



Cisco Catalyst 9800 Wireless Controller Series Web UI Deployment Guide

Table of Contents

Cisco Catalyst 9800	1
Wireless Controller Series	1
Web UI Deployment Guide	1
Introduction.....	5
Feature Overview	6
Elements of the configuration model – Profiles and Tags	6
Profiles	6
WLAN Profile.....	7
Policy Profile	7
AP Join Profile.....	7
Flex Profile	8
RF Profile	8
Tags	9
Policy Tag	10
Site Tag.....	10
RF Tag	10
Association of tags to APs	11
Day 0 Express Setup	13
Configuring wireless controller	13
Accessing Day 0 Express Setup using Web UI	15
Accessing Day 0 Express Setup using CLI	23
Day 0 configuration for C9800-40, C9800-80 and C9800-L.....	25
DAY 0 configuration for C9800-CL on Private Cloud	28
Configuring the basic C9800-CL settings.....	28
C9800-CL Day-0 Configuration Setup Wizard.....	29
C9800-CL configuring via CLI: skipping the DAY 0 guided flow.....	33

DAY 0 configuration for C9800-CL on Public Cloud	35
Configuring the AP certificate manually.....	38
Wireless Basic Workflow.....	38
Wireless Advanced Workflow.....	45
Guided workflow and Use cases	45
Use Case 1 - Global SSID(s) across the campus	47
Use Case 2 – Local sites within a Campus	56
Use Case 3 – Remote sites across the WAN.....	61
Additional Use case Examples.....	66
WLAN Wizard Overview	67
Creating a PSK SSID	68
Creating a DOT1X SSID.....	70
AireOS to Catalyst 9800 Wireless Controller Migration.....	73
Migration Web Tool	73
AireOS Config Translator	78
Migration using Prime Infrastructure 3.5.....	80



Introduction

This document introduces the new configuration model for the Elastic Wireless LAN Controller and provides general guidelines for its deployment. The purpose of this document is to:

- Provide an overview of the configuration model
- Highlight key use cases and deployments
- Provide details on best practices, monitoring and migration

Feature Overview

Introduction to the Best-Practice driven configuration model

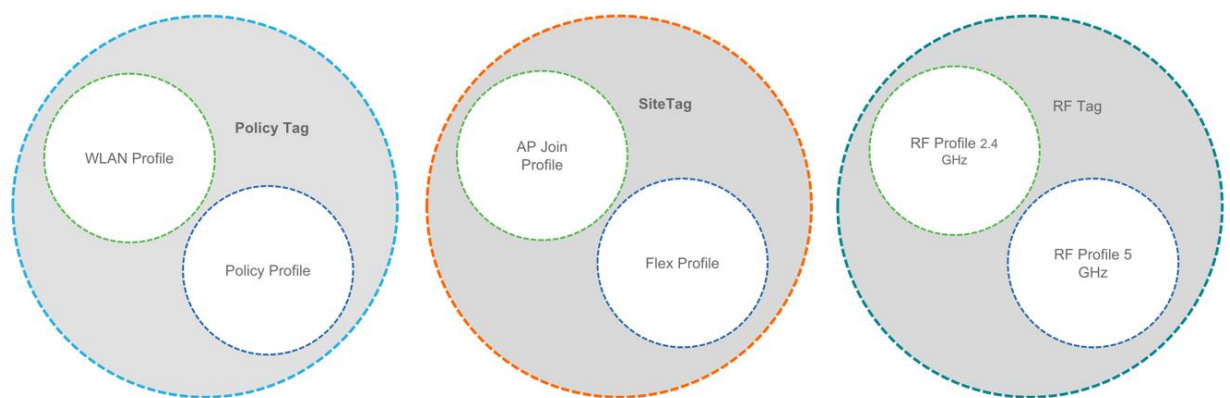
Cisco Catalyst 9800 Wireless Controller configuration data model is based on design principles of reusability, simplified provisioning, enhanced flexibility and modularization to help manage networks as they scale and simplify management of dynamically changing business and IT requirements.

This model provides a model for the client/AP devices to derive their configurations from profiles, which are contained within Tags. AP can be mapped to the tags either statically or as part of the rule engine that runs on the controller and comes into effect during the AP join process. Configuration objects are modularized as objects, which helps in reusability of configuration. In addition, a flat tag-based configuration model eliminates the complexities associated with inheritance and container-based grouping leading to a simpler and more flexible configuration that can ease change management.

Elements of the configuration model – Profiles and Tags

Profiles

Profiles define the properties of the AP or associated clients. Profiles are reusable entities, which can be used across tags. Default Policy profile, AP Join profile, Flex profile and 2.4/5GHz RF profiles are available by default on the wireless controller at boot time.



There are different kinds of profiles depending on the characteristic of the network they define. These profiles are in turn part of a larger construct called a Tag, as defined in the previous section.

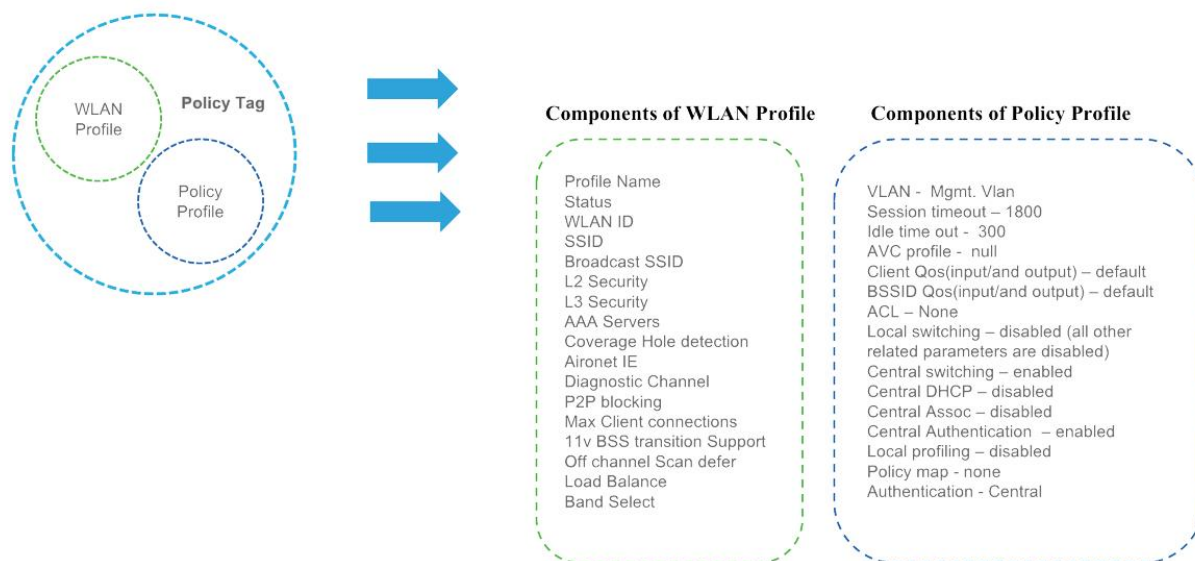
WLAN Profile

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

The policy profile defines the network policies and the switching policies 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 switching policies define central switching or local switching attribute of a WLAN.

The WLAN Profile and Policy Profile are both parts 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. A policy profile once defined can be reused across different Site Tags with same/different WLANs.

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.

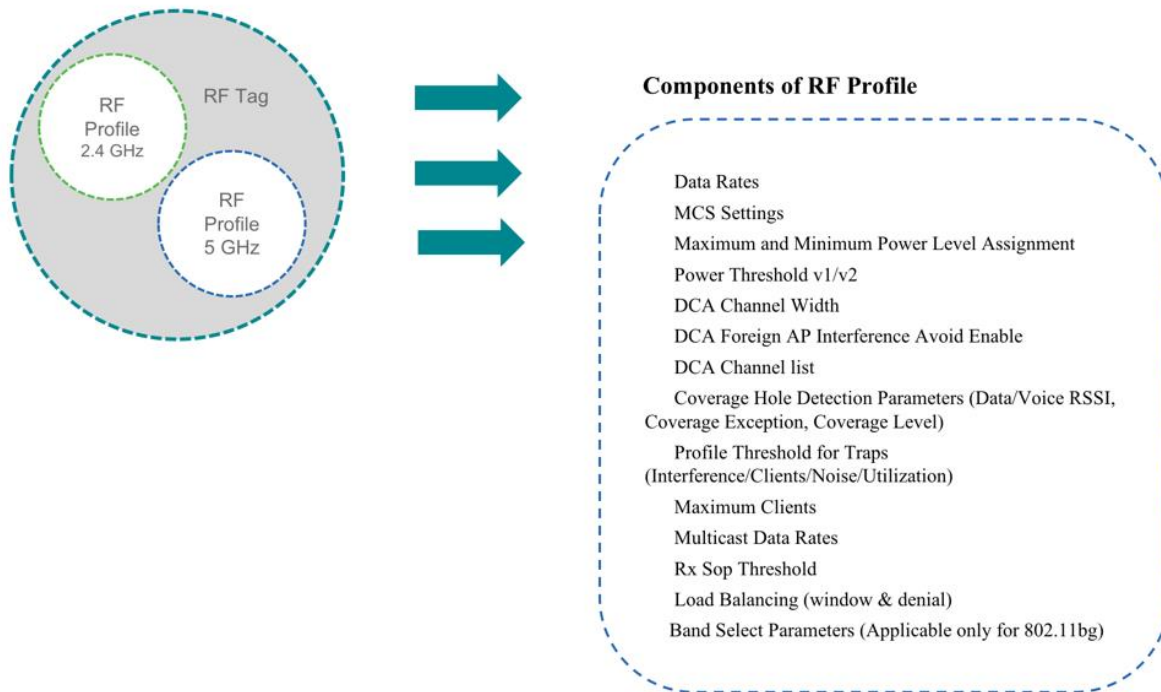
The AP Join Profile and Flex Profile are both parts a Site Tag and define the characteristics of a local or remote site.

Note: When a site tag contains a Flex Profile, APs tagged with this site tag will be converted to FlexConnect mode. No reboot is required when AP is moving from Local to FlexConnect mode but CAPWAP is reset.



RF Profile

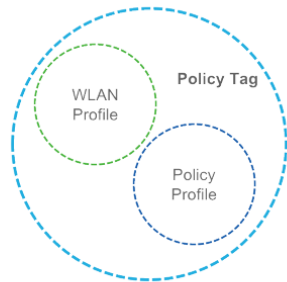
By default, there exists two default RF Profiles (one for 802.11a and one for 802.11b). RF profiles constitute the RF specific configurations such as Data rates, MCS settings, Power assignment, DCA parameters, CHDM variables and HDX features. One 802.11a RF profile and one 802.11b RF profile can be added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



Tags

A Tag's property is defined by the policies 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

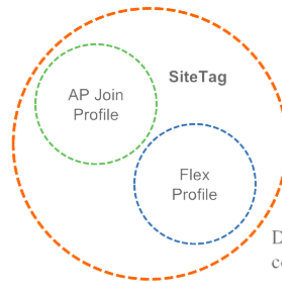
There are three kinds of tags.



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



Defines the RF properties of the network



Defines the properties of the central and the remote site APs

Policy Tag

Policy tag constitutes the mapping of WLAN Profiles to Policy profiles.

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

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. 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.

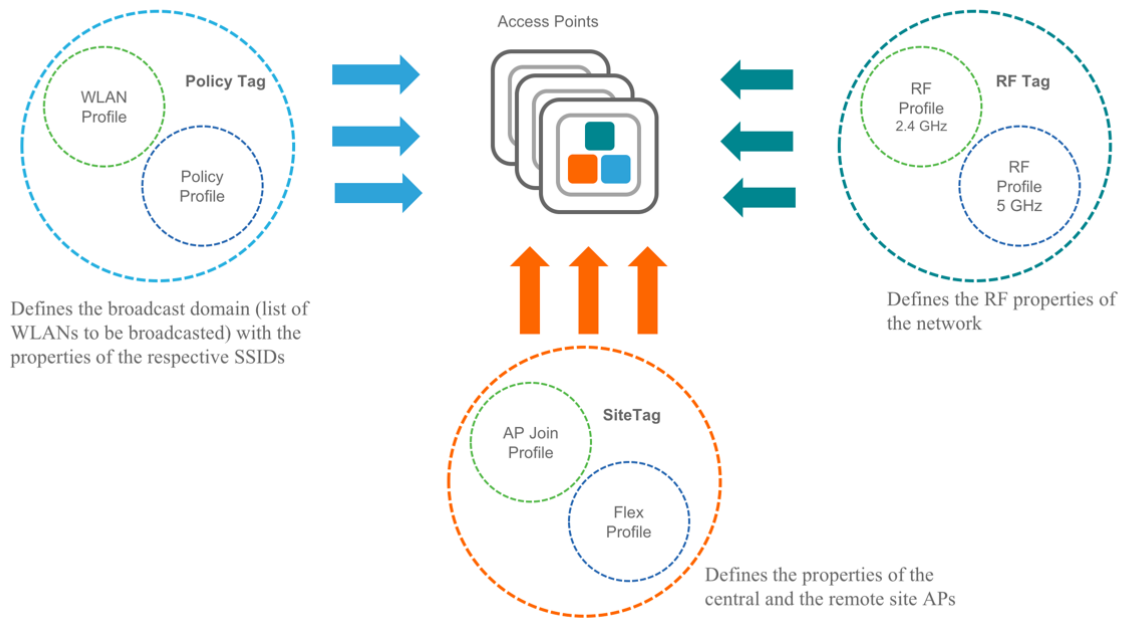
RF Tag

RF tag constitutes of the 2.4 and 5GHz RF profiles

Default RF Tag constitutes of the default 2.4GHz RF profile and the default 5GHz RF Profile. The default 2.4 and 5GHz RF profiles contain default values for global RF profiles for the respective radios.

Association of tags to APs

Access Points are tagged based on broadcast domain, the site it belongs to and the RF characteristics desired. Once tagged, the AP gets a list of WLANs to be broadcasted along with the properties of the respective SSIDs, properties of the APs on the local/remote site and the RF properties of the network. By default, an AP is tagged with the default policy, site and RF tag unless explicitly changed. When a tag associated with an AP is changed, the AP resets its CAPWAP connection.





Day 0 Express Setup

The Cisco Catalyst 9800 Wireless Controller provides a simplified first time out of box installation and configuration interface for all series of wireless controllers. This section provides a set of instructions to help easily setup the wireless controller to operate in a small, medium, or large network wireless environment, where access point(s) can join and together as a simple solution and provide various services, such as corporate employee or guest wireless access on the network.

Note that the Express Setup can be used only for the first time in out of box installations or when controller configuration is reset to factory defaults.

Configuring wireless controller

The general steps to configure the wireless controller are as follows:

Procedure

- Step 1** Complete the configuration checklist.
- Step 2** Unpack, connect, and power on the wireless controller.
- Step 3** Connect a client machine to Service Port of the wireless controller with an Ethernet cable.
- Step 4** Open a client web browser to access the wireless controller startup GUI.
- Step 5** Enter the settings from the completed configuration checklist.
- Step 6** Disconnect the wireless controller from client machine and connect to the network switch.
- Step 7** Connect access point(s) to the network switch. Access points join the wireless controller, and the configured wireless network become available.
- Step 8** Connect wireless client(s) to the available network.

Configuration Checklist

The following checklist helps you to make the installation process easier, while using the GUI wizard to configure the wireless controller. While most of the information from the list is mandatory, there is some information that is optional (*). Take a moment to fill out:

- Network switch requirement:
 - Wireless controller switch port number assigned
 - Wireless controller assigned switch port
 - Is the switch port configured as trunk?
 - Is there a management VLAN? Management VLAN ID
 - Is there a guest VLAN? Guest VLAN ID
- a. Wireless controller Settings:
 - New admin account name
 - Admin account password
 - System name for the wireless controller
 - The current time zone
 - Is there an NTP server available? NTP server IP address
 - Wireless controller Management Interface:
 - IP address
 - Subnet mask
 - Default gateway
 - Management VLAN ID
- Corporate Wireless Network
- Corporate wireless name/SSID
- Is a RADIUS server required?
- Security authentication option to select:
 - WPA/WPA2 Personal
 - Corporate pass phrase (PSK)
 - WPA/WPA2 Enterprise)
 - RADIUS server IP address and shared secret
 - Is a DHCP server known? DHCP server IP address
- Guest Wireless Network - optional:
 - Guest wireless name/SSID
 - Is a password required for guest?
 - Guest pass phrase (PSK)

- Guest VLAN id (use id)
- Guest networking:
 - IP address
 - Subnet mask
 - Default gateway
- Advanced option—Configure RF Parameters for Client Density as Low, Medium, or High.

Accessing Day 0 Express Setup using Web UI

Step 1 Upon confirming that there is an IP address of **192.168.1.x** assigned to your computer, open a web browser (preferably Chrome and Safari) and open the URL: **http://192.168.1.1**. The following screen appears in your browser.

Note Keep the checklist that you have prepared earlier, as this will be very helpful to proceed with the following steps.

To create an admin account, do the following:

Create a new admin account name, for example, **admin**.

Provide the new admin account's password, for example, **Cisco123**.

Confirm the password.

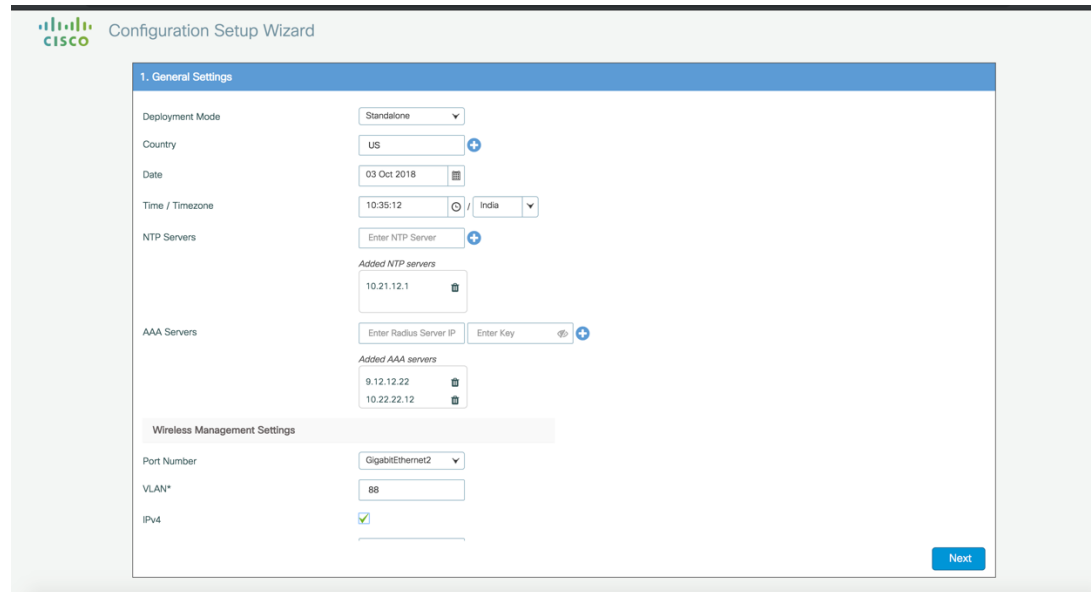
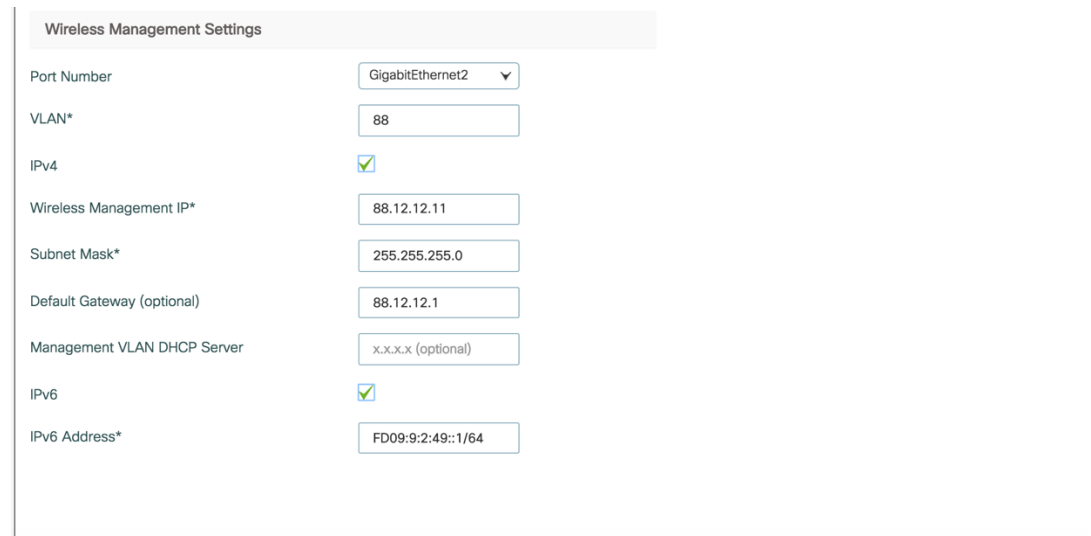
Click **Start** to continue.

Step 2 Once you are logged into the controller, in the **General Settings** screen, with the help of the checklist, fill in the following:

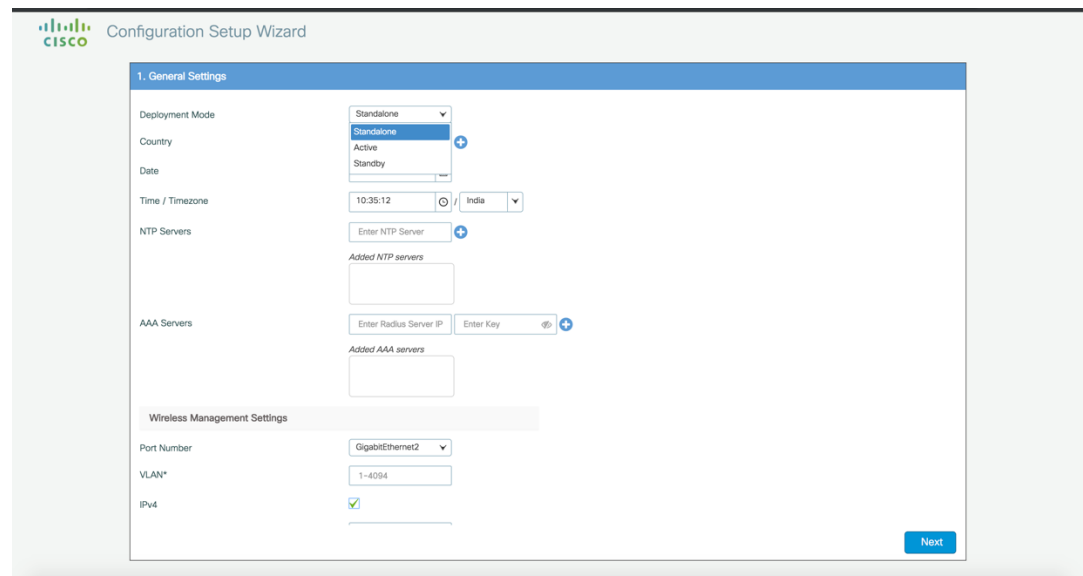
- Deployment mode – standalone, Active or Standby
- Country Code
- Date
- **Time/ Timezone**
- NTP servers
- AAA Servers
- Wireless Management Settings
 - Port number
 - VLAN
- IPv4
 - Wireless Management IP
 - Subnet mask
 - Default gateway
 - Management VLAN DHCP Server
- IPv6
 - IPv6 Address

Note The wizard will attempt to import the clock information (date and time) from the computer via JavaScript. It is highly recommended that you confirm this before continuing. Access points rely on correct clock settings to be able to join the wireless controller.

Figure 3. Sample configuration

Three modes for Day 0: Standalone, Active, Standby (Active and Standby have options to setup HA SSO with local IP, remote IP and subnet mask configuration)



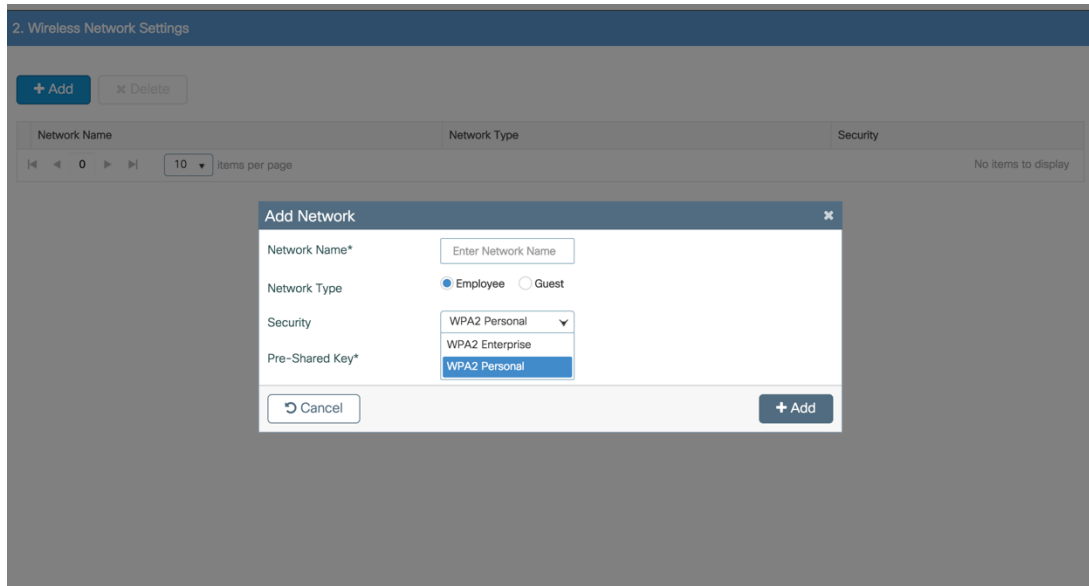
Step 5 In the **Wireless Networks Settings** screen, in the **Employee** area, with the help of the checklist, fill in the following:

Network name/SSID

Security, for example, **WPA/WPA2 Personal**

WPA/WPA2 Personal—Provide a pass phrase (PSK /for example, **Cisco123** and confirm the pass phrase).

