Configuración de la Autenticación Web Central con Anclaje en Catalyst 9800

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Configure un Catalyst 9800 anclado a otro Catalyst 9800
Diagrama de la red
Configuración de AAA en ambos 9800
Configure las WLAN en los WLC
Cree el perfil de política y la etiqueta de política en el WLC externo
Cree el perfil de política en el WLC de anclaje
Redirigir configuración de ACL en ambos 9800
Configuración de ISE
Configure un Catalyst 9800 anclado a un WLC AireOS
Configuración externa de Catalyst 9800
Configuraciones AAA en el WLC AireOS de anclaje
Configuración WLAN en el WLC AireOS
Redirigir ACL en el WLC AireOS
Configuración de ISE
Diferencias en la configuración cuando el WLC de AireOS es el externo y el Catalyst 9800 es el ancla
Verificación
Troubleshoot
Información de Troubleshooting de Catalyst 9800
Detalles del cliente
Captura de paquetes integrada
Rastreo de RadioActive
Información de resolución de problemas de AireOS
Detalles del cliente
Depuraciones desde la CLI
Referencias

Introducción

Este documento describe cómo configurar y resolver problemas de autenticación web central (CWA) en el Catalyst 9800 que apunta a otro controlador de LAN inalámbrica (WLC) como ancla de movilidad, que abarca el destino con AireOS u otro WLC 9800.

Prerequisites

Requirements

Se recomienda que tenga una comprensión básica del WLC 9800, AireOS WLC y Cisco ISE. Se asume que antes de iniciar la configuración de anclaje de CWA ya ha activado el túnel de movilidad entre los dos WLC. Esto está fuera del alcance de este ejemplo de configuración. Si necesita ayuda con esto, consulte el documento titulado "Creación de túneles de movilidad en los controladores Catalyst 9800"

Componentes Utilizados

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

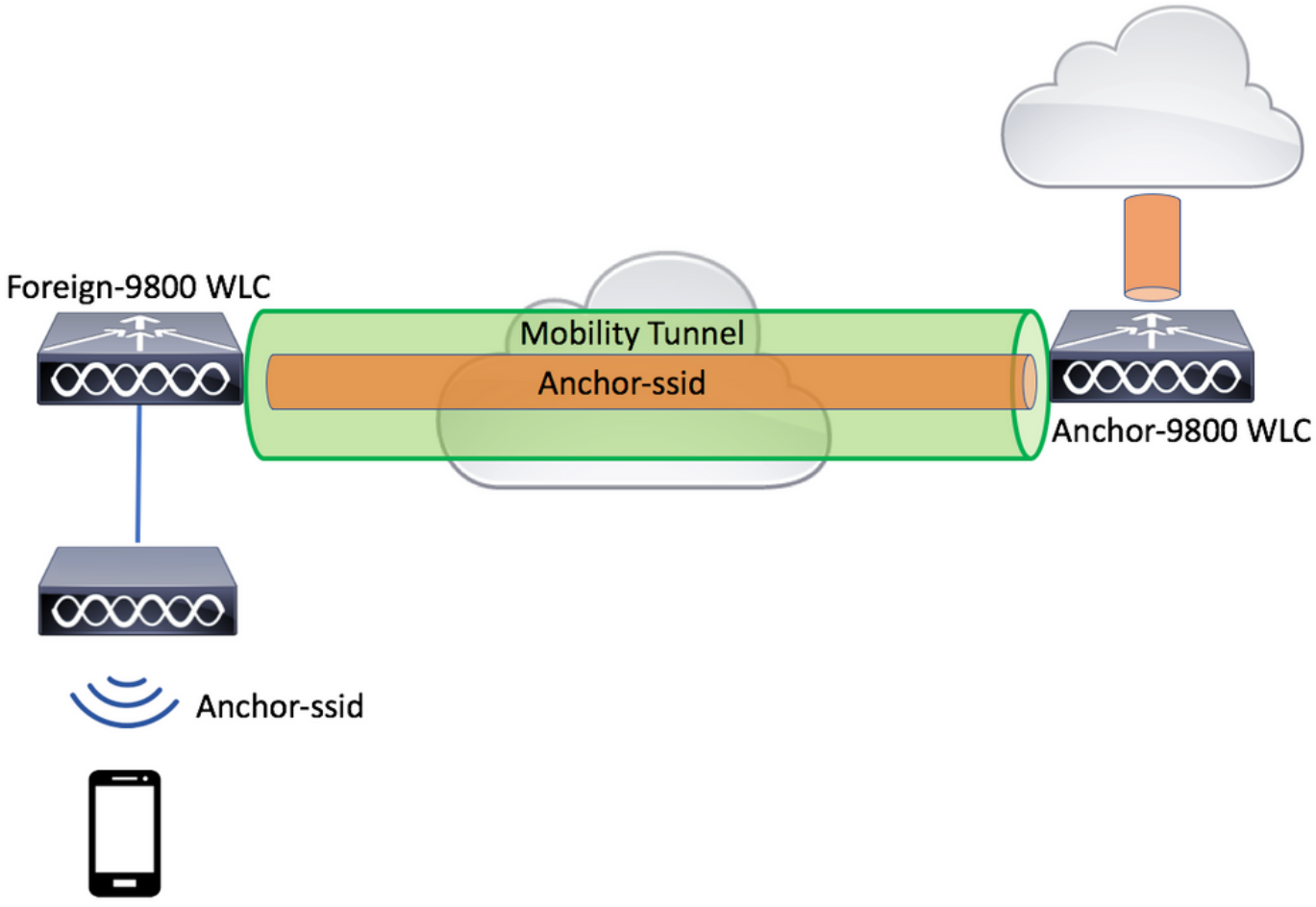
9800 17.2.1

5520 8.5.164 Imagen IRCM

ISE 2.4

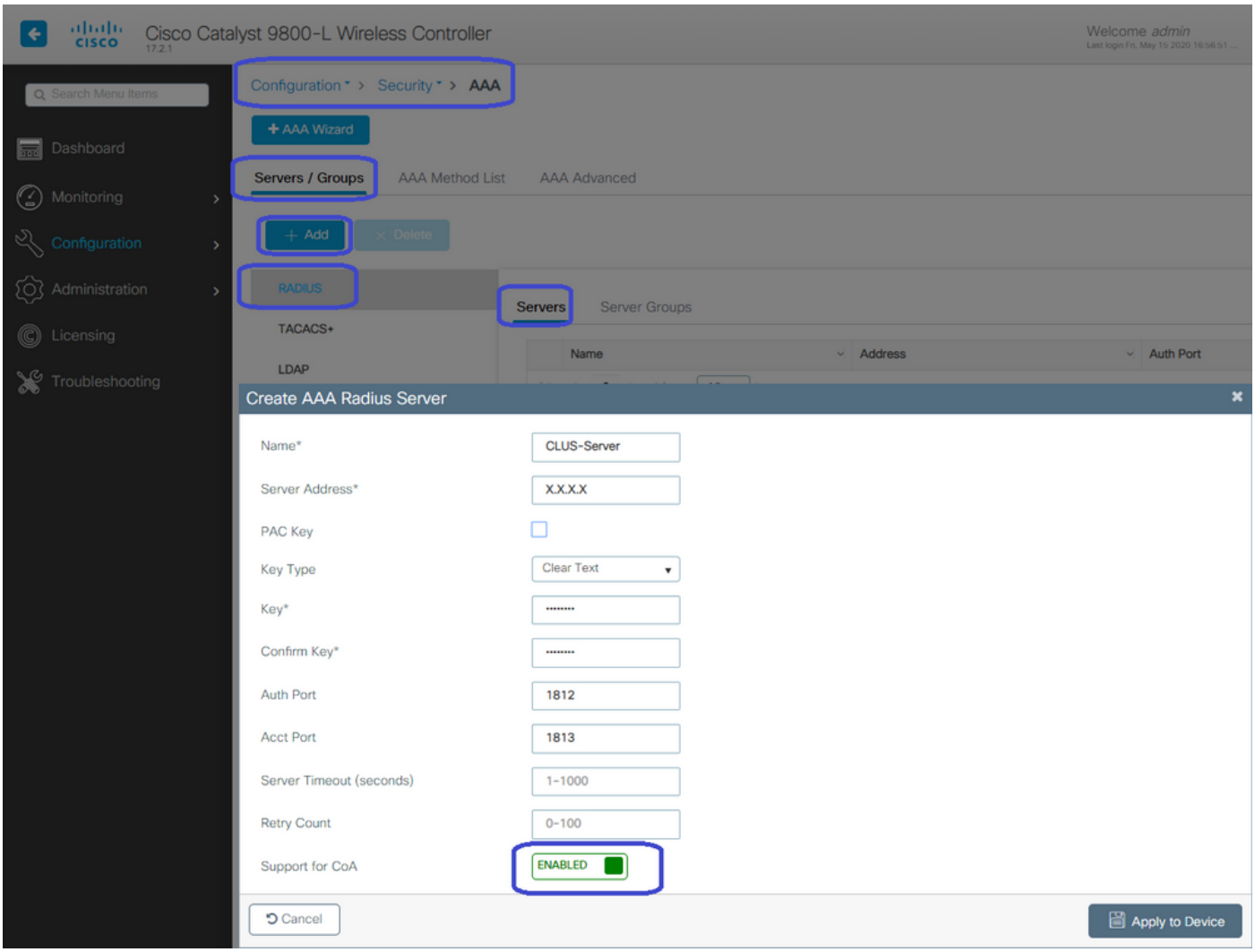
Configure un Catalyst 9800 anclado a otro Catalyst 9800

Diagrama de la red

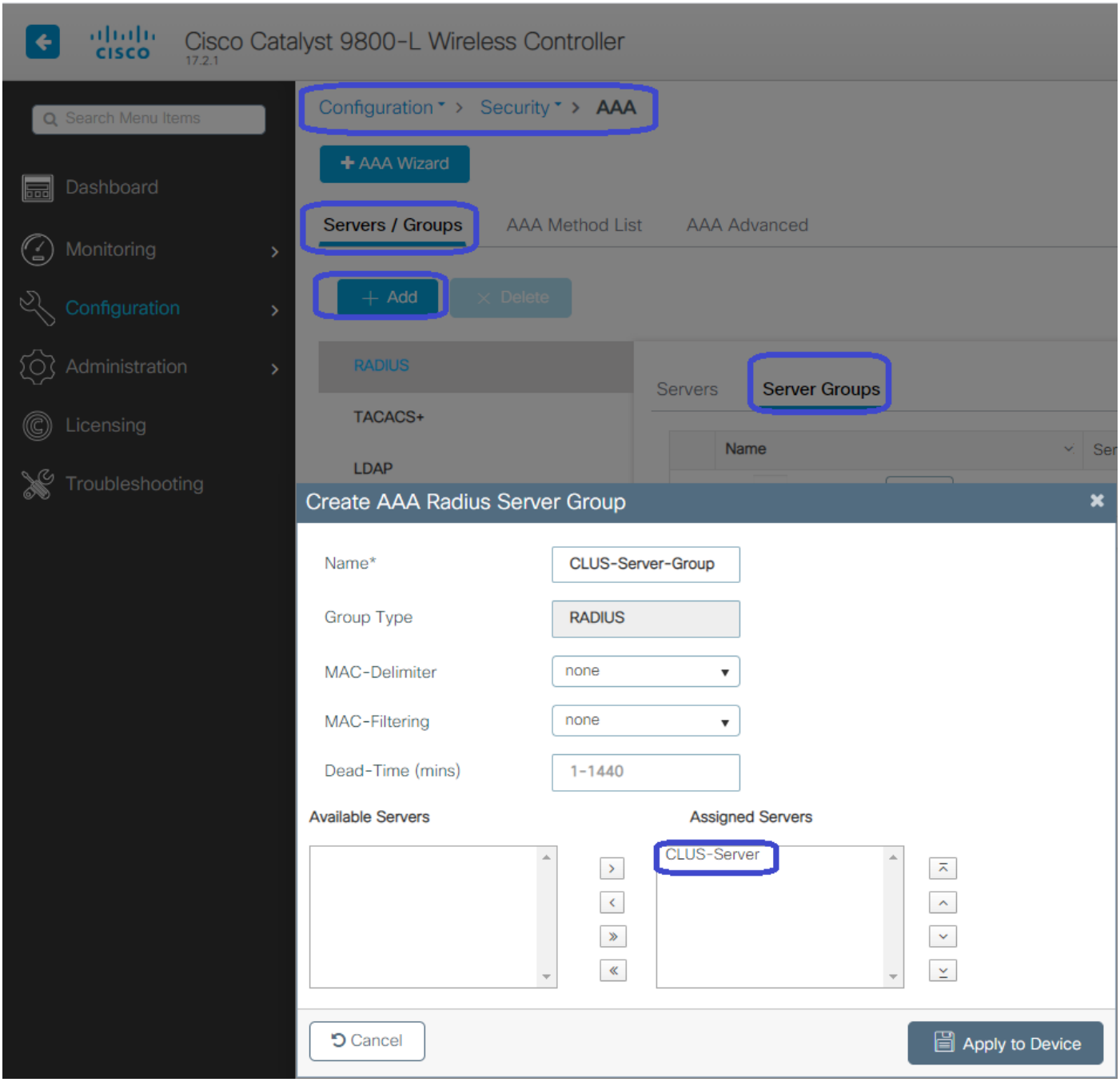


Configuración de AAA en ambos 9800

Tanto en el anclaje como en el externo deberá agregar primero el servidor RADIUS y asegurarse de que la CoA esté habilitada. Esto se puede hacer en el menú**Configuration>Security>AAA>Servers/Groups>Server> Haga clic en el botón Add**

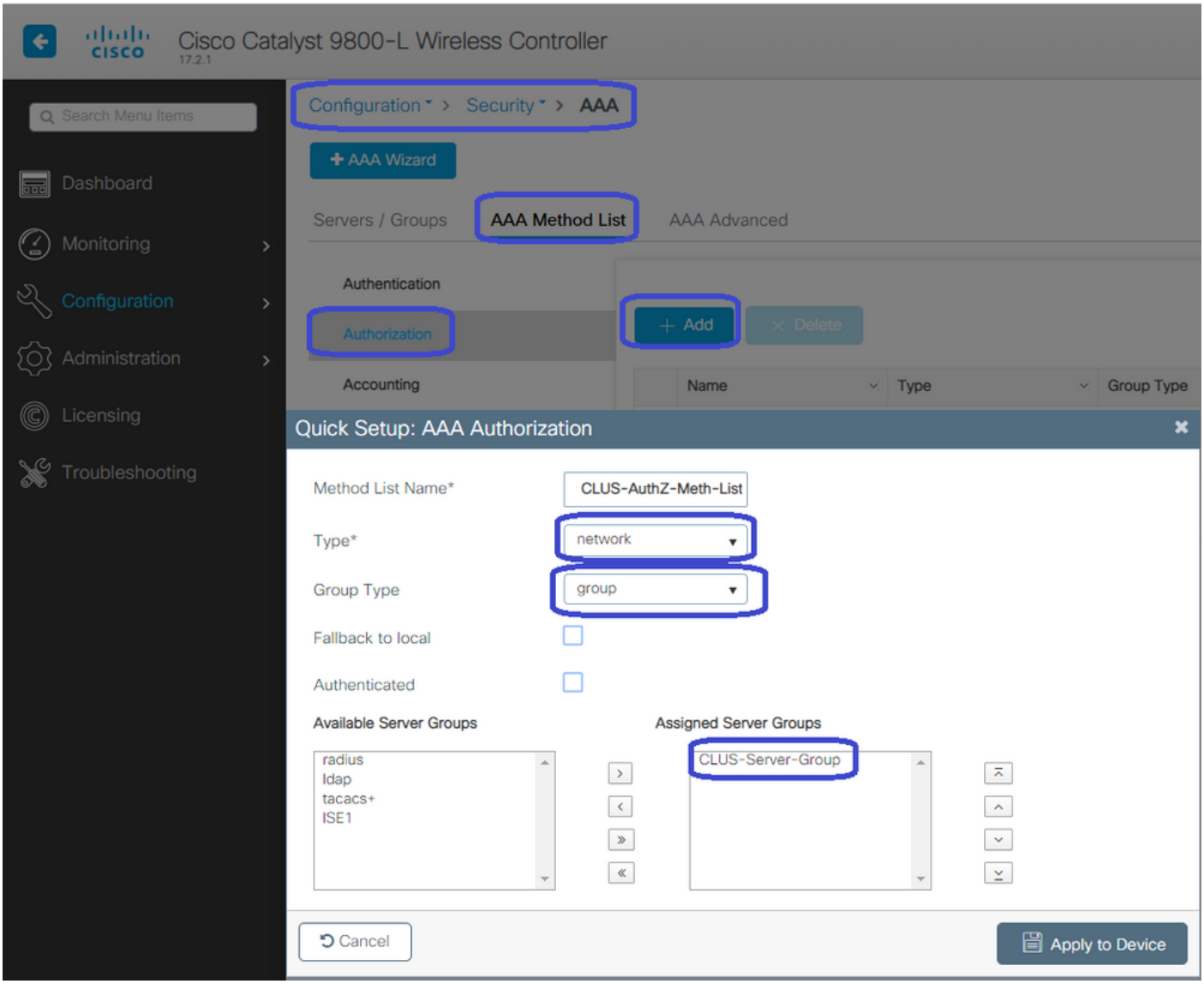


Ahora tendrá que crear un grupo de servidores y colocar el servidor que acaba de configurar en ese grupo. Esto se hace aquí **Configuration>Security>AAA>Servers/Groups>Server Groups>+Add**.

