

Configure OEAP and RLAN on Catalyst 9800 WLC

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Network Diagram](#)

[AP Join behind the NAT](#)

[Configuration](#)

[Verify](#)

[Log into OEAP and Configure the Personal SSID](#)

[Configure RLAN on 9800 WLC](#)

[Troubleshoot](#)

Introduction

This document explains how to configure the Cisco OfficeExtend access point (OEAP) and the Remote Local Area Network (RLAN) on 9800 WLC.

A Cisco OfficeExtend access point (OEAP) provides secure communications from a controller to a Cisco AP at a remote location, seamlessly extending the corporate WLAN over the Internet to an employee's residence. A user's experience at the home office is exactly the same as it would be at the corporate office. Datagram Transport Layer Security (DTLS) encryption between an access point and the controller ensures that all communications have the highest level of security.

A Remote LAN (RLAN) is used for authenticating wired clients using the controller. Once the wired client successfully joins the controller, the LAN ports switch the traffic between central or local switching modes. The traffic from the wired clients is treated as wireless client traffic. The RLAN in Access Point (AP) sends the authentication request to authenticate the wired client. The authentication of the wired clients in RLAN is similar to the central authenticated wireless client.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- 9800 WLC
- Command-line Interface (CLI) access to the wireless controllers and Access Points

Components Used

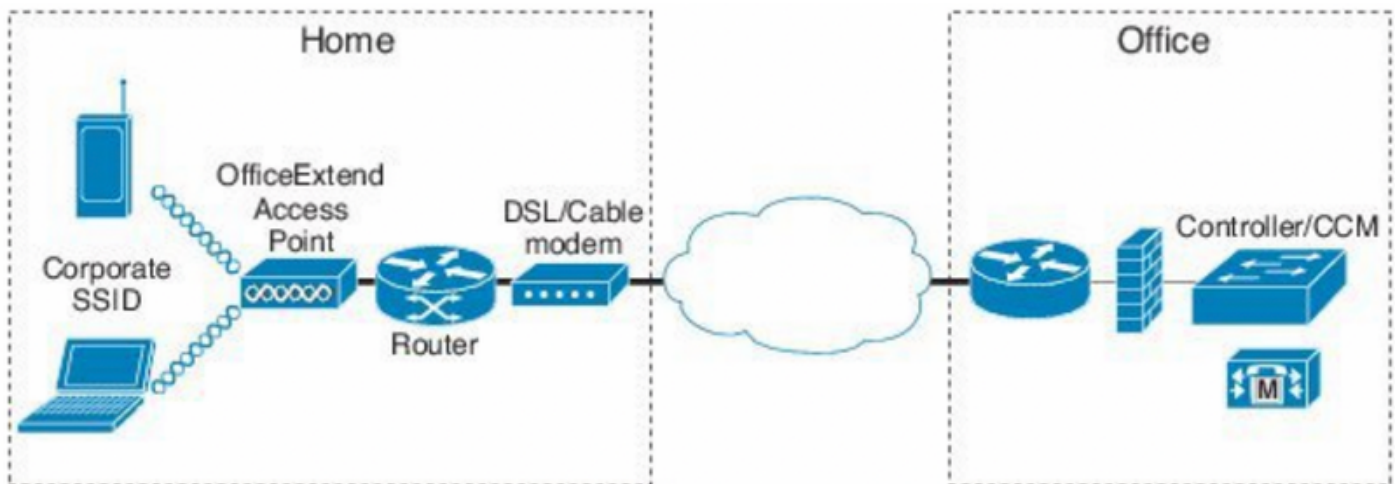
The information in this document is based on these software and hardware versions:

- Catalyst 9800 WLC version 17.02.01
- 1815/1810 Series AP

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.

