

設定Catalyst 9800和FlexConnect OEAP分割通道

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[概觀](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[組態](#)

[定義分割隧道的訪問控制清單](#)

[將ACL策略連結到已定義的ACL](#)

[配置無線配置檔案策略和拆分MAC ACL名稱](#)

[將WLAN對映到策略配置檔案](#)

[配置AP加入配置檔案以及與站點標籤的關聯](#)

[將策略標籤和站點標籤附加到接入點](#)

[驗證](#)

[相關檔案](#)

簡介

本文說明如何將室記憶體取點(AP)設定為FlexConnect Office Extend(OEAP)，以及如何啟用分割通道，以便您可以定義哪些流量可以在總部本地交換，哪些流量必須在WLC集中交換。

必要條件

需求

本檔案中的組態假設已在DMZ中啟用NAT設定WLC，且AP可從總部加入WLC。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行Cisco IOS-XE 17.3.1軟體的無線LAN控制器9800。
- Wave1 AP:1700/2700/3700 .
- Wave2 AP:1800/2800/3800/4800和Catalyst 9100系列。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

概觀

Cisco OfficeExtend接入點(Cisco OEAP)提供從Cisco WLC到遠端位置的Cisco AP的安全通訊，從而通過網際網路將公司WLAN無縫擴展到員工的住所。使用者在家庭辦公室中的體驗與在公司辦公室中的體驗完全相同。接入點和控制器之間的資料包傳輸層安全(DTLS)加密可確保所有通訊具有最高級別的安全性。FlexConnect模式下的任何室內AP都可以充當OEAP。

背景資訊

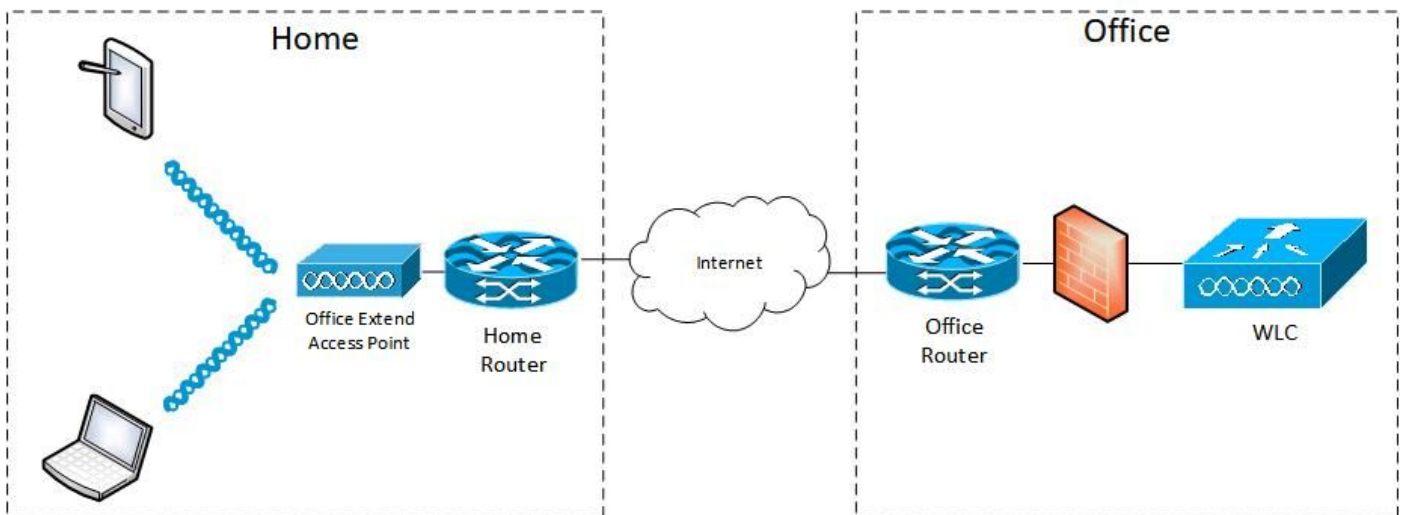
FlexConnect指接入點(AP)在遠端位置（例如，通過WAN）運行時處理無線客戶端的能力。他們還可以決定來自無線客戶端的流量是直接放在AP級別的網路上（本地交換），還是根據WLAN將流量集中到9800控制器（中央交換）並通過WAN傳送回。

有關FlexConnect的詳細資訊，請檢查[瞭解Catalyst 9800無線控制器上的FlexConnect](#)文檔。

OEAP模式是FlexConnect AP中提供的一種選項，用於允許使用其他功能，例如用於家庭接入的個人本地SSID，還可以提供分割隧道功能，從而更加精細地定義必須在家庭辦公室本地交換的流量和必須在單個WLAN上在WLC集中交換的流量

設定

網路圖表



組態

定義分割隧道的訪問控制清單

步驟1.選擇Configuration > Security > ACL。選擇新增。

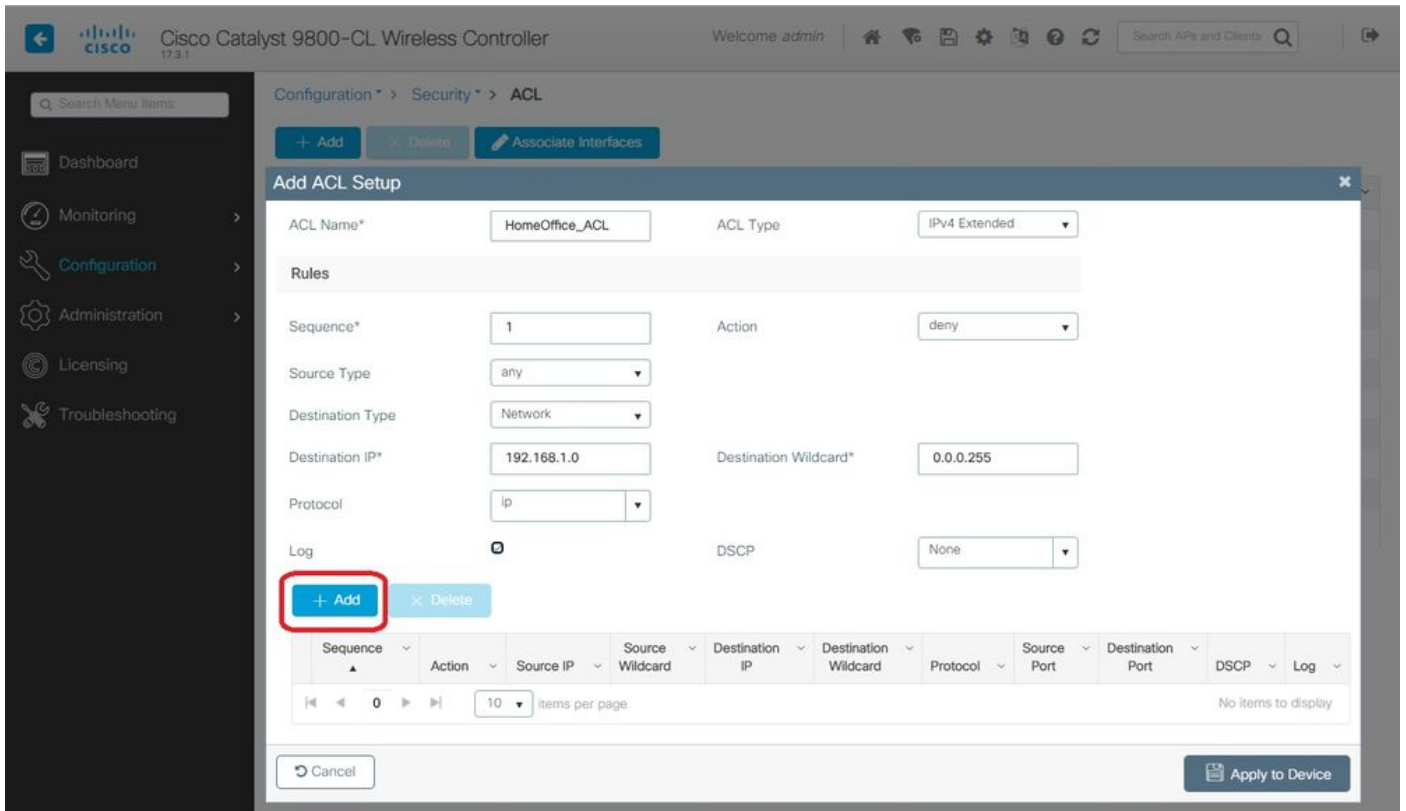
步驟2.在新增ACL設定對話方塊中，輸入ACL名稱，從ACL型別下拉選單中選擇ACL型別，並在Rules設定下輸入序列號。然後選擇「操作」作為「允許」或「拒絕」。