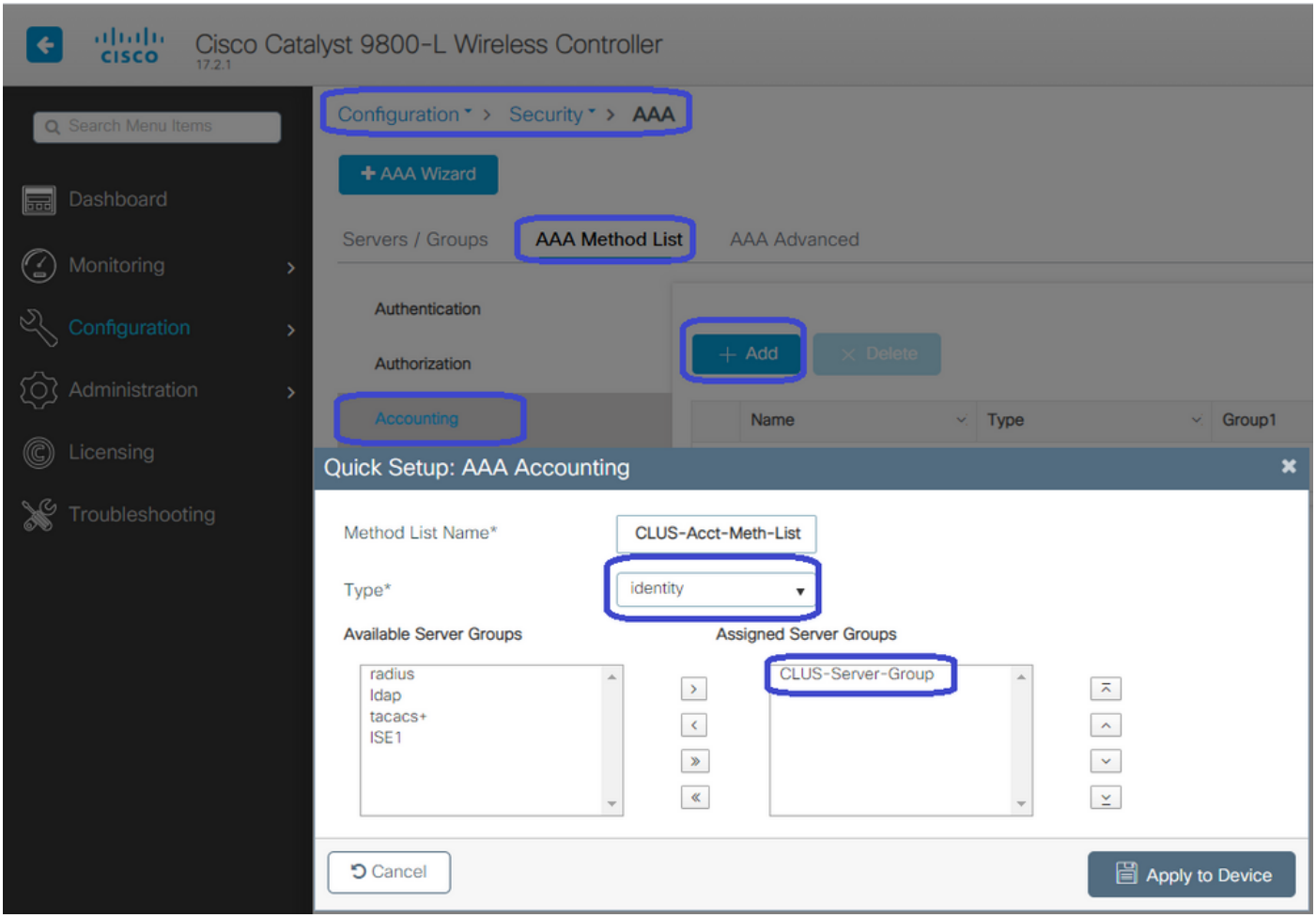


Ahora, cree una lista de métodos de **autorización** (no se requiere una lista de métodos de autenticación para CWA) donde el tipo es red y el tipo de grupo es group. Agregue el grupo de servidores de la acción anterior a esta lista de métodos.

Esta configuración se realiza aquí **Configuration>Security>AAA>Servers/AAA Method List>Authorization>+Add**

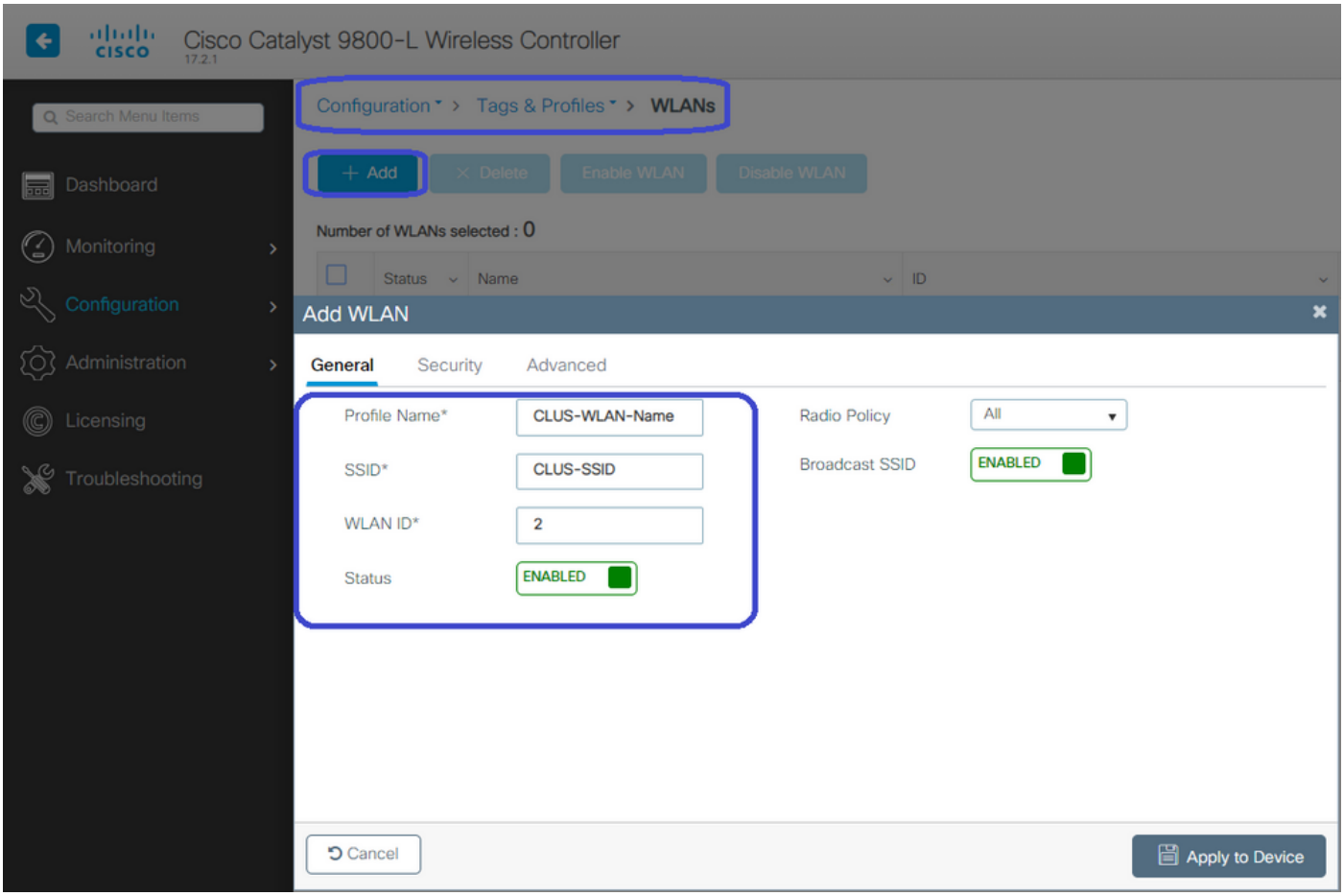


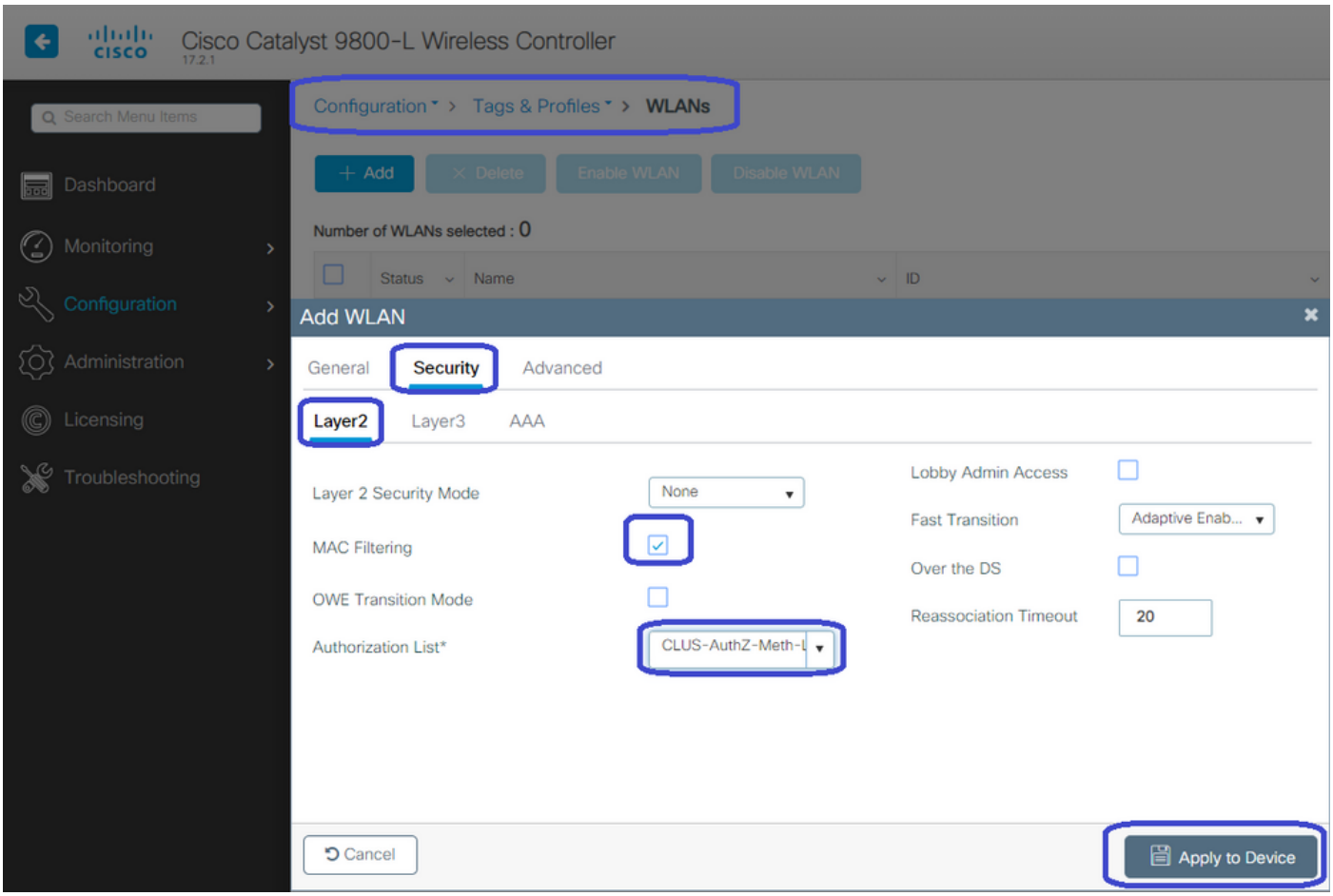
(Opcional) Cree una lista de métodos de contabilidad utilizando el mismo grupo de servidores que la lista de métodos de autorización. La lista de contabilidad se puede crear aquí **Configuration>Security>AAA>Servers/AAA Method List>Accounting>+Add**



Configure las WLAN en los WLC

Cree y configure las WLAN en ambos WLC. Las WLAN deben coincidir en ambos. El tipo de seguridad debe ser el filtrado mac y se debe aplicar la lista de métodos de autorización del paso anterior. Esta configuración se realiza en **Configuración>Etiquetas y perfiles>WLANs>+Agregar**