Configure

Network Diagram



AP Join behind the NAT

In 16.12.x codes, you need to configure NAT IP address from the CLI. There is no GUI option available. You can also select CAPWAP discovery through public or private IP.

```
(config)#wireless management interface vlan 1114 nat public-ip x.x.x.x
(config-nat-interface)#capwap-discovery ?
  private  Include private IP in CAPWAP Discovery Response

  public   Include public IP in CAPWAP Discovery Response
```

In 17.x codes, navigate to **Configuration > Interface > Wireless** and then click **Wireless Management Interface**, to configure NAT IP and CAPWAP-discovery type from the GUI.

+ Add × Delete

Interface Name	Interface Type	Trustpoint Name	VLAN ID
Vlan1119	Management		1119

10 Items per page

Edit Management Interface

Interface:

Trustpoint:

NAT Status: ENABLED

IPv4 / IPv6 Server Address:
Invalid IP address

CAPWAP Discovery: Private Public

Configuration

1. In order to create a Flex profile, enable **Office Extend AP** and navigate to **Configuration > Tags & Profiles > Flex**.

Add Flex Profile

General	Local Authentication	Policy ACL	VLAN	Umbrella
Name*	<input type="text" value="OEAP-FLEX"/>			Fallback Radio Shut <input type="checkbox"/>
Description	<input type="text" value="OEAP-FLEX"/>			Flex Resilient <input type="checkbox"/>
Native VLAN ID	<input type="text" value="37"/>			ARP Caching <input checked="" type="checkbox"/>
HTTP Proxy Port	<input type="text" value="0"/>			Efficient Image Upgrade <input checked="" type="checkbox"/>
HTTP-Proxy IP Address	<input type="text" value="0.0.0.0"/>			Office Extend AP <input checked="" type="checkbox"/>
CTS Policy				Join Minimum Latency <input type="checkbox"/>

2. In order to create a Site Tag and map Flex Profile, navigate to **Configuration > Tags & Profiles > Tags**.

Add Site Tag

Name*

Home-Office

Description

Enter Description

AP Join Profile

default-ap-profile

Flex Profile

OEAP-FLEX

Control Plane Name

Enable Local Site

Cancel

3. Navigate to tag the 1815 AP with the Site Tag created by **Configuration > Wireless Setup > Advanced > Tag APs**.

Tag APs



Tags

Policy

default-policy-tag

Site

Home-Office

RF

default-rf-tag

Changing AP Tag(s) will cause associated AP(s) to reconnect

Cancel



Apply to Device

Verify

Once the 1815 AP re-joins the WLC, verify this output:

```
vk-9800-1#show ap name AP1815 config general
```

```
Cisco AP Name      : AP1815
```

```
=====
```

Cisco AP Identifier	:	002c.c8de.3460
Country Code	:	Multiple Countries : IN,US
Regulatory Domain Allowed by Country	:	802.11bg:-A 802.11a:-ABDN
AP Country Code	:	US - United States
Site Tag Name	:	Home-Office
RF Tag Name	:	default-rf-tag
Policy Tag Name	:	default-policy-tag
AP join Profile	:	default-ap-profile
Flex Profile	:	OEAP-FLEX
Administrative State	:	Enabled
Operation State	:	Registered
AP Mode	:	FlexConnect
AP VLAN tagging state	:	Disabled
AP VLAN tag	:	0
CAPWAP Preferred mode	:	IPv4
CAPWAP UDP-Lite	:	Not Configured
AP Submode	:	Not Configured
Office Extend Mode	:	Enabled
Dhcp Server	:	Disabled
Remote AP Debug	:	Disabled

```
vk-9800-1#show ap link-encryption
```

	Encryption	Dnstream	Upstream	Last
AP Name	State	Count	Count	Update

N2	Disabled	0	0	06/08/20 00:47:33

when you enable the OfficeExtend mode for an access point DTLS data encryption is enabled automatically.

```
AP1815#show capwap client config
```

```
AdminState           : ADMIN_ENABLED(1)
Name                  : AP1815
Location              : default location
Primary controller name : vk-9800-1
ssh status            : Enabled
ApMode                : FlexConnect
ApSubMode             : Not Configured
Link-Encryption      : Enabled
OfficeExtend AP     : Enabled
Discovery Timer       : 10
Heartbeat Timer       : 30
Syslog server         : 255.255.255.255
Syslog Facility       : 0
Syslog level          : informational
```

