

Understand Catalyst 9800 Wireless Controllers Configuration Model

Contents

[Introduction](#)

[Background information](#)

[Policy Tag](#)

[Site Tag](#)

[RF Tag](#)

[List of Settings per Profile](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Network Diagram](#)

[Configurations](#)

[Declare Client's VLANs](#)

[Wizard Based Configuration - Recommended for New 9800 WLC Deployments](#)

[AAA Wizard](#)

[Basic Wireless Setup](#)

[Advanced Wireless Setup](#)

[Menu Based Configuration - Recommended for Existing 9800 WLCs Deployment](#)

[AAA on 9800 WLCs](#)

[WLANs on 9800 WLCs](#)

[AP Join Settings on 9800 WLCs](#)

[RF Profiles on 9800 WLCs](#)

[Verification](#)

[VLANs/Interfaces Configuration](#)

[AAA Configuration](#)

[WLAN Configuration](#)

[AP Configuration](#)

[Tag Configuration](#)

[Profile Configuration](#)

[FAQs](#)

Introduction

This document describes, in detail, the new configuration model of tags and profiles that is available on Catalyst 9800 Series Wireless Controllers. It also provides a walk through the various GUI options - wizard and menu based that are available to design and deploy your 9800 WLC to service SSIDs at multiple sites.

[Video: Basic Configuration of Cisco Catalyst 9800 Series Wireless Controller](#)

Background information

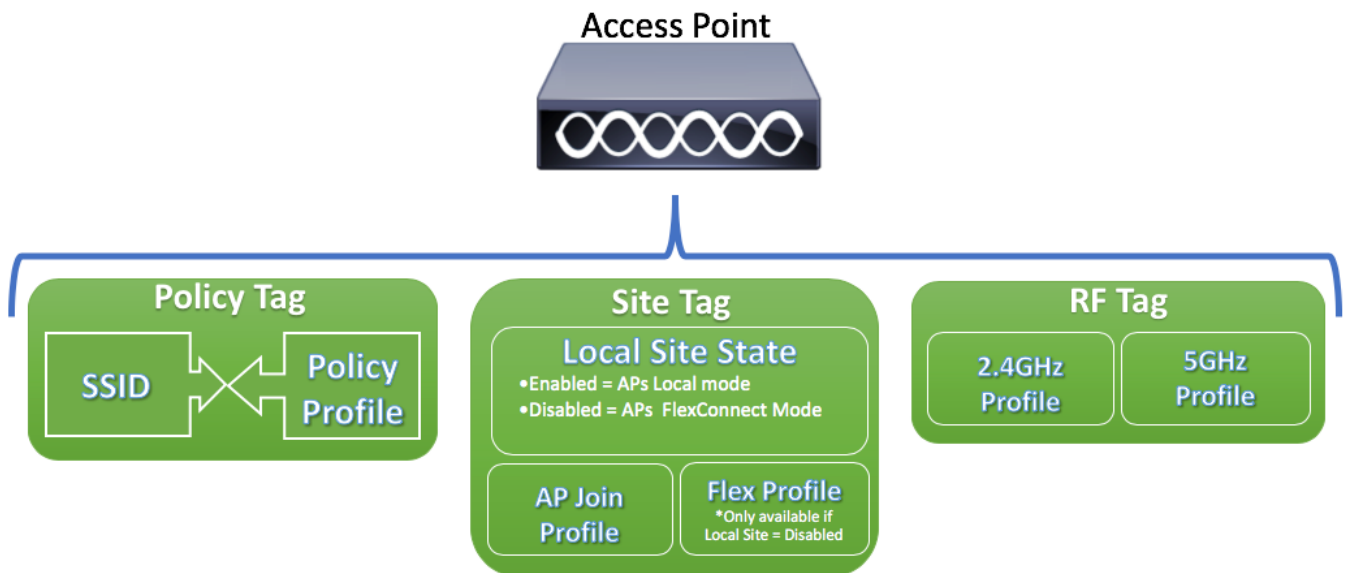
If you are familiar with AireOS Wireless LAN Controllers (WLCs), you are aware of Access Points (APs) and FlexConnect Groups. Those groups allow you to control what capabilities (Ex: which Wireless Local Area Networks [WLANs] or Radio Frequency [RF] profiles) are available for each AP, based on their AP group association.

On 9800 WLCs, tags are used to control the features that are available for each AP. Tags are assigned to every AP and inside every tag, you can find all the settings that were applied to the AP.

There are three tags:

- Policy Tag
- Site Tag
- RF Tag

Visual scheme of an AP configuration:



Policy Tag

Policy Tag is the link between a WLAN Profile [Service Set Identifier (SSID)] and a Policy Profile.



- Policy Profile

Inside a Policy Profile you can specify Virtual Local Area Network (VLAN) ID, If traffic is central or local switching, Mobility Anchors, Quality of Service (QoS), timers, among other settings.

- SSID

Inside a SSID you can specify the WLAN name, Security type for the WLAN, advanced protocols like 802.11k among other settings.

Site Tag

Site Tag defines if the APs are in Local Mode or Flexconnect mode . Other AP modes like Sniffer, Sensor, Monitor, Bridge can be configured directly on the AP. The Site Tag also contains the AP Join Profile and Flex Profile that are applied to the AP.

Note: Flex Profile Setting only becomes available if the Local Site setting is disabled.

