Configure and Verify Layer 3 Security in Wi-Fi 6E WLANs

Contents

Introduction

This document describes how to configure Layer 3 security in Wi-Fi 6E WLANs and what to expect on different clients.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Wireless Lan Controllers (WLC) 9800
- Cisco Access Points (APs) that support Wi-Fi 6E.
- IEEE Standard 802.11ax.
- Tools: Wireshark v4.0.6

Components Used

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

- WLC 9800-CL with IOS® XE 17.9.4.
- APs C9136, CW9162, CW9164 and CW9166.
- Wi-Fi 6E Clients:

- Lenovo X1 Carbon Gen11 with Intel AX211 Wi-Fi 6 and 6E Adapter with driver version 22.200.2(1).
- Mobile Phone Pixel 6a with Android 13;
- Mobile Phone Samsung S23 with Android 13.

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

The key thing to know is that Wi-Fi 6E is not an entirely new standard, but an extension. At its base, Wi-Fi 6E is an extension of the Wi-Fi 6 (802.11ax) wireless standard into the 6-GHz radio-frequency band.

Wi-Fi 6E builds on Wi-Fi 6, which is the latest generation of the Wi-Fi standard, but only Wi-Fi 6E devices and applications can operate in the 6-GHz band.

Layer 3 Security in WiFi 6E is the same as in WiFi 5 or 6, is a sense that the Web authentication flow does not differ in any scenario. The only difference of having Layer 3 Security in WiFI 6E is the fact that any WLAN in WiFI 6E must have Layer 2 security configured with WPA3 and PMF which are mandatory in WiFi 6E.

To know more about WiFi 6E Layer 2 security, please go through the document: Configure and Verify Wi-Fi 6E WLAN Layer 2 Security .

Web Authentication

Web authentication is a Layer 3 security solution designed for providing easy and secure guest access to hosts on WLAN with open authentication or appropriate layer 2 security methods.

These are the different types of web authentication methods:

- Local Web Authentication (LWA): Configured as Layer 3 security on the controller, the web authentication page and the pre-authentication ACL are locally configured on the controller. The controller intercepts htttp(s) traffic and redirects the client to the internal web page for authentication. The credentials entered by the client on the login page is authenticated by the controller locally or through a RADIUS or LDAP server.

- External Web Authentication (EWA): Configured as Layer 3 security on the controller, the controller intercepts htttp(s) traffic and redirects the client to the login page hosted on the external web server. The credentials entered by the client on the login page is authenticated by the controller locally or through a RADIUS or LDAP server. The pre-authentication ACL is configured statically on the controller.

- Central Web Authentication (CWA): Configured mostly as Layer 2 security on the controller, the redirection URL and the pre-authentication ACL reside on ISE and are pushed during layer 2 authentication to the controller. The controller redirects all web traffic from the client to the ISE login page. ISE validates the credentials entered by the client through HTTPS and authenticates the user.

You can find more details in the document Web-Based Authentication on Cisco Catalyst 9800 Series Controllers .

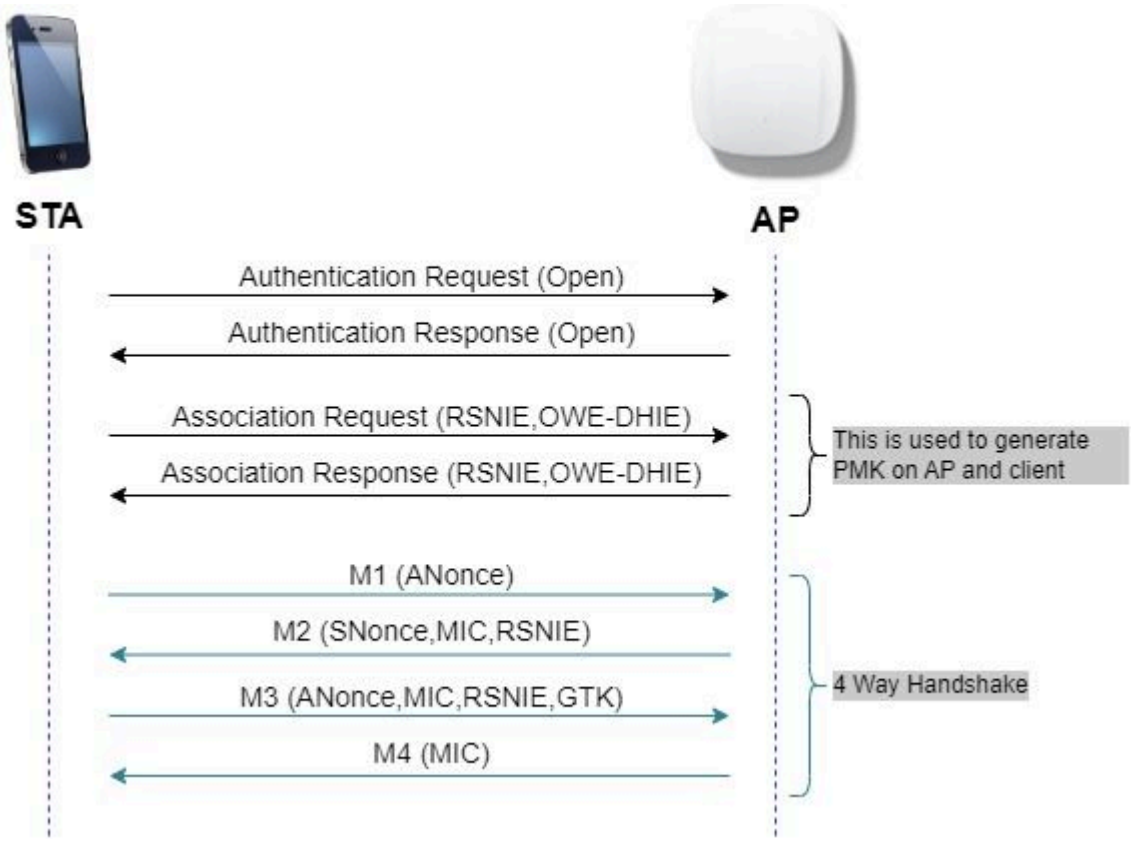
Traditionally, Wi-Fi hotspots and guest WLANs have used open security without encryption or authentication. The Wi-Fi CERTIFIED Enhanced Open certification defines improved data privacy in open

Wi-Fi networks.

This certification is based on the Opportunistic Wireless Encryption (OWE) protocol. OWE is defined in the IETF RFC 8110. The OWE protocol integrates established cryptography mechanisms to provide each user with unique individual encryption, protecting the data exchange between the user and the access point.

The OWE uses the Diffie-Hellman algorithms based Cryptography to setup the wireless encryption. With OWE, the client and AP perform a Diffie-Hellman key exchange during the access procedure and use the resulting pairwise master key (PMK) secret with the 4-way handshake.

As shown in the next diagram, standard open authentication and association occur, and then the 4-Way Handshake process generates the necessary keys for encryption.



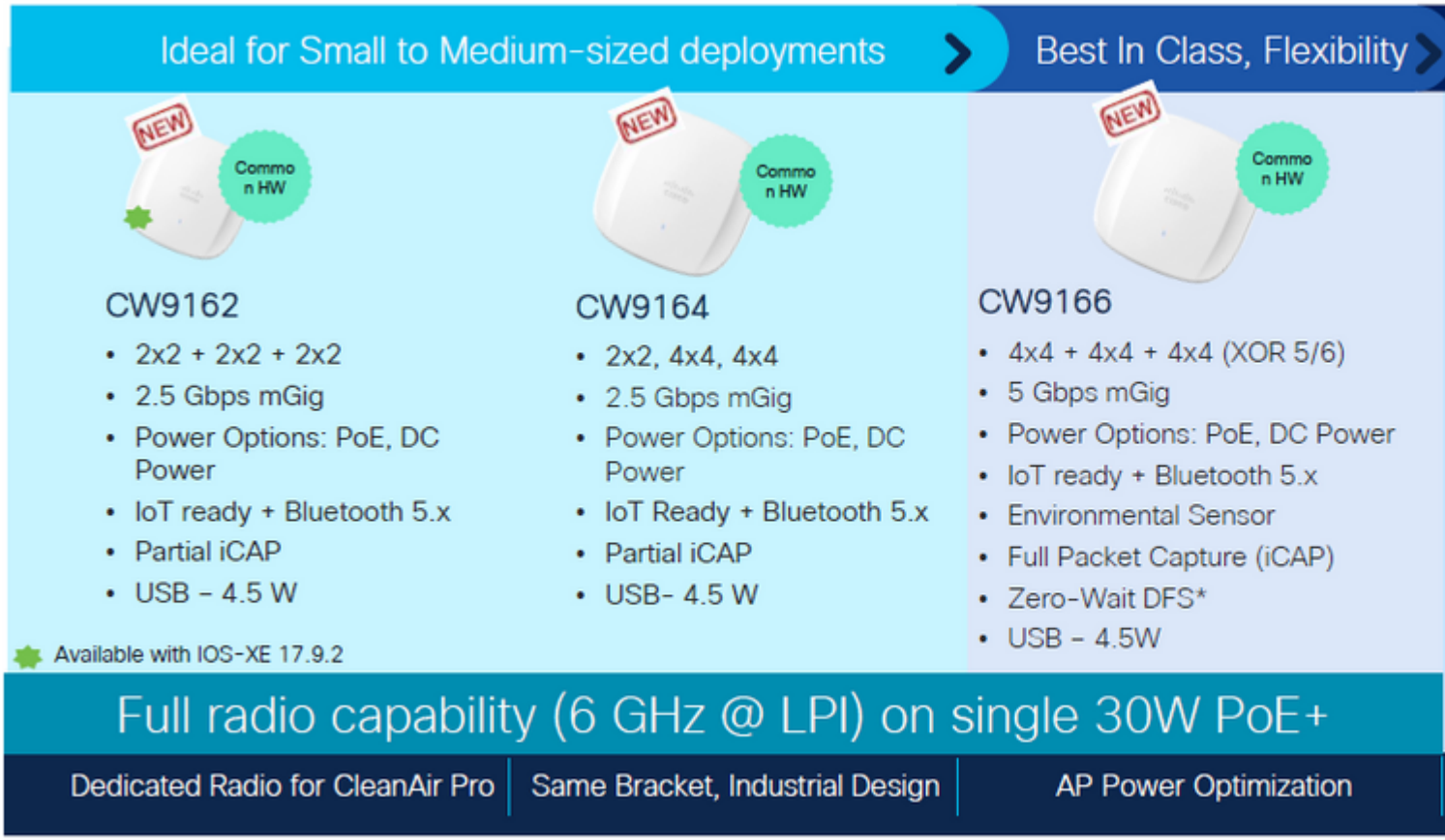
OWE frame exchange

You can find more details in the document Configure Enhanced Open SSID with Transition Mode - OWE .

