



The bridge to possible

# Successfully Configuring Catalyst 9800 Wireless on Your First Shot

Jesus Herrera, Software Engineer

BRKEWN-2094

CISCO *Live!*

#CiscoLive

# Cisco Webex App

## Questions?

Use Cisco Webex App to chat with the speaker after the session

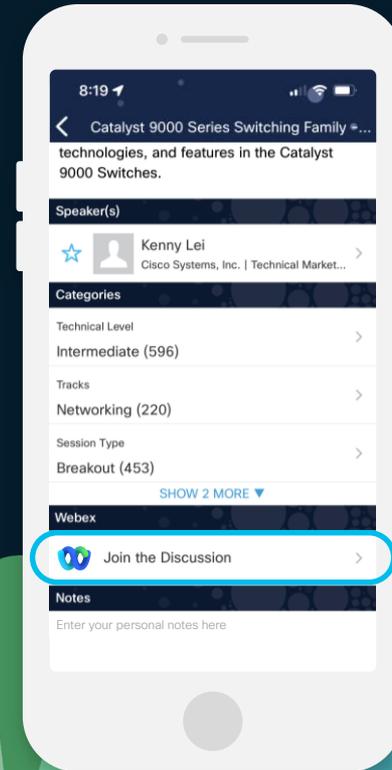
## How

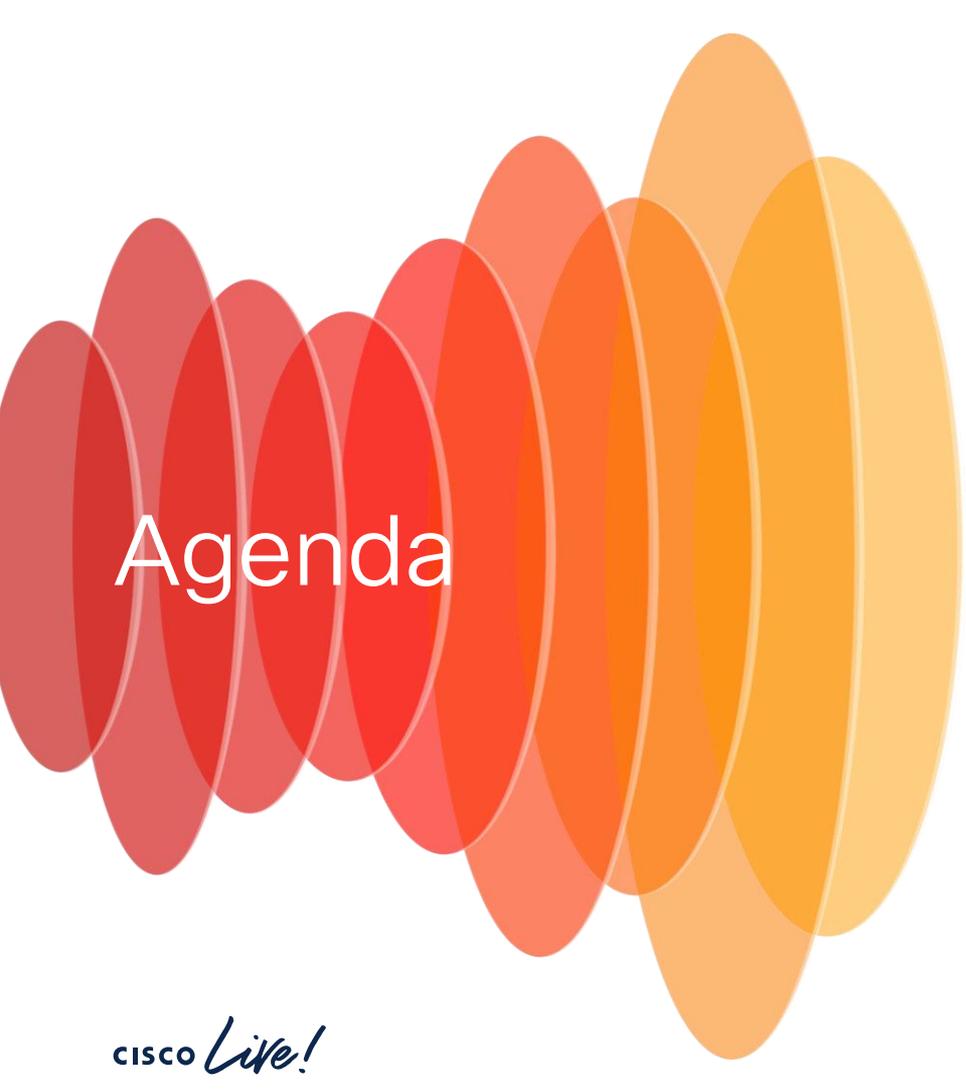
- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 7, 2024.

**CISCO** *Live!*

<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKEWN-2094>





# Agenda

1. Introduction
2. Basic network connectivity
3. Objects that make up an SSID
4. Different SSID use cases
5. Optimizations

# Jesus Herrera

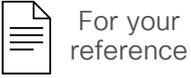
- ~7 years at Cisco
  - 4 years as a Customer Support Engineer (CSE)
  - ~3 years as a Software Engineer in CEAD
- Full time Wireless enthusiast and admirer



I didn't forget any parts,  
I just built it better...



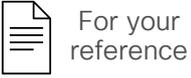
# For your reference



- There are slides in the PDF that will not be presented, or quickly presented
- They are valuable, but included only “For your reference”



# Configuration template available here



- The text format of all the configuration examples in this presentation is available here:  
[https://github.com/fedezil/CLEU24\\_BRKEWN-2094/blob/main/BRKEWN-2094\\_9800\\_config\\_template.txt](https://github.com/fedezil/CLEU24_BRKEWN-2094/blob/main/BRKEWN-2094_9800_config_template.txt)
- Do not hesitate to modify names, IPs, passwords or any other settings according to your own setup and needs

# Today is the day we say “no”!

## To this question...

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

We will address the installation of a 9800 from scratch, without any other tools (DNA/Catalyst Center, 3rd party management, automation, etc.)

1. Basic settings for connectivity, CLI/GUI\* access and authentication
2. Configuration objects and how to use them for our SSIDs
3. 802.1X, FlexConnect and Guest use cases/examples
4. Additional optimizations

\* Although screenshots may refer to different 9800 models and IOS-XE releases than yours, options are very similar throughout different platforms/versions

In the following examples we assume we're already here

```
--- System Configuration Dialog ---
```

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

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

```
Press RETURN to get started!
```

```
WLC>en
```

```
WLC#conf t
```

```
WLC(config)#
```

# Some rules only for maniacs...

Not mandatory, just for more comfortable operations:

- We could avoid the name “test” for any... test

✘ test

✔ POLICY\_TAG\_BRANCH

- For as many 9800’s internal objects as possible, we could use words in CAPITAL letters and separated\_by\_underscores for increased readability

✘ testbranch

✔ POLICY\_TAG\_BRANCH

- We could repeat the object’s type as the initial part of its name, to quickly recognize what kind of object that name is used for

✘ TEST\_BRANCH

✔ POLICY\_TAG\_BRANCH

- These tips could help us identify objects much more easily in a “show run”, and separating words with underscores ‘\_’ (dashes ‘-’ work too...) would help selecting the whole name with a double-click for copying/pasting in text editors and client terminals (e.g. Putty, Tera Term, iTerm, etc.)

✘ show run | sec test

✔ show run | sec POLICY\_TAG\_BRANCH

# Uplink IP and Wireless Management Interface (WMI)

```
hostname MY-9800
!  
vlan 10  
  name VLAN_WIRELESS_MGMT  
!  
interface Vlan10  
  ip address 192.168.1.200 255.255.255.0  
  no shutdown  
!  
interface TenGigabitEthernet0/1/0  
  switchport trunk native vlan 10  
  switchport mode trunk  
!  
ip route 0.0.0.0 0.0.0.0 192.168.1.254  
!  
wireless management interface Vlan10
```

We need a L3 interface as the wireless management interface (WMI)

This is used at least for uplink connectivity to the APs, and management too (a service port is optional)

The default GW is the wireless management's one

The wireless management VLAN does not need to be the native one (it usually isn't)

# WMI's trustpoint

On a physical 9800 (-L / -40 / -80) it's pre-installed

```
show wireless management trustpoint
```

It should be set to "CISCO\_IDEVID\_SUDI", but if not...

```
show crypto pki trustpoints
!  
no wireless management trustpoint  
wireless management trustpoint CISCO_IDEVID_SUDI
```

On a virtual 9800-CL we need to generate it

```
wireless config vwlc-ssc key-size 2048 signature-algo sha256 password 0 <OUR_PWD>  
show wireless management trustpoint
```

If not automatically associated to the WMI, we need to configure it

```
show crypto pki trustpoints
!  
no wireless management trustpoint  
wireless management trustpoint <ewlc-default-tp / CONTROLLER-9800_WLC_TP / etc. >
```



Without a trustpoint for the WMI, APs won't be able to join

# CLI/GUI access

```
username admin privilege 15 password <MY_PWD>
!
aaa new-model
aaa authentication login default local
aaa authentication login MLIST_CONSOLE none
aaa authentication login MLIST_LOGIN_LOCAL local
aaa authorization exec default local
aaa authorization exec MLIST_EXEC_LOCAL local
!
line con 0
  exec-timeout 720 0
  privilege level 15
  login authentication MLIST_CONSOLE
line vty 0 4
  exec-timeout 720 0
  privilege level 15
  authorization exec MLIST_EXEC_LOCAL
  login authentication MLIST_LOGIN_LOCAL
  transport input ssh
```

Method lists are used to configure through which resources (local, radius, tacacs, etc.) we authenticate/authorize users/identities for different services (login, exec, dot1x, etc.)

Sometime we use a method list with no authentication for console access (for backup)

Two technically distinct method lists, one for login authentication and the other for exec authorization

“default” method lists may be used too

# CLI/GUI access

```
line vty 5 50
  exec-timeout 720 0
  privilege level 15
  authorization exec MLIST_EXEC_LOCAL
  login authentication MLIST_LOGIN_LOCAL
  transport input ssh
!
service tcp-keepalives-in
service tcp-keepalives-out
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
!
no ip http server
ip http authentication local
ip http secure-server
ip http secure-trustpoint <HTTPS_TRUSTPOINT>
ip http client source-interface Vlan10
```

The GUI pages and HTTPS requests rely on VTY lines: to avoid slowing down or locking the GUI because of too few VTY lines, we increase their number to 50

Note: we could also just configure all VTY lines in one shot with “line vty 0 50”

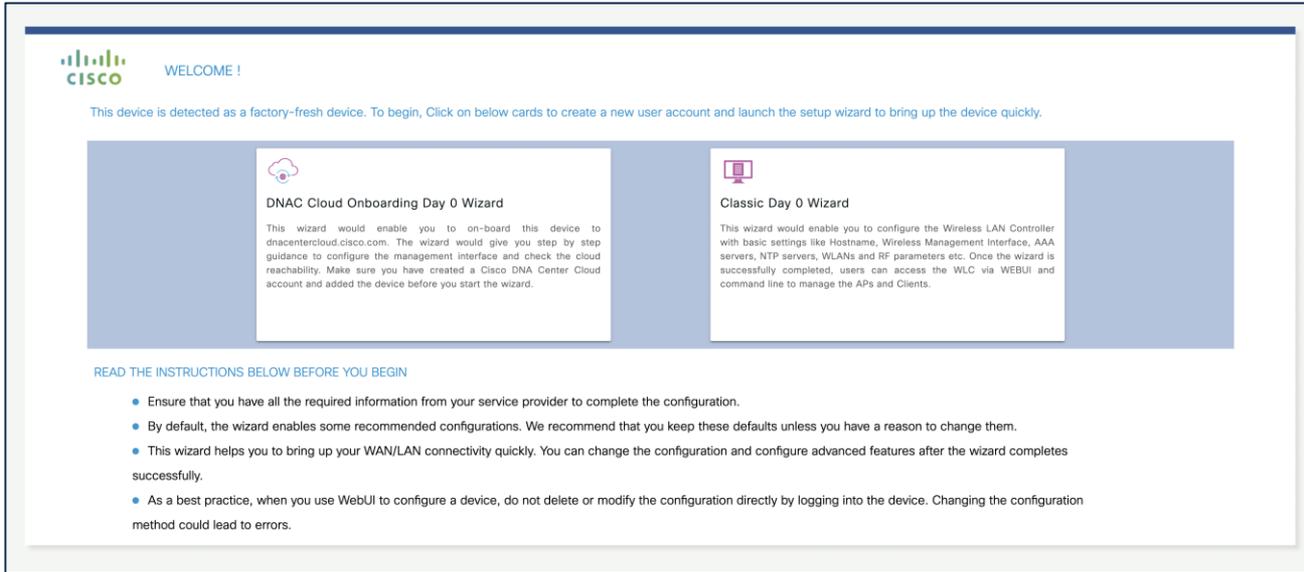
To avoid “stale” SSH/HTTPS sessions

For easier troubleshooting logs/debugs

To increase the “consistency” of GUI access, we can fix a trustpoint (to keep it simple, it could be the same as the WMI), as well as a source interface, for all HTTPS admin traffic

# Country code

If we don't configure at least one Country code on the 9800 and we try to access the GUI, we are redirected to the Day-0 wizard



The screenshot shows the Cisco Day-0 wizard interface. At the top left is the Cisco logo and the text "WELCOME!". Below this is a message: "This device is detected as a factory-fresh device. To begin, Click on below cards to create a new user account and launch the setup wizard to bring up the device quickly." There are two cards: "DNAC Cloud Onboarding Day 0 Wizard" and "Classic Day 0 Wizard". Below the cards is a section titled "READ THE INSTRUCTIONS BELOW BEFORE YOU BEGIN" with three bullet points.

**DNAC Cloud Onboarding Day 0 Wizard**

This wizard would enable you to on-board this device to dnacentercld.cisco.com. The wizard would give you step by step guidance to configure the management interface and check the cloud reachability. Make sure you have created a Cisco DNA Center Cloud account and added the device before you start the wizard.

