Configuración de la función de movilidad de anclaje WLAN en Catalyst 9800

Contenido

Introducción

Este documento describe cómo configurar una red de área local inalámbrica (WLAN) en un escenario externo/de anclaje con los controladores inalámbricos Catalyst 9800.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso mediante interfaz de línea de comandos (CLI) o interfaz gráfica de usuario (GUI) a los controladores inalámbricos
- Movilidad en los controladores de LAN inalámbrica (WLC) de Cisco
- Controladores inalámbricos 9800
- WLC de AireOS

Componentes Utilizados

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

- AireOS WLC versión 8.8 MR2 (también puede utilizar Inter Release Controller Mobility (IRCM) imágenes especiales 8.5)

- 9800 WLC v16.10 o posterior
- Modelo de configuración de 9800 WLC

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.

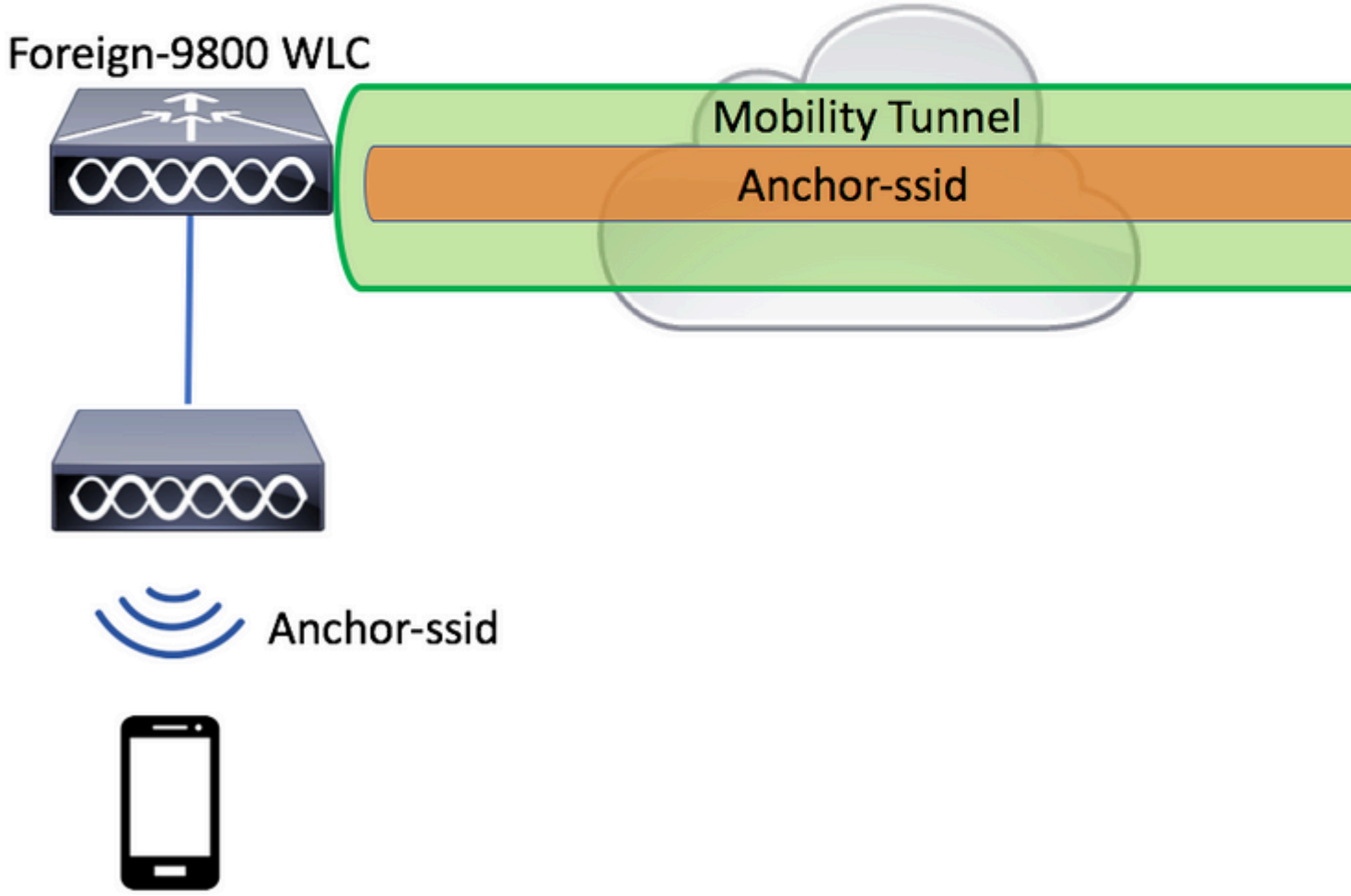
Configurar

Esta es una función que se utiliza normalmente para escenarios de acceso de invitado, para terminar todo el tráfico de los clientes en un único punto de salida L3, incluso si los clientes provienen de diferentes controladores y ubicaciones físicas. El túnel de movilidad proporciona un mecanismo para mantener el tráfico aislado mientras atraviesa la red.

Escenario externo/de anclaje entre 9800 WLC

Este escenario representa los dos Catalyst 9800 utilizados.

Diagrama de red: dos WLC Catalyst 9800



Para los escenarios de invitados de movilidad, existen dos funciones principales de controlador:

- Controlador externo: este WLC posee la capa 2 o el lado inalámbrico. Tiene puntos de acceso conectados. Todo el tráfico del cliente para las WLANs ancladas se encapsula en el túnel de movilidad para ser enviado al anclaje. No existe localmente.
- Controlador de anclaje: este es el punto de salida de la capa 3. Recibe los túneles de movilidad de los controladores externos y desencapsula o termina el tráfico del cliente en el punto de salida (VLAN). Este es el punto donde los clientes se ven en la red, por lo tanto el nombre del ancla.

Los puntos de acceso en el WLC externo difunden los SSID de WLAN y tienen una etiqueta de política asignada que enlaza el perfil WLAN con el perfil de política apropiado. Cuando un cliente inalámbrico se conecta a este SSID, el controlador externo envía ambos, el nombre SSID y el perfil de política como parte de la información del cliente al WLC de anclaje. Tras la recepción, el WLC de anclaje verifica su propia configuración para que coincida con el nombre SSID así como el nombre del perfil de política. Una vez que el WLC del ancla encuentra una coincidencia, aplica la configuración que corresponde a él y un punto de salida al cliente inalámbrico. Por lo tanto, es obligatorio que los nombres y las configuraciones de WLAN y

del perfil de política coincidan en el WLC 9800 externo y el WLC 9800 de anclaje con la excepción de VLAN en el perfil de política.

Nota: Los nombres del perfil WLAN y del perfil de política pueden coincidir en el 9800 Anchor y el 9800 Foreign WLC.

Configuración de un 9800 Foreign con un 9800 Anchor

Paso 1. Construya un túnel de movilidad entre el WLC Foreign 9800 y el WLC Anchor 9800.

Puede consultar este documento: Configuración de topologías de movilidad en Catalyst 9800

Paso 2. Cree el SSID deseado en ambos WLC 9800.

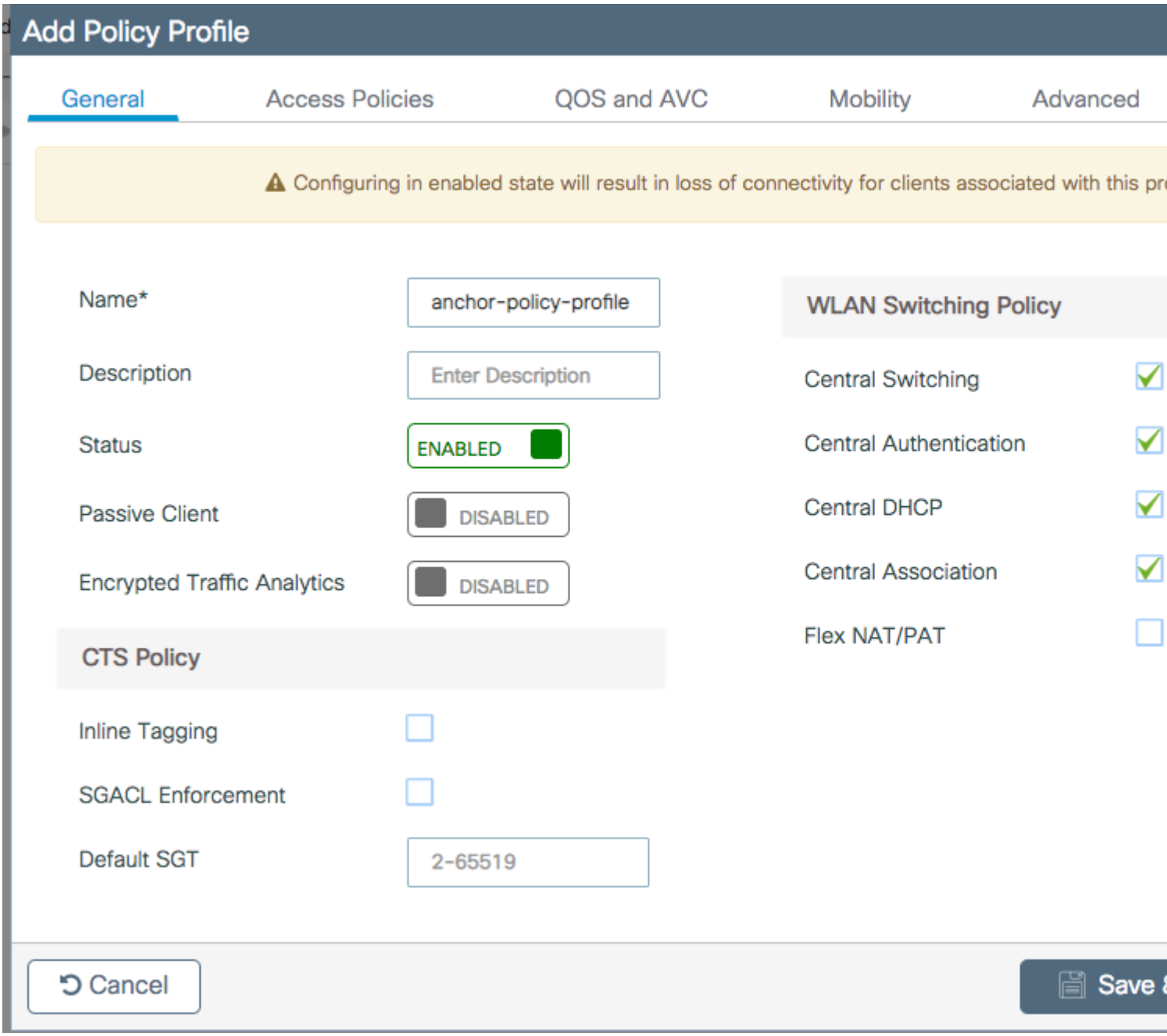
Métodos de seguridad admitidos:

- Abierto
- filtro MAC
- PSK
- Punto1x
- Autenticación web local/externa (LWA)
- Autenticación web central (CWA)

