Configuration de la tunnellisation fractionnée OEAP Catalyst 9800 et FlexConnect

Contenu

Introduction

Ce document décrit comment configurer un point d'accès intérieur (AP) en tant que FlexConnect Office Extend (OEAP) et comment activer la transmission tunnel partagée afin que vous puissiez définir quel trafic peut être commuté localement au bureau à domicile et quel trafic doit être commuté centralement au WLC.

Conditions préalables

Conditions requises

La configuration de ce document suppose que le WLC est déjà configuré dans une DMZ avec NAT activé et que l'AP est capable de rejoindre le WLC depuis le bureau à domicile.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleurs LAN sans fil 9800 exécutant le logiciel Cisco IOS-XE 17.3.1.

- Points d'accès Wave1 : 1700/2700/3700 .
- Points d'accès Wave2 : Gammes 1800/2800/3800/4800 et 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Aperçu

Un point d'accès Cisco OfficeExtend (Cisco OEAP) fournit des communications sécurisées d'un WLC Cisco à un point d'accès Cisco sur un site distant, étendant de manière transparente le WLAN d'entreprise via Internet à la résidence d'un employé. L'expérience de l'utilisateur au bureau à domicile est exactement la même que celle du bureau de l'entreprise. Le chiffrement DTLS (Datagram Transport Layer Security) entre le point d'accès et le contrôleur garantit que toutes les communications ont le niveau de sécurité le plus élevé. Tout point d'accès intérieur en mode FlexConnect peut agir en tant qu'OEAP.

Informations générales

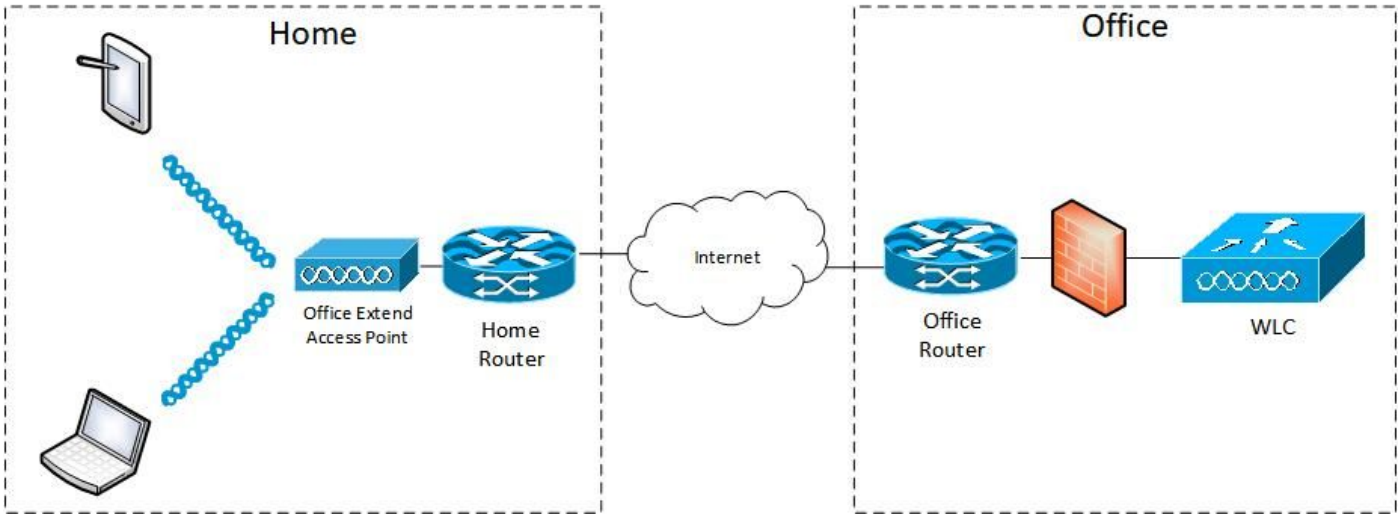
FlexConnect désigne la capacité d'un point d'accès (AP) à gérer des clients sans fil lorsqu'ils fonctionnent sur des sites distants, par exemple, sur un WAN. Ils peuvent également décider si le trafic des clients sans fil est directement placé sur le réseau au niveau du point d'accès (commutation locale) ou si le trafic est centralisé sur le contrôleur 9800 (commutation centrale) et renvoyé sur le WAN, par WLAN.

Consultez ce document Comprendre FlexConnect sur le contrôleur sans fil Catalyst 9800 pour obtenir des informations détaillées sur FlexConnect.

Le mode OEAP est une option disponible dans un point d'accès FlexConnect, pour permettre des fonctionnalités supplémentaires, par exemple, un SSID local personnel pour l'accès domestique, et peut également fournir une fonctionnalité de tunnellisation partagée, pour une granularité plus grande pour définir le trafic devant être commuté localement au bureau à domicile et le trafic devant être commuté centralement au WLC, sur un seul WLAN

Configuration

Diagramme du réseau



Configurations

Définition d'une liste de contrôle d'accès pour la transmission tunnel partagée

Étape 1. Choisissez Configuration > Security > ACL. Sélectionnez Ajouter.

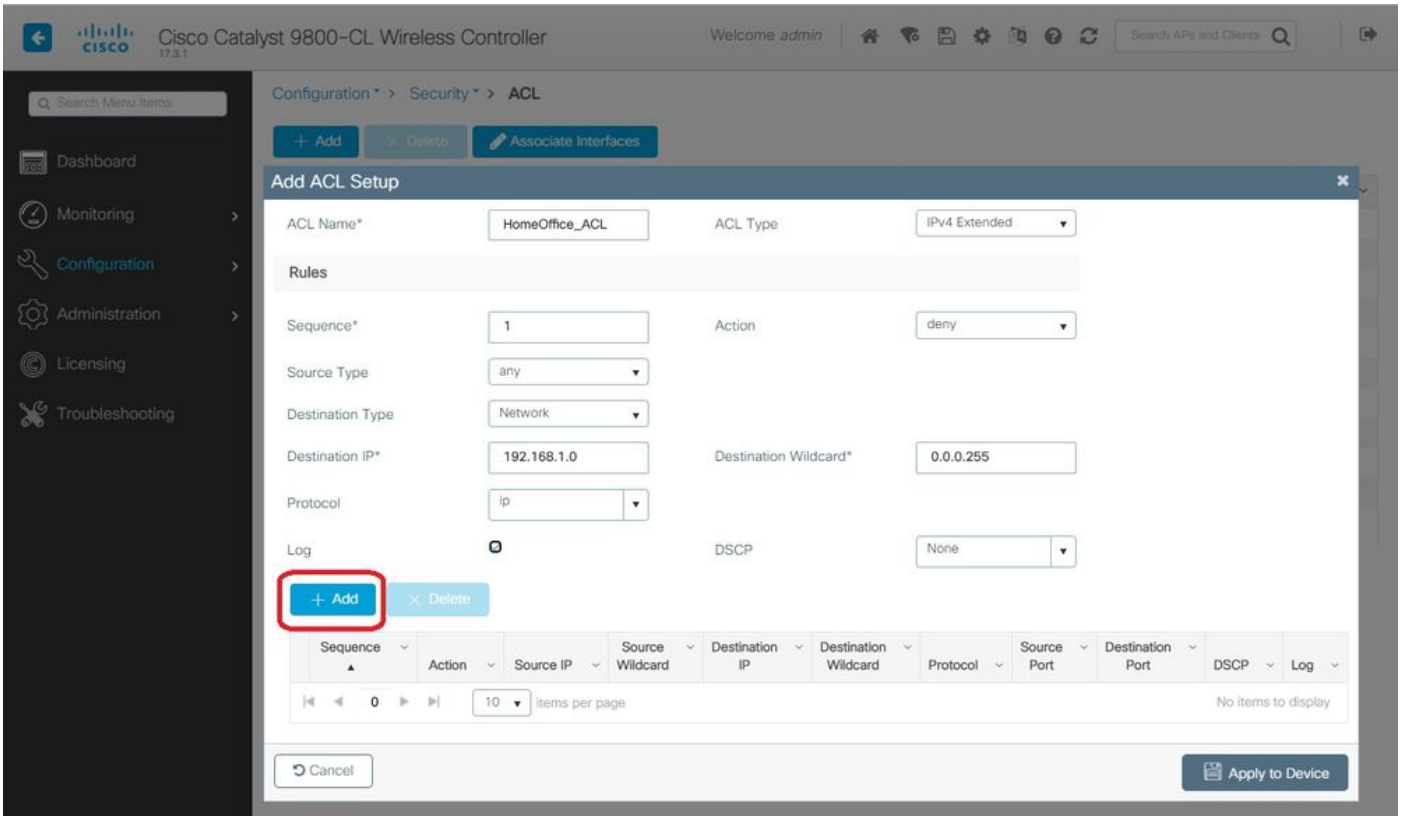
Étape 2. Dans la boîte de dialogue Ajouter une configuration de liste de contrôle d'accès, saisissez le nom de la liste de contrôle d'accès, sélectionnez le type de liste dans la liste déroulante Type de liste de contrôle d'accès et, sous les paramètres Règles, saisissez le numéro de séquence. Choisissez ensuite l'action comme autorisation ou refus.

