

# Configuración y Troubleshooting de la Autenticación Web Externa en 9800 WLC

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configurar parámetros web](#)

[Resumen de la configuración CLI:](#)

[Configuración de los parámetros AAA](#)

[Configurar políticas y etiquetas](#)

[Verificación](#)

[Troubleshoot](#)

[Seguimiento siempre activo](#)

[Depuración condicional y seguimiento activo por radio](#)

[Capturas de paquetes integradas](#)

[Solución de problemas del cliente](#)

[Solución de problemas del explorador HAR](#)

[Captura de paquetes del lado cliente](#)

[Ejemplo de un intento exitoso](#)

---


## Introducción

Este documento describe cómo configurar y resolver problemas de autenticación web externa (EWA) en un Catalyst 9800 Wireless LAN Controller (WLC).

## Prerequisites


Este documento asume que el servidor web está configurado correctamente para permitir la comunicación externa y que la página web está configurada correctamente para enviar todos los parámetros necesarios para que el WLC autentique al usuario y mueva las sesiones del cliente al estado RUN.

---

 Nota: Dado que el acceso a los recursos externos está restringido por el WLC a través de permisos de lista de acceso, todos los scripts, fuentes, imágenes, etc. que se utilizan en la

---

---

 página web deben descargarse y permanecer locales en el servidor web.

---

Los parámetros necesarios para la autenticación de usuario son:

- **buttonClicked:** Este parámetro debe configurarse en el valor "4" para que el WLC detecte la acción como un intento de autenticación.
- **redirectUrl:** el controlador utiliza el valor de este parámetro para dirigir al cliente a un sitio web específico tras una autenticación correcta.
- **err\_flag:** este parámetro se utiliza para indicar algún error, como información incompleta o credenciales incorrectas; en las autenticaciones correctas, se establece en "0".
- **username:** Este parámetro sólo se utiliza para los mapas de parámetro webauth, si el mapa de parámetro se establece en consentir, se puede ignorar. Debe completarse con el nombre de usuario del cliente inalámbrico.
- **password:** Este parámetro sólo se utiliza para los mapas de parámetro webauth, si el mapa de parámetro se establece en consentir, se puede ignorar. Se debe rellenar con la contraseña del cliente inalámbrico.

## Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Desarrollo web de lenguaje de marcado de hipertexto (HTML)
- Funciones inalámbricas de Cisco IOS®-XE
- Herramientas de desarrollador del navegador web

## Componentes Utilizados

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

- C9800-CL WLC Cisco IOS®-XE versión 17.3.3
- Microsoft Windows Server 2012 con funciones de Internet Information Services (IIS)
- Puntos de acceso 2802 y 9117

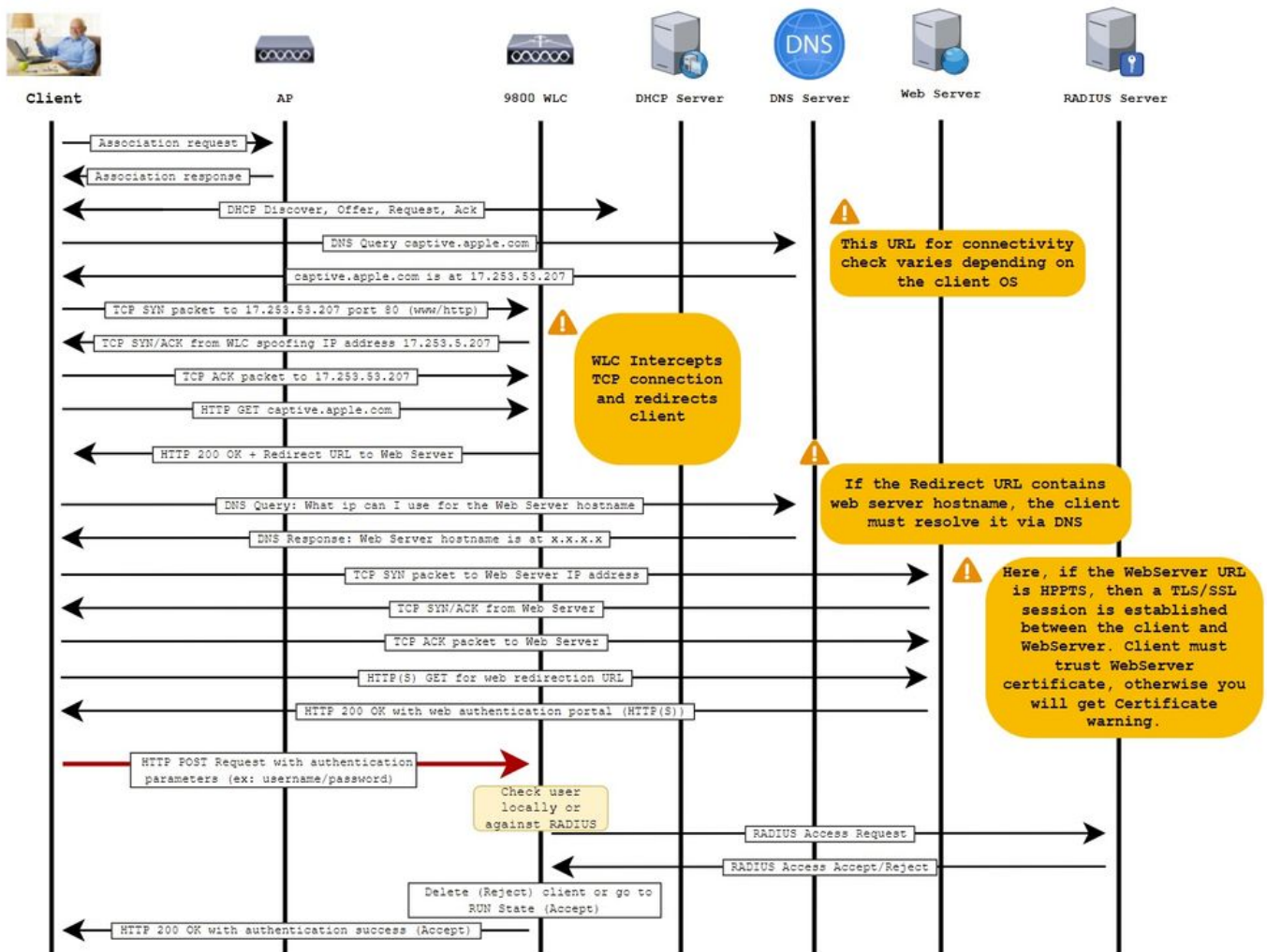
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender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

## Antecedentes

La autenticación web externa aprovecha un portal web alojado fuera del WLC en un servidor web dedicado o servidores multifunción como Identity Services Engine (ISE) que permiten el acceso y la gestión granulares de los componentes web. El protocolo de enlace necesario para incorporar correctamente un cliente a una WLAN de autenticación web externa se representa en la imagen. La imagen enumera las interacciones secuenciales entre el cliente inalámbrico, el WLC, el

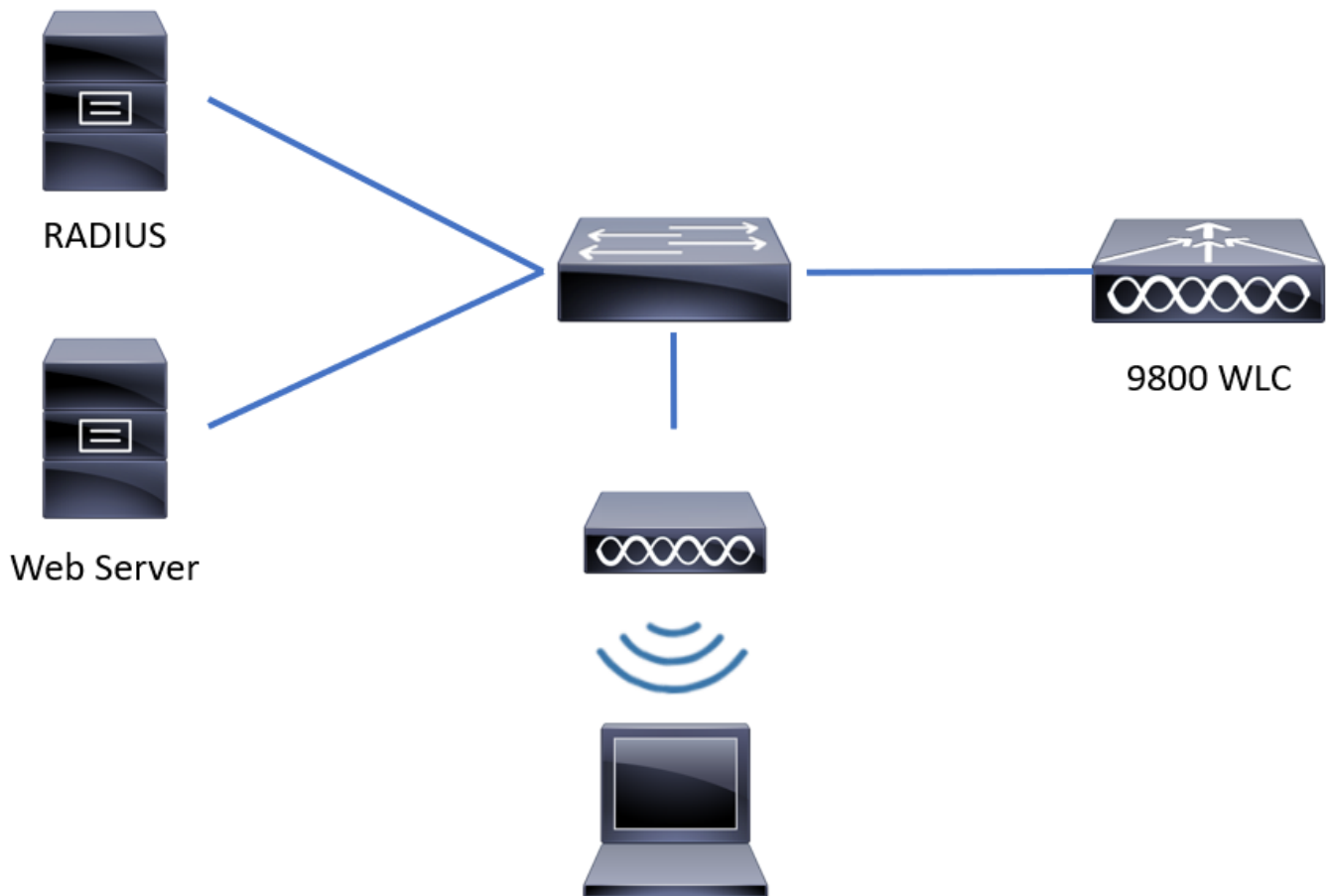
servidor del sistema de nombres de dominio (DNS) que resuelve la ubicación de recursos uniforme (URL) y el servidor web donde el WLC valida las credenciales de usuario localmente. Este flujo de trabajo resulta útil para solucionar cualquier problema de error.

**Nota:** Antes de la llamada HTTP POST del cliente al WLC, si se habilita la autenticación web segura en el mapa de parámetros y si el WLC no tiene un punto de confianza firmado por una autoridad de certificación de confianza, se muestra una alerta de seguridad en el navegador. El cliente necesita saltarse esta advertencia y aceptar el reenvío del formulario para que el controlador coloque las sesiones del cliente en estado RUN.



