

# 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 WiFi 6E is the same as in WiFi 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 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 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](#) .

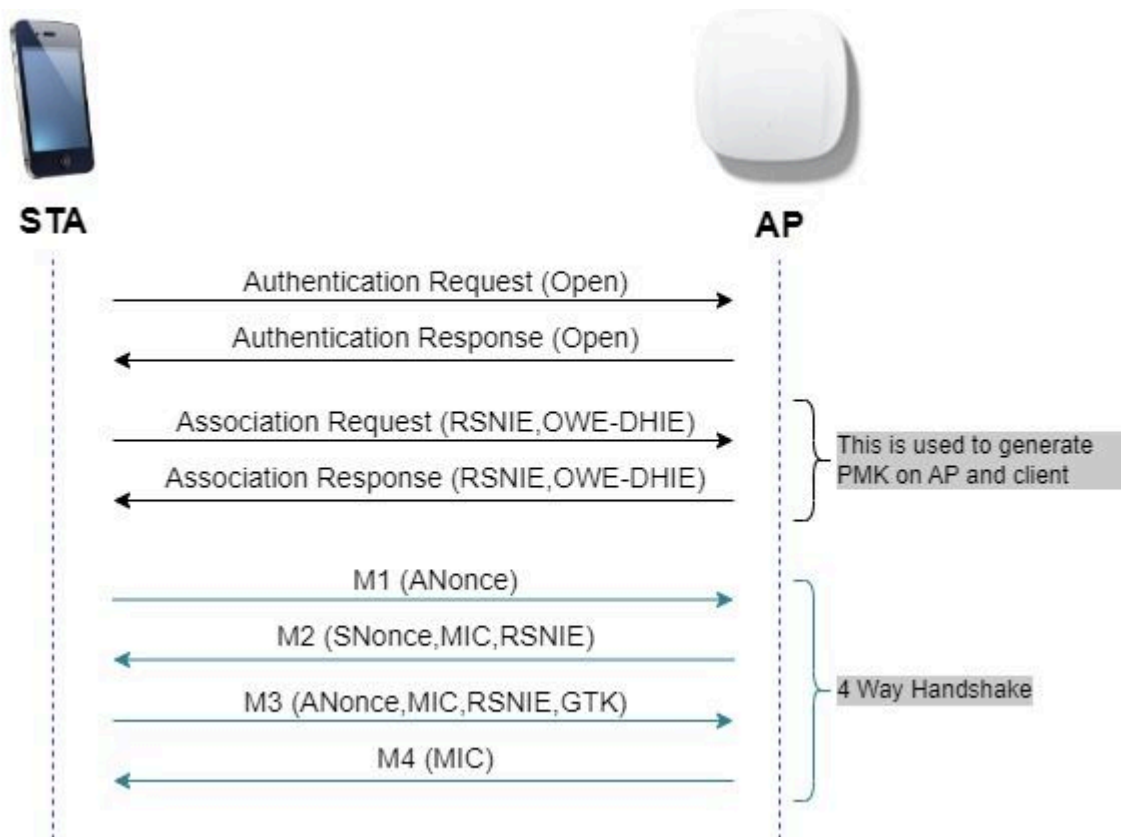
Traditionally, Wi-Fi hotspots and guest WLANs have used open security without encryption or authentication. The Wi-Fi CERTIFIED Enhanced Open certification defines improved data privacy in open

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.