Figure 4. Example of an Employee Network Configured with WPA/WPA2 Personal Using PSK (pre-shared key / pass phrase)

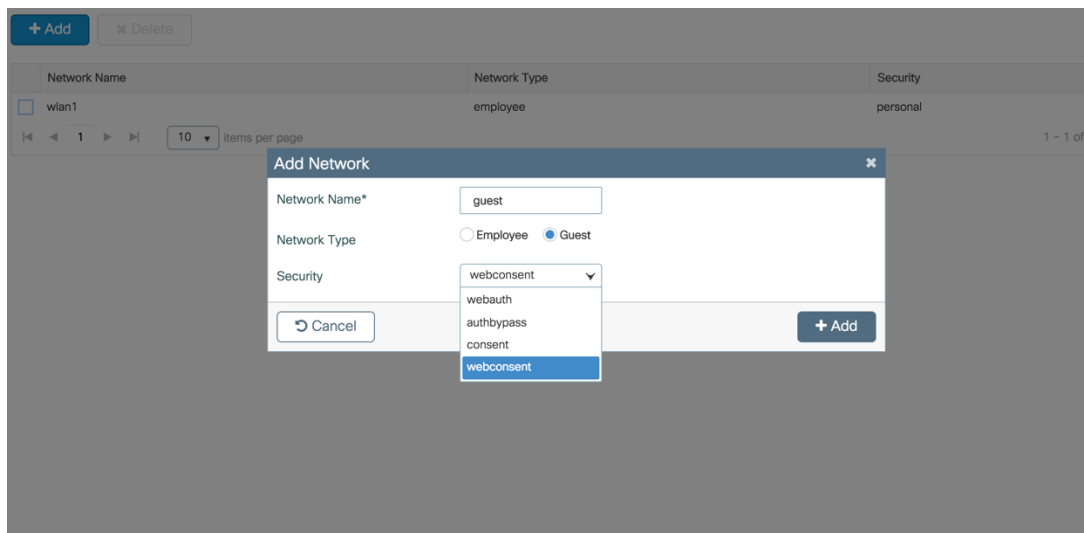


Step 6 (Optional) In the **Wireless Networks Settings** screen, in the **Guest** area, with the help of the checklist, fill in the following:

Network name/SSID, for example, **guest**

Security, for example, **Web Consent**

Figure 5. Example of a Guest Network Configured with Web Consent

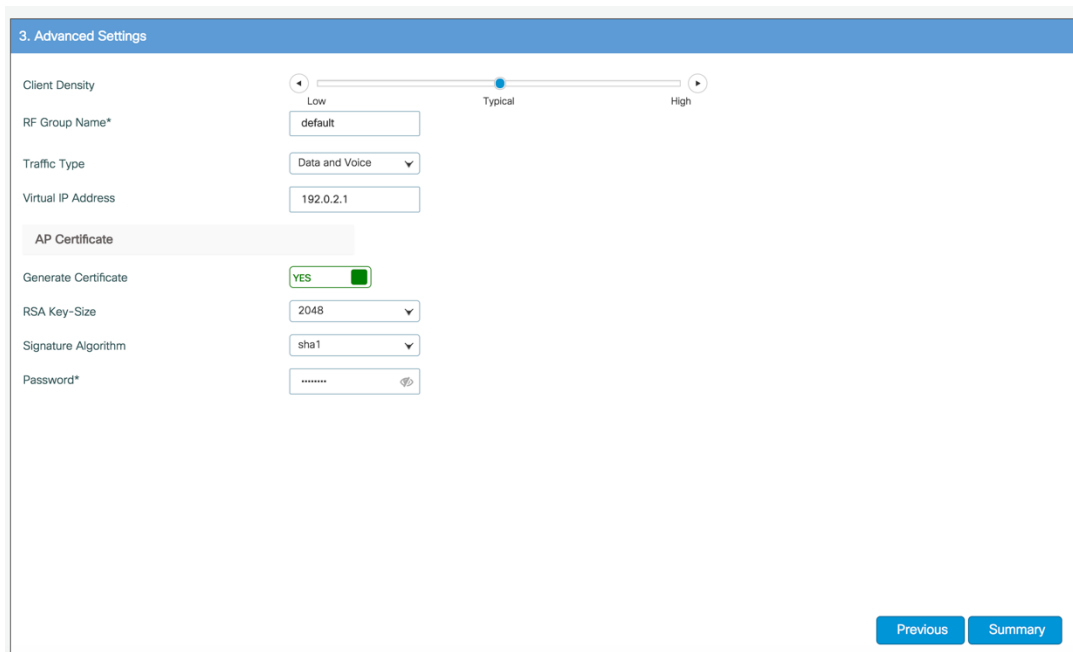


Step 7 In the **Advanced Settings** screen, in the RF Parameter Optimization area, do the following:

Select the client density as Low, Typical, or High.

Configure the RF parameters for RF Traffic Type, such as Data and Voice.

For VM and Cloud instances, AP Trustpoint certificate is generated by default as shown below



The following CLIs depicts the default values when Low, Typical, or High Client density is selected

Typical-Client-Density-802.11a

```
ap dot11 5ghz rrm txpower min -10
ap dot11 5ghz rrm txpower max 30
ap dot11 5ghz rrm tpc-threshold -70
ap dot11 5ghz rx-sop threshold auto
ap dot11 5ghz rrm coverage data rssi-threshold -80
ap dot11 5ghz rrm coverage voice rssi-threshold -80
ap dot11 5ghz rrm coverage level global 3
ap dot11 5ghz cleanair
no ap dot11 5ghz rrm channel cleanair-event
ap dot11 5ghz rate RATE_12M mandatory
ap dot11 5ghz rate RATE_9M supported
ap dot11 5ghz rate RATE_6M disable
no ap dot11 5ghz rrm channel cleanair-event
wireless client band-select client-rssi -80
```

High-Client-Density-802.11a

```
ap dot11 5ghz rrm txpower min 7
```

```
ap dot11 5ghz rrm txpower max 30
ap dot11 5ghz rrm tpc-threshold -65
ap dot11 5ghz rx-sop threshold -78
ap dot11 5ghz rrm coverage data rssi-threshold -80
ap dot11 5ghz rrm coverage voice rssi-threshold -80
ap dot11 5ghz rrm coverage level global 3
ap dot11 5ghz cleanair
no ap dot11 5ghz rrm channel cleanair-event
ap dot11 5ghz rate RATE_12M mandatory
ap dot11 5ghz rate RATE_9M supported
ap dot11 5ghz rate RATE_6M disable
no ap dot11 5ghz rrm channel cleanair-event
wireless client band-select client-rssi -80
```

Low-Client-Density-802.11a

```
ap dot11 5ghz rrm txpower min -10
ap dot11 5ghz rrm txpower max 30
ap dot11 5ghz rrm tpc-threshold -60
ap dot11 5ghz rx-sop threshold -80
ap dot11 5ghz rrm coverage data rssi-threshold -90
ap dot11 5ghz rrm coverage voice rssi-threshold -90
ap dot11 5ghz rrm coverage level global 2
ap dot11 5ghz cleanair
no ap dot11 5ghz rrm channel cleanair-event
no wireless client band-select client-rssi
```

Typical-Client-Density-802.11bg

```
ap dot11 24ghz rrm txpower min -10
ap dot11 24ghz rrm txpower max 30
ap dot11 24ghz rrm tpc-threshold -70
ap dot11 24ghz rx-sop threshold auto
ap dot11 24ghz rrm coverage data rssi-threshold -80
ap dot11 24ghz rrm coverage voice rssi-threshold -80
ap dot11 24ghz rrm coverage level global 3
ap dot11 24ghz cleanair
no ap dot11 24ghz rrm channel cleanair-event
ap dot11 24ghz rate RATE_12M mandatory
ap dot11 24ghz rate RATE_9M supported
ap dot11 24ghz rate RATE_18M disable
ap dot11 24ghz rate RATE_24M disable
ap dot11 24ghz rate RATE_36M disable
ap dot11 24ghz rate RATE_48M disable
```

```
ap dot11 24ghz rate RATE_54M disable
ap dot11 24ghz rate RATE_6M disable
no ap dot11 24ghz rrm channel cleanair-event
wireless client band-select client-rssi -80
```

High-Client-Density-802.11bg

```
ap dot11 24ghz rrm txpower min 7
ap dot11 24ghz rrm txpower max 30
ap dot11 24ghz rrm tpc-threshold -70
ap dot11 24ghz rx-sop threshold -82
ap dot11 24ghz rrm coverage data rssi-threshold -80
ap dot11 24ghz rrm coverage voice rssi-threshold -80
ap dot11 24ghz rrm coverage level global 3
ap dot11 24ghz cleanair
no ap dot11 24ghz rrm channel cleanair-event
ap dot11 24ghz rate RATE_12M mandatory
ap dot11 24ghz rate RATE_9M supported
ap dot11 24ghz rate RATE_18M disable
ap dot11 24ghz rate RATE_24M disable
ap dot11 24ghz rate RATE_36M disable
ap dot11 24ghz rate RATE_48M disable
ap dot11 24ghz rate RATE_54M disable
ap dot11 24ghz rate RATE_6M disable
no ap dot11 24ghz rrm channel cleanair-event
wireless client band-select client-rssi -80
```

Low-Client-Density-802.11bg

```
ap dot11 24ghz rrm txpower min -10
ap dot11 24ghz rrm txpower max 30
ap dot11 24ghz rrm tpc-threshold -65
ap dot11 24ghz rx-sop threshold -85
ap dot11 24ghz rrm coverage data rssi-threshold -90
ap dot11 24ghz rrm coverage voice rssi-threshold -90
ap dot11 5ghz rrm coverage level global 2
ap dot11 24ghz cleanair
no ap dot11 24ghz rrm channel cleanair-event
ap dot11 24ghz rate RATE_12M mandatory
ap dot11 24ghz rate RATE_9M mandatory
ap dot11 24ghz rate RATE_18M mandatory
ap dot11 24ghz rate RATE_24M mandatory
```

```

ap dot11 24ghz rate RATE_36M mandatory
ap dot11 24ghz rate RATE_48M mandatory
ap dot11 24ghz rate RATE_54M mandatory
ap dot11 24ghz rate RATE_6M mandatory
no ap dot11 24ghz rrm channel cleanair-event
no wireless client band-select client-rssi
    
```

Step 8 If all the settings are correct, click **Finish**

Configuration Setup Wizard

4. Summary

General Settings

Deployment Mode	standalone
Country	US
Date	03 Oct 2018
Time / Timezone	10:35:12 / India
NTP Servers	10.21.12.1
AAA Servers	9.12.12.22,10.22.22.12

Wireless Management Settings

Port Number	GigabitEthernet2
Wireless Management VLAN	88
Wireless Management IP	88.12.12.11
Subnet Mask	255.255.255.0
Default Gateway	88.12.12.1
IPv6	FD09:9:2:49::1/64

Wireless Network Settings

Network Name	Network Type	Security
wan1	employee	personal
guest	guest	authbypass

1 - 2 of 2 items

[Previous](#) [Finish](#)

Wireless Network Settings

Network Name	Network Type	Security
wan1	employee	personal
guest	guest	authbypass

1 - 2 of 2 items

Advanced Settings

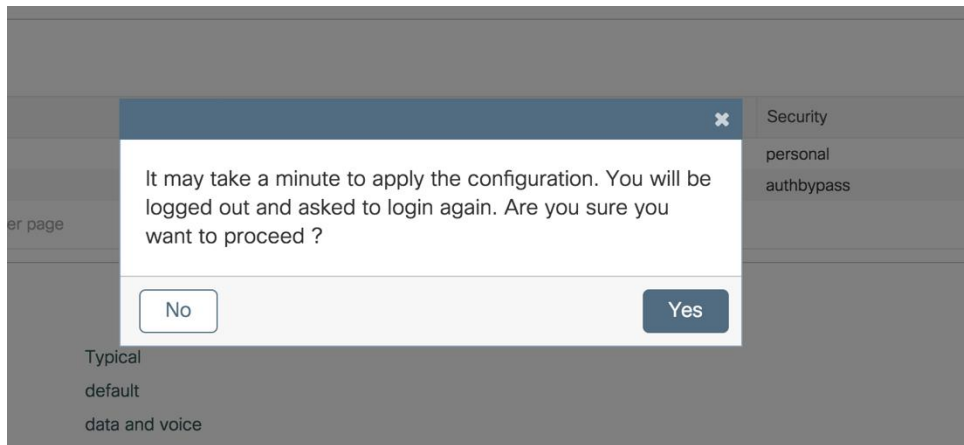
Client Density	Typical
RF Group Name	default
Traffic Type	data and voice
Virtual IPv4 Address	192.0.2.1

AP Certificate

Generate Certificate	Yes
RSA Key-Size	2048
Signature Algorithm	sha1

[Previous](#) [Finish](#)

Step 9 A message appears with a prompt *It may take a minute to apply the configuration. You will be logged out and asked to login again. Are you sure you want to proceed?*



Click OK to apply final settings. The wireless controller logs out and the user needs to re-login to continue to the fully setup wireless controller.

Accessing Day 0 Express Setup using CLI

Prior to Release 17.4, the default Day0 CLI wizard does not support wireless specific fields. The user is required to manually configure via config mode CLI or, partially configure the management interface and move to Web UI Day0 flow. Day 0 configuration is not available via Day 0 CLI setup and is manually configured at Day 1

Starting 17.4, a full-fledged configuration via the CLI in the Day0 of the box is available. As a result, the controller is ready for access point and client join post Day0 CLI Wizard. HA SSO can be configured at Day 0 and successful pairing happens after the controllers reload. This is supported on all physical appliances and 9800-CL private cloud. There is no support for public cloud since the images are bootstrapped and don't need a day0 configuration.

A fresh box or rebooting a pre-configured box upon 'write erase' will bring the box into day0 mode. The following screenshots show a sample Day 0 CLI flow.

- The device management and wireless management addresses should be in different subnets

```
Would you like to enter the initial configuration dialog? [yes/no]:
Num of cpu cores      4
Maximum number of AP's supported  1000
yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '['].

This is a Wireless LAN Controller (WLC) basic setup wizard.
Please complete the basic management setup to access the UI wizard over http/https.

Setup device management interface? [yes]:
No startup-config, starting autoinstall/pnp/ztp...

Autoinstall will terminate if any input is detected on console

Select interface to be used for device management
 1. GigabitEthernet1 [Up]
 2. GigabitEthernet2 [Up]
 3. GigabitEthernet3 [Up]
Choose the interface to config [1]: 1
Configure static IP address? [yes]:
  Enter the interface IP [GigabitEthernet1]: 10.104.171.17
  Enter the subnet mask [GigabitEthernet1] [255.0.0.0]: 255.255.255.0

Configure static route? [yes]: no

Enter the management username: admin
Enter the password: *****
Reenter the password: *****
```

- The configurations required for a box configured as standby will be lesser than standalone/active boxes.
- VLAN ID is a mandatory config for wireless management interface since it is by default an SVI

```
Choose the deployment mode
 1. Standalone
 2. Active
 3. Standby
Enter your selection [1]: 1

Configuring wireless management interface
Select interface to be used for wireless management
 1. GigabitEthernet2 [Up]
 2. GigabitEthernet3 [Up]
Choose the interface to config [1]: 1
Enter the vlan ID (1-4094): 18
Configure IPv4 address? [yes]:
Enter the interface IP [GigabitEthernet2]: 9.8.18.90
Enter the subnet mask [GigabitEthernet2] [255.0.0.0]: 255.255.255.0
Configure IPv6 address? [yes]: no
Do you want to configure a VLAN DHCP Server? [yes]:
Enter the VLAN DHCP Server IP [GigabitEthernet2]: 9.1.0.101

Configure static route? [yes]:
Enter the destination prefix [0.0.0.0]:
Enter the destination mask [0.0.0.0]:
Enter the forwarding router IP: 9.8.18.1
Enter the hostname [WLC]:

Configure credentials for management access on Access Points? [yes]:
Enter the management username: admin
Enter the management password: *****
Reenter the password: *****
Error! Passwords dont match, please retry
Enter the management password: *****
Reenter the password: *****
Enter the privileged mode access password: *****
Reenter the password: *****

Configure country code(s) for wireless operation in ISO format [US]: US,IN
Configure a NTP server now? [yes]: no
Configure the system time now? [yes]:
```

- Self Signed Certificate generation for 9800-CL will take place once the initial configuration is applied.
- Hence the user will not be able to see it in running config before exiting the wizard

```
Configure a NTP server now? [yes]: no
Configure the system time now? [yes]:
Enter the date in MM/DD/YYYY format: 09/02/2020
Enter the time in HH:MM:SS format: 13:13:40

Configure timezone? [yes]:
Enter name of timezone: UTC
Enter hours offset from UTC (-23,23): 5
Enter mins offset from UTC (0,59) [0]: 30

Configure Wireless client density? [yes]: no
Configure AAA servers? [yes]: no
Configure Wireless network settings? [yes]: no
Configure virtual IP? [yes]:
Enter the virtual IP [192.0.6.1]:

Configure RF-Network Name? [yes]: no

Auto generate certificate for AP join? [yes]:
Choose key size
 1. 2048
 2. 3072
 3. 4096
Enter your selection [1]: 3
Choose the signature algorithm
 1. SHA256
 2. SHA384
Enter your selection [1]: 2
Enter secret key(minimum 8 characters): *****
Self Signed Certificate generation will be done after system boots up.
```

- User can verify the configuration generated
- User can terminate Day-0 wizard by executing CTRL+C at any point during the process.


```
The following configuration command script was created:
|
| interface GigabitEthernet1
| no switchport
| no shutdown
| no ip address dhcp
| ip address 10.104.171.17 255.255.255.0
| no mop enabled
|
| username admin privilege 15 secret 9 $9SydJg9CYGnosXCUS.zx10bbYwZc6ZkwSS7mGj08oUkexY09zaRn0Z1drvhc
|
|
| vlan 18
| no shutdown
|
| interface GigabitEthernet2
| switchport
| switchport mode trunk
| switchport trunk allowed vlan 18
| no shutdown
|
| interface vlan 18
| no switchport
| no shutdown
| no ip address dhcp
| ip address 9.8.18.90 255.255.255.0
| ip helper-address 9.1.0.101
| no mop enabled
|
| ip route 0.0.0.0 0.0.0.0 9.8.18.1
|
| wireless management interface vlan 18
|
| hostname WLC
|
| ap profile default-ap-profile
| mgmtuser username admin password 0 Cisco@123 secret 0 Cisco@123
```

- The user will be presented with an option to save the config or to reconfigure entire config at the end of the wizard
- There is no option to go back and modify individual config

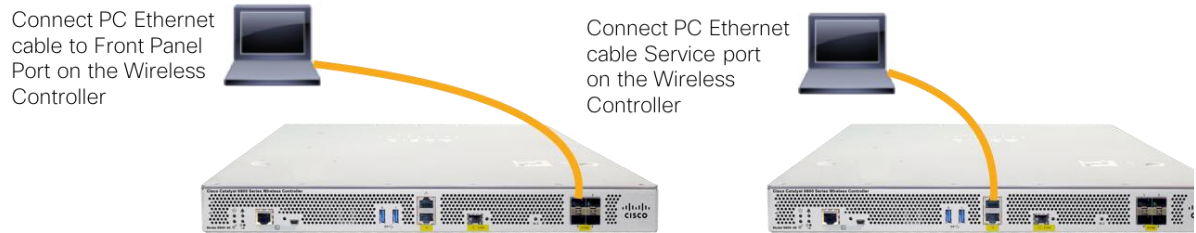
```
ntp server 9.8.22.20 maxpoll 4 minpoll 4
|
| end
|
| wireless profile policy default-policy-profile
| shutdown
| vlan 18
| no shutdown
| exit
| wireless country US
| wireless country IN
|
| [0] Go to the IOS command prompt without saving this config.
| [1] Return back to the setup without saving this config.
| [2] Save this configuration to nvram and exit.
|
| Enter your selection [2]: 2
| Building configuration...
| [OK]
| Use the enabled mode 'configure' command to modify this configuration.
|
| Building configuration...
| [OK]
|
| Press RETURN to get started!
|
| *Sep 2 10:58:30.092: %SYS-5-CONFIG P: Configured programmatically by process Setup from console as console
| *Sep 2 10:58:30.116: %SELINUX-3-MISMATCH: chassis 1 R0/0: audispd: type=AVC msg=audit(1599044310.115:139): avc: denied { getattr } for pid=2851 comm="" read
| link" path="/dev/sda1" dev="devtmpfs" ino=20799 scontext=system_u:system_r:polaris_psd t:s0 tcontext=system_u:object_r:fixed_disk_device_t:s0 tclass=blk_file
| permissions]
| *Sep 2 10:58:30.817: %LINK-3-UPDOWN: Interface GigabitEthernet1, changed state to up
| *Sep 2 10:58:30.836: %LINK-3-UPDOWN: Interface GigabitEthernet2, changed state to up
| WLC
```

Day 0 configuration for C9800-40, C9800-80 and C9800-L

Procedure

- Step 1** Connect a PC laptop's wired Ethernet port directly to Front Panel Port or to the Service Port IP (DHCP or Static) of the wireless controller (see the following figure). The port LEDs blink to indicate that both machines are properly connected. To connect via service port, connect the console, connect the uplink and service port to switch ports and then remotely login to set the hostname, user credential, IP and route on the device management interface. Once this is setup Day 0 on service port can be accessed by pointing the https browser session to the statically assigned IP.

Figure 1. Front Panel and Service port support Day 0 UI



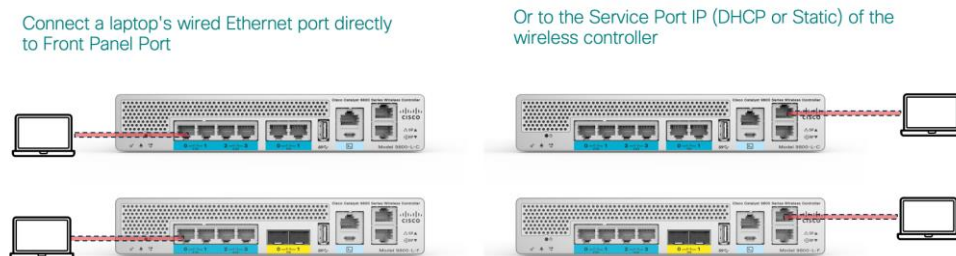
Note It may take several minutes for the wireless controller to fully power on to make the GUI available to the PC. Do not auto configure controller.

The LEDs on the front panel provide system status:

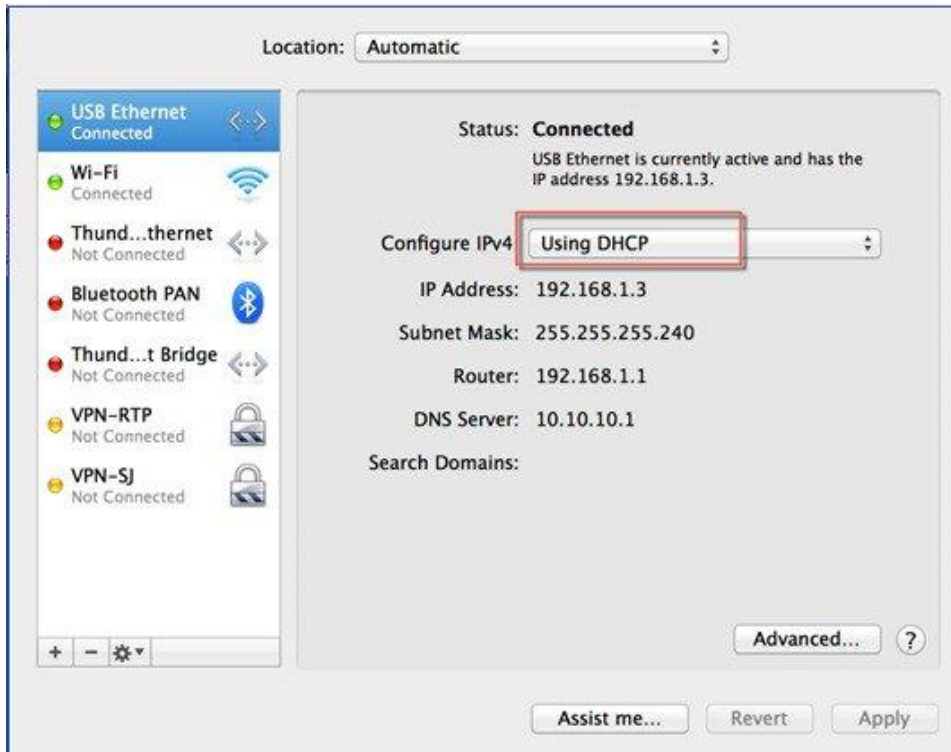
The system is not ready – LEDs is OFF

The controller is ready – LED is solid green

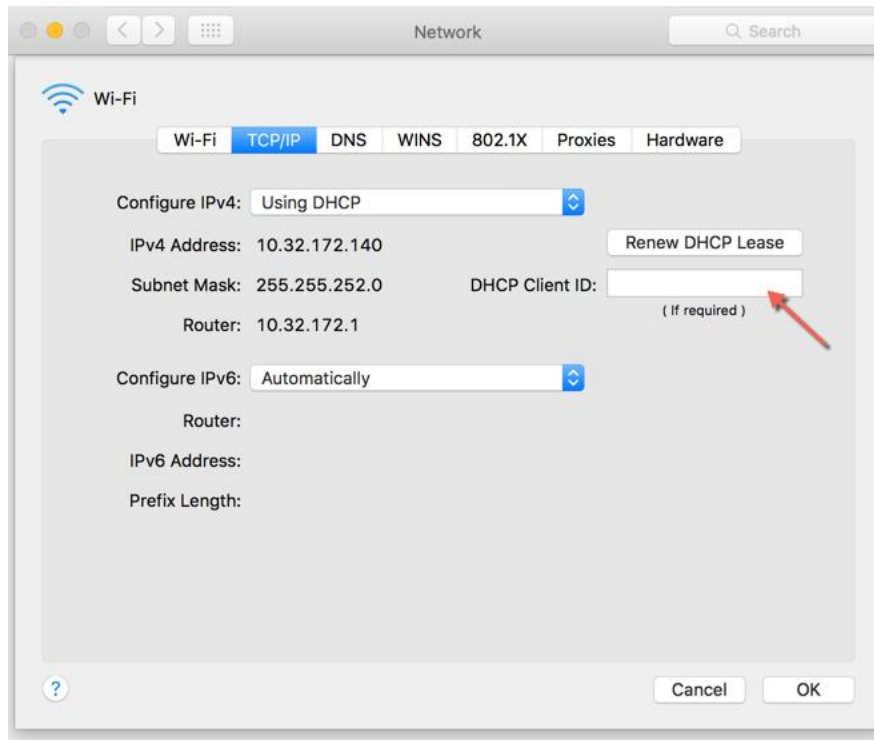
On the Catalyst 9800-L wireless controller, connect a PC laptop's wired Ethernet port directly to Front Panel Port or Service Port to access the Express Day 0 UI as shown below



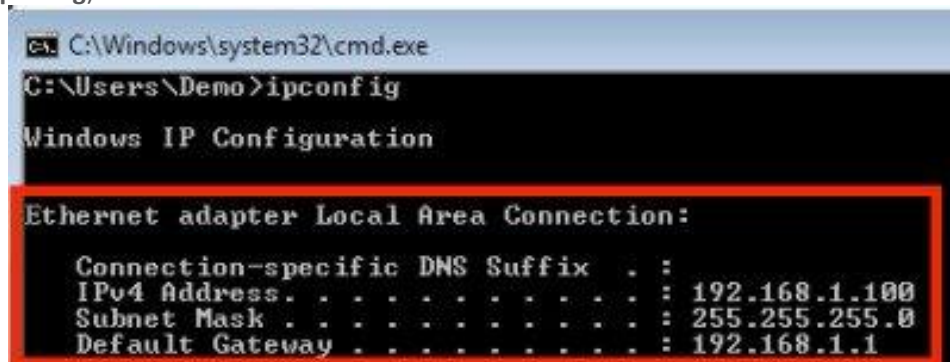
Step 2 Configure DHCP option on the Laptop if connecting to the Front Panel port. This assigns an IP address to your Laptop (192.168.1.X) or you can assign static IP address 192.168.1.X to your Laptop to access the wireless controller GUI; both options are supported. The following figure shows an example of the Mac Laptop getting an IP address from the DHCP service port for the initial configuration of the controller.



