

Configure Local Web Authentication with Local Authentication

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Parameter Map](#)

[Database for Authentication](#)

[Configure](#)

[Local Web Authentication with Local Authentication on the CLI](#)

[Method Lists for Local Authentication](#)

[Parameter Maps](#)

[WLAN Security Parameters](#)

[Create a Policy Profile](#)

[Create a Policy Tag](#)

[Assign a Policy Tag to an AP](#)

[Create Guest Username](#)

[Local Web Authentication with Local Authentication via WebUI](#)

[Verify](#)

[Local Web Authentication on FlexConnect Local Switching](#)

[Verify](#)

[Troubleshoot](#)

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.

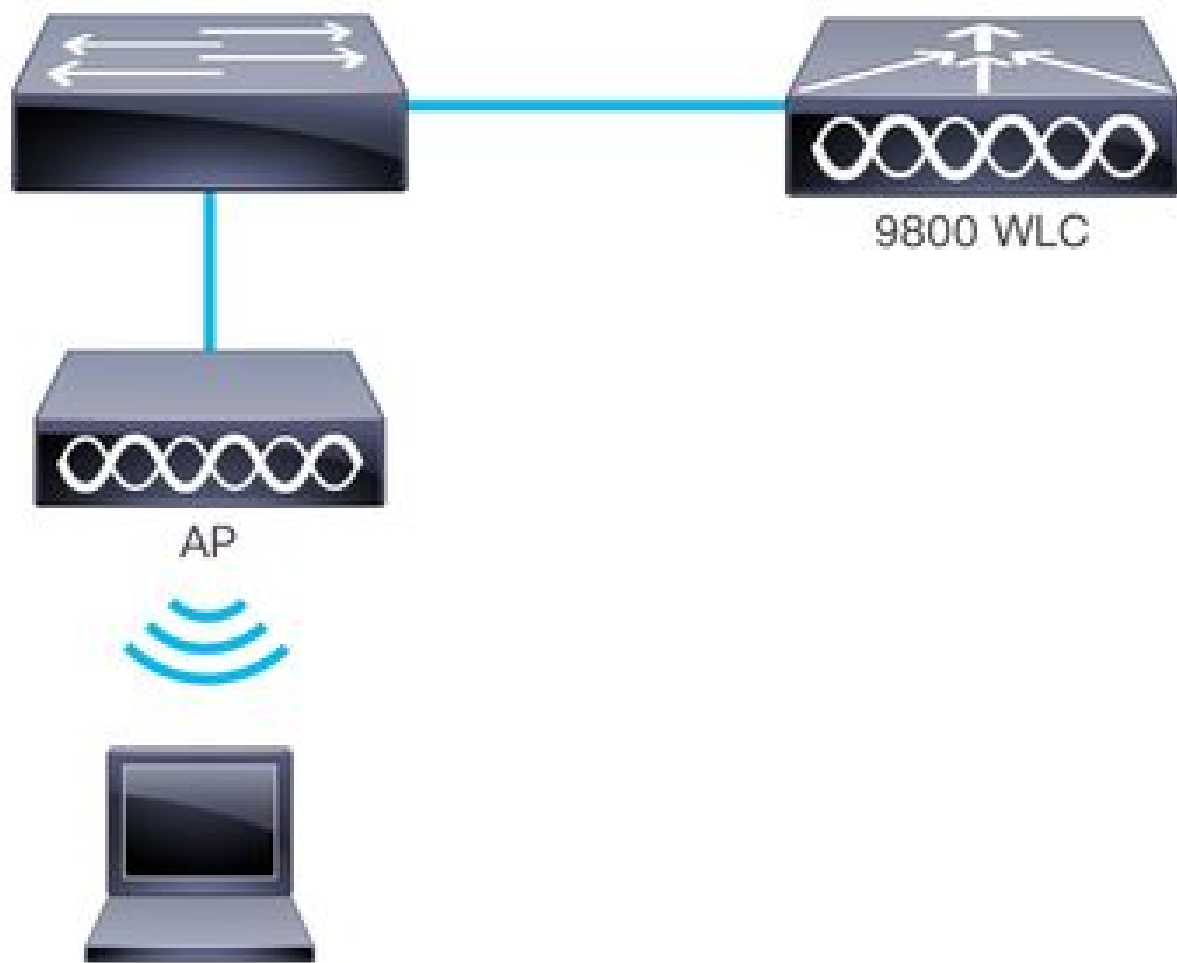
The Wireless LAN Controller comes with a default global parameter map, but administrators have the option to create custom parameter maps to customize the Web Authentication behavior according to specific needs.

