



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

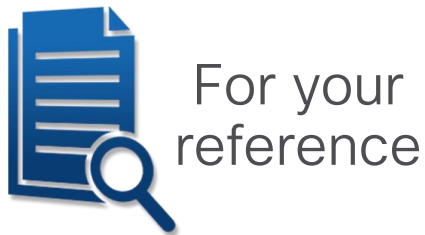
- ~18 years at 
 - 4 years as a Customer Support Engineer (CSE)
 - 3 years as a Specialized Systems Engineer
 - 5 years as a Consulting Systems Engineer (CSE)
 - ~6 years as a Technical Solutions Architect (TSA)
- Always focused on Wireless and NAC



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”



Webex App

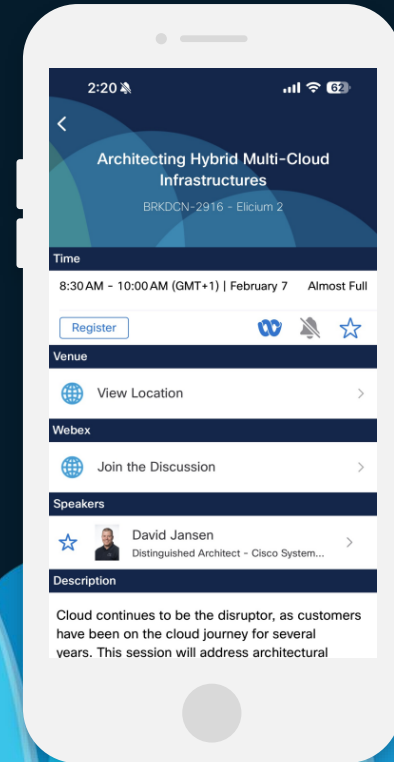
Questions?

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.



Configuration template available here



- The text format of all the configuration examples in this presentation is available here:
https://github.com/fedezil/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/versions

In the following examples we assume we're already here

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

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

I know... but if I don't do this I will freak out



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

Configuration Setup Wizard

1. General Settings

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

Service Port Settings

DHCP: ☐

Static IP*: 10.0.0.1



WELCOME !

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.

DNAC Cloud Onboarding Day 0 Wizard

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

Classic Day 0 Wizard

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

READ THE INSTRUCTIONS BELOW BEFORE YOU BEGIN

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

https://<9800_IP>/webui/#/dayzeroWireless 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.

Apply (3)

⚠ Configuring High Throughput Parameters will result in loss of connectivity of all clients across 802.11be enabled radios of the APs

> 11ax

11be (2)

⚠ 11be check enables Wi-Fi 7 capability 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

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

Save! Save! Save!

(wr → write memory)



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

Administration > Software Management



For your reference

Administration > Software Management

Software Upgrade

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

One-Shot Install Upgrade ☐

Transport Type: My Desktop

File System: bootflash Free Space: 19437.06 MB

Source File Path*

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

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

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

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

Our first SSIDs



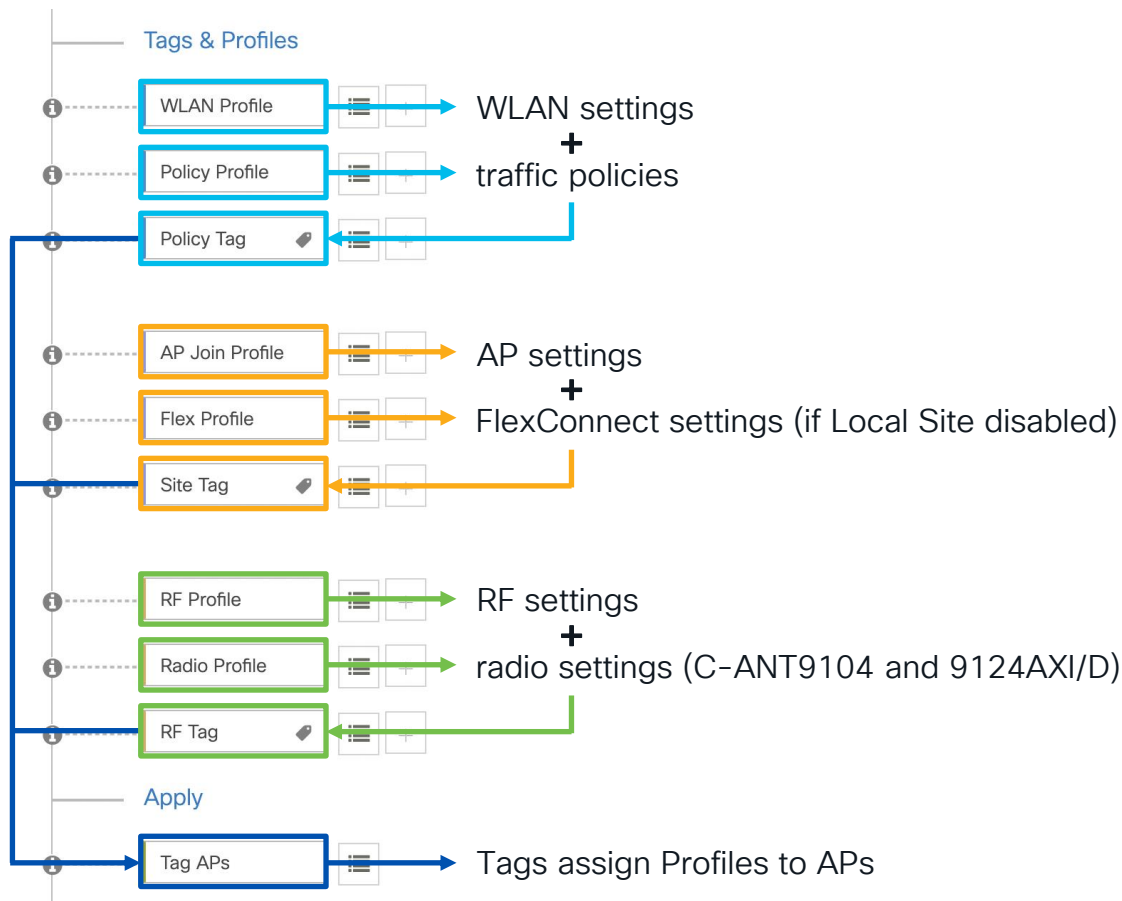
Profiles and Tags: the main configuration objects

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

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

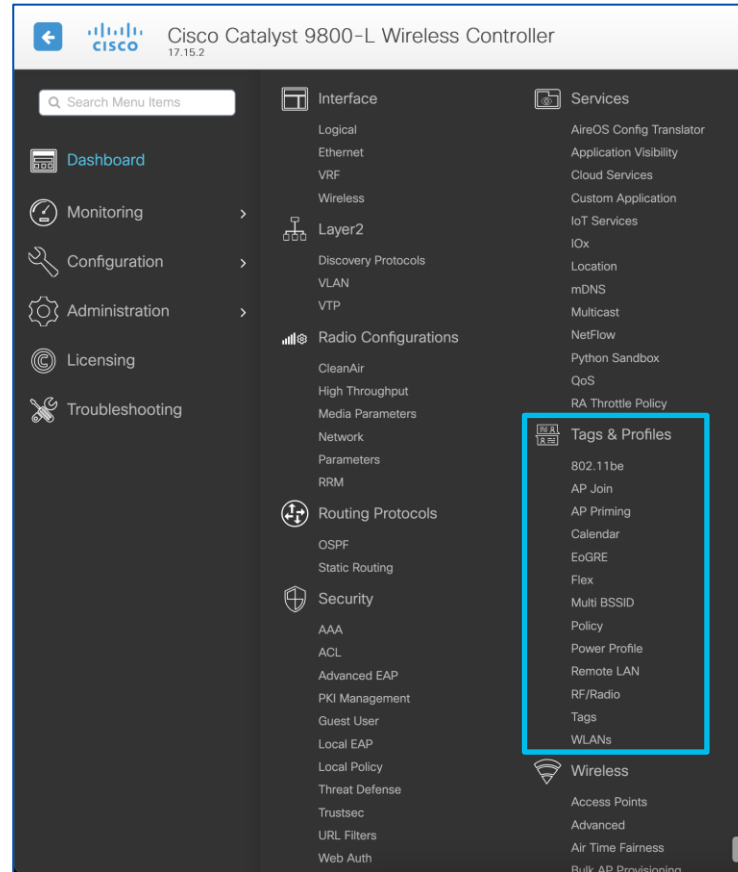
Profiles and Tags: the main configuration objects

Configuration >
Wireless Setup >
Advanced >
Start Now



Profiles and Tags: a more dedicated menu

Configuration >
Tags & Profiles



Client VLANs should be configured and trunked

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

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration page. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled 'Configuration > Layer2 > VLAN'. Below this, there are tabs for 'SVI' and 'VLAN', with 'VLAN' selected. There are 'Add' and 'Delete' buttons. A table lists the configured VLANs:

VLAN ID	Name	Status	Ports
<input type="checkbox"/> 1	default	active	Tw0/0/0, Tw0/0/1, Tw0/0/2, Tw0/0/3, Te0/1/1
<input type="checkbox"/> 10	VLAN_WIRELESS_MGMT	active	
<input type="checkbox"/> 110	VLAN_EMPLOYEE	active	
<input type="checkbox"/> 120	VLAN_VOICE	active	
<input type="checkbox"/> 130	VLAN_GUEST	active	
<input type="checkbox"/> 140	VLAN_IOT	active	

At the bottom of the table, there are navigation controls showing '1' of 10 items.

Configuring a RADIUS server

Configuration > Security > AAA > Add RADIUS Server

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

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

At the bottom of the dialog, there are 'Cancel' and 'Apply to Device' buttons. The background interface shows the left-hand navigation menu with options like Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The top right of the interface includes a search bar and a feedback button.

Configuring a RADIUS server group

Configuration > Security > AAA > Add RADIUS Server Group

The screenshot displays the Cisco Catalyst 9800-L Wireless Controller configuration interface. The main navigation pane on the left includes links for Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The central pane shows the configuration path: Configuration > Security > AAA > Servers / Groups. A modal dialog titled 'Create AAA Radius Server Group' is open, allowing for the configuration of a new RADIUS server group. The dialog includes fields for Name, Group Type, MAC-Delimiter, MAC-Filtering, Dead-Time (mins), Load Balance, IPv4 Source Interface, IPv4 VRF, IPv6 Source Interface, and IPv6 VRF. It also features sections for Available Servers and Assigned Servers, with a list of servers including RADIUS_SVR_GRP_01 and RADIUS_SVR_GRP_02. The dialog has 'Cancel' and 'Apply to Device' buttons at the bottom.

Configuration > Security > AAA > Add RADIUS Server Group

Create AAA Radius Server Group

Name* RADIUS_SVR_GRP_01

Group Type RADIUS

MAC-Delimiter none

MAC-Filtering none

Dead-Time (mins) 5

Load Balance ☐ DISABLED

IPv4 Source Interface Vlan10

IPv4 VRF Search or Select

IPv6 Source Interface Search or Select

IPv6 VRF Search or Select

Available Servers

Assigned Servers

RADIUS_SVR_GRP_01

RADIUS_SVR_GRP_02

Cancel Apply to Device

Configuring a AAA Method List for 802.1X

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

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation path is Configuration > Security > AAA > AAA Method List > Authentication > Add (Type = dot1x). The 'Quick Setup: AAA Authentication' dialog box is open, displaying the following configuration details:

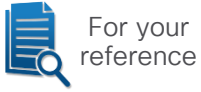
- Method List Name*: MLIST_AUTHC_1X
- Type*: dot1x
- Group Type: group
- Fallback to local: ☐
- Available Server Groups: radius, ldap, tacacs+
- Assigned Server Groups: RADIUS_SRV_GRP_01

The dialog box includes 'Cancel' and 'Apply to Device' buttons. In the background, a table shows server group assignments for Group3 and Group4, all marked as N/A.

