

The background features a vibrant, abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, green, and yellow, creating a sunburst effect.

CISCO *Live!*

Let's go

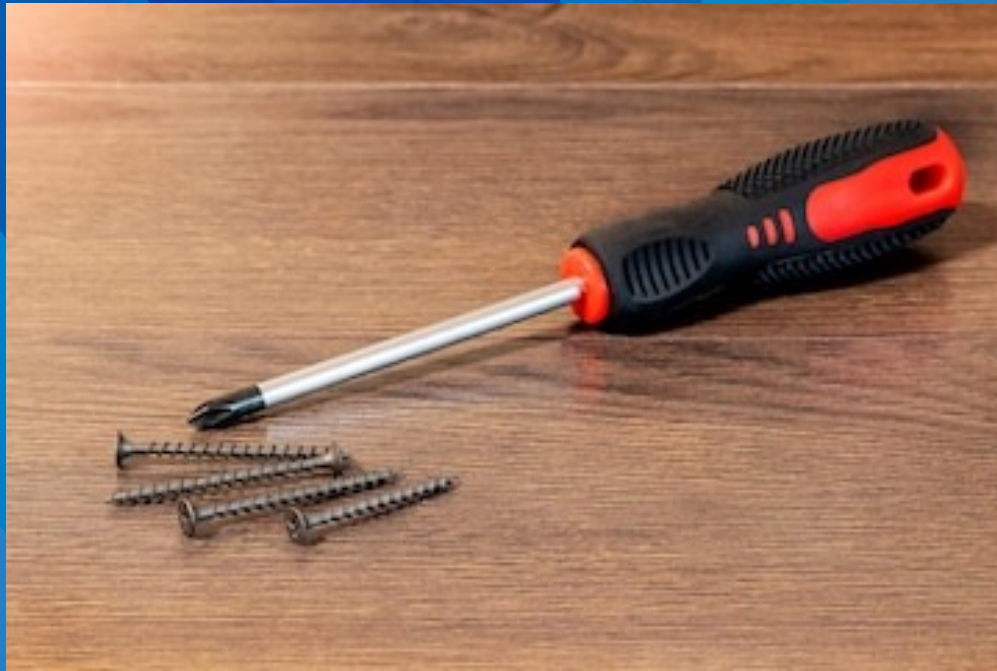


The bridge to possible

# Successfully Configuring Catalyst 9800 Wireless on Your First Shot

Federico Ziliotto, Technical Solutions Architect  
CCIE – 23280 (Wireless, R&S)

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

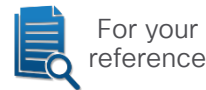


# Federico → Fede

- ~17 years at 
  - 4 years as a Customer Support Engineer (CSE)
  - 3 years as a Specialized Systems Engineer
  - 5 years as a Consulting Systems Engineer (CSE)
  - ~5 year as a Technical Solutions Architect (TSA)
- Always focused on Wireless and NAC



# 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”



# Webex App

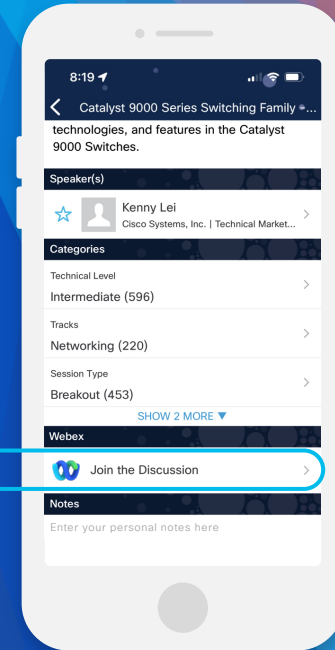
## Questions?

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

## How

- 1 Find this session in the Cisco Events 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 February 23, 2024.



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

# 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)#
```

# 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
```



