



Successfully Configuring Catalyst 9800 Wireless on Your First Shot

Federico Ziliotto – Technical Solutions Architect
CCIE – 23280 (Wireless, R&S)
BRKEWN-2094

*“Please tell me I didn’t
forget the net at home...”*



Federico → Fede

- ~18 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)
- ~6 years 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”



For your
reference

Webex App

Questions?

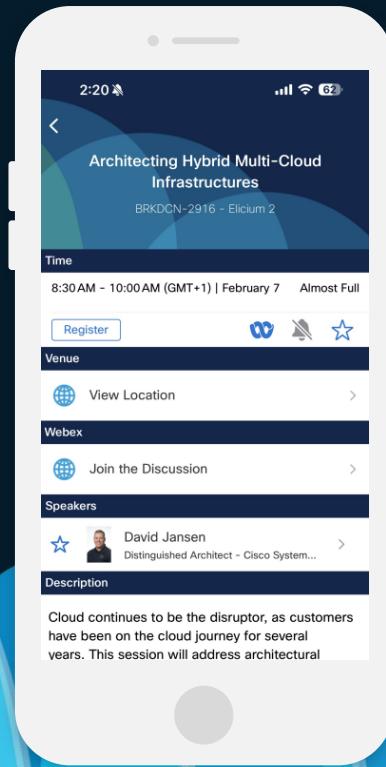
Use the Webex app to chat with the speaker after the session

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 28, 2025.

CISCO *Live!*



Configuration template available here



- The text format of all the configuration examples in this presentation is available here:

https://github.com/fedezi/CLEU25_BRKEWN-2094/blob/main/CLEU25_BRKEWN-2094_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, WPA3 and Guest/OWE use cases/examples
4. With Wi-Fi 7 in mind

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

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  
...  
[0] Go to the IOS command prompt without saving this config.  
...  
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/M/H) it's pre-installed

```
show wireless management trustpoint
```



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

It should be set to "CISCO_IDEVID_CMCA3_SUDI", but if not...

```
show crypto pki trustpoints
!
no wireless management trustpoint
wireless management trustpoint CISCO_IDEVID_CMCA3_SUDI
```

17.9.5+ and 17.12.1+
CISCO_IDEVID_SUDI is an HW-SUDI (vs SW-SUDI before)
CISCO_IDEVID_CMCA3_SUDI is the new SW-SUDI and recommended for CAPWAP performances

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 CISCO_IDEVID_SUDI), 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 two overlapping web pages. The background page is the 'Configuration Setup Wizard' titled '1. General Settings'. It includes fields for Deployment Mode (Standalone), Host Name (MY-9800), Country (US), Date (21 Jan 2025), Time / Timezone (10:29:04 Central), NTP Servers (Enter NTP Server), AAA Servers (admin), and Service Port Settings (DHCP, Static IP). The foreground page is the 'WELCOME!' screen for the 'Day-0 wizard'. It features a 'Cisco' logo and a 'WELCOME!' 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.' It displays two cards: 'DNAC Cloud Onboarding Day 0 Wizard' (describing the wizard's purpose) and 'Classic Day 0 Wizard' (describing the wizard's purpose). Below these cards is a section titled 'READ THE INSTRUCTIONS BELOW BEFORE YOU BEGIN' with the following bullet points:

- 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 or https://<9800_IP>/webui/#/dayzeroPnpOrCli

Shutting 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
```

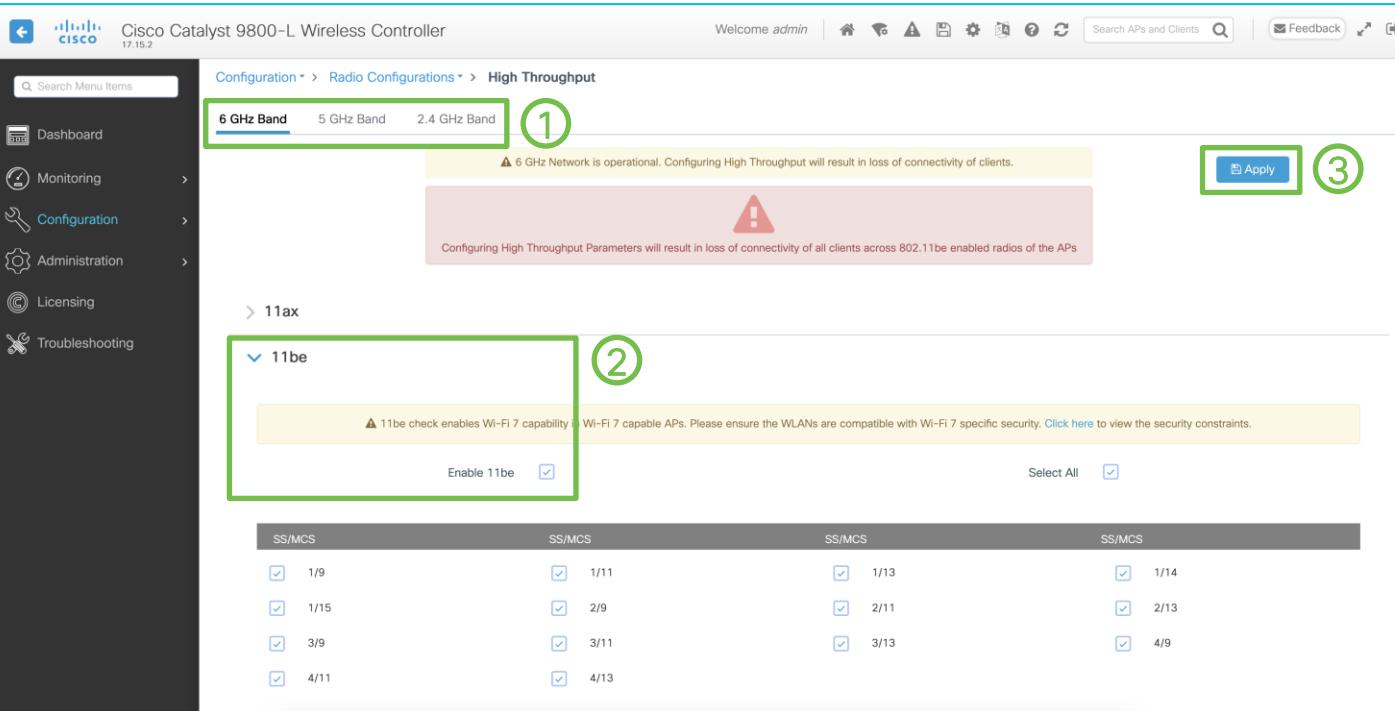


```
ap dot11 24ghz rate RATE_11M mandatory
ap dot11 24ghz rate RATE_1M disable
ap dot11 24ghz rate RATE_2M disable
ap dot11 24ghz rate RATE_5_5M disable
ap dot11 24ghz rate RATE_6M disable
ap dot11 24ghz rate RATE_9M disable
ap dot11 24ghz rate RATE_12M supported
ap dot11 24ghz rate RATE_18M supported
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
!
ap dot11 6ghz rf-profile default-rf-profile-6ghz
shutdown
channel chan-width maximum WIDTH_80MHz
rate RATE_12M mandatory
rate RATE_24M supported
rate RATE_6M disable
rate RATE_9M disable
no shutdown
```

CISCO Live! * On more recent IOS-XE versions (e.g., 17.9.x) this is not needed anymore

802.11be / Wi-Fi 7 must be explicitly enabled

Configuration > Radio Configurations > High Throughput > 2.4/5/6 GHz Band



Configuration > Radio Configurations > High Throughput

6 GHz Band 5 GHz Band 2.4 GHz Band ①

6 GHz Network is operational. Configuring High Throughput will result in loss of connectivity of clients.

③

11ax

11be ②

11be check enables Wi-Fi 7 capability on Wi-Fi 7 capable APs. Please ensure the WLANs are compatible with Wi-Fi 7 specific security. [Click here](#) to view the security constraints.

Enable 11be Select All

SS/MCS	SS/MCS	SS/MCS	SS/MCS
<input checked="" type="checkbox"/> 1/9	<input checked="" type="checkbox"/> 1/11	<input checked="" type="checkbox"/> 1/13	<input checked="" type="checkbox"/> 1/14
<input checked="" type="checkbox"/> 1/15	<input checked="" type="checkbox"/> 2/9	<input checked="" type="checkbox"/> 2/11	<input checked="" type="checkbox"/> 2/13
<input checked="" type="checkbox"/> 3/9	<input checked="" type="checkbox"/> 3/11	<input checked="" type="checkbox"/> 3/13	<input checked="" type="checkbox"/> 4/9
<input checked="" type="checkbox"/> 4/11	<input checked="" type="checkbox"/> 4/13		

```
ap dot11 24ghz dot11be  
ap dot11 5ghz dot11be  
ap dot11 6ghz dot11be
```

- 11be support is disabled by default
- Enabling it will cause Wi-Fi 7 capable and enabled radios to reset

Save! Save! Save!

(wr → write memory)

*Maybe they won't
notice that I didn't save
before reloading...*



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

Administration > Software Management



For your
reference

Cisco Catalyst 9800-L Wireless Controller
17.6.4

Administration > Software Management

Click here for Latest Recommended Software

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: Select File

Download & Install **Save Configuration & Activate**

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

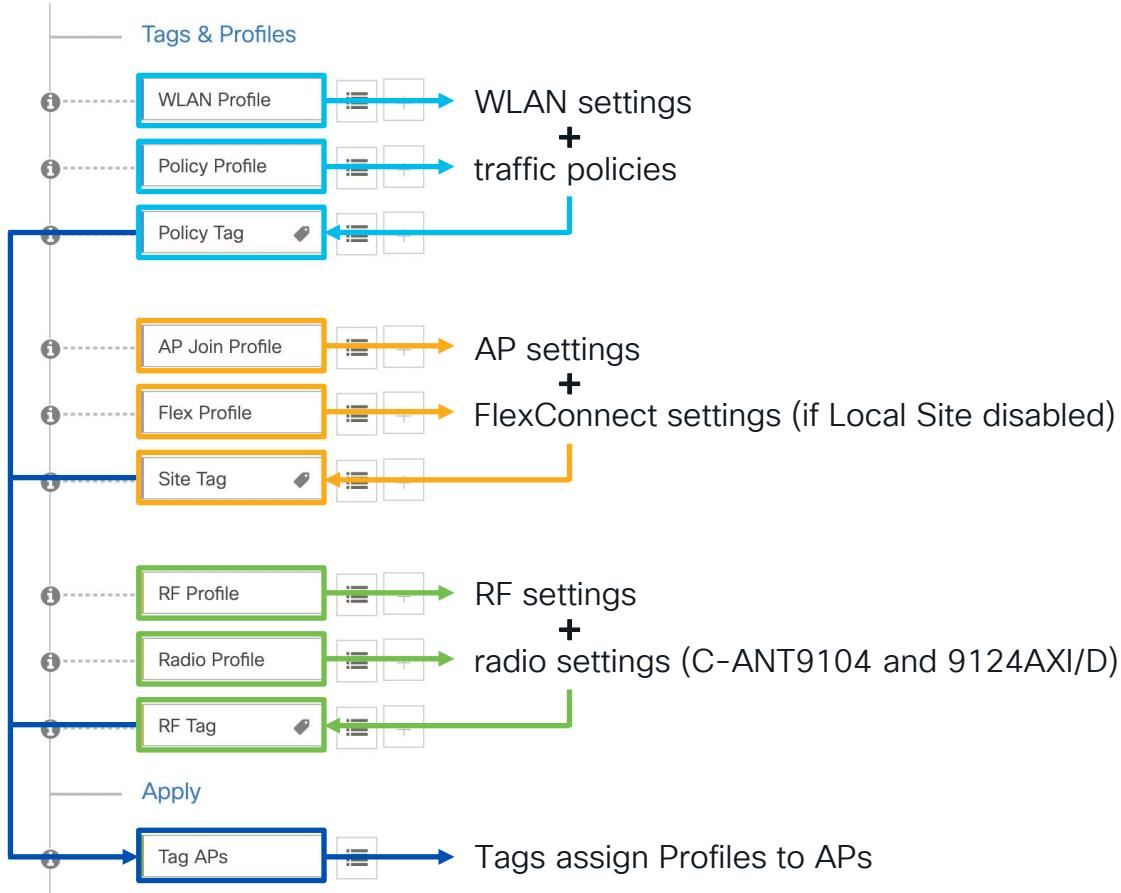
Profiles and Tags: the main configuration objects

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)

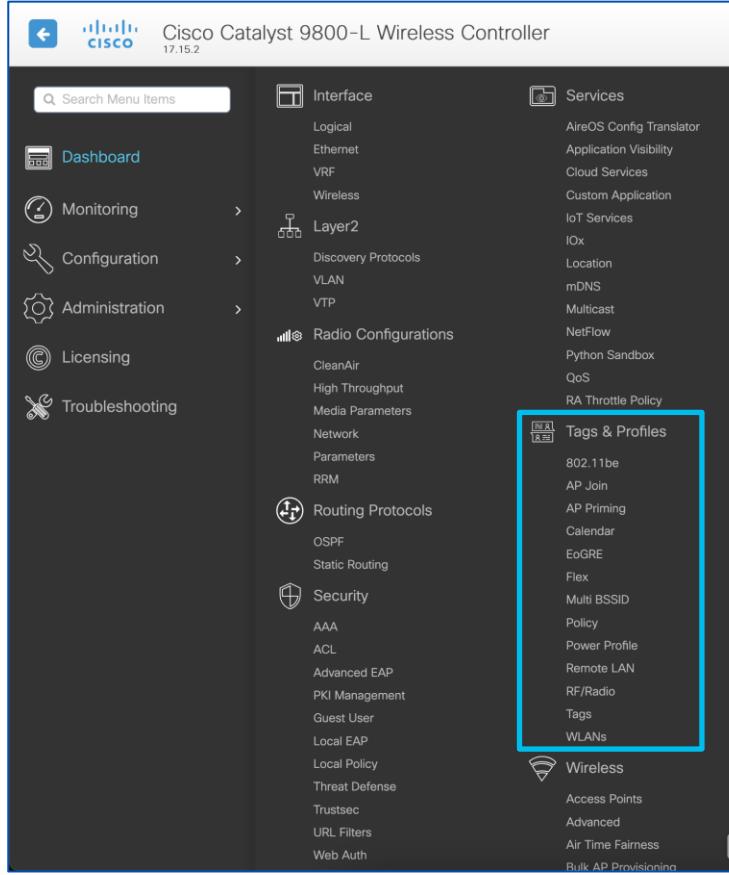
Profiles and Tags: the main configuration objects

Configuration >
Wireless Setup >
Advanced >
Start Now



Profiles and Tags: a more dedicated menu

Configuration >
Tags & Profiles



The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The main menu includes sections for Dashboard, Monitoring, Configuration, Administration, Licensing, Troubleshooting, Routing Protocols, Security, and various Services. A search bar is at the top. The 'Configuration' section is expanded, showing sub-options like Logical, Ethernet, VRF, Wireless, Layer2, Discovery Protocols, VLAN, VTP, Radio Configurations, Media Parameters, Network, Parameters, RRM, OSPF, Static Routing, AAA, ACL, Advanced EAP, PKI Management, Guest User, Local EAP, Local Policy, Threat Defense, Trustsec, URL Filters, and Web Auth. The 'Radio Configurations' section is also expanded, listing CleanAir, High Throughput, Media Parameters, Network, Parameters, RRM, OSPF, and Static Routing. The 'Tags & Profiles' section, which is highlighted with a blue box, contains the following items: 802.11be, AP Join, AP Priming, Calendar, EoGRE, Flex, Multi BSSID, Policy, Power Profile, Remote LAN, RF/Radio, Tags, and WLANs. The 'Services' section includes AireOS Config Translator, Application Visibility, Cloud Services, Custom Application, IoT Services, IOx, Location, mDNS, Multicast, NetFlow, Python Sandbox, QoS, RA Throttle Policy, and WLANs. The 'Wireless' section includes Access Points, Advanced, Air Time Fairness, and Bulk AP Provisioning.

Client VLANs should be configured and trunked

```
vlan 110
  name VLAN_EMPLOYEE
vlan 120
  name VLAN_VOICE
vlan 130
  name VLAN_GUEST
vlan 140
  name VLAN_IOT
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	
140	VLAN_IOT	active	
		act/unsup	

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller web interface. The left sidebar includes links for Dashboard, Monitoring, Configuration (selected), Administration, Licensing, and Troubleshooting. The main content area is titled 'Configuration > Layer2 > VLAN' and shows a table of 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), 130 (VLAN_GUEST), and 140 (VLAN_IOT). All VLANs are marked as 'active' and have 'Tw0/0/0, Tw0/0/1, Tw0/0/2, Tw0/0/3, Te0/1/1' listed under 'Ports'.

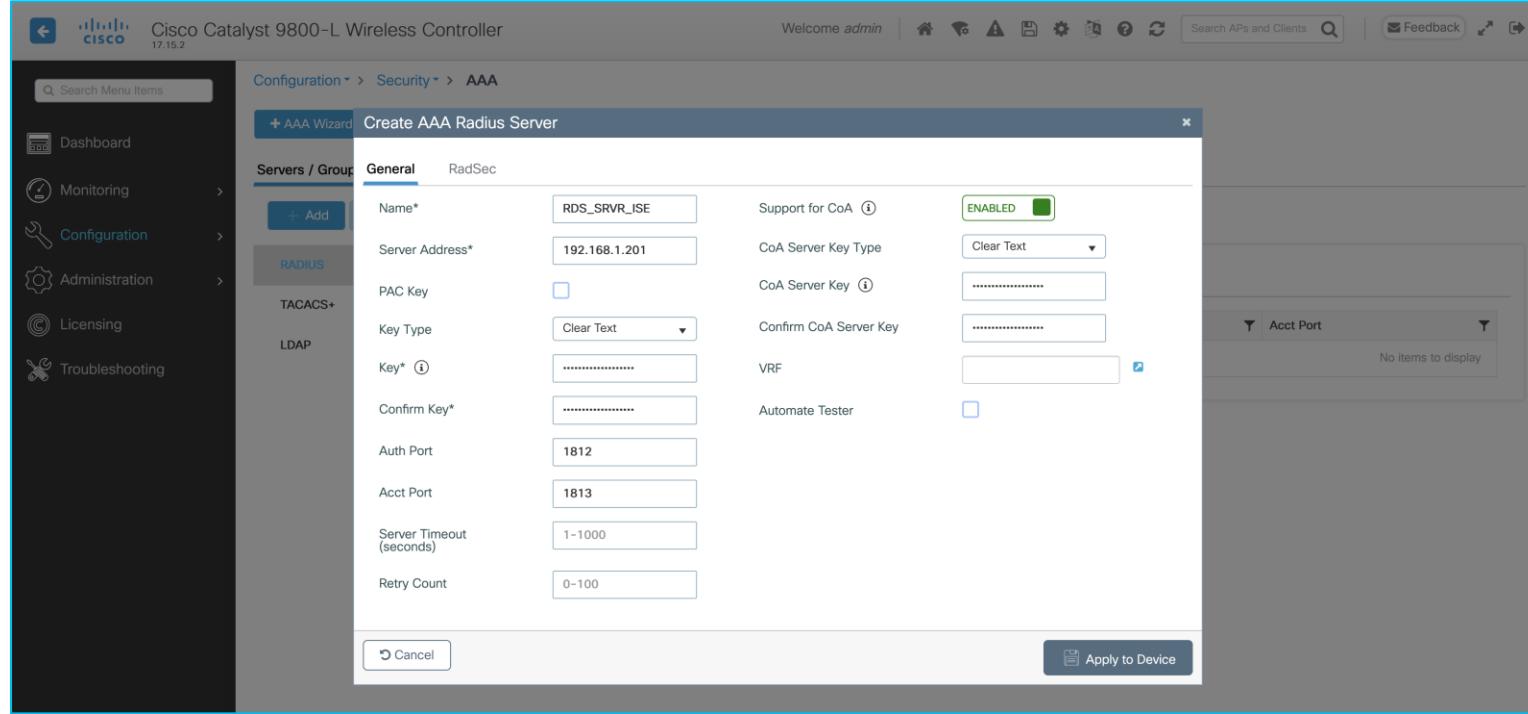
VLAN ID	Name	Status	Ports
1	default	active	Tw0/0/0, Tw0/0/1, Tw0/0/2, Tw0/0/3, Te0/1/1
10	VLAN_WIRELESS_MGMT	active	
110	VLAN_EMPLOYEE	active	
120	VLAN_VOICE	active	
130	VLAN_GUEST	active	
140	VLAN_IOT	active	

Configuration > Layer2 > VLAN (VLAN tab)

CISCO Live!

