

Configure FlexConnect EWA on Catalyst 9800 WLC and ISE

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Network Diagram](#)

[Configurations](#)

[Verify](#)

[RA Trace Example of a Successful Attempt](#)

[Related Information](#)

Introduction

This document describes how to configure a FlexConnect EWA on Catalyst 9800 WLC and ISE.

Prerequisites

Requirements

Cisco recommends that you have knowledge of 9800 Wireless LAN Controllers (WLC) configuration.

Components Used

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

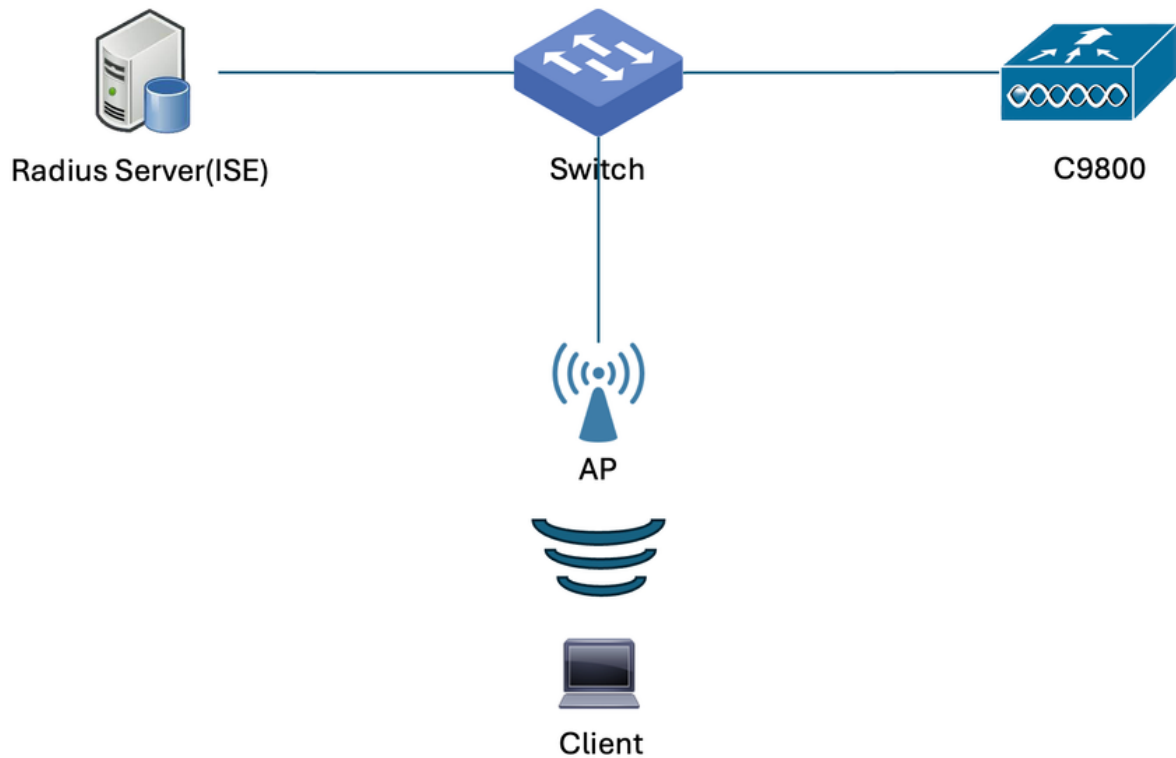
- Cisco Catalyst 9800 WLC Cisco IOS®XE Version 17.15.3
- Identity Service Engine (ISE) v3.4.0.608

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.

Configure

Network Diagram

This document is based on this topology:

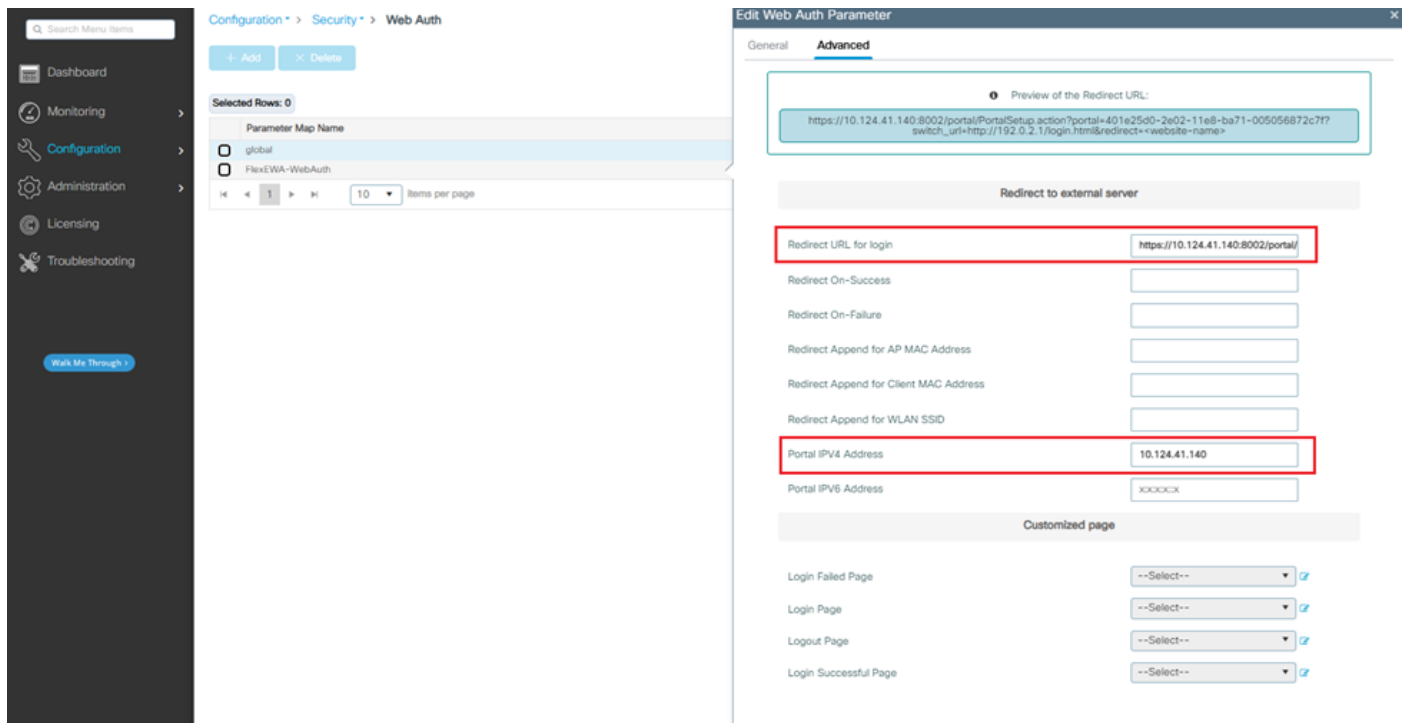


Configurations

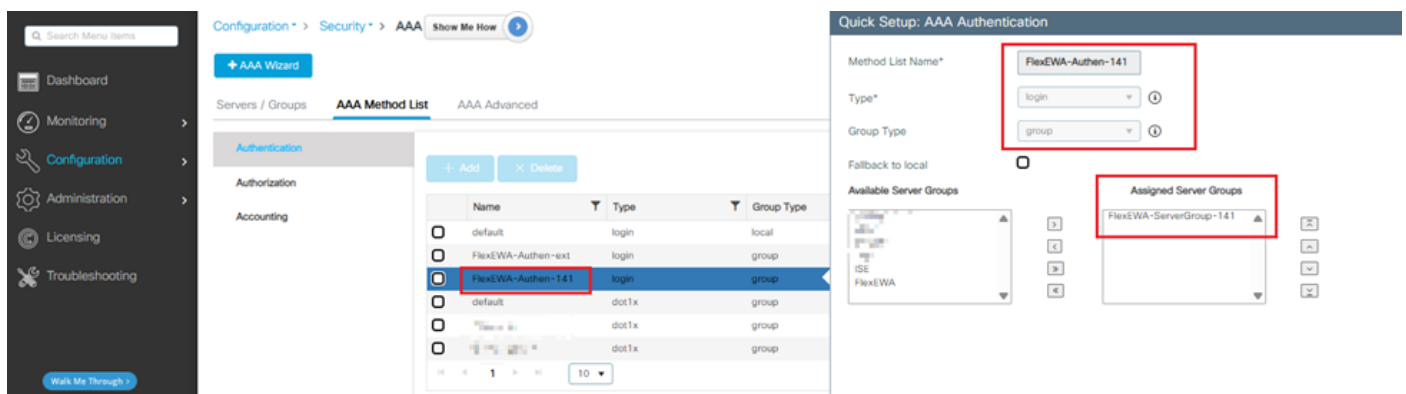
Step 1. Navigate to **Configuration > Security > Web Auth > +Add a Web Auth Parameter Map**.

The screenshot shows the Cisco configuration interface. On the left is a sidebar with navigation options: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main area displays the 'Configuration > Security > Web Auth' path. A table lists 'Parameter Map Name' entries: 'global', 'FlexEWA-WebAuth', and 'FlexEWA-WebAuth-141'. The 'Edit Web Auth Parameter' dialog is open, showing the 'General' tab. The 'Parameter-map Name' is set to 'FlexEWA-WebAuth-1'. The 'Type' is set to 'webauth'. The 'Banner Configuration' section shows 'Banner Title' and 'Banner Type' (set to 'None'). Other settings include 'Maximum HTTP connections' (100), 'Init-State Timeout(secs)' (120), and 'Sleeping Client Timeout (minutes)' (720).

The portal URL is generated from ISE (step 7).



Step 2. Navigate to **Configuration > Security > AAA > AAA Method List > Authentication > + Add an Authentication List**.



Step 3. Suppose HTTPS port is 8002, refer to the auto-generated ACL WA-sec-10.124.41.140 to add a new preauthentication ACL.

The screenshot shows the 'Configuration > Security > ACL' page. The 'ACL Name' list on the left highlights 'FlexEWA141-sec-ACL'. The 'Edit ACL' window on the right shows the configuration for 'FlexEWA141-sec-ACL' with the following rules:

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
10	permit	any		10.124.41.141		tcp	None	eq www	None	Disabled
15	permit	any		10.124.41.141		tcp	None	eq 8002	None	Disabled
20	permit	any		10.124.41.141		tcp	None	eq 443	None	Disabled
25	permit	10.124.41.141		any		tcp	eq 8002	None	None	Disabled
30	permit	10.124.41.141		any		tcp	eq www	None	None	Disabled
40	permit	10.124.41.141		any		tcp	eq 443	None	None	Disabled
50	permit	any		any		tcp	None	eq domain	None	Disabled
60	permit	any		any		udp	None	eq domain	None	Disabled
70	permit	any		any		udp	None	eq bootpc	None	Disabled
80	permit	any		any		udp	None	eq bootps	None	Disabled

Step 4. Check the auto-generated ACL WA-v4-int 10.124.41.141.

