Troubleshoot Catalyst 9800 Wireless Controllers Common Wireless Client Connectivity Issues

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Collect Logs

- Scenarios When the Client Cannot Connect
  - Web Authentication Credentials Do Not Work
  - No Valid VLAN Defined on Policy Profile
  - Wrong Password
  - Access Control List (ACL) Sent by RADIUS does not Exist on 9800 WLC
  - VLAN Sent by RADIUS does not Exist on 9800 WLC
  - Disconnected due to Changes in the WLAN or Policy Profile
  - The Client is Manually Removed from the Network
  - Disconnected due to EAP Timeout
  - Disconnected due to AP Radio Reset
  - Disconnected due to Web Authentication Timeout
  - Disconnected due to Session Timeout
  - Disconnected due to Idle Timeout
  - The Client Moved Between SSIDs

Introduction

This document describes the most common wireless client connectivity issues scenarios and how to resolve them on Catalyst 9800 Wireless Controllers.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Catalyst 9800 Series Wireless Controllers
- Command Line Interface (CLI) access to the wireless controllers

Components Used

The information in this document is based on the Cisco IOS® XE Gibraltar 16.10 or later software and hardware versions.

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.

Collect Logs

WLC 9800 provides ALWAYS-ON tracing capabilities. This ensures all client connectivity-related errors, warnings, and notice-level messages are constantly logged and you can view logs for an incident or failure condition after it has occurred.

Note: Depending on the volume of logs generated, you can go back a few hours to several days.

In order to view the traces that 9800 WLC collected by default, you can connect via SSH/Telnet to the 9800 WLC and follow these steps (ensure your session is logged to a text file).

Step 1. Check the controller current time so you can track the logs in the time back to when the issue happened.

```
# show clock
```

Step 2. Collect syslogs from the controller buffer or the external syslog as dictated by the system configuration. This provides a quick view into the health and errors of the system if any.

```
# show logging
```

Step 3. Verify if any debug conditions are enabled.

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Tracing Configs:


Packet Infra debugs:

Ip Address                                              Port
------------------------------------------------------|----------
```

Note: If you see any condition listed, it means the traces are logged up to debug level for all the processes that encounter the enabled conditions (mac address, ip address, and so on). This increases the volume of logs. Therefore, it is recommended to clear all conditions when not actively debugging.

Step 4. Assuming the mac address under test was not listed as a condition in Step 3., collect the always-on notice level traces for the specific mac address.

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file always-on-
```

You can either display the content on the session or you can copy the file to an external TFTP server.

```
# more bootflash:always-on-<FILENAME.txt>
or
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

Conditional Debugging and Radio Active Tracing:

If the always-on traces do not give you enough information to determine the trigger for the problem under investigation, you can enable conditional debugging and capture Radio Active (RA) trace, which provides debug-level traces for all processes that interact with the specified condition (client mac address in this case). In order to enable conditional debugging, check these steps.

Step 5. Ensure there are no debug conditions enabled.

```
# clear platform condition all
```

Step 6. Enable the debug condition for the wireless client mac address that you want to monitor.

This command starts to monitor the provided mac address for 30 minutes (1800 seconds). You can optionally increase this time to up to 2085978494 seconds.

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

Note: In order to monitor more than one client at a time, run debug wireless mac <aaaa.bbbb.cccc>

command per mac address.

Note: You do not see the output of the client activity on the terminal session, as everything is buffered internally to be viewed later.

Step 7. Reproduce the issue or behavior that you want to monitor.

Step 8. Stop the debugs if the issue is reproduced before the default or configured monitor time is up.

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

Once the monitor time has elapsed or the debug wireless has been stopped, the 9800 WLC generates a local file with the name:

ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Step 9. Collect the file of the mac address activity. You can either copy the ra trace .log to an external server or display the output directly on the screen.

Check the name of the RA traces file.

```
# dir bootflash: | inc ra_trace
```

Copy the file to an external server:

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.
```

Display the content:

```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Step 10. If the root cause is still not obvious, collect the internal logs which are a more verbose view of

debug-level logs. You do not need to debug the client again as this is only to take a further detailed look at debug logs that have been already collected and internally stored.

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file r
```

Note: This command output returns traces for all logging levels for all processes and is quite voluminous. Engage Cisco TAC to help parse through these traces.

You can either copy the ra-internal-FILENAME.txt to an external server or display the output directly on the screen.

Copy the file to an external server:

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

Display the content:

```
# more bootflash:ra-internal-<FILENAME>.txt
```

Step 11. Remove the debug conditions.

```
# clear platform condition all
```

Note: Ensure that you always remove the debug conditions after a troubleshoot session.

Scenarios When the Client Cannot Connect

Web Authentication Credentials Do Not Work

Log example:

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [auth-mgr] [27915]: UUID: 100000000015b, ra: 15, (info): [e4b
```

Reason:

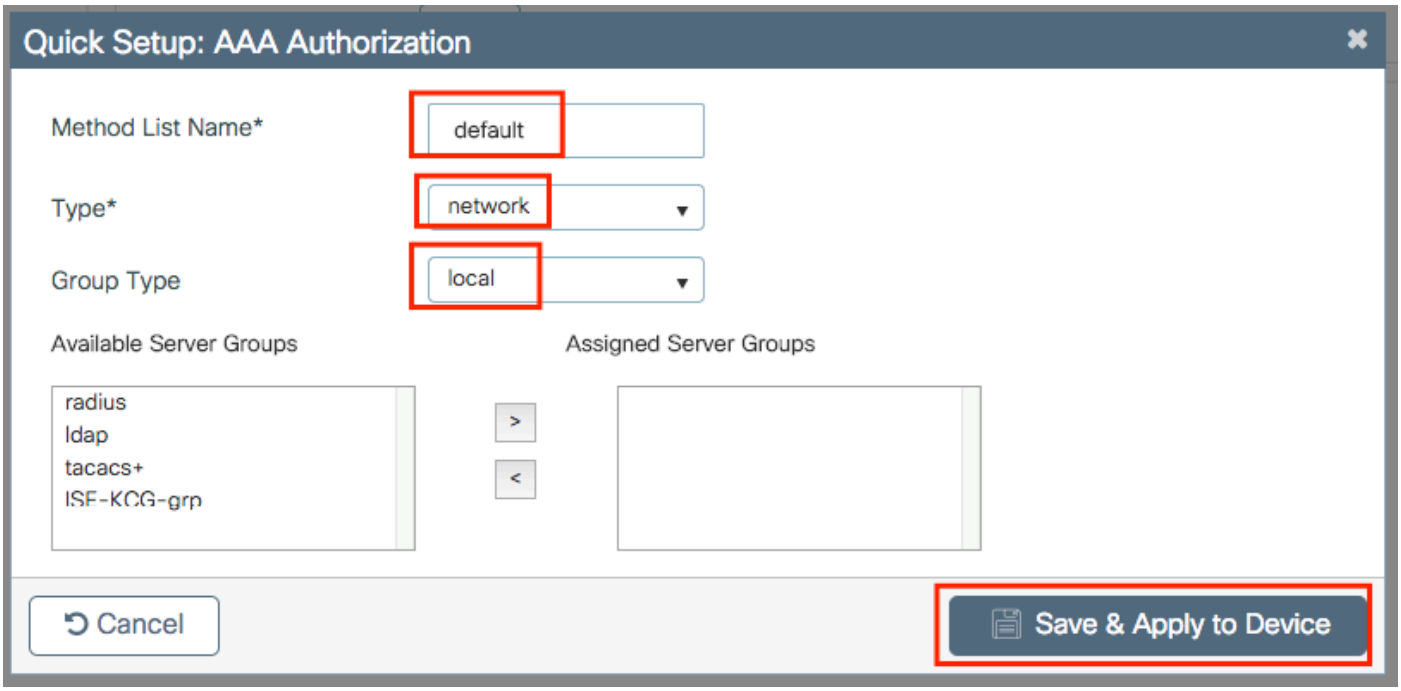
- The client is not using valid credentials
- There is no default authorization network defined on the 9800 WLC

Possible solutions:

- Ensure the client is using valid credentials
- Add a default authorization network method

GUI:

Navigate to Configuration > Security > AAA > AAA Method List > Authorization > + Add and create a new authorization method with these parameters.



CLI:

```
# config t
# aaa authorization network default local
```

No Valid VLAN Defined on Policy Profile

Log example:

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [epm] [25054]: UUID: 1000000000019, ra: 15, (ERR): EPM_PLUGIN
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [sanet-shim-miscellaneous] [25054]: UUID: 1000000000019, ra:
```