Site Tag

Local Site State

- Enabled = APs Local mode
- Disabled = APs FlexConnect Mode

AP Join Profile

Flex Profile

*Only available if
Local Site = Disabled

- AP Join Profile

Inside an AP Join Profile you can specify settings such as Control and Provisioning of Wireless Access Points (CAPWAP) timers, remote access to APs (Telnet/Secure Shell [SSH]), backup controller configuration and others.

- Flex Profile

On a Flex Profile, you have settings such as Address Resolution Protocol (ARP) caching, VLAN/ACL mapping and so on.

RF Tag

Inside an RF tag you can either select any RF profile or select to use the Global RF configuration.

RF Tag

2.4GHz Profile

5GHz Profile

- 2.4 GHz Profile

Allows you to define specific data rates to be used, Transmit Power Control (TPC)

settings, Dynamic Channel Assignment (DCA) and some other Radio Resource Management (RRM) settings for the 2.4GHz band.

- 5GHz Profile

Allows you to define specific data rates to be used, Transmit Power Control (TPC) settings, Dynamic Channel Assignment (DCA) and some other Radio Resource Management (RRM) settings for the 5GHz band.

By default, the APs get assigned the default Tags (Default Policy Tag, Default Site Tag, Default RF Tag) and the default Tags gets assigned the default profiles (Default Policy Profile, Default AP Join Profile, Default Flex Profile).

Note: You can modify all the default settings except for the Default Policy Tag. The Default Policy Tag automatically links any SSID with a WLAN ID from 1 to 16 to the default policy profile and those links cannot be modified.

List of Settings per Profile

If you are familiar with AireOS, you are used to configure all characteristics for an SSID under WLAN configuration. On 9800 WLCs, these settings are split between WLAN Profile and Policy Profile. Also, some of the configuration seen under the Global AP Configuration Page on AireOS GUI has been moved to the AP Join Profile. Here you can find the list of all the settings that you can configure under each profile.

WLAN Profile

- 802.11k
- Band select
- Broadcast SSID
- 802.11v (BSS, DMS, TFS, WNM)
- CCX
- Off Channel Scan Deferral
- Coverage Hole Detection (CHD)
- Client Association Limit
- Diagnostic Channel Capability
- Delivery Traffic Indication Message (DTIM)
- Access Control List (ACLs)
- Load Balance
- Local Authentication Settings
- Security Settings (i.e. PSK, 802.1x, WebAuth)
- Media-stream settings
- Management Frame Protection (MFP)
- 802.11ac settings per WLAN
- Peer-to-peer blocking
- Radio Policy
- Roamed Voice Clients re-anchor
- Static IP Clients Support
- Unscheduled automatic power save delivery (U-APSD) for WLAN
- Work Group Bridge (WGB) Support

- Universal AP
- Wifi Direct
- Wi-Fi Multimedia (WMM)
- Authentication List (Remote Authentication Dial-In User Service [RADIUS] servers)

Policy Profile

- Authentication, Authorization, and Accounting (AAA) override
- AAA Policy
- Accounting List
- Auto QoS
- Call Snooping
- Central/Local Switching
- CiscoTrustSec (CTS) Security group access control lists (SGACLs)
- Datalink ACL
- Description
- Type-Length-Value (TLV) Caching (Dynamic Host Configuration Protocol [DHCP], Hypertext Transfer Protocol [HTTP])
- Idle Timeout
- Idle Threshold
- Fabric Profile
- Flex Network Address Translation / Port Address Translation (NAT/PAT)
- Flex Split MAC ACL
- Flex VLAN Based Central Switching
- IP Network-based Application Recognition (NBAR) Protocol Discovery
- IPv4/v6 ACL
- IPv4 DHCP
- IPv4/IPv6 Flexible Netflow Monitor
- Mobility Anchor
- Multicast VLAN
- Network Access Control (NAC)
- Passive Client
- RADIUS Profiling
- Reanchor
- Service Policy
- Session Timeout
- Session Initiation Protocol (SIP) Call Admission Control (CAC)
- Static IP Mobility
- Subscriber Policy Name
- Umbrella Parameter Map
- Uniform Resource Locator (URL) filter
- VLAN
- WGB VLAN
- WGB Broadcast Tagging

AP Join Profile

- CAPWAP Backup

- CAPWAP Fallback
- CAPWAP Retransmit
- CAPWAP Timers
- CAPWAP Window
- Cisco Discovery Protocol (CDP) for APs
- Core Dump Trivial File Transfer Protocol (TFTP)
- Country Code
- Description
- 2.4GHz / 5GHz Client Reporting interval
- 802.1x Credentials for APs acting as supplicants
- Extended Module support
- Hyperlocation
- Internet Content Adaptation Protocol (ICAP)
- Jumbo Maximum Transmission Unit (MTU) status
- Link Aggregation (LAG) for APs
- Lawful Interception
- Light-Emitting Diode (LED) status
- Link Encryption
- Link Latency
- Mesh Profile
- AP's Management user
- Network Time Protocol (NTP)
- Packet Capture Profile
- Power over Ethernet (PoE)
- AP's Preferred Mode (IPv4/IPv6)
- Rogue Detection Settings (Containment, min Received Signal Strength Indicator [RSSI], min transient time, report interval)
- SSH/Telnet
- Persisten SSID
- Statistics Timer
- Syslog
- Transmission Control Protocol - Maximum Segment Size (TCP MSS) Adjust
- TFTP Downgrade
- AP Trace Profile
- Universal Serial Bus (USB) enable

