Configurazione di Catalyst 9800 e FlexConnect OEAP Split Tunneling

Sommario

Introduzione

Questo documento descrive come configurare un access point interno (AP) come FlexConnect Office Extend (OEAP) e come abilitare il tunneling suddiviso in modo da poter definire quale traffico potrebbe essere commutato localmente all'ufficio di casa e quale traffico deve essere commutato centralmente sul WLC.

Prerequisiti

Requisiti

La configurazione di questo documento presume che il WLC sia già configurato in una DMZ con NAT abilitato e che l'AP sia in grado di collegarsi al WLC dall'ufficio di casa.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Wireless LAN Controller 9800 con software Cisco IOS-XE 17.3.1.
- AP Wave1: 1700/2700/3700 .

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica

Un Cisco OfficeExtend Access Point (Cisco OEAP) fornisce comunicazioni sicure da un WLC Cisco a un Cisco AP in una postazione remota, estendendo senza problemi la WLAN aziendale su Internet fino alla residenza di un dipendente. L'esperienza dell'utente al suo domicilio è esattamente la stessa che si avrebbe al suo ufficio aziendale. La crittografia Datagram Transport Layer Security (DTLS) tra il punto di accesso e il controller assicura che tutte le comunicazioni abbiano il massimo livello di sicurezza. Qualsiasi access point interno in modalità FlexConnect può funzionare come OEAP.

Premesse

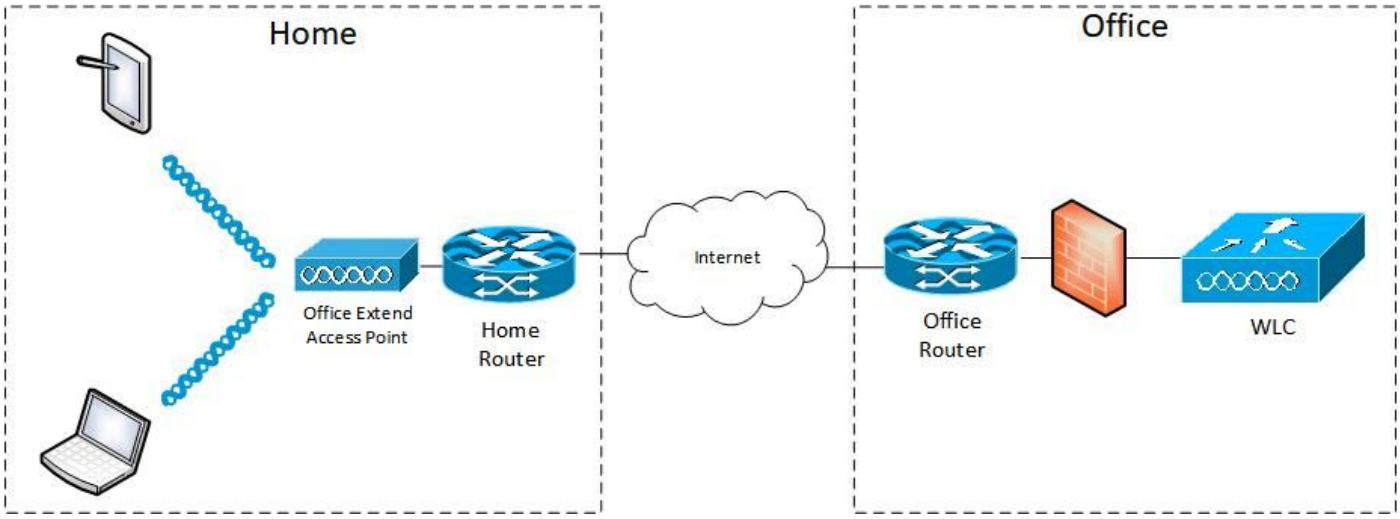
FlexConnect si riferisce alla capacità di un punto di accesso (AP) di gestire client wireless in postazioni remote, ad esempio su una WAN. Possono anche decidere se il traffico proveniente dai client wireless viene immesso direttamente sulla rete a livello di punto di accesso (switching locale) o se il traffico viene centralizzato sul controller 9800 (switching centrale) e inviato nuovamente sulla WAN, per singola WLAN.

Per informazioni dettagliate su FlexConnect, consultare il documento Understand FlexConnect on Catalyst 9800 Wireless Controller.

La modalità OEAP è un'opzione disponibile in un access point FlexConnect per consentire funzionalità aggiuntive, ad esempio un SSID locale personale per l'accesso a casa, e può anche fornire la funzione di tunneling suddiviso, per una maggiore granularità e definire quale traffico deve essere commutato localmente nell'ufficio di casa e quale traffico deve essere commutato centralmente nel WLC, su una singola WLAN

Configurazione

Esempio di rete



Configurazioni

Definizione di una lista di controllo dell'accesso per il tunneling ripartito

Passaggio 1. Scegliere Configurazione > Sicurezza > ACL. Selezionare Aggiungi.

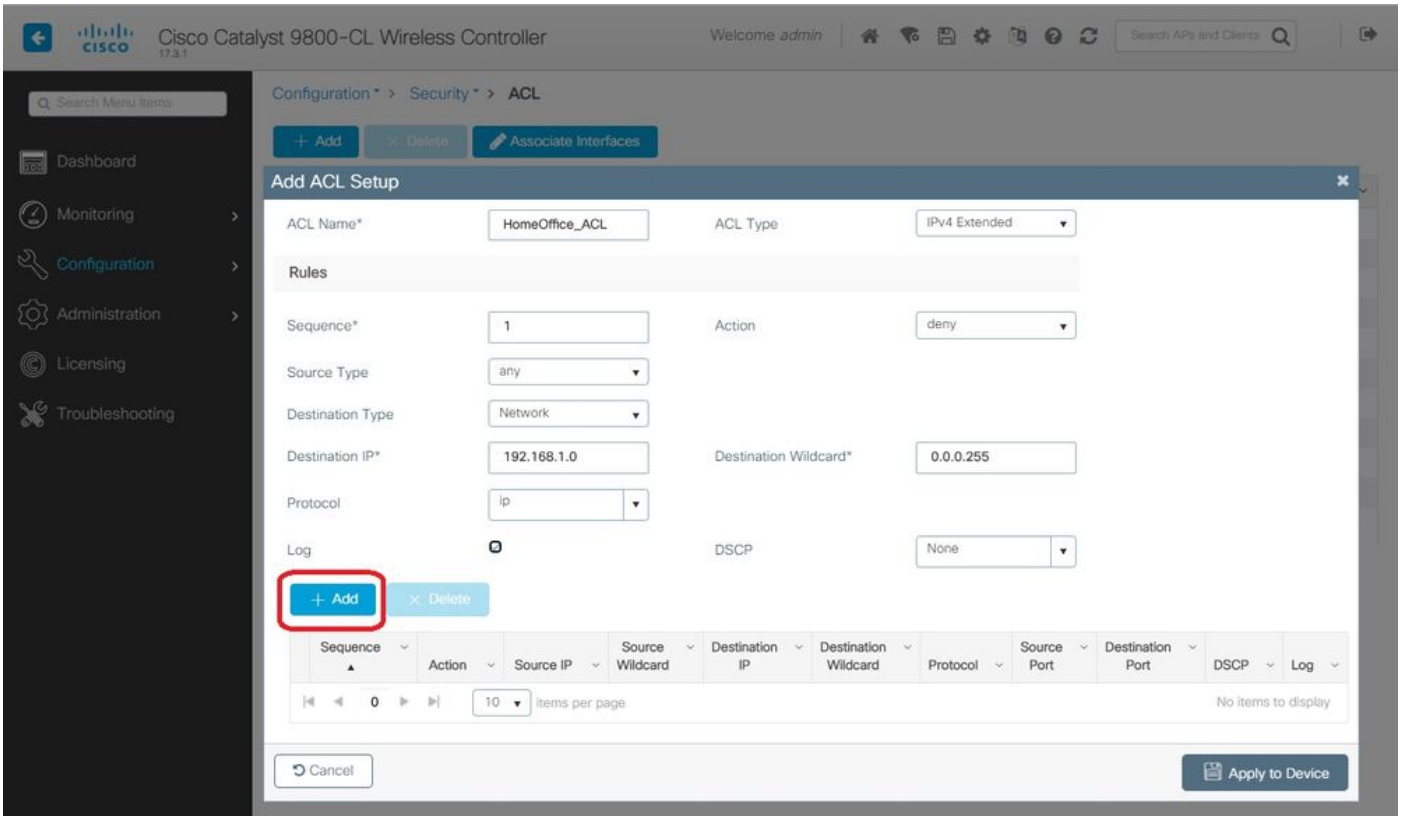
Passaggio 2. Nella finestra di dialogo Add ACL Setup, immettere il nome dell'ACL, scegliere il tipo di ACL dall'elenco a discesa ACL Type (Tipo ACL), quindi immettere il numero di sequenza nelle impostazioni Rules. Scegliere quindi Azione come Consenti o Nega.

