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

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

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 <u>Web-Based Authentication on Cisco Catalyst 9800 Series</u> <u>Controllers</u>.

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

Wi-Fi networks.

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

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

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



OWE frame exchange

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

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

Cisco Catalyst Wi-Fi 6E APs

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



Wi-Fi 6E Access Points

Configure and Verify

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

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

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

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

Network Diagram

This is the lab setup diagram used in this document.



```
aaa new-model
1
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
I
aaa authentication login LWA_Radius group ISE_RADIUS
T
parameter-map type webauth global
 type webauth
 virtual-ip ipv4 192.0.2.1
trustpoint eWLC-9800-01_WLC_TP
webauth-http-enable
I
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
T
radius server PSN01
 address ipv4 192.168.1.7 auth-port 1812 acct-port 1813
 key 7 xxxxxxxxxxxx
1
wireless profile policy CentralSwPolicyProfile
1
 ipv4 dhcp required
 vlan default
 no shutdown
ļ
wireless tag policy Wifi6E_TestPolicy
wlan wifi6E_test policy CentralSwPolicyProfile
Ţ
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
I
```

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 855 Id	Info	_		Frame 105: 297 bytes on wire (2176 bits), 297 bytes
242.00	385 13 37 58, 134081	9.94499	Entabling seiserer	CLACO_MCVP.38	802.11	297 0010F12d1dd17d136	Association Report, SNe22, Field, Flags		. 113	Ethernet II, Src: Class_Sci45:24 (Mar3d:b4:Sci45:24)
	106 13:37:58.134981	0.00000	IntelCor_98:58:04	Cisco_dd:7d:38	882.11	255 00:df:1d:dd:7d:58	Association Request, SNv22, FNv8, Flagsv, SSIDw"widths_test"		. 113	/ MOLIQ VIPTORI LAN, PMI: 0, DEI: 0, ID: 1
	387 13:37:58,297987	0.0000	CLISCO_AD174(18	IntelCor_98:38:0H	802.11	254.00x0F(38).08/26(38	Association Response, 30-0, Flags		LIE:	> Deternet Protocol Welson 4, SPC: 302.588.1.201, DE
	108 13:37:58.197967	0.00000	Ciaco_dd:7d:38	IntelCor_98:58:04	802.33	254 00:df:1d:dd:7d:98	Association Response, 50-0, FM-0, Flags			2 User Detagram Protocol, SPC Port: 5248, Det Port: 5
	200 13:37:58.299986	8.00222	Detablier_SHISBORF	Broadcast	LLC.	138 001dF12d1dd17d130	U, func-ut; SNAP, OUI exemned (Officially Aeros, but electricite is more comm	ai i	183	Control and Providegoing of advectes Access Polities
	118 33:37:58.222908	0.02299	Ciaco_dd:7d:38	IntelCor_98:58:00	EAPOL	200 00:df:2d:dd:7d:38	Key (Metage 1 of 4)		112	/ LEE 002.11 ANNOLISTIC Request, Fings:
	333 33137158.222988	0.00000	CL600_68179138	IntelCor_98/18:00	EAPOL	283 001dF13d1dd17d138	Key (Message 1 of 4)			7 DIEL MOLIE MUNDERS Paragement
	112 13:37:58.226979	0.00399	IntelCor_98:58:64	Cisco_dd:7d:38	EAPOL	223 00:dV:1d:dd:7d:30	Key (Message 2 of 4)			> Fixed parameters (4 bytes)
	113 13:37:98.226978	0.00000	IntelCor_SHISBIRF	CLND, 40:70:38	EAPOL	228 00x8F13dx8dx7dx30	Key (Nessage 2 of 4)	-		 Tagged parameters (all bytes)
	\$14 13:37:58.226978	0.00000	Cisco_dd:7d:38	IntelCor_98:58:00	EAPOL	277 00:df:1d:dd:7d:18	Key (Message 3 of 4)			> Tag: 5520 parameter set: "v51346_text"
	115 13:37:58.228978	8.00000	CLINES_60174138	IntelCor_98:58:04	EAPOL	277 001dF13d1dd17d138	Key (Ressage 3 of 4)			5 Tag: Supported Rates 6(8), 9, 32(8), 28, 24
	116 13:37:58.229983	0.00300	IntelCor_98:58:84	Eisco_dd:7d:38	EAPOL.	195 00:dV:1d:dd:7d:30	Key (Nessage 4 of 4)			> Tag: Power Capability PLA: 0, Pak: 9
	117 13:37:58.229983	0.00000	DetelCor SHISBIRF	Clinco_dd:7d:3W	EAPS.	393 00107134100176198	Key (Ressage 4 of 4)	1000		 Tagi Kok Information
	118 13:37:58.271973	0.042996	0.0.0.0	255.255.255.255	DHCP	456 00:d7:1d:dd:7d:30	DKP Request - Transaction ID exiat/4747			Tag Number: KNW Difformation (48)
	126 13:37:58.333992	0.062005	112.168.1.254	192.168.1.159	DHCP	392 00:07:10:00:70:38	DHCP ACK - Transaction ID exiat4ff47			hag bength) as
	127 13:37:58.392969	0.058083	7 292.168.1.159	238.0.0.252	2999V2	128 00:d7:1d:dd:7d:30	Membership Report group 224.0.0.252			RVN Version: 1
	\$28 33:37:58.392969	8.00000	192.168.1.159	224.0.0.2	10PPv2	128 00:df:1d:dd:7d:30	Leave Group 224.8.4.252			> short clother subter workerse (been was
	129 13:37:58.302969	0.000000	292.168.1.199	228.0.0.252	2999v2	128 00:df:1d:dd:7d:30	Hestership Report group 224.0.0.252			Paindise Cipher Solte Count: 1
	130 13:37:58.392960	0.00000	8 192.168.1.159	224.0.0.252	LOW	157 00:df:1d:dd:7d:30	Standard query extraits ANY CSCD-W-PY4450KE			> Pairwise Cipher Suite List 000041ac (in
	102 10137158.441000	0.00000	P 993,831,234,2392	102.10111.159	107	202 00:00:14:14:14:14:18	[107 Netranenission] 441 + 50534 [FDS, PGF, ACK] Seq-1 Ack+1 Min+344 Lame77			Anth Ley Steamstor (Art) Suits Fourt-
	183 11:37:58.582964	0.029995	IntelCor_98:58:0f	Broadcast	ANP.	124 00:df:1d:dd:7d:30	who has 192,168,1.2542 Tell 192,168,1.159			 Auth Key Ranagement (ARR) List 00:01140
	242 13137158.587968	0.005005	AlticeLa_Sw:50:af	intelior_98:58:84		138 00:dF:1d:dd:7d:18	192.166.1.254 is at Hicfc2809ec59caf			 Auth key Paragement (ARR) Sugte: 00
	142 13:37:58.517963	0.002224	132.168.1.159	192.388.1.254	015	156 00:df:1d:dd:7d:30	Standard query 9x6517 A spad.clsco.com			Auth Key Receptered (1908) (121)
	145 13:37:58.818956	0.100000	Hershiller Skitslief	Broadcast		124 00:df:18:dd:7d:30	Who has \$92,508.1.2547 Tell \$92,568.1.159	-		Auch key Hanagement (AKH) type:
	152 11:37:58.629963	8.00000	Alticala_Sectoral	Intellor_98:58:99	389	130 00:df:1d:dd:7d:38	152.168.1.254 is at 58:4c:28:9e:59:af			 KNI Opsettitting, entert
	254 23137158.638959	8.018994	1 232.168.1.254	192.168.1.199	015	295 WeidFt3dtddt7dt38	Standard query response 8x5537 No such name & upad.cisco.com 55A rs1.cisco.com	-		
	155 13:37:58.643965	0.00300	5 292.168.1.159	192.168.1.254	015	151 00:df:1d:dd:7d:30	Standard query 8xd/92 A spad.Hose			
	158 13137158.652966	8.011803	1 292.168.1.254	192.368.1.199	016	254 001dF15d1dd17d138	Standard query response exempts no such name A spad. How SOA a root-servers.net			11 = ROM PTROA Rep
	159 13:37:58.721947	0.068983	IntelCor_98:58:6f	Broadcast	489	124 00:df:1d:dd:7d:30	Who has 192.168.1.159? (##P Probe)			THE
	361 13/37/58,722947	0.000000	9 292.148.1.159	224.0.0.252	2999v2	128 001dF1581dd178130	Hentership Report group 224.0.0.252			+ Management Pr
	167 13:37:58.800953	0.073000	132.168.1.159	234.8.8.252	LUNK	157 00:df:1d:dd:7d:30	Standard query exb28c ANY CSCD-W-PY4650KE			uno ono lon ono + Management Pri
	168 13:37:58.906050	0.105093	7 292.168.1.159	192.368.1.254	046	365 00:0F:3d:dd:7d:30	Standard query Robbic A www.msPtconnecttest.com			
	171 13:37:58.917951	0.011000	1 192.168.1.254	192.348.1.159	DNS .	303 00:df:5d:dd:7d:30	Standard query response Buddlic A www.msftconvecttest.com CNIPE ncs1-geo.traffic	-		
	172 13:37:58.921949	9.003030	1 292.268.3.259	194,65,15,176	TCP.	348 00107150100170190	60437 + 88 (SYN) Seg-8 w3n-64348 Len-8 PSS-5258 MS-256 SACK_PERM			c.0 + Extended key
	174 11:37:58.021949	0.000000	1 234.45.25.276	192.348.1.159	TOP	136 00:df:1d:dd:7d:18	88 - 60437 [576, ACK] Sep-0 Ack+1 M2+42720 Len+0 M5-4060 SACK PERH M5+128			PMMID Count: #
	175 13:37:58.923948	8.002200	F 192.168.1.159	194.65.15.176	TOP	136 00:df:1d:dd:7d:30	60437 + 80 (ACK) Seg-1 Ack+1 Win+262400 Len+0			HARD FIN
	177 11:17:58.523948	0.00000	1 192.168.1.159	194.45.15.176	WITE	347 00:dV:1d:dd:7d:10	GET /connectbest.txt HFTP/1.1	_) Group Management Cipher SuSter: 00:0f:ac
	179 13:37:58.523948	0.00000	114.85.15.176	392.368.1.399	DCP.	124 00:07:10:00:70:18	88 = 68437 (ACX) 5eq-1 Ack-112 Win+62728 Len-8			
	280 23127158,922948	0.00000	1 224.45.15.176	192.168.1.159	INTER	606 00:dF:1d:dd:7d:18	HTTP/5.1 1000 OK (text/Rtml)			> Tag: AM Enabled Capabilities (5 octets)
	181 13:37:58.923948	8.00000	114.45.15.176	192.388.1.159	TOP	124 00:df:1d:dd:7d:18	80 - 60437 [Y1N, ACK] Seq-573 Ack-512 Min+62720 Lett-0			> Tag: Extended Capabilities (b# octets)
	182 13:37:58.525946	9.002299	1 192.108.1.159	194.65.15.176	TCP	136 00:df:1d:dd:7d:30	60617 + 80 [ACK] Seq-112 Ack+578 MEn+261888 Lam-0			> Tag: Vendor Specific: Microsoft Corp.: WMV
	184 13:37:58.926908	0.000000	192.168.1.159	194.65.15.178	TOP	136 00:df:1d:dd:7d:90	68437 - 88 (FIN, ACX) Sep-112 Ack+574 Win-261888 Len-8) Tag: Vendor Specific: Intel Wireless Network
	186 13:37:58,926938	0.00000	1 204.45.15.176	192.168.1.199	ICP	124 00:0F:1d:dd:7d:18	80 - 60437 [ACK] Seq-574 Ack+113 MdA+62720 Len+0			> Ext Tag: OME DSP/Se-relian Parameter
	187 13:37:50.000000	0.073063	1 192.168.1.159	152.168.1.254	245	156 00:df:1d:dd:7d:30	Standard query exi55d A upad.clsco.com			5 EVE TAGI HE CADADULITIAN
	198 13:37:99.851992	0.011993	1 192.168.1.254	192.368.1.399	015	295 00:d7:3d:dd:7d:38	Standard query response BH555 No such name & wpad.claco.com SDA msl.claco.com			> Ext Tag: HE 6 GHz Band Capabilities
	191 13:37:50.404998	0.003000	5 192.168.1.159	192.168.1.254	015	151 00:07:10:00:70:30	Standard query Brifflif A upad.tone			> Tag: Vendor Specific: Cisco Systems, Inc: A
	294 13:37:99.808991	0.012000	1 282.268.1.254	192.168.1.199	015	254 00:07:5d:dd:7d:38	Standard query response #eFF1F to such name & spad.Home SOA a,root-servers.net	-		3 Tag: Vendor Specific: Cisco Systems, Inc: &
	195 13:37:99.274979	8.247988	192.168.1.159	192.368.3.254	015	155 00:07:1d:dd:7d:30	Standard query 8x1876 A mus.cisco.com	_		
	198 13:37:50.275071	0.000000	1 192.168.1.254	192.368.1.159	015	159 00:07:1d:dd:7d:18	Standard query response BufE/6 & mus.claco.com & 72.163.1.88	-		
	100 11-17-10 MARCH	a tataat	1 102 TAK T 150	102, 168, 1, 258	1995	142 00-01-14-04-24-00	Chandred many dolbler Vill (VD.), PERMIT class con			

