Configure Local Web Authentication with Local Authentication

Contents

Introduction

This document describes how to configure Local Web Authentication with Local Authentication on a 9800 Wireless LAN Controller (WLC).

Prerequisites

Cisco recommends that you have knowledge of 9800 WLC configuration model.

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco WLC 9800 series.
- Comprehensive knowledge of Web Authentication.

Components Used

The information in this document is based on these software and hardware versions:

- 9800-CL WLC Cisco IOS® XE version 17.12.5
- Cisco Access Point C9117AXI.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Local Web Authentication (LWA) is a Wireless Local Area Network (WLAN) authentication method that can be configured on the WLC. When a user selects the WLAN from the available network list, they are redirected to a web portal. In this portal, depending on the configuration, the user can be prompted to enter a username and password, accept an Acceptable Use Policy (AUP), or a combination of both actions to finalize their connection.

For information about the four types of web authentication pages presented during the login process, refer to the Configure Local Web Authentication guide and review the available options for the type of Web Authentication. You can also consult the Configure Local Web Authentication with External Authentication guide under the Types of Authentication section.

Parameter Map

Parameter Map is an essential configuration element on a WLC that enables Web Authentication. It consists of a set of settings that govern various facets of the web authentication process, including the authentication type, redirect URLs, appended parameters, timeouts, and custom web pages. To activate and manage web-based authentication for a particular SSID, this map must be linked to the WLAN profile.

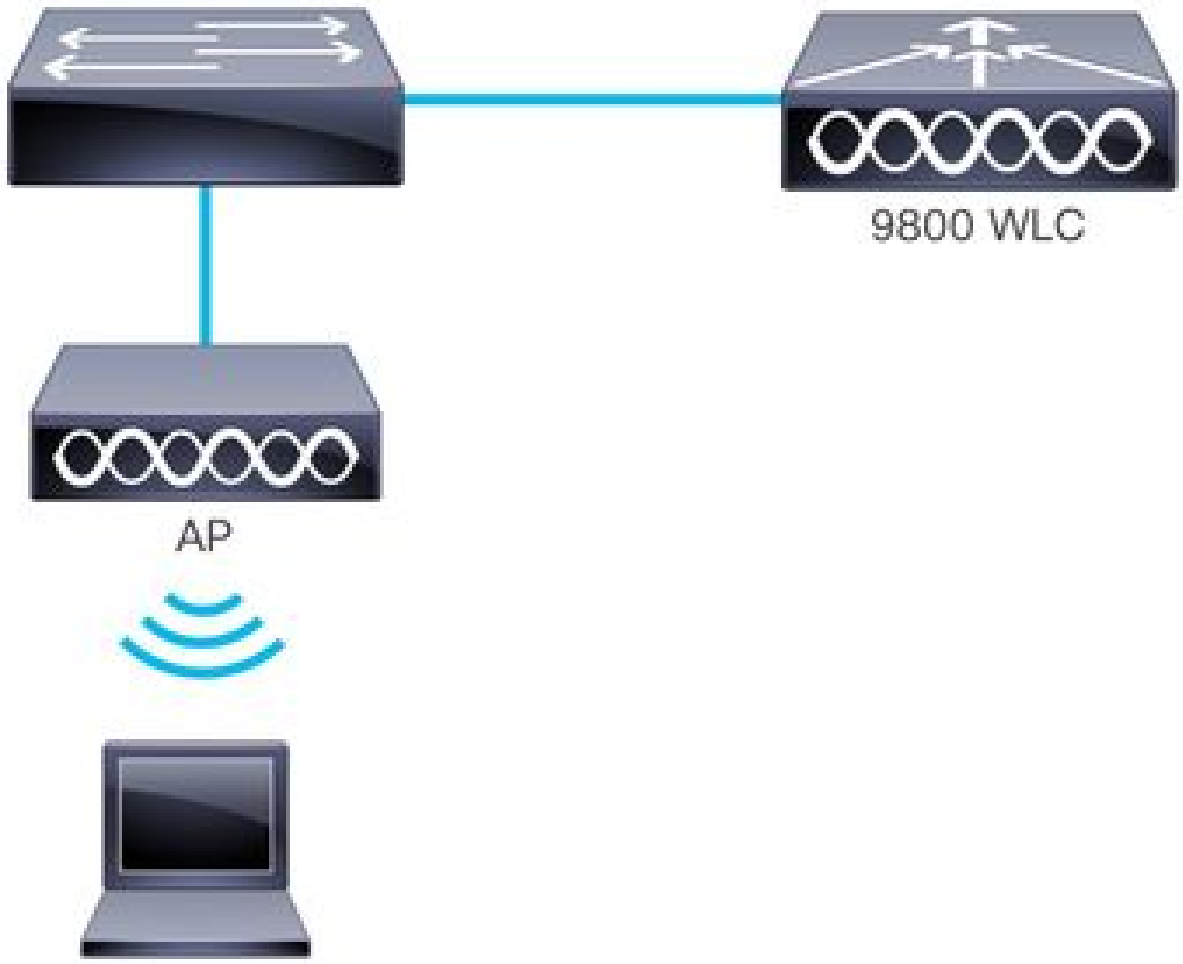
The Wireless LAN Controller comes with a default global parameter map, but administrators have the option to create custom parameter maps to customize the Web Authentication behavior according to specific needs.

Database for Authentication

If the parameter map is configured to use a username and password, you must define the authentication credentials, which are stored locally on the WLC. When you create a guest user account through the GUI, you can set the maximum number of simultaneous logins permitted per guest account. Valid values range from 0 to 64, where 0 indicates that unlimited simultaneous logins are allowed for that guest user.

LWA is primarily intended for small deployments. It supports integration with other authentication methods, you can check the Supported Combination of Authentications for a Client for further information.

The image represents a generic topology of LWA:



Generic Topology of LWA with Local Authentication

Devices in the network topology of LWA:

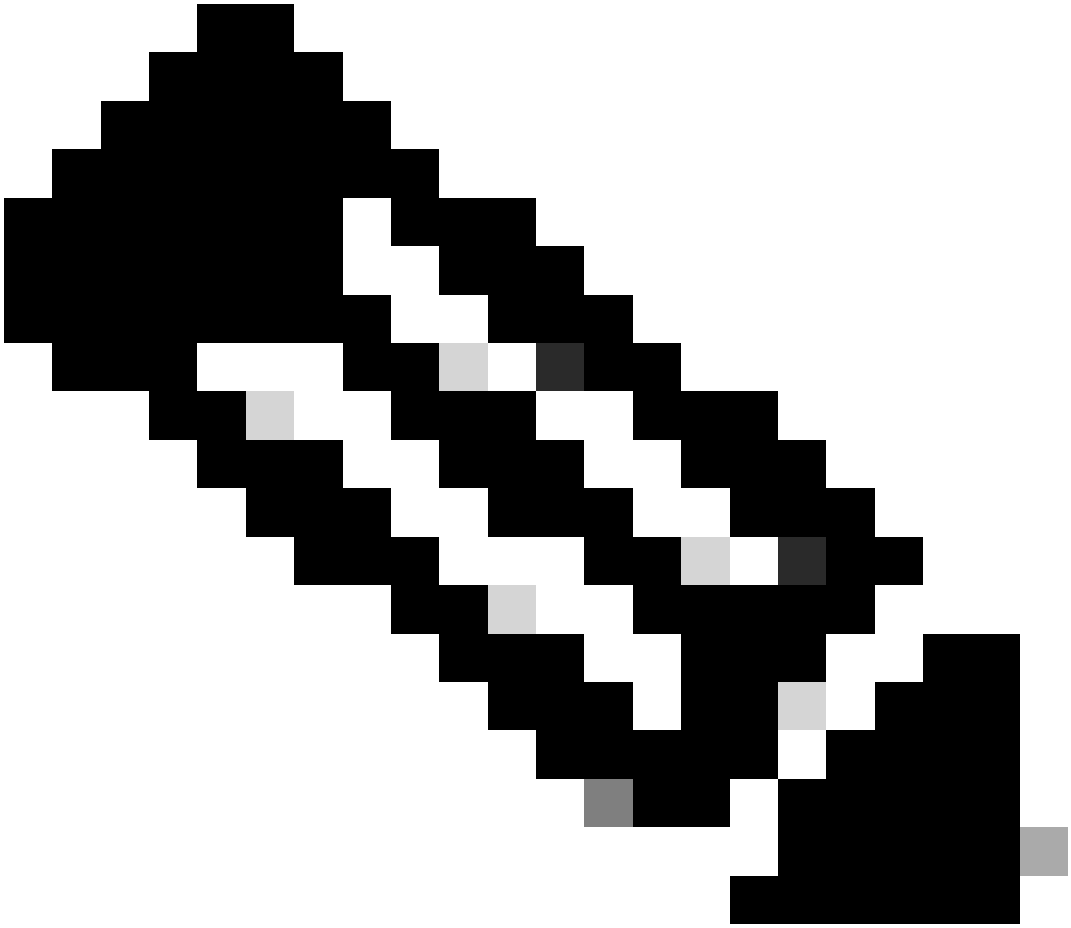
- **Client/Supplicant:** Initiates connection request to the WLAN, later to the DHCP and DNS servers, and responds to communications from the WLC.
- **Access Point:** Connected to a switch, it broadcasts the guest WLAN and provides wireless connectivity to guest devices. It permits DHCP and DNS traffic before the guest user completes authentication by entering valid credentials, accept an AUP, or a combination of both actions.
- **WLC/Authenticator:** Manages the APs and client devices. The WLC hosts the redirect URL and enforces the Access Control List (ACL) that governs traffic and its created by default when configuring the parameter map. It intercepts HTTP requests from guest users and redirects them to a web portal (login page) where users must authenticate. The WLC captures user credentials, authenticates guests, and check the local database to verify credential validity.
- **Authentication server:** In this scenario, the WLC functions as the authentication server. It validates guest user credentials and either grants or denies network access accordingly.

Configure

Local Web Authentication with Local Authentication on the CLI

Method Lists for Local Authentication

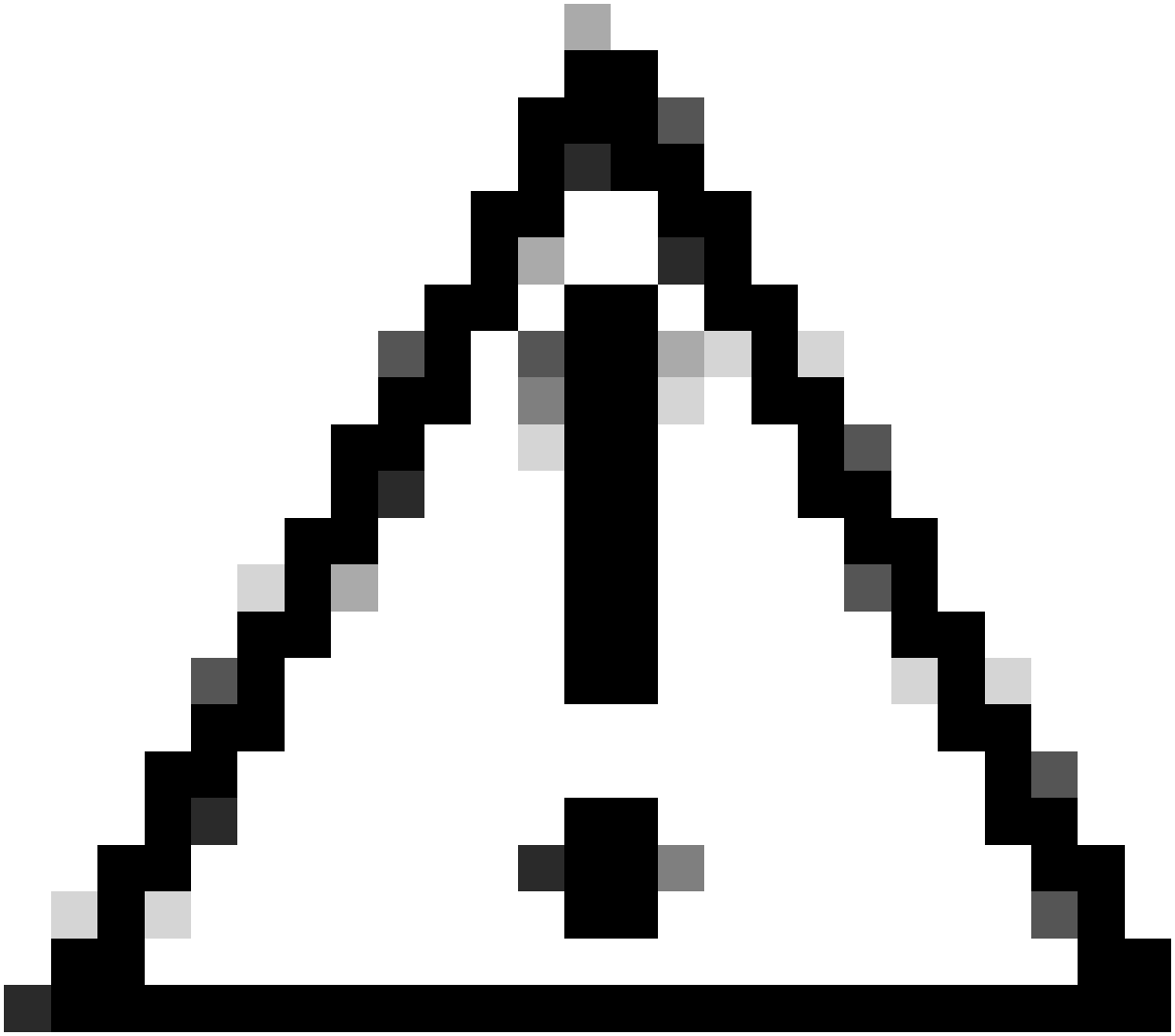
```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#aaa new-model
9800WLC(config)#aaa authentication login LWA_AUTHENTICATION local
9800WLC(config)#aaa authorization network default local
9800WLC(config)#end
```



Note: For Local Login Method List to work, ensure the configuration aaa authorization network default local exists on the WLC. This is necessary as the WLC authorizes the user into the network.

Parameter Maps

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#parameter-map type webauth global
9800WLC(config-params-parameter-map)#type webauth
9800WLC(config-params-parameter-map)#virtual-ip ipv4 192.0.2.1
9800WLC(config-params-parameter-map)#trustpoint <trustpoint name>
9800WLC(config-params-parameter-map)#webauth-http-enable
9800WLC(config-params-parameter-map)#end
```



Caution: Virtual IP must be a non-routable address proposed on RFC 5737. By default, the IP 192.0.2.1 is set. See more information on Virtual IP address from Cisco Catalyst 9800 Series Configuration Best Practices. On AireOs most of the time the IP used was 1.1.1.1. This is not recommended anymore as it became a public IP.

The capability to create multiple parameter maps enables tailored flows: customized web pages, and specific presentation parameters for each WLAN. The global parameter map determines the Trustpoint and thus the certificate that the WLC presents to the client on the redirection portal. Additionally, it controls the types of

client traffic intercepted, such as HTTP/HTTPS for the redirection portal, domain or hostname resolution for the virtual IP address. This separation allows the global map to handle overarching settings like certificate presentation and traffic interception, while user-defined parameter maps provide granular experience per WLAN.

WLAN Security Parameters

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#wlan LWA_LA 1 "LWA LA"
9800WLC(config-wlan)#no security wpa
9800WLC(config-wlan)#no security wpa wpa2
9800WLC(config-wlan)#no security wpa wpa2 ciphers aes
9800WLC(config-wlan)#no security wpa akm dot1x
9800WLC(config-wlan)#security web-auth
9800WLC(config-wlan)#security web-auth authentication-list LWA_AUTHENTICATION
9800WLC(config-wlan)#security web-auth parameter-map global
9800WLC(config-wlan)#no shutdown
9800WLC(config-wlan)#end
```

Create a Policy Profile

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#wireless profile policy <POLICY_PROFILE>
9800WLC(config-wireless-policy)#vlan <vlan name>
9800WLC(config-wireless-policy)#no shutdown
9800WLC(config-wireless-policy)#end
```

Create a Policy Tag

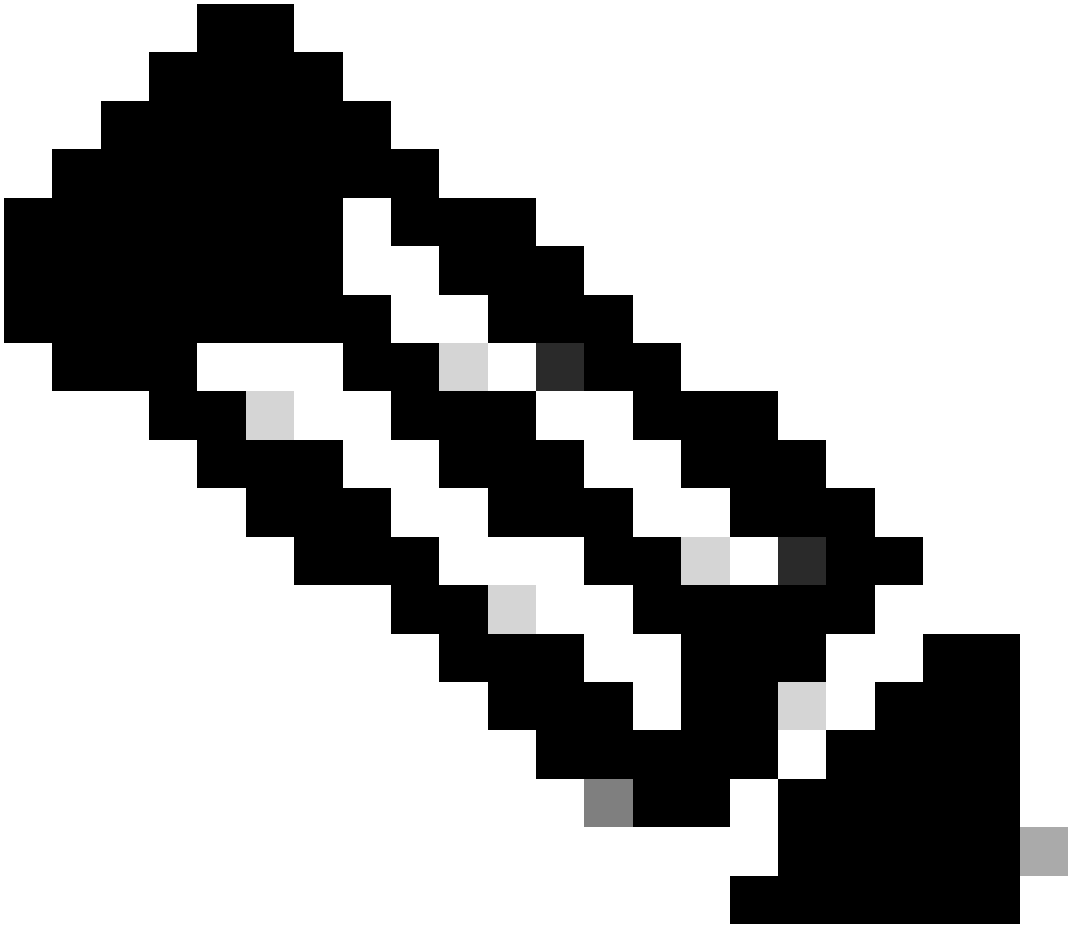
```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#wireless tag policy <POLICY_TAG>
9800WLC(config-policy-tag)#wlan LWA_LA policy <POLICY_PROFILE>
9800WLC(config-policy-tag)# end
```

Assign a Policy Tag to an AP

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#ap <MAC Address>
9800WLC(config-ap-tag)#policy-tag POLICY_TAG
9800WLC(config-ap-tag)#end
```

Create Guest Username

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#user-name johndoe
9800WLC(config-user-name)#description Guest-User
9800WLC(config-user-name)#password 0 Cisco123
9800WLC(config-user-name)#type network-user description <description> guest-user lifetime year 0 month
9800WLC(config-user-name)#end
```

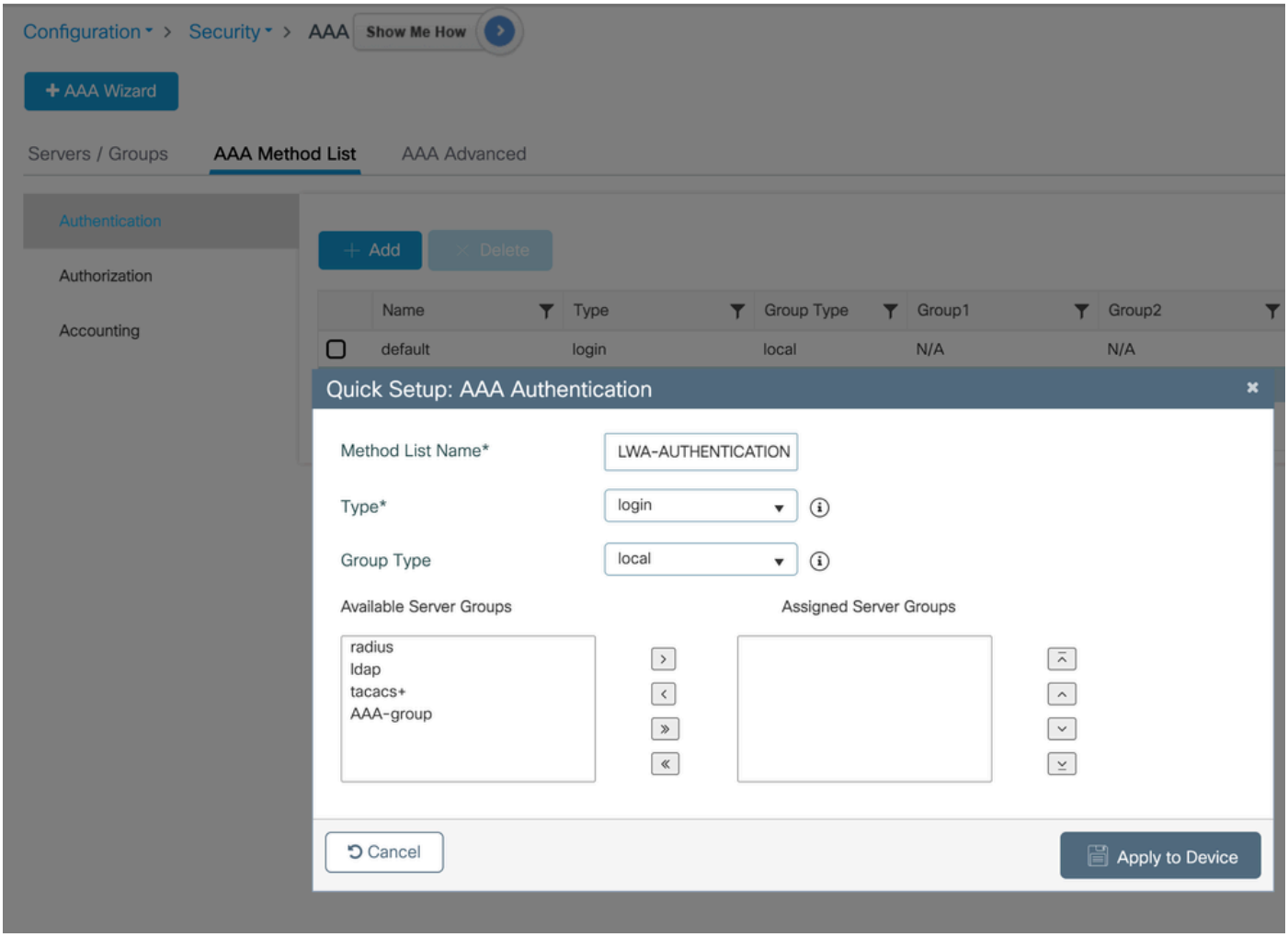


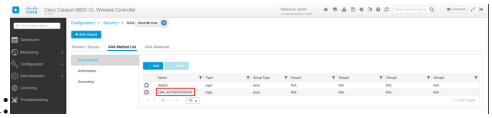
Note: When setting the lifetime for the guest user, if the year is set to 1, you can not specify the subsequent parameters that is months, days, hours and minutes since the maximum lifetime is 1 year.

Local Web Authentication with Local Authentication via WebUI

Method Lists for Local Authentication

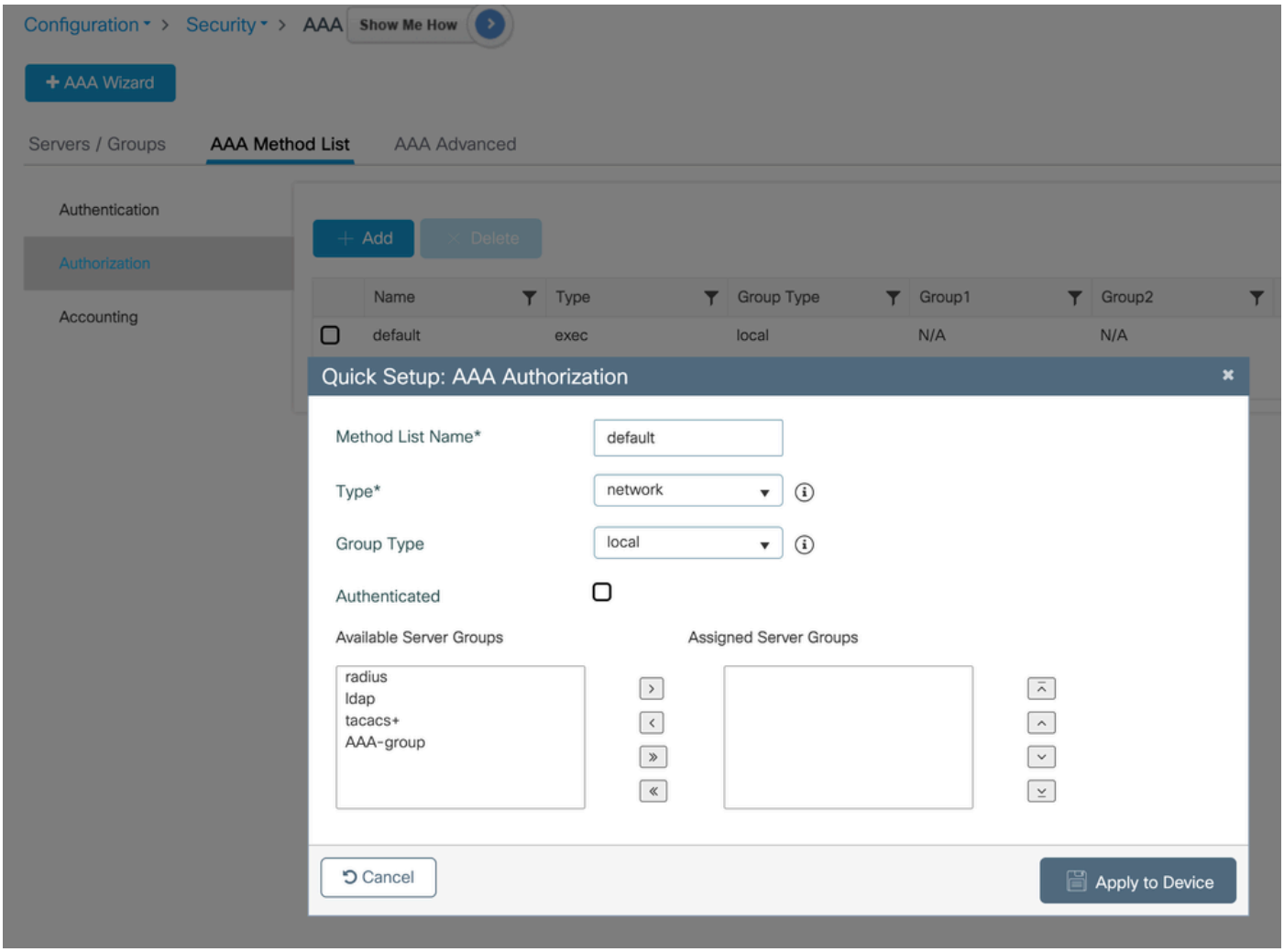
Navigate to **Configuration > Security > AAA > AAA Method List > Authentication > Add** to create the method list later to be used in the WLAN configuration.



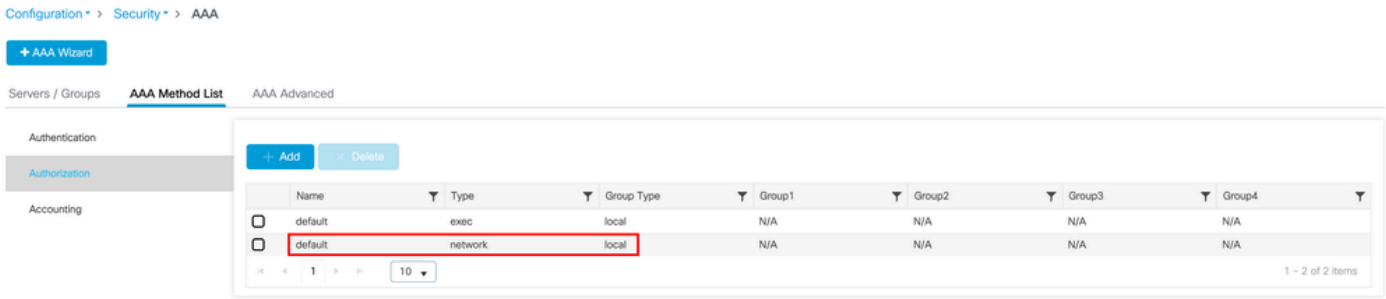
After clicking **Apply to Device**, confirm the AAA method list creation: 

Ensure there is a local authorization method list, this is a requirement for the local login method list created to work.

Configuration > Security > AAA > AAA Method List > Authorization > Add

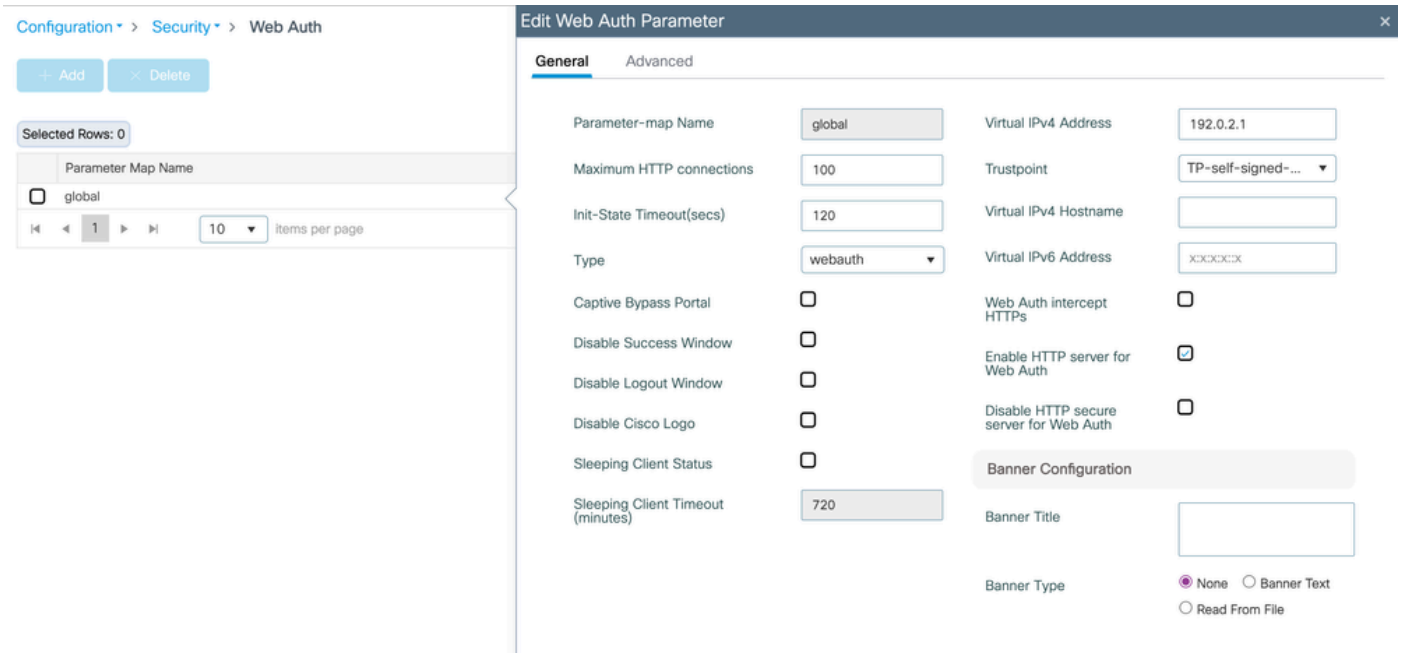


After clicking **Apply to Device**, confirm the AAA method list creation:

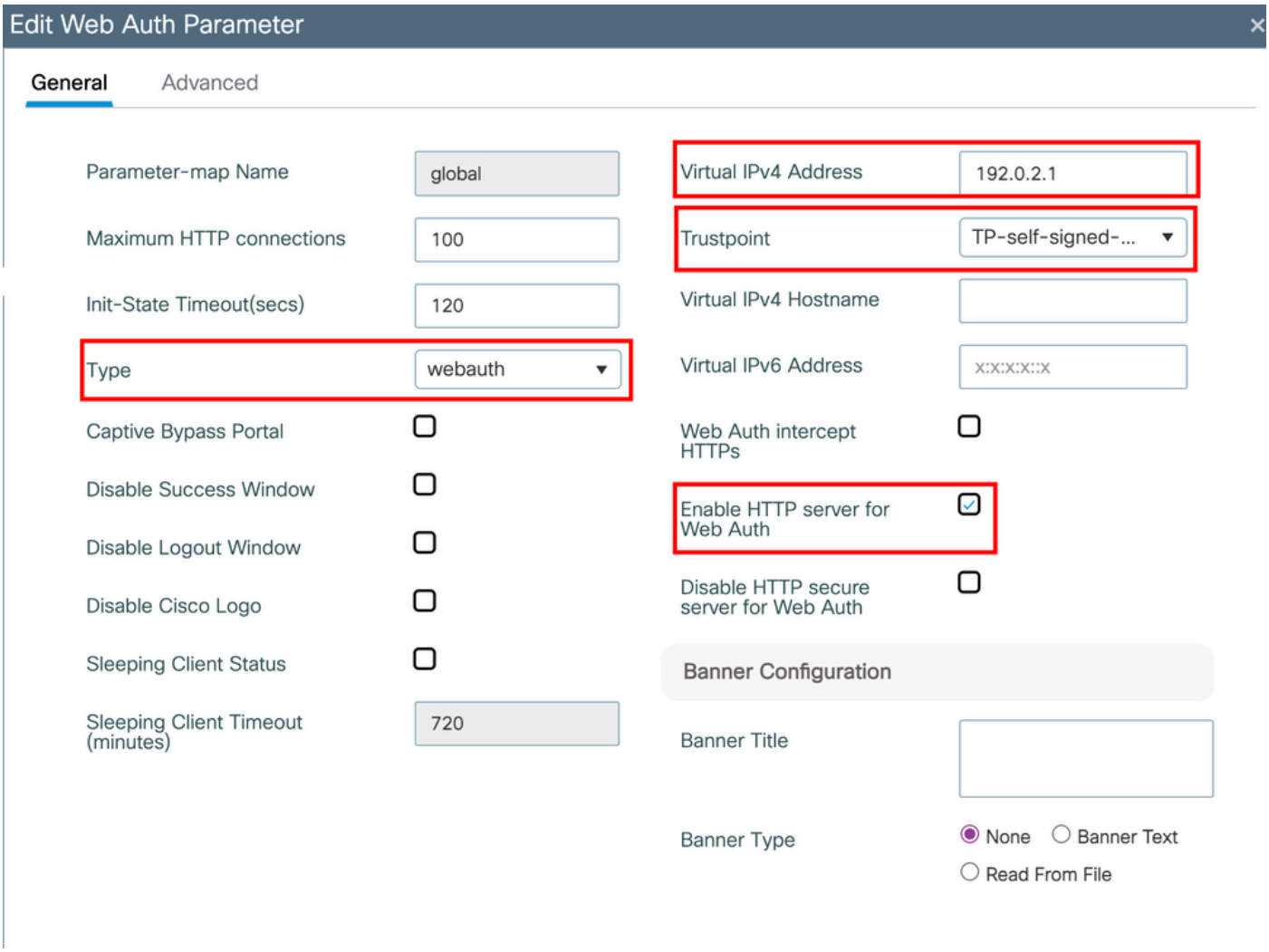


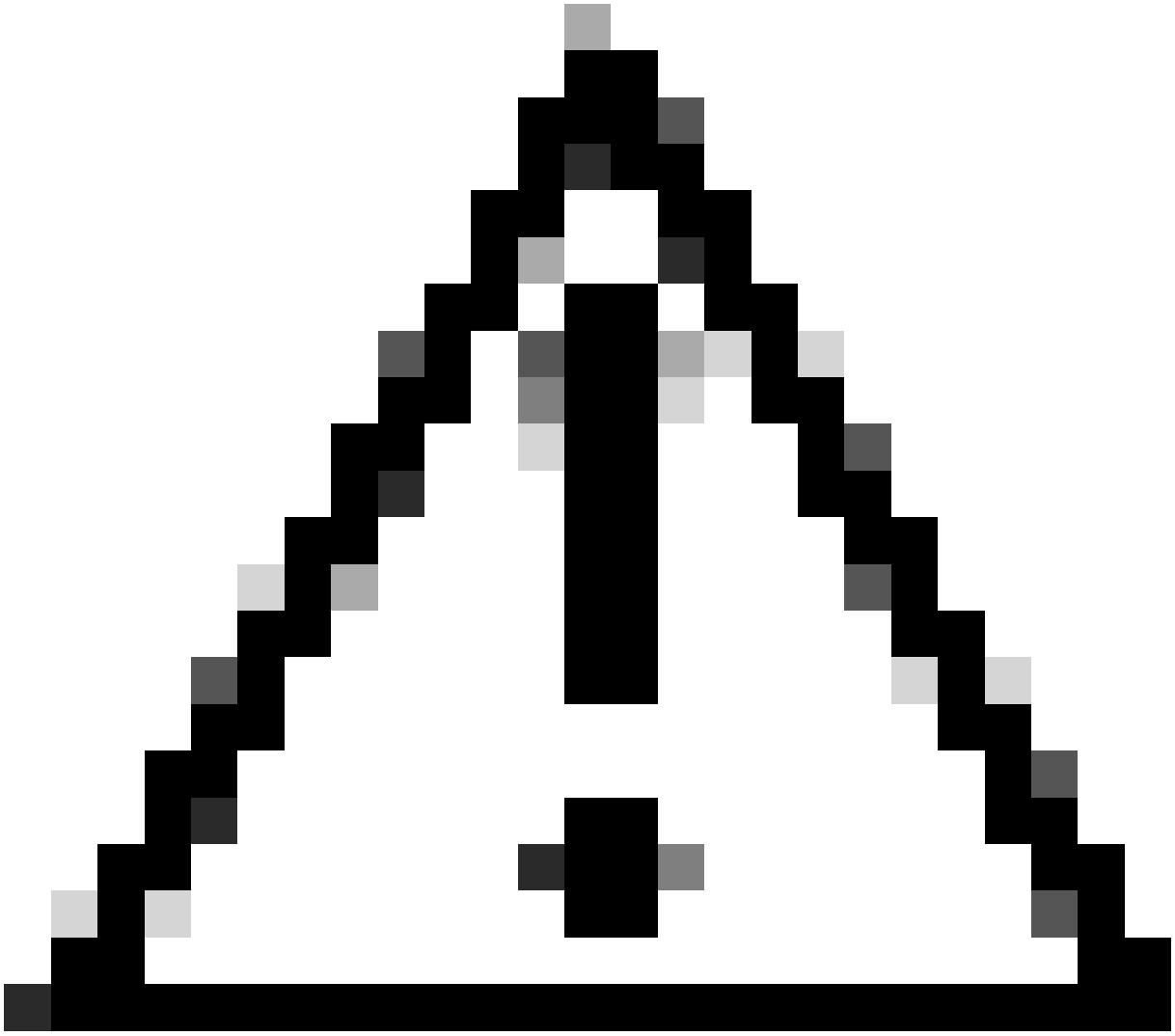
Parameter Maps

Edit the Global Parameter Map on **Configuration > Security > Web Auth**



Select the type of web authentication to be used, Virtual IP and the Trustpoint the WLC presents on the web portal. In this case, the Self-Signed certificate is selected and is likely to cause a disclaimer of the kind "your connection is not private net::ERR_CERT_AUTHORITY_INVALID" as this is a Locally Significant Certificate (LSC) and is not signed by a recognizable CA on the internet. To amend this, use a third party signed certificate. Details are depicted on Generate and Download CSR Certificates on Catalyst 9800 WLCs or there is a video option that explains the upload and Truspoint creation Renew Certificates for WebAuth & WebAdmin on Cisco 9800 WLC | Secure Wireless LAN Controller Setup.

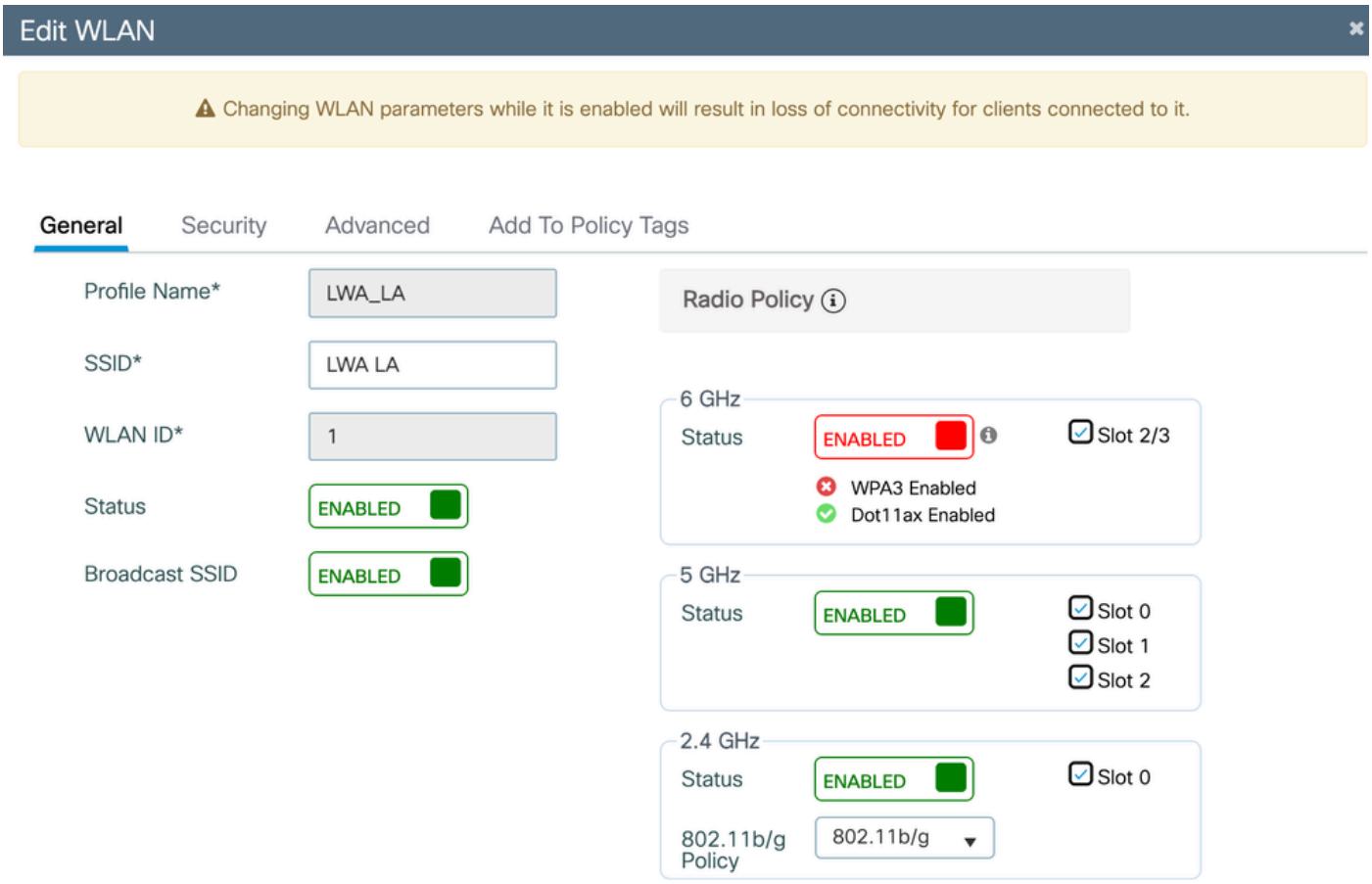

Edit Web Auth Parameter
General
Advanced
Parameter-map Name
global
Maximum HTTP connections
100
Init-State Timeout(secs)
120
Type
webauth
Captive Bypass Portal
Disable Success Window
Disable Logout Window
Disable Cisco Logo
Sleeping Client Status
Sleeping Client Timeout (minutes)
720
Virtual IPv4 Address
192.0.2.1
Trustpoint
TP-self-signed-...
Virtual IPv4 Hostname
Virtual IPv6 Address
x:x:x:x::x
Web Auth intercept HTTPs
Enable HTTP server for Web Auth
Disable HTTP secure server for Web Auth
Banner Configuration
Banner Title
Banner Type
None
Banner Text
Read From File



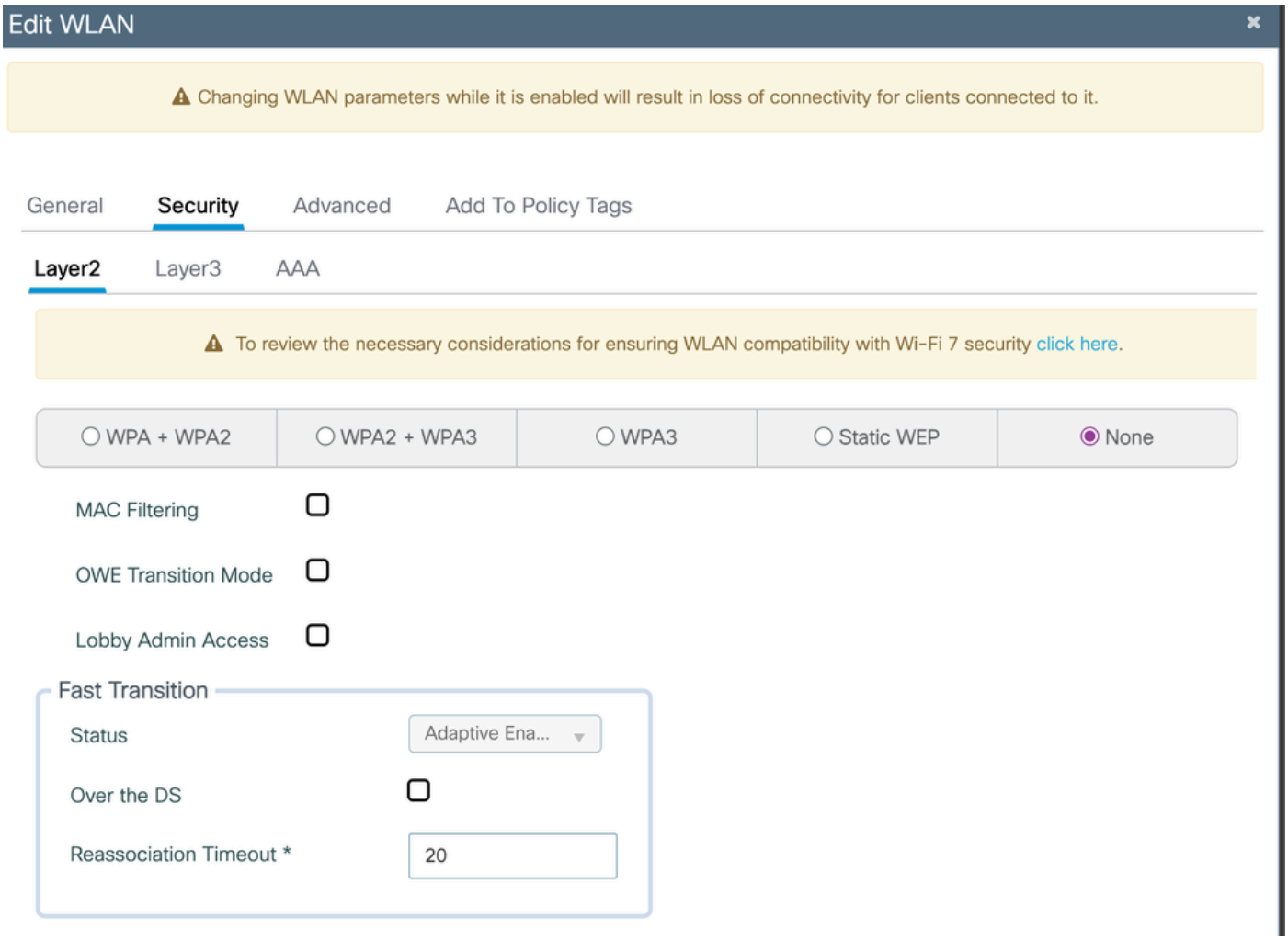
Caution: If you have HTTP globally disabled on the 9800, ensure you have the Enable HTTP server for Web Auth checked as Cisco separated the dependency of these processes. Clients or Supplicants are expected to initiate an HTTP connection process and that session is intercepted by the controller to present the web portal. For that reason it is not recommended to enable Web Auth Intercept HTTPS unless absolutely required, as this setting is unnecessary for most deployments and can increase the controller CPU utilization, potentially impacting performance.

WLAN Security Parameters

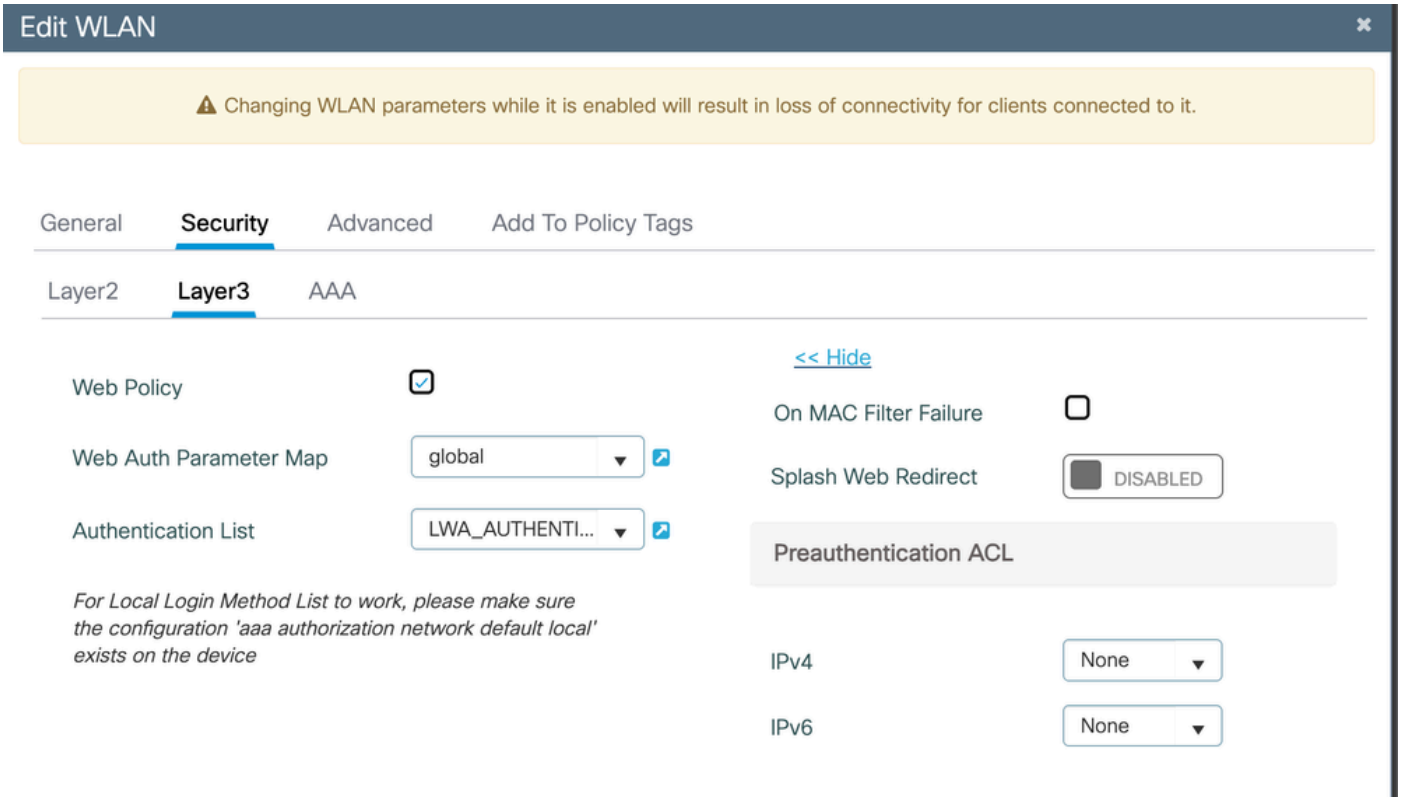
Navigate to **Configuration > Tags & Profiles > WLANs**, click **Add**.



On the Security tab, for Layer2 select **None**.

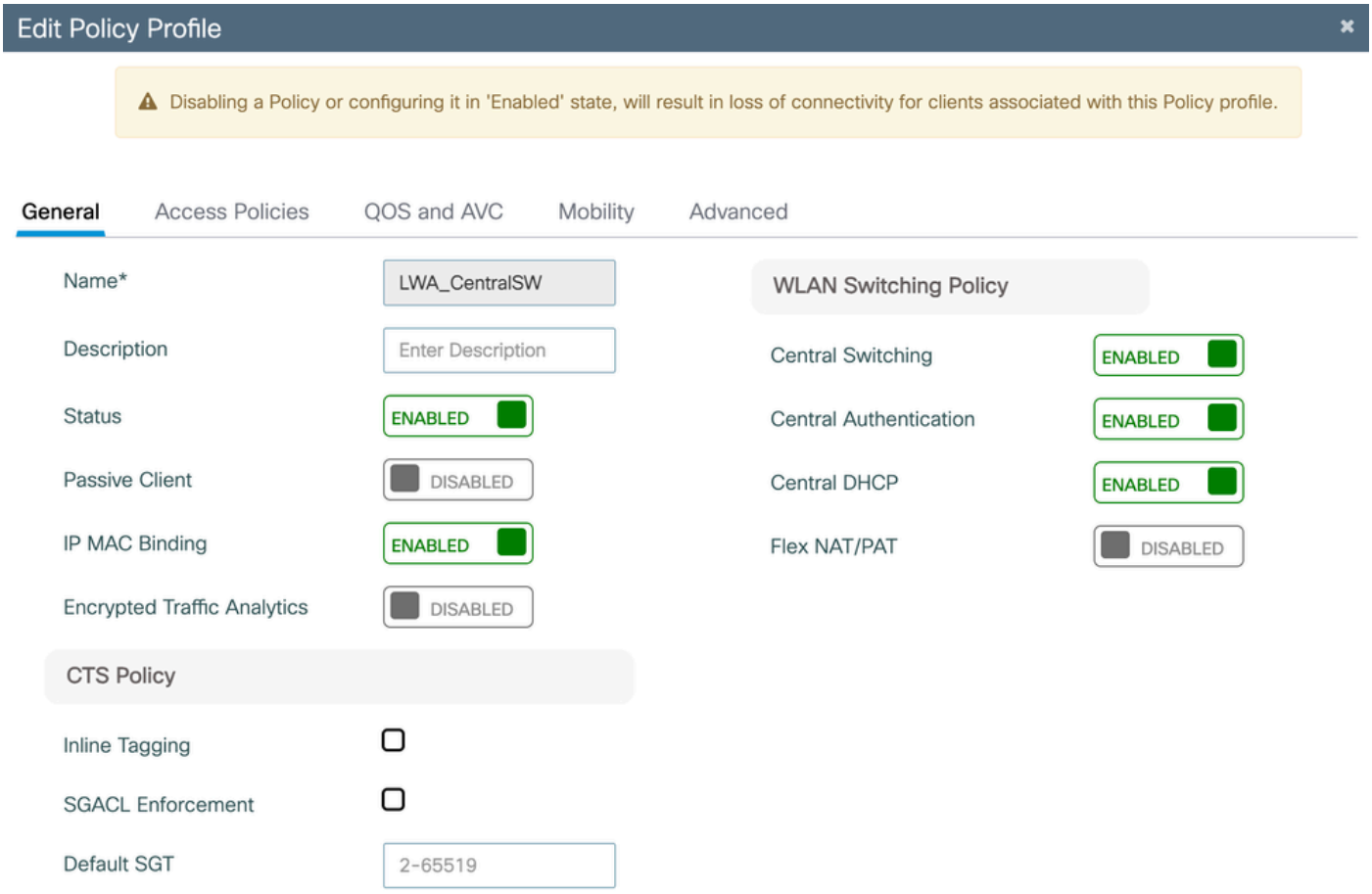


On the Security tab, for Layer3 check the Web Policy box, select the Parameter Map previously configured from the drop-down menu and the Authentication List.

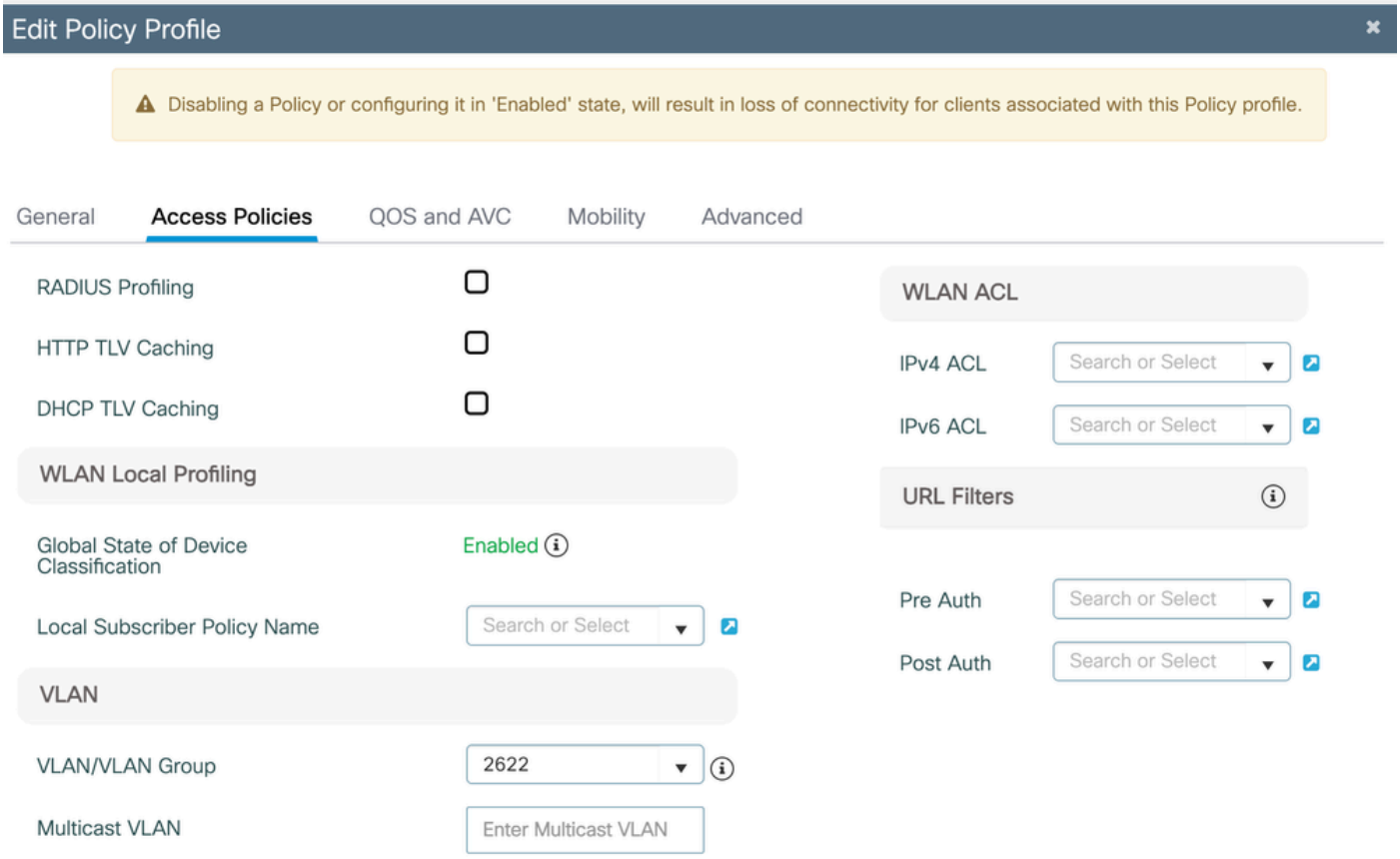


Create a Policy Profile

In order to create the Policy Profile that to be linked to the WLAN profile, navigate to **Configuration > Tags & Profiles > Policy**.

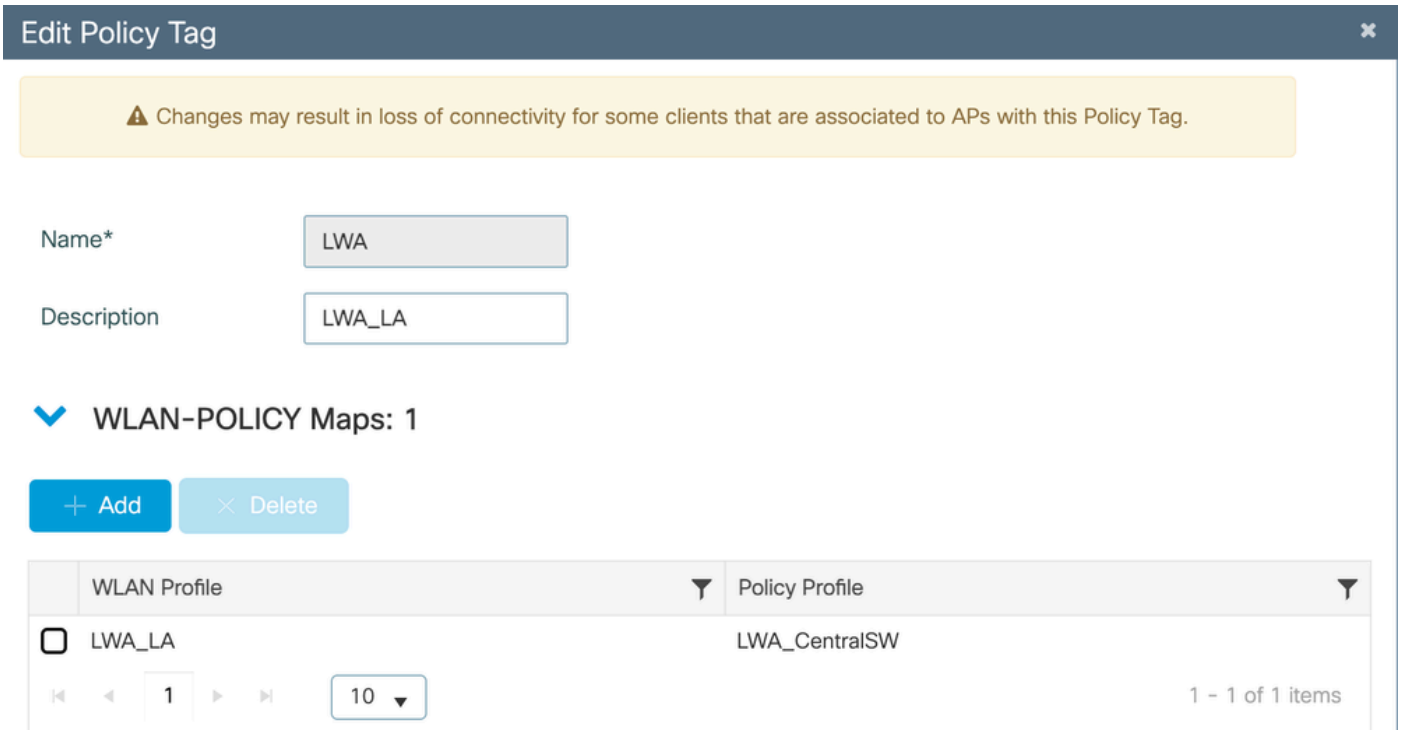


On the **Access Policies** tab, select the VLAN from where the Clients/Supplicants to request an IP.



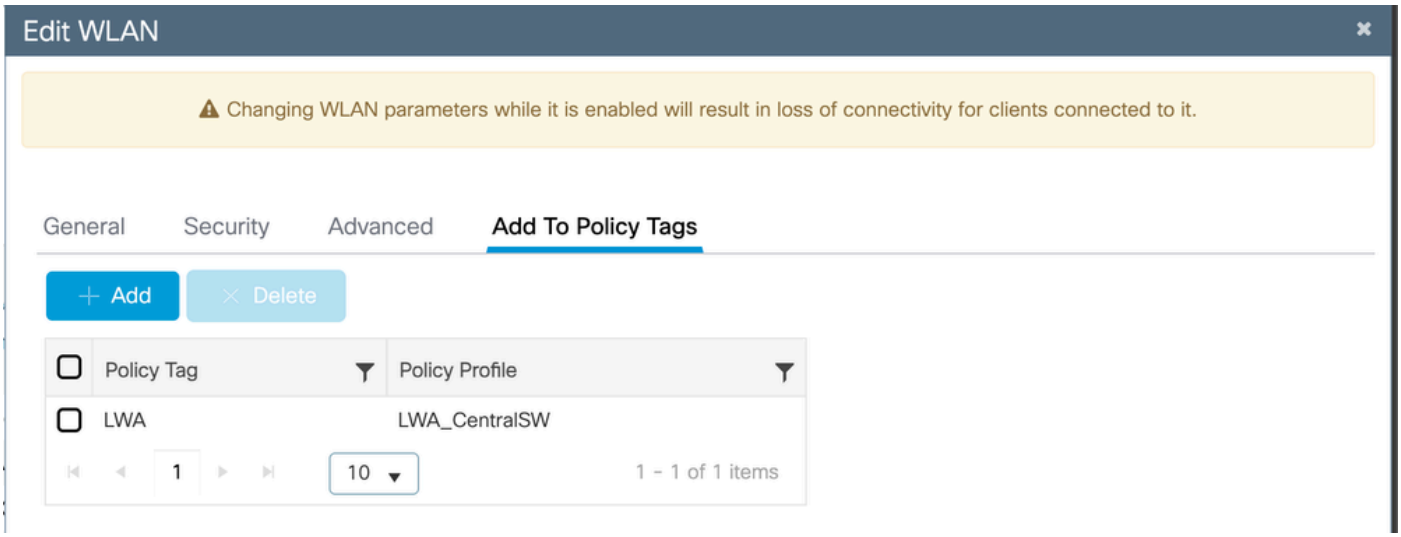
Create a Policy Tag

For this configuration guide, we created a custom policy tag named LWA.



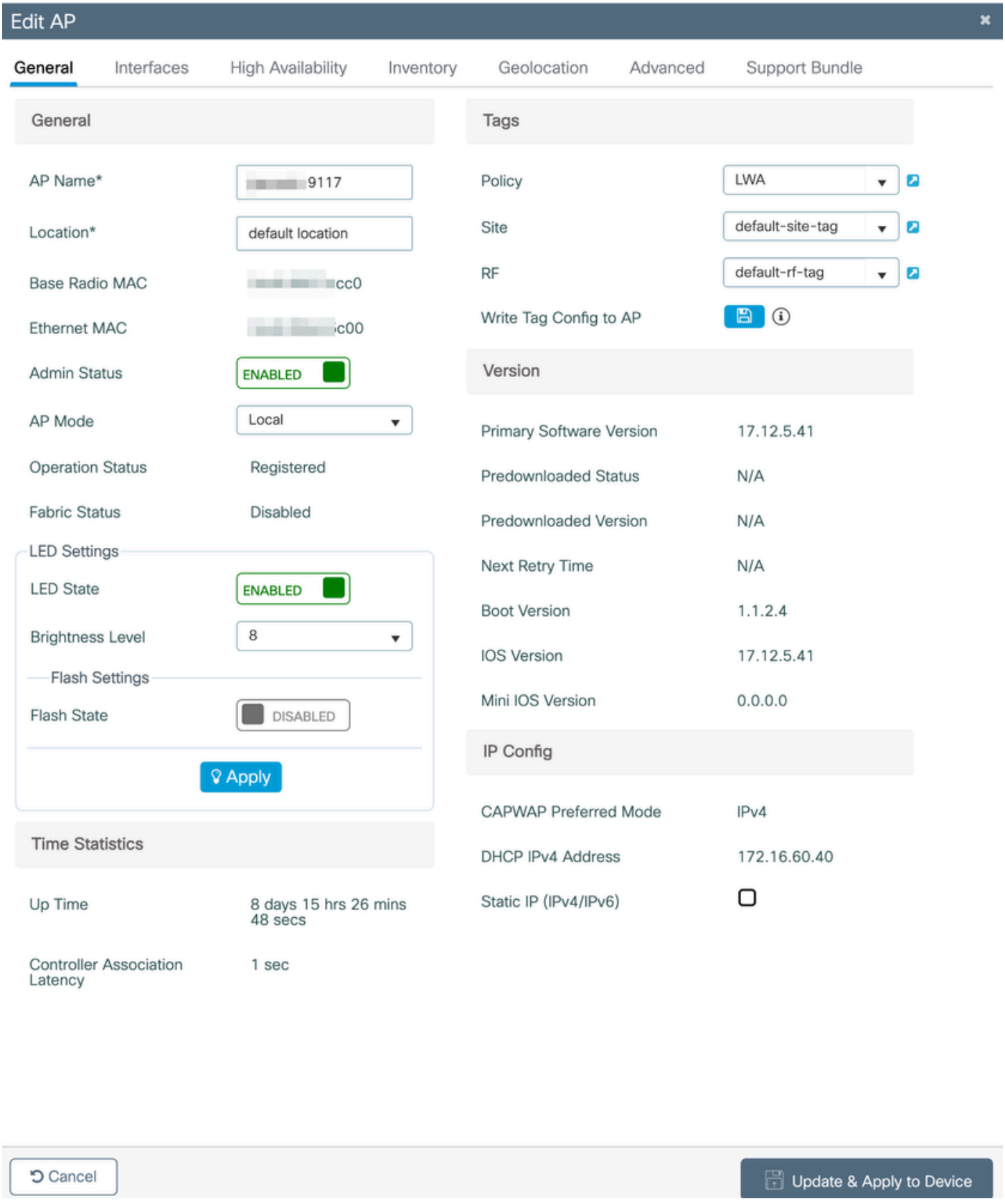
Associate the WLAN and Policy Profile

In order to link the switching policies from the Policy Profile and the WLAN, navigate to **Configuration > Tags & Profiles > WLANs**, select the WLAN Profile, click **Add to Policy Tags**.



Assign a Policy Tag to an AP

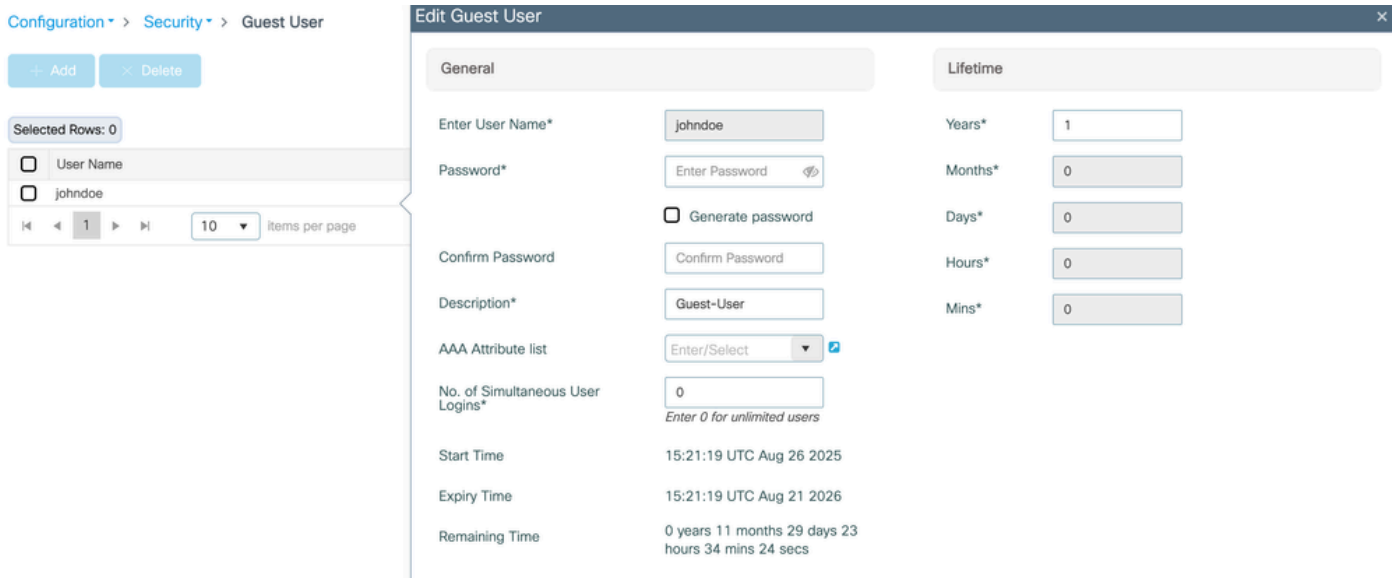
In order to tag the AP with the Policy Tag created, navigate to **Configuration > Wireless > Access Points,** select the AP and on the General tab, right side there are the tags used by the AP.



Create Guest User-Name

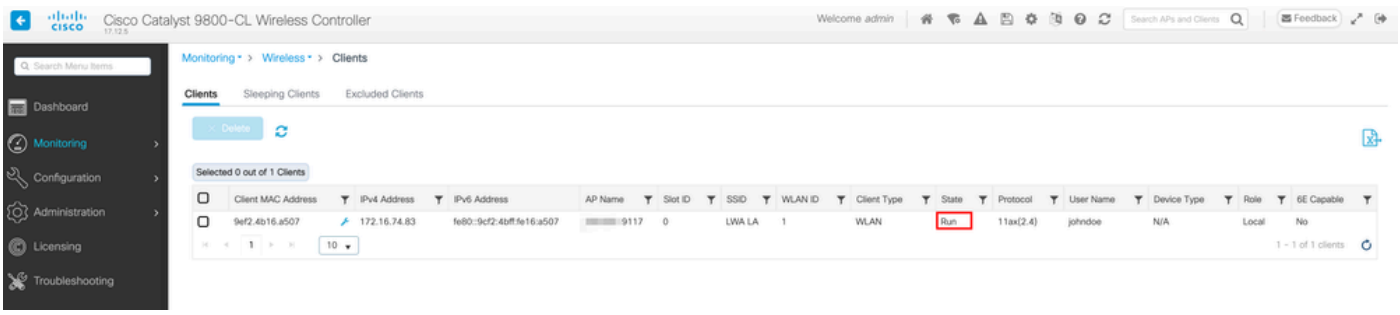
If you selected the webauth type on the Parameter Map, a Guest User-Name is needed, to create it navigate to **Configuration > Security > Guest User.**

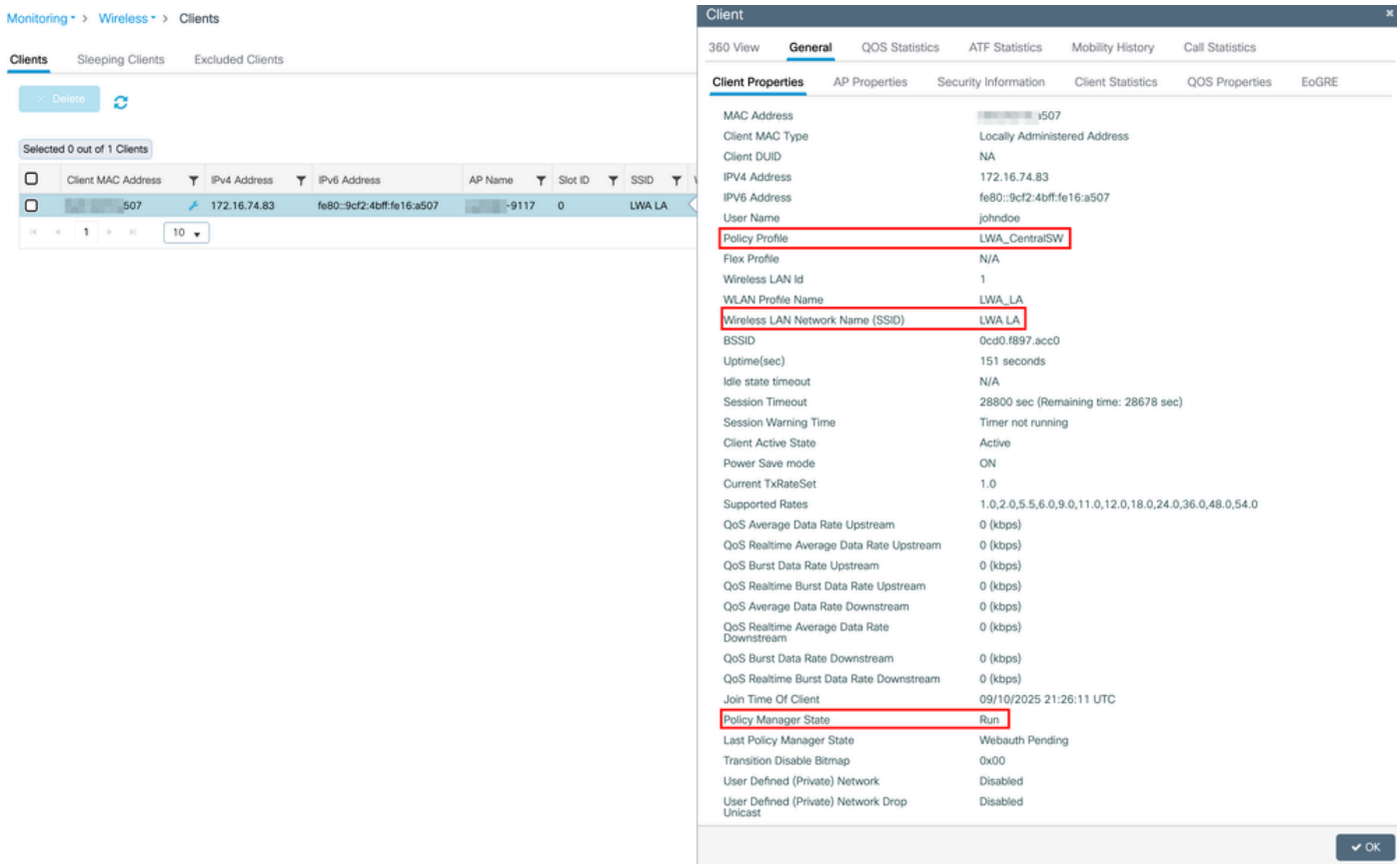
The maximum lifetime of the user is 1 year. You can specify otherwise with the available options.



Verify

Via GUI





Via CLI

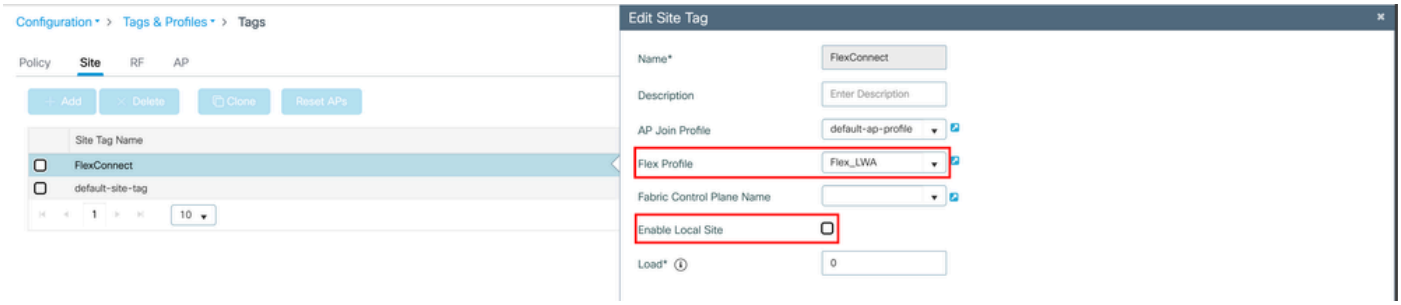
```
9800WLC>enable
9800WLC#show wireless client summary
Number of Clients: 1
MAC Address      AP Name       Type ID State Protocol  Method    Role
-----------------------------------------------------------------------------------------------------
9ef2.4b16.a507   xxxxx-9117 WLAN 1  Run   11ax(2.4) Web Auth  Local
9800WLC#show wireless client mac-address <aaaa.bbbb.cccc> detail
Client MAC Address : 9ef2.4b16.a507
Client MAC Type : Locally Administered Address
Client DUID: NA
Client IPv4 Address : 172.16.74.83
Client IPv6 Addresses : fe80::9cf2:4bff:fe16:a507
Client Username : johndoe
AP MAC Address : 0cd0.f897.acc0
AP Name: xxxxx-9117
AP slot : 0
Client State : Associated
Policy Profile : LWA_CentralSW
Flex Profile : N/A
Wireless LAN Id: 1
WLAN Profile Name: LWA_LA
Wireless LAN Network Name (SSID): LWA LA
BSSID : 0cd0.f897.acc0
Connected For : 392 seconds
Protocol : 802.11ax - 2.4 GHz
Channel : 11
Client IIF-ID : 0xa0000002
Association Id : 1
Authentication Algorithm : Open System
Idle state timeout : N/A
Session Timeout : 28800 sec (Remaining time: 28455 sec)
Session Warning Time : Timer not running
Input Policy Name : None
Input Policy State : None
Input Policy Source : None
Output Policy Name : None
Output Policy State : None
Output Policy Source : None
WMM Support : Enabled
U-APSD Support : Disabled
Fastlane Support : Disabled
Client Active State : Active
Power Save : ON
Current Rate : m0 ss2
Supported Rates : 1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0
AAA QoS Rate Limit Parameters:
QoS Average Data Rate Upstream : 0 (kbps)
QoS Realtime Average Data Rate Upstream : 0 (kbps)
QoS Burst Data Rate Upstream : 0 (kbps)
QoS Realtime Burst Data Rate Upstream : 0 (kbps)
QoS Average Data Rate Downstream : 0 (kbps)
QoS Realtime Average Data Rate Downstream : 0 (kbps)
QoS Burst Data Rate Downstream : 0 (kbps)
QoS Realtime Burst Data Rate Downstream : 0 (kbps)
Mobility:
Move Count : 0
Mobility Role : Local
Mobility Roam Type : None
```