Passaggio 3. Scegliere il tipo di origine richiesto dall'elenco a discesa Tipo di origine.

Se si sceglie il tipo di origine Host, è necessario immettere il nome host/IP.

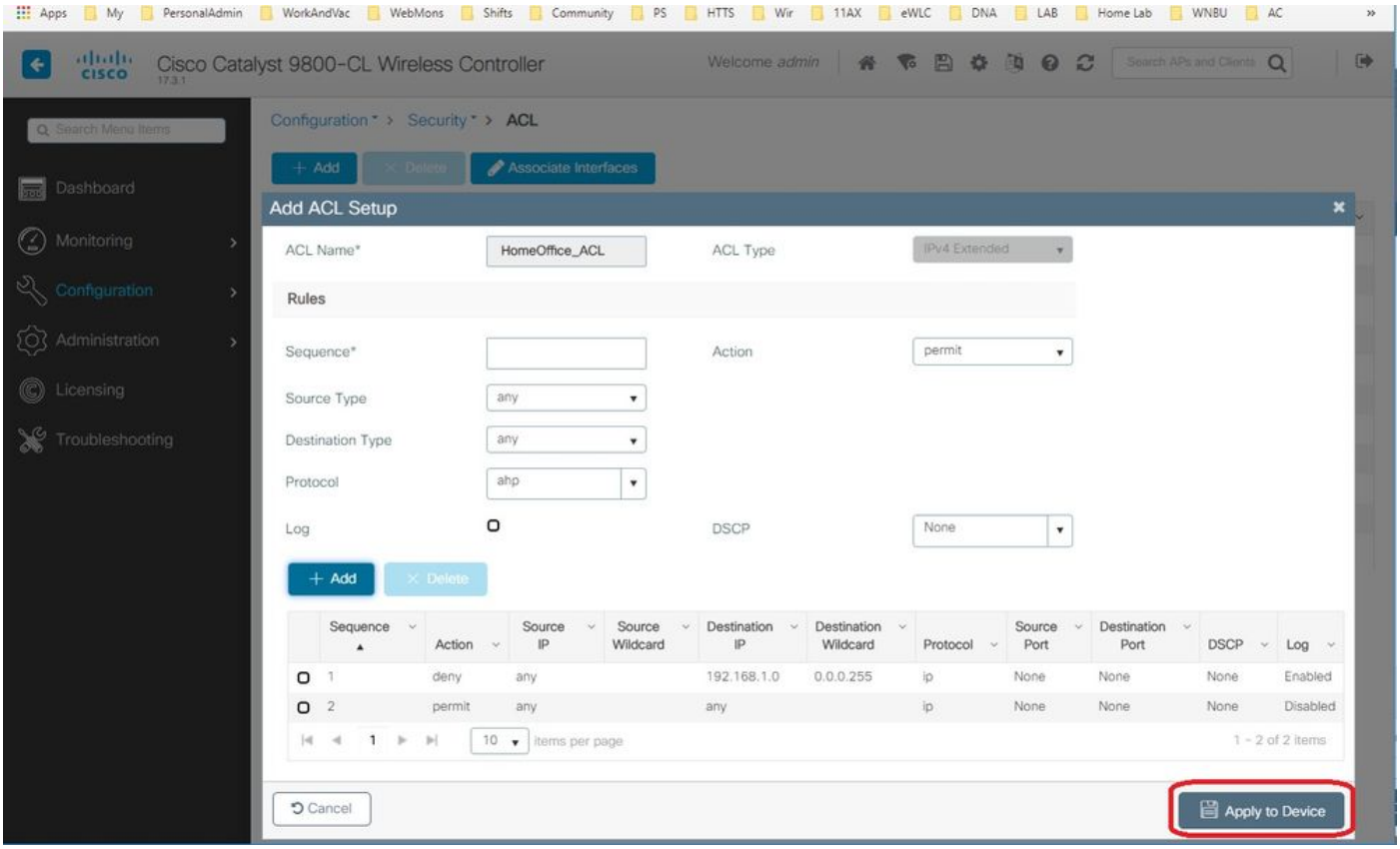
Se si sceglie il tipo di origine Rete, è necessario specificare l'indirizzo IP di origine e la maschera del carattere jolly di origine.

Nell'esempio, tutto il traffico tra un host e la subnet 192.168.1.0/24 viene commutato centralmente (negazione) e tutto il resto del traffico viene commutato localmente (autorizzazione).



Passaggio 4. Selezionare la casella di controllo Registro se si desidera visualizzare i registri e selezionare Aggiungi.

Passaggio 5. Aggiungere le altre regole e selezionare Applica a dispositivo.

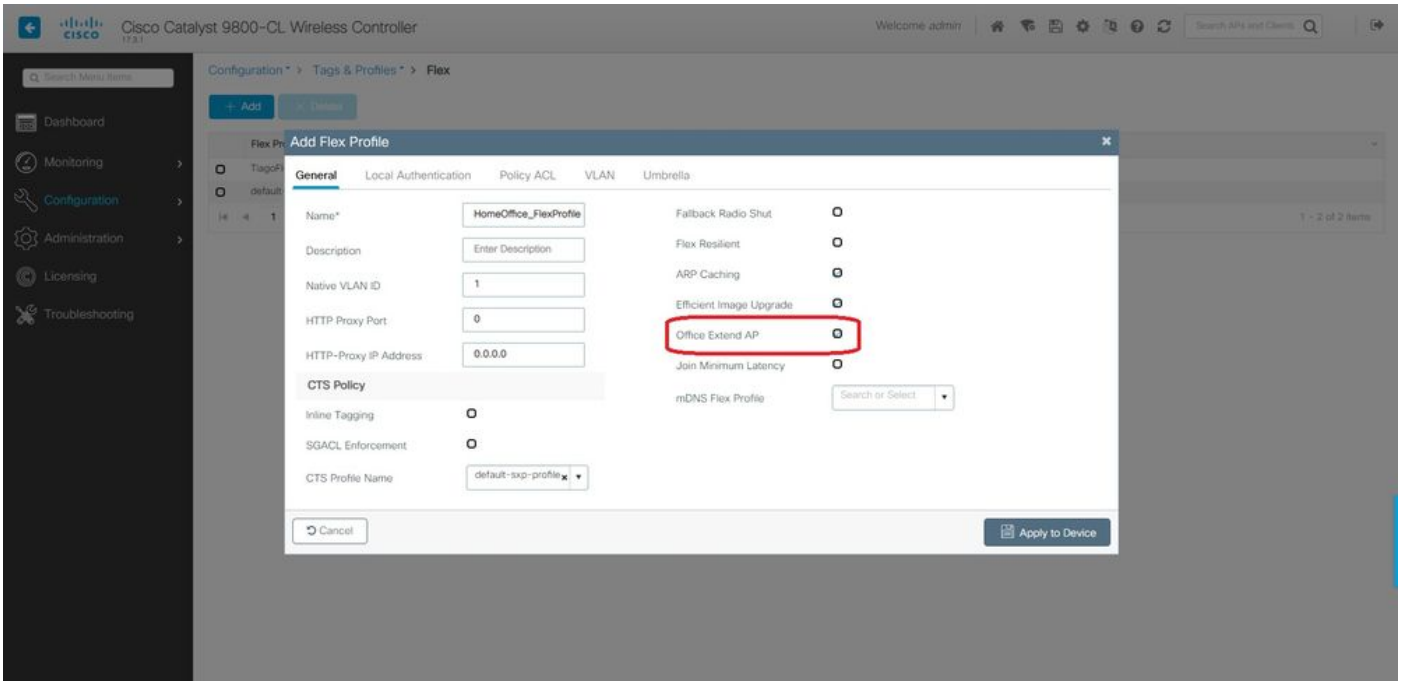


Collegamento di un criterio ACL all'ACL definito

Passaggio 1. Creare un nuovo profilo Flex. Andare a Configurazione > Tag e profili > Flex.