LWA OWE Association

Followed by the DHCP, DNS and HTTP redirection:

No.	Time	Delta	Source	Destination	Protocol	Length BSS 1d	Info		13	Frame 180: 606 bytes on wire (5568 bits), 60
	305 33:37:58.294043	9.94499	Intelcor_selisater	CLACO_60176138	802.13	297 00:27(10)20:38	Association Request, 99-22, Ph-0, Flags+	1	12	Ethernet II, Src: Cisco_Ab:88:49 (00:1e:bd:4
	305 11:37:58.234961	0.000000	IntelCor_98:58:04	Cisco_dd:7d:38	802.11	293 00:df:1d:dd:7d:38	Association Request, SN+22, FN+0, Flags+, SSID+"wdFid6_test"		112	Internet Protocol Version 4, Src: 192.168.1.
	187 13:37:58.297987	0.003000	Cisco_6d:70:38	IntelCor_98:58:6f	892.11	254 00:df:1d:dd:7d:38	Association Response, SN+R, FN+R, Flags+	100	12	User Datagram Protocol, Src Port: 5247, DST
	108 13:37:58.297987	0.00000	Cisco_dd:7d:38	IntelCor_98:58:04	802.11	254 00:df:1d:dd:7d:30	Association Response, SN+0, Flags+		112	control And Provisioning of Mirebess Access
	189 13:37:58.299986	0.002390	intelior_98:58:84	Broadcast	LLC	138 00:d7:1d:dd:7d:30	U, func-cl) SWP, dif monosee (Officially Xerox, but #:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#:	1	112	IEEE 842.31 QoS Data, Flags:F.
	110 11:37:58.222980	0.022594	Cisco_dd:7d:38	IntelCor_98:58:8f	EAPOL	200 00:d/:1d:dd:7d:30	Key (Message 1 of 4)		112	Logical-Link Control
	111 13:37:58.222980	0.000000	Cisco_dd:7d:38	IntelCor_98:58:04	EAPOL	203 00:df:1d:dd:7d:30	Key (Message 1 of 4)	-	12	Internet Protocol Version 4, Src1 194.65.15
	112 13:37:58.226978	0.003394	IntelCor_98:58:0F	CLSC0_68178138	EAPOL	223 00:07:30:00:70:30	Key (Hessage 2 of 4)		12	Transmission Control Protocol, Src Port: 80,
	113 13:37:58.226978	0.000000	IntelCor_98:58:0f	Cisco_dd:7d:38	EAPOL	229 00:df:1d:dd:7d:30	Key (Nessage 2 of 4) OWF Association	-	112	Hypertext Transfer Protocol
	114 13:37:58.226978	0.000000	Cisco_dd:7d:10	IntelCor_98:58:04	EAPOL	277 00:df:3d:dd:7d:30	Key (Hestage 3 of 4)		~	Line-based text data: text/html (9 lines)
	115 13:37:58.226078	0.000000	Cisco_dd:7d:38	IntelCor_98:58:0f	EAPOL	277 00:01:16:66:76:38	Key (Hessage 3 of 4)			ocessioneta name="vseuport" content="uso
	136 13:37:58.229983	0.003005	IntelCor 98:58:6F	Cisco_60:70:38	EAPOL	195 0010F;10100;70100	Key (Hessage 4 of 4)			oranta
	117 11:17:58.229983	8.0000	IntelCor 98:58:04	Ciaco dd:7d:38	EAPOL.	191 00:df:1d:dd:7d:30	Key (Pessage 4 of 4)			ATTRES Web Authentication Redirects/TIT
	118 13:37:58.271973	0.04150	0.0.0.0	255,255,255,255	ONCP	456 00:07:14:44:74:30	DEP Recent - Transaction 10 ex5454647			<pre>rPRTA http-equiv="Cache-control" content</pre>
	126 13:37:58.333982	8,662,69	192.168.1.254	192,168,1,159	DHCP	392 4010113030124138	DKP ACK - Transaction ID examined DHCP Exchange			oPETA http-equiv="Pragsa" content+"no-ci
	127 13:37:58.392969	0.058087	102.108.1110	200-0-0-054	Dane.	1.18 001091101001101.00	NUMBER OF STATE STATE LAL & M. 252			ONETA http-equGu+"Expires" content+"-1"
	128 11:17:58.102960	0.000000	192,168,1,159	224.0.0.2	109912	128 00:07:1d:dd:7d:30	Leave Group 224.8.8.252			<PETA http-equive"refresh" content="1; 4</td>
	129 13:37:58,392909	0.000000	192,168,1,159	224.0.0.252	109912	128 00-of-1d-dd-1d-50	Nembership Report proup 224.8.9.252			C/HEAD/VA
	130 13:37:58.302909	0.000000	192.188.1.198	224.0.0.252	LOW	157 08107134144174198	Standard overy Indole INF (SCO-W-IN4450KE			
	11211111198.402000	0.0000000	100.00172M0190	192-198-11192	102	Manual Contract of Contract of Contract	[ICP Astronomization] 441 + 18514 [FIN, PDF, ACK] Sec-1 Actor administration??			
	133 13:37:58.582964	0.020995	IntelCor 98:58:8V	Broadcast	189	124 00:df:1d:dd:7d:10	Mho has 192.168.1.1547 [e11 192.168.1.159			
	141 13:37:58.587969	0.005205	AlticeLa Sec39:af	IntelCor 98:58:04	489	130 00:df:1d:dd:7d:30	192.358.3.254 is at 58:fc:28:9e:59:af			
	142 13137(58,517963	0.000004	192.168.1.199	192,168,1,254	016	156 00107(14)00174:30	Standard query 86537 A woad, claco, con	_		
	145 13137158.618956	0.100993	IntelCon 98:58:84	Broadcast	189	124-00107124144174130	Who has 192,168,1.2547 5ell 192,168,1.159			
	152 13:37:58.629963	0.001007	Alticels 94:59:sf	IntelCor 98:58:00	189	138 00:01:10:00:76:38	192.198.1.254 is at 58:4c:20:50:af			
	154 13:37:58.438950	0.01899	192.168.1.254	192.168.1.159	.015	195 00:df:1d:dd:7d:38	Standard query response 8x5537 No such name A wood, clisco.com 50A m1, clisco.com			
	155 13137:58.641965	0.00100	192,168,1,199	192,168.1.254	085	151 001dF(1d)dd(2d)30	Standard overy Buffig A used Home			
	158 11:17:58.652966	0.01100	192.168.1.254	292.168.1.199	095	254 00:07:10:0d:7d:30	Standard query response indFig No such name & upad. How SQL a.root-servers.net			
	159 13:37:58,721947	8.06808	IntelCor 98:58:81	Broadcast	100	124 Weidf:1d:dd:7d:30	ieho has 192,168,1,1597 (889 Probe)		Ine	IS Percelution for automatic
	161 13:37:58,721947	0.00000	192.168.1.199	224.0.0.252	209912	128 00:0f:1d:dd:7d:50	Netbership Report group 224.8.8,252			vo Resolution for automatic
	167 13:37:58.88953	0.07000	192.168.1.199	224.0.0.252	LUNK	157 0010F110100174198	Standard overy Indulic MM CSCD-W-IH4650KE	_		
	168 11:17:58.986958	0.10999	192.168.1.199	192.168.1.254	095	165 00:07:1d:dd:7d:30	Standard query middle A way sufficiencecttest, con			
	171 13:37:58.917951	0.011001	192.168.1.254	192,168,1,199	016	303 00:df:1d:dd:7d:30	Standard query response Budilic & www.msftconnecttest.com DWME ncsi-peo.traffi			
-	172 11:37:58.921949	0.001120	107-108-11150	194.45.15.175	162	144 and on the shell do not	MALT & BUILVING Second according Lange ROALING MARTIN SALE FOR			
	174 11:17:58.021949	0.00000	204.45.25.228	192,168,1,199	TOP	136 00107120100170138	HE + ADDIT TSML ACKT Second Acked MiterACTOR Lange MSS-ROAD SACK PERM MS-128	1-		
	175 13137-58 921548	0.001100	197, 168, 1, 199	194.45.15.176	TOP	136 08100110100170130	60417 + 80 (AV) Send Arket Man 30380 Land			
	177 13:37-58.523548	4.00000	192.168.1.199	194.45.15.176	INTE	147 doi:of-14-34-34-30	GRT /connections.tut HTTP/1.1	_		
T	179 10 17 48 92 9948	0.00000	194.45.15.126	192, 168, 1, 199	TOP	134 00105-14144734788	IN a MARY TAXY Send Amount Amount Amount INA Dedire	tion		
-	188 11117-58.027548	6.00000	194, 65, 25, 276	192,168,1,159	HTTP	606 00100 110 A1174 18	HTP/L1 200 (K (test/brd))	- HOIT-		
T	183 13:37:58.921948	P. 000000	194.65.15.178	192,168,1,159	TEP	124 00:07:10:00:14-16	88 + 60617 TFIN, ACK1 Sec-571 Acky112 Min-62729 Lan-8			
	187 11:37:58 225555	0.001100	192.166.1.199	194.85.15.175	TEP	136.001-01-14-44-24-30	59417 + 80 (ACC) Secult2 Adv574 Minu261888 Level			
	184 18187-58.024018	0.00000	192,168,1,159	194.45.15.135	tre	135.0010512434124138	SHAIT & BO (FID. ACK) Security Arks/VIA MissionIRR Land			
	105 13-27-58 030000		And an on the	107 148 1 100	1VP	The second standard by the	IN a SMIT INVI GROUP AND MARKING LAND			