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

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.>
```

# 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”

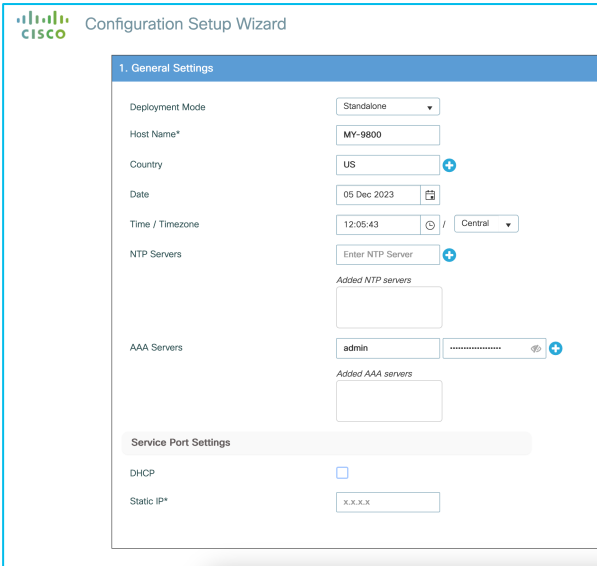
To avoid “stale” SSH/HTTPS sessions

For easier troubleshooting logs/debugs

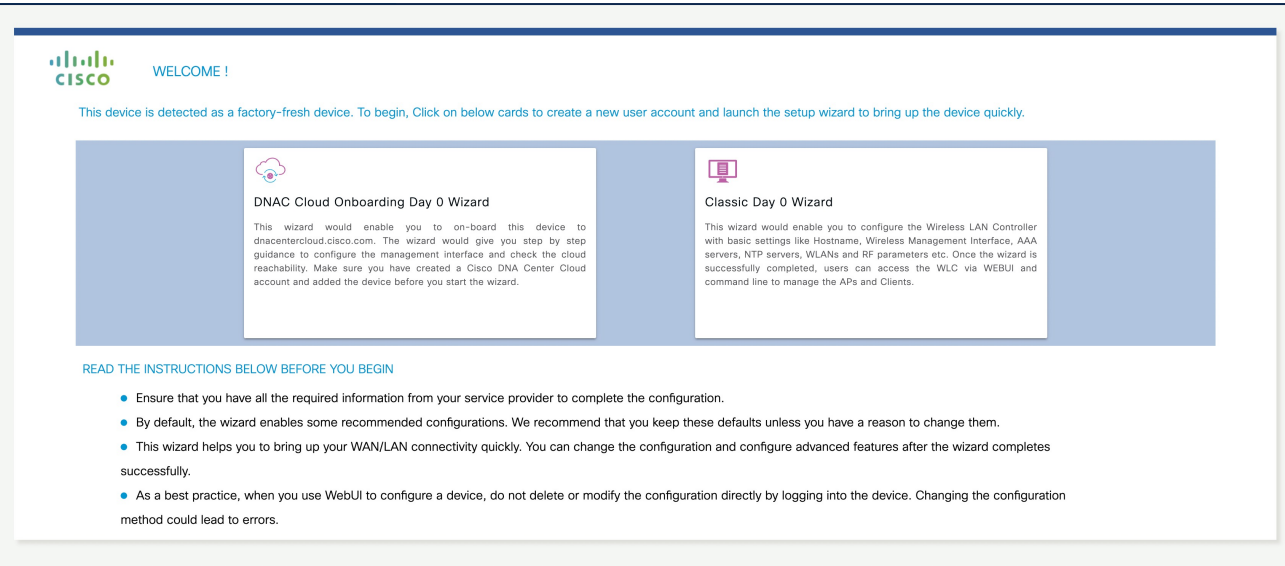
To increase the “consistency” of GUI access, we can fix a trustpoint (to keep it simple, it could be the same as the WMI), as well as a source interface, for all HTTPS admin traffic

# 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 image shows the 'Configuration Setup Wizard' for a Cisco device. The '1. General Settings' tab is active. It contains several configuration fields: 'Deployment Mode' is set to 'Standalone'; 'Host Name\*' is 'MY-9800'; 'Country' is 'US' with a plus icon; 'Date' is '05 Dec 2023' with a calendar icon; 'Time / Timezone' is '12:05:43' with a clock icon and a 'Central' dropdown; 'NTP Servers' has an 'Enter NTP Server' button and a plus icon; 'AAA Servers' has an 'admin' username, a masked password, and a plus icon. Below these are 'Service Port Settings' including 'DHCP' (unchecked) and 'Static IP\*' (x.x.x.x).



The image shows the 'WELCOME !' screen of the Cisco Day-0 Wizard. It features the Cisco logo and 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 main cards: 'DNAC Cloud Onboarding Day 0 Wizard' and 'Classic Day 0 Wizard'. Below the cards, there is a section titled 'READ THE INSTRUCTIONS BELOW BEFORE YOU BEGIN' with three bullet points: 1. Ensure that you have all the required information from your service provider to complete the configuration. 2. By default, the wizard enables some recommended configurations. We recommend that you keep these defaults unless you have a reason to change them. 3. 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. 4. 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

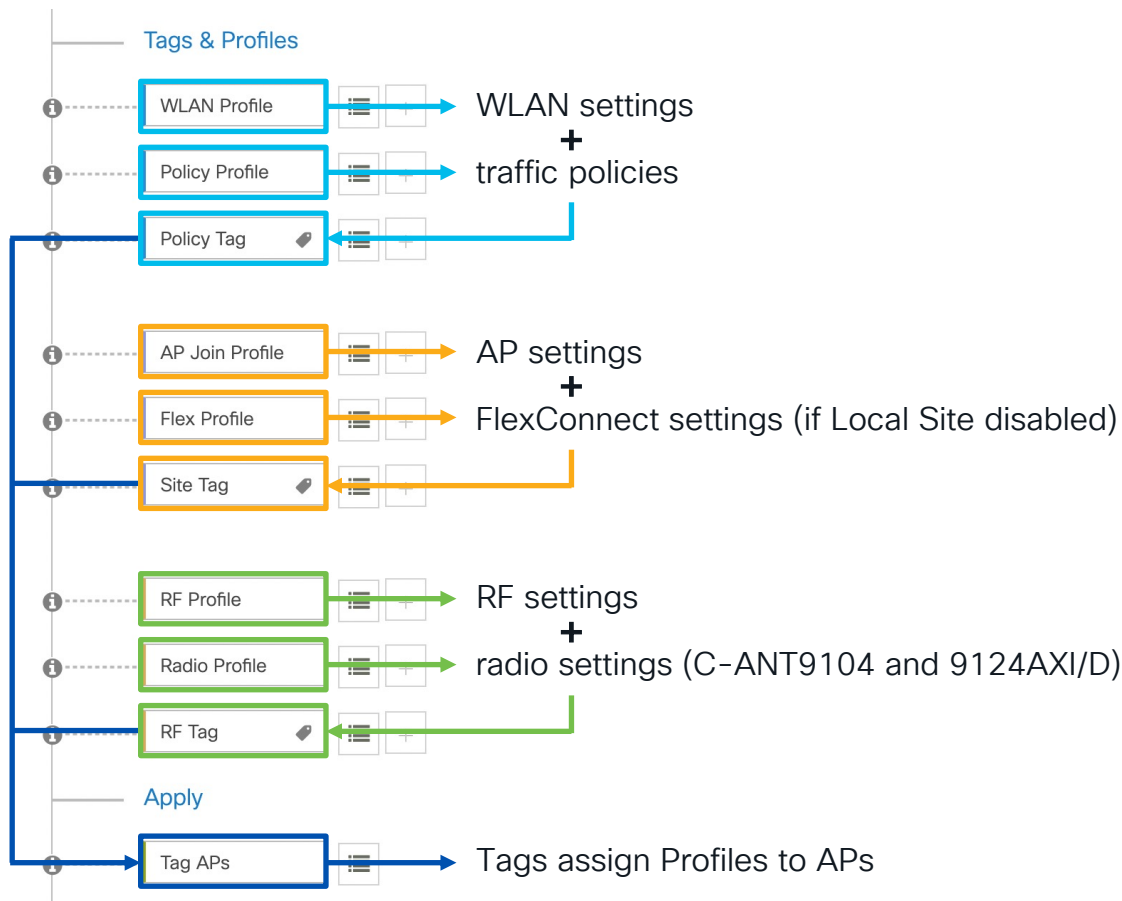
# Profiles and Tags: the main configuration objects

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)

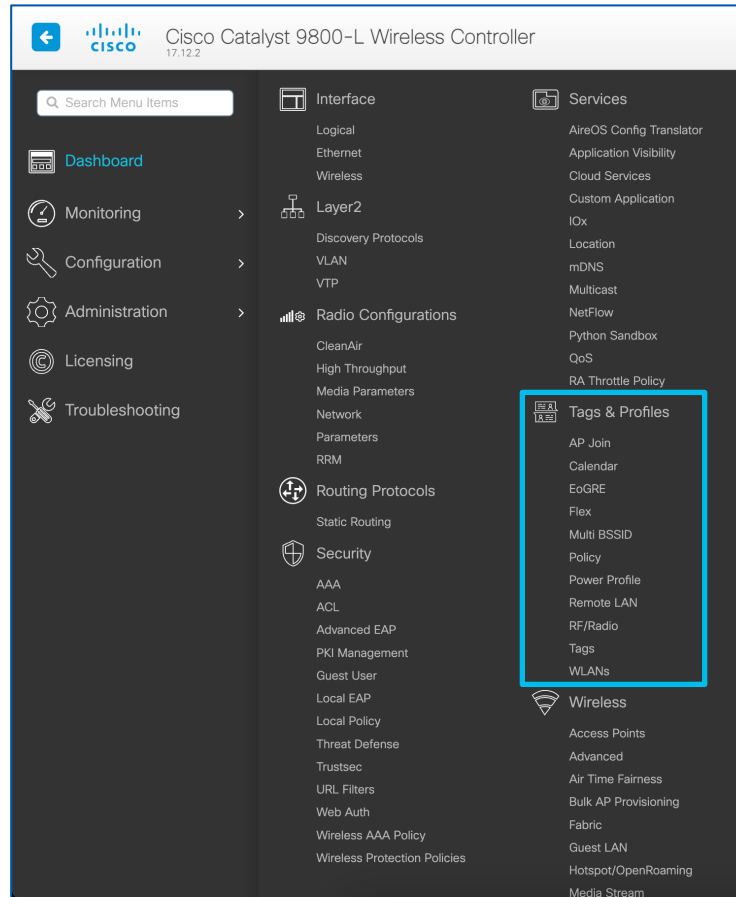
# Profiles and Tags: the main configuration objects

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 VLAN tab is selected, showing a table of configured VLANs. The table has columns for VLAN ID, Name, Status, and Ports. The VLANs listed are 1 (default), 10 (VLAN\_WIRELESS\_MGMT), 110 (VLAN\_EMPLOYEE), 120 (VLAN\_VOICE), and 130 (VLAN\_GUEST). All VLANs are in an 'active' status. The interface also includes a sidebar with navigation options like Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting.

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 titled 'Create AAA Radius Server' is open, allowing for the configuration of a new RADIUS server. The dialog contains the following fields and options:

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

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 > Add RADIUS Server Group. The left sidebar shows the navigation menu with options like Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area shows the 'Create AAA Radius Server Group' dialog box with the following fields:

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

Below these fields are two sections: 'Available Servers' (empty) and 'Assigned Servers' (containing RADIUS\_SRVR\_ISE). Navigation arrows are present between these sections. At the bottom of the dialog 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 shows 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 'Quick Setup: AAA Authentication' dialog box is open, displaying the following configuration details:

- 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 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

1 - 3 of 3 items

# 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 left sidebar contains navigation links: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled 'Configuration > Security > AAA'. A 'Quick Setup: AAA Authorization' dialog box is open, displaying the following fields:

- 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 at the bottom of the dialog include 'Cancel' and 'Apply to Device'. In the background, a table shows configuration for Group3 and Group4:

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

Page 1 - 2 of 2 items

Mainly used for MAC filtering based WLANs

# Configuring a AAA Method List for accounting

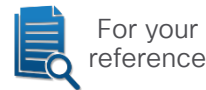
Configuration > Security > AAA > AAA Method List > Accounting > Add (Type = identity)

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 'Quick Setup: AAA Accounting' dialog box is open, showing the following configuration:

- Method List Name\*: MLIST\_ACCT\_ID
- Type\*: identity
- Available Server Groups: radius, ldap, tacacs+
- Assigned Server Groups: RADIUS\_SRVR\_GRP\_01

The dialog box includes 'Cancel' and 'Apply to Device' buttons. The background interface shows the 'AAA Method List' configuration page with tabs for 'Servers / Groups', 'AAA Method List', and 'AAA Advanced'. The 'Accounting' tab is selected, and the 'Add' button is visible.

