# 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
- Verificación
- Troubleshoot
  - Seguimiento siempre activo
  - Depuración condicional y seguimiento activo por radio
  - Capturas de paquetes integradas
  - Solución de problemas del cliente
    - Solucionar 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:

- haga clic en: 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".
- nombre de usuario: Este parámetro sólo se utiliza para los mapas de parámetros de 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 parámetros de 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.

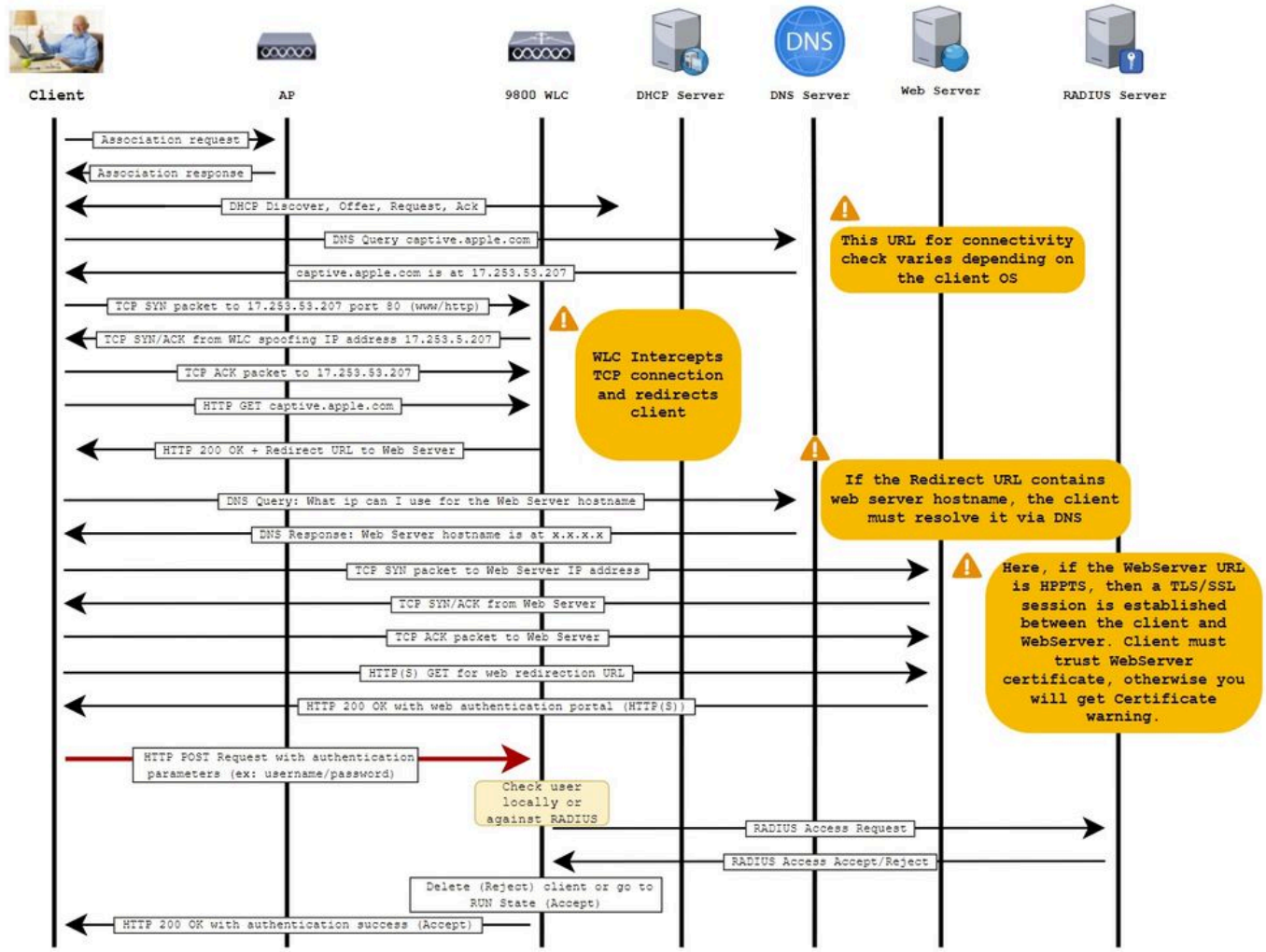
- C9800-CL WLC Cisco IOS®-XE versión 17.3.3
- Microsoft Windows Server 2012 con funciones de Internet Information Services (IIS)
- Puntos de acceso 2802 y 9117

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

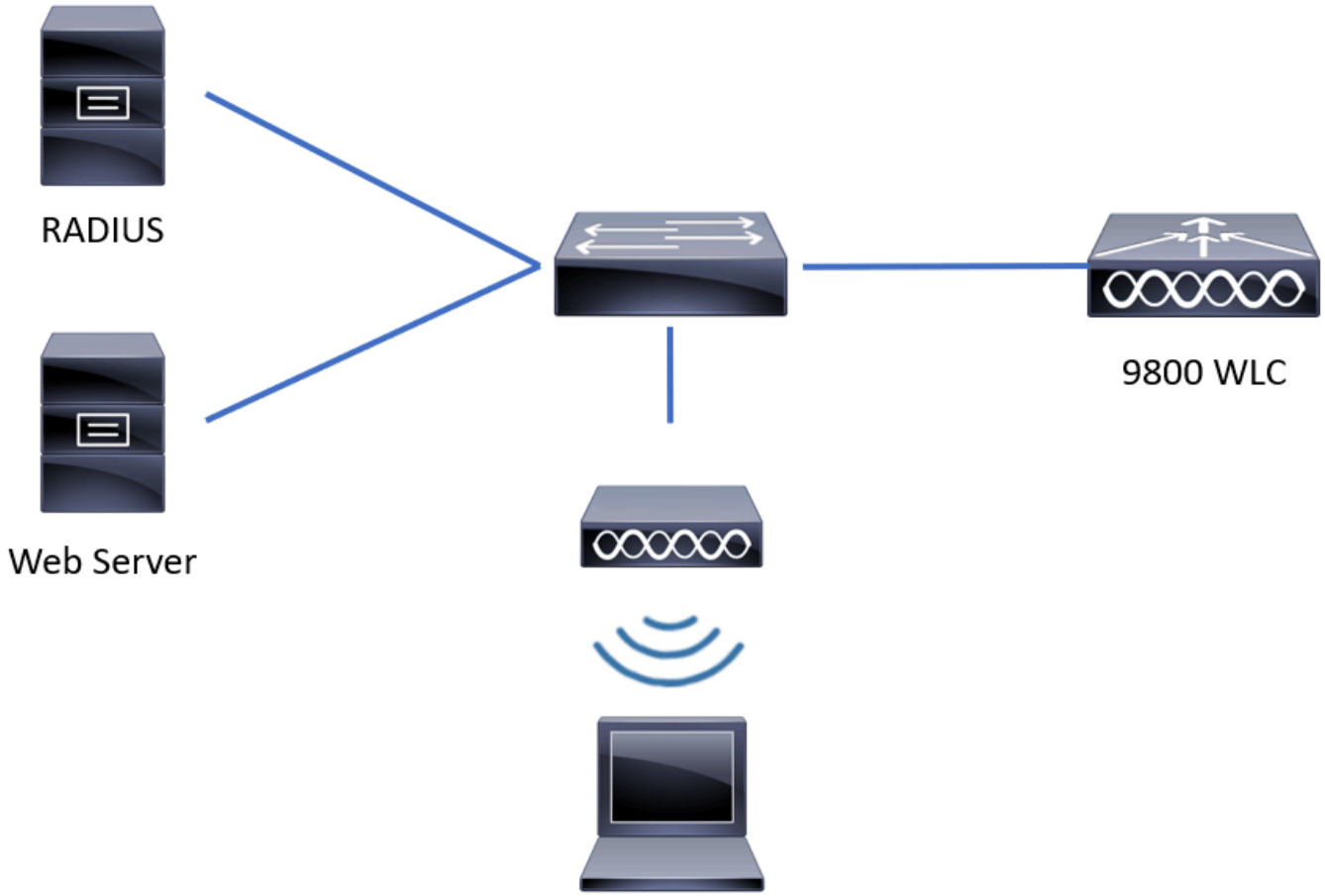
La autenticación web externa aprovecha un portal web alojado fuera del WLC en un servidor web dedicado o servidores multifunción como Identity Services Engine (ISE) que permiten el acceso y la gestión granulares de los componentes web. El protocolo de enlace necesario para incorporar correctamente un 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



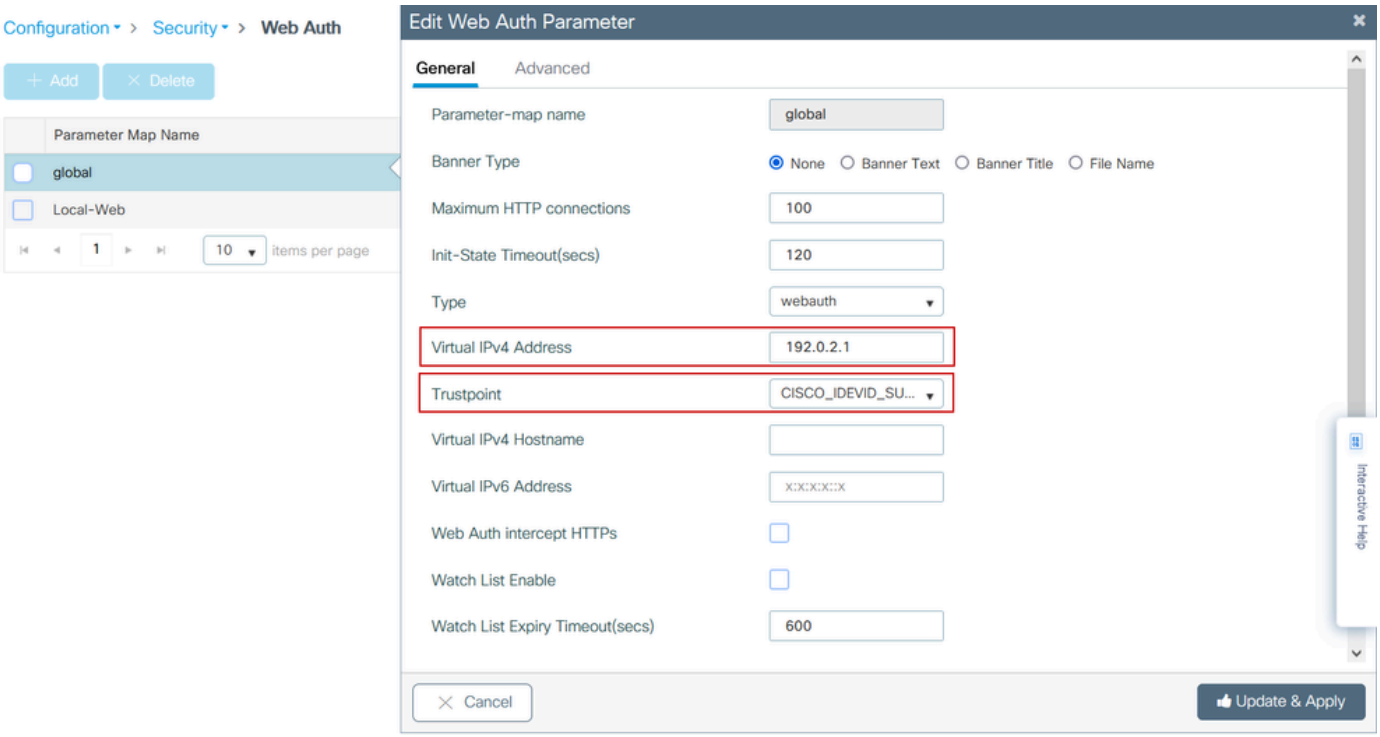

## Configurar parámetros web

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. Si tiene IPv6 habilitado en la red, también es obligatorio tener una dirección IPv6 virtual configurada. Sin las IP virtuales, es posible que la redirección no tenga lugar y que las credenciales se puedan enviar de forma no segura.

---

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 verificar Web Auth intercept HTTPs; sin embargo, no se recomienda esta configuración, ya que aumenta el uso de la CPU.