Show DHCP client-id needs to be populated when connecting via the front panel port



The following figure shows an example of network settings on Windows PC (Start > Run > CMD > ipconfig).



DAY 0 configuration for C9800-CL on Private Cloud

Configuring the basic C9800-CL settings

Let's configure the minimal configuration to then connect to the web GUI interface of C9800-CL and use the DAY 0 guided flow to get the controller fully operational.

At FCS, DAY 0 assumes that the box has two separated virtual interfaces (one for device management and one for wireless management and client traffic) and that the first login happens on the device management (out of band) interface. The wireless management interface is configured via the DAY 0. If you have a different setup and for example you want to use only one interface, please see the next section on how you can skip DAY 0 guided flow and configure the initial settings via CLI.

Connect to the CLI via the VGA console and follow these steps for the basic configuration:

- Terminate the configuration wizard (this is the general ios CLI wizard and it's not specific for wireless)

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

```
Would you like to terminate autoinstall? [yes]:yes
```

- Optionally set the hostname:

```
WLC(config)#hostname C9800
```

- Add login credentials using the following command:

```
C9800(config)#username <name> privilege 15 password <yourpwd>
```

- Add an IP address on the device Management interface. The example assumes you have mapped GigabitEthernet 1 to the out of band/device management network during VM bootstrap:

```
C9800(config)#interface g1
```

```
C9800(config-if)#no switchport
```

```
C9800(config-if)#ip address 10.58.55.5 255.255.255.0
```

- Add the route to the remote network where you want to manage the C9800-CL from

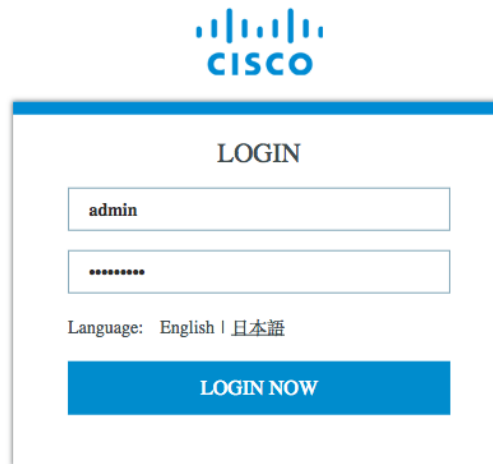
```
C9800(config)#ip route 10.58.0.0 255.255.0.0 10.58.55.254
```

Verify that you can ping your management station and then from there just <https://<IP of the device management interface>>. Use the credentials you have entered earlier. Since the box has never been configured, the web GUI will redirect you to the DAY 0 page. Please see the DAY 0 section later in the document

C9800-CL Day-0 Configuration Setup Wizard

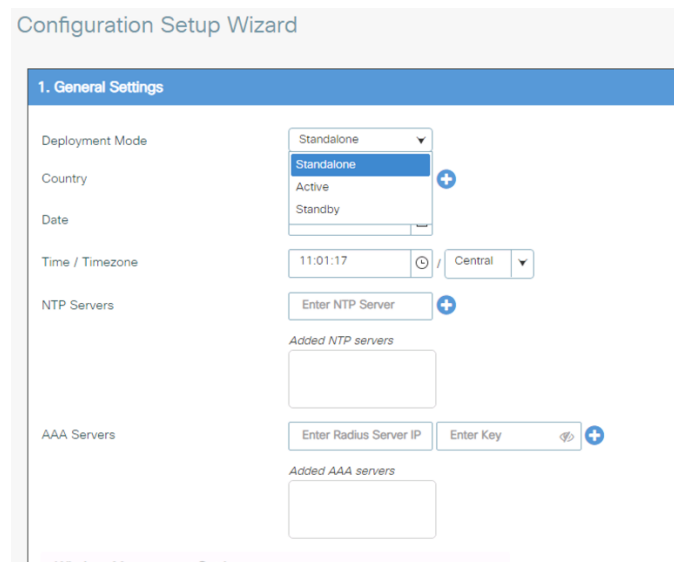
To simplify the bootstrap process of a Catalyst wireless controller, a Day-0 wizard will appear after a virtual instance is deployed, with network connectivity but without any other wireless configuration.

To connect to the DAY 0 GUI, login to the defined Device Management interface via https.



To login use the username and password credentials given during the C9800 instance creation described in the previous sections.

Once logged in, the user is presented with a simplified configuration flow to set the basic parameters and have the controller fully operational. In the first page, enter the required information:



These are: Deployment mode, Country code, Date and Time, NTP (optional) and AAA Server (optional). Note how for the VM you can chose standalone or active/standby if you want to configure SSO. Then enter the wireless Management interface configuration:

Configuration Setup Wizard

1. General Settings

Added AAA servers

Wireless Management Settings

Port Number	GigabitEthernet2
VLAN*	1-4094
IPv4	<input checked="" type="checkbox"/>
Wireless Management IP*	x.x.x.x
Subnet Mask*	x.x.x.x
Default Gateway*	x.x.x.x
Management VLAN DHCP Server	x.x.x.x (optional)
IPv6	<input type="checkbox"/>

Notice that you can only select an interface that is different from the one you used to access the GUI (so you can either select gig 2 or gi3 in this case). You can configure the interface Gigabit 2 by choosing the VLAN, the IP address and the default gateway. This will automatically configure the interface as trunk, the SVI interface for wireless management and the default gateway. Click Next

In the next page you can add a WLAN (optional) so that clients can connect. In this example the PSK dialogue is shown:

Configuration Setup Wizard

2. Wireless Network Settings

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

Network Name	Network Type
0	

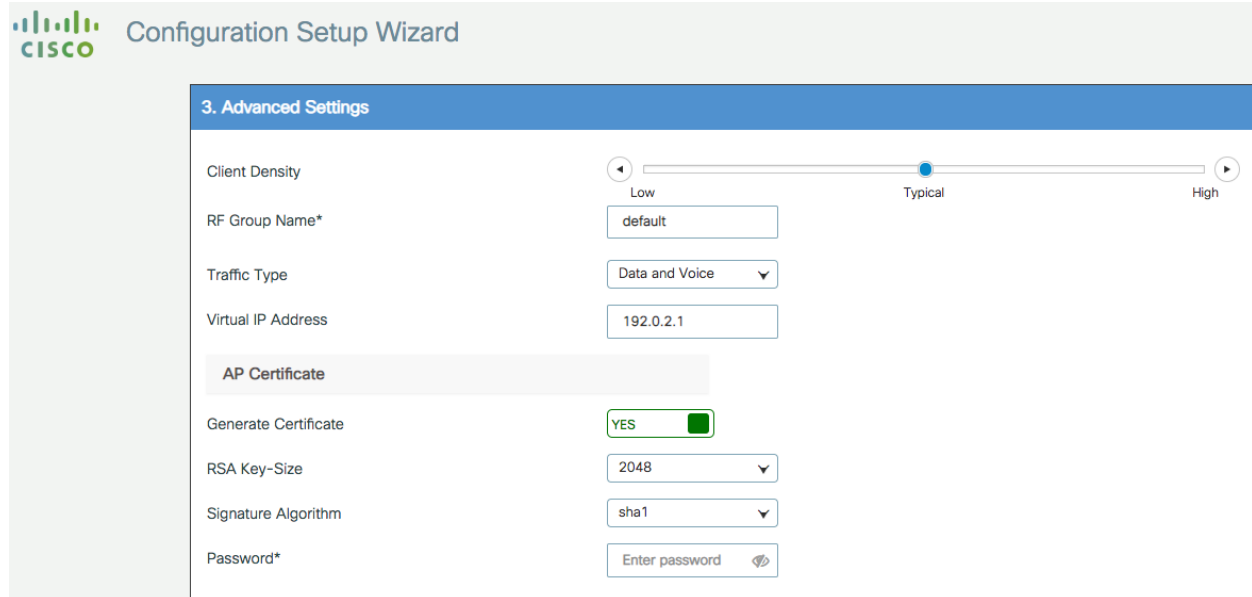
10 items per page

Add Network

Network Name*	Enter Network Name
Network Type	<input checked="" type="radio"/> Employee <input type="radio"/> Guest
Security	WPA2 Personal
Pre-Shared Key*	<input type="text"/>

[Cancel](#) [+ Add](#)

In the next page the user can set some basic RF parameters and the AP certificate.



3. Advanced Settings

Client Density

RF Group Name*

Traffic Type

Virtual IP Address

AP Certificate

Generate Certificate YES

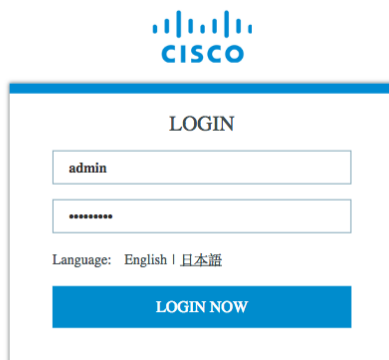
RSA Key-Size

Signature Algorithm

Password*

A trust point is basically a certificate authority that you trust, and it is called a trust point because you implicitly trust this authority. A trust point certificate is a self-signed certificate, hence the name trust point, since it does not rely on the trust of anyone else or other party. A trust point is needed for AP to join the C9800-CL and the user can decide to auto generate one during DAY 0, or can toggle the “Generate Certificate” to NO and then it will have to configure its own certificate authority at DAY 1 for APs to join.

Click Summary to review the configuration and then click Finish. The configuration and trust point will be pushed to the device and the user will be logged out. The 9800-CL controller will not reboot but it will take about 60s to prompt the user to login again; enter the same credentials:



LOGIN

Language: English | 日本語

LOGIN NOW

This time it will skip the DAY 0 page since the box has already an initial configuration, and the user will

be redirected to the main Dashboard for DAY 1 configuration

C9800-CL configuring via CLI: skipping the DAY 0 guided flow

If the user doesn't want to use two separated virtual interfaces for device management and wireless management, then he/she can configure the day zero configuration via CLI and then access the GUI for DAY 1 configuration.

Follow these steps to configure the c9800 with a wireless management interface and skip the DAY 0. This example assumes that Gigabit Ethernet 1 is connected to a trunk interface on the switch and you want to configure multiple VLANs and dedicate one for Wireless Management interface

Step 1. Access the CLI via the vga/monitor console of ESXi

Step 2. Terminate the configuration wizard (this wizard it's not specific for wireless controller)

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

```
Would you like to terminate autoinstall? [yes]:yes
```

Step 3. Optionally set the hostname:

```
WLC(config)#hostname C9800
```

Step 4. Enter the config mode and add login credentials using the following command:

```
C9800(config)#username <name> privilege 15 password <yourpwd>
```

Step 5. Configure the VLAN for wireless management interface

```
C9800#conf t  
Enter configuration commands, one per line. End with CNTL/Z.
```

```
C9800(config)#vlan 122
```

```
C9800(config-vlan)#name wireless_management
```

Step 6. Configure the SVI for wireless management interface, for example:

```
C9800(config)#int vlan 122
```

```
C9800(config-if)#ip address 172.20.229.21 255.255.255.192
```

```
C9800(config-if)#no shutdown
```

Step 7. Configure the interface gigabit 1 as trunk:

```
C9800(config-if)#interface GigabitEthernet1
```

```
C9800(config-if)#switchport mode trunk
```

```
C9800(config-if)#switchport trunk allowed vlan 122
```

```
C9800(config-if)#shut
```

```
C9800(config-if)#no shut
```

Step 8. Configure a default route (or a more specific route) to reach the box:

```
C9800(config-if)#ip route 0.0.0.0 0.0.0.0 172.20.229.1
```

Step 9. Disable the wireless network to configure the country code:

```
C9800(config)#ap dot11 5ghz shutdown
```

Disabling the 802.11a network may strand mesh APs.

```
Are you sure you want to continue? (y/n)[y]: y
```

```
C9800(config)#ap dot11 24ghz shutdown
```

Disabling the 802.11b network may strand mesh APs.

```
Are you sure you want to continue? (y/n)[y]: y
```

Step 10. Configure the AP country domain. This configuration is what will trigger the GUI to skip the DAY 0 flow as the C9800 needs a country code to be operational:

```
C9800(config)# c9800-10-30(config)#ap country ?
```

WORD Enter the country code (e.g. US,MX,IN) upto a maximum of 20 countries

Step 11. A certificate is needed for the AP to join the virtual C9800. This can be created automatically via the DAY 0 flow or manually using the following commands

- Specify the interface to be the wireless management interface

```
C9800(config)#wireless management interface vlan 122
```

- in exec mode, issue the following command:

```
C9800(#wireless config vwlc-ssc key-size 2048 signature-algo sha256 password 0 <pwd>
Configuring vWLC-SSC...
Script is completed
```

This is a script the automates the whole certificate creation:

- Verifying Certificate Installation:

```
C9800#show wireless management trust point
Trustpoint Name : ewlc-default-tp
Certificate Info : Available
Certificate Type : SSC
Certificate Hash : e55e61b683181ff0999ef317bb5ec7950ab86c9e
Private key Info : Available
```

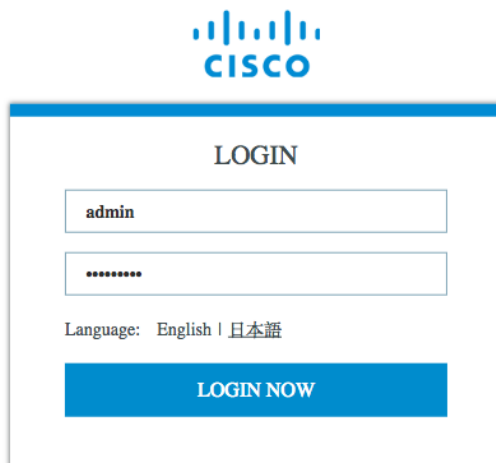
Note: you can skip the certificate/trust point configuration but if you do it, APs will not able to join. You would need to go to the GUI and configure it from there by importing the desired certificate.

Verify that you can ping the wireless management interface and then just <https://<IP>> of the device wireless management interface>. Use the credentials you have entered earlier. Since the box has a country code configured, the GUI will skip DAY 0 page and you will get access to the main Dashboard for DAY 1 configuration.

DAY 0 configuration for C9800-CL on Public Cloud

The purpose of the DAY 0 Web Graphical User Interface (GUI) is to facilitate the first Catalyst 9800 Wireless Controller setup and provide the instance with the necessary configurations for APs and clients to join. The DAY 0 GUI is triggered every time the wireless controller has not been configured with a Regulatory Country Domain and hence is not operational.

To connect to the DAY 0 GUI, login to the defined Device Management/Wireless Management interface via https.



To login use the username and password credentials given during the C9800 instance creation described in the previous sections.

Once logged in, the user is presented with a simplified configuration flow to set the basic parameters and have the controller fully operational.

In the first page, enter the required information:

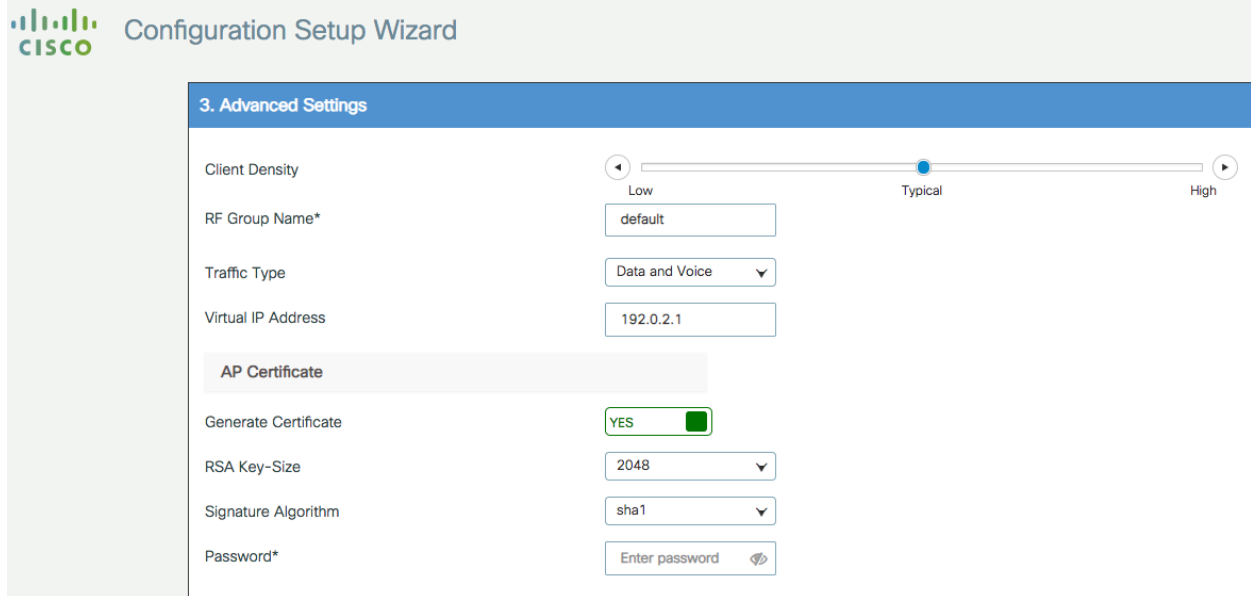
The screenshot shows the '1. General Settings' step of the Configuration Setup Wizard. It includes fields for Country (US,IT), Date (25 Oct 2018), Time / Timezone (15:16:54, CEST), NTP Servers (172.16.254.254), and AAA Servers (172.16.3.51). Below these is the 'Wireless Management Settings' section with Port Number (GigabitEthernet1) and IP Address (10.10.20.5).

These are: Country code, Date and Time, NTP (optional) and AAA Server (optional). Notice that only interface Gigabit 1 is present on the box as only one interface is supported. Click Next

In the next page you can add a WLAN (optional) so that clients can connect. In this example the PSK dialogue is shown:

The screenshot shows the '2. Wireless Network Settings' step. It features a table with columns for Network Name and Network Type. A modal dialog titled 'Add Network' is open, containing fields for Network Name*, Network Type (Employee selected, Guest unselected), Security (WPA2 Personal), and Pre-Shared Key*.


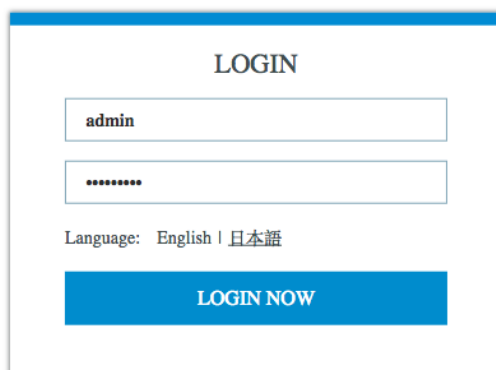
In the next page the user can set some basic RF parameters and the AP certificate.



The screenshot shows the '3. Advanced Settings' page of the Configuration Setup Wizard. It includes a slider for 'Client Density' set to 'Typical', a text field for 'RF Group Name*' with 'default', a dropdown for 'Traffic Type' with 'Data and Voice', and a text field for 'Virtual IP Address' with '192.0.2.1'. Under the 'AP Certificate' section, 'Generate Certificate' is set to 'YES', 'RSA Key-Size' is '2048', 'Signature Algorithm' is 'sha1', and 'Password*' is 'Enter password'.

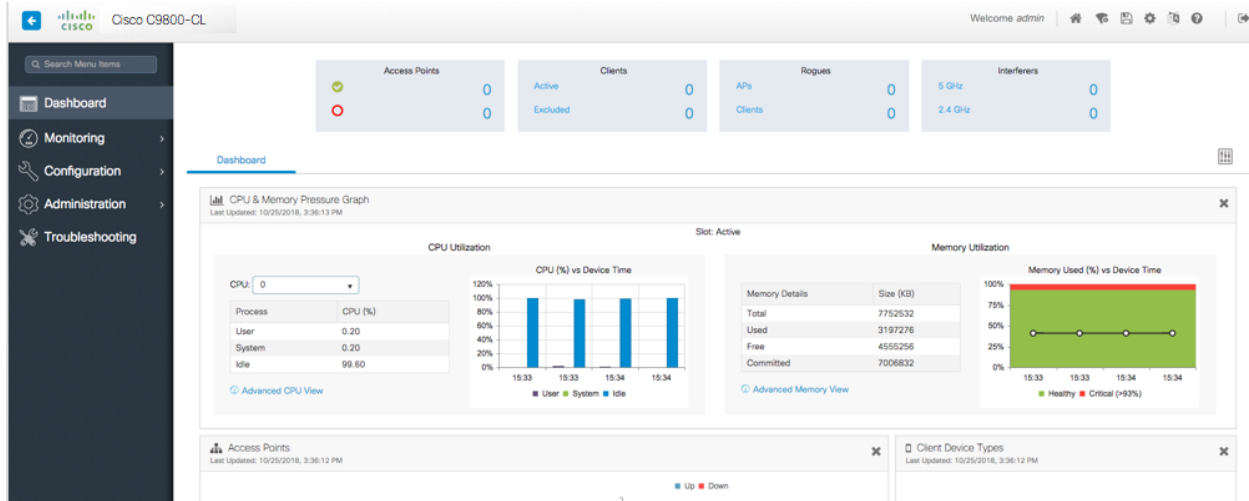
A trust point is basically a certificate authority that you trust, and it is called a trust point because you implicitly trust this authority. A trust point certificate is a self-signed certificate, hence the name trust point, since it does not rely on the trust of anyone else or other party. A trust point is needed for AP to join the C9800-CL and the user can decide to auto generate one during DAY 0, or can toggle the “Generate Certificate” to NO and then it will have to configure its own certificate authority at DAY 1 for APs to join.

Click Summary to review the configuration and then click Finish. The configuration and trust point will be pushed to the device and the user will be logged out. The 9800-CL controller will not reboot but it will take about 60s to prompt the user to login again; enter the same credentials:

The screenshot shows a 'LOGIN' form with a text field containing 'admin', a password field with masked characters, a language selection 'Language: English | 日本語', and a blue 'LOGIN NOW' button.

This time it will skip the DAY 0 page since the box has already an initial configuration, and the user will be redirected to the main Dashboard:



Configuring the AP certificate manually

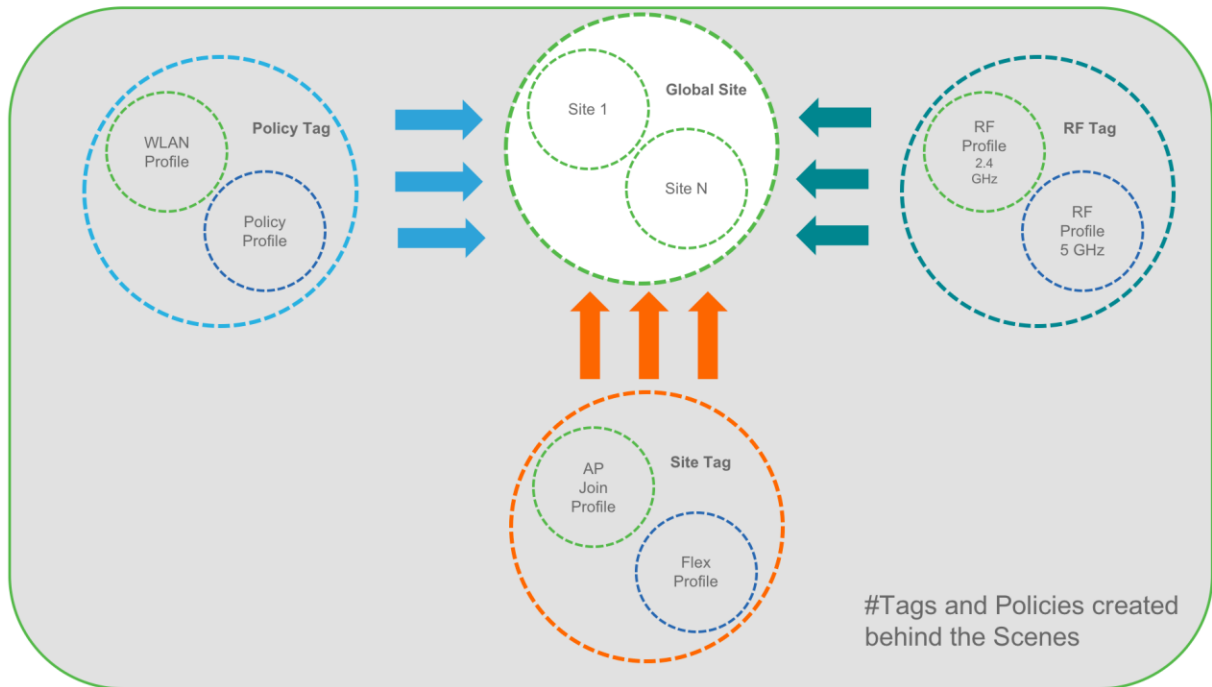
In case the customer skips day 0 and goes directly to the DAY 1 GUI of the controller, the user has to do the following steps before he can access the controller main GUI:

- 1) Assign a country code via the ios command
`c9800-10-30(config)#ap country <country code>`
 Once set, the GUI will skip the DAY 0
- 2) For APs you join you need to create a certificate. If you want to have an internally generated certificate, you can it manually running the following script:
`C9800-CL(config)# wireless config vwlc-ssc key-size 2048 signature-algo sha256 password`
 Verify the command is successful and that you can
`c9800-CL#sh wireless management trust point`
Trustpoint Name : ewlc-default-tp
Certificate Info : Available
Certificate Type : SSC
Certificate Hash : 10c07d17e69c8a04658ff96262db9c7babc55247
Private key Info : Available
FIPS suitability : Not Applicable

Your Cisco Catalyst 9800 is ready to use! Please use the general configuration guide for DAY 1 configuration

Wireless Basic Workflow

The wireless basic setup uses intent-based workflows to define local and remote sites, create wireless networks for these sites, define policies such as VLAN, ACL and QoS and also fine-tune RF characteristics. Corresponding policies and tags are created in the backend in accordance with the new configuration model but are transparent to the end-user. Access points are assigned to the site and in turn are assigned policy, RF and site tags.



