# Troubleshoot Central Web Authentication (CWA) with Wireless Lan Controller (WLC) 9800 and Identity Services Engine (ISE)

## Contents



## Introduction

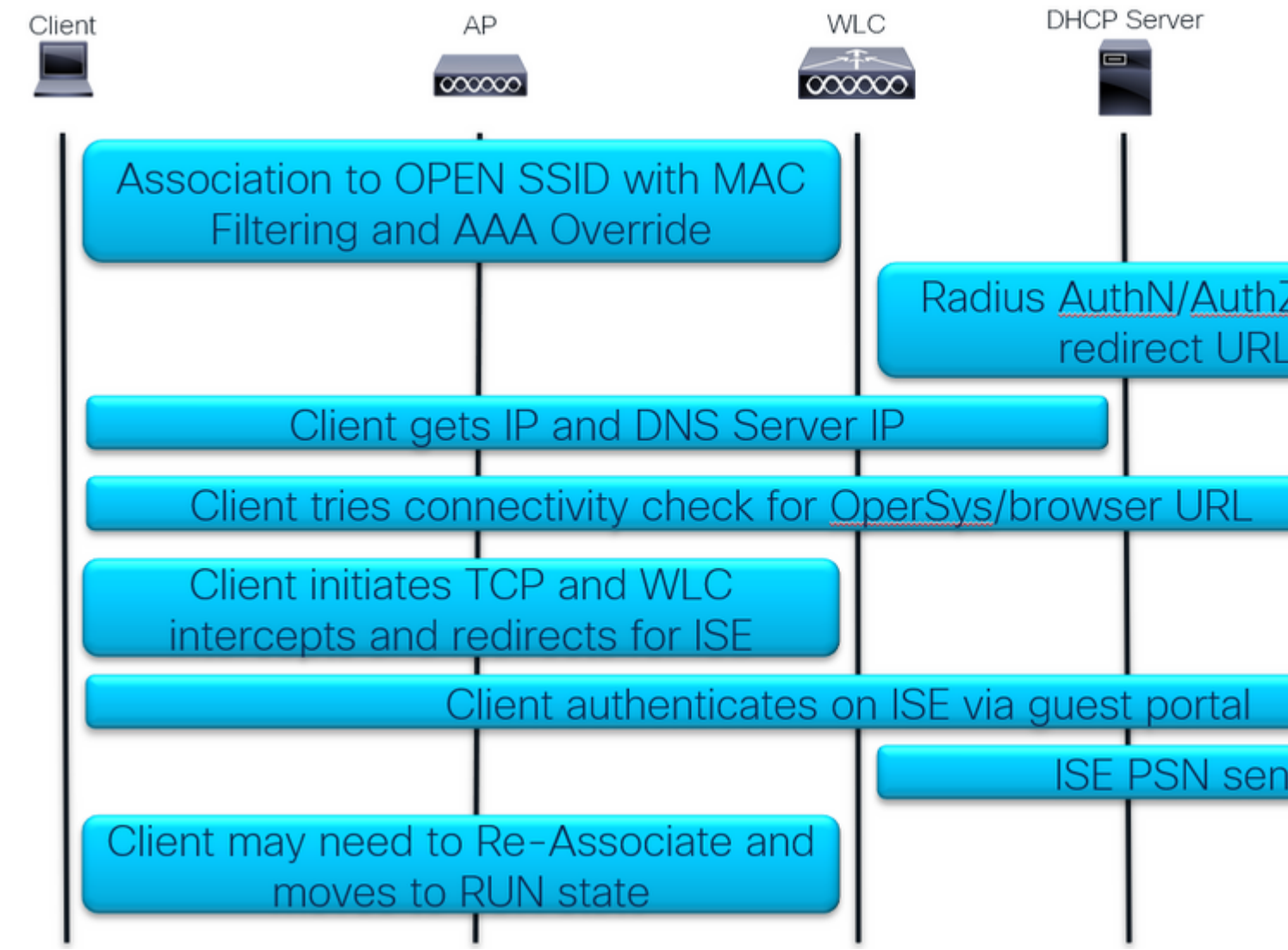
This document describes how to troubleshoot Central Web Authentication (CWA) with WLC 9800 and ISE.

## Background Info

There are so many personal devices currently that network administrators that look for securing Wireless access normally opt for Wireless networks that use CWA.
In this document, we focus on the flow chart of CWA, that helps in the troubleshooting of the common issues that affect us.
We look at the common gotchas of the process, how to collect logs related to CWA, how to analyze these logs, and how to collect an embedded packet capture on the WLC to confirm traffic flow.

CWA is the most common setup for companies that allow users to connect to the company network using their personal devices, also known as BYOD.
Any network administrator is interested in the gotchas and troubleshooting steps to perform to fix their problems prior to opening a TAC case.