**Classic Day 0 Wizard**

This wizard would enable you to configure the Wireless LAN Controller with basic settings like Hostname, Wireless Management Interface, AAA servers, NTP servers, VLANs and RF parameters etc. Once the wizard is successfully completed, users can access the WLC via WEBUI and command line to manage the APs and Clients.

**READ THE INSTRUCTIONS BELOW BEFORE YOU BEGIN**

- Ensure that you have all the required information from your service provider to complete the configuration.
- By default, the wizard enables some recommended configurations. We recommend that you keep these defaults unless you have a reason to change them.
- This wizard helps you to bring up your WAN/LAN connectivity quickly. You can change the configuration and configure advanced features after the wizard completes successfully.
- As a best practice, when you use WebUI to configure a device, do not delete or modify the configuration directly by logging into the device. Changing the configuration method could lead to errors.

[https://<9800\\_IP>/webui/#/dayzeroWireless](https://<9800_IP>/webui/#/dayzeroWireless) or [https://<9800\\_IP>/webui/#/dayzeroPnpOrCli](https://<9800_IP>/webui/#/dayzeroPnpOrCli)

# Since we anyway have to shut the radios...

- 1 To configure a Country code, we need to first shut down all radio networks \*

```
ap dot11 24ghz shutdown
! ('y' and/or Return to confirm)
!
ap dot11 5ghz shutdown
! ('y' and/or Return to confirm)
!
wireless country <COUNTRY_CODE>
```

- 2 Since we already shut down all radio networks, we could also configure some more optimized data rates

- 3 Then we can enable our networks again

```
no ap dot11 24ghz shutdown
no ap dot11 5ghz shutdown
```

```
ap dot11 24ghz rate RATE_11M mandatory
ap dot11 24ghz rate RATE_1M disable
ap dot11 24ghz rate RATE_2M disable
ap dot11 24ghz rate RATE_5_5M disable
ap dot11 24ghz rate RATE_6M disable
ap dot11 24ghz rate RATE_9M disable
ap dot11 24ghz rate RATE_12M supported
ap dot11 24ghz rate RATE_18M supported
ap dot11 24ghz rate RATE_24M supported
ap dot11 24ghz rate RATE_36M supported
ap dot11 24ghz rate RATE_48M supported
ap dot11 24ghz rate RATE_54M supported
!
ap dot11 5ghz rate RATE_12M mandatory
ap dot11 5ghz rate RATE_6M disable
ap dot11 5ghz rate RATE_9M disable
ap dot11 5ghz rate RATE_18M supported
ap dot11 5ghz rate RATE_24M supported
ap dot11 5ghz rate RATE_36M supported
ap dot11 5ghz rate RATE_48M supported
ap dot11 5ghz rate RATE_54M supported
```

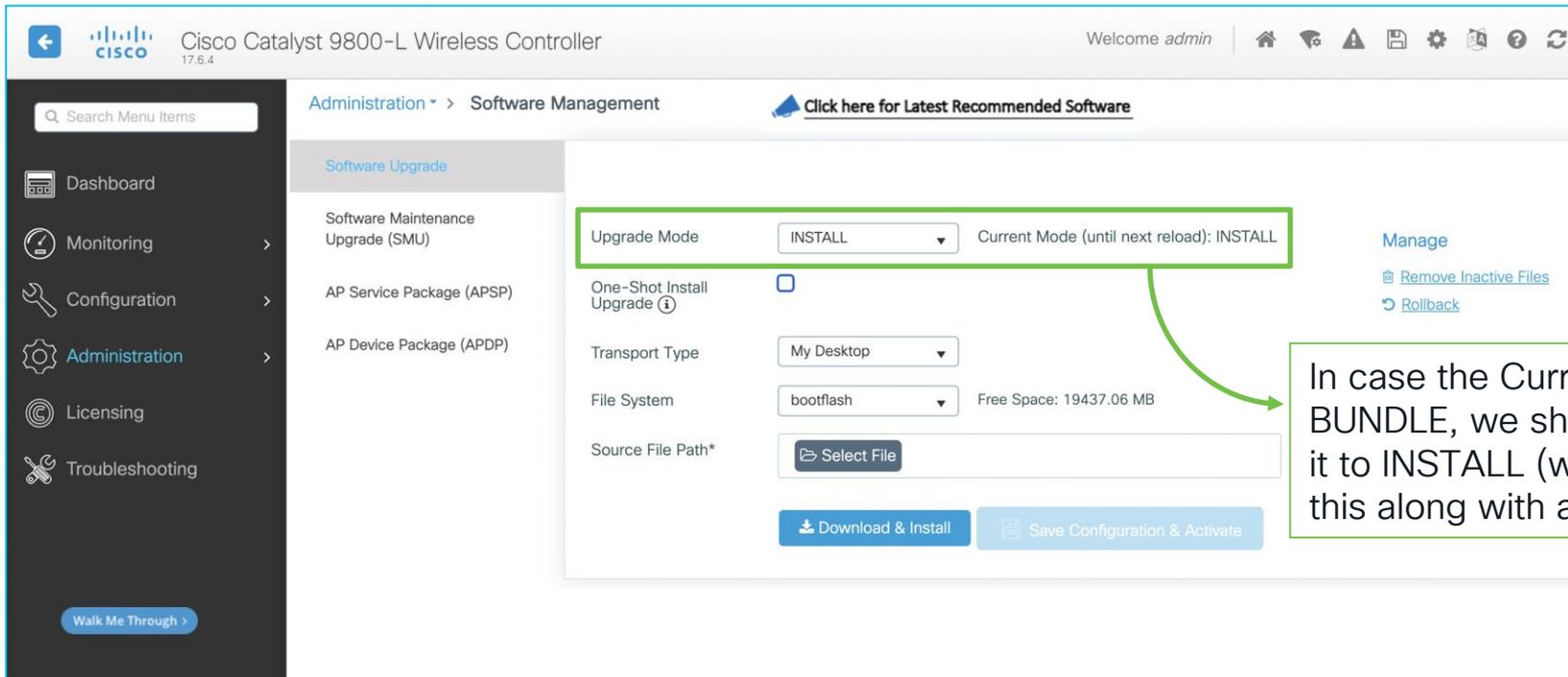
Save! Save! Save!  
(wr → write memory)



# If we'd like to upgrade, this could be a good time

Administration > Software Management

 For your reference



Administration > Software Management

Software Upgrade

Upgrade Mode: **INSTALL** (Current Mode (until next reload): **INSTALL**)

One-Shot Install Upgrade:

Transport Type: My Desktop

File System: bootflash (Free Space: 19437.06 MB)

Source File Path\*:

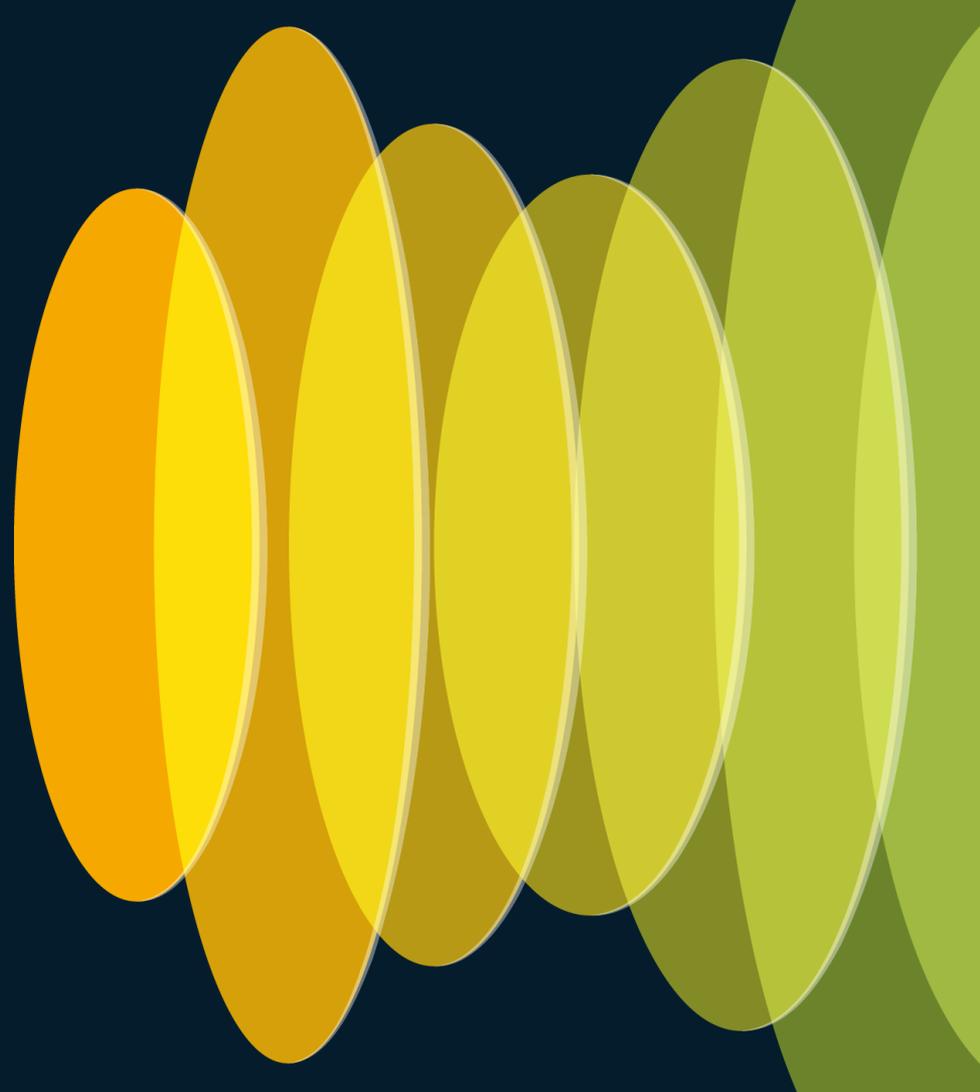
Manage  
[Remove Inactive Files](#)  
[Rollback](#)

In case the Current Mode is BUNDLE, we should change it to INSTALL (we could do this along with an upgrade)

Convert Installation Mode Between Install and Bundle on Catalyst 9800 Wireless Controller

<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/217050-convert-installation-mode-between-instal.html>

# Our first SSIDs



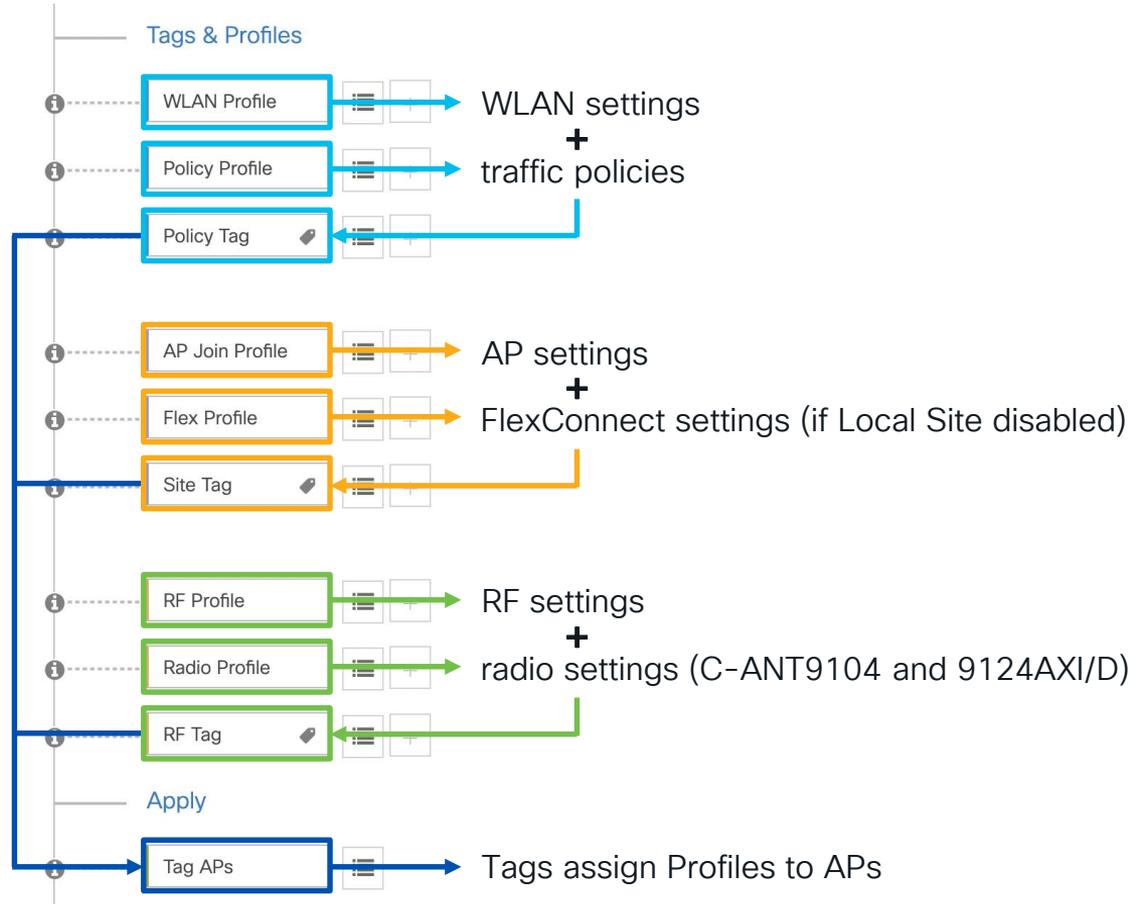
# Profiles and Tags: the main configuration objects

For configuring SSIDs, traffic policies, AP's settings, some RF/radio settings, the 9800 uses 2 main objects:

1. **Profile:** it defines the settings of specific categories
  - WLAN Profile → WLAN settings and security
  - Policy Profile → L2/L3+ traffic policies
  - AP Join Profile → AP settings
  - Flex Profile → FlexConnect settings
  - RF Profile → RF settings
  - Radio Profile → radio settings for C-ANT9104 or 9124AXI/D APs (as of 17.6.1)
2. **Tag:** it applies to an AP and defines which profiles we assign to that AP
  - Policy Tag → WLAN Profile + Policy Profile
  - Site Tag → AP Join Profile + AP mode (+ Flex Profile)
  - RF Tag → RF Profile (+ Radio Profile)

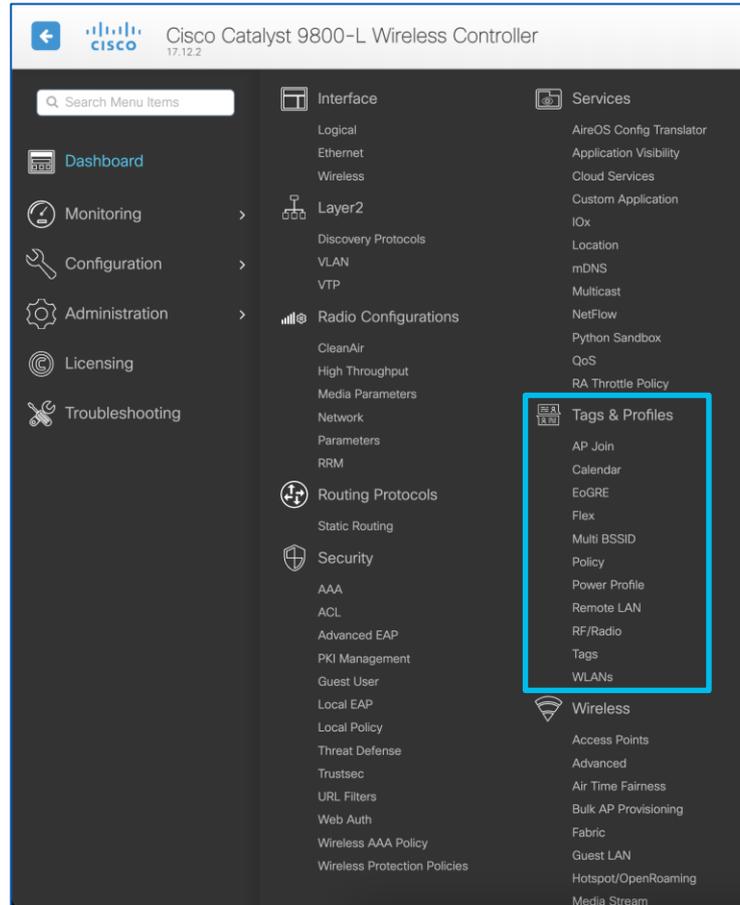
# Profiles and Tags: the main configuration objects

Configuration >  
Wireless Setup >  
Advanced >  
Start Now



# Profiles and Tags: a more dedicated menu

Configuration >  
Tags & Profiles



# Client VLANs should be configured and trunked

```
vlan 110
 name VLAN_EMPLOYEE
vlan 120
 name VLAN_VOICE
vlan 130
 name VLAN_GUEST
exit
```



```
show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Tw0/0/0
10	VLAN_WIRELESS_MGMT	active	
110	VLAN_EMPLOYEE	active	
120	VLAN_VOICE	active	
130	VLAN_GUEST	active	

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration page. The breadcrumb navigation is Configuration > Layer2 > VLAN. The page displays a table of configured VLANs:

VLAN ID	Name	Status	Ports
1	default	active	Tw0/0/0, Tw0/0/1, Tw0/0/2, Te0/1/1
10	VLAN_WIRELESS_MGMT	active	Tw0/0/3
110	VLAN_EMPLOYEE	active	
120	VLAN_VOICE	active	
130	VLAN_GUEST	active	

Configuration > Layer2 > VLAN (VLAN tab)

# Configuring a RADIUS server

Configuration > Security > AAA > Add RADIUS Server

The screenshot displays the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation path is Configuration > Security > AAA > Add RADIUS Server. A modal dialog box titled "Create AAA RADIUS Server" is open, showing the following configuration fields:

Field	Value	Field	Value
Name*	RADIUS_SRVR_ISE	Support for CoA ⓘ	ENABLED <input checked="" type="checkbox"/>
Server Address*	192.168.1.201	CoA Server Key Type	Clear Text
PAC Key	<input type="checkbox"/>	CoA Server Key ⓘ	.....
Key Type	Clear Text	Confirm CoA Server Key	.....
Key* ⓘ	.....	Automate Tester	<input type="checkbox"/>
Confirm Key*	.....		
Auth Port	1812		
Acct Port	1813		
Server Timeout (seconds)	1-1000		
Retry Count	0-100		

At the bottom of the dialog, there are "Cancel" and "Apply to Device" buttons.

# Configuring a RADIUS server group

Configuration > Security > AAA > Add RADIUS Server Group

The screenshot displays the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation path is Configuration > Security > AAA. A modal dialog box titled "Create AAA Radius Server Group" is open, showing the following configuration options:

- Name\*: RADIUS\_SVR\_GRP\_01
- Group Type: RADIUS
- MAC-Delimiter: none
- MAC-Filtering: none
- Dead-Time (mins): 5
- Load Balance:  DISABLED
- Source Interface VLAN ID: 1

Below the configuration fields, there are two lists: "Available Servers" (empty) and "Assigned Servers" (containing RADIUS\_SVR\_ISE). Navigation arrows are present between the lists. At the bottom of the dialog, there are "Cancel" and "Apply to Device" buttons.

# Configuring a AAA Method List for 802.1X

Configuration > Security > AAA > AAA Method List > Authentication > Add (Type = dot1x)

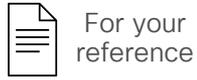
The screenshot displays the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation path is Configuration > Security > AAA > AAA Method List > Authentication > Add (Type = dot1x). The main configuration area shows the 'AAA Method List' configuration page with tabs for 'Servers / Groups', 'AAA Method List', and 'AAA Advanced'. The 'Authentication' tab is active, and the 'Quick Setup: AAA Authentication' dialog box is open. The dialog box contains the following fields and options:

- Method List Name\*: MLIST\_AUTHC\_1X
- Type\*: dot1x
- Group Type: group
- Fallback to local:
- Available Server Groups: radius, ldap, tacacs+
- Assigned Server Groups: RADIUS\_SRVR\_GRP\_01

The dialog box also includes 'Cancel' and 'Apply to Device' buttons. In the background, a table shows the configuration for Group3 and Group4, with all cells containing 'N/A'.

Group3	Group4
N/A	N/A
N/A	N/A
N/A	N/A

# AAA Method List for authorization



Configuration > Security > AAA > AAA Method List > Authorization > Add (Type = network)

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation is Configuration > Security > AAA. A modal dialog titled "Quick Setup: AAA Authorization" is open, showing the following configuration:

- Method List Name\*: MLIST\_AUTHZ\_NTWRK
- Type\*: network
- Group Type: group
- Fallback to local:
- Authenticated:
- Available Server Groups: radius, ldap, tacacs+
- Assigned Server Groups: RADIUS\_SRVR\_GRP\_01

Buttons for "Cancel" and "Apply to Device" are visible at the bottom of the dialog. In the background, a table shows configuration for Group3 and Group4.

Group3	Group4
N/A	N/A
N/A	N/A

Mainly used for MAC filtering based WLANs

# Configuring a AAA Method List for accounting

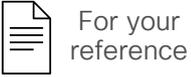
Configuration > Security > AAA > AAA Method List > Accounting > Add (Type = identity)

The screenshot displays the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation path is Configuration > Security > AAA > AAA Method List > Accounting > Add (Type = identity). The main configuration area shows the 'AAA Method List' configuration page with a 'Quick Setup: AAA Accounting' dialog box open. The dialog box contains the following fields and options:

- Method List Name\*:** MLIST\_ACCT\_ID
- Type\*:** identity (selected from a dropdown menu)
- Available Server Groups:** radius, ldap, tacacs+
- Assigned Server Groups:** RADIUS\_SRVR\_GRP\_01

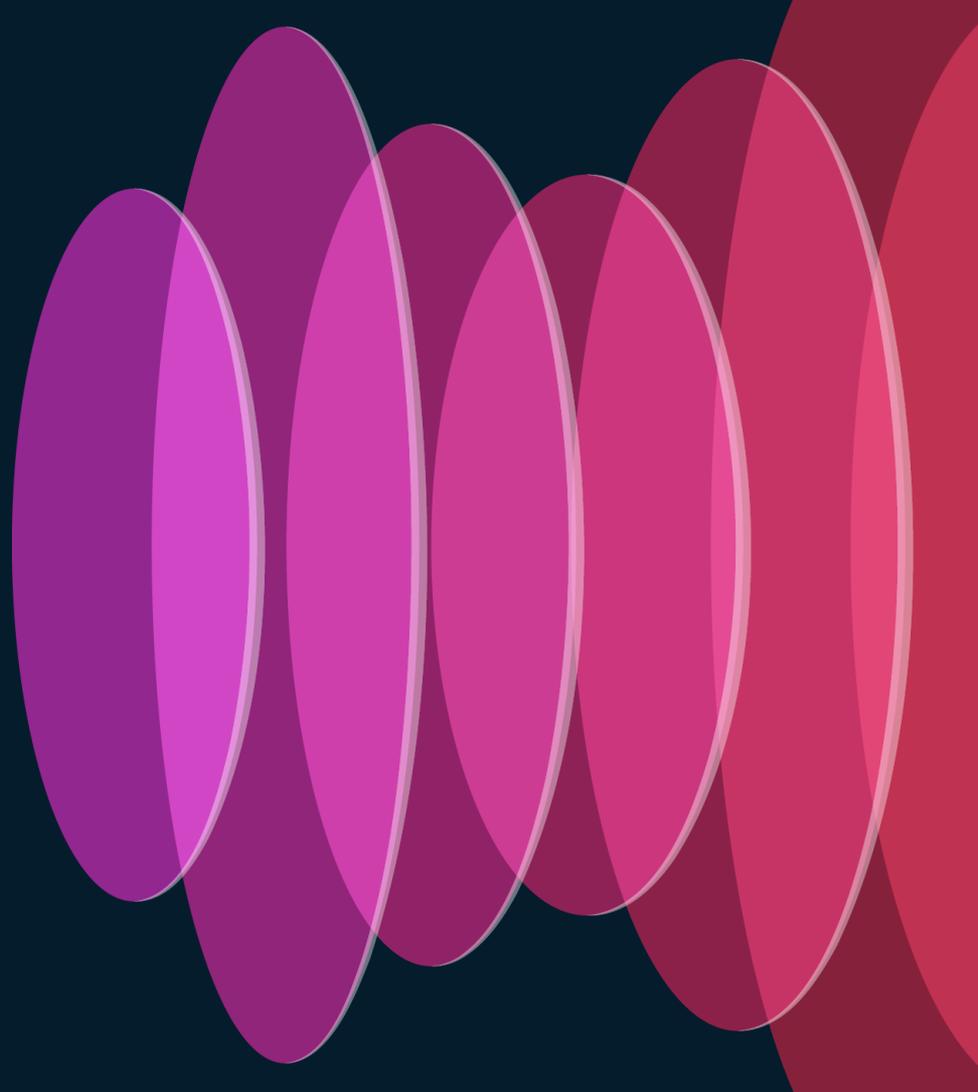
The dialog box also includes 'Cancel' and 'Apply to Device' buttons.

# Or also with a quick CLI copy/paste