Flex Profile

- ACL Policy
- ARP Caching
- CTS
- Description
- Fallback Radio Interface Shutdown
- HTTP Client Proxy
- Min Latency Join for Flex AP
- Local Authentication parameters
- Multicast Parameters for Flex APs
- Native VLAN ID

- OfficeExtended AP mode
- Predownload
- Resilient (For Flex+Bridge APs)
- VLAN name mapping

RF Profile

- Airtime Fairness
- Band Select settings (Only on 2.4GHz profile)
- Channel
- Client Network Preference
- Coverage Hole Detection (CHD) settings
- Description
- 802.11n only mode
- High Density automatic settings
- High-Speed Roam (HSR)
- Load Balance Settings
- Rates
- Traps
- TX Power Levels

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

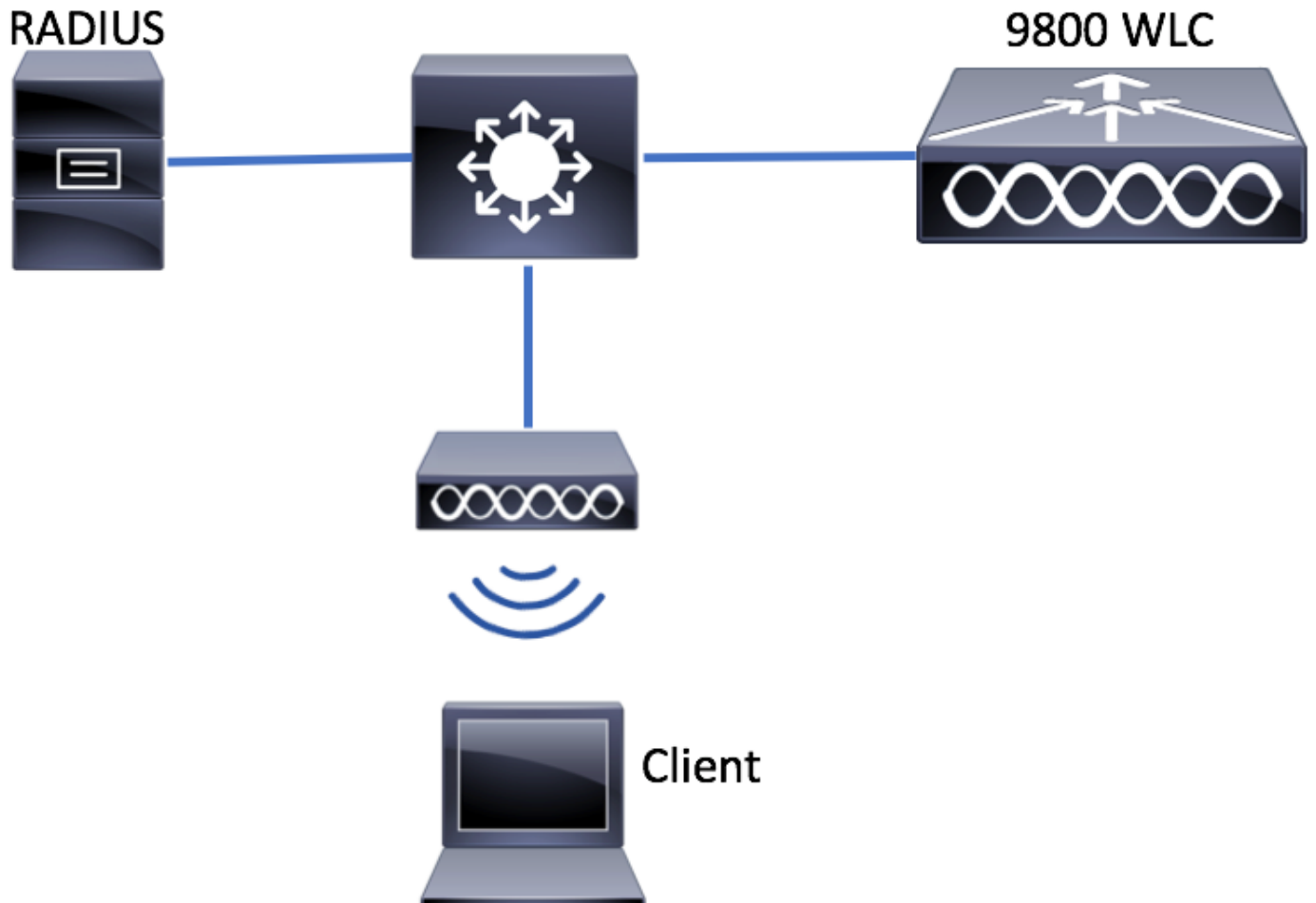
The information in this document is based on these software and hardware versions:

- Cisco Catalyst 9800 Wireless Controllers running IOS-XE Gibraltar v16.10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Network Diagram

This document is based on this topology:



Configurations

Declare Client's VLANs

Before you start any configuration you need to add the needed VLANs (VLANs where the wireless clients are assigned).

Step 1. Navigate to **Configuration > Layer2 > VLAN > VLAN > + Add**.

VLAN

SVI **VLAN** VLAN Group

+ Add **x Delete**

	VLAN ID	Name
<input type="checkbox"/>	1	default
<input type="checkbox"/>	100	VLAN100
<input type="checkbox"/>	210	VLAN210
<input type="checkbox"/>	2602	VLAN2602

Step 2. Enter the needed information.