The screenshot shows the 'Configuration > Security > ACL' page. The 'ACL Name' list on the left highlights 'WA-v4-int-10.124.41.141'. The 'Edit ACL' window on the right shows the configuration for 'WA-v4-int-10.124.41.141' with the following rules:

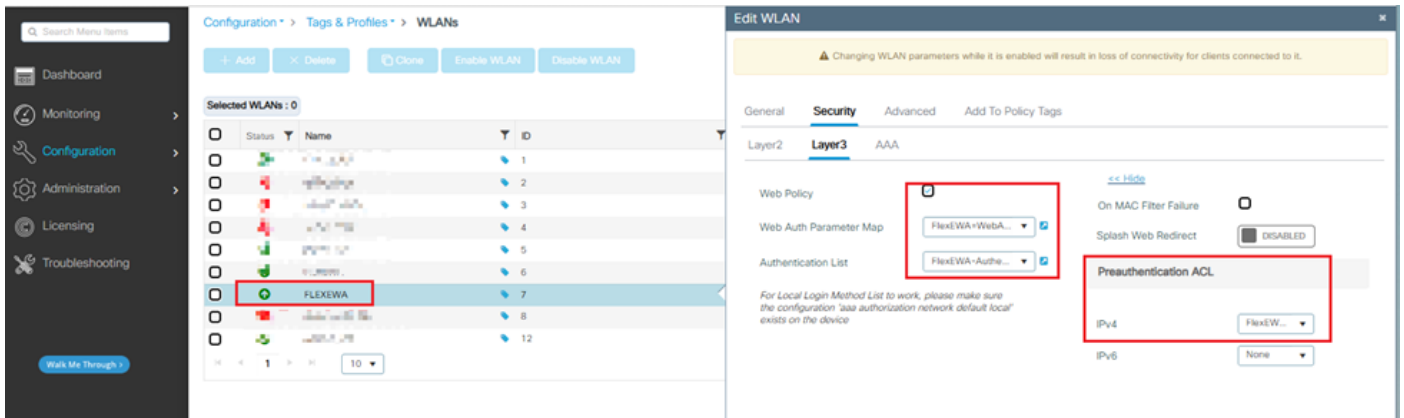
Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
10	deny	any		10.124.41.141		tcp	None	eq www	None	Disabled
20	permit	any		any		tcp	None	eq www	None	Disabled

Step 5. Apply the two ACLs to **Configuration > Tags&Profiles > Flex > Flex Profile > Policy ACL**.

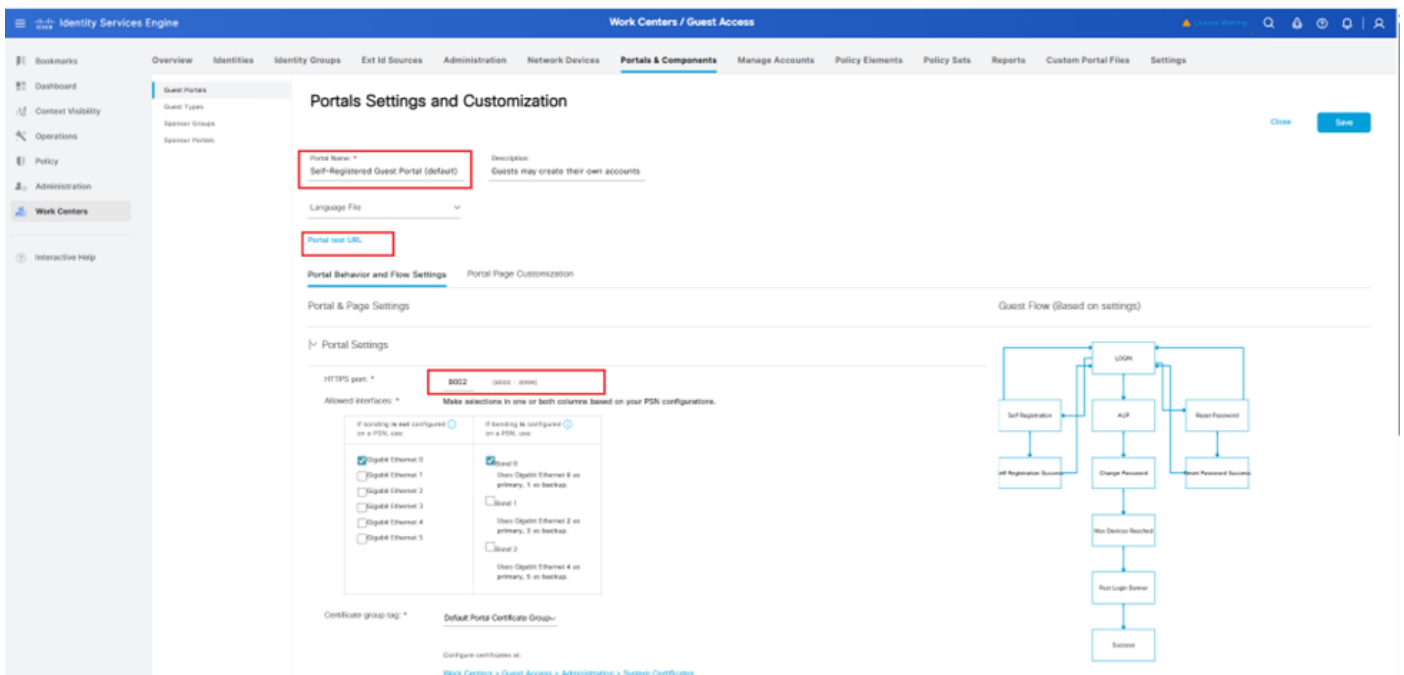
The screenshot shows the 'Configuration > Tags & Profiles > Flex' page. The 'Flex Profile Name' list on the left highlights 'default-flex-profile'. The 'Edit Flex Profile' window on the right shows the 'Policy ACL' tab with the following ACLs applied:

ACL Name	Central Web Auth	URL Filter
FlexEWA141-sec-ACL	Disabled	
WA-v4-int-10.124.41.141	Disabled	