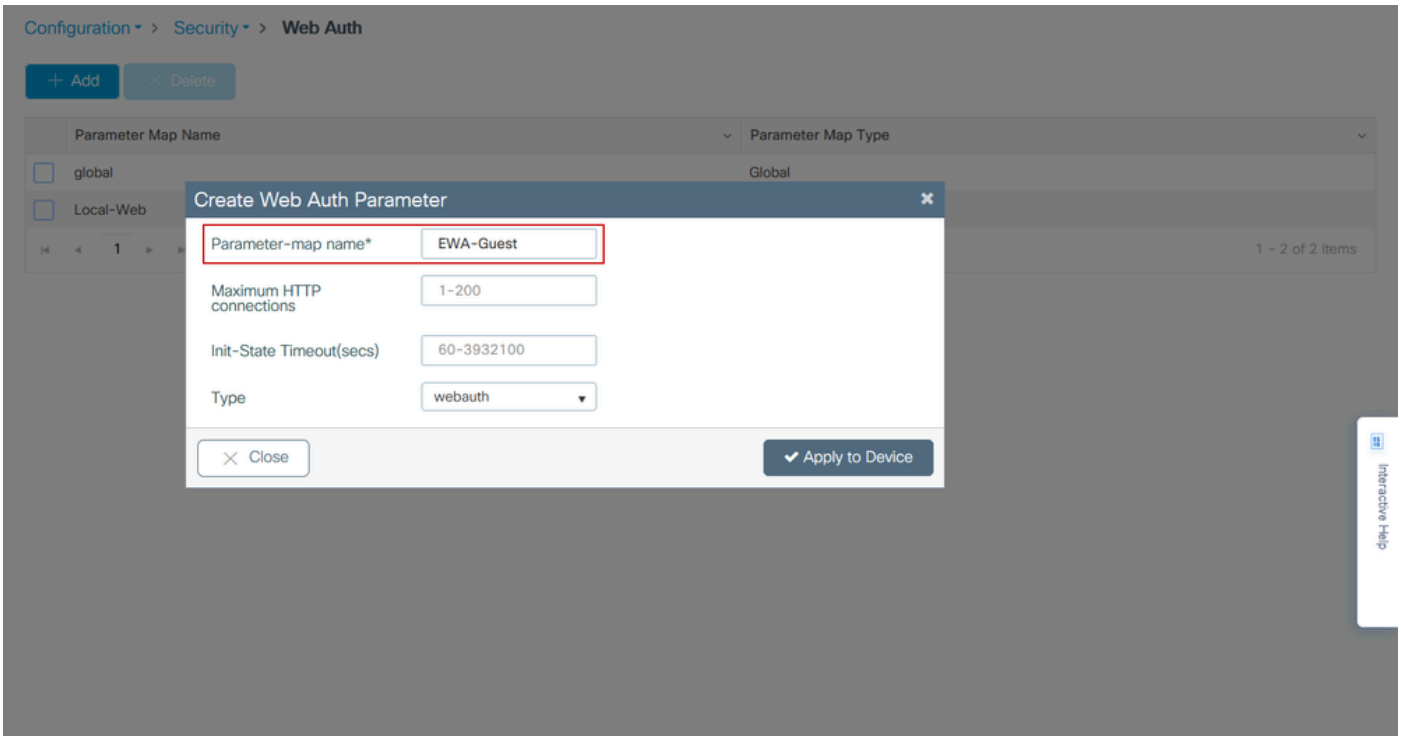
---



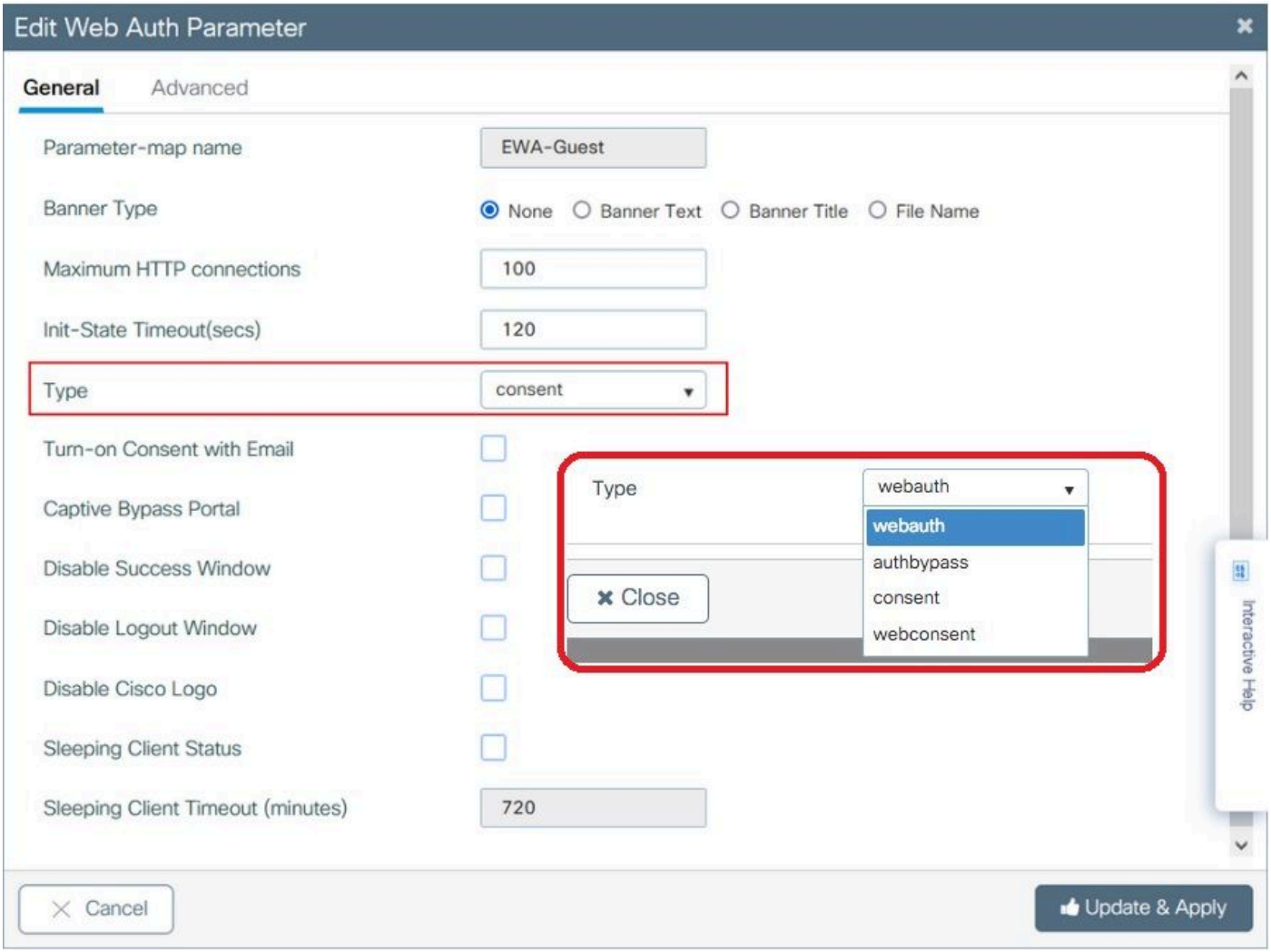

Configuración de CLI:

```
<#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
```

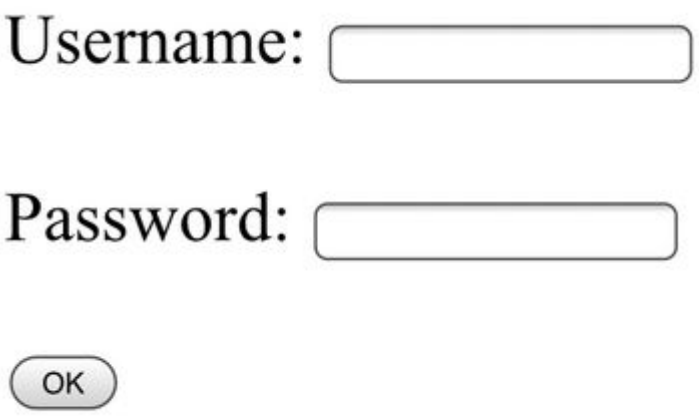
Paso 2. Seleccione + Add y configure un nombre para el nuevo mapa de parámetro que apunta al servidor externo. Opcionalmente, configure el número máximo de fallas de autenticación HTTP antes de que el cliente sea excluido y el tiempo (en segundos) que un cliente puede permanecer en el estado de autenticación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



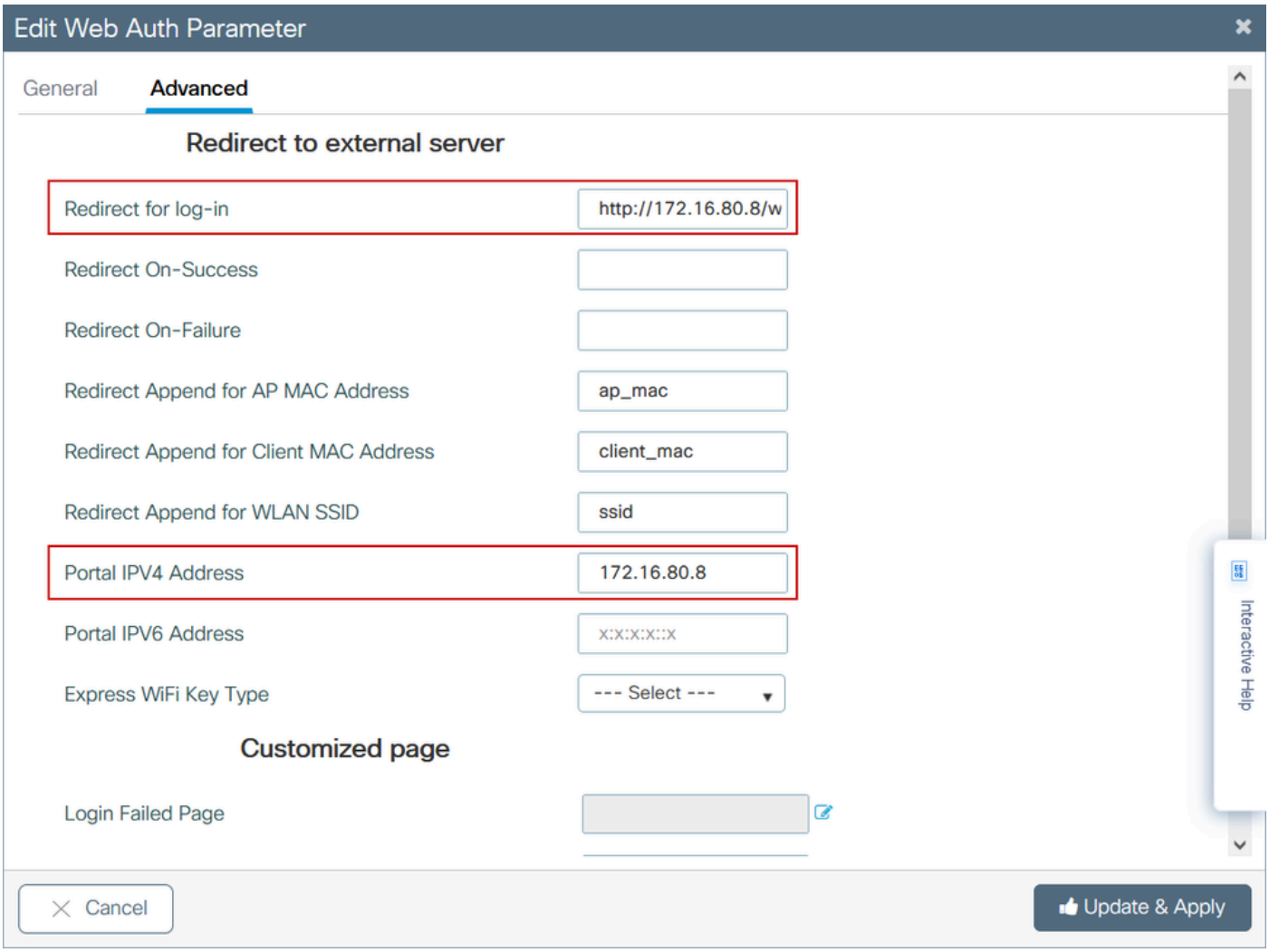

Paso 3. Seleccione el mapa de parámetro recién creado, en la pestaña General, configure el tipo de autenticación de la lista desplegable Tipo.