Note: You can enable or disable DTLS data encryption for a specific access point or for all access points using the ap link-encryption command

```
vk-9800-1(config)#ap profile default-ap-profile
```

```
vk-9800-1(config-ap-profile)#no link-encryption
```

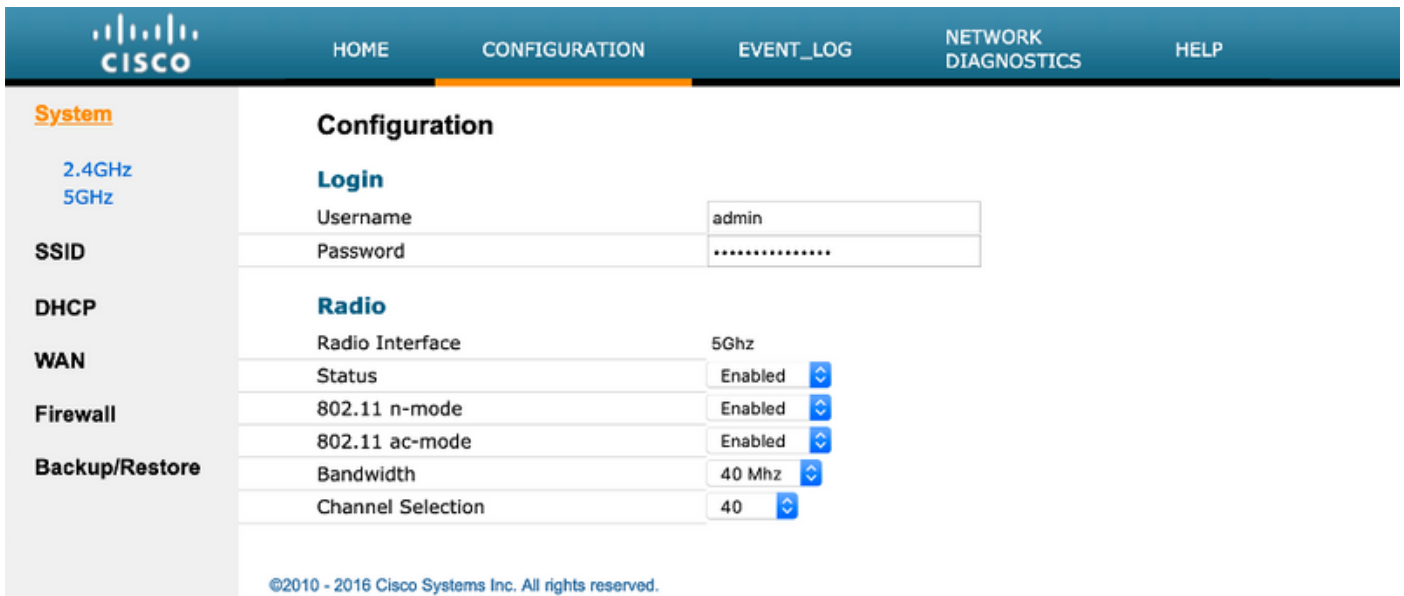
Disabling link-encryption globally will reboot the APs with link-encryption.

```
Are you sure you want to continue? (y/n) [y]:y
```

