Configurar o tunelamento dividido do Catalyst 9800 e FlexConnect OEAP

Contents

Introduction

Este documento descreve como configurar um ponto de acesso interno (AP) como um FlexConnect Office Extend (OEAP) e como habilitar o tunelamento dividido para que você possa definir que tráfego pode ser comutado localmente no escritório doméstico e que tráfego deve ser comutado centralmente no WLC.

Prerequisites

Requirements

A configuração neste documento pressupõe que a WLC já está configurada em um DMZ com NAT habilitado e que o AP pode ingressar na WLC do escritório doméstico.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Wireless LAN Controllers 9800 executando o software Cisco IOS-XE 17.3.1.
- APs Wave1: 1700/2700/3700.
- APs Wave2: séries 1800/2800/3800/4800 e Catalyst 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

Um Cisco OfficeExtend Access Point (Cisco OEAP) fornece comunicações seguras de uma WLC Cisco para um AP Cisco em um local remoto, estendendo perfeitamente a WLAN corporativa pela Internet para a residência de um funcionário. A experiência do usuário no escritório doméstico é exatamente a mesma que seria no escritório corporativo. A criptografia DTLS (Datagram Transport Layer Security) entre o access point e o controlador garante que todas as comunicações tenham o mais alto nível de segurança. Qualquer AP interno no modo FlexConnect pode atuar como um OEAP.

Informações de Apoio

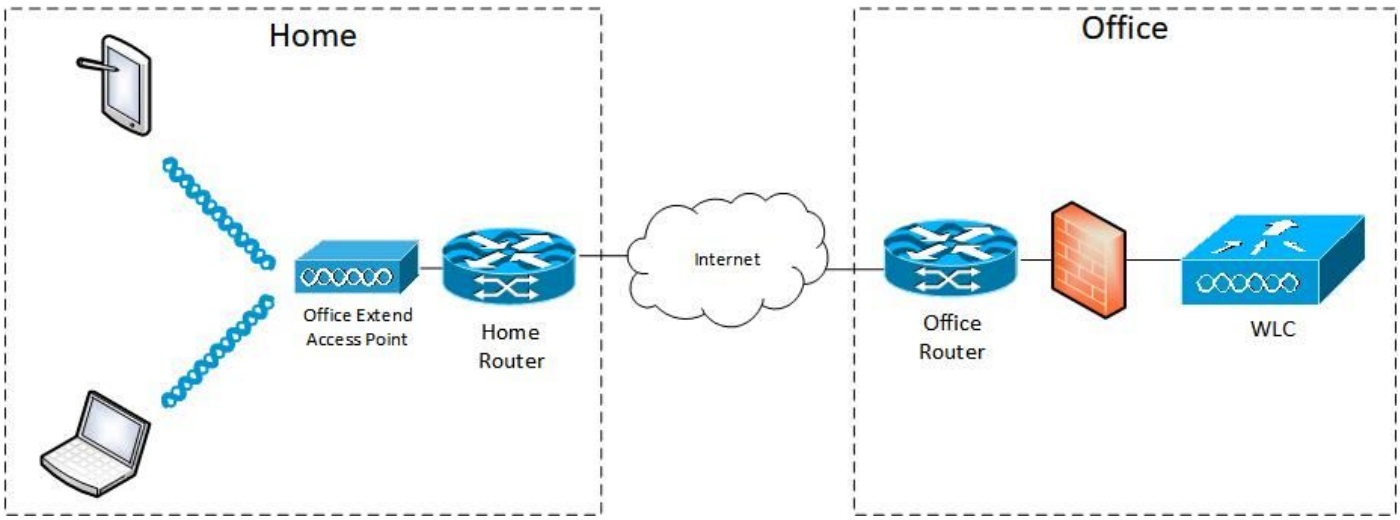
O FlexConnect refere-se à capacidade de um ponto de acesso (AP) para lidar com clientes sem fio enquanto opera em locais remotos, por exemplo, através de uma WAN. Eles também podem decidir se o tráfego dos clientes sem fio é colocado diretamente na rede no nível de AP (Local switching) ou se o tráfego é centralizado no controlador 9800 (Central Switching) e enviado de volta pela WAN, de acordo com a WLAN.

Consulte este documento Compreenda o FlexConnect no Catalyst 9800 Wireless Controller para obter informações detalhadas sobre o FlexConnect.

O modo OEAP é uma opção disponível em um AP FlexConnect, para permitir funcionalidade adicional, por exemplo, um SSID local pessoal para acesso residencial, e também pode fornecer recurso de tunelamento dividido, para uma granularidade maior para definir qual tráfego deve ser comutado localmente no escritório residencial e qual tráfego deve ser comutado centralmente na WLC, em uma única WLAN

Configurar

Diagrama de Rede



Configurações

Definição de uma lista de controle de acesso para tunelamento dividido

Etapa 1. Escolha Configuration > Security > ACL (Configuração > Segurança > ACL). Selecione Adicionar.

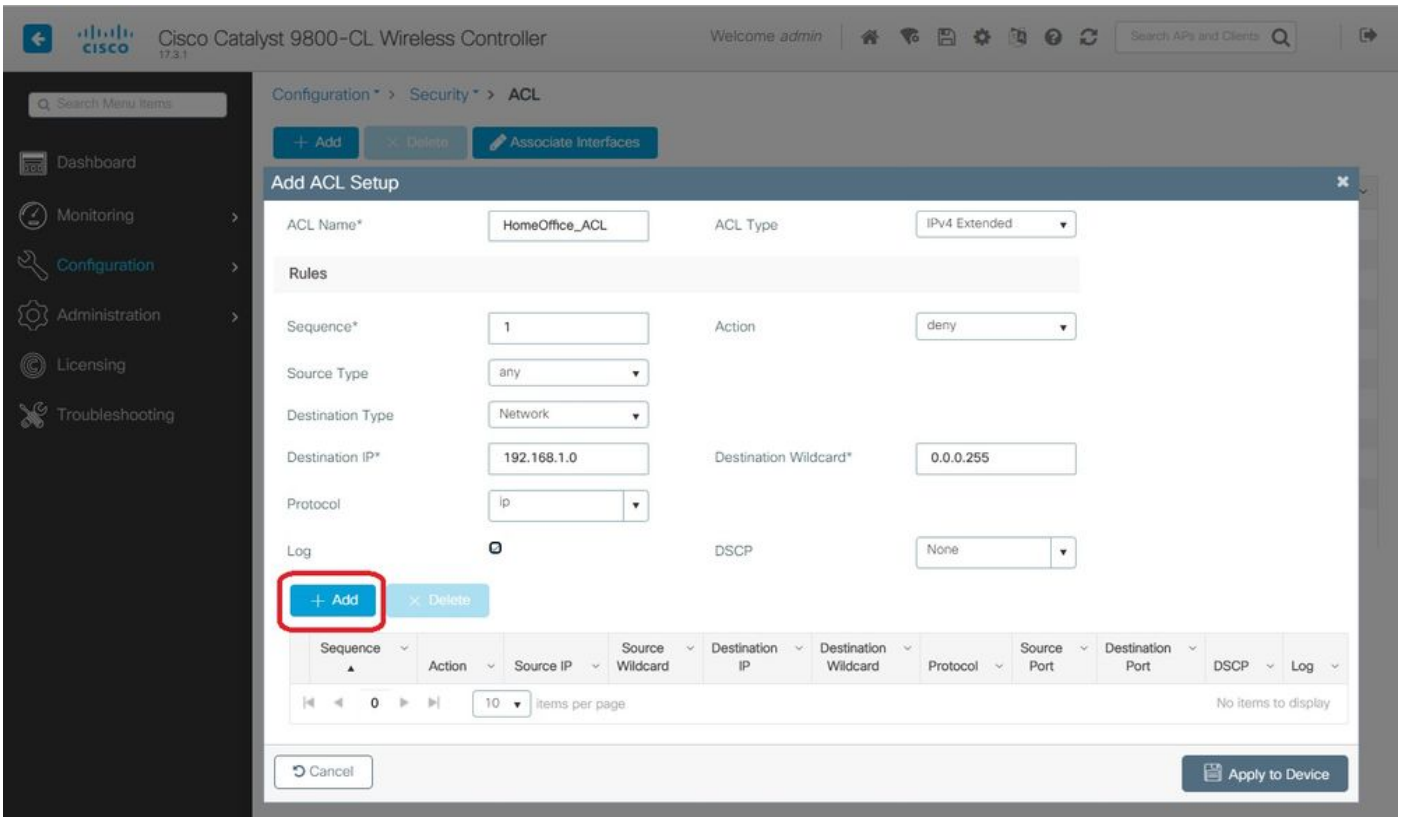
Etapa 2. Na caixa de diálogo Adicionar configuração da ACL, digite o nome da ACL, escolha o tipo da ACL na lista suspensa Tipo de ACL e, nas configurações de Regras, digite o número de sequência. Em seguida, escolha a ação como permitir ou negar.

