Troubleshoot Common Issues with LWA on 9800 WLCs

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Radioactive (RA) Traces on the 9800 WLC

Expected Flow

- Stages the Client Undergoes from the Client Perspective
- Stages the Client Undergoes from the WLC Perspective

Common Troubleshooting Scenarios

- Authentication Failures
- Portal is not Shown to the User but Client Appears Connected
- Portal is not Shown to the User and Client Does Not Connect
- End clients are not getting an IP address
- Customized Portal is not Shown to the End Client
- Customized Portal is not Correctly Shown to the End Client
- Portal Says that "Your connection is not secure/verify signature failed"

Related Information

Introduction

This document describes the common issues with clients connecting to a WLAN with Local Web Authentication (LWA).

Prerequisites

Requirements

Cisco recommends you have basic knowledge of:

- Cisco Wireless LAN Controller (WLC) 9800 series.
- General understanding of Local Web Authentication (LWA) and its configuration.

Components Used

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

- 9800-CL WLC
- Cisco Access Point 9120AXI

- 9800 WLC Cisco IOS® XE version 17.9.3

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

LWA is a type of WLAN authentication that can be configured on the WLC where the end client that attempts to connect, after they select the WLAN from the list, presents a portal to the user. In this portal, the user could enter a username and password (depending on the configuration selected) to finish the connection to the WLAN.

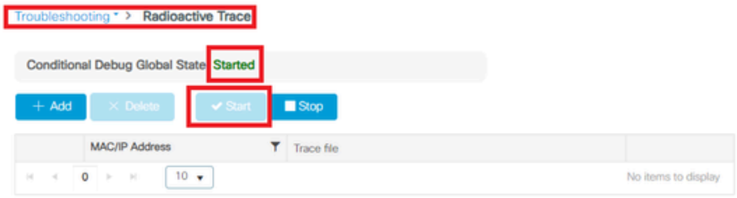
Refer to the Configure Local Web Authentication configuration guide for more information on how to configure LWA on the 9800 WLC.

Radioactive (RA) Traces on the 9800 WLC

Radioactive traces are a great troubleshooting tool that can be used when troubleshooting various issues with the WLC and client connectivity. In order to collect RA traces do the steps:

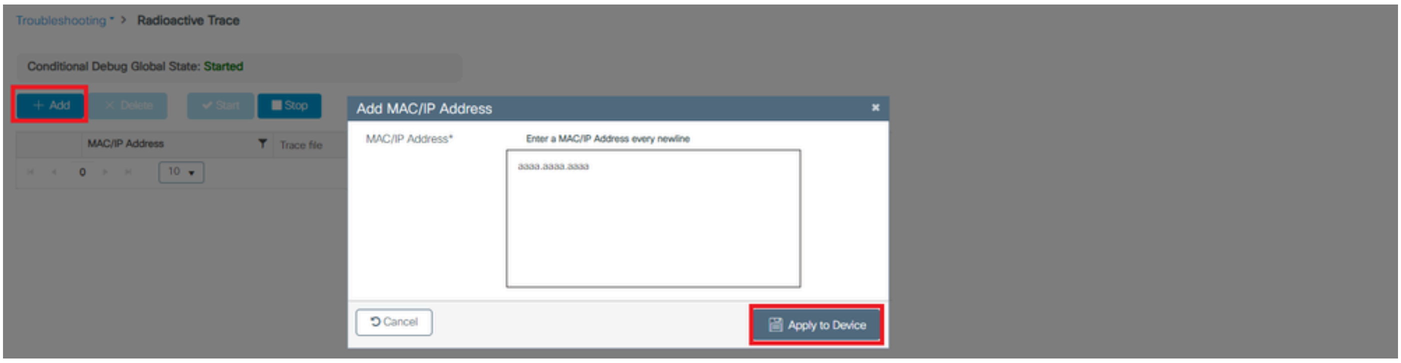
From the GUI:

1. Go to **Troubleshooting** > **Radioactive Trace.**
2. Click on Start to enable **Conditional Debug Global State.**
3. Click on **+ Add**. A pop-up window is opened open. Enter the MAC address of the client. Any MAC address format is accepted (**aabb.ccdd.eeff, AABB.CCDD.EEEE**, **aa:bb:cc:dd:ee:ff**, or **AA:BB:CC:DD:EE:FF**). Then click on **Apply to Device.**
4. Have the client reproduce the issue 3 or 4 times.
5. Once the issue has been reproduced, click on **Generate.**
6. A new pop-up window is opened. Generate logs for the last **10 minutes.** (In this case it is not necessary to enable the Internal Logs). Click on **Apply to Device** and wait for the file to be processed.
7. Once the file has been generated, click on the **Download** icon.



