使用轉換模式設定增強開放式 SSID - OWE

目錄

簡介

本檔案介紹如何在Catalyst 9800無線LAN控制器(9800 WLC)上設定Enhanced Open（具有過渡模式）並疑難排解。

必要條件

需求

思科建議您瞭解以下主題：

- 思科無線 LAN 控制器 (WLC) 9800.
- 支援WPA3的思科接入點(AP)。
- IEEE 標準 802.11ax
- Wireshark.

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- WLC 9800-CL 搭配 IOS® XE 17.9.3。
- 接入點C9130、C9136、CW9162、CW9164和CW9166。
- Wi-Fi 6客戶端：
  - IOS 16上的iPhone SE3第1代

    - Mac OS 12上的MacBook。
- Wi-Fi 6客戶端：
    - Lenovo X1 Carbon Gen11 搭載 Intel AX211 Wi-Fi 6 和 6E 介面卡，並搭配 22.200.2(1) 版驅動程式
    - Netgear A8000 Wi-Fi 6 和 6E 介面卡搭配驅動程式 v1(0.0.108)
    - 搭載 Android 13 的手機 Pixel 6a
    - 搭載 Android 13 的手機 Samsung S23

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。

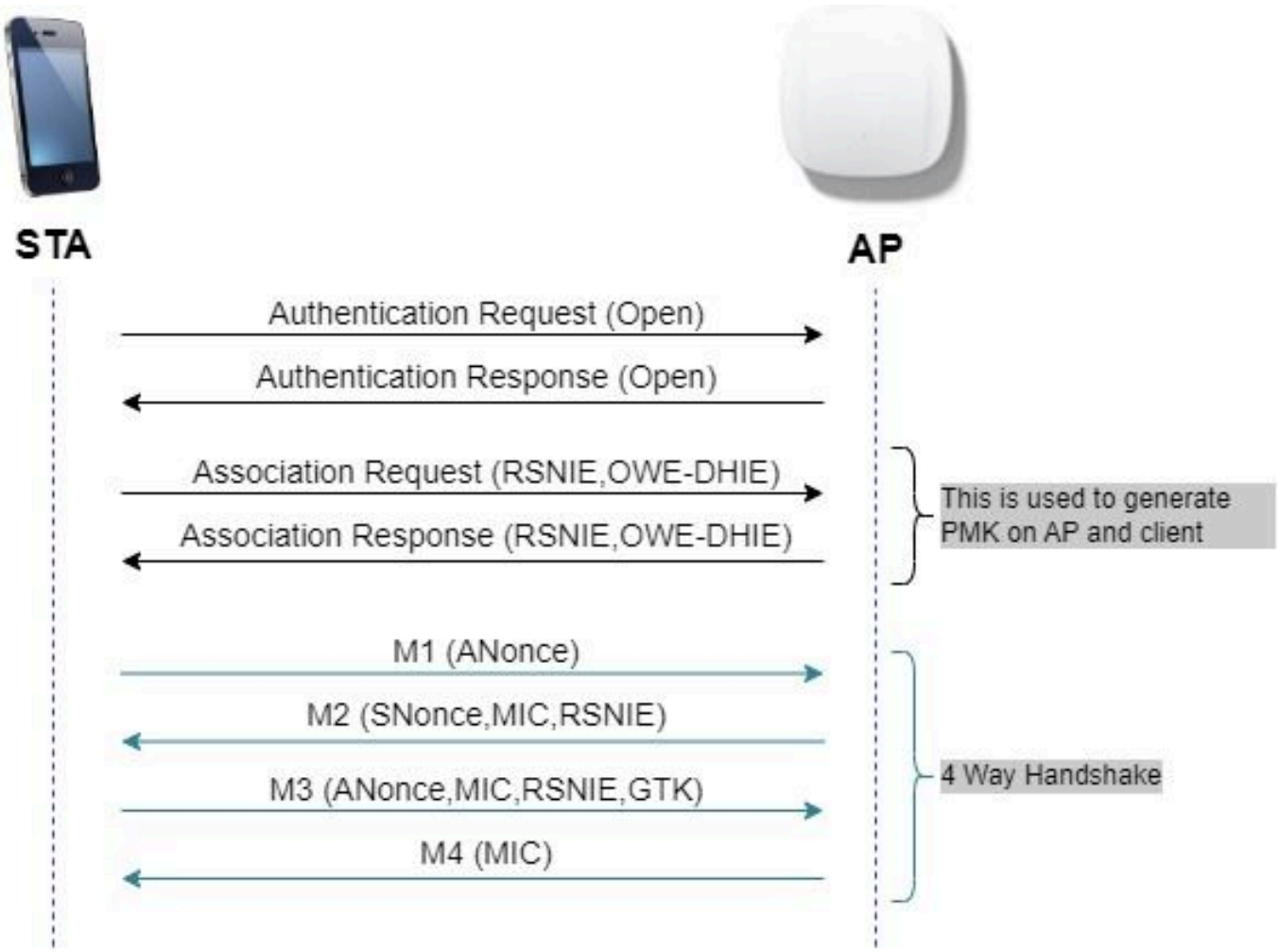
背景資訊

增強開放是WiFi聯盟提供的認證，是WPA3無線安全標準的一部分。與公共PSK無線網路相比，它在開放式（未經驗證的）網路上使用機會無線加密(OWE)來防止被動監聽並防止簡單攻擊。

使用增強型Open時，使用者端和WLC（在中央驗證的情況下）或AP（在FlexConnect本地驗證的情況下）在關聯過程中執行Diffie-Hellman金鑰交換，並在四次握手中使用成對主金鑰密碼(PMK)。

OWE

機會性無線加密 (OWE) 是 IEEE 802.11 的延伸，可為無線媒體提供加密 (IETF RFC 8110)。 OWE 型驗證目的在於避免 AP 和用戶端之間開啟不安全的無線連線。OWE 使用 Diffie-Hellman 演算法型的加密來設定無線加密。使用OWE時，客戶端和AP在訪問過程中執行Diffie-Hellman金鑰交換，並使用生成的成對主金鑰(PMK)金鑰和4次握手。使用 OWE 可提升部署開放式或共用 PSK 型網路時的無線網路安全性。



OWE 訊框交換

過渡模式

通常，企業網路只有一個未加密訪客SSID，並且偏好使用不支援增強型開放客戶端的舊客戶端和增強型開放到共存的較新客戶端。過渡模式是專為迎合此情況而引入的。

這要求配置兩個SSID — 一個隱藏SSID以支援OWE，另一個為開放式SSID且已廣播。

機會無線加密(OWE)轉換模式使OWE和非OWE STA能夠同時連線到同一個SSID。當所有OWE STA都在OWE轉換模式下看到SSID時，它們會使用OWE進行連線。

開放式WLAN和OWE WLAN都會傳輸信標幀。來自OWE WLAN的信標和探測響應幀包括Wi-Fi Alliance供應商IE封裝開放WLAN的BSSID和SSID，類似地，開放WLAN也包括OWE WLAN。

OWE STA只應在可用網路清單中向使用者顯示在OWE轉換模式下運行的OWE AP的開放BSS的SSID，並抑制該OWE AP的OWE BSS SSID的顯示。

准則和限制：

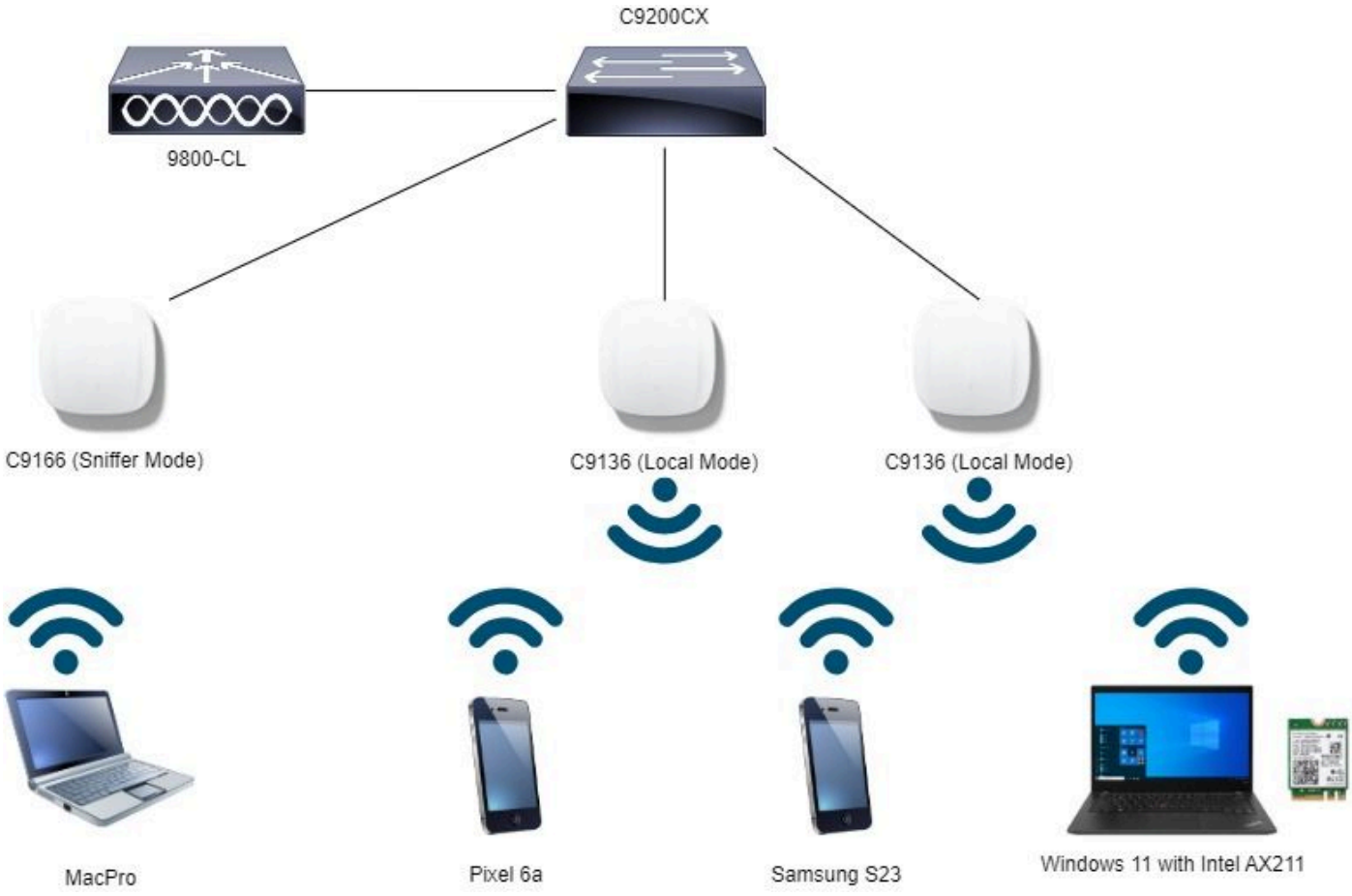
- 增強型開放要求僅使用WPA3策略。Cisco Wave 1(基於Cisco IOS®)AP不支援WPA3。
- 必須將受保護管理幀(PMF)設定為「必需」。預設情況下，該設定僅使用WPA3第2層安全設定。

- 增強型Open只在運行支援Enhanced Open的較新版本的最終客戶端上起作用。
- 6GHz頻段上不允許Wi-Fi增強型開放式過渡模式。根據WPA3™規範v3.4:存在與6GHz和Wi-Fi 7（EHT — 超高吞吐量或MLO — 多鏈路操作）相關的限制：
  - 「當AP在6 GHz頻段中運行BSS時：[...]AP的BSS配置不應允許Wi-Fi增強型開放過渡模式（即，OWE過渡模式元素包含在信標和探測響應中）」。
  - 「當AP在啟用EHT或MLO的情況下運行BSS時[...]:AP的BSS配置不允許使用Wi-Fi增強型開放過渡模式（即信標和探測響應中包含OWE過渡模式元素）。

設定

典型的使用案例，管理員想要配置增強型Open，但仍然允許較舊客戶端連線到訪客SSID。

網路圖表



網路拓撲

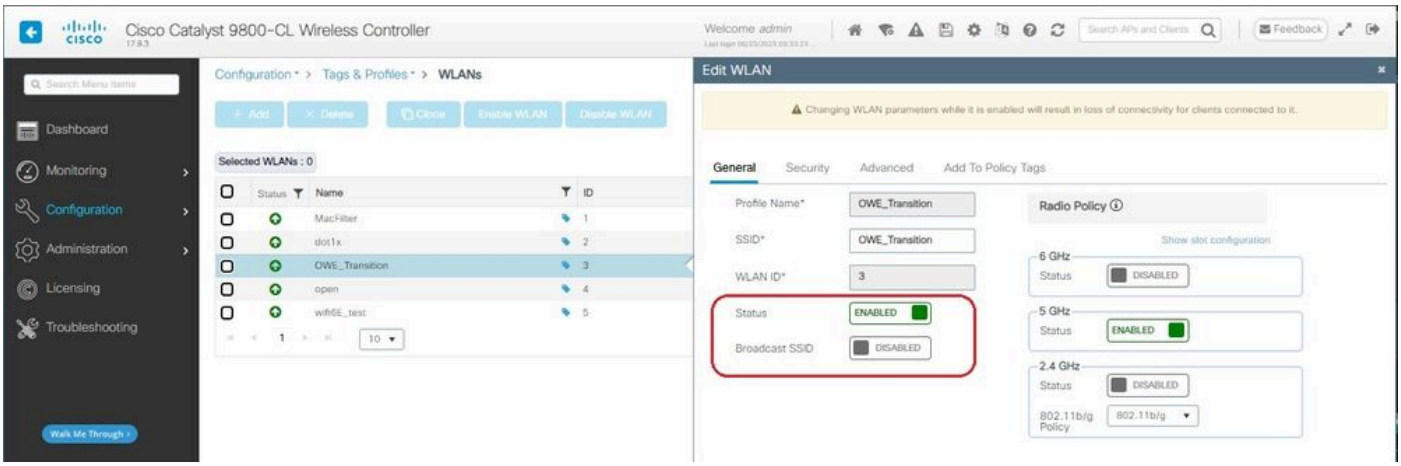
GUI的配置步驟：

建立第一個SSID，特此稱為「OWE_Transition」。在此範例中，WLAN ID 3，並確保其在停用選項「Broadcast SSID」時隱藏：

步驟1選擇Configuration > Tags & Profiles > WLANs以開啟WLANs頁面。

第2步點選Add以新增的WLAN >新增的WLAN名稱「OWE_Transition」>將Status變更為Enable

>確保Broadcast SSID已停用。



OWE轉換增強型開放式SSID隱藏

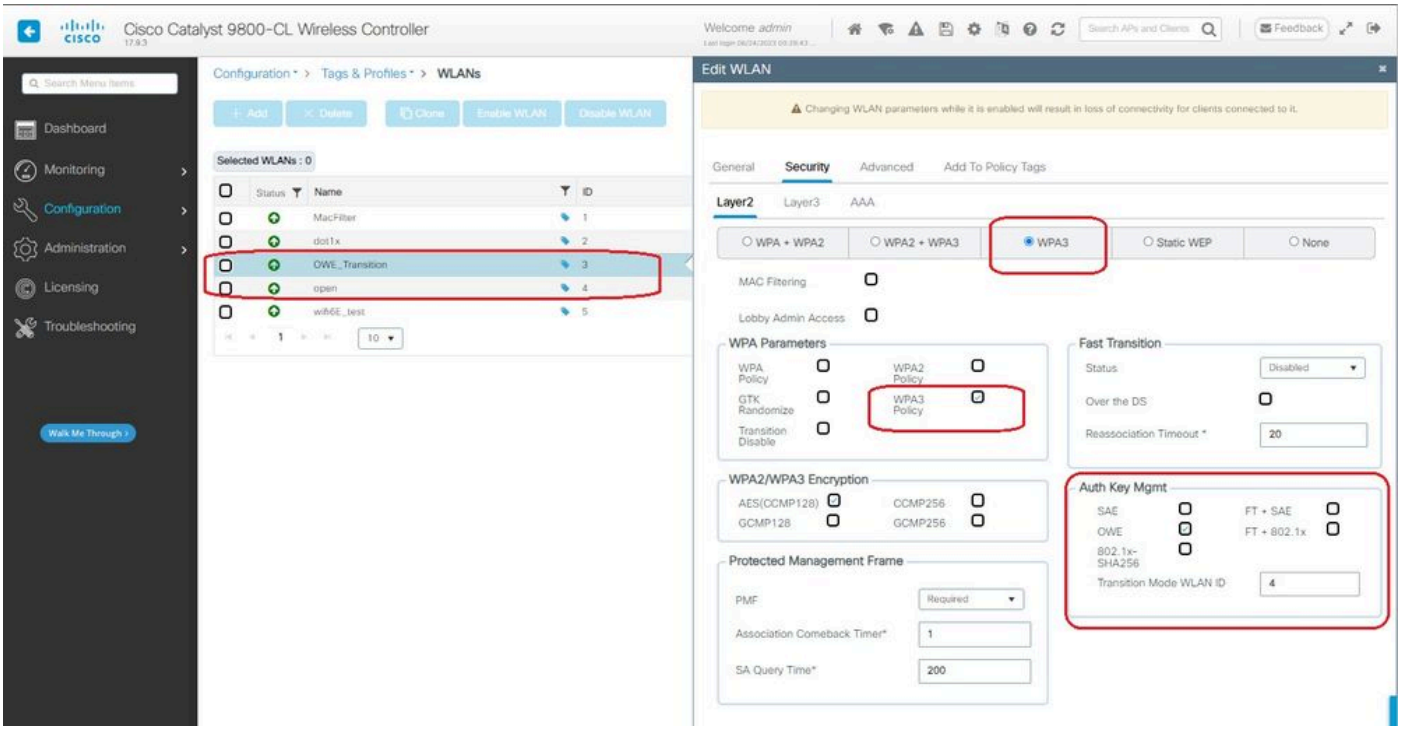
第3步選擇Security > Layer 2頁籤>選擇WPA3。

第4步將受保護管理幀(PMF)設置為必需。

第5步在WPA Parameters >檢查WPA3策略。選擇AES(CCMP128)Encryption and OWE Auth Key Management。

第6步將WLAN ID 4（開放式WLAN）新增到「Transition Mode WLAN ID」框中。

第7步點擊Apply to Device。

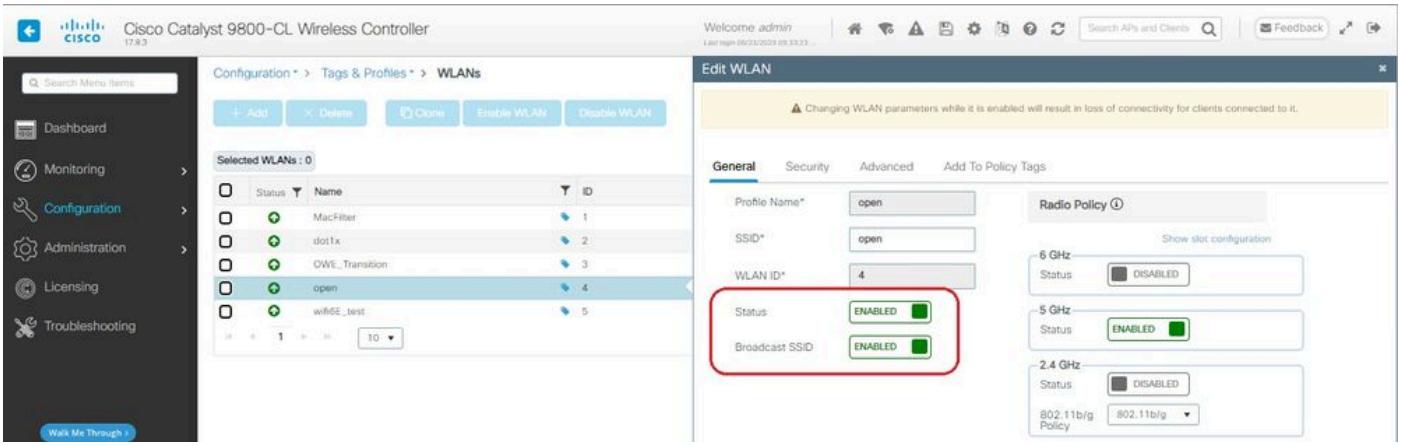


OWE轉換模式 — OWE SSID

建立第二個SSID，在本例中將其稱為「open」（開放），WLAN ID 4，並確保啟用「Broadcast SSID」：

步驟1選擇Configuration > Tags & Profiles > WLANs以開啟WLANs頁面。

第2步點選Add以新增的WLAN >新增的WLAN名稱「open」>將Status變更為Enable >確保Broadcast SSID已啟用。

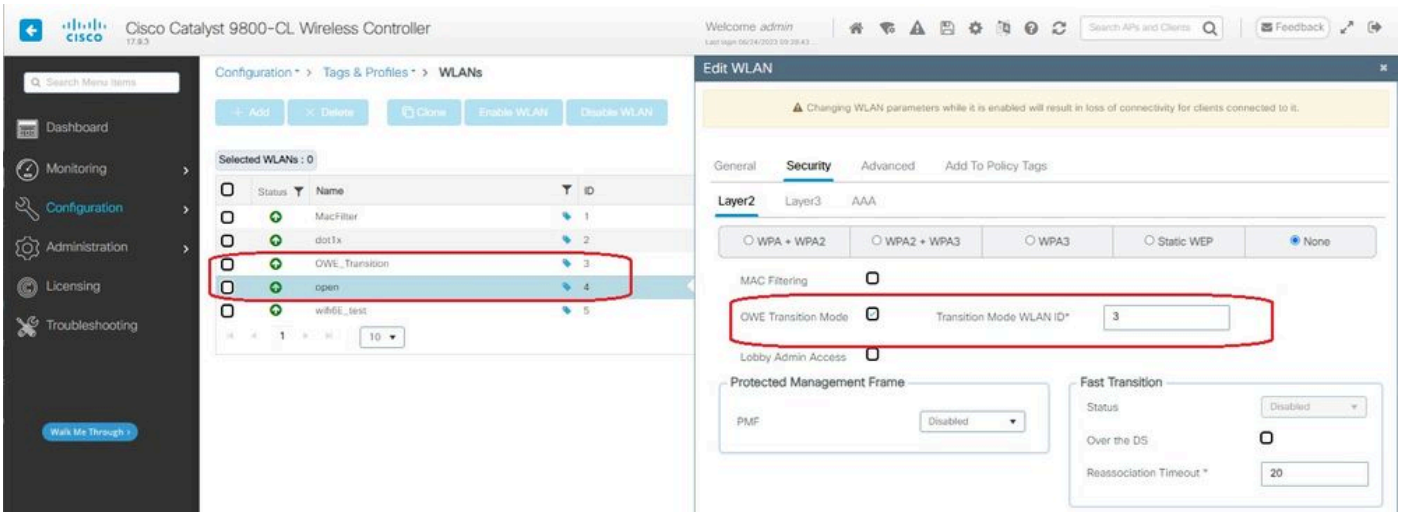


OWE轉換開放式SSID

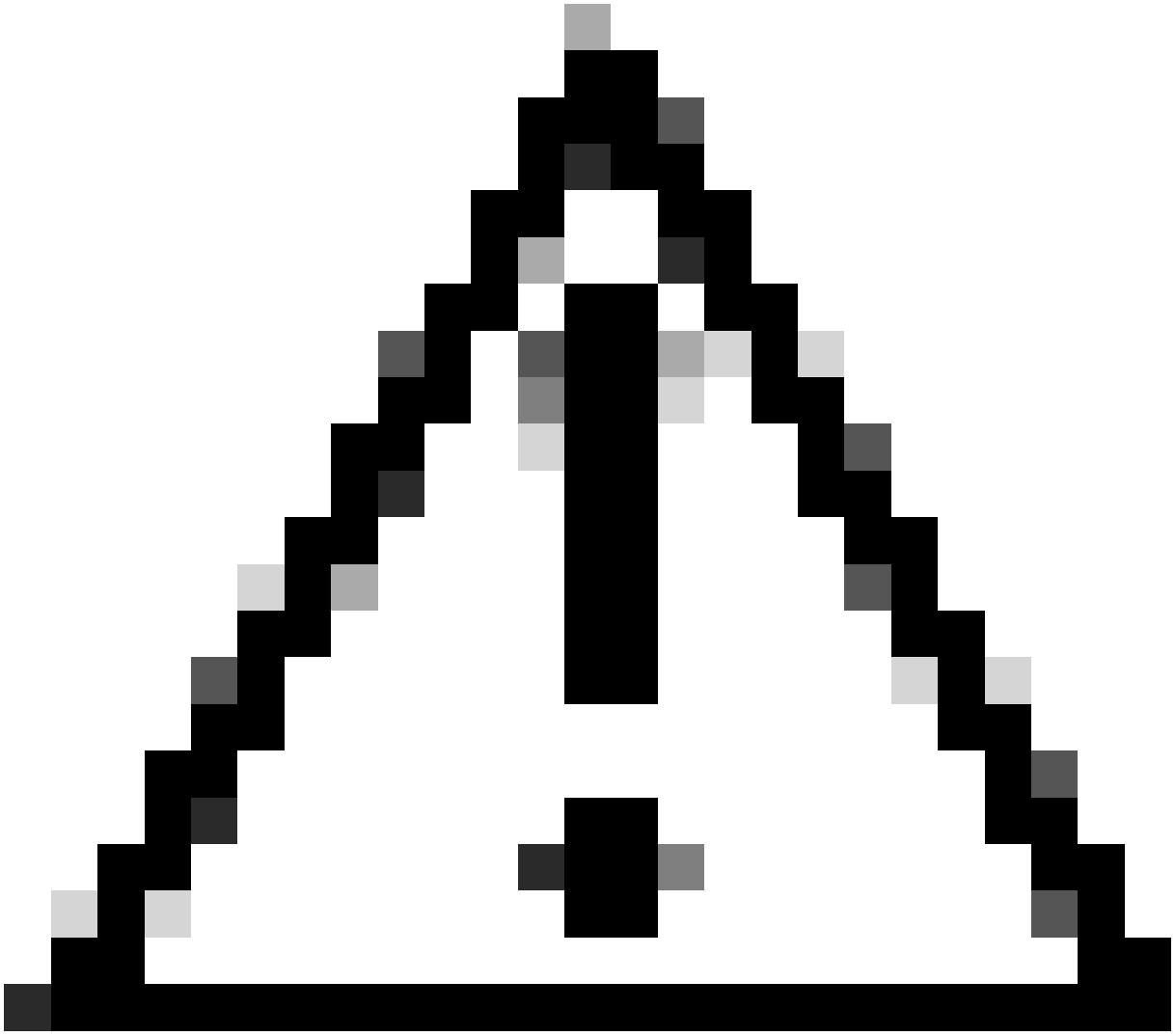
步驟3選擇Security > Layer 2索引標籤>選擇None。

第4步將WLAN ID 3(OWE_Transition)新增到「Transition Mode WLAN ID」框中。

步驟5按一下「Apply to Device」。

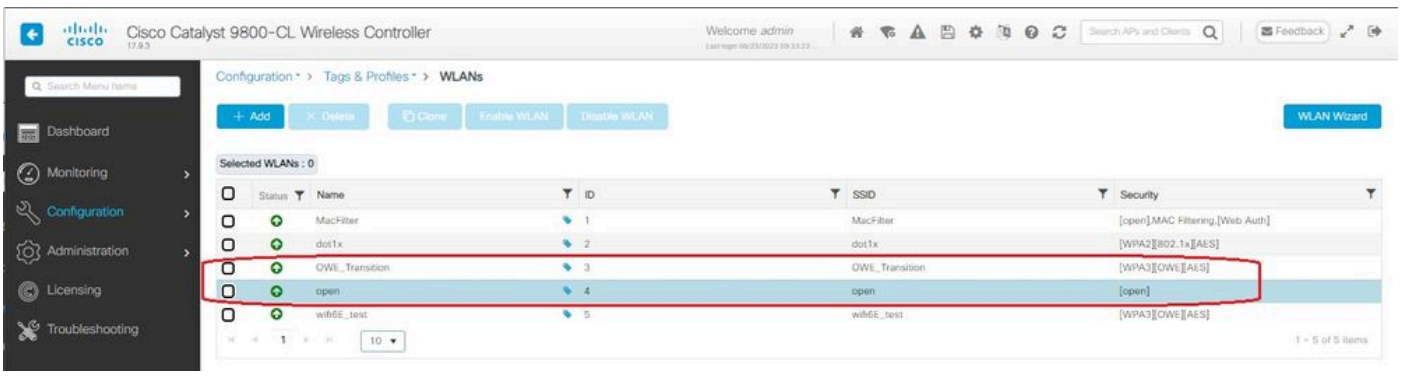


*OWE*轉換模式開放式*WLAN*安全



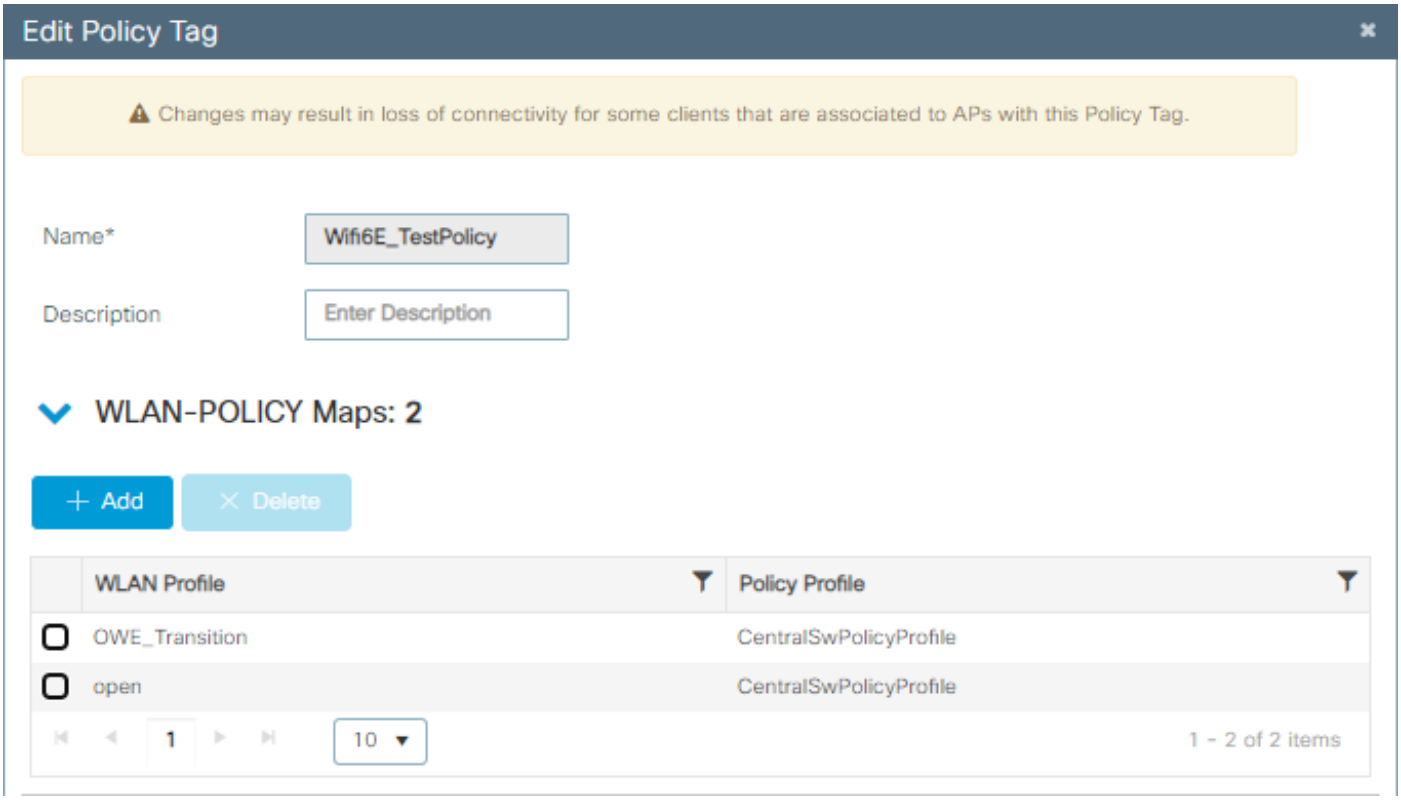
注意：如果您之前使用相同的OWE WLAN SSID的開放式WLAN，則Windows客戶端會將「2」附加到SSID名稱。要解決此問題，請導航到「Network & Internet > Wi-Fi > Manage known networks」（網路和網際網路> Wi-Fi >管理已知網路）並刪除舊連線。

此螢幕截圖顯示了最終結果：一個為WPA3+OWE+WPA3(名為「OWE_Transition」)提供安全保護並進行配置，另一個為名為「open」的完全開放SSID。 只有名為「open」的完全開放SSID的SSID在信標中廣播其SSID，而「OWE_Transition」被隱藏。



OWE轉換模式WLAN

步驟6 將建立的WLAN映射到所需的策略配置檔案到策略標籤，並將其應用到AP。



策略標籤

為CLI配置：

增強型開放SSID:

```
Device# conf t
Device(config)# wlan OWE_Transition 3 OWE_Transition
Device(config)# no broadcast-ssid
Device(config)# no security ft adaptive
Device(config)# no security wpa wpa2
Device(config)# no security wpa akm dot1x
Device(config)# security wpa akm owe
Device(config)# security wpa transition-mode-wlan-id 4
Device(config)# security wpa wpa3
Device(config)# security pmf mandatory
Device(config)# no shutdown
```

開放式SSID:

```
Device# conf t
Device(config)# wlan open 4 open
Device(config)# no security ft adaptive
Device(config)# no security wpa
```

```
Device(config)# no security wpa wpa2
Device(config)# no security wpa wpa2 ciphers aes
Device(config)# no security wpa akm dot1x
Device(config)# security wpa transition-mode-wlan-id 3
Device(config)# no shutdown
```

策略配置檔案：

```
Device(config)# wireless tag policy Wifi6E_TestPolicy
Device(config-policy-tag)# wlan open policy CentralSwPolicyProfile
Device(config-policy-tag)# wlan OWE_Transition policy CentralSwPolicyProfile
```

驗證

這是檢驗部分。

在CLI上驗證WLAN配置：

<#root>

```
Device#show wlan id 3
WLAN Profile Name : OWE_Transition
==================================================
```

Identifier : 3

Description :

Network Name (SSID) : OWE_Transition

Status : Enabled

Broadcast SSID : Disabled

[...]
Security

802.11 Authentication : Open System

Static WEP Keys : Disabled

Wi-Fi Protected Access (WPA/WPA2/WPA3) : Enabled

WPA (SSN IE) : Disabled
WPA2 (RSN IE) : Disabled

WPA3 (WPA3 IE) : Enabled

AES Cipher : Enabled

CCMP256 Cipher : Disabled
GCMP128 Cipher : Disabled
GCMP256 Cipher : Disabled
Auth Key Management
802.1x : Disabled
PSK : Disabled
CCKM : Disabled
FT dot1x : Disabled
FT PSK : Disabled
FT SAE : Disabled
Dot1x-SHA256 : Disabled
PSK-SHA256 : Disabled
SAE : Disabled

OWE : Enabled

SUITEB-1X : Disabled
SUITEB192-1X : Disabled
SAE PWE Method : Hash to Element, Hunting and Pecking(H2E-HNP)

Transition Disable : Disabled

CCKM TSF Tolerance (msecs) : 1000

OWE Transition Mode : Enabled

OWE Transition Mode WLAN ID : 4

OSEN : Disabled
FT Support : Disabled
FT Reassociation Timeout (secs) : 20
FT Over-The-DS mode : Disabled

PMF Support : Required

PMF Association Comeback Timeout (secs): 1
PMF SA Query Time (msecs) : 200
[...]
#show wlan id 4
WLAN Profile Name : open
==========

Identifier : 4

Description :

Network Name (SSID) : open

Status : Enabled

Broadcast SSID : Enabled

[...]
Security

```
802.11 Authentication : Open System
Static WEP Keys : Disabled
```

Wi-Fi Protected Access (WPA/WPA2/WPA3) : Disabled

OWE Transition Mode : Enabled

OWE Transition Mode WLAN ID : 3

```
OSEN : Disabled
FT Support : Disabled
FT Reassociation Timeout (secs) : 20
FT Over-The-DS mode : Disabled
```

PMF Support : Disabled

```
PMF Association Comeback Timeout (secs): 1
PMF SA Query Time (msecs) : 200
[...]
```