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

1 - 3 of 3 items

AAA Method List for authorization



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

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled 'Configuration > Security > AAA'. A 'Quick Setup: AAA Authorization' dialog box is open, displaying the following fields:

- Method List Name*: MLIST_AUTHZ_NTWRK
- Type*: network
- Group Type: group
- Fallback to local: ☐
- Authenticated: ☐
- Available Server Groups: radius, ldap, tacacs+
- Assigned Server Groups: RADIUS_SVR_GRP_01

Buttons at the bottom of the dialog include 'Cancel' and '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 displays the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation path is Configuration > Security > AAA > AAA Method List > Accounting > Add (Type = identity). The 'AAA Method List' tab is selected, and the 'Accounting' sub-tab is active. A 'Quick Setup: AAA Accounting' dialog box is open, showing the following configuration:

- Method List Name*: MLIST_ACCT_ID
- Type*: identity
- Available Server Groups: radius, ldap, tacacs+, RADIUS_SRVR_GRP_01
- Assigned Server Groups: RADIUS_SRVR_GRP_01

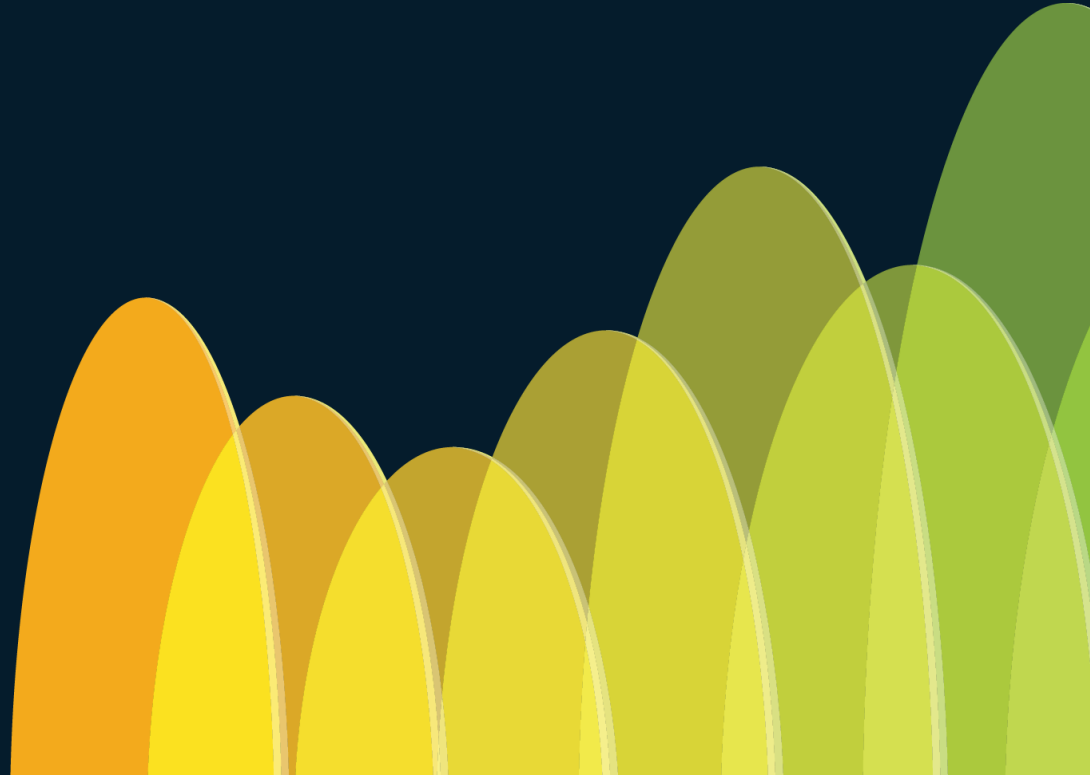
The dialog box includes 'Cancel' and 'Apply to Device' buttons. The background interface shows the 'Servers / Groups' section with tabs for 'AAA Method List' and 'AAA Advanced'. The 'AAA Method List' tab is active, and the 'Accounting' sub-tab is selected. The 'Servers / Groups' section shows a list of groups, including 'Group3' and 'Group4', with a 'No items to display' message.