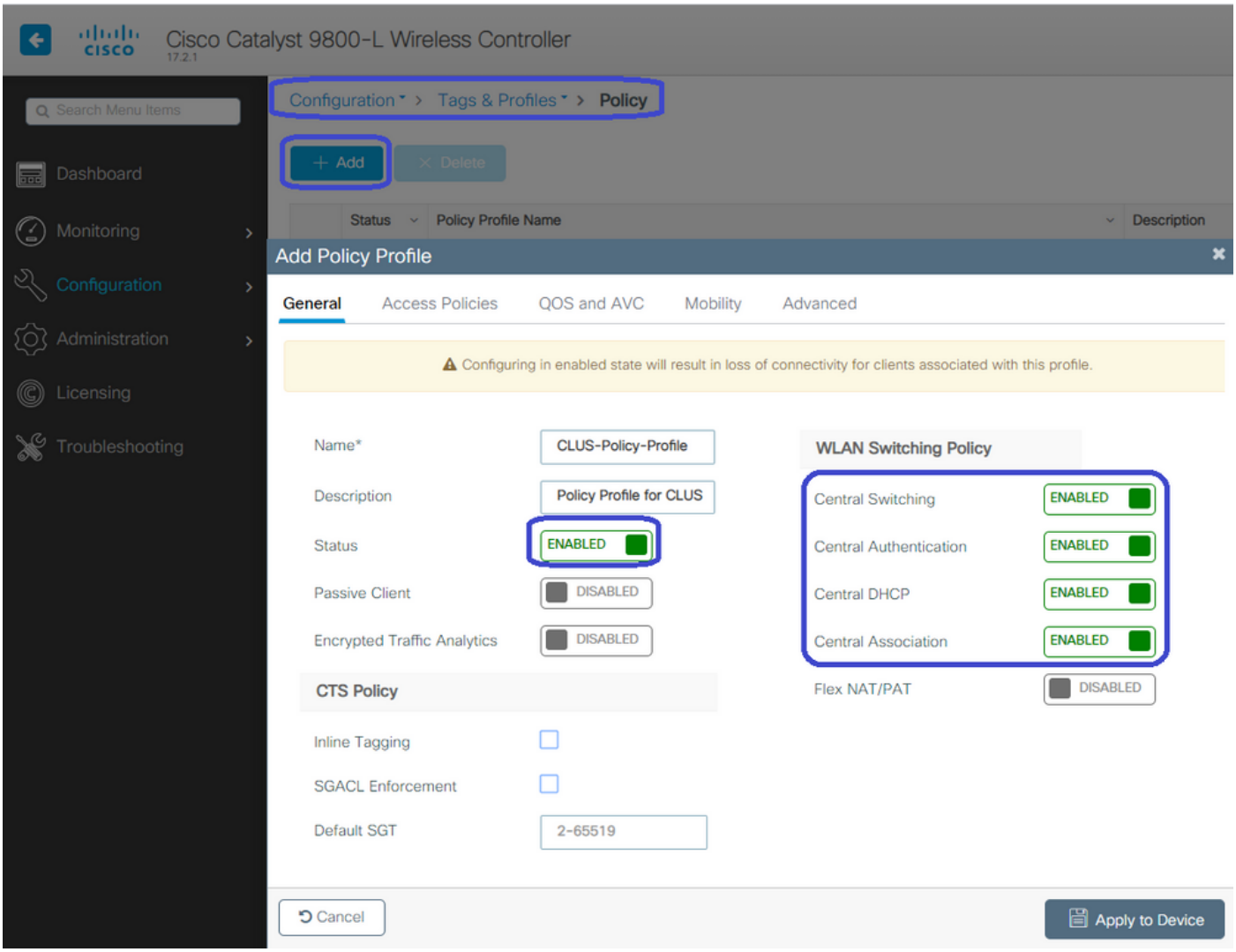


Cree el perfil de política y la etiqueta de política en el WLC externo

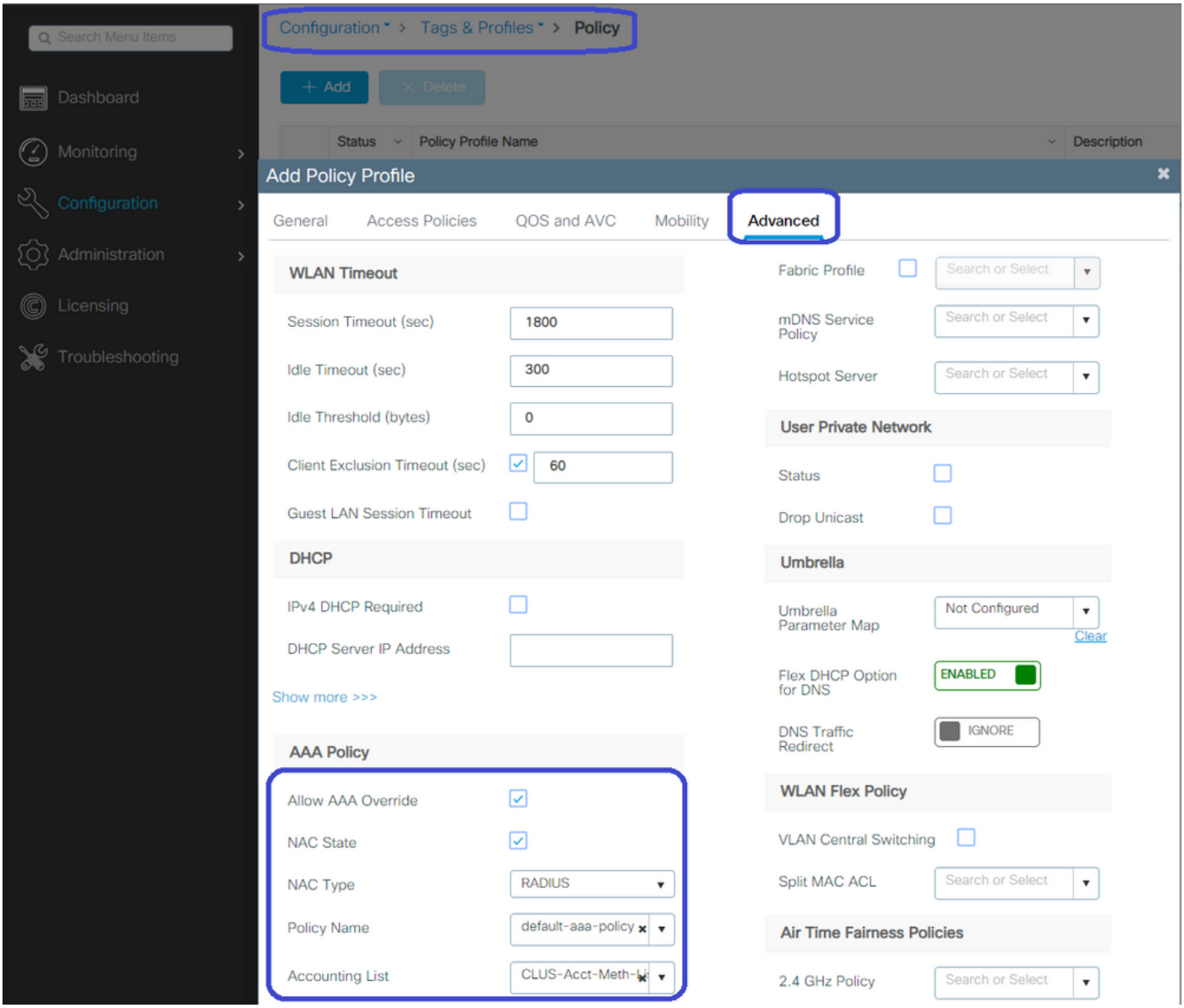
Vaya a la interfaz de usuario web del WLC externo.

Para crear el perfil de política, vaya a **Configuration>Tags & Profiles>Policy>+Add**

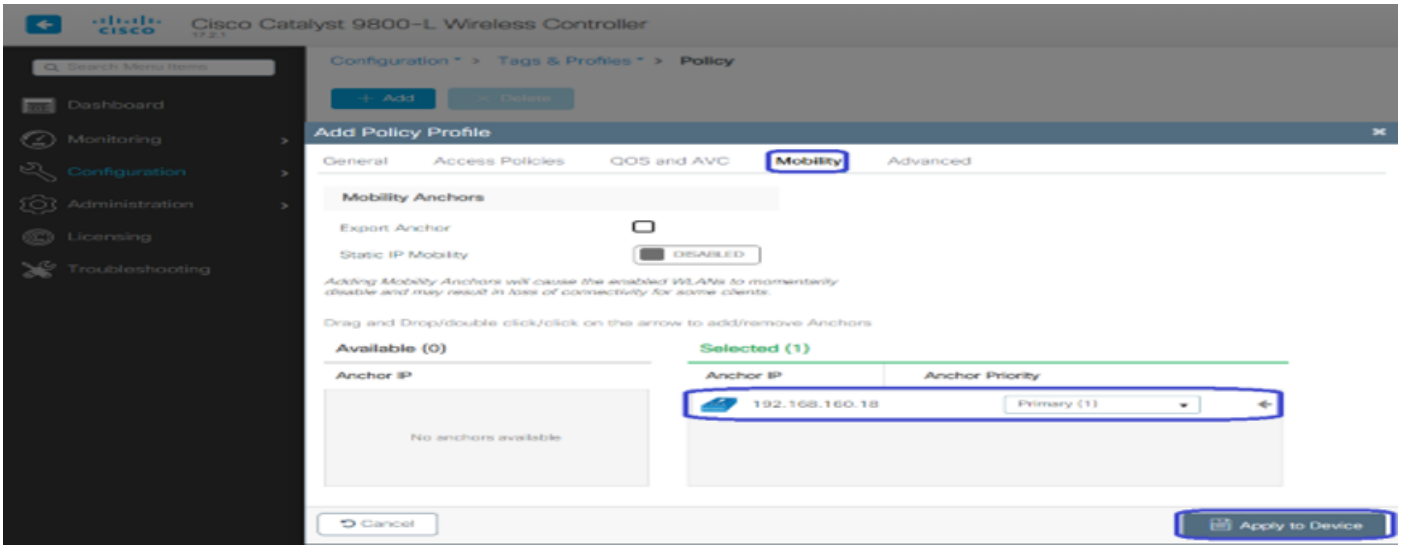
Al anclar, debe utilizar el switching central.



En la ficha "Avanzado", la anulación de AAA y RADIUS NAC son obligatorias para CWA. Aquí también puede aplicar la lista de métodos de contabilidad si decide hacerlo.



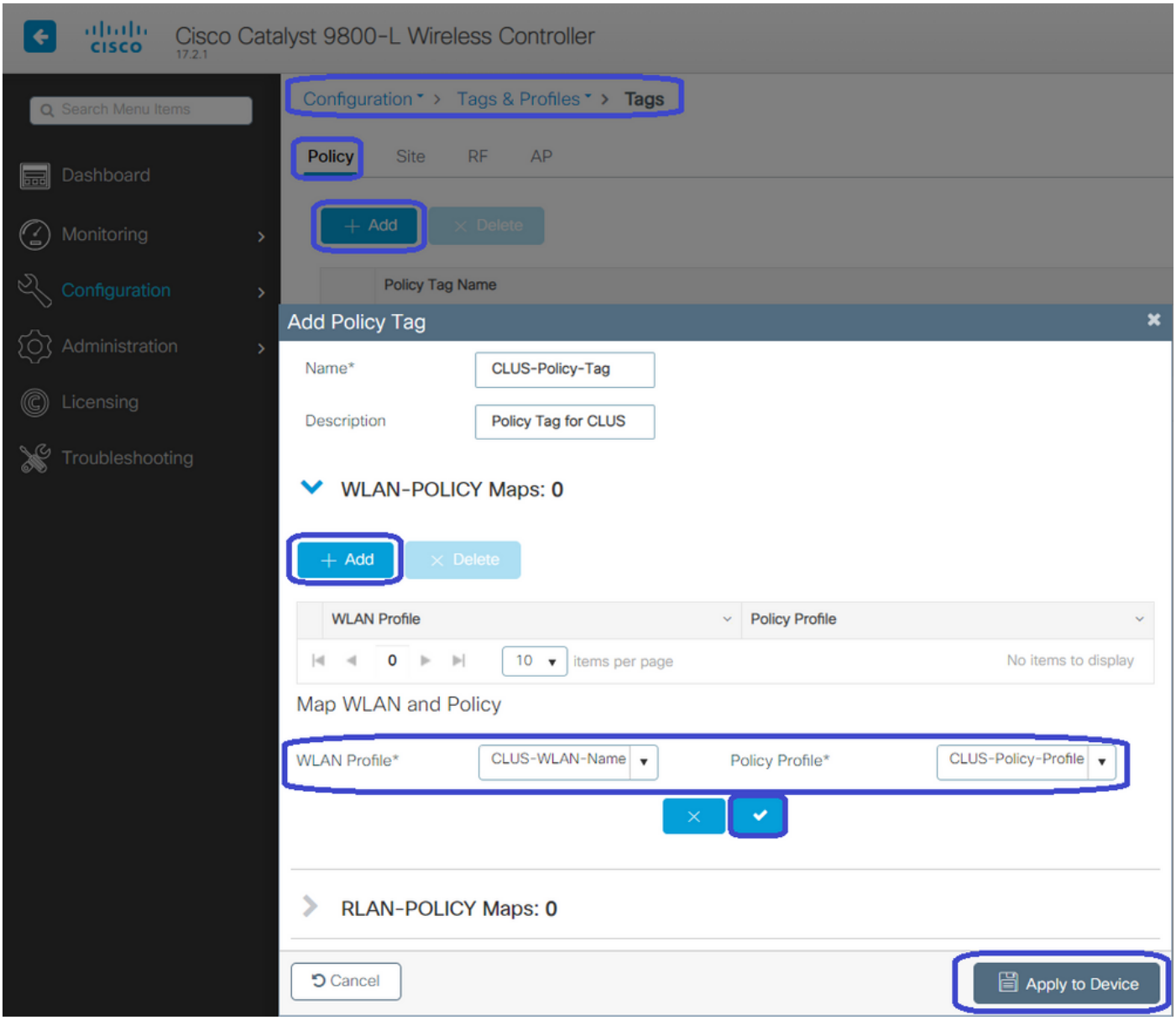
En la pestaña "Movilidad" **NO** marque la casilla de verificación "exportar anclaje" sino más bien agregue el WLC de anclaje a la lista de anclaje. Asegúrese de pulsar "Aplicar al dispositivo". Como recordatorio, esto supone que ya tiene una configuración de túnel de movilidad entre los dos controladores



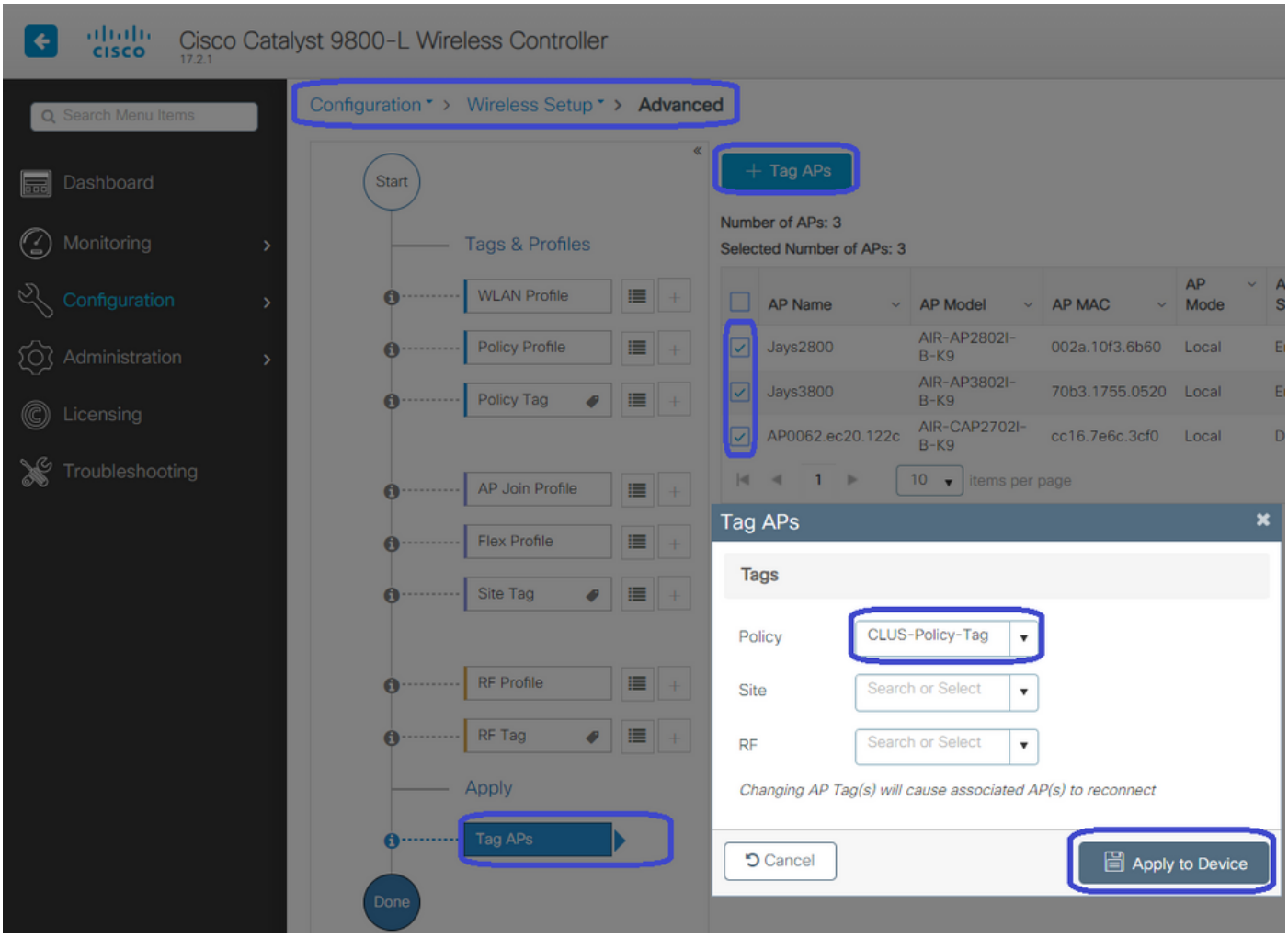
Para que los APs usen este perfil de política, necesitará crear una etiqueta de política y aplicarla a

los APs que desea utilizar.

Para crear la etiqueta de política, vaya a **Configuration>Tags & Profiles>Tags?Policy>+Add**



Para agregar esto a varios AP al mismo tiempo, vaya a **Configuration>Wireless Setup>Advanced>Start Now**. Haga clic en las barras de viñetas junto a "Tag APs" y agregue la etiqueta a los AP que elija.