Conditional Debug Global State Started

Enable Conditional Debugging

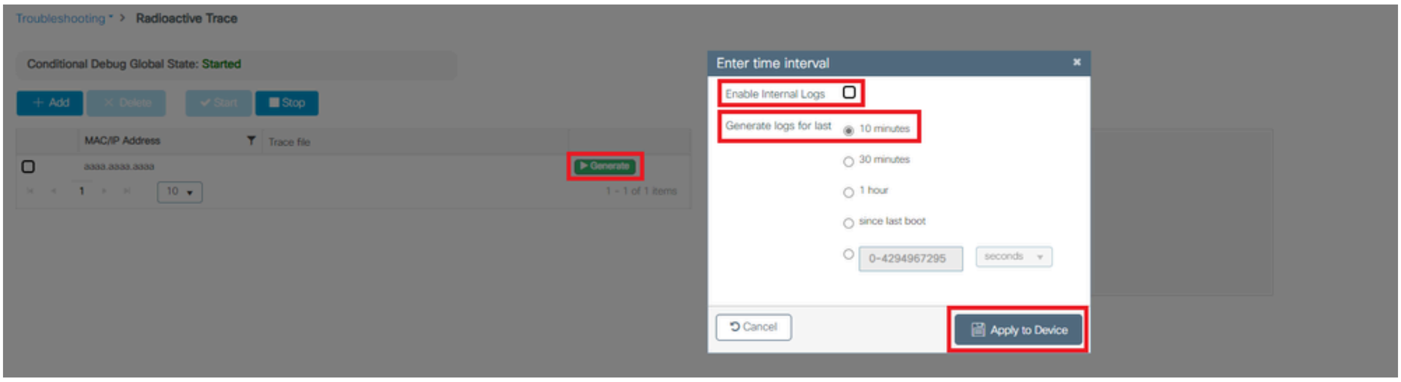


Conditional Debug Global State: Started

MAC/IP Address*: Enter a MAC/IP Address every newline

aaaa.aaaa.aaaa

Add a client MAC address



Conditional Debug Global State: Started

aaaa.aaaa.aaaa

1 - 1 of 1 items

Enable Internal Logs □

Generate logs for last ● 10 minutes

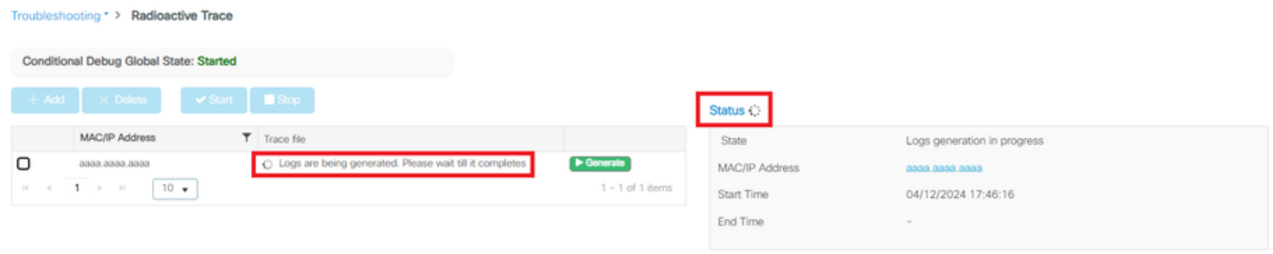
○ 30 minutes

○ 1 hour

○ since last boot

○ 0-4294967295 seconds

Generate Logs for the Last 10 Minutes



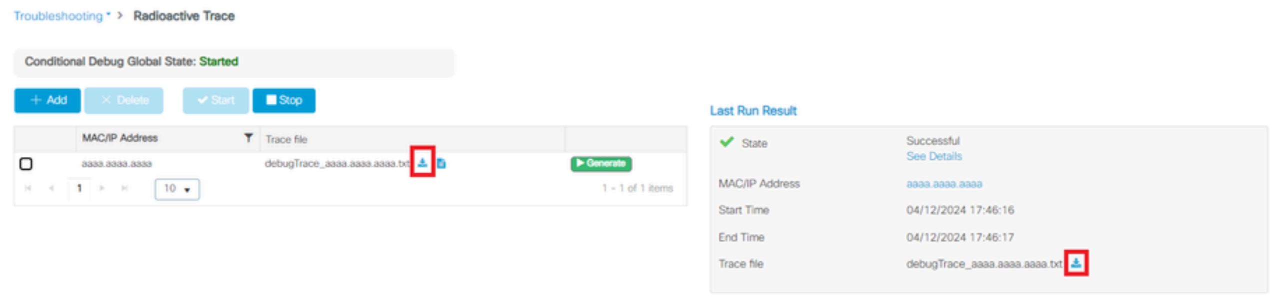
Conditional Debug Global State: Started

aaaa.aaaa.aaaa — Logs are being generated. Please wait till it completes

1 - 1 of 1 items

State	Logs generation in progress
MAC/IP Address	aaaa.aaaa.aaaa
Start Time	04/12/2024 17:46:16
End Time	-

Wait for the File to be Generated



Conditional Debug Global State: Started

aaaa.aaaa.aaaa — debugTrace_aaaa.aaaa.aaaa.txt

1 - 1 of 1 items

✓ State	Successful See Details
MAC/IP Address	aaaa.aaaa.aaaa
Start Time	04/12/2024 17:46:16
End Time	04/12/2024 17:46:17
Trace file	debugTrace_aaaa.aaaa.aaaa.txt

Download the File

From the CLI:

<#root>

```
WLC# debug wireless mac

<mac-address>

 monitor-time 600
```

A new file in the bootflash is be generated called **ra_trace_MAC_<mac-address>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log**

<#root>

```
WLC# more bootflash:

ra_trace_MAC_<mac-address>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Copy the file to an external server for analysis

<#root>

```
WLC# copy bootflash:

ra_trace_MAC_<mac-address>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

 ftp://username:password@<ftp-server-ip>/path/RATRACE_FILENAME.txt
```

For more information about Radioactive Tracing please refer to this link.

Expected Flow

Refer to the information to understand the working scenario for LWA.

Stages the Client Undergoes from the Client Perspective

1. End client associates to the WLAN.
2. Client gets an IP address assigned.
3. Portal is presented to the end client.
4. End client enters login credentials.
5. End client is authenticated.
6. End client is able to browse the Internet.

Stages the Client Undergoes from the WLC Perspective

Caution: Many logs from the Radio Active (RA) trace were left out for simplicity purposes.

End client associates to the WLAN

<#root>

```
MAC: aaaa.bbbb.cccc

Association received

. BSSID d4e8.801a.3063, WLAN LWA-SSID, Slot 0 AP d4e8.801a.3060, APD4E8.8019.608C, old BSSID d4e8.801a.
MAC: aaaa.bbbb.cccc Received Dot11 association request. Processing started,SSID: LWA-SSID, Policy profi
MAC: aaaa.bbbb.cccc Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS
MAC: aaaa.bbbb.cccc Dot11 ie validate ext/supp rates. Validation Passed for Supported rates radio_type 
MAC: aaaa.bbbb.cccc WiFi direct: Dot11 validate P2P IE. P2P IE not present.
MAC: aaaa.bbbb.cccc dot11 send association response. Framing association response with resp_status_code
MAC: aaaa.bbbb.cccc Dot11 Capability info byte1 1, byte2: 14
MAC: aaaa.bbbb.cccc WiFi direct: skip build Assoc Resp with P2P IE: Wifi direct policy disabled
MAC: aaaa.bbbb.cccc Clearing old call info.
MAC: aaaa.bbbb.cccc dot11 send association response. Sending assoc response of length: 161 with resp_st
MAC: aaaa.bbbb.cccc
```

```
Association success.

 AID 1, Roaming = True, WGB = False, 11r = False, 11w = False Fast roam = False
MAC: aaaa.bbbb.cccc DOT11 state transition: S_DOT11_ASSOCIATED -> S_DOT11_ASSOCIATED
```

L2 Authentication

<#root>

```
MAC: aaaa.bbbb.cccc Starting L2 authentication. Bssid in state machine:d4e8.801a.3063 Bssid in request 
MAC: aaaa.bbbb.cccc Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_L2_AUTH_IN_PROGRESS
MAC: aaaa.bbbb.cccc L2 Authentication initiated. method WEBAUTH, Policy VLAN 0, AAA override = 1
[aaaa.bbbb.cccc:capwap_90400002] -

authc_list: forwebauth


[aaaa.bbbb.cccc:capwap_90400002] - authz_list: Not present under wlan configuration
MAC: aaaa.bbbb.cccc Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUT
MAC: aaaa.bbbb.cccc IP-learn state transition: S_IPLEARN_COMPLETE -> S_IPLEARN_COMPLETE
MAC: aaaa.bbbb.cccc Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUT
MAC: aaaa.bbbb.cccc

L2 Authentication of station is successful.

, L3 Authentication : 1
```

Client Gets an IP Address Assigned

<#root>

```
MAC: aaaa.bbbb.cccc Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS
MAC: aaaa.bbbb.cccc IP-learn state transition: S_IPLEARN_COMPLETE -> S_IPLEARN_COMPLETE
MAC: aaaa.bbbb.cccc

Received ip learn response. method: IPLEARN_METHOD_DHCP
```

L3 Authentication

<#root>

```
MAC: aaaa.bbbb.cccc Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS
MAC: aaaa.bbbb.cccc

L3 Authentication initiated. LWA


MAC: aaaa.bbbb.cccc Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUT
```

Client Gets an IP Address

<#root>

```
RX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
TX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
RX: DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y
TX: DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y
RX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
TX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
RX: DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y
TX: DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y
MAC: aaaa.bbbb.cccc IP-learn state transition: S_IPLEARN_COMPLETE ->

 S_IPLEARN_COMPLETE
```

Portal Processing

<#root>

```
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

HTTP GET request


[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

Parse GET, src [X.X.X.X] dst [Z.Z.Z.Z] url [http://connectivitycheck.gstatic.com/generate_204]


[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Read complete: parse_request return 8
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Param-map used: lwa-parameter_map
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

State GET_REDIRECT -> GET_REDIRECT

[...]



[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

GET rcvd when in GET_REDIRECT state

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

HTTP GET request

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

Parse GET, src [X.X.X.X] dst [192.0.2.1] url [https://<virtual-ip-address>:443/login.html?redirect=http:

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Read complete: parse_request return 10



[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

Param-map used: lwa-parameter_map

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

State GET_REDIRECT -> LOGIN


[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002
```

Sending Webauth login form

```
, len 8076
[...]
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002
```

POST rcvd when in LOGIN state

```
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 get url: /login.html
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Read complete: parse_request return 4
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Param-map used: lwa-parameter_map
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 State LOGIN -> AUTHENTICATING
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 45876/176 IO state READING -> AUTHENTICATING
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Param-map used: lwa-parameter_map
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002
```

State AUTHENTICATING -> AUTHC_SUCCESS

WLC Processes Information to be Applied to the Connecting End Client

<#root>

```
[aaaa.bbbb.cccc:capwap_90400002]
```

Authc success from WebAuth, Auth event success

```
[aaaa.bbbb.cccc:capwap_90400002] Raised event
```

APPLY_USER_PROFILE

```
 (14)
[aaaa.bbbb.cccc:capwap_90400002] Raised event RX_METHOD_AUTHC_SUCCESS (3)
[aaaa.bbbb.cccc:capwap_90400002] SM will not send event Template Deactivated to PRE for 0xAE000012
[aaaa.bbbb.cccc:capwap_90400002] SM will not send event Template Deactivated to PRE for 0xAE000012
```

Authentication Success.