- 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 |
|---|---|---|
|  | texto | |

Paso 4. En la ficha Advanced, configure Redirect for log-in y Portal IPV4 Address con la dirección IP y la URL del sitio del servidor específicas, respectivamente.




Configuración CLI para los pasos 2, 3 y 4:

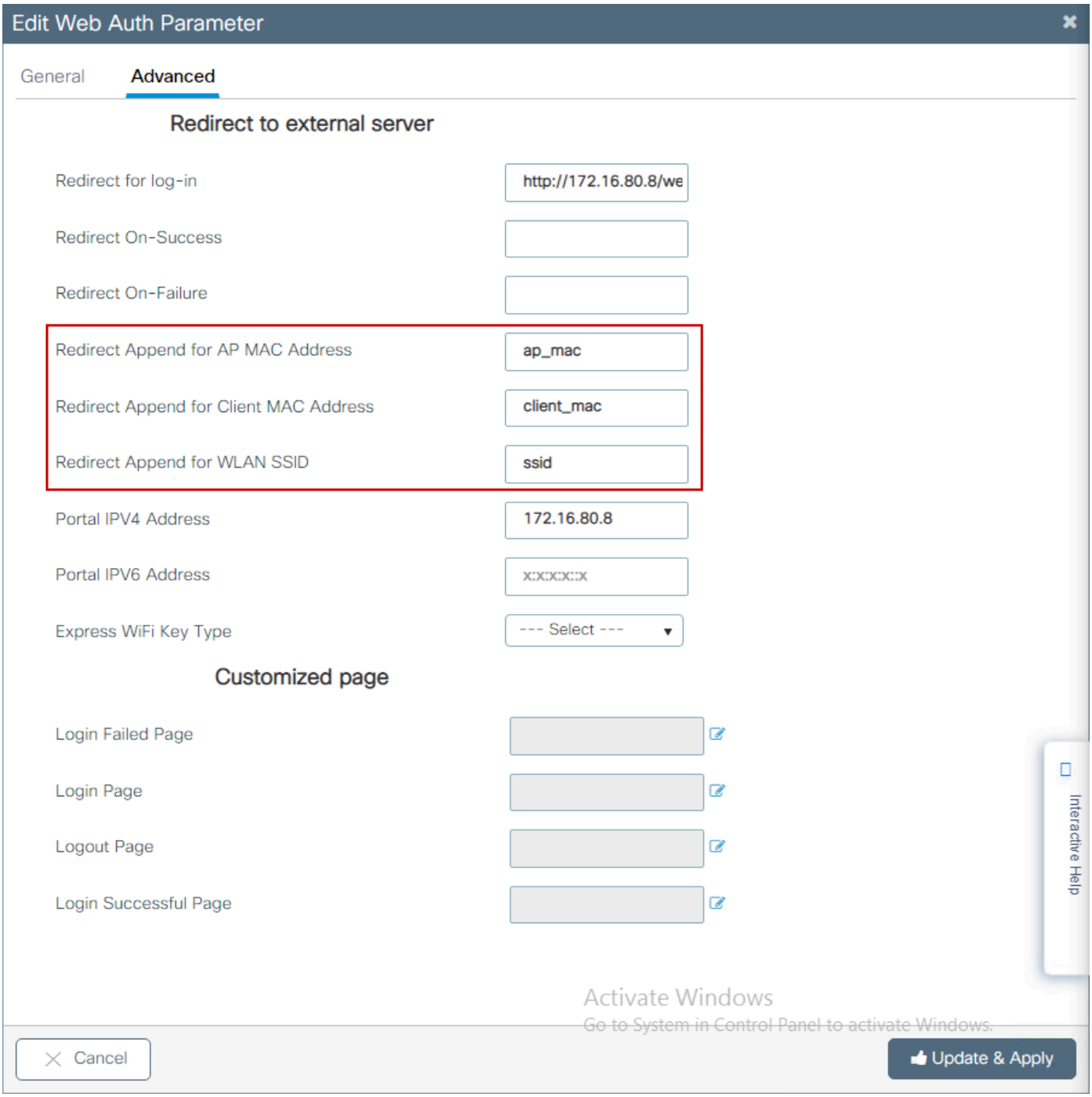
<#root>

```
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 Avanzado, y configure el nombre para 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




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_ma
```

Nota: al agregar la dirección IPV4 del portal información añade 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 de modo que se permita cualquier URL que coincida con una 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
```

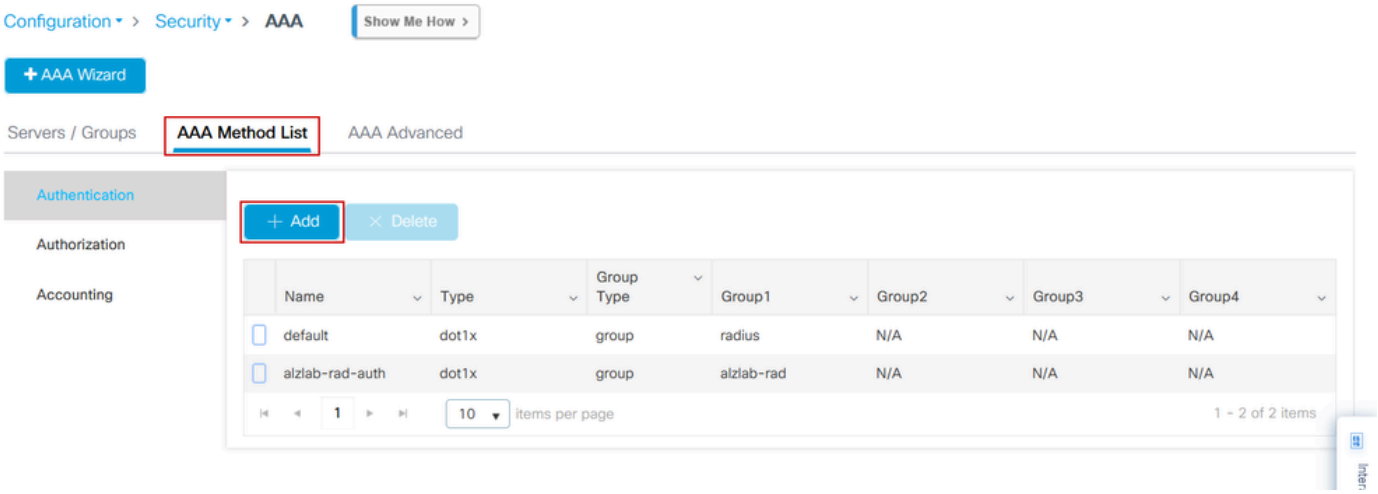
Servidor web externo

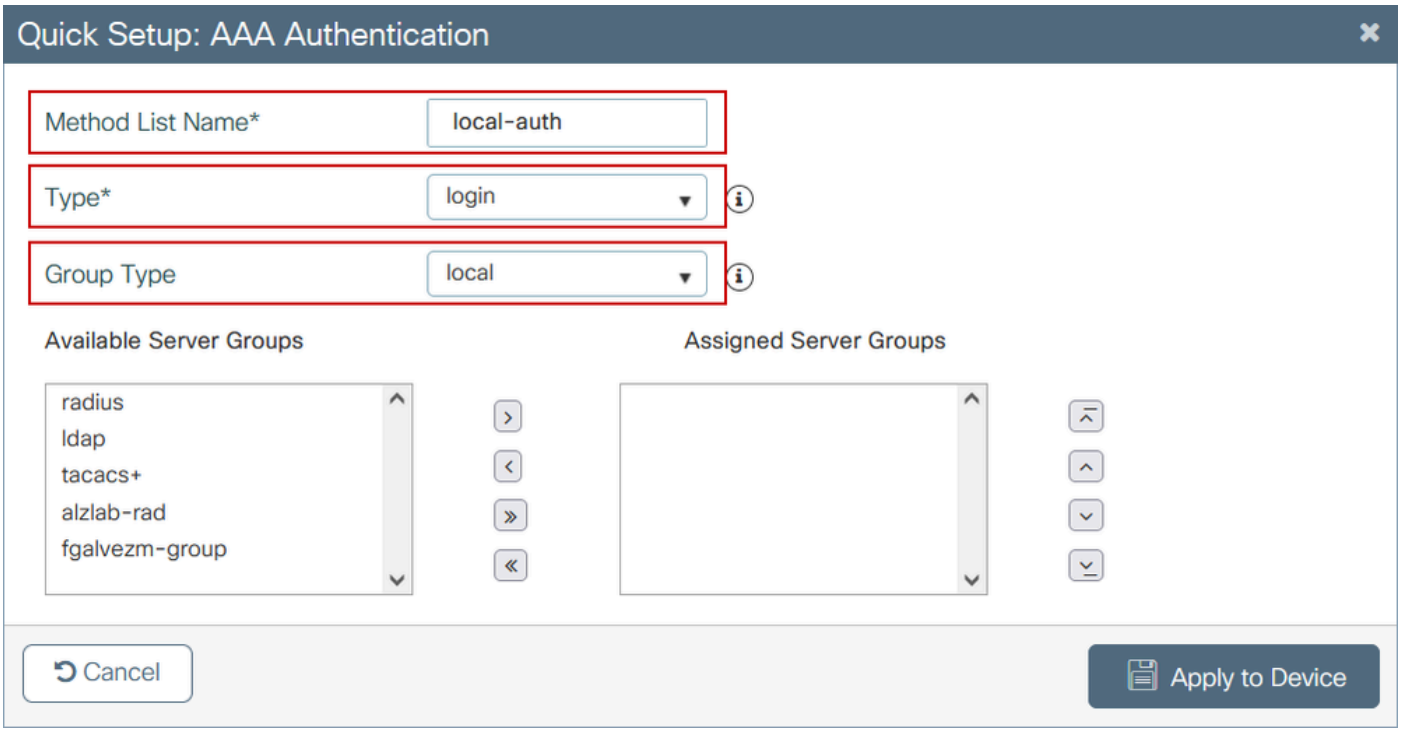
```
parameter-map type webauth <web-parameter-map-name>
 type webauth
 timeout init-state sec 300
 redirect for-login <URL-for-webauth>
 redirect portal ipv4 <external-server's-IP
 max-http-conns 10
```

## 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.

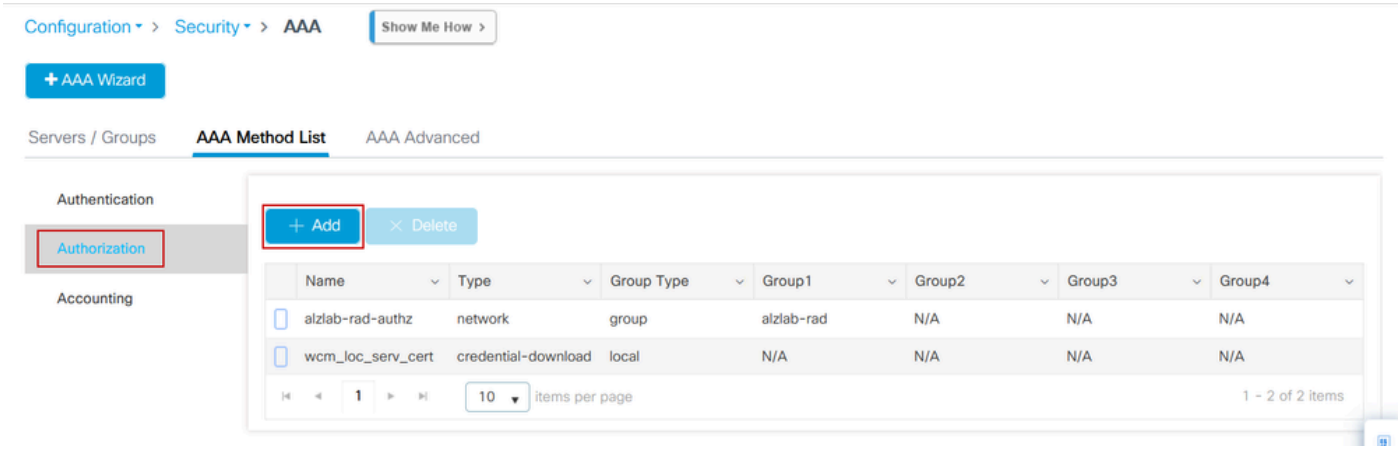
Paso 1. Navegue hasta Configuration > Security > AAA, luego seleccione AAA Method List. Configure una nueva lista de métodos, seleccione + Add y rellene los detalles de la lista; asegúrese de que Type esté configurado como "login" como se muestra en la imagen.

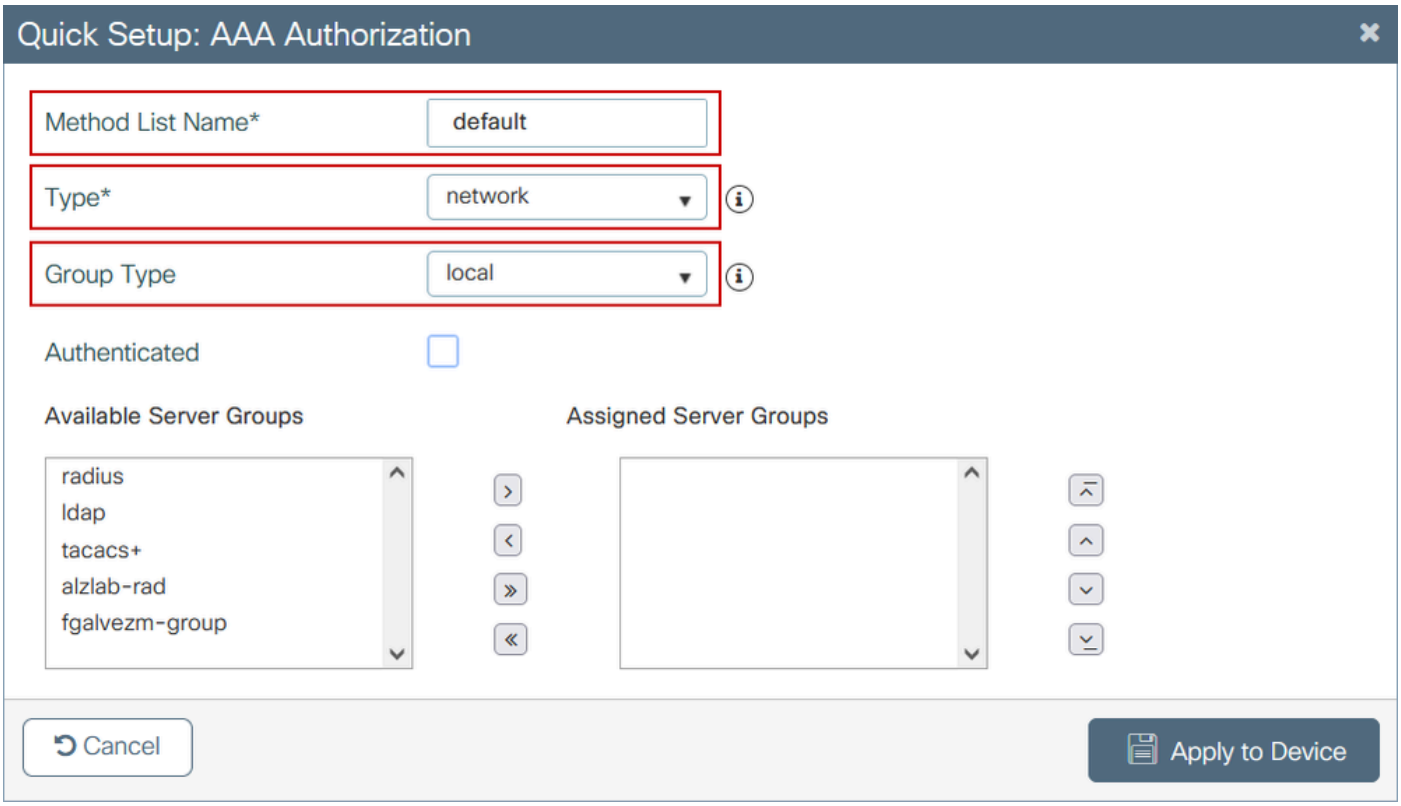





Paso 2. Seleccione Autorización y luego seleccione + Agregar para crear una nueva lista de métodos. Asígnele el nombre predeterminado con Type as network (Tipo como red), como se muestra en la imagen.

Nota: Como lo anuncia el controlador 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.






Configuración CLI para los pasos 1 y 2:

<#root>