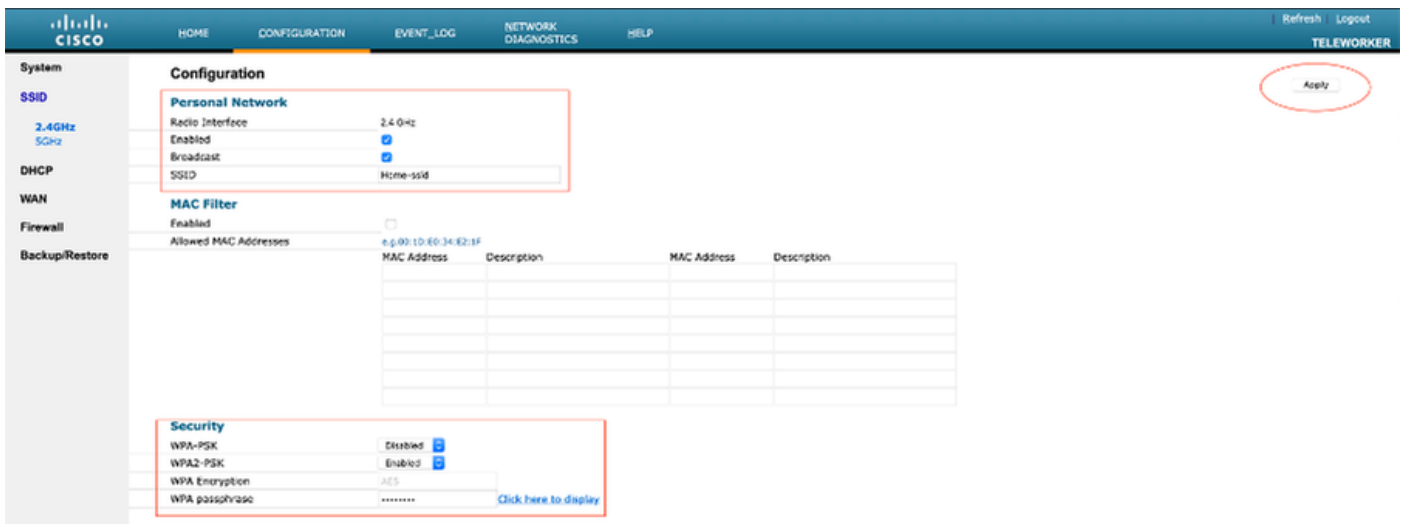
Log into OEAP and Configure the Personal SSID

1. You can access the web interface of the OEAP with its IP address. The default credentials to log in are **admin** and **admin**.

2. It is recommended to change the default credentials for security reasons.



3. Navigate to **Configuration> SSID> 2.4GHz/5GHz** to configure the personal SSID.



4. Enable Radio interface.

5. Enter the SSID and enable Broadcast

6. For encryption, choose **WPA-PSK** or **WPA2-PSK** and enter the passphrase for corresponding security type.

7. Click Apply for settings to take effect.

8. Clients that connect to the personal SSID gets the IP address from 10.0.0.1/24 network by default.

9. Home users can use the same AP to connect for their home use & that traffic is not passed via the DTLS tunnel.

10. In order to check client associations on the OEAP, navigate to **Home > Client**. You are able to see the local clients and Corporate clients associated with the OEAP.

Association							Show all
Local Clients							
Client MAC	Client IP	WLAN SSID	Radio/LAN	Association Time	Pkts In/Out		
90:17:7C:88:13:D8	10.0.0.59	Home-ssid	2.4Ghz	00d:00h:24m:55s	332/101		
Corporate Clients							
Client MAC	Client IP	WLAN SSID	Radio/LAN	Association Time	Pkts In/Out		
50:3E:AA:B7:0F:F4	10.106.37.115	corporate-ssid	2.4Ghz	00d:00h:07m:09s	499/269		

To clear personal ssid from office-extend ap

```
ewlc#ap name cisco-ap clear-personalssid-config
```

clear-personalssid-config Clears the Personal SSID config on an OfficeExtend AP

Configure RLAN on 9800 WLC

A Remote LAN (RLAN) is used for authenticating wired clients using the controller. Once the wired client successfully joins the controller, the LAN ports switch the traffic between central or local switching modes. The traffic from the wired clients is treated as wireless client traffic. The RLAN in Access Point (AP) sends the authentication request to authenticate the wired client. The

The authentication of the wired clients in RLAN is similar to the central authenticated wireless client.

Note: Local EAP is being used for RLAN client authentication in this example. Local EAP configuration has to be present on the WLC to configure the below steps. It includes aaa authentication & authorization methods, Local EAP profile, and Local credentials.