# 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 fields for Profile Name\* (WLAN\_PRFL\_EMPLOYEE), SSID\* (.:.: Employee), WLAN ID\* (1), Status (ENABLED), and Broadcast SSID (ENABLED). A 'Radio Policy' section shows 6 GHz, 5 GHz, and 2.4 GHz bands, all with 'ENABLED' status. The 6 GHz band has a red 'ENABLED' status with a warning icon and text indicating 'WPA3 Enabled' and 'Dot11ax Enabled'. The 5 GHz and 2.4 GHz bands also show 'ENABLED' status. A 'Show slot configuration' link is present. At the bottom, there are 'Cancel' and 'Apply to Device' buttons.

This screenshot shows the 'Security' tab of the 'Add WLAN' configuration page. It includes sections for 'Layer2', 'Layer3', and 'AAA'. Under 'Layer2', there are radio buttons for WPA + WPA2 (selected), WPA2 + WPA3, WPA3, Static WEP, and None. Below this are checkboxes for MAC Filtering and Lobby Admin Access. The 'WPA Parameters' section includes checkboxes for WPA Policy, WPA2 Policy (checked), GTK Randomize, and OSEN Policy. The 'WPA2 Encryption' section includes checkboxes for AES(CCMP128), CCMP256, GCMP128, and GCMP256. The 'Protected Management Frame' section has a dropdown for PMF set to 'Optional'. The 'Fast Transition' section includes a 'Status' dropdown set to 'Enabled', an 'Over the DS' checkbox, and a 'Reassociation Timeout \*' field set to 20. The 'Auth Key Mgmt' section includes checkboxes for 802.1x, Easy-PSK, FT + 802.1x, 802.1x-SHA256, PSK, CCKM (with a warning icon), FT + PSK, and PSK-SHA256.

This screenshot shows the 'AAA' tab of the 'Add WLAN' configuration page. It includes a section for 'Authentication List' with a dropdown menu showing 'MLIST\_AUTHC\_1' and a 'Select a value' button. Below this is a 'Local EAP Authentication' section with a dropdown menu showing 'MLIST\_AUTHC\_1X'. A green arrow points from the text 'The AAA Method List for dot1x authentication' to the 'MLIST\_AUTHC\_1X' option in the dropdown.

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

Association Comeback Timer\*

SA Query Time\*

**Fast Transition**

Status

Over the DS ☐

Reassociation Timeout \*

**Auth Key Mgmt**

802.1X ☒ PSK ☐  
Easy-PSK ☐ CKM ☐  
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

**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*

**Device Analytics**

Advertise Support: ☒

Advertise PC Analytics Support: ☒

Share Data with Client: ☒

**11ax**

Enable 11ax: ☒

Downlink OFDMA: ☒

Uplink OFDMA: ☒

Downlink MU-MIMO: ☒

Uplink MU-MIMO: ☒

BSS Target Wake Up Time: ☐

**11k Beacon Radio Measurement**

Client Scan Report

On Association: ☒

On Roam: ☒

- 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

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The 'Add Policy Profile' dialog box is open, displaying the 'General' tab. The 'Name\*' field is set to 'POLICY\_PRFL\_EMPLOYEE'. The 'Status' is set to 'ENABLED'. The 'WLAN Switching Policy' section is highlighted with a blue box, showing 'Central Switching', 'Central Authentication', and 'Central DHCP' all set to 'ENABLED'. The 'CTS Policy' section shows 'Inline Tagging' and 'SGACL Enforcement' as checkboxes, and 'Default SGT' as a text field with the value '2-65519'. A blue arrow points from the 'ENABLED' status to the text 'Policy Profile for central switching'. Another blue arrow points from the 'WLAN Switching Policy' section to the text 'As for a WLAN Profile, we need to explicitly enable it'.

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

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

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

☒

☒

☒

WLAN Local Profiling

Global State of Device Classification

Local Subscriber Policy Name

VLAN

VLAN/VLAN Group

Multicast VLAN

WLAN ACL

IPv4 ACL

IPv6 ACL

URL Filters

Pre Auth

Post Auth

VLAN\_EMPLOYEE

default

VLAN\_EMPLOYEE

VLAN\_GUEST

VLAN\_VOICE

VLAN\_WIRELESS\_MGMT

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

CISCO *Live!*

BRKEWN-2094

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

36

# 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)

86400

i

Idle Timeout (sec)

300

Idle Threshold (bytes)

0

Client Exclusion Timeout (sec)

☒

60

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

CISCO *Live!*

BRKEWN-2094

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

37

# 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

RADIUS



Policy Name

default-aaa-policy



Accounting List

MLIST\_ACCT\_ID



### WGB Parameters

Broadcast Tagging



WGB VLAN



### Policy Proxy Settings

ARP Proxy

ENABLED



IPv6 Proxy

None



### Advanced

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

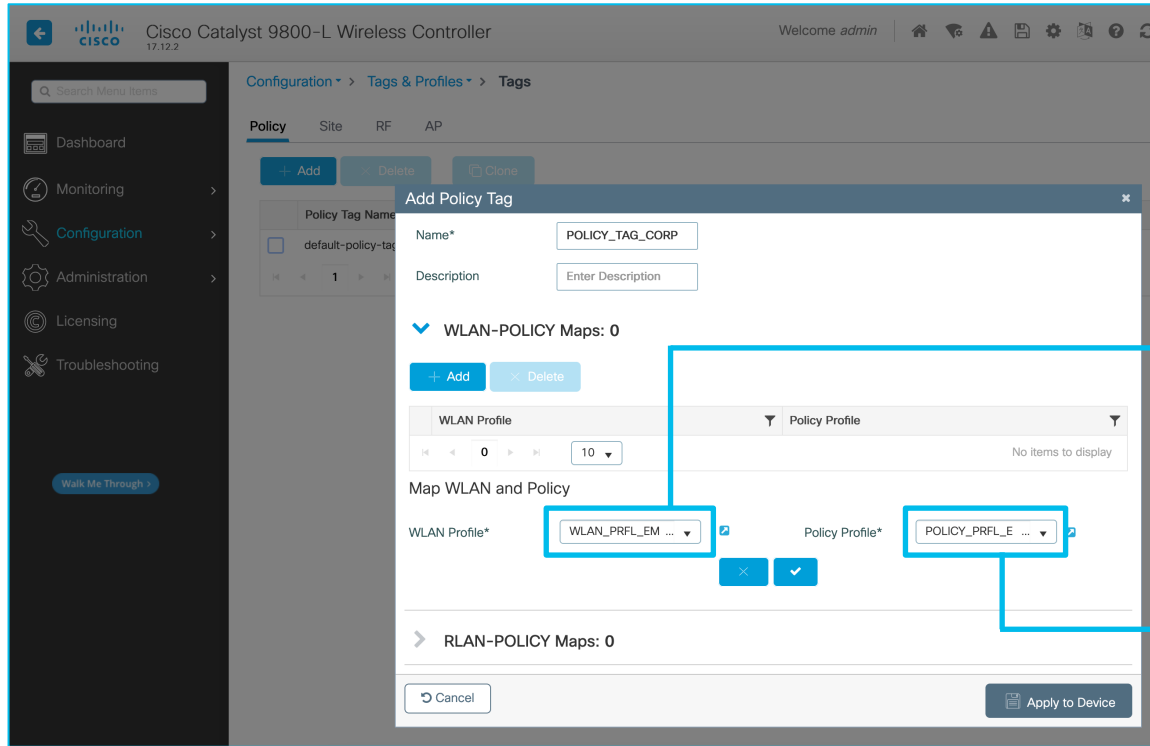
Not Configured



Clear

# Configuring the Policy Tag

Configuration > Tags & Profiles > Tags > Policy > Add



Policy Tag

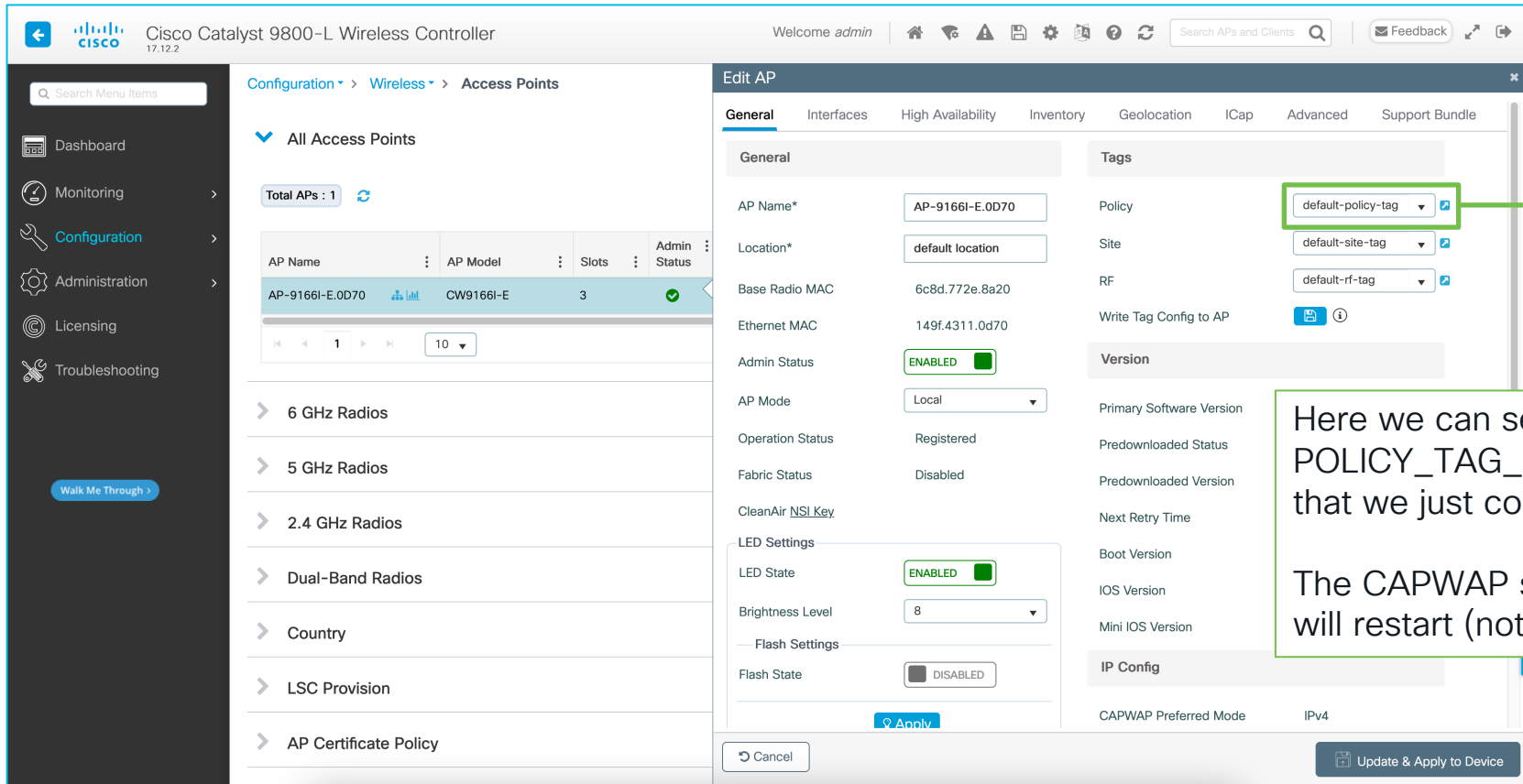
=

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 interface. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is divided into two panes. The left pane shows the 'All Access Points' list with a table of APs. The right pane shows the 'Edit AP' configuration for AP-9166I-E.0D70. The 'Tags' section is highlighted, and the 'Policy' dropdown menu is set to 'default-policy-tag'. A green box and arrow point to this dropdown menu. A text box explains that this tag is the POLICY\_TAG\_CORP tag configured previously, and that the CAPWAP service will restart (not a reload).

Configuration > Wireless > Access Points

▼ All Access Points

Total APs : 1

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

6 GHz Radios

5 GHz Radios

2.4 GHz Radios

Dual-Band Radios

Country

LSC Provision

AP Certificate Policy

Edit AP

General Interfaces High Availability Inventory Geolocation ICap Advanced Support Bundle

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

CleanAir NSI Key

LED Settings

LED State ENABLED

Brightness Level 8

Flash Settings

Flash State DISABLED

Tags

Policy default-policy-tag

Site default-site-tag

RF default-rf-tag

Write Tag Config to AP

Version

Primary Software Version

Predownloaded Status