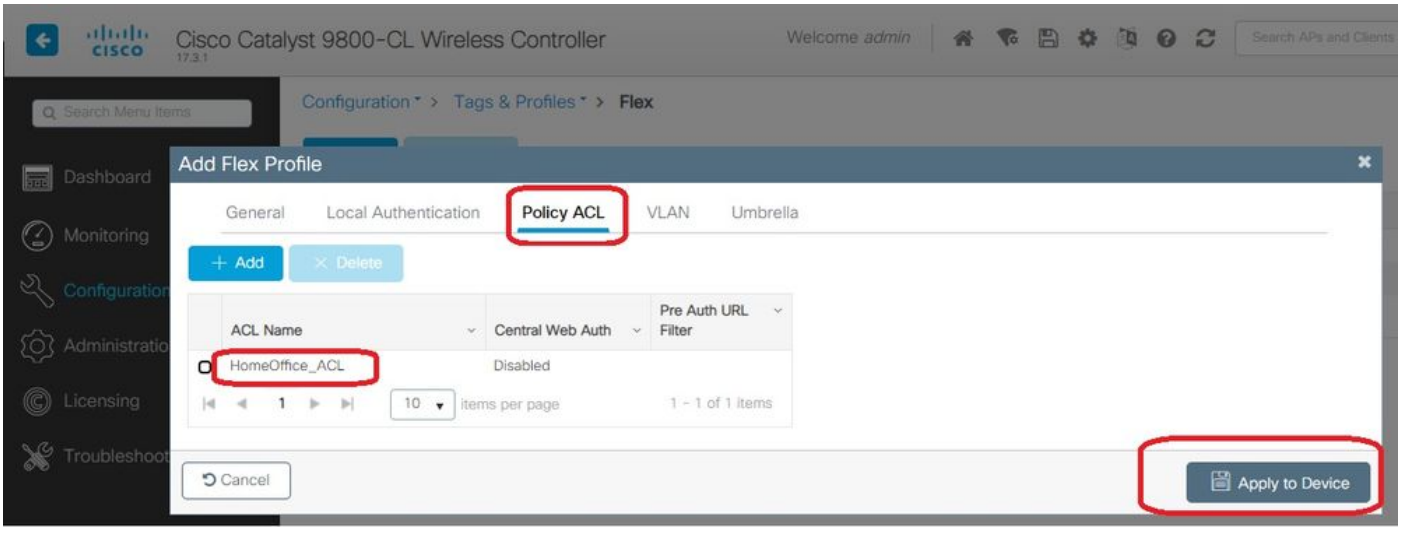
selezionare Aggiungi.

Passaggio 2. Inserire un nome e abilitare OEAP. Inoltre, verificare che l'ID della VLAN nativa sia quello indicato sulla porta dello switch AP.



> **Nota:** Quando si attiva la modalità Office-Extend, anche la crittografia del collegamento viene attivata per impostazione predefinita e non può essere modificata anche se si disattiva la crittografia del collegamento nel profilo di join AP.

Passaggio 3. Passare alla scheda ACL criterio e selezionare Aggiungi. Aggiungere qui l'ACL al profilo e applicarlo al dispositivo.