Create VLAN

VLAN ID* 2601

Name

State **ACTIVATED**

RA Throttle Policy None

IGMP Snooping **DISABLED**

ARP Broadcast **DISABLED**

Port Members

Available (2)

- Gi2 →
- Gi3 →

Associated (0)

No Associated Members

Save & Apply to Device

Note: If you don't specify a **Name**, the VLAN automatically gets assigned the name of VLANXXXX, where XXXX is its VLAN id.


Repeat steps 1 and 2 for all the needed VLANs, once done you can continue to step 3.

Step 3. Verify the VLANs are allowed in your data interfaces.

If you are using port channels, navigate to **Configuration > Interface > Logical > PortChannel name > General**. If you see it configured as **Allowed Vlan = All** you are done with the configuration. If you see **Allowed VLAN = Vlan IDs**, add the needed VLANs and after that click **Update & Apply to Device**.

If you are not using port channels, navigate to **Configuration > Interface > Ethernet > Interface Name > General**. If you see it configured as **Allowed Vlan = All** you are done with the configuration. If you see **Allowed VLAN = Vlan IDs**, add the needed VLANs and after that click **Update & Apply to Device**.

No changes needed:

<u>General</u>	Advanced
Interface	GigabitEthernet3
Description	<input type="text"/> (1-200 Characters)
Admin Status	UP 
Port Fast	<input type="text" value="disable"/>
Enable Layer 3 Address	<input type="checkbox"/> DISABLED
Switchport Mode	<input type="text" value="trunk"/>
Allowed Vlan	<input checked="" type="radio"/> All <input type="radio"/> Vlan IDs
Native Vlan	<input type="text"/>

VLAN Id needs to be added:

Configure Interface GigabitEthernet2



General

Advanced

Interface	GigabitEthernet2	
Description	<input type="text"/>	(1-200 Characters)
Admin Status	<input type="button" value="UP"/>	
Port Fast	<input type="text" value="disable"/>	
Enable Layer 3 Address	<input type="checkbox"/> DISABLED	
Switchport Mode	<input type="text" value="trunk"/>	
Allowed Vlan	<input type="radio"/> All <input checked="" type="radio"/> Vlan IDs	
Vlan IDs	<input type="text" value="210,2602,2685,2601"/>	(e.g., 2,4,6-10)
Native Vlan	<input type="text" value="1"/>	

Cancel

Update & Apply to Device

CLI:

```
# config t
# vlan <vlan-id>
# exit
```

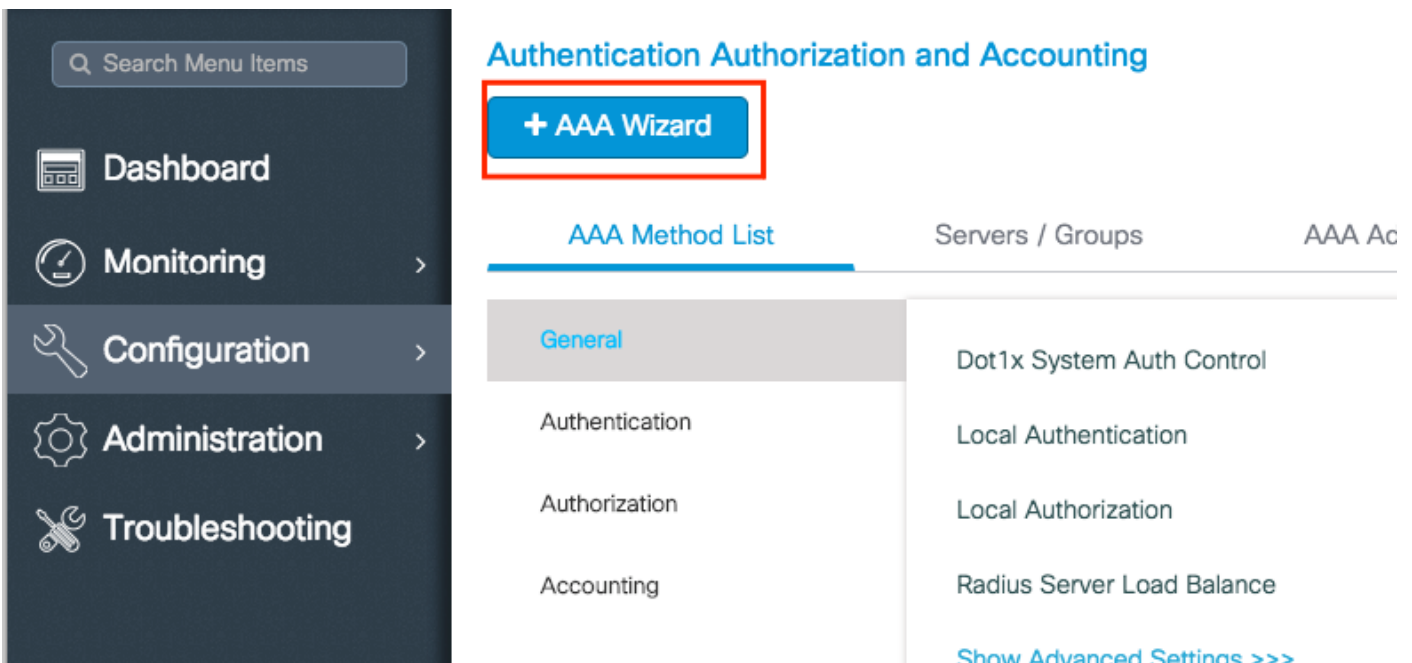
```
# interface <interface-id>
# switchport trunk allowed vlan add <vlan-id>
# end
```

Wizard Based Configuration - Recommended for New 9800 WLC Deployments

For Catalyst 9800 WLCs installation, you can follow configuration wizards made available to guide you through the configuration process. If you need to use RADIUS servers on your deployment, you can follow the AAA Wizard first and then choose between the Basic or Advanced Wireless Setup. If you don't use RADIUS servers on your deployment, you can go directly to either Basic or Advanced Wireless Setup.