Or also with a quick CLI copy/paste



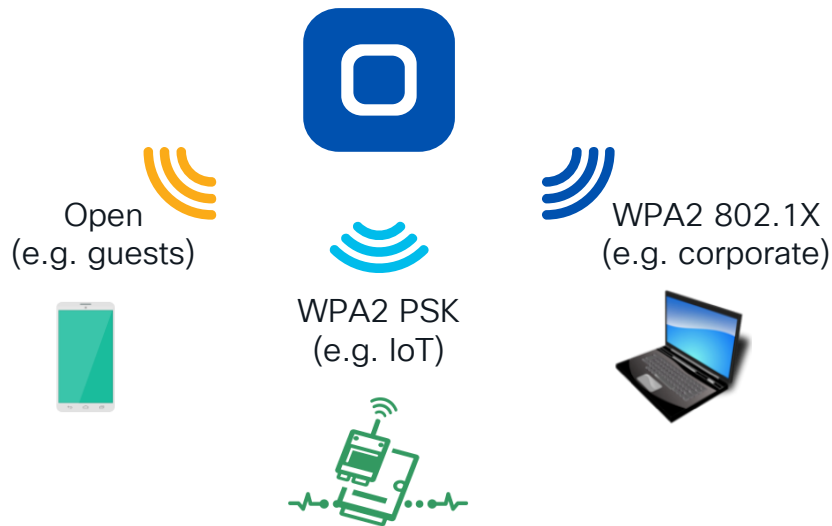
```
radius server RADIUS_SRVR_ISE
  address ipv4 192.168.1.201 auth-port 1812 acct-port 1813
  key <RADIUS_SHARED_SECRET>
!
aaa server radius dynamic-author
  client 192.168.1.201 server-key <RADIUS_SHARED_SECRET>
!
aaa group server radius RADIUS_SRVR_GRP_01
  server name RADIUS_SRVR_ISE
  ip radius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

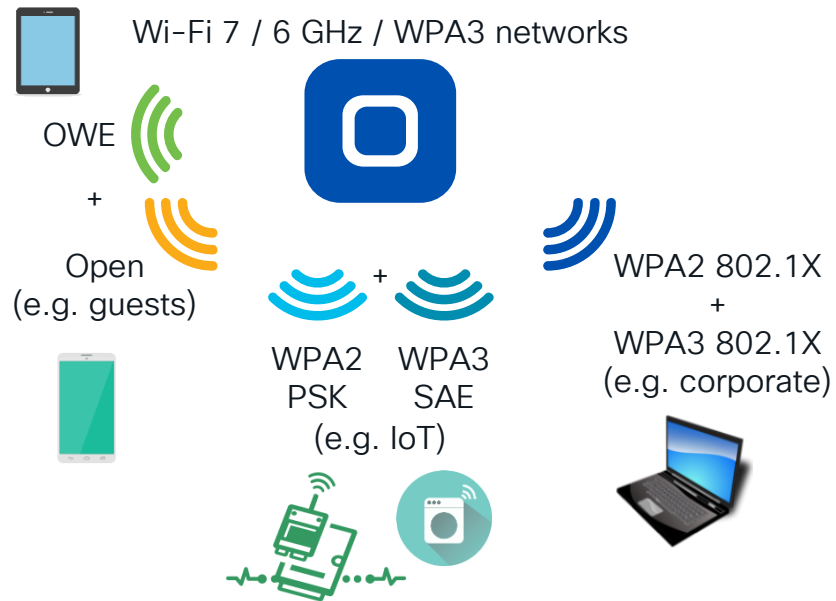


Wi-Fi 7 features mandate WPA3/OWE

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

The screenshot shows the 'Add WLAN' configuration page in the Cisco Catalyst 9800-L Wireless Controller. The 'General' tab is active, showing fields for Profile Name (WLAN_PRFL_EMPLOYEE), SSID (Employee), WLAN ID (1), Status (ENABLED), and Broadcast SSID (ENABLED). The 'Radio Policy' section shows 6 GHz Status as ENABLED, 5 GHz Status as ENABLED, and 2.4 GHz Status as DISABLED. A note indicates that WPA3 and Dot1x are enabled for 6 GHz broadcast.

The screenshot shows the 'Security' tab for the WLAN configuration. The 'Layer2' tab is active, showing WPA2 + WPA3 selected as the security protocol. The 'WPA Parameters' section shows WPA Policy, GTK Randomize, and Transition Disable all checked. The 'WPA2/WPA3 Encryption' section shows AES(CCMP128) and GCMP128 both checked. The 'Protected Management Frame' section shows PMF set to Required. The 'Fast Transition' section shows Status set to Enabled. The 'Auth Key Mgmt (AKM)' section shows 802.1X, 802.1X-SHA256, and PSK all checked.

The screenshot shows the 'AAA' tab for the WLAN configuration. The 'Authentication List' dropdown is open, showing 'MLIST_AUTHC_1' selected. The 'Local EAP Authentication' section is visible below.

The AAA Method List for dot1x authentication

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☐

WPA2 Policy☒

GTK Randomize☐

WPA3 Policy☒

Transition Disable☐

Beacon Protection☒

WPA2/WPA3 Encryption

AES(CCMP128)☒

CCMP256☐

GCMP128☐

GCMP256☐

Protected Management Frame

PMF

Required

Association Comeback Timer*

1

SA Query Time*

200

Fast Transition

Status

Enabled

Over the DS

☐

Reassociation Timeout *

20

Auth Key Mgmt (AKM)

802.1X☒

FT + 802.1X☒

802.1X-SHA256☒

CCKM⚠☐

PSK☐

FT + PSK☐

PSK-SHA256☐

SAE☐

FT + SAE☐

SAE-EXT-KEY☐

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

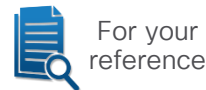
CISCO Live!

BRKEWN-2094

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

33

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"/>

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

Association Comeback Timer*

SA Query Time*

Fast Transition

Status

Over the DS ☐

Reassociation Timeout *

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

Assisted Roaming (11k)

Prediction Optimization: ☐

Neighbor List: ☒

Dual Band Neighbor List: ☐

DTIM Period (in beacon intervals)

5 GHz Band (1-255): 1

2.4 GHz Band (1-255): 1

11v BSS Transition Support

BSS Transition: ☒

Dual Neighbor List: ☐

BSS Max Idle Service: ☒

BSS Max Idle Protected: ☐

Directed Multicast Service: ☒

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

11ax

Enable 11ax: ☒

OFDMA Downlink: ☒

OFDMA Uplink: ☒

MU-MIMO Downlink: ☒

MU-MIMO Uplink: ☒

BSS Target Wake Up Time: ☐

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

The screenshot shows the 'Add Policy Profile' dialog in the Cisco Catalyst 9800-L Wireless Controller configuration interface. The dialog has a warning at the top: 'Disabling a Policy or configuring it in "Enabled" state, will result in loss of connectivity for clients associated with this Policy profile.' The 'General' tab is selected, showing fields for Name (POLICY_PRFL_EMPLOYEE), Description (Enter Description), Status (ENABLED), Passive Client (DISABLED), IP MAC Binding (ENABLED), Encrypted Traffic Analytics (DISABLED), and CTS Policy (Inline Tagging, SGACL Enforcement, Default SGT). A blue box highlights the 'WLAN Switching Policy' section, which includes Central Switching (ENABLED), Central Authentication (ENABLED), Central DHCP (ENABLED), and Flex NAT/PAT (DISABLED). A blue arrow points from the 'ENABLED' status of the 'Status' field to the 'WLAN Switching Policy' section. Another blue arrow points from the 'WLAN Switching Policy' section to the text 'Policy Profile for central switching'. A third blue arrow points from the 'WLAN Switching Policy' section to the text 'As for a WLAN Profile, we need to explicitly enable it'.

Configuration > Tags & Profiles > Policy > Add

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

General Access Policies QOS and AVC Mobility Advanced

Name* POLICY_PRFL_EMPLOYEE

Description Enter Description

Status **ENABLED**

Passive Client **DISABLED**

IP MAC Binding **ENABLED**

Encrypted Traffic Analytics **DISABLED**

CTS Policy

Inline Tagging ☐

SGACL Enforcement ☐

Default SGT 2-65519

WLAN Switching Policy

Central Switching **ENABLED**

Central Authentication **ENABLED**

Central DHCP **ENABLED**

Flex NAT/PAT **DISABLED**

Cancel Apply to Device

Policy Profile for central switching

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

Configuring the Policy Profile

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

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

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

This VLAN must already exist in the 9800's database

Configuring the Policy Profile

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

For increased
security/control

Add Policy Profile

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

General

Access Policies

QOS and AVC

Mobility

Advanced

WLAN Timeout

Session Timeout (sec)

86400

i

Idle Timeout (sec)

300

Idle Threshold (bytes)

0

Client Exclusion Timeout (sec)

☒

60

Guest LAN Session Timeout

☐

DHCP

IPv4 DHCP Required

☒

DHCP Server IP Address

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

▼

Clear

CISCO *Live!*

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
RADIUS Accounting
and CoA too

For increased
security/control

Add Policy Profile

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

AAA Policy

Allow AAA Override☒

NAC State☒

Policy Name

default-aaa-policy x

Accounting List

MLIST_ACCT_ID x

Interim Accounting

ENABLED

WGB Parameters

Broadcast Tagging☐

WGB VLAN☐

Policy Proxy Settings

ARP Proxy

ENABLED

IPv6 Proxy

None

Advanced

Fabric Profile☐

Search or Select

Link-Local Bridging☐

mDNS Service Policy

Search or Select

Hotspot Server

Search or Select

L3 Access

DISABLED

User Defined (Private) Network

Status☐

Drop Unicast☐

DNS Layer Security

DNS Layer Security Parameter Map

Not Configured

CISCO *Live!*

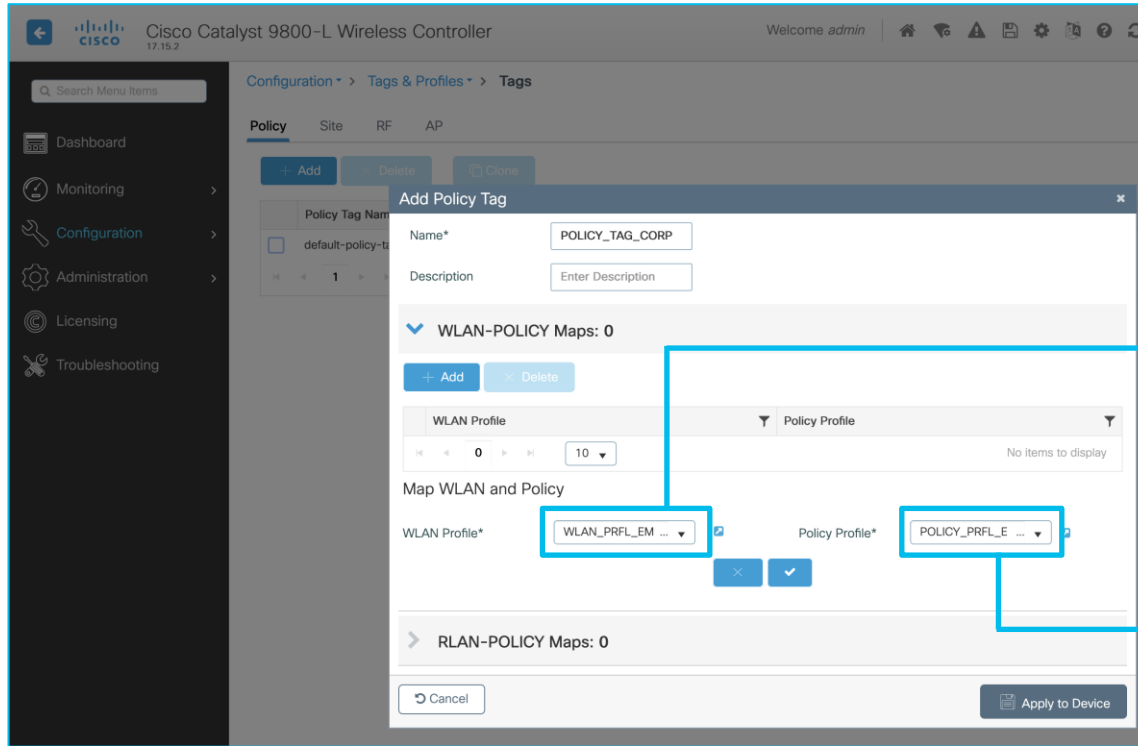
BRKEWN-2094

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

40

Configuring the Policy Tag