## Configurar


### Diagrama de la red



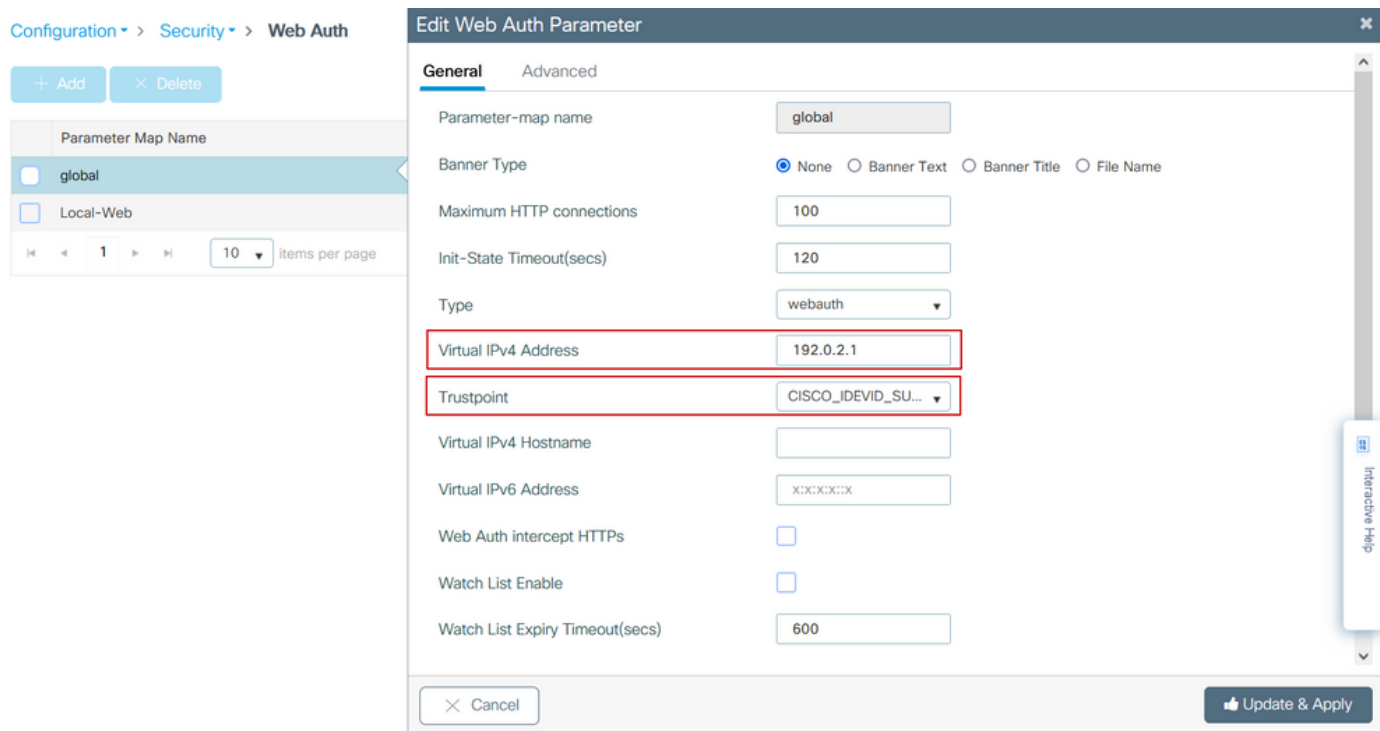
## Configurar parámetros web

Paso 1. Navegue hasta Configuration > Security > Web Auth y elija el mapa de parámetro global. Verifique que Virtual IPv4 Address y Trustpoint estén configurados para proporcionar capacidades de redirección adecuadas.

---

 Nota: De forma predeterminada, los navegadores utilizan un sitio web HTTP para iniciar el proceso de redirección; si se necesita la redirección HTTPS, se debe comprobar Web Auth intercept HTTPs; sin embargo, esta configuración no se recomienda, ya que aumenta el uso de la CPU.

---



## Configuración de CLI:

```
<#root>
```

```
9800#
```

```
configure terminal
```

```
9800(config)#
```

```
parameter-map type webauth global
```

```
9800(config-params-parameter-map)#
```

```
virtual-ip ipv4 192.0.2.1
```

```
9800(config-params-parameter-map)#
```

```
trustpoint CISCO_IDEVID_SUDI
```

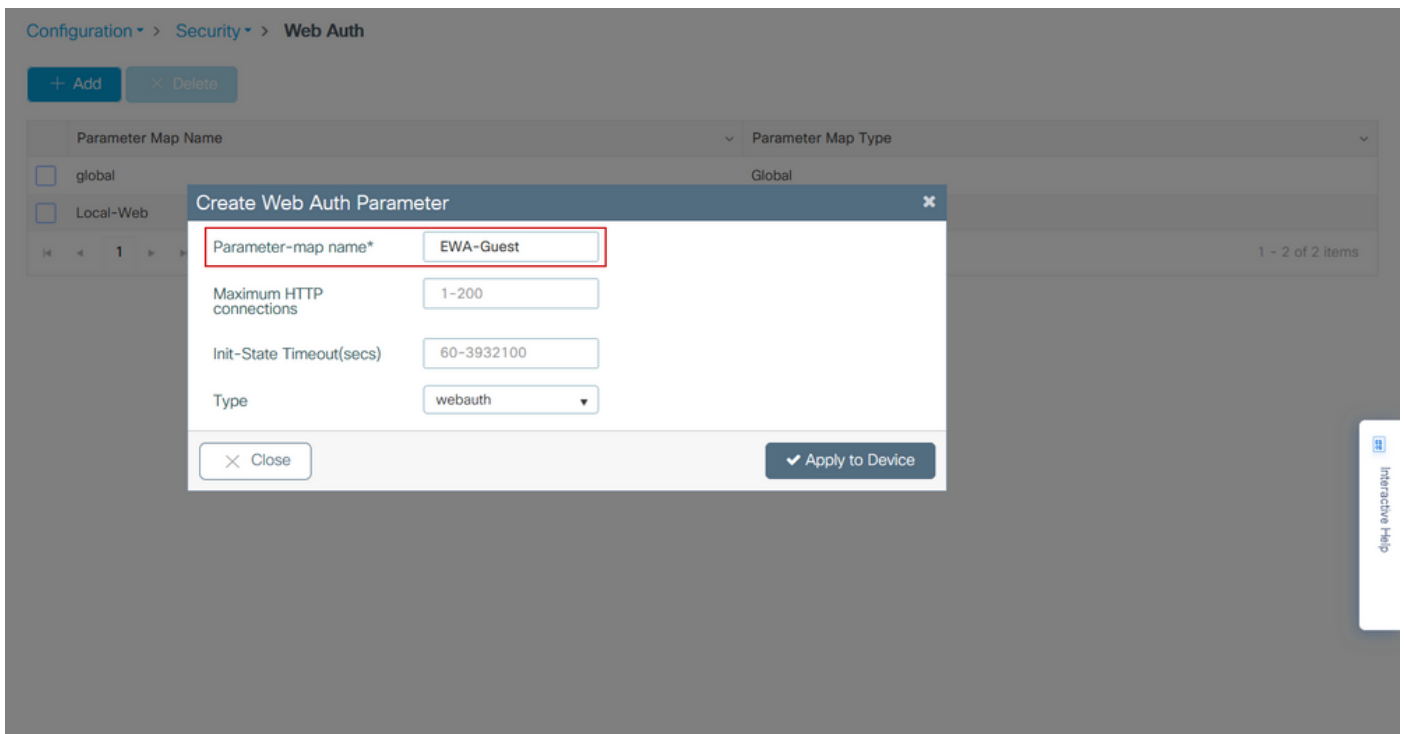
```
9800(config-params-parameter-map)#
```

```
secure-webauth-disable
```

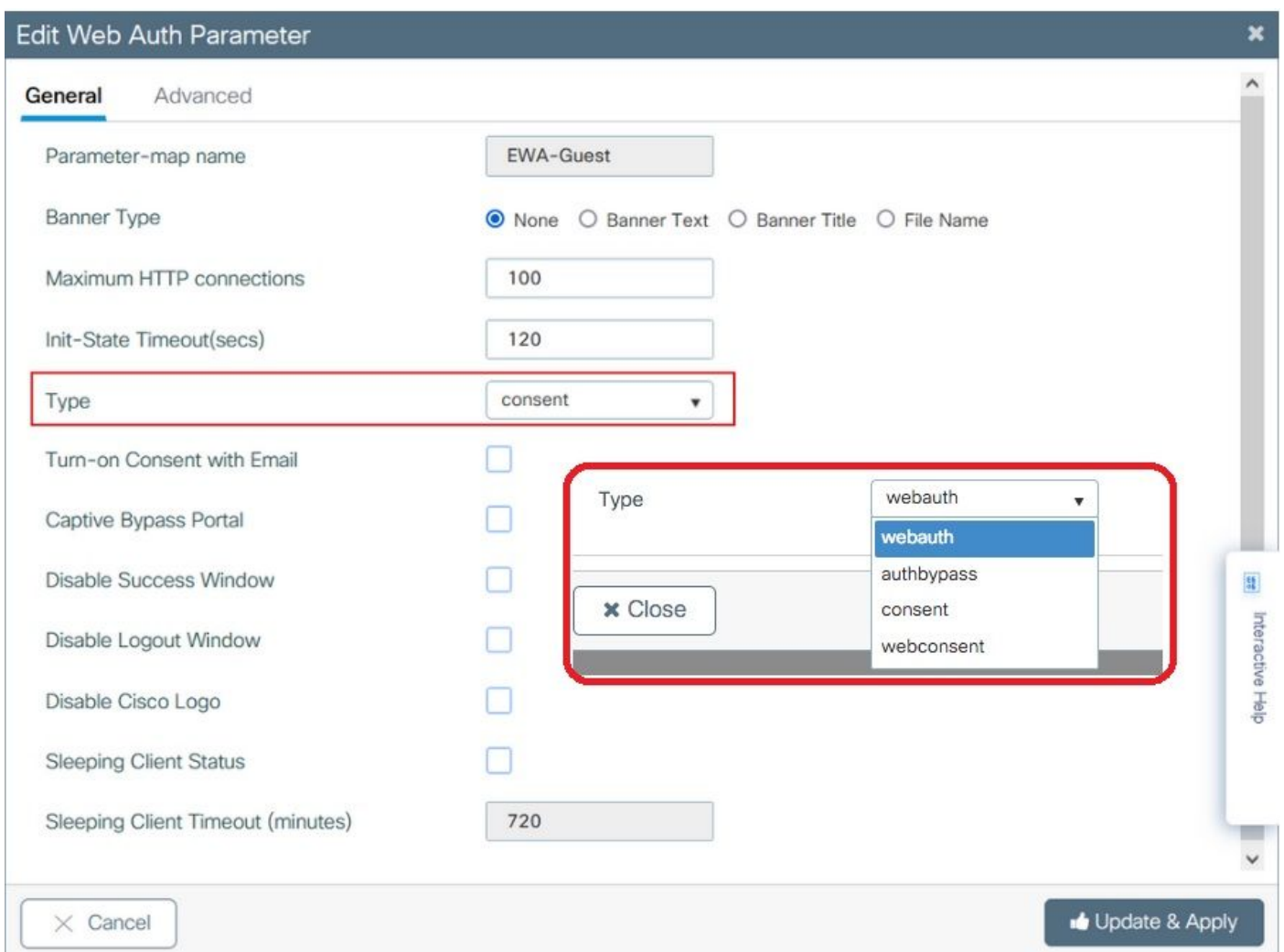
```
9800(config-params-parameter-map)#
```

```
webauth-http-enable
```

Paso 2. Seleccione + Add y configure un nombre para el nuevo mapa de parámetro que apunta al servidor externo. Opcionalmente, configure el número máximo de fallas de autenticación HTTP antes de que el cliente sea excluido y el tiempo (en segundos) que un cliente puede permanecer en el estado de autenticación web.