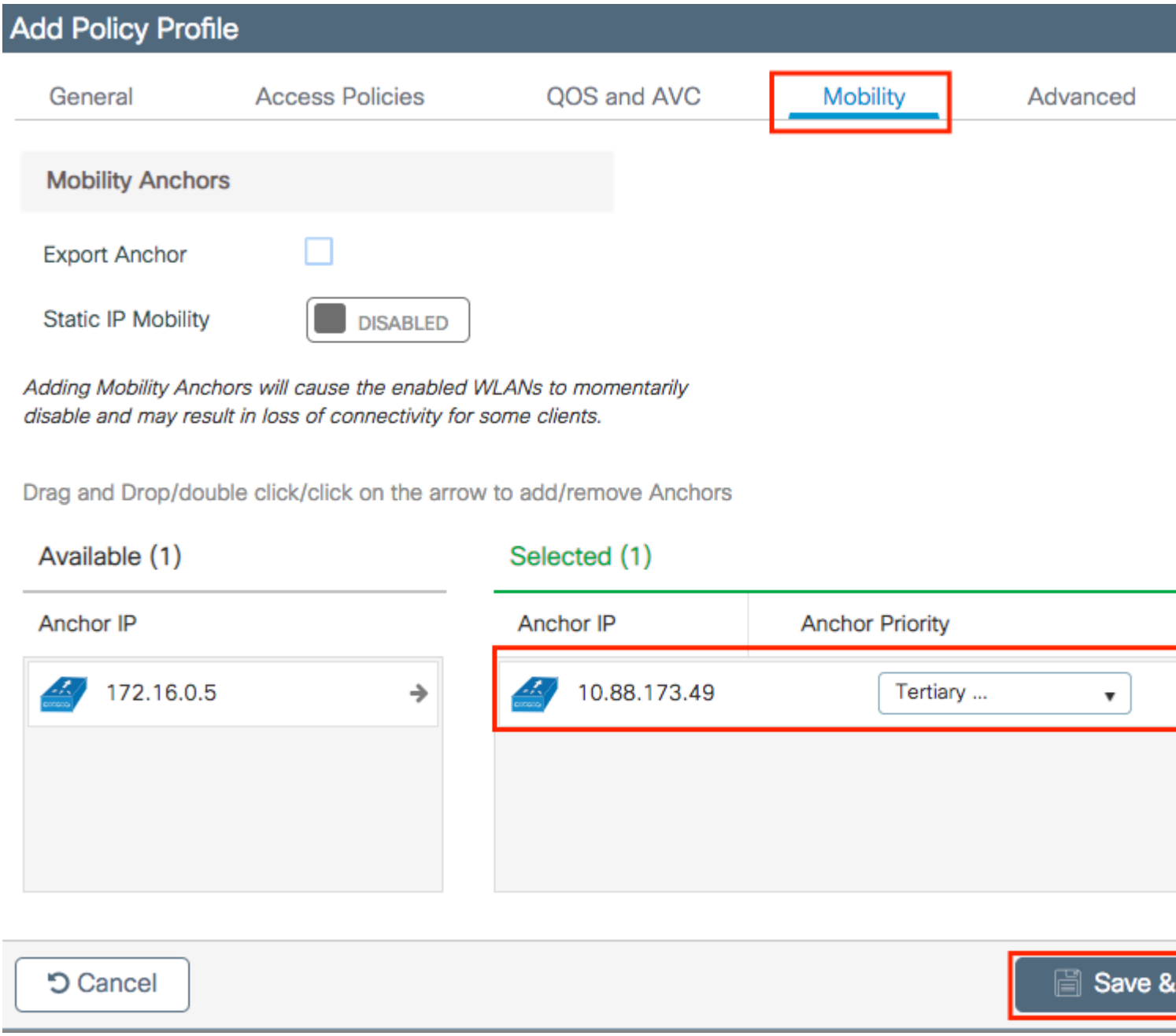
Nota: Ambos WLC 9800 deben tener el mismo tipo de configuración, de lo contrario el ancla no funciona.

Paso 3. Inicie sesión en el WLC 9800 externo y defina la dirección IP del WLC 9800 de anclaje en el perfil de política.

Desplácese hasta Configuration > Tags & Profiles > Policy > + Add.

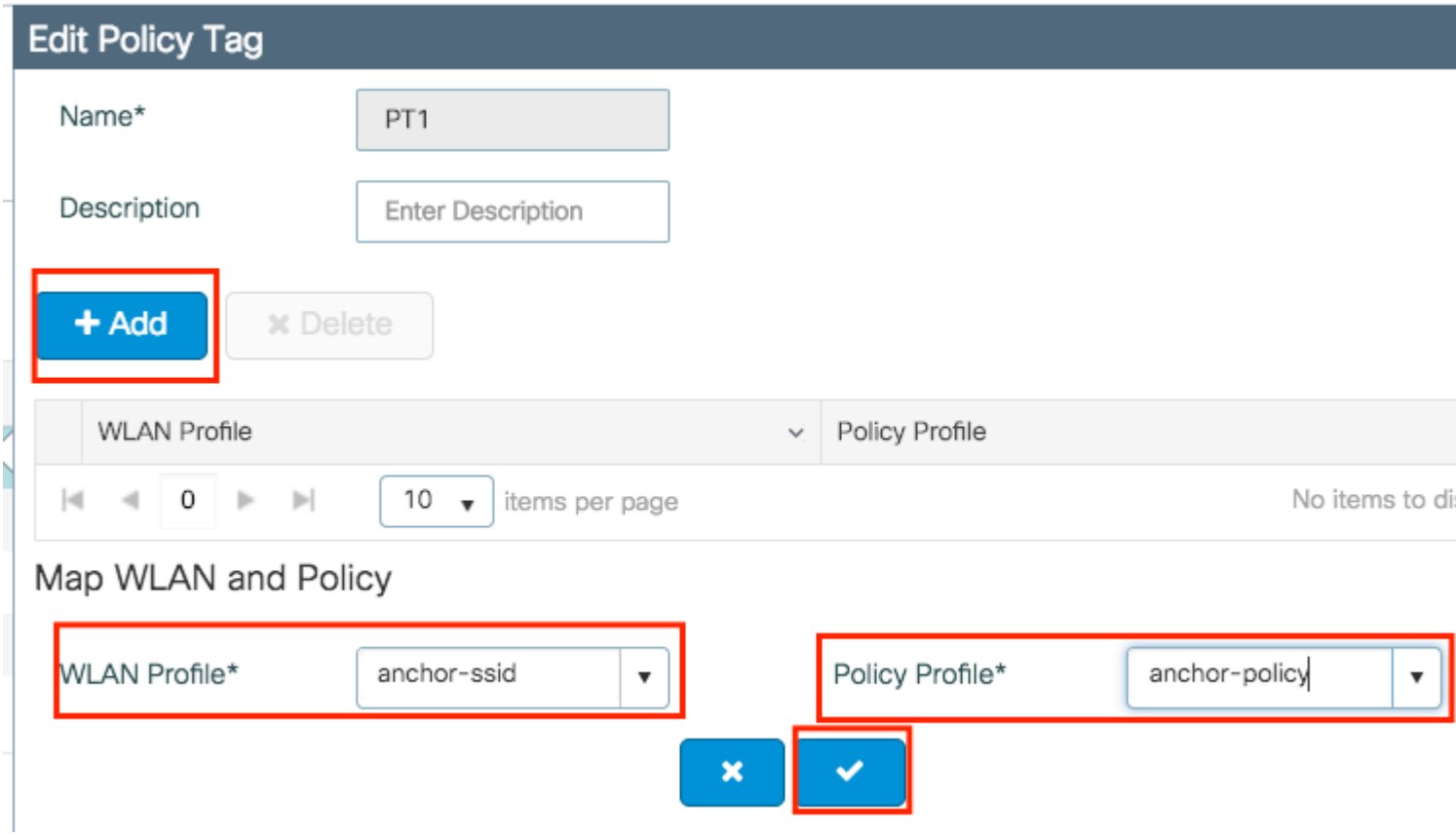


En el Mobility , elija la dirección IP del WLC 9800 de anclaje.

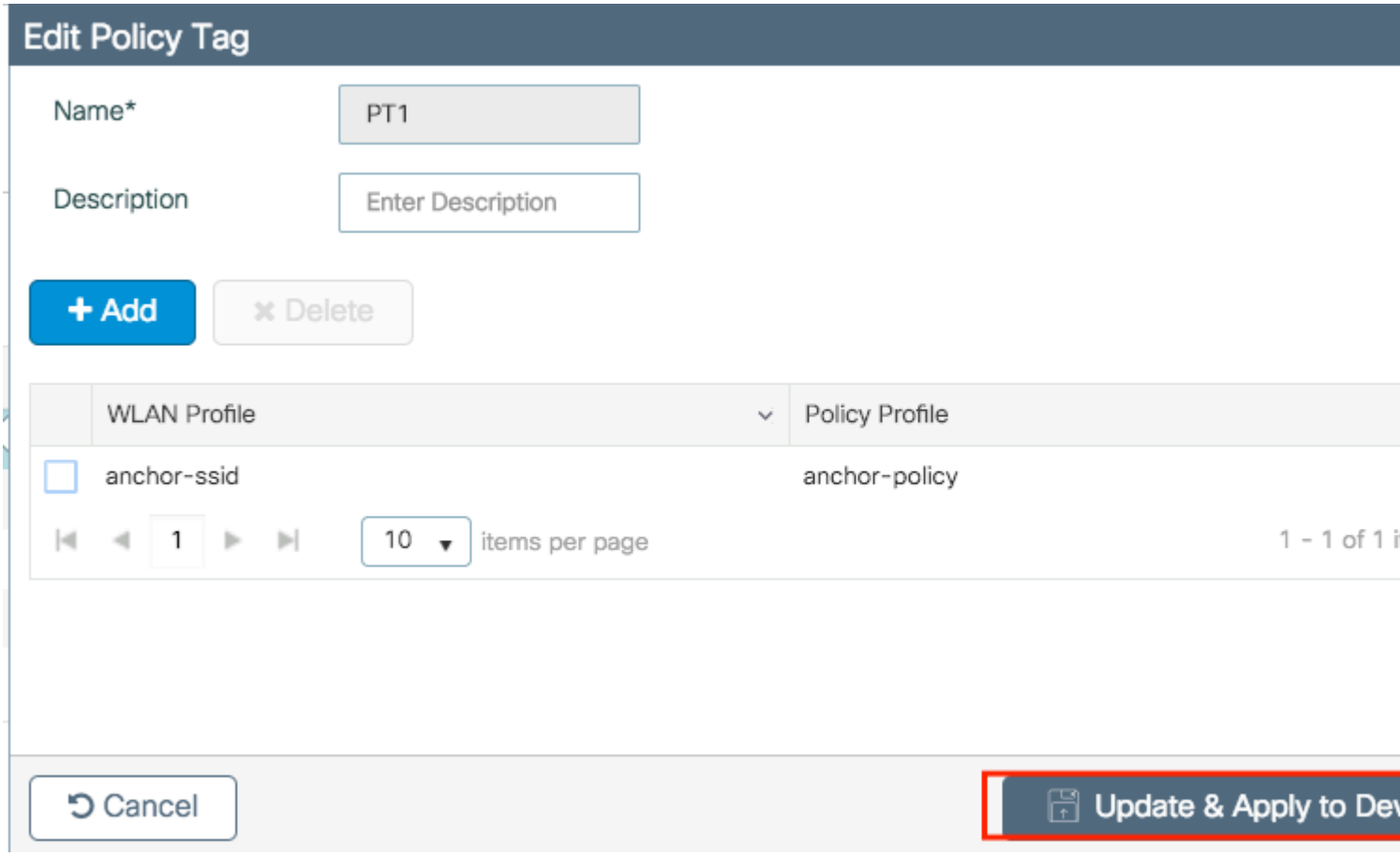


Paso 4. Enlace el perfil de política con la WLAN dentro de la etiqueta de política asignada a los AP asociados con el controlador externo que atiende a esta WLAN.