Configuration > Tags & Profiles > Tags > Policy > Add



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.)

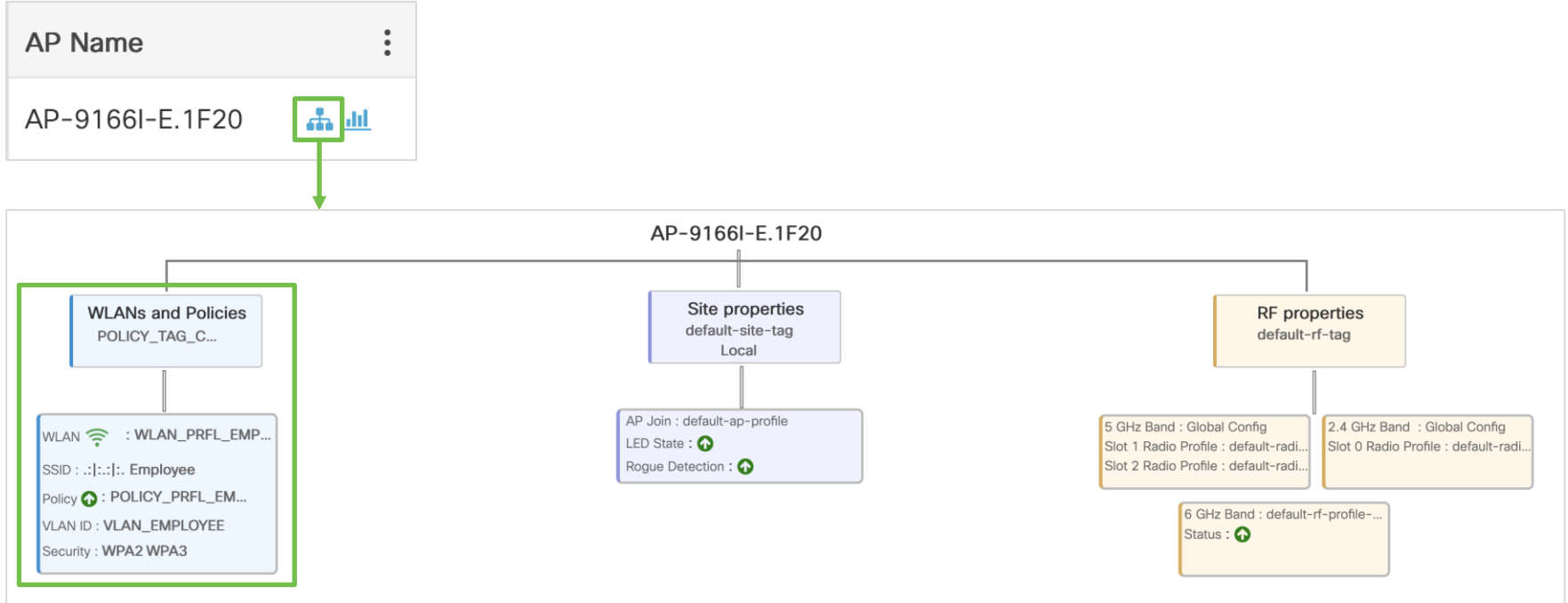
Assigning the Policy Tag to the AP

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled 'Configuration > Wireless > Access Points' and shows 'All Access Points' with a table of APs. The table has columns for AP Name, AP Model, Slots, and Admin Status. The AP 'AP-9166I-E.1F20' is selected. Below the table are expandable sections for 6 GHz Radios, 5 GHz Radios, 2.4 GHz Radios, Dual-Band Radios, Country, LSC Provision, and AP Certificate Policy. The 'Edit AP' modal is open, showing tabs for General, Interfaces, High Availability, Inventory, Geolocation, ICap, Advanced, and Support Bundle. The 'General' tab is active, showing fields for AP Name, Location, Base Radio MAC, Ethernet MAC, Admin Status (ENABLED), AP Mode (Local), Operation Status (Registered), Fabric Status (Disabled), CleanAir NSI Key, LED Settings (ENABLED), Brightness Level (8), Flash Settings (DISABLED), and a 'Write Tag Config to AP' button. The 'Tags' section is highlighted, showing a dropdown for 'Policy' set to 'POLICY_TAG_CO ...'. A green arrow points from this dropdown to a text box on the right.

Here we can select the POLICY_TAG_CORP that we just configured

The CAPWAP service will restart (not a reload)

Checking Tags and Profiles assignment



Other options to assign Tags

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

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration page. The breadcrumb navigation is Configuration > Tags & Profiles > Tags. The 'AP' tab is selected, and the 'Tag Source' sub-tab is active. A table lists four tag sources: Static (Priority 0), Location (Priority 1), Filter (Priority 2), and AP (Priority 3). Each source has a checkbox for selection, all of which are checked. Below the table, there are options to 'Revalidate Tag Sources on APs' and 'Enable AP Tag Persistence', both with checkboxes. An 'Apply' button is at the bottom.

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

Through regex rules for the AP names

The 'Associate Tags to AP' form is shown. It includes fields for Rule Name* (FILTER_CORP), AP name regex* (^AP-.*), Active (YES), and Priority* (1023). On the right, there are dropdown menus for Policy Tag Name (POLICY_TAG_CO...), Site Tag Name (default-site-tag), and RF Tag Name (default-rf-tag).

The 'Create Location and associate APs' form is shown. It includes fields for Location* (LOC_CORP), Description, Policy Tag Name (POLICY_TAG_CO...), Site Tag Name (default-site-tag), and RF Tag Name (default-rf-tag).

The 'AP Provisioning' form is shown. It includes sections for 'Add/Select APs' and 'APs on this Location'. The 'Add/Select APs' section has a table with columns for AP MAC and AP Name. The 'APs on this Location' section has a table with columns for AP MAC, AP Name, and Status.

Through a "Location" or group of APs

The 'AP Tag mappings' table is shown. It has columns for AP MAC Address, Policy Tag Name, Site Tag Name, RF Tag Name, and Priming Profile. The table contains one row with AP MAC Address 149f.4310.1f20, Policy Tag Name POLICY_TAG_CORP, Site Tag Name default-site-tag, RF Tag Name default-rf-tag, and Priming Profile. There are 'Add' and 'Delete' buttons above the table, and a 'Select File' button to the right.

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	

"Manually" or through a CSV file

Enabling Tags persistency



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

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 ☐

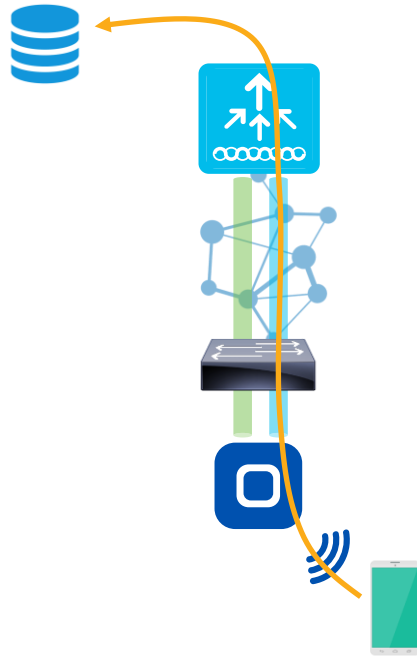
Apply

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

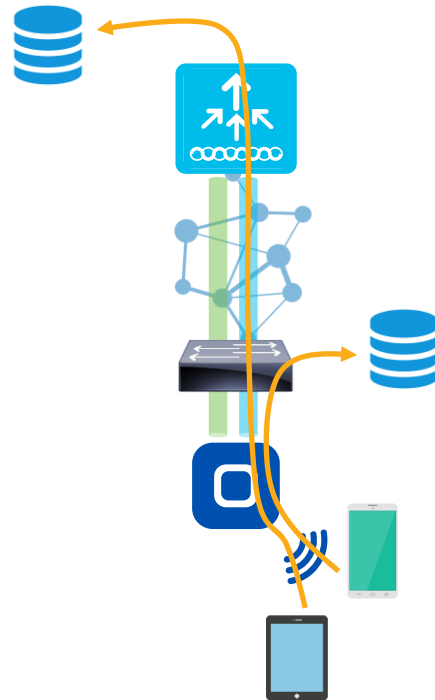
The same Tags must be present on the new destination controller and they are applied according to the AP's memory if no other mappings (static, filter, etc.) supersede them

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

Configuration > Tags & Profiles > Tags

Policy Site RF AP

+ Add - Delete Clone Reset APs

Site Tag Name
default-site-tag

1 10

Edit Site Tag

Name* default-site-tag

Description default site tag

AP Join Profile default-ap-profile

Fabric Control Plane Name

Enable Local Site ☒

Configuration > Tags & Profiles > Tags > Site

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

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

Name* default-site-tag

Description default site tag

AP Join Profile default-ap-profile

Flex Profile default-flex-profile

Fabric Control Plane Name

Enable Local Site ☐

Going FlexConnect

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

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation is Configuration > Tags & Profiles > Tags. The 'Site' tab is selected under the 'Tags & Profiles' section. A modal dialog titled 'Add Site Tag' is open, showing the following fields:

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

The 'Apply to Device' button is visible at the bottom right of the dialog.

Configuration > Tags & Profiles > Tags > Site

Going FlexConnect

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

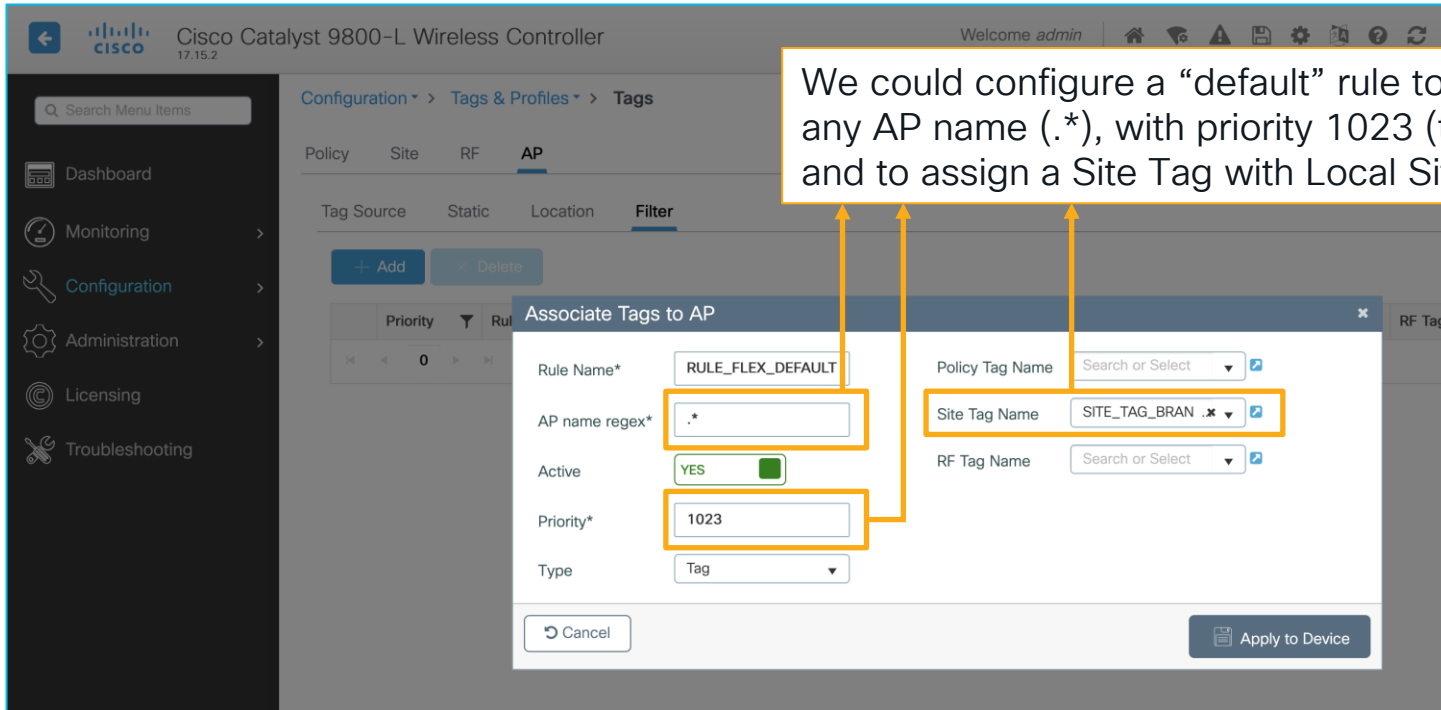
The screenshot displays the Cisco Catalyst 9800-L Wireless Controller interface. The left sidebar shows the navigation menu with options: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is divided into two panels. The left panel, titled 'Configuration > Wireless > Access Points', shows a table of 'All Access Points' with columns for AP Name, AP Model, Slots, and Admin Status. The table lists one AP: AP-9166I-E.1F20, model CW9166I-E, with 3 slots and an enabled status. Below the table are sections for '6 GHz Radios' and '5 GHz Radios'. The right panel, titled 'Edit AP', shows the configuration for the selected AP. The 'General' tab is active, displaying fields for AP Name, Location, Base Radio MAC, Ethernet MAC, Admin Status (ENABLED), AP Mode (Local), Operation Status (Registered), and Fabric Status (Disabled). The 'Tags' section on the right shows a warning message: '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 the warning, there are dropdown menus for 'Policy' (POLICY_TAG_CO ...) and 'Site' (SITE_TAG_BRANCH). A search bar is also present. A blue box highlights the 'SITE_TAG_BRANCH' dropdown, and a blue arrow points from it 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



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

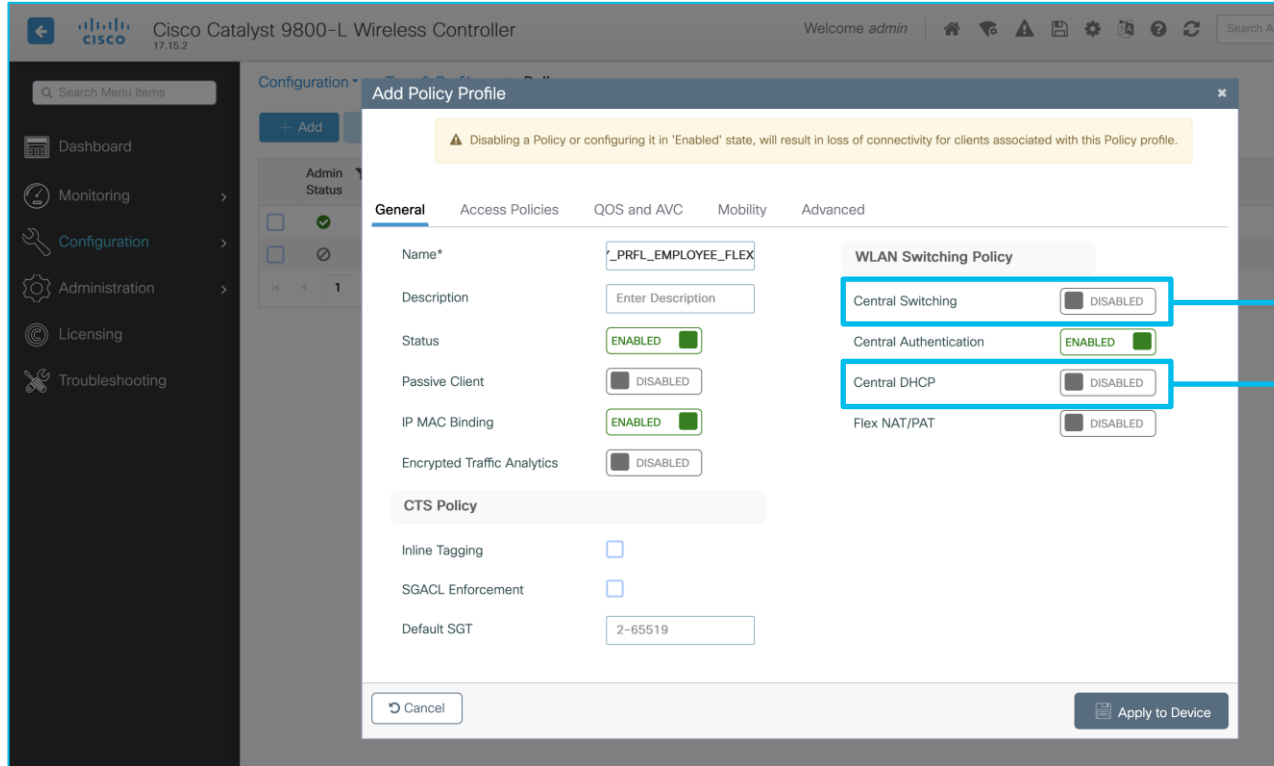
- Rule Name*: RULE_FLEX_DEFAULT
- AP name regex*: .*
- Active: YES (checked)
- Priority*: 1023
- Type: Tag
- Policy Tag Name: Search or Select
- Site Tag Name: SITE_TAG_BRAN .*
- RF Tag Name: Search or Select

Arrows point from the text box to the AP name regex, Priority, and Site Tag Name fields.

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

Going FlexConnect