Paso 3. Seleccione el mapa de parámetro recién creado, en la ficha General, configure el tipo de autenticación en la lista desplegable Tipo.



- Parameter-map name = Nombre asignado al mapa de parámetro WebAuth
- Número máximo de conexiones HTTP = número de errores de autenticación antes de que se excluya al cliente
- Tiempo de espera de estado inicial (segundos) = Segundos que un cliente puede estar en estado de autenticación web
- Tipo = Tipo de autenticación Web

webauth	authbypass	asentimiento	consentimiento web
<p>Username: <input type="text"/></p> <p>Password: <input type="password"/></p> <p><input type="button" value="OK"/></p>	<p>El cliente se conecta al SSID y obtiene una dirección IP, luego el 9800 WLC comprueba si la dirección MAC se le permite introducir el red, si la respuesta es sí, se mueve al estado RUN, si no lo es no se le permite unirse.</p> <p>(No recurre a la autenticación web)</p>	<p>banner1</p> <p><input checked="" type="radio"/> Accept</p> <p><input type="radio"/> Don't Accept</p> <p><input type="button" value="OK"/></p>	<p>banner login</p> <p><input checked="" type="radio"/> Accept</p> <p><input type="radio"/> Don't Accept</p> <p>Username: <input type="text"/></p> <p>Password: <input type="password"/></p> <p><input type="button" value="OK"/></p>

Paso 4. En la ficha Advanced, configure Redirect para el inicio de sesión y la dirección IPV4 del portal con la dirección URL e IP del sitio del servidor específico, respectivamente.

Edit Web Auth Parameter
✕

General

Advanced

Redirect to external server

Redirect for log-in	http://172.16.80.8/w
Redirect On-Success	
Redirect On-Failure	
Redirect Append for AP MAC Address	ap_mac
Redirect Append for Client MAC Address	client_mac
Redirect Append for WLAN SSID	ssid
Portal IPv4 Address	172.16.80.8
Portal IPv6 Address	x::x::x::x
Express WiFi Key Type	--- Select --- ▾

Customized page

Login Failed Page	
-------------------	--

✕ Cancel

👍 Update & Apply

? Interactive Help

Configuración CLI para los pasos 2, 3 y 4:

```

<#root>
9800(config)#
parameter-map type webauth EWA-Guest
9800(config-params-parameter-map)#
type consent
9800(config-params-parameter-map)#
redirect for-login http://172.16.80.8/webauth/login.html
9800(config-params-parameter-map)#
redirect portal ipv4 172.16.80.8
  
```

Paso 5. (Opcional) El WLC puede enviar los parámetros adicionales a través de la cadena de consulta. Esto suele ser necesario para que 9800 sea compatible con portales externos de terceros. Los campos "Redirigir Append para dirección MAC de AP", "Redirigir Append para dirección MAC de cliente" y "Redirigir Append para SSID de WLAN" permiten que se agreguen



parámetros adicionales a la ACL de redirección con un nombre personalizado. Seleccione el mapa de parámetro recién creado y navegue hasta la pestaña Advanced, configure el nombre de los parámetros necesarios. Los parámetros disponibles son:

- Dirección MAC del punto de acceso (en formato aa:bb:cc:dd:ee:ff)
- Dirección MAC del cliente (en formato aa:bb:cc:dd:ee:ff)
- Nombre de SSID

**Edit Web Auth Parameter**

General **Advanced**

**Redirect to external server**

Redirect for log-in	<input type="text" value="http://172.16.80.8/we"/>
Redirect On-Success	<input type="text"/>
Redirect On-Failure	<input type="text"/>
Redirect Append for AP MAC Address	<input type="text" value="ap_mac"/>
Redirect Append for Client MAC Address	<input type="text" value="client_mac"/>
Redirect Append for WLAN SSID	<input type="text" value="ssid"/>
Portal IPV4 Address	<input type="text" value="172.16.80.8"/>
Portal IPV6 Address	<input type="text" value="x:x:x:x:x"/>
Express WiFi Key Type	<input type="text" value="--- Select ---"/>

**Customized page**

Login Failed Page	<input type="text"/>	
Login Page	<input type="text"/>	
Logout Page	<input type="text"/>	
Login Successful Page	<input type="text"/>	

Activate Windows  
Go to System in Control Panel to activate Windows.

Interactive Help

Configuración de CLI:

```
<#root>
```

```
9800(config)#
```

```
parameter-map type webauth EWA-Guest
```

```
9800(config-params-parameter-map)#
```

```
redirect append ap-mac tag ap_mac
```

```
9800(config-params-parameter-map)#
```

```
redirect append wlan-ssid tag ssid
```


```
9800(config-params-parameter-map)#
```

```
redirect append client-mac tag client_mac
```

Para este ejemplo, la URL de redirección enviada al cliente da como resultado:


```
http://172.16.80.8/webauth/consent.html?switch_url=http://192.0.2.1/login.html&ap_mac=&ssid=&client_mac=
```

---

 Nota: Cuando agrega la información de Dirección IPV4 del portal, agrega automáticamente una ACL que permite el tráfico HTTP y HTTPS de los clientes inalámbricos al servidor de autenticación web externo, por lo que no tiene que configurar ninguna ACL adicional previa a la autenticación. En caso de que desee permitir varias direcciones IP o URL, la única opción es configurar un filtro de URL para que se permita cualquier URL que coincida con una dirección IP antes de que se lleve a cabo la autenticación. No es posible agregar estáticamente más de una dirección IP del portal a menos que utilice filtros de URL.

---

---

 Nota: El mapa de parámetros global es el único en el que puede definir la dirección IPv4 e IPv6 virtual, los HTTP de intercepción de Webauth, el portal de omisión cautivo, la activación de la lista de observación y la configuración del tiempo de espera de vencimiento de la lista de observación.

---

Resumen de la configuración CLI:

Servidor web local

```
parameter-map type webauth <web-parameter-map-name>  
type { webauth | authbypass | consent | webconsent }  
timeout init-state sec 300  
banner text ^Cbanner login^C
```

## Servidor web externo

```
parameter-map type webauth <web-parameter-map-name>
type webauth
timeout init-state sec 300
redirect for-login <URL-for-webauth>
redirect portal ipv4 <external-server's-IP>
max-http-conns 10
```

## Configuración de los parámetros AAA

Esta sección de configuración sólo es necesaria para los mapas de parámetros que se configuran para el tipo de autenticación webauth o webaccept.

Paso 1. Vaya a Configuration > Security > AAA, luego seleccione AAA Method List. Configure una nueva lista de métodos, seleccione + Add y rellene los detalles de la lista; asegúrese de que Type esté configurado como "login" como se muestra en la imagen.

Configuration > Security > AAA Show Me How >

+ AAA Wizard

Servers / Groups **AAA Method List** AAA Advanced

Authentication  
Authorization  
Accounting

+ Add × Delete

	Name	Type	Group Type	Group1	Group2	Group3	Group4
<input type="checkbox"/>	default	dot1x	group	radius	N/A	N/A	N/A
<input type="checkbox"/>	alziab-rad-auth	dot1x	group	alziab-rad	N/A	N/A	N/A

10 items per page 1 - 2 of 2 items

Quick Setup: AAA Authentication ✕

Method List Name\*

Type\*  ⓘ

Group Type  ⓘ

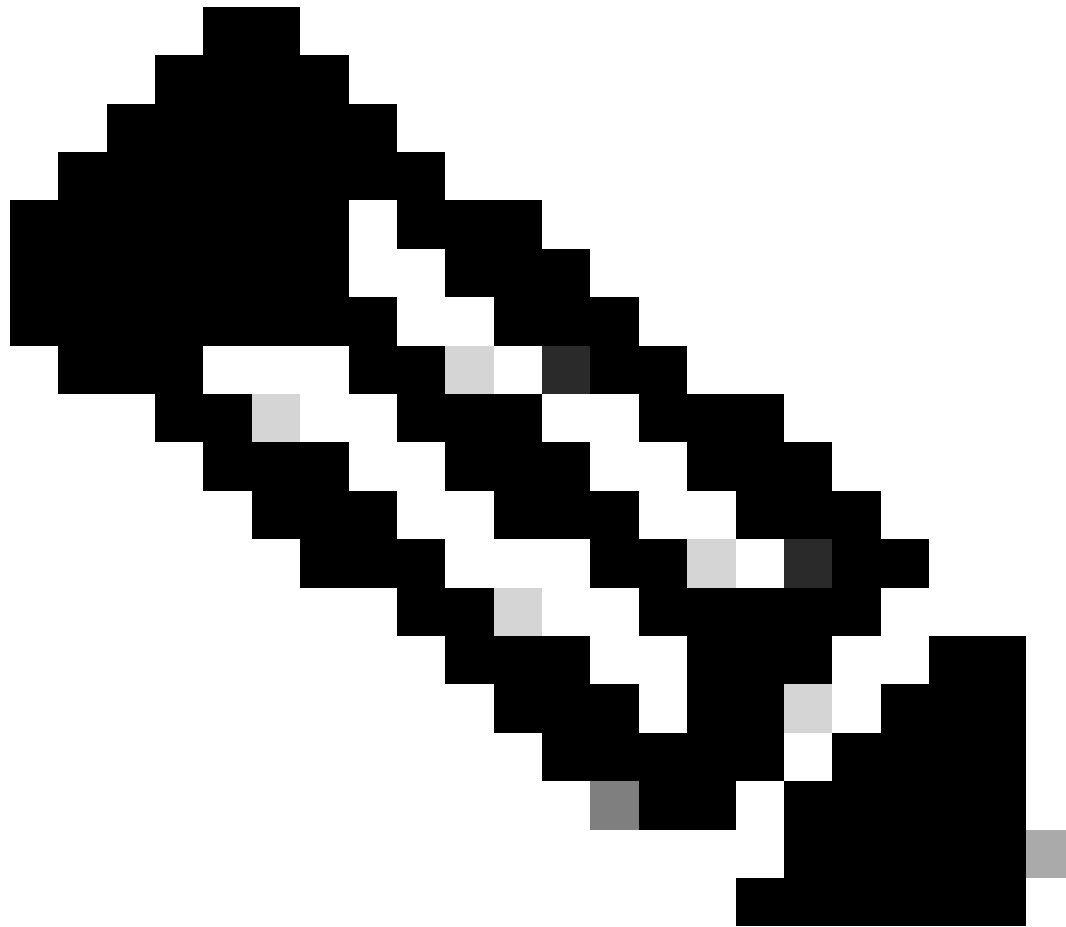
Available Server Groups

- radius
- ldap
- tacacs+
- alzlab-rad
- fgalvezm-group

Assigned Server Groups

Cancel Apply to Device

Paso 2. Seleccione Authorization y, a continuación, seleccione + Add para crear una nueva lista de métodos. Asígnele el nombre predeterminado con Type as network (Tipo como red), como se muestra en la imagen.



