Configuración de la Tunelización Dividida de Catalyst 9800 y FlexConnect OEAP

Contenido

Introducción

Este documento describe cómo configurar un punto de acceso interior (AP) como FlexConnect Office Extend (OEAP) y cómo habilitar la tunelización dividida para que pueda definir qué tráfico se puede conmutar localmente en la oficina doméstica y qué tráfico se debe conmutar centralmente en el WLC.

Prerequisites

Requirements

La configuración en este documento asume que el WLC ya está configurado en una DMZ con NAT habilitado y que el AP puede unirse al WLC desde la oficina principal.

Componentes Utilizados

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

- Wireless LAN Controllers 9800 que ejecuta Cisco IOS-XE 17.3.1 Software.
- AP Wave1: 1700/2700/3700.

- AP Wave2: 1800/2800/3800/4800 y Catalyst serie 9100.

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.

Overview

Un punto de acceso Cisco OfficeExtend (Cisco OEAP) proporciona comunicaciones seguras desde un Cisco WLC a un Cisco AP en una ubicación remota, ampliando sin problemas la WLAN corporativa a través de Internet a la residencia de un empleado. La experiencia del usuario en la oficina doméstica es exactamente la misma que en la oficina corporativa. El cifrado de seguridad de la capa de transporte del datagrama (DTLS) entre el punto de acceso y el controlador garantiza que todas las comunicaciones tengan el mayor nivel de seguridad. Cualquier punto de acceso interior en modo FlexConnect puede actuar como OEAP.

Antecedentes

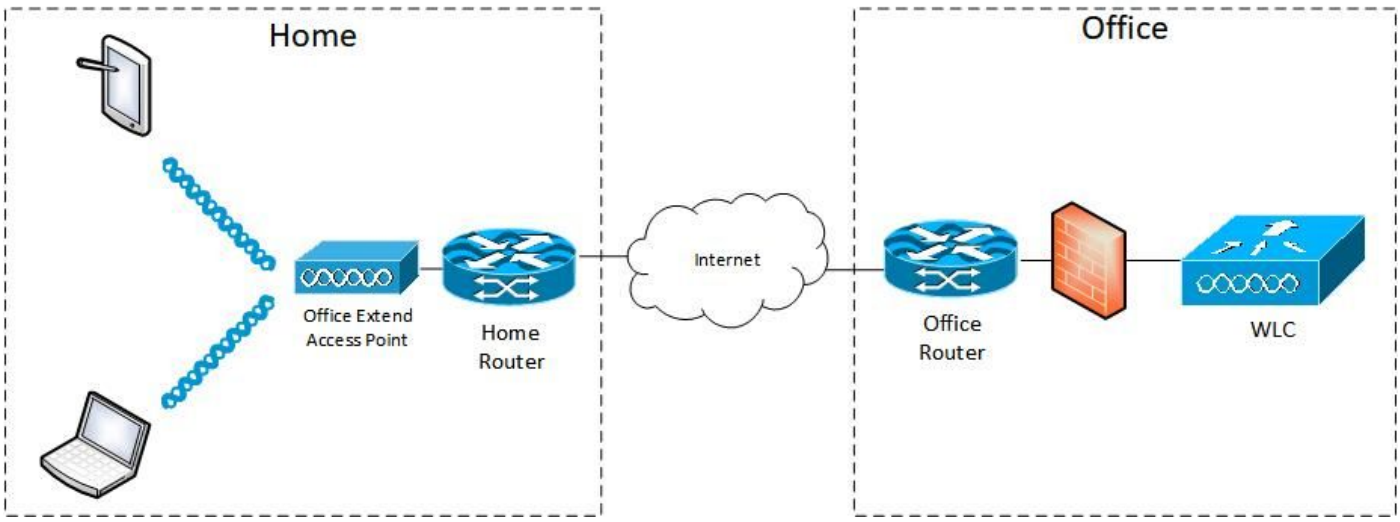
FlexConnect hace referencia a la capacidad de un punto de acceso (AP) para gestionar clientes inalámbricos mientras se trabaja en ubicaciones remotas, por ejemplo, a través de una WAN. También pueden decidir si el tráfico de los clientes inalámbricos se coloca directamente en la red en el nivel AP (conmutación local) o si el tráfico se centraliza en el controlador 9800 (conmutación central) y se envía de vuelta a través de la WAN, por WLAN.

Consulte este documento Comprender FlexConnect en el controlador inalámbrico Catalyst 9800 para obtener información detallada sobre FlexConnect.

El modo OEAP es una opción disponible en un punto de acceso FlexConnect, para permitir funcionalidad adicional, por ejemplo, un SSID local personal para el acceso doméstico, y también puede proporcionar una función de tunelización dividida, para obtener una mayor granularidad para definir qué tráfico debe conmutarse localmente en la oficina doméstica y qué tráfico debe conmutarse centralmente en el WLC, a través de una sola WLAN

Configurar

Diagrama de la red



Configuraciones

Definición de una Lista de Control de Acceso para la Tunelización Dividida

Paso 1. Elija Configuration > Security > ACL. Seleccione Agregar.

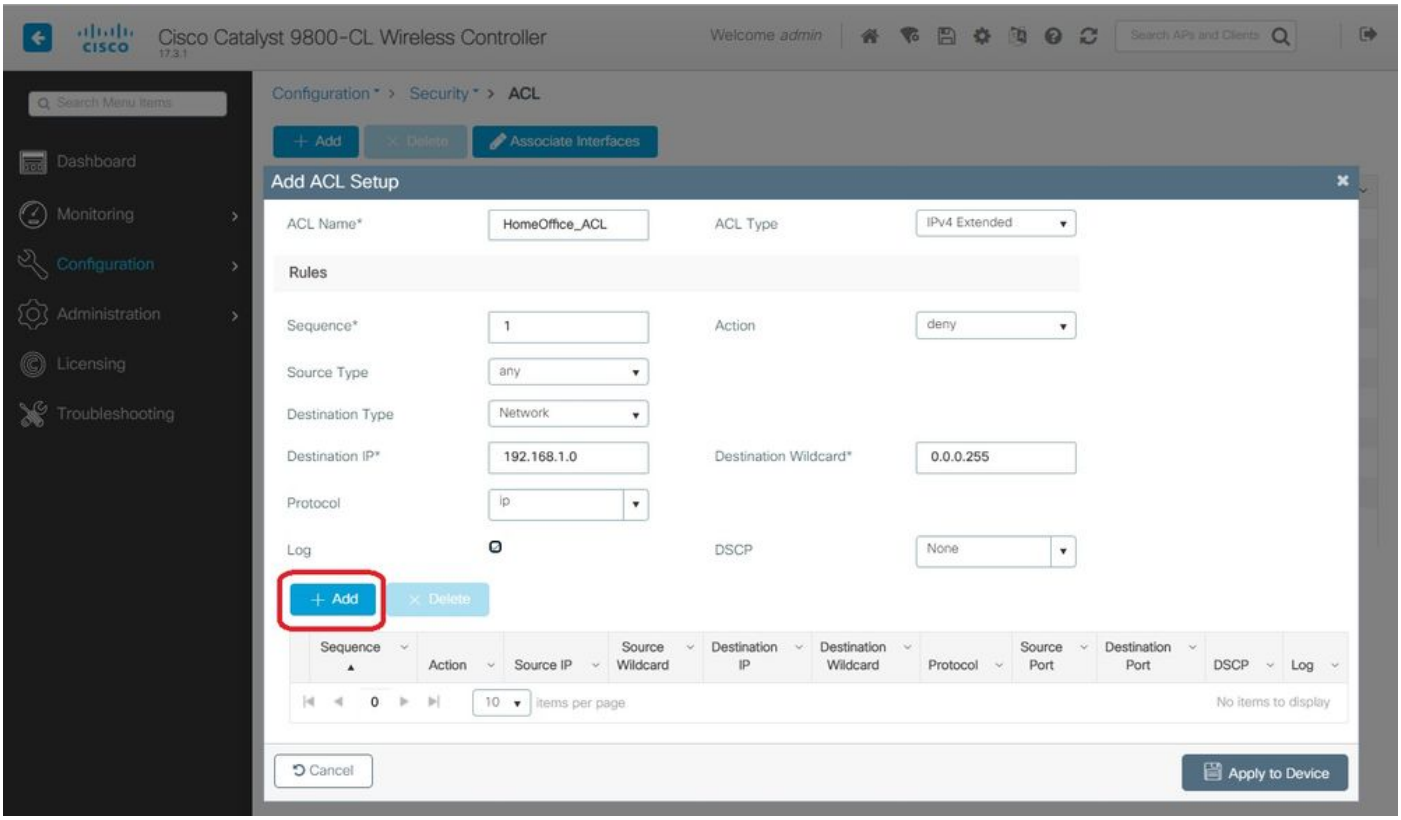
Paso 2. En el cuadro de diálogo Add ACL Setup (Agregar configuración de ACL), introduzca el nombre de la ACL, elija el tipo de ACL en la lista desplegable ACL Type (Tipo de ACL) y, en Rules settings (Parámetros de reglas), introduzca el número de secuencia. A continuación, elija la acción como permit o deny.