LWA OWE Redirection

On the WLC GUI we can see the client details:

CISCO IIII		- GL 1110000 GUND										arrays barranteen () and a
Q. Sauruh Meny harts	Monitori	ng* > Wreless* > Cile	ents								_ C	lient
Deshboard	Clients	Sleeping Clients	Excluded Cile	ontsi							3	160 View General QOS Statistics
Monitoring		0									1	Client State Servers Olient ACLs
Configuration	Selecti	ed 0 out of 3 Clients										Client Entry Croote Time
Ch annual in	0	Client MAC Address	T IPv	4 Address	T 1	Pv6 Address	AP Name	▼ SSD	T WU	N ID	т	Policy Type
{O} Administration >	0	0429.2ec9.e371	× 193	2.168.1.160	- 1	w80: 6a20 54e8 a010 6332	AP9136_5C.F524	witter, text	5			Encryption Cipher
C Licensing	0	2495.2772.8x66	A 10	2.168.1.162	1	w90:.ls13.f107:7c5f.w7w0	AP9136_5C.F524	white, test	.6			EAP Type

```
aaa new-model
I.
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
I
aaa authentication login EWA_Radius group ISE_RADIUS
T
parameter-map type webauth global
 type webauth
virtual-ip ipv4 192.0.2.1
trustpoint eWLC-9800-01_WLC_TP
webauth-http-enable
I.
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
I
radius server PSN01
 address ipv4 192.168.1.7 auth-port 1812 acct-port 1813
 key 7 xxxxxxxxxxx
ļ
wireless profile policy CentralSwPolicyProfile
1
ipv4 dhcp required
 vlan default
no shutdown
ļ
wireless tag policy Wifi6E_TestPolicy
wlan wifi6E_EWA policy CentralSwPolicyProfile
L
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
!
```