Configuring a RADIUS server

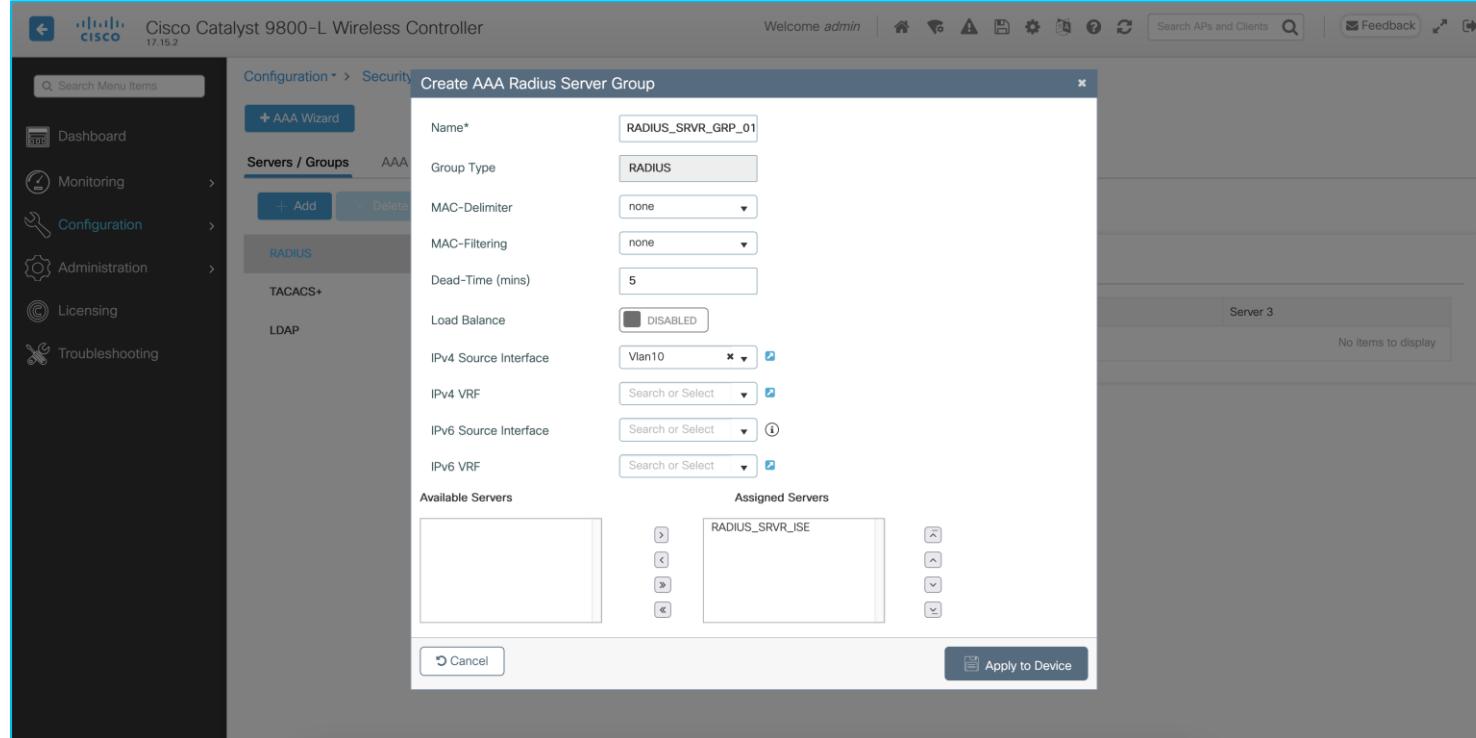
Configuration > Security > AAA > Add RADIUS Server



The screenshot shows the Cisco Catalyst 9800-L Wireless Controller interface. The left sidebar includes links for Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main navigation bar at the top shows 'Configuration > Security > AAA'. A sub-menu on the left under 'AAA' lists 'Servers / Group', 'RADIUS', 'TACACS+', and 'LDAP'. A central dialog box titled 'Create AAA Radius Server' is open, showing the 'General' tab. The 'Name*' field is set to 'RDS_SRVR_ISE'. The 'Server Address*' field is set to '192.168.1.201'. The 'Support for CoA' switch is set to 'ENABLED'. Other fields include 'CoA Server Key Type' (set to 'Clear Text'), 'CoA Server Key' (redacted), 'Confirm CoA Server Key' (redacted), 'VRF' (empty), and 'Authenticate Tester' (unchecked). Buttons at the bottom include 'Cancel' and 'Apply to Device'.

Configuring a RADIUS server group

Configuration > Security > AAA > Add RADIUS Server Group



The screenshot shows the Cisco Catalyst 9800-L Wireless Controller interface. The left sidebar includes links for Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main navigation bar at the top shows 'Cisco Catalyst 9800-L Wireless Controller' and the user 'admin'. The 'Configuration > Security > AAA' path is selected. A sub-menu for 'Servers / Groups' is open, with 'RADIUS' selected. A modal dialog box titled 'Create AAA Radius Server Group' is displayed. The 'Name*' field contains 'RADIUS_SRVR_GRP_01'. The 'Group Type' is set to 'RADIUS'. Other fields include 'MAC-Delimiter' (none), 'MAC-Filtering' (none), 'Dead-Time (mins)' (5), and 'Load Balance' (disabled). Under 'IPv4' and 'IPv6' sections, 'Source Interface' and 'VRF' dropdowns are present. The 'Available Servers' section is empty. The 'Assigned Servers' section contains 'RADIUS_SRVR_ISE'. At the bottom 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 web interface. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled 'Configuration > Security > AAA' and shows the 'AAA Method List' tab selected. A sub-dialog box titled 'Quick Setup: AAA Authentication' is open. In this dialog, the 'Method List Name*' field is set to 'MLIST_AUTHC_1X', the 'Type*' field is set to 'dot1x', and the 'Group Type' field is set to 'group'. The 'Fallback to local' checkbox is unchecked. The 'Available Server Groups' list includes 'radius', 'ldap', and 'tacacs+'. The 'Assigned Server Groups' list contains 'RADIUS_SRVR_GRP_01'. There are buttons for 'Cancel' and 'Apply to Device' at the bottom. The background shows a table with columns 'Group3' and 'Group4', both of which have 'N/A' listed under them. A footer at the bottom right indicates '1 - 3 of 3 items'.

AAA Method List for authorization



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

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

Method List Name*: MLIST_AUTHZ_NTWRK

Type*: network

Group Type: group

Available Server Groups: radius, ldap, tacacs+

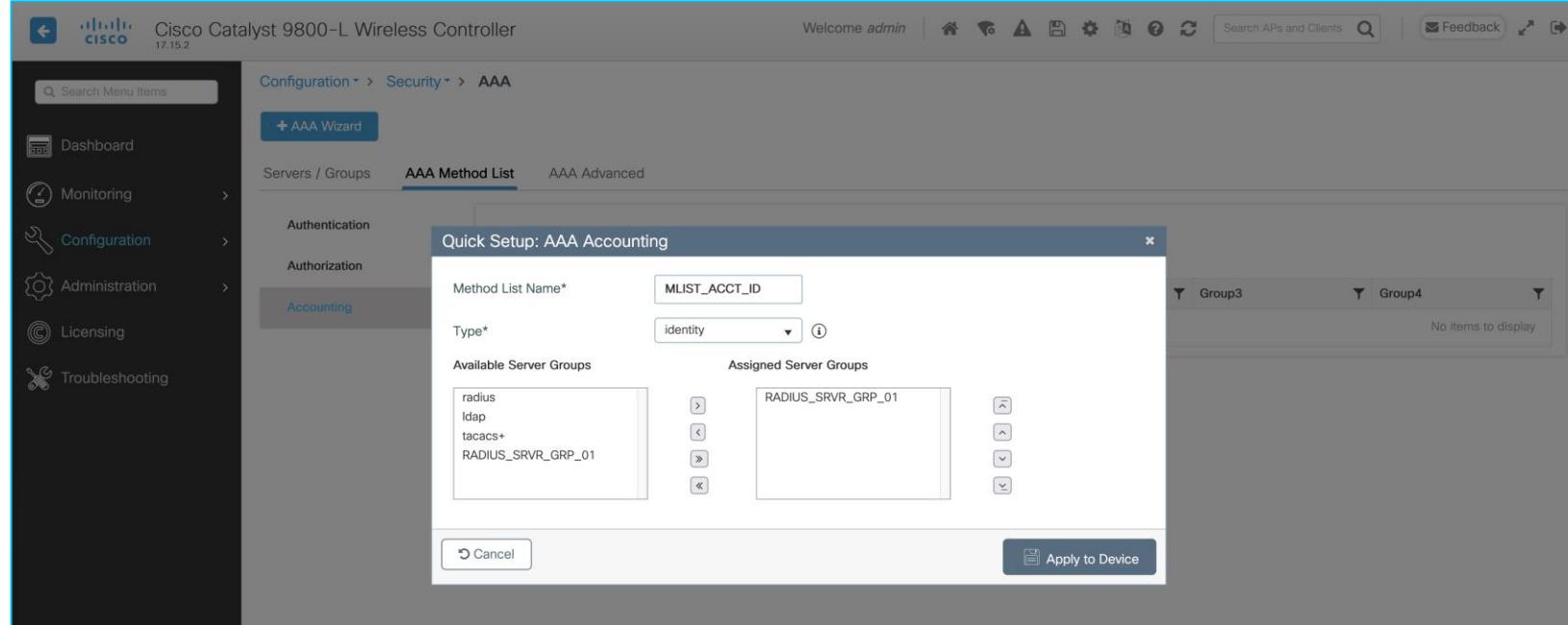
Assigned Server Groups: RADIUS_SRVR_GRP_01

Cancel Apply to Device

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 shows the Cisco Catalyst 9800-L Wireless Controller web interface. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main header shows 'Cisco Catalyst 9800-L Wireless Controller' and the time '17:15:2'. The top navigation bar includes 'Welcome admin', various icons, and links for 'Search APs and Clients', 'Feedback', and 'Help'.

The main content area is titled 'Configuration > Security > AAA'. Below this, there are three tabs: 'AAA Method List' (selected), 'AAA Advanced', and 'AAA Wizard'. The 'AAA Method List' tab is active, and a sub-dialog box titled 'Quick Setup: AAA Accounting' is displayed.

The 'Quick Setup: AAA Accounting' dialog box contains the following fields:

- Method List Name***: MLIST_ACCT_ID
- Type***: identity
- Available Server Groups**: A list box containing 'radius', 'Idap', 'tacacs+', and 'RADIUS_SRVR_GRP_01'.
- Assigned Server Groups**: A list box containing 'RADIUS_SRVR_GRP_01'.
- Buttons**: 'Cancel' and 'Apply to Device'.

Below the dialog box, the main interface shows 'Group3' and 'Group4' with the message 'No items to display'.