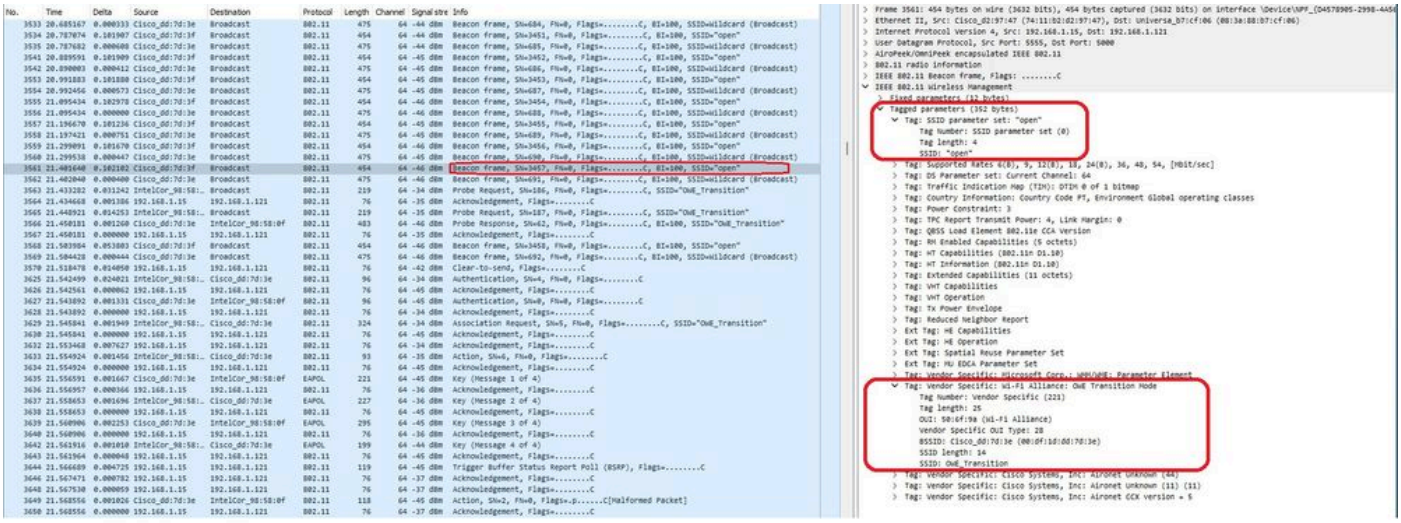
在WLC中，您可以前往AP組態，驗證兩個WLAN在AP上是否均處於使用中狀態：

OWE轉換模式AP操作配置檢視器

啟用時，AP僅使用開放式SSID但帶有OWE轉換模式資訊元素(IE)的信標。 當能夠增強開放連線的

客戶端連線到此SSID時，它會自動使用OWE在關聯後加密所有流量。

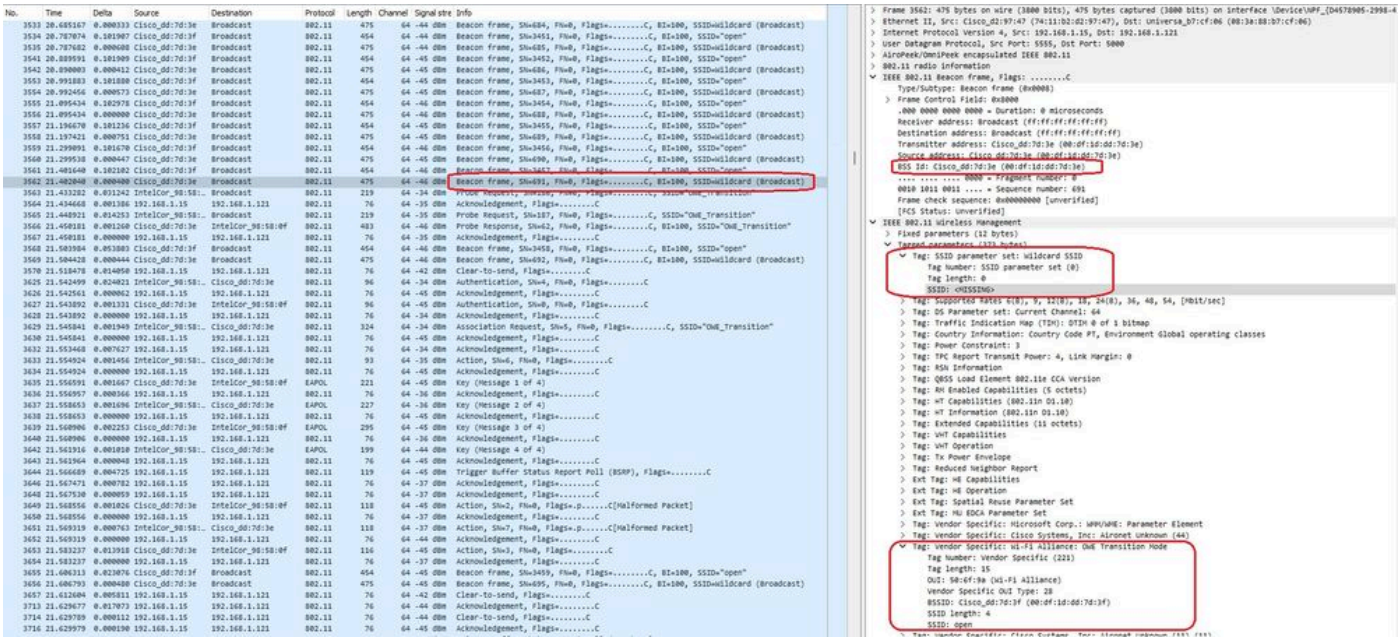
以下是在空中觀察的內容(OTA):



OWE轉換開放式SSID信標

使用SSID「open」傳送的信標包含內部具有增強開放SSID詳細資訊的OWE轉換模式IE，如BSSID和SSID名稱「OWE_Transition」。

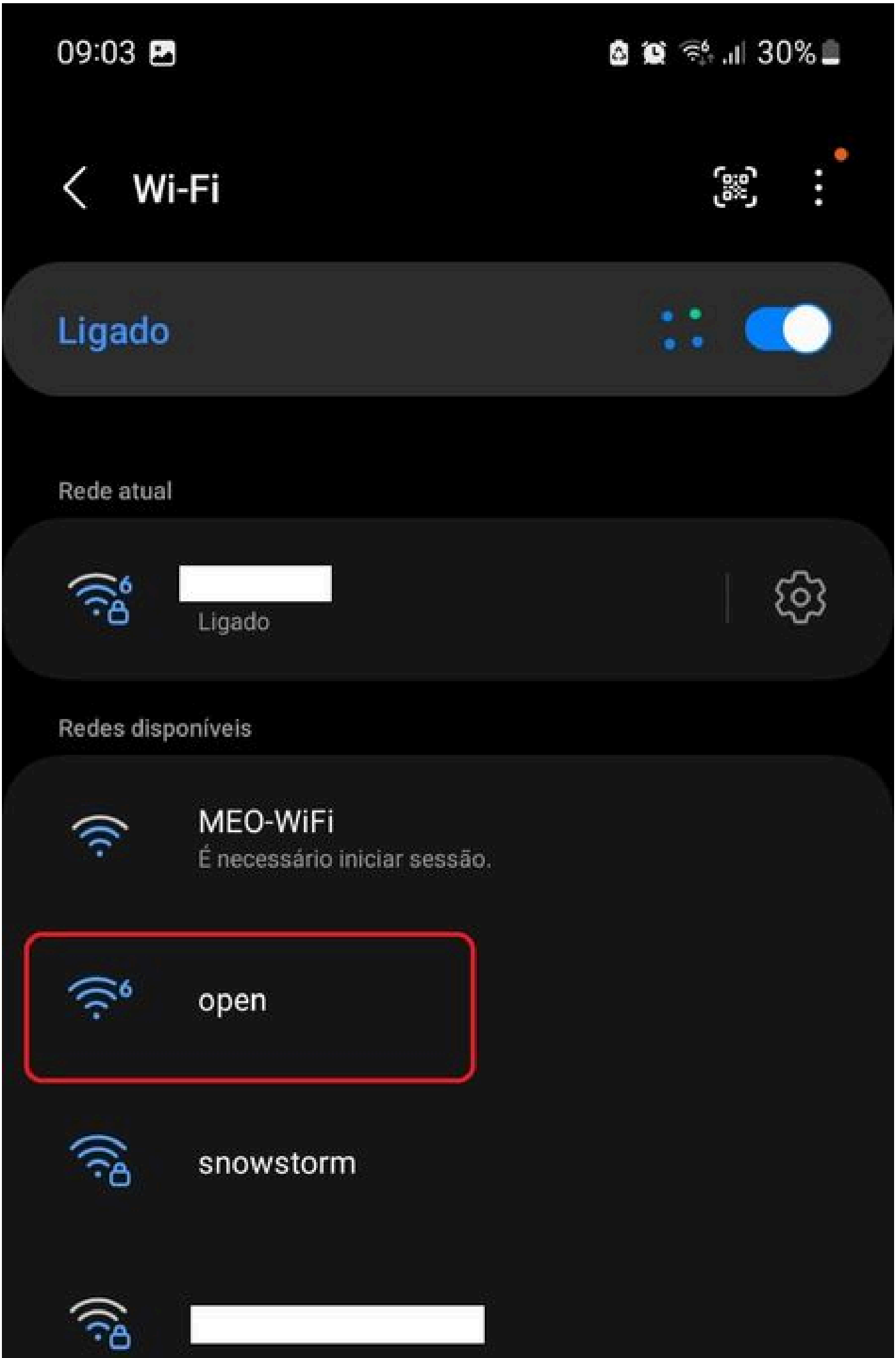
也有隱藏SSID的信標OTA，如果我們按bssid進行過濾，則幀將傳送到BSSID 00:df:1d:dd:7d:3e，該地址是OWE轉換模式IE：中的BSSID



OWE信標

您還可以看到，OWE隱藏信標還包含帶有開放式ssid BSSID和SSID名稱「開放」的OWE轉換模式IE。

以下螢幕截圖顯示了支援「增強開放」的Android手機：它只顯示不帶鎖圖示的開放式SSID（鎖圖示會使使用者認為需要密碼進行連線），但一旦連線後，安全顯示使用增強型開放安全。


09:03
30%
Wi-Fi
Ligado
Rede atual
Ligado
Redes disponíveis
MEO-WiFi
É necessário iniciar sessão.
open
snowstorm

```
Client MAC Address : 286b.3598.580f
[...]
AP Name: AP9136_5C.F524
AP slot : 1
Client State : Associated
Policy Profile : CentralSwPolicyProfile
Flex Profile : N/A
Wireless LAN Id: 3
```

WLAN Profile Name: OWE_Transition

Wireless LAN Network Name (SSID): OWE_Transition

```
BSSID : 00df.1ddd.7d3e
Connected For : 682 seconds
Protocol : 802.11ax - 5 GHz
Channel : 64
Client IIF-ID : 0xa0000003
Association Id : 2
```

Authentication Algorithm : Open System

```
Idle state timeout : N/A
[...]
```

Policy Type : WPA3

Encryption Cipher : CCMP (AES)

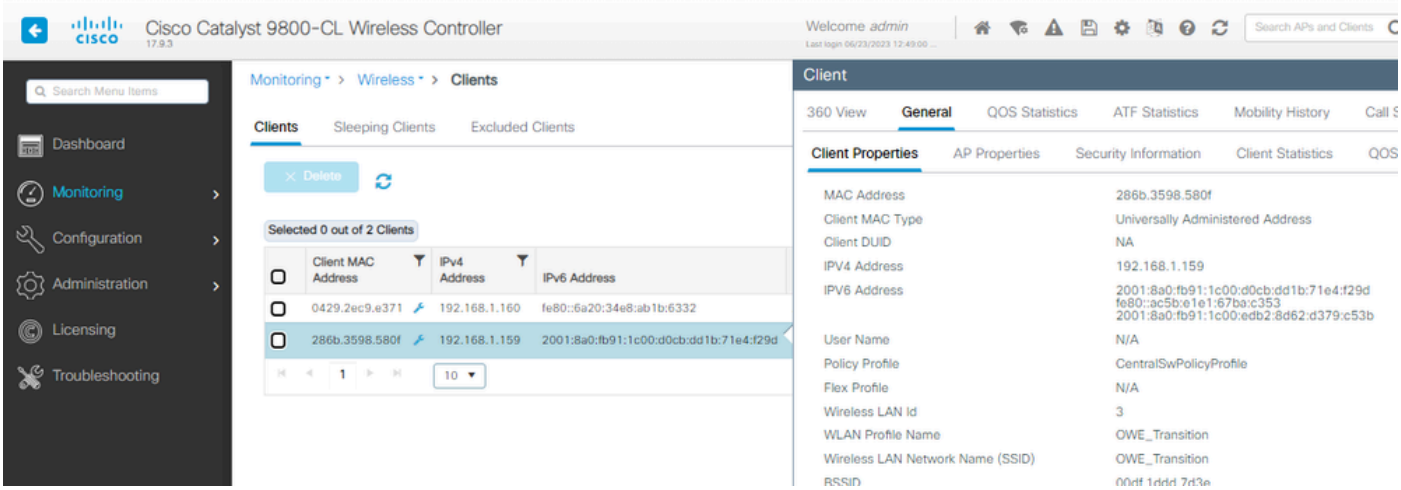
Authentication Key Management : OWE

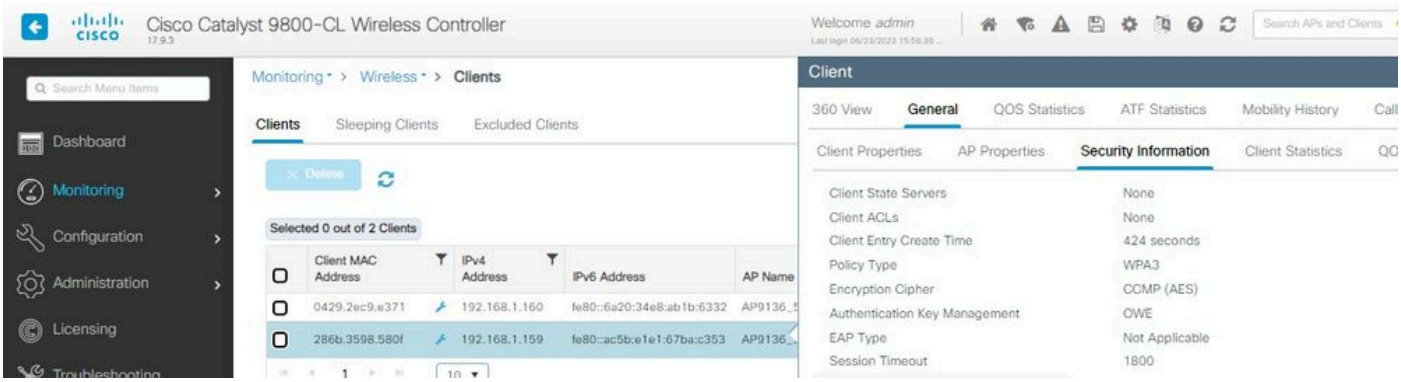
```
Transition Disable Bitmap : None
User Defined (Private) Network : Disabled
User Defined (Private) Network Drop Unicast : Disabled
Encrypted Traffic Analytics : No
```