Étape 3. Choisissez le type de source requis dans la liste déroulante Type de source.

Si vous choisissez le type source comme Hôte, vous devez entrer le nom d'hôte/l'adresse IP.

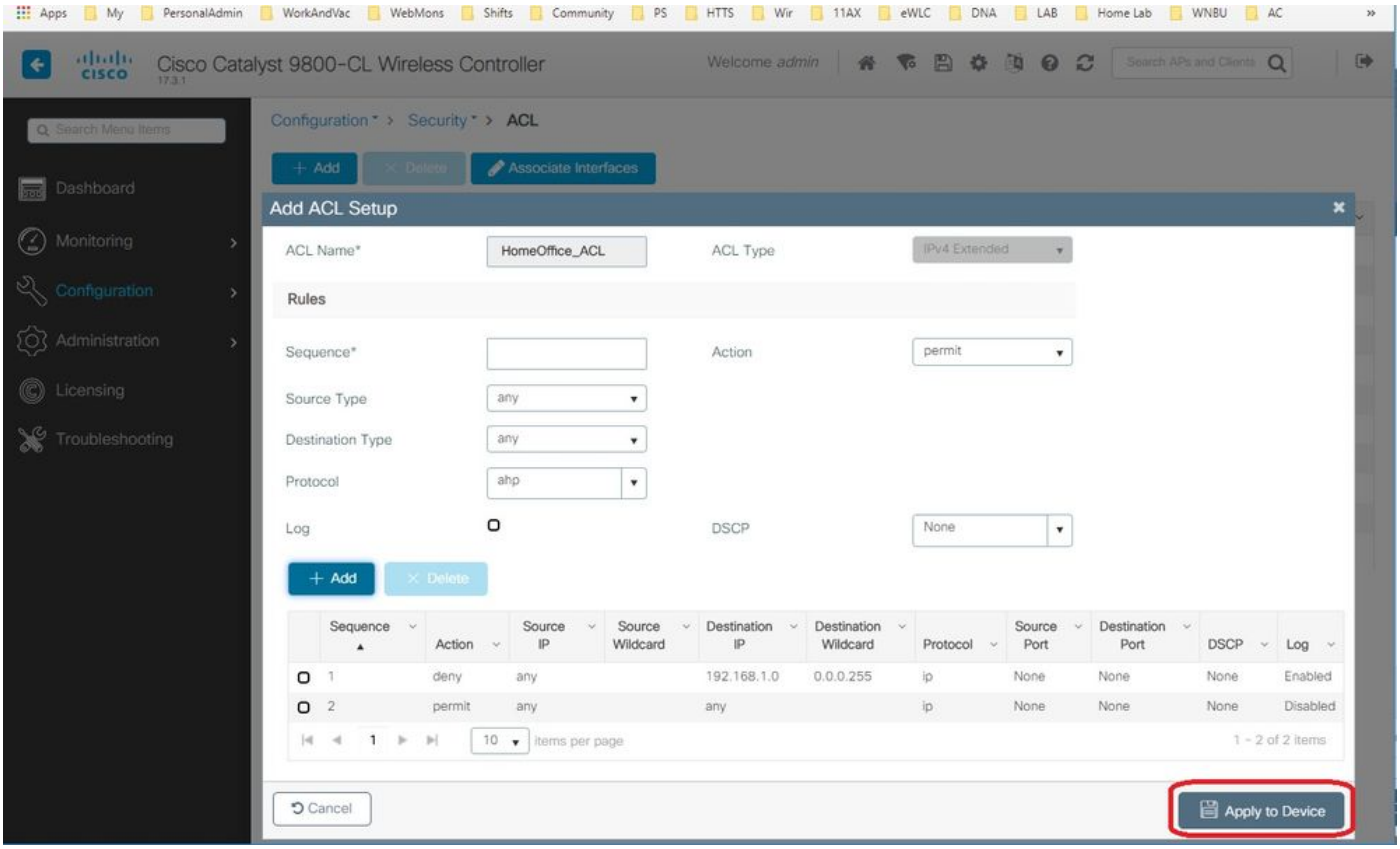
Si vous choisissez le type de source comme Réseau, vous devez spécifier l'adresse IP source et le masque générique source.

Dans cet exemple, tout le trafic de n'importe quel hôte vers le sous-réseau 192.168.1.0/24 est commuté de manière centralisée (deny) et tout le reste du trafic est commuté localement (permit).



Étape 4. Cochez la case Log (Journal) si vous souhaitez afficher les journaux, puis sélectionnez Add (Ajouter).

Étape 5. Ajoutez le reste des règles et sélectionnez Appliquer au périphérique.

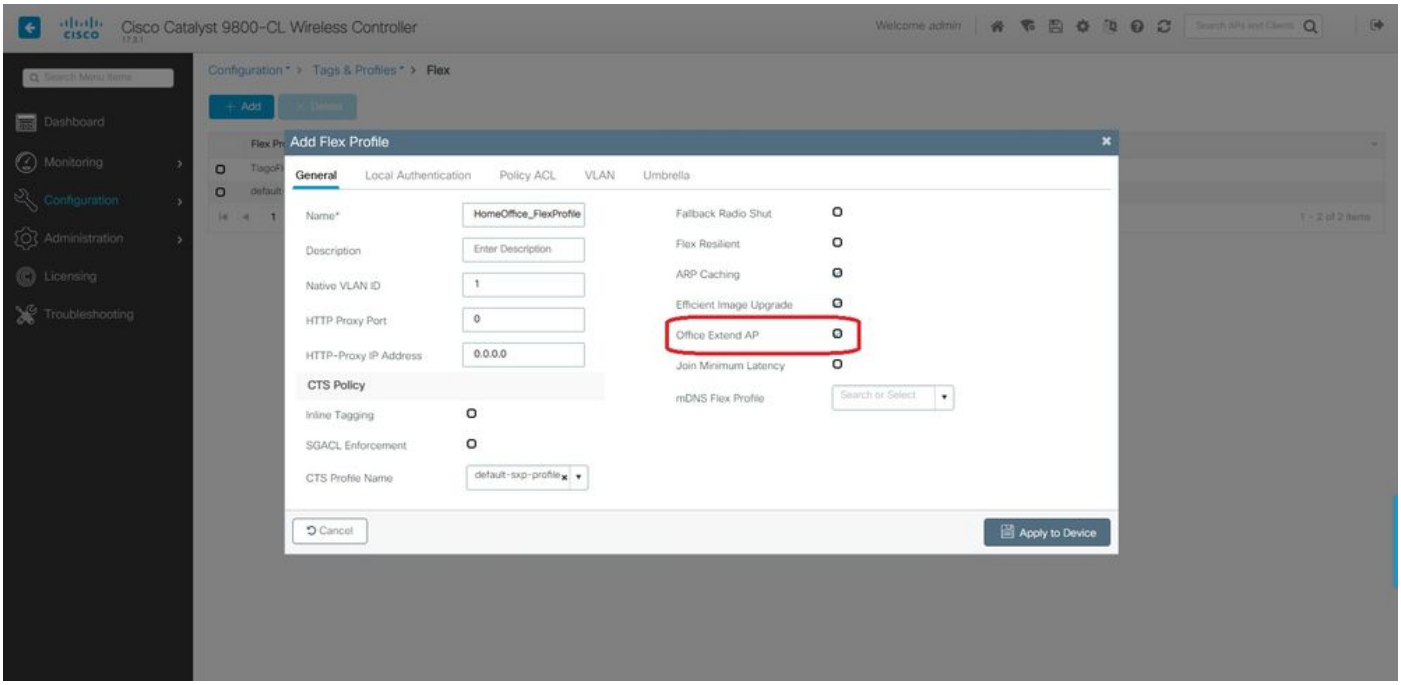


Liaison d'une stratégie de liste de contrôle d'accès à la liste de contrôle d'accès définie