AAA Wizard

Step 1. Navigate to **Configuration > Security > AAA > + AAA Wizard**.



The screenshot displays the Cisco configuration interface. On the left is a dark sidebar menu with a search bar and navigation items: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main content area is titled "Authentication Authorization and Accounting" and features a blue button labeled "+ AAA Wizard" which is highlighted with a red rectangular box. Below this button are three tabs: "AAA Method List" (selected), "Servers / Groups", and "AAA Ac". Under the "AAA Method List" tab, there is a "General" section with sub-items for Authentication, Authorization, and Accounting. To the right of these sub-items, there is a list of server types: "Dot1x System Auth Control", "Local Authentication", "Local Authorization", and "Radius Server Load Balance". At the bottom right of the main content area, there is a link that says "Show Advanced Settings >>>".

Step 2. Enable the needed kind of servers and enter a server's name (It can be the IP address or any other string), the server's IP and the shared secret. After that click **Next**.

Add Wizard Basic Advanced

SERVER SERVER GROUP ASSOCIATION MAP AAA

RADIUS TACACS+ LDAP

RADIUS

Name*

Server Address*

Shared Secret*

Confirm Shared Secret*

Cancel Next →

Step 3. Enter the information to create a server group. Ensure you add the server specified in previous step to the **Assigned Servers**.

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

> <

← Previous Next →

Step 4. Enable **Authentication** and create an Authentication method.

Navigate to the **Authentication** tab and enter the needed information, once done click **Save & Apply to Device**.

Add Wizard ● Basic ○ Advanced

SERVER SERVER GROUP ASSOCIATION MAP AAA

General **Authentication** Authorization Accounting

General **Authentication**

Method List Name*

Type*

Group Type

Fallback to local

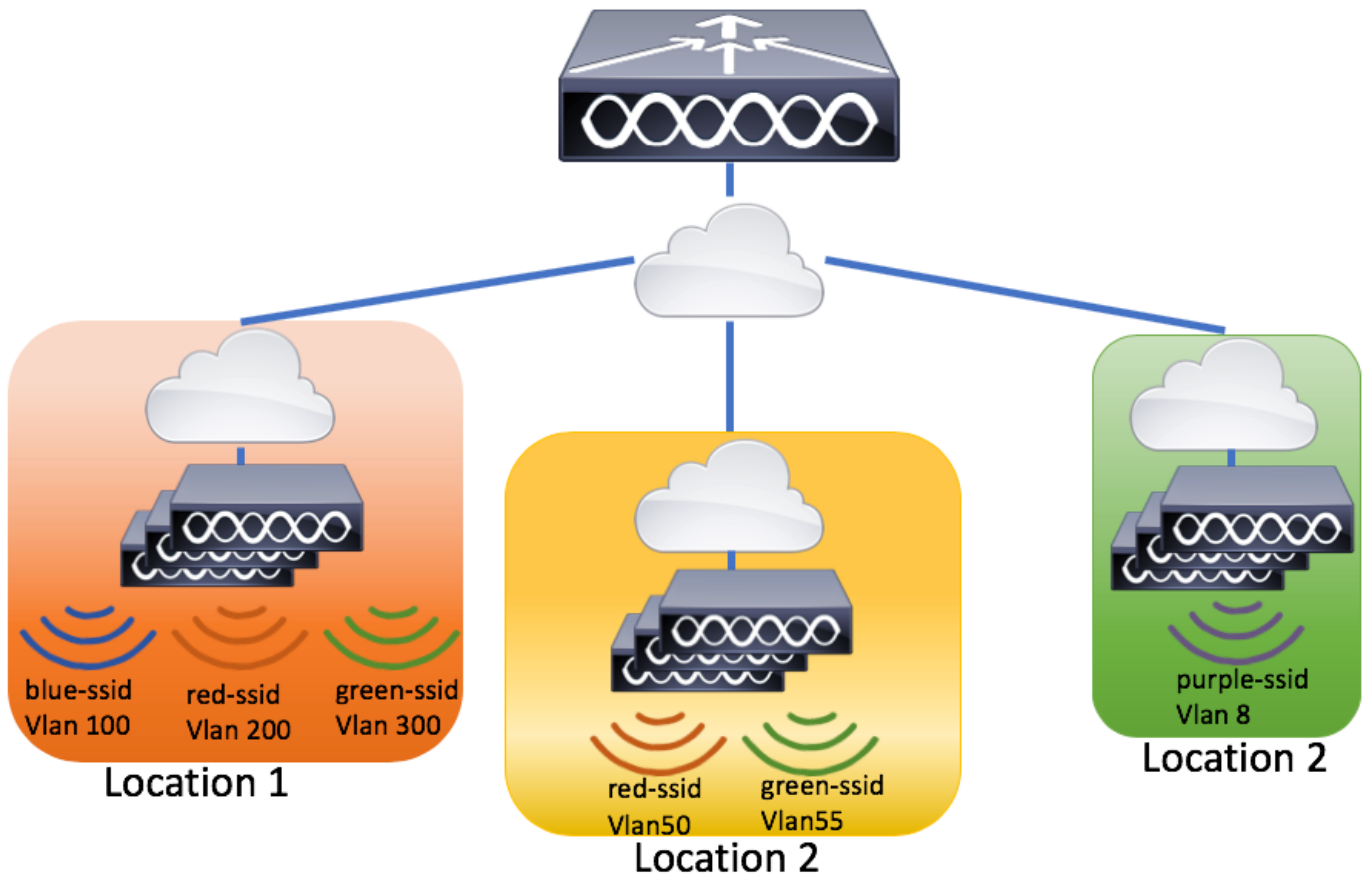
Available Server Groups: radius, ldap, tacacs+, ISE-kcg-grp