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



We could have also modified the existing POLICY_PRFL_EMPLOYEE profile. A new, dedicated one for FlexConnect could be more reusable

Going FlexConnect

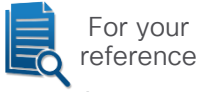
3. Configuring a locally switched VLAN ID or a VLAN name (in this case the Flex Profile must follow)

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



For your
reference

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

Add Policy Profile

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

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

RADIUS Profiling ☒

HTTP TLV Caching ☒

DHCP TLV Caching ☒

WLAN Local Profiling

Global State of Device Classification ⓘ

Local Subscriber Policy Name

VLAN

VLAN/VLAN Group ⓘ

Multicast VLAN

WLAN ACL

IPv4 ACL

IPv6 ACL

URL Filters ⓘ

Pre Auth

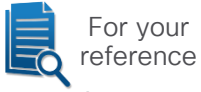
Post Auth

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)

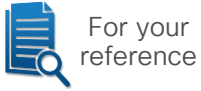
Configuration > Tags & Profiles > Flex

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

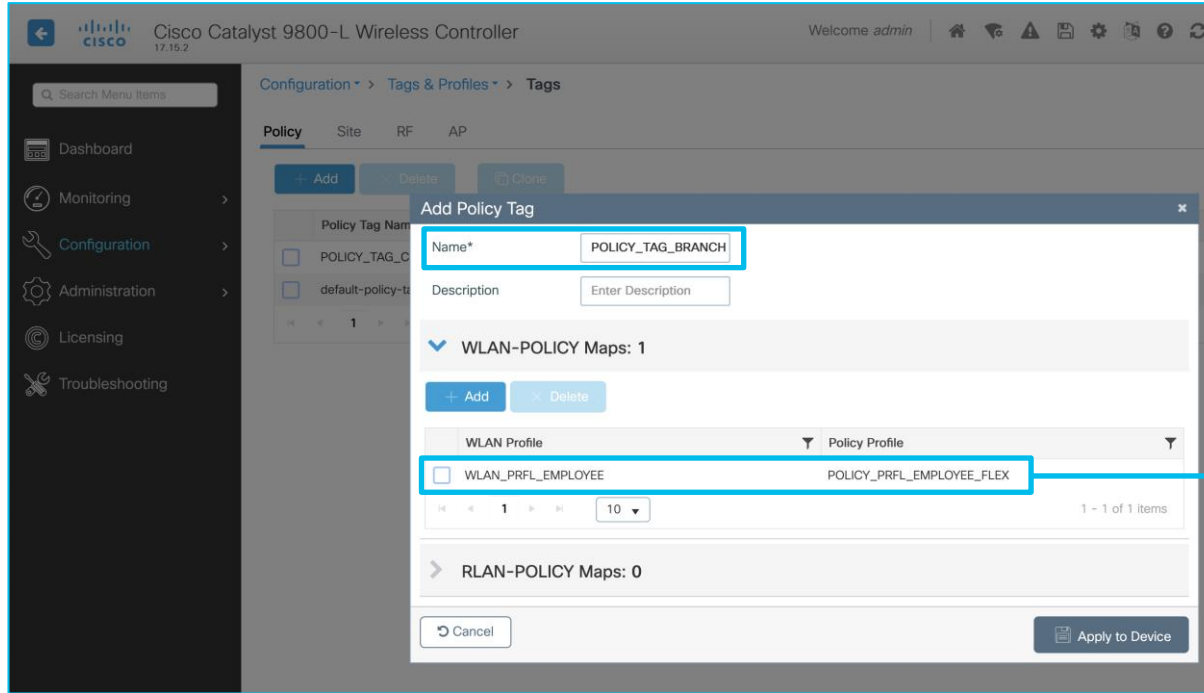


Configuration > Tags & Profiles > Flex

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



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

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

Configuration > Tags & Profiles > Tags > Policy

Assigning the Policy Tag to the AP

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

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller interface. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is divided into two panels. The left panel, titled 'All Access Points', shows a table of APs with columns for AP Name, AP Model, Slots, and Admin Status. The right panel, titled 'Edit AP', shows the configuration for AP-9166I-E.1F20. The 'Tags' section is highlighted, showing a dropdown menu for 'Policy' with options: 'POLICY_TAG_BRANCH', 'default-policy-tag', and 'POLICY_TAG_CORP'. A blue arrow points from the 'POLICY_TAG_BRANCH' option to the text below.

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

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

Configuring a passphrase based WLAN Profile

Configuration > Tags & Profiles > WLANs > Add

Cisco Catalyst 9800-L Wireless Controller

Configuration > Tags & Profiles > WLANs > Add

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**

5 GHz Status **ENABLED**

2.4 GHz Status **ENABLED**

802.11b/g Policy 802.11b/g

[Show slot configuration](#)

[Cancel](#)

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 ☒

WPA2/WPA3 Encryption

AES(CCMP128) ☒ CCMP256 ☐

GCMP128 ☐ GCMP256 ☒

Protected Management Frame

PMF Required

Association Comeback Timer* 1

SA Query Time* 200

Fast Transition

Status Enabled

Over the DS ☐

Reassociation Timeout* 20

Auth Key Mgmt (AKM)

FT + 802.1X ☐ 802.1X-SHA256 ☐

SUITEB192-1X ☐ 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* *

SAE Password Element ① Both H2E and...

Zoom on Layer 2 Security for Wi-Fi 7 support

The screenshot shows the 'Security' tab in the configuration interface, with the 'Layer2' sub-tab selected. A yellow warning banner at the top states: 'To review the necessary considerations for ensuring WLAN compatibility with Wi-Fi 7 security [click here](#).' Below this, the 'WPA3' radio button is selected among other options like 'WPA + WPA2', 'WPA2 + WPA3', 'Static WEP', and 'None'. The 'MAC Filtering' and 'Lobby Admin Access' checkboxes are unchecked. The 'WPA Parameters' section includes 'WPA Policy', 'WPA2 Policy', 'GTK Randomize', 'WPA3 Policy' (checked), 'Transition Disable', and 'Beacon Protection' (checked). The 'WPA2/WPA3 Encryption' section shows 'AES(CCMP128)' (checked), 'CCMP256', 'GCMP128', and 'GCMP256' (checked). The 'Protected Management Frame' section has 'PMF' set to 'Required'. The 'Fast Transition' section shows 'Status' as 'Enabled', 'Over the DS' as unchecked, and 'Reassociation Timeout' as 20. The 'Auth Key Mgmt (AKM)' section shows 'FT + 802.1X', '802.1X-SHA256', 'SAE' (checked), 'FT + SAE' (checked), 'SAE-EXT-KEY' (checked), and 'FT + SAE-EXT-KEY' (checked). Other settings include 'Anti Clogging Threshold' (1500), 'Max Retries' (5), 'Retransmit Timeout' (400), 'PSK Format' (ASCII), 'PSK Type' (Unencrypted), 'Pre-Shared Key' (password field), and 'SAE Password Element' (Both H2E and...).

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"/>
GCMP128	<input type="checkbox"/>	GCMP256	<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"/>	CKM	<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 image displays three screenshots from the Cisco Catalyst 9800-L Wireless Controller interface, illustrating the process of cloning a policy profile.

Left Screenshot: The main configuration page for the Cisco Catalyst 9800-L Wireless Controller (version 17.15.2). The navigation menu on the left includes Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area shows the 'Policy' configuration page under 'Configuration > Tags & Profiles > Policy'. A table lists existing policy profiles, with 'POLICY_PRFL_EMPLOYEE' highlighted. The 'Clone' button is visible in the top right of the table.

Middle Screenshot: A dialog box titled 'Clone of Policy Profile (POLICY_PRFL_EMPLOYEE)'. The 'General' tab is active. The 'Name*' field is set to 'POLICY_PRFL_IOT'. The 'Status' is 'ENABLED'. The 'Passive Client' and 'IP MAC Binding' are 'ENABLED'. The 'Encrypted Traffic Analytics' is 'DISABLED'. The 'CTS Policy' section shows 'Inline Tagging' and 'SGACL Enforcement' as 'DISABLED', and 'Default SGT' as '2-65519'. A 'Cancel' button is at the bottom left.

Right Screenshot: A dialog box titled 'Clone of Policy Profile (POLICY_PRFL_EMPLOYEE)'. The 'Access Policies' tab is active. The 'RADIUS Profiling' is 'DISABLED'. The 'HTTP TLV Caching' and 'DHCP TLV Caching' are 'ENABLED'. The 'WLAN Local Profiling' section shows 'Global State of Device Classification' as 'Disabled'. The 'Local Subscriber Policy Name' is 'Search or Select'. The 'VLAN' section shows 'VLAN/VLAN Group' as 'VLAN_IOT' (highlighted in a dropdown menu). The 'Multicast VLAN' is 'Search or Select'. The 'WLAN ACL' section shows 'IPv4 ACL' and 'IPv6 ACL' as 'Search or Select'. The 'URL Filters' section shows 'Pre Auth' and 'Post Auth' as 'Search or Select'. An 'Apply to Device' button is at the bottom right.

Add the WLAN and Policy Profiles to the Policy Tag

Configuration > Tags & Profiles > Tags > Policy

The screenshot displays the Cisco Catalyst 9800-L Wireless Controller configuration interface. The left sidebar shows the navigation menu with 'Configuration' selected. The main content area shows the 'Tags & Profiles' section, specifically the 'Policy' tab. A list of policy tags is shown, with 'POLICY_TAG_CORP' selected. The 'Edit Policy Tag' dialog is open, showing the following details:

- Name:** POLICY_TAG_CORP
- Description:** Enter Description
- WLAN-POLICY Maps:** 1
- WLAN Profile:** WLAN_PRFL_EMPLOYEE
- Policy Profile:** POLICY_PRFL_EMPLOYEE
- Map WLAN and Policy:** WLAN Profile* is set to WLAN_PRFL_IOT and Policy Profile* is set to POLICY_PRFL_IOT.

The dialog also includes a warning message: "Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag." and buttons for 'Cancel' and 'Update & Apply to Device'.

Add the WLAN and Policy Profiles to the Policy Tag

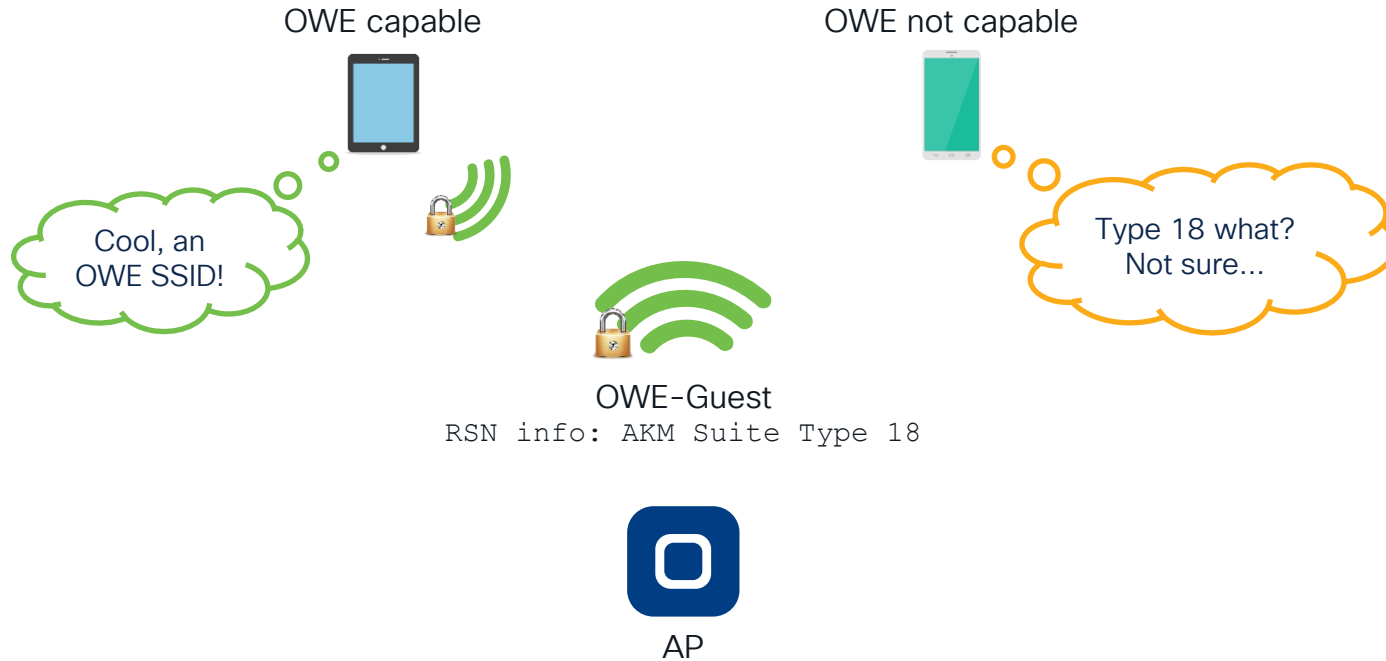
Configuration > Tags & Profiles > Tags > Policy

The screenshot displays the Cisco Catalyst 9800-L Wireless Controller configuration interface. The left sidebar shows the navigation menu with options: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled 'Configuration > Tags & Profiles > Tags'. Under the 'Policy' tab, a list of policy tags is shown: POLICY_TAG_CORP, POLICY_TAG_BRANCH (selected), and default-policy-tag. The 'Edit Policy Tag' dialog is open, showing the following details:

- Name***: POLICY_TAG_BRANCH
- Description**: Enter Description
- WLAN-POLICY Maps: 1**: A table showing one map with WLAN Profile 'WLAN_PRFL_EMPLOYEE' and Policy Profile 'POLICY_PRFL_EMPLOYEE_FLEX'.
- Map WLAN and Policy**: A section with two dropdowns: 'WLAN Profile*' set to 'WLAN_PRFL_IOT' and 'Policy Profile*' set to 'POLICY_PRFL_IOT'. Both have checkboxes that are checked.
- RLAN-POLICY Maps: 0**: A section showing no maps.

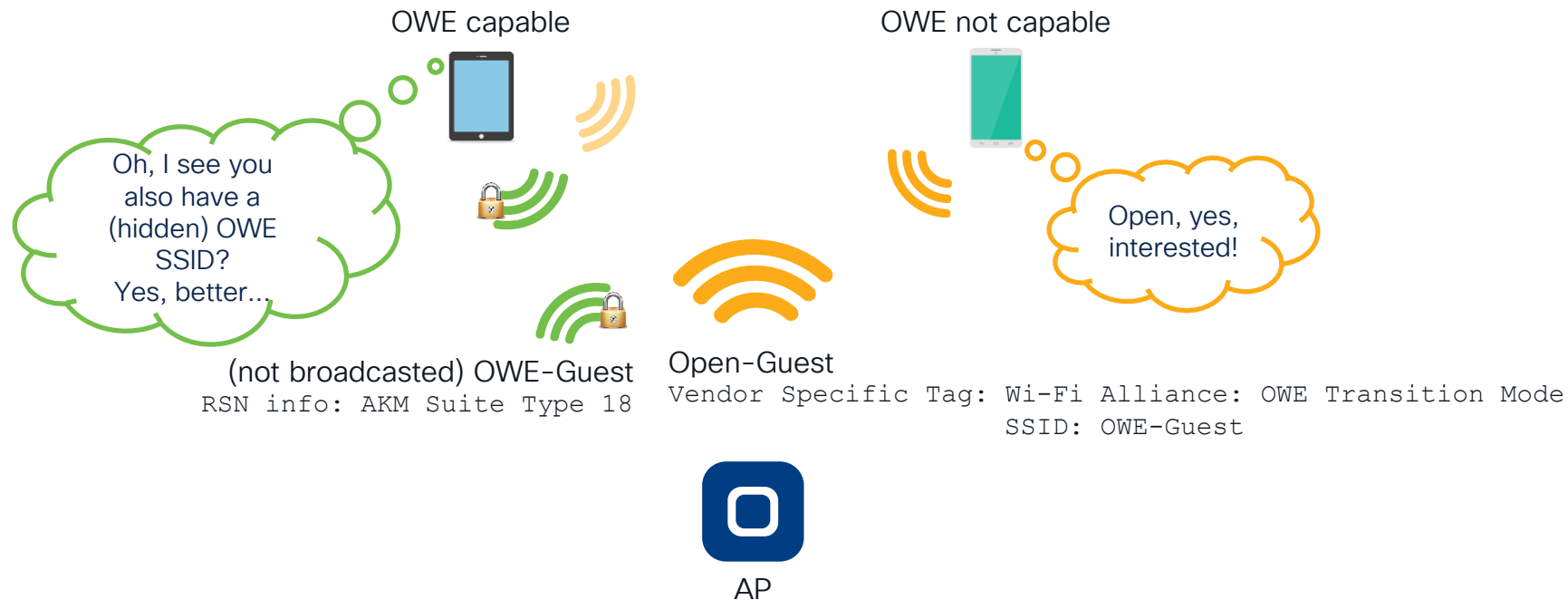
At the bottom of the dialog, there are 'Cancel' and 'Update & Apply to Device' buttons. A warning message at the top of the dialog states: 'Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.'

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 configuration interface. The breadcrumb navigation is Configuration > Security > ACL. The 'Edit ACL' dialog is open for 'ACL_LWA_INTERNAL_F'. The ACL Type is 'IPv4 Extended'. The Rules section shows three rules:

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

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

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


Adding a Guest SSID (LWA with internal portal)

Configuration > Security > Web Auth

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled 'Configuration > Security > Web Auth'. A table lists 'Parameter Map Name' with entries 'global' and 'WEBAUTH_PMAP'. The 'global' entry is selected. The 'Edit Web Auth Parameter' window is open, showing the 'General' tab. The 'Parameter-map Name' is set to 'global'. The 'Virtual IPv4 Address' is set to '192.0.2.1'. The 'Virtual IPv6 Address' is set to 'FE80:0:0:0:903A::11E4'. The 'Enable HTTP server for Web Auth' checkbox is checked. The 'Banner Configuration' section is visible at the bottom.

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

Other custom Web Auth Parameter Maps will inherit these settings

Recommended:

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

Adding a Guest SSID (LWA with internal portal)

Configuration > Security > Web Auth

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation is Configuration > Security > Web Auth. The 'Edit Web Auth Parameter' dialog box is open, showing the 'General' tab. The 'Parameter-map Name' is 'WEBAUTH_PMAP'. The 'Maximum HTTP connections' is 100. The 'Init-State Timeout(secs)' is 120. The 'Type' is set to 'consent'. The 'Banner Configuration' section is also visible. The 'Type' dropdown is highlighted with a green box.

Configuration > Security > Web Auth

Selected Rows: 0

Parameter Map Name
<input type="checkbox"/> global
<input type="checkbox"/> WEBAUTH_PMAP

10 items per page

General Advanced

Parameter-map Name: WEBAUTH_PMAP

Maximum HTTP connections: 100

Init-State Timeout(secs): 120

Type: consent

Turn-on Consent with Email: ☐

Captive Bypass Portal: ☐

Disable Success Window: ☐

Disable Logout Window: ☒

Disable Cisco Logo: ☐

Sleeping Client Status: ☐

Sleeping Client Timeout (minutes): 720

Cancel Update & Apply to Device

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

webauth = login + password

consent = accept terms and conditions

webconsent = login/pwd + terms & conditions

authbypass = not supported

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

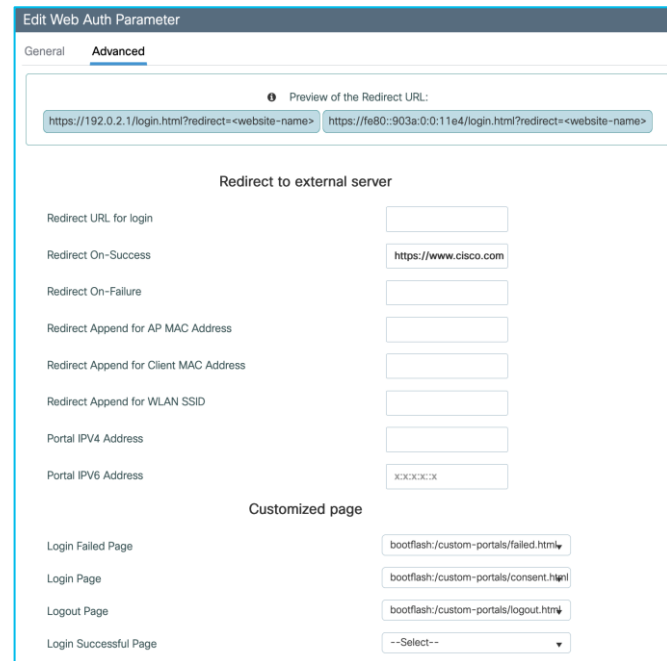
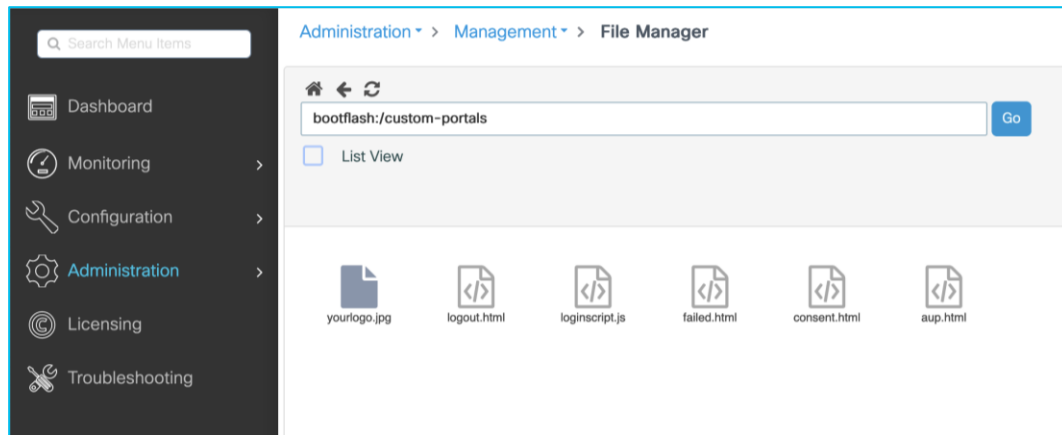
Method lists and custom files



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

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

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



Adding a Guest SSID (LWA with internal portal)

Configuration > Security > Web Auth

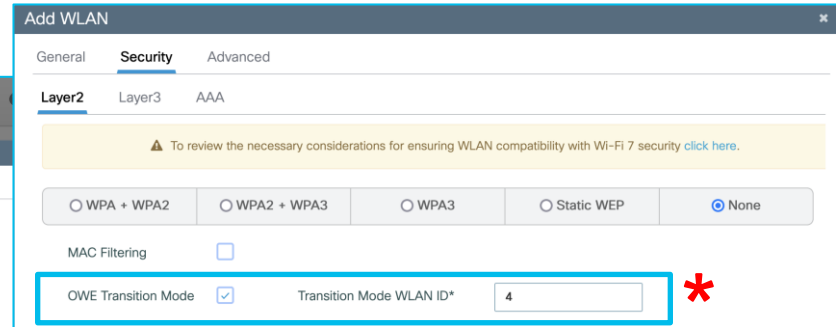
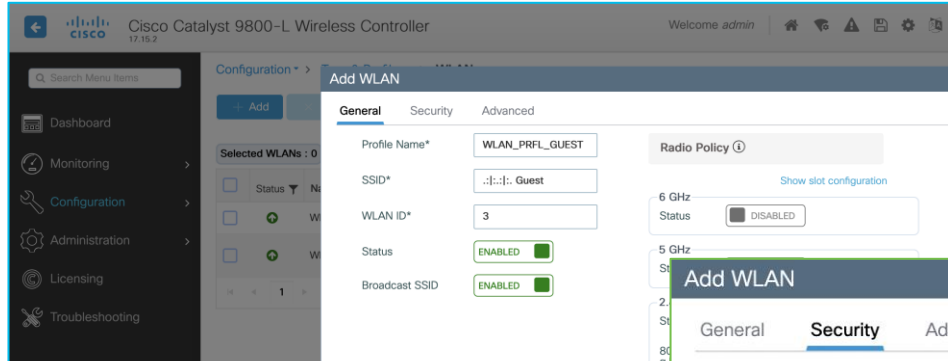
The screenshot shows the 'Add WLAN' configuration page in the Cisco Catalyst 9800-L Wireless Controller. The 'General' tab is active. The 'Profile Name*' is 'WLAN_PRFL_GUEST', 'SSID*' is 'Guest', and 'WLAN ID*' is '3'. The 'Status' is 'ENABLED' and 'Broadcast SSID' is 'ENABLED'. The 'Radio Policy' section shows '6 GHz' and '5 GHz' bands with 'Status' set to 'DISABLED' and 'ENABLED' respectively. The '2.4 GHz' band is also 'DISABLED'. The '802.11b/g Policy' is set to '802.11b/g'. The 'Apply to Device' button is visible at the bottom right.

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

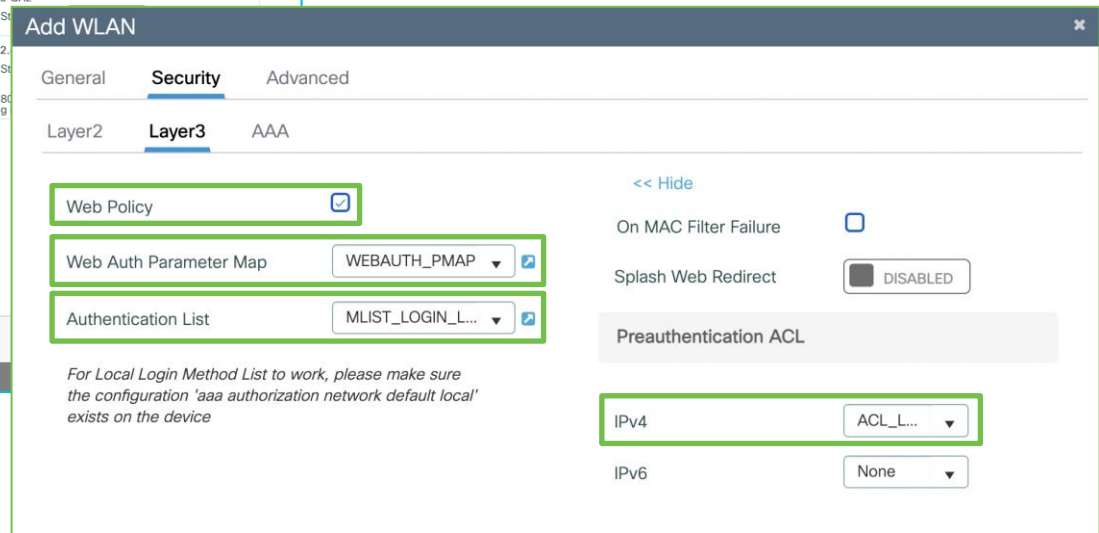
The screenshot shows the 'Add WLAN' configuration page in the Cisco Catalyst 9800-L Wireless Controller, specifically the 'Security' tab. The 'Layer2' tab is active. The 'Security' section shows 'WPA + WPA2', 'WPA2 + WPA3', 'WPA3', 'Static WEP', and 'None' options. The 'None' option is selected. The 'MAC Filtering' checkbox is unchecked. The 'OWE Transition Mode' checkbox is checked, and the 'Transition Mode WLAN ID*' is set to '4'. The 'Lobby Admin Access' checkbox is unchecked. The 'Fast Transition' section shows 'Status' set to 'Disabled', 'Over the DS' checkbox is unchecked, and 'Reassociation Timeout *' is set to '20'. A red asterisk is placed next to the 'Transition Mode WLAN ID*' field.

Adding a Guest SSID (LWA with internal portal)

Configuration > Security > Web Auth

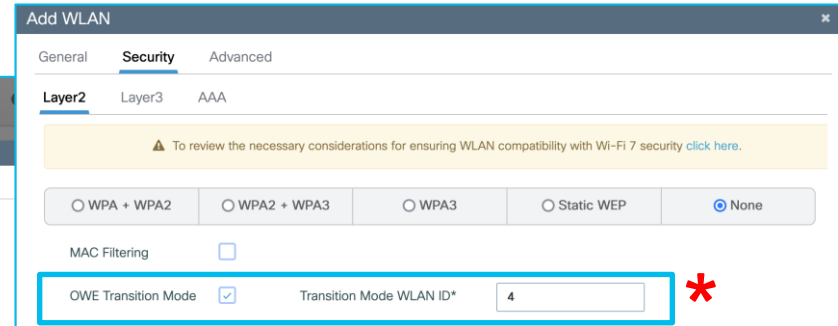
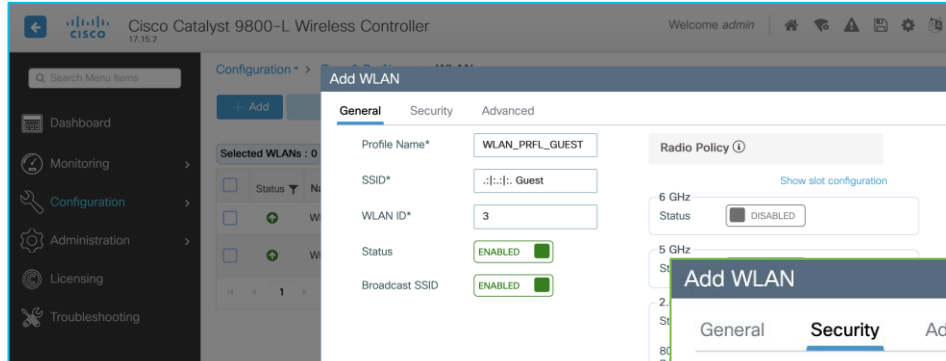


1. New guest WLAN with no L2 security (i.e., fully open) and OWE Transition Mode pointing to the future OWE WLAN ID
2. L3 security as Web Policy, pointing to our Web Auth Parameter Map, with an authC method list for local login and our ACL too

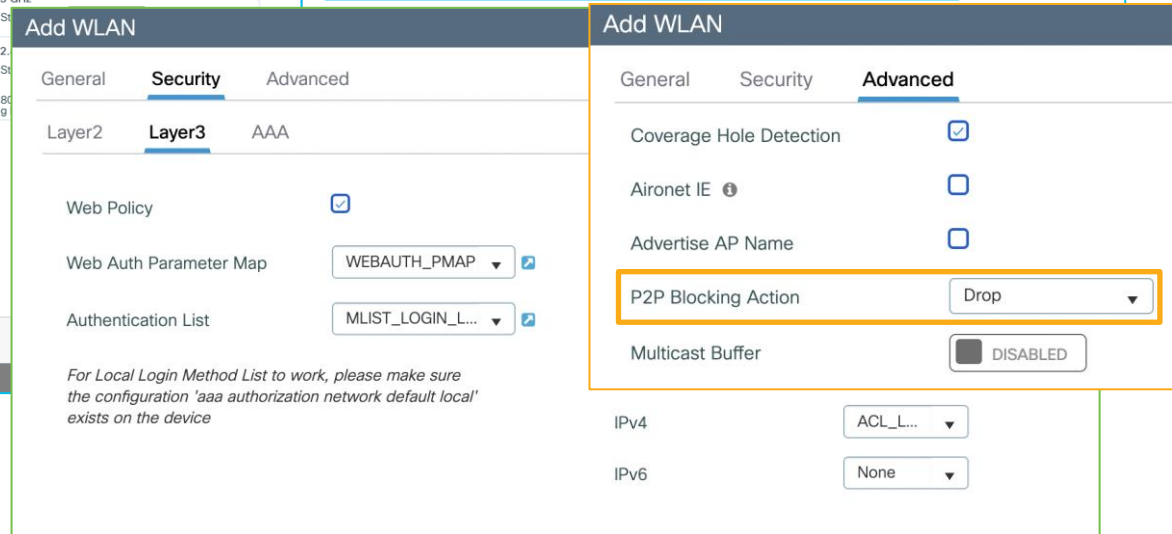


Adding a Guest SSID (LWA with internal portal)

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