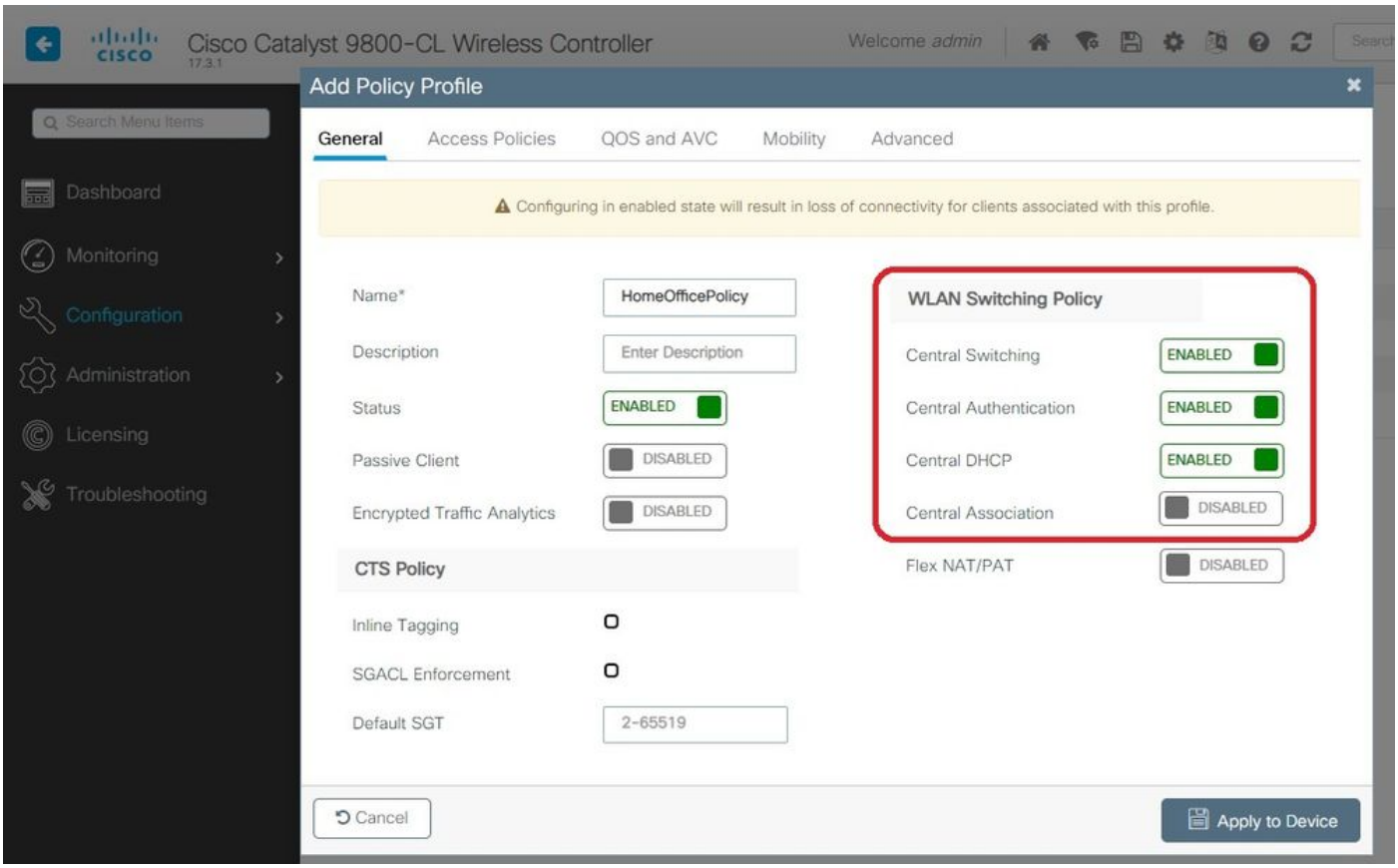


Configurazione di un criterio di profilo wireless e di un nome ACL MAC diviso

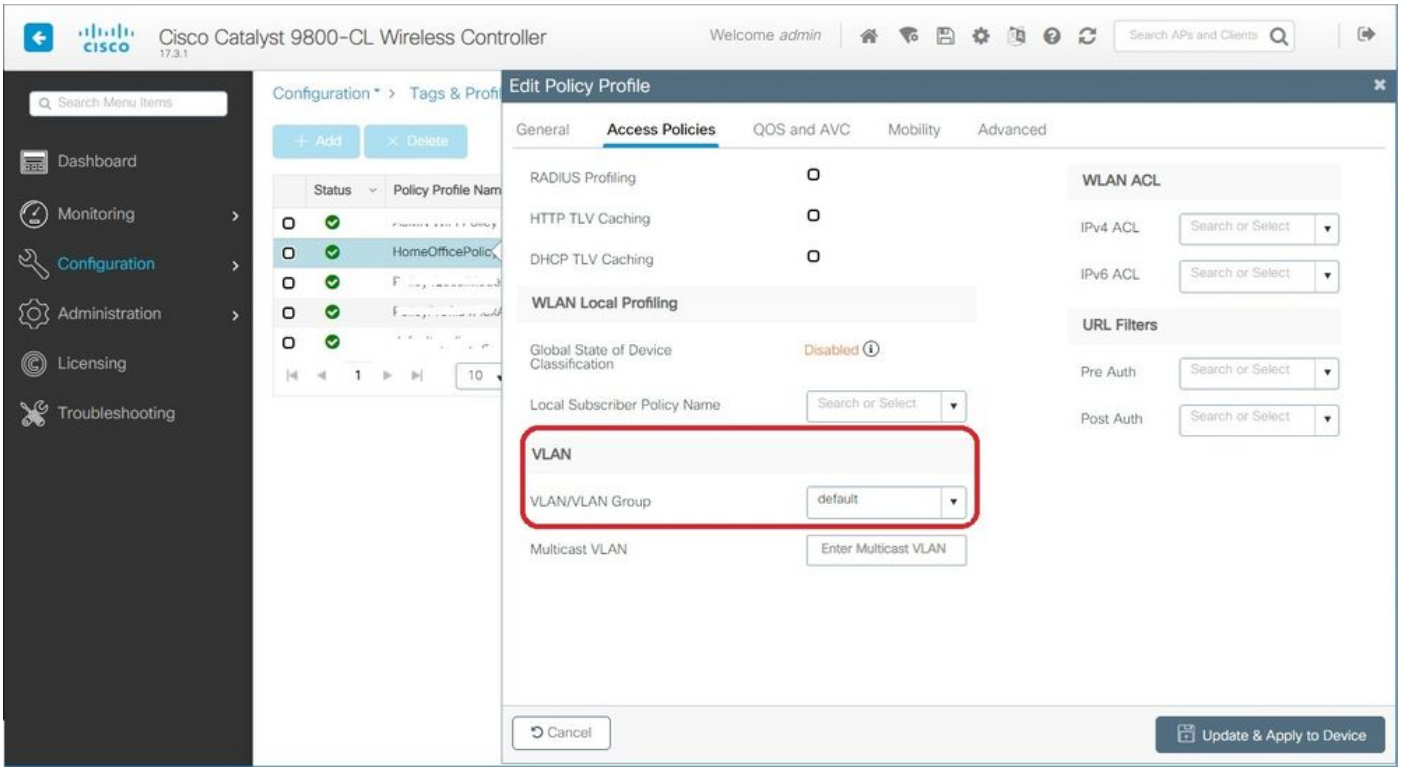
Passaggio 1. Creare un profilo WLAN. In questo esempio viene utilizzato un SSID denominato HomeOffice con protezione WPA2-PSK.

Passaggio 2. Creare un profilo criteri. Andare a Configurazione > Tag > Criterio e selezionare

Aggiungi. In Generale, assicurarsi che questo profilo sia centralizzato, come mostrato nell'esempio:

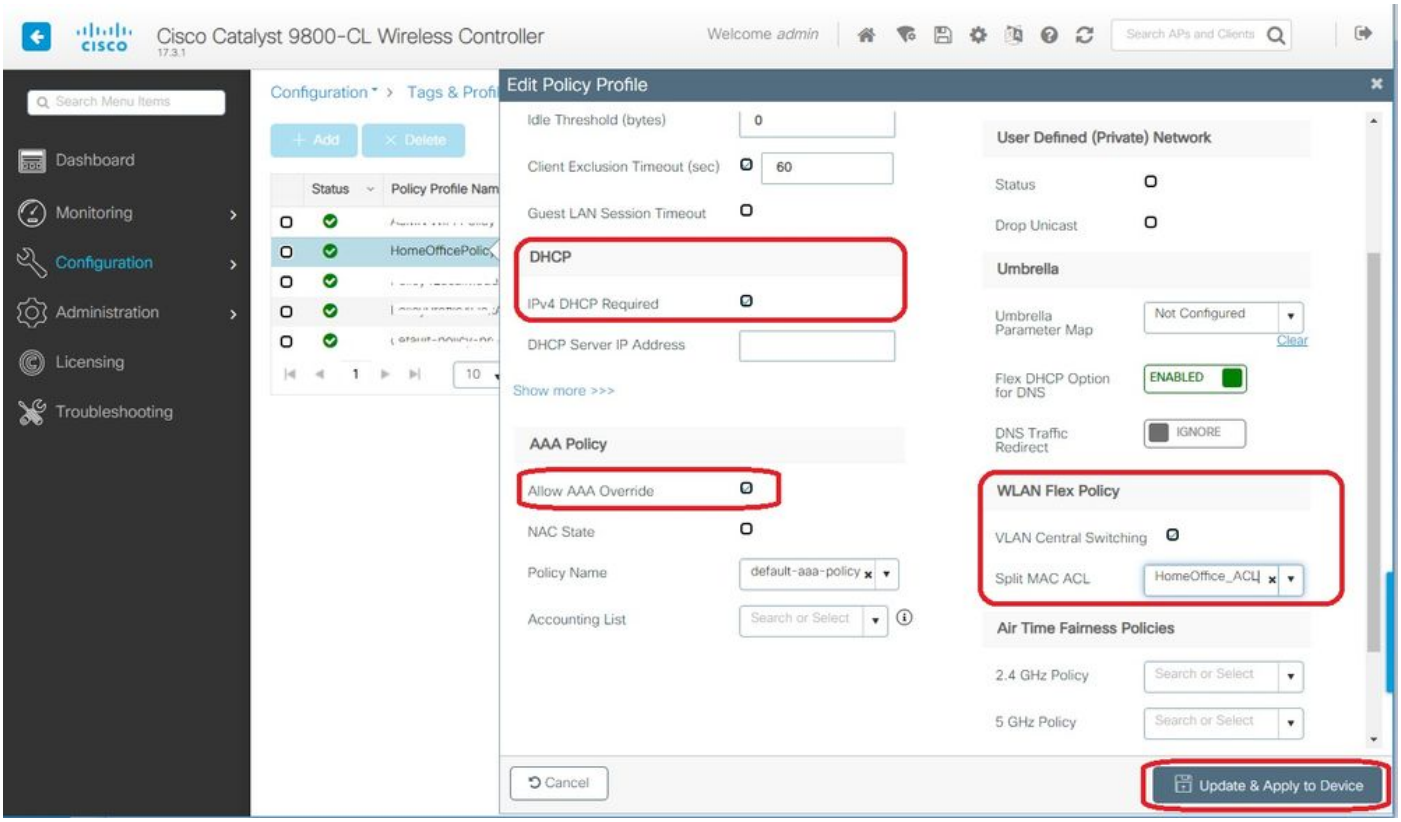


Passaggio 3. All'interno del profilo della policy, accedere a Policy di accesso e definire la VLAN per il traffico da commutare centralmente. I client ricevono un indirizzo IP nella subnet assegnata a questa VLAN.