Assigned Server Groups: **server-group**

Basic Wireless Setup

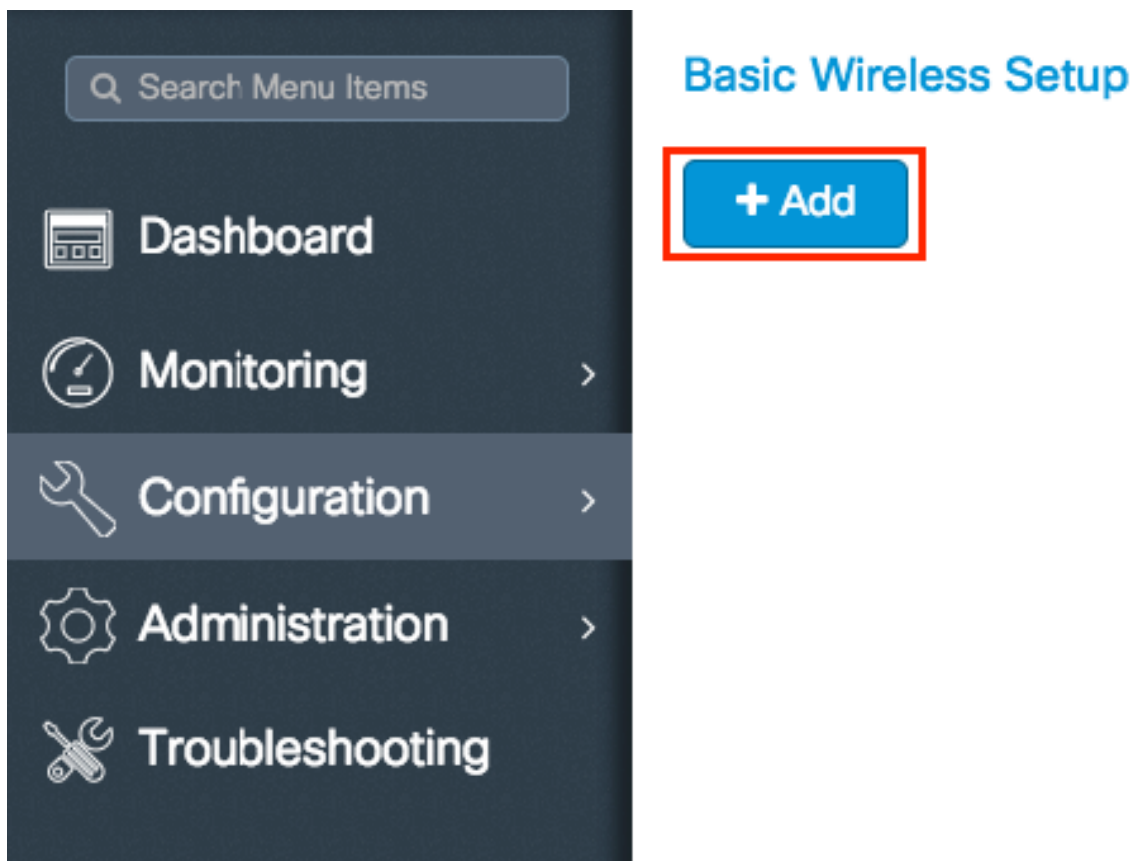
This wizard guides you through a basic wireless setup. It allows you to segment the APs function with little effort.

Example of a deployment you can accomplish with the basic wireless setup wizard.



Step 1. Create a new location.

Navigate to **Configuration > Wireless Setup > Basic > +Add**.



Step 2. Enter the needed information on the **General** tab.

Basic Wireless Setup:

← Back

General	Wireless Networks	AP Provisioning
Location Name*	<input type="text" value="Enter Name"/>	
Description	<input type="text" value="Enter Description"/>	
Location Type	<input checked="" type="radio"/> Local <input type="radio"/> Flex	
Client Density	<input type="range" value="Typical"/>	

Location Name = Name of the new location

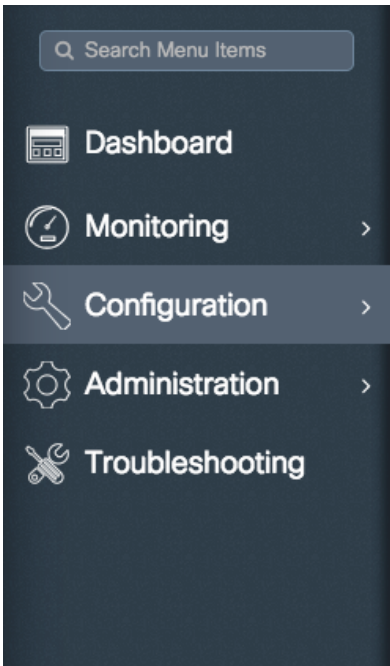
Description = Optional description of the location

Location Type = Local (Local mode APs), Flex (FlexConnect Mode APs)

Client Density = Adjusts RF configuration for the specified Client Density.

