Configuración de Web Local con Autenticación Local en 9800 WLC

Contenido

Introducción

Este documento describe cómo configurar la autenticación Web local con autenticación local en un controlador LAN inalámbrico 9800 (WLC).

Prerequisites

Cisco recomienda que tenga conocimiento del modelo de configuración del WLC 9800.

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco WLC serie 9800.
- Conocimiento completo de la autenticación Web.

Componentes Utilizados

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

- 9800-CL WLC Cisco IOS® XE versión 17.12.5
- Punto de acceso Cisco C9117AXI.

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 local (LWA) es un método de autenticación de la red de área local inalámbrica (WLAN) que se puede configurar en el WLC. Cuando un usuario selecciona la WLAN de la lista de redes disponibles, se le redirige a un portal web. En este portal, en función de la configuración, se le puede solicitar al usuario que introduzca un nombre de usuario y una contraseña, que acepte una política de uso aceptable (AUP) o una combinación de ambas acciones para finalizar la conexión.

Para obtener información sobre los cuatro tipos de páginas de autenticación Web presentadas durante el proceso de inicio de sesión, refiérase a la guía Configure Local Web Authentication y revise las opciones disponibles para el tipo de autenticación Web. También puede consultar la guía Configure Local Web Authentication with External Authentication en la sección Types of Authentication .

Mapa de parámetro

El mapa de parámetro es un elemento de configuración esencial en un WLC que habilita la autenticación Web. Consta de un conjunto de configuraciones que gobiernan varias facetas del proceso de autenticación web, incluido el tipo de autenticación, las URL de redirección, los parámetros agregados, los tiempos de espera y las páginas web personalizadas. Para activar y administrar la autenticación basada en web para un SSID determinado, este mapa debe estar vinculado al perfil WLAN.

El controlador de LAN inalámbrica viene con un mapa de parámetro global predeterminado, pero los administradores tienen la opción de crear mapas de parámetro personalizados para personalizar el comportamiento de la autenticación Web según necesidades específicas.

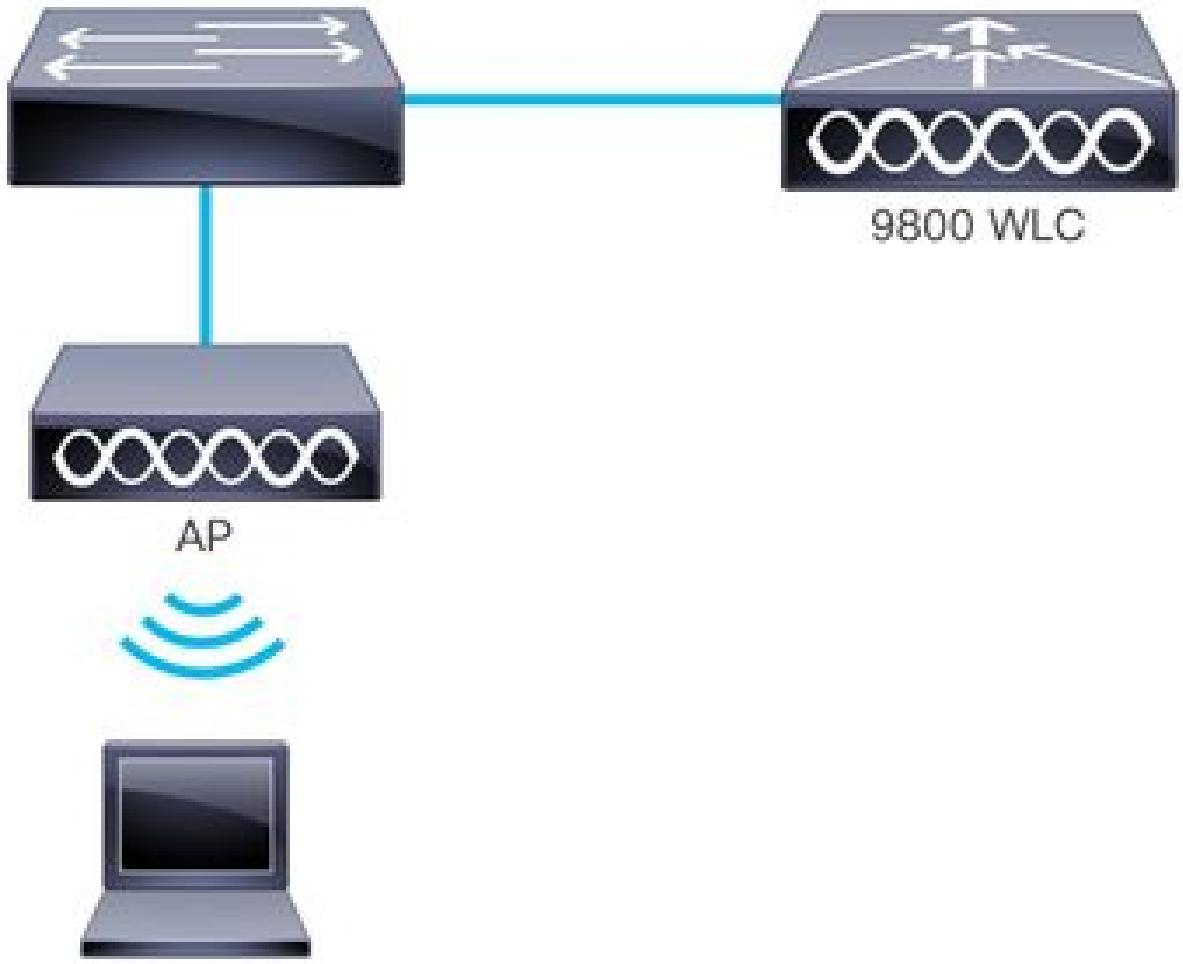
Base de datos para autenticación

Si el mapa de parámetro se configura para utilizar un nombre de usuario y una contraseña, debe definir las credenciales de autenticación, que se almacenan localmente en el WLC. Al crear una cuenta de usuario invitado a través de la GUI, puede establecer el número máximo de inicios de sesión simultáneos permitidos por cuenta de invitado. Los valores válidos oscilan entre 0 y 64,

donde 0 indica que se permiten inicios de sesión simultáneos ilimitados para ese usuario invitado.

LWA se ha diseñado principalmente para implementaciones pequeñas. Es compatible con la integración con otros métodos de autenticación, puede verificar la Combinación de autenticaciones admitidas para un cliente para obtener más información.

La imagen representa una topología genérica de LWA:



Topología genérica de LWA con autenticación local

Dispositivos en la topología de red de LWA:

- Cliente/Suplicante: Inicia la solicitud de conexión a la WLAN, más tarde a los servidores DHCP y DNS, y responde a las comunicaciones del WLC.
- Punto de acceso: conectado a un switch, transmite la WLAN del invitado y proporciona conectividad inalámbrica a los dispositivos invitados. Permite el tráfico DHCP y DNS antes de que el usuario invitado complete la autenticación mediante la introducción de credenciales válidas, la aceptación de una PUA o una combinación de ambas acciones.
- WLC/Autenticador: Administra los puntos de acceso y los dispositivos cliente. El WLC aloja

la URL de redirección y aplica la Lista de control de acceso (ACL) que gobierna el tráfico y su creación por defecto al configurar el mapa de parámetro. Intercepta solicitudes HTTP de usuarios invitados y los redirige a un portal web (página de inicio de sesión) donde los usuarios deben autenticarse. El WLC captura las credenciales del usuario, autentica a los invitados, y verifica la base de datos local para verificar la validez de las credenciales.

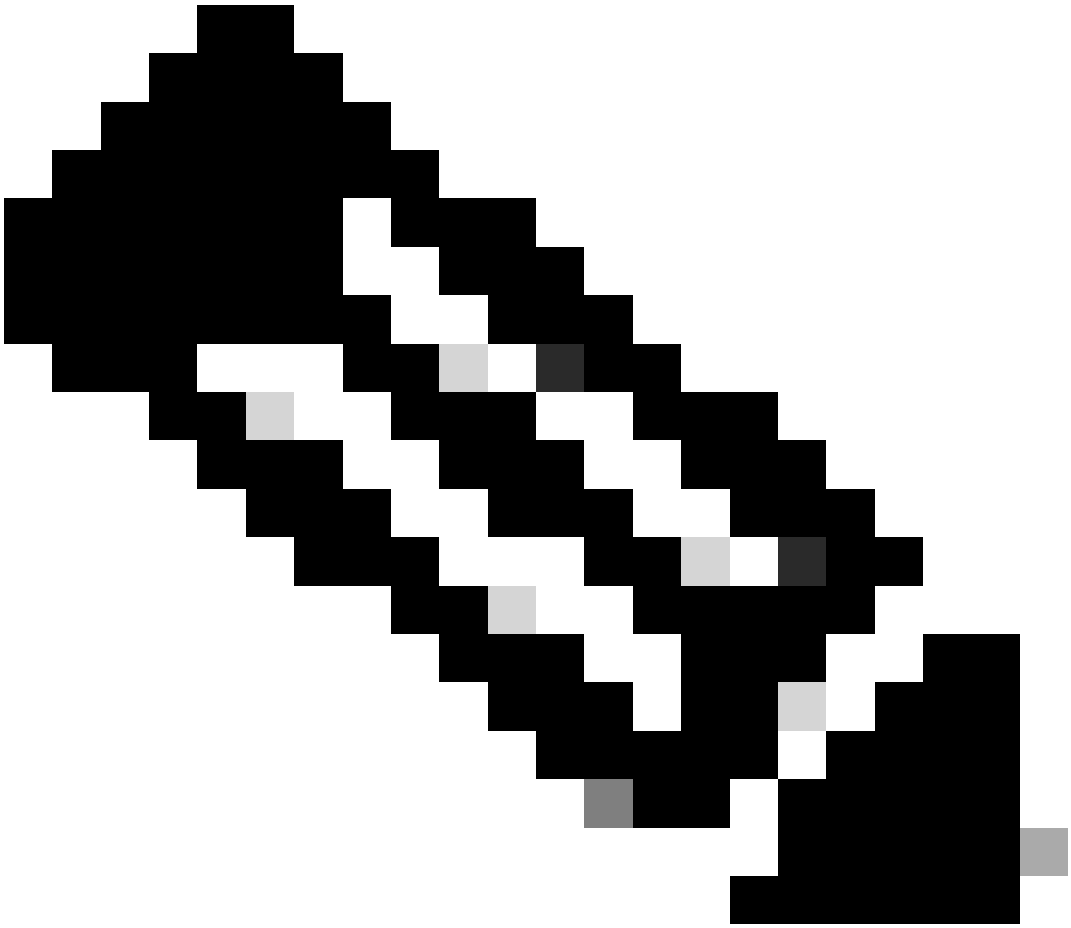
- Servidor de autenticación: En este escenario, el WLC funciona como el servidor de autenticación. Valida las credenciales de usuario invitado y concede o deniega el acceso a la red en consecuencia.

Configurar

Autenticación Web Local con Autenticación Local en la CLI

Listas de métodos para autenticación local

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#aaa new-model
9800WLC(config)#aaa authentication login LWA_AUTHENTICATION local
9800WLC(config)#aaa authorization network default local
9800WLC(config)#end
```



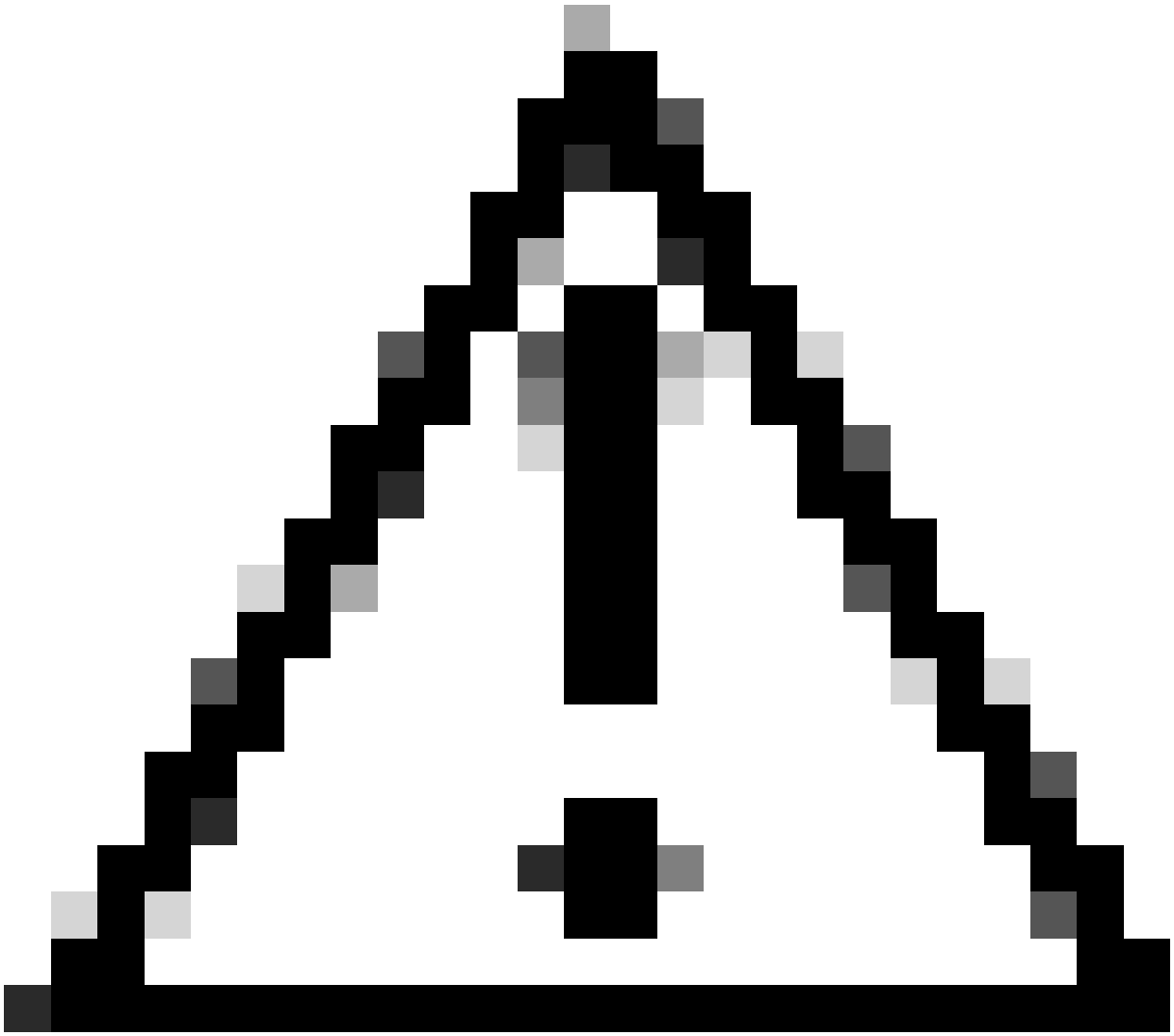
Nota: Para que la lista de métodos de inicio de sesión local funcione, asegúrese de que la configuración aaa authorization network default local exista en el WLC. Esto es necesario ya que el WLC autoriza al usuario en la red.

Mapas de parámetro

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#parameter-map type webauth global
9800WLC(config-params-parameter-map)#type webauth
9800WLC(config-params-parameter-map)#virtual-ip ipv4 192.0.2.1
9800WLC(config-params-parameter-map)#trustpoint
```

```
9800WLC(config-params-parameter-map)#webauth-http-enable
```

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



Precaución: La IP virtual debe ser una dirección no enrutable propuesta en RFC 5737. De forma predeterminada, el IP 192.0.2.1 está configurado. Vea más información sobre la dirección IP virtual en Prácticas recomendadas de configuración de Cisco Catalyst serie 9800. En AireOs la mayor parte del tiempo la IP utilizada fue 1.1.1.1. Esto ya no se recomienda ya que se convirtió en una IP pública.