Passaggio 4. Per configurare il tunneling con split locale su un access point, è necessario

verificare che il protocollo DCHP richiesto sia stato abilitato sulla WLAN. In questo modo, il client che si sta associando alla WLAN suddivisa non eseguirà il DHCP. È possibile attivare questa opzione nella scheda Profilo criterio in Avanzate. Selezionare la casella di controllo DHCP IPv4 richiesto. Nelle impostazioni dei criteri Flex della WLAN, selezionare l'ACL MAC suddiviso creato in precedenza dall'elenco a discesa ACL MAC suddiviso. Selezionare Applica a dispositivo:



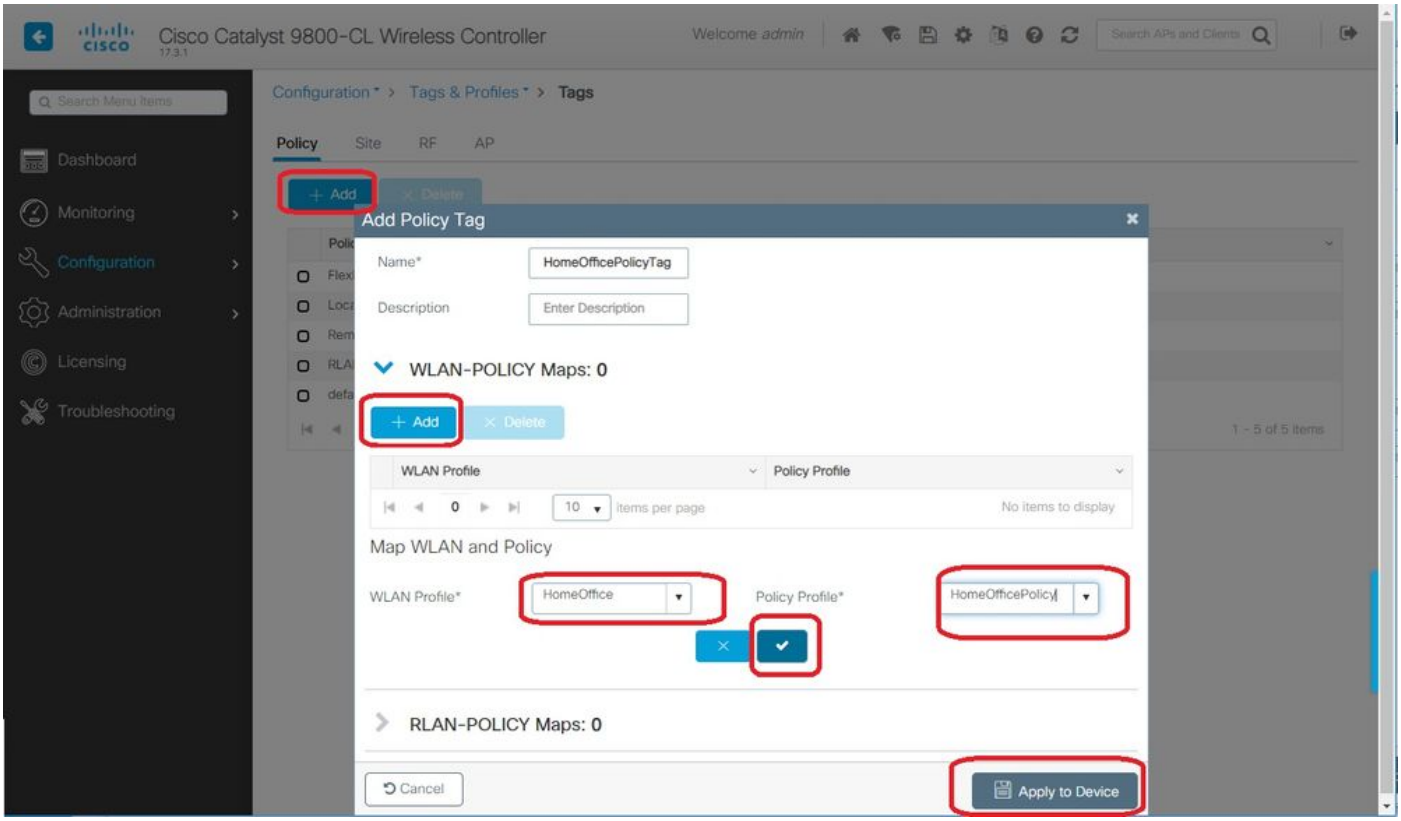
Nota: Affinché il tunneling suddiviso funzioni, i client Apple iOS devono impostare l'opzione 6 (DNS) nell'offerta DHCP.

Mappatura di una WLAN a un profilo delle policy

Passaggio 1. Scegliere Configurazione > Tag e profili > Tag. Nella scheda Criterio selezionare Aggiungi.

Passaggio 2. Immettere il nome del Tag Policy e in WLAN-POLICY Maps scheda, selezionare Add.

Passaggio 3. Selezionare il profilo WLAN dall'elenco a discesa Profilo WLAN e scegliere il profilo Policy dall'elenco a discesa Profilo policy. Selezionare l'icona Tick, quindi Applica al dispositivo.

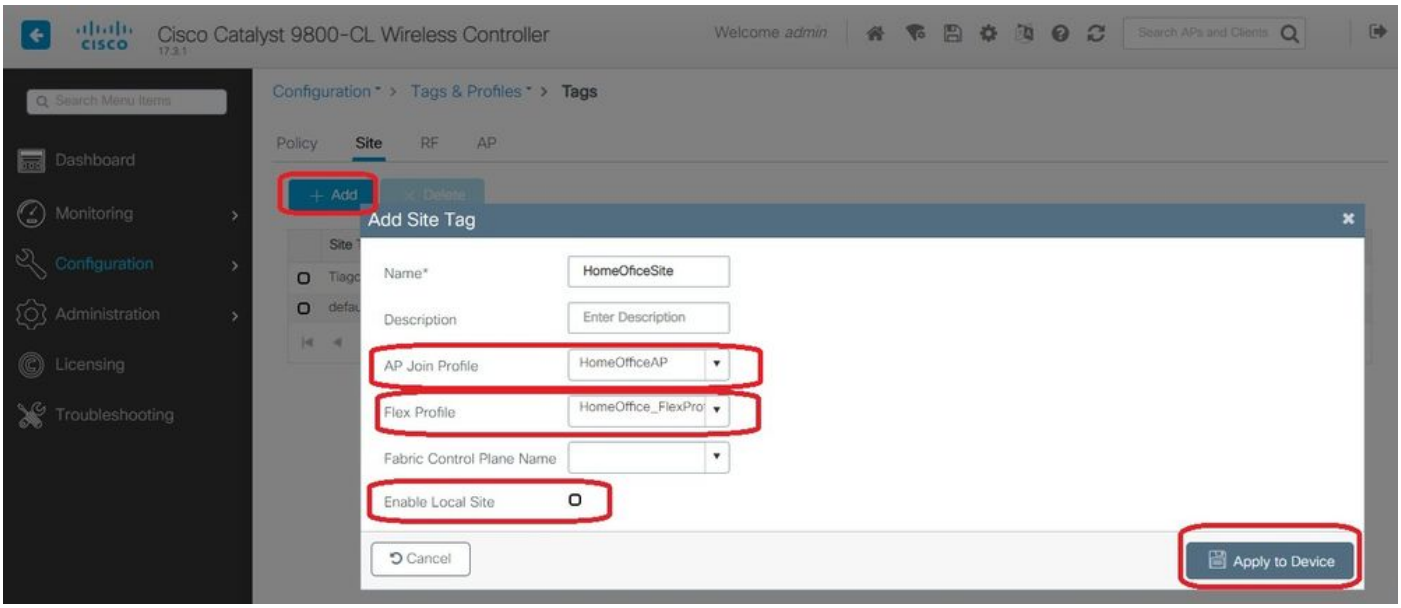


Configurazione di un profilo di aggiunta AP e associazione con il tag del sito

Passaggio 1. Passare a Configurazione > Tag e profili > AP Join e selezionare Aggiungi. Inserire un nome. È possibile abilitare il protocollo SSH per consentire la risoluzione dei problemi e disabilitarlo in seguito, se non necessario.

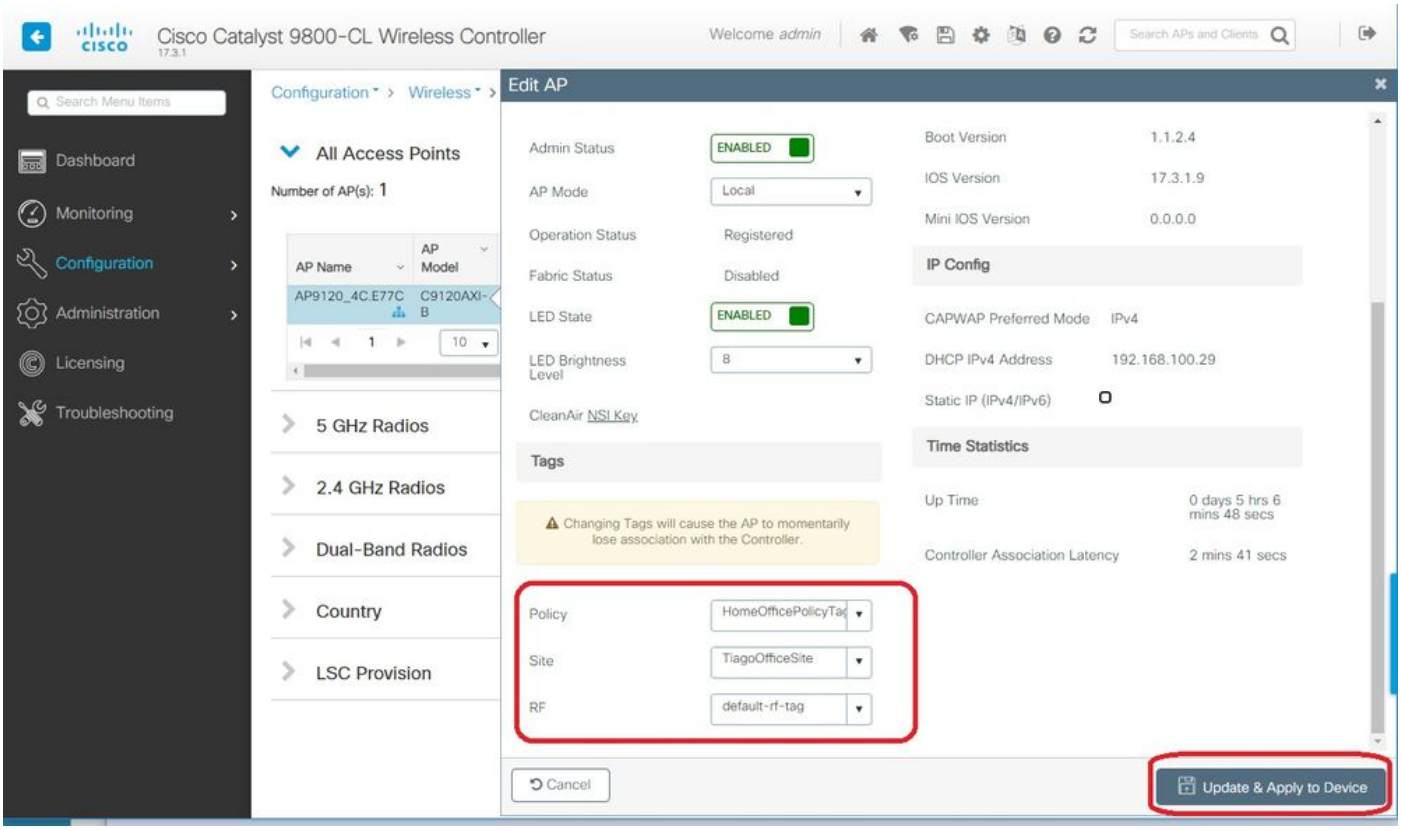
Passaggio 2. Scegliere Configurazione > Tag e profili > Tag. Nella scheda Sito selezionare Aggiungi.

Passaggio 3. Inserire il nome del tag della sede, deselezionare Abilita sede locale, quindi selezionare Profilo di aggiunta AP e Profilo flessibile (creato in precedenza) dagli elenchi a discesa. Quindi Applica al dispositivo.