_									_	
1	io. Time	Delta	Source	Destination	Protocol	Length	BSS 1d	Info	Т	> Frame 401: 404 bytes or
	398 89:51:24.537423	0.020585	C1sco_dd17d138	Broadcast	882.11	354	0010F15d1dd17d138	Beacon frame, SN-3093, FN-0, FlagsC, 82-300, SSID-"xdF16E_D4A"		> Televier and protocol lines
	391 09:51:24.557748	0.020325	Cisco_dd:7d:38	Broadcast	882.11	311	00:df:1d:dd:7d:38	Probe Response, SN-3094, FN-0, FlagsC, 81+380, SSID="widf166_EMA") lines futures Bostocol
	392 @9151124.578356	0.020608	CLNC0_M17d138	Broadcast	882.11	311	001dF13d1dd17d138	Probe Response, SN-3005, FN-0, FlagsC, 82-300, SS2D="wif156_DM"		> User Datagran Protocos,
	393 @9:51:24.588572	0.038235	Samungl_c9:e3:71	Cisco_dd:7d:38	882.11	238	00:df:1d:dd:7d:38	Probe Request, SN+2351, FN+0, Flags+C, SSID+"hdfi6E_DW"	ан.	> All order, um preek encag
	394 09:51:24.588572	0.000000	192.168.1.15	192.168.1.121	882.11	26		Acknowledgement, Flags+C		> BULII Fallo Informatio
	395 @9:51:24.589544	0.000972	Cisco_dd:7d:38	Sansungt_c9:e3:71	882.11	311	00:df:1d:dd:7d:38	Probe Response, 5N-7, FN-0, FlagsC, 82-300, 5520-"xdf16E_DM"		> DEEL BA2.11 AMOCLATION
	396 09:51:24.589544	0.000000	192.168.1.15	192.168.1.121	882.11	26		Acknowledgement, Flags+C		 DELE MOZ.11 MEPHDESS PG
	397 @9:51:24.589696	0.000152	Sansungl_c9:e3:71	Cisco_dd:7d:38	882.11	96	00:df:1d:dd:7d:38	Authentication, SN+2352, FN+0, FlagsC		> Fixed parameters (4
	398 09:51:24.589696	0.000000	192.168.1.15	192.168.1.121	882.11	26		Acknowledgement, Flags+C		 Tagged parameters (
	399 @9:51:24.593486	0.003790	Cisco_dd:7d:38	Sansungt_c9:e3:71	882.11	96	00:df:1d:dd:7d:38	Authentication, SNel3, FNe0, FlagsC		> Tag: SOLD paran
	400 09:51:24.593486	0.000000	192.168.1.15	192.168.1.121	882.11	26		Acknowledgement, Flags+C		> Tag: Supported
	401 09:51:24.596809	0.002503	Sansungt_c9:e3:71	Cisco_dd:7d:38	882.11	404	00:df:1d:dd:7d:38	Association Request, SN+2353, FN+0, Flags+C, SSED+"wif166_ENA"		> Tag: Power Capa
	482 09:51:24.596889	0.000000	192.168.1.15	192.168.1.121	882.11	26		Acknowledgement, Flags+C		> Tag: Supported
	403 09:51:24.598683	0.002554	Cisco_dd:7d:38	Broadcast	882.11	331	00:df:1d:dd:7d:38	Probe Response, 5N:3007, FN:0, FlagsC, 82:300, 5523="wdf16E_DMR"		 Tag: ROA Inform
	404 09:51:24,604656	0.005973	Sansungl_c91e3171	Broadcast	LLC	114	0010F15d1d017d138	S, func-RNR, N(R)=67; DSAP Bud8 Group, SSAP Bul4 Response		Tag Number:
	405 09:51:24.607923	0.003267	Cisco_dd:7d:38	Sansungt_c9:e3:71	882.11	275	00:df:1d:dd:7d:38	Association Response, SN+0, Flags+C		Tag Length:
	406 09:51:24,607923	0.000000	192.168.1.15	192.168.1.121	882.11	26		Acknowledgement, Flags+C		KON VErsion
	412 09:51:24.611324	0.003485	Cisco_dd:7d:38	Sansungt_c9:e3:71	EAPOL	225	00:df:1d:dd:7d:38	Key (Message 1 of 4)		> Group Ciphe
	413 09:51:24,611324	0.000000	192.168.1.15	192.168.1.121	882.11	76		Acknowledgement, Flags+C		Patridse Ci
	414 09:51:24.619609	0.008285	Cisco_dd:7d:38	Broadcast	882.11	331	00:df:1d:dd:7d:38	Probe Response, 5N=3008, FN=0, Flags+C, 82+380, 5523+"wdf16E_DMR"		> Pathdae C
	415 09:51:24.629175	0.000566	Sansungl_c91e3171	Cisco_dd:7d:38	EAPOL	243	0010F15d1d017d138	Key (Message 2 of 4)		Auth key Pa
	416 09:51:24.629175	0.000000	192.168.1.15	192.168.1.121	882.11	76		Acknowledgement, Flags+C		 Auth key Pa
	417 09:51:24,630862	0.005587	Cisco_dd:7d:38	Sansungl_c9:e3:71	EAPOL	295	0010F15d1d017d138	Key (Message 3 of 4)		V Auth ta
	418 09:51:24.630862	0.000000	192.168.1.15	192.168.1.121	882.11	26		Acknowledgement, Flags+C		Aut
	419 09:51:24,635603	0.004741	Sansungl_c9:e3:71	Cisco_dd:7d:38	EAPOL	199	0010F15d1d017d138	Key (Message 4 of 4)		Aut
	428 09:51:24.635683	0.000000	192.168.1.15	192.168.1.121	882.11	26		Acknowledgement, Flags+C		> RSN Capabil
	421 09:51:24.639768	0.004165	CLoco_dd:7d:38	Broadcast	882.11	354	00:0F15d:0d:7d:38	Beacon frame, SN-3899, FN-0, Flags+C, 81-580, SSID-"x6FL6E_D4A"		PMKID Count
	422 09:51:24.649941	0.020173	Cisco Sc: #5:24	Sansungt_c9:e3:71	LLC	183	00:df:1d:dd:7d:38	5, func-8R, N(R)+1; DSAP 0x56 Group, SSAP 0xb2 Response		> PMKID List
	412 00-01-14 600001		103 169 1 16	103 168 5 135	893.51	14		Mandatasan Dar. F		> Group Manag

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:

	EWA_P	CAP.pcap									
E	le Edit	View Go	Capture A	inalyze Statistics	Telephony Wireless To	ols Help					
	1		2 0 9	****	1 🗐 🗐 @ @ @ !						
	tcp.port	==80 or bootp	or dris or radius	1							
No		Time	Delta	Source	Destination	Protocol	Leooth RSS 14	Info		Т	> Frame 1171: 960 bytes on wire (7680 bi
	985	09152126.72294	7 0.00	0.0.0.0	255.255.255.255	DHOP	430 00:07:38:08:78:30	DKP Request - Transaction 2D Bolos563c8		111	> Ethernet II, Src: Cisco_6b:80:FF (00:1
	985	09:52:26.72295	4 0.000	0.0.0.0	255.255.255.255	DHCP	348	DICP Request - Transaction ID Informatical DILCD Exchange		11) Internet Protocol Version 4, Src: 192.
	989	09:52:26.74095	8 0.0240	04 292.568.1.254	292.268.1.260	DHCP	326	DKP ACK - Transaction 10 Beloef63c8			> User catagram Protocol, Src Port: 5347
	990	09:52:26.74895	s 0.000	09 192.168.1.254	292.168.1.160	DHCP	392 00:df:1d:dd:7d:38	DKP ACK) Control And Provisioning of Wireless A
	2052	09:52:26.84494	2 0.50	64 292.558.1.200	202.208.2.298	640	258 00109120100170130	SERVERA GORY MOLLY & MILLE. BOGLE. CON			> itte soluti qui tota, riage
	1853	09:52:26.84494	2 0.000	00 192.168.1.160	192.168.1.254	ONS:	76	Standard query 0x512f A stalk.google.com			 Logicki-Link Controls Teternet Destaced Mercine A. Serie 143.
	2054	09:52:26.84594	9 0.00 I	07 292.268.1.254	292.568.1.560	ONG.	96	Standard query response 0x512F A stalk.google.com A 142.250.110.188			Transmission Control Protocol, for Bar
	1855	09:52:26.84594	9 0.00	00 192.168.1.254	192.168.1.160	ONS-	162 00:df:1d:dd:7d:38	Standard query response 0x512# A stalk_google.com A 142.250.110.188			historia Transfer Pottorol
	2874	09:52:26.85794	2 0.05 5	03 292.268.1.260	292.568.1.254	ONS.	171 00:df:1d:dd:7d:30	Standard query BulbaD A connectivitycheck.gstatic.com			Y Line-based text data: text/html /0 line
	1875	09:52:26.85794	2 0.000	00 192.168.1.160	292.168.1.254	ON/S	89	Standard query 0x2ba9 A connectivitycheck.gstatic.com	-		diffuscrets name "viewport" conten
	2876	09152126.85894	9 0.001	07 192.168.1.254	192.168.1.160	ONG-	260	Standard query response 0x2ba9 A connectivitycheck.gstatic.com A 142.250.178.163			(HEAD) A
	1877	09:52:26.85894	9 0.000	00 192.168.1.254	192.168.1.160	DNS	175 00:df:1d:dd:7d:38	Standard query response 0x2ba9 A connectivitycheck.gstatic.com A 142.250.178.163			(TITLE) Web Authentication Redirect
	2894	09152126-86295	4 0.0030	45 192.568.1.560	292.568.1.254	046	256 00109120100170130	Standard query exercit A way, googse.com DNS Resolution for auto redi	ectic	m	WETA http-equiv="Cache-control" of
	1895	09:52:26.86295	4 0.0000	00 192.168.1.160	192.168.1.254	ONS	74	Standard query exercit A www.google.com	1		OFEIA http-equive"Pragma" content+
	1200	09152126.86294	6 0.0000	02 192.168.1.254	292.268.2.260	ONS-	94	Standard query response 0x8Fd7 A www.google.com A 142.250.184.4			WETA http-equiv="Expires" content
	1301	09152126-86294	5 0.0000	80 192.158.1.254	192.068.1.060	UND	150 00:07:10:00:70:38	Standard query response exerci A MAV.google.com A 142.250.184.4			[truncated]/PETA http-equive"refin
	1208	09152126-86494	5 0.001	09 192.268.1.260	192.168.1.254	CND-	361 00107130100170130	Standard query excl34 A time.cloudflare.com			\n
	1389	09:52:25.85494	5 0.000	NO 192.258.1.250	192.108.1.256	UND OT		Standard query exclusion destilit a plan electronic con a sub and and a sub and and and			
	1122	00152126-87794	5 0.4134	00 232.258.1.254	292.258.1.250	UND-	113	Standard query response excline A time.cloueriare.com A 162.159.200.1 A 162.159.200.11			
	1123	09152126-87796 00152126-87796	5 0.000	NO 192.208.1.254	192.208.1.200	UND I	181 00:00110:000700.08	Standard guery response excluses the cloudy large con a 162,159,200,1 a 162,159,200,12			
Г	1116	00-51-26.06304	e e.eess	142.250.178.161	542-250-278-283 552-568-3-568	TOP	144 00-01-14-04-74-18	BA + 1928 FOR ANY Send Adult Mandilla Land Michield City 2008 Tout-10020508	3-		
	1167	00-51-16 0640A	6 0.000	103 102 1 100	141 250 178 163	100	100 00100110100170100	1010 - 80 [AV] faul Arest blacklik Land Tuni-Tistikh Terra-Mittistikh			
	1168	00-53-36 06404	6 0.000	102.000.1.000	143, 250, 178, 163	HTTP	125 00-01-14-04-24-30	GET / managements 2014 METRYS 1			
T	1160	00152126-06404	6 0.0000	142,258,178,161	192, 568, 1, 569	TCP	116 08-0110-08-76-78	88 - 1000 (AVI) Gen-1 Ark-228 Mon-6404 Lan-8 Think-100265623 There-22682443			
	1171	09-53-26 96494	6 0.0000	142,250,178,163	292, 568, 3, 560	HTTP	260 08-01-14-05-76-18	HTTP/1.1 200 (X (text/html))			EWA Redirection for
	1181	09152126-96793	7 0.0025	312.568.1.560	142,250,178,163	TCP	148 0010F116106176130	13978 + 88 [ACK] Sep-228 Ark-825 Min+67584 Len+8 TSval+72587445 TSerr+3892853623	-		automal login nortal
	1182	09:52:26.96793	7 0,0000	192.558.1.350	142.250.178.163	TCP	148 00:01:14:45:75:30	33970 + 80 [FDN, ACK1 Sec+228 Ack+825 Win+67584 Len+0 T5va1+72587446 T5ecr+3692853623			external login portal
	1183	09:52:26.96793	7 0.0000	142.250.178.163	292.568.1.560	TCP	136 08107134144174138	88 + 33978 [FIN, ACK] Seo-825 Ark+329 MIN+65804 Len+8 TSv82+3692853626 TSerr+72587666			
L	1214	09:52:26.97893	0.0110	97 192.568.1.560	142.250.178.163	TCP	148 00:df:1d:dd:7d:30	33978 + 88 [ACK] Sec+229 Ack+826 Min+67584 Len+8 TSval+72587458 TSecr+3692853626			