```
 Resolved Policy bitmap:4 for client aaaa.bbbb.cccc
Applying Attribute :
```

username 0 "cisco"

```
Applying Attribute : aaa-author-type 0 1 (0x1)
Applying Attribute : aaa-author-service 0 16 (0x10)
Applying Attribute : clid-mac-addr 0 3a e6 3b 9a fc 4a
Applying Attribute : addr 0 0xac104206
Applying Attribute : addrv6 0 "þ€"
Applying Attribute : addrv6 0 " Ì□"
Applying Attribute : addrv6 0 " Ì□"
Applying Attribute : addrv6 0 " Ì□"
Applying Attribute : target-scope 0 0 [client]
Applying Attribute : audit-session-id 0 "1A4210AC0000001C5B12A51C"
Applying Attribute : aaa-unique-id 0 28 (0x1c)
Applying Attribute : client-iif-id 0 4261415483 (0xfe000a3b)
Applying Attribute :
```

vlan-id 0 100 (0xa63)

```
Applying Attribute : session-linksec-secured 0 False
Applying Attribute : nas-ip-address 0 0x0
Applying Attribute : nas-ipv6-Address 0 ""
Applying Attribute : interface 0 ""
Applying Attribute : port-type 0 19 [802.11 wireless]
Applying Attribute : nas-port 0 10014 (0x40eba)
Applying Attribute :
```

cisco-wlan-ssid 0 "LWA-SSID"

```
Applying Attribute :
```

wlan-profile-name 0 "LWA-SSID"

```
Applying Attribute : dnis 0 "d4-e8-80-1a-30-60:LWA-SSID"
Applying Attribute : formatted-clid 0 "3a-e6-3b-9a-fc-4a"
Applying Attribute : bsn-wlan-id 0 16 (0x10)
Applying Attribute : nas-identifier-wireless 0 "LWA-SSID"
Applying Attribute : timeout 0 86400 (0x15180)
Applying Attribute : priv-lvl 0 1 (0x1)
Applying Attribute : timeout 0 86400 (0x15180)
Applying Attribute :
```

method 0 1 [webauth]

```
Applying Attribute : clid-mac-addr 0 3a e6 3b 9a fc 4a
Applying Attribute : intf-id 0 2420113410 (0x90400002)
[aaaa.bbbb.cccc:capwap_90400002] auth mgr attr add/change notification is received for attr username(45
[aaaa.bbbb.cccc:capwap_90400002] SM Notified attribute
```

Add/Update username cisco

```
[aaaa.bbbb.cccc:capwap_90400002]
```

Received User-Name cisco for client aaaa.bbbb.cccc

```
[aaaa.bbbb.cccc:capwap_90400002] auth mgr attr add/change notification is received for attr auth-domain
[aaaa.bbbb.cccc:capwap_90400002] Method webauth changing state from 'Running' to 'Authc Success'
[aaaa.bbbb.cccc:capwap_90400002] Context changing state from 'Running' to 'Authc Success'
[aaaa.bbbb.cccc:capwap_90400002]
```

Username cisco received

```
[aaaa.bbbb.cccc:capwap_90400002]
```

WLAN ID 16 received

WLC Applies User Profile to the Connected End Client

<#root>

```
Applied User Profile: aaa-author-type 0 1 (0x1)
Applied User Profile: aaa-author-service 0 16 (0x10)
Applied User Profile: clid-mac-addr 0 3a e6 3b 9a fc 4a
Applied User Profile: target-scope 0 0 [client]
Applied User Profile: aaa-unique-id 0 28 (0x1c)
Applied User Profile: client-iif-id 0 4261415483 (0xfe000a3b)
Applied User Profile: vlan-id 0 100 (0xa63)
Applied User Profile:session-linksec-secured 0 False
Applied User Profile: nas-ip-address 0 0x0
Applied User Profile: nas-ipv6-Address 0 ""
Applied User Profile: interface 0 ""
Applied User Profile: port-type 0 19 [802.11 wireless]
Applied User Profile: nas-port 0 10014 (0x40eba)
Applied User Profile:

cisco-wlan-ssid 0 "LWA-SSID"


Applied User Profile:

 wlan-profile-name 0 "LWA-SSID"


Applied User Profile:nas-identifier-wireless 0 "LWA-SSID"
Applied User Profile: priv-lvl 0 1 (0x1)
Applied User Profile: method 0 1 [webauth]
Applied User Profile:

clid-mac-addr 0 3a e6 3b 9a fc 4a


Applied User Profile: intf-id 0 2420113410 (0x90400002)
Applied User Profile:

 username 0 "cisco"


Applied User Profile: bsn-wlan-id 0 16 (0x10)
Applied User Profile: timeout 0 86400 (0x15180)
Applied User Profile: timeout 0 86400 (0x15180)
MAC: aaaa.bbbb.cccc Link-local bridging not enabled for this client, not checking VLAN validity
[aaaa.bbbb.cccc:capwap_90400002]

User Profile applied successfully - REPLACE

[aaaa.bbbb.cccc:capwap_90400002] auth mgr attr add/change notification is received for attr method(757)



[aaaa.bbbb.cccc:capwap_90400002]

Raised event AUTHZ_SUCCESS (11)

[aaaa.bbbb.cccc:capwap_90400002]

Context changing state from 'Authc Success' to 'Authz Success'
```

Web Authentication is Completed

<#root>

```
MAC: aaaa.bbbb.cccc

L3 Authentication Successful.

 ACL:[]
MAC: aaaa.bbbb.cccc Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING ->

S_AUTHIF_WEBAUTH_DONE
```

AAA Attributes Applied to End Client

<#root>

```
[ Applied attribute : username 0 "

cisco

" ]
[ Applied attribute : bsn-wlan-id 0 16 (0x10) ]
[ Applied attribute : timeout 0 86400 (0x15180) ]
[ Applied attribute : timeout 0 86400 (0x15180) ]
[ Applied attribute :bsn-vlan-interface-name 0 "

myvlan

" ]
```

End Client Reaches *Run* State

<#root>

```
Managed client RUN state notification: aaaa.bbbb.cccc
MAC: aaaa.bbbb.cccc Client state transition: S_CO_L3_AUTH_IN_PROGRESS ->

S_CO_RUN
```

Common Troubleshooting Scenarios

Authentication Failures

Considerations

- Portal shown says "Authentication Failed" after entering correct credentials.
- WLC shows Client in "Web Auth Pending" state.
- The initial splash page is shown again to the user.

WLC RA Traces

<#root>

```
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Param-map used: lwa-parameter_map
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 State LOGIN -> AUTHENTICATING
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 40828/176 IO state READING -> AUTHENTICATING
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