OWE is the natural successor of an Open network in WiFi 6E, therefore, in this document, we use OWE as layer 2 security for WiFi6E compliance.

Cisco Catalyst Wi-Fi 6E APs

Quick reference to the WiFi 6E APs available at the time of writting this doc:



Wi-Fi 6E Access Points

Configure and Verify

In this section, we show how to configure and verify the connection of WiFi 6E clients to a WLAN using L3 Authentication.

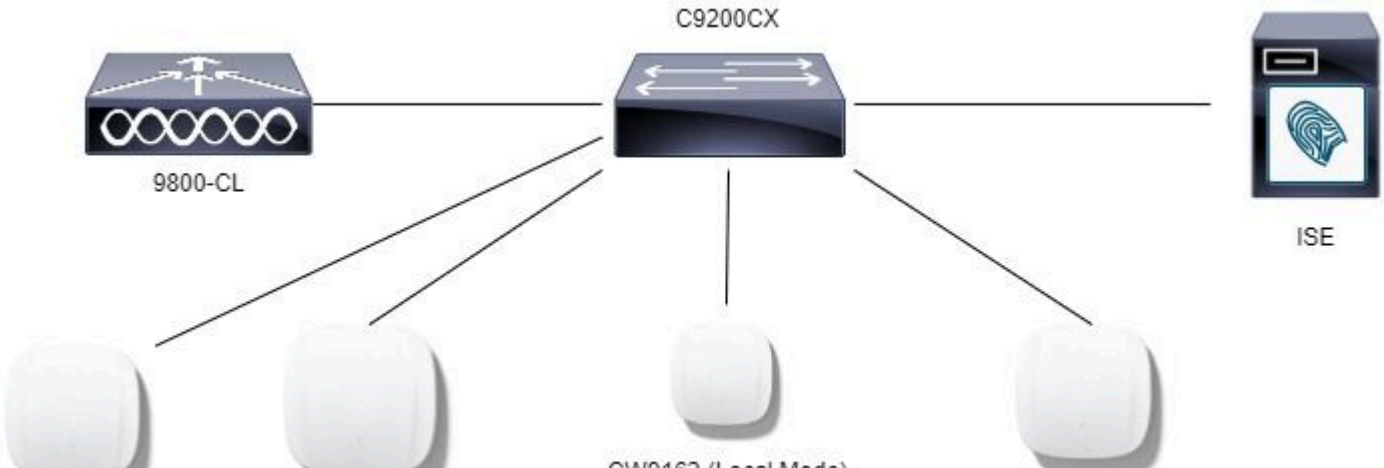
The Layer 2 Security settings are be locked to Opportunistic Wireless Encryption (OWE) which is the closest to an "Open" network we can have in WiFi 6E.

We configure and verify these types of web authentication with WiFi 6E:

- Local Web Authentication
- External Web Authentication
- Central Web Authentication

Network Diagram

This is the lab setup diagram used in this document.



```
aaa new-model
!
aaa group server radius ISE_RADIUS
 server name PSN01
 deadtime 5
 load-balance method least-outstanding
 subscriber mac-filtering security-mode mac
 mac-delimiter colon
!
aaa authentication login LWA_Radius group ISE_RADIUS
!
parameter-map type webauth global
 type webauth
 virtual-ip ipv4 192.0.2.1
 trustpoint eWLC-9800-01_WLC_TP
 webauth-http-enable
!
parameter-map type webauth LocalWebAuth
 type webauth
 timeout init-state sec 60
 max-http-conns 10
 custom-page login device bootflash:/custom_webauth/login.html
 custom-page success device bootflash:/custom_webauth/aup.html
 custom-page failure device bootflash:/custom_webauth/failed.html
 custom-page login expired device bootflash:/custom_webauth/logout.html
!
radius server PSN01
 address ipv4 192.168.1.7 auth-port 1812 acct-port 1813
 key 7 xxxxxxxxxxxx
!
wireless profile policy CentralSwPolicyProfile
!
 ipv4 dhcp required
 vlan default
 no shutdown
!
wireless tag policy Wifi6E_TestPolicy
 wlan wifi6E_test policy CentralSwPolicyProfile
!
wlan wifi6E_test 5 wifi6E_test
 dot11ax target-waketime
 dot11ax twt-broadcast-support
 radio policy dot11 6ghz
 no security ft adaptive
 no security wpa wpa2
 no security wpa akm dot1x
 security wpa akm owe
 security wpa wpa3
 security dot1x authentication-list ISE_RADIUS
 security pmf mandatory
 security web-auth
 security web-auth authentication-list LWA_Radius
 security web-auth parameter-map LocalWebAuth
 no shutdown
!
```

Here we can observe the OWE phase using AX211 client in this example. To note that this is an EPC at the

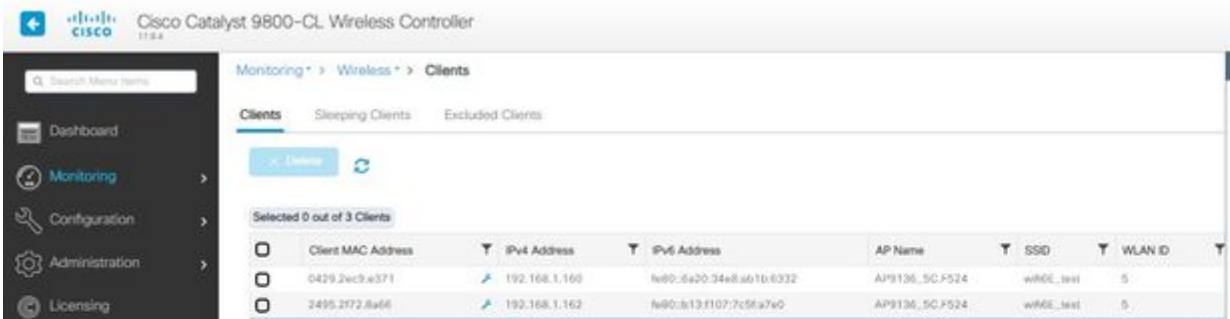
WLC interface:

LWA OWE Association

Followed by the DHCP, DNS and HTTP redirection:

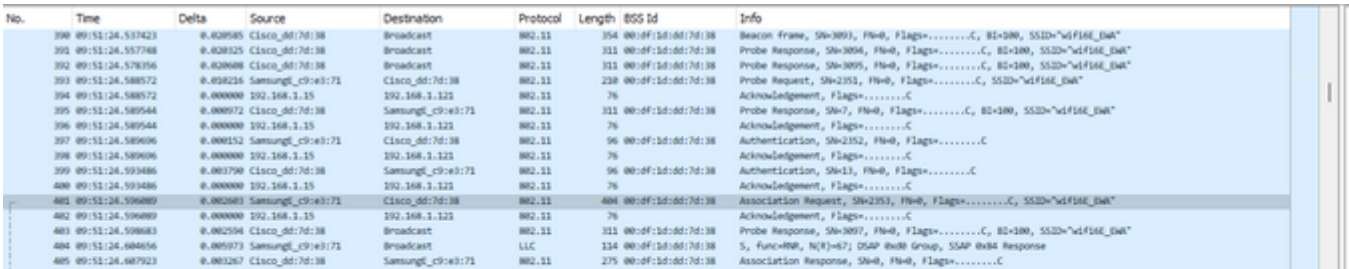
LWA OWE Redirection

On the WLC GUI we can see the client details:



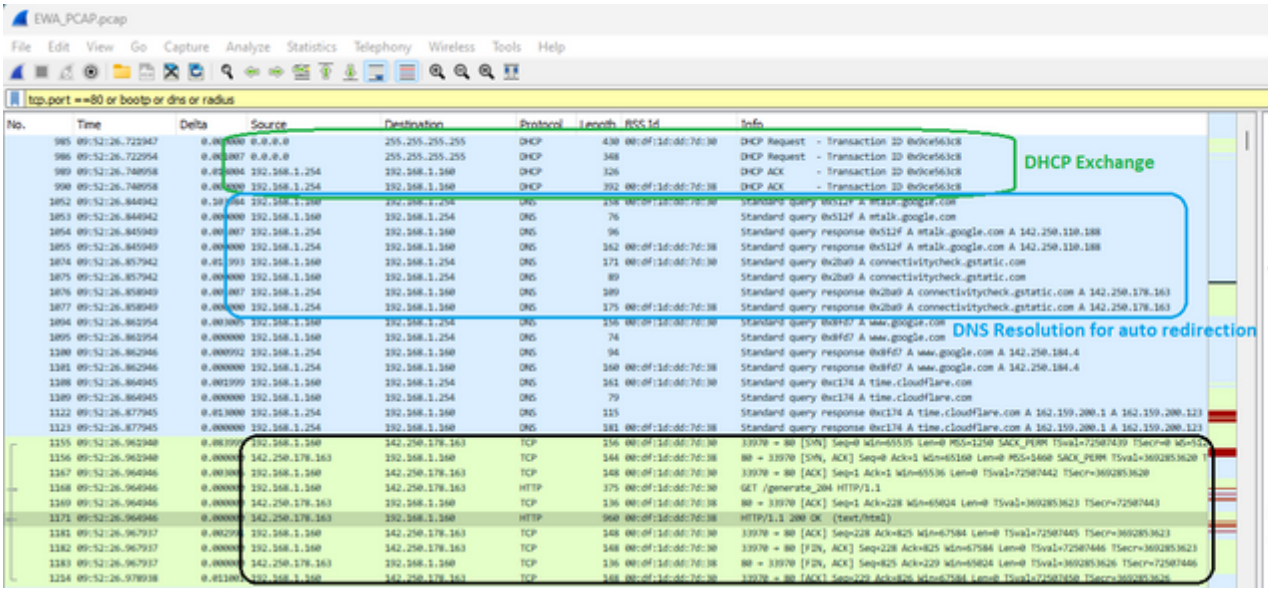
```
aaa new-model
!
aaa group server radius ISE_RADIUS
 server name PSN01
 deadtime 5
 load-balance method least-outstanding
 subscriber mac-filtering security-mode mac
 mac-delimiter colon
!
aaa authentication login EWA_Radius group ISE_RADIUS
!
parameter-map type webauth global
 type webauth
 virtual-ip ipv4 192.0.2.1
 trustpoint eWLC-9800-01_WLC_TP
 webauth-http-enable
!
parameter-map type webauth ExternalWebAuth
 type webauth
 timeout init-state sec 60
 redirect for-login https://192.168.1.17/EWAPortal/login.html
 redirect append ap-mac tag ap_mac
 redirect append client-mac tag client_mac
 redirect append wlan-ssid tag ssid


 redirect portal ipv4 192.168.1.17
 max-http-conns 10
!
radius server PSN01
 address ipv4 192.168.1.7 auth-port 1812 acct-port 1813
 key 7 xxxxxxxxxxxx
!
wireless profile policy CentralSwPolicyProfile
!
 ipv4 dhcp required
 vlan default
 no shutdown
!
wireless tag policy Wifi6E_TestPolicy
 wlan wifi6E_EWA policy CentralSwPolicyProfile
!
wlan wifi6E_EWA 6 wifi6E_EWA
 radio policy dot11 6ghz
 no security ft adaptive
 no security wpa wpa2
 no security wpa akm dot1x
 security wpa akm owe
 security wpa wpa3
 security pmf mandatory
 security web-auth
 security web-auth authentication-list EWA_Radius
 security web-auth parameter-map ExternalWebAuth
 no shutdown
!
```