Desplácese hasta Configuration > Tags & Profiles > Tags y crear uno nuevo o utilizar el que existe.

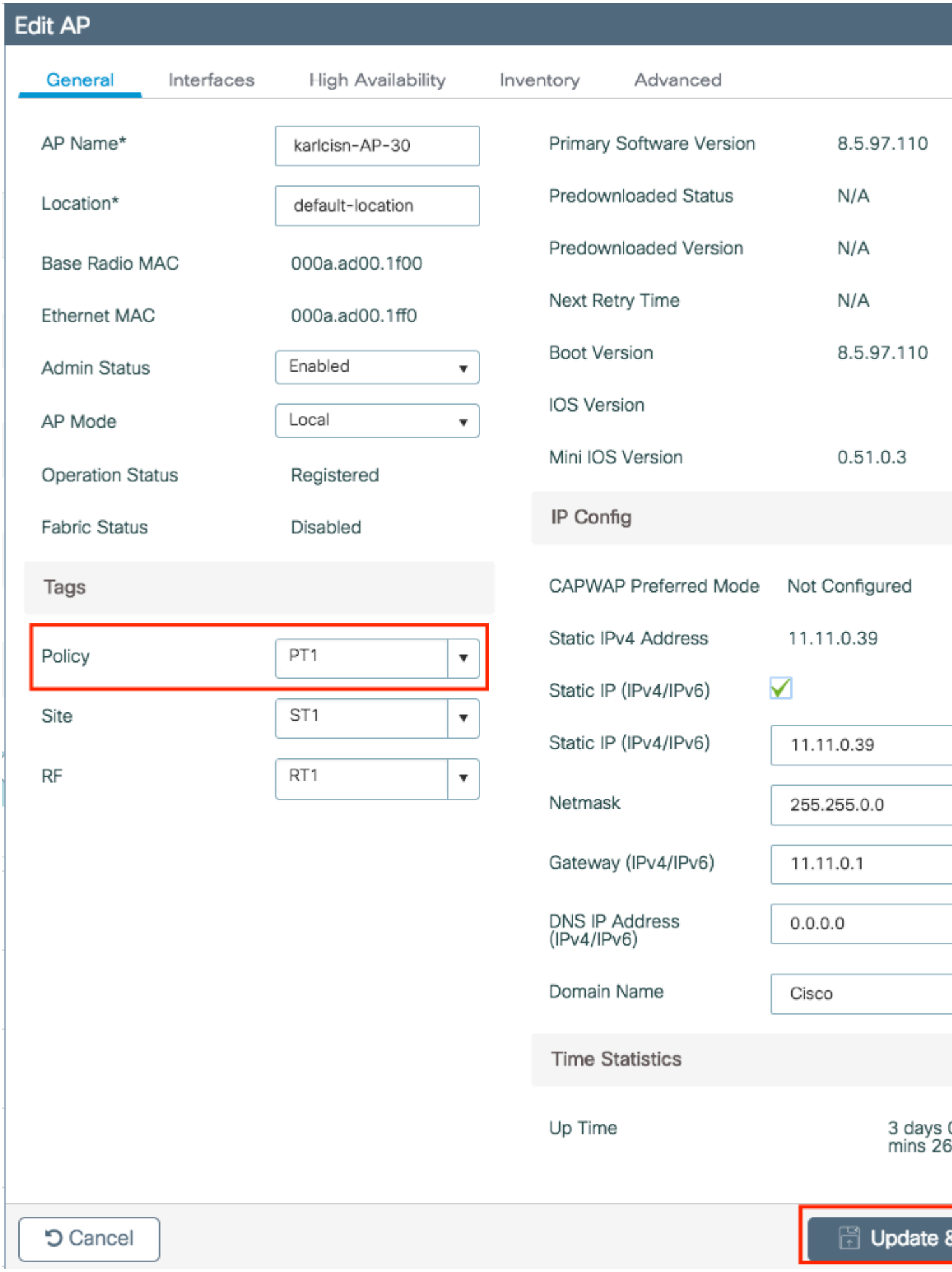


Asegúrese de elegir Update & Apply to Device para aplicar los cambios a la etiqueta de directiva.



Paso 5 (opcional). Asigne la etiqueta de política a un AP o verifique que ya la tiene.

Desplácese hasta Configuration > Wireless > Access Points > AP name > General.


Edit AP
General
Interfaces
High Availability
Inventory
Advanced
AP Name*
karlcisn-AP-30
Location*
default-location
Base Radio MAC
000a.ad00.1f00
Ethernet MAC
000a.ad00.1ff0
Admin Status
Enabled
AP Mode
Local
Operation Status
Registered
Fabric Status
Disabled
Tags
Policy
PT1
Site
ST1
RF
RT1
Primary Software Version
8.5.97.110
Predownloaded Status
N/A
Predownloaded Version
N/A
Next Retry Time
N/A
Boot Version
8.5.97.110
IOS Version
Mini IOS Version
0.51.0.3
IP Config
CAPWAP Preferred Mode
Not Configured
Static IPv4 Address
11.11.0.39
Static IP (IPv4/IPv6)
Static IP (IPv4/IPv6)
11.11.0.39
Netmask
255.255.0.0
Gateway (IPv4/IPv6)
11.11.0.1
DNS IP Address (IPv4/IPv6)
0.0.0.0
Domain Name
Cisco
Time Statistics
Up Time
3 days
mins 26
Cancel
Update

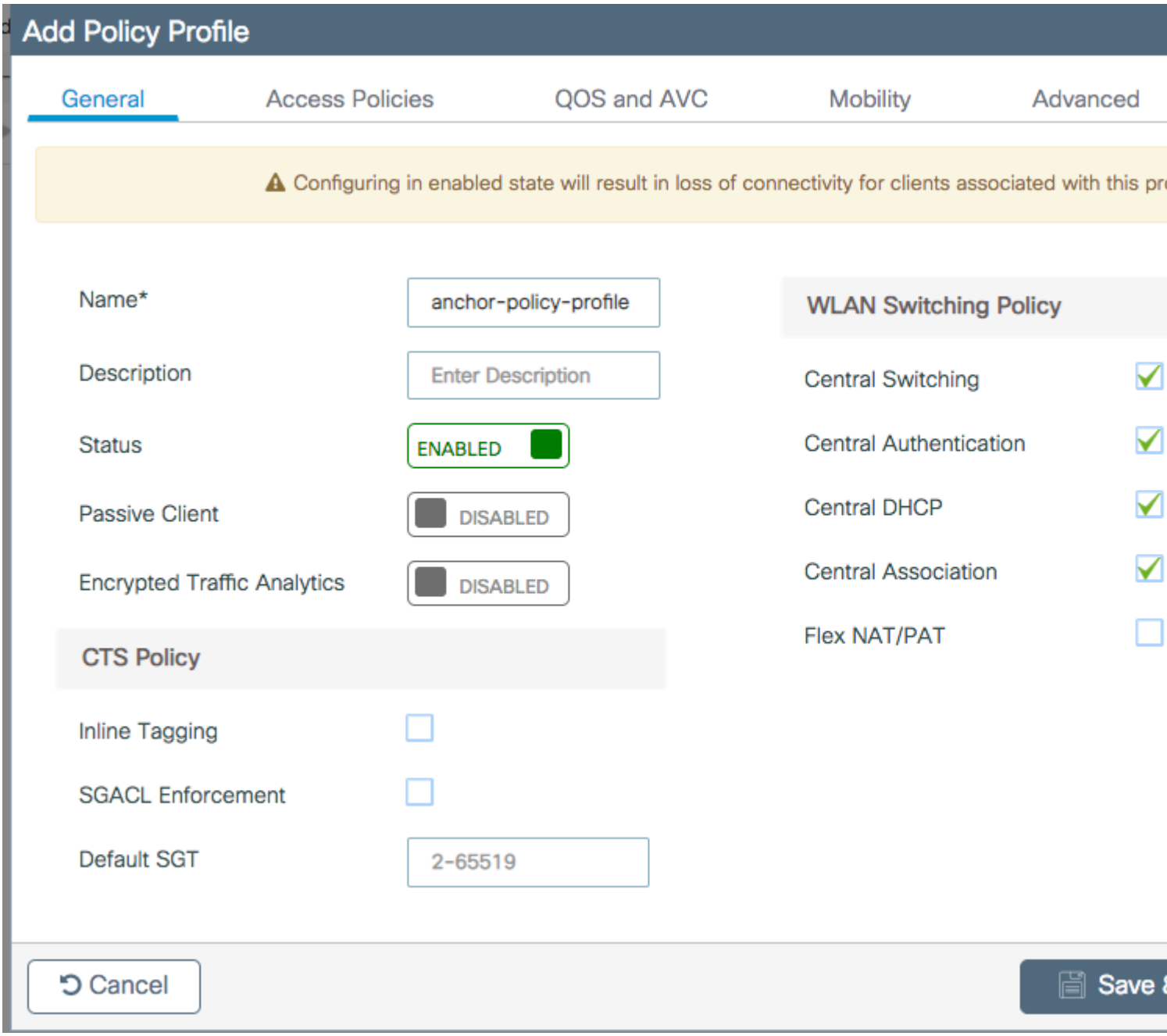
Nota: Tenga en cuenta que si realiza un cambio en la etiqueta AP después de elegir Update & Apply to Device, el AP reinicia su túnel CAPWAP, por lo que pierde la asociación con el WLC 9800 y luego lo recupera.

Desde la CLI:

```
Foreign 9800 WLC

# config t
# wireless profile policy anchor-policy
# mobility anchor 10.88.173.105 priority 3
# no shutdown
# exit

# wireless tag policy PT1
# wlan anchor-ssid policy anchor-policy
# exit

# ap aaaa.bbbb.dddd
# site-tag PT1
# exit
```

Paso 6. Inicie sesión en el WLC del ancla 9800 y cree el perfil de política de anclaje. Asegúrese de que tenga exactamente el mismo nombre que utilizó en los WLC 9800 extranjeros.