Param-map used: lwa-parameter_map


[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 State AUTHENTICATING ->

AUTHC_FAIL [INVALID CREDENTIALS]
```

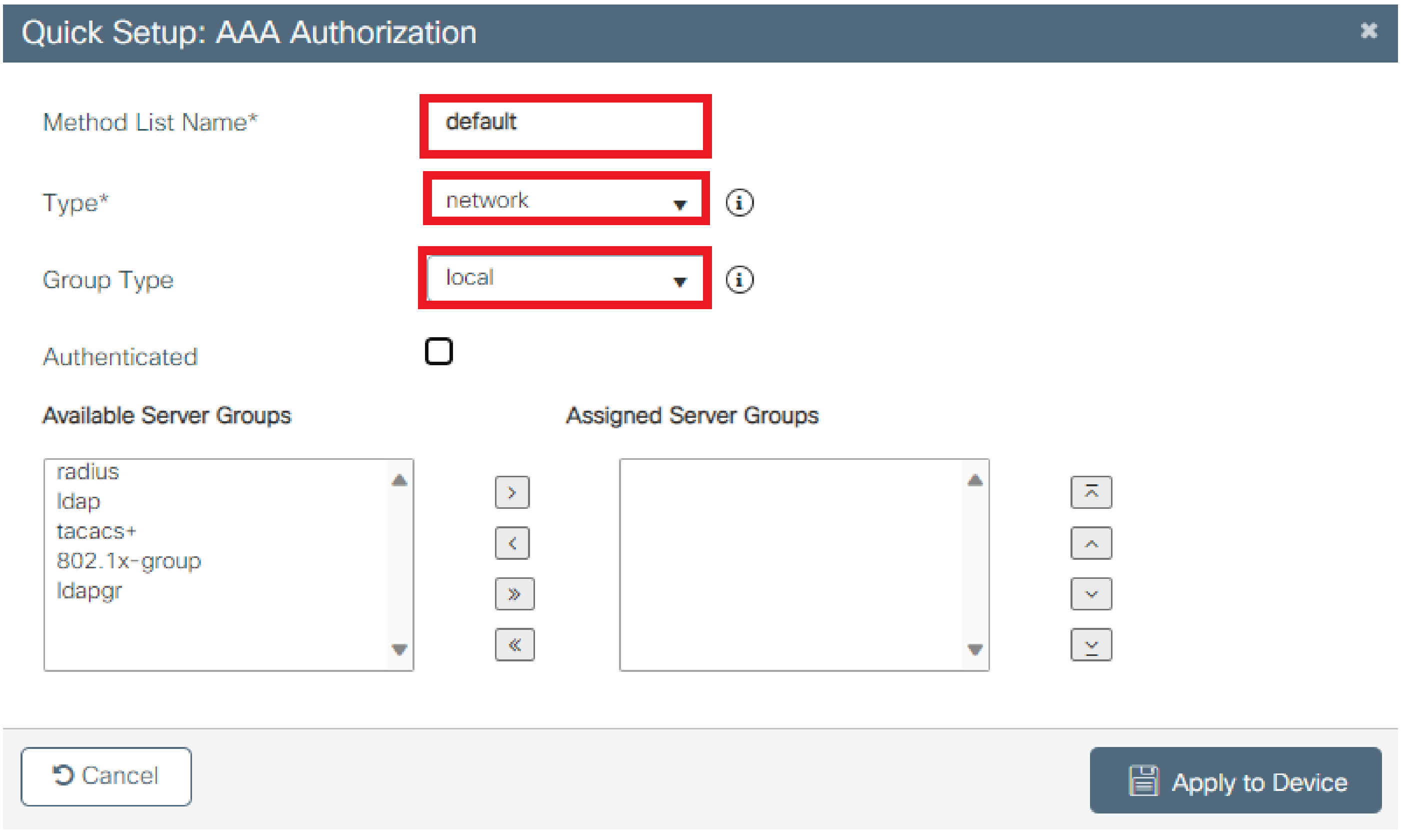
```
[aaaa.bbbb.cccc:capwap_90400002] Authc failure from WebAuth, Auth event fail
[aaaa.bbbb.cccc:capwap_90400002] (Re)try failed method WebAuth - aaaa.bbbb.cccc
[aaaa.bbbb.cccc:capwap_90400002] Method webauth changing state from 'Running' to 'Authc Failed'
```

Recommended Solutions

Ensure that the default AAA Method List for network authorization does exist on the WLC configuration.

From the GUI:

1. Go to **Configuration** > **Security** > **AAA** > **AAA Method List** > **Authorization.** Click on + **Add.**
2. Configure it as:
    1. Method List Name: default
    2. Type: network
    3. Group Type: local
3. Click **Apply to Device.**



Quick Setup: AAA Authorization

Method List Name* default

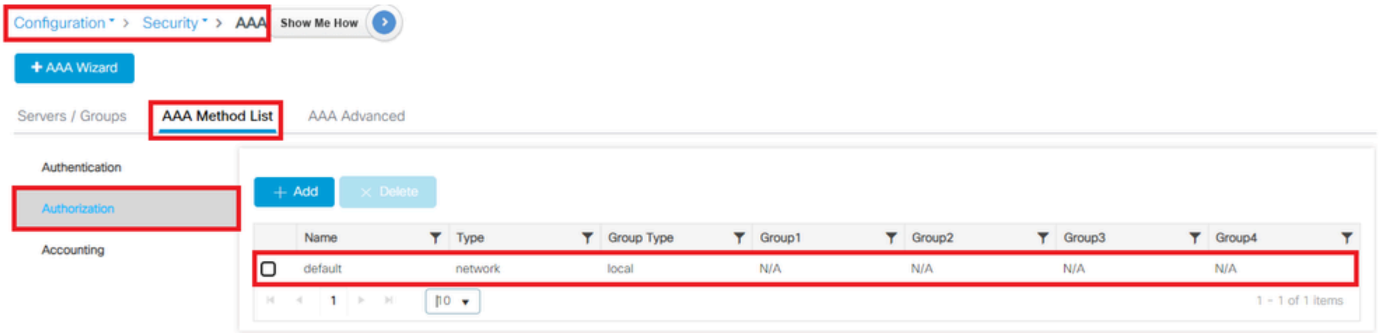
Type* network

Group Type local

Authenticated □

Available Server Groups: radius, ldap, tacacs+, 802.1x-group, ldapgr

Assigned Server Groups



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

1 - 1 of 1 items

From the CLI:

<#root>

```
WLC# configure terminal
WLC(config)# aaa authorization default network local
```

Portal is not Shown to the User but Client Appears Connected

Possible Behavior Experienced fom the End Client

- End client sees their device as "Connected".

- End client does not see the portal.
- End client does not enter any credentials.
- End client has an IP address assigned.
- WLC shows the client in "Run" state.

WLC RA Traces

Cient gets an IP address assigned and it is immediately moved to "Run" state on the WLC. User attributes only show the VLAN assigned to the end client.

<#root>

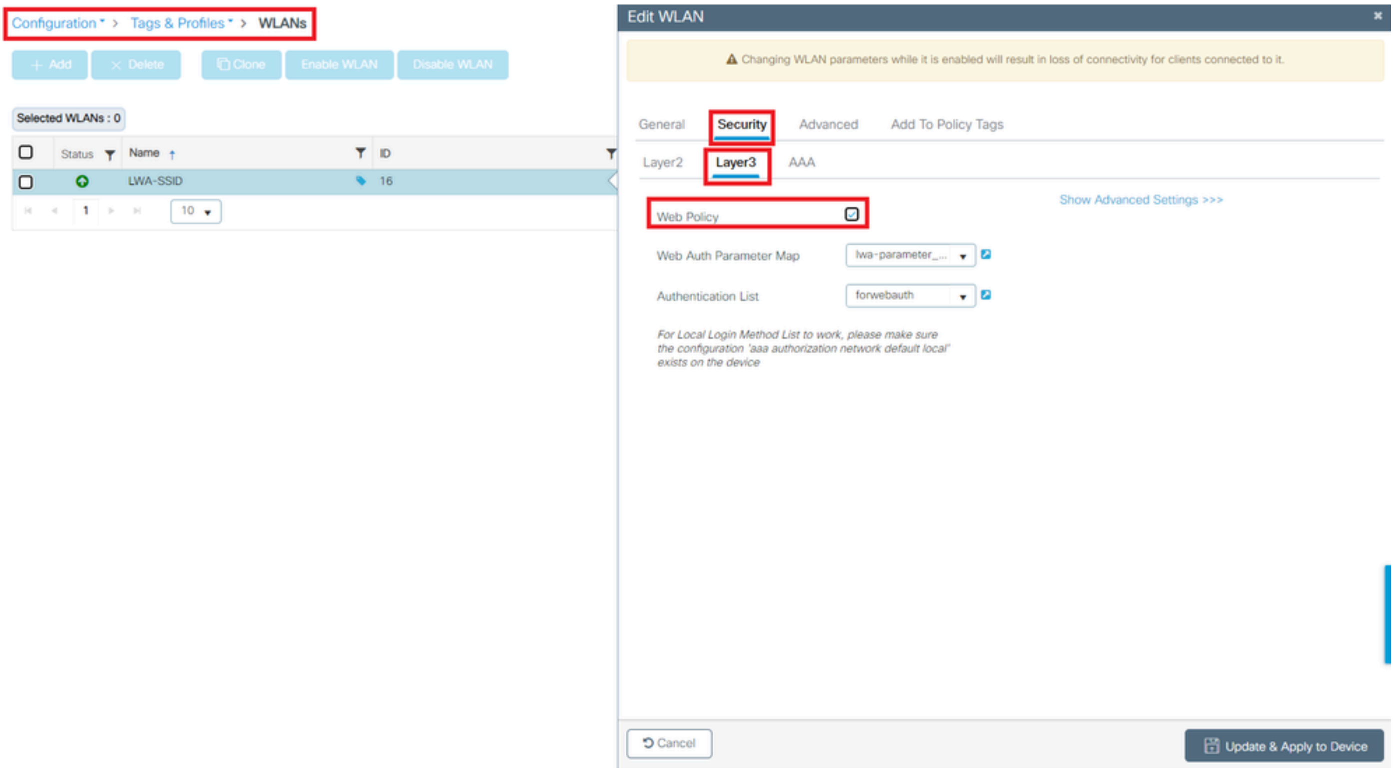
```
MAC: aaaa.bbbb.cccc

