

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

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Background Information](#)
[Web Authentication](#)
[Cisco Catalyst Wi-Fi 6E APs](#)
[Configure and Verify](#)
[Network Diagram](#)
[Configure OWE with Local Web Authentication](#)
[Verify](#)
[Configure OWE with External Web Authentication](#)
[Verify](#)
[Configure OWE with Central Web Authentication](#)
[Verify](#)
[Troubleshoot](#)
[OWE with LWA](#)
[OWE with EWA](#)
[OWE with CWA](#)
[Related Information](#)

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

To know more about Wi-Fi 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 http(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 http(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](#).

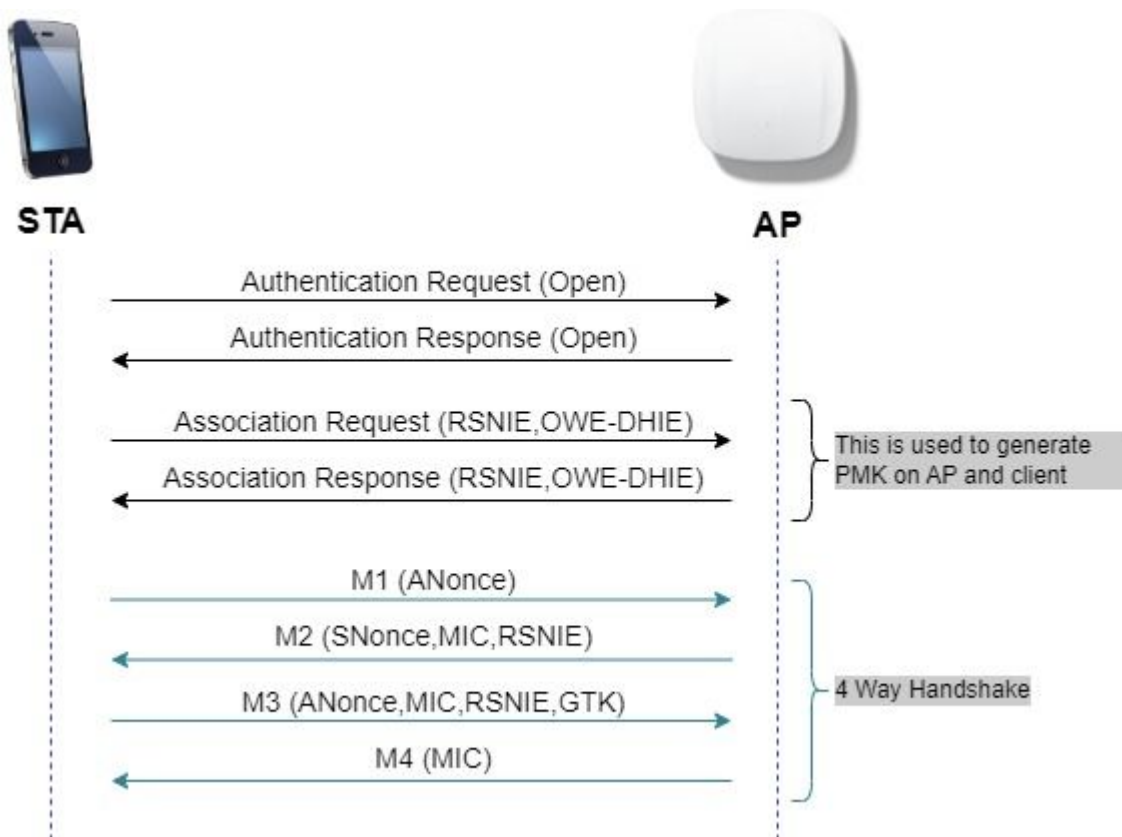
Traditionally, Wi-Fi hotspots and guest WLANs have used open security without encryption or authentication. The Wi-Fi CERTIFIED Enhanced Open certification defines improved data privacy in open

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 writing this doc:

Ideal for Small to Medium-sized deployments

Best In Class, Flexibility



CW9162

- 2x2 + 2x2 + 2x2
- 2.5 Gbps mGig
- Power Options: PoE, DC Power
- IoT ready + Bluetooth 5.x
- Partial iCAP
- USB - 4.5 W



CW9164

- 2x2, 4x4, 4x4
- 2.5 Gbps mGig
- Power Options: PoE, DC Power
- IoT Ready + Bluetooth 5.x
- Partial iCAP
- USB- 4.5 W



CW9166

- 4x4 + 4x4 + 4x4 (XOR 5/6)
- 5 Gbps mGig
- Power Options: PoE, DC Power
- IoT ready + Bluetooth 5.x
- Environmental Sensor
- Full Packet Capture (iCAP)
- Zero-Wait DFS*
- USB - 4.5W

Available with IOS-XE 17.9.2

Full radio capability (6 GHz @ LPI) on single 30W PoE+

Dedicated Radio for CleanAir Pro

Same Bracket, Industrial Design

AP Power Optimization

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.

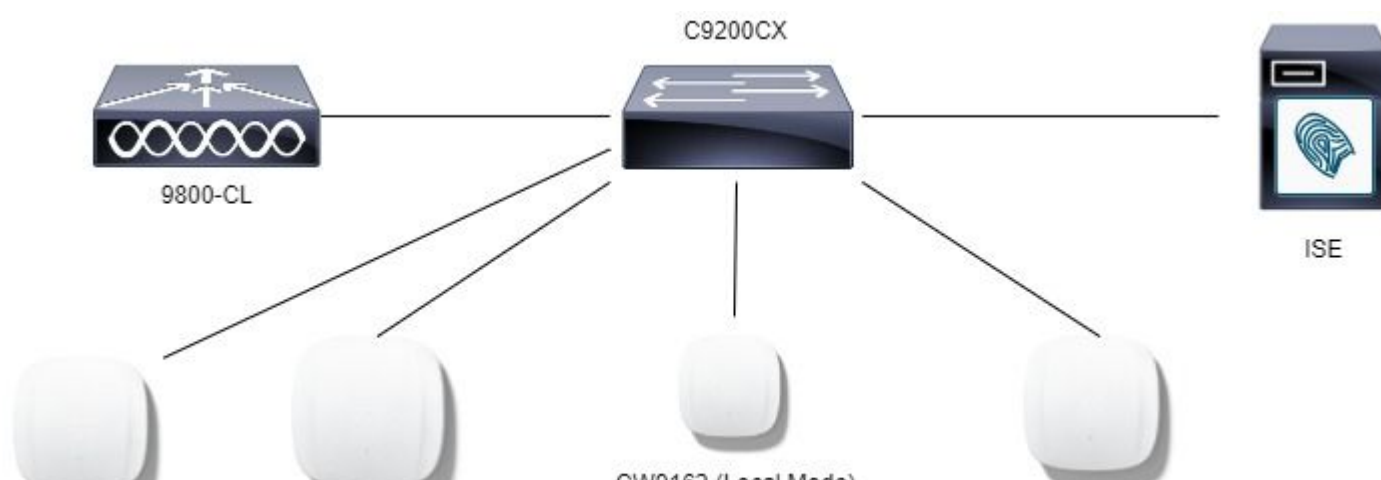
The Layer 2 Security settings are be locked to Opportunistic Wireless Encryption (OWE) which is the closest to an "Open" network we can have in WiFi 6E.

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:

No.	Time	Delta	Source	Destination	Protocol	Length	SSS Id	Info
105	13:37:58.234081	0.944095	Inte1Cor_98/58:0f	Cisco_4d/7d:38	802.11	297	00:0f:1d:0d:7d:38	Association Request, S/W=2, H/W=, Flags=..... SSID="wifisat_test"
106	13:37:58.234082	0.000000	Inte1Cor_98/58:0f	Cisco_4d/7d:38	802.11	293	00:0f:1d:0d:7d:38	Association Request, S/W=2, H/W=, Flags=..... SSID="wifisat_test"
107	13:37:58.237987	0.003806	Cisco_4d/7d:38	Inte1Cor_98/58:0f	802.11	254	00:0f:1d:0d:7d:38	Association Response, S/W=, H/W=, Flags=.....
108	13:37:58.237987	0.000000	Cisco_4d/7d:38	Inte1Cor_98/58:0f	802.11	254	00:0f:1d:0d:7d:38	Association Response, S/W=, H/W=, Flags=.....
109	13:37:58.239986	0.002199	Inte1Cor_98/58:0f	Broadcast	LLC	120	00:0f:1d:0d:7d:38	U, Func=01 SNAP, Out 00000000 (Officially Xerox, but 00:0c:0c:0c:0c:0c is more common)
110	13:37:58.222980	0.022294	Cisco_4d/7d:38	Inte1Cor_98/58:0f	EAPOL	263	00:0f:1d:0d:7d:38	Key (Message 1 of 4)
111	13:37:58.222980	0.000000	Inte1Cor_98/58:0f	Cisco_4d/7d:38	EAPOL	263	00:0f:1d:0d:7d:38	Key (Message 1 of 4)
112	13:37:58.226978	0.003998	Inte1Cor_98/58:0f	Cisco_4d/7d:38	EAPOL	223	00:0f:1d:0d:7d:38	Key (Message 2 of 4)
113	13:37:58.226978	0.000000	Inte1Cor_98/58:0f	Cisco_4d/7d:38	EAPOL	223	00:0f:1d:0d:7d:38	Key (Message 2 of 4)
114	13:37:58.226978	0.000000	Cisco_4d/7d:38	Inte1Cor_98/58:0f	EAPOL	277	00:0f:1d:0d:7d:38	Key (Message 3 of 4)
115	13:37:58.226978	0.000000	Inte1Cor_98/58:0f	Cisco_4d/7d:38	EAPOL	277	00:0f:1d:0d:7d:38	Key (Message 3 of 4)
116	13:37:58.222980	0.003806	Inte1Cor_98/58:0f	Cisco_4d/7d:38	EAPOL	295	00:0f:1d:0d:7d:38	Key (Message 4 of 4)
117	13:37:58.222980	0.000000	Inte1Cor_98/58:0f	Cisco_4d/7d:38	EAPOL	302	00:0f:1d:0d:7d:38	Key (Message 4 of 4)
118	13:37:58.227973	0.042296	0.0.0.0	255.255.255.255	DHCP	456	00:0f:1d:0d:7d:38	DHCP Request - Transaction ID 0x0a4f4f4f
119	13:37:58.313982	0.062099	192.168.1.254	192.168.1.259	DHCP	302	00:0f:1d:0d:7d:38	DHCP ACK - Transaction ID 0x0a4f4f4f
120	13:37:58.392980	0.076087	192.168.1.259	224.0.0.252	DHCPv2	128	00:0f:1d:0d:7d:38	Membership Report group 224.0.0.252
121	13:37:58.392980	0.000000	192.168.1.259	224.0.0.2	DHCPv2	128	00:0f:1d:0d:7d:38	Leave Group 224.0.0.252
122	13:37:58.392980	0.000000	192.168.1.259	224.0.0.252	DHCPv2	128	00:0f:1d:0d:7d:38	Membership Report group 224.0.0.252
123	13:37:58.392980	0.000000	192.168.1.259	224.0.0.252	L2MP	157	00:0f:1d:0d:7d:38	Standard query 0x0c0c: 0x0 CSD-4-PW450KE
124	13:37:58.401980	0.000000	99.83.234.150	192.168.1.159	TCP	202	00:0f:1d:0d:7d:38	[TCP Retransmission] 403 > 50534 [FIN, RST, ACK] Seq=1 Ack=1 Win=0 Len=77
125	13:37:58.582984	0.020995	Inte1Cor_98/58:0f	Broadcast	ARP	120	00:0f:1d:0d:7d:38	who has 192.168.1.254? Tell 192.168.1.159
126	13:37:58.582984	0.000000	Altiocla_9e/50:af	Inte1Cor_98/58:0f	ARP	120	00:0f:1d:0d:7d:38	192.168.1.254 is at 58:fc:20:9e:50:af
127	13:37:58.527983	0.000994	192.168.1.159	192.168.1.254	DNS	156	00:0f:1d:0d:7d:38	Standard query 0x0537 A wpad.cisco.com
128	13:37:58.438986	0.100993	Inte1Cor_98/58:0f	Broadcast	ARP	124	00:0f:1d:0d:7d:38	who has 192.168.1.254? Tell 192.168.1.159
129	13:37:58.438986	0.002087	Altiocla_9e/50:af	Inte1Cor_98/58:0f	ARP	120	00:0f:1d:0d:7d:38	192.168.1.254 is at 58:fc:20:9e:50:af
130	13:37:58.438986	0.002087	Altiocla_9e/50:af	Inte1Cor_98/58:0f	ARP	120	00:0f:1d:0d:7d:38	Standard query response 0x0537 No such name A wpad.cisco.com SOA msl.cisco.com
131	13:37:58.438986	0.002087	192.168.1.254	192.168.1.159	DNS	195	00:0f:1d:0d:7d:38	Standard query response 0x0537 No such name A wpad.cisco.com SOA msl.cisco.com
132	13:37:58.438986	0.002087	192.168.1.254	192.168.1.159	DNS	151	00:0f:1d:0d:7d:38	Standard query response 0x0537 No such name A wpad.cisco.com SOA msl.cisco.com
133	13:37:58.438986	0.002087	192.168.1.254	192.168.1.159	DNS	254	00:0f:1d:0d:7d:38	Standard query response 0x0537 No such name A wpad.cisco.com SOA msl.cisco.com
134	13:37:58.438986	0.002087	192.168.1.254	192.168.1.159	DNS	254	00:0f:1d:0d:7d:38	Standard query response 0x0537 No such name A wpad.cisco.com SOA msl.cisco.com
135	13:37:58.723987	0.000994	192.168.1.159	224.0.0.252	DHCPv2	128	00:0f:1d:0d:7d:38	Membership Report group 224.0.0.252
136	13:37:58.723987	0.000000	192.168.1.259	224.0.0.252	DHCPv2	128	00:0f:1d:0d:7d:38	Membership Report group 224.0.0.252
137	13:37:58.800980	0.076087	192.168.1.259	224.0.0.252	L2MP	157	00:0f:1d:0d:7d:38	Standard query 0x0c0c: 0x0 CSD-4-PW450KE
138	13:37:58.800980	0.100993	192.168.1.259	224.0.0.252	DNS	165	00:0f:1d:0d:7d:38	Standard query 0x0c0c: A www.mftconnecttest.com
139	13:37:58.927982	0.013083	192.168.1.254	192.168.1.159	DNS	303	00:0f:1d:0d:7d:38	Standard query response 0x0c0c: A www.mftconnecttest.com CNAME ncsi-go.traffic
140	13:37:58.927982	0.000994	192.168.1.259	194.65.15.176	TCP	148	00:0f:1d:0d:7d:38	60437 > 80 [SYN] Seq=614048000 Len=0 MSS=256 SACK_PERM
141	13:37:58.927982	0.000000	192.168.1.259	194.65.15.176	TCP	136	00:0f:1d:0d:7d:38	80 > 60437 [SYN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
142	13:37:58.927982	0.002999	192.168.1.259	194.65.15.176	TCP	136	00:0f:1d:0d:7d:38	60437 > 80 [ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
143	13:37:58.927982	0.002999	192.168.1.259	194.65.15.176	HTTP	247	00:0f:1d:0d:7d:38	GET /connecttest.txt HTTP/1.1
144	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
145	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	HTTP	606	00:0f:1d:0d:7d:38	HTTP/1.1 200 OK (text/html)
146	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
147	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
148	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	136	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
149	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
150	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
151	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
152	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
153	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
154	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
155	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
156	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
157	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
158	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
159	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
160	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
161	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
162	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
163	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
164	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
165	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
166	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