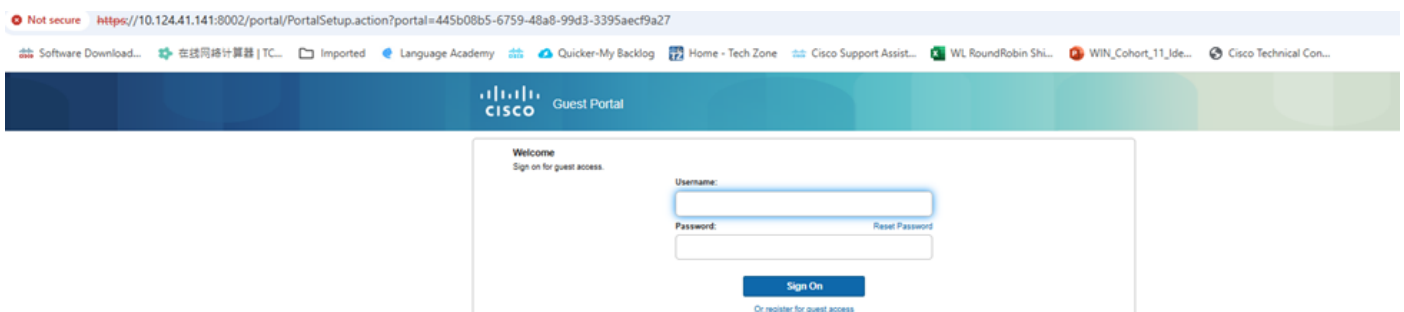
Step 6. Apply the newly-created Web Auth Parameter Map, Authentication List, and Preauthentication ACL to WLAN.



Step 7. Navigate to **Work Centers > Portals & Components > Guest Portals > Portals Settings and Customization > Portal Name > Self-Registered Guest Portal (default)** to generate Portal URL from ISE.

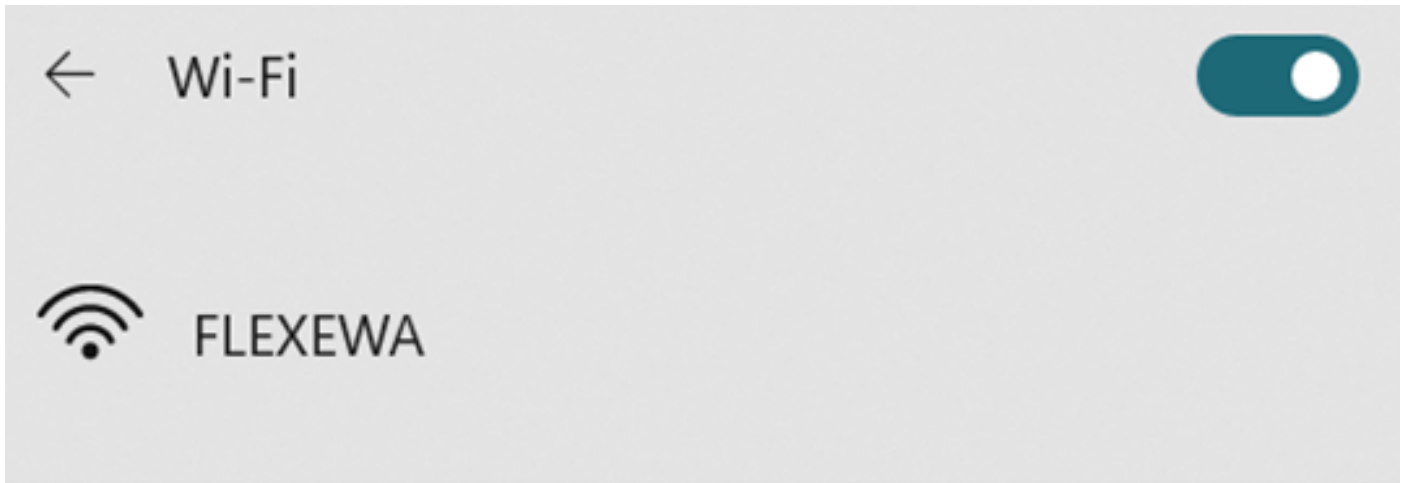


This listed web portal is popped out after clicking Portal test URL.