La capacidad de crear múltiples mapas de parámetros permite flujos personalizados: páginas web personalizadas y parámetros de presentación específicos para cada WLAN. El mapa de parámetro global determina el Trustpoint y, por lo tanto, el certificado que el WLC presenta al cliente en el portal de redirección. Además, controla los tipos de tráfico de cliente interceptados,

como HTTP/HTTPS para el portal de redirección, el dominio o la resolución de nombres de host para la dirección IP virtual. Esta separación permite que el mapa global maneje configuraciones generales como la presentación de certificados y la interceptación de tráfico, mientras que los mapas de parámetros definidos por el usuario proporcionan una experiencia granular por WLAN.

Parámetros de seguridad de WLAN

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#wlan LWA_LA 1 "LWA LA"
9800WLC(config-wlan)#no security wpa
9800WLC(config-wlan)#no security wpa wpa2
9800WLC(config-wlan)#no security wpa wpa2 ciphers aes
9800WLC(config-wlan)#no security wpa akm dot1x
9800WLC(config-wlan)#security web-auth
9800WLC(config-wlan)#security web-auth authentication-list LWA_AUTHENTICATION
9800WLC(config-wlan)#security web-auth parameter-map global
9800WLC(config-wlan)#no shutdown
9800WLC(config-wlan)#end
```

Crear un perfil de política

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#wireless profile policy
```

```
9800WLC(config-wireless-policy)#vlan
```

```
9800WLC(config-wireless-policy)#no shutdown
```

```
9800WLC(config-wireless-policy)#end
```

Crear una etiqueta de directiva

```
9800WLC>enable
9800WLC#configure terminal
```

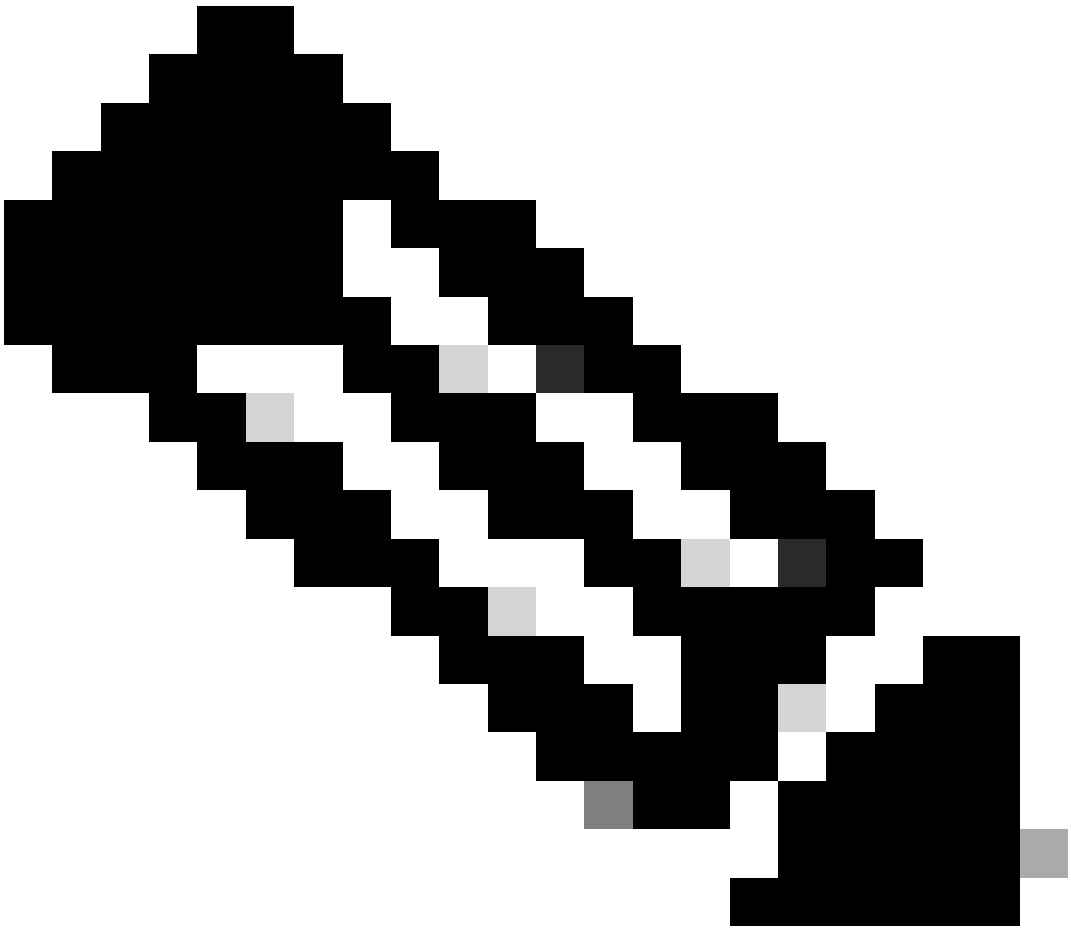
```
9800WLC(config)#wireless tag policy


9800WLC(config-policy-tag)#wlan LWA_LA policy


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

Asignar una etiqueta de política a un AP

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#ap


       >


9800WLC(config-ap-tag)#policy-tag POLICY_TAG


9800WLC(config-ap-tag)#end
```

Crear nombre de usuario de invitado

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#user-name johndoe
9800WLC(config-user-name)#description Guest-User
9800WLC(config-user-name)#password 0 Cisco123
9800WLC(config-user-name)#type network-user description


        guest-user lifetime year 0 month 11 day 30 hour 23


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

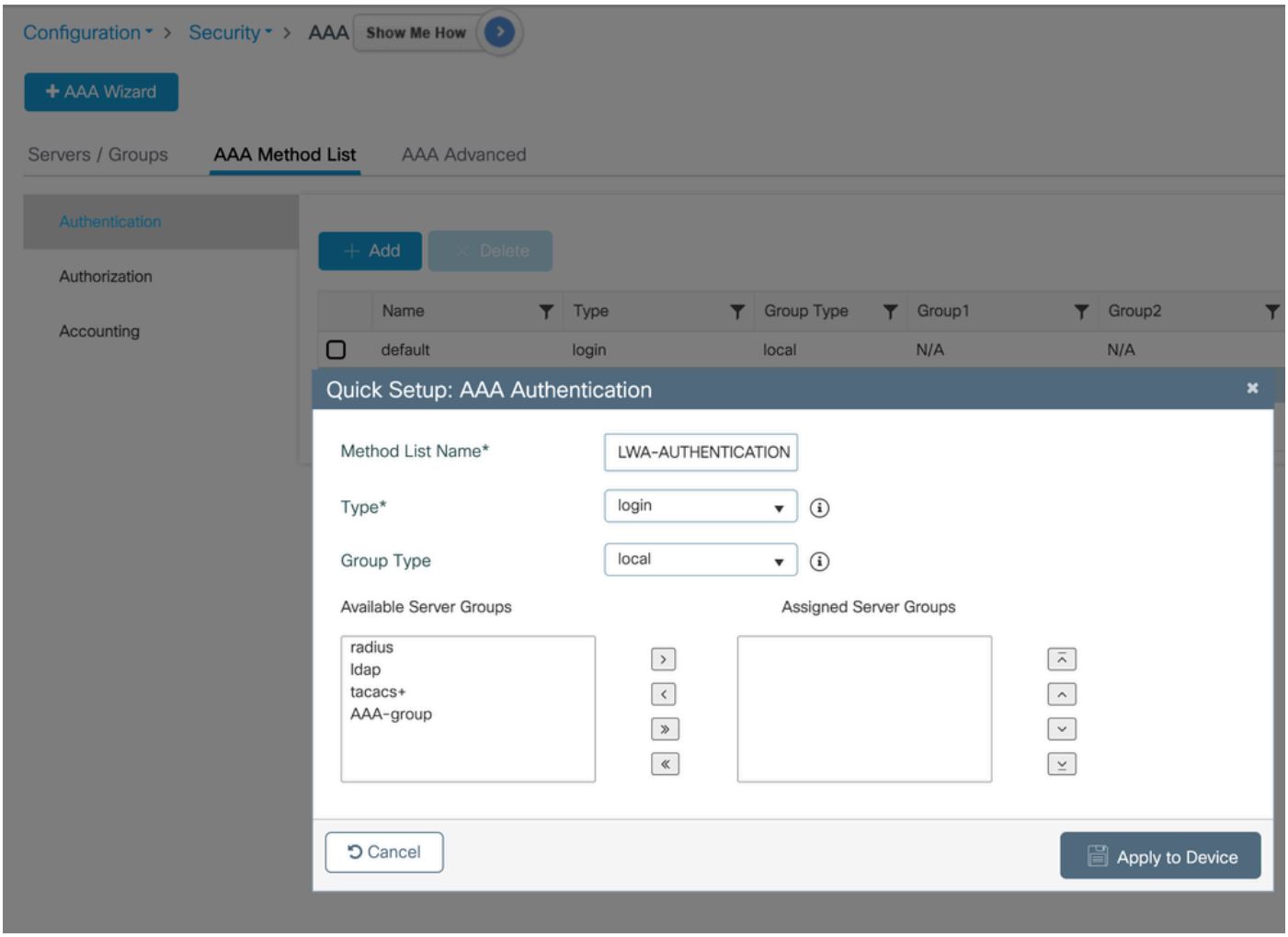


Nota: Al establecer la duración para el usuario invitado, si el año está establecido en 1, no puede especificar los parámetros siguientes: meses, días, horas y minutos, ya que la duración máxima es de 1 año.

Autenticación Web Local con Autenticación Local a través de WebUI

Listas de métodos para autenticación local

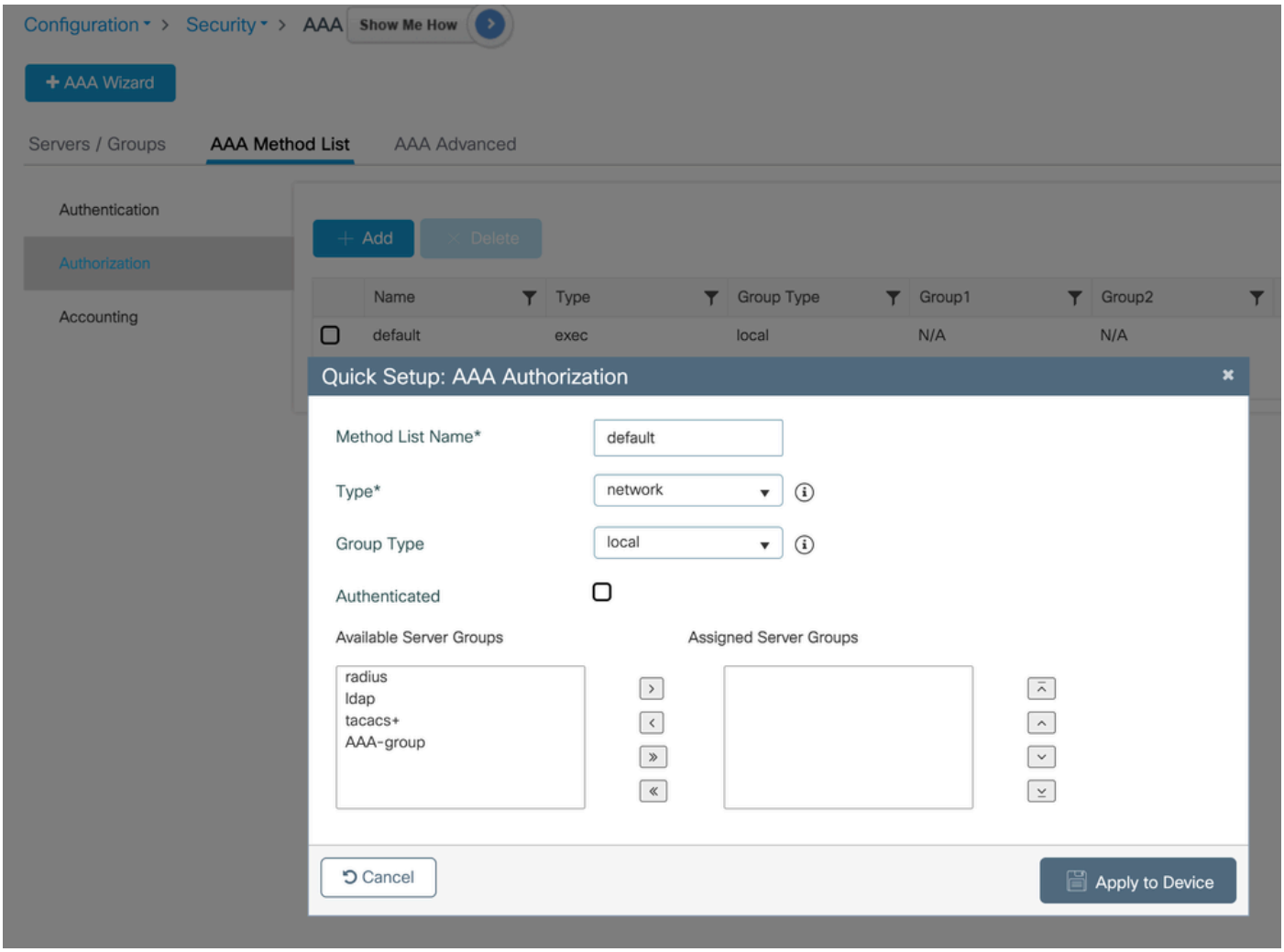
Vaya a Configuration > Security > AAA > AAA Method List > Authentication > Add para crear la lista de métodos que se utilizará más adelante en la configuración WLAN.



