

# Sustitución de WLAN FlexConnect con AAA 802.1x en los controladores inalámbricos Catalyst 9800

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración](#)

[Configuración AAA en el WLC 9800](#)

[Configuración de WLAN](#)

[Establecer AP como modo FlexConnect](#)

[Configuración del switch](#)

[Configuración del perfil de política](#)

[Configuración de la etiqueta de política](#)

[Asignación de etiqueta de política](#)

[Configuración de ISE](#)

[Verificación](#)

[Troubleshoot](#)

## Introducción

Este documento describe cómo configurar un controlador LAN inalámbrico elástico (9800 WLC) con puntos de acceso en modo FlexConnect (AP) y una red de área local inalámbrica (WLAN) conmutada localmente 802.1x con autenticación, autorización y contabilidad (AAA) de red de área local virtual (VLAN).

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- 9800 modo de configuración WLC
- FlexConnect

### Componentes Utilizados

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

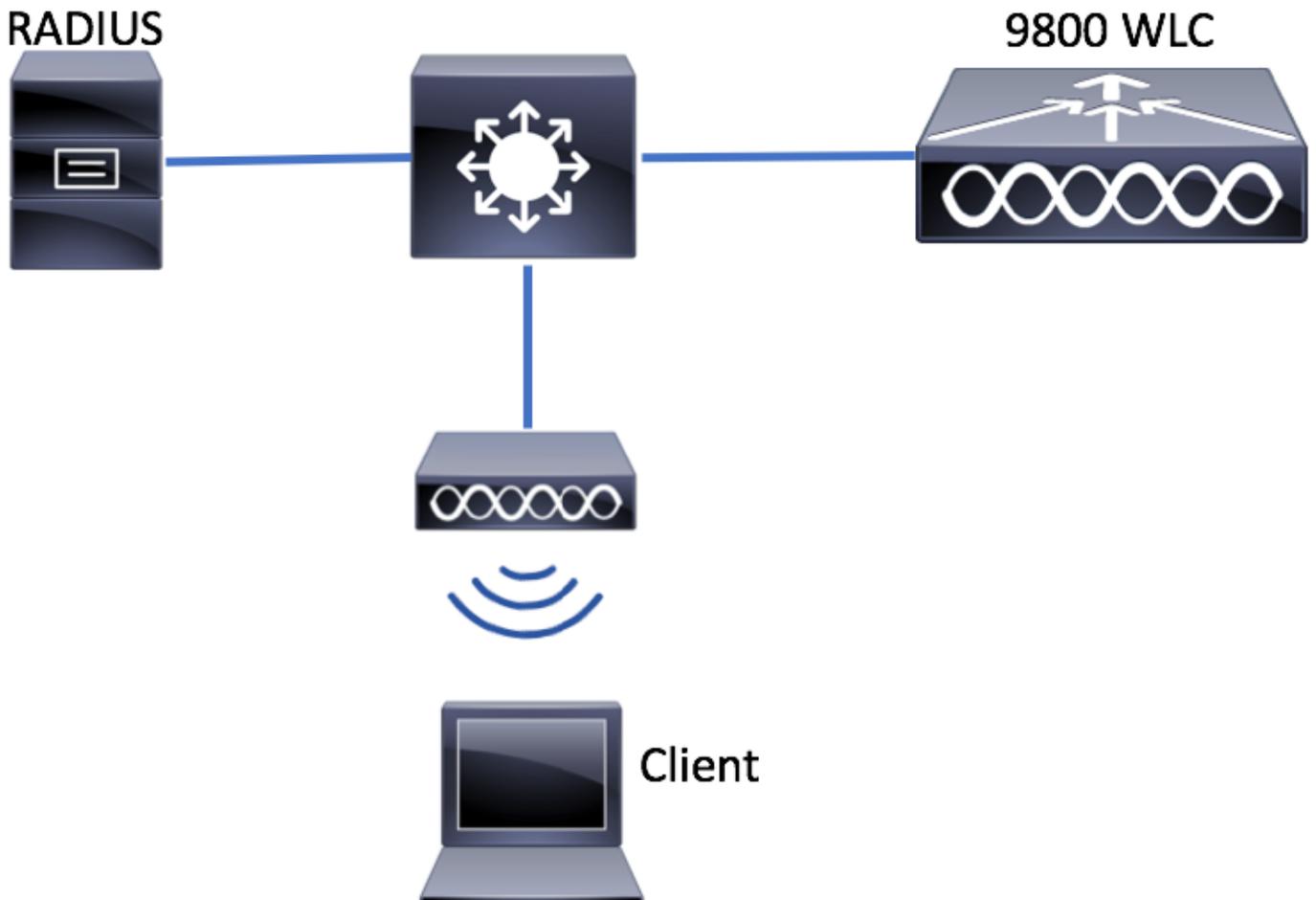
hardware.

- 9800 WLC v16.10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Configurar

### Diagrama de la red



## Configuración

### Configuración AAA en el WLC 9800

Puede seguir las instrucciones de este enlace:

[Configuración AAA en el WLC 9800](#)

### Configuración de WLAN

Puede seguir las instrucciones de este enlace:

## Configuración de WLAN

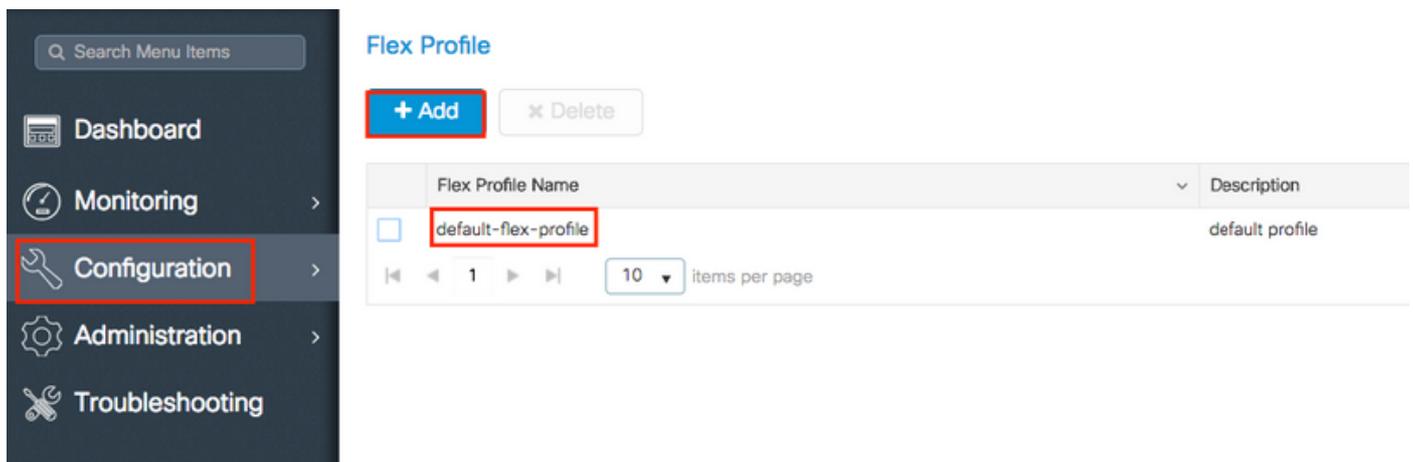
### Establecer AP como modo FlexConnect

A diferencia de la configuración de AireOS, en el WLC 9800 no es posible configurar el modo local o flexconnect AP directamente desde el AP. Siga estos pasos para configurar un AP en el modo FlexConnect.

GUI

Paso 1. Configure un perfil flexible.

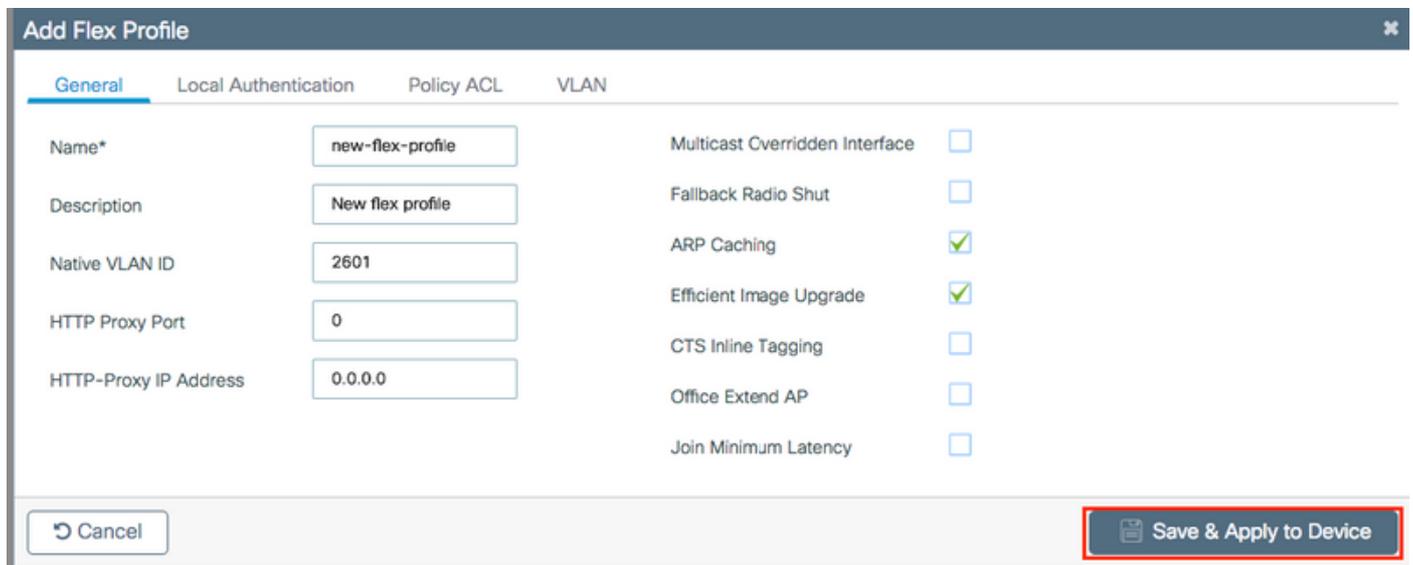
Vaya a **Configuración > Etiquetas y perfiles > Flex** y modifique el **perfil flex predeterminado** o haga clic en **+Agregar** para crear uno nuevo.



The screenshot shows the 'Flex Profile' configuration page. On the left, a navigation menu has 'Configuration' highlighted with a red box. The main content area shows a table with the following data:

Flex Profile Name	Description
default-flex-profile	default profile

Below the table, there are navigation controls including a page number '1' and '10 items per page'. A '+ Add' button is highlighted with a red box.



The screenshot shows the 'Add Flex Profile' dialog box with the 'General' tab selected. The fields and their values are:

- Name\*: new-flex-profile
- Description: New flex profile
- Native VLAN ID: 2601
- HTTP Proxy Port: 0
- HTTP-Proxy IP Address: 0.0.0.0

Checkboxes for various options are shown on the right:

- Multicast Overridden Interface:
- Fallback Radio Shut:
- ARP Caching:
- Efficient Image Upgrade:
- CTS Inline Tagging:
- Office Extend AP:
- Join Minimum Latency:

At the bottom, there is a 'Cancel' button and a 'Save & Apply to Device' button highlighted with a red box.

Paso 2. Agregue las VLAN necesarias (tanto las VLAN de WLAN predeterminadas como las VLAN enviadas desde ISE).

**Nota:** En el paso 3 de la sección **Configuración del perfil de política**, debe seleccionar la **VLAN predeterminada asignada al SSID**. Si utiliza un nombre de VLAN en ese paso, asegúrese de utilizar el mismo nombre de VLAN en la configuración de Flex Profile; de lo contrario, los clientes no podrán conectarse a la WLAN.

## Edit Flex Profile

General

Local Authentication

Policy ACL

VLAN

+ Add

✕ Delete

VLAN Name

ID

ACL Name



0

10

items per page

No items to display

Opcionalmente, puede agregar ACL específicas por VLAN.

VLAN Name\*

vlan2602

VLAN Id\*

2602

ACL Name

Select ACL

✓ Save

↺ Cancel

Opcionalmente, asigne un grupo de servidores Radius para permitir que los AP de FlexConnect realicen la autenticación local.

### Edit Flex Profile

General **Local Authentication** Policy ACL VLAN

Radius Server Group **ISE-kcg-grp** LEAP

EAP Fast Profile Select Profile PEAP

TLS

**RADIUS**

Users

**+ Add**

Username

10 items per page

No items to display

Paso 3. Configure una etiqueta de sitio.

Vaya a **Configuración > Etiquetas y perfiles > Etiquetas > Sitio**. Modifique la **etiqueta de sitio predeterminado** (que es la etiqueta asignada de forma predeterminada a todos los AP) o cree una nueva (Haga clic **+Agregar** para crear una nueva).

Q Search Menu Items

- Dashboard
- Monitoring >
- Configuration** >
- Administration >
- Troubleshooting

### Manage Tags

Policy **Site** RF AP

**+ Add**

Site Tag Name

**default-site-tag**

10 items per page

Asegúrese de desactivar la opción **Habilitar sitio local**; de lo contrario, la opción **Perfil flexible** no está disponible.

**Add Site Tag**

Name\*

Description

AP Join Profile

Flex Profile

Enable Local Site

**Nota:** Cualquier AP que obtenga una etiqueta de sitio con **Habilitar sitio local** habilitado, se configura como modo local. Asimismo, cualquier AP que obtenga una etiqueta de sitio con **Habilitar sitio local** inhabilitado, se configura como modo flexconnect.

Paso 4. Haga un AP asociado al WLC 9800 y asigne la etiqueta Site configurada en el Paso 2.

Navegue hasta **Configuration > Wireless > Access Points > AP name** y establezca la etiqueta Site. A continuación, haga clic en **Update & Apply to Device** para establecer el cambio.

**Access Points**

All APS

AP Name	AP Model	Base Radio MAC	AP Mode	Admin Status
AP1702-05	AIR-CAP1702I-A-K9	00:c...	Local	En...

Number of AP(s): 1

10 Items per page

Configuration > Wireless > Access Points > AP1702-05

**Edit AP**

General | Interfaces | High Availability | Inventory | Advanced

**General**

AP Name\*

Location\*

Base Radio MAC

Ethernet MAC

Admin Status

AP Mode

Operation Status

Fabric Status

**Tags**

Policy

Site

RF

**Version**

Primary Software Version 16.8.1.5

Predownloaded Status N/A

Predownloaded Version N/A

Next Retry Time N/A

Boot Version 15.3.0.0

IOS Version 15.0(20100801)J5348/S

Mini IOS Version 0.0.0.0

**IP Config**

IP Address 172.16.0.200

Static IP

**Time Statistics**

Up Time 0 days 19 hrs 8 mins 11 secs

Controller Associated Time 0 days 18 hrs 57 mins 16 secs

Controller Association Latency 0 days 0 hrs 10 mins 44 secs

**Nota:** Tenga en cuenta que después de cambiar la etiqueta en un AP, pierde su asociación con el WLC 9800 y se une en aproximadamente 1 minuto.

Paso 5. Una vez que el AP se une, observe que el modo AP es Flex

The screenshot shows the Cisco ISE GUI. On the left is a navigation menu with options: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main area is titled 'Access Points' and shows a table of APs. The first AP is AP1702-05, model AIR-CAP1702I-A-K9, with Base Radio MAC 00:c8:8b:26:2c:d0 and AP Mode Flex. Below the table are expandable sections for Radios 802.11a/n/ac, Radios 802.11b/g/n, and Dual-Band Radios. On the right, the 'Edit AP' page is open, showing the 'General' tab. The 'AP Mode' dropdown is set to 'Flex'.

## CLI

```
# config t
# wireless profile flex new-flex-profile
# arp-caching
# description "New flex profile"
# native-vlan-id 2601

# config t
# wireless tag site new-flex-site
# flex-profile new-flex-profile
# no local-site
# site-tag new-flex-site

# config t
# ap <eth-mac-address>
# site-tag new-flex-site
Associating site-tag will cause associated AP to reconnect
# exit

#show ap name <ap-name> config general | inc AP Mode
AP Mode                               : FlexConnect
```

## Configuración del switch

Configure la interfaz del switch a la que se conecta el AP.

```
# config t
# interface <int-id>
# switchport trunk native vlan 2601
# switchport mode trunk
# spanning-tree portfast trunk
# end
```

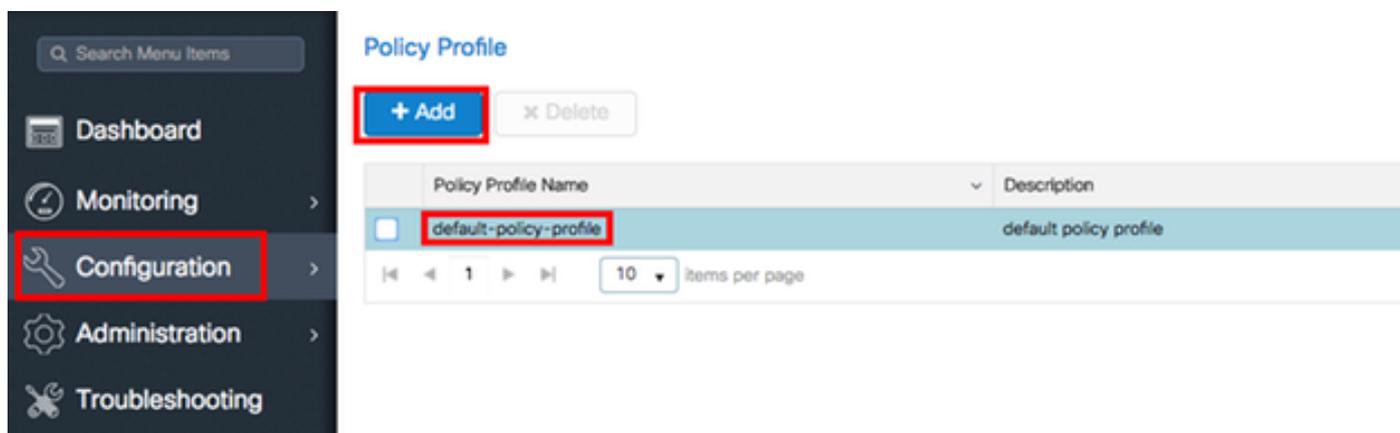
## Configuración del perfil de política

Dentro de un perfil de política puede decidir a qué VLAN asignar los clientes, entre otras configuraciones (como la Lista de controles de acceso [ACL], la Calidad de servicio [QoS], el anclaje de movilidad, los temporizadores, etc.).

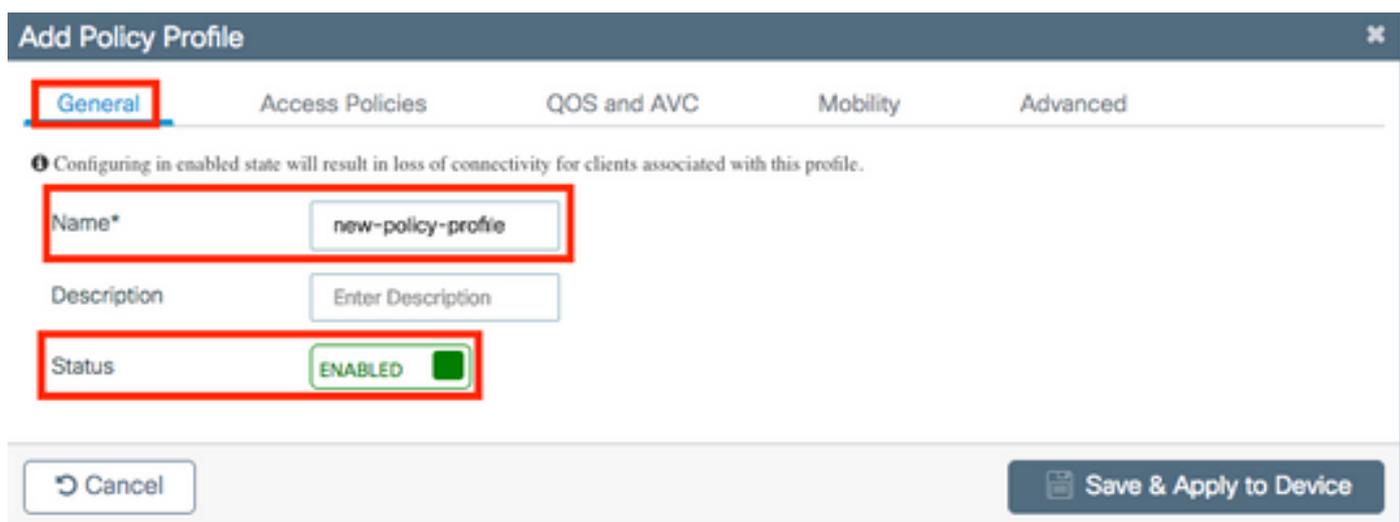
## GUI

Paso 1. Configure el perfil de política que se asignará a la WLAN.

Navegue hasta **Configuration > Tags & Profiles > Policy** y cree uno nuevo o modifique el **default-policy-profile**.



Paso 2. En la **ficha General**, asigne un nombre al perfil de política y cambie su estado a **ACTIVADO**.



Paso 3. En la pestaña **Políticas de acceso** asigne la VLAN a la que se asignan los clientes inalámbricos cuando se conectan a esta WLAN de forma predeterminada.

Puede seleccionar un nombre de VLAN en la lista desplegable o escribir manualmente un id de vlan.

**Nota:** Si selecciona un nombre vlan del menú desplegable, asegúrese de que coincida con el nombre vlan utilizado en el paso 2 de la sección **Establecer AP como modo FlexConnect**.

### Add Policy Profile

General **Access Policies** QOS and AVC Mobility Advanced

**WLAN Local Profiling**

Local HTTP Profiling

Radius HTTP Profiling

Local DHCP Profiling

Local Subscriber Policy Name

**WLAN ACL**

IPv4 ACL

IPv6 ACL

**VLAN**

VLAN/VLAN Group

or

### Edit Policy Profile

General **Access Policies** QOS and AVC Mobility Advanced

**WLAN Local Profiling**

Local HTTP Profiling

Radius HTTP Profiling

Local DHCP Profiling

Local Subscriber Policy Name

**WLAN ACL**

IPv4 ACL

IPv6 ACL

**VLAN**

VLAN/VLAN Group

Paso 4. Navegue hasta la **pestaña Avanzadas** y habilite **Autenticación Central Habilitar** y Permitir Opciones de Sobrecarga AAA. El **switching central** debe estar desactivado.

**La autenticación central** debe estar habilitada si desea que el WLC 9800 realice el proceso de autenticación de forma centralizada. Desactívelo si desea que los AP de FlexConnect autentiquen los clientes inalámbricos.

# Edit Policy Profile



General

Access Policies

QOS and AVC

Mobility

**Advanced**

## WLAN Timeout

Session Timeout (sec)\*

Idle Timeout (sec)\*

Idle Threshold (bytes)\*

Client Exclusion Timeout (sec)\*

## DHCP

DHCP Enable

DHCP Server IP Address

DHCP Opt82 Enable

DHCP Opt82 Ascii

DHCP Opt82 RID

DHCP Opt82 Format

DHCP AP MAC

DHCP SSID

DHCP AP ETH MAC

DHCP AP NAME

DHCP Policy Tag

DHCP AP Location

DHCP VLAN ID

## AAA Policy

Allow AAA Override

NAC State

Policy Name

Fabric Profile

## WLAN Switching Policy

Central Switching

Central Authentication

Central DHCP

Central Association Enable

Flex NAT/PAT

## WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Cancel

**Update & Apply to Device**

## CLI

```
# config t
# wireless profile policy new-policy-profile # central association # vlan <vlan-id or vlan-name>
```

# no shutdown

## Configuración de la etiqueta de política

La etiqueta de política se utiliza para vincular el SSID con el perfil de política. Puede crear una nueva etiqueta de política o utilizar la etiqueta de política predeterminada.

**Nota:** La etiqueta de política predeterminada asigna automáticamente cualquier SSID con un ID de WLAN entre 1 y 16 al perfil de política predeterminado. No se puede modificar ni eliminar. Si tiene una WLAN con ID 17 o superior, no se puede utilizar la etiqueta de política predeterminada.

GUI:

Vaya a **Configuration > Tags & Profiles > Tags > Policy** y agregue uno nuevo si es necesario.

The screenshot shows the 'Manage Tags' page in the configuration GUI. On the left is a dark sidebar with navigation options: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main content area is titled 'Manage Tags' and has four tabs: 'Policy', 'Site', 'RF', and 'AP'. The 'Policy' tab is selected and highlighted with a red box. Below the tabs are '+ Add' and 'x Delete' buttons, with the '+ Add' button highlighted in red. A table below shows two policy tags: 'central-anchor' and 'default-policy-tag'. The 'default-policy-tag' row is highlighted in light blue and has the description 'default policy-tag'. At the bottom of the table, there are navigation arrows and a dropdown menu set to '10 items per page'.

Enlace el perfil WLAN al perfil de política deseado.

The screenshot shows the 'Add Policy Tag' dialog box. It has a title bar with a close button (X). The form contains a 'Name\*' field with the value 'PolicyTagName' and a 'Description' field with the placeholder 'Enter Description'. Below the form are '+ Add' and 'x Delete' buttons, with the '+ Add' button highlighted in red. At the bottom, there are two dropdown menus: 'WLAN Profile' and 'Policy Profile'. Below these are navigation arrows and a dropdown menu set to '10 items per page'. The text 'No items to display' is shown on the right. At the bottom left is a 'Cancel' button, and at the bottom right is a 'Save & Apply to Device' button.

**Add Policy Tag** ✕

Name\*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
<span>◀ ▶</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">0</span> <span>▶ ▶</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">10</span> items per page <span style="float: right;">No items to display</span>	

Map WLAN and Policy

WLAN Profile\*  Policy Profile\*

✕
✓

↶ Cancel
📄 Save & Apply to Device

**Add Policy Tag** ✕

Name\*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> prof-name	default-policy-profile
<span>◀ ▶</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">1</span> <span>▶ ▶</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">10</span> items per page <span style="float: right;">1 - 1 of 1 items</span>	

↶ Cancel
📄 Save & Apply to Device

CLI:

```
# config t
# wireless tag policy <policy-tag-name>
# wlan <profile-name> policy <policy-profile-name>
```

### Asignación de etiqueta de política

Asignar la etiqueta de política al AP

## GUI

Para asignar la etiqueta a un AP navegue a **Configuration > Wireless > Access Points > AP Name > General Tags**, realice la asignación necesaria y luego haga clic en **Update & Apply to Device**.

The screenshot shows the 'Edit AP' configuration page with the following details:

Field	Value
AP Name*	AP1702-05
Location*	default location
Base Radio MAC	00:c:.....
Ethernet MAC	00:.....
Admin Status	Enabled
AP Mode	Flex
Operation Status	Registered
Fabric Status	Disabled
Policy (in red box)	new-policy-tag
Site	new-flex-site
RF	default-rf-tag

Version information:

Field	Value
Primary Software Version	15.0...
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	15.0...
iOS Version	15.0...
Mini iOS Version	0.0.0.0

IP Config:

Field	Value
IP Address	172.16.0.200
Static IP	<input type="checkbox"/>

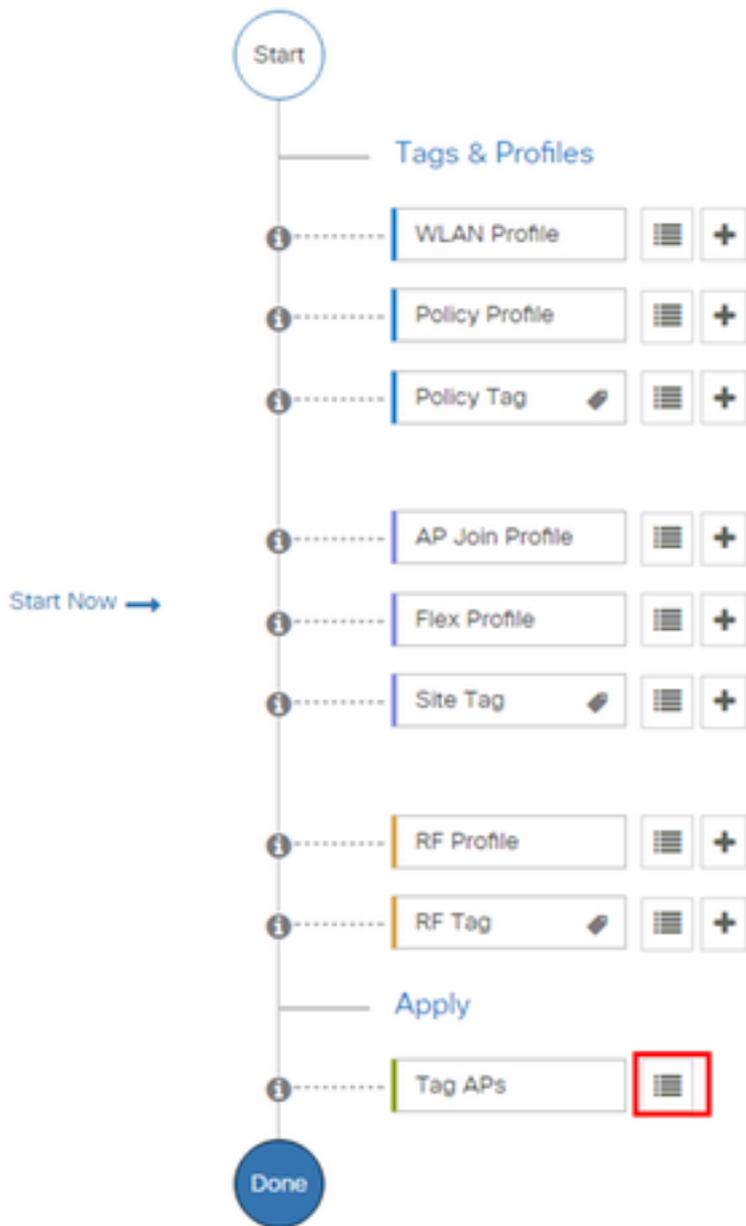
Time Statistics:

Field	Value
Up Time	1 days 1 hrs 44 mins 59 secs
Controller Associated Time	0 days 5 hrs 32 mins 5 secs
Controller Association Latency	0 days 20 hrs 11 mins 24 secs

Buttons: Cancel (left), Update & Apply to Device (right, in red box).

**Nota:** Tenga en cuenta que después de cambiar la etiqueta de política en un AP, pierde su asociación con el WLC 9800 y se une en aproximadamente 1 minuto.

Para asignar la misma etiqueta de política a varios AP, navegue hasta **Configuration > Wireless > Wireless Setup > Start Now > Apply**.



Seleccione los AP a los que desea asignar la etiqueta y haga clic en + Tag AP

**+ Tag APs**

Number of APs: 3  
Selected Number of APs: 3

<input checked="" type="checkbox"/>	AP Name	AP Model	AP MAC	AP Mode	Admin Status	Operation Status	Policy Tag	Site Tag
<input checked="" type="checkbox"/>	AP3802-02-WS	AIR-AP3802I-A-K9	C0-40-00-10-11-00	Local	Enabled	Registered	default-policy-tag	default-site-tag
<input checked="" type="checkbox"/>	AP3802-01	AIR-AP2802I-B-K9	28-40-00-10-11-00	Local	Enabled	Registered	default-policy-tag	default-site-tag
<input checked="" type="checkbox"/>	AP3802-02	AIR-AP3802I-B-K9	C0-40-00-10-11-00	Local	Enabled	Registered	default-policy-tag	default-site-tag

10 items per page | 1 - 3 of 3 items

Seleccione la etiqueta blanca y haga clic en **Guardar y aplicar al dispositivo**

**Tag APs** [X]

Tags

Policy:  ▼

Site:  ▼

RF:  ▼

## CLI

```
# config t
# ap <ethernet-mac-addr>
# policy-tag <policy-tag-name>
# end
```

## Configuración de ISE

Para la configuración de ISE v1.2, verifique este enlace:

[Configuración de ISE](#)

## Verificación

Puede utilizar estos comandos para verificar la configuración actual

```
# show run wlan
# show run aaa
# show aaa servers
# show ap config general
# show ap name <ap-name> config general
# show ap tag summary
# show ap name <AP-name> tag detail
# show wlan { summary | id | name | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```

## Troubleshoot

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

**Nota:** Dependiendo del volumen de registros que se generen, puede retornar unas horas a varios días.

Para ver los seguimientos que el WLC 9800 recolectó de forma predeterminada, puede conectarse a través de SSH/Telnet con el WLC 9800 y seguir 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 de vuelta al momento en que ocurrió el problema.

```
# show clock
```

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

```
# show logging
```

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

```
# 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 están registrando al nivel de depuración para todos los procesos que encuentran las condiciones activadas (dirección mac, dirección ip, etc). Esto aumentaría el volumen de registros. Por lo tanto, se recomienda borrar todas las condiciones cuando no se realiza la depuración activa

Paso 4. Suponiendo que la dirección mac en prueba no se enumeró como condición en el Paso 3, recopile los seguimientos de nivel de aviso siempre activos para la dirección mac específica.

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

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

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

### Debugging condicional y Rastreo Activo de Radio

Si los seguimientos siempre activos no le 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 proporcionará 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, siga estos pasos.

Paso 5. Asegúrese de que no haya condiciones de depuración habilitadas.

```
# clear platform condition all
```

Paso 6. 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 2085978494 segundos.

```
# 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 <aaaa.bbbb.cccc>` por dirección mac.

**Nota:** No ve el resultado de la actividad del cliente en la sesión de terminal, ya que todo se almacena en búfer internamente para ser visto más tarde.

Paso 7. Reproduzca el problema o comportamiento que desea supervisar.

Paso 8. Detenga las depuraciones si el problema se reproduce antes de que se active la hora de monitor predeterminada o configurada.

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

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

```
ra_trace_MAC_aaabbccccc_HHMMSS.XXX_timezone_Day_Week_Month_Day_year.log
```

Paso 9. Recopile el archivo de la actividad de la dirección mac. Puede copiar el archivo ra trace .log en un servidor externo o mostrar el resultado directamente en la pantalla.

Verifique el nombre del archivo de seguimientos de RA

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

Copie el archivo a un servidor externo:

```
# copy bootflash:ra_trace_MAC_aaaabbbccccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log  
tftp://a.b.c.d/ra-FILENAME.txt
```

Mostrar el contenido:

```
# more bootflash:ra_trace_MAC_aaaabbbccccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Paso 10. Si la causa raíz todavía no es obvia, recopile los registros internos que son una vista más detallada de los registros de nivel de depuración. No es necesario que vuelva a depurar el cliente, ya que sólo estamos examinando más detalladamente los registros de depuración que ya se han recopilado y almacenado internamente.

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> }  
to-file ra-internal-<FILENAME>.txt
```

**Nota:** Este resultado del comando devuelve seguimientos para todos los niveles de registro para todos los procesos y es bastante voluminoso. Póngase en contacto con el TAC de Cisco para que le ayude a analizar estos seguimientos.

Puede copiar ra-internal-FILENAME.txt en un servidor externo o mostrar el resultado directamente en la pantalla.

Copie el archivo a un servidor externo:

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

Mostrar el contenido:

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

Paso 11. Elimine las condiciones de depuración.

```
# clear platform condition all
```

**Nota:** Asegúrese de quitar siempre las condiciones de depuración después de una sesión de resolución de problemas.