Étape 1. Créez un profil flexible. Accédez à Configuration > Tags & Profiles > Flex. sélectionnez

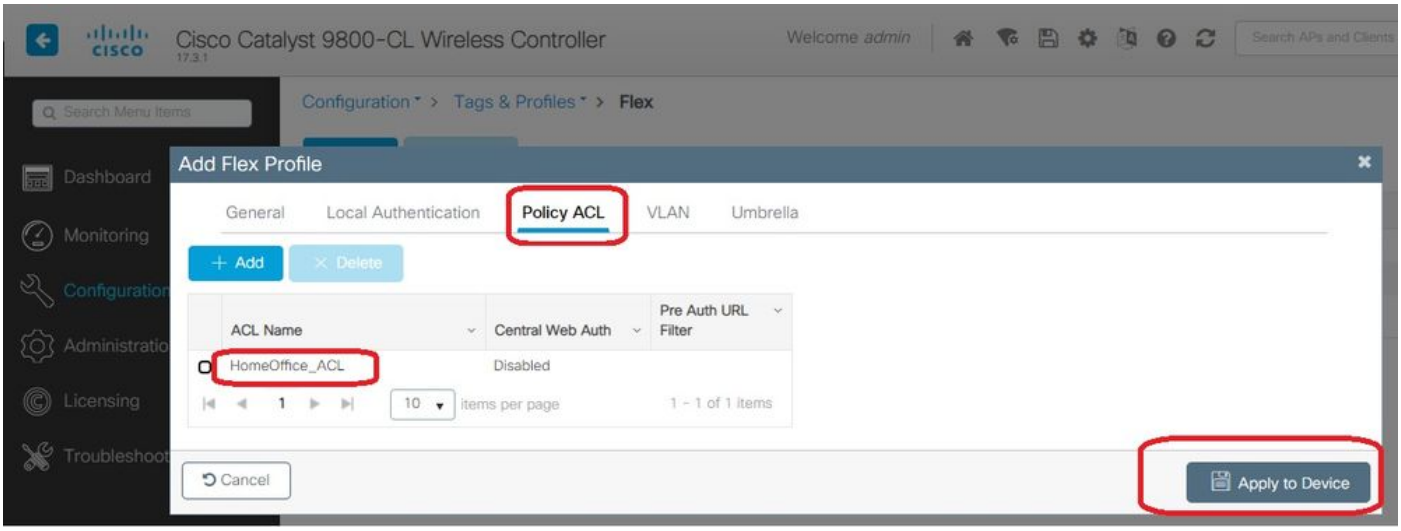
Ajouter.

Étape 2. Entrez un nom et activez OEAP. Vérifiez également que l'ID de VLAN natif est celui du port de commutation AP.



Note: Lorsque vous activez le mode Office-Extend, le chiffrement de liaison est également activé par défaut et ne peut pas être modifié même si vous désactivez le chiffrement de liaison dans le profil de jointure AP.

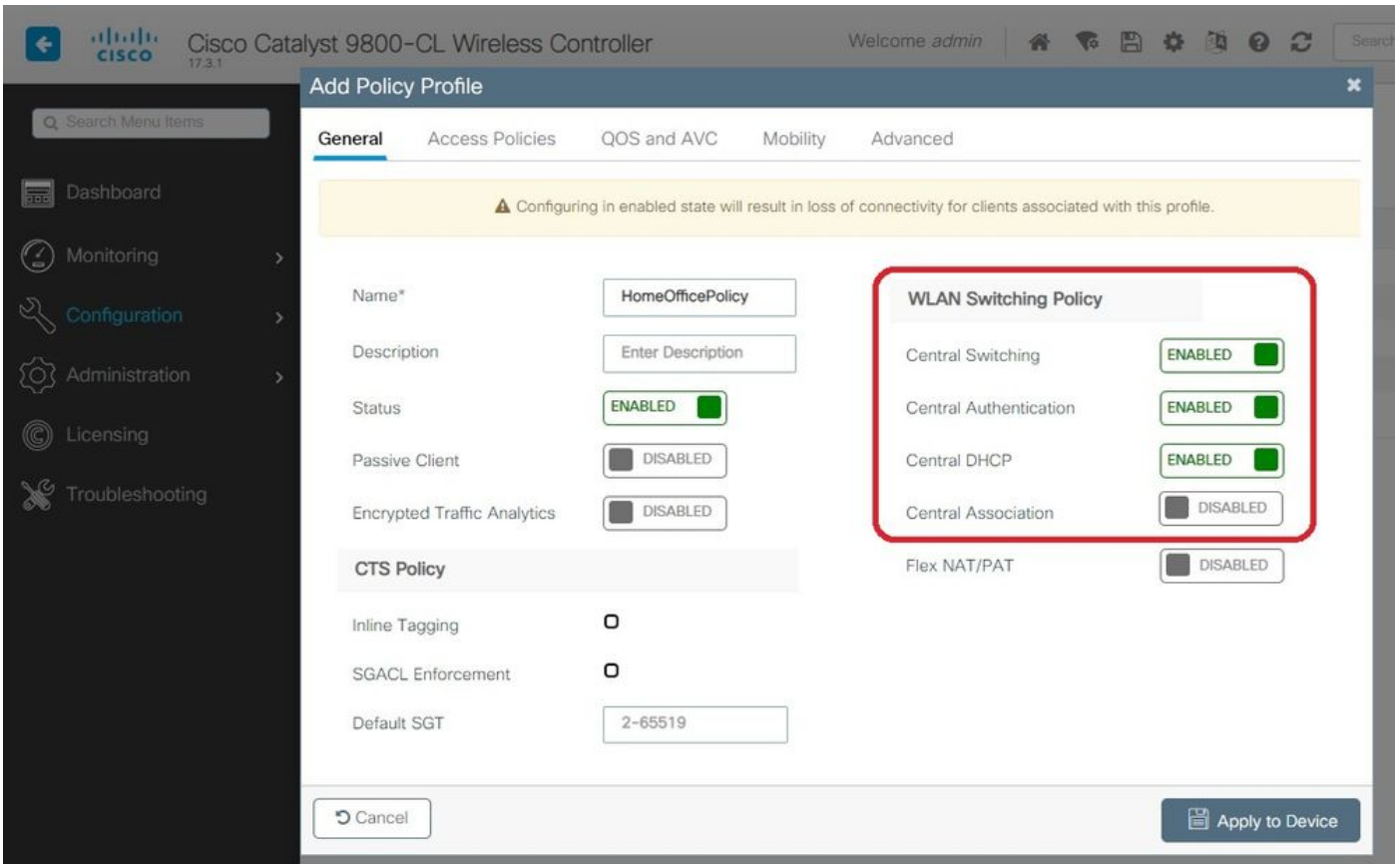
Étape 3. Accédez à l'onglet Liste de contrôle d'accès de stratégie et sélectionnez Ajouter. Ajoutez la liste de contrôle d'accès au profil et appliquez-la au périphérique.