Etapa 3. Escolha o tipo de origem necessário na lista suspensa Tipo de origem.

Se você escolher o tipo de origem como Host, você deverá digitar o Host Name/IP.

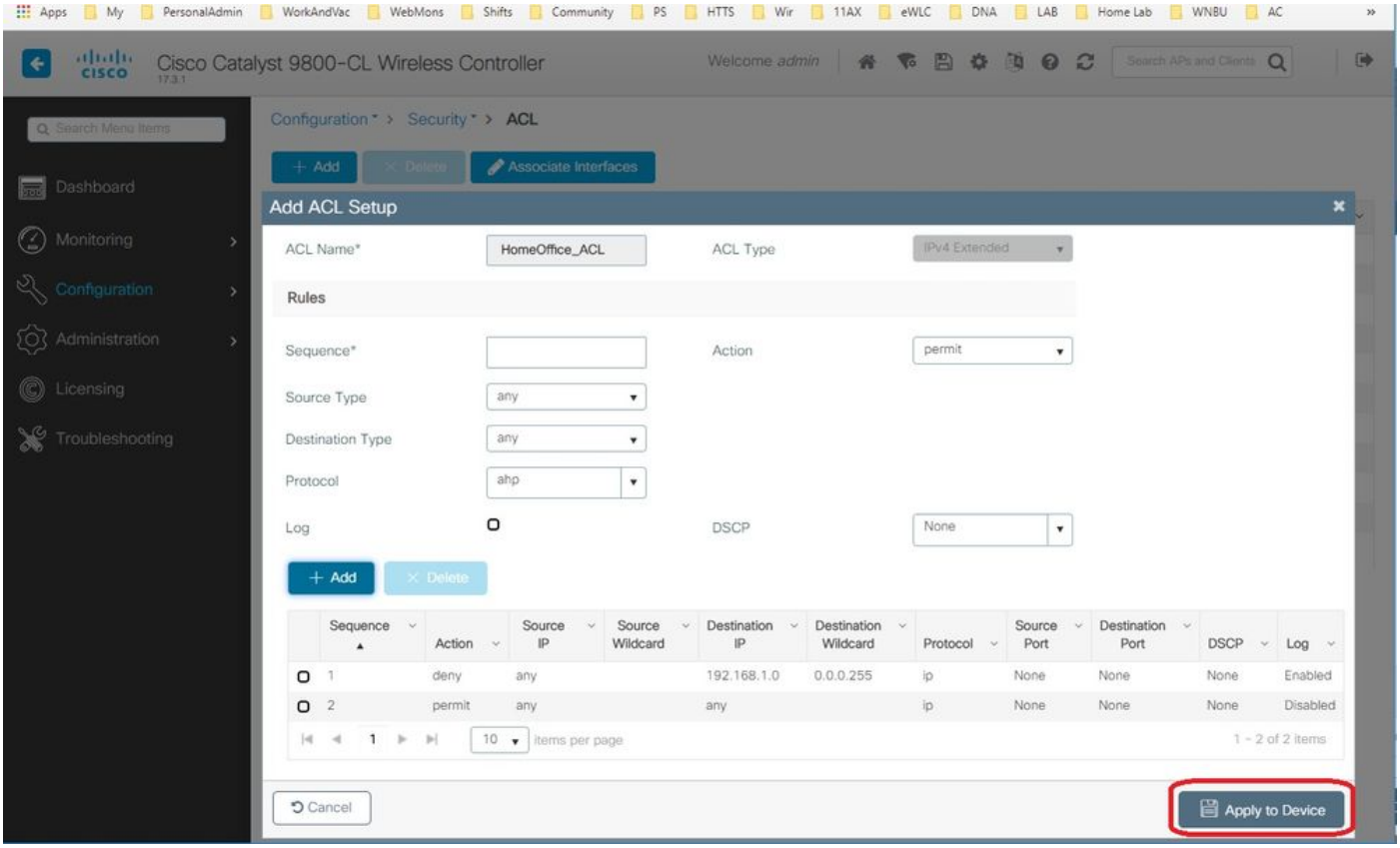
Se você escolher o tipo de origem como Rede, deverá especificar o endereço IP de origem e a máscara curinga de origem.

Neste exemplo, todo o tráfego de qualquer host para a sub-rede 192.168.1.0/24 é comutado centralmente (deny) e todo o restante do tráfego é comutado localmente (permit).



Etapa 4. Marque a caixa de seleção Log (Log) se desejar os logs e selecione Add (Adicionar).

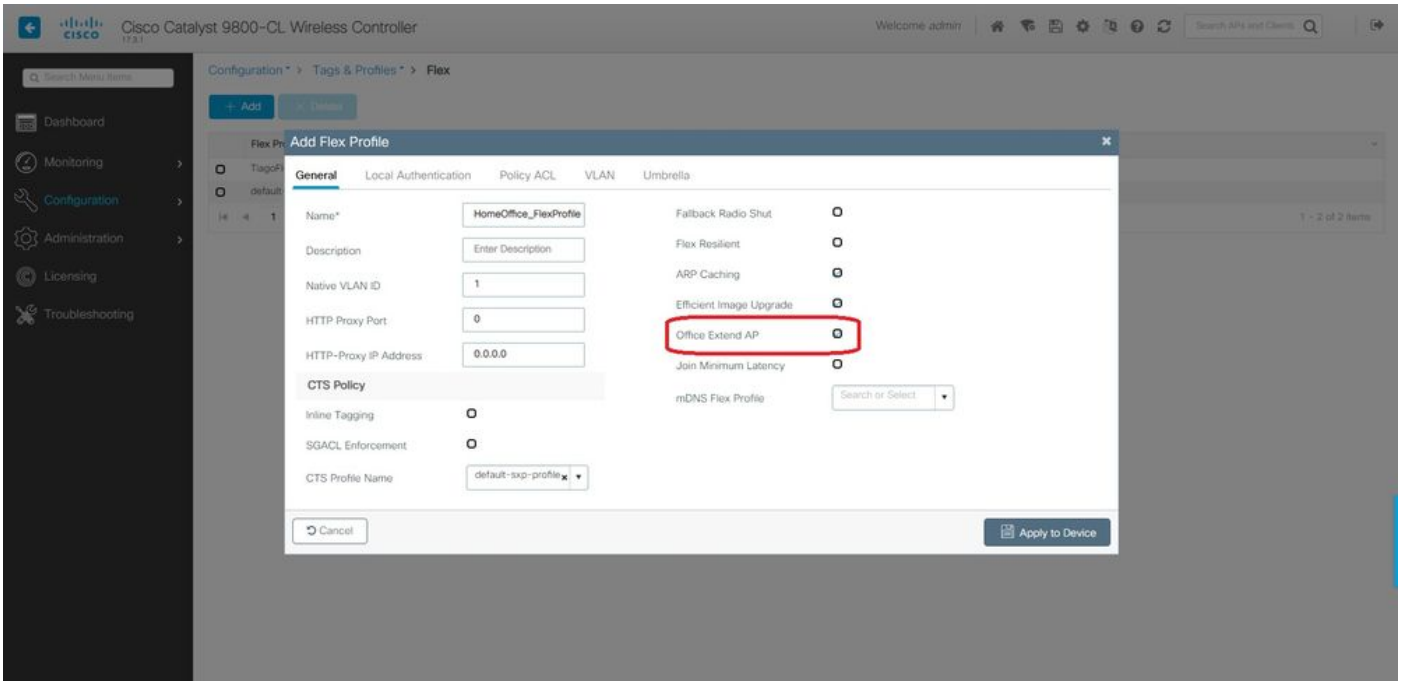
Etapa 5. Adicione o resto das regras e selecione Aplicar ao dispositivo.



