

Configuración de FlexConnect EWA en Catalyst 9800 WLC e ISE

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Ejemplo de Seguimiento de RA de un Intento Exitoso](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar un FlexConnect EWA en Catalyst 9800 WLC e ISE.

Prerequisites

Requirements

Cisco recomienda conocer la configuración de los controladores LAN inalámbricos (WLC) 9800.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

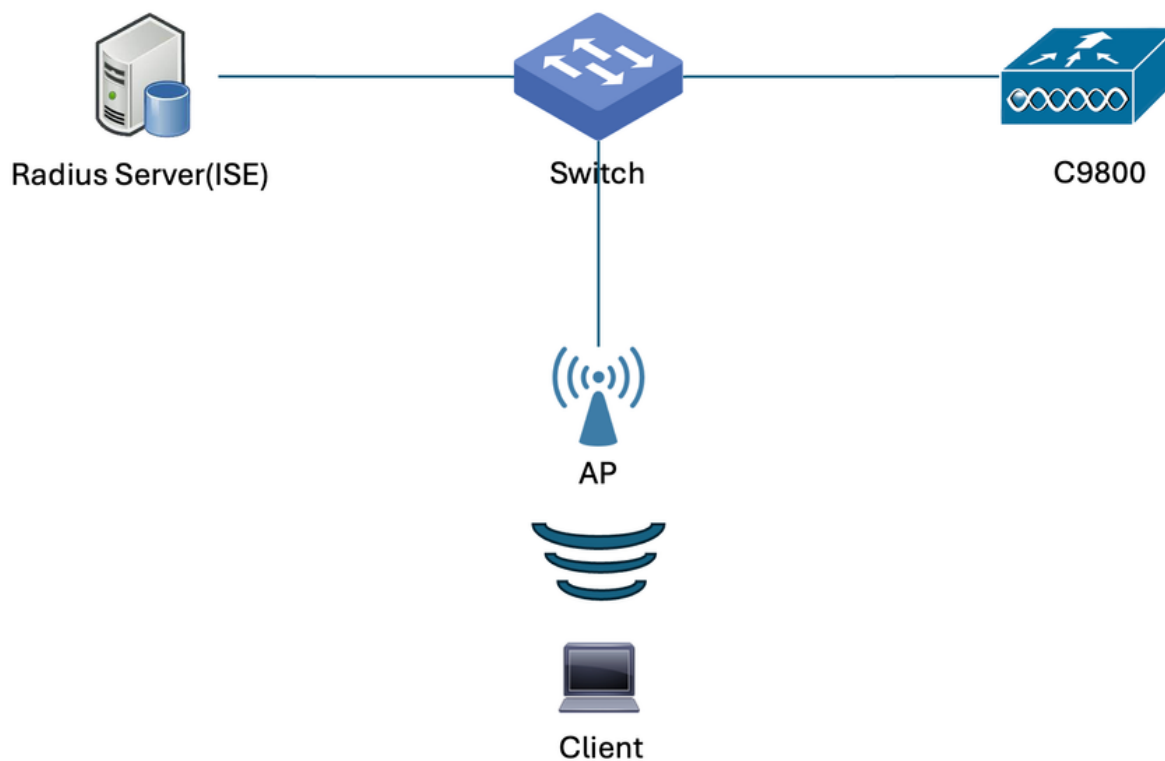
- Cisco Catalyst 9800 WLC Cisco IOS®XE versión 17.15.3
- Identity Service Engine (ISE) v3.4.0.608

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de la red

Este documento se basa en esta topología:

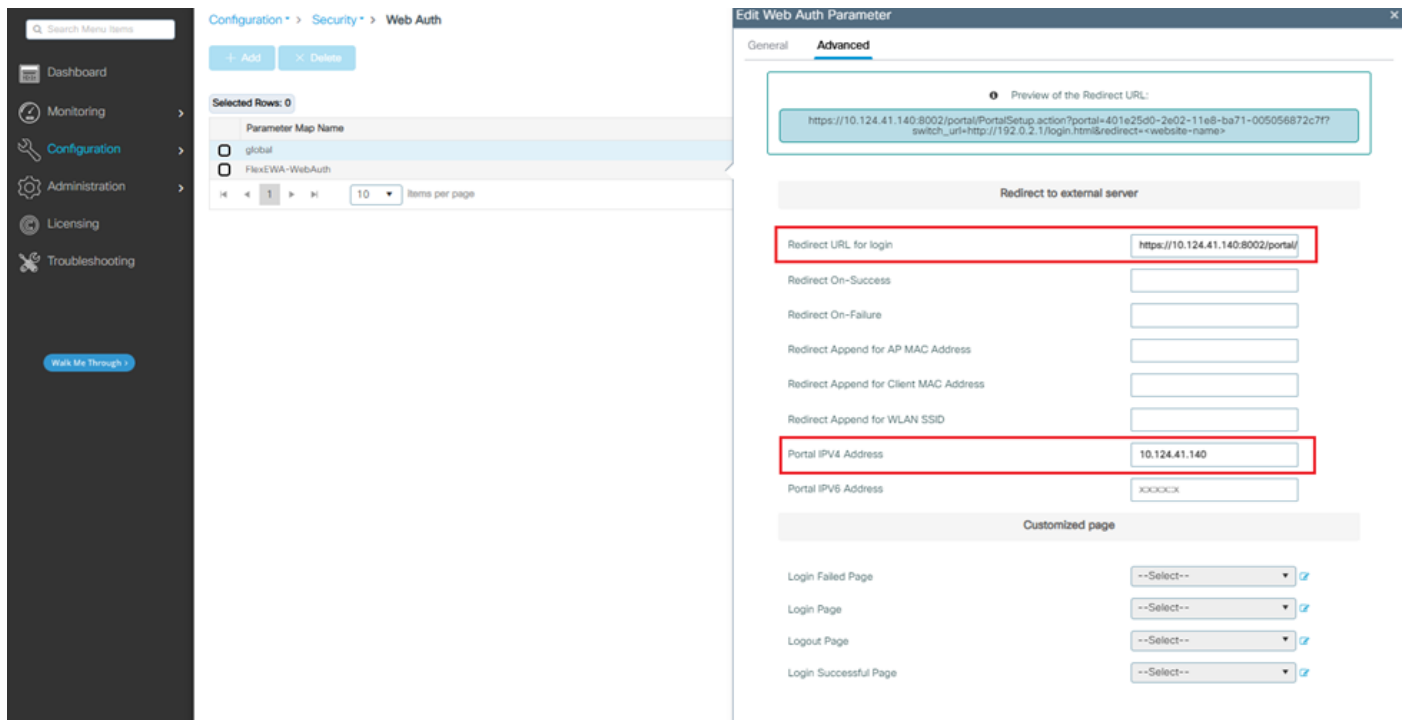


Configuraciones

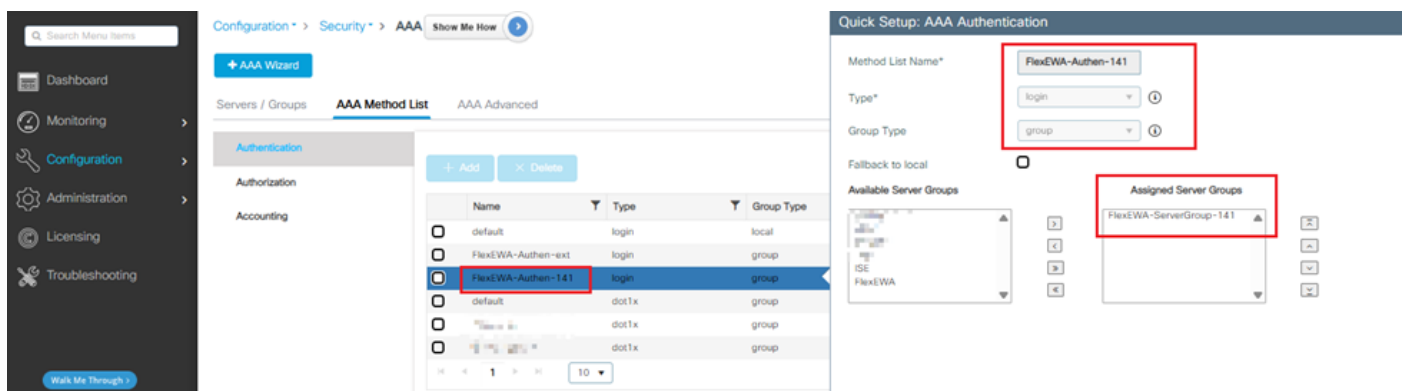
Paso 1. Navegue hasta Configuración > Seguridad > Autenticación Web > +Agregar un mapa de parámetro de autenticación Web.

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

La URL del portal se genera desde ISE (paso 7).



Paso 2. Navegue hasta Configuración > Seguridad > AAA > Lista de Métodos AAA > Autenticación > + Agregar una Lista de Autenticación.



Paso 3. Suponga que el puerto HTTPS es 8002, consulte la ACL WA-sec-10.124.41.140 generada automáticamente para agregar una nueva ACL de autenticación previa.

The screenshot shows the 'Edit ACL' configuration page for 'FlexEWA141-sec-ACL'. The ACL Type is 'IPv4 Extended'. The Rules section shows a table of 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

Paso 4. Verifique la ACL WA-v4-int 10.124.41.141 generada automáticamente.

The screenshot shows the 'Edit ACL' configuration page for 'WA-v4-int-10.124.41.141'. The ACL Type is 'IPv4 Extended'. The Rules section shows a table of rules:

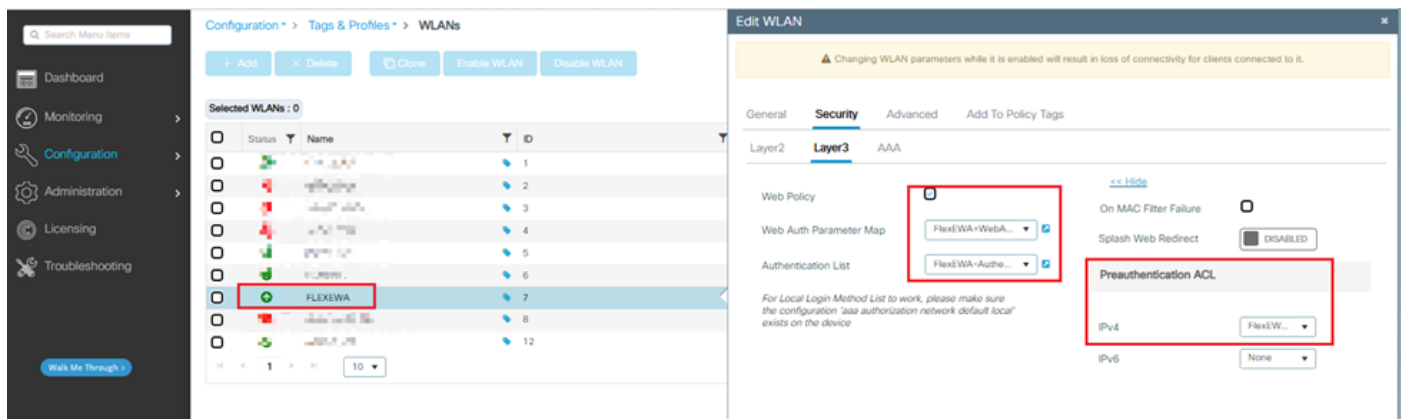
Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
10	deny	any		10.124.41.141		tcp	None	eq www	None	Disabled
20	permit	any		any		tcp	None	eq www	None	Disabled

Paso 5. Aplique las dos ACL a Configuration > Tags&Profiles > Flex > Flex Profile > Policy ACL.

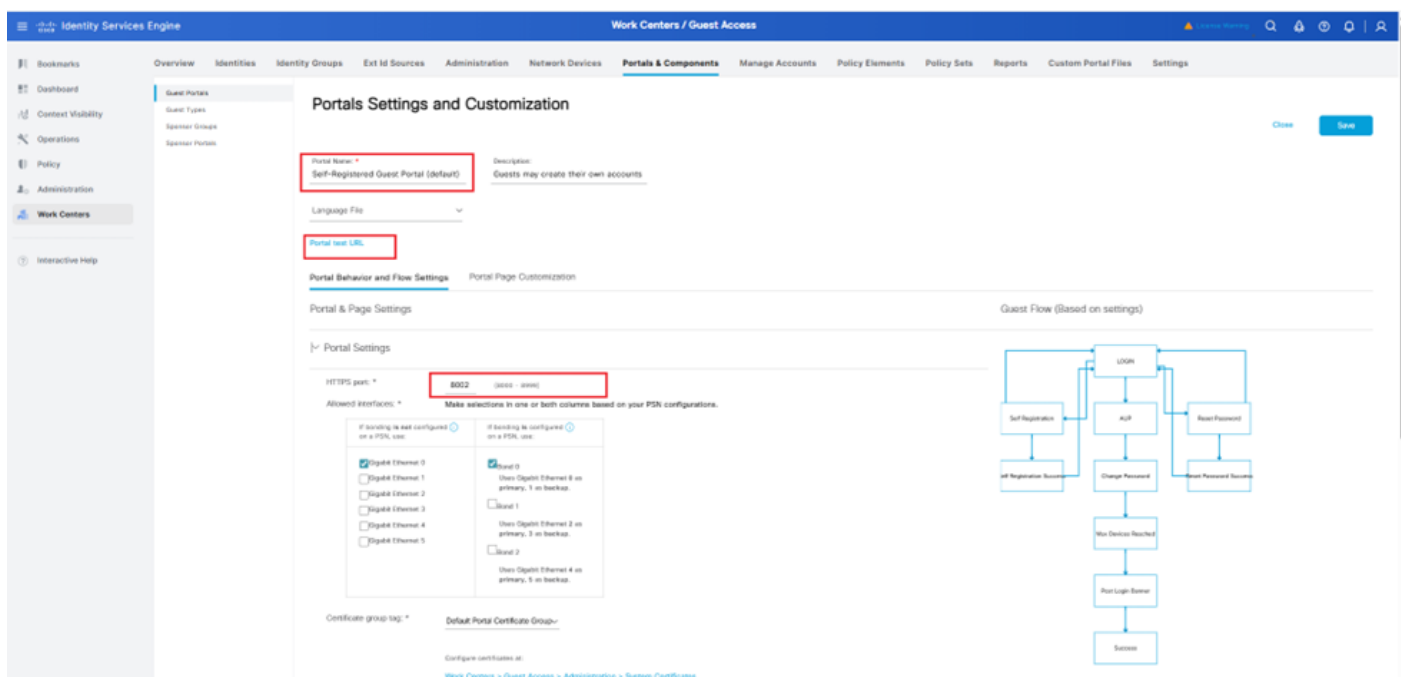
The screenshot shows the 'Edit Flex Profile' configuration page for 'default-flex-profile'. The 'Policy ACL' tab is selected, showing a table of ACLs:

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

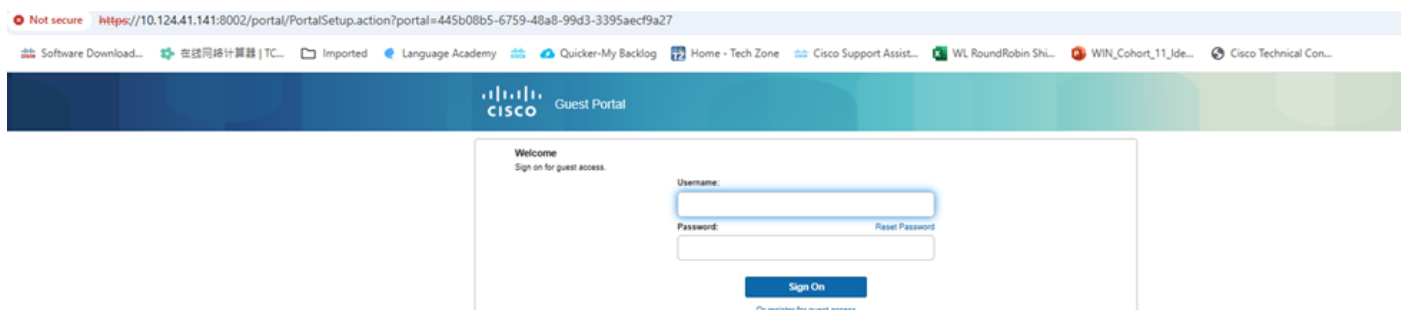
Paso 6. Aplique el recién creado mapa de parámetro de autenticación Web, lista de autenticación y ACL de autenticación previa a WLAN.



Paso 7. Vaya a Centros de trabajo > Portales y componentes > Portales de invitado > Configuración y personalización de portales > Nombre del portal > Portal de invitado de autorregistro (predeterminado) para generar la URL del portal desde ISE.

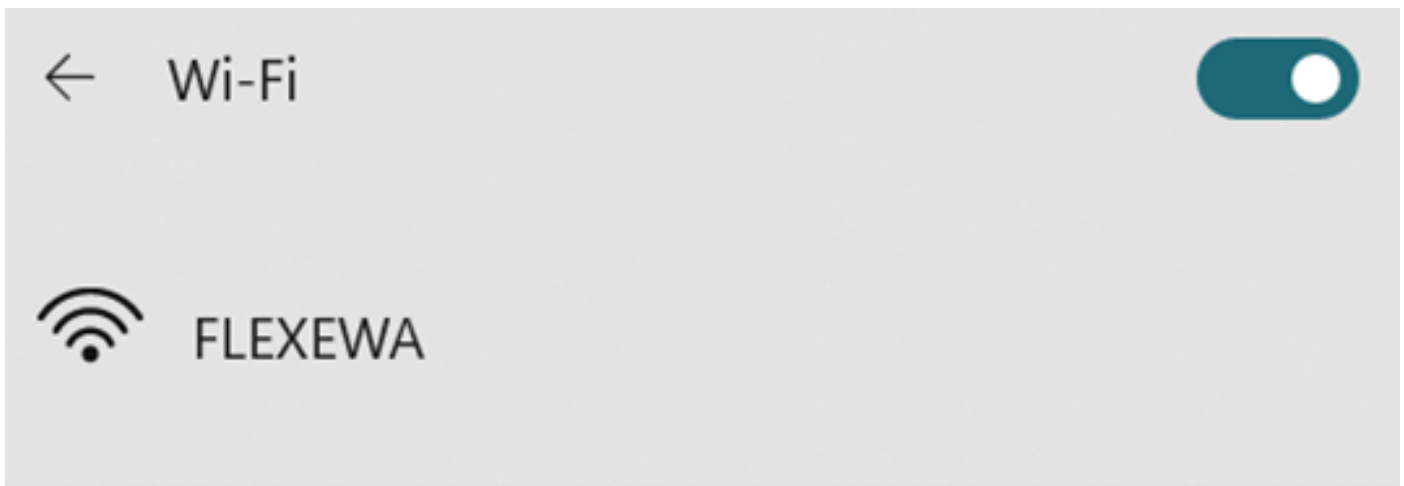


Este portal web listado aparece después de hacer clic en Portal de prueba URL.