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [sanet-shim-miscellaneous] [25054]: UUID: 1000000000019, ra:
```

Reason:

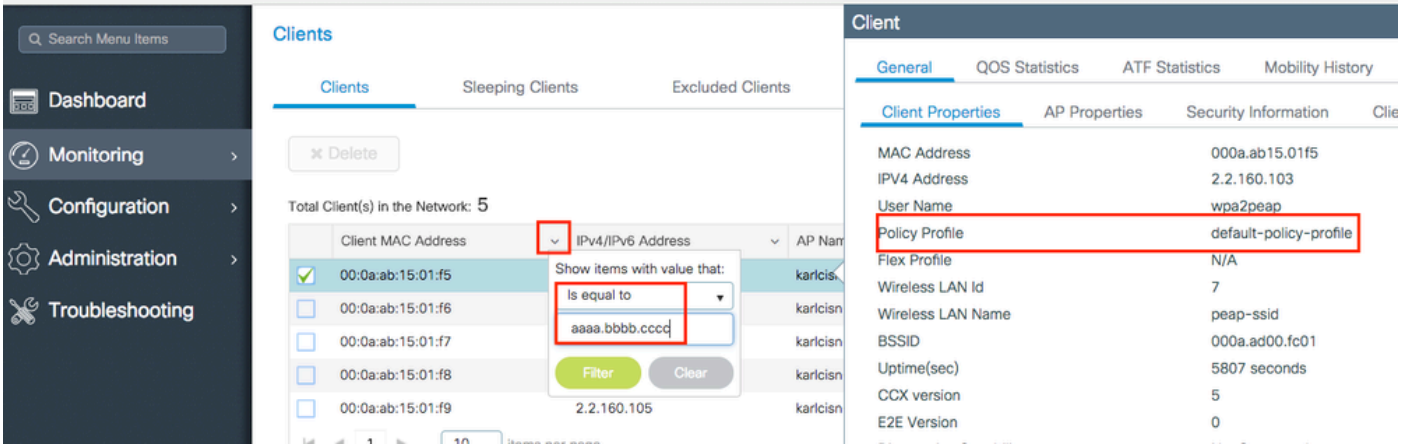
There is no valid VLAN defined on the policy profile assigned to the WLAN.

Solution:

1. Verify which Policy profile is used by the client.

GUI:

Navigate to Monitoring > Wireless > Clients > Client row > Client Properties (optional search for a specific client using its mac address).



CLI:

<#root>

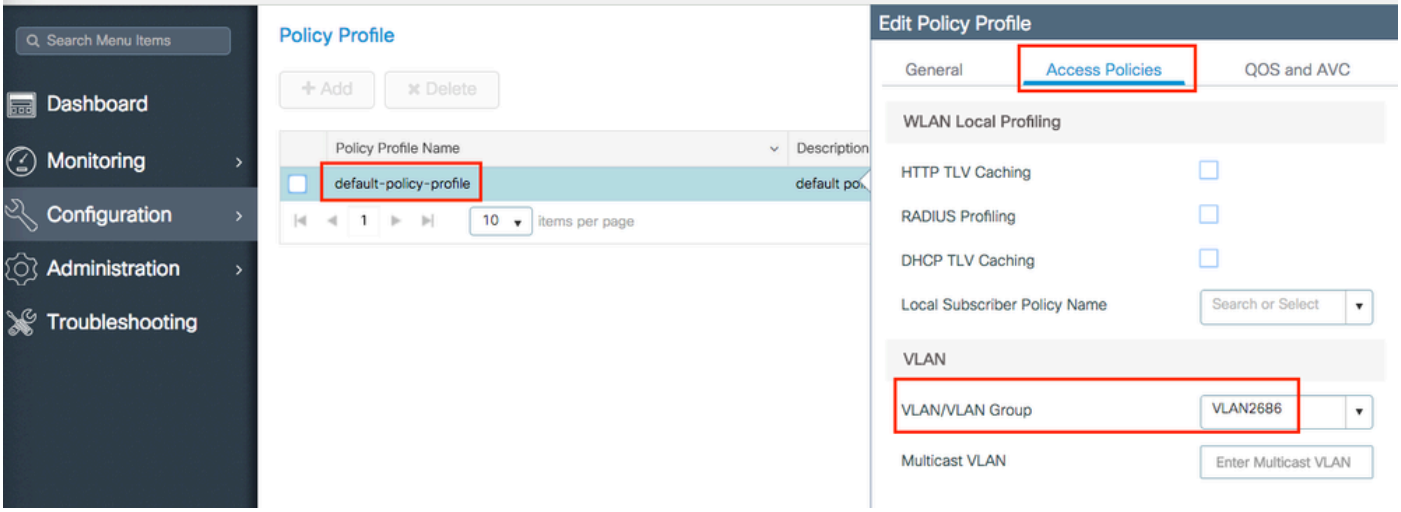
```
# show wireless client mac-address <aaaa.bbbb.cccc> detail | inc Policy Profile
Policy Profile :
```

default-policy-profile

2. Verify which VLAN is assigned to that Policy Profile.

GUI:

Navigate to Configuration > Tags & Profiles > Policy > Policy Profile row > Access Policies .



CLI:

<#root>

```
# show wireless profile policy detailed
```

`default-policy-profile`

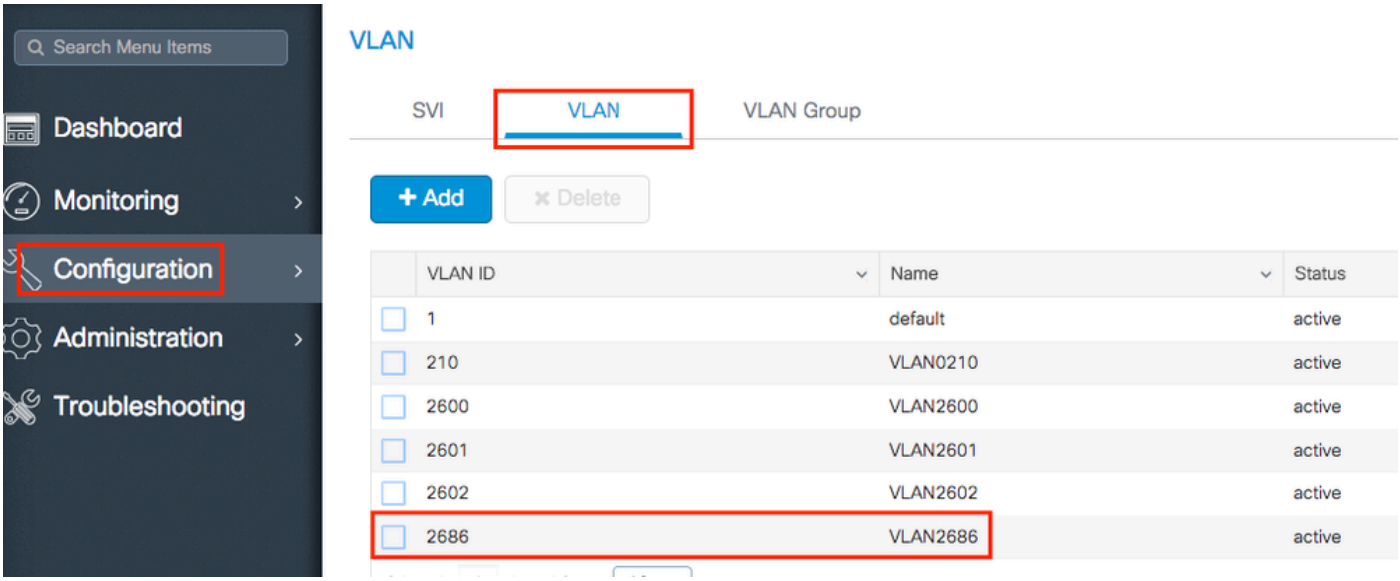
```
 | inc VLAN
VLAN                            :
```

`VLAN2686`

3. Ensure that the VLAN parameter has a VLAN name or VLAN ID valid and active.

GUI:

Navigate to Configuration > Layer2 > VLAN > VLAN .



CLI:

<#root>

