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 Cisco Systems
  - 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`

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
```

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

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 degault GW is the wireless management's one

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

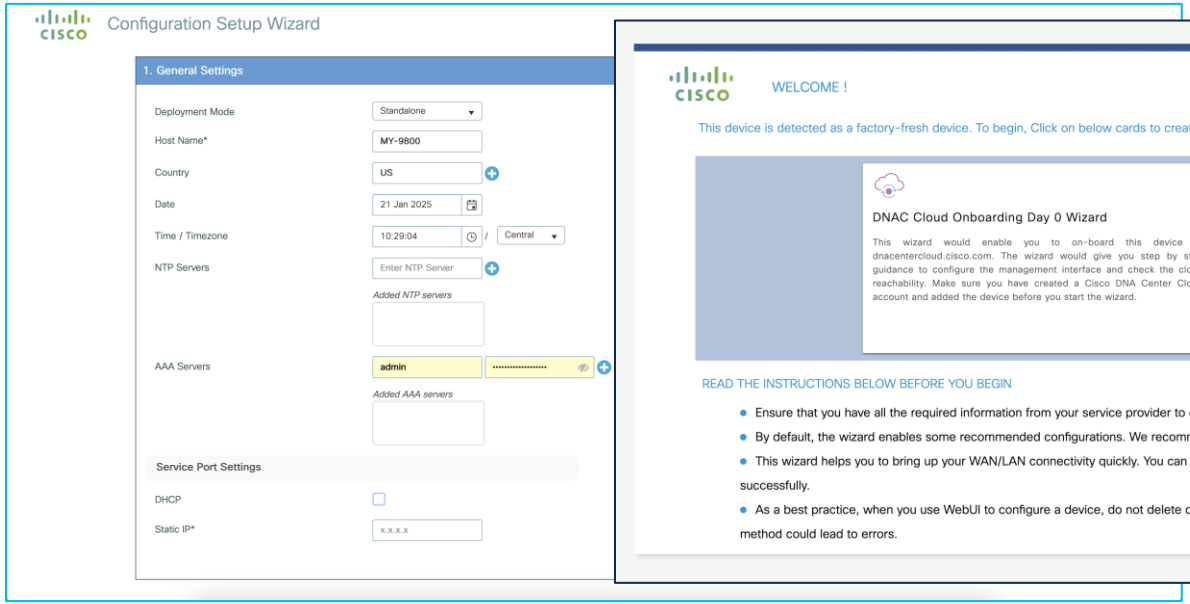
For easier troubleshooting logs/debugs

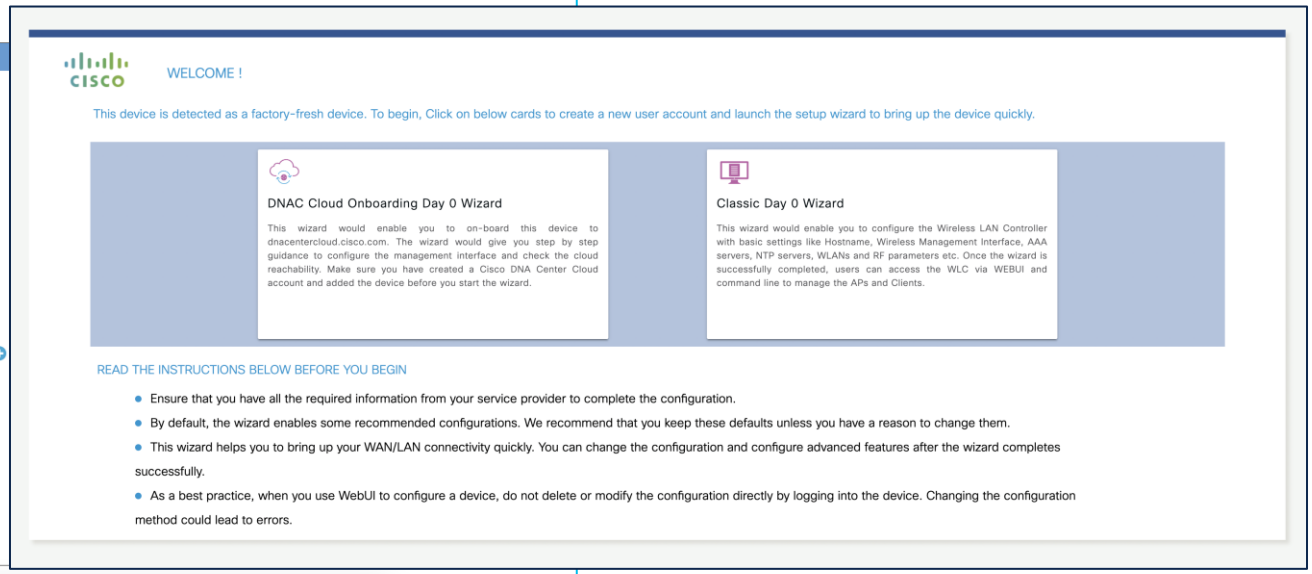
To increase the "consistency" of GUI access, we can fix a trustpoint (to keep it simple, it could be CISCO_IDEVID_SUDI), as well as a source interface, for all HTTPS admin traffic

Country code

For your reference

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





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

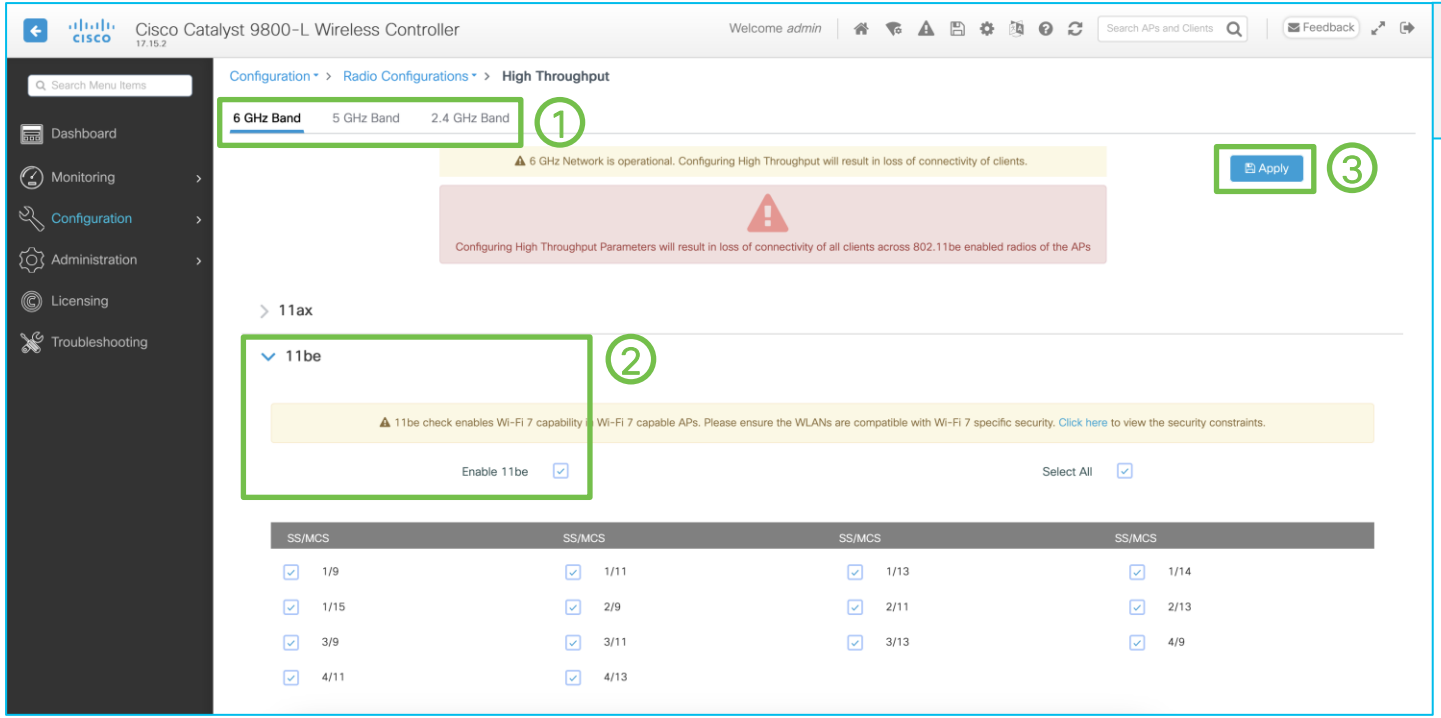
```
no ap dot11 24ghz shutdown
no ap dot11 5ghz shutdown
```

```
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
```

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

802.11be / Wi-Fi 7 must be explicitely enabled

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




```
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...

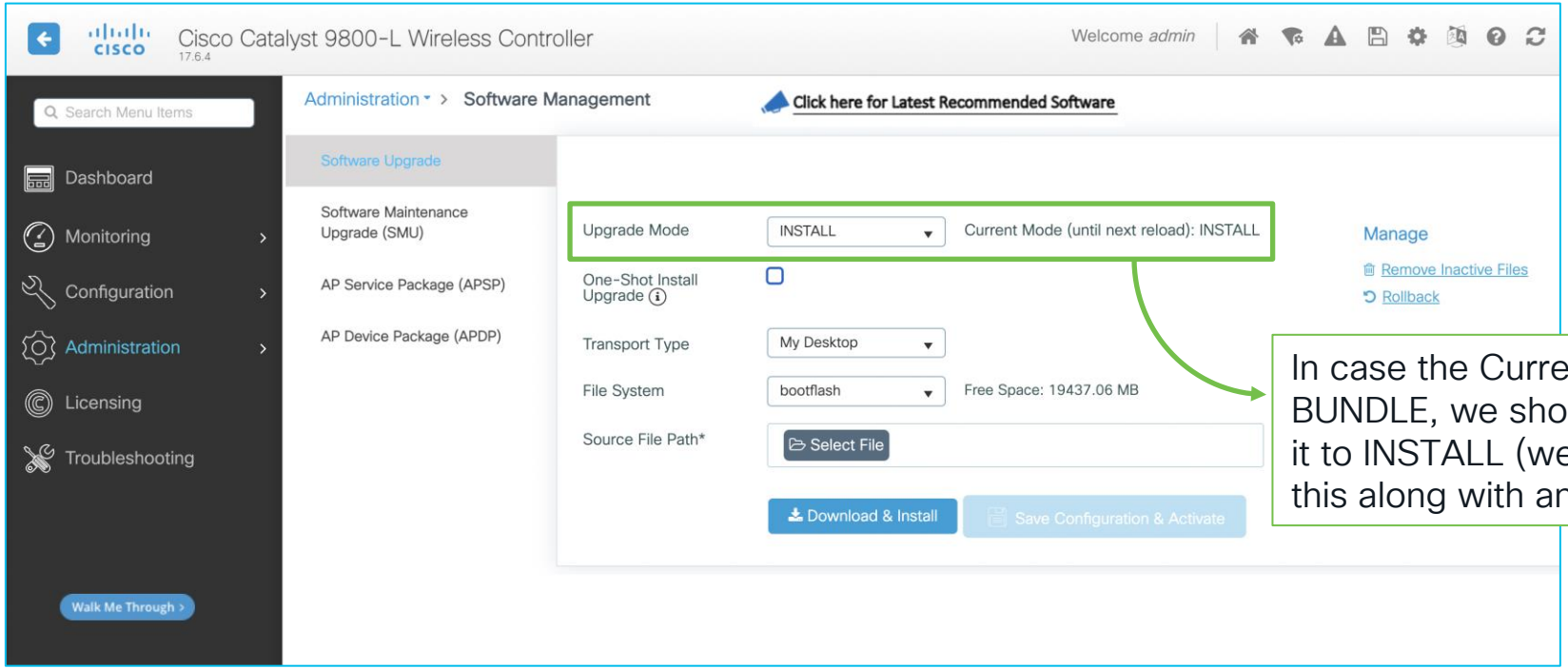
Save! Save! Save!

(`wr` ➔ `write memory`)

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

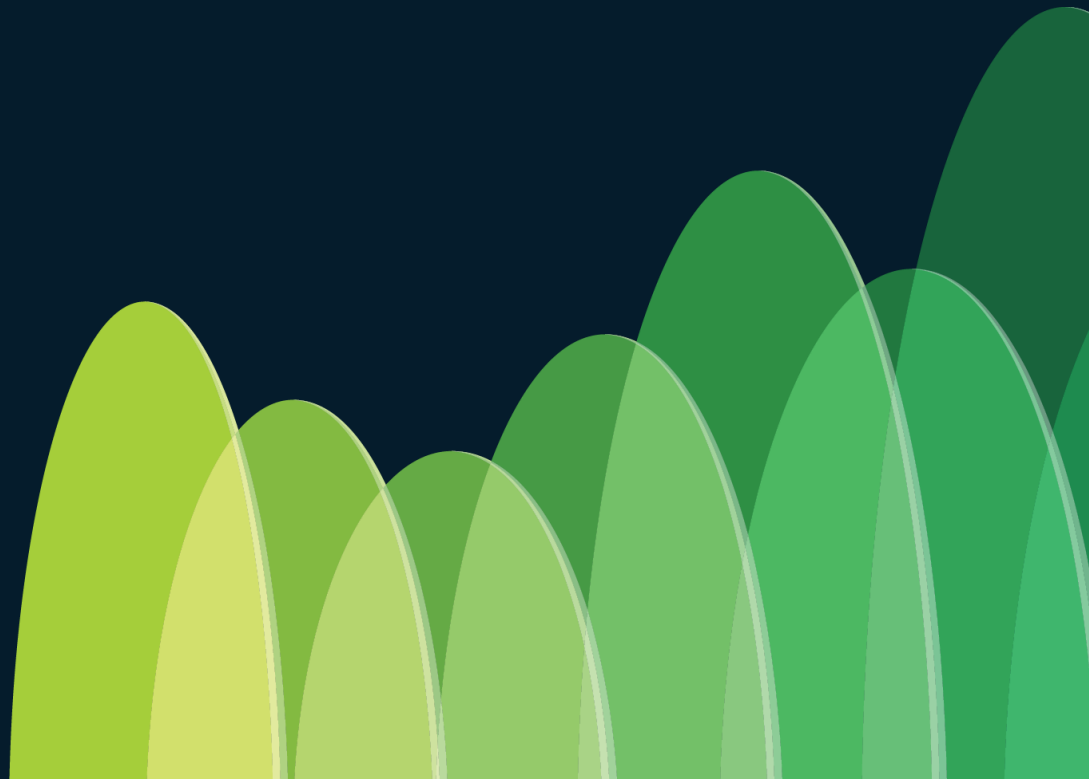
For your reference

Administration > Software Management



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



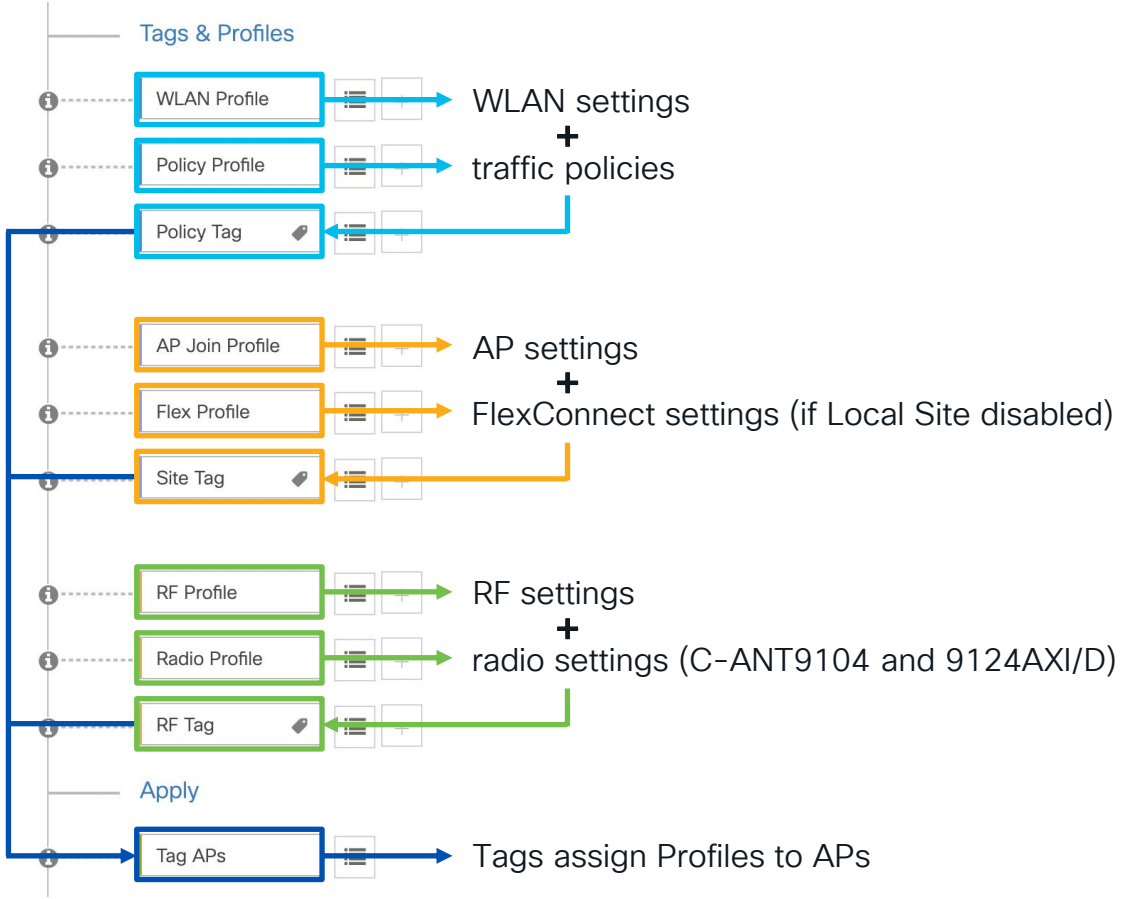
Profiles and Tags: the main configuration objects

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)

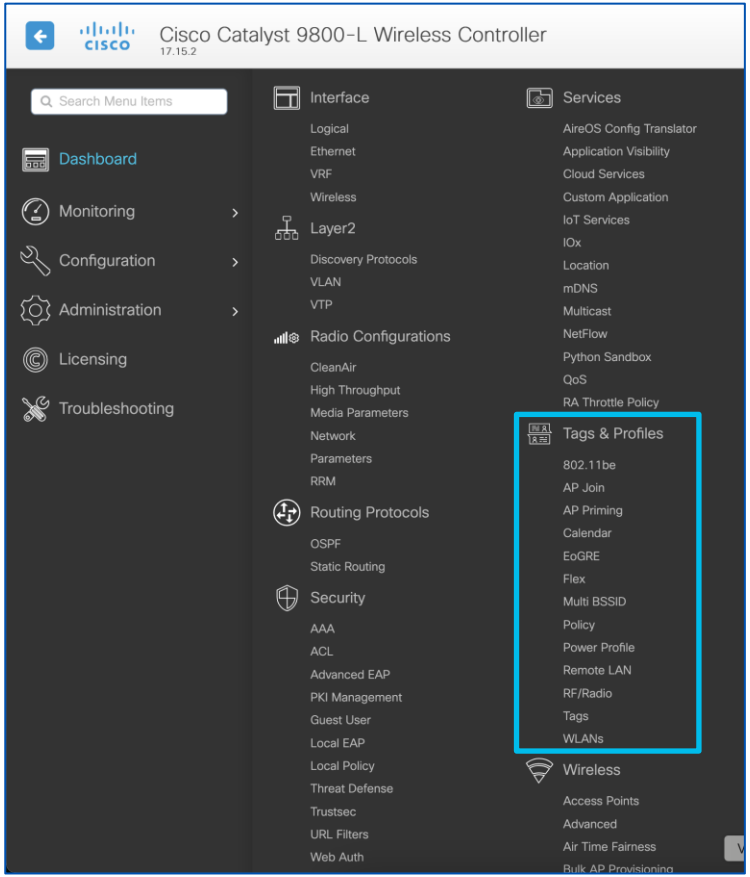
Profiles and Tags: the main configuration objects

Configuration >
Wireless Setup >
Advanced >
Start Now



Profiles and Tags: a more dedicated menu

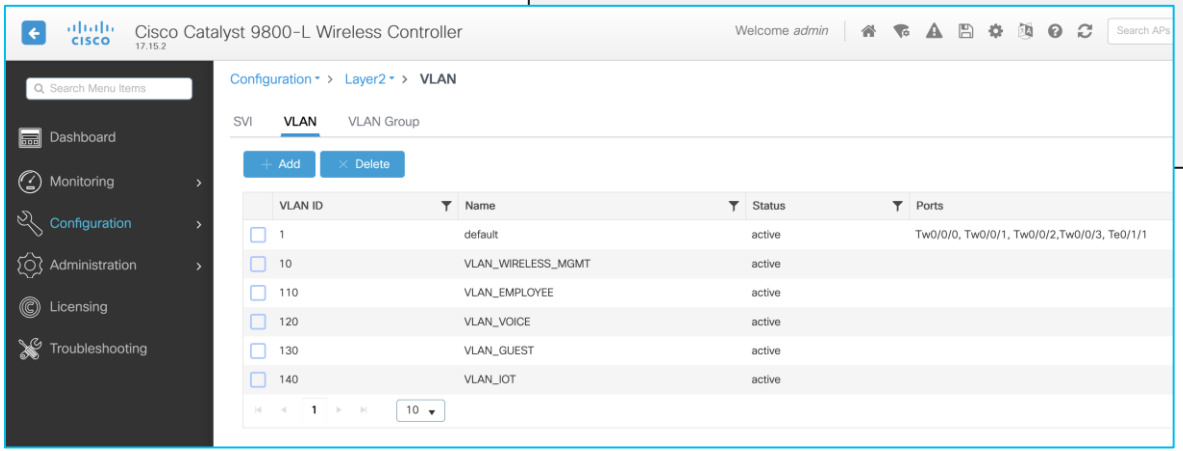
Configuration >
Tags & Profiles



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
```

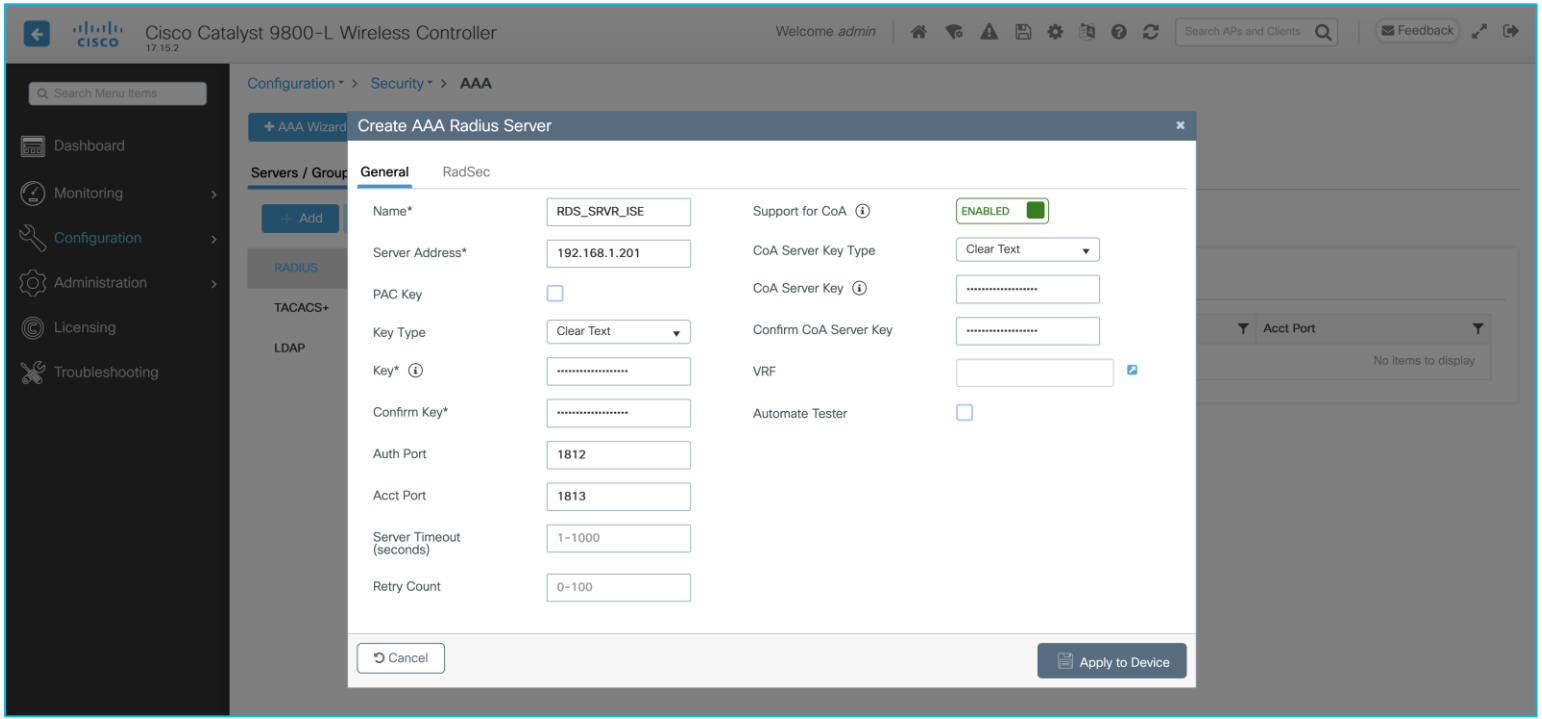
```
show vlan brief