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 screenshot displays the Cisco Catalyst 9800-L Wireless Controller interface. On the left, the navigation menu includes Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main area shows the 'WLANs' configuration page with a table 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. A modal window titled 'Clone of WLAN Profile (WLAN_PRFL_GUEST)' is open, showing the configuration for the new profile 'WLAN_PRFL_GUEST_OWE'. The 'General' tab is active, showing the SSID as ':-::-: Guest-OWE', WLAN ID as 4, and Status as 'ENABLED'. The 'Broadcast SSID' option is set to 'DISABLED'. The 'Radio Policy' section shows the 6 GHz status as 'DISABLED' (highlighted with a red star and a blue box), 5 GHz as 'ENABLED', and 2.4 GHz as 'DISABLED'. The '802.11b/g Policy' is set to '802.11b/g'. The 'Apply to Device' button is visible at the bottom right of the modal.

Configuration > Tags & Profiles > WLANs

Selected WLANs : 1

Status	Name	ID
<input type="checkbox"/>	WLAN_PRFL_EMPLOYEE	1
<input type="checkbox"/>	WLAN_PRFL_IOT	2
<input checked="" type="checkbox"/>	WLAN_PRFL_GUEST	3

Clone of WLAN Profile (WLAN_PRFL_GUEST)

General Security Advanced

Profile Name* WLAN_PRFL_GUEST_OWE

SSID* :-::-: Guest-OWE

WLAN ID* 4

Status ENABLED

Broadcast SSID DISABLED

Radio Policy

6 GHz Status DISABLED

5 GHz Status ENABLED

2.4 GHz Status DISABLED

802.11b/g Policy 802.11b/g

Cancel Apply to Device

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 ☐ WPA2 Policy ☐
GTK Randomize ☐ WPA3 Policy ☒
Transition Disable ☐ Beacon Protection ☐

WPA2/WPA3 Encryption

AES(CCMP128) ☒ CCMP256 ☐
GCMP128 ☐ GCMP256 ☒

Protected Management Frame

PMF

Association Comeback Timer*

SA Query Time*

Fast Transition

Status

Over the DS ☐

Reassociation Timeout *

Auth Key Mgmt (AKM)

FT + 802.1X ☐ 802.1X-SHA256 ☐
SUITEB192-1X ☐ OWE ☒
SAE ☐ FT + SAE ☐
SAE-EXT-KEY ☐ FT + SAE-EXT-KEY ☐

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

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The main menu on the left includes Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The 'Configuration' menu is selected, and the 'Add Policy Profile' dialog box is open. The dialog box has a warning at the top: 'Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.' The 'General' tab is active, showing the following fields:

- Name*: POLICY_PRFL_GUEST
- Description: Enter Description
- Status: ENABLED (checked)
- Passive Client: DISABLED
- IP MAC Binding: ENABLED (checked)
- Encrypted Traffic Analytics: DISABLED
- CTS Policy
 - Inline Tagging: ☐
 - SGACL Enforcement: ☐
 - Default SGT: 2-65519

On the right side of the dialog box, the 'WLAN Switching Policy' section is visible, showing the following settings:

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

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

We create our guest Policy Profile with its dedicated VLAN

Adding a Guest SSID (LWA with internal portal)

Configuration > Tags & Profiles > Policy

The image shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The 'Add Policy Profile' dialog box is open, displaying the 'General' tab. The 'Name*' field is set to 'POLICY_PRFL_GUEST'. The 'Status' is set to 'ENABLED'. The 'Passive Client' is set to 'DISABLED'. The 'IP MAC Binding' is set to 'ENABLED'. The 'Encrypted Traffic Analytics' is set to 'DISABLED'. The 'CTS Policy' section shows 'Inline Tagging' and 'SGACL Enforcement' as 'DISABLED', and 'Default SGT' as '2-65519'. A warning message at the top states: 'Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.'

We create our guest Policy Profile with its dedicated VLAN

The image shows the 'Add Policy Profile' dialog box with the 'Access Policies' tab selected. The 'RADIUS Profiling' checkbox is unchecked. The 'HTTP TLV Caching' and 'DHCP TLV Caching' checkboxes are checked. The 'WLAN Local Profiling' section shows 'Global State of Device Classification' as 'default' and 'Local Subscriber Policy Name' as 'Search or Select'. The 'VLAN' section shows 'VLAN/VLAN Group' as 'VLAN_GUEST' (selected from a dropdown menu) and 'Multicast VLAN' as 'default'. The 'WLAN ACL' section shows 'IPv4 ACL' and 'IPv6 ACL' as 'Search or Select'. The 'URL Filters' section shows 'Pre Auth' and 'Post Auth' as 'Search or Select'. A warning message at the top states: 'Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.'

Configuring the Policy Profile

Configuration > Tags & Profiles > Policy

Add Policy Profile

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

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

WLAN Timeout

Session Timeout (sec) ⓘ

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec) ☒

Guest LAN Session Timeout ☐

DHCP

IPv4 DHCP Required ☒

DHCP Server IP Address

DHCP Server VRF ⓘ

Fabric Profile ☐ ⓘ

Link-Local Bridging ☐

mDNS Service Policy ⓘ

Hotspot Server ⓘ

L3 Access ☐ DISABLED

User Defined (Private) Network

Status ☐

Drop Unicast ☐

DNS Layer Security

DNS Layer Security Parameter Map Clear

Policy Proxy Settings

ARP Proxy ☒ **ENABLED**

IPv6 Proxy

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

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled 'Configuration > Tags & Profiles > Tags'. The 'Policy' tab is selected, showing a list of Policy Tags: POLICY_TAG_CORP, POLICY_TAG_BRANCH, and default-policy-tag. The 'Edit Policy Tag' window for POLICY_TAG_CORP is open. It shows the Name as POLICY_TAG_CORP and a description field. Below, the 'WLAN-POLICY Maps' section shows a table with 4 maps. The row for WLAN_PRFL_GUEST and POLICY_PRFL_GUEST is highlighted with a blue box.

WLAN Profile	Policy Profile
<input type="checkbox"/> WLAN_PRFL_IOT	POLICY_PRFL_IOT
<input type="checkbox"/> WLAN_PRFL_EMPLOYEE	POLICY_PRFL_EMPLOYEE
<input type="checkbox"/> WLAN_PRFL_GUEST	POLICY_PRFL_GUEST
<input type="checkbox"/> WLAN_PRFL_GUEST_OWE	POLICY_PRFL_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

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled 'Configuration > Tags & Profiles > Tags'. The 'Policy' tab is selected, showing a list of Policy Tags: POLICY_TAG_CORP, POLICY_TAG_BRANCH, and default-policy-tag. The 'Edit Policy Tag' window for POLICY_TAG_BRANCH is open. It shows the Name as POLICY_TAG_BRANCH and a description field. Below, the 'WLAN-POLICY Maps' section shows a table with 4 maps. The row for WLAN_PRFL_GUEST and POLICY_PRFL_GUEST is highlighted with a blue box.

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

Additional references for Guest WLANs

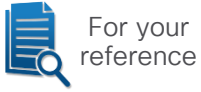


BRKEWN-2284

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

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

Additional references for Guest WLANs



For your
reference

- 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>

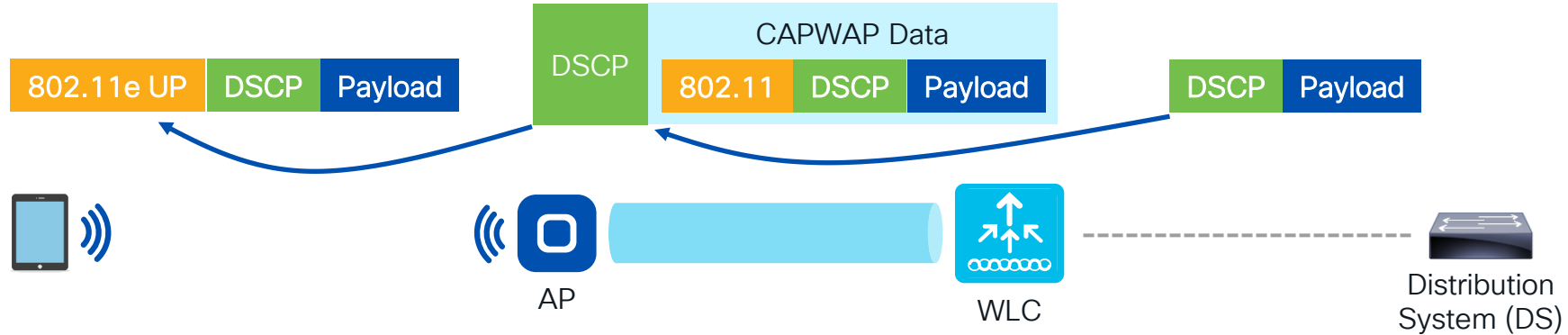
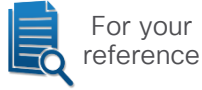
Further tweaks



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)

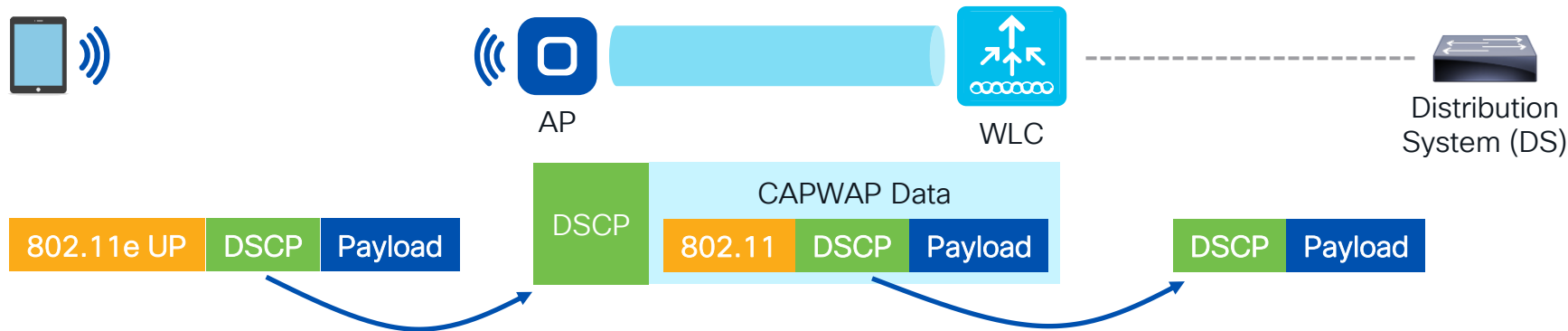
QoS – Trust DSCP Upstream: the one to start with

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
```