In order to access the Basic Wireless Setup, click on the Wireless Setup Icon on the top-right hand corner of the dashboard page and select 'Basic' as shown below

The screenshot shows the Cisco Catalyst 9800 Wireless Controller GUI. At the top, there is a navigation bar with "Welcome admin" and various icons. Below this is a "Wireless Setup" section with a "Select Type" dropdown menu. The dropdown menu is open, showing options: "Basic" and "Advanced". A red arrow points to the "Advanced" option. Below the dropdown are three summary cards: "Access Points" (4 Active, 0 Excluded), "Clients" (0 Active, 0 Excluded), and "Rogues" (257 APs, 55 Clients). Below these is a "Dashboard" section with a "CPU & Memory Pressure Graph" widget. The widget is titled "Slot: Active" and "Last Updated: 11/6/2018, 2:55:10 PM". It contains two sub-sections: "CPU Utilization" and "Memory Utilization".

CPU Utilization

CPU: 0

Process	CPU (%)
User	0.99
System	0.49
Idle	98.30

CPU (%) vs Device Time

14:45

Legend: User (purple), System (green), Idle (blue)

Memory Utilization

Memory Details	Size (KB)
Total	16370104
Used	3670696
Free	12699408
Committed	14897684

Memory Used (%) vs Device Time

14:45

Legend: Healthy (green), Critical (>93%) (red)

Step 1: Creation of new site and General Site Settings

A location is defined as a site either in the campus(local) or across the WAN in a branch (remote) that has a specific set of services, policies and RF. Select a Name, description and Location type (Local or Flex) as well as client density as Low, Typical, or High. In the flow below, a local site is created with the name LocalSite

← Back

General | Wireless Networks | AP Provisioning

Location Name*

Description

Location Type Local Flex

Client Density (Low, Typical, High)

Step 2: Creation of Wireless Network and policies within the site

WLANs created as part of Day 0 setup are available to add to this site. These WLANs can be added as is or modified for the policy details that are required for this network in the local site. Alternatively, new SSIDs can be created using the Define new button.

← Back

✕ Delete Location

General | **Wireless Networks** | AP Provisioning

WLANs on this Location

WLAN Name	VLAN/VLAN Group
No items to display	

Wireless Network Details

WLAN* or

Policy Details

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

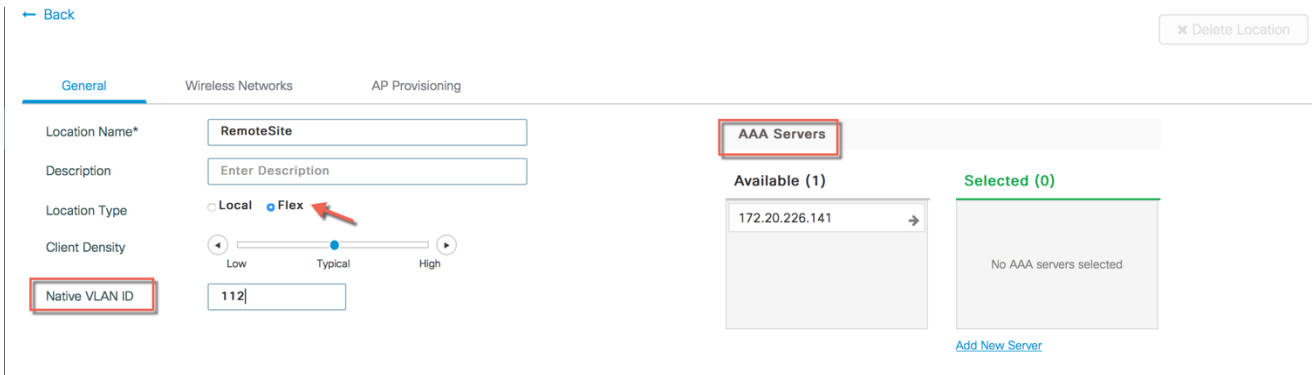
ACL or [Define new](#)

QoS

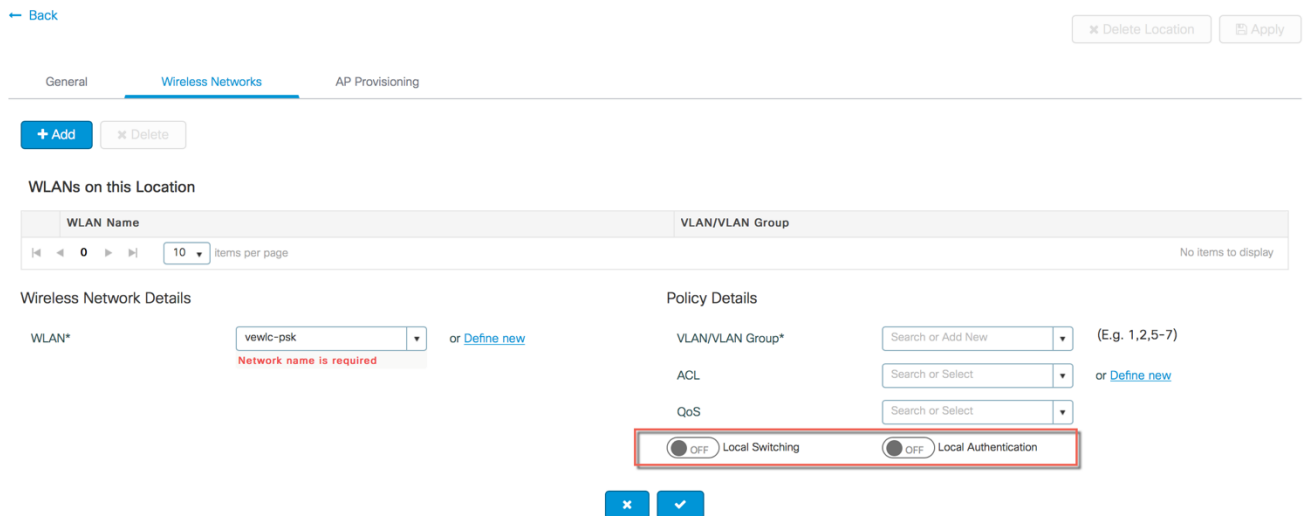
Creation of a Remote Site

Similarly, selecting Location type as “Flex” can create a remote site. In addition to the field available on the local site, remote site-specific parameters such as native VLAN ID and local AAA Servers can be configured

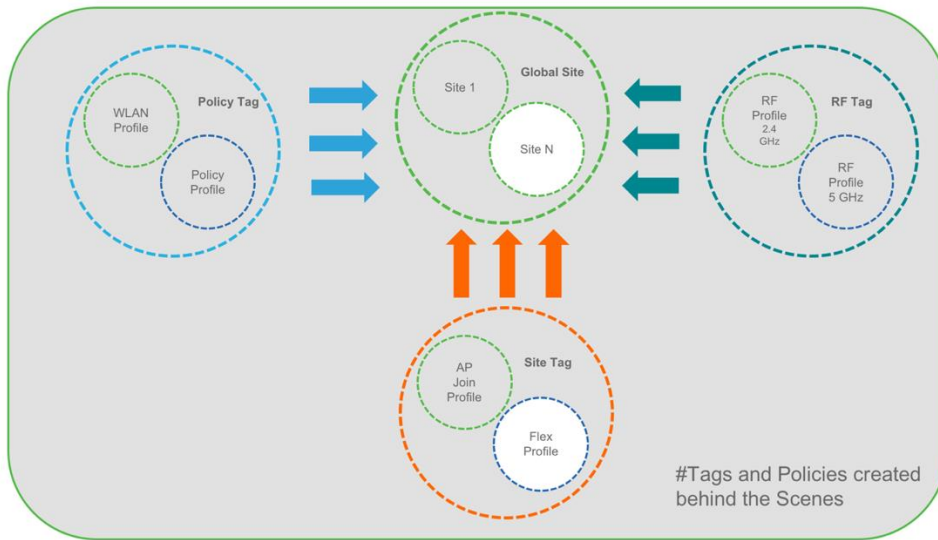
on this page. Globally defined AAA server can be used or a new server can be added using the 'Add New Server' link.



On the Wireless networks tab, the SSID being added to the remote site can be configured as a local switching, local authentication SSID.



In the backend, a custom Site tag with a custom Flex profile is defined and associated with this remote site



Step 3 : Provisioning APs to Site

Once the Wireless network and RF characteristics are setup, Access points can be added to the local/remote site either using static AP MAC address assignment or by assigning already joined APs to a specific location

← Back ✖ Delete Location Apply

General Wireless Networks **AP Provisioning**

Add/Select APs

AP MAC Address

Available AP list

Number of selected APs : 1

AP MAC	AP Name
<input checked="" type="checkbox"/> 005d.735c.b544	AP005D.735C.B544

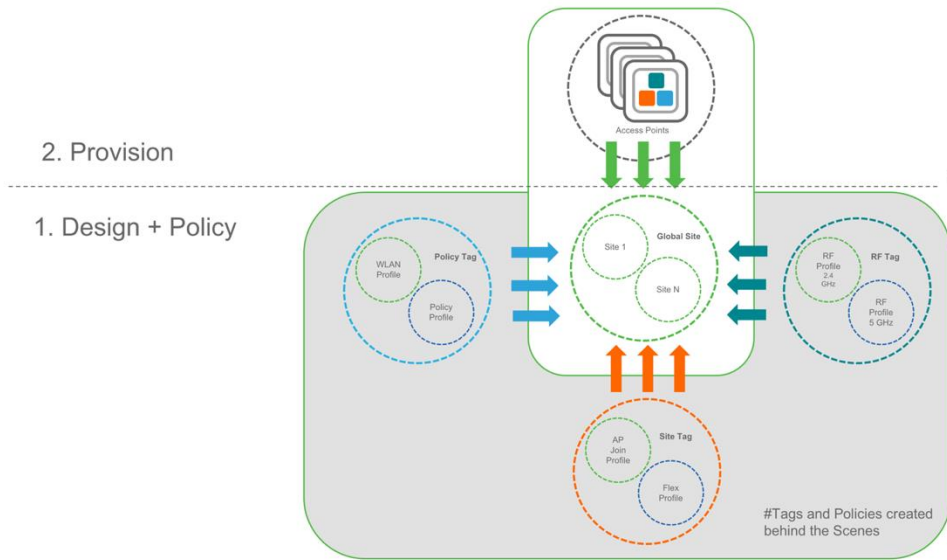
APs on this Location

Associated AP list

Number of selected APs : 0

AP MAC	AP Name	Status
No items to display		

Policy, Site and RF tags are automatically pushed to the access points upon provisioning.



Wireless Advanced Workflow

Guided workflow and Use cases

In order to access the Advanced Wireless Setup, click on the Wireless Setup Icon on the top-right hand corner of the dashboard page and select 'Advanced' as shown below

The screenshot shows the Cisco Catalyst 9800 Wireless Controller dashboard. At the top right, there is a 'Welcome admin' message and a 'Wireless Setup' icon. A dropdown menu is open, showing 'Select Type' with options for 'Basic' and 'Advanced'. A red arrow points to the 'Advanced' option. Below the dashboard, there is a 'CPU & Memory Pressure Graph' section. It includes a table for CPU Utilization, a bar chart for CPU (%) vs Device Time, a table for Memory Details, and a bar chart for Memory Used (%) vs Device Time.

Process	CPU (%)
User	0.99
System	0.49
Idle	98.30

Memory Details	Size (KB)
Total	16370104
Used	3670696
Free	12699408
Committed	14897684

A guided workflow has been created for easy navigation thru the steps required to setup the network using Cisco Catalyst 9800 Wireless Controller.

WLAN 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)
 - WLAN Profile
 - Policy Profile
 - Policy Tag
- Site Policy (Optional)
 - AP Join Profile
 - Flex Profile
 - Site Tag
- Radio Policy (Optional)
 - RF Profile
 - RF 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

Tags & Profiles

- Start
- WLAN Profile
- Policy Profile
- Policy Tag
- AP Join Profile
- Flex Profile
- Site Tag
- RF Profile
- RF Tag
- Apply
- Tag APs
- Done

The following set of steps defines the logical order of configuration. Note that apart from the WLAN profile, all profiles and tags have a default object associated with it

1. Creation of profiles

- Create the required WLAN profiles (SSIDs)
- Create the policy profiles(if non-default needed)
- Create the RF profiles(if non-default needed)
- Create the Site profile (if non-default needed)

2. Creation of Tags

- Create the Policy tag(if non-default needed)and map the SSIDs above to the policy profiles as required
- Create the RF Tag (if non-default needed) and add the RF profiles for 11a and 11b to it
- Create the Site tag(if non-default needed) and add the Flex profile (if site is a remote site) and the AP join profile(most cases will use the default)

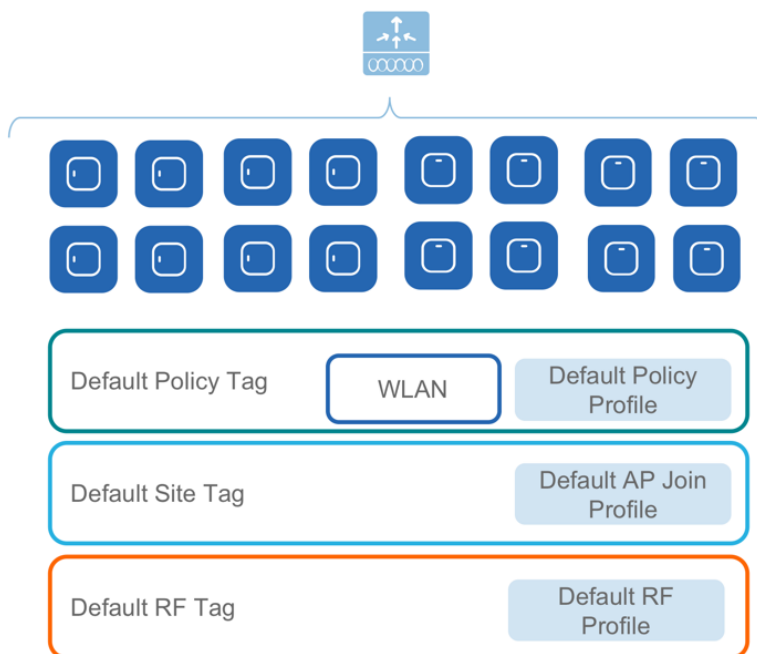
3. Associate the Tags to APs

If no custom tags are needed, this step is not required as default tags are associated with the APs
If the tag to be associated is non-default, associate the tags to the APs

- Associate RF Tag to the AP/set of APs
- Associate Policy Tag to the AP/set of APs
- Associate Site Tag to the AP/ set of APs

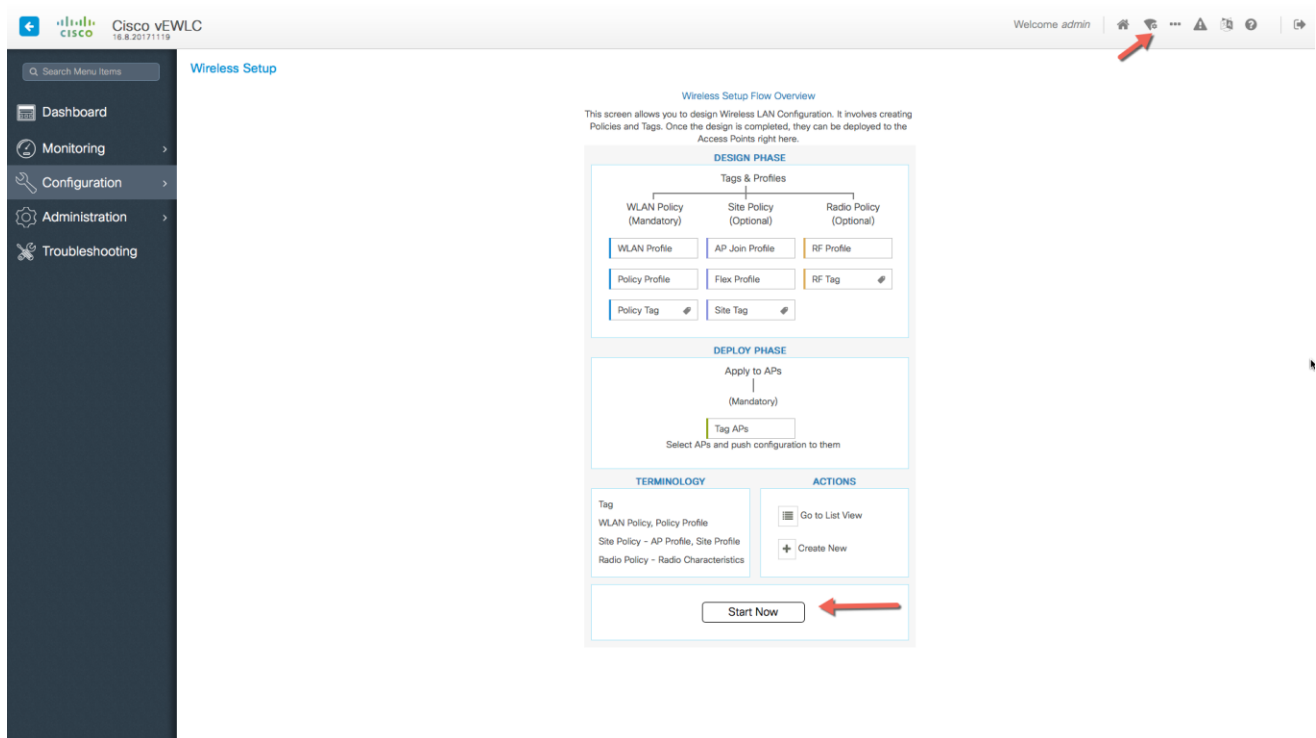
Use Case 1 - Global SSID(s) across the campus

This is a simple use-case where an enterprise has the requirement of setting up an 802.1x, IOT or Guest SSID across the campus such that it is broadcasted on all access points across the deployment. The same policies and RF characteristics are applicable to all APs that are part of this global site. This section explains how that can be achieved using the Advanced Wireless Setup workflow

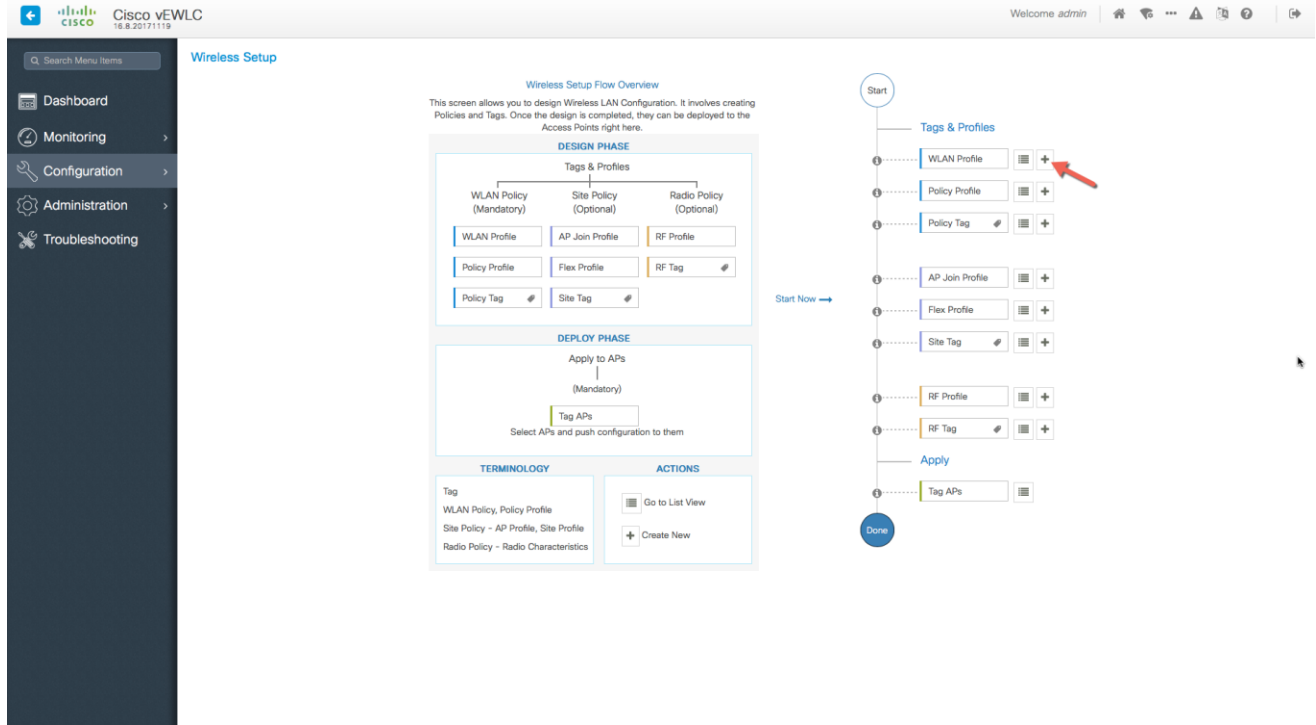


Central site – Default config with minimal changes

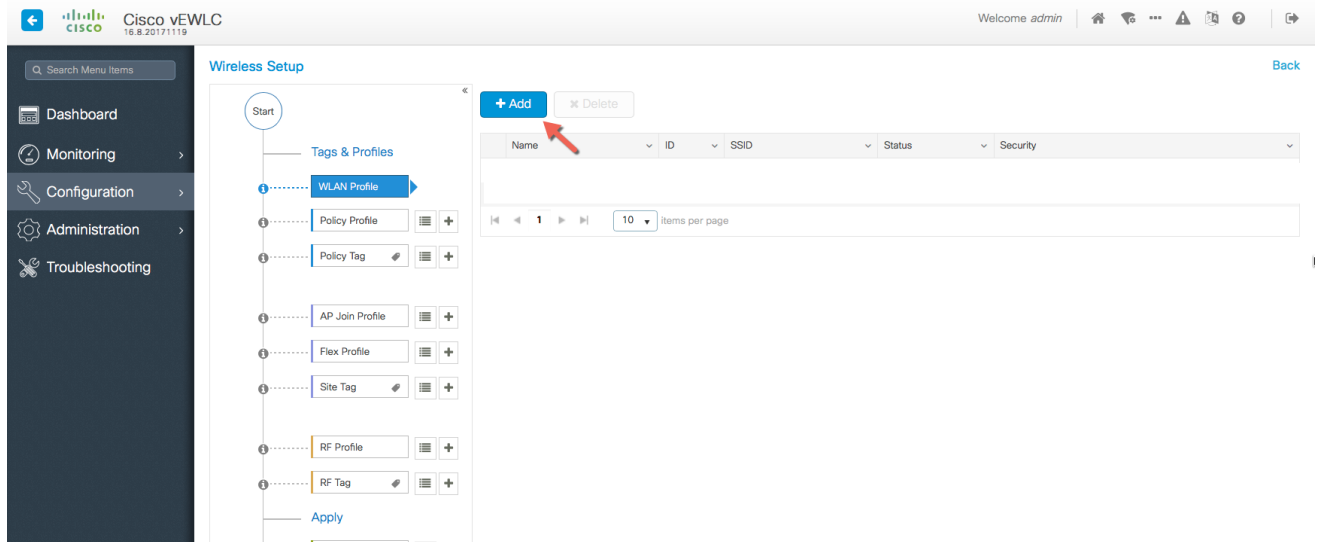
1. Create SSIDs [WLAN ID between 1-16]
 1. Click on the Wireless Setup button on the top right hand menu of the dashboard and click on Start Now after reviewing the notes on this page. The flow chart describes the set of steps in the general workflow of the Cisco Catalyst 9800 Wireless Controller configuration.