Vinculando uma política de ACL à ACL definida

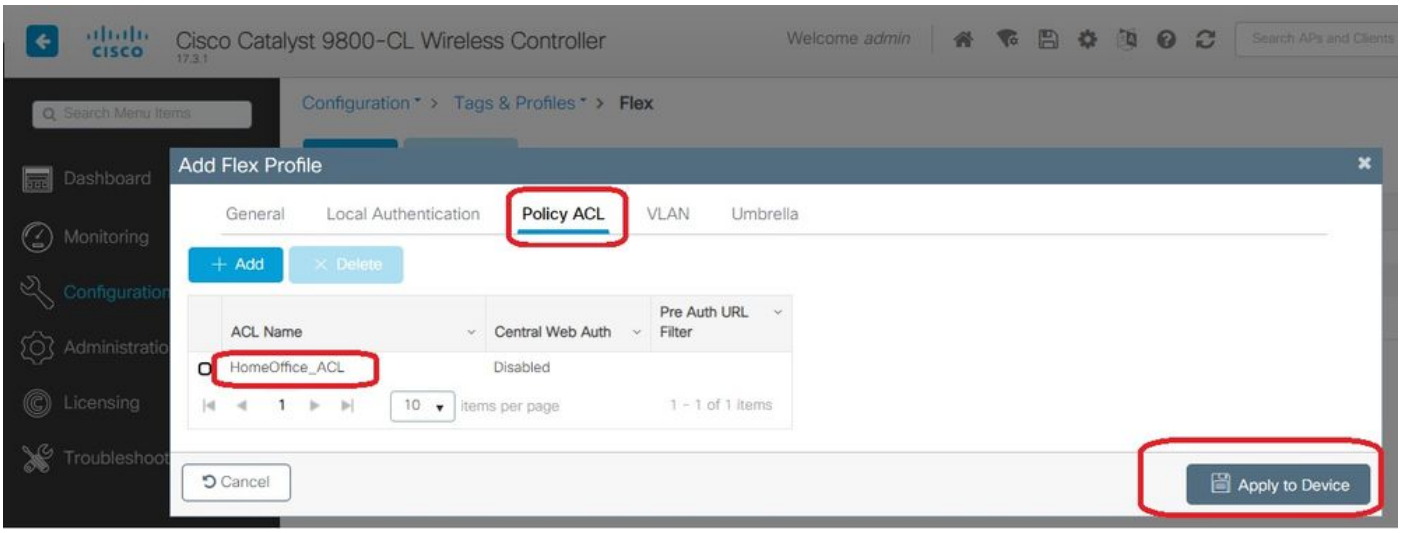
Etapa 1. Crie um novo perfil Flex. Vá para Configuration > Tags & Profiles > Flex. selecione Adicionar.

Etapa 2. Insira um nome e ative o OEAP. Além disso, certifique-se de que o ID da VLAN nativa seja o da porta do switch AP.



Note: Quando você habilita o Office-Extend Mode, a criptografia de link também é habilitada por padrão e não pode ser alterada mesmo que você desabilite a Criptografia de link no AP Join Profile.

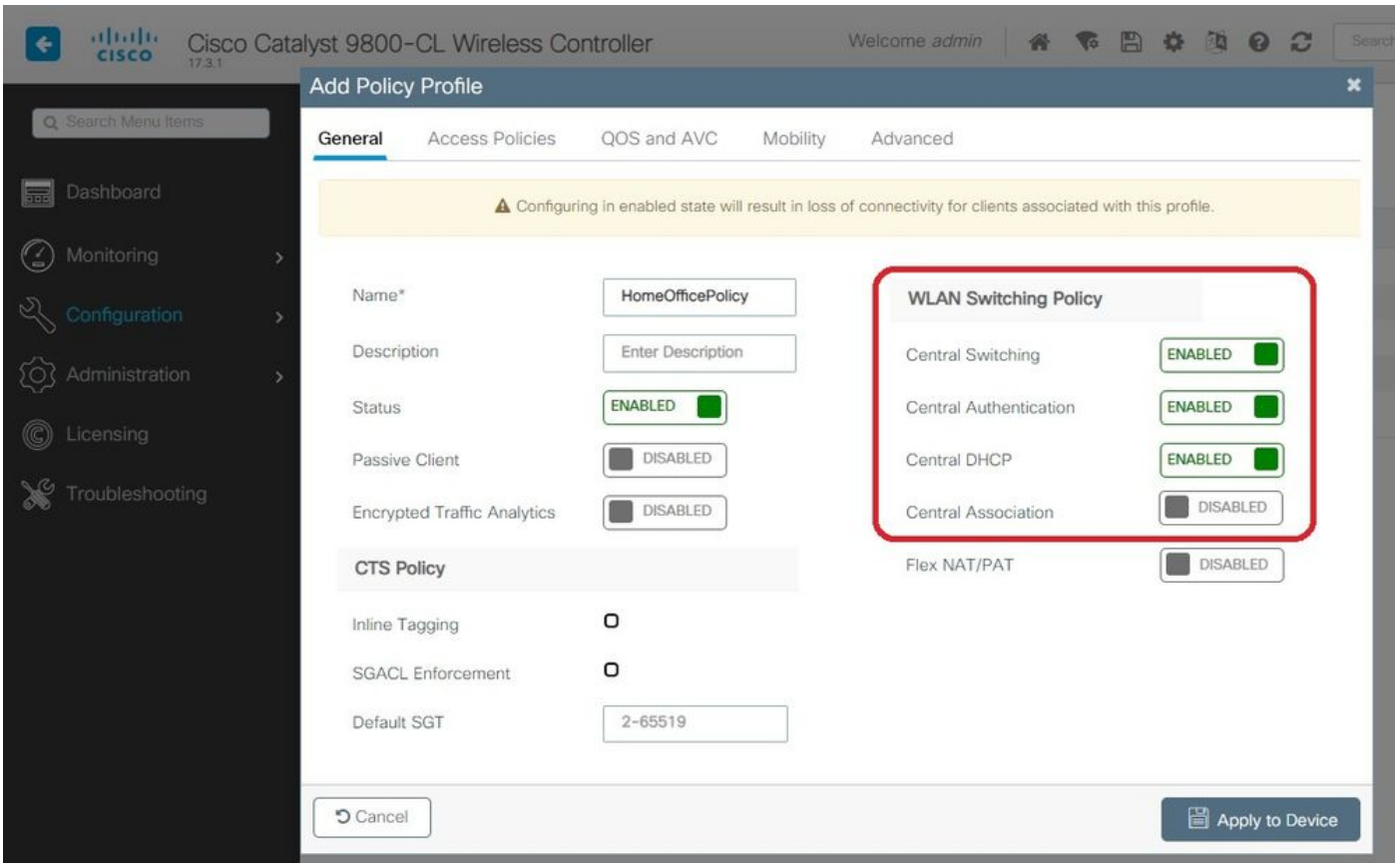
Etapa 3. Vá até a guia ACL de política e selecione Adicionar. Aqui adicione a ACL ao perfil e aplique ao dispositivo.