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
```



Configuration > Layer2 > VLAN (VLAN tab)

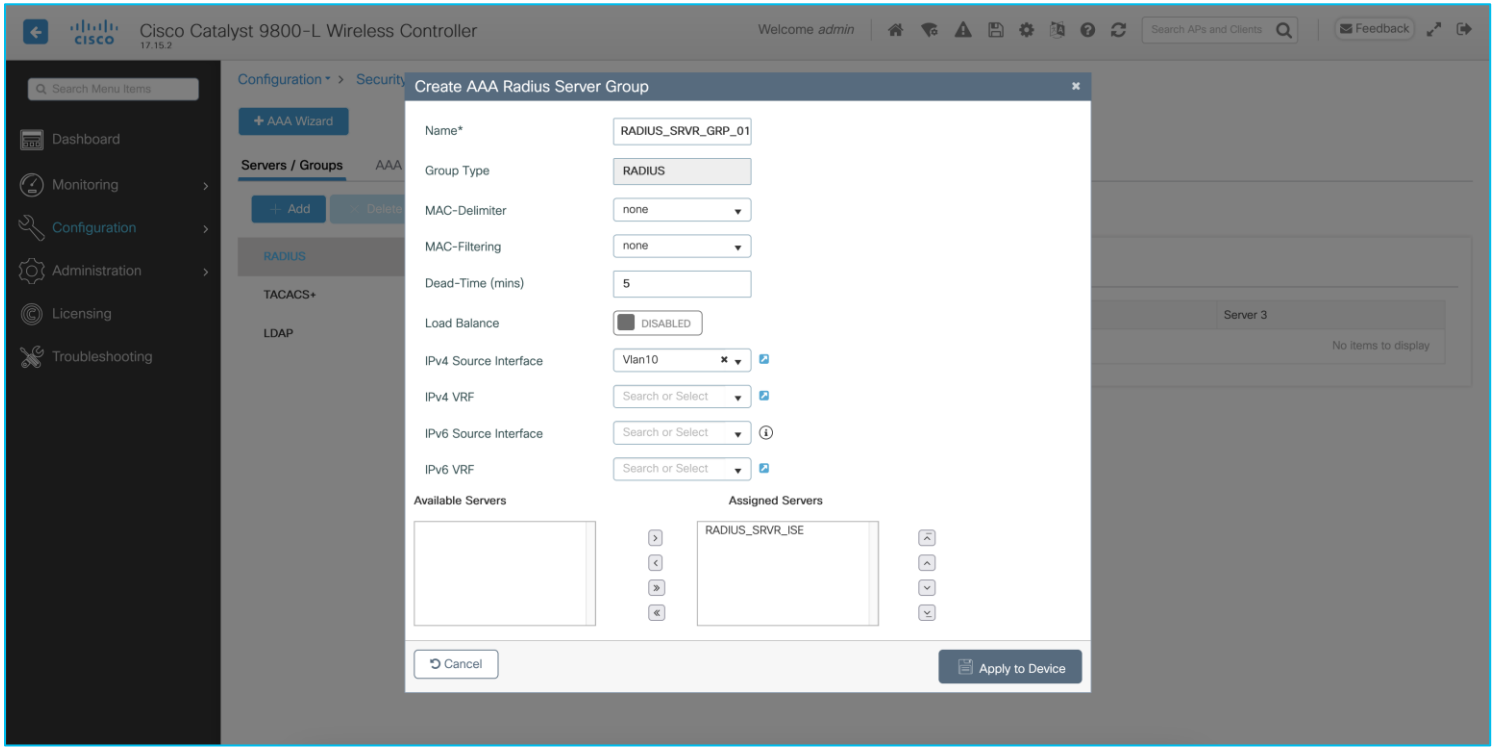
Configuring a RADIUS server

Configuration > Security > AAA > Add RADIUS Server



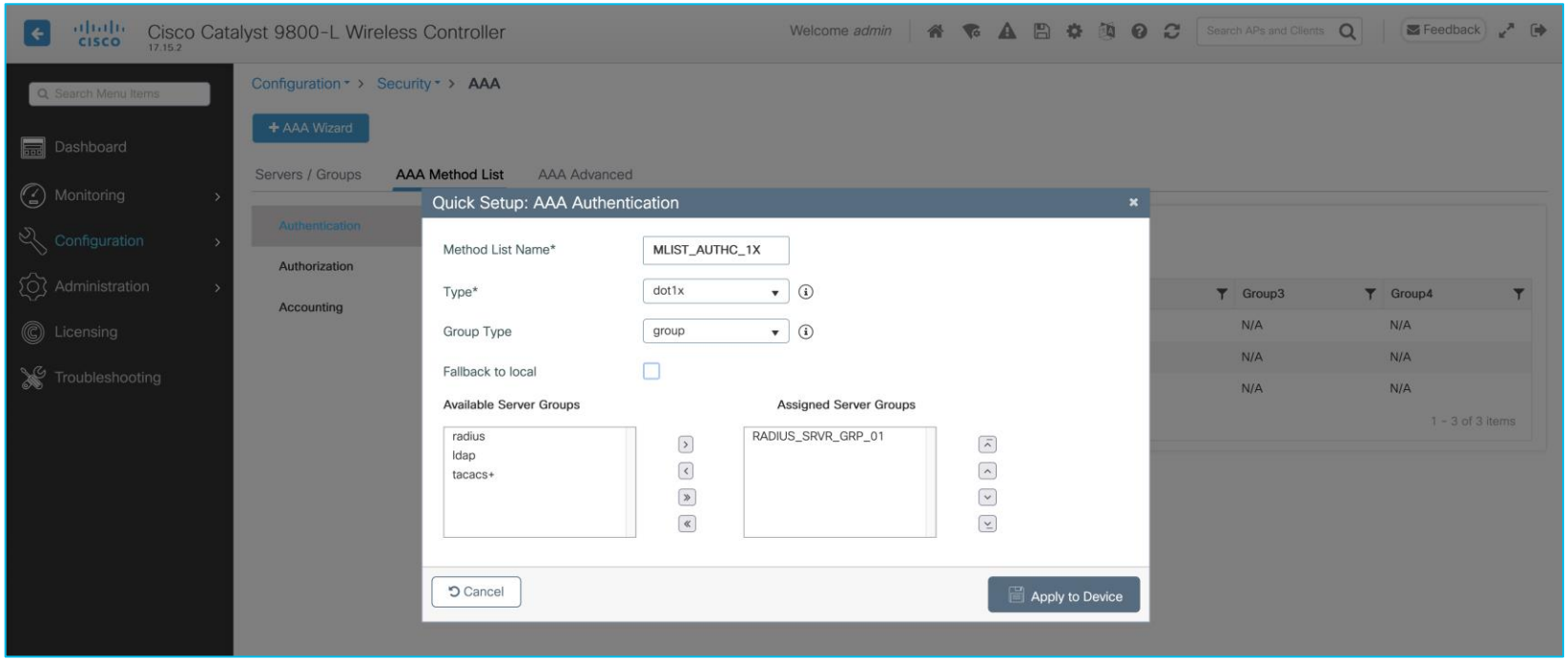
Configuring a RADIUS server group

Configuration > Security > AAA > Add RADIUS Server Group



Configuring a AAA Method List for 802.1X

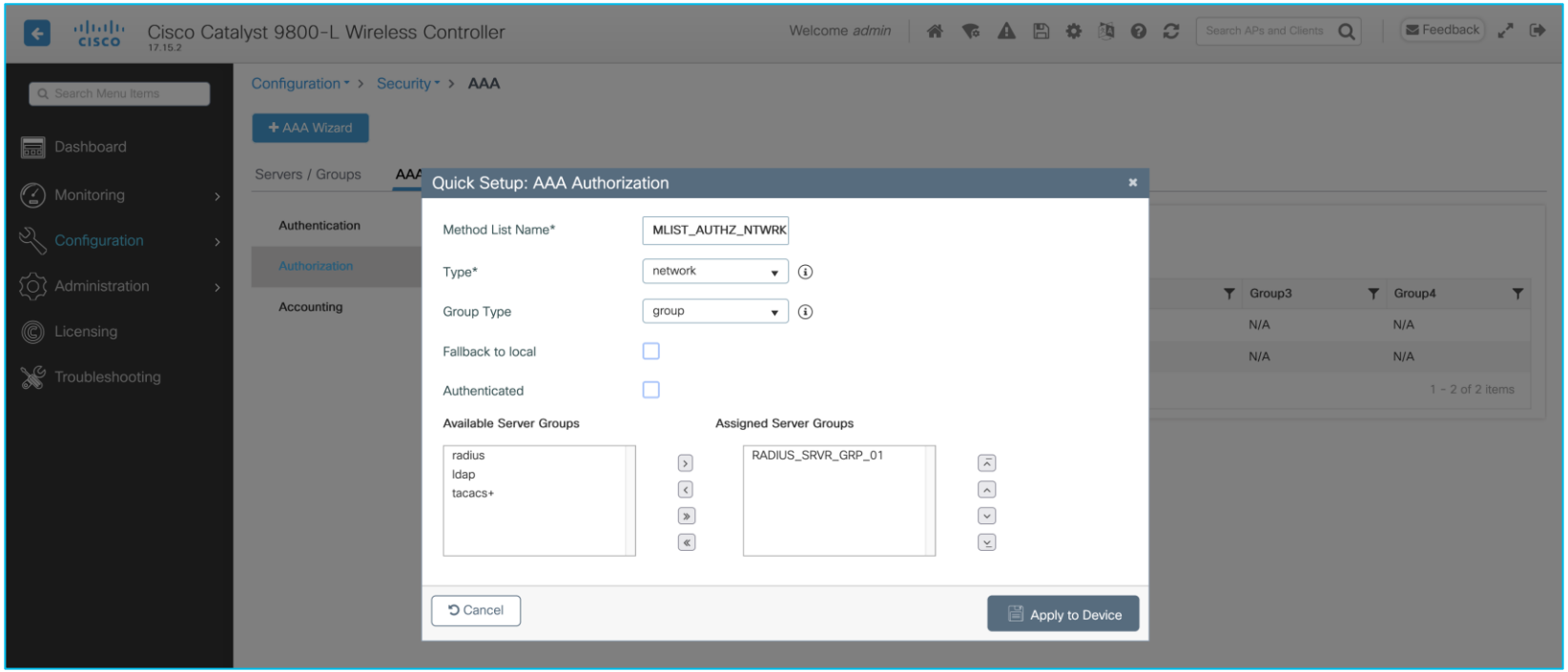
Configuration > Security > AAA > AAA Method List > Authentication > Add (Type = dot1x)



AAA Method List for authorization

For your reference

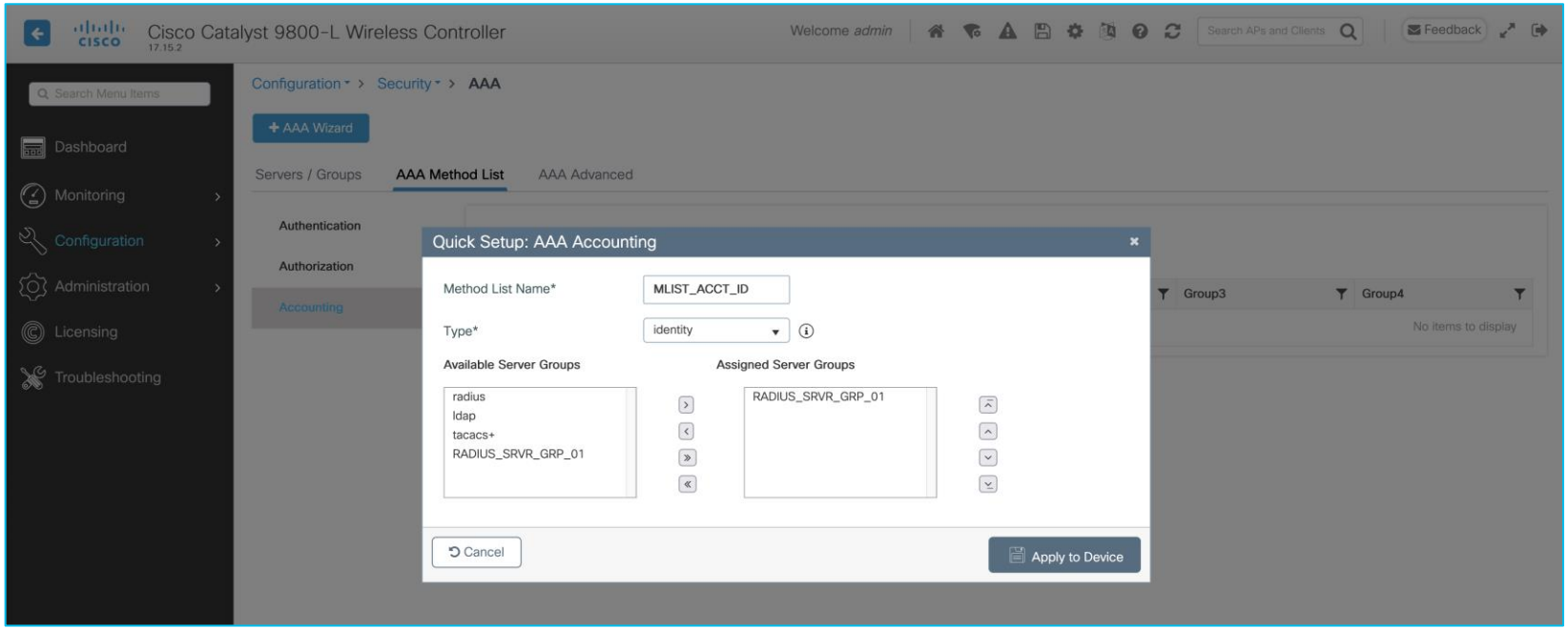
Configuration > Security > AAA > AAA Method List > Authorization > Add (Type = network)



Mainly used for MAC filtering based WLANs

Configuring a AAA Method List for accounting

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

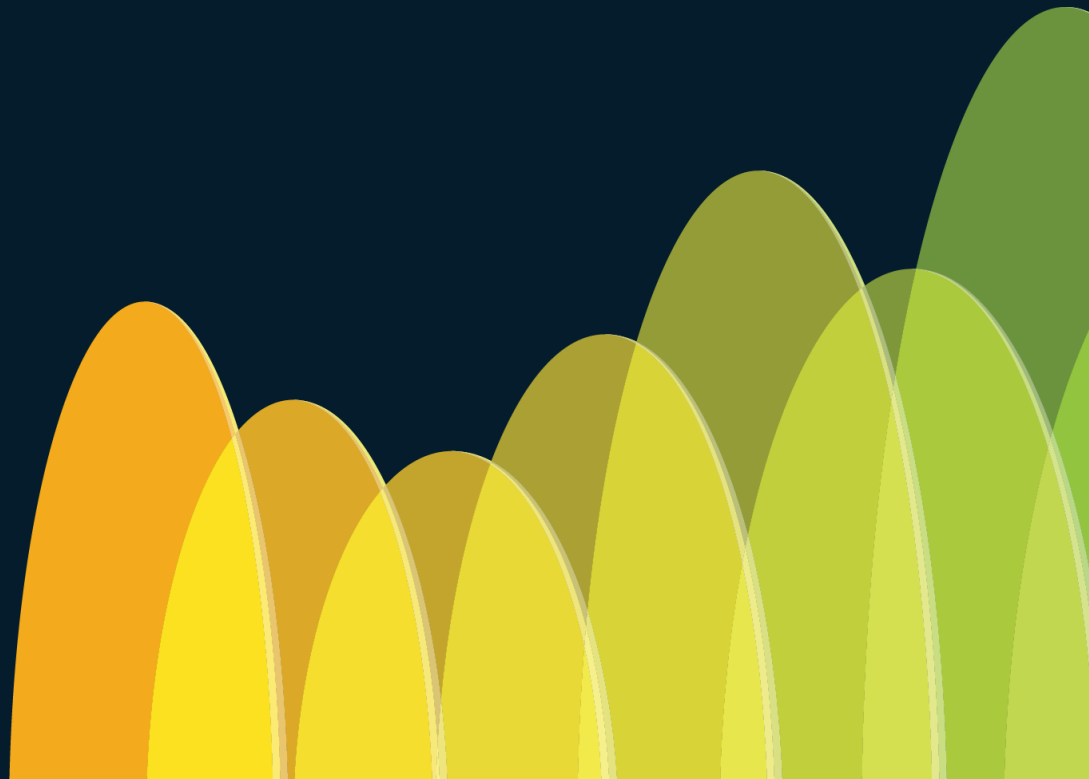


Or also with a quick CLI copy/paste

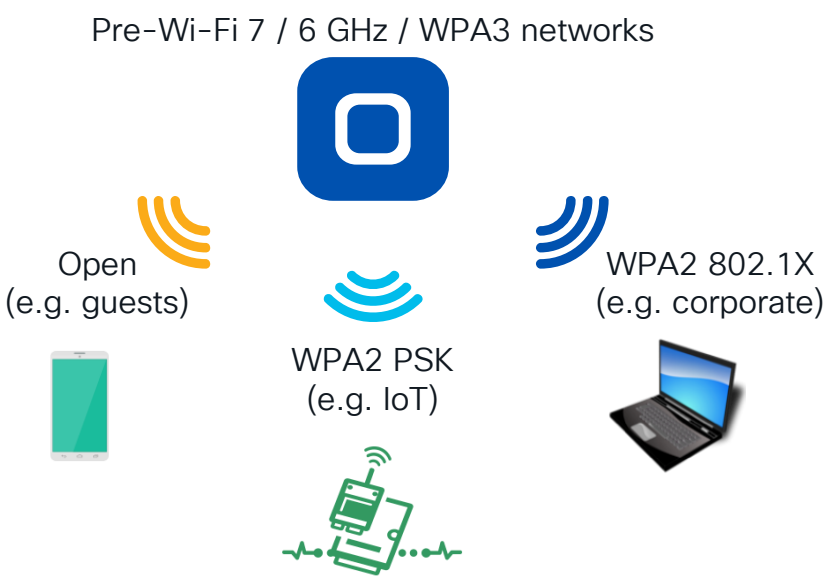
For your reference

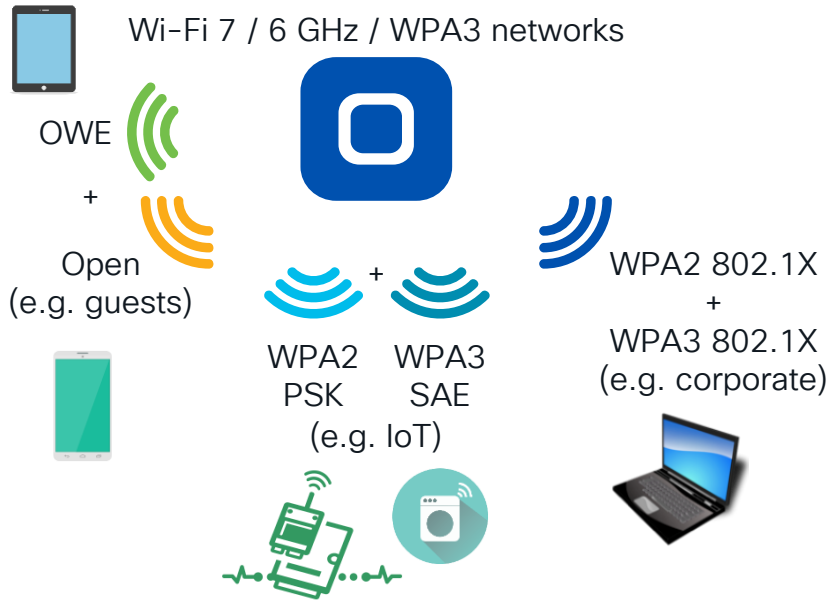
```
radius server RADIUS_SRVR_ISE
 address ipv4 192.168.1.201 auth-port 1812 acct-port 1813
 key <RADIUS_SHARED_SECRET>
!
aaa server radius dynamic-author
 client 192.168.1.201 server-key <RADIUS_SHARED_SECRET>
!
aaa group server radius RADIUS_SRVR_GRP_01
 server name RADIUS_SRVR_ISE
 ip radius source-interface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



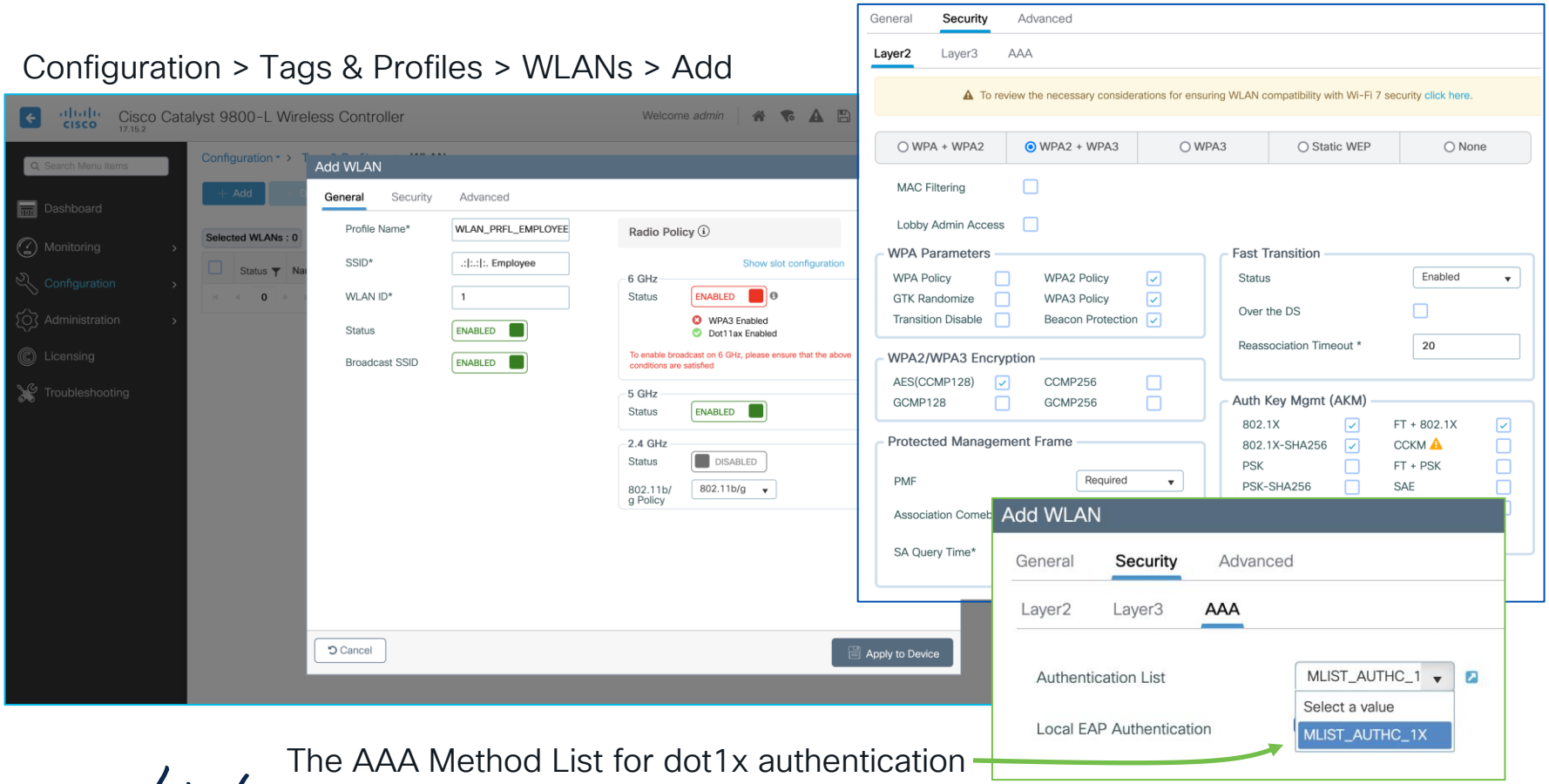
Wi-Fi 7 features mandate WPA3/OWE





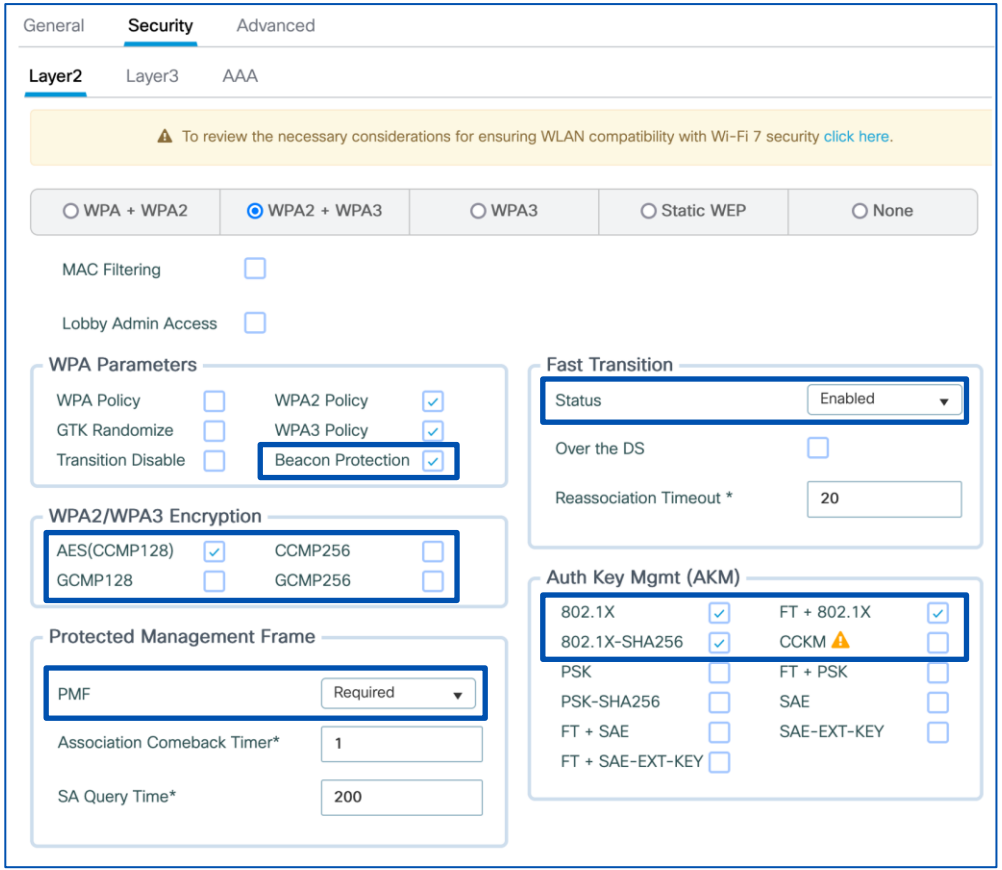
Configuring an 802.1X WLAN Profile

Configuration > Tags & Profiles > WLANs > Add



The AAA Method List for dot1x authentication

Zoom on Layer 2 Security for Wi-Fi 7 support



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

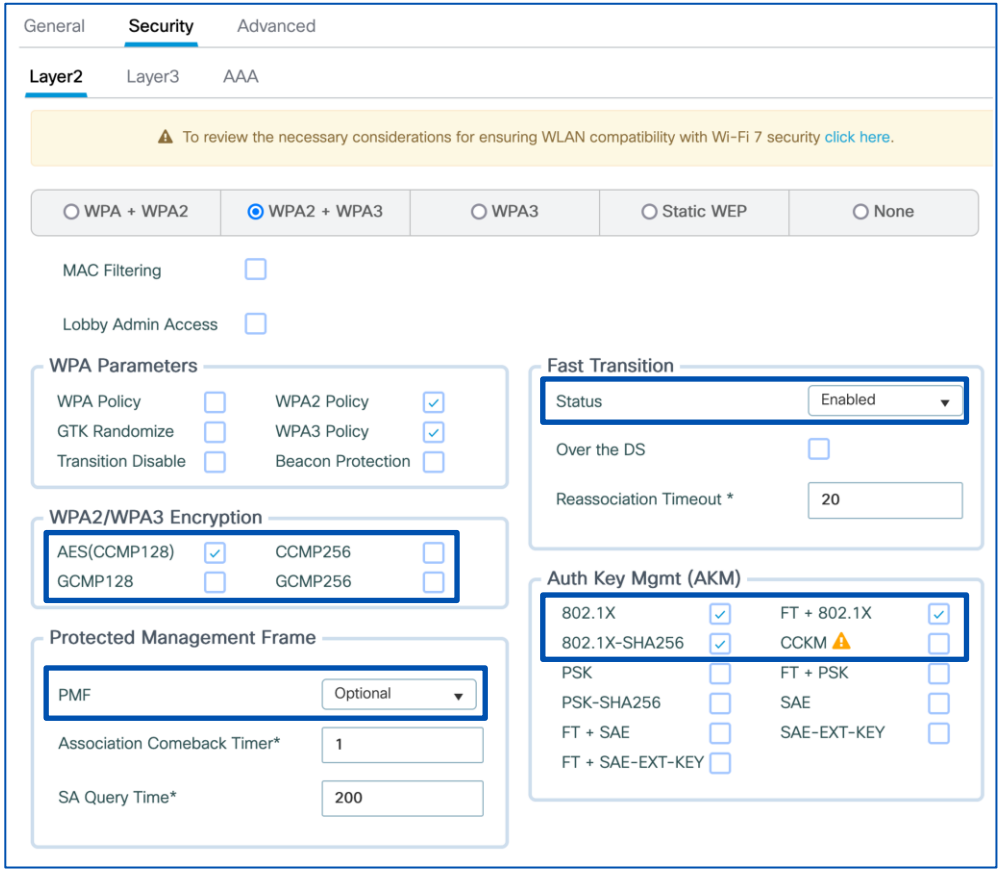
No “Adaptive Enabled”, as it would benefit Apple/Samsung endpoints only

Over the DS = unchecked

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

For max WPA2 compatibility (no Wi-Fi 7)

For your reference



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

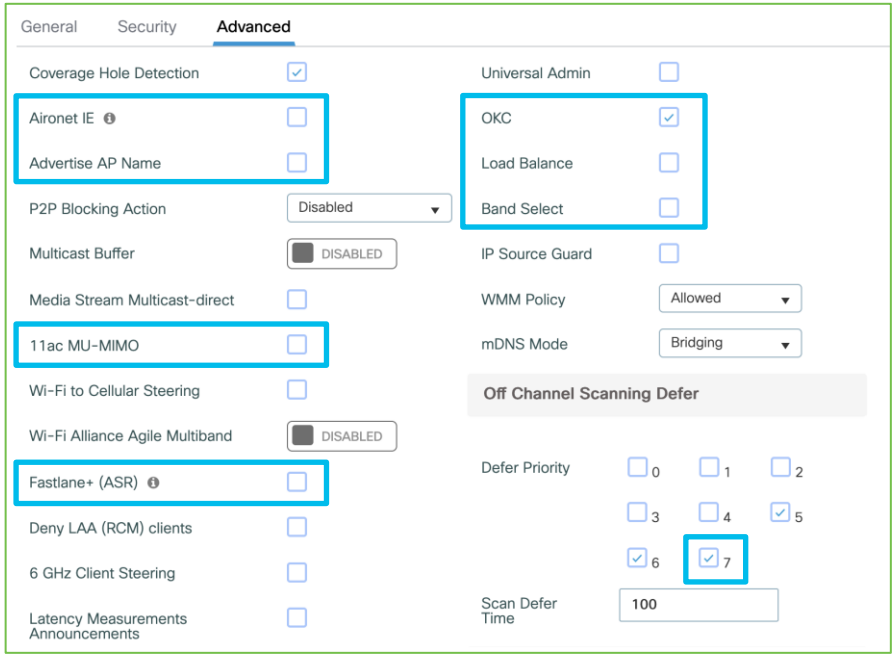
WPA2/WPA3 settings:
- AES(CCMP128)