Here we can observe the OWE phase OTA using Samsung S23 as example:



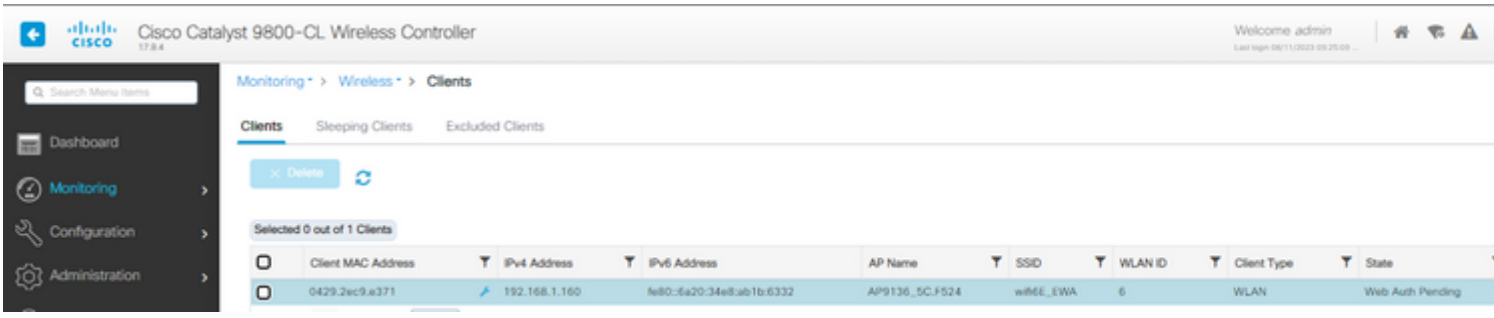
OWE detail in EWA WLAN Association/Authentication

Followed by the DHCP, DNS and HTTP redirection. Please note that this capture is the view via EPC at the WLC because OTA the traffic is encrypted:

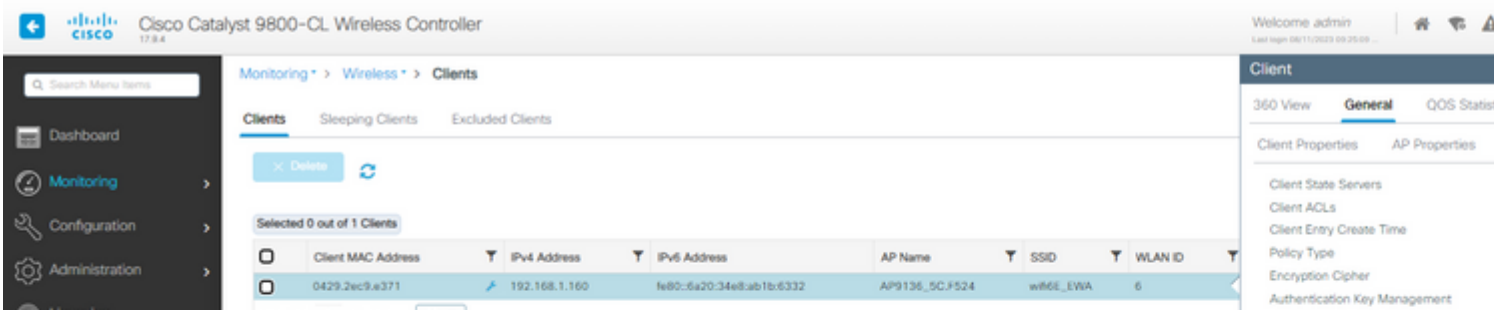


Packet capture detail on EWA

At this stage the client is in Web Auth Pending:

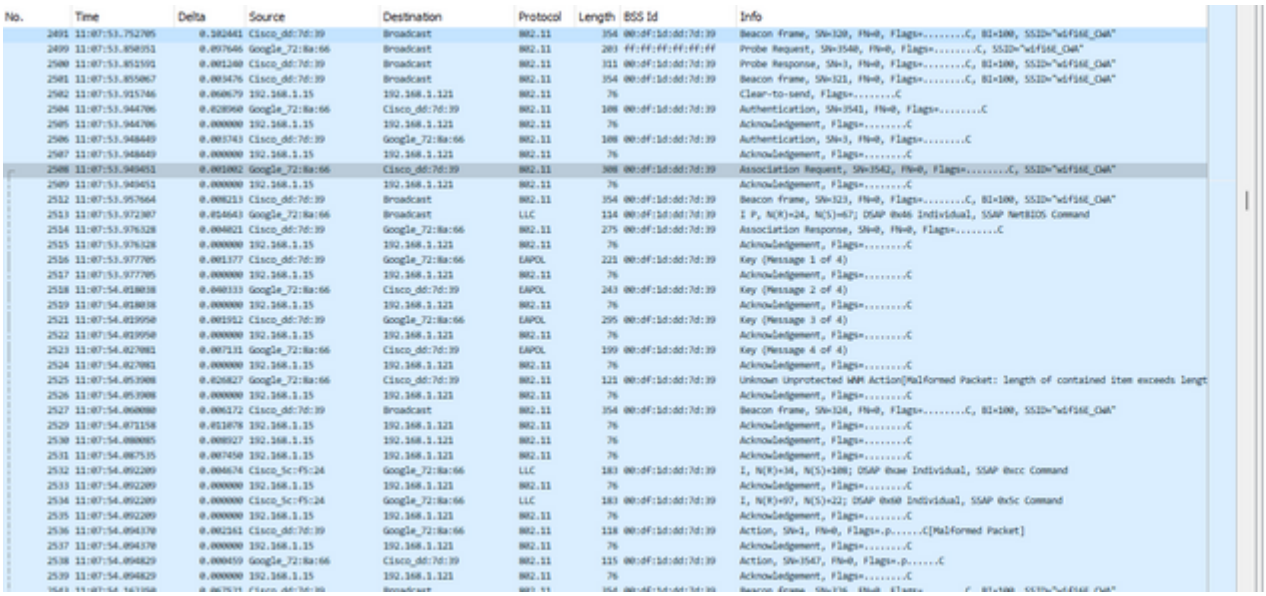


EWA client in Web Auth Pending



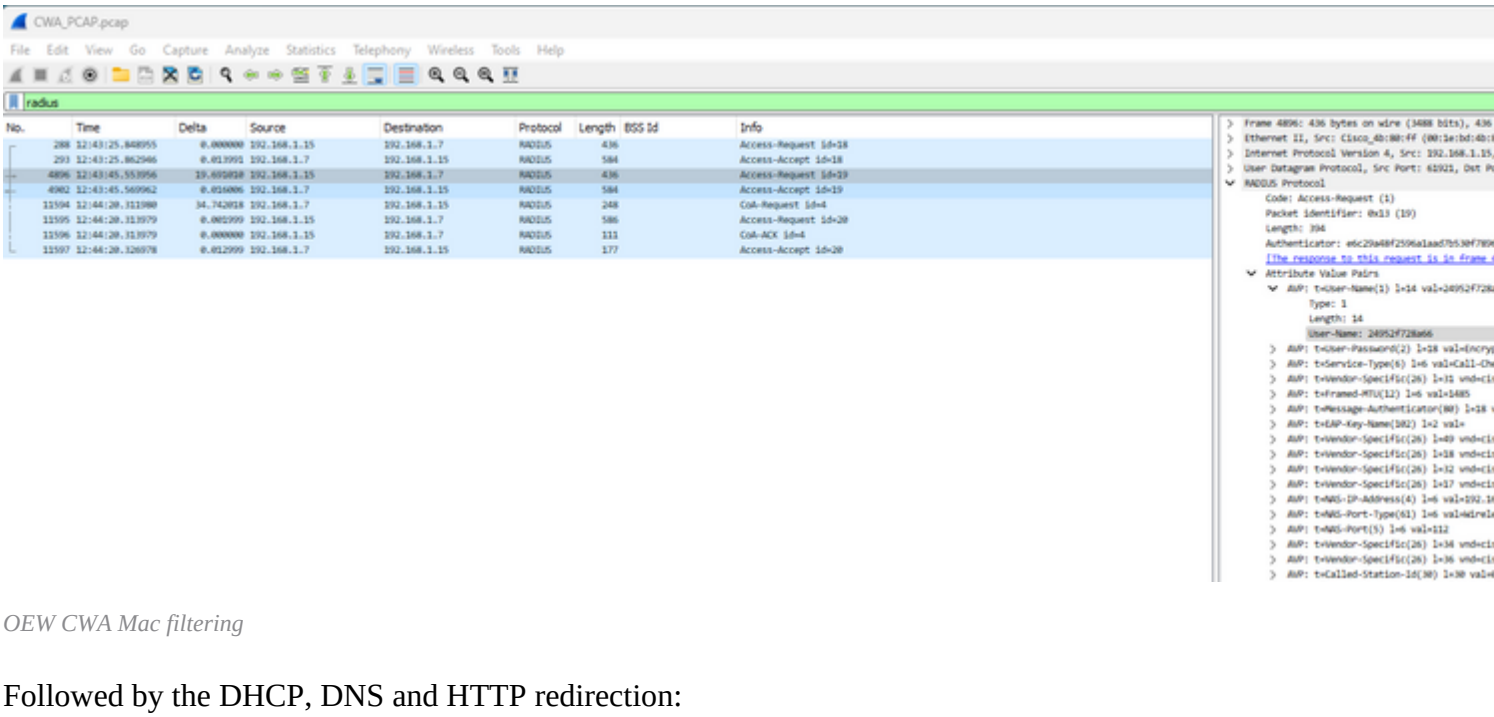
```
aaa new-model
!
aaa group server radius ISE_RADIUS
 server name PSN01
 deadtime 5
 load-balance method least-outstanding
 subscriber mac-filtering security-mode mac
 mac-delimiter colon
!
aaa authorization network RadiusAuthor group ISE_RADIUS local
!
parameter-map type webauth global
 type webauth
 virtual-ip ipv4 192.0.2.1
 trustpoint eWLC-9800-01_WLC_TP
 webauth-http-enable
!
radius server PSN01
 address ipv4 192.168.1.7 auth-port 1812 acct-port 1813
 key 7 xxxxxxxxxxxx
!
wireless profile policy CentralSwPolicyProfile
!
 ipv4 dhcp required
 vlan default
 no shutdown
!
wireless tag policy Wifi6E_TestPolicy
 wlan wifi6E_CWA policy CentralSwPolicyProfile
!
wlan wifi6E_CWA 7 wifi6E_CWA
 mac-filtering RadiusAuthor
 radio policy dot11 6ghz
 no security ft adaptive
 no security wpa wpa2
 no security wpa akm dot1x
 security wpa akm owe
 security wpa wpa3
 security pmf mandatory
 no shutdown
!
```