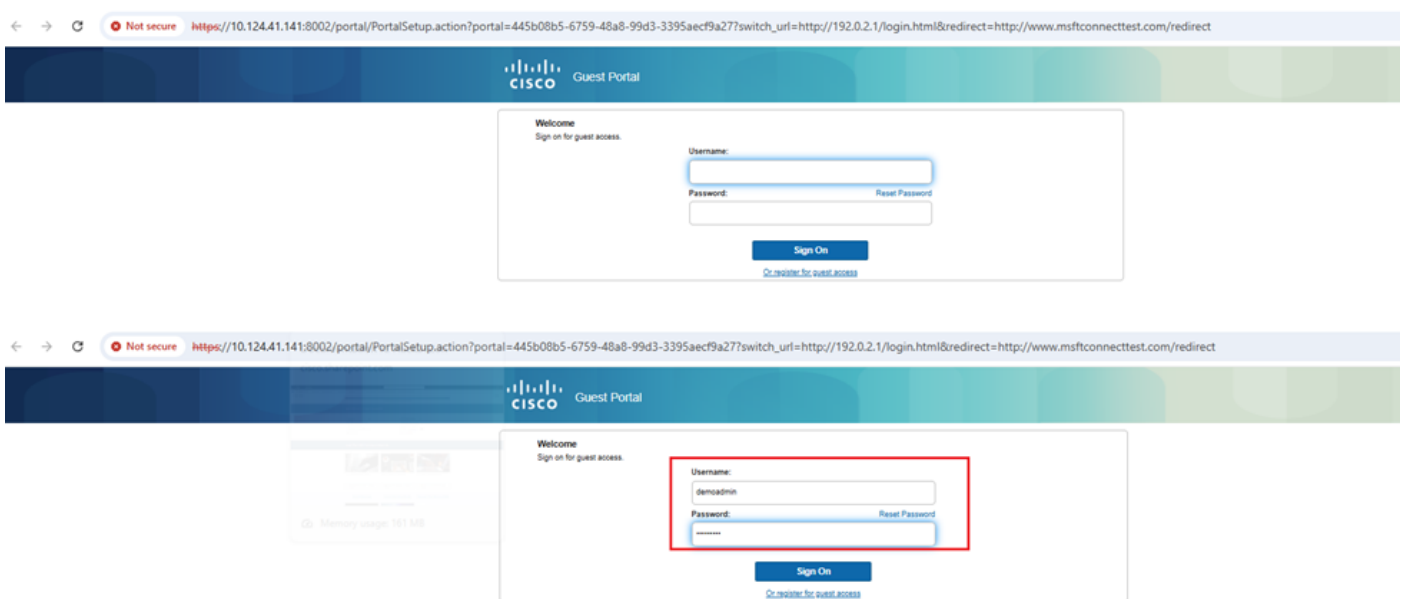


Verificación

Paso 1. Conexión de FLEXEWA SSID.



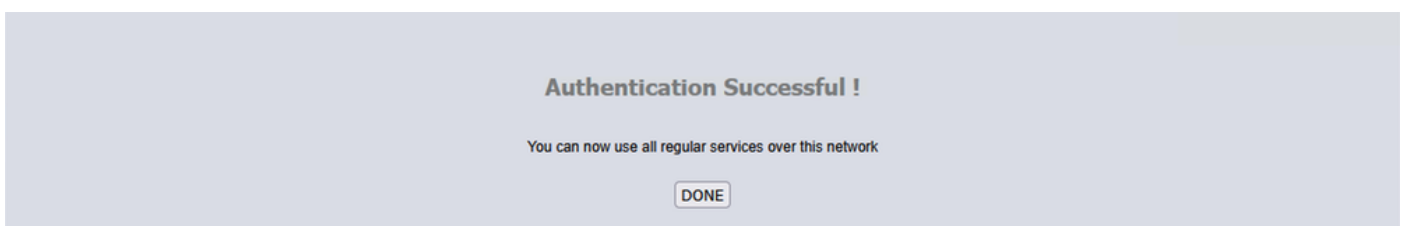
Paso 2. Redirigir al portal e introducir el nombre de usuario y la contraseña.



Paso 3. Aparece el portal de invitados:



Paso 4. Después de hacer clic en Continue, Authentication is Successful:



Ejemplo de Seguimiento de RA de un Intento Exitoso

Ésta es la salida de un intento de conexión correcto desde la perspectiva de seguimiento de Radio Active. Utilícelo como referencia para identificar las fases de la sesión del cliente para los clientes que se conectan a un SSID de autenticación web de capa 3.

Cliente asociado correctamente:

2025/09/09 15:21:48.617769958 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: (nota): MAC: f0b6.1e39.9ce8 Asociación recibida. BSSID c418.fc82.bb0b, WLAN FLEXEWA, ranura 1 AP c418.fc82.bb00, 9178_1, etiqueta de sitio HK, etiqueta de política default-policy-tag, perfil de política default-policy-profile, central de switching, retraso de socket 0ms, BSSID de AP MAC c418.fc82.bb0b

2025/09/09 15:21:48.617813534 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: (depuración): MAC: f0b6.1e39.9ce8 Solicitud de asociación Dot11 recibida. Procesamiento iniciado, SSID: FLEXEWA, Perfil de política: default-policy-profile, nombre de AP: 9178_1, Ap Dirección Mac: c418.fc82.bb00 BSSID ID MAC 0000.0000.0000 wlan ID: 7 RSSI: -30, SNR: 67

2025/09/09 15:21:48.618002570 {wncd_x_R0-0}{1}: [client-orch-state] [17842]: (nota): MAC: f0b6.1e39.9ce8 Transición de estado de cliente: 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 No se pudo obtener el registro dot11

2025/09/09 15:21:48.618301251 {wncd_x_R0-0}{1}: [dot11-validate] [17842]: (información): MAC: f0b6.1e39.9ce8 Dot11 ie valida las velocidades ext/supp. Validación aprobada para tasas admitidas radio_type 2

2025/09/09 15:21:48.618320304 {wncd_x_R0-0}{1}: [dot11-validate] [17842]: (depuración): MAC: f0b6.1e39.9ce8 Dot11 ie validate rsnx, el cliente no utiliza sae, omitir comprobación

2025/09/09 15:21:48.618339230 {wncd_x_R0-0}{1}: [dot11-validate] [17842]: (información): MAC: f0b6.1e39.9ce8 WiFi directo: Dot11 valida el IE P2P. El IE P2P no está presente.