[Local EAP authentication on Catalyst 9800 WLC configuration example](#)

1. In order to create RLAN profile, navigate to **Configuration > Wireless > Remote LAN** and enter a Name and RLAN ID for the RLAN profile, as shown in this image.

Add RLAN Profile

General Security

Profile Name*

RLAN ID*

Status **ENABLED**

Client Association Limit

mDNS Mode

2. Navigate to **Security > Layer2**, in order to enable 802.1x for an RLAN, set the 802.1x status as Enabled, as shown in this image.

Edit RLAN Profile

General **Security**

Layer2 Layer3 AAA

802.1x **ENABLED**

MAC Filtering

Authentication List

3. Navigate to **Security > AAA**, set the Local EAP Authentication to enabled, and choose the required EAP Profile Name from the drop-down list, as shown in this image.

Edit RLAN Profile

General **Security**

Layer2 Layer3 **AAA**

Local EAP Authentication

ENABLED

EAP Profile Name

Local-EAP

4. In order to Create RLAN policy, navigate to **Configuration > Wireless > Remote LAN** and on the Remote LAN page, click **RLAN Policy** tab, as shown in this image.

Edit RLAN Policy

General **Access Policies** Advanced

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this policy.

Policy Name*	RLAN-Policy	RLAN Switching Policy
Description	Enter Description	Central Switching <input checked="" type="checkbox"/>
Status	ENABLED <input checked="" type="checkbox"/>	Central DHCP <input checked="" type="checkbox"/>
PoE	<input type="checkbox"/>	
Power Level	4 <input type="text"/>	

Navigate to Access Policies and configure the VLAN and Host Mode and apply the settings.

Edit RLAN Policy

General **Access Policies** Advanced

Pre-Authentication	<input type="checkbox"/>	Host Mode	singlehost <input type="text"/>
VLAN	VLAN0039 <input type="text"/>		
Remote LAN ACL			
IPv4 ACL	Not Configured <input type="text"/>		
IPv6 ACL	Not Configured <input type="text"/>		

5. In order to create Policy tag and Map RLAN profile to RLAN policy, navigate to **Configuration > Tags & Profiles > Tags**.

Add Policy Tag



Name*

RLAN-TAG

Description

Enter Description

WLAN-POLICY Maps: 0

RLAN-POLICY Maps: 0

+ Add

× Delete

Port ID	RLAN Profile	RLAN Policy Profile
No items to display		

Map RLAN and Policy

Port ID*

3

RLAN Profile*

RLAN-TEST

RLAN Policy Profile*

RLAN-Policy



Cancel

Apply to Device

Add Policy Tag ✕

Name*

RLAN-TAG

Description

Enter Description

➤ WLAN-POLICY Maps: 0

▼ RLAN-POLICY Maps: 1

+ Add

✕ Delete

	Port ID	RLAN Profile	RLAN Policy Profile
<input type="checkbox"/>	3	RLAN-TEST	RLAN-Policy

⏪ ⏩ 1 ⏪ ⏩ 10 items per page 1 - 1 of 1 items

↶ Cancel

📄 Apply to Device

6. Enable the LAN port and apply the Policy TAG on the AP. Navigate to **Configuration > Wireless > Access Points** and click on the **AP**.

Edit AP

Location*	default location	Predownloaded Status	N/A
Base Radio MAC	0042.5ab7.8f60	Predownloaded Version	N/A
Ethernet MAC	0042.5ab6.4ab0	Next Retry Time	N/A
Admin Status	ENABLED <input checked="" type="checkbox"/>	Boot Version	1.1.2.4
AP Mode	Local ▼	IOS Version	17.2.1.11
Operation Status	Registered	Mini IOS Version	0.0.0.0
Fabric Status	Disabled	IP Config	
LED State	<input type="checkbox"/> DISABLED	CAPWAP Preferred Mode	Not Configured
LED Brightness Level	8 ▼	DHCP IPv4 Address	10.106.39.198
Tags		Static IP (IPv4/IPv6)	<input type="checkbox"/>
<p>⚠ Changing Tags will cause the AP to momentarily lose association with the Controller.</p>			
Policy	RLAN-TAG ▼	Time Statistics	
Site	default-site-tag ▼	Up Time	0 days 13 hrs 33 mins 40 secs
RF	default-rf-tag ▼	Controller Association Latency	20 secs

Apply the setting and the AP re-joins the WLC. Click on the **AP**, then select **Interfaces** and enable the LAN port.