```
Mobility Complete Timestamp : 09/10/2025 21:41:11 UTC
Client Join Time:
Join Time Of Client : 09/10/2025 21:41:11 UTC
Client State Servers : None
Client ACLs : None
Policy Manager State: Run
Last Policy Manager State : Webauth Pending
Client Entry Create Time : 392 seconds
Policy Type : N/A
Encryption Cipher : None
Transition Disable Bitmap : 0x00
User Defined (Private) Network : Disabled
User Defined (Private) Network Drop Unicast : Disabled
Encrypted Traffic Analytics : No
Protected Management Frame - 802.11w : No
EAP Type : Not Applicable
VLAN Override after Webauth : No
VLAN : 2667
Multicast VLAN : 0
VRF Name : N/A
WiFi Direct Capabilities:
WiFi Direct Capable : No
Central NAT : DISABLED
Session Manager:
Point of Attachment : capwap_90400005
IIF ID : 0x90400005
Authorized : TRUE
Session timeout : 28800
Common Session ID: 044A10AC0000000F359351E3
Acct Session ID : 0x00000000
Auth Method Status List
Method : Web Auth
Webauth State : Authz
Webauth Method : Webauth
Local Policies:
Service Template : IP-Adm-V4-LOGOUT-ACL (priority 100)
URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL
Service Template : wlan_svc_LWA_CentralSW_local (priority 254)
VLAN : 2667
Absolute-Timer : 28800
Server Policies:
Resultant Policies:
URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL
VLAN Name : xxxxx
VLAN : 2667
Absolute-Timer : 28800
DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
Client Capabilities
CF Pollable : Not implemented
CF Poll Request : Not implemented
Short Preamble : Not implemented
PBCC : Not implemented
Channel Agility : Not implemented
Listen Interval : 0
Fast BSS Transition Details :
Reassociation Timeout : 0
11v BSS Transition : Implemented
11v DMS Capable : No
QoS Map Capable : Yes
FlexConnect Data Switching : N/A
FlexConnect Dhcp Status : N/A
```