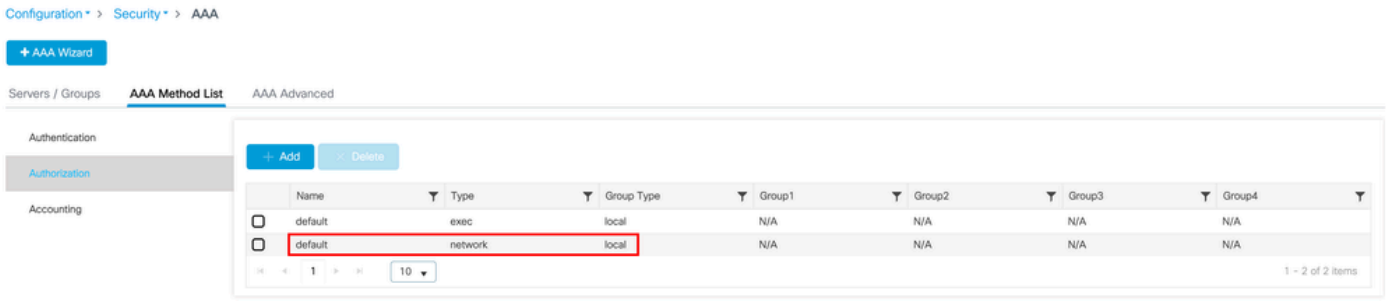
Después de hacer clic en Apply to Device, confirme la creación de la lista de métodos AAA:

Asegúrese de que haya una lista de métodos de autorización local; se trata de un requisito para que la lista de métodos de inicio de sesión local creada funcione.

Configuration > Security > AAA > AAA Method List > Authorization > Add

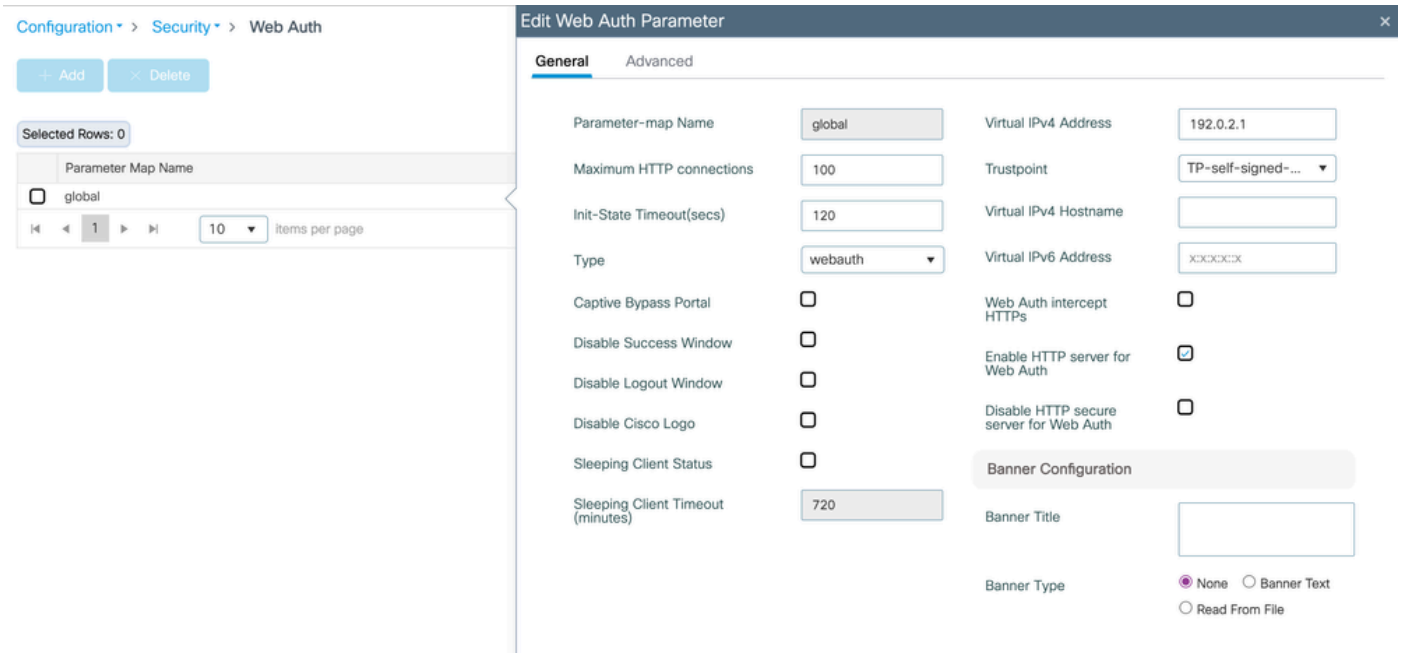


Después de hacer clic en Apply to Device, confirme la creación de la lista de métodos AAA:

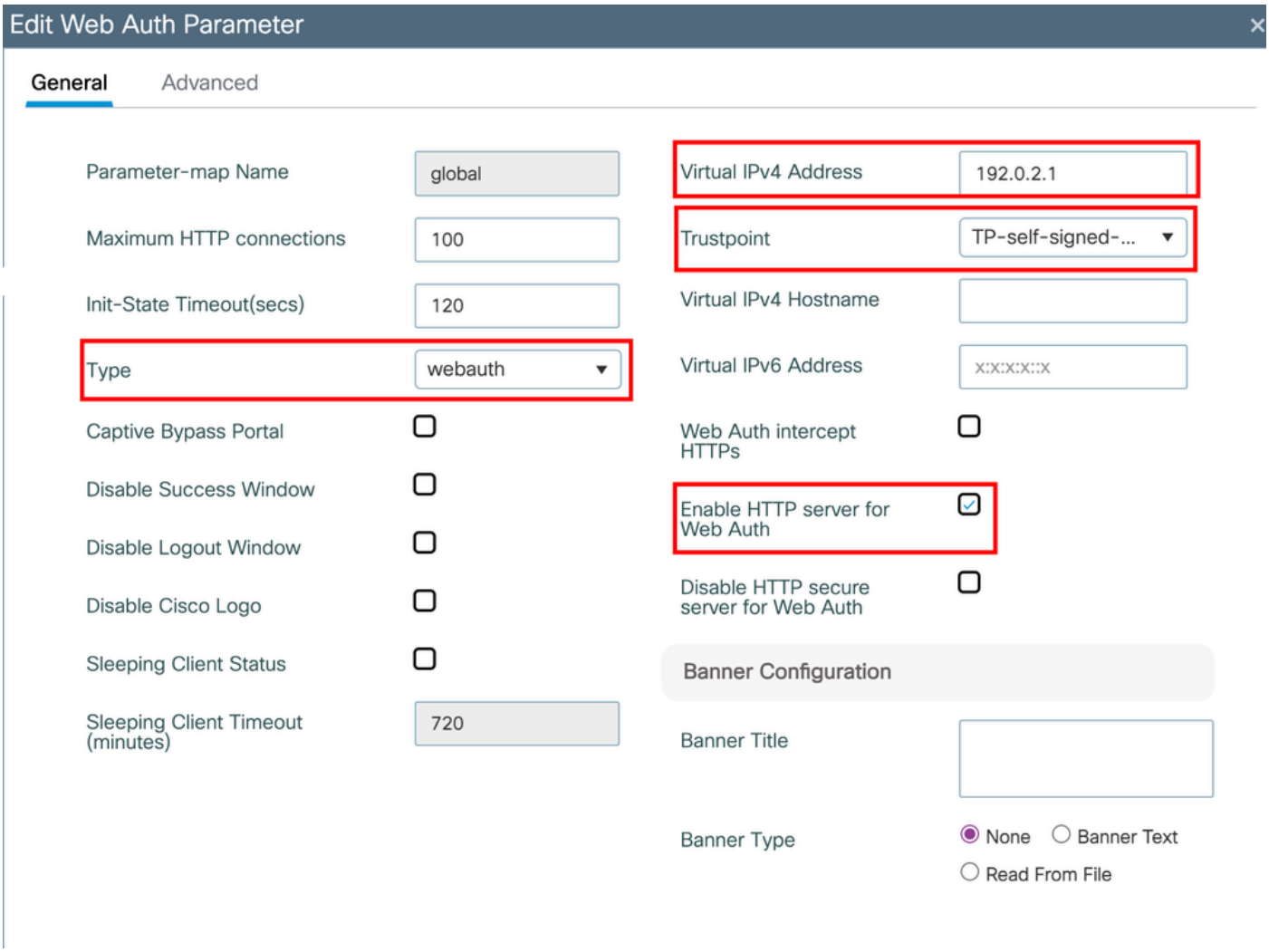


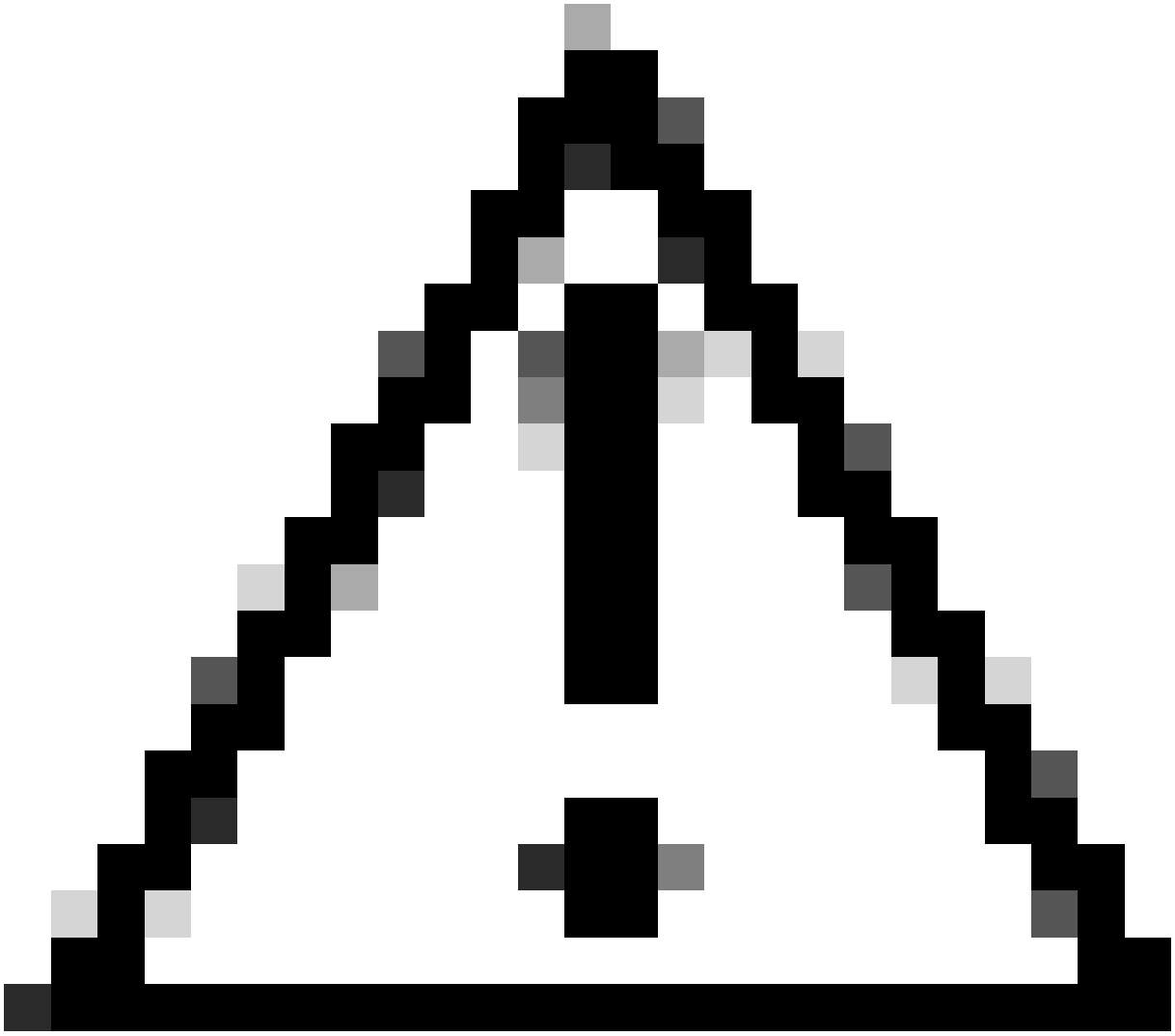
Mapas de parámetro

Edite el mapa de parámetro global en Configuration > Security > Web Auth



Seleccione el tipo de autenticación web que se utilizará, la IP virtual y el Trustpoint que el WLC presenta en el portal web. En este caso, se selecciona el certificado autofirmado y es probable que se genere una renuncia de responsabilidad del tipo "su conexión no es red privada::ERR_CERT_AUTHORITY_INVALID", ya que se trata de un certificado de importancia local (LSC) y no está firmado por una CA reconocible en Internet. Para enmendarlo, utilice un certificado firmado por un tercero. Los detalles se describen en Generar y descargar certificados CSR en WLC Catalyst 9800 o hay una opción de video que explica la carga y la creación de Truspoint Renovar certificados para WebAuth y WebAdmin en WLC Cisco 9800 | Configuración del controlador de LAN inalámbrica segura.