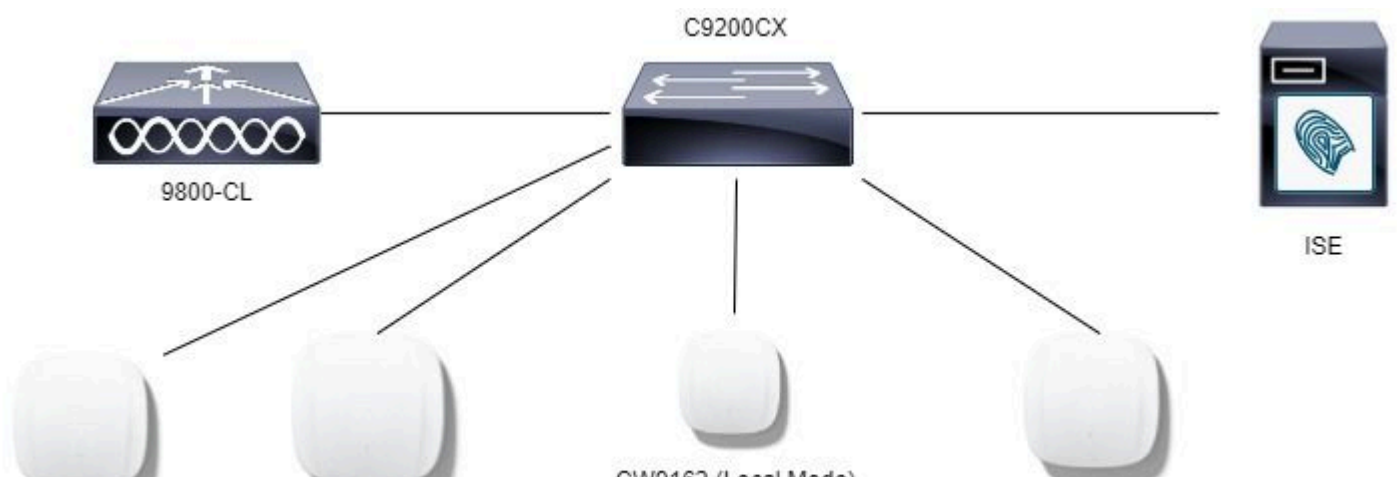
The Layer 2 Security settings are be locked to Opportunistic Wireless Encryption (OWE) which is the closest to an "Open" network we can have in WiFi 6E.

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:





```

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_did:70:38	Broadcast	802.11	354	00:ff:fd:dd:7d:38
399	09:51:24.537748	0.000325	Cisco_did:70:38	Broadcast	802.11	311	00:ff:fd:dd:7d:38
402	09:51:24.578356	0.000408	Cisco_did:70:38	Broadcast	802.11	311	00:ff:fd:dd:7d:38
403	09:51:24.588572	0.000226	Samsung_c9:e3:71	Cisco_did:7d:38	802.11	230	00:ff:fd:dd:7d:38
404	09:51:24.588572	0.000000	192.168.1.121	192.168.1.121	802.11	76	
405	09:51:24.589544	0.000072	Cisco_did:70:38	Samsung_c9:e3:71	802.11	311	00:ff:fd:dd:7d:38
406	09:51:24.589544	0.000000	192.168.1.121	192.168.1.121	802.11	76	
407	09:51:24.589606	0.000152	Samsung_c9:e3:71	Cisco_did:7d:38	802.11	96	00:ff:fd:dd:7d:38
408	09:51:24.589606	0.000000	192.168.1.121	192.168.1.121	802.11	76	
409	09:51:24.593486	0.001796	Cisco_did:70:38	Samsung_c9:e3:71	802.11	96	00:ff:fd:dd:7d:38
400	09:51:24.593486	0.000000	192.168.1.121	192.168.1.121	802.11	76	
401	09:51:24.596889	0.002683	Samsung_c9:e3:71	Cisco_did:7d:38	802.11	404	00:ff:fd:dd:7d:38
402	09:51:24.596889	0.000000	192.168.1.121	192.168.1.121	802.11	76	
403	09:51:24.596889	0.002594	Cisco_did:70:38	Broadcast	802.11	311	00:ff:fd:dd:7d:38
404	09:51:24.604556	0.000873	Samsung_c9:e3:71	802.11	114	00:ff:fd:dd:7d:38	
405	09:51:24.607923	0.001267	Cisco_did:70:38	Samsung_c9:e3:71	802.11	275	00:ff:fd:dd:7d:38
406	09:51:24.607923	0.000000	192.168.1.121	192.168.1.121	802.11	76	
412	09:51:24.611124	0.001045	Cisco_did:70:38	Samsung_c9:e3:71	802.11	221	00:ff:fd:dd:7d:38
413	09:51:24.611124	0.000000	192.168.1.121	192.168.1.121	802.11	76	
414	09:51:24.612069	0.000285	Cisco_did:70:38	Broadcast	802.11	311	00:ff:fd:dd:7d:38
415	09:51:24.629275	0.000566	Samsung_c9:e3:71	Cisco_did:7d:38	802.11	243	00:ff:fd:dd:7d:38
416	09:51:24.629275	0.000000	192.168.1.121	192.168.1.121	802.11	76	
417	09:51:24.630862	0.000587	Cisco_did:70:38	Samsung_c9:e3:71	802.11	295	00:ff:fd:dd:7d:38
418	09:51:24.630862	0.000000	192.168.1.121	192.168.1.121	802.11	76	
419	09:51:24.635683	0.000743	Samsung_c9:e3:71	Cisco_did:7d:38	802.11	139	00:ff:fd:dd:7d:38
420	09:51:24.635683	0.000000	192.168.1.121	192.168.1.121	802.11	76	
421	09:51:24.639758	0.004165	Cisco_did:70:38	Broadcast	802.11	354	00:ff:fd:dd:7d:38
422	09:51:24.640941	0.002173	Cisco_Sc:F5:24	Samsung_c9:e3:71	LLC	183	00:ff:fd:dd:7d:38

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:

The image shows a Wireshark capture of network traffic. Key packets are annotated:

- DHCP Exchange:** A series of DHCP messages (Request, Offer, ACK) between the client and the DHCP server.
- DNS Resolution for auto redirection:** Multiple DNS queries for domains like 'www.google.com' and 'time.cloudflare.com'.
- EWA Redirection for external login portal:** HTTP GET requests to 'http://1.200.0k' and subsequent 302 redirects to external login portals.

Packet capture detail on EWA

At this stage the client is in Web Auth Pending:

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The 'Clients' tab is active, and a client with MAC address 0429.2ec9.a371 is shown in the 'Web Auth Pending' state.

Client MAC Address	IPv4 Address	IPv6 Address	AP Name	SSID	WLAN ID	Client Type	Status
0429.2ec9.a371	192.168.1.160	fe80::6a20:34e8:ab1b:6332	AP9136_5C.F524	wME_EWA	6	WLAN	Web Auth Pending

EWA client in Web Auth Pending

This is another view of the Cisco Catalyst 9800-CL Wireless Controller interface, showing the same client in the 'Web Auth Pending' state. The interface includes navigation menus for Dashboard, Monitoring, Configuration, and Administration.

```

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	BSS Id	Info
2493	11:07:53.752705	0.000443	Cisco_d6:7c:39	Broadcast	802.11	354	00:0f:1d:0d:7d:39	Beacon frame, S/W=120, F/W=0, Flags=.....C, BI=100, SSID="wifisat_0A"
2499	11:07:53.808353	0.000546	Google_72:8a:66	Broadcast	802.11	203	ff:ff:ff:ff:ff:ff:ff	Probe Request, S/W=1540, F/W=0, Flags=.....C, SSID="wifisat_0A"
2500	11:07:53.8125193	0.001240	Cisco_d6:7c:39	Broadcast	802.11	354	00:0f:1d:0d:7d:39	Probe Response, S/W=1, F/W=0, Flags=.....C, BI=100, SSID="wifisat_0A"
2501	11:07:53.850667	0.000476	Cisco_d6:7c:39	Broadcast	802.11	354	00:0f:1d:0d:7d:39	Beacon frame, S/W=121, F/W=0, Flags=.....C, BI=100, SSID="wifisat_0A"
2502	11:07:53.925746	0.006079	192.168.1.121	192.168.1.121	802.11	76		Clear-to-send, Flags=.....C
2504	11:07:53.944706	0.020950	Google_72:8a:66	Cisco_d6:7c:39	802.11	108	00:0f:1d:0d:7d:39	Authentication, S/W=1541, F/W=0, Flags=.....C
2505	11:07:53.944706	0.000000	192.168.1.121	192.168.1.121	802.11	76		Acknowledgment, Flags=.....C
2506	11:07:53.948449	0.001743	Cisco_d6:7c:39	Google_72:8a:66	802.11	108	00:0f:1d:0d:7d:39	Authentication, S/W=1, F/W=0, Flags=.....C
2507	11:07:53.948449	0.000000	192.168.1.121	192.168.1.121	802.11	76		Acknowledgment, Flags=.....C
2508	11:07:53.948451	0.001002	Google_72:8a:66	Cisco_d6:7c:39	802.11	308	00:0f:1d:0d:7d:39	Association Request, S/W=1542, F/W=0, Flags=.....C, SSID="wifisat_0A"