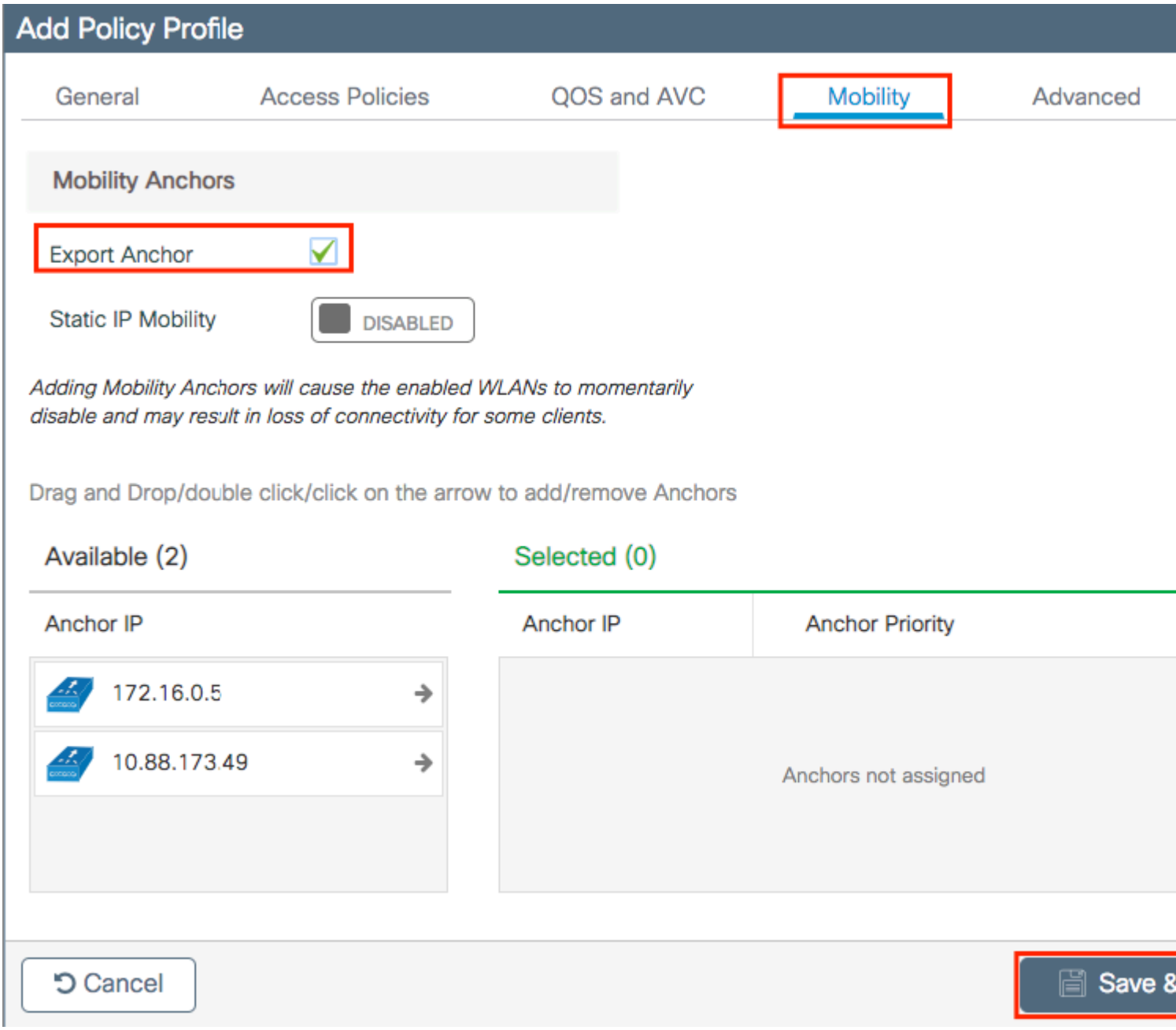
Desplácese hasta Configuration > Tags & Profiles > Policy > + Add.



Desplácese hasta Mobility y activar Export Anchor.Esto indica al WLC 9800 que es el WLC 9800 de anclaje para cualquier WLAN que utilice ese perfil de política. Cuando el WLC 9800 extranjero envía los clientes al WLC 9800 de anclaje, informa sobre la WLAN y el perfil de política al que está asignado el cliente, por lo que el WLC 9800 de anclaje sabe qué perfil de política local debe utilizar.

Nota: No debe configurar pares de movilidad y anclaje de exportación al mismo tiempo. Se trata de un escenario de configuración no válido.

Nota: No debe utilizar el parámetro Export Anchor para ningún perfil de política vinculado a un perfil WLAN en un controlador con puntos de acceso. Esto impide que se transmita el SSID, por lo que esta política debe utilizarse exclusivamente para la funcionalidad de anclaje.



Desde la CLI:

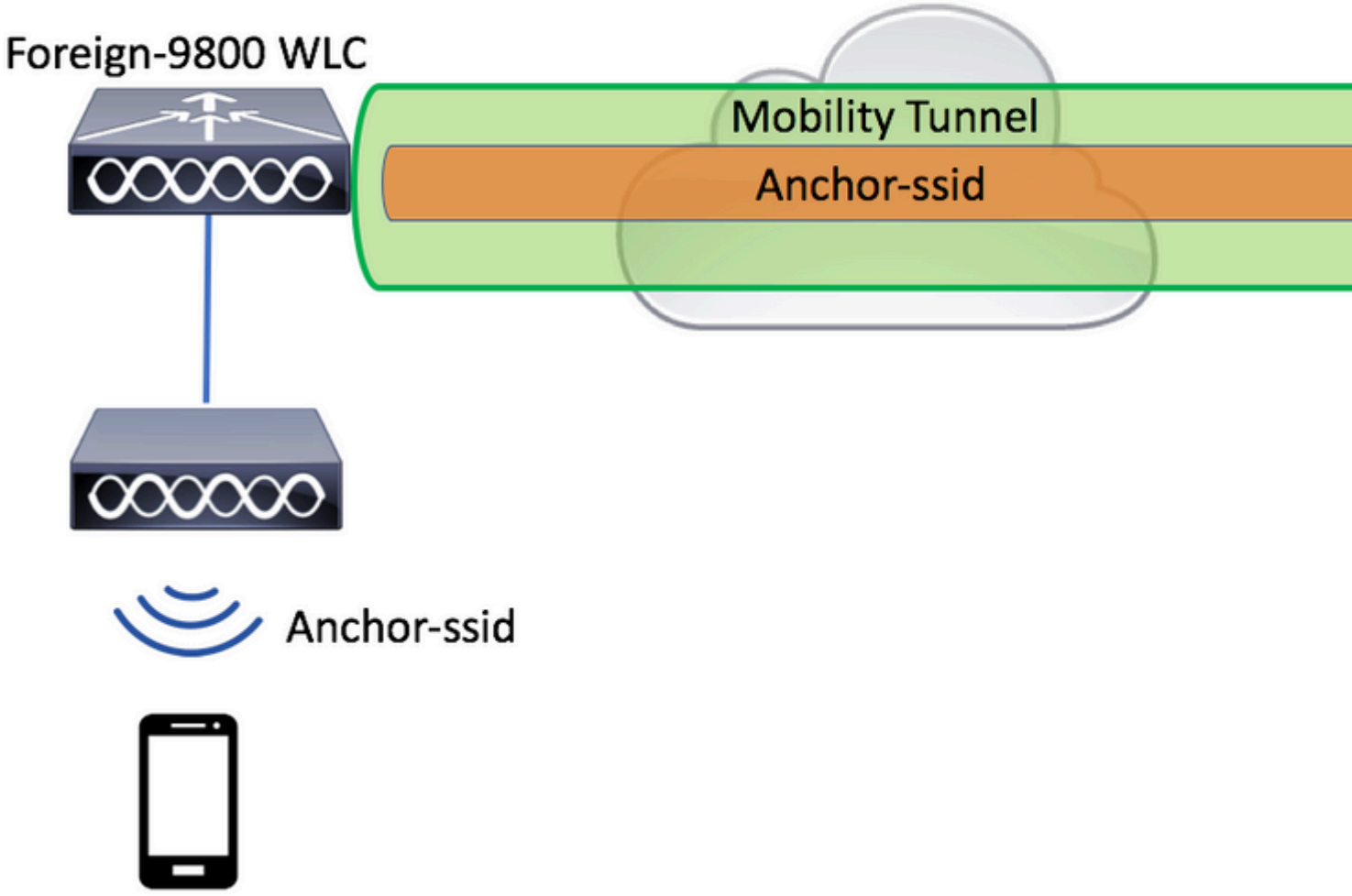
```
Anchor 9800 WLC

# config t
# wireless profile policy <anchor-policy>
# mobility anchor
# vlan <VLAN-id_VLAN-name>
# no shutdown
# exit
```

WLC Foreign 9800: Anchor AireOS

Esta configuración representa el escenario donde un WLC de Catalyst 9800 se utiliza como externo con un

WLC de AireOS Unified utilizado como anclaje.

Diagrama de red de anclaje de Catalyst 9800 externo - AireOS



Configuración de 9800 Foreign con AireOS Anchor

Paso 1. Construya un túnel de movilidad entre el WLC Foreign 9800 y el WLC Anchor AireOS.

Consulte este documento: Configuración de topologías de movilidad en Catalyst 9800

Paso 2. Cree las WLAN deseadas en ambos WLC.

Métodos de seguridad admitidos:

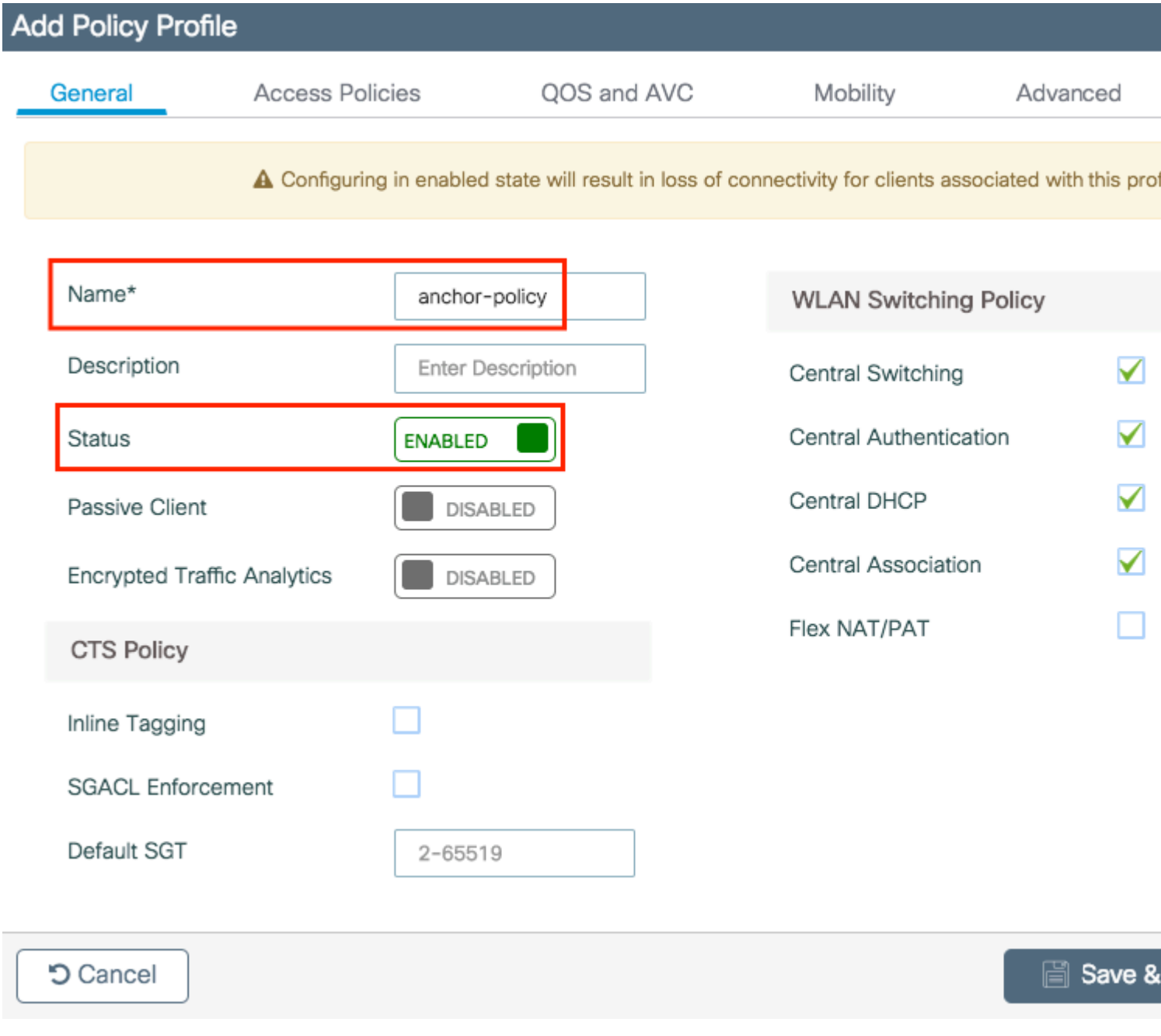
- Abierto

- filtro MAC
- PSK
- Punto1x
- Autenticación web local/externa (LWA)
- Autenticación web central (CWA)

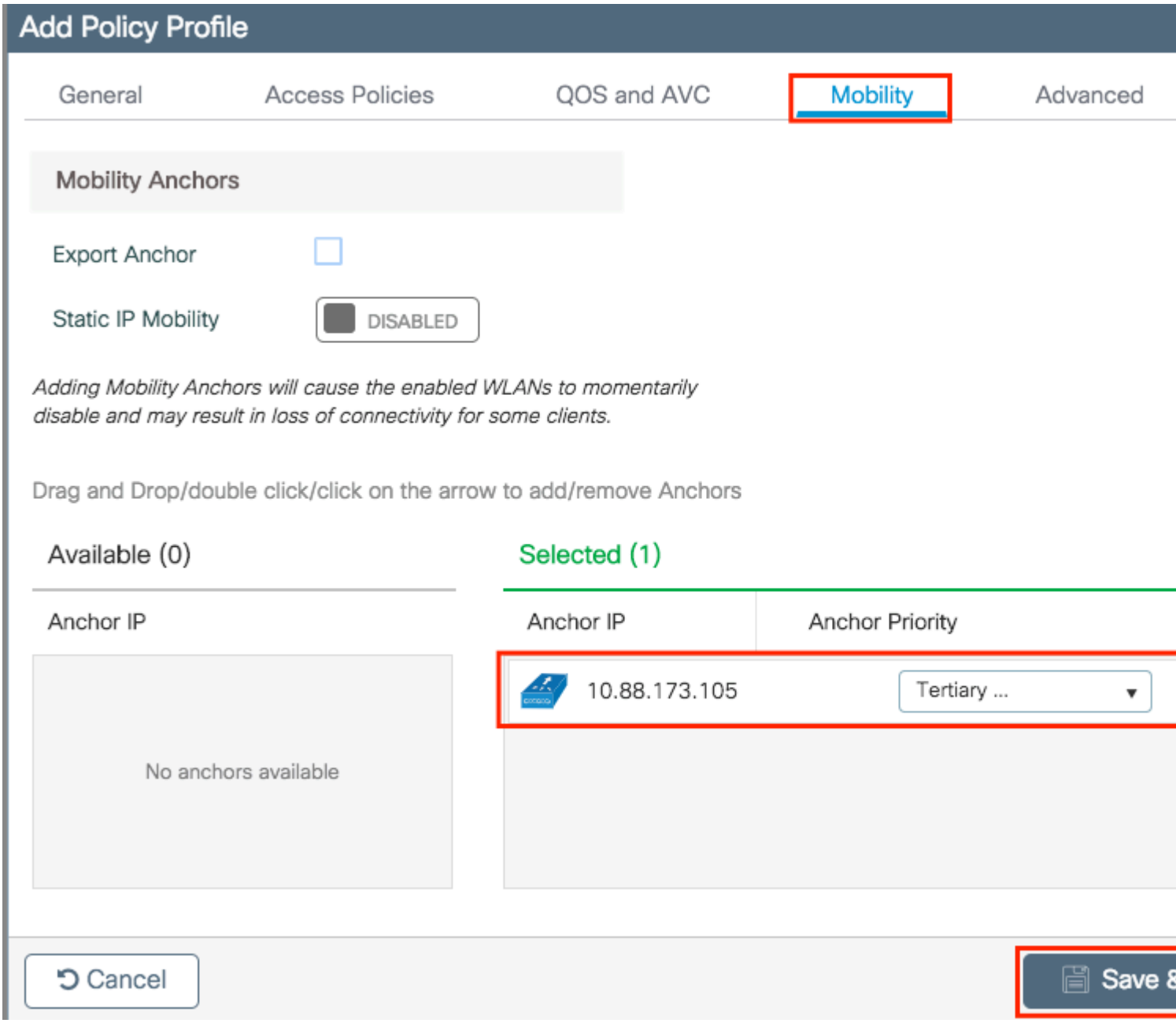
Nota: Tanto el WLC de AireOS como el WLC de 9800 deben tener el mismo tipo de configuración, de lo contrario el ancla no funciona.

Paso 3. Inicie sesión en el WLC 9800 (que actúa como externo) y cree el perfil de política de anclaje.

Desplácese hasta Configuration > Tags & Profiles > Policy > + Add .

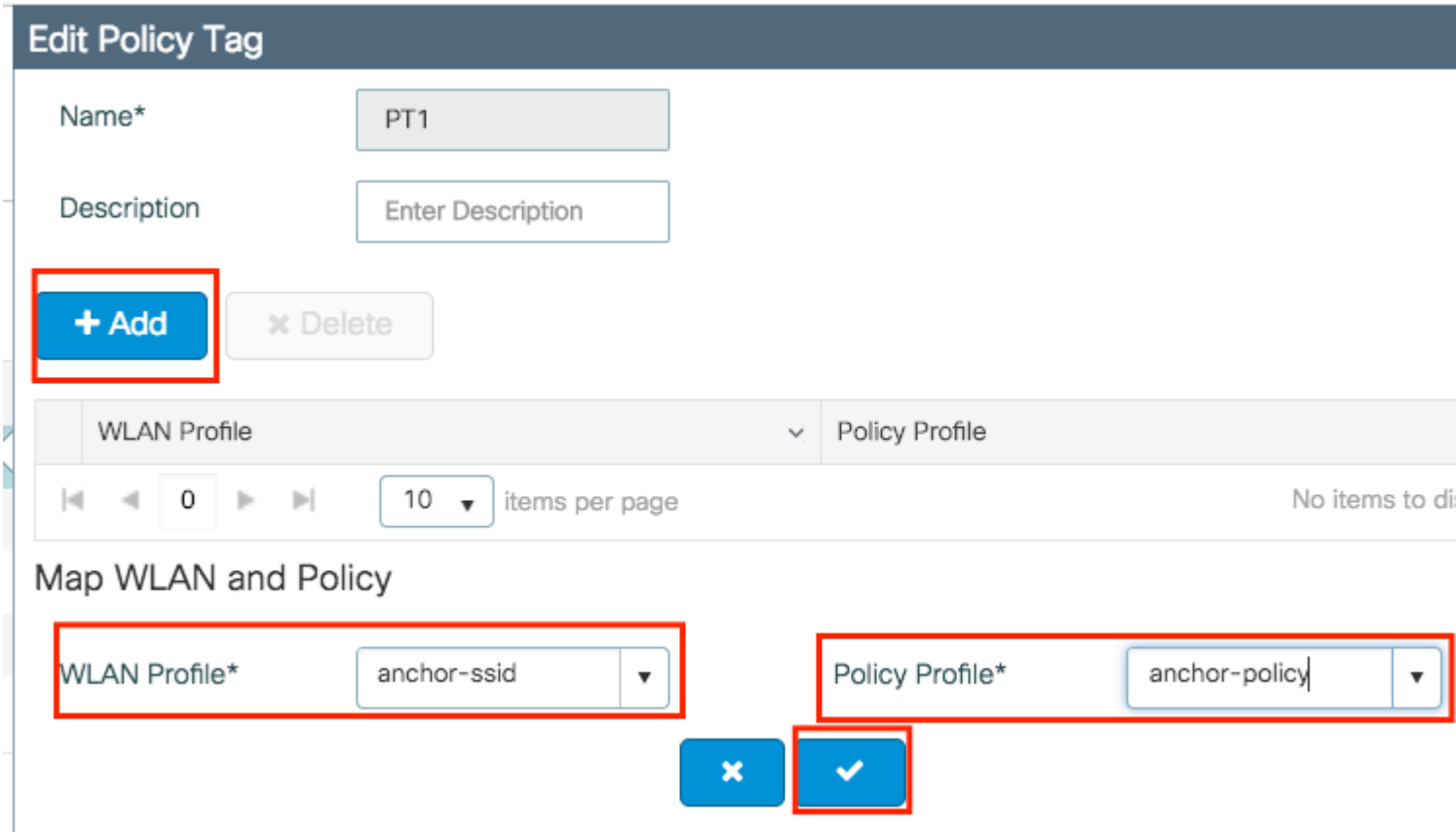


Desplácese hasta Mobility y elija el WLC AireOS ancla. El WLC 9800 reenvía el tráfico del SSID asociado con este perfil de política al anclaje elegido.