2. Begin the WLAN configuration by clicking the '+' sign next to WLAN Profile

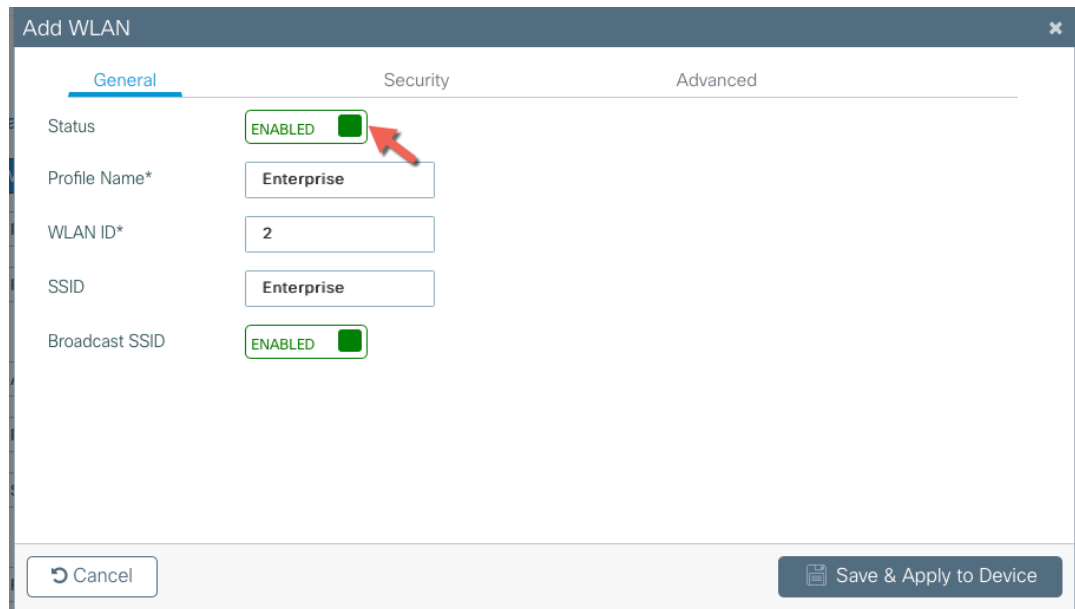


3. Click on Add button

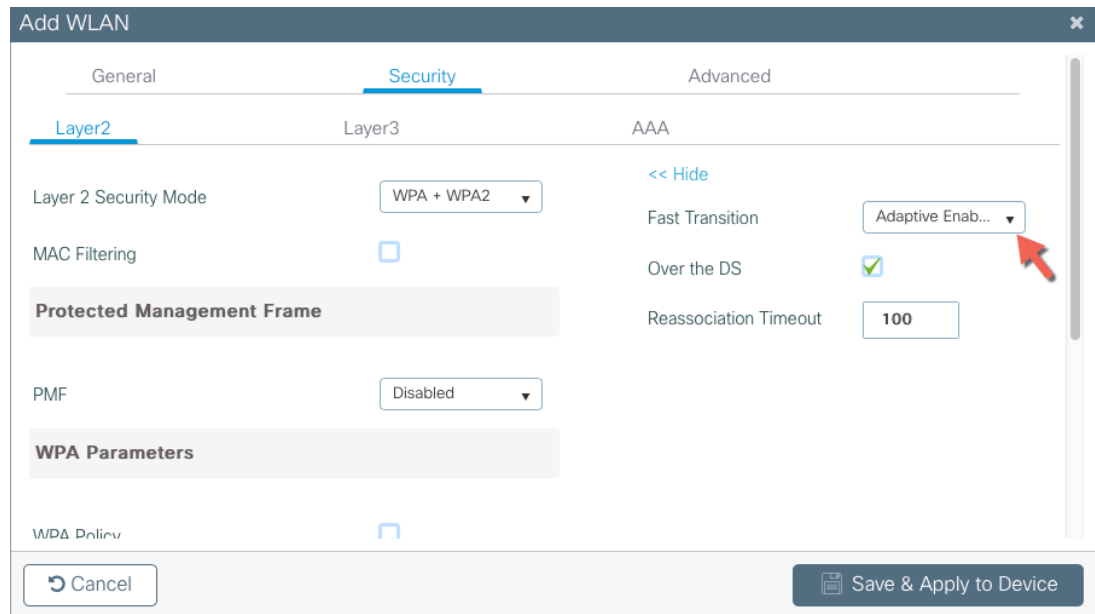


Note: SSIDs created during the Day 0 flow will automatically show up here on the WLAN profiles page

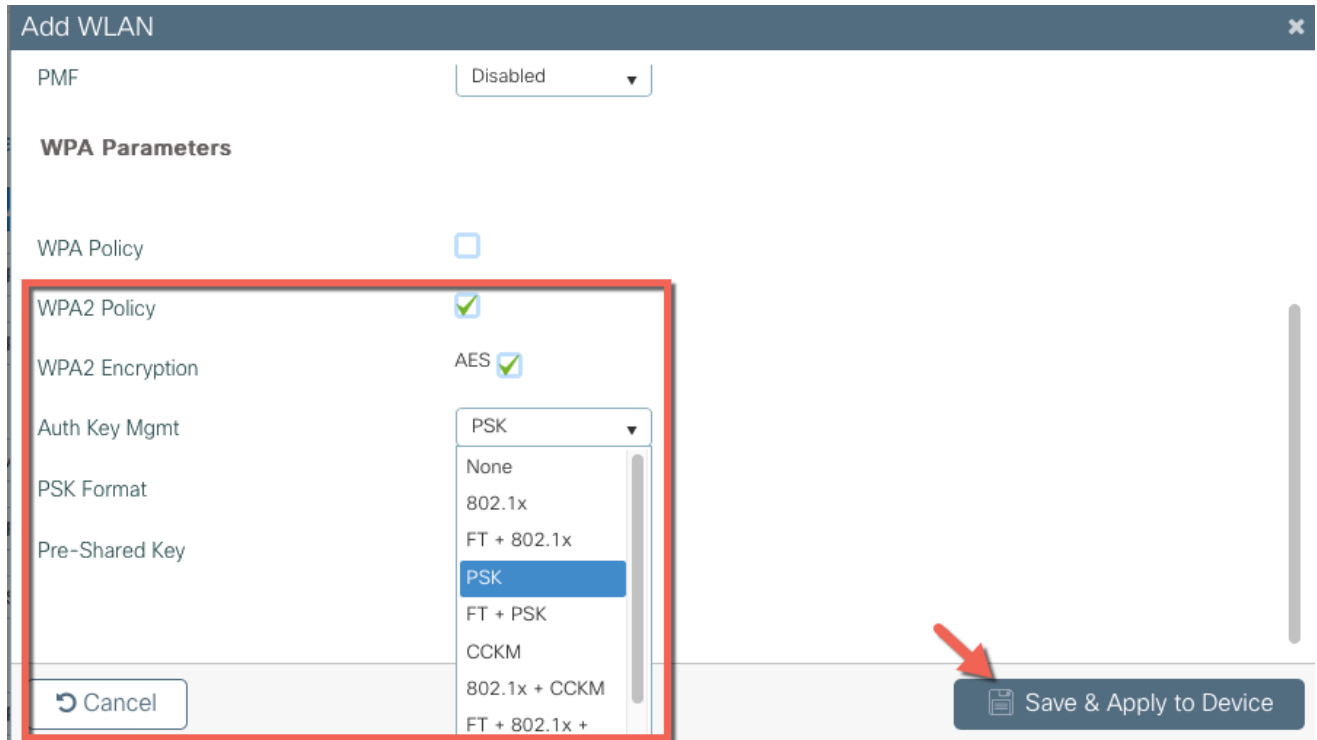
4. Specify the Profile Name of your choice, WLAN ID 1 – 16 and set the Status toggle button to Enabled.



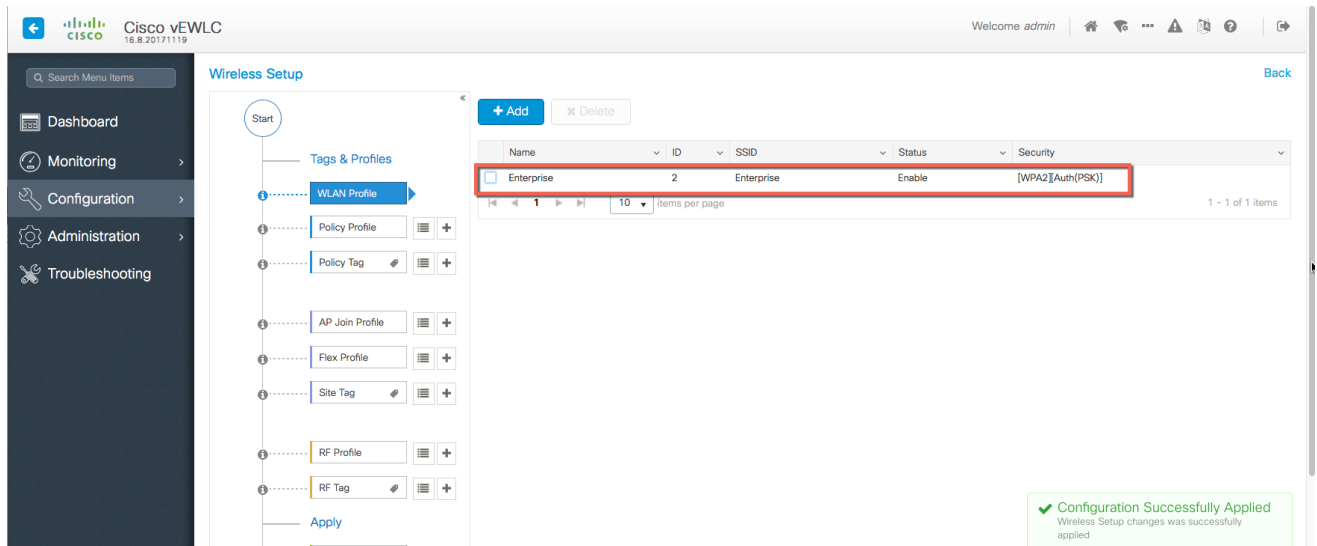
Adaptive 11r and other best practices are turned on by default



5. Select PSK or 802.1x as the Authentication Key Management (AKM) under the security tab .Save and Apply to device.



Verify that a WLAN profile is created as follows

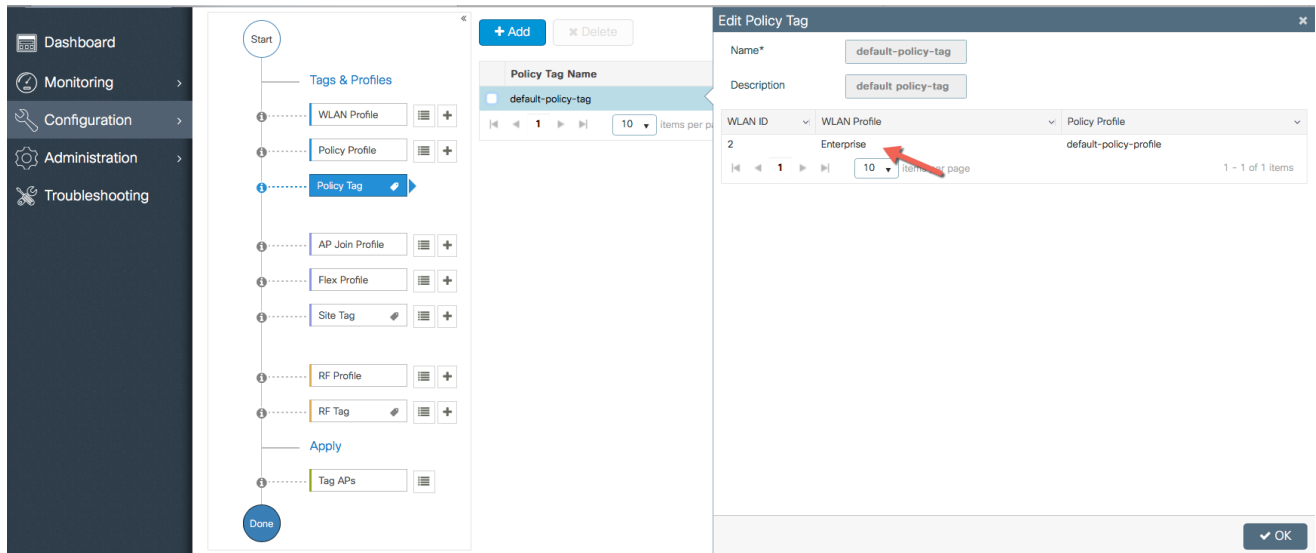


2. A Default Policy Profile and Default Policy Tag are pre-configured so no specific policy configuration is required. By default, WLAN IDs 1-16 are associated with the default policy tag

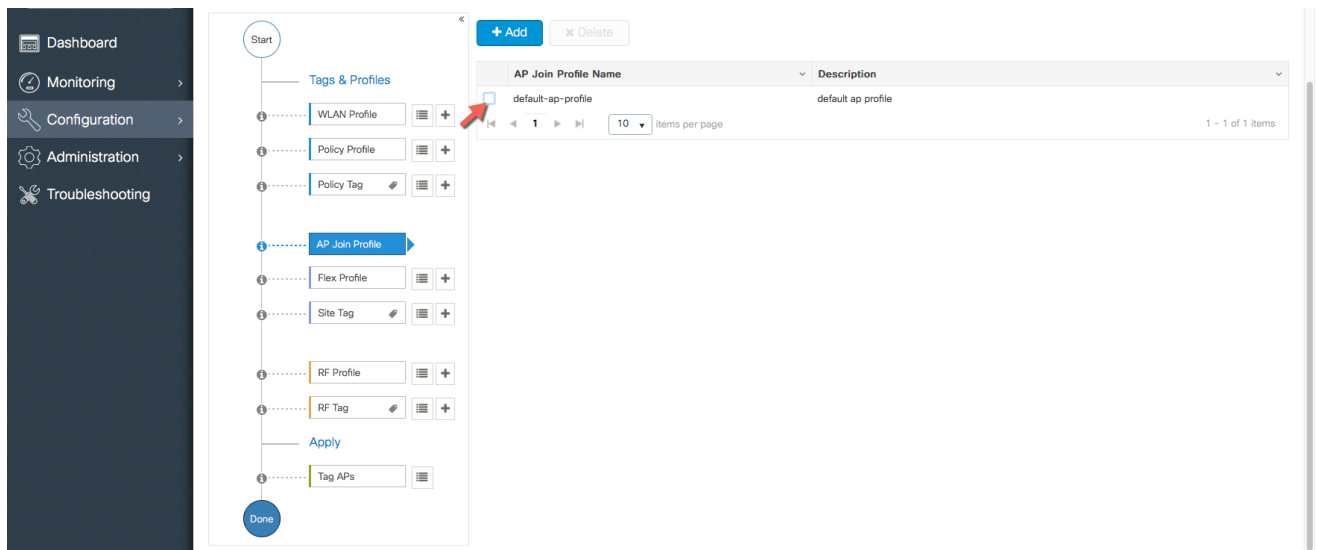
Policy Profile Name	Description	Status
default-policy-profile	default policy profile	Enable

Policy Tag Name	Description
default-policy-tag	default policy-tag

The SSID created in the first step is automatically added to this Default Policy Tag as shown below



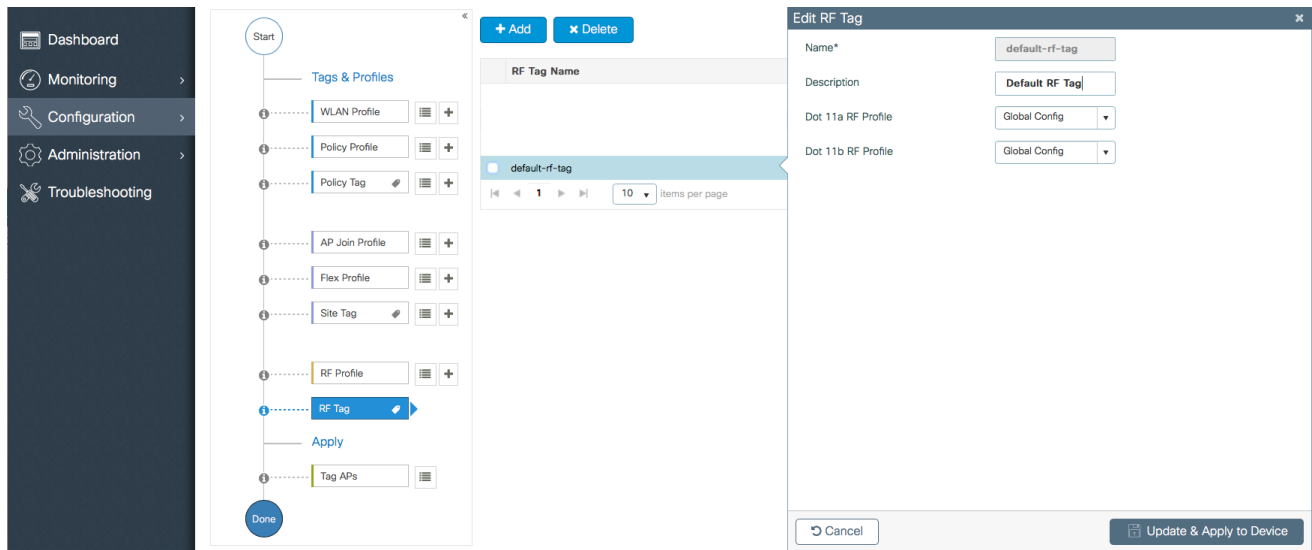
3. A Default AP Join Profile and Site Tag is available automatically so no specific site configuration is required



Site Tag Name	Description
default-site-tag	default site tag

4. A Default RF Profiles and RF Tag is pre-configured so no RF configuration is required

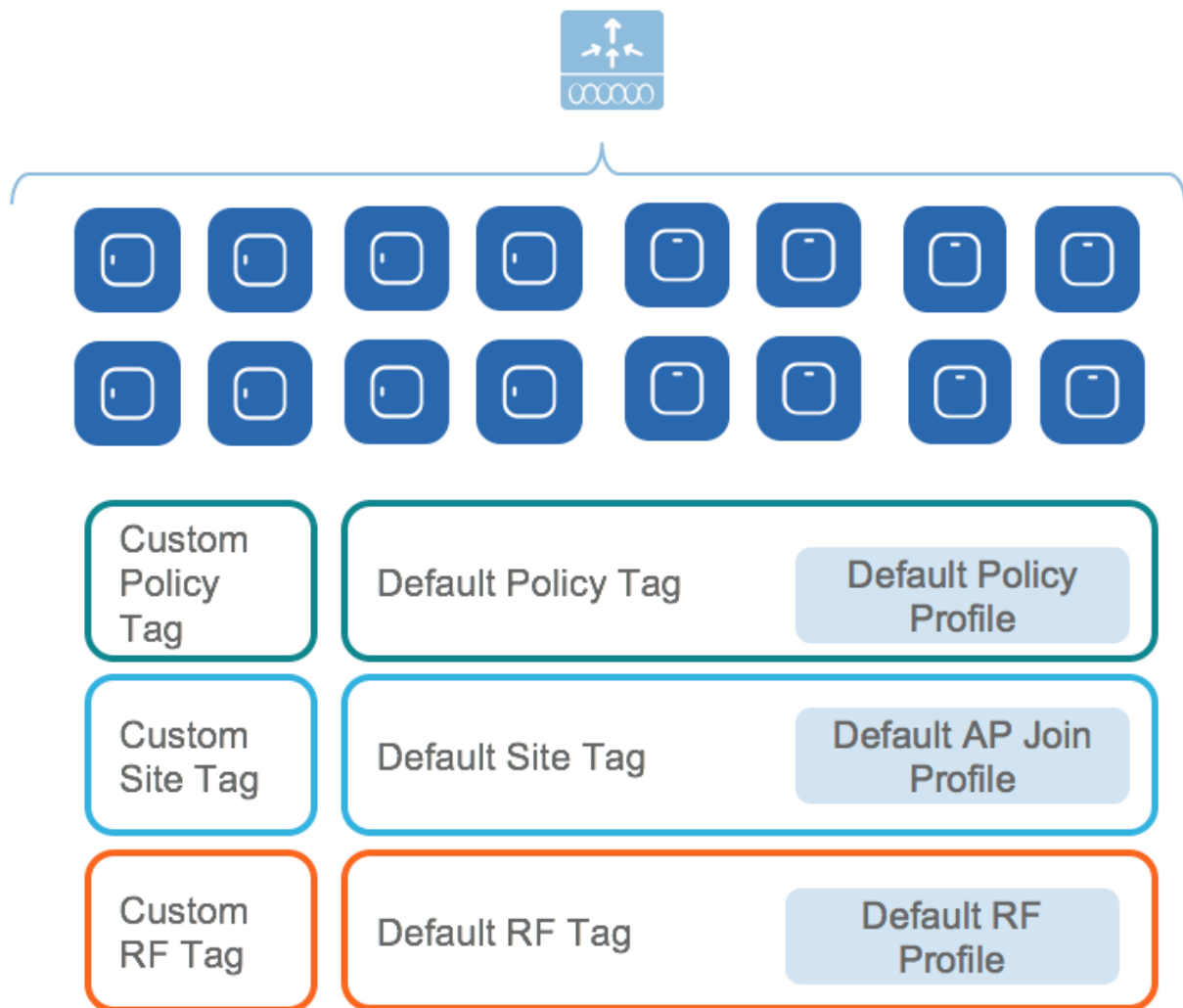
RF Profile Name	Band	State	Description
Low_Client_Density_rf_5gh	802.11a	Enable	pre configured Low Client Density rprofile for 5gh radio
High_Client_Density_rf_5gh	802.11a	Enable	pre configured High Client Density rprofile for 5gh radio
Low_Client_Density_rf_24gh	802.11b/g	Enable	pre configured Low Client Density rprofile for 2.4gh radio
High_Client_Density_rf_24gh	802.11b/g	Enable	pre configured High Client Density rprofile for 2.4gh radio
Typical_Client_Density_rf_5gh	802.11a	Enable	pre configured Typical Density rprofile for 5gh radio
Typical_Client_Density_rf_24gh	802.11b/g	Enable	pre configured Typical Client Density rprofile for 2.4gh radio



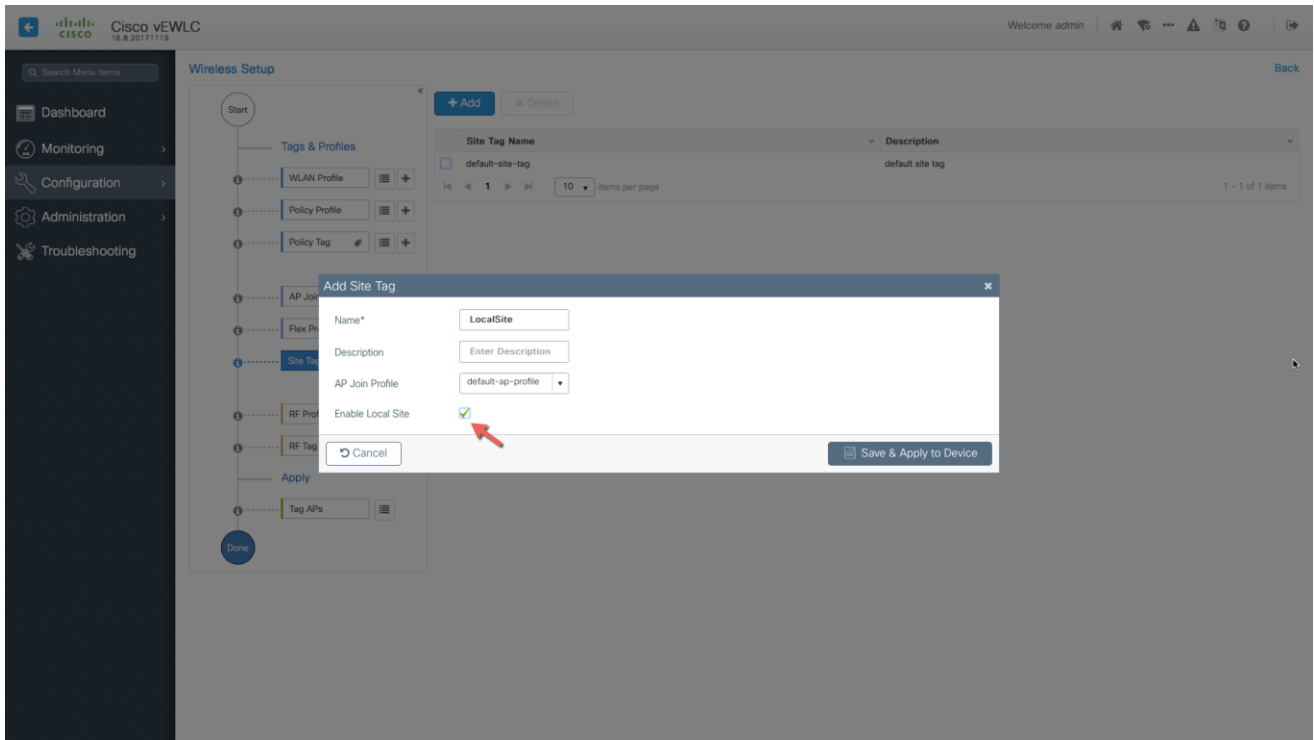
5. APs are tagged with the default policy, site and RF tags automatically so no explicit tagging is needed and the SSIDs will start broadcasting across the campus network

Use Case 2 – Local sites within a Campus

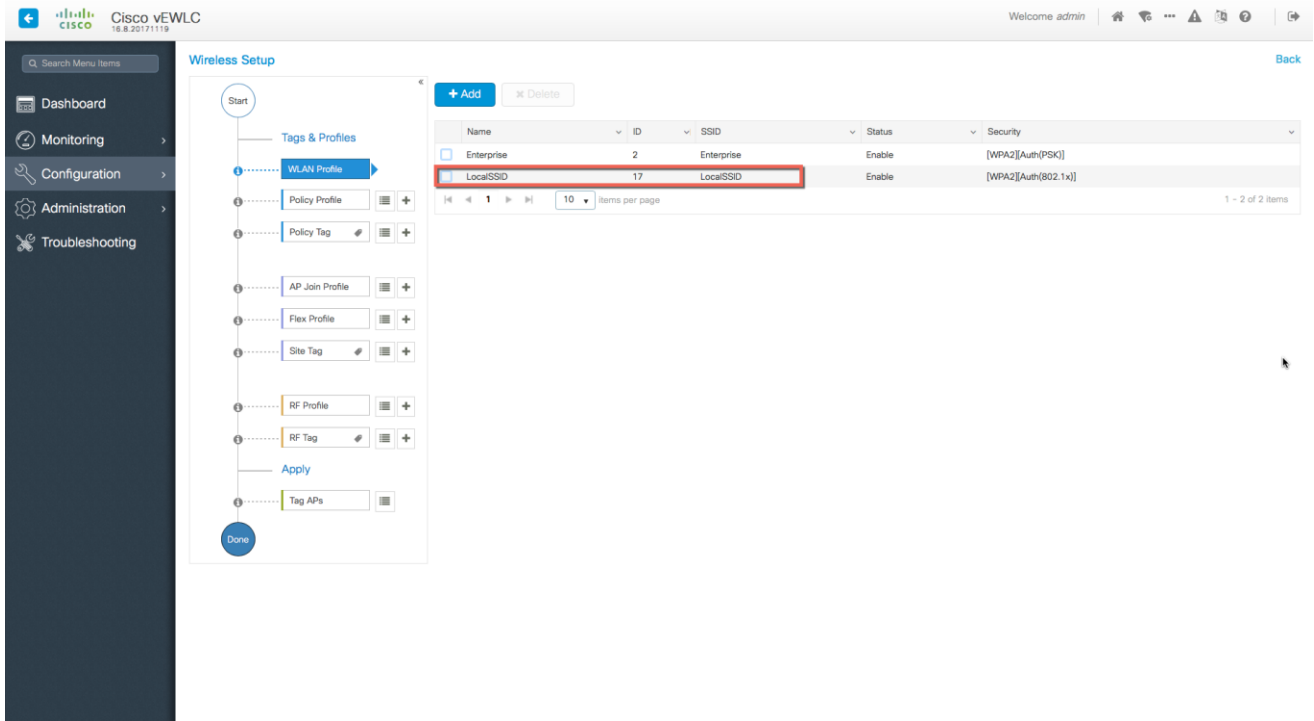
This use-case adds a local site to the campus deployment with custom SSIDs, Policies and RF characteristics. For example, a building in an enterprise campus that has the requirement to broadcast a custom SSID with a custom policy and has RF characteristics that are specific to a given site.