2509	11:07:53.948451	0.000000	192.168.1.121	192.168.1.121	802.11	76		Acknowledgment, Flags=.....C
2512	11:07:53.976787	0.000211	Cisco_d6:7c:39	Broadcast	802.11	354	00:0f:1d:0d:7d:39	Beacon frame, S/W=123, F/W=0, Flags=.....C, BI=100, SSID="wifisat_0A"
2513	11:07:53.976787	0.000461	Google_72:8a:66	Broadcast	LIC	134	00:0f:1d:0d:7d:39	I, N(X)=24, N(S)=07: DSAP Basic Individual, SSAP Net8025 Command
2514	11:07:53.976788	0.000021	Cisco_d6:7c:39	Google_72:8a:66	802.11	275	00:0f:1d:0d:7d:39	Association Response, S/W=0, F/W=0, Flags=.....C
2515	11:07:53.976788	0.000000	192.168.1.121	192.168.1.121	802.11	76		Acknowledgment, Flags=.....C
2516	11:07:53.977705	0.001377	Google_72:8a:66	Cisco_d6:7c:39	EAPOL	221	00:0f:1d:0d:7d:39	Key (Message 1 of 4)
2517	11:07:53.977705	0.000000	192.168.1.121	192.168.1.121	802.11	76		Acknowledgment, Flags=.....C
2518	11:07:53.977705	0.000133	Google_72:8a:66	Cisco_d6:7c:39	EAPOL	243	00:0f:1d:0d:7d:39	Key (Message 2 of 4)
2519	11:07:54.018038	0.000000	192.168.1.121	192.168.1.121	802.11	76		Acknowledgment, Flags=.....C
2521	11:07:54.019950	0.000192	Cisco_d6:7c:39	Google_72:8a:66	EAPOL	295	00:0f:1d:0d:7d:39	Key (Message 3 of 4)
2522	11:07:54.019950	0.000000	192.168.1.121	192.168.1.121	802.11	76		Acknowledgment, Flags=.....C
2523	11:07:54.027081	0.000713	Google_72:8a:66	Cisco_d6:7c:39	EAPOL	199	00:0f:1d:0d:7d:39	Key (Message 4 of 4)
2524	11:07:54.027081	0.000000	192.168.1.121	192.168.1.121	802.11	76		Acknowledgment, Flags=.....C
2525	11:07:54.053908	0.024827	Google_72:8a:66	Cisco_d6:7c:39	802.11	111	00:0f:1d:0d:7d:39	Unknown Unprotected WLAN Action[Malformed Packet: length of contained item exceeds length]
2526	11:07:54.053908	0.000000	192.168.1.121	192.168.1.121	802.11	76		Acknowledgment, Flags=.....C
2527	11:07:54.060000	0.006172	Cisco_d6:7c:39	Broadcast	802.11	354	00:0f:1d:0d:7d:39	Beacon frame, S/W=124, F/W=0, Flags=.....C, BI=100, SSID="wifisat_0A"
2529	11:07:54.071158	0.011079	192.168.1.121	192.168.1.121	802.11	76		Acknowledgment, Flags=.....C
2530	11:07:54.080000	0.000027	192.168.1.121	192.168.1.121	802.11	76		Acknowledgment, Flags=.....C
2531	11:07:54.087515	0.007450	192.168.1.121	192.168.1.121	802.11	76		Acknowledgment, Flags=.....C
2532	11:07:54.092200	0.000674	Cisco_Sc:75:24	Google_72:8a:66	LIC	183	00:0f:1d:0d:7d:39	I, N(X)=14, N(S)=20: DSAP Basic Individual, SSAP Basic Command
2533	11:07:54.092200	0.000000	192.168.1.121	192.168.1.121	802.11	76		Acknowledgment, Flags=.....C
2534	11:07:54.092200	0.000000	Cisco_Sc:75:24	Google_72:8a:66	LIC	183	00:0f:1d:0d:7d:39	I, N(X)=07, N(S)=22: DSAP Basic Individual, SSAP Basic Command