Paso 3. Elija el tipo de origen requerido en la lista desplegable Tipo de Origen.

Si elige el tipo de origen como Host, debe introducir el nombre de host/IP.

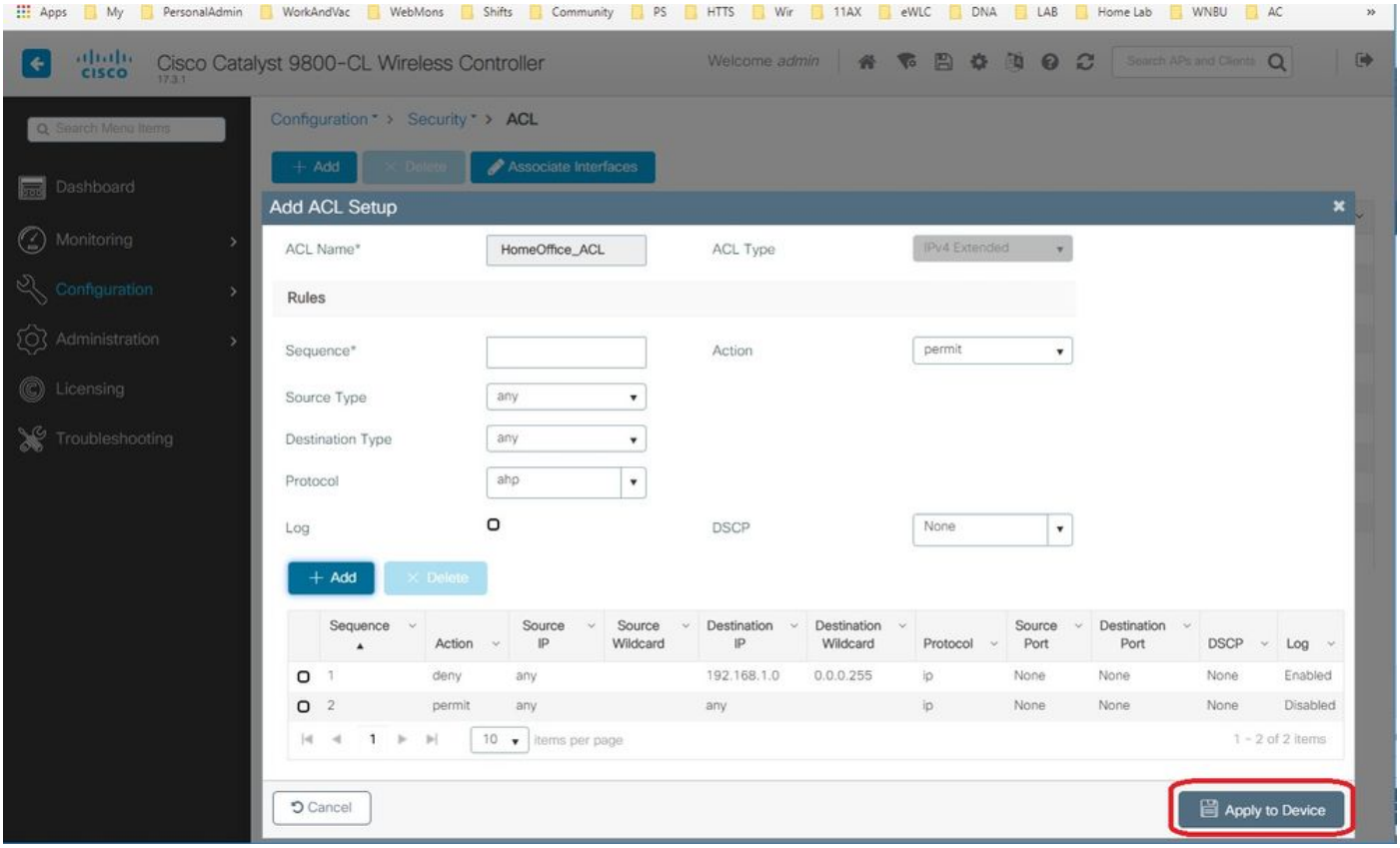
Si elige el tipo de origen como Red, debe especificar la dirección IP de origen y la máscara de comodín de origen.

En este ejemplo, todo el tráfico desde cualquier host a la subred 192.168.1.0/24 se conmuta centralmente (deny) y todo el resto del tráfico se conmuta localmente (permit).



Paso 4. Marque la casilla de verificación Registro si desea los registros y seleccione Agregar.

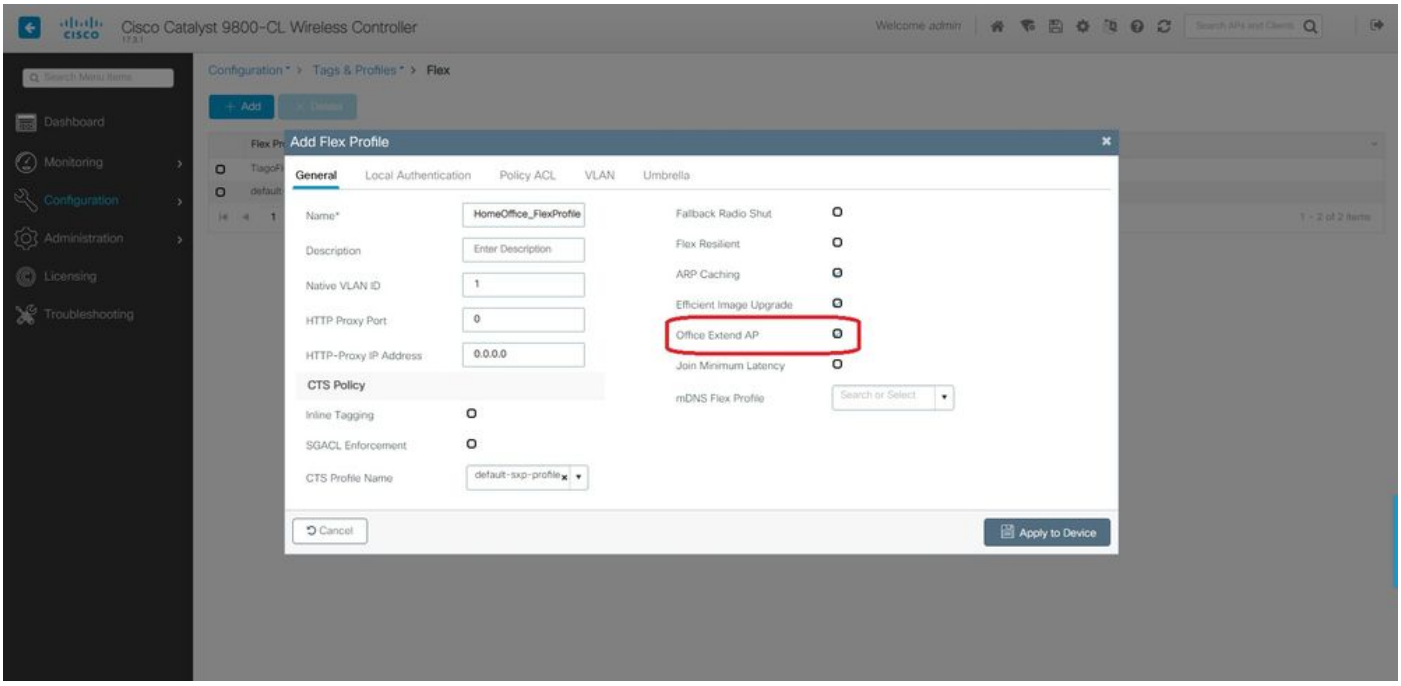
Paso 5. Agregue el resto de las reglas y seleccione Aplicar al dispositivo.



Vinculación de una Política ACL a la ACL Definida

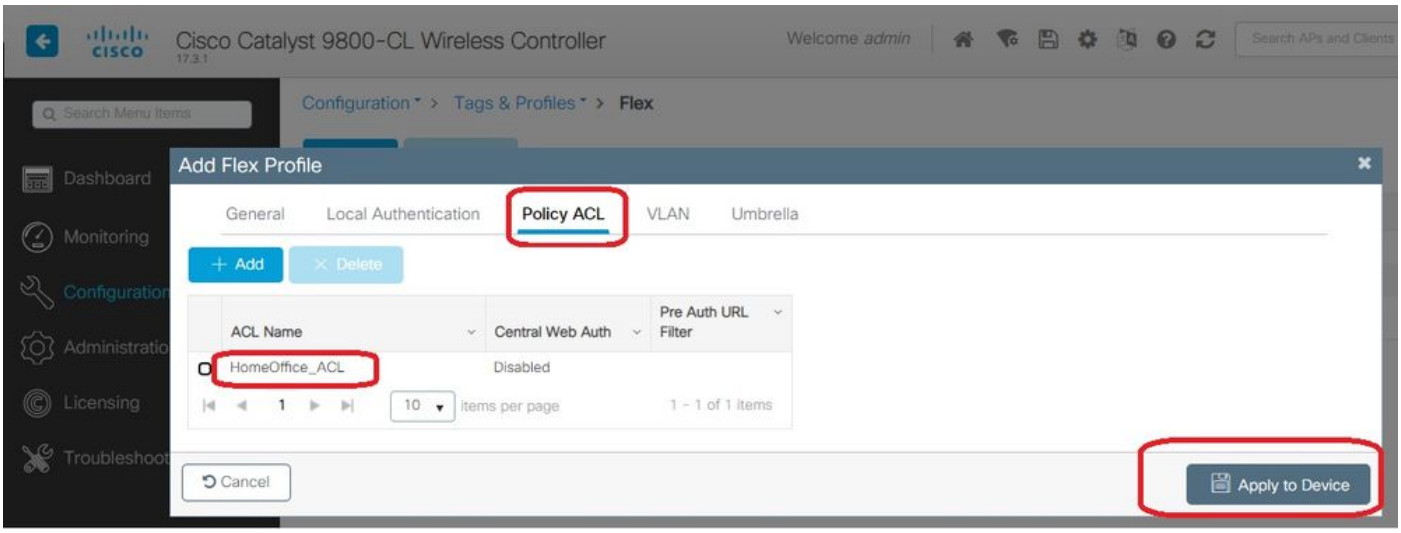
Paso 1. Cree un nuevo perfil flexible. Vaya a Configuration > Tags & Profiles > Flex. seleccione Agregar.

Paso 2. Introduzca un nombre y active OEAP. Además, asegúrese de que el ID de VLAN nativo sea el del switchport de AP.



Nota: Cuando habilita el modo Office-Extend, el Link-Encryption también se habilita de forma predeterminada y no se puede cambiar aunque inhabilite Link Encryption en el AP Join Profile.

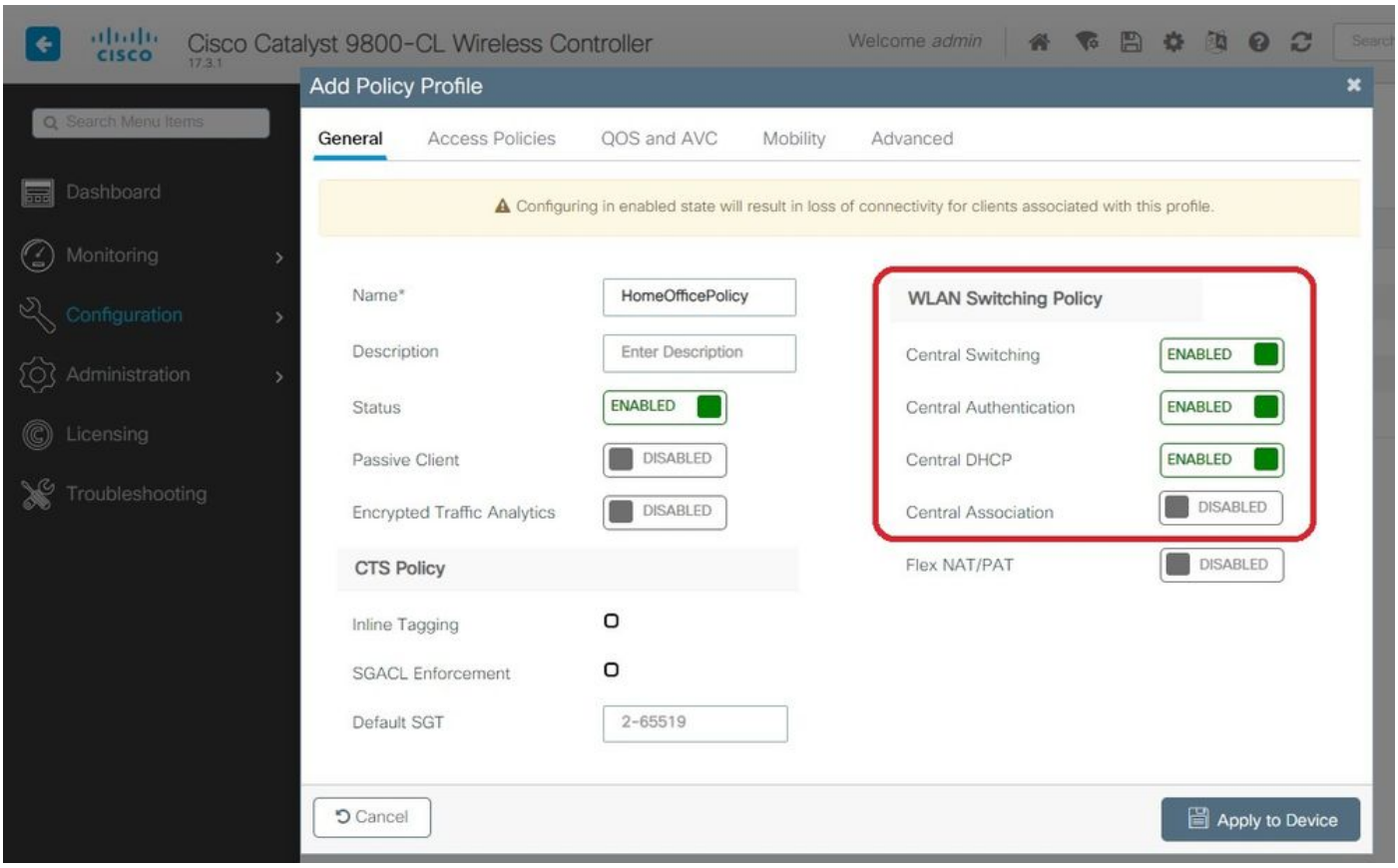
Paso 3. Vaya a la ficha Policy ACL (Política de ACL) y seleccione Add (Agregar). Aquí agregue la ACL al perfil y aplíquela al dispositivo.



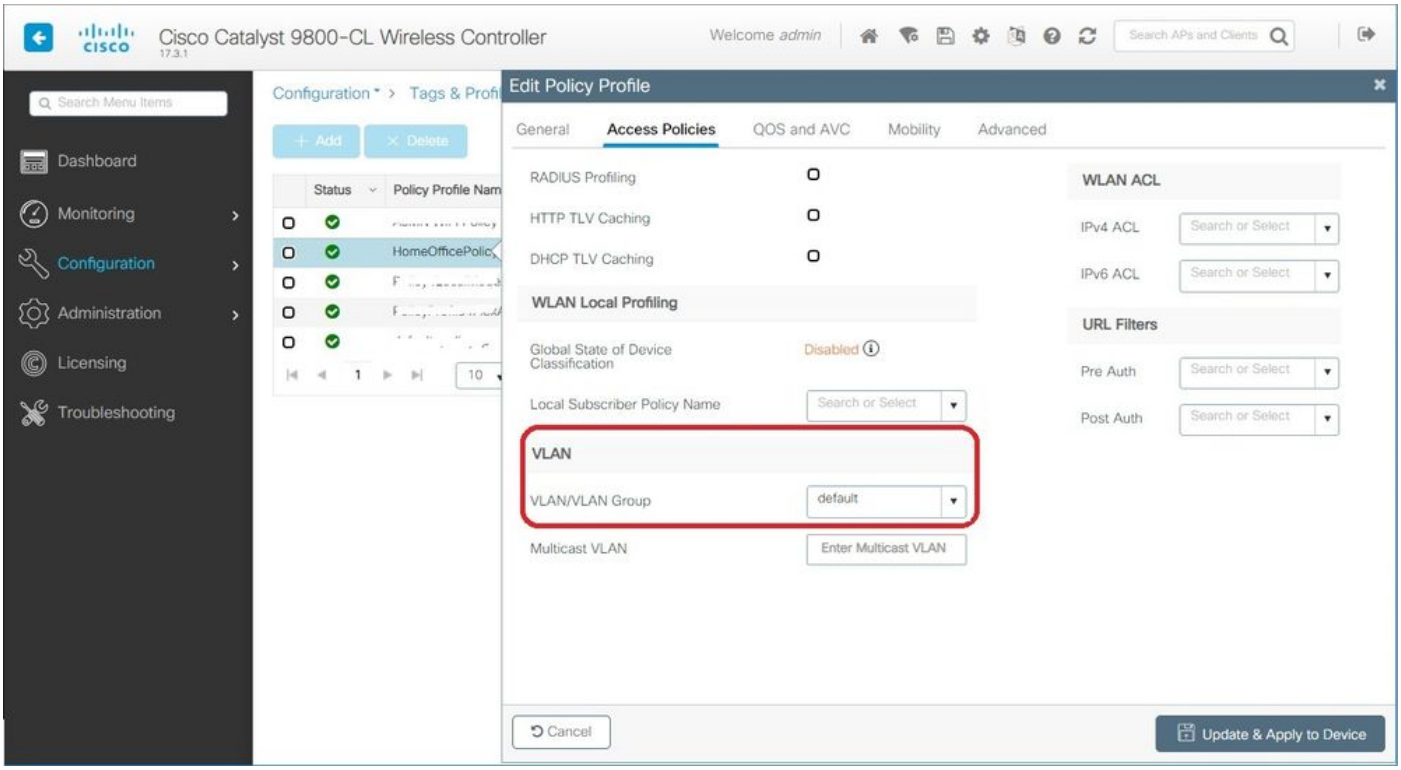
Configuración de una Política de Perfil Inalámbrico y un Nombre MAC ACL Dividido

Paso 1. Cree un perfil WLAN. En este ejemplo, se utilizó un SSID denominado HomeOffice con seguridad WPA2-PSK.

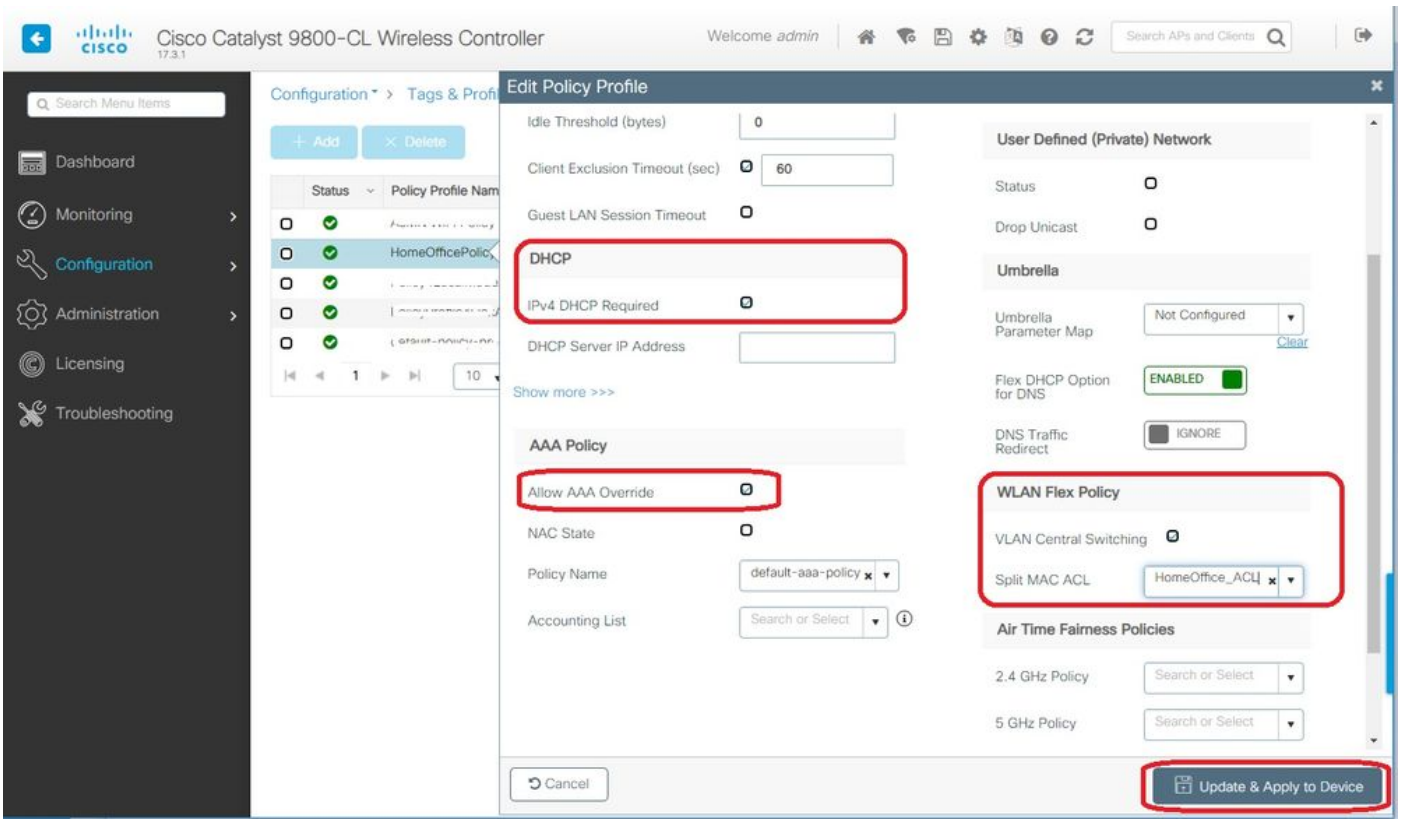
Paso 2. Cree un perfil de política. Vaya a Configuration > Tags > Policy y seleccione Add . En General, asegúrese de que este perfil sea una política conmutada centralmente como se muestra en este ejemplo:



Paso 3. Dentro del perfil de política, vaya a Políticas de acceso y defina la VLAN para que el tráfico se conmute centralmente. Los clientes obtienen una dirección IP en la subred asignada a esta VLAN.



Paso 4. Para configurar la tunelización dividida local en un AP, debe asegurarse de haber habilitado el DCHP requerido en la WLAN. Esto asegura que el cliente que se asocia con la WLAN dividida haga DHCP. Puede activar esta opción en el perfil de política en la ficha Opciones avanzadas. Active la casilla de verificación IPv4 DHCP Required. En la configuración de la política flexible de WLAN, elija la ACL MAC dividida creada anteriormente en la lista desplegable Dividir ACL MAC. Seleccione Aplicar al dispositivo:



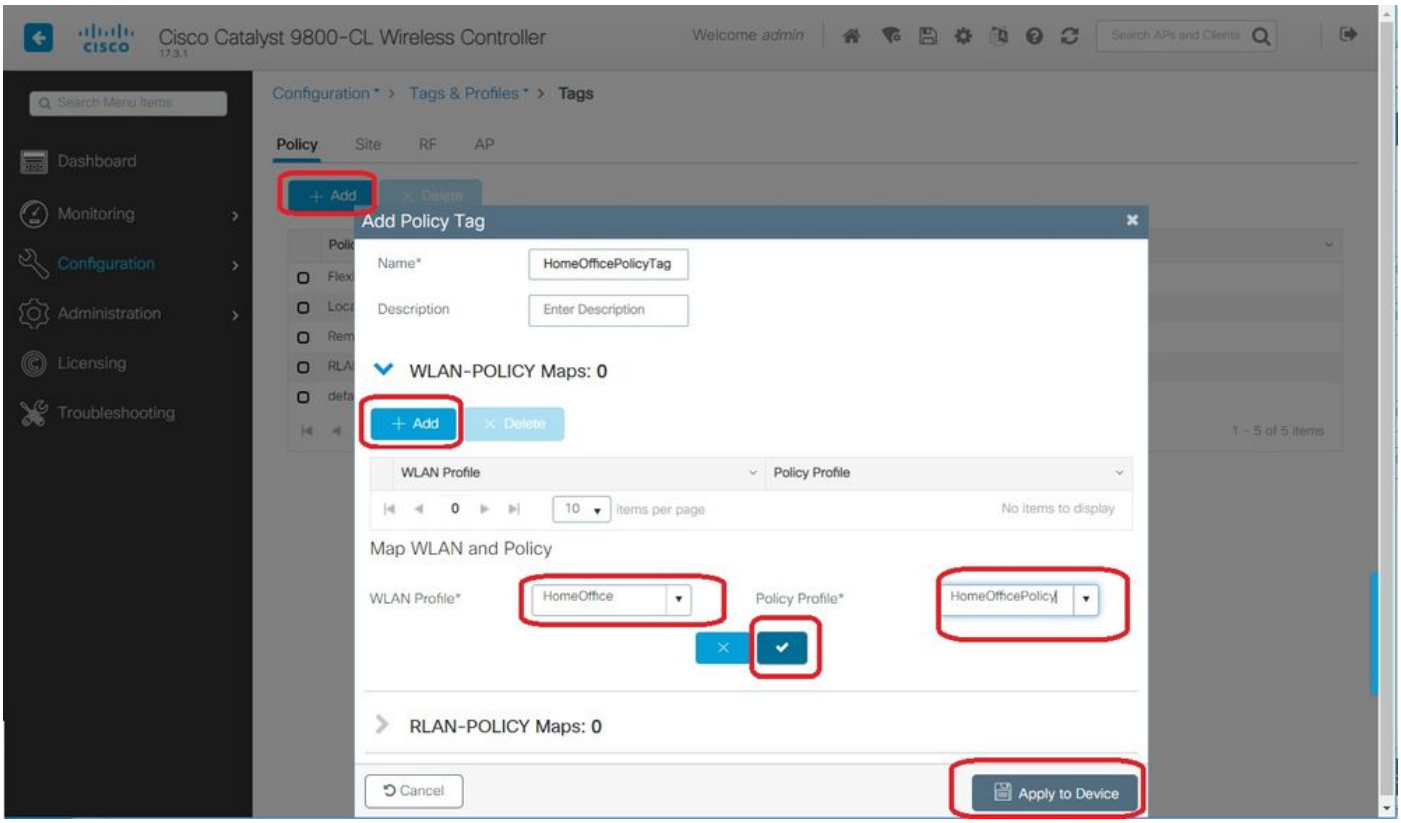
Nota: Los clientes Apple iOS necesitan que la opción 6 (DNS) se configure en la oferta DHCP para que funcione la tunelización dividida.

Asignación de una WLAN a un Perfil de Política

Paso 1. Elija Configuration > Tags & Profiles > Tags. En la ficha Política, seleccione Agregar.

Paso 2. Introduzca el nombre de la política de etiquetas y, en la ficha WLAN-POLICY Maps (Mapas de POLÍTICA WLAN), seleccione Add (Agregar).

Paso 3. Elija el perfil WLAN de la lista desplegable Perfil WLAN y elija el perfil de política de la lista desplegable Perfil de política. Seleccione el icono Marcar y, a continuación, Aplicar al dispositivo.

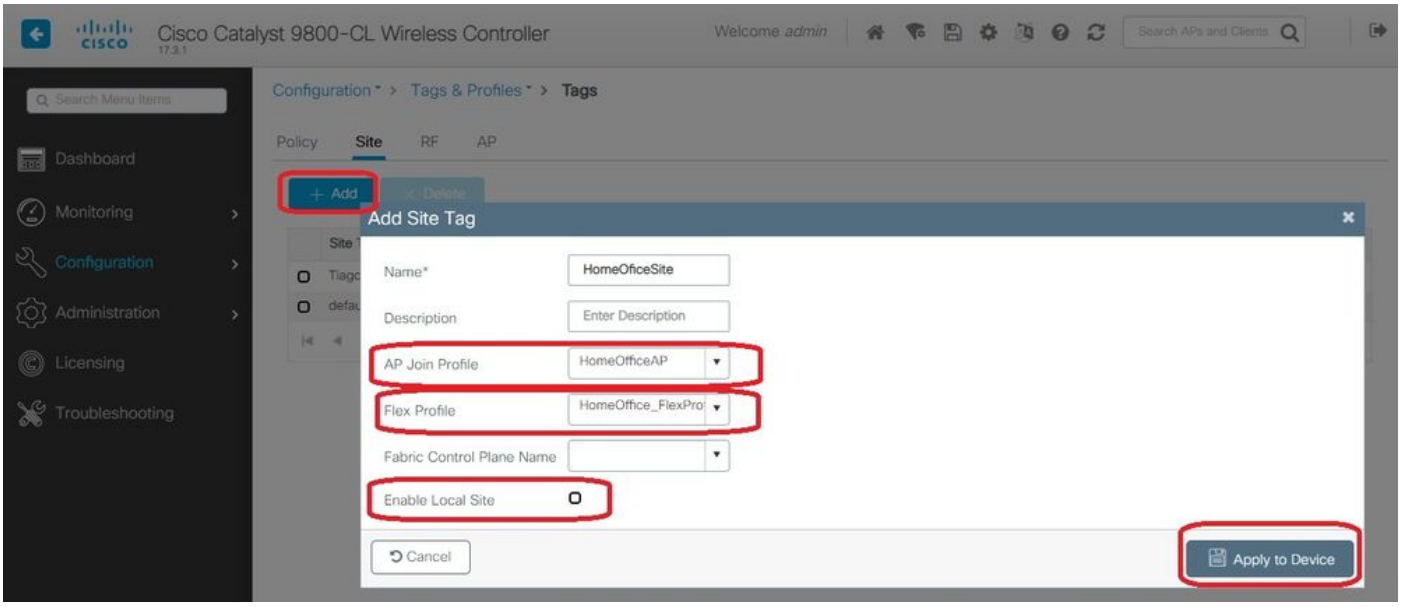


Configuración de un Perfil de Unión AP y Asociación con la Etiqueta del Sitio

Paso 1. Vaya a Configuration > Tags & Profiles > AP Join y seleccione Add . Introduzca un nombre. Opcionalmente, puede habilitar SSH para permitir la resolución de problemas y después desactivarla si no es necesario.

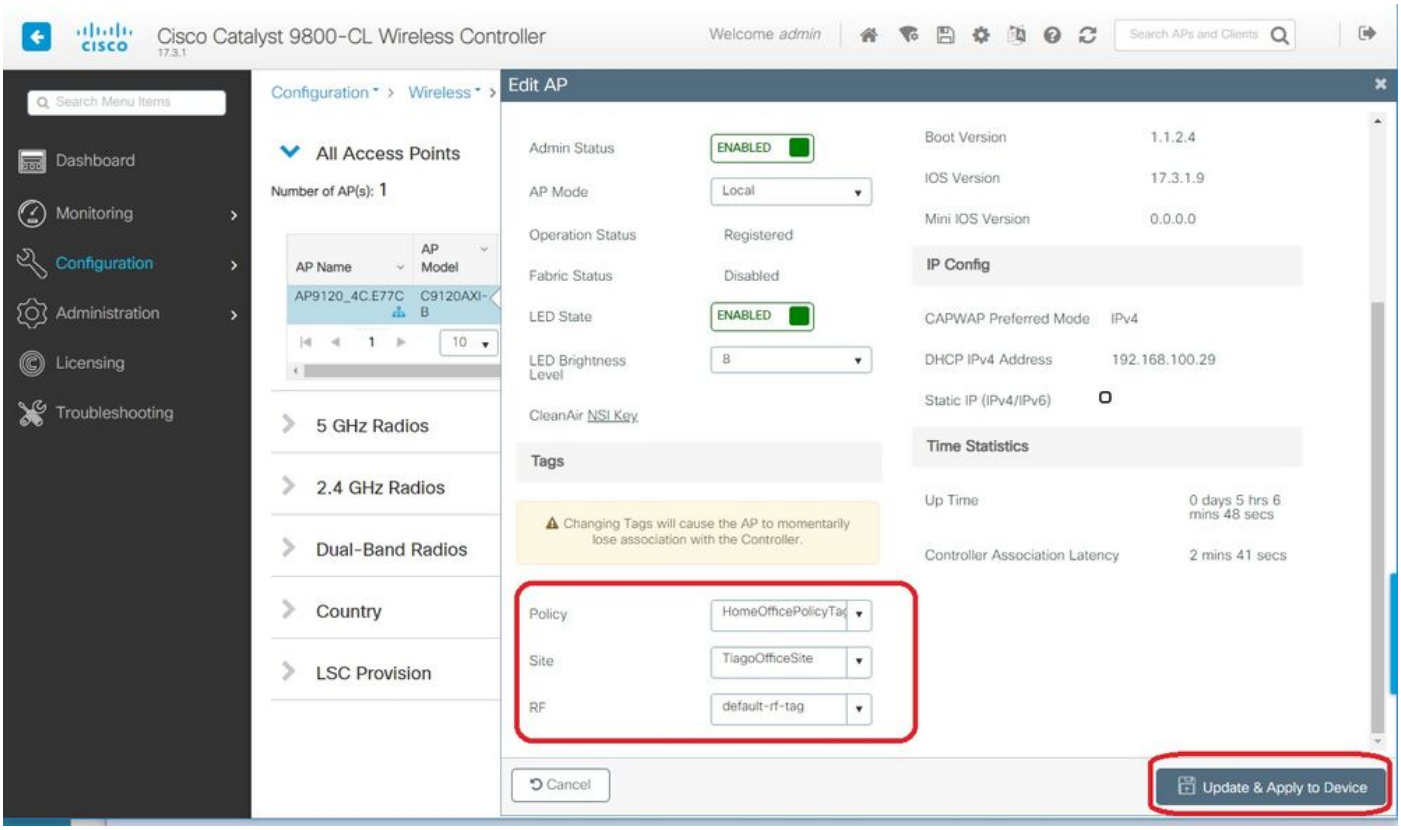
Paso 2. Elija Configuration > Tags & Profiles > Tags. En la ficha Sitio, seleccione Agregar.

Paso 3. Ingrese el nombre de la etiqueta del sitio, desmarque Enable Local Site (Activar sitio local) y, a continuación, seleccione el perfil de conexión de AP y el perfil flexible (creado antes) en las listas desplegables. A continuación, aplique al dispositivo.

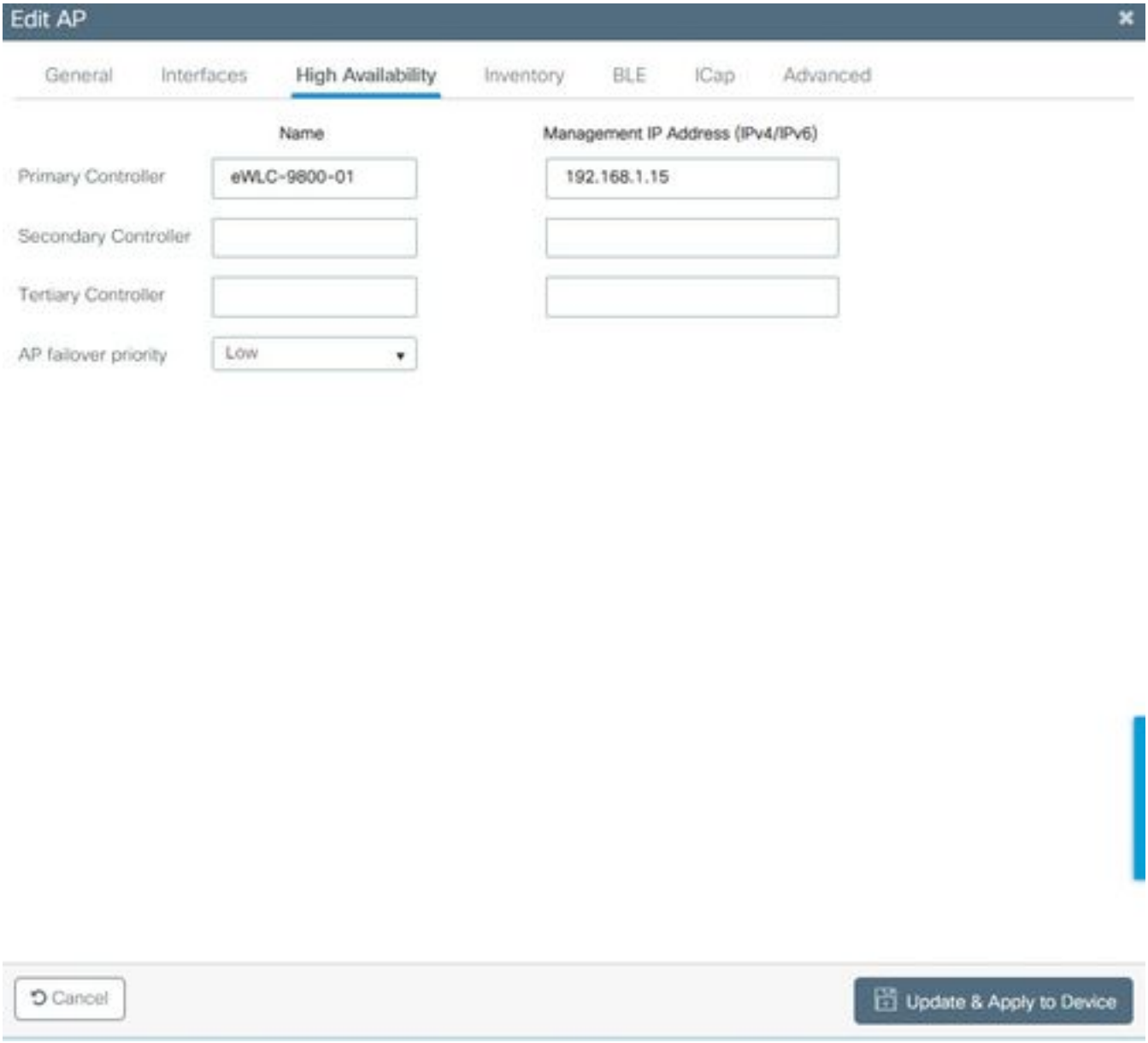


Asociación de una etiqueta de política y una etiqueta de sitio a un punto de acceso

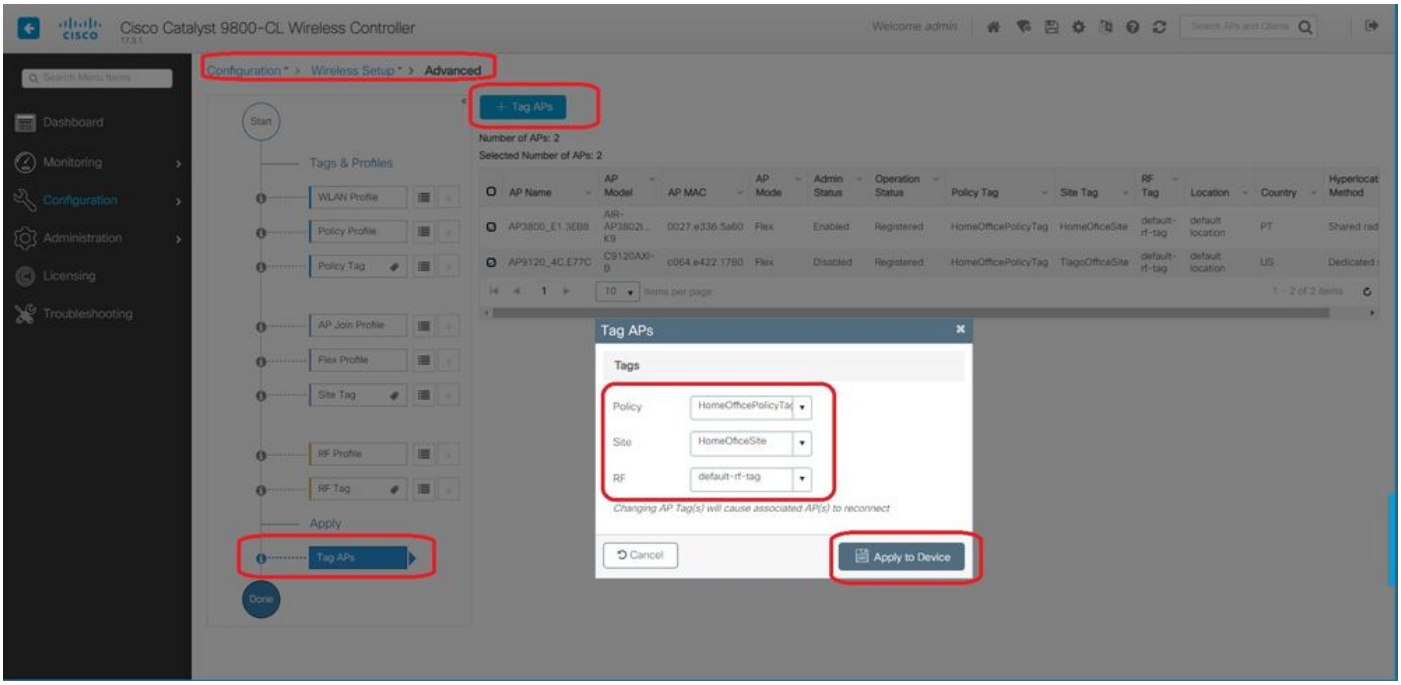
Opción 1. Esta opción requiere que configure 1 AP a la vez. Vaya a Configuration > Wireless > Access Points (Configuración > Tecnología inalámbrica > Puntos de acceso). Seleccione el AP que desea mover al Home Office y luego seleccione las Etiquetas del Home Office. Seleccione Actualizar y Aplicar al dispositivo:



También se recomienda configurar un controlador primario para que el AP conozca la IP/Nombre del WLC para alcanzar una vez que se implementa en el Home Office. Puede hacer esto editando el AP directamente a la pestaña Alta Disponibilidad:



Opción 2. Esta opción le permite configurar varios AP simultáneamente. Vaya a Configuration > Wireless Setup > Advanced > Tag AP. Seleccione las etiquetas creadas anteriormente y seleccione Aplicar al dispositivo.



Los APs se reinician y se reunen al WLC con las nuevas configuraciones.

Verificación

Puede verificar la configuración mediante GUI o CLI. Esta es la configuración resultante en CLI:

```
!
ip access-list extended HomeOffice_ACL
1 deny ip any 192.168.1.0 0.0.0.255 log
2 permit ip any any log
!
wireless profile flex HomeOffice_FlexProfile
acl-policy HomeOffice_ACL
office-extend
!
wireless profile policy HomeOfficePolicy
no central association
aaa-override
flex split-mac-acl HomeOffice_ACL
flex vlan-central-switching
ipv4 dhcp required
vlan default
no shutdown
!
wireless tag site HomeOficeSite
flex-profile HomeOffice_FlexProfile
no local-site
!
wireless tag policy HomeOfficePolicyTag
wlan HomeOffice policy HomeOfficePolicy
!
wlan HomeOffice 5 HomeOffice
security wpa psk set-key ascii 0 xxxxxxx
no security wpa akm dot1x
security wpa akm psk
no shutdown
!
ap 70db.98e1.3eb8
```

```
policy-tag HomeOfficePolicyTag
site-tag HomeOficeSite
!
ap c4f7.d54c.e77c
policy-tag HomeOfficePolicyTag
site-tag HomeOficeSite
!
```

Verificación de la configuración de AP:

```
eWLC-9800-01#show ap name AP3800_E1.3EB8 config general

Cisco AP Name : AP3800_E1.3EB8
=================================================

Cisco AP Identifier : 0027.e336.5a60
...
MAC Address : 70db.98e1.3eb8
IP Address Configuration : DHCP
IP Address : 192.168.1.99
IP Netmask : 255.255.255.0
Gateway IP Address : 192.168.1.254
...
SSH State : Enabled
Cisco AP Location : default location
Site Tag Name : HomeOficeSite
RF Tag Name : default-rf-tag
Policy Tag Name : HomeOfficePolicyTag
AP join Profile : HomeOfficeAP
Flex Profile : HomeOffice_FlexProfile
Primary Cisco Controller Name : eWLC-9800-01
Primary Cisco Controller IP Address : 192.168.1.15
...
AP Mode : FlexConnect
AP VLAN tagging state : Disabled
AP VLAN tag : 0
CAPWAP Preferred mode : IPv4
CAPWAP UDP-Lite : Not Configured
AP Submode : Not Configured
Office Extend Mode : Enabled
...
```

Puede conectarse directamente al AP y también verificar la configuración:

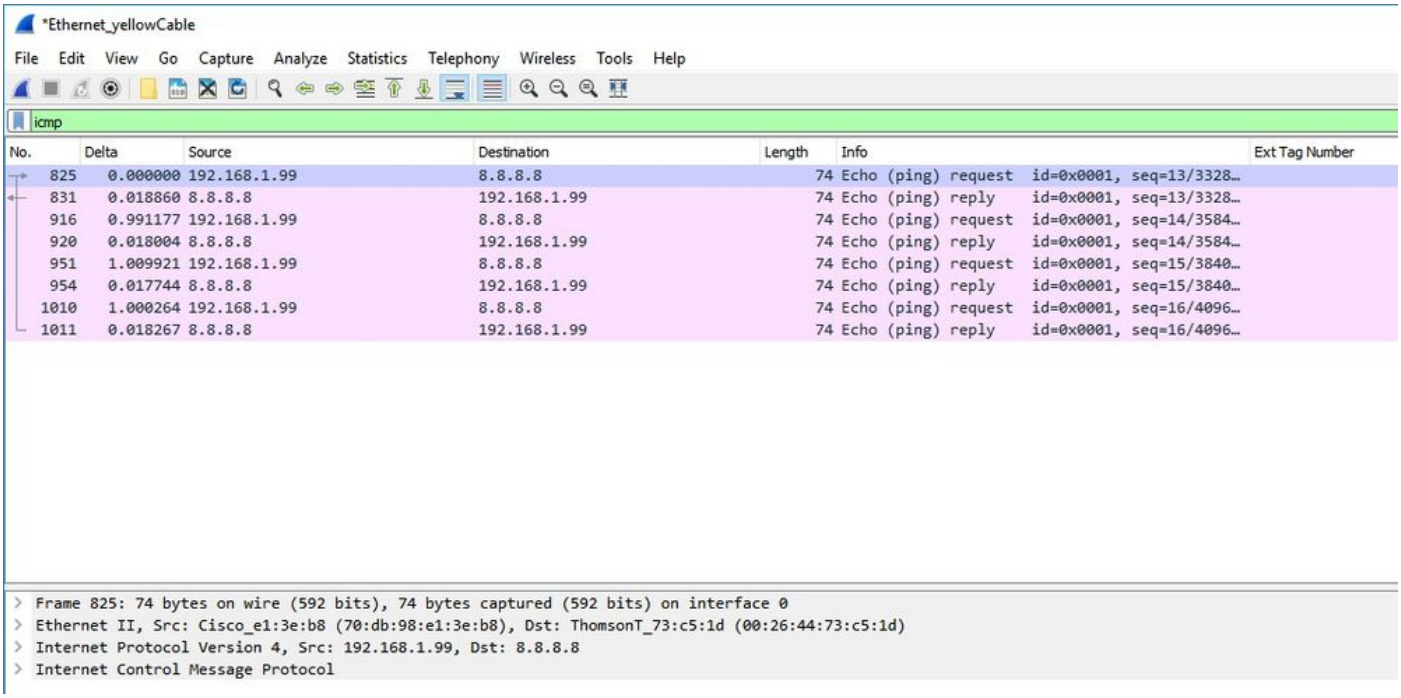
```
AP3800_E1.3EB8#show ip access-lists
Extended IP access list HomeOffice_ACL
1 deny ip any 192.168.1.0 0.0.0.255
2 permit ip any any

AP3800_E1.3EB8#show capwap client detailrcb
SLOT 0 Config

SSID : HomeOffice
Vlan Id : 0
Status : Enabled
...
otherFlags : DHCP_REQUIRED VLAN_CENTRAL_SW
...
Profile Name : HomeOffice
...
```