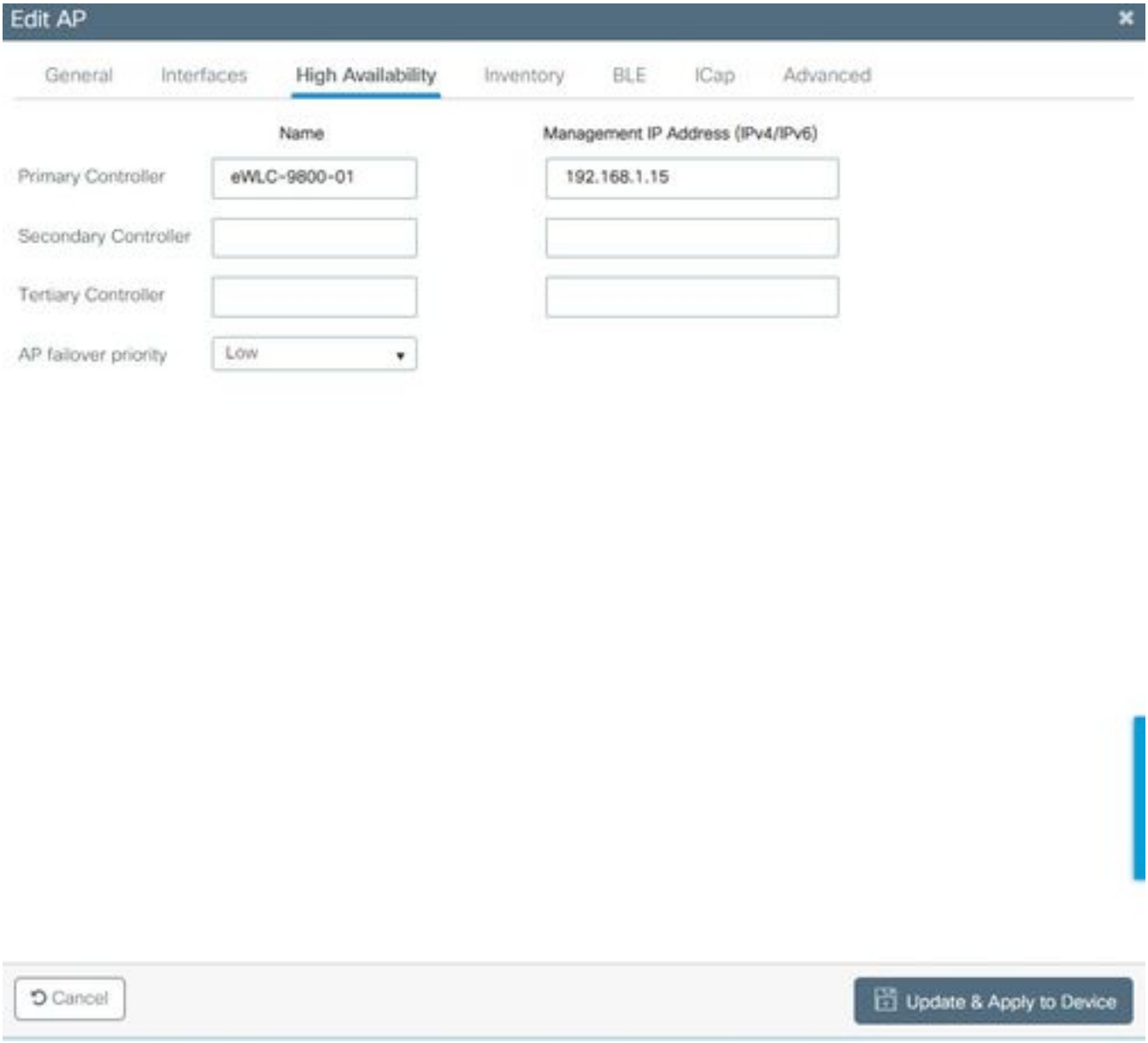


Associazione di un tag di criteri e di siti a un punto di accesso

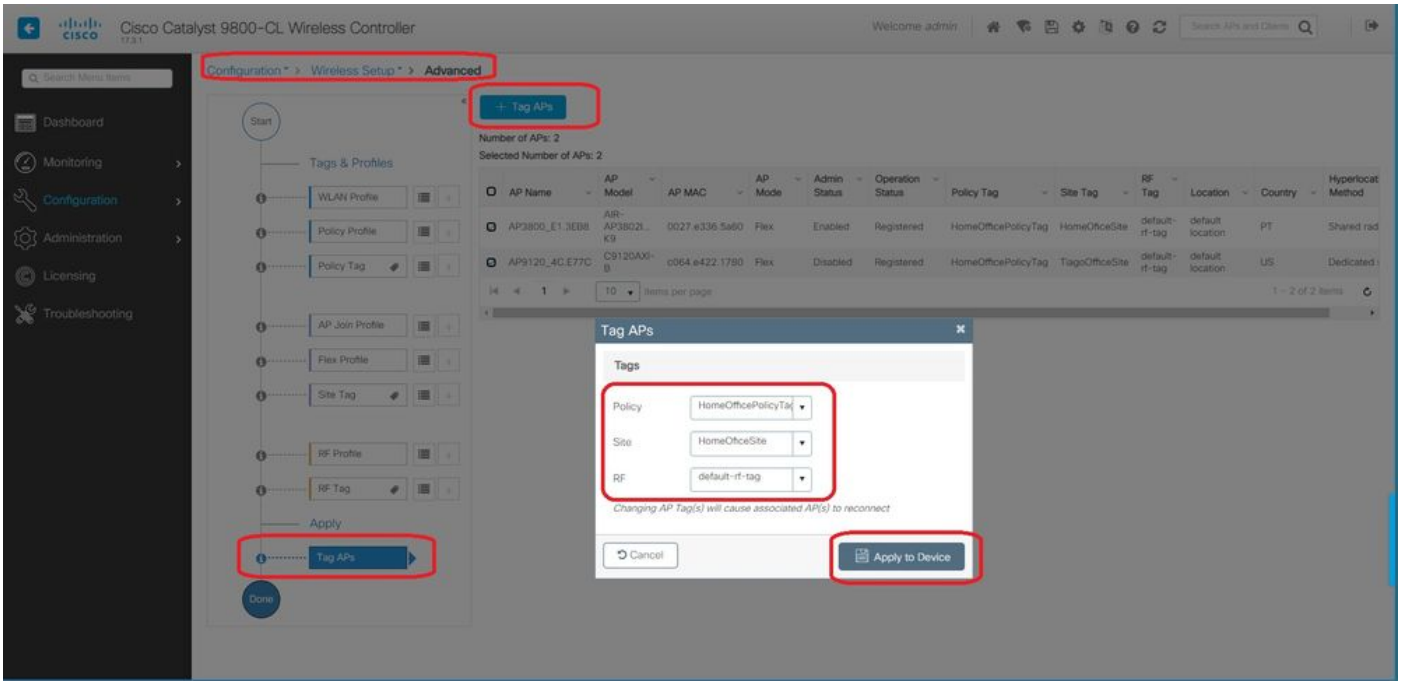
Opzione 1. Questa opzione richiede la configurazione di 1 access point alla volta. Andare a Configurazione > Wireless > Access Point. Selezionare il punto di accesso che si desidera spostare nella home office, quindi selezionare i tag della home office. Selezionare Aggiorna e Applica al dispositivo:



Si consiglia inoltre di configurare un controller primario in modo che l'access point conosca l'IP/il nome del WLC da raggiungere una volta distribuito nell'home office. A tale scopo, è possibile modificare il punto di accesso passando direttamente alla scheda Alta disponibilità:



Opzione 2. Questa opzione consente di configurare più access point contemporaneamente. Selezionare Configurazione > Wireless Setup > Avanzate > Tag AP. Selezionare le etichette create in precedenza e scegliere Applica a dispositivo.



Gli AP si riavviano e si uniscono nuovamente al WLC con le nuove impostazioni.

Verifica

Èpossibile verificare la configurazione tramite GUI o CLI. Questa è la configurazione risultante nella 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
!
```

Controllo configurazione punto di accesso:

```
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
...
```

Èpossibile connettersi direttamente all'access point e verificare la configurazione:

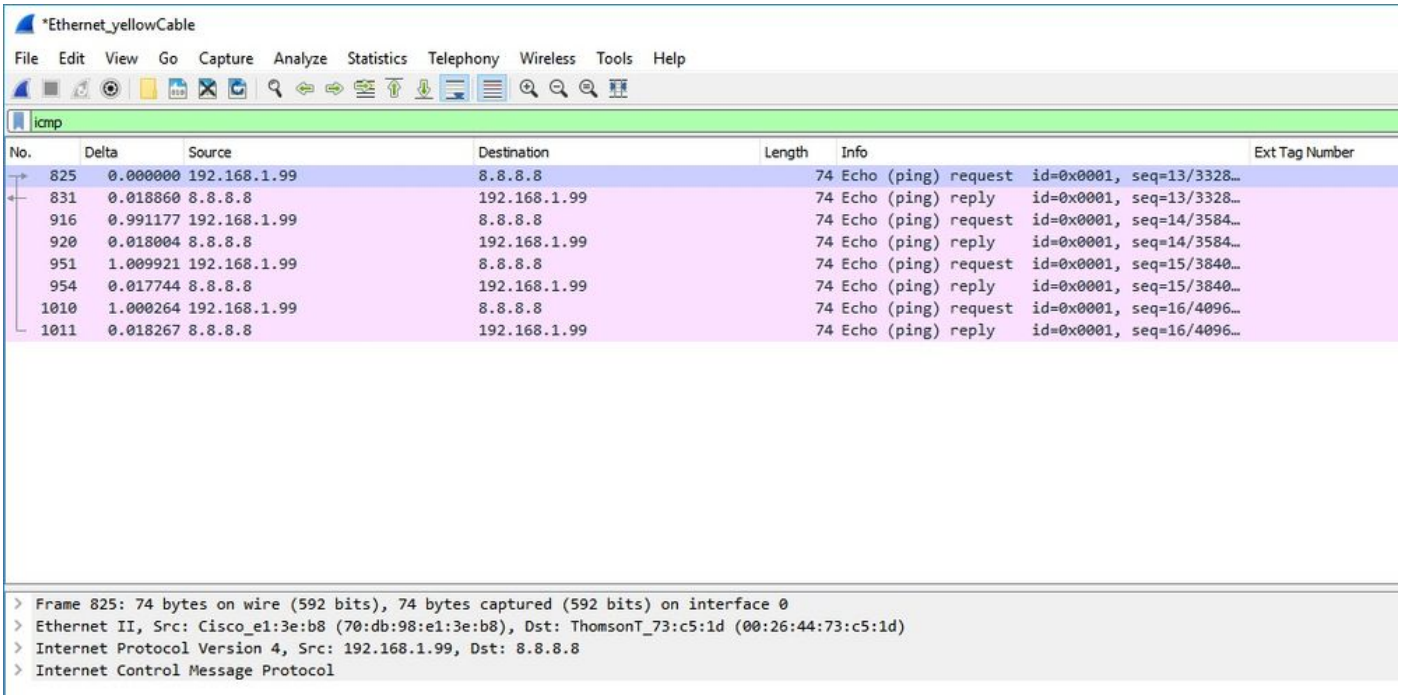
```
AP3800_E1.3EB8#show ip access-lists
Extended IP access list HomeOffice_ACL
1 deny ip any 192.168.1.0 0.0.0.255
2 permit ip any any

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
...
```

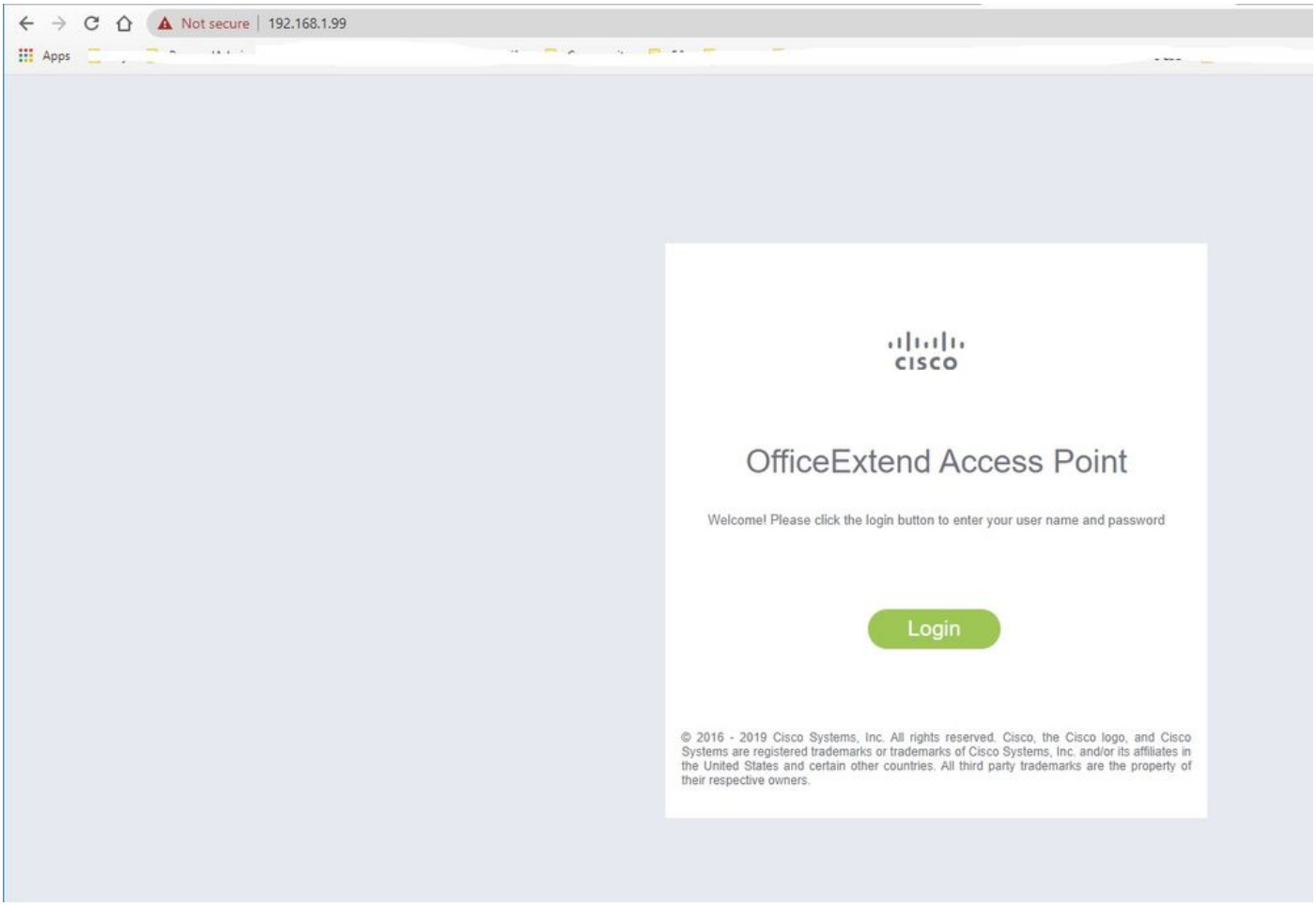
```
AP3800_E1.3EB8#show capwap client config
AdminState : ADMIN_ENABLED(1)
Name : AP3800_E1.3EB8
Location : default location
Primary controller name : eWLC-9800-01
Primary controller IP : 192.168.1.15
Secondary controller name : c3504-01
Secondary controller IP : 192.168.1.14
Tertiary controller name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