步驟3.從「來源型別」下拉式清單選擇所需的來源型別。

如果選擇源型別為主機，則必須輸入主機名/IP。

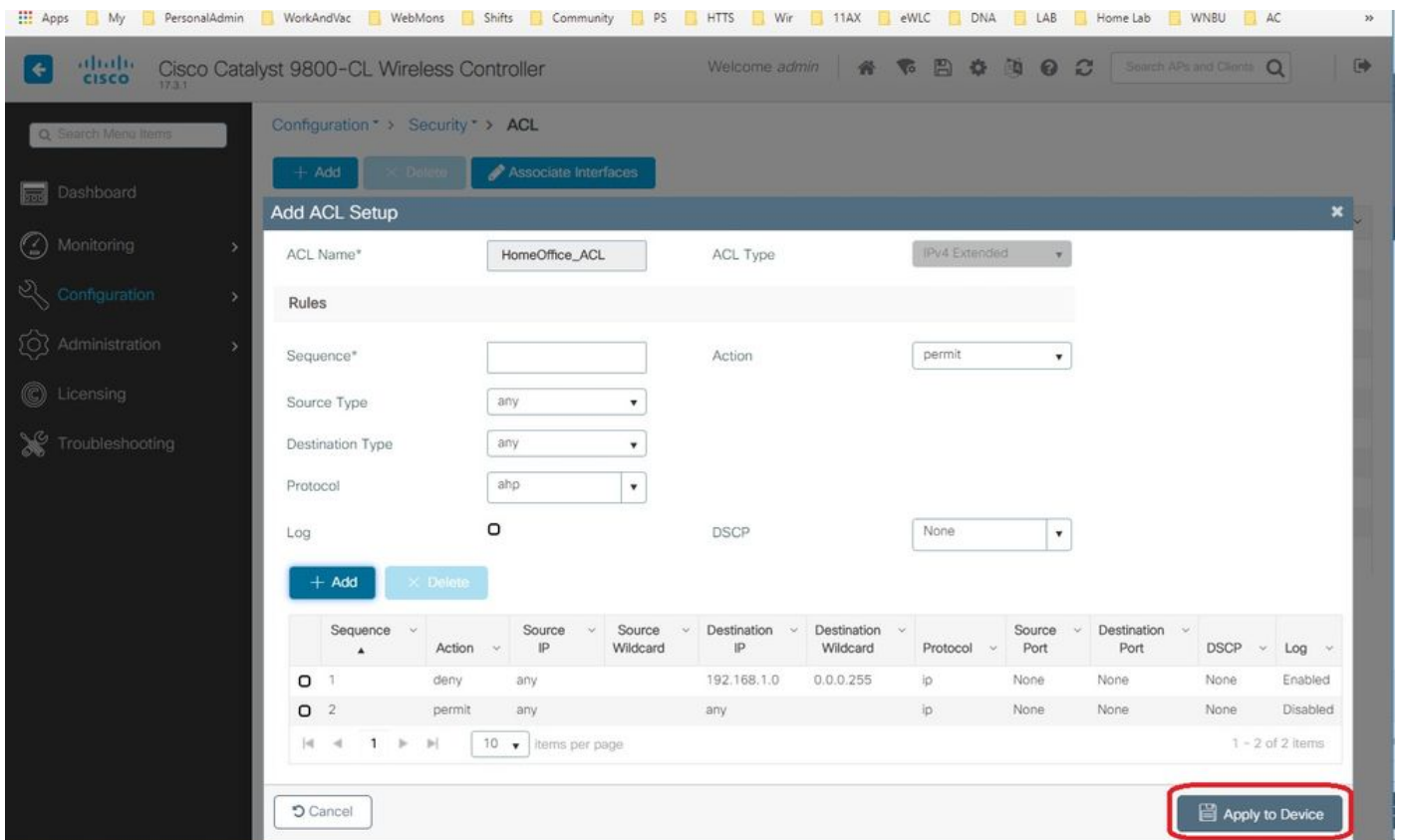
如果選擇源型別為網路，則必須指定源IP地址和源萬用字元掩碼。

在本示例中，從任何主機到子網192.168.1.0/24的所有流量都集中交換（拒絕），而其餘所有流量則本地交換（允許）。



步驟4.如果想要日誌，請選中Log覈取方塊，然後選擇Add。

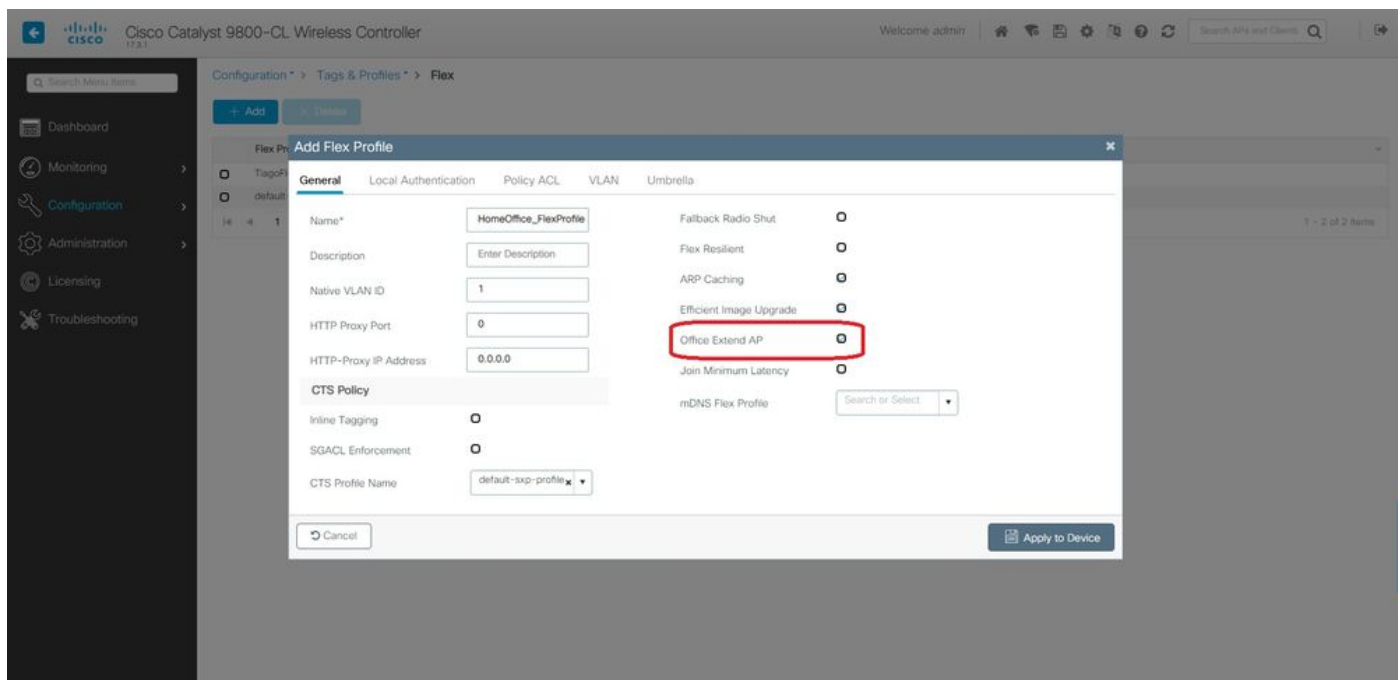
步驟5.新增其餘規則並選擇Apply to Device。



將ACL策略連結到已定義的ACL