```
9800(config)#
```

**aaa new-model**

```
9800(config)#
```

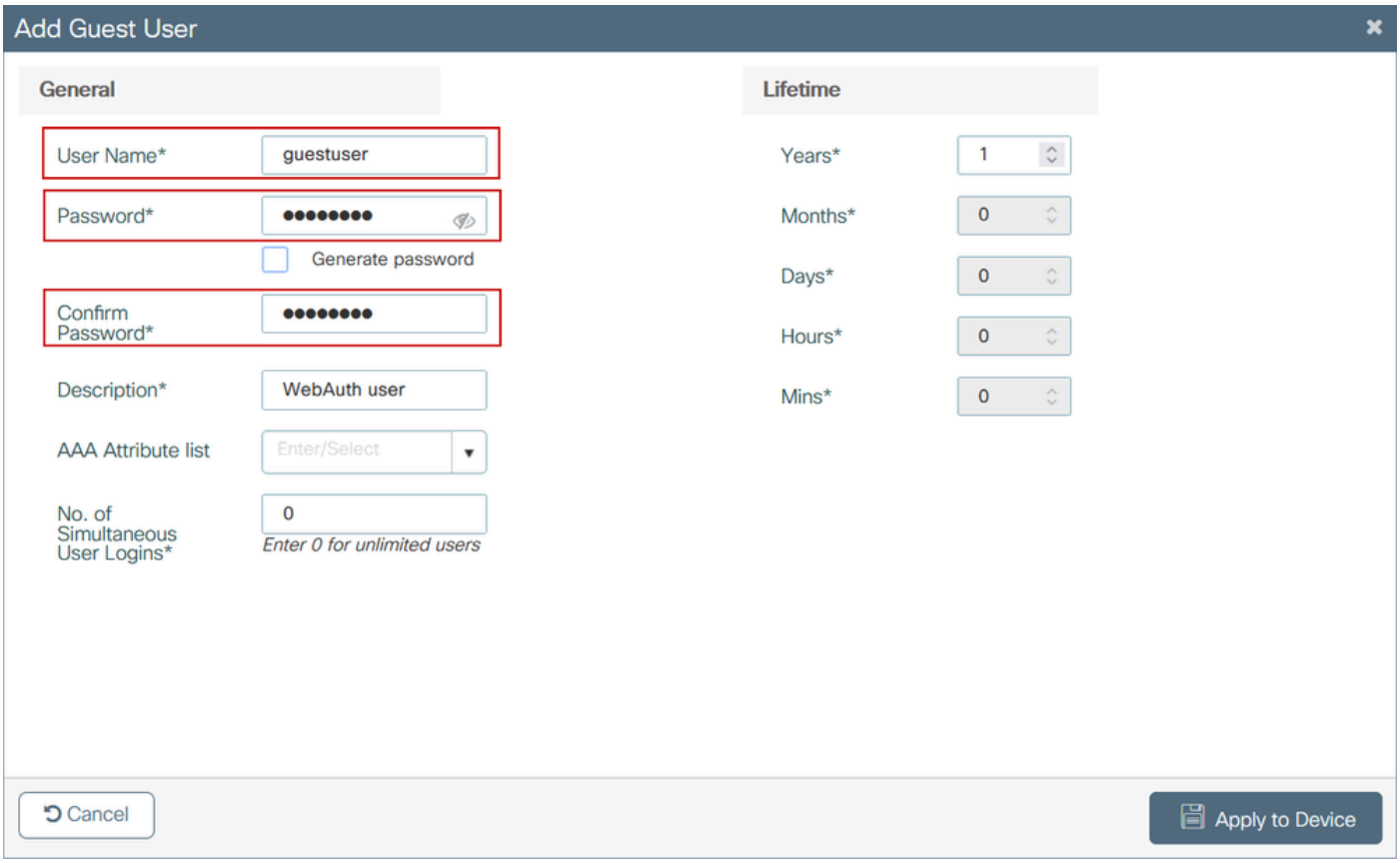
**aaa authentication login local-auth local**

```
9800(config)#
```

**aaa authorization network default local**

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

Paso 3. Navegue hasta Configuración > Seguridad > Usuario invitado. Seleccione + Agregar y configure los detalles de la cuenta de usuario invitado.




Configuración de CLI:

<#root>

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

9800(config-user-name)#
description "WebAuth user"

9800(config-user-name)#
password 0




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
```

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.

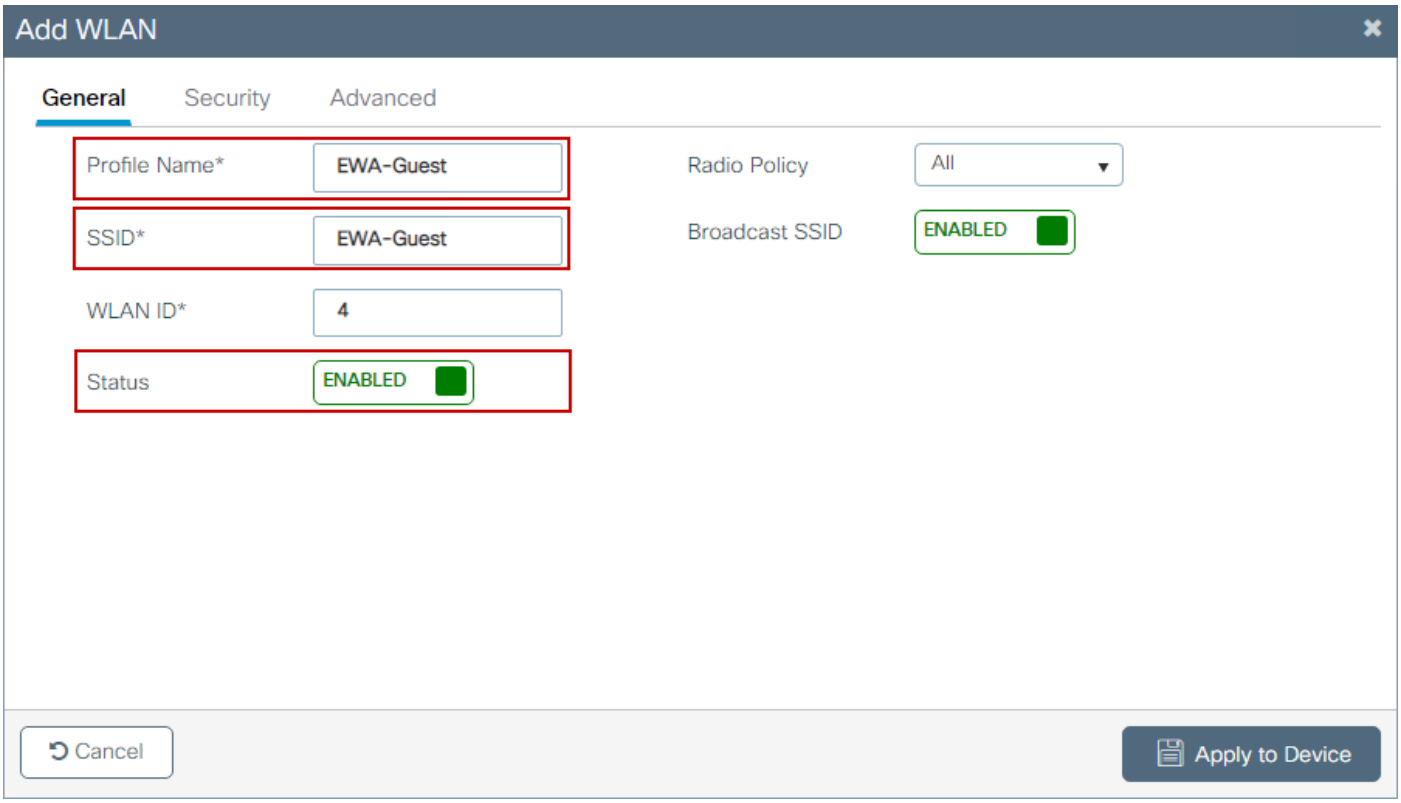
Las reglas de ACL creadas automáticamente son:

<#root>

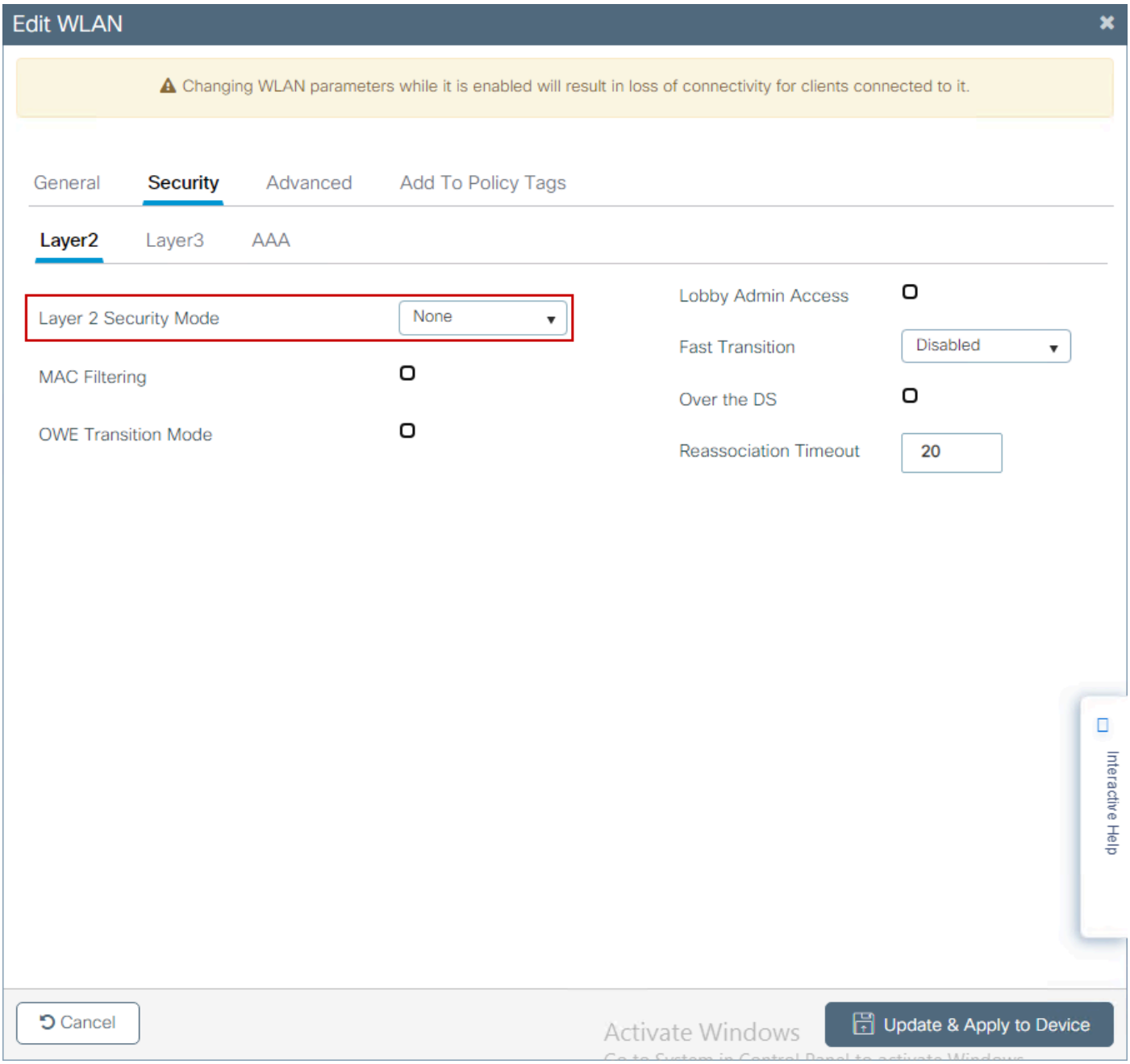
```
alz-9800#
show ip access-list

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
```

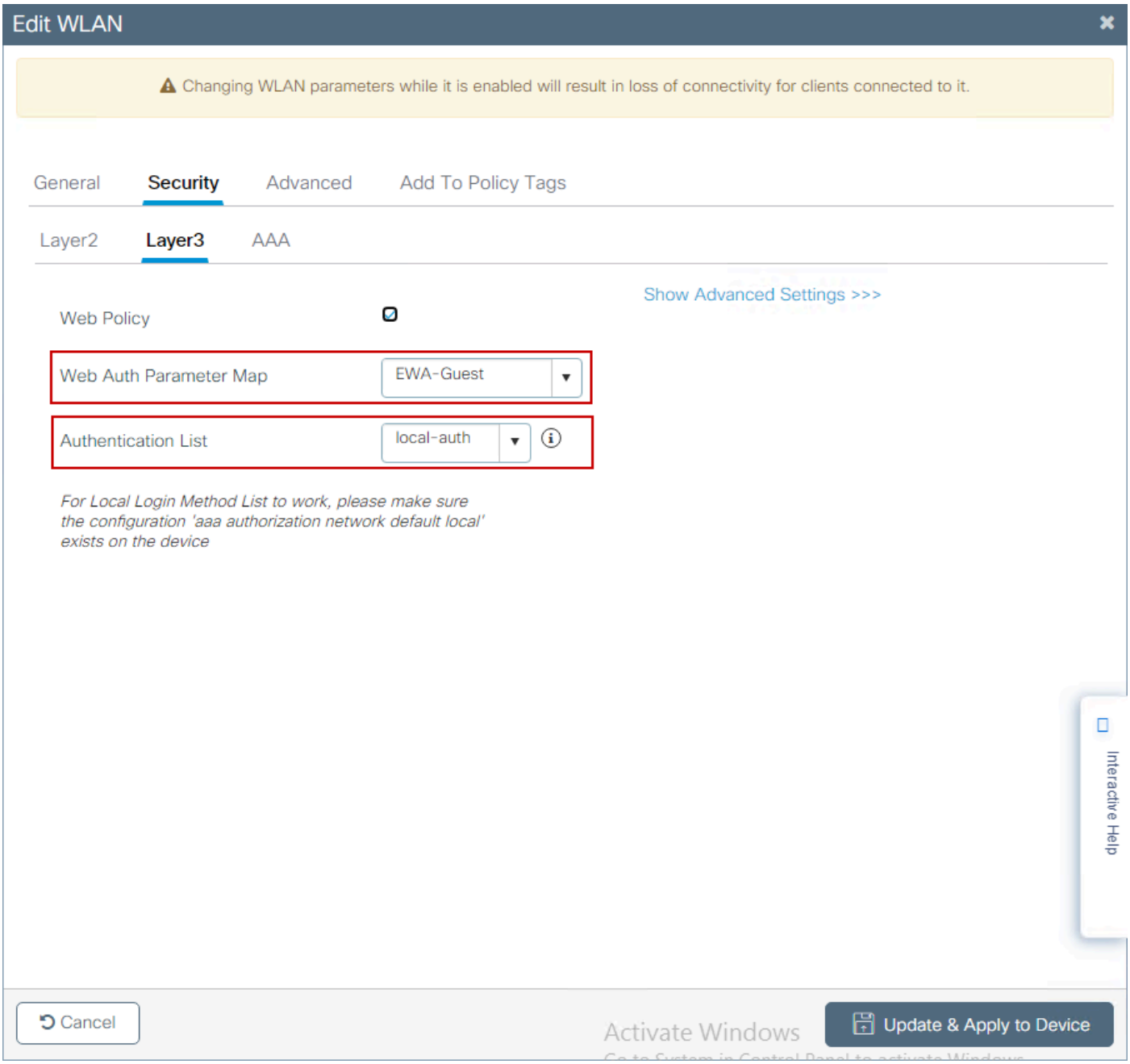
## Configurar políticas y etiquetas

Paso 1. Navegue hasta 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.




Paso 2. Seleccione la pestaña Seguridad y establezca la autenticación de la Capa 2 en Ninguno si no necesita ningún mecanismo de encripción 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.


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
Layer 2 Security Mode
None
MAC Filtering
OWE Transition Mode
Lobby Admin Access
Fast Transition
Disabled
Over the DS
Reassociation Timeout
20
Interactive Help
Cancel
Activate Windows
Update & Apply to Device



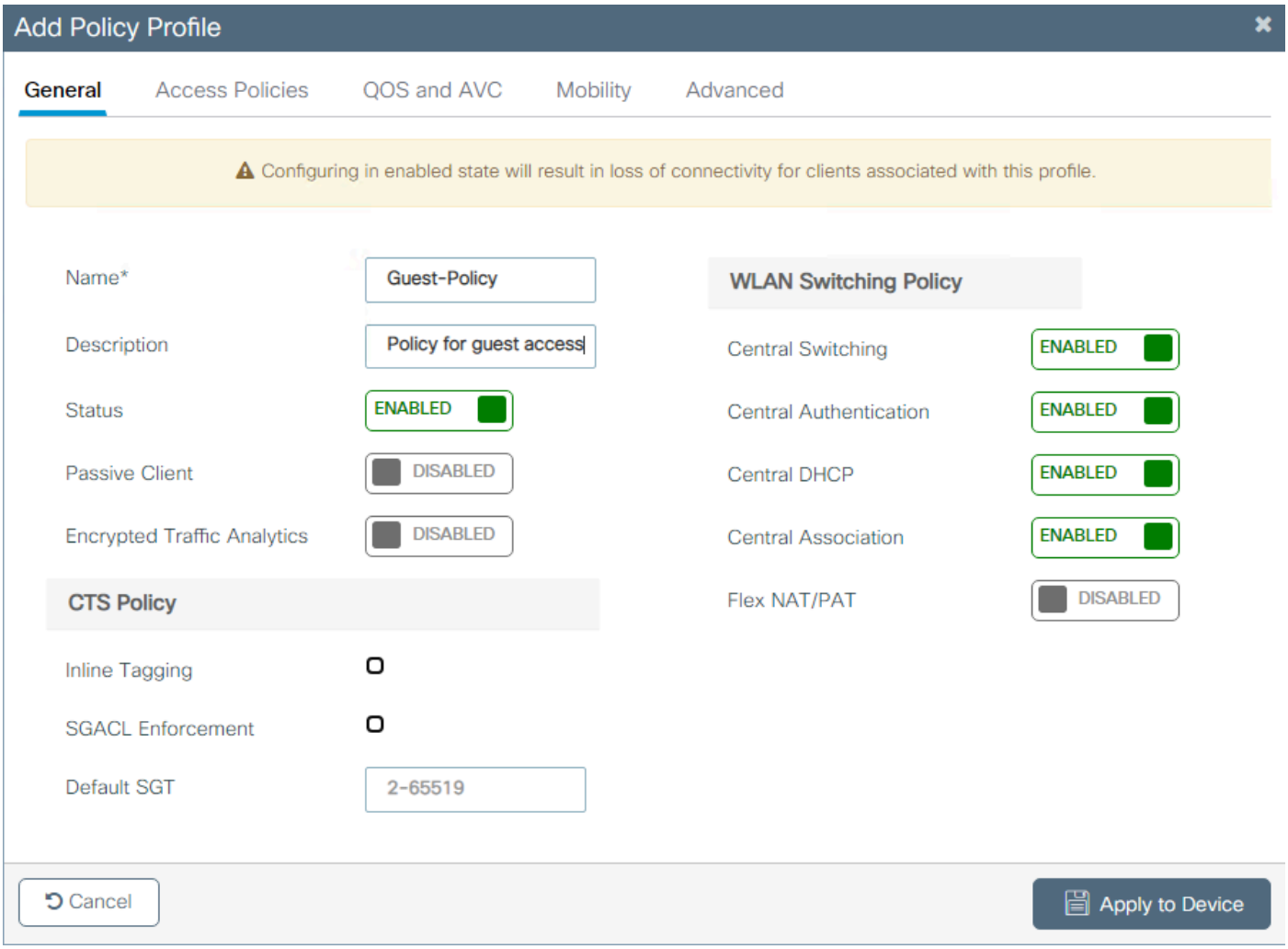

Configuraciones CLI:

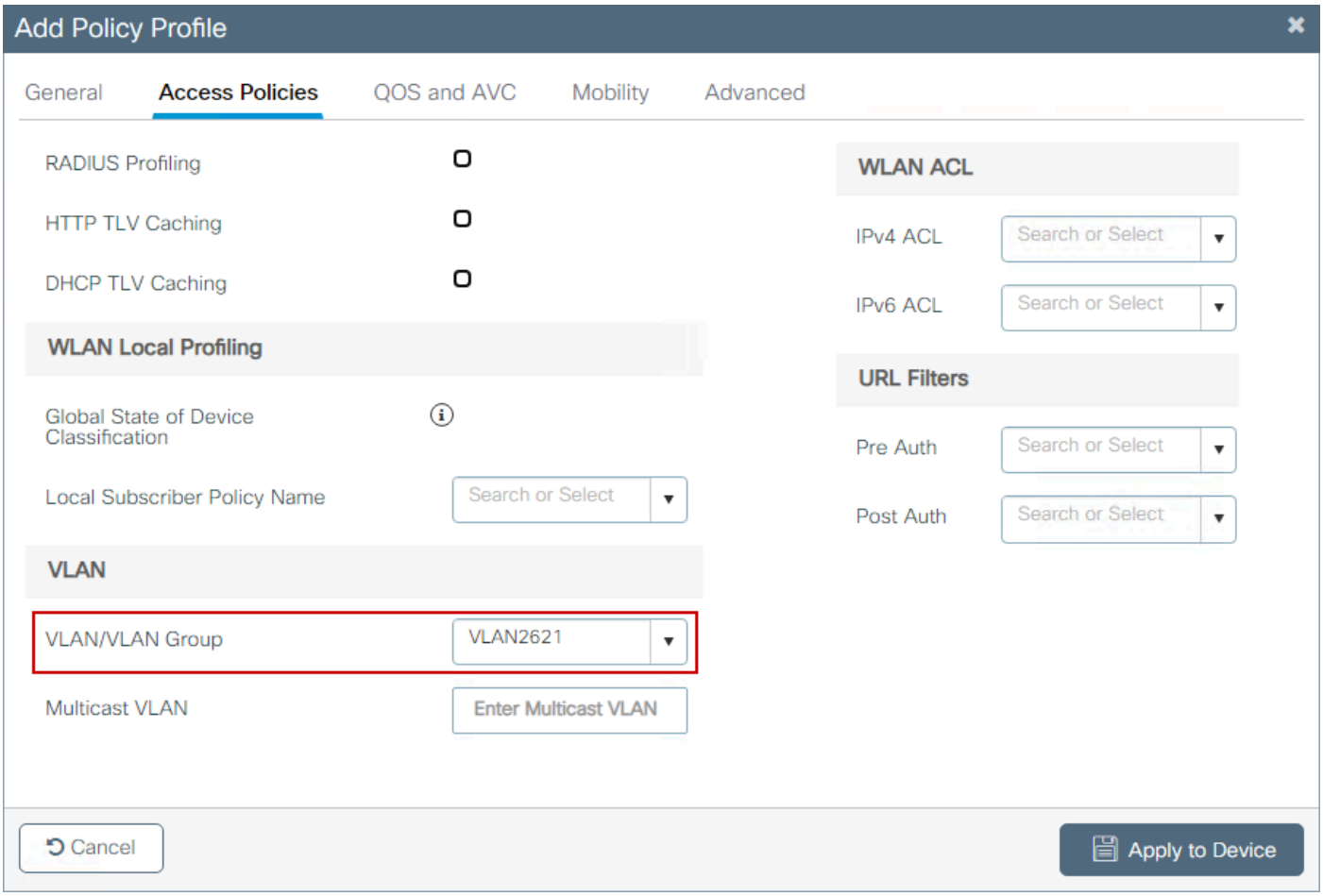
<#root>

```
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. Navegue hasta Configuración > Etiquetas y perfiles > Política y seleccione + Agregar. Definir 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.

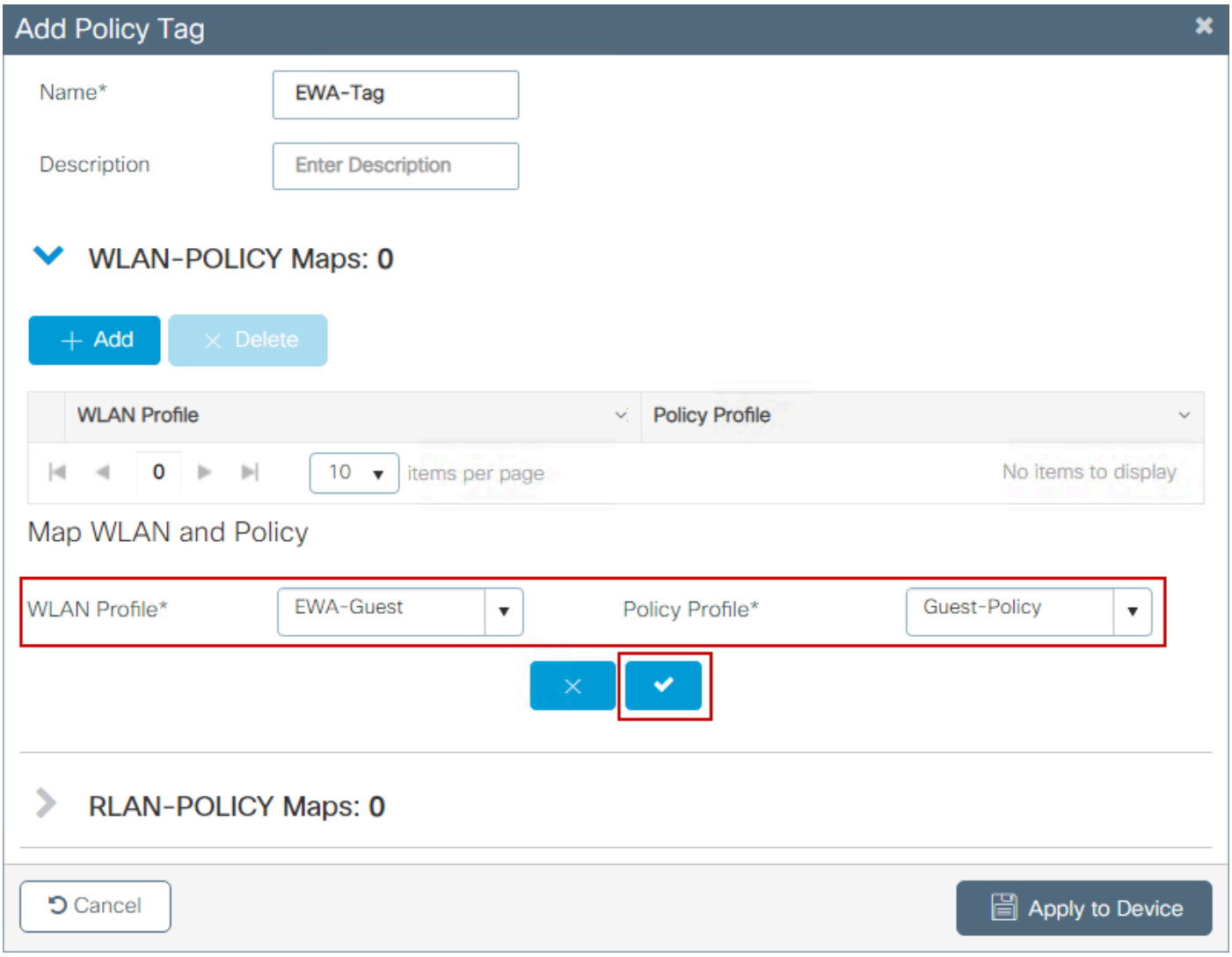

Add Policy Profile
General
Access Policies
QOS and AVC
Mobility
Advanced
Configuring in enabled state will result in loss of connectivity for clients associated with this profile.
Name*
Guest-Policy
Description
Policy for guest access
Status
ENABLED
Passive Client
DISABLED
Encrypted Traffic Analytics
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




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
```

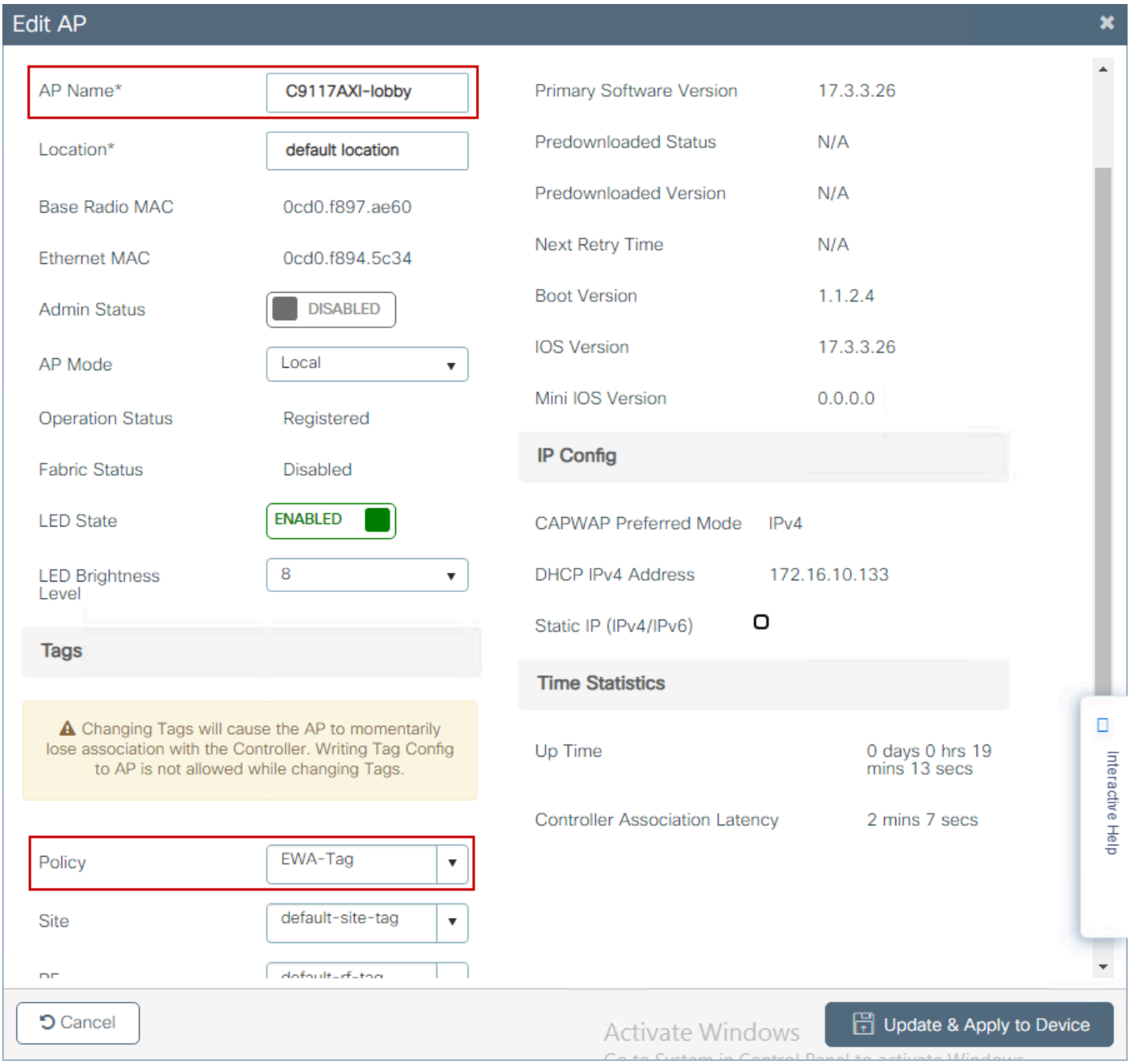
Paso 4. Navegue hasta Configuration > Tags & Profiles > Tags, dentro de la pestaña Policy seleccione + Add. Defina un nombre de etiqueta y, a continuación, en WLAN-POLICY Maps, seleccione + Add y agregue el perfil de política y WLAN creado anteriormente.




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.