Here we can observe the OWE phase OTA using Pixel 6a as example:



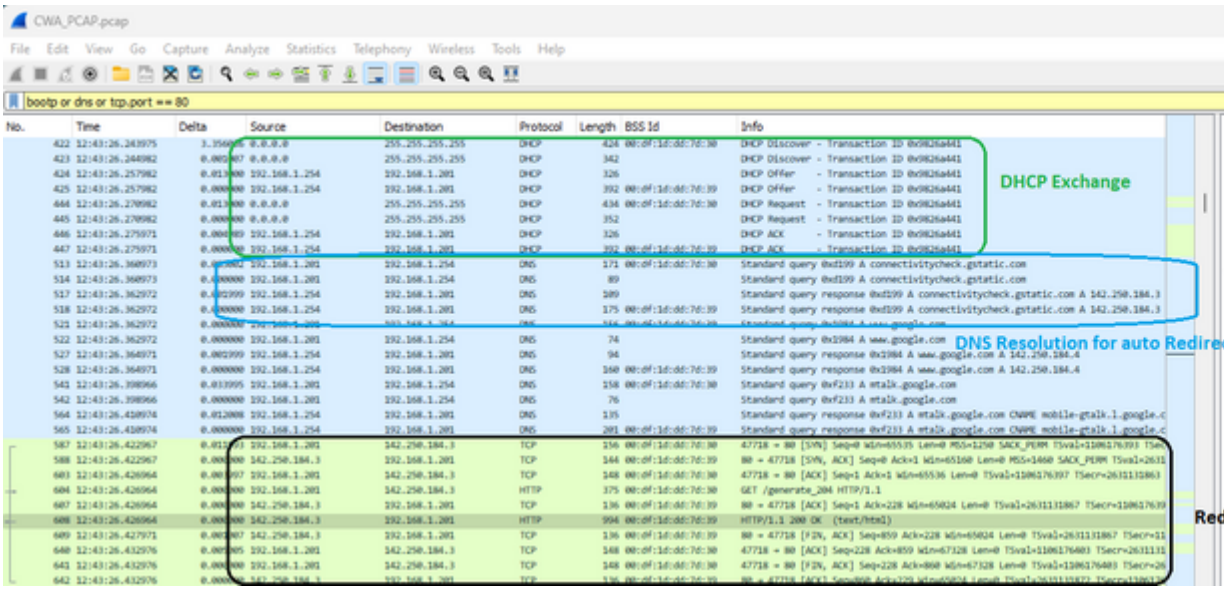
CWA OWE OTA connection

Then we have the Radius Exchange for the mac filtering:



OEW CWA Mac filtering

Followed by the DHCP, DNS and HTTP redirection:



CWA DHCP, DNS and Redirection

```
[...]
2023/08/08 13:37:58.198092314 {wncd_x_R0-0}{1}: [dot11] [15154]: (note): MAC: 286b.3598.580f

Association success

. AID 36, Roaming = False, WGB = False, 11r = False, 11w = True Fast roam = False
[...]
2023/08/08 13:37:58.198287303 {wncd_x_R0-0}{1}: [client-orch-sm] [15154]: (debug): MAC: 286b.359
2023/08/08 13:37:58.198308994 {wncd_x_R0-0}{1}: [client-orch-state] [15154]: (note): MAC: 286b.3

Client state transition: S_CO_ASSOCIATING -> S_CO_L2_AUTH_IN_PROGRESS


[...]
2023/08/08 13:37:58.200859342 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [15154]: (note):

Authentication Success

. Resolved Policy bitmap:11 for client 286b.3598.580f
[...]
2023/08/08 13:37:58.222523865 {wncd_x_R0-0}{1}: [client-auth] [15154]: (info): MAC: 286b.3598.58

Client auth-interface state transition: S_AUTHIF_ADD_MOBILE_ACK_WAIT_KM -> S_AUTHIF_PSK_AUTH_KEY_XCHNG_P


2023/08/08 13:37:58.222547149 {mobilityd_R0-0}{1}: [mm-client] [16404]: (debug): MAC: 0000.0000.
2023/08/08 13:37:58.222630557 {mobilityd_R0-0}{1}: [mm-dgram-io] [16404]: (debug): MAC: 0000.000
2023/08/08 13:37:58.222641428 {mobilityd_R0-0}{1}: [mm-dgram-io] [16404]: (debug): MAC: 0000.000
2023/08/08 13:37:58.222666535 {wncd_x_R0-0}{1}: [client-keymgmt] [15154]: (info): MAC: 286b.3598
2023/08/08 13:37:58.222678418 {wncd_x_R0-0}{1}: [client-keymgmt] [15154]: (info): MAC: 286b.3598
2023/08/08 13:37:58.227626495 {wncd_x_R0-0}{1}: [client-keymgmt] [15154]: (info): MAC: 286b.3598
2023/08/08 13:37:58.227791247 {wncd_x_R0-0}{1}: [client-keymgmt] [15154]: (info): MAC: 286b.3598
2023/08/08 13:37:58.227792680 {wncd_x_R0-0}{1}: [client-keymgmt] [15154]: (info): MAC: 286b.3598
2023/08/08 13:37:58.230572903 {wncd_x_R0-0}{1}: [client-keymgmt] [15154]: (info): MAC: 286b.3598
2023/08/08 13:37:58.230575999 {wncd_x_R0-0}{1}: [client-keymgmt] [15154]: (note): MAC: 286b.3598

EAP Key management successful. AKM:OWE Cipher:CCMP WPA Version: WPA3


2023/08/08 13:37:58.230603571 {wncd_x_R0-0}{1}: [client-keymgmt] [15154]: (info): MAC: 286b.3598
2023/08/08 13:37:58.230702678 {wncd_x_R0-0}{1}: [client-auth] [15154]: (note): MAC: 286b.3598.58
2023/08/08 13:37:58.230791777 {wncd_x_R0-0}{1}: [auth-mgr] [15154]: (info): [286b.3598.580f:capw
2023/08/08 13:37:58.230807848 {wncd_x_R0-0}{1}: [auth-mgr] [15154]: (info): [286b.3598.580f:capw

Wireless session sequence, create context with method WebAuth


2023/08/08 13:37:58.230831713 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [15154]: (info): [286b.
2023/08/08 13:37:58.230834488 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [15154]: (info): [286b.
2023/08/08 13:37:58.230857151 {wncd_x_R0-0}{1}: [client-auth] [15154]: (info): MAC: 286b.3598.58

S_AUTHIF_PSK_AUTH_KEY_XCHNG_PENDING -> S_AUTHIF_L2_WEBAUTH_PENDING


2023/08/08 13:37:58.230912145 {wncd_x_R0-0}{1}: [auth-mgr] [15154]: (info): [286b.3598.580f:capw
2023/08/08 13:37:58.230915511 {wncd_x_R0-0}{1}: [auth-mgr] [15154]: (info): [286b.3598.580f:capw
2023/08/08 13:37:58.230971648 {wncd_x_R0-0}{1}: [auth-mgr] [15154]: (info): [286b.3598.580f:capw
2023/08/08 13:37:58.230998298 {wncd_x_R0-0}{1}: [auth-mgr] [15154]: (info): [286b.3598.580f:capw
2023/08/08 13:37:58.231001354 {wncd_x_R0-0}{1}: [auth-mgr] [15154]: (info): [286b.3598.580f:capw
2023/08/08 13:37:58.231043724 {wncd_x_R0-0}{1}: [auth-mgr] [15154]: (info): [286b.3598.580f:capw
[...]
2023/08/08 13:37:58.231245206 {wncd_x_R0-0}{1}: [webauth-state] [15154]: (info): capwap_9000000b

Param-map used: LocalWebAuth
```

```
2023/08/08 13:37:58.231251037 {wncd_x_R0-0}{1}: [webauth-state] [15154]: (info): capwap_9000000b[286b.35
2023/08/08 13:37:58.231273499 {wncd_x_R0-0}{1}: [webauth-acl] [15154]: (info): capwap_9000000b[286b.3598
```

Applying IPv4 intercept ACL via SVM, name: IP-Adm-V4-Int-ACL-global

```
, priority: 50, IIF-ID: 0
[...]
2023/08/08 13:37:58.239843453 {wncd_x_R0-0}{1}: [client-iplearn] [15154]: (info): MAC: 286b.3598.580f IP
2023/08/08 13:37:58.239903667 {wncd_x_R0-0}{1}: [client-iplearn] [15154]: (note): MAC: 286b.3598.580f
```