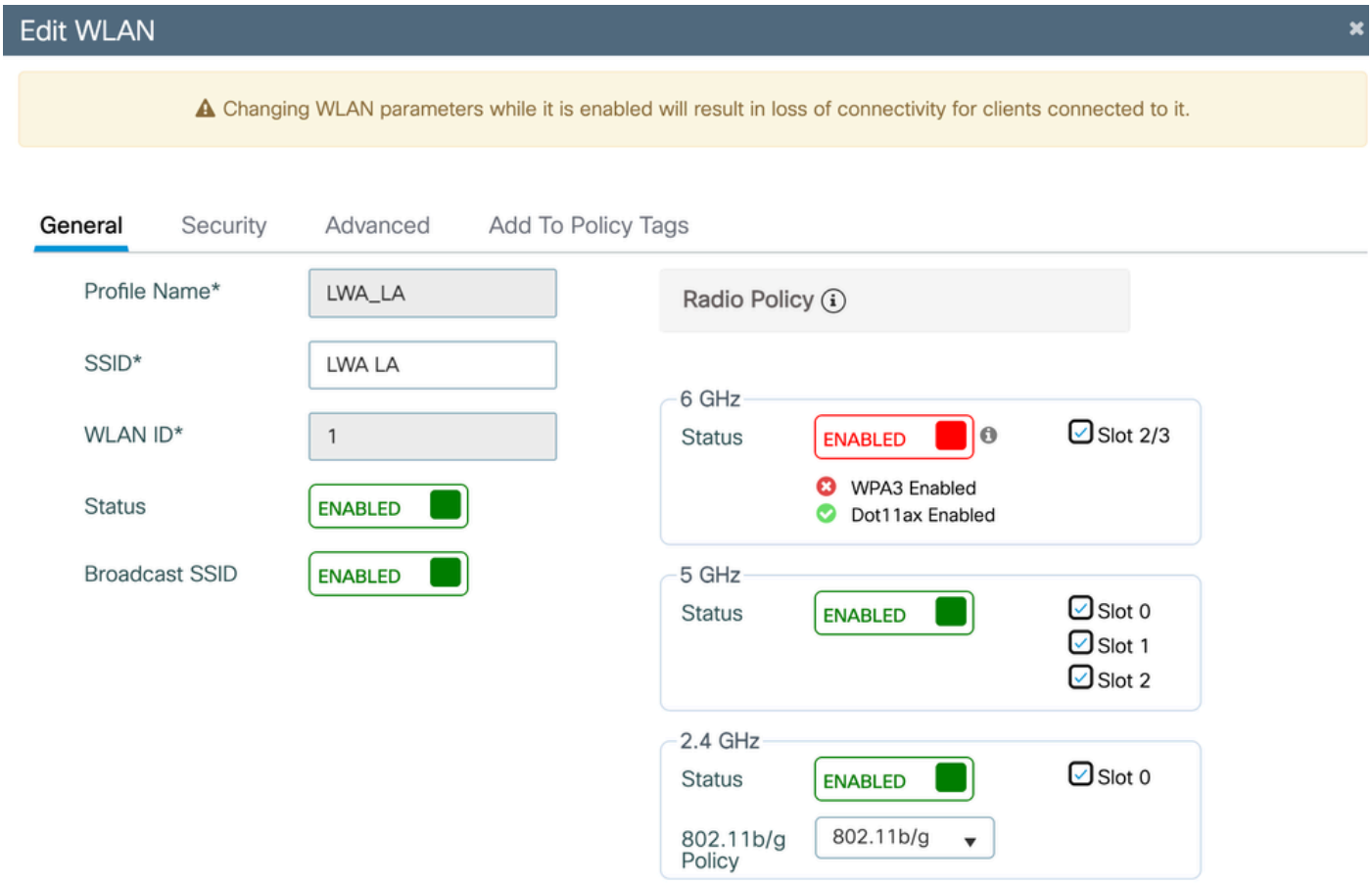

Edit Web Auth Parameter
General
Advanced
Parameter-map Name
global
Maximum HTTP connections
100
Init-State Timeout(secs)
120
Type
webauth
Captive Bypass Portal
Disable Success Window
Disable Logout Window
Disable Cisco Logo
Sleeping Client Status
Sleeping Client Timeout (minutes)
720
Virtual IPv4 Address
192.0.2.1
Trustpoint
TP-self-signed-...
Virtual IPv4 Hostname
Virtual IPv6 Address
x:x:x:x::x
Web Auth intercept HTTPs
Enable HTTP server for Web Auth
Disable HTTP secure server for Web Auth
Banner Configuration
Banner Title
Banner Type
None
Banner Text
Read From File



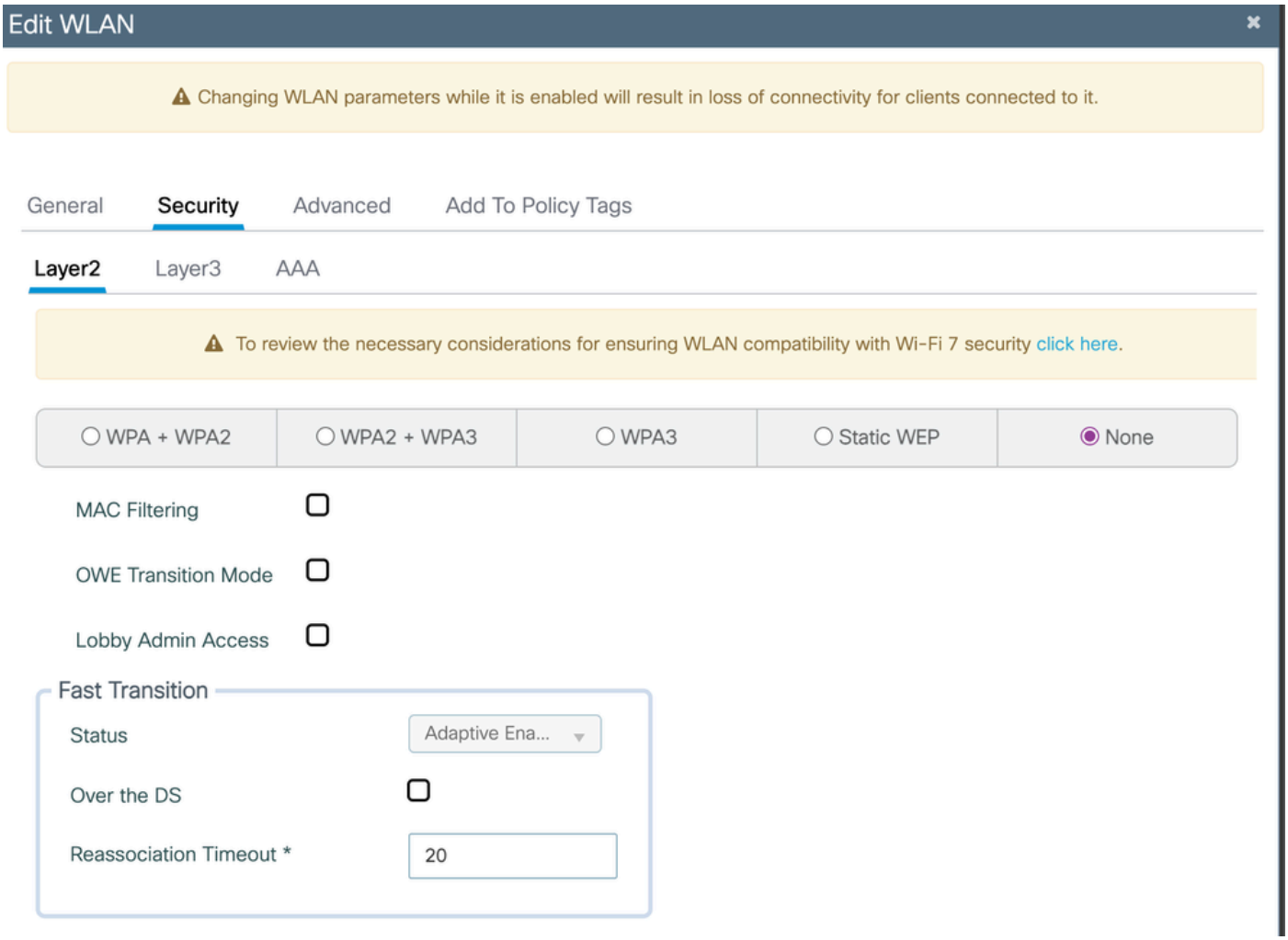
Precaución: Si tiene HTTP deshabilitado globalmente en el 9800, asegúrese de que la opción Enable HTTP server for Web Auth (Habilitar servidor HTTP para autenticación web) esté marcada, ya que Cisco separó la dependencia de estos procesos. Se espera que los clientes o suplicantes inicien un proceso de conexión HTTP y que el controlador intercepte esa sesión para presentar el portal web. Por esa razón, no se recomienda habilitar Web Auth Intercept HTTPS a menos que sea absolutamente necesario, ya que esta configuración es innecesaria para la mayoría de las implementaciones y puede aumentar el uso de la CPU del controlador, lo que puede afectar el rendimiento.

Parámetros de seguridad de WLAN

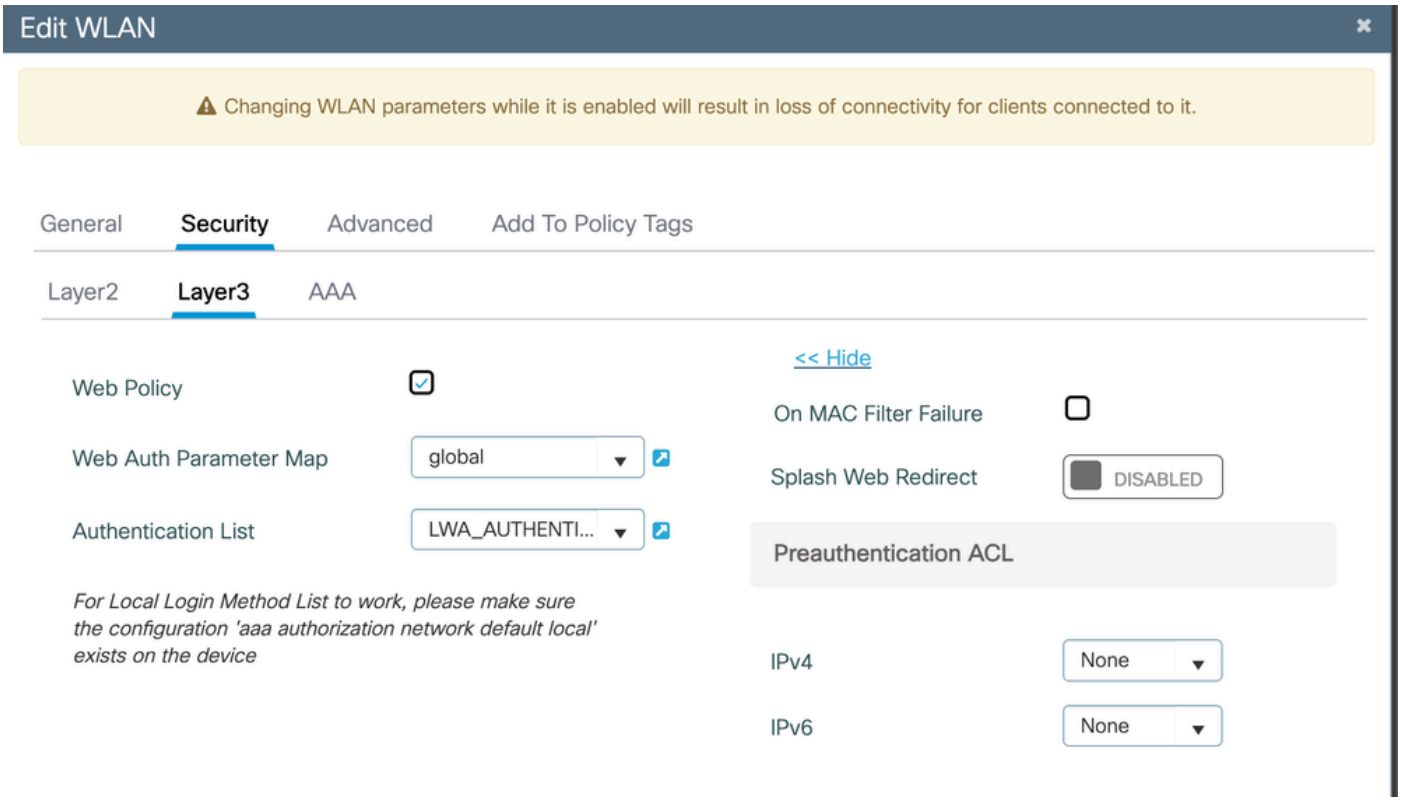
Vaya a Configuration > Tags & Profiles > WLANs, haga clic en Add.



En la ficha Seguridad, para la capa 2, seleccione Ninguno.