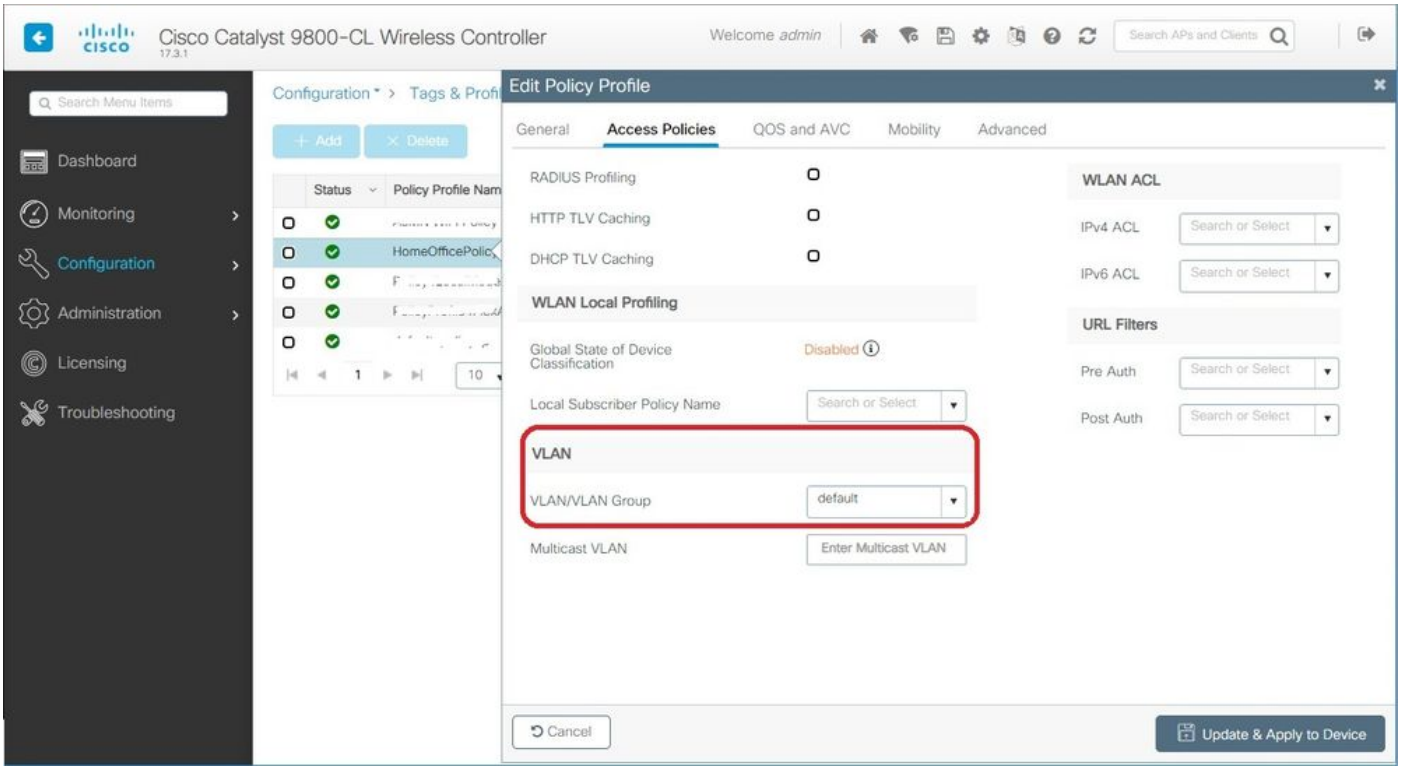
Configurando uma política de perfil de rede sem fio e um nome dividido da ACL MAC

Etapa 1. Crie um perfil de WLAN**.** Neste exemplo, ele usou um SSID chamado HomeOffice com segurança WPA2-PSK.

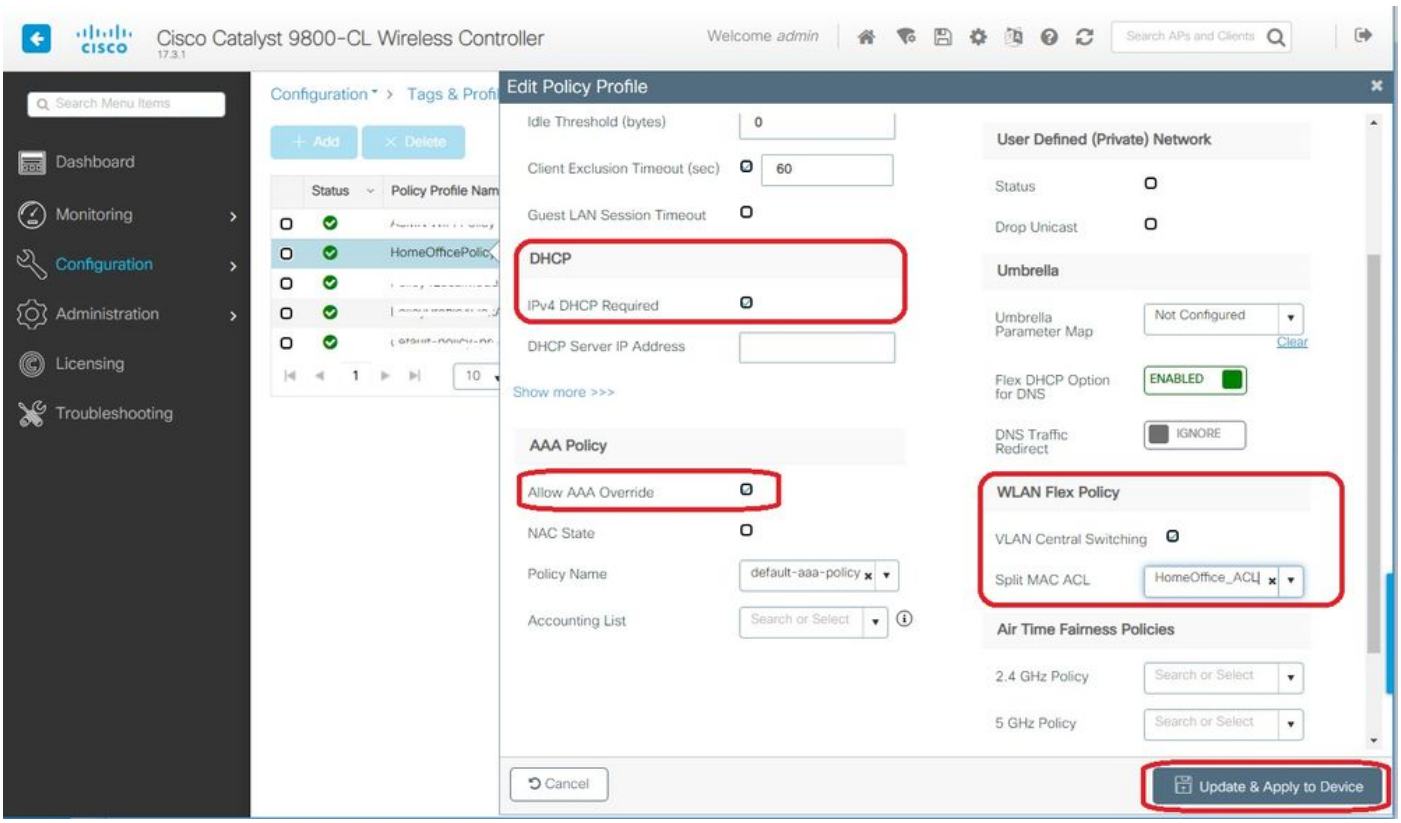
Etapa 2. Criar um perfil de política. Vá para Configuration > Tags > Policy e selecione Add. Em Geral, certifique-se de que este perfil é de políticas comutadas centralmente, como mostrado neste exemplo:



Etapa 3. Dentro do perfil de política, vá para Políticas de acesso e defina a VLAN para que o tráfego seja comutado centralmente. Os clientes obtêm um endereço IP na sub-rede atribuída a esta VLAN.