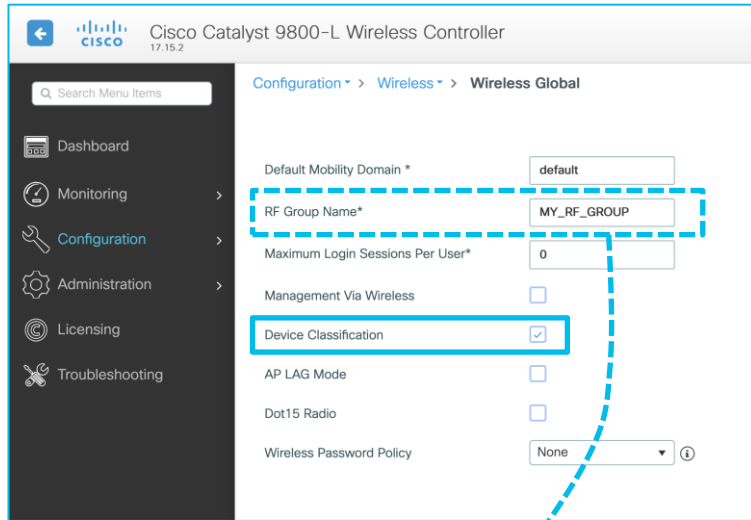


Upstream: the 802.11e UP value from the endpoint (if any) is ignored; the original DSCP value is used to mark the CAPWAP data tunnel too, then preserved all the way up to the DS.
(assuming no remarking is applied at the WLC level)



Devices and applications visibility

Configuration > Wireless > Wireless Global



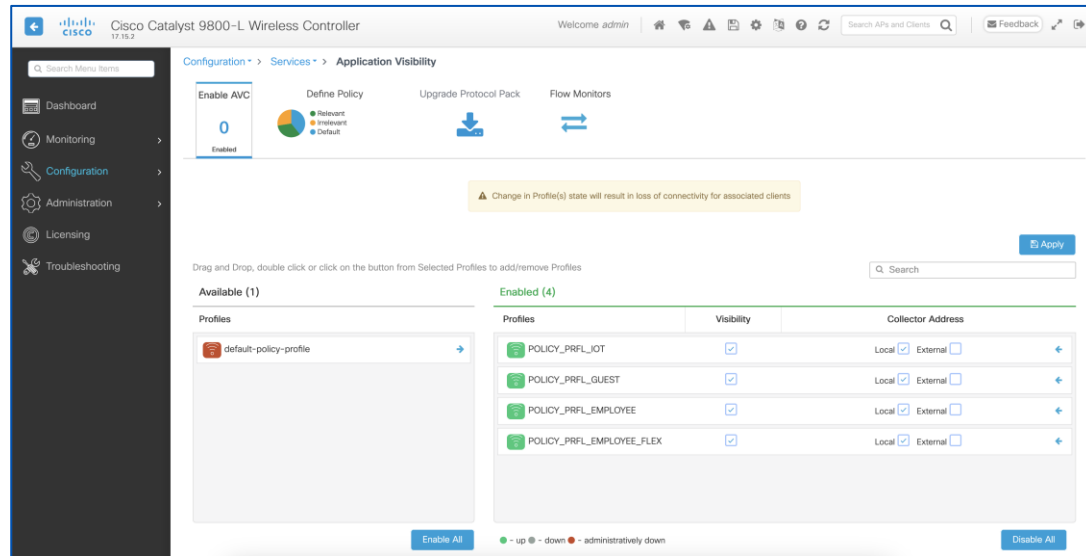
Especially during a PoC/test, we may want to keep the RF group name unique, so that it does not match and interact with others already in production (unless needed)

CISCO Live!

✎ 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



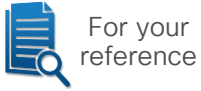
If not already enabled, let's turn on CleanAir



Configuration > Radio Configurations > CleanAir

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

Energy efficiency



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

Configuration > Tags & Profiles > Power Profile

Selected Rows: 0

Profile Name: Add Power Profile

Name*: PWR_PRFL_1G_1X1

Description: Enter Description

Power Save Client Threshold: 3

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

Selected Rows: 0

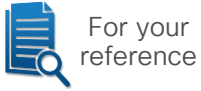
Sequence number	Interface	Interface ID	Parameter	Parameter value
0	Ethernet	GigabitEthernet0	Speed	1000 MBPS
1	Radio	2.4 GHz	Spatial Stream	1x1
2	Radio	5 GHz	Spatial Stream	1x1
3	Radio	Secondary 5 GHz	Spatial Stream	1x1
4	Radio	6 GHz	Spatial Stream	1x1

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



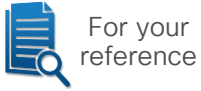
Configuration > Tags & Profiles > Calendar (i.e., when the APs should do it)

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation is Configuration > Tags & Profiles > Calendar. A modal dialog titled 'Add Calendar Profile' is open. It contains a warning 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'. The form fields are: Name* (CALENDAR_PRFL_NIGH), Recurrence (Daily), Start Time (22:00:00), and End Time (06:00:00). At the bottom, there 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)

Configuration > Tags & Profiles > AP Join

AP Join Profile Name

default-ap-profile

1 10

Edit AP Join Profile

General Client CAPWAP AP Management Security ICap QoS Geolocation

Name* default-ap-profile

Description default ap profile

Country Code NL

Deployment Mode Default

Time Zone

☒ Not Configured

☐ Use-Controller

☐ Delta from WLC

LED State ☒

LAG Mode ☐

NTP Server 0.0.0.0

GAS AP Rate Limit ☐

USB Enable ☐

Apphost ☐

Fallback to DHCP ☒

OfficeExtend AP Configuration

Local Access ☒

Link Encryption ☒

Rogue Detection ☐

Provisioning SSID ☒

Antenna Monitoring

Antenna Monitoring ☐

RSSI Fall Threshold(dB)* 40

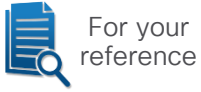
Weak RSSI(dBm)* -60

Detection Time(min)* 12

Cancel Update & Apply to Device

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)

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

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.

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

...and don't forget to save the configuration!



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



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.

Contact me at: fziliott@cisco.com



Thank you

CISCO *Live!*

GO BEYOND

The background of the slide features a series of overlapping, teardrop-shaped elements in various shades of blue, ranging from light sky blue to deep navy blue. These shapes are arranged in a way that creates a sense of depth and movement, resembling a stylized horizon or a series of waves. The overall composition is clean and modern, with the text elements clearly legible against the white background.