Edit AP

General **Interfaces** High Availability Inventory ICap Advanced

Radio Interfaces

Slot No	Interface	Band	Admin Status	Operation Status	Spectrum Admin Status	Spectrum Operation Status	Regulatory Domain
0	802.11n - 2.4 GHz	All	Enabled		Disabled		-A
1	802.11ac	All	Enabled		Disabled		-D

10 items per page 1 - 2 of 2 items

Power Over Ethernet Settings

Power Type/Mode: Power Injector/Normal Mode

PoE Pre-Standard Switch: Disabled

PoE Power Injector MAC Address: Disabled

LAN Port Settings

Port ID	Status	VLAN ID	PoE	Power Level	RLAN
LAN1	<input type="checkbox"/>	0	<input type="checkbox"/>	NA	
LAN2	<input type="checkbox"/>	0	NA	NA	
LAN3	<input checked="" type="checkbox"/>	39	NA	NA	

10 items per page 1 - 3 of 3 items

Apply the settings and verify the status.

Edit AP

General **Interfaces** High Availability Inventory ICap Advanced

Radio Interfaces

Slot No	Interface	Band	Admin Status	Operation Status	Spectrum Admin Status	Spectrum Operation Status	Regulatory Domain
0	802.11n - 2.4 GHz	All	Enabled		Disabled		-A
1	802.11ac	All	Enabled		Disabled		-D

10 items per page 1 - 2 of 2 items

Power Over Ethernet Settings

Power Type/Mode: Power Injector/Normal Mode

PoE Pre-Standard Switch: Disabled

PoE Power Injector MAC Address: Disabled

LAN Port Settings

Port ID	Status	VLAN ID	PoE	Power Level	RLAN
LAN1	<input type="checkbox"/>	0	<input type="checkbox"/>	NA	
LAN2	<input type="checkbox"/>	0	NA	NA	
LAN3	<input checked="" type="checkbox"/>	39	NA	NA	

10 items per page 1 - 3 of 3 items

7. Connect a PC in the LAN3 port of the AP. PC will be authenticated via 802.1x and get an IP address from the configured VLAN.

Navigate to **Monitoring > Wireless > Clients** to check the client status.

Delete



Total Client(s) in the Network: 2
 Number of Client(s) selected: 0

Client MAC Address	IPv4 Address	IPv6 Address	AP Name	SSID	WLAN ID	State	Protocol	User Name	Device Type	Role
503e.aab7.0ff4	10.106.39.227	2001::c	AP1815	corporate-ssid	3	Run	11n(2.4)		N/A	Local
b496.9126.dd6c	10.106.39.191	fe80:d8cax582:2703:f24e	AP1810	RLAN-TEST	1	Run	Ethernet	vinodh	N/A	Local

Client

360 View General QOS Statistics ATF Statistics Mobility History Call Statistics

Client Properties AP Properties Security Information Client Statistics QOS Properties EoGRE

Session Manager

IIF ID	0x9000000C
Authorized	TRUE
Common Session ID	00000000000000E79E8C7A9A
Acct Session ID	0x00000000
Auth Method Status List	
Method	Dot1x
SM State	AUTHENTICATED
SM Bend State	IDLE

```
vk-9800-1#show wireless client summary
```

```
Number of Clients: 2
```

```
MAC Address      AP Name          Type ID  State
Protocol Method   Role
```

```
-----
503e.aab7.0ff4 AP1815          WLAN 3    Run
11n(2.4) None      Local
b496.9126.dd6c AP1810          RLAN 1    Run
Ethernet Dot1x      Local
```

```
Number of Excluded Clients: 0
```

Troubleshoot

Common issues:

- Only local SSID's work, SSID's configured on WLC not being broadcasted: Check if AP has joined the Controller properly.
- Not able to access the OEAP GUI: Check if ap has IP address and verify reachability (firewall, ACL, etc in-network)
- Centrally Switched Wireless or wired clients not able to authenticate or get the IP address: Take RA traces, always on traces, etc.