Etapa 4. Para configurar o tunelamento dividido local em um AP, você precisa garantir que tenha habilitado o DCHP obrigatório na WLAN. Isso garante que o cliente que está associado à WLAN dividida faça DHCP. Você pode habilitar essa opção no Perfil da política na guia Avançado. Ative a caixa de seleção IPv4 DHCP obrigatório. Nas configurações de política flexível da WLAN, escolha a divisão da ACL MAC criada antes, na lista suspensa Dividir ACL MAC. Selecione Aplicar ao dispositivo:



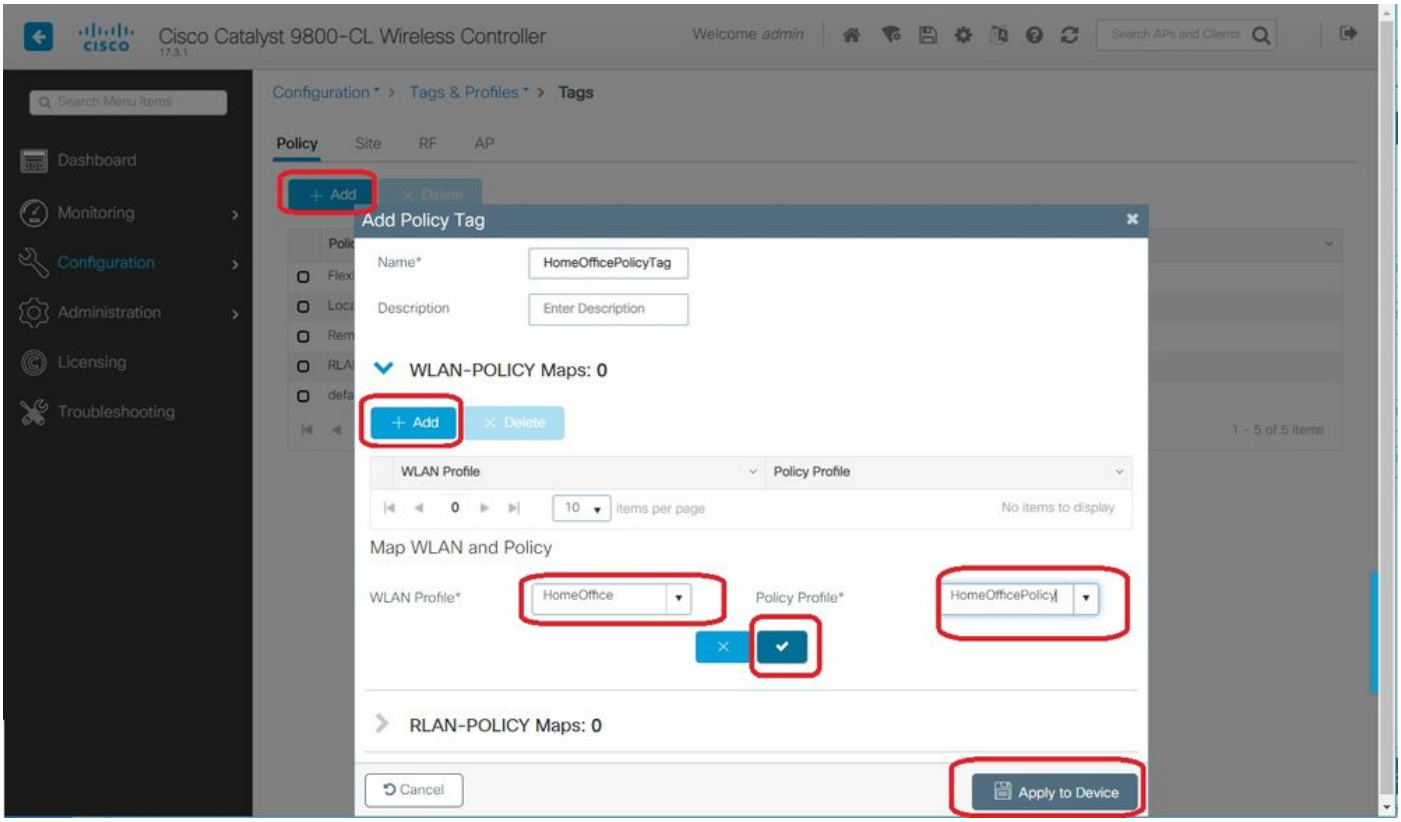
Note: Os clientes Apple iOS precisam que a opção 6 (DNS) seja definida na oferta DHCP para que o tunelamento dividido funcione.

Mapeamento de uma WLAN para um perfil de política

Etapa 1. Escolha Configuration > Tags & Profiles > Tags. Na guia Política, selecione Adicionar.

Etapa 2. Insira o nome da diretiva de marca e, na guia Mapas de política de WLAN, selecione Adicionar.

Etapa 3. Escolha o perfil da WLAN na lista suspensa Perfil da WLAN e escolha o perfil de política na lista suspensa Perfil de política. Selecione o ícone Tick e depois Apply to Device.

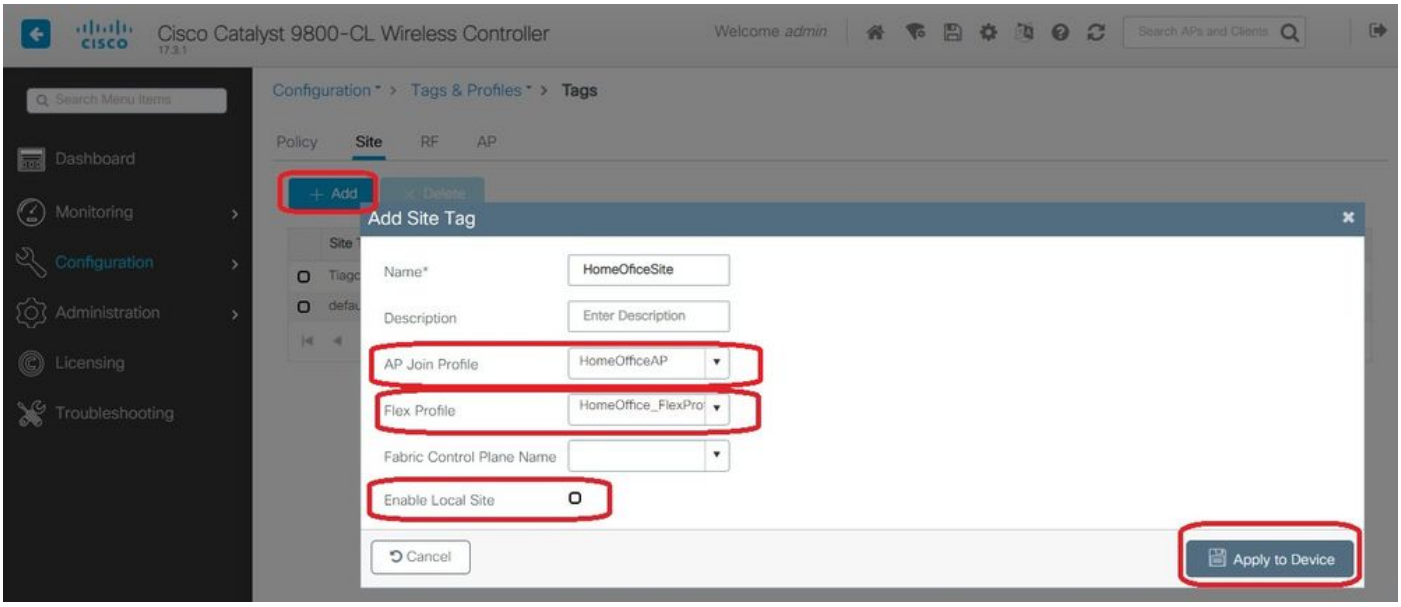


Configurando um perfil de união AP e associação com a etiqueta do site

Etapa 1. Navegue até Configuration > Tags & Profiles > AP Join e selecione Add. Digite um nome. Opcionalmente, você pode habilitar o SSH para permitir a solução de problemas e, posteriormente, desabilitá-lo se não for necessário.

