address: 9.1.11.252

AP Name: ap-1-3800

WLAN: 10

State: Run

Protocol: 11ac

User Name: sand-wireless

Device Type: Local

Role: Local

1 - 1 of 1 clients

Clients

Client Properties

Client MAC Address: 1c36.bbef.6492

IPv4/Pv6 Address: 9.1.11.252

AP Name: ap-1-3800

10 items per page

click on the client mac to open up details page

Client

General

Client Properties

AP Properties

Security Information

Client Statistics

QOS Properties

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

COX version: No COX 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

Client

General QOS Statistics ATF Statistics Mobility History Call Statistics

Client Properties AP Properties Security Information Client Statistics QOS Properties

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 VLAN failure.
- If the VLAN is returned as one of the AAA attributes and that VLAN is present in the Flex Connect 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.

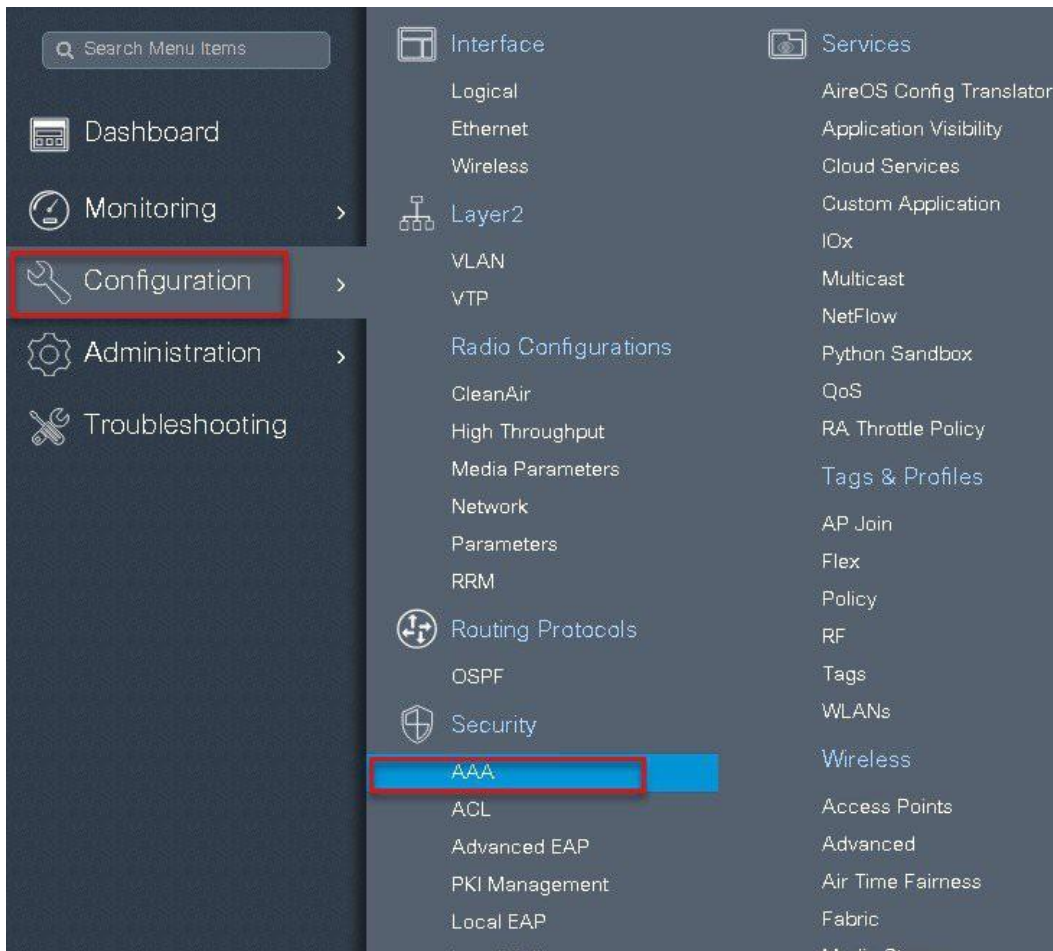
Traffic flow on WLANs configured for Local Switching when Flex APs are in Standalone Mode:

- 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.

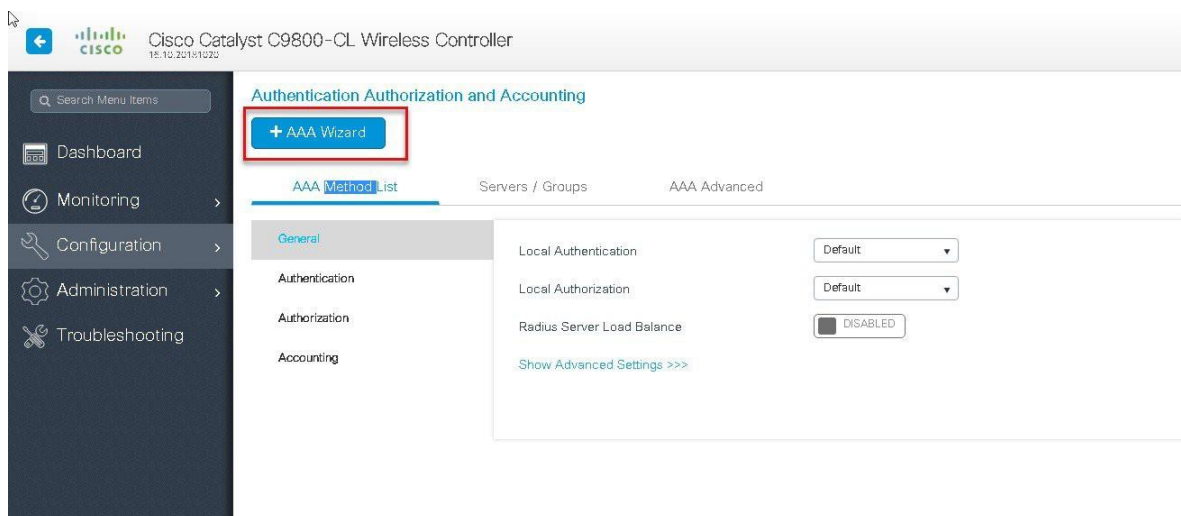
Steps to configure FlexConnect VLAN Based Central Switching

Procedure

-
- Step 1** Define a 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.



Step2 Use the AAA wizard to create the server and server groups.



Step3 Define a name for the server and specify the IP address and shared secret.

Add Wizard ✕

● Basic ○ Advanced

● SERVER
● SERVER GROUP ASSOCIATION
● MAP AAA

RADIUS
 TACACS+
 LDAP

RADIUS

Name*

IPv4 / IPv6 Server Address*

PAC Key

Key*

Confirm Key*

Step4 Create a server group and map the server in the group.

Add Wizard ✕

● Basic ○ Advanced

✓ SERVER
● SERVER GROUP ASSOCIATION
● MAP AAA

RADIUS

Name*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Available Servers

freerad	<input type="button" value=">"/> <input type="button" value="<"/>	Assigned Servers
ISE-2		ISE
ISE		


Step5 Enable dot1x system control and check mark 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

Local Authorization

Radius Server Load Balance **DISABLED**

[Show Advanced Settings >>>](#)

← Previous Save & Apply to Device

Step6 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*

Type*

Group Type

Fallback to local

Available Server Groups

ldap tacacs+ rad-group freerad radgrp_branch	<input type="button" value=">"/> <input type="button" value="<"/>	Assigned Server Groups <input type="text" value="ISE"/>
--	--	---

← Previous Save & Apply to Device

Step7 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*

Type*

Group Type

Fallback to local

Available Server Groups

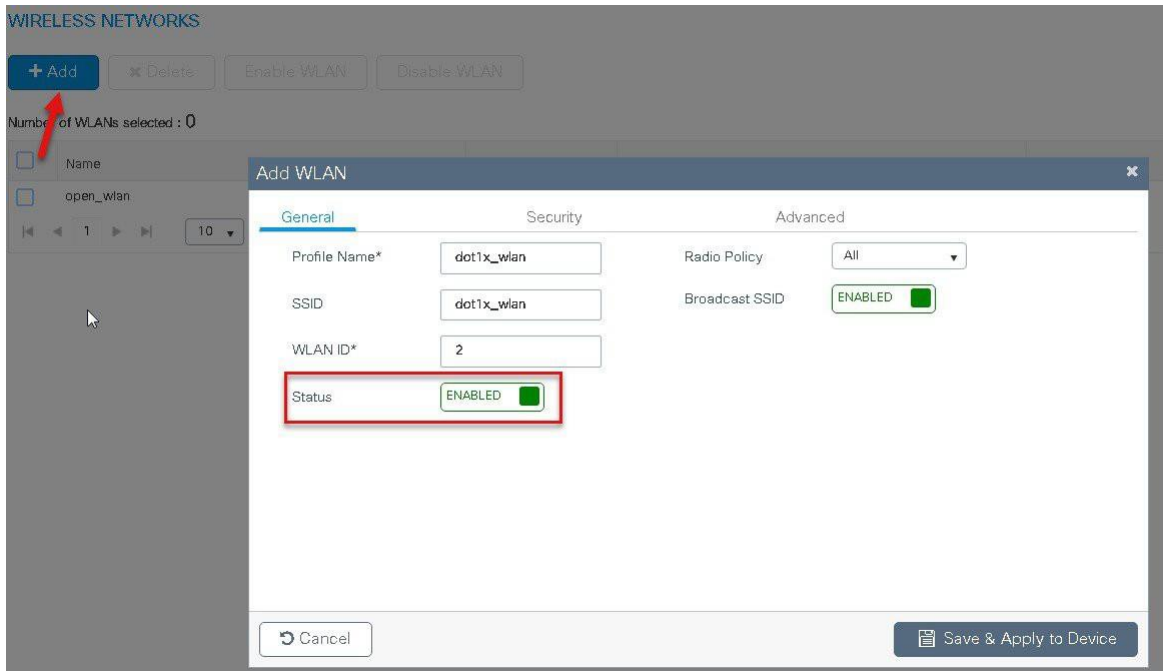
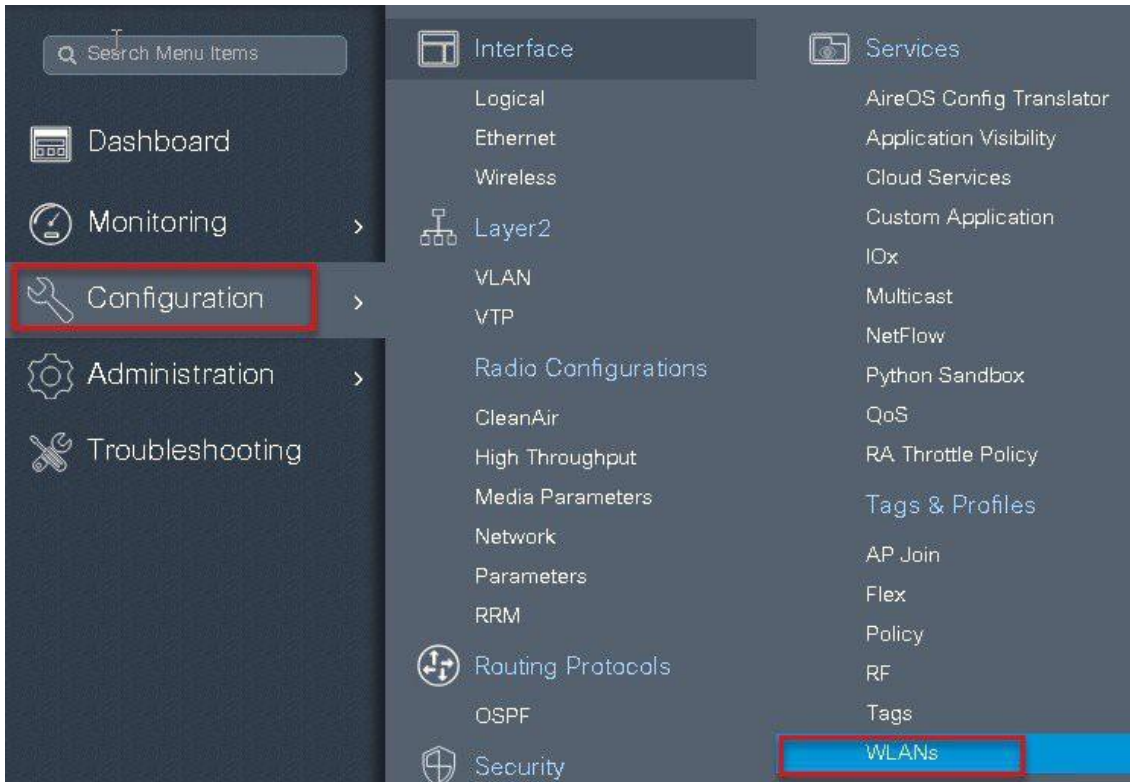
- ldap
- tacacs+
- rad-group
- freerad
- radgrp_branch

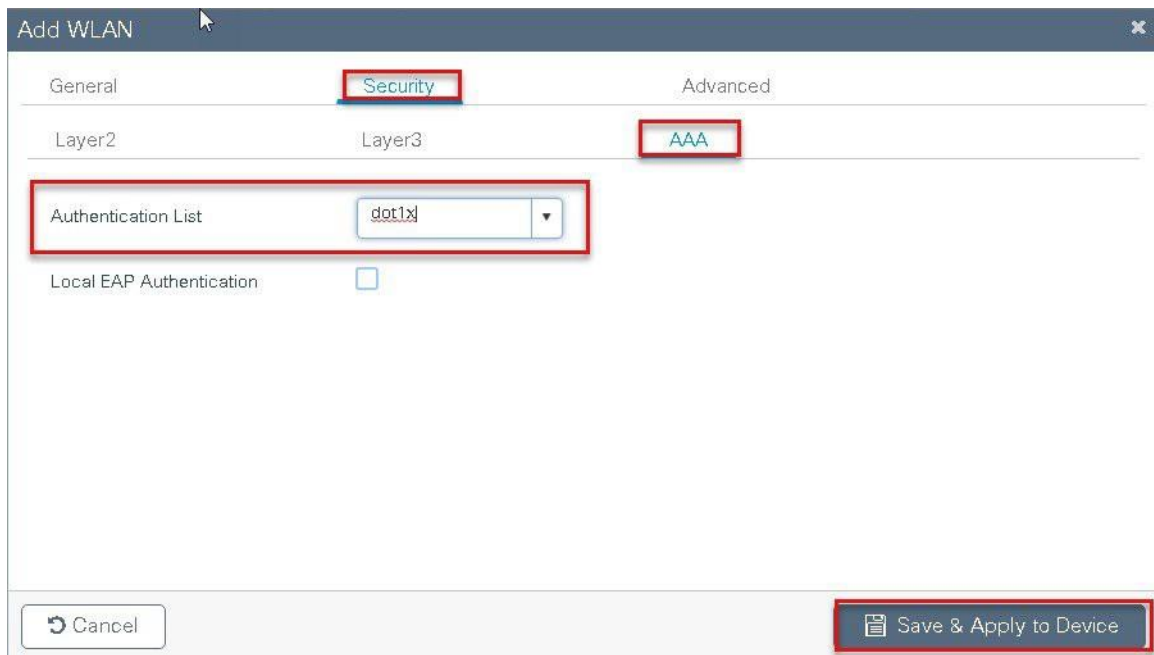
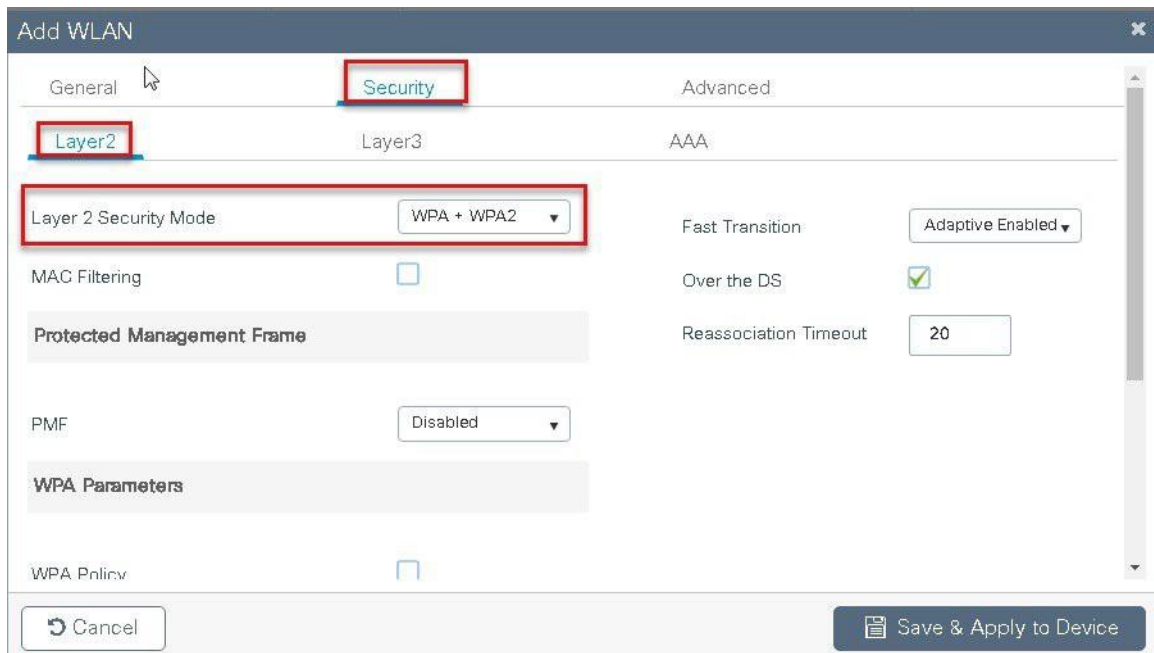
> <

Assigned Server Groups

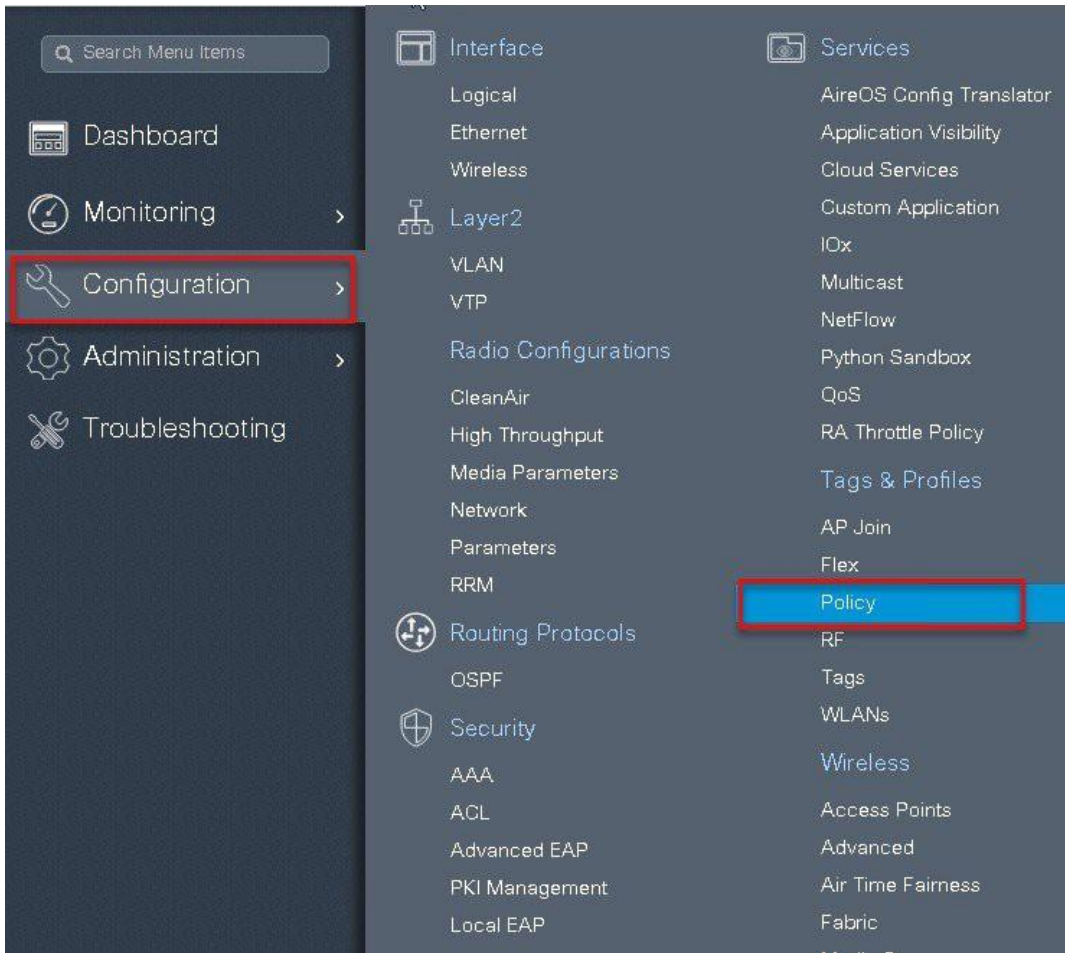
- ISE

Step 8 Create a Dot1x WLAN and map the method list on the WLAN.
 To create an SSID navigate to Configuration > Tags & Profiles > WLANs.
 s





Step9 Create a policy profile enable local switching and central authentication on the profile also map the default vlan for the WLAN and enable AAA override .



Policy Profile

+ Add *** Delete**

Policy Profile Name

- open_wlan
- default-policy-profile

1 10

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*

Description

Status **ENABLED** ■

Passive Client DISABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

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

VLAN

VLAN/VLAN Group

Multicast VLAN

WLAN ACL

- IPv4 ACL
- IPv6 ACL

URL Filters

- Pre Auth
- Post Auth

Add Policy Profile ✕

General
Access Policies
QOS and AVC
Mobility
Advanced

WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

DHCP

DHCP Enable

DHCP Server IP Address

[Show more >>>](#)

AAA Policy

Allow AAA Override

NAC State

Policy Name

Accounting List

Fabric Profile

Umbrella Parameter Map

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Air Time Fairness Policies

2.4 GHz Policy

5 GHz Policy

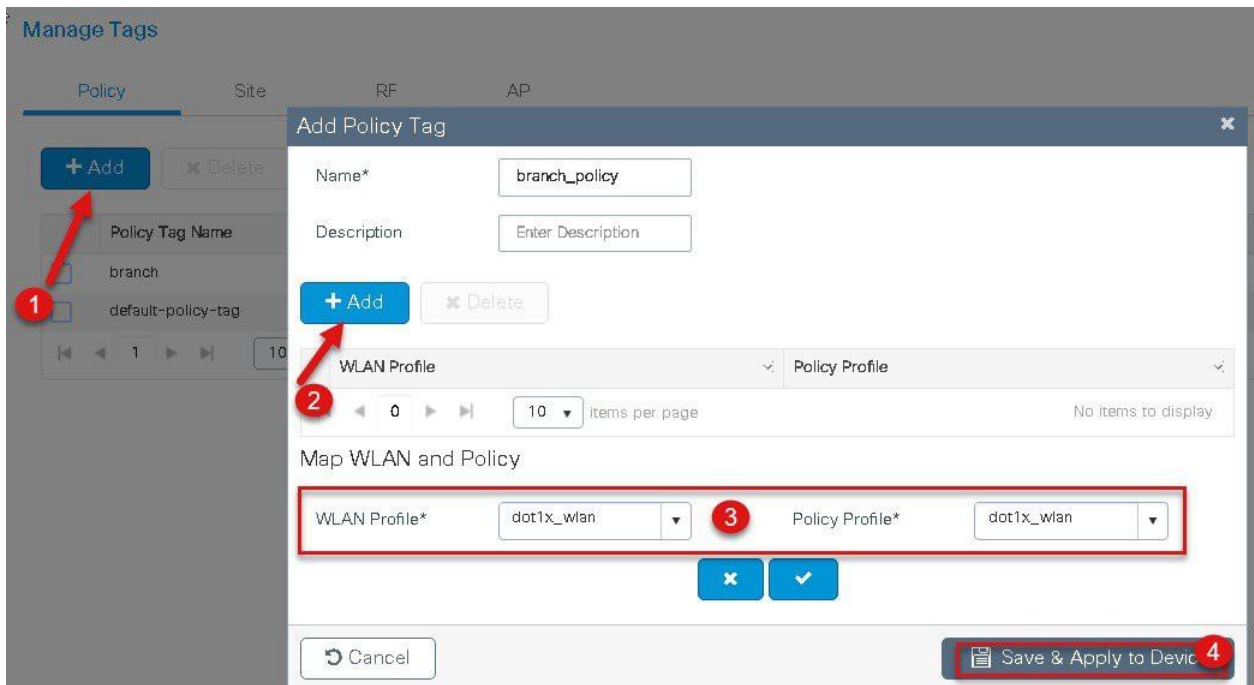
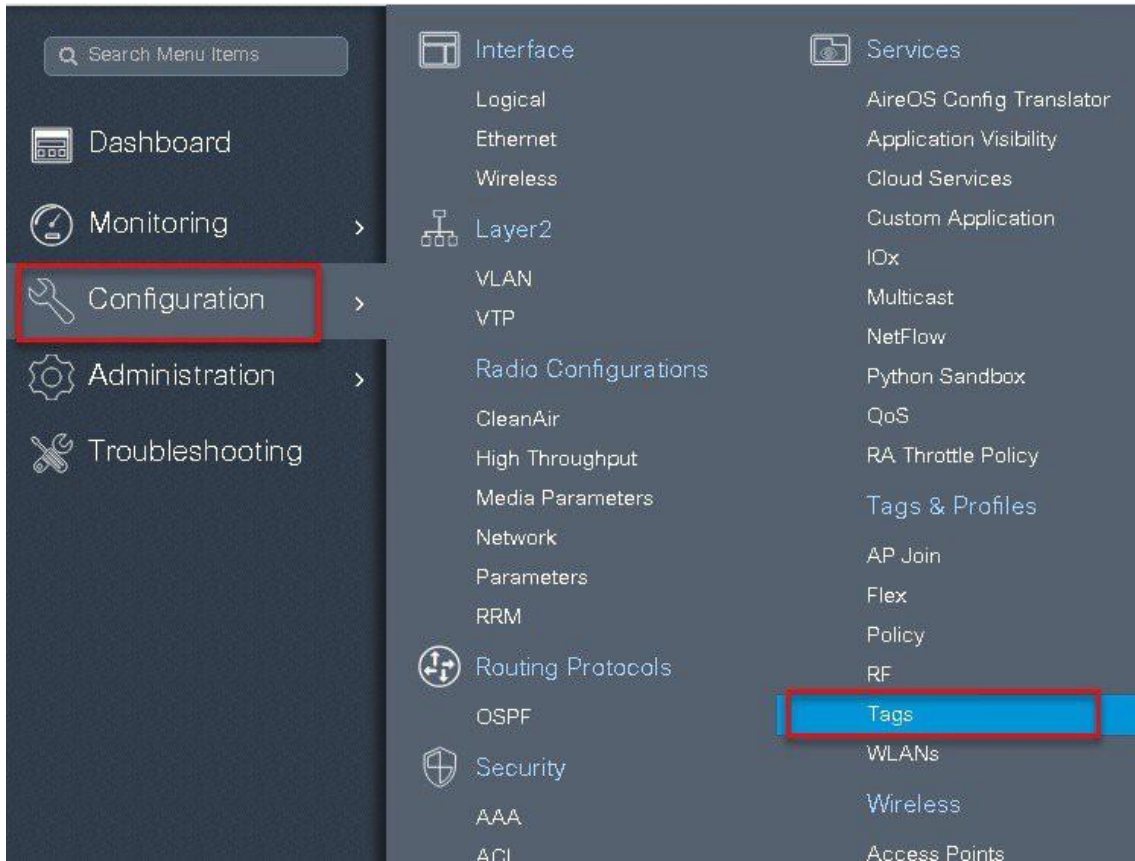
↶ Cancel