```
# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Te0/0/2, Te0/0/3
210  VLAN0210                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
2600 VLAN2600                         active
2601 VLAN2601                         active
2602 VLAN2602                         active
2686
```

VLAN2686

```
                         active
```

Note: If a VLAN name is used, it is case sensitive so ensure it is exactly the same one seen on the show vlan brief command.

---

4. Fix the VLAN as needed.

GUI:

Navigate back to Configuration > Tags & Profiles > Policy > Policy Profile row > Access Policies and fix the VLAN.

CLI:

```
# config t
# wireless profile policy default-policy-profile
# shutdown
# vlan <vlan-# or vlan-name>
# no shutdown
```

Wrong Password

Log example:

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-keymgmt] [27782]: UUID: 1000000000088, ra: 15, (ERR):
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-keymgmt] [27782]: UUID: 1000000000088, ra: 15, (ERR):
```

Reason:

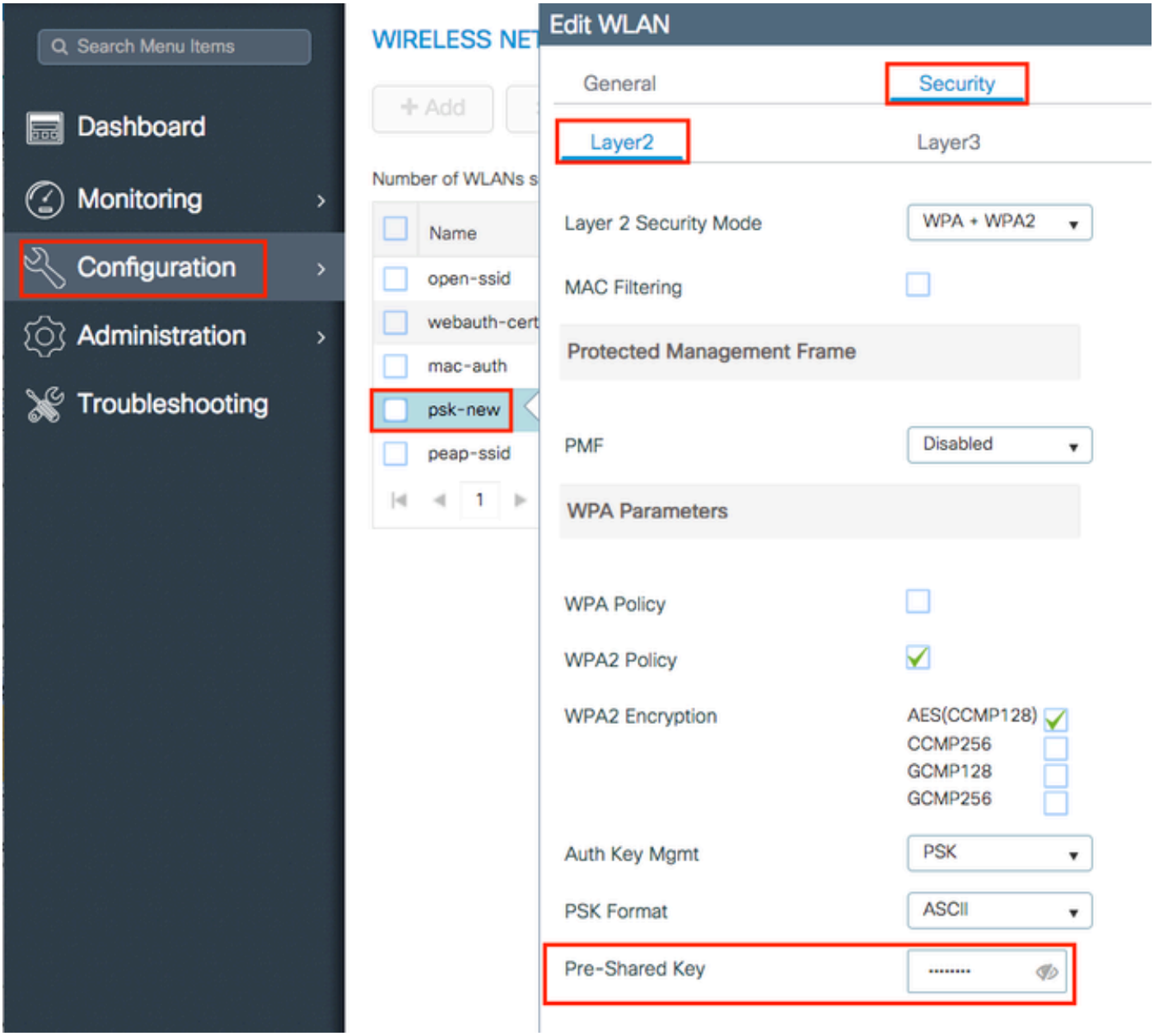
The client is entering a wrong password.

Possible solutions:

- Fix the password in the endpoint device
- Fix the password on the SSID

GUI:

Navigate to Configuration > Wireless > WLANs > WLAN name > Security > Layer2 , and fix the password.