167	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
168	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
169	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
170	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
171	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
172	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
173	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
174	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
175	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
176	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
177	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
178	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
179	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
180	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
181	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
182	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128
183	13:37:58.927982	0.000000	194.65.15.176	192.168.1.159	TCP	124	00:0f:1d:0d:7d:38	80 > 60437 [FIN, ACK] Seq=614048000 Len=0 MSS=256 SACK_PERM Win=128

```

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:

No.	Time	Delta	Source	Destination	Protocol	Length	Info
398	09:51:24.537423	0.000585	Cisco_d0:7d:38	Broadcast	802.11	354	00:0f:1d:dd:7d:38 Beacon frame, S=3093, P=0, Flags=.....C, BI=000, SSID="wif16E_EWA"
399	09:51:24.537508	0.000025	Cisco_d0:7d:38	Broadcast	802.11	311	00:0f:1d:dd:7d:38 Probe Response, S=3094, P=0, Flags=.....C, BI=100, SSID="wif16E_EWA"
399	09:51:24.537656	0.000048	Cisco_d0:7d:38	Broadcast	802.11	311	00:0f:1d:dd:7d:38 Probe Response, S=3095, P=0, Flags=.....C, BI=100, SSID="wif16E_EWA"
399	09:51:24.588572	0.000236	Samsung_c9:e3:71	Cisco_d0:7d:38	802.11	220	00:0f:1d:dd:7d:38 Probe Request, S=2051, P=0, Flags=.....C, SSID="wif16E_EWA"
399	09:51:24.588572	0.000000	192.168.1.125	192.168.1.125	802.11	76	Acknowledgement, Flags=.....C
399	09:51:24.589544	0.000072	Cisco_d0:7d:38	Samsung_c9:e3:71	802.11	311	00:0f:1d:dd:7d:38 Probe Response, S=2052, P=0, Flags=.....C, BI=100, SSID="wif16E_EWA"
399	09:51:24.589544	0.000000	192.168.1.125	192.168.1.125	802.11	76	Acknowledgement, Flags=.....C
399	09:51:24.589606	0.000052	Samsung_c9:e3:71	Cisco_d0:7d:38	802.11	96	00:0f:1d:dd:7d:38 Authentication, S=2052, P=0, Flags=.....C
399	09:51:24.589606	0.000000	192.168.1.125	192.168.1.125	802.11	76	Acknowledgement, Flags=.....C
399	09:51:24.593486	0.001790	Cisco_d0:7d:38	Samsung_c9:e3:71	802.11	96	00:0f:1d:dd:7d:38 Authentication, S=11, P=0, Flags=.....C
400	09:51:24.593486	0.000000	192.168.1.125	192.168.1.125	802.11	76	Acknowledgement, Flags=.....C
400	09:51:24.596809	0.000263	Samsung_c9:e3:71	Cisco_d0:7d:38	802.11	404	00:0f:1d:dd:7d:38 Association Request, S=2053, P=0, Flags=.....C, SSID="wif16E_EWA"
400	09:51:24.596809	0.000000	192.168.1.125	192.168.1.125	802.11	76	Acknowledgement, Flags=.....C
400	09:51:24.596809	0.000294	Cisco_d0:7d:38	Broadcast	802.11	311	00:0f:1d:dd:7d:38 Probe Response, S=3097, P=0, Flags=.....C, BI=100, SSID="wif16E_EWA"
400	09:51:24.604056	0.000077	Samsung_c9:e3:71	Cisco_d0:7d:38	802.11	134	00:0f:1d:dd:7d:38 S, func=00, N(0)=0; DSAP 0x00 Group, SSAP 0x04 Response
400	09:51:24.607923	0.000267	Cisco_d0:7d:38	Samsung_c9:e3:71	802.11	275	00:0f:1d:dd:7d:38 Association Response, S=0, P=0, Flags=.....C
400	09:51:24.607923	0.000000	192.168.1.125	192.168.1.125	802.11	76	Acknowledgement, Flags=.....C
412	09:51:24.611124	0.000465	Cisco_d0:7d:38	Samsung_c9:e3:71	EAPOL	221	00:0f:1d:dd:7d:38 Key (Message 1 of 4)
413	09:51:24.611124	0.000000	192.168.1.125	192.168.1.125	802.11	76	Acknowledgement, Flags=.....C
414	09:51:24.619609	0.000285	Cisco_d0:7d:38	Broadcast	802.11	311	00:0f:1d:dd:7d:38 Probe Response, S=3098, P=0, Flags=.....C, BI=100, SSID="wif16E_EWA"
415	09:51:24.629275	0.000566	Samsung_c9:e3:71	Cisco_d0:7d:38	EAPOL	243	00:0f:1d:dd:7d:38 Key (Message 2 of 4)
416	09:51:24.629275	0.000000	192.168.1.125	192.168.1.125	802.11	76	Acknowledgement, Flags=.....C
417	09:51:24.630862	0.000687	Cisco_d0:7d:38	Samsung_c9:e3:71	EAPOL	295	00:0f:1d:dd:7d:38 Key (Message 3 of 4)
418	09:51:24.630862	0.000000	192.168.1.125	192.168.1.125	802.11	76	Acknowledgement, Flags=.....C
419	09:51:24.635683	0.000741	Samsung_c9:e3:71	Cisco_d0:7d:38	EAPOL	139	00:0f:1d:dd:7d:38 Key (Message 4 of 4)
420	09:51:24.635683	0.000000	192.168.1.125	192.168.1.125	802.11	76	Acknowledgement, Flags=.....C
421	09:51:24.639768	0.000465	Cisco_d0:7d:38	Broadcast	802.11	354	00:0f:1d:dd:7d:38 Beacon frame, S=3099, P=0, Flags=.....C, BI=000, SSID="wif16E_EWA"
422	09:51:24.640941	0.000171	Cisco_Sc:F5:24	Samsung_c9:e3:71	LLC	183	00:0f:1d:dd:7d:38 S, func=00, N(0)=0; DSAP 0x06 Group, SSAP 0x02 Response

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:

No.	Time	Delta	Source	Destination	Protocol	Length	Info
985	09:52:26.722947	0.000000	0.0.0.0	255.255.255.255	DHCP	430	00:0f:1d:dd:7d:38 DHCP Request - Transaction ID 0d0ce63c8
986	09:52:26.722954	0.000007	0.0.0.0	255.255.255.255	DHCP	348	DHCP Request - Transaction ID 0d0ce63c8
989	09:52:26.748958	0.000004	192.168.1.254	192.168.1.160	DHCP	126	DHCP ACK - Transaction ID 0d0ce63c8
990	09:52:26.748958	0.000000	192.168.1.254	192.168.1.160	DHCP	392	00:0f:1d:dd:7d:38 DHCP ACK - Transaction ID 0d0ce63c8
1052	09:52:26.844042	0.000000	192.168.1.254	192.168.1.160	DNS	178	00:0f:1d:dd:7d:38 Standard query 0x12f A www.google.com
1054	09:52:26.845049	0.000007	192.168.1.254	192.168.1.160	DNS	96	Standard query response 0x12f A www.google.com A 142.250.110.188
1055	09:52:26.845049	0.000000	192.168.1.254	192.168.1.160	DNS	162	00:0f:1d:dd:7d:38 Standard query response 0x12f A www.google.com A 142.250.110.188
1074	09:52:26.857942	0.000000	192.168.1.254	192.168.1.160	DNS	171	00:0f:1d:dd:7d:38 Standard query 0x2b0 A connectivitycheck.gstatic.com
1075	09:52:26.857942	0.000000	192.168.1.254	192.168.1.160	DNS	89	Standard query response 0x2b0 A connectivitycheck.gstatic.com A 142.250.178.163
1076	09:52:26.858049	0.000007	192.168.1.254	192.168.1.160	DNS	169	Standard query response 0x2b0 A connectivitycheck.gstatic.com A 142.250.178.163
1077	09:52:26.858049	0.000000	192.168.1.254	192.168.1.160	DNS	175	00:0f:1d:dd:7d:38 Standard query response 0x2b0 A connectivitycheck.gstatic.com A 142.250.178.163
1094	09:52:26.862954	0.000000	192.168.1.254	192.168.1.160	DNS	156	00:0f:1d:dd:7d:38 Standard query 0x01f A www.google.com
1095	09:52:26.862954	0.000000	192.168.1.254	192.168.1.160	DNS	74	Standard query response 0x01f A www.google.com
1200	09:52:26.862946	0.000002	192.168.1.254	192.168.1.160	DNS	94	Standard query response 0x01f A www.google.com A 142.250.184.4
1301	09:52:26.862946	0.000000	192.168.1.254	192.168.1.160	DNS	160	00:0f:1d:dd:7d:38 Standard query response 0x01f A www.google.com A 142.250.184.4