Step 3. Add the needed WLANs.

Navigate to the **Wireless Networks** tab and click **+Add**.



Basic Wireless Setup: Location-typical-density

[← Back](#)

General

Wireless Networks

AP Provisioning

+ Add

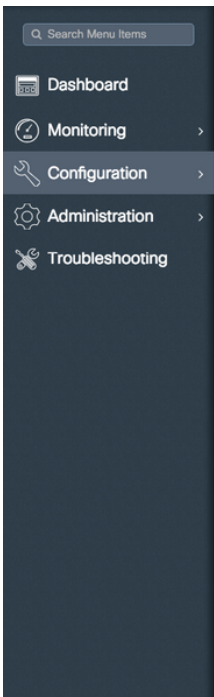
x Delete

WLANs on this Location

WLAN Name
0

10 items per page

You can either select **Define new** to create a new WLAN from scratch or select a pre-existing one from the **WLAN*** drop down list.



Basic Wireless Setup: Location-typical-density

[← Back](#)

x Delete Location

General

Wireless Networks

AP Provisioning

+ Add

x Delete

WLANs on this Location

WLAN Name	VLAN/VLAN Group
0	No items to c

10 items per page

Wireless Network Details

WLAN* [or Define new](#)
Network name is required

Policy Details

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

ACL [or Define new](#)

QoS

ON Central Switching

ON Central Authentication

ON Central DHCP

ON Central Association

x **✓**

If you select **Define new**, a menu like this appears, where you can choose an SSID name, type of security and other SSID related settings. Once you complete the configuration of the new SSID click **Save & Apply to Device**.

Add WLAN ✕

General
Security
Advanced

Profile Name*

SSID

WLAN ID*

Status ENABLED

Radio Policy

Broadcast SSID ENABLED

↶ Cancel

📄 Save & Apply to Device

Step 4. Select the VLAN (and any other configuration) that you want to apply to that SSID. Once done click on the checkmark.

- Dashboard
- Monitoring >
- Configuration >
- Administration >
- Troubleshooting

✕ Delete Location

General
Wireless Networks
AP Provisioning

+ Add
✕ Delete

WLANs on this Location

WLAN Name	VLAN/VLAN Group
No item	

Wireless Network Details

WLAN* or [Define new](#)

Policy Details

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

ACL

QoS

Central Switching Central Authentication

Central DHCP Central Association

✕
✓

Basic Wireless Setup: Location-typical-density

← Back

General **Wireless Networks** AP Provisioning

+ Add **× Delete**

WLANs on this Location

WLAN Name	VLAN/VLAN Group
<input type="checkbox"/> new-ssid	VLAN2601

10 items per page

Repeat steps 3 and 4 for all the needed WLANs.

Step 5. Assign the configuration to the needed APs.

Navigate to **AP Provisioning** tab and select the APs to which you want to apply the current configuration. Once selected moved them from **Add/Select APs** to **APs on this Location**.

Basic Wireless Setup: Location-typical-density

← Back

General Wireless Networks **AP Provisioning** **× Delete**

Add/Select APs

AP MAC Address

Available AP list

Number of selected APs : 2

AP MAC	AP Name
<input checked="" type="checkbox"/> 0042.68a0.d022	AP3802-karlicsn
<input checked="" type="checkbox"/> 0896.ad9d.143e	AP2802-01

500 items per page 1 - 2 of 2 items

APs on this Location

Associated AP list

Number of selected APs : 0

AP MAC	AP Name	Status
<input type="checkbox"/>		

500 items per page

Step 6. To apply the configuration to the APs, click **Apply**.

Basic Wireless Setup: Location-typical-density

← Back

General Wireless Networks **AP Provisioning** **× Delete Location** **Apply**

Add/Select APs

AP MAC Address

Available AP list

Number of selected APs : 0

AP MAC	AP Name
<input type="checkbox"/>	

500 items per page No items to display

APs on this Location

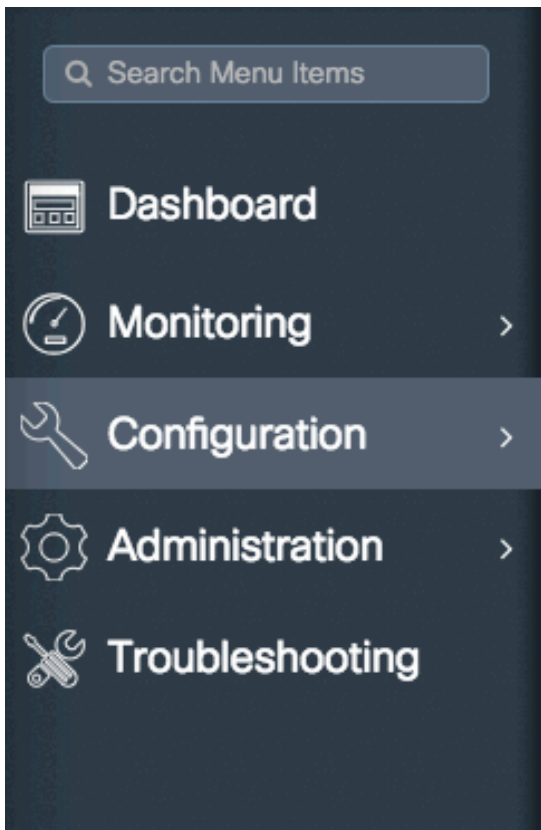
Associated AP list

Number of selected APs : 0

AP MAC	AP Name	Status
<input type="checkbox"/> 0896.ad9d.143e	AP2802-01	Joined
<input type="checkbox"/> 0042.68a0.d022	AP3802-karlicsn	Joined

500 items per page 1 - 2 of 2 items

Once you click **Apply**, you can see the new Location created. At the beginning you see **0 Joined APs** because when the configuration was applied to the APs they restart its association to the controller (they restart the CAPWAP tunnel).



Basic Wireless Setup

+ Add

A card representing a location. At the top is a location pin icon. Below the icon is the text "Location-typical-density". At the bottom of the card, there are two statistics: "0 Joined APs" and "0 Clients".

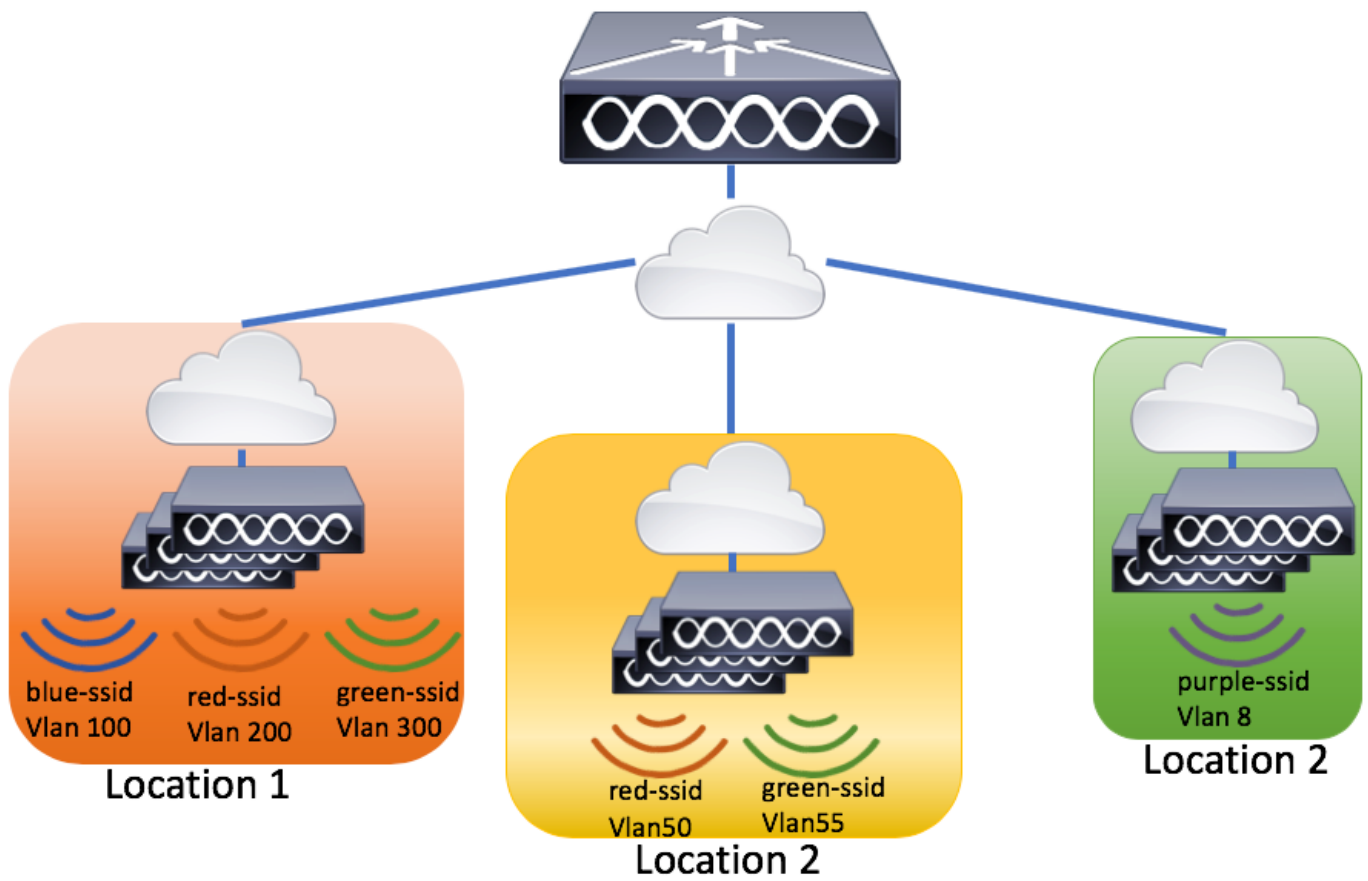
Location	Joined APs	Clients
Location-typical-density	0	0

Repeat all the steps described so far for all the locations that will be serviced by this 9800 WLC.

If you need to add more APs or WLANs to an existing location you can click on the location and navigate to the relevant tab to make the desired changes.

Advanced Wireless Setup

This wizard guides you through an advanced wireless setup. It allows you to segment the APs functions with more detail.



Step 1. Start the Advanced Wireless Setup.

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