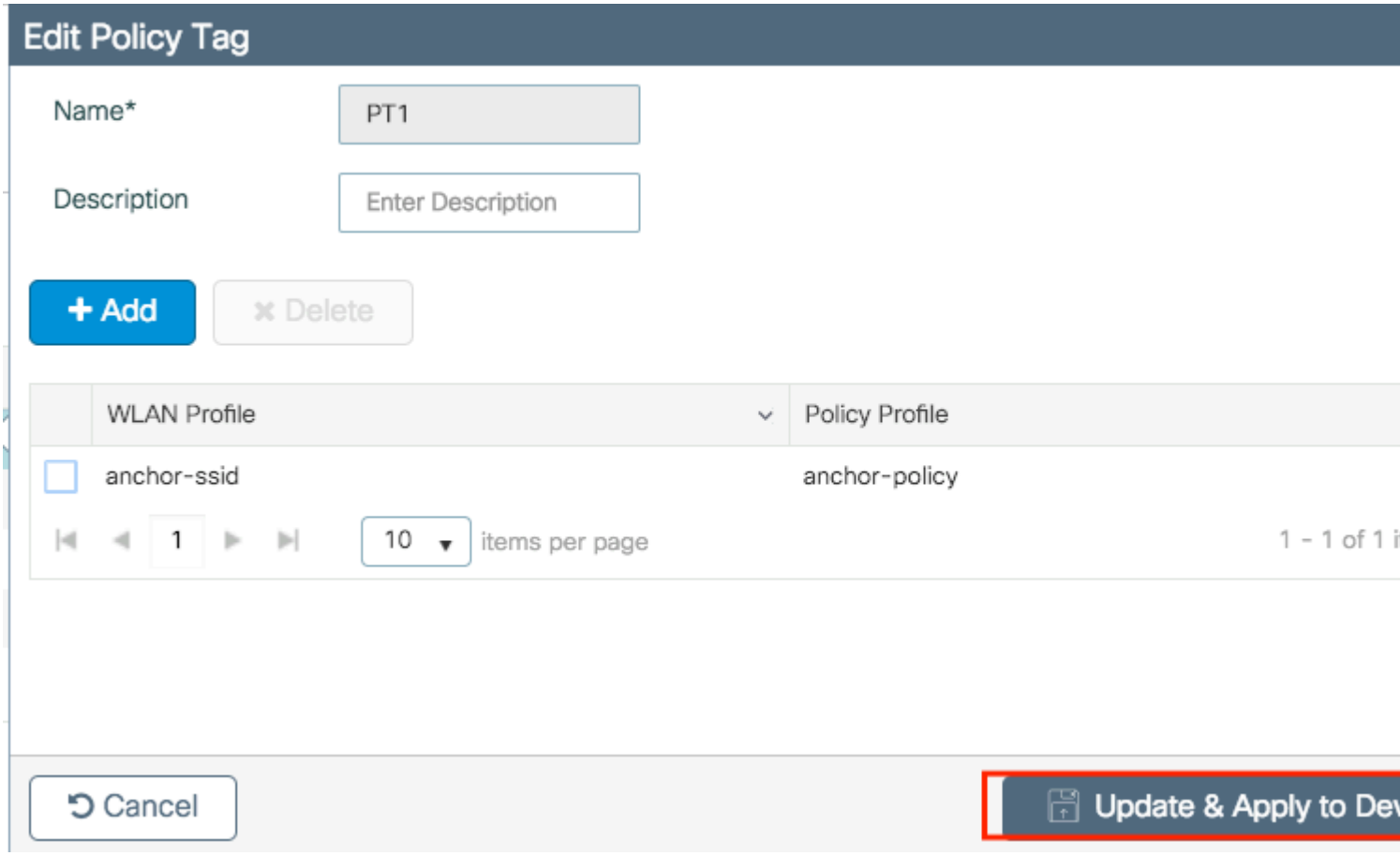


Paso 4. Enlace el perfil de política con la WLAN dentro de la etiqueta de política asignada a los AP asociados con el controlador externo que atiende a esta WLAN.

Desplácese hasta Configuration > Tags & Profiles > Tags y crear uno nuevo o utilizar el que existe.

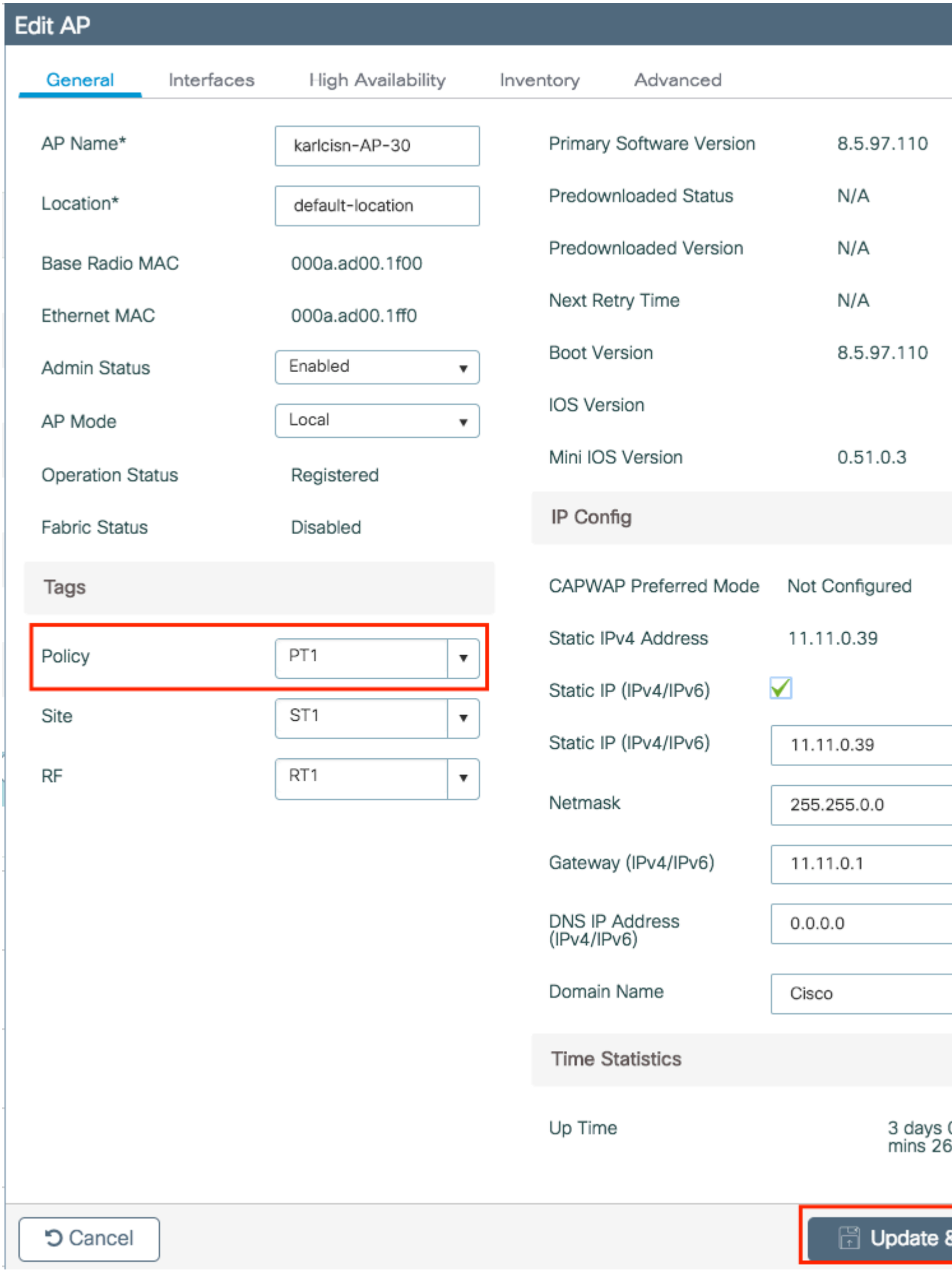


Asegúrese de elegir Update & Apply to Device para aplicar los cambios a la etiqueta de directiva.



Paso 5 (opcional). Asigne el sitio a un AP o verifique que ya lo tiene.

Desplácese hasta Configuration > Wireless > Access Points > AP name > General.


Edit AP
General
Interfaces
High Availability
Inventory
Advanced
AP Name*
karlcisn-AP-30
Location*
default-location
Base Radio MAC
000a.ad00.1f00
Ethernet MAC
000a.ad00.1ff0
Admin Status
Enabled
AP Mode
Local
Operation Status
Registered
Fabric Status
Disabled
Tags
Policy
PT1
Site
ST1
RF
RT1
Primary Software Version
8.5.97.110
Predownloaded Status
N/A
Predownloaded Version
N/A
Next Retry Time
N/A
Boot Version
8.5.97.110
IOS Version
Mini IOS Version
0.51.0.3
IP Config
CAPWAP Preferred Mode
Not Configured
Static IPv4 Address
11.11.0.39
Static IP (IPv4/IPv6)
Static IP (IPv4/IPv6)
11.11.0.39
Netmask
255.255.0.0
Gateway (IPv4/IPv6)
11.11.0.1
DNS IP Address (IPv4/IPv6)
0.0.0.0
Domain Name
Cisco
Time Statistics
Up Time
3 days
mins 26
Cancel
Update

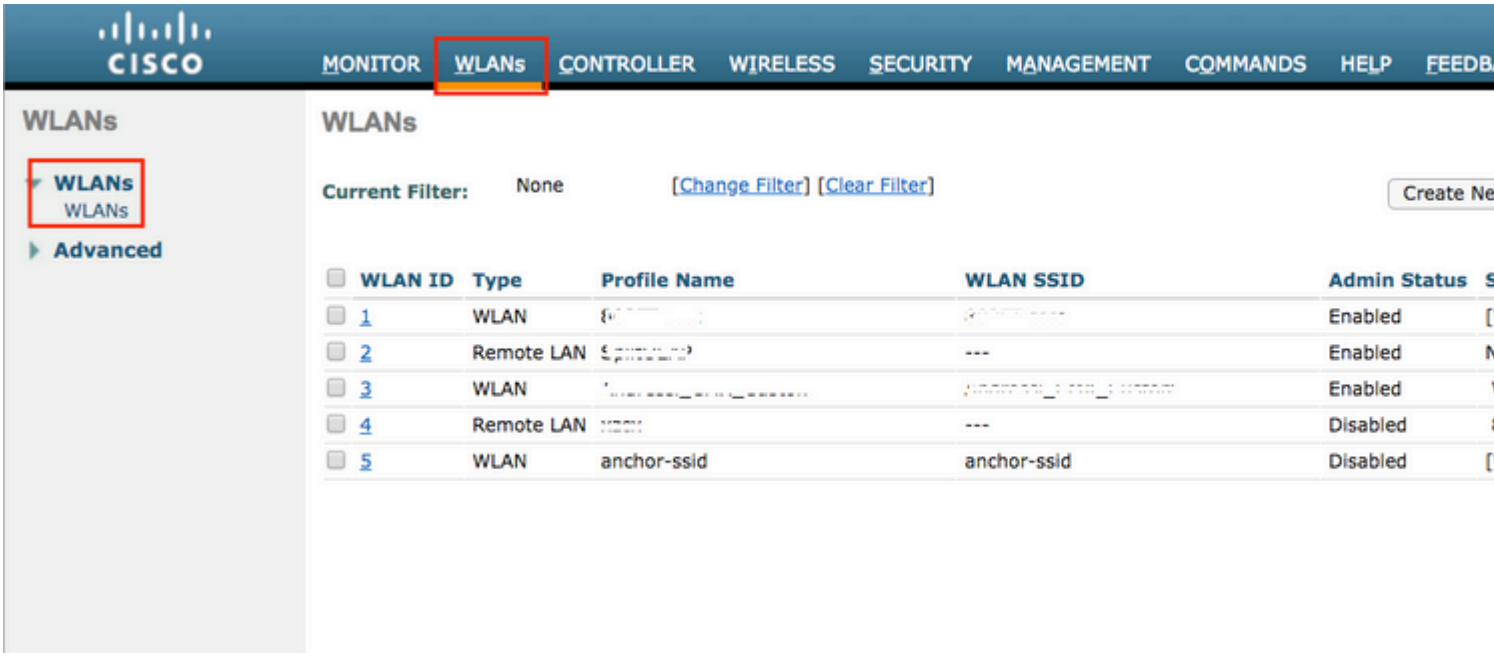
Nota: Tenga en cuenta que si realiza un cambio en la etiqueta AP después de elegir Update & Apply to Device, el AP reinicia su túnel CAPWAP, por lo que pierde la asociación con el WLC 9800 y luego lo recupera.