Or also with a quick CLI copy/paste



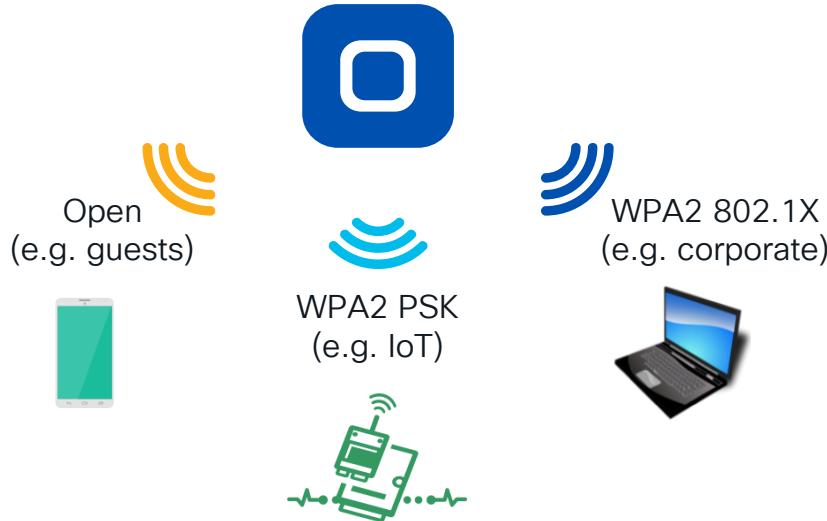
```
radius server RADIUS_SRVR_ISE
  address ipv4 192.168.1.201 auth-port 1812 acct-port 1813
  key <RADIUS_SHARED_SECRET>
!
aaa server radius dynamic-author
  client 192.168.1.201 server-key <RADIUS_SHARED_SECRET>
!
aaa group server radius RADIUS_SRVR_GRP_01
  server name RADIUS_SRVR_ISE
  ip radius 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

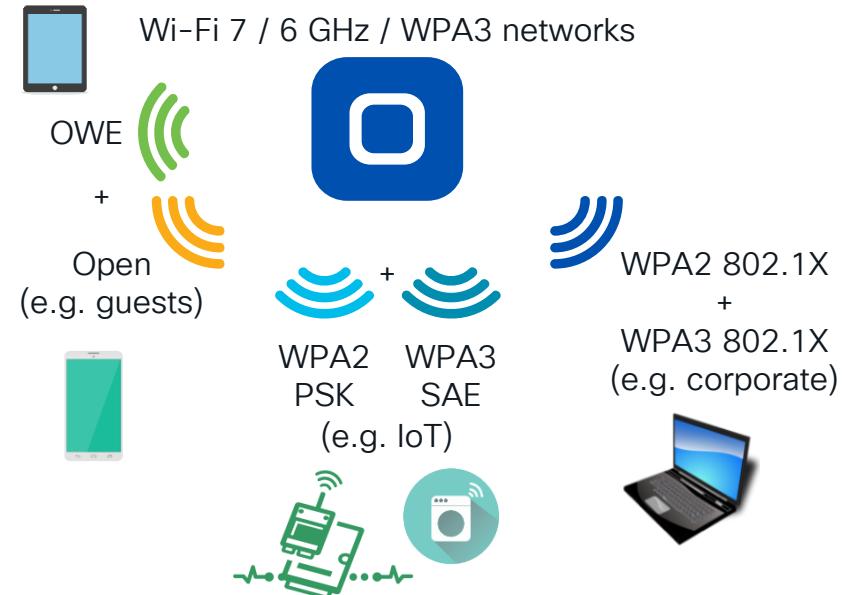


Wi-Fi 7 features mandate WPA3/OWE

Pre-Wi-Fi 7 / 6 GHz / WPA3 networks

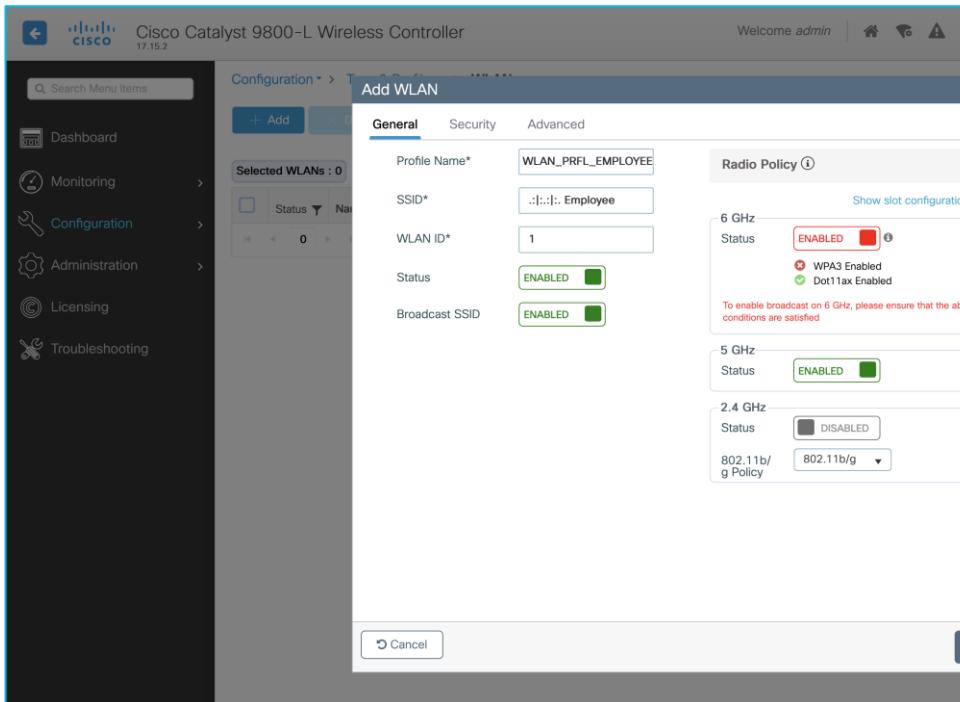


Wi-Fi 7 / 6 GHz / WPA3 networks



Configuring an 802.1X WLAN Profile

Configuration > Tags & Profiles > WLANs > Add



Cisco Catalyst 9800-L Wireless Controller

Configuration > Tags & Profiles > WLANs > Add

General Security Advanced

Profile Name* WLAN_PRFL_EMPLOYEE

SSID* ::::: Employee

WLAN ID* 1

Status ENABLED

Broadcast SSID ENABLED

Radio Policy

6 GHz Status ENABLED

WPA3 Enabled Dot11ax Enabled

To enable broadcast on 6 GHz, please ensure that the above conditions are satisfied

5 GHz Status ENABLED

2.4 GHz Status DISABLED

802.11b/g Policy 802.11b/g

General Security Advanced

Layer2 Layer3 AAA

To review the necessary considerations for ensuring WLAN compatibility with Wi-Fi 7 security [click here](#).

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering

Lobby Admin Access

WPA Parameters

WPA Policy WPA2 Policy

GTK Randomize WPA3 Policy

Transition Disable Beacon Protection

Fast Transition

Status Enabled

Over the DS

Reassociation Timeout * 20

Auth Key Mgmt (AKM)

802.1X FT + 802.1X CCKM

802.1X-SHA256 FT + PSK

PSK PSK-SHA256 SAE

Add WLAN

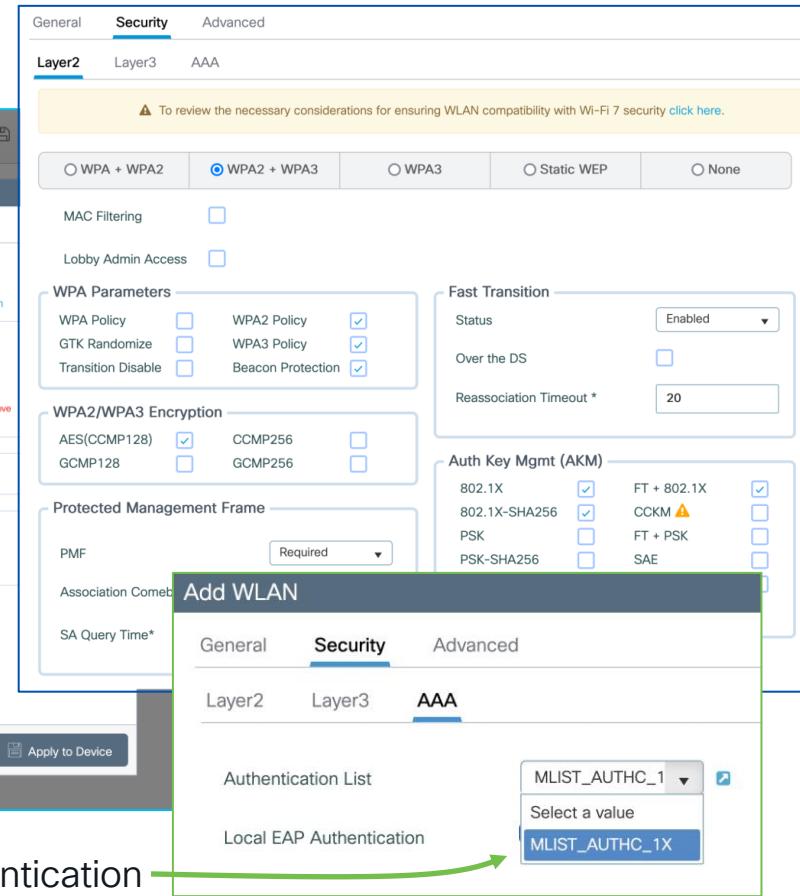
General Security Advanced

Layer2 Layer3 AAA

Authentication List MLIST_AUTHC_1

Select a value MLIST_AUTHC_1X

Local EAP Authentication MLIST_AUTHC_1X



General Security Advanced

Layer2 Layer3 AAA

To review the necessary considerations for ensuring WLAN compatibility with Wi-Fi 7 security [click here](#).

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering

Lobby Admin Access

WPA Parameters

WPA Policy WPA2 Policy

GTK Randomize WPA3 Policy

Transition Disable Beacon Protection

Fast Transition

Status Enabled

Over the DS

Reassociation Timeout * 20

Auth Key Mgmt (AKM)

802.1X FT + 802.1X CCKM

802.1X-SHA256 FT + PSK

PSK PSK-SHA256 SAE

Add WLAN

General Security Advanced

Layer2 Layer3 AAA

Authentication List MLIST_AUTHC_1

Select a value MLIST_AUTHC_1X

Local EAP Authentication MLIST_AUTHC_1X

The AAA Method List for dot1x authentication

CISCO Live!

Zoom on Layer 2 Security for Wi-Fi 7 support

General **Security** Advanced

Layer2 Layer3 AAA

⚠ To review the necessary considerations for ensuring WLAN compatibility with Wi-Fi 7 security [click here](#).

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering

Lobby Admin Access

WPA Parameters

WPA Policy <input type="checkbox"/>	WPA2 Policy <input checked="" type="checkbox"/>
GTK Randomize <input type="checkbox"/>	WPA3 Policy <input checked="" type="checkbox"/>
Transition Disable <input type="checkbox"/>	Beacon Protection <input checked="" type="checkbox"/>

Fast Transition

Status <input type="button" value="Enabled"/>
Over the DS <input type="checkbox"/>
Reassociation Timeout * 20

WPA2/WPA3 Encryption

AES(CCMP128) <input checked="" type="checkbox"/>	CCMP256 <input type="checkbox"/>
GCMP128 <input type="checkbox"/>	GCMP256 <input type="checkbox"/>

Protected Management Frame

PMF <input type="button" value="Required"/>
Association Comeback Timer* 1
SA Query Time* 200

Auth Key Mgmt (AKM)

802.1X <input checked="" type="checkbox"/>	FT + 802.1X <input checked="" type="checkbox"/>
802.1X-SHA256 <input checked="" type="checkbox"/>	CCKM <input type="checkbox"/>
PSK <input type="checkbox"/>	FT + PSK <input type="checkbox"/>
PSK-SHA256 <input type="checkbox"/>	SAE <input type="checkbox"/>
FT + SAE <input type="checkbox"/>	SAE-EXT-KEY <input type="checkbox"/>
FT + SAE-EXT-KEY <input type="checkbox"/>	

WPA2/WPA3 settings:

- Beacon Protection
- AES(CCMP128)

PMF: Required (for Device Analytics too)

Fast Transition: Enabled

AKM:

- 802.1X
- FT + 802.1X
- 802.1X-SHA256

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

For max WPA2 compatibility (no Wi-Fi 7)



General **Security** Advanced

Layer2 Layer3 AAA

⚠ To review the necessary considerations for ensuring WLAN compatibility with Wi-Fi 7 security [click here](#).

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering

Lobby Admin Access

WPA Parameters

WPA Policy <input type="checkbox"/>	WPA2 Policy <input checked="" type="checkbox"/>
GTK Randomize <input type="checkbox"/>	WPA3 Policy <input checked="" type="checkbox"/>
Transition Disable <input type="checkbox"/>	Beacon Protection <input type="checkbox"/>

Fast Transition

Status <input type="button" value="Enabled"/>
Over the DS <input type="checkbox"/>
Reassociation Timeout * 20

WPA2/WPA3 Encryption

AES(CCMP128) <input checked="" type="checkbox"/>	CCMP256 <input type="checkbox"/>
GCMP128 <input type="checkbox"/>	GCMP256 <input type="checkbox"/>

Protected Management Frame

PMF <input type="button" value="Optional"/>
Association Comeback Timer* 1
SA Query Time* 200

Auth Key Mgmt (AKM)

802.1X <input checked="" type="checkbox"/>	FT + 802.1X <input checked="" type="checkbox"/>
802.1X-SHA256 <input checked="" type="checkbox"/>	CCKM <input type="checkbox"/>
PSK <input type="checkbox"/>	FT + PSK <input type="checkbox"/>
PSK-SHA256 <input type="checkbox"/>	SAE <input type="checkbox"/>
FT + SAE <input type="checkbox"/>	SAE-EXT-KEY <input type="checkbox"/>
FT + SAE-EXT-KEY <input type="checkbox"/>	

Setting PMF Optional (hence no Beacon Protection) for max WPA2 compatibility won't allow Wi-Fi 7 support, but it can still let us support 6 GHz / Wi-Fi 6E

WPA2/WPA3 settings:

- AES(CCMP128)

PMF: Optional (for Device Analytics too)

Fast Transition: Enabled

AKM:

- 802.1X
- FT + 802.1X
- 802.1X-SHA256

Fast Transition / 802.11r = Enabled

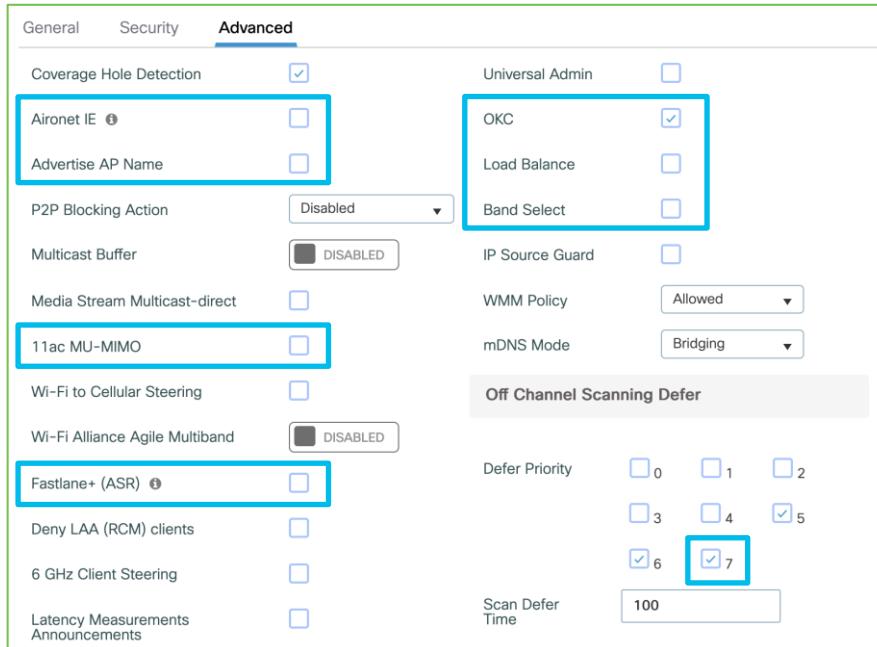
No "Adaptive Enabled", as it would benefit Apple/Samsung endpoints only

Over the DS = unchecked

Over the Air (OTA) is the technique all endpoints are supporting

802.1X WLAN Profile – Advanced Settings

WLAN Profile > Advanced



General Security Advanced

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
- 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

802.1X WLAN Profile – Advanced Settings

WLAN Profile > Advanced

Max Client Connections

Per WLAN: 0

Per AP Per WLAN: 0

Per AP Radio Per WLAN: 200

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:

OFDMA Downlink:

OFDMA Uplink:

MU-MIMO Downlink:

MU-MIMO Uplink:

BSS Target Wake Up Time:

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:

Geolocation

Fine Time Measurement (FTM) Responder: DISABLED

- 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

Search Menu Items

Cisco Catalyst 9800-L Wireless Controller

Welcome admin

Dashboard

Monitoring

Configuration

Administration

Licensing

Troubleshooting

Configuration > Tags & Profiles > Policy > Add

Name* POLICY_PRFL_EMPLOYEE

Description Enter Description

Status ENABLED

Passive Client DISABLED

IP MAC Binding ENABLED

Encrypted Traffic Analytics DISABLED

CTS 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 *i*

Local Subscriber Policy Name

VLAN

VLAN/VLAN Group

Multicast VLAN

VLAN EMPLOYEE *i*

- default
- VLAN_EMPLOYEE**
- VLAN_GUEST
- VLAN_IOT
- VLAN_VOICE
- VLAN_WIRELESS_MGMT

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

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

DHCP Server VRF Search or Select

Fabric Profile Search or Select

Link-Local Bridging

mDNS Service Policy Search or Select

Hotspot Server Search or Select

L3 Access DISABLED

User Defined (Private) Network

Status

Drop Unicast

DNS Layer Security

DNS Layer Security Parameter Map Not Configured

BRKEWN-2094

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public 39

Configuring the Policy Profile

Allow AAA Override to support dynamic RADIUS attributes

NAC State/Type for CoA support

Accounting List for RADIUC Accounting and CoA too

For increased security/control