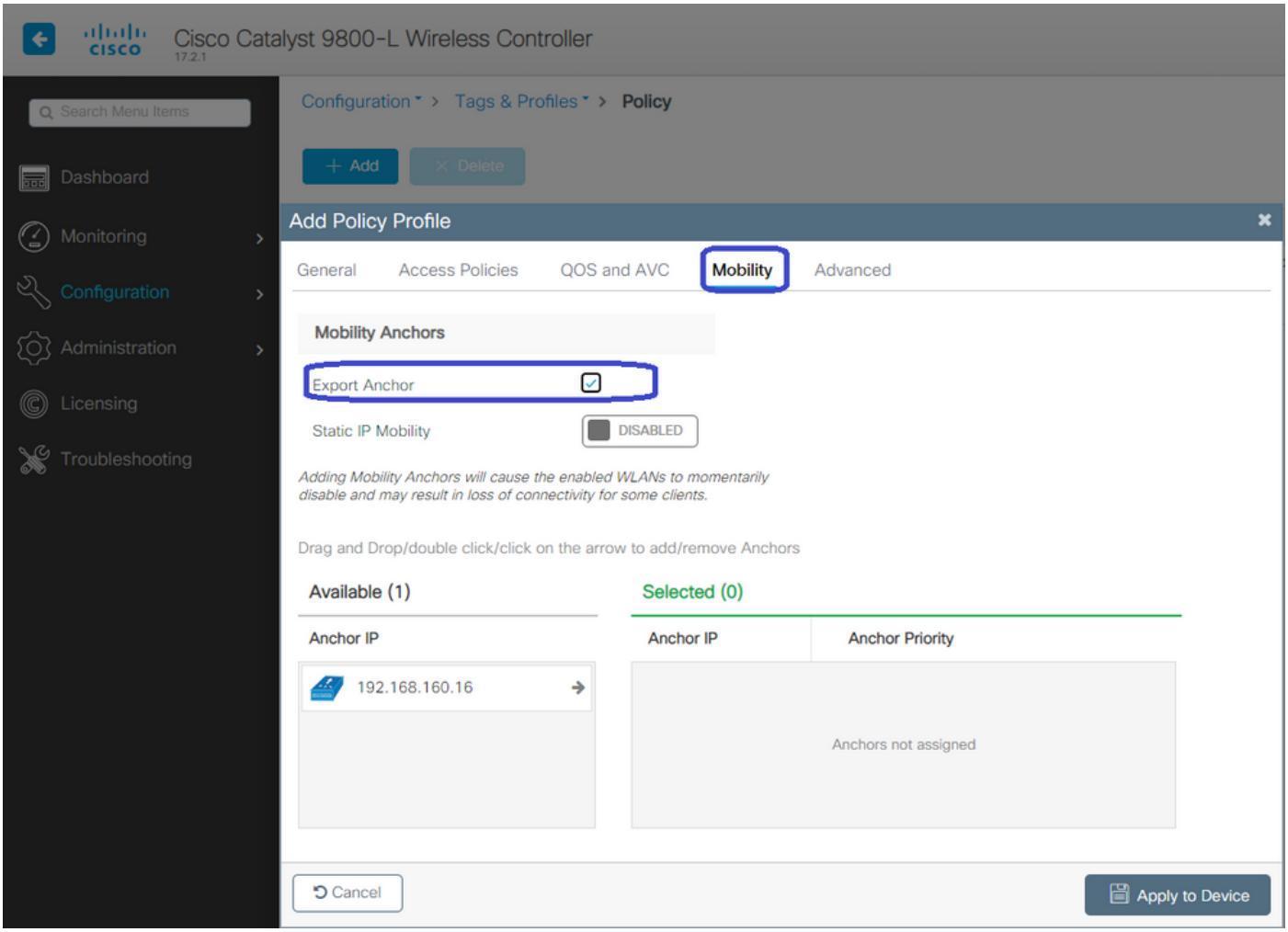


Cree el perfil de política en el WLC de anclaje

Vaya a la interfaz de usuario web del WLC de anclaje. Agregue el perfil de política en el anclaje 9800 bajo **Configuración>Etiquetas y perfiles>Etiquetas>Política>+Agregar**. Asegúrese de que coincide con el perfil de política hecho en el externo excepto para la pestaña de movilidad y la lista de contabilidad.

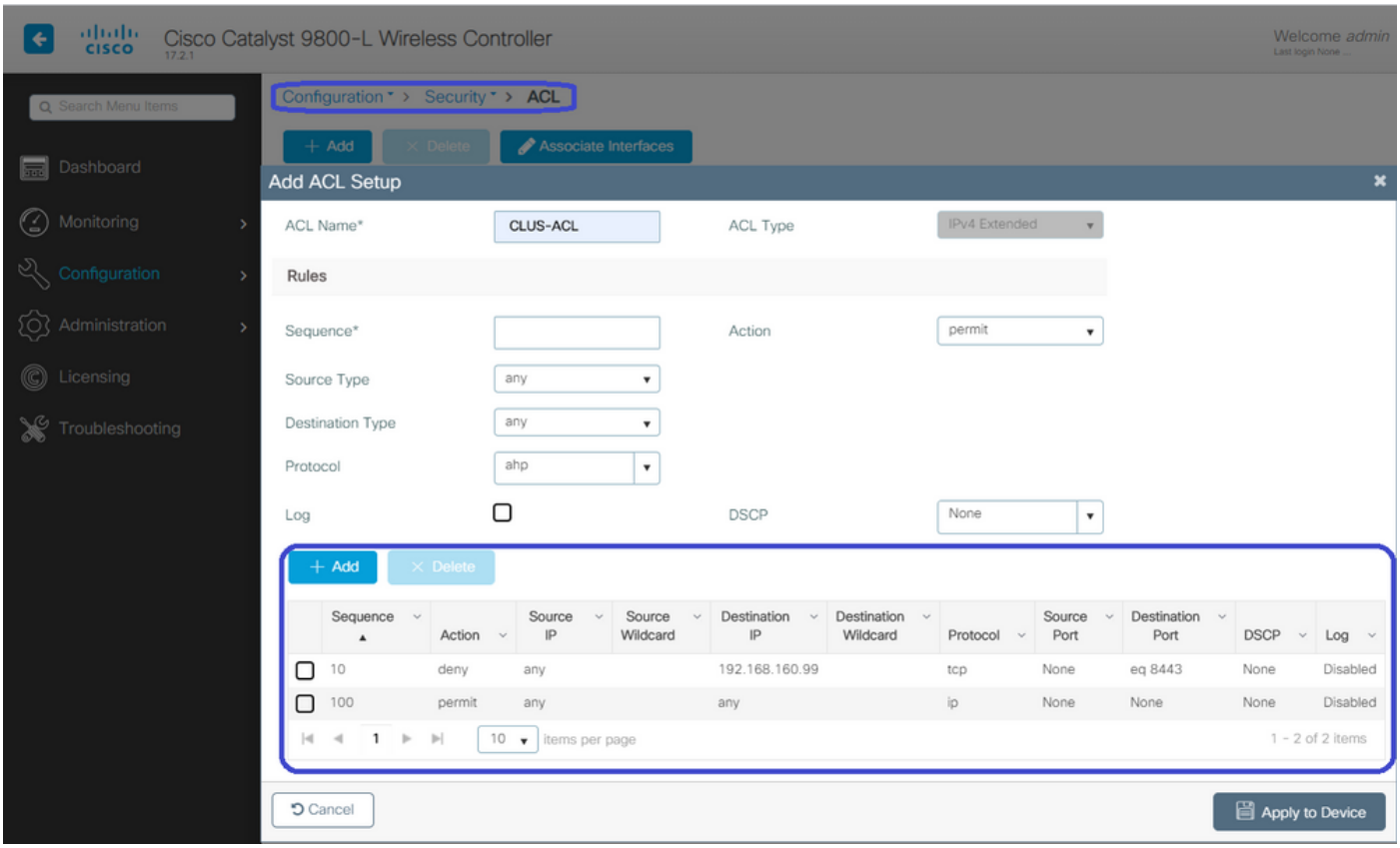
Aquí no agrega un anclaje, pero sí marca la casilla de verificación "Exportar anclaje". No agregue la lista de cuentas aquí. Como recordatorio, esto supone que ya tiene una configuración de túnel de movilidad entre los dos controladores

Nota: No hay razón para asociar este perfil a una WLAN en una etiqueta de política. Esto creará problemas si lo hace. Si desea utilizar la misma WLAN para AP en este WLC, cree otro perfil de política para él.



Redirigir configuración de ACL en ambos 9800

A continuación, debe crear la configuración de ACL de redirección en ambos 9800. Las entradas en el Foreign no importan ya que será el WLC de anclaje que aplica la ACL al tráfico. El único requisito es que esté allí y tenga alguna entrada. Las entradas en el ancla tienen que "denegar" el acceso a ISE en el puerto 8443 y "permitir" todo lo demás. Esta ACL sólo se aplica al tráfico que llega "dentro" del cliente, por lo que no se necesitan reglas para el tráfico de retorno. DHCP y DNS pasarán sin entradas en la ACL.

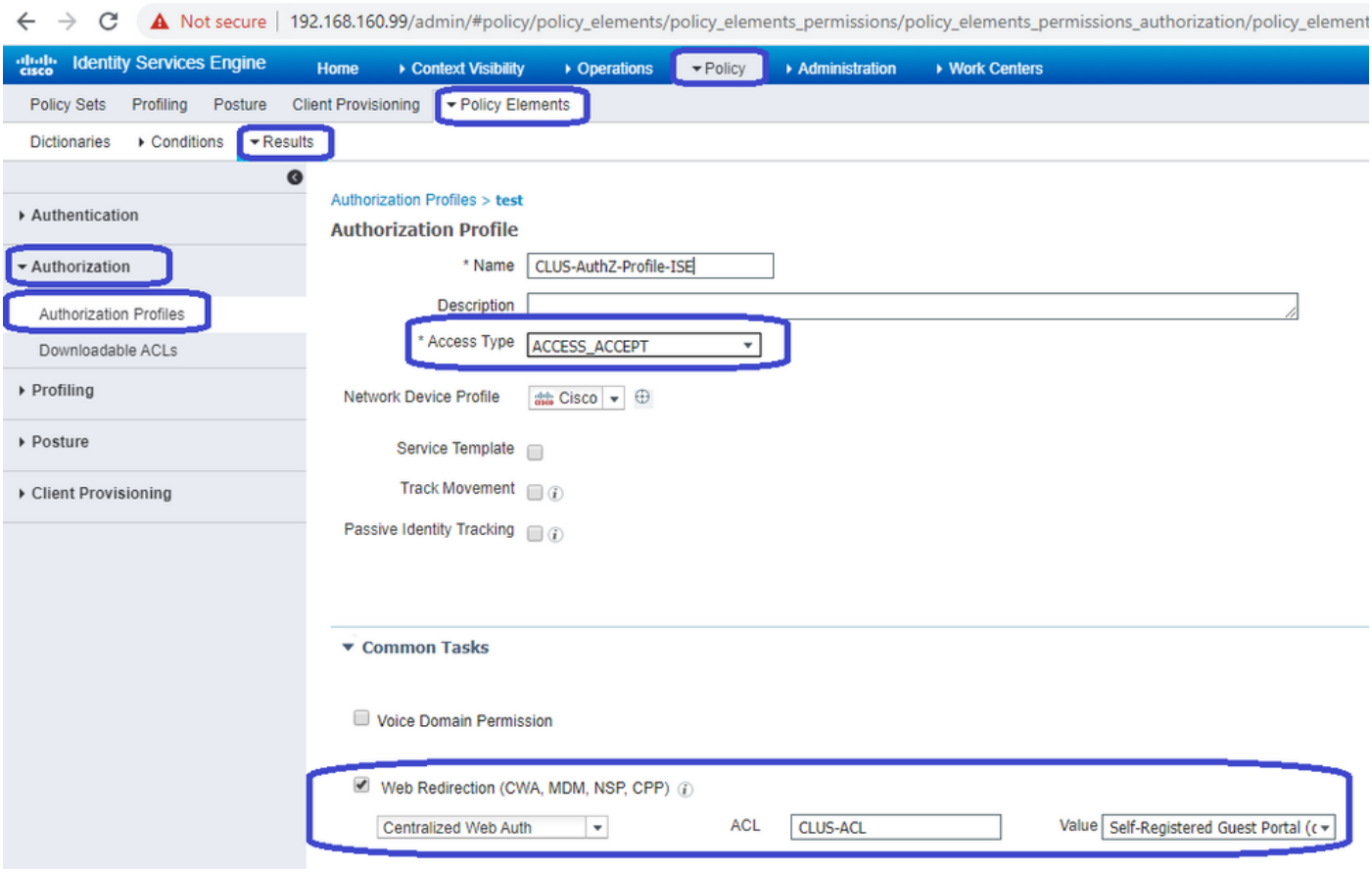


Configuración de ISE

El último paso es configurar ISE para CWA. Hay muchas opciones para esto, pero este ejemplo se ceñirá a lo básico y usará el portal de invitados autoregistrado predeterminado.

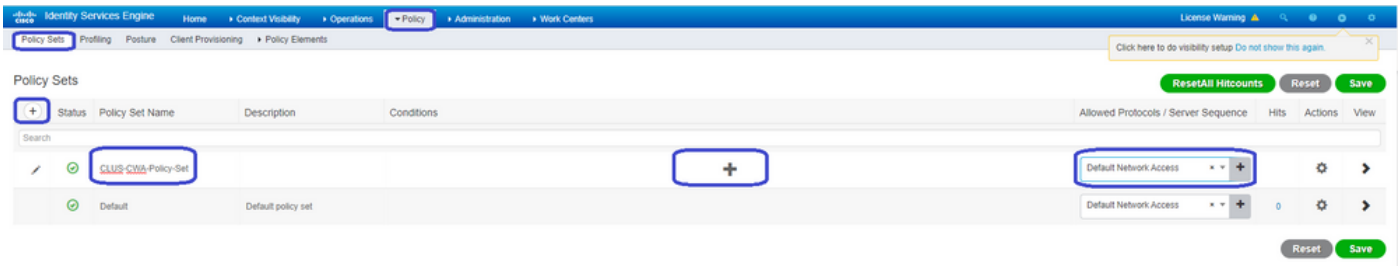
En ISE, debe crear un perfil de autorización, un conjunto de políticas con una política de autenticación y una política de autorización que utilice el perfil de autorización, agregar el 9800(external) a ISE como dispositivo de red y crear un nombre de usuario y una contraseña para iniciar sesión en la red.

Para crear el perfil de autorización, vaya a **Policy>Policy Elements>Authorization>Results>Authorization Profiles>**, a continuación, haga clic en **Add**. Asegúrese de que el tipo de acceso devuelto es "access_accept" y, a continuación, establezca los AVP(pares valor-atributo) que desea devolver. Para CWA, la ACL de redirección y la URL de redirección son obligatorias, pero también puede enviar cosas como el ID de VLAN y el tiempo de espera de sesión. Es importante que el nombre de la ACL coincida con el nombre de la ACL de redirección en el externo y el 9800 de anclaje.