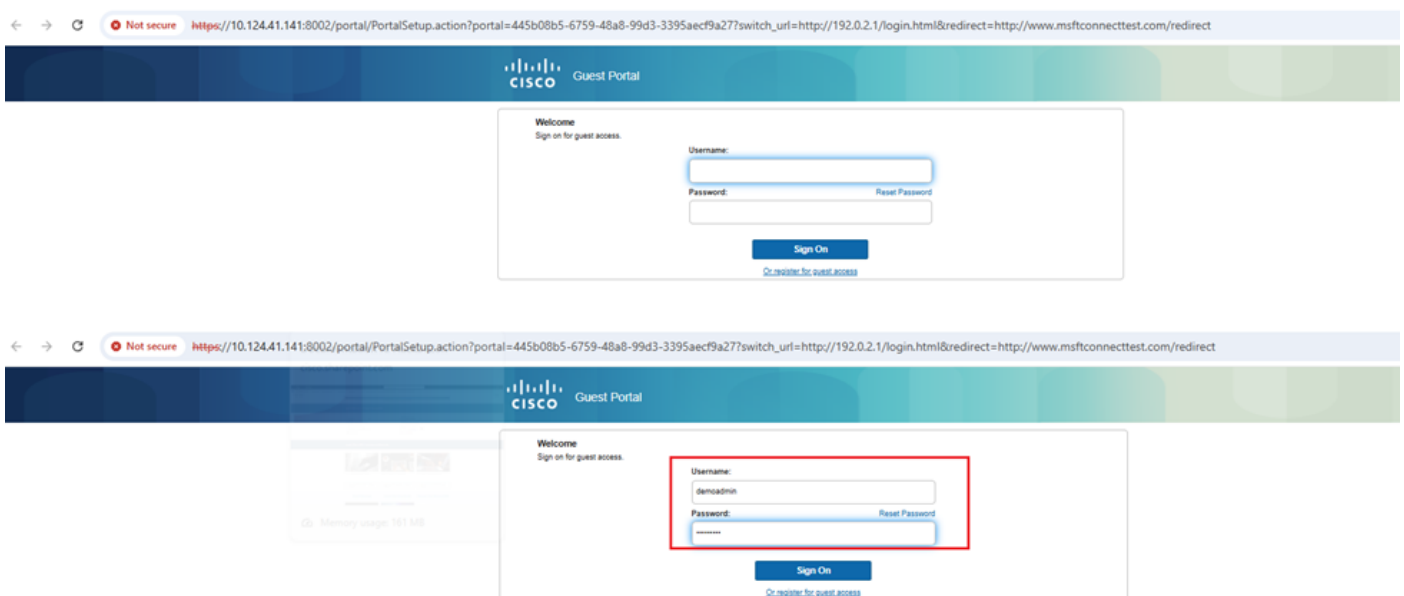


Verify

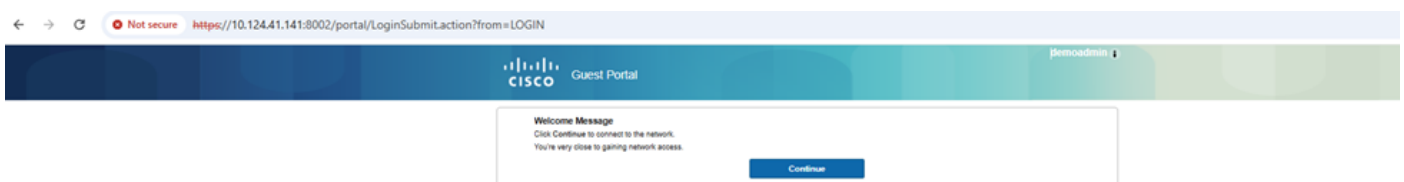
Step 1. Connecting FLEXEWA SSID.



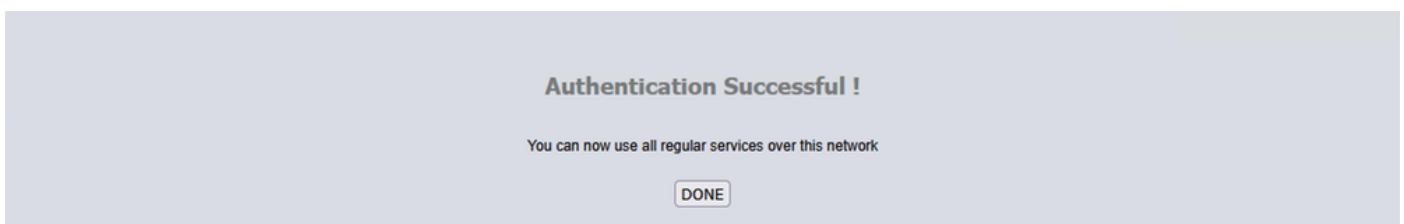
Step 2. Redirect to portal and input **username** and **password**.



Step 3. The Guest Portal pops up:



Step 4. After clicking **Continue**, Authentication is Successful:



RA Trace Example of a Successful Attempt

This is the output of a successful connection attempt from the Radio Active trace perspective. Use this as a reference to identify client session stages for clients that connect to a Layer 3 web authentication SSID.

Client associated successfully:

```
2025/09/09 15:21:48.617769958 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: (note): MAC:
f0b6.1e39.9ce8 Association received. BSSID c418.fc82.bb0b, WLAN FLEXEWA, Slot 1 AP
c418.fc82.bb00, 9178_1, Site tag HK, Policy tag default-policy-tag, Policy profile default-policy-profile,
Switching Central, Socket delay 0ms, AP BSSID MAC c418.fc82.bb0b
2025/09/09 15:21:48.617813534 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: (debug): MAC:
f0b6.1e39.9ce8 Received Dot11 association request. Processing started,SSID: FLEXEWA, Policy profile:
default-policy-profile, AP Name: 9178_1, Ap Mac Address: c418.fc82.bb00BSSID
MAC0000.0000.0000wlan ID: 7RSSI: -30, SNR: 67
2025/09/09 15:21:48.618002570 {wncd_x_R0-0}{1}: [client-orch-state] [17842]: (note): MAC:
f0b6.1e39.9ce8 Client state transition: S_CO_INIT -> S_CO_ASSOCIATING
2025/09/09 15:21:48.618017149 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: (ERR): MAC:
f0b6.1e39.9ce8 Failed to get dot11 record
2025/09/09 15:21:48.618301251 {wncd_x_R0-0}{1}: [dot11-validate] [17842]: (info): MAC:
f0b6.1e39.9ce8 Dot11 ie validate ext/supp rates. Validation Passed for Supported rates radio_type 2
2025/09/09 15:21:48.618320304 {wncd_x_R0-0}{1}: [dot11-validate] [17842]: (debug): MAC:
f0b6.1e39.9ce8 Dot11 ie validate rsnx, client not using sae, skip check
2025/09/09 15:21:48.618339230 {wncd_x_R0-0}{1}: [dot11-validate] [17842]: (info): MAC:
f0b6.1e39.9ce8 WiFi direct: Dot11 validate P2P IE. P2P IE not present.
2025/09/09 15:21:48.618598747 {wncd_x_R0-0}{1}: [dot11] [17842]: (debug): MAC: f0b6.1e39.9ce8
dot11 send association response. Framing association response with resp_status_code: 0
2025/09/09 15:21:48.618604733 {wncd_x_R0-0}{1}: [dot11] [17842]: (debug): MAC: f0b6.1e39.9ce8
Dot11 Capability info byte1 1, byte2: 11
2025/09/09 15:21:48.618696034 {wncd_x_R0-0}{1}: [dot11-frame] [17842]: (info): MAC: f0b6.1e39.9ce8
WiFi direct: skip build Assoc Resp with P2P IE: Wifi direct policy disabled
2025/09/09 15:21:48.618785409 {wncd_x_R0-0}{1}: [dot11] [17842]: (info): MAC: f0b6.1e39.9ce8 dot11
send association response. Sending assoc response of length: 177 with resp_status_code: 0,
DOT11_STATUS: DOT11_STATUS_SUCCESS
2025/09/09 15:21:48.618791096 {wncd_x_R0-0}{1}: [dot11] [17842]: (note): MAC: f0b6.1e39.9ce8
Association success. AID 33, Roaming = False, WGB = False, 11r = False, 11w = False Fast roam = False
2025/09/09 15:21:48.618806595 {wncd_x_R0-0}{1}: [dot11] [17842]: (info): MAC: f0b6.1e39.9ce8
DOT11 state transition: S_DOT11_INIT -> S_DOT11_ASSOCIATED
2025/09/09 15:21:48.618855282 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: (debug): MAC:
f0b6.1e39.9ce8 Station Dot11 association is successful.
```