Protected Management Frame - 802.11w : Yes

```
EAP Type : Not Applicable
```

而且我們可在WLC GUI中觀察到相同情況：





對於不支援「增強開放」的客戶端，它們只能看到並連線到開放的SSID，而不進行加密。

如圖所示，這些客戶端不支援增強開放（分別是IOS 15上的iPhone和Mac OS 12上的MacBook），並且只能看到開放的訪客SSID，並且不使用加密。


Proximus
17:04
Settings
Wi-Fi
Wi-Fi
open
Unsecured Network
MY NETWORKS
[redacted]
OTHER NETWORKS
apr0v0
[redacted]
Other...
Ask to Join Networks
Notify

```
Client MAC Address : b44b.d623.a199
[...]
AP Name: AP9136_5C.F524
AP slot : 1
Client State : Associated
Policy Profile : CentralSwPolicyProfile
Flex Profile : N/A

Wireless LAN Id: 4


WLAN Profile Name: open


Wireless LAN Network Name (SSID): open


BSSID : 00df.1ddd.7d3f
[...]

Authentication Algorithm : Open System


[...]

Protected Management Frame - 802.11w : No


EAP Type : Not Applicable
```

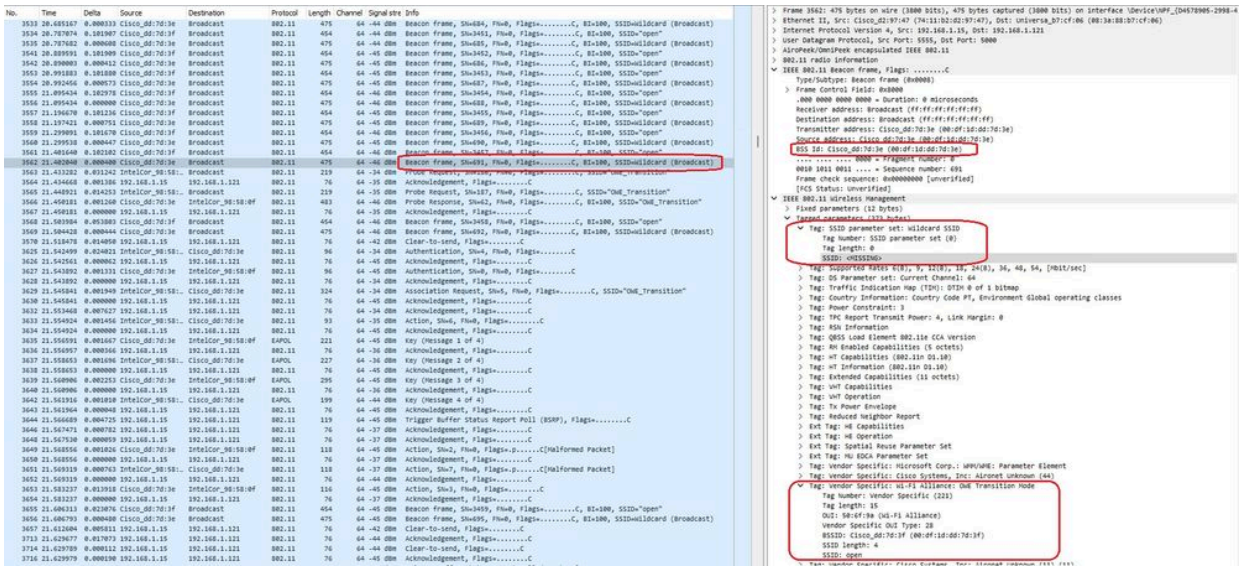
疑難排解

1. 確保客戶端支援OWE，因為並非所有客戶端都支援OWE。檢視客戶端供應商文檔，例如Apple在此處記錄了對其裝置的支援。
2. 由於OWE轉換模式IE的存在，某些較舊的客戶端甚至可能不接受開放的ssid信標，並且在範圍內的網路中不會顯示SSID。如果您的使用者端無法看到開放式SSID，請從WLAN組態中移除Transition VLAN（設為0），然後檢查其是否看到WLAN。
3. 如果客戶端看到開放的SSID，支援OWE，但是它們仍然連線不帶WPA3，然後驗證轉換VLAN ID是否正確並在兩個WLAN的信標中廣播。您可以在監聽器模式下使用AP來捕獲OTA流量。請執行以下步驟在監聽器模式下配置AP：在監聽器模式下配置AP Catalyst 91xx。
    - 使用SSID「open」傳送的信標包含內部具有增強開放SSID詳細資訊的OWE轉換模式IE，如BSSID和SSID名稱「OWE_Transition」：

      OWE轉換開放式SSID信標

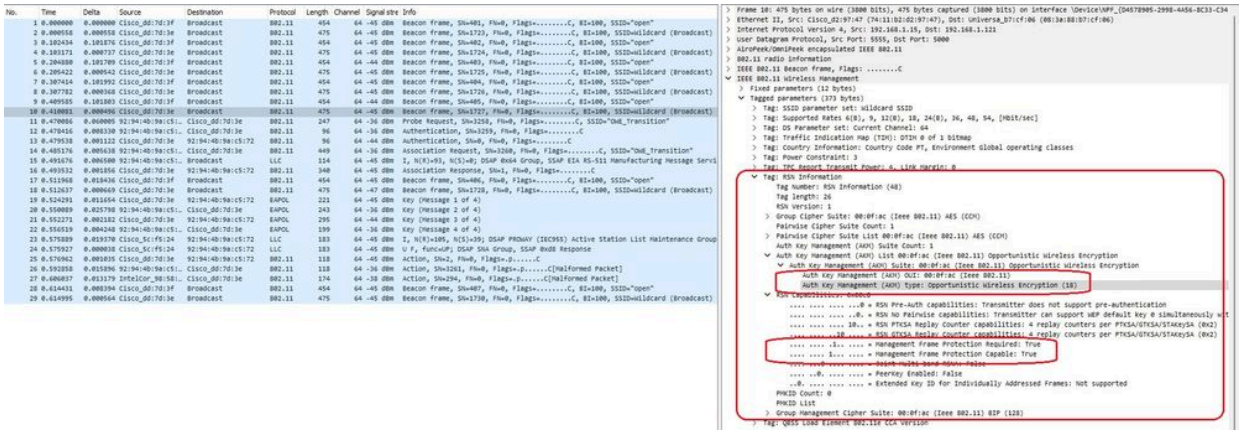
    - 也有隱藏SSID的信標OTA，如果我們按bssid進行過濾，則幀將傳送到BSSID 00:df:1d:dd:7d:3e，該地址是OWE轉換模式IE：中的BSSID



OWE信標

您還可以看到，OWE隱藏信標還包含帶有開放式ssid BSSID和SSID名稱「開放」的OWE轉換模式IE。

- 您還可以檢視AKM資訊並驗證MFP是否通告為「必需」和「支援」：



OWE Beacon AKM

4. 根據客戶端MAC地址收集RadioActive跟蹤，您會看到類似如下所示的日誌：

2023/06/23 15:08:58.567933 {wncd_x_R0-0}{1}: [client-keymgmt] [14854]: (note): MAC: xxxx.xxxx.xxxx EAP Key management successful. AKM:OWE Cipher:CCMP WPA Version: WPA3

2023/06/23 15:10:06.971651 {wncd_x_R0-0}{1}: [client-orch-state] [14854]: (note): MAC: xxxx.xxxx.xxxx Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN

參考資料

Cisco Catalyst 9800 系列無線控制器軟體設定指南 17.9.x

WPA3 部署指南

Wi-Fi聯盟® WPA3™規格v3.4

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。