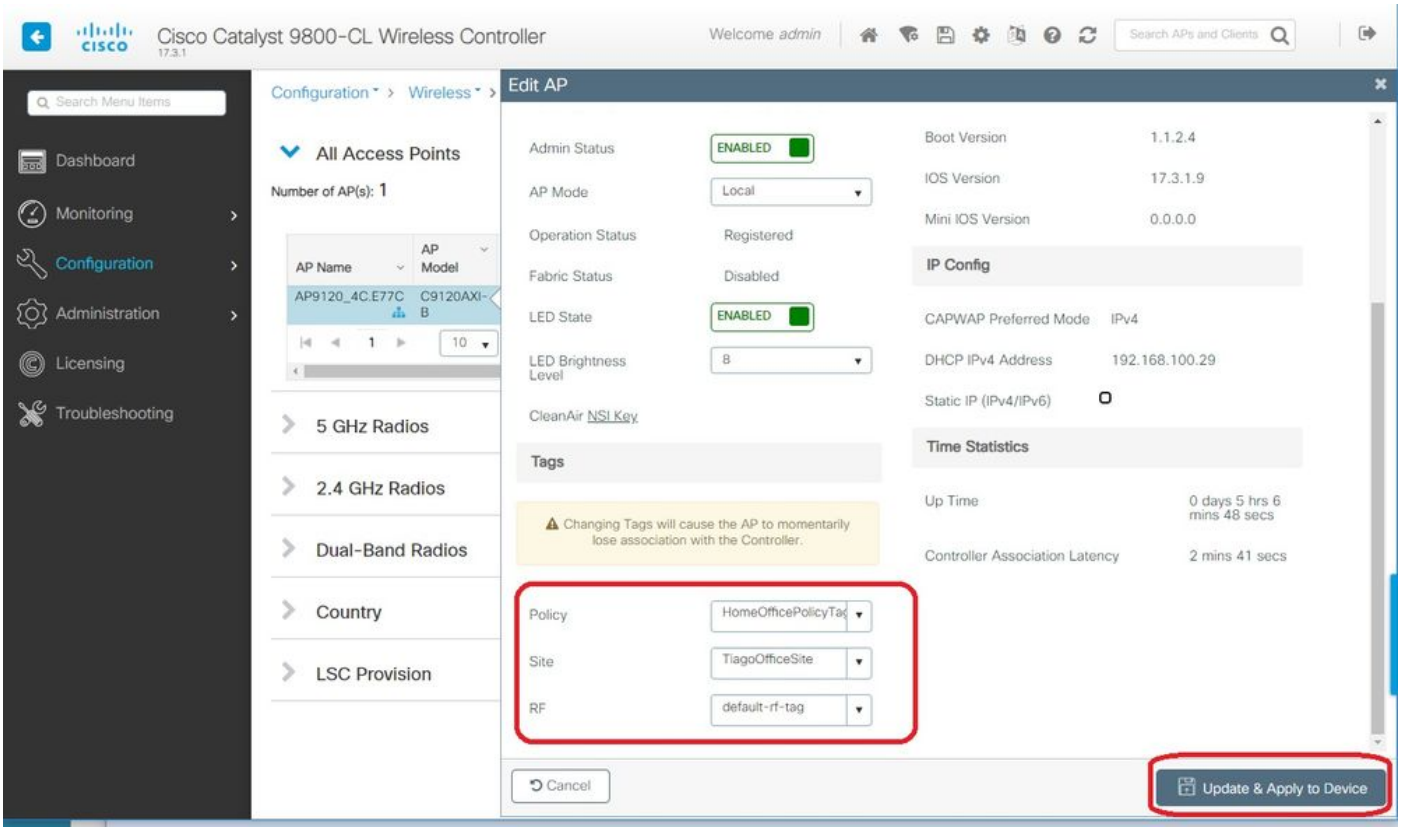
Etapa 2. Escolha Configuration > Tags & Profiles > Tags. Na guia Site, selecione Adicionar.

Etapa 3. Insira o nome da marca de site, desmarque Ativar local e selecione Perfil de junção do AP e Perfil flexível (criado antes) nas listas suspensas. Em seguida, aplique ao dispositivo.