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

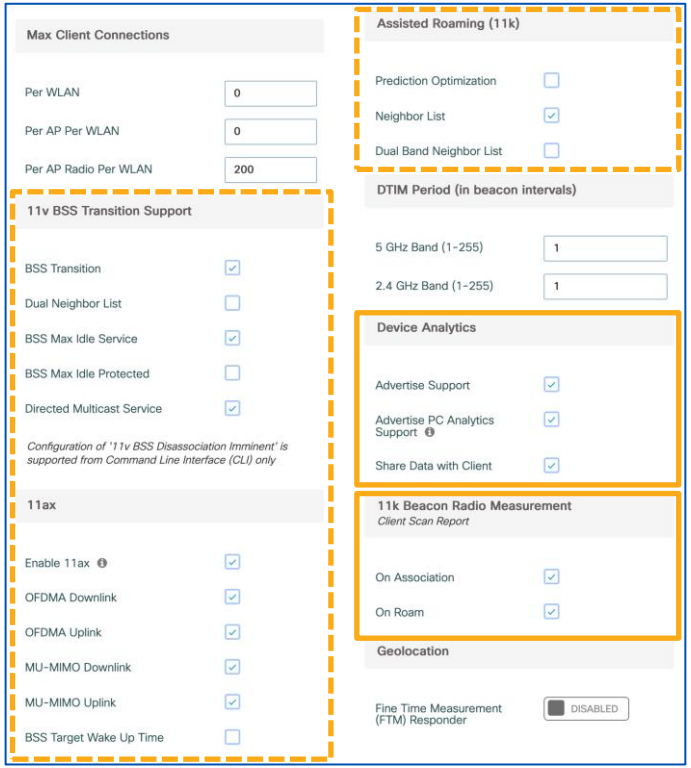
WLAN Profile > Advanced



- 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

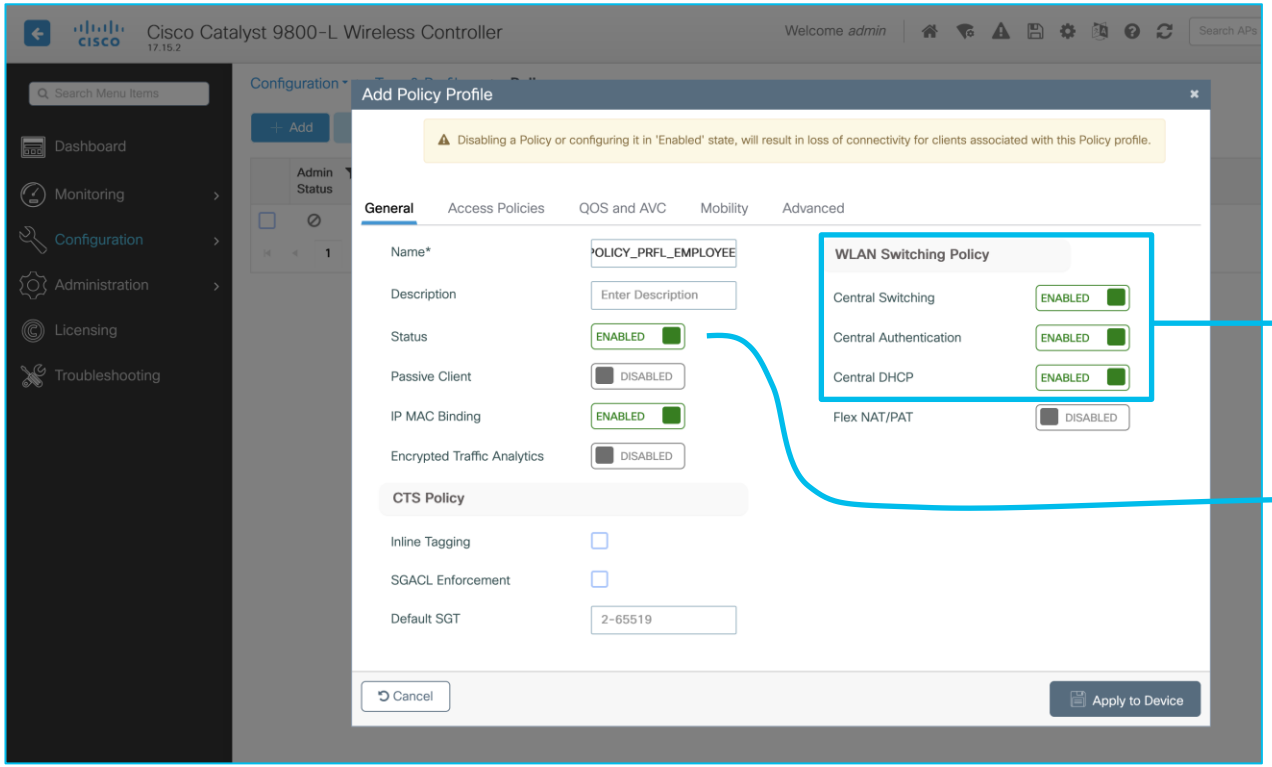
WLAN Profile > Advanced



- 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

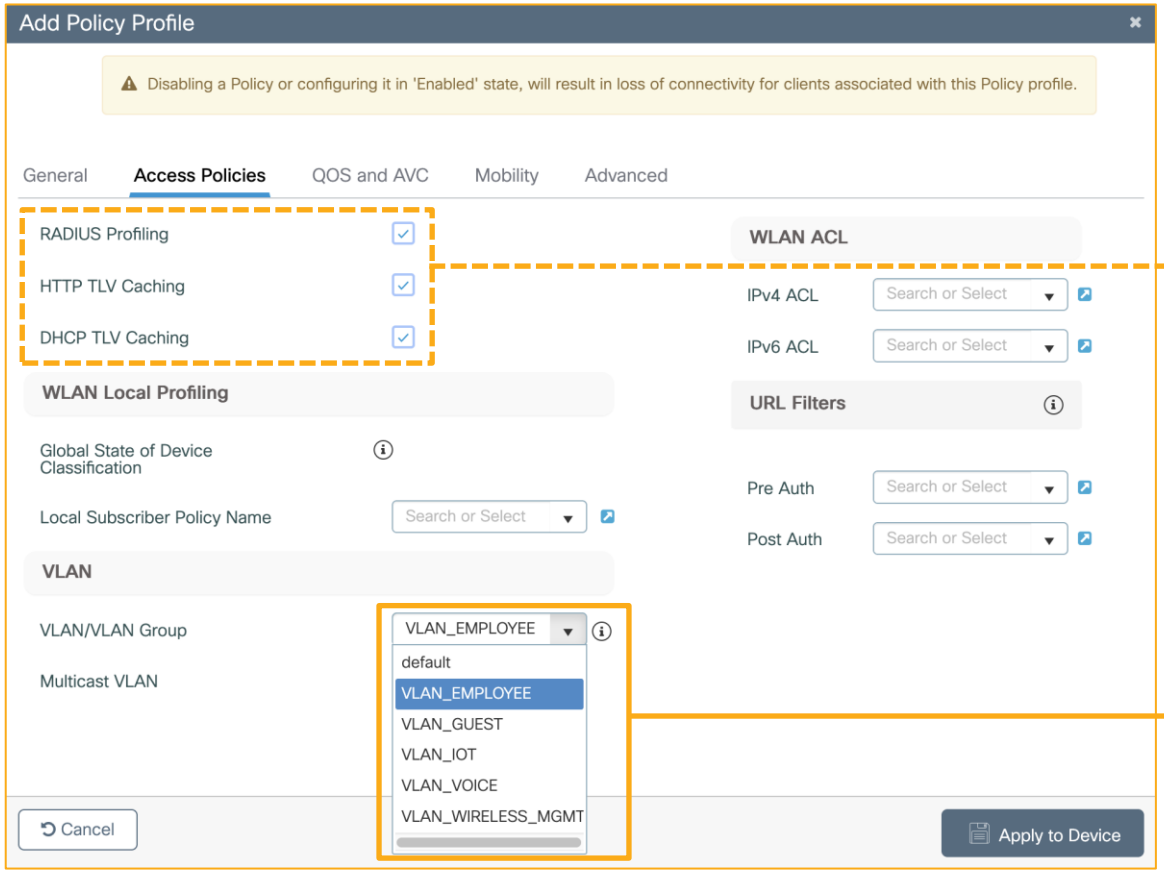
Configuration > Tags & Profiles > Policy > Add



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

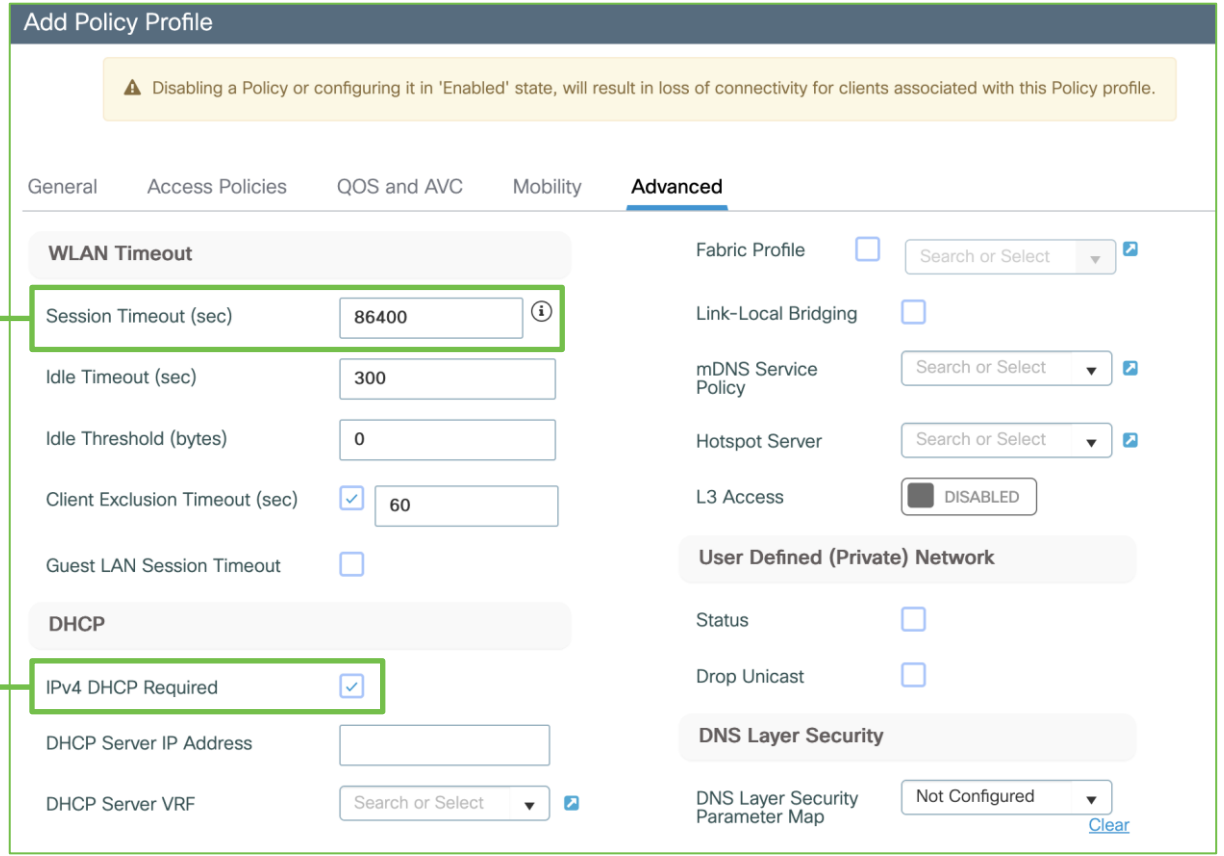
If we are not dynamically assigning VLANs via RADIUS, we can select the centrally switched VLAN under the Access Policies tab of the Policy Profile

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



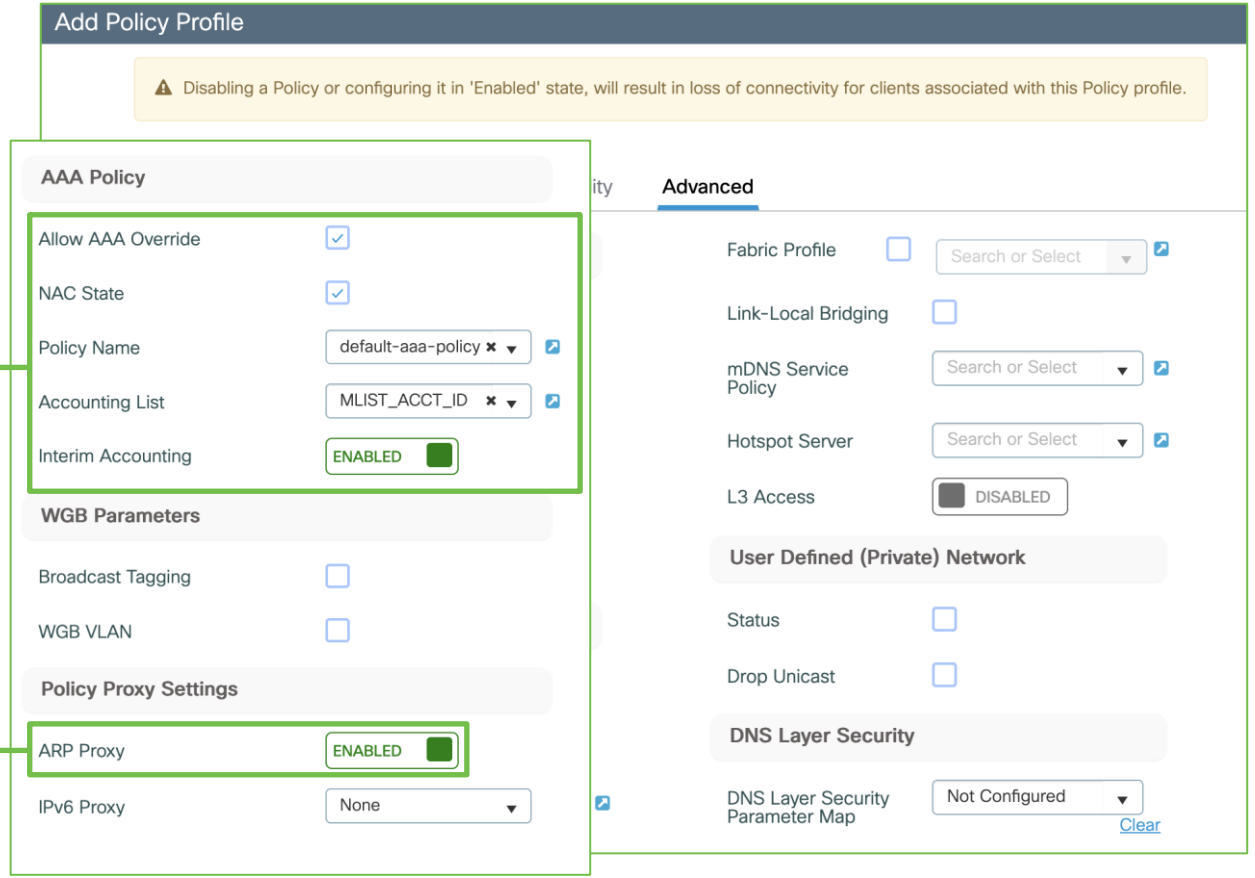
Configuring the Policy Profile

Allow AAA Override to support dynamic RADIUS attributes

NAC State/Type for CoA support

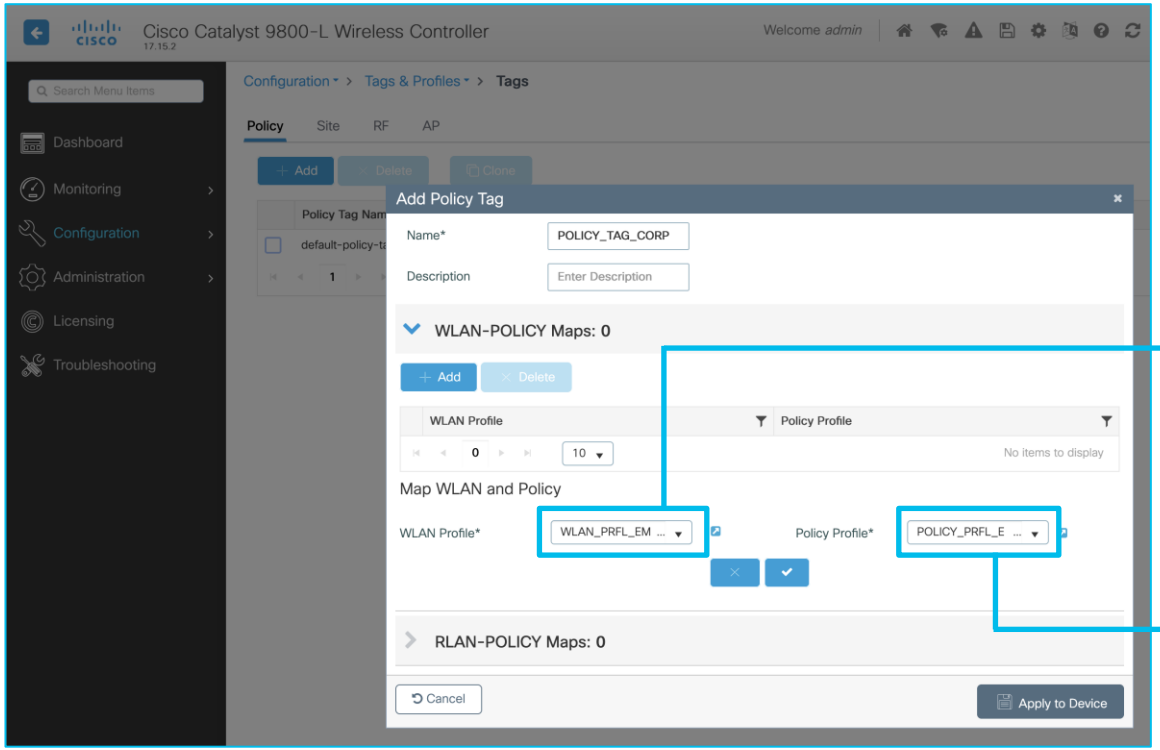
Accounting List for RADIUC Accounting and CoA too

For increased security/control



Configuring the Policy Tag

Configuration > Tags & Profiles > Tags > Policy > Add



Policy Tag

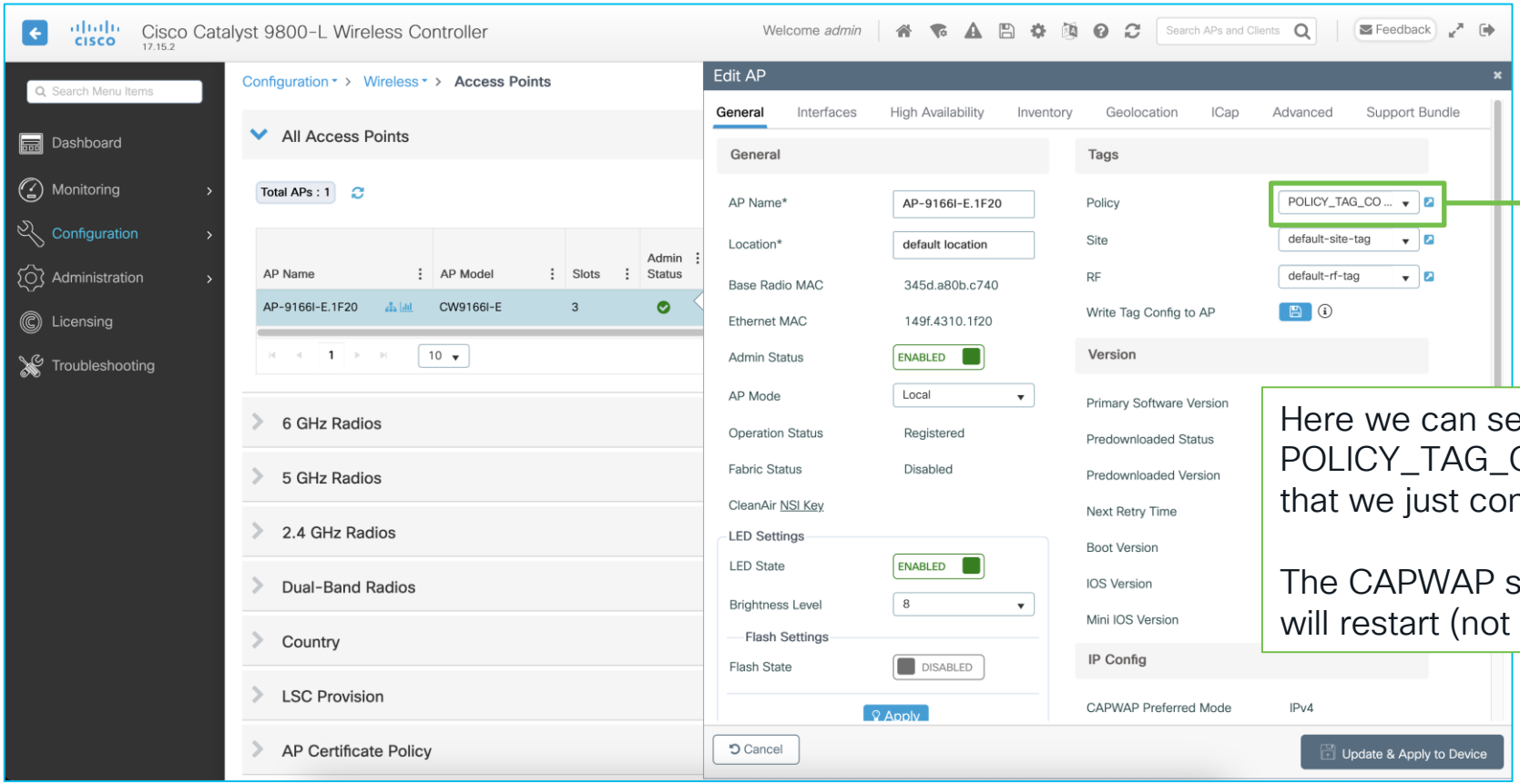
=

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

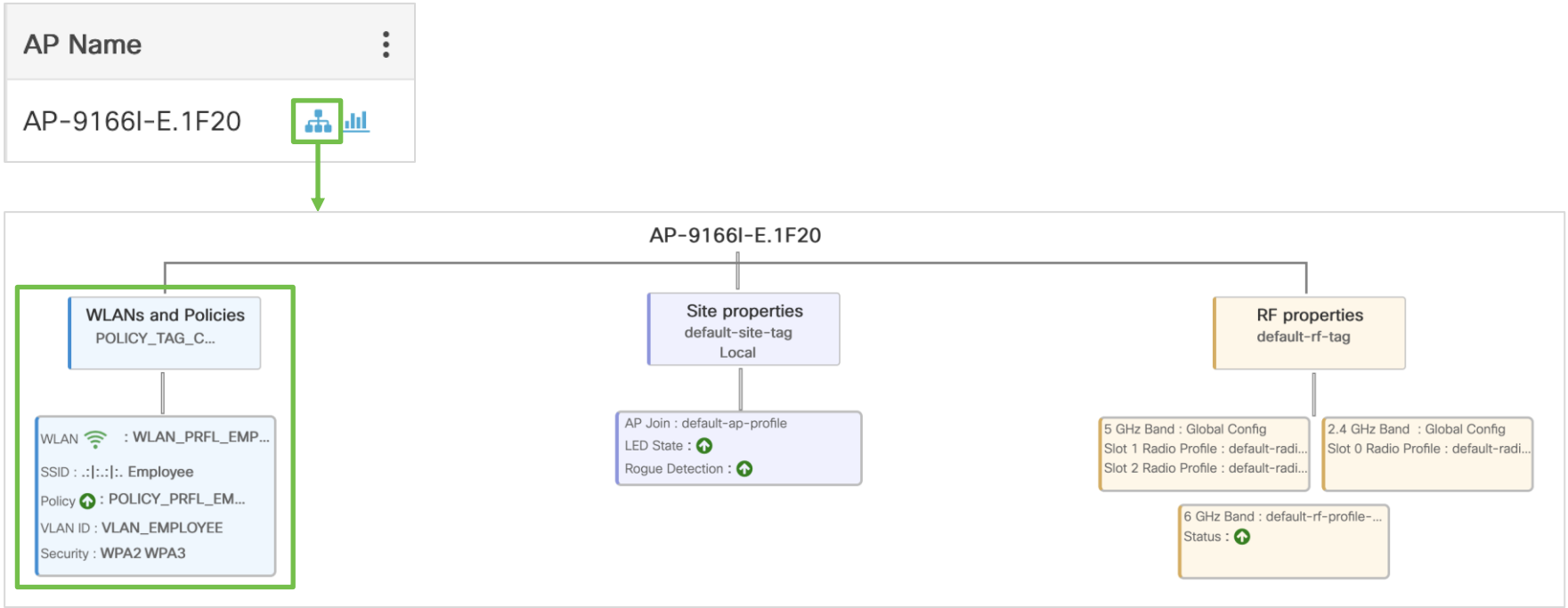


Here we can select the POLICY_TAG_CORP that we just configured

The CAPWAP service will restart (not a reload)

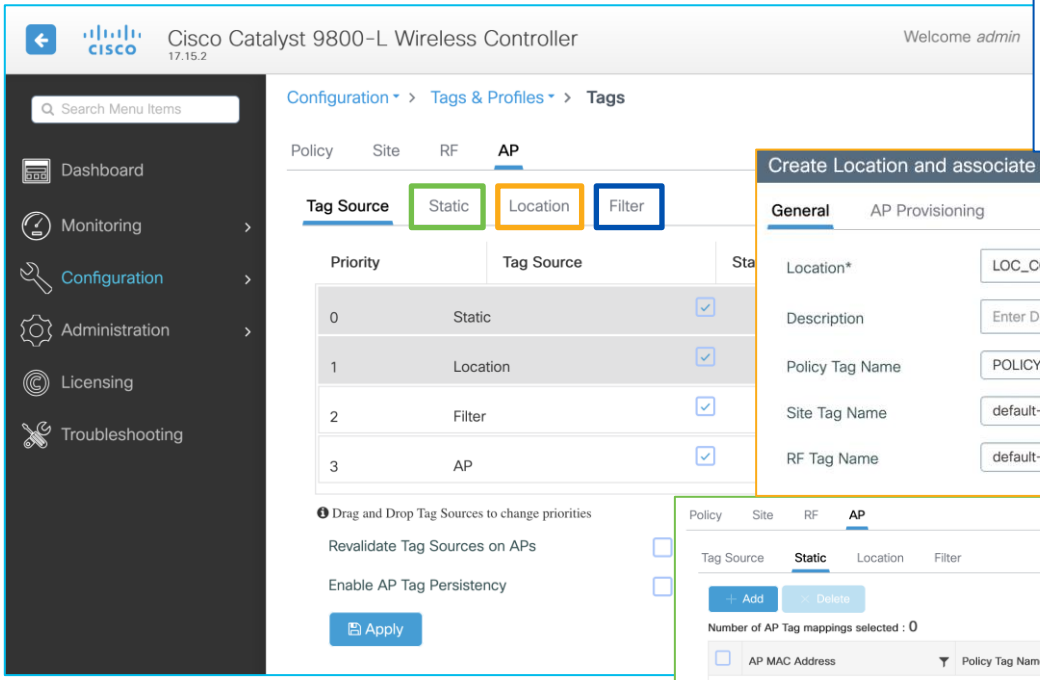
Configuration > Wireless > Access Points