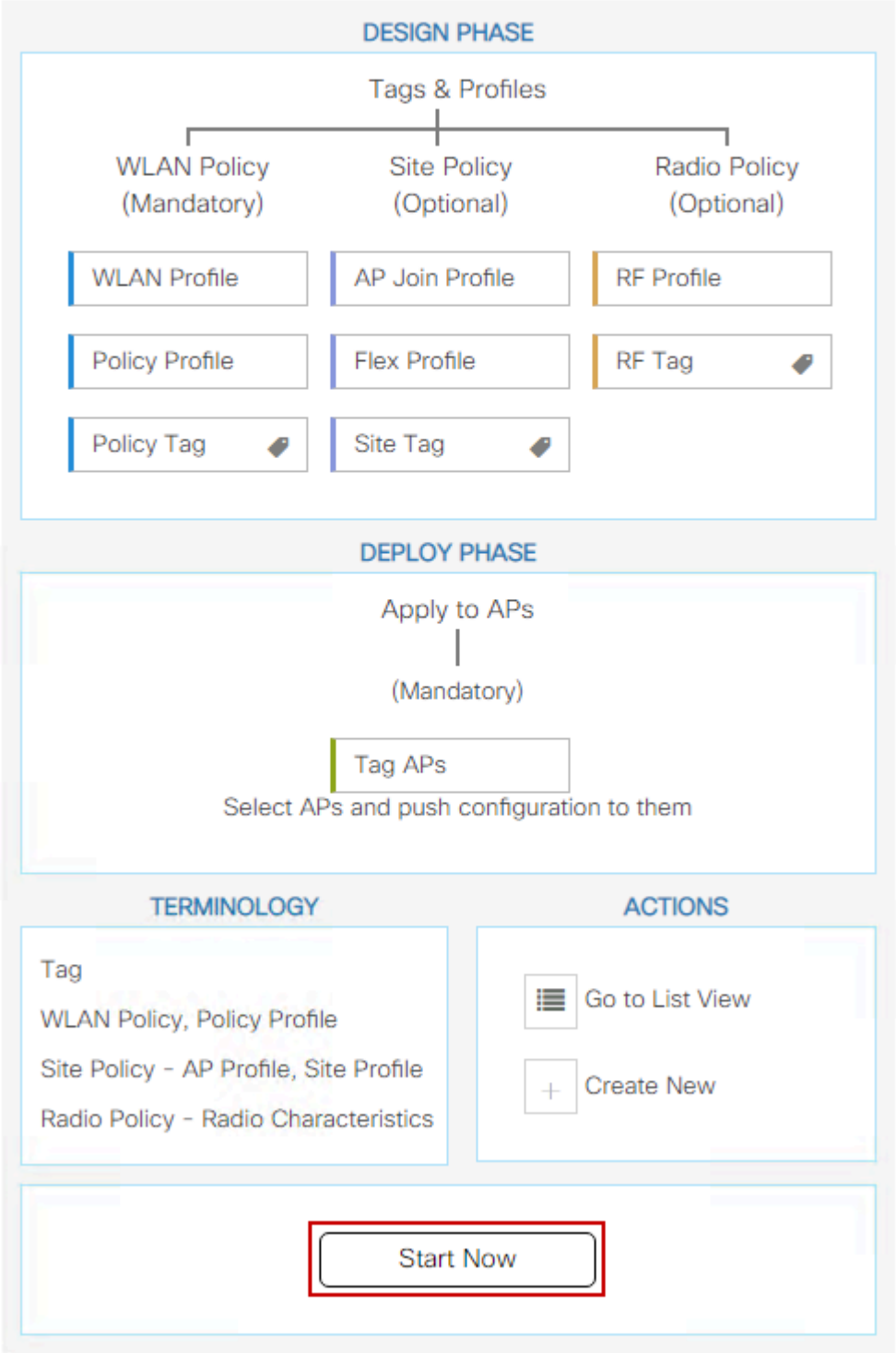


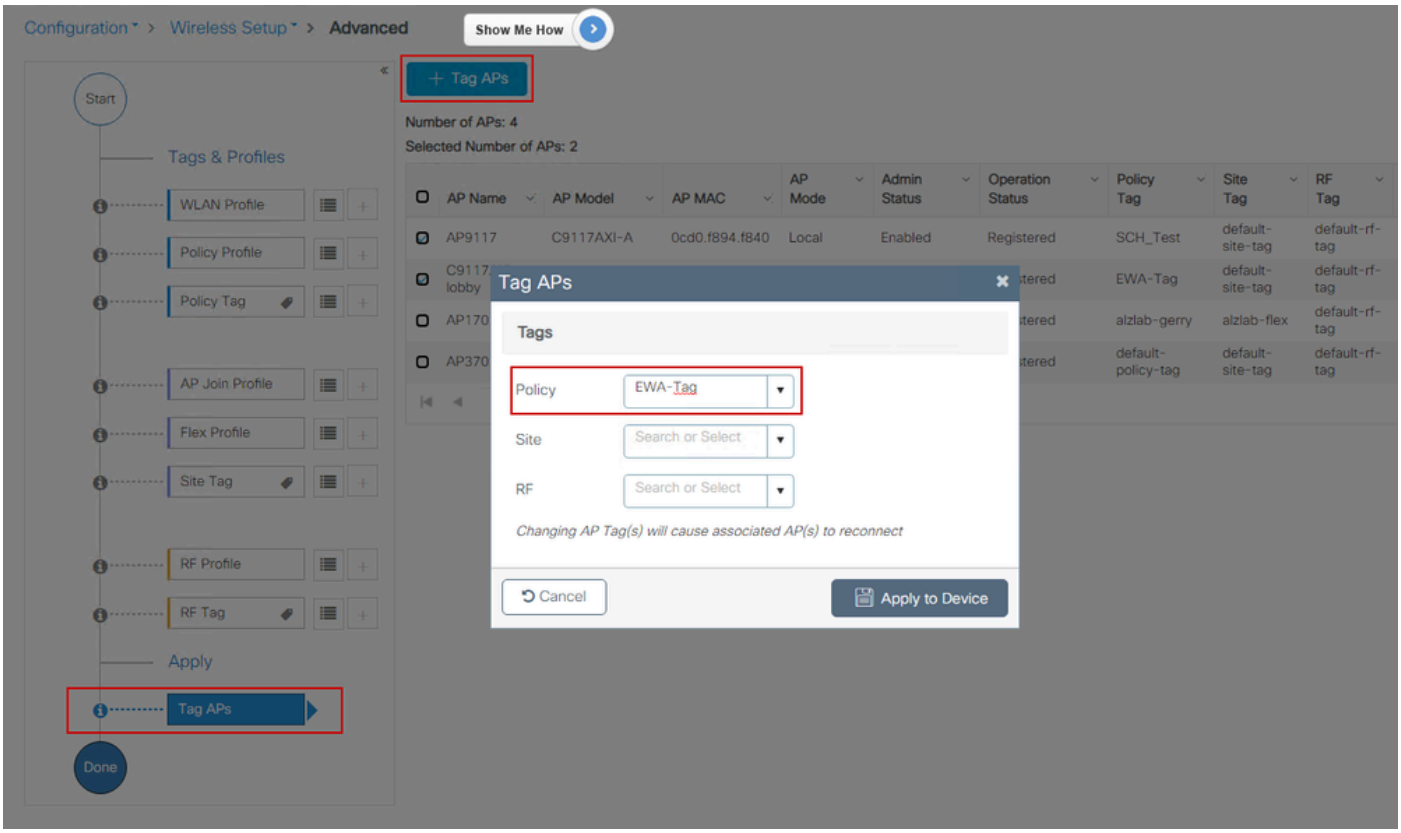

Si es necesario etiquetar varios AP al mismo tiempo, hay dos opciones disponibles:

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.

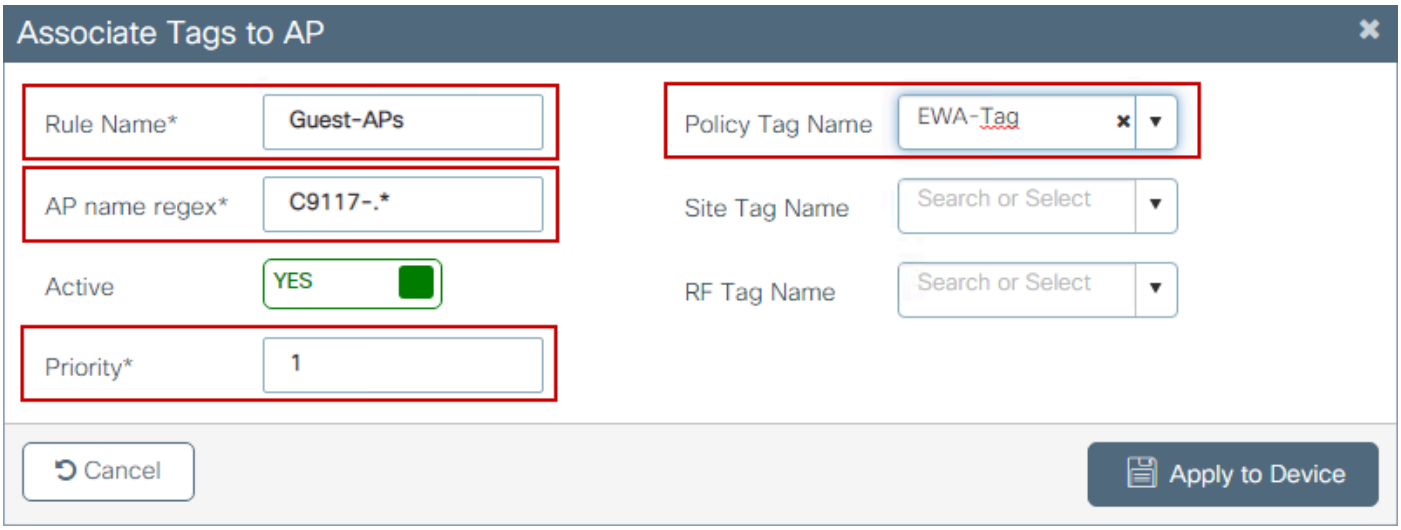
## Wireless Setup Flow Overview

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.






Opción B. Vaya a Configuración > Etiquetas y perfiles > Etiquetas. a continuación, seleccione la pestaña AP. En la ficha Filtro, seleccione + Agregar. 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.




# Verificación

Utilize 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**

**config general**

9800#

**show ap name**

**tag detail**

9800#

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

9800#

**show wireless tag policy detailed**

9800#

**show wireless profile policy detailed**

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**

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 0xf**

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**

**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: En función del 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. Verifique la hora actual del controlador para que pueda rastrear los registros en el tiempo hasta cuando ocurrió el problema.

```
<#root>

9800#

show clock
```

Paso 2. Recopile los syslogs del buffer del controlador o del syslog 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. Compruebe si se ha habilitado alguna condición de depuración.

<#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 en prueba no se incluyó como condición en el Paso 3. Recopile los seguimientos de nivel de aviso siempre activo para la dirección MAC específica.

