Konfigurationsbeispiel für Catalyst 9800 und FlexConnect OEAP Split Tunneling

Inhalt

Einleitung

Dieses Dokument zeigt, wie der WLC 9800 mit Access Points für Innenbereiche im FlexConnect Office Extend (OEAP)-Modus konfiguriert und Split-Tunneling aktiviert wird, um festzulegen, welcher Datenverkehr lokal im Heimbüro geswitcht werden kann und welcher Datenverkehr zentral am WLC weitergeleitet und geschaltet werden sollte.

Voraussetzungen

Anforderungen

Bei der Konfiguration in diesem Dokument wird davon ausgegangen, dass der WLC bereits in einer DMZ mit aktivierter NAT konfiguriert ist und dass der Access Point vom Heimbüro aus dem WLC beitreten kann.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Wireless LAN Controller 9800 mit IOS-XE 17.3.1 Software

- Wave1-APs: 1700/2700/3700.
- Wave2-APs: 1800/2800/3800/4800 und der Catalyst Serie 9100.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung.

Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Überblick

Ein Cisco OfficeExtend Access Point (Cisco OEAP) bietet eine sichere Kommunikation von einem Cisco WLC zu einem Cisco AP an einem Remote-Standort und erweitert nahtlos das Unternehmens-WLAN über das Internet auf den Wohnsitz eines Mitarbeiters. Das Anwendererlebnis im Heimbüro ist genauso wie im Büro. Die DTLS-Verschlüsselung (Datagram Transport Layer Security) zwischen Access Point und Controller stellt sicher, dass alle Kommunikationen ein Höchstmaß an Sicherheit bieten. Jeder Access Point in Innenräumen in FlexConnect kann als Office Extend AP fungieren.

Hintergrundinformationen

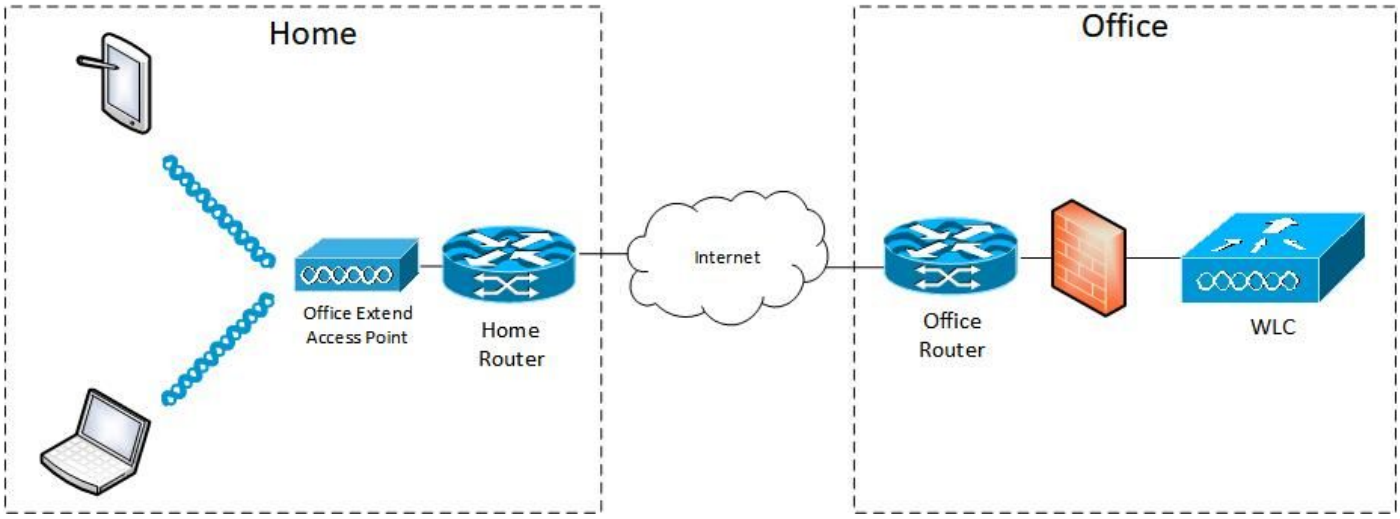
FlexConnect bezieht sich auf die Fähigkeit eines Access Points (AP), Wireless-Clients zu verwalten, während diese an entfernten Standorten betrieben werden, z. B. über ein WAN. Sie können auch entscheiden, ob der Datenverkehr von den Wireless-Clients direkt auf der AP-Ebene (Lokales Switching) in das Netzwerk geleitet wird oder ob der Datenverkehr zentralisiert an den 9800-Controller (Central Switching) geleitet und auf WLAN-Basis über das WAN zurückgesendet wird.

Weitere Informationen zu FlexConnect finden Sie in diesem Dokument Verstehen von FlexConnect auf Catalyst 9800 Wireless Controller.

Der Office Extend-Modus ist eine Option, die in einem FlexConnect-Access Point verfügbar ist, um zusätzliche Funktionen bereitzustellen, z. B. eine persönliche lokale SSID für den Heimzugriff, und kann auch Split-Tunneling-Funktion bereitstellen, um detaillierter festzulegen, welcher Datenverkehr lokal im Heimbüro und welcher Datenverkehr zentral im WLC über ein einzelnes WLAN geschaltet werden soll.

Konfigurieren

Netzwerkdiagramm



Konfigurationen

Definieren einer Zugriffskontrollliste für Split Tunneling

Schritt 1: Wählen Sie Configuration > Security > ACL aus. Klicken Sie auf Hinzufügen.

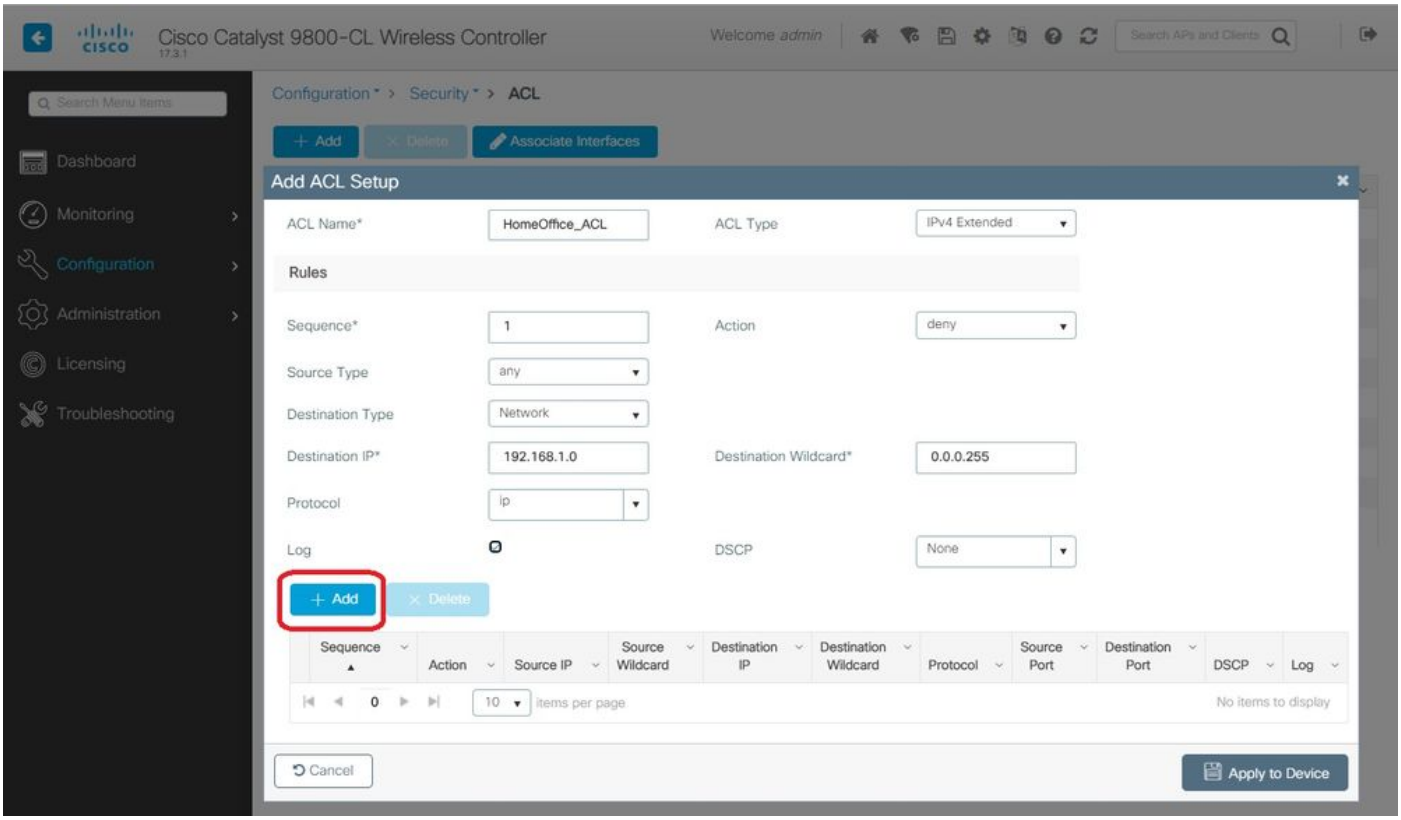
Schritt 2: Geben Sie im Dialogfeld Add ACL Setup (ACL-Einrichtung hinzufügen) den ACL-Namen ein, wählen Sie in der Dropdown-Liste ACL Type (ACL-Typ) den ACL-Typ aus, und geben Sie unter Rules settings (Regeleinstellungen) die Sequenznummer ein. Wählen Sie dann Aktion entweder als Zulassen oder Ablehnen aus.

