Catalyst 9800 en FlexConnect GOEDKOPE splitter-tunneling configureren

Inhoud

Inleiding

In dit document wordt beschreven hoe u een access point (AP) voor buitengebruik kunt configureren als een FlexConnect Office Extend (OEAP) en hoe u gesplitste tunneling mogelijk kunt maken zodat u kunt definiëren wat er lokaal op het thuiskantoor kan worden geschakeld en welk verkeer centraal moet worden geschakeld op WLC.

Voorwaarden

Vereisten

De configuratie op dit document gaat ervan uit dat de WLC al is ingesteld in een DMZ met NAT ingeschakeld en dat AP vanuit het thuiskantoor aan de WLC kan deelnemen.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Draadloze LAN-controllers 9800 die Cisco IOS-XE 17.3.1 software uitvoeren.
- Wave1 AP's: 1700/2700/3700.
- Wave2 access points: 1800/2800/3800/4800 en Catalyst 9100 Series.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Overzicht

Een Cisco OfficeExtend access point (Cisco OEAP) biedt beveiligde communicatie van een Cisco WLC naar een Cisco AP op een afgelegen locatie, waardoor de bedrijfs WLAN via het internet naadloos wordt uitgebreid naar de verblijfplaats van een werknemer. De ervaring van de gebruiker op het thuiskantoor is precies dezelfde als bij het hoofdkantoor. Datagram Transport Layer Security (DTLS)-encryptie tussen het access point en de controller zorgt ervoor dat alle communicatie het hoogste beveiligingsniveau heeft. Elke AP binnen in FlexConnect modus kan als een OEAP fungeren.

Achtergrondinformatie

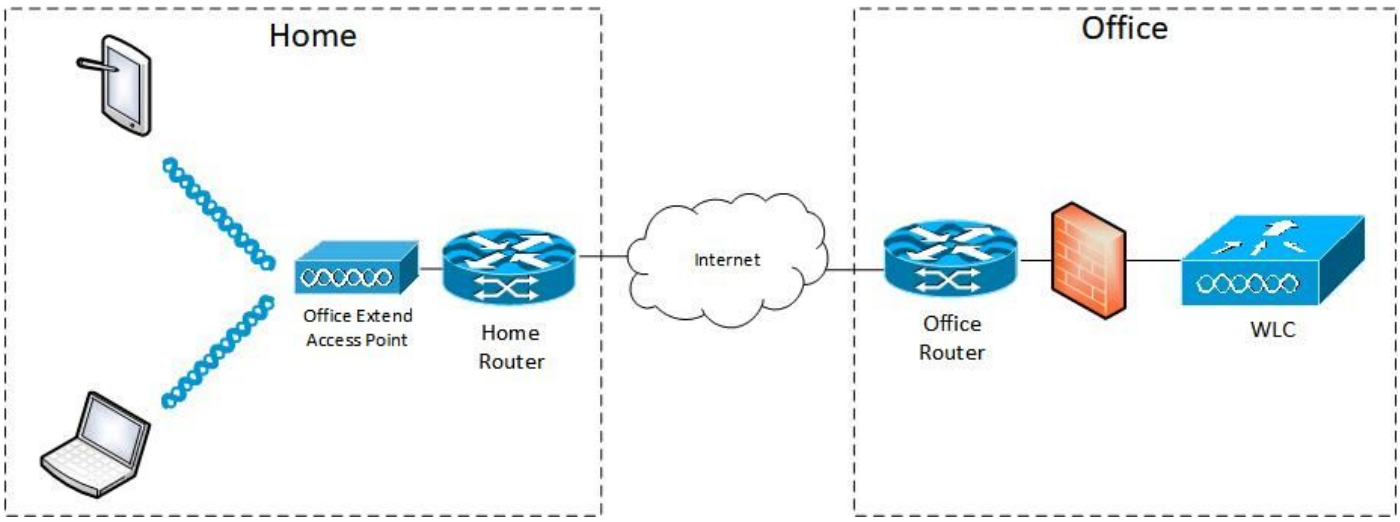
FlexConnect verwijst naar de mogelijkheid van een access point (AP) om draadloze clients af te handelen terwijl u op externe locaties werkt, bijvoorbeeld via een WAN. Ze kunnen ook beslissen of het verkeer van de draadloze klanten rechtstreeks op het netwerk op het AP-niveau (Local Switching) wordt gezet of of of het verkeer gecentraliseerd is naar de 9800 controller (Central Switching) en via het WAN wordt teruggestuurd, op een WLAN-basis.

Controleer dit document op FlexConnect op Catalyst 9800 draadloze controller voor meer informatie over FlexConnect.

De OEAP-modus is een optie die beschikbaar is in een FlexConnect AP, om extra functionaliteit toe te staan, bijvoorbeeld een persoonlijke lokale SSID voor de toegang tot het thuisnetwerk, en kan ook splitsingen tunneling bieden, voor een groter detail om te bepalen wat verkeer lokaal op het thuiskantoor moet worden geschakeld en wat verkeer centraal bij WLC, via één WLAN moet worden geschakeld

Configureren

Netwerkdiagram



Configuraties

Een toegangscontrolelijst voor splitter-tunneling definiëren

Stap 1. Kies Configuration > Security > ACL. Selecteer Toevoegen.

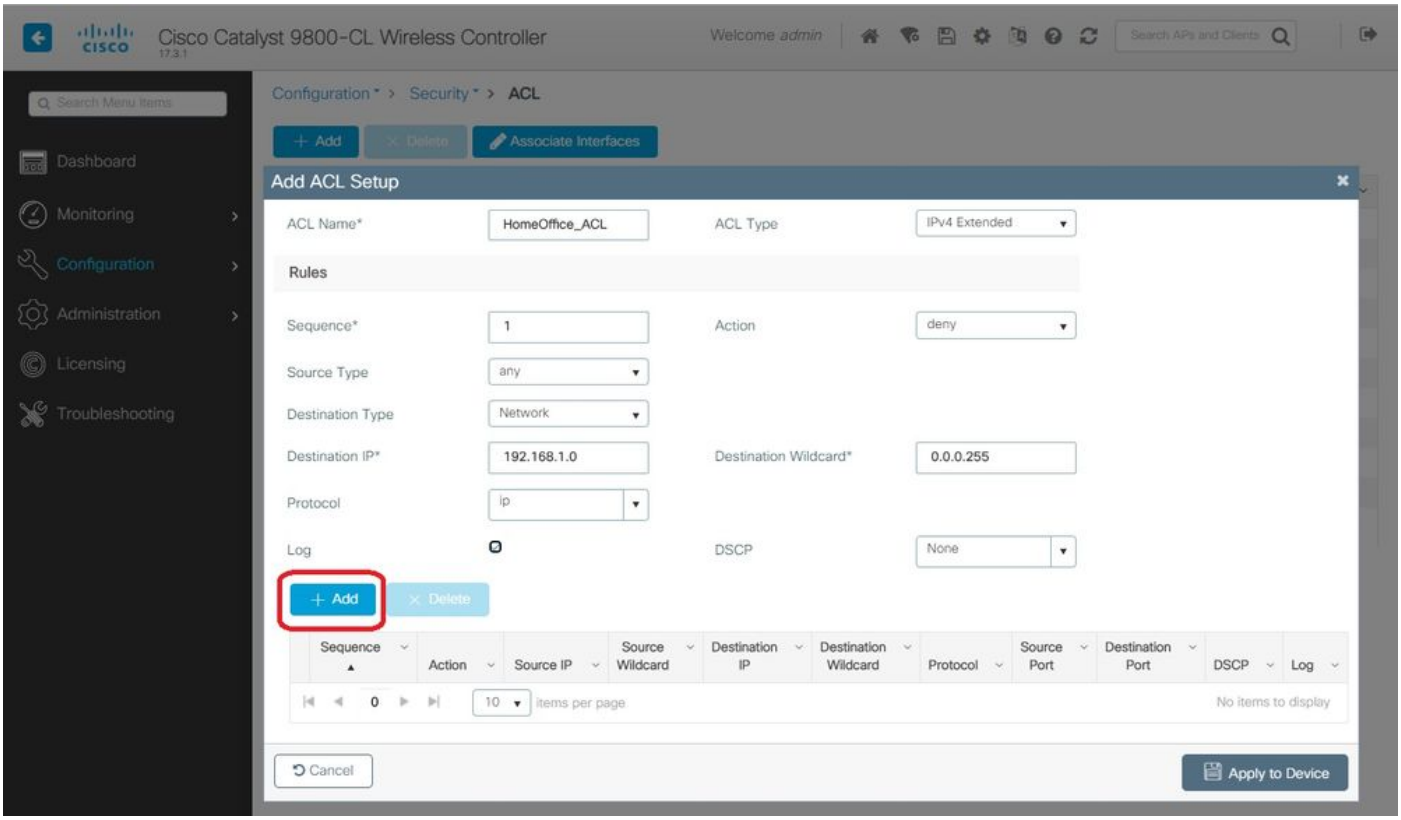
Stap 2. In het dialoogvenster ACL-instelling toevoegen voert u de ACL-naam in (ACL-naam). Kies het ACL-type in de vervolgkeuzelijst Type en voer onder de Regelinstellingen het sequentienummer in. Kies vervolgens de Actie als toegestaan of ontkennen.

Stap 3. Kies het gewenste brontype in de vervolgkeuzelijst Brontype.

Als u het brontype als host kiest, moet u de hostnaam/IP invoeren.

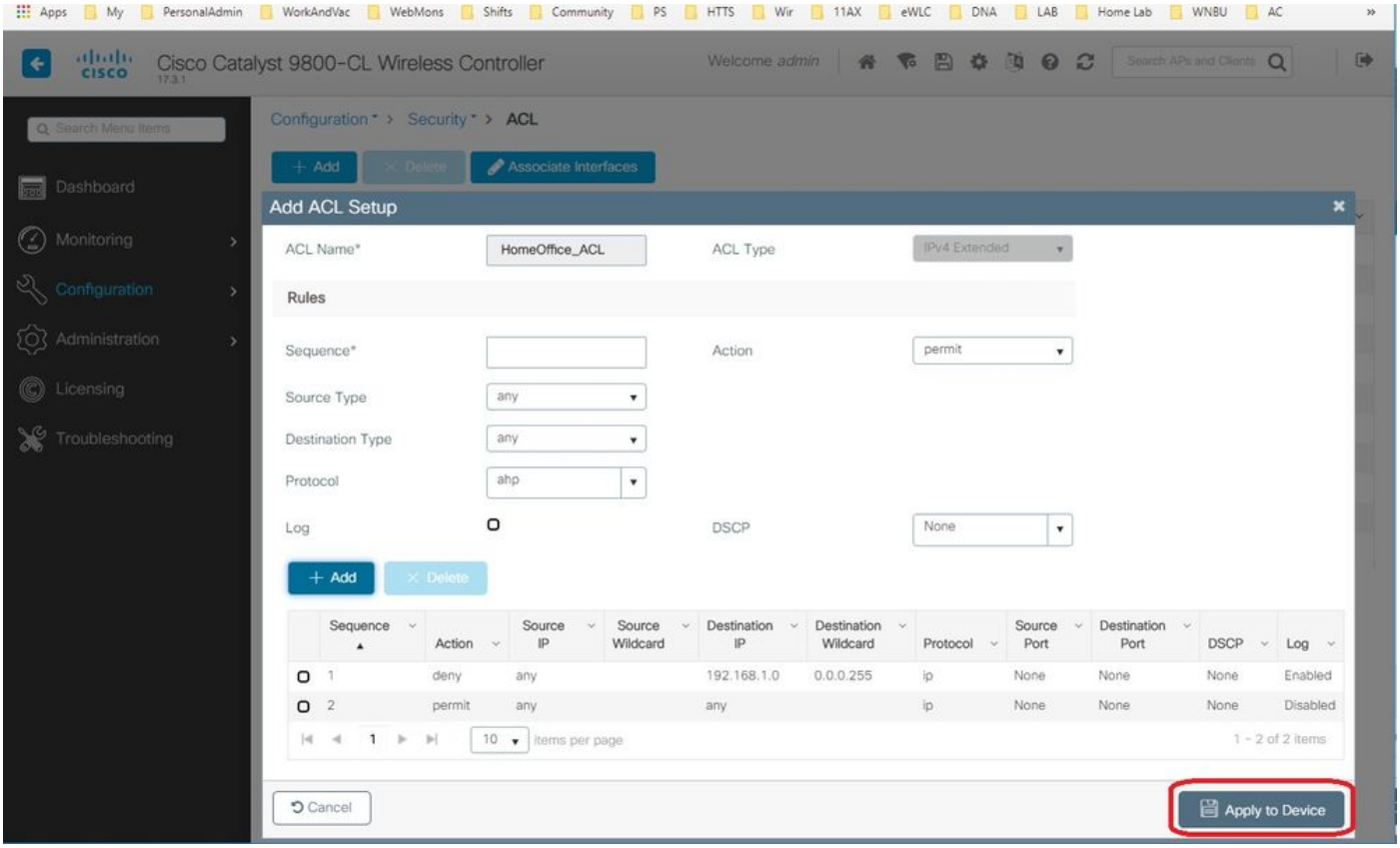
Als u het brontype als Netwerk kiest, moet u het Bron IP adres en het Bron Wildcard masker specificeren.

In dit voorbeeld, wordt al verkeer van om het even welke gastheer aan Subnet 192.168.1.0/24 centraal geschakeld (ontkennen) en al de rest van het verkeer lokaal geschakeld (vergunning).



Stap 4. Controleer het aanvinkvakje in Log als u de logs wilt toevoegen en selecteer Toevoegen.

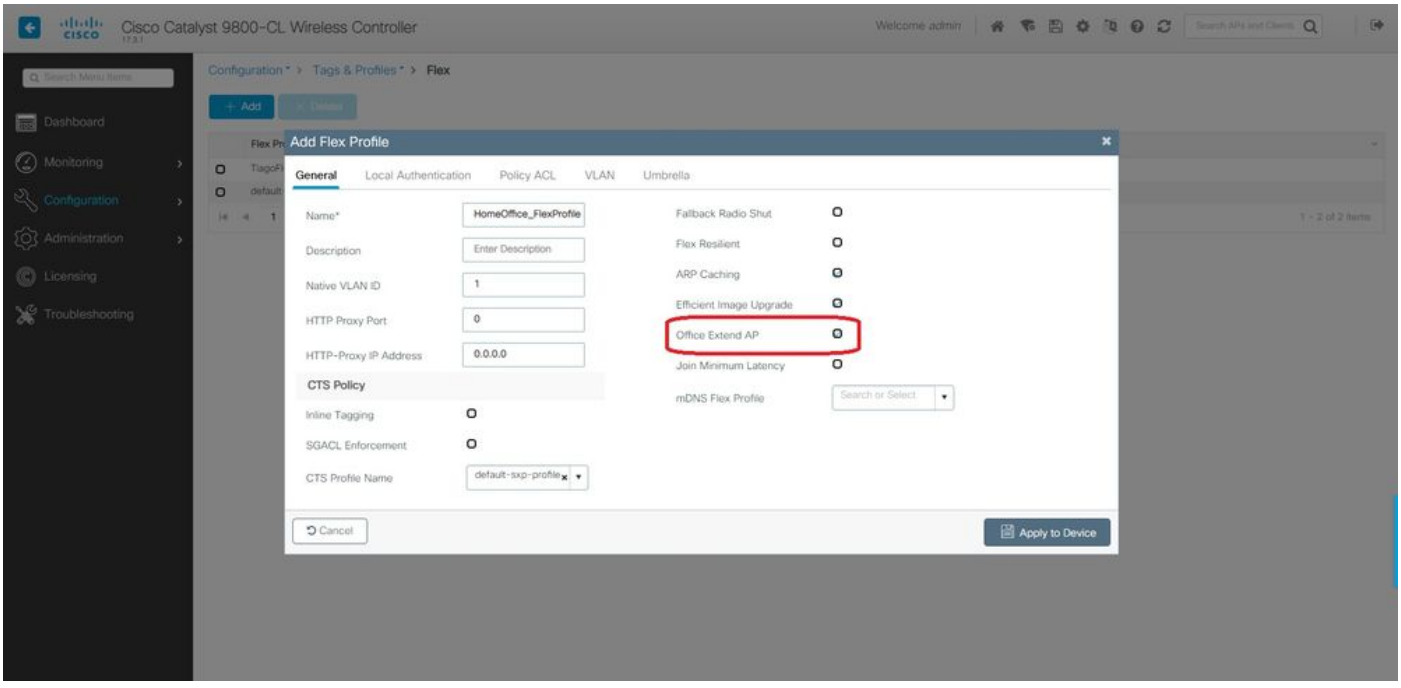
Stap 5. Voeg de rest van de regels toe en selecteer Toepassen op apparaat.



Een ACL-beleid verbinden met de gedefinieerde ACL

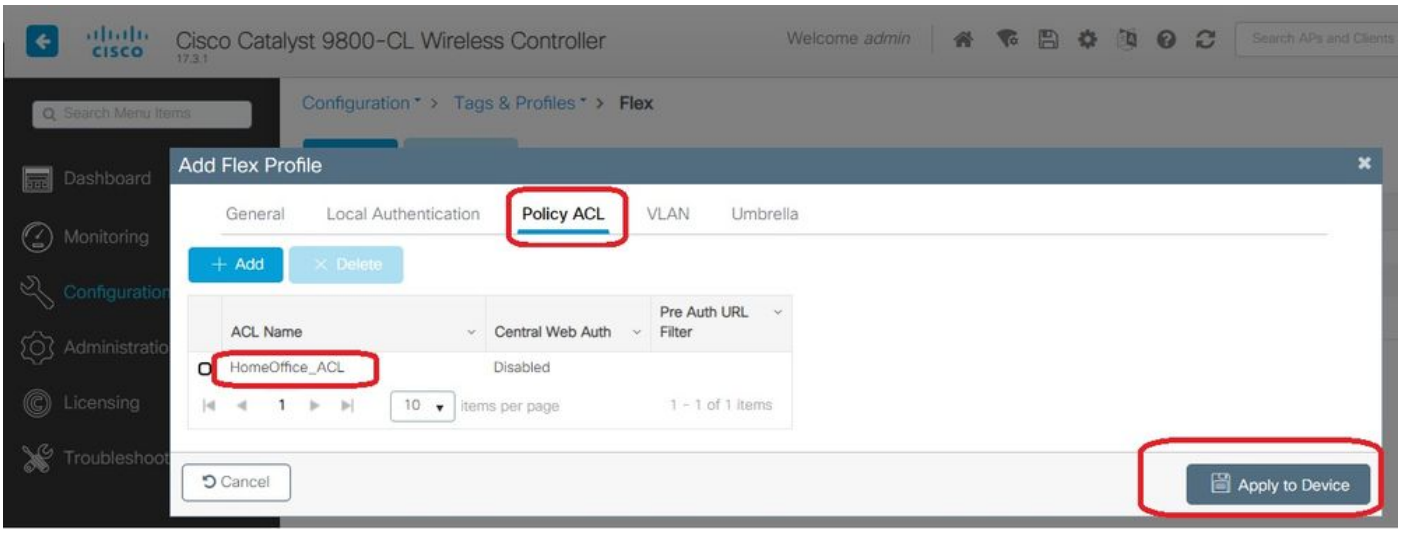
Stap 1. Maak een nieuw Flex Profile. Ga naar configuratie > Tags en profielen > Flex. Selecteer Toevoegen.

Stap 2. Voer een naam in en schakelt u OEAP in. Zorg er ook voor dat de native VLAN-id degene is in de AP-switchpoort.



Opmerking: Wanneer u Office-Extend-modus activeert, wordt de Link-Encryptie ook standaard ingeschakeld en kan deze niet worden gewijzigd, zelfs niet als u Link Encryption in het AP-profiel uitschakelt.

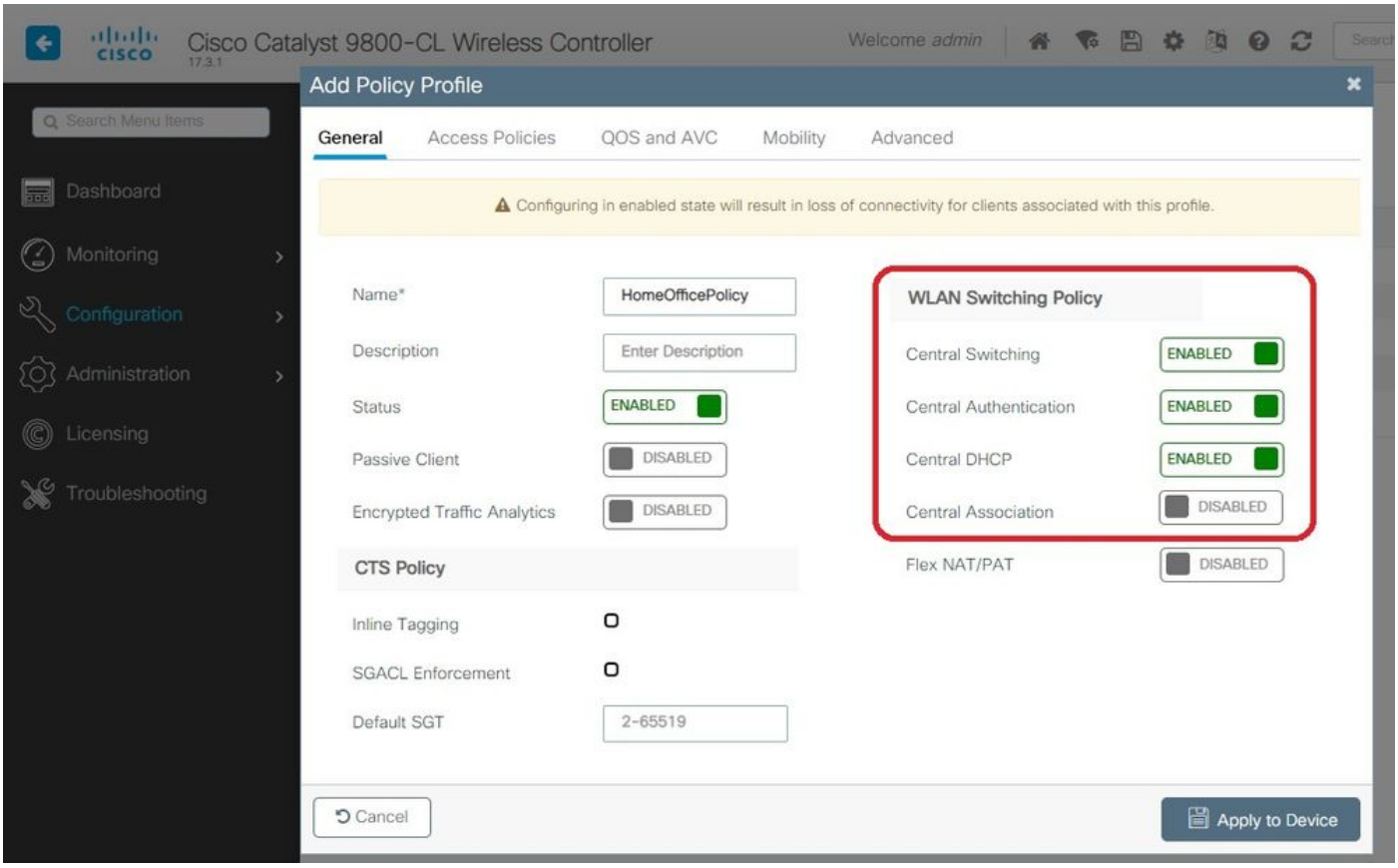
Stap 3. Verplaats naar het tabblad Policy ACL en selecteer Toevoegen. Voeg hier ACL aan het profiel toe en pas op apparaat toe.



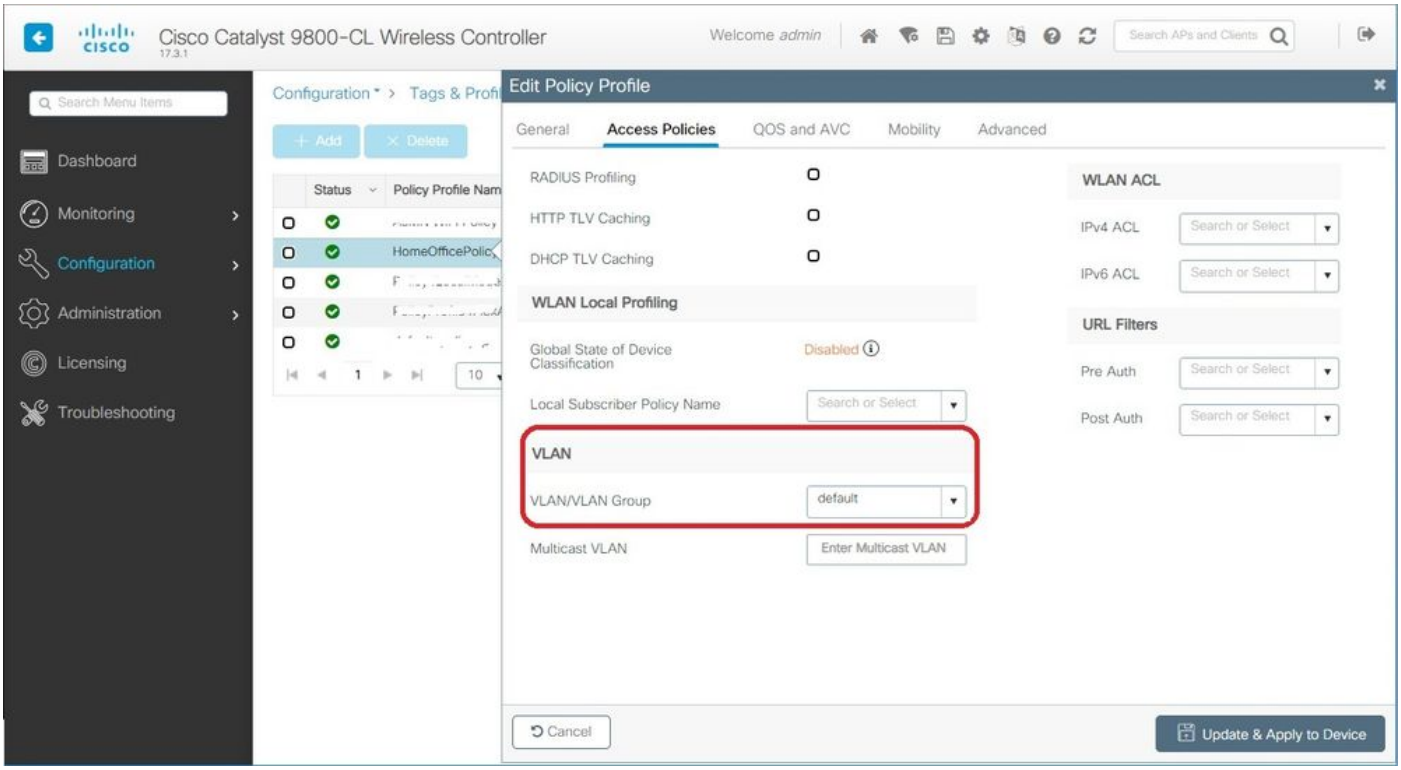
Een draadloos Profile-beleid en een Split MAC-naam configureren

Stap 1. Maak een WLAN-profiel. In dit voorbeeld, gebruikt het een SSID genoemd HomeOffice met de veiligheid van WAP2-PSK.

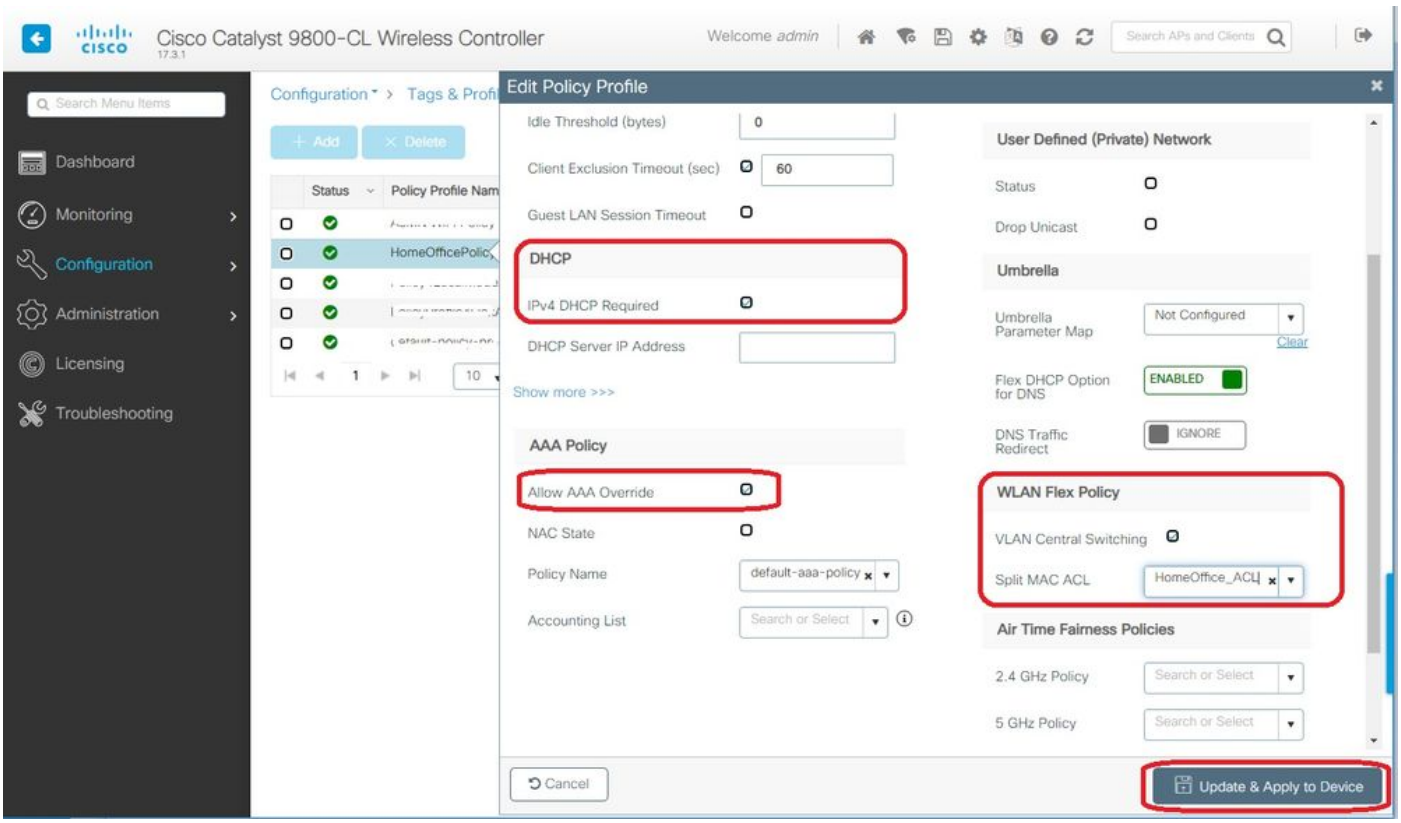
Stap 2. Maak een beleidsprofiel. Ga naar Configuration > Tags > Policy en selecteer Toevoegen. Onder General, zorg ervoor dat dit profiel een centraal geschakeld beleid is, zoals in dit voorbeeld:



Stap 3. In het beleidsprofiel gaat u naar Toegangsbeleid en definieert u het VLAN voor het centraal geschakelde verkeer. De klanten krijgen een IP adres in Subnet toegewezen aan dit VLAN.



Stap 4. Om lokale gesplitste tunneling op een AP te configureren moet u ervoor zorgen dat u DCHP Benodigd op WLAN hebt ingeschakeld. Dit waarborgt dat de client die wordt geassocieerd met de gesplitste WLAN, DHCP doet. U kunt deze optie in het tabblad Beleidsprofiel inschakelen onder het tabblad Geavanceerd. Schakel het vakje IPv4 DHCP in dat vereist is. Kies onder de WLAN Flex Policy-instellingen de gesplitste MAC die hiervoor is gemaakt, uit de vervolgkeuzelijst Split MAC ACL-ACL. Selecteer Toepassen op apparaat:



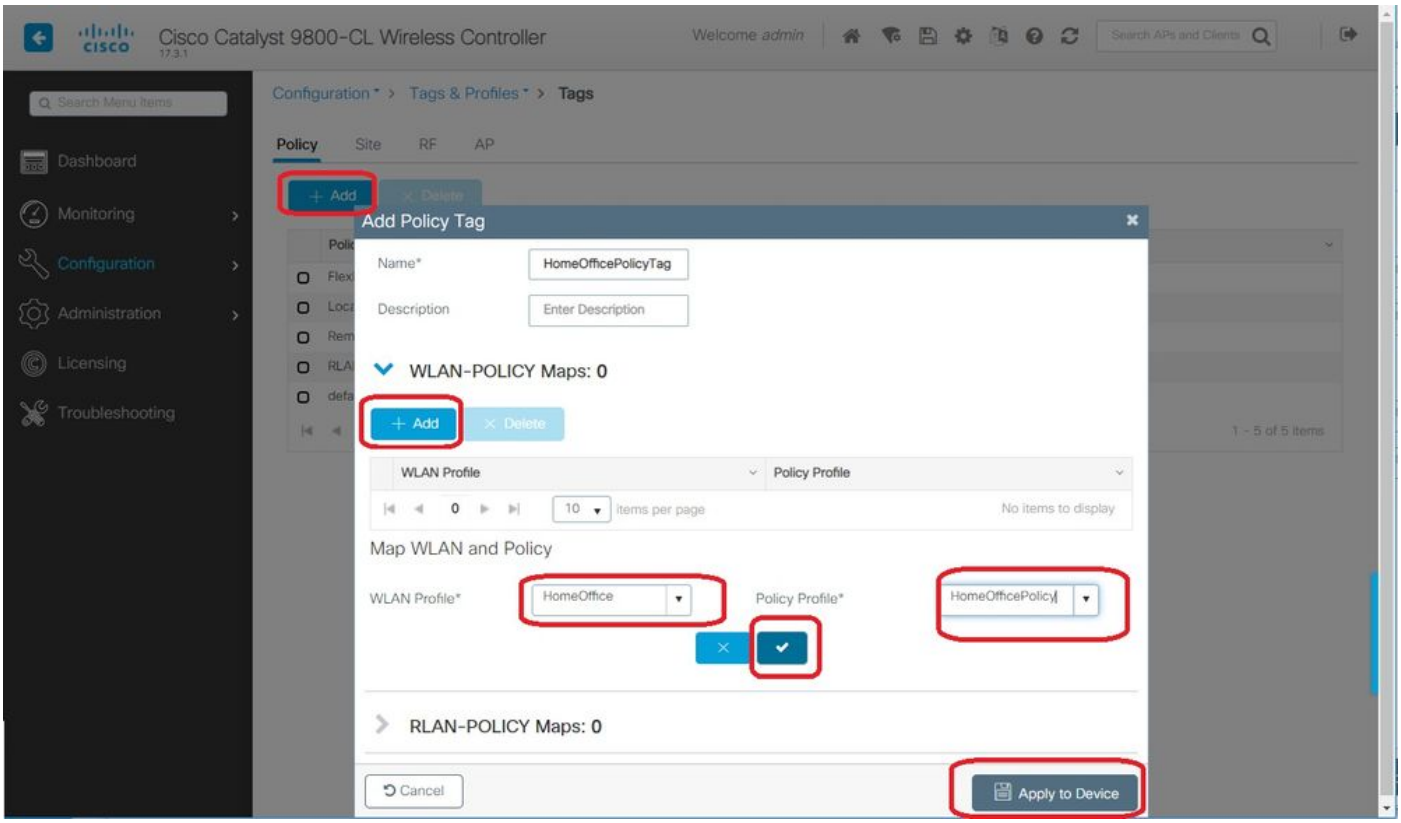
Opmerking: Clients van Apple iOS hebben optie 6 (DNS) nodig om in DHCP-aanbieding te worden ingesteld voor gesplitste tunneling om te kunnen werken.

Een WLAN aan een beleidsprofiel toewijzen

Stap 1. Kies configuratie > Tags en profielen > Tags. Selecteer in het tabblad Beleid de optie Toevoegen.

Stap 2. Voer de naam van het markeringsbeleid in en selecteer onder het tabblad WLAN-BELEIDSKaarten de optie Toevoegen.

Stap 3. Kies het WLAN-profiel in de vervolgkeuzelijst WLAN-profiel en kies het beleidsprofiel uit de vervolgkeuzelijst Policy Profile. Selecteer het pictogram Tik en pas vervolgens op apparaat toe.

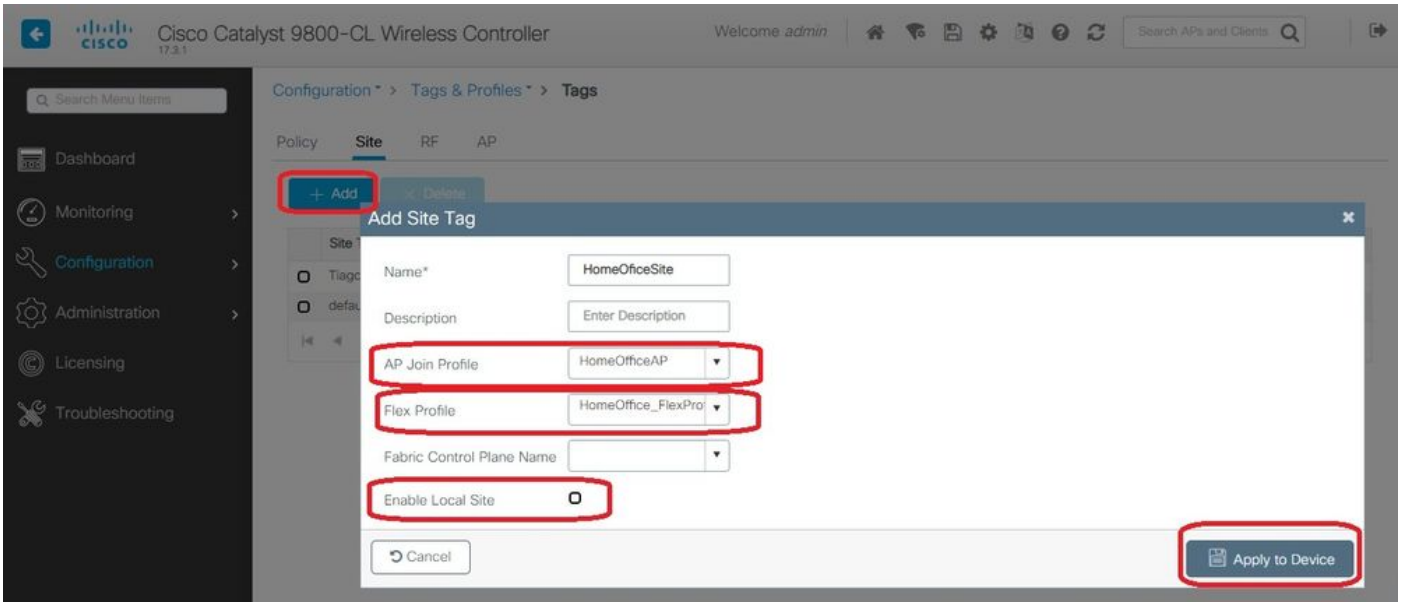


Een AP-toegangsprofiel en een associatie met site-tag configureren

Stap 1. navigeren naar Configuration > Tags en profielen > AP Join en selecteer Add. Voer een naam in. U kunt SSH naar keuze toestaan voor probleemoplossing en later deze indien niet nodig uitschakelen.

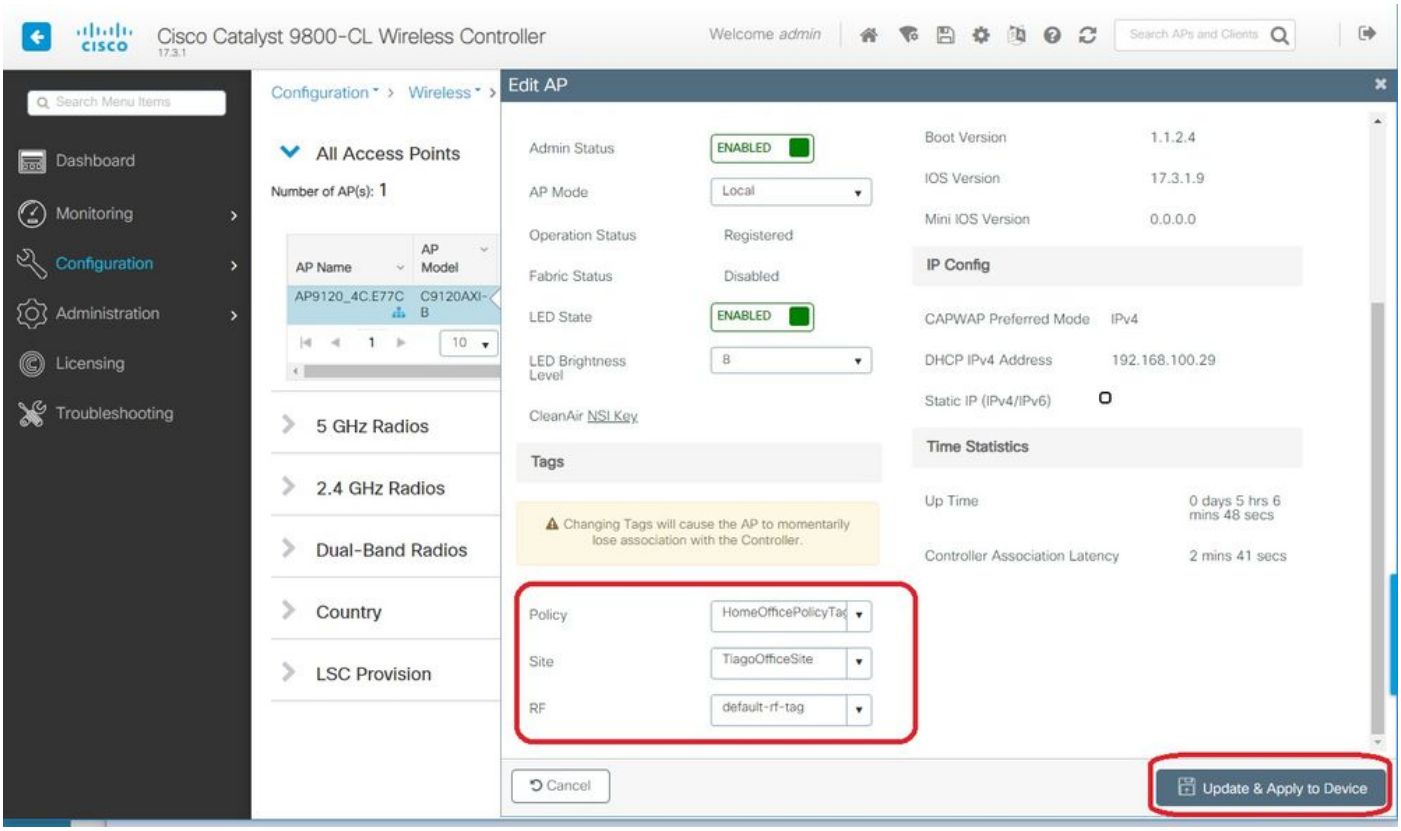
Stap 2. Kies configuratie > Tags en profielen > Tags. Selecteer in het tabblad Site de optie Toevoegen.

Stap 3. Voer de naam van de site-tag in, maak de optie Local Site inschakelen en selecteer vervolgens het AP Join Profile en Flex Profile (dat eerder gemaakt is) uit de vervolgkeuzelijsten. Toepassen op apparaat.

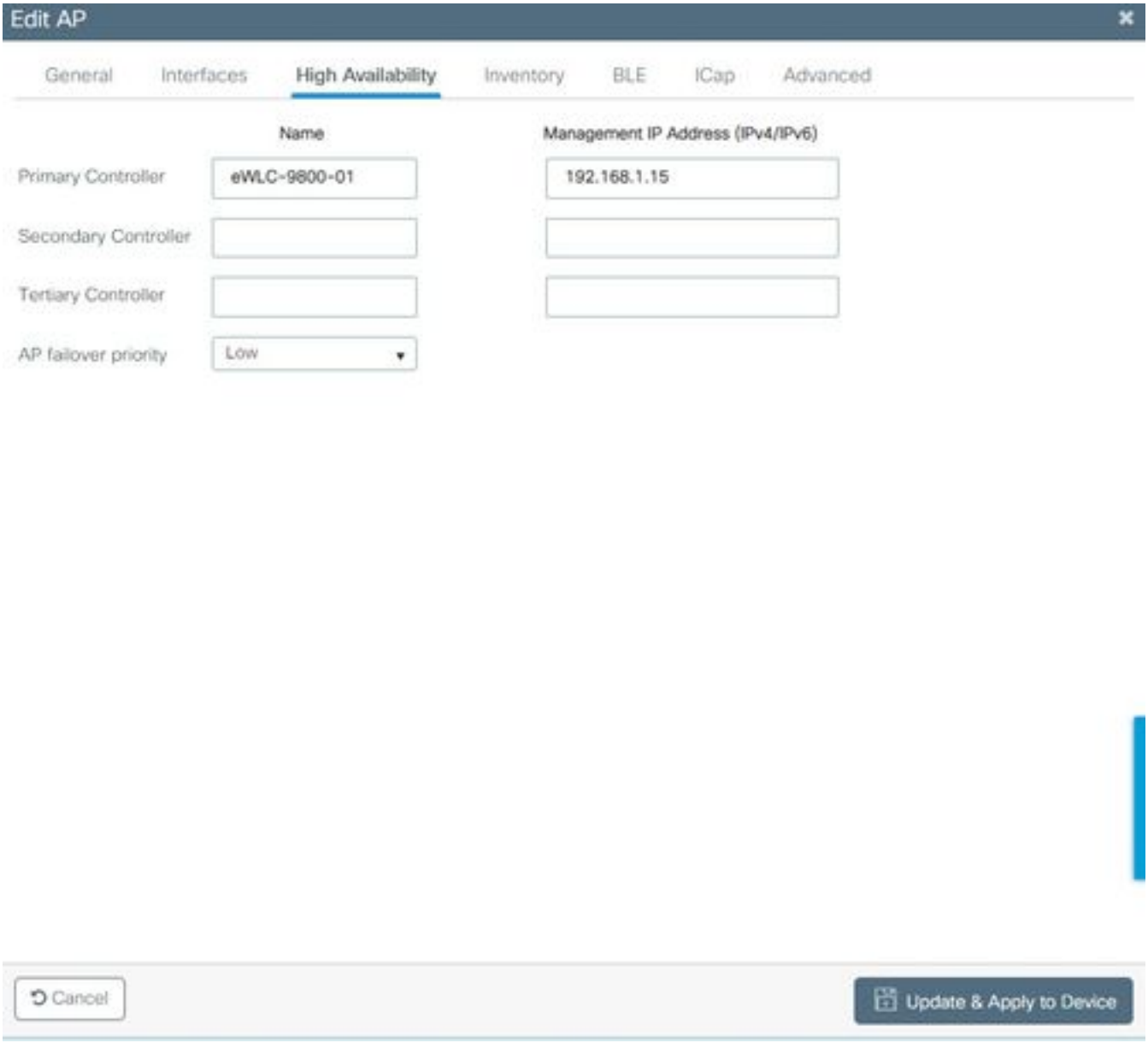


Een beleidslaag en site-tag aansluiten op een access point

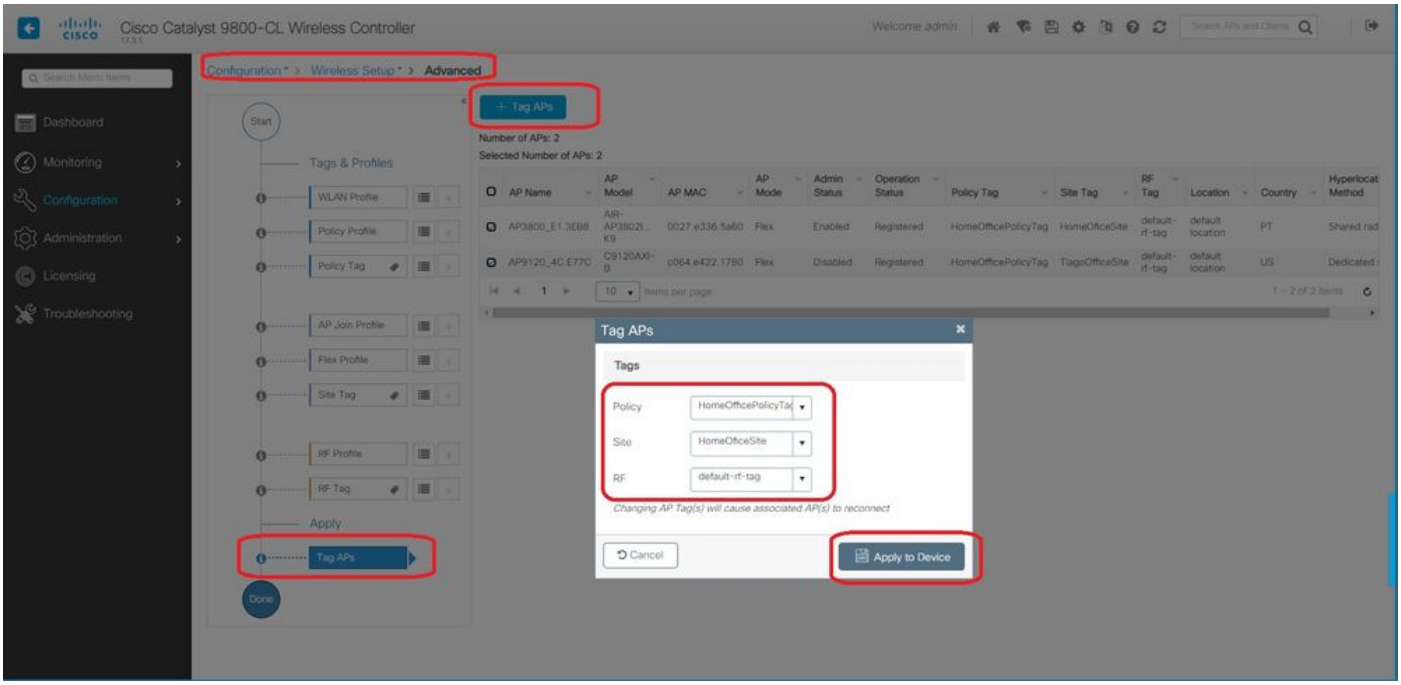
Optie 1. Voor deze optie moet u 1 AP tegelijk configureren. Ga naar configuratie > Draadloos > access points. Selecteer de AP die u naar het Bureau van het Huis wilt verplaatsen en selecteer dan de Tags van het Huis. Selecteer Update en toepassen op apparaat:



Het wordt ook aanbevolen om een Primaire controller te configureren zodat AP de IP/naam van de WLC weet om te bereiken wanneer deze in het thuiskantoor wordt ingezet. U kunt dit doen door de AP te bewerken en rechtstreeks naar het tabblad Hoge beschikbaarheid te gaan:



Optie 2. Met deze optie kunt u meerdere AP's tegelijkertijd configureren. Navigeer naar Configuratie > Draadloze Instellen > Geavanceerd > Handelingen van de tag. Selecteer de eerder gemaakte tags en selecteer Toepassen op apparaat.



De APs herstart en sluit zich opnieuw aan bij de WLC met de nieuwe instellingen.

Verifiëren

U kunt de configuratie controleren via GUI of CLI. Dit is de resulterende configuratie in 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
!
```

Configuratie AP controleren:

```
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
...
```

U kunt direct verbinding maken met AP en ook de configuratie controleren:

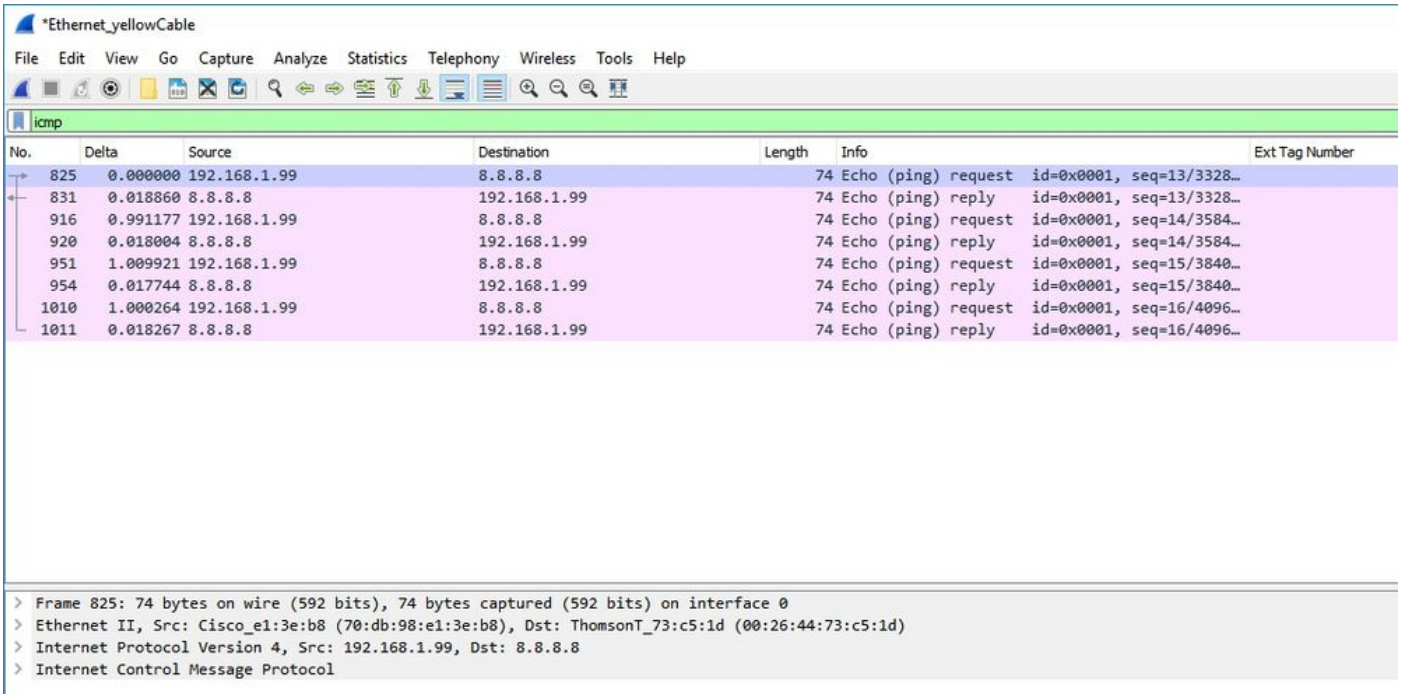
```
AP3800_E1.3EB8#show ip access-lists
Extended IP access list HomeOffice_ACL
1 deny ip any 192.168.1.0 0.0.0.255
2 permit ip any any