```
radius server RADIUS_SRVR_ISE
  address ipv4 192.168.1.201 auth-port 1812 acct-port 1813
  key <RADIUS_SHARED_SECRET>
!
aaa server radius dynamic-author
  client 192.168.1.201 server-key <RADIUS_SHARED_SECRET>
!
aaa group server radius RADIUS_SRVR_GRP_01
  server name RADIUS_SRVR_ISE
  ip radius source-interface Vlan10
!
aaa authentication dot1x MLIST_AUTHC_1X group RADIUS_SRVR_GRP_01
aaa authorization network MLIST_AUTHZ_NTWRK group RADIUS_SRVR_GRP_01
aaa accounting identity MLIST_ACCT_ID start-stop group RADIUS_SRVR_GRP_01
```

# GUI Time



# Configuring an 802.1X WLAN Profile

Configuration > Tags & Profiles > WLANs > Add

The screenshot shows the 'Add WLAN' configuration page in the Cisco Catalyst 9800-L Wireless Controller. The 'General' tab is active, showing the following configuration:

- Profile Name\*: WLAN\_PRFL\_EMPLOYEE
- SSID\*: :[:]:. Employee
- WLAN ID\*: 1
- Status: ENABLED (green)
- Broadcast SSID: ENABLED (green)

Radio Policy configuration:

- 6 GHz Status: ENABLED (red)
- 5 GHz Status: ENABLED (green)
- 2.4 GHz Status: ENABLED (green)
- 802.11b/g Policy: 802.11b/g

Buttons: Cancel, Apply to Device

The screenshot shows the 'Add WLAN' configuration page, Security tab. The 'Layer2' tab is active, showing the following configuration:

- Security: WPA + WPA2 (selected)
- MAC Filtering: Disabled
- Lobby Admin Access: Disabled
- WPA Parameters: WPA2 Policy (checked), WPA Policy (unchecked), GTK Randomize (unchecked), OSEN Policy (unchecked)
- WPA2 Encryption: AES(CCMP128) (checked), GCMP128 (unchecked), CCMP256 (unchecked), GCMP256 (unchecked)
- Protected Management Frame: PMF (Optional)
- Fast Transition: Status (Enabled), Over the DS (unchecked), Reassociation Timeout\* (20)
- Auth Key Mgmt: 802.1x (checked), Easy-PSK (unchecked), FT + 802.1x (checked), 802.1x-SHA256 (unchecked), PSK (unchecked), CCKM (unchecked), FT + PSK (unchecked), PSK-SHA256 (unchecked)

The screenshot shows the 'Add WLAN' configuration page, AAA tab. The 'Authentication List' dropdown is open, showing the following options:

- MLIST\_AUTHC\_1 (selected)
- Select a value
- MLIST\_AUTHC\_1X

The AAA Method List for dot1x authentication

# Configuring an 802.1X WLAN Profile

## WLAN Profile > Security > Layer2

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 AAA

WPA + WPA2  WPA2 + WPA3  WPA3  Static WEP  None

MAC Filtering

Lobby Admin Access

WPA Parameters

WPA Policy  WPA2 Policy   
GTK Randomize  OSEN Policy

WPA2 Encryption

AES(CCMP128)  CCMP256   
GCMP128  GCMP256

Protected Management Frame

PMF  Optional

Association Comeback Timer\*

SA Query Time\*

Fast Transition

Status

Over the DS

Reassociation Timeout\*

Auth Key Mgmt

802.1X  PSK   
Easy-PSK  CCKM   
FT + 802.1X  FT + PSK   
802.1X-SHA256  PSK-SHA256

MPSK Configuration

Enable MPSK

- **Fast Transition / 802.11r = Enabled**  
No “Adaptive Enabled”, as it would benefit Apple/Samsung endpoints only
- **Over the DS = unchecked**  
Over the Air (OTA) is the technique all endpoints are supporting
- **Auth Key Mgmt = 802.1X and FT + 802.1X**  
To support both 802.11r capable and non-capable endpoints
- **PMF = Optional**  
For Device Analytics support

# Configuring an 802.1X WLAN Profile

## WLAN Profile > Advanced

General Security **Advanced** Add To Policy Tags

Coverage Hole Detection

Aironet IE

Advertise AP Name

P2P Blocking Action Disabled

Multicast Buffer  DISABLED

Media Stream Multicast-direct

11ac MU-MIMO

Wi-Fi to Cellular Steering

Wi-Fi Alliance Agile Multiband  DISABLED

Fastlane+ (ASR)

Deny LAA (RCM) clients

6 GHz Client Steering

Latency Measurements Announcements

Universal Admin

OKC

Load Balance

Band Select

IP Source Guard

WMM Policy Allowed

mDNS Mode Bridging

Off Channel Scanning Defer

Defer Priority  0  1  2  3  4  5  6  7

Scan Defer Time 100

- **Aironet IE = unchecked**  
Used along with “Advertise AP Name” for site surveys, but not in production (unless with WGBs)
- **11ac MU-MIMO = unchecked**  
Some 802.11ac endpoints showed caveats with MU-MIMO and don’t use it anyway
- **Fastlane+ (ASR) = unchecked**  
Supported by some Apple endpoints only
- **6 GHz Client Steering = checked**  
If using 6 GHz
- **OKC = checked**  
For endpoints not supporting 802.11r
- **Load Balance / Band Select = unchecked**  
As they are false friends for (not) steering endpoints away
- **Off Channel Scanning Defer Priority 7**  
Because EAP frames are sent with 802.11 UP 7

# Configuring an 802.1X WLAN Profile

## WLAN Profile > Advanced

**Max Client Connections**

Per WLAN: 0

Per AP Per WLAN: 0

Per AP Radio Per WLAN: 200

**Assisted Roaming (11k)**

Prediction Optimization:

Neighbor List:

Dual Band Neighbor List:

**DTIM Period (in beacon intervals)**

5 GHz Band (1-255): 1

2.4 GHz Band (1-255): 1

**Device Analytics**

Advertise Support:

Advertise PC Analytics Support:

Share Data with Client:

**11k Beacon Radio Measurement**  
*Client Scan Report*

On Association:

On Roam:

**11v BSS Transition Support**

BSS Transition:

Dual Neighbor List:

BSS Max Idle Service:

BSS Max Idle Protected:

Directed Multicast Service:

*Configuration of '11v BSS Disassociation Imminent' is supported from Command Line Interface (CLI) only*

**11ax**

Enable 11ax:

Downlink OFDMA:

Uplink OFDMA:

Downlink MU-MIMO:

Uplink MU-MIMO:

BSS Target Wake Up Time:

- 802.11k, 802.11v and 802.11ax defaults  
Usually we don't change these, unless specifically needed
- Device Analytics  
All options enabled, along with PMF Optional/Required under L2 security settings
- 802.11k reports on association/roam  
For additional client reports and more informed roaming decisions

# Configuring the Policy Profile

Configuration > Tags & Profiles > Policy > Add

Configuration > Tags & Profiles > Policy > Add

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

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

Name\* POLICY\_PRFL\_EMPLOYEE

Description Enter Description

Status **ENABLED**

Passive Client **DISABLED**

IP MAC Binding **ENABLED**

Encrypted Traffic Analytics **DISABLED**

**CTS Policy**

Inline Tagging

SGACL Enforcement

Default SGT 2-65519

**WLAN Switching Policy**

Central Switching **ENABLED**

Central Authentication **ENABLED**

Central DHCP **ENABLED**

Flex NAT/PAT **DISABLED**

Cancel Apply to Device

Policy Profile for central switching

As for a WLAN Profile, we need to explicitly enable it

# Configuring the Policy Profile

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

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

RADIUS Profiling  
 HTTP TLV Caching  
 DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification ⓘ

Local Subscriber Policy Name Search or Select

VLAN

VLAN/VLAN Group  
Multicast VLAN

VLAN/VLAN Group dropdown menu:  
VLAN\_EMPLOYEE (selected)  
default  
VLAN\_EMPLOYEE  
VLAN\_GUEST  
VLAN\_VOICE  
VLAN\_WIRELESS\_MGMT

WLAN ACL

IPv4 ACL Search or Select  
IPv6 ACL Search or Select

URL Filters ⓘ

Pre Auth Search or Select  
Post Auth Search or Select

Cancel Apply to Device

For local profiling, as well as sharing profiling attributes via RADIUS Accounting with ISE (Identity Services Engine)

VLANs dynamically assigned via RADIUS take precedence over the VLAN statically selected under the Policy Profile

If we are not dynamically assigning VLANs via RADIUS, we can select the centrally switched VLAN under the Access Policies tab of the Policy Profile

This VLAN must already exist in the 9800's database

# Configuring the Policy Profile

To avoid too many reauthentications  
(28800 secs / 8 hours by default as of IOS-XE 17.12)

For increased security/control

### Add Policy Profile

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

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

**WLAN Timeout**

Session Timeout (sec)  ⓘ

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

**DHCP**

IPv4 DHCP Required

DHCP Server IP Address

Fabric Profile  Search or Select

Link-Local Bridging

mDNS Service Policy Search or Select

Hotspot Server Search or Select

**User Defined (Private) Network**

Status

Drop Unicast

**DNS Layer Security**

DNS Layer Security Parameter Map Not Configured [Clear](#)

# Configuring the Policy Profile

Allow AAA Override to support dynamic RADIUS attributes

NAC State/Type for CoA support

Accounting List for RADIUS Accounting and CoA too

For increased security/control

**Add Policy Profile**

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

**AAA Policy**

Allow AAA Override

NAC State

NAC Type

Policy Name

Accounting List

**WGB Parameters**

Broadcast Tagging

WGB VLAN

**Policy Proxy Settings**

ARP Proxy

IPv6 Proxy

**Advanced**

Fabric Profile

Link-Local Bridging

mDNS Service Policy

Hotspot Server

**User Defined (Private) Network**

Status

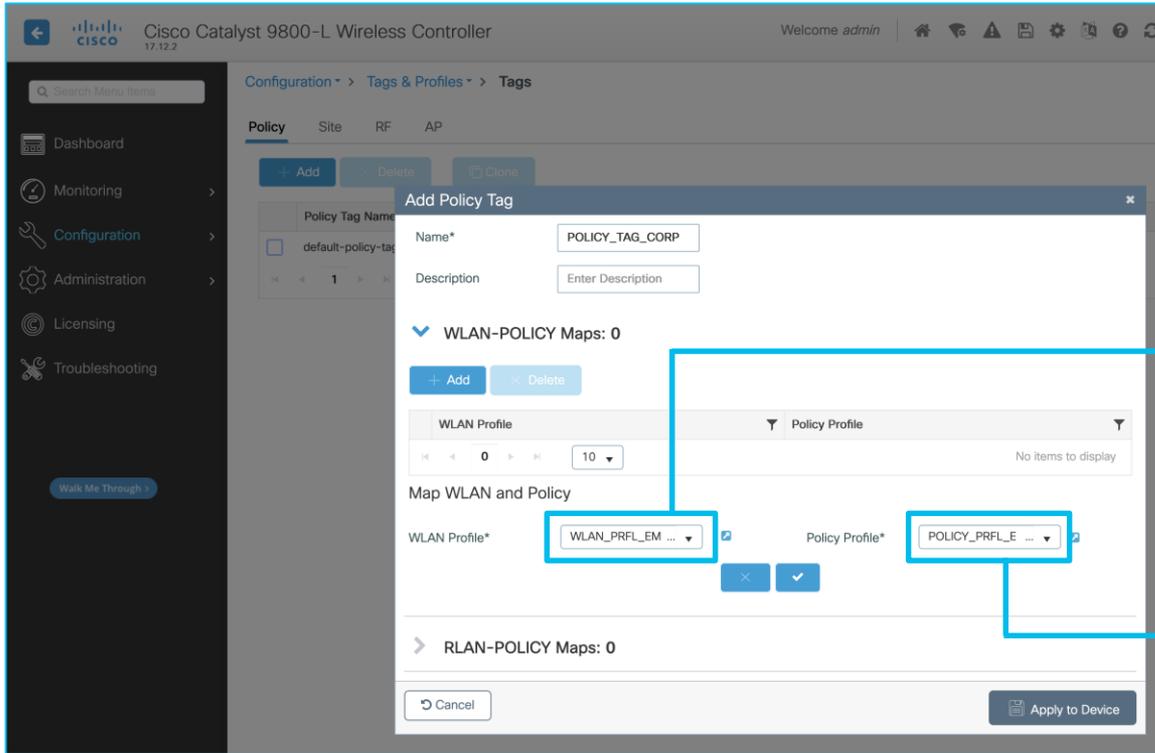
Drop Unicast

**DNS Layer Security**

DNS Layer Security Parameter Map  [Clear](#)

# Configuring the Policy Tag

Configuration > Tags & Profiles > Tags > Policy > Add



Policy Tag

=

WLAN Profile  
(it defines the SSID,  
radio options, security  
options, etc.)

+

Policy Profile  
(it defines switching  
techniques, traffic handling,  
L2/L3 ACLs, QoS, etc.)

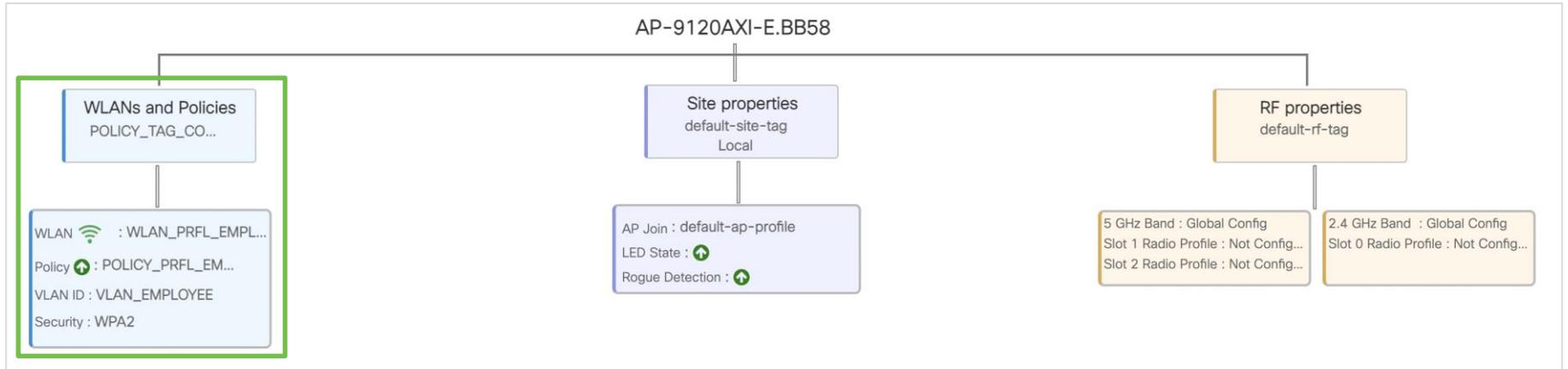
# Assigning the Policy Tag to the AP

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The main navigation pane on the left includes Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The breadcrumb path is Configuration > Wireless > Access Points. The 'All Access Points' section shows a table with one AP: AP-9166I-E.0D70, model CW9166I-E, with 3 slots. The 'Edit AP' dialog is open, showing the 'Tags' section. The 'Policy' dropdown is set to 'default-policy-tag'. A callout box points to this dropdown with the text: 'Here we can select the POLICY\_TAG\_CORP that we just configured. The CAPWAP service will restart (not a reload)'. The 'Update & Apply to Device' button is visible at the bottom right of the dialog.

# Checking Tags and Profiles assignment

AP Name ⋮

AP-9166I-E.0D70 



# Other options to assign Tags

Configuration > Tags & Profiles > Tags > AP > Tag Source

Through regex rules for the AP names

### Associate Tags to AP

Rule Name*	<input type="text" value="FILTER_CORP"/>	Policy Tag Name	<input type="text" value="POLICY_TAG_CO..."/>
AP name regex*	<input type="text" value="^AP-.*"/>	Site Tag Name	<input type="text" value="default-site-tag"/>
Active	<input checked="" type="checkbox"/>	RF Tag Name	<input type="text" value="default-rf-tag"/>
Priority*	<input type="text" value="1023"/>		

Cisco Catalyst 9800-L Wireless Controller 17.12.2

Configuration > Tags & Profiles > Tags

Policy Site RF **AP**

Tag Source Static Location Filter

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

Drag and Drop Tag Sources to change priorities

Revalidate Tag Sources on APs

Enable AP Tag Persistence

Apply

### Create Location and associate APs

General AP Provisioning

Location*	<input type="text" value="LOC_CORP"/>
Description	<input type="text" value="Enter Description"/>
Policy Tag Name	<input type="text" value="POLICY_TAG_CO..."/>
Site Tag Name	<input type="text" value="default-site-tag"/>
RF Tag Name	<input type="text" value="default-rf-tag"/>

### Create Location and associate APs

General AP Provisioning

Add/Select APs

Import AP MAC

AP MAC Address

Available AP list

AP MAC	AP Name
<input type="checkbox"/>	149f.4311.0d70
<input type="checkbox"/>	AP-9166f-E.0D70

Number of selected APs: 0

APs on this Location

Associated AP list

AP MAC	AP Name	Status
No items to display		

Through a "Location" or group of APs

Policy Site RF **AP**

Tag Source Static Location Filter

+ Add - Delete

Select File Upload File

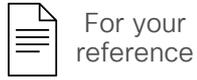
Number of AP Tag mappings selected: 0

AP MAC Address	Policy Tag Name	Site Tag Name	RF Tag Name
<input type="checkbox"/>	149f.4311.0d70	POLICY_TAG_CORP	default-site-tag
<input type="checkbox"/>			default-rf-tag

"Manually" or through a CSV file



# Enabling Tags persistency



Configuration > Tags & Profiles > Tags > AP > Tag Source

The screenshot shows the configuration page for AP Tag Source. The breadcrumb navigation is Configuration > Tags & Profiles > Tags. The page title is Cisco Catalyst 9800-L Wireless Controller, version 17.12.2, with a welcome message for admin. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area shows the configuration for AP Tag Source. A table lists the tag sources with their priorities and status. The 'Enable AP Tag Persistency' checkbox is checked and highlighted with an orange box. Below the table, there is a note: 'Drag and Drop Tag Sources to change priorities'. There are also checkboxes for 'Revalidate Tag Sources on APs' (unchecked) and 'Enable AP Tag Persistency' (checked). An 'Apply' button is at the bottom.