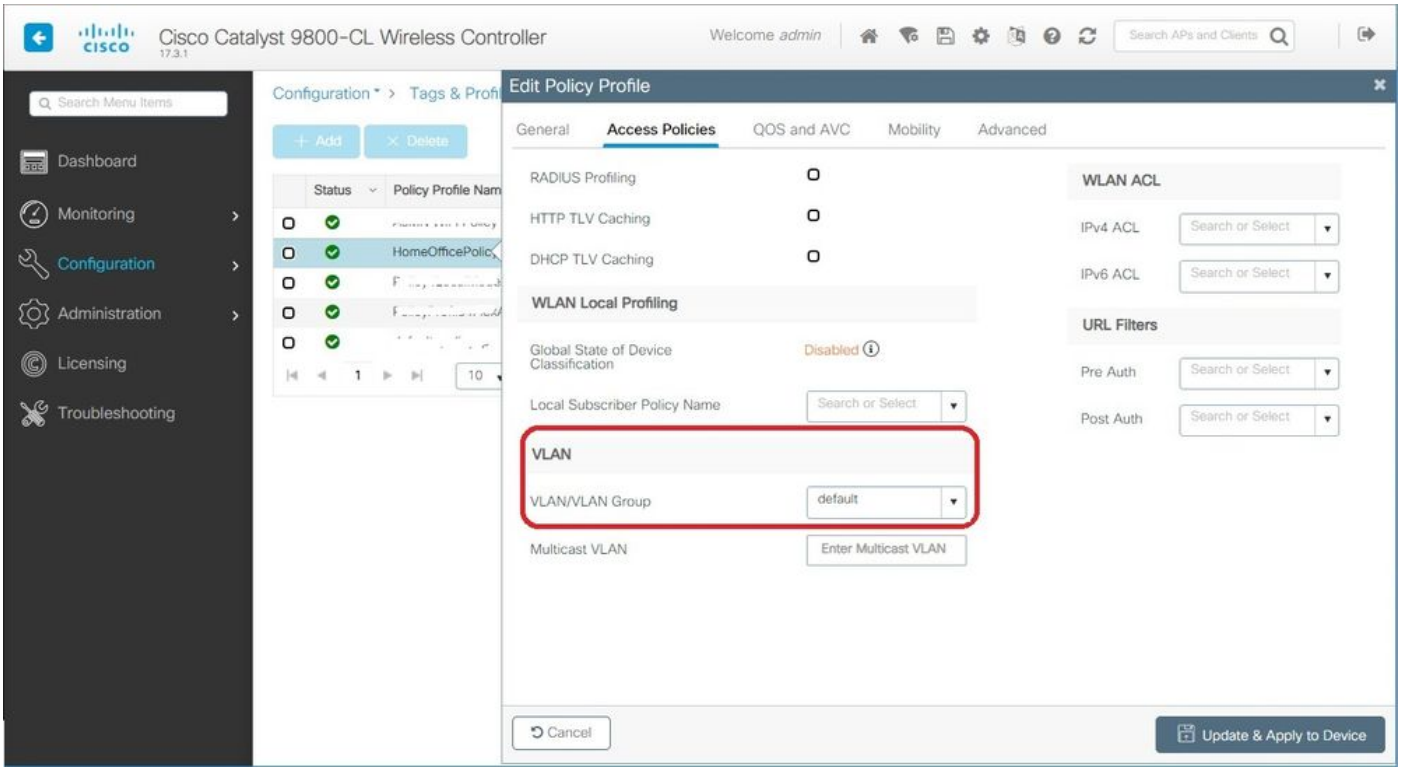
Configuration d'une stratégie de profil sans fil et d'un nom de liste de contrôle d'accès MAC partagée

Étape 1. Créez un profil WLAN. Dans cet exemple, il a utilisé un SSID nommé HomeOffice avec la sécurité WPA2-PSK.

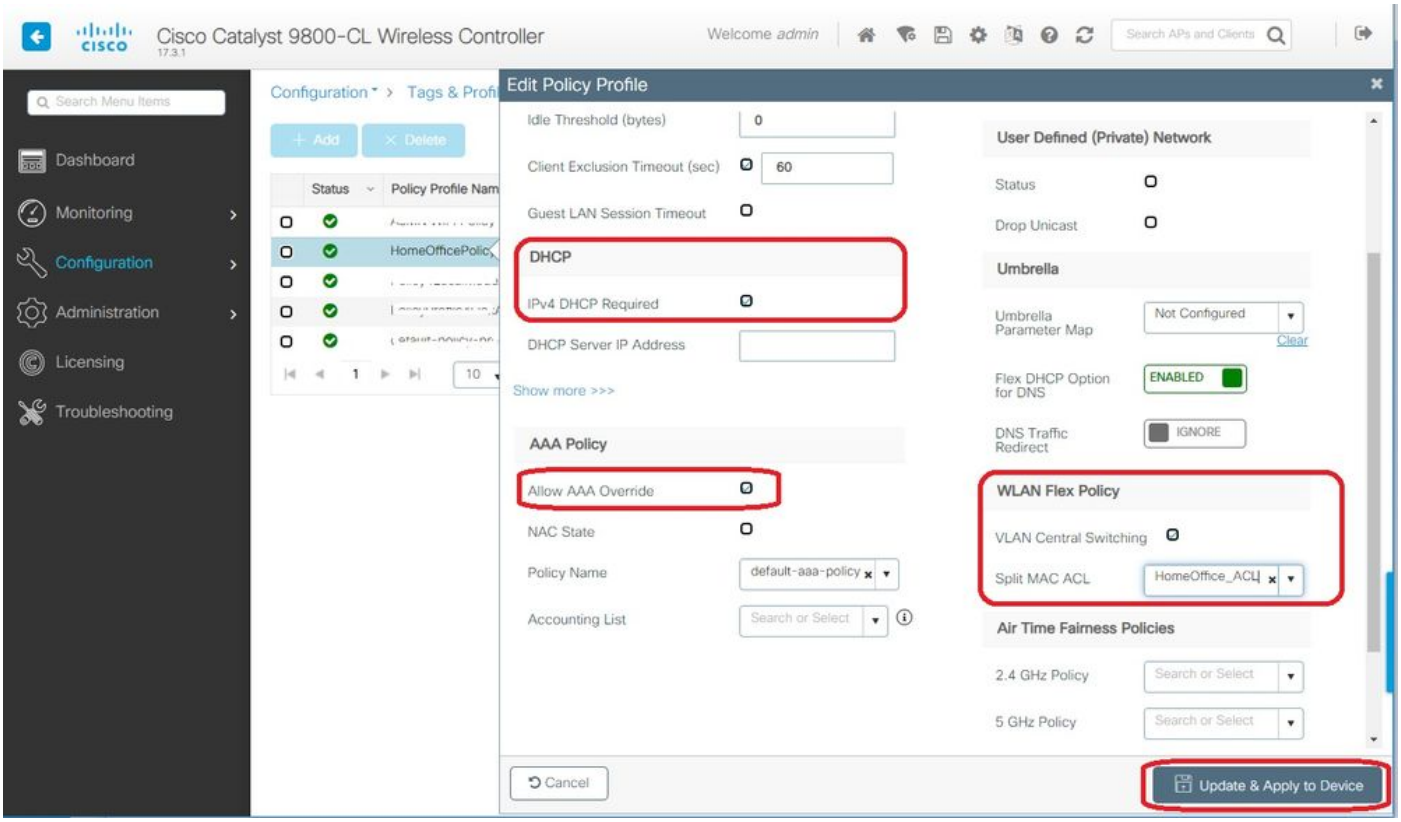
Étape 2. Créez un profil de stratégie. Accédez à Configuration > Tags > Policy et sélectionnez Add. Sous Général, assurez-vous que ce profil est des stratégies commutées de manière centralisée comme indiqué dans cet exemple :



Étape 3. Dans le profil de stratégie, accédez à Politiques d'accès et définissez le VLAN pour le trafic à commuter de manière centralisée. Les clients obtiennent une adresse IP dans le sous-réseau attribué à ce VLAN.