2025/09/09 15:21:48.618598747 {wncd_x_R0-0}{1}: [dot11] [17842]: (depuración): MAC: f0b6.1e39.9ce8 dot11 send association response. Respuesta de asociación de tramas con resp_status_code: 0

2025/09/09 15:21:48.618604733 {wncd_x_R0-0}{1}: [dot11] [17842]: (depuración): MAC: f0b6.1e39.9ce8 Información de capacidad Dot11 byte1 1, byte2: 11

2025/09/09 15:21:48.618696034 {wncd_x_R0-0}{1}: [dot11-frame] [17842]: (información): MAC: f0b6.1e39.9ce8 WiFi directo: omitir compilación Assoc Resp con P2P IE: Política de Wifi Direct desactivada

2025/09/09 15:21:48.618785409 {wncd_x_R0-0}{1}: [dot11] [17842]: (información): MAC: f0b6.1e39.9ce8 dot11 send association response. Enviando respuesta assoc de longitud: 17 con resp_status_code: 0, DOT11_STATUS: DOT11_STATUS_SUCCESS

2025/09/09 15:21:48.618791096 {wncd_x_R0-0}{1}: [dot11] [17842]: (nota): MAC: f0b6.1e39.9ce8 Éxito de asociación. AID 33, Itinerancia = Falso, WGB = Falso, 11r = Falso, 11w = Itinerancia rápida falsa = Falso

2025/09/09 15:21:48.618806595 {wncd_x_R0-0}{1}: [dot11] [17842]: (información): MAC: f0b6.1e39.9ce8 transición de estado DOT11: S_DOT11_INIT -> S_DOT11_ASSOCIATED

2025/09/09 15:21:48.618855282 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: (depuración): MAC: f0b6.1e39.9ce8 La asociación Dot11 de la estación se ha realizado correctamente.

Autenticación de capa 2 omitida:

2025/09/09 15:21:48.618992721 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: (depuración): MAC: f0b6.1e39.9ce8 Iniciando autenticación L2. Bssid en el estado máquina:c418.fc82.bb0b Bssid en la solicitud es:c418.fc82.bb0b

2025/09/09 15:21:48.619006036 {wncd_x_R0-0}{1}: [client-orch-state] [17842]: (nota): MAC: f0b6.1e39.9ce8 Transición de estado de cliente: S_CO_ASSOCIATING -> S_CO_L2_AUTH_IN_PROGRESS

2025/09/09 15:21:48.619093387 {wncd_x_R0-0}{1}: [client-auth] [17842]: (nota): MAC: f0b6.1e39.9ce8 Autenticación L2 iniciada. método WEBAUTH, política VLAN 0, anulación AAA = 0
[...]

2025/09/09 15:21:48.623839337 {wncd_x_R0-0}{1}: [client-auth] [17842]: (información): MAC: f0b6.1e39.9ce8 Transición de estado de interfaz de autenticación de cliente: 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]: (información): [f0b6.1e39.9ce8:capwap_90000008] El tipo de dispositivo para la sesión se detecta como Intel-Device y el nombre antiguo de Intel-Device & Device para la sesión se detecta como INTEL CORPORATE y el antiguo mapa de protocolo 1 de INTEL CORPORATE & Old y el nuevo es 1
2025/09/09 15:21:48.623873529 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (información):

[f0b6.1e39.9ce8:capwap_90000008] auth mgr attr se recibe una notificación de adición/cambio para attr dc-profile-name(1130)

2025/09/09 15:21:48.623911035 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: (depuración): MAC: f0b6.1e39.9ce8 Autenticación L2 de la estación correcta., Autenticación L3: 1

sondeo de ACL:

2025/09/09 15:21:48.620896754 {wncd_x_R0-0}{1}: [webauth-sm] [17842]: (información): [0.0.0.0]Iniciando 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]: (información): [f0b6.1e39.9ce8][0.0.0.0]Param-map utilizado: global

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

2025/09/09 15:21:48.620942683 {wncd_x_R0-0}{1}: [webauth-sess] [17842]: (información): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Crear sesión, Agregar dirección 0.0.0.0

2025/09/09 15:21:48.620946808 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [17842]: (información): [0000.0000.0000:unknown] Recuperado id de zona 0x0 para bssid 12364632846638254486

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

2025/09/09 15:21:48.620962048 {wncd_x_R0-0}{1}: [webauth-state] [17842]: (información): 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]: (información): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Iniciar sesión, estado de reenvío a 0 IF 0x90000008 mac [f0b6.1e39.9ce8]

2025/09/09 15:21:48.620981018 {wncd_x_R0-0}{1}: [webauth-sm] [17842]: (información): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Iniciar sesión, SM iniciar sesiones 5

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

2025/09/09 15:21:48.620991618 {wncd_x_R0-0}{1}: [webauth-state] [17842]: (información): 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]: (información): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Aplicación de ACL de intercepción IPv4 a través de SVM, name: WA-v4-int-10.124.41.141-7, prioridad: 50, IIF-ID: 0

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

2025/09/09 15:21:48.621786262 {wncd_x_R0-0}{1}: [epm] [17842]: (información): La función [f0b6.1e39.9ce8:capwap_90000008] (EPM URL PLUG-IN) se ha iniciado (estado Correcto)

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

2025/09/09 15:21:48.622151544 {wncd_x_R0-0}{1}: [epm] [17842]: (información): La función [f0b6.1e39.9ce8:capwap_90000008] (PLUG-IN de ACL de EPM) se ha iniciado (estado Correcto)

2025/09/09 15:21:48.622187815 {wncd_x_R0-0}{1}: [svm] [17842]: (información): SVM_INFO: La respuesta de epm es SINCRONIZACIÓN con el código devuelto Correcto