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

Drag and Drop Tag Sources to change priorities

Revalidate Tag Sources on APs

Enable AP Tag Persistency

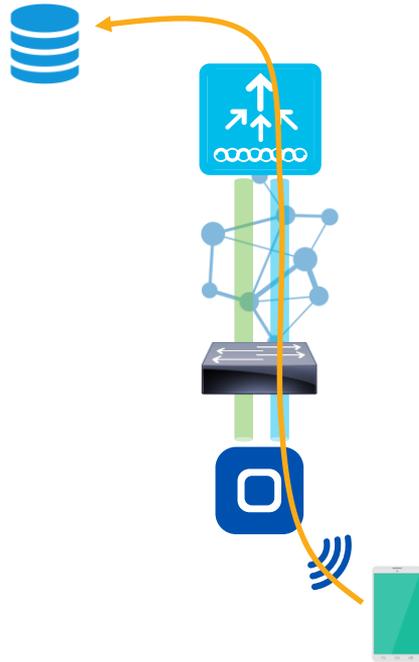
Apply

AP Tag Persistency can be useful if we want APs to keep their Tags when moving between controllers (e.g., N+1 HA)

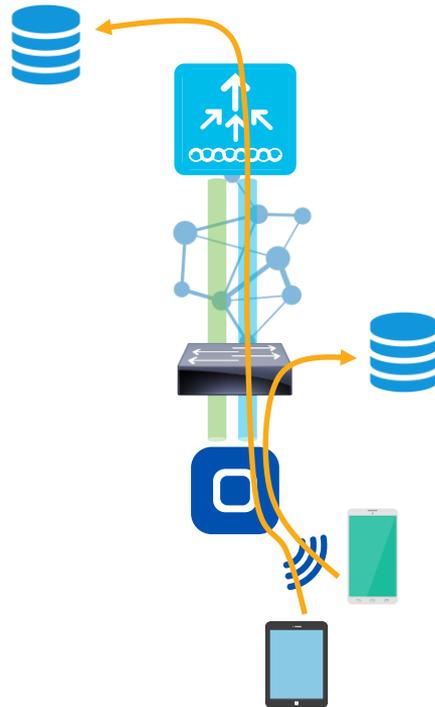
The same Tags must be present on the new destination controller and they are applied according to the AP's memory if no other mappings (static, filter, etc.) supersede them

# Central or (FlexConnect) Local Switching

Local Mode AP  
(Central Switching)



FlexConnect mode AP  
(Central / Local Switching)



— CAPWAP Control  
— CAPWAP Data

# Going FlexConnect

## 1. The AP must be in FlexConnect mode

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation is Configuration > Tags & Profiles > Tags. The 'Site' tab is selected. In the 'Edit Site Tag' form, the 'Name\*' field is 'default-site-tag', 'Description' is 'default site tag', 'AP Join Profile' is 'default-ap-profile', and 'Fabric Control Plane Name' is empty. The 'Enable Local Site' checkbox is checked. A green box highlights the 'Enable Local Site' checkbox, and a green arrow points from it to a zoomed-in view of the form.

Configuration > Tags & Profiles > Tags > Site

Enable Local Site → all APs assigned to the Site Tag are in Local mode (central switching)

Disable Local Site → all APs assigned to the Site Tag are in FlexConnect mode

This is a zoomed-in view of the 'Edit Site Tag' form. The 'Flex Profile' dropdown is set to 'default-flex-profile'. The 'Enable Local Site' checkbox is unchecked. Dashed blue boxes highlight the 'Flex Profile' and 'Enable Local Site' fields.

# Going FlexConnect

1. The AP must be in FlexConnect mode (with a new dedicated Site Tag)

The screenshot displays the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation path is Configuration > Tags & Profiles > Tags. The 'Site' tab is selected, and the 'Add Site Tag' dialog box is open. The dialog box contains the following fields:

- Name\*: SITE\_TAG\_BRANCH
- Description: Enter Description
- AP Join Profile: default-ap-profile
- Flex Profile: default-flex-profile
- Fabric Control Plane Name: (empty)
- Enable Local Site:
- Load\*: 0

The 'Flex Profile' and 'Enable Local Site' fields are highlighted with red dashed boxes. The 'Apply to Device' button is visible at the bottom right of the dialog box.

Configuration > Tags & Profiles > Tags > Site

# Going FlexConnect

1. The AP must be in FlexConnect mode (with a new dedicated Site Tag)

The screenshot displays the Cisco Catalyst 9800-L Wireless Controller interface. The left sidebar shows the navigation menu with 'Configuration' selected. The main content area is divided into two panes. The left pane shows the 'All Access Points' configuration page, with a table listing APs. The right pane shows the 'Edit AP' configuration page for AP-9166I-E.0D70. In the 'Tags' section, the 'SITE\_TAG\_BRANCH' dropdown is highlighted with a blue box, and a blue arrow points to it from below. A yellow warning box is also visible in the 'Tags' section.

Configuration > Wireless > Access Points

AP Name	AP Model	Slots	Admin Status
AP-9166I-E.0D70	CW9166I-E	3	✓

General

AP Name\* AP-9166I-E.0D70

Location\* default location

Base Radio MAC 6c8d.772e.8a20

Ethernet MAC 149f.4311.0d70

Admin Status ENABLED

AP Mode Local

Operation Status Registered

Fabric Status Disabled

Tags

Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.

Policy POLICY\_TAG\_CO ...

Site SITE\_TAG\_BRANCH

RF default-site-tag

Write Tag Config to AP SITE\_TAG\_BRANCH

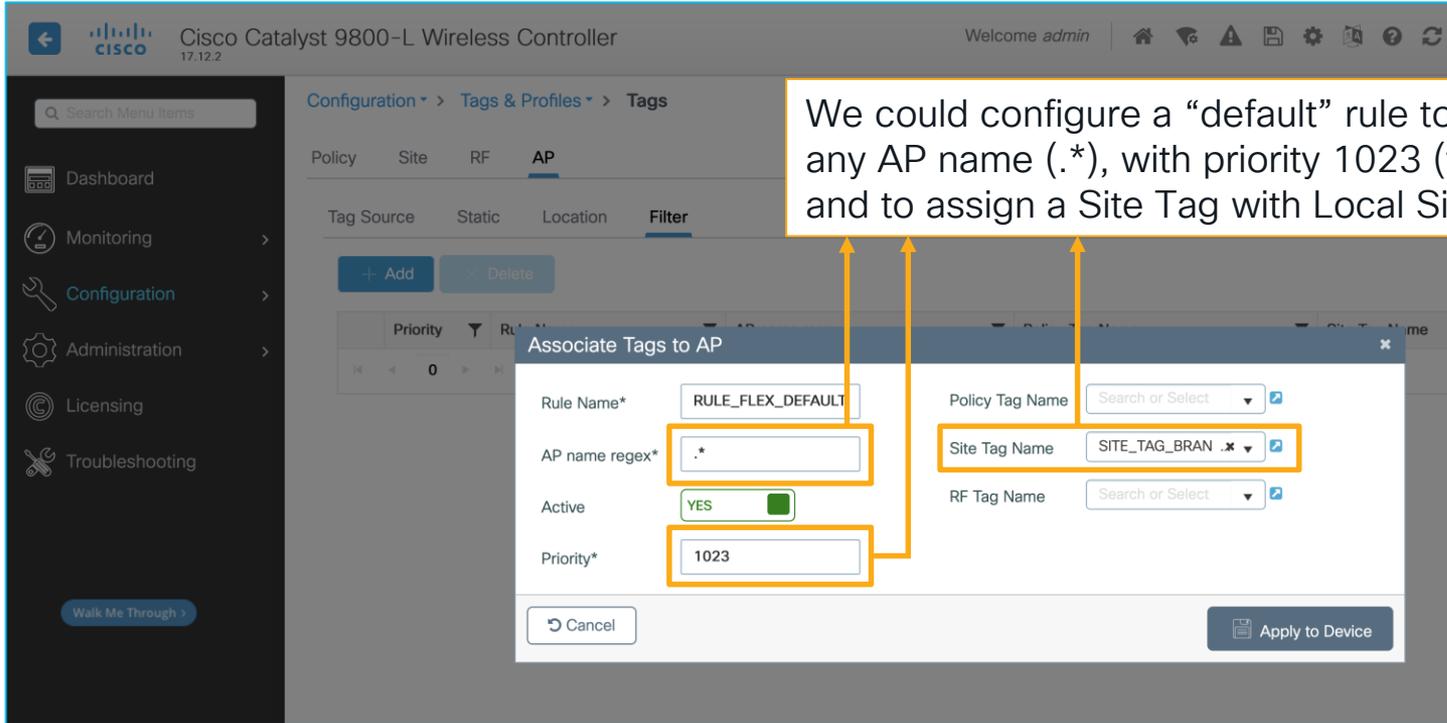
Configuration > Wireless > Access Points

Assigning APs to a Site Tag with “Local Site” disabled converts them to FlexConnect mode

# Quick tip: default all APs to FlexConnect mode

Configuration > Tags & Profiles > Tags > AP > Filter

 For your reference



The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation is Configuration > Tags & Profiles > Tags > AP > Filter. The 'Filter' tab is selected, and the 'Associate Tags to AP' dialog box is open. The dialog box contains the following fields:

- Rule Name\*: RULE\_FLEX\_DEFAULT
- AP name regex\*: .\*
- Active: YES (checked)
- Priority\*: 1023
- Policy Tag Name: Search or Select
- Site Tag Name: SITE\_TAG\_BRAN .x
- RF Tag Name: Search or Select

Orange boxes highlight the 'AP name regex\*', 'Priority\*', and 'Site Tag Name' fields. Three orange arrows point from a text box above to these three fields.

We could configure a “default” rule to match on any AP name (.\*), with priority 1023 (the lowest) and to assign a Site Tag with Local Site disabled

# Going FlexConnect

2. The Policy Profile must have Central Switching (and usually Central DHCP) disabled

The screenshot shows the 'Add Policy Profile' configuration window. A warning message at the top reads: "Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile." The 'General' tab is selected. The 'Name' field contains "\_PRFL\_EMPLOYEE\_FLEX". The 'WLAN Switching Policy' section is highlighted with a blue box and contains the following settings:

Setting	Value
Central Switching	DISABLED
Central Authentication	ENABLED
Central DHCP	DISABLED
Flex NAT/PAT	DISABLED

Other settings in the 'General' tab include: Description (Enter Description), Status (ENABLED), Passive Client (DISABLED), IP MAC Binding (ENABLED), Encrypted Traffic Analytics (DISABLED), CTS Policy (Inline Tagging, SGACL Enforcement, Default SGT: 2-65519). Buttons for 'Cancel' and 'Apply to Device' are at the bottom.

We could have also modified the existing POLICY\_PRFL\_EMPLOYEE profile. A new, dedicated one for FlexConnect could be more reusable

# Going FlexConnect

## 3. Configuring a locally switched VLAN ID or a VLAN name (in this case the Flex Profile must follow)

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

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

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification ⓘ

Local Subscriber Policy Name Search or Select

VLAN

VLAN/VLAN Group 211 ⓘ

Multicast VLAN Enter Multicast VLAN

WLAN ACL

IPv4 ACL Search or Select

IPv6 ACL Search or Select

URL Filters ⓘ

Pre Auth Search or Select

Post Auth Search or Select

Cancel Apply to Device

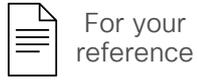
VLANs dynamically assigned via RADIUS take precedence over the VLAN statically defined under the Policy Profile.

If you are not dynamically assigning VLANs via RADIUS, you can define the locally switched VLAN under the Access Policies tab of the Policy Profile. Be aware that:

- when using the VLAN number, this VLAN does not need to exist in the 9800's database;
- when using the VLAN name, the VLAN must exist both in the 9800's local database and under the Flex Profile, with exactly the same name and ID.

Configuration > Tags & Profiles > Policy

# Going FlexConnect



## 3. Configuring a locally switched VLAN ID or a VLAN name (in this case the Flex Profile must follow)

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

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

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification ⓘ

Local Subscriber Policy Name Search or Select ▾

VLAN

VLAN/VLAN Group **VLAN\_EMPLOYEE** ⓘ

- default
- VLAN\_EMPLOYEE**
- VLAN\_GUEST
- VLAN\_VOICE
- VLAN\_WIRELESS\_MGMT

Multicast VLAN

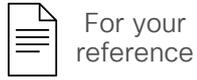
Cancel Apply to Device

VLANs dynamically assigned via RADIUS take precedence over the VLAN statically defined under the Policy Profile.

If you are not dynamically assigning VLANs via RADIUS, you can define the locally switched VLAN under the Access Policies tab of the Policy Profile. Be aware that:

- when using the VLAN number, this VLAN does not need to exist in the 9800's database;
- **when using the VLAN name, the VLAN must exist both in the 9800's local database and under the Flex Profile, with exactly the same name and ID.**

# Going FlexConnect



## 3. Configuring a locally switched VLAN ID or a VLAN name (in this case the Flex Profile must follow)

yst 9800-L Wireless Controller | Welcome admin

Configuration > Tags & Profiles > Flex

Edit Flex Profile

General | Local Authentication | Policy ACL | **VLAN** | DNS Layer Security

+ Add | - Delete

VLAN Name	ID	Ingress ACL	Egress ACL
<input type="checkbox"/> VLAN_EMPLOYEE	110		

1 - 1 of 1 items

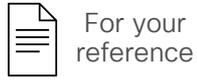
Configuration > Tags & Profiles > Flex

VLANs dynamically assigned via RADIUS take precedence over the VLAN statically defined under the Policy Profile.

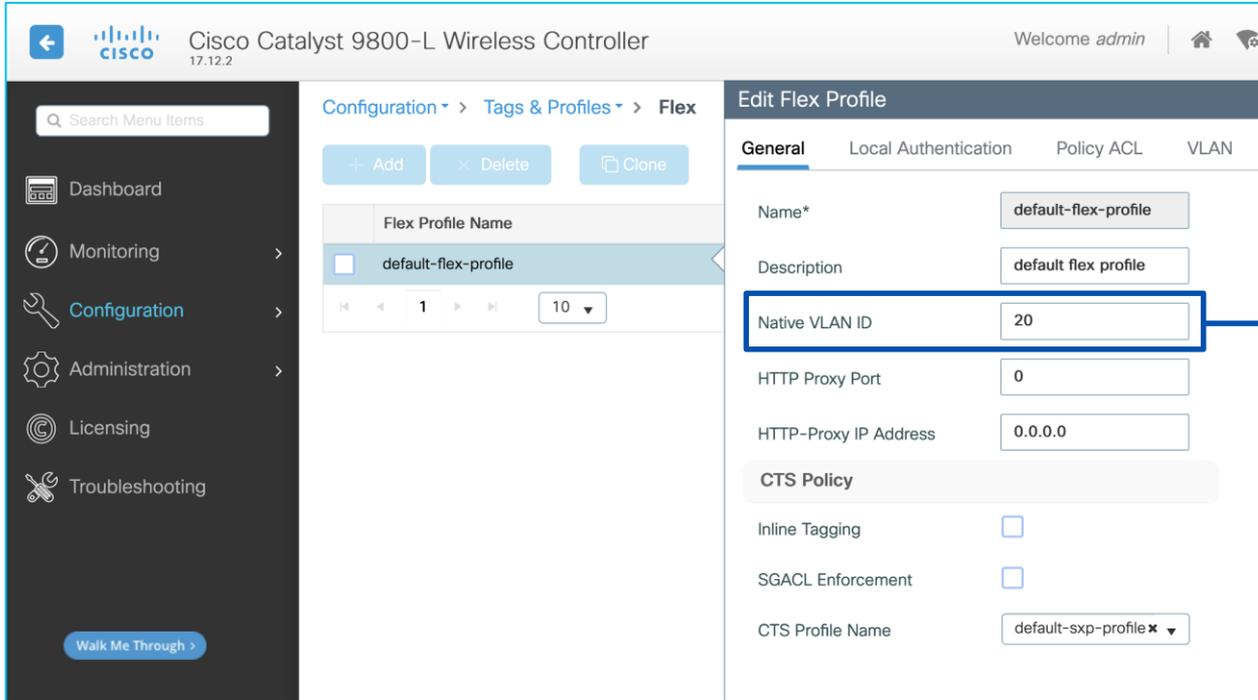
If you are not dynamically assigning VLANs via RADIUS, you can define the locally switched VLAN under the Access Policies tab of the Policy Profile. Be aware that:

- when using the VLAN number, this VLAN does not need to exist in the 9800's database;
- **when using the VLAN name, the VLAN must exist both in the 9800's local database and under the Flex Profile, with exactly the same name and ID.**

# FlexConnect Native VLAN ID consistency



Configuration > Tags & Profiles > Flex



The screenshot shows the 'Edit Flex Profile' configuration page for a Cisco Catalyst 9800-L Wireless Controller. The breadcrumb navigation is 'Configuration > Tags & Profiles > Flex'. The 'Flex Profile Name' is 'default-flex-profile'. The 'Native VLAN ID' field is set to '20' and is highlighted with a blue box. A blue arrow points from this box to the explanatory text on the right. Other fields include 'Name\*' (default-flex-profile), 'Description' (default flex profile), 'HTTP Proxy Port' (0), 'HTTP-Proxy IP Address' (0.0.0.0), 'CTS Policy' (Inline Tagging, SGACL Enforcement), and 'CTS Profile Name' (default-sxp-profile).

Although not always technically necessary for this to work, it is highly recommended for consistency purposes to match the Native VLAN ID of the Flex Profile with the actual native VLAN number of the trunk port, where the FlexConnect AP is connected

# Going FlexConnect

Linking the (existing) WLAN Profile with the new Policy Profile for local switching

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation is Configuration > Tags & Profiles > Tags > Policy. A modal dialog titled "Add Policy Tag" is open. The "Name\*" field is filled with "POLICY\_TAG\_BRANCH". Below it is a "Description" field with the placeholder "Enter Description". Under the "WLAN-POLICY Maps: 1" section, there is a table with two columns: "WLAN Profile" and "Policy Profile". The first row shows "WLAN\_PRFL\_EMPLOYEE" in the "WLAN Profile" column and "POLICY\_PRFL\_EMPLOYEE\_FLEX" in the "Policy Profile" column. A blue arrow points from the text on the right to the "POLICY\_PRFL\_EMPLOYEE\_FLEX" cell. At the bottom of the dialog are "Cancel" and "Apply to Device" buttons.

We can create a new Policy Tag, which links the same WLAN Profile for our employees' use case, but now with the new Policy Profile for FlexConnect local switching

The WLAN Profile stays the same, only the traffic policies change

Configuration > Tags & Profiles > Tags > Policy

# Assigning the Policy Tag to the AP

If we use a new Policy Tag, we need to assign it to our AP(s) as per usual

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller interface. The main navigation menu on the left includes Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The current view is 'Configuration > Wireless > Access Points'. The 'All Access Points' section shows a table with one AP: AP-9166i-E.0D70, model CW9166i-E, 3 slots, and Admin Status 'ENABLED'. The 'Edit AP' window is open, showing the 'Tags' section. The 'Policy' field is set to 'POLICY\_TAG\_BRANCH'. A warning message states: 'Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.'

Statically assigning TAGs directly under the APs is a quick option for demos/labs/PoC's.

For more scalable options we could use filters with regex, locations or even NETCONF with external tools.

# Adding a Guest SSID (LWA with internal portal)

Configuration > Security > ACL

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation is Configuration > Security > ACL. The 'Edit ACL' window is open for 'ACL\_LWA\_INTERNAL\_F'. The ACL Type is 'IPv4 Extended'. The Rules section shows three rules:

Sequence	Action	Source Type	Destination Type	Protocol	Log	DSCP
10	permit	any	any	udp	<input type="checkbox"/>	None
20	permit	any	any	udp	<input type="checkbox"/>	None
30	deny	any	any	ip	<input type="checkbox"/>	None

Below the table is a summary of the ACL rules:

```
ip access-list extended ACL_LWA_INTERNAL_PORTAL
permit udp any any eq bootps log
permit udp any any eq domain log
deny ip any any log
```

This ACL is technically not mandatory, because the 9800 will auto-assign a pre-canned one for LWA internal portals. Still recommended in case we'd like to distinguish ACLs and monitor ACE's hits.

# Adding a Guest SSID (LWA with internal portal)

Configuration > Security > Web Auth

The screenshot shows the configuration page for the 'global' Web Auth Parameter Map. The 'General' tab is active, displaying various settings. The 'Virtual IPv4 Address' is set to '192.0.2.1', and the 'Virtual IPv6 Address' is set to 'fe80::903a:0:0:'. The 'Enable HTTP server for Web Auth' checkbox is checked. The 'Banner Configuration' section is also visible, with the 'Banner Title' field empty and the 'Banner Type' set to 'None'.

The “global” Web Auth Parameter Map determines the Virtual IP and the trustpoint certificate used for LWA redirections

Other custom Web Auth Parameter Maps will inherit these settings

Recommended:

- Always configure a Virtual IPv4 (192.0.2.1) and IPv6 (FE80:0:0:0:903A::11E4), the latter to ensure IPv6 endpoints are not redirected to the internal portal when using an external one
- Keep the HTTP server globally disabled on the 9800 (for security reasons)
- Enable “HTTP server for Web Auth” under the Web Auth Parameter Map, to still support HTTP redirection

# Adding a Guest SSID (LWA with internal portal)

Configuration > Security > Web Auth

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation is Configuration > Security > Web Auth. The 'Edit Web Auth Parameter' dialog box is open, showing the 'General' tab. The 'Parameter-map Name' is 'WEBAUTH\_PMA'. The 'Type' dropdown is set to 'consent'. Other settings include 'Maximum HTTP connections' (100), 'Init-State Timeout(secs)' (120), 'Turn-on Consent with Email' (unchecked), 'Captive Bypass Portal' (unchecked), 'Disable Success Window' (unchecked), 'Disable Logout Window' (checked), 'Disable Cisco Logo' (unchecked), 'Sleeping Client Status' (unchecked), and 'Sleeping Client Timeout (minutes)' (720). The 'Banner Configuration' tab is also visible.

We can create our own Web Auth Parameter Map for even more control on different portals. The “Type” option defines the kind of portal we’d like to use:

- webauth = login + password
- consent = accept terms and conditions
- webconsent = login/pwd + terms & conditions
- authbypass = not supported

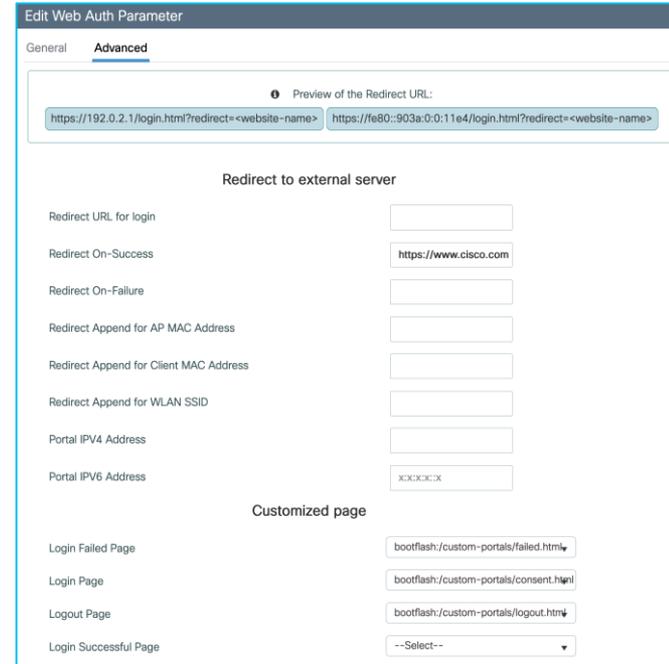
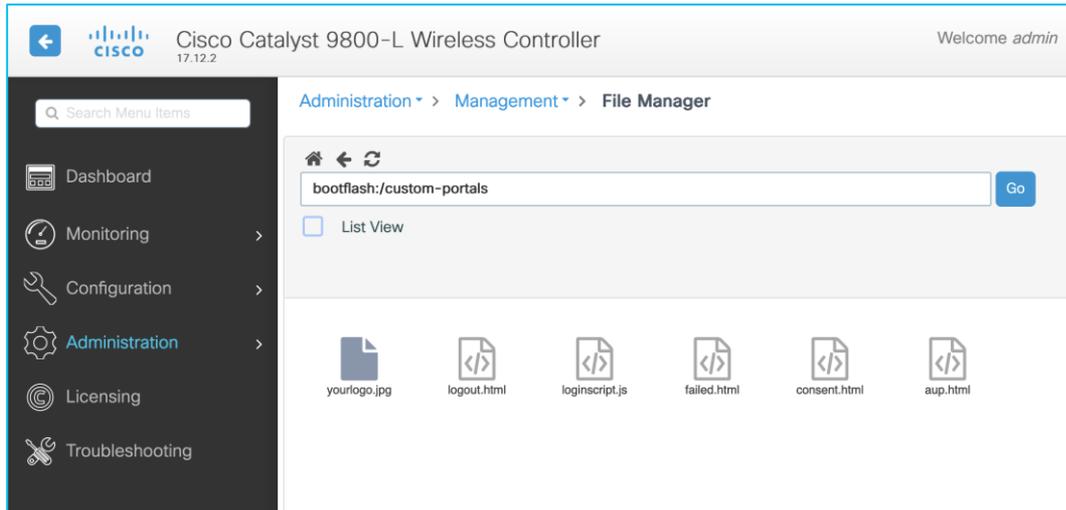
In the Advanced tab we can also choose the “Redirect On-Success” URL and select custom portal files if needed (to be uploaded to the bootflash)

# Method lists and custom files

If using a “consent” portal type or the 9800’s local database for guest users, we should configure default method lists for authentication (login) and authorization (network), pointing to local accounts