2535	11:07:54.092200	0.000000	192.168.1.121	192.168.1.121	802.11	76		Acknowledgment, Flags=.....C
2536	11:07:54.094370	0.002143	Cisco_d6:7c:39	Google_72:8a:66	802.11	118	00:0f:1d:0d:7d:39	Action, S/W=1, F/W=0, Flags=.....[Malformed Packet]
2537	11:07:54.094370	0.000000	192.168.1.121	192.168.1.121	802.11	76		Acknowledgment, Flags=.....C
2538	11:07:54.094829	0.000410	Google_72:8a:66	Cisco_d6:7c:39	802.11	115	00:0f:1d:0d:7d:39	Action, S/W=1547, F/W=0, Flags=.....C
2539	11:07:54.094829	0.000000	192.168.1.121	192.168.1.121	802.11	76		Acknowledgment, Flags=.....C
2540	11:07:54.101300	0.000701	Cisco_d6:7c:39	Broadcast	802.11	354	00:0f:1d:0d:7d:39	Beacon frame, S/W=125, F/W=0, Flags=.....C, BI=100, SSID="wifisat_0A"

```

> Frame 2508: 308 bytes on wire (2464 bits), 436
> Ethernet II, Src: Cisco_d6:7c:39 (7d:39:39:39:39:39)
> Internet Protocol Version 4, Src: 192.168.1.121
> User Datagram Protocol, Src Port: 5555
> All/IPv6/IPv4/IPv6 encapsulated IEEE 802.11
> IEEE 802.11 Association Request, Flags=.....C
  > Fixed parameters (4 bytes)
  > Tagged parameters (234 bytes)
    > Tag: SSID parameter set: "wifisat_0A"
    > Tag: Supported rates (60), 9, 11, 12, 18, 24, 36, 48, 54, 60, 66, 72, 81, 90, 96, 108, 120, 132, 144, 150, 162, 180, 192, 200, 216, 225, 234, 240, 252, 270, 288, 300, 312, 324, 336, 348, 360, 378, 396, 420, 432, 450, 468, 480, 495, 510, 522, 540, 558, 576, 594, 612, 630, 648, 666, 684, 702, 720, 735, 750, 765, 780, 798, 810, 825, 840, 855, 870, 885, 900, 915, 930, 945, 960, 975, 990, 1008, 1020, 1035, 1050, 1065, 1080, 1095, 1110, 1125, 1140, 1155, 1170, 1185, 1200, 1215, 1230, 1245, 1260, 1275, 1290, 1305, 1320, 1335, 1350, 1365, 1380, 1395, 1410, 1425, 1440, 1455, 1470, 1485, 1500, 1515, 1530, 1545, 1560, 1575, 1590, 1605, 1620, 1635, 1650, 1665, 1680, 1695, 1710, 1725, 1740, 1755, 1770, 1785, 1800, 1815, 1830, 1845, 1860, 1875, 1890, 1905, 1920, 1935, 1950, 1965, 1980, 1995, 2010, 2025, 2040, 2055, 2070, 2085, 2100, 2115, 2130, 2145, 2160, 2175, 2190, 2205, 2220, 2235, 2250, 2265, 2280, 2295, 2310, 2325, 2340, 2355, 2370, 2385, 2400, 2415, 2430, 2445, 2460, 2475, 2490, 2505, 2520, 2535, 2550, 2565, 2580, 2595, 2610, 2625, 2640, 2655, 2670, 2685, 2700, 2715, 2730, 2745, 2760, 2775, 2790, 2805, 2820, 2835, 2850, 2865, 2880, 2895, 2910, 2925, 2940, 2955, 2970, 2985, 3000, 3015, 3030, 3045, 3060, 3075, 3090, 3105, 3120, 3135, 3150, 3165, 3180, 3195, 3210, 3225, 3240, 3255, 3270, 3285, 3300, 3315, 3330, 3345, 3360, 3375, 3390, 3405, 3420, 3435, 3450, 3465, 3480, 3495, 3510, 3525, 3540, 3555, 3570, 3585, 3600, 3615, 3630, 3645, 3660, 3675, 3690, 3705, 3720, 3735, 3750, 3765, 3780, 