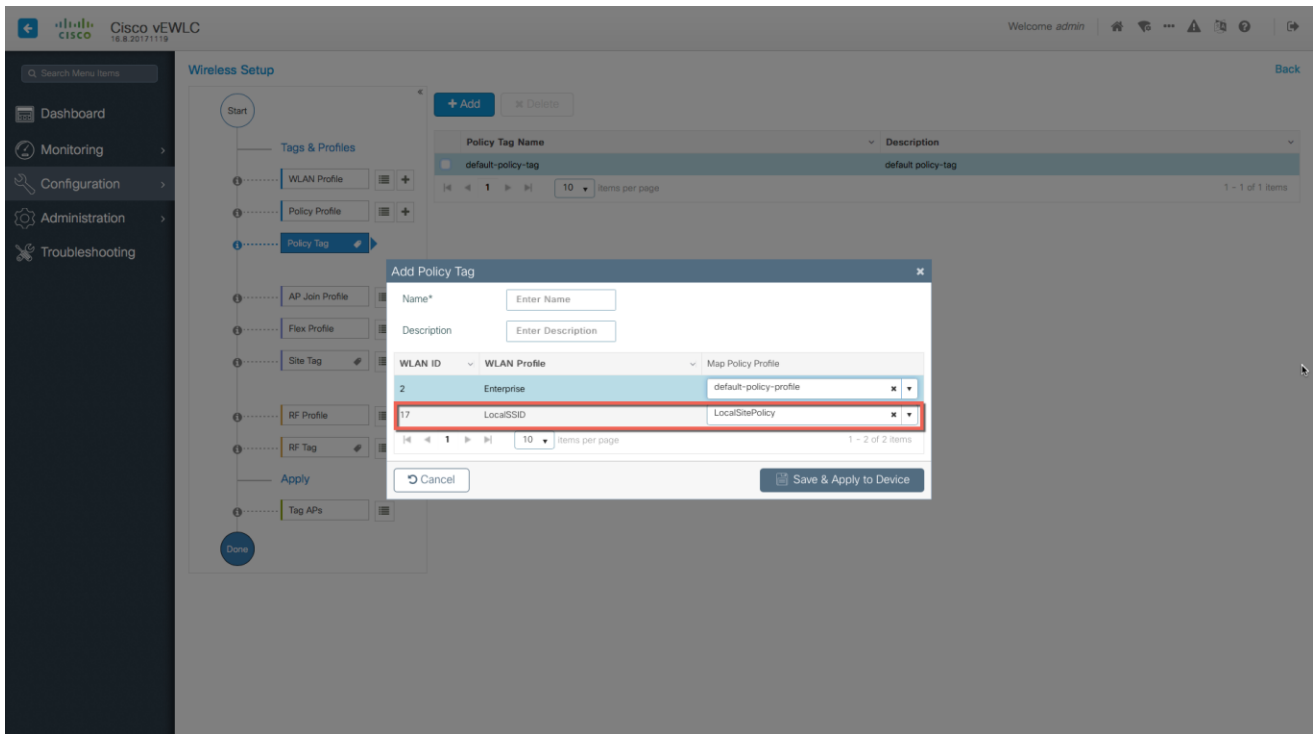
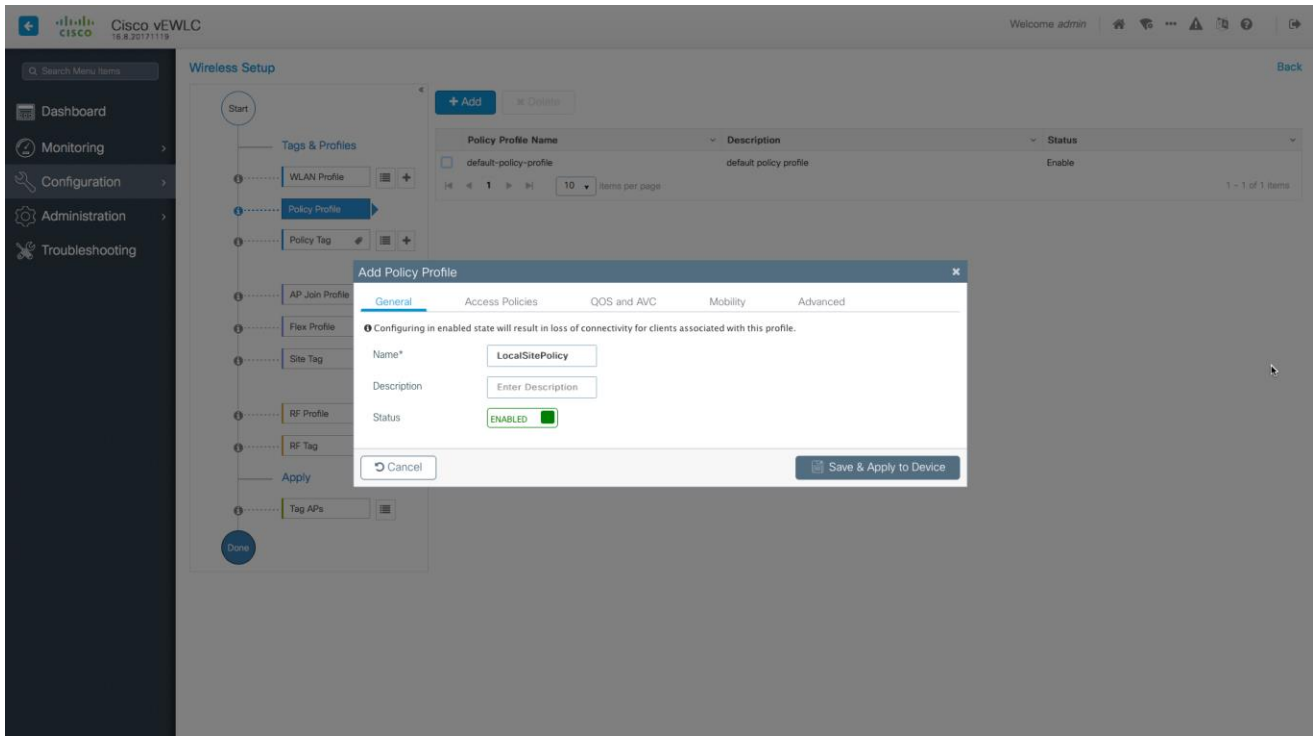


1. Create a custom Site Tag to tags APs belonging to this local site

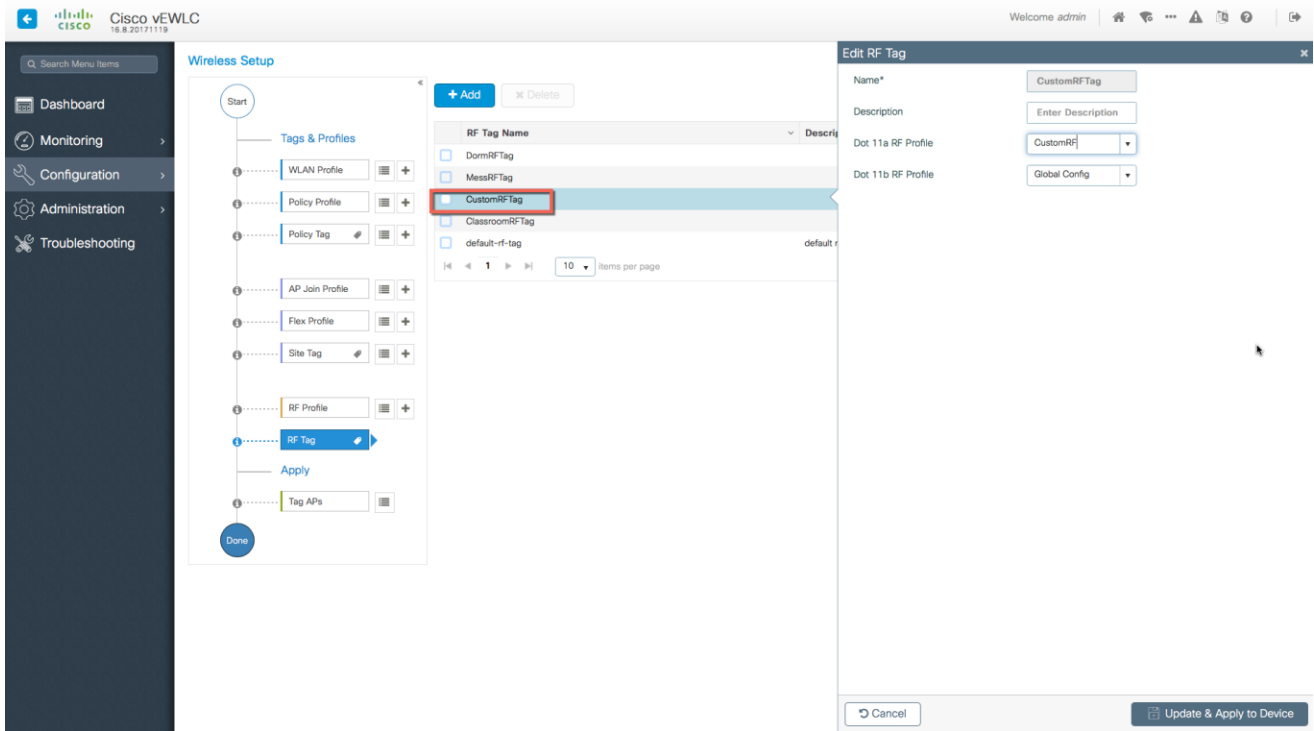
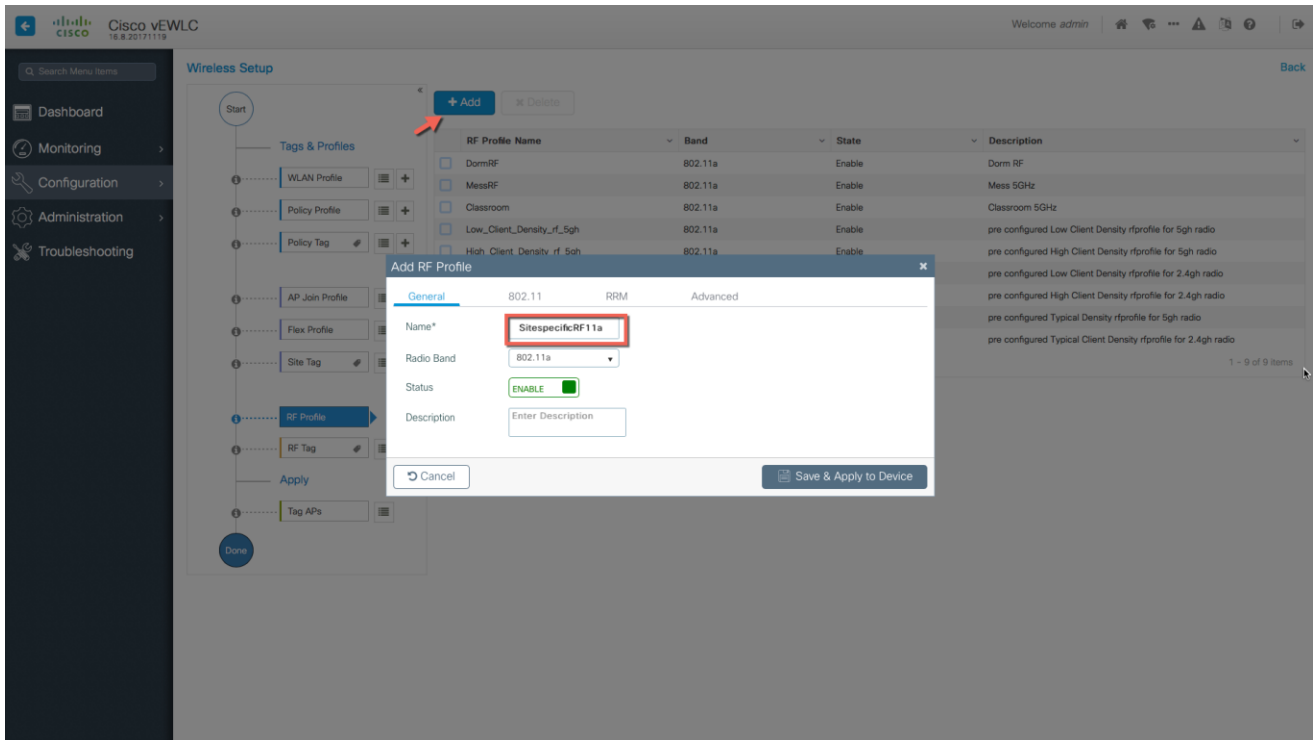


2. Creation of site-specific SSIDs and Policies for the Local site





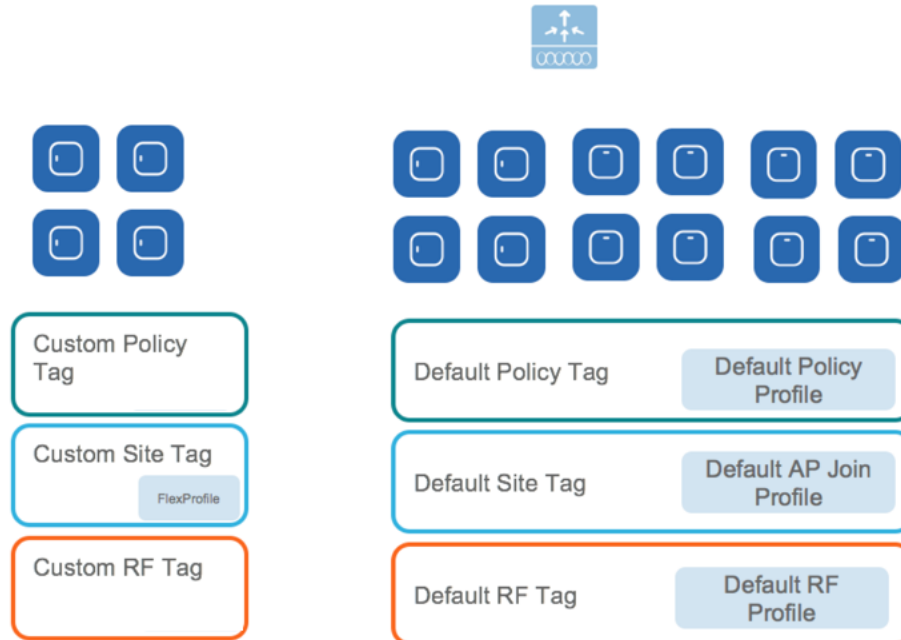
3. Creation of specific RF profile and tag for the local site



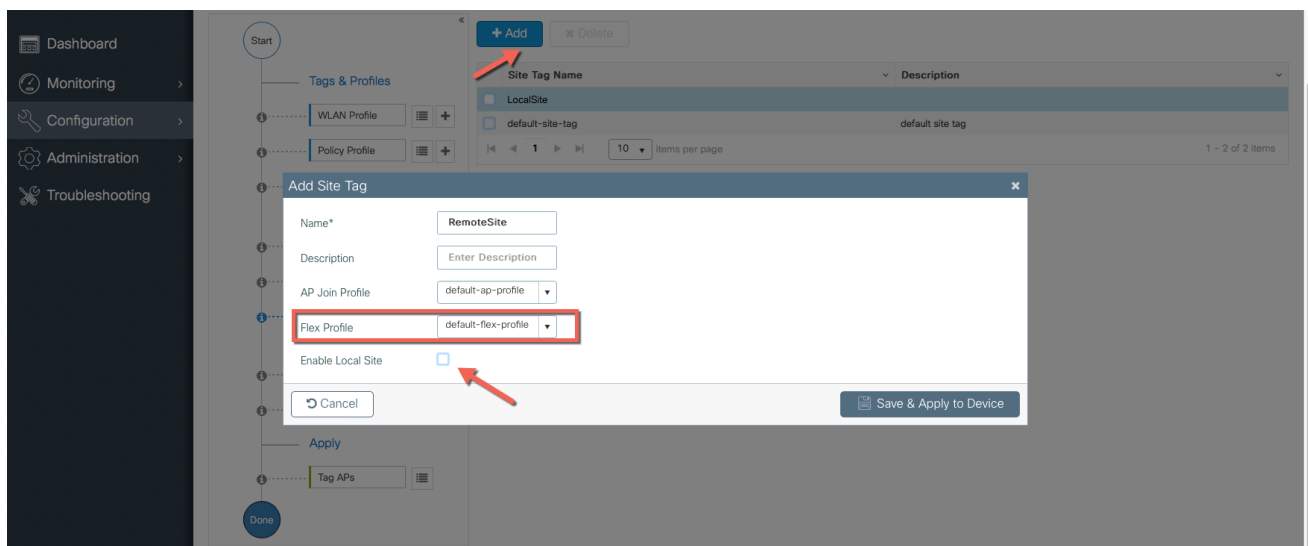


Use Case 3 – Remote sites across the WAN

1. Creation of Remote sites with site-specific SSIDs and RF



Simply creating another site Tag and unchecking the box “Local Site” to add a Flex Profile can add a remote site. An existing site can also be converted to a remote site with this simple action.



2. The APs in the remote site now need to be Tagged with the RemoteSite Tag and with the Policy and RF Tag if non-default configuration is required. Once tagged with the remote site TAG, the AP s will be converted to FlexConnect mode dynamically.

Tagging APs with Tags

By Default, APs are tagged with the default policy tag, default site tag and default RF Tag

The screenshot shows the Cisco vEWC Wireless Setup interface. On the left, a navigation pane includes Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main area is titled 'Wireless Setup' and contains a 'Tags & Profiles' section with options for WLAN Profile, Policy Profile, Policy Tag, AP Join Profile, Flex Profile, Site Tag, RF Profile, and RF Tag. The 'Tag APs' button is highlighted. To the right, a table lists 4 APs with their configurations. The 'Policy Tag', 'Site Tag', and 'RF Tag' columns for all APs are highlighted with a red box, showing default values: 'default-policy-tag', 'default-site-tag', and 'default-rf-tag'.

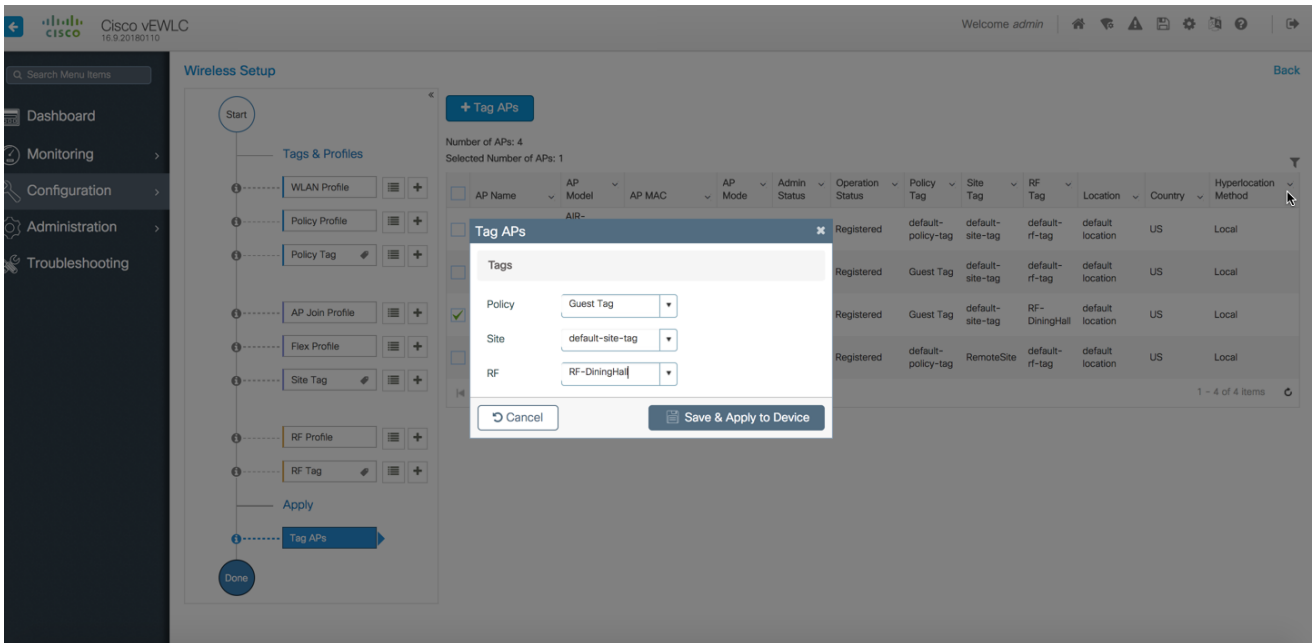
AP Name	AP Model	AP MAC	AP Mode	Admin Status	Operation Status	Policy Tag	Site Tag	RF Tag	Location	Country	Hyperlocation Method
eWLC42-AP1-Classroom	AIR-AP3802I-B-K9		Local	Enabled	Registered	default-policy-tag	default-site-tag	default-rf-tag	default location	US	Local
eWLC42-AP2-Dorm	AIR-AP3802I-B-K9		Local	Enabled	Registered	Guest Tag	default-site-tag	default-rf-tag	default location	US	Local
eWLC42-AP3-DiningHall	AIR-AP3802I-B-K9		Local	Enabled	Registered	Guest Tag	default-site-tag	RF-DiningHall	default location	US	Local
eWLC42-AP3700-RemoteClassroom	AIR-CAP3702E-B-K9		Flex	Enabled	Registered	default-policy-tag	RemoteSite	default-rf-tag	default location	US	Local

Specific/custom Policy, site and RF Tags can be added to APs as shown below

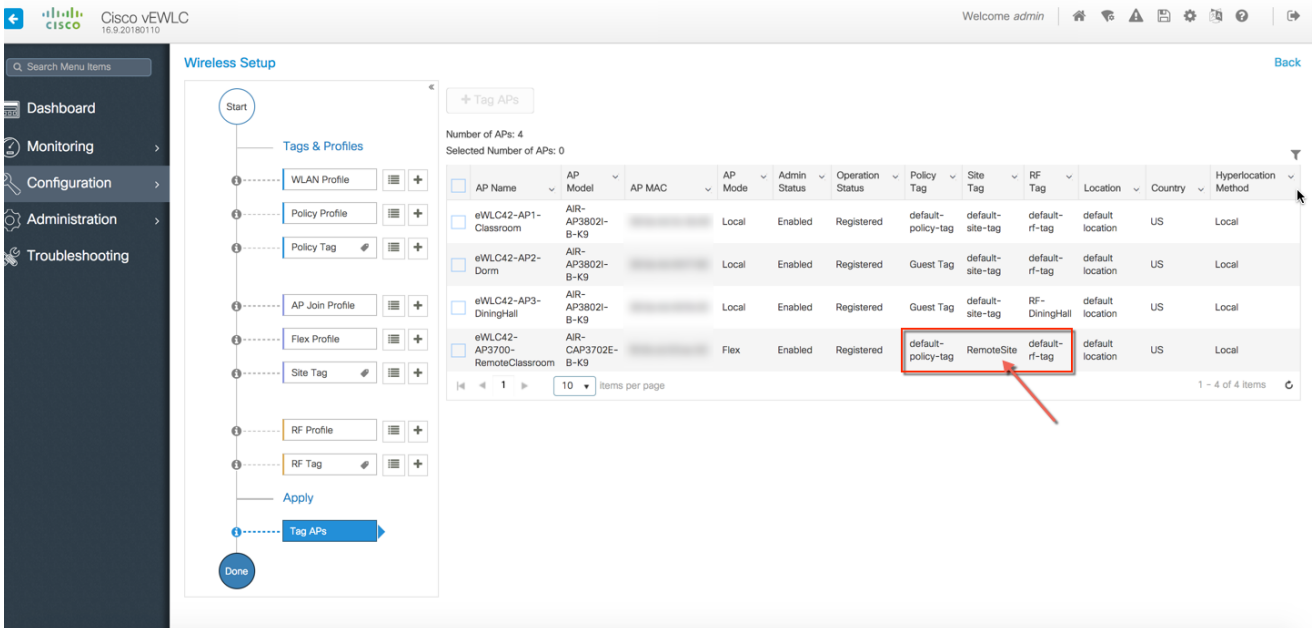
The screenshot shows the Cisco vEWC Wireless Setup interface with custom tagging. The 'Policy Tag', 'Site Tag', and 'RF Tag' columns for the second and third APs are highlighted with a red box, showing custom values: 'Guest Tag', 'default-site-tag', and 'RF-DiningHall'.

AP Name	AP Model	AP MAC	AP Mode	Admin Status	Operation Status	Policy Tag	Site Tag	RF Tag	Location	Country	Hyperlocation Method
eWLC42-AP1-Classroom	AIR-AP3802I-B-K9		Local	Enabled	Registered	default-policy-tag	default-site-tag	default-rf-tag	default location	US	Local
eWLC42-AP2-Dorm	AIR-AP3802I-B-K9		Local	Enabled	Registered	Guest Tag	default-site-tag	default-rf-tag	default location	US	Local
eWLC42-AP3-DiningHall	AIR-AP3802I-B-K9		Local	Enabled	Registered	Guest Tag	default-site-tag	RF-DiningHall	default location	US	Local
eWLC42-AP3700-RemoteClassroom	AIR-CAP3702E-B-K9		Flex	Enabled	Registered	default-policy-tag	RemoteSite	default-rf-tag	default location	US	Local

In the example below a custom Policy tag for Guest SSID and a custom RF Tag is being added to an AP



For remote sites, a site tag with a default/custom flex profile needs to be added



The screenshot shows the Cisco vEWC interface. On the left is a navigation menu with options like Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main area is titled 'Access Points' and shows a table of APs. The 'Edit AP' window is open on the right, showing configuration details for an AP named 'eWLC42-AP3700-Rem'. The 'AP Mode' dropdown menu is set to 'Flex', indicated by a red arrow. Other settings include 'Admin Status' (Enabled), 'Operation Status' (Registered), and 'Fabric Status' (Disabled). The 'Tags' section shows 'Policy' set to 'default-policy-tag', 'Site' set to 'RemoteSite', and 'RF' set to 'default-rf-tag'. The 'Update & Apply to Device' button is visible at the bottom right.

Once tagged with the remote site TAG, the AP s will be converted to FlexConnect mode dynamically.