Save & Apply to Device

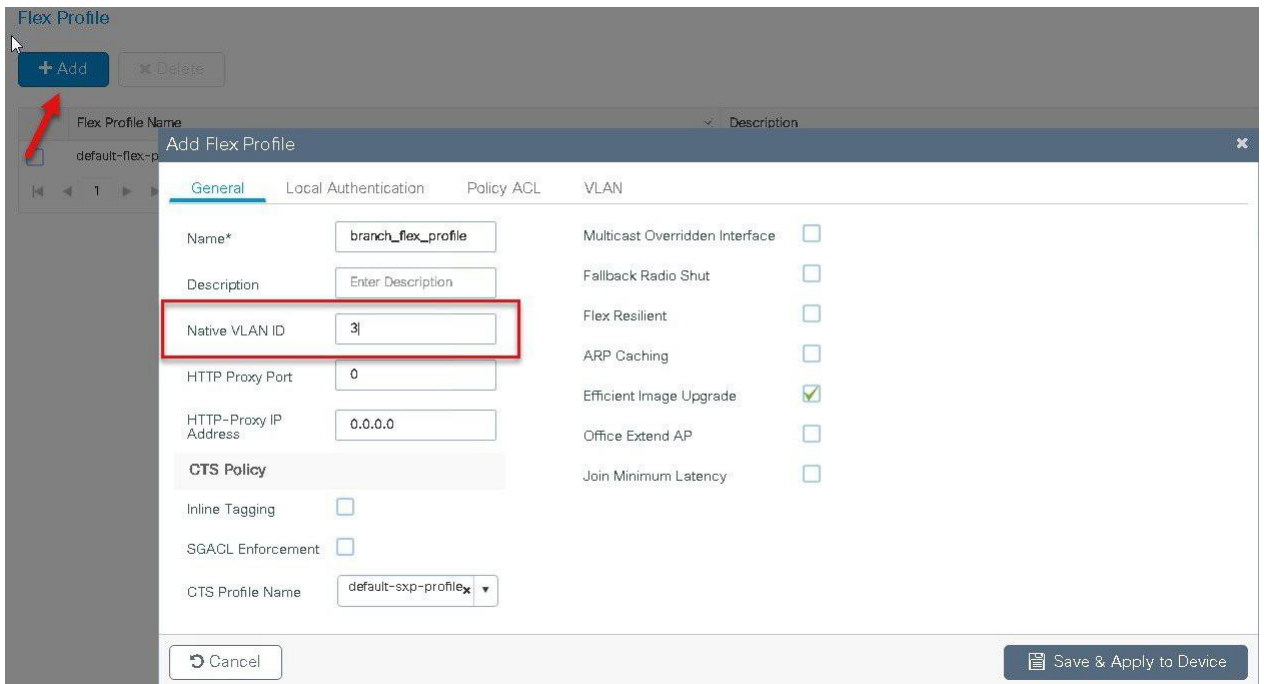
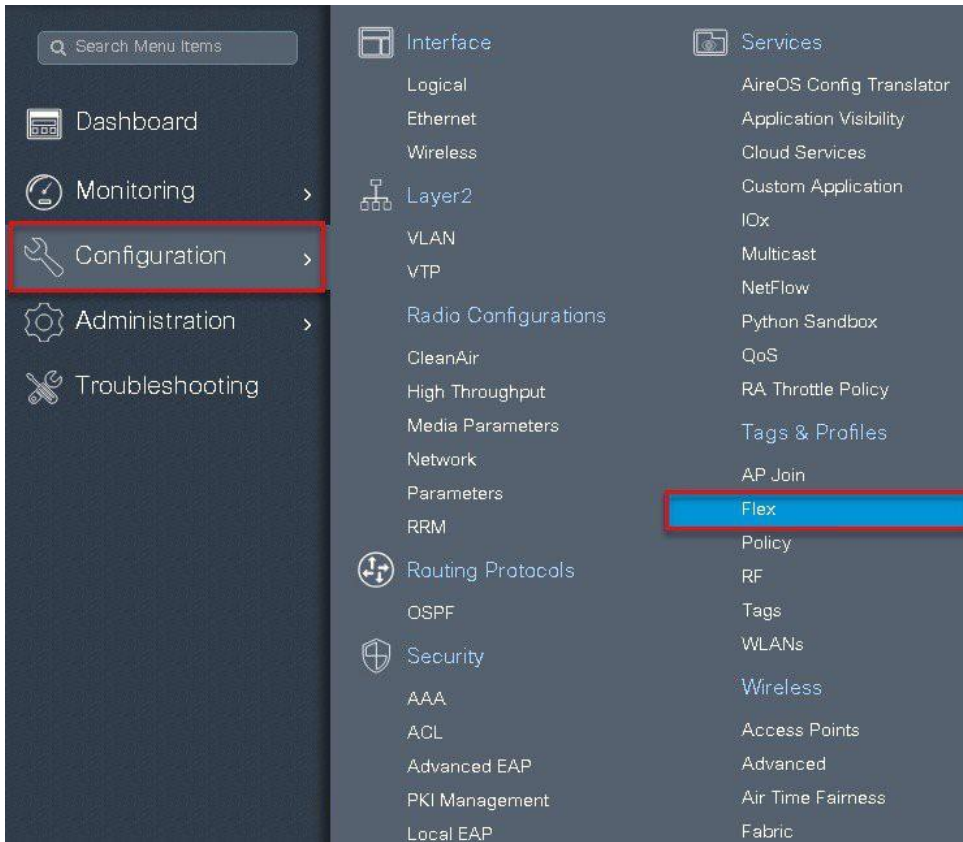
Step 10

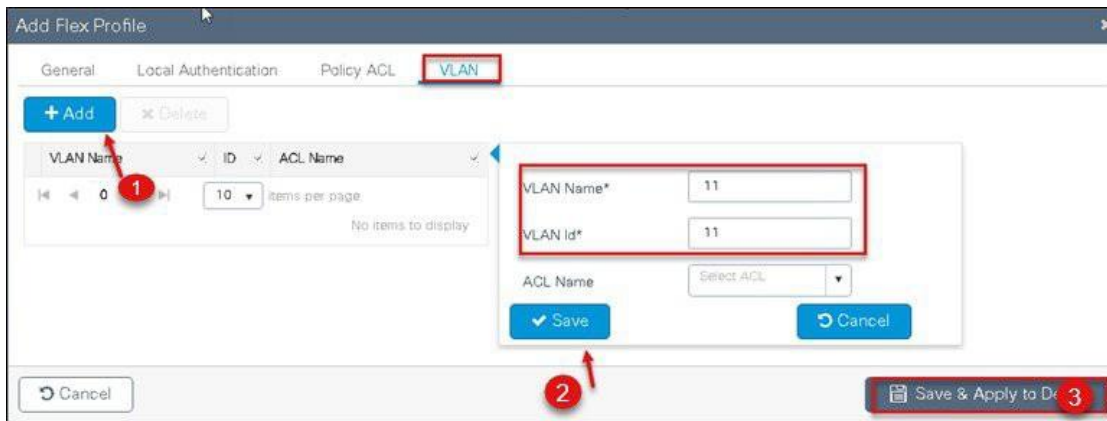
Map the WLAN to policy profile.

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



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



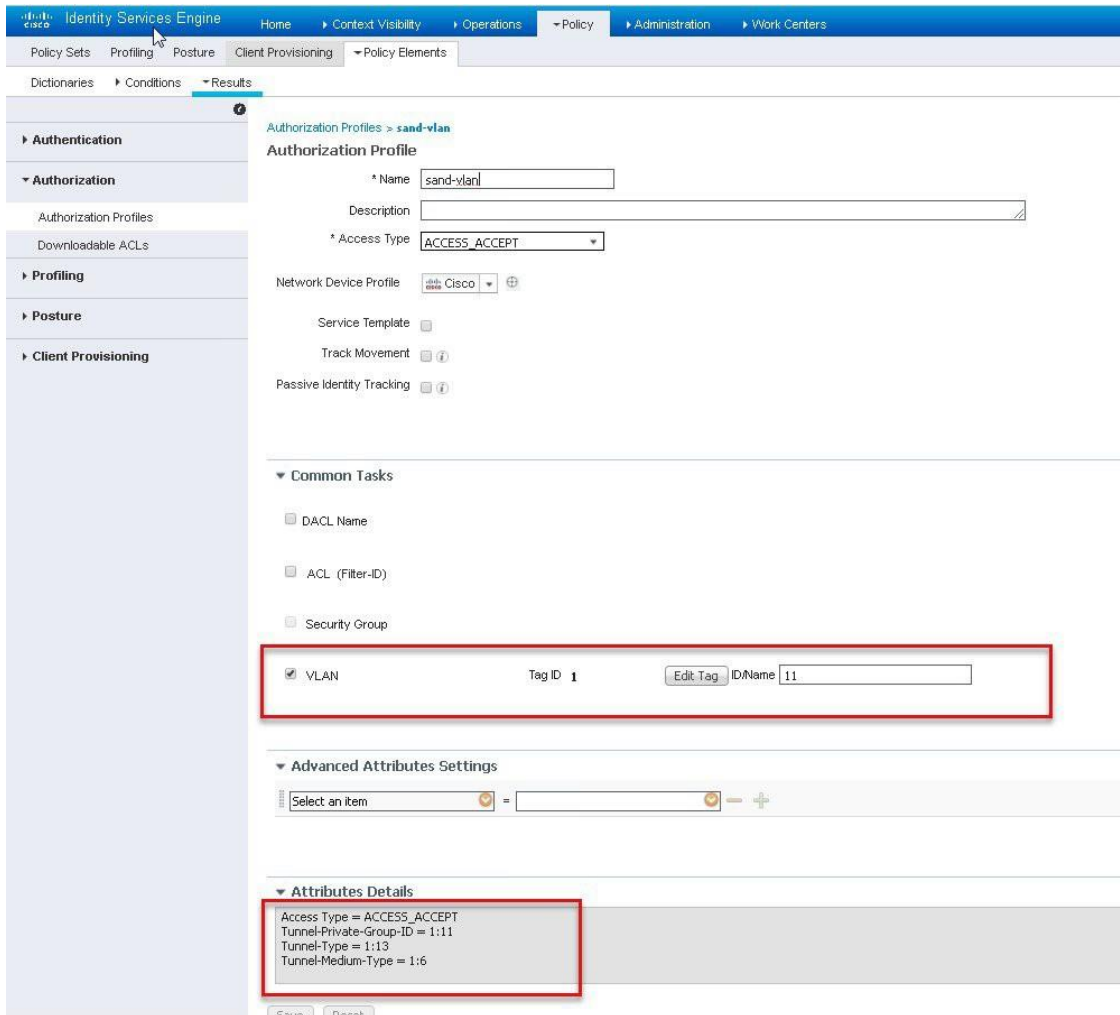


Step 12

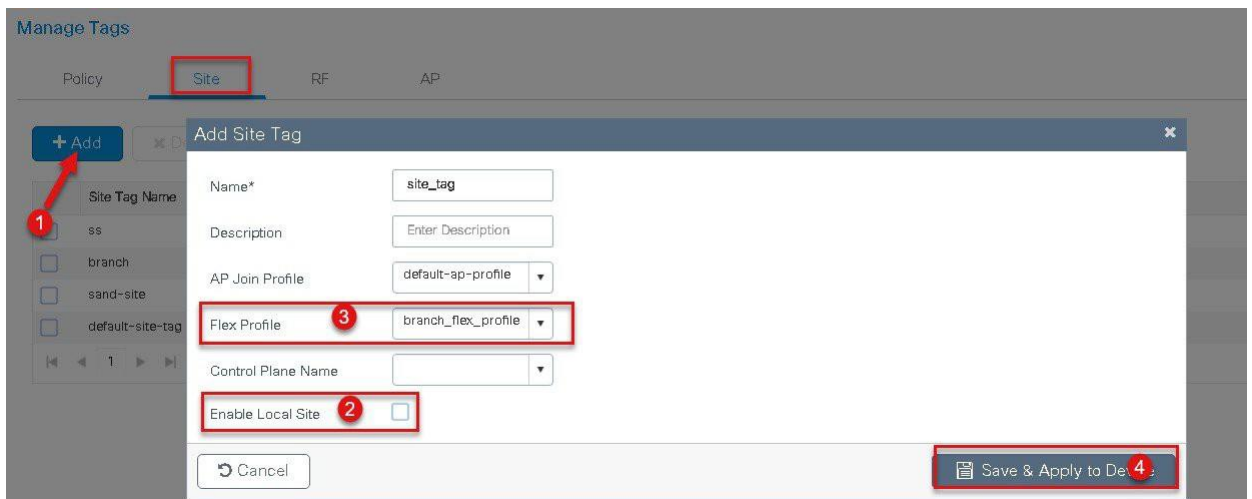
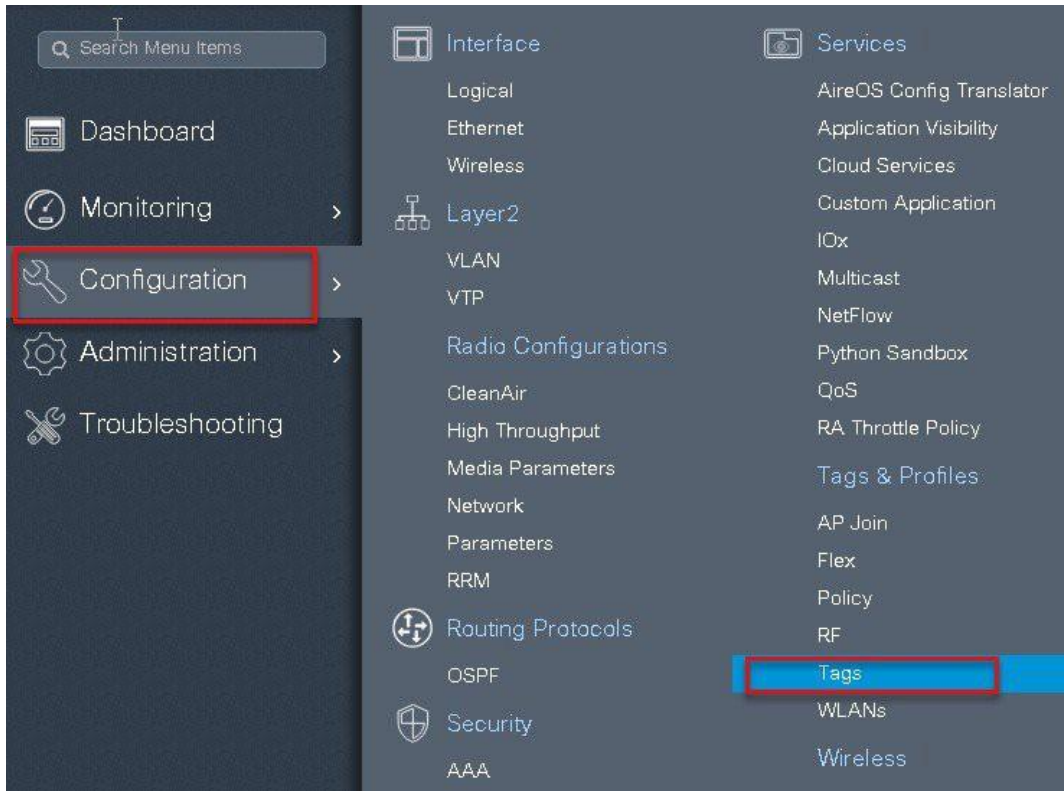
Create an Authorization profile on the ISE to override the VLAN.

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

In this example vlan 11 is present on the AP and would make the client in local switched mode.



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



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

Assigning a site tag on a 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

Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Troubleshooting

Interface

- Logical
- Ethernet
- Wireless
- Layer2
- VLAN
- VTP
- Radio Configurations
- CleanAir
- High Throughput
- Media Parameters
- Network
- Parameters
- RRM
- Routing Protocols
- OSPF
- Security
- AAA
- ACL
- Advanced EAP
- PKI Management
- Local EAP
- Local Policy
- TrustSec
- Threat Defense
- URL Filters
- Web Auth
- Wireless AAA Policy
- Wireless Protection Policies

Services

- AireOS Config Translator
- Application Visibility
- Cloud Services
- Custom Application
- IOx
- Multicast
- NetFlow
- Python Sandbox
- QoS
- RA Throttle Policy
- Tags & Profiles
- AP Join
- Flex
- Policy
- RF
- Tags
- WLANs
- Wireless
- Access Points
- Advanced
- Air Time Fairness
- Fabric
- Media Stream
- Mesh
- Mobility
- Wireless Setup
- Basic
- 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.

DESIGN PHASE

Tags & Profiles

- WLAN Policy (Mandatory)
- Site Policy (Optional)
- Radio Policy (Optional)

WLAN Profile | AP Join Profile | RF Profile

Policy Profile | Flex Profile | RF Tag

Policy Tag | Site Tag

DEPLOY PHASE

Apply to APs (Mandatory)

Tag APs

Select APs and push configuration to them

TERMINOLOGY

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

ACTIONS

Go to List View
Create New

Start Now

Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Troubleshooting

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.

DESIGN PHASE

Tags & Profiles

- WLAN Policy (Mandatory)
- Site Policy (Optional)
- Radio Policy (Optional)

WLAN Profile | AP Join Profile | RF Profile

Policy Profile | Flex Profile | RF Tag

Policy Tag | Site Tag

DEPLOY PHASE

Apply to APs (Mandatory)

Tag APs

Select APs and push configuration to them

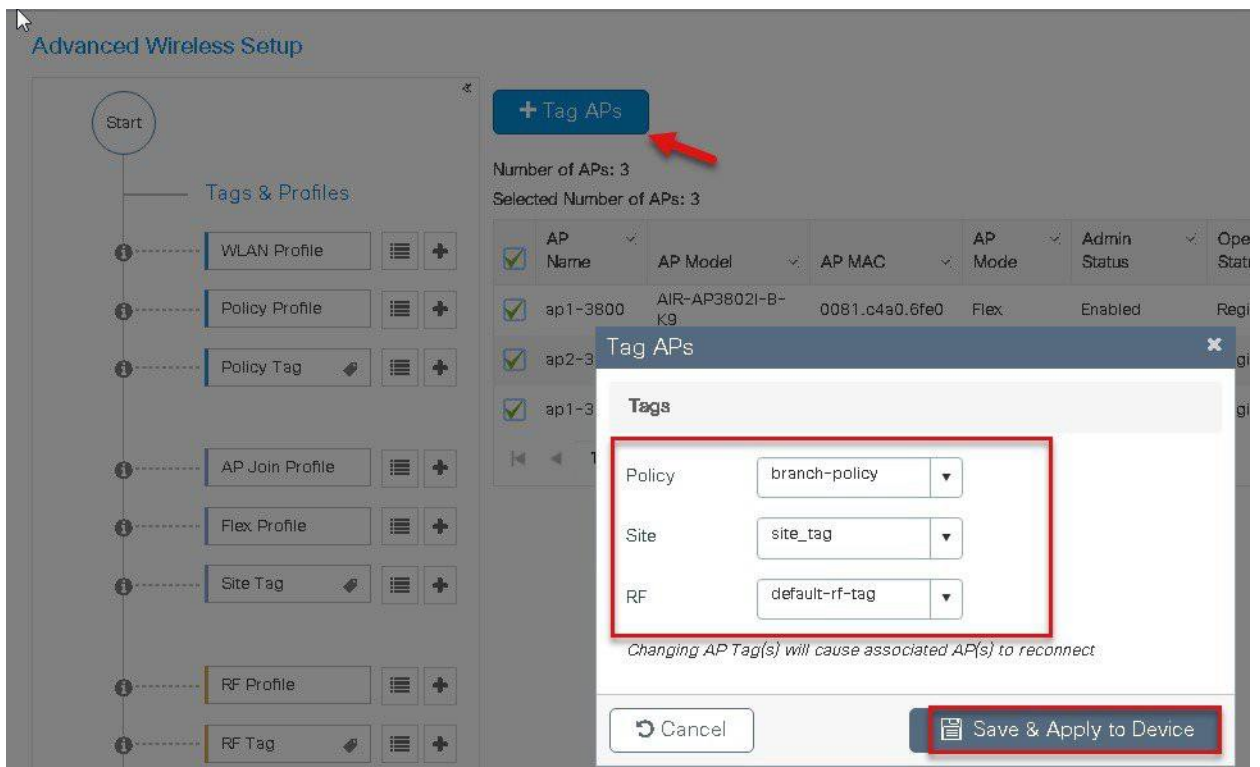
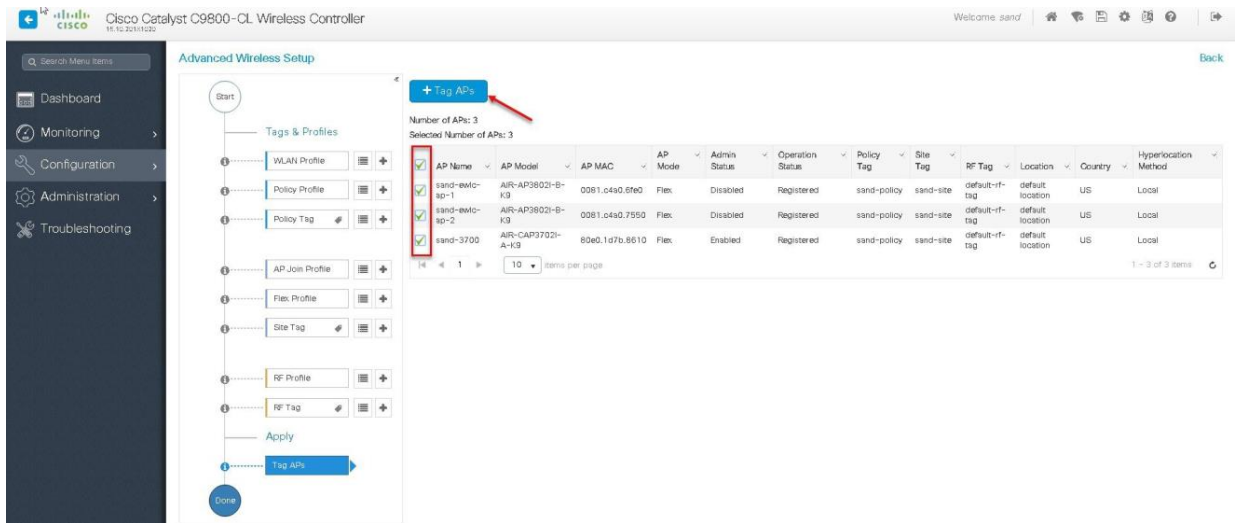
TERMINOLOGY

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

ACTIONS

Go to List View
Create New





Step 15

Associate a client on the WLAN and authenticate using the user name 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.

In this step the AAA returns vlan 11 which is present in the AP database results in local switched WLAN.

Double click on the client mac to open up the details of the Client session

Cisco Catalyst C9800-CL Wireless Controller

Welcome sand

Search Menu Items

- Dashboard
- Monitoring
- Configuration
- Administration
- Troubleshooting

Clients

Clients Sleeping Clients Excluded Clients

1 Client(s) in the Network: 1

Client MAC Address	IPv4/IPv6 Address	AP Name	WLAN	State	Protocol	User Name	Device Type	Role
1c36.0bef.6492	9.1.11.252	ap-1-3800	10	Run	11ac	isand-wireless		Local

1 - 1 of 1 clients

Client

General QOS Statistics ATF Statistics Mobility History Call Statistics

Client Properties AP Properties Security Information Client Statistics QOS Properties

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

Client

General QOS Statistics ATF Statistics Mobility History Call Statistics

Client Properties AP Properties Security Information Client Statistics QOS Properties

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	100401090000000F03A,55440
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 which is not present on the AP database but on the WLC.

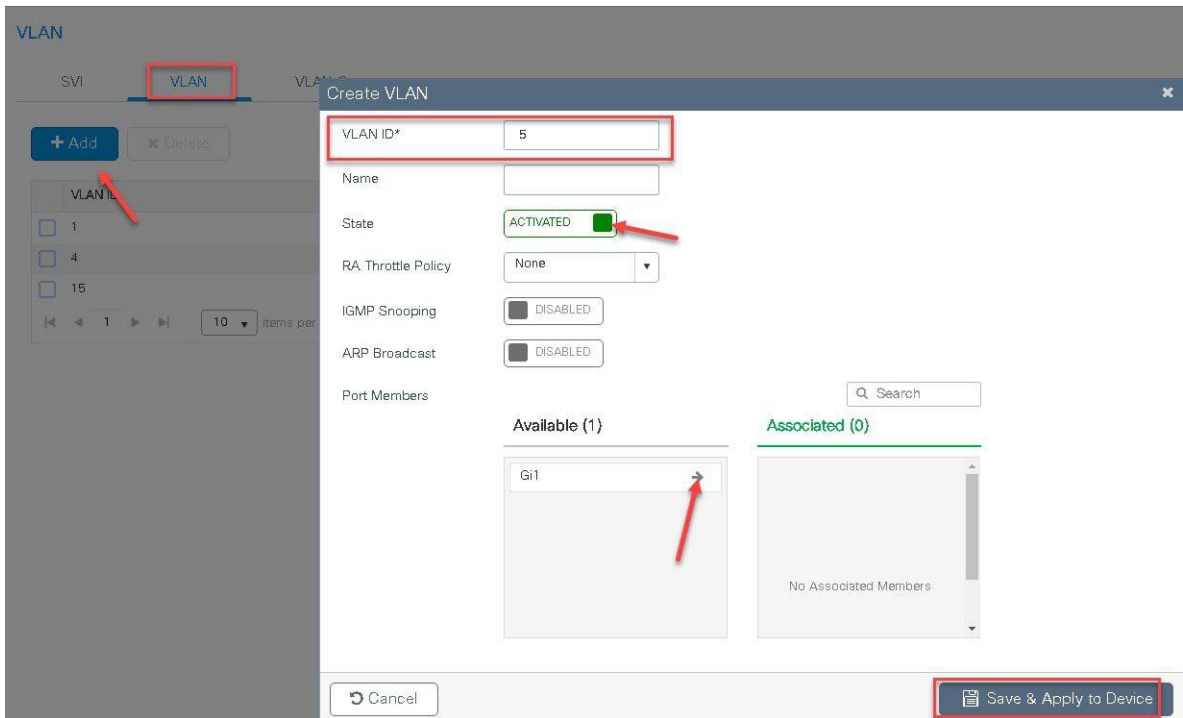
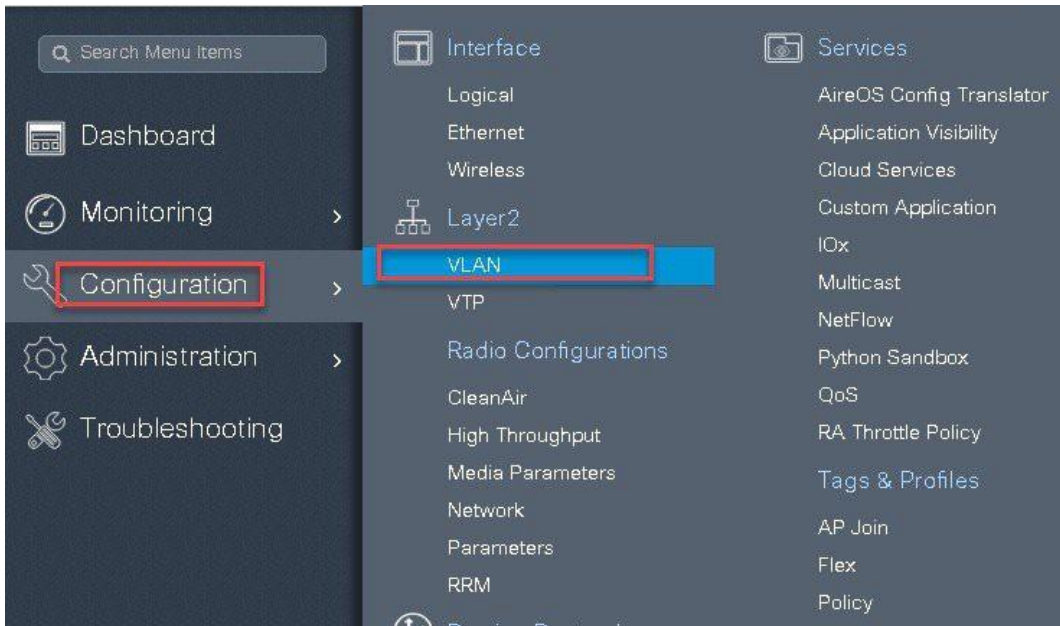
In this example VLAN 5 is present on the WLC and not on the AP database which results in WLAN being central switched.