Packet capture detail on EWA

At this stage the client is in Web Auth Pending:



EWA client in Web Auth Pending



```
aaa new-model
!
aaa group server radius ISE_RADIUS
 server name PSN01
 deadtime 5
 load-balance method least-outstanding
 subscriber mac-filtering security-mode mac
mac-delimiter colon
Т
aaa authorization network RadiusAuthor group ISE_RADIUS local
1
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
trustpoint eWLC-9800-01_WLC_TP
webauth-http-enable
I.
radius server PSN01
 address ipv4 192.168.1.7 auth-port 1812 acct-port 1813
 key 7 xxxxxxxxxxx
1
wireless profile policy CentralSwPolicyProfile
1
 ipv4 dhcp required
 vlan default
no shutdown
I
wireless tag policy Wifi6E_TestPolicy
wlan wifi6E_CWA policy CentralSwPolicyProfile
1
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	> Frame 2508: 308 bytes on wire (2464 b)
	2491 11:07:53.752705	0.502441 Cisco_dd:7d:39	Broadcast	802.11	354 00:dF:1d:dd:7d:39	Beacon Frane, SN-320, FN-0, Flags+C, 81+100, 5535+"xdF16E_OM"	> Ethernet II, Src: Cisco_d2:97:47 (74:1)
	2499 11:07:53.850051	0.007646 Google_72:8a:66	Broadcast	882.11	283 ff:ff:ff:ff:ff:ff:ff	Probe Request, SN+3540, FN+0, Flags+C, SSID+"xd-Fist_OA"	> Internet Protocol Version 4, Src: 192.3
	2500 11:07:53.852591	0.001240 Cisco_dd:7d:39	Broadcast	802.11	331 00:dF:1d:dd:7d:39	Probe Response, Stirl, Flieb, Flags+C, 81-100, SS3D-"sd-Fibl_OA"	> User Datagram Protocol, Src Port: 5555,
	2501 11:07:53.855067	0.003476 Cisco_dd:7d:39	Broadcast	882.11	354 00:df:1d:dd:7d:39	Beacon frame, SW-321, FN-0, Flags+C, 81+100, SSID+"v6F16E_OA"	> Alroneek/Ompreek encapsulated little BK
	2582 11:07:53.915746	0.060679 192.168.1.15	192.368.1.121	802.11	26	Clear-to-serd, Flags+C	> BM2.11 radio information
	2584 11:07:53.944786	0.020960 Google_72:8a:66	Cisco_dd:7d:39	882.11	108 00:df:1d:dd:7d:39	Authentication, SN+3541, FN+0, Flags+C	> ILLE BRO.11 Association Request, Flags
	2505 11:07:53.944706	0.000000 192.168.1.15	192.368.1.121	802.11	26	Acknowledgement, Flags+C	 IEEE B02.11 kireless Panagement
	2586 11:07:53.948449	0.003743 Cisco_dd:7d:39	Google_72:8a:66	882.11	108 00:df:1d:dd:7d:39	Authentication, SN+3, FN+0, Flags+C	> Fixed parameters (4 bytes)
	2587 11:07:53.948449	0.000000 192.168.1.15	192.368.1.121	802.11	26	Acknowledgement, Flags+C	✓ Tagged parameters (254 bytes)
10	2568 11:07:53.949451	0.001002 Google_72:8a:66	Cisco_dd:7d:39	892.11	308 00:df:1d:dd:7d:39	Association Request, SNv3542, FNv0, FlagsC, SSIDv"wifikE_OA"	> Tag: SSED parameter set: "WEFE
	2509 11:07:53.949451	0.000000 192.168.1.15	192.368.1.121	802.11	26	Acknowledgement, Flags+C	> tag: supported Rates e(0), 9, 1
	2512 11:07:53.957664	0.000213 Cisco_dd:7d:39	Broadcast	882.11	354 00:df:1d:dd:7d:39	Beacon frame, SN-323, FN-0, Flags+C, 81+100, SSID+"vd-fi6E_OA"	> Tag: Power Capability Min: -7,
	2513 11:07:53.972307	0.054643 Google_72:8a:66	Broadcast	LLC	334 00:dF:3d:dd:7d:39	I P, N(R)+24, N(S)+67; DSAP 0x46 Individual, SSAP NetBIOS Command	 > tag: supported channels
	2514 11:07:53.976328	0.004821 Cisco_dd:7d:39	Google_72:8a:66	882.11	275 00:df:1d:dd:7d:39	Association Response, SN+0, Flags+C	 Tag: KON information
	2515 11:07:53.976328	0.000000 192.168.1.15	192.368.1.121	802.11	76	Acknowledgement, Flags+C	Tag hunder: Kon Linomation
	2516 11:07:53.977705	0.001377 Cisco_dd:7d:39	Google_72:8a:66	EAPOL	221 00:df:1d:dd:7d:39	Key (Message 1 of 4)	Tag Length: 42
	2517 11:07:53.977705	0.000000 192.168.1.15	192.368.1.121	882.11	76	Acknowledgement, Flags+C	Kon version: a
	2518 11:07:54.018038	0.060333 Google_72:8a:66	Cisco_dd:7d:39	EAPOL	243 00:df:1d:dd:7d:39	Key (Message 2 of 4)	> Group Cipher Suite: eecers
	2519 11:07:54.018038	0.000000 192.168.1.15	192.368.1.121	882.11	76	Acknowledgement, Flags+C	Pagnage capter sugge count
	2521 11:07:54.019950	0.001912 Cisco_dd:7d:39	Google_72:8a:66	EAPOL	295 00:df:1d:dd:7d:39	Key (Message 3 of 4)	> Michiele Capiter State List
	2522 11:07:54.029950	0.000000 192.168.1.15	192.168.1.121	882.11	26	Acknowledgement, FlagsC	Auch key Ranagement (AKR)
	2523 11:07:54.027081	0.007131 Google_72:8a:66	Cisco_dd:7d:39	EAPOL	199 00:df:1d:dd:7d:39	Key (Ressage 4 of 4)	 Auto key rangement, (Akri) (
	2524 11:07:54.027081	0.000000 192.168.1.15	192.168.1.121	882.11	76	Acknowledgement, FlagsC	 Autor Key Hanagement, Las
	2525 11:07:54.053908	0.026827 Google_72:8a:66	Cisco_dd:7d:39	802.11	121 00:df:1d:dd:7d:39	Unknown Unprotected WMM Action(Malformed Packet: length of contained item exceeds lengt	Auth Key Paragener
	2526 11:07:54.053908	0.000000 192.168.1.15	192.168.1.121	882.11	76	Acknowledgement, FlagsC	Auto May Panagement
	2527 11:07:54.060080	0.006172 Cisco_dd:7d:39	Broadcast	802.11	354 00:dF:1d:dd:7d:39	Beacon frame, SNo324, FNo0, Flags+C, 81×100, SS1Dv"xdF16E_OM"	 Kow Capaciticies: execce
	2529 11:07:54.071158	0.011878 192.168.1.15	192.168.1.121	882.11	76	Acknowledgement, FlagsC	
	2530 11:07:54.000085	0.008927 192.168.1.15	192.368.1.121	802.11	26	Acknowledgement, FlagsC	
	2531 11:07:54.087535	0.007450 192.168.1.15	192.168.1.121	882.11	76	Acknowledgement, FlagsC	
	2532 11:07:54.092209	0.004674 Cisco_5c:F5:24	Google_72:8a:66	LLC	183 00:dF:1d:dd:7d:39	I, N(R)+34, N(S)+388; DSAP that Individual, SSAP these Command	
	2533 11:07:54.092209	0.000000 192.168.1.15	192.168.1.121	882.11	76	Acknowledgement, Flags+C	
	2534 11:07:54.092209	0.000000 Cisco_5c:F5:24	Google_72:8a:66	LLC	183 00:dF:1d:dd:7d:39	I, N(R)+07, N(S)+22; DSAP 0x60 Individual, SSAP 0x5c Command	
	2535 11:07:54.092209	0.000000 152.168.1.15	192.168.1.121	882.11	76	Acknowledgement, Flags+C	
	2536 11:07:54.094370	0.002161 Cisco_dd:7d:39	Google_72:8a:66	802.11	118 00:dF:1d:dd:7d:39	Action, SNe1, FNe0, Flags+.pC[Halformed Facket]	
	2537 11:07:54.094370	0.000000 192.168.1.15	192.168.1.121	882.11	76	Acknowledgement, FlagsC	PMID Count: 1
	2538 11:07:54.094829	0.000459 Google_72:8a:66	Cisco_dd:7d:39	802.11	115 00:df:1d:dd:7d:39	Action, SN+3547, FN+0, Flags+.pC	> PERID List
	2539 11:07:54.094829	0.000000 152.168.1.15	192.168.1.121	882.11	76	Acknowledgement, FlagsC) Group Hanaparent (Loher Su
	3543 11-07-54 16335a	8 867671 / Loop de 16-36	Boostrat	800.11	ISA BROAD BROAD BROAD BROAD	Barrow Frank Shuffle Diale Flams / Blutte CON-School Flam	1 A many conditions of the second se second second sec

CWA OWE OTA connection

Then we have the Radius Exchange for the mac filtering:

Image: No. Time Delta Source Destination Protocol Length IDS 1d Info Image: ABDE 1435, Marces Image: ABDE 1435, Marces	∡ ≡ ∠ ⊗ > ⊖	🗙 🖸 I ۹ 🗢 🗢 🕾 🖗	4 🗐 🗐 Q Q (B. 11			
	Image: Control of the state of the	Col Col <th>Cestnation 100.188.1.7 100.188.1.7 100.188.1.7 100.188.1.7 100.188.1.7 100.188.1.7 100.188.1.7 100.188.1.7 100.188.1.7 100.188.1.1</th> <th>Protocol L Anatolis Matolis Matolis Matolis Matolis Matolis Matolis Matolis Matolis</th> <th>ength BSS 1d 436 584 436 585 585 585 133 137 277</th> <th>Info Access-Meguest 16-18 Access-Meguest 16-18 Access-Meguest 16-19 CoM-Meguest 16-19 Access-Meguest 16-19 Access-Meguest 16-20 CoM-ACK 16-4 Access-Accept 16-20</th> <th><pre>> Frame 4800: 486 bytes on wire (MARE bits), 43 > (thermer II, Src: Cisco_do:Mit:ff (Writerbid) > Difference Probool Version 4, Src: 102.106.11 > User Durgrams Protocol (Src: Port: 6502.00.11 > User Durgrams Protocol (Src: Port: 6502.00.11 > Disco Sectors)</pre></th>	Cestnation 100.188.1.7 100.188.1.7 100.188.1.7 100.188.1.7 100.188.1.7 100.188.1.7 100.188.1.7 100.188.1.7 100.188.1.7 100.188.1.1	Protocol L Anatolis Matolis Matolis Matolis Matolis Matolis Matolis Matolis Matolis	ength BSS 1d 436 584 436 585 585 585 133 137 277	Info Access-Meguest 16-18 Access-Meguest 16-18 Access-Meguest 16-19 CoM-Meguest 16-19 Access-Meguest 16-19 Access-Meguest 16-20 CoM-ACK 16-4 Access-Accept 16-20	<pre>> Frame 4800: 486 bytes on wire (MARE bits), 43 > (thermer II, Src: Cisco_do:Mit:ff (Writerbid) > Difference Probool Version 4, Src: 102.106.11 > User Durgrams Protocol (Src: Port: 6502.00.11 > User Durgrams Protocol (Src: Port: 6502.00.11 > Disco Sectors)</pre>