1308	09:52:26.864345	0.000000	192.168.1.254	192.168.1.160	DNS	161	00:0f:1d:dd:7d:38 Standard query 0xc134 A time.cloudflare.com
1309	09:52:26.864345	0.000000	192.168.1.254	192.168.1.160	DNS	79	Standard query response 0xc134 A time.cloudflare.com
1322	09:52:26.877945	0.000000	192.168.1.254	192.168.1.160	DNS	115	Standard query response 0xc134 A time.cloudflare.com A 162.159.200.1 A 162.159.200.123
1323	09:52:26.877945	0.000000	192.168.1.254	192.168.1.160	DNS	181	00:0f:1d:dd:7d:38 Standard query response 0xc134 A time.cloudflare.com A 162.159.200.1 A 162.159.200.123
1335	09:52:26.962948	0.000000	192.168.1.254	142.250.178.163	TCP	136	00:0f:1d:dd:7d:38 13978 -> 80 [ACK] Seq=61085533 Len=0 Window=65536
1336	09:52:26.962948	0.000000	142.250.178.163	192.168.1.160	TCP	144	00:0f:1d:dd:7d:38 80 -> 13978 [ACK] Seq=61085533 Len=0 Window=65536
1347	09:52:26.964046	0.000000	192.168.1.254	142.250.178.163	TCP	140	00:0f:1d:dd:7d:38 13978 -> 80 [ACK] Seq=61085533 Len=0 Window=65536
1348	09:52:26.964046	0.000000	192.168.1.254	142.250.178.163	HTTP	375	00:0f:1d:dd:7d:38 GET /generate_204 HTTP/1.1
1349	09:52:26.964046	0.000000	142.250.178.163	192.168.1.160	TCP	136	00:0f:1d:dd:7d:38 80 -> 13978 [ACK] Seq=61085533 Len=0 Window=65536
1371	09:52:26.964046	0.000000	142.250.178.163	192.168.1.160	HTTP	360	00:0f:1d:dd:7d:38 HTTP/1.1 200 OK (text/html)
1381	09:52:26.967937	0.000290	142.250.178.163	142.250.178.163	TCP	140	00:0f:1d:dd:7d:38 13978 -> 80 [ACK] Seq=61085533 Len=0 Window=65536
1382	09:52:26.967937	0.000000	192.168.1.254	142.250.178.163	TCP	140	00:0f:1d:dd:7d:38 13978 -> 80 [ACK] Seq=61085533 Len=0 Window=65536
1383	09:52:26.967937	0.000000	142.250.178.163	192.168.1.160	TCP	136	00:0f:1d:dd:7d:38 80 -> 13978 [ACK] Seq=61085533 Len=0 Window=65536
1384	09:52:26.970938	0.000000	192.168.1.254	142.250.178.163	TCP	140	00:0f:1d:dd:7d:38 13978 -> 80 [ACK] Seq=61085533 Len=0 Window=65536

Packet capture detail on EWA

At this stage the client is in Web Auth Pending:

Cisco Catalyst 9800-CL Wireless Controller							Welcome admin	
Monitoring > Wireless > Clients							Last login 08/11/2023 09:25:08	
Clients								
Selected 0 out of 1 Clients								
☐	Client MAC Address	IPV4 Address	IPV6 Address	AP Name	SSID	WLAN ID	Client Type	State
☐	0429.2ec9.e371	192.168.1.160	fe80::6a20:34e8:ab1b:6332	AP9136_5C:F524	wifi_EWA	6	WLAN	Web Auth Pending

Cisco Catalyst 9800-CL Wireless Controller							Welcome admin	
Monitoring > Wireless > Clients							Last login 08/11/2023 09:25:08	
Clients								
Selected 0 out of 1 Clients								
☐	Client MAC Address	IPV4 Address	IPV6 Address	AP Name	SSID	WLAN ID	Client Type	State
☐	0429.2ec9.e371	192.168.1.160	fe80::6a20:34e8:ab1b:6332	AP9136_5C:F524	wifi_EWA	6	WLAN	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:

No.	Time	Delta	Source	Destination	Protocol	Length	855 Id	Info
2491	11:07:53.752705	0.302481	Cisco,d0:70:39	Broadcast	802.11	354	000f:0d:0d:70:39	Beacon frame, Src=328, Pw=0, Flags=.....C, B1=100, SSID="wifish_OA"
2499	11:07:53.808351	0.007666	Google,72:8a:66	Broadcast	802.11	203	ffff:ff:ff:ff:ff	Probe Request, Src=548, Pw=0, Flags=.....C, SSID="wifish_OA"
2498	11:07:53.813159	0.000000	Cisco,d0:70:39	Broadcast	802.11	211	000f:0d:0d:70:39	Probe Response, Src=3, Pw=0, Flags=.....C, B1=100, SSID="wifish_OA"
2501	11:07:53.853687	0.003476	Cisco,d0:70:39	Broadcast	802.11	354	000f:0d:0d:70:39	Beacon frame, Src=328, Pw=0, Flags=.....C, B1=100, SSID="wifish_OA"
2502	11:07:53.915746	0.006079	192.168.1.15	192.168.1.121	802.11	76		Clear-to-send, Flags=.....C
2504	11:07:53.944706	0.026960	Google,72:8a:66	Cisco,d0:70:39	802.11	100	000f:0d:0d:70:39	Authentication, Src=541, Pw=0, Flags=.....C
2505	11:07:53.944706	0.000000	192.168.1.15	192.168.1.121	802.11	76		ACKnowledgment, Flags=.....C
2506	11:07:53.944849	0.003743	Cisco,d0:70:39	Google,72:8a:66	802.11	100	000f:0d:0d:70:39	Authentication, Src=3, Pw=0, Flags=.....C
2507	11:07:53.944849	0.000000	192.168.1.15	192.168.1.121	802.11	76		ACKnowledgment, Flags=.....C
2508	11:07:53.945051	0.001802	Google,72:8a:66	Cisco,d0:70:39	802.11	308	000f:0d:0d:70:39	Association Request, Src=542, Pw=0, Flags=.....C, SSID="wifish_OA"
2509	11:07:53.945051	0.000000	192.168.1.15	192.168.1.121	802.11	76		ACKnowledgment, Flags=.....C
2512	11:07:53.957664	0.002213	Cisco,d0:70:39	Broadcast	802.11	354	000f:0d:0d:70:39	Beacon frame, Src=328, Pw=0, Flags=.....C, B1=100, SSID="wifish_OA"
2513	11:07:53.972307	0.016461	Google,72:8a:66	Broadcast	LLC	134	000f:0d:0d:70:39	I P, N(R)=24, N(S)=47; OSAP 0x00 Individual, SSAP 0x00 Command
2514	11:07:53.976328	0.000621	Cisco,d0:70:39	Google,72:8a:66	802.11	275	000f:0d:0d:70:39	Association Response, Src=0, Pw=0, Flags=.....C
2515	11:07:53.976328	0.000000	192.168.1.15	192.168.1.121	802.11	76		ACKnowledgment, Flags=.....C
2516	11:07:53.977705	0.001177	Cisco,d0:70:39	LAPOL	802.11	221	000f:0d:0d:70:39	Key (Message 1 of 4)
2517	11:07:53.977705	0.000000	192.168.1.15	192.168.1.121	802.11	76		ACKnowledgment, Flags=.....C
2518	11:07:54.018018	0.040113	Google,72:8a:66	Cisco,d0:70:39	LAPOL	243	000f:0d:0d:70:39	Key (Message 2 of 4)
2519	11:07:54.018018	0.000000	192.168.1.15	192.168.1.121	802.11	76		ACKnowledgment, Flags=.....C
2521	11:07:54.019598	0.001932	Cisco,d0:70:39	Google,72:8a:66	LAPOL	295	000f:0d:0d:70:39	Key (Message 3 of 4)
2522	11:07:54.019598	0.000000	192.168.1.15	192.168.1.121	802.11	76		ACKnowledgment, Flags=.....C
2523	11:07:54.027082	0.007111	Google,72:8a:66	Cisco,d0:70:39	LAPOL	109	000f:0d:0d:70:39	Key (Message 4 of 4)
2524	11:07:54.027082	0.000000	192.168.1.15	192.168.1.121	802.11	76		ACKnowledgment, Flags=.....C
2525	11:07:54.057008	0.026827	Google,72:8a:66	Cisco,d0:70:39	802.11	121	000f:0d:0d:70:39	Unknown Unprotected WPA Action[Malformed Packet: length of contained len exceeds length]
2526	11:07:54.057008	0.000000	192.168.1.15	192.168.1.121	802.11	76		ACKnowledgment, Flags=.....C
2527	11:07:54.060808	0.003612	Cisco,d0:70:39	Broadcast	802.11	354	000f:0d:0d:70:39	Beacon frame, Src=328, Pw=0, Flags=.....C, B1=100, SSID="wifish_OA"
2529	11:07:54.071154	0.010167	192.168.1.15	192.168.1.121	802.11	76		ACKnowledgment, Flags=.....C
2530	11:07:54.080805	0.008027	192.168.1.15	192.168.1.121	802.11	76		ACKnowledgment, Flags=.....C
2531	11:07:54.087535	0.007450	192.168.1.15	192.168.1.121	802.11	76		ACKnowledgment, Flags=.....C
2532	11:07:54.092209	0.006674	Cisco,fc:5c:fc:24	Google,72:8a:66	LLC	183	000f:0d:0d:70:39	I, N(R)=34, N(S)=108; OSAP 0x00 Individual, SSAP 0x00 Command
2533	11:07:54.092209	0.000000	192.168.1.15	192.168.1.121	802.11	76		ACKnowledgment, Flags=.....C
2534	11:07:54.092209	0.000000	Cisco,fc:5c:fc:24	Google,72:8a:66	LLC	183	000f:0d:0d:70:39	I, N(R)=97, N(S)=22; OSAP 0x00 Individual, SSAP 0x00 Command