The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface for an Authorization Profile named 'vlan-wlc'. The left sidebar shows navigation options: Authentication, Authorization, Profiling, Posture, and Client Provisioning. The main content area is titled 'Authorization Profiles > vlan-wlc' and includes the following sections:

- Authorization Profile:**
 - Name: vlan-wlc
 - Description: (empty)
 - Access Type: ACCESS_ACCEPT
 - Network Device Profile: Cisco
 - Service Template: (unchecked)
 - Track Movement: (unchecked)
 - Passive Identity Tracking: (unchecked)
- Common Tasks:**
 - DACL Name: (unchecked)
 - ACL (Filter-ID): (unchecked)
 - Security Group: (unchecked)
 - VLAN:** (checked) Tag ID 1, ID/Name 5 (highlighted with a red box)
- Advanced Attributes Settings:** (empty)
- Attributes Details:** (highlighted with a red box)
 - Access Type = ACCESS_ACCEPT
 - Tunnel-Private-Group-ID = 1:5
 - Tunnel-Type = 1:13
 - Tunnel-Medium-Type = 1:6

Buttons for 'Save' and 'Reset' are located at the bottom of the configuration area.

Step 17 Validation on the presence of VLAN 5 on the WLC .
 Navigate to Configuration >Vlan.



Step 18

Associate a client on the WLAN and authenticate using the user name 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 and switching properties for the client.

Double click on the client mac to open up the details of the Client session.

Search Menu Items

- Dashboard
- Monitoring
- Configuration
- Administration
- Troubleshooting

Clients

Clients Sleeping Clients Excluded Clients

✖ Delete

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	

10 items per page

click on client mac to open the details

Client

General QOS Statistics ATF Statistics Mobility History Call Statistics

Client Properties AP Properties Security Information Client Statistics QOS Properties

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

The screenshot shows the 'Client' configuration window with the 'Security Information' tab selected. The 'VLAN' field is highlighted in red in both the 'Local Policies' and 'Resultant Policies' sections.

Section	Field	Value
General	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	100401090000001303BC4500
	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 arise certain concerns with central authentication at the WLC.

How can wireless clients perform 802.1X authentication and access Data Center services if WLC fails?

How can wireless clients perform 802.1X authentication if WAN link between Branch and Data Center fails?

Is there any impact on branch mobility during WAN failures?

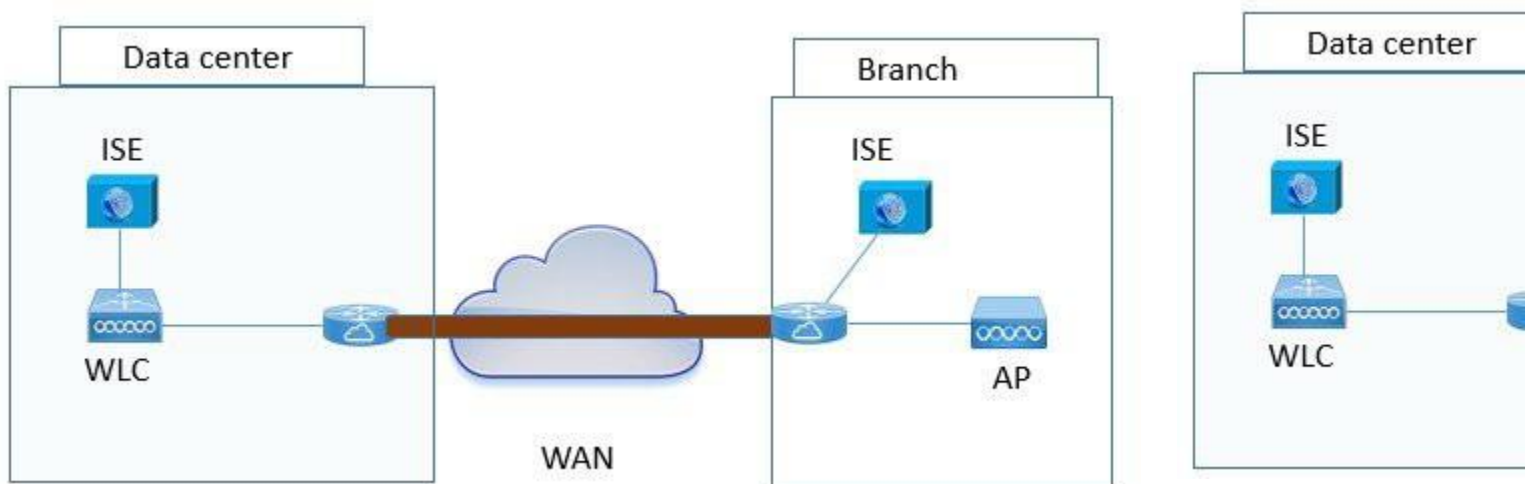
Does the Flex Connect Solution provide no operational branch downtime?

Flexconnect Local authentication and Backup/Local Radius can address the above concerns by enabling branch to operate independently in case of 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 Wave1 AP's.
- This feature can be used with central authentication or local authentication .In 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

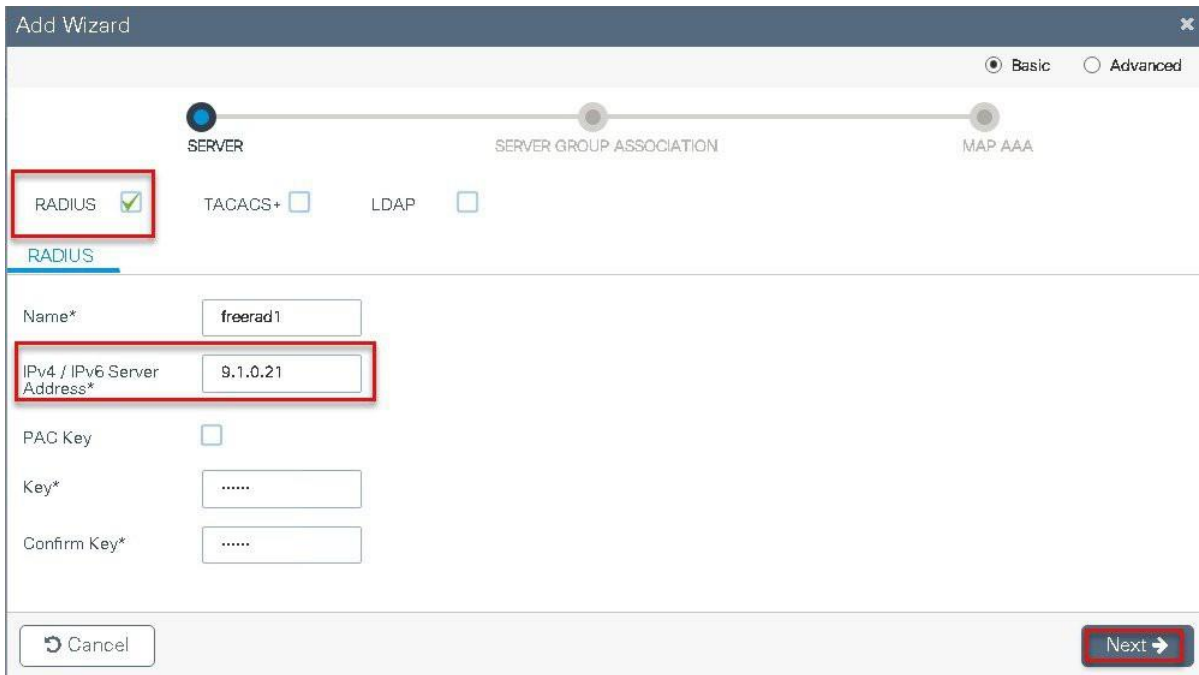
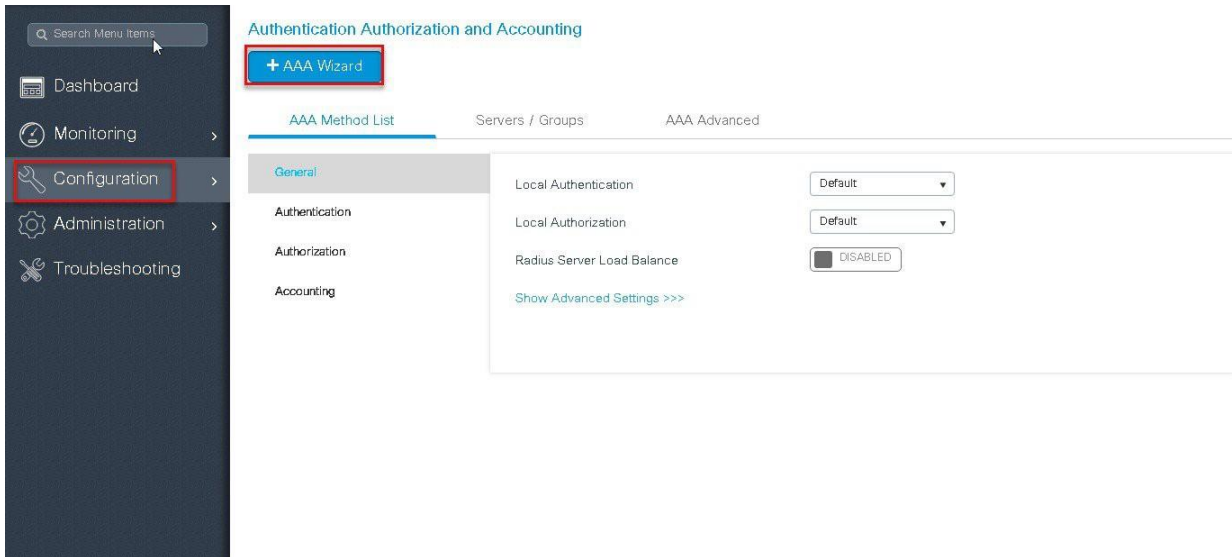


Steps for Local Authentication and Backup Radius server

Procedure

-
- Step1** 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 .



Add Wizard Basic Advanced

SERVER
 SERVER GROUP ASSOCIATION
 MAP AAA

RADIUS

Name*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Available Servers

ISE
freerad

Assigned Servers
 freerad

Add Wizard Basic Advanced

SERVER
 SERVER GROUP ASSOCIATION
 MAP AAA

General
 Authentication
 Authorization
 Accounting

General | Authentication | Authorization

aaa_dot1x_system_auth_control

Local Authentication

Local Authorization

Radius Server Load Balance

[Show Advanced Settings >>>](#)

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

- radius
- ldap
- tacacs+
- rad-group
- radgrp_branch

Assigned Server Groups

- freerad

Previous Save & Apply to Device

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

- radius
- ldap
- tacacs+
- rad-group
- radgrp_branch

Assigned Server Groups

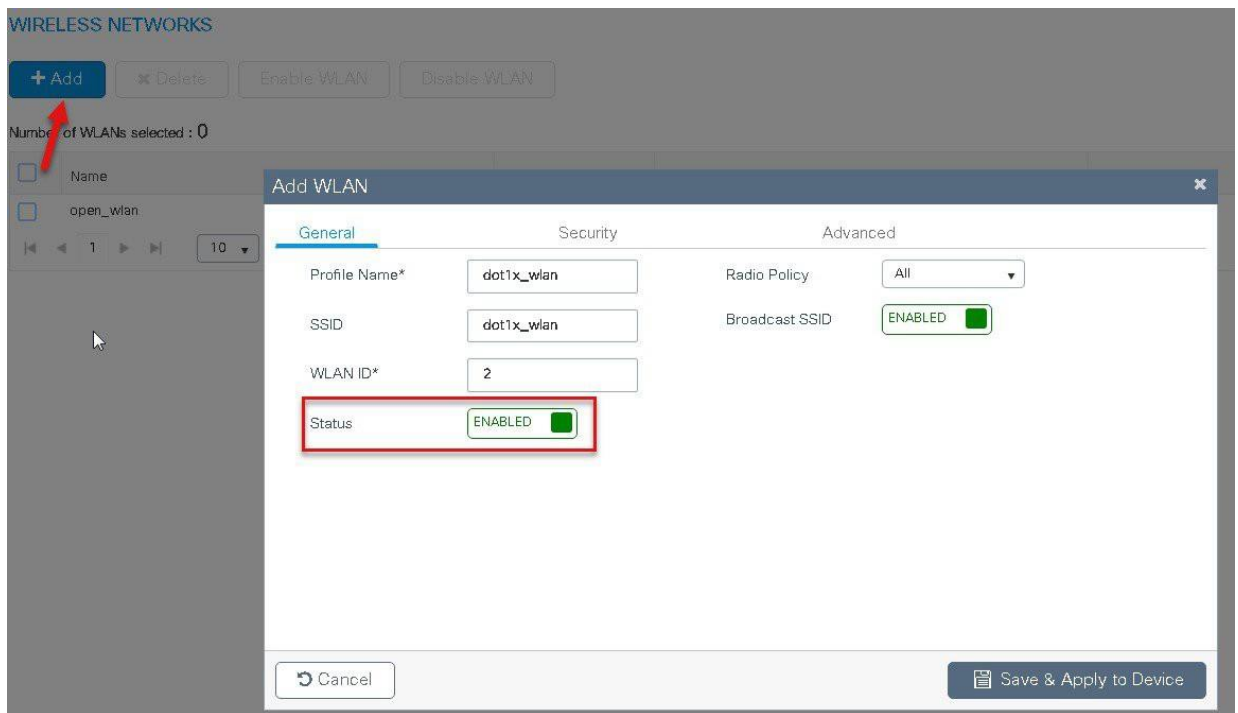
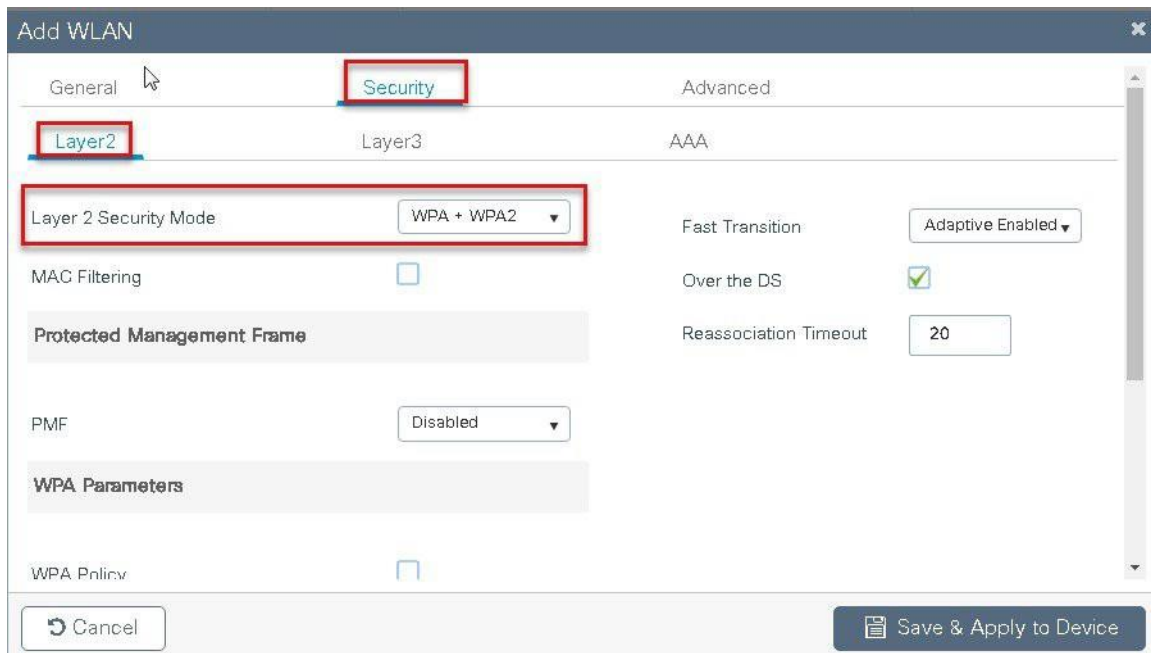
- freerad

Previous Save & Apply to Device

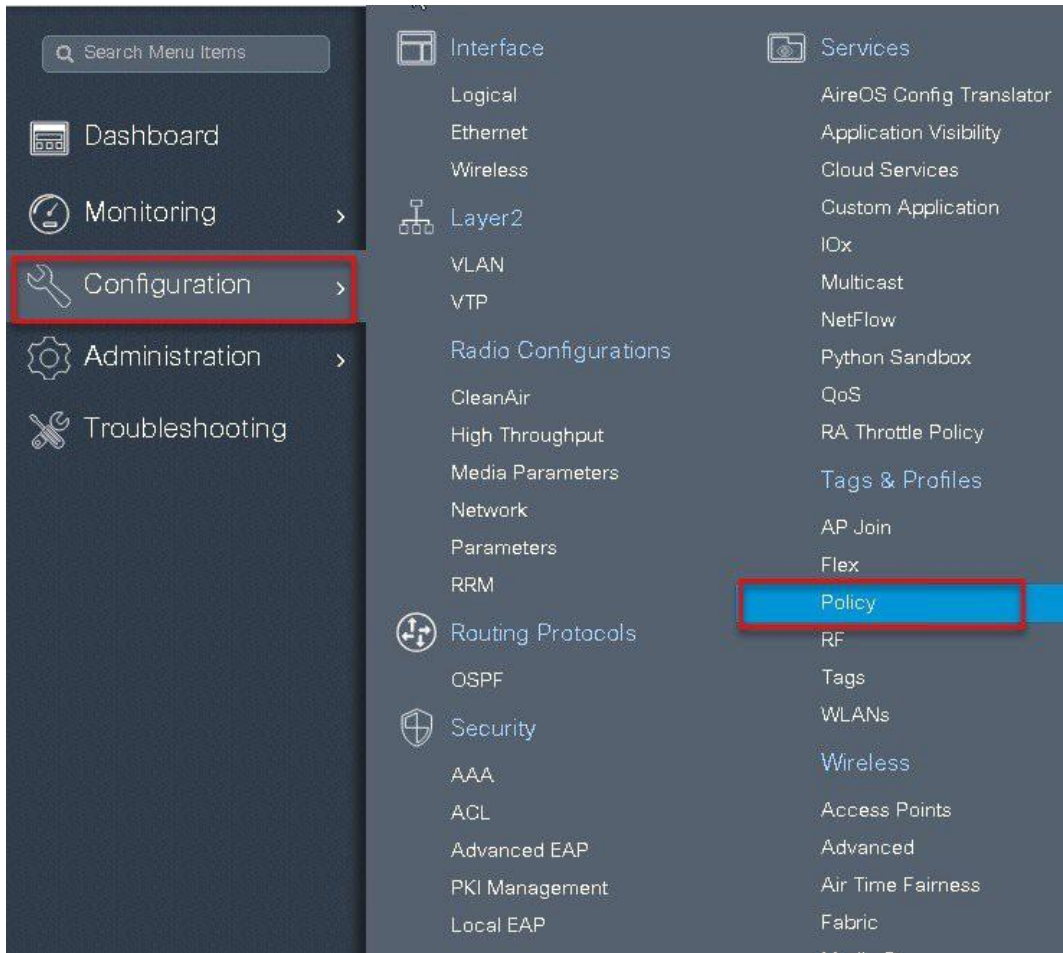
- Step2** Create an SSID on the controller for dot1x authentication.
To create an SSID navigate to Configuration >Tags& profiles >WLANs.

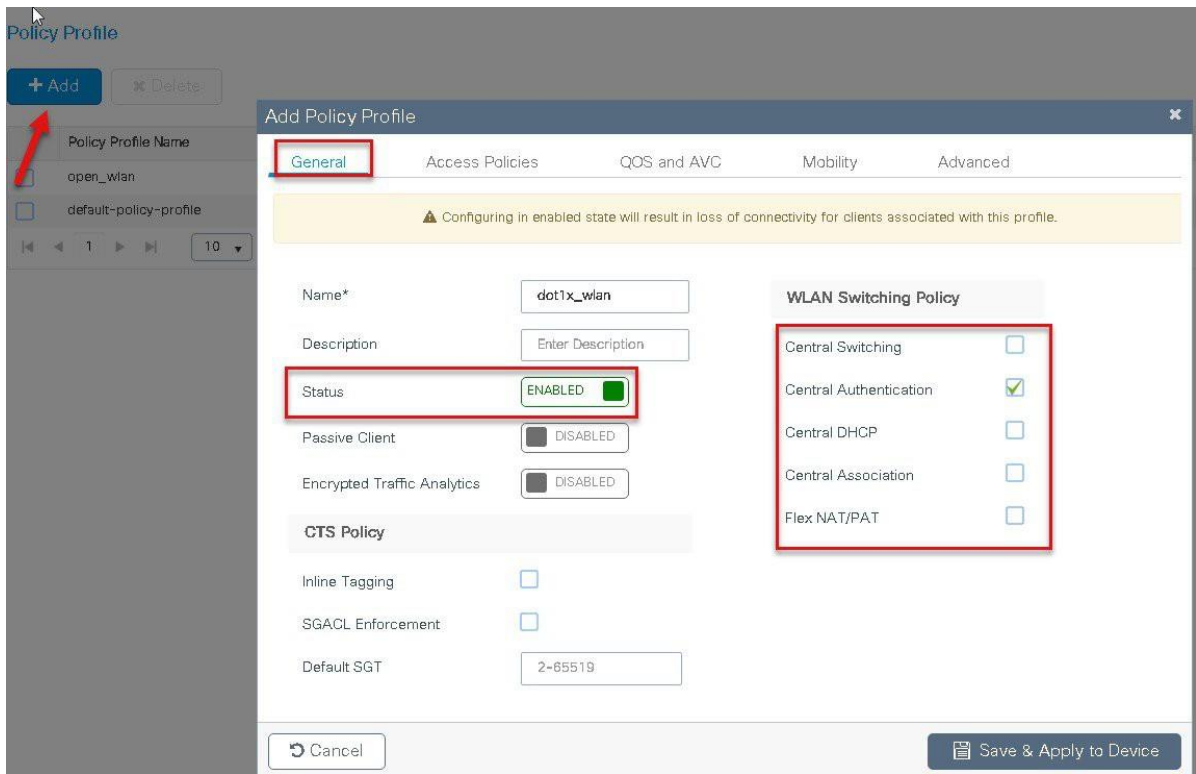
Defines the method list created for dot1x on the WLAN AAA settings.

The image shows a network configuration interface. The top part is a menu with a search bar and several categories: Dashboard, Monitoring, Configuration (highlighted with a red box), Administration, and Troubleshooting. Under Configuration, there are sub-menus: Interface (Logical, Ethernet, Wireless), Layer2 (VLAN, VTP), Radio Configurations (CleanAir, High Throughput, Media Parameters, Network, Parameters, RRM), Routing Protocols (OSPF), and Security (highlighted with a red box). Under Security, there is a sub-menu 'WLANs' (highlighted with a red box). The bottom part of the image shows the 'Add WLAN' dialog box. It has three tabs: General, Security (highlighted with a red box), and Advanced. Under the Security tab, there are sub-sections: Layer2, Layer3, and AAA (highlighted with a red box). Under the AAA section, there is a dropdown menu for 'Authentication List' with 'dot1x' selected (highlighted with a red box). Below this is a checkbox for 'Local EAP Authentication' which is unchecked. At the bottom of the dialog, there are two buttons: 'Cancel' and 'Save & Apply to Device' (highlighted with a red box).

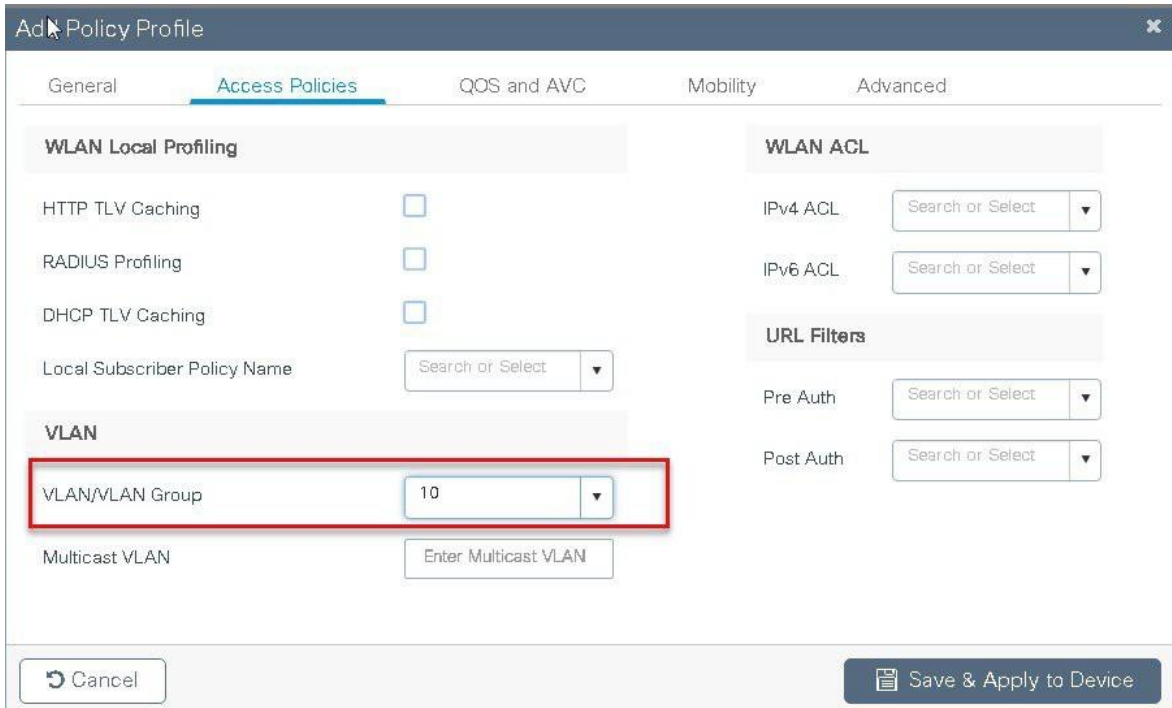


Step3 Create a policy profile enable local switching and central authentication on the profile.