CLI:

```
# config t
# wlan <wlan-name>
# shut
# security wpa psk set-key ascii 0 <clear-text-password>
# no shut
```

Access Control List (ACL) Sent by RADIUS does not Exist on 9800 WLC

Log example:

<#root>

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [epm-acl] [8104]: (ERR): ACL
```

acl-sent-by-ise

```
 is missing in configuration for mac e4b3.187c.3058
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [epm-acl] [8104]: (ERR): Unable to parse EPM attributes
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [wncd_0] [8104]: (info): Sanet App Event EV_PLUGIN_CONF
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [epm] [8104]: (ERR): Error in activating feature (EPM ACL PLU
.
.
.
EPM Data Base:
 Number of Authz_info: 2
 Authz info 1 details
 Number of feat info: 2, State: Success, Priority: 254
 EPM Vlan PLUG-IN Status: Success
 VLAN Group: VLAN2602
 VLAN-ID: 2602
 SM Reauth PLUG-IN Status: Success
 Authz info 2 details
 Number of feat info: 4, State: Fail, Priority: 100
 EPM MISC PLUG-IN Status: Success
 Anchor Vlan: 0
```

EPM ACL PLUG-IN Status: Activate Failure

```
 SM ACCOUNTING PLUG-IN Status: Success
 linksec Status: Success
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [9800 WLC-infra-evq-lib] [8104]: (note): already started radi
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [wncd_0] [8104]: (info): Sanet App Event EV_SVM_APPLY_UP_FAIL
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [auth-mgr] [8104]: (ERR): [e4b3.187c.3058:capwap_90000003] SM
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [auth-mgr] [8104]: (ERR): [e4b3.187c.3058:capwap_90000003] Un
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [wncd_0] [8104]: (info): Sanet eventQ: AUTH_MGR_MQ, message:3
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-auth] [8104]: (ERR): MAC: e4b3.187c.3058 client authz
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-exclusion] [8104]: (info): MAC: e4b3.187c.3058  Add c
```

Reason:

The ACL sent by the RADIUS server does not exist on 9800 WLC.

Possible solutions:

- Fix the RADIUS server configuration to send the right ACL name
- Add the missing ACL to the 9800 WLC

VLAN Sent by RADIUS does not Exist on 9800 WLC

Log example:

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [epm] [8104]: (ERR): Error in activating feature (EPM Vlan PL
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [wncd_0] [8104]: (info): Sanet App Event EV_START_CALL
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [9800 WLC-infra-evq] [8104]: (ERR):
EPM Data Base:
 Number of Authz_info: 2
 Authz info 1 details
 Number of feat info: 2, State: Success, Priority: 254
 EPM Vlan PLUG-IN Status: Conflict
 SM Reauth PLUG-IN Status: Success
 Authz info 2 details
 Number of feat info: 4, State: Activate, Priority: 100
 EPM MISC PLUG-IN Status: Success
 Anchor Vlan: 0
 SM ACCOUNTING PLUG-IN Status: Success
 EPM Vlan PLUG-IN Status: Activate Failure
 VLAN Group: vlan-sent-by-ise
 VLAN-ID: 0
 linksec Status: Success
.
.
.
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [wncd_0] [8104]: (info): Sanet App Event EV_SVM_APPLY_UP_FAIL
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [auth-mgr] [8104]: (ERR): [e4b3.187c.3058:capwap_90000003] SM
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [auth-mgr] [8104]: (ERR): [e4b3.187c.3058:capwap_90000003] Un
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [wncd_0] [8104]: (info): Sanet eventQ: AUTH_MGR_MQ, message:3
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-auth] [8104]: (ERR): MAC: e4b3.187c.3058 client authz
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-exclusion] [8104]: (info): MAC: e4b3.187c.3058 Add cl
```

Reason:

The VLAN sent by the RADIUS server does not exist on the 9800 WLC.

Possible solutions:

- Fix the RADIUS server configuration to send the right VLAN name/ID
- Add the missing VLAN to the 9800 WLC

Disconnected due to Changes in the WLAN or Policy Profile

Log example:

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [9800 WLC-infra-evq] [8522]: (note): Mcast: Sent L2 MGID 2602
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [apmgr-bssid] [8522]: (ERR): 00c8.8b26.d790 Radio:0 BSSID:1 -
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-sm] [8522]: (info): MAC: e4b3.187c.3058 Deleting
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-sm] [8522]: (note): MAC: e4b3.187c.3058 Client d
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-state] [8522]: (note): MAC: e4b3.187c.3058 Clien
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [9800 WLC-qos-client] [8522]: (ERR): MAC: e4b3.187c.3058 Fail
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [multicast-main] [8522]: (info): MAC: e4b3.187c.3058 No Flex/
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-iplearn] [8522]: (info): MAC: e4b3.187c.3058 IP-learn
YYYY/DD/MM HH:MM:SS.xxx {mobilityd_R0-0}{1}: [mm-transition] [19496]: (info): MAC: e4b3.187c.3058 MMFSM
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [dpath_svc] [8522]: (note): MAC: e4b3.187c.3058 Client datapa
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [mm-transition] [8522]: (info): MAC: e4b3.187c.3058 MMIF FSM
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [mm-client] [8522]: (ERR): MAC: e4b3.187c.3058 Invalid transm
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [wncd_0] [8522]: (info): Sanet App Event EV_SESSION_DELETE
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [auth-mgr] [8522]: (info): [e4b3.187c.3058:capwap_90000003] D
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [aaa-attr-inf] [8522]: (info): [ Applied attribute :bsn-vlan-
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [aaa-attr-inf] [8522]: (info): [ Applied attribute : timeout
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-auth] [8522]: (info): MAC: e4b3.187c.3058 Client auth
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [dot11] [8522]: (info): MAC: e4b3.187c.3058 Sent deauth to cl
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [dot11] [8522]: (info): MAC: e4b3.187c.3058 DOT11 state trans
```

Reason:

There were changes done in the GUI or the SSID or Policy Profile was manually disabled.

Solution:

This is normal behavior, avoid making changes to the SSIDs or policy profiles on production hours.

The Client is Manually Removed from the Network

Log example:

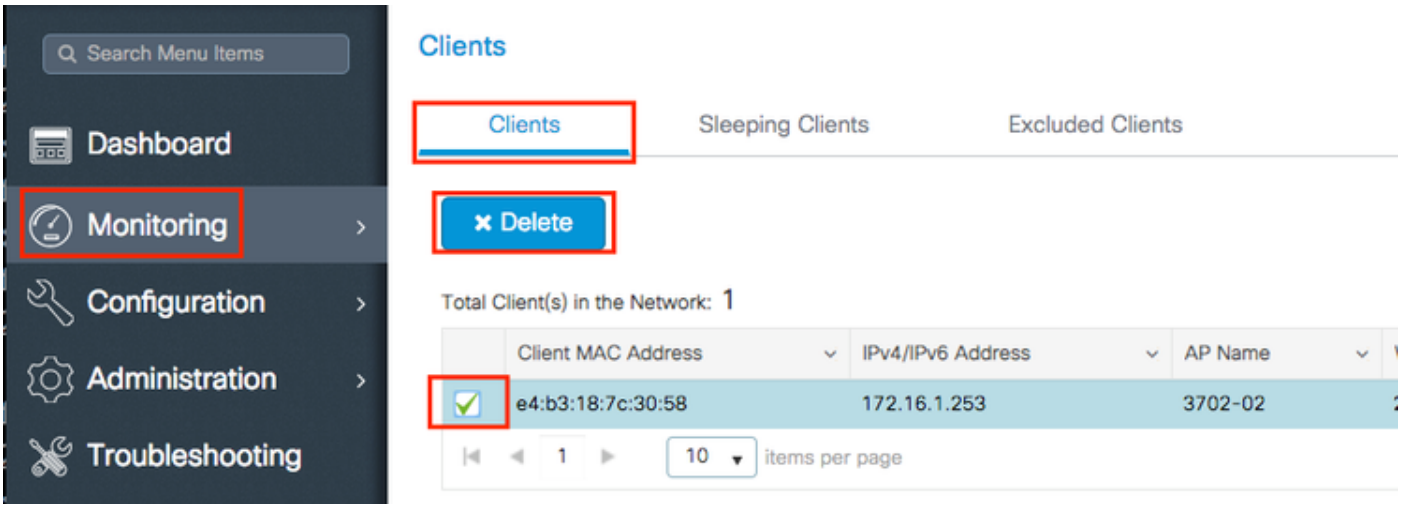
```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-sm] [8522]: (info): MAC: e4b3.187c.3058 Deleting
YYYY/DD/MM HH:MM:SS.xxx {mobilityd_R0-0}{1}: [mm-transition] [19496]: (info): MAC: e4b3.187c.3058 MMFSM
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-sm] [8522]: (note): MAC: e4b3.187c.3058 Client d
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-state] [8522]: (note): MAC: e4b3.187c.3058 Clien
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [9800 WLC-qos-client] [8522]: (ERR): MAC: e4b3.187c.3058 Fail
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [multicast-main] [8522]: (info): MAC: e4b3.187c.3058 No Flex/
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-iplearn] [8522]: (info): MAC: e4b3.187c.3058 IP-learn
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [dpath_svc] [8522]: (note): MAC: e4b3.187c.3058 Client datapa
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [mm-transition] [8522]: (info): MAC: e4b3.187c.3058 MMIF FSM
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [mm-client] [8522]: (ERR): MAC: e4b3.187c.3058 Invalid transm
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [wncd_0] [8522]: (info): Sanet App Event EV_SESSION_DELETE
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [auth-mgr] [8522]: (info): [e4b3.187c.3058:capwap_90000003] D
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [aaa-attr-inf] [8522]: (info): [ Applied attribute :bsn-vlan-
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [aaa-attr-inf] [8522]: (info): [ Applied attribute : timeout
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-auth] [8522]: (info): MAC: e4b3.187c.3058 Client auth
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [dot11] [8522]: (info): MAC: e4b3.187c.3058 Sent deauth to cl
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [dot11] [8522]: (info): MAC: e4b3.187c.3058 DOT11 state trans
```

Reason:

The client was manually removed from the network by either CLI:

```
# wireless client mac-address aaaa.bbbb.cccc deauthenticate
```

Or by GUI:



Solution:

None, normal behavior initiated by the user.

Disconnected due to EAP Timeout

Log example:

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [errmsg] [8681]: (note): %DOT1X-5-FAIL: Authentication failed
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [auth-mgr] [8681]: (info): [0874.0277.1345:capwap_90800003] A
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [auth-mgr] [8681]: (info): [0874.0277.1345:capwap_90800003] (
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [auth-mgr] [8681]: (info): [0874.0277.1345:capwap_90800003] R
.
.
.
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-orch-sm] [8681]: (info): MAC: 0874.0277.1345 Deleting
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-orch-sm] [8681]: (note): MAC: 0874.0277.1345 Client d
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-orch-state] [8681]: (note): MAC: 0874.0277.1345 Clien
.
.
.
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [mm-transition] [8681]: (info): MAC: 0874.0277.1345 MMIF FSM
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [mm-client] [8681]: (ERR): MAC: 0874.0277.1345 Client not pre
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [wncd_2] [8681]: (info): Sanet App Event EV_SESSION_DELETE
```