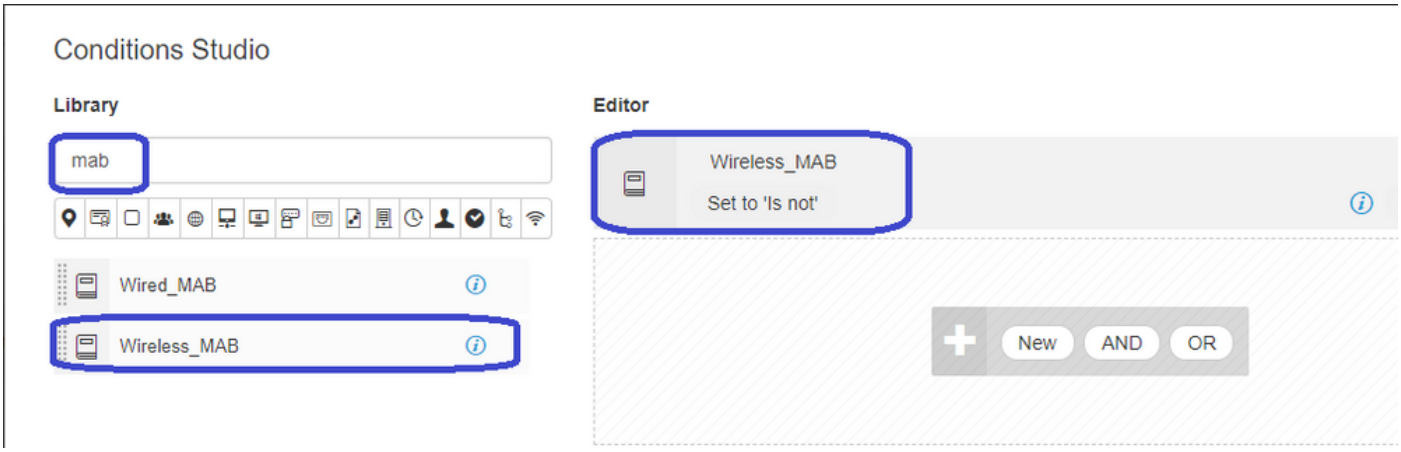


A continuación, debe configurar una forma de aplicar el perfil de autorización que acaba de crear a los clientes que pasan por CWA. Para lograrlo, una manera es crear un conjunto de políticas que omite la autenticación cuando se usa MAB y aplicar el perfil de autorización cuando se usa el SSID enviado en el ID de estación llamada. De nuevo, hay muchas maneras de lograrlo, así que si necesita algo más específico o más seguro, esta es la forma más simple de hacerlo.

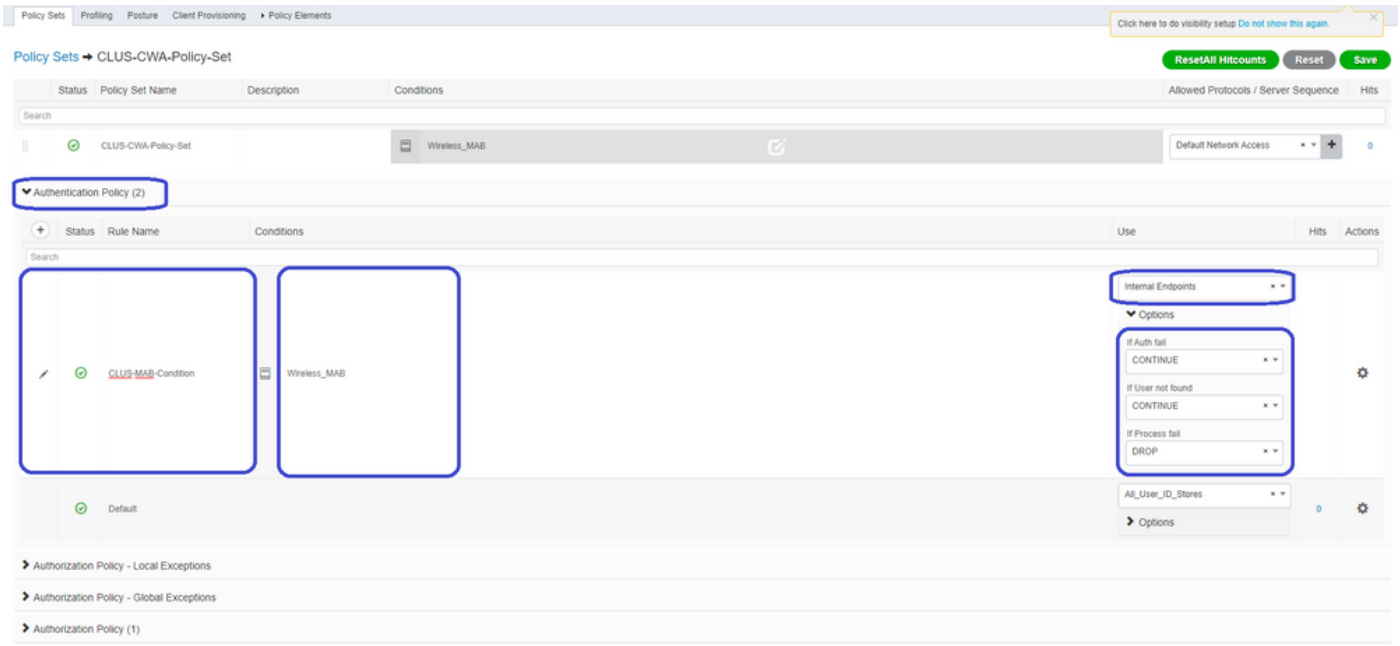
Para crear el conjunto de políticas, vaya a **Policy>Policy Set** y pulse el botón + en el lado izquierdo de la pantalla. Asigne el nombre al nuevo conjunto de políticas y asegúrese de que esté configurado como "acceso a la red predeterminado" o cualquier lista de protocolos permitidos que permita "Búsqueda de host de procesos" para MAB(para verificar la lista de protocolos permitidos vaya a Política>Elementos de políticas>Resultados>Autenticación>Protocolos permitidos). Ahora, presione el signo + en medio del nuevo conjunto de políticas que creó.



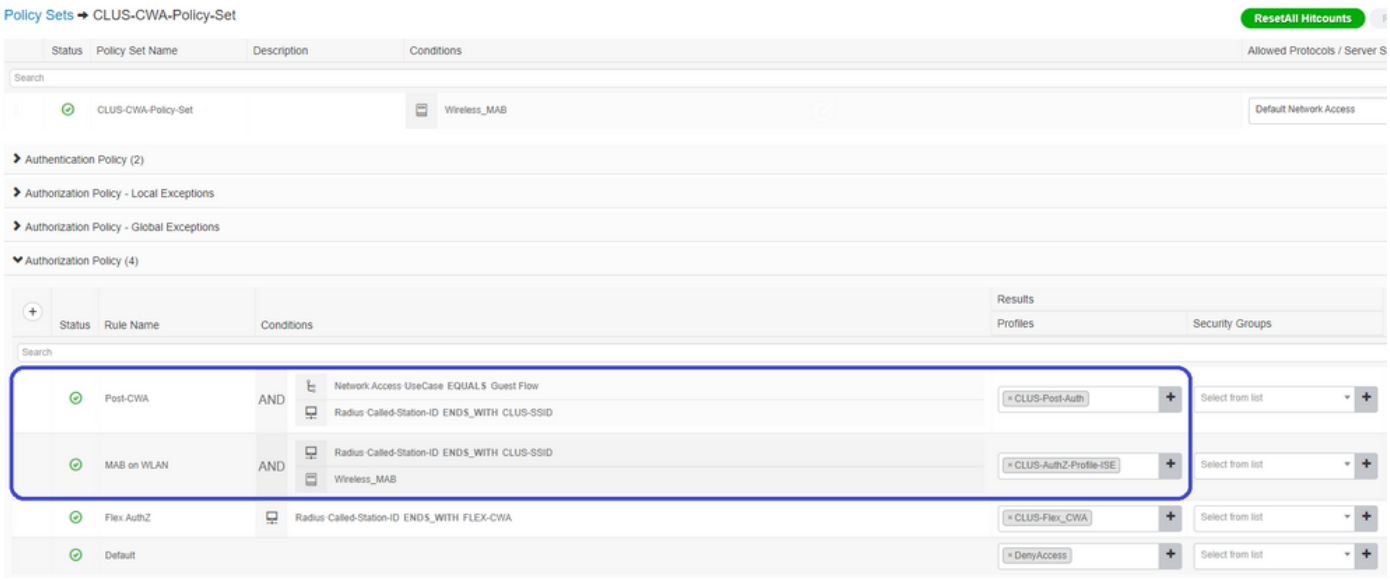
Para este conjunto de políticas cada vez que MAB se utiliza en ISE, pasará a través de este conjunto de políticas. Posteriormente, puede hacer políticas de autorización que coincidan con el ID de la estación llamada para que se puedan aplicar resultados diferentes dependiendo de la WLAN que se esté utilizando. Este proceso es muy personalizable con muchas cosas en las que puede coincidir.



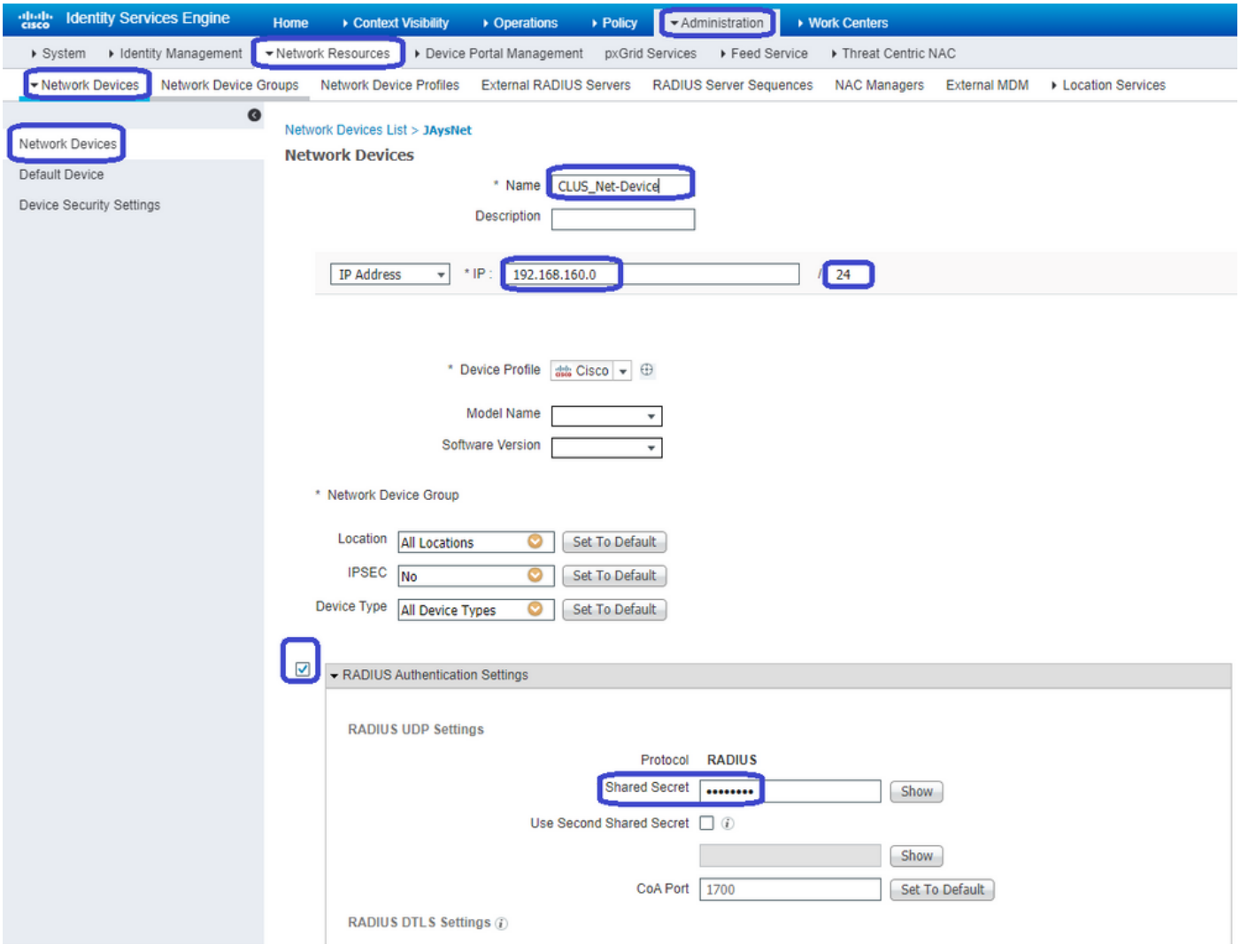
Dentro del conjunto de políticas , cree las políticas. La política de autenticación puede coincidir de nuevo en MAB, pero necesita cambiar el almacén de ID para utilizar "terminales internos" y debe cambiar las opciones para continuar con la autenticación de error y el usuario no encontrado.



Una vez establecida la política de autenticación, debe crear dos reglas en la política de autorización. Esta política se lee como una ACL, por lo que el orden necesita tener la regla post-auth arriba y la regla pre-auth abajo. La regla posterior a la autenticación coincidirá con los usuarios que ya han pasado por guest-flow. Esto es para decir que si ya firmaron, golpearán esa regla y pararán ahí. Si no han iniciado sesión, continuarán por la lista y aplicarán la regla anterior a la autenticación obteniendo la redirección.Es una buena idea hacer coincidir las reglas de la política de autorización con el ID de la estación llamada que termina con el SSID para que sólo llegue a las WLAN configuradas para hacerlo.

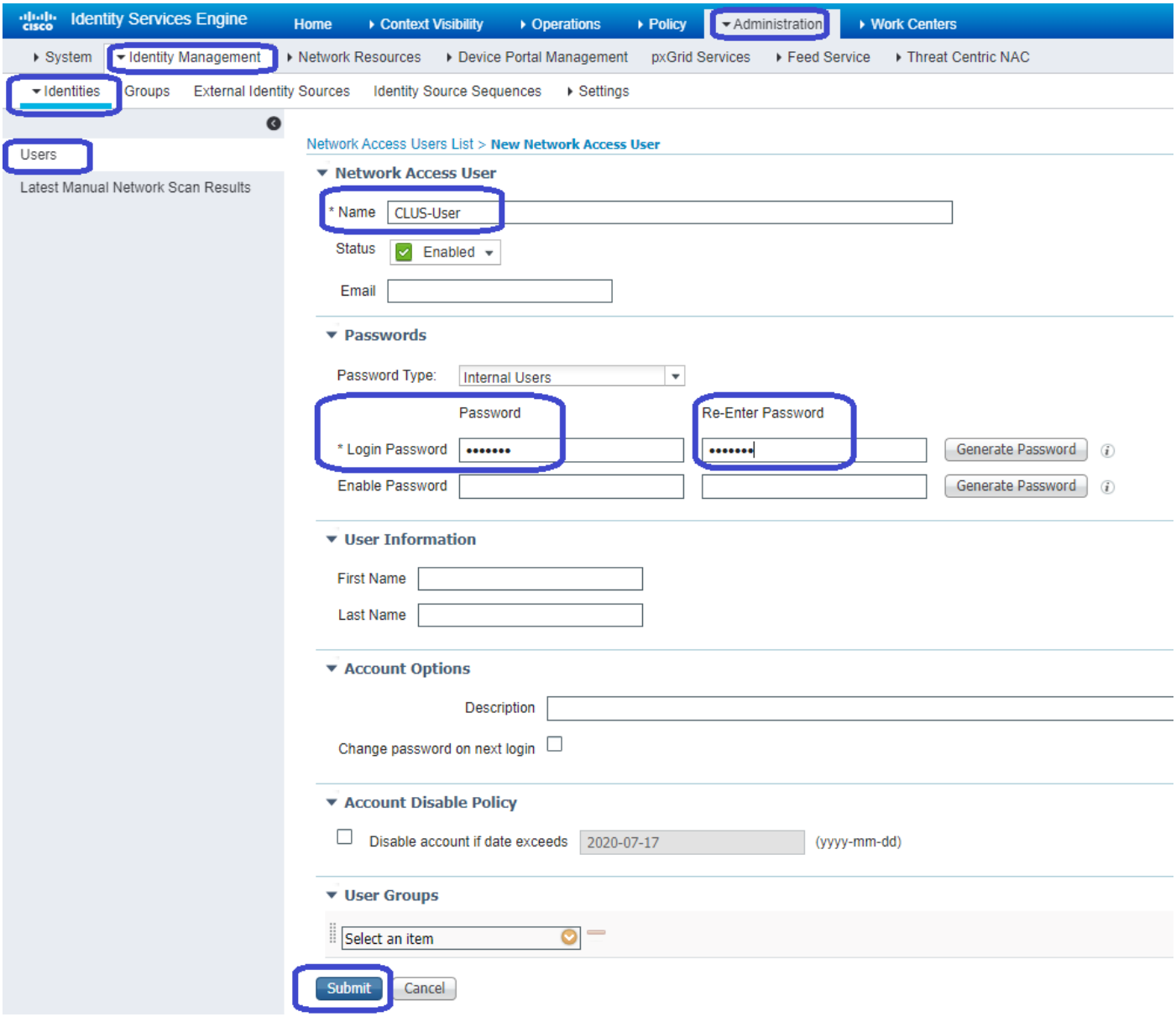


Ahora que el conjunto de políticas está configurado, debe informar a ISE acerca del 9800 (Foreign) para que ISE confíe en él como un autenticador. Esto se puede hacer en **Admin>Network Resources>Network Device>+**. Debe asignarle un nombre, establecer la dirección IP (o, en este caso, toda la subred de administración), activar RADIUS y establecer el secreto compartido. El secreto compartido en ISE debe coincidir con el secreto compartido en el 9800 o este proceso fallará. Después de agregar la configuración, pulse el botón enviar para guardarla.