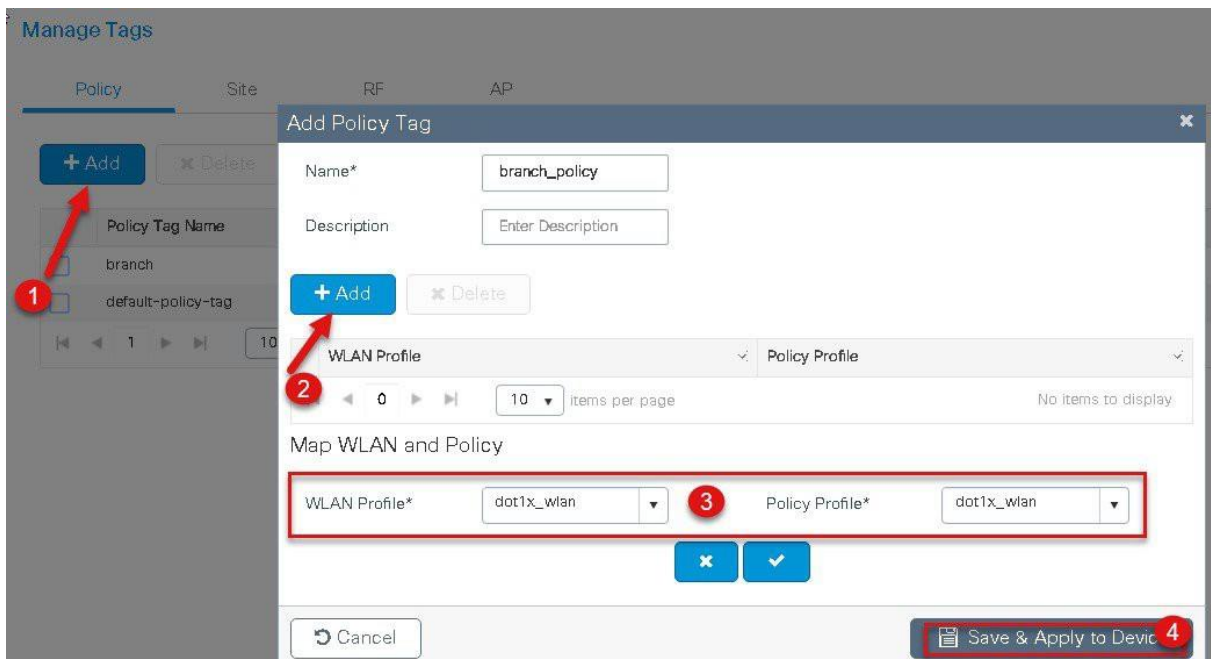
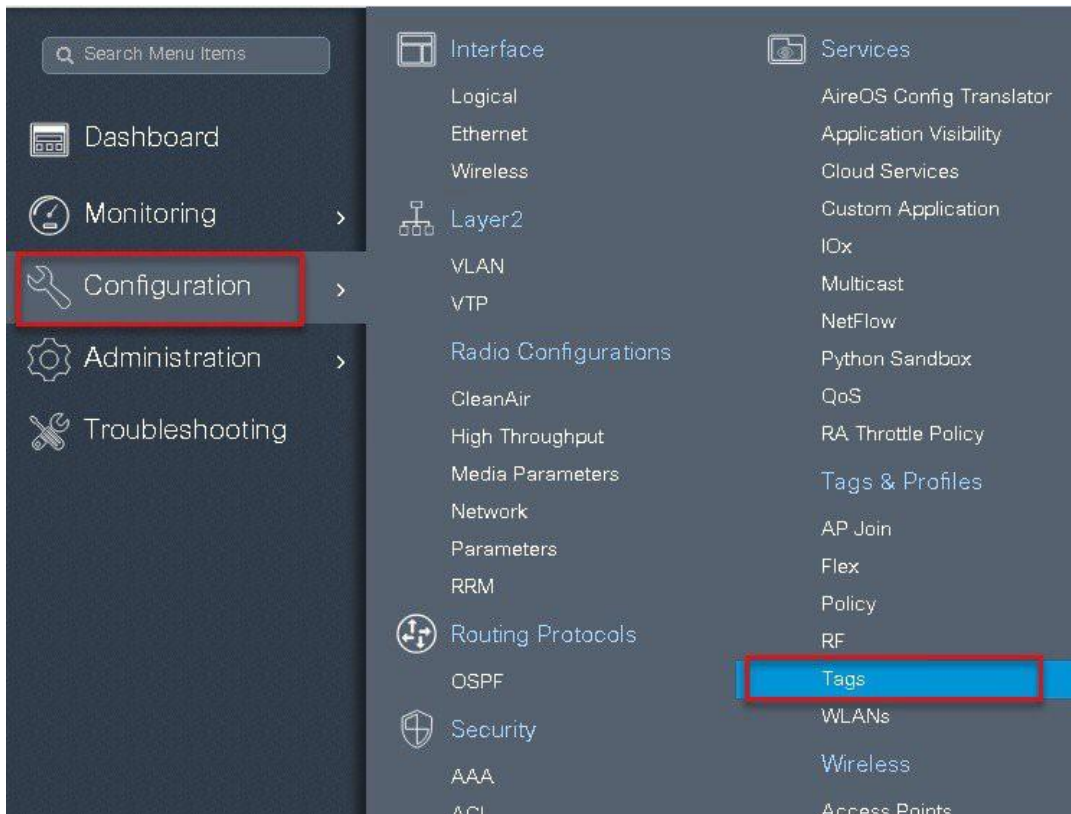


Step4 Map the Default VLAN for the WLAN.

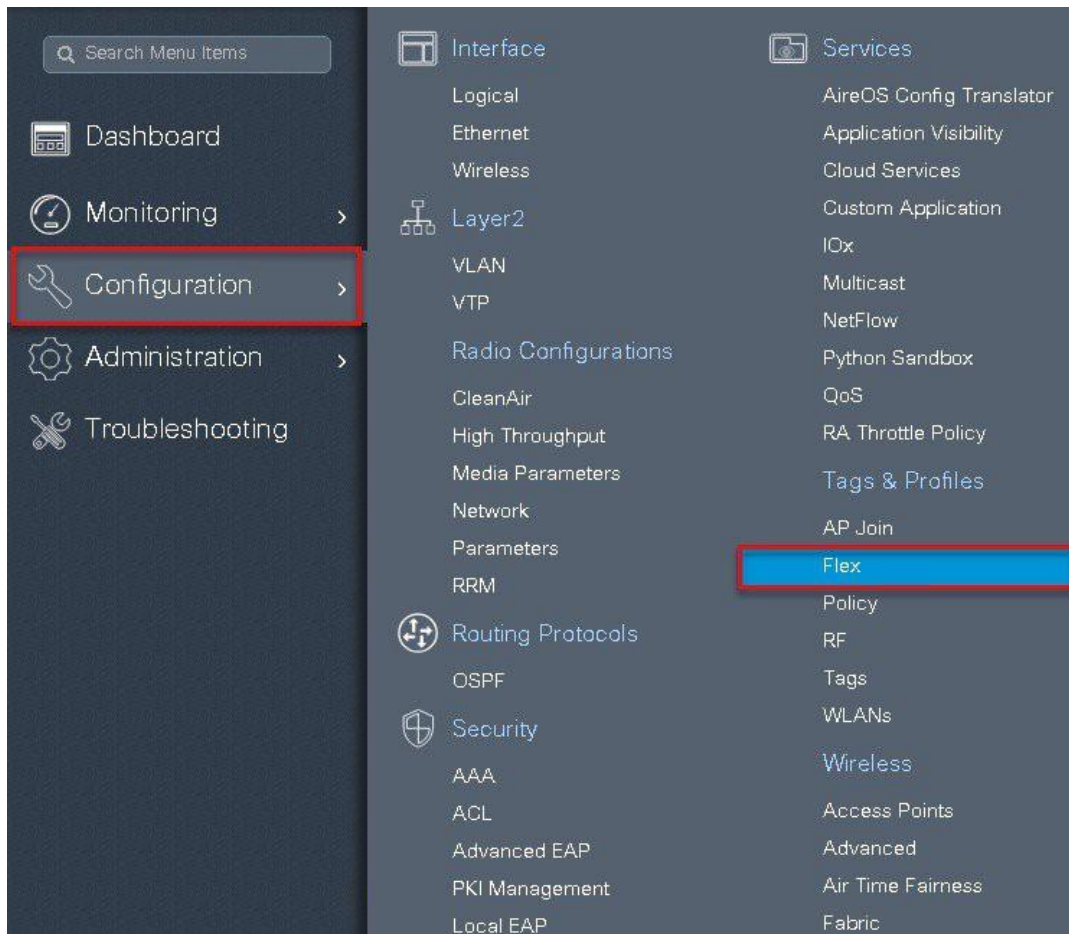


Step5 Map the WLAN to policy profile.

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



Step6 Create a flex profile to create the VLAN on the profile to be used by the SSID.



Flex Profile

[+ Add](#) [x Delete](#)

Flex Profile Name: default-flex-p Description:

Add Flex Profile

General Local Authentication Policy ACL VLAN

Name* Multicast Overridden Interface

Description Fallback Radio Shut

Native VLAN ID Flex Resilient

HTTP Proxy Port ARP Caching

HTTP-Proxy IP Address Efficient Image Upgrade

Office Extend AP

Join Minimum Latency

CTS Policy

Inline Tagging

SGACL Enforcement

CTS Profile Name [x](#)

[Cancel](#) [Save & Apply to Device](#)

Add Flex Profile

General **Local Authentication** Policy ACL VLAN

Radius Server Group [v](#)

EAP Fast Profile [v](#)

Users

[+ Add](#) [x Delete](#)

Username

0 items per page

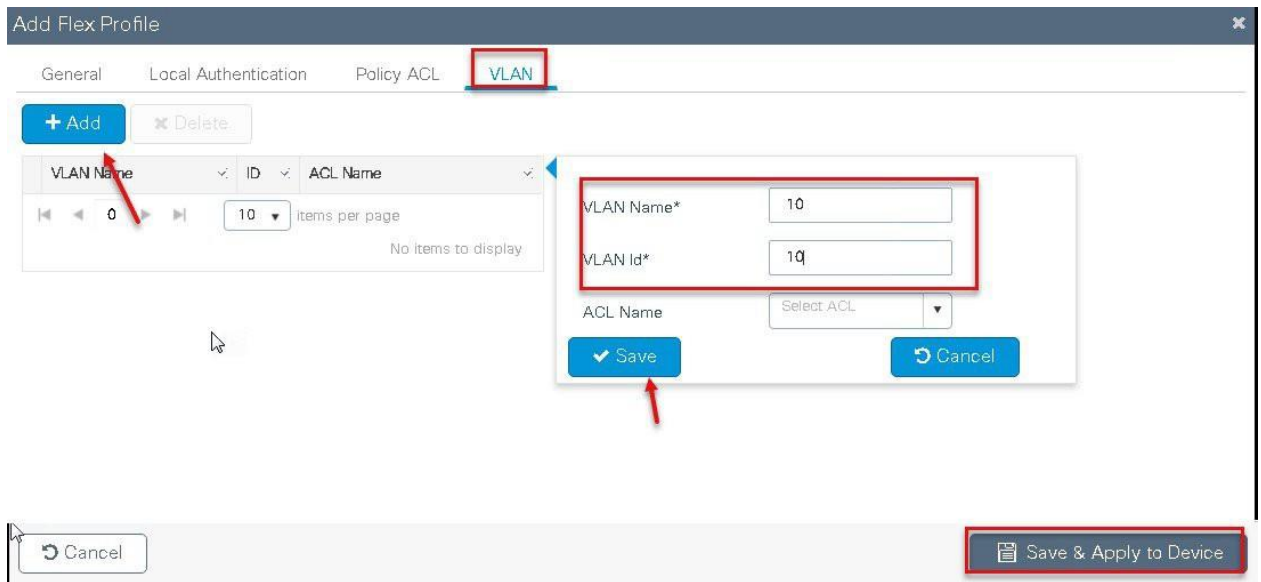
No Items to display

LEAP

PEAP

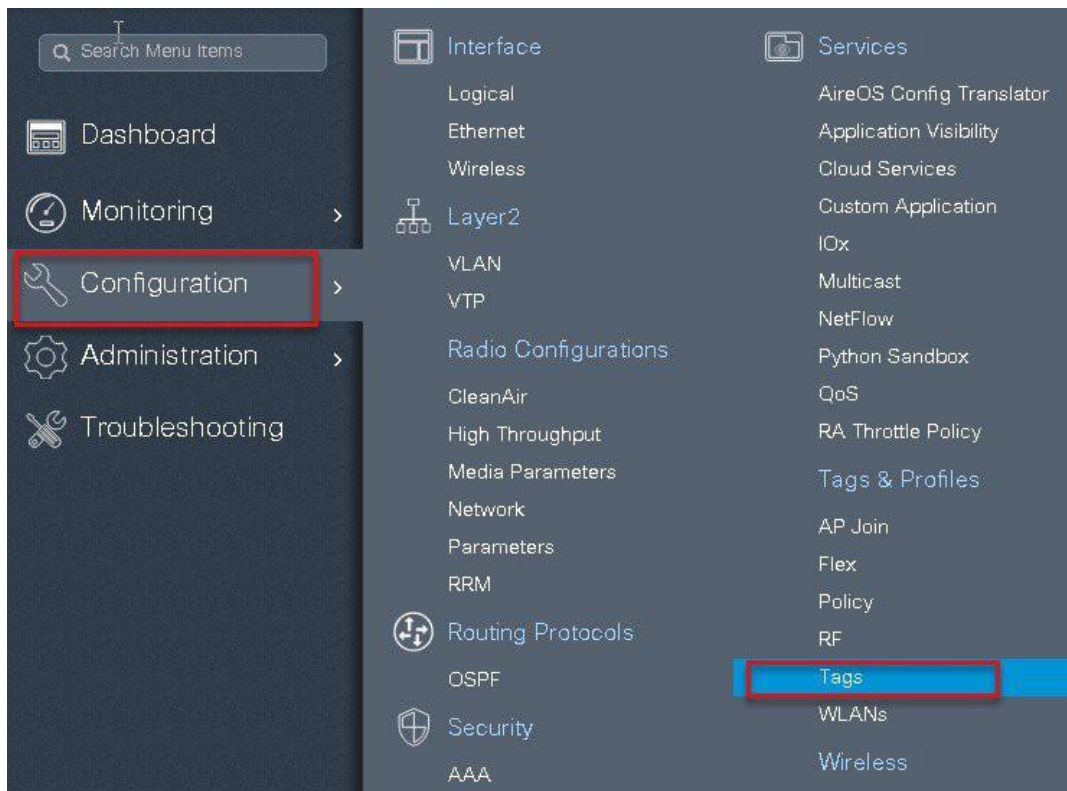
TLS

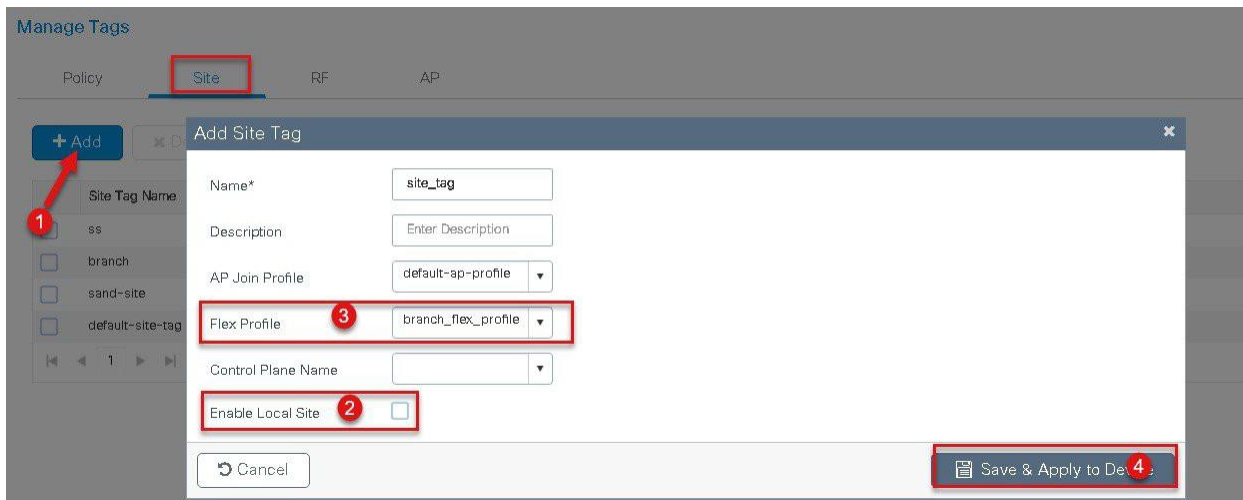
RADIUS



Step7 Create a site tag and map the flex profile on the site tag.

Uncheck the “Enable local site “ to add the flex profile on the site tag .





Step8 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 a 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

Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Troubleshooting

Interface

- Logical
- Ethernet
- Wireless
- Layer2
- VLAN
- VTP
- Radio Configurations
- CleanAir
- High Throughput
- Media Parameters
- Network
- Parameters
- RRM
- Routing Protocols
- OSPF
- Security
- AAA
- ACL
- Advanced EAP
- PKI Management
- Local EAP
- Local Policy
- TrustSec
- Threat Defense
- URL Filters
- Web Auth
- Wireless AAA Policy
- Wireless Protection Policies

Services

- AireOS Config Translator
- Application Visibility
- Cloud Services
- Custom Application
- IOx
- Multicast
- NetFlow
- Python Sandbox
- QoS
- RA Throttle Policy
- Tags & Profiles
- AP Join
- Flex
- Policy
- RF
- Tags
- WLANs
- Wireless
- Access Points
- Advanced
- Air Time Fairness
- Fabric
- Media Stream
- Mesh
- Mobility
- Wireless Setup
- Basic
- 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.

DESIGN PHASE

Tags & Profiles

- WLAN Policy (Mandatory)
- Site Policy (Optional)
- Radio Policy (Optional)

WLAN Profile | AP Join Profile | RF Profile

Policy Profile | Flex Profile | RF Tag

Policy Tag | Site Tag

DEPLOY PHASE

Apply to APs (Mandatory)

Tag APs

Select APs and push configuration to them

TERMINOLOGY

Tag

WLAN Policy, Policy Profile

Site Policy - AP Profile, Site Profile

Radio Policy - Radio Characteristics

ACTIONS

Go to List View

Create New

Start Now

Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Troubleshooting

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.

DESIGN PHASE

Tags & Profiles

- WLAN Policy (Mandatory)
- Site Policy (Optional)
- Radio Policy (Optional)

WLAN Profile | AP Join Profile | RF Profile

Policy Profile | Flex Profile | RF Tag

Policy Tag | Site Tag

DEPLOY PHASE

Apply to APs (Mandatory)

Tag APs

Select APs and push configuration to them

TERMINOLOGY

Tag

WLAN Policy, Policy Profile

Site Policy - AP Profile, Site Profile

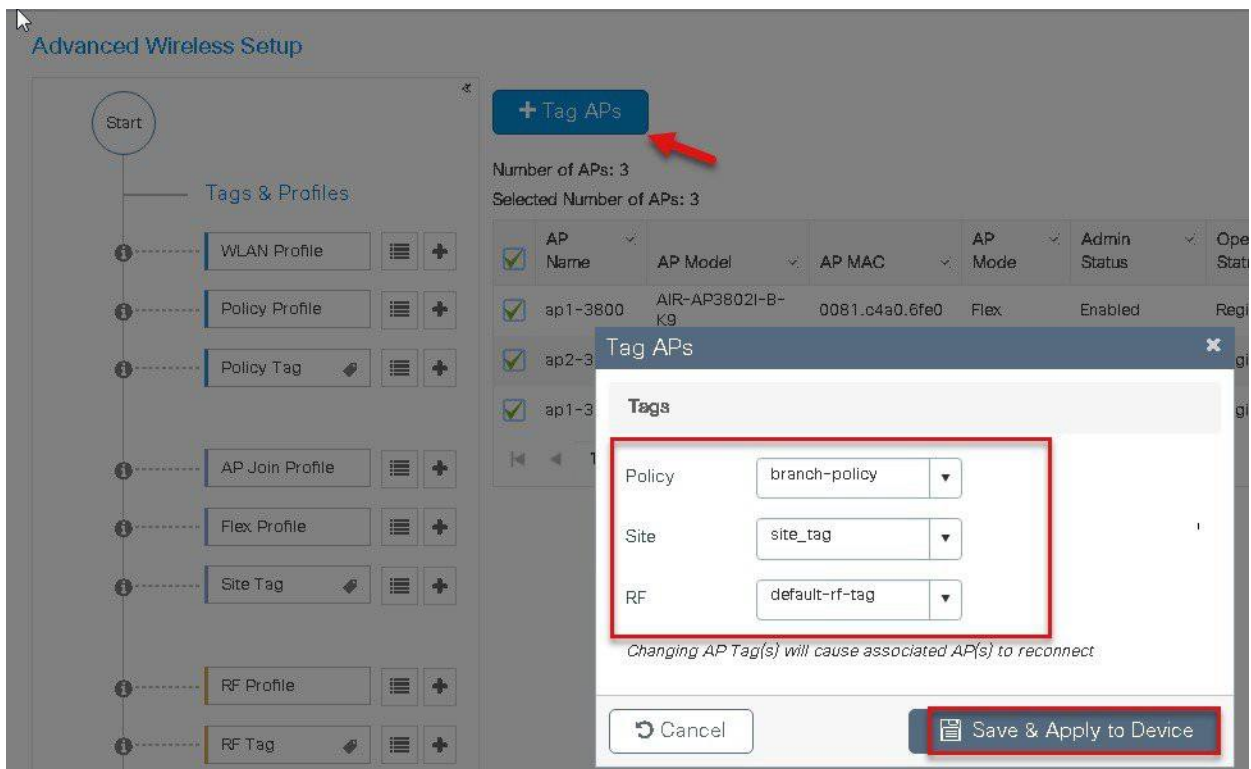
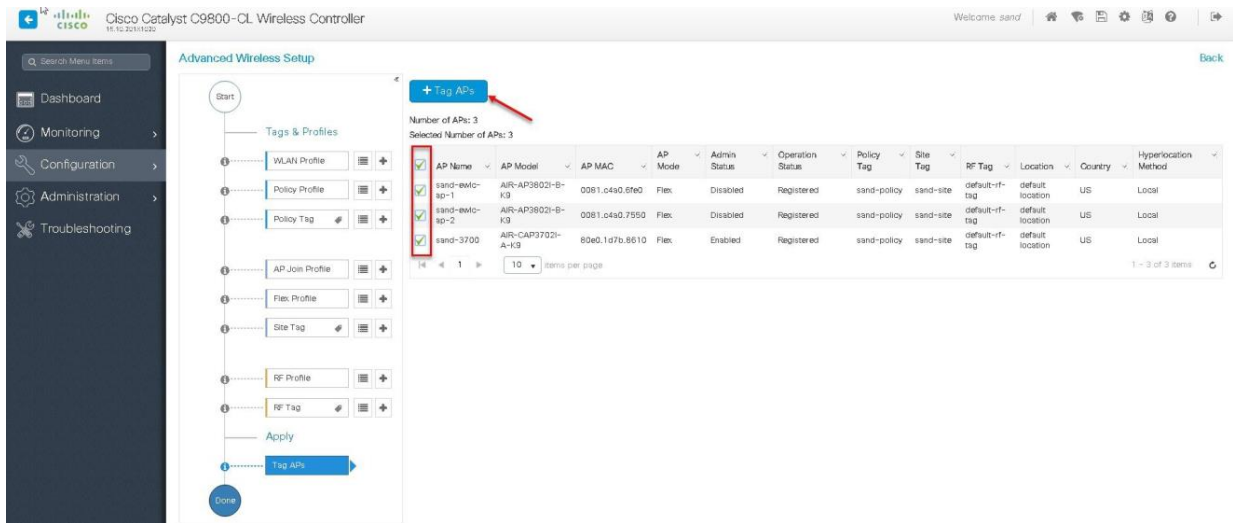
Radio Policy - Radio Characteristics

ACTIONS

Go to List View

Create New





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 do dot1x authentication on the AP itself using the local radius facility.

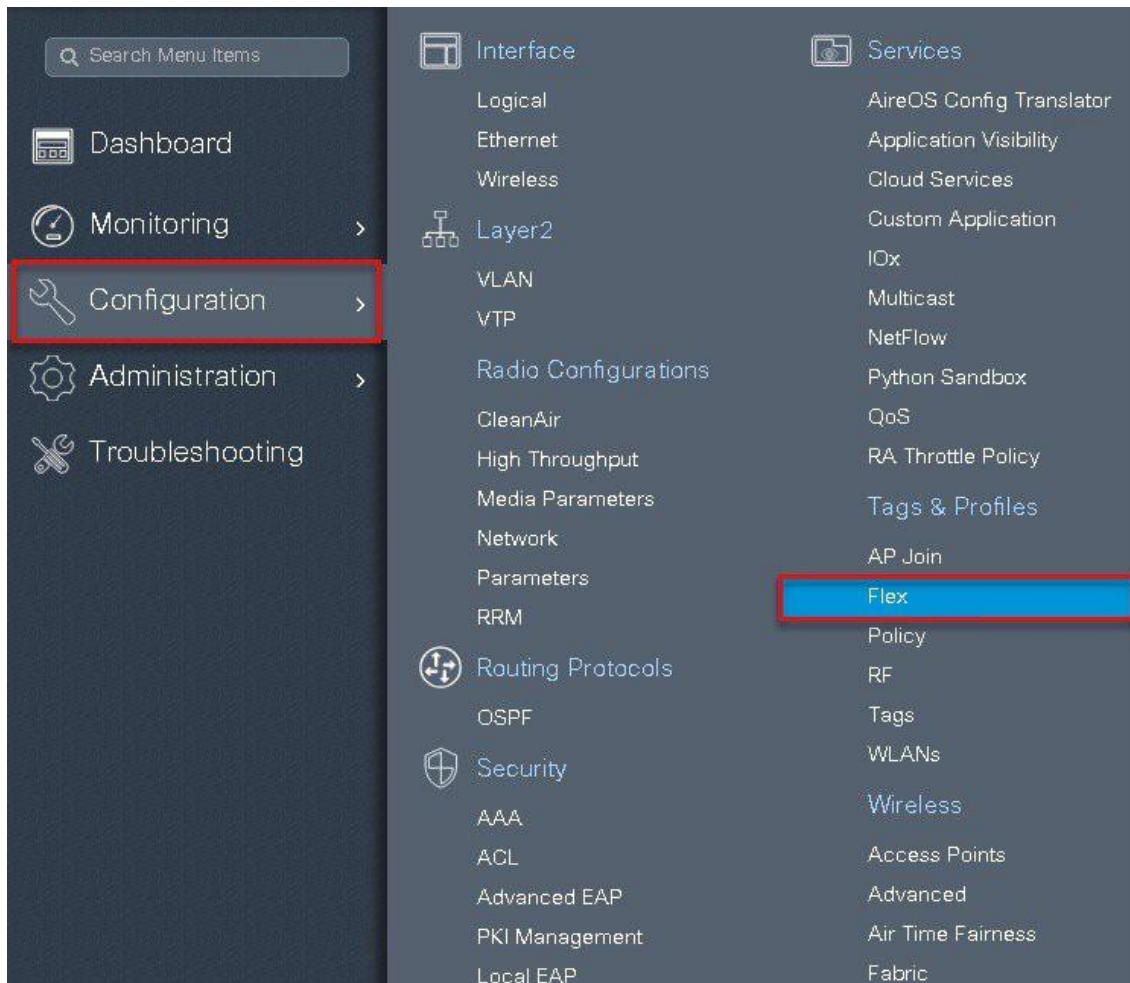
Procedure

To have the flexconnect AP configured as the radius server repeat the steps 2 ,3 ,4 ,5,7 and 8 in the procedure section of Local Authentication with External radius server 1.

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

Procedure

Step1 Create a flex profile, Navigate to Configuration > Flex.