```
aaa authentication login default local
aaa authorization network default local
```

Custom portal files can be uploaded to the bootflash and then selected under the Web Auth Parameter Map (Advanced tab)



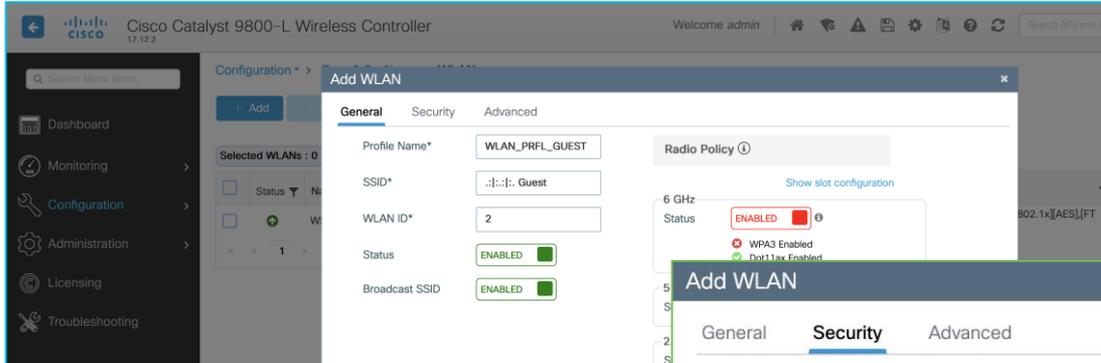
# Adding a Guest SSID (LWA with internal portal)

Configuration > Security > Web Auth

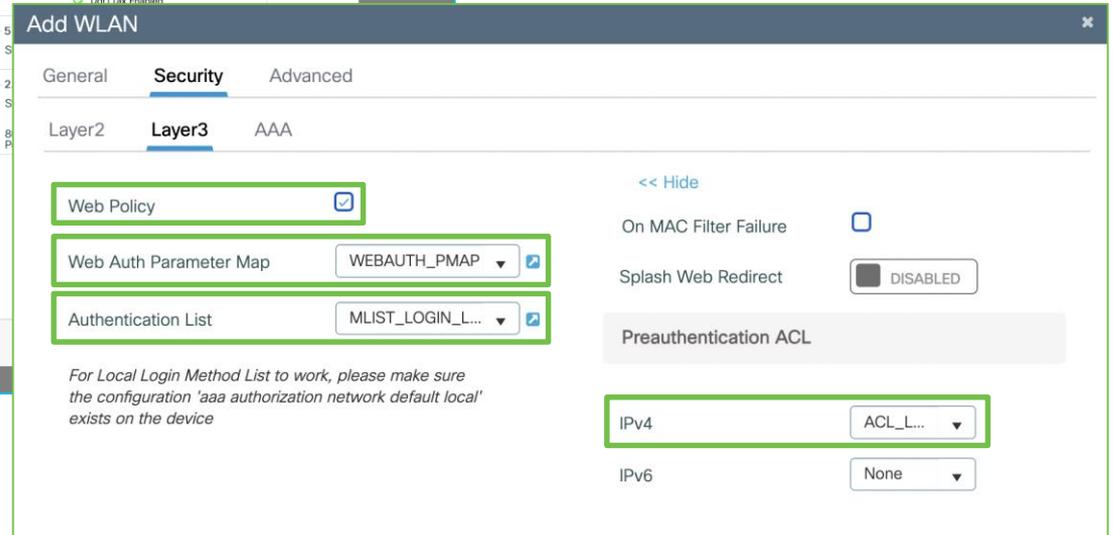
1. New guest WLAN with no L2 security (i.e., fully open)

# Adding a Guest SSID (LWA with internal portal)

Configuration > Security > Web Auth



1. New guest WLAN with no L2 security (i.e., fully open)
2. L3 security as Web Policy, pointing to our Web Auth Parameter Map, with an authC method list for general login and our ACL too



# Adding a Guest SSID (LWA with internal portal)

Configuration > Tags & Profiles > WLANs

1. New guest WLAN with no L2 security (i.e., fully open)
2. L3 security as Web Policy, pointing to our Web Auth Parameter Map, with an authC method list for local login and our ACL too
3. As a recommendation, we block P2P traffic too

# Adding a Guest SSID (LWA with internal portal)

Configuration > Tags & Profiles > Policy

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The main window is titled 'Add Policy Profile' and contains a warning message: 'Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.' The 'General' tab is selected, showing the following configuration options:

- Name\*: POLICY\_PRFL\_GUEST
- Description: Enter Description
- Status: ENABLED
- Passive Client: DISABLED
- IP MAC Binding: ENABLED
- Encrypted Traffic Analytics: DISABLED

The 'WLAN Switching Policy' section includes:

- Central Switching: ENABLED
- Central Authentication: ENABLED
- Central DHCP: ENABLED
- Flex NAT/PAT: DISABLED

The 'CTS Policy' section includes:

- Inline Tagging:
- SGACL Enforcement:
- Default SGT: 2-65519

Buttons at the bottom include 'Cancel' and 'Apply to Device'.

We create our guest Policy Profile with its dedicated VLAN

# Adding a Guest SSID (LWA with internal portal)

Configuration > Tags & Profiles > Policy

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The main window displays the 'Add Policy Profile' dialog box with the 'General' tab selected. The 'Name\*' field is set to 'POLICY\_PRFL\_GUEST'. The 'Status' is 'ENABLED'. The 'Default SGT' is '2-65519'. A warning message at the top of the dialog states: 'Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.'

We create our guest Policy Profile with its dedicated VLAN

The screenshot shows the 'Add Policy Profile' dialog box with the 'Access Policies' tab selected. The 'WLAN ACL' section has 'IPv4 ACL' and 'IPv6 ACL' both set to 'Search or Select'. The 'WLAN Local Profiling' section has 'Global State of Device Classification' set to 'Search or Select'. The 'VLAN' section has 'VLAN/VLAN Group' set to 'VLAN\_GUEST' and 'Multicast VLAN' set to 'default'. A warning message at the top of the dialog states: 'Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.'

# Configuring the Policy Profile

Configuration > Tags & Profiles > Policy

**Add Policy Profile**

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

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

**WLAN Timeout**

Session Timeout (sec)  ⓘ

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

**DHCP**

IPv4 DHCP Required

DHCP Server IP Address

Fabric Profile  Search or Select

Link-Local Bridging

mDNS Service Policy Search or Select

Hotspot Server Search or Select

**User Defined (Private) Network**

Status

Drop Unicast

**DNS Layer Security**

DNS Layer Security Parameter Map Not Configured Clear

**Policy Proxy Settings**

ARP Proxy **ENABLED**

IPv6 Proxy None

To avoid too many reauthentications

For increased security/control

For increased security/control

# Assign the WLAN Profile to the Policy Profile

Configuration > Tags & Profiles > Tags

Here we can reuse our existing Policy Tags, so that APs will automatically start broadcasting the guest SSID as soon as we add it to the Policy Tag with its corresponding Policy Profile

The image displays two screenshots of the Cisco Catalyst 9800-L Wireless Controller configuration interface, illustrating the process of assigning a WLAN Profile to a Policy Profile for a Policy Tag.

**Top Screenshot:** The interface shows the "Edit Policy Tag" configuration for "POLICY\_TAG\_CORP". The "WLAN-POLICY Maps" section is expanded, showing a table with two entries:

WLAN Profile	Policy Profile
<input type="checkbox"/> WLAN_PRFL_GUEST	POLICY_PRFL_GUEST
<input type="checkbox"/> WLAN_PRFL_EMPLOYEE	POLICY_PRFL_EMPLOYEE

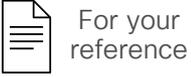
The "WLAN\_PRFL\_GUEST" entry is highlighted with a blue box, indicating it is selected for assignment.

**Bottom Screenshot:** The interface shows the "Edit Policy Tag" configuration for "POLICY\_TAG\_BRANCH". The "WLAN-POLICY Maps" section is expanded, showing a table with two entries:

WLAN Profile	Policy Profile
<input type="checkbox"/> WLAN_PRFL_GUEST	POLICY_PRFL_GUEST
<input type="checkbox"/> WLAN_PRFL_EMPLOYEE	POLICY_PRFL_EMPLOYEE_FLEX

The "WLAN\_PRFL\_GUEST" entry is highlighted with a blue box, indicating it is selected for assignment.

# Additional references for Guest WLANs

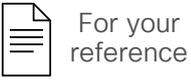


BRKEWN-2284

Becoming a Wi-Fi Guest star:  
Better Practices for Guest Networks on Cisco Catalyst Wireless

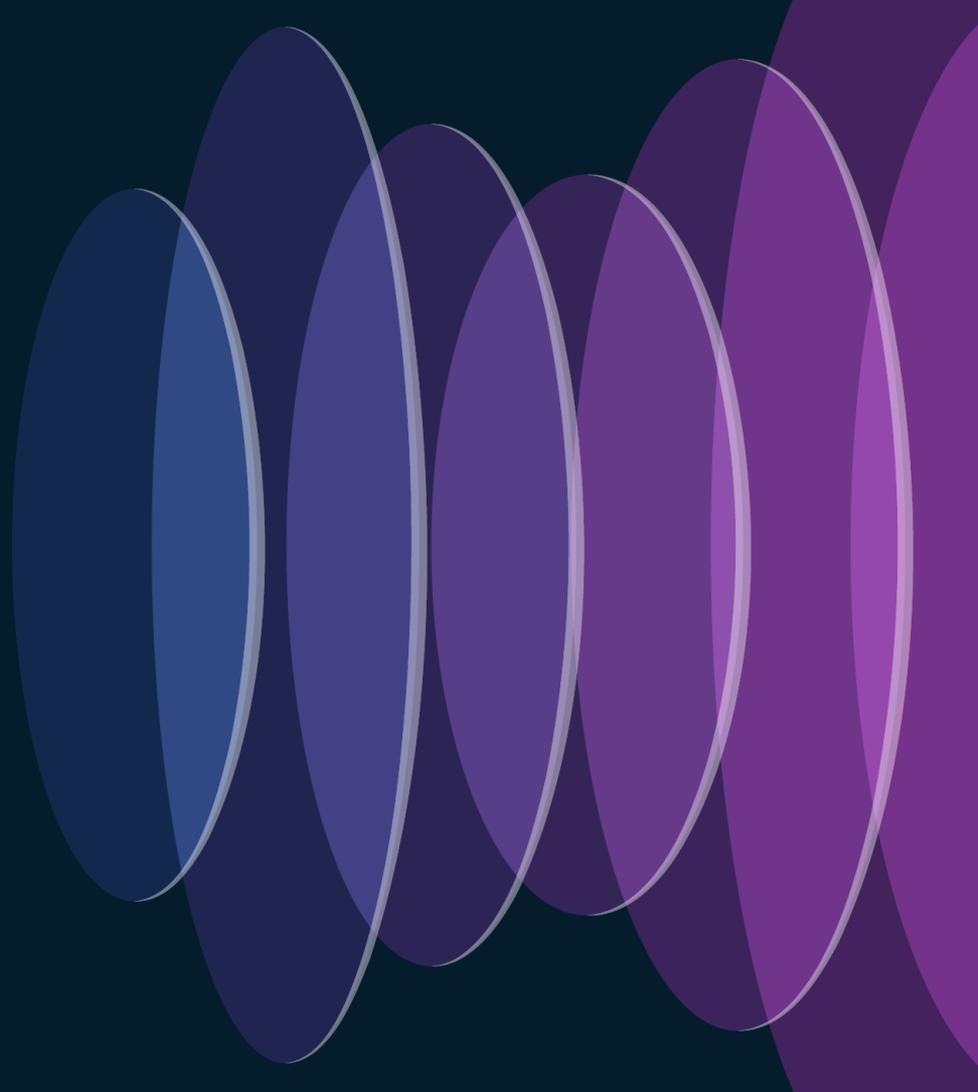
<https://www.ciscolive.com/on-demand/on-demand-library.html?#/session/1675722373660001tDKB>

# Additional references for Guest WLANs



- Web Auth Bundle example with customizable portals  
<https://software.cisco.com/download/home/286322605/type/282791507/release/16.10.1>
- Customize the Web Authentication Portal on Catalyst 9800 WLC  
<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/216121-custom-web-authentication-on-catalyst-98.html>
- Configure 9800 WLC Lobby Ambassador with RADIUS and TACACS+ Authentication  
<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/215552-9800-wlc-lobby-ambassador-with-radius-an.html>
- Configure and Troubleshoot External Web-Authentication on 9800 WLC  
<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/217457-configure-and-troubleshoot-external-web.html>
- Configure DNA Spaces Captive Portal with Catalyst 9800 WLC  
<https://www.cisco.com/c/en/us/support/docs/wireless/dna-spaces/215423-dna-spaces-captive-portal-with-9800-cont.html>
- Configure Central Web Authentication (CWA) on Catalyst 9800 WLC and ISE  
<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213920-central-web-authentication-cwa-on-cata.html>
- Configure Central Web Authentication with Anchor on Catalyst 9800  
<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/216500-catalyst-9800-central-web-authenticati.html>
- Configure FlexConnect with Authentication on Catalyst 9800 WLC  
<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213921-flexconnect-configuration-with-central-a.html>

# Further tweaks

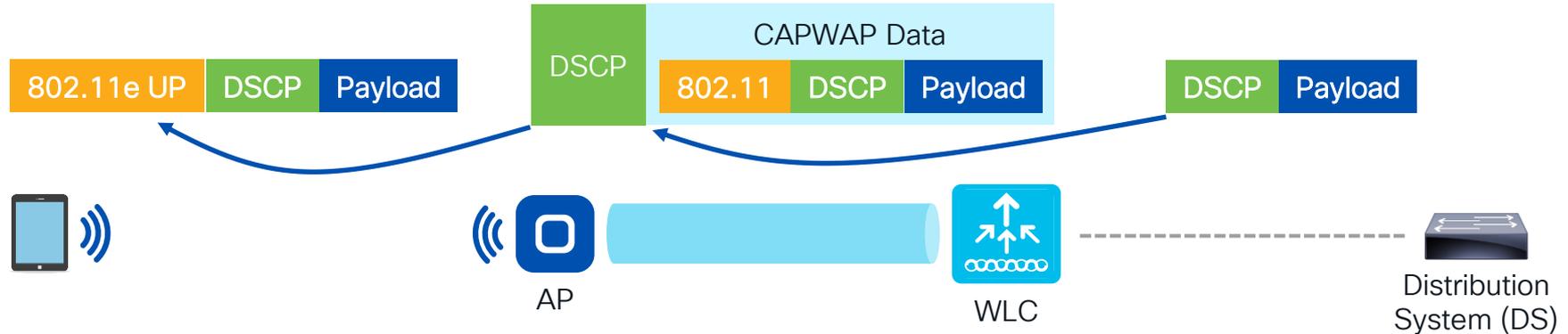


# QoS – Trust DSCP Upstream: the one to start with

As of IOS-XE 17.4.1 it is always enabled by default, but if not:

 For your reference