Layer 2 authentication skipped:

```
2025/09/09 15:21:48.618992721 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: (debug): MAC:
f0b6.1e39.9ce8 Starting L2 authentication. Bssid in state machine:c418.fc82.bb0b Bssid in request
is:c418.fc82.bb0b
2025/09/09 15:21:48.619006036 {wncd_x_R0-0}{1}: [client-orch-state] [17842]: (note): MAC:
f0b6.1e39.9ce8 Client state transition: S_CO_ASSOCIATING -> S_CO_L2_AUTH_IN_PROGRESS
2025/09/09 15:21:48.619093387 {wncd_x_R0-0}{1}: [client-auth] [17842]: (note): MAC: f0b6.1e39.9ce8
L2 Authentication initiated. method WEBAUTH, Policy VLAN 0, AAA override = 0
[...]
2025/09/09 15:21:48.623839337 {wncd_x_R0-0}{1}: [client-auth] [17842]: (info): MAC: f0b6.1e39.9ce8
Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_PENDING ->
S_AUTHIF_L2_WEBAUTH_DONE
2025/09/09 15:21:48.623863687 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] Device type for the session is detected as Intel-Device and old Intel-
```

Device & Device name for the session is detected as INTEL CORPORATE and old INTEL CORPORATE & Old protocol map 1 and new is 1

2025/09/09 15:21:48.623873529 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] auth mgr attr add/change notification is received for attr dc-profile-name(1130)

2025/09/09 15:21:48.623911035 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: (debug): MAC:
f0b6.1e39.9ce8 L2 Authentication of station is successful., L3 Authentication : 1

ACL plumb:

2025/09/09 15:21:48.620896754 {wncd_x_R0-0}{1}: [webauth-sm] [17842]: (info): [0.0.0.0]Starting
Webauth, mac [f0:b6:1e:39:9c:e8],IIF 0 , audit-ID D1257C0A000000CA2D54F867

2025/09/09 15:21:48.620927053 {wncd_x_R0-0}{1}: [webauth-state] [17842]: (info): [f0b6.1e39.9ce8][
0.0.0.0]Param-map used: global

2025/09/09 15:21:48.620935005 {wncd_x_R0-0}{1}: [webauth-state] [17842]: (info): [f0b6.1e39.9ce8][
0.0.0.0]State Invalid State -> INIT

2025/09/09 15:21:48.620942683 {wncd_x_R0-0}{1}: [webauth-sess] [17842]: (info):
capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Create session, Add address 0.0.0.0

2025/09/09 15:21:48.620946808 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [17842]: (info):
[0000.0000.0000:unknown] Retrieved zone id 0x0 for bssid 12364632846638254486

2025/09/09 15:21:48.620958619 {wncd_x_R0-0}{1}: [webauth-state] [17842]: (info):
capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Param-map used: FlexEWA=WebAuth-141

2025/09/09 15:21:48.620962048 {wncd_x_R0-0}{1}: [webauth-state] [17842]: (info):
capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]State INIT -> INIT

2025/09/09 15:21:48.620978097 {wncd_x_R0-0}{1}: [webauth-sm] [17842]: (info):
capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Initiate session, forward state to 0 IF 0x900000008 mac
[f0b6.1e39.9ce8]

2025/09/09 15:21:48.620981018 {wncd_x_R0-0}{1}: [webauth-sm] [17842]: (info):
capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Initiate session, SM init sessions 5

2025/09/09 15:21:48.620988217 {wncd_x_R0-0}{1}: [webauth-state] [17842]: (info):
capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Param-map used: FlexEWA=WebAuth-141

2025/09/09 15:21:48.620991618 {wncd_x_R0-0}{1}: [webauth-state] [17842]: (info):
capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]State INIT -> INIT

2025/09/09 15:21:48.621023019 {wncd_x_R0-0}{1}: [webauth-acl] [17842]: (info):
capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Applying IPv4 intercept ACL via SVM, name: WA-v4-int-
10.124.41.141-7, priority: 50, IIF-ID: 0

2025/09/09 15:21:48.621032776 {wncd_x_R0-0}{1}: [svm] [17842]: (info): SVM_INFO: Applying Svc
Templ WA-v4-int-10.124.41.141-7 (ML:NONE)

2025/09/09 15:21:48.621786262 {wncd_x_R0-0}{1}: [epm] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] Feature (EPM URL PLUG-IN) has been started (status Success)

2025/09/09 15:21:48.621804034 {wncd_x_R0-0}{1}: [epm-acl] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] Filter-Id : FlexEWA141-sec-ACL received

2025/09/09 15:21:48.622151544 {wncd_x_R0-0}{1}: [epm] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] Feature (EPM ACL PLUG-IN) has been started (status Success)

2025/09/09 15:21:48.622187815 {wncd_x_R0-0}{1}: [svm] [17842]: (info): SVM_INFO: Response of epm
is SYNC with return code Success

2025/09/09 15:21:48.622226011 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] Raising ext evt Template Activated (9) on this session, client
(unknown) (0)

2025/09/09 15:21:48.622265240 {wncd_x_R0-0}{1}: [webauth-acl] [17842]: (info):
capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Applying IPv6 intercept ACL via SVM, name: IP-Adm-V6-
Int-ACL-global-7, priority: 52, IIF-ID: 0