Predownloaded Version

Next Retry Time

Boot Version

IOS Version

Mini IOS Version

IP Config


CAPWAP Preferred Mode IPv4

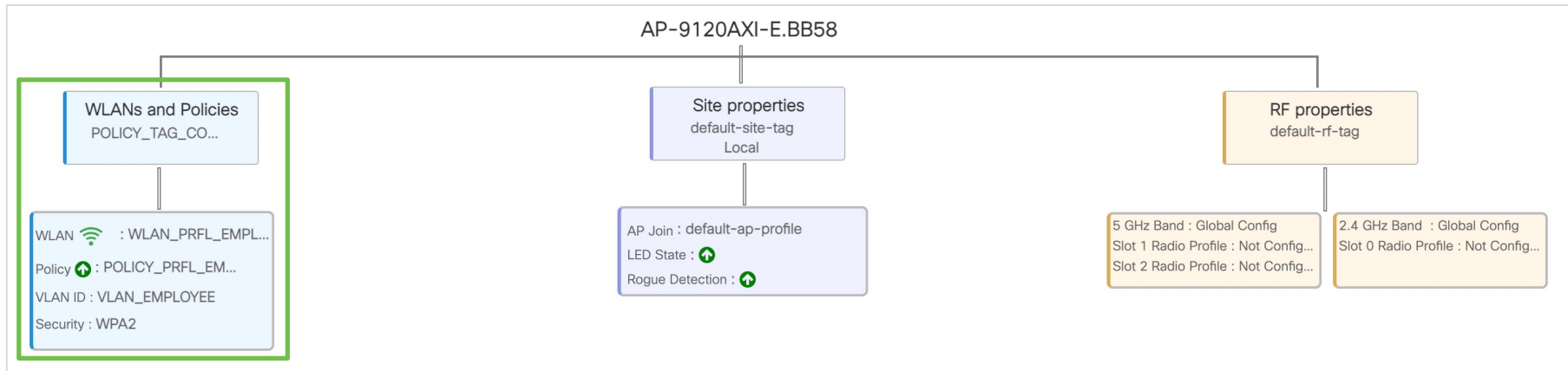
Update & Apply to Device

# Checking Tags and Profiles assignment

AP Name

AP-9166I-E.0D70





# Other options to assign Tags

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

The image displays the Cisco Catalyst 9800-L Wireless Controller configuration interface, specifically the 'Tags & Profiles > Tags > AP > Tag Source' section. The interface is divided into several panels and tabs.

**Tag Source Configuration:** The 'Tag Source' tab is active, showing a table of tag sources. The 'Static' source is highlighted in green, 'Location' in orange, and 'Filter' in blue. The table lists the following tag sources:

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"/>

Below the table, there are instructions: 'Drag and Drop Tag Sources to change priorities', 'Revalidate Tag Sources on APs', and 'Enable AP Tag Persistence'. An 'Apply' button is at the bottom.

**Associate Tags to AP:** This panel shows the configuration for associating tags to APs. It includes fields for 'Rule Name\*' (FILTER\_CORP), 'AP name regex\*' (^AP-.\*), 'Active' (YES), and 'Priority\*' (1023). It also has dropdowns for 'Policy Tag Name' (POLICY\_TAG\_CO...), 'Site Tag Name' (default-site-tag), and 'RF Tag Name' (default-rf-tag).

**Create Location and associate APs:** This panel shows the configuration for creating a location and associating APs. It includes fields for 'Location\*' (LOC\_CORP), 'Description' (Enter Description), 'Policy Tag Name' (POLICY\_TAG\_CO...), 'Site Tag Name' (default-site-tag), and 'RF Tag Name' (default-rf-tag).

**AP Provisioning:** This panel shows the configuration for AP provisioning. It includes fields for 'Import AP MAC' (Select File), 'AP MAC Address', and 'Available AP list'. The 'Available AP list' shows a table of APs:

AP MAC	AP Name
149f.4311.0d70	AP-9166f-E.0D70

Below the table, there are instructions: 'Number of selected APs: 0', 'No items to display', and a '500' dropdown.

**Through a "Location" or group of APs:** This panel shows the configuration for associating tags to APs through a location or group of APs. It includes fields for 'Tag Source' (Static), 'Location' (LOC\_CORP), 'Policy Tag Name' (POLICY\_TAG\_CO...), 'Site Tag Name' (default-site-tag), and 'RF Tag Name' (default-rf-tag). It also has a table of APs:

AP MAC Address	Policy Tag Name	Site Tag Name	RF Tag Name
149f.4311.0d70	POLICY_TAG_CORP	default-site-tag	default-rf-tag

Below the table, there are instructions: 'Number of AP Tag mappings selected: 0', '1' dropdown, and a '10' dropdown.

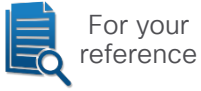
**Through regex rules for the AP names:** This panel shows the configuration for associating tags to APs through regex rules for the AP names. It includes fields for 'Rule Name\*' (FILTER\_CORP), 'AP name regex\*' (^AP-.\*), 'Active' (YES), and 'Priority\*' (1023). It also has dropdowns for 'Policy Tag Name' (POLICY\_TAG\_CO...), 'Site Tag Name' (default-site-tag), and 'RF Tag Name' (default-rf-tag).

**Manually or through a CSV file:** This panel shows the configuration for associating tags to APs manually or through a CSV file. It includes fields for 'Tag Source' (Static), 'Location' (LOC\_CORP), 'Policy Tag Name' (POLICY\_TAG\_CO...), 'Site Tag Name' (default-site-tag), and 'RF Tag Name' (default-rf-tag). It also has a table of APs:

AP MAC Address	Policy Tag Name	Site Tag Name	RF Tag Name
149f.4311.0d70	POLICY_TAG_CORP	default-site-tag	default-rf-tag

Below the table, there are instructions: 'Number of AP Tag mappings selected: 0', '1' dropdown, and a '10' dropdown.

# Enabling Tags persistency



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

←

Cisco Catalyst 9800-L Wireless Controller  
17.12.2

Welcome admin

Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Licensing

Troubleshooting

Walk Me Through >

Configuration > Tags & Profiles > Tags

Policy Site RF **AP**

Tag Source

StaticLocationFilter

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** ☒

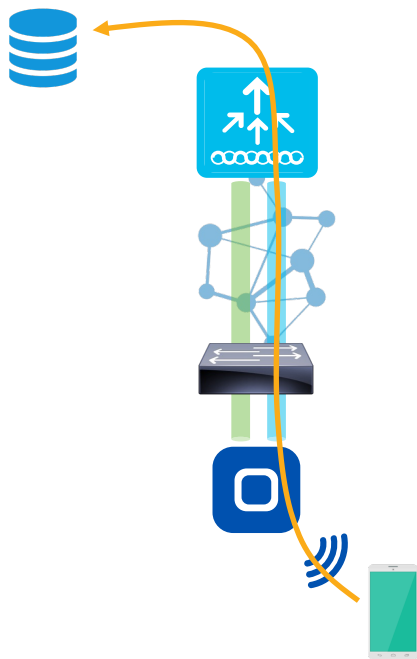
Apply

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

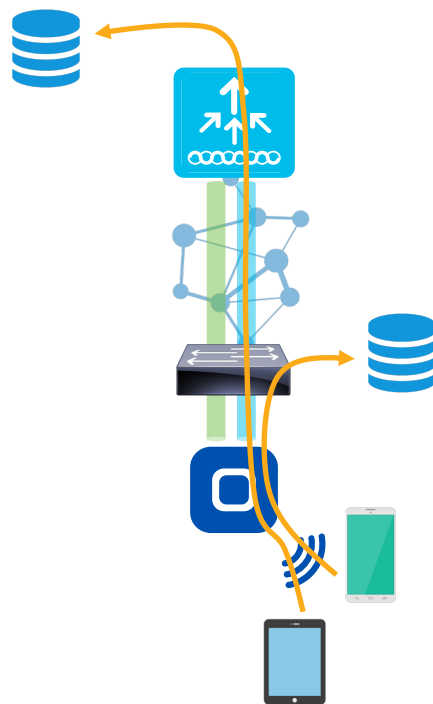
The same Tags must be present on the new destination controller and they are applied according to the AP's memory if no other mappings (static, filter, etc.) supersede them


# 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

Configuration > Tags & Profiles > Tags

Policy Site RF AP

+ Add × Delete Clone Reset APs

Site Tag Name

default-site-tag

1 10

Edit Site Tag

Name\* default-site-tag

Description default site tag

AP Join Profile default-ap-profile

Fabric Control Plane Name

Enable Local Site ☒

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

Name\* default-site-tag

Description default site tag

AP Join Profile default-ap-profile

Flex Profile default-flex-profile

Fabric Control Plane Name

Enable Local 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 configuration page. The breadcrumb navigation at the top reads: Configuration > Tags & Profiles > Tags. The 'Site' tab is selected under the 'Tags & Profiles' section. A modal dialog titled 'Add Site Tag' is open, showing the following fields:

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

Buttons at the bottom of the dialog include 'Cancel' and 'Apply to Device'. The background interface shows a sidebar with navigation options like Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting.