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
...
```

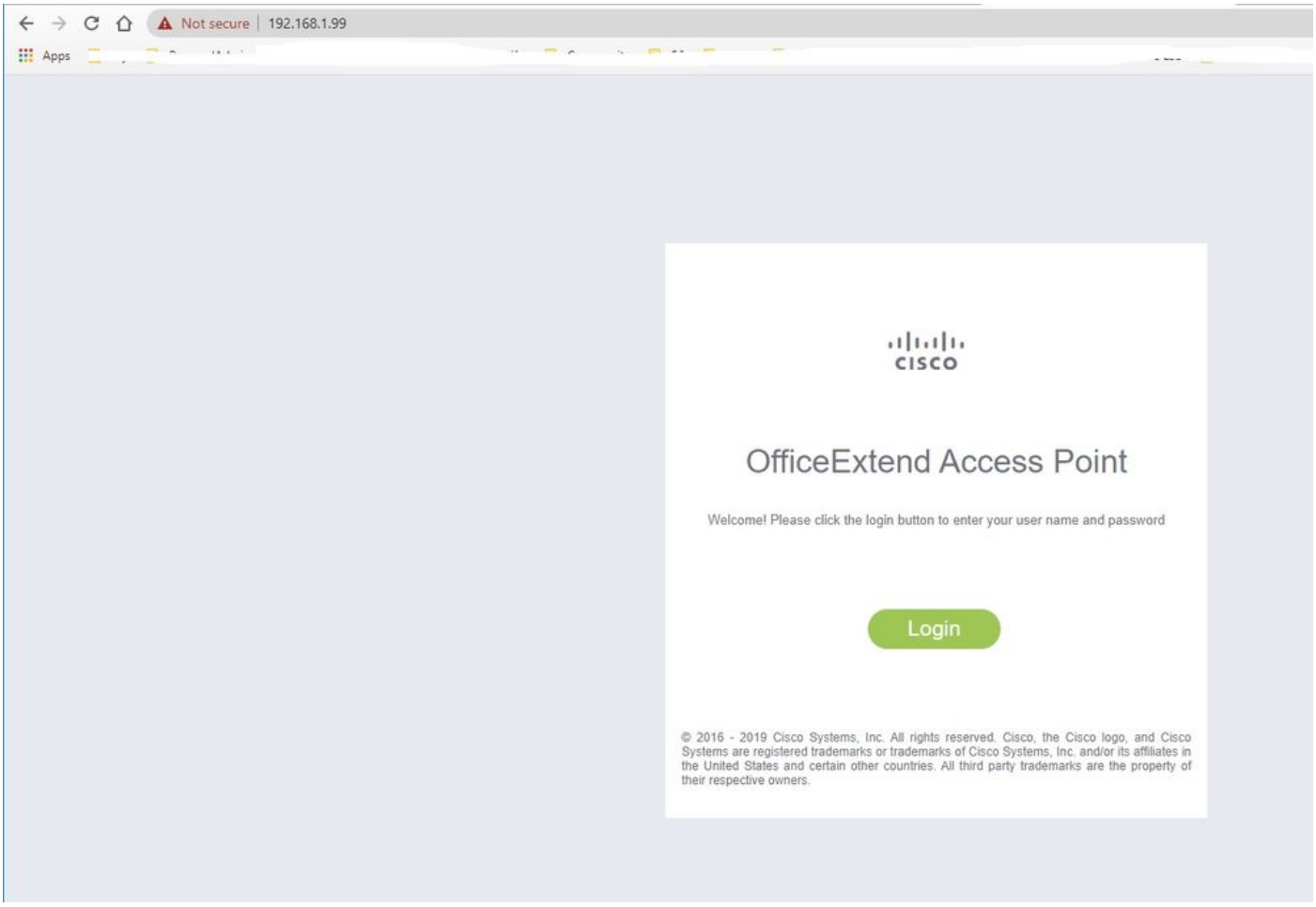
```
AP3800_E1.3EB8#show capwap client config
AdminState : ADMIN_ENABLED(1)
Name : AP3800_E1.3EB8
Location : default location
Primary controller name : eWLC-9800-01
Primary controller IP : 192.168.1.15
Secondary controller name : c3504-01
Secondary controller IP : 192.168.1.14
Tertiary controller name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

Hier is een voorbeeld van pakketvastlegging die verkeer toont dat lokaal wordt geschakeld. Hier was de test een 'ping' van een client met IP 192.168.1.98 naar de Google DNS-server en daarna naar 192.168.1.254. Je kunt ICMP zien vanuit het IP van het AP IP-adres 192.168.1.99, verzonden naar de DNS naar de AP NATing het verkeer lokaal. Er is geen ICMP op 192.168.1.254 omdat het verkeer versleuteld wordt in de DTLS-tunnel en alleen Application Data Frames worden gezien.

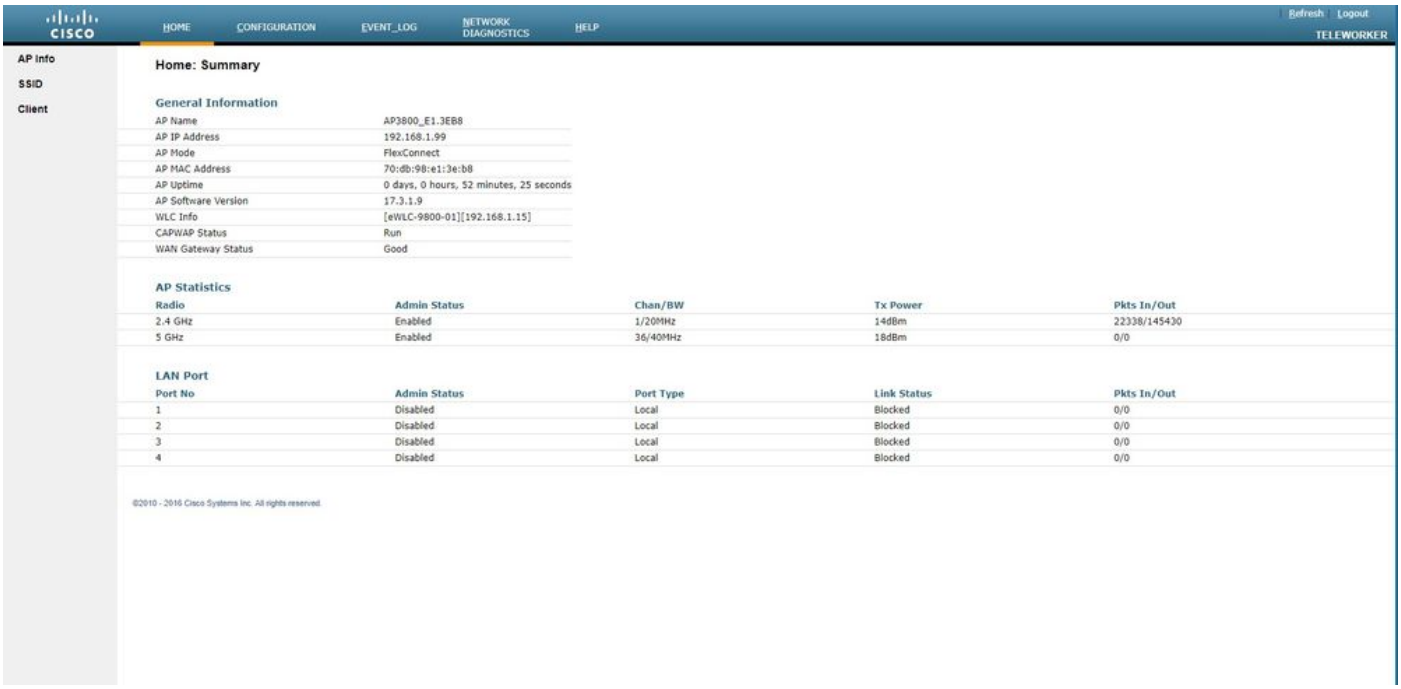


> **Opmerking:** Het verkeer dat lokaal geschakeld wordt is NATed door AP omdat in normale scenario's, clientnet tot het netwerk van het Bureau behoort en de lokale apparaten op het bureau van het huis weten niet hoe te om de cliëntensubnet te bereiken. AP vertaalt het clientverkeer met behulp van het AP IP-adres dat in het lokale kantoornet is.

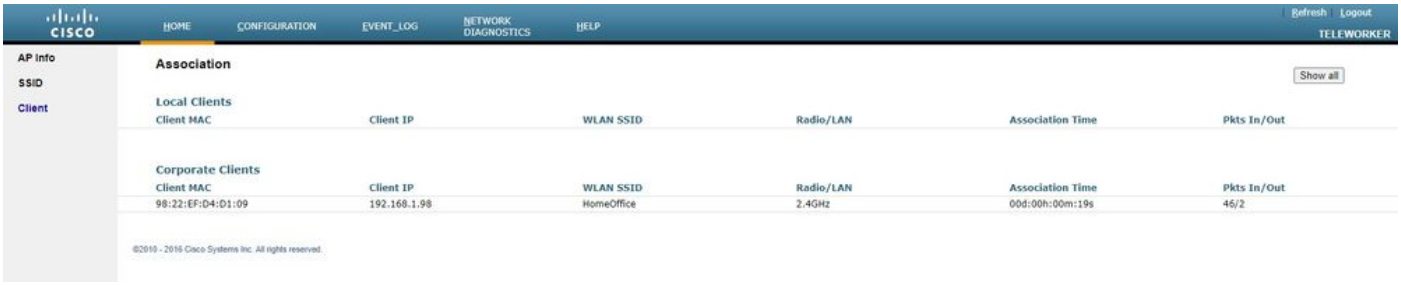
U hebt toegang tot de OEAP GUI die een browser opent en de URL intypt op het AP-adres AP. De standaardaanmeldingsgegevens zijn admin/admin. en u moet ze bij de eerste aanmelding wijzigen.



Zodra u inlogt, hebt u toegang tot de GUI:



U hebt toegang tot typische informatie in een OEAP, zoals AP info, SSIDs en Clients verbonden:



Verwante documentatie

[Begrijp FlexConnect op Catalyst 9800 draadloze controller]

[Split-tunneling voor FlexConnect]

[EAP en RLAN op Catalyst 9800 WLC configureren]