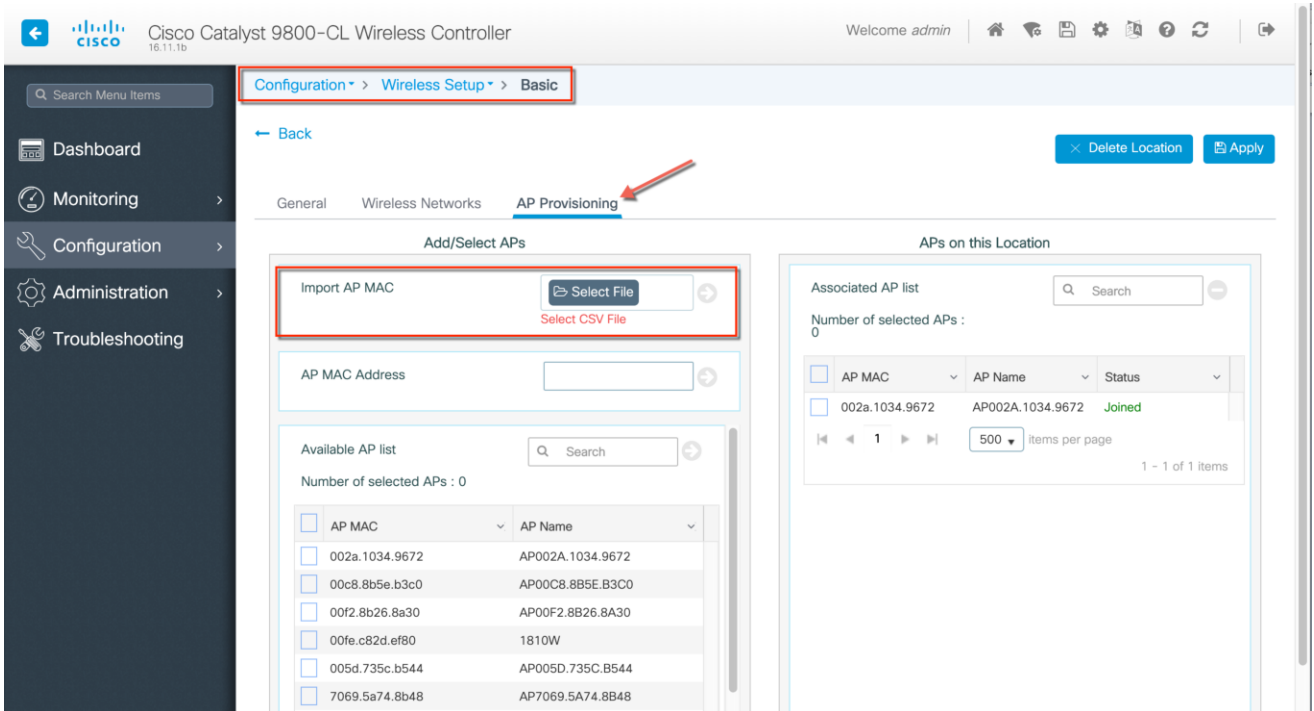
Static Tagging of APs

Optionally, APs can be tagged statically by specifying the MAC Address under **Configuration> Tags & Profiles> Tags**

The screenshot shows the 'Associate Tags to AP' configuration window. It contains four input fields with dropdown menus: 'AP MAC Address*' (with a text input field 'Enter MAC Address'), 'Policy Tag Name' (set to 'default-policy-tag'), 'Site Tag Name' (set to 'default-site-tag'), and 'RF Tag Name' (set to 'default-rf-tag'). At the bottom, there are 'Cancel' and 'Save & Apply to Device' buttons.

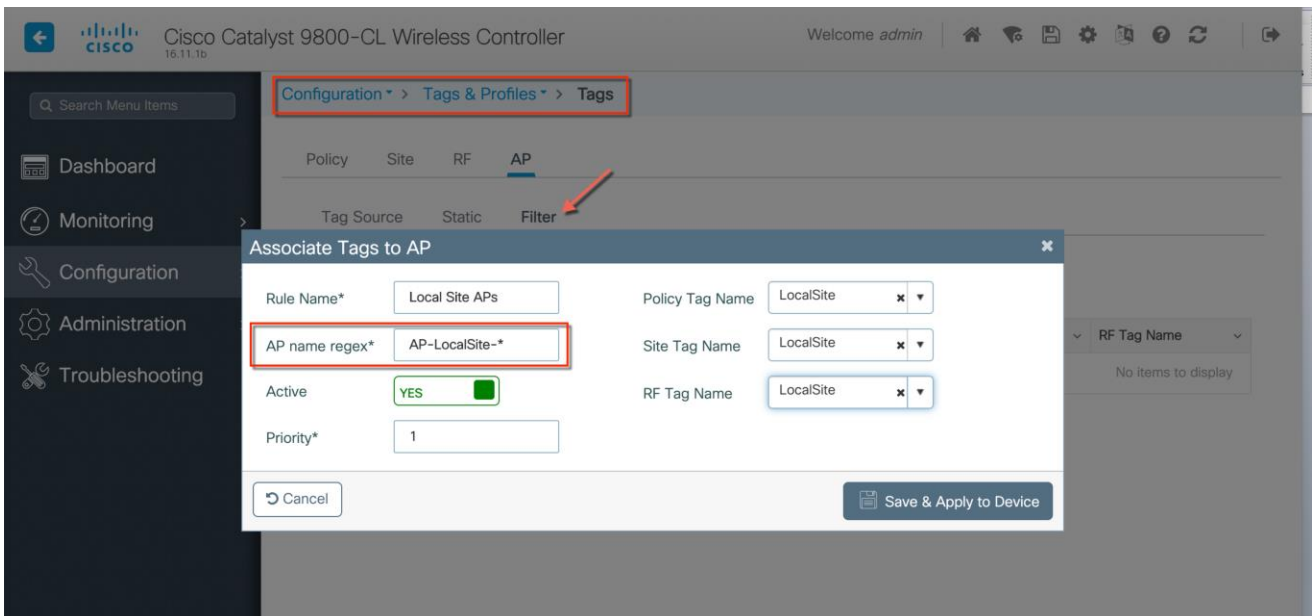
Static Tagging of APs using CSV file import

Static tagging of APs using a CSV file for MAC address import is available on the Wireless Basic > AP Provisioning Page



Regular-expression Based rules for AP Tagging

Regular expression based rules can be configured to match on access point name and associate the appropriate policy, site and RF tags to access points.

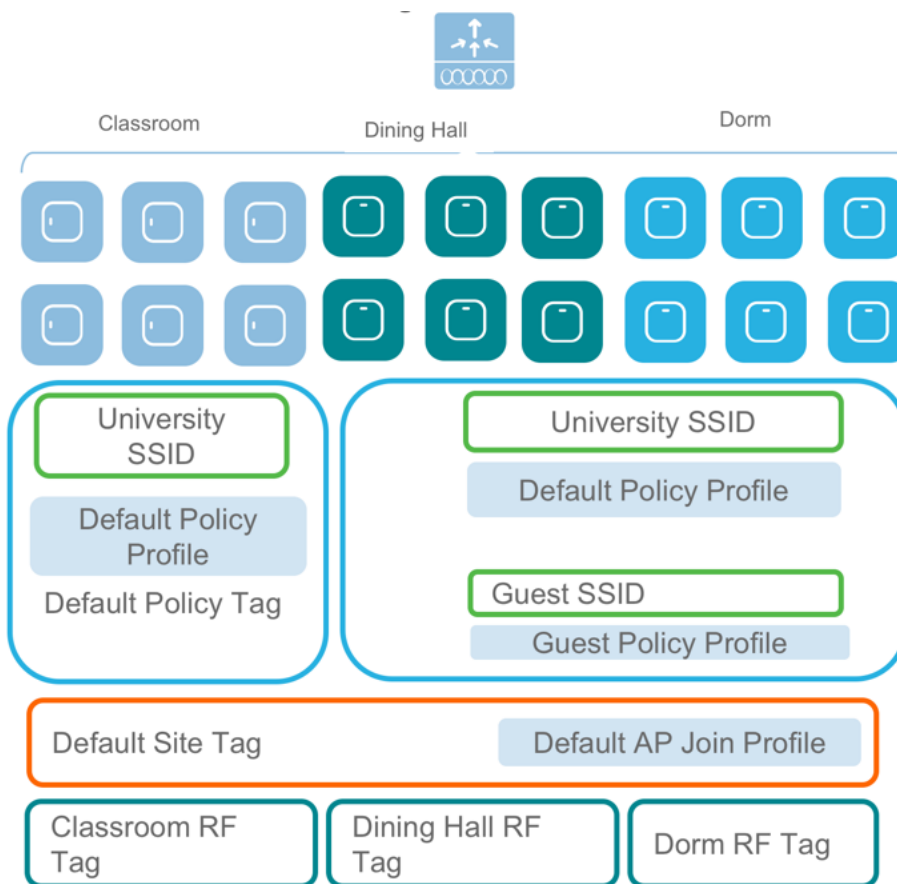


Once the configuration is complete, the SSIDs start broadcasting and clients can now be connected.

Additional Use case Examples

More involved use-cases can also be achieved with the configuration model detail in this document.

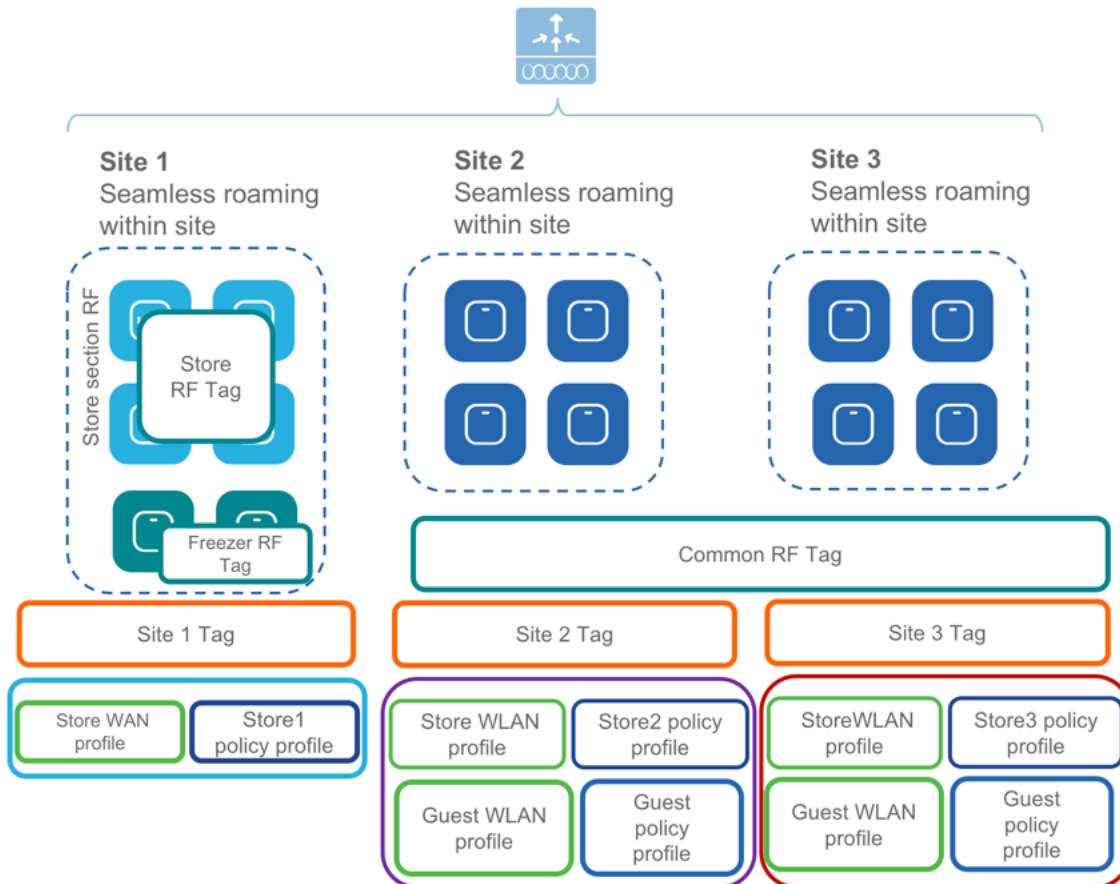
1. For example, a University Deployment with the following requirements can be deployed with profiles and tags as shown in the figure below:
2. Campus-wide University SSID for students and teachers
3. Dorms and Dining Halls to broadcast Guest SSID
4. Custom Guest policies for VLAN segregation
5. Custom RF characteristic of Dining Hall, classrooms and dorms



A multi-site retail deployment with the following requirements can be deployed with profiles and tags as shown in the figure below:

1. All sites should broadcast the same common SSID 'Store'
2. All the sites should have same policies per SSID

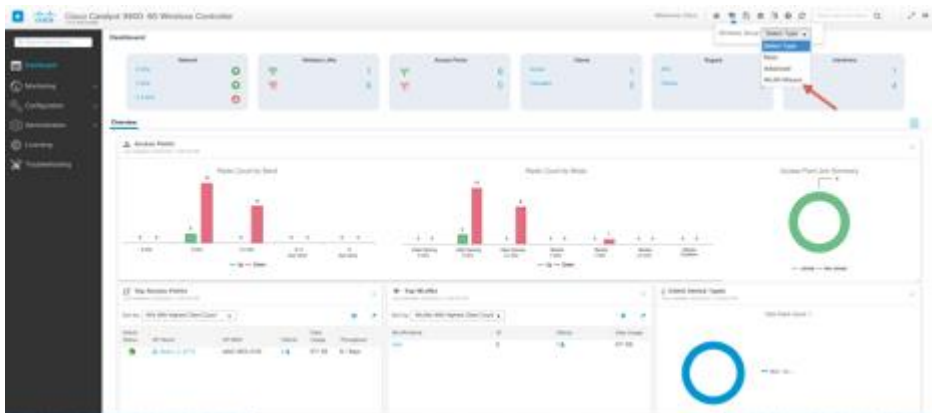
3. Roaming is expected per store/flex-grp
4. All sites should have the same Site parameters
5. APs near freezer needs to have a different RF policy
6. Site 2 and 3 have additionally 'Guest' SSIDs
7. Independent Per site parameters
8. The Common SSID need to have store-specific policies



Note: It is not recommended to mix and match basic with advanced workflow. When using the basic setup workflow for creating local and remote sites, corresponding policies and tags are created in the backend in accordance with the new configuration model. The tags and policies, thus, created shouldn't be modified using the advanced workflow.

WLAN Wizard Overview

With Cisco IOS XE 17.6 Release, a WLAN Wizard is available under the Wireless Setup icon. This wizard eases the process of creating WLANs for Local Mode, FlexConnect Mode and guest access by guiding the user in a step-by-step workflow.



The following WLAN types are supported through this wizard.

Local Mode

- PSK
- Dot1x
- Local Webauth
- External Webauth
- Central Web Auth

FlexConnect Mode

- Local Webauth
- External Webauth
- Central Web Auth

Guest CWA

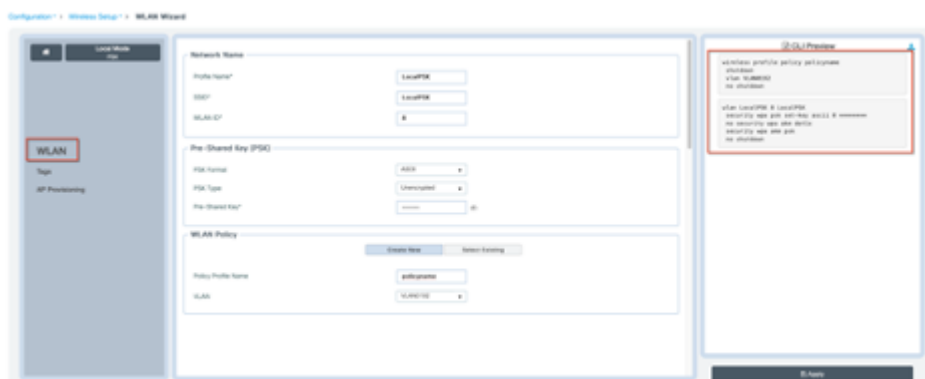
- Foreign
- Anchor



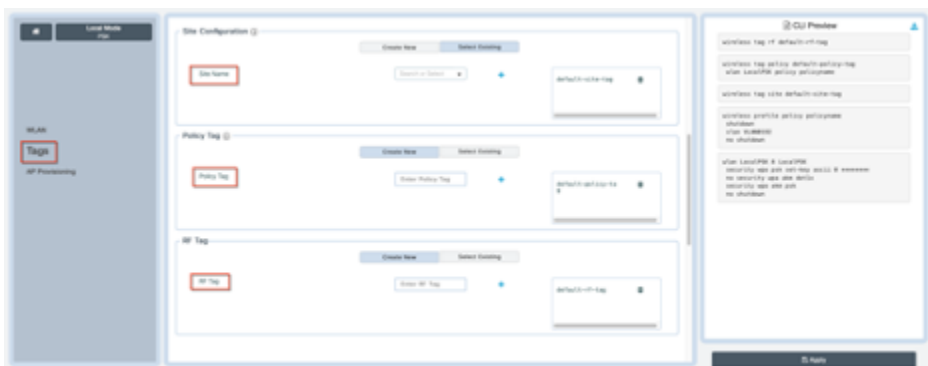
Creating a PSK SSID

The following section demonstrates the process of creating a PSK SSID in Local Mode using this wizard.

Step 1: Create the WLAN by specifying the Profile Name, SSID and PSK Pre-Shared key. Specify the WLAN Policy either by creating a new policy or selecting an existing policy. As you can see on the right hand side, the CLI preview of the entered configuration is generated in real-time for reference.



Step 2: Click on Tags and specify the Site Tag, Policy Tag and RF Tag either by creating new tags or selecting existing tags. Click on the blue '+' sign to enter the selection. Again, note the corresponding CLI commands that are auto-generated.

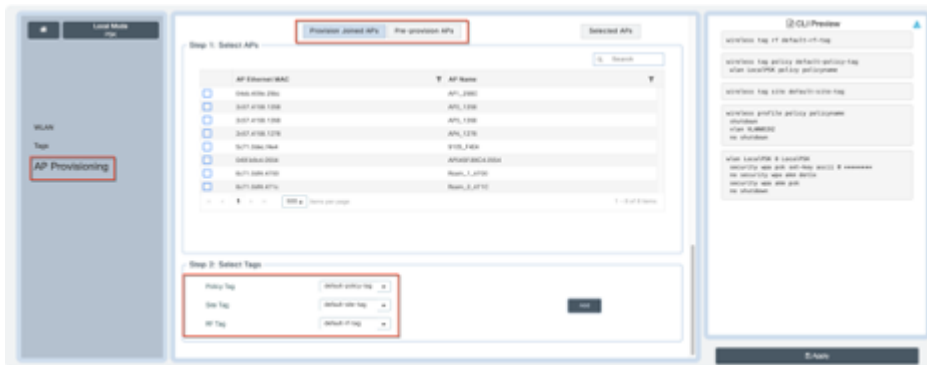


Step 3: Click on AP Provisioning to associate tags with APs. This can be done in two ways:

- Provision joined APs by selecting them from a list and associating the site, policy and RF tags.
- Pre-provision APs using MAC address or a CSV file before the APs join the controller.

Once done, Click Apply. And optionally, you can also download the CLI Preview file by clicking on the

download icon on the CLI Preview box.

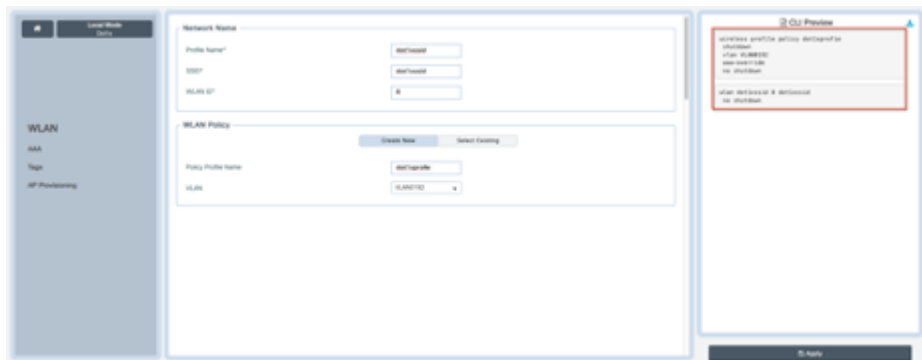


Creating a DOT1X SSID

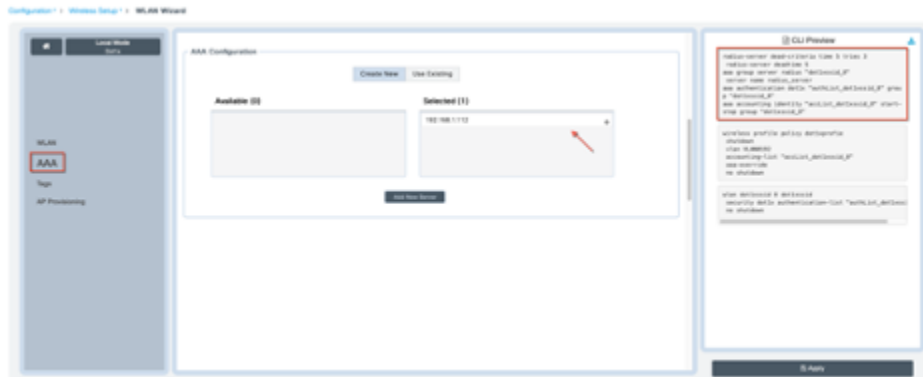
The following section demonstrates the process of creating a Dot1x SSID in Local Mode using this wizard.

Step 1: Create the WLAN by specifying the Profile Name and SSID. Specify the WLAN Policy either by creating a new policy or selecting an existing policy.

As you can see on the right hand side, the CLI preview of the entered configuration is generated in real-time for reference.



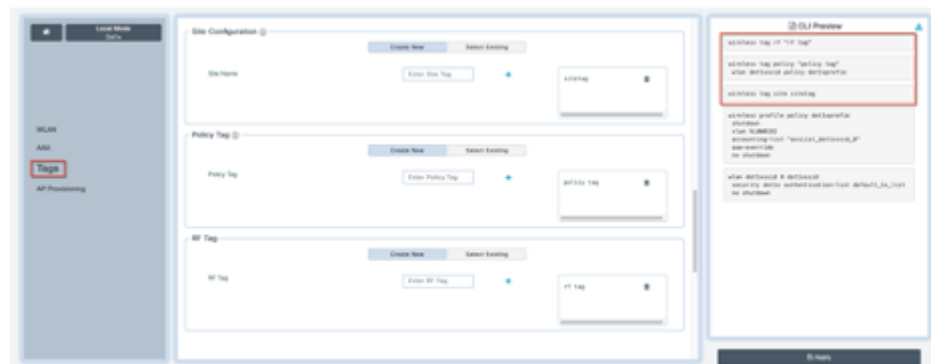
Step 2: Click on AAA and either create a new AAA server or use existing.



If choosing an existing AAA server, select the server from the list as shown below.



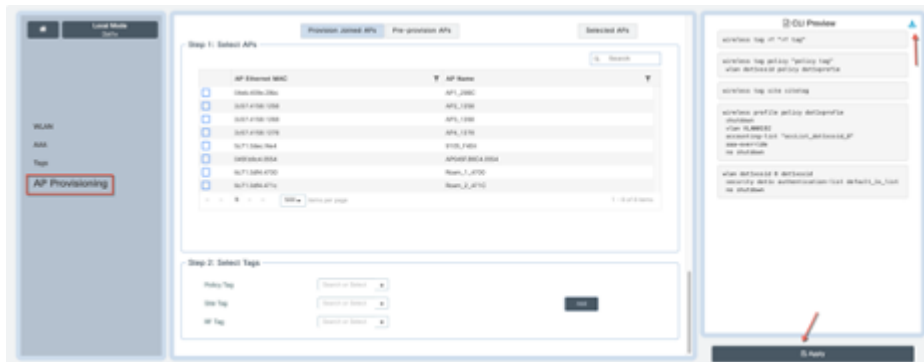
Step3: Click on Tags and specify the Site Tag, Policy Tag and RF Tag either by creating new tags or selecting existing tags. Click on the blue '+' sign to enter the selection. Again, note the corresponding CLI commands that are auto-generated.



Step 4: Click on AP Provisioning to associate tags with APs. This can be done in two ways:

- Provision joined APs by selecting them from a list and associating the site, policy and RF tags.
- Pre-provision APs using MAC address or a CSV file before the APs join the controller.

Once done, Click Apply. And optionally, you can also download the CLI Preview file by clicking on the download icon on the CLI Preview box.

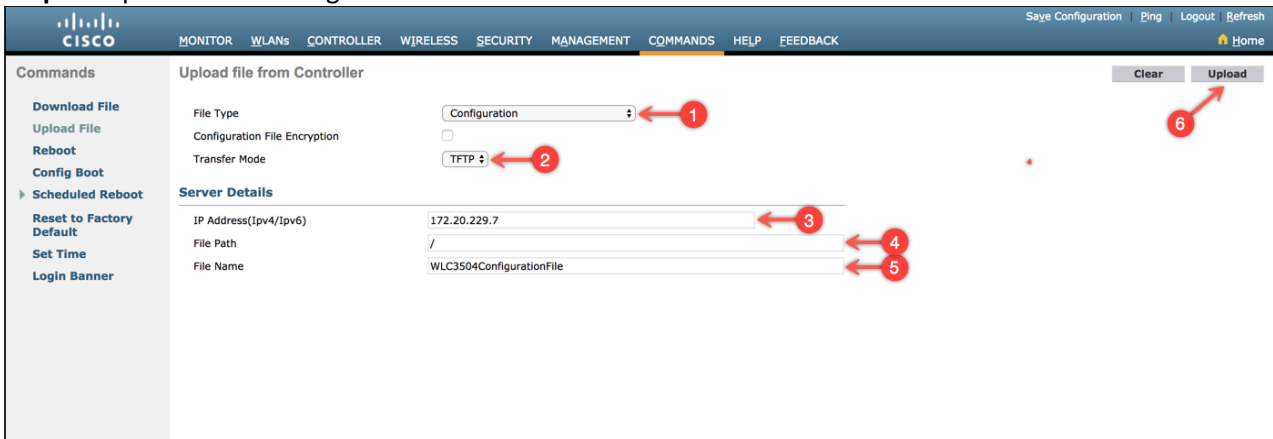


AireOS to Catalyst 9800 Wireless Controller Migration

Migration Web Tool

The migration tool provides configuration transition and is designed to translate AireOS configuration to the new configuration model for the Catalyst 9800 Wireless Controller. The migration tool is available as an offline tool or as an embedded tool in the C9800 Web UI. It uses as input the AireOS configuration commands (exported as a file to TFTP server) and AP Group information (through the “show run-config” command).