3795, 3810, 3825, 3840, 3855, 3870, 3885, 3900, 3915, 3930, 3945, 3960, 3975, 3990, 4005, 4020, 4035, 4050, 4065, 4080, 4095, 4110, 4125, 4140, 4155, 4170, 4185, 4200, 4215, 4230, 4245, 4260, 4275, 4290, 4305, 4320, 4335, 4350, 4365, 4380, 4395, 4410, 4425, 4440, 4455, 4470, 4485, 4500, 4515, 4530, 4545, 4560, 4575, 4590, 4605, 4620, 4635, 4650, 4665, 4680, 4695, 4710, 4725, 4740, 4755, 4770, 4785, 4800, 4815, 4830, 4845, 4860, 4875, 4890, 4905, 4920, 4935, 4950, 4965, 4980, 4995, 5010, 5025, 5040, 5055, 5070, 5085, 5100, 5115, 5130, 5145, 5160, 5175, 5190, 5205, 5220, 5235, 5250, 5265, 5280, 5295, 5310, 5325, 5340, 5355, 5370, 5385, 5400, 5415, 5430, 5445, 5460, 5475, 5490, 5505, 5520, 5535, 5550, 5565, 5580, 5595, 5610, 5625, 5640, 5655, 5670, 5685, 5700, 5715, 5730, 5745, 5760, 5775, 5790, 5805, 5820, 5835, 5850, 5865, 5880, 5895, 5910, 5925, 5940, 5955, 5970, 5985, 6000, 6015, 6030, 6045, 6060, 6075, 6090, 6105, 6120, 6135, 6150, 6165, 6180, 6195, 6210, 6225, 6240, 6255, 6270, 6285, 6300, 6315, 6330, 6345, 6360, 6375, 6390, 6405, 6420, 6435, 6450, 6465, 6480, 6495, 6510, 6525, 6540, 6555, 6570, 6585, 6600, 6615, 6630, 6645, 6660, 6675, 6690, 6705, 6720, 6735, 6750, 6765, 6780, 6795, 6810, 6825, 6840, 6855, 6870, 6885, 6900, 6915, 6930, 6945, 6960, 6975, 6990, 7005, 7020, 7035, 7050, 7065, 7080, 7095, 7110, 7125, 7140, 7155, 7170, 7185, 7200, 7215, 7230, 7245, 7260, 7275, 7290, 7305, 7320, 7335, 7350, 7365, 7380, 7395, 7410, 7425, 7440, 7455, 7470, 7485, 7500, 7515, 7530, 7545, 7560, 7575, 7590, 7605, 7620, 7635, 7650, 7665, 7680, 7695, 7710, 7725, 7740, 7755, 7770, 7785, 7800, 7815, 7830, 7845, 7860, 7875, 7890, 7905, 7920, 7935, 7950, 7965, 7980, 7995, 8010, 8025, 8040, 8055, 8070, 8085, 8100, 8115, 8130, 8145, 8160, 8175, 8190, 8205, 8220, 8235, 8250, 8265, 8280, 8295, 8310, 8325, 8340, 8355, 8370, 8385, 8400, 8415, 8430, 8445, 8460, 8475, 8490, 8505, 8520, 8535, 8550, 8565, 8580, 8595, 8610, 8625, 8640, 8655, 8670, 8685, 8700, 8715, 8730, 8745, 8760, 8775, 8790, 8805, 8820, 8835, 8850, 8865, 8880, 8895, 8910, 8925, 8940, 8955, 8970, 8985, 9000, 9015, 9030, 9045, 9060, 9075, 9090, 9105, 9120, 9135, 9150, 9165, 9180, 9195, 9210, 9225, 9240, 9255, 9270, 9285, 9300, 9315, 9330, 9345, 9360, 9375, 9390, 9405, 9420, 9435, 9450, 9465, 9480, 9495, 9510, 9525, 9540, 9555, 9570, 9585, 9600, 9615, 9630, 9645, 9660, 9675, 9690, 9705, 9720, 9735, 9750, 9765, 9780, 9795, 9810, 9825, 9840, 9855, 9870, 9885, 9900, 9915, 9930, 9945, 9960, 9975, 9990, 10005, 10020, 10035, 10050, 10065, 10080, 10095, 10110, 10125, 10140, 10155, 10170, 10185, 10200, 10215, 10230, 