Nota: dado que el controlador lo anuncia durante la [configuración de seguridad de capa 3 de WLAN](#): Para que la lista de métodos de inicio de sesión local funcione, asegúrese de que la configuración 'aaa authorization network default local' exista en el dispositivo. Esto significa que la lista de métodos de autorización con el nombre default debe ser definida para configurar la autenticación web local correctamente. En esta sección, se configura esta lista de métodos de autorización en particular.

---

Configuration > Security > AAA Show Me How >

[+ AAA Wizard](#)

Servers / Groups **AAA Method List** AAA Advanced

Authentication

**Authorization**

Accounting

[+ Add](#) [x Delete](#)

Name	Type	Group Type	Group1	Group2	Group3	Group4
alzlab-rad-authz	network	group	alzlab-rad	N/A	N/A	N/A
wcm_loc_serv_cert	credential-download	local	N/A	N/A	N/A	N/A

10 items per page 1 - 2 of 2 items

### Quick Setup: AAA Authorization

Method List Name\*

Type\*  ⓘ

Group Type  ⓘ

Authenticated

Available Server Groups

- radius
- ldap
- tacacs+
- alzlab-rad
- fgalvezm-group

Assigned Server Groups


[Cancel](#) [Apply to Device](#)

Configuración CLI para los pasos 1 y 2:

```
<#root>
9800(config)#
aaa new-model

9800(config)#
aaa authentication login local-auth local

9800(config)#
aaa authorization network default local
```

 Nota: Si es necesaria la autenticación RADIUS externa, lea estas instrucciones relacionadas con la configuración del servidor RADIUS en WLC 9800: [Configuración AAA en WLC 9800](#). Asegúrese de que la lista de métodos de autenticación tenga "login" configurado como tipo en lugar de dot1x.

Paso 3. Vaya a Configuration > Security > Guest User. Seleccione + Agregar y configure los detalles de la cuenta de usuario invitado.

### Add Guest User

General	Lifetime
User Name* guestuser	Years* 1
Password* ●●●●●●●● <input type="checkbox"/> Generate password	Months* 0
Confirm Password* ●●●●●●●●	Days* 0
Description* WebAuth user	Hours* 0
AAA Attribute list Enter/Select	Mins* 0
No. of Simultaneous User Logins* 0 <i>Enter 0 for unlimited users</i>	

Configuración de CLI:

```
<#root>
```

```
9800(config)#
```

```
user-name guestuser
```

```
9800(config-user-name)#
```

```
description "WebAuth user"
```

```
9800(config-user-name)#
```

```
password 0 <password>
```

```
9800(config-user-name)#
```

```
type network-user description "WebAuth user" guest-user lifetime year 1
```

If permanent users are needed then use this command:

```
9800(config)#
```

```
username guestuserperm privilege 0 secret 0 <password>
```

Paso 4. (Opcional) Según la definición del mapa de parámetros, se crean automáticamente un par de listas de control de acceso (ACL). Estas ACL se utilizan para definir qué tráfico desencadena una redirección al servidor web y por qué tráfico se permite el paso. Si existen requisitos específicos, como varias direcciones IP o filtros de URL del servidor web, navegue hasta Configuración > Seguridad > ACL, seleccione + Agregar y defina las reglas necesarias; las sentencias permit se redirigen mientras que las sentencias deny definen el tráfico que pasa a través.

Las reglas de ACL creadas automáticamente son:

```
<#root>
```

```
alz-9800#
```

```
show ip access-list
```

```
Extended IP access list WA-sec-172.16.80.8
```

```
10 permit tcp any host 172.16.80.8 eq www
```

```
20 permit tcp any host 172.16.80.8 eq 443
```

```
30 permit tcp host 172.16.80.8 eq www any
```

```
40 permit tcp host 172.16.80.8 eq 443 any
```

```
50 permit tcp any any eq domain
```

```
60 permit udp any any eq domain
```

```
70 permit udp any any eq bootpc
```

```
80 permit udp any any eq bootps
```

```
90 deny ip any any (1288 matches)
```

```
Extended IP access list WA-v4-int-172.16.80.8
```

```
10 deny tcp any host 172.16.80.8 eq www
```

```
20 deny tcp any host 172.16.80.8 eq 443
```

```
30 permit tcp any any eq www
```

```
40 permit tcp any host 192.0.2.1 eq 443
```

## Configurar políticas y etiquetas

Paso 1. Vaya a Configuration > Tags & Profiles > WLANs, seleccione + Add para crear una nueva WLAN. Defina el perfil y el nombre de SSID, y el Estado en la pestaña General.



### Add WLAN ✕

**General**   Security   Advanced

Profile Name*	<input type="text" value="EWA-Guest"/>	Radio Policy	<input type="text" value="All"/>
SSID*	<input type="text" value="EWA-Guest"/>	Broadcast SSID	<input checked="" type="checkbox"/> ENABLED
WLAN ID*	<input type="text" value="4"/>		
Status	<input checked="" type="checkbox"/> ENABLED		

Paso 2. Seleccione la pestaña Seguridad y establezca la autenticación de Capa 2 en Ninguno si no necesita ningún mecanismo de encriptación por aire. En la ficha Layer 3 (Capa 3), active la casilla Web Policy (Directiva web), seleccione el mapa de parámetros en el menú desplegable y elija la lista de autenticación en el menú desplegable. Opcionalmente, si se definió una ACL personalizada anteriormente, seleccione Show Advanced Settings y seleccione la ACL apropiada en el menú desplegable.

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

**Layer2** Layer3 AAA

Layer 2 Security Mode

MAC Filtering

OWE Transition Mode

Lobby Admin Access

Fast Transition

Over the DS

Reassociation Timeout

Interactive Help

Activate Windows

Go to System in Control Panel to activate Windows

Edit WLAN ✕

**⚠** Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 **Layer3** AAA

Web Policy  [Show Advanced Settings >>>](#)

Web Auth Parameter Map EWA-Guest ▼

Authentication List local-auth ▼ ⓘ

*For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device*

↶ Cancel Activate Windows Update & Apply to Device

[Interactive Help](#)

## Configuraciones CLI:

```
<#root>
```

```
9800(config)#
```

```
wlan EWA-Guest 4 EWA-Guest
```

```
9800(config-wlan)#
```

```
no security ft adaptive
```

```
9800(config-wlan)#
```

```
no security wpa
```

```
9800(config-wlan)#
```

```
no security wpa wpa2
```

```
9800(config-wlan)#
```

```
no security wpa wpa2 ciphers aes
```

```
9800(config-wlan)#
```

```
no security wpa akm dot1x
```

```
9800(config-wlan)#
```

```
security web-auth
```

```
9800(config-wlan)#
```

```
security web-auth authentication-list local-auth
```

```
9800(config-wlan)#
```

```
security web-auth parameter-map EWA-Guest
```

```
9800(config-wlan)#
```

```
no shutdown
```

Paso 3. Vaya a Configuration > Tags & Profiles > Policy y seleccione + Add. Defina el nombre y el estado de la política; asegúrese de que la configuración central en la política de conmutación WLAN esté habilitada para los AP del modo local. En la pestaña Access Policies, seleccione la VLAN correcta del menú desplegable VLAN/VLAN Group como se muestra en la imagen.

## Add Policy Profile



### General

Access Policies

QOS and AVC

Mobility

Advanced

Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name\*

Guest-Policy

Description

Policy for guest access

Status

ENABLED

Passive Client

DISABLED

Encrypted Traffic Analytics

DISABLED

### CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

2-65519

### WLAN Switching Policy

Central Switching

ENABLED

Central Authentication

ENABLED

Central DHCP

ENABLED

Central Association

ENABLED

Flex NAT/PAT

DISABLED

Cancel

Apply to Device

Add Policy Profile ✕

General
Access Policies
QOS and AVC
Mobility
Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

**WLAN Local Profiling**

Global State of Device Classification ⓘ

Local Subscriber Policy Name

**VLAN**

VLAN/VLAN Group

Multicast VLAN

**WLAN ACL**

IPv4 ACL

IPv6 ACL

**URL Filters**

Pre Auth

Post Auth

↶ Cancel

📄 Apply to Device

Configuración de CLI:

```

<#root>
9800(config)#
wireless profile policy Guest-Policy

9800(config-wireless-policy)#
description "Policy for guest access"

9800(config-wireless-policy)#
vlan VLAN2621

9800(config-wireless-policy)#
no shutdown

```

Paso 4. Vaya a Configuration > Tags & Profiles > Tags, dentro de la pestaña Policy, seleccione + Add. Defina un nombre de etiqueta y, a continuación, en WLAN-POLICY Maps, seleccione + Add y agregue el perfil de política y WLAN creado anteriormente.

✕

## Add Policy Tag

Name\*

Description

▼ **WLAN-POLICY Maps: 0**

+ Add
✕ Delete

WLAN Profile	Policy Profile
<div style="display: flex; justify-content: space-between; align-items: center;"> <span>◀ 0 ▶</span> <span>10 items per page</span> <span>No items to display</span> </div>	

Map WLAN and Policy

WLAN Profile\*  Policy Profile\*

✕
✓

➤ **RLAN-POLICY Maps: 0**

↶ Cancel

📄 Apply to Device

Configuración de CLI:

```
<#root>
```

```
9800(config)#
```

```
wireless tag policy EWA-Tag
```

```
9800(config-policy-tag)#
```

```
wlan EWA-Guest policy Guest-Policy
```

Paso 5. Navegue hasta Configuration > Wireless > Access Points y seleccione el AP que se utiliza para difundir este SSID. En el menú Edit AP, seleccione la etiqueta recién creada en el menú desplegable Policy.