Step2 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 resides on the AP .

Add Flex Profile

General Local Authentication Policy ACL VLAN

Name* Multicast Overridden Interface

Description Fallback Radio Shut

Native VLAN ID Flex Resilient

HTTP Proxy Port ARP Caching

HTTP-Proxy IP Address Efficient Image Upgrade

Office Extend AP

Join Minimum Latency

CTS Policy

Inline Tagging

SGACL Enforcement

CTS Profile Name

Add Flex Profile

General Local Authentication Policy ACL VLAN

Radius Server Group

EAP Fast Profile

LEAP

PEAP

TLS

RADIUS

Users

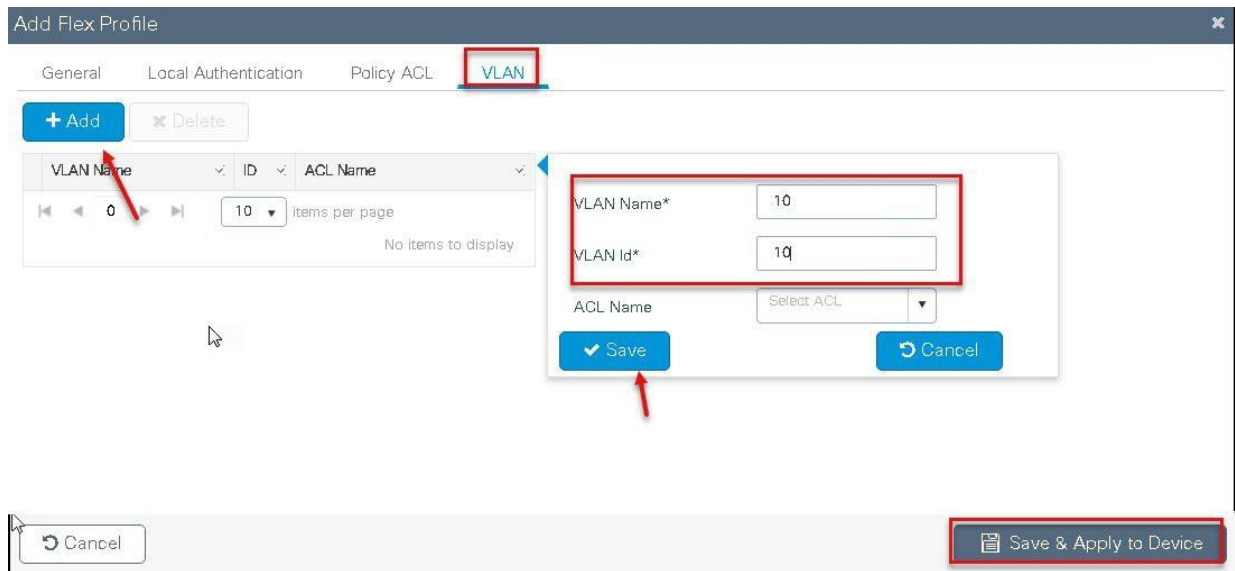
Username

Password Type

Password *

Confirm *

Password



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 master 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, the controller takes care of distributing the master key to the AP's. The controller distributes the master key to all the Ap's whose site tag and policy tag are the same, this results in ability to do fast roaming across the AP within the same site. The distribution of the master key is done based on the site tag of the AP site the client initially associates, the controller now find's all the AP's which has a similar site tag and policy tag and pushes the master key on those AP' and thus enabling fast roaming among the AP's.

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 AP's . On 16.10 the EAP method supported for AP as radius server is EAP-LEAP.
- Fast roaming is not supported with default site-tag, if the AP's are mapped to a default site tag then the master 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 Up-Stream – 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 WLC to FlexConnect APs.
- Peer-to-peer blocking action configured as drop or upstream-forward on WLAN is treated as peer-to-peer blocking enabled on FlexConnect AP.

Steps

Procedure

Refer 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.

The screenshot shows the 'Add WLAN' configuration wizard with the 'Advanced' tab selected. The 'P2P Blocking Action' dropdown menu is open, showing three options: 'Disabled', 'Drop', and 'Forward-UpStream'. The 'Advanced' tab is highlighted with a red box. Other settings include Coverage Hole Detection (checked), Aironet IE (checked), Diagnostic Channel (unchecked), Universal Admin (unchecked), Load Balance (unchecked), Band Select (checked), IP Source Guard (unchecked), WMM Policy (Allowed), and Off Channel Scanning Defer (Defer Priority 5 checked). The 'Max Client Connections' is set to 0 per WLAN. The 'Save & Apply to Device' button is visible at the bottom right.

Once the P2P Blocking action is configured on the WLAN configured 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 which 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 applied on the WLAN dot11 interface and is enforced to all the client connecting on that SSID
- WLAN ACL - The ACL applied on the WLAN dot11 interface and is enforced to all the client connecting on that SSID
- Client ACL- The ACL 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 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 exclusion list .

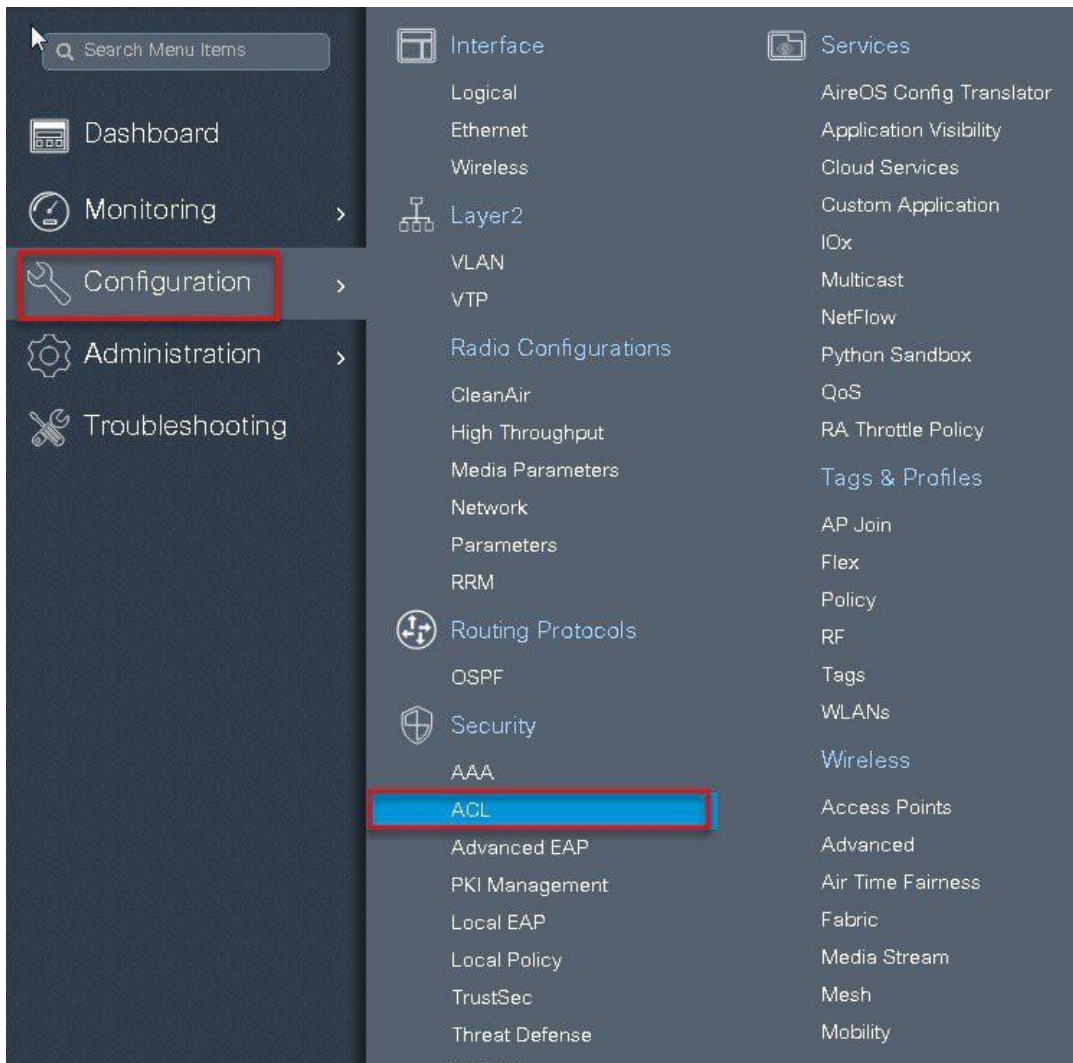
Procedure for WLAN ACL

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 and 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 the ACL works.

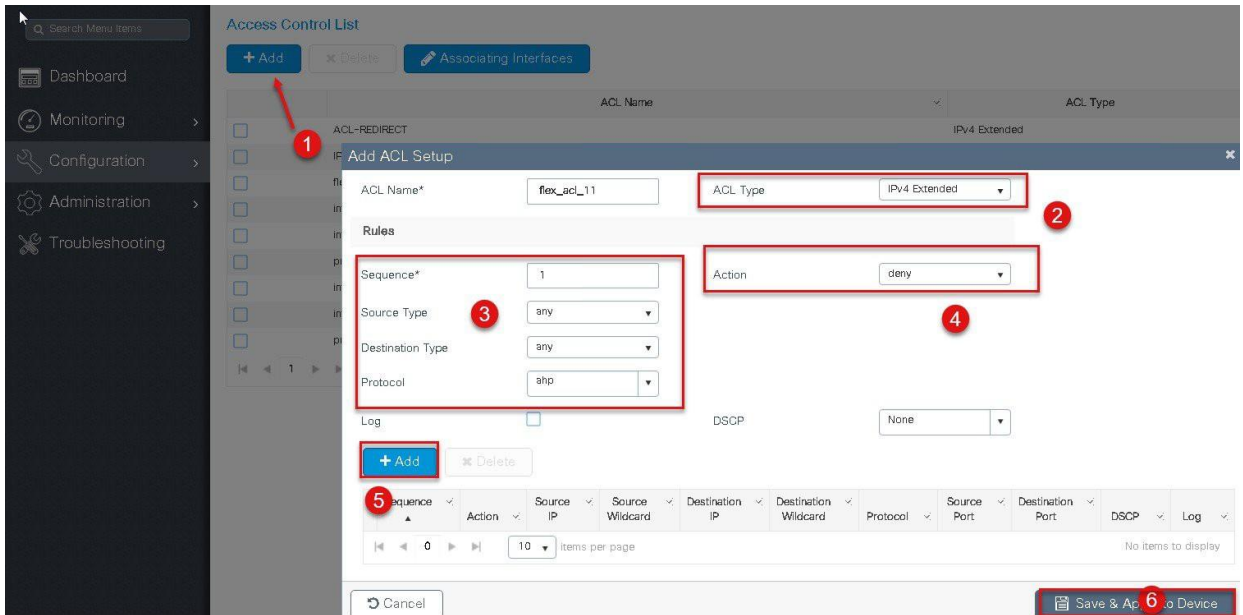
Procedure

Step1 Create an ACL on the WLC by navigating to Configuration > Security > ACL.



Step2 Perform the following steps:

- Click on Add to create an ACL, 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



Step3 Refer the steps in the procedure of advanced configuration wizard for the following :

- Create a WLAN
- Creation of policy profile (refer the screenshot below to add the ACL)
- Policy tag mapping
- Flex profile (refer the screenshot below to map the ACL using the Policy ACL)
- 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 [Close]

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*

Description

Status **ENABLED**

Passive Client DISABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

WLAN Switching Policy

Central Switching

Central Authentication

Central DHCP

Central Association

Flex NAT/PAT

Add Policy Profile [Close]

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

WLAN Local Profiling

HTTP TLV Caching

RADIUS Profiling

DHCP TLV Caching

Local Subscriber Policy Name

VLAN

VLAN/VLAN Group

Multicast VLAN

WLAN ACL

IPv4 ACL

IPv6 ACL

URL Filters

Pre Auth

Post Auth

Step4 Assign the ACL on the Flex profile , by mapping the VLAN and ACL.

Define the native VLAN for the flexconnect AP's.

The screenshot shows the 'Add Flex Profile' configuration window with the 'General' tab selected. The 'Native VLAN ID' field is highlighted with a red box and contains the value '2'. The 'Save & Apply to Device' button is also highlighted with a red box. Other fields include Name* (branch_flex_profile), Description (Enter Description), HTTP Proxy Port (0), HTTP-Proxy IP Address (0.0.0.0), and CTS Profile Name (default-sxp-profile).

Step5 Push the ACL to AP by using the Policy ACL configuration on the flex profile .

The screenshot shows the 'Add Flex Profile' configuration window with the 'Policy ACL' tab selected. The 'Add' button is highlighted with a red circle and arrow labeled '1'. The 'ACL Name*' dropdown menu is highlighted with a red box and arrow labeled '2', showing 'flex-acl11'. The 'Save' button is highlighted with a red circle and arrow labeled '3'. The 'Save & Apply to Device' button is highlighted with a red box and arrow labeled '4'. The 'Policy ACL' tab is also highlighted with a red box.

Step6 Verification on the controller.
Navigate to Monitoring > Wireless > Clients

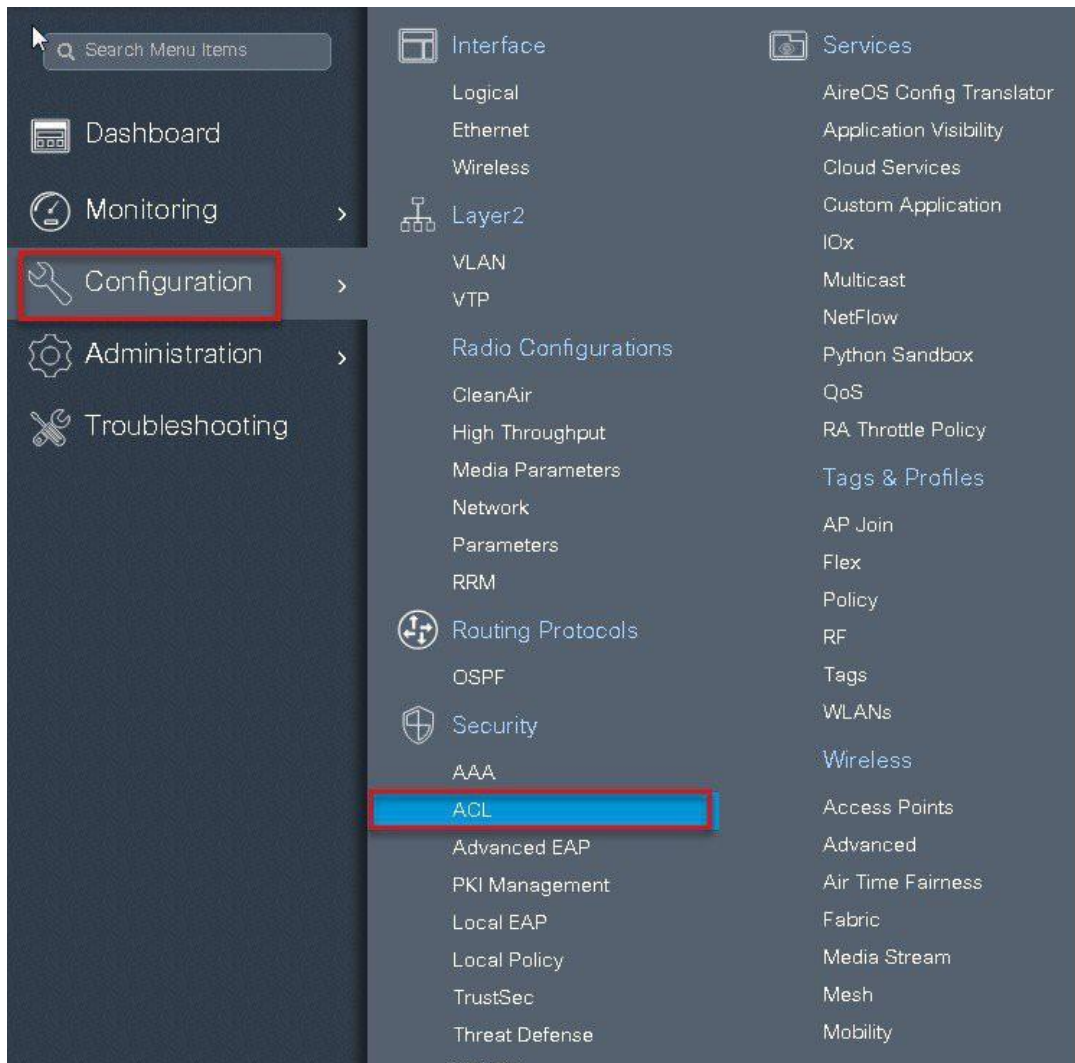
The screenshot displays the Cisco WLC interface for client configuration. On the left, the 'Clients' tab is active, showing a table with columns for Client MAC Address, IPv4/IPv6 Address, and AP Name. A red arrow points to the MAC address '1c:36:bb:ef:64:92', which is enclosed in a red box with the text 'click on Mac address' below it. On the right, the 'Client' configuration page is shown, with the 'Security Information' tab selected. This tab contains sections for 'Local Policies', 'Server Policies', and 'Resultant Policies'. In the 'Server Policies' and 'Resultant Policies' sections, the 'Filter-ID' field is highlighted with a red box and contains the value '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 the ACL works.

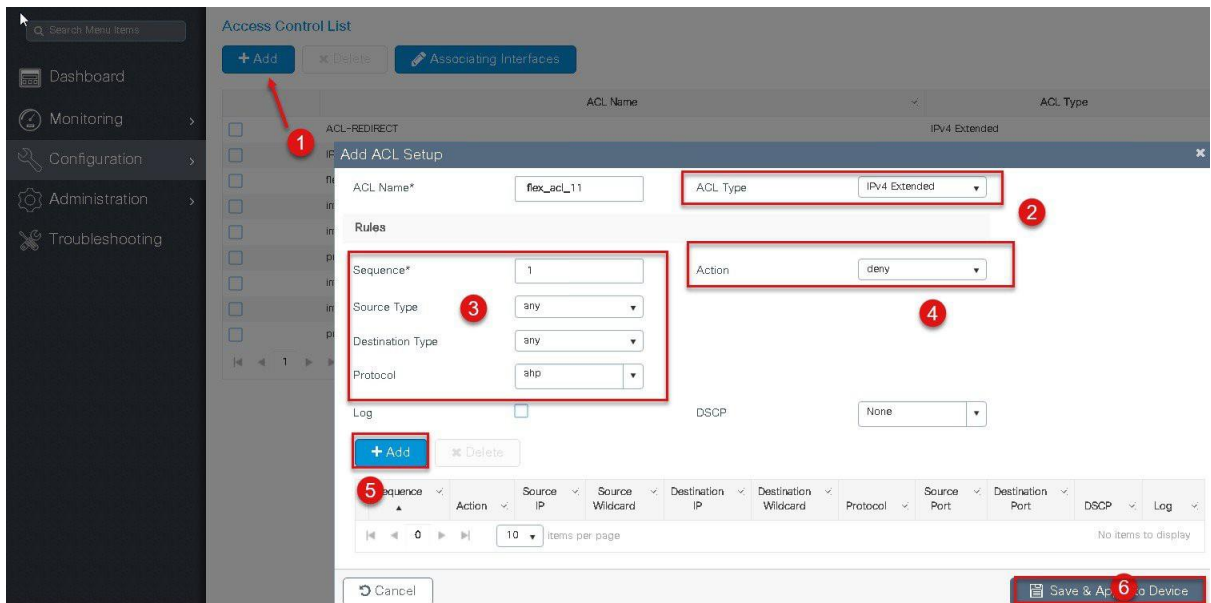
Procedure

Step1 Create an ACL on the WLC by navigating to Configuration > Security > ACL.



Step2 Perform the steps below:

- Click on Add to create an ACL, 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



Step3 Refer the steps in the procedure of 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 ✕

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*

Description

Status **ENABLED**

Passive Client DISABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

WLAN Switching Policy

Central Switching	<input type="checkbox"/>
Central Authentication	<input checked="" type="checkbox"/>
Central DHCP	<input type="checkbox"/>
Central Association	<input type="checkbox"/>
Flex NAT/PAT	<input type="checkbox"/>

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

VLAN

VLAN/VLAN Group

Multicast VLAN

WLAN ACL

IPv4 ACL

IPv6 ACL

URL Filters

Pre Auth

Post Auth

Step4 Assign the ACL on the Flex profile, by mapping the VLAN and ACL.
Define the native VLAN for the flexconnect AP's.

Add Flex Profile

General Local Authentication Policy ACL VLAN

Name*

Description

Native VLAN ID

HTTP Proxy Port

HTTP-Proxy IP Address

CTS Policy

Inline Tagging

SGACL Enforcement

CTS Profile Name

Multicast Overridden Interface

Fallback Radio Shut

Flex Resilient

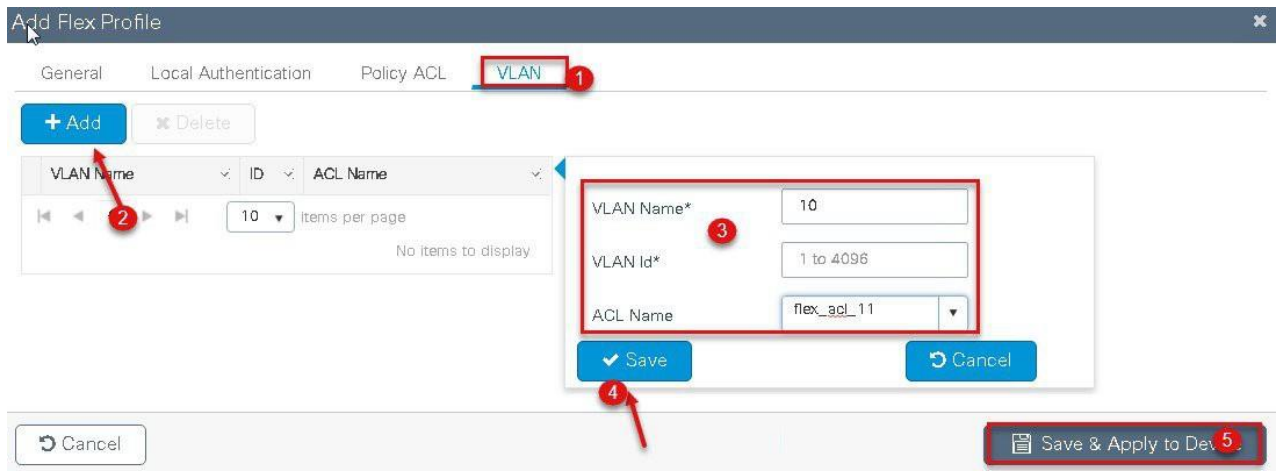
ARP Caching

Efficient Image Upgrade

Office Extend AP

Join Minimum Latency

Step5 Define the VLAN and ACL mapping on the flex profile.



Client ACL overview

- This feature allows application of 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 AP's that has 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 AAA

For the creation of ACL refer the steps in the WLAN ACL use case .Refer the step5 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 the procedure section of the VLAN override Use case Flexconnect VLAN override

Procedure

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

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

DACL Name

ACL (Filter-ID) .in

Security Group

VLAN

Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
Filter-ID = flex_acl_12.in

Step2 verification of ACL getting enforced on the AP and WLC .
Navigate to Monitor > wireless > Clients

The image shows two screenshots from the Cisco Prime Network Manager interface. The left screenshot shows the 'Clients' page with a table of client information. A red arrow points to the MAC address '1c:38:bb:ef:64:92' with a callout box that says 'click on Mac address'. The right screenshot shows the 'Client' details page, with the 'Security Information' tab selected. This tab displays various policy settings, including 'Local Policies', 'Server Policies', and 'Resultant Policies'. Red boxes highlight the 'Filter-ID' field in the 'Server Policies' and 'Resultant Policies' sections, both showing the value 'flex_acl_12'.

Limitations

- The use of downloadable ACL is not supported on flex connect local switching , downloadable ACL 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 as ACL failure.
- In case of the Local authentication the client will be Deauthenticated 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 preimage download to work the controller should be 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

Step1 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
```

Step2 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     : 0
  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 : 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          16.10.1.33        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 : 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    16.10.1.33          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#
```

Step3 After the AP has been reset, using 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 packages 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 systems is rebooted ,use the following CLI to have the changes persist across reboot.

“Install Commit“

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

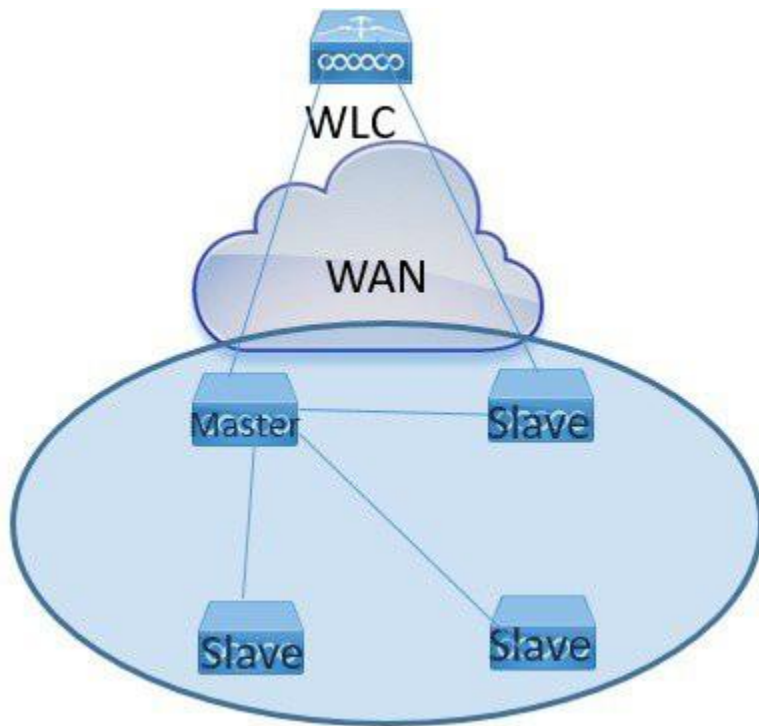
The Controller needs to be install mode for the AP pre-image to work, if a controller works in bundle mode it needs to be converted to install mode. Please refer cisco.com for the conversion for bundle mode to install mode.

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 Master/Server, and the rest of the APs of the same model will work as

Slave/Client and will pre-download the AP image from the master. 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.