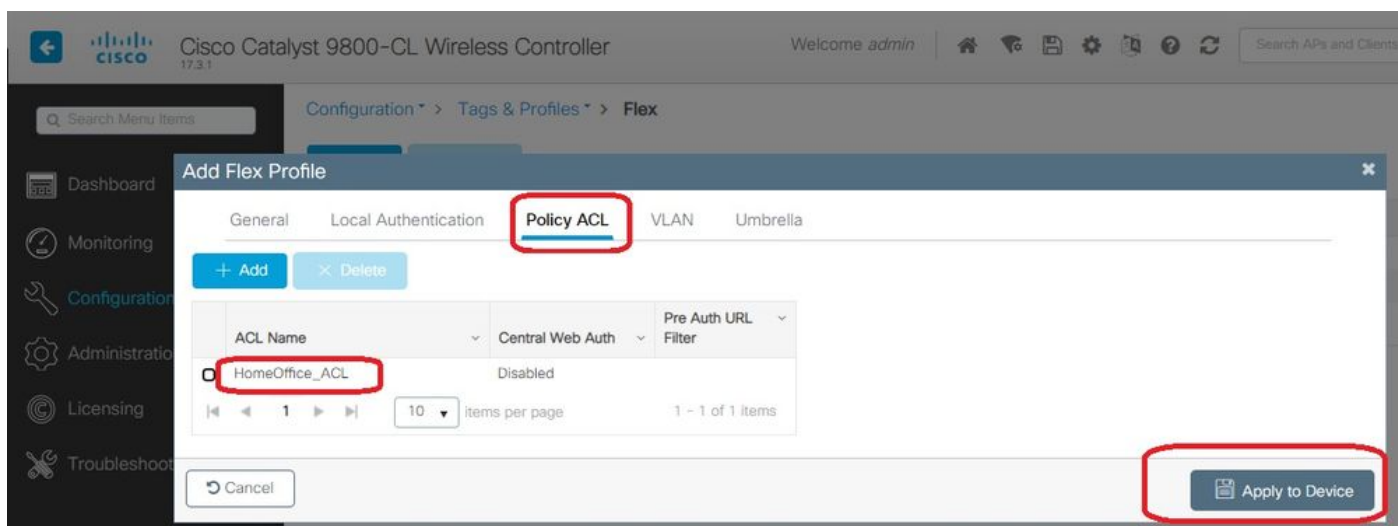
步驟1.建立新的Flex配置檔案。轉至Configuration > Tags & Profiles > Flex。選擇新增。

步驟2.輸入名稱並啟用OEAP。此外，請確保本徵VLAN ID是AP交換機埠中的VLAN ID。



附註：啟用Office-Extend模式時，預設情況下也會啟用鏈路加密，即使在AP加入配置檔案中禁用鏈路加密也無法更改。

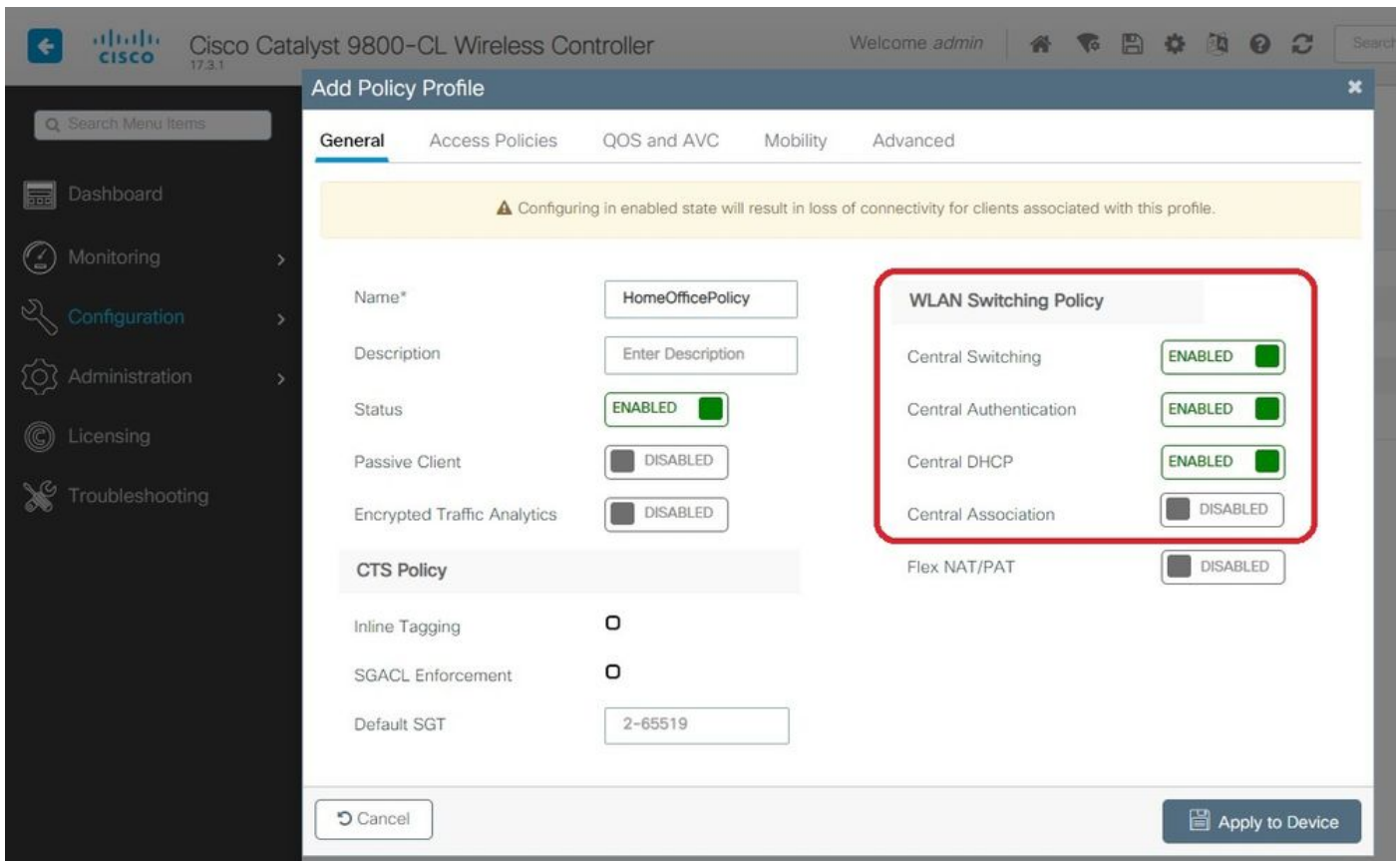
步驟3.轉到Policy ACL頁籤並選擇Add。此處將ACL新增到配置檔案並應用到裝置。