Edit AP
✕

<b>AP Name*</b>	C9117AXI-lobby	Primary Software Version	17.3.3.26
Location*	default location	Predownloaded Status	N/A
Base Radio MAC	0cd0.f897.ae60	Predownloaded Version	N/A
Ethernet MAC	0cd0.f894.5c34	Next Retry Time	N/A
Admin Status	<input type="checkbox"/> DISABLED	Boot Version	1.1.2.4
AP Mode	Local ▼	IOS Version	17.3.3.26
Operation Status	Registered	Mini IOS Version	0.0.0.0
Fabric Status	Disabled	<b>IP Config</b>	
LED State	ENABLED <input checked="" type="checkbox"/>	CAPWAP Preferred Mode	IPv4
LED Brightness Level	8 ▼	DHCP IPv4 Address	172.16.10.133
<b>Tags</b>		Static IP (IPv4/IPv6)	<input type="checkbox"/>
⚠ Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.			
Policy	EWA-Tag ▼	<b>Time Statistics</b>	
Site	default-site-tag ▼	Up Time	0 days 0 hrs 19 mins 13 secs
...	default-site-tag ▼	Controller Association Latency	2 mins 7 secs

↶ Cancel
Activate Windows  
Go to System in Control Panel to activate Windows
Update & Apply to Device

Interactive Help

Si es necesario etiquetar varios AP al mismo tiempo, hay dos opciones disponibles:

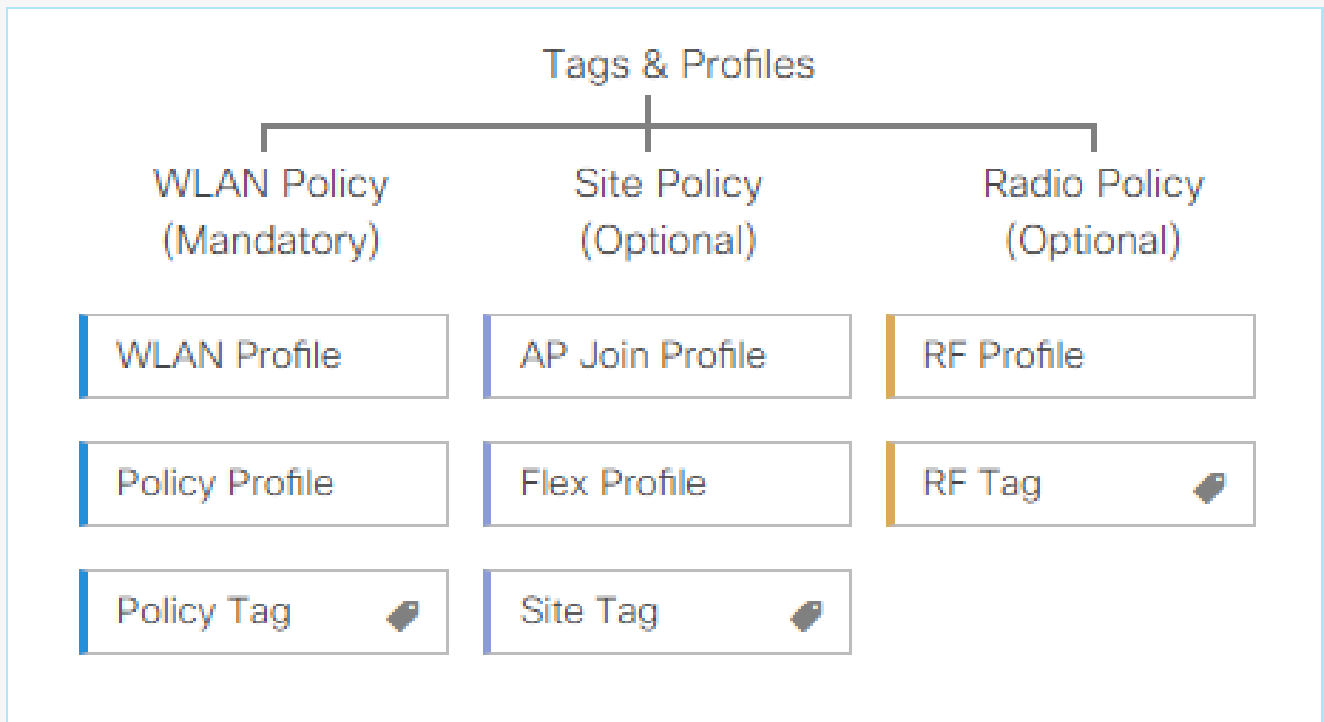
Opción A. Vaya a Configuration > Wireless Setup > Advanced desde allí, seleccione Start Now para mostrar la lista del menú de configuración. Seleccione el icono de lista junto a Tag APs, esto muestra la lista de todos los AP en estado de unión, verifique los AP necesarios y luego seleccione + Tag APs, seleccione la etiqueta de política creada del menú desplegable.



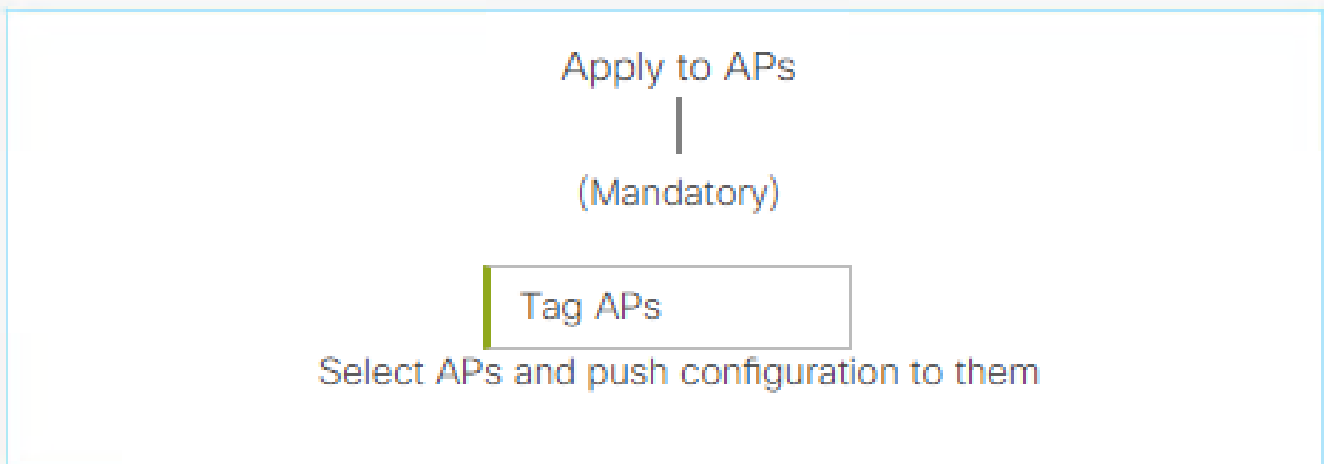
## Wireless Setup Flow Overview

This screen allows you to design Wireless LAN Configuration. It involves creating Policies and Tags. Once the design is completed, they can be deployed to the Access Points right here.

### DESIGN PHASE



### DEPLOY PHASE



### TERMINOLOGY

Tag

WLAN Policy, Policy Profile

Site Policy - AP Profile, Site Profile

Radio Policy - Radio Characteristics

### ACTIONS



Go to List View



Create New

. Defina el nombre de la regla, el regex del nombre del AP (esta configuración permite que el controlador defina qué AP se etiquetan), la prioridad (los números más bajos tienen mayor prioridad) y las etiquetas necesarias.

### Associate Tags to AP ✕

Rule Name*	Guest-APs	Policy Tag Name	EWA-Tag <span>✕</span> <span>▼</span>
AP name regex*	C9117-.*	Site Tag Name	Search or Select <span>▼</span>
Active	YES <input checked="" type="checkbox"/>	RF Tag Name	Search or Select <span>▼</span>
Priority*	1		

↶ Cancel Apply to Device

## Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente:

```
<#root>
```

```
9800#
```

```
show running-config wlan
```

```
9800#
```

```
show running-config aaa
```

```
9800#
```

```
show aaa servers
```

```
9800#
```

```
show ap tag summary
```

```
9800#
```

```
show ap name <ap-name> config general
```

```
9800#
```

```
show ap name <ap-name> tag detail
```

```
9800#
```

```
show wlan [summary | id | name | all]
```

```
9800#
```

```
show wireless tag policy detailed <policy-tag name>
```

```
9800#
```

```
show wireless profile policy detailed <policy-profile name>
```

Verifique el estado y la disponibilidad del servidor http con show ip http server status:

```
<#root>
```

```
9800#
```

```
show ip http server status
```

```
HTTP server status: Enabled
```

```
HTTP server port: 80
```

```
HTTP server active supplementary listener ports: 21111
```

```
HTTP server authentication method: local
```

```
HTTP server auth-retry 0 time-window 0
```

```
HTTP server digest algorithm: md5
```

```
HTTP server access class: 0
```

```
HTTP server IPv4 access class: None
```

```
HTTP server IPv6 access class: None
```

```
[...]
```

```
HTTP server active session modules: ALL
```

```
HTTP secure server capability: Present
```

```
HTTP secure server status: Enabled
```

```
HTTP secure server port: 443
```

```
HTTP secure server ciphersuite: rsa-aes-cbc-sha2 rsa-aes-gcm-sha2
```

```
dhe-aes-cbc-sha2 dhe-aes-gcm-sha2 ecdhe-rsa-aes-cbc-sha2
```

```
ecdhe-rsa-aes-gcm-sha2 ecdhe-ecdsa-aes-gcm-sha2
```

```
HTTP secure server TLS version: TLSv1.2 TLSv1.1
```

```
HTTP secure server client authentication: Disabled
```

```
HTTP secure server PIV authentication: Disabled
```

```
HTTP secure server PIV authorization only: Disabled
```

```
HTTP secure server trustpoint: CISCO_IDEVID_SUDI
```

```
HTTP secure server peer validation trustpoint:
```

```
HTTP secure server ECDHE curve: secp256r1
```

```
HTTP secure server active session modules: ALL
```

Verifique la conexión ACL a la sesión del cliente con estos comandos:

<#root>

9800#

show platform software wireless-client chassis active R0 mac-address <Client mac in aaaa.bbbb.cccc format>

ID : 0xa0000002  
MAC address : aaaa.bbbb.cccc  
Type : Normal  
Global WLAN ID : 4

SSID : EWA-Guest

Client index : 0  
Mobility state : Local

Authentication state : L3 Authentication

VLAN ID : 2621  
[...]  
Disable IPv6 traffic : No

Dynamic policy template : 0x7b 0x73 0x0b 0x1e 0x46 0x2a 0xd7 0x8f 0x23 0xf3 0xfe 0x9e 0x5c 0xb0 0xeb 0xf1

9800#

show platform software cgacl chassis active F0

Template ID

Group Index

Lookup ID Number of clients

-----  
0x7B 0x73 0x0B 0x1E 0x46 0x2A 0xD7 0x8F 0x23 0xF3 0xFE 0x9E 0x5C 0xB0 0xEB 0xF8 0x0000000a

0x0000001a 1

9800#

show platform software cgacl chassis active F0 group-idx <group index> acl

ACL ID ACL Name CGACL Type Protocol Direction Sequence

-----  
16 IP-Adm-V6-Int-ACL-global Punt IPv6 IN 1

25 WA-sec-172.16.80.8 Security IPv4 IN 2

```
26 WA-v4-int-172.16.80.8 Punt IPv4 IN 1
```


```
19 implicit_deny Security IPv4 IN 3  
21 implicit_deny_v6 Security IPv6 IN 3  
18 preauth_v6 Security IPv6 IN 2
```

## Troubleshoot

### Seguimiento siempre activo

El WLC 9800 proporciona capacidades de seguimiento SIEMPRE ACTIVO. Esto garantiza que todos los mensajes de nivel de aviso, advertencia y errores relacionados con la conectividad del cliente se registren constantemente y que pueda ver los registros de una condición de incidente o falla después de que haya ocurrido.

---

 Nota: Según el volumen de registros generados, puede retroceder de unas horas a varios días.

---

Para ver los seguimientos que 9800 WLC recolectó por defecto, puede conectarse vía SSH/Telnet al 9800 WLC y leer estos pasos (asegúrese de registrar la sesión en un archivo de texto).

Paso 1. Compruebe la hora actual del controlador para poder realizar un seguimiento de los registros en el tiempo hasta el momento en que ocurrió el problema.

```
<#root>  
  
9800#  
  
show clock
```

Paso 2. Recopile registros del sistema del buffer del controlador o del registro del sistema externo según lo dicte la configuración del sistema. Esto proporciona una vista rápida del estado del sistema y de los errores, si los hubiera.

```
<#root>  
  
9800#  
  
show logging
```

Paso 3. Verifique si hay alguna condición de depuración habilitada.

```
<#root>
```

```
9800#
```

```
show debugging
```

```
IOSXE Conditional Debug Configs:
```

```
Conditional Debug Global State: Stop
```

```
IOSXE Packet Tracing Configs:
```


```
Packet Infra debugs:
```

```
Ip Address
```

```
Port
```

```
-----|-----
```

---

 Nota: Si ve alguna condición en la lista, significa que los seguimientos se registran en el nivel de depuración para todos los procesos que encuentran las condiciones habilitadas (dirección MAC, dirección IP, etc.). Esto aumenta el volumen de registros. Por lo tanto, se recomienda borrar todas las condiciones cuando no se está depurando activamente.