Summary

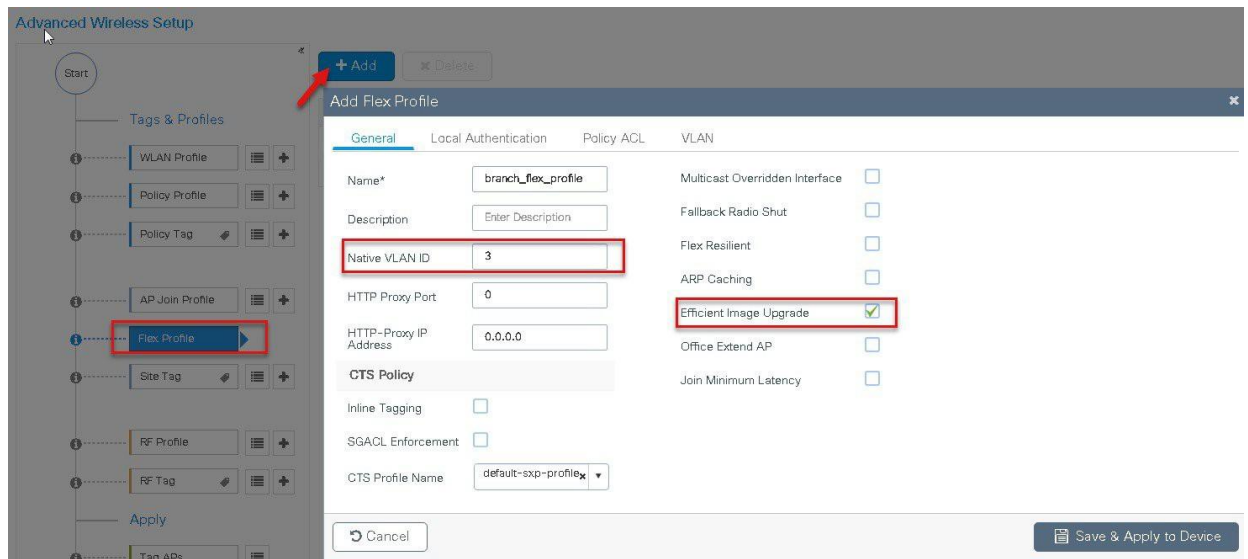
- Master and Slave APs are selected for each AP Model per site tag
- Master downloads image from WLC
- Slave downloads image from Master AP using tftp
- Reduces downtime and saves WAN bandwidth
- The master is chosen by the system , the AP with the lowest mac among the same type and model is to become a master

Procedure

Procedure

-
- Step1** For steps to create a flex profile and to have it applied on the AP , refer the steps in the Advanced config wizard of the document at Advanced wireless setup wizard

Enable smart AP image upgrade on the flex profile.

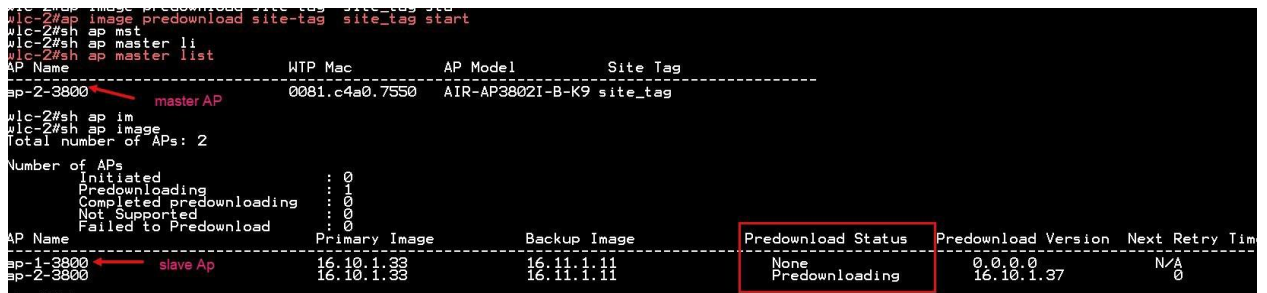


Step2 Download the image on the controller as outlined in step1 of the AP image pre-download process. Issue the CLI below to initiate the smart ap image upgrade and also to see the master AP elected for a given type of AP and the also master downloading image from the controller.

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.



Step3 After the image predownload 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 reboot

```
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 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 : 3
  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 master AP and the decision on who the master 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 master 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 supports 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 play 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

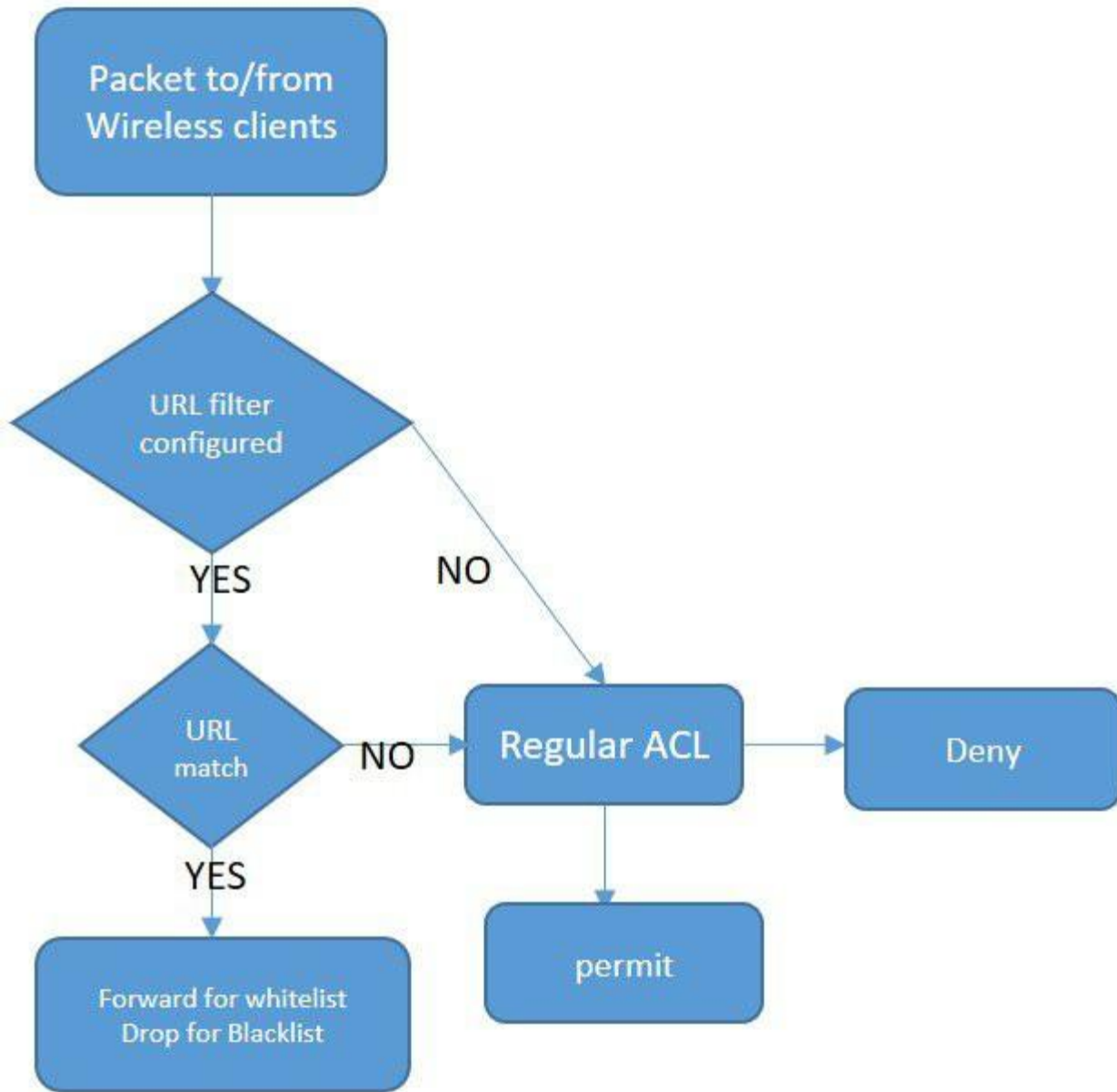
Pre-auth ACL refers to a state when a wireless client would require access to resources prior to getting authenticated. In case of the LW/CWA or BYOD the client might require access to resources before getting full access into the network. The URL filtering for flex is supported only on the Wave 2 platforms. The url filtering follows a whitelist and black 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, 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 white listing or blacklisting. 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.

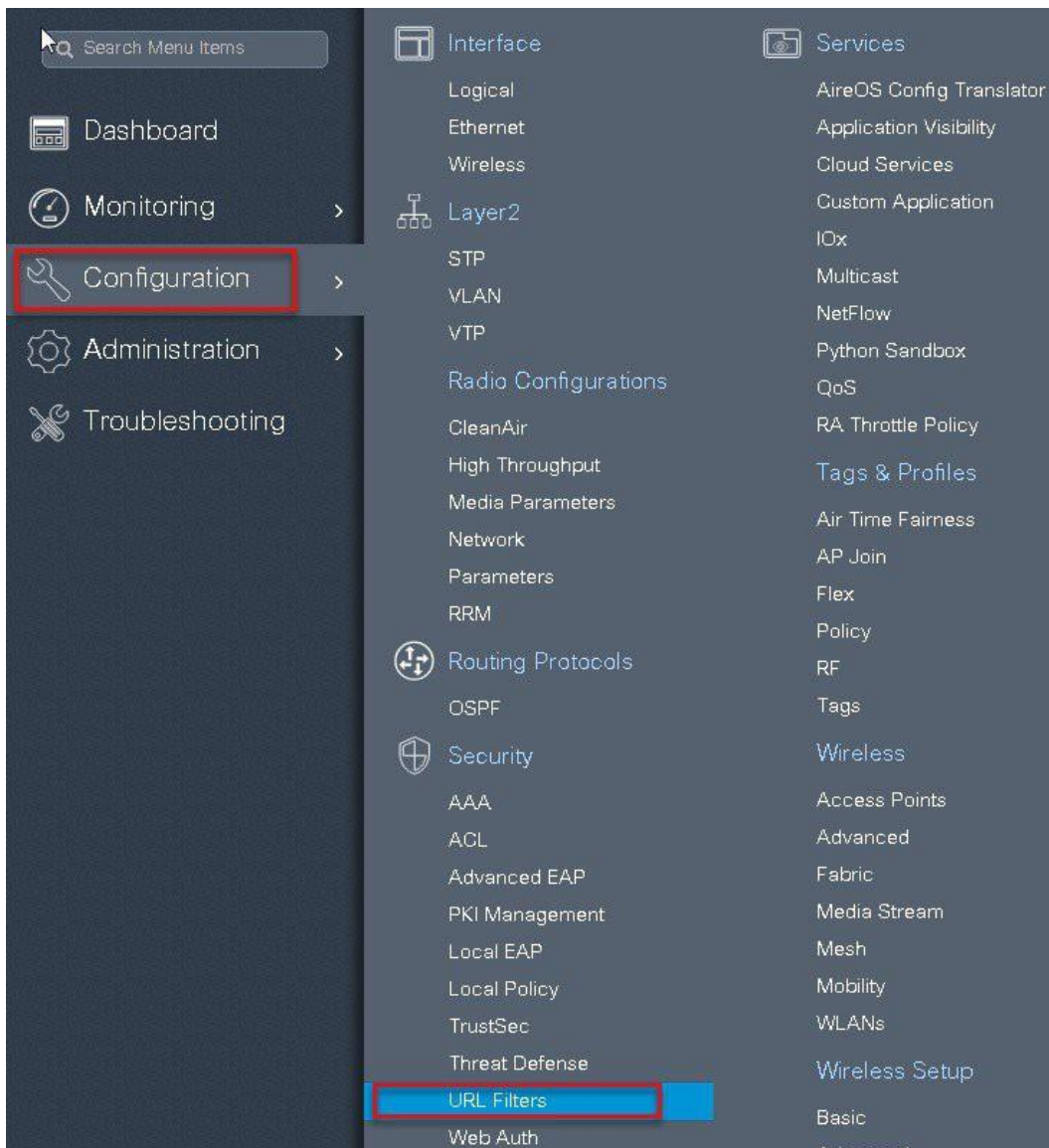


LWA flow with URL filter

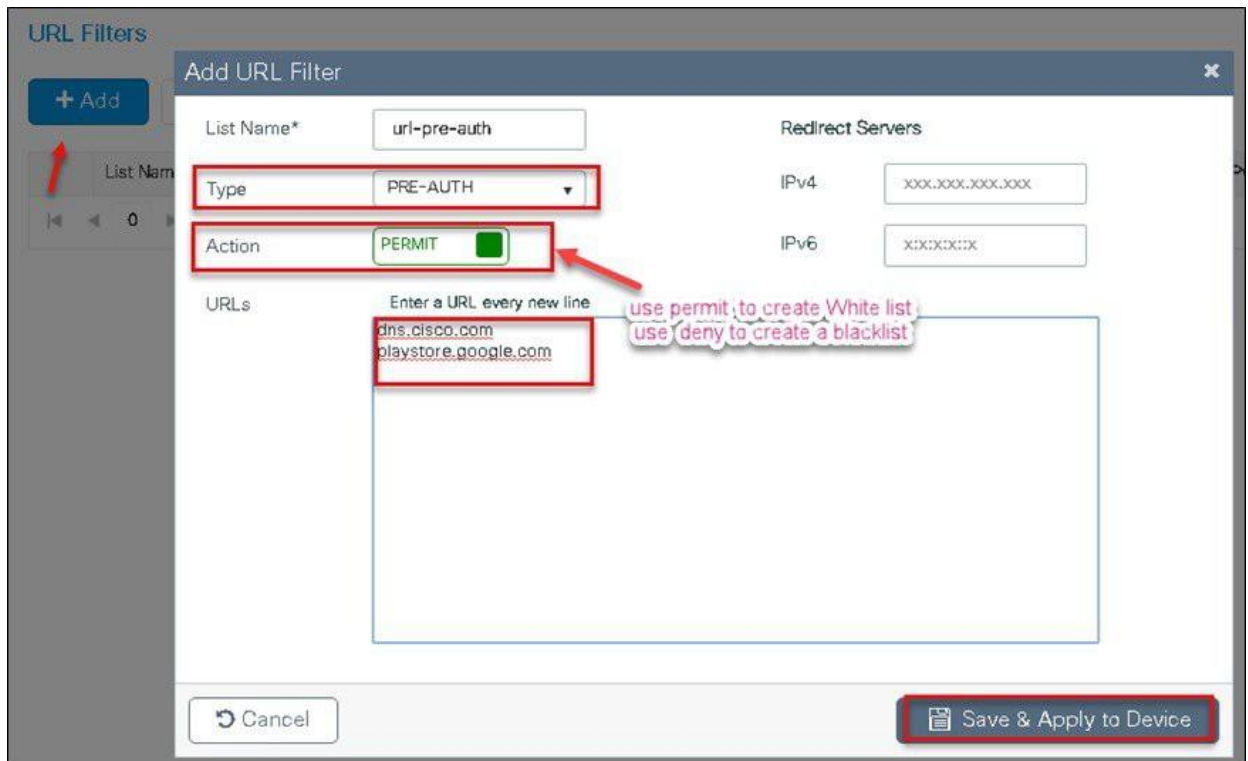
This section describes the steps to set up LWA with pre-auth ACL and URL filter, for the local web authentication the pre-auth ACL and URL filtering is optional.

Procedure

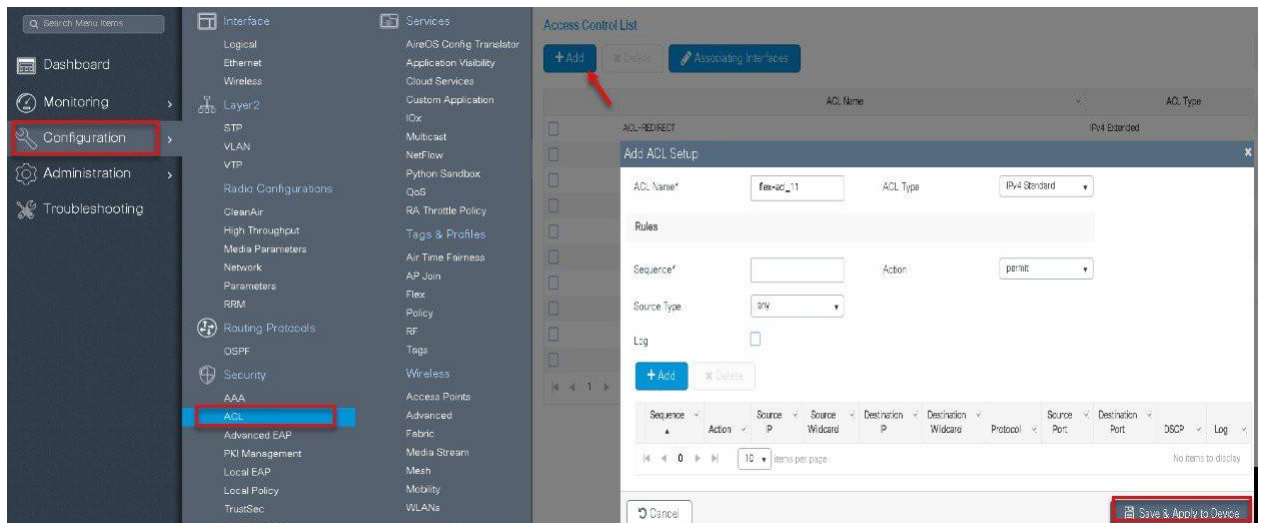
Step1 To create a URL filter navigate to Configuration > security and URL filters.



Step2 Create a URL filter.



Step3 Create an ACL on the WLC to link with the URL ACL.



Step4 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

Authentication Authorization and Accounting

+ AAA Wizard

AAA Method List Servers / Groups AAA Advanced

+ Add

RADIUS

1 TACACS+

LDAP

Create AAA Radius Server

Name* freerad

IPv4 / IPv6 Server Address* 9.1.0.21 2

PAC Key

Key*

Confirm Key*

Auth Port 1812

Acct Port 1813

Server Timeout (seconds) 1-1000

Retry Count 0-100

Support for CoA ENABLED

Cancel Save & Apply to Device 3

Authentication Authorization and Accounting

+ AAA Wizard

AAA Method List Servers / Groups AAA Advanced

+ Add Delete

RADIUS

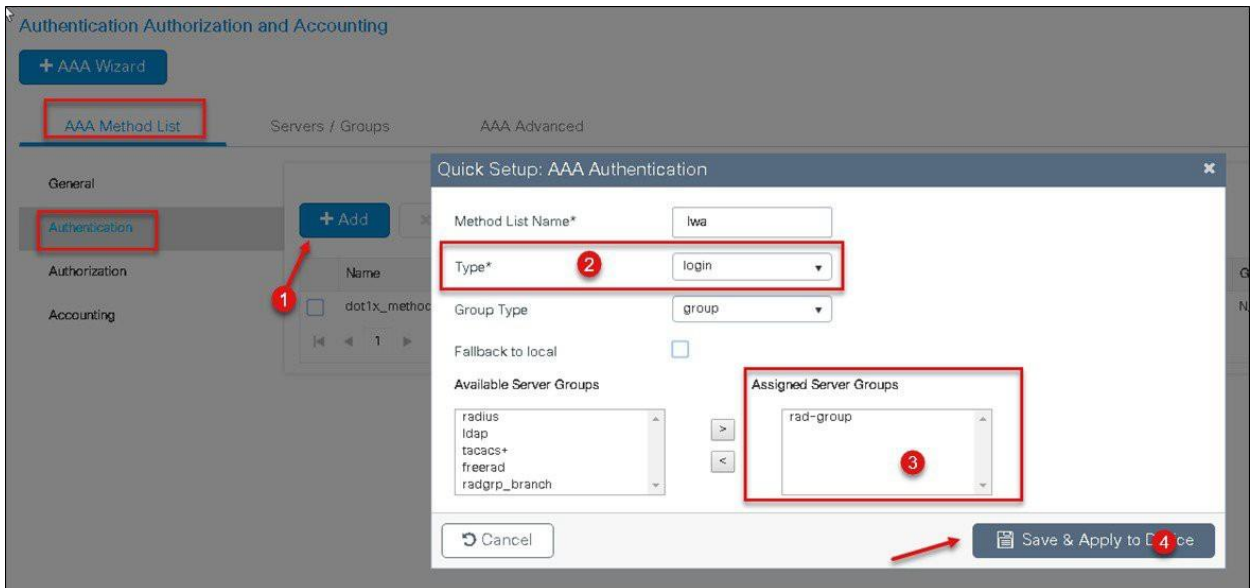
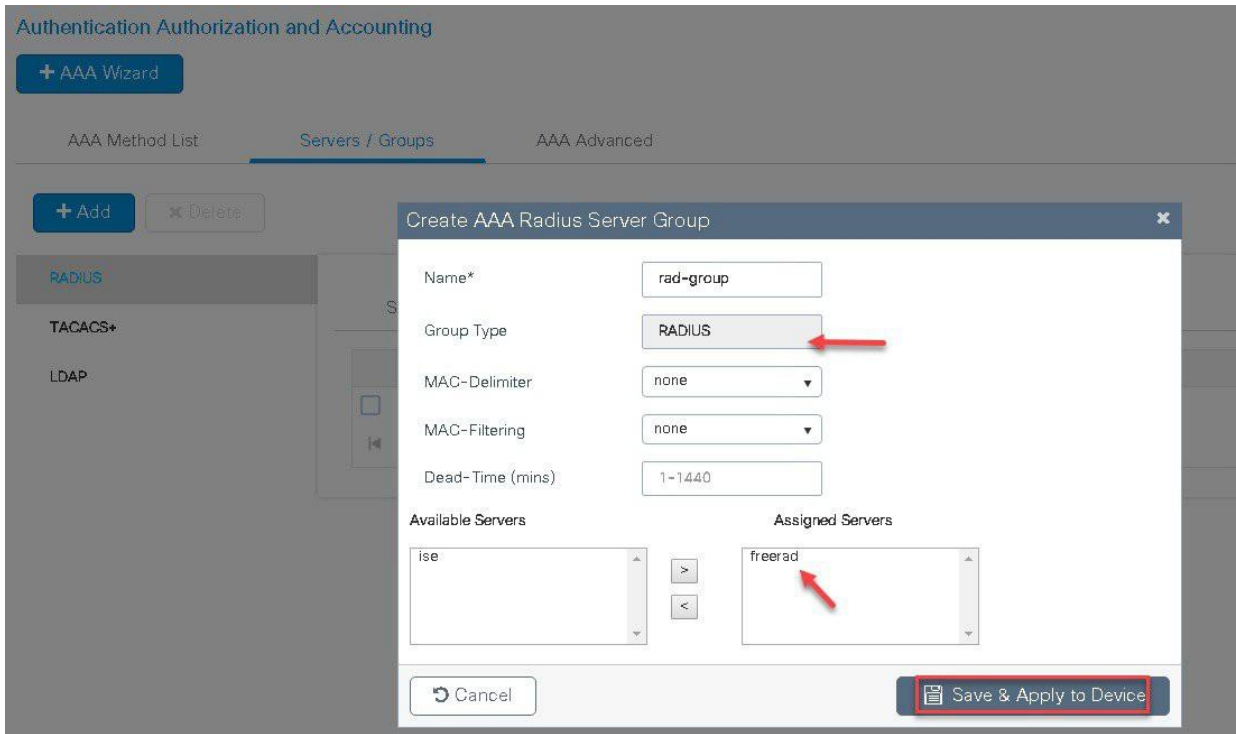
TACACS+

LDAP

Servers Server Groups

Name	Server 1	Server 2	Server 3
<input type="checkbox"/> ise	ise	N/A	N/A

10 items per page



Step5 Create a WLAN to local web-authentication flow.
 Navigate to Configuration > Tags& profiles > WLAN.

WIRELESS NETWORKS

+ Add × Delete

Number of WLANs selected : 0

- Name
- open_wlan
- dot1x_wlan

1 10

Add WLAN

General Security Advanced

Profile Name* wlc-lwa Radio Policy All

SSID wlc-lwa Broadcast SSID ENABLED

WLAN ID* 2

Status ENABLED

Cancel Save & Apply to Device

Add WLAN

General Security Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode None

MAC Filtering

Fast Transition Adaptive Enabled

Over the DS

Reassociation Timeout 20

Cancel Save & Apply to Device

Add WLAN

General Security Advanced

Layer2 Layer3 AAA

Web Policy

Webauth Parameter Map global

Authentication List lwa

Select a value

lwa

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

Show Advanced Settings >>>

click on Advanced Settings

Cancel Save & Apply to Device

Add WLAN

<< Hide

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

Preauthentication ACL

IPv4 flex_acl_11

IPv6 none

Cancel Save & Apply to Device

Step6 Create a policy profile.

Policy Profile

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*

Description

Status **ENABLED**

Passive Client **DISABLED**

Encrypted Traffic Analytics **DISABLED**

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

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

VLAN

VLAN/VLAN Group

Multicast VLAN

WLAN ACL

IPv4 ACL

IPv6 ACL

URL Filters

Pre Auth

Post Auth

Step7 Create a flex profile.

Navigate to Configuration > Tags & Profiles > Flex

Add Flex Profile

General | Local Authentication | Policy ACL | VLAN

Name*

Description

Native VLAN ID

HTTP Proxy Port

HTTP-Proxy IP Address

CTS Policy

Inline Tagging

SGACL Enforcement

CTS Profile Name

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

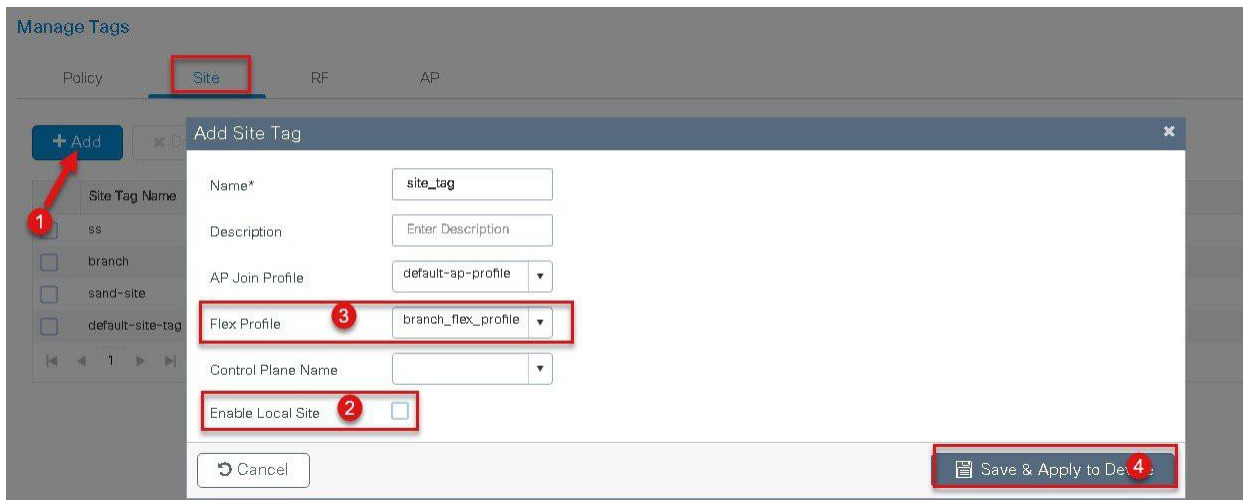
Name*

Description

WLAN Profile Policy Profile

Map WLAN and Policy

WLAN Profile* Policy Profile*



Step9 Map the tags on the AP , Once the AP's are tagged with a policy profile the AP 's will reboot due to conversion from local mode to flex-connect mode.

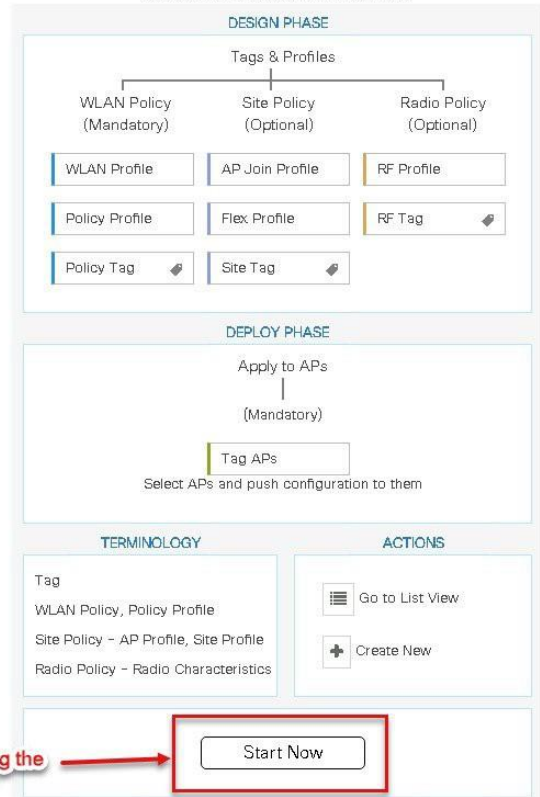
If the AP's are already in flex mode , the reboot wouldn't be triggered .

Navigate to Configuration > Wireless Setup > Advanced

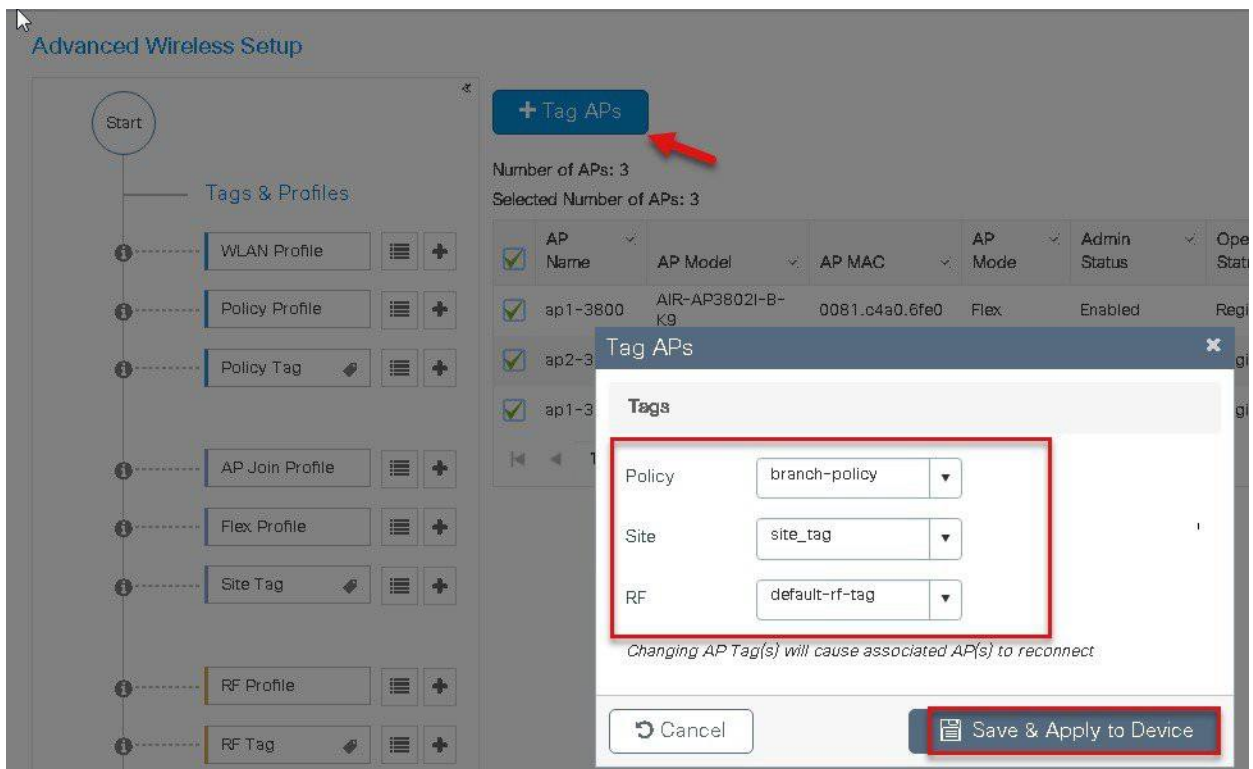
Advanced Wireless Setup

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.



Advanced Wireless Setu



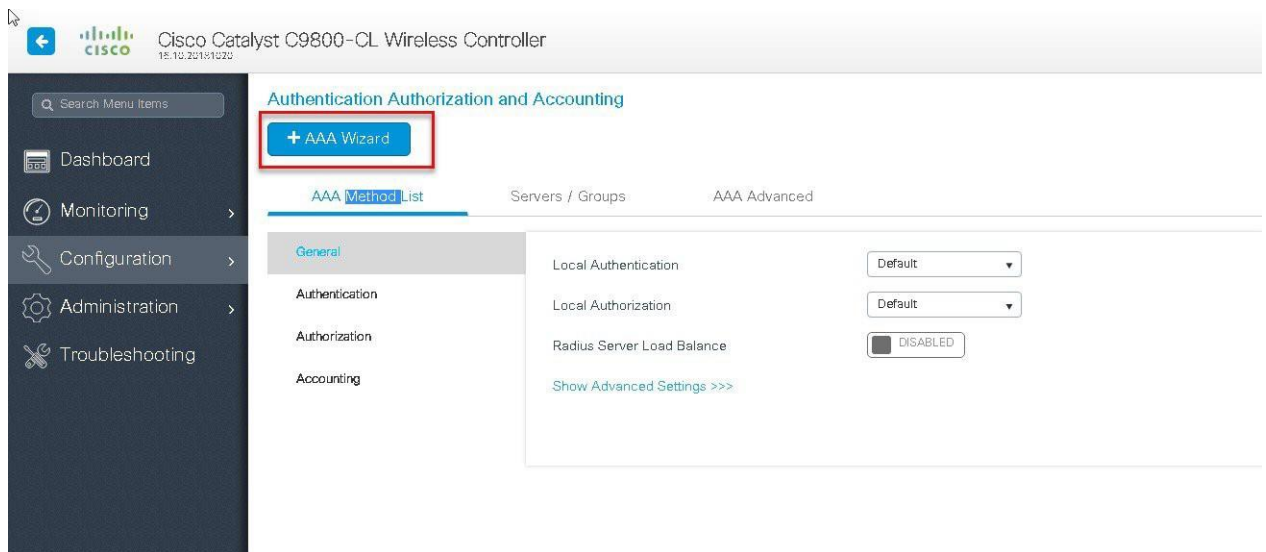
CWA flow on Flex

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

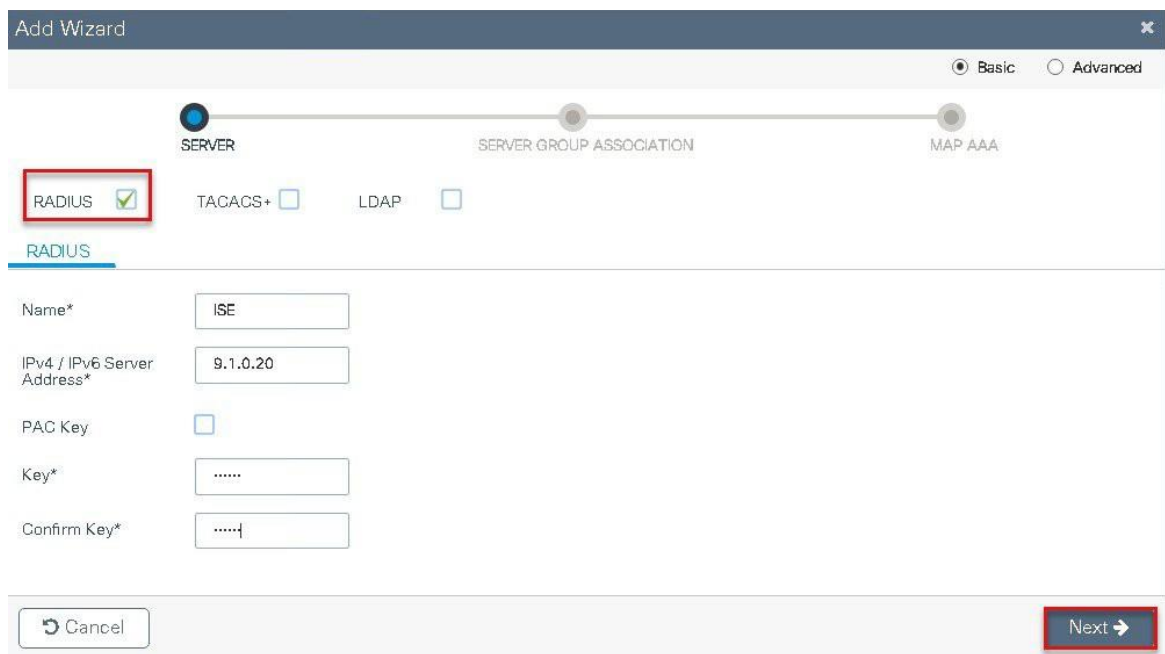
- Create a server and server group for mac auth and AAA attributes
- Create an authorization list on the controller
- Create a MAB SSID and map the authorization list on the SSID
- Create a redirect ACL and a URL filter(optional) on the controller
- Bind the URL filter and ACL on the flex profile
- Create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

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.



Step2 Define a name for the server and specify the IP address and shared secret.



Step3 Create a server group and map the server in the group .

Add Wizard Basic Advanced

SERVER SERVER GROUP ASSOCIATION MAP AAA

RADIUS

Name*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Available Servers

Assigned Servers

Step4 Enable dot1x system control and check mark 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

Local Authentication

Local Authorization

Radius Server Load Balance

[Show Advanced Settings >>>](#)

Step5 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*

Type*

Group Type

Fallback to local

Available Server Groups

- Idap
- tacacs+
- rad-group
- freerad
- radgrp_branch

Assigned Server Groups

- ISE

Step 6 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*

Type*

Group Type

Fallback to local

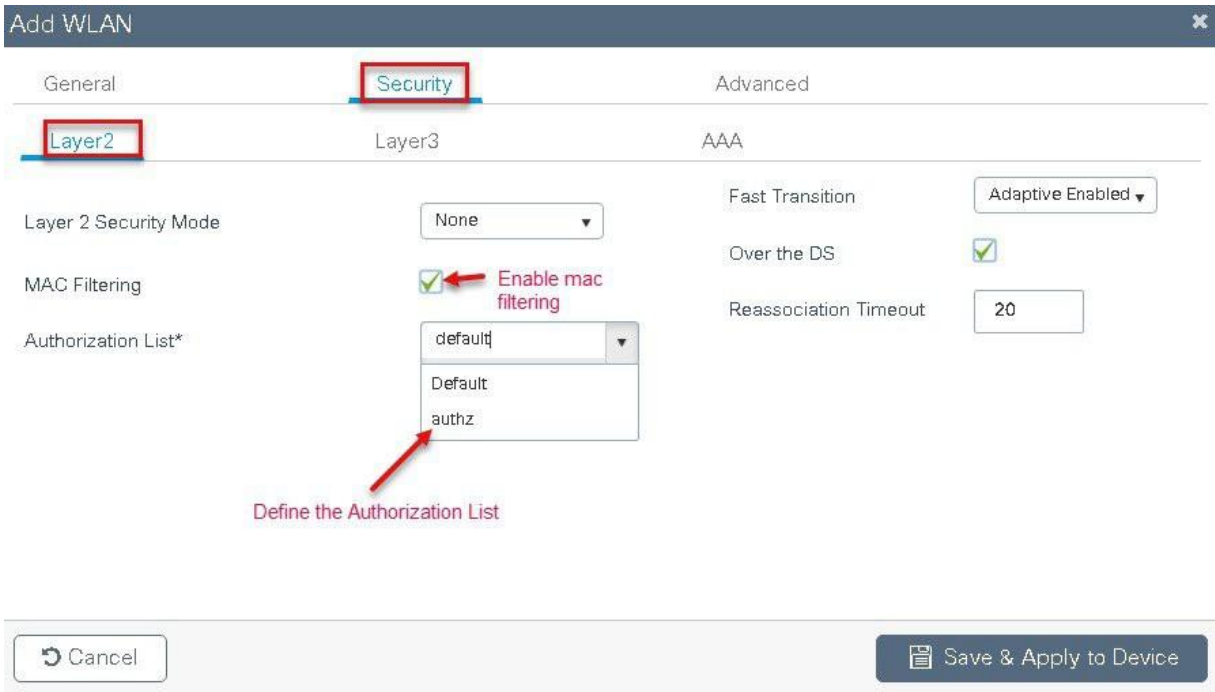
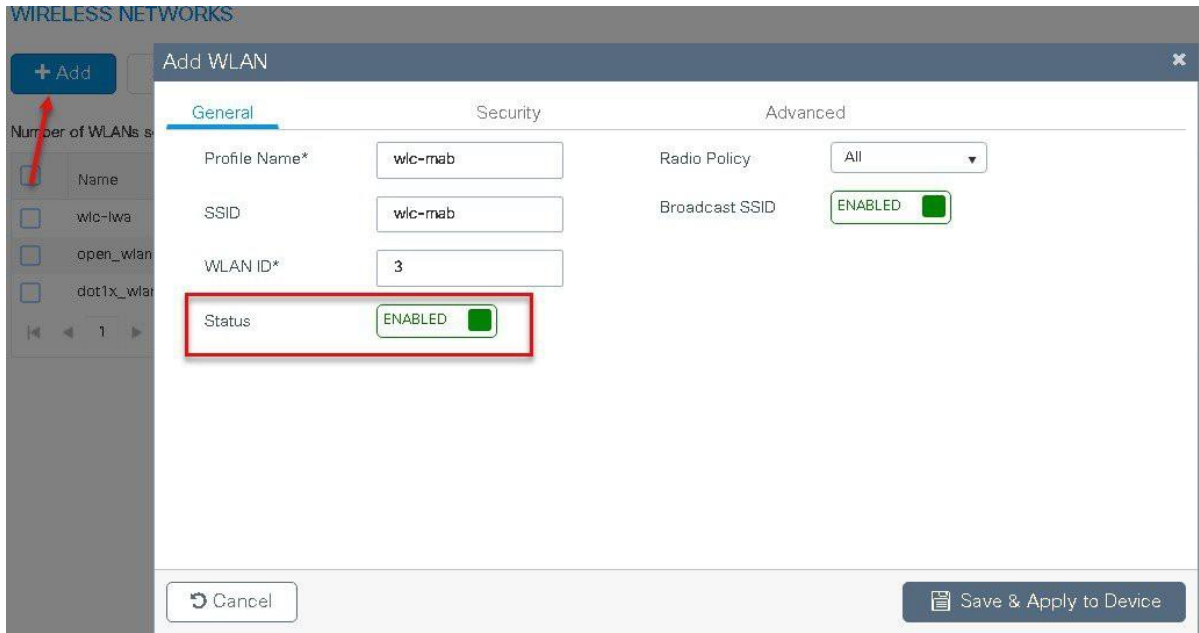
Available Server Groups

- Idap
- 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.



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

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*

Description

Status ENABLED

Passive Client DISABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

WLAN Switching Policy

Central Switching

Central Authentication

Central DHCP

Central Association

Flex NAT/PAT

Cancel | Save & Apply to Device

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

VLAN

VLAN/VLAN Group

Multicast VLAN

WLAN ACL

IPv4 ACL

IPv6 ACL

URL Filters

Pre Auth

Post Auth

Add Policy Profile ✕

General Access Policies QoS and AVC Mobility **Advanced**

WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

DHCP

DHCP Enable

DHCP Server IP Address

[Show more >>>](#)

AAA Policy

Allow AAA Override

NAC State

Policy Name

Accounting List

Fabric Profile

Umbrella Parameter Map

WLAN Flex Policy

VLAN Central Switching

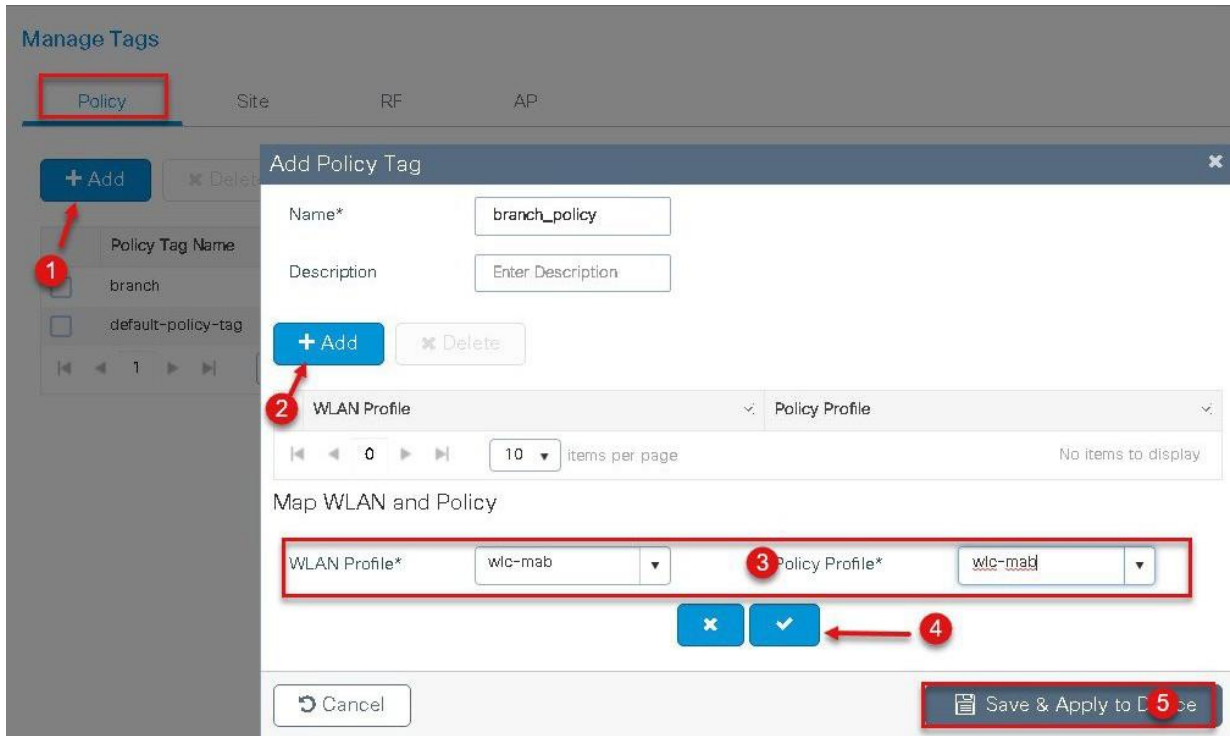
Split MAC ACL

Air Time Fairness Policies

2.4 GHz Policy

5 GHz Policy

Step9 Map the policy profile to the WLAN in the policy tag .
 Navigate to configuration > tags and profiles > tags



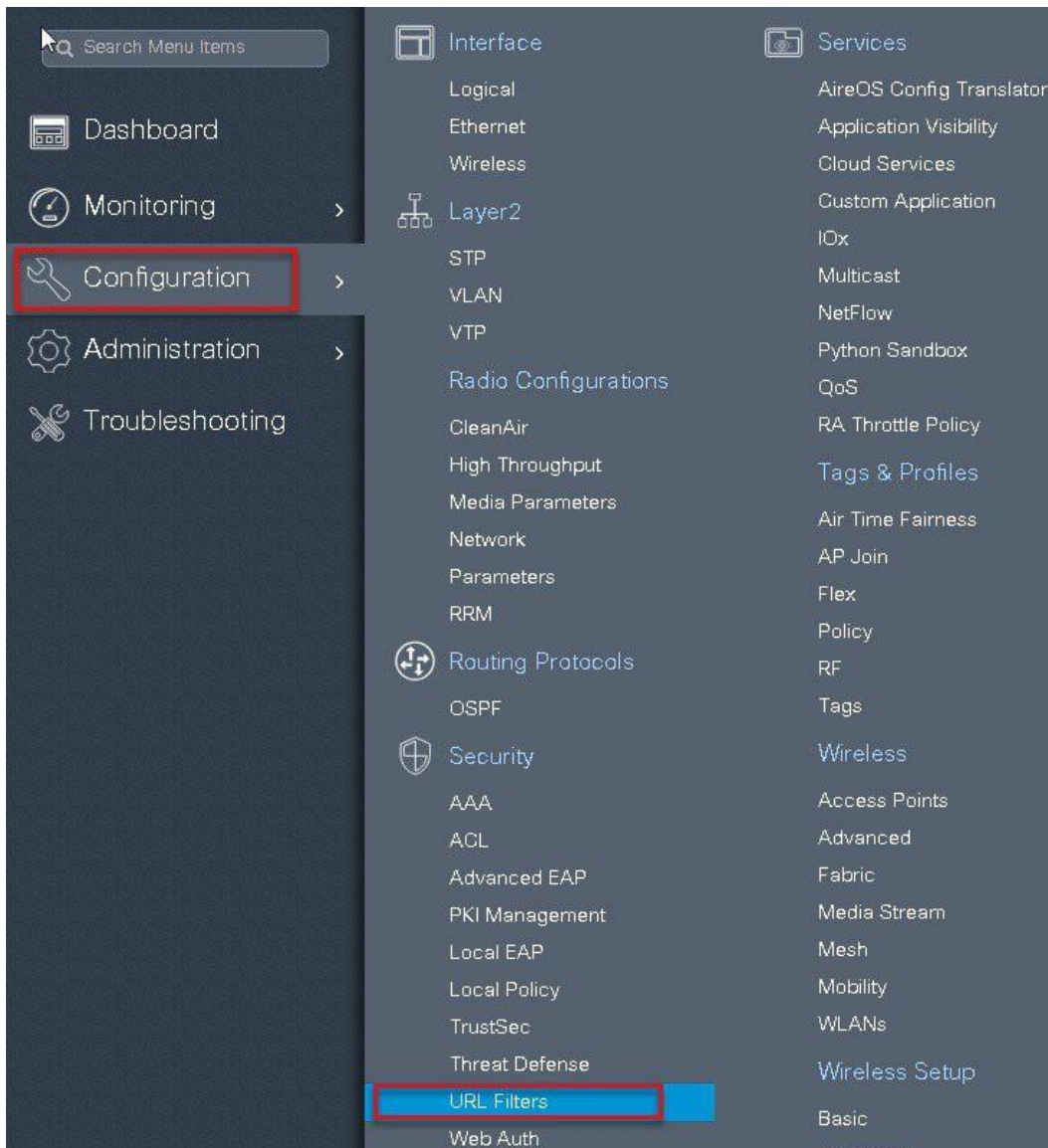
Step 10 Create a redirect ACL and an optional URL filter. The option to create a URL filter depends on access to resources during the pre-auth phase.

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 ← ACL to allow DNS access
deny tcp any any eq domain
remark adding "DHCP ACCESS"
deny udp any any eq bootps any ← ACL to allow DHCP access
deny udp any any eq bootpc
remark adding "ISE ACCESS"
deny ip any host 9.1.0.20 ← ACL to allow ISE ACCESS
deny ip host 9.1.0.20 any
remark adding "rules for redirection"
permit tcp any any eq www ← Punt ACL rules for redirection
permit tcp any any eq 443
  