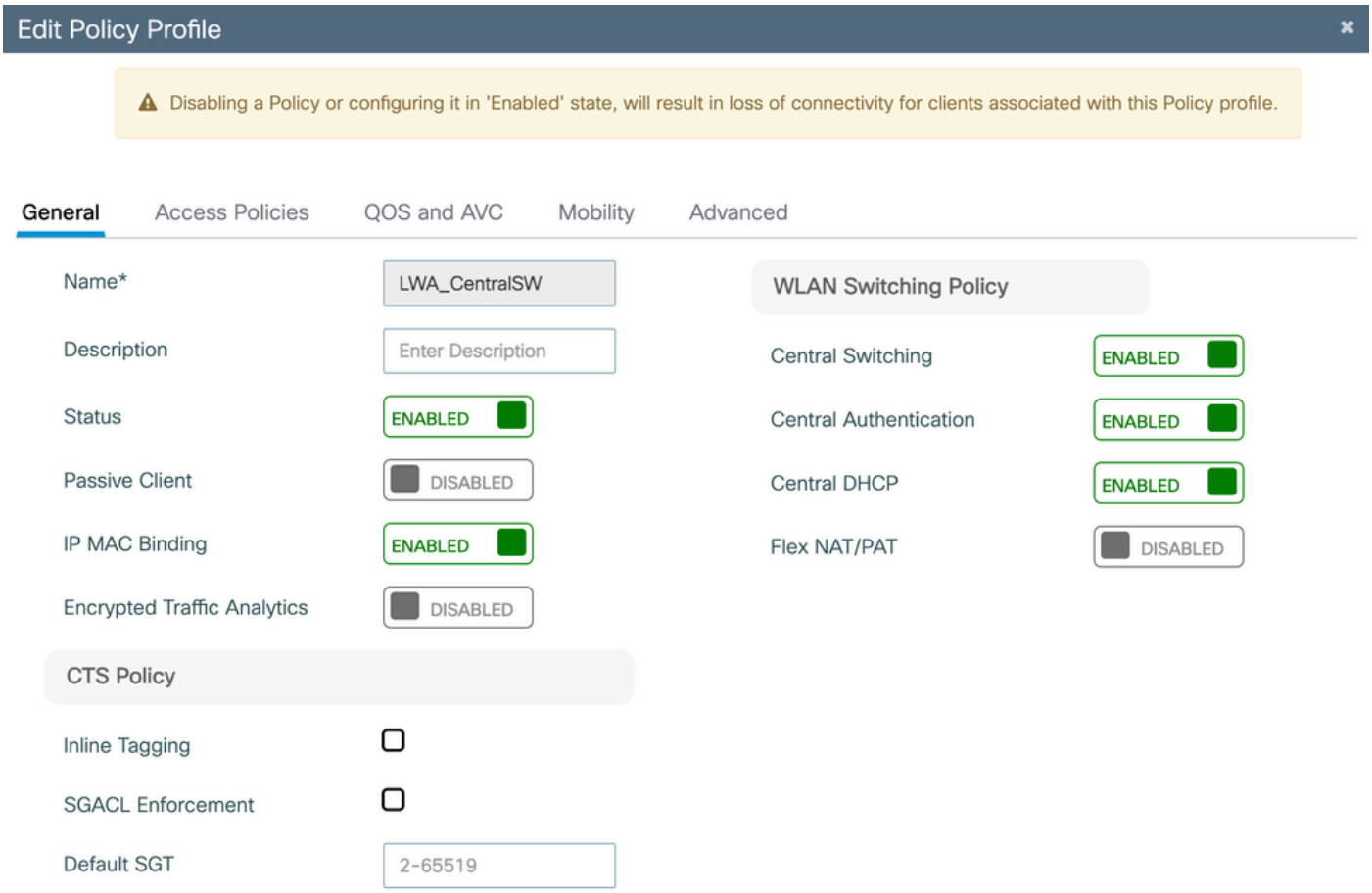


En la ficha Security (Seguridad), para Layer3, active la casilla Web Policy (Directiva web) y, a continuación, seleccione el mapa de parámetros configurado anteriormente en el menú desplegable y en la lista Authentication (Autenticación).

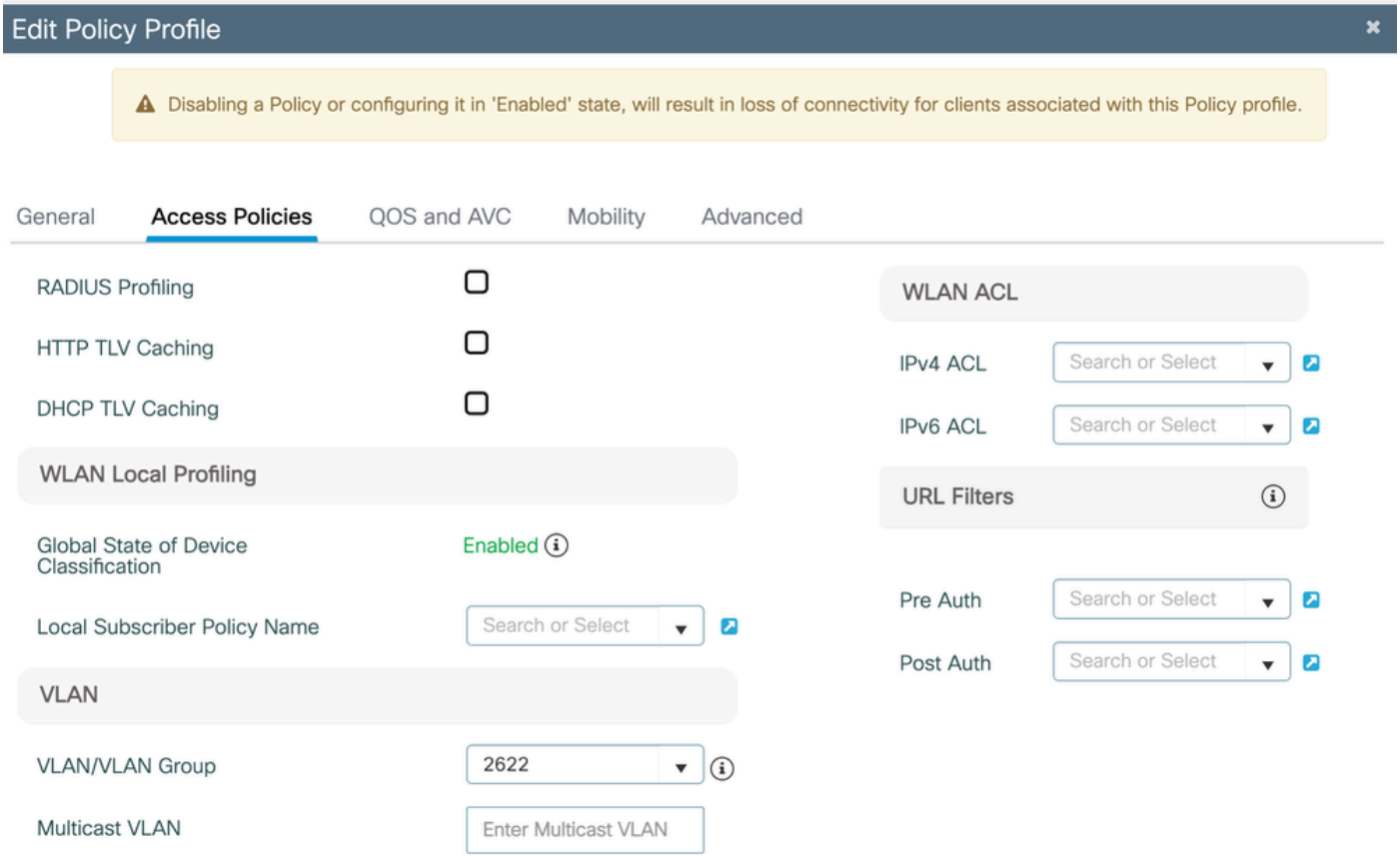


Crear un perfil de política

Para crear el perfil de política que se vinculará al perfil WLAN, navegue hasta Configuration > Tags & Profiles > Policy.

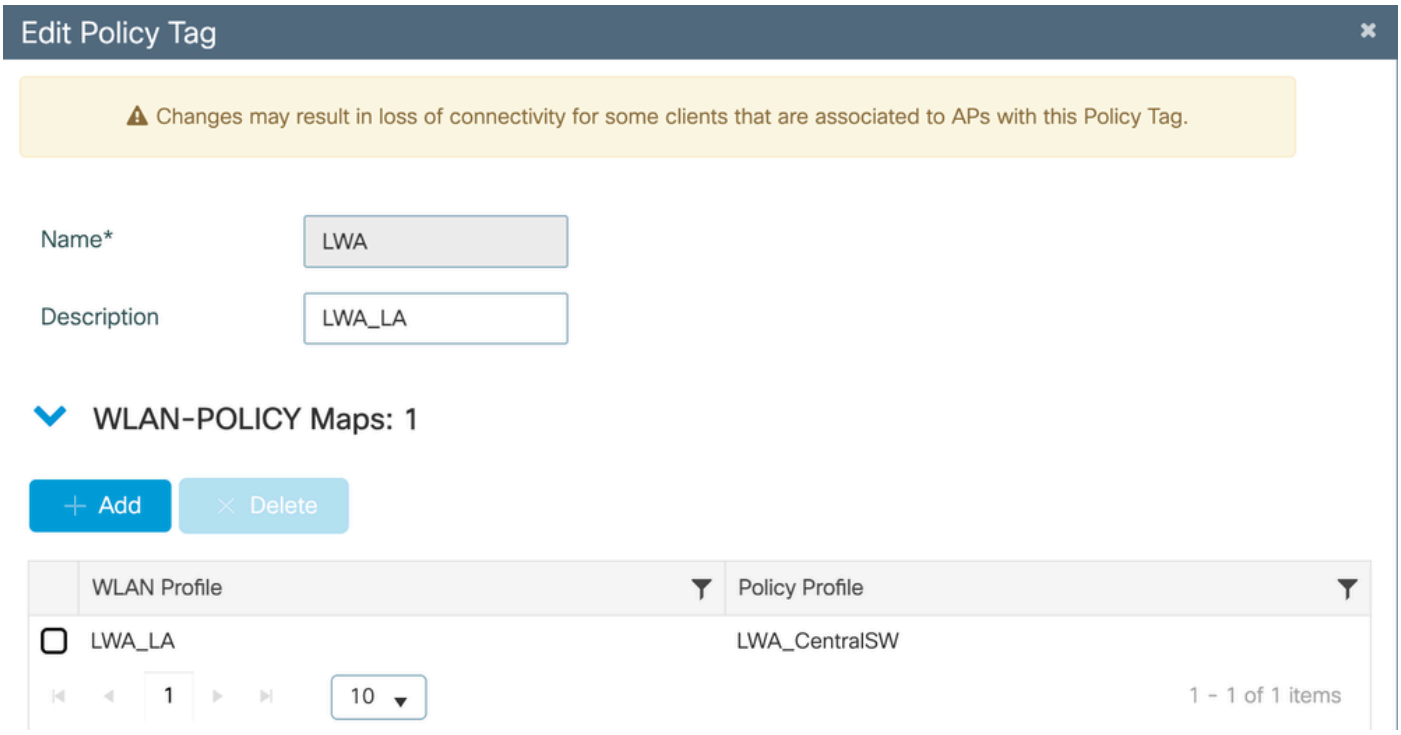


En la pestaña Access Policies, seleccione la VLAN desde donde los Clientes/Suplicantes solicitan una IP.



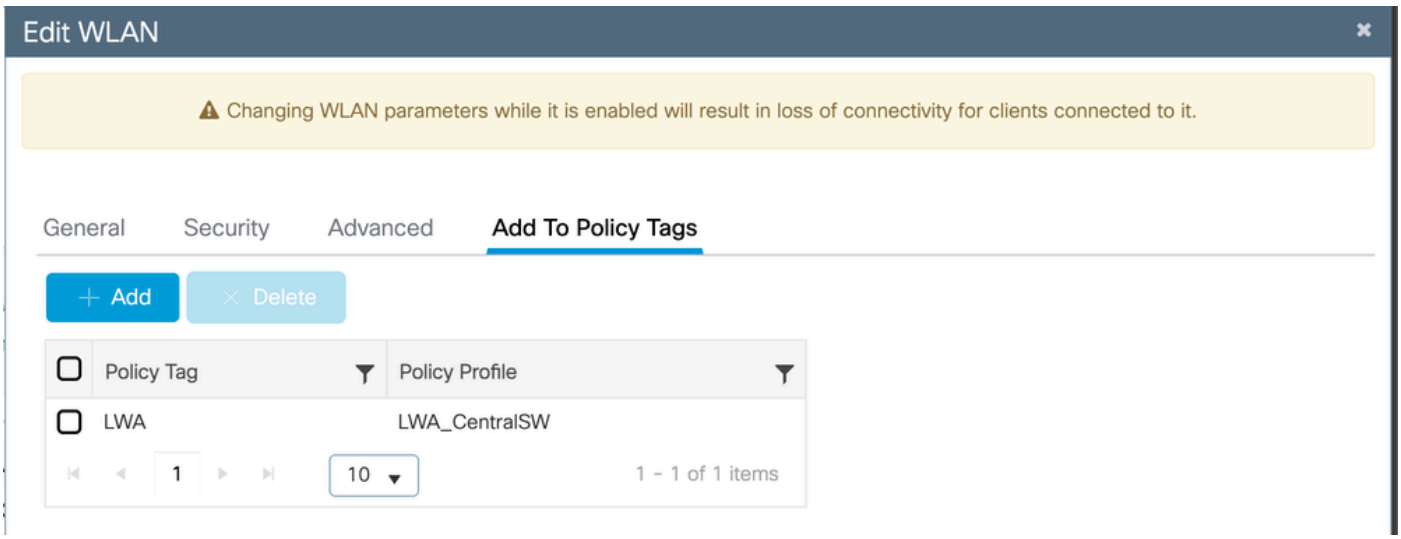
Crear una etiqueta de directiva

Para esta guía de configuración, creamos una etiqueta de política personalizada denominada LWA.