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 configuration interface. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main configuration area is titled 'Configuration > Wireless > Access Points' and shows 'All Access Points' with a table listing APs. The selected AP is 'AP-9166I-E.0D70'. The right pane shows the 'Edit AP' configuration for this AP, with tabs for General, Interfaces, High Availability, Inventory, Geolocation, ICap, Advanced, and Support Bundle. The 'General' tab is active, showing fields for AP Name, Location, Base Radio MAC, Ethernet MAC, Admin Status (ENABLED), AP Mode (Local), Operation Status (Registered), and Fabric Status (Disabled). A 'Tags' section on the right shows a warning about changing tags and a dropdown menu for selecting a tag, with 'SITE\_TAG\_BRANCH' selected.

## 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



Cisco Catalyst 9800-L Wireless Controller

Welcome admin

Configuration > Tags & Profiles > Tags

Policy Site RF AP

Tag Source Static Location Filter

+ Add - Delete

Associate Tags to AP

Rule Name\* RULE\_FLEX\_DEFAULT

AP name regex\* .\*

Active YES

Priority\* 1023

Policy Tag Name Search or Select

Site Tag Name SITE\_TAG\_BRAN .x

RF Tag Name Search or Select

Cancel Apply to Device

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' dialog in the Cisco Catalyst 9800-L Wireless Controller configuration interface. The 'General' tab is selected, and the 'WLAN Switching Policy' section is highlighted with a red box. The 'Central Switching' and 'Central DHCP' options are set to 'DISABLED', while 'Central Authentication' is set to 'ENABLED'. The 'CTS Policy' section is also visible, with 'Inline Tagging' and 'SGACL Enforcement' set to 'DISABLED' and 'Default SGT' set to '2-65519'. A warning message at the top states: 'Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.'

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)

**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

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

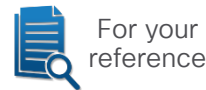
VLANs dynamically assigned via RADIUS take precedence over the VLAN statically defined under the Policy Profile.

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)

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

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 ⓘ

Multicast VLAN

Cancel Apply to Device

WLAN ACL

IPv4 ACL Search or Select

IPv6 ACL Search or Select

URL Filters ⓘ

Pre Auth Search or Select

Post Auth Search or Select

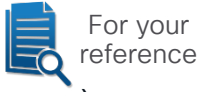
VLANs dynamically assigned via RADIUS take precedence over the VLAN statically defined under the Policy Profile.

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)

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 Clone

Flex Profile Name

☐ default-flex-profile

1 10

+ Add - Delete

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

1 - 1 of 1 items

1 10

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 Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation is Configuration > Tags & Profiles > Flex. The 'Edit Flex Profile' page is displayed for the 'default-flex-profile'. The 'General' tab is active, showing fields for Name (default-flex-profile), Description (default flex profile), and Native VLAN ID (20). The 'CTS Policy' section shows Inline Tagging and SGACL Enforcement as unchecked, and CTS Profile Name as default-sxp-profile. A blue box highlights the 'Native VLAN ID' field, with a blue arrow pointing from it to the explanatory text on the right.

Field	Value
Name*	default-flex-profile
Description	default flex profile
Native VLAN ID	20
HTTP Proxy Port	0
HTTP-Proxy IP Address	0.0.0.0
<b>CTS Policy</b>	
Inline Tagging	<input type="checkbox"/>
SGACL Enforcement	<input type="checkbox"/>
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'. The 'Policy' tab is selected. A modal dialog titled 'Add Policy Tag' is open. In the dialog, the 'Name\*' field is set to 'POLICY\_TAG\_BRANCH'. The 'WLAN-POLICY Maps: 1' section shows a table with two columns: 'WLAN Profile' and 'Policy Profile'. The first row has 'WLAN\_PRFL\_EMPLOYEE' in the 'WLAN Profile' column and 'POLICY\_PRFL\_EMPLOYEE\_FLEX' in the 'Policy Profile' column. Both fields in this row are highlighted with a blue box. The 'Add' button is visible. 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 displays the Cisco Catalyst 9800-L Wireless Controller interface. The left sidebar shows navigation options: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is divided into two panels. The left panel, titled 'All Access Points', shows a table of APs with columns for AP Name, AP Model, Slots, and Admin Status. The right panel, titled 'Edit AP', shows the configuration for AP-9166I-E.0D70. The 'Tags' section is highlighted, showing a dropdown menu for 'Policy' with options: 'POLICY\_TAG\_BRAN', 'Search or Select', 'default-policy-tag', 'POLICY\_TAG\_BRANCH', and 'POLICY\_TAG\_CORP'. A blue arrow points from the 'POLICY\_TAG\_BRANCH' option to the text below.

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 page. The breadcrumb navigation is Configuration > Security > ACL. The ACL configuration page is titled 'Edit ACL' and shows the configuration for 'ACL\_LWA\_INTERNAL\_PORTAL'. 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

The table also includes columns for Source IP, Source Wildcard, Destination IP, Destination Wildcard, Source Port, Destination Port, and Log. The Log column is currently disabled for all rules.

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.