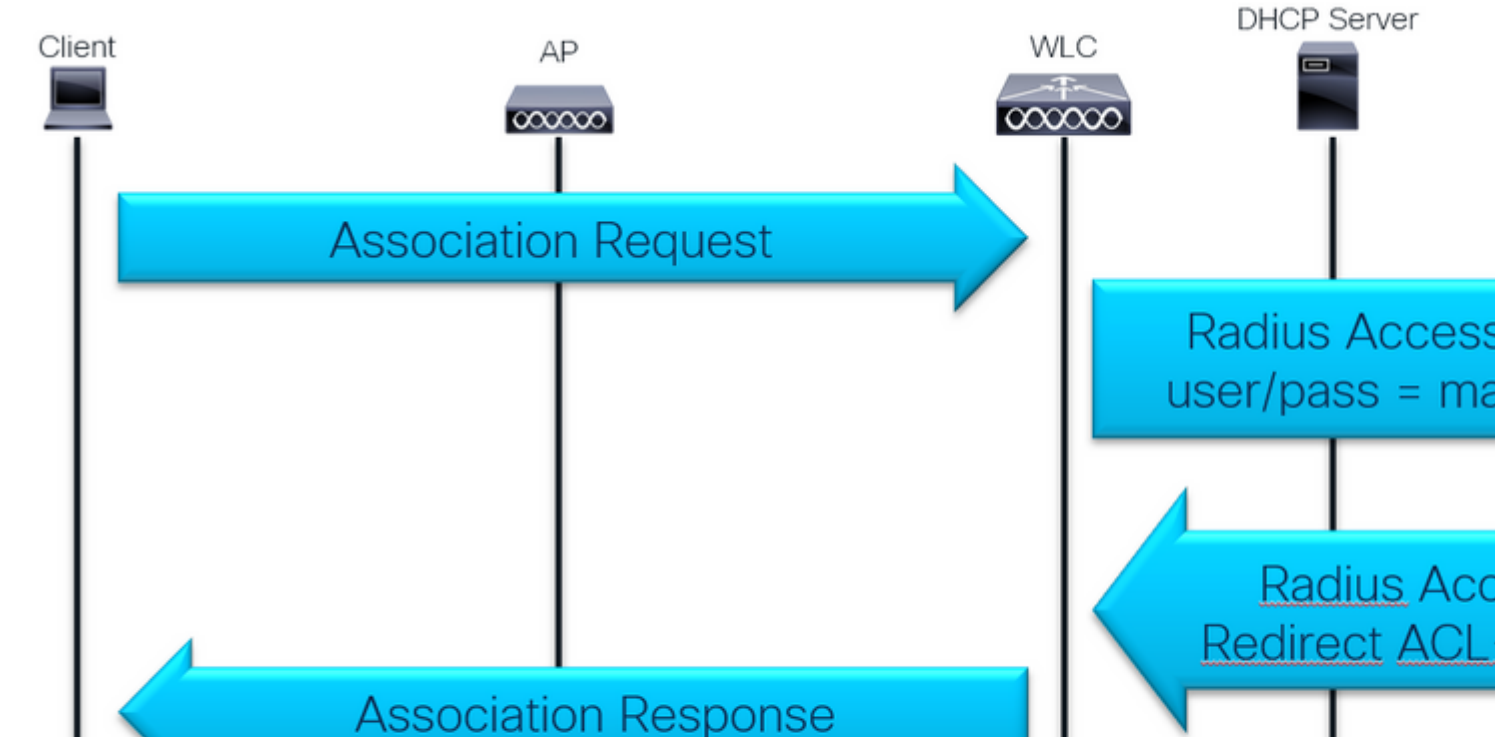
Here is the CWA packet flow:




*CWA Packet Flow*

## Detailed flow

First Association and RADIUS Authentication:



: On version 17.4.X and later, ensure to also configure the CoA server key when you configure the RADIUS server. Use the same key as the shared secret (they are the same by default on ISE). The purpose is to optionally configure a different key for CoA than the shared secret if that is what your RADIUS server configured. In Cisco IOS® XE 17.3, the web UI simply used the same shared secret as CoA key.

---

As from version 17.6.1, RADIUS (including CoA) is supported through this port. If you want to use the Service Port for RADIUS then you need this configuration:

<#root>

```
aaa server radius dynamic-author
 client 10.48.39.28
```

**vrf**

**Mgmt-intf**

```
 server-key cisco123

interface GigabitEthernet0
```

**vrf**

**forwarding**

**Mgmt-intf**

```
 ip address x.x.x.x x.x.x.x

!if using aaa group server:
aaa group server radius group-name
 server name nicoISE
```

**ip**

**vrf**

**forwarding**

**Mgmt-intf**

**ip**

**radius**

```
source

-interface GigabitEthernet0
```

# Conclusion

**This is the resumed CWA checklist:**

- Make sure client sits on correct VLAN and gets IP address and DNS.
  - Get client details at WLC and run packet captures to see DHCP exchange.
- Verify that client can resolve hostnames via DNS.
  - Ping hostname from cmd.
- WLC must be listening on port 80
  - Verify global command *ip http server* or global parameter map command *webauth-http-enable*.
- To get rid of certificate warning, install trusted certificate on ISE.
  - No need to install trusted certificate on WLC in CWA.
- Authentication Policy at ISE Advanced option â€œContinueâ€ If user not found
  - To allow sponsored Guest users to connect and get URL Redirect and ACL.

**And the main tools used in the troubleshoot:**

- WLC EPC
  - Inner filters: DHCP protocol, mac address.
- WLC Monitor
  - Check client security details.
- WLC RA tracing
  - Debugs with detailed info at WLC side.
- ISE Live Logs
  - Authentication details.
- ISE TCPDump
  - Collect packet captures at ISE PSN interface.

# References

Configure Central Web Authentication (CWA) on Catalyst 9800 WLC and ISE