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [auth-mgr] [8681]: (info): [0874.0277.1345:capwap_90800003] D
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-auth] [8681]: (info): MAC: 0874.0277.1345 Client auth
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [dot11] [8681]: (info): MAC: 0874.0277.1345 Sent deauth to cl
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [dot11] [8681]: (info): MAC: 0874.0277.1345 DOT11 state trans
.
.
.
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-auth] [8681]: (info): MAC: 0874.0277.1345 Client auth
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [wncd_2] [8681]: (info): Sanet eventQ: EAP_CORE_MQ, message:2
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-orch-state] [8681]: (note): MAC: 0874.0277.1345 Clien
```

Reason:

The client is not responding to the Extensible Authentication Protocol (EAP) packet sent by the 9800 WLC within the EAP-Request Timeout interval nor the EAP-Request Max Retries times.

Possible solutions:

- Update wireless client drivers to the latest one
- Ensure wireless client trust RADIUS' certificate
- Increase the EAP-Request Timeout and/or the EAP-Request Max Retries

CLI:

```
# config t
# wireless security dot1x request retries <0-20>
# wireless security dot1x timeout <1-120 seconds>
```

GUI:

Navigate to Configuration > Security > Advanced EAP and customize the needed settings.

Disconnected due to AP Radio Reset

Log example:

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [apmgr-capwap-config] [8621]: (info): f07f.06ee.f590 Radio: 1
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [apmgr-db] [8621]: (note): MAC: f07f.06ee.f590 Radio 1 is dis
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [radio-history-reset] [8621]: (info): Radio reset of the AP f
YYYY/DD/MM HH:MM:SS.xxx {mobilityd_R0-0}{1}: [mm-transition] [19496]: (info): MAC: e4b3.187c.3058 MMFSM
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-orch-sm] [8621]: (info): MAC: e4b3.187c.3058 Deleting
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-orch-sm] [8621]: (note): MAC: e4b3.187c.3058 Client d
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-orch-state] [8621]: (note): MAC: e4b3.187c.3058 Clien
.
.
.
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [dpath_svc] [8621]: (note): MAC: e4b3.187c.3058 Client datapa
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [mm-transition] [8621]: (info): MAC: e4b3.187c.3058 MMIF FSM
```

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [mm-client] [8621]: (ERR): MAC: e4b3.187c.3058 Invalid transm
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [wncd_1] [8621]: (info): Sanet App Event EV_SESSION_DELETE
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [auth-mgr] [8621]: (info): [e4b3.187c.3058:capwap_90400003] D
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-auth] [8621]: (info): MAC: e4b3.187c.3058 Client auth
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [dot11] [8621]: (info): MAC: e4b3.187c.3058 Sent deauth to cl
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [dot11] [8621]: (info): MAC: e4b3.187c.3058 DOT11 state trans
```

Reason:

The AP with which the client was associated changed the channel or power, causing a radio reset.

Possible solutions:

- This is a normal behavior
- You could configure how often the 9800 WLC is allowed to make channel changes

CLI:

```
# config t
# ap dot11 { 5ghz | 24ghz } rrm channel dca interval <0-24>

Valid values 1,2,3,4,6,8,12 and 24 hours, 0 = 10 minutes (default)
```

GUI:

Navigate to **Configuration > Radio Configurations > RRM > 5 GHz Band/2.4 GHz Band > DCA > Increase Interval Setting.**

Disconnected due to Web Authentication Timeout

Log example:

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [auth-mgr] [8681]: (info): [0874.0277.1345:capwap_90800003] A
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [wncd_2] [8681]: (info): Sanet eventQ: AUTH_MGR_MQ, message:6
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [wncd_2] [8681]: (info): Sanet App Event EV_SESSION_AUTHC_FAI
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [auth-mgr] [8681]: (info): [0874.0277.1345:capwap_90800003] A
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [9800 WLC-infra-evq] [8681]: (ERR): Authc failure for mac 087
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [auth-mgr] [8681]: (info): [0874.0277.1345:capwap_90800003] S
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [errmsg] [8681]: (note): %SESSION_MGR-5-FAIL: Authorization f
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [auth-mgr] [8681]: (info): [0874.0277.1345:capwap_90800003] A
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [wncd_2] [8681]: (info): Sanet App Event EV_SESSION_AUTHZ_FAI
.
.
.
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-auth] [8681]: (info): MAC: 0874.0277.1345 Client auth
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-auth] [8681]: (ERR): MAC: 0874.0277.1345 L3 Authentic
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-auth] [8681]: (info): MAC: 0874.0277.1345 Client auth
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [9800 WLC-infra-evq] [8681]: (ERR): WLAN profile = prof-name,
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-orch-sm] [8681]: (info): MAC: 0874.0277.1345 Deleting
```