Étape 4. Pour configurer la transmission tunnel partagée locale sur un point d'accès, vous devez vous assurer que vous avez activé DCHP Required sur le WLAN. Cela garantit que le client associé au WLAN partagé fait le DHCP. Vous pouvez activer cette option dans le profil de stratégie sous l'onglet Avancé. Activez la case à cocher IPv4 DHCP Required. Sous Paramètres de stratégie flexible WLAN, sélectionnez la liste de contrôle d'accès MAC fractionnée créée précédemment dans la liste déroulante Liste de contrôle d'accès MAC fractionnée. Sélectionnez Appliquer au périphérique :



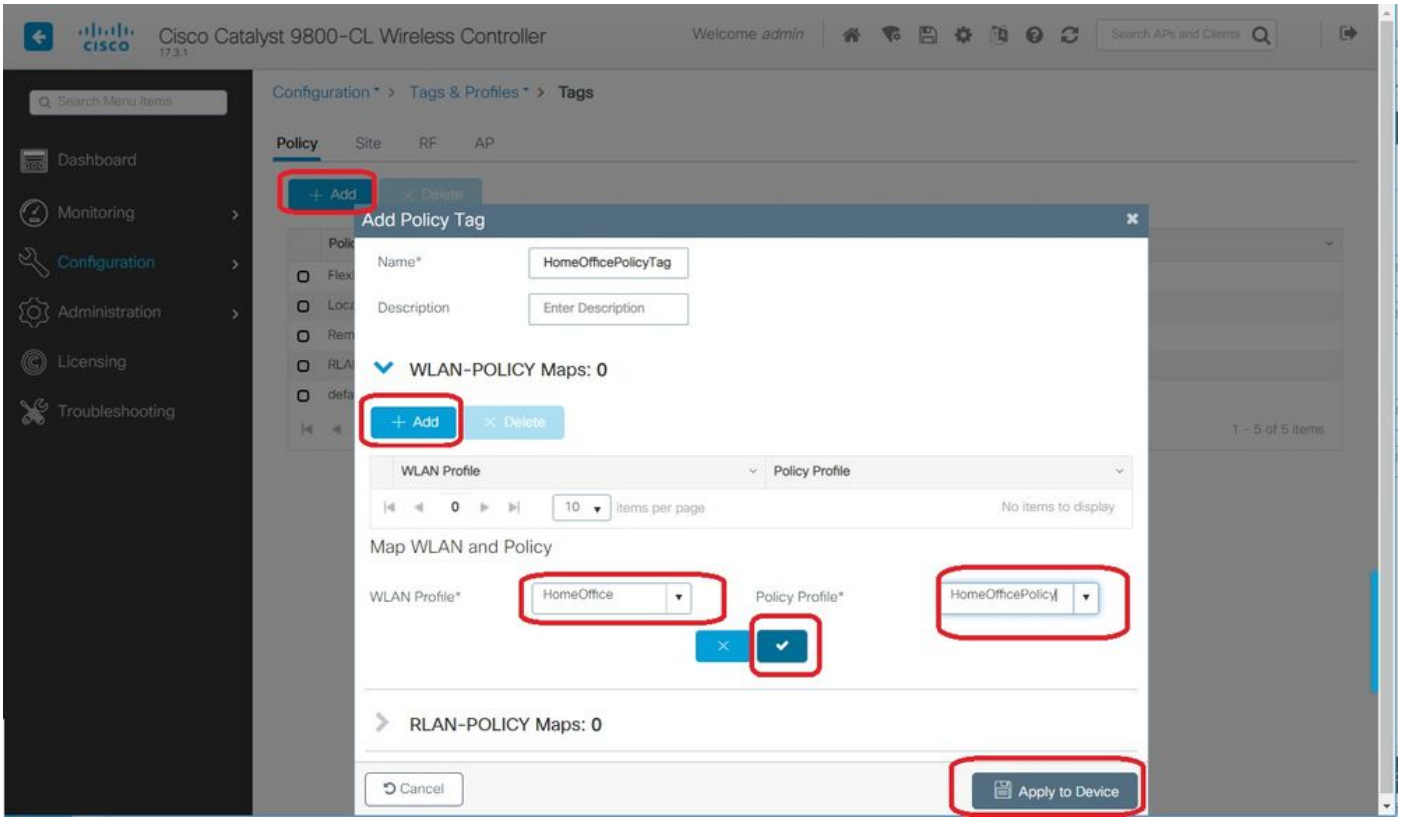
Note: Les clients Apple iOS ont besoin de l'option 6 (DNS) à définir dans l'offre DHCP pour que la tunnellisation partagée fonctionne.

Mappage d'un WLAN à un profil de stratégie

Étape 1. Choisissez Configuration > Tags & Profiles > Tags. Dans l'onglet Stratégie, sélectionnez Ajouter.

Étape 2. Saisissez le nom de la stratégie de balise et sous l'onglet WLAN-POLICY Maps, sélectionnez Ajouter.

Étape 3. Choisissez le profil WLAN dans la liste déroulante WLAN Profile et choisissez le profil Policy dans la liste déroulante Policy Profile. Sélectionnez l'icône de sélection, puis Appliquer au périphérique.

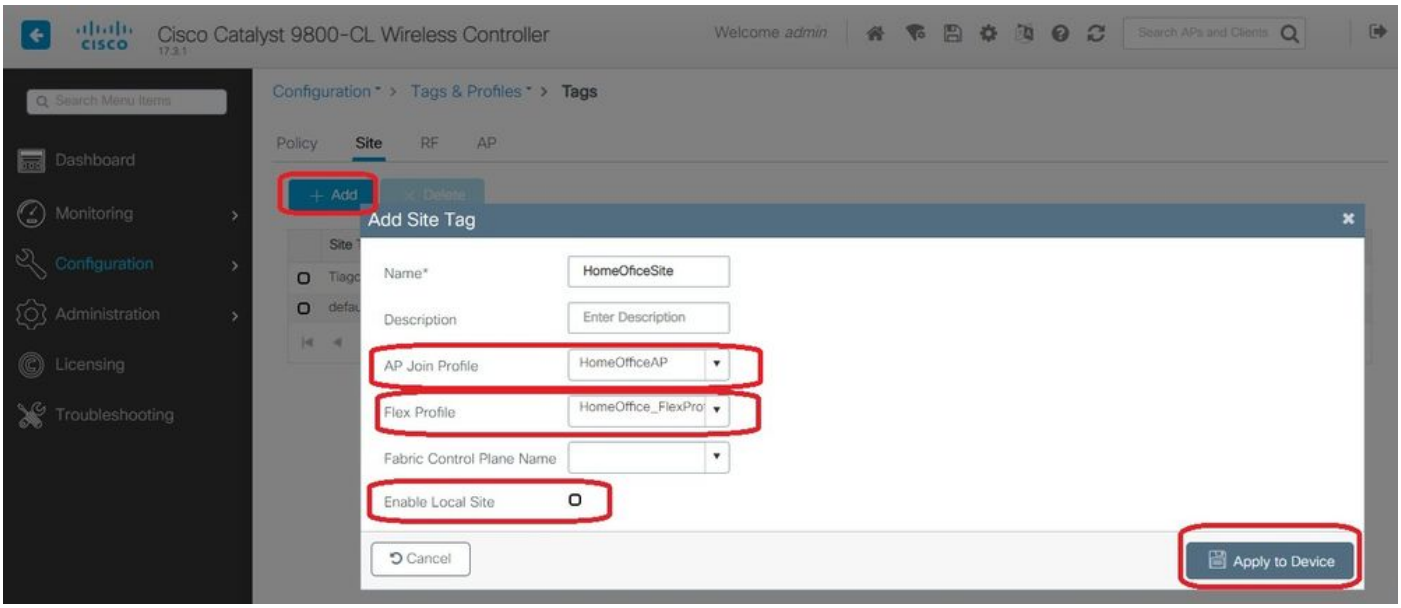


Configuration d'un profil de jointure AP et association avec la balise de site

Étape 1. Naviguez jusqu'à Configuration > Tags & Profiles > AP Join et sélectionnez Add. Saisissez un nom. Vous pouvez éventuellement activer SSH pour autoriser le dépannage et, ultérieurement, le désactiver si nécessaire.