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:

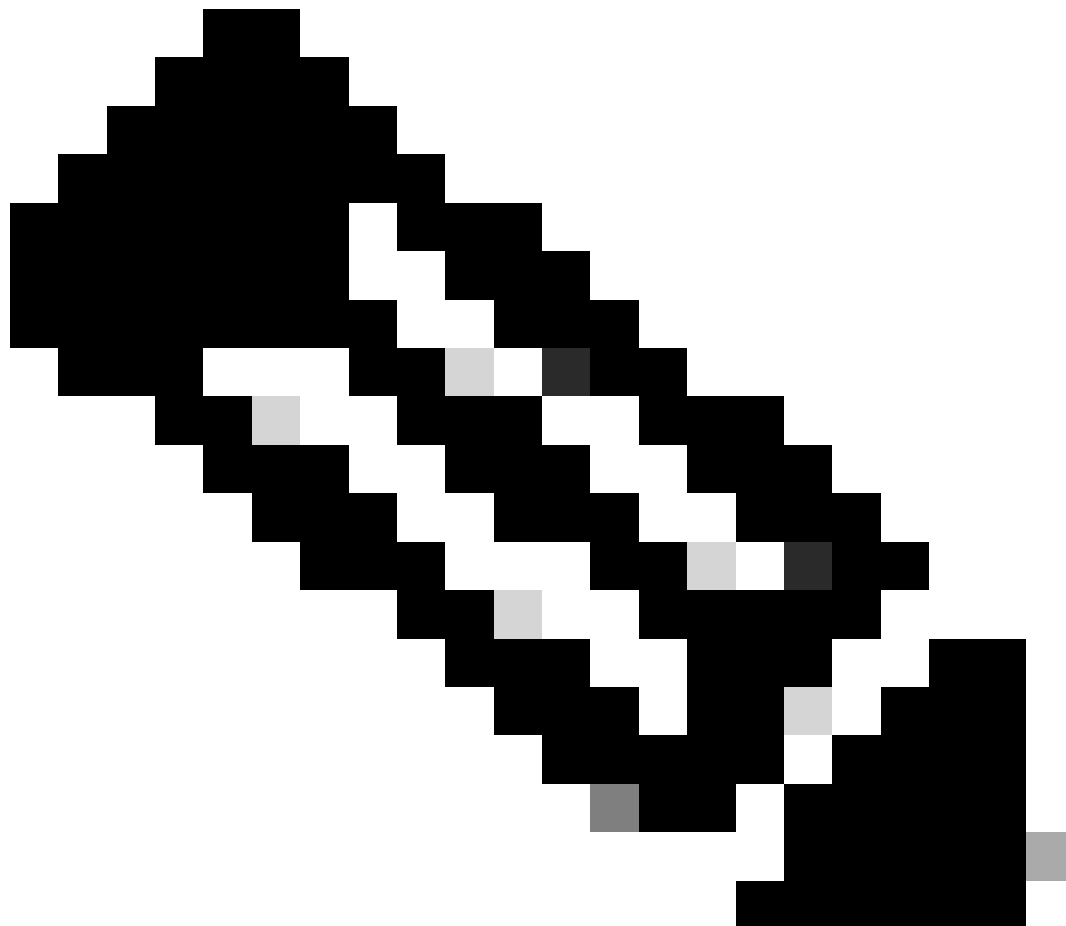
- **Client/Supplicant:** Initiates connection request to the WLAN, later to the DHCP and DNS servers, and responds to communications from the WLC.
- **Access Point:** Connected to a switch, it broadcasts the guest WLAN and provides wireless connectivity to guest devices. It permits DHCP and DNS traffic 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

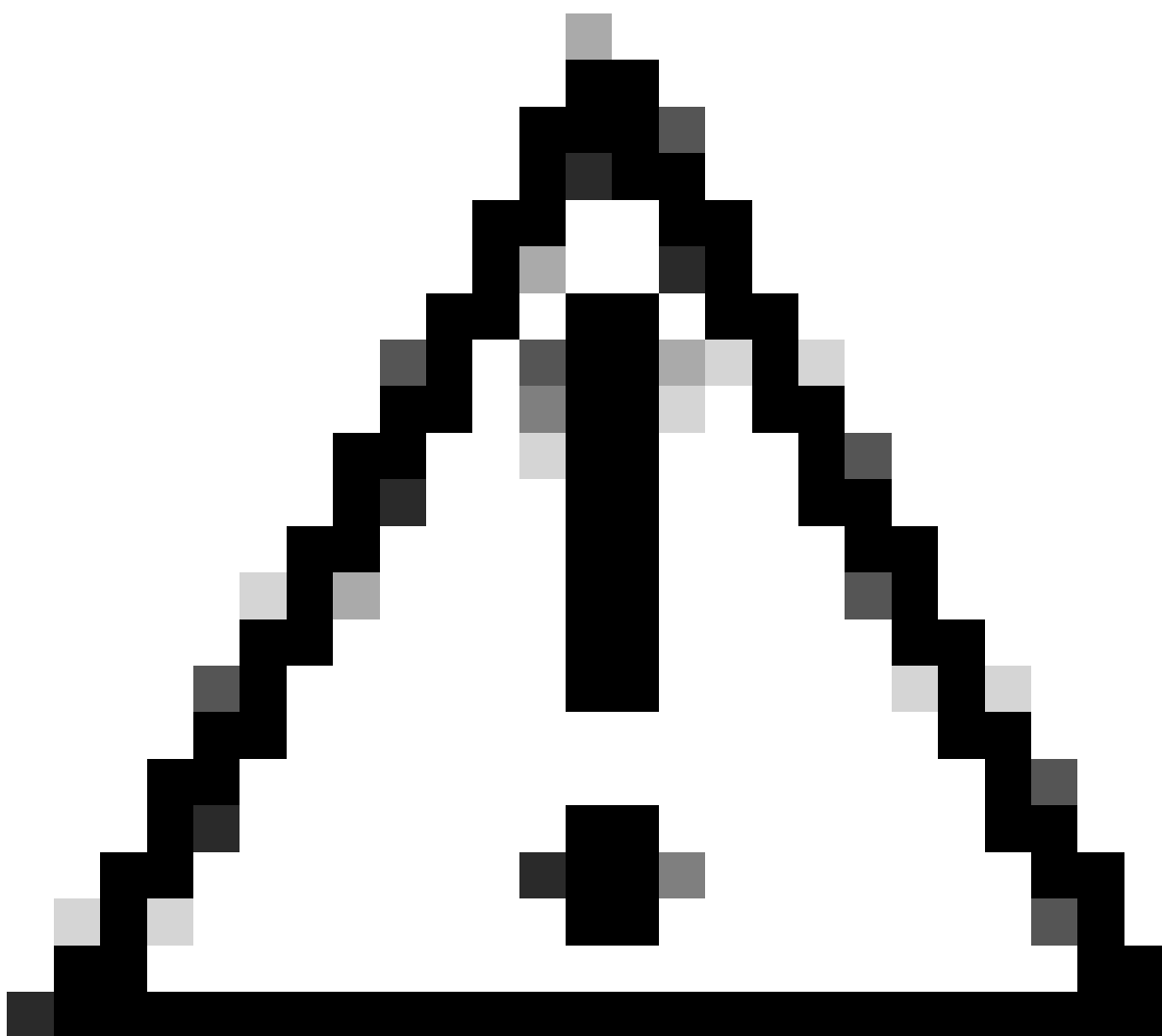
```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#aaa new-model
9800WLC(config)#aaa authentication login LWA_AUTHENTICATION local
9800WLC(config)#aaa authorization network default local
9800WLC(config)#end
```



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

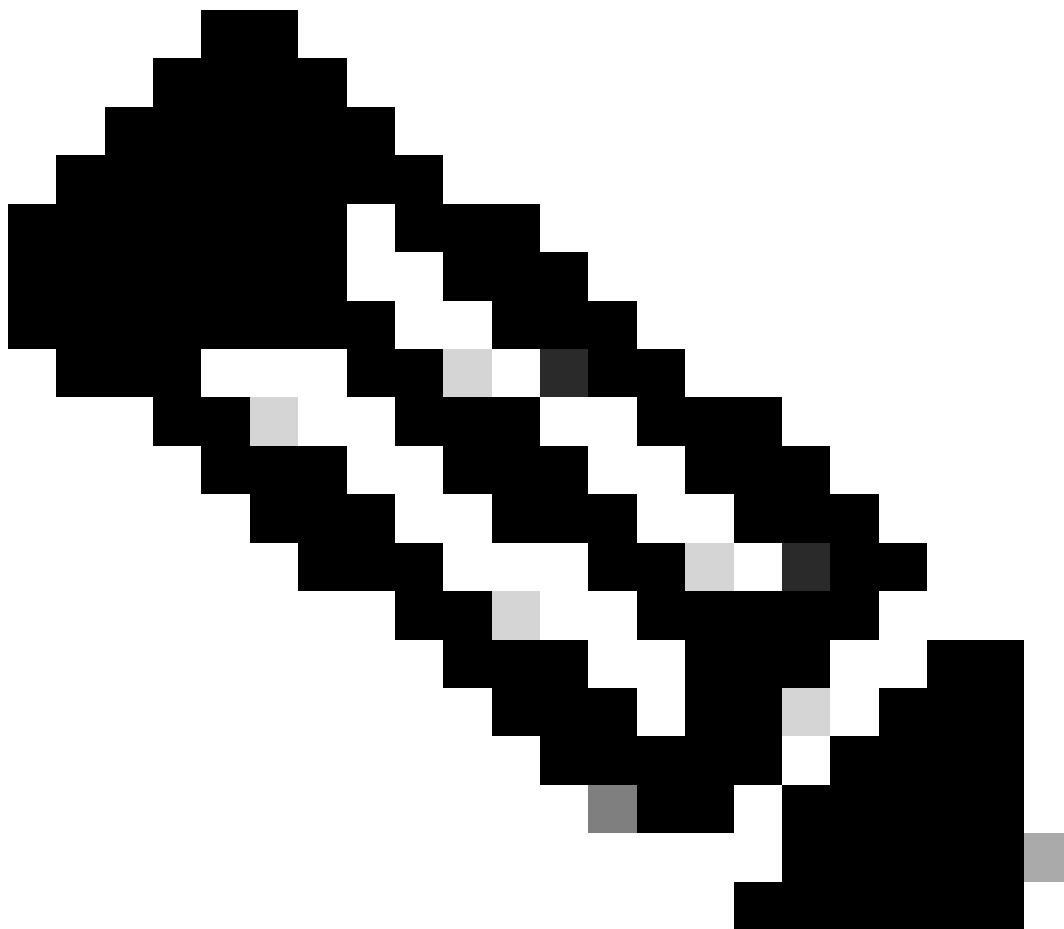
```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#wireless tag policy <POLICY_TAG>
9800WLC(config-policy-tag)#wlan LWA_LA policy <POLICY_PROFILE>
9800WLC(config-policy-tag)# end
```

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 0
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.

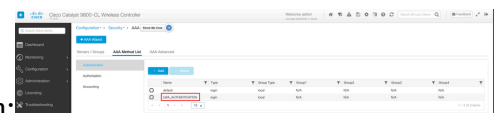
Local Web Authentication with Local Authentication via WebUI

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.

The screenshot shows the Cisco Catalyst 9800-CL WebUI configuration page for AAA Method List. The breadcrumb navigation is Configuration > Security > AAA. The page has tabs for Servers / Groups, AAA Method List (selected), and AAA Advanced. A sidebar on the left shows Authentication (selected), Authorization, and Accounting. The main area has a table with columns: Name, Type, Group Type, Group1, and Group2. The table contains one entry: default, login, local, N/A, N/A. Below the table is a 'Quick Setup: AAA Authentication' dialog box. The dialog has fields for Method List Name* (LWA-AUTHENTICATION), Type* (login), and Group Type (local). It also has sections for Available Server Groups (radius, ldap, tacacs+, AAA-group) and Assigned Server Groups. At the bottom of the dialog are 'Cancel' and 'Apply to Device' buttons.