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-orch-sm] [8681]: (note): MAC: 0874.0277.1345 Client d
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-orch-state] [8681]: (note): MAC: 0874.0277.1345 Clien
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [9800 WLC-qos-client] [8681]: (ERR): MAC: 0874.0277.1345 Fail
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [multicast-main] [8681]: (info): MAC: 0874.0277.1345 No Flex/
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-iplearn] [8681]: (info): MAC: 0874.0277.1345 IP-learn
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [dpath_svc] [8681]: (note): MAC: 0874.0277.1345 Client datapa
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [mm-transition] [8681]: (info): MAC: 0874.0277.1345 MMIF FSM
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [mm-client] [8681]: (ERR): MAC: 0874.0277.1345 Invalid transm
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [wncd_2] [8681]: (info): Sanet App Event EV_SESSION_DELETE
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [auth-mgr] [8681]: (info): [0874.0277.1345:capwap_90800003] D
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [aaa-attr-inf] [8681]: (info): [ Applied attribute :bsn-vlan-
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [aaa-attr-inf] [8681]: (info): [ Applied attribute : timeout
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [client-auth] [8681]: (info): MAC: 0874.0277.1345 Client auth
YYYY/DD/MM HH:MM:SS.xxx {mobilityd_R0-0}{1}: [mm-transition] [19496]: (info): MAC: 0874.0277.1345 MMFSM
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-2}{1}: [dot11] [8681]: (info): MAC: 0874.0277.1345 DOT11 state trans
```

Reason:

The client did not complete the web authentication within the allowed time (around 120 seconds).

Solution:
Ensure clients complete web authentication within 120 seconds.

Disconnected due to Session Timeout

Log example:

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-auth] [8621]: (info): MAC: e4b3.187c.3058 Client auth
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-orch-sm] [8621]: (info): MAC: e4b3.187c.3058 Deleting
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-orch-sm] [8621]: (note): MAC: e4b3.187c.3058 Client d
YYYY/DD/MM HH:MM:SS.xxx {mobilityd_R0-0}{1}: [mm-transition] [19496]: (info): MAC: e4b3.187c.3058 MMFSM
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-orch-state] [8621]: (note): MAC: e4b3.187c.3058 Clien
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [9800 WLC-qos-client] [8621]: (ERR): MAC: e4b3.187c.3058 Fail
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [multicast-main] [8621]: (info): MAC: e4b3.187c.3058 No Flex/
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-iplearn] [8621]: (info): MAC: e4b3.187c.3058 IP-learn
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [dpath_svc] [8621]: (note): MAC: e4b3.187c.3058 Client datapa
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [mm-transition] [8621]: (info): MAC: e4b3.187c.3058 MMIF FSM
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [mm-client] [8621]: (ERR): MAC: e4b3.187c.3058 Invalid transm
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-auth] [8621]: (info): MAC: e4b3.187c.3058 Client auth
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [dot11] [8621]: (info): MAC: e4b3.187c.3058 Sent deauth to cl
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [dot11] [8621]: (info): MAC: e4b3.187c.3058 DOT11 state trans
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-orch-state] [8621]: (note): MAC: e4b3.187c.3058 Clien
```

Reason:

The client reached its session timeout.

Possible solutions:

- This is a normal behavior
- Increase the policy profile session timeout associated with the SSID

CLI:

```
# config t
# wireless profile policy <policy-profile-name>
# shutdow
# session-timeout <20-86400 seconds>
# no shutdown
```

GUI:

Navigate to Configuration > Tags & Profiles > Policy > Policy Profile Name > Advanced > WLAN Timeout and customize timers as needed.

Disconnected due to Idle Timeout

Log example:

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-sm] [7807]: (note): MAC: e4b3.187c.3058 Client d
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-state] [7807]: (note): MAC: e4b3.187c.3058 Clien
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [9800 WLC-qos-client] [7807]: (ERR): MAC: e4b3.187c.3058 Fail
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [dpath_svc] [7807]: (note): MAC: e4b3.187c.3058 Client datapa
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [mm-client] [7807]: (ERR): MAC: e4b3.187c.3058 Invalid transm
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-state] [7807]: (note): MAC: e4b3.187c.3058 Clien
```

Reason:

The client did not send traffic (or enough traffic) within the idle timeout configured interval.

Possible solutions:

- This is a normal behavior
- Customize the policy profile idle settings associated with the SSID

CLI:

```
# config t
# wireless profile policy <policy-profile-name>
# shutdow
# idle-timeout <15-100000 seconds>
# idle-threshold  <0-4294967295 bytes>
# no shutdown
```

GUI:

Navigate to Configuration > Tags & Profiles > Policy > Policy Profile Name > Advanced > WLAN Timeout and customize the idle settings as needed.

Note: If you do not configure the idle-threshold, the client needs to send any amount of traffic within the idle-timeout period to not get disconnected. If you configure the idle-threshold, the client must send that amount of bytes within the idle-timeout to not get disconnected (that is, you configure an idle-threshold of 10 bytes and an idle-timeout of 30 seconds, the wireless clients need to send at least 10 bytes of traffic every 30 seconds to not be disconnected from the network).

The Client Moved Between SSIDs

Log example:

```
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-sm] [7807]: (note): MAC: e4b3.187c.3058 Associat
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-sm] [7807]: (ERR): MAC: e4b3.187c.3058 Failed to
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-state] [7807]: (note): MAC: e4b3.187c.3058 Client
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-sm] [7807]: (note): MAC: e4b3.187c.3058 Client de
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-state] [7807]: (note): MAC: e4b3.187c.3058 Client
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [9800 WLC-qos-client] [7807]: (ERR): MAC: e4b3.187c.3058 Fail
YYYY/DD/MM HH:MM:SS.xxx {fman_fp_F0-0}{1}: [wireless-client] [10254]: UUID: 1000000006930, ra: 5 (note)
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [dpath_svc] [7807]: (note): MAC: e4b3.187c.3058 Client datapa
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [mm-client] [7807]: (ERR): MAC: e4b3.187c.3058 Invalid transm
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-0}{1}: [client-orch-state] [7807]: (note): MAC: e4b3.187c.3058 Client
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-orch-sm] [8009]: (note): MAC: e4b3.187c.3058 Associat
YYYY/DD/MM HH:MM:SS.xxx {wncd_x_R0-1}{1}: [client-orch-state] [8009]: (note): MAC: e4b3.187c.3058 Client
```

Reason:

The client was connected to an SSID and moved to a different one.

Possible solutions:

- Normal behavior
- Remove the 2nd SSID from the client