2535	11:07:54.092209	0.000000	192.168.1.15	192.168.1.121	802.11	76		ACKnowledgment, Flags=.....C
2536	11:07:54.094370	0.002261	Cisco,d0:70:39	Google,72:8a:66	802.11	138	000f:0d:0d:70:39	Action, Src=1, Pw=0, Flags=.....C[Malformed Packet]
2537	11:07:54.094370	0.000000	192.168.1.15	192.168.1.121	802.11	76		ACKnowledgment, Flags=.....C
2538	11:07:54.094829	0.000459	Google,72:8a:66	Cisco,d0:70:39	802.11	115	000f:0d:0d:70:39	Action, Src=547, Pw=0, Flags=.....C
2539	11:07:54.094829	0.000000	192.168.1.15	192.168.1.121	802.11	76		ACKnowledgment, Flags=.....C
2540	11:07:54.095051	0.000000	192.168.1.15	192.168.1.121	802.11	76		ACKnowledgment, Flags=.....C

Frame 2508(1) 308 bytes on wire (2464 bits) captured on interface II, Src: Cisco,d0:70:39:47:7d:76:13, Dst: Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.121, User Datagram Protocol, Src Port: 5555, Dst Port: 5555, AirPeeh/Oem/Peek encapsulated IEEE 802.11 radio information

IEEE 802.11 Association Request, Flags=.....C

IEEE 802.11 Wireless Management

Fixed parameters (4 bytes)

Tagged parameters (124 bytes)

Tag: SSID parameter set: "wifish_OA"

Tag: Supported Rates (60), 0, 1, 2, 5.5, 11, 22, 36, 48, 54, 60, 66, 81, 96, 108, 120, 132, 144, 165, 180, 240, 270, 300, 360, 420, 480, 540, 600, 660, 720, 780, 840, 900, 960, 1080, 1140, 1200, 1260, 1320, 1380, 1440, 1500, 1560, 1620, 1680, 1740, 1800, 1860, 1920, 1980, 2040, 2100, 2160, 2220, 2280, 2340, 2400, 2460, 2520, 2580, 2640, 2700, 2760, 2820, 2880, 2940, 3000, 3060, 3120, 3180, 3240, 3300, 3360, 3420, 3480, 3540, 3600, 3660, 3720, 3780, 3840, 3900, 3960, 4020, 4080, 4140, 4200, 4260, 4320, 4380, 4440, 4500, 4560, 4620, 4680, 4740, 4800, 4860, 4920, 4980, 5040, 5100, 5160, 5220, 5280, 5340, 5400, 5460, 5520, 5580, 5640, 5700, 5760, 5820, 5880, 5940, 6000, 6060, 6120, 6180, 6240, 6300, 6360, 6420, 6480, 6540, 6600, 6660, 6720, 6780, 6840, 6900, 6960, 7020, 7080, 7140, 7200, 7260, 7320, 7380, 7440, 7500, 7560, 7620, 7680, 7740, 7800, 7860, 7920, 7980, 8040, 8100, 8160, 8220, 8280, 8340, 8400, 8460, 8520, 8580, 8640, 8700, 8760, 8820, 8880, 8940, 9000, 9060, 9120, 9180, 9240, 9300, 9360, 9420, 9480, 9540, 9600, 9660, 9720, 9780, 9840, 9900, 9960, 10020, 10080, 10140, 10200, 10260, 10320, 10380, 10440, 10500, 10560, 10620, 10680, 10740, 10800, 10860, 10920, 10980, 11040, 11100, 11160, 11220, 11280, 11340, 11400, 11460, 11520, 11580, 11640, 11700, 11760, 11820, 11880, 11940, 12000, 12060, 12120, 12180, 12240, 12300, 12360, 12420, 12480, 12540, 12600, 12660, 12720, 12780, 12840, 12900, 12960, 13020, 13080, 13140, 13200, 13260, 13320, 13380, 13440, 13500, 13560, 13620, 13680, 13740, 13800, 13860, 13920, 13980, 14040, 14100, 14160, 14220, 14280, 14340, 14400, 14460, 14520, 14580, 14640, 14700, 14760, 14820, 14880, 14940, 15000, 15060, 15120, 15180, 15240, 15300, 15360, 15420, 15480, 15540, 15600, 15660, 15720, 15780, 15840, 15900, 15960, 16020, 16080, 16140, 16200, 16260, 16320, 16380, 16440, 16500, 16560, 16620, 16680, 16740, 16800, 16860, 16920, 16980, 17040, 17100, 17160, 17220, 17280, 17340, 17400, 17460, 17520, 17580, 17640, 17700, 17760, 17820, 17880, 17940, 18000, 18060, 18120, 18180, 18240, 18300, 18360, 18420, 18480, 18540, 18600, 18660, 18720, 18780, 18840, 18900, 18960, 19020, 19080, 19140, 19200, 19260, 19320, 19380, 19440, 19500, 19560, 19620, 19680, 19740, 19800, 19860, 19920, 19980, 20040, 20100, 20160, 20220, 20280, 20340, 20400, 20460, 20520, 20580, 20640, 20700, 20760, 20820, 20880, 20940, 21000, 21060, 21120, 21180, 21240, 21300, 21360, 21420, 21480, 21540, 21600, 21660, 21720, 21780, 21840, 21900, 21960, 22020, 22080, 22140, 22200, 22260, 22320, 22380, 22440, 22500, 22560, 22620, 22680, 22740, 22800, 22860, 22920, 22980, 23040, 23100, 23160, 23220, 23280, 23340, 23400, 23460, 23520, 23580, 23640, 23700, 23760, 23820, 23880, 23940, 24000, 24060, 24120, 24180, 24240, 24300, 24360, 24420, 24480, 24540, 24600, 24660, 24720, 24780, 24840, 24900, 24960, 25020, 25080, 25140, 25200, 25260, 25320, 25380, 25440, 25500, 25560, 25620, 25680, 25740, 25800, 25860, 25920, 25980, 26040, 26100, 26160, 26220, 26280, 26340, 26400, 26460, 26520, 26580, 26640, 26700, 26760, 26820, 26880, 26940, 27000, 27060, 27120, 27180, 27240, 27300, 27360, 27420, 27480, 27540, 27600, 27660, 27720, 27780, 27840, 27900, 27960, 28020, 28080, 28140, 28200, 28260, 28320, 28380, 28440, 28500, 28560, 28620, 28680, 28740, 28800, 28860, 28920, 28980, 29040, 29100, 29160, 29220, 29280, 29340, 29400, 29460, 29520, 29580, 29640, 29700, 29760, 29820, 29880, 29940, 30000, 30060, 30120, 30180, 30240, 30300, 30360, 30420, 30480, 30540, 30600, 30660, 30720, 30780, 30840, 30900, 30960, 31020, 31080, 31140, 31200, 31260, 31320, 31380, 31440, 31500, 31560, 31620, 31680, 31740, 31800, 31860, 31920, 31980, 32040, 32100, 32160, 32220, 32280, 32340, 32400, 32460, 32520, 32580, 32640, 32700, 32760, 32820, 32880, 32940, 33000, 33060, 33120, 33180, 33240, 33300, 33360, 33420, 33480, 33540, 33600, 33660, 33720, 33780, 33840, 33900, 33960, 34020, 34080, 34140, 34200, 34260, 34320, 34380, 34440, 34500, 34560, 34620, 34680, 34740, 34800, 34860, 34920, 34980, 35040, 35100, 35160, 35220, 35280, 35340, 35400, 35460, 35520, 35580, 35640, 35700, 35760, 35820, 35880, 35940, 36000, 36060, 36120, 36180, 36240, 36300, 36360, 36420, 36480, 36540, 36600, 36660, 36720, 36780, 36840, 36900, 36960, 37020, 37080, 37140, 37200, 37260, 37320, 37380, 37440, 37500, 37560, 37620, 37680, 37740, 37800, 37860, 37920, 37980, 38040, 38100, 38160, 38220, 38280, 38340, 38400, 38460, 38520, 38580, 38640, 38700, 38760, 38820, 38880, 38940, 39000, 39060, 39120, 39180, 39240, 39300, 39360, 39420, 39480, 39540, 39600, 39660, 39720, 39780, 39840, 39900, 39960, 40020, 40080, 40140, 40200, 40260, 40320, 40380, 40440, 40500, 40560, 40620, 40680, 40740, 40800, 40860, 40920, 40980, 41040, 41100, 41160, 41220, 41280, 41340, 41400, 41460, 41520, 41580, 41640, 41700, 41760, 41820, 41880, 41940, 42000, 42060, 42120, 42180, 42240, 42300, 42360, 42420, 42480, 42540, 42600, 42660, 42720, 42780, 42840, 42900, 42960, 43020, 43080, 43140, 43200, 43260, 43320, 43380, 43440, 43500, 43560, 43620, 43680, 43740, 43800, 43860, 43920, 43980, 44040, 44100, 44160, 44220, 44280, 44340, 44400, 44460, 44520, 44580, 44640, 44700, 44760, 44820, 44880, 44940, 45000, 45060, 45120, 45180, 45240, 45300, 45360, 45420, 45480, 45540, 45600, 45660, 45720, 45780, 45840, 45900, 45960, 46020, 46080, 46140, 46200, 46260, 46320, 46380, 46440, 46500, 46560, 46620, 46680, 46740, 46800, 46860, 46920, 46980, 47040, 47100, 47160, 47220, 47280, 47340, 47400, 47460, 47520, 47580, 47640, 47700, 47760, 47820, 47880, 47940, 48000, 48060, 48120, 48180, 48240, 48300, 48360, 48420, 48480, 48540, 48600, 48660, 