

# Configuración de la autenticación 802.1X en Catalyst serie 9800 Wireless Controller

## Contenido

---

### [Introducción](#)

### [Prerequisites](#)

#### [Requirements](#)

#### [Componentes Utilizados](#)

### [Configurar](#)

#### [Diagrama de la red](#)

#### [Configuración de WLC](#)

##### [Configuración AAA en WLC 9800](#)

##### [Configuración del perfil WLAN](#)

##### [Configuración del perfil de la política](#)

##### [Configuración de etiquetas de políticas](#)

##### [Asignación de etiquetas de políticas](#)

#### [Configuración de ISE](#)

##### [Declare el WLC en ISE](#)

##### [Crear nuevo usuario en ISE](#)

##### [Creación del perfil de autorización](#)

##### [Crear un conjunto de políticas](#)

##### [Crear política de autenticación](#)

##### [Crear directiva de autorización](#)

### [Verificación](#)

### [Troubleshoot](#)

#### [Troubleshooting en el WLC](#)

#### [Resolución de problemas en ISE](#)

---

## Introducción

Este documento describe cómo configurar una WLAN con seguridad 802.1X en un Cisco Catalyst 9800 Series Wireless Controller.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- 802.1x

### Componentes Utilizados

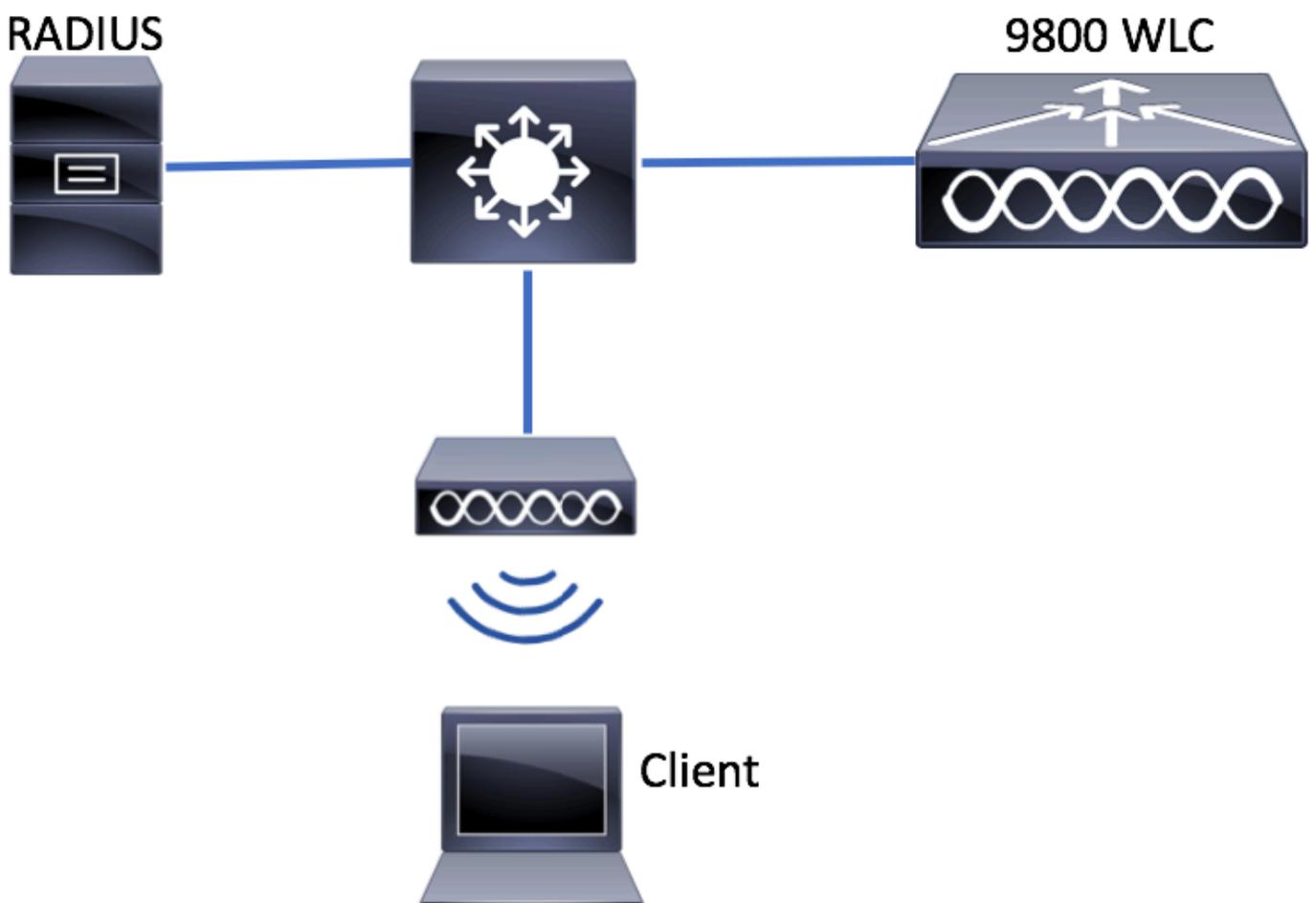
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Controlador inalámbrico Catalyst serie 9800 (Catalyst 9800-CL)
- Cisco IOS® XE Gibraltar 17.3.x
- Cisco ISE 3.0

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

## Configurar

Diagrama de la red

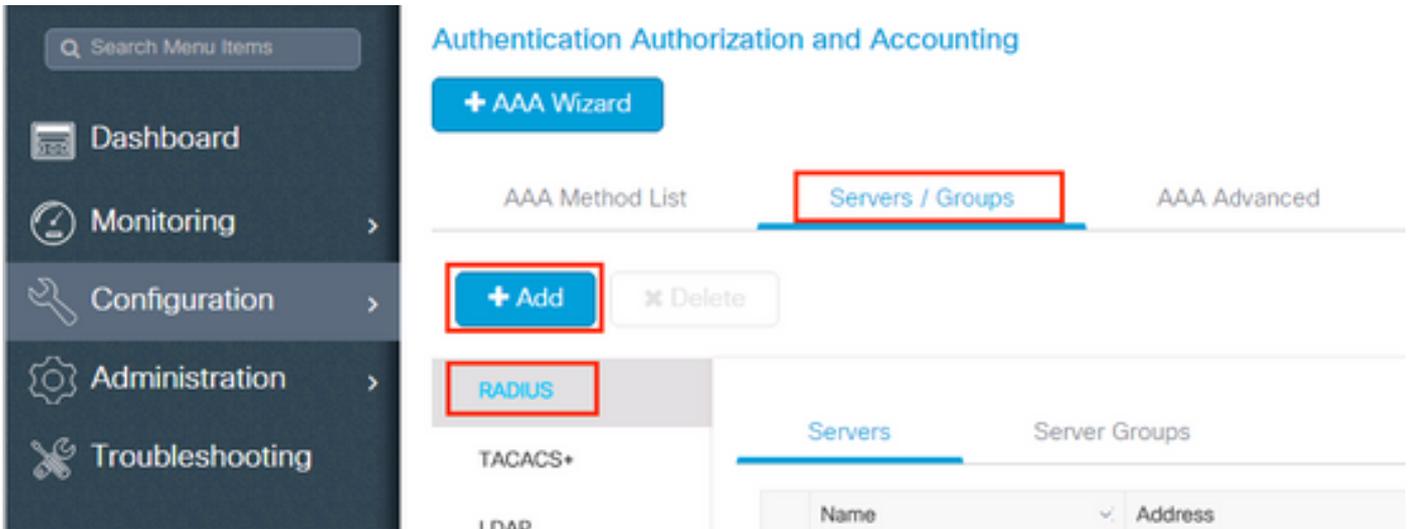


## Configuración de WLC

Configuración AAA en WLC 9800

GUI:

Paso 1. Declarar servidor RADIUS. Desplácese hasta **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add** la información del servidor RADIUS e introdúzcala.



Asegúrese de que **Support for CoA** esté habilitado si planea utilizar la Autenticación web central (o cualquier tipo de seguridad que requiera un cambio de autorización [CoA]) en el futuro.

A screenshot of the 'Create AAA Radius Server' form. The form contains the following fields and options:

- Name\*: ISE-kcg
- IPV4/IPV6 Server Address\*: 172.16.0.11
- Shared Secret\*: .....
- Confirm Shared Secret\*: .....
- Auth Port: 1812
- Acct Port: 1813
- Server Timeout (seconds): 1-1000
- Retry Count: 0-100
- Support for CoA: ENABLED (with a green toggle switch)
- Clear PAC Key:
- Set New PAC Key:

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

Paso 2. Agregue el servidor RADIUS a un grupo RADIUS. Desplácese hasta **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add**. Asignar un nombre al grupo y mueva el servidor que creó anteriormente en la lista de **Assigned Servers**.

**Create AAA Radius Server Group**

Name\*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Available Servers

Assigned Servers

Paso 3. Cree una lista de métodos de autenticación. Desplácese hasta **Configuration > Security > AAA > AAA Method List > Authentication > + Add**.

**Authentication Authorization and Accounting**

Servers / Groups

General

Authorization

Name

Introduzca la información:

Quick Setup: AAA Authentication

Method List Name\*

Type\*

Group Type

Fallback to local

Available Server Groups

- radius
- ldap
- tacacs+
- ISE-kcg-grp

Assigned Server Groups

- ISE-grp-name

**CLI:**

```
# config t # aaa new-model # radius server <radius-server-name> # address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813 # timeout 300 # retransmit 5
# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>
# aaa authentication dot1x <dot1x-list-name> group <radius-grp-name>
```

**Nota sobre la Detección de Servidor Muerto AAA**

Una vez configurado el servidor RADIUS, puede comprobar si se considera "ACTIVO":

```
#show aaa servers | s WNCDC Platform State from WNCDC (1) : current UP Platform State from WNCDC (2) : current
```

Usted puede configurar el **dead criteria**, así como el en **deadtime** su WLC, especialmente si usted utiliza servidores RADIUS múltiples.

```
#radius-server dead-criteria time 5 tries 3 #radius-server deadtime 5
```

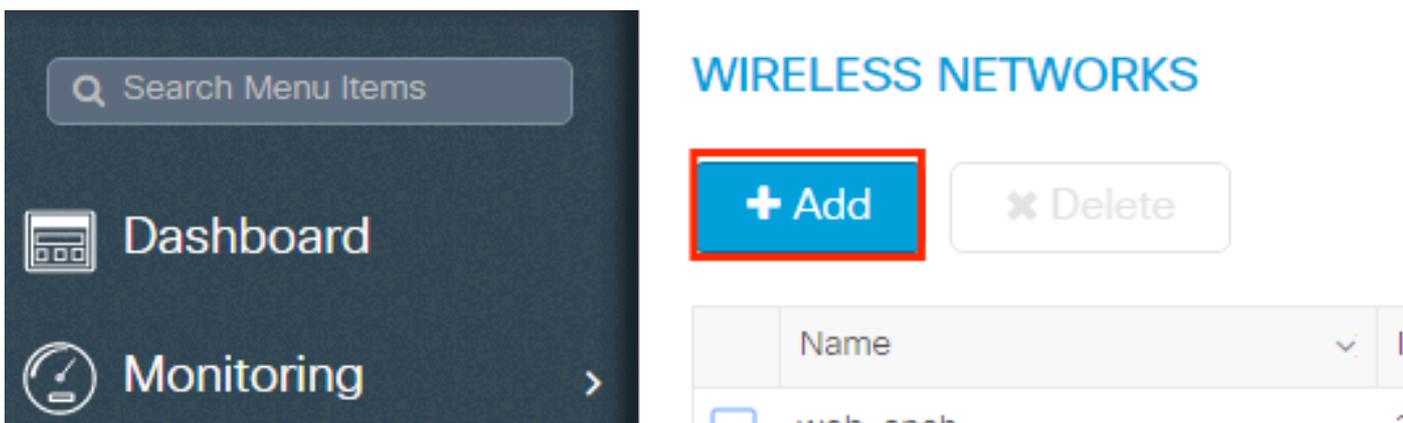
 **Nota:** El **dead criteria** es el criterio utilizado para marcar un servidor RADIUS como muerto. Consta de: 1. Un tiempo de espera (en segundos) que representa la cantidad de tiempo que debe transcurrir desde la última vez que el controlador recibió un paquete válido del servidor RADIUS hasta el momento en que el servidor se marca como muerto. 2. Un contador, que representa el número de tiempos de espera consecutivos que deben ocurrir en el controlador antes de que el servidor RADIUS se marque como muerto.

 **Nota:** El **deadtime** especifica la cantidad de tiempo (en minutos) que el servidor permanece en estado inactivo después de que el criterio de inactividad lo marque como inactivo. Una vez que vence el tiempo muerto, el controlador marca el servidor como ACTIVO (ALIVE) y notifica a los clientes registrados sobre el cambio de estado. Si el servidor sigue siendo inalcanzable después de que el estado se marque como ACTIVO y si se cumple el criterio de inactividad, el servidor se marcará de nuevo como inactivo durante el intervalo de tiempo muerto.

## Configuración del perfil WLAN

### GUI:

Paso 1. Cree la WLAN. Vaya a **Configuration > Wireless > WLANs > + Add** y configure la red según sea necesario.



Paso 2. Introduzca la información de la WLAN

### Add WLAN

**General**      Security      Advanced

Profile Name*	<input type="text" value="prof-name"/>	Radio Policy	<input type="text" value="All"/>
SSID	<input type="text" value="ssid-name"/>	Broadcast SSID	<input checked="" type="checkbox"/> ENABLED
WLAN ID*	<input type="text" value="1"/>		
Status	<input checked="" type="checkbox"/> ENABLED		

Paso 3. Vaya a la ficha Seguridad y seleccione el método de seguridad necesario. En este caso, **WPA2 + 802.1x**.

**Add WLAN** ✕

General      **Security**      Advanced

Layer2      Layer3      AAA

Layer 2 Security Mode      WPA + WPA2 ▼

MAC Filtering     

**Protected Management Frame**

Fast Transition      Adaptive Enab... ▼

Over the DS     

Reassociation Timeout      20

PMF      Disabled ▼

**WPA Parameters**

WPA Policy     

**Add WLAN** ✕

PMF      Disabled ▼

**WPA Parameters**

WPA Policy     

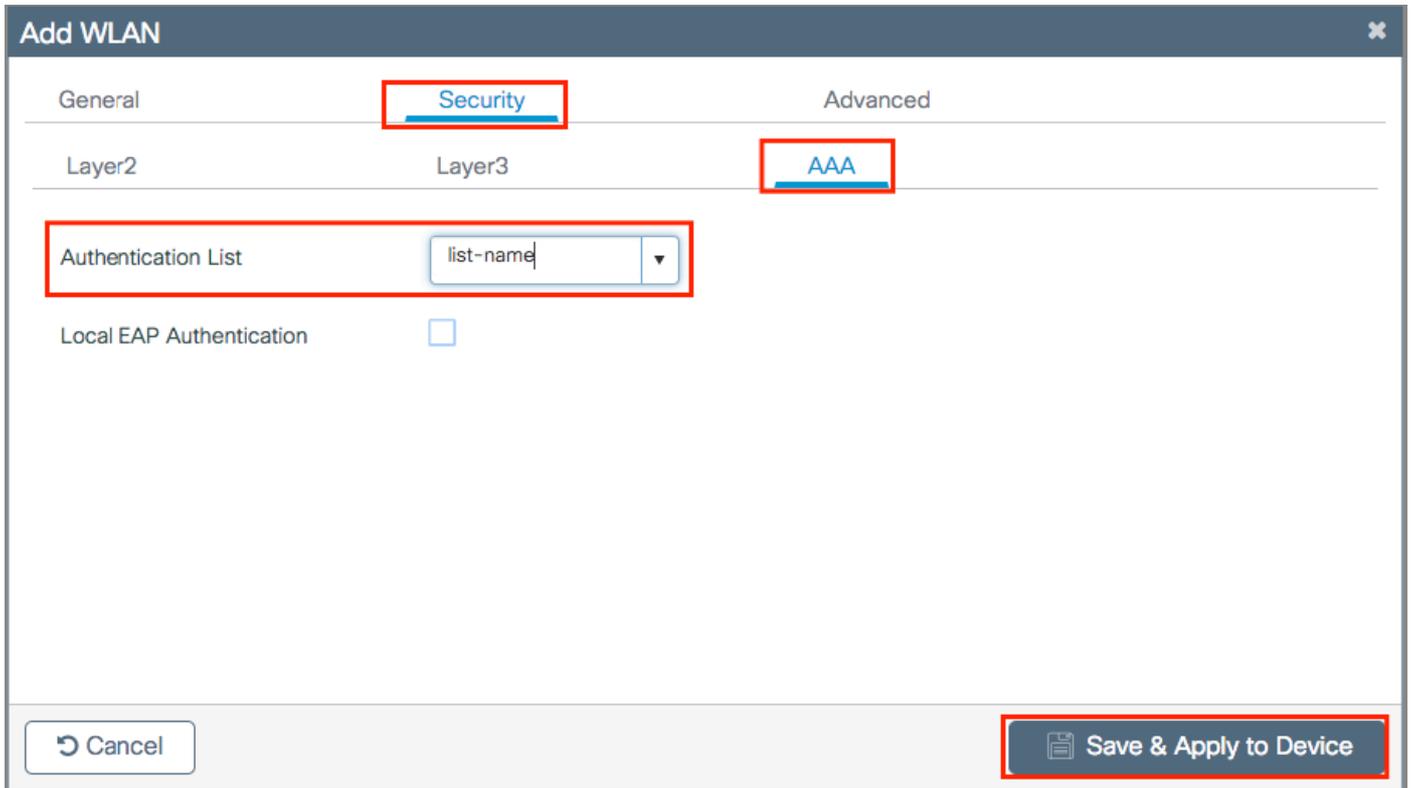
WPA2 Policy     

WPA2 Encryption      AES(CCMP128)   
 CCMP256   
 GCMP128   
 GCMP256

Auth Key Mgmt      802.1x ▼

Paso 4. En la **Security** > **AAA** pestaña, seleccione el método de autenticación creado en el Paso 3 de la sección Configuración AAA en el WLC 9800.



#### CLI:

```
# config t # wlan <profile-name> <wlan-id> <ssid-name> # security dot1x authentication-list <dot1x-list-name> # no shutdown
```

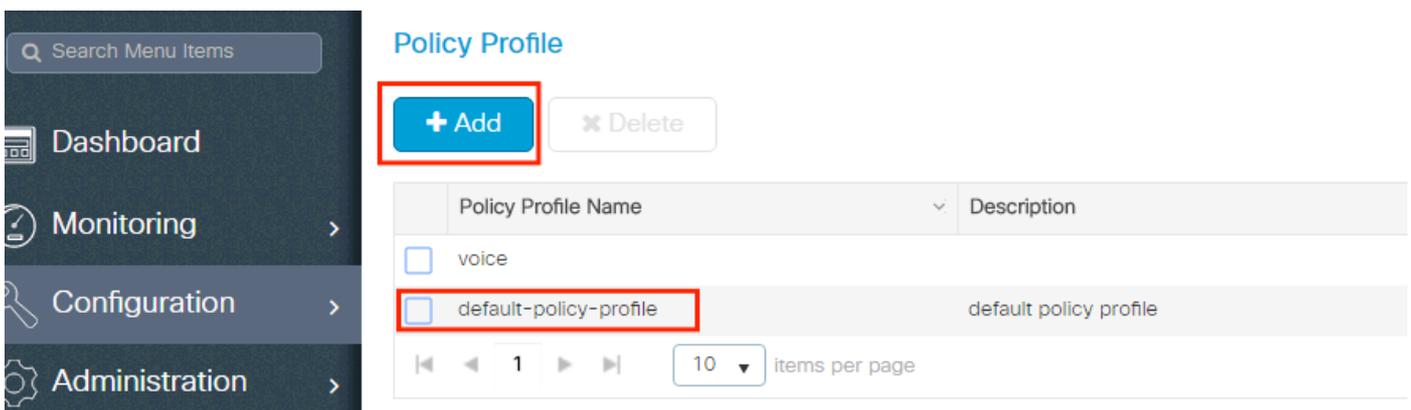
Configuración del perfil de la política

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], calidad de servicio [QoS], ancla de movilidad, temporizadores, etc.).

Puede utilizar el perfil de directiva predeterminado o puede crear un nuevo perfil.

#### GUI:

Navegue hasta **Configuration > Tags & Profiles > Policy Profile** y configure su **default-policy-profile** o cree uno nuevo.



Asegúrese de que el perfil esté habilitado.

Además, si el punto de acceso (AP) está en modo local, asegúrese de que el perfil de política tenga activados **Central Switching** y **Central Authentication**.

### Edit 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*	default-policy-profile
Description	default policy profile
Status	ENABLED <input checked="" type="checkbox"/>
Passive Client	<input type="checkbox"/> DISABLED
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED

#### CTS Policy

Inline Tagging	<input type="checkbox"/>
SGACL Enforcement	<input type="checkbox"/>
Default SGT	2-65519

#### WLAN Switching Policy

Central Switching	<input checked="" type="checkbox"/>
Central Authentication	<input checked="" type="checkbox"/>
Central DHCP	<input checked="" type="checkbox"/>
Central Association Enable	<input checked="" type="checkbox"/>
Flex NAT/PAT	<input type="checkbox"/>

Seleccione la VLAN a la que se deben asignar los clientes en la pestaña **Políticas de acceso**.

## Edit Policy Profile

General

**Access Policies**

QOS and AVC

Mobility

Advanced

### WLAN Local Profiling

HTTP TLV Caching

RADIUS Profiling

DHCP TLV Caching

Local Subscriber Policy Name

Search or Select



### VLAN

VLAN/VLAN Group

VLAN2602



Multicast VLAN

Enter Multicast VLAN

### WLAN ACL

IPv4 ACL

Search or Select



IPv6 ACL

Search or Select



### URL Filters

Pre Auth

Search or Select



Post Auth

Search or Select



Si tiene pensado que ISE devuelva atributos en la asignación de VLAN de tipo Access-Accept, habilite la anulación de AAA en la **Advanced** ficha:

✕
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**

IPv4 DHCP Required

DHCP Server IP Address

Show more >>>

**AAA Policy**

Allow AAA Override

NAC State

Policy Name

Fabric Profile

Umbrella Parameter Map

mDNS Service Policy  [Clear](#)

**WLAN Flex Policy**

VLAN Central Switching

Split MAC ACL

**Air Time Fairness Policies**

2.4 GHz Policy

5 GHz Policy

Cancel
Update & Apply to Device

**CLI:**

```
# config # wireless profile policy <policy-profile-name>
# aaa-override # central switching # description "<description>" # vlan <vlanID-or-VLAN_name> # no shutdown
```

Configuración de etiquetas de políticas

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

**Nota:** default-policy-tag 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 default-policy-tag.

**GUI:**

Desplácese hasta uno nuevo **Configuation > Tags & Profiles > Tags > Policy** y agréguelo si es necesario.

Search Menu Items

Dashboard

Monitoring >

Configuration >

Administration >

Troubleshooting

### Manage Tags

Policy Site RF AP

+ Add x Delete

Policy Tag Name	Description
<input type="checkbox"/> central-anchor	
<input type="checkbox"/> default-policy-tag	default policy-tag

1 10 items per page

Vincule su perfil de WLAN con el perfil de política deseado.

### Add Policy Tag

Name\* PolicyTagName

Description Enter Description

+ Add x Delete

WLAN Profile Policy Profile

0 10 items per page No items to display

Cancel Save & Apply to Device

**Add Policy Tag** ✕

Name\*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
◀ ◁ 0 ▷ ▶	10 items per page
No items to display	

Map WLAN and Policy

WLAN Profile\*

Policy Profile\*

✕
✓

↶ Cancel
📄 Save & Apply to Device

**Add Policy Tag** ✕

Name\*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
◀ ◁ 1 ▷ ▶	10 items per page
<input type="checkbox"/> prof-name	default-policy-profile
1 - 1 of 1 items	

↶ Cancel
📄 Save & Apply to Device

**CLI:**

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

Asignación de etiquetas de políticas

Asigne la etiqueta de política a los AP necesarios.

**GUI:**

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

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

- General Tab:** AP Name\* (AP3802-02-WS), Location\* (default location), Base Radio MAC (00:42:68:c6:41:20), Ethernet MAC (00:42:68:a0:d0:22), Admin Status (Enabled), AP Mode (Local), Operation Status (Registered), Fabric Status (Disabled).
- Tags Section:** Policy (default-policy-tag), Site (default-site-tag), RF (default-rf-tag).
- Version Section:** Primary Software Version (10.0.200.50), Predownloaded Status (N/A), Predownloaded Version (N/A), Next Retry Time (N/A), Boot Version (1.0.0), IOS Version (10.0.200.52), Mini IOS Version (0.0.0.0).
- IP Config Section:** IP Address (172.16.0.207), Static IP (unchecked).
- Time Statistics Section:** Up Time (9 days 1 hrs 17 mins 24 secs), Controller Associated Time (0 days 3 hrs 26 mins 41 secs), Controller Association Latency (8 days 21 hrs 50 mins 33 secs).

Buttons at the bottom: Cancel (left), Update & Apply to Device (right, highlighted).

 **Nota:** Tenga en cuenta que cuando se cambia la etiqueta de la política en un AP, deja caer su asociación al WLC 9800 y se une de nuevo unos momentos más tarde.

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

Start

### Tags & Profiles



WLAN Profile



Policy Profile



Policy Tag



AP Join Profile



Flex Profile



Site Tag



RF Profile



RF Tag



### Apply



Tag APs

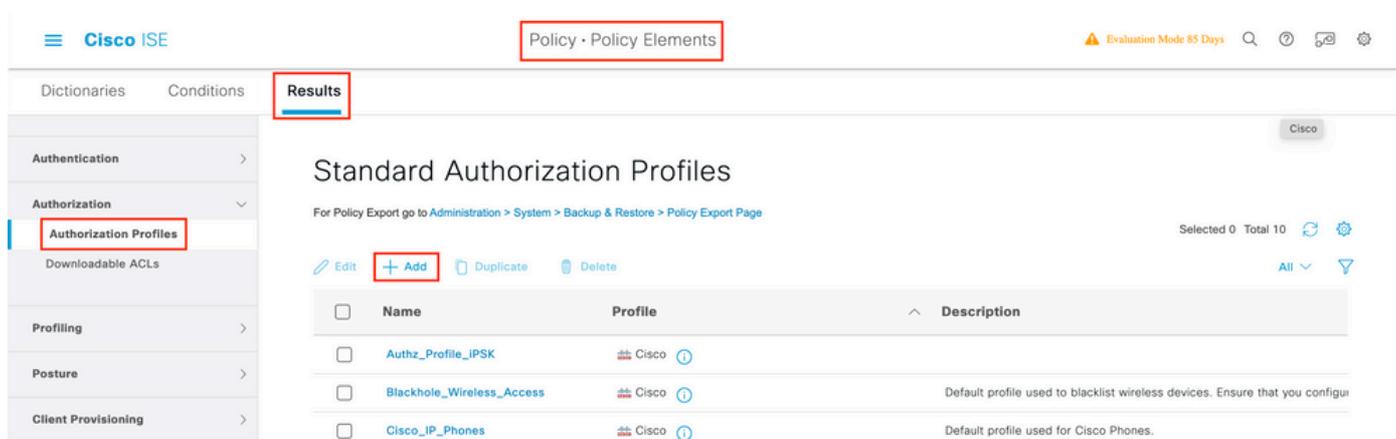


Done

Start Now →

consta de un conjunto de atributos que se devuelven cuando se coincide una condición. El perfil de autorización determina si el cliente tiene acceso o no a la red, las listas de control de acceso (ACL) de inserción, la invalidación de VLAN o cualquier otro parámetro. El perfil de autorización que se muestra en este ejemplo envía una aceptación de acceso para el cliente y asigna el cliente a la VLAN 1416.

Paso 1. Desplácese hasta **Policy > Policy Elements > Results > Authorization > Authorization Profiles** y haga clic en el **Add** botón .



Paso 2. Introduzca los valores como se muestra en la imagen. Aquí podemos devolver atributos de anulación AAA como VLAN por ejemplo. El WLC 9800 acepta los atributos de túnel 64, 65, 81 que utilizan el ID o el nombre de VLAN, y acepta también el uso del **AirSpace-Interface-Name** atributo.

Cisco ISE Policy - Policy Elements Evaluation Mode 85 Days

Dictionarys Conditions **Results**

Authentication >

Authorization >

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

Authorization Profiles > PermitAccessVlan1416

### Authorization Profile

\* Name PermitAccessVlan1416

Description

\* Access Type ACCESS\_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

#### Common Tasks

Security Group

VLAN Tag ID 1 [Edit Tag](#) ID/Name 1416

Voice Domain Permission

#### Advanced Attributes Settings

Select an item

#### Attributes Details

Access Type = ACCESS\_ACCEPT

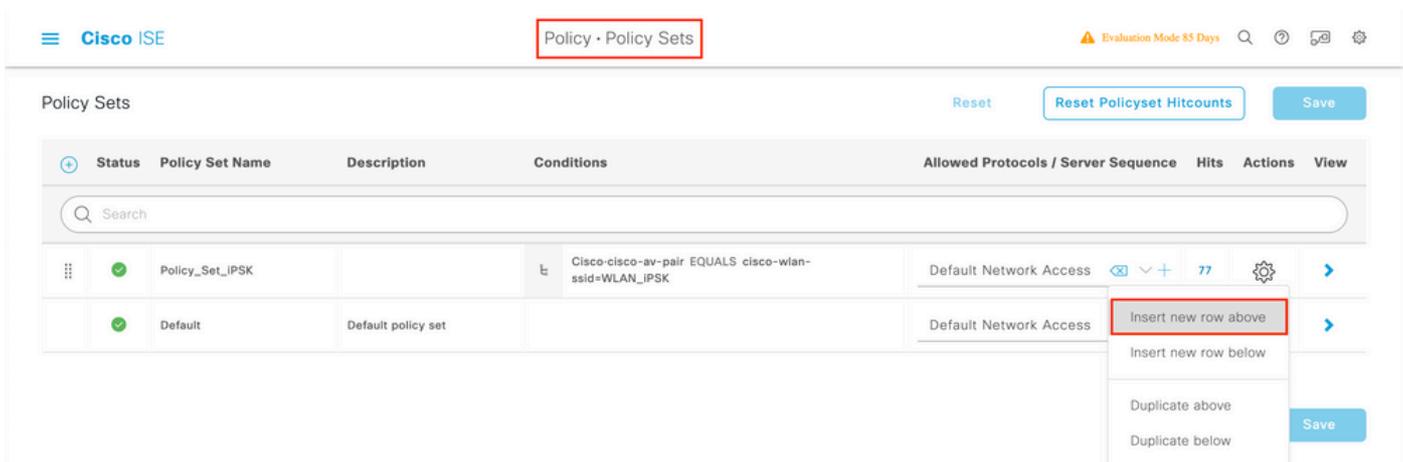
Tunnel-Private-Group-ID = 1:1416

Tunnel-Type = 1:13

Tunnel-Medium-Type = 1:6

## Crear un conjunto de políticas

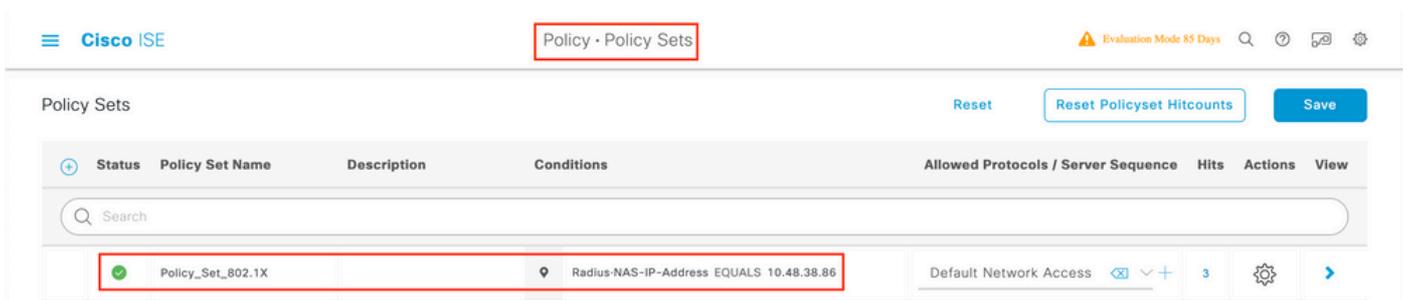
Un conjunto de directivas define una colección de reglas de autenticación y autorización. Para crear uno, vaya a **Policy > Policy Sets**, haga clic en el engranaje del primer conjunto de políticas de la lista y seleccione **Insert new row above** como se muestra en esta imagen:



Configure un nombre y cree una condición para este conjunto de directivas. En este ejemplo, la condición específica que coincidamos con el tráfico que viene del WLC:

Radius:NAS-IP-Address EQUALS X.X.X.X // X.X.X.X is the WLC IP address

Asegúrese de que **Default Network Access** está seleccionado en **Allowed Protocols / Server Sequence**.



### Crear política de autenticación

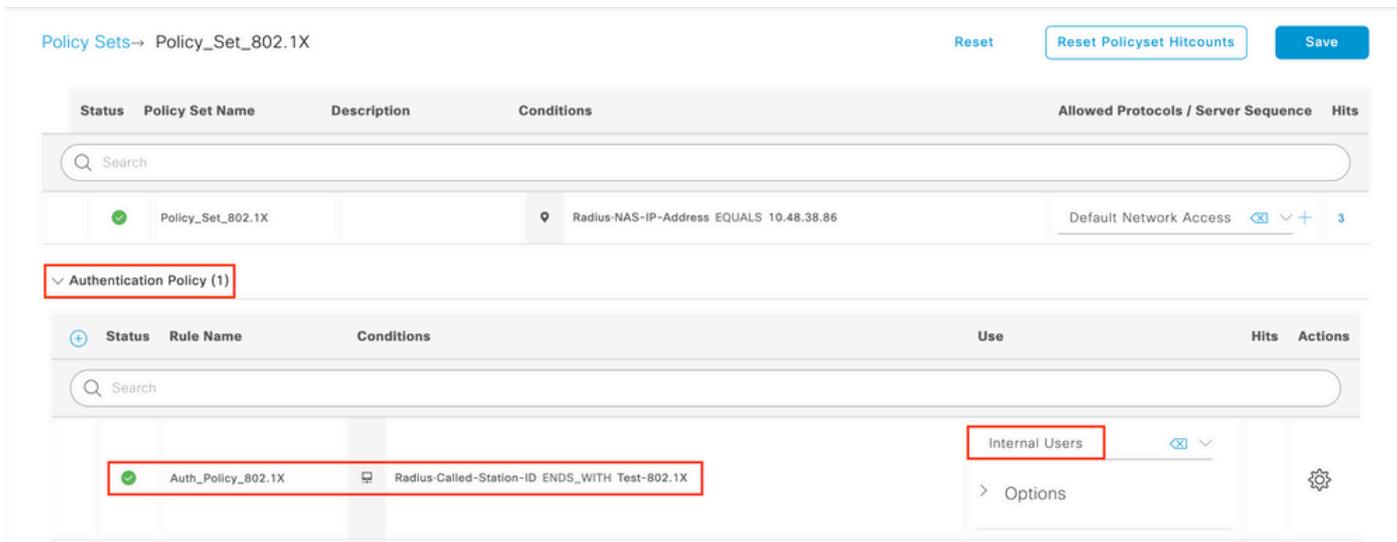
Para configurar las directivas de autenticación y autorización, debe introducir la configuración del conjunto de directivas. Esto se puede hacer si hace clic en la flecha azul a la derecha de la **Policy Set** línea:



Las **políticas de autenticación** se utilizan para verificar si las credenciales de los usuarios son correctas (verificar si el usuario es realmente quien dice ser). En **Authenticaton Policy**, cree una política de autenticación y configúrela como se muestra en esta imagen. La condición para la política utilizada en este ejemplo es:

RADIUS:Called-Station-ID ENDS\_WITH <SSID> // <SSID> is the SSID of your WLAN

Además, elija **Usuarios internos** en la **Use** pestaña de esta Política de autenticación.

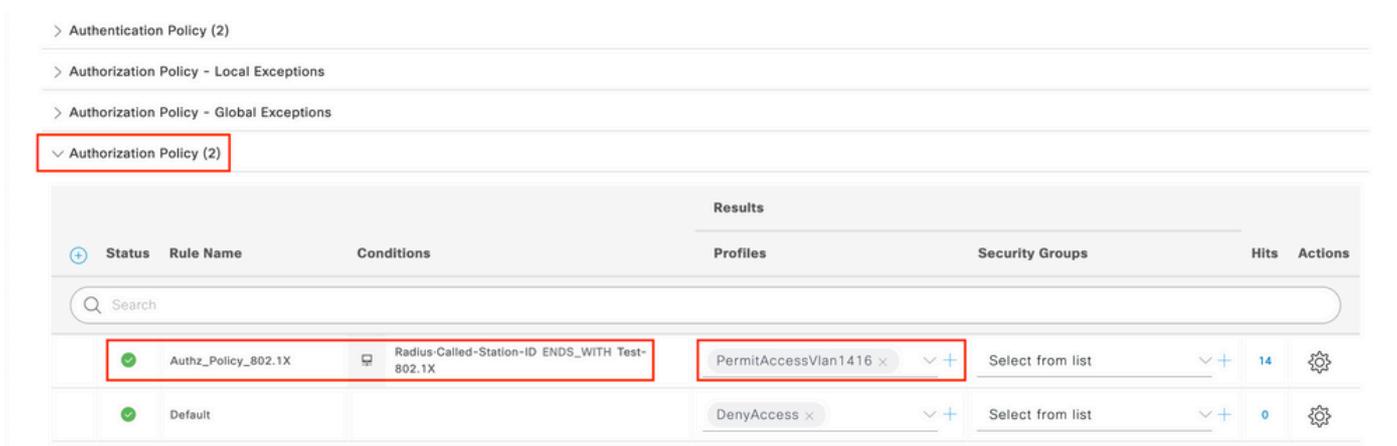


### Crear directiva de autorización

En la misma página, vaya a **Authorization Policy** y cree una nueva. La condición para esta directiva de autorización es:

RADIUS:Called-Station-ID ENDS\_WITH <SSID> // <SSID> is the SSID of your WLAN

En la **Result > Profiles** ficha de esta directiva, seleccione la directiva **Authorization Profile** que creó anteriormente. Esto hace que ISE envíe los atributos correctos al WLC si el usuario está autenticado.



En este momento, toda la configuración para el WLC e ISE está completa, ahora puede intentar conectarse con un cliente.

Para obtener más información sobre las políticas de ISE Allow Protocols, consulte el capítulo: [Manage Authentication Policies from the Cisco Identity Services Engine Administrator Guide](#) [Manage Authentication Policies](#)

Para obtener más información sobre las fuentes de identidad de ISE, consulte el capítulo: Administración de usuarios y fuentes de identidad externas de la Guía del administrador de Cisco Identity Services Engine: [fuentes de identidad](#)

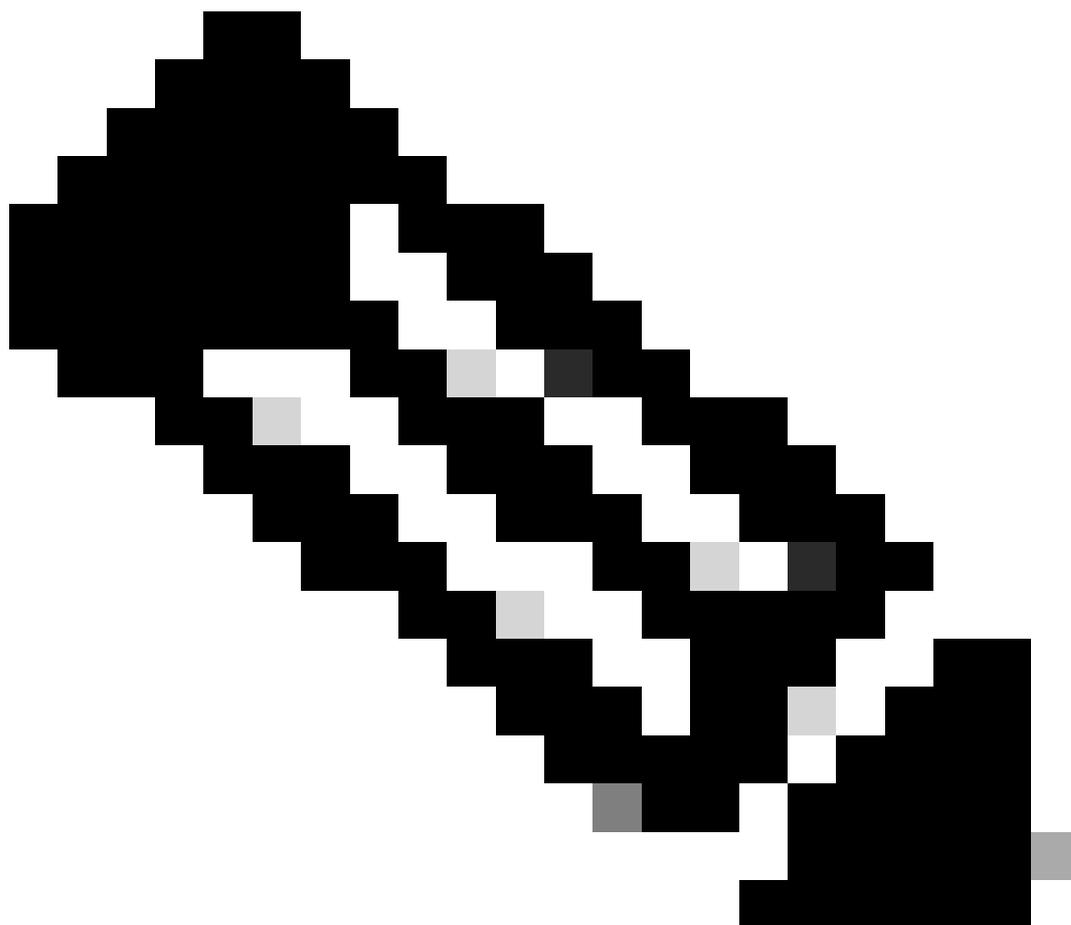
## Verificación

Puede utilizar estos comandos para verificar su configuración actual:

```
# show run wlan // WLAN configuration # show run aaa // AAA configuration (server, server group, methods) # show aaa servers // Configured AAA servers
# show ap tag summary // Tag information for AP'S
# show wlan { summary | id | name | all } // WLAN details
# show wireless tag policy detailed <policy-tag name> // Detailed information on given policy tag
# show wireless profile policy detailed <policy-profile name> // Detailed information on given policy profile
```

## Troubleshoot

---



---

**Nota:** El uso de balanceadores de carga externos es correcto. Sin embargo, asegúrese de que el equilibrador de carga funcione por cliente mediante el atributo RADIUS call-station-id. Confiar en el puerto de origen UDP no es un mecanismo admitido para equilibrar las solicitudes RADIUS del 9800.

---

## Troubleshooting en el WLC

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

Depende del volumen de registros generados, pero por lo general, puede retroceder unas horas a varios días.

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

Paso 1. Verifique la hora actual del WLC para que pueda rastrear los registros en el tiempo hasta cuando ocurrió el problema.

```
# show clock
```

Paso 2. Recopile los syslogs del buffer del WLC 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 corresponde.

```
# 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 Ad
```

---

 **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. Suponga que la dirección MAC en prueba no se incluyó como condición en el Paso 3, recopile los seguimientos del nivel de aviso

siempre activo 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 de la sesión o copiar el archivo en 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>
```

### 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). Puede hacerlo a través de la GUI o la CLI.

#### CLI:

Para habilitar la depuración condicional, siga estos pasos:

Paso 5. Asegúrese de que no hay 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.

Este comando comienza 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:** Usted no ve la salida de la actividad del cliente en una sesión de terminal, ya que todo se almacena en buffer internamente para ser visto más tarde.

---

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

Paso 8. Detenga las depuraciones si el problema se reproduce antes de que transcurra el tiempo de supervisión predeterminado o configurado.

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

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

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

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

Verifique el nombre del archivo de seguimiento activo por radio:

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

Copie el archivo en un servidor externo:

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

Muestre el contenido:

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

Paso 10. 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 examinamos 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:** Esta salida de comando devuelve seguimientos para todos los niveles de registro para todos los procesos y es bastante voluminosa. Utilice Cisco TAC para analizar estos seguimientos.

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

Copie el archivo en un servidor externo:

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

Muestre el contenido:

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

Paso 11. Elimine las condiciones de depuración.

```
# clear platform condition all
```



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

## GUI:

Paso 1. Vaya a **Troubleshooting > Radioactive Trace > + Add** y especifique la dirección MAC/IP del cliente o clientes para los que desea solucionar problemas.

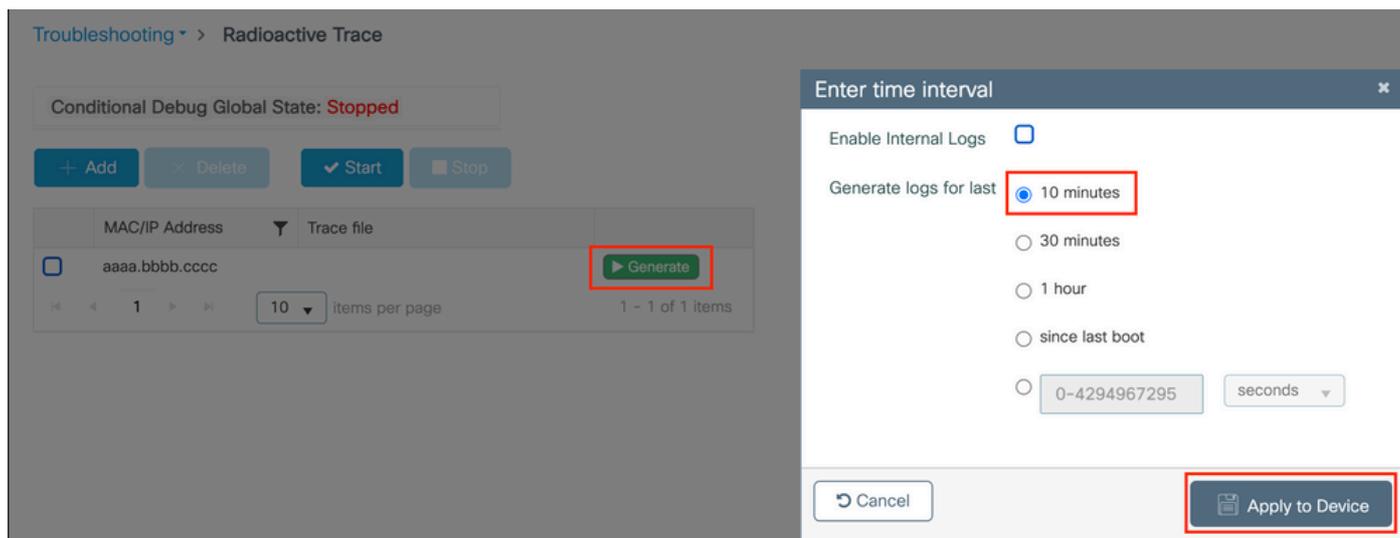
The screenshot displays the Cisco GUI interface for 'Radioactive Trace'. On the left, a navigation sidebar is visible with the 'Troubleshooting' menu item highlighted in red. The main content area shows the 'Radioactive Trace' configuration page. At the top, the 'Conditional Debug Global State' is set to 'Stopped'. Below this, there are four buttons: '+ Add' (highlighted in red), 'Delete', 'Start', and 'Stop'. A table below the buttons has two columns: 'MAC/IP Address' and 'Trace file'. The table is currently empty, showing '0' items and 'No items to display'. The page also includes a search bar and a 'Items per page' dropdown set to '10'.

Paso 2. Haga clic en Start (Inicio).

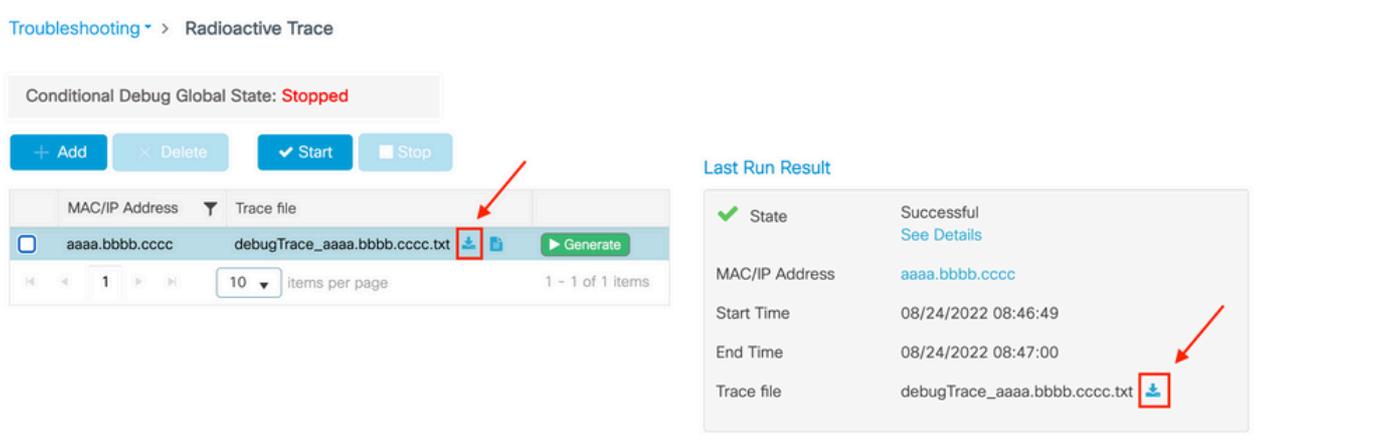
Paso 3. Reproduzca el problema.

Paso 4. Haga clic en **Stop**.

Paso 5. Haga clic en el **Generate** botón, seleccione el intervalo de tiempo para el que desea obtener los registros y haga clic en **Apply to Device**. In this example, the logs for the last 10 minutes are requested.



Paso 6. Descargue Radioactive Trace en su equipo y haga clic en el botón de descarga y consúltelo.



## Resolución de problemas en ISE

Si experimenta problemas con la autenticación del cliente, puede verificar los registros en el servidor ISE. Vaya a **Operations > RADIUS > Live Logs** y verá la lista de solicitudes de autenticación, así como el conjunto de directivas que coincidió, el resultado de cada solicitud, etc. Puede obtener más detalles si hace clic en la lupa situada debajo de la **Details** pestaña de cada línea, como se muestra en la imagen:

Live Logs

Live Sessions

Misconfigured Supplicants 0

Misconfigured Network Devices 0

RADIUS Drops 0

Client Stopped Responding 2

Repeat Counter 0

Refresh: Never | Show: Latest 20 records | Within: Last 3 hours

Refresh | Reset Repeat Counts | Export To

Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Netwo
Aug 23, 2022 06:18:42.5...	<span style="color: blue;">●</span>		0	user1	08:BE:AC:27:85:...	Unknown	Policy_Set...	Policy_Set...	PermitAcc...	10.14.16.112,...	
Aug 23, 2022 09:45:48.1...	<span style="color: red;">●</span>			user1	BC:D0:74:2B:6D:...						9800-W

## 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).