Desde la CLI:

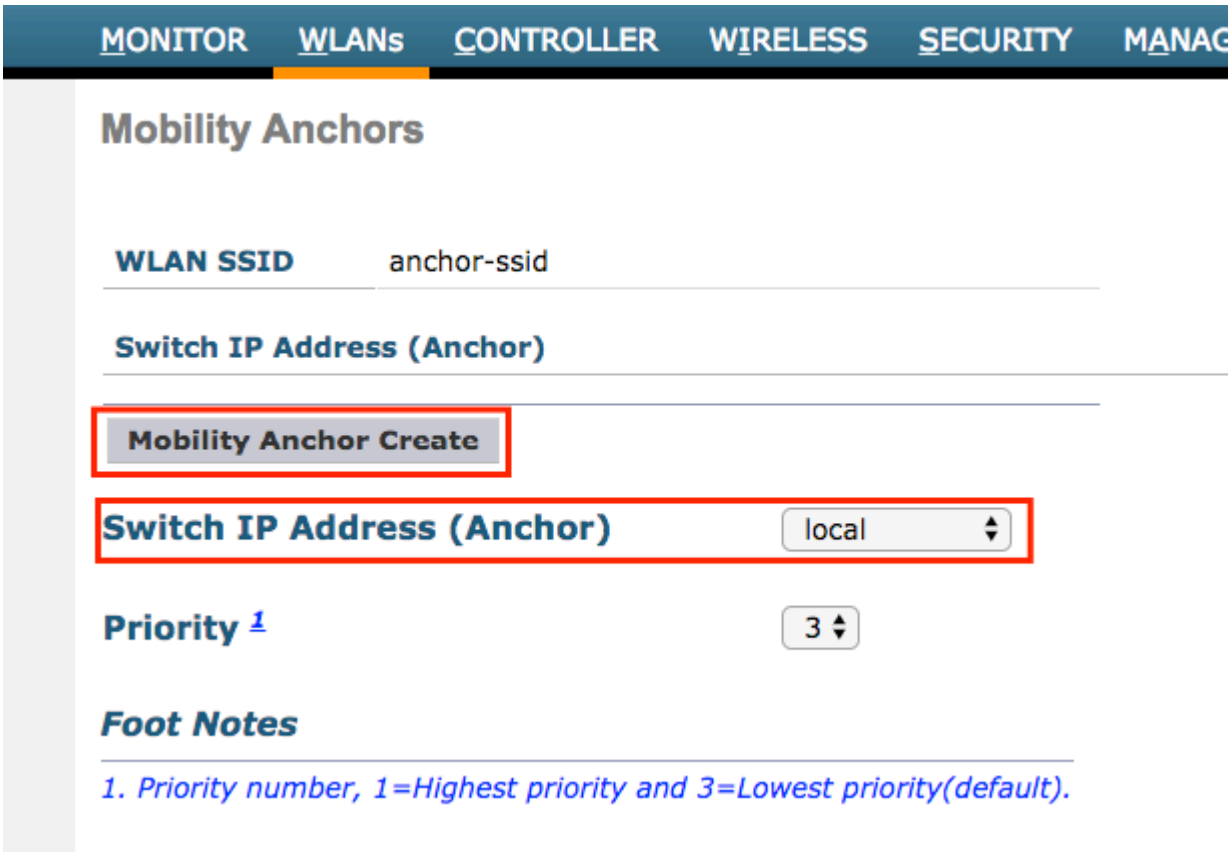
```
# config t
# wireless profile policy anchor-policy
# mobility anchor 10.88.173.105 priority 3
# no shutdown
# exit

# wireless tag policy PT1
# wlan anchor-ssid policy anchor-policy
# exit

# ap aaaa.bbbb.dddd
# site-tag PT1
# exit
```

Paso 6. Configure el WLC de AireOS como el ancla.

Inicie sesión en AireOS y navegue hasta WLANs > WLANs. Elija la flecha al extremo derecho de la fila WLAN para navegar al menú desplegable y elegir Mobility Anchors.



Ajústelo como delimitador local.

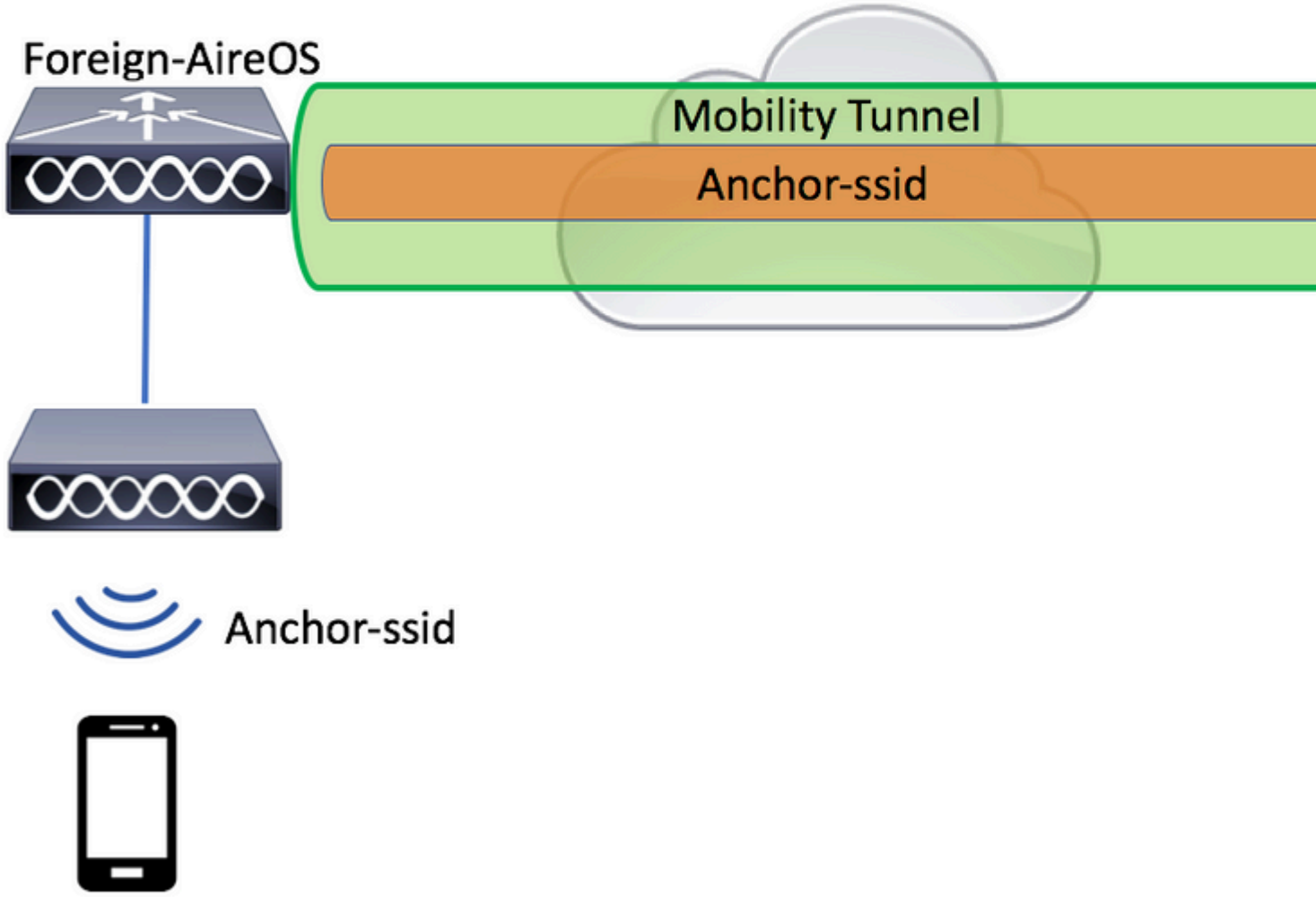


Desde la CLI:

```
> config wlan disable <wlan-id>
> config wlan mobility anchor add <wlan-id> <AireOS-WLC's-mgmt-interface>
> config wlan enable <wlan-id>
```

Foreign AireOS - Anchor 9800 WLC

Diagrama de red de anclaje AireOS Foreign con 9800



Configuración de un Foreign 9800 con un Anchor AireOS

Paso 1. Construya un túnel de movilidad entre el WLC Foreign 9800 y el WLC Anchor AireOS.

Puede consultar este documento: Configuración de topologías de movilidad en Catalyst 9800

Paso 2. Cree el SSID deseado en ambos WLC.

Métodos de seguridad admitidos:

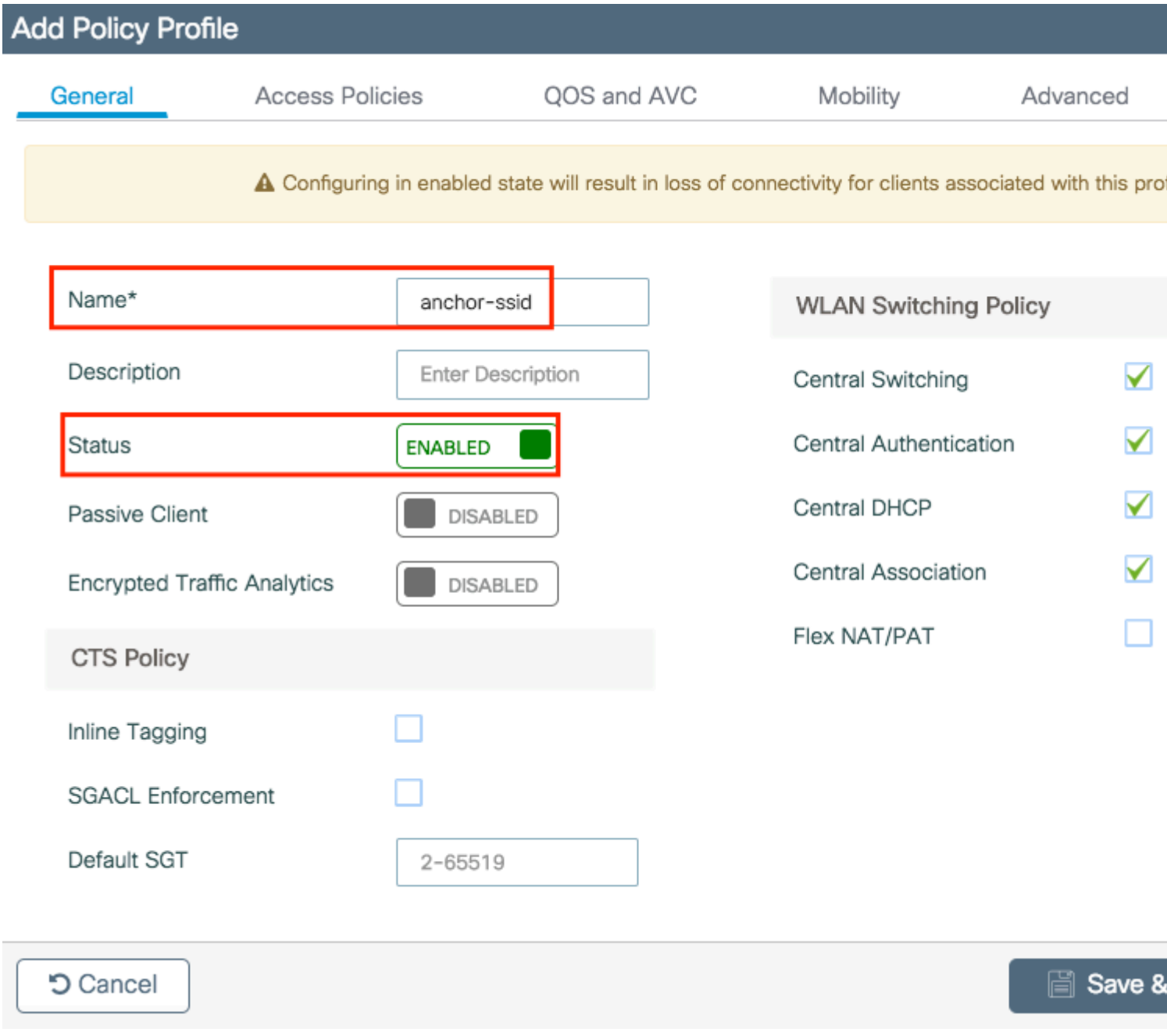
- Abierto
- filtro MAC
- PSK
- Punto1x
- Autenticación web local/externa (LWA)