48720, 48780, 48840, 48900, 48960, 49020, 49080, 49140, 49200, 49260, 49320, 49380, 49440, 49500, 49560, 49620, 49680, 49740, 49800, 49860, 49920, 49980, 50040, 50100, 50160, 50220, 50280, 50340, 50400, 50460, 50520, 50580, 50640, 50700, 50760, 50820, 50880, 50940, 51000, 51060, 51120, 51180, 51240, 51300, 51360, 51420, 51480, 51540, 51600, 51660, 51720, 51780, 51840, 51900, 51960, 52020, 52080, 52140, 52200, 52260, 52320, 52380, 52440, 52500, 52560, 52620, 52680, 52740, 52800, 52860, 52920, 52980, 53040, 53100, 53160, 53220, 53280, 53340, 53400, 53460, 53520, 53580, 53640, 53700, 53760, 53820, 53880, 53940, 54000, 54060, 54120, 54180, 54240, 54300, 54360, 54420, 54480, 54540, 54600, 54660, 54720, 54780, 54840, 54900, 54960, 55020, 55080, 55140, 55200, 55260, 55320, 55380, 55440, 55500, 55560, 55620, 55680, 55740, 55800, 55860, 55920, 55980, 56040, 56100, 56160, 56220, 56280, 56340, 56400, 56460, 56520, 56580, 56640, 56700, 56760, 56820, 56880, 56940, 57000, 57060, 57120, 57180, 57240, 57300, 57360, 57420, 57480, 57540, 57600, 57660, 57720, 57780, 57840, 57900, 57960, 58020, 58080, 58140, 58200, 58260, 58320, 58380, 58440, 58500, 58560, 58620, 58680, 58740, 58800, 58860, 58920, 58980, 59040, 59100, 59160, 59220, 59280, 59340, 59400, 59460, 59520, 59580, 59640, 59700, 59760, 59820, 59880, 59940, 60000, 60060, 60120, 60180, 60240, 60300, 60360, 60420, 60480, 60540, 60600, 60660, 60720, 60780, 60840, 60900, 60960, 61020, 61080, 61140, 61200, 61260, 61320, 61380, 61440, 61500, 61560, 61620, 61680, 61740, 61800, 61860, 61920, 61980, 62040, 62100, 62160, 62220, 62280, 62340, 62400, 62460, 62520, 62580, 62640, 62700, 62760, 62820, 62880, 62940, 63000, 63060, 63120,

CWA OWE OTA connection

The image shows a Wireshark packet capture analysis of a RADIUS protocol exchange. The packet list on the left shows several packets, with the selected packet being an Access-Request (18) from 192.168.1.7 to 192.168.1.15. The packet details pane on the right shows the structure of the Access-Request (18) packet, including fields like User-Name, User-Password, Service-Type, and Framed-IP-Address.

No.	Time	Delta	Source	Destination	Protocol	Length	BSS Id	Info
288	12:43:25.848955	0.000000	192.168.1.15	192.168.1.7	RADIUS	436		Access-Request 18-18
293	12:43:25.862946	0.013991	192.168.1.7	192.168.1.15	RADIUS	584		Access-Accept 19-18
4806	12:43:45.353956	19.692918	192.168.1.15	192.168.1.7	RADIUS	436		Access-Request 18-20
4902	12:43:45.569962	0.025046	192.168.1.7	192.168.1.15	RADIUS	584		Access-Accept 19-20
12394	12:44:20.121980	34.742018	192.168.1.7	192.168.1.15	RADIUS	248		CoA-Request 10-4
12395	12:44:20.131979	0.000299	192.168.1.15	192.168.1.7	RADIUS	586		Access-Request 19-20
12396	12:44:20.131979	0.000000	192.168.1.15	192.168.1.7	RADIUS	111		CoA-Ack 10-4
12397	12:44:20.126978	0.012999	192.168.1.7	192.168.1.15	RADIUS	177		Access-Accept 19-20

Packet details for the selected packet (Access-Request 18-18):

- Code: Access-Request (1)
- Packet Identifier: 0x13 (19)
- Length: 396
- Authenticator: 46c29a8f2596a1ad76536f789c
- The response to this request is in frame 293
- Attribute Value Pairs
 - AVP: t=User-Name(1) 1-14 val=24952728a6
 - Type: 1
 - Length: 14
 - User-Name: 24952728a6
 - AVP: t=User-Password(2) 1-28 val=1ncry
 - AVP: t=Service-Type(4) 1-6 val=Call-Cl
 - AVP: t=Vendor-Specific(26) 1-11 vnd=cis
 - AVP: t=Framed-RTT(12) 1-6 val=1485
 - AVP: t=Message-Authenticator(80) 1-18
 - AVP: t=EAP-Key-Name(182) 1-2 val=
 - AVP: t=Vendor-Specific(26) 1-49 vnd=cis
 - AVP: t=Vendor-Specific(26) 1-18 vnd=cis
 - AVP: t=Vendor-Specific(26) 1-32 vnd=cis
 - AVP: t=Vendor-Specific(26) 1-17 vnd=cis
 - AVP: t=IPv6-Address(4) 1-6 val=192.16
 - AVP: t=IPv6-Port-Type(31) 1-6 val=strel
 - AVP: t=IPv6-Port(5) 1-6 val=112
 - AVP: t=Vendor-Specific(26) 1-34 vnd=cis
 - AVP: t=Vendor-Specific(26) 1-36 vnd=cis
 - AVP: t=Called-Station-ID(30) 1-30 val=

OEW CWA Mac filtering

CWA_PCAP.pcap

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

bootp or dns or tcp.port == 80

No.	Time	Delta	Source	Destination	Protocol	Length	BSS Id	Info
432	12:43:26.243975	1.366000	0.0.0.0	255.255.255.255	DHCP	424	00:0f:1d:dd:7d:30	DHCP Discover -> Transaction ID 0x00000001
433	12:43:26.244002	0.000000	0.0.0.0	255.255.255.255	DHCP	342		DHCP Discover -> Transaction ID 0x00000001
434	12:43:26.257982	0.013000	192.168.1.254	192.168.1.201	DHCP	326		DHCP Offer -> Transaction ID 0x00000001
435	12:43:26.257982	0.000000	192.168.1.201	192.168.1.254	DHCP	392	00:0f:1d:dd:7d:30	DHCP Offer -> Transaction ID 0x00000001
444	12:43:26.270982	0.013000	0.0.0.0	255.255.255.255	DHCP	434	00:0f:1d:dd:7d:30	DHCP Request -> Transaction ID 0x00000001
445	12:43:26.270982	0.000000	0.0.0.0	255.255.255.255	DHCP	352		DHCP Request -> Transaction ID 0x00000001
446	12:43:26.270971	0.000000	192.168.1.254	192.168.1.201	DHCP	326		DHCP ACK -> Transaction ID 0x00000001
447	12:43:26.270971	0.000000	192.168.1.201	192.168.1.254	DHCP	392	00:0f:1d:dd:7d:30	DHCP ACK -> Transaction ID 0x00000001
533	12:43:26.360973	0.000000	192.168.1.201	192.168.1.254	DNS	171	00:0f:1d:dd:7d:30	Standard query request 0x00000001 A connectivitecheck.gstatic.com
534	12:43:26.360973	0.000000	0.0.0.0	192.168.1.254	DNS	89		Standard query response 0x00000001 A connectivitecheck.gstatic.com
537	12:43:26.362972	0.002999	192.168.1.254	192.168.1.201	DNS	280		Standard query response 0x00000001 A connectivitecheck.gstatic.com A 142.250.184.3
538	12:43:26.362972	0.000000	192.168.1.201	192.168.1.254	DNS	175	00:0f:1d:dd:7d:30	Standard query request 0x00000001 A connectivitecheck.gstatic.com A 142.250.184.3
539	12:43:26.362972	0.000000	192.168.1.201	192.168.1.254	DNS	175	00:0f:1d:dd:7d:30	Standard query request 0x00000001 A connectivitecheck.gstatic.com A 142.250.184.3
542	12:43:26.380966	0.013995	192.168.1.201	192.168.1.254	DNS	158	00:0f:1d:dd:7d:30	Standard query request 0x00000001 A www.google.com
543	12:43:26.380966	0.000000	192.168.1.254	192.168.1.201	DNS	94		Standard query response 0x00000001 A www.google.com A 142.250.184.4
544	12:43:26.380966	0.000000	192.168.1.254	192.168.1.201	DNS	280	00:0f:1d:dd:7d:30	Standard query response 0x00000001 A www.google.com A 142.250.184.4
545	12:43:26.380966	0.000000	192.168.1.201	192.168.1.254	DNS	158	00:0f:1d:dd:7d:30	Standard query request 0x00000001 A www.google.com
546	12:43:26.380966	0.000000	192.168.1.201	192.168.1.254	DNS	76		Standard query request 0x00000001 A www.google.com
564	12:43:26.410974	0.012008	192.168.1.254	192.168.1.201	DNS	195		Standard query response 0x00000001 A www.google.com CNAME mobile-stalk.1.google.c
565	12:43:26.410974	0.000000	192.168.1.254	192.168.1.201	DNS	281	00:0f:1d:dd:7d:30	Standard query response 0x00000001 A www.google.com CNAME mobile-stalk.1.google.c