10245, 10260, 10275, 10290, 10305, 10320, 10335, 10350, 10365, 10380, 10395, 10410, 10425, 10440, 10455, 10470, 10485, 10500, 10515, 10530, 10545, 10560, 10575, 10590, 10605, 10620, 10635, 10650, 10665, 10680, 10695, 10710, 10725, 10740, 10755, 10770, 10785, 10800, 10815, 10830, 10845, 10860, 10875, 10890, 10905, 10920, 10935, 10950, 10965, 10980, 10995, 11010, 11025, 11040, 11055, 11070, 11085, 11100, 11115, 11130, 11145, 11160, 11175, 11190, 11205, 11220, 11235, 11250, 11265, 11280, 11295, 11310, 11325, 11340, 11355, 11370, 11385, 11400, 11415, 11430, 11445, 11460, 11475, 11490, 11505, 11520, 11535, 11550, 11565, 11580, 11595, 11610, 11625, 11640, 11655, 11670, 11685, 11700, 11715, 11730, 11745, 11760, 11775, 11790, 11805, 11820, 11835, 11850, 11865, 11880, 11895, 11910, 11925, 11940, 11955, 11970, 11985, 12000, 12015, 12030, 12045, 12060, 12075, 12090, 12105, 12120, 12135, 12150, 12165, 12180, 12195, 12210, 12225, 12240, 12255, 12270, 12285, 12300, 12315, 12330, 12345, 12360, 12375, 12390, 12405, 12420, 12435, 12450, 12465, 12480, 12495, 12510, 12525, 12540, 12555, 12570, 12585, 12600, 12615, 12630, 12645, 12660, 12675, 12690, 12705, 12720, 12735, 12750, 12765, 12780, 12795, 12810, 12825, 12840, 12855, 12870, 12885, 12900, 12915, 12930, 12945, 12960, 12975, 12990, 13005, 13020, 13035, 13050, 13065, 13080, 13095, 13110, 13125, 13140, 13155, 13170, 13185, 13200, 13215, 13230, 13245, 13260, 13275, 13290, 13305, 13320, 13335, 13350, 13365, 13380, 13395, 13410, 13425, 13440, 13455, 13470, 13485, 13500, 13515, 13530, 13545, 13560, 13575, 13590, 13605, 13620, 13635, 13650, 13665, 13680, 13695, 13710, 13725, 13740, 13755, 13770, 13785, 13800, 13815, 13830, 13845, 13860, 13875, 13890, 13905, 13920, 13935, 13950, 13965, 13980, 13995, 14010, 14025, 14040, 14055, 14070, 14085, 14100, 14115, 14130, 14145, 14160, 14175, 14190, 14205, 14220, 14235, 14250, 14265, 14280, 14295, 14310, 14325, 14340, 14355, 14370, 14385, 14400, 14415, 14430, 14445, 14460, 14475, 14490, 14505, 14520, 14535, 14550, 14565, 14580, 14595, 14610, 14625, 14640, 14655, 14670, 14685, 14700, 14715, 14730, 14745, 14760, 14775, 14790, 14805, 14820, 14835, 14850, 14865, 14880, 14895, 14910, 14925, 14940, 14955, 14970, 14985, 15000, 15015, 15030, 15045, 15060, 15075, 15090, 15105, 15120, 15135, 15150, 15165, 15180, 15195, 15210, 15225, 15240, 15255, 15270, 15285, 15300, 15315, 15330, 15345, 15360, 15375, 15390, 15405, 15420, 15435, 15450, 15465, 15480, 15495, 15510, 15525, 15540, 15555, 15570, 15585, 15600, 15615, 15630, 15645, 15660, 15675, 15690, 15705, 15720, 15735, 15750, 15765,
```



[...]  