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

Configuration > Security > AAA [Show Me How](#)

[+ AAA Wizard](#)

Servers / Groups **AAA Method List** AAA Advanced

Authentication

Authorization

Accounting

[+ Add](#) [- Delete](#)

Name	Type	Group Type	Group1	Group2
☐ default	exec	local	N/A	N/A

Quick Setup: AAA Authorization

Method List Name*

Type* ⓘ

Group Type ⓘ

Authenticated ☐

Available Server Groups

- radius
- ldap
- tacacs+
- AAA-group

Assigned Server Groups

[Cancel](#) [Apply to Device](#)

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

Configuration > Security > AAA

[+ AAA Wizard](#)

Servers / Groups **AAA Method List** AAA Advanced

Authentication

Authorization

Accounting

[+ Add](#) [- Delete](#)

Name	Type	Group Type	Group1	Group2	Group3	Group4
☐ default	exec	local	N/A	N/A	N/A	N/A
☐ default	network	local	N/A	N/A	N/A	N/A

1 10 1 - 2 of 2 items

Parameter Maps

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

Configuration > Security > Web Auth

+ Add - Delete

Selected Rows: 0

Parameter Map Name
☐ global

10 items per page

General

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

Advanced

Virtual IPv4 Address: 192.0.2.1

Trustpoint: TP-self-signed-...

Virtual IPv4 Hostname:

Virtual IPv6 Address: :::::::

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

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 Trustpoint creation [Renew Certificates for WebAuth & WebAdmin on Cisco 9800 WLC | Secure Wireless LAN Controller Setup](#).

Edit Web Auth Parameter



General

Advanced

Parameter-map Name

Maximum HTTP connections

Init-State Timeout(secs)

Type

Captive Bypass Portal ☐

Disable Success Window ☐

Disable Logout Window ☐

Disable Cisco Logo ☐

Sleeping Client Status ☐

Sleeping Client Timeout (minutes)

