

Configuración de FlexConnect con autenticación en el WLC Catalyst 9800

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

Introducción

Este documento describe cómo configurar FlexConnect con autenticación central o local en el controlador de LAN inalámbrica de Catalyst 9800.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Modelo de configuración de Catalyst Wireless 9800
- FlexConnect
- 802.1x

Componentes Utilizados

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

- C9800-CL, Cisco IOS-XE® 17.3.4

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.

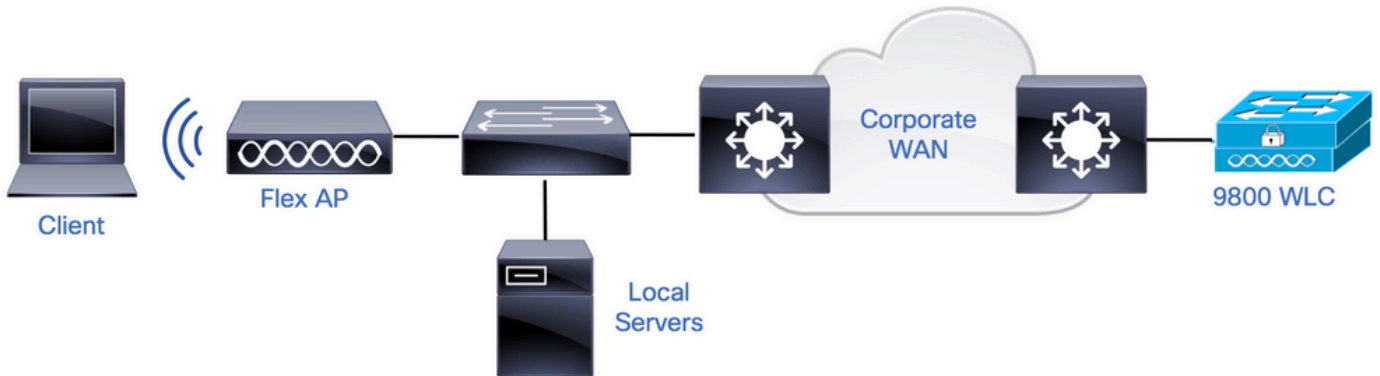
Antecedentes

FlexConnect es una solución inalámbrica para la implementación en oficinas remotas. Permite configurar puntos de acceso (AP) en ubicaciones remotas desde la oficina corporativa a través de un enlace de red de área extensa (WAN) sin necesidad de implementar un controlador en cada ubicación. Los AP FlexConnect pueden conmutar el tráfico de

datos del cliente localmente y realizar la autenticación del cliente localmente cuando se pierde la conexión con el controlador. En el modo conectado, los puntos de acceso de FlexConnect también pueden realizar la autenticación local.

Configurar

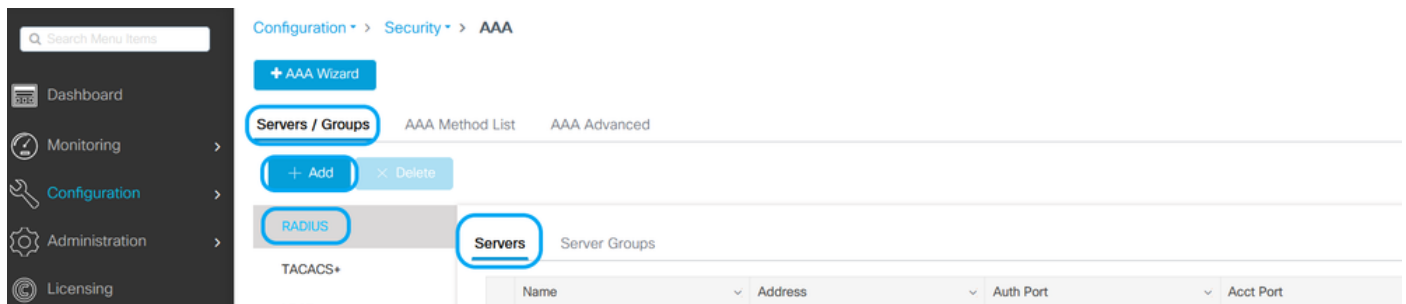
Diagrama de la red



Configuraciones

Configuración AAA en WLC 9800


Paso 1. Declarar servidor RADIUS. **Desde GUI:** Navegue hasta Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add e ingrese la información del servidor RADIUS.



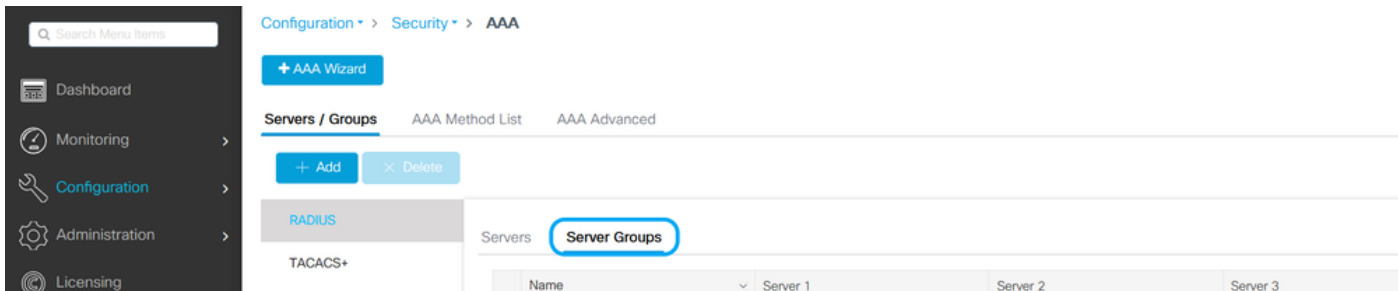
Asegúrese de que Support for CoA esté habilitado si planea utilizar cualquier tipo de seguridad que requiera CoA en el futuro.

Edit AAA Radius Server ✕

Name*	<input type="text" value="AmmlSE"/>
Server Address*	<input type="text" value="10.48.76.30"/>
PAC Key	<input type="checkbox"/>
Key Type	<input type="text" value="Hidden"/>
Key* ⓘ	<input type="password" value="●●●●●●●●●●●●●●●●"/>
Confirm Key*	<input type="password" value="●●●●●●●●●●●●●●●●"/>
Auth Port	<input type="text" value="1812"/>
Acct Port	<input type="text" value="1813"/>
Server Timeout (seconds)	<input type="text" value="5"/>
Retry Count	<input type="text" value="3"/>
Support for CoA	<input checked="" type="checkbox"/> ENABLED

 **Nota:** Radius CoA no se admite en la implementación de autenticación local de Flex Connect. .

Paso 2. Agregue el servidor RADIUS a un grupo RADIUS. **En GUI:** vaya a Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add.



Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add X Delete

RADIUS

TACACS+

Servers **Server Groups**

Name	Server 1	Server 2	Server 3
------	----------	----------	----------

Edit AAA Radius Server Group ✕

Name*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Source Interface VLAN ID

Available Servers

- >
- <
- >>
- <<

Assigned Servers

- ⬆
- ⬆
- ⬇
- ⬇

↶ Cancel

📄 Update & Apply to Device

Paso 3. Cree una lista de métodos de autenticación. **En GUI:** vaya a Configuration > Security > AAA > AAA Method List > Authentication > + Add

- 📊 Dashboard
- 🕒 Monitoring >
- 🔧 Configuration >
- ⚙️ Administration >

Configuration > Security > AAA

+ AAA Wizard

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

Authentication
Authorization

+ Add ✕ Delete

Name	Type
------	------

Quick Setup: AAA Authentication



Method List Name*

Type* ⓘ

Group Type ⓘ

Fallback to local

Available Server Groups

- radius
- ldap
- tacacs+

Assigned Server Groups

- AmmISE

Cancel

Desde 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 3
# key <shared-key>
# exit

# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>

# aaa authentication dot1x <dot1x-list-name> group <radius-grp-name>
```

Configuración de WLAN

Paso 1. **Desde GUI:** Navegue hasta Configuration > Wireless > WLANs **y haga clic en +Add** para crear una nueva WLAN, e ingrese la información de WLAN. A continuación, haga clic en Aplicar al dispositivo.

The screenshot displays the WLAN configuration interface. On the left is a dark sidebar with a search bar and menu items for 'Dashboard' and 'Monitoring'. The main content area shows the breadcrumb 'Configuration > Tags & Profiles > WLANs' and a toolbar with buttons for '+ Add', 'Delete', 'Enable WLAN', and 'Disable WLAN'. Below the toolbar, it indicates 'Number of WLANs selected : 0' and a table with columns for 'Status', 'Name', 'ID', and 'SSID'. The '+ Add' button is highlighted with a red circle.

Below this, the 'Add WLAN' dialog box is open, showing the 'General' tab. The fields are as follows:

Field	Value	Field	Value
Profile Name*	802.1x-WLAN	Radio Policy	All
SSID*	802.1x	Broadcast SSID	ENABLED
WLAN ID*	1		
Status	ENABLED		

At the bottom of the dialog, there are 'Cancel' and 'Apply to Device' buttons.

Paso 2. **Desde la GUI:** Vaya a la pestaña Security para configurar el modo de seguridad de capa 2/capa 3, siempre y cuando el método de cifrado y la lista de autenticación estén en uso. A continuación, haga clic en Update & Apply to Device.

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

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 AAA

Layer 2 Security Mode

MAC Filtering

Protected Management Frame

PMF

WPA Parameters

WPA Policy

WPA2 Policy

GTK Randomize

OSEN Policy

WPA2 Encryption AES(CCMP128)
 CCMP256
 GCMP128
 GCMP256

Auth Key Mgmt 802.1x
 PSK
 CCKM
 FT + 802.1x
 FT + PSK

Lobby Admin Access

Fast Transition

Over the DS

Reassociation Timeout

MPSK Configuration

MPSK

Cancel

Update & Apply to Device

Configuración del perfil de la política

Paso 1. **En GUI:** vaya a Configuration > Tags & Profiles > Policy y haga clic en +Add para crear un perfil de política.



Search Menu Items



Dashboard

Configuration > Tags & Profiles > Policy

+ Add

× Delete

Status



Policy Profile Name

Paso 2. Agregue el nombre y desmarque la casilla Central Switching. Con esta configuración, el controlador gestiona la autenticación del cliente y el punto de acceso FlexConnect conmuta los paquetes de datos del cliente localmente.

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

General


Access Policies

QOS and AVC

Mobility

Advanced

Name* Description Status **ENABLED** Passive Client DISABLEDEncrypted Traffic Analytics DISABLED**CTS Policy**Inline Tagging SGACL Enforcement Default SGT **WLAN Switching Policy**Central Switching DISABLEDCentral Authentication **ENABLED** Central DHCP **ENABLED** Central Association DISABLEDFlex NAT/PAT DISABLED

 Nota: La asociación y el switching deben estar siempre emparejados, si el switching central está inhabilitado, la asociación central también debe inhabilitarse en todos los perfiles de políticas cuando se utilizan AP Flexconnect.

Paso 3. **Desde GUI:** Vaya a la pestaña Access Policies **para asignar la VLAN a la que se pueden asignar los clientes inalámbricos cuando se conectan a esta WLAN de forma predeterminada.** Puede seleccionar un nombre de VLAN en el menú desplegable o, como práctica recomendada, escribir manualmente

un ID de VLAN.

Edit Policy Profile ✕

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

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

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification **Disabled** ⓘ

Local Subscriber Policy Name

VLAN

VLAN/VLAN Group

Multicast VLAN

WLAN ACL

IPv4 ACL

IPv6 ACL

URL Filters

Pre Auth

Post Auth

Paso 4. **Desde la GUI:** vaya a la pestaña Advanced para configurar los tiempos de espera de WLAN, DHCP, la política WLAN Flex y la política AAA en caso de que estén en uso. A continuación, haga clic en Update & Apply to Device.

Edit Policy Profile
✕

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

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

WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

DHCP

IPv4 DHCP Required

DHCP Server IP Address

Show more >>>

AAA Policy

Allow AAA Override

NAC State

Policy Name

Accounting List ⓘ

Fabric Profile

mDNS Service Policy [Clear](#)

Hotspot Server

User Defined (Private) Network

Status

Drop Unicast

Umbrella

Umbrella Parameter Map [Clear](#)

Flex DHCP Option for DNS **ENABLED**

DNS Traffic Redirect **IGNORE**

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Air Time Fairness Policies

2.4 GHz Policy

5 GHz Policy

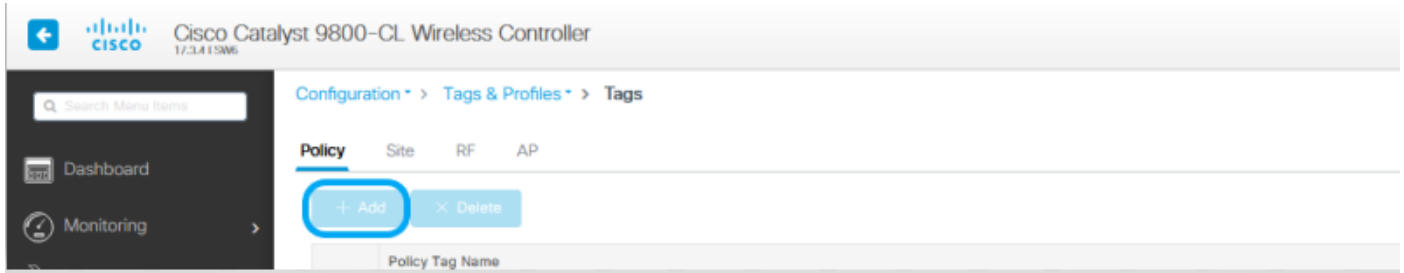
EoGRE Tunnel Profiles

↶ Cancel

📄 Update & Apply to Device

Configuración de etiquetas de políticas

Paso 1. **En GUI:** vaya a Configuration > Tags & Profiles > Tags > Policy > +Add.



Paso 2. Asigne un nombre y asigne el perfil de política y el perfil WLAN antes de crear.

Edit Policy Tag



⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name*

Description

WLAN-POLICY Maps: 1

+ Add

× Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> 802.1x-WLAN	VLANX

10 items per page 1 - 1 of 1 items

Map WLAN and Policy

WLAN Profile*

Policy Profile*

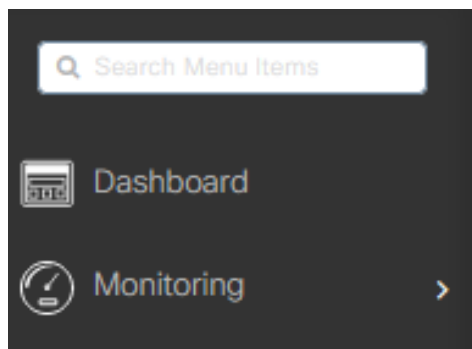


RLAN-POLICY Maps: 0

Cancel

Update & Apply to Device

Paso 1. **Desde GUI:** Navegue hasta Configuration > Tags & Profiles > Flex y haga clic en +Add para crear uno nuevo.



Configuration > Tags & Profiles > Flex





	Flex Profile Name
<input type="checkbox"/>	Sal_Flex

Edit Flex Profile ✕

General Local Authentication Policy ACL VLAN Umbrella

Name*	<input type="text" value="Flex-Pro"/>	Fallback Radio Shut	<input type="checkbox"/>
Description	<input type="text" value="Enter Description"/>	Flex Resilient	<input type="checkbox"/>
Native VLAN ID	<input type="text" value="71"/>	ARP Caching	<input checked="" type="checkbox"/>
HTTP Proxy Port	<input type="text" value="0"/>	Efficient Image Upgrade	<input checked="" type="checkbox"/>
HTTP-Proxy IP Address	<input type="text" value="0.0.0.0"/>	OfficeExtend AP	<input type="checkbox"/>
CTS Policy		Join Minimum Latency	<input type="checkbox"/>
Inline Tagging	<input type="checkbox"/>	IP Overlap	<input type="checkbox"/>
SGACL Enforcement	<input type="checkbox"/>	mDNS Flex Profile	<input type="text" value="Search or Select"/>
CTS Profile Name	<input type="text" value="default-sxp-profile"/>		

 Nota: El ID de VLAN nativa hace referencia a la VLAN utilizada por los AP que pueden asignar este Flex Profile y debe ser el mismo ID de VLAN configurado como nativo en el

 puerto del switch donde se conectan los AP.

Paso 2. En la pestaña VLAN, agregue las VLAN necesarias, las asignadas de forma predeterminada a la WLAN a través de un perfil de política o las que envía un servidor RADIUS. A continuación, haga clic en Update & Apply to Device.

Edit Flex Profile ✕

General Local Authentication Policy ACL **VLAN** Umbrella

+ Add ✕ Delete

VLAN Name	ID	ACL Name
No items to display		

10 items per page


VLAN Name*


VLAN Id*

ACL Name

✓ Save ↻ Cancel

↻ Cancel 📄 Update & Apply to Device

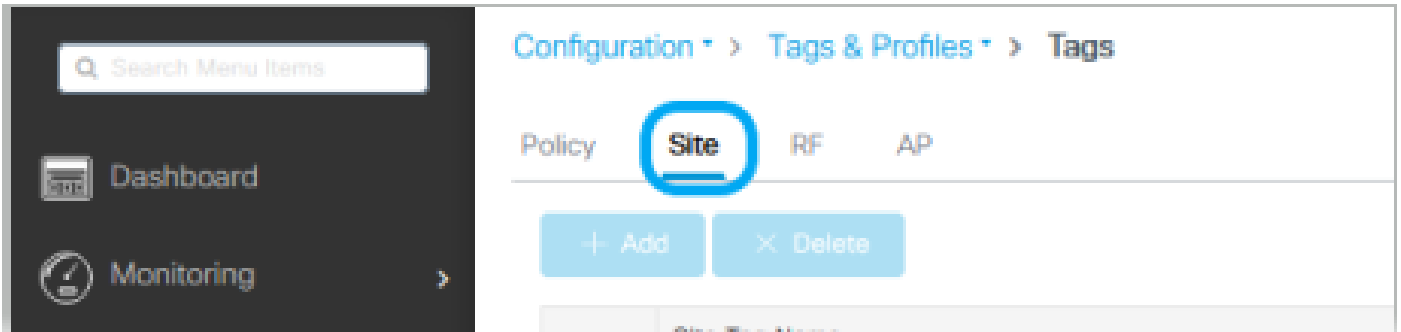
 Nota: Para Policy Profile, cuando selecciona la VLAN predeterminada asignada al SSID. Si utiliza un nombre de VLAN en ese paso, asegúrese de que utiliza el mismo nombre de VLAN en la configuración de Flex Profile; de lo contrario, los clientes no podrán conectarse a la WLAN.

 Nota: Para configurar una ACL para flexConnect con anulación de AAA, solo configúrela en la "política ACL"; si la ACL está asignada a una VLAN específica, agregue la ACL al agregar

 la VLAN y, a continuación, agregue la ACL en la "política ACL".

Configuración de etiqueta de sitio

Paso 1. **En GUI:** vaya a Configuration > Tags & Profiles > Tags > Site **y haga clic en** +Add para crear una nueva etiqueta Site. Desmarque la casilla Enable Local Site para permitir que los APs conmuten el tráfico de datos del cliente localmente, y agregue el Flex Profile creado anteriormente.




Edit Site Tag

Name*	<input type="text" value="Flex_Site"/>
Description	<input type="text" value="Flex_Site"/>
AP Join Profile	<input type="text" value="default-ap-profile"/>
Flex Profile	<input type="text" value="Flex-Pro"/>
Fabric Control Plane Name	<input type="text"/>
Enable Local Site	<input type="checkbox"/>

Cancel

Update & Apply to Device

 Nota: al deshabilitar la opción Habilitar sitio local, los AP a los que se asigna esta etiqueta de sitio se pueden configurar como modo FlexConnect.

Paso 2. **Desde GUI:** Navegue hasta Configuration > Wireless > Access Points > AP name para agregar la etiqueta Site Tag **y la etiqueta Policy a un AP asociado**. Esto puede hacer que el AP reinicie su túnel CAPWAP y vuelva a unirse al WLC 9800.

Search Menu Items




Dashboard



Monitoring



[Configuration](#) > [Wireless](#) > **Access Points**

 **All Access Points**

Number of AP(s): 1

General

AP Name*	<input type="text" value="talomar1"/>
Location*	<input type="text" value="default location"/>
Base Radio MAC	b4de.31d7.b920
Ethernet MAC	005d.7319.bb2a
Admin Status	ENABLED <input checked="" type="checkbox"/>
AP Mode	<input style="border: 2px solid blue; border-radius: 10px;" type="text" value="Local"/>
Operation Status	Registered
Fabric Status	Disabled
LED State	ENABLED <input checked="" type="checkbox"/>
LED Brightness Level	<input type="text" value="8"/>

Version

Primary Software Version	17.3.4.154
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	1.1.2.4
IOS Version	17.3.4.154
Mini IOS Version	0.0.0.0

Tags

⚠ Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.

Policy	<input type="text" value="Policy"/>
Site	<input style="border: 2px solid blue; border-radius: 10px;" type="text" value="Flex_Site"/>
RF	<input type="text" value="default-rf-tag"/>
Write Tag Config to AP	<input type="checkbox"/>

IP Config

CAPWAP Preferred Mode	IPv4
DHCP IPv4 Address	10.48.70.77
Static IP (IPv4/IPv6)	<input type="checkbox"/>

Time Statistics

Up Time	0 days 0 hrs 3 mins 28 secs
Controller Association Latency	2 mins 40 secs

Una vez que el AP se une nuevamente, observe que el AP está ahora en el modo FlexConnect.

All Access Points

Number of AP(s): 1

AP Name	AP Model	Slots	Admin Status	IP Address	Base Radio MAC	AP Mode	Operation Status	Configuration Status	Policy Tag	Site Tag	RF Tag	Tag Source	Location	Country
talaman1	AR-AP2802I-E-K9	2		10.48.70.77	b4de.31d7.8920	Flex	Registered	Healthy	Policy	Flex_Site	default-rt-tag	Static	default location	ES

Autenticación local con servidor RADIUS externo

Paso 1. Agregue el AP como un dispositivo de red en el servidor RADIUS. Para ver un ejemplo, consulte [Cómo utilizar Identity Service Engine \(ISE\) como servidor RADIUS](#)

Paso 2. Cree una WLAN.

La configuración puede ser la misma que la configurada anteriormente.

Add WLAN

General Security Advanced

Profile Name*	Local auth	Radio Policy	All
SSID*	Local auth	Broadcast SSID	ENABLED
WLAN ID*	9		
Status	ENABLED		

Cancel Apply to Device

Paso 3. Configuración del perfil de la política.

Puede crear uno nuevo o utilizar el configurado anteriormente. Esta vez, desmarque las casillas Central Switching, Central Authentication, Central DHCP y Central Association Enable.

Add Policy Profile



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

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

Local

Description

Enter Description

Status

ENABLED

Passive Client

DISABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

2-65519

WLAN Switching Policy

Central Switching

DISABLED

Central Authentication

DISABLED

Central DHCP

DISABLED

Central Association

DISABLED

Flex NAT/PAT

DISABLED

Cancel

Apply to Device

Paso 4. Configuración de etiquetas de políticas.

Asocie la WLAN configurada y el perfil de política creado.

Paso 5. Configuración de Flex Profile.

Cree un Flex Profile, navegue hasta la ficha Local Authentication, configure el Radius Server Group y marque la casilla RADIUS.

Radius Server Group	<input type="text" value="AmmlSE"/>	LEAP	<input type="checkbox"/>
Local Accounting Radius Server Group	<input type="text" value="Select Accounting S"/>	PEAP	<input type="checkbox"/>
Local Client Roaming	<input type="checkbox"/>	TLS	<input type="checkbox"/>
EAP Fast Profile	<input type="text" value="Select Profile"/>	RADIUS	<input checked="" type="checkbox"/>

Users

Select CSV File

Username	
No items to display	

Paso 6. Configuración de la etiqueta del sitio.
Configure el Flex Profile configurado en el paso 5 y desmarque la casilla Enable Local Site.

Add Site Tag ✕

Name*	<input type="text" value="Local Auth"/>
Description	<input type="text" value="Enter Description"/>
AP Join Profile	<input type="text" value="default-ap-profile"/> ▼
Flex Profile	<input type="text" value="Local"/> ▼
Fabric Control Plane Name	<input type="text"/> ▼
Enable Local Site	<input type="checkbox"/>

Verificación

En GUI: vaya a Monitoring > Wireless > Clients y confirme el estado del administrador de políticas y los parámetros de FlexConnect.

Autenticación central:

General

QOS Statistics

ATF Statistics

Mobility History

Call Statistics

Client Properties

AP Properties

Security Information

Client Statistics

QOS Properties

MAC Address	484b.aa52.5937
IPv4 Address	172.16.76.41
User Name	address1
Policy Profile	VLAN2669
Flex Profile	RemoteSite1
Wireless LAN Id	1
Wireless LAN Name	eWLC_do1x
BSSID	38ed.18c6.902f
Uptime(sec)	9 seconds
CCX version	No CCX support
Power Save mode	OFF
Supported Rates	9.0,18.0,36.0,48.0,54.0
Policy Manager State	Run
Last Policy Manager State	IP Learn Complete
Encrypted Traffic Analytics	No
Multicast VLAN	0
Access VLAN	2669
Anchor VLAN	0
Server IP	10.88.173.94
DNS Snooped IPv4 Addresses	None
DNS Snooped IPv6 Addresses	None
11v DNS Capable	No
FlexConnect Data Switching	Local
FlexConnect DHCP Status	Local
FlexConnect Authentication	Central
FlexConnect Central Association	Yes

Autenticación local:

General	QOS Statistics	ATF Statistics	Mobility History	Call Statistics
Client Properties	AP Properties	Security Information	Client Statistics	QOS Properties
MAC Address		484b.aa52.5937		
IPv4 Address		172.16.76.41		
IPv6 Address		fe80::80c6e782:7c78:68f9		
User Name		address1		
Policy Profile		VLAN2669		
Flex Profile		RemoteSite1		
Wireless LAN Id		1		
Wireless LAN Name		eWLC_do1x		
BSSID		38ed.18c6.932f		
Uptime(sec)		11 seconds		
CCX version		No CCX support		
Power Save mode		OFF		
Policy Manager State		Run		
Last Policy Manager State		IP Learn Complete		
Encrypted Traffic Analytics		No		
Multicast VLAN		0		
Access VLAN		2669		
Anchor VLAN		0		
DNS Snooped IPv4 Addresses		None		
DNS Snooped IPv6 Addresses		None		
11v DMS Capable		No		
FlexConnect Data Switching		Local		
FlexConnect DHCP Status		Local		
FlexConnect Authentication		Local		
FlexConnect Central Association		No		


Puede utilizar estos comandos para verificar la configuración actual:

Desde CLI:

```
# show wlan { summary | id | name | all }
# 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 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.

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

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

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

Desde CLI:

```
# show clock
```

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

Desde CLI:

```
# show logging
```

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

Desde CLI:


```
# show debugging
IOSXE Conditional Debug Configs:
```

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

```
IOSXE Packet Tracing Configs:
```

```
Packet Infra debugs:
```

```
Ip Address _____|_____ Port
```

 Nota: Si encuentra 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 depura activamente.

Paso 4. Si asume 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.

Desde CLI:

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

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

Desde CLI:

```
# 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 de radio activo

Si los seguimientos siempre activos no proporcionan suficiente información para determinar el desencadenador del problema que se está investigando, puede habilitar la depuración condicional y capturar el seguimiento de Radio Activo (RA), que puede proporcionar 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.

Desde CLI:

```
# 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 2 085 978 494 segundos.

Desde CLI:

```
# 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 el resultado de la actividad del cliente en la 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 se agote el tiempo de monitoreo predeterminado o configurado.

Desde CLI:

```
# 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 de seguimiento activo por radio .log en un servidor externo o mostrar el resultado directamente en la pantalla.

Verifique el nombre del archivo de seguimiento activo por radio

Desde CLI:

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

Copie el archivo en un servidor externo:

Desde CLI:

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

Muestre el contenido:


Desde CLI:

```
# 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 ha realizado un examen detallado de los registros de depuración que ya se han recopilado y almacenado internamente.

Desde CLI:

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

 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:

Desde CLI:

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

Muestre el contenido:


Desde CLI:

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

Paso 11. Elimine las condiciones de depuración.

Desde CLI:

```
# clear platform condition all
```

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

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).