# Configuración del SSID de autenticación de MAC en los controladores inalámbricos Catalyst 9800

## Contenido



## Introducción

Este documento describe cómo configurar una red de área local inalámbrica (WLAN) con seguridad de autenticación MAC en Cisco Catalyst 9800 WLC.

## Prerequisites

### Requisito

Cisco recomienda que tenga conocimiento sobre estos temas:

- Dirección MAC
- Controladores inalámbricos Cisco Catalyst serie 9800
- Identity Service Engine (ISE)

### Componentes Utilizados

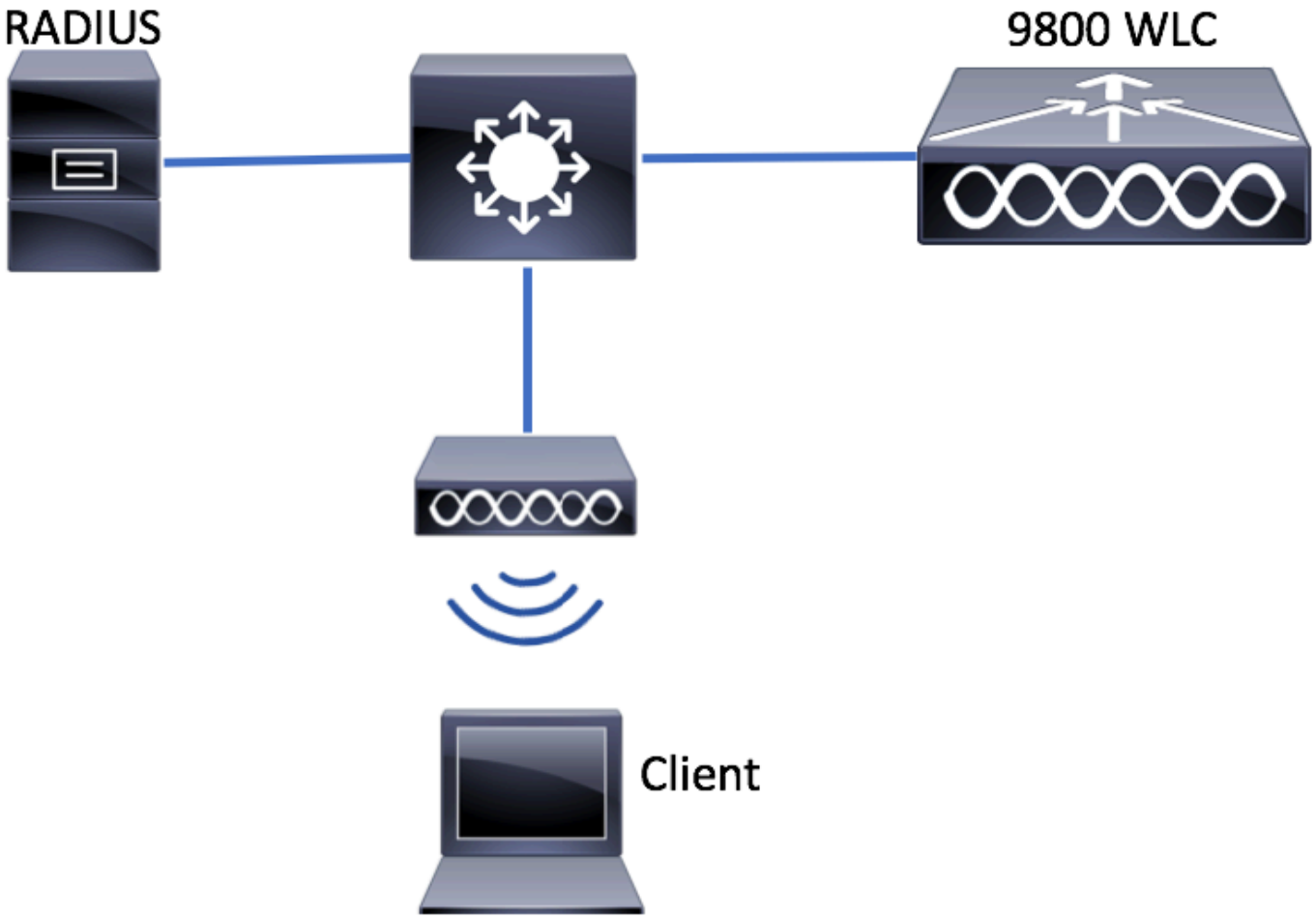
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco IOS® XE Gibraltar v16.12
- ISE v2.2

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 AAA en WLC 9800

Autenticar clientes con servidor externo

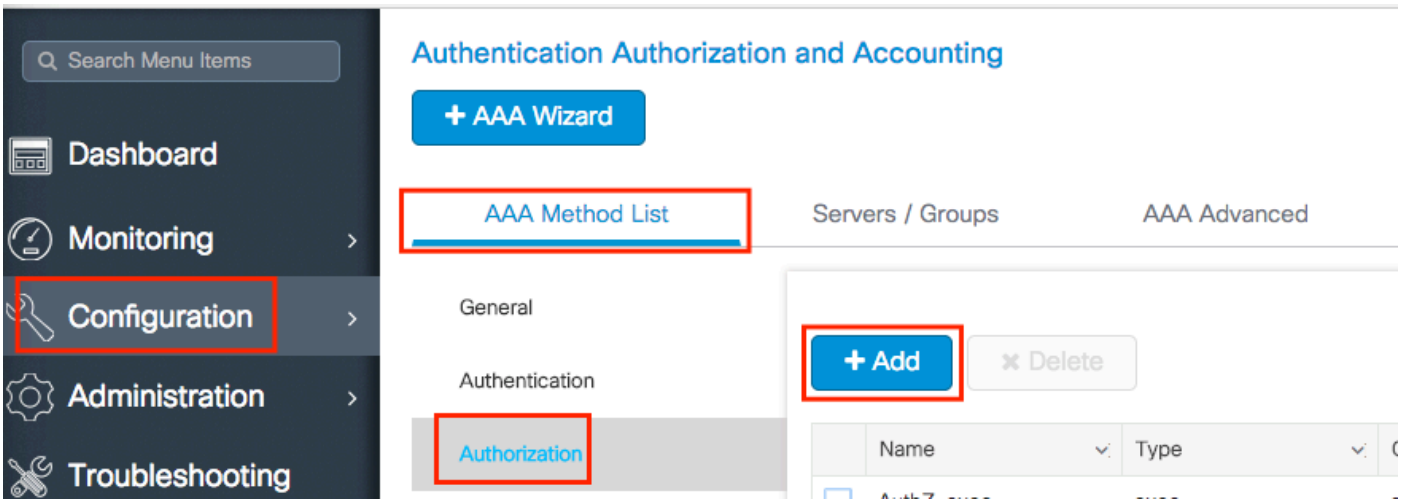
GUI:

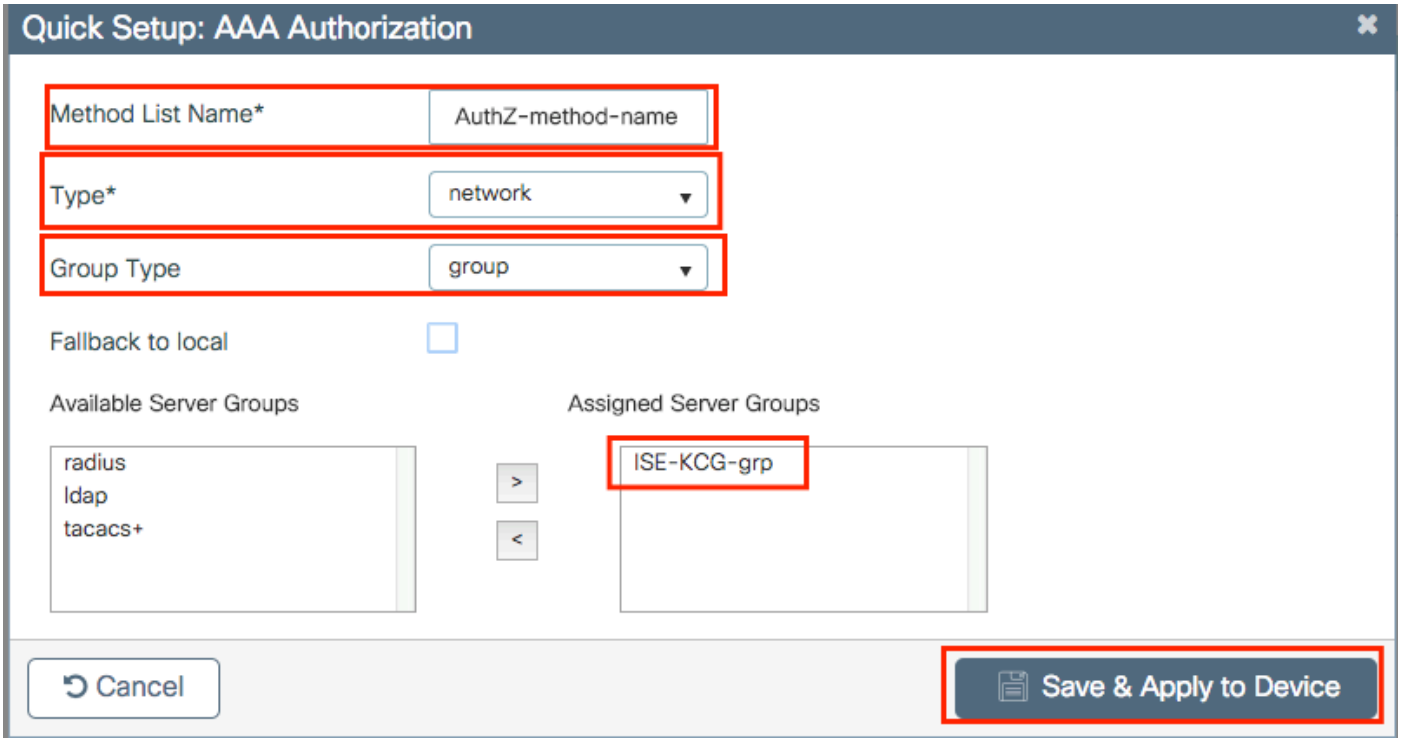
Lea los pasos 1-3 de la sección 'Configuración AAA en WLC 9800' de este link:

[Configuración AAA en el WLC de la serie 9800]

Paso 4. Cree un método de red de autorización.

Desplácese hasta yConfiguration > Security > AAA > AAA Method List > Authorization > + Addcréelo.




CLI:

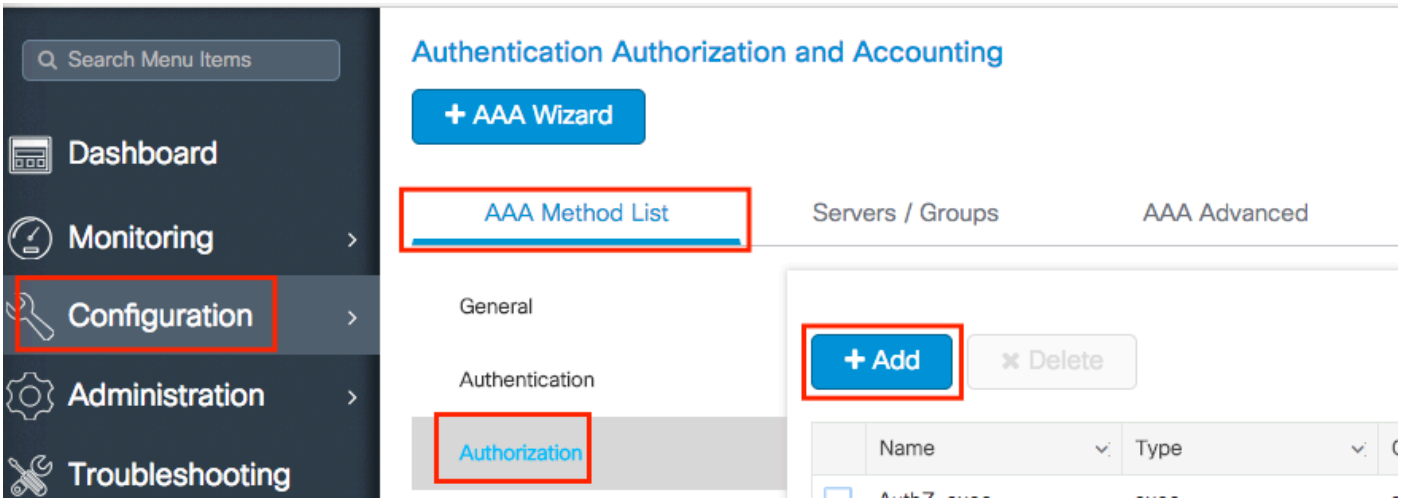
```
# config t
# aaa new-model

# radius server <radius-server-name>
# address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813
# timeout 300
```

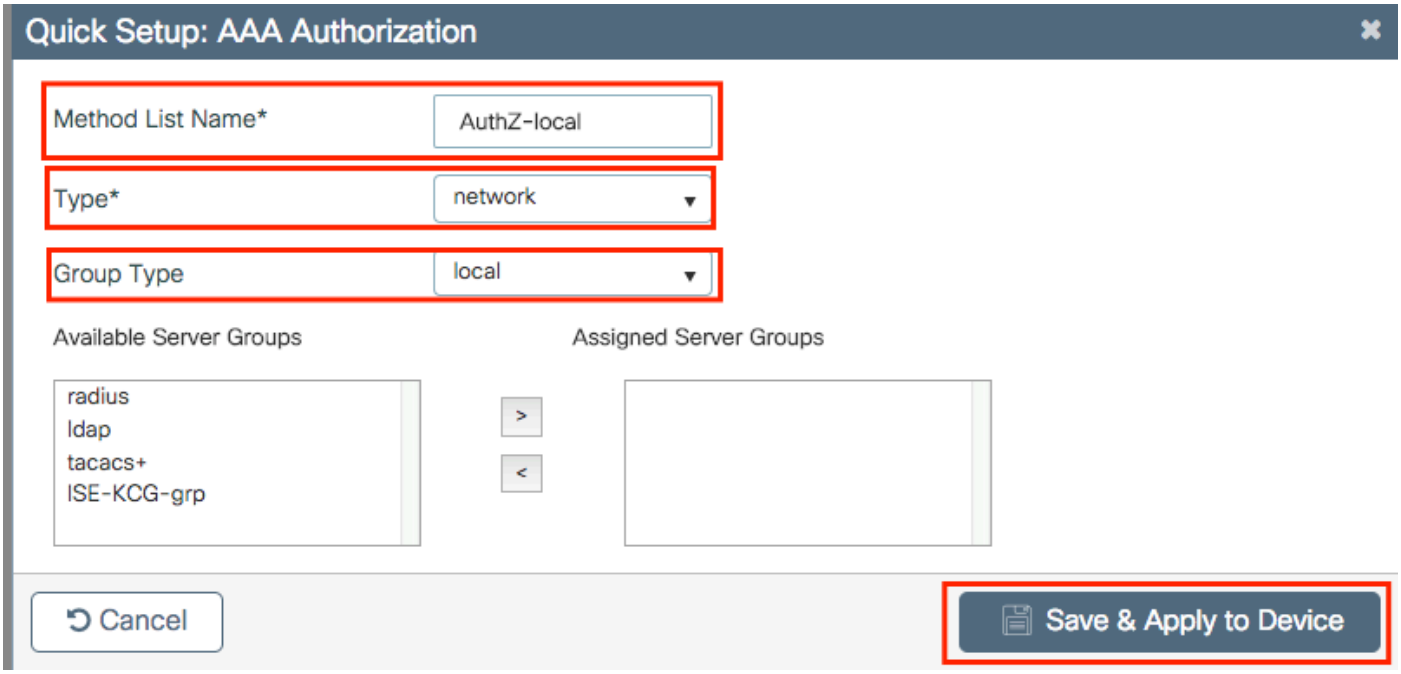
```
# retransmit 3
# key <shared-key>
# exit

# 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 authorization network <AuthZ-method-name> group <radius-grp-name>
```

Autenticar clientes localmente

Cree un método de red de autorización local.

Desplácese hasta yConfiguration > Security > AAA > AAA Method List > Authorization > + Addcréelo.



CLI:

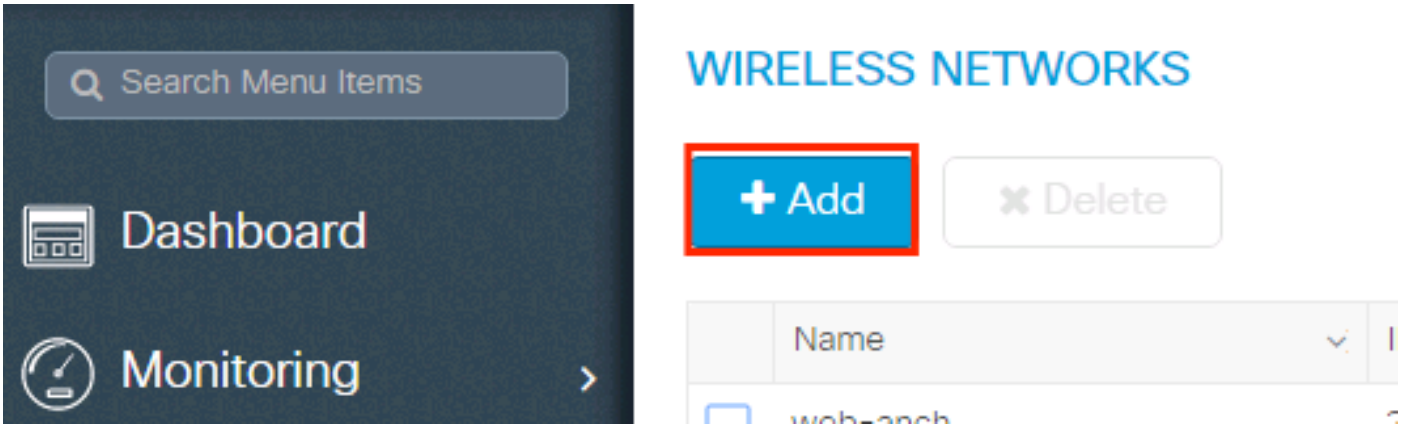
```
# config t
# aaa new-model
# aaa authorization network AuthZ-local local
```

## Configuración de WLAN

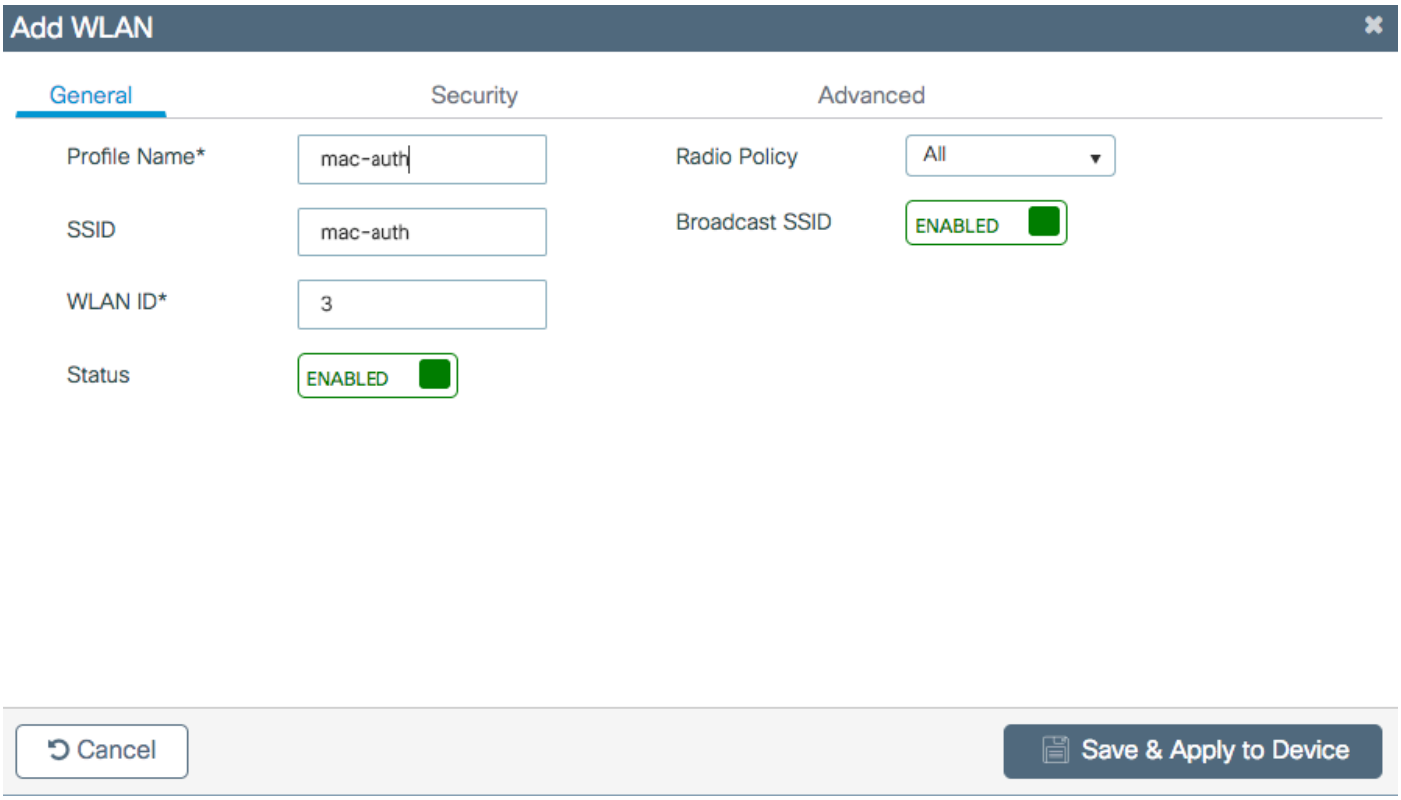
GUI:

Paso 1. Cree la WLAN.

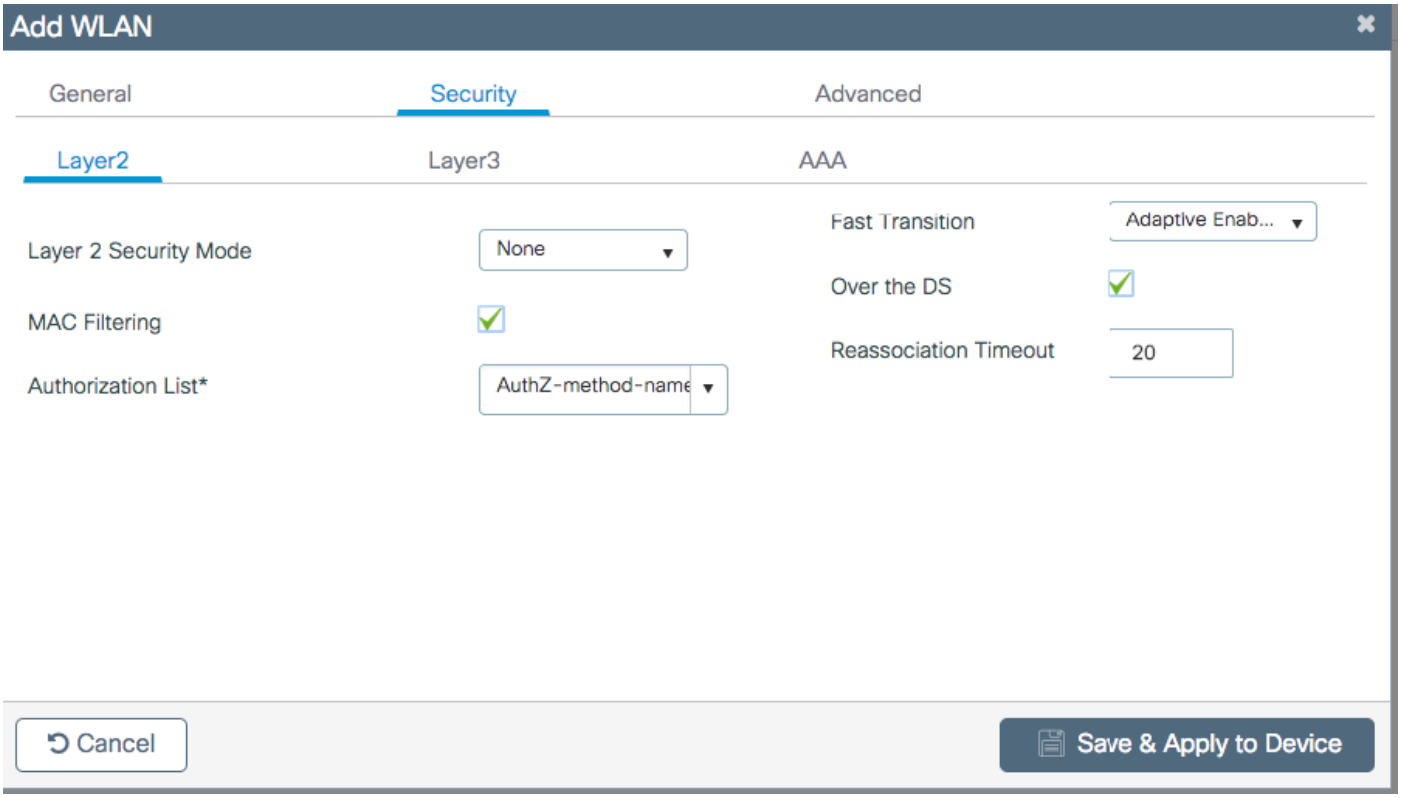
Configuration > Wireless > WLANs > + AddDesplácese hasta la red y configúrela según sea necesario.




Paso 2. Introduzca la información de la WLAN.




Paso 3. Vaya a laSecurityficha y desactiveLayer 2 Security Modey activeMAC Filtering. EnAuthorization List, elija el método de autorización creado en el paso anterior. A continuación, haga clic enSave & Apply to Device.




CLI:

```
# config t
# wlan <profile-name> <wlan-id> <ssid-name>
# mac-filtering <authZ-network-method>
# no security wpa akm dot1x
# no security wpa wpa2 ciphers aes
# no shutdown
```

## Configuración del perfil de la política

Debe activaraaa-overrideen el perfil de política para asegurarse de que el filtrado de MAC por SSID funciona correctamente.

Configuración del perfil de política en 9800 WLC

Configuración de etiquetas de políticas

Etiqueta de política en el WLC 9800

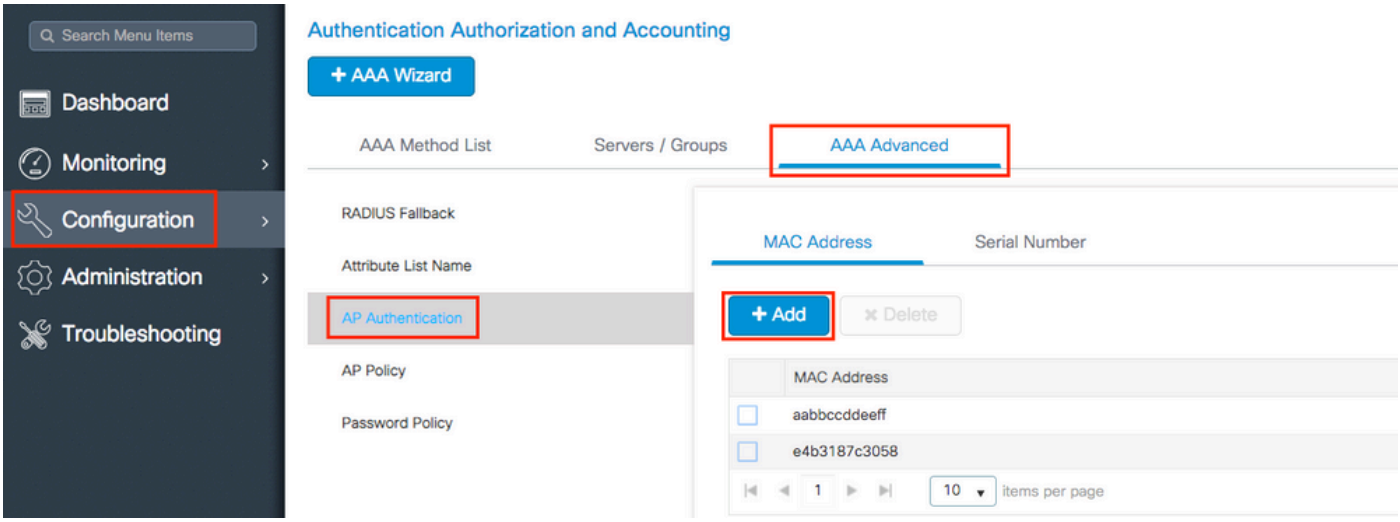
Asignación de etiquetas de políticas

Asignación de etiquetas de políticas en el WLC 9800

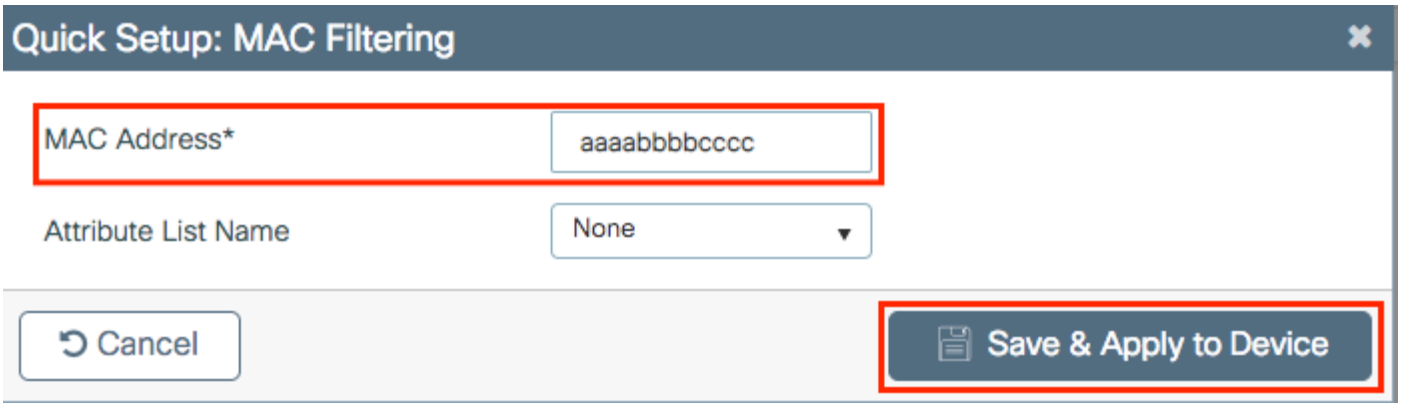
Registre la dirección MAC permitida.

Registre localmente la dirección MAC en el WLC para la autenticación local

Desplácese hastaConfiguration > Security > AAA > AAA Advanced > AP Authentication > + Add.




Escriba la dirección MAC en minúsculas sin separadores y haga clic enSave & Apply to Device.



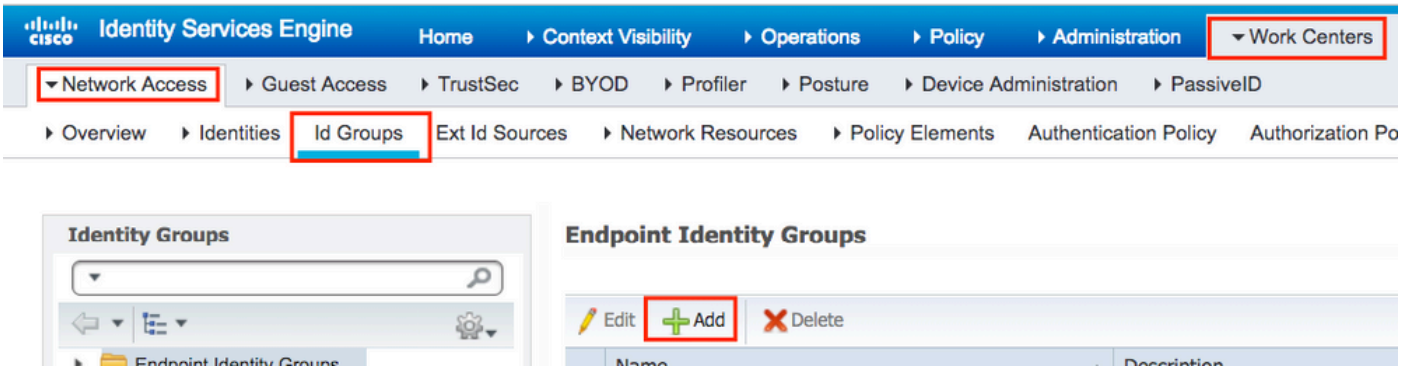

Nota: En las versiones anteriores a la 17.3, la interfaz de usuario web cambió cualquier formato MAC que haya escrito al formato 'sin separador' que se muestra en la ilustración. En la versión 17.3 y posteriores, la interfaz de usuario web respeta cualquier diseño que haya introducido y, por lo tanto, es esencial no introducir ningún separador. El Id. de bug Cisco CSCvv43870 de la mejora rastrea el soporte de varios formatos para la autenticación MAC.

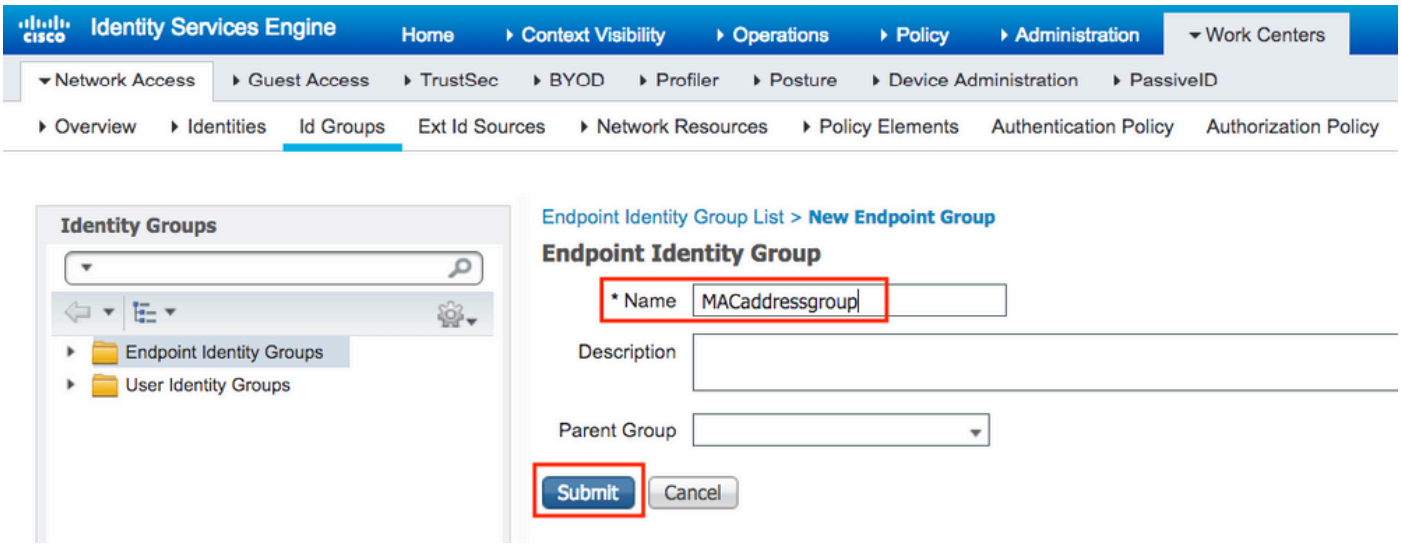
CLI:

```
# config t
# username <aabbccddeeff> mac
```

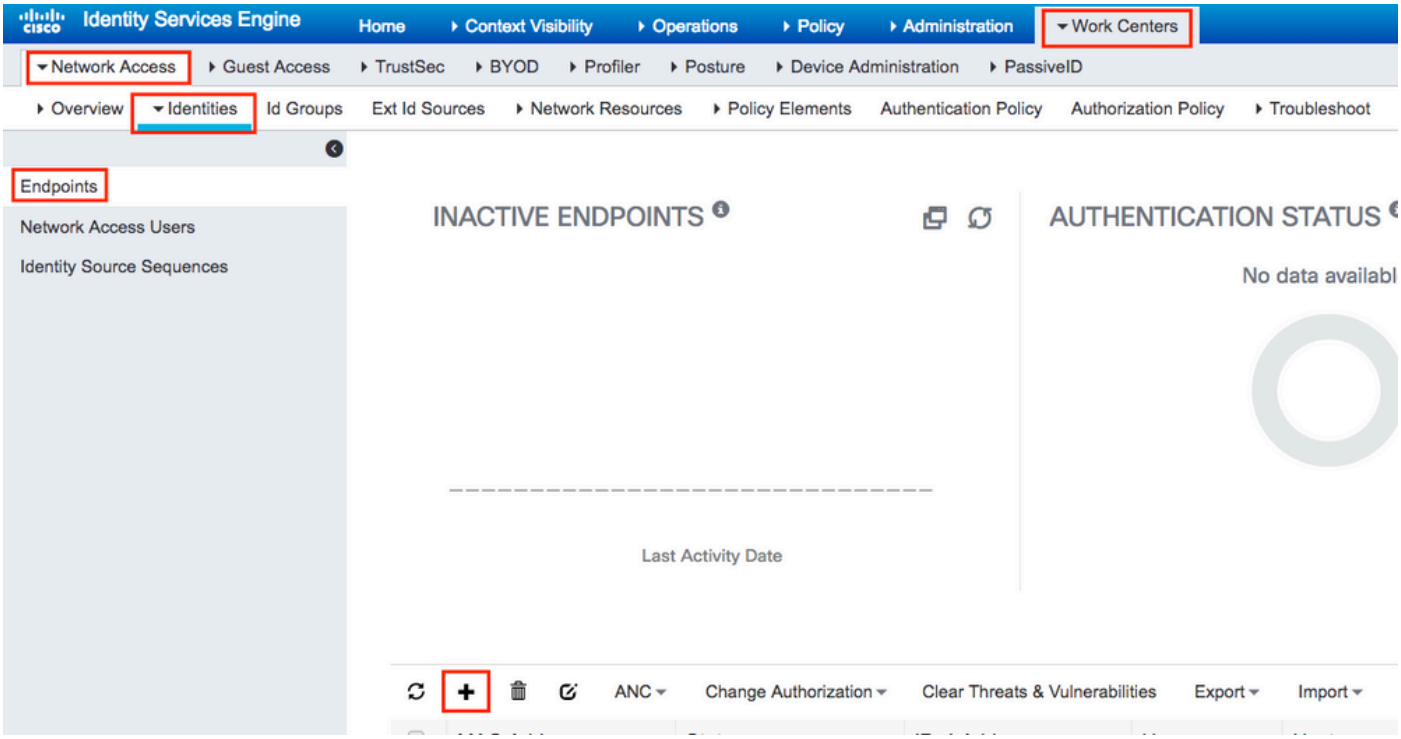
Introduzca la dirección MAC en la base de datos de terminales ISE

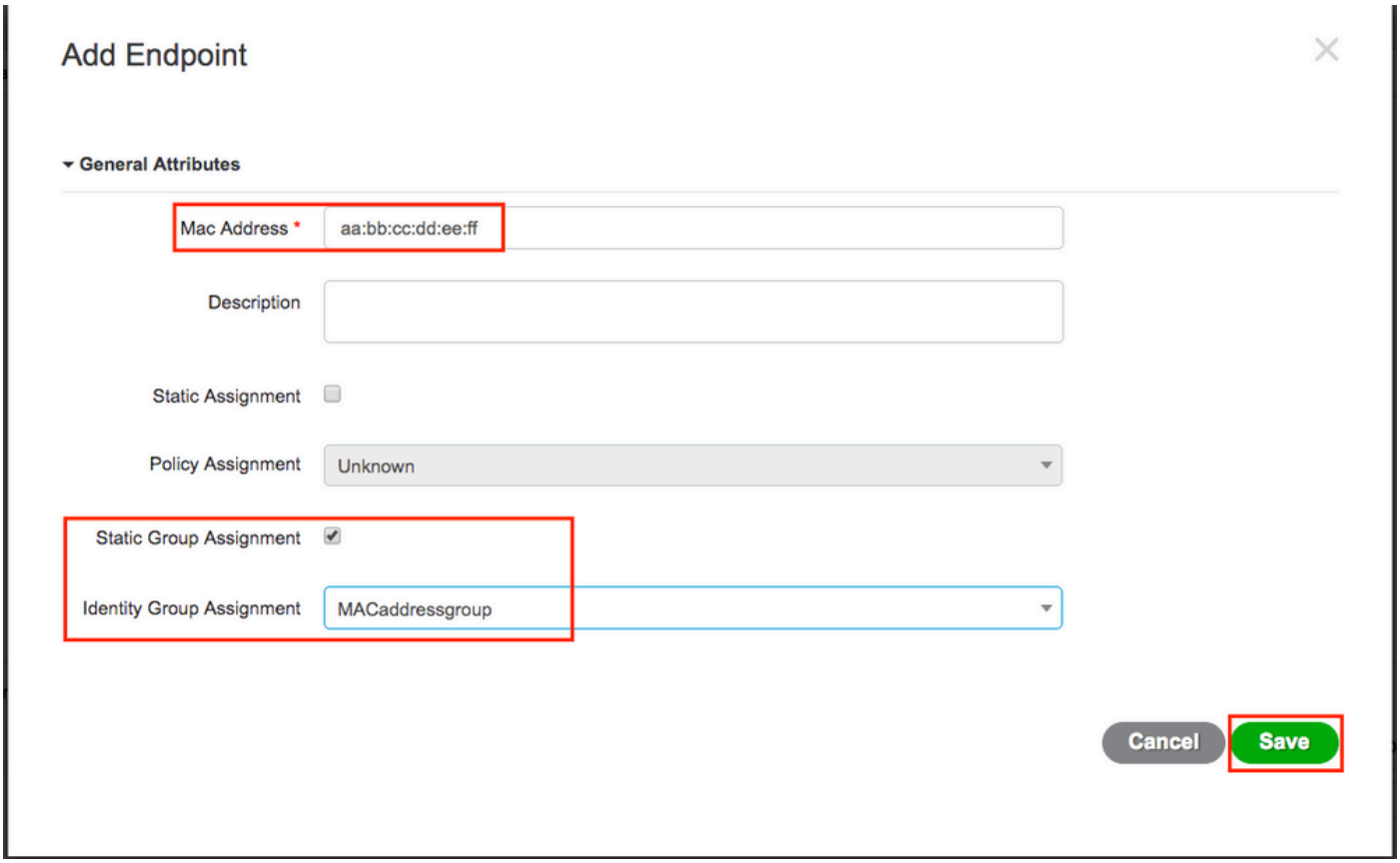
Paso 1. (Opcional) Cree un nuevo grupo de terminales.
Desplácese hastaWork Centers > Network Access > Id Groups > Endpoint Identity Groups > + Add.






Paso 2. Desplácese hasta Work Centers > Network Access > Identities > Endpoints > +Add.






Configuración de ISE

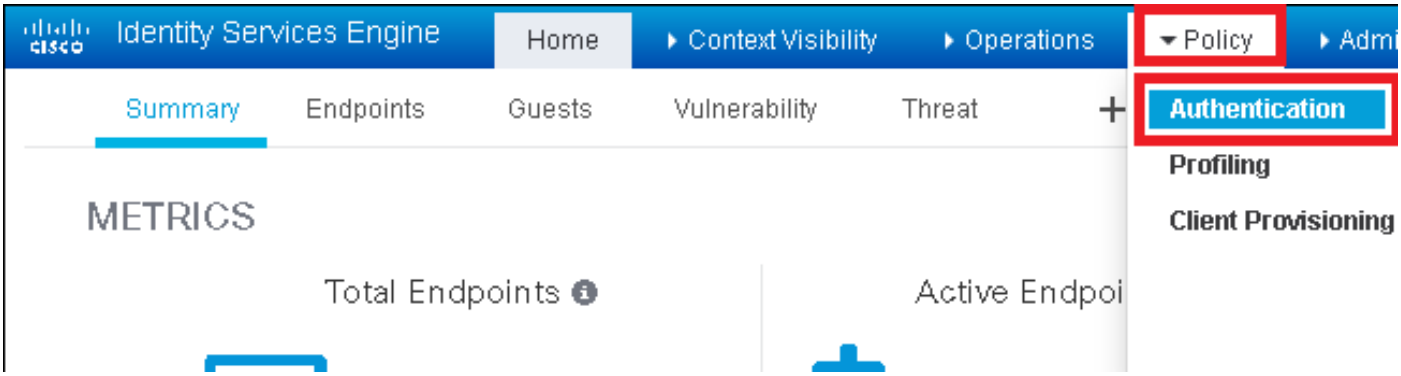
Adición del WLC 9800 a ISE.

Lea las instrucciones de este enlace: Declare el WLC a ISE.

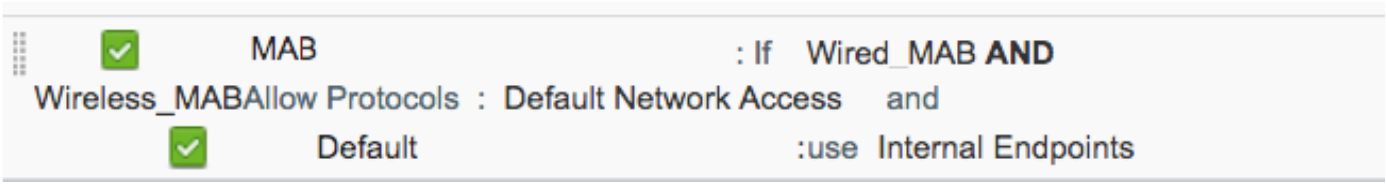
## Crear una regla de autenticación

Las reglas de autenticación se utilizan para comprobar si las credenciales de los usuarios son correctas (comprobar si el usuario es realmente quien dice ser) y limitar los métodos de autenticación que puede utilizar.

Paso 1. Desplácese hasta Policy > Authentication como se muestra en la imagen.
Confirme que la regla MAB predeterminada existe en su ISE.



Paso 2. Verifique que la regla de autenticación predeterminada para MAB ya existe:

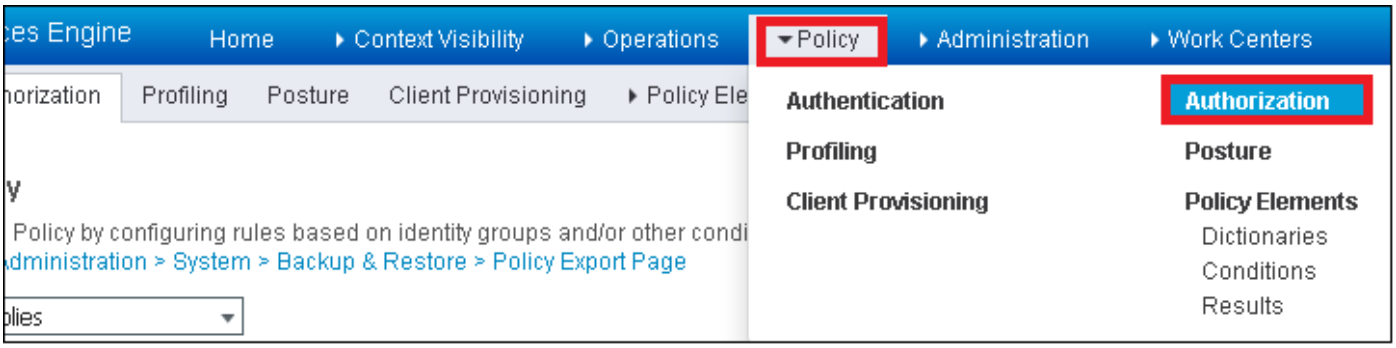



Si no es así, puede agregar uno nuevo al hacer clic enInsert new row above.

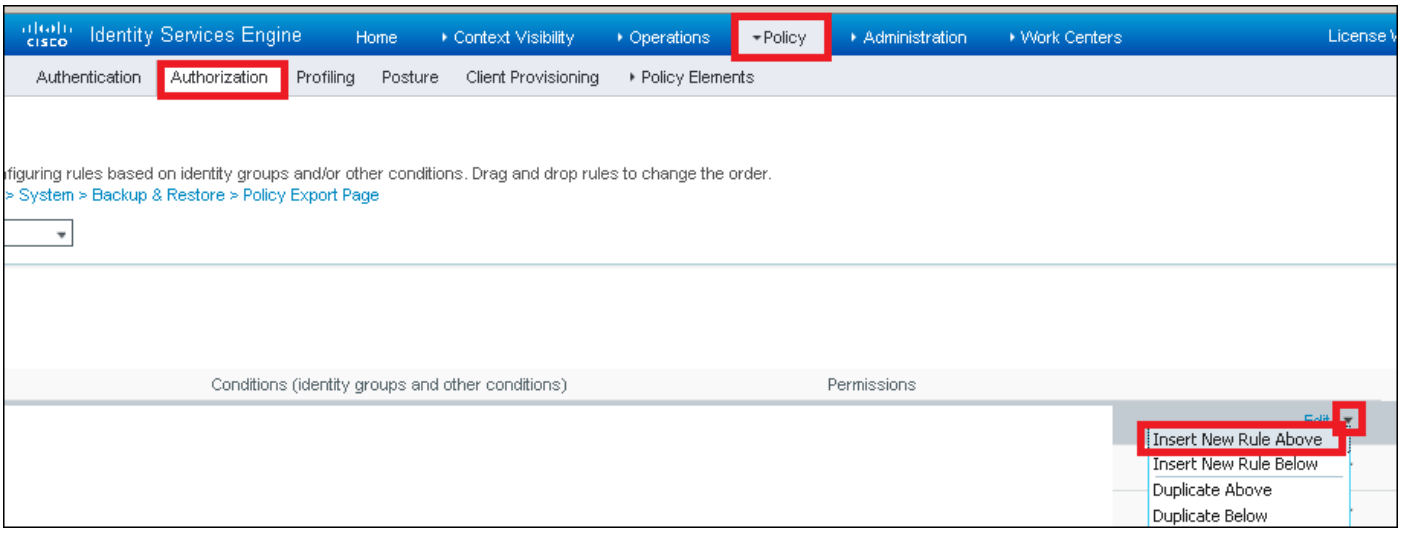

Creación de reglas de autorización

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

Paso 1. Desplácese hastaPolicy > Authorizationcomo se muestra en la imagen.

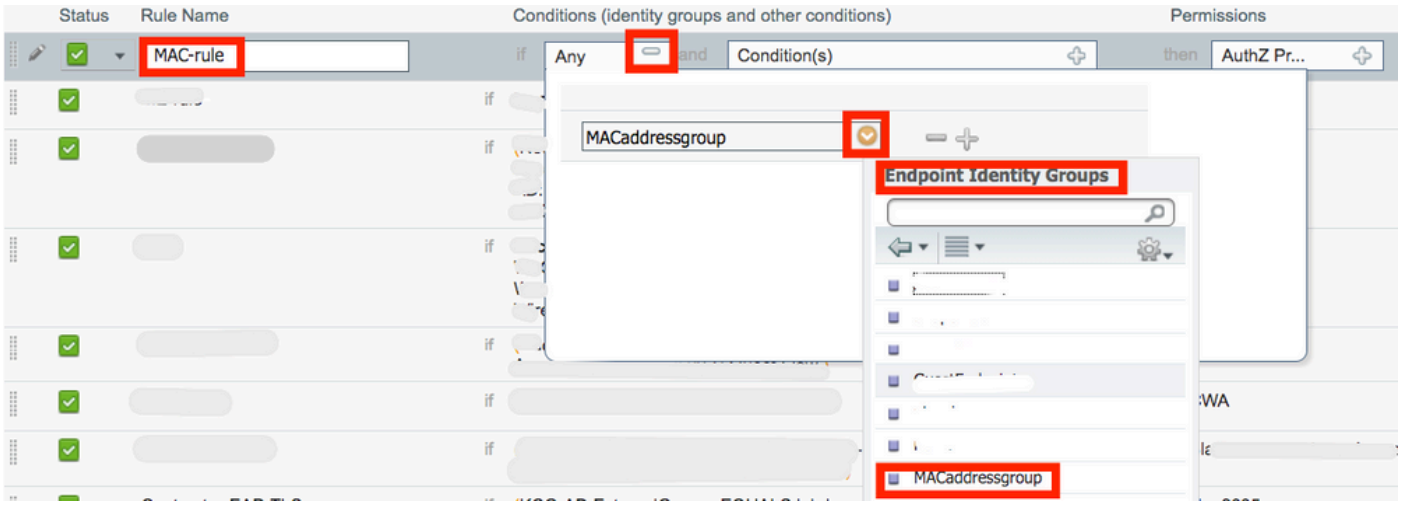



Paso 2. Inserte una nueva regla como se muestra en la imagen.

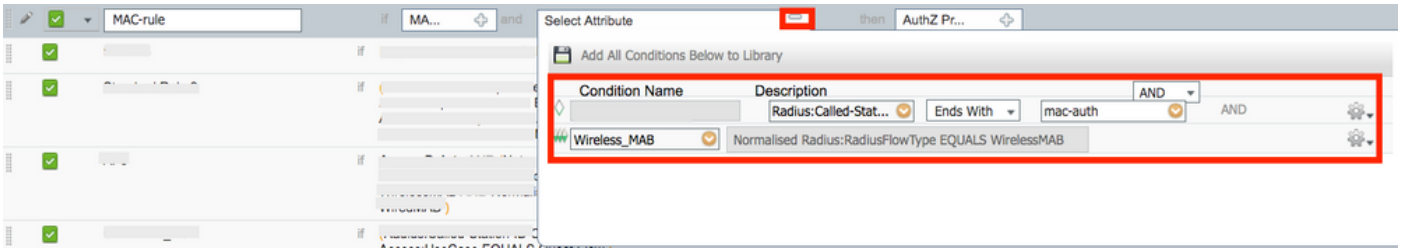



Paso 3. Introduzca los valores.

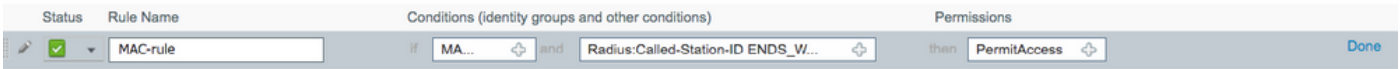
En primer lugar, elija un nombre para la regla y el grupo de identidad donde se almacena el extremo (**MACaddressgroup**), como se muestra en la imagen.




Después de esto, elija otras condiciones que realizan el proceso de autorización para que se ajusten a esta regla. En este ejemplo, el proceso de autorización llega a esta regla si utiliza Wireless MAB y su ID de estación llamada (el nombre del SSID) termina con`mac-auth`como se muestra en la imagen.




Por último, elija el perfil de autorización que se asigna, en este caso,`PermitAccess`a los clientes que cumplen esa regla. Haga clic`Done`y guárdelo.



# Verificación

Puede utilizar estos comandos para verificar la configuración actual:

```
# 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 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: Aunque depende del 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 leer 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 desde el momento en que se produjo el problema.

```
# 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 y los errores del sistema, si los hubiera.

```
# show logging
```

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

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Tracing Configs:


Packet Infra debugs:

Ip Address                                              Port
------------------------------------------------------|----------
```

---

Nota: Si ve alguna condición en la lista, significa que los seguimientos se 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. Si la dirección MAC en la 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-
```

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). Para habilitar la depuración condicional, lea 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.

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.

```
# 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 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.

```
# 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_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 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:

```
# 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.
```

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 solo se tiene en cuenta un aspecto más detallado de 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 r
```

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 elra-internal-FILENAME.txten 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 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).

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).