Schritt 3: Wählen Sie in der Dropdown-Liste Source Type (Quellentyp) den gewünschten Quelltyp aus.

Wenn Sie den Quelltyp als Host auswählen, müssen Sie den Hostnamen/die IP-Adresse eingeben.

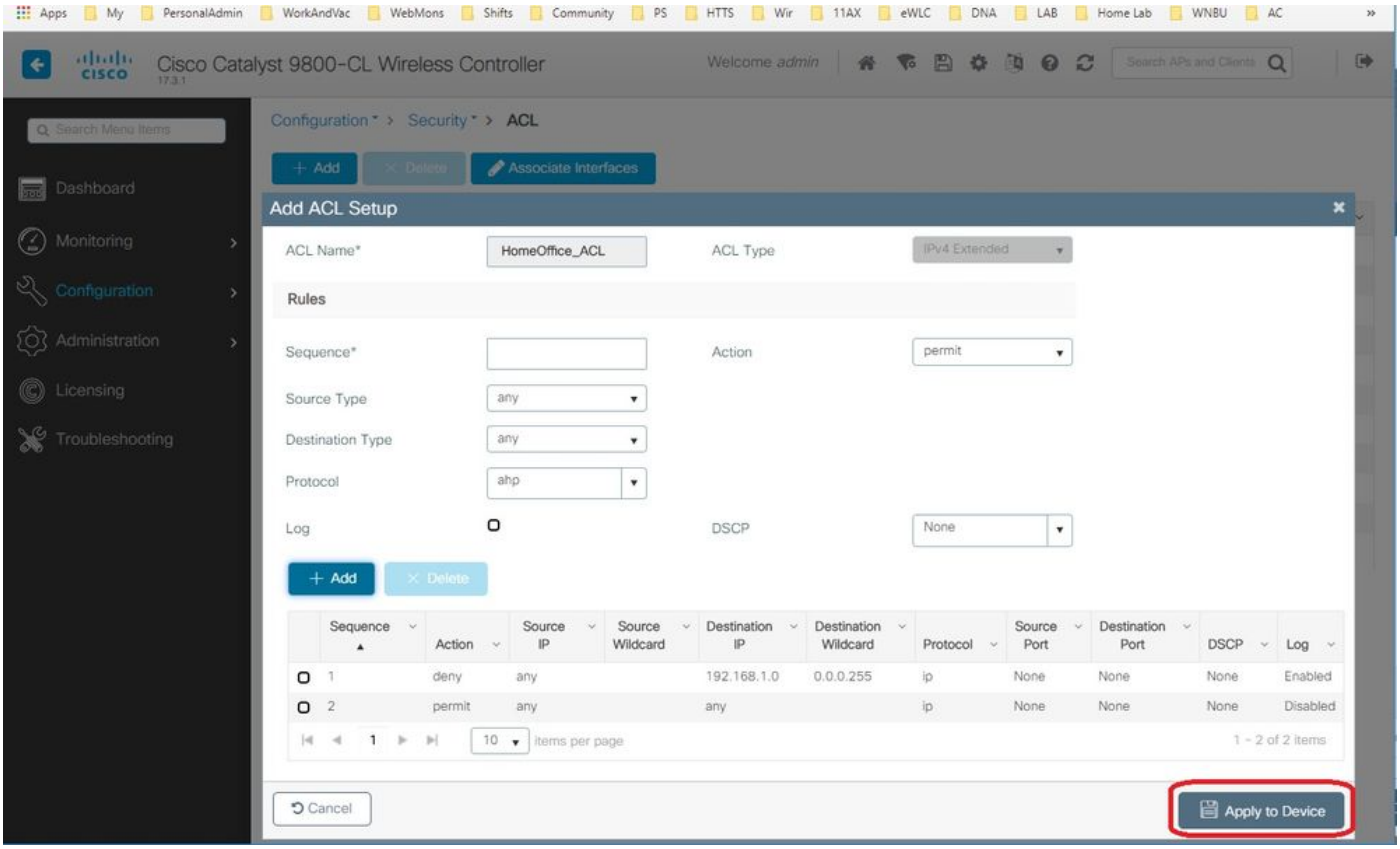
Wenn Sie den Quelltyp als Netzwerk auswählen, müssen Sie die Quell-IP-Adresse und die Platzhaltermaske angeben.

In diesem Beispiel wird der gesamte Datenverkehr von einem Host zum Subnetz 192.168.1.0/24 zentral umgeleitet (verweigern), und der restliche Datenverkehr wird lokal geschaltet (zulassen).



Schritt 4: Aktivieren Sie das Kontrollkästchen Protokoll, wenn Sie die Protokolle speichern möchten, und klicken Sie auf Hinzufügen.

Schritt 5: Fügen Sie die übrigen Regeln hinzu, und klicken Sie auf Auf Gerät anwenden.

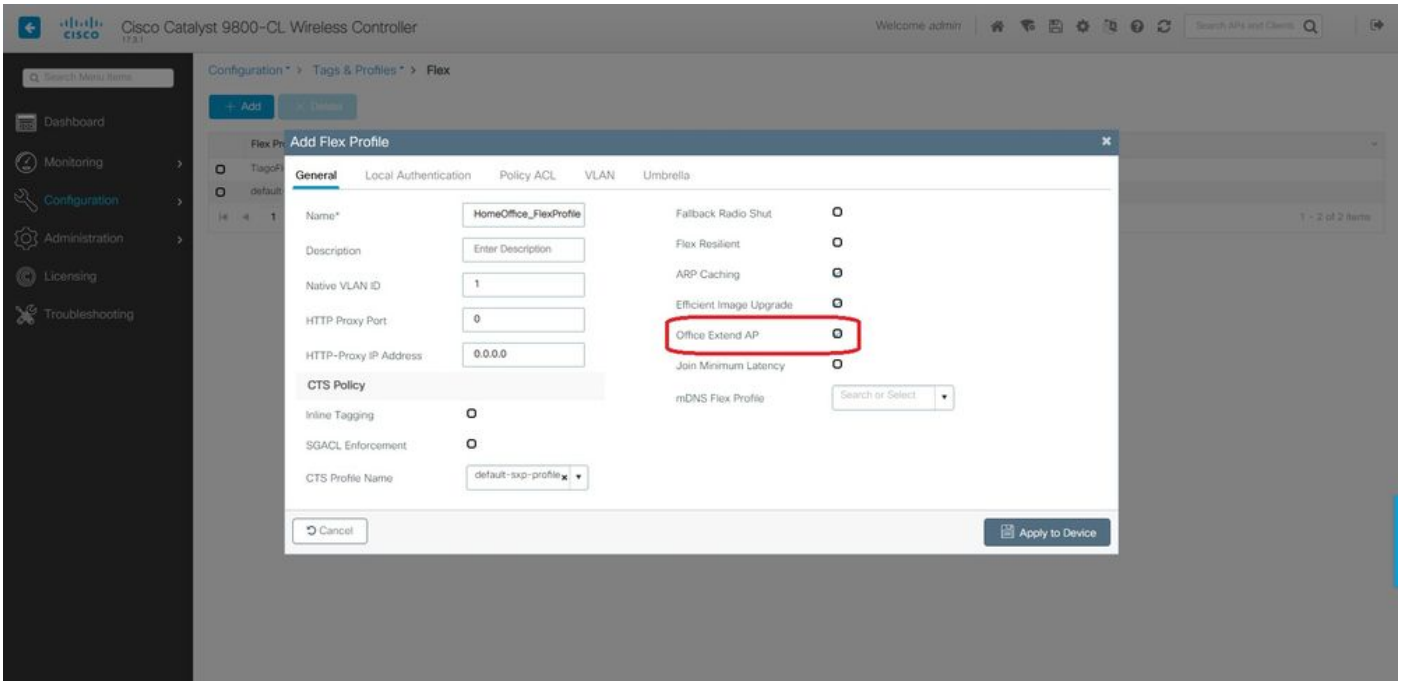


Verknüpfen einer ACL-Richtlinie mit der definierten ACL

Schritt 1: Erstellen Sie ein neues Flex-Profil. Gehen Sie zu Konfiguration > Tags & Profile > Flex.

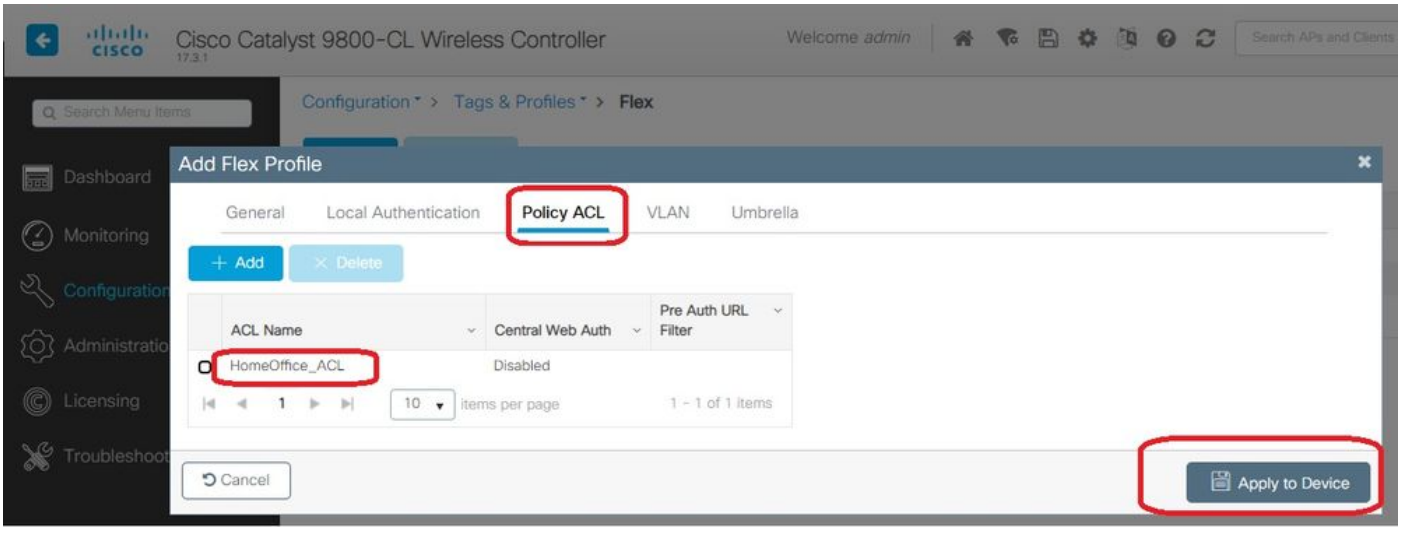
Klicken Sie auf Hinzufügen.

Schritt 2: Geben Sie einen Namen ein, und aktivieren Sie Office Extend AP. Stellen Sie außerdem sicher, dass die native VLAN-ID die im AP-Switch-Port ist.



> **Anmerkung:** Wenn Sie den Office-Extend-Modus aktivieren, ist die Link-Encryption ebenfalls standardmäßig aktiviert und kann nicht geändert werden, selbst wenn Sie die Link-Verschlüsselung im AP-Join-Profil deaktivieren.

Schritt 3: Wechseln Sie zur Registerkarte "Policy ACL", und klicken Sie auf Hinzufügen. Fügen Sie hier die ACL zum Profil hinzu, und wenden Sie sie auf das Gerät an.

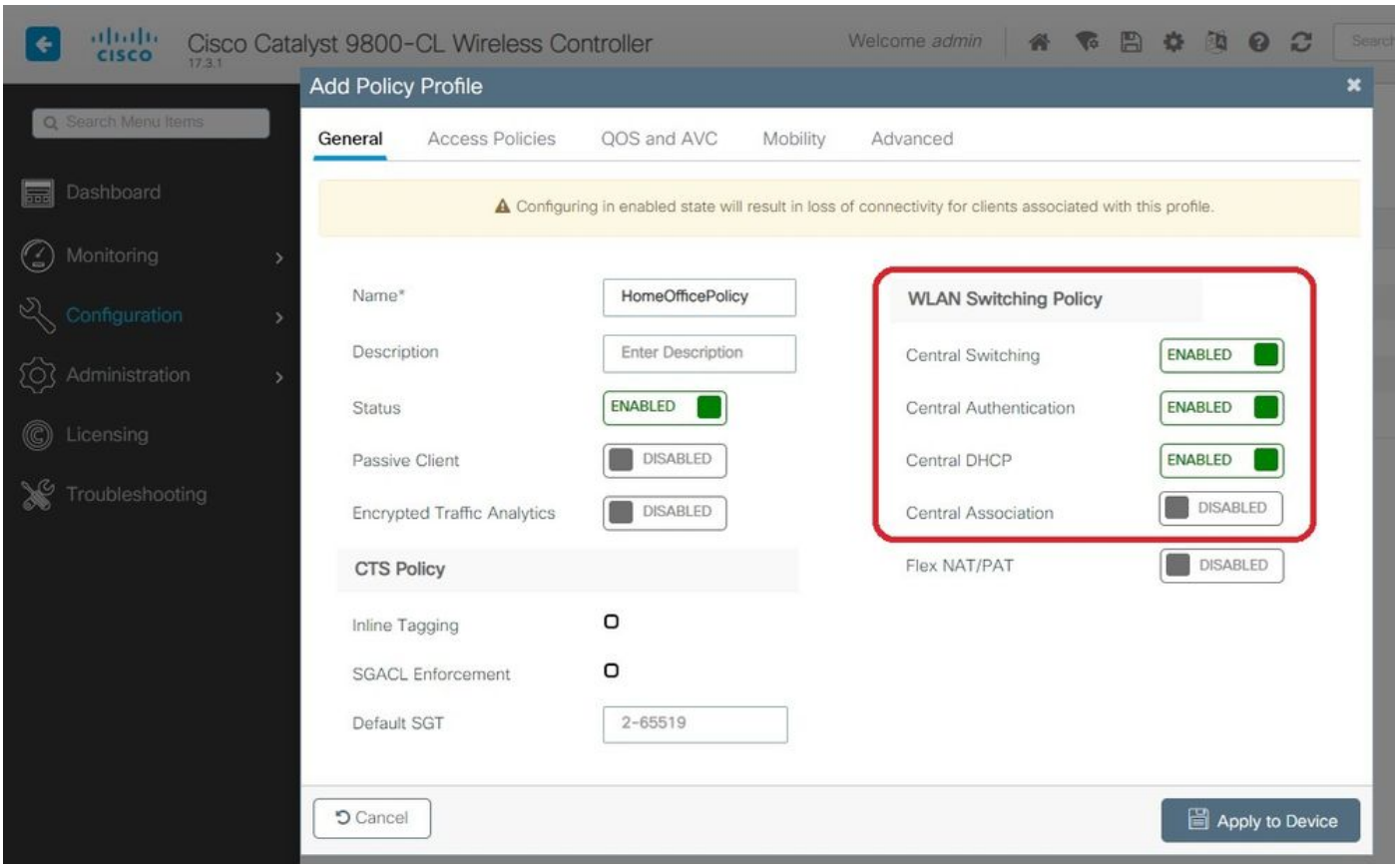


Konfigurieren einer Wireless-Profilrichtlinie und eines Split MAC ACL-Namens

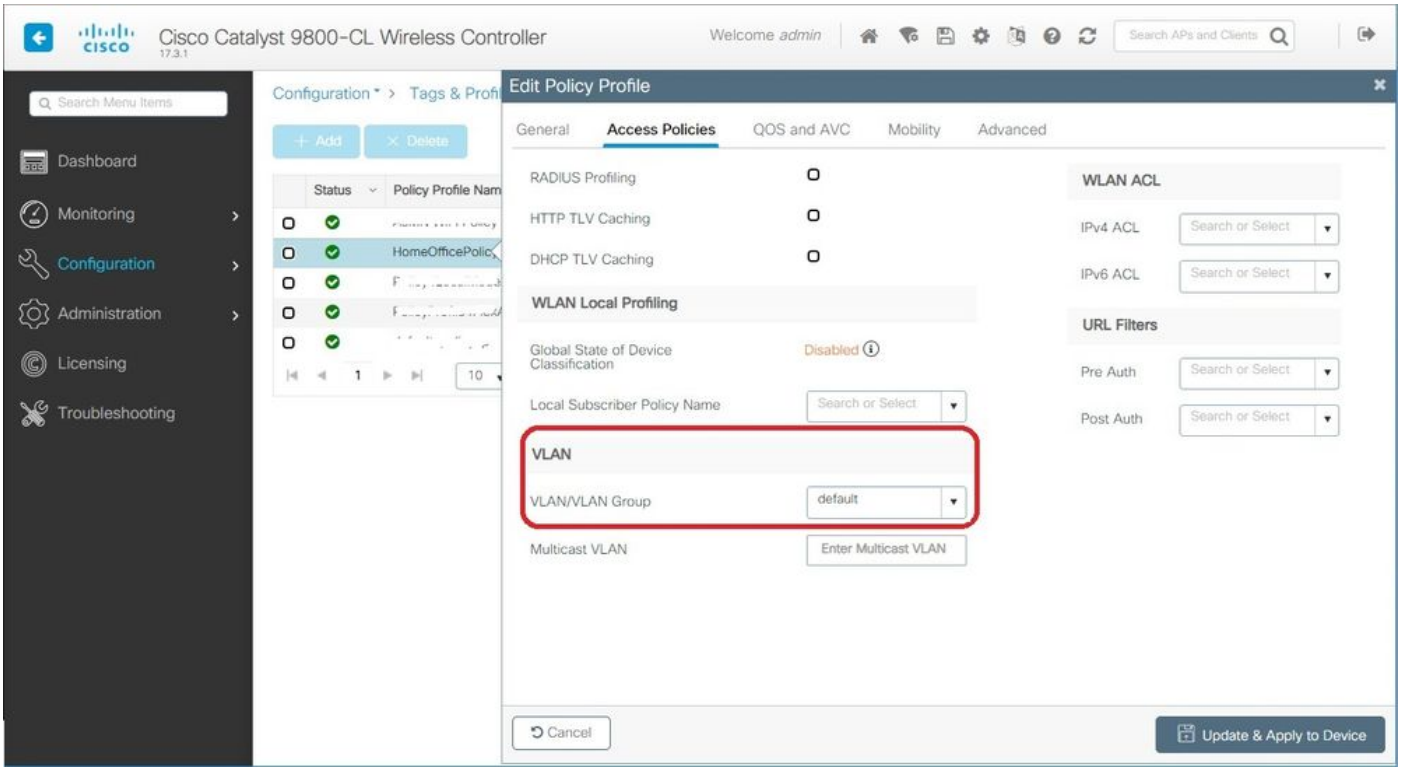
Schritt 1: Erstellen Sie ein WLAN-Profil. In diesem Beispiel wurde eine SSID mit dem Namen HomeOffice mit WPA2-PSK-Sicherheit verwendet.

Schritt 2: Erstellen eines Richtlinienprofils Gehen Sie zu Konfiguration > Tags > Richtlinie, und

klicken Sie auf Hinzufügen. Stellen Sie unter Allgemein sicher, dass dieses Profil zentral geswitchte Richtlinien hat, wie in diesem Beispiel gezeigt:

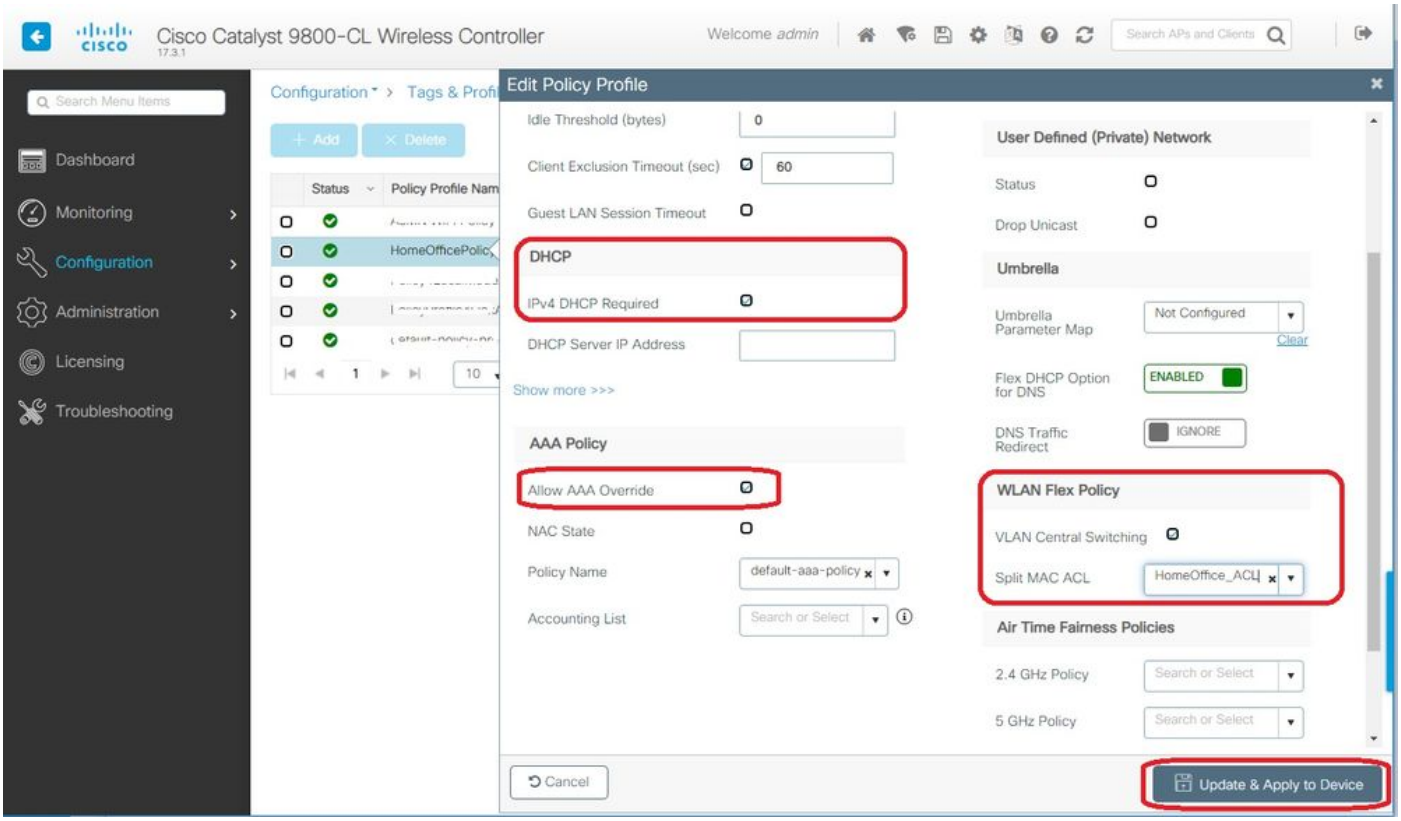


Schritt 3: Gehen Sie im Richtlinienprofil zu Access Policies (Zugriffsrichtlinien), und definieren Sie das VLAN für den Datenverkehr, der zentral geswitcht werden soll. Die Clients erhalten die IP-Adresse im Subnetz, das diesem VLAN zugewiesen ist.



Schritt 4: Um lokales Split-Tunneling auf einem WAP zu konfigurieren, müssen Sie sicherstellen,

dass DCHP Required im WLAN aktiviert ist. Dadurch wird sichergestellt, dass der Client, der dem geteilten WLAN zugeordnet ist, DHCP ausführt. Sie können diese Option auf der Registerkarte Erweitert im Richtlinienprofil aktivieren. Aktivieren Sie das Kontrollkästchen IPv4 DHCP Required. Wählen Sie unter den Einstellungen für die WLAN-Flex-Richtlinie die zuvor erstellte geteilte MAC-ACL aus der Dropdown-Liste "MAC-ACL aufteilen" aus. Klicken Sie auf Auf Gerät anwenden:



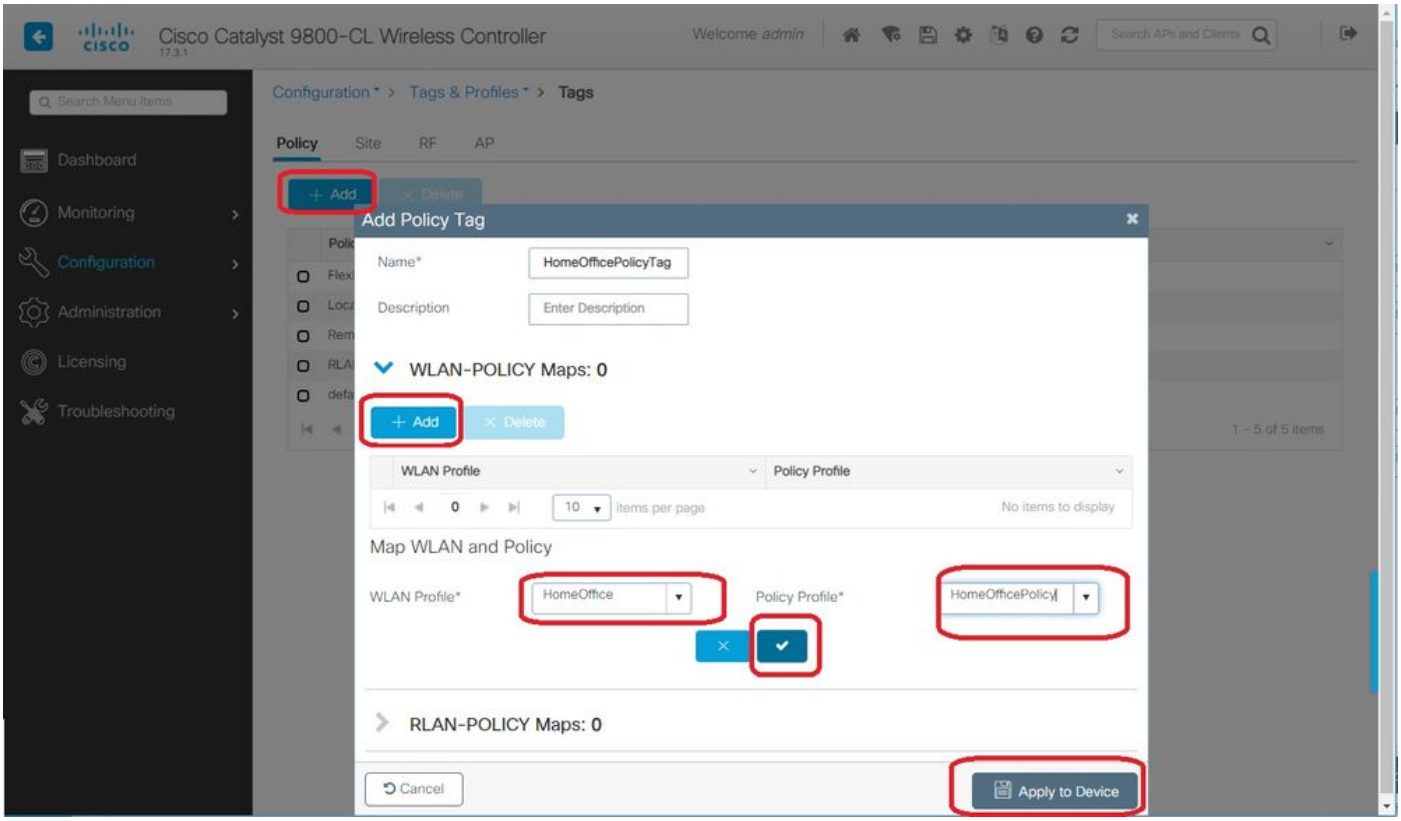
Anmerkung: Apple iOS-Clients benötigen Option 6 (DNS), um im DHCP-Angebot für Split-Tunneling konfiguriert zu werden.

Zuordnen eines WLAN zu einem Richtlinienprofil

Schritt 1: Wählen Sie Konfiguration > Tags & Profile > Tags aus. Klicken Sie auf der Registerkarte Richtlinien auf Hinzufügen.

Schritt 2: Geben Sie den Namen der Tag-Richtlinie ein, und klicken Sie auf der Registerkarte WLAN-POLICY Maps (WLAN-POLICY-Karten) auf Hinzufügen.

Schritt 3: Wählen Sie das WLAN-Profil aus der Dropdown-Liste WLAN Profile (WLAN-Profil) aus, und wählen Sie das Richtlinienprofil aus der Dropdown-Liste Policy Profile (Richtlinienprofil) aus. Klicken Sie auf das Symbol Tick und dann auf Gerät anwenden.

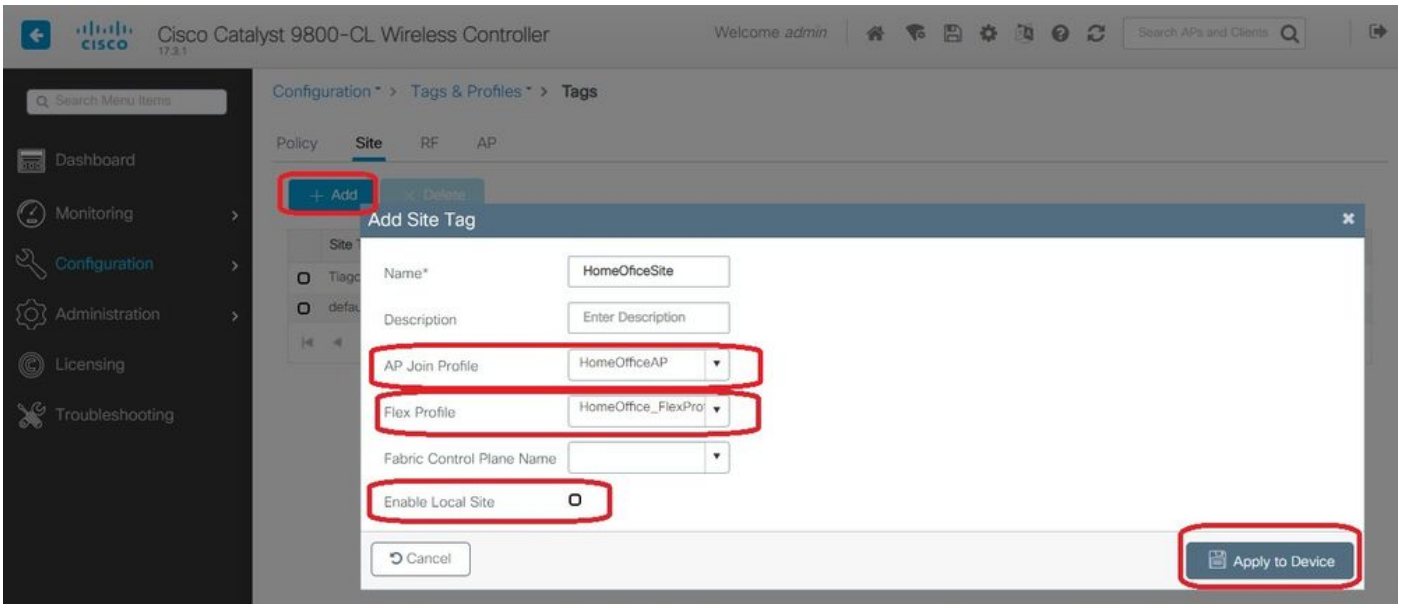


Konfigurieren eines AP-Join-Profils und der Verknüpfung mit dem Site-Tag

Schritt 1: Navigieren Sie zu Konfiguration > Tags & Profile > AP Join (Konfiguration > Tags und Profile > AP Join), und klicken Sie auf Add (Hinzufügen). Geben Sie einen Namen ein. Optional können Sie SSH aktivieren, um die Fehlerbehebung zu ermöglichen, und diese später deaktivieren, wenn sie nicht benötigt wird.

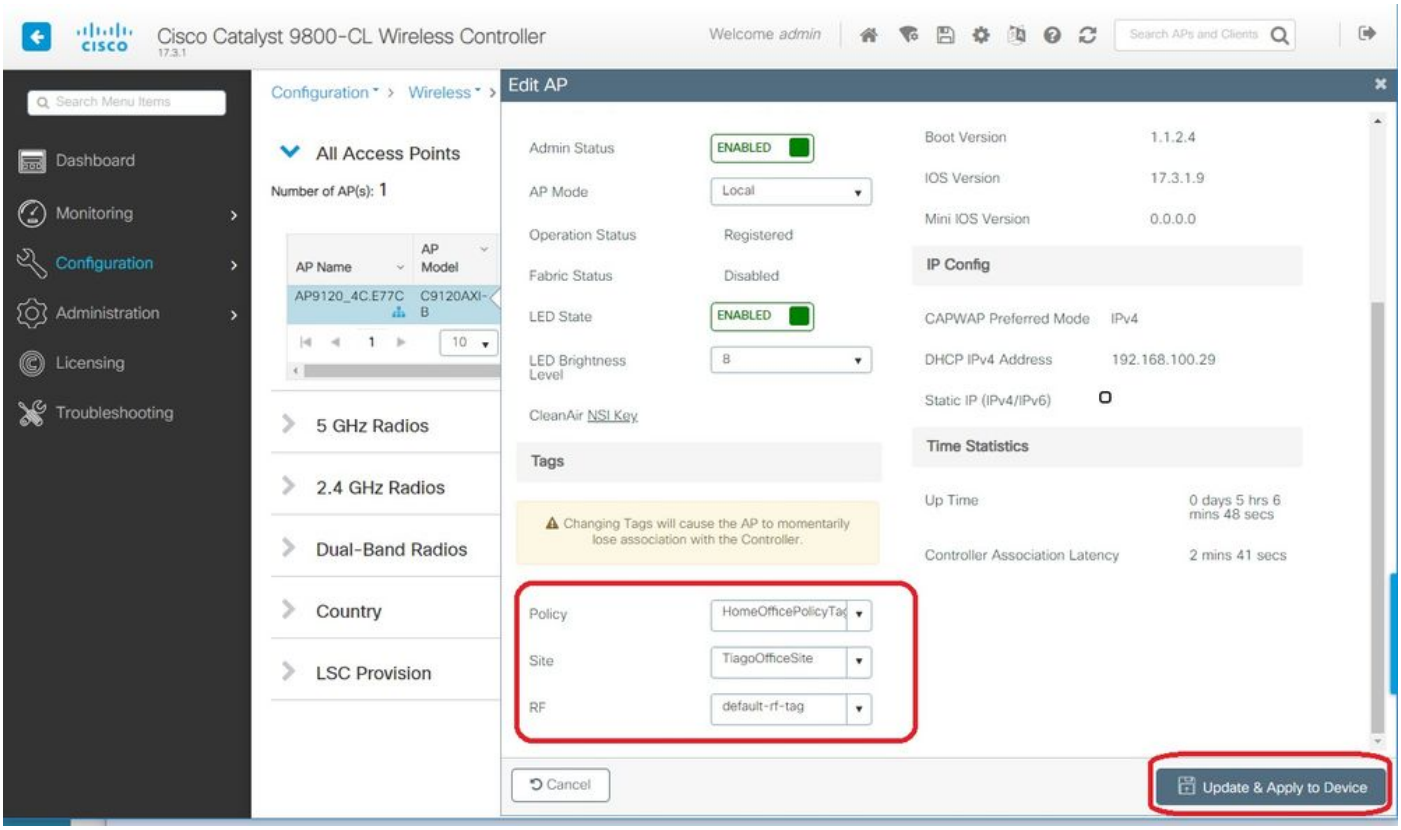
Schritt 2: Wählen Sie Konfiguration > Tags & Profile > Tags aus. Klicken Sie auf der Registerkarte Standort auf Hinzufügen.

Schritt 3: Geben Sie den Namen des Standorts-Tags ein, deaktivieren Sie die Option Lokalen Standort aktivieren, und wählen Sie dann das AP-Join-Profil und das Flex-Profil (zuvor erstellt) aus den Dropdown-Listen aus. Dann auf Gerät anwenden.

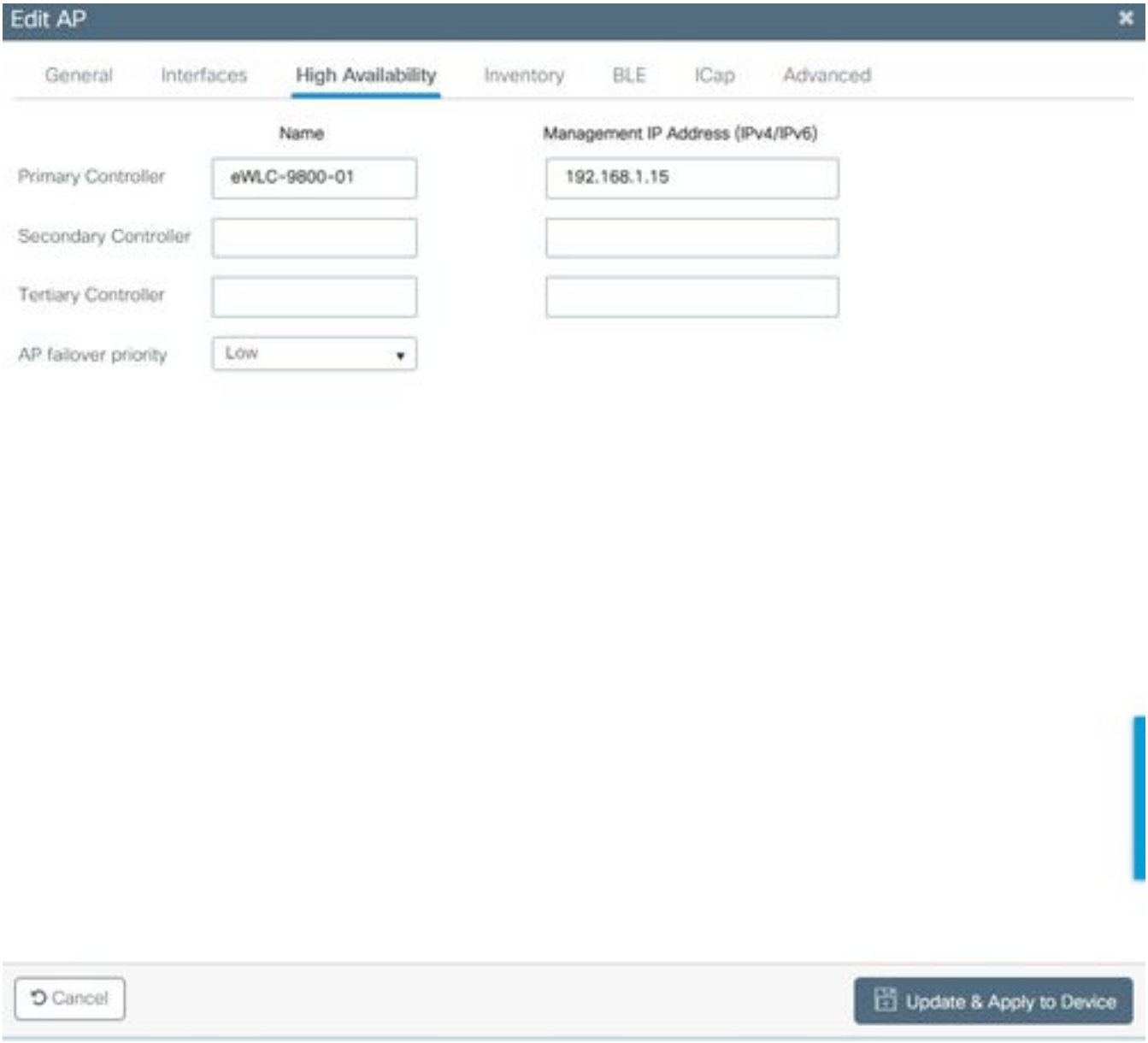


Anfügen eines Richtlinien-Tags und eines Site-Tags an einen Access Point

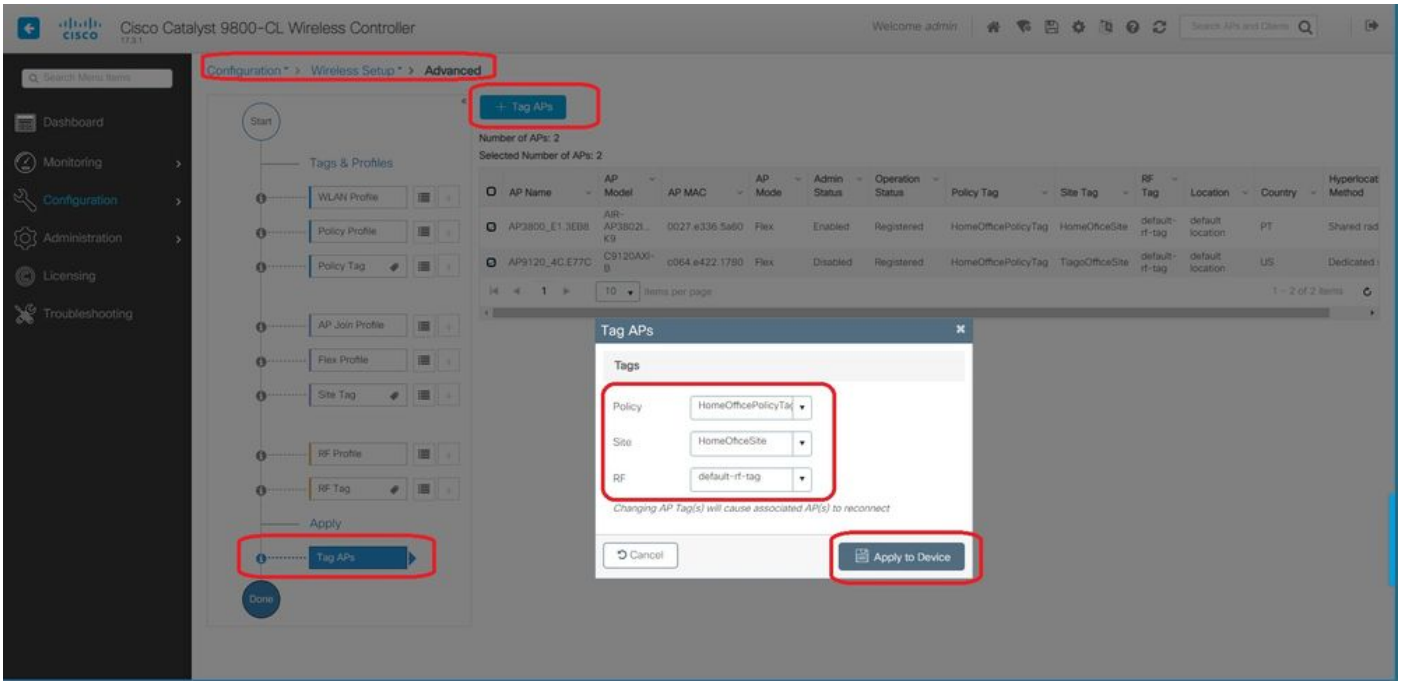
Option 1: Bei dieser Option müssen Sie jeweils einen Access Point konfigurieren. Gehen Sie zu Configuration > Wireless > Access Points. Wählen Sie den AP aus, den Sie zum Heimbüro verschieben möchten, und wählen Sie dann die Home Office-Tags aus. Klicken Sie auf Aktualisieren und auf Gerät anwenden:



Es wird empfohlen, einen primären Controller zu konfigurieren, damit der Access Point die IP/Name des WLC kennt, die nach der Bereitstellung im Heimbüro erreicht werden soll. Sie können dies bearbeiten, indem Sie den Access Point direkt auf die Registerkarte "Hohe Verfügbarkeit" setzen:



Option 2: Mit dieser Option können Sie mehrere APs gleichzeitig konfigurieren. Navigieren Sie zu Configuration > Wireless Setup > Advanced > Tag APs. Wählen Sie die zuvor erstellten Tags aus, und klicken Sie auf Auf Gerät anwenden.



Die APs werden neu gestartet, und der WLC wird mit den neuen Einstellungen neu verbunden.

Überprüfung

Sie können die Konfiguration über GUI oder CLI überprüfen. Dies ist die resultierende Konfiguration in der 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
!
```

AP-Konfiguration wird geprüft:

```
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
...
```

Sie können eine direkte Verbindung zum Access Point herstellen und auch die Konfiguration überprüfen:

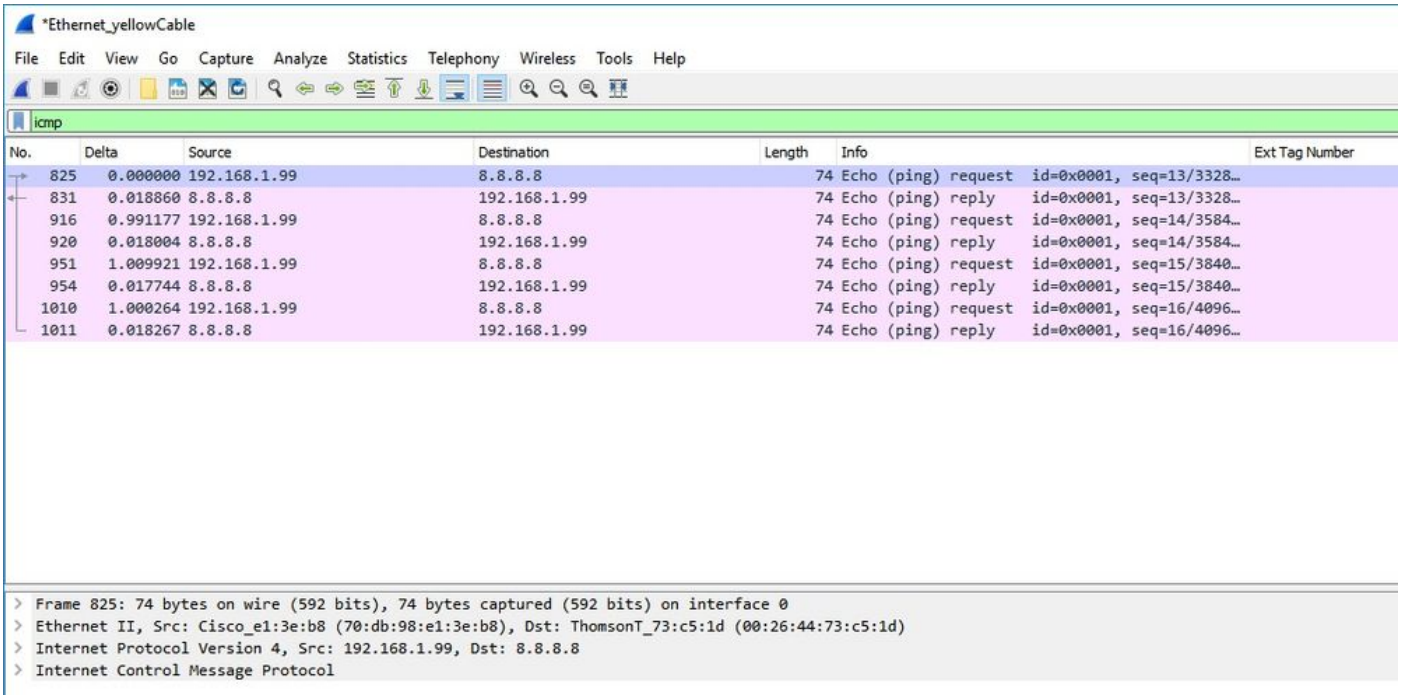
```
AP3800_E1.3EB8#show ip access-lists
Extended IP access list HomeOffice_ACL
1 deny ip any 192.168.1.0 0.0.0.255
2 permit ip any any

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
...
```

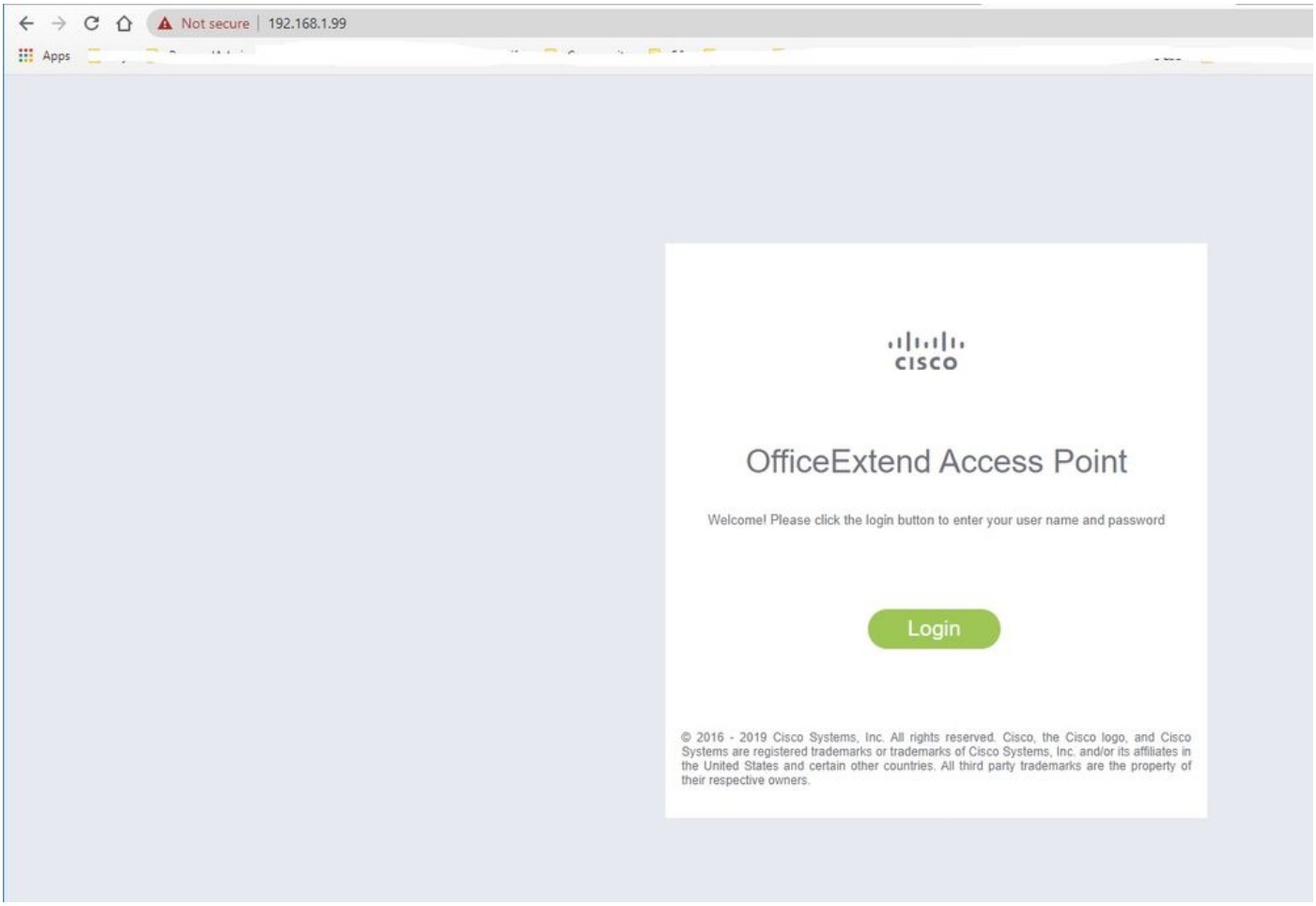
```
AP3800_E1.3EB8#show capwap client config
AdminState : ADMIN_ENABLED(1)
Name : AP3800_E1.3EB8
Location : default location
Primary controller name : eWLC-9800-01
Primary controller IP : 192.168.1.15
Secondary controller name : c3504-01
Secondary controller IP : 192.168.1.14
Tertiary controller name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

Hier ein Beispiel für Paketerfassungen, die zeigen, dass der Datenverkehr lokal geschaltet wird. Dabei wurde ein "Ping" von einem Client mit IP 192.168.1.98 auf 8.8.8.8 und dann auf 192.168.1.254 getestet. Sie sehen, dass der ICMP, der die IP-Adresse der AP-IP-Adresse 192.168.1.99 erhält, an 8.8.8.8 gesendet wurde, da der Access Point NAT den Datenverkehr lokal verarbeitet. Es gibt kein icmp bis 192.168.1.254, da der Datenverkehr im DTLS-Tunnel verschlüsselt wird und nur Anwendungsdaten-Frames angezeigt werden.

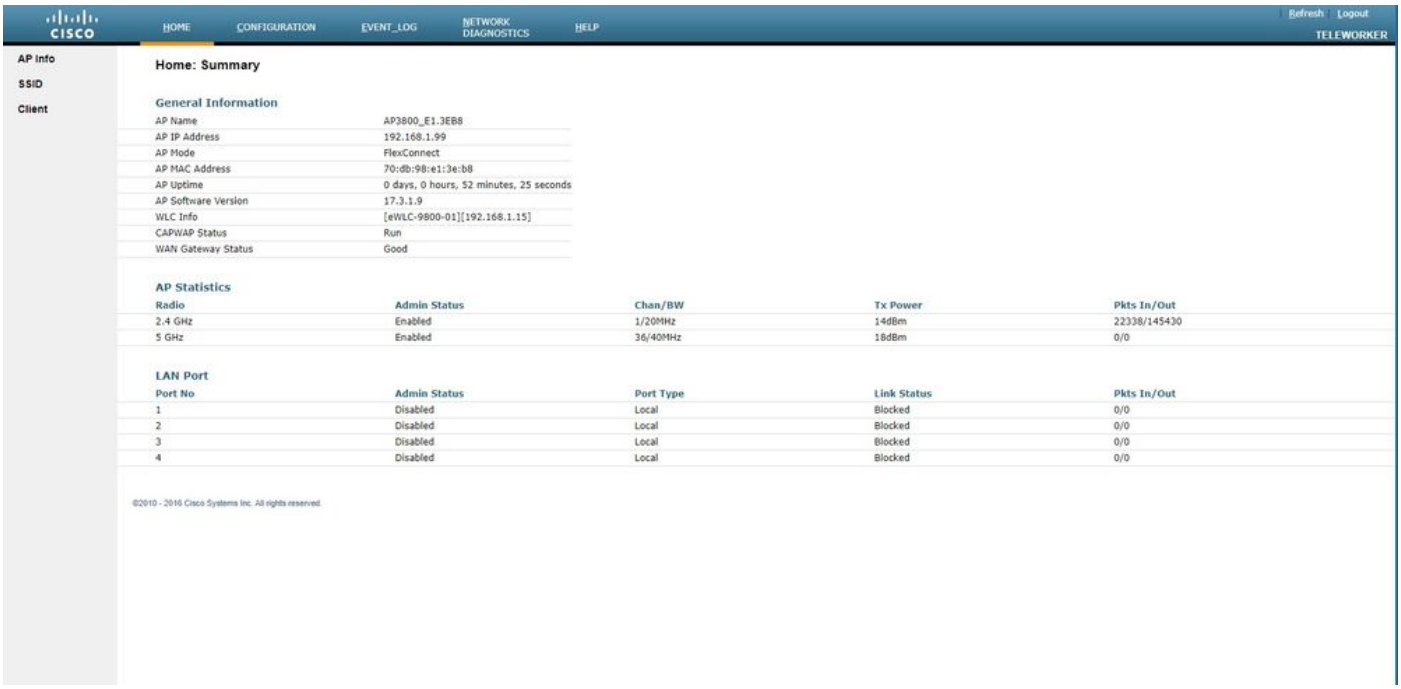


> **Anmerkung:** Der lokal geswitchte Datenverkehr wird vom Access Point NATed verarbeitet, da das Client-Subnetz in normalen Szenarien zum Office-Netzwerk gehört und die lokalen Geräte im Heimbüro nicht wissen, wie das Client-Subnetz erreicht werden kann. Der AP übersetzt den Client-Datenverkehr mithilfe der AP-IP-Adresse, die sich im Subnetz des lokalen Heimbüros befindet.

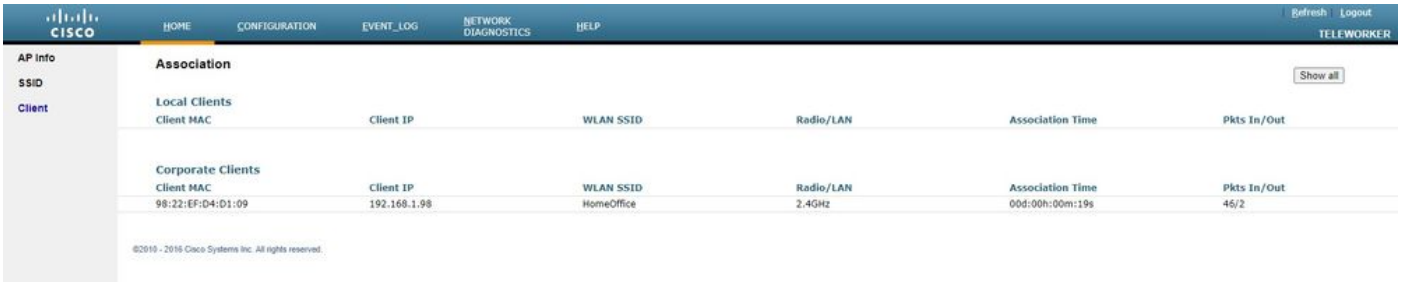
Sie können auf die Access Point Office Extend-GUI zugreifen, einen Browser öffnen und die URL und die AP-IP-Adresse eingeben. Die Standardanmeldeinformationen sind admin/admin. Sie werden bei der ersten Anmeldung aufgefordert, sie zu ändern.



Nach der Anmeldung haben Sie Zugriff auf die GUI:



Sie haben Zugriff auf typische Informationen in einem Office Extend AP, wie AP-Informationen, SSIDs und Clients verbunden:



Zugehörige Dokumentation

FlexConnect auf Catalyst 9800 Wireless Controller

Split Tunneling für FlexConnect

Konfigurieren von OEAP und RLAN auf Catalyst 9800 WLC