2025/09/09 15:21:48.622226011 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (información): [f0b6.1e39.9ce8:capwap_90000008] Se activó la plantilla de eventos de salida (9) en esta sesión, cliente (desconocido) (0)

2025/09/09 15:21:48.622265240 {wncd_x_R0-0}{1}: [webauth-acl] [17842]: (información): capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]Aplicación de ACL de intercepción IPv6 a través de SVM, name: IP-Adm-V6-Int-ACL-global-7, prioridad: 52, IIF-ID: 0

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

2025/09/09 15:21:48.622898831 {wncd_x_R0-0}{1}: [epm] [17842]: (información): La función [f0b6.1e39.9ce8:capwap_90000008] (EPM URL PLUG-IN) se ha iniciado (estado Correcto)

2025/09/09 15:21:48.622932973 {wncd_x_R0-0}{1}: [svm] [17842]: (información): SVM_INFO: La respuesta de epm es SINCRONIZACIÓN con el código devuelto Correcto

2025/09/09 15:21:48.622957784 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (información): [f0b6.1e39.9ce8:capwap_90000008] Se activó la plantilla de eventos de salida (9) en esta sesión, cliente (desconocido) (0)

2025/09/09 15:21:48.623119047 {wncd_x_R0-0}{1}: [dot11] [17842]: (depuración): MAC: f0b6.1e39.9ce8 Dot11 SAE encuentra el progreso de ipsk como 0, no en estado pendiente

2025/09/09 15:21:48.623126095 {wncd_x_R0-0}{1}: [llbridge-main] [17842]: (depuración): MAC: f0b6.1e39.9ce8 El puente local de enlace no está habilitado para este cliente, no comprueba la validez de VLAN

2025/09/09 15:21:48.623205421 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (información): [f0b6.1e39.9ce8:capwap_90000008] Contexto cambiando el estado de 'Inactivo' a 'En ejecución'

2025/09/09 15:21:48.623209350 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (información): [f0b6.1e39.9ce8:capwap_90000008] Método webauth cambiar el estado de 'No ejecutado' a 'En ejecución'

2025/09/09 15:21:48.623572855 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (información): [f0b6.1e39.9ce8:capwap_90000008] SM no puede enviar la plantilla de eventos activada a PRE para 0x8D0000C0

2025/09/09 15:21:48.623680228 {wncd_x_R0-0}{1}: [client-auth] [17842]: (información): MAC:

f0b6.1e39.9ce8 Transición de estado de interfaz de autenticación de cliente:
S_AUTHIF_AWAIT_L2_WEBAUTH_START_RESP -> S_AUTHIF_L2_WEBAUTH_PENDING

Proceso de aprendizaje de IP:

2025/09/09 15:21:51.628124695 {wncd_x_R0-0}{1}: [client-orch-state] [17842]: (nota): MAC: f0b6.1e39.9ce8 Transición de estado de cliente: 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]: (información): MAC: f0b6.1e39.9ce8 Transición de estado de aprendizaje de IP: S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS

2025/09/09 15:21:51.632284534 {wncd_x_R0-0}{1}: [client-auth] [17842]: (información): MAC: f0b6.1e39.9ce8 Transición de estado de interfaz de autenticación de cliente: 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]: (información): RX: DHCP IPv6 de intf capwap_90000008 en vlan 174 Src MAC: f0b6.1e39.9ce8 Dst MAC: 3333 0001 0002 Ipv6 SRC: fe80::3f83:2848:d30:7aea, Ipv6 DST: ff02::1:2, tipo: tipo de mensaje: DHCPV6_MSG_SOLICIT xid: 14443573

2025/09/09 15:21:51.676541447 {wncd_x_R0-0}{1}: [sisf-packet] [17842]: (información): TX: DHCP IPv6 de intf capwap_90000008 en vlan 174 Src MAC: f0b6.1e39.9ce8 Dst MAC: 3333 0001 0002 Ipv6 SRC: fe80::3f83:2848:d30:7aea, Ipv6 DST: ff02::1:2, tipo: tipo de mensaje: DHCPV6_MSG_SOLICIT xid: 14443573

2025/09/09 15:21:51.706187097 {wncd_x_R0-0}{1}: [sisf-packet] [17842]: (información): RX: ARP de la interfaz capwap_90000008 en vlan 174 MAC de origen: f0b6.1e39.9ce8 MAC de destino: ffff.ffff.ffff ARP REQUEST, ARP sender MAC: f0b6.1e39.9ce8 ARP target MAC: 0000.0000.0000 IP de remitente ARP: 169.254.137.222, IP de destino ARP: 169.254.137.222, [...]