The screenshot shows the 'Add Policy Profile' configuration page. The 'AAA Policy' section is highlighted with a green box and contains the following settings:

- Allow AAA Override:
- NAC State:
- Policy Name: default-aaa-policy
- Accounting List: MLIST_ACCT_ID
- Interim Accounting:

The 'Advanced' section contains the following settings:

- Fabric Profile: Search or Select
- Link-Local Bridging:
- mDNS Service Policy: Search or Select
- Hotspot Server: Search or Select
- L3 Access: DISABLED

The 'User Defined (Private) Network' section contains the following settings:

- Status:
- Drop Unicast:

The 'DNS Layer Security' section contains the following settings:

- DNS Layer Security Parameter Map: Not Configured

The 'Policy Proxy Settings' section contains the following settings:

- ARP Proxy:
- IPv6 Proxy: None

Configuring the Policy Tag

Configuration > Tags & Profiles > Tags > Policy > Add

Cisco Catalyst 9800-L Wireless Controller

Configuration > Tags & Profiles > Tags

Policy Tag Name: POLICY_TAG_Corp

Description: Enter Description

WLAN-POLICY Maps: 0

WLAN Profile: WLAN_PRFL_EM

Policy Profile: POLICY_PRFL_E

Map WLAN and Policy

Apply to Device

Policy Tag

WLAN Profile
(it defines the SSID, band 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 includes links for Dashboard, Monitoring, Configuration (which is selected), Administration, Licensing, and Troubleshooting. The main content area shows the 'Configuration > Wireless > Access Points' path. The 'Edit AP' page is open for an AP named 'AP-9166I-E.1F20'. In the 'Tags' section, the 'Policy' dropdown is highlighted with a green box and a green arrow points to a callout box that reads: 'Here we can select the POLICY_TAG_CO... that we just configured'. The 'Update & Apply to Device' button at the bottom right is also highlighted with a blue box.

Configuration > Wireless > Access Points

Configuration AP

General

AP Name* AP-9166I-E.1F20

Location* default location

Base Radio MAC 345d.a80b.c740

Ethernet MAC 149f.4310.1f20

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 POLICY_TAG_CO...

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

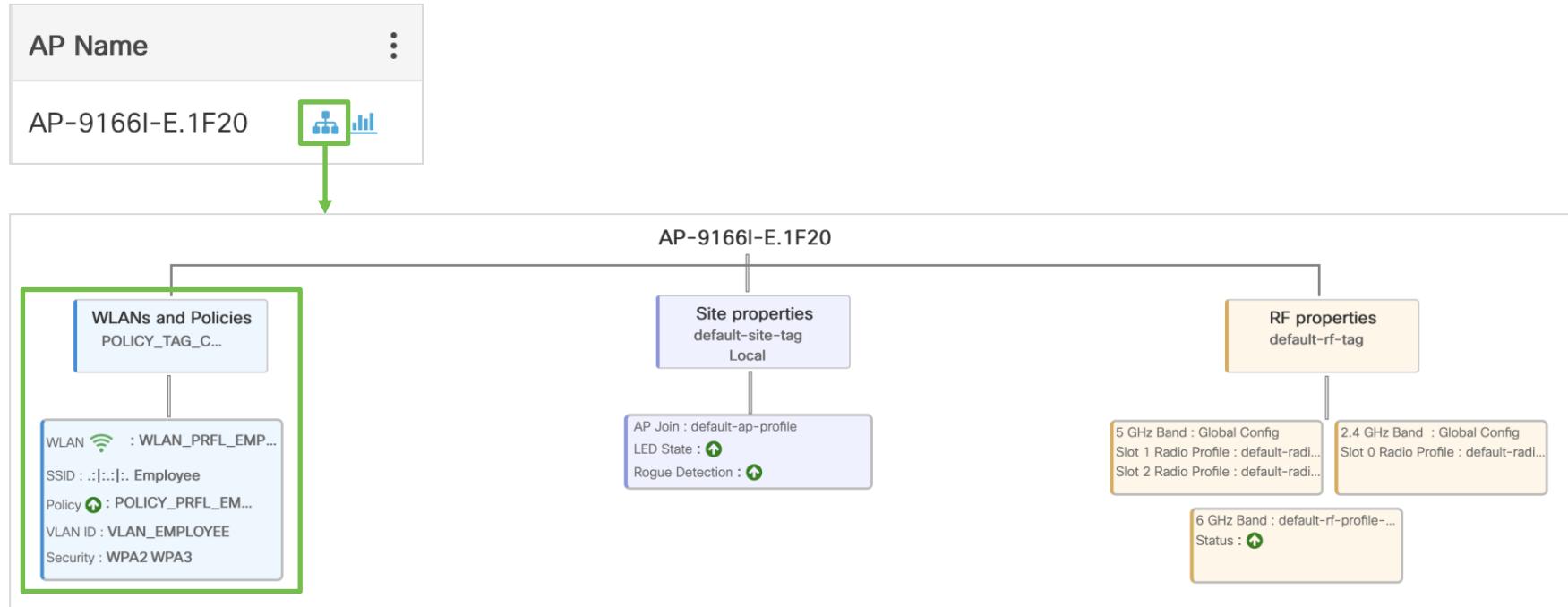
Mini IOS Version

IP Config

CAPWAP Preferred Mode IPv4

Update & Apply to Device

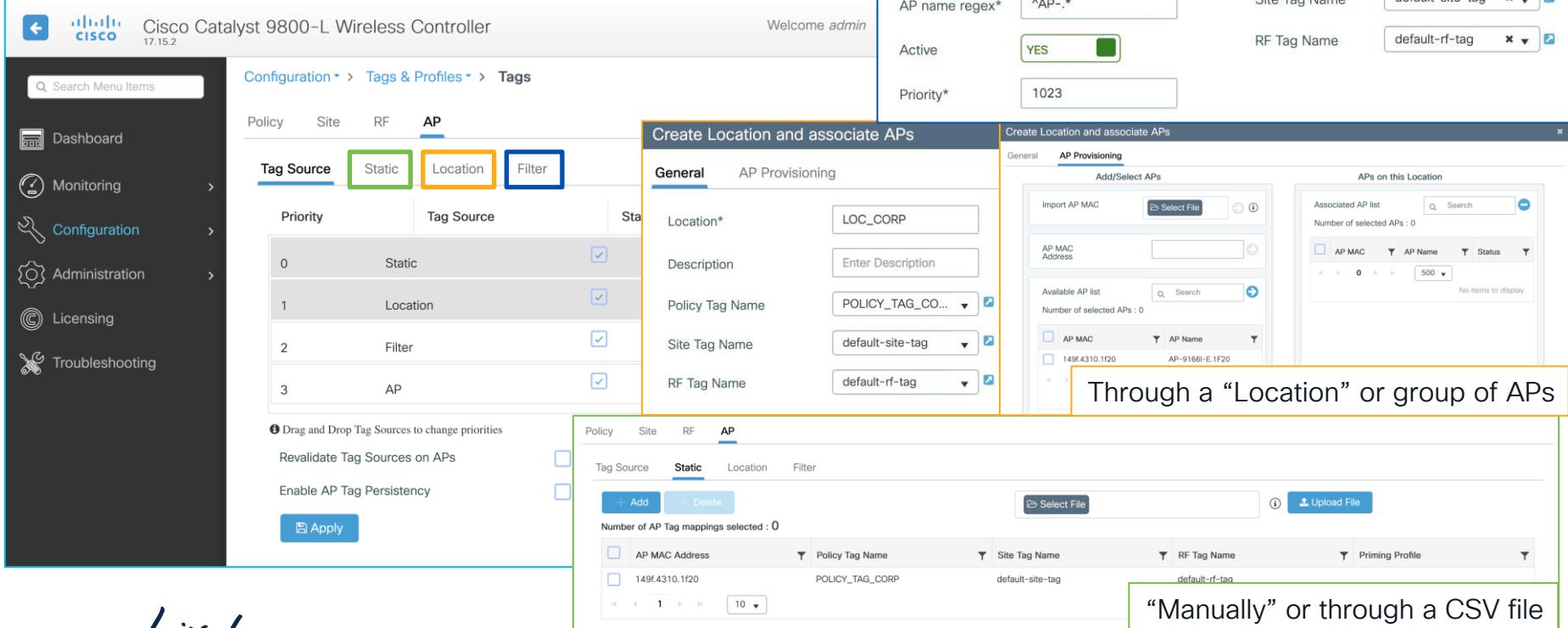
Checking Tags and Profiles assignment



Other options to assign Tags

Through regex rules for the AP names

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



The screenshot shows the Cisco Catalyst 9800-L Wireless Controller interface under Configuration > Tags & Profiles > Tags > AP > Tag Source. The AP tab is selected. The Tag Source section has three tabs: Tag Source (selected), Static, and Location. The Location tab is highlighted with an orange box. The Location tab displays a table with four rows: 0 (Static), 1 (Location), 2 (Filter), and 3 (AP). Each row has a checkbox in the 'Tag Source' column. Below the table are three buttons: 'Drag and Drop Tag Sources to change priorities', 'Revalidate Tag Sources on APs', and 'Enable AP Tag Persistence'. A 'Select File' button and an 'Upload File' button are also present. A green box highlights the 'AP' tab in the main navigation bar.

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

AP

Tag Source Static Location Filter

Priority Tag Source

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

Select File Upload File

AP

Tag Source Static Location Filter

+ Add × Delete

Number of AP Tag mappings selected : 0

AP MAC Address	Policy Tag Name	Site Tag Name	RF Tag Name	Priming Profile
149f.4310.1f20	POLICY_TAG_CORP	default-site-tag	default-rf-tag	

Associate Tags to AP

Rule Name* FILTER_CORP

AP name regex* ^AP_.*

Active YES

Priority* 1023

Policy Tag Name POLICY_TAG_CO...

Site Tag Name default-site-tag

RF Tag Name default-rf-tag

Create Location and associate APs

General AP Provisioning

Location* LOC_CORP

Description Enter Description

Policy Tag Name POLICY_TAG_CO...

Site Tag Name default-site-tag

RF Tag Name default-rf-tag

Create Location and associate APs

General AP Provisioning

Add/Select APs

Import AP MAC

AP MAC Address

Available AP list

Number of selected APs : 0

AP MAC AP Name

149f.4310.1f20	AP-9166i-E.1F20
----------------	-----------------

Associated AP list

Number of selected APs : 0

AP MAC AP Name Status

149f.4310.1f20	AP-9166i-E.1F20	
----------------	-----------------	--

Through a “Location” or group of APs

“Manually” or through a CSV file

Enabling Tags persistency



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

Cisco Catalyst 9800-L Wireless Controller
17.15.2 Welcome admin

Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Licensing

Troubleshooting

Configuration > Tags & Profiles > Tags

Policy Site RF AP

Tag Source Static Location Filter

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

Drag and Drop Tag Sources to change priorities

Revalidate Tag Sources on APs

Enable AP Tag Persistency

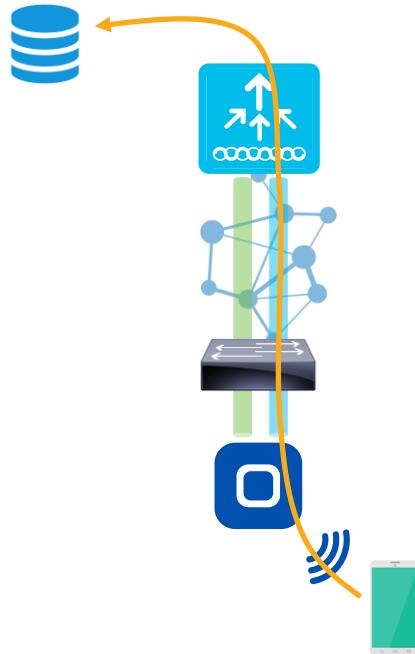
Apply

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

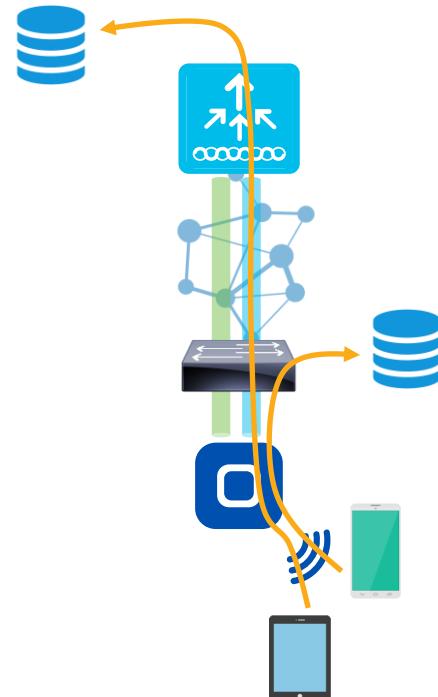
The same Tags must be present on the new destination controller and they are applied according to the AP's memory if no other mappings (static, filter, etc.) supersede them

Central or (FlexConnect) Local Switching

Local Mode AP
(Central Switching)



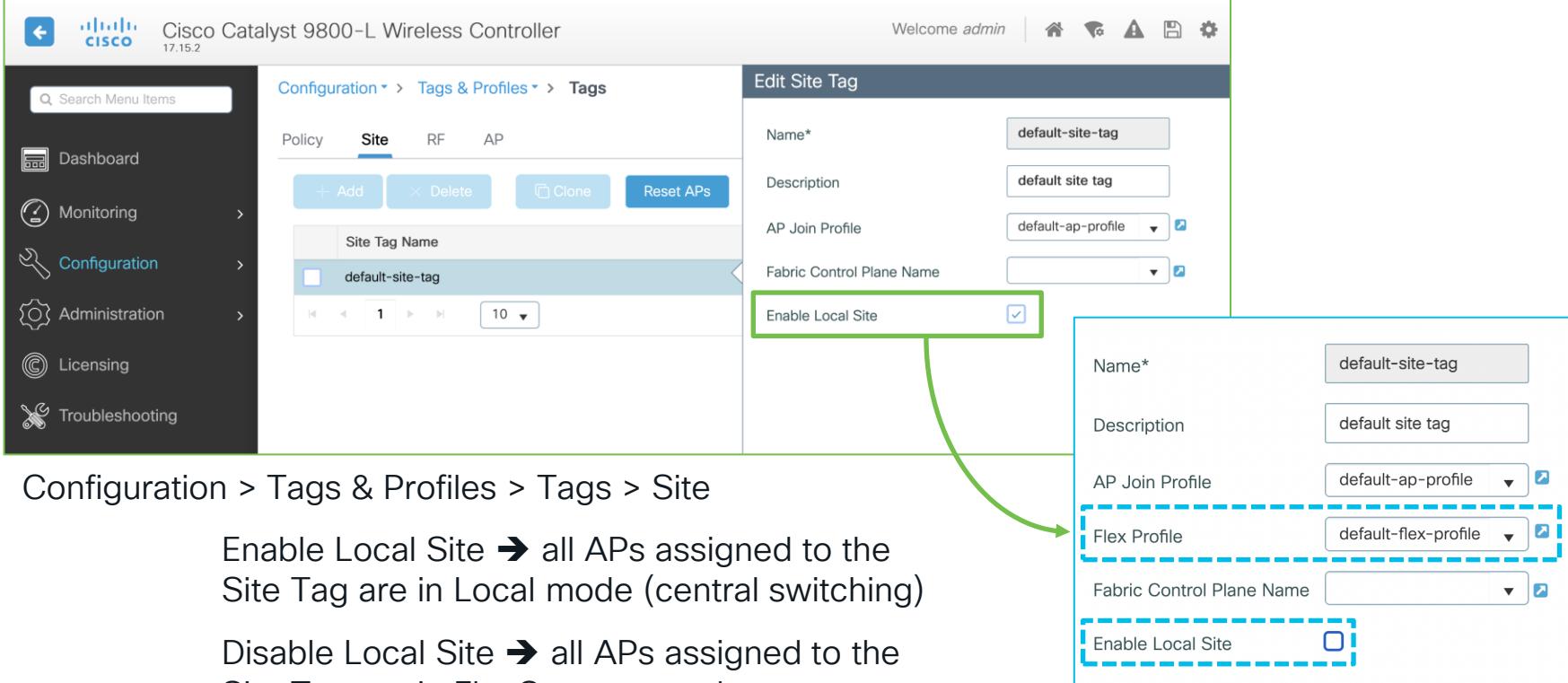
FlexConnect mode AP
(Central / Local Switching)



CAPWAP Control
 CAPWAP Data

Going FlexConnect

1. The AP must be in FlexConnect mode



The screenshot shows the Cisco Catalyst 9800-L Wireless Controller interface. The left sidebar includes links for Dashboard, Monitoring, Configuration (selected), Administration, Licensing, and Troubleshooting. The main area shows the 'Configuration > Tags & Profiles > Tags > Site' path. The 'Site' tab is selected. A list of Site Tags shows 'default-site-tag' selected. A detailed 'Edit Site Tag' dialog is open for this tag. In the edit dialog, the 'Enable Local Site' checkbox is checked and highlighted with a green border. In the main configuration area, this checkbox is also checked and highlighted with a green border. A green arrow points from the checked checkbox in the main area to the checked checkbox in the edit dialog. A blue dashed box highlights the 'Flex Profile' and 'Enable Local Site' fields in the edit dialog, indicating they are specific to FlexConnect mode.

Cisco Catalyst 9800-L Wireless Controller
17.15.2

Configuration > Tags & Profiles > Tags > Site

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

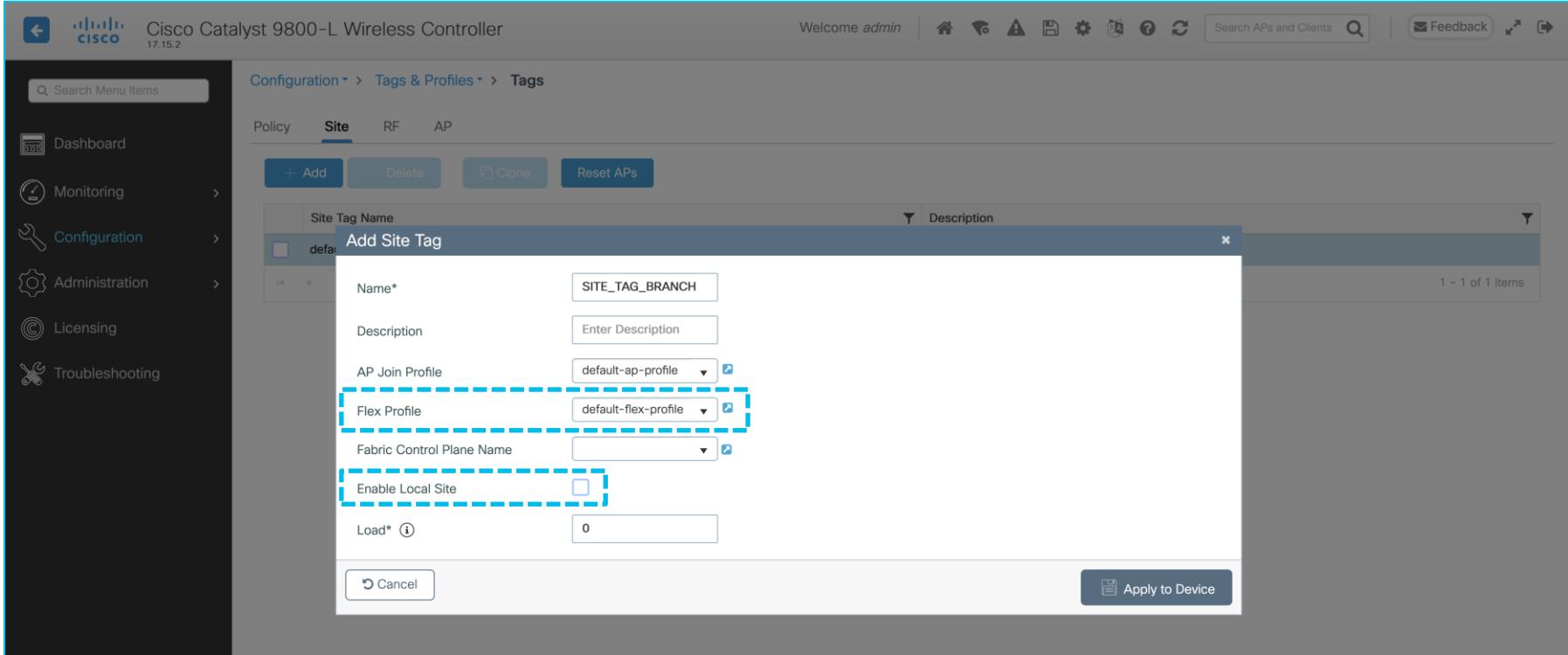
Disable Local Site → all APs assigned to the Site Tag are in FlexConnect mode

Edit Site Tag	
Name*	default-site-tag
Description	default site tag
AP Join Profile	default-ap-profile
Fabric Control Plane Name	
Enable Local Site	<input checked="" type="checkbox"/>

Site Tag	
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	<input type="checkbox"/>

Going FlexConnect

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



The screenshot shows the Cisco Catalyst 9800-L Wireless Controller web interface. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration (selected), Administration, Licensing, and Troubleshooting. The main content area is titled 'Configuration > Tags & Profiles > Tags'. A sub-menu bar at the top of the content area shows 'Policy', 'Site' (selected), 'RF', and 'AP'. Below this are buttons for '+ Add', 'Delete', 'Clone', and 'Reset APs'. A modal dialog box is open, titled 'Add Site Tag'. The dialog contains the following fields:

- Name***: SITE_TAG_BRANCH
- Description**: Enter Description
- AP Join Profile**: default-ap-profile
- Flex Profile**: default-flex-profile (highlighted with a blue dashed box)
- Fabric Control Plane Name**: (dropdown menu)
- Enable Local Site**: (checkbox, highlighted with a blue dashed box)
- Load***: 0

At the bottom of the dialog are 'Cancel' and 'Apply to Device' buttons. The background of the main interface shows a table with one item: '1 - 1 of 1 items'.

Configuration > Tags & Profiles > Tags > Site

Going FlexConnect

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