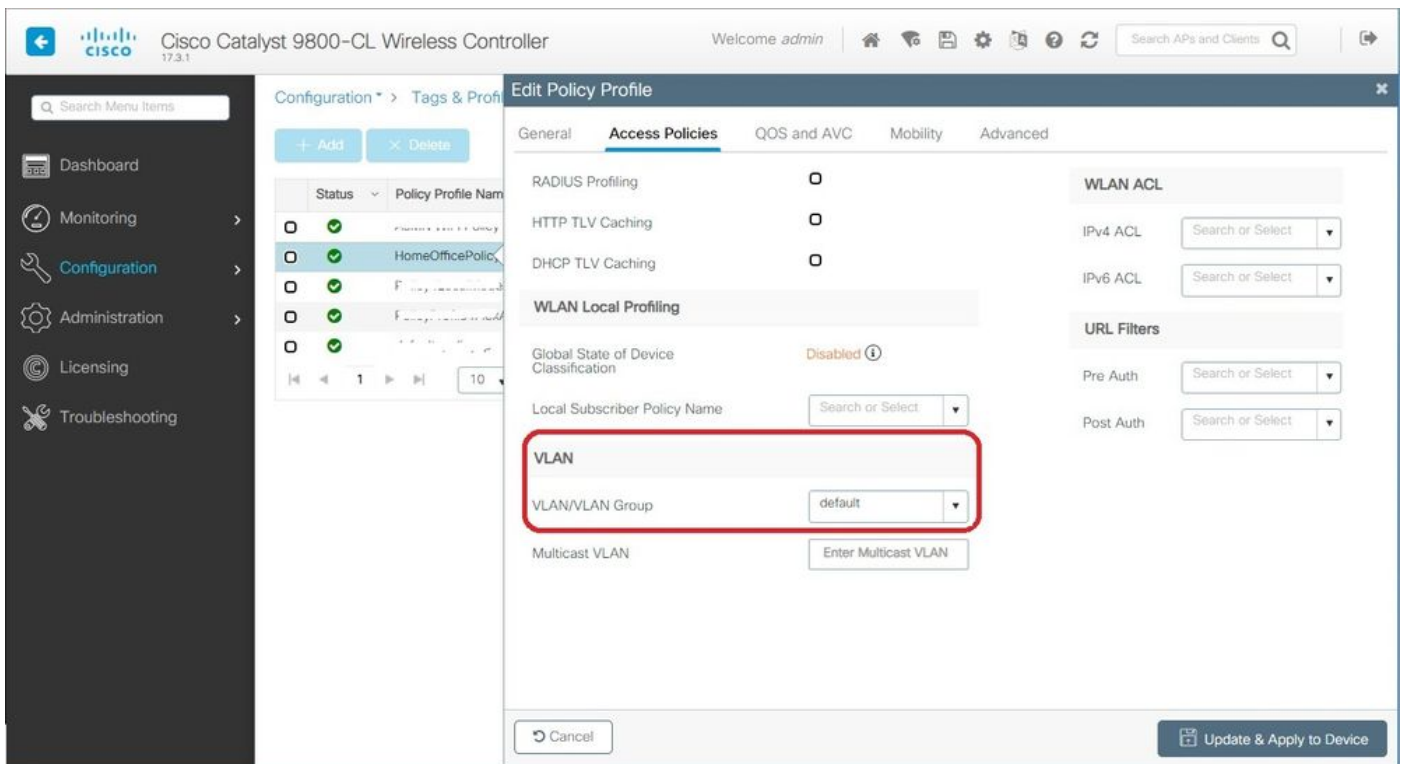
配置無線配置檔案策略和拆分MAC ACL名稱

步驟1.建立WLAN設定檔。在本示例中，它使用名為HomeOffice的SSID和WPA2-PSK安全性。

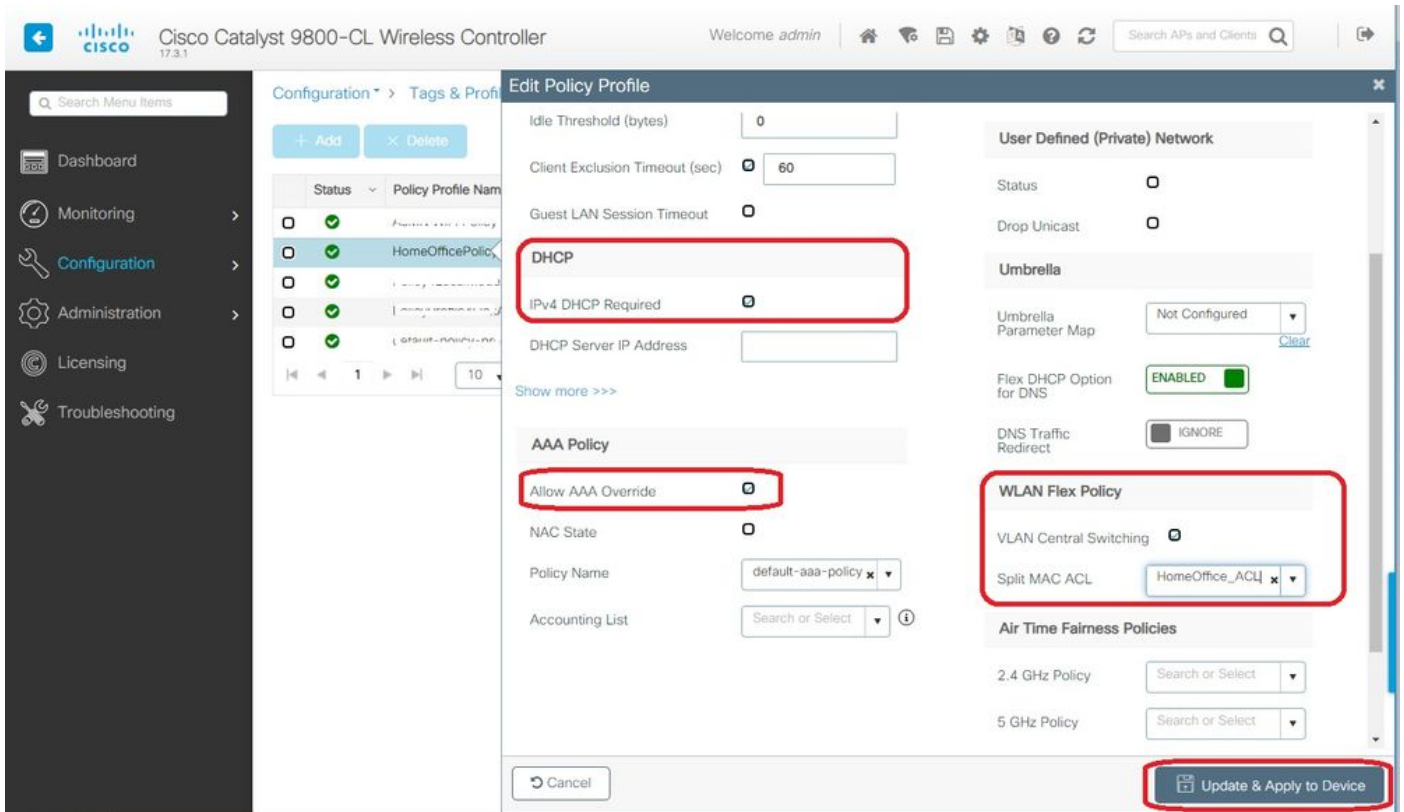
步驟2.建立策略配置檔案。轉至Configuration > Tags > Policy,然後選擇Add。在General下，確保此配置檔案是集中交換的策略，如以下示例所示：



步驟3.在Policy Profile中，轉至Access Policies並為要集中交換的流量定義VLAN。使用者端會取得指定給此VLAN的子網中的IP位址。



步驟4.要在AP上配置本地拆分隧道，需要確保在WLAN上啟用了DCHP Required。這可確保與拆分WLAN關聯的客戶端執行DHCP。您可以在Advanced頁籤下的Policy Profile中啟用此選項。啟用覈取方塊IPv4 DHCP Required。在WLAN Flex Policy設定下，從Split MAC ACL下拉選單中選擇之前建立的拆分MAC ACL。選擇應用到裝置：



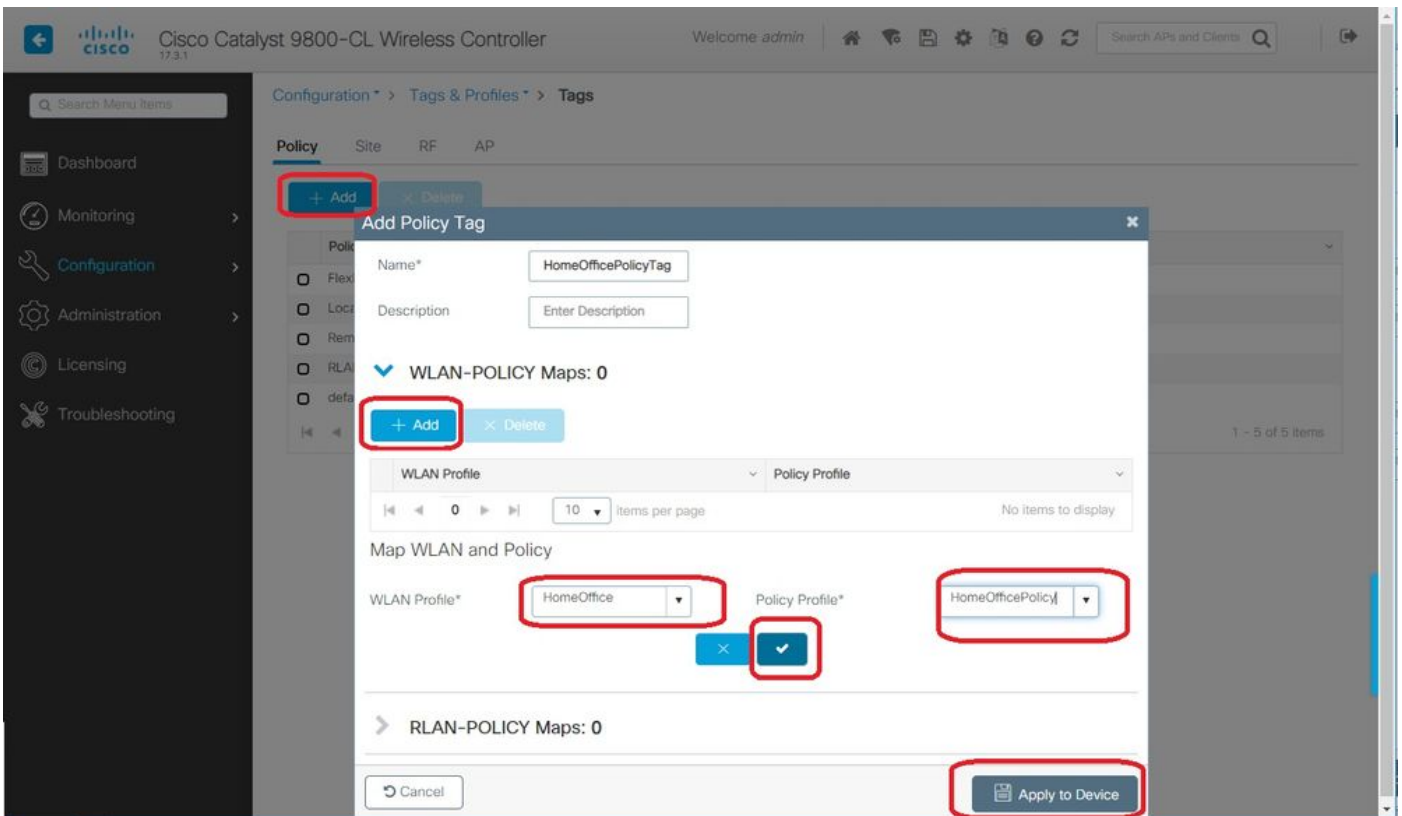
附註：Apple iOS客戶端需要在DHCP提供中設定選項6(DNS)，以便分割隧道正常工作。

將WLAN對映到策略配置檔案

步驟1.選擇Configuration > Tags & Profiles > Tags。在Policy頁籤中選擇Add。

步驟2.輸入標籤策略的名稱，然後在WLAN-POLICY Maps頁籤下選擇Add。

步驟3.從WLAN Profile下拉選單中選擇WLAN profile，然後從Policy Profile下拉選單中選擇Policy profile。選擇勾選圖示，然後選擇應用到裝置。