Virtual IPv4 Address

Trustpoint

Virtual IPv4 Hostname

Virtual IPv6 Address

Web Auth intercept HTTPs ☐

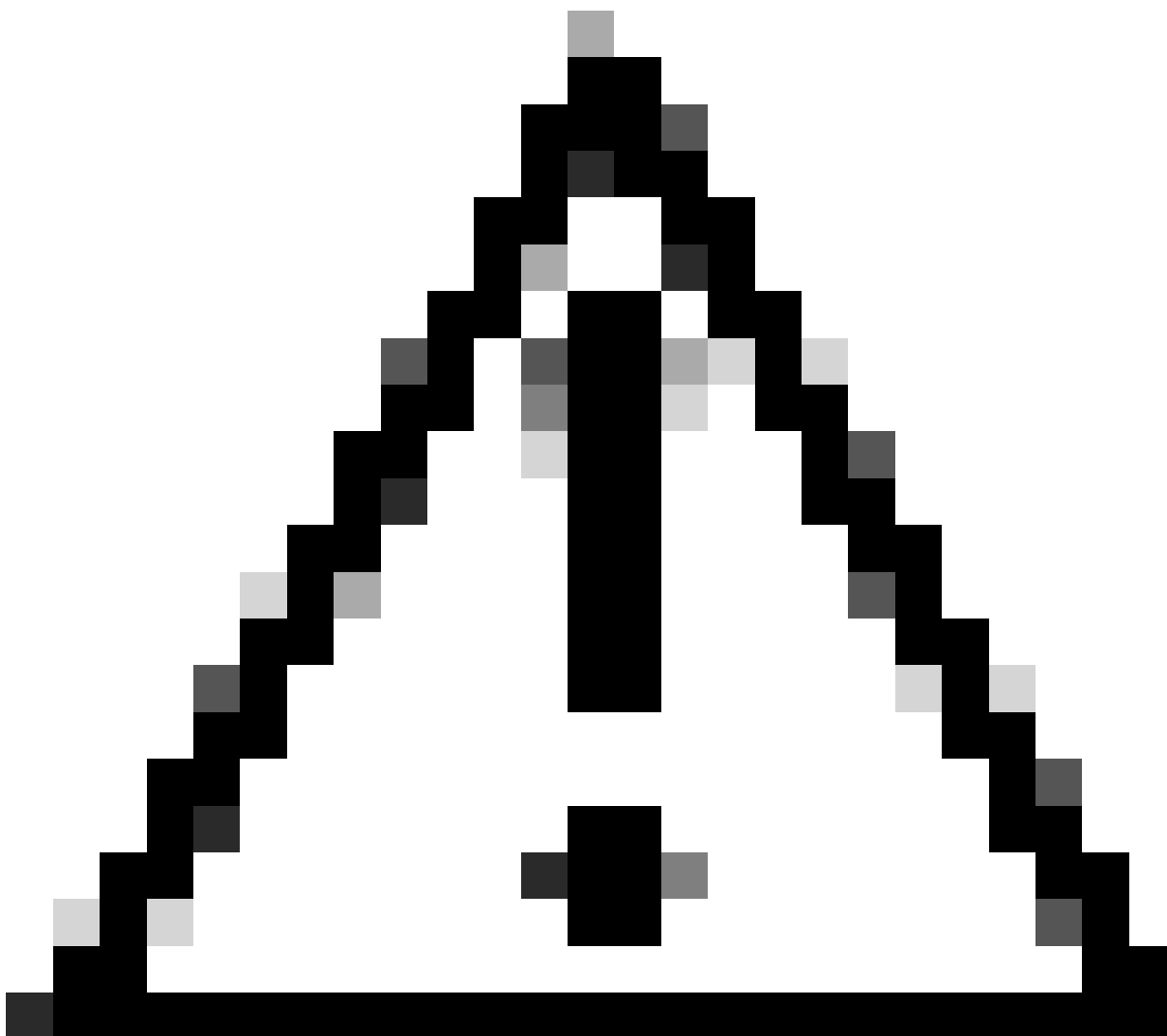
Enable HTTP server for Web Auth ☒

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**.

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General

Security

Advanced

Add To Policy Tags

Profile Name*

LWA_LA

SSID*

LWA LA

WLAN ID*

1

Status

ENABLED ☒

Broadcast SSID

ENABLED ☒

Radio Policy ⓘ

6 GHz

Status

ENABLED ☒☒ Slot 2/3

✖ WPA3 Enabled

✔ Dot11ax Enabled

5 GHz

Status

ENABLED ☒☒ Slot 0☒ Slot 1☒ Slot 2

2.4 GHz

Status

ENABLED ☒☒ Slot 0802.11b/g
Policy

802.11b/g ▼

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

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 AAA

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

☐ WPA + WPA2

☐ WPA2 + WPA3

☐ WPA3

☐ Static WEP

☒ None

MAC Filtering ☐

OWE Transition Mode ☐

Lobby Admin Access ☐

Fast Transition

Status

Over the DS ☐

Reassociation Timeout *

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.

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 **Layer3** AAA

Web Policy ☒

Web Auth Parameter Map

Authentication List

For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device

[<< Hide](#)

On MAC Filter Failure ☐

Splash Web Redirect ☐ DISABLED

Preauthentication ACL

IPv4

IPv6

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**.

Edit 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

Name*

LWA_CentralSW

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

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

Edit 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

Enabled ⓘ

Local Subscriber Policy Name

Search or Select ▼

VLAN

VLAN/VLAN Group

2622 ▼ ⓘ

Multicast VLAN

Enter Multicast VLAN

WLAN ACL

IPv4 ACL

Search or Select ▼

IPv6 ACL

Search or Select ▼

URL Filters ⓘ

Pre Auth

Search or Select ▼

Post Auth

Search or Select ▼

Create a Policy Tag

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

Edit Policy Tag

⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name*

LWA

Description

LWA_LA

✓ WLAN-POLICY Maps: 1

+ Add

× Delete

WLAN Profile

Policy Profile



☐ LWA_LA

LWA_CentralSW

1

10 ▼

1 - 1 of 1 items

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**.