Checking Tags and Profiles assignment

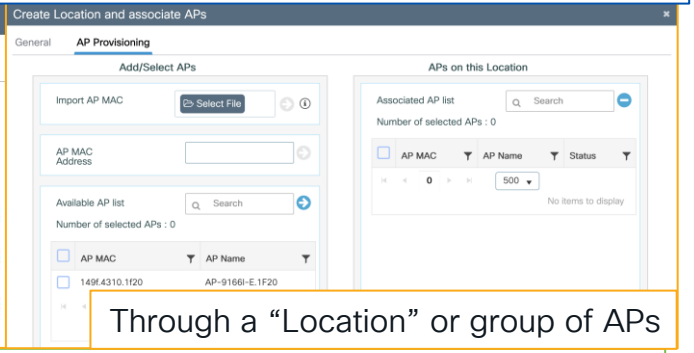


Other options to assign Tags

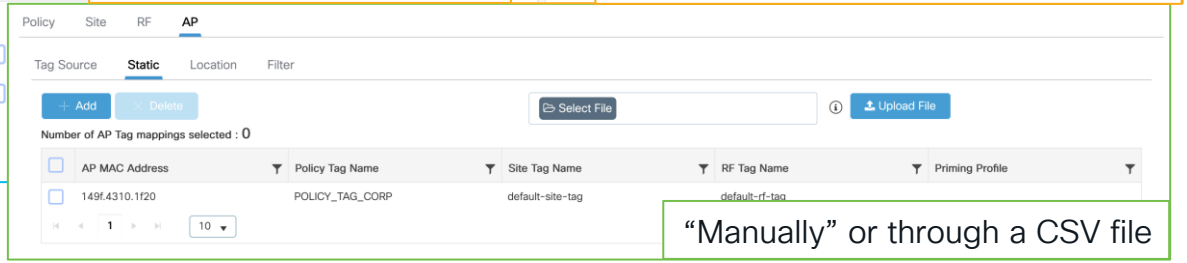
Configuration > Tags & Profiles > Tags > AP > Tag Source



Through regex rules for the AP names



Through a “Location” or group of APs

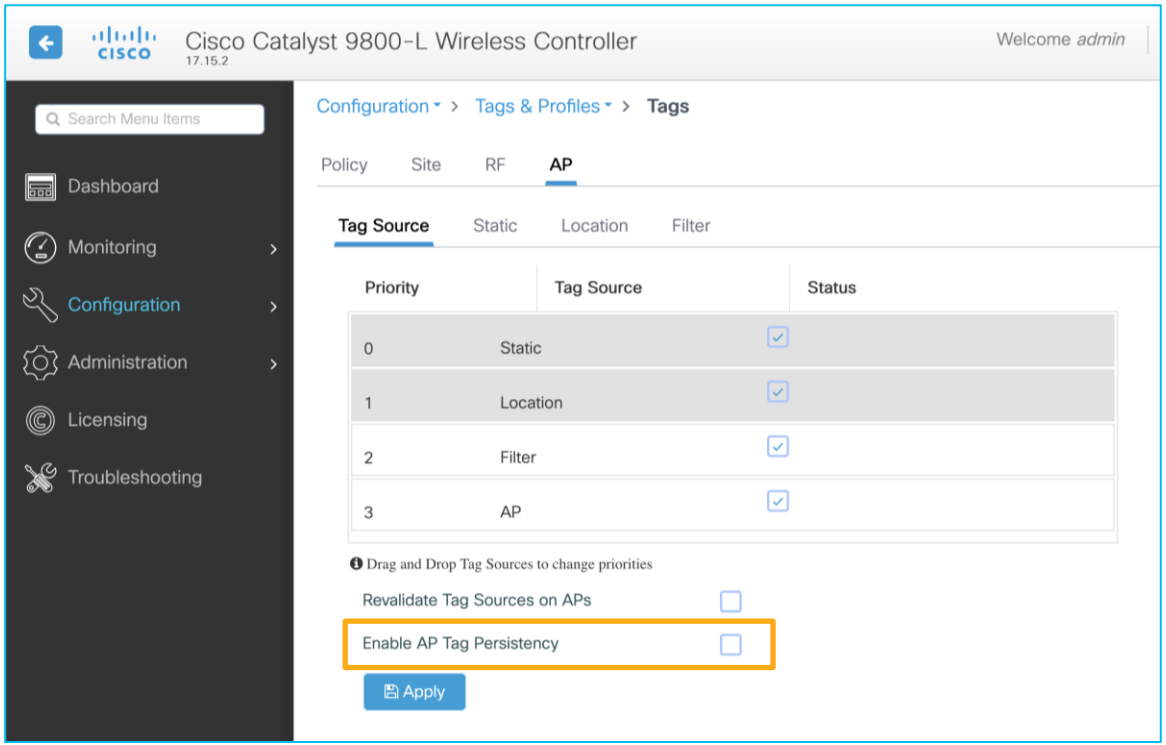


“Manually” or through a CSV file

Enabling Tags persistency

For your reference

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

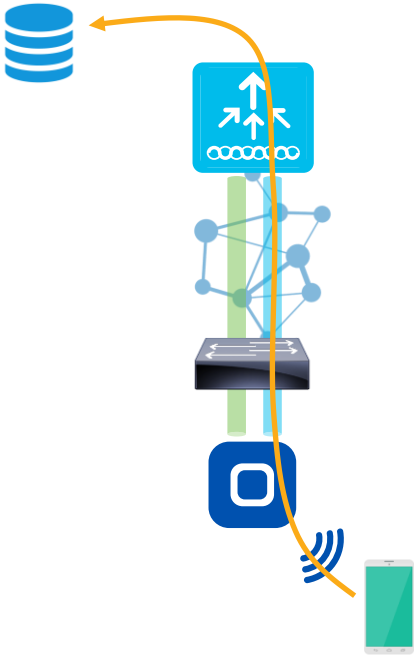


AP Tag Persistency can be useful if we want APs to keep their Tags when moving between controllers (e.g., N+1 HA)

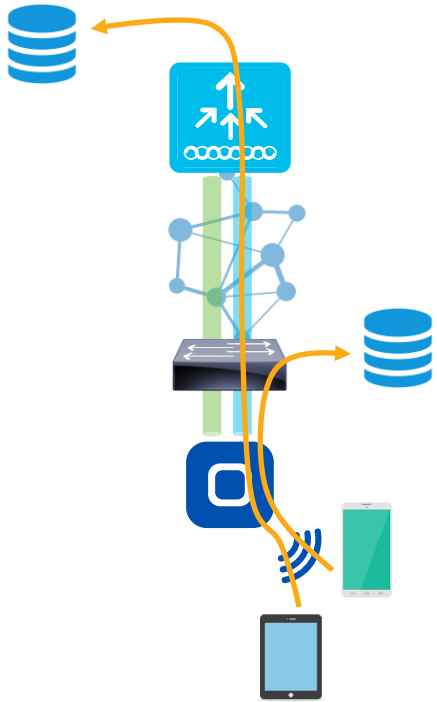
The same Tags must be present on the new destination controller and they are applied according to the AP's memory if no other mappings (static, filter, etc.) supersede them

Central or (FlexConnect) Local Switching

Local Mode AP
(Central Switching)



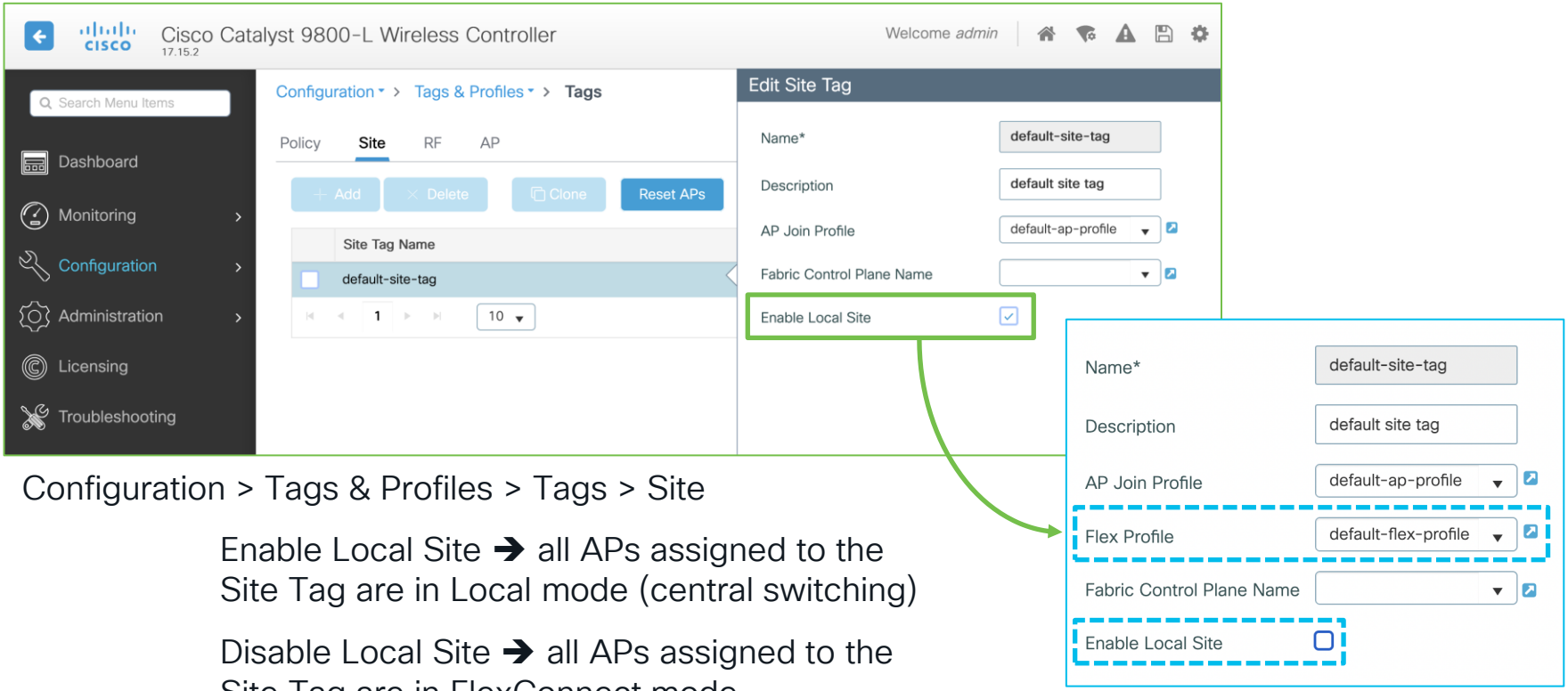
FlexConnect mode AP
(Central / Local Switching)



CAPWAP Control
CAPWAP Data

Going FlexConnect

1. The AP must be in FlexConnect mode



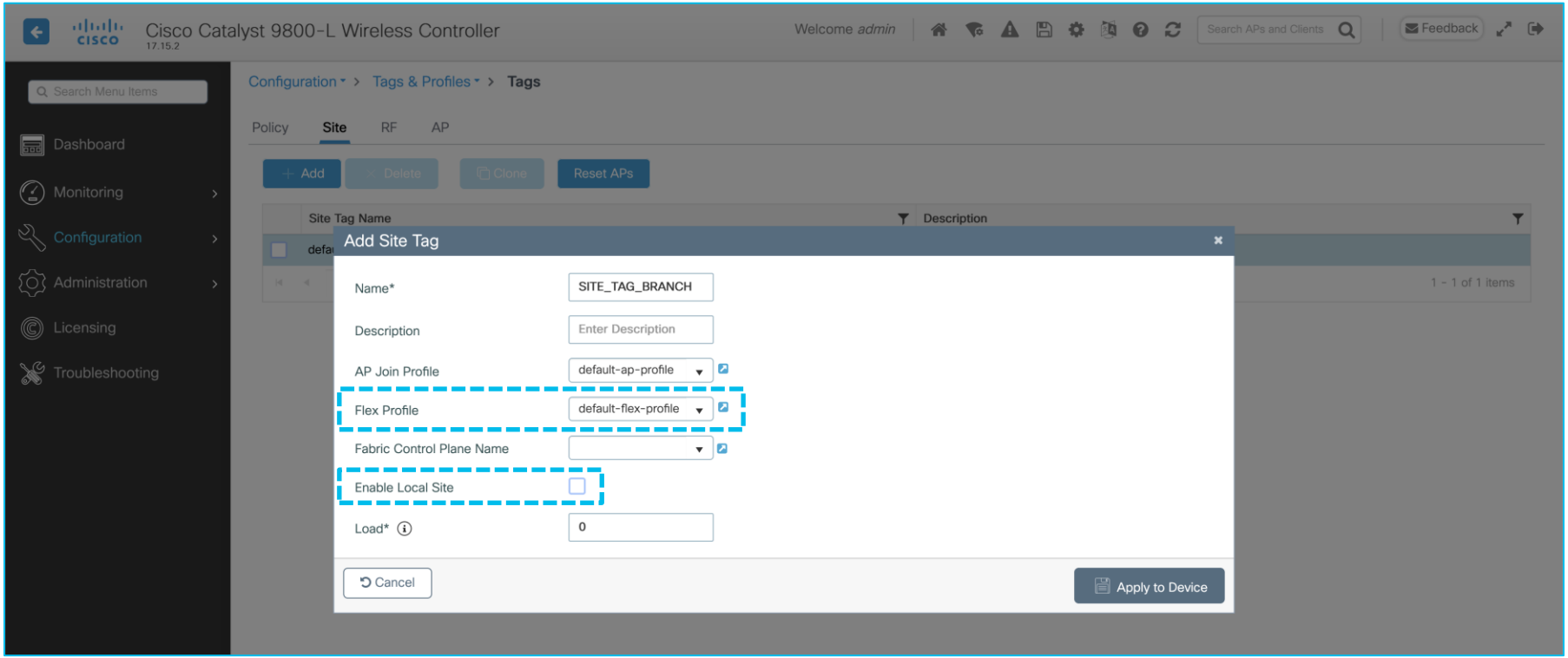
Configuration > Tags & Profiles > Tags > Site

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

Going FlexConnect

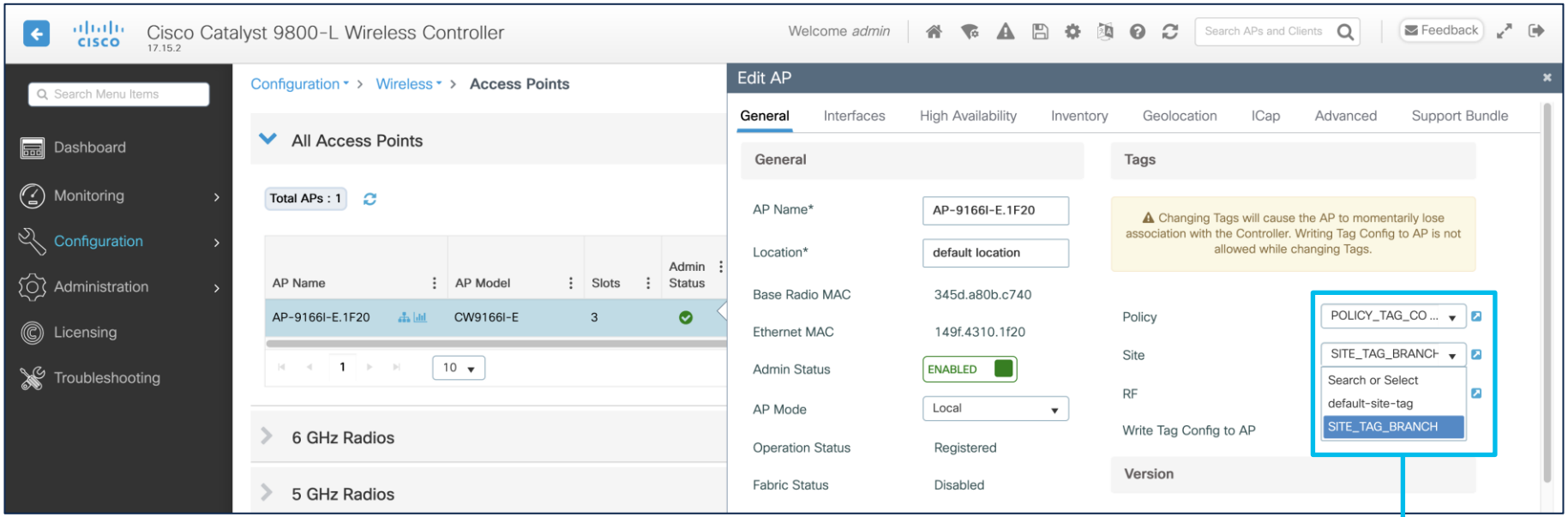
1. The AP must be in FlexConnect mode (with a new dedicated Site Tag)



Configuration > Tags & Profiles > Tags > Site

Going FlexConnect

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



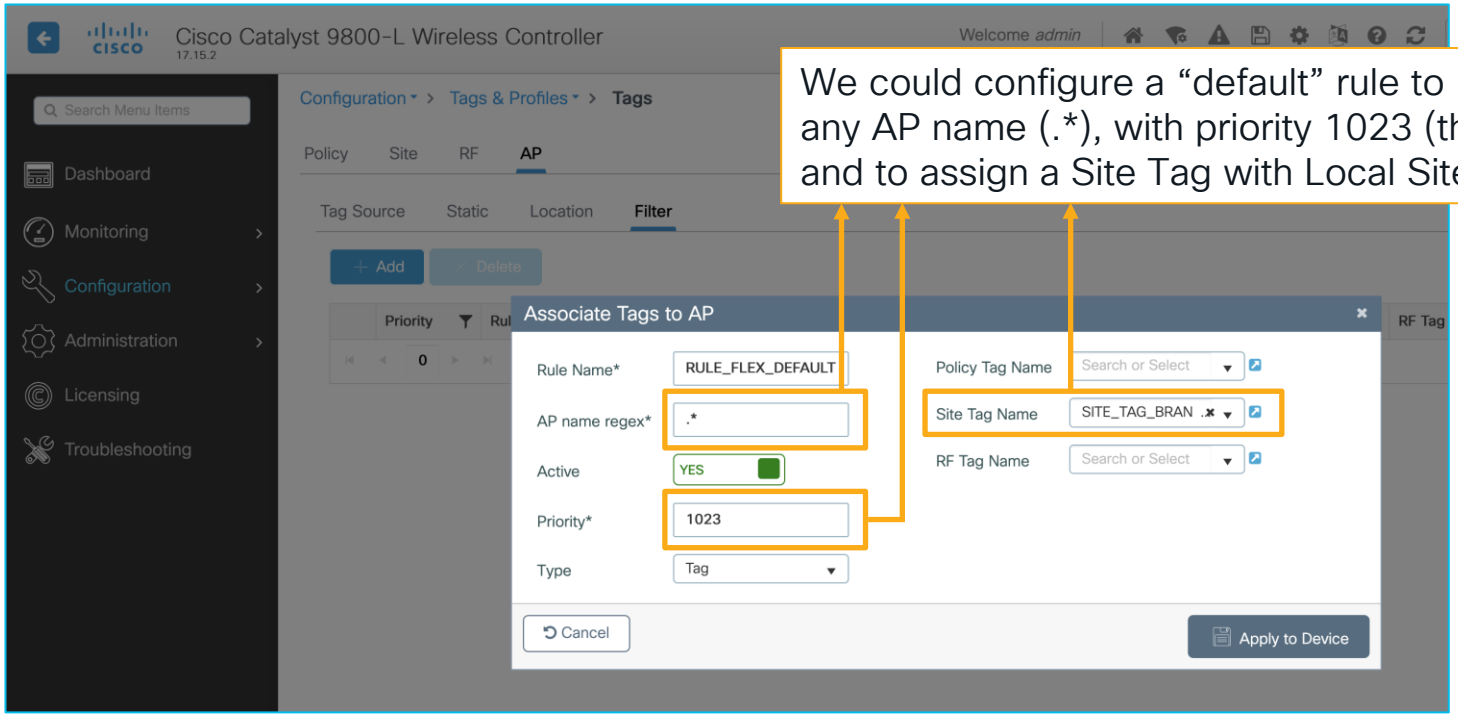
Configuration > Wireless > Access Points

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

Quick tip: default all APs to FlexConnect mode

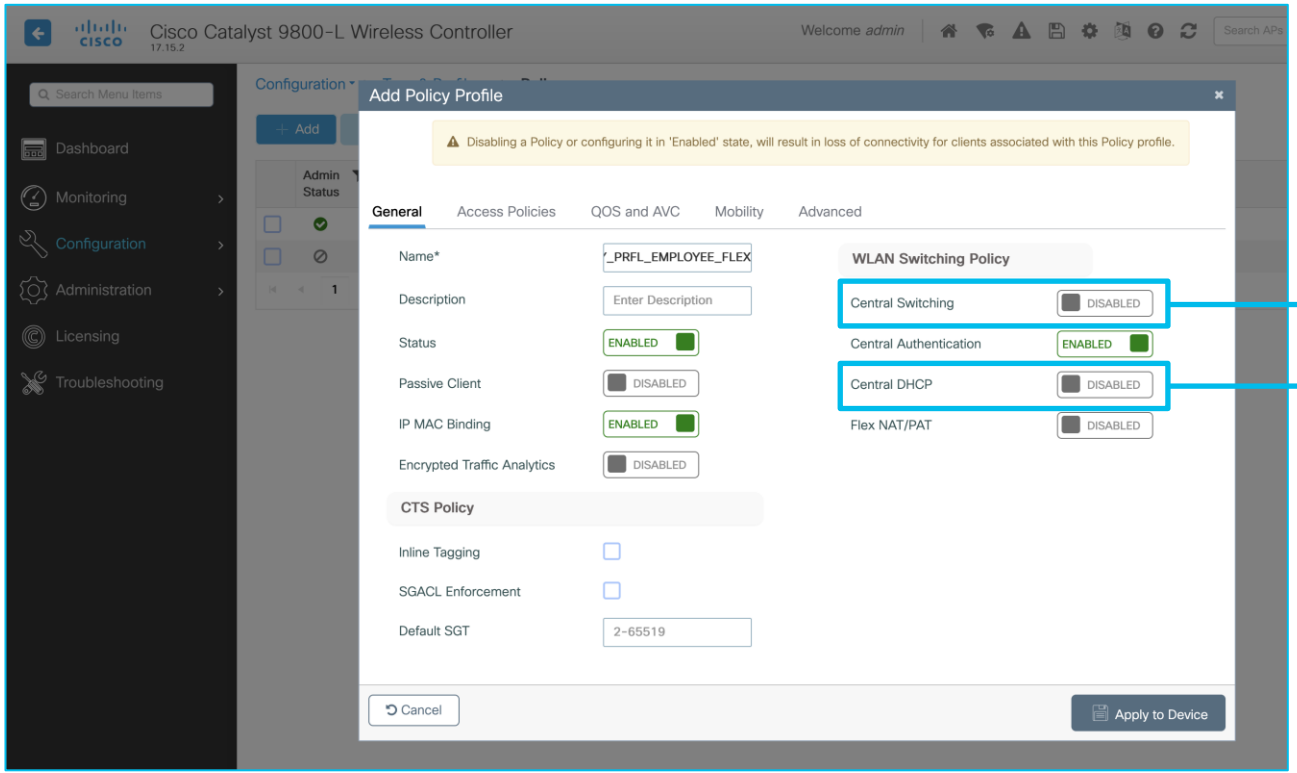
Configuration > Tags & Profiles > Tags > AP > Filter

For your reference



Going FlexConnect

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

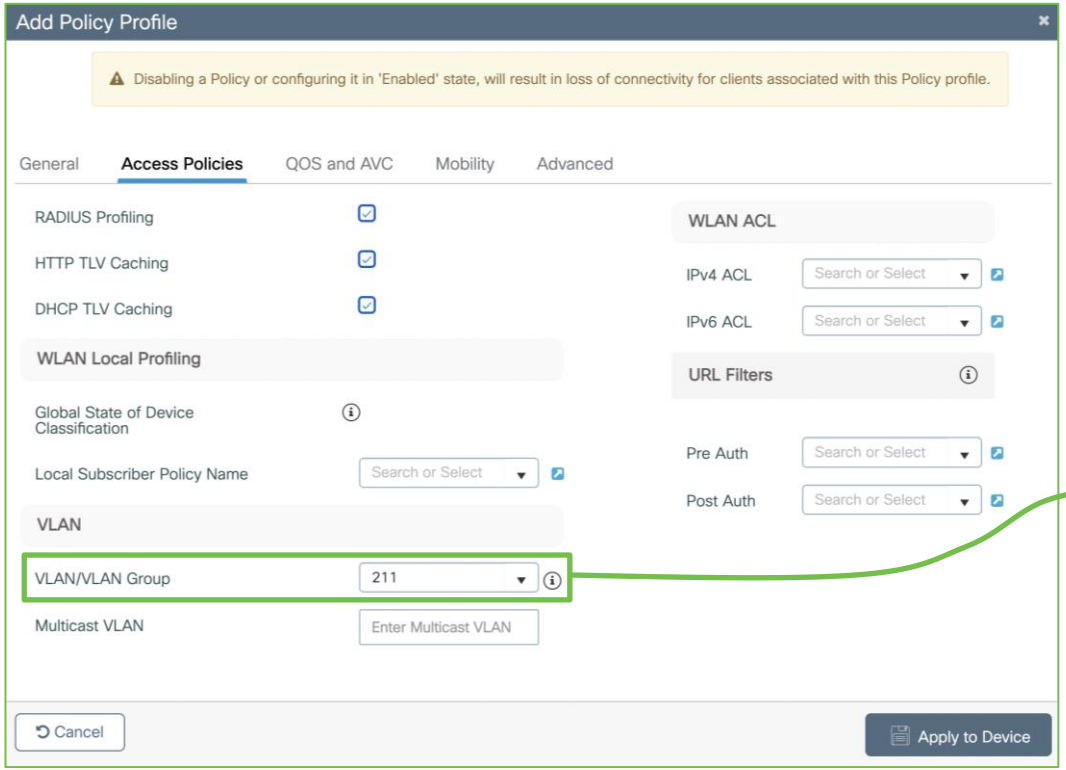


We could have also modified the existing POLICY_PRFL_EMPLOYEE profile. A new, dedicated one for FlexConnect could be more reusable

Configuration > Tags & Profiles > Policy

Going FlexConnect

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



Configuration > Tags & Profiles > Policy

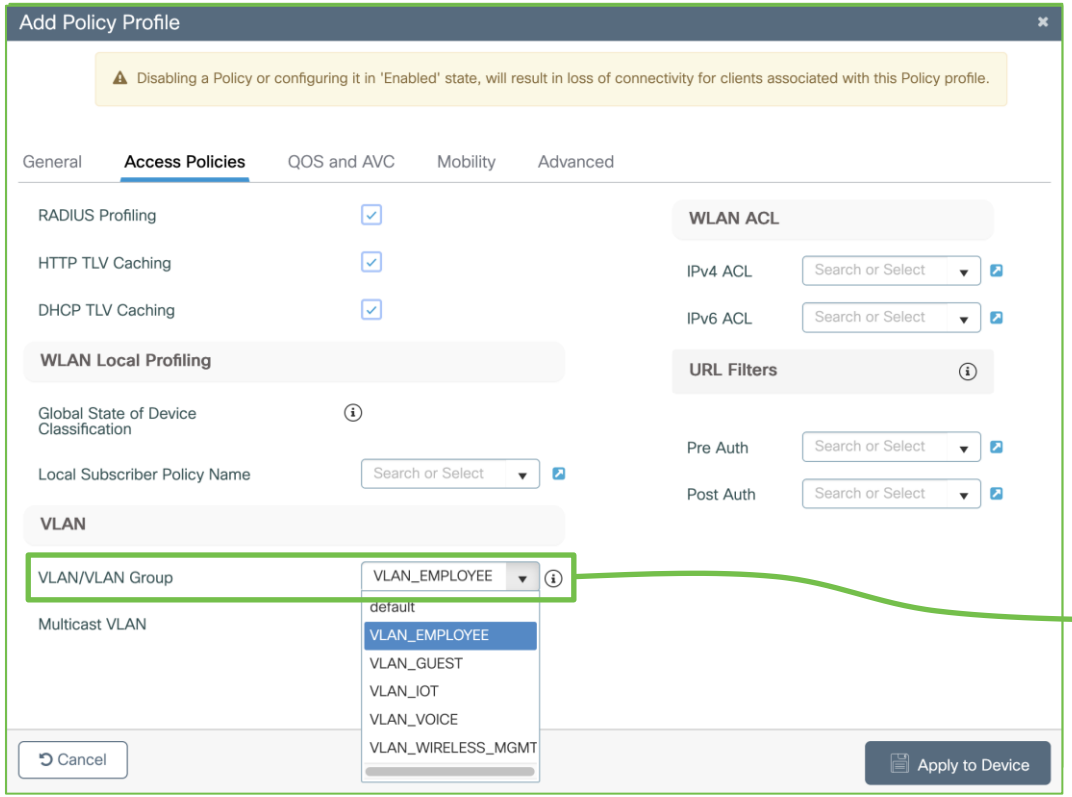
VLANs dynamically assigned via RADIUS take precedence over the VLAN statically defined under the Policy Profile.
If you are not dynamically assigning VLANs via RADIUS, you can define the locally switched VLAN under the Access Policies tab of the Policy Profile. Be aware that:

- **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)



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

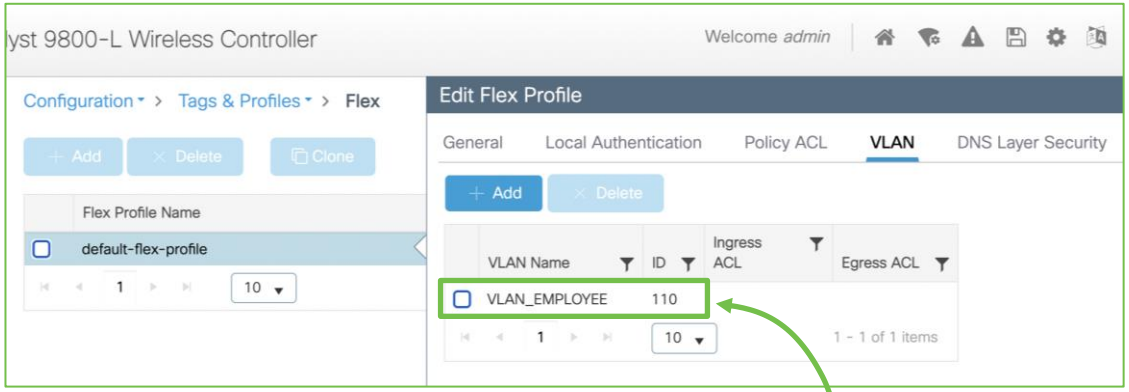
- when using the VLAN number, this VLAN does not need to exist in the 9800's database;
- **when using the VLAN name, the VLAN must exist both in the 9800's local database and under the Flex Profile, with exactly the same name and ID.**

Configuration > Tags & Profiles > Policy

Going FlexConnect

For your reference

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



Configuration > Tags & Profiles > Flex

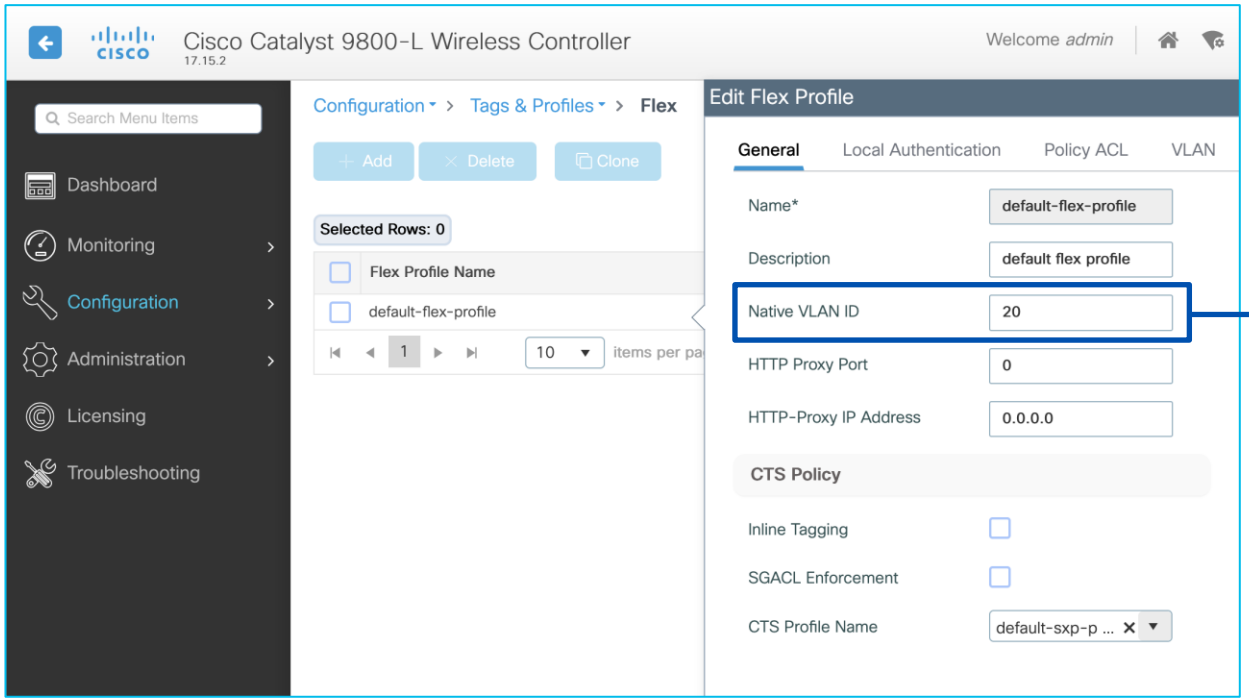
VLANs dynamically assigned via RADIUS take precedence over the VLAN statically defined under the Policy Profile.
If you are not dynamically assigning VLANs via RADIUS, you can define the locally switched VLAN under the Access Policies tab of the Policy Profile. Be aware that:

- 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

For your reference

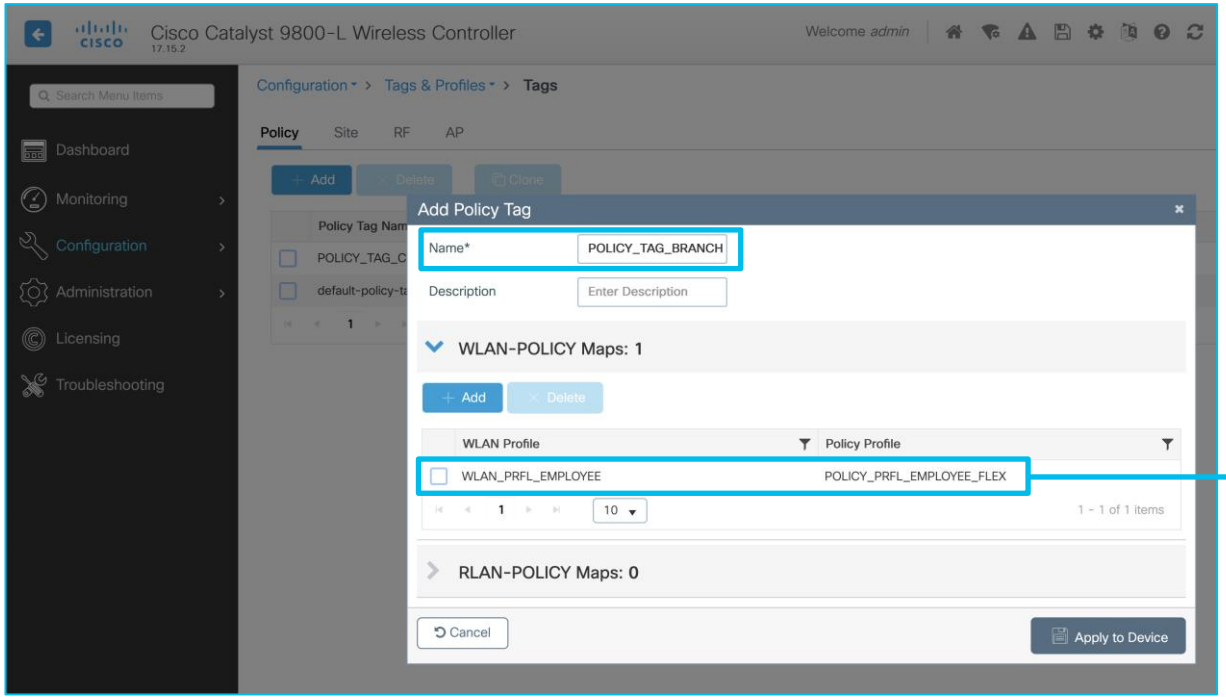
Configuration > Tags & Profiles > Flex



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



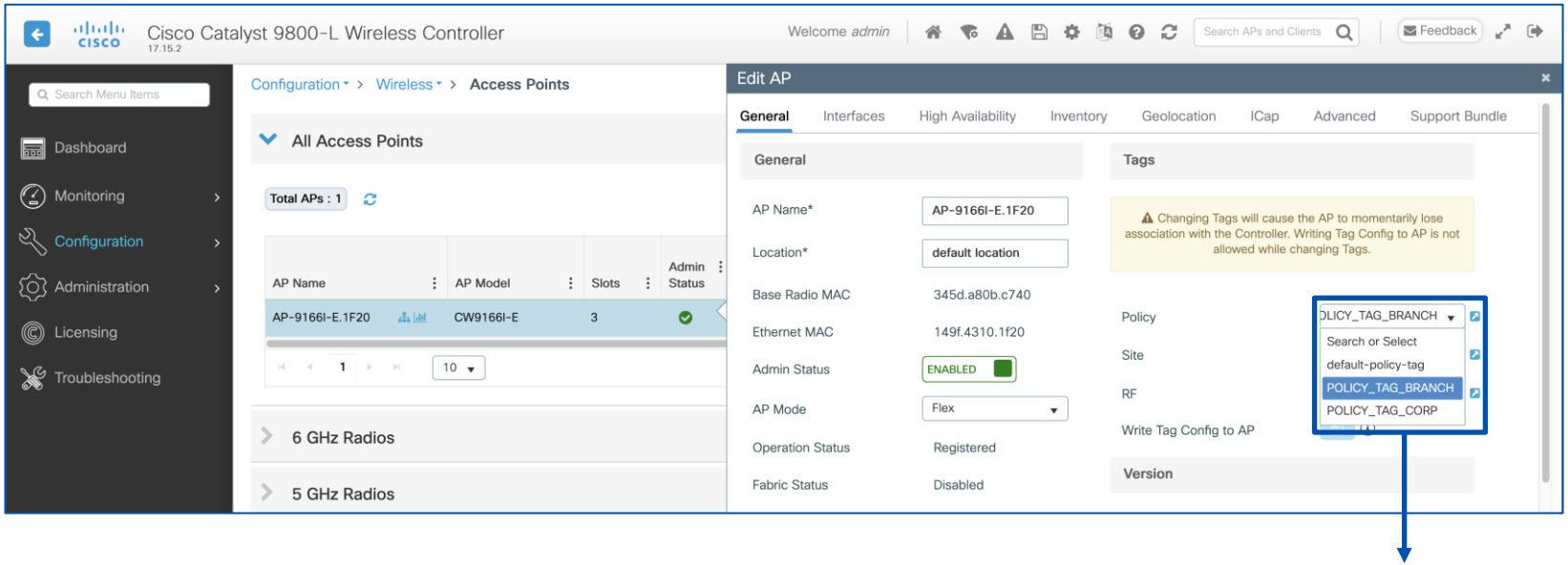
We can create a new Policy Tag, which links the same WLAN Profile for our employees' use case, but now with the new Policy Profile for FlexConnect local switching

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

Configuration > Tags & Profiles > Tags > Policy

Assigning the Policy Tag to the AP

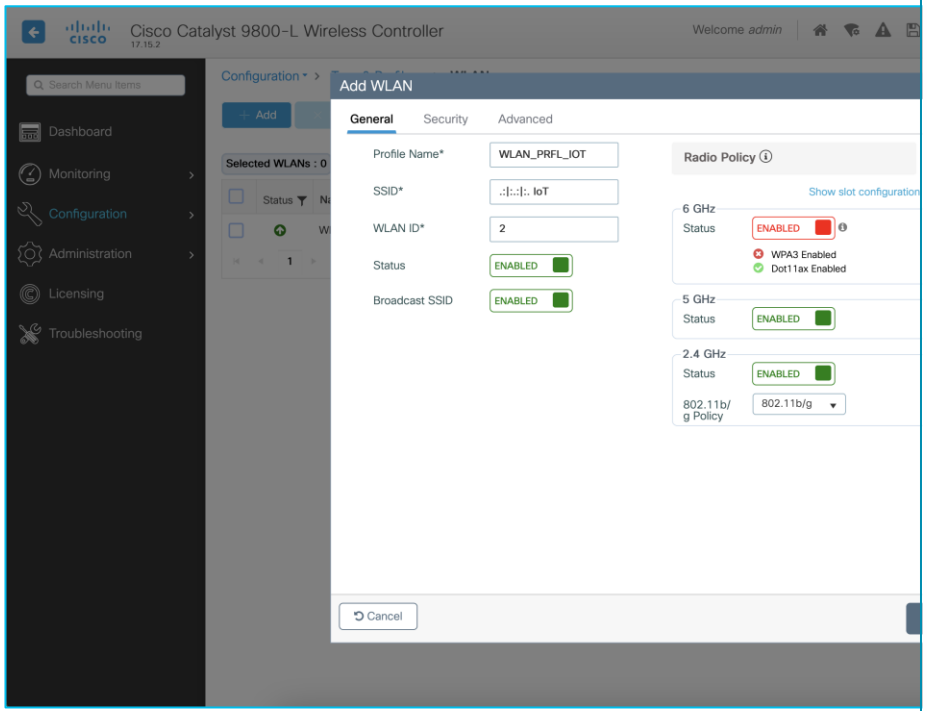
If we use a new Policy Tag, we need to assign it to our AP(s) as per usual

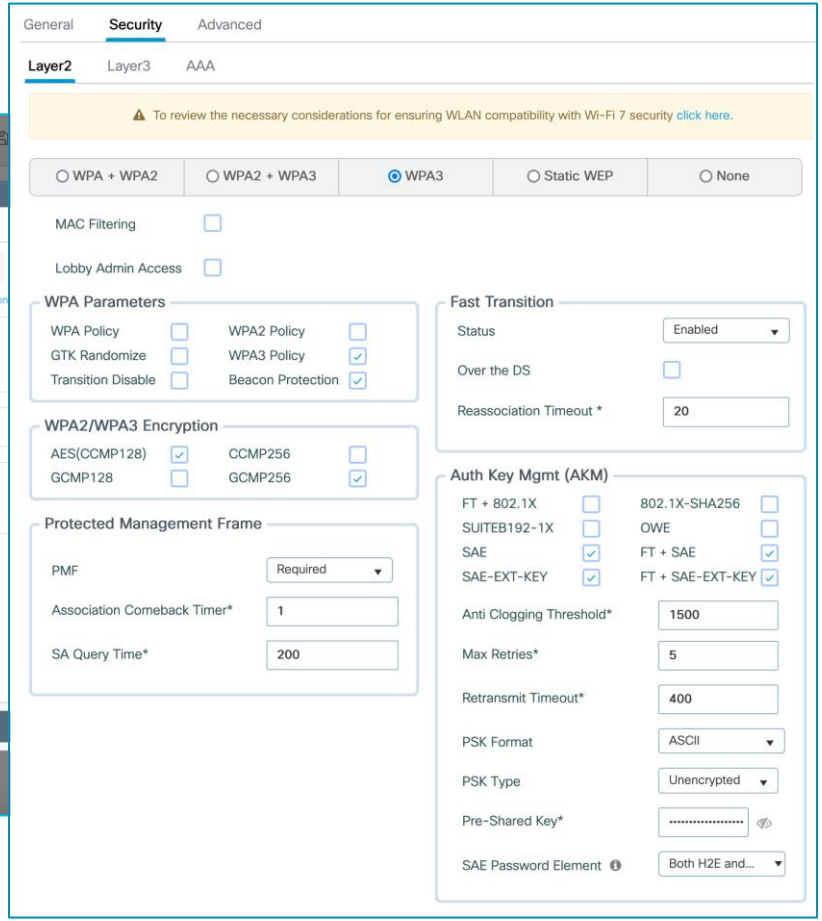


Statically assigning TAGs directly under the APs is a quick option for demos/labs/PoC's.
For more scalable options we could use filters with regex, locations or even NETCONF with external tools.

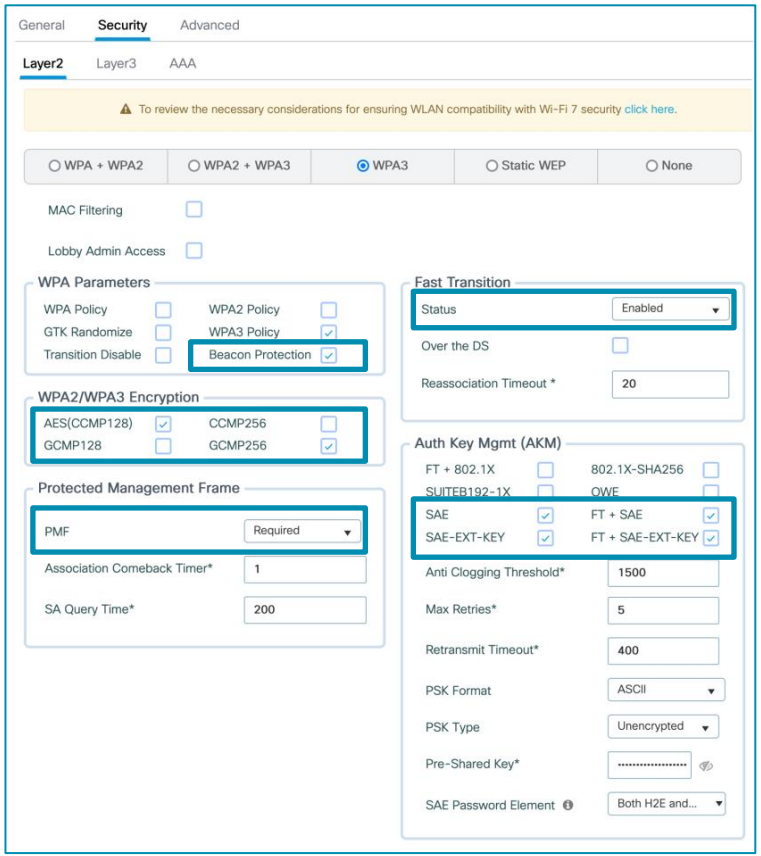
Configuring a passphrase based WLAN Profile

Configuration > Tags & Profiles > WLANs > Add





Zoom on Layer 2 Security for Wi-Fi 7 support



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

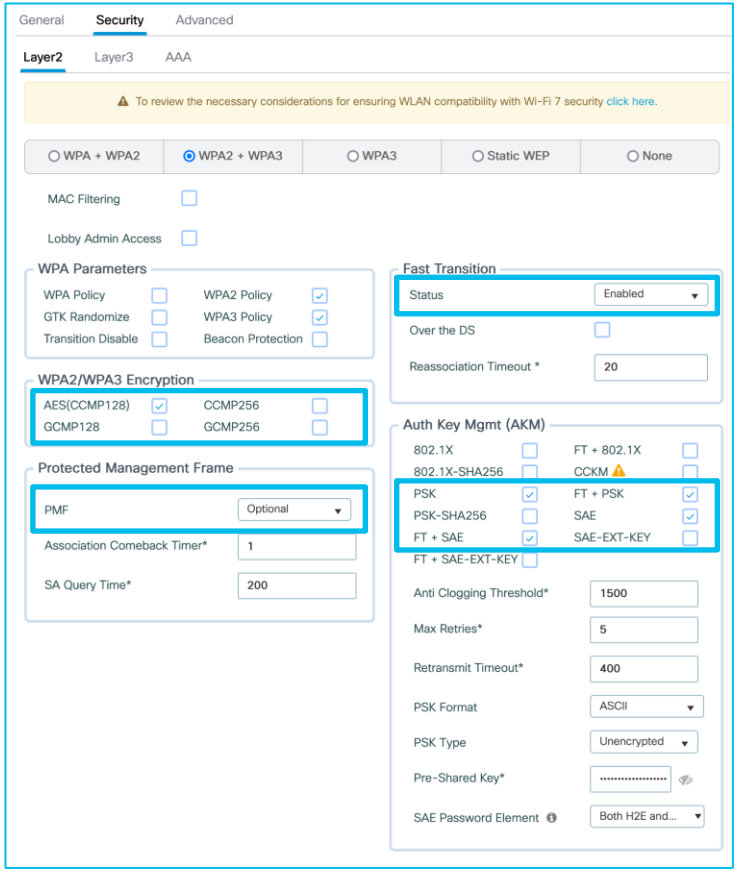
No “Adaptive Enabled”, as it would benefit Apple/Samsung endpoints only

Over the DS = unchecked

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

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

For your reference



Still supporting 6 GHz / Wi-Fi 6E

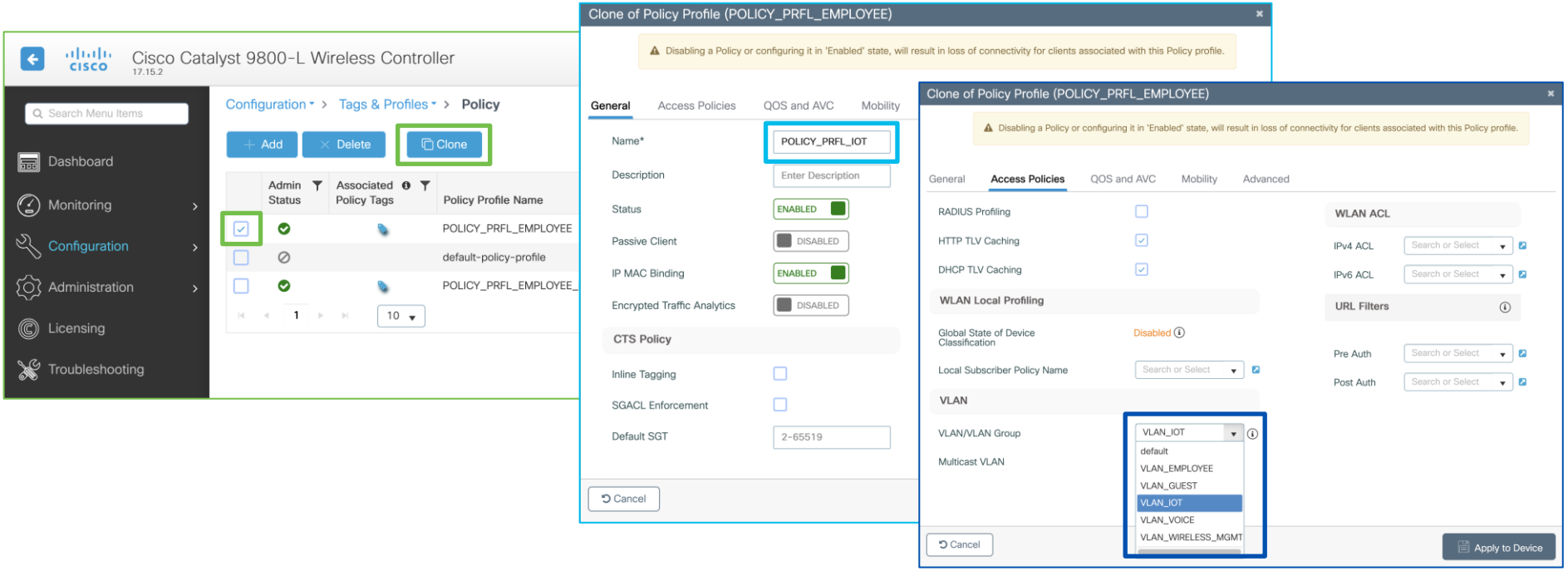
WPA2/WPA3 settings:
- AES(CCMP128)

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

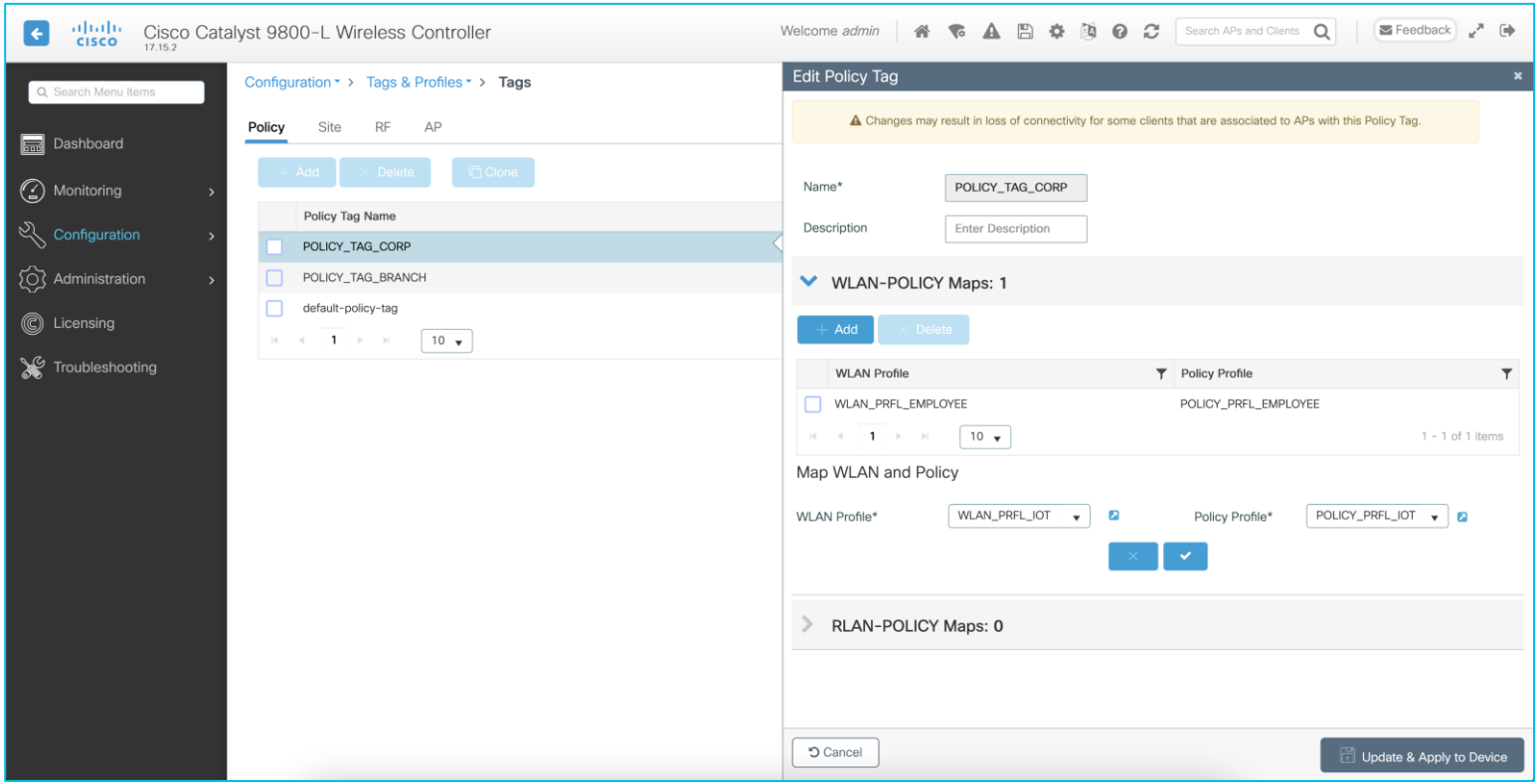
Policy Profile similar to the “Employee” one

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):



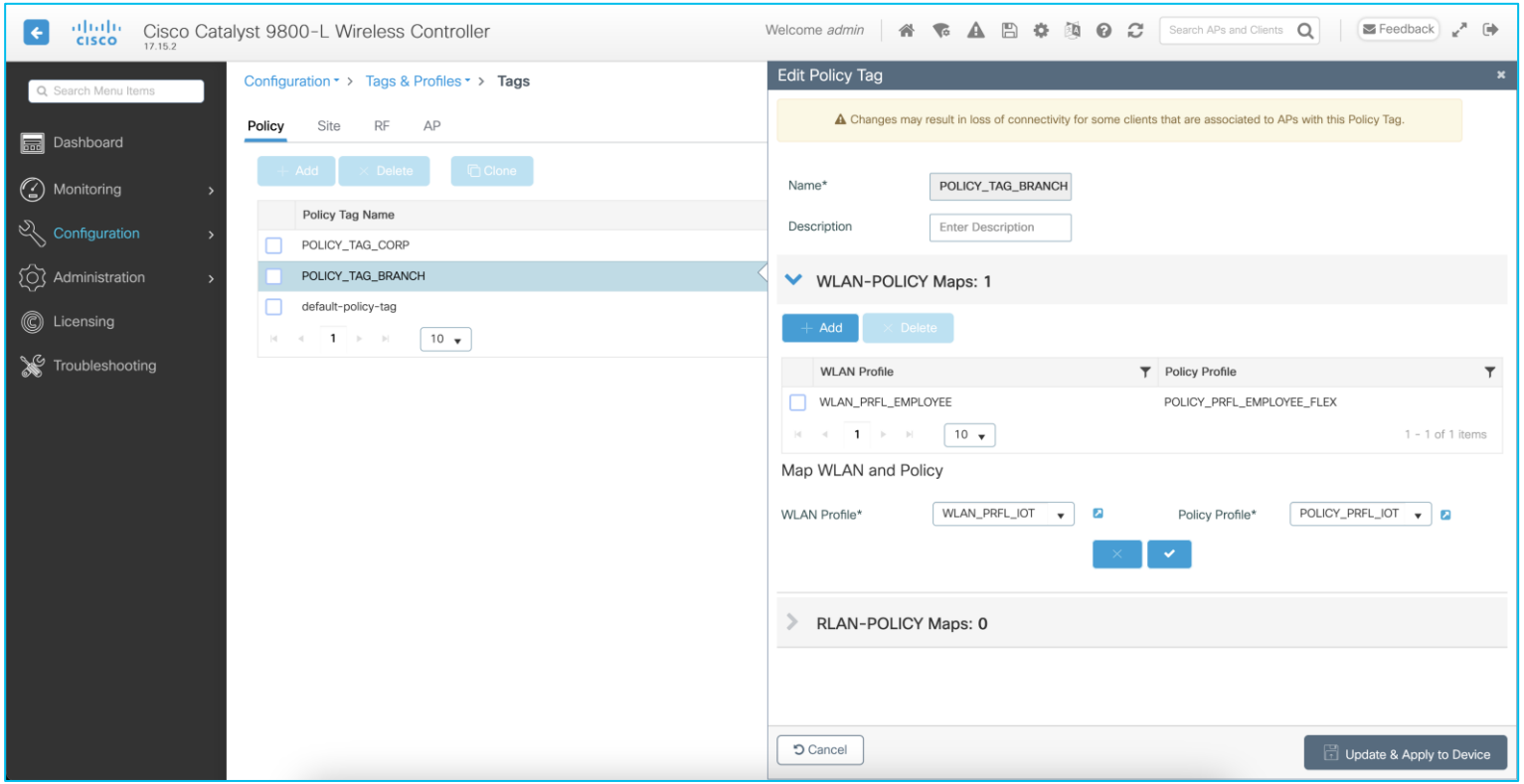
Add the WLAN and Policy Profiles to the Policy Tag

Configuration > Tags & Profiles > Tags > Policy

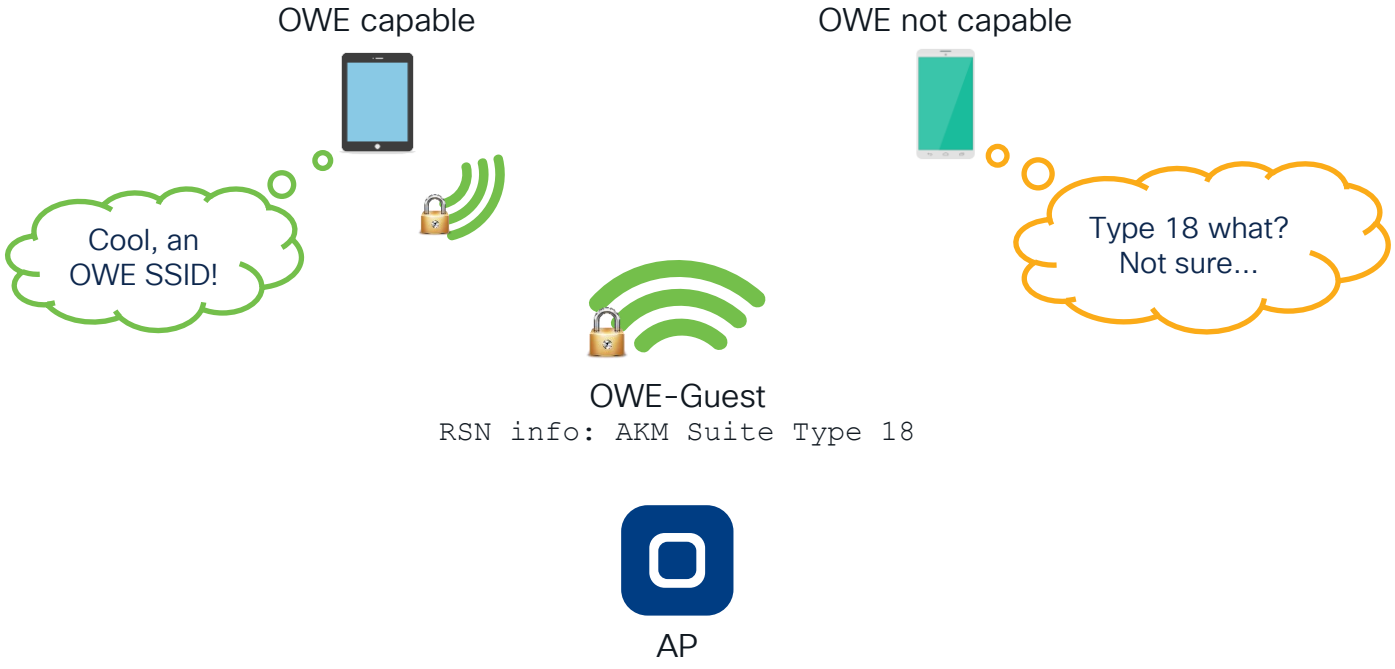


Add the WLAN and Policy Profiles to the Policy Tag

Configuration > Tags & Profiles > Tags > Policy

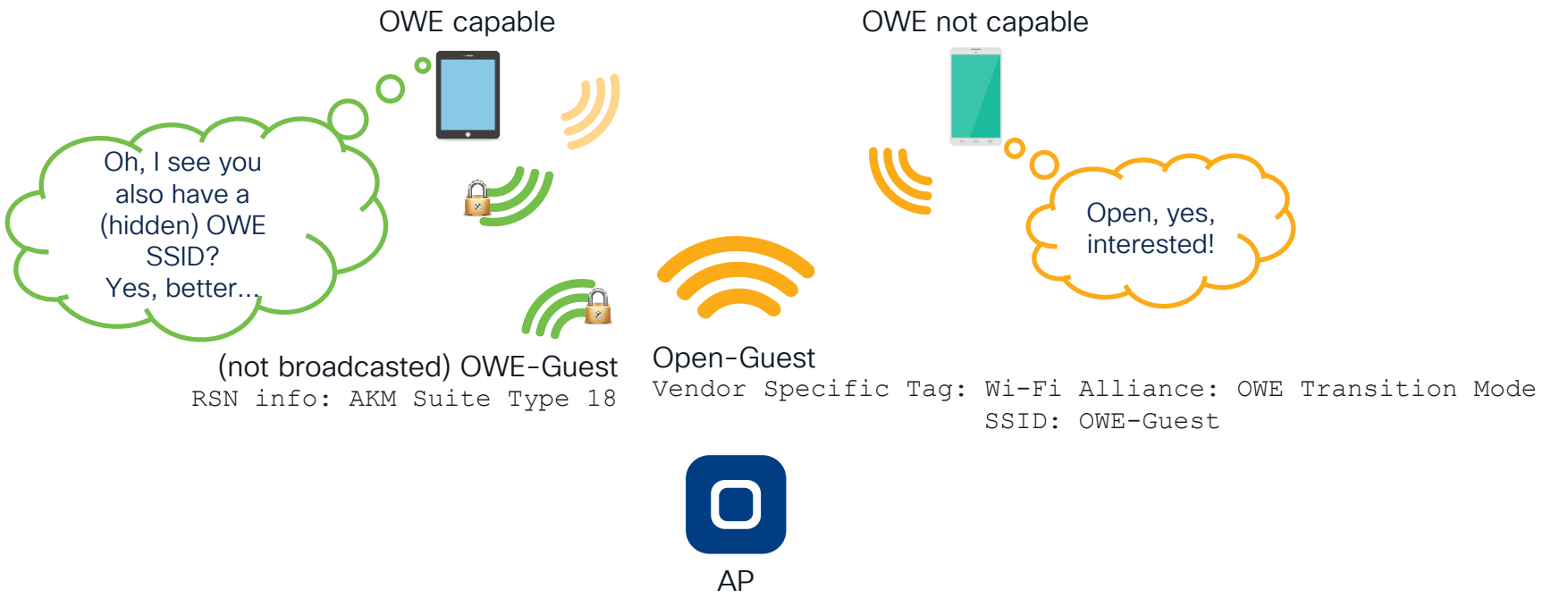


Opportunistic Wireless Encryption (OWE)



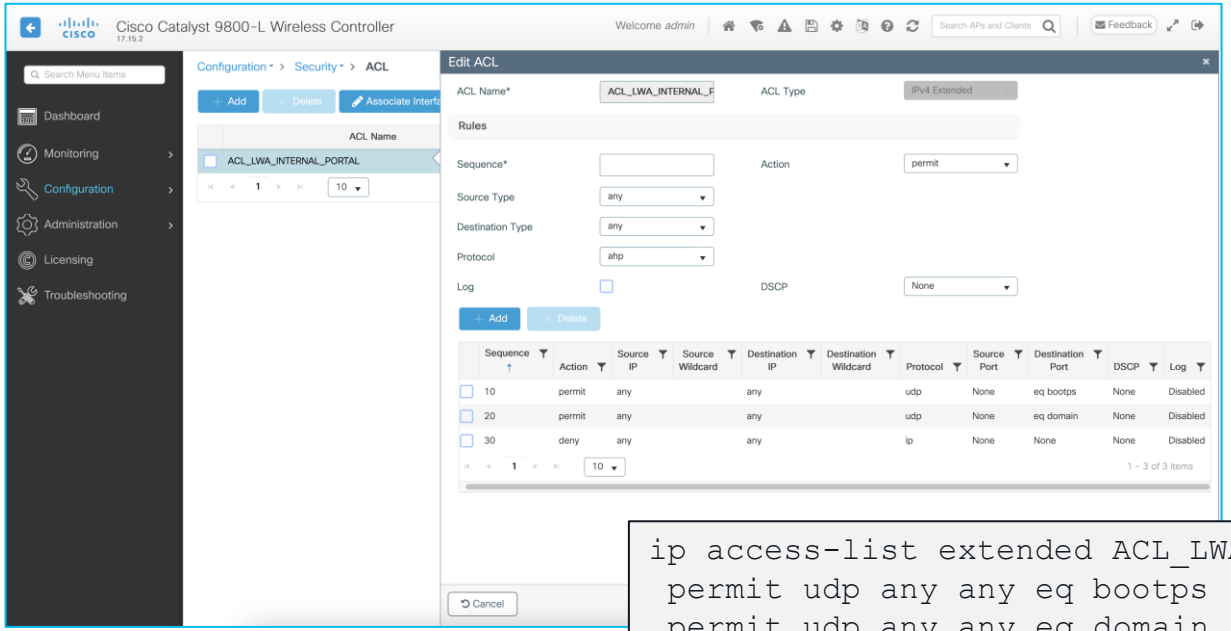
OWE Transition Mode

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



Adding a Guest SSID (LWA with internal portal)

Configuration > Security > ACL

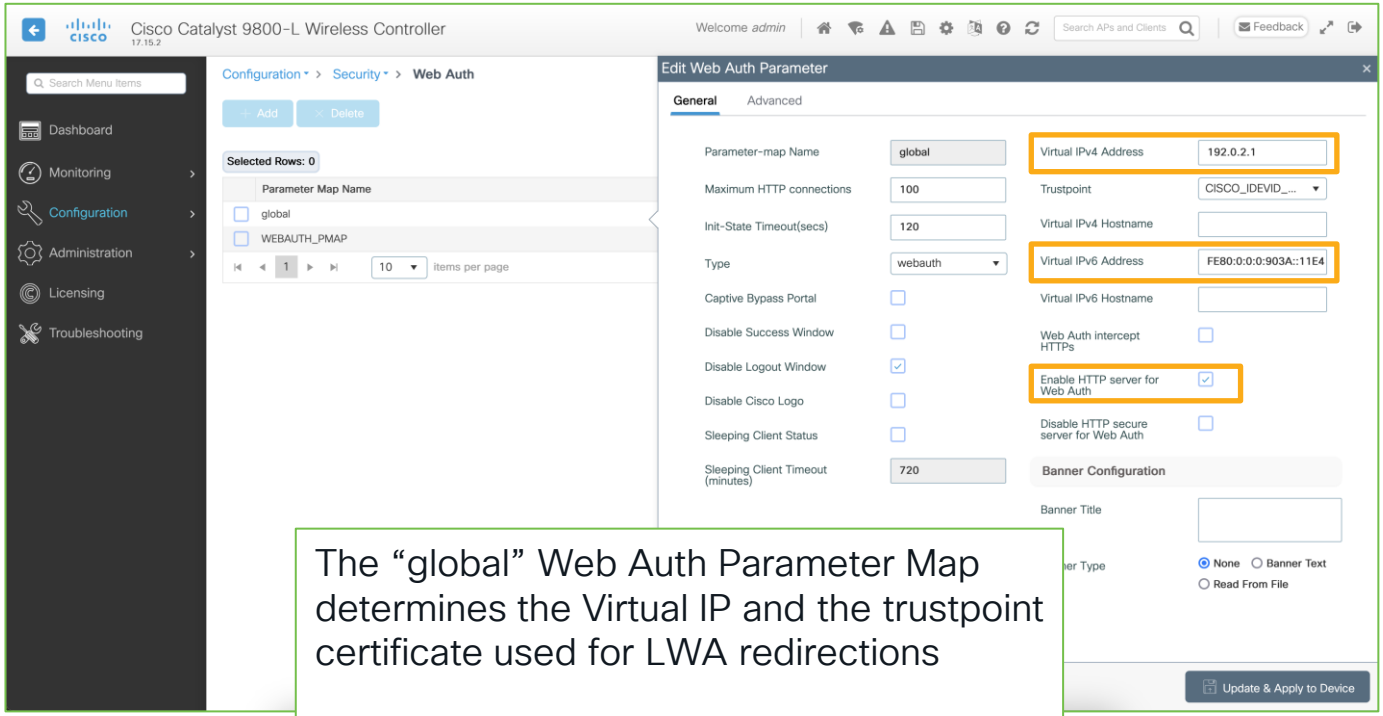


This ACL is technically not mandatory, because the 9800 will auto-assign a pre-canned one for LWA internal portals.
Still recommended in case we'd like to distinguish ACLs and monitor ACE's hits.

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

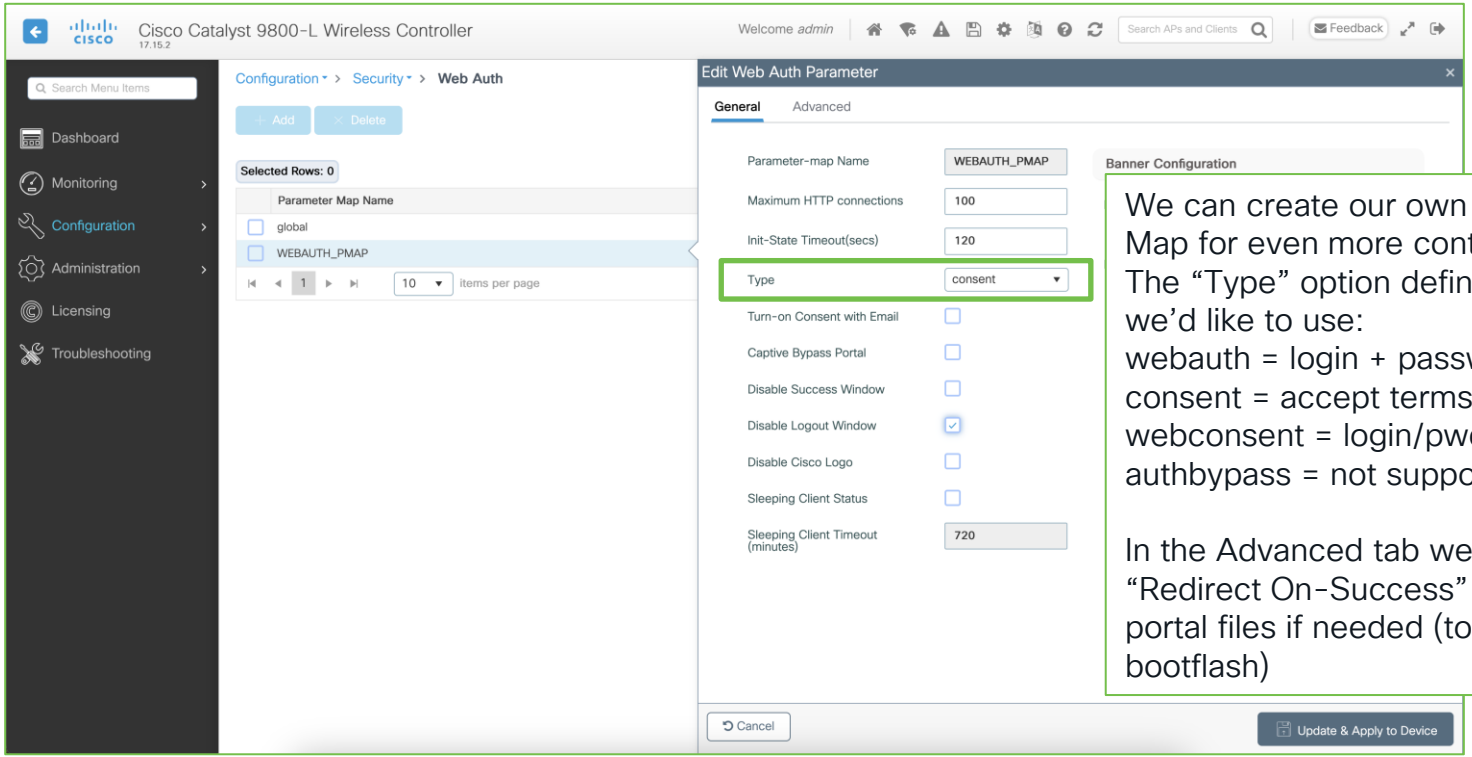
Other custom Web Auth Parameter Maps will inherit these settings

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



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)

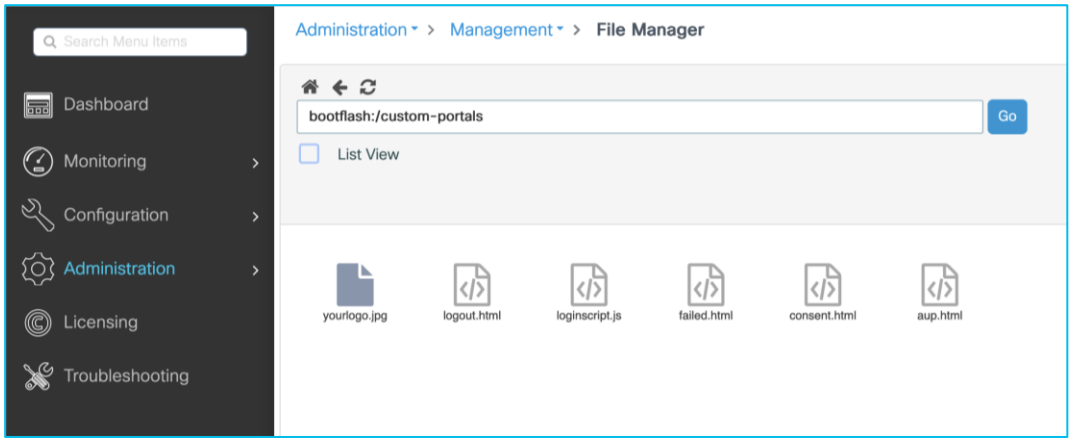
Method lists and custom files

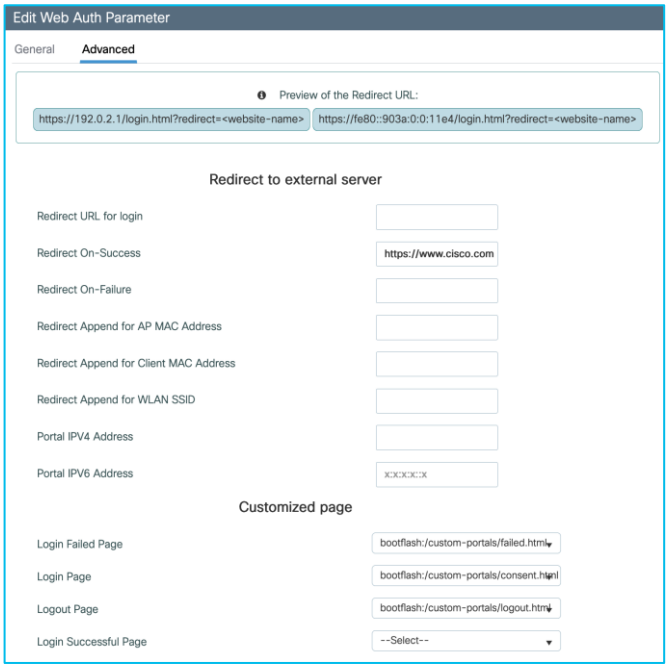
For your reference

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

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

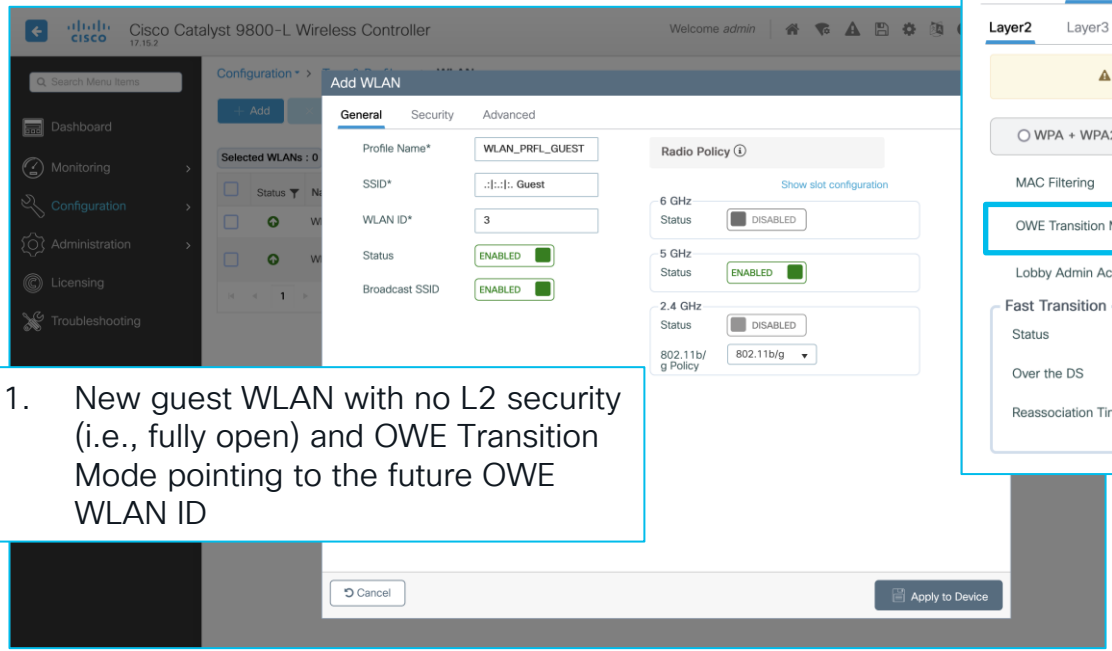
Custom portal files can be uploaded to the bootflash and then selected under the Web Auth Parameter Map (Advanced tab)

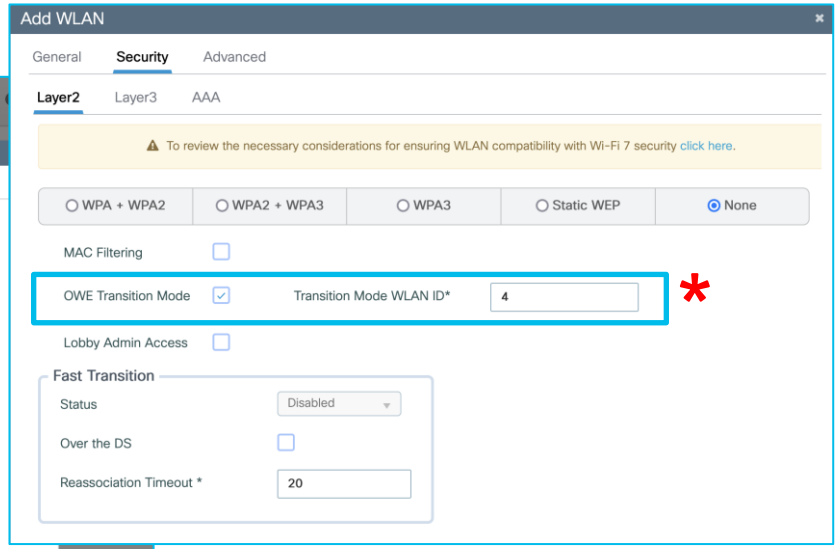




Adding a Guest SSID (LWA with internal portal)

Configuration > Security > Web Auth



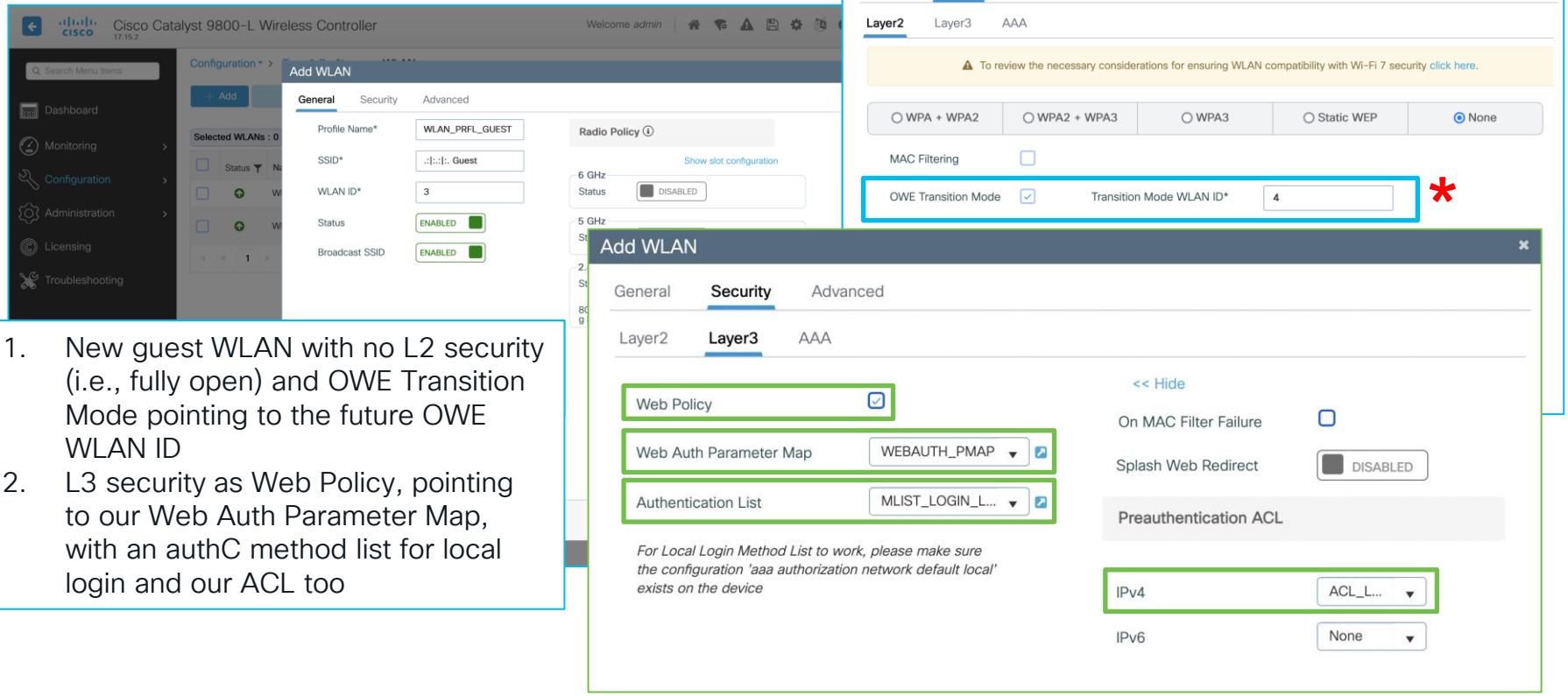


1. New guest WLAN with no L2 security (i.e., fully open) and OWE Transition Mode pointing to the future OWE WLAN ID

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

Adding a Guest SSID (LWA with internal portal)

Configuration > Security > Web Auth

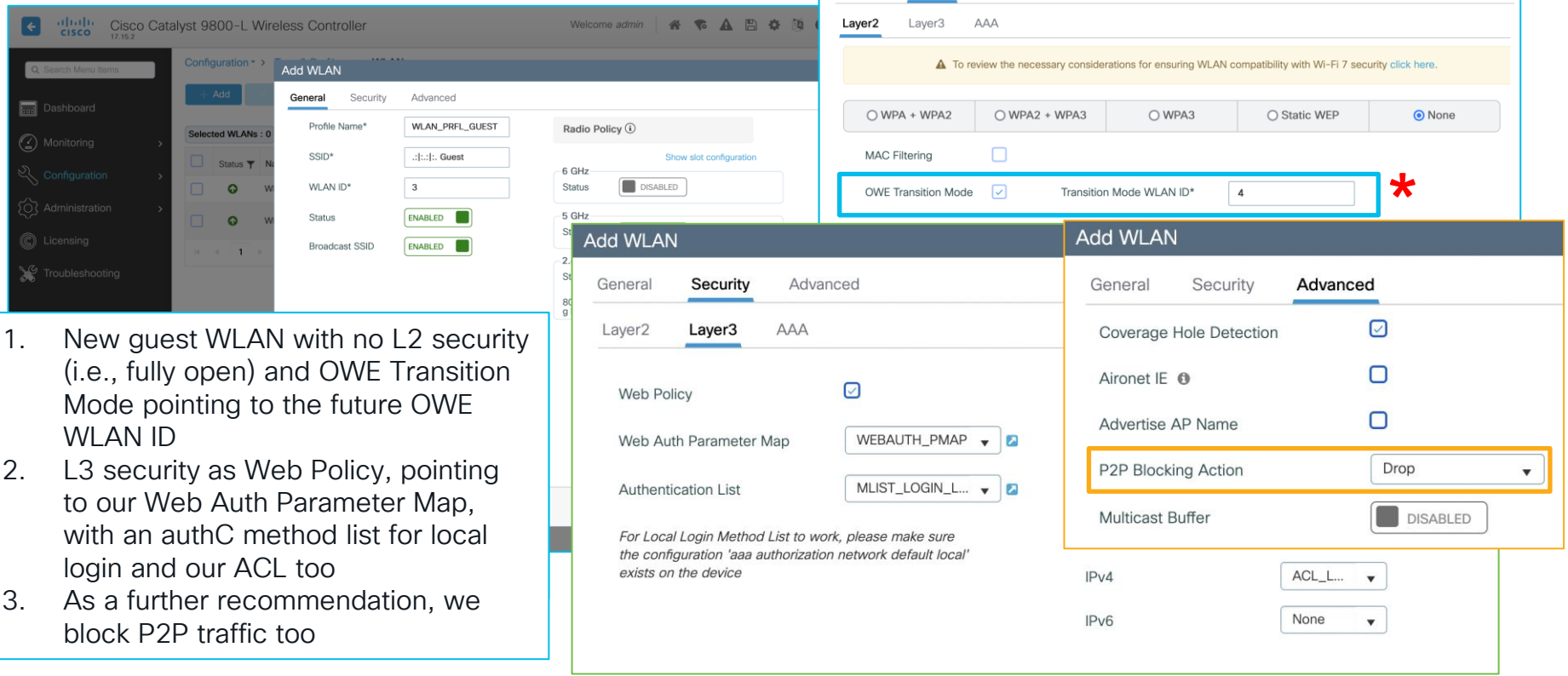


1. New guest WLAN with no L2 security (i.e., fully open) and OWE Transition Mode pointing to the future OWE WLAN ID
2. L3 security as Web Policy, pointing to our Web Auth Parameter Map, with an authC method list for local login and our ACL too

*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

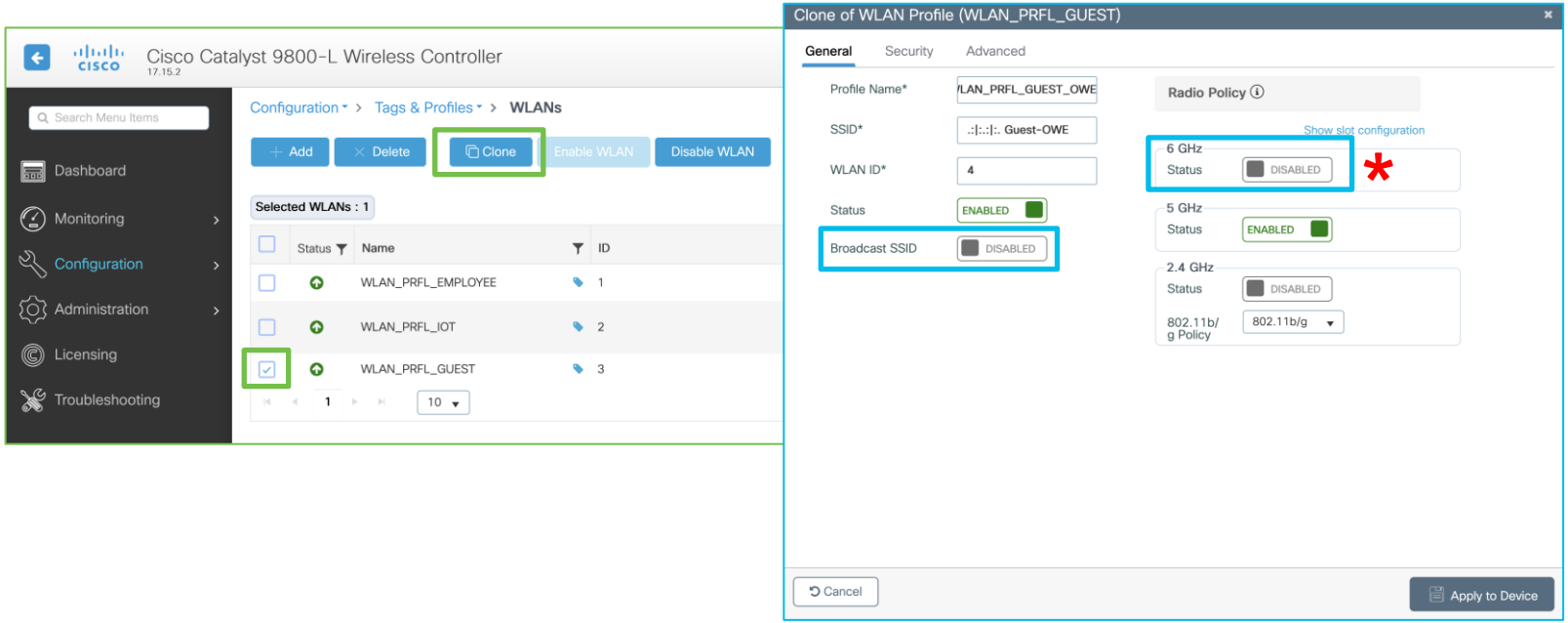


1. New guest WLAN with no L2 security (i.e., fully open) and OWE Transition Mode pointing to the future OWE WLAN ID
2. L3 security as Web Policy, pointing to our Web Auth Parameter Map, with an authC method list for local login and our ACL too
3. As a further recommendation, we block P2P traffic too

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

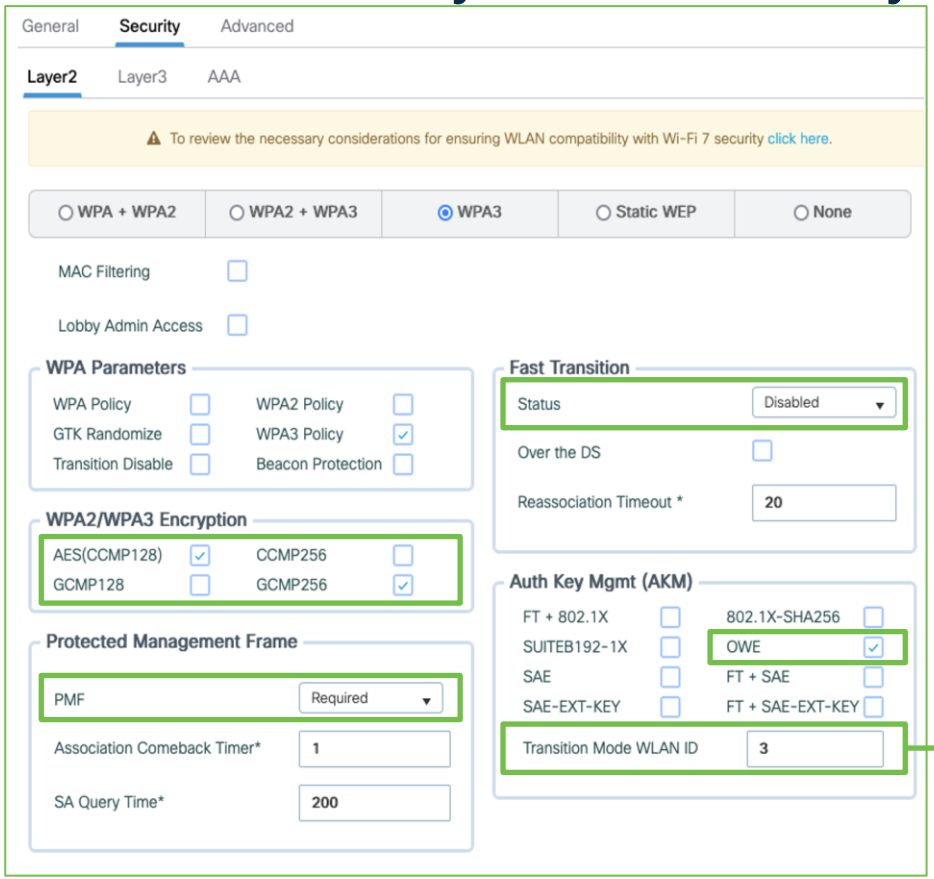
Adding the OWE Guest SSID

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



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

Zoom on Layer 2 Security



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

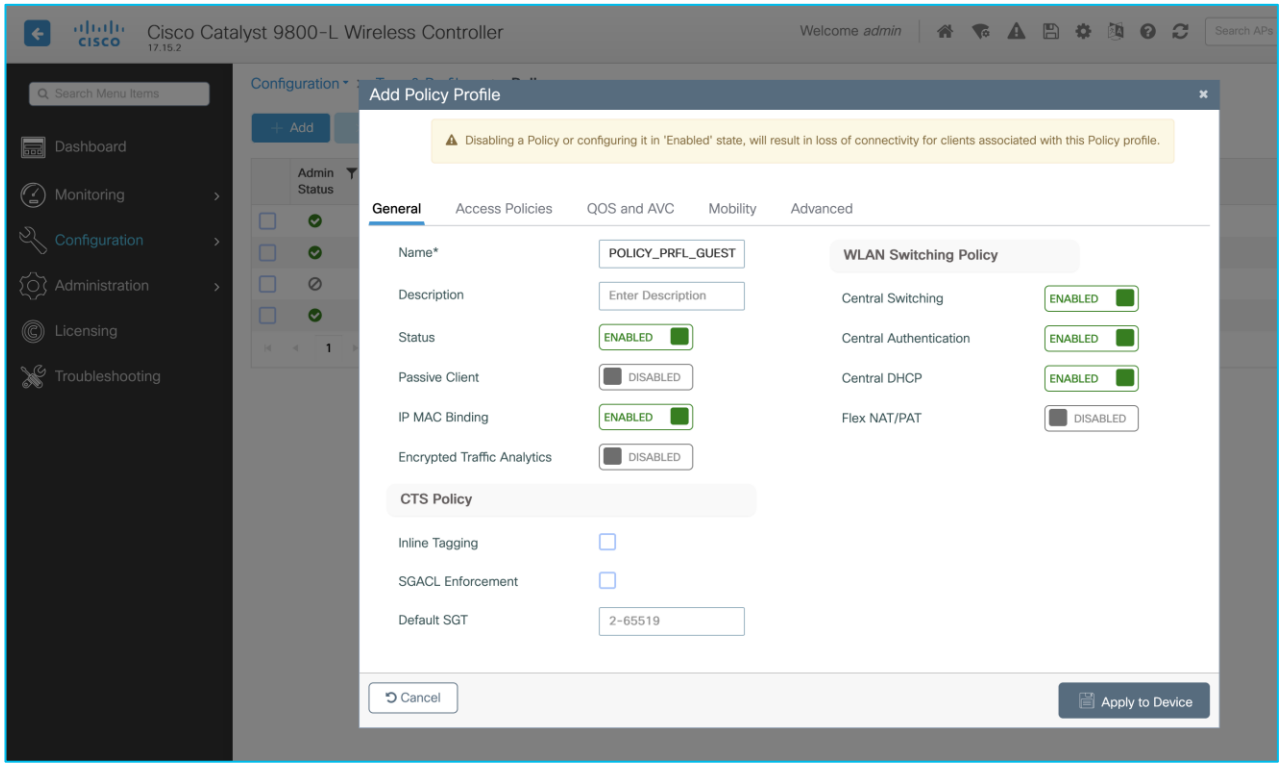
WPA3 settings:
- AES(CCMP128)
- GCMP256

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)

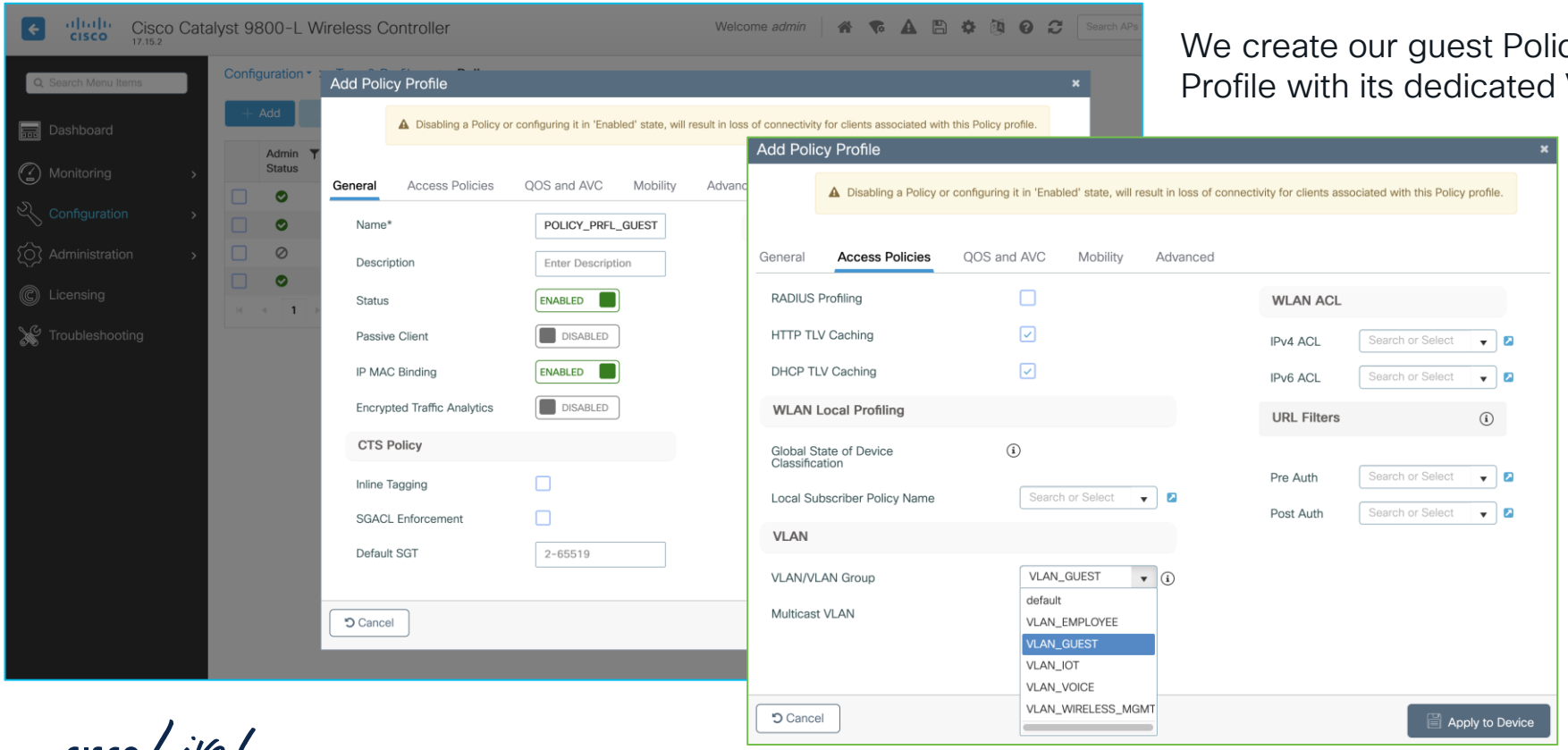
Configuration > Tags & Profiles > Policy



We create our guest Policy Profile with its dedicated VLAN

Adding a Guest SSID (LWA with internal portal)

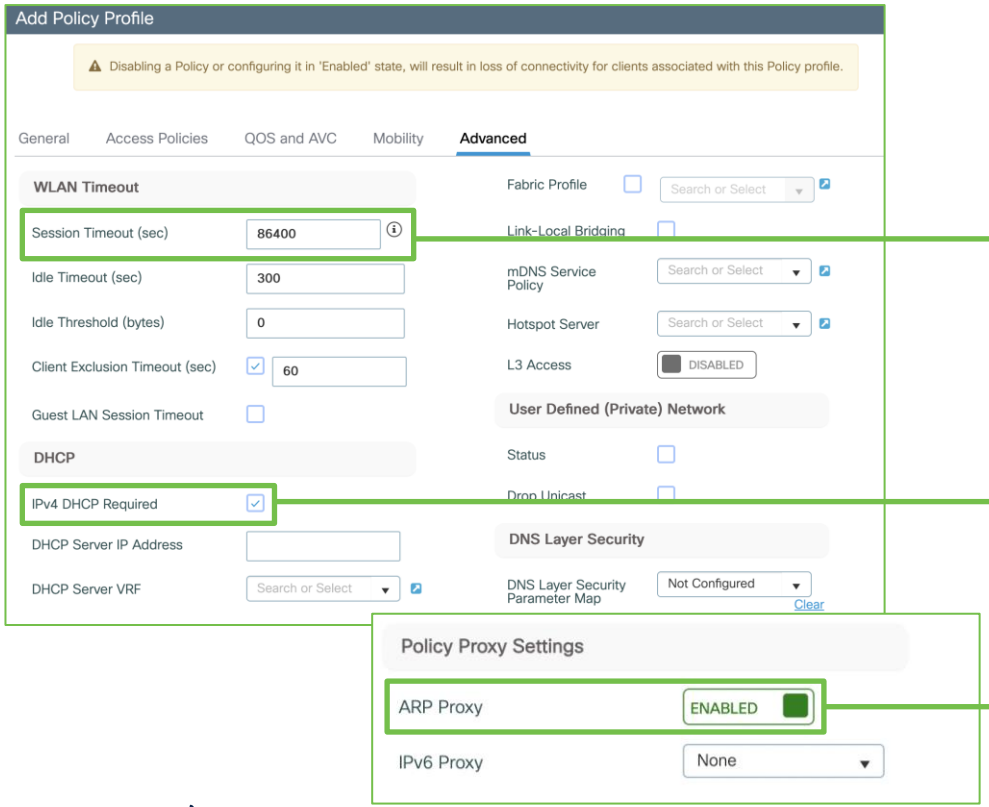
Configuration > Tags & Profiles > Policy



We create our guest Policy Profile with its dedicated VLAN

Configuring the Policy Profile

Configuration > Tags & Profiles > Policy



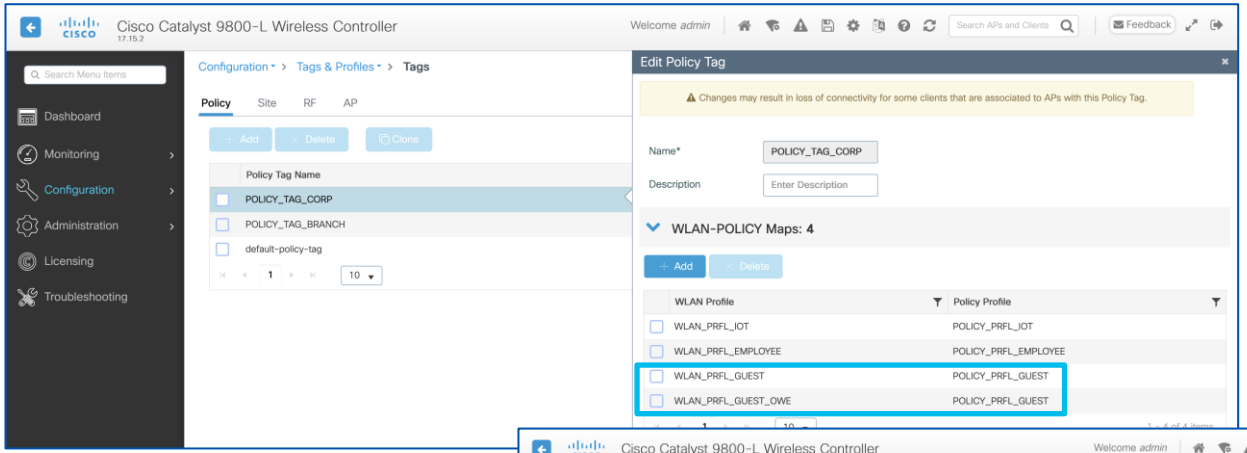
To avoid too many reauthentications

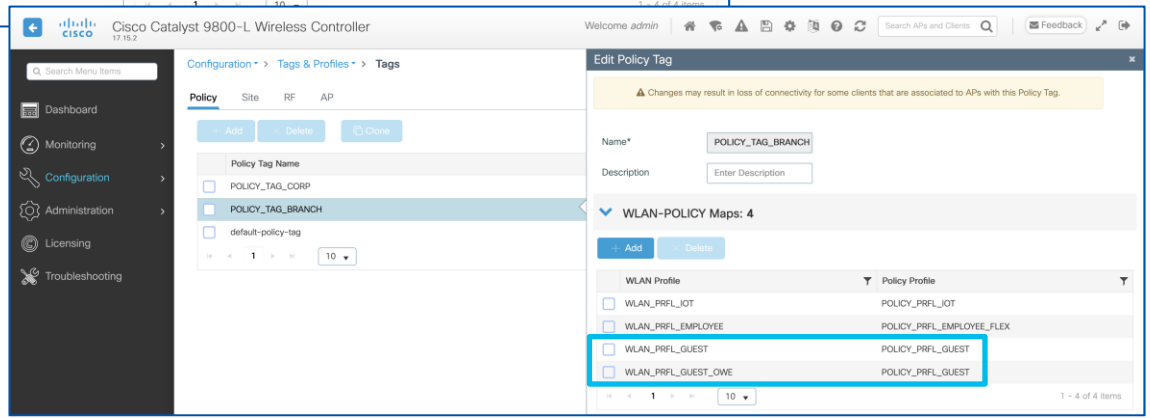
For increased security/control

For increased security/control

Assign the WLAN Profile to the Policy Profile

Configuration > Tags & Profiles > Tags





Here we can reuse our existing Policy Tags, so that APs will automatically start using bith 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