```
FlexConnect Authentication : N/A
Client Statistics:
Number of Bytes Received from Client : 111696
Number of Bytes Sent to Client : 62671
Number of Packets Received from Client : 529
Number of Packets Sent to Client : 268
Number of Data Retries : 136
Number of RTS Retries : 0
Number of Tx Total Dropped Packets : 1
Number of Duplicate Received Packets : 0
Number of Decrypt Failed Packets : 0
Number of Mic Failured Packets : 0
Number of Mic Missing Packets : 0
Number of Policy Errors : 0
Radio Signal Strength Indicator : -61 dBm
Signal to Noise Ratio : 4 dB
Fabric status : Disabled
Radio Measurement Enabled Capabilities
Capabilities: Link Measurement, Neighbor Report, Repeated Measurements, Passive Beacon Measurement, Act
Client Scan Report Time : Timer not running
Client Scan Reports
Assisted Roaming Neighbor List
Nearby AP Statistics:
EoGRE : Pending Classification
Max Client Protocol Capability: Wi-Fi6 (802.11ax)
WiFi to Cellular Steering : Not implemented
Cellular Capability : N/A
Advanced Scheduling Requests Details:
Apple Specific Requests(ASR) Capabilities/Statistics:
Regular ASR support: DISABLED
```

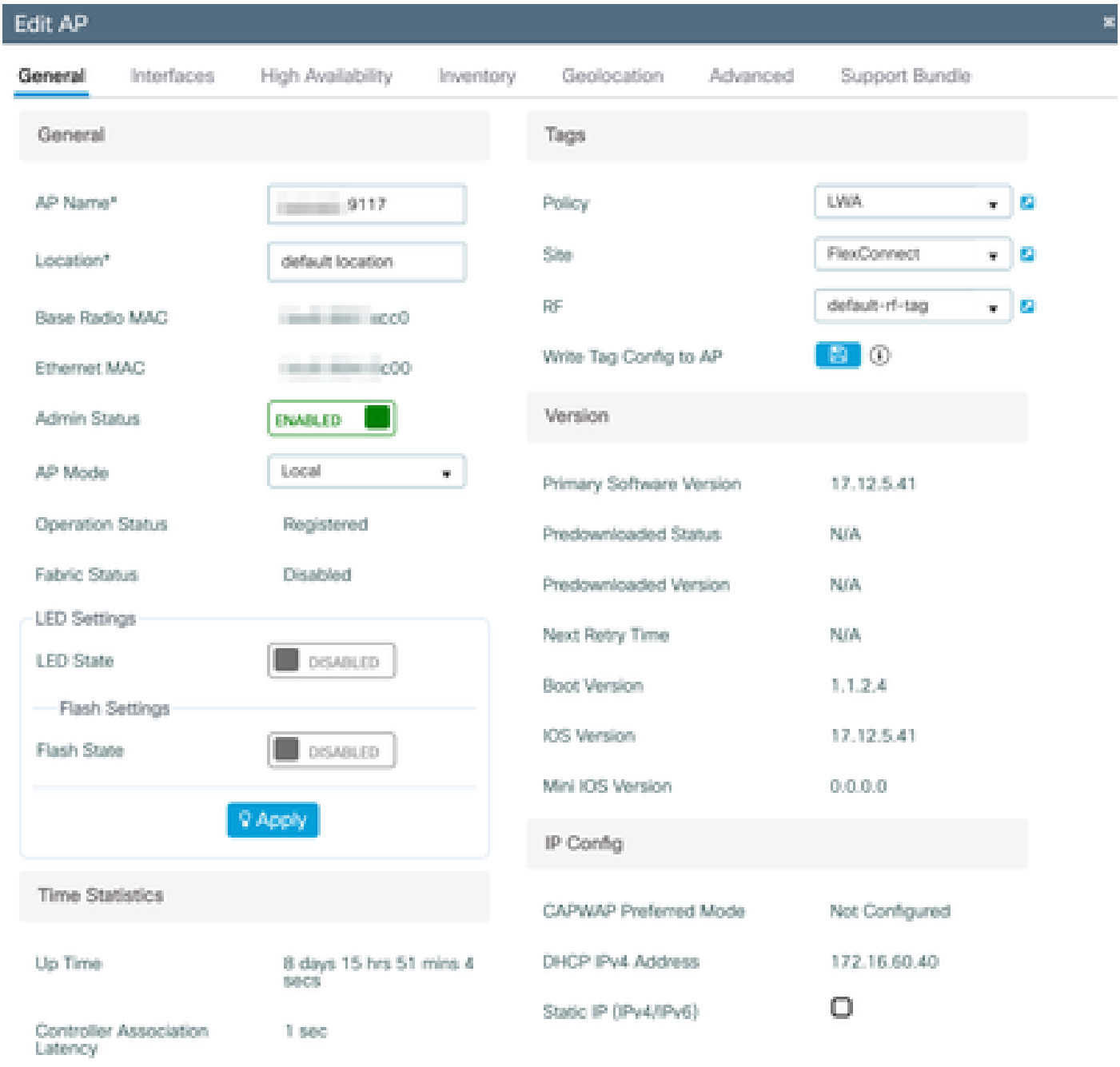
Local Web Authentication on FlexConnect Local Switching

For this scenario, the AP is assumed to be in FlexConnect Mode. For an AP to be in FlexConnect Mode, you need a Flex Profile associated on the SiteTag, where the Enable Local Site checkbox is disabled. This Site Tag uses the default-ap-join and a custom flex profile name Flex_LWA:



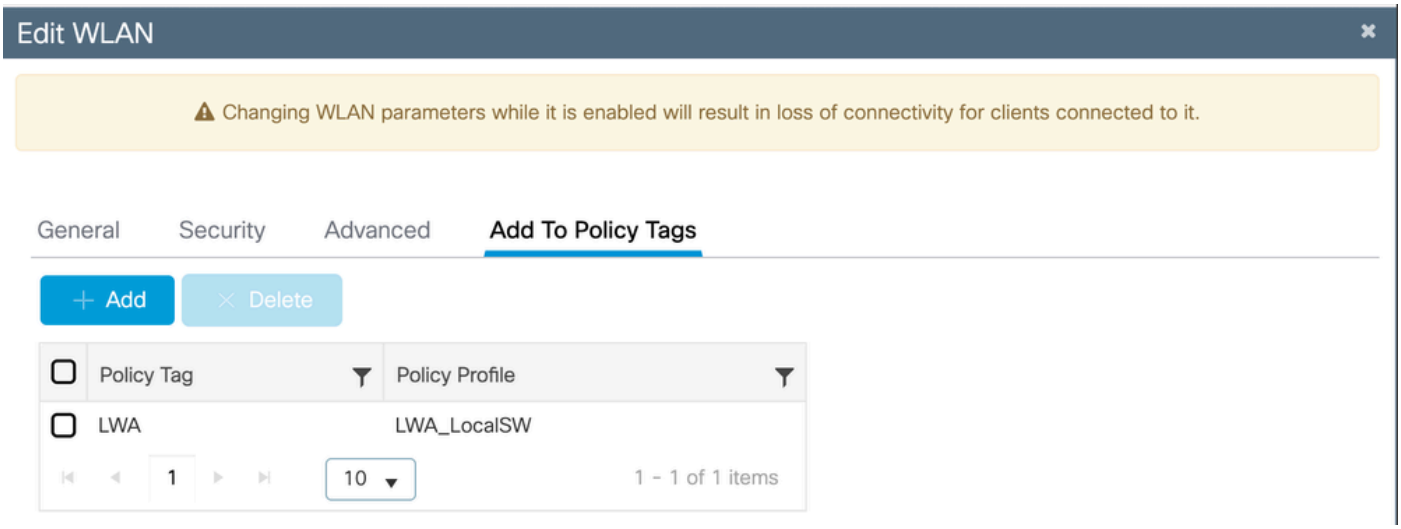
Assign a Policy Tag to an AP

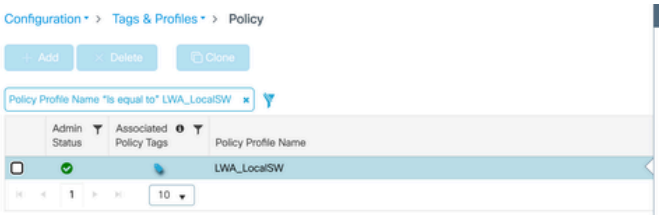
Navigate to **Configuration > Wireless > Access Points**, select the AP and on the General tab, right side there are the tags used by the AP.

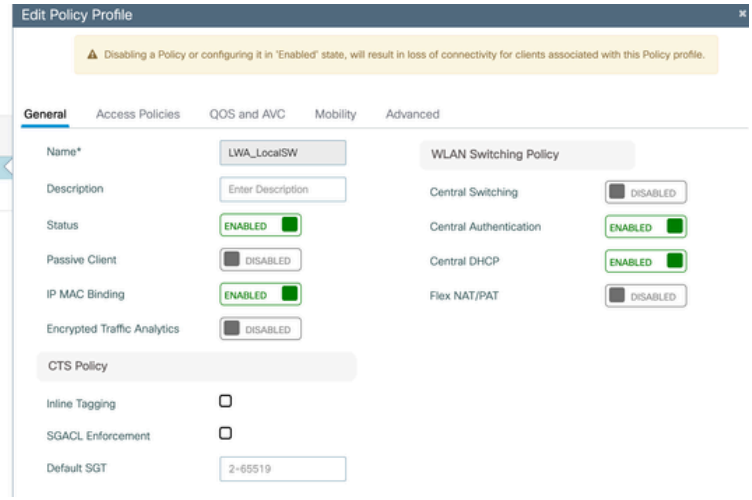

Edit AP
General
Interfaces
High Availability
Inventory
Geolocation
Advanced
Support Bundle
General
AP Name*
9117
Location*
default location
Base Radio MAC
Ethernet MAC
Admin Status
ENABLED
AP Mode
Local
Operation Status
Registered
Fabric Status
Disabled
LED Settings
LED State
DISABLED
Flash Settings
Flash State
DISABLED
Apply
Time Statistics
Up Time
8 days 15 hrs 51 mins 4 secs
Controller Association Latency
1 sec
Tags
Policy
LWA
Site
FlexConnect
RF
default-rf-tag
Write Tag Config to AP
Version
Primary Software Version
17.12.5.41
Predownloaded Status
N/A
Predownloaded Version
N/A
Next Retry Time
N/A
Boot Version
1.1.2.4
IOS Version
17.12.5.41
Mini IOS Version
0.0.0.0
IP Config
CAPWAP Preferred Mode
Not Configured
DHCP IPv4 Address
172.16.60.40
Static IP (IPv4/IPv6)

Warning: Changing the tags cause the AP to disjoin the WLC.

The Policy Profile associated with the WLAN is Local Switching







Verify

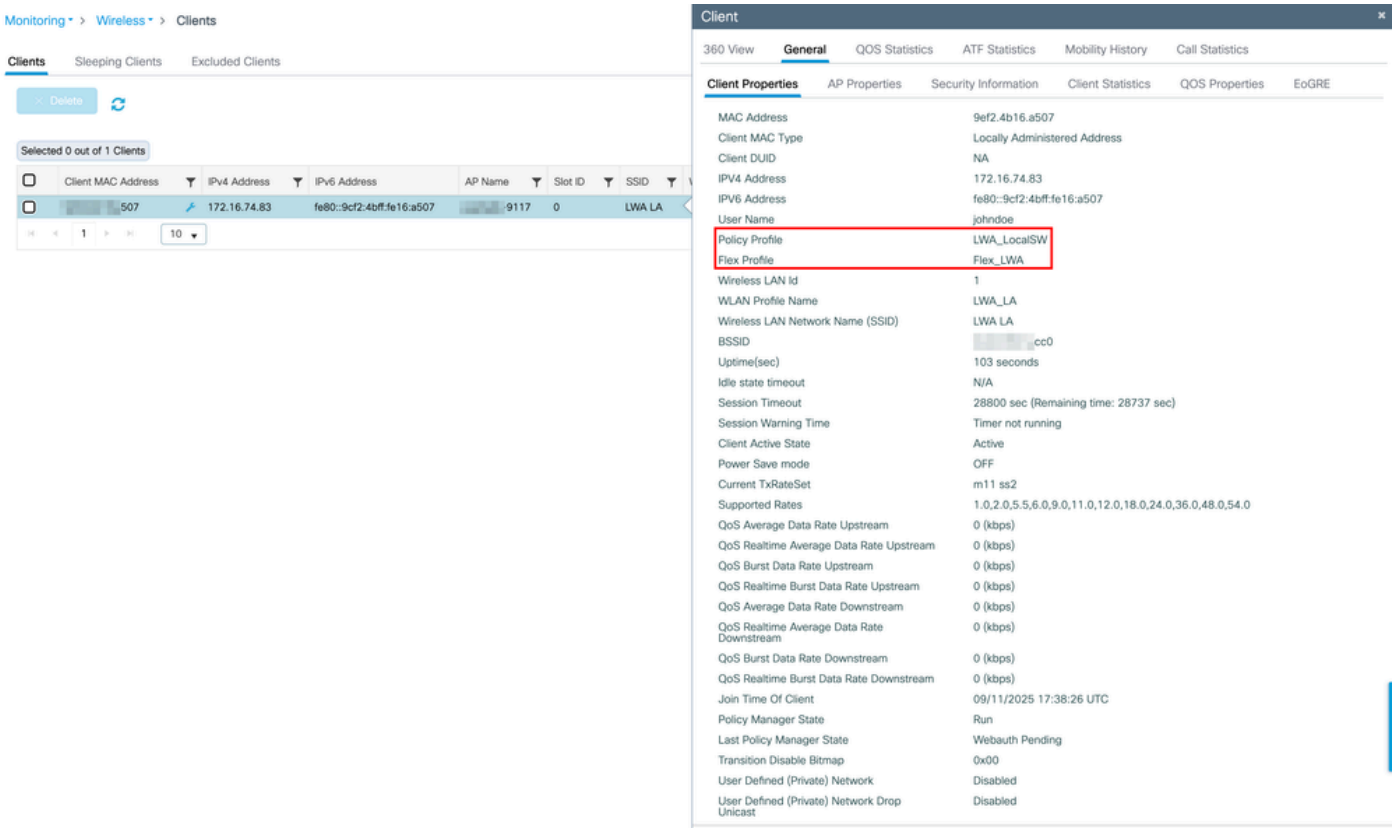
```
9800WLC>enable
9800WLC#show wireless client summary
Number of Clients: 1
MAC Address      AP Name         Type ID  State Protocol  Method    Role
-----------------------------------------------------------------------------------------------
9ef2.4b16.a507 xxxxx-9117 WLAN 1 Run 11ax(2.4) Web Auth Local