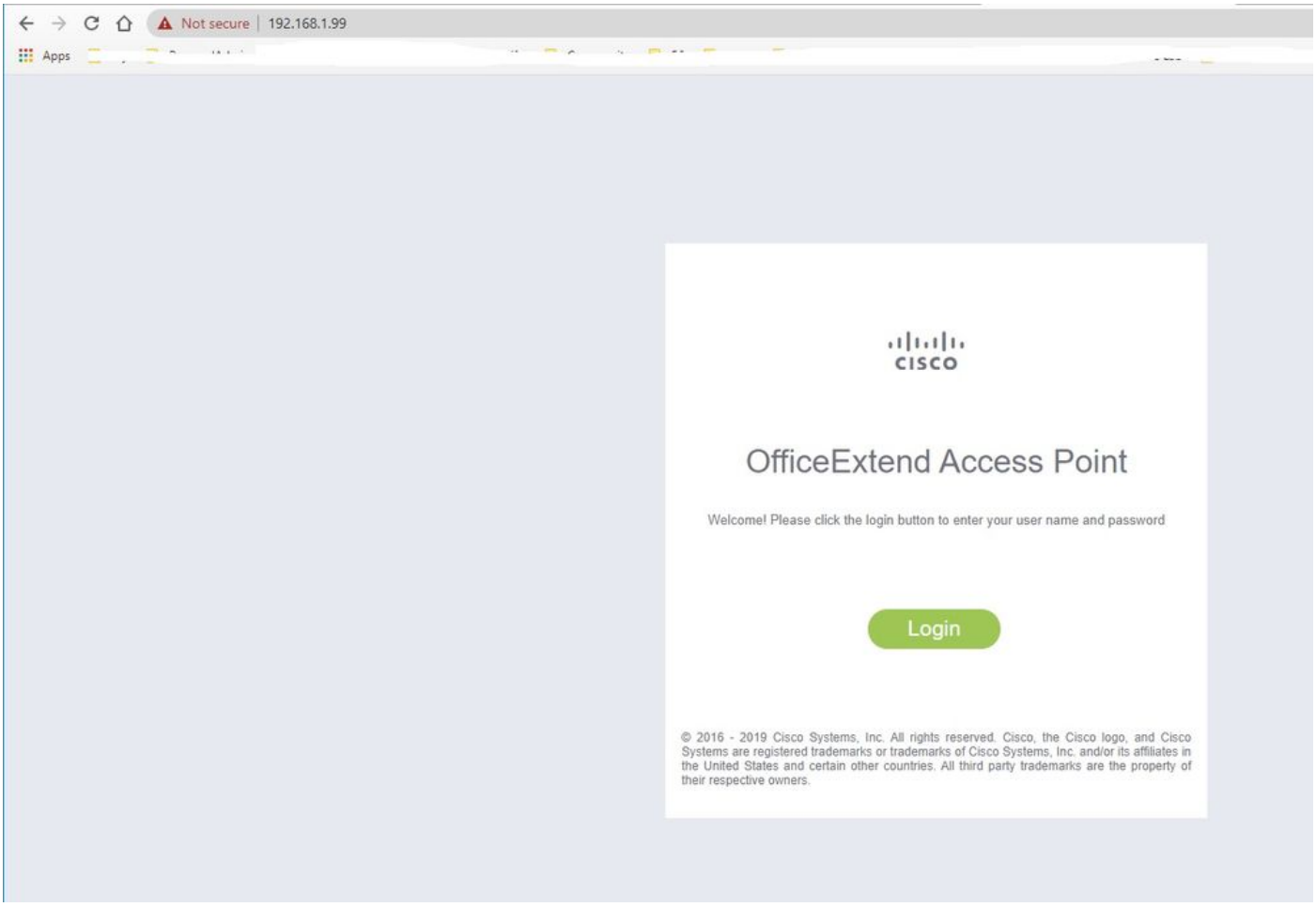
```
AP3800_E1.3EB8#show capwap client config
AdminState : ADMIN_ENABLED(1)
Name : AP3800_E1.3EB8
Location : default location
Primary controller name : eWLC-9800-01
Primary controller IP : 192.168.1.15
Secondary controller name : c3504-01
Secondary controller IP : 192.168.1.14
Tertiary controller name :
ssh status : Enabled
ApMode : FlexConnect
ApSubMode : Not Configured
Link-Encryption : Enabled
OfficeExtend AP : Enabled
Discovery Timer : 10
Heartbeat Timer : 30
...
```

Este es un ejemplo de capturas de paquetes que muestran el tráfico conmutado localmente. Aquí, la prueba realizada fue un "ping" de un cliente con IP 192.168.1.98 al servidor DNS de Google y luego a 192.168.1.254. Puede ver el ICMP originado con la IP de la dirección IP AP 192.168.1.99 enviada al DNS de Google debido a que el AP NATing el tráfico localmente. No hay icmp a 192.168.1.254 porque el tráfico se cifra en el túnel DTLS y sólo se ven tramas de datos de aplicación.

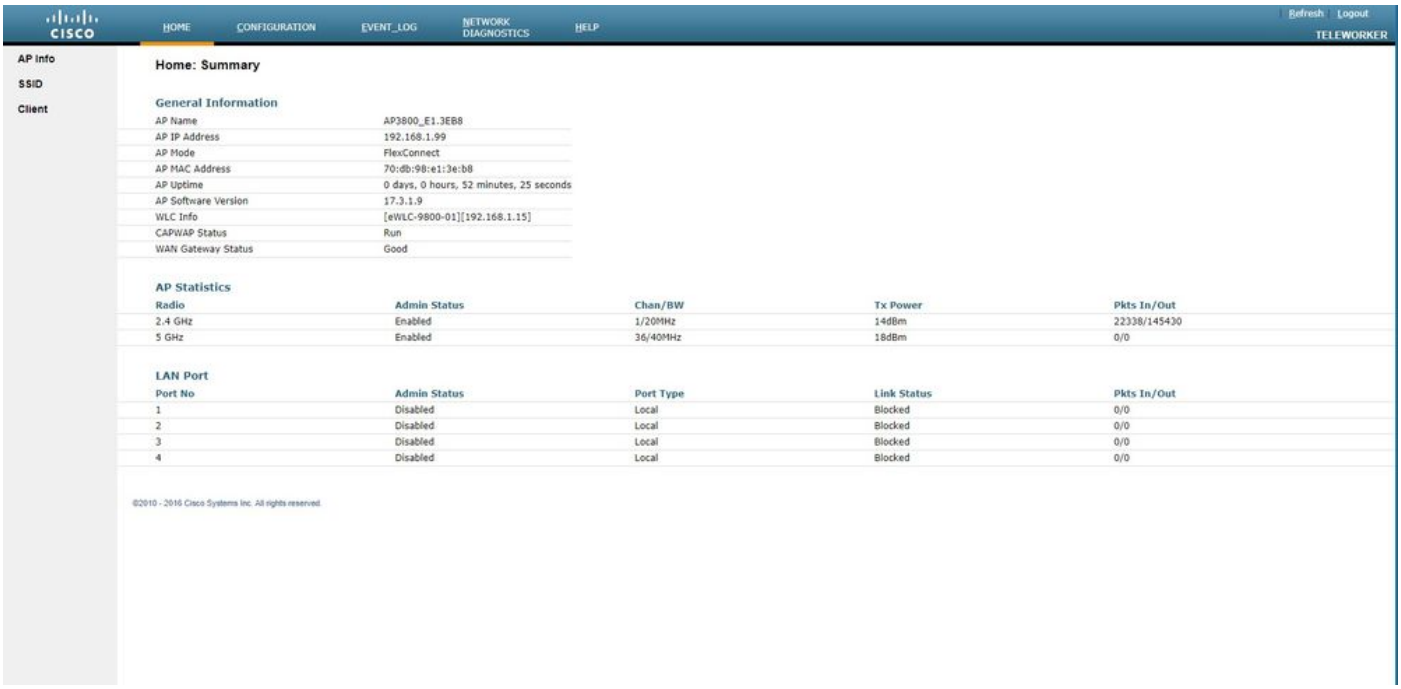


> **Nota:** El tráfico que se conmuta localmente es NATed por el AP porque en escenarios normales, la subred del cliente pertenece a la red de Office y los dispositivos locales en la oficina doméstica no saben cómo alcanzar la subred del cliente. El AP traduce el tráfico del cliente usando la dirección IP AP que está en la subred de la oficina local.

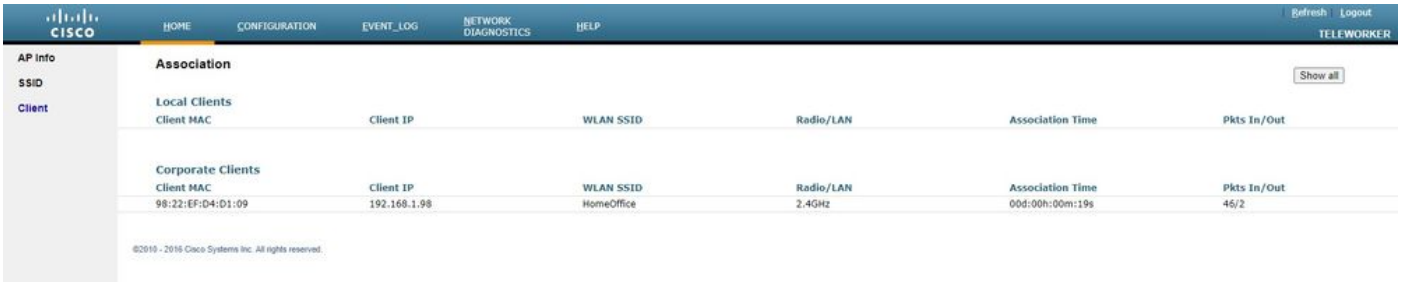
Puede acceder a la GUI de OEAP abriendo un navegador y escribiendo la URL de la dirección IP de AP. Las credenciales predeterminadas son admin/admin y debe cambiarlas en el inicio de sesión inicial.



Una vez que inicie sesión, tendrá acceso a la GUI:



Tiene acceso a información típica en un OEAP, como información de AP, SSID y clientes conectados:



Documentación relacionada

Introducción a FlexConnect en el controlador inalámbrico Catalyst 9800

Tunelización dividida para FlexConnect

Configuración de OEAP y RLAN en el WLC Catalyst 9800