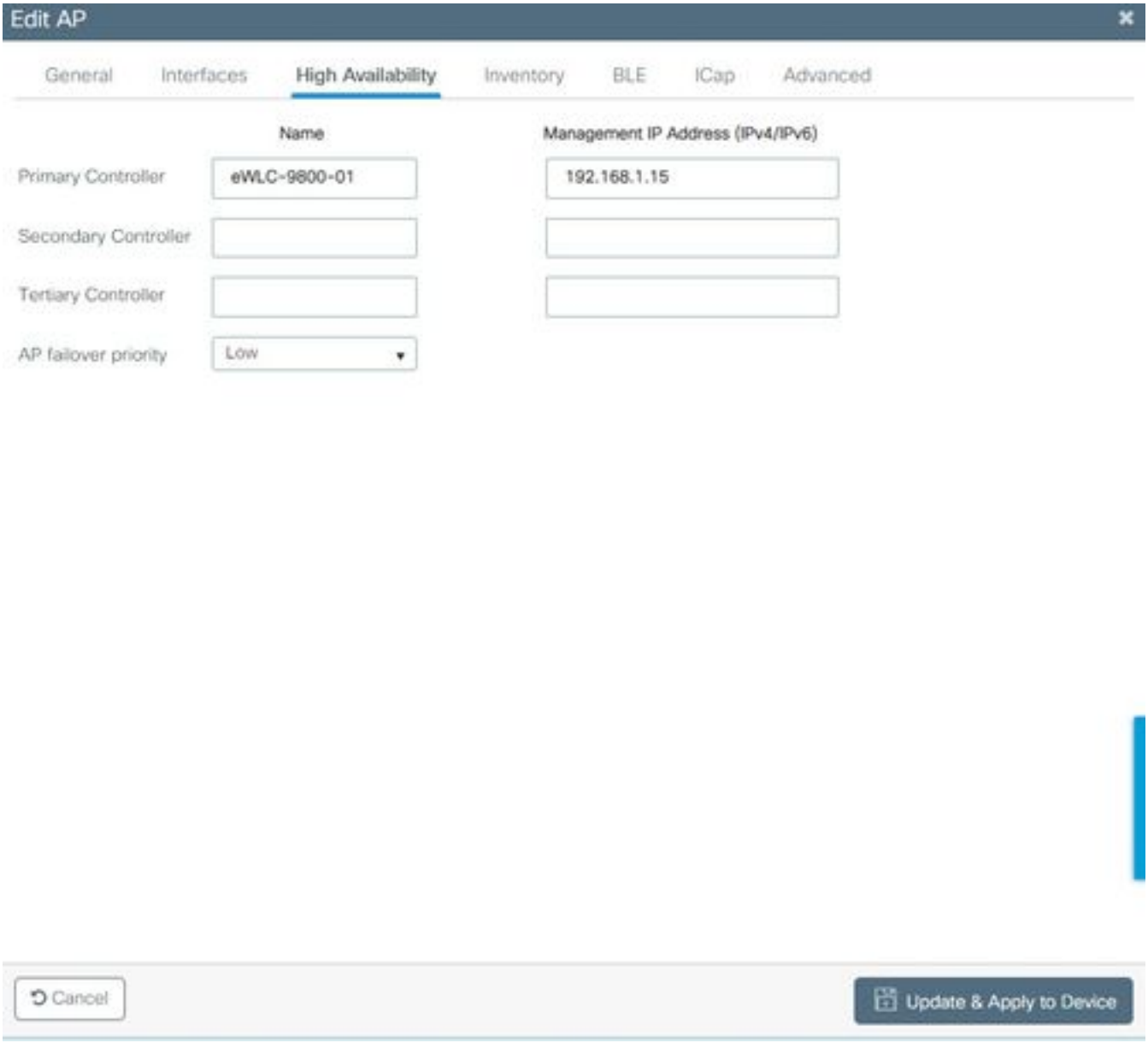


Anexando uma etiqueta de política e uma etiqueta de site a um ponto de acesso

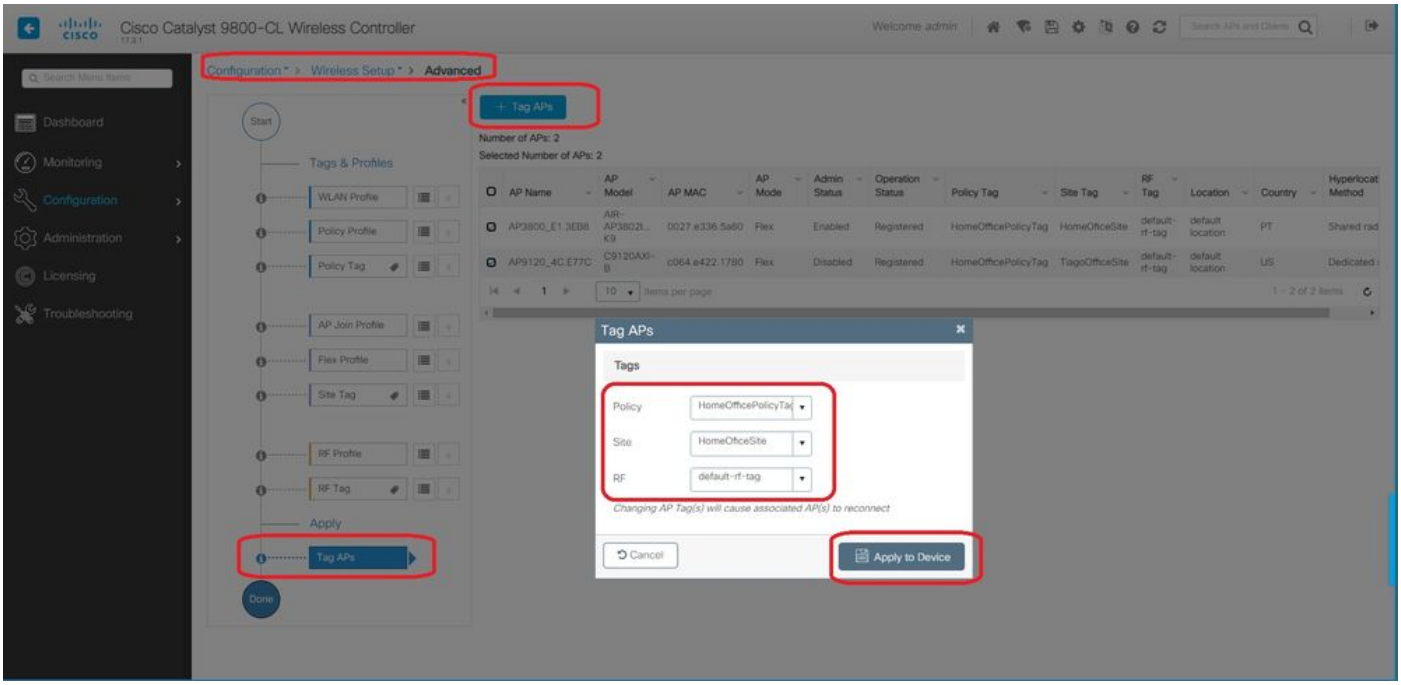
Opção 1. Essa opção exige que você configure 1 AP de cada vez. Vá para Configuration > Wireless > Access Points. Selecione o AP que deseja mover para o Home Office e selecione as Marcas do Home Office. Selecione Atualizar e Aplicar ao dispositivo:



Também é recomendável configurar um controlador principal para que o AP conheça o IP/Nome da WLC a ser acessado assim que for implantado no escritório doméstico. Você pode fazer isso editando o AP diretamente para a guia Alta disponibilidade:



Opção 2. Essa opção permite configurar vários APs simultaneamente. Navegue até Configuration > Wireless Setup > Advanced > Tag APs. Selecione as Marcas criadas anteriormente e selecione Aplicar ao dispositivo.



Os APs reinicializam e reingressam na WLC com as novas configurações.

Verificar

Você pode verificar a configuração via GUI ou CLI. Esta é a configuração resultante na 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
!
```

Verificando a configuração do 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
...
```

Você pode se conectar diretamente ao AP e também verificar a configuração:

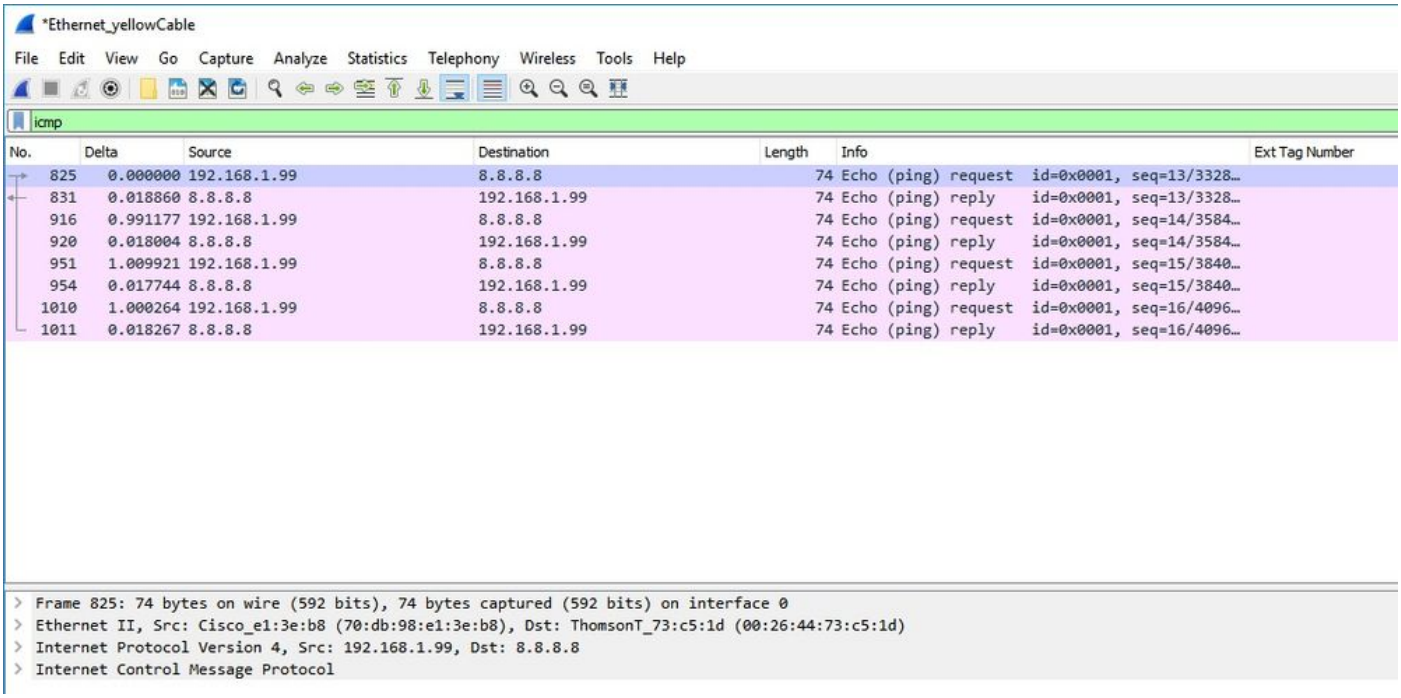
```
AP3800_E1.3EB8#show ip access-lists
Extended IP access list HomeOffice_ACL
1 deny ip any 192.168.1.0 0.0.0.255
2 permit ip any any

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
...
```