OEW CWA Mac filtering

Followed by the DHCP, DNS and HTTP redirection:

	CWA_PCAP.pcap							
Fi	ile Edit View Go	Capture Analyze Statistics	s Telephony Wireless Te	ools Help				
1		2 D 9 + + S 3		11				
Ē	bootp or drs or top.port -	-80	1 1 1 1 4 4 4 4	246				
Nio	. Time	Delta Source	Destination	Protocol	Lenoth BSS Id	Info		> Frame 608: 994 bytes on wire (7952 bits), 994
	422 12:43:26.243975	3.1569.5 0.0.0.0	255.255.255.255	0.02	424 00:07:10:00:70:30	DICP Discover - Transaction ID 0x0006a041		> Ethernet II, Src: Cisco_4b:80:ff (80:1e:bd:4b:
	423 12143126.344982	0.00247 0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x0826a441		> Internet Protocol Version 4, Src: 192.168.1.15
	424 12:43:26.257982	0.013 00 192.168.1.254	192.168.1.201	DHCP	326	DKP Offer - Transaction ID 0x9826a441 DLLCD Fund-serves		> User Datagram Protocol, Src Port: 5247, Ost Po
	425 12:43:26.257982	0.000 00 192.168.1.254	192.168.1.201	DHCP	392 00:07:34:44:74:39	DKP Offer - Transaction ID ex0826441 DHCP Exchange		> Control And Provisioning of Wireless Access Po
	444 12:43:26.270982	0.01300 0.0.0.0	255.255.255.255	DHCP	434 00:07:3d:dd:7d:30	DHCP Request - Transaction ID 0x04D5a641		> IEEE MALTI QOS DACA, Flags:F.
	445 12:43:26.270982	0.000 00 0.0.0.0	255.255.255.255	DHCP	352	DKP Request - Transaction ID 0x0826a441		> Logical-Link control
	446 12:43:26.275971	0.000 09 192.168.1.254	192.168.1.201	DHCP	326	DKP ACK - Transaction 1D 0x09036441		> Internet Protocol Version 4, Src: 542.298.384.
	447 12:43:26.275971	0.000000 192.168.1.254	192.168.1.201	DHCP	392 00:df:1d:dd:7d:39	DKP ACK - Transaction ID 0x0826a441) Inwakission compassioners, she porti an, o
	513 12:43:26.360973	0.000002 192.168.1.201	292.268.2.254	015	171 00:df:1d:dd:7d:30	Standard query 0xd199 A connectivitycheck.gstatic.com		> Hypercent frantier Protocol
	514 12:43:26.368973	0.400000 192.168.1.201	192.168.1.254	ONS-	89	Standard query 0xd199 A connectivitycheck.gstatic.com		 Line-based text back text/rets (2 lines) diffe unsta same "disport" contents "diffe
	517 12:43:26.362972	0.022999 192.168.1.254	292.168.1.201	DNS.	209	Standard query response 0xd199 A connectivitycheck.gstatic.com A 142.150.184.)		SERVICE THE PARTY PARTY CONCERCY RADO
	518 12:43:26.362972	0.00000 192.168.1.254	192.168.1.201	DNS-	175 00:df:1d:dd:7d:39	Standard query response 0xd199 A connectivitycheck.gstatic.com A 142.250.184.3		(TTDE) ish Athentication Ballmarts/TTDE
	521 12:43:26.362972	0.000000 172-100-1-200	505 KER 8 564	1945	102.00.02.10.00.00.00	Exected youry defield A case graphs are		OFTE MED ADDARTACHERS MADE ADDARTS
	522 12:43:26.362972	0.000000 192.168.1.201	192.168.1.254	DNS	74	Standard query ex1984 A www.google.com DNS Resolution for auto	Redi	rection with http-spine "kname" contents" on carb
	527 12:43:26.364971	0.002999 192.168.1.254	292.268.3.203	DND.	94	Standard query response 0x2984 A www.google.com A 142.250.184.4	-	OFTA MTO-environ"(unices" contents",1")/o
	528 12:43:26.364971	0.000000 192.168.1.254	192.168.1.201	DNS	160 00:df:1d:dd:7d:39	Standard query response 0x1984 A www.google.com A 142.250.184.4		[truncatef]d#14 http-equipy"refresh" con
	541 12:43:26.308966	0.033995 192.168.1.201	192.168.1.254	DND-	158 00:df:1d:dd:7d:30	Standard query 0xF233 A stalk.google.com		(/##2)/4
	542 12:43:26.398966	0.000000 192.168.1.201	192.168.1.254	ONIS	76	Standard query 0xf233 A mtalk.google.com		(ATRA)
	564 12:43:26.410974	0.012008 192.168.1.254	292.168.1.201	DND-	135	Standard query response 0x9233 A stalk.google.com CMPHE mobile-gtalk.l.google.	4	
	565 12:43:26.410974	0.000000 192.168.1.254	192.168.1.201	ONS	201 00:df:1d:dd:7d:39	Standard query response 0xf233 A stalk.google.com OWPE mobile-gtalk.l.google.	4	
Г	587 12143126.422967	0.01103 192.168.1.201	342.250.384.3	TOP	256 00107120100170130	47718 + 80 [5/N] Seg-0 MLN-65535 Len-0 MSS-1250 SACK_PERM 15va1+1206276393 TSe		
	588 12:43:26.422967	0.000000 142.250.184.3	192.168.1.201	TCP	144 00:df:1d:dd:7d:39	80 + 47718 [SVN, ACK] Seq+0 Ack+1 Hin+65160 Len+0 MSS+1460 SACK_PERM TSva1+263	12	
	603 12143126.426064	0.00.007 192.168.1.201	342.250.384.3	TOP	248 00107120100170130	47718 = 80 [ACK] Seg-1 ADO-1 M20-65536 Lenve TSV42+1106176397 TSeC*-2631133863		
+	604 12:43:25.420964	0.000000 192.168.1.201	142.250.184.3	HTTP	375 00:01:10:00:70:30	GET /generate_204 HTTP/1.1		
	647 12143126.426964	0.000000 142.250.184.3	192.168.1.201	TOP	196 00107110100170139	80 = 47718 [ACK] Seq=1 ADX=228 Min=65024 Len=0 TSva1=2631131867 TSecr=12061763	° 0	adiraction to ISE portal
-	008 12:43:25.426964	0.000000 142.250.154.3	197.108.1.201	HI IP	794 00:07:10:00:70:39	HTTP/1.1 200 CK (THRT/HER1)		eunection to ise portai
	609 12(43)26,427971	0.002007 142.250.184.3	292.168.1.201	10	196 0010F110104174199	80 = 47718 [F2N, ACK] Seq-859 ACX-228 MSN-65824 Lenve TSV81-2631131867 TSeCF-1		
	640 12:43:25.432976	0.000005 192.168.1.201	142.250.164.3	TOP	148 00:07:16:06:76:30	47718 + 80 [ALK] 5404228 ACK-859 925-67328 Len-0 T5921-1106276403 T56079263113		
	641 12/43/26,432976	0.00000 102.168.1.201	942.250.184.3	100	246 0010F130100170190	47718 * 80 [F194, ALA] Sequitas Accesse Minet/S28 Level Tyval-1386176485 TSecret)	
Au.	042 12:43:26.432976	0.000 Str. 20 10.1	TV-104-1-38		10.00.00.00.00.00	The strict list is seen active scherolist land realizabilities in section.		

CWA DHCP DNS and Redirection

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

Association success

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

Client state transition: S_CO_ASSOCIATING -> S_CO_L2_AUTH_IN_PROGRESS

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

Authentication Success

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

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

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

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

Wireless session sequence, create context with method WebAuth

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

S_AUTHIF_PSK_AUTH_KEY_XCHNG_PENDING -> S_AUTHIF_L2_WEBAUTH_PENDING

2023/08/08 13:37:58.230912145 {wncd_x_R0-0}{1}: [auth-mgr] [15154]: (info): [286b.3598.580f:capw 2023/08/08 13:37:58.230915511 {wncd_x_R0-0}{1}: [auth-mgr] [15154]: (info): [286b.3598.580f:capw 2023/08/08 13:37:58.230971648 {wncd_x_R0-0}{1}: [auth-mgr] [15154]: (info): [286b.3598.580f:capw 2023/08/08 13:37:58.230998298 {wncd_x_R0-0}{1}: [auth-mgr] [15154]: (info): [286b.3598.580f:capw 2023/08/08 13:37:58.231001354 {wncd_x_R0-0}{1}: [auth-mgr] [15154]: (info): [286b.3598.580f:capw 2023/08/08 13:37:58.231001354 {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_900000k

Param-map used: LocalWebAuth

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

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

, priority: 50, IIF-ID: 0

[...]
2023/08/08 13:37:58.239843453 {wncd_x_R0-0}{1}: [client-iplearn] [15154]: (info): MAC: 286b.3598.580f IF
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 IF
2023/08/08 13:37:58.240437257 {wncd_x_R0-0}{1}: [client-orch-sm] [15154]: (debug): MAC: 286b.3598.580f IF
2023/08/08 13:37:58.240457105 {wncd_x_R0-0}{1}: [client-orch-sm] [15154]: (debug): MAC: 286b.3598.580f IF
2023/08/08 13:37:58.240459018 {wncd_x_R0-0}{1}: [client-orch-sm] [15154]: (note): MAC: 286b.3598.580f IF
```