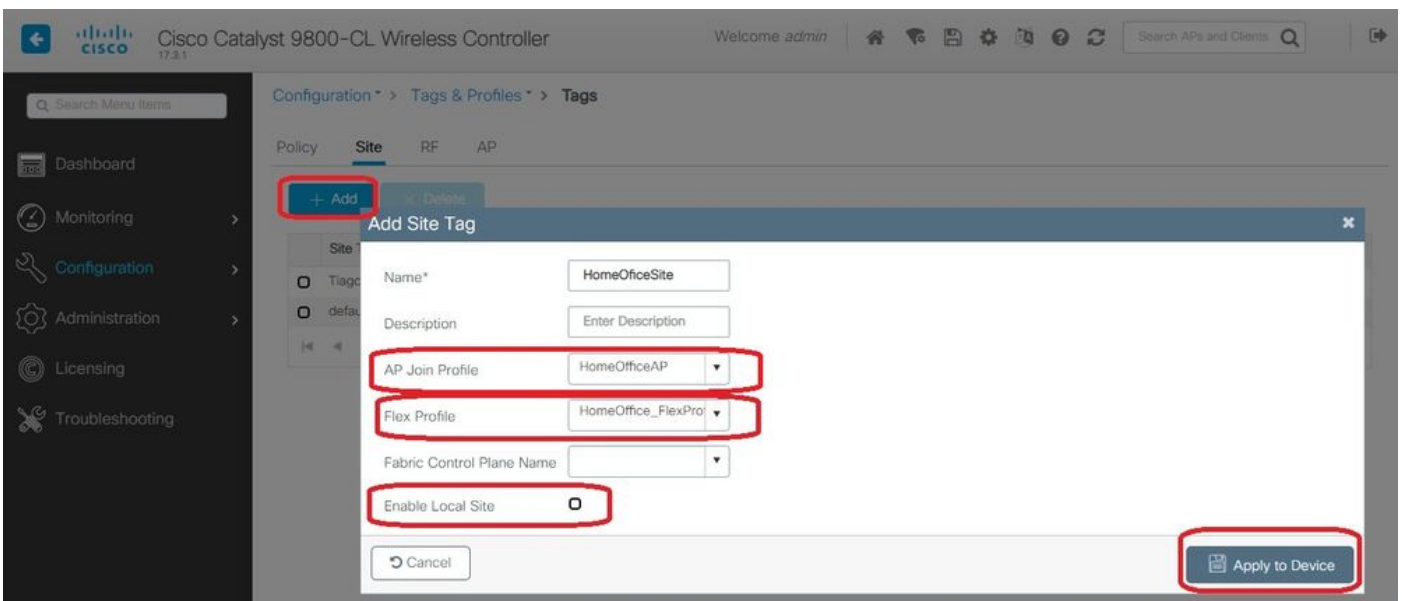


配置AP加入配置檔案以及與站點標籤的關聯

步驟1. 導航到 Configuration > Tags & Profiles > AP Join 並選擇 Add。輸入名稱。或者，您可以啟用 SSH 以允許進行故障排除，並在以後不需要時將其禁用。

步驟2. 選擇 Configuration > Tags & Profiles > Tags。在「站點」頁籤中選擇「新增」。

步驟3. 輸入站點標籤的名稱，取消選中「啟用本地站點」，然後從下拉選單中選擇「AP加入配置檔案」和「Flex配置檔案」（之前建立的）。然後應用到裝置。



將策略標籤和站點標籤附加到接入點

選項1：此選項要求您一次配置1個AP。轉至 Configuration > Wireless > Access Points。選擇要移

動到家庭辦公室的AP，然後選擇家庭辦公室標籤。選擇更新並應用到裝置：

The screenshot displays the 'Edit AP' configuration page in the Cisco Catalyst 9800-CL Wireless Controller interface. The left sidebar shows navigation options like Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is divided into sections for 'All Access Points', '5 GHz Radios', '2.4 GHz Radios', 'Dual-Band Radios', 'Country', and 'LSC Provision'. The 'Edit AP' section is active, showing various settings for the selected AP (AP9120_4C.E77C, C9120AXI-B). The 'Tags' section is highlighted with a red box, showing 'Policy' set to 'HomeOfficePolicyTag', 'Site' set to 'TiagoOfficeSite', and 'RF' set to 'default-rf-tag'. A warning message states: 'Changing Tags will cause the AP to momentarily lose association with the Controller.' The 'Update & Apply to Device' button is also highlighted with a red box.

此外，還建議配置主控制器，以便AP知道WLC在部署到家庭辦公室後要訪問的IP/名稱。您可以直接將編輯的AP轉到「高可用性」頁籤：

Edit AP ✕

General
Interfaces
High Availability
Inventory
BLE
ICap
Advanced

	Name	Management IP Address (IPv4/IPv6)
Primary Controller	<input type="text" value="eWLC-9800-01"/>	<input type="text" value="192.168.1.15"/>
Secondary Controller	<input type="text"/>	<input type="text"/>
Tertiary Controller	<input type="text"/>	<input type="text"/>
AP failover priority	<input type="text" value="Low"/>	

Cancel
Update & Apply to Device

選項2：此選項允許您同時配置多個AP。導航至Configuration > Wireless Setup > Advanced > Tag APs。選擇以前建立的標籤，然後選擇「應用到裝置」。

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The breadcrumb path is Configuration > Wireless Setup > Advanced. The '+ Tag APs' button is highlighted. The table below shows the selected APs:

AP Name	AP Model	AP MAC	AP Mode	Admin Status	Operation Status	Policy Tag	Site Tag	RF Tag	Location	Country	Hyperlocat Method
AP3800_E1.3E8B	AR-AP3802-K9	0027.e336.5a60	Flex	Enabled	Registered	HomeOfficePolicyTag	HomeOfficeSite	default-rf-tag	default location	PT	Shared rad
AP9120_4C.E77C	C9120AXI-B	c064.e422.1780	Flex	Disabled	Registered	HomeOfficePolicyTag	TagsOfficeSite	default-rf-tag	default location	US	Dedicated

The 'Tag APs' modal window is open, showing the following configuration:

- Policy: HomeOfficePolicyTag
- Site: HomeOfficeSite
- RF: default-rf-tag

The 'Apply to Device' button is highlighted.