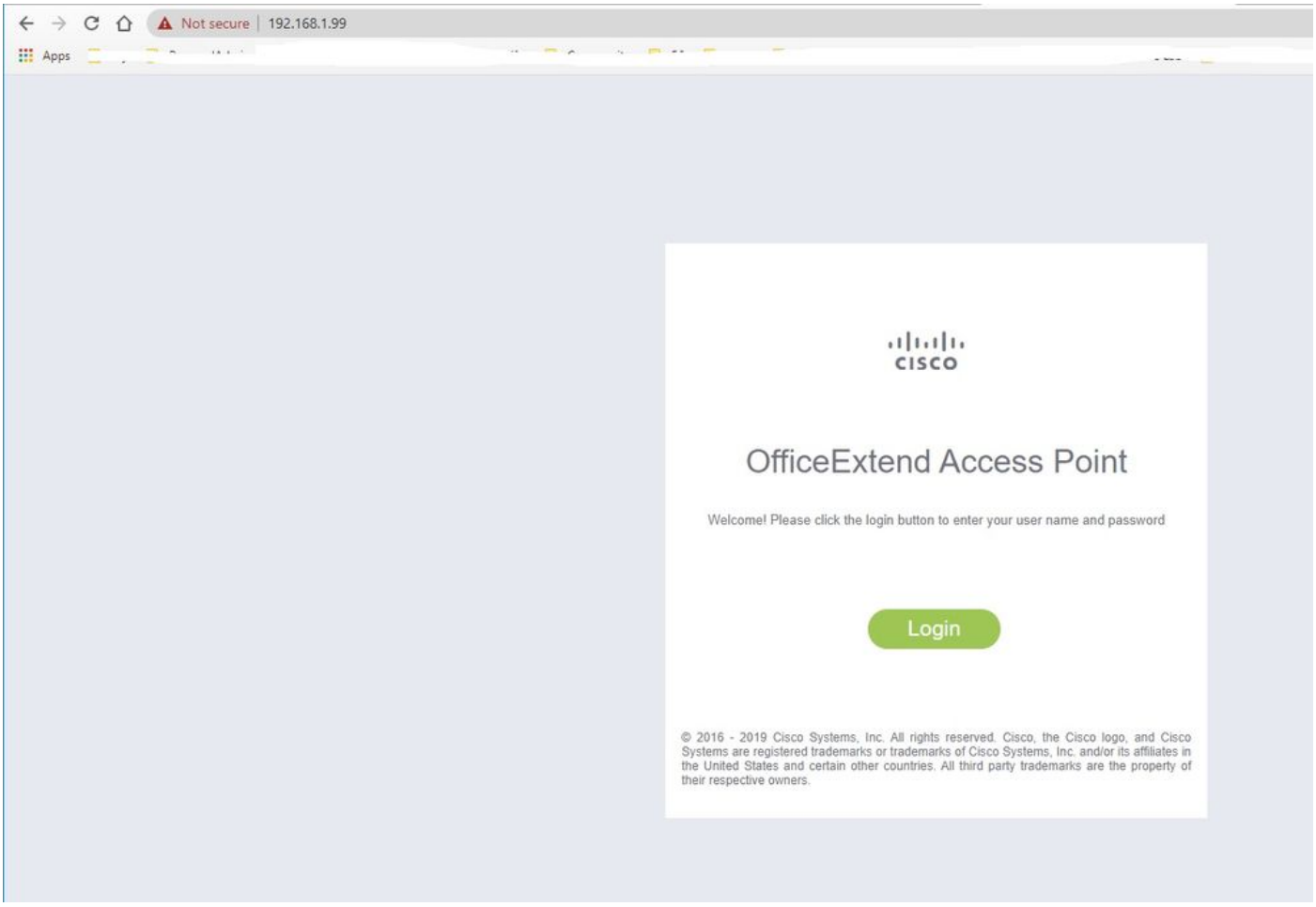
```
AP3800_E1.3EB8#show capwap client config
AdminState : ADMIN_ENABLED(1)
Name : AP3800_E1.3EB8
Location : default location
Primary controller name : eWLC-9800-01
Primary controller IP : 192.168.1.15
Secondary controller name : c3504-01
Secondary controller IP : 192.168.1.14
Tertiary controller name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

Aqui está um exemplo de capturas de pacotes que mostram o tráfego sendo comutado localmente. Aqui o teste foi feito com um "ping" de um cliente com IP 192.168.1.98 para o servidor DNS do Google e, em seguida, para 192.168.1.254. Você pode ver o ICMP originado com o IP do endereço IP do AP 192.168.1.99 enviado ao Google DNS devido ao AP NATing do tráfego localmente. Não há icmp para 192.168.1.254 porque o tráfego é criptografado no túnel DTLS e somente quadros de dados de aplicativo são vistos.

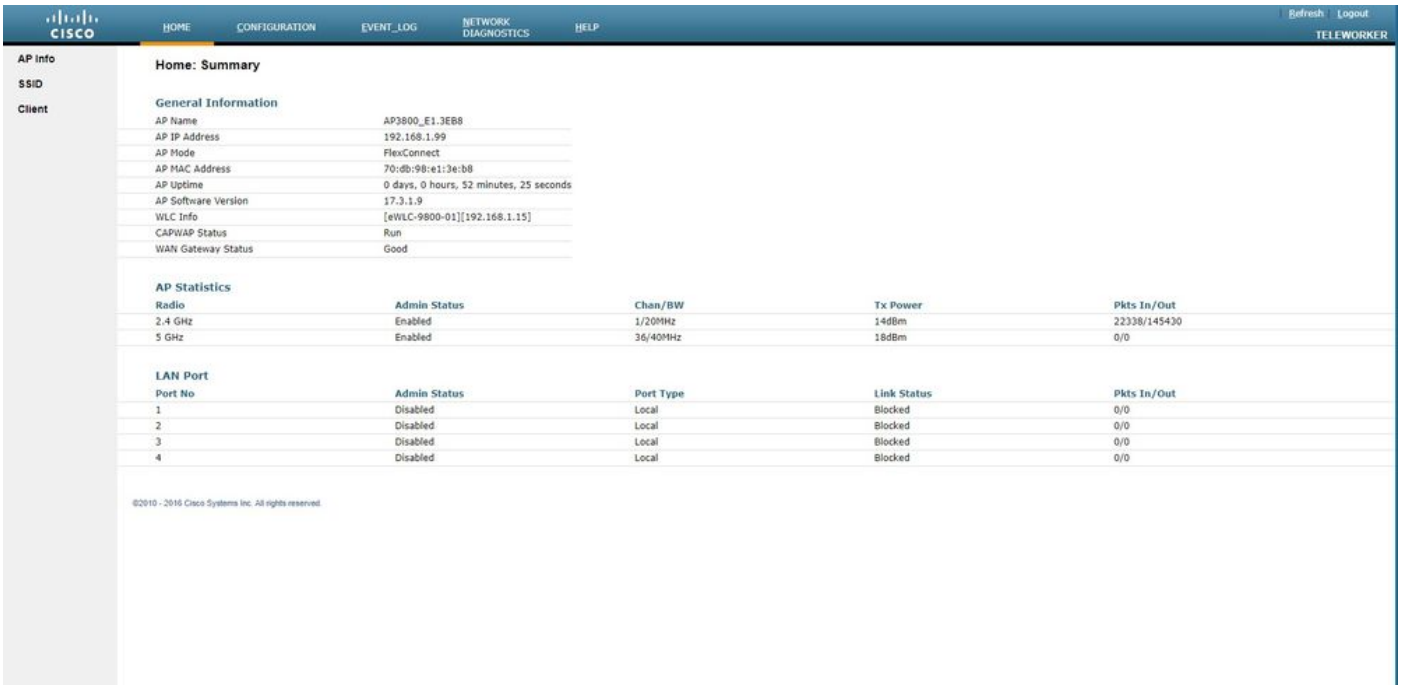


> **Note**: O tráfego que é comutado localmente é NATed pelo AP porque, em cenários normais, a sub-rede do cliente pertence à rede do Office e os dispositivos locais no escritório doméstico não sabem como acessar a sub-rede do cliente. O AP converte o tráfego do cliente usando o endereço IP do AP que está na sub-rede do home office local.

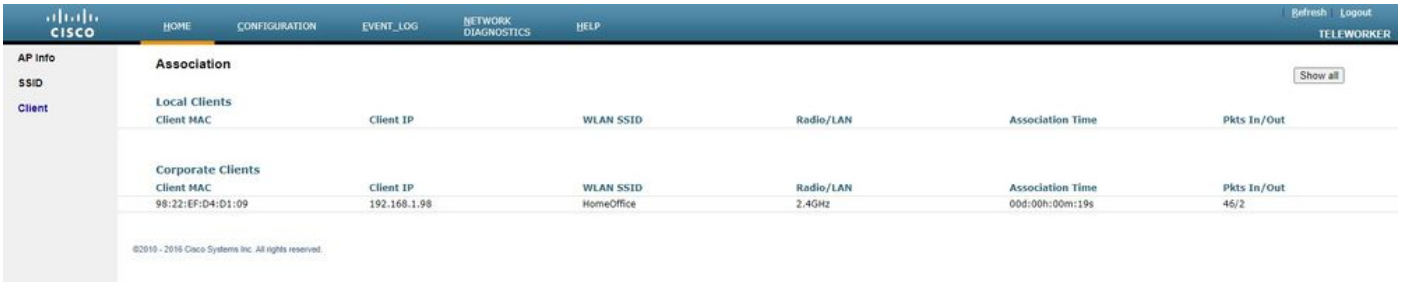
Você pode acessar a GUI do OEAP abrindo um navegador e digitando na URL o endereço ip do AP. As credenciais padrão são admin/admin e você deve alterá-las no login inicial.



Depois de fazer login, você tem acesso à GUI:



Você tem acesso a informações típicas em um OEAP, como informações de AP, SSIDs e clientes conectados:



Documentação relacionada

Entender o FlexConnect no Catalyst 9800 Wireless Controller

Separação de túneis para FlexConnect

Configurar OEAP e RLAN no Catalyst 9800 WLC