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller interface. On the left, the navigation menu includes Dashboard, Monitoring, Configuration (selected), Administration, Licensing, and Troubleshooting. The main content area shows the 'Configuration > Wireless > Access Points' section. Under 'All Access Points', there is one entry: AP Name: AP-9166I-E.1F20, AP Model: CW9166I-E, Slots: 3, Admin Status: Enabled. Below this, sections for 6 GHz Radios and 5 GHz Radios are shown. On the right, the 'Edit AP' dialog is open for the selected AP. The 'General' tab is selected, showing fields for AP Name (AP-9166I-E.1F20), Location (default location), Base Radio MAC (345d.a80b.c740), Ethernet MAC (149f.4310.1f20), Admin Status (ENABLED), AP Mode (Local), Operation Status (Registered), and Fabric Status (Disabled). The 'Tags' tab is also visible, containing a warning about changing tags and a dropdown menu for Site Tags. A blue box highlights the 'SITE_TAG_BRANCH' dropdown, and a blue arrow points from this box to the text below.

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
17.15.2

Configuration > Tags & Profiles > Tags

Policy Site RF AP

Tag Source Static Location Filter

+ Add × Delete

Priority Rule

Rule Name* RULE_FLEX_DEFAULT

AP name regex*

Active YES

Priority* 1023

Type Tag

Policy Tag Name Search or Select

Site Tag Name SITE_TAG_BRAN .x

RF Tag Name Search or Select

Associate Tags to AP

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

Cisco Catalyst 9800-L Wireless Controller

Welcome admin

Search APs

Configuration > Tags & Profiles > Policy

Add Policy Profile

General

Name*: '_PRFL_EMPLOYEE_FLEX'

Description: Enter Description

Status: ENABLED

Passive Client: DISABLED

IP MAC Binding: ENABLED

Encrypted Traffic Analytics: DISABLED

WLAN Switching Policy

Central Switching: DISABLED

Central Authentication: ENABLED

Central DHCP: DISABLED

Flex NAT/PAT: DISABLED

CTS Policy

Inline Tagging:

SGACL Enforcement:

Default SGT: 2-65519

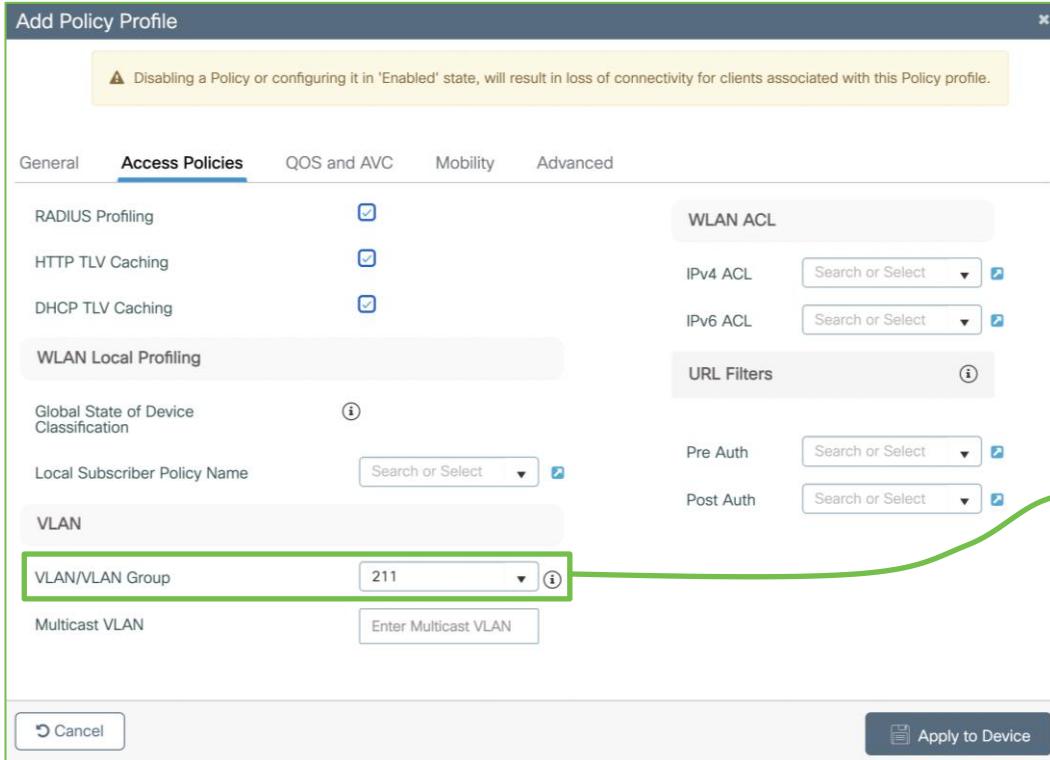
Cancel

Apply to Device

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)



Configuration > Tags & Profiles > Policy

CISCO Live!

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

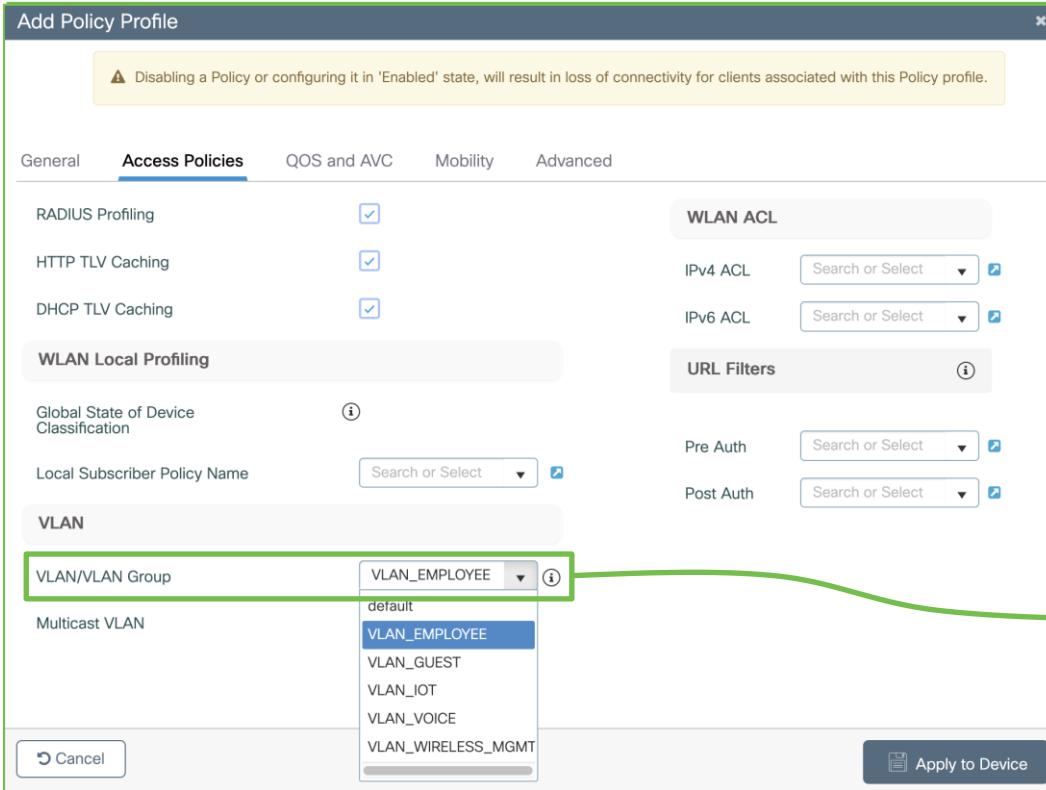
If you are not dynamically assigning VLANs via RADIUS, you can define the locally switched VLAN under the Access Policies tab of the Policy Profile. Be aware that:

- 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)



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)

Configuration > Tags & Profiles > Flex

VLAN Name	ID	Ingress ACL	Egress ACL
VLAN_EMPLOYEE	110		

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



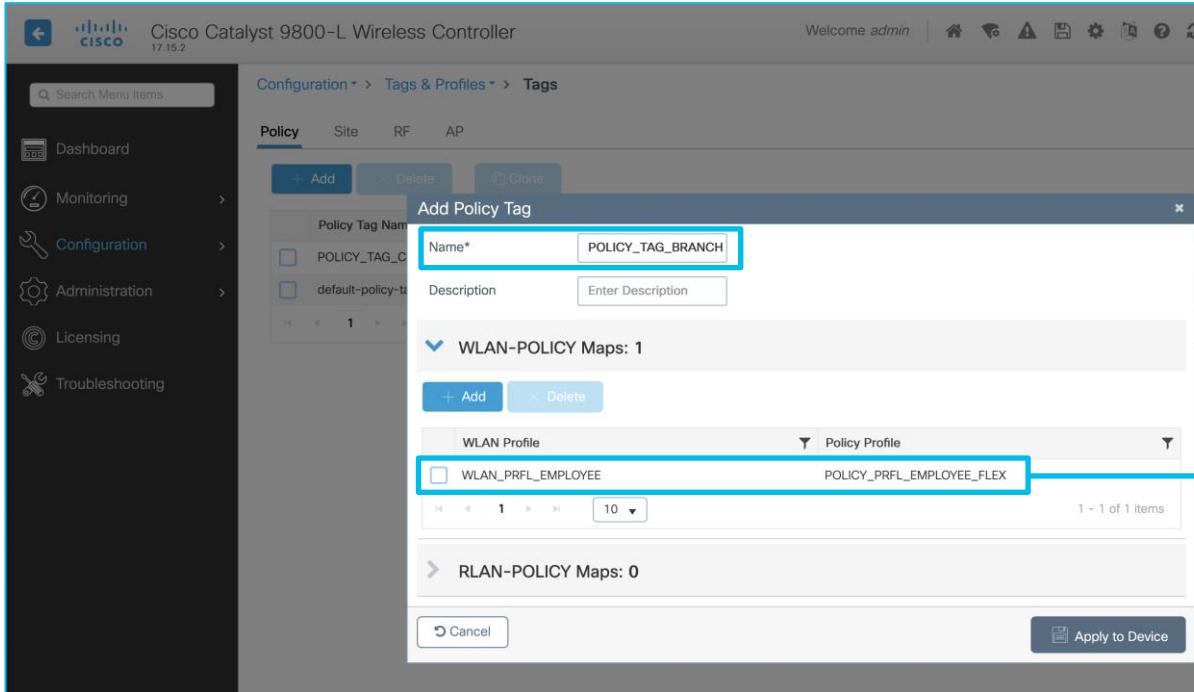
Configuration > Tags & Profiles > Flex

The screenshot shows the 'Edit Flex Profile' dialog for a 'default-flex-profile'. The 'Native VLAN ID' field is set to '20'. 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' (disabled), 'Inline Tagging' (disabled), 'SGACL Enforcement' (disabled), and 'CTS Profile Name' (default-sxp-p ...).

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 'Add Policy Tag' dialog box. The 'Name*' field is filled with 'POLICY_TAG_BRANCH'. Under 'WLAN-POLICY Maps: 1', there is one entry: 'WLAN_PRFL_EMPLOYEE' (WLAN Profile) is paired with 'POLICY_PRFL_EMPLOYEE_FLEX' (Policy Profile). A blue arrow points from the 'POLICY_PRFL_EMPLOYEE_FLEX' text to the explanatory text on the right.

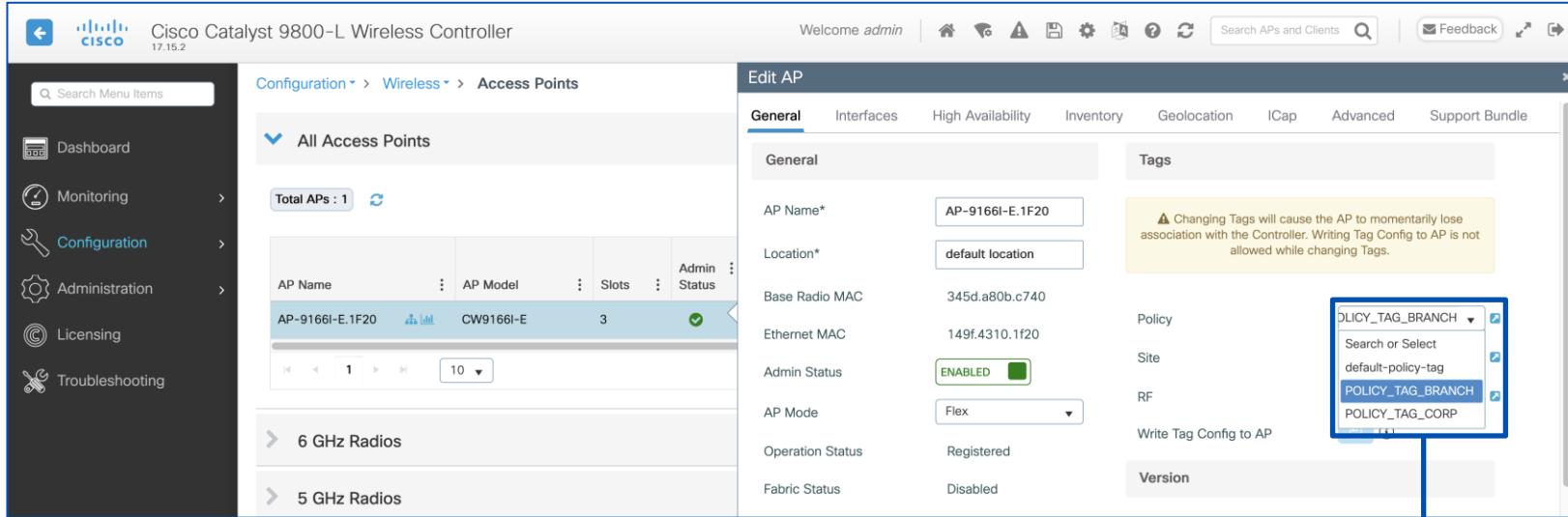
Configuration > Tags & Profiles > Tags > Policy

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

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 left sidebar includes links for Dashboard, Monitoring, Configuration (which is selected), Administration, Licensing, and Troubleshooting. The main content area shows 'All Access Points' with a total of 1 AP. The selected AP is AP-9166I-E.1F20, which is a CW9166I-E model with 3 slots and an enabled admin status. The 'Edit AP' dialog is open, specifically the 'General' tab. In the 'Tags' section, 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.' Below this, the 'Policy' dropdown is set to 'POLICY_TAG_BRANCH', with other options like 'default-policy-tag', 'POLICY_TAG_CORP', and 'POLICY_TAG_BRANCH' (repeated) visible. The 'Version' field is also present.

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.

Configuring a passphrase based WLAN Profile

Configuration > Tags & Profiles > WLANs > Add

Cisco Catalyst 9800-L Wireless Controller

Configuration > WLANs > Add WLAN

General Security Advanced

Profile Name* WLAN_PRFL_IOT

SSID* .:.; IoT

WLAN ID* 2

Status **ENABLED**

Broadcast SSID **ENABLED**

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

General Security Advanced

Layer2 Layer3 AAA

WPA3 To review the necessary considerations for ensuring WLAN compatibility with Wi-Fi 7 security [click here](#).

WPA + WPA2 WPA2 + WPA3 **WPA3** Static WEP None

MAC Filtering

Lobby Admin Access

WPA Parameters

WPA Policy WPA2 Policy WPA3 Policy Beacon Protection

GTK Randomize WPA3 Policy

Transition Disable

Fast Transition

Status **Enabled**

Over the DS

Reassociation Timeout* 20

WPA2/WPA3 Encryption

AES(CCMP128) CCMP256 GCM128 GCMP256

Protected Management Frame

PMF **Required**

Association Comeback Timer* 1

SA Query Time* 200

Auth Key Mgmt (AKM)

FT + 802.1X 802.1X-SHA256 SUITE192-1X OWE SAE FT + SAE SAE-EXT-KEY FT + SAE-EXT-KEY

Anti Clogging Threshold* 1500

Max Retries* 5

Retransmit Timeout* 400

PSK Format **ASCII**

PSK Type **Unencrypted**

Pre-Shared Key* Both H2E and...

SAE Password Element

Zoom on Layer 2 Security for Wi-Fi 7 support

The screenshot shows the Cisco WPA3 configuration interface for Layer 2 security. Key settings highlighted with blue boxes include:

- WPA Parameters:** Beacon Protection is checked.
- WPA2/WPA3 Encryption:** AES(CCMP128) and GCMP256 are checked.
- Protected Management Frame:** PMF is set to Required.
- Fast Transition:** Status is set to Enabled.
- Auth Key Mgmt (AKM):** SAE and FT + SAE are checked.

WPA3 settings:

- Beacon Protection
- AES(CCMP128)
- GCMP256

PMF: Required (for Device Analytics too)

Fast Transition: Enabled

AKM:

- SAE, FT + SAE
- SAE-EXT-KEY, FT + SAE-EXT-KEY

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

WPA2 PSK + WPA3 SAE (no Wi-Fi 7)



General **Security** Advanced

Layer2 Layer3 AAA

⚠ To review the necessary considerations for ensuring WLAN compatibility with Wi-Fi 7 security [click here](#).

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering

Lobby Admin Access

WPA Parameters

WPA Policy <input type="checkbox"/>	WPA2 Policy <input checked="" type="checkbox"/>
GTK Randomize <input type="checkbox"/>	WPA3 Policy <input checked="" type="checkbox"/>
Transition Disable <input type="checkbox"/>	Beacon Protection <input type="checkbox"/>

WPA2/WPA3 Encryption

AES(CCMP128) <input checked="" type="checkbox"/>	CCMP256 <input type="checkbox"/>
GCM128 <input type="checkbox"/>	GCM256 <input type="checkbox"/>

Protected Management Frame

PMF Optional

Association Comeback Timer* 1

SA Query Time* 200

Fast Transition

Status Enabled

Over the DS

Reassociation Timeout* 20

Auth Key Mgmt (AKM)

802.1X <input type="checkbox"/>	FT + 802.1X <input type="checkbox"/>
802.1X-SHA256 <input type="checkbox"/>	CCKM <input checked="" type="checkbox"/>
PSK <input checked="" type="checkbox"/>	FT + PSK <input checked="" type="checkbox"/>
PSK-SHA256 <input type="checkbox"/>	SAE <input checked="" type="checkbox"/>
FT + SAE <input checked="" type="checkbox"/>	SAE-EXT-KEY <input type="checkbox"/>
FT + SAE-EXT-KEY <input type="checkbox"/>	

Anti Clogging Threshold* 1500

Max Retries* 5

Retransmit Timeout* 400

PSK Format ASCII

PSK Type Unencrypted

Pre-Shared Key*

SAE Password Element Both H2E and...

Still supporting 6 GHz / Wi-Fi 6E

WPA2/WPA3 settings:

- AES(CCMP128)

PMF: Optional (for Device Analytics too)

Fast Transition: Enabled

AKM:

- PSK, FT + PSK
- SAE, FT + SAE

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

Policy Profile similar to the “Employee” one

We could in fact just clone the previous Policy Profile, give it another name and assign it to another VLAN (disable RADIUS related settings too, if not needed):