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_9000000k
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_900000b[286b.3598
2023/08/08 13:37:58.924590710 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_900000b[286b.3598
2023/08/08 13:37:58.924606621 {wncd_x_R0-0}{1}: [webauth-httpd] [15154]: (info): capwap_9000000b[286b.35
2023/08/08 13:37:58.924617631 {wncd_x_R0-0}{1}: [webauth-httpd] [15154]: (info): capwap_9000000b[286b.35
2023/08/08 13:37:58.924646336 {wncd_x_R0-0}{1}: [webauth-httpd] [15154]: (info): capwap_9000000b[286b.35
2023/08/08 13:37:58.924646336 {wncd_x_R0-0}{1}: [webauth-httpd] [15154]: (info): capwap_9000000b[286b.35
2023/08/08 13:37:58.924811559 {wncd_x_R0-0}{1}: [webauth-httpd] [15154]: (info): capwap_9000000b[286b.35
2023/08/08 13:37:58.924823291 {wncd_x_R0-0}{1}: [webauth-state] [15154]: (info): capwap_9000000b[286b.35
2023/08/08 13:37:58.924830184 {wncd_x_R0-0}{1}: [webauth-state] [15154]: (info): capwap_9000000b[286b.35]
```

State INIT -> GET_REDIRECT

```
2023/08/08 13:37:58.924836706 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_900000b[286b.3598.
2023/08/08 13:37:58.924893704 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_900000b[286b.3598.
[...]
2023/08/08 13:38:16.814516928 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_900000b[286b.3598.
2023/08/08 13:38:16.814739389 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_900000b[286b.3598.
2023/08/08 13:38:16.843721875 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_9000000b[286b.3598.
2023/08/08 13:38:16.863779947 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_9000000b[286b.3598.
2023/08/08 13:38:16.863779947 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_9000000b[286b.3598.
2023/08/08 13:38:16.863779947 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_9000000b[286b.3598.
```

[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_900000b[286b.39
2023/08/08 13:38:16.863857023 {wncd_x_R0-0}{1}: [webauth-httpd] [15154]: (info): capwap_900000b[286b.39
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_900000b[286b.39
2023/08/08 13:38:16.864026684 {wncd_x_R0-0}{1}: [webauth-state] [15154]: (info): capwap_9000000b[286b.39
2023/08/08 13:38:16.864039067 {wncd_x_R0-0}{1}: [webauth-io] [15154]: (info): capwap_9000000b[286b.398
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 al
2023/08/08 13:38:16.864194552 {wncd_x_R0-0}{1}: [radius] [15154]: (info): RADIUS: Calling-Station-Id [3:
2023/08/08 13:38:16.864197568 {wncd_x_R0-0}{1}: [radius] [15154]: (info): RADIUS: User-Name [1] 7 "tiage
[...]
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.39
2023/08/08 13:38:16.879513532 {wncd_x_R0-0}{1}: [webauth-state] [15154]: (info): capwap_9000000b[286b.39]
2023/08/08 13:38:16.879530745 {wncd_x_R0-0}{1}: [webauth-acl] [15154]: (info): capwap_9000000b[286b.3598
Unapply IPv4 intecept ACL via SVM, name "IP-Adm-V4-Int-ACL-global"
, pri 50, IIF 0
[...]
2023/08/08 13:38:16.880956564 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [15154]: (note):
Authentication Success
. Resolved Policy bitmap:4 for client 286b.3598.580f
[...]
2023/08/08 13:38:16.882320225 {wncd_x_R0-0}{1}: [errmsg] [15154]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD
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 <u>Configure Local Web Authentication with External Authentication</u> 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: 0429.2ed
2023/08/10 14:35:20.685226454 {wncd_x_R0-0}{1}: [client-orch-state] [15195]: (info): MAC: 0429.2ed
2023/08/10 14:35:20.685420591 {wncd_x_R0-0}{1}: [dot11-validate] [15195]: (info): MAC: 0429.2ed
2023/08/10 14:35:20.685422154 {wncd_x_R0-0}{1}: [dot11-validate] [15195]: (info): MAC: 0429.2ed
2023/08/10 14:35:20.685864592 {wncd_x_R0-0}{1}: [dot11] [15195]: (debug): MAC: 0429.2ec9.e371 dd
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 Dot
2023/08/10 14:35:20.685886032 {wncd_x_R0-0}{1}: [dot11] [15195]: (info): MAC: 0429.2ec9.e371 Dot
2023/08/10 14:35:20.685886032 {wncd_x_R0-0}{1}: [dot11] [15195]: (info): MAC: 0429.2ec9.e371 Dot
2023/08/10 14:35:20.685886032 {wncd_x_R0-0}{1}: [dot11] [15195]: (info): MAC: 0429.2ec9.e371 Dot
2023/08/10 14:35:20.685886032 {wncd_x_R0-0}{1}: [dot11] [15195]: (info): MAC: 0429.2ec9.e371 Dot
2023/08/10 14:35:20.685886032 {wncd_x_R0-0}{1}: [dot11] [15195]: (info): MAC: 0429.2ec9.e371 Dot
2023/08/10 14:35:20.685886032 {wncd_x_R0-0}{1}: [dot11] [15195]: (info): MAC: 0429.2ec9.e371 Dot
2023/08/10 14:35:20.685886032 {wncd_x_R0-0}{1}: [dot11] [15195]: (info): MAC: 0429.2ec9.e371 Dot
2023/08/10 14:35:20.685886032 {wncd_x_R0-0}{1}: [dot11-frame] [15195]: (info): MAC: 0429.2ec9.e371 Dot
2023/08/10 14:35:20.685886032 {wncd_x_R0-0}{1}: [dot11-frame] [15195]: (info): MAC: 0429.2ec9.e371 Dot
2023/08/10 14:35:20.685886032 {wncd_x_R0-0}{1}: [dot11-frame] [15195]: (info): MAC: 0429.2ec9.e371 Dot
2023/08/10 14:35:20.685886032 {wncd_x_R0-0}{1}: [dot11-frame] [15195]: (info): MAC: 0429.2ec9.e371 Dot
2023/08/10 14:35:20.685886032 {wncd_x_R0-0}{1}: [dot11-frame] [15195]: (info): MAC: 0429.2ec9.e371 Dot
2023/08/10 14:35:20.685886032 {wncd_x_R0-0}{1}: [dot11-frame] [15195]: (info): MAC: 0429.2ec9.e371 Dot
2023/08/10 14:35:20.6
```