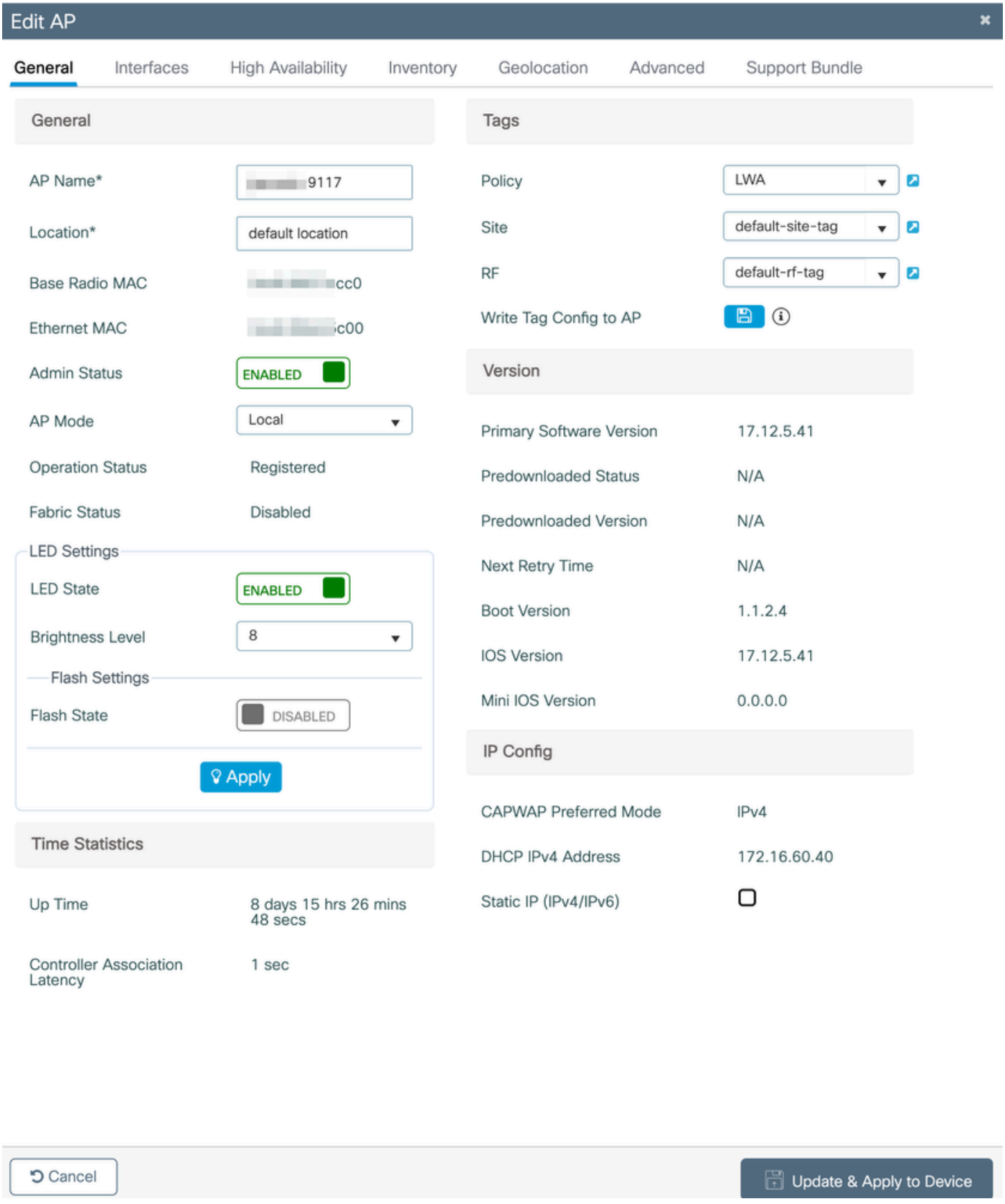
Asociar el perfil de WLAN y de política

Para vincular las políticas de switching del perfil de política y la WLAN, navegue hasta Configuration > Tags & Profiles > WLANs, seleccione el perfil WLAN, haga clic en Add to Policy Tags.



Asignar una etiqueta de política a un AP

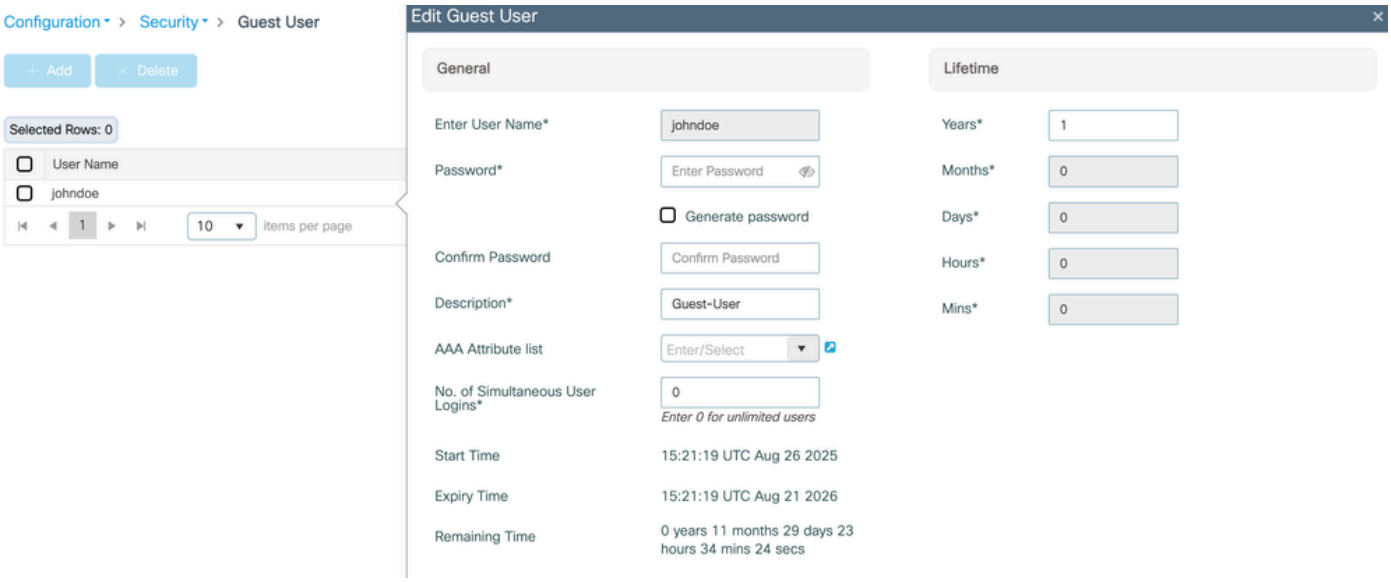
Para etiquetar el AP con la etiqueta de política creada, navegue hasta Configuration > Wireless > Access Points, seleccione el AP y en la pestaña General, en el lado derecho están las etiquetas utilizadas por el AP.



Crear nombre de usuario de invitado

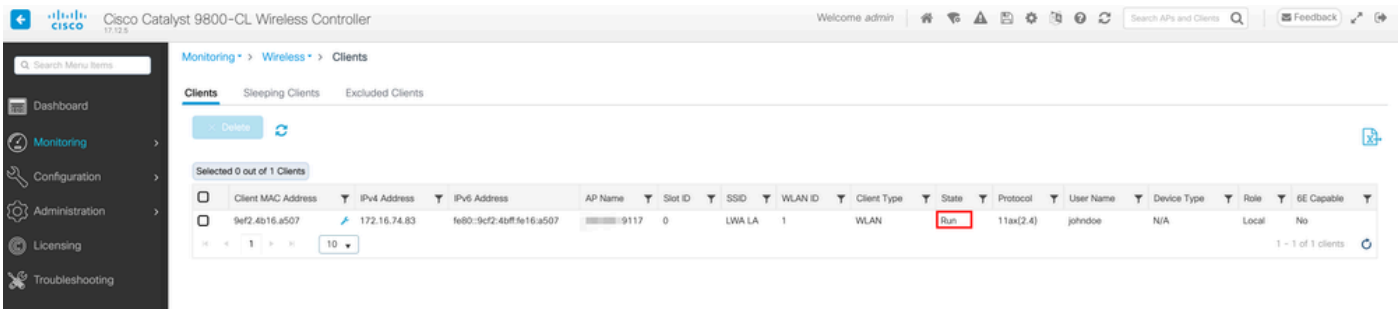
Si seleccionó el tipo de webauth en el mapa de parámetro, se necesita un nombre de usuario de invitado para crearlo, navegue hasta Configuration > Security > Guest User .

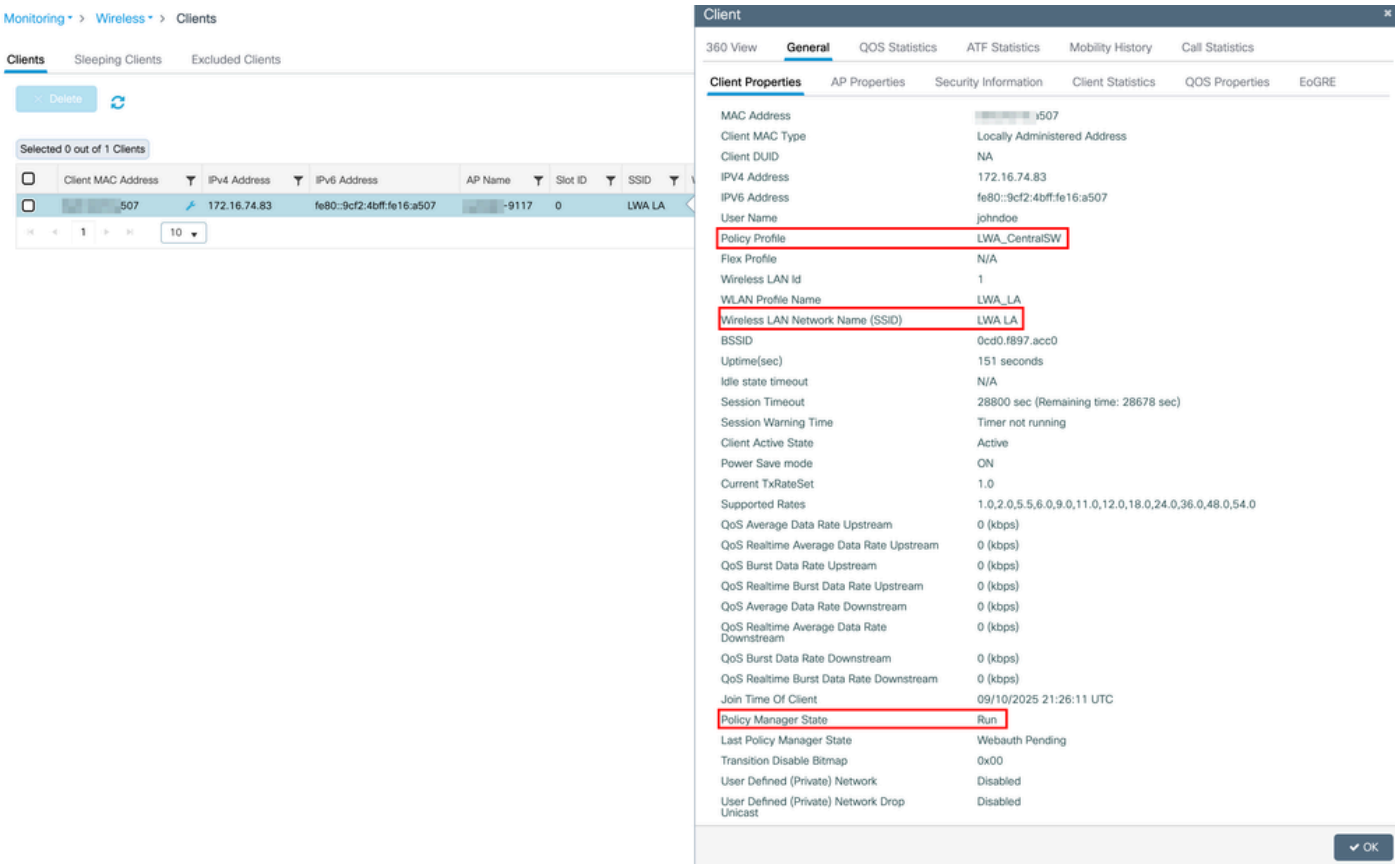
La duración máxima del usuario es de 1 año. Puede especificar lo contrario con las opciones disponibles.



Verificación

Mediante GUI





Mediante CLI

```
9800WLC>enable
9800WLC#show wireless client summary
Number of Clients: 1
MAC Address      AP Name       Type ID State Protocol  Method    Role
-----------------------------------------------------------------------------------------------------
9ef2.4b16.a507   xxxxx-9117 WLAN 1  Run   11ax(2.4) Web Auth  Local
9800WLC#show wireless client mac-address


        detail


Client MAC Address : 9ef2.4b16.a507


Client MAC Type : Locally Administered Address


Client DUID: NA


Client IPv4 Address : 172.16.74.83


Client IPv6 Addresses : fe80::9cf2:4bff:fe16:a507


Client Username : johndoe
```

AP MAC Address : 0cd0.f897.acc0

AP Name: xxxxx-9117

AP slot : 0

Client State : Associated

Policy Profile : LWA_CentralSW

Flex Profile : N/A

Wireless LAN Id: 1

WLAN Profile Name: LWA_LA

Wireless LAN Network Name (SSID): LWA LA

BSSID : 0cd0.f897.acc0

Connected For : 392 seconds

Protocol : 802.11ax - 2.4 GHz

Channel : 11

Client IIF-ID : 0xa0000002

Association Id : 1

Authentication Algorithm : Open System

Idle state timeout : N/A

Session Timeout : 28800 sec (Remaining time: 28455 sec)

Session Warning Time : Timer not running

Input Policy Name : None

Input Policy State : None

Input Policy Source : None

Output Policy Name : None

Output Policy State : None

Output Policy Source : None

WMM Support : Enabled

U-APSD Support : Disabled

Fastlane Support : Disabled

Client Active State : Active

Power Save : ON

Current Rate : m0 ss2

Supported Rates : 1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0

AAA QoS Rate Limit Parameters:

QoS Average Data Rate Upstream : 0 (kbps)

QoS Realtime Average Data Rate Upstream : 0 (kbps)

QoS Burst Data Rate Upstream : 0 (kbps)

QoS Realtime Burst Data Rate Upstream : 0 (kbps)

QoS Average Data Rate Downstream : 0 (kbps)

QoS Realtime Average Data Rate Downstream : 0 (kbps)

QoS Burst Data Rate Downstream : 0 (kbps)

QoS Realtime Burst Data Rate Downstream : 0 (kbps)

Mobility:

Move Count : 0

Mobility Role : Local

Mobility Roam Type : None

Mobility Complete Timestamp : 09/10/2025 21:41:11 UTC

Client Join Time:

Join Time Of Client : 09/10/2025 21:41:11 UTC

Client State Servers : None

Client ACLs : None

Policy Manager State: Run

Last Policy Manager State : Webauth Pending

Client Entry Create Time : 392 seconds

Policy Type : N/A

Encryption Cipher : None

Transition Disable Bitmap : 0x00

User Defined (Private) Network : Disabled

User Defined (Private) Network Drop Unicast : Disabled

Encrypted Traffic Analytics : No

Protected Management Frame - 802.11w : No

EAP Type : Not Applicable

VLAN Override after Webauth : No

VLAN : 2667

Multicast VLAN : 0

VRF Name : N/A

WiFi Direct Capabilities:

WiFi Direct Capable : No

Central NAT : DISABLED

Session Manager:

Point of Attachment : capwap_90400005

IIF ID : 0x90400005

Authorized : TRUE

Session timeout : 28800

Common Session ID: 044A10AC0000000F359351E3

Acct Session ID : 0x00000000

Auth Method Status List

Method : Web Auth

Webauth State : Authz

Webauth Method : Webauth

Local Policies:

Service Template : IP-Adm-V4-LOGOUT-ACL (priority 100)

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

Service Template : wlan_svc_LWA_CentralSW_local (priority 254)

VLAN : 2667

Absolute-Timer : 28800

Server Policies:

Resultant Policies:

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

VLAN Name : xxxxx

VLAN : 2667

Absolute-Timer : 28800

DNS Snooped IPv4 Addresses : None

DNS Snooped IPv6 Addresses : None

Client Capabilities

CF Pollable : Not implemented

CF Poll Request : Not implemented

Short Preamble : Not implemented

PBCC : Not implemented

Channel Agility : Not implemented

Listen Interval : 0

Fast BSS Transition Details :

Reassociation Timeout : 0

11v BSS Transition : Implemented

11v DMS Capable : No

QoS Map Capable : Yes

FlexConnect Data Switching : N/A

FlexConnect Dhcp Status : N/A

FlexConnect Authentication : N/A

Client Statistics:

Number of Bytes Received from Client : 111696

Number of Bytes Sent to Client : 62671

Number of Packets Received from Client : 529

Number of Packets Sent to Client : 268

Number of Data Retries : 136

Number of RTS Retries : 0

Number of Tx Total Dropped Packets : 1

Number of Duplicate Received Packets : 0

Number of Decrypt Failed Packets : 0

Number of Mic Failured Packets : 0

Number of Mic Missing Packets : 0

Number of Policy Errors : 0

Radio Signal Strength Indicator : -61 dBm

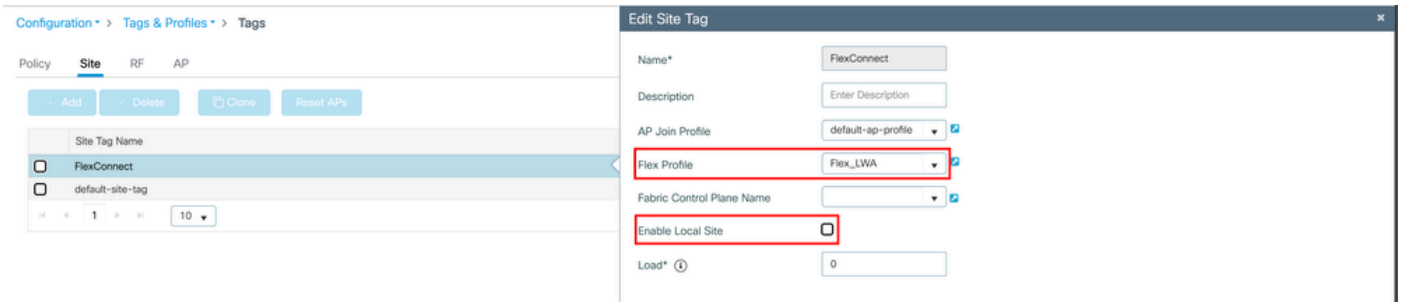
Signal to Noise Ratio : 4 dB

Fabric status : Disabled

```
Radio Measurement Enabled Capabilities

Capabilities: Link Measurement, Neighbor Report, Repeated Measurements, Passive Beacon Measurement, Act

Client Scan Report Time : Timer not running

Client Scan Reports

Assisted Roaming Neighbor List

Nearby AP Statistics:

EoGRE : Pending Classification

Max Client Protocol Capability: Wi-Fi6 (802.11ax)

WiFi to Cellular Steering : Not implemented

Cellular Capability : N/A

Advanced Scheduling Requests Details:

Apple Specific Requests(ASR) Capabilities/Statistics:

Regular ASR support: DISABLED
```

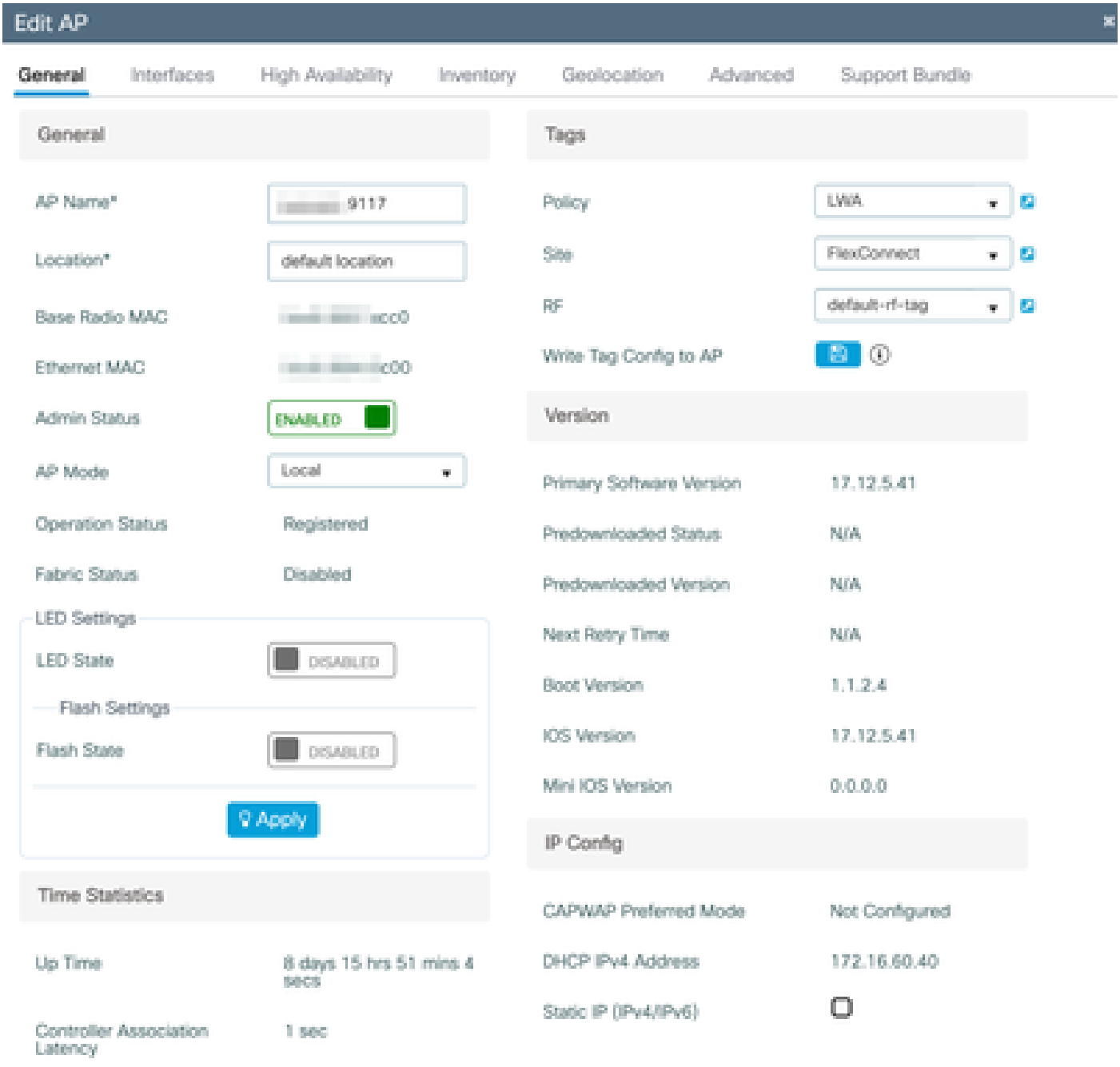
Autenticación Web Local en FlexConnect Local Switching

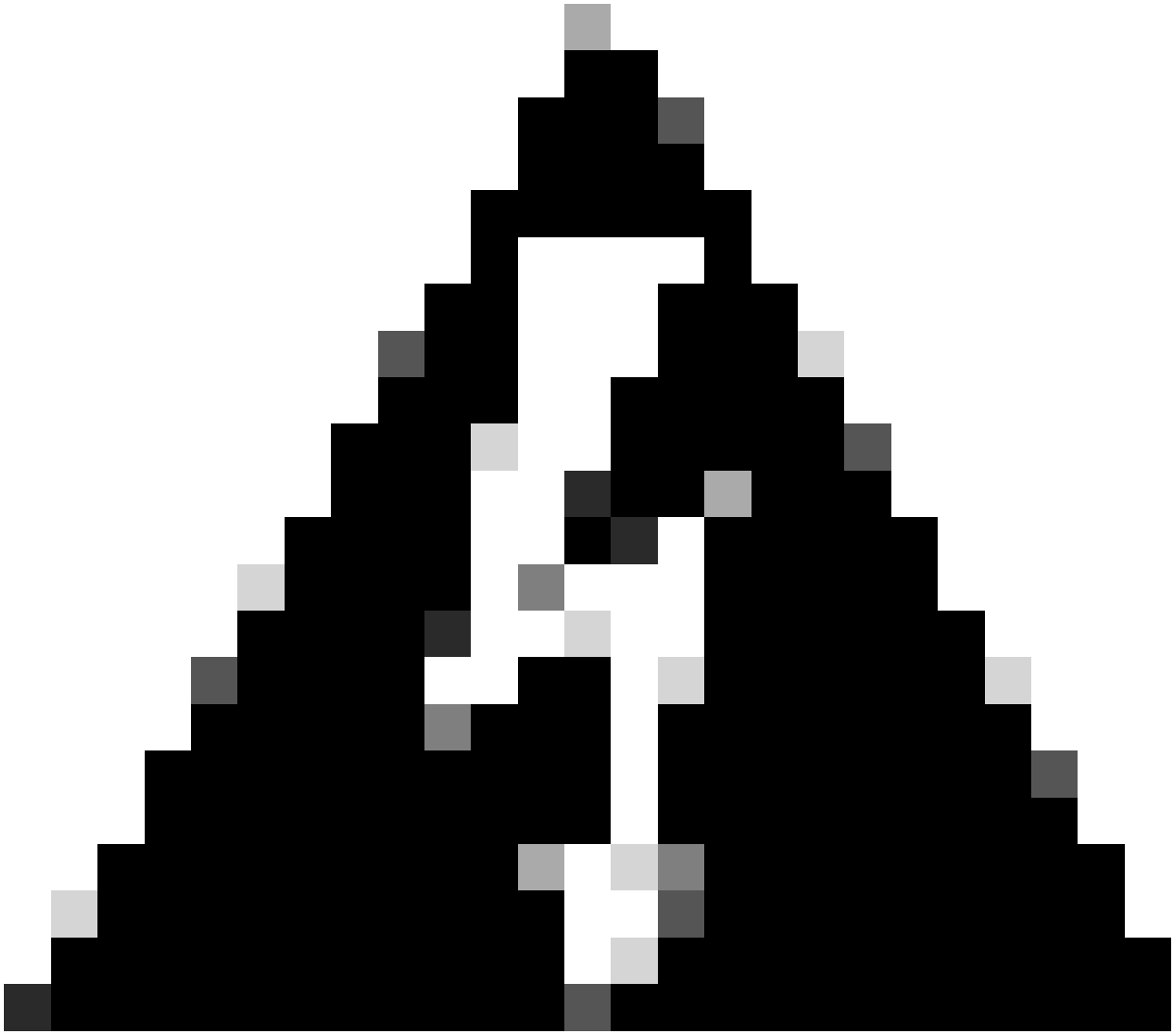
Para este escenario, se supone que el AP está en el modo FlexConnect. Para que un AP esté en el modo FlexConnect, necesita un perfil Flex asociado en SiteTag, donde la casilla de verificación Enable Local Site está inhabilitada. Esta etiqueta del sitio utiliza el nombre de perfil flex Flex_LWA y default-ap-join:



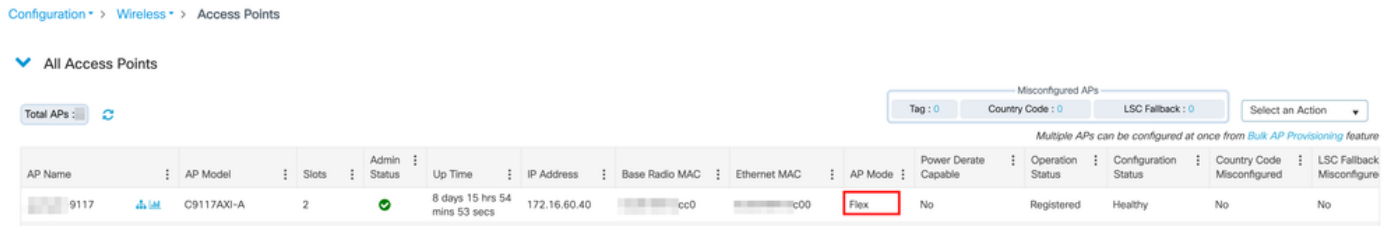
Asignar una etiqueta de política a un AP

Navegue hasta Configuration > Wireless > Access Points, seleccione el AP y en la ficha General, a la derecha están las etiquetas utilizadas por el AP.