Di seguito è riportato un esempio di acquisizioni di pacchetti che mostrano il traffico modificato localmente. Il test è stato eseguito effettuando un "ping" tra un client con IP 192.168.1.98 e il server DNS Google, quindi 192.168.1.254. L'ICMP ha origine con l'IP dell'indirizzo IP dell'access point 192.168.1.99 inviato al DNS Google a causa del NAT dell'access point che gestisce il traffico a livello locale. Non è disponibile alcun protocollo icmp per 192.168.1.254 in quanto il traffico viene crittografato nel tunnel DTLS e vengono visualizzati solo i frame dati dell'applicazione.

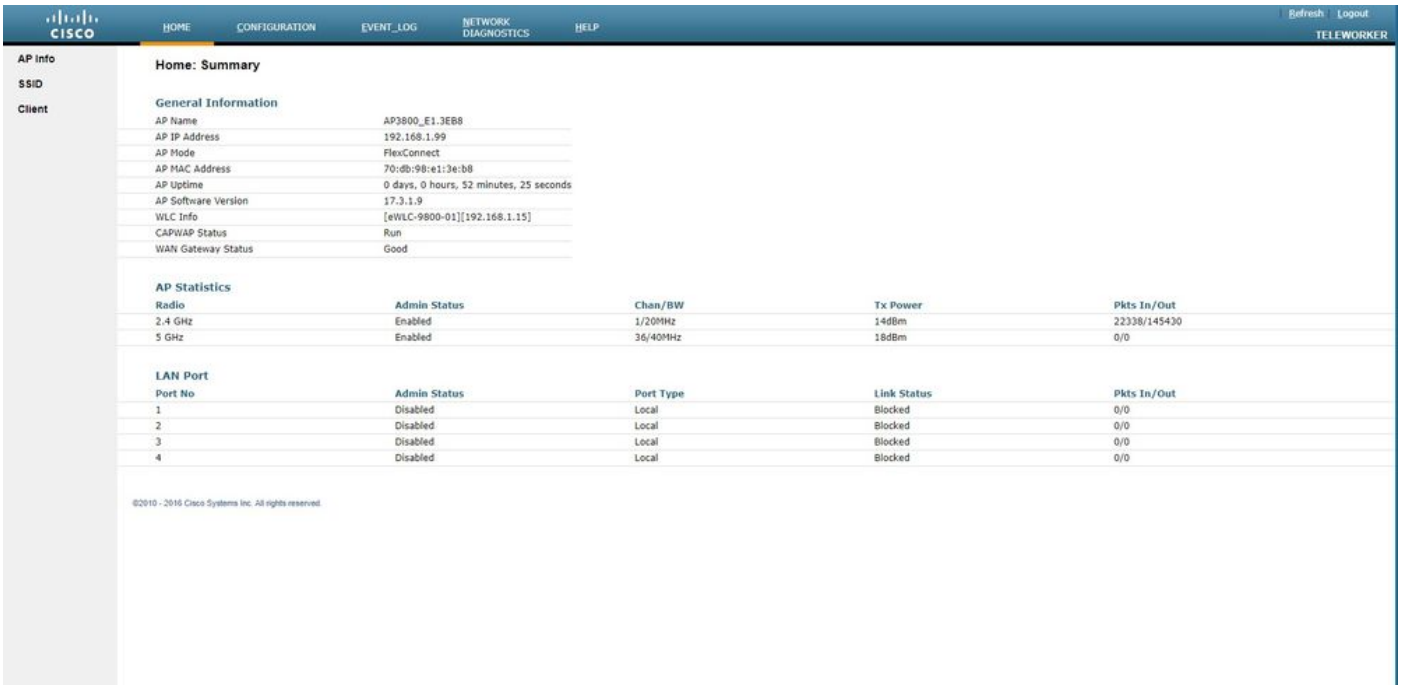


> **Nota:** Il traffico che viene commutato localmente è NAT dal punto di accesso perché in scenari normali, la subnet client appartiene alla rete Office e i dispositivi locali dell'ufficio domestico non sanno come raggiungere la subnet client. Il punto di accesso converte il traffico del client utilizzando l'indirizzo IP del punto di accesso che si trova nella subnet dell'ufficio locale.

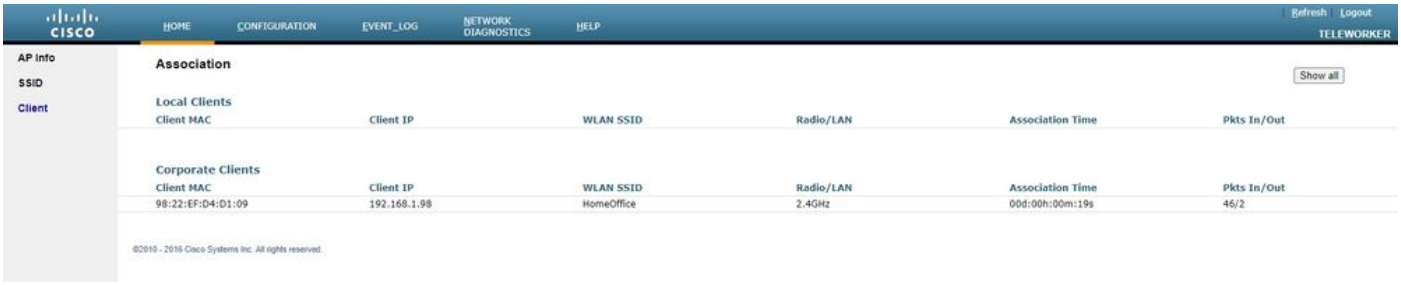
Èpossibile accedere alla GUI OEAP aprendo un browser e digitando nell'URL l'indirizzo IP dell'access point. Le credenziali predefinite sono admin/admin ed è necessario modificarle all'accesso iniziale.



Dopo aver effettuato l'accesso, è possibile accedere alla GUI:



Èpossibile accedere alle informazioni tipiche di un OEAP, come le informazioni dell'access point, gli SSID e i client connessi:



Documentazione correlata

Informazioni su FlexConnect su Catalyst 9800 Wireless Controller

Tunneling ripartito per FlexConnect

Configurazione di OEAP e RLAN su Catalyst 9800 WLC