---

Paso 4. Suponiendo que la dirección MAC sometida a la prueba no figuraba como condición en el paso 3. Recopile los seguimientos del nivel de aviso siempre activo para la dirección MAC específica.

```
<#root>
```

```
9800#
```

```
show logging profile wireless filter [mac | ip] [<aaaa.bbbb.cccc> | <a.b.c.d>] to-file always-on-<FILENAME>
```

Puede mostrar el contenido de la sesión o copiar el archivo en un servidor TFTP externo.

```
<#root>
```

```
9800#
```

```
more bootflash:always-on-<FILENAME.txt>
```

```
or
```

```
9800#
```

```
copy bootflash:always-on-<FILENAME.txt> tftp://<a.b.c.d>/<path>/always-on-<FILENAME.txt>
```

## Depuración condicional y seguimiento activo por radio

Si los seguimientos siempre activos no proporcionan suficiente información para determinar el desencadenador del problema que se está investigando, puede habilitar la depuración condicional y capturar el seguimiento de Radio Activo (RA), que proporciona seguimientos de nivel de depuración para todos los procesos que interactúan con la condición especificada (dirección MAC del cliente en este caso). Para habilitar la depuración condicional, lea estos pasos.

Paso 1. Asegúrese de que no haya condiciones de depuración habilitadas.


```
<#root>
9800#
clear platform condition all
```

Paso 2. Habilite la condición de depuración para la dirección MAC del cliente inalámbrico que desea monitorear.


Estos comandos comienzan a monitorear la dirección MAC proporcionada durante 30 minutos (1800 segundos). Opcionalmente, puede aumentar este tiempo hasta 2 085 978 494 segundos.

```
<#root>
9800#
debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

---

 Nota: Para monitorear más de un cliente a la vez, ejecute el comando debug wireless mac por dirección mac.

---

 Nota: La actividad del cliente inalámbrico no se muestra en la sesión de terminal, ya que todos los registros se almacenan en buffer internamente para poder visualizarlos más tarde.

---

Paso 3. Reproduzca el problema o el comportamiento que desea monitorear.

Paso 4. Detenga las depuraciones si el problema se reproduce antes de que se agote el tiempo de monitoreo predeterminado o configurado.

```
<#root>
9800#
no debug wireless mac <aaaa.bbbb.cccc>
```

Una vez que ha transcurrido el tiempo de monitoreo o se ha detenido la depuración inalámbrica, el WLC 9800 genera un archivo local con el nombre:

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Paso 5. Recopile el archivo de la actividad de la dirección MAC. Puede copiar el archivo de seguimiento activo por radio .log en un servidor externo o mostrar el resultado directamente en la

pantalla.

Verifique el nombre del archivo de seguimiento activo por radio.

```
<#root>
```

```
9800#
```

```
dir bootflash: | inc ra_trace
```

Copie el archivo en un servidor externo:

```
<#root>
```

```
9800#
```

```
copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://<a.b.c.d>
```

Muestre el contenido:

```
<#root>
```

```
9800#
```

```
more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```


Paso 6. Si la causa raíz aún no es obvia, recopile los registros internos, que son una vista más detallada de los registros de nivel de depuración. No es necesario depurar el cliente de nuevo, ya que el comando proporciona registros de depuración que ya se han recopilado y almacenado internamente.

```
<#root>
```

```
9800#
```

```
show logging profile wireless internal filter [mac | ip] [<aaaa.bbbb.cccc> | <a.b.c.d>] to-file ra-inter
```

---

 Nota: Esta salida de comando devuelve seguimientos para todos los niveles de registro para todos los procesos y es bastante voluminosa. Póngase en contacto con Cisco TAC para obtener ayuda con el análisis de estos seguimientos.

---

```
<#root>
```



```
9800#
```

```
copy bootflash:ra-internal-<FILENAME>.txt tftp://<a.b.c.d>/ra-internal-<FILENAME>.txt
```

Muestre el contenido:


```
<#root>
```

```
9800#
```

```
more bootflash:ra-internal-<FILENAME>.txt
```

Paso 7. Elimine las condiciones de depuración.

---

 Nota: Asegúrese de eliminar siempre las condiciones de depuración después de una sesión de solución de problemas.

---

## Capturas de paquetes integradas

Los controladores 9800 pueden rastrear paquetes de forma nativa; esto permite resolver problemas más fácilmente a medida que se visualiza el procesamiento de paquetes del plano de control.

Paso 1. Defina una ACL para filtrar el tráfico de interés. Para la autenticación web, se recomienda permitir el tráfico desde y hacia el servidor web, así como el tráfico desde y hacia un par de AP donde los clientes están conectados.

```
<#root>
```

```
9800(config)#
```

```
ip access-list extended EWA-pcap
```

```
9800(config-ext-nacl)#
```

```
permit ip any host <web server IP>
```

```
9800(config-ext-nacl)#
```

```
permit ip host <web server IP> any
```

```
9800(config-ext-nacl)#
```

```
permit ip any host <AP IP>
```

```
9800(config-ext-nacl)#
```

```
permit ip host <AP IP> any
```

Paso 2. Defina los parámetros de captura de monitor. Asegúrese de que el tráfico del plano de control esté habilitado en ambas direcciones, la interfaz se refiere al link ascendente físico de su controlador.

```
<#root>
```

```
9800#
```

```
monitor capture EWA buffer size <buffer size in MB>
```

```
9800#
```

```
monitor capture EWA access-list EWA-pcap
```

```
9800#
```

```
monitor capture EWA control-plane both interface <uplink interface> both
```

```
<#root>
```

```
9800#
```

```
show monitor capture EWA
```

```
Status Information for Capture EWA
```

```
Target Type:
```

```
Interface: Control Plane, Direction: BOTH
```

```
Interface: TenGigabitEthernet0/1/0, Direction: BOTH
```

```
Status : Inactive
```

```
Filter Details:
```

```
Access-list: EWA-pcap
```

```
Inner Filter Details:
```

```
Buffer Details:
```

```
Buffer Type: LINEAR (default)
```

```
Buffer Size (in MB): 100
```

```
Limit Details:
```

```
Number of Packets to capture: 0 (no limit)
```

```
Packet Capture duration: 0 (no limit)
```

```
Packet Size to capture: 0 (no limit)
```

```
Packet sampling rate: 0 (no sampling)
```

Paso 3. Inicie la captura del monitor y reproduzca el problema.

```
<#root>
```

9800#

```
monitor capture EWA start
```

```
Started capture point : EWA
```

Paso 4. Detenga la captura de monitor y expórtela.

<#root>

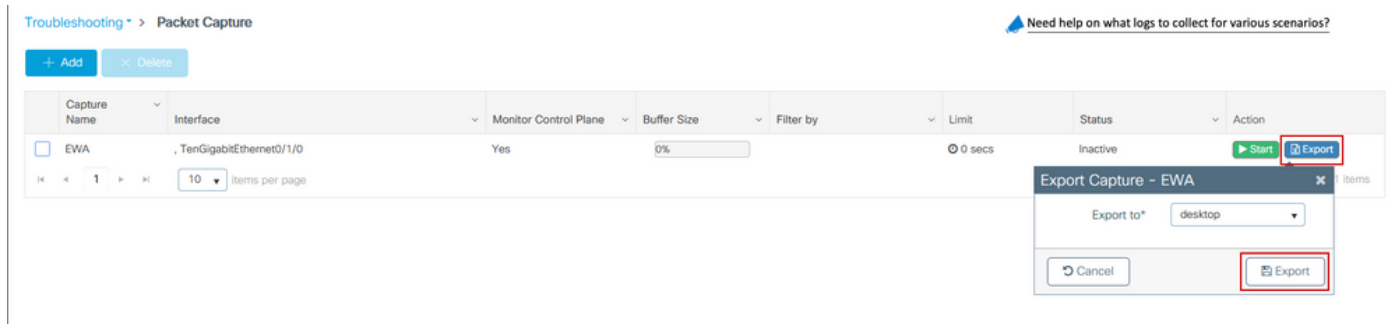
9800#

```
monitor capture EWA stop
```

```
Stopped capture point : EWA
```

```
9800#monitor capture EWA export tftp://<a.b.c.d>/EWA.pcap
```

Como alternativa, la captura se puede descargar de la GUI, navegue hasta Troubleshooting > Packet Capture y seleccione Export en la captura configurada. Seleccione escritorio en el menú desplegable para descargar la captura a través de HTTP en la carpeta deseada.



## Solución de problemas del cliente

Las WLANs de autenticación Web dependen del comportamiento del cliente; sobre esta base, el conocimiento y la información del comportamiento del cliente es clave para identificar la causa raíz de los comportamientos incorrectos de autenticación Web.

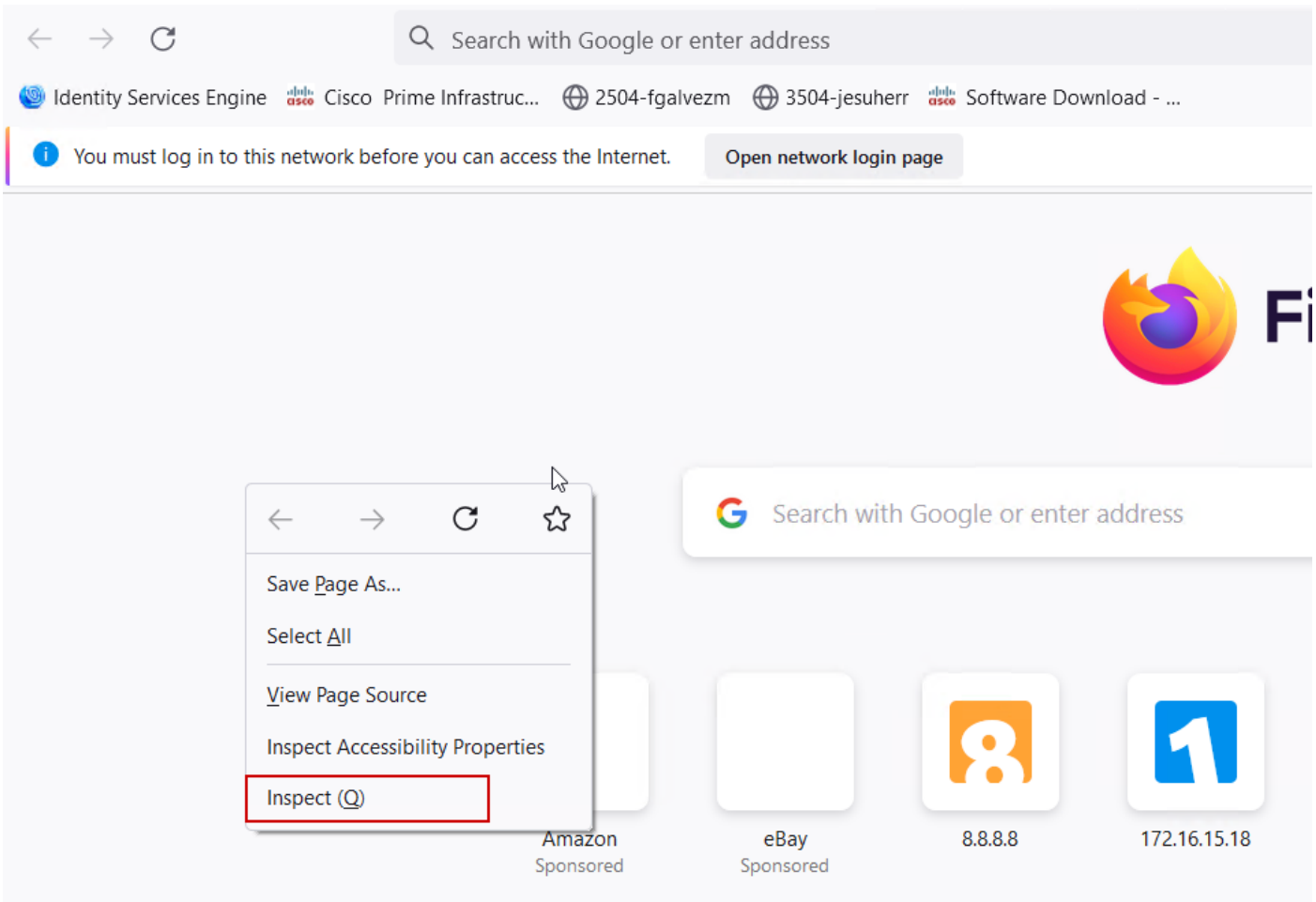
## Solución de problemas del explorador HAR