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller interface. On the left, the navigation bar includes Dashboard, Monitoring, Configuration (selected), Administration, Licensing, and Troubleshooting. The main area shows the 'Configuration > Tags & Profiles > Policy' section. A list of policy profiles is displayed, with 'POLICY_PRFL_EMPLOYEE' selected and highlighted with a green box. The 'Clone' button is also highlighted with a green box. A modal window titled 'Clone of Policy Profile (POLICY_PRFL_EMPLOYEE)' is open, showing the cloned profile 'POLICY_PRFL_IOT'. The 'Access Policies' tab is selected, showing that RADIUS Profiling is disabled. The 'VLAN' tab is open, showing a dropdown menu for 'VLAN/VLAN Group' with 'VLAN_IOT' selected and highlighted with a blue box. Other options in the dropdown include 'default', 'VLAN_EMPLOYEE', 'VLAN_GUEST', 'VLAN_VOICE', and 'VLAN_WIRELESS_MGMT'. The 'Apply to Device' button is at the bottom right of the modal.

Add the WLAN and Policy Profiles to the Policy Tag

Configuration > Tags & Profiles > Tags > Policy

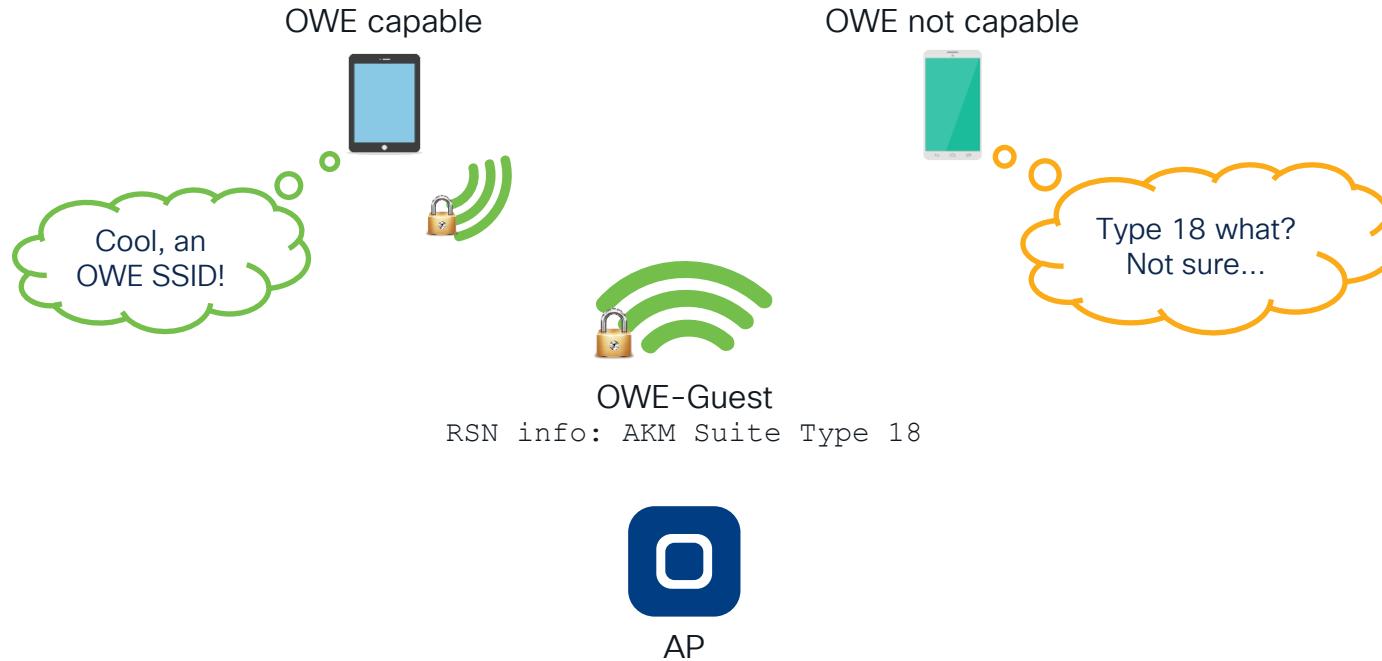
The screenshot shows the Cisco Catalyst 9800-L Wireless Controller interface. The left sidebar includes links for Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main navigation bar shows 'Configuration > Tags & Profiles > Tags'. The 'Policy' tab is selected. On the left, a list of Policy Tags shows 'POLICY_TAG_CORP' selected. The right side displays the 'Edit Policy Tag' dialog box. The 'Name*' field is set to 'POLICY_TAG_CORP'. The 'Description' field is empty, with a placeholder 'Enter Description'. Under 'WLAN-POLICY Maps: 1', there is one entry: 'WLAN Profile' 'WLAN_PRFL_EMPLOYEE' is paired with 'Policy Profile' 'POLICY_PRFL_EMPLOYEE'. The 'Map WLAN and Policy' section shows 'WLAN Profile*' 'WLAN_PRFL_IOT' and 'Policy Profile*' 'POLICY_PRFL_IOT'. The bottom right of the dialog box contains a 'Cancel' button and a large 'Update & Apply to Device' button.

Add the WLAN and Policy Profiles to the Policy Tag

Configuration > Tags & Profiles > Tags > Policy

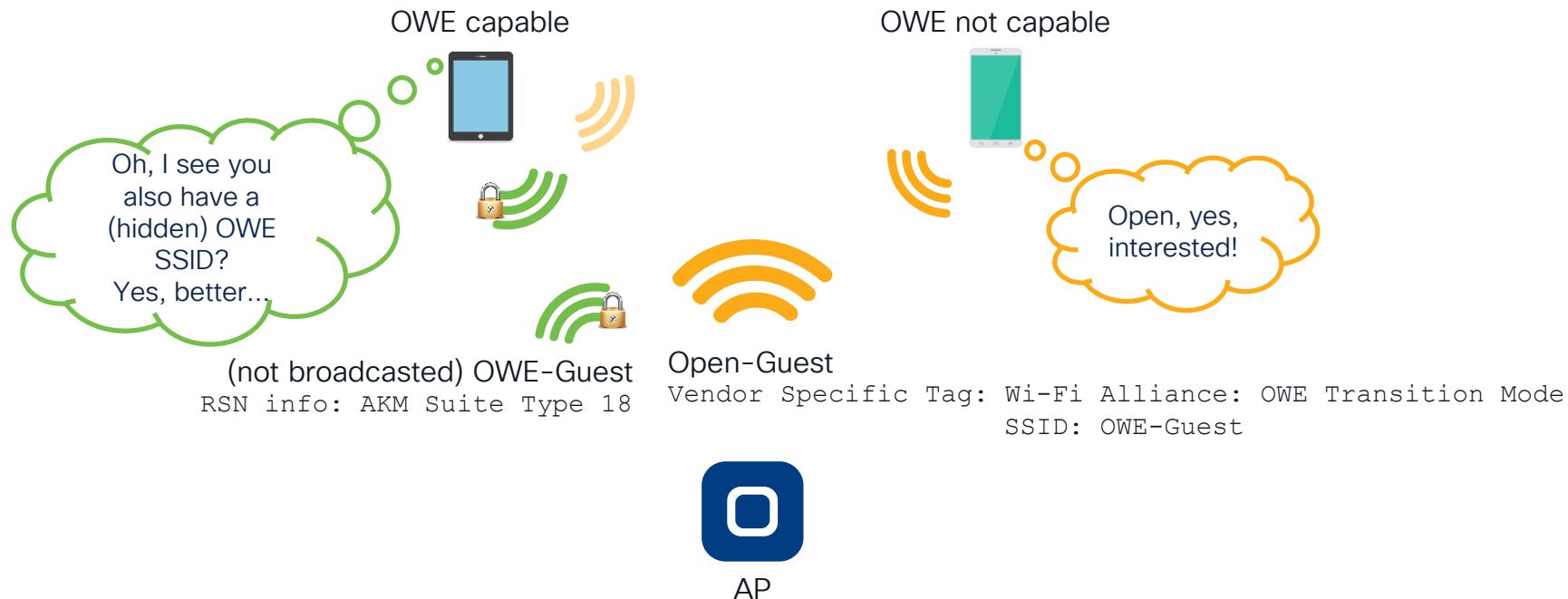
The screenshot shows the Cisco Catalyst 9800-L Wireless Controller interface. The left sidebar includes links for Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main navigation bar shows 'Configuration > Tags & Profiles > Tags'. The 'Policy' tab is selected. On the left, a list of Policy Tags is shown, with 'POLICY_TAG_BRANCH' selected. The right side displays the 'Edit Policy Tag' dialog box. The 'Name*' field is set to 'POLICY_TAG_BRANCH'. The 'Description' field is empty. Under 'WLAN-POLICY Maps: 1', there is one entry: 'WLAN Profile' is 'WLAN_PRFL_EMPLOYEE' and 'Policy Profile' is 'POLICY_PRFL_EMPLOYEE_FLEX'. The 'Map WLAN and Policy' section shows 'WLAN Profile*' as 'WLAN_PRFL_IOT' and 'Policy Profile*' as 'POLICY_PRFL_IOT'. The 'RLAN-POLICY Maps: 0' section is empty. At the bottom are 'Cancel' and 'Update & Apply to Device' buttons.

Opportunistic Wireless Encryption (OWE)



OWE Transition Mode

Not supported for 6 GHz / Wi-Fi 6E / Wi-Fi 7



Adding a Guest SSID (LWA with internal portal)

Configuration > Security > ACL

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller interface. The left sidebar includes links for Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main navigation bar shows 'Configuration > Security > ACL'. A sub-menu for 'ACL' is open, showing a list of existing ACLs: 'ACL_LWA_INTERNAL_PORTAL' (selected), 'ACL_LWA_EXTERNAL_PORTAL', and 'ACL_WIRELESS_CLIENT'. The 'Edit ACL' dialog is open for 'ACL_LWA_INTERNAL_PORTAL'. The 'ACL Name' is set to 'ACL_LWA_INTERNAL_PORTAL' and the 'ACL Type' is 'IPv4 Extended'. The 'Rules' section shows three entries: a permit rule for UDP port 67 (bootps), another permit rule for UDP port 53 (domain), and a deny rule for IP port 0 (any). The 'Log' and 'DSCP' fields are set to 'None'. The table below shows the detailed configuration of these rules.

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
10	permit	any			any	udp	None	eq bootps	None	Disabled
20	permit	any			any	udp	None	eq domain	None	Disabled
30	deny	any			any	ip	None	None	None	Disabled

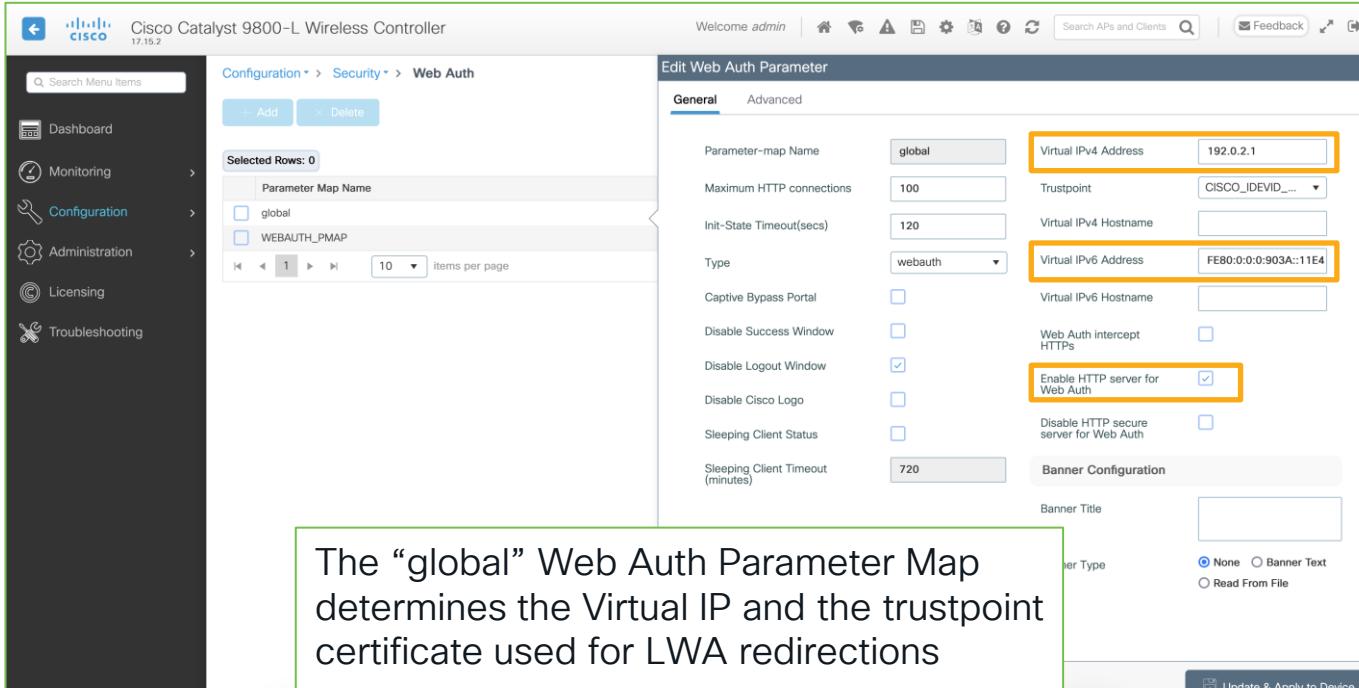
At the bottom of the dialog, there are 'Add' and 'Delete' buttons, and a 'Cancel' button.

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

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 Cisco Catalyst 9800-L Wireless Controller interface. On the left, the navigation bar includes 'Dashboard', 'Monitoring', 'Configuration' (which is selected), 'Administration', 'Licensing', and 'Troubleshooting'. The main area shows 'Selected Rows: 0' and a list of 'Parameter Map Name' with 'global' and 'WEBAUTH_PMAP' selected. The 'Edit Web Auth Parameter' dialog is open, showing the 'General' tab. Key settings include:

- Parameter-map Name: global
- Virtual IPv4 Address: 192.0.2.1
- Trustpoint: CISCO_IDEVID...
- Virtual IPv6 Address: FE80:0:0:903A::11E4
- Type: webauth
- Captive Bypass Portal: (checkbox)
- Disable Success Window: (checkbox)
- Disable Logout Window: (checkbox) checked
- Disable Cisco Logo: (checkbox)
- Sleeping Client Status: (checkbox)
- Sleeping Client Timeout (minutes): 720
- Enable HTTP server for Web Auth: (checkbox) checked
- Disable HTTP secure server for Web Auth: (checkbox)
- Banner Configuration: (checkbox) None
- Banner Title: (input field)
- Banner Type: (radio buttons) None, Banner Text, Read From File

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

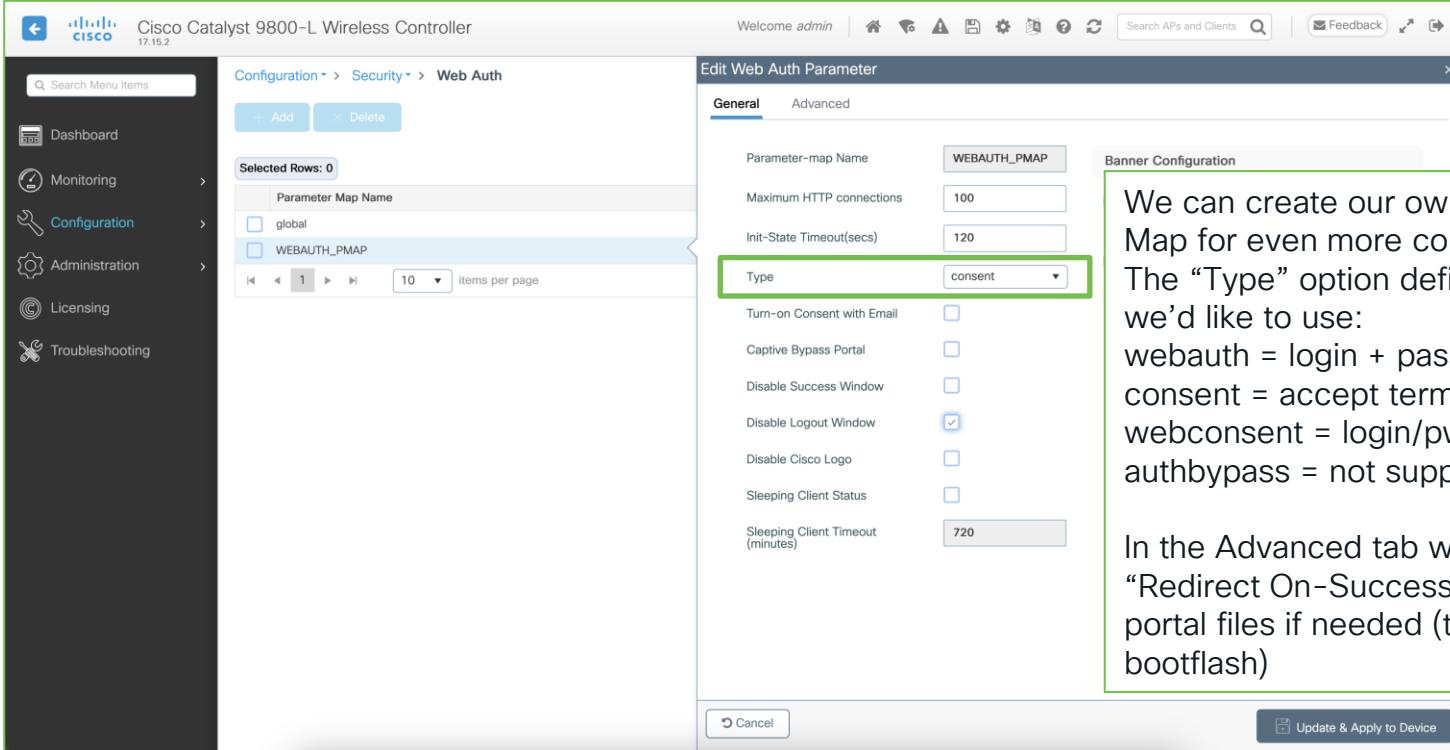
Other custom Web Auth Parameter Maps will inherit these settings

Recommended:

- Always configure a Virtual IPv4 (192.0.2.1) and IPv6 (FE80:0:0:903A::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's configuration interface. The left sidebar includes links for Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main navigation bar shows 'Configuration > Security > Web Auth'. The 'Edit Web Auth Parameter' dialog is open, showing the 'General' tab. It displays a 'Parameter-map Name' of 'WEBAUTH_PMAP', a 'Maximum HTTP connections' of '100', and an 'Init-State Timeout(secs)' of '120'. The 'Type' dropdown is set to 'consent'. Below these are several configuration options with checkboxes: '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)' set to '720'. At the bottom of the dialog are 'Cancel' and 'Update & Apply to Device' buttons. A green box highlights the 'Type' dropdown. To the right of the dialog, a text box provides information about the 'Type' options: 'consent' (accept terms and conditions), 'webauth' (login + password), 'webconsent' (login/pwd + terms & conditions), and 'authbypass' (not supported). It also mentions the 'Advanced' tab for redirect URLs and custom portal files.

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)

Administration > Management > File Manager

bootflash:/custom-portals

yourlogo.jpg logout.html loginscript.js failed.html consent.html aup.html

Edit Web Auth Parameter

General Advanced

Preview of the Redirect URL:
https://192.0.2.1/login.html?redirect=<website-name> https://fe80::903a:0:0:11e4/login.html?redirect=<website-name>

Redirect to external server

Redirect URL for login: https://www.cisco.com

Redirect On-Success:

Redirect On-Failure:

Redirect Append for AP MAC Address:

Redirect Append for Client MAC Address:

Redirect Append for WLAN SSID:

Portal IPV4 Address:

Portal IPV6 Address: XXXXX:XX

Customized page

Login Failed Page: bootflash:/custom-portals/failed.html

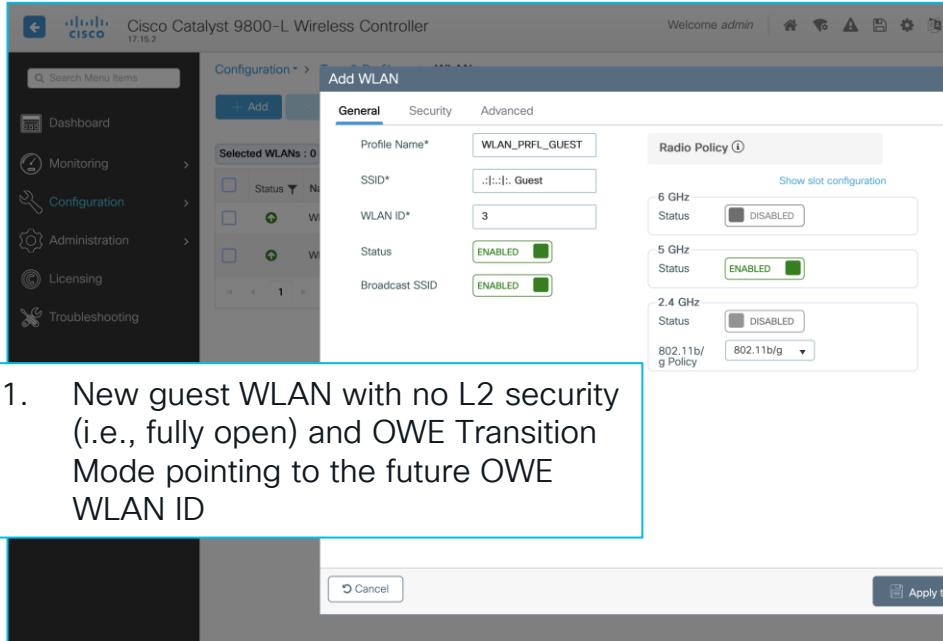
Login Page: bootflash:/custom-portals/consent.html

Logout Page: bootflash:/custom-portals/logout.html

Login Successful Page: --Select--

Adding a Guest SSID (LWA with internal portal)

Configuration > Security > Web Auth



Cisco Catalyst 9800-L Wireless Controller
17.15.2

Configuration > Add WLAN

General Security Advanced

Profile Name* WLAN_PRF1_GUEST

SSID* .1.1.1. Guest

WLAN ID* 3

Status ENABLED

Broadcast SSID ENABLED

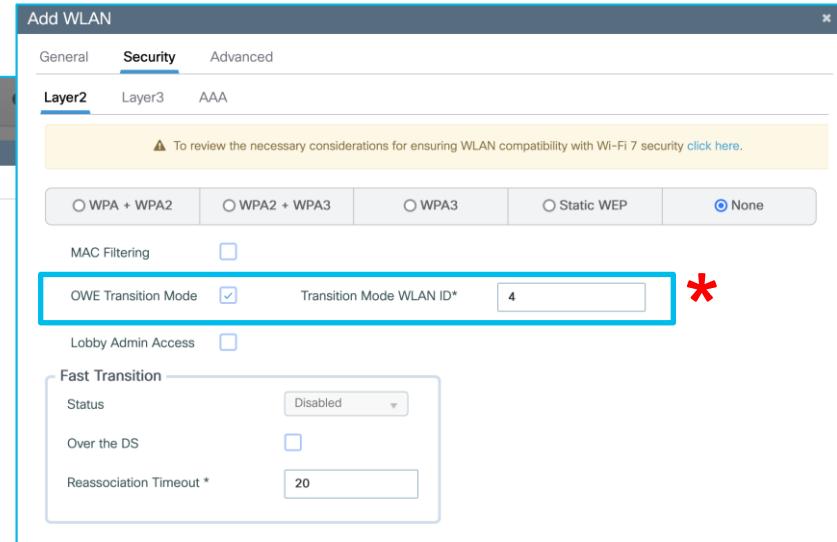
Radio Policy Show slot configuration

- 6 GHz Status DISABLED
- 5 GHz Status ENABLED
- 2.4 GHz Status DISABLED