Step 1: Export AireOS configuration to a TFTP server

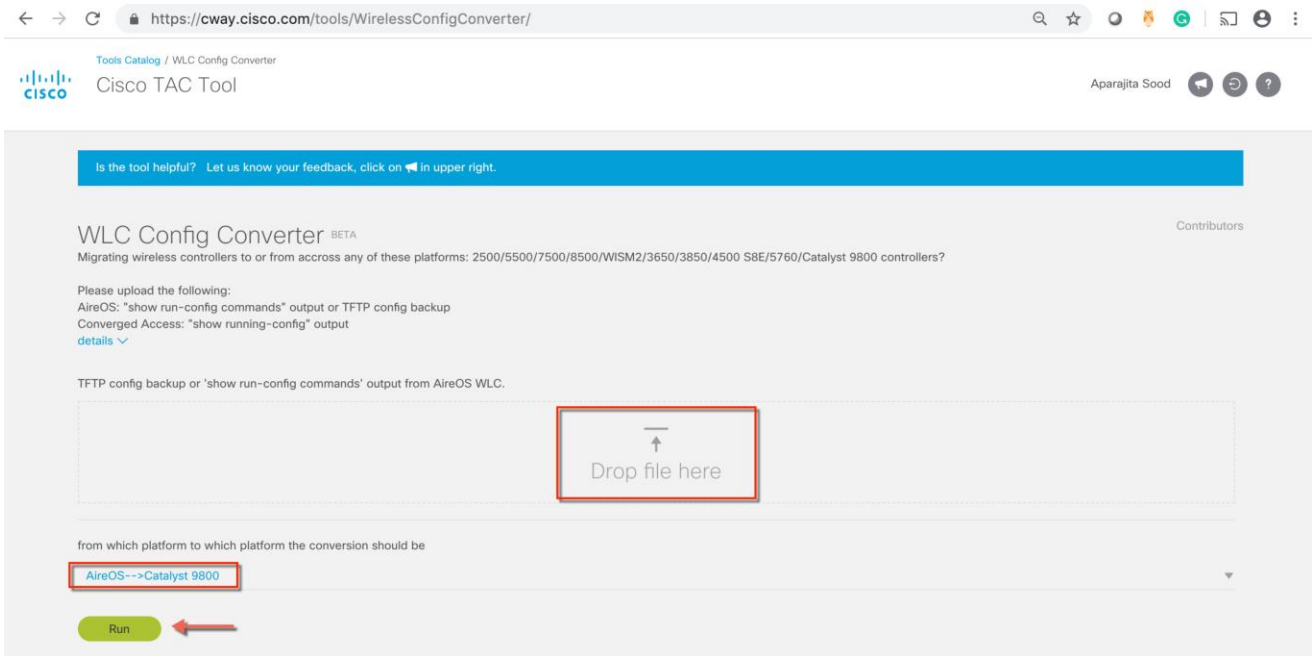


The screenshot shows the Cisco Catalyst 9800 Web UI Migration Web Tool interface. The interface is divided into a left sidebar with navigation options and a main content area. The main content area is titled "Upload file from Controller" and contains a form with the following fields:

- File Type: Configuration (indicated by red arrow 1)
- Configuration File Encryption:
- Transfer Mode: TFTP (indicated by red arrow 2)
- Server Details:
 - IP Address(Ipv4/Ipv6): 172.20.229.7 (indicated by red arrow 3)
 - File Path: / (indicated by red arrow 4)
 - File Name: WLC3504ConfigurationFile (indicated by red arrow 5)

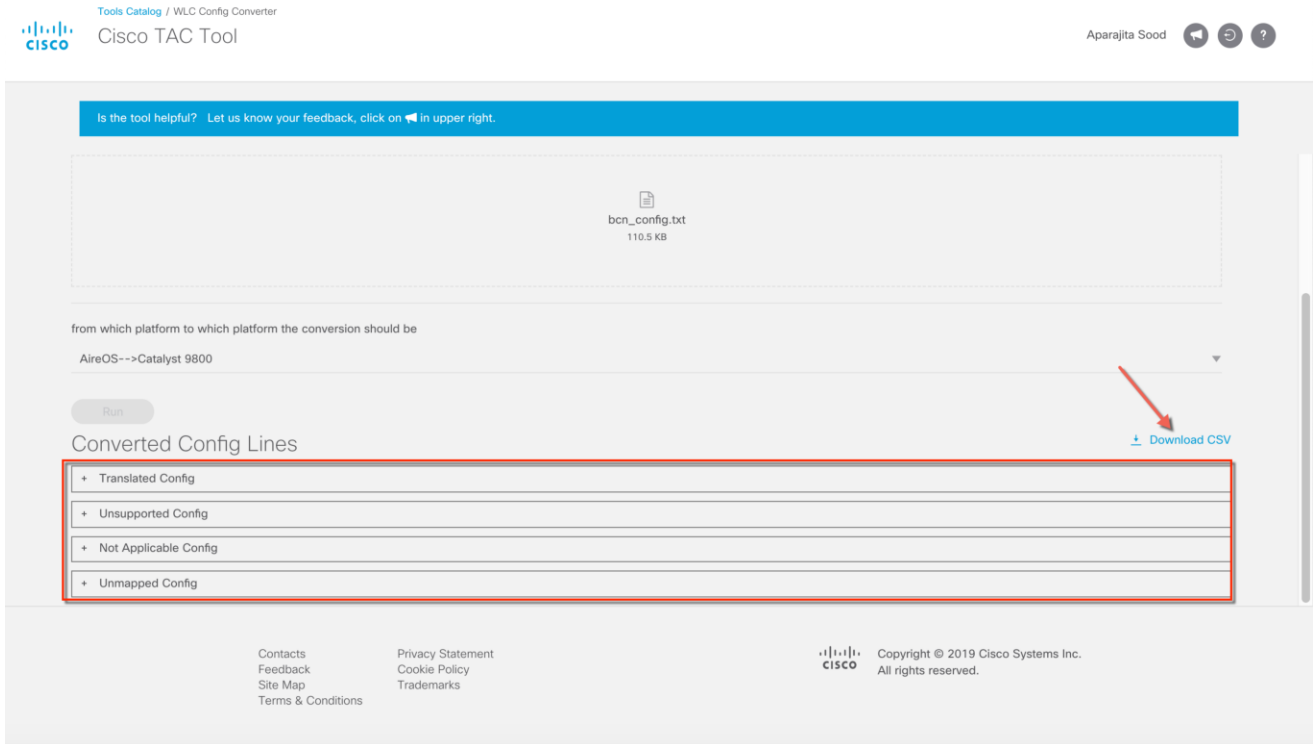
At the top right of the form, there are "Clear" and "Upload" buttons. A red arrow (indicated by red arrow 6) points to the "Upload" button.

Step 2: Import the configuration into the tool as shown below, Select AireOS->9800 and click on Run



Step 3: The resultant output displays metrics on the configuration that is

- a. Supported and successfully translated
- b. Unsupported in the current release
- c. Configuration that is either deprecated, obsolete or irrelevant in the current context of the Cisco Catalyst Wireless Controller.

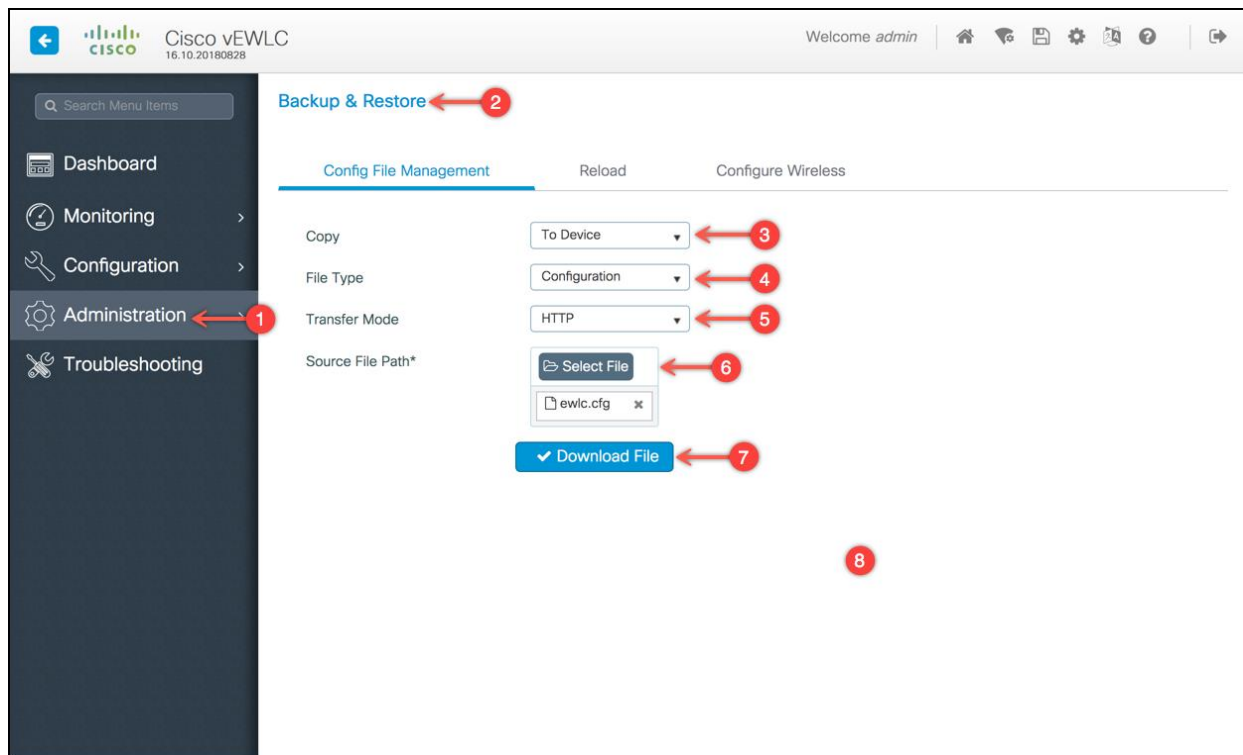


This configuration can also be exported for further analysis by clicking on 'Download CSV'. A detailed list of CLIs can be obtained by expanding the sections.

Step 4: The tool displays the translated configuration in the form of a CLI output with the translated configuration and the corresponding AireOS configuration (preceded by a '!' sign). Download the translated configuration, update shared secrets, passwords, IP and port information and prepare the file to be uploaded on the target C9800 controller

```
- Translated Config
=====
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! Interface Configuration
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! config interface vlan management 30
! config interface address management 10.75.192.30 255.255.255.0 10.75.192.1
! config interface dhcp management primary 199.231.22.90
vlan 30
name "management"
no shutdown
interface vlan 30
description "management"
ip address 10.75.192.30 255.255.255.0
ip helper-address 199.231.22.90
no shutdown
```

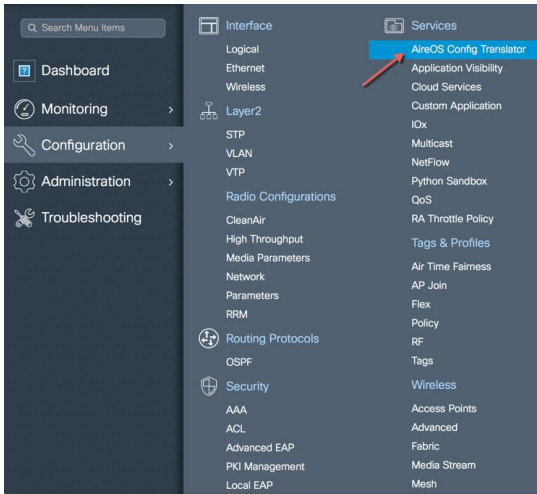
Step 5: Import Downloaded file to the C9800 controller to complete configuration migration





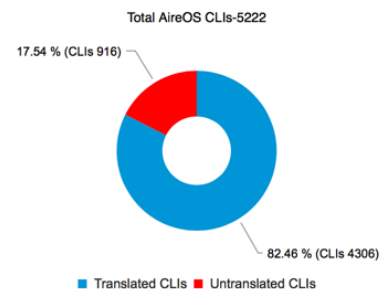
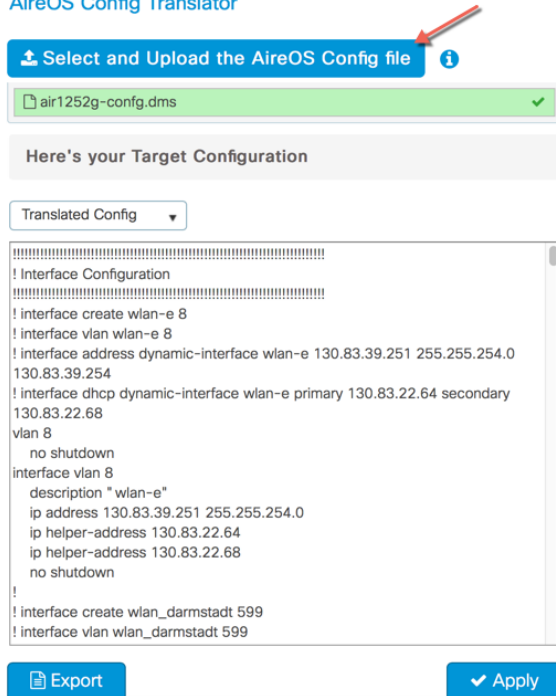
AireOS Config Translator

The AireOS config translator tool is natively built into the controller software and allows an AireOS configuration to be migrated to the Cisco Catalyst Wireless Controller configuration. To access the tool, go under Configuration > Services > AireOS Config Translator



From an AireOS controller, export the configuration to a TFTP server and upload the file on the tool as shown below. The tool displays the translated configuration in the form of a CLI output with the translated configuration and the corresponding AireOS configuration (preceded by a '! sign)

AireOS Config Translator



The configuration can then be exported as a file to make modifications such as re-entering passwords, IP addresses if changed and port details or, applied directly to the running configuration of the device. The pie chart on the right shows the breakdown of translated vs. untranslated configs

Unsupported configuration is configuration that is currently unsupported on the controller and will be addressed in the upcoming releases

AireOS Config Translator

Select and Upload the AireOS Config file ⓘ

air1252g-config.dms ✓

Here's your Target Configuration

Unsupported ▾

```
802.11a cac video cac-method static
802.11a cleanair alarm unclassified threshold 1
802.11b cac video cac-method static
802.11b cleanair alarm unclassified threshold 1
advanced 802.11a packet bronze max-client-count 0
advanced 802.11a packet bronze max-packet-count 0
advanced 802.11a packet bronze max-retry 0
advanced 802.11a packet bronze timeout 0
advanced 802.11a packet gold max-client-count 0
advanced 802.11a packet gold max-packet-count 0
advanced 802.11a packet gold max-retry 0
advanced 802.11a packet gold timeout 0
advanced 802.11a packet platinum max-client-count 0
advanced 802.11a packet platinum max-packet-count 0
advanced 802.11a packet platinum max-retry 0
advanced 802.11a packet platinum timeout 0
advanced 802.11a packet silver max-client-count 0
advanced 802.11a packet silver max-packet-count 0
advanced 802.11a packet silver max-retry 0
advanced 802.11a packet silver timeout 0
```

Export

Total AireOS CLIs-5222

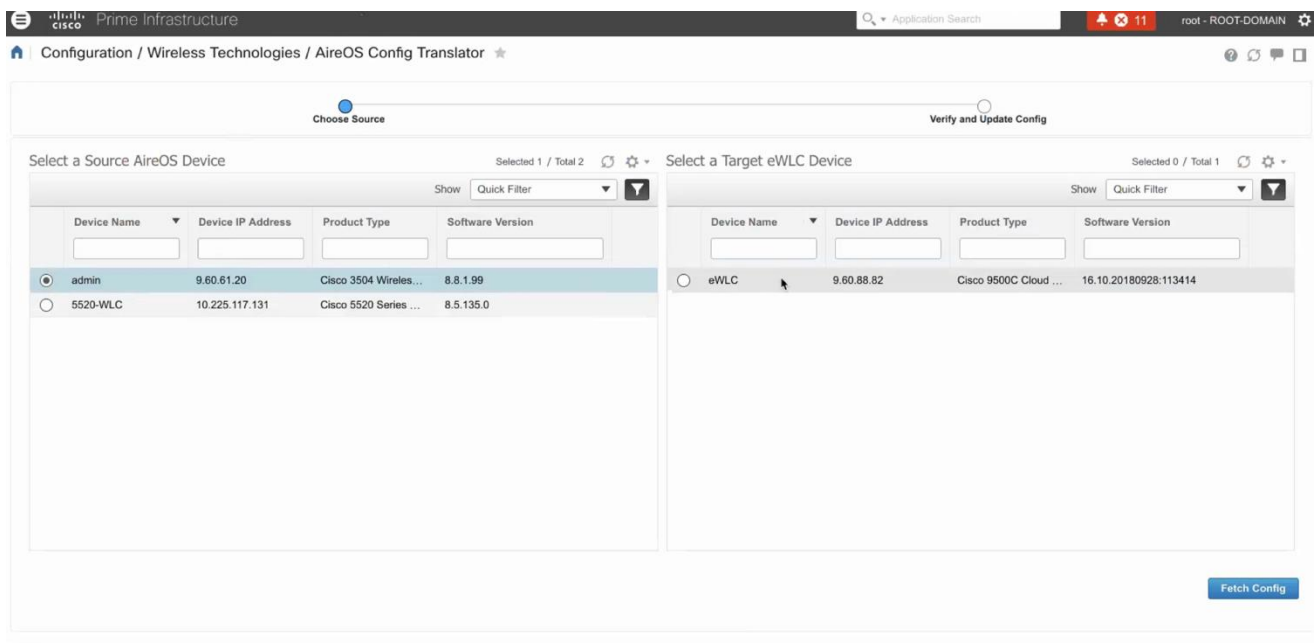
Category	Percentage	Count
Translated CLIs	82.46%	4306
Untranslated CLIs	17.54%	916

Migration using Prime Infrastructure 3.5

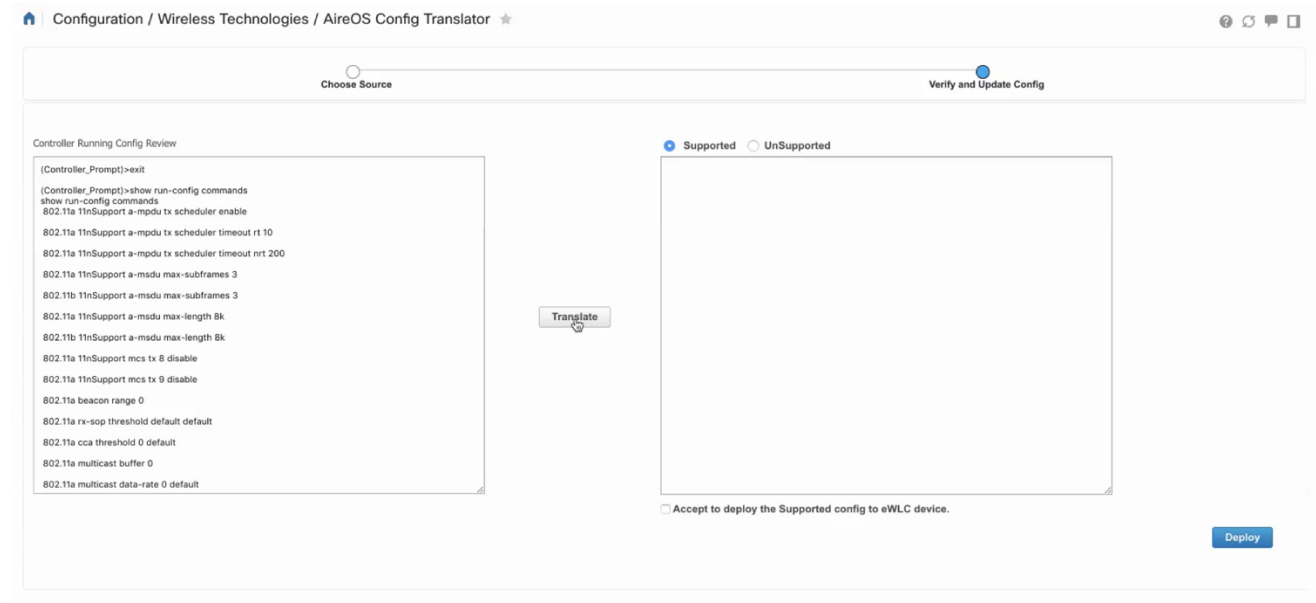
Prime Infrastructure 3.5 can be used to migrate existing AireOS controllers to the new Cisco Catalyst 9800 wireless controllers. Once these devices, both AireOS and Catalyst Wireless Controllers, have been discovered and added into the network devices database of Prime, specific source AireOS controllers can be selected and their configuration migrated to the target controllers in a simple process as detailed below.

SELECT SOURCE AND TARGET WIRELESS CONTROLLERS

From the left hand menu, select the Source AireOS Wireless LAN Controller that needs to be migrated. On the right hand menu, choose the Wireless Controller that the translated configuration will be applied to. Click on Fetch Config to pull in the latest running configuration from the AireOS controller.

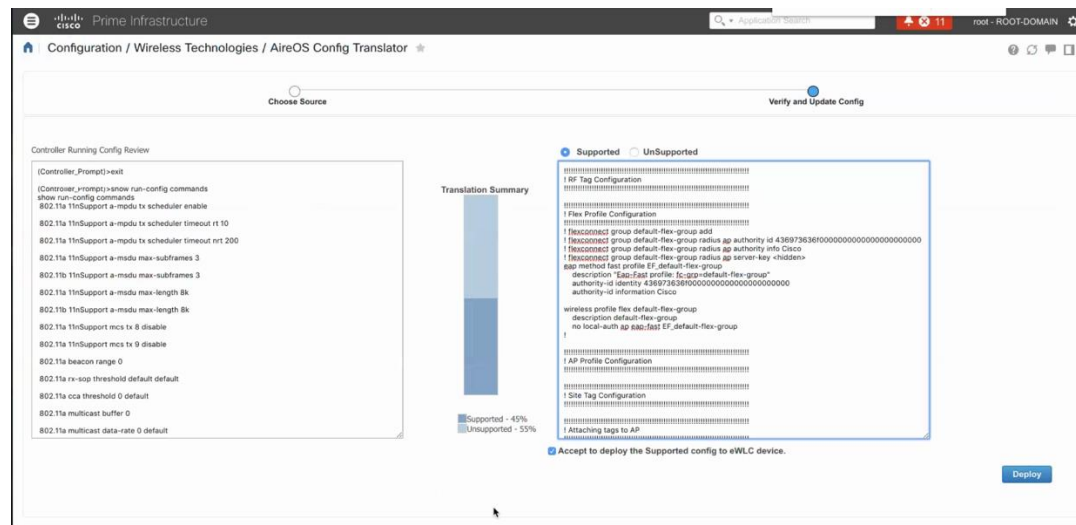


Once the configuration has been fetched, click on the translate button to start the translation of AireOS to Catalyst 9800 configuration.



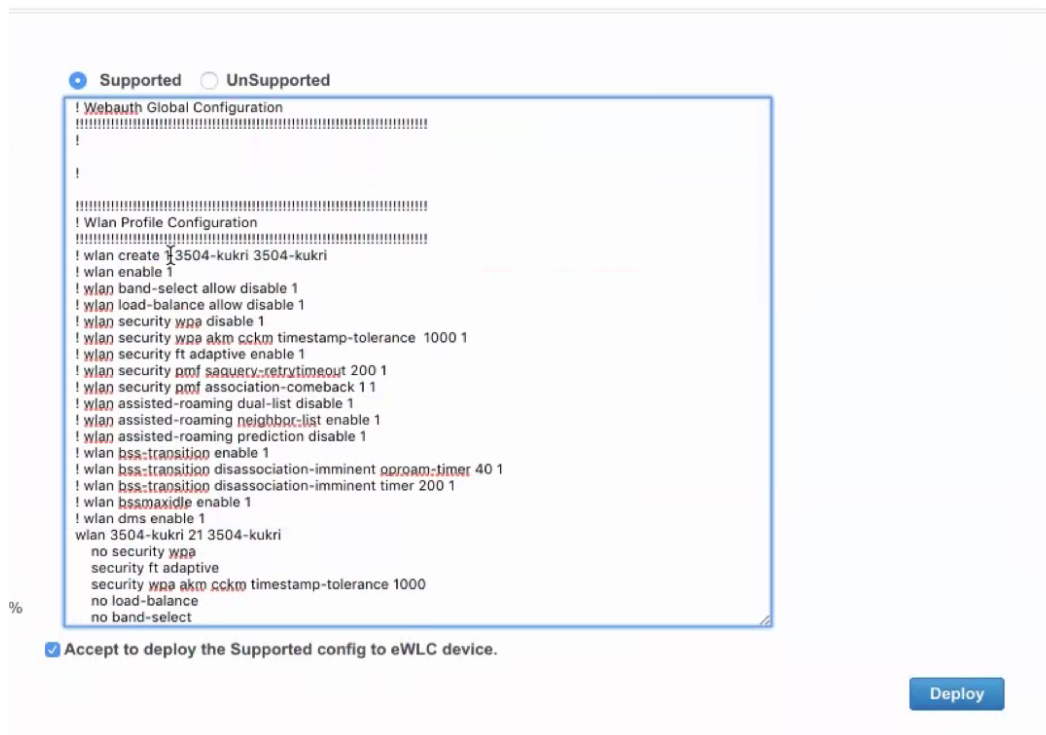
TRANSLATE AND VERIFY/UPDATE PASSWORDS, SHARED SECRETS, IP AND PORTS

The translation summary represents the percentage of supported/ translated vs. unsupported configuration. The translated configuration is displayed in the text box on the right hand side.



DEPLOY TRANSLATED AND UPDATED CONFIGURATION

The tool does not translate shared secret and passwords, as these are stored encrypted and have to be re-entered by the user. For easy identification of such configurations, they are highlighted and required to be edited manually by the user. Once the necessary edits have been made, click on the 'Accept to deploy' checkbox and click Deploy.



Supported UnSupported

```
! Webauth Global Configuration
!
!
!
!
!
! Wlan Profile Configuration
! wlan create 3504-kukri 3504-kukri
! wlan enable 1
! wlan band-select allow disable 1
! wlan load-balance allow disable 1
! wlan security wpa disable 1
! wlan security wpa akm cckm timestamp-tolerance 1000 1
! wlan security ft adaptive enable 1
! wlan security pmf saquery-retrytimeout 200 1
! wlan security pmf association-comeback 1 1
! wlan assisted-roaming dual-list disable 1
! wlan assisted-roaming neighbor-list enable 1
! wlan assisted-roaming prediction disable 1
! wlan bss-transition enable 1
! wlan bss-transition disassociation-imminent oproom-timer 40 1
! wlan bss-transition disassociation-imminent timer 200 1
! wlan bssmaxidle enable 1
! wlan dms enable 1
wlan 3504-kukri 21 3504-kukri
  no security wpa
  security ft adaptive
  security wpa akm cckm timestamp-tolerance 1000
  no load-balance
  no band-select
```

Accept to deploy the Supported config to eWLC device.

Deploy

Once deployed, the configuration is pushed to the target wireless controller.

```
Trying 9.60.88.82...
Connected to 9.60.88.82.
Escape character is '^]'.

User Access Verification
Username: cisco
Password:
admin>show wlan summary

Number of WLANs: 11
WLAN Profile Name          SSID          Status
-----
1 123213                     1234567       UP
3 Dot1x_LWA                 Dot1x_LWA     DOWN
4 test_none_16_10         test_none_16_10 DOWN
5 wep_new                   wep_new       DOWN
6 new_dot1x_test           new_dot1x_test DOWN
7 test_wlanprof            aa            DOWN
10 check                    check         DOWN
14 0021x_16_10              0021x_16_10 DOWN
21 3504-kukri                3504-kukri   UP

Number of WLANs: 11
WLAN Profile Name          SSID          Status
-----
55 ttt                      ttt          DOWN
```

DISCOVER TEMPLATES FROM MIGRATED WIRELESS CONTROLLER

Optionally, templates can be discovered from the Cisco 9800 Catalyst Wireless Controller and re-used to apply configuration to other Wireless Controllers.