Muchos navegadores modernos, como Mozilla Firefox y Google Chrome, proporcionan herramientas de desarrollador de consolas para depurar las interacciones de las aplicaciones web. Los archivos HAR son registros de las interacciones cliente-servidor y proporcionan una línea de tiempo de las interacciones HTTP junto con la información de solicitud y respuesta (encabezados, código de estado, parámetros, etc.).

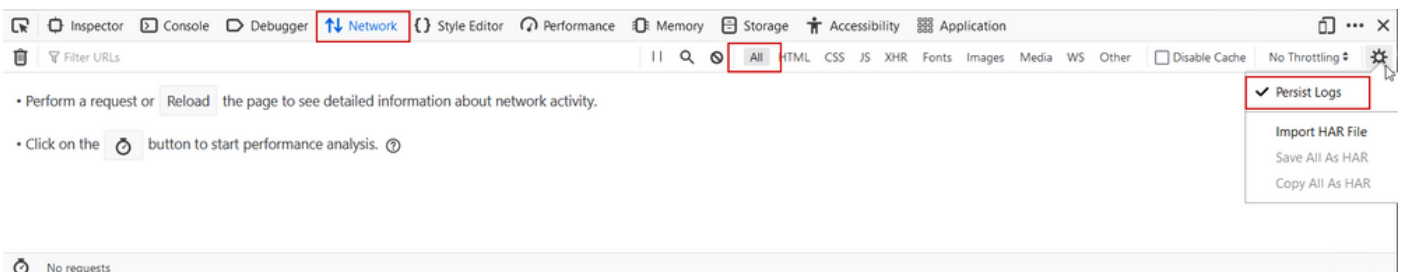
Los archivos HAR se pueden exportar desde el explorador cliente e importar en un explorador diferente para su posterior análisis. Este documento describe cómo recopilar el archivo HAR de

## Mozilla Firefox.

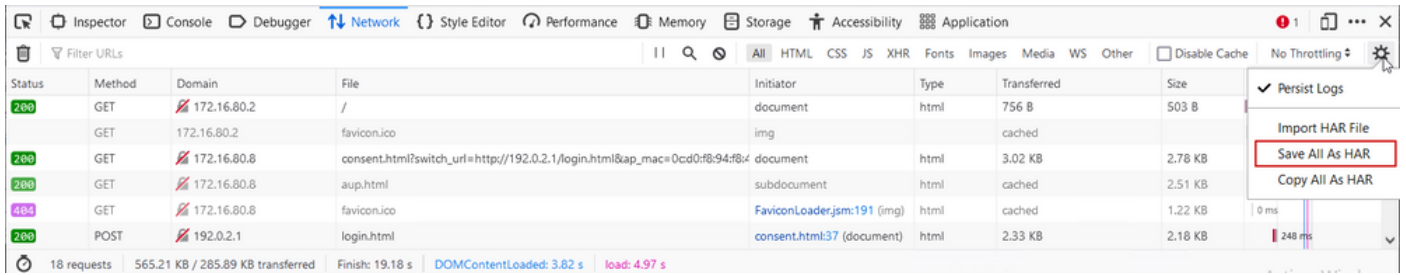
Paso 1. Abra Web Developer Tools con Ctrl + Shift + I, alternativamente haga clic con el botón derecho dentro del contenido del navegador y seleccione Inspeccionar.



Paso 2. Vaya a Red, asegúrese de que está seleccionado "Todos" para capturar todos los tipos de solicitudes. Seleccione el icono de engranaje y asegúrese de que Persist Logs tenga una flecha junto a él, de lo contrario los registros de solicitud se borran cada vez que se activa un cambio de dominio.



Paso 3. Reproduzca el problema y asegúrese de que el explorador registre todas las solicitudes. Una vez reproducido el problema, detenga el registro de la red, seleccione el icono del engranaje y seleccione Guardar todo como HAR.



## Captura de paquetes del lado cliente

Los clientes inalámbricos con SO como Windows o MacOS pueden olfatear paquetes en su adaptador de tarjeta inalámbrico. Aunque no son una sustitución directa de las capturas de paquetes por aire, pueden proporcionar un vistazo del flujo de autenticación web general.

## Solicitud de DNS:

11868	2021-09-28 06:44:07.364395	172.16.21.153	172.16.21.7	DNS	182	53	Standard query 0x8586 A prod.detectportal.prod.cloudops.mozgcp.net
11869	2021-09-28 06:44:07.375372	172.16.21.7	172.16.21.153	DNS	195	57857	Standard query response 0x8586 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME prod.detectportal.prod.cloudops.mozgcp.net A 34.187.221.8
11870	2021-09-28 06:44:07.418773	172.16.21.7	172.16.21.153	DNS	118	51759	Standard query response 0x8586 A prod.detectportal.prod.cloudops.mozgcp.net A 34.187.221.82

## Protocolo de enlace TCP inicial y HTTP GET para redirección:

444	2021-09-27 21:53:46....	172.16.21.153	52.185.211.133	TCP	66	54623 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
445	2021-09-27 21:53:46....	172.16.21.153	96.7.93.42	HTTP	205	GET /files/vpn_ssid_notif.txt HTTP/1.1
446	2021-09-27 21:53:46....	96.7.93.42	172.16.21.153	HTTP	866	HTTP/1.1 200 OK (text/html)
447	2021-09-27 21:53:46....	172.16.21.153	96.7.93.42	TCP	54	65421 → 80 [ACK] Seq=303 Ack=1625 Win=131072 Len=0

## Protocolo de enlace TCP con servidor externo:

11889	2021-09-28 06:44:07.872917	172.16.21.153	172.16.80.8	TCP	66	65209 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
11890	2021-09-28 06:44:07.880494	172.16.80.8	172.16.21.153	TCP	66	80 → 65209 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1250 WS=256 SACK_PERM=1
11891	2021-09-28 06:44:07.888947	172.16.21.153	172.16.80.8	TCP	54	65209 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0

## HTTP GET a servidor externo (solicitud de portal cautivo):

11106	2021-09-28 06:44:08.524191	172.16.21.153	172.16.80.8	HTTP	563	GET /webauth/consent.html?switch_url=http://192.0.2.1/login.html&ap_mac=0c0d0f8:97ae:60&client_mac=34:23:87:4c:6b:f7&ssid=84a-Guest&redirect=http://www.ms
11107	2021-09-28 06:44:08.522258	172.16.80.8	172.16.21.153	TCP	54	80 → 65209 [ACK] Seq=1 Ack=510 Win=66048 Len=0
11112	2021-09-28 06:44:08.706215	172.16.80.8	172.16.21.153	TCP	1384	80 → 65209 [ACK] Seq=1 Ack=510 Win=66048 Len=1250 [TCP segment of a reassembled PDU]
11113	2021-09-28 06:44:08.787182	172.16.80.8	172.16.21.153	TCP	1384	80 → 65209 [ACK] Seq=1251 Ack=510 Win=66048 Len=1250 [TCP segment of a reassembled PDU]
11114	2021-09-28 06:44:08.787487	172.16.21.153	172.16.80.8	TCP	54	65209 → 80 [ACK] Seq=510 Ack=2501 Win=131072 Len=0
11115	2021-09-28 06:44:08.787653	172.16.80.8	172.16.21.153	HTTP	648	HTTP/1.1 200 OK (text/html)
11116	2021-09-28 06:44:08.834606	172.16.21.153	172.16.80.8	TCP	54	65209 → 80 [ACK] Seq=510 Ack=3095 Win=130560 Len=0

## HTTP POST a IP virtual para autenticación:

12331	2021-09-28 06:44:50.644118	172.16.21.153	192.0.2.1	TCP	66	52359 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
12332	2021-09-28 06:44:50.648080	192.0.2.1	172.16.21.153	TCP	66	80 → 52359 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1250 SACK_PERM=1 WS=120
12333	2021-09-28 06:44:50.649166	172.16.21.153	192.0.2.1	TCP	54	52359 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
12334	2021-09-28 06:44:50.667759	172.16.21.153	192.0.2.1	HTTP	609	POST /login.html HTTP/1.1 (application/x-www-form-urlencoded)
12335	2021-09-28 06:44:50.672372	192.0.2.1	172.16.21.153	TCP	54	80 → 52359 [ACK] Seq=1 Ack=556 Win=64128 Len=0
12337	2021-09-28 06:44:50.680599	192.0.2.1	172.16.21.153	TCP	1014	80 → 52359 [ACK] Seq=1 Ack=556 Win=64128 Len=968 [TCP segment of a reassembled PDU]
12338	2021-09-28 06:44:50.680996	192.0.2.1	172.16.21.153	TCP	1014	80 → 52359 [ACK] Seq=961 Ack=556 Win=64128 Len=968 [TCP segment of a reassembled PDU]
12339	2021-09-28 06:44:50.681125	172.16.21.153	192.0.2.1	TCP	54	52359 → 80 [ACK] Seq=556 Ack=1921 Win=131072 Len=0
12340	2021-09-28 06:44:50.681261	192.0.2.1	172.16.21.153	HTTP	544	HTTP/1.1 200 OK (text/html)
12341	2021-09-28 06:44:50.681423	192.0.2.1	172.16.21.153	TCP	54	80 → 52359 [FIN, ACK] Seq=2411 Ack=556 Win=64128 Len=0
12342	2021-09-28 06:44:50.681591	172.16.21.153	192.0.2.1	TCP	54	52359 → 80 [ACK] Seq=556 Ack=2411 Win=130560 Len=0
12353	2021-09-28 06:44:50.749948	172.16.21.153	192.0.2.1	TCP	54	52359 → 80 [ACK] Seq=556 Ack=2412 Win=130560 Len=0

## Ejemplo de un intento exitoso

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

## Autenticación y asociación 802.11:

<#root>

2021/09/28 12:59:51.781967 {wncd\_x\_R0-0}{1}: [client-orch-sm] [26328]: (note): MAC: 3423.874c.6bf7 Assoc  
2021/09/28 12:59:51.782009 {wncd\_x\_R0-0}{1}: [client-orch-sm] [26328]: (debug): MAC: 3423.874c.6bf7

Received Dot11 association request.