Client IP learn successful. Method: DHCP IP: X.X.X.X


[aaaa.bbbb.cccc:capwap_90400002] auth mgr attr add/change notification is received for attr addr(8)
[aaaa.bbbb.cccc:capwap_90400002] SM Notified attribute Add/Update addr X.X.X.X
MAC: aaaa.bbbb.cccc IP-learn state transition:

 S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE


MAC: aaaa.bbbb.cccc Received ip learn response. method: IPLEARN_METHOD_DHCP
[ Applied attribute :bsn-vlan-interface-name 0 "

myvlan

" ]
[ Applied attribute : timeout 0 1800 (0x708) ]
MAC: aaaa.bbbb.cccc Client QoS run state handler
Managed client RUN state notification: aaaa.bbbb.cccc
MAC: aaaa.bbbb.cccc Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN
```

Recommended Solutions

Ensure that the Web Policy is enabled on the WLAN.

From the GUI:

1. Go to **Configuration** > **Tags & Profiles** > **WLANs.**
2. Select the LWA WLANs.
3. Go to **Security** > **Layer 3.**
4. Ensure the **Web Policy** checkbox is enabled.



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

Web Policy ☑

Web Auth Parameter Map: lwa-parameter_...

Authentication List: forwebauth

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

Web Policy Needs to be Enabled

From the CLI:

<#root>

```
WLC# configure terminal



WLC(config)# wlan
```

```
<wlan>
```

```
WLC(config-wlan)# shutdown
WLC(config-wlan)# security webauth
WLC(config-wlan)# no shutdown
```

Portal is not Shown to the User and Client Does Not Connect

Possible Behavior Experienced fom the End Client

- End client sees their device is continuously trying to connect.
- End client does not see the portal.
- End client does not have an IP address assigned.

- WLC shows the client in "Webauth Pending" state.

Recommended Solutions

Enable necessary HTTP/HTTPS servers. It is now possible to have more control over which HTTP/HTTPS servers need to be enabled to fully adapt to the needs of the network. Please refer to this link for more Information About Configuring HTTP and HTTPS Requests for Web Authentication as there are several HTTP combinations supported; for example, HTTPs can be used for webadmin only and HTTP used for webauth.

To allow administrative device management and web authentication with both HTTP and HTTPS access, from the CLI:

```
WLC# configure terminal
WLC(config)# ip http server
WLC(config)# ip http secure-server
```

Caution: If both these servers are disabled, there is no access to the Graphical User Interface (GUI) of the WLC.

End clients are not getting an IP address

Possible Behavior Experienced fom the End Client

- End clients see their device is continuously trying to get an IP address.
- WLC shows the client in "IP Learning" state.

WLC RA Traces

Disovery requests with no offer back.

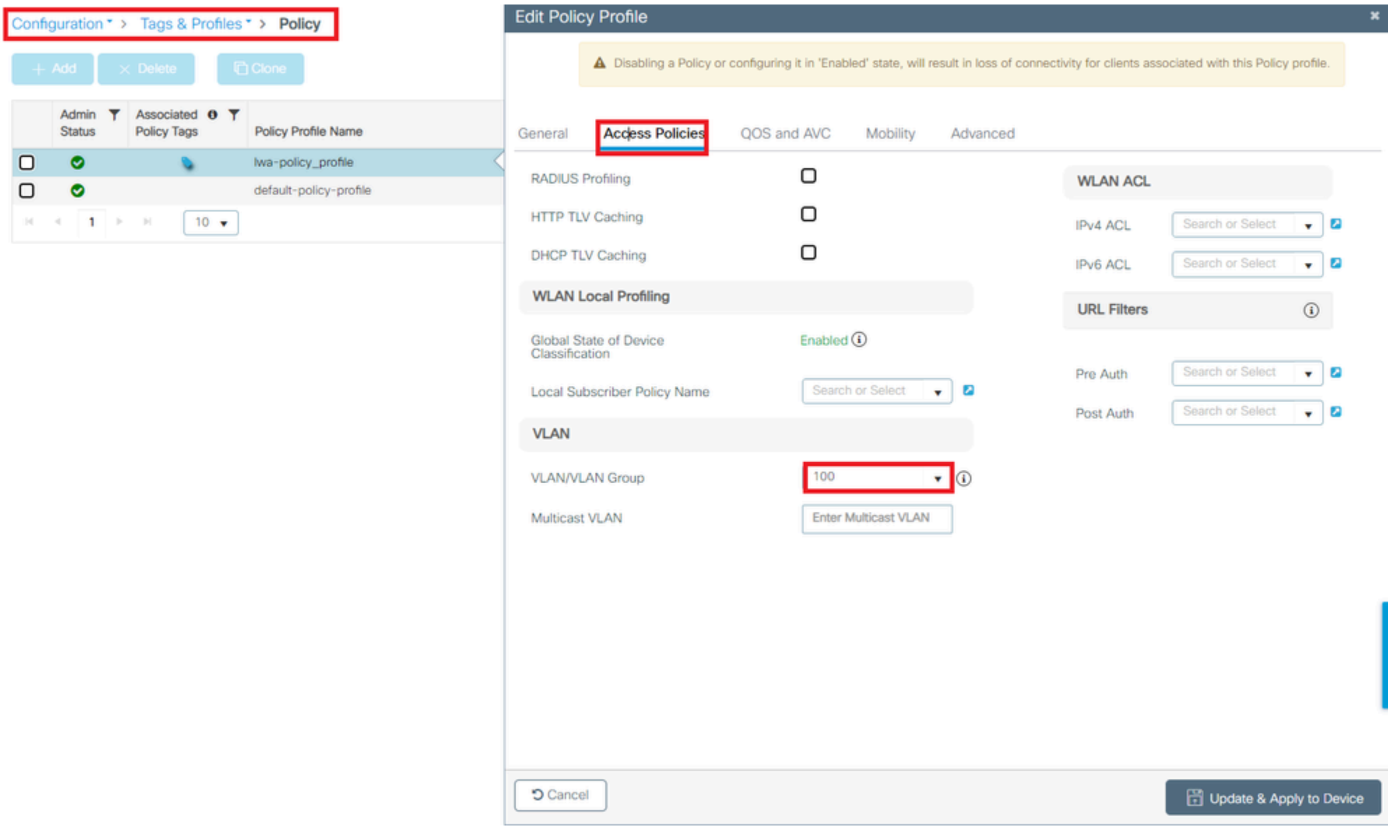
```
RX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
TX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s
```

Recommended Solutions

First: Ensure that the Policy Profile has the correct VLAN assigned.

From the GUI:

1. Go to **Configuration > Tags & Profiles > Policy.**
2. Select the used policy profile.
3. Go to **Access Policies.**
4. Select the right VLAN.



	Admin Status	Associated Policy Tags	Policy Profile Name
□	✓	●	lwa-policy_profile
□	✓		default-policy-profile

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

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: 100

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

From the CLI:

<#root>

```
WLC# show wireless profile policy detailed

<policy-profile>


Policy Profile Name :

 <policy-profile>


Description :

 <policy-profile>


Status : ENABLED
VLAN :

VLAN-selected


[...]

WLC# configure terminal
WLC(config)# wireless profile policy

 <policy-profile>


WLC(config-wireless-policy)#

vlan <correct-vlan>
```

Second: Ensure that there is a DHCP pool available for the user somewhere. Check its configuration, and its reachability. RA traces show under which VLAN DHCP DORA process is going through. Ensure this VLAN is the right VLAN.

```
DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff src_i
DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y.Y,
DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff src_i
DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y.Y,
```

Customized Portal is not Shown to the End Client

Possible Behavior Experienced fom the End Client

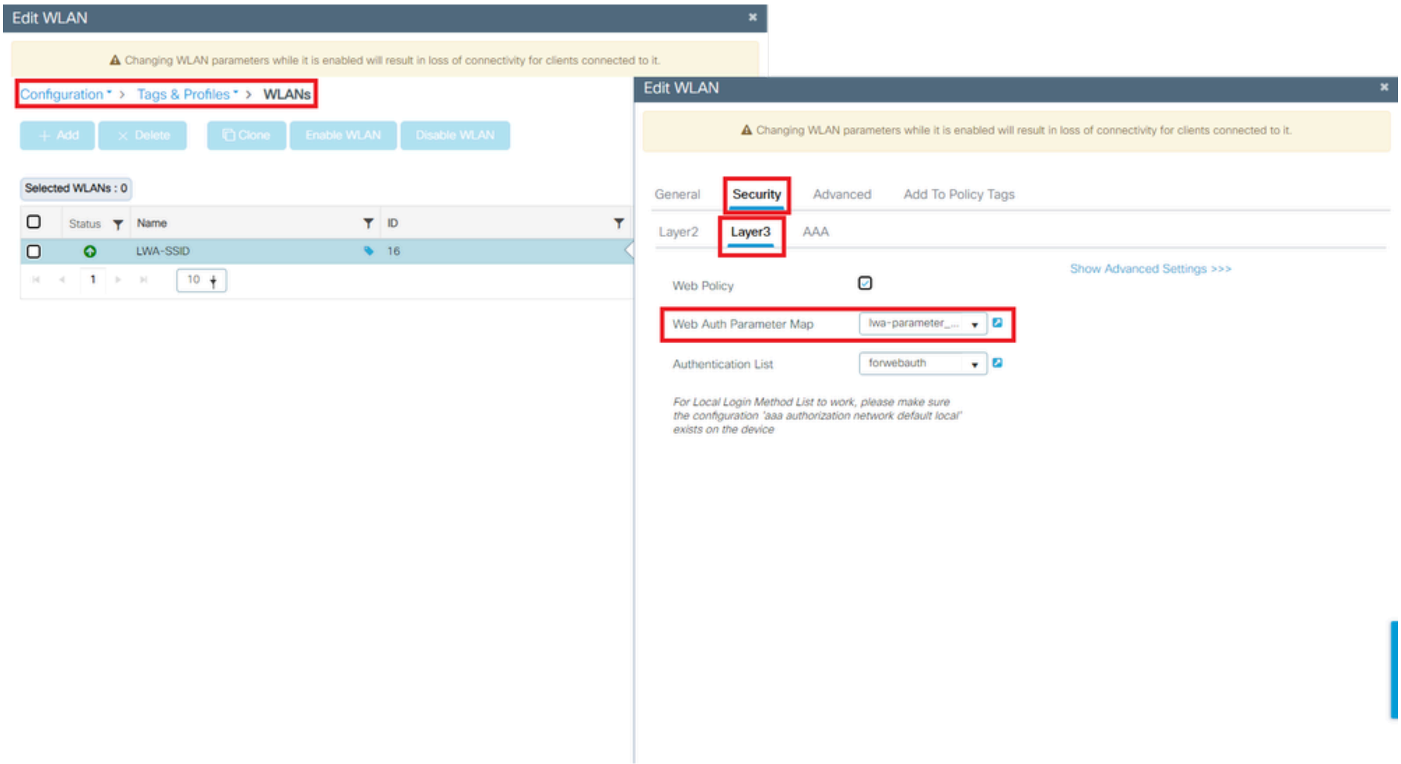
- The default portal of the WLC is seen.

Recommended Solutions

First: Make sure that the WLAN is using the customized Web Auth Parameter Map.

From the GUI:

1. Go to **Configuration** > **Tags & Profiles** > **WLANs.**
2. Select the WLAN from the list.
3. Go to **Security** > **Layer 3.**
4. Select the customized Web Auth Parameter map.



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

□	Status	Name	ID
□	●	LWA-SSID	16

Web Policy ☑

Web Auth Parameter Map: lwa-parameter_...

Authentication List: forwebauth

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

Custom Parameter Map Selected

From the CLI:

<#root>

```
WLC# show wlan name LWA-SSID
WLAN Profile Name : LWA-SSID
================================================
[...]
Security:
     Webauth Parameter Map :
```

`<parameter-map>`

```
WLC# configure terminal
WLC(config)# wlan
```

`<wlan>`

```
WLC(config-wlan)# security web-auth parameter-map
```

`<parameter-map>`

Second: It is important to note that the customized dowloaded from Cisco.com web portal does not work with a very sturdy and complicated programming interface. It is generally recommended to make changes *only* at a CSS level and perhaps adding or removing images. Applets, PHP, modify variables, React.js, and so on, are not supported. If a customized portal is not shown to the client, try using the default WLC pages and see if the issue can be replicated. If the portal is successfully seen, then there is something that is not supported on the customized pages that are supposed to be used.

Third: If using an EWC (Embedded Wireless Controller) it is suggested to use the CLI to add the customized pages to ensure that they are properly displayed:

<#root>

```
EWC# configure terminal
EWC(config)# parameter-map type
```

`<parameter-map>`

```
EWC(config-params-parameter-map)# custom-page login device flash:loginsantosh.html
EWC(config-params-parameter-map)# custom-page login expired device flash:loginexpire.html
EWC(config-params-parameter-map)# custom-page failure device flash:loginfail.html
EWC(config-params-parameter-map)# custom-page success device flash:loginsucess.html
EWC(config-params-parameter-map)# end
```

Customized Portal is not Correctly Shown to the End Client

Possible Behavior Experienced fom the End Client

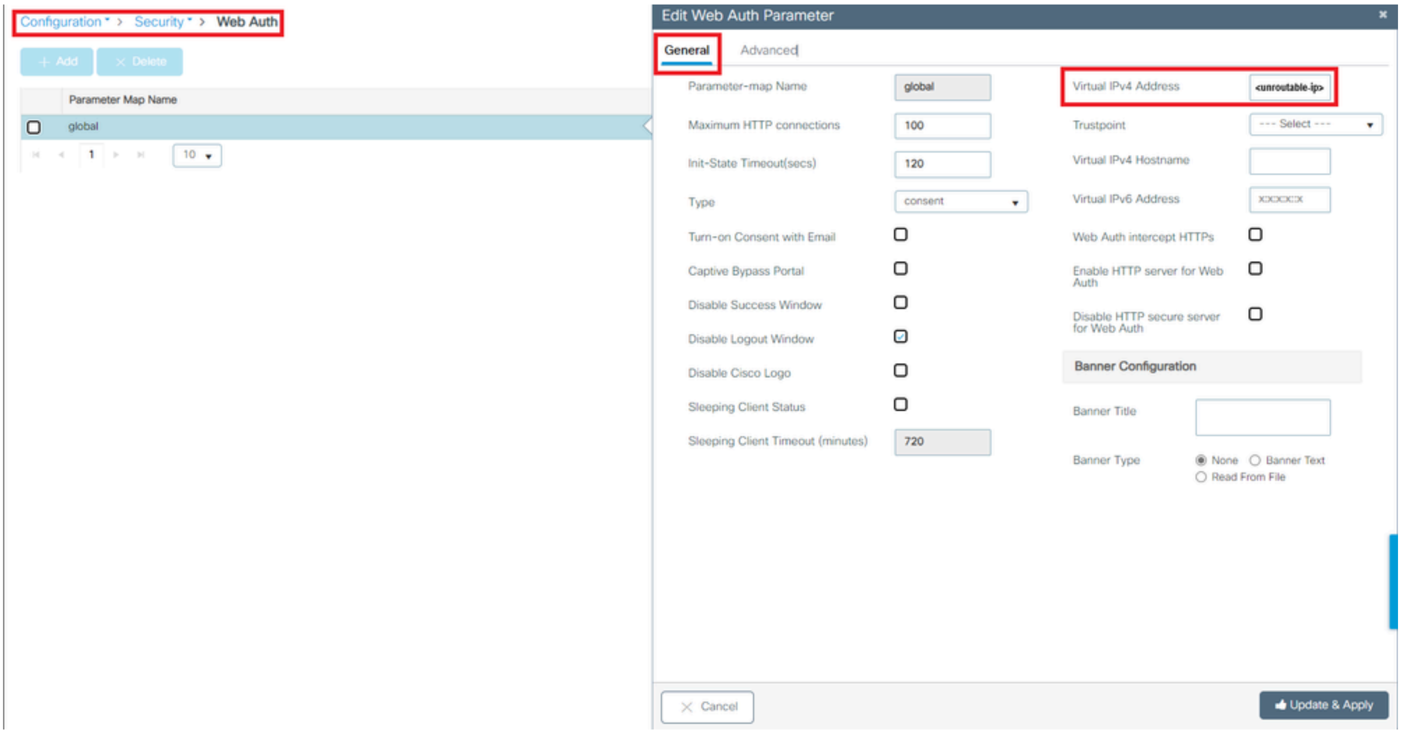
- Customized portal is not rendered correctly (that is images are not displayed).

Recommended Solutions

Make sure that the global parameter map has a virtual IP address assigned.

From the GUI:

1. Go to **Configuration** > **Security** > **Web Auth.**
2. Select the **global** parameter map from the list.
3. Add an unroutable virtual IP address.



Parameter-map Name: global

Maximum HTTP connections: 100

Init-State Timeout(secs): 120

Type: consent

Turn-on Consent with Email □

Captive Bypass Portal □

Disable Success Window □

Disable Logout Window ☑

Disable Cisco Logo □

Sleeping Client Status □

Sleeping Client Timeout (minutes): 720

Virtual IPv4 Address: <unroutable-ip>

Trustpoint: --- Select ---

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

Virtual IP Address on Global Parameter Map Set to an Unroutable IP Address

From the CLI:

<#root>

```
WLC# show parameter-map type webauth global
Parameter Map Name : global
[...]
Virtual-ipv4 :

<unroutable-ip>


[...]

WLC# configure terminal
WLC(config)# parameter-map type webauth global
WLC(config-params-parameter-map)# virtual-ip ipv4

<unroutable-ip>
```

Tip: The virtual IP address serves as the redirect address for the web authentication login page. No other device on the network must have the same IP, it must not be mapped to a physical port, nor exist on any routing table. Therefore, it is recommended to configure the virtual IP as a non-routable IP address, only those that are on the RFC5737 can be used.

Portal Says that "Your connection is not secure/verify signature failed"

Possible Behavior Experienced fom the End Client

- Upon opening the portal the client sees an error saying that the connection is not secure.
- The portal is expected to use a certificate.

Things to Know

If the portal is expected to be displayed under HTTPS, it means that it needs to use an SSL (Secure Socket

Layer) certificate. Said certificate must be issued by a 3rd party Certificate Authority (CA) to validate that the domain is fact real; providing trust to end clients when entering their credentials and/or viewing the portal. In order to upload a certificate to the WLC, please refer to this document.

Recommended Solutions

First: Restart desired HTTP/HTTPS services. It is now possible to have more control over which HTTP/HTTPS servers need to be enabled to fully adapt to the needs of the network. Please refer to this link for more Information About Configuring HTTP and HTTPS Requests for Web Authentication.

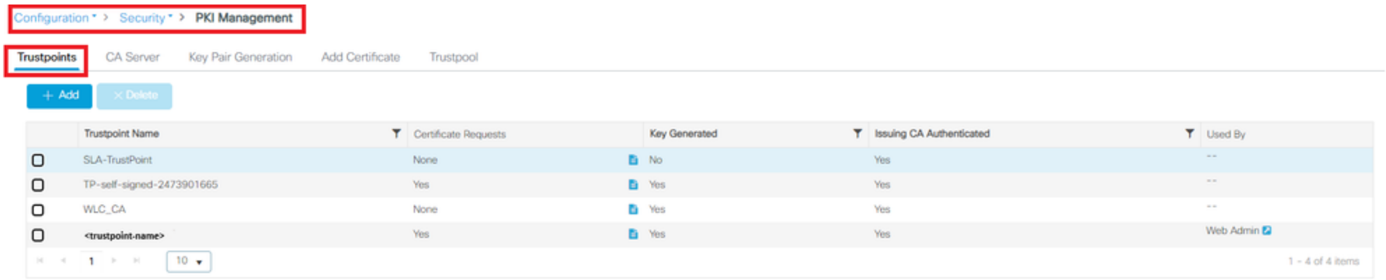
From the CLI:

```
WLC# configure terminal
WLC(config)# no ip http server
WLC(config)# no ip http secure-server
WLC(config)# ip http server
WLC(config)# ip http secure-server
```

Second: Make sure that the certificate is correctly uploaded to the WLC and that its validity date is correct.

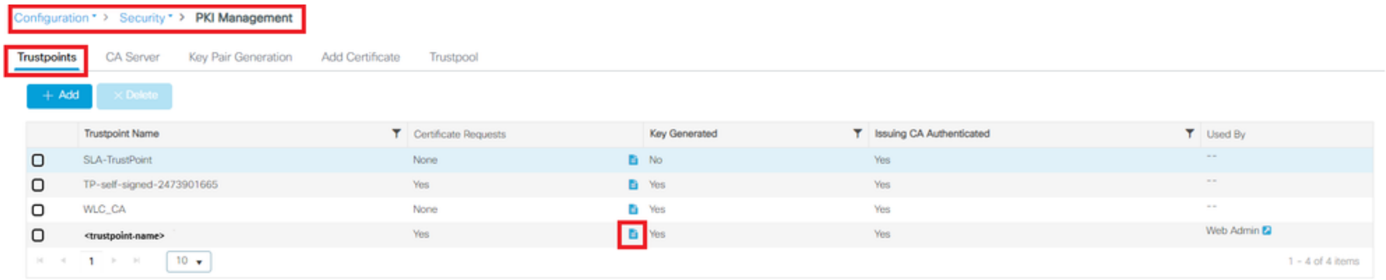
From the GUI:

1. Go to **Configuration** > **Security** > **PKI Management**
2. Search for the Trustpoint on the list
3. Check its details



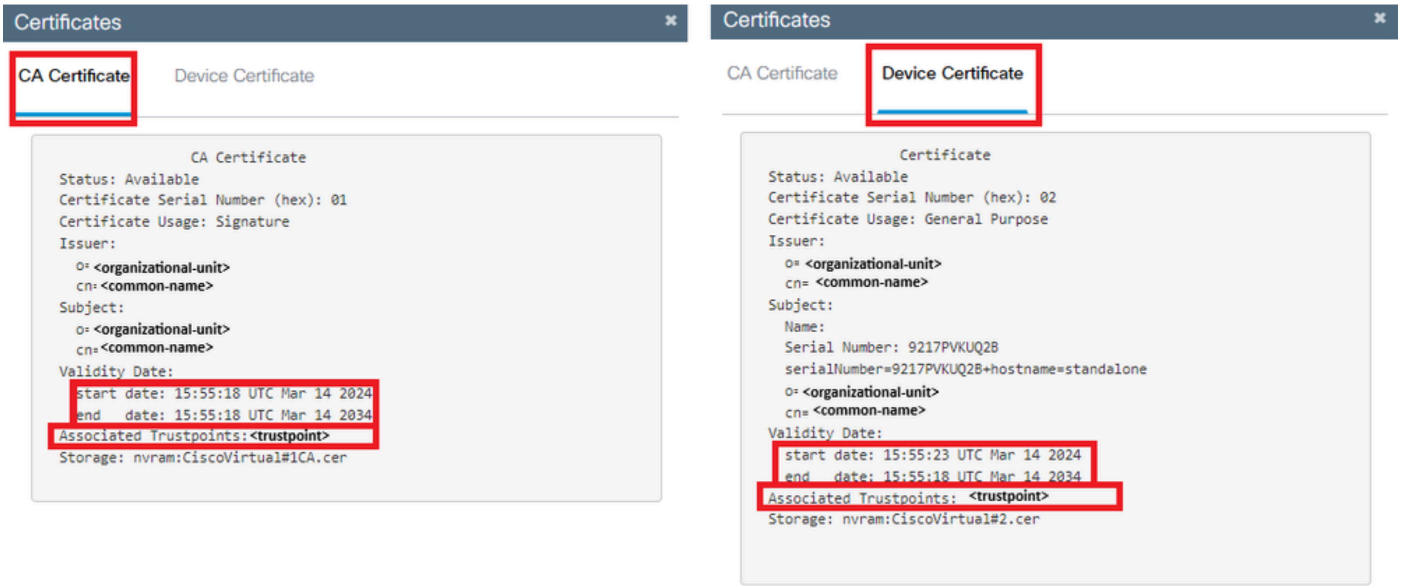
	Trustpoint Name	Certificate Requests		Key Generated	Issuing CA Authenticated	Used By
□	SLA-TrustPoint	None	🗎	No	Yes	--
□	TP-self-signed-2473901665	Yes	🗎	Yes	Yes	--
□	WLC_CA	None	🗎	Yes	Yes	--
□	<trustpoint-name>	Yes	🗎	Yes	Yes	Web Admin

Check the Trustpoint Exists



	Trustpoint Name	Certificate Requests		Key Generated	Issuing CA Authenticated	Used By
□	SLA-TrustPoint	None	🗎	No	Yes	--
□	TP-self-signed-2473901665	Yes	🗎	Yes	Yes	--
□	WLC_CA	None	🗎	Yes	Yes	--
□	<trustpoint-name>	Yes	🗎	Yes	Yes	Web Admin

Check Trustpoint Details