```

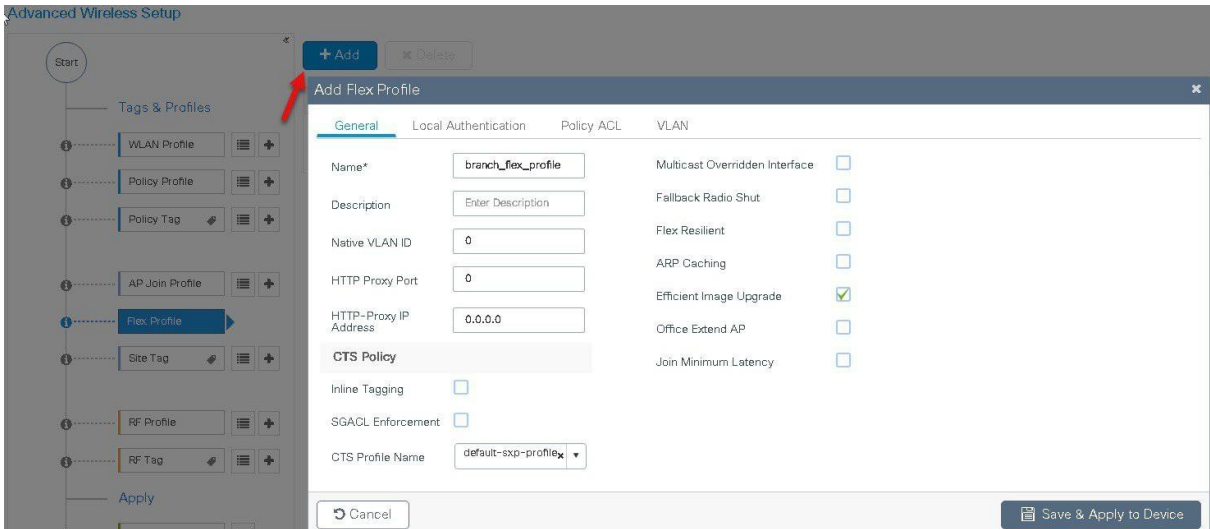
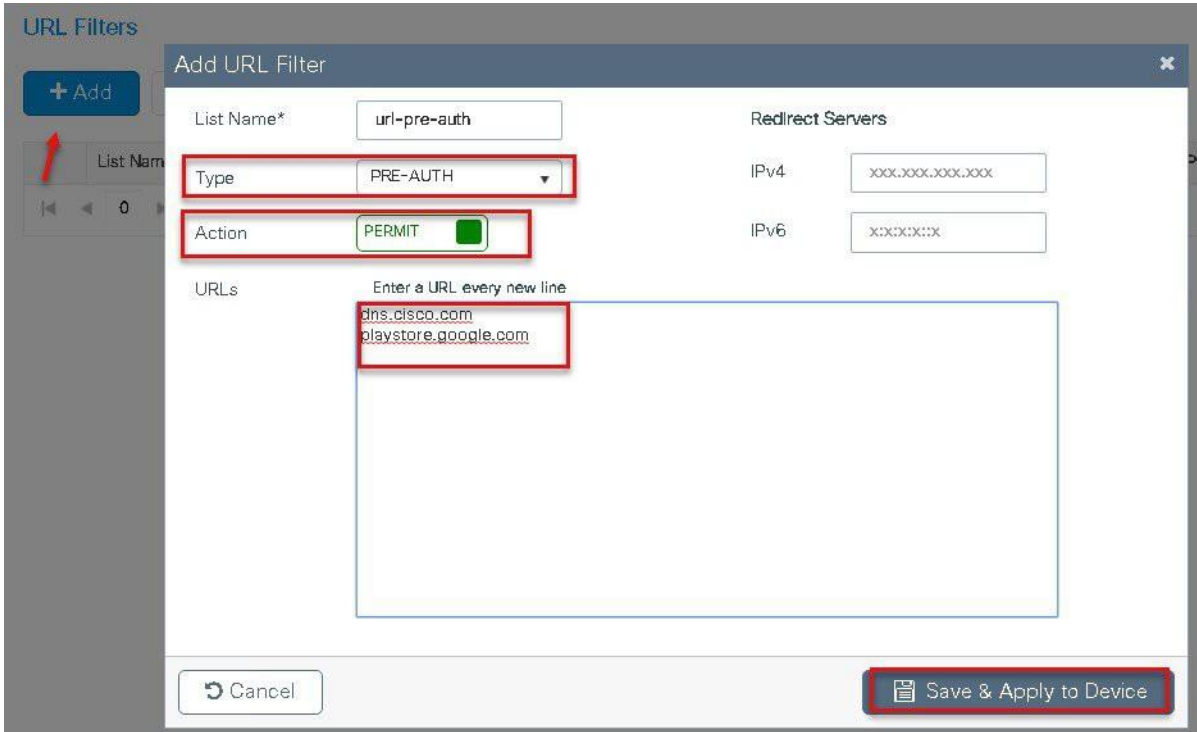
To create a URL filter navigate to Configuration > security and URL filters.