```
ap profile <AP_JOIN_PROFILE_NAME>  
  qos-map trust-dscp-upstream
```



Downstream: the original DSCP value from the DS (Distribution System) is preserved; the same DSCP value is used to mark the CAPWAP data tunnel, then translated to the 802.11e UP value in the 802.11 header. (assuming no remarking is applied at the WLC level)

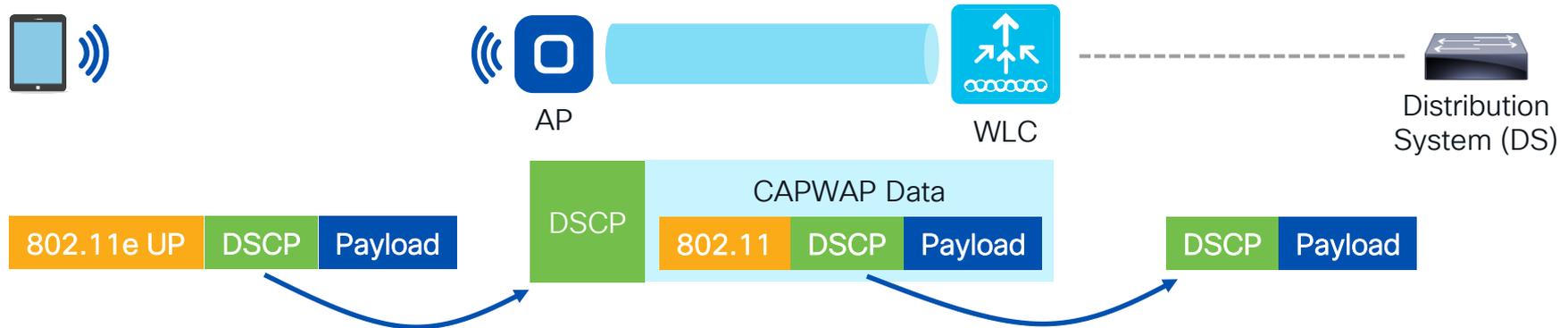
# QoS – Trust DSCP Upstream: the one to start with

As of IOS-XE 17.4.1 it is always enabled by default, but if not:

 For your reference

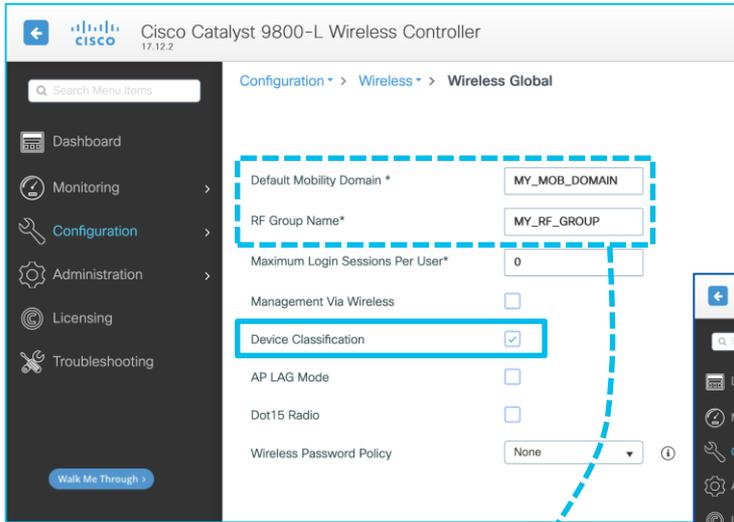
```
ap profile <AP_JOIN_PROFILE_NAME>  
  qos-map trust-dscp-upstream
```

Upstream: the 802.11e UP value from the endpoint (if any) is ignored; the original DSCP value is used to mark the CAPWAP data tunnel too, then preserved all the way up to the DS.  
(assuming no remarking is applied at the WLC level)



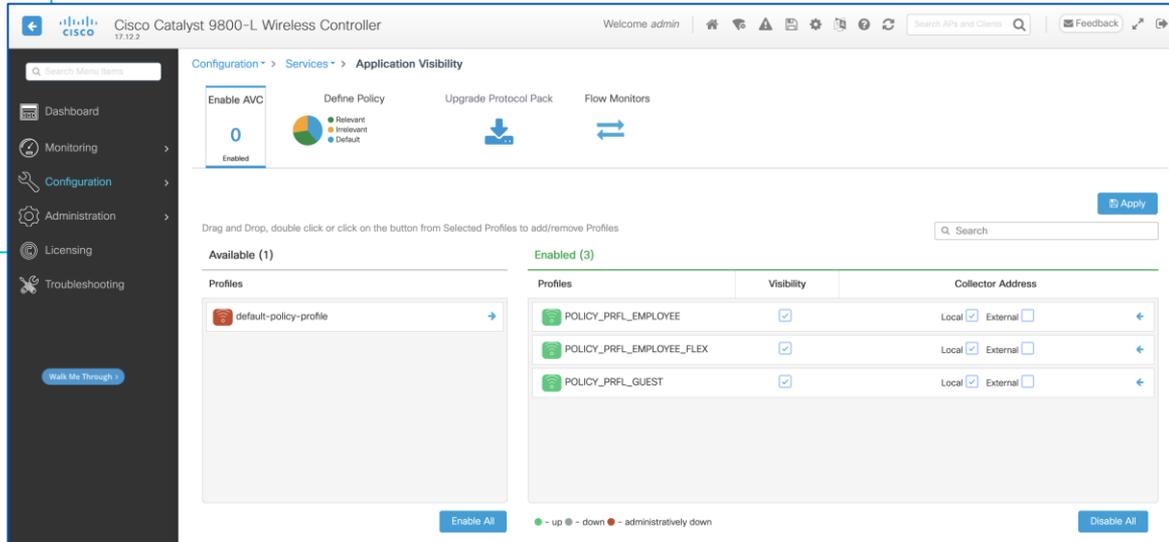
# Devices and applications visibility

Configuration > Wireless > Wireless Global



- ✎ Application visibility (and control) is done at the WLC level (downstream and upstream) for central switching, and at the AP level for FlexConnect local switching
- ✎ If the same WLAN Profile is linked to different Policy Profiles, these Policy Profiles must have the same central or local switching settings and the same flow monitor

Configuration > Services > Application Visibility



Especially during a PoC/test, we may want to keep the mobility domain and the RF group names unique, so that they do not match and interact with those already in production (unless needed)

# If not already enabled, let's turn on CleanAir

Configuration > Radio Configurations > CleanAir

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration page. The breadcrumb navigation is Configuration > Radio Configurations > CleanAir. The 6 GHz Band is selected. Under the General tab, the following options are checked: Enable CleanAir and Report Interferers. The Available Interference Types list is empty.

For high density environments we can avoid BT detection to optimize logs/operations

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration page for the 5 GHz Band. Under the General tab, the following options are checked: Enable CleanAir and Report Interferers. The Interference Types to detect list includes: TDD Transmitter, Jammer, Continuous Transmitter, DECT-like Phone, and Video Camera.

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration page for the 2.4 GHz Band. Under the General tab, the following options are checked: Enable CleanAir and Report Interferers. In the Available Interference Types list, Bluetooth Discovery and Bluetooth Link are selected and highlighted with an orange box. An orange arrow points from the text above to this box. The Interference Types to detect list includes: TDD Transmitter, Jammer, Continuous Transmitter, DECT-like Phone, and Video Camera.

# Energy efficiency

Configuration > Tags & Profiles > Power Profile (i.e., what the APs should do)

While X (or more) clients are connected, the AP does not apply the Power Profile

**Add Power Profile**

Name\* PWR\_PRFL\_1G\_1X1

Description Enter Description

Power Save Client Threshold 3

Rule

Sequence number\* 4

Interface Radio Parameter Spatial Stream

Interface ID 6 GHz Parameter value 1x1

Sequence	Interface	Interface ID	Parameter	Parameter Value
<input type="checkbox"/> 0	Ethernet	GigabitEthernet0	Speed	1000 MBPS
<input type="checkbox"/> 1	Radio	2.4 GHz	Spatial Stream	1x1
<input type="checkbox"/> 2	Radio	5 GHz	Spatial Stream	1x1
<input type="checkbox"/> 3	Radio	Secondary 5 GHz	Spatial Stream	1x1

Example of a Power Profile for lower consumption:

- Ethernet = 1 Gbps
- 2.4 GHz radio = 1x1\*
- 5 GHz radio(s) = 1x1\*
- 6 GHz radio = 1x1\*

\* The Spatial Stream option under the Power Profile was introduced in IOS-XE 17.10.1, hence today we need at least IOS-XE 17.12.x

# Energy efficiency

Configuration > Tags & Profiles > Calendar (i.e., when the APs should do it)

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation is Configuration > Tags & Profiles > Calendar. A modal dialog titled 'Add Calendar Profile' is open, displaying the following configuration:

- Name\*:** CALENDAR\_PRFL\_NIGHT
- Recurrence:** Daily
- Start Time:** 22:00:00
- End Time:** 06:00:00

A notification message at the top of the dialog states: "This profile will be in effect at 22:00:00 and has a duration of 08:00:00 which extends to next day ending at 06:00:00". The dialog includes 'Cancel' and 'Apply to Device' buttons.

Example of a Calendar Profile for non-working hours:

- Daily
- 10pm to 6am

# Energy efficiency

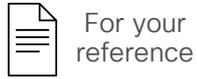
Configuration > Tags & Profiles > AP Join > (Edit AP Join Profile) > AP > Power Management

The screenshot displays the Cisco Catalyst 9800-L Wireless Controller configuration interface. The main navigation pane on the left includes Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The breadcrumb trail indicates the path: Configuration > Tags & Profiles > AP Join. The 'Edit AP Join Profile' window is open, showing the 'Power Management' tab. Under the 'Calendar Profile - Power Profile Map' section, a calendar profile is configured with a recurrence of 'Daily', a start time of 22:00:00, and an end time of 06:00:00. The power profile is detailed with a table of parameters for various interfaces.

Sequence	Interface	Interface ID	Parameter	Parameter Value
0	Ethernet	GigabitEthernet0	Speed	1000 MBPS
1	Radio	2.4 GHz	Spatial Stream	1x1
2	Radio	5 GHz	Spatial Stream	1x1
3	Radio	Secondary 5 GHz	Spatial Stream	1x1
4	Radio	6 GHz	Spatial Stream	1x1

Under the “Calendar Profile – Power Profile Map” of the AP Join Profile, we can then link our Calendar Profile(s) with the wanted Power Profile(s)

# AP Join Profile optimizations

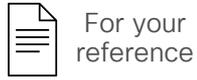


Configuration > Tags & Profiles > AP Join (General tab)

The screenshot shows the 'Edit AP Join Profile' configuration page. The 'Country Code' is set to 'NL' and the 'Time Zone' is set to 'Not Configured'. A blue dashed box highlights these two fields, with an arrow pointing to the text on the right. Other settings include 'Local Access', 'Link Encryption', 'Rogue Detection', 'Provisioning SSID', 'Antenna Monitoring', 'RSSI Fail Threshold', 'Weak RSSI', and 'Detection Time'.

Not always mandatory for APs to work, but generally recommended to set the Country Code, as well as the Time Zone (often “Use-Controller”) for consistency and troubleshooting

# AP Join Profile optimizations



Configuration > Tags & Profiles > AP Join (Management > Device/User tabs)

By default APs send syslog messages to 255.255.255.255  
This could cause unwanted broadcast traffic, especially when demultiplied by many APs. It is highly recommended to set the syslog server IP for APs to a real one, or even to a bogus one if not used.

Enabling SSH (and configuring the User account) is highly recommended for additional troubleshooting options

# Just a more custom technique

- These first steps could kick start PoC's and initial deployments with some solid basis
- Although not an automated approach, it lets us maintain detailed control on what we are configuring
- An optimized “master” configuration could then massively be deployed through faster centralized orchestration tools
- Our mileage may vary according to many other deployment-specific factors



# Some suggestions on where to go next



- Any “BRKEWN” session
- BRKEWN-2339  
Catalyst 9800 Configuration Best Practices
- IBOEWN-2031  
The Inner Workings of QoS for Modern Wireless Networks
- BRKEWN-2043  
Saving Energy and Money with Your Cisco Wireless Network
- BRKEWN-3413  
Advanced RF Tuning for Wi-Fi 6E with Catalyst Wireless: Become an Expert, while getting a little help from AI
- BRKEWN-3628  
Troubleshoot Catalyst 9800 Wireless Controllers
- BRKEWN-3002  
Make a Wireless Engineer’s Life Easy by Using Automation to Troubleshoot and Analyze Logs

# Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

---



**Earn 100 points** per survey completed and compete on the Cisco Live Challenge leaderboard.

---



Level up and earn **exclusive prizes!**

---



Complete your surveys in the **Cisco Live mobile app**.

# Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at [www.CiscoLive.com/on-demand](https://www.CiscoLive.com/on-demand)



The bridge to possible

# Thank you

CISCO *Live!*

#CiscoLive