2025/09/09 15:21:48.622270327 {wncd_x_R0-0}{1}: [svm] [17842]: (info): SVM_INFO: Applying Svc
Templ IP-Adm-V6-Int-ACL-global-7 (ML:NONE)

2025/09/09 15:21:48.622898831 {wncd_x_R0-0}{1}: [epm] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] Feature (EPM URL PLUG-IN) has been started (status Success)
2025/09/09 15:21:48.622932973 {wncd_x_R0-0}{1}: [svm] [17842]: (info): SVM_INFO: Response of epm
is SYNC with return code Success
2025/09/09 15:21:48.622957784 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] Raising ext evt Template Activated (9) on this session, client
(unknown) (0)
2025/09/09 15:21:48.623119047 {wncd_x_R0-0}{1}: [dot11] [17842]: (debug): MAC: f0b6.1e39.9ce8
Dot11 SAE finds ipsk progress as 0, not in pending state
2025/09/09 15:21:48.623126095 {wncd_x_R0-0}{1}: [llbridge-main] [17842]: (debug): MAC:
f0b6.1e39.9ce8 Link-local bridging not enabled for this client, not checking VLAN validity
2025/09/09 15:21:48.623205421 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] Context changing state from 'Idle' to 'Running'
2025/09/09 15:21:48.623209350 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] Method webauth changing state from 'Not run' to 'Running'
2025/09/09 15:21:48.623572855 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] SM cannot send event Template Activated to PRE for 0x8D0000C0
2025/09/09 15:21:48.623680228 {wncd_x_R0-0}{1}: [client-auth] [17842]: (info): MAC: f0b6.1e39.9ce8
Client auth-interface state transition: S_AUTHIF_AWAIT_L2_WEBAUTH_START_RESP ->
S_AUTHIF_L2_WEBAUTH_PENDING

IP Learn process:

2025/09/09 15:21:51.628124695 {wncd_x_R0-0}{1}: [client-orch-state] [17842]: (note): MAC:
f0b6.1e39.9ce8 Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS ->
S_CO_IP_LEARN_IN_PROGRESS
2025/09/09 15:21:51.628463813 {wncd_x_R0-0}{1}: [client-iplearn] [17842]: (info): MAC:
f0b6.1e39.9ce8 IP-learn state transition: S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS
2025/09/09 15:21:51.632284534 {wncd_x_R0-0}{1}: [client-auth] [17842]: (info): MAC: f0b6.1e39.9ce8
Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_DONE ->
S_AUTHIF_L2_WEBAUTH_DONE
2025/09/09 15:21:51.676501288 {wncd_x_R0-0}{1}: [sisf-packet] [17842]: (info): RX: IPv6 DHCP from
intf capwap_90000008 on vlan 174 Src MAC: f0b6.1e39.9ce8 Dst MAC: 3333.0001.0002 Ipv6 SRC:
fe80::3f83:2848:d30:7aea, Ipv6 DST: ff02::1:2, type: msg type: DHCPV6_MSG_SOLICIT xid: 14443573
2025/09/09 15:21:51.676541447 {wncd_x_R0-0}{1}: [sisf-packet] [17842]: (info): TX: IPv6 DHCP from
intf capwap_90000008 on vlan 174 Src MAC: f0b6.1e39.9ce8 Dst MAC: 3333.0001.0002 Ipv6 SRC:
fe80::3f83:2848:d30:7aea, Ipv6 DST: ff02::1:2, type: msg type: DHCPV6_MSG_SOLICIT xid: 14443573
2025/09/09 15:21:51.706187097 {wncd_x_R0-0}{1}: [sisf-packet] [17842]: (info): RX: ARP from interface
capwap_90000008 on vlan 174 Source MAC: f0b6.1e39.9ce8 Dest MAC: ffff.ffff.ffff ARP REQUEST,
ARP sender MAC: f0b6.1e39.9ce8 ARP target MAC: 0000.0000.0000 ARP sender IP: 169.254.137.222,
ARP target IP: 169.254.137.222,
[...]
2025/09/09 15:21:52.686190945 {wncd_x_R0-0}{1}: [client-iplearn] [17842]: (note): MAC:
f0b6.1e39.9ce8 Client IP learn successful. Method: DHCP IP: 10.124.37.251
2025/09/09 15:21:52.686244192 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] auth mgr attr add/change notification is received for attr addr(8)
2025/09/09 15:21:52.686285422 {wncd_x_R0-0}{1}: [webauth-sess] [17842]: (info):
capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Change notif CB, Add address 10.124.37.251 [f0b6.1e39.9ce8]
2025/09/09 15:21:52.686289265 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [17842]: (info):
[0000.0000.0000:unknown] Retrieved zone id 0x0 for bssid 12364632846638254486
2025/09/09 15:21:52.686291647 {wncd_x_R0-0}{1}: [webauth-sess] [17842]: (info): adding webauth
session to ipv4 hash table for vrf id 0, ipv4 vrf table id 0
2025/09/09 15:21:52.686430038 {wncd_x_R0-0}{1}: [auth-mgr-feat_acct] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] SM Notified attribute Add/Update addr 10.124.37.251

2025/09/09 15:21:52.686456653 {wncd_x_R0-0}{1}: [epm] [17842]: (info): [0000.0000.0000:unknown]
HDL = 0x0 vlan 174 fail count 0 dirty_counter 0 is_dirty 0
2025/09/09 15:21:52.686710209 {wncd_x_R0-0}{1}: [client-iplearn] [17842]: (info): MAC:
f0b6.1e39.9ce8 IP-learn state transition: S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE

Layer 3 authentication and redirection process:

2025/09/09 15:21:52.687395906 {wncd_x_R0-0}{1}: [client-auth] [17842]: (note): MAC: f0b6.1e39.9ce8
L3 Authentication initiated. LWA
2025/09/09 15:21:52.687472722 {wncd_x_R0-0}{1}: [client-auth] [17842]: (info): MAC: f0b6.1e39.9ce8
Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_DONE ->
S_AUTHIF_WEBAUTH_PENDING