```
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
```

# 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 left sidebar contains navigation links: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled 'Configuration > Security > Web Auth'. A 'Parameter Map Name' list shows 'global' selected. The 'Edit Web Auth Parameter' window is open, showing the 'General' tab. The 'Parameter-map Name' is 'global'. The 'Maximum HTTP connections' is 100. The 'Init-State Timeout(secs)' is 120. The 'Type' is 'consent'. The 'Turn-on Consent with Email' checkbox is unchecked. The 'Captive Bypass Portal' checkbox is unchecked. The 'Disable Success Window' checkbox is unchecked. The 'Disable Logout Window' checkbox is checked. The 'Disable Cisco Logo' checkbox is unchecked. The 'Sleeping Client Status' checkbox is unchecked. The 'Sleeping Client Timeout (minutes)' is 720. The 'Virtual IPv4 Address' is 192.0.2.1. The 'Trustpoint' is CISCO\_IDEVID\_S... The 'Virtual IPv4 Hostname' is empty. The 'Virtual IPv6 Address' is fe80::903a:0:0. The 'Virtual IPv6 Hostname' is empty. The 'Web Auth intercept HTTPs' checkbox is unchecked. The 'Enable HTTP server for Web Auth' checkbox is checked. The 'Disable HTTP secure server for Web Auth' checkbox is unchecked. The 'Banner Configuration' section shows 'Banner Title' as empty and 'Banner Type' as 'None'. The 'Update & Apply' button is at the bottom right.

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'. The 'Maximum HTTP connections' is 100, and the 'Init-State Timeout(secs)' is 120. The 'Banner Configuration' tab is also visible. The 'Type' dropdown is highlighted with a green box.

Configuration > Security > Web Auth

Edit Web Auth Parameter

General Advanced

Parameter-map Name: WEBAUTH\_PMA

Maximum HTTP connections: 100

Init-State Timeout(secs): 120

Type: consent

Turn-on Consent with Email: ☐

Captive Bypass Portal: ☐

Disable Success Window: ☐

Disable Logout Window: ☒

Disable Cisco Logo: ☐

Sleeping Client Status: ☐

Sleeping Client Timeout (minutes): 720

Update & Apply

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

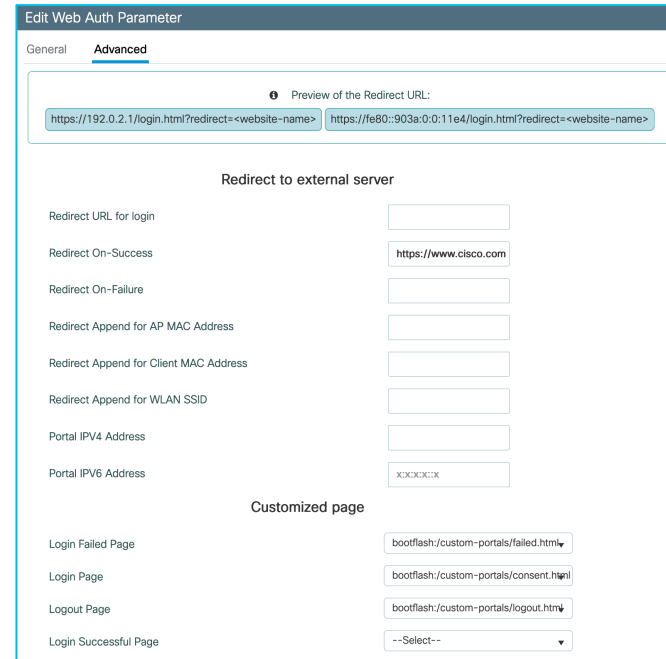
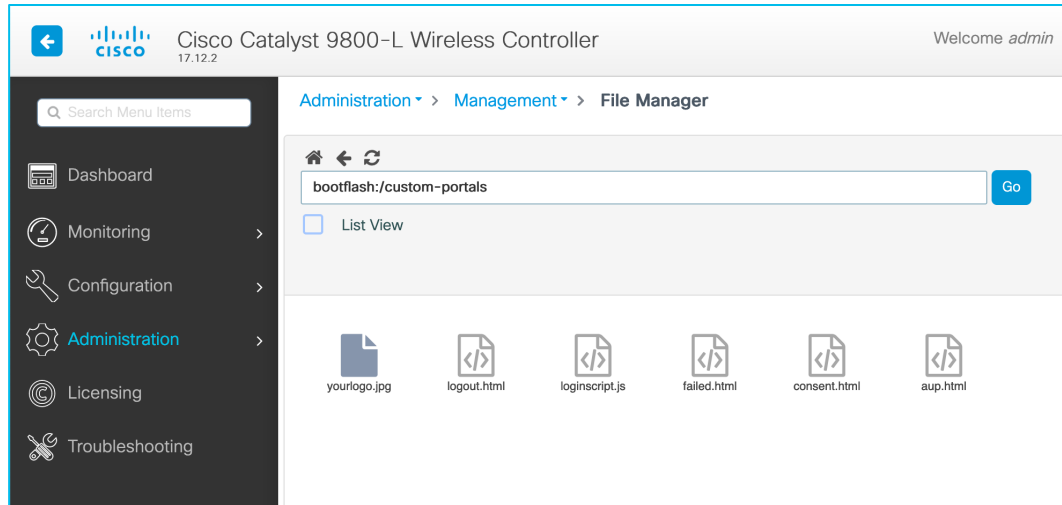
In the Advanced tab we can also choose the “Redirect On-Success” URL and select custom portal files if needed (to be uploaded to the bootflash)

# 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

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The 'Add WLAN' dialog box is open, displaying the 'General' tab. The configuration details are as follows:

Field	Value
Profile Name*	WLAN_PRFL_GUEST
SSID*	.:.:.: Guest
WLAN ID*	2
Status	ENABLED <input checked="" type="checkbox"/>
Broadcast SSID	ENABLED <input checked="" type="checkbox"/>

Radio Policy ①

6 GHz Status: ENABLED ☒ ⓘ  
WPA3 Enabled  
Dot11ax Enabled

5 GHz Status: ENABLED ☒

2.4 GHz Status: ENABLED ☒

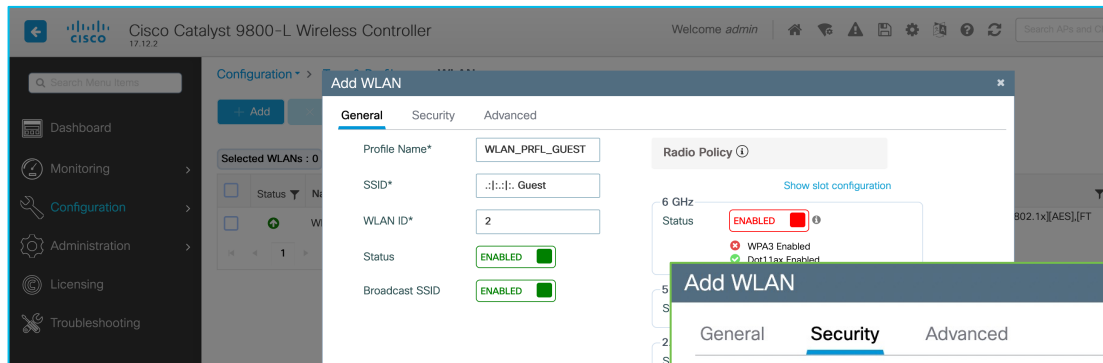
802.11b/g Policy: 802.11b/g

Buttons: Cancel, Apply to Device

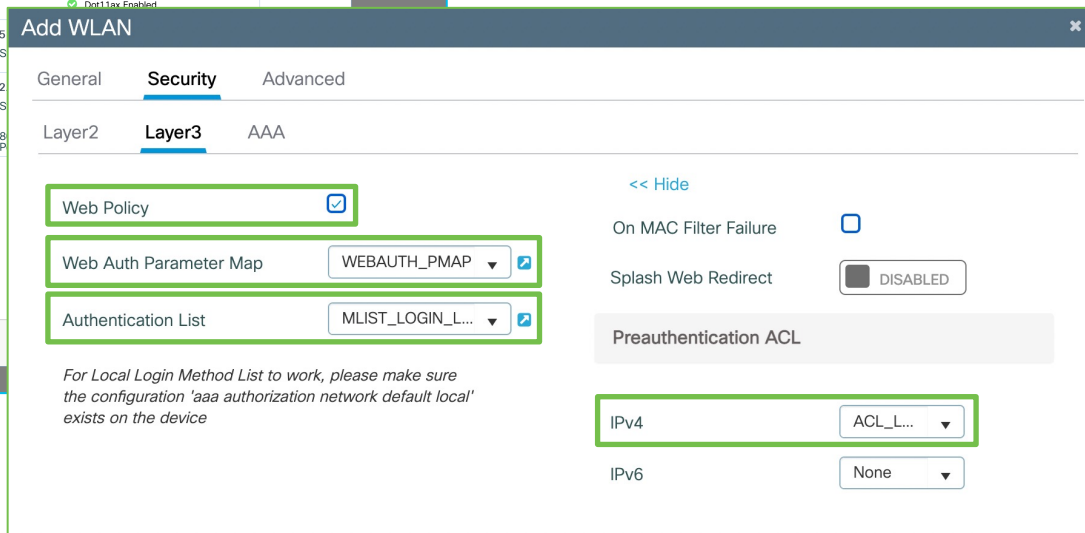
1. New guest WLAN with no L2 security (i.e., fully open)

# 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 local login and our ACL too



# Adding a Guest SSID (LWA with internal portal)

Configuration > Tags & Profiles > WLANs

The screenshot shows the 'Add WLAN' configuration page on a Cisco Catalyst 9800-L Wireless Controller. The 'General' tab is active, showing the following fields: Profile Name\* (WLAN\_PRFL\_GUEST), SSID\* (.:.:.: Guest), WLAN ID\* (2), Status (ENABLED), and Broadcast SSID (ENABLED). The 'Radio Policy' section shows a 6 GHz radio with status 'ENABLED'. The 'Security' tab is also visible, showing 'Web Policy' (checked), 'Web Auth Parameter Map' (WEBAUTH\_PMAP), and 'Authentication List' (MLIST\_LOGIN\_L...). A note at the bottom states: 'For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device'.

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

The screenshot shows the 'Add WLAN' configuration page on a Cisco Catalyst 9800-L Wireless Controller, with the 'Advanced' tab active. The 'P2P Blocking Action' is set to 'Drop'. The 'Multicast Buffer' is set to 'DISABLED'. The 'On MAC Filter Failure' is set to 'DISABLED'. The 'Splash Web Redirect' is set to 'DISABLED'. The 'Preauthentication ACL' section shows 'IPv4' set to 'ACL\_L...' and 'IPv6' set to 'None'.

# 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 left sidebar contains navigation links: Dashboard, Monitoring, Configuration (highlighted), Administration, Licensing, and Troubleshooting. The main content area displays the 'Add Policy Profile' dialog box. The dialog has a title bar 'Add Policy Profile' and 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 dialog is divided into tabs: General, Access Policies, QOS and AVC, Mobility, and Advanced. The 'General' tab is active. It contains the following fields and controls:

- Name\*: POLICY\_PRFL\_GUEST
- Description: Enter Description
- Status: ENABLED (checked)
- Passive Client: DISABLED
- IP MAC Binding: ENABLED (checked)
- Encrypted Traffic Analytics: DISABLED
- WLAN Switching Policy section:
  - Central Switching: ENABLED (checked)
  - Central Authentication: ENABLED (checked)
  - Central DHCP: ENABLED (checked)
  - Flex NAT/PAT: DISABLED
- CTS Policy section:
  - Inline Tagging: ☐
  - SGACL Enforcement: ☐
  - Default SGT: 2-65519

At the bottom of the dialog are 'Cancel' and 'Apply to Device' buttons.

We create our guest Policy Profile with its dedicated VLAN

# Adding a Guest SSID (LWA with internal portal)

Configuration > Tags & Profiles > Policy

The image shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The main menu on the left includes Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The 'Configuration' menu is selected, and the 'Add Policy Profile' dialog is open. The dialog has a warning at the top: "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 active, showing fields for Name\* (POLICY\_PRFL\_GUEST), 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), and a Cancel button.

We create our guest Policy Profile with its dedicated VLAN

The image shows the Cisco Catalyst 9800-L Wireless Controller configuration interface, specifically the 'Add Policy Profile' dialog with the 'Access Policies' tab selected. The dialog has a warning at the top: "Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile." The 'Access Policies' tab is active, showing fields for RADIUS Profiling, HTTP TLV Caching, DHCP TLV Caching, WLAN Local Profiling (Global State of Device Classification, Local Subscriber Policy Name), VLAN (VLAN/VLAN Group, Multicast VLAN), WLAN ACL (IPv4 ACL, IPv6 ACL), URL Filters, Pre Auth, and Post Auth. The 'VLAN' dropdown menu is open, showing options: VLAN\_GUEST, default, VLAN\_EMPLOYEE, VLAN\_GUEST (selected), VLAN\_VOICE, and VLAN\_WIRELESS\_MGMT. There is a Cancel button and an Apply to Device button.

# 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)

86400

Idle Timeout (sec)

300

Idle Threshold (bytes)

0

Client Exclusion Timeout (sec)

☒ 60

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

CISCO *Live!*

BRKEWN-2094

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

65

# 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 interface, illustrating the process of assigning a WLAN Profile to a Policy Profile.

**Top Screenshot:** The interface shows the 'Configuration > Tags & Profiles > Tags' path. The 'Policy' tab is selected, and the 'POLICY\_TAG\_CORP' tag is highlighted. The 'Edit Policy Tag' window is open, showing the 'Name' field set to 'POLICY\_TAG\_CORP'. Under 'WLAN-POLICY Maps: 2', the 'WLAN\_Profile' dropdown is set to 'POLICY\_PRFL\_GUEST'.

**Bottom Screenshot:** The interface shows the 'Configuration > Tags & Profiles > Tags' path. The 'Policy' tab is selected, and the 'POLICY\_TAG\_BRANCH' tag is highlighted. The 'Edit Policy Tag' window is open, showing the 'Name' field set to 'POLICY\_TAG\_BRANCH'. Under 'WLAN-POLICY Maps: 2', the 'WLAN\_Profile' dropdown is set to 'POLICY\_PRFL\_GUEST'.

# Additional references for Guest WLANs

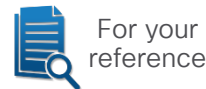


BRKEWN-2284

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



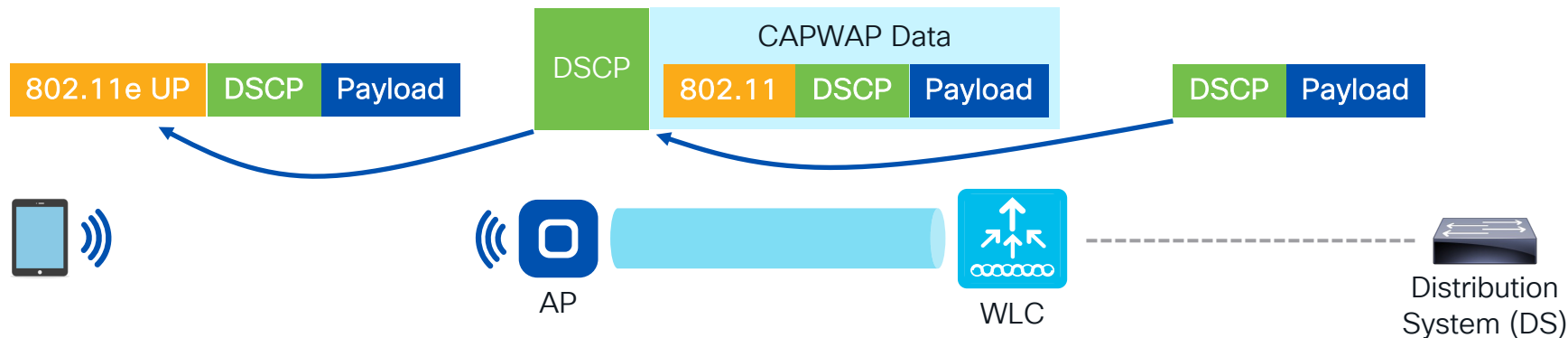
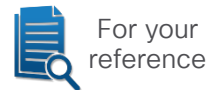
- Web Auth Bundle example with customizable portals  
<https://software.cisco.com/download/home/286322605/type/282791507/release/16.10.1>
- Customize the Web Authentication Portal on Catalyst 9800 WLC  
<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/216121-custom-web-authentication-on-catalyst-98.html>
- 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:

```
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)

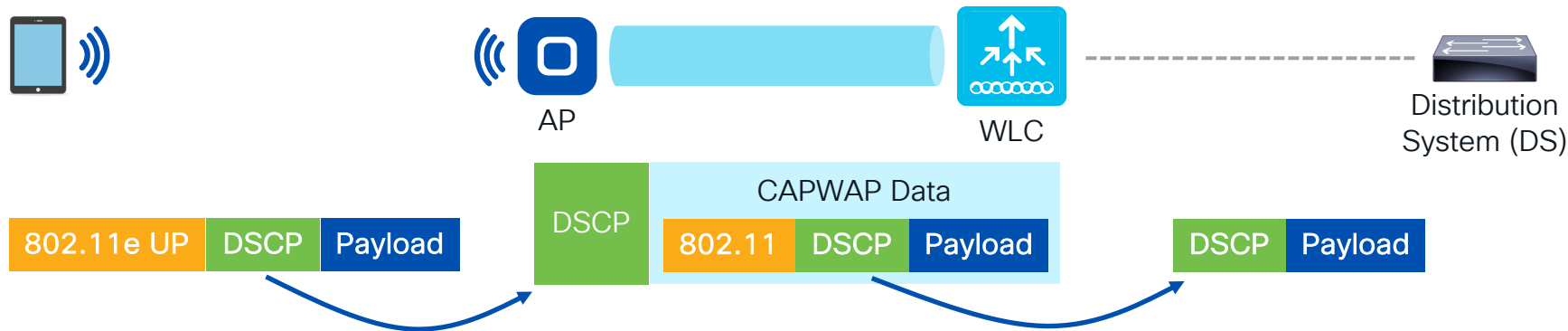
# QoS – Trust DSCP Upstream: the one to start with