```
              CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
  o= <organizational-unit>
  cn: <common-name>
Subject:
  o: <organizational-unit>
  cn: <common-name>
Validity Date:
  start date: 15:55:18 UTC Mar 14 2024
  end   date: 15:55:18 UTC Mar 14 2034
Associated Trustpoints:<trustpoint>
Storage: nvram:CiscoVirtual#1CA.cer
```

```
              Certificate
Status: Available
Certificate Serial Number (hex): 02
Certificate Usage: General Purpose
Issuer:
  o= <organizational-unit>
  cn= <common-name>
Subject:
  Name:
  Serial Number: 9217PVKUQ2B
  serialNumber=9217PVKUQ2B+hostname=standalone
  o= <organizational-unit>
  cn= <common-name>
Validity Date:
  start date: 15:55:23 UTC Mar 14 2024
  end   date: 15:55:18 UTC Mar 14 2034
Associated Trustpoints:  <trustpoint>
Storage: nvram:CiscoVirtual#2.cer
```

CheckTrustpoint Validity

From the CLI:

<#root>

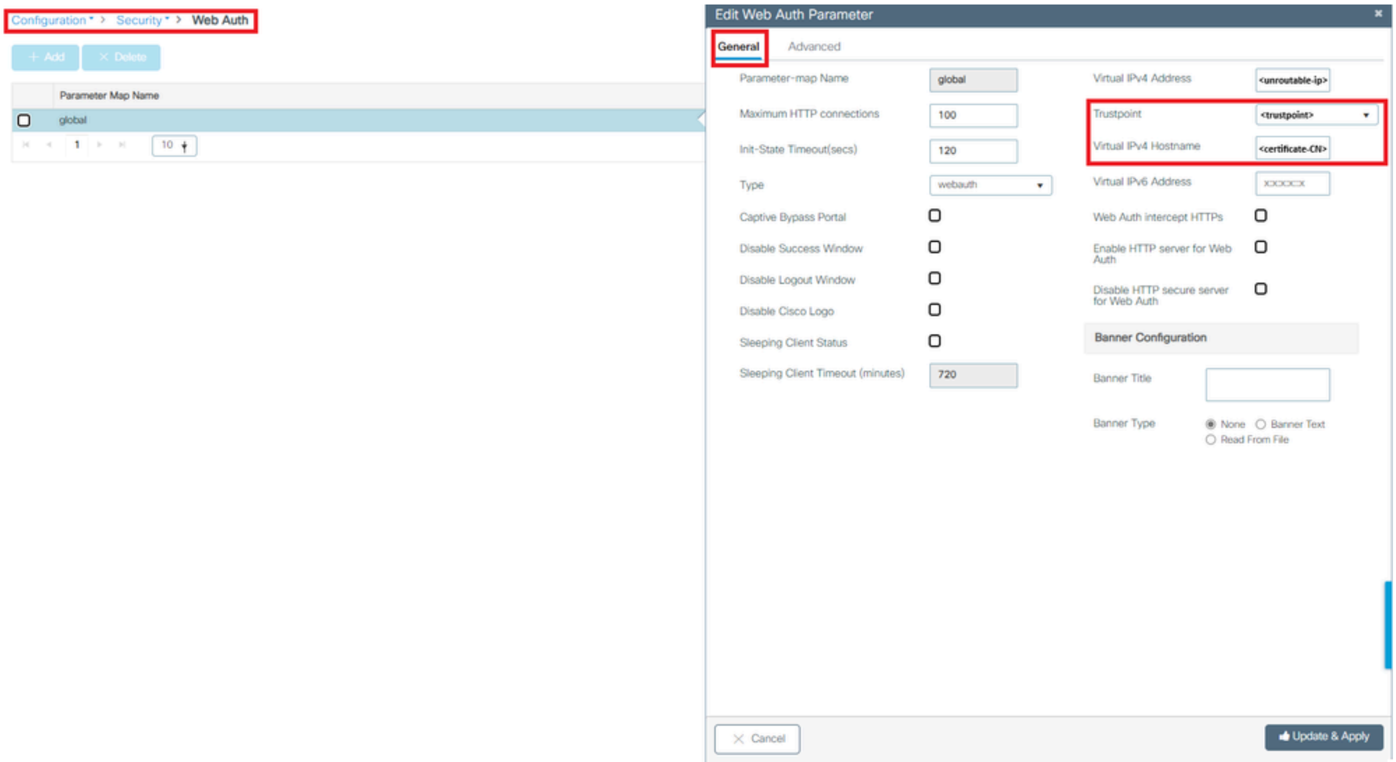
```
WLC# show crypto pki certificate

 [<certificate>]


CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=<Common Name>
    o=<Organizational Unit>
  Subject:
    cn=<Common Name>
    o=<Organizational Unit>
  Validity Date:

    start date: <start-date>



    end date: <end-date>




 Associated Trustpoints: <trustpoint>
```

Third: Make sure that the correct certificate selected for usage on the WebAuth parameter map and that the Virtual IPv4 Hostname matches the Common Name (CN) in the certificate.

From the GUI:

1. Go to **Configuration** > **Security** > **Web Auth.**

2. Select the used parameter map from the list.
3. Check that the trustpoint and Virtual IPv4 Hostname are correct.



Parameter Map Name
□ global

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: <unroutable-ip>
Trustpoint: <trustpoint>
Virtual IPv4 Hostname: <certificate-CN>
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 Title:
Banner Type: ● None ○ Banner Text ○ Read From File

Check Trustpoint and Cirtual IPv4 Hostname

From the CLI:

<#root>

```
WLC# show run | section paramter-map type

 <type> <name>

parameter-map type

 <type> <name>

 [...]
 virtual-ip ipv4

 <unroutable-ip> <certificate-common-name>



 trustpoint

<trustpoint>
```

Related Information

- Configure Local Web Authentication
- Web-Based Authentication (EWC)
- Customize the Web Authentication Portal on Catalyst 9800 WLC
- Generate and Download CSR Certificates on Catalyst 9800 WLCs

- Configuring Virtual Interfaces