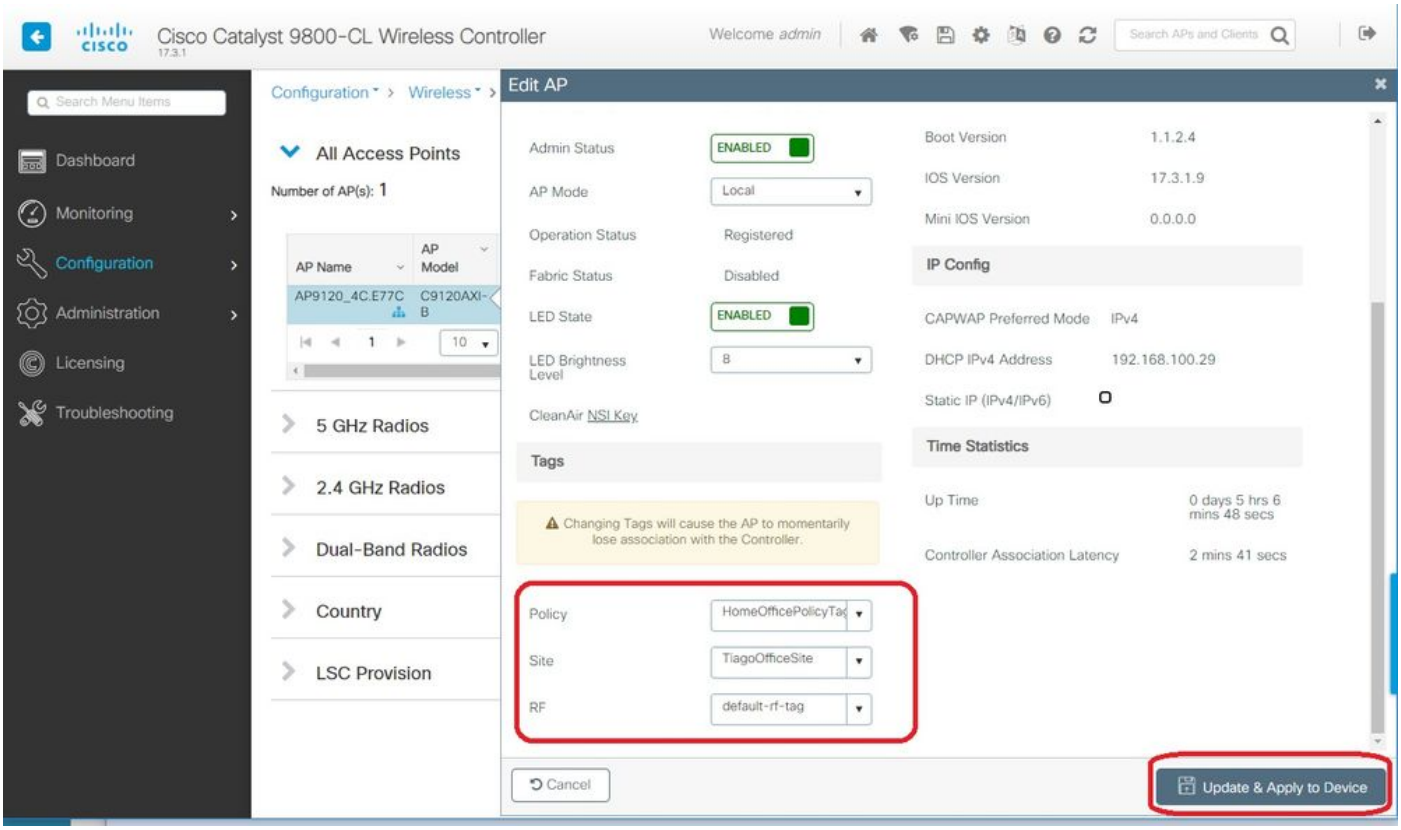
Étape 2. Choisissez Configuration > Tags & Profiles > Tags. Dans l'onglet Site, sélectionnez Ajouter.

Étape 3. Entrez le nom de la balise de site, décochez Activer le site local, puis sélectionnez le profil de jointure AP et le profil flexible (créés avant) dans les listes déroulantes. Appliquez ensuite au périphérique.