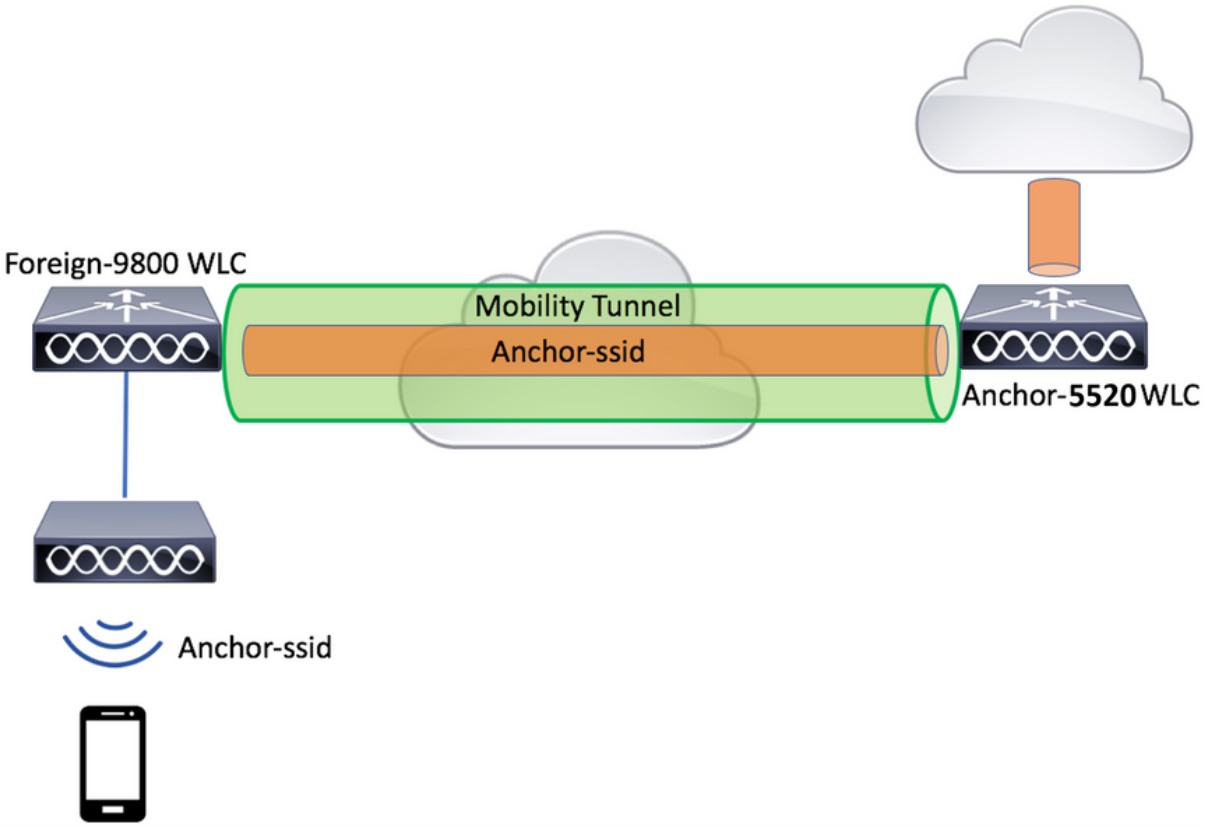


Finalmente, deberá agregar el nombre de usuario y la contraseña que el cliente ingresará en la

página de inicio de sesión para validar que deben tener acceso a la red. Esto se realiza bajo **Admin>Identity Management>Identity>Users>+Add** y asegúrese de enviar después de agregarlo. Al igual que todo lo demás con ISE, esto es personalizable y no tiene que ser un usuario almacenado localmente, pero, de nuevo, es la configuración más sencilla.



Configure un Catalyst 9800 anclado a un WLC AireOS

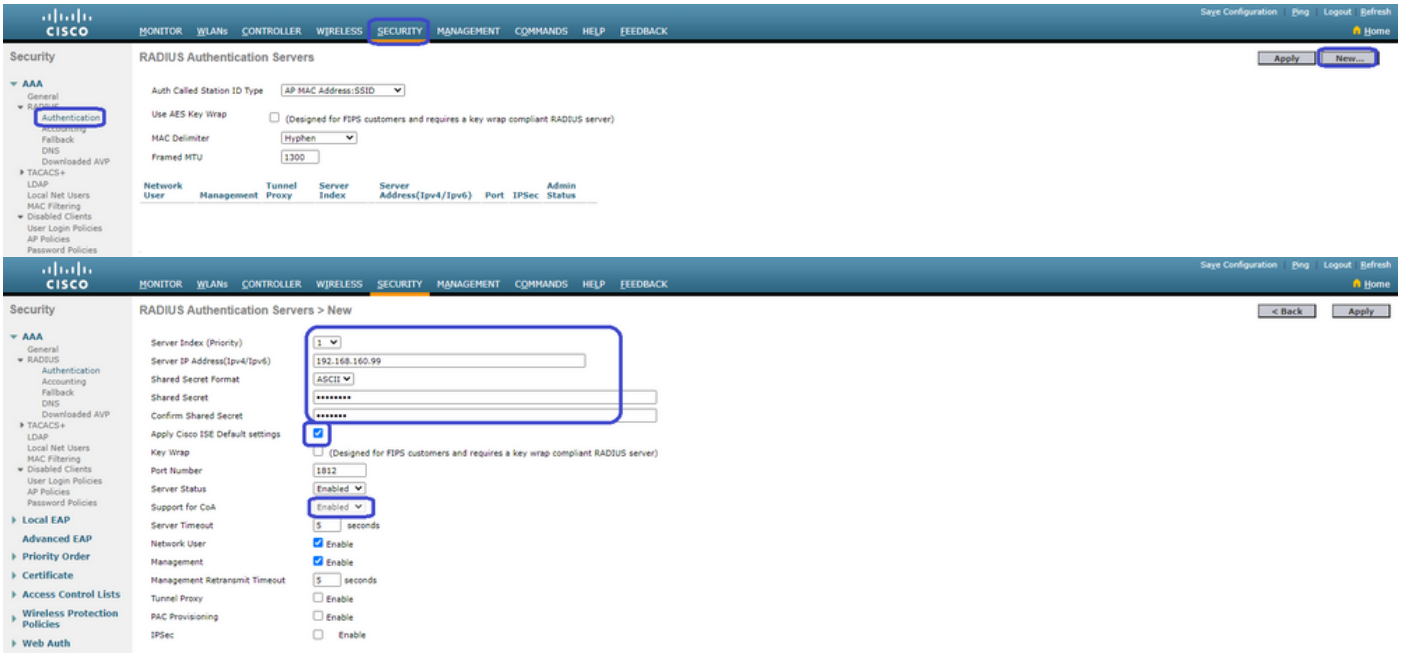


Configuración externa de Catalyst 9800

Siga los mismos pasos descritos anteriormente, saltando la sección "*Crear el perfil de política en el WLC de anclaje*".

Configuraciones AAA en el WLC AireOS de anclaje

Agregue el servidor al WLC yendo a **Security>AAA>RADIUS>Authentication>New**. Agregue la dirección IP del servidor, el secreto compartido y la compatibilidad con CoA.

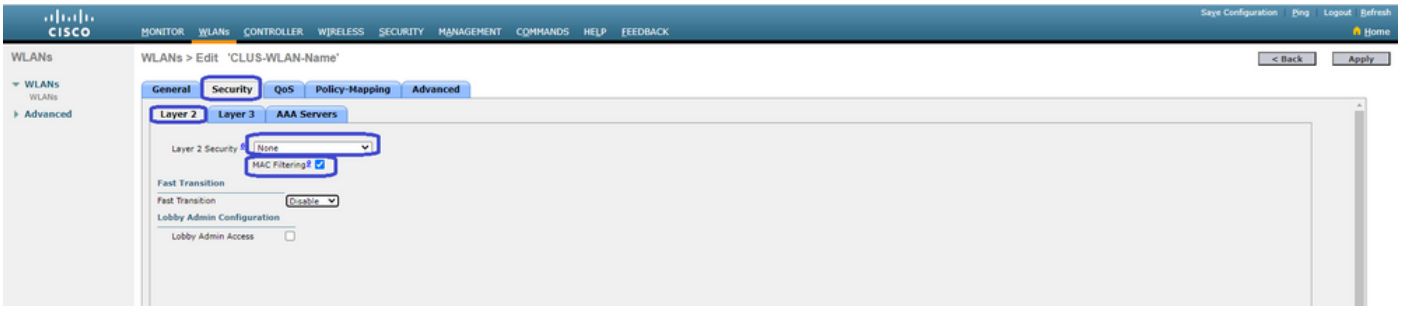


Configuración WLAN en el WLC AireOS

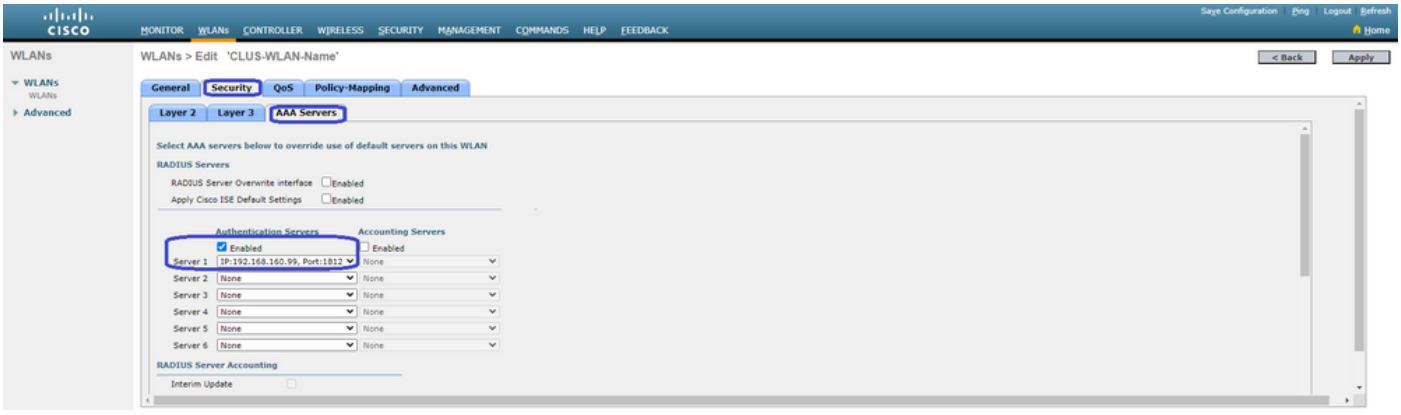
Para crear la WLAN, vaya a **WLANs>Create New>Go**.

Configure el nombre del perfil, el ID de WLAN y el SSID, luego presione "Aplicar".

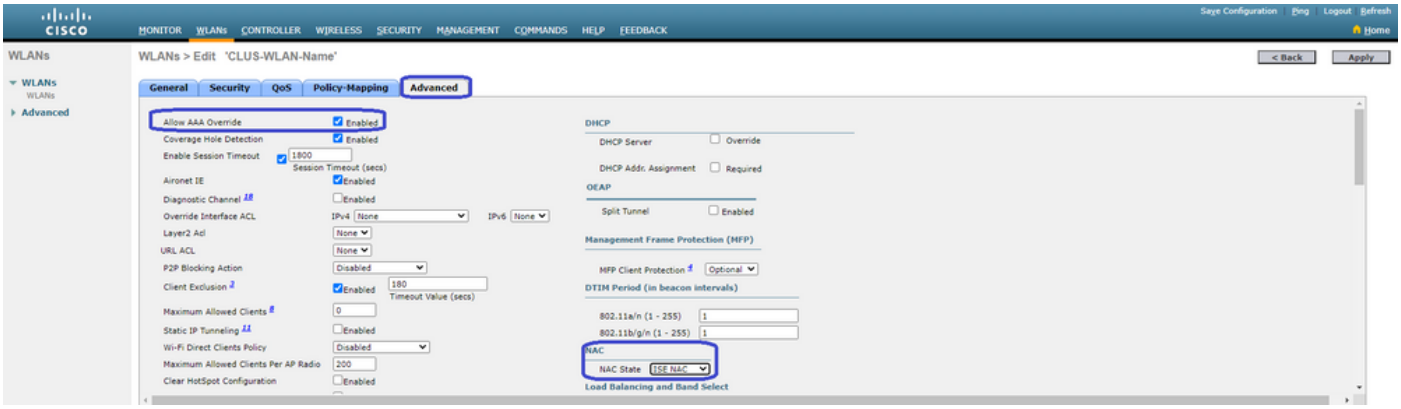
Esto le llevará a la configuración de WLAN. En la ficha "General" puede agregar la interfaz que desea que utilicen los clientes si no va a configurar ISE para enviarla en los AVP. A continuación, vaya a la ficha **Security>Layer2** y haga coincidir la configuración de "Layer 2 Security" que utilizó en el 9800 y active "MAC Filtering".



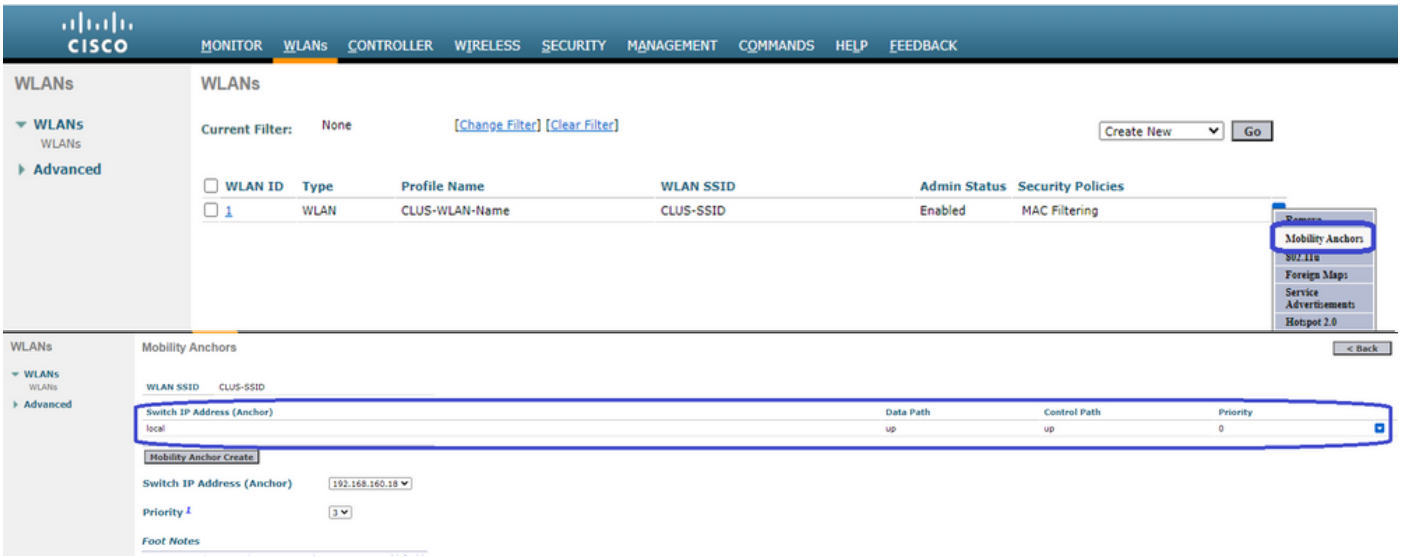
Ahora pase a la ficha **Security>AAA Servers** y establezca el servidor ISE como "Authentication Servers" (Servidores de autenticación). **No** establezca nada para los "servidores de contabilidad". Desmarque la casilla "Habilitar" para la contabilización.