- Autenticación web central (CWA)

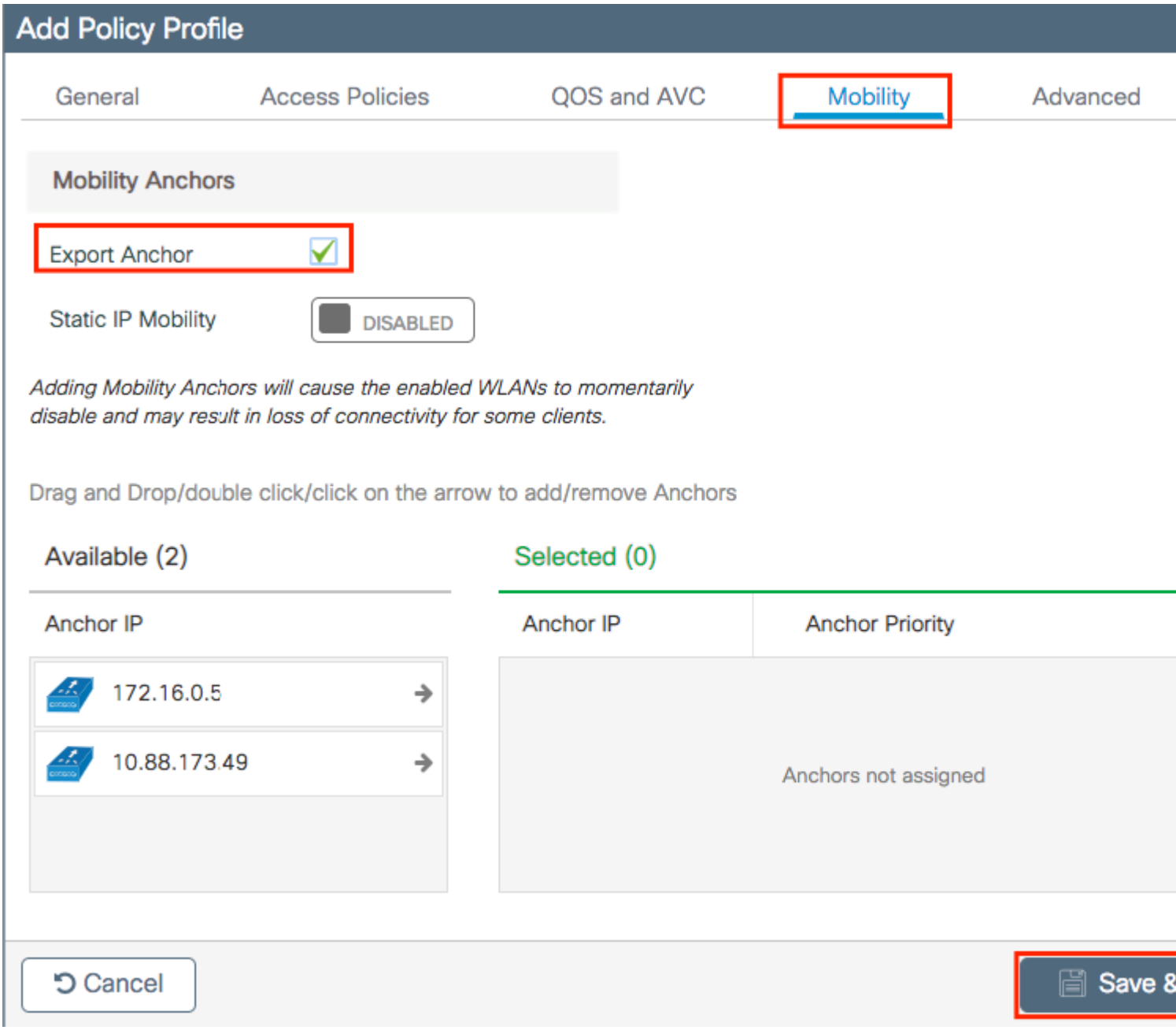
Nota: Tanto el WLC de AireOS como el WLC de 9800 deben tener el mismo tipo de configuración, de lo contrario el ancla no funciona.

Paso 3. Inicie sesión en el WLC 9800 (que actúa como anclaje) y cree el perfil de política de anclaje.

Desplácese hasta Configuration > Tags & Profiles > Policy > + Add.Asegúrese de que el nombre del perfil de política en 9800 sea exactamente el mismo nombre que el nombre del perfil en el WLC de AireOS; de lo contrario, no funcionará.



Desplácese hasta Mobility y activar Export Anchor.Esto indica al WLC 9800 que es el WLC 9800 de anclaje para cualquier WLAN que utilice ese perfil de política. Cuando el WLC de AireOS externo envía los clientes al WLC de anclaje 9800, informa sobre el nombre WLAN al que está asignado el cliente, de modo que el WLC de anclaje 9800 sabe qué configuración WLAN local debe utilizar y también utiliza este nombre para saber qué perfil de política local debe utilizar.



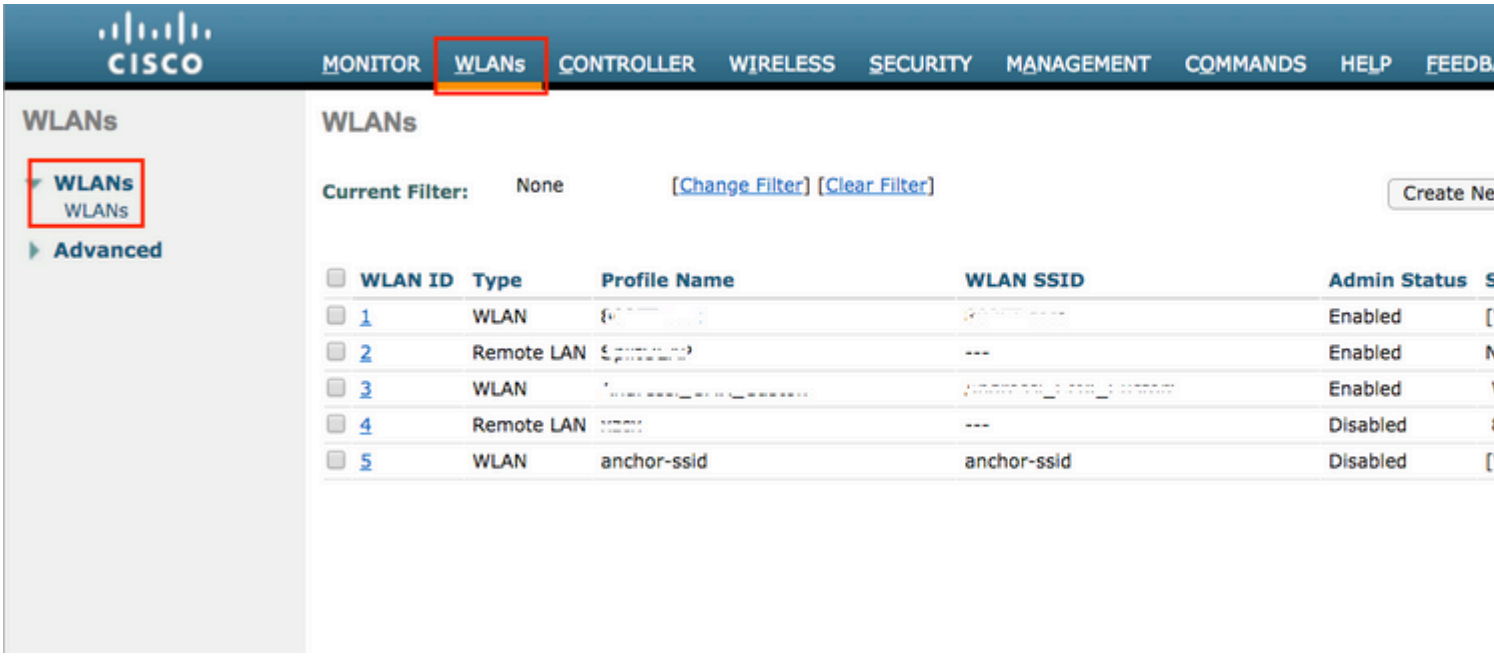
Nota: Asegúrese de utilizar este perfil de política exclusivamente para recibir tráfico de controladores externos.

Desde la CLI:

```
Anchor 9800 WLC

# config t
# wireless profile policy <anchor-policy>
# mobility anchor
# vlan <VLAN-id_VLAN-name>
# no shutdown
# exit
```

Paso 4. Configure el WLC de AireOS como externo.

Inicie sesión en AireOS y navegue hasta WLANs > WLANs.Navegue hasta la flecha abajo al final de la fila WLAN y elija Mobility Anchors .



Establezca el WLC 9800 como un ancla para este SSID.

Desde la CLI:

```
> config wlan disable <wlan-id>
> config wlan mobility anchor add <wlan-id> <9800 WLC's-mgmt-interface>
> config wlan enable <wlan-id>
```

Verificación

Puede utilizar estos comandos para verificar la configuración y el estado de los clientes inalámbricos con el uso de un SSID externo/de anclaje.

Verifique en el 9800 WLC

```
# show run wlan
# show wlan summary
# show wireless client summary
# show wireless mobility summary
# show ap tag summary
# show ap <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>
```

Verificar en el WLC de AireOS

```
> show client summary
> show client detail <client-mac-addr>
> show wlan summary
> show wlan <wlan-id>
```

Troubleshoot

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 eventos de una condición de incidente o error después de que se haya producido.

Nota: Dependiendo 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 consultar 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 los syslogs del buffer del controlador 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.

```
# show logging
```

Paso 3. Recopile los seguimientos del nivel de aviso siempre activo para la dirección MAC o IP específica. El par de movilidad remota puede filtrar esto, si sospecha un problema de túnel de movilidad, o por dirección MAC del cliente inalámbrico.

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

Paso 4. 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 seguimientos 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, consulte 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<aaaa.bbbb.cccc> por dirección MAC.

Nota: Usted no ve el resultado de la actividad del cliente en la sesión de terminal, ya que todo se almacena en buffer internamente para ser visto más tarde.

Paso 7. Reproduzca el problema o el comportamiento que desea monitorear.

Paso 8. Detenga las depuraciones si el problema se reproduce antes de que se agote el tiempo de monitoreo predeterminado o configurado.

```
# 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 seguimiento de RA .log a un servidor externo o muestre 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.d
```

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 los registros ya se escribieron en la memoria del controlador y sólo es necesario rellenar una vista más detallada de ellos.

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

> **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 archivo ra-internal-FILENAME.txt a un servidor externo o muestre 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.

Verifique el WLC de AireOS

Puede ejecutar este comando para monitorear la actividad de un cliente inalámbrico en un WLC de AireOS.

```
> debug client <client-mac-add>
```

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).