Processing started,

SSID: EWA-Guest, Policy profile: Guest-Policy

, AP Name: C9117AXI-lobby, Ap Mac Address: 0cd0.f897.ae60 BSSID MAC0000.0000.0000 wlan ID: 4RSSI: -39,  
2021/09/28 12:59:51.782152 {wncd\_x\_R0-0}{1}: [client-orch-state] [26328]: (note): MAC: 3423.874c.6bf7 C  
2021/09/28 12:59:51.782357 {wncd\_x\_R0-0}{1}: [dot11-validate] [26328]: (info): MAC: 3423.874c.6bf7 Wi-Fi  
2021/09/28 12:59:51.782480 {wncd\_x\_R0-0}{1}: [dot11] [26328]: (debug): MAC: 3423.874c.6bf7 dot11 send a

Sending association response with resp\_status\_code: 0

2021/09/28 12:59:51.782483 {wncd\_x\_R0-0}{1}: [dot11] [26328]: (debug): MAC: 3423.874c.6bf7 Dot11 Capabi  
2021/09/28 12:59:51.782509 {wncd\_x\_R0-0}{1}: [dot11-frame] [26328]: (info): MAC: 3423.874c.6bf7 Wi-Fi di  
2021/09/28 12:59:51.782519 {wncd\_x\_R0-0}{1}: [dot11] [26328]: (info): MAC: 3423.874c.6bf7 dot11 send as  
2021/09/28 12:59:51.782611 {wncd\_x\_R0-0}{1}: [dot11] [26328]: (note): MAC: 3423.874c.6bf7

Association success. AID 1

, Roaming = False, WGB = False, 11r = False, 11w = False  
2021/09/28 12:59:51.782626 {wncd\_x\_R0-0}{1}: [dot11] [26328]: (info): MAC: 3423.874c.6bf7 DOT11 state t  
2021/09/28 12:59:51.782676 {wncd\_x\_R0-0}{1}: [client-orch-sm] [26328]: (debug): MAC: 3423.874c.6bf7

Station Dot11 association is successful.

Autenticación de capa 2 omitida:

<#root>

2021/09/28 12:59:51.782727 {wncd\_x\_R0-0}{1}: [client-orch-sm] [26328]: (debug): MAC: 3423.874c.6bf7 Sta  
2021/09/28 12:59:51.782745 {wncd\_x\_R0-0}{1}: [client-orch-state] [26328]: (note): MAC: 3423.874c.6bf7 C  
2021/09/28 12:59:51.782785 {wncd\_x\_R0-0}{1}: [client-auth] [26328]: (note): MAC: 3423.874c.6bf7

L2 Authentication initiated. method WEBAUTH

, Policy VLAN 2621,AAA override = 0  
2021/09/28 12:59:51.782803 {wncd\_x\_R0-0}{1}: [sanet-shim-translate] [26328]: (ERR): 3423.874c.6bf7 wlan  
[...]  
2021/09/28 12:59:51.787912 {wncd\_x\_R0-0}{1}: [client-auth] [26328]: (info): MAC: 3423.874c.6bf7 Client  
2021/09/28 12:59:51.787953 {wncd\_x\_R0-0}{1}: [client-auth] [26328]: (info): MAC: 3423.874c.6bf7 Client  
2021/09/28 12:59:51.787966 {wncd\_x\_R0-0}{1}: [client-orch-sm] [26328]: (debug): MAC: 3423.874c.6bf7

L2 Authentication of station is successful., L3 Authentication : 1

sondeo de ACL:

<#root>

2021/09/28 12:59:51.785227 {wncd\_x\_R0-0}{1}: [webauth-sm] [26328]: (info): [ 0.0.0.0]Starting Webauth, r  
2021/09/28 12:59:51.785307 {wncd\_x\_R0-0}{1}: [auth-mgr-feat\_wireless] [26328]: (info): [0000.0000.0000:  
2021/09/28 12:59:51.785378 {wncd\_x\_R0-0}{1}: [webauth-ac1] [26328]: (info): capwap\_9000000b[3423.874c.6

Applying IPv4 intercept ACL via SVM, name: WA-v4-int-172.16.80.8

, priority: 50, IIF-ID: 0  
2021/09/28 12:59:51.785738 {wncd\_x\_R0-0}{1}: [epm-redirect] [26328]: (info): [0000.0000.0000:unknown]  
URL-Redirect-ACL = WA-v4-int-172.16.80.8

2021/09/28 12:59:51.786324 {wncd\_x\_R0-0}{1}: [webauth-ac1] [26328]: (info): capwap\_9000000b[3423.874c.6  
Applying IPv6 intercept ACL via SVM, name: IP-Adm-V6-Int-ACL-global, priority: 52

, IIF-ID: 0  
2021/09/28 12:59:51.786598 {wncd\_x\_R0-0}{1}: [epm-redirect] [26328]: (info): [0000.0000.0000:unknown]  
URL-Redirect-ACL = IP-Adm-V6-Int-ACL-global

2021/09/28 12:59:51.787904 {wncd\_x\_R0-0}{1}: [client-auth] [26328]: (info): MAC: 3423.874c.6bf7 Client

### Proceso de aprendizaje de IP:

<#root>

2021/09/28 12:59:51.799515 {wncd\_x\_R0-0}{1}: [client-orch-state] [26328]: (note): MAC: 3423.874c.6bf7 C  
2021/09/28 12:59:51.799716 {wncd\_x\_R0-0}{1}: [client-iplearn] [26328]: (info): MAC: 3423.874c.6bf7  
IP-learn state transition: S\_IPLEARN\_INIT -> S\_IPLEARN\_IN\_PROGRESS

2021/09/28 12:59:51.802213 {wncd\_x\_R0-0}{1}: [client-auth] [26328]: (info): MAC: 3423.874c.6bf7 Client  
2021/09/28 12:59:51.916777 {wncd\_x\_R0-0}{1}: [sisf-packet] [26328]: (debug): RX: ARP from interface cap  
[...]  
2021/09/28 12:59:52.810136 {wncd\_x\_R0-0}{1}: [client-iplearn] [26328]: (note): MAC: 3423.874c.6bf7  
Client IP learn successful. Method: ARP IP: 172.16.21.153

2021/09/28 12:59:52.810185 {wncd\_x\_R0-0}{1}: [epm] [26328]: (info): [0000.0000.0000:unknown] HDL = 0x0  
2021/09/28 12:59:52.810404 {wncd\_x\_R0-0}{1}: [auth-mgr] [26328]: (info): [3423.874c.6bf7:capwap\_9000000  
2021/09/28 12:59:52.810794 {wncd\_x\_R0-0}{1}: [auth-mgr-feat\_wireless] [26328]: (info): [0000.0000.0000:  
2021/09/28 12:59:52.810863 {wncd\_x\_R0-0}{1}: [client-iplearn] [26328]: (info): MAC: 3423.874c.6bf7  
IP-learn state transition: S\_IPLEARN\_IN\_PROGRESS -> S\_IPLEARN\_COMPLETE

### Proceso de redirección y autenticación de capa 3:

<#root>

2021/09/28 12:59:52.811141 {wncd\_x\_R0-0}{1}: [client-auth] [26328]: (note): MAC: 3423.874c.6bf7  
L3 Authentication initiated. LWA

2021/09/28 12:59:52.811154 {wncd\_x\_R0-0}{1}: [client-auth] [26328]: (info): MAC: 3423.874c.6bf7 Client  
2021/09/28 12:59:55.324550 {wncd\_x\_R0-0}{1}: [webauth-httpd] [26328]: (info): capwap\_9000000b[3423.874c  
2021/09/28 12:59:55.324565 {wncd\_x\_R0-0}{1}: [webauth-httpd] [26328]: (info): capwap\_9000000b[3423.874c  
HTTP GET request

2021/09/28 12:59:55.324588 {wncd\_x\_R0-0}{1}: [webauth-httpd] [26328]: (info): capwap\_900000b[3423.874c.6bf7]  
[...]

2021/09/28 13:01:29.859434 {wncd\_x\_R0-0}{1}: [webauth-httpd] [26328]: (info): capwap\_900000b[3423.874c.6bf7]

POST rcvd when in LOGIN state

2021/09/28 13:01:29.859636 {wncd\_x\_R0-0}{1}: [webauth-ac1] [26328]: (info): capwap\_900000b[3423.874c.6bf7]

2021/09/28 13:01:29.860335 {wncd\_x\_R0-0}{1}: [webauth-ac1] [26328]: (info): capwap\_900000b[3423.874c.6bf7]

2021/09/28 13:01:29.861092 {wncd\_x\_R0-0}{1}: [auth-mgr] [26328]: (info): [3423.874c.6bf7:capwap\_900000b[3423.874c.6bf7]

Authc success from WebAuth, Auth event success

2021/09/28 13:01:29.861151 {wncd\_x\_R0-0}{1}: [ewlc-infra-evq] [26328]: (note): Authentication Success.

2021/09/28 13:01:29.862867 {wncd\_x\_R0-0}{1}: [client-auth] [26328]: (note): MAC: 3423.874c.6bf7

L3 Authentication Successful.

ACL:[]

2021/09/28 13:01:29.862871 {wncd\_x\_R0-0}{1}: [client-auth] [26328]: (info): MAC: 3423.874c.6bf7

Client auth-interface state transition: S\_AUTHIF\_WEBAUTH\_PENDING -> S\_AUTHIF\_WEBAUTH\_DONE

Transición al estado RUN:

<#root>

2021/09/28 13:01:29.863176 {wncd\_x\_R0-0}{1}: [client-auth] [26328]: (note): MAC: 3423.874c.6bf7 ADD MOB

2021/09/28 13:01:29.863272 {wncd\_x\_R0-0}{1}: [errmsg] [26328]: (info): %CLIENT\_ORCH\_LOG-6-CLIENT\_ADDED\_

Username entry (3423.874C.6BF7) joined with ssid (EWA-Guest) for device with MAC: 3423.874c.6bf7

2021/09/28 13:01:29.863334 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [26328]: (info): [ Applied attribute :bsn-v

2021/09/28 13:01:29.863336 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [26328]: (info): [ Applied attribute : time

2021/09/28 13:01:29.863343 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [26328]: (info): [ Applied attribute : url-

2021/09/28 13:01:29.863387 {wncd\_x\_R0-0}{1}: [ewlc-qos-client] [26328]: (info): MAC: 3423.874c.6bf7 Cli

2021/09/28 13:01:29.863409 {wncd\_x\_R0-0}{1}: [rog-proxy-capwap] [26328]: (debug):

Managed client RUN state notification

: 3423.874c.6bf7

2021/09/28 13:01:29.863451 {wncd\_x\_R0-0}{1}: [client-orch-state] [26328]: (note): MAC: 3423.874c.6bf7

Client state transition: S\_CO\_L3\_AUTH\_IN\_PROGRESS -> S\_CO\_RUN



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).