Mientras aún se encuentra en las configuraciones de WLAN, pase a la pestaña "Avanzado" y habilite "Permitir Anulación AAA", así como cambie el "Estado NAC" a "NAC ISE"



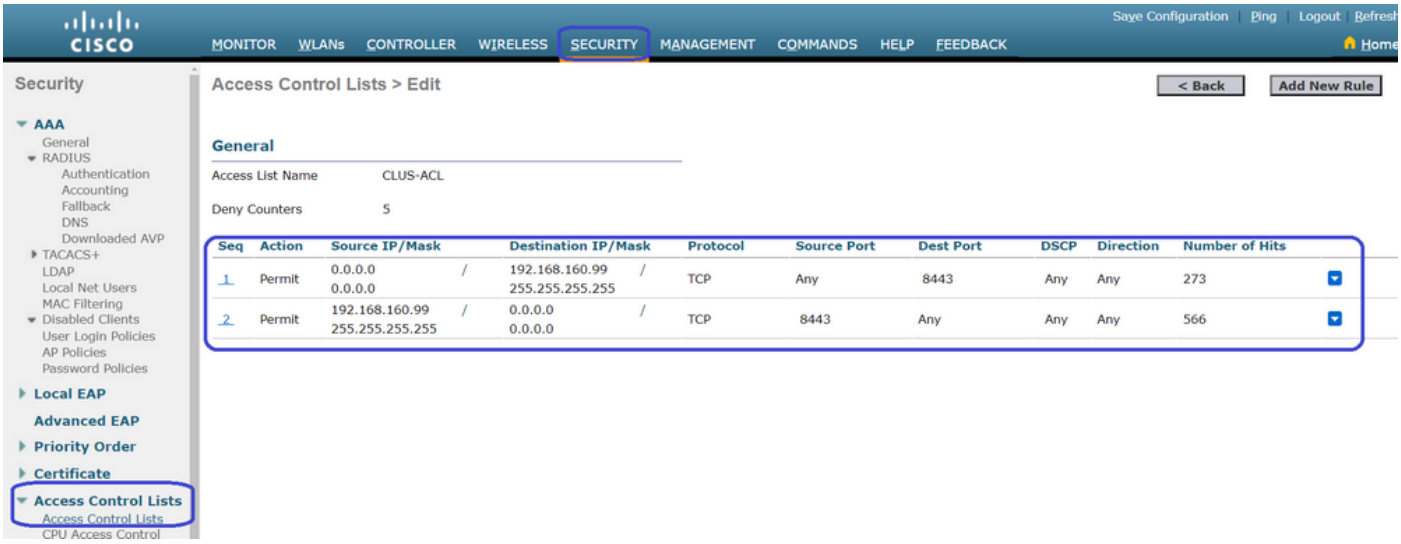
Lo último es anclarlo a sí mismo. Para ello, vuelva a la página **WLANs** y pase el cursor sobre el cuadro azul de la derecha de WLAN>Mobility Anchors. Establezca "Cambiar dirección IP (delimitador)" en local y pulse el botón "Crear anclaje de movilidad". Luego debe aparecer con prioridad 0 anclada local.



Redirigir ACL en el WLC AireOS

Esta es la configuración final necesaria en el WLC AireOS. Para crear la ACL de redirección, vaya a **Security>Access Control Lists>Access Control Lists>New**. Introduzca el nombre de la ACL (debe coincidir con lo que se envía en los AVP) y pulse "Aplicar".

Ahora haga clic en el nombre de la ACL que acaba de crear. Haga clic en el botón "Agregar nueva regla". A diferencia del controlador 9800, en el WLC AireOS, usted configura una sentencia permit para el tráfico que se permite alcanzar ISE sin ser redirigido. DHCP y DNS se permiten de forma predeterminada.

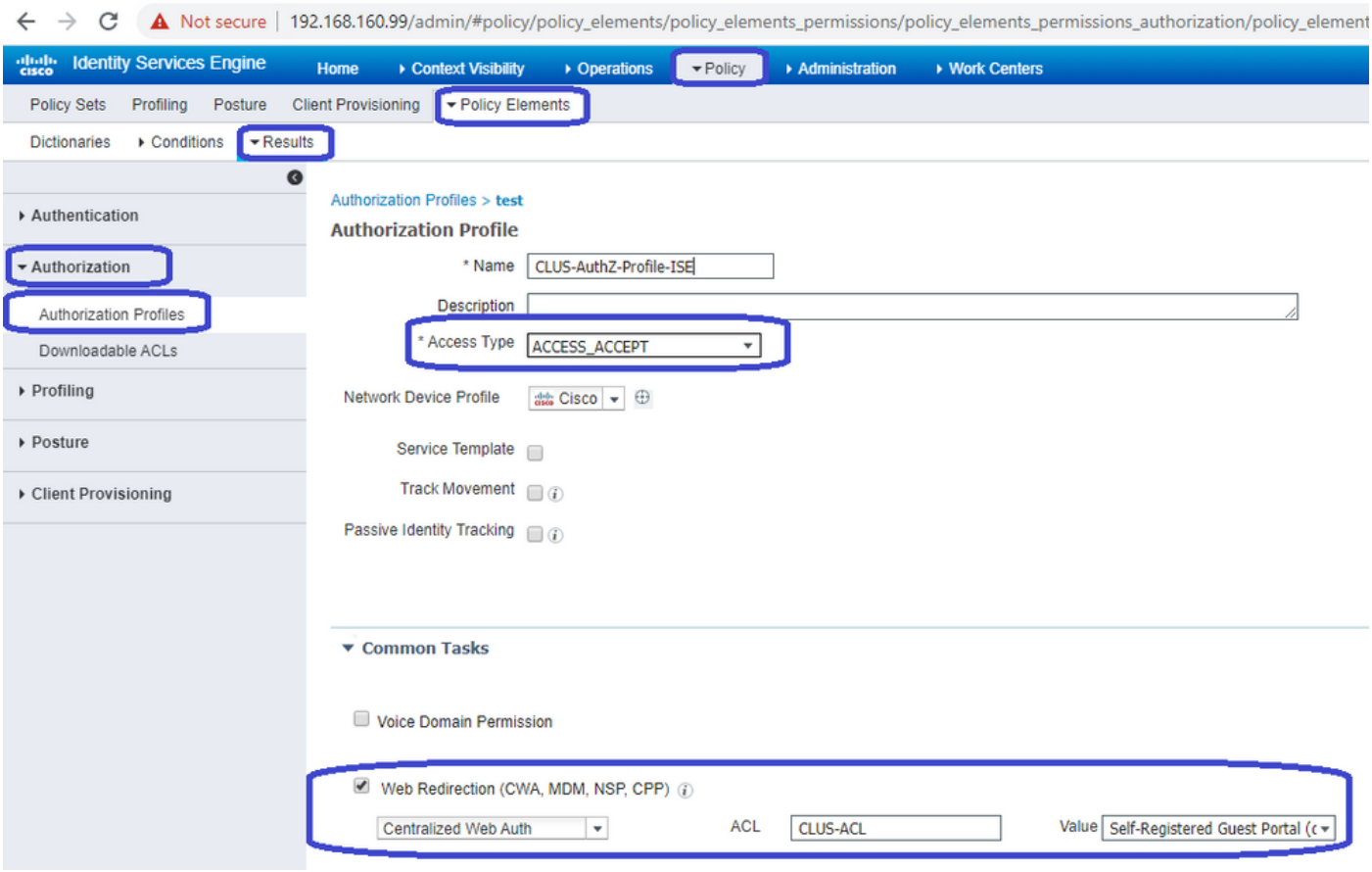


Configuración de ISE

El último paso es configurar ISE para CWA. Hay muchas opciones para esto, pero este ejemplo se ceñirá a lo básico y usará el portal de invitados autoregistrado predeterminado.

En ISE, debe crear un perfil de autorización, un conjunto de políticas con una política de autenticación y una política de autorización que utilice el perfil de autorización, agregar el 9800(external) a ISE como dispositivo de red y crear un nombre de usuario y una contraseña para iniciar sesión en la red.

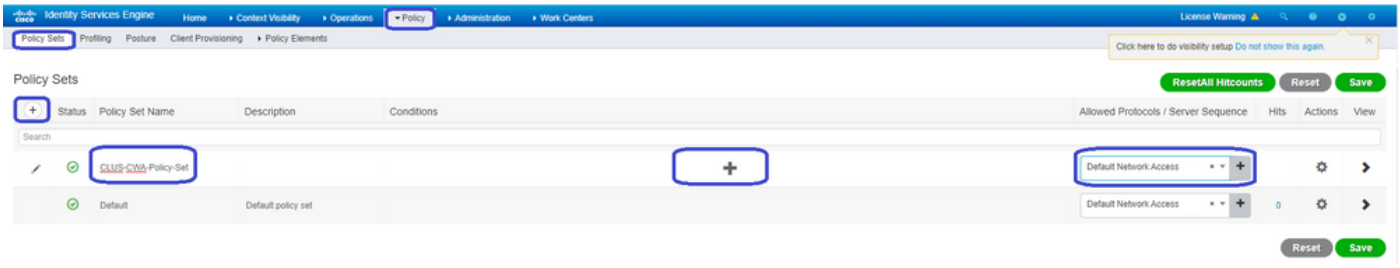
Para crear el perfil de autorización, vaya **aPolicy>Policy Elements>Authorization>Results>Authorization Profiles>+Add**. Asegúrese de que el tipo de acceso devuelto es "access_accept" y, a continuación, establezca los AVP(pares valor-atributo) que desea devolver. Para CWA, la ACL de redirección y la URL de redirección son obligatorias, pero también puede enviar cosas como el ID de VLAN y el tiempo de espera de sesión. Es importante que el nombre de la ACL coincida con el nombre de la ACL de redirección en el WLC externo y el WLC de anclaje.



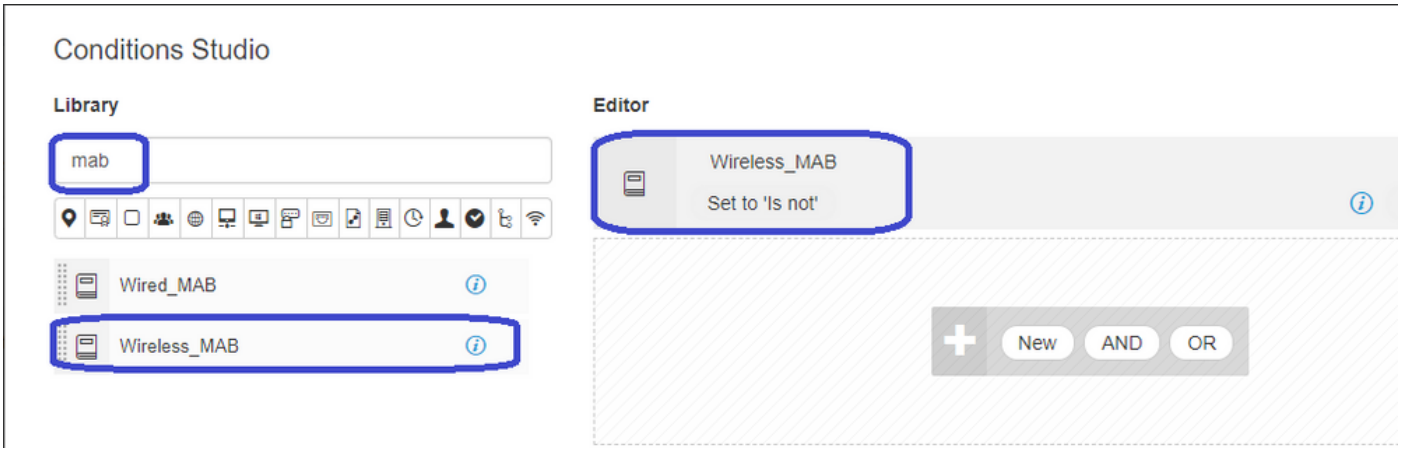
A continuación, debe configurar una forma de aplicar el perfil de autorización que acaba de crear a los clientes que pasan por

CWA. Para lograrlo, una manera es crear un conjunto de políticas que omite la autenticación cuando se usa MAB y aplicar el perfil de autorización cuando se usa el SSID enviado en el ID de estación llamada. De nuevo, hay muchas maneras de lograrlo, así que si necesita algo más específico o más seguro, esta es la forma más simple de hacerlo.

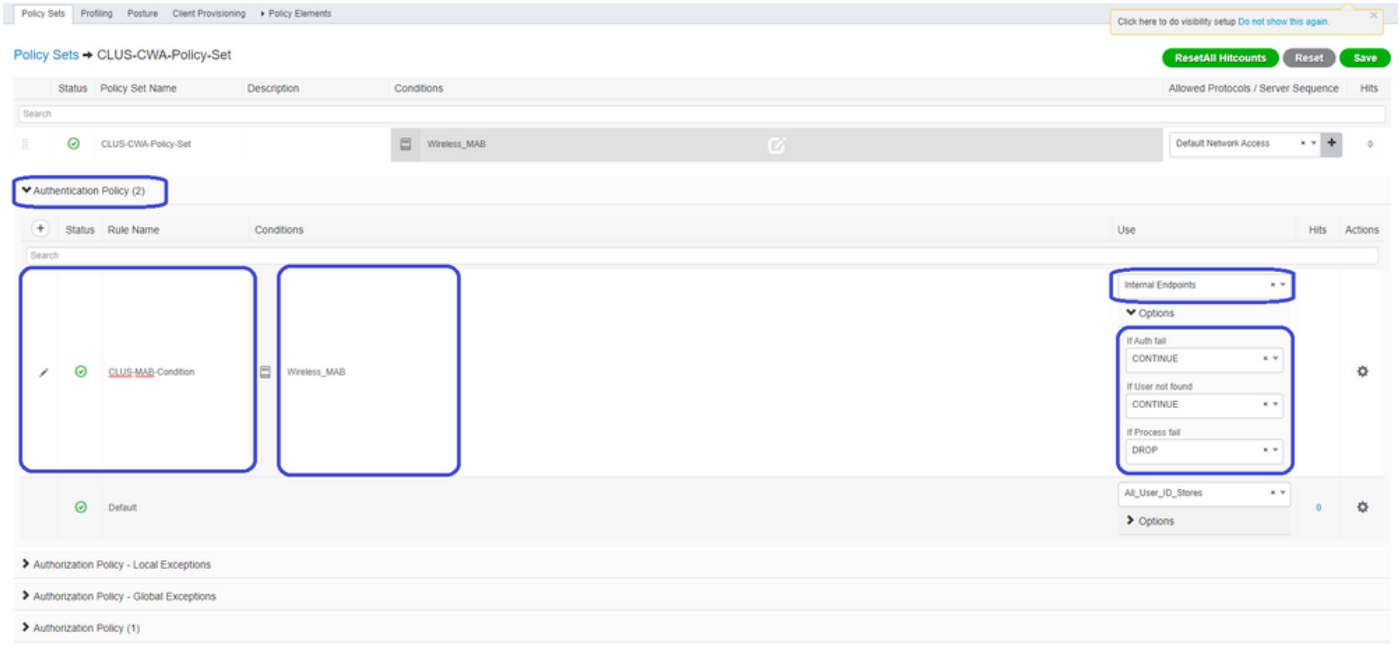
Para crear el conjunto de políticas, vaya **aPolicy>Policy** Settings y presione el botón + en el lado izquierdo de la pantalla. Asigne el nombre al nuevo conjunto de políticas y asegúrese de que esté configurado como "acceso a la red predeterminado" o cualquier lista de protocolos permitidos que permita "Búsqueda de host de procesos" para MAB(para verificar la lista de protocolos permitidos vaya a Política>Elementos de políticas>Resultados>Autenticación>Protocolos permitidos). Ahora, presione el signo + en medio del nuevo conjunto de políticas que creó.