587	12:43:26.422967	0.012008	192.168.1.201	142.250.184.3	TCP	54		47738 -> 80 [WIN] Seq=65535 Len=65535 MSS=1460 SACK_PERM TSval=110867 TSecr=110867
588	12:43:26.422967	0.000000	142.250.184.3	192.168.1.201	TCP	54		80 -> 47738 [ACK] Seq=65535 Len=65535 MSS=1460 SACK_PERM TSval=26311 TSecr=110867
603	12:43:26.426964	0.000000	192.168.1.201	142.250.184.3	TCP	54		47738 -> 80 [ACK] Seq=65535 Len=65535 MSS=1460 SACK_PERM TSval=110867 TSecr=110867
604	12:43:26.426964	0.000000	192.168.1.201	142.250.184.3	HTTP	375		GET /generate_204 HTTP/1.1
607	12:43:26.426964	0.000000	142.250.184.3	192.168.1.201	TCP	54		80 -> 47738 [ACK] Seq=65535 Len=65535 MSS=1460 SACK_PERM TSval=26311 TSecr=110867
608	12:43:26.426964	0.000000	142.250.184.3	192.168.1.201	HTTP	994		HTTP/1.1 200 OK (text/html)
609	12:43:26.427971	0.000000	142.250.184.3	192.168.1.201	TCP	54		80 -> 47738 [FIN, ACK] Seq=65535 Len=0 MSS=1460 SACK_PERM TSval=26311 TSecr=110867
640	12:43:26.432976	0.000000	192.168.1.201	142.250.184.3	TCP	54		47738 -> 80 [ACK] Seq=228 Acks=859 Len=0 MSS=1460 SACK_PERM TSval=26311 TSecr=26311
641	12:43:26.432976	0.000000	142.250.184.3	192.168.1.201	TCP	54		80 -> 47738 [ACK] Seq=228 Acks=859 Len=0 MSS=1460 SACK_PERM TSval=110867 TSecr=26311
642	12:43:26.432976	0.000000	142.250.184.3	192.168.1.201	TCP	54		80 -> 47738 [ACK] Seq=228 Acks=859 Len=0 MSS=1460 SACK_PERM TSval=110867 TSecr=26311

Frame 608: 994 bytes on wire (7952 bits), 994 captured (7952 bits) on 0
Ethernet II, Src: Cisco-40:06:00:00:00:00, Dst: 02:00:00:00:00:00
Internet Protocol Version 4, Src: 192.168.1.15
User Datagram Protocol, Src Port: 5247, Dst Port: 80
Control And Provisioning of Wireless Access Protocol
IEEE 802.11 QoS Data, Flags:F.
Logical-Link Control
Internet Protocol Version 4, Src: 142.250.184.3
Transmission Control Protocol, Src Port: 80, Dst Port: 80
Hypertext Transfer Protocol
Line-based text data: text/html (9 lines)
<html>
<!--meta name="viewport" content="width=device-width, initial-scale=1.0">
</html>

DHCP Exchange

DNS Resolution for auto Redirection

Redirection to ISE portal

[...]
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.3598.580f
2023/08/08 13:37:58.198308994 {wncd_x_R0-0}{1}: [client-orch-state] [15154]: (note): MAC: 286b.3598.580f

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.3598.580f

Client auth-interface state transition: S_AUTHIF_ADD_MOBILE_ACK_WAIT_KM -> S_AUTHIF_PSK_AUTH_KEY_XCHNG_PENDING

2023/08/08 13:37:58.222547149 {mobilityd_R0-0}{1}: [mm-client] [16404]: (debug): MAC: 0000.0000.0000
2023/08/08 13:37:58.222630557 {mobilityd_R0-0}{1}: [mm-dgram-io] [16404]: (debug): MAC: 0000.0000.0000
2023/08/08 13:37:58.222641428 {mobilityd_R0-0}{1}: [mm-dgram-io] [16404]: (debug): MAC: 0000.0000.0000
2023/08/08 13:37:58.222666535 {wncd_x_R0-0}{1}: [client-keymgmt] [15154]: (info): MAC: 286b.3598.580f
2023/08/08 13:37:58.222678418 {wncd_x_R0-0}{1}: [client-keymgmt] [15154]: (info): MAC: 286b.3598.580f
2023/08/08 13:37:58.227626495 {wncd_x_R0-0}{1}: [client-keymgmt] [15154]: (info): MAC: 286b.3598.580f
2023/08/08 13:37:58.227791247 {wncd_x_R0-0}{1}: [client-keymgmt] [15154]: (info): MAC: 286b.3598.580f
2023/08/08 13:37:58.227792680 {wncd_x_R0-0}{1}: [client-keymgmt] [15154]: (info): MAC: 286b.3598.580f
2023/08/08 13:37:58.230572903 {wncd_x_R0-0}{1}: [client-keymgmt] [15154]: (info): MAC: 286b.3598.580f
2023/08/08 13:37:58.230575999 {wncd_x_R0-0}{1}: [client-keymgmt] [15154]: (note): MAC: 286b.3598.580f

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.3598.580f
2023/08/08 13:37:58.230702678 {wncd_x_R0-0}{1}: [client-auth] [15154]: (note): MAC: 286b.3598.580f
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.3598.580f:capw
2023/08/08 13:37:58.230834488 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [15154]: (info): [286b.3598.580f:capw
2023/08/08 13:37:58.230857151 {wncd_x_R0-0}{1}: [client-auth] [15154]: (info): MAC: 286b.3598.580f

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_90000000b

Param-map used: LocalWebAuth

2023/08/08 13:37:58.231251037 {wncd_x_R0-0}{1}: [webauth-state] [15154]: (info): capwap_9000000b[286b.3598.580f]
2023/08/08 13:37:58.231273499 {wncd_x_R0-0}{1}: [webauth-acl] [15154]: (info): capwap_9000000b[286b.3598.580f]

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 F
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.3598.580f]
2023/08/08 13:37:58.924590710 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_9000000b[286b.3598.580f]
2023/08/08 13:37:58.924606621 {wncd_x_R0-0}{1}: [webauth-httpd] [15154]: (info): capwap_9000000b[286b.3598.580f]
2023/08/08 13:37:58.924617631 {wncd_x_R0-0}{1}: [webauth-httpd] [15154]: (info): capwap_9000000b[286b.3598.580f]
2023/08/08 13:37:58.924646336 {wncd_x_R0-0}{1}: [webauth-httpd] [15154]: (info): capwap_9000000b[286b.3598.580f]
2023/08/08 13:37:58.924811559 {wncd_x_R0-0}{1}: [webauth-httpd] [15154]: (info): capwap_9000000b[286b.3598.580f]
2023/08/08 13:37:58.924823291 {wncd_x_R0-0}{1}: [webauth-state] [15154]: (info): capwap_9000000b[286b.3598.580f]
2023/08/08 13:37:58.924830184 {wncd_x_R0-0}{1}: [webauth-state] [15154]: (info): capwap_9000000b[286b.3598.580f]

State INIT -> GET_REDIRECT

2023/08/08 13:37:58.924836706 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_9000000b[286b.3598.580f]
2023/08/08 13:37:58.924893704 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_9000000b[286b.3598.580f]

[...]

2023/08/08 13:38:16.814516928 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_9000000b[286b.3598.580f]
2023/08/08 13:38:16.814739389 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_9000000b[286b.3598.580f]
2023/08/08 13:38:16.843721875 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_9000000b[286b.3598.580f]
2023/08/08 13:38:16.863779947 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_9000000b[286b.3598.580f]
2023/08/08 13:38:16.863799384 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_9000000b[286b.3598.580f]

[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.3598.580f]
2023/08/08 13:38:16.863857023 {wncd_x_R0-0}{1}: [webauth-httpd] [15154]: (info): capwap_9000000b[286b.3598.580f]
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.3598.580f]
2023/08/08 13:38:16.864026684 {wncd_x_R0-0}{1}: [webauth-state] [15154]: (info): capwap_9000000b[286b.3598.580f]
2023/08/08 13:38:16.864039067 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_9000000b[286b.3598.580f]
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.3598
2023/08/08 13:38:16.879513532 {wncd_x_R0-0}{1}: [webauth-state] [15154]: (info): capwap_9000000b[286b.3598
2023/08/08 13:38:16.879530745 {wncd_x_R0-0}{1}: [webauth-ac1] [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_ADDDE
```