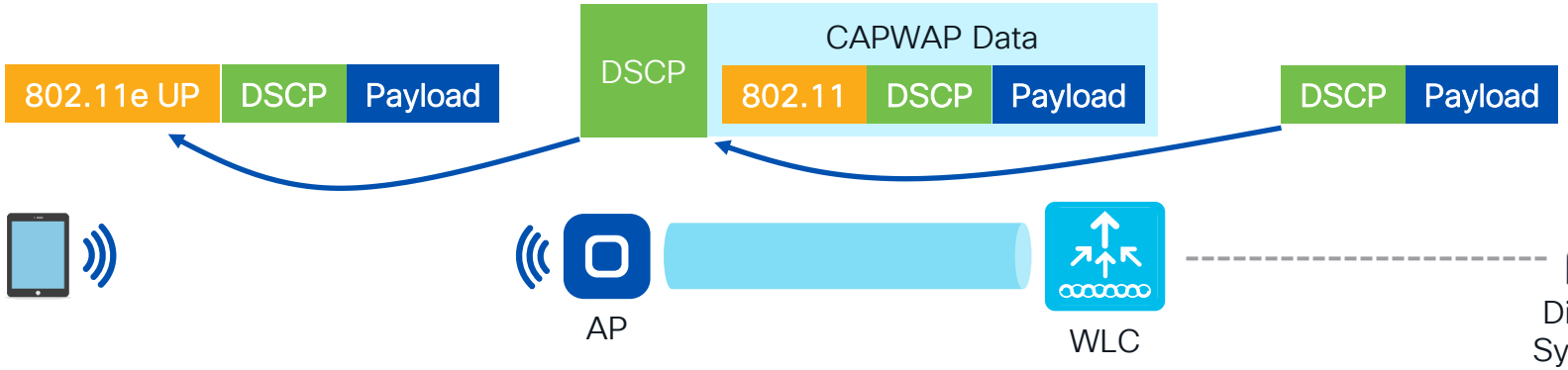
Further tweaks

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
```

For your reference



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)

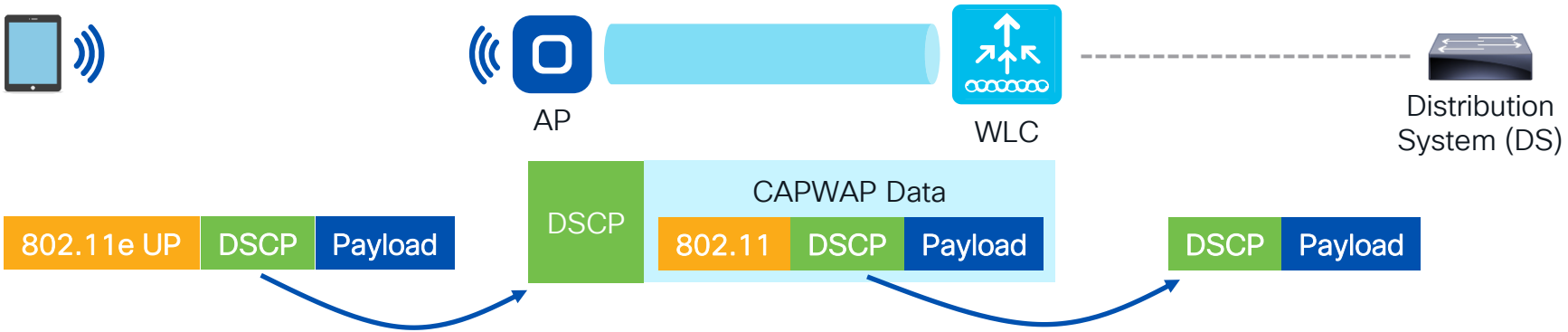
QoS – Trust DSCP Upstream: the one to start with

For your reference

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

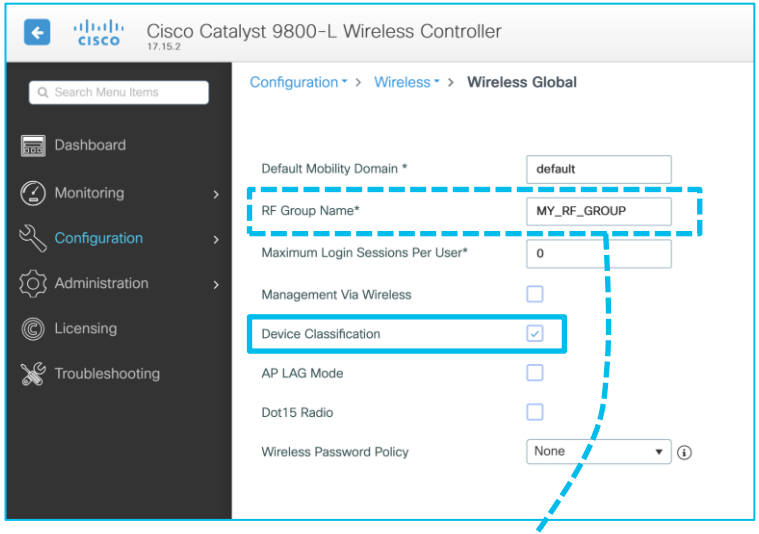
```
ap profile <AP_JOIN_PROFILE_NAME>
 qos-map trust-dscp-upstream
```

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

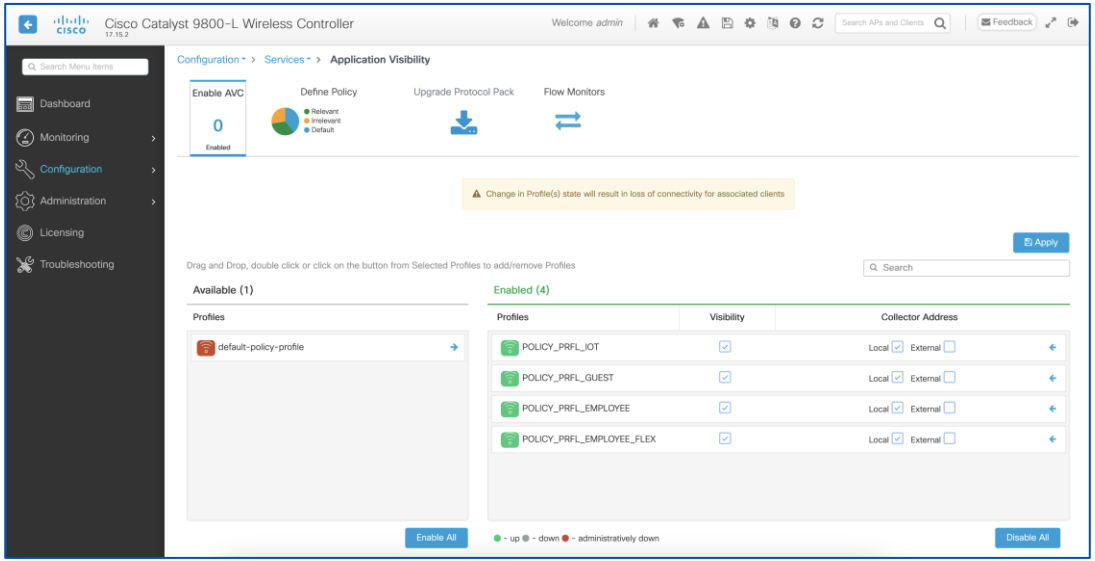


Especially during a PoC/test, we may want to keep the RF group name unique, so that it does not match and interact with others already in production (unless needed)

☞ 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

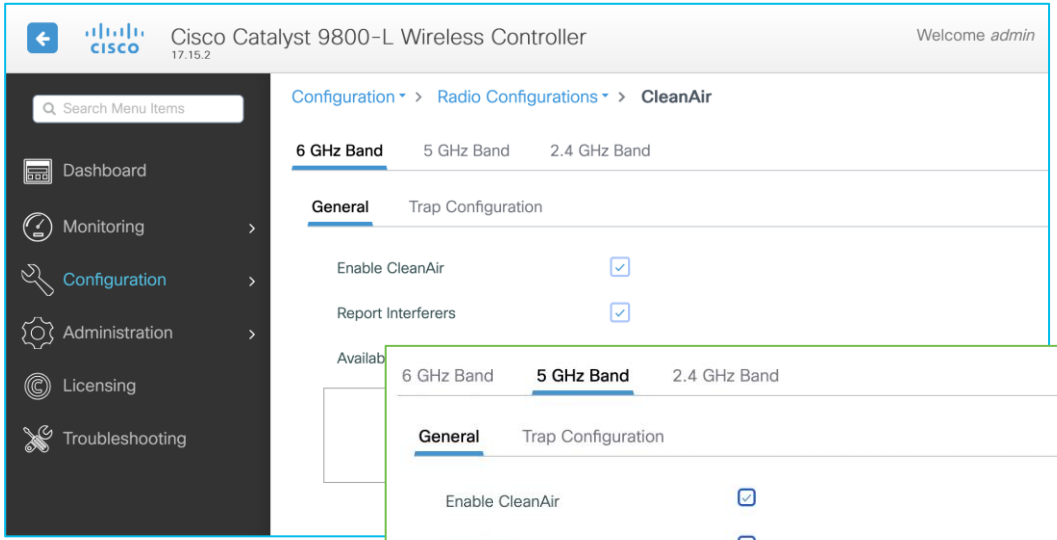
Configuration > Services > Application Visibility

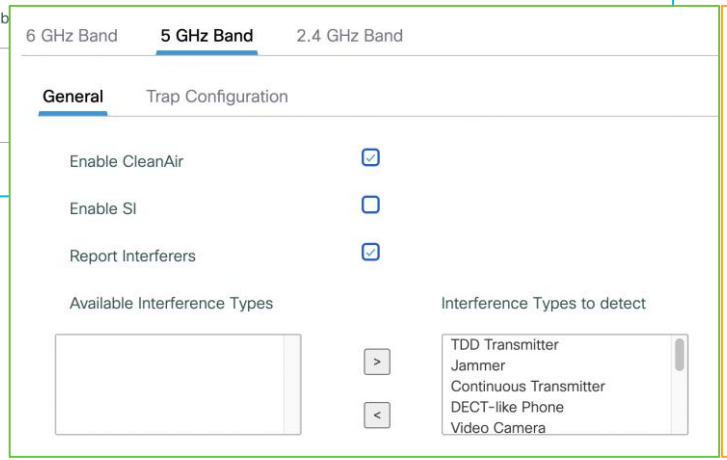


If not already enabled, let's turn on CleanAir

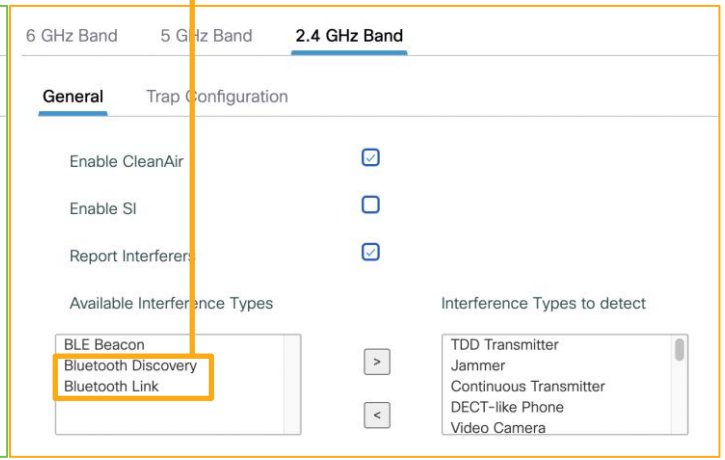
For your reference

Configuration > Radio Configurations > CleanAir





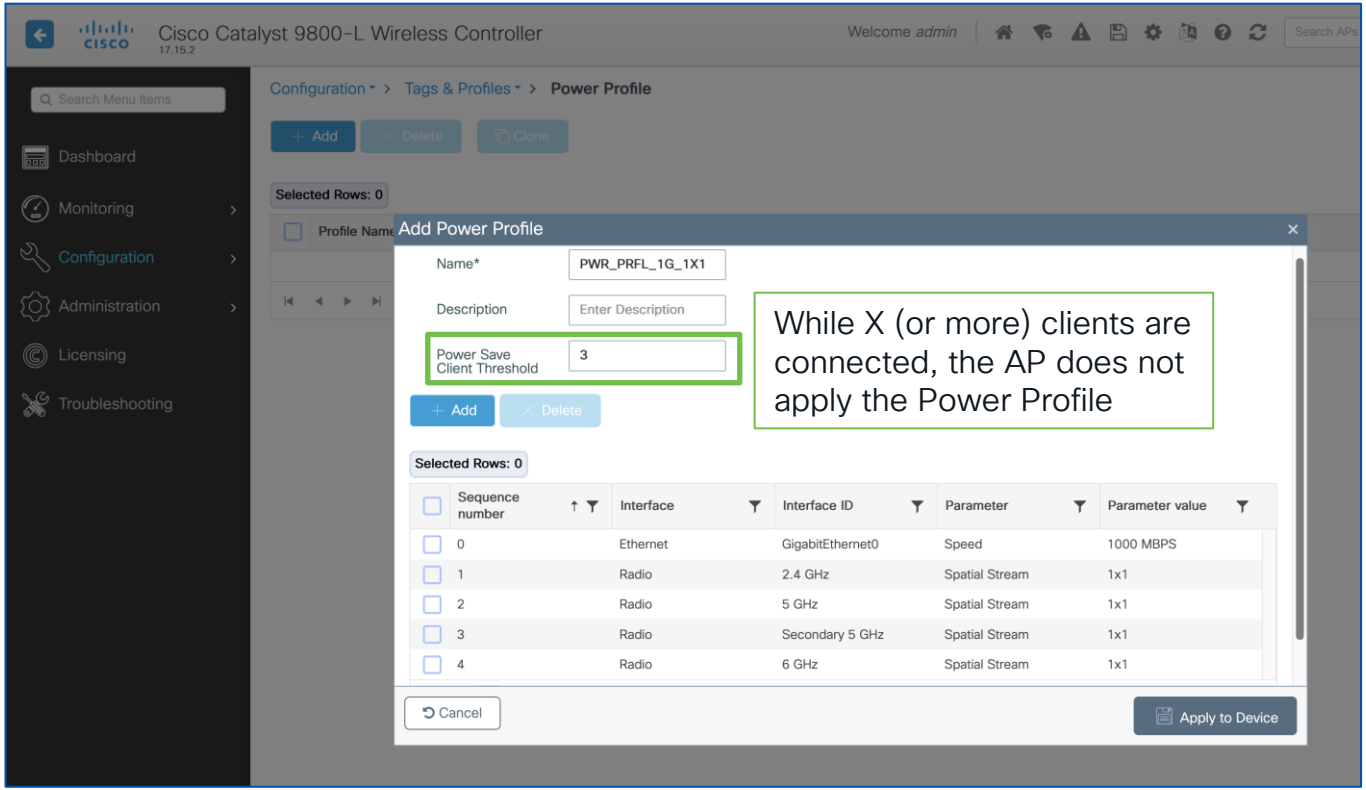
For high density environments we can avoid BT detection to optimize logs/operations



Energy efficiency

For your reference

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



Example of a Power Profile for lower consumption:

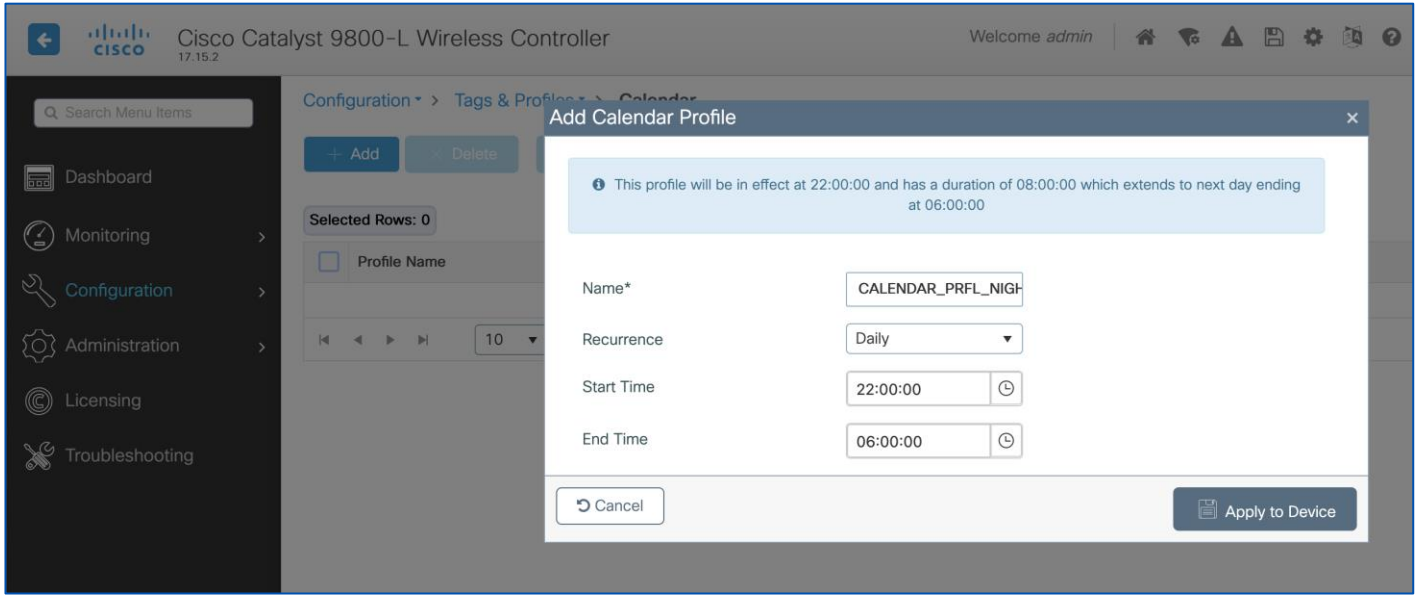
- Ethernet = 1 Gbps
- 2.4 GHz radio = 1x1*
- 5 GHz radio(s) = 1x1*
- 6 GHz radio = 1x1*

* 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

For your reference

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



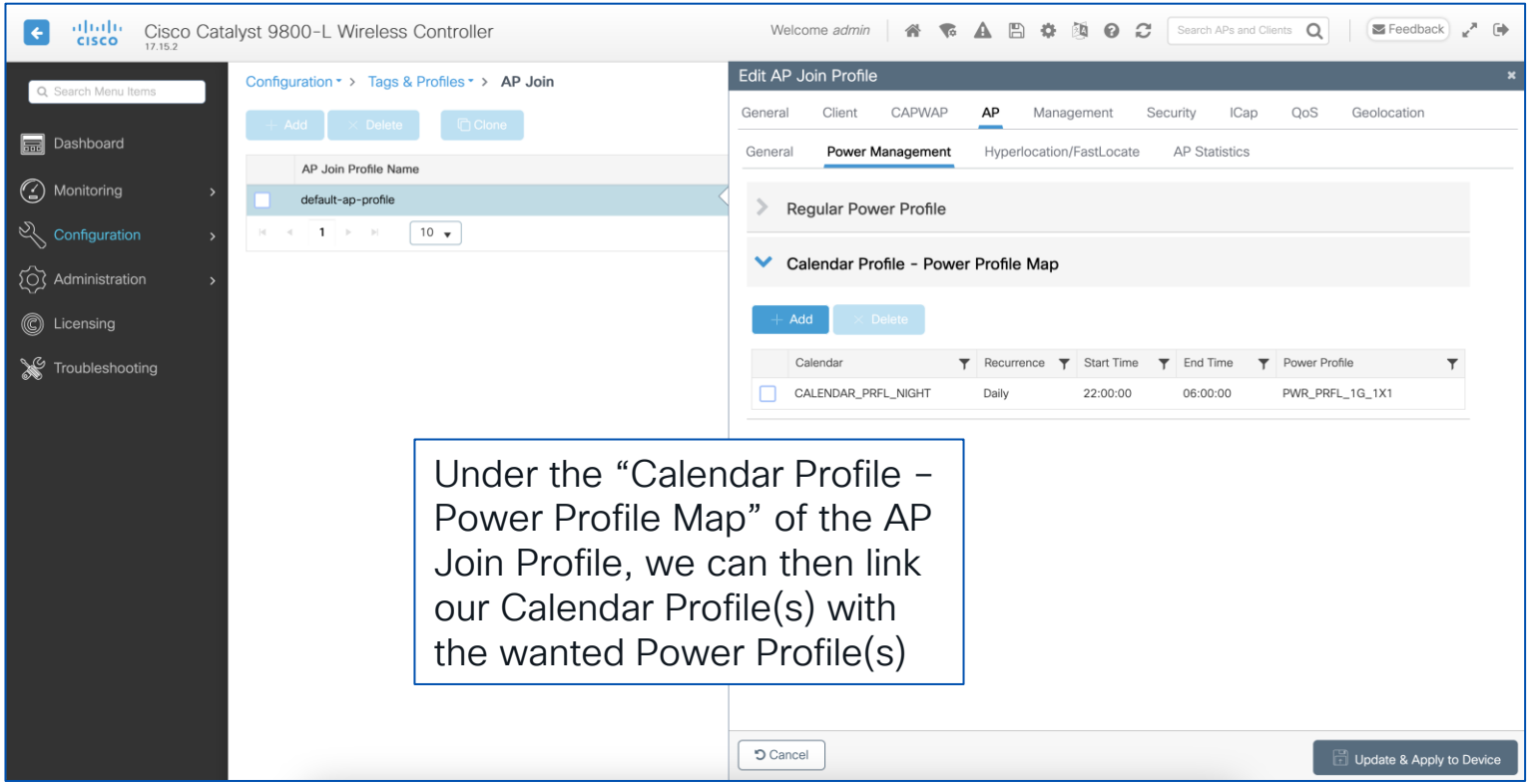
Example of a Calendar Profile for non-working hours:

- Daily
- 10pm to 6am

Energy efficiency

For your reference

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

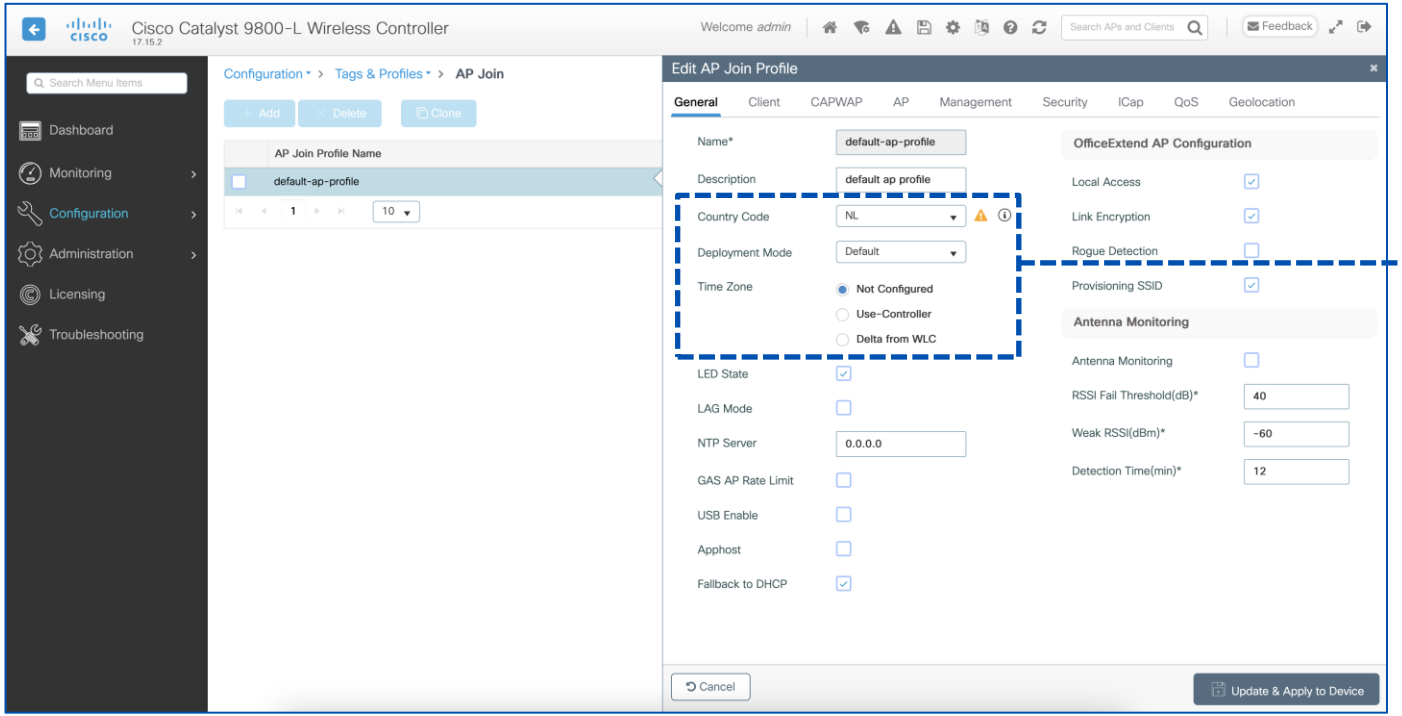


Under the “Calendar Profile – Power Profile Map” of the AP Join Profile, we can then link our Calendar Profile(s) with the wanted Power Profile(s)

AP Join Profile optimizations

For your reference

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

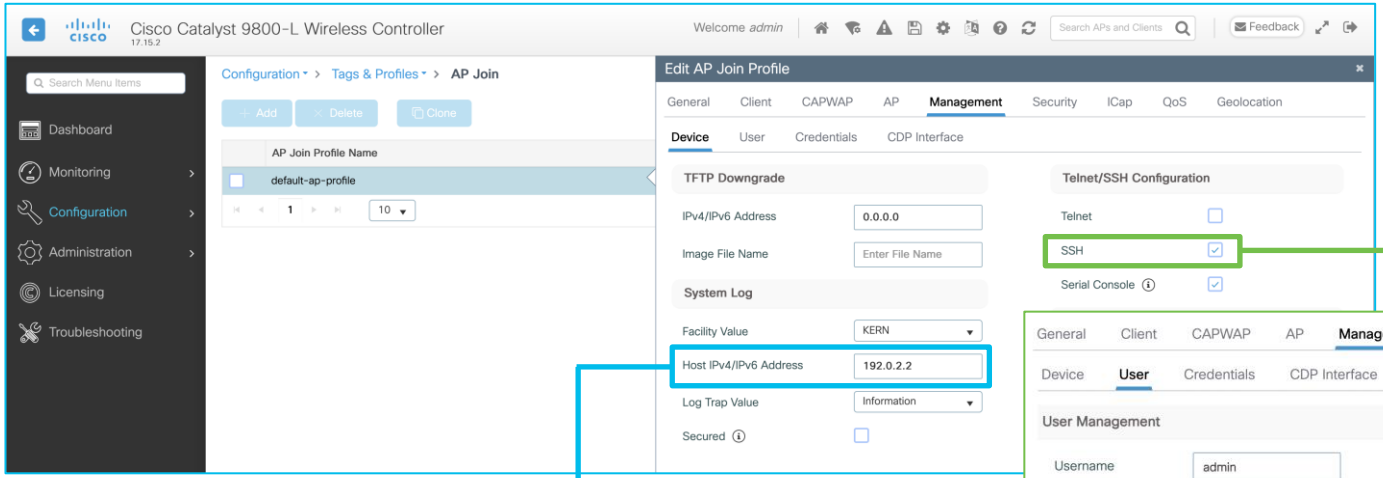


Not always mandatory for APs to work, but generally recommended to set the Country Code, as well as the Time Zone (often “Use-Controller”) for consistency and troubleshooting

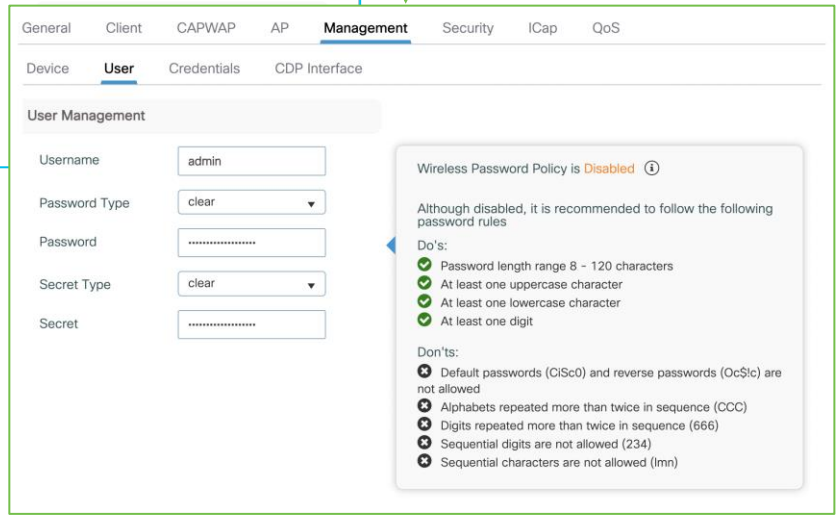
AP Join Profile optimizations

For your reference

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

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

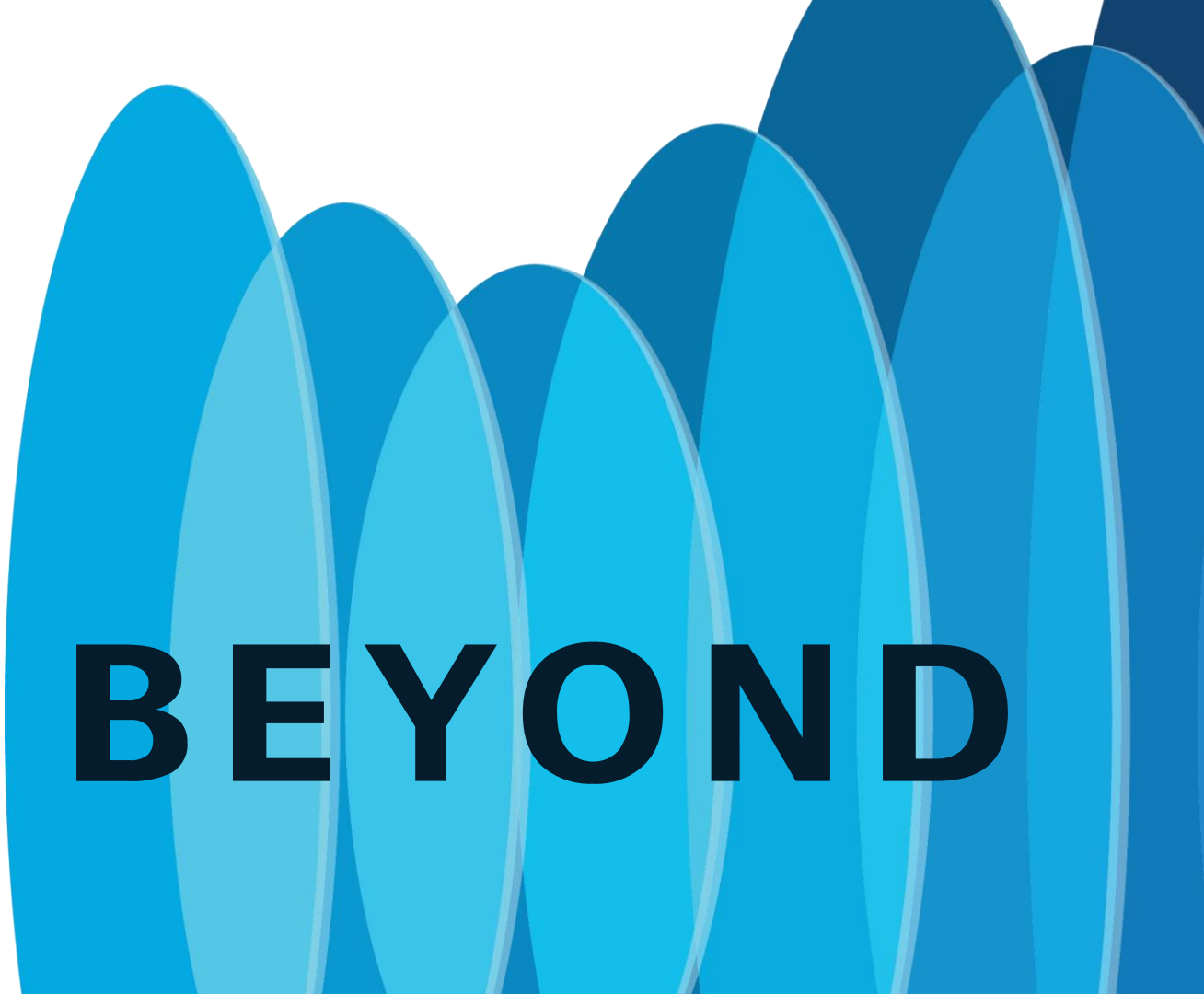
Continue your education

- 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


cisco
Thank you
cisco Live!

cisco Live!



GO BEYOND