

# Configuración de Central Web Authentication (CWA) en Catalyst 9800 WLC e ISE

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración de AAA en WLC 9800](#)

[Configuración de WLAN](#)

[Configuración del perfil de la política](#)

[Configuración de etiquetas de políticas](#)

[Asignación de etiquetas de políticas](#)

[Configuración de ACL de redireccionamiento](#)

[Habilitar redirección para HTTP o HTTPS](#)

[Configuración de ISE](#)

[Adición del WLC 9800 a ISE](#)

[Creación de un usuario nuevo en ISE](#)

[Creación del perfil de autorización](#)

[Configuración de la regla de autenticación](#)

[Configuración de las reglas de autorización](#)

[SOLO puntos de acceso de switching local de FlexConnect](#)

[Certificados](#)

[Verificación](#)

[Troubleshoot](#)

[Lista de Verificación](#)

[Soporte de Puerto de Servicio para RADIUS](#)

[Recopilar depuraciones](#)

[Examples](#)

---

## Introducción

Este documento describe cómo configurar una LAN inalámbrica CWA en un WLC Catalyst 9800 e ISE.

## Prerequisites

### Requirements

Cisco recomienda conocer la configuración de los controladores LAN inalámbricos (WLC) 9800.

## Componentes Utilizados

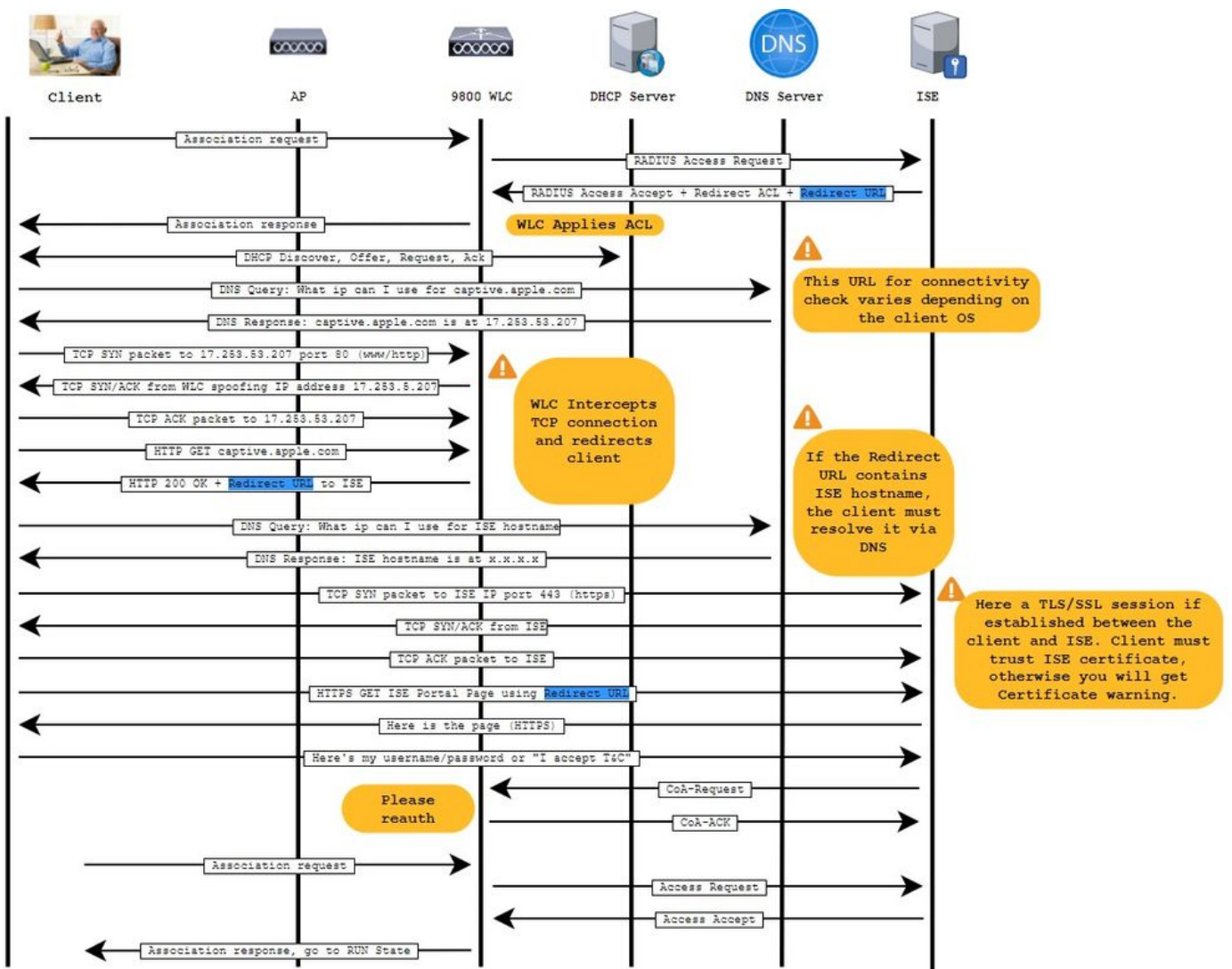
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- 9800 WLC Cisco IOS® XE Gibraltar v17.6.x
- Identity Service Engine (ISE) v3.0

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.

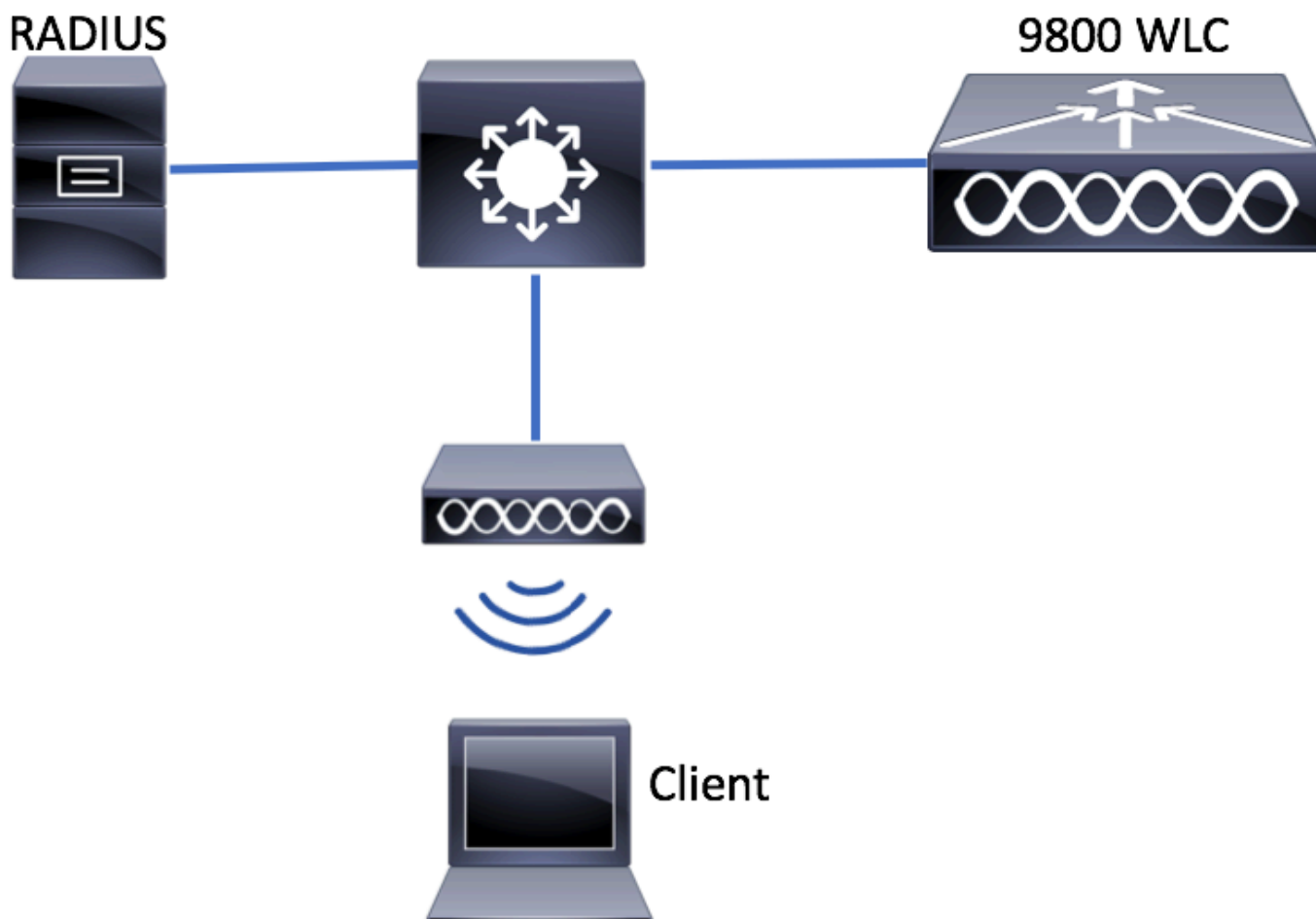
## Antecedentes

El proceso CWA se muestra aquí, donde puede ver el proceso CWA de un dispositivo Apple como ejemplo:



# Configurar

## Diagrama de la red



## Configuración de AAA en WLC 9800

Paso 1. Agregue el servidor ISE a la configuración del WLC 9800.

Navegue hasta `Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add` e ingrese la información del servidor RADIUS como se muestra en las imágenes.

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups    AAA Method List    AAA Advanced

+ Add    × Delete

RADIUS

TACACS+

LDAP

Servers    Server Groups

Name	Address
0 items per page	

Asegúrese de que el soporte para CoA esté habilitado si planea utilizar la autenticación web central (o cualquier tipo de seguridad que requiera CoA) en el futuro.

### Create AAA Radius Server

Name\*    ISE-server

Server Address\*    [Redacted]

PAC Key   

Key Type    Clear Text

Key\*    [Redacted]

Confirm Key\*    [Redacted]

Auth Port    1812

Acct Port    1813

Server Timeout (seconds)    1-1000

Retry Count    0-100

Support for CoA     ENABLED

CoA Server Key Type    Clear Text

CoA Server Key    [Redacted]

Confirm CoA Server Key    [Redacted]

Automate Tester   

Cancel    Apply to Device

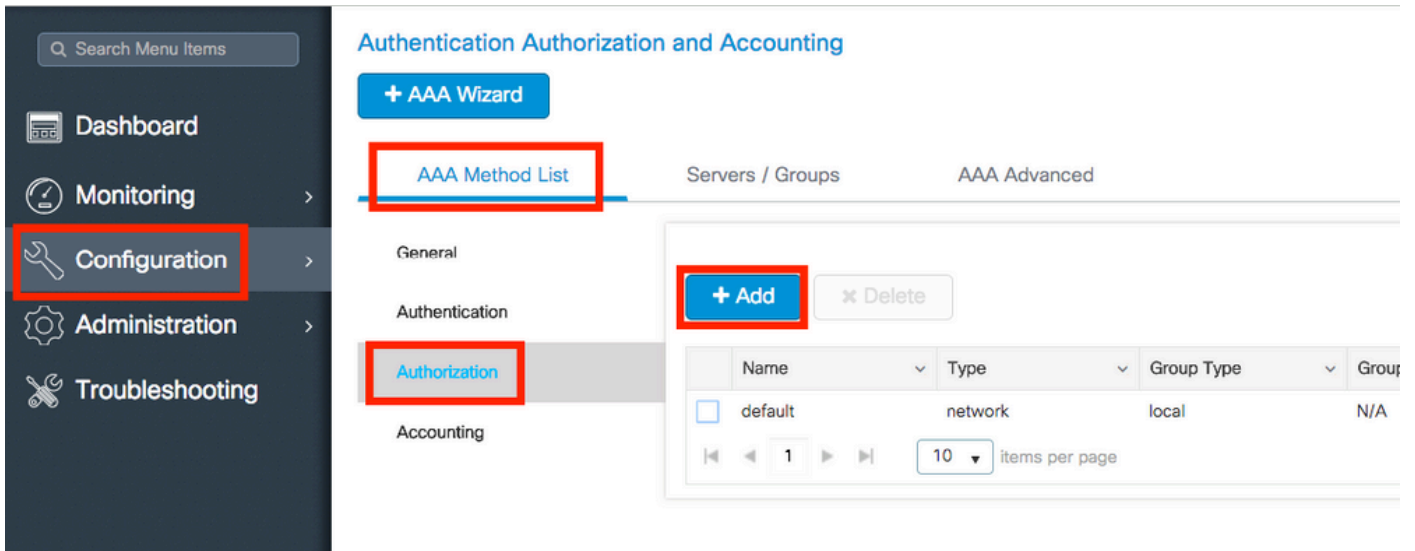


**Nota:** En la versión 17.4.X y posteriores, asegúrese de configurar también la clave del servidor CoA cuando configure el servidor RADIUS. Utilice la misma clave que el secreto compartido (son las mismas de forma predeterminada en ISE). El propósito es configurar opcionalmente una clave diferente para CoA que el secreto compartido si es lo que su servidor RADIUS configuró. En Cisco IOS XE 17.3, la interfaz de usuario web simplemente utilizaba el mismo secreto compartido que la clave CoA.

---

Paso 2. Cree una lista de métodos de autorización.

Desplácese hasta Configuration > Security > AAA > AAA Method List > Authorization > + Add como se muestra en la imagen.



## Quick Setup: AAA Authorization

Method List Name\*

Type\*

Group Type

Fallback to local

Authenticated

### Available Server Groups

ldap  
tacacs+

>  
<  
>>  
<<

### Assigned Server Groups

radius

⏪  
⏩  
⏴  
⏵

Paso 3. (Opcional) Cree una lista de métodos de contabilidad como se muestra en la imagen.

Dashboard  
Monitoring  
**Configuration**  
Administration  
Troubleshooting

+ AAA Wizard

AAA Method List

Servers / Groups

General  
Authentication  
Authorization  
**Accounting**

+ Add

Name

0

### Quick Setup: AAA Accounting

Method List Name\*

Type\*

Available Server Groups

ldap	>	radius	<
tacacs+	<		>
	>>		<<
	<<		>>

Assigned Server Groups

**Nota:** CWA no funciona si decide equilibrar la carga (desde la configuración CLI de Cisco IOS XE) de sus servidores RADIUS debido al ID de error de funcionamiento de Cisco [CSCvh03827](https://www.cisco.com/cisco/web/bugtools/bugsearch.html?bugid=CSCvh03827). 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.

Paso 4. (Opcional) Puede definir la política AAA para enviar el nombre SSID como un atributo Called-station-id, lo que puede ser útil si desea aprovechar esta condición en ISE más adelante en el proceso.

Desplácese hasta Configuration > Security > Wireless AAA Policy y edite la política AAA predeterminada o cree una nueva.

- ☰ Dashboard
- 🕒 Monitoring >
- 🔧 **Configuration** >
- ⚙️ Administration >
- 🔧 Troubleshooting

Configuration > Security > **Wireless AAA Policy**

+ Add
× Delete

Policy Name
<input type="checkbox"/> default-aaa-policy

⏪
⏩
1
⏪
⏩
10
▼ items per page

Puede elegir SSID como opción 1. Tenga en cuenta que incluso cuando elige solo SSID, el ID de la estación llamada sigue agregando la dirección MAC del AP al nombre SSID.

## Edit Wireless AAA Policy

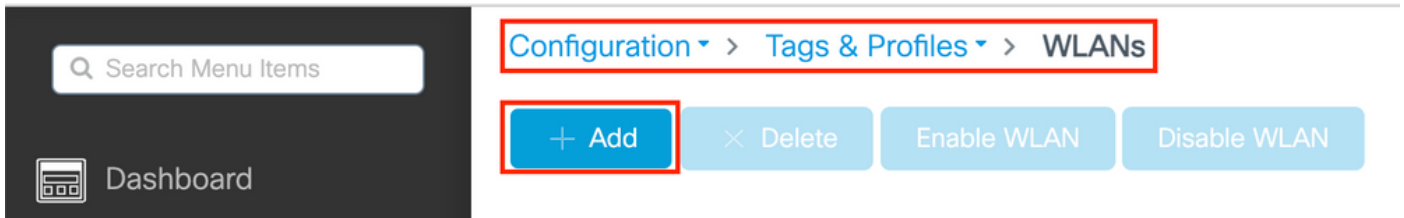
Policy Name*	<input style="width: 90%; border: 1px solid #ccc; background-color: #f2f2f2;" type="text" value="default-aaa-policy"/>
Option 1	<input style="background-color: #e0f2f7;" type="text" value="SSID"/>
Option 2	<input style="background-color: #e0f2f7;" type="text" value="Not Configured"/>
Option 3	<input style="background-color: #e0f2f7;" type="text" value="Not Configured"/>

### Configuración de WLAN

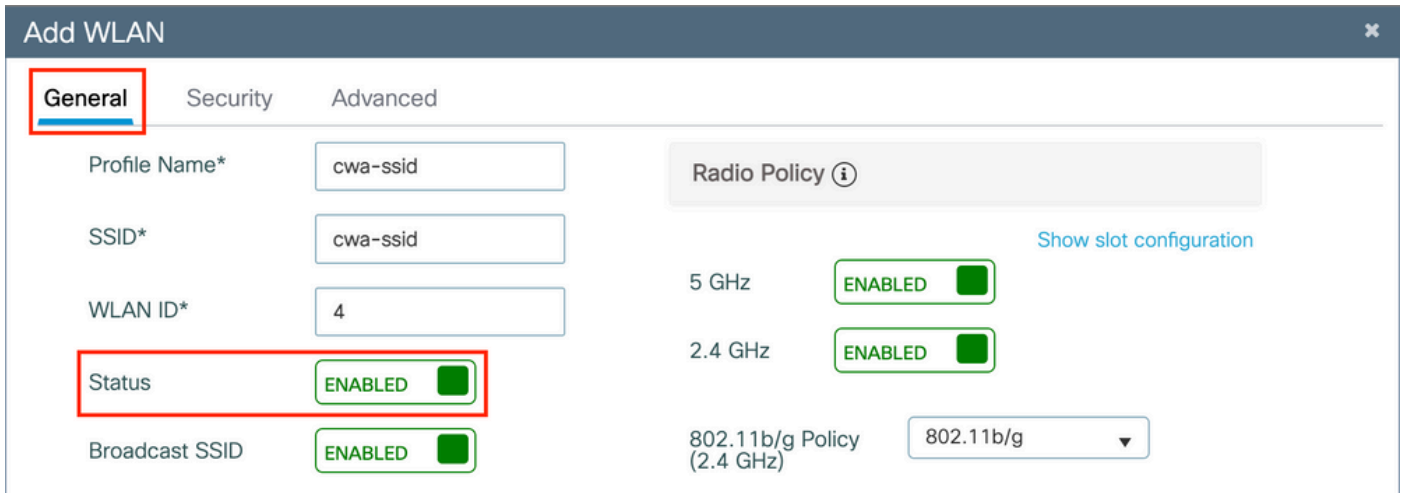
Paso 1. Cree la WLAN.

Desplácese hasta Configuration > Tags & Profiles > WLANs > + Add la red y configúrela según sea necesario.

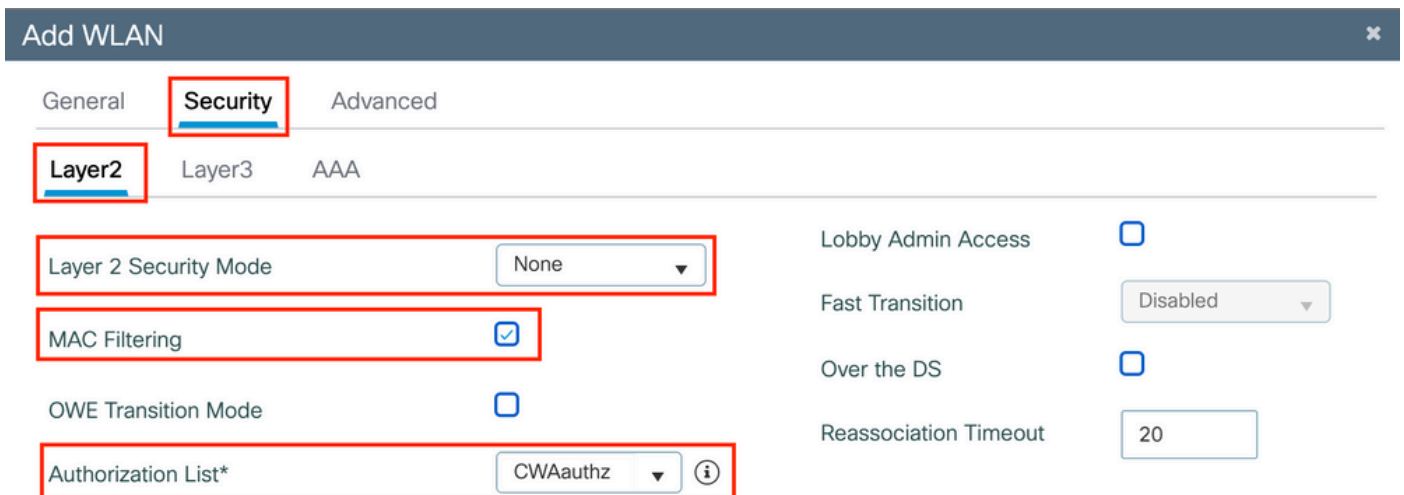




Paso 2. Introduzca la información general de WLAN.



Paso 3. Vaya a la Security ficha y seleccione el método de seguridad necesario. En este caso, solo se necesitan el 'Filtrado MAC' y la lista de autorización AAA (que creó en el paso 2 de la AAA Configuration sección).



CLI:

```
#config t
(config)#wlan cwa-ssid 4 cwa-ssid
(config-wlan)#mac-filtering CWAauthz
(config-wlan)#no security ft adaptive
(config-wlan)#no security wpa
(config-wlan)#no security wpa wpa2
```

```
(config-wlan)#no security wpa wpa2 ciphers aes
(config-wlan)#no security wpa akm dot1x
(config-wlan)#no shutdown
```

## Configuración del perfil de la política

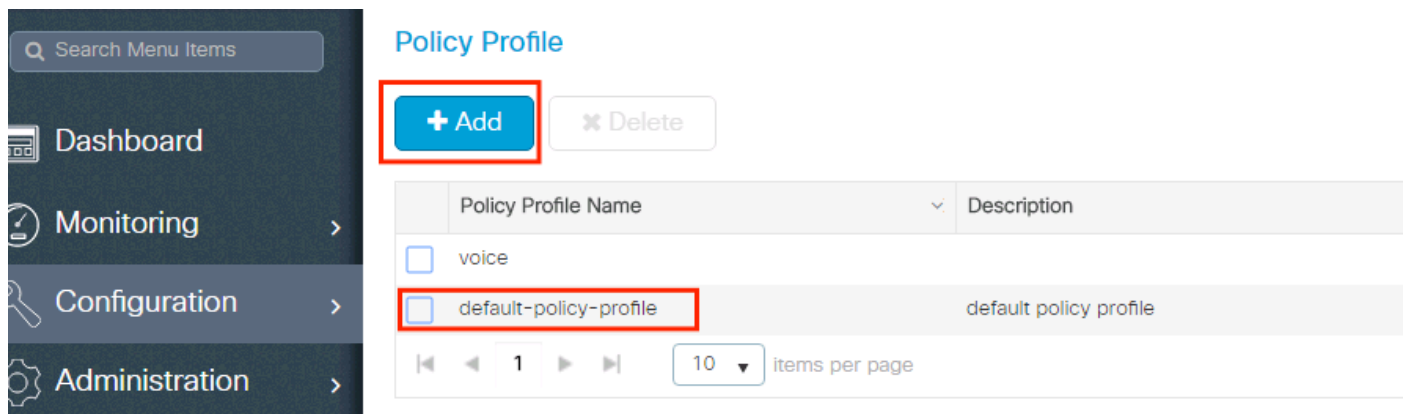
Dentro de un perfil de política, puede decidir asignar los clientes a los que se aplicará la VLAN, entre otras configuraciones (como la lista de controles de acceso (ACL), la calidad de servicio (QoS), el ancla de movilidad, los temporizadores, etc.).

Puede utilizar su perfil de política predeterminado o puede crear uno nuevo.

GUI:

Paso 1. Crear un nuevo Policy Profile.

Desplácese hasta Configuration > Tags & Profiles > Policy y configure el default-policy-profile o cree uno nuevo.



The screenshot displays the 'Policy Profile' configuration page. On the left is a dark sidebar with a search bar and menu items: Dashboard, Monitoring, Configuration, and Administration. The main area has a title 'Policy Profile' and two buttons: '+ Add' (highlighted with a red box) and 'x Delete'. Below these is a table with two columns: 'Policy Profile Name' and 'Description'. The table contains two rows: 'voice' and 'default-policy-profile' (highlighted with a red box). At the bottom of the table is a pagination control showing '1' items per page and a dropdown menu set to '10 items per page'.

Asegúrese de que el perfil esté habilitado.

## Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

### General

Access Policies

QOS and AVC

Mobility

Advanced

Name\*

Description

Status  ENABLED

Passive Client  DISABLED

Encrypted Traffic Analytics  DISABLED

#### CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

#### WLAN Switching Policy

Central Switching  ENABLED

Central Authentication  ENABLED

Central DHCP  ENABLED

Flex NAT/PAT  DISABLED

Paso 2. Elija la VLAN.

Navegue hasta la Access Policies pestaña y elija el nombre de la VLAN en la lista desplegable o escriba manualmente el VLAN-ID. No configure una ACL en el perfil de política.

## Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy 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

Search or Select ▼

VLAN

VLAN/VLAN Group

VLAN1416 ▼

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 ▼

Paso 3. Configure el perfil de política para aceptar anulaciones de ISE (Permitir anulación AAA) y cambios de autorización (CoA) (Estado NAC). Opcionalmente, también puede especificar un método de contabilidad.

## Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

**Advanced**

### WLAN Timeout

Session Timeout (sec)	<input type="text" value="1800"/>
Idle Timeout (sec)	<input type="text" value="300"/>
Idle Threshold (bytes)	<input type="text" value="0"/>
Client Exclusion Timeout (sec)	<input checked="" type="checkbox"/> <input type="text" value="60"/>
Guest LAN Session Timeout	<input type="checkbox"/>

### DHCP

IPv4 DHCP Required	<input type="checkbox"/>
DHCP Server IP Address	<input type="text"/>

[Show more >>>](#)

### AAA Policy

Allow AAA Override	<input checked="" type="checkbox"/>
NAC State	<input checked="" type="checkbox"/>
NAC Type	<input type="text" value="RADIUS"/>
Policy Name	<input type="text" value="default-aaa-policy"/>
Accounting List	<input type="text" value="CWAacct"/> ⓘ ✕

### WGB Parameters

Broadcast Tagging	<input type="checkbox"/>
WGB VLAN	<input type="checkbox"/>

### Policy Proxy Settings

ARP Proxy	<input type="checkbox"/> DISABLED
IPv6 Proxy	<input type="text" value="None"/>

Fabric Profile

Link-Local Bridging

mDNS Service Policy  [Clear](#)

Hotspot Server

### User Defined (Private) Network

Status

Drop Unicast

### DNS Layer Security

DNS Layer Security Parameter Map  [Clear](#)

Flex DHCP Option for DNS  ENABLED

Flex 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


Tunnel Profile

CLI:

```
# config # wireless profile policy <policy-profile-name> # aaa-override
# nac
# vlan <vlan-id_or_vlan-name>
# accounting-list <acct-list>
# no shutdown
```

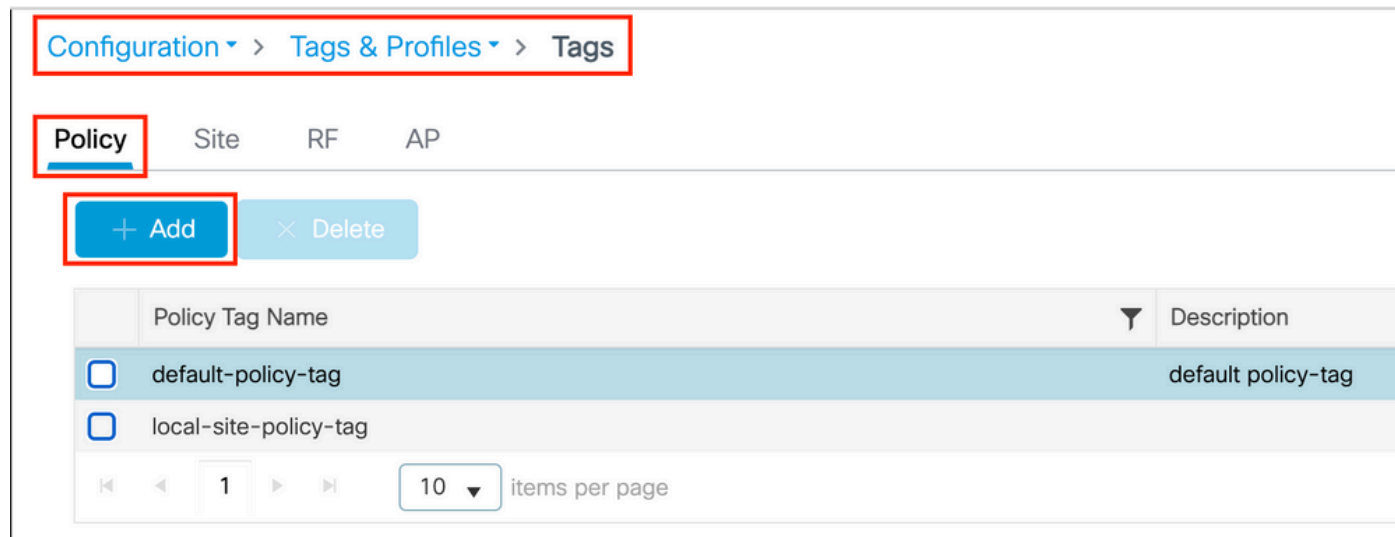
## Configuración de etiquetas de políticas

Dentro de la etiqueta de política se encuentra el enlace del SSID con el perfil de política. Puede crear una nueva etiqueta de política o utilizar la etiqueta de política predeterminada.

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

GUI:

Desplácese hasta Configuration > Tags & Profiles > Tags > Policy y agregue uno nuevo si es necesario, como se muestra en la imagen.



Configuration > Tags & Profiles > Tags

Policy Site RF AP

+ Add × Delete

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

1 10 items per page

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

**Add Policy Tag** ✕

Name\*

Description

---

**WLAN-POLICY Maps: 1**

+ Add ✕ Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> cwa-ssid	default-policy-profile

⏪ ⏩ 1 ▶ ⏪ 10 items per page 1 - 1 of 1 items

---

**RLAN-POLICY Maps: 0**

↶ Cancel
📄 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, realice la asignación necesaria y luego haga clic en Update & Apply to Device.

### Edit AP

- General**
- Interfaces
- High Availability
- Inventory
- ICap
- Advanced
- Support Bundle

General	Tags
AP Name*	<p>⚠ Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.</p>
Location*	
Base Radio MAC	Policy <input type="text" value="cwa-policy-tag"/>
Ethernet MAC	Site <input type="text" value="default-site-tag"/>
Admin Status <input checked="" type="checkbox"/> ENABLED	RF <input type="text" value="default-rf-tag"/>
AP Mode <input type="text" value="Local"/>	Write Tag Config to AP <input type="checkbox"/> ⓘ
Operation Status Registered	

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

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



Start

## Tags & Profiles



WLAN Profile



Policy Profile



Policy Tag



AP Join Profile



Flex Profile



Site Tag



RF Profile



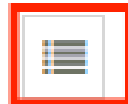
RF Tag



## Apply



Tag APs



Done

Start Now →

Configuration > Wireless Setup > Advanced

Show Me How

+ Tag APs

Number of APs: 2  
Selected Number of APs: 2

<input checked="" type="checkbox"/>	AP Name	AP Model	AP MAC	Serial Number	AP Mode	Admin Status	Operation Status	Policy Tag	Site Tag	RF Tag
<input checked="" type="checkbox"/>	[blurred]	AIR-AP1815I-E-K9	[blurred]	[blurred]	Flex	Disabled	Registered	local-site-policy-tag	flex-site-tag	defa rf-ta
<input checked="" type="checkbox"/>	[blurred]	AIR-AP1815I-E-K9	[blurred]	[blurred]	Local	Enabled	Registered	default-policy-tag	default-site-tag	defa rf-ta

10 items per page 1 - 2 of 2 items

Elija la etiqueta wished y haga clic Save & Apply to Device como se muestra en la imagen.

## Tag APs

Tags

Policy

Site

RF

*Changing AP Tag(s) will cause associated AP(s) to rejoin and disrupt connected client(s)*

CLI:

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

## Configuración de ACL de redireccionamiento

Paso 1. Navegue hasta Configuration > Security > ACL > + Add para crear una nueva ACL.

Elija un nombre para la ACL y haga que IPv4 Extended escriba y agregue cada regla como una secuencia, como se muestra en la imagen.

**Add ACL Setup**
✕

ACL Name\*

ACL Type

**Rules**

Sequence\*

Action

Source Type

Destination Type

Host Name\*  ! This field is mandatory

Protocol

DSCP

Log

+ Add

✕ Delete

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
No items to display										

↶ Cancel

📄 Apply to Device

Debe denegar el tráfico a los nodos de PSN de ISE, así como también debe denegar el DNS y permitir el resto. Esta ACL de redirección no es una ACL de seguridad, sino una ACL de punt que define qué tráfico va a la CPU (en permisos) para un tratamiento adicional (como la redirección) y qué tráfico permanece en el plano de datos (en negación) y evita la redirección.

La ACL debe tener el siguiente aspecto (reemplace 10.48.39.28 con su dirección IP de ISE en este ejemplo):


Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
<input type="checkbox"/> 10	deny	any		10.48.39.28		ip			None	Disabled
<input type="checkbox"/> 20	deny	10.48.39.28		any		ip			None	Disabled
<input type="checkbox"/> 30	deny	any		any		udp		eq domain	None	Disabled
<input type="checkbox"/> 40	deny	any		any		udp	eq domain		None	Disabled
<input type="checkbox"/> 50	permit	any		any		tcp		eq www	None	Disabled

**Nota:** Para la ACL de redirección, piense en la deny acción como una redirección de denegación (no tráfico de denegación) y la permit acción como redirección de permiso. El WLC mira solamente en el tráfico que puede redirigir (los puertos 80 y 443 por defecto).

CLI:

```
ip access-list extended REDIRECT
deny ip any host <ISE-IP>
deny ip host<ISE-IP> any
deny udp any any eq domain
deny udp any eq domain any
permit tcp any any eq 80
```

---

 **Nota:** Si finaliza la ACL con un permit ip any any en lugar de un permiso centrado en el puerto 80, el WLC también redirige HTTPS, que a menudo no es deseable ya que tiene que proporcionar su propio certificado y siempre crea una violación de certificado. Esta es la excepción a la declaración anterior que dice que no necesita un certificado en el WLC en caso de CWA: necesita uno si tiene la interceptación HTTPS habilitada pero nunca se considera válido de todos modos.

---

Puede mejorar la ACL mediante una acción para denegar solo el puerto de invitado 8443 al servidor ISE.

#### Habilitar redirección para HTTP o HTTPS

La configuración del portal de administración web está ligada a la configuración del portal de autenticación web y necesita escuchar en el puerto 80 para redirigir. Por lo tanto, HTTP debe estar habilitado para que la redirección funcione correctamente. Puede optar por habilitarlo globalmente (con el uso del comando ip http server) o puede habilitar HTTP sólo para el módulo de autenticación web (con el uso del comando webauth-http-enable bajo el mapa de parámetro).



**Nota:** La redirección del tráfico HTTP ocurre dentro de CAPWAP, incluso en el caso de FlexConnect Local Switching. Dado que es el WLC que hace el trabajo de la interceptación, el AP envía los paquetes HTTP(S) dentro del túnel CAPWAP y recibe la redirección del WLC de nuevo en CAPWAP

---

Si desea ser redirigido cuando intenta acceder a una URL HTTPS, agregue el comando `intercept-https-enable` bajo el mapa de parámetro pero observe que esta no es una configuración óptima, que tiene un impacto en la CPU del WLC y genera errores de certificado de todos modos:

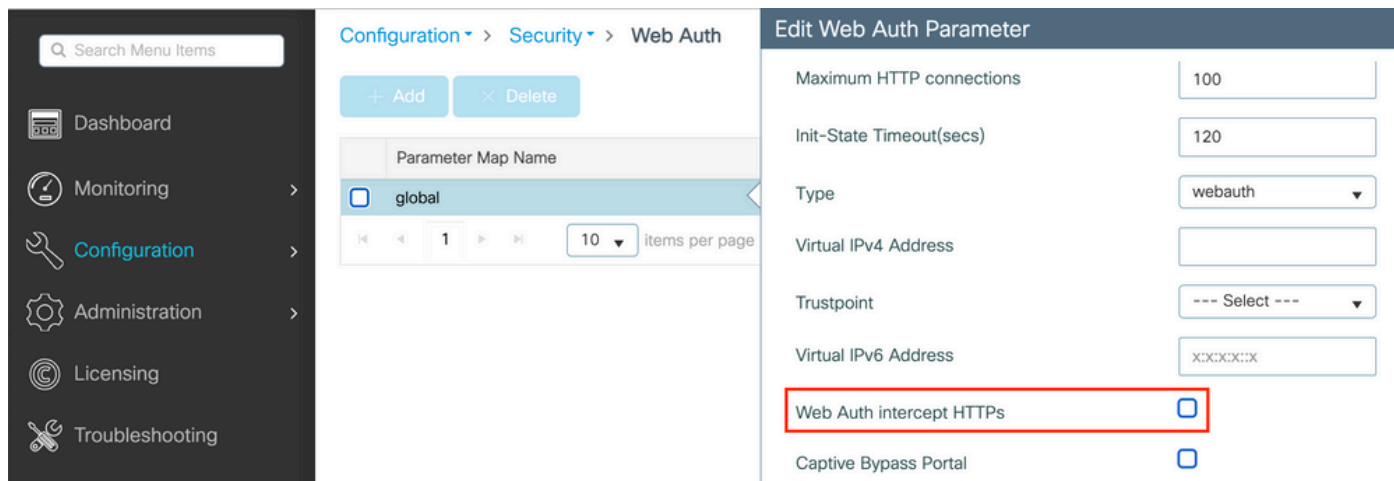
`<#root>`

```
parameter-map type webauth global
type webauth
```

`intercept-https-enable`

`trustpoint xxxxx`

También puede hacerlo a través de la GUI con la opción 'Web Auth intercept HTTPS' marcada en el mapa de parámetros (Configuration > Security > Web Auth).





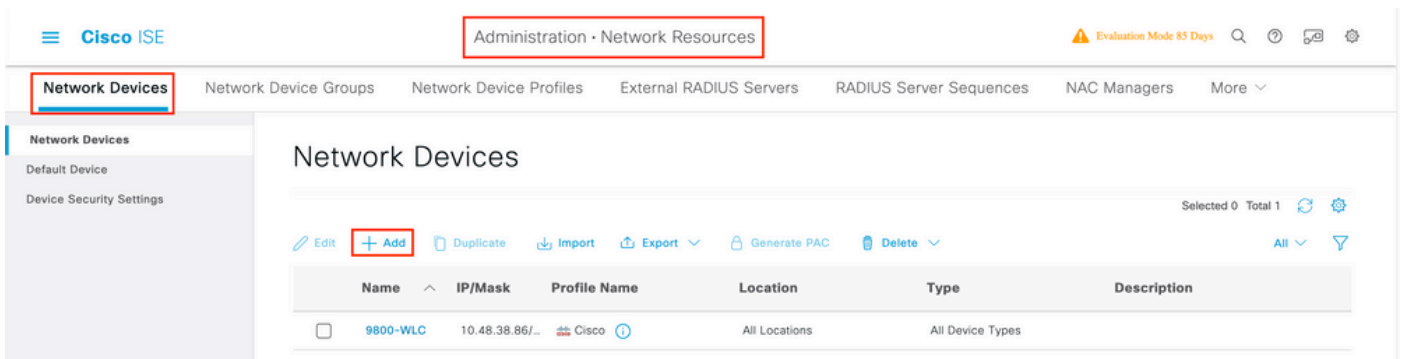
**Nota:** De forma predeterminada, los navegadores utilizan un sitio web HTTP para iniciar el proceso de redirección. Si se necesita redirección HTTPS, debe comprobarse HTTPS de intercepción de autenticación Web; sin embargo, esta configuración no se recomienda ya que aumenta el uso de la CPU.

---

## Configuración de ISE

### Adición del WLC 9800 a ISE

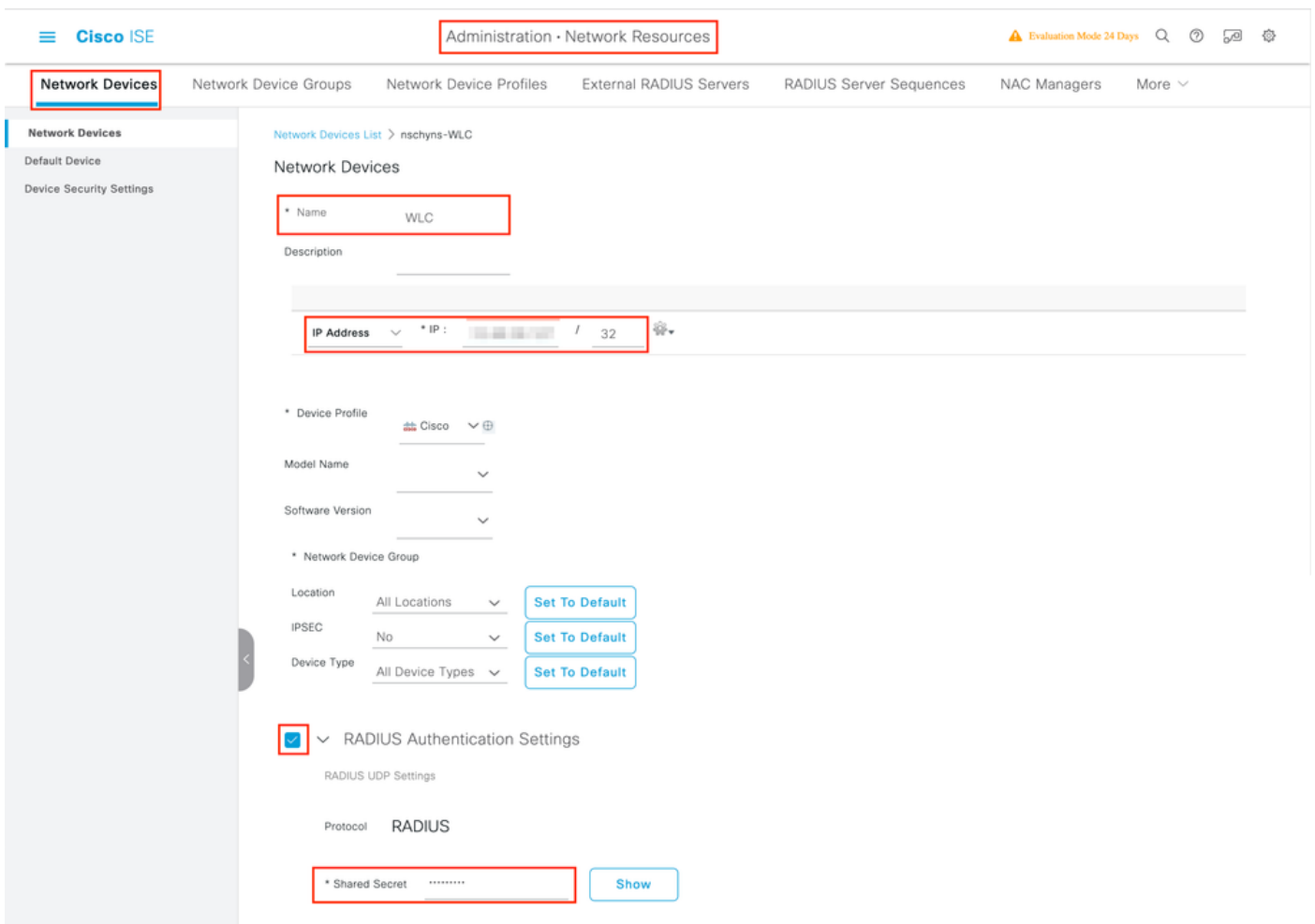
Paso 1. Abra la consola de ISE y desplácese hasta `Administration > Network Resources > Network Devices > Add` la imagen que se muestra.



Paso 2. Configure el dispositivo de red.

Opcionalmente, puede ser un nombre de modelo, versión de software y descripción especificados, y asignar grupos de dispositivos de red basados en tipos de dispositivos, ubicación o WLC.

La dirección IP aquí corresponde a la interfaz WLC que envía las solicitudes de autenticación. De forma predeterminada, es la interfaz de administración tal como se muestra en la imagen:



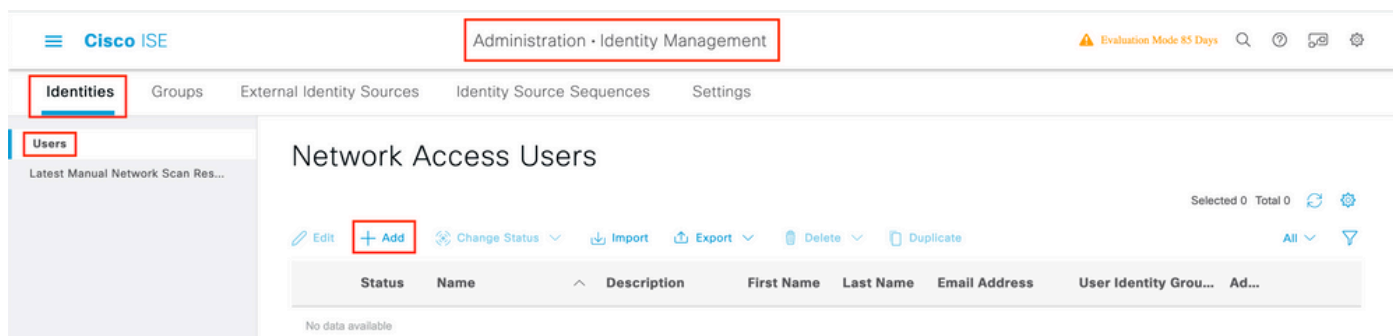
Para obtener más información sobre los grupos de dispositivos de red, consulte el capítulo sobre la guía de administración de ISE:

Administración de dispositivos de red: [ISE - Grupos de dispositivos de red](#).

Creación de un usuario nuevo en ISE

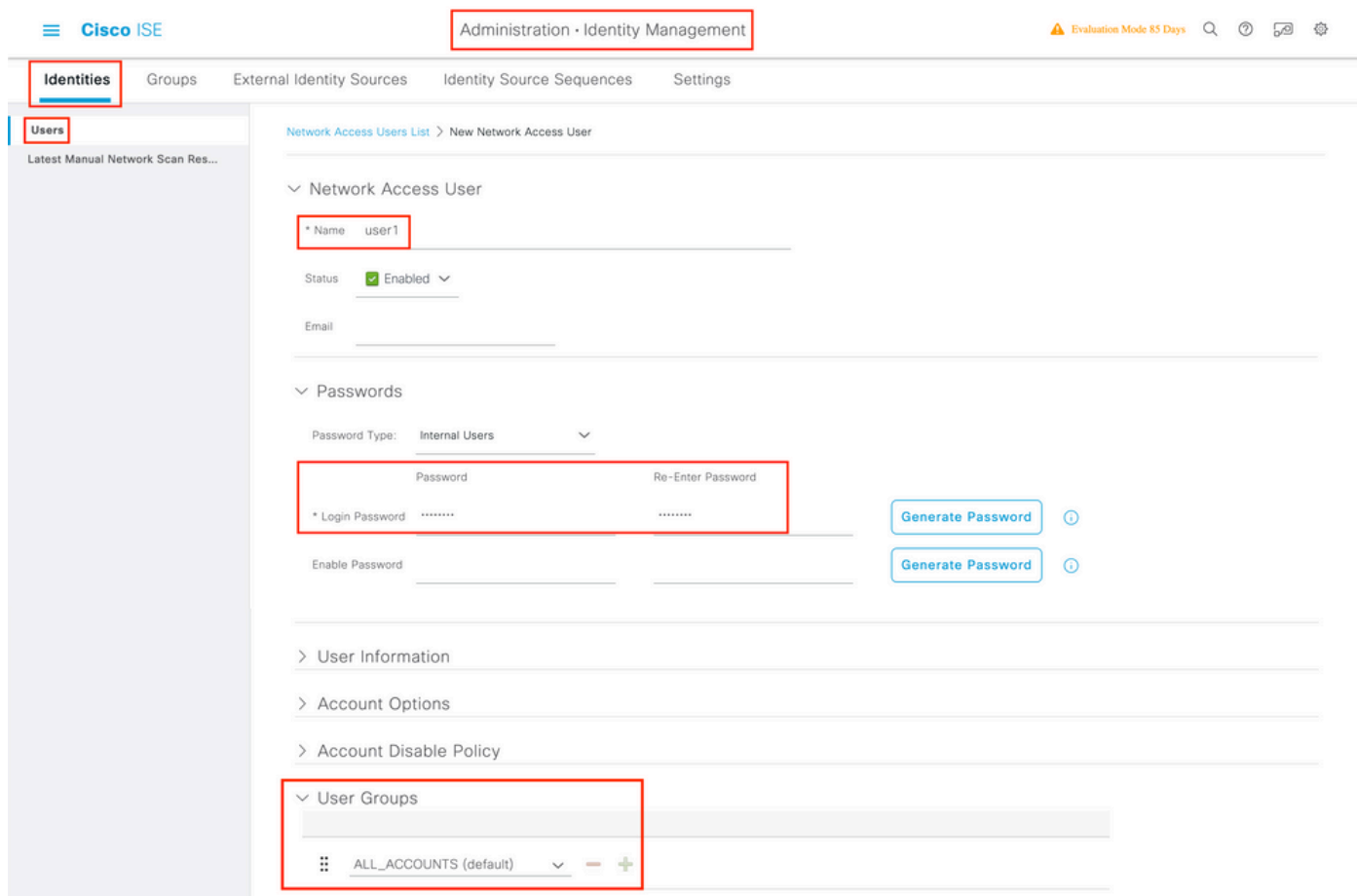


Paso 1. Desplácese hasta Administration > Identity Management > Identities > Users > Add como se muestra en la imagen.



Paso 2. Introduzca la información.

En este ejemplo, este usuario pertenece a un grupo llamado ALL\_ACCOUNTS pero se puede ajustar según sea necesario, como se muestra en la imagen.



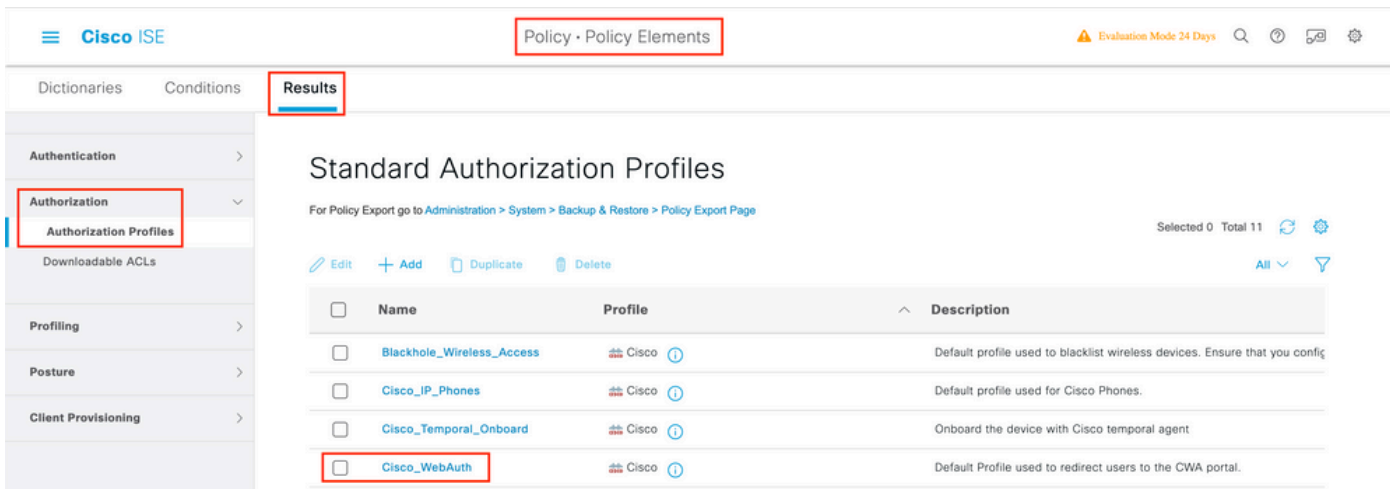
### Creación del perfil de autorización

El perfil de política es el resultado asignado a un cliente en función de sus parámetros (como dirección MAC, credenciales, WLAN utilizada, etc.). Puede asignar configuraciones específicas, como redes de área local virtuales (VLAN), listas de control de acceso (ACL), redirecciones de localizador uniforme de recursos (URL), etc.

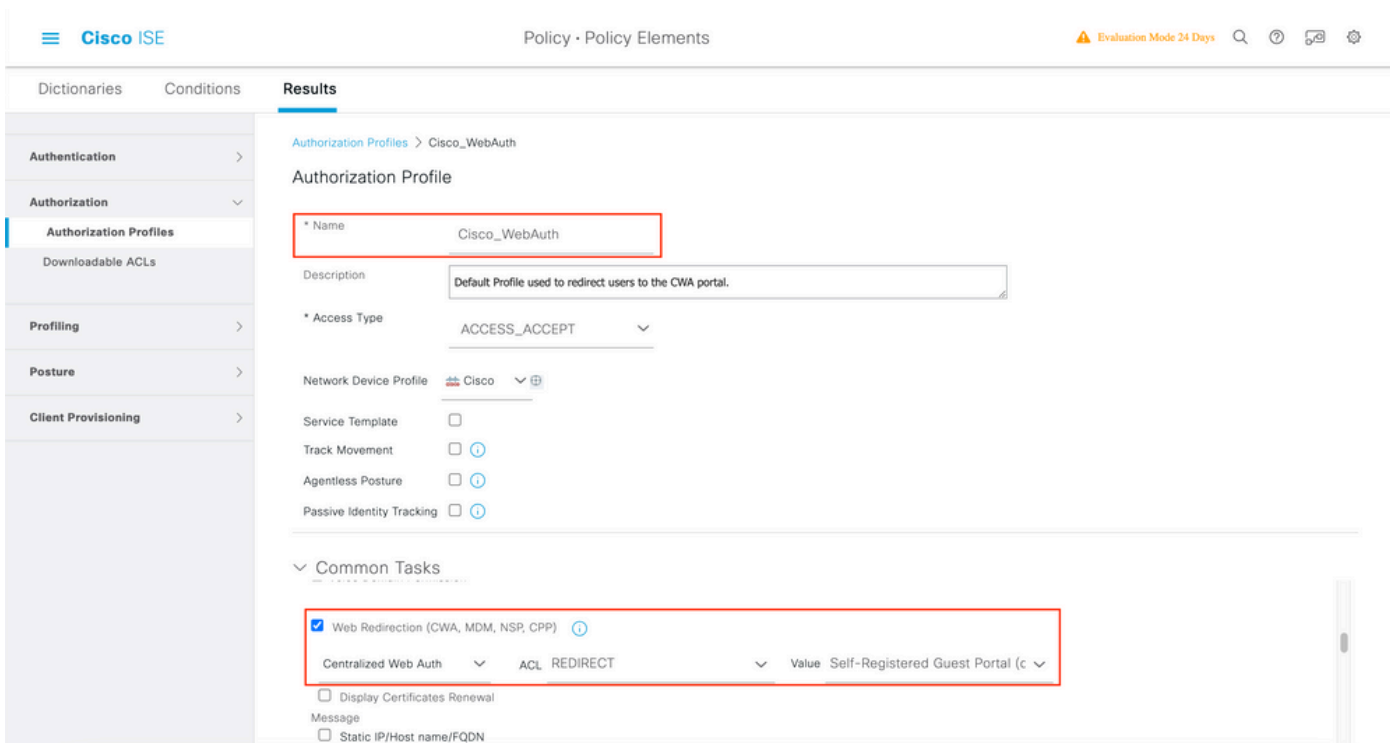
Tenga en cuenta que en versiones recientes de ISE ya existe un resultado de autorización Cisco\_Webauth. Aquí puede editarlo para modificar el

nombre de la ACL de redireccionamiento para que coincida con lo que configuró en el WLC.

Paso 1. Desplácese hasta Policy > Policy Elements > Results > Authorization > Authorization Profiles. Haga clic add para crear su propio o editar el Cisco\_Webauth resultado predeterminado.

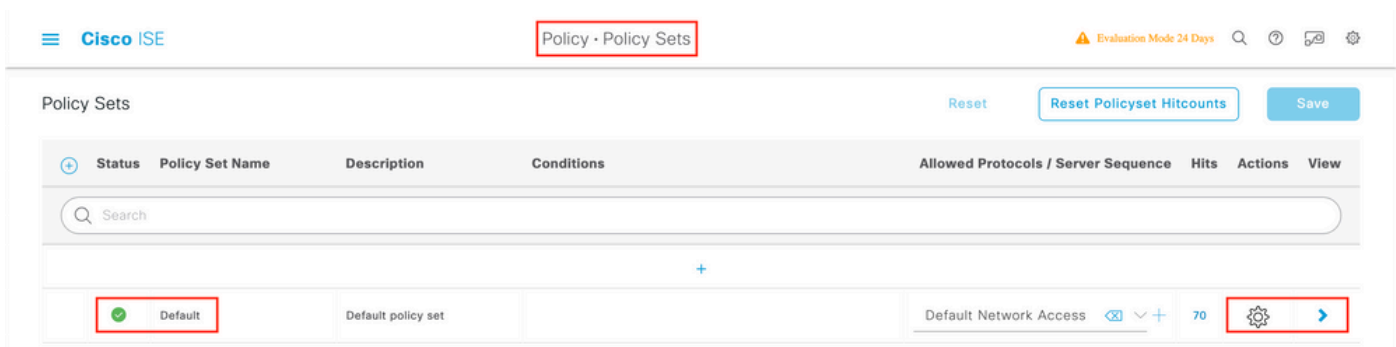


Paso 2. Introduzca la información de redireccionamiento. Asegúrese de que el nombre de ACL sea el mismo que fue configurado en el WLC 9800.

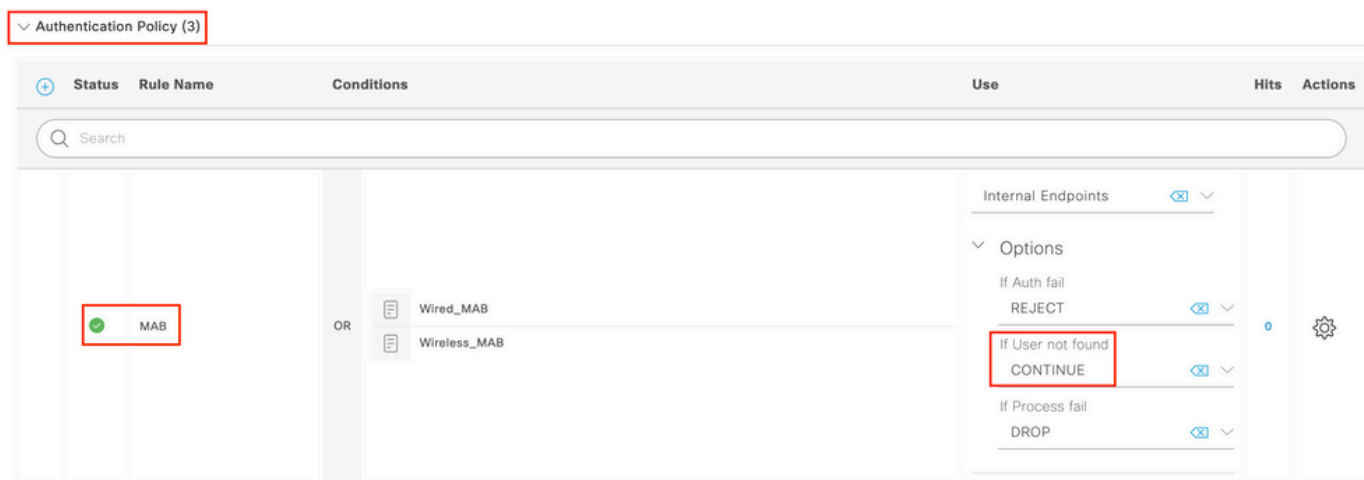


### Configuración de la regla de autenticación

Paso 1. Un conjunto de directivas define una colección de reglas de autenticación y autorización. Para crear uno, desplácese hasta Policy > Policy Sets, haga clic en el engranaje del primer conjunto de directivas de la lista y Insert new row elija o haga clic en la flecha azul de la derecha para elegir el conjunto de directivas predeterminado.



Paso 2. Expanda Authentication la directiva. Para la MAB regla (coincidencia en el MAB por cable o inalámbrico), expanda Options y elija la CONTINUE opción en caso de que vea "If User not found" (Si no se encuentra el usuario).

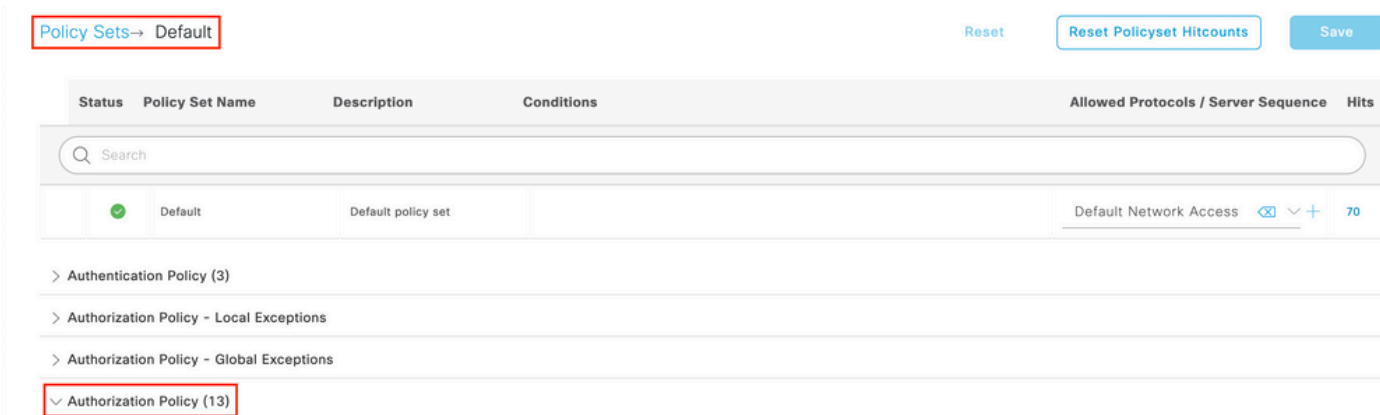


Paso 3. Haga clic Save para guardar los cambios.

### Configuración de las reglas de autorización

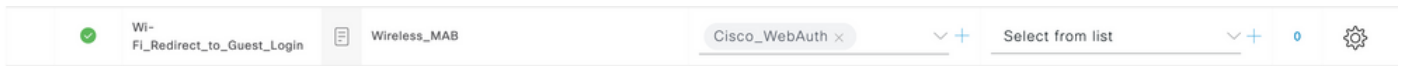
La regla de autorización es la encargada de determinar qué resultado de permiso (perfil de autorización) se aplica al cliente.

Paso 1. En la misma página Conjunto de directivas, cierre el Authentication Policy y expanda Authorziation Policy como se muestra en la imagen.

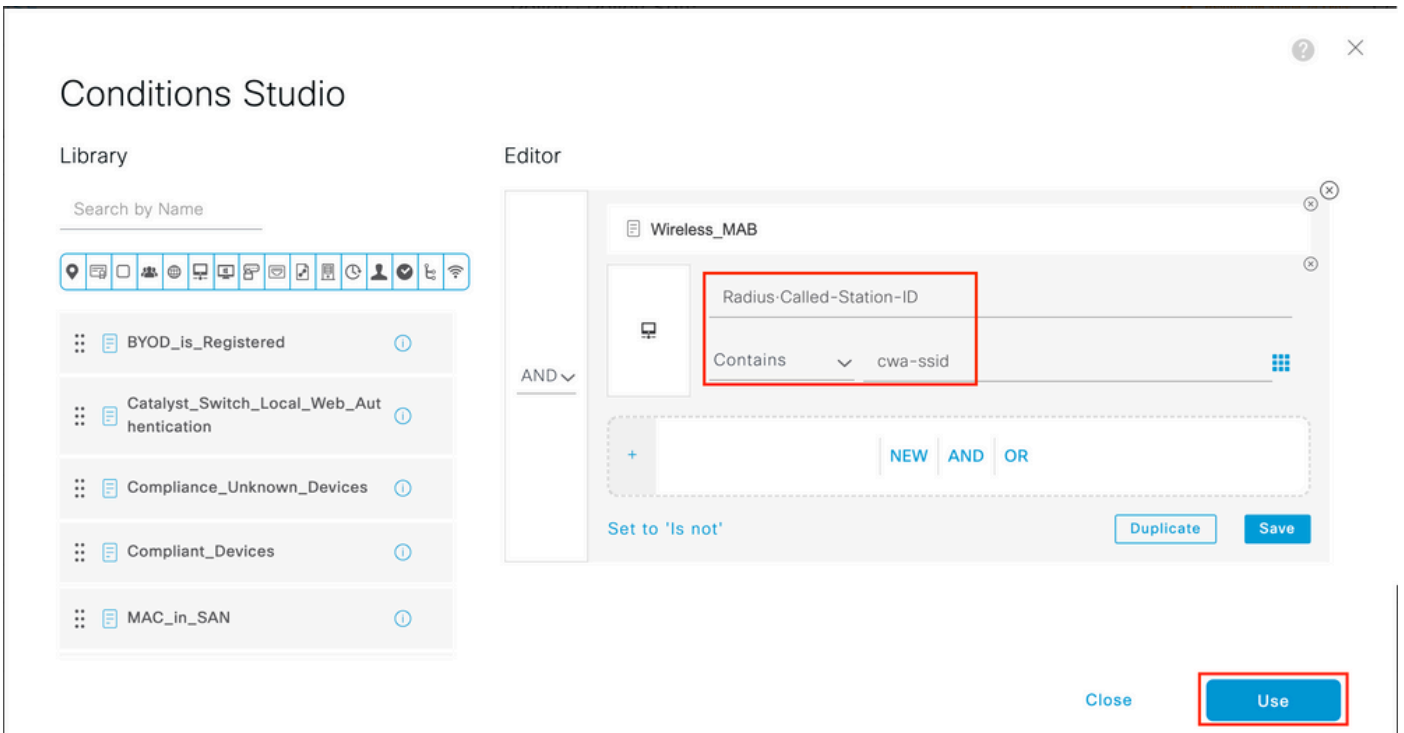


Paso 2. Las versiones recientes de ISE comienzan con una regla creada previamente llamada Wifi\_Redirect\_to\_Guest\_Login que se adapta

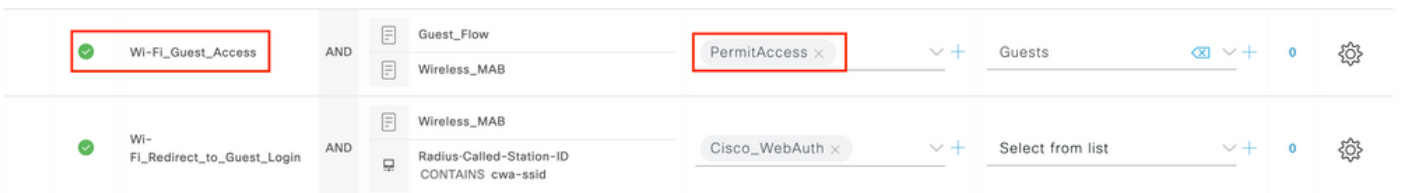
principalmente a nuestras necesidades. Gire el signo gris de la izquierda a enable.



Paso 3. Esa regla coincide solo con Wireless\_MAB y devuelve los atributos de redireccionamiento de la CWA. Ahora, puede agregar opcionalmente un pequeño giro y hacer que coincida solo con el SSID específico. Elija la condición (Wireless\_MAB a partir de ahora) para que aparezcan las condiciones de Studio. Agregue una condición a la derecha y elija el Radius diccionario con el Called-Station-ID atributo. Haga que coincida con su nombre de SSID. Realice la validación con el Use en la parte inferior de la pantalla, como se muestra en la imagen.



Paso 4. Ahora necesita una segunda regla, definida con una prioridad más alta, que coincida con la Guest Flow condición para devolver los detalles de acceso a la red una vez que el usuario se haya autenticado en el portal. Puede utilizar la Wifi Guest Access regla, que también se crea previamente de forma predeterminada en las versiones recientes de ISE. Entonces, solo tiene que habilitar la regla con una marca verde a la izquierda. Puede devolver el valor predeterminado PermitAccess o configurar restricciones de lista de acceso más precisas.



Paso 5. Guarde las reglas.

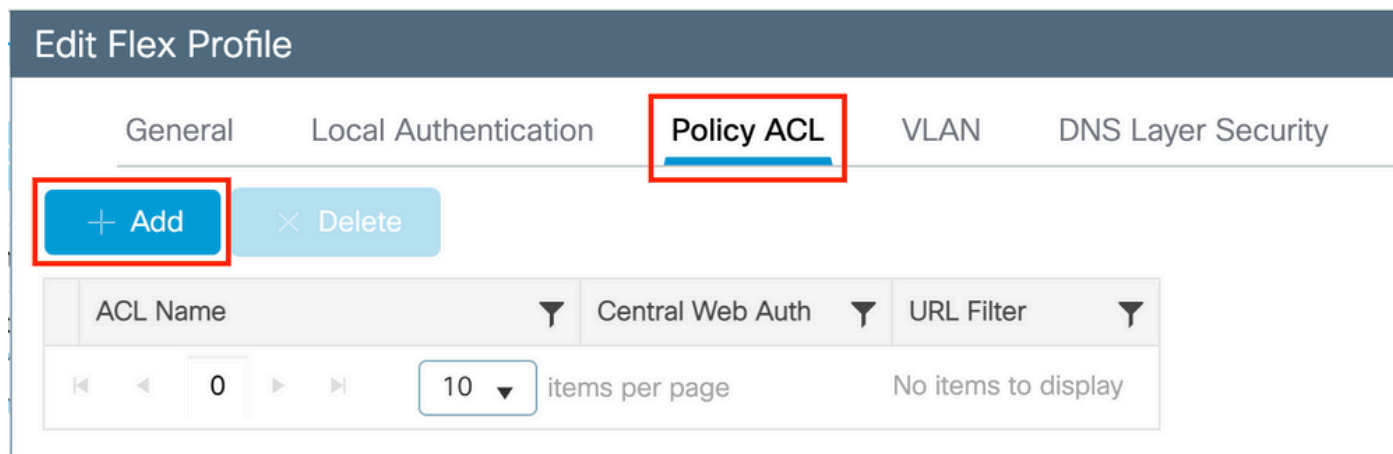
Haga clic Save en la parte inferior de las reglas.

SOLO puntos de acceso de switching local de FlexConnect

¿Qué sucede si tiene puntos de acceso de switching local y WLAN de FlexConnect? Las secciones anteriores siguen siendo válidas. Sin embargo, necesita un paso adicional para empujar la ACL de redirección a los AP con anticipación.

Desplácese hasta Configuration > Tags & Profiles > Flex y elija su perfil Flex. A continuación, vaya a la Policy ACL ficha.

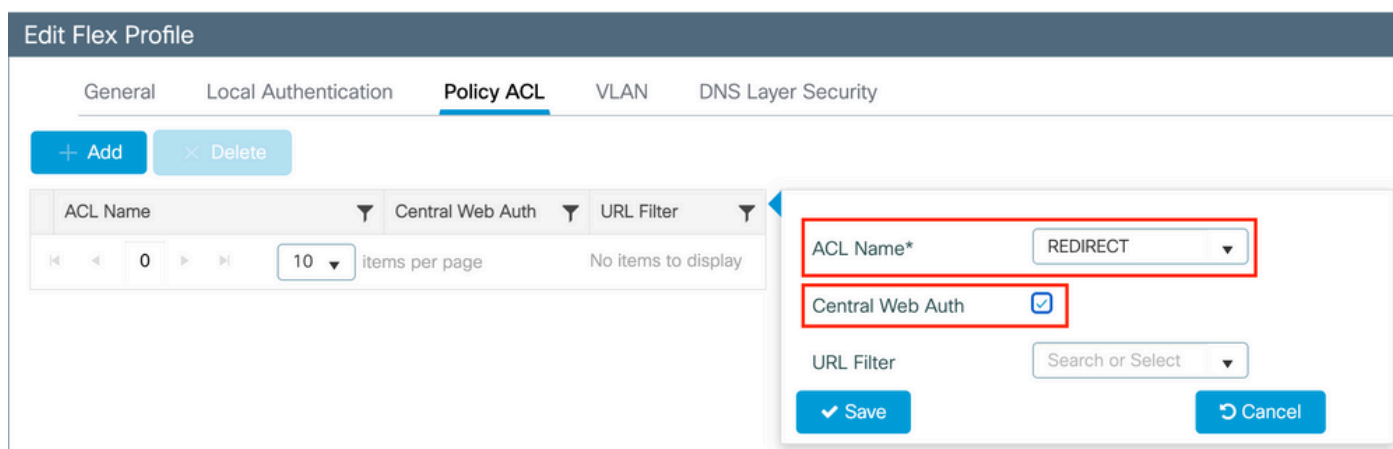
Haga clic Add como se muestra en la imagen.



Elija su nombre de ACL de redirección y habilite la autenticación web central. Esta casilla de verificación invierte automáticamente la ACL en el propio AP (esto se debe a que una sentencia 'deny' significa 'no redirigir a esta IP' en el WLC en Cisco IOS XE. Sin embargo, en el AP, la sentencia "deny" significa lo contrario. Por lo tanto, esta casilla de verificación intercambia automáticamente todos los permisos y los niega cuando realiza la transferencia al AP. Puede verificar esto con una show ip access list de la CLI del AP).

**Nota:** En el escenario de switching local de Flexconnect, la ACL debe mencionar específicamente las sentencias de retorno (lo que no es necesario en el modo local), de modo que asegúrese de que todas las reglas de la ACL cubran ambos modos de tráfico (hacia y desde ISE, por ejemplo).

No te olvides de golpear Save y luego Update and apply to the device.



## Certificados

Para que el cliente confíe en el certificado de autenticación web, no es necesario instalar ningún certificado en el WLC ya que el único certificado presentado es el certificado ISE (que tiene que ser de confianza por el cliente).

## Verificación

Puede utilizar estos comandos para verificar la configuración actual.

```
<#root>
```

```
# 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 | nme | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```

Aquí está la parte relevante de la configuración del WLC que corresponde a este ejemplo:

```
<#root>
```

```
aaa new-model !
aaa authorization network CWAauthz group radius aaa accounting identity CWAacct start-stop group radius ! aaa server radius dynamic-author client <ISE
mac-filtering CWAauthz
no security ft adaptive
no security wpa
no security wpa wpa2
no security wpa wpa2 ciphers aes
no security wpa akm dot1x
no shutdown
ip http server (or "webauth-http-enable" under the parameter map)
ip http secure-server
```

## Troubleshoot

### Lista de Verificación

- Asegúrese de que el cliente se conecta y obtiene una dirección IP válida.
- Si la redirección no es automática, abra un explorador y pruebe con una dirección IP aleatoria. Por ejemplo, 10.0.0.1. Si la redirección funciona, es posible que tenga un problema de resolución de DNS. Verifique que tiene un servidor DNS válido proporcionado a través de DHCP y que puede resolver los nombres de host.
- Asegúrese de tener el comando `ip http server` configurado para la redirección en HTTP para que funcione. La configuración del portal de administración web está vinculada a la configuración del portal de autenticación web y debe aparecer en el puerto 80 para

poder redirigir. Puede optar por habilitarlo globalmente (con el uso del comando ip http server) o puede habilitar HTTP sólo para el módulo de autenticación web (con el uso del comando webauth-http-enable bajo el mapa de parámetro).

- Si no se le redirige cuando intenta acceder a una URL HTTPS y eso es necesario, verifique que tenga el comando intercept-https-enable bajo el mapa de parámetro:

```
<#root>
```

```
parameter-map type webauth global  
type webauth
```

```
intercept-https-enable
```

```
trustpoint xxxxx
```

También puede verificar a través de la GUI que tiene la opción 'Web Auth intercept HTTPS' marcada en el mapa de parámetro:

The screenshot shows the Cisco GUI configuration page for 'Web Auth'. The breadcrumb navigation is 'Configuration > Security > Web Auth'. The page title is 'Edit Web Auth Parameter'. On the left, a sidebar menu includes Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area shows a table of 'Parameter Map Name' with one entry, 'global', which is selected. Below the table, there are navigation controls and a '10 items per page' dropdown. On the right, the 'Edit Web Auth Parameter' form contains several fields: 'Maximum HTTP connections' (100), 'Init-State Timeout(secs)' (120), 'Type' (webauth), 'Virtual IPv4 Address' (empty), 'Trustpoint' (--- Select ---), 'Virtual IPv6 Address' (xxxx:xx:xx:xx), 'Web Auth intercept HTTPS' (checked), and 'Captive Bypass Portal' (unchecked). The 'Web Auth intercept HTTPS' checkbox is highlighted with a red box.

Soporte de Puerto de Servicio para RADIUS

El controlador inalámbrico Catalyst de Cisco serie 9800 tiene un puerto de servicio que se denomina GigabitEthernet 0puerto. A partir de la versión 17.6.1, RADIUS (que incluye CoA) es compatible con este puerto.

Si desea utilizar el puerto de servicio para RADIUS, necesita esta configuración:

```
<#root>
```

```
aaa server radius dynamic-author  
client 10.48.39.28
```

```
vrf Mgmt-intf
```

```
server-key cisco123

interface GigabitEthernet0

vrf forwarding Mgmt-intf

ip address x.x.x.x x.x.x.x

!if using aaa group server:
aaa group server radius group-name
server name nicoISE

ip vrf forwarding Mgmt-intf

ip radius source-interface GigabitEthernet0
```

Recopilar depuraciones

El WLC 9800 ofrece capacidades de seguimiento SIEMPRE ACTIVAS. Esto garantiza que todos los errores, advertencias y mensajes de nivel de notificación 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:** Puede retroceder unas horas a varios días en los registros, pero depende del volumen de registros generados.

---

Para ver los seguimientos que 9800 WLC recolectó por defecto, puede conectarse vía 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.

```
<#root>
```

```
# 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 los hubiera.

```
<#root>
```

```
# show logging
```




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

```
<#root>
```

```
# show debugging Cisco IOS XE Conditional Debug Configs: Conditional Debug Global State: Stop Cisco IOS XE Packet Tracing Configs: Packet Infra d
```

---

 **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 realiza una depuración activa.

---

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

```
<#root>
```

```
# 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.

```
<#root>
```

```
# 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). Para habilitar la depuración condicional, continúe con estos pasos.

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

```
<#root>
```

```
# 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 2 085 978 494 segundos.

```
<#root>
```

```
# 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 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.

```
<#root>
```

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

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

```
ra_trace_MAC_aaaabbbccccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

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

Verifique el nombre del archivo de seguimiento activo por radio.

```
<#root>
```

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

Copie el archivo en un servidor externo:

```
<#root>
```

```
# 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:

```
<#root>
```

```
# 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 solo examinamos con más detalle los registros de depuración que ya se han recopilado y almacenado internamente.

```
<#root>
```

```
# 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. Póngase en contacto con el TAC de Cisco para analizar estos seguimientos.

---

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

Copie el archivo en un servidor externo:

```
<#root>
```

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

Muestre el contenido:

```
<#root>
```

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

Paso 11. Elimine las condiciones de depuración.

```
<#root>
```

```
# clear platform condition all
```



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

## Examples

Si el resultado de la autenticación no es el esperado, es importante navegar hasta la página de ISEOperations > Live logs y obtener los detalles del resultado de la autenticación.

Se le indica el motivo del error (si se produce) y todos los atributos RADIUS recibidos por ISE.

En el siguiente ejemplo, ISE rechazó la autenticación porque no coincidía ninguna regla de autorización. Esto se debe a que ve el atributo Called-station-ID enviado como el nombre SSID agregado a la dirección MAC del AP, mientras que la autorización es una coincidencia exacta con el nombre SSID. Se fija con el cambio de esa regla a 'contiene' en lugar de 'igual'.

Event	5400 Authentication failed
Failure Reason	15039 Rejected per authorization profile
Resolution	Authorization Profile with ACCESS_REJECT attribute was selected as a result of the matching authorization rule. Check the appropriate Authorization policy rule-results.
Root cause	Selected Authorization Profile contains ACCESS_REJECT attribute
Username	E8:36:17:1F:A1:62

```
15048 Queried PIP - Radius.NAS-Port-1 type
15048 Queried PIP - Network Access.UserName
15048 Queried PIP - IdentityGroup.Name (2 times)
15048 Queried PIP - EndPoints.LogicalProfile
15048 Queried PIP - Radius.Called-Station-ID
15048 Queried PIP - Network Access.AuthenticationStatus
15016 Selected Authorization Profile - DenyAccess
15039 Rejected per authorization profile
11003 Returned RADIUS Access-Reject
```

## Other Attributes

ConfigVersionId	140
Device Port	58209
DestinationPort	1812
RadiusPacketType	AccessRequest
Protocol	Radius
NAS-Port	71111
Framed-MTU	1485
OriginalUserName	e836171fa162
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	nicolse26/356963261/1
UseCase	Host Lookup
SelectedAuthenticationIdentityStores	Internal Endpoints
IdentityPolicyMatchedRule	MAB
AuthorizationPolicyMatchedRule	Default
EndPointMACAddress	E8-36-17-1F-A1-62
ISEPolicySetName	Default
IdentitySelectionMatchedRule	MAB
DTLSSupport	Unknown
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
RADIUS Username	E8:36:17:1F:A1:62
NAS-Identifler	cwa-ssid
Device IP Address	10.48.71.120
CPMSessionID	7847300A0000012DFC227BF1
Called-Station-ID	00-27-e3-8f-33-a0:cwa-ssid
CiscoAVPair	service-type=Call Check, audit-session-id=7847300A0000012DFC227BF1, method=mab, client-if-id=3003124185, vlan-id=1468, cisco-wlan-ssid=cwa-ssid

Troubleshooting > Radioactive Trace

Conditional Debug Global State: **Stopped**

+ Add - Delete Start Stop

MAC/IP Address	Trace file
<input type="checkbox"/> e836.171f.a162	debugTrace_e836.171f.a162.txt <a href="#">Download</a>

1 10 items per page 1 - 1 of 1 items

Generate

En este caso, el problema radica en el hecho de que cometió un error tipográfico cuando creó el nombre de ACL y no coincide con el nombre de ACL devuelto por ISE o el WLC se queja de que no existe tal ACL como la solicitada por ISE:

<#root>

2019/09/04 12:00:06.507 {wncd\_x\_R0-0}{1}: [client-auth] [24264]: (ERR): MAC: e836.171f.a162 client authz result: FAILURE 2019/09/04 12:00:06.51

## 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).