Client IP learn successful. Method: DHCP IP: 192.168.1.159

```
[...]
2023/08/08 13:37:58.240371152 {wncd_x_R0-0}{1}: [auth-mgr-feat_acct] [15154]: (info): [286b.3598.580f:ca
2023/08/08 13:37:58.240390128 {wncd_x_R0-0}{1}: [client-iplearn] [15154]: (info): MAC: 286b.3598.580f IP
2023/08/08 13:37:58.240437257 {wncd_x_R0-0}{1}: [client-orch-sm] [15154]: (debug): MAC: 286b.3598.580f P
2023/08/08 13:37:58.240457105 {wncd_x_R0-0}{1}: [client-orch-sm] [15154]: (debug): MAC: 286b.3598.580f T
2023/08/08 13:37:58.240459018 {wncd_x_R0-0}{1}: [client-orch-state] [15154]: (note): MAC: 286b.3598.580f
```

Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS

```
2023/08/08 13:37:58.240527728 {wncd_x_R0-0}{1}: [dot1x] [15154]: (info): [0000.0000.0000:capwap_9000000b
2023/08/08 13:37:58.240760238 {wncd_x_R0-0}{1}: [client-auth] [15154]: (note): MAC: 286b.3598.580f L3 Au
2023/08/08 13:37:58.240767232 {wncd_x_R0-0}{1}: [client-auth] [15154]: (info): MAC: 286b.3598.580f
```

Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING

```
[...]
2023/08/08 13:37:58.924439975 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_9000000b[286b.3598.
2023/08/08 13:37:58.924590710 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_9000000b[286b.3598.
2023/08/08 13:37:58.924606621 {wncd_x_R0-0}{1}: [webauth-httpd] [15154]: (info): capwap_9000000b[286b.35
2023/08/08 13:37:58.924617631 {wncd_x_R0-0}{1}: [webauth-httpd] [15154]: (info): capwap_9000000b[286b.35
2023/08/08 13:37:58.924646336 {wncd_x_R0-0}{1}: [webauth-httpd] [15154]: (info): capwap_9000000b[286b.35
2023/08/08 13:37:58.924811559 {wncd_x_R0-0}{1}: [webauth-httpd] [15154]: (info): capwap_9000000b[286b.35
2023/08/08 13:37:58.924823291 {wncd_x_R0-0}{1}: [webauth-state] [15154]: (info): capwap_9000000b[286b.35
2023/08/08 13:37:58.924830184 {wncd_x_R0-0}{1}: [webauth-state] [15154]: (info): capwap_9000000b[286b.35
```

State INIT -> GET_REDIRECT

```
2023/08/08 13:37:58.924836706 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_9000000b[286b.3598.
2023/08/08 13:37:58.924893704 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_9000000b[286b.3598.
[...]
2023/08/08 13:38:16.814516928 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_9000000b[286b.3598.
2023/08/08 13:38:16.814739389 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_9000000b[286b.3598.
2023/08/08 13:38:16.843721875 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_9000000b[286b.3598.
2023/08/08 13:38:16.863779947 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_9000000b[286b.3598.
2023/08/08 13:38:16.863799384 {wncd_x_R0-0}{1}:
```

[webauth-httpd] [15154]: (info): capwap_9000000b[286b.3598.580f][192.168.1.159]POST rcvd when in LOGIN

```
2023/08/08 13:38:16.863812318 {wncd_x_R0-0}{1}: [webauth-httpd] [15154]: (info): capwap_9000000b[286b.35
2023/08/08 13:38:16.863857023 {wncd_x_R0-0}{1}: [webauth-httpd] [15154]: (info): capwap_9000000b[286b.35
2023/08/08 13:38:16.863981829 {wncd_x_R0-0}{1}: [caaa-authen] [15154]: (info): [CAAA:AUTHEN:c8000018] NU
2023/08/08 13:38:16.864023268 {wncd_x_R0-0}{1}: [webauth-state] [15154]: (info): capwap_9000000b[286b.35
2023/08/08 13:38:16.864026684 {wncd_x_R0-0}{1}: [webauth-state] [15154]: (info): capwap_9000000b[286b.35
2023/08/08 13:38:16.864039067 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_9000000b[286b.3598.
2023/08/08 13:38:16.864184873 {wncd_x_R0-0}{1}: [radius] [15154]: (info): RADIUS:
```

Send Access-Request

```
 to 192.168.1.7:1812 id 0/5, len 390
2023/08/08 13:38:16.864190705 {wncd_x_R0-0}{1}: [radius] [15154]: (info): RADIUS: authenticator 50 a9 ab
2023/08/08 13:38:16.864194552 {wncd_x_R0-0}{1}: [radius] [15154]: (info): RADIUS: Calling-Station-Id [31
2023/08/08 13:38:16.864197568 {wncd_x_R0-0}{1}: [radius] [15154]: (info): RADIUS: User-Name [1] 7 "tiago
[...]
2023/08/08 13:38:16.879241798 {wncd_x_R0-0}{1}: [radius] [15154]: (info): RADIUS:

Received from id 1812/5 192.168.1.7:0, Access-Accept

, len 128
[...]
2023/08/08 13:38:16.879504014 {wncd_x_R0-0}{1}: [webauth-state] [15154]: (info): capwap_9000000b[286b.35
2023/08/08 13:38:16.879513532 {wncd_x_R0-0}{1}: [webauth-state] [15154]: (info): capwap_9000000b[286b.35
2023/08/08 13:38:16.879530745 {wncd_x_R0-0}{1}: [webauth-acl] [15154]: (info): capwap_9000000b[286b.3598

Unapply IPv4 intecept ACL via SVM, name "IP-Adm-V4-Int-ACL-global"

, pri 50, IIF 0
[...]
2023/08/08 13:38:16.880956564 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [15154]: (note):

Authentication Success

. Resolved Policy bitmap:4 for client 286b.3598.580f
[...]
2023/08/08 13:38:16.882320225 {wncd_x_R0-0}{1}: [errmsg] [15154]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADDE

Username entry (tiago) joined with ssid (wifi6E_test) for device with MAC: 286b.3598.580f


[...]
2023/08/08 13:38:16.882451875 {wncd_x_R0-0}{1}: [rog-proxy-capwap] [15154]: (debug): Managed client RUN
2023/08/08 13:38:16.882495928 {wncd_x_R0-0}{1}: [client-orch-state] [15154]: (note):

MAC: 286b.3598.580f Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RUN


[...]
```

Refer to document Configure Local Web Authentication with External Authentication for detailed troubleshoot steps.

OWE with EWA

Here we can see an example of EWA in the RA traces:

<#root>

```
2023/08/10 14:35:20.685078384 {wncd_x_R0-0}{1}: [client-orch-sm] [15195]: (note): MAC: 0429.2ec9

Association received. BSSID 00df.1ddd.7d39, WLAN wifi6E_EWA

, Slot 3 AP 00df.1ddd.7d30, AP9136_5C.F524
2023/08/10 14:35:20.685117718 {wncd_x_R0-0}{1}: [client-orch-sm] [15195]: (debug): MAC: 0429.2ec
2023/08/10 14:35:20.685226454 {wncd_x_R0-0}{1}: [client-orch-state] [15195]: (note): MAC: 0429.2
2023/08/10 14:35:20.685420591 {wncd_x_R0-0}{1}: [dot11-validate] [15195]: (info): MAC: 0429.2ec9
2023/08/10 14:35:20.685422154 {wncd_x_R0-0}{1}: [dot11-validate] [15195]: (info): MAC: 0429.2ec9
2023/08/10 14:35:20.685864592 {wncd_x_R0-0}{1}: [dot11] [15195]: (debug): MAC: 0429.2ec9.e371 do
2023/08/10 14:35:20.685865002 {wncd_x_R0-0}{1}: [dot11] [15195]: (info): MAC: 0429.2ec9.e371 Dot
2023/08/10 14:35:20.685867818 {wncd_x_R0-0}{1}: [dot11] [15195]: (debug): MAC: 0429.2ec9.e371 Do
2023/08/10 14:35:20.685886032 {wncd_x_R0-0}{1}: [dot11-frame] [15195]: (info): MAC: 0429.2ec9.e3
```

```
2023/08/10 14:35:20.685991953 {wncd_x_R0-0}{1}: [dot11] [15195]: (info): MAC: 0429.2ec9.e371

dot11 send association response. Sending assoc response of length: 183 with resp_status_code: 0, DOT11_S


2023/08/10 14:35:20.685995339 {wncd_x_R0-0}{1}: [dot11] [15195]: (note): MAC: 0429.2ec9.e371 Ass
2023/08/10 14:35:20.686003685 {wncd_x_R0-0}{1}: [dot11] [15195]: (info): MAC: 0429.2ec9.e371 DOT
2023/08/10 14:35:20.686061695 {wncd_x_R0-0}{1}: [client-orch-sm] [15195]: (debug): MAC: 0429.2ec
2023/08/10 14:35:20.686088796 {wncd_x_R0-0}{1}: [client-orch-sm] [15195]: (debug): MAC: 0429.2ec
2023/08/10 14:35:20.686099576 {wncd_x_R0-0}{1}: [client-orch-state] [15195]: (note): MAC: 0429.2
2023/08/10 14:35:20.686125926 {wncd_x_R0-0}{1}: [client-auth] [15195]: (note): MAC: 0429.2ec9.e3
[...]
2023/08/10 14:35:20.687526737 {wncd_x_R0-0}{1}: [auth-mgr] [15195]: (info): [0429.2ec9.e371:capw
2023/08/10 14:35:20.687530575 {wncd_x_R0-0}{1}: [auth-mgr] [15195]: (info): [0429.2ec9.e371:capw
2023/08/10 14:35:20.687533620 {wncd_x_R0-0}{1}: [auth-mgr] [15195]: (info): [0429.2ec9.e371:capw

Authorized open auth session for 0429.2ec9.e371


[...]
2023/08/10 14:35:20.687804543 {wncd_x_R0-0}{1}: [client-auth] [15195]: (info): MAC: 0429.2ec9.e3
2023/08/10 14:35:20.687807038 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [15195]: (note): Authentication
[...]
2023/08/10 14:35:20.691676380 {wncd_x_R0-0}{1}: [client-auth] [15195]: (info): MAC: 0429.2ec9.e3

S_AUTHIF_PSK_AUTH_KEY_XCHNG_PENDING


2023/08/10 14:35:20.691841904 {wncd_x_R0-0}{1}: [client-keymgmt] [15195]: (info): MAC: 0429.2ec9
2023/08/10 14:35:20.691844278 {wncd_x_R0-0}{1}: [client-keymgmt] [15195]: (info): MAC: 0429.2ec9
2023/08/10 14:35:20.721636921 {wncd_x_R0-0}{1}: [client-keymgmt] [15195]: (info): MAC: 0429.2ec9
2023/08/10 14:35:20.721730809 {wncd_x_R0-0}{1}: [client-keymgmt] [15195]: (info): MAC: 0429.2ec9
2023/08/10 14:35:20.721736890 {wncd_x_R0-0}{1}: [client-keymgmt] [15195]: (info): MAC: 0429.2ec9
2023/08/10 14:35:20.739641625 {wncd_x_R0-0}{1}: [client-keymgmt] [15195]: (info): MAC: 0429.2ec9
2023/08/10 14:35:20.739644982 {wncd_x_R0-0}{1}: [client-keymgmt] [15195]: (note): MAC: 0429.2ec9

EAP Key management successful. AKM:OWE Cipher:CCMP WPA Version: WPA3


2023/08/10 14:35:20.739650121 {wncd_x_R0-0}{1}: [client-keymgmt] [15195]: (info): MAC: 0429.2ec9
2023/08/10 14:35:20.739744971 {wncd_x_R0-0}{1}: [client-auth] [15195]: (note): MAC: 0429.2ec9.e3
2023/08/10 14:35:20.739838779 {wncd_x_R0-0}{1}: [auth-mgr] [15195]: (info): [0429.2ec9.e371:capw
2023/08/10 14:35:20.739847004 {wncd_x_R0-0}{1}: [auth-mgr] [15195]: (info): [0429.2ec9.e371:capw
2023/08/10 14:35:20.739861071 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [15195]: (info): [0429.
[...]
2023/08/10 14:35:20.740069114 {wncd_x_R0-0}{1}: [webauth-state] [15195]: (info): capwap_9000001

Param-map used: ExternalWebAuth


2023/08/10 14:35:20.740071629 {wncd_x_R0-0}{1}: [webauth-state] [15195]: (info): capwap_9000001
2023/08/10 14:35:20.740083452 {wncd_x_R0-0}{1}: [webauth-sm] [15195]: (info): capwap_90000010[04
2023/08/10 14:35:20.740085425 {wncd_x_R0-0}{1}: [webauth-sm] [15195]: (info): capwap_90000010[04
2023/08/10 14:35:20.740091236 {wncd_x_R0-0}{1}: [webauth-state] [15195]: (info): capwap_9000001
2023/08/10 14:35:20.740093601 {wncd_x_R0-0}{1}: [webauth-state] [15195]: (info): capwap_9000001
2023/08/10 14:35:20.740103810 {wncd_x_R0-0}{1}: [webauth-acl] [15195]: (info): capwap_90000010[0
[...]
2023/08/10 14:35:21.942607594 {wncd_x_R0-0}{1}: [client-iplearn] [15195]: (note): MAC: 0429.2ec9

Client IP learn successful. Method: DHCP IP: 192.168.1.160


[...]
2023/08/10 14:35:21.943838504 {wncd_x_R0-0}{1}: [client-iplearn] [15195]: (info): MAC: 0429.2ec9
```

S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE

```
2023/08/10 14:35:21.944028273 {wncd_x_R0-0}{1}: [client-orch-sm] [15195]: (debug): MAC: 0429.2ec
2023/08/10 14:35:21.944069521 {wncd_x_R0-0}{1}: [client-orch-sm] [15195]: (debug): MAC: 0429.2ec
2023/08/10 14:35:21.944074851 {wncd_x_R0-0}{1}: [client-orch-state] [15195]: (note): MAC: 0429.2
2023/08/10 14:35:21.944201671 {wncd_x_R0-0}{1}: [dot1x] [15195]: (info): [0000.0000.0000:capwap_
2023/08/10 14:35:21.944759066 {wncd_x_R0-0}{1}: [client-auth] [15195]: (note): MAC: 0429.2ec9.e3
```

L3 Authentication initiated. LWA

```
2023/08/10 14:35:21.944776669 {wncd_x_R0-0}{1}: [client-auth] [15195]: (info): MAC: 0429.2ec9.e3
```

S_AUTHIF_WEBAUTH_PENDING

```
[...]
2023/08/10 14:35:24.110614486 {wncd_x_R0-0}{1}: [webauth-io] [15195]: (info): capwap_90000010[04
2023/08/10 14:35:24.110679789 {wncd_x_R0-0}{1}: [webauth-io] [15195]: (info): capwap_90000010[04
2023/08/10 14:35:24.110699827 {wncd_x_R0-0}{1}: [webauth-httpd] [15195]: (info): capwap_9000001
```

GET rcvd when in LOGIN state

```
2023/08/10 14:35:24.110718893 {wncd_x_R0-0}{1}: [webauth-httpd] [15195]: (info): capwap_9000001
```

HTTP GET request

```
2023/08/10 14:35:24.110754721 {wncd_x_R0-0}{1}: [webauth-httpd] [15195]: (info): capwap_9000001
2023/08/10 14:35:24.110951163 {wncd_x_R0-0}{1}: [webauth-httpd] [15195]: (info): capwap_9000001
2023/08/10 14:35:24.110960801 {wncd_x_R0-0}{1}: [webauth-state] [15195]: (info): capwap_9000001
```

Param-map used: ExternalWebAuth

```
2023/08/10 14:35:24.110971331 {wncd_x_R0-0}{1}: [webauth-state] [15195]: (info): capwap_9000001
2023/08/10 14:35:24.111046654 {wncd_x_R0-0}{1}: [webauth-page] [15195]: (info): capwap_90000010[
[...]
2023/08/10 14:35:35.761960632 {wncd_x_R0-0}{1}: [webauth-io] [15195]: (info): capwap_90000010[04
2023/08/10 14:35:35.776669018 {wncd_x_R0-0}{1}: [webauth-io] [15195]: (info): capwap_90000010[04
2023/08/10 14:35:37.805884475 {wncd_x_R0-0}{1}: [webauth-io] [15195]: (info): capwap_90000010[04
2023/08/10 14:35:37.807261842 {wncd_x_R0-0}{1}: [webauth-io] [15195]: (info): capwap_90000010[04
2023/08/10 14:35:37.807273253 {wncd_x_R0-0}{1}: [webauth-httpd] [15195]: (info): capwap_9000001
```

POST rcvd when in LOGIN state

```
2023/08/10 14:35:37.807287911 {wncd_x_R0-0}{1}: [webauth-httpd] [15195]: (info): capwap_9000001
2023/08/10 14:35:37.807331213 {wncd_x_R0-0}{1}: [webauth-httpd] [15195]: (info): capwap_9000001
[...]
2023/08/10 14:35:37.807498470 {wncd_x_R0-0}{1}: [webauth-state] [15195]: (info): capwap_9000001
```

Param-map used: ExternalWebAuth

```
2023/08/10 14:35:37.807503619 {wncd_x_R0-0}{1}: [webauth-state] [15195]: (info): capwap_9000001
2023/08/10 14:35:37.807515502 {wncd_x_R0-0}{1}: [webauth-io] [15195]: (info): capwap_90000010[04
2023/08/10 14:35:37.807653884 {wncd_x_R0-0}{1}: [radius] [15195]: (info):
```

RADIUS: Send Access-Request

```
 to 192.168.1.7:1812 id 0/1, len 531
2023/08/10 14:35:37.807663221 {wncd_x_R0-0}{1}: [radius] [15195]: (info): RADIUS: authenticator
2023/08/10 14:35:37.807667159 {wncd_x_R0-0}{1}: [radius] [15195]: (info): RADIUS: Calling-Static
```

```
2023/08/10 14:35:37.807670215 {wncd_x_R0-0}{1}: [radius] [15195]: (info): RADIUS: User-Name [1]

tiago

"
2023/08/10 14:35:37.807673040 {wncd_x_R0-0}{1}: [radius] [15195]: (info): RADIUS: Vendor, Cisco
2023/08/10 14:35:37.807676226 {wncd_x_R0-0}{1}: [radius] [15195]: (info): RADIUS: Cisco AVpair [
2023/08/10 14:35:37.807680083 {wncd_x_R0-0}{1}: [radius] [15195]: (info): RADIUS: Framed-IP-Addr
2023/08/10 14:35:37.807682217 {wncd_x_R0-0}{1}: [radius] [15195]: (info): RADIUS: Message-Auther
2023/08/10 14:35:37.807701825 {wncd_x_R0-0}{1}: [radius] [15195]: (info): RADIUS: Service-Type [
2023/08/10 14:35:37.807703838 {wncd_x_R0-0}{1}: [radius] [15195]: (info): RADIUS: Vendor, Cisco
2023/08/10 14:35:37.807709459 {wncd_x_R0-0}{1}: [radius] [15195]: (info): RADIUS: Cisco AVpair [
2023/08/10 14:35:37.807711783 {wncd_x_R0-0}{1}: [radius] [15195]: (info): RADIUS: Vendor, Cisco
2023/08/10 14:35:37.807714509 {wncd_x_R0-0}{1}: [radius] [15195]: (info): RADIUS: Cisco AVpair [

webauth

"
[...]
2023/08/10 14:35:37.887128821 {wncd_x_R0-0}{1}: [radius] [15195]: (info): RADIUS:

Received from id 1812/1 192.168.1.7:0, Access-Accept

, len 130
2023/08/10 14:35:37.887152085 {wncd_x_R0-0}{1}: [radius] [15195]: (info): RADIUS: authenticator
2023/08/10 14:35:37.887166342 {wncd_x_R0-0}{1}: [radius] [15195]: (info): RADIUS: User-Name [1]

tiago

"
[...]
2023/08/10 14:35:37.890143566 {wncd_x_R0-0}{1}: [auth-mgr] [15195]: (info): [0429.2ec9.e371:capw

Authc success from WebAuth, Auth event success


[...]
2023/08/10 14:35:37.893926155 {wncd_x_R0-0}{1}: [rog-proxy-capwap] [15195]: (debug): Managed cli
2023/08/10 14:35:37.893979316 {wncd_x_R0-0}{1}: [client-orch-state] [15195]: (note): MAC: 0429.2

S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RUN


[...]
```

Refer to document Configure and Troubleshoot External Web-Authentication on 9800 WLC for more detailed troubleshoot steps.

OWE with CWA

Here we can see an example of CWA in the RA traces:

<#root>

```
2023/08/11 12:43:45.551148898 {wncd_x_R0-0}{1}: [client-orch-sm] [15200]: (note): MAC: 2495.2f72

Association received. BSSID 00df.1ddd.7d39, WLAN wifi6E_CWA

, Slot 3 AP 00df.1ddd.7d30, AP9136_5C.F524
2023/08/11 12:43:45.551185236 {wncd_x_R0-0}{1}: [client-orch-sm] [15200]: (debug): MAC: 2495.2f7
[...]
```

2023/08/11 12:43:45.551873379 {wncd_x_R0-0}{1}: [client-auth] [15200]: (note): MAC: 2495.2f72.8a

MAB Authentication initiated.

Policy VLAN 0, AAA override = 1, NAC = 1
2023/08/11 12:43:45.551925177 {wncd_x_R0-0}{1}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:capw
2023/08/11 12:43:45.551935427 {wncd_x_R0-0}{1}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:capw
2023/08/11 12:43:45.551947760 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [15200]: (info): [2495.

authc_list: RadiusAuthor

[...]
2023/08/11 12:43:45.553164283 {wncd_x_R0-0}{1}: [mab] [15200]: (info): [2495.2f72.8a66:capwap_90

MAB authentication started for 2495.2f72.8a66

[...]
2023/08/11 12:43:45.553769929 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS:

Send Access-Request to 192.168.1.7:1812

id 0/19, len 394
2023/08/11 12:43:45.553775189 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: authenticator
2023/08/11 12:43:45.553778666 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS:

User-Name [1] 14 "24952f728a66"

2023/08/11 12:43:45.553781110 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: User-Password
2023/08/11 12:43:45.553786901 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Service-Type [
2023/08/11 12:43:45.553789196 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Vendor, Cisco
2023/08/11 12:43:45.553792211 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Cisco AVpair [
2023/08/11 12:43:45.553795428 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Framed-MTU [12
2023/08/11 12:43:45.553797431 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Message-Auther
2023/08/11 12:43:45.553814193 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: EAP-Key-Name [
2023/08/11 12:43:45.553818431 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Vendor, Cisco
2023/08/11 12:43:45.553821036 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Cisco AVpair [
2023/08/11 12:43:45.553823100 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Vendor, Cisco
2023/08/11 12:43:45.553829221 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS:

Cisco AVpair [1] 12 "method=mab"

2023/08/11 12:43:45.553831265 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Vendor, Cisco
2023/08/11 12:43:45.553833720 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Cisco AVpair [
2023/08/11 12:43:45.553835684 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Vendor, Cisco
2023/08/11 12:43:45.553838048 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Cisco AVpair [
2023/08/11 12:43:45.553841395 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: NAS-IP-Address
2023/08/11 12:43:45.553844270 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: NAS-Port-Type
2023/08/11 12:43:45.553846955 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: NAS-Port [5] 6
2023/08/11 12:43:45.553848758 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Vendor, Cisco
2023/08/11 12:43:45.553851193 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS:

Cisco AVpair [1] 28 "cisco-wlan-ssid=wifi6E_CWA"

2023/08/11 12:43:45.553853177 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Vendor, Cisco
2023/08/11 12:43:45.553855591 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Cisco AVpair [
2023/08/11 12:43:45.553858246 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS:

Called-Station-Id [30] 30 "00-df-1d-dd-7d-30:wifi6E_CWA"

2023/08/11 12:43:45.553860811 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Calling-Static
2023/08/11 12:43:45.553863015 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Vendor, Airesp
2023/08/11 12:43:45.553865510 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Airespace-WLAN
2023/08/11 12:43:45.553867995 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Nas-Identifier
2023/08/11 12:43:45.553929331 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Started 5 sec
2023/08/11 12:43:45.570301533 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS:

Received from id 1812/19 192.168.1.7:0, Access-Accept

, len 538
2023/08/11 12:43:45.570313767 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: authenticator
2023/08/11 12:43:45.570319247 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: User-Name [1]
2023/08/11 12:43:45.570321902 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Class [25] 51
2023/08/11 12:43:45.570375383 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Message-Auther
2023/08/11 12:43:45.570390662 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Vendor, Cisco
2023/08/11 12:43:45.570393618 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS:

Cisco AVpair [1] 27 "url-redirect-acl=REDIRECT"

2023/08/11 12:43:45.570395732 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Vendor, Cisco
2023/08/11 12:43:45.570403947 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS:

Cisco AVpair [1] 183 "url-redirect=https://192.168.1.7:8443/portal/gateway?sessionId=0F01A8C00000001EE49

2023/08/11 12:43:45.570435186 {wncd_x_R0-0}{1}: [radius] [15200]: (info): Valid Response Packet,
2023/08/11 12:43:45.570612622 {wncd_x_R0-0}{1}: [mab] [15200]: (info): [2495.2f72.8a66:capwap_90

MAB received an Access-Accept for (2495.2f72.8a66)

2023/08/11 12:43:45.570621699 {wncd_x_R0-0}{1}: [mab] [15200]: (info): [2495.2f72.8a66:capwap_90
2023/08/11 12:43:45.570648140 {wncd_x_R0-0}{1}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:capw
2023/08/11 12:43:45.570657648 {wncd_x_R0-0}{1}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:capw
2023/08/11 12:43:45.570668839 {wncd_x_R0-0}{1}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:capw
2023/08/11 12:43:45.570709836 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15200]: (info): Applying Attribu
2023/08/11 12:43:45.570718393 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15200]: (info): Applying Attribu
2023/08/11 12:43:45.570719545 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15200]: (info): Applying Attribu
2023/08/11 12:43:45.570720517 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15200]: (info): Applying Attribu

url-redirect-acl 0 "REDIRECT"

2023/08/11 12:43:45.570722440 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15200]: (info): Applying Attribu

url-redirect 0 "https://192.168.1.7:8443/portal/gateway?sessionId=0F01A8C00000001EE49FCD0F&portal=26d195

[...]
2023/08/11 12:43:45.571261140 {wncd_x_R0-0}{1}: [webauth-dev] [15200]: (info): [2495.2f72.8a66]

Central Webauth URL Redirect, Received a request to create a CWA session for a mac [24:95:2f:72:8a:66]

[...]
2023/08/11 12:43:45.571316064 {wncd_x_R0-0}{1}: [webauth-state] [15200]: (info): [2495.2f72.8a66
2023/08/11 12:43:45.571318869 {wncd_x_R0-0}{1}: [webauth-state] [15200]: (info): [2495.2f72.8a66
[...]
2023/08/11 12:43:45.572346865 {wncd_x_R0-0}{1}: [dot11] [15200]: (info): MAC: 2495.2f72.8a66

dot11 send association response. Sending assoc response of length: 183 with resp_status_code: 0, DOT11_S

[...]

2023/08/11 12:43:45.576047520 {wncd_x_R0-0}{1}: [client-auth] [15200]: (info): MAC: 2495.2f72.8a

S_AUTHIF_ADD_MOBILE_ACK_WAIT_KM -> S_AUTHIF_PSK_AUTH_KEY_XCHNG_PENDING

2023/08/11 12:43:45.576136850 {wncd_x_R0-0}{1}: [client-keymgmt] [15200]: (info): MAC: 2495.2f72
2023/08/11 12:43:45.576138984 {wncd_x_R0-0}{1}: [client-keymgmt] [15200]: (info): MAC: 2495.2f72
2023/08/11 12:43:45.576247599 {mobilityd_R0-0}{1}: [mm-client] [16431]: (debug): MAC: 0000.0000.
2023/08/11 12:43:45.576379639 {mobilityd_R0-0}{1}: [mm-dgram-io] [16431]: (debug): MAC: 0000.000
2023/08/11 12:43:45.576397212 {mobilityd_R0-0}{1}: [mm-dgram-io] [16431]: (debug): MAC: 0000.000
2023/08/11 12:43:45.632584865 {wncd_x_R0-0}{1}: [client-keymgmt] [15200]: (info): MAC: 2495.2f72
2023/08/11 12:43:45.632765557 {wncd_x_R0-0}{1}: [client-keymgmt] [15200]: (info): MAC: 2495.2f72
2023/08/11 12:43:45.632766960 {wncd_x_R0-0}{1}: [client-keymgmt] [15200]: (info): MAC: 2495.2f72
2023/08/11 12:43:45.641844995 {wncd_x_R0-0}{1}: [client-keymgmt] [15200]: (info): MAC: 2495.2f72
2023/08/11 12:43:45.641846798 {wncd_x_R0-0}{1}: [client-keymgmt] [15200]: (note): MAC: 2495.2f72

EAP Key management successful. AKM:OWE Cipher:CCMP WPA Version: WPA3

2023/08/11 12:43:45.641851597 {wncd_x_R0-0}{1}: [client-keymgmt] [15200]: (info): MAC: 2495.2f72
[...]
2023/08/11 12:43:45.645536693 {wncd_x_R0-0}{1}: [client-orch-state] [15200]: (note): MAC: 2495.2

Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS

[...]
2023/08/11 12:43:46.103210515 {wncd_x_R0-0}{1}: [client-iplearn] [15200]: (note):

MAC: 2495.2f72.8a66 Client IP learn successful. Method: DHCP IP: 192.168.1.162

2023/08/11 12:43:46.103745268 {wncd_x_R0-0}{1}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:capw
2023/08/11 12:43:46.104324815 {wncd_x_R0-0}{1}: [webauth-sess] [15200]: (info): [2495.2f72.8a66]
2023/08/11 12:43:46.104343430 {wncd_x_R0-0}{1}: [webauth-sess] [15200]: (info): adding webauth s
2023/08/11 12:43:46.104416388 {wncd_x_R0-0}{1}: [auth-mgr-feat_acct] [15200]: (info): [2495.2f72
2023/08/11 12:43:46.104460371 {wncd_x_R0-0}{1}: [client-iplearn] [15200]: (info): MAC: 2495.2f72
2023/08/11 12:43:46.104607690 {wncd_x_R0-0}{1}: [client-orch-sm] [15200]: (debug): MAC: 2495.2f7
2023/08/11 12:43:46.104669668 {wncd_x_R0-0}{1}: [client-orch-sm] [15200]: (debug): MAC: 2495.2f7
2023/08/11 12:43:46.104674096 {wncd_x_R0-0}{1}: [client-orch-state] [15200]: (note):