802.11b/g Policy 802.11b/g

Cancel Apply to Device

1. New guest WLAN with no L2 security (i.e., fully open) and OWE Transition Mode pointing to the future OWE WLAN ID



Add WLAN

General Security Advanced

Layer2 Layer3 AAA

To review the necessary considerations for ensuring WLAN compatibility with Wi-Fi 7 security click here.

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering

OWE Transition Mode Transition Mode WLAN ID* 4 *

Lobby Admin Access

Fast Transition

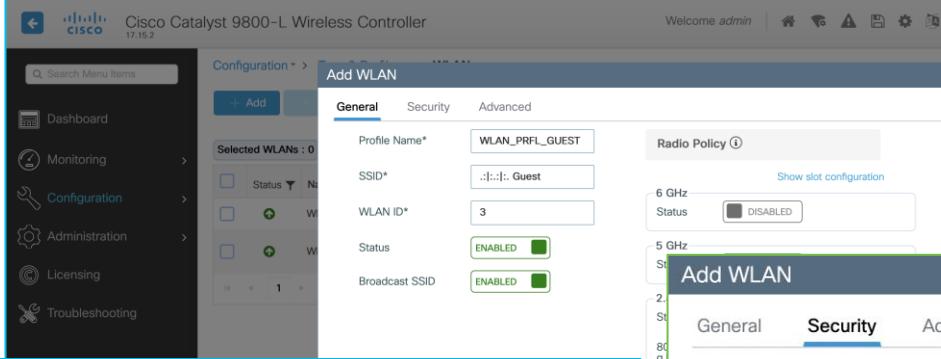
Status Disabled

Over the DS

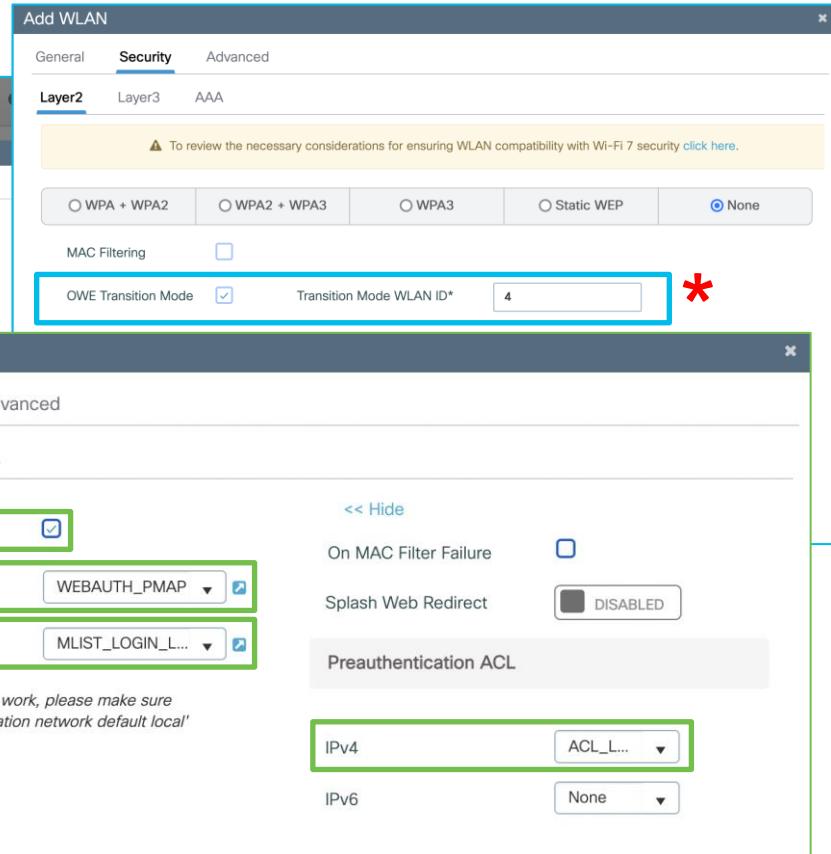
Reassociation Timeout * 20

Adding a Guest SSID (LWA with internal portal)

Configuration > Security > Web Auth



1. New guest WLAN with no L2 security (i.e., fully open) and OWE Transition Mode pointing to the future OWE WLAN ID
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

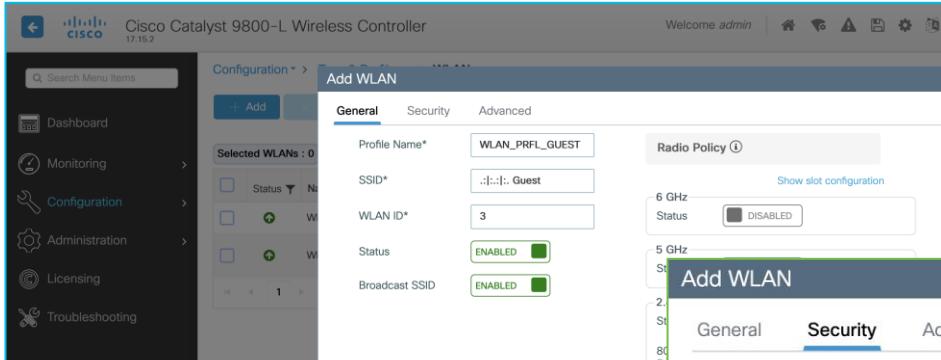


CISCO Live!

* OWE Transition Mode is not supported for 6 GHz / Wi-Fi 6E / Wi-Fi 7

Adding a Guest SSID (LWA with internal portal)

Configuration > Tags & Profiles > WLANs



1. New guest WLAN with no L2 security (i.e., fully open) and OWE Transition Mode pointing to the future OWE WLAN ID
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 further recommendation, we block P2P traffic too

The screenshots illustrate the configuration steps for a guest WLAN:

- Security Tab:** Shows OWE Transition Mode checked. A red asterisk and a callout note that OWE Transition Mode is not supported for 6 GHz / Wi-Fi 6E / Wi-Fi 7.
- Layer3 Tab:** Shows Web Policy and Web Auth Parameter Map selected.
- Advanced Tab:** Shows P2P Blocking Action set to 'Drop'.

CISCO Live!

*** OWE Transition Mode is not supported for 6 GHz / Wi-Fi 6E / Wi-Fi 7**

Adding the OWE Guest SSID

We could in fact clone the open guest WLAN Profile, give it another SSID name, disable broadcasting and enable 6 GHz too

The image shows two screenshots of the Cisco Catalyst 9800-L Wireless Controller interface. The left screenshot shows the 'WLANs' configuration page with a list of existing profiles: WLAN_PRFL_EMPLOYEE (ID 1), WLAN_PRFL_IOT (ID 2), and WLAN_PRFL_GUEST (ID 3). The 'Clone' button is highlighted with a green box. The right screenshot shows the 'Clone of WLAN Profile (WLAN_PRFL_GUEST)' dialog box. In the 'General' tab, the 'Profile Name' is set to 'WLAN_PRFL_GUEST_OWE', the 'SSID' is '.:.:.: Guest-OWE', the 'WLAN ID' is '4', and the 'Status' is 'ENABLED'. The 'Broadcast SSID' is set to 'DISABLED'. In the 'Radio Policy' section, the '6 GHz' radio is selected, showing 'Status: DISABLED' with a red asterisk indicating an error. The '5 GHz' and '2.4 GHz' sections show 'Status: ENABLED'. The '802.11b/g Policy' dropdown is set to '802.11b/g'. At the bottom are 'Cancel' and 'Apply to Device' buttons.

Zoom on Layer 2 Security

General **Security** Advanced

Layer2 Layer3 AAA

⚠ To review the necessary considerations for ensuring WLAN compatibility with Wi-Fi 7 security [click here](#).

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering

Lobby Admin Access

WPA Parameters

WPA Policy <input type="checkbox"/>	WPA2 Policy <input type="checkbox"/>
GTK Randomize <input type="checkbox"/>	WPA3 Policy <input checked="" type="checkbox"/>
Transition Disable <input type="checkbox"/>	Beacon Protection <input type="checkbox"/>

WPA2/WPA3 Encryption

AES(CCMP128) <input checked="" type="checkbox"/>	CCMP256 <input type="checkbox"/>
GCMP128 <input type="checkbox"/>	GCMP256 <input checked="" type="checkbox"/>

Protected Management Frame

PMF <input type="checkbox"/>	Required <input type="checkbox"/>
Association Comeback Timer* <input type="text" value="1"/>	
SA Query Time* <input type="text" value="200"/>	

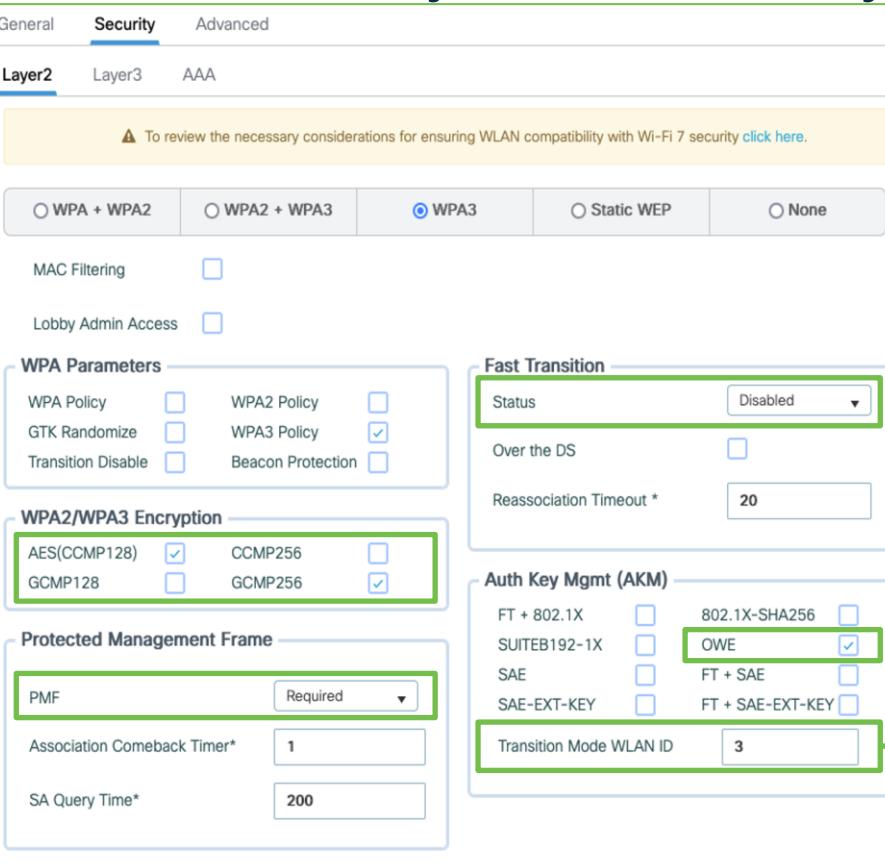
Fast Transition

Status <input type="checkbox"/>	Disabled
Over the DS <input type="checkbox"/>	
Reassociation Timeout *	20

Auth Key Mgmt (AKM)

FT + 802.1X <input type="checkbox"/>	802.1X-SHA256 <input type="checkbox"/>
SUITEB192-1X <input type="checkbox"/>	OWE <input checked="" type="checkbox"/>
SAE <input type="checkbox"/>	FT + SAE <input type="checkbox"/>
SAE-EXT-KEY <input type="checkbox"/>	FT + SAE-EXT-KEY <input type="checkbox"/>

Transition Mode WLAN ID



Note: for 6 GHz / Wi-Fi 6E / Wi-Fi 7 support, do not configure “Transition Mode” (to be disabled under the open SSID too) and enable “Beacon Protection” too

WPA3 settings:

- AES(CCMP128)

- GCMP256

PMF: Required

Fast Transition: Disabled

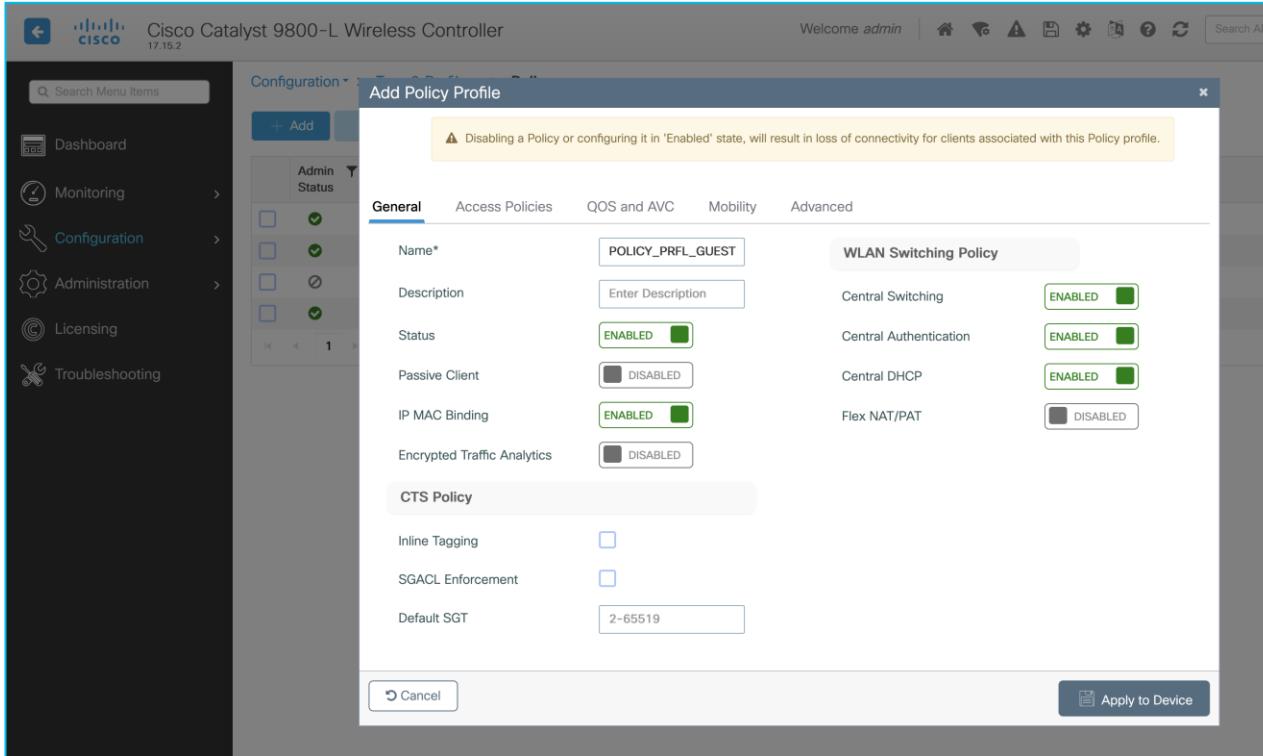
AKM: OWE

Transition Mode WLAN ID == the open WLAN ID *

* OWE Transition Mode is not supported for 6 GHz / Wi-Fi 6E / Wi-Fi 7

Adding a Guest SSID (LWA with internal portal)

Configuration > Tags & Profiles > Policy



Cisco Catalyst 9800-L Wireless Controller

Welcome admin | Home | Alerts | Configuration | Search APs

Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Licensing

Troubleshooting

Configuration > Tags & Profiles > Policy

Add Policy Profile

General

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

WLAN Switching Policy

Central Switching **ENABLED**

Central Authentication **ENABLED**

Central DHCP **ENABLED**

Flex NAT/PAT **DISABLED**

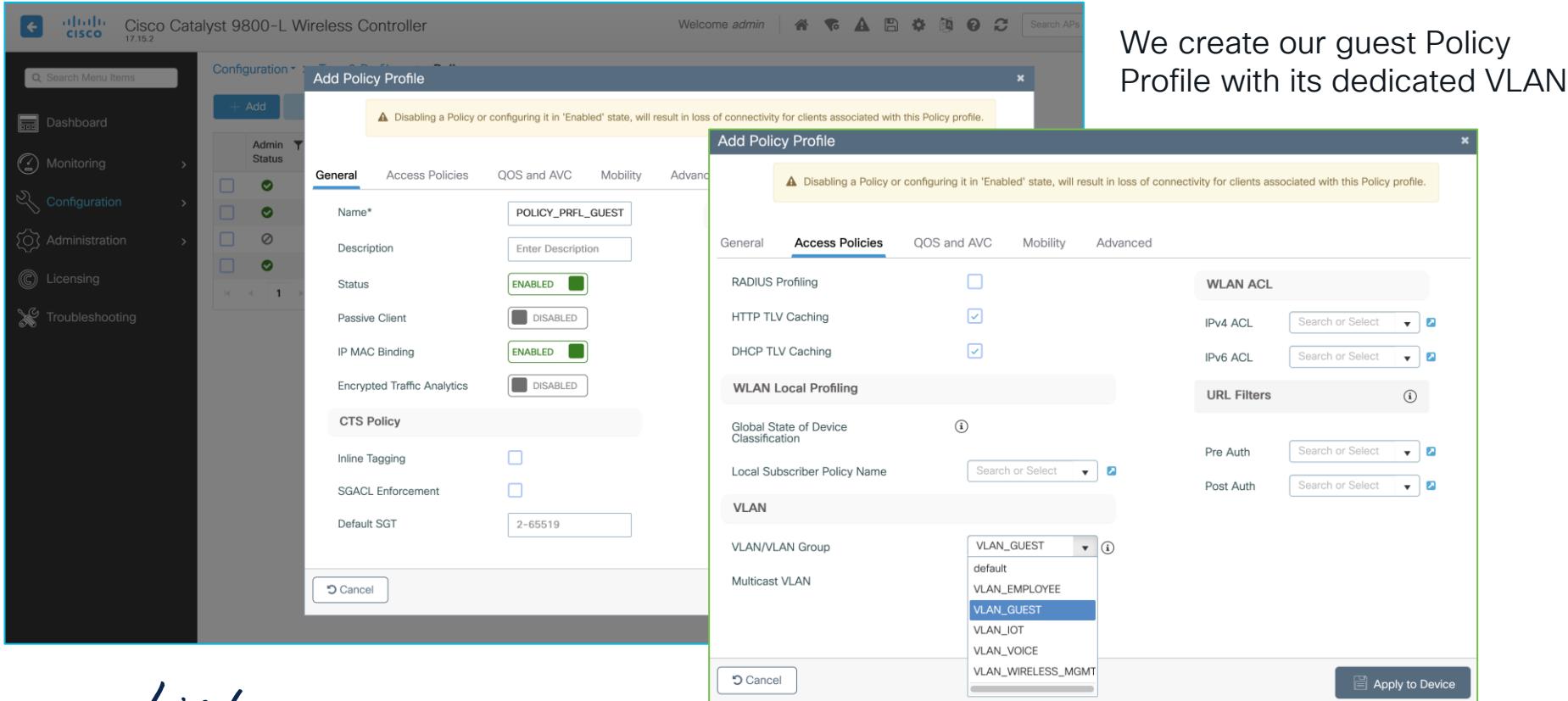
Cancel

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 interface. On the left, the navigation menu includes Dashboard, Monitoring, Configuration (selected), Administration, Licensing, and Troubleshooting. The main area shows the 'Add Policy Profile' dialog. The 'General' tab is selected, showing fields for Name (POLICY_PRFL_GUEST), Description (Enter Description), Status (ENABLED), and other options like Passive Client and IP MAC Binding. The 'Access Policies' tab is also shown, detailing RADIUS Profiling, WLAN ACL, and various caching and URL filtering options. A dropdown menu for the VLAN/VLAN Group field is open, showing options like default, VLAN_EMPLOYEE, VLAN_GUEST (which is selected), VLAN_IOT, VLAN_VOICE, and VLAN_WIRELESS_MGMT. A note at the top of both dialogs 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

CISCO Live!

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	<input type="checkbox"/>

Fabric Profile Search or Select

Link-Local Bridging

mDNS Service Policy Search or Select

Hotspot Server Search or Select

L3 Access DISABLED

User Defined (Private) Network

DHCP

IPv4 DHCP Required	<input checked="" type="checkbox"/>
DHCP Server IP Address	<input type="text"/>
DHCP Server VRF	<input type="checkbox"/> Search or Select

Status

Drop Unicast

DNS Layer Security

DNS Layer Security Parameter Map	Not Configured	<input type="button" value="Clear"/>
----------------------------------	----------------	--------------------------------------

Policy Proxy Settings

ARP Proxy	<input checked="" type="checkbox"/> ENABLED
IPv6 Proxy	<input type="button" value="None"/>

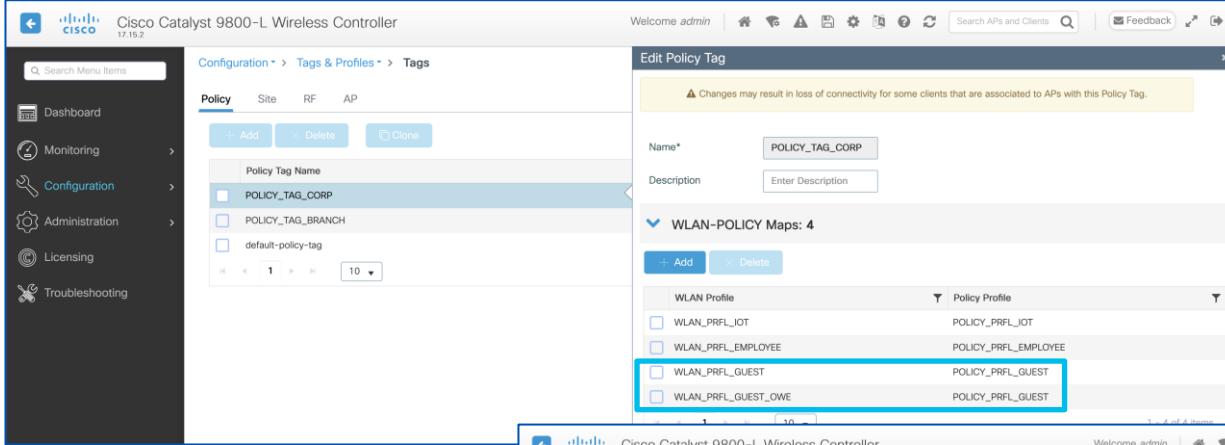
To avoid too many reauthentications

For increased security/control

For increased security/control

Assign the WLAN Profile to the Policy Profile

Configuration > Tags & Profiles > Tags

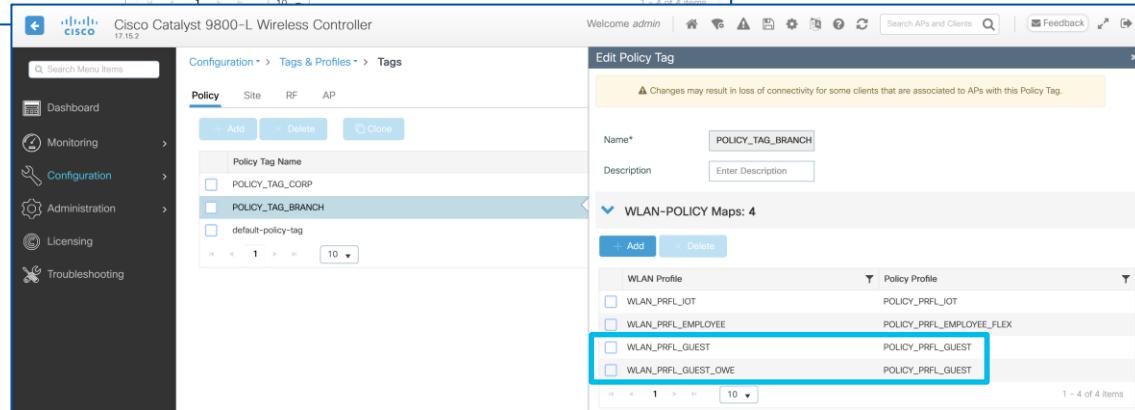


Configuration > Tags & Profiles > Tags

Policy Tag Name: POLICY_TAG_CORP

WLAN-POLICY Maps: 4

WLAN Profile	Policy Profile
WLAN_PROFILE_IOT	POLICY_PROFILE_IOT
WLAN_PROFILE_EMPLOYEE	POLICY_PROFILE_EMPLOYEE
WLAN_PROFILE_GUEST	POLICY_PROFILE_GUEST
WLAN_PROFILE_GUEST_OWE	POLICY_PROFILE_GUEST



Configuration > Tags & Profiles > Tags

Policy Tag Name: POLICY_TAG_BRANCH

WLAN-POLICY Maps: 4

WLAN Profile	Policy Profile
WLAN_PROFILE_IOT	POLICY_PROFILE_IOT
WLAN_PROFILE_EMPLOYEE	POLICY_PROFILE_EMPLOYEE_FLEX
WLAN_PROFILE_GUEST	POLICY_PROFILE_GUEST
WLAN_PROFILE_GUEST_OWE	POLICY_PROFILE_GUEST

Here we can reuse our existing Policy Tags, so that APs will automatically start using both the guest and the OWE SSIDs assigned to the same guest Policy Profile

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>

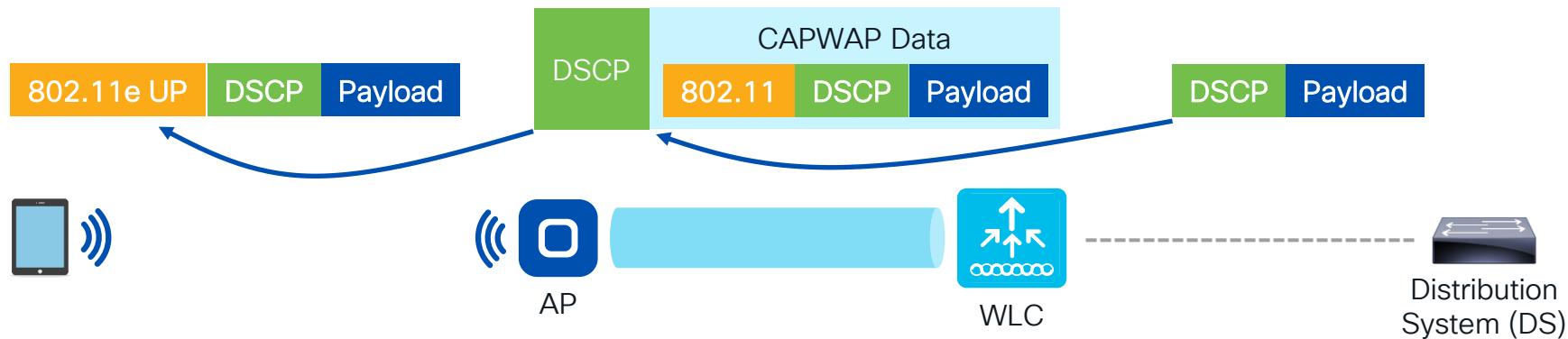
Further tweaks

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)

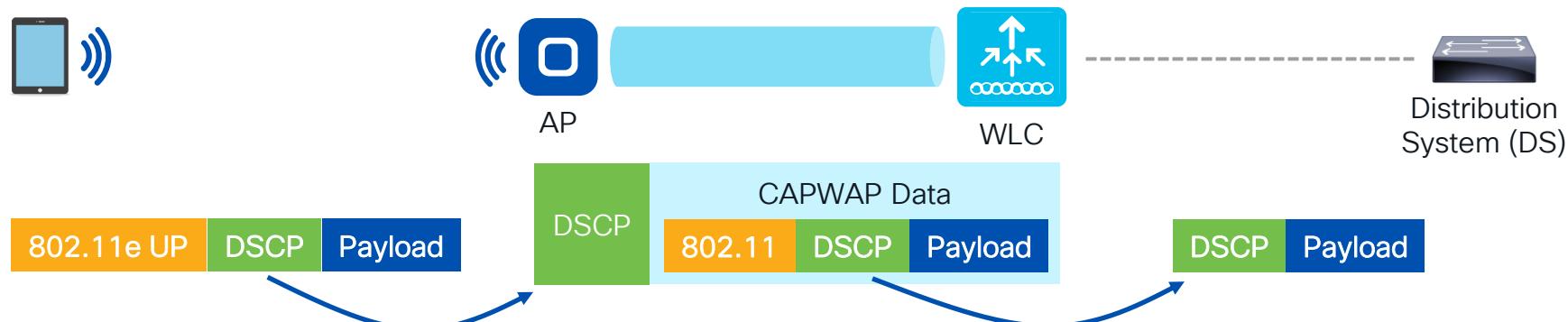
QoS - Trust DSCP Upstream: the one to start with

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
```