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General

Security

Advanced

Add To Policy Tags

+ Add

× Delete

☐	Policy Tag	Policy Profile
☐	LWA	LWA_CentralSW

1

10

1 - 1 of 1 items

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.

Edit AP

General

Interfaces

High Availability

Inventory

Geolocation

Advanced

Support Bundle

General

AP Name*

Location*

Base Radio MAC

Ethernet MAC

Admin Status ENABLED ☒

AP Mode

Operation Status Registered

Fabric Status Disabled

LED Settings

LED State ENABLED ☒

Brightness Level

Flash Settings

Flash State DISABLED ☐

 Apply

Time Statistics

Up Time 8 days 15 hrs 26 mins 48 secs

Controller Association Latency 1 sec

Tags

Policy

Site

RF

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 IPv4

DHCP IPv4 Address 172.16.60.40

Static IP (IPv4/IPv6) ☐

 Cancel

 Update & Apply to Device

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.

[+ Add](#) [- Delete](#)

Selected Rows: 0

- ☐
- User Name
-
- ☐
- johndoe

1 10 items per page

Edit Guest User

General

Enter User Name*

johndoe

Password*

Enter Password

☐ Generate password

Confirm Password

Confirm Password

Description*

Guest-User

AAA Attribute list

Enter/Select

No. of Simultaneous User Logins*

0

Enter 0 for unlimited users

Start Time

15:21:19 UTC Aug 26 2025

Expiry Time

15:21:19 UTC Aug 21 2026

Remaining Time

0 years 11 months 29 days 23 hours 34 mins 24 secs

Lifetime

Years*

1

Months*

0

Days*

0

Hours*

0

Mins*

0

Verify

Via GUI

Cisco Catalyst 9800-CL Wireless Controller

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Selected 0 out of 1 Clients

Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type	Role	6E Capable
9ef2.4b16.a507	172.16.74.83	fe80::9cf2:4bff:fe16:a507	-9117	0	LWA_LA	1	WLAN	Run	11ax(2.4)	johndoe	N/A	Local	No

1 - 1 of 1 clients

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

[Delete](#) [Refresh](#)

Selected 0 out of 1 Clients

Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID
507	172.16.74.83	fe80::9cf2:4bff:fe16:a507	-9117	0	LWA_LA

Client

360 View General QoS Statistics ATF Statistics Mobility History Call Statistics

Client Properties AP Properties Security Information Client Statistics QoS Properties EoGRE

MAC Address	9ef2.4b16.a507
Client MAC Type	Locally Administered Address
Client DUID	NA
IPv4 Address	172.16.74.83
IPv6 Address	fe80::9cf2:4bff:fe16:a507
User Name	johndoe
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
Uptime(sec)	151 seconds
Idle state timeout	N/A
Session Timeout	28800 sec (Remaining time: 28678 sec)
Session Warning Time	Timer not running
Client Active State	Active
Power Save mode	ON
Current TxRateSet	1.0
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
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)
Join Time Of Client	09/10/2025 21:26:11 UTC
Policy Manager State	Run
Last Policy Manager State	Webauth Pending
Transition Disable Bitmap	0x00
User Defined (Private) Network	Disabled
User Defined (Private) Network Drop Unicast	Disabled

OK

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 Failed 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