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: 0429.2ec9
2023/08/10 14:35:20.685226454 {wncd_x_R0-0}{1}: [client-orch-state] [15195]: (note): MAC: 0429.2ec9
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_90000010

Param-map used: ExternalWebAuth

2023/08/10 14:35:20.740071629 {wncd_x_R0-0}{1}: [webauth-state] [15195]: (info): capwap_90000010

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_90000010

2023/08/10 14:35:20.740093601 {wncd_x_R0-0}{1}: [webauth-state] [15195]: (info): capwap_90000010

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: 0429.2ec9.e3
2023/08/10 14:35:21.944069521 {wncd_x_R0-0}{1}: [client-orch-sm] [15195]: (debug): MAC: 0429.2ec9.e3
2023/08/10 14:35:21.944074851 {wncd_x_R0-0}{1}: [client-orch-state] [15195]: (note): MAC: 0429.2ec9.e3
2023/08/10 14:35:21.944201671 {wncd_x_R0-0}{1}: [dot1x] [15195]: (info): [0000.0000.0000:capwap_900000010]
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_900000010[04
2023/08/10 14:35:24.110679789 {wncd_x_R0-0}{1}: [webauth-io] [15195]: (info): capwap_900000010[04
2023/08/10 14:35:24.110699827 {wncd_x_R0-0}{1}: [webauth-httpd] [15195]: (info): capwap_900000010
```

GET rcvd when in LOGIN state

```
2023/08/10 14:35:24.110718893 {wncd_x_R0-0}{1}: [webauth-httpd] [15195]: (info): capwap_900000010
```

HTTP GET request

```
2023/08/10 14:35:24.110754721 {wncd_x_R0-0}{1}: [webauth-httpd] [15195]: (info): capwap_900000010
2023/08/10 14:35:24.110951163 {wncd_x_R0-0}{1}: [webauth-httpd] [15195]: (info): capwap_900000010
2023/08/10 14:35:24.110960801 {wncd_x_R0-0}{1}: [webauth-state] [15195]: (info): capwap_900000010
```

Param-map used: ExternalWebAuth

```
2023/08/10 14:35:24.110971331 {wncd_x_R0-0}{1}: [webauth-state] [15195]: (info): capwap_900000010
2023/08/10 14:35:24.111046654 {wncd_x_R0-0}{1}: [webauth-page] [15195]: (info): capwap_900000010
```

[...]

```
2023/08/10 14:35:35.761960632 {wncd_x_R0-0}{1}: [webauth-io] [15195]: (info): capwap_900000010[04
2023/08/10 14:35:35.776669018 {wncd_x_R0-0}{1}: [webauth-io] [15195]: (info): capwap_900000010[04
2023/08/10 14:35:37.805884475 {wncd_x_R0-0}{1}: [webauth-io] [15195]: (info): capwap_900000010[04
2023/08/10 14:35:37.807261842 {wncd_x_R0-0}{1}: [webauth-io] [15195]: (info): capwap_900000010[04
2023/08/10 14:35:37.807273253 {wncd_x_R0-0}{1}: [webauth-httpd] [15195]: (info): capwap_900000010
```

POST rcvd when in LOGIN state

```
2023/08/10 14:35:37.807287911 {wncd_x_R0-0}{1}: [webauth-httpd] [15195]: (info): capwap_900000010
2023/08/10 14:35:37.807331213 {wncd_x_R0-0}{1}: [webauth-httpd] [15195]: (info): capwap_900000010
```

[...]

```
2023/08/10 14:35:37.807498470 {wncd_x_R0-0}{1}: [webauth-state] [15195]: (info): capwap_900000010
```

Param-map used: ExternalWebAuth

```
2023/08/10 14:35:37.807503619 {wncd_x_R0-0}{1}: [webauth-state] [15195]: (info): capwap_900000010
2023/08/10 14:35:37.807515502 {wncd_x_R0-0}{1}: [webauth-io] [15195]: (info): capwap_900000010[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-Addri
2023/08/10 14:35:37.807682217 {wncd_x_R0-0}{1}: [radius] [15195]: (info): RADIUS: Message-Authen
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: 2495.2f72.8a66

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:capwap]

2023/08/11 12:43:45.551935427 {wncd_x_R0-0}{1}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:capwap]

2023/08/11 12:43:45.551947760 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [15200]: (info): [2495.2f72.8a66:capwap]

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-Authenticator

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-Identifie
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: 2495.2f72.8a66

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: 2495.2f72.8a66
2023/08/11 12:43:45.576138984 {wncd_x_R0-0}{1}: [client-keymgmt] [15200]: (info): MAC: 2495.2f72.8a66
2023/08/11 12:43:45.576247599 {mobilityd_R0-0}{1}: [mm-client] [16431]: (debug): MAC: 0000.0000.0000
2023/08/11 12:43:45.576379639 {mobilityd_R0-0}{1}: [mm-dgram-io] [16431]: (debug): MAC: 0000.0000.0000
2023/08/11 12:43:45.576397212 {mobilityd_R0-0}{1}: [mm-dgram-io] [16431]: (debug): MAC: 0000.0000.0000
2023/08/11 12:43:45.632584865 {wncd_x_R0-0}{1}: [client-keymgmt] [15200]: (info): MAC: 2495.2f72.8a66
2023/08/11 12:43:45.632765557 {wncd_x_R0-0}{1}: [client-keymgmt] [15200]: (info): MAC: 2495.2f72.8a66
2023/08/11 12:43:45.632766960 {wncd_x_R0-0}{1}: [client-keymgmt] [15200]: (info): MAC: 2495.2f72.8a66
2023/08/11 12:43:45.641844995 {wncd_x_R0-0}{1}: [client-keymgmt] [15200]: (info): MAC: 2495.2f72.8a66
2023/08/11 12:43:45.641846798 {wncd_x_R0-0}{1}: [client-keymgmt] [15200]: (note): MAC: 2495.2f72.8a66

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: 2495.2f72.8a66
[...]
2023/08/11 12:43:45.645536693 {wncd_x_R0-0}{1}: [client-orch-state] [15200]: (note): MAC: 2495.2f72.8a66

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:capwap]
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): [2495.2f72.8a66]
2023/08/11 12:43:46.104460371 {wncd_x_R0-0}{1}: [client-iplearn] [15200]: (info): MAC: 2495.2f72.8a66
2023/08/11 12:43:46.104607690 {wncd_x_R0-0}{1}: [client-orch-sm] [15200]: (debug): MAC: 2495.2f72.8a66
2023/08/11 12:43:46.104669668 {wncd_x_R0-0}{1}: [client-orch-sm] [15200]: (debug): MAC: 2495.2f72.8a66
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 address
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 address
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] 0
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 [1
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 [1
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-Static
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-ID
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-Authenticat
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-Authen
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): RADIUS: 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 v

[...]

```
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](#)