

# Configure Enhanced Open SSID with Transition Mode - OWE

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[OWE](#)

[Transition Mode](#)

[Guidelines and Restrictions:](#)

[Configure](#)

[Network Diagram](#)

[Configuration steps for GUI:](#)

[Configure for CLI:](#)

[Verify](#)

[Troubleshoot](#)

## Introduction

This document describes how to configure and troubleshoot Enhanced Open with Transition Mode on Catalyst 9800 Wireless LAN Controller (9800 WLC).

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Wireless Lan Controllers (WLC) 9800.
- Cisco Access Points (APs) that support Wi-Fi 6E.
- IEEE Standard 802.11ax.
- Wireshark.

### Components Used

The information in this document is based on these software and hardware versions:

- WLC 9800-CL with IOS® XE 17.9.3.
- APs C9130, C9136, CW9162, CW9164 and CW9166.
- Wi-Fi 6 Clients:
  - iPhone SE3rd gen on IOS 16
  - MacBook on Mac OS 12.
- Wi-Fi 6E Clients:
  - Lenovo X1 Carbon Gen11 with Intel AX211 Wi-Fi 6 and 6E Adapter with driver version 22.200.2(1).

- Netgear A8000 Wi-Fi 6 and 6E Adapter with driver v1(0.0.108);
- Mobile Phone Pixel 6a with Android 13;
- Mobile Phone Samsung S23 with Android 13.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

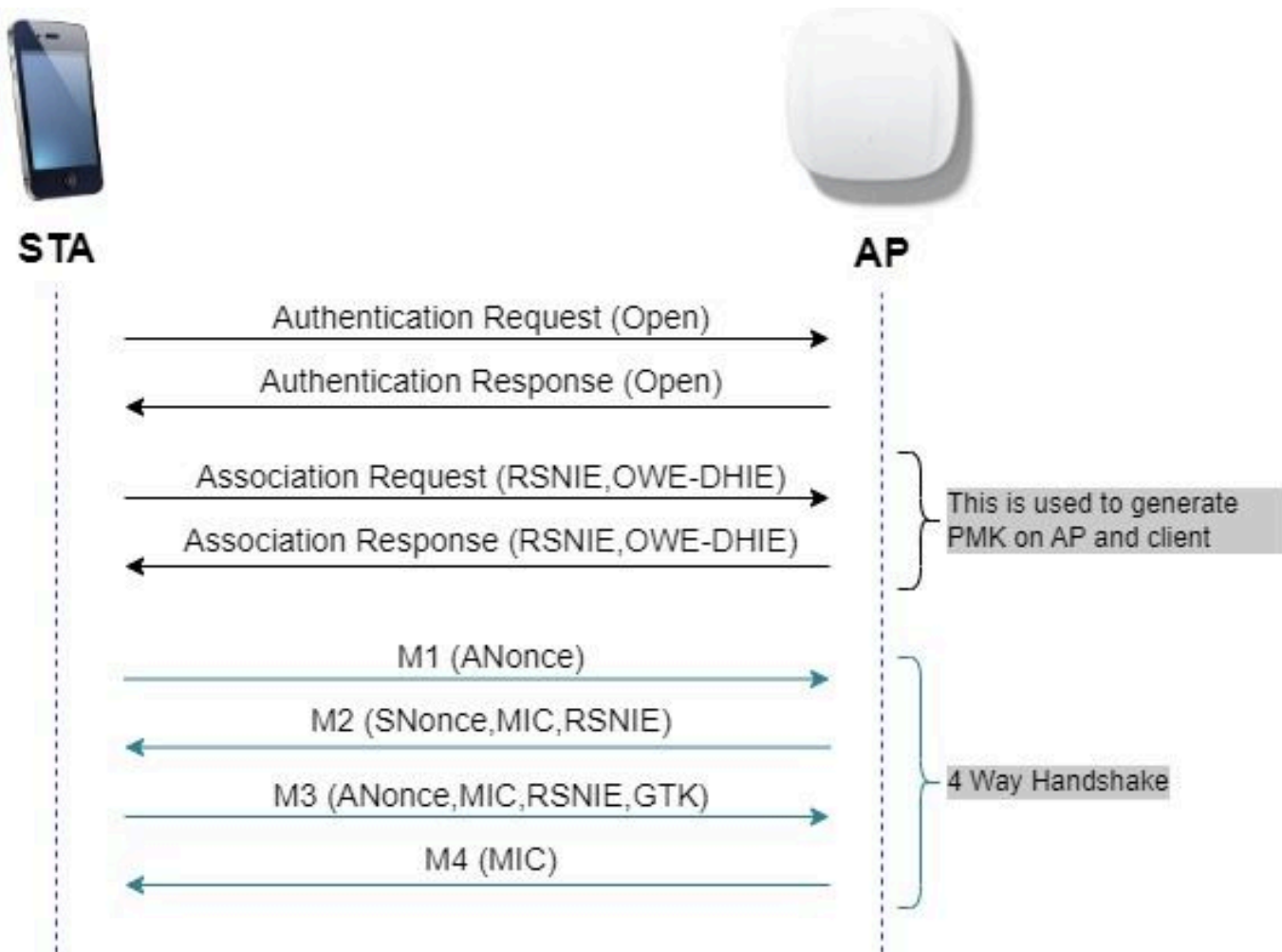
## **Background Information**

The Enhanced Open is a certification provided by WiFi alliance as part of the WPA3 wireless security standard. It uses Opportunistic Wireless Encryption (OWE) on Open (unauthenticated) networks to prevent passive sniffing and prevent simple attacks as compared to a public PSK wireless network.

With Enhanced Open, clients and the WLC (in case of Central Authentication) or the AP (in case of FlexConnect Local Authentication) perform a Diffie-Hellman key exchange during the association process and use the pairwise master key secret (PMK) with the 4-way handshake.

### **OWE**

Opportunistic Wireless Encryption (OWE) is an extension to IEEE 802.11 that provides encryption of the wireless medium ([IETF RFC 8110](#)). The purpose of OWE based authentication is avoid open unsecured wireless connectivity between the AP's and clients. The OWE uses the Diffie-Hellman algorithms based Cryptography to setup the wireless encryption. With OWE, the client and AP perform a Diffie-Hellman key exchange during the access procedure and use the resulting pairwise master key (PMK) secret with the 4-way handshake. The use of OWE enhances wireless network security for deployments where Open or shared PSK based networks are deployed.



OWE frame exchange

## Transition Mode

Typically enterprise networks only have one unencrypted guest SSID and prefer to have both older clients