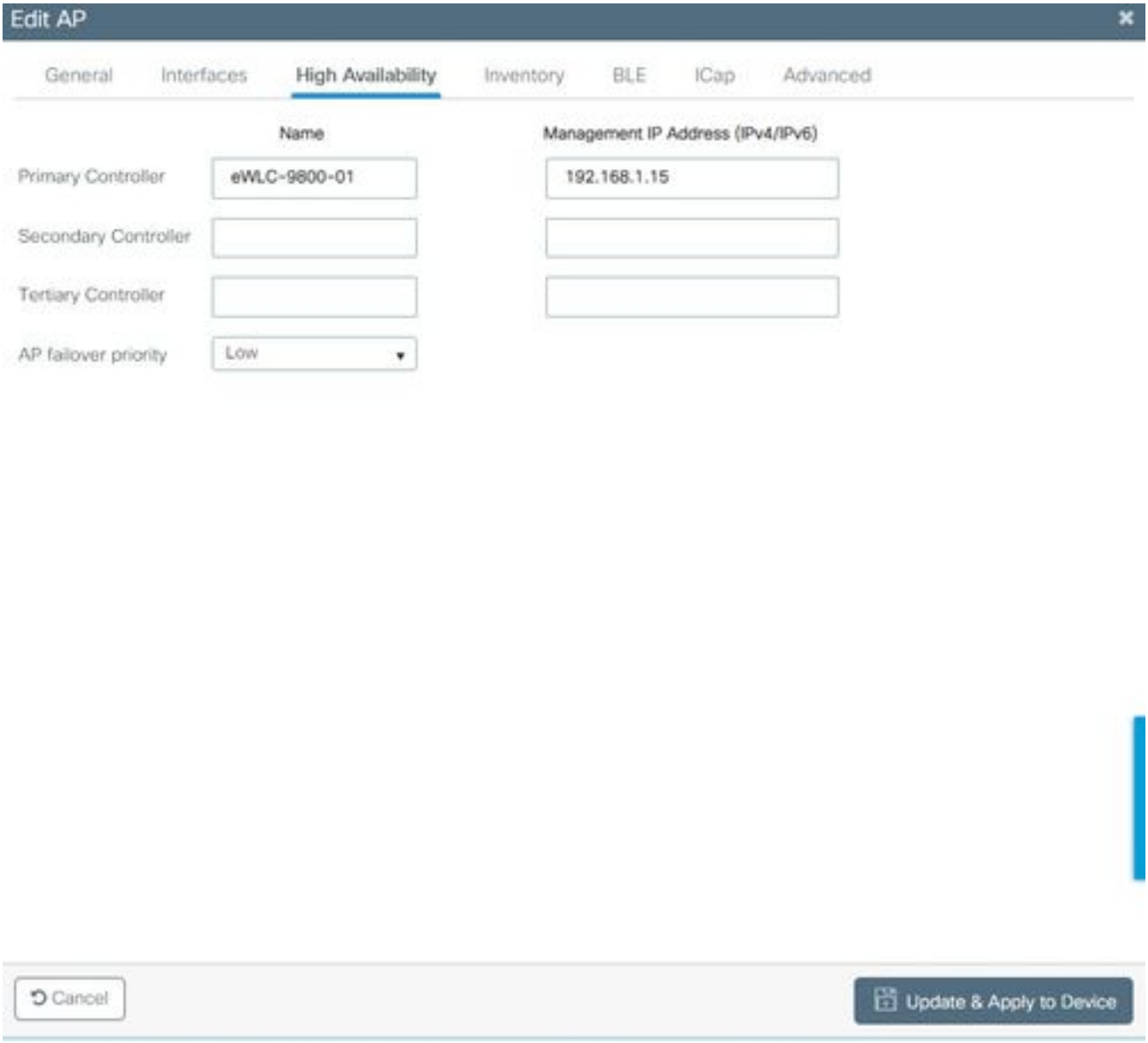


Fixation d'une balise de stratégie et d'une balise de site à un point d'accès

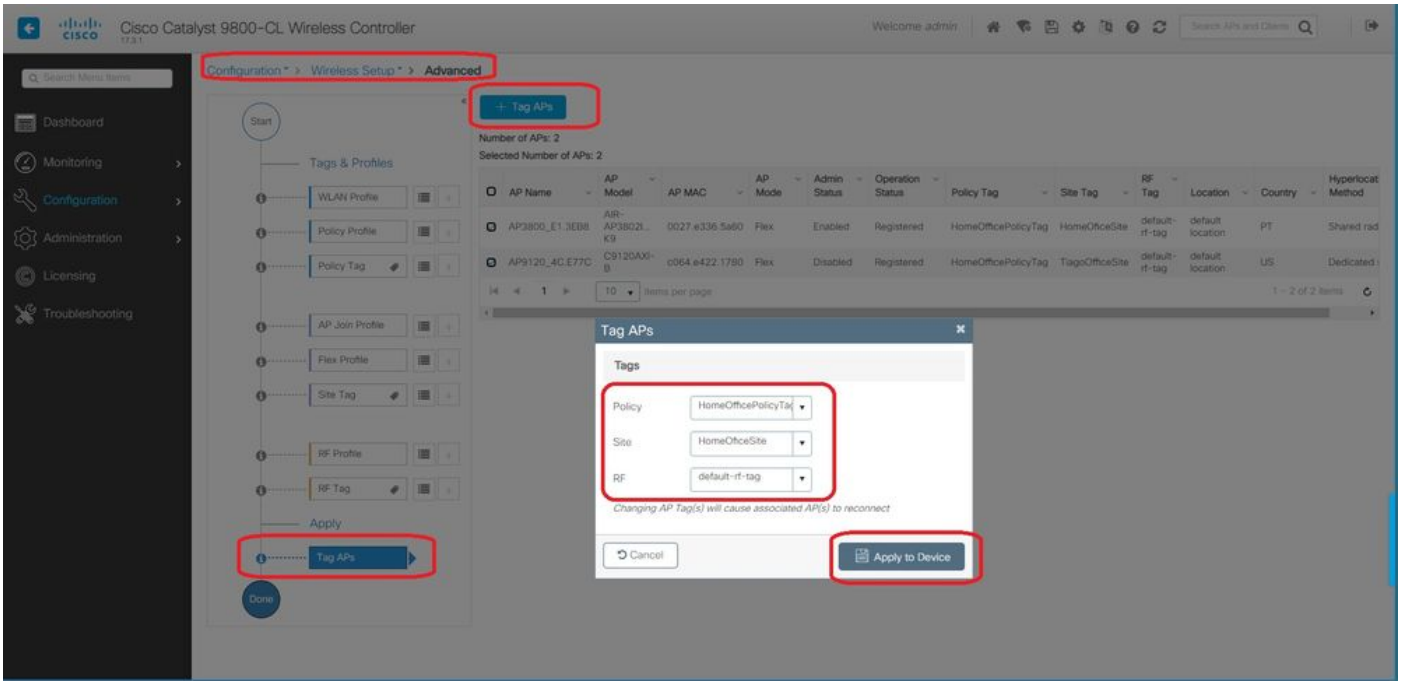
Option 1. Cette option nécessite que vous configuriez 1 point d'accès à la fois. Accédez à Configuration > Wireless > Access Points. Sélectionnez le point d'accès à déplacer vers le bureau à domicile, puis sélectionnez les balises du bureau à domicile. Sélectionnez Mettre à jour et appliquer au périphérique :



Il est également recommandé de configurer un contrôleur principal de sorte que le point d'accès connaisse l'adresse IP/nom du WLC à atteindre une fois qu'il est déployé dans le bureau à domicile. Vous pouvez modifier le point d'accès directement en accédant à l'onglet Haute disponibilité :



Option 2. Cette option vous permet de configurer plusieurs points d'accès simultanément. Accédez à Configuration > Wireless Setup > Advanced > Tag APs. Sélectionnez les balises créées précédemment et sélectionnez Appliquer au périphérique.



Les AP redémarrent et rerejoignent le WLC avec les nouveaux paramètres.

Vérification

Vous pouvez vérifier la configuration via l'interface utilisateur graphique ou l'interface de ligne de commande. Voici la configuration résultante dans l'interface de ligne de commande :

```
!
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
!
```

Vérification de la configuration du point d'accès :

```
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
...
```

Vous pouvez vous connecter directement au point d'accès et vérifier également la configuration :

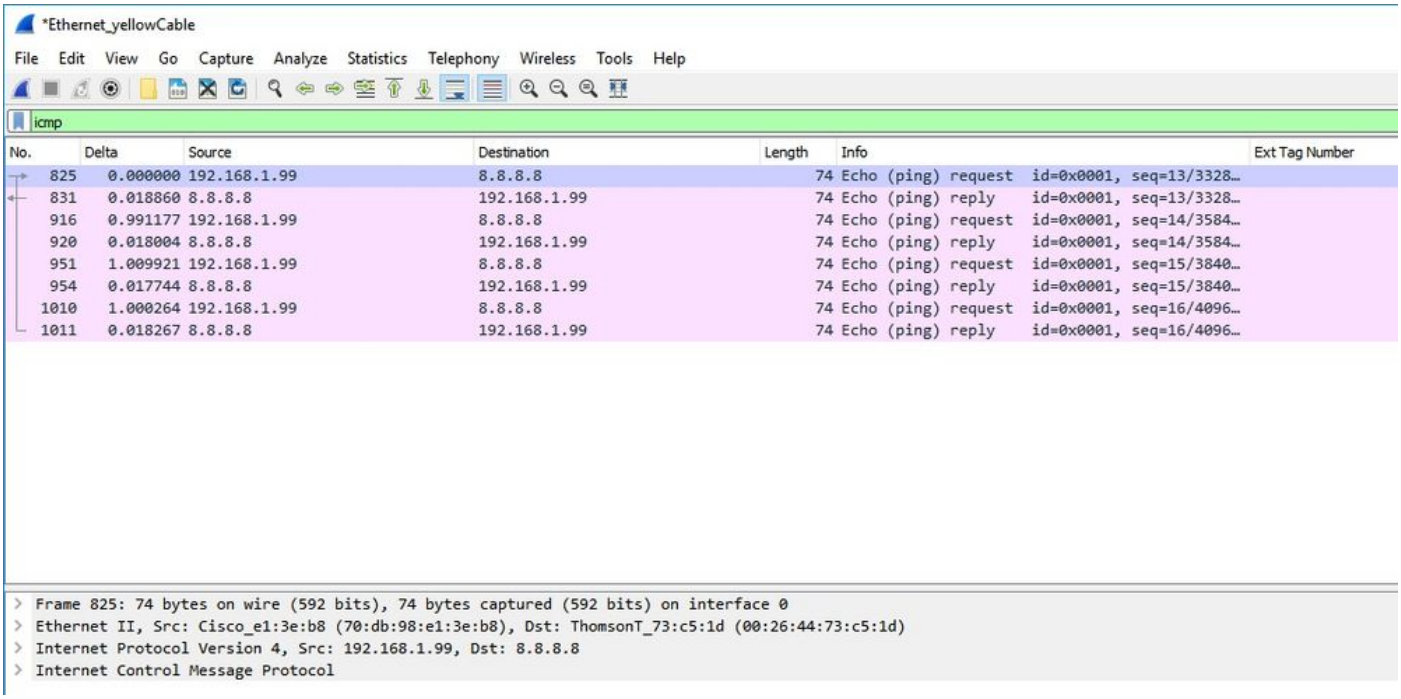
```
AP3800_E1.3EB8#show ip access-lists
Extended IP access list HomeOffice_ACL
1 deny ip any 192.168.1.0 0.0.0.255
2 permit ip any any

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
...
```