Sample of Always on traces for Wired 802.1x client:

[client-orch-sm] [18950]: (note): MAC: <client-mac> Association received. BSSID 00b0.e187.cfc0, old BSSID 0000.0000.0000, WLAN test_rlan, Slot 2 AP 00b0.e187.cfc0, Ap_1810

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_INIT -> S_CO_ASSOCIATING

[dot11-validate] [18950]: (ERR): MAC: <client-mac> Failed to dot11 determine ms physical radio type. Invalid radio type :0 of the client.

[dot11] [18950]: (ERR): MAC: <client-mac> Failed to dot11 send association response. Encoding of assoc response failed for client reason code: 14.

[dot11] [18950]: (note): MAC: <client-mac> Association success. AID 1, Roaming = False, WGB = False, llr = False, llw = False AID list: 0x1| 0x0| 0x0| 0x0

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_ASSOCIATING -> S_CO_L2_AUTH_IN_PROGRESS

[client-auth] [18950]: (note): MAC: <client-mac> ADD MOBILE sent. Client state flags: 0x71 BSSID: MAC: 00b0.e187.cfc0 capwap IFID: 0x90000012

[client-auth] [18950]: (note): MAC: <client-mac> L2 Authentication initiated. method DOT1X, Policy VLAN 1119,AAA override = 0 , NAC = 0

[ewlc-infra-evq] [18950]: (note): Authentication Success. Resolved Policy bitmap:11 for client <client-mac>

[client-orch-sm] [18950]: (note): MAC: <client-mac> Mobility discovery triggered. Client mode: Local

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_L2_AUTH_IN_PROGRESS -> S_CO_MOBILITY_DISCOVERY_IN_PROGRESS

[mm-client] [18950]: (note): MAC: <client-mac> Mobility Successful. Roam Type None, Sub Roam Type MM_SUB_ROAM_TYPE_NONE, Previous BSSID MAC: 0000.0000.0000 Client IFID: 0xa0000003, Client Role: Local PoA: 0x90000012 PoP: 0x0

[client-auth] [18950]: (note): MAC: <client-mac> ADD MOBILE sent. Client state flags: 0x72 BSSID: MAC: 00b0.e187.cfc0 capwap IFID: 0x90000012

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_MOBILITY_DISCOVERY_IN_PROGRESS -> S_CO_DPATH_PLUMB_IN_PROGRESS

[dot11] [18950]: (note): MAC: <client-mac> Client datapath entry params - ssid:test_rlan,slot_id:2 bssid ifid: 0x0, radio_ifid: 0x90000006, wlan_ifid: 0xf0404001

[dpath_svc] [18950]: (note): MAC: <client-mac> Client datapath entry created for ifid 0xa0000003

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS

[client-iplearn] [18950]: (note): MAC: <client-mac> Client IP learn successful. Method: DHCP IP: <Client-IP>

[apmgr-db] [18950]: (ERR): 00b0.e187.cfc0 Get ATF policy name from WLAN profile:: Failed to get wlan profile. Searched wlan profile test_rlan

[apmgr-db] [18950]: (ERR): 00b0.e187.cfc0 Failed to get ATF policy name

[apmgr-bssid] [18950]: (ERR): 00b0.e187.cfc0 Failed to get ATF policy name from WLAN profile name: No such file or directory

[client-orch-sm] [18950]: (ERR): Failed to get client ATF policy name: No such file or directory

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition:
S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN