Configuración de la lista de autorización AP de controladores inalámbricos Catalyst 9800

Contenido

Introducción

Este documento describe cómo configurar la política de autenticación del punto de acceso (AP) del controlador LAN inalámbrico Catalyst 9800.

Antecedentes

Para autorizar un punto de acceso (AP), la dirección MAC Ethernet del AP debe autorizarse frente a la base de datos local con el controlador de LAN inalámbrica 9800 o frente a un servidor externo del servicio de usuario de acceso telefónico de autenticación remota (RADIUS).

Esta función garantiza que solo los puntos de acceso (AP) autorizados puedan conectarse a un controlador de LAN inalámbrica Catalyst 9800. Este documento no cubre el caso de los AP de malla (serie 1500) que requieren una entrada de filtro mac para unirse al controlador pero no rastrean el flujo de autorización de AP típico (ver referencias).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- WLC 9800
- Acceso mediante la interfaz de línea de comandos (CLI) a los controladores inalámbricos

Componentes Utilizados

9800 WLC v17.3

AP 1810W

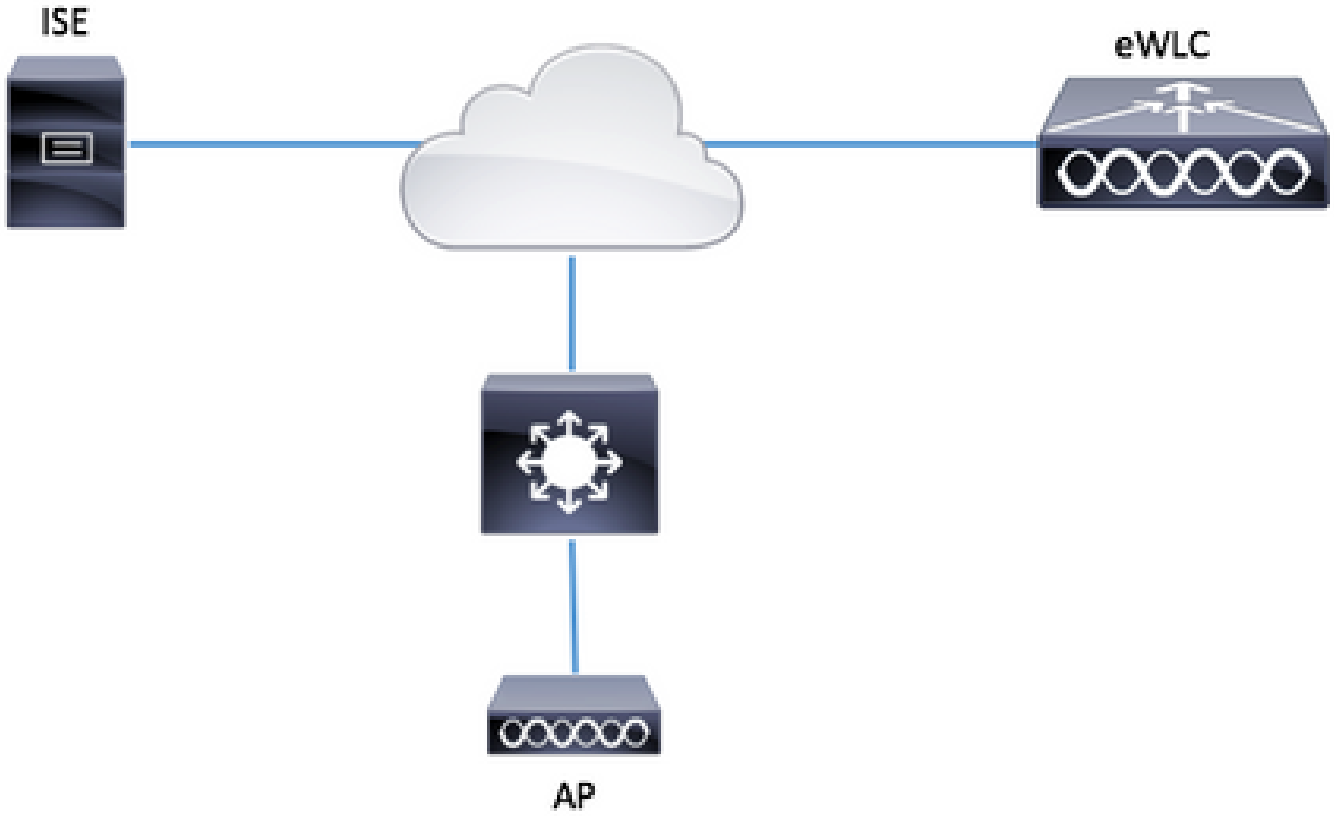
AP 1700

Identity Service Engine (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



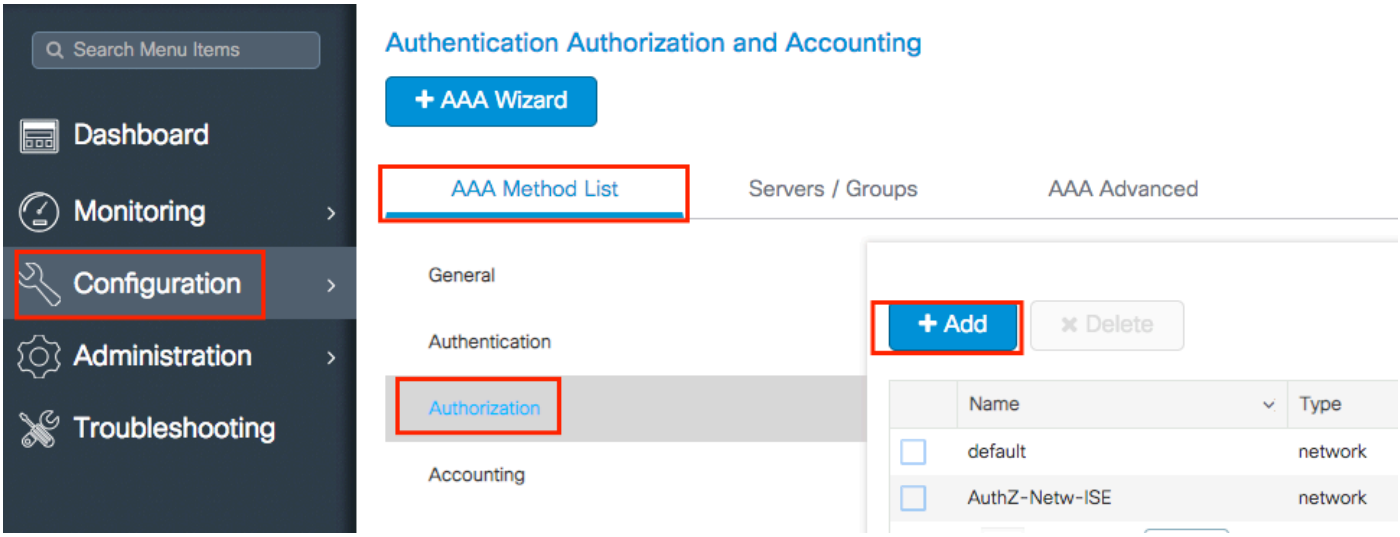
Configuraciones

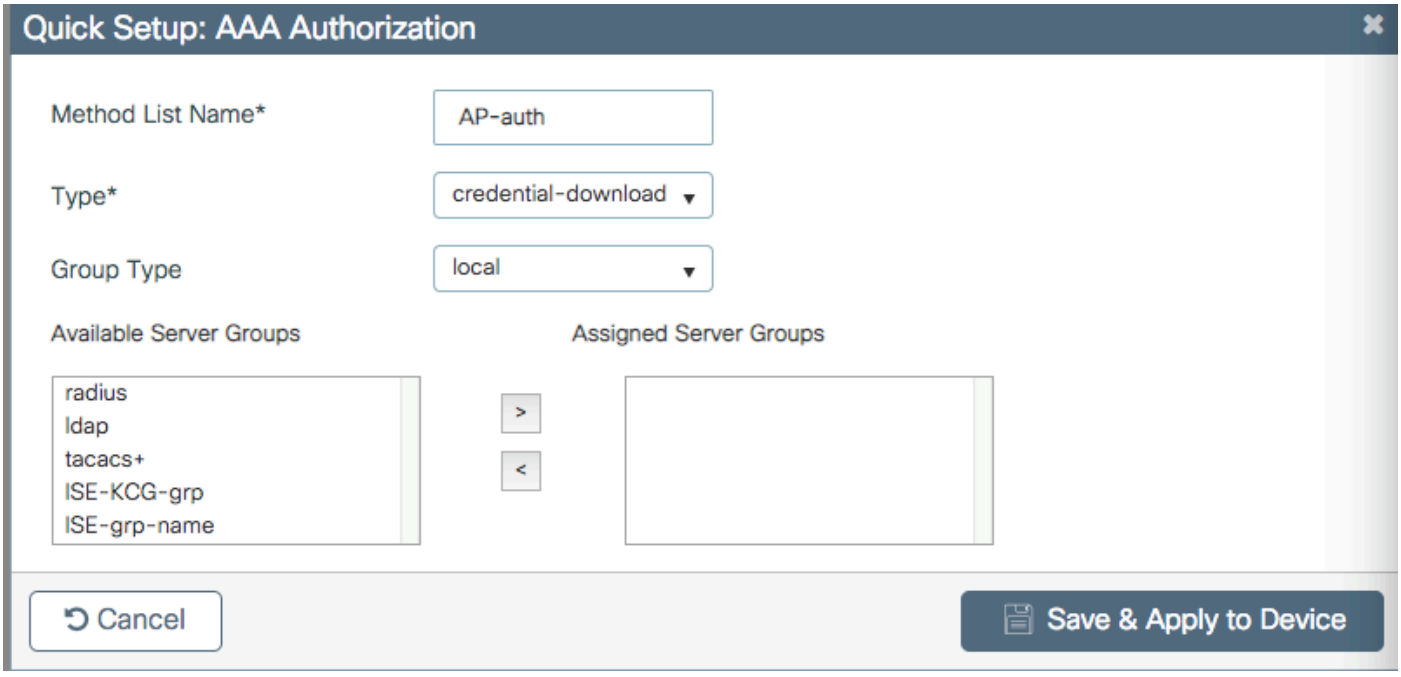
Lista de autorizaciones de MAC AP: local

La dirección MAC de los AP autorizados se almacena localmente en el WLC 9800.

Paso 1. Cree una lista de métodos de descarga de credenciales de autorización local.

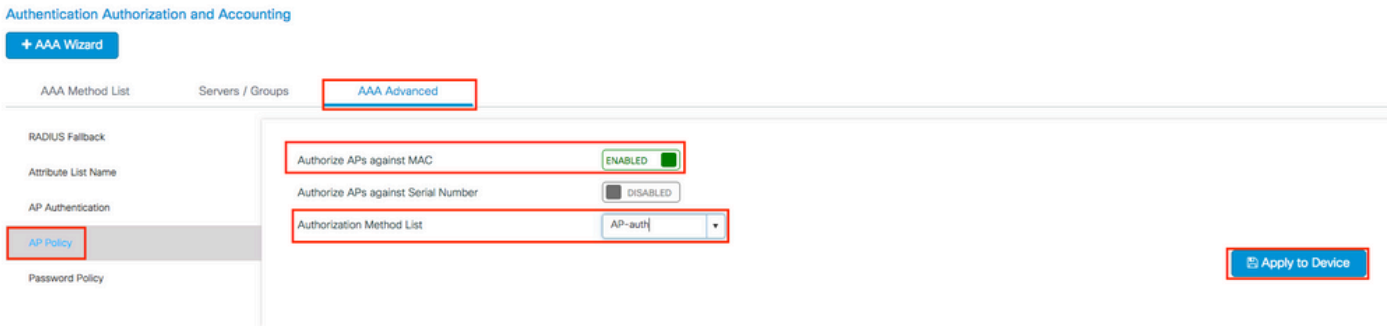
Vaya a Configuration > Security > AAA > AAA Method List > Authorization > + Add





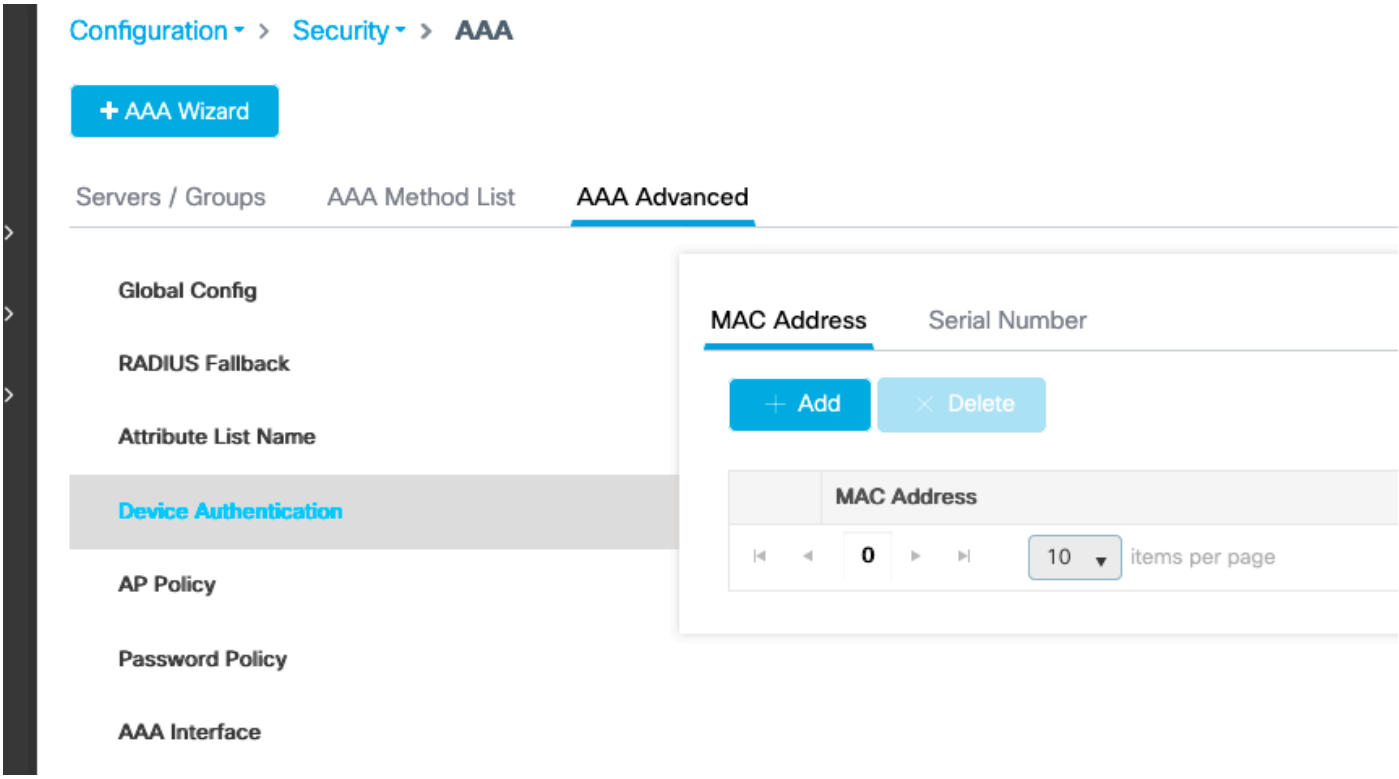
Paso 2. Habilite la autorización MAC de AP.

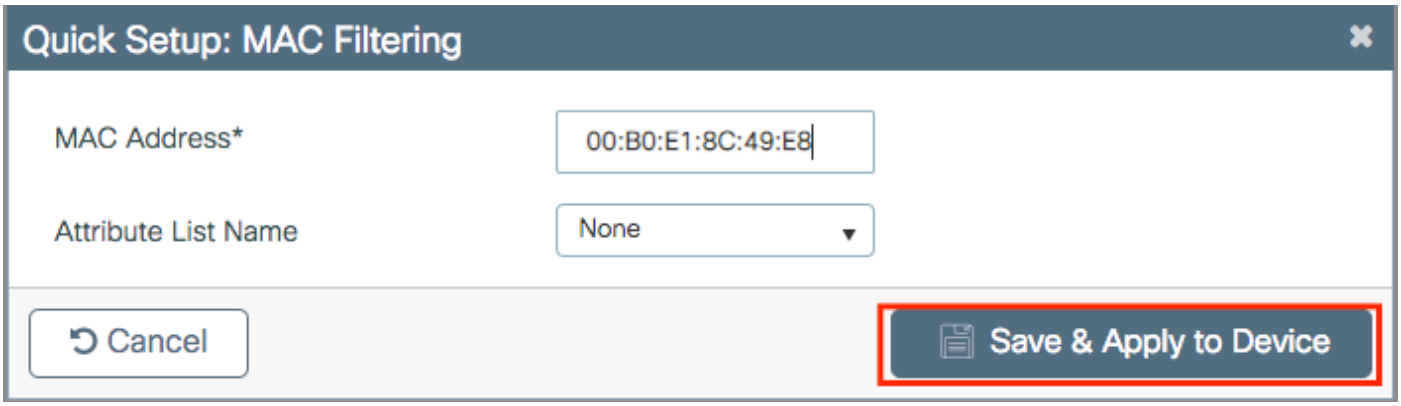
Vaya a Configuration > Security > AAA > AAA Advanced > AP Policy . Habilite Authorize APs contra MAC y seleccione la Lista de Métodos de Autorización creada en el Paso 1.



Paso 3. Agregue la dirección MAC de Ethernet del AP.

Vaya a Configuration > Security > AAA > AAA Advanced > Device Authentication > MAC Address > + Add





Nota: La dirección MAC Ethernet del punto de acceso debe tener uno de estos formatos cuando se introduce en la interfaz de usuario web(xx:xx:xx:xx:xx (o) xxxx.xxxx.xxxx (o) xx-xx-xx-xx-xx-xx) en la versión 16.12. En la versión 17.3, deben estar en el formato xxxxxxxxxxxx sin ningún separador. El formato CLI siempre es xxxxxxxxxxxx en cualquier versión (en 16.12, la interfaz de usuario web elimina los separadores de la configuración). El ID de bug de Cisco CSCvv43870 permite el uso de cualquier formato en CLI o interfaz de usuario web en versiones posteriores.

CLI:

```
# config t
# aaa new-model
# aaa authorization credential-download <AP-auth> local

# ap auth-list authorize-mac
# ap auth-list method-list <AP-auth>

# username <aaaabbbbcccc> mac
```

Lista de autorización de MAC AP: servidor RADIUS externo

Configuración de 9800 WLC

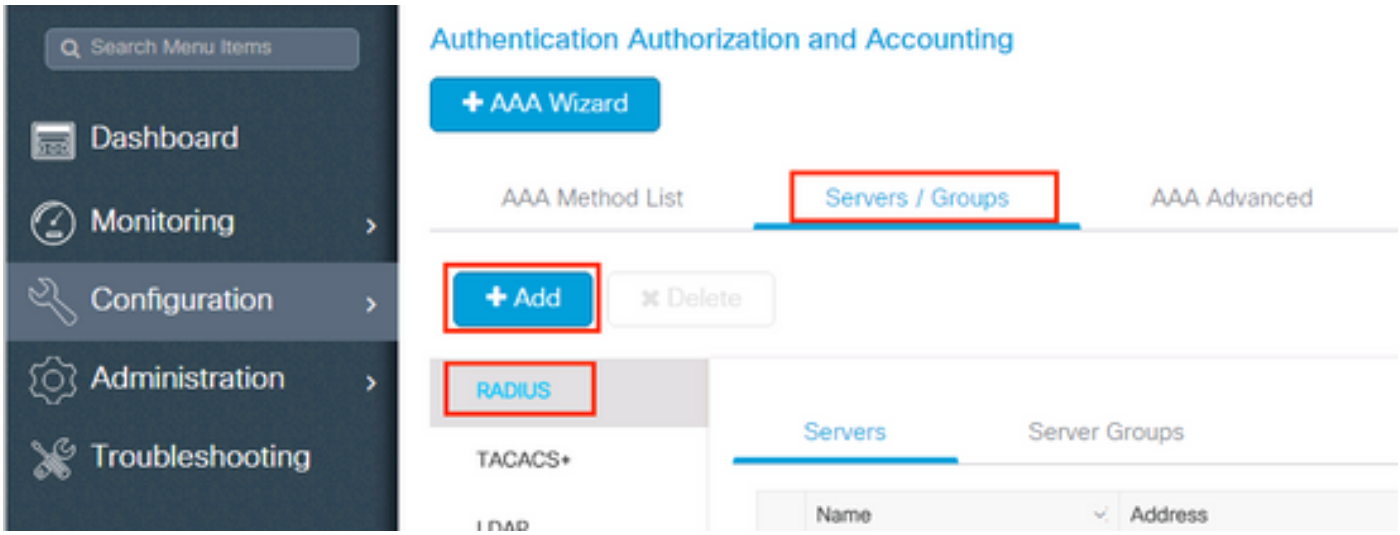
La dirección MAC de los AP autorizados se almacena en un servidor RADIUS externo, en este ejemplo ISE.

En ISE, puede registrar la dirección MAC de los puntos de acceso como nombres de usuario/contraseña o como terminales. A lo largo de los pasos se le indica cómo seleccionar utilizar una forma u otra.

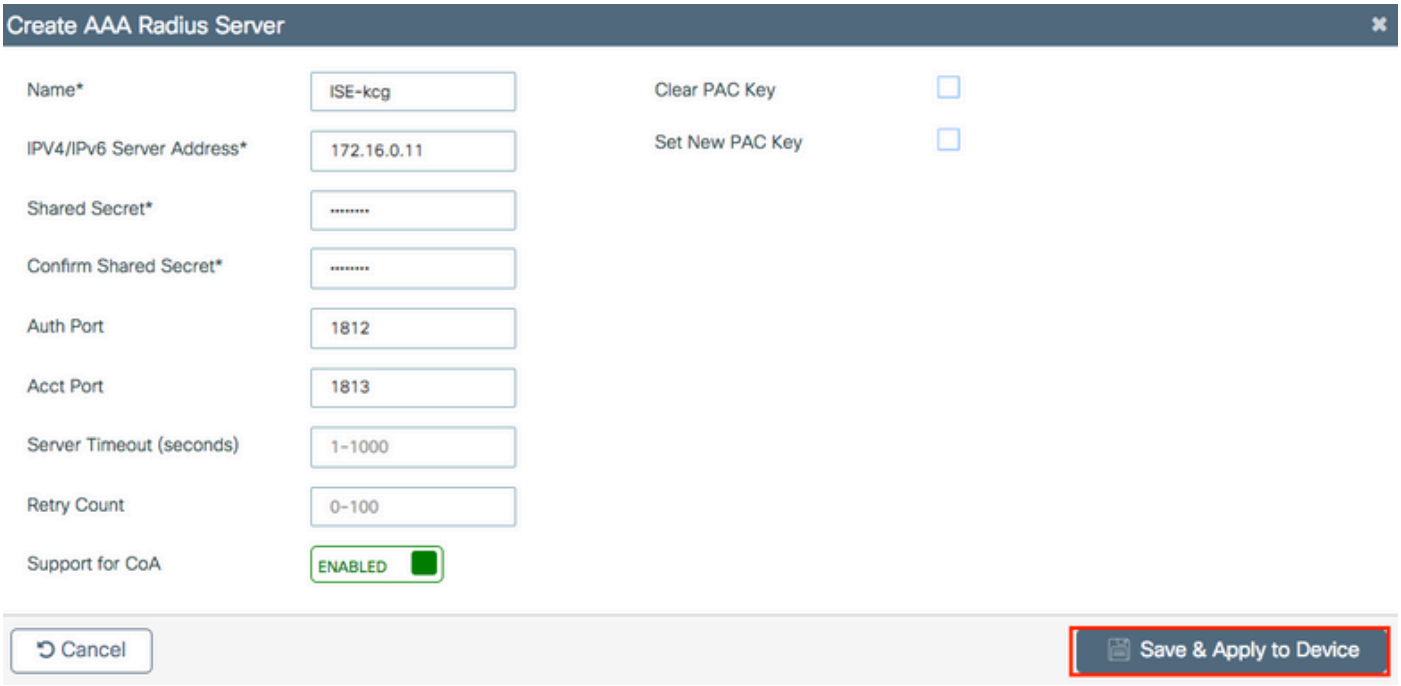
GUI:

Paso 1. Declarar servidor RADIUS

Navegue hasta Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add e ingrese la información del servidor RADIUS.



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.

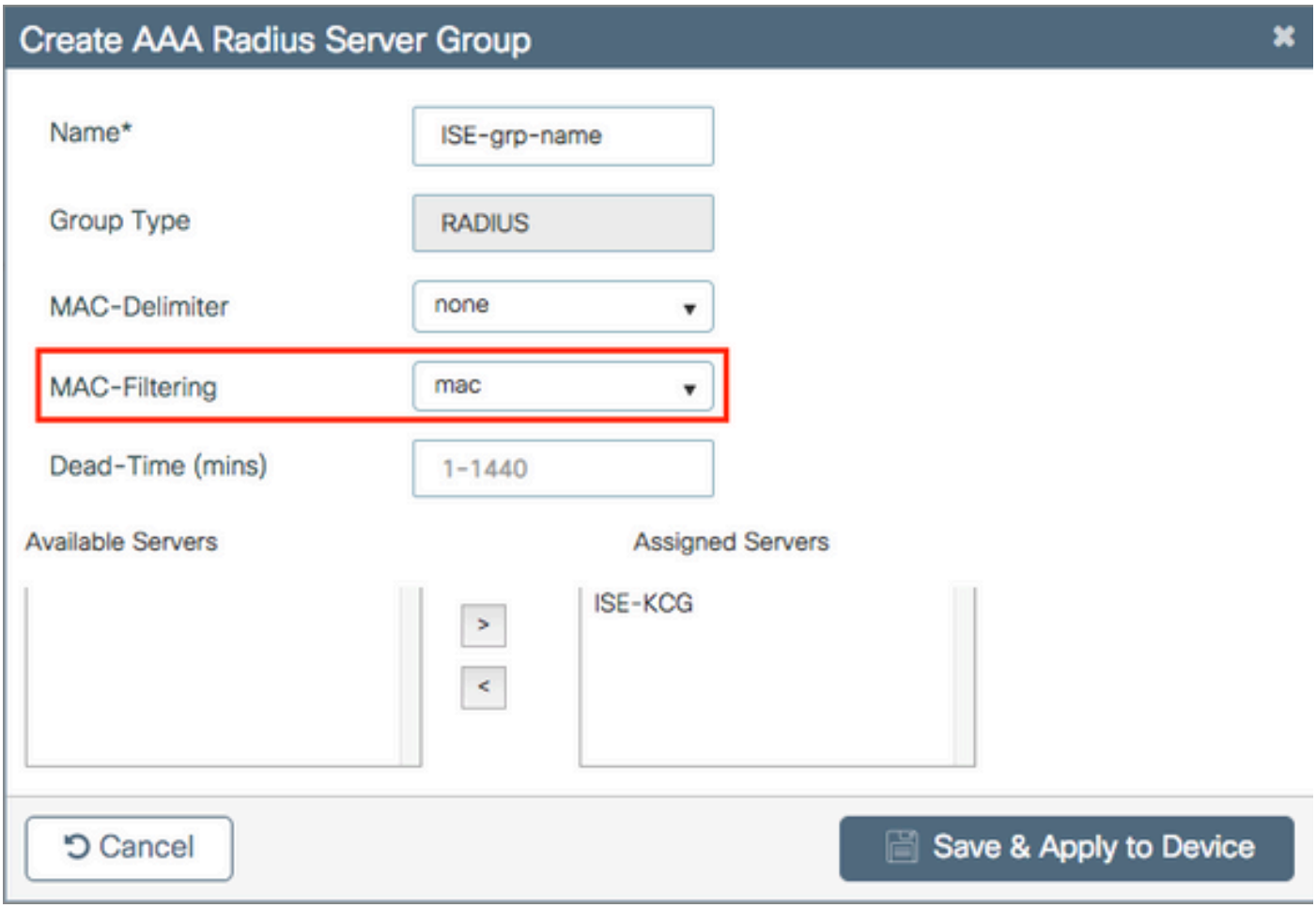


Paso 2. Agregar el servidor RADIUS a un grupo RADIUS

Vaya a Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add

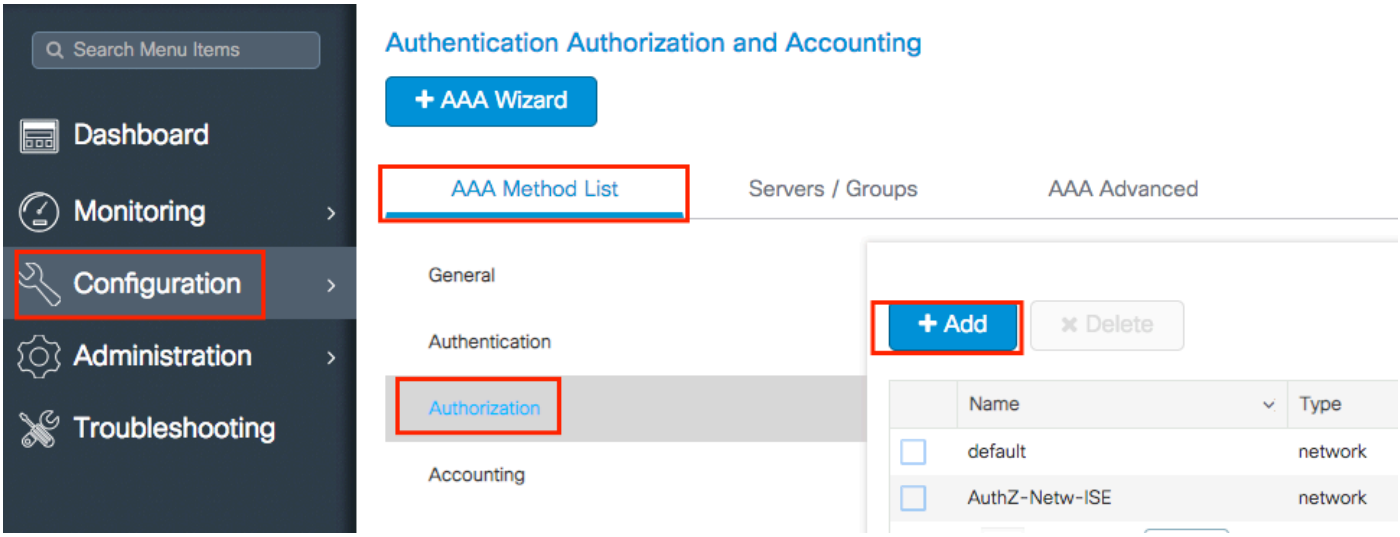
Para que ISE autentique la dirección MAC del punto de acceso cuando los nombres de usuario dejen el filtrado de direcciones MAC como ninguno.

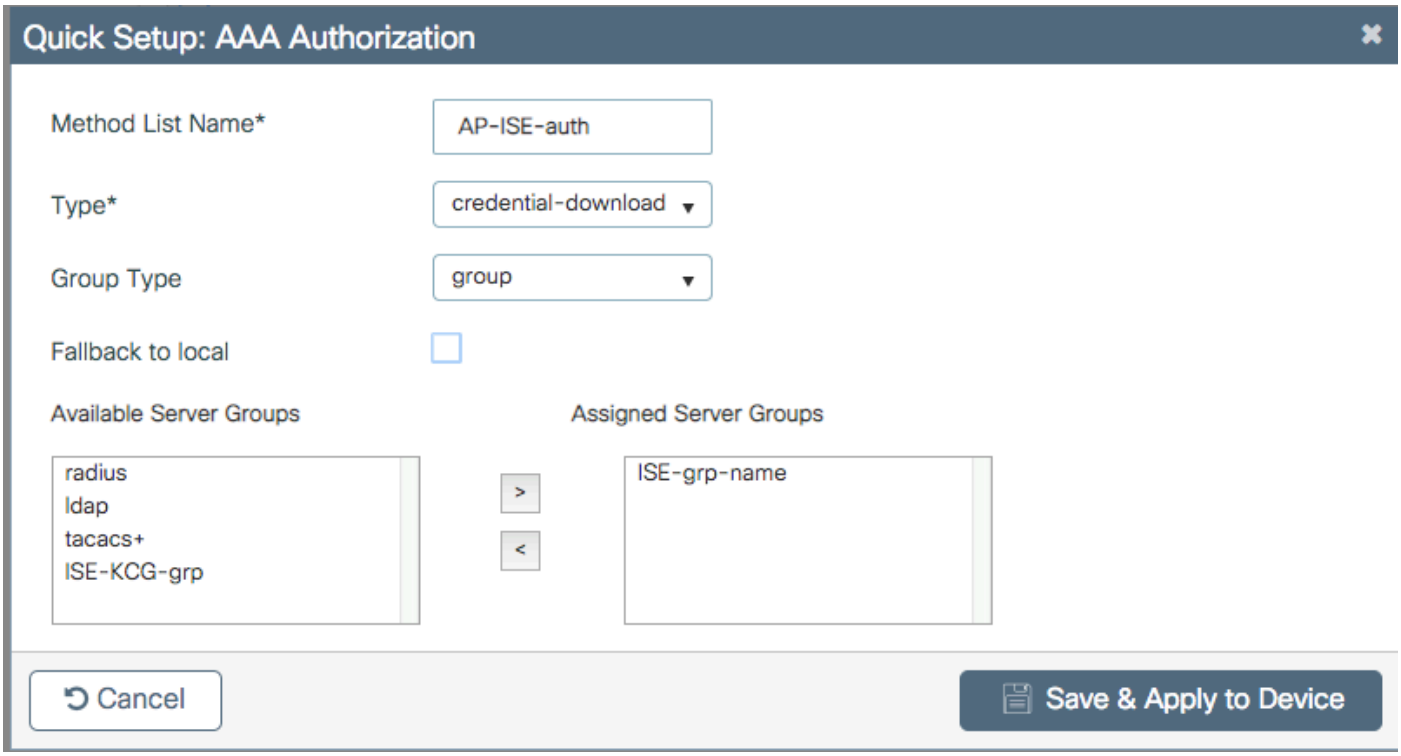
Para que ISE autentique la dirección MAC del punto de acceso cuando los terminales cambien el filtrado de MAC a MAC.



Paso 3. Cree una lista de métodos de descarga de credenciales de autorización.

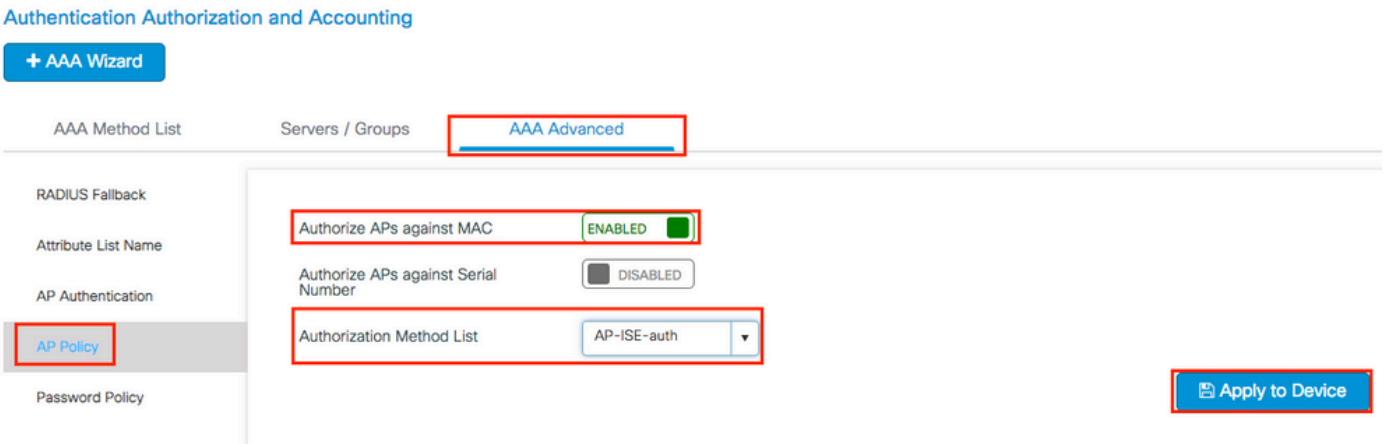
Vaya a Configuration > Security > AAA > AAA Method List > Authorization > + Add





Paso 4. Habilite la autorización MAC de AP.

Vaya a Configuration > Security > AAA > AAA Advanced > AP Policy . Habilite Authorize APs contra MAC y seleccione la Lista de Métodos de Autorización creada en el Paso 3.



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 credential-download <AP-auth> group <radius-grp-name>
# ap auth-list authorize-mac
# ap auth-list method-list <AP-ISE-auth>
```

Configuración de ISE

Paso 1. Para agregar 9800 WLC a ISE:

Declarar 9800 WLC en ISE

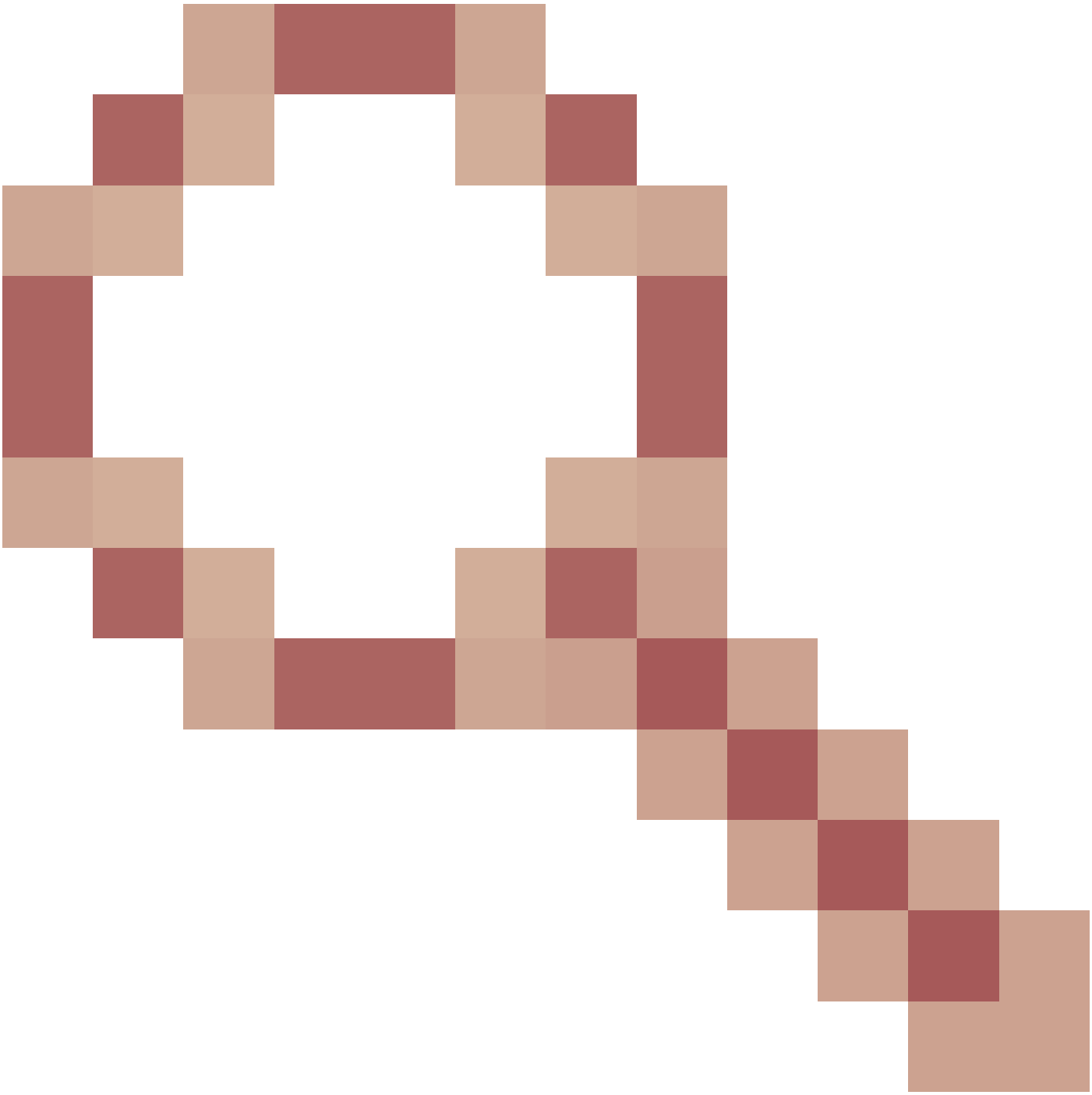
Elija configurar en función de la autenticación la dirección MAC de los AP con los pasos requeridos:

Configure USE para autenticar la dirección MAC como terminales

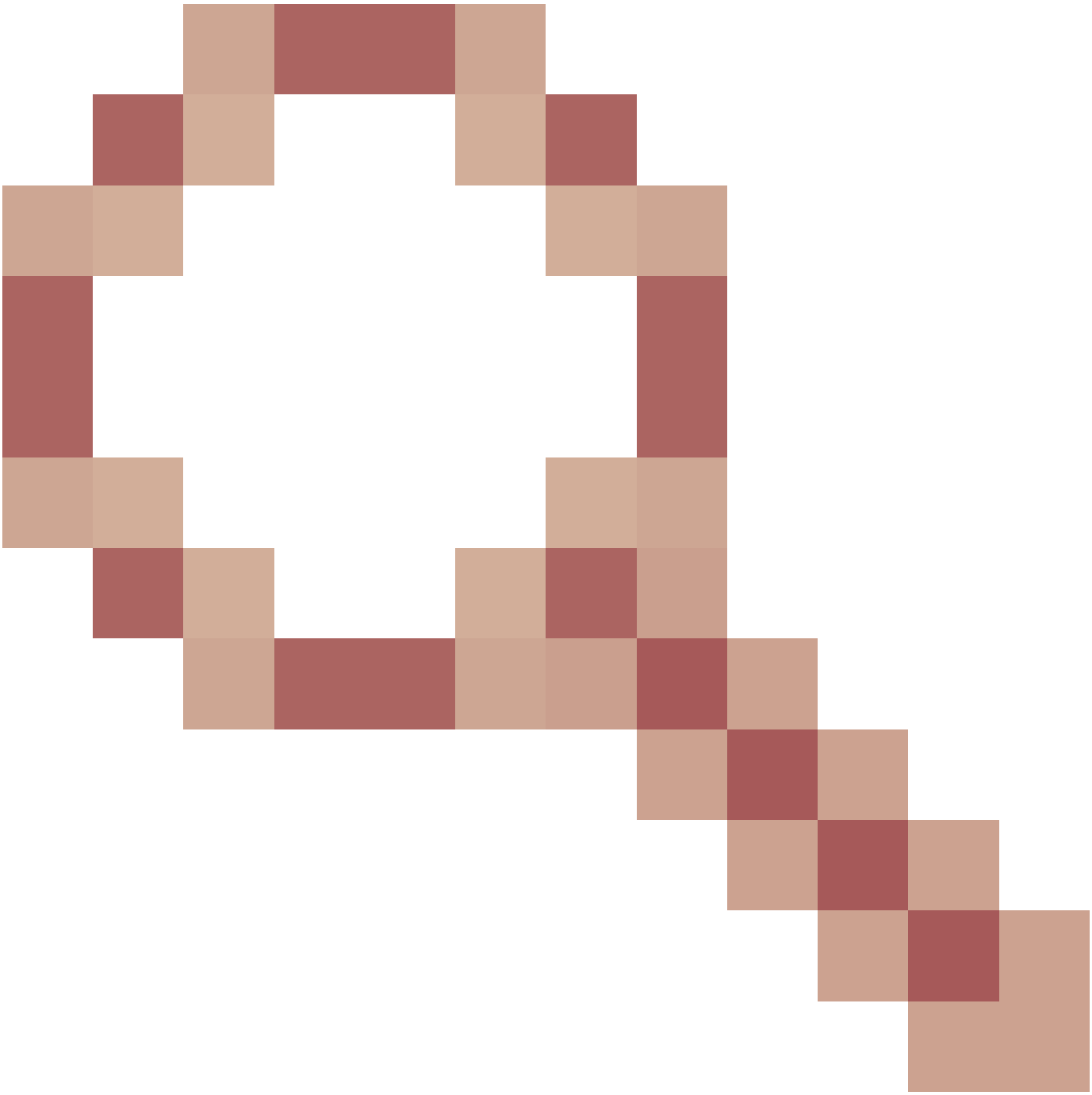
Configuración de ISE para autenticar la dirección MAC como nombre de usuario/contraseña

Configuración de ISE para autenticar la dirección MAC como terminales

Paso 2. (Opcional) Crear un grupo de identidad para puntos de acceso

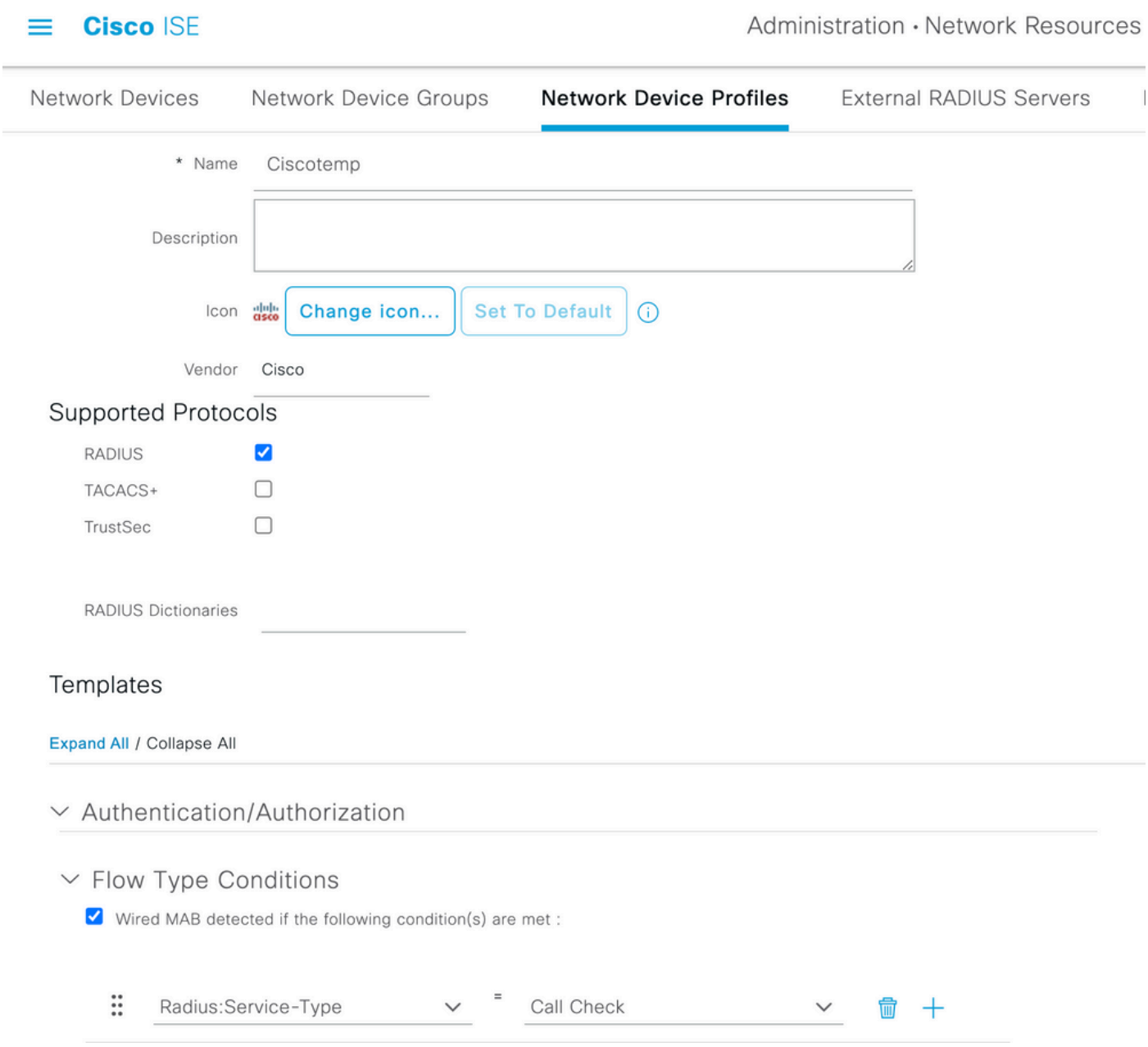


Debido a que el 9800 no envía el atributo NAS-port-Type con autorización de AP Cisco bug IDCSCvy74904



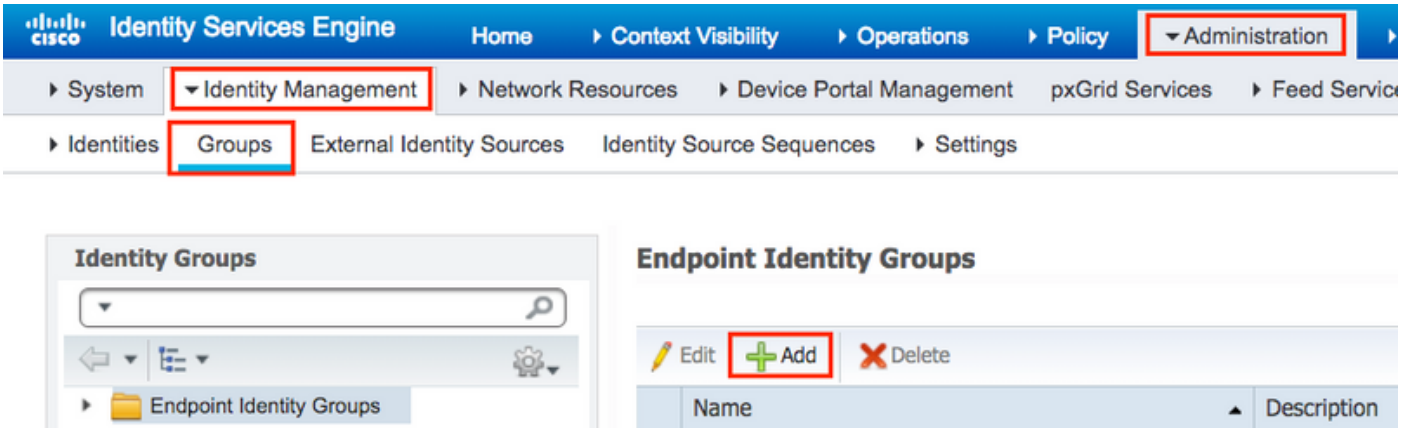
), ISE no reconoce una autorización de AP como un flujo de trabajo MAB y, por lo tanto, no es posible autenticar un AP si la dirección MAC del AP se coloca en la lista de terminales a menos que modifique los flujos de trabajo MAB para no requerir el atributo NAS-PORT-type en ISE.

Vaya a Administrator > Network device profile y cree un nuevo perfil de dispositivo. Active RADIUS y agregue service-type=call-check para el MAB con cables. Puede copiar el resto del perfil original de Cisco, la idea es no tener ninguna condición "nas-port-type" para el MAB cableado.

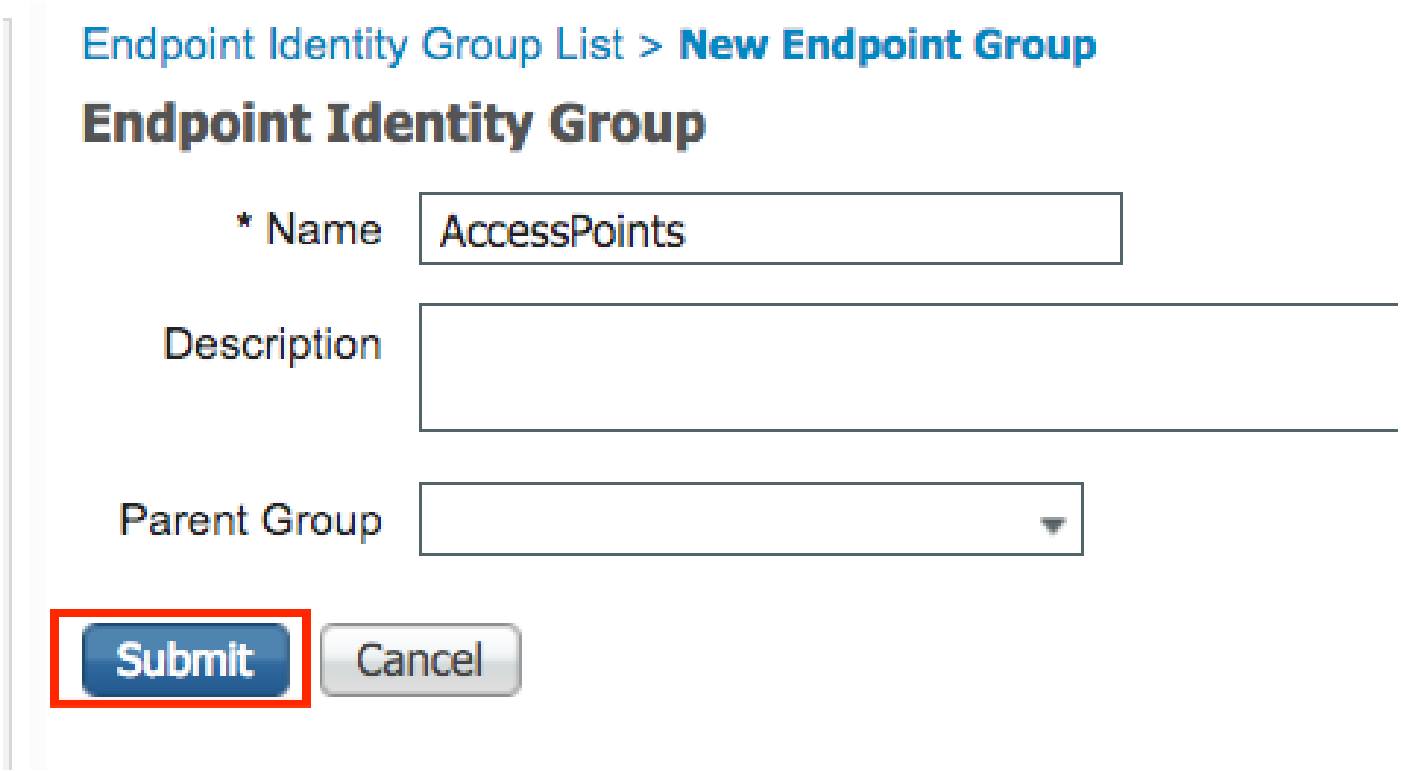


Vuelva a la entrada del dispositivo de red para el 9800 y establezca su perfil en el perfil del dispositivo recién creado.

Vaya a Administration > Identity Management > Groups > Endpoint Identity Groups > + Add.

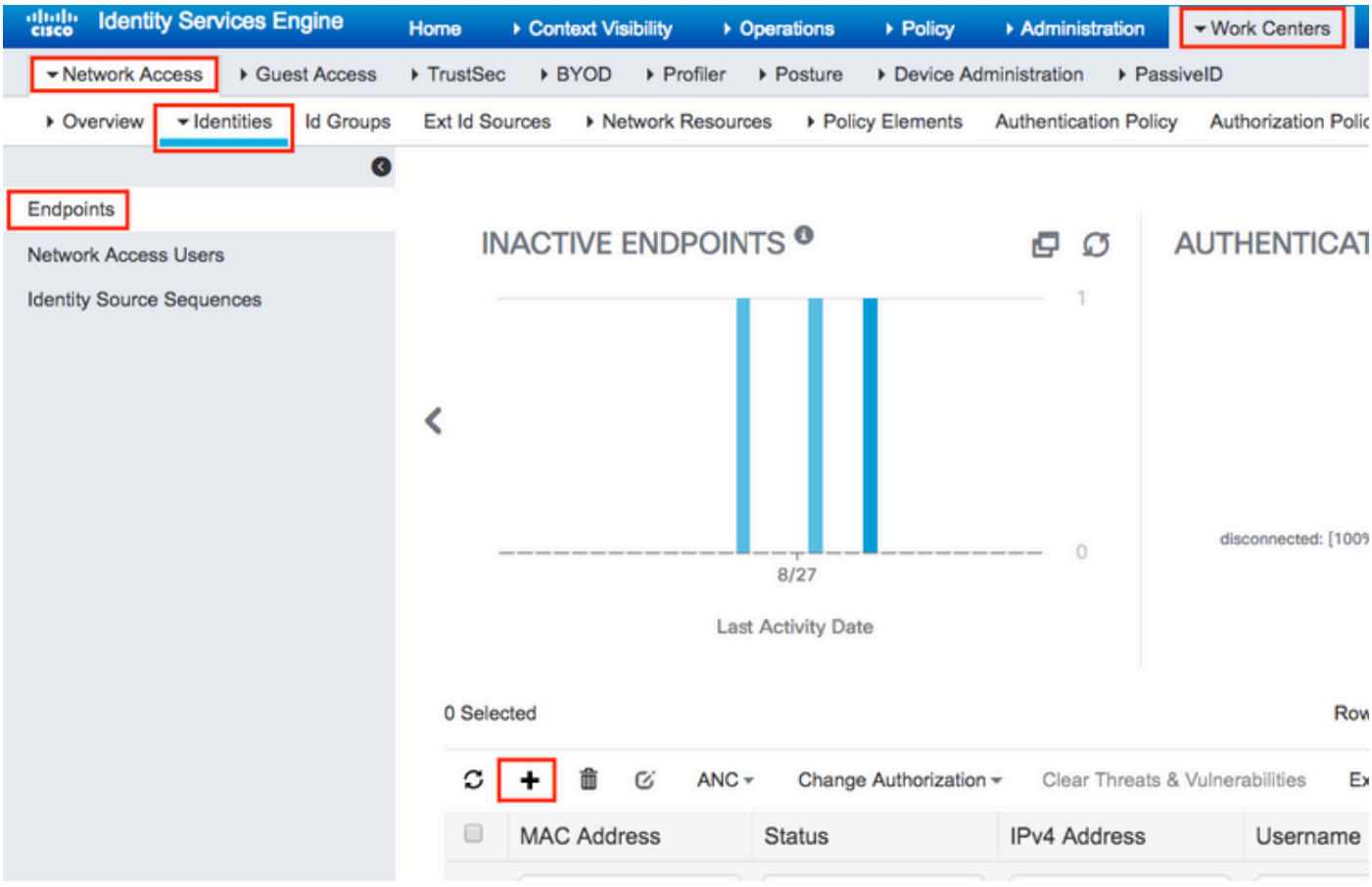


Elija un nombre y haga clic en Enviar.

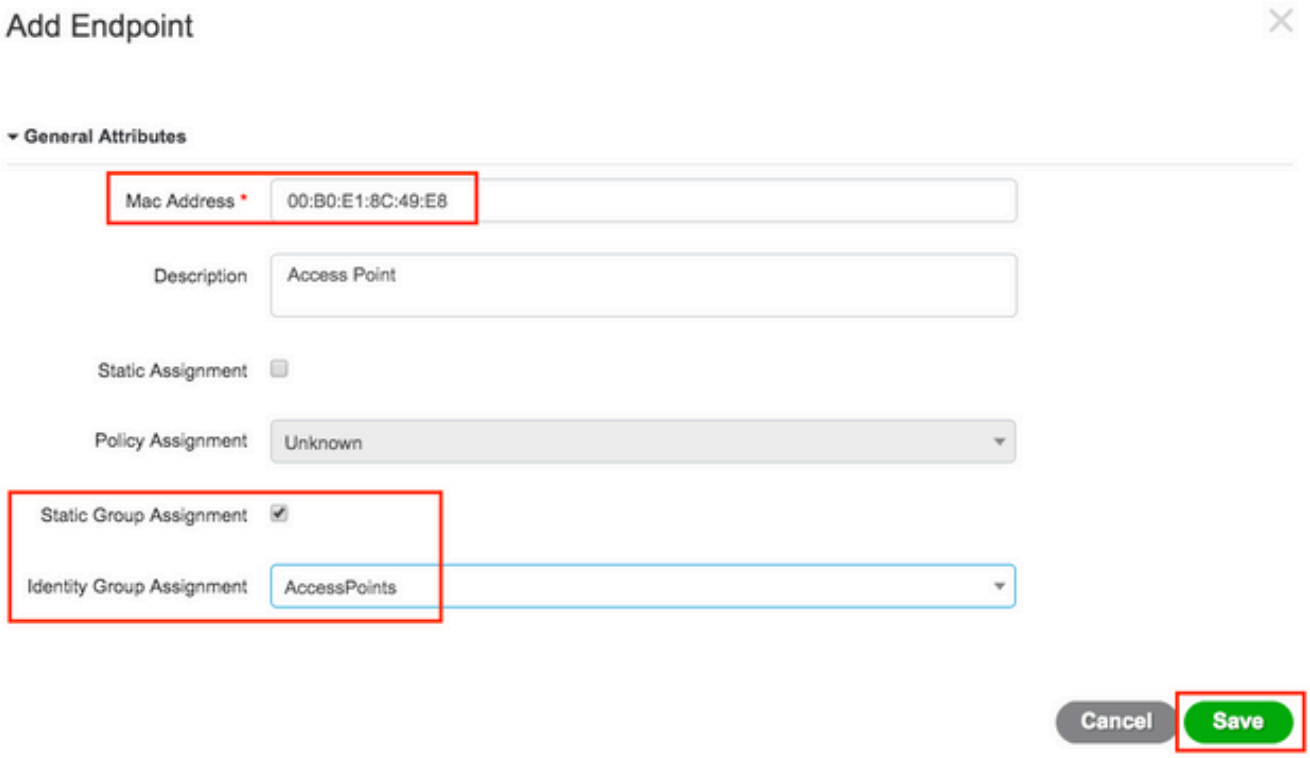


Paso 3. Agregue la dirección MAC de Ethernet AP a su grupo de identidad de terminal.

Vaya a Centros de trabajo > Acceso a la red > Identidades > Terminales > +

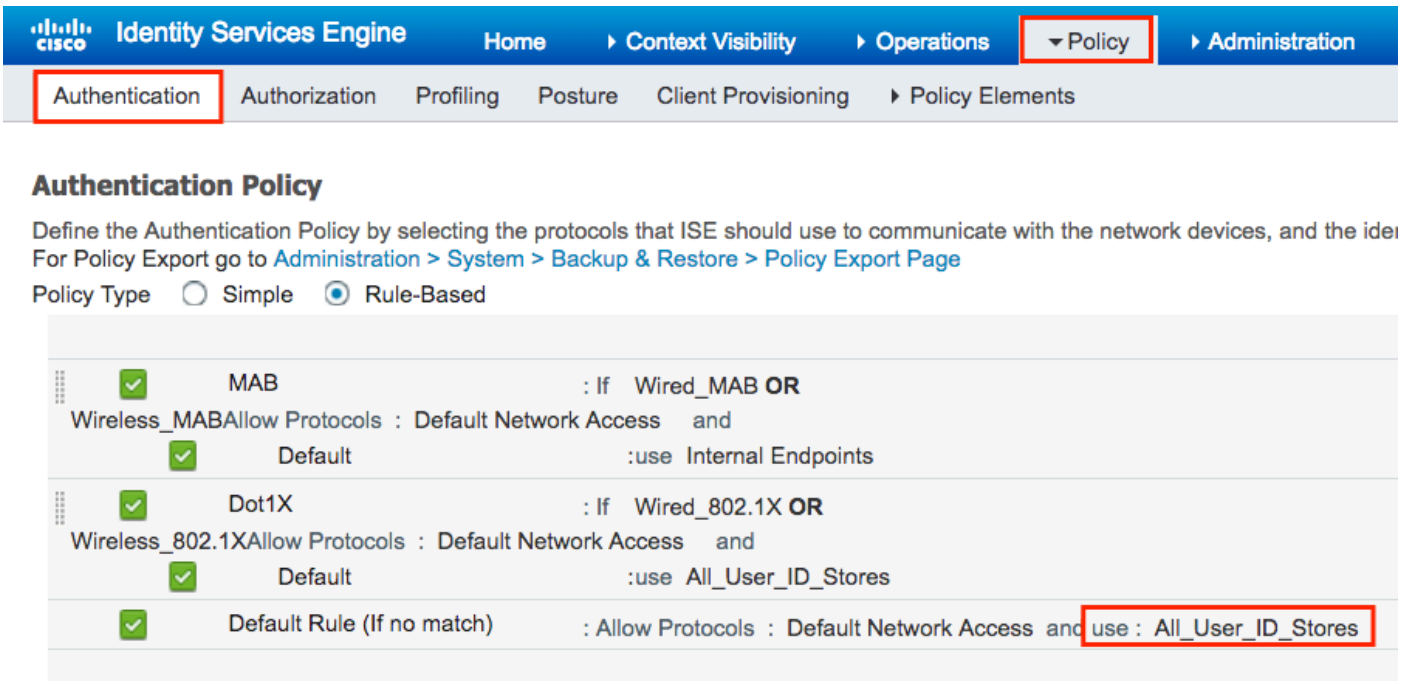


Introduzca la información necesaria.

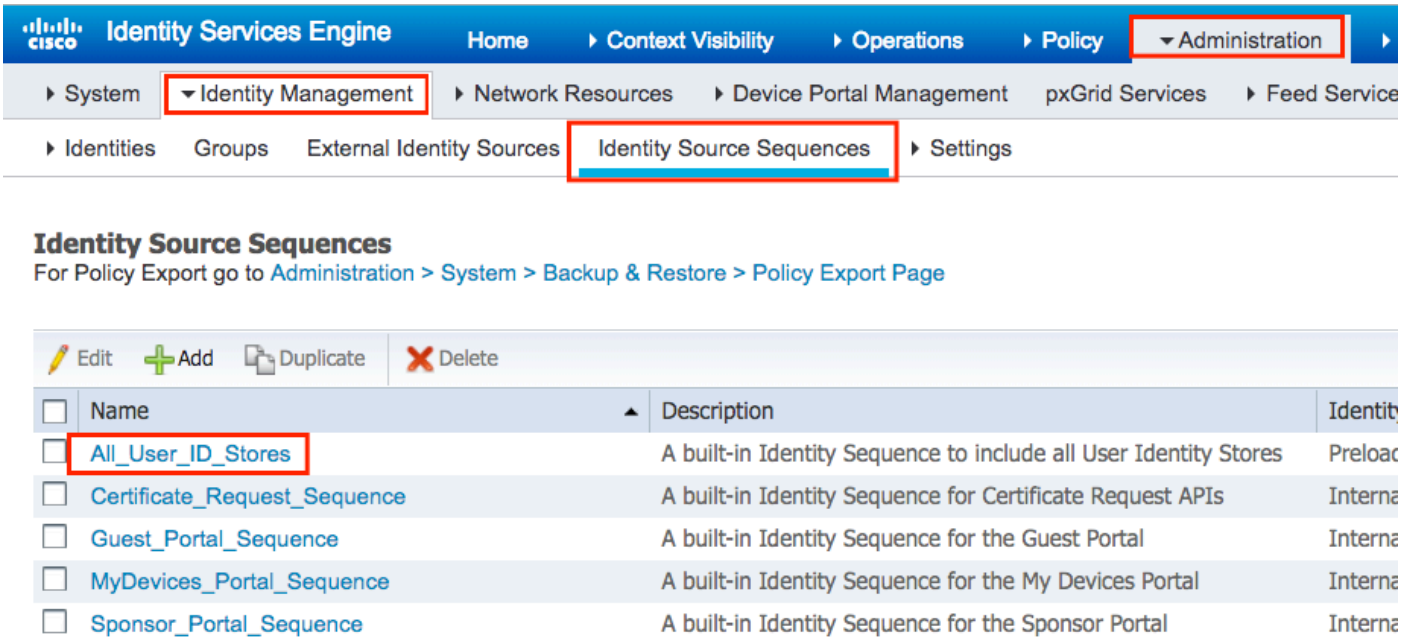


Paso 4. Compruebe que el almacén de identidades utilizado en la regla de autenticación predeterminada contenga los extremos internos.

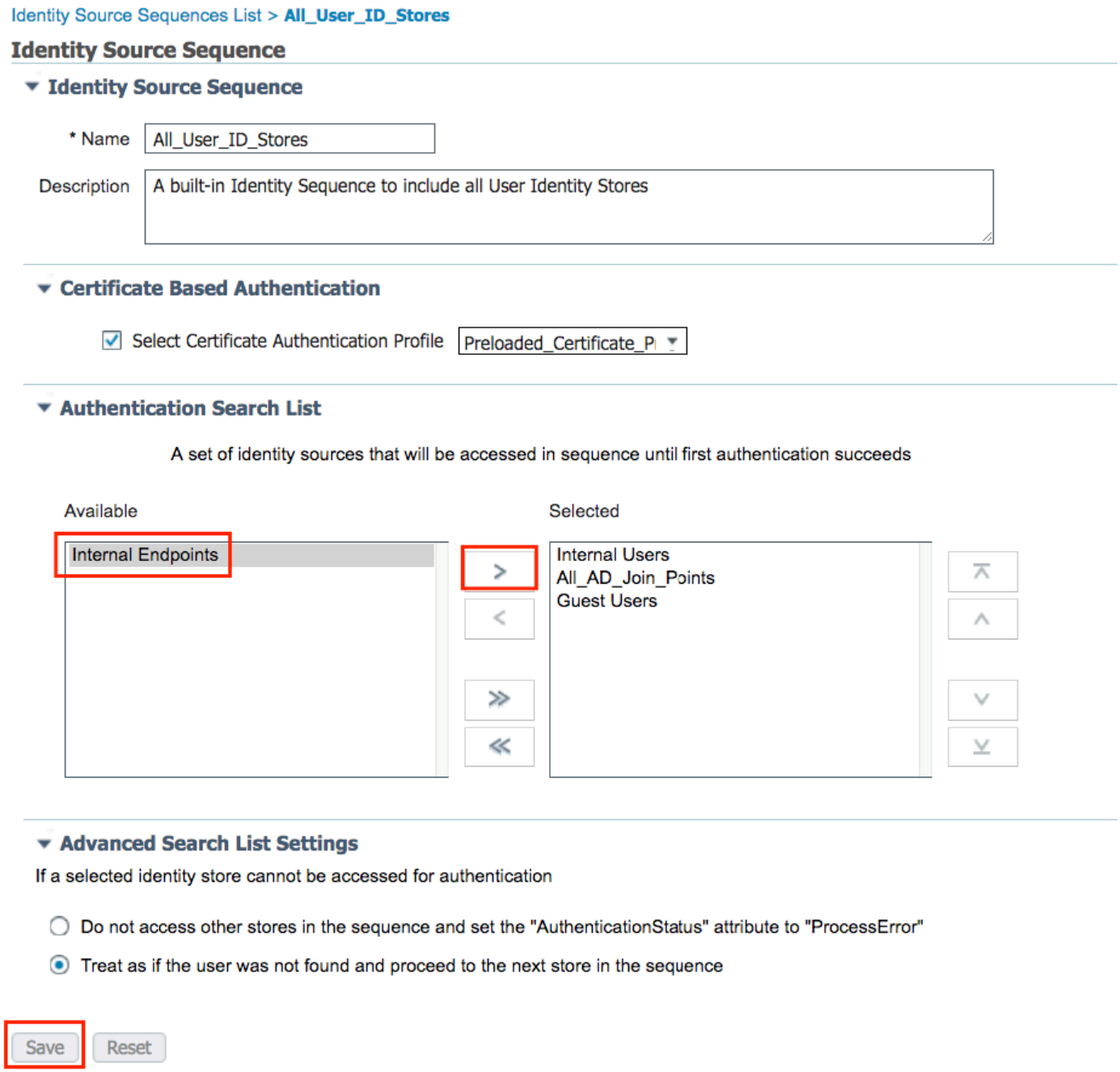
A. Navegue hasta Policy > Authentication y tome nota del almacén de identidad.



B. Vaya a Administración > Gestión de Identidad > Secuencias de Origen de Identidad > Nombre de Identidad.



C. Asegúrese de que los terminales internos le pertenezcan; si no es así, agréguelo.



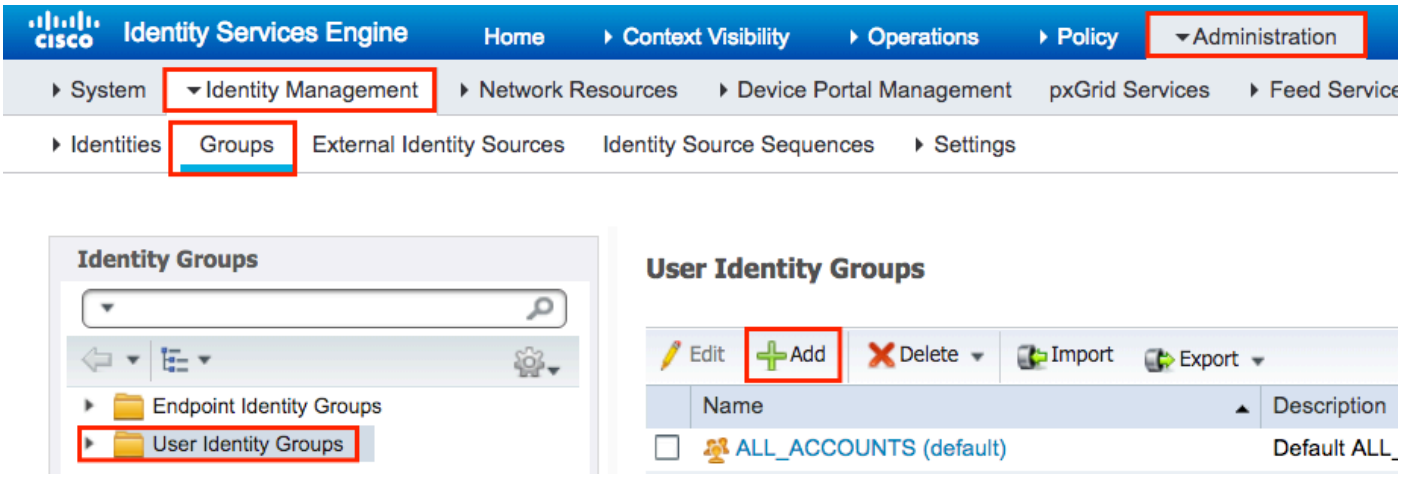
Configuración de ISE para autenticar la dirección MAC como nombre de usuario/contraseña

No se recomienda este método, ya que requiere políticas de contraseña más bajas para permitir la misma contraseña que el nombre de usuario.

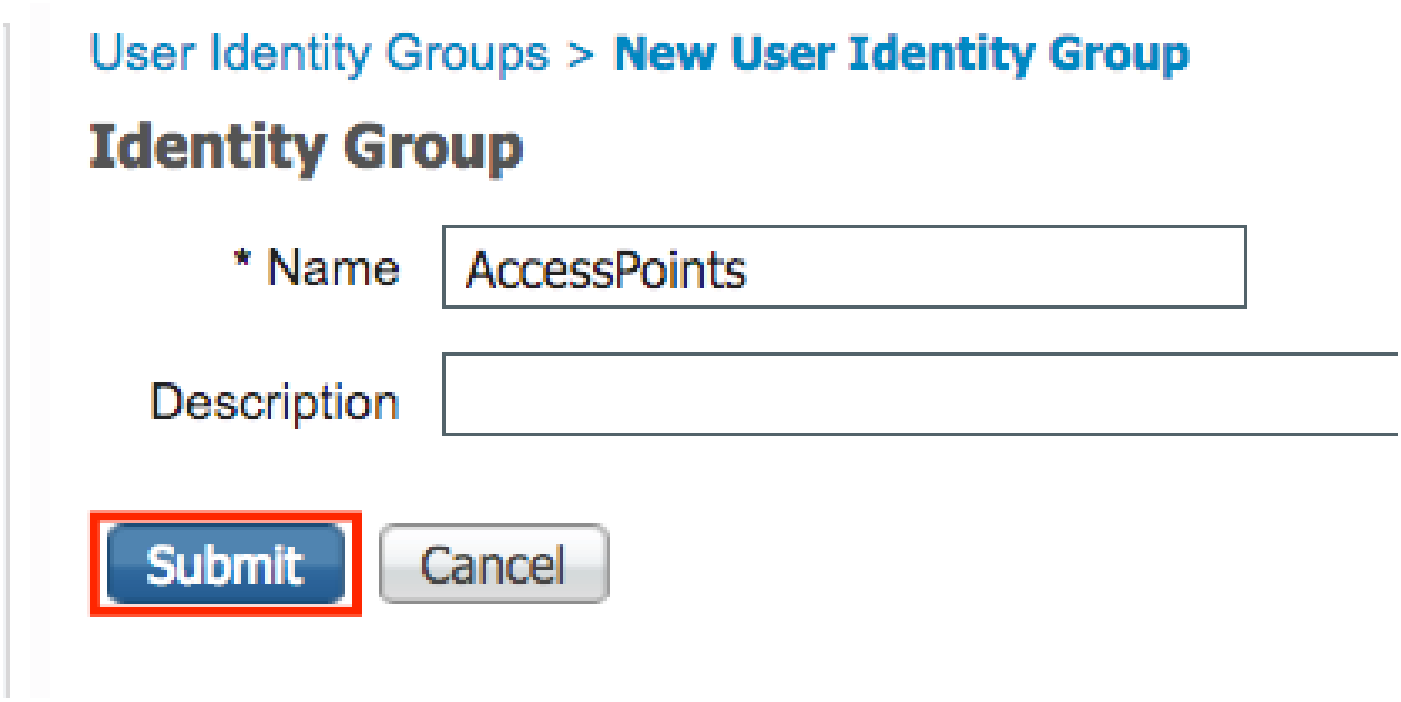
Sin embargo, puede ser una solución alternativa en caso de que no pueda modificar su perfil de dispositivo de red

Paso 2. (Opcional) Crear un grupo de identidad para puntos de acceso

Vaya a Administration > Identity Management > Groups > User Identity Groups > + Add.

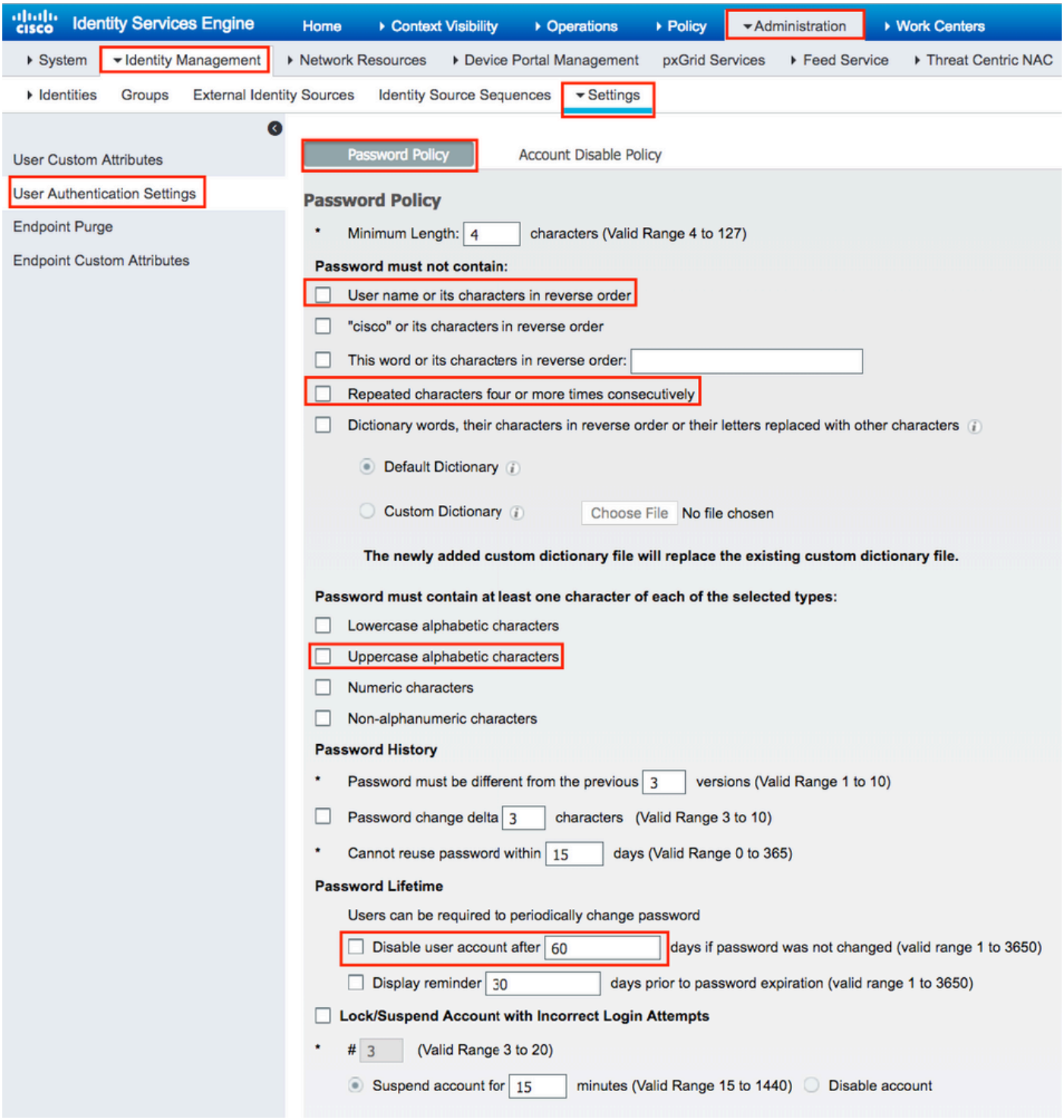


Elija un nombre y haga clic en Enviar.



Paso 3. Compruebe que la directiva de contraseñas actual le permite agregar una dirección MAC como nombre de usuario y contraseña.

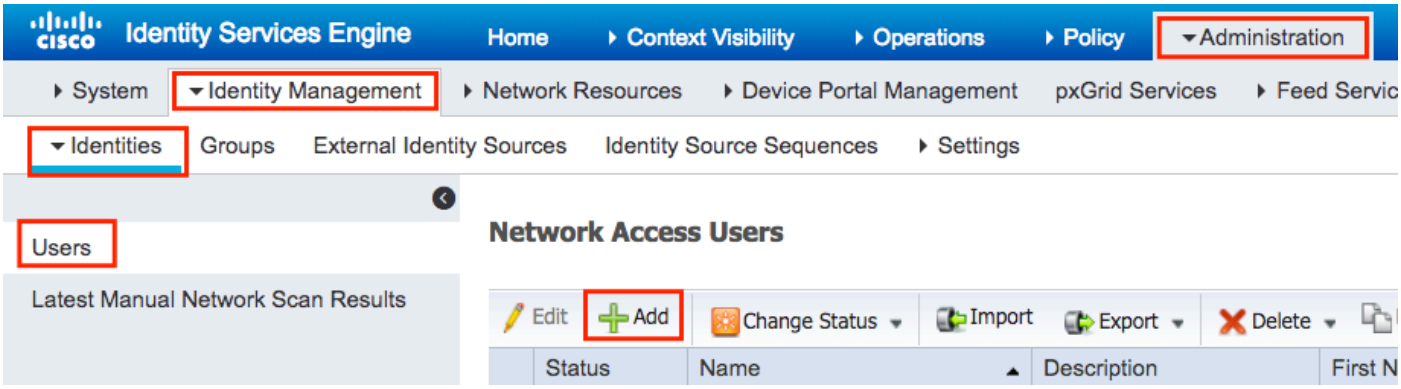
Vaya a Administration > Identity Management > Settings > User Authentication Settings > Password Policy y asegúrese de que al menos estas opciones estén inhabilitadas:



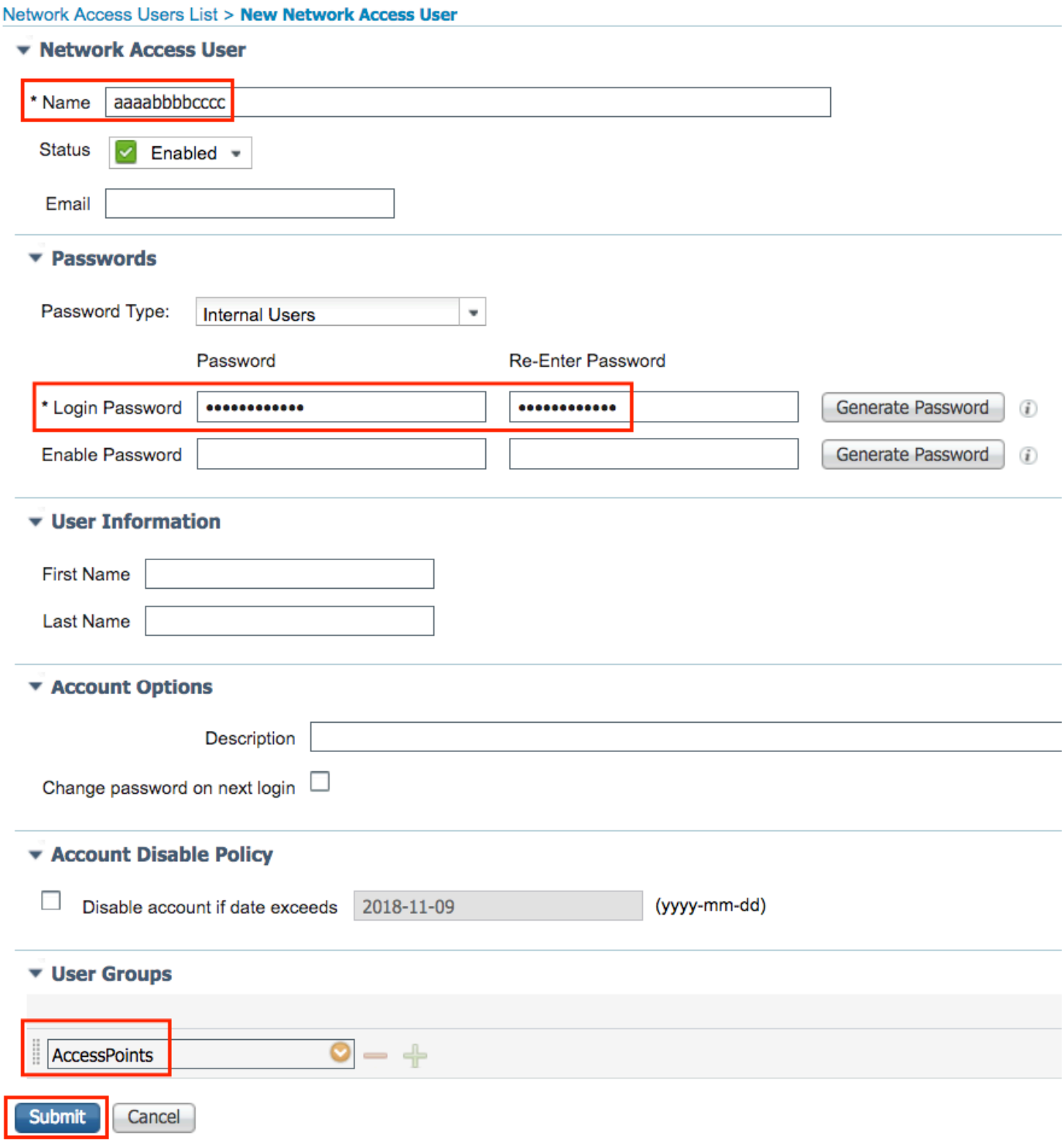
Nota: También puede deshabilitar la opción Deshabilitar la cuenta de usuario después de XX días si la contraseña no se cambió.Como se trata de una dirección MAC, la contraseña nunca cambia.

Paso 4. Agregue la dirección MAC de Ethernet del AP.

Vaya a Administration > Identity Management > Identities > Users > + Add .



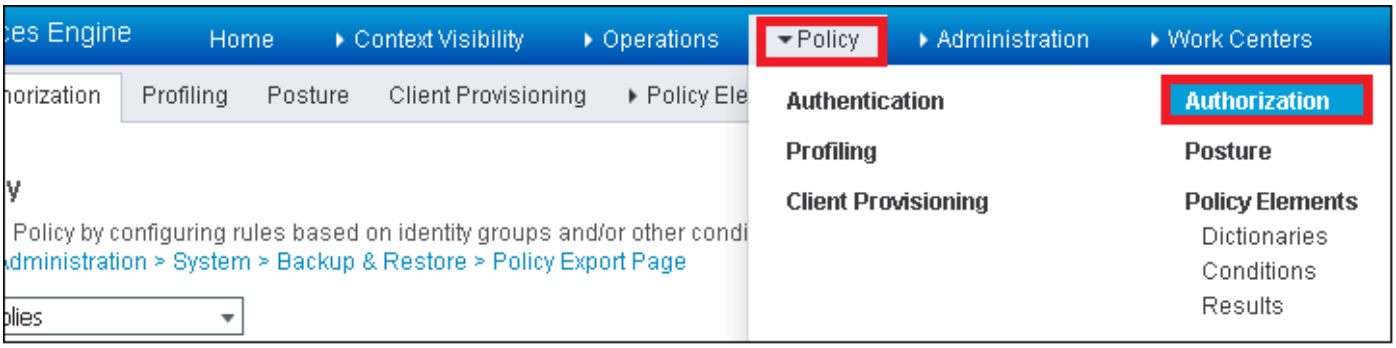
Introduzca la información necesaria.



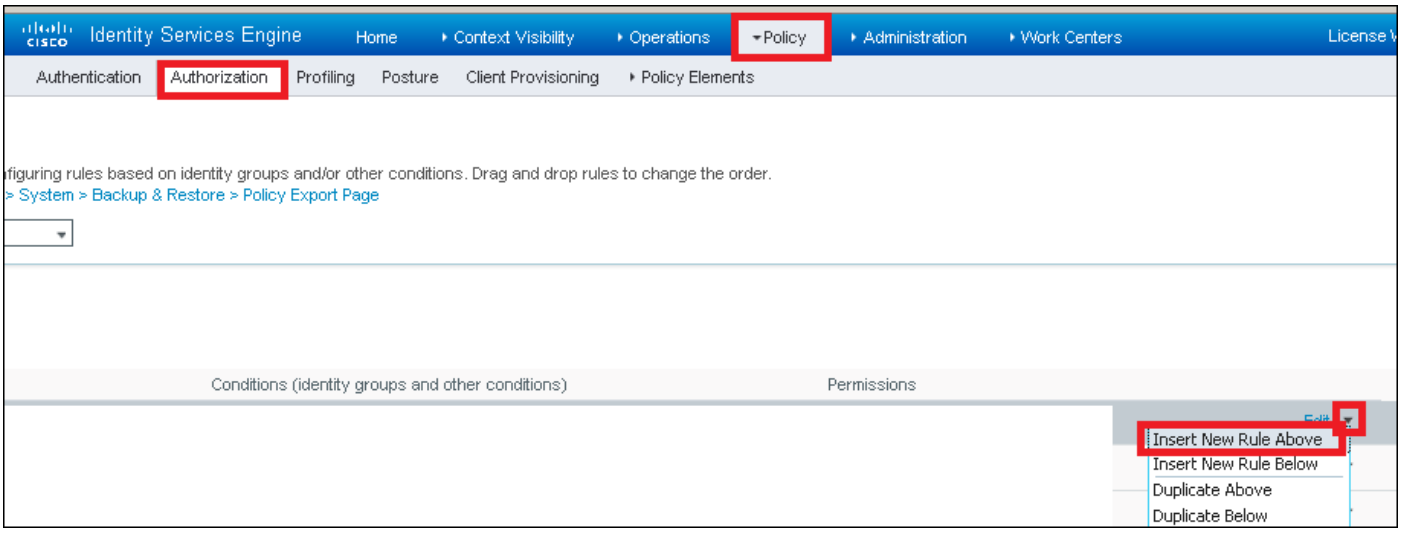
Nota: El campo Name y Login Password debe ser la dirección MAC de Ethernet del AP, todas en minúsculas y sin separadores.

Política de autorización para autenticar AP

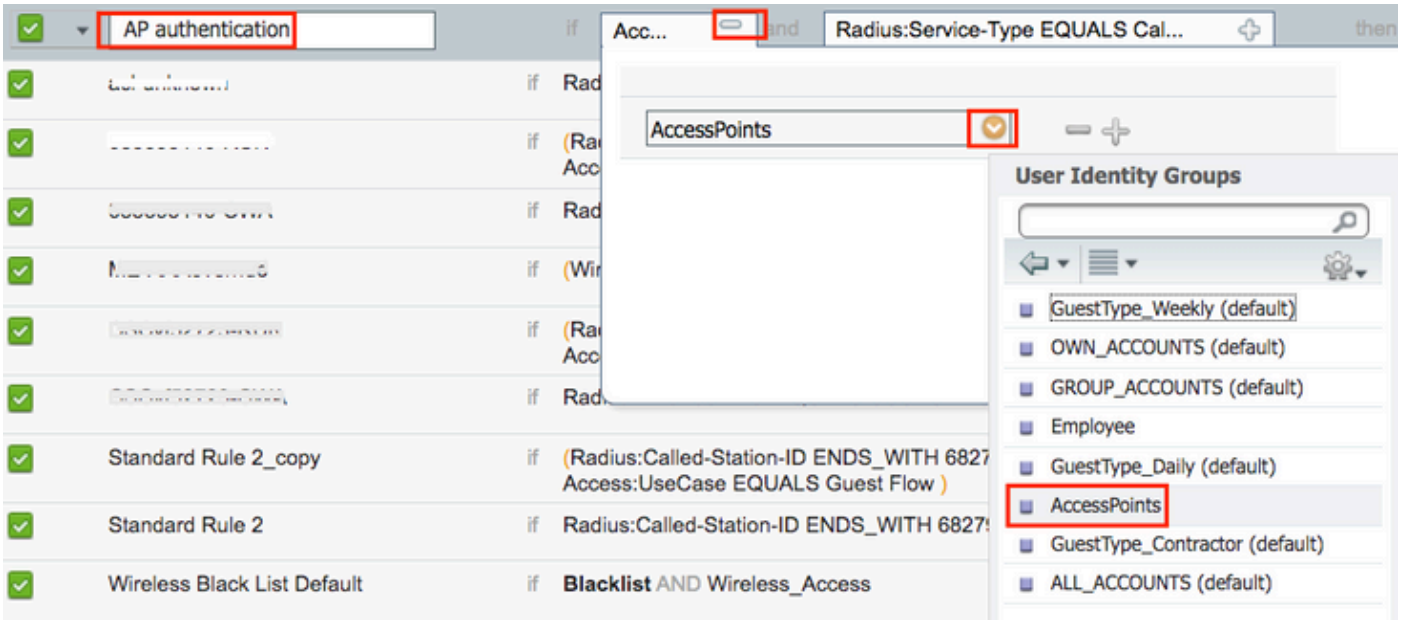
Vaya a Policy > Authorization como se muestra en la imagen.



Inserte una nueva regla como se muestra en la imagen.

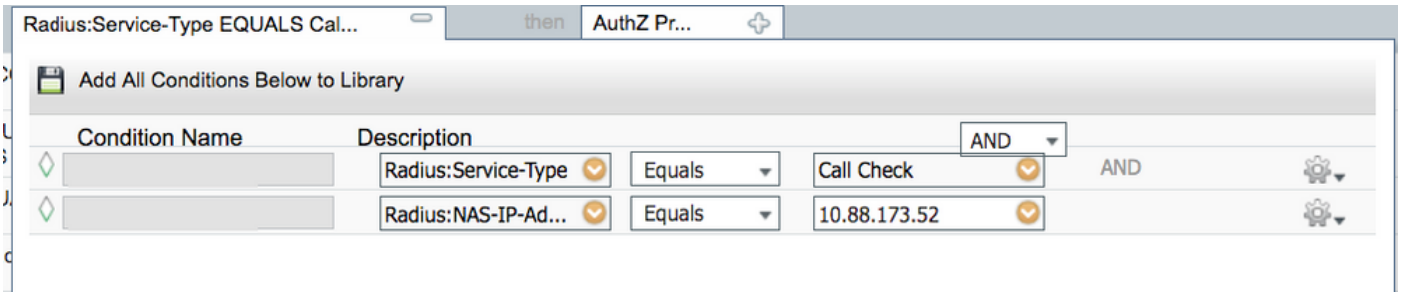


En primer lugar, seleccione un nombre para la regla y el grupo de identidad donde se almacena el punto de acceso (AccessPoints). Seleccione User Identity Groups si decidió autenticar la dirección MAC como nombre de usuario y contraseña o Endpoint Identity Groups si elige autenticar la dirección MAC de AP como extremos.

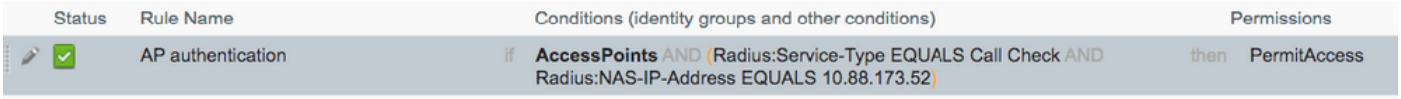


A continuación, seleccione otras condiciones que realizan el proceso de autorización para que se ajusten a esta regla. En este ejemplo, el proceso de autorización llega a esta regla si utiliza la

Verificación de llamada de tipo de servicio y la solicitud de autenticación proviene de la dirección IP 10.88.173.52.



Finalmente, seleccione el perfil de autorización que se asigna a los clientes que alcanzaron esa regla, haga clic enFinalizado y guárdelo como se muestra en la imagen.



Nota: Los AP que ya se unieron en el controlador no pierden su asociación. Sin embargo, si después de habilitar la lista de autorización, pierden la comunicación con el controlador e intentan volver a unirse, pasan por el proceso de autenticación. Si sus direcciones MAC no están listadas localmente o en el servidor RADIUS, no podrán unirse de nuevo al controlador.

Verificación

Verifique si el WLC 9800 ha habilitado la lista de autenticación de AP

<#root>

```
# show ap auth-list
```

```
Authorize APs against MAC : Disabled
Authorize APs against Serial Num : Enabled
Authorization Method List : <auth-list-name>
```

Verificar configuración de RADIUS:

<#root>

```
#
show run aaa
```

Troubleshoot

El WLC 9800 proporciona capacidades de seguimiento SIEMPRE ACTIVO. Esto garantiza que todos los mensajes de nivel de advertencia, advertencia y errores relacionados con la unión de AP se registren constantemente y que pueda ver los registros de una condición de incidente o falla después de que haya ocurrido.

Nota: El volumen de registros generados varía de unas horas a varios días.

Para ver los seguimientos que el WLC 9800 recolectó por defecto, puede conectarse vía SSH/Telnet al WLC 9800 a través de 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.

```
# 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 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 Trace 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 depura activamente.

Paso 4. Suponga que la dirección MAC en la prueba no aparece como una condición en el Paso 3, recopile los seguimientos del nivel de aviso siempre activo para la dirección MAC de radio 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).

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

```
# clear platform condition all
```

Paso 6. Habilite la condición de depuración para la dirección MAC del cliente inalámbrico que desea monitorear.

Estos comandos comienzan a monitorear la dirección MAC proporcionada durante 30 minutos (1800 segundos). Opcionalmente, puede aumentar este tiempo hasta 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<aaaa.bbbb.cccc> por dirección MAC.

Nota: No verá el resultado de la actividad del cliente en la sesión del terminal, ya que todo se almacena internamente para verlo más adelante.

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 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

```
# 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 examinamos con más detalle 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. 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 troubleshooting.

Referencias

Incorporación de puntos de acceso de malla al WLC 9800

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).