MAC: 2495.2f72.8a66 Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS

2023/08/11 12:43:46.104749168 {wncd_x_R0-0}{1}: [dot1x] [15200]: (info): [0000.0000.0000:capwap_
2023/08/11 12:43:46.104996176 {wncd_x_R0-0}{1}: [client-auth] [15200]: (note):

MAC: 2495.2f72.8a66 L3 Authentication initiated. CWA

2023/08/11 12:43:46.105004562 {wncd_x_R0-0}{1}: [client-auth] [15200]: (info):

MAC: 2495.2f72.8a66 Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH

[...]
2023/08/11 12:43:46.281818709 {wncd_x_R0-0}{1}: [webauth-state] [15200]: (info):

[2495.2f72.8a66][192.168.1.162]Param-map used: global

2023/08/11 12:43:46.281822877 {wncd_x_R0-0}{1}: [webauth-state] [15200]: (info):

[2495.2f72.8a66][192.168.1.162]State INIT -> GET_REDIRECT

```
2023/08/11 12:43:46.281825292 {wncd_x_R0-0}{1}: [webauth-io] [15200]: (info): [2495.2f72.8a66][
2023/08/11 12:43:46.281856060 {wncd_x_R0-0}{1}: [webauth-io] [15200]: (info): [2495.2f72.8a66][
2023/08/11 12:43:46.281857933 {wncd_x_R0-0}{1}: [webauth-httpd] [15200]: (info): [2495.2f72.8a66
[...]
2023/08/11 12:44:20.312534457 {wncd_x_R0-0}{1}: [caaa-ch] [15200]: (info):

[CAAA:COMMAND HANDLER:35000014] Processing CoA request under Command Handler ctx.


2023/08/11 12:44:20.312571788 {wncd_x_R0-0}{1}: [caaa-ch] [15200]: (info):

[CAAA:COMMAND HANDLER:35000014] Reauthenticate request (0x560210e99bf8) for 2495.2f72.8a66


2023/08/11 12:44:20.312626401 {wncd_x_R0-0}{1}: [sadb-attr] [15200]: (info): Removing ipv6 addre
2023/08/11 12:44:20.312673230 {wncd_x_R0-0}{1}: [mab] [15200]: (info):

[2495.2f72.8a66:capwap_9000000f] MAB re-authentication started for (2495.2f72.8a66)


2023/08/11 12:44:20.312713736 {wncd_x_R0-0}{1}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:capw
2023/08/11 12:44:20.312720158 {wncd_x_R0-0}{1}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:capw
2023/08/11 12:44:20.312740637 {wncd_x_R0-0}{1}: [aaa-coa] [15200]: (info): radius coa proxy rela
2023/08/11 12:44:20.312746478 {wncd_x_R0-0}{1}: [aaa-coa] [15200]: (info):

CoA Response Details


2023/08/11 12:44:20.312756237 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15200]: (info): << ssg-command-c
2023/08/11 12:44:20.312758912 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15200]: (info): << formatted-cli
2023/08/11 12:44:20.312762318 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15200]: (info): << error-cause 0
2023/08/11 12:44:20.312774040 {wncd_x_R0-0}{1}: [aaa-coa] [15200]: (info): server:192.168.1.15 c
2023/08/11 12:44:20.312876905 {wncd_x_R0-0}{1}: [caaa-ch] [15200]: (info): [CAAA:COMMAND HANDLER
2023/08/11 12:44:20.312886633 {wncd_x_R0-0}{1}: [caaa-ch] [15200]: (info): [CAAA:COMMAND HANDLER
2023/08/11 12:44:20.312902744 {wncd_x_R0-0}{1}: [mab] [15200]: (info):

[2495.2f72.8a66:capwap_9000000f] Received event 'MAB_REAUTHENTICATE' on (2495.2f72.8a66)


2023/08/11 12:44:20.313249801 {wncd_x_R0-0}{1}: [sadb-attr] [15200]: (info): Removing ipv6 addre
2023/08/11 12:44:20.313380288 {wncd_x_R0-0}{1}: [caaa-author] [15200]: (info): [CAAA:AUTHOR:3500
2023/08/11 12:44:20.313702758 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS:

Send Access-Request to 192.168.1.7

:1812 id 0/20, len 544
2023/08/11 12:44:20.313714140 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: authenticator
2023/08/11 12:44:20.313722686 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS:

User-Name [1] 14 "24952f728a66"


[...]
2023/08/11 12:44:20.313914609 {smd_R0-0}{1}: [aaa-coa] [17281]: (info): ++++++ Received CoA resp
2023/08/11 12:44:20.313917665 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: NAS-IP-Address
2023/08/11 12:44:20.313924488 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: NAS-Port-Type
2023/08/11 12:44:20.313931051 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: NAS-Port [5] 6
2023/08/11 12:44:20.313935559 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Vendor, Cisco
2023/08/11 12:44:20.313941611 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Cisco AVpair [
2023/08/11 12:44:20.313946640 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Vendor, Cisco
2023/08/11 12:44:20.313952692 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Cisco AVpair [
2023/08/11 12:44:20.313959174 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Called-Station
2023/08/11 12:44:20.313965616 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Calling-Stati
2023/08/11 12:44:20.313978210 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Vendor, Airesp
2023/08/11 12:44:20.313978350 {smd_R0-0}{1}: [radius] [17281]: (info): RADIUS(00000000):
```

Send CoA Ack Response to 192.168.1.7

:42721 id 4, len 69
2023/08/11 12:44:20.313984442 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Airespace-WLAN
2023/08/11 12:44:20.313989972 {smd_R0-0}{1}: [radius] [17281]: (info): RADIUS: authenticator c3
2023/08/11 12:44:20.313990713 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Nas-Identifier
2023/08/11 12:44:20.313993459 {smd_R0-0}{1}: [radius] [17281]: (info): RADIUS: Vendor, Cisco [26
2023/08/11 12:44:20.313996655 {smd_R0-0}{1}: [radius] [17281]: (info): RADIUS: ssg-command-code
2023/08/11 12:44:20.314073240 {smd_R0-0}{1}: [radius] [17281]: (info): RADIUS: Calling-Station-I
2023/08/11 12:44:20.314077337 {smd_R0-0}{1}: [radius] [17281]: (info): RADIUS:

Dynamic-Author-Error-Cause[101] 6 Success [200]

2023/08/11 12:44:20.314079431 {smd_R0-0}{1}: [radius] [17281]: (info): RADIUS: Message-Authentic
2023/08/11 12:44:20.314098387 {smd_R0-0}{1}: [aaa-pod] [17281]: (info): CoA response source port
2023/08/11 12:44:20.314099289 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Started 5 sec
2023/08/11 12:44:20.327831023 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS:

Received from id 1812/20 192.168.1.7:0, Access-Accept

, len 131
2023/08/11 12:44:20.327850400 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: authenticator
2023/08/11 12:44:20.327861140 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS:

User-Name [1] 7 "tiago"

2023/08/11 12:44:20.327867512 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Class [25] 51
2023/08/11 12:44:20.327938827 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Message-Auther
2023/08/11 12:44:20.327978472 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Vendor, Cisco
2023/08/11 12:44:20.327985516 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Cisco AVpair [
2023/08/11 12:44:20.328027385 {wncd_x_R0-0}{1}: [radius] [15200]: (info): Valid Response Packet,
2023/08/11 12:44:20.328322423 {wncd_x_R0-0}{1}: [mab] [15200]: (info): [2495.2f72.8a66:capwap_90
2023/08/11 12:44:20.328341299 {wncd_x_R0-0}{1}: [mab] [15200]: (info): [2495.2f72.8a66:capwap_90
2023/08/11 12:44:20.328394871 {wncd_x_R0-0}{1}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:capw
2023/08/11 12:44:20.328412885 {wncd_x_R0-0}{1}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:capw
2023/08/11 12:44:20.328421270 {wncd_x_R0-0}{1}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:capw
2023/08/11 12:44:20.328519506 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15200]: (info): Applying Attribu
[...]
2023/08/11 12:44:20.328759310 {wncd_x_R0-0}{1}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:capw

Received User-Name tiago for client 2495.2f72.8a66

2023/08/11 12:44:20.328773066 {wncd_x_R0-0}{1}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:capw

Method mab changing state from 'Running' to 'Authc Success'

2023/08/11 12:44:20.328791892 {wncd_x_R0-0}{1}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:capw
[...]
2023/08/11 12:44:20.330928236 {wncd_x_R0-0}{1}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:capw
2023/08/11 12:44:20.330937604 {wncd_x_R0-0}{1}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:capw
2023/08/11 12:44:20.331059194 {wncd_x_R0-0}{1}: [client-auth] [15200]: (note): MAC: 2495.2f72.8a
2023/08/11 12:44:20.331065276 {wncd_x_R0-0}{1}: [client-auth] [15200]: (info):

MAC: 2495.2f72.8a66 Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH

[...]
2023/08/11 12:44:20.332171950 {wncd_x_R0-0}{1}: [errmsg] [15200]: (info): %CLIENT_ORCH_LOG-6-

CLIENT_ADDED_TO_RUN_STATE: R0/0: wncd: Username entry (tiago) joined with ssid (wifi6E_CWA) for device w

```
[...]
2023/08/11 12:44:20.332437363 {wncd_x_R0-0}{1}: [rog-proxy-capwap] [15200]: (debug): Managed cli
2023/08/11 12:44:20.332544836 {wncd_x_R0-0}{1}: [client-orch-state] [15200]: (note):
```

MAC: 2495.2f72.8a66 Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RUN

```
[...]
2023/08/11 12:44:20.337221359 {wncd_x_R0-0}{1}: [client-auth] [15200]: (info): MAC: 2495.2f72.8a
```

Refer to document Configure Central Web Authentication (CWA) on Catalyst 9800 WLC and ISE for more detailed troubleshoot steps.

Related Information

What is Wi-Fi 6E?

What Is Wi-Fi 6 vs. Wi-Fi 6E?

Wi-Fi 6E At-a-Glance

Wi-Fi 6E: The Next Great Chapter in Wi-Fi White Paper

Cisco Live - Architecting Next Generation Wireless Network with Catalyst Wi-Fi 6E Access Points

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide 17.9.x

WPA3 Deployment Guide

Configure Local Web Authentication with External Authentication

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