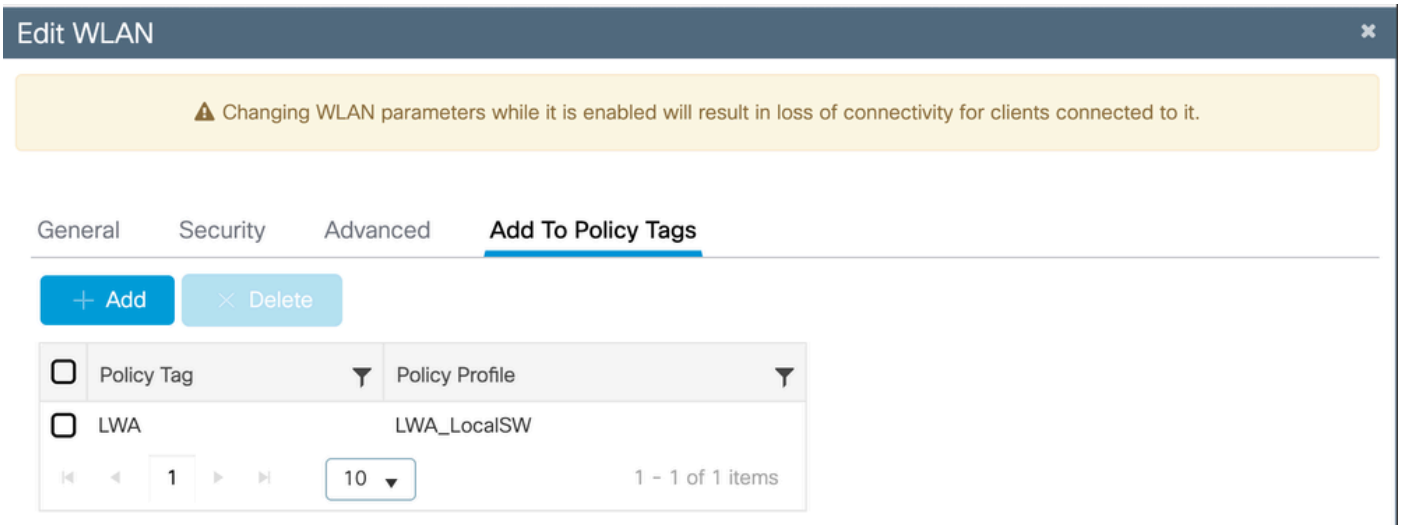


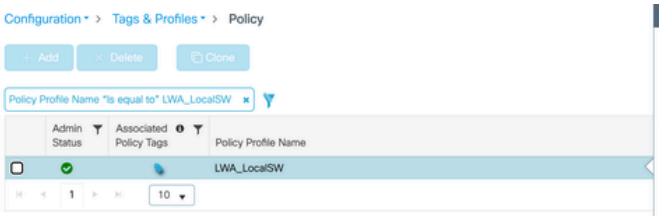


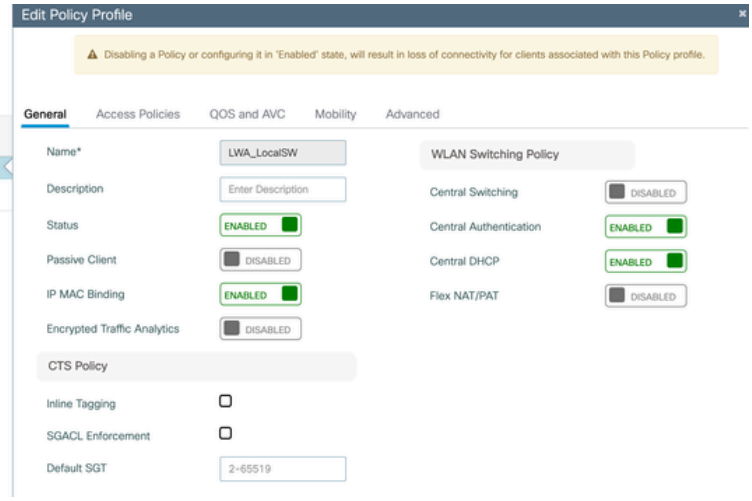
Advertencia: El cambio de las etiquetas hace que el AP se separe del WLC.



El perfil de política asociado con la WLAN es Local Switching







Verificación

```
9800WLC>enable
9800WLC#show wireless client summary
Number of Clients: 1
MAC Address      AP Name        Type ID  State Protocol  Method    Role
-----------------------------------------------------------------------------------------------
9ef2.4b16.a507 xxxxx-9117 WLAN 1 Run 11ax(2.4) Web Auth Local

9800WLC#show wireless client mac-address


        detail


Client MAC Address :



Client MAC Type : Locally Administered Address


Client DUID: NA
```

Client IPv4 Address : 172.16.74.83

Client IPv6 Addresses : fe80::9cf2:4bff:fe16:a507

Client Username : johndoe

AP MAC Address : xxxx.xxxx.xcc0

AP Name: xxxxxx-9117

AP slot : 0

Client State : Associated

Policy Profile : LWA_LocalSW

Flex Profile : Flex_LWA

Wireless LAN Id: 1

WLAN Profile Name: LWA_LA

Wireless LAN Network Name (SSID): LWA LA

BSSID : 0cd0.f897.acc0

Connected For : 315 seconds

Protocol : 802.11ax - 2.4 GHz

Channel : 6

Client IIF-ID : 0xa0000004

Association Id : 1

Authentication Algorithm : Open System

Idle state timeout : N/A

Session Timeout : 28800 sec (Remaining time: 28525 sec)

Session Warning Time : Timer not running

Input Policy Name : None

Input Policy State : None

Input Policy Source : None

Output Policy Name : None

Output Policy State : None

Output Policy Source : None

WMM Support : Enabled

U-APSD Support : Disabled

Fastlane Support : Disabled

Client Active State : Active

Power Save : ON

Current Rate : m11 ss2

Supported Rates : 1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0

AAA QoS Rate Limit Parameters:

QoS Average Data Rate Upstream : 0 (kbps)

QoS Realtime Average Data Rate Upstream : 0 (kbps)

QoS Burst Data Rate Upstream : 0 (kbps)

QoS Realtime Burst Data Rate Upstream : 0 (kbps)

QoS Average Data Rate Downstream : 0 (kbps)

QoS Realtime Average Data Rate Downstream : 0 (kbps)

QoS Burst Data Rate Downstream : 0 (kbps)

QoS Realtime Burst Data Rate Downstream : 0 (kbps)

Mobility:

Move Count : 0

Mobility Role : Local

Mobility Roam Type : None

Mobility Complete Timestamp : 09/11/2025 17:38:26 UTC

Client Join Time:

Join Time Of Client : 09/11/2025 17:38:26 UTC

Client State Servers : None

Client ACLs : None

Policy Manager State: Run

Last Policy Manager State : Webauth Pending

Client Entry Create Time : 315 seconds

Policy Type : N/A

Encryption Cipher : None

Transition Disable Bitmap : 0x00

User Defined (Private) Network : Disabled

User Defined (Private) Network Drop Unicast : Disabled

Encrypted Traffic Analytics : No

Protected Management Frame - 802.11w : No

EAP Type : Not Applicable

VLAN Override after Webauth : No

VLAN : 2667

Multicast VLAN : 0

VRF Name : N/A

WiFi Direct Capabilities:

WiFi Direct Capable : No

Central NAT : DISABLED

Session Manager:

Point of Attachment : capwap_90400005

IIF ID : 0x90400005

Authorized : TRUE

Session timeout : 28800

Common Session ID: 044A10AC0000002A39DB6F52

Acct Session ID : 0x00000000

Auth Method Status List

Method : Web Auth

Webauth State : Authz

Webauth Method : Webauth

```
Local Policies:

Service Template : IP-Adm-V4-LOGOUT-ACL (priority 100)

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

Service Template : wlan_svc_LWA_LocalSW (priority 254)

VLAN : 2667

Absolute-Timer : 28800

Server Policies:

Resultant Policies:

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

VLAN Name : xxxxx

VLAN : 2667

Absolute-Timer : 28800

DNS Snooped IPv4 Addresses : None

DNS Snooped IPv6 Addresses : None

Client Capabilities

CF Pollable : Not implemented

CF Poll Request : Not implemented

Short Preamble : Not implemented

PBCC : Not implemented

Channel Agility : Not implemented

Listen Interval : 0
```

Fast BSS Transition Details :

Reassociation Timeout : 0

11v BSS Transition : Implemented

11v DMS Capable : No

QoS Map Capable : Yes

FlexConnect Data Switching : Local

FlexConnect Dhcp Status : Central

FlexConnect Authentication : Central

Client Statistics:

Number of Bytes Received from Client : 295564

Number of Bytes Sent to Client : 90146

Number of Packets Received from Client : 1890

Number of Packets Sent to Client : 351

Number of Data Retries : 96

Number of RTS Retries : 0

Number of Tx Total Dropped Packets : 0

Number of Duplicate Received Packets : 0

Number of Decrypt Failed Packets : 0

Number of Mic Failured Packets : 0

Number of Mic Missing Packets : 0

Number of Policy Errors : 0

Radio Signal Strength Indicator : -34 dBm

Signal to Noise Ratio : 31 dB

Fabric status : Disabled

Radio Measurement Enabled Capabilities

Capabilities: Link Measurement, Neighbor Report, Repeated Measurements, Passive Beacon Measurement, Act

Client Scan Report Time : Timer not running

Client Scan Reports

Assisted Roaming Neighbor List

Nearby AP Statistics:

EoGRE : Pending Classification

Max Client Protocol Capability: Wi-Fi6 (802.11ax)

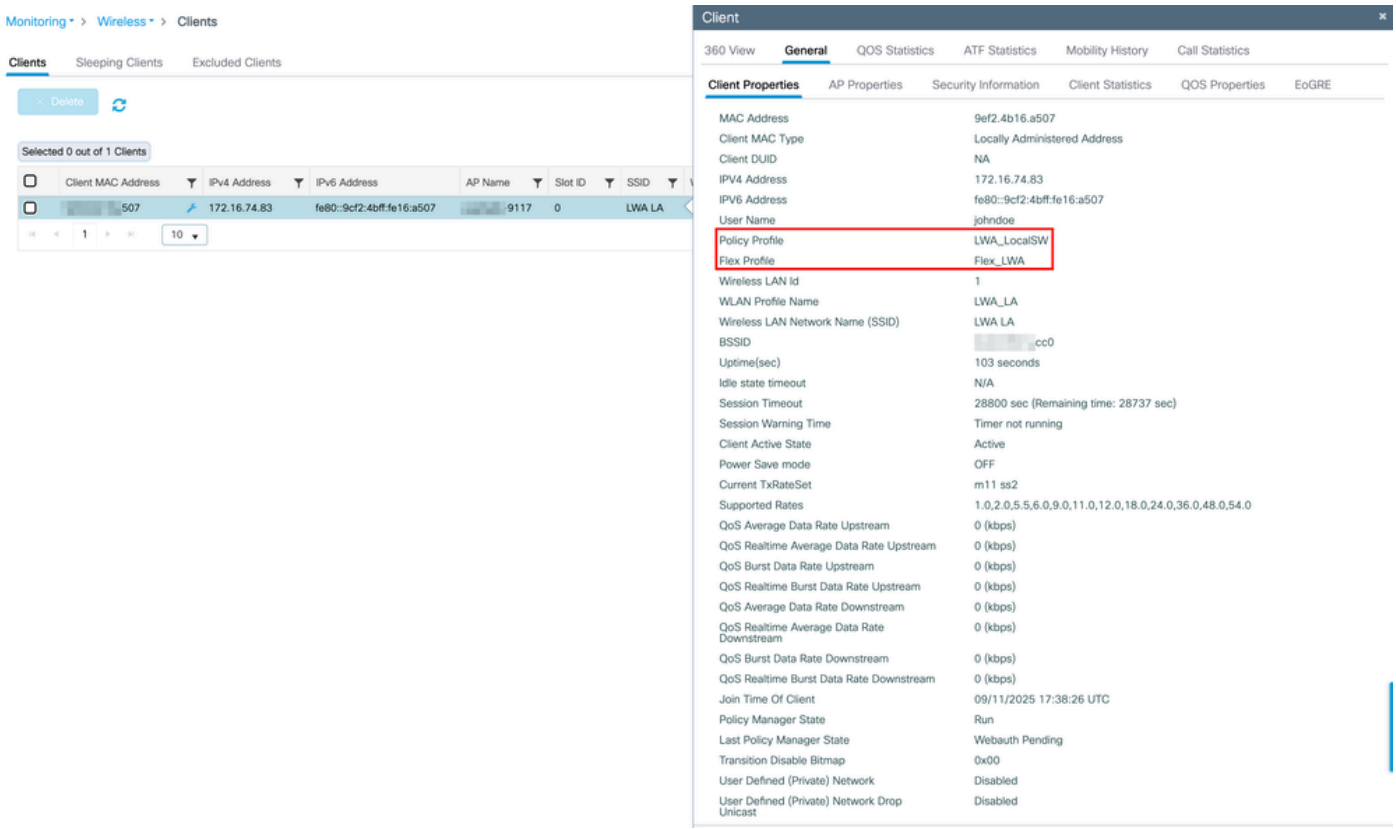
WiFi to Cellular Steering : Not implemented

Cellular Capability : N/A

Advanced Scheduling Requests Details:

Apple Specific Requests(ASR) Capabilities/Statistics:

Regular ASR support: DISABLED



Troubleshoot

El estado "Autenticación web pendiente" indica que el cliente se ha asociado con el punto de acceso pero aún no ha completado el proceso de autenticación web. Durante este estado, el controlador intercepta el tráfico HTTP del cliente y lo redirige a un portal de autenticación web para que el usuario inicie sesión o acepte los términos. El cliente permanece en este estado hasta que se completa la autenticación web exitosa, después de lo cual el estado del administrador de políticas de cliente pasa a "Ejecutar" y se concede acceso completo a la red.

para ver visualmente el flujo de la conexión del cliente, verifique el flujo de LWA desde Configure Local Web Authentication with External Authentication.

Las etapas que el cliente pasa desde la perspectiva del cliente se representan en Troubleshooting Common Issues with LWA on 9800 WLC.

- Soporte Técnico y Documentación - Cisco Systems

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).