2025/09/09 15:21:52.687723489 {wncd_x_R0-0}{1}: [sisf-packet] [17842]: (info): RX: DHCPv4 from
interface Po1 on vlan 174 Src MAC: 4006.d589.4e78 Dst MAC: ffff.ffff.ffff src_ip: 10.124.37.242, dst_ip:
255.255.255.255, BOOTPREPLY, SISF_DHCPACK, giaddr: 0.0.0.0, yiaddr: 10.124.37.251, CMAC:
f0b6.1e39.9ce8

2025/09/09 15:21:52.687992316 {wncd_x_R0-0}{1}: [sisf-packet] [17842]: (info): TX: DHCPv4 from
interface Po1 on vlan 174 Src MAC: 4006.d589.4e78 Dst MAC: f0b6.1e39.9ce8 src_ip: 10.124.37.242,
dst_ip: 255.255.255.255, BOOTPREPLY, SISF_DHCPACK, giaddr: 0.0.0.0, yiaddr: 10.124.37.251,
CMAC: f0b6.1e39.9ce8

2025/09/09 15:21:52.688020475 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [17842]: (verbose):
Type:EWLC_CAPWAP_HDR_AP, Id:23277
[...]

2025/09/09 15:21:55.663715832 {wncd_x_R0-0}{1}: [webauth-io] [17842]: (info):
capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]54129/197 IO state NEW -> READING

2025/09/09 15:21:55.664060604 {wncd_x_R0-0}{1}: [webauth-io] [17842]: (info):
capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]54129/197 Read event, Message ready

2025/09/09 15:21:55.664071121 {wncd_x_R0-0}{1}: [webauth-httpd] [17842]: (info):
capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]GET rcvd when in INIT state

2025/09/09 15:21:55.664077798 {wncd_x_R0-0}{1}: [webauth-httpd] [17842]: (info):
capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]HTTP GET request

2025/09/09 15:21:55.664094019 {wncd_x_R0-0}{1}: [webauth-httpd] [17842]: (info):
capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]Parse GET, src [10.124.37.251] dst [23.5.165.82] url
<http://www.msftconnecttest.com/connecttest.txt>

[...]

2025/09/09 15:22:16.420792303 {wncd_x_R0-0}{1}: [webauth-httpd] [17842]: (info):
capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]POST rcvd when in LOGIN state

2025/09/09 15:22:32.375197748 {wncd_x_R0-0}{1}: [webauth-acl] [17842]: (info):
capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]Unapply IPv4 intecept ACL via SVM, name "WA-v4-
int-10.124.41.141-7", pri 50, IIF 0

2025/09/09 15:22:32.376230716 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] Raising ext evt Template Deactivated (11) on this session, client
(unknown) (0)

2025/09/09 15:22:32.376262689 {wncd_x_R0-0}{1}: [webauth-acl] [17842]: (info):
capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]Unapply IPv6 intecept ACL via SVM, name "IP-Adm-
V6-Int-ACL-global", pri 52, IIF 0

2025/09/09 15:22:32.376734374 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info):
[f0b6.1e39.9ce8:capwap_90000008] Raising ext evt Template Deactivated (11) on this session, client
(unknown) (0)

2025/09/09 15:22:32.376865998 {wncd_x_R0-0}{1}: [dot11] [17842]: (debug): MAC: f0b6.1e39.9ce8
Dot11 SAE finds ipsk progress as 0, not in pending state

2025/09/09 15:22:32.376870611 {wncd_x_R0-0}{1}: [llbridge-main] [17842]: (debug): MAC: f0b6.1e39.9ce8 Link-local bridging not enabled for this client, not checking VLAN validity
2025/09/09 15:22:32.376949875 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (info): [f0b6.1e39.9ce8:capwap_900000008] Authc success from WebAuth, Auth event success

Transition to RUN state:

2025/09/09 15:22:32.379351256 {wncd_x_R0-0}{1}: [client-auth] [17842]: (note): MAC: f0b6.1e39.9ce8 ADD MOBILE sent. Client state flags: 0x38 BSSID: MAC: c418.fc82.bb0b capwap IFID: 0x900000008, Add mobiles sent: 1
2025/09/09 15:22:32.379583842 {wncd_x_R0-0}{1}: [errmsg] [17842]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: R0/0: wncd: Username entry (demoadmin) joined with ssid (FLEXEWA) for device with MAC: f0b6.1e39.9ce8 on channel (100)
2025/09/09 15:22:32.379671775 {wncd_x_R0-0}{1}: [aaa-attr-inf] [17842]: (info): [Applied attribute :bsn-vlan-interface-name 0 "wlc-management"]
2025/09/09 15:22:32.379673695 {wncd_x_R0-0}{1}: [aaa-attr-inf] [17842]: (info): [Applied attribute : timeout 0 28800 (0x7080)]
2025/09/09 15:22:32.379683417 {wncd_x_R0-0}{1}: [aaa-attr-inf] [17842]: (info): [Applied attribute : url-redirect-acl 0 "IP-Adm-V4-LOGOUT-ACL"]
2025/09/09 15:22:32.379727993 {wncd_x_R0-0}{1}: [ewlc-qos-client] [17842]: (info): MAC: f0b6.1e39.9ce8 Client QoS run state handler
2025/09/09 15:22:32.379756610 {wncd_x_R0-0}{1}: [rog-proxy-capwap] [17842]: (debug): Managed client RUN state notification: f0b6.1e39.9ce8
2025/09/09 15:22:32.379810670 {wncd_x_R0-0}{1}: [client-orch-state] [17842]: (note): MAC: f0b6.1e39.9ce8 Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RUN

Related Information

- [Configure and Troubleshoot External Web-Authentication on 9800 WLC](#)