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 D01 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: 0429.2ec 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

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 14:35:20.721736890 {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 14:35:20.739644625 {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]: (info): 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.e371:capw 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): [0429.2ec9.e371:capw 2023/08/10 14:35:20.739861071 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [15195]: (info): [0429.2ec9.e371:capw 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[04 2023/08/10 14:35:20.740103810 {wncd_x_R0-0}{1}: [webauth-acl] [15195]: (info): capwap_90000010[04 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 2023/08/10 14:35:21.944028273 {wncd_x_R0-0}{1}: [client-orch-sm] [15195]: (debug): MAC: 0429.2ed 2023/08/10 14:35:21.944069521 {wncd_x_R0-0}{1}: [client-orch-sm] [15195]: (debug): MAC: 0429.2ed 2023/08/10 14:35:21.944074851 {wncd_x_R0-0}{1}: [client-orch-state] [15195]: (note): MAC: 0429.2ed 2023/08/10 14:35:21.944201671 {wncd_x_R0-0}{1}: [dot1x] [15195]: (info): [0000.0000.0000:capwap_ 2023/08/10 14:35:21.944759066 {wncd_x_R0-0}{1}: [client-auth] [15195]: (note): MAC: 0429.2ec9.e3

L3 Authentication initiated. LWA

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

S_AUTHIF_WEBAUTH_PENDING

```
[...]
```

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

GET rcvd when in LOGIN state

2023/08/10 14:35:24.110718893 {wncd_x_R0-0}{1}: [webauth-httpd] [15195]: (info): capwap_90000010

HTTP GET request

2023/08/10 14:35:24.110754721 {wncd_x_R0-0}{1}: [webauth-httpd] [15195]: (info): capwap_90000010 2023/08/10 14:35:24.110951163 {wncd_x_R0-0}{1}: [webauth-httpd] [15195]: (info): capwap_90000010 2023/08/10 14:35:24.110960801 {wncd_x_R0-0}{1}: [webauth-state] [15195]: (info): capwap_90000010

Param-map used: ExternalWebAuth

POST rcvd when in LOGIN state

2023/08/10 14:35:37.807287911 {wncd_x_R0-0}{1}: [webauth-httpd] [15195]: (info): capwap_90000010 2023/08/10 14:35:37.807331213 {wncd_x_R0-0}{1}: [webauth-httpd] [15195]: (info): capwap_90000010 [...] 2023/08/10 14:35:37.807498470 {wncd_x_R0-0}{1}: [webauth-state] [15195]: (info): capwap_90000010

Param-map used: ExternalWebAuth

2023/08/10 14:35:37.807503619 {wncd_x_R0-0}{1}: [webauth-state] [15195]: (info): capwap_90000010 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

```
CTU:
```

```
...
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-Add
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
[\ldots]
2023/08/10 14:35:37.890143566 {wncd_x_R0-0}{1}: [auth-mgr] [15195]: (info): [0429.2ec9.e371:cap
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
[\ldots]
```

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

OWE with CWA

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

<#root>

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

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

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

2023/08/11 12:43:45.551873379 {wncd x R0-0}{1}: [client-auth] [15200]: (note): MAC: 2495.2f72.8a MAB Authentication initiated. Policy VLAN 0, AAA override = 1, NAC = 1 2023/08/11 12:43:45.551925177 {wncd_x_R0-0}{1}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:cap 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 $[\ldots]$ 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 $[\ldots]$ 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

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:

2023/08/11 12:43:45.553851193 {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-Statio
2023/08/11	12:43:45.553863015	{wncd_x_R0-0}{1}:	[radius]	[15200]:	(info):	RADIUS:	Vendor, Aires
2023/08/11	12:43:45.553865510	{wncd_x_R0-0}{1}:	[radius]	[15200]:	(info):	RADIUS:	Airespace-WLA
2023/08/11	12:43:45.553867995	{wncd_x_R0-0}{1}:	[radius]	[15200]:	(info):	RADIUS:	Nas-Identifier
2023/08/11	12:43:45.553929331	{wncd_x_R0-0}{1}:	[radius]	[15200]:	(info):	RADIUS:	Started 5 sec
2023/08/11	12:43:45.570301533	{wncd_x_R0-0}{1}:	[radius]	[15200]:	(info):	RADIUS:	

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

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

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

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

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

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

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

2023/08/11 12:43:45.570621699 {wncd_x_R0-0}{1}: [mab] [15200]: (info): [2495.2f72.8a66:capwap_90 2023/08/11 12:43:45.570648140 {wncd_x_R0-0}{1}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:capw 2023/08/11 12:43:45.570657648 {wncd_x_R0-0}{1}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:capw 2023/08/11 12:43:45.570668839 {wncd_x_R0-0}{1}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:capw 2023/08/11 12:43:45.570709836 {wncd_x_R0-0}{1}: [auth-mgr] [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 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 Attribuurl-redirect 0 "https://192.168.1.7:8443/portal/gateway?sessionId=0F01A8C00000001EE49FCD0F&portal=26d19

[...]
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_6

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

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

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

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

[...]
2023/08/11 12:43:46.103210515 {wncd_x_R0-0}{1}: [client-iplearn] [15200]: (note):
MAC: 2495.2f72.8a66 Client IP learn successful. Method: DHCP IP: 192.168.1.162

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

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

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

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

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

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

[...]
2023/08/11 12:43:46.281818709 {wncd_x_R0-0}{1}: [webauth-state] [15200]: (info):
[2495.2f72.8a66][192.168.1.162]Param-map used: global

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

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

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

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

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

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

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

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

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

CoA Response Details

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

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

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

Send Access-Request to 192.168.1.7

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

User-Name [1] 14 "24952f728a66"

[...] 2023/08/11 12:44:20.313914609 {smd_R0-0}{1}: [aaa-coa] [17281]: (info): +++++ Received CoA resp 2023/08/11 12:44:20.313917665 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: NAS-IP-Address 2023/08/11 12:44:20.313924488 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: NAS-Port-Type 2023/08/11 12:44:20.313931051 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: NAS-Port [5] 6 2023/08/11 12:44:20.31393559 {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-Statior 2023/08/11 12:44:20.313965616 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Calling-Statior 2023/08/11 12:44:20.313978210 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Calling-Statior 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: Vendor, Airesp 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-Identifien
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-1
2023/08/11 12:44:20.314077337 {smd_R0-0}{1}: [radius] [17281]: (info): RADIUS:
```

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

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

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

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

User-Name [1] 7 "tiago"

2023/08/11 12:44:20.327867512 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Class [25] 51 2023/08/11 12:44:20.327938827 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Message-Auther 2023/08/11 12:44:20.327978472 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Vendor, Cisco 2023/08/11 12:44:20.327985516 {wncd_x_R0-0}{1}: [radius] [15200]: (info): RADIUS: Cisco AVpair | 2023/08/11 12:44:20.328027385 {wncd_x_R0-0}{1}: [radius] [15200]: (info): Valid Response Packet, 2023/08/11 12:44:20.328322423 {wncd_x_R0-0}{1}: [mab] [15200]: (info): [2495.2f72.8a66:capwap_90 2023/08/11 12:44:20.328341299 {wncd_x_R0-0}{1}: [mab] [15200]: (info): [2495.2f72.8a66:capwap_90 2023/08/11 12:44:20.328394871 {wncd_x_R0-0}{1}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:capwap_90 2023/08/11 12:44:20.328412885 {wncd_x_R0-0}{1}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:capw 2023/08/11 12:44:20.32841285 {wncd_x_R0-0}{1}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:capw 2023/08/11 12:44:20.32841270 {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}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:capw 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:capv
[...]
2023/08/11 12:44:20.330928236 {wncd_x_R0-0}{1}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:capv
2023/08/11 12:44:20.330937604 {wncd_x_R0-0}{1}: [auth-mgr] [15200]: (info): [2495.2f72.8a66:capv
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-6CLIENT_ADDED_TO_RUN_STATE: R0/0: wncd: Username entry (tiago) joined with ssid (wifi6E_CWA) for device with a specific content of the state of the

```
[...]
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: 2495.2f72.8a66
```

Refer to document <u>Configure Central Web Authentication (CWA) on Catalyst 9800 WLC and ISE</u> 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