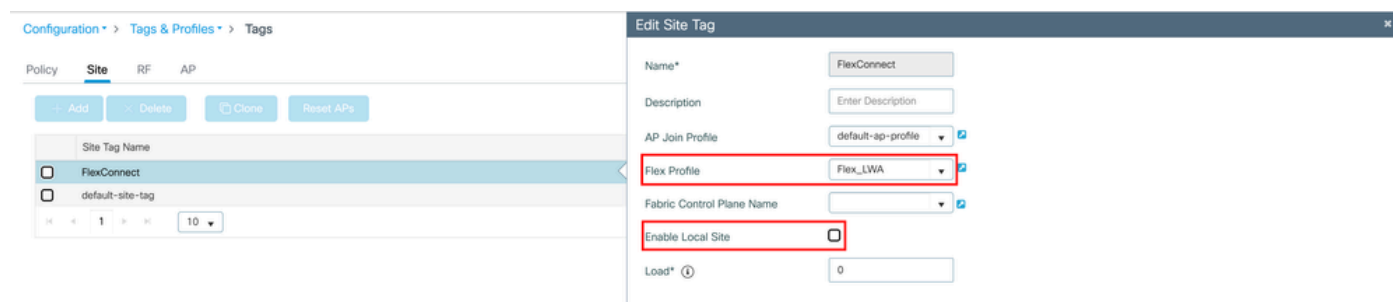
Advanced Scheduling Requests Details:

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.

General

Interfaces

High Availability

Inventory

Geolocation

Advanced

Support Bundle

General

AP Name*

9117

Location*

default location

Base Radio MAC

cc00

Ethernet MAC

cc00

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.

Configuration > Wireless > Access Points

▼ All Access Points

Total APs: 1

Misconfigured APs
Tag : 0 Country Code : 0 LSC Falback : 0 Select an Action ▼

Multiple APs can be configured at once from [Bulk AP Provisioning](#) feature

AP Name	AP Model	Slots	Admin Status	Up Time	IP Address	Base Radio MAC	Ethernet MAC	AP Mode	Power Derate Capable	Operation Status	Configuration Status	Country Code Misconfigured	LSC Falback Misconfigure
9117	C9117AXI-A	2	✓	8 days 15 hrs 54 mins 53 secs	172.16.60.40	cc0	c00	Flex	No	Registered	Healthy	No	No

The Policy Profile associated with the WLAN is Local Switching

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General
Security
Advanced
Add To Policy Tags

+ Add
Delete

☐ Policy Tag
☐ Policy Profile

☐ LWA
LWA_LocalSW

1
10
1 - 1 of 1 items

Configuration > Tags & Profiles > Policy

Add
Delete
Clone

Policy Profile Name "is equal to" LWA_LocalSW

Admin Status	Associated Policy Tags	Policy Profile Name
☒		LWA_LocalSW

1
10

Edit 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

Name*
LWA_LocalSW
WLAN Switching Policy

Description
Enter Description
Central Switching
DISABLED

Status
ENABLED
Central Authentication
ENABLED

Passive Client
DISABLED
Central DHCP
ENABLED

IP MAC Binding
ENABLED
Flex NAT/PAT
DISABLED

Encrypted Traffic Analytics
DISABLED

CTS Policy

Inline Tagging
SGACL Enforcement
Default SGT
2-65519

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 Failed 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

The screenshot displays the Cisco WLC interface for monitoring wireless clients. On the left, a table lists client details, including MAC Address, Client MAC Type, Client DUID, IPv4 Address, IPv6 Address, AP Name, Slot ID, and SSID. The client with MAC address 9e12.4b16.a507 is highlighted. On the right, a detailed view of the client properties is shown, including MAC Address, Client MAC Type, Client DUID, IPv4 Address, IPv6 Address, User Name, Policy Profile, Flex Profile, Wireless LAN Id, WLAN Profile Name, Wireless LAN Network Name (SSID), BSSID, Uptime(sec), Idle state timeout, Session Timeout, Session Warning Time, Client Active State, Power Save mode, Current TxRateSet, Supported Rates, QoS Average Data Rate Upstream, QoS Realtime Average Data Rate Upstream, QoS Burst Data Rate Upstream, QoS Realtime Burst Data Rate Upstream, QoS Average Data Rate Downstream, QoS Realtime Average Data Rate Downstream, QoS Burst Data Rate Downstream, QoS Realtime Burst Data Rate Downstream, Join Time Of Client, Policy Manager State, Last Policy Manager State, Transition Disable Bitmap, User Defined (Private) Network, User Defined (Private) Network Drop, and Unicast. The 'Policy Profile' is 'LWA_LocalSW' and the 'Flex Profile' is 'Flex_LWA'. The 'Client Active State' is 'Active' and the 'Policy Manager State' is 'Run'.

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](#)