AP重新啟動並使用新設定重新加入WLC。

驗證

您可以通過GUI或CLI驗證設定。這是CLI中的結果配置：

```
!  
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 HomeOfficeSite  
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 xxxxxxxx  
no security wpa akm dot1x  
security wpa akm psk  
no shutdown  
!  
ap 70db.98e1.3eb8  
policy-tag HomeOfficePolicyTag  
site-tag HomeOfficeSite  
!  
ap c4f7.d54c.e77c  
policy-tag HomeOfficePolicyTag  
site-tag HomeOfficeSite  
!
```

正在檢查AP配置：

```
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 : HomeOfficeSite
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
...
```

您可以直接連線到AP，也可以驗證配置：

```
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
```

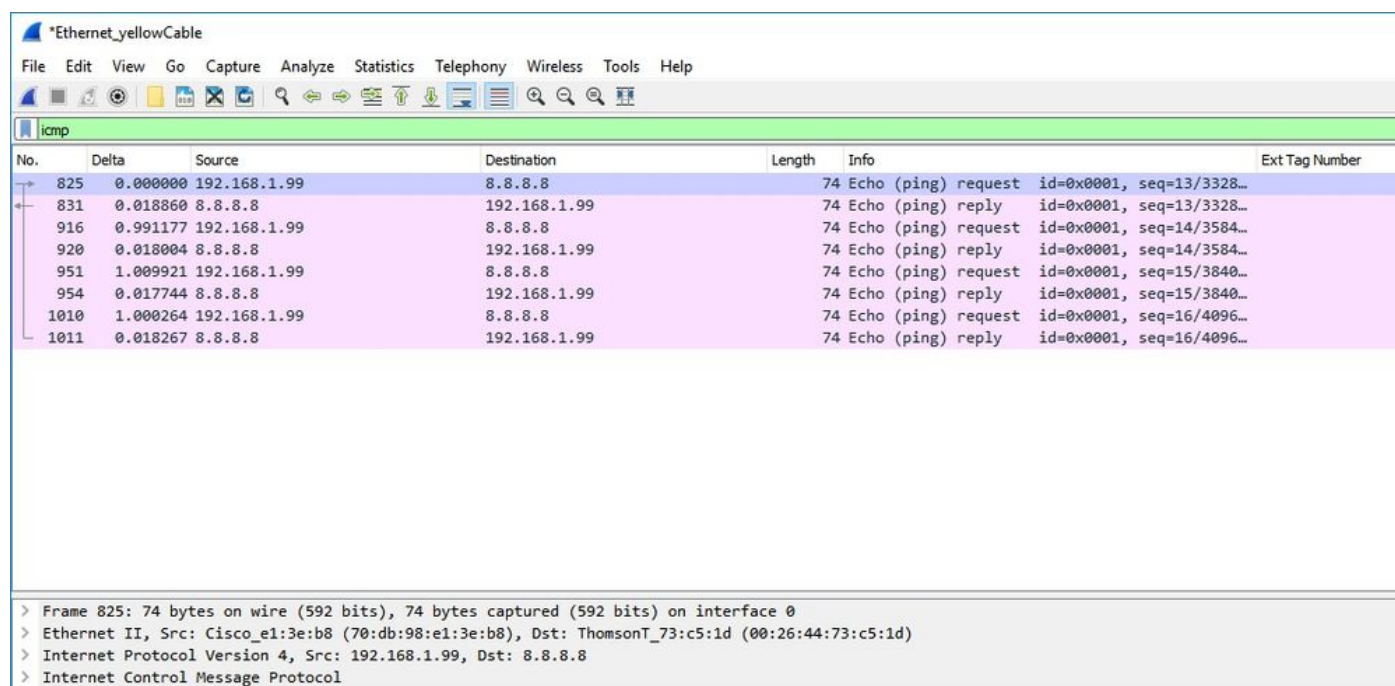
```
AP3800_E1.3EB8#show capwap client detailrcb
SLOT 0 Config
```

```
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
...
```

以下是顯示流量在本地交換的封包擷取範例。此處所做的測試是從使用IP 192.168.1.98的客戶端對Google DNS伺服器執行「ping」操作，然後對192.168.1.254執行「ping」操作。您可以看到來源為AP IP地址192.168.1.99的IP的ICMP傳送到Google DNS，因為AP在本地對流量執行NAT。沒有

icmp到192.168.1.254，因為流量在DTLS通道中加密，並且只看到應用資料幀。



The image shows a Wireshark capture of ICMP traffic on an Ethernet interface. The capture is filtered for 'icmp'. The packet list pane shows several ping request and reply packets. The packet details pane for packet 825 shows the following structure:

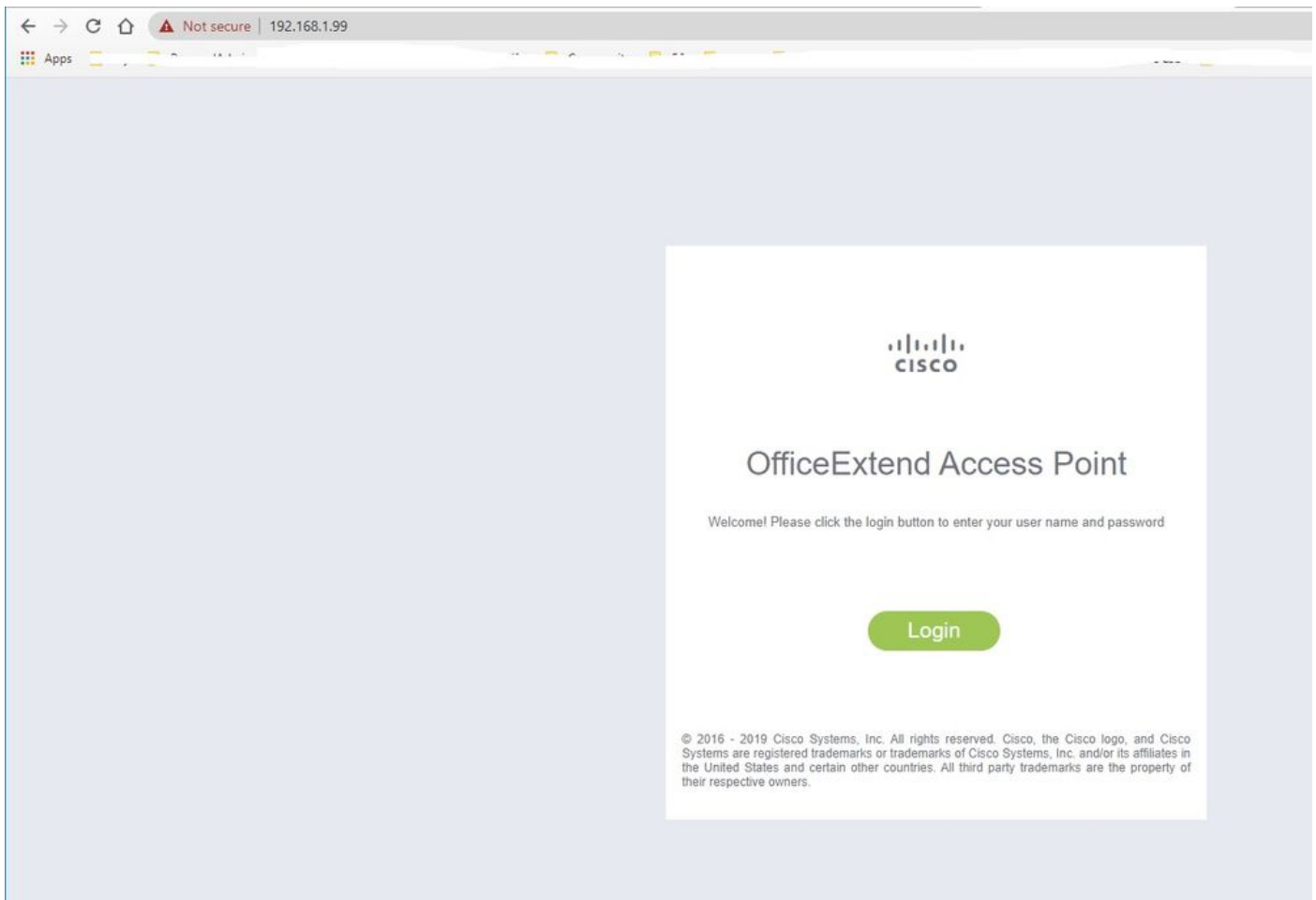
No.	Delta	Source	Destination	Length	Info	Ext Tag Number
825	0.000000	192.168.1.99	8.8.8.8	74	Echo (ping) request id=0x0001, seq=13/3328...	
831	0.018860	8.8.8.8	192.168.1.99	74	Echo (ping) reply id=0x0001, seq=13/3328...	
916	0.991177	192.168.1.99	8.8.8.8	74	Echo (ping) request id=0x0001, seq=14/3584...	
920	0.018004	8.8.8.8	192.168.1.99	74	Echo (ping) reply id=0x0001, seq=14/3584...	
951	1.009921	192.168.1.99	8.8.8.8	74	Echo (ping) request id=0x0001, seq=15/3840...	
954	0.017744	8.8.8.8	192.168.1.99	74	Echo (ping) reply id=0x0001, seq=15/3840...	
1010	1.000264	192.168.1.99	8.8.8.8	74	Echo (ping) request id=0x0001, seq=16/4096...	
1011	0.018267	8.8.8.8	192.168.1.99	74	Echo (ping) reply id=0x0001, seq=16/4096...	