9800WLC#show wireless client mac-address <aaaa.bbbb.cccc> detail
Client MAC Address :<aaaa.bbbb.cccc>
Client MAC Type : Locally Administered Address
Client DUID: NA
Client IPv4 Address : 172.16.74.83
Client IPv6 Addresses : fe80::9cf2:4bff:fe16:a507
Client Username : johndoe
AP MAC Address : xxxx.xxxx.xcc0
AP Name: xxxxxx-9117
AP slot : 0
Client State : Associated
Policy Profile : LWA_LocalSW
Flex Profile : Flex_LWA
Wireless LAN Id: 1
WLAN Profile Name: LWA_LA
Wireless LAN Network Name (SSID): LWA LA
```

```
BSSID : 0cd0.f897.acc0
Connected For : 315 seconds
Protocol : 802.11ax - 2.4 GHz
Channel : 6
Client IIF-ID : 0xa0000004
Association Id : 1
Authentication Algorithm : Open System
Idle state timeout : N/A
Session Timeout : 28800 sec (Remaining time: 28525 sec)
Session Warning Time : Timer not running
Input Policy Name : None
Input Policy State : None
Input Policy Source : None
Output Policy Name : None
Output Policy State : None
Output Policy Source : None
WMM Support : Enabled
U-APSD Support : Disabled
Fastlane Support : Disabled
Client Active State : Active
Power Save : ON
Current Rate : m11 ss2
Supported Rates : 1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0
AAA QoS Rate Limit Parameters:
 QoS Average Data Rate Upstream : 0 (kbps)
QoS Realtime Average Data Rate Upstream : 0 (kbps)
QoS Burst Data Rate Upstream : 0 (kbps)
QoS Realtime Burst Data Rate Upstream : 0 (kbps)
QoS Average Data Rate Downstream : 0 (kbps)
QoS Realtime Average Data Rate Downstream : 0 (kbps)
QoS Burst Data Rate Downstream : 0 (kbps)
QoS Realtime Burst Data Rate Downstream : 0 (kbps)
Mobility:
Move Count : 0
Mobility Role : Local
Mobility Roam Type : None
Mobility Complete Timestamp : 09/11/2025 17:38:26 UTC
Client Join Time:
Join Time Of Client : 09/11/2025 17:38:26 UTC
Client State Servers : None
Client ACLs : None
Policy Manager State: Run
Last Policy Manager State : Webauth Pending
Client Entry Create Time : 315 seconds
Policy Type : N/A
Encryption Cipher : None
Transition Disable Bitmap : 0x00
User Defined (Private) Network : Disabled
User Defined (Private) Network Drop Unicast : Disabled
Encrypted Traffic Analytics : No
Protected Management Frame - 802.11w : No
EAP Type : Not Applicable
VLAN Override after Webauth : No
VLAN : 2667
Multicast VLAN : 0
VRF Name : N/A
WiFi Direct Capabilities:
WiFi Direct Capable : No
Central NAT : DISABLED
Session Manager:
Point of Attachment : capwap_90400005
IIF ID : 0x90400005
```

```
Authorized : TRUE
Session timeout : 28800
Common Session ID: 044A10AC0000002A39DB6F52
Acct Session ID : 0x00000000
Auth Method Status List
Method : Web Auth
Webauth State : Authz
Webauth Method : Webauth
Local Policies:
Service Template : IP-Adm-V4-LOGOUT-ACL (priority 100)
URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL
Service Template : wlan_svc_LWA_LocalSW (priority 254)
VLAN : 2667
Absolute-Timer : 28800
Server Policies:
Resultant Policies:
URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL
VLAN Name : xxxxx
VLAN : 2667
Absolute-Timer : 28800
DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
Client Capabilities
CF Pollable : Not implemented
CF Poll Request : Not implemented
Short Preamble : Not implemented
PBCC : Not implemented
Channel Agility : Not implemented
Listen Interval : 0
Fast BSS Transition Details :
Reassociation Timeout : 0
11v BSS Transition : Implemented
11v DMS Capable : No
QoS Map Capable : Yes
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Central
FlexConnect Authentication : Central
Client Statistics:
Number of Bytes Received from Client : 295564
Number of Bytes Sent to Client : 90146
Number of Packets Received from Client : 1890
Number of Packets Sent to Client : 351
Number of Data Retries : 96
Number of RTS Retries : 0
Number of Tx Total Dropped Packets : 0
Number of Duplicate Received Packets : 0
Number of Decrypt Failed Packets : 0
Number of Mic Failured Packets : 0
Number of Mic Missing Packets : 0
Number of Policy Errors : 0
Radio Signal Strength Indicator : -34 dBm
Signal to Noise Ratio : 31 dB
Fabric status : Disabled
Radio Measurement Enabled Capabilities
Capabilities: Link Measurement, Neighbor Report, Repeated Measurements, Passive Beacon Measurement, Act
Client Scan Report Time : Timer not running
Client Scan Reports
Assisted Roaming Neighbor List
Nearby AP Statistics:
EoGRE : Pending Classification
Max Client Protocol Capability: Wi-Fi6 (802.11ax)
WiFi to Cellular Steering : Not implemented
```

```
Cellular Capability : N/A
Advanced Scheduling Requests Details:
Apple Specific Requests(ASR) Capabilities/Statistics:
Regular ASR support: DISABLED
```



Troubleshoot

The "Web Auth Pending" status indicates that the client has associated with the access point but has not yet completed the web authentication process. During this state, the controller intercepts the client HTTP traffic and redirects it to a web authentication portal for user login or acceptance of terms. The client remains in this state until successful web authentication is completed, after which the client policy manager state transitions to "Run" and full network access is granted.

In order to see the flow of the client connection visually, verify LWA Flow from Configure Local Web Authentication with External Authentication.

The stages the Client Undergoes from the Client Perspective are depicted on Troubleshoot Common Issues with LWA on 9800 WLCs.

- Technical Support & Documentation - Cisco Systems