<#root>

9800#

**show logging profile wireless filter [mac | ip] [**

**|**

**] to-file always-on-**

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

<#root>

9800#

**more bootflash:always-on-**

or
9800#

**copy bootflash:always-on-**

**tftp://**

**/**

**/always-on-**

## 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 Active (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



        {monitor-time



        }
```

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 el búfer interno para poder visualizarlos más tarde.

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

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

```
<#root>

9800#

no debug wireless mac
```

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 direcciones mac. Puede copiar el archivo .log de seguimiento de ra 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://**

**/ra-FILENAME.txt**

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] [**

**|**

**] to-file ra-internal-**

**.txt**

Nota: Este resultado del comando devuelve seguimientos para todos los niveles de registro y todos los procesos y es bastante voluminoso. Póngase en contacto con Cisco TAC para obtener ayuda con el análisis de estos seguimientos.

<#root>

9800#

**copy bootflash:ra-internal-**

**.txt tftp://**

**/ra-internal-**

```
.txt
```

Muestre el contenido:

```
<#root>
9800#
more bootflash:ra-internal-
```

```
.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

9800(config-ext-nacl)#
permit ip host

        any

9800(config-ext-nacl)#
permit ip any host

9800(config-ext-nacl)#
permit ip host

        any
```

Paso 2. Defina los parámetros de captura del 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
```

9800#

**monitor capture EWA access-list EWA-pcap**

9800#

**monitor capture EWA control-plane both 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**

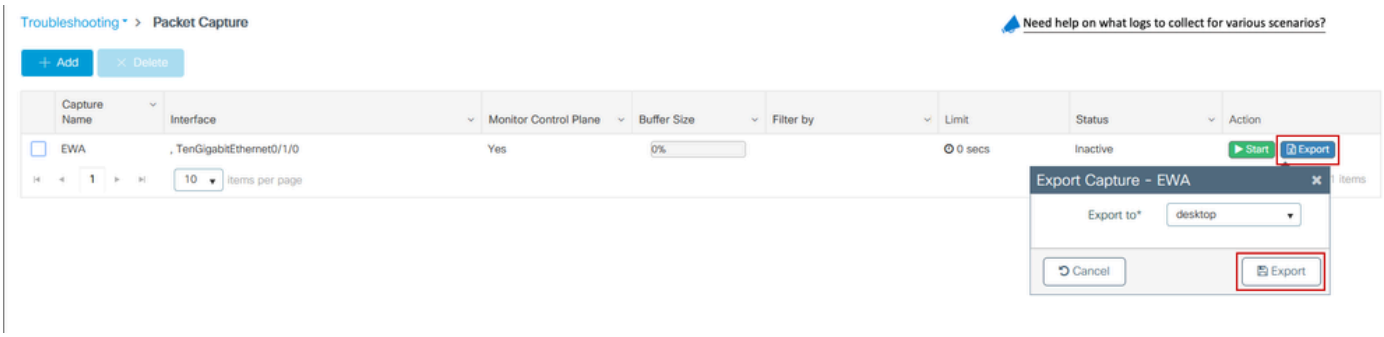
```
Started capture point : EWA
```

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.

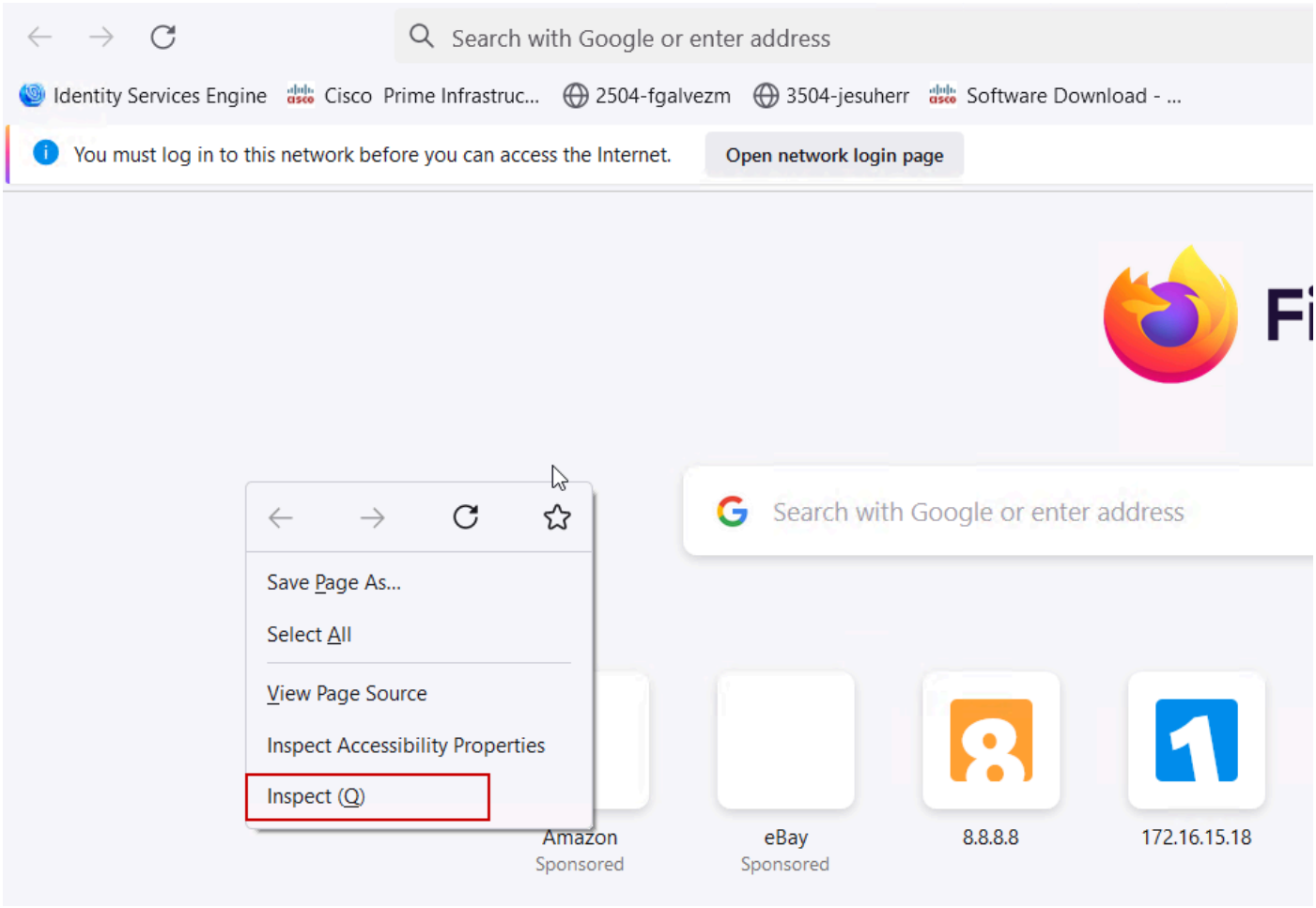
Solución de problemas del explorador HAR

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.).

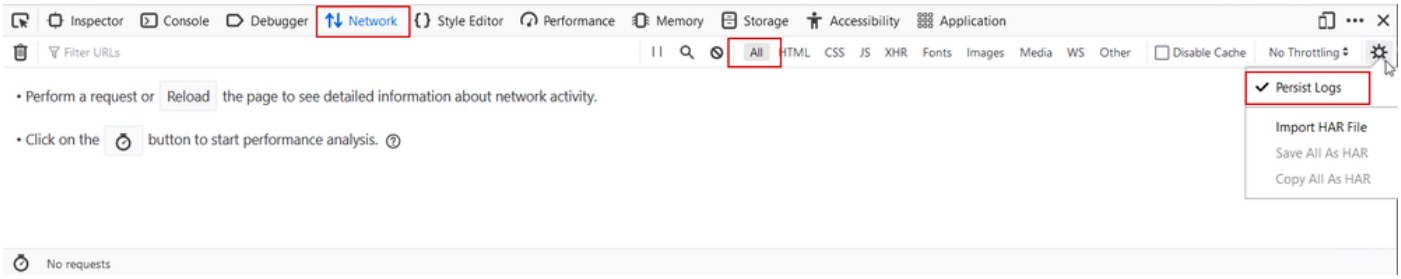
Los archivos HAR se pueden exportar desde el explorador cliente e importar en un explorador diferente para su posterior análisis. Este documento describe cómo recopilar el archivo HAR de Mozilla Firefox.

Paso 1. Abra Web Developer Tools con Ctrl + Shift + I, alternativamente haga clic con el botón

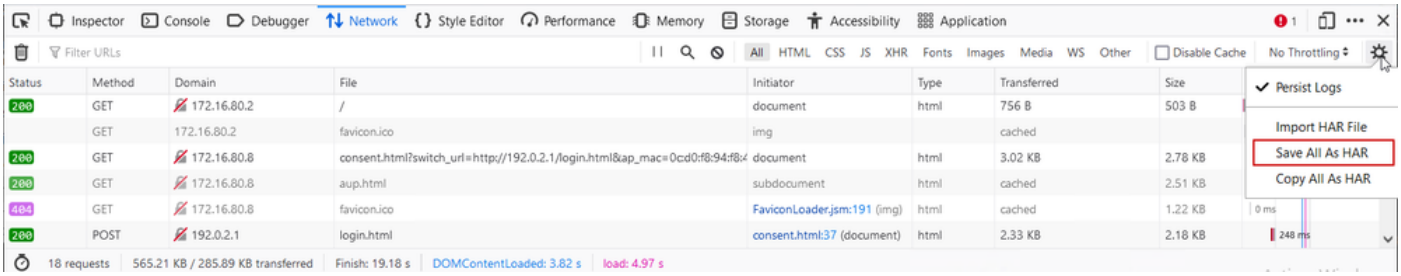
derecho dentro del contenido del navegador y seleccione Inspeccionar.




Paso 2. Vaya a Red, asegúrese de que esté 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.



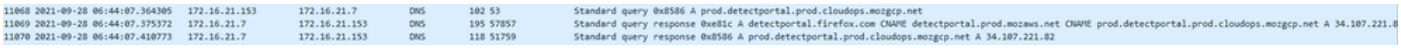

Paso 3. Reproduzca el problema y asegúrese de que el explorador registre todas las solicitudes. Una vez reproducido el problema, detenga el registro de la red, seleccione el icono del engranaje y seleccione Guardar todo como HAR.



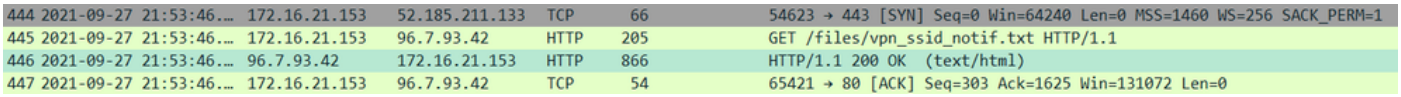

Captura de paquetes del lado cliente

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.

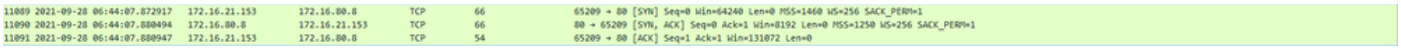
Solicitud de DNS:



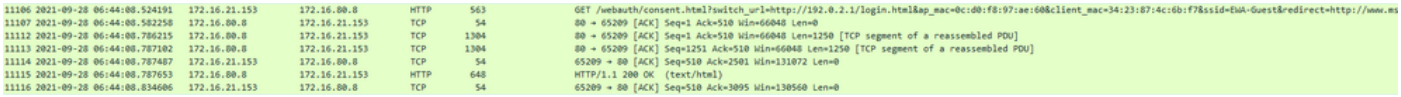

Protocolo de enlace TCP inicial y HTTP GET para redirección:



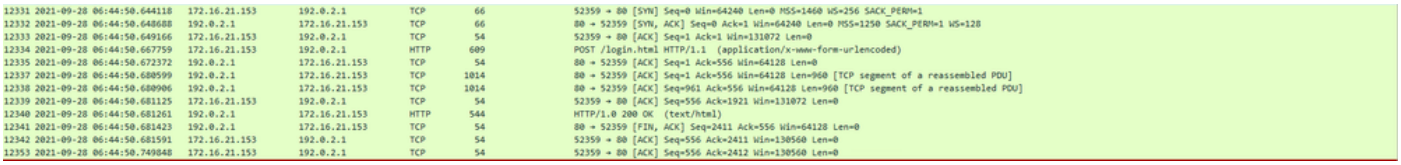

Protocolo de enlace TCP con servidor externo:




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




HTTP POST a IP virtual para autenticación:




## Ejemplo de un intento exitoso

Ésta es la salida de un intento de conexión exitoso desde la perspectiva de seguimiento de Radio Active; utilícela 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 Asso
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 WiFi
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 WiFi 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,
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-acl] [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-acl] [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_900000
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_9000000b[3423.874c
[...]
2021/09/28 13:01:29.859434 {wncd_x_R0-0}{1}: [webauth-httpd] [26328]: (info): capwap_9000000b[3423.874c
```

**POST rcvd when in LOGIN state**

```
2021/09/28 13:01:29.859636 {wncd_x_R0-0}{1}: [webauth-acl] [26328]: (info): capwap_9000000b[3423.874c.6
2021/09/28 13:01:29.860335 {wncd_x_R0-0}{1}: [webauth-acl] [26328]: (info): capwap_9000000b[3423.874c.6
2021/09/28 13:01:29.861092 {wncd_x_R0-0}{1}: [auth-mgr] [26328]: (info): [3423.874c.6bf7:capwap_900000
```

**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).