The packet details pane for packet 825 shows the following structure:

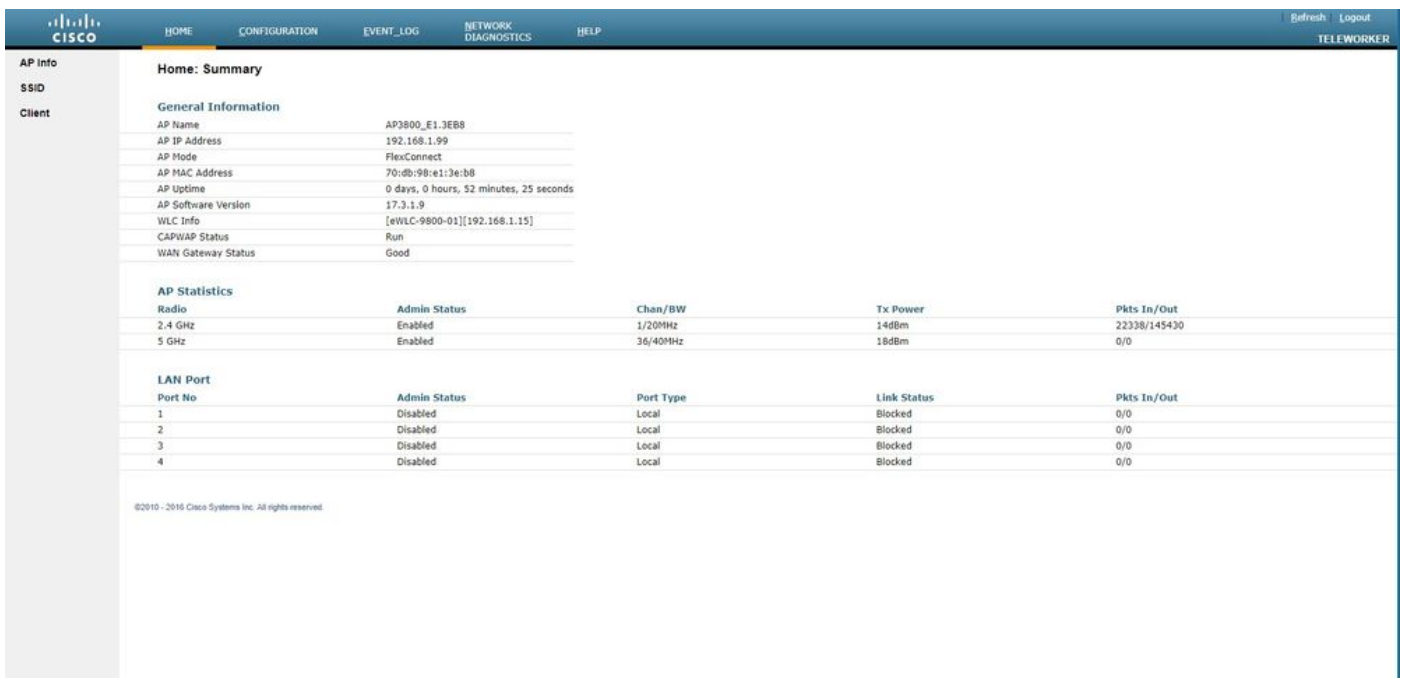
- > Frame 825: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
- > Ethernet II, Src: Cisco_e1:3e:b8 (70:db:98:e1:3e:b8), Dst: ThomsonT_73:c5:1d (00:26:44:73:c5:1d)
- > Internet Protocol Version 4, Src: 192.168.1.99, Dst: 8.8.8.8
- > Internet Control Message Protocol

附註：本地交換的流量由AP進行NAT轉換，因為在正常情況下，客戶端子網屬於Office網路，而家庭辦公室的本地裝置不知道如何到達客戶端子網。AP使用本地家庭辦公室子網中的AP IP地址轉換客戶端流量。

您可以訪問OEAP GUI，開啟瀏覽器並輸入URL中的AP IP地址。預設憑據為admin/admin，您必須在初始登入時更改這些憑據。



一旦登入，您就可以存取GUI：



您可以訪問OEAP中的典型資訊，例如AP資訊、SSID和連線的客戶端：

The screenshot shows the Cisco Catalyst 9800 WLC configuration interface. The top navigation bar includes links for HOME, CONFIGURATION, EVENT_LOG, NETWORK DIAGNOSTICS, and HELP. On the right, there are links for Refresh, Logout, and TELEWORKER. The left sidebar contains a menu with AP Info, SSID, and Client. The main content area is titled 'Association' and features a 'Show all' button. It is divided into two sections: 'Local Clients' and 'Corporate Clients'. The 'Corporate Clients' section contains a table with the following data:

Client MAC	Client IP	WLAN SSID	Radio/LAN	Association Time	Pkts In/Out
98:22:EF:D4:D1:09	192.168.1.98	HomeOffice	2.4GHz	00d:00h:00m:19s	45/2

At the bottom of the page, there is a copyright notice: ©2010 - 2016 Cisco Systems Inc. All rights reserved.

相關檔案

[瞭解Catalyst 9800無線控制器上的FlexConnect](#)

[適用於FlexConnect的分割通道](#)

[在Catalyst 9800 WLC上設定OEAP和RLAN](#)