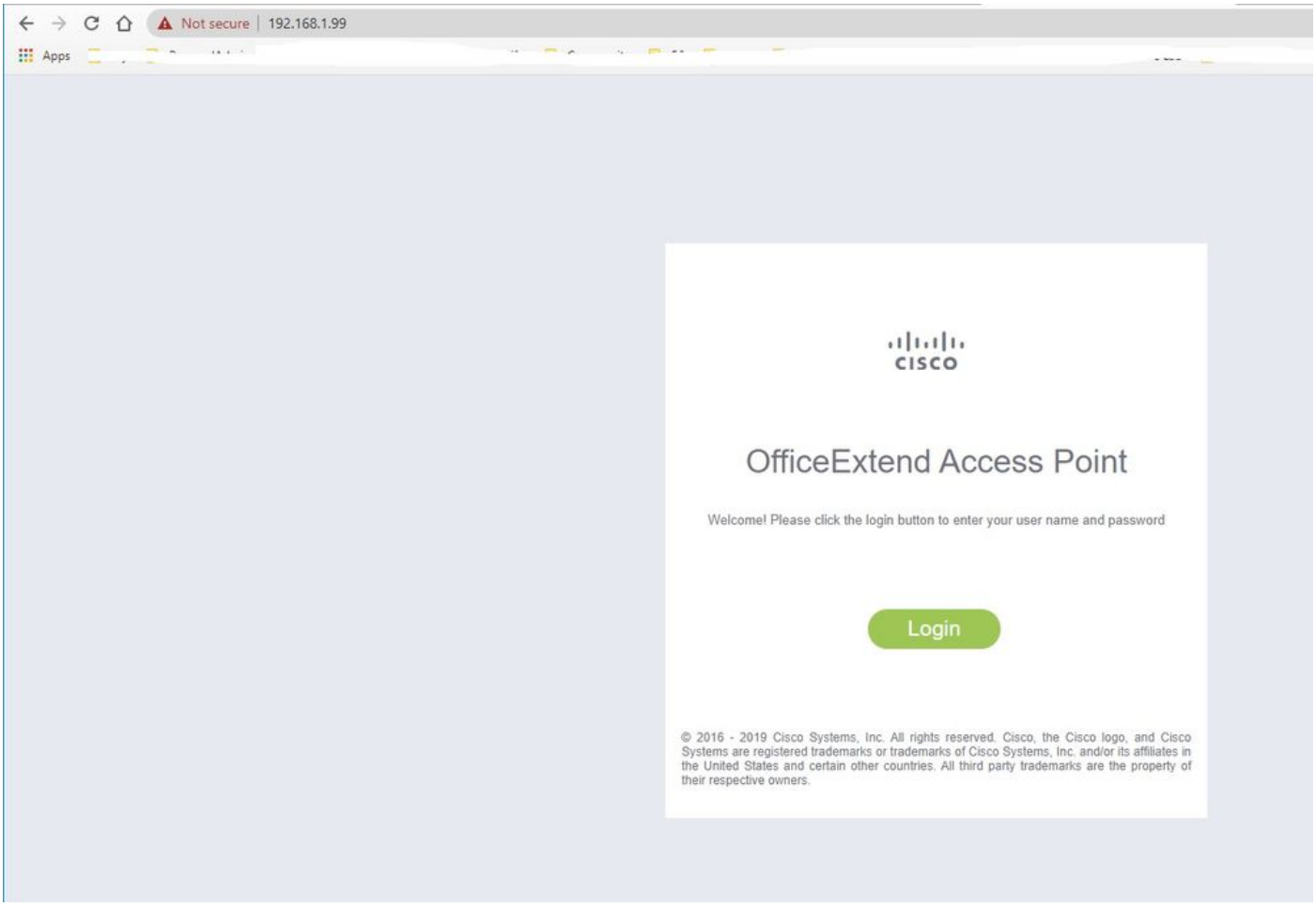
```
AP3800_E1.3EB8#show capwap client config
AdminState : ADMIN_ENABLED(1)
Name : AP3800_E1.3EB8
Location : default location
Primary controller name : eWLC-9800-01
Primary controller IP : 192.168.1.15
Secondary controller name : c3504-01
Secondary controller IP : 192.168.1.14
Tertiary controller name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

Voici un exemple de capture de paquets montrant le trafic commuté localement. Ici, le test effectué était un ping d'un client avec IP 192.168.1.98 vers le serveur DNS de Google, puis vers 192.168.1.254. Vous pouvez voir l'ICMP provenant de l'adresse IP de l'AP 192.168.1.99 envoyée au DNS Google en raison de la NAT de l'AP qui effectue le trafic localement. Il n'y a pas de icmp vers 192.168.1.254, car le trafic est chiffré dans le tunnel DTLS et seules les trames de données d'application sont vues.

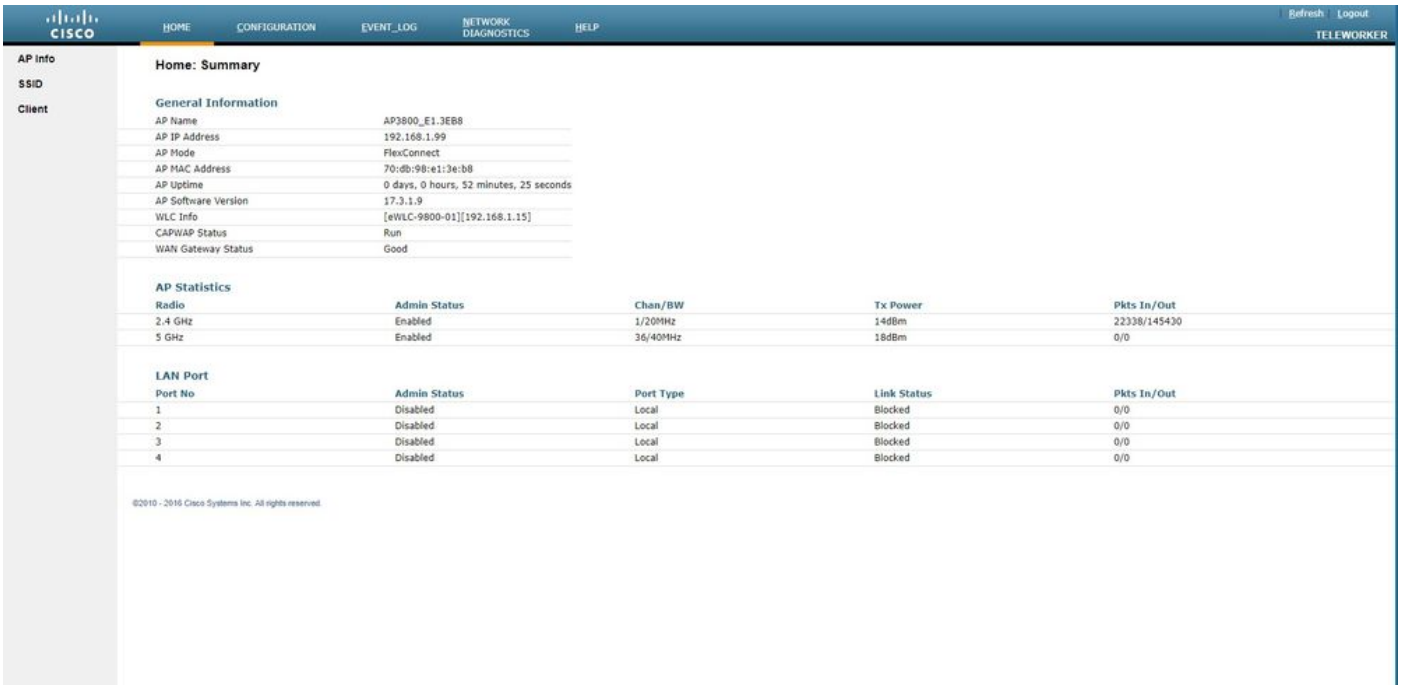


> **Note**: Le trafic qui est commuté localement est NATed par le point d'accès, car dans des scénarios normaux, le sous-réseau du client appartient au réseau Office et les périphériques locaux du bureau à domicile ne savent pas comment atteindre le sous-réseau du client. Le point d'accès traduit le trafic client à l'aide de l'adresse IP du point d'accès qui se trouve dans le sous-réseau du bureau à domicile local.

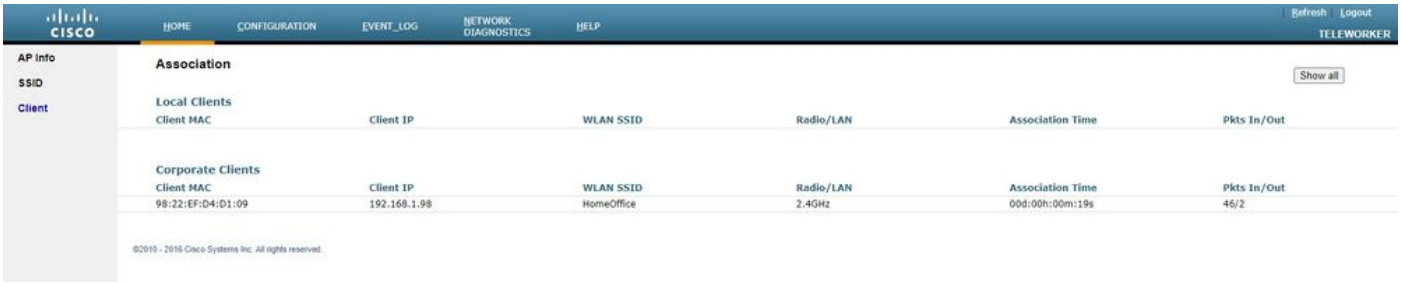
Vous pouvez accéder à l'interface utilisateur graphique OEAP en ouvrant un navigateur et en tapant l'URL de l'adresse IP AP. Les informations d'identification par défaut sont admin/admin et vous devez les modifier lors de la connexion initiale.



Une fois connecté, vous avez accès à l'interface utilisateur graphique :



Vous avez accès aux informations standard d'un OEAP, telles que les informations de point d'accès, les SSID et les clients connectés :



Documentation associée

[Comprendre FlexConnect sur le contrôleur sans fil Catalyst 9800]

[Fractionnement de la transmission tunnel pour FlexConnect]

[Configurer OEAP et RLAN sur le WLC Catalyst 9800]