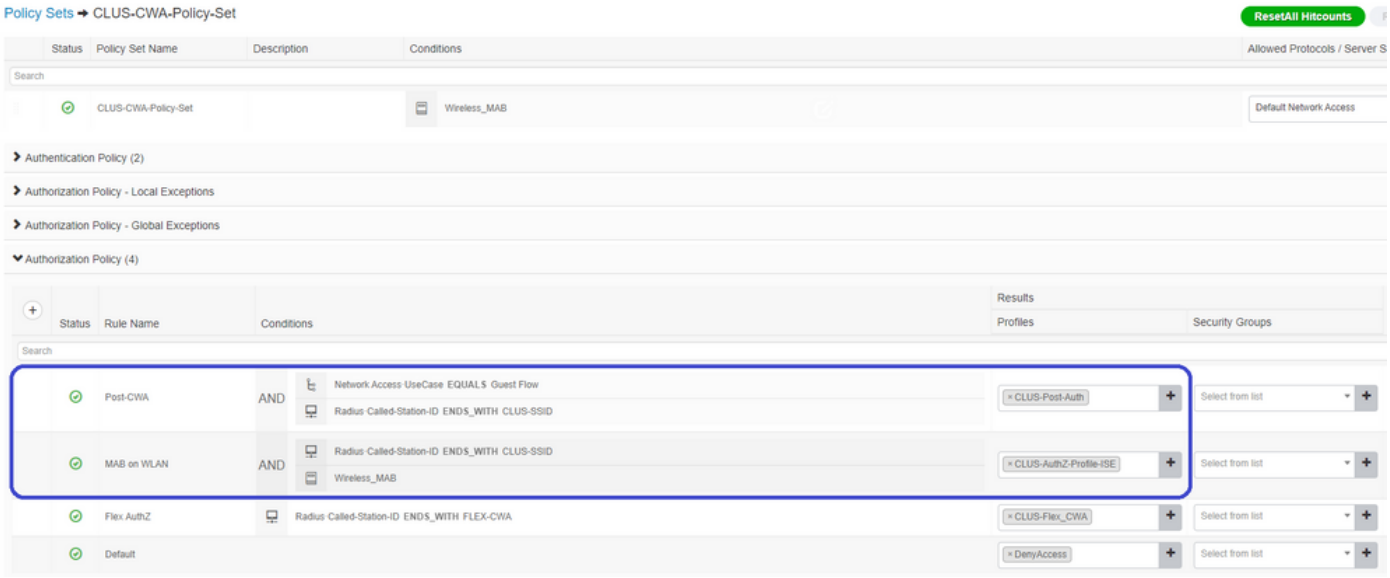
Para este conjunto de políticas cada vez que MAB se utiliza en ISE, pasará a través de este conjunto de políticas. Posteriormente, puede hacer políticas de autorización que coincidan con el ID de la estación llamada para que se puedan aplicar resultados diferentes dependiendo de la WLAN que se esté utilizando. Este proceso es muy personalizable con muchas cosas en las que puede
coincidir



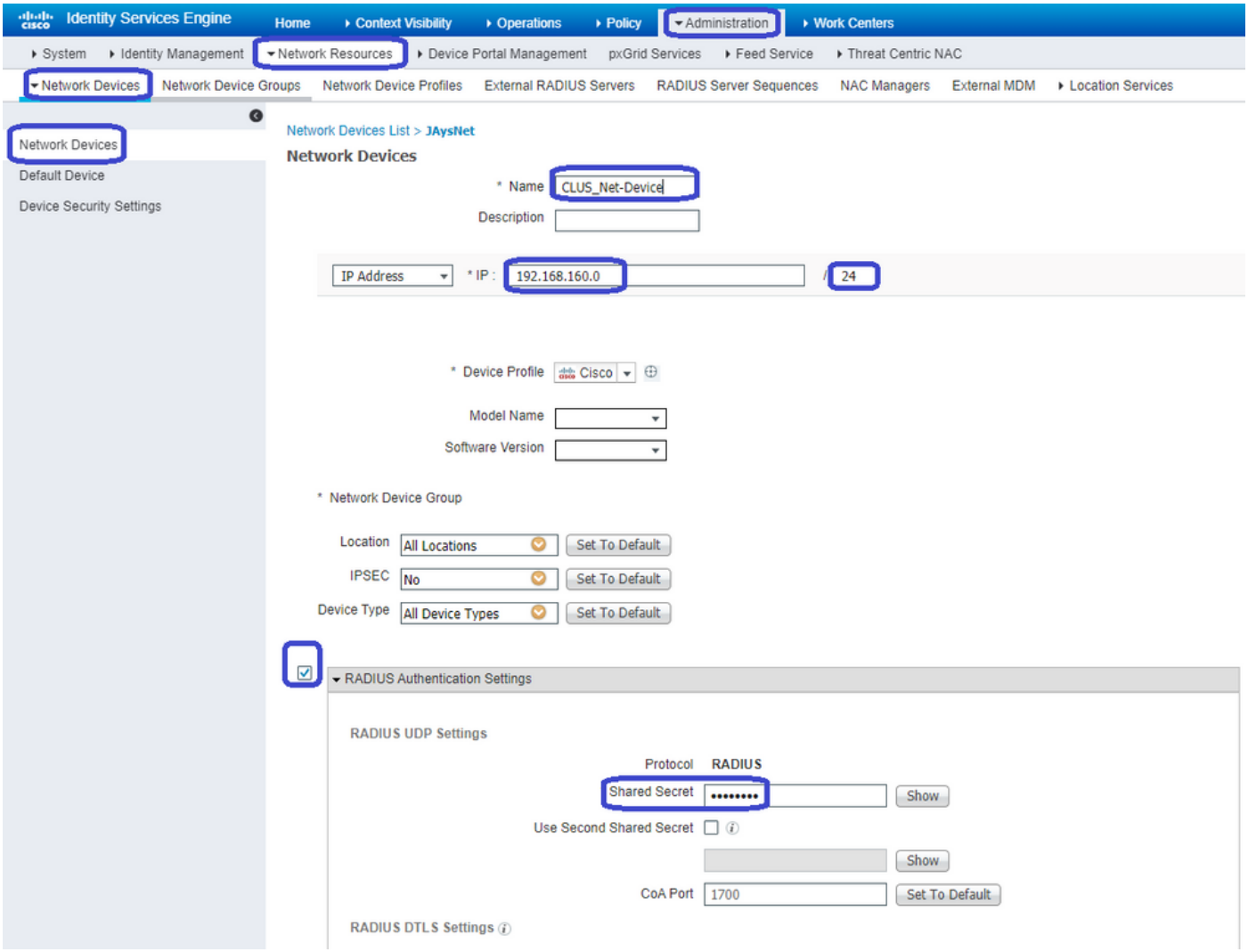
Dentro del conjunto de políticas , cree las políticas. La política de autenticación puede coincidir de nuevo en MAB, pero necesita cambiar el almacén de ID para utilizar "terminales internos" y debe cambiar las opciones para continuar con la autenticación de error y el usuario no encontrado.



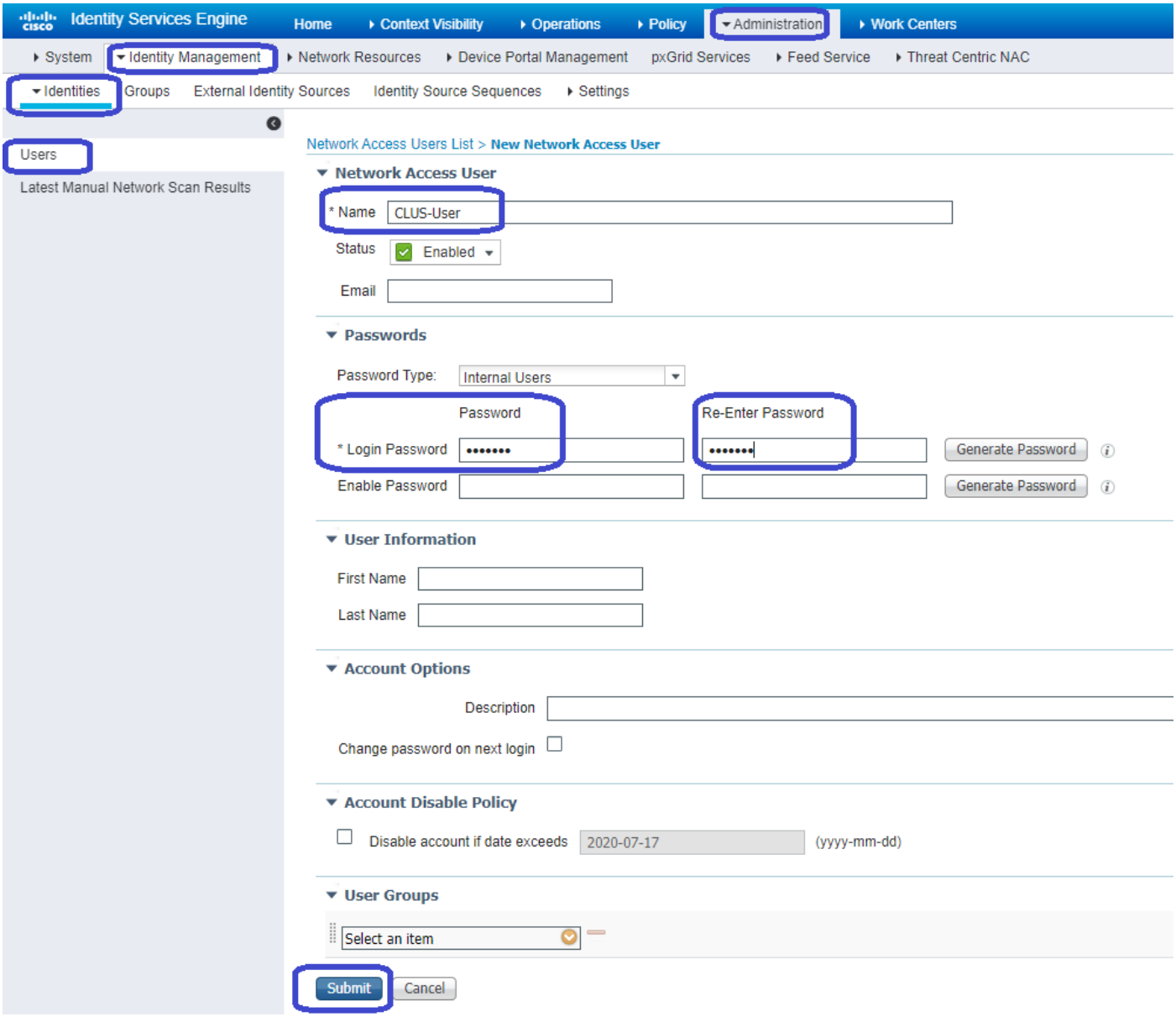
Una vez establecida la política de autenticación, debe crear dos reglas en la política de autorización. Esta política se lee como una ACL, por lo que el orden necesita tener la regla post-auth arriba y la regla pre-auth abajo. La regla posterior a la autenticación coincidirá con los usuarios que ya han pasado por guest-flow. Esto es para decir que si ya firmaron, golpearán esa regla y pararán ahí. Si no han iniciado sesión, continuarán por la lista y aplicarán la regla anterior a la autenticación obteniendo la redirección.Es una buena idea hacer coincidir las reglas de la política de autorización con el ID de la estación llamada que termina con el SSID para que sólo llegue a las WLAN configuradas para hacerlo.



Ahora que el conjunto de políticas está configurado, debe informar a ISE acerca del 9800 (Foreign) para que ISE confíe en él como un autenticador. Esto se puede hacer en**Admin>Recursos de red>Dispositivo de red>**+. Debe asignarle un nombre, establecer la dirección IP (o, en este caso, toda la subred de administración), activar RADIUS y establecer el secreto compartido. El secreto compartido en ISE debe coincidir con el secreto compartido en el 9800 o este proceso fallará. Después de agregar la configuración, pulse el botón enviar para guardarla.



Finalmente, deberá agregar el nombre de usuario y la contraseña que el cliente ingresará en la página de inicio de sesión para validar que deben tener acceso a la red. Esto se hace en**Admin>Identity Management>Identity>Users>+Add**y asegúrese de enviar después de agregarlo. Al igual que todo lo demás con ISE, esto es personalizable y no tiene que ser un usuario almacenado localmente, pero, de nuevo, es la configuración más sencilla.



Diferencias en la configuración cuando el WLC de AireOS es el externo y el Catalyst 9800 es el ancla

Si desea que el WLC de AireOs sea el controlador externo, la configuración es la misma que antes con sólo dos diferencias.

1. La contabilidad AAA nunca se realiza en el anclaje, por lo que el 9800 no tendría una lista de métodos contables y el WLC AireOS tendría la contabilización habilitada y apuntando a ISE.
2. El AireOS tendría que anclar al 9800 en lugar de a sí mismo. En el perfil de política, el 9800 no tendría un anclaje seleccionado pero tendría la casilla "Exportar anclaje" activada.
3. Es importante tener en cuenta que cuando los WLC de AireOS exportan el cliente al 9800, no hay concepto de perfiles de política, envía solamente el Nombre del Perfil de WLAN. Por lo tanto, el 9800 aplicará el Nombre del Perfil WLAN enviado desde AireOS tanto al Nombre del Perfil WLAN como al Nombre del Perfil de Política. Eso dijo que cuando se anclan de un WLC AireOS a un WLC 9800, el Nombre del Perfil WLAN en ambos WLC y el Nombre del Perfil de Política en el 9800, todos deben coincidir.

Verificación

Para verificar las configuraciones en el 9800 WLC ejecute los comandos

- AAA

```
Show Run | section aaa|radius
```

- WLAN

```
Show wlan id <wlan id>
```

- Perfil de política

```
Show wireless profile policy detailed <profile name>
```

- Etiqueta de política

```
Show wireless tag policy detailed <policy tag name>
```

- ACL

```
Show IP access-list <ACL name>
```

- Verificar que la movilidad esté a la altura del ancla

```
Show wireless mobility summary
```

Para verificar las configuraciones en el WLC AireOS ejecute los comandos

- AAA

```
Show radius summary
```

Nota: RFC3576 es la configuración de CoA

- WLAN

```
Show WLAN <wlan id>
```

- ACL

```
Show acl detailed <acl name>
```

- Verificar que la movilidad esté a la altura de lo que ocurre en el extranjero

```
Show mobility summary
```

Troubleshoot

La resolución de problemas tiene un aspecto diferente en función del punto del proceso que detenga el cliente. Por ejemplo, si el WLC nunca obtiene una respuesta de ISE en MAB, el cliente se quedaría atascado en el "Estado del Administrador de Políticas: Asociando" y no se exportaría al ancla. En esta situación, usted sólo resolvería problemas en el Foreign y podría recolectar un seguimiento de RA y una captura de paquetes para el tráfico entre el WLC y el ISE. Otro ejemplo sería que MAB ha pasado correctamente pero el cliente no recibe la redirección. En este caso,

debe asegurarse de que el extranjero recibió la redirección en los AVPs y la aplicó al cliente. También debe verificar el anclaje para asegurarse de que el cliente esté allí con la ACL correcta. Este alcance de la solución de problemas está fuera del diseño de este documento técnico (verifique las referencias de las pautas genéricas de troubleshooting del cliente).

Para obtener más ayuda con la solución de problemas de CWA en el WLC 9800, consulte Cisco Live. presentación DGTL-TSCENT-404

Información de Troubleshooting de Catalyst 9800

Detalles del cliente

`show wireless client mac-address`
Aquí debe ver el "Estado del administrador de políticas", "Administrador de sesiones>Método de autenticación", "Función de movilidad".

También puede encontrar esta información en la GUI en Monitoring>Clients

Captura de paquetes integrada

Desde la CLI, el comando inicia *#monitor capture <nombre de captura>* luego las opciones vienen después de eso.

Desde la GUI, vaya a Solucionar problemas>Captura de paquetes>+Agregar

Rastreo de RadioActive

Desde la CLI

`debug wireless mac|ip`
Utilice la forma no del comando para detenerlo. Esto se registrará en un archivo en la memoria flash de inicialización denominado "ra_trace", luego en la dirección MAC o IP del cliente y la fecha y hora.

Desde la GUI, vaya a Solucionar problemas>Seguimiento radiactivo>+Agregar. Agregue la dirección mac o ip del cliente, haga clic en apply y luego presione start. Después de haber pasado por el proceso varias veces, detenga el seguimiento, genere el registro y descárguelo en su dispositivo.

Información de resolución de problemas de AireOS

Detalles del cliente

Desde la CLI *show client details <client mac>*

Desde el monitor GUI>Clientes

Depuraciones desde la CLI

```
Debug client

Debug mobility handoff

Debug mobility config
```

Referencias

Creación de túneles de movilidad con 9800 controladores

Depuración inalámbrica y recopilación de registros en 9800