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

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

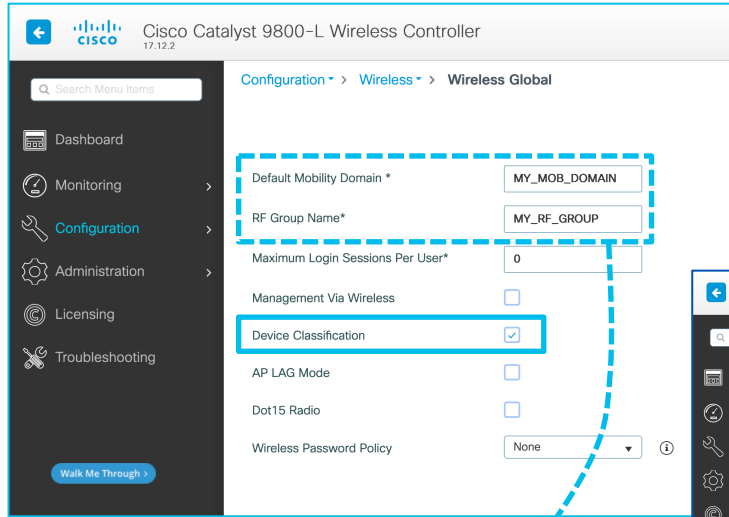


Upstream: the 802.11e UP value from the endpoint (if any) is ignored; the original DSCP value is used to mark the CAPWAP data tunnel too, then preserved all the way up to the DS.  
(assuming no remarking is applied at the WLC level)



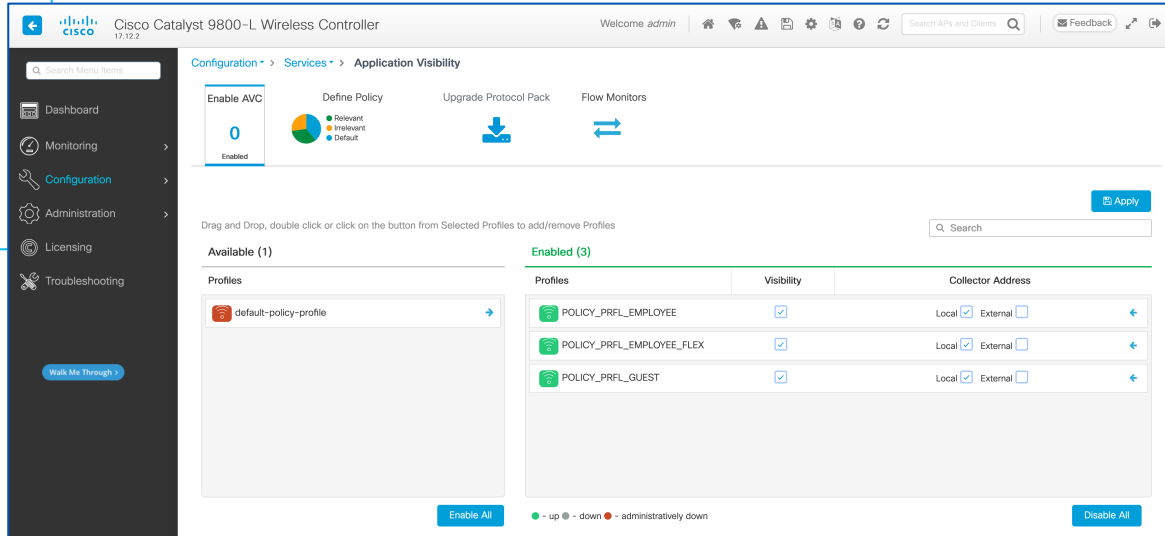
# Devices and applications visibility

## 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 interface. The breadcrumb navigation is Configuration > Radio Configurations > CleanAir. The 6 GHz Band is selected. Under the General tab, 'Enable CleanAir' and 'Report Interferers' are both checked. A 'Walk Me Through' button is visible in the bottom left of the sidebar.

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

This screenshot shows the 5 GHz Band configuration for CleanAir. 'Enable CleanAir' and 'Report Interferers' are checked. In the 'Interference Types to detect' list, 'Bluetooth Discovery' and 'Bluetooth Link' are highlighted with a green box.

This screenshot shows the 2.4 GHz Band configuration for CleanAir. 'Enable CleanAir' and 'Report Interferers' are checked. In the 'Interference Types to detect' list, 'Bluetooth Discovery' and 'Bluetooth Link' are highlighted with an orange box. An orange arrow points from the text 'For high density environments we can avoid BT detection to optimize logs/operations' to this box.

# 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

+ Add - Delete

Rule

Sequence number\* 4

Interface Radio Parameter Spatial Stream

Interface ID 6 GHz Parameter value 1x1

1 - 4 of 4 items

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

Cancel Apply to Device

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. The 'Add Calendar Profile' dialog box is open, displaying the following information:

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

A notification 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 left sidebar shows the navigation menu with options like Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is divided into two panes. The left pane shows the 'AP Join' configuration with a table of AP Join Profiles, including 'default-ap-profile'. The right pane is titled 'Edit AP Join Profile' and has tabs for General, Client, CAPWAP, AP, Management, Security, ICap, QoS, and Geolocation. The 'AP' tab is selected, and the 'Power Management' sub-tab is active. This sub-tab contains a 'Regular Power Profile' section and a 'Calendar Profile - Power Profile Map' section. The 'Calendar Profile - Power Profile Map' section includes an 'Add' button and a 'Delete' button. Below these buttons is a 'Calendar' dropdown menu, a 'Recurrence' dropdown menu, and fields for 'Start Time' and 'End Time'. The 'Power Profile Detailed' section shows a table of power profiles with columns for Sequence, Interface, Interface ID, Parameter, and Parameter Value. The table lists five items, including Ethernet, Radio, and GigabitEthernet0, with parameters like Speed, Spatial Stream, and Power Profile. A text box overlay on the left side of the screenshot states: '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)'. At the bottom of the right pane, there are 'Cancel' and 'Update & Apply to Device' buttons.

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 Cisco Catalyst 9800-L Wireless Controller configuration interface. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area displays the 'Edit AP Join Profile' window for the 'default-ap-profile'. The 'General' tab is active, showing fields for Name, Description, Country Code, Time Zone, LED State, LAG Mode, NTP Server, GAS AP Rate Limit, USB Enable, Apphost, and Failback to DHCP. A dashed blue box highlights the 'Country Code' (NL) and 'Time Zone' (Not Configured) fields. A blue arrow points from the 'Time Zone' field to the text on the right.

Field	Value
Name*	default-ap-profile
Description	default ap profile
Country Code	NL
Time Zone	Not Configured
LED State	<input checked="" type="checkbox"/>
LAG Mode	<input type="checkbox"/>
NTP Server	0.0.0.0
GAS AP Rate Limit	<input type="checkbox"/>
USB Enable	<input type="checkbox"/>
Apphost	<input type="checkbox"/>
Fallback to DHCP	<input checked="" type="checkbox"/>

OfficeExtend AP Configuration

Field	Value
Local Access	<input checked="" type="checkbox"/>
Link Encryption	<input checked="" type="checkbox"/>
Rogue Detection	<input type="checkbox"/>
Provisioning SSID	<input checked="" type="checkbox"/>

Antenna Monitoring

Field	Value
Antenna Monitoring	<input type="checkbox"/>
RSSI Fail Threshold(dB)*	40
Weak RSSI(dBm)*	-60
Detection Time(min)*	12

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-2667  
Catalyst Wireless Supercharged by Cisco DNA Center: The Ultimate Guide to Bring Your Wireless Operation to the Next Level
- 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

# Fill out your session surveys!



Participants who fill out a minimum of **four session surveys and the overall event survey** will get a Cisco Live t-shirt (from 11:30 on Thursday, while supplies last)!

All surveys can be taken in the Cisco Events Mobile App or by logging into the Session Catalog and clicking the 'Participant Resource Center' link at <https://www.ciscolive.com/emea/learn/session-catalog.html>.



# 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 [ciscolive.com/on-demand](https://ciscolive.com/on-demand). Sessions from this event will be available from February 23.



The bridge to possible

# Thank you

CISCO *Live!*

The background is a vibrant, abstract graphic. On the left, there are overlapping, wavy shapes in shades of red, orange, and yellow, resembling a stylized cloud or a series of overlapping circles. On the right, a bright white light source emits a series of colorful rays in shades of blue, green, and yellow, creating a sunburst or starburst effect. The overall color palette is a rainbow spectrum, transitioning from red/orange on the left to blue/green on the right.

cisco *Live!*

Let's go