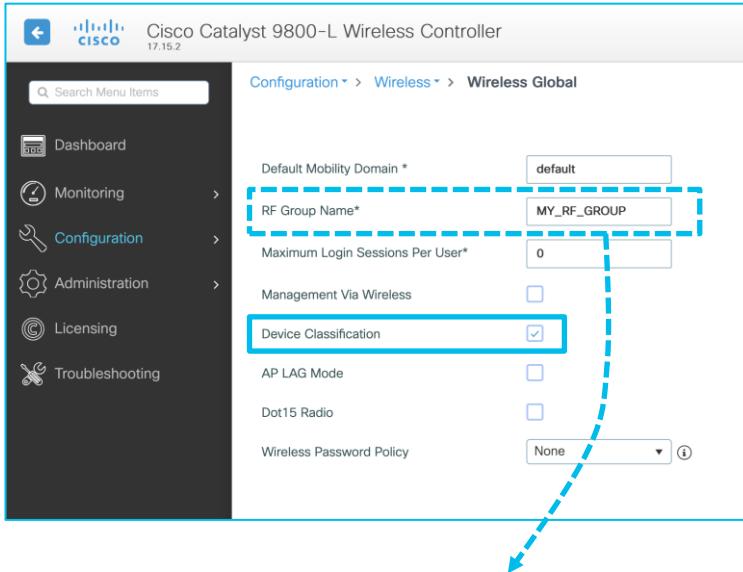


Upstream: the 802.11e UP value from the endpoint (if any) is ignored; the original DSCP value is used to mark the CAPWAP data tunnel too, then preserved all the way up to the DS.
(assuming no remarking is applied at the WLC level)



Devices and applications visibility

Configuration > Wireless > Wireless Global



Cisco Catalyst 9800-L Wireless Controller
17.15.2

Configuration > Wireless > Wireless Global

Default Mobility Domain * default

RF Group Name* MY_RF_GROUP

Maximum Login Sessions Per User* 0

Management Via Wireless

Device Classification

AP LAG Mode

Dot15 Radio

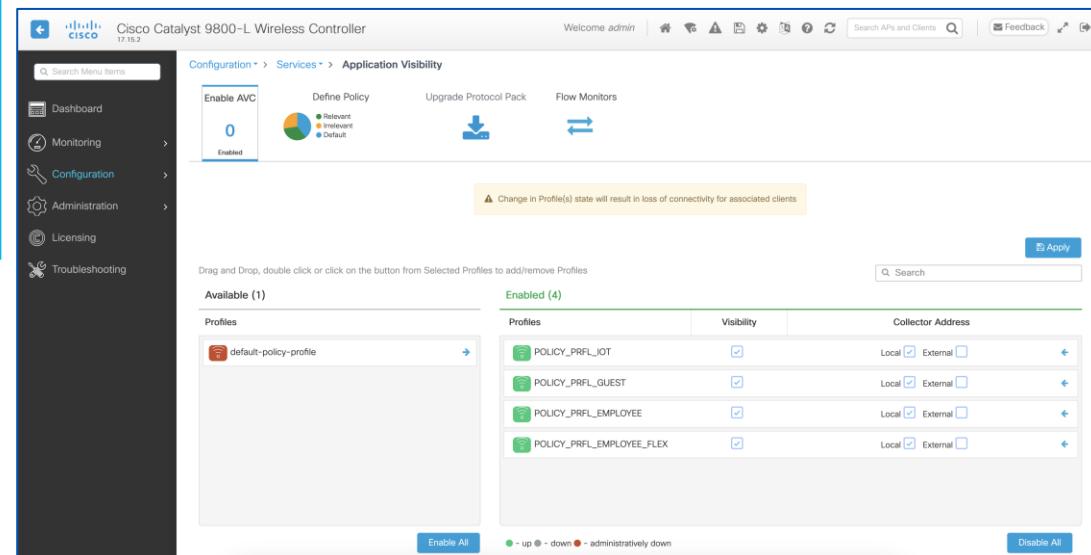
Wireless Password Policy None

Especially during a PoC/test, we may want to keep the RF group name unique, so that it does not match and interact with others already in production (unless needed)

☞ 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



Cisco Catalyst 9800-L Wireless Controller
17.15.2

Configuration > Services > Application Visibility

Enable AVC 0 Enabled

Define Policy Relevant Irrelevant Default

Upgrade Protocol Pack Flow Monitors

Change in Profile(s) state will result in loss of connectivity for associated clients

Drag and Drop, double click or click on the button from Selected Profiles to add/remove Profiles

Available (1)

Enabled (4)

Profiles	Visibility	Collector Address
POLICY_PRFL_IOT	<input checked="" type="checkbox"/>	Local <input checked="" type="checkbox"/> External <input type="checkbox"/>
POLICY_PRFL_GUEST	<input checked="" type="checkbox"/>	Local <input checked="" type="checkbox"/> External <input type="checkbox"/>
POLICY_PRFL_EMPLOYEE	<input checked="" type="checkbox"/>	Local <input checked="" type="checkbox"/> External <input type="checkbox"/>
POLICY_PRFL_EMPLOYEE_FLEX	<input checked="" type="checkbox"/>	Local <input checked="" type="checkbox"/> External <input type="checkbox"/>

Enable All Disable All

If not already enabled, let's turn on CleanAir



Configuration > Radio Configurations > CleanAir

Cisco Catalyst 9800-L Wireless Controller
17.15.2

Welcome admin

Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Licensing

Troubleshooting

Configuration > Radio Configurations > CleanAir

6 GHz Band 5 GHz Band 2.4 GHz Band

General Trap Configuration

Enable CleanAir

Report Interferers

Available Interference Types

6 GHz Band 5 GHz Band 2.4 GHz Band

General Trap Configuration

Enable CleanAir

Enable SI

Report Interferers

Available Interference Types

Interference Types to detect

TDD Transmitter
Jammer
Continuous Transmitter
DECT-like Phone
Video Camera

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

6 GHz Band 5 GHz Band 2.4 GHz Band

General Trap Configuration

Enable CleanAir

Enable SI

Report Interferers

Available Interference Types

Interference Types to detect

BLE Beacon
Bluetooth Discovery
Bluetooth Link

TDD Transmitter
Jammer
Continuous Transmitter
DECT-like Phone
Video Camera

Energy efficiency



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

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller interface. In the center, a modal window titled 'Add Power Profile' is open. The 'Name*' field contains 'PWR_PRFL_1G_1X1'. The 'Power Save Client Threshold' field is highlighted with a green box and contains the value '3'. A callout box with the text 'While X (or more) clients are connected, the AP does not apply the Power Profile' points to this field. Below the modal, a table lists configuration details for five interfaces: Ethernet (GigabitEthernet0) and four Radio interfaces (2.4 GHz, 5 GHz, Secondary 5 GHz, 6 GHz) all set to 1x1 Spatial Stream. At the bottom right of the modal is a 'Apply to Device' button.

Sequence number	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

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 interface. The top navigation bar includes the Cisco logo, the device name 'Cisco Catalyst 9800-L Wireless Controller', the IP address '17.15.2', and a user 'admin'. The main menu on the left lists 'Dashboard', 'Monitoring', 'Configuration' (which is selected), 'Administration', 'Licensing', and 'Troubleshooting'. The 'Configuration' menu has a sub-item 'Tags & Profiles'. The 'Tags & Profiles' page shows a table with a single row selected, and a modal dialog box titled 'Add Calendar Profile' is open. The dialog box contains the following information:

- Info message:** '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'
- Name:** CALENDAR_PRFL_NIGH
- Recurrence:** Daily
- Start Time:** 22:00:00
- End Time:** 06:00:00

At the bottom of the dialog box are '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

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 interface. On the left, a navigation bar includes links for Dashboard, Monitoring, Configuration (which is selected), Administration, Licensing, and Troubleshooting. The main content area shows the 'Configuration > Tags & Profiles > AP Join' path. A table lists an 'AP Join Profile Name' row with 'default-ap-profile' selected. A detailed configuration dialog box is open, titled 'Edit AP Join Profile'. The 'General' tab is selected, showing fields for Name (default-ap-profile), Description (default ap profile), Country Code (NL), Deployment Mode (Default), Time Zone (Not Configured), LED State (checked), LAG Mode (unchecked), NTP Server (0.0.0.0), GAS AP Rate Limit (unchecked), USB Enable (unchecked), Apphost (unchecked), and Fallback to DHCP (checked). To the right, under 'OfficeExtend AP Configuration', are sections for Local Access (checked), Link Encryption (checked), Rogue Detection (unchecked), Provisioning SSID (checked), Antenna Monitoring (unchecked), RSSI Fail Threshold(dBm) (40), Weak RSSI(dBm) (-60), and Detection Time(min) (12). At the bottom of the dialog are 'Cancel' and 'Update & Apply to Device' buttons.

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



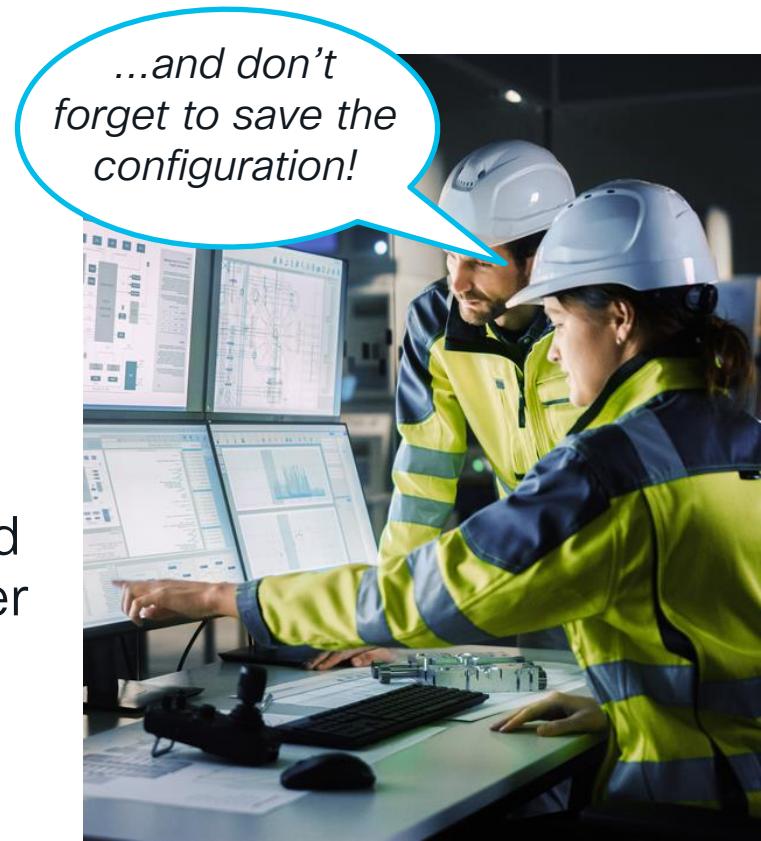
Configuration > Tags & Profiles > AP Join (Management > Device/User tabs)

By default APs send syslog messages to 255.255.255.255. This could cause unwanted broadcast traffic, especially when multiplied 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-2025
Wi-Fi 7 is here - Are you Ready?
- BRKEWN-2926
Tune your Cisco Wireless networks for Roaming clients and demanding Real-Time applications...with some help from AI!
- BRKEWN-2325
Secure Your Cisco Wireless Network with Identity Services Engine (ISE)
- BRKEWN-2667
Cisco Wireless Supercharged by Catalyst Center: The Ultimate Guide
- BRKEWN-2043
Saving Energy and Money with Your Cisco Wireless Network
- BRKEWN-3628
Troubleshoot Catalyst 9800 Wireless Controllers

Fill Out Your Session Surveys



Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique 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 in to the Session Catalog and clicking the 'Participant Dashboard'



Content Catalog



Continue your education

CISCO *Live!*

- 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 cisco.com/on-demand. Sessions from this event will be available from March 3.

Contact me at: fziliott@cisco.com

Thank you

cisco *Live!*



GO BEYOND