2025/09/09 15:21:52.686190945 {wncd_x_R0-0}{1}: [client-iplearn] [17842]: (nota): MAC: f0b6.1e39.9ce8 La IP del cliente se ha aprendido correctamente. Método: IP de DHCP: 10.124.37.251

2025/09/09 15:21:52.686244192 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (información): [f0b6.1e39.9ce8:capwap_90000008] auth mgr attr se recibe una notificación de adición/cambio para attr addr(8)

2025/09/09 15:21:52.686285422 {wncd_x_R0-0}{1}: [webauth-sess] [17842]: (información): 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]: (información): [0000.0000.0000:unknown] Recuperado id de zona 0x0 para bssid 12364632846638254486

2025/09/09 15:21:52.686291647 {wncd_x_R0-0}{1}: [webauth-sess] [17842]: (información): adición de sesión webauth a tabla hash ipv4 para id de vrf 0, id de tabla vrf ipv4 0

2025/09/09 15:21:52.686430038 {wncd_x_R0-0}{1}: [auth-mgr-feat_acct] [17842]: (información): [f0b6.1e39.9ce8:capwap_90000008] Atributo notificado SM Add/Update addr 10.124.37.251

2025/09/09 15:21:52.686456653 {wncd_x_R0-0}{1}: [epm] [17842]: (información): [0000.0000.0000:desconocido] HDL = 0x0 vlan 174 fail count 0 ensuciar_contador 0 is_sucio 0

2025/09/09 15:21:52.686710209 {wncd_x_R0-0}{1}: [client-iplearn] [17842]: (información): MAC:

f0b6.1e39.9ce8 Transición de estado de aprendizaje de IP: S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE

Proceso de redirección y autenticación de capa 3:

2025/09/09 15:21:52.687395906 {wncd_x_R0-0}{1}: [client-auth] [17842]: (nota): MAC: f0b6.1e39.9ce8 Autenticación L3 iniciada. LWA

2025/09/09 15:21:52.687472722 {wncd_x_R0-0}{1}: [client-auth] [17842]: (información): MAC: f0b6.1e39.9ce8 Transición de estado de interfaz de autenticación de cliente: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING

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

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

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

[...]

2025/09/09 15:21:55.663715832 {wncd_x_R0-0}{1}: [webauth-io] [17842]: (información): capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]54129/197 estado de E/S NUEVO -> LECTURA

2025/09/09 15:21:55.664060604 {wncd_x_R0-0}{1}: [webauth-io] [17842]: (información): 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]: (información): capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]GET rcvd cuando está en estado INIT

2025/09/09 15:21:55.664077798 {wncd_x_R0-0}{1}: [webauth-httpd] [17842]: (información): 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]: (información): 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]: (información): capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]POST rcvd cuando está en estado LOGIN

2025/09/09 15:22:32.375197748 {wncd_x_R0-0}{1}: [webauth-acl] [17842]: (información): capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]No aplicar ACL de intercepción IPv4 mediante 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]: (información): [f0b6.1e39.9ce8:capwap_90000008] Provocando plantilla de evento de texto desactivada (11) en esta sesión, cliente (desconocido) (0)

2025/09/09 15:22:32.376262689 {wncd_x_R0-0}{1}: [webauth-acl] [17842]: (información): capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]Anular la aplicación de la ACL de intercepción

IPv6 mediante 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]: (información):
[f0b6.1e39.9ce8:capwap_90000008] Provocando plantilla de evento de texto desactivada (11) en
esta sesión, cliente (desconocido) (0)
2025/09/09 15:22:32.376865998 {wncd_x_R0-0}{1}: [dot11] [17842]: (depuración): MAC:
f0b6.1e39.9ce8 Dot11 SAE encuentra el progreso de ipsk como 0, no en estado pendiente
2025/09/09 15:22:32.376870611 {wncd_x_R0-0}{1}: [llbridge-main] [17842]: (depuración): MAC:
f0b6.1e39.9ce8 El puente local de enlace no está habilitado para este cliente, no comprueba la
validez de VLAN
2025/09/09 15:22:32.376949875 {wncd_x_R0-0}{1}: [auth-mgr] [17842]: (información):
[f0b6.1e39.9ce8:capwap_90000008] Éxito Authc de WebAuth, éxito del evento Auth

Transición al estado RUN:

2025/09/09 15:22:32.379351256 {wncd_x_R0-0}{1}: [client-auth] [17842]: (nota): MAC:
f0b6.1e39.9ce8 ADD MOBILE enviado. Indicadores de estado del cliente: 0x38 BSSID: MAC:
c418.fc82.bb0b capwap IFID: 0x90000008, Agregar móviles enviados: 1
2025/09/09 15:22:32.379583842 {wncd_x_R0-0}{1}: [errmsg] [17842]: (información):
%CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: R0/0: wncd: Entrada de nombre
de usuario (demoadmin) junto con ssid (FLEXEWA) para el dispositivo con MAC: f0b6.1e39.9ce8
en el canal (100)
2025/09/09 15:22:32.379671775 {wncd_x_R0-0}{1}: [aaa-attr-inf] [17842]: (información): [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]: (información): [Atributo
aplicado : timeout 0 28800 (0x7080)]
2025/09/09 15:22:32.379683417 {wncd_x_R0-0}{1}: [aaa-attr-inf] [17842]: (información): [Atributo
aplicado : 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]: (información): MAC:
controlador de estado de ejecución de QoS de cliente f0b6.1e39.9ce8
2025/09/09 15:22:32.379756610 {wncd_x_R0-0}{1}: [rog-proxy-capwap] [17842]: (depuración):
Notificación de estado de EJECUCIÓN del cliente administrado: f0b6.1e39.9ce8
2025/09/09 15:22:32.379810670 {wncd_x_R0-0}{1}: [client-orch-state] [17842]: (nota): MAC:
f0b6.1e39.9ce8 Transición de estado de cliente: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RUN

Información Relacionada

- [Configuración y Troubleshooting de la Autenticación Web Externa en 9800 WLC](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).