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 intercept 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_ADDP
```

**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 Do
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: 0429.2ec9

2023/08/10 14:35:20.686088796 {wncd\_x\_R0-0}{1}: [client-orch-sm] [15195]: (debug): MAC: 0429.2ec9

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\_90000010]  
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\_90000010[04]

GET rcvd when in LOGIN state

2023/08/10 14:35:24.110718893 {wncd\_x\_R0-0}{1}: [webauth-httpd] [15195]: (info): capwap\_90000010[04]

HTTP GET request

2023/08/10 14:35:24.110754721 {wncd\_x\_R0-0}{1}: [webauth-httpd] [15195]: (info): capwap\_90000010[04]  
2023/08/10 14:35:24.110951163 {wncd\_x\_R0-0}{1}: [webauth-httpd] [15195]: (info): capwap\_90000010[04]  
2023/08/10 14:35:24.110960801 {wncd\_x\_R0-0}{1}: [webauth-state] [15195]: (info): capwap\_90000010[04]

Param-map used: ExternalWebAuth

2023/08/10 14:35:24.110971331 {wncd\_x\_R0-0}{1}: [webauth-state] [15195]: (info): capwap\_90000010[04]  
2023/08/10 14:35:24.111046654 {wncd\_x\_R0-0}{1}: [webauth-page] [15195]: (info): capwap\_90000010[04]

[...]

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\_90000010[04]

POST rcvd when in LOGIN state

2023/08/10 14:35:37.807287911 {wncd\_x\_R0-0}{1}: [webauth-httpd] [15195]: (info): capwap\_90000010[04]  
2023/08/10 14:35:37.807331213 {wncd\_x\_R0-0}{1}: [webauth-httpd] [15195]: (info): capwap\_90000010[04]

[...]

2023/08/10 14:35:37.807498470 {wncd\_x\_R0-0}{1}: [webauth-state] [15195]: (info): capwap\_90000010[04]

Param-map used: ExternalWebAuth

2023/08/10 14:35:37.807503619 {wncd\_x\_R0-0}{1}: [webauth-state] [15195]: (info): capwap\_90000010[04]  
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-Addri
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: 2495.2f72.8a66

**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: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-Identified  
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=0F01A8C0000001EE49"

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=0F01A8C0000001EE49FCD0F&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] [
[...]

[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:capwap\_9000000f]

2023/08/11 12:44:20.312720158 {wncd\_x\_R0-0}{1}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:capwap\_9000000f]

2023/08/11 12:44:20.312740637 {wncd\_x\_R0-0}{1}: [aaa-coa] [15200]: (info): radius coa proxy relationship

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-configuration

2023/08/11 12:44:20.312758912 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [15200]: (info): << formatted-configuration

2023/08/11 12:44:20.312762318 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [15200]: (info): << error-cause code

2023/08/11 12:44:20.312774040 {wncd\_x\_R0-0}{1}: [aaa-coa] [15200]: (info): server:192.168.1.15

2023/08/11 12:44:20.312876905 {wncd\_x\_R0-0}{1}: [caaa-ch] [15200]: (info): [CAAA:COMMAND HANDLER:35000014]

2023/08/11 12:44:20.312886633 {wncd\_x\_R0-0}{1}: [caaa-ch] [15200]: (info): [CAAA:COMMAND HANDLER:35000014]

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:35000014]

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 response

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 [

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-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-Identifi  
2023/08/11 12:44:20.313993459 {smd\_R0-0}{1}: [radius] [17281]: (info): RADIUS: Vendor, Cisco [2  
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-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 [1  
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 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](#)