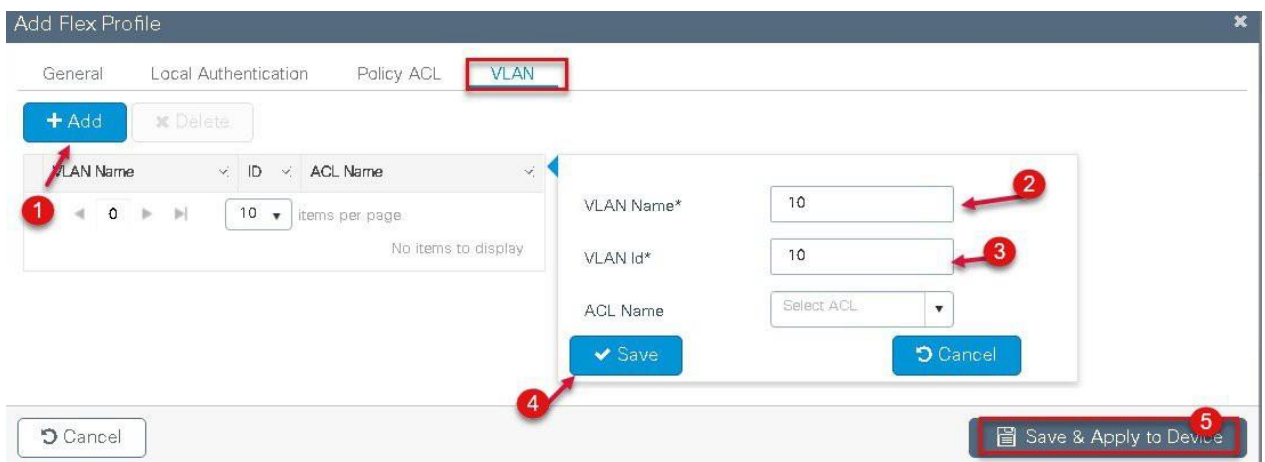
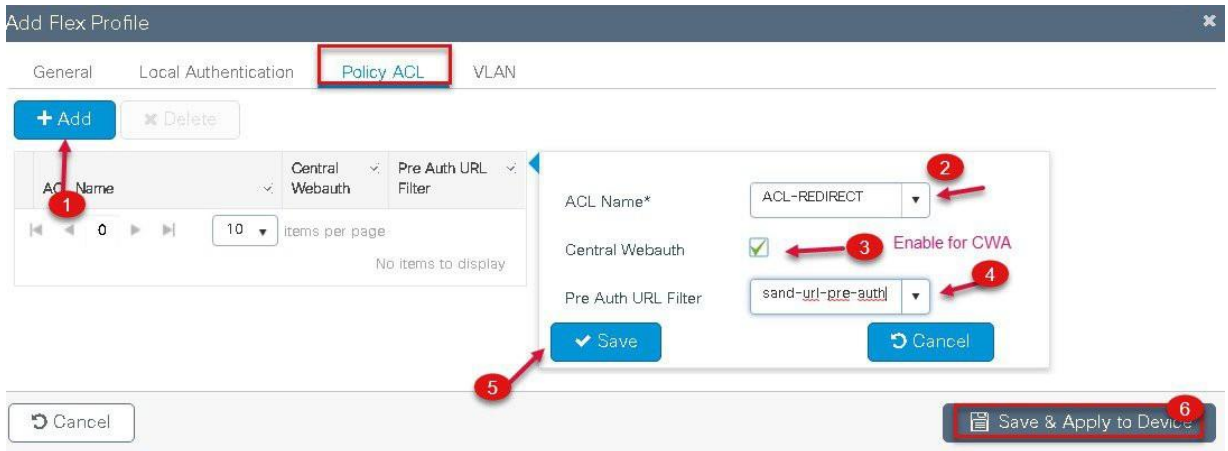


Step11 Create a URL filter.
Permit action creates a whitelist while the deny action creates a blacklist.

Step12 Enable the following on the flex profile.
Navigate to configuration > tags and profiles > flex.

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





Step 13 For assigning the flex profile on the site tag and mapping it on the AP, refer 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 the deployment guide.

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

Voice Domain Permission

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

Value

Display Certificates Renewal Message

Static IP/Host name/FQDN

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

<https://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 wave2 AP's 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 address 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 are limited on a per WLAN basis

Per AP Per WLAN–here the client Association are limited on a per WLAN per AP basis

Per AP radio per WLAN–Client association limited on a per radio per WLAN basis

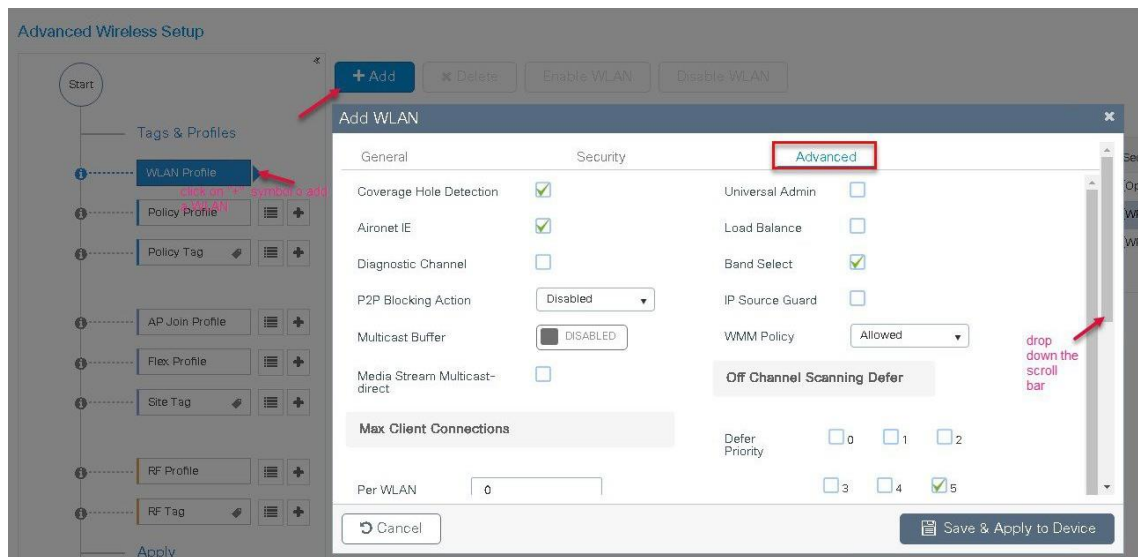
Procedure

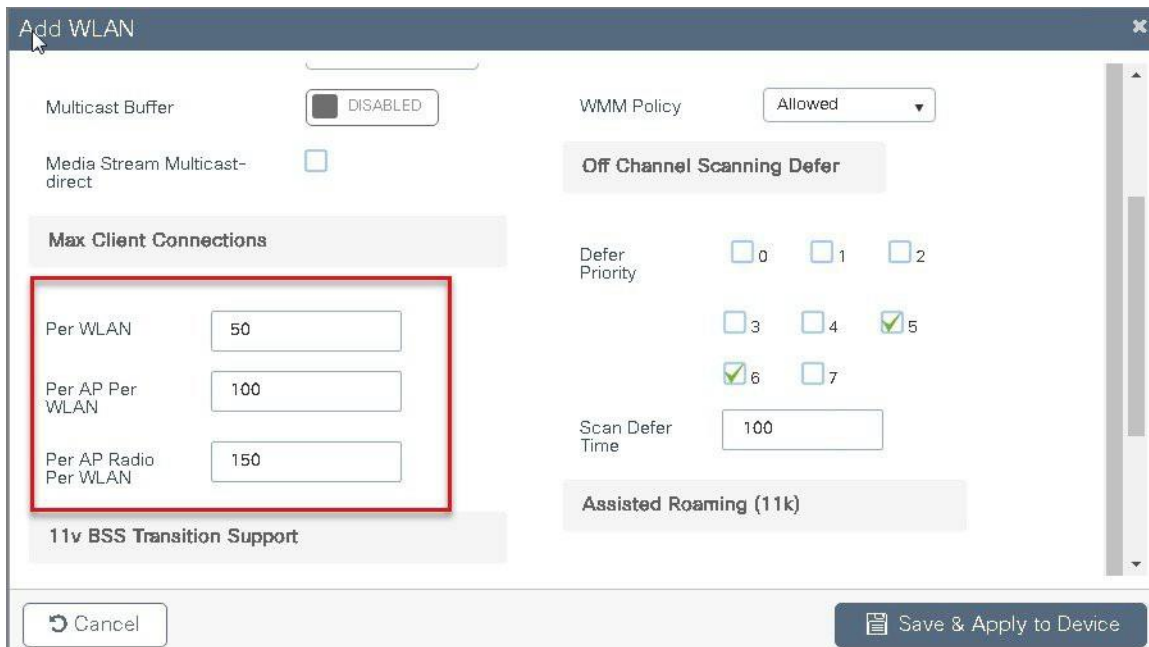
To enable a WLAN please refer the section of setting up the WLAN in the advanced config wizard of this document.

Advanced wireless setup wizard

Procedure

During the WLAN configuration phase enable the feature,





Limitations

This feature does not enforce client limit when the Flex Connect is in 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 Flex Connect 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 to works smoothly both the controller needs to have identical config such as:

- Wlan 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 Wave1 and Wave 2 AP's.

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 recompensates 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 networks multicast and broadcast is send 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 application 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 AP's
- Supported for flexconnect local switching and Central authentication
- With video stream in flex connect 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 the branch network is enabled for multicast. Please refer the cisco.com on enabling multicast on the switching platforms.

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 rather on the wireless controller.

Procedure for enabling Video Stream

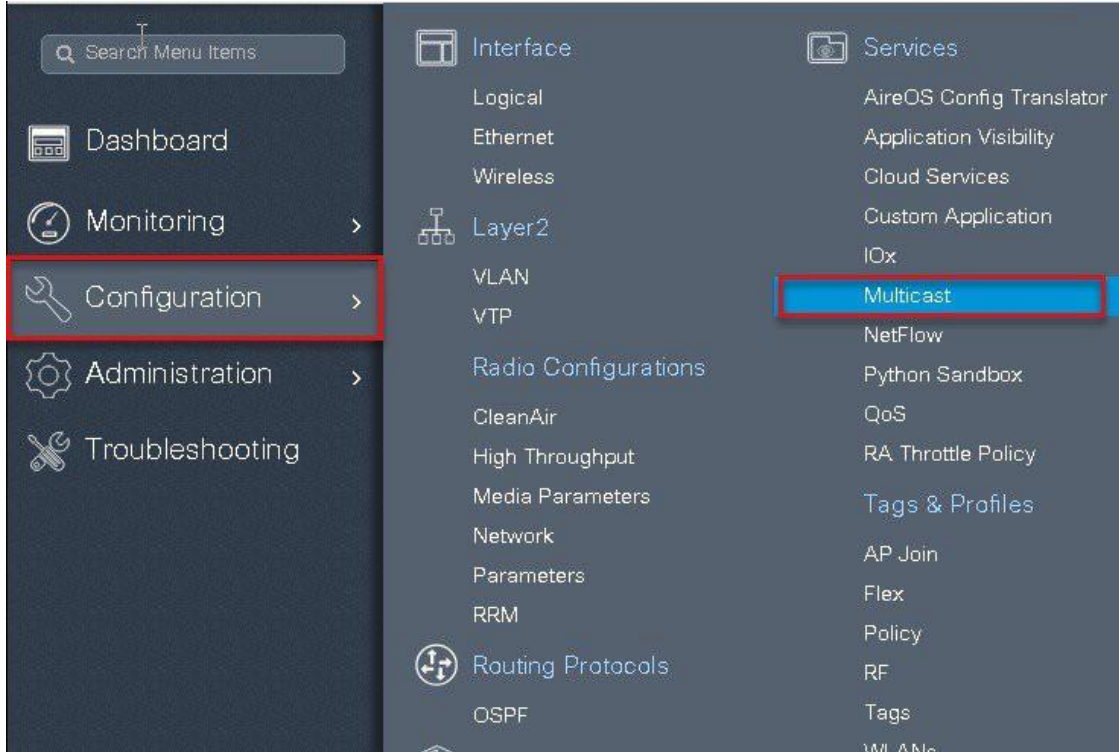
: The steps here includes only the changes to enable video stream

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

Procedure

Step1 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

MLD Snooping DISABLED

IGMP Snooping Querier ENABLED

IGMP Snooping ENABLED

Last Member Querier Interval (milliseconds)

IGMP Snooping

Disabled		
Status	VLAN ID	Name
No Vlan available		
<input type="button" value="Enable All"/>		

Enabled		
Status	VLAN ID	Name
<input checked="" type="checkbox"/>	1	default
<input checked="" type="checkbox"/>	4	VLAN0004
<input checked="" type="checkbox"/>	15	VLAN0015
<input type="button" value="Disable All"/>		

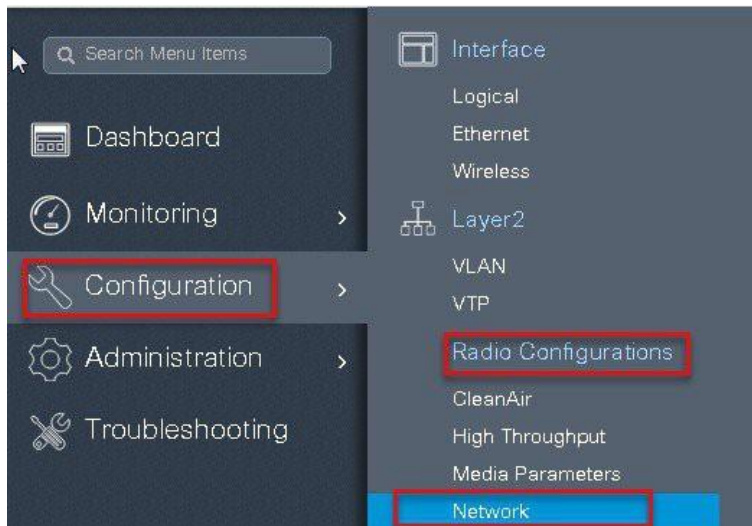
Step2

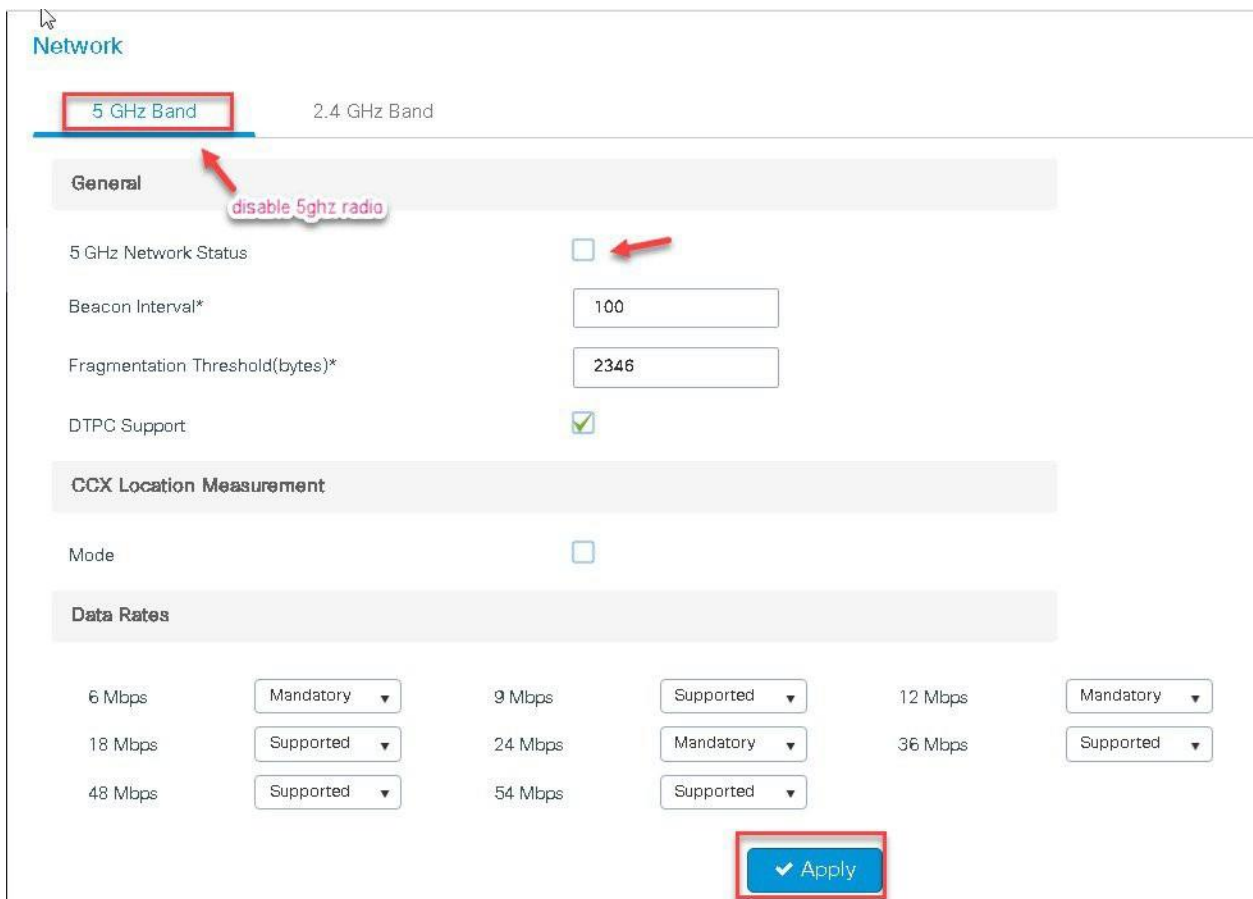
Enable media stream on the Dot11 interface.

Disable the appropriate radio interface before enabling the media stream

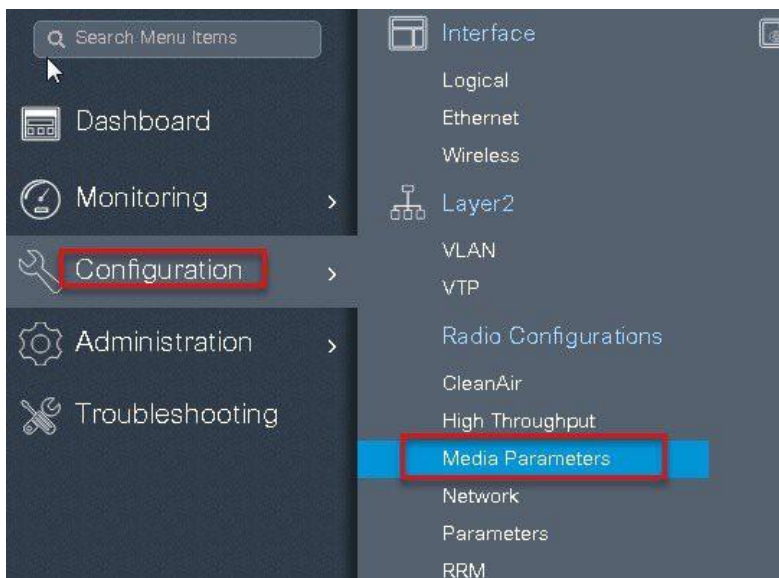
Navigate to Configuration > Radio Configurations > Network.

Disable 5ghz or 2.4 ghz radio, in this example we are enabling media stream on 5ghz radio.





Step3 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 (%)*

Maximum Media Bandwidth (%)*

Client Minimum Phy Rate (kbps)

Maximum Retry Percent (%)*

Media Stream - Multicast Direct Parameters

Multicast Direct Enable

Max streams per Radio

Max streams per Client

Inactivity Timeout

Voice

Call Admission Control (CAC)

Admission Control (ACM)

Traffic Stream Metrics

Metrics Collection

Stream Size*

Max Streams*

Inactivity Timeout

Step4 Enable media stream on the WLAN creation page on the advanced TAB, Refer the advanced configuration wizard section for WLAN creation.

Add WLAN

General Security **Advanced**

Coverage Hole Detection

Aironet IE

Diagnostic Channel

P2P Blocking Action

Multicast Buffer

Media Stream Multicast-direct

Max Client Connections

Per WLAN

Universal Admin

Load Balance

Band Select

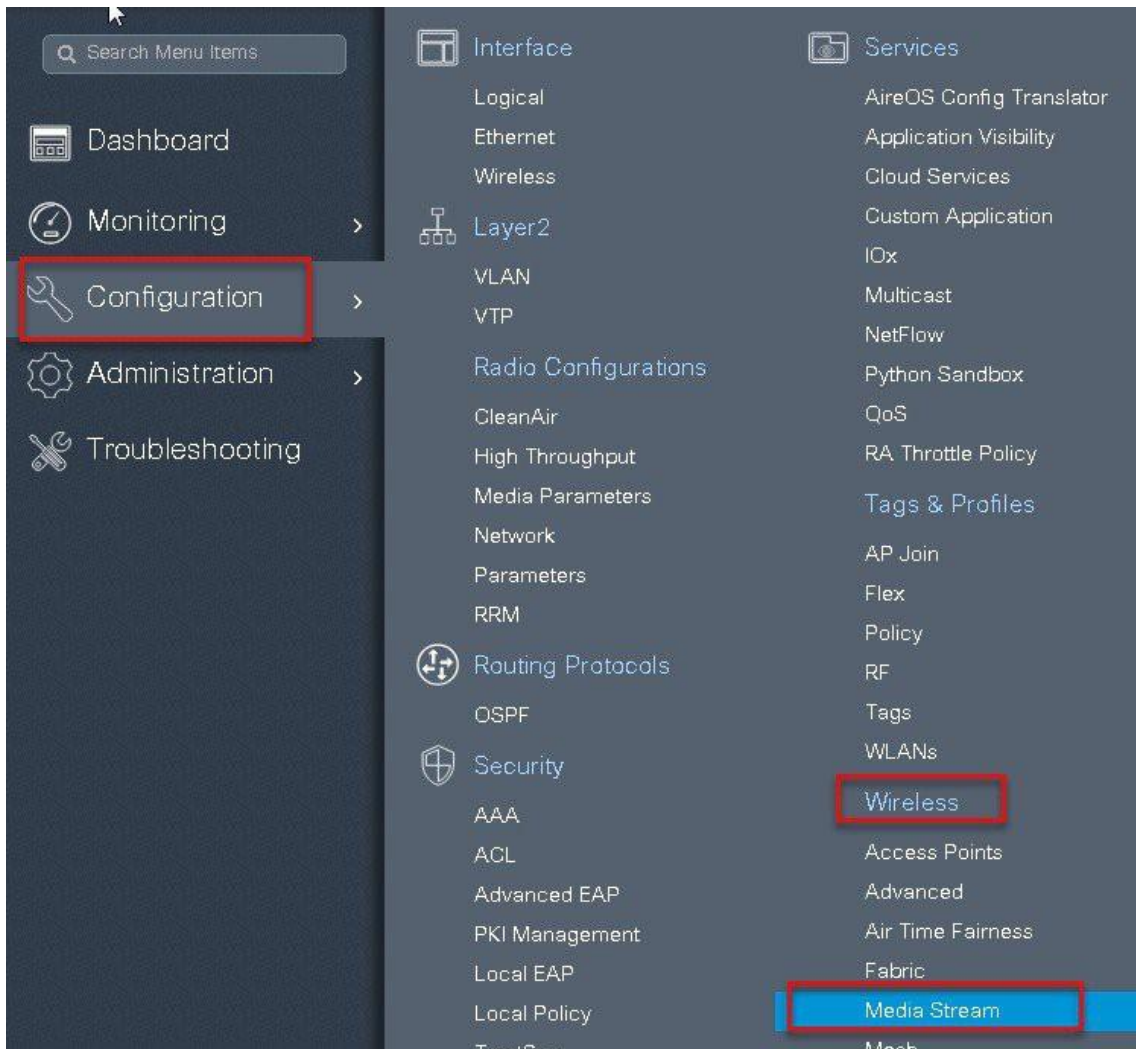
IP Source Guard

WMM Policy

Off Channel Scanning Defer

Defer Priority 0 1 2 3 4 5

Step5 Define the media stream multicast address configuration.
Navigate to wireless > Mediastream



Media Stream

General

Streams

Multicast Direct Enable



Session Message Config

Session Announcement State



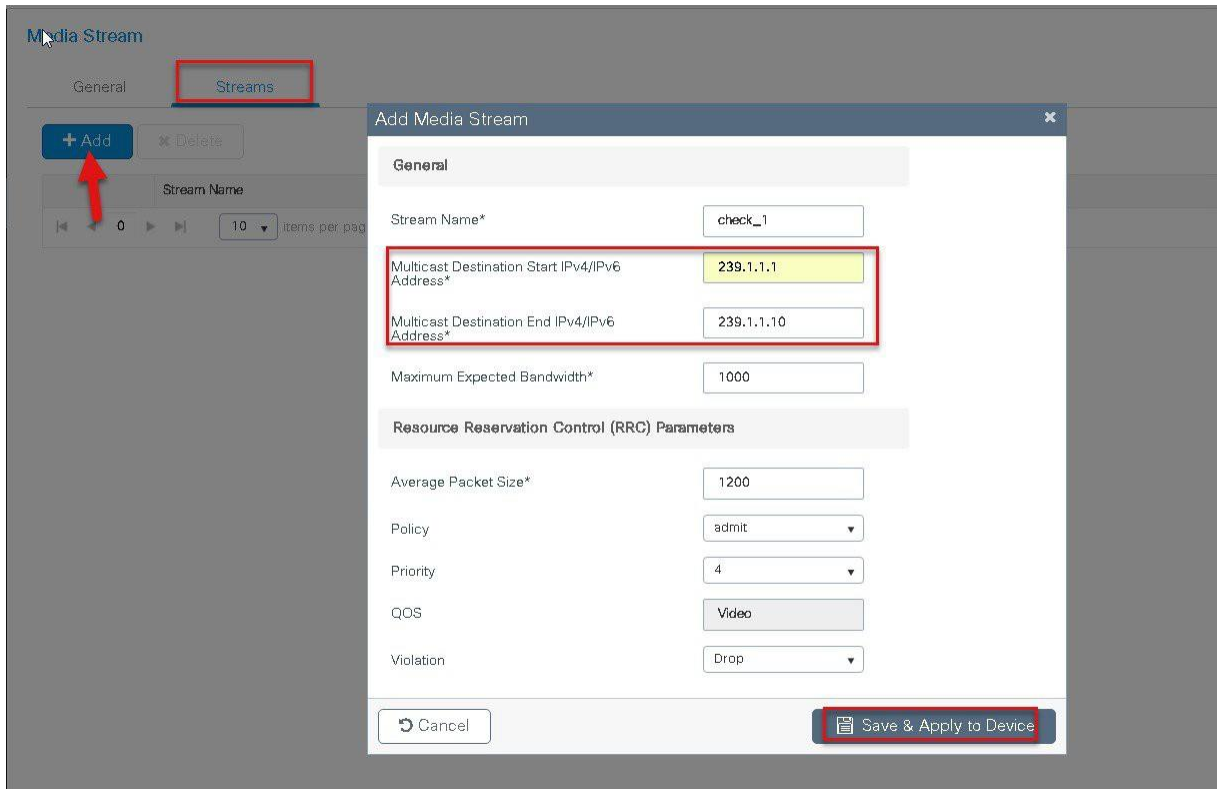
Session Announcement URL

Session Announcement Email

Session Announcement Phone

Session Announcement Note

✓ Apply



Step 6 Enable the dot11 interface on which 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*

Fragmentation Threshold(bytes)*

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 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
```

Glossary

- VLAN—Virtual LAN
- RF—Radio frequency
- FT—Fault Tolerance
- WAVE1 AP—All AP which supports WAVE1 802.11ac (Cisco -3700AP)
- WAVE2 AP – AP which supports WAVE2 802.11ac (Cisco 1800/2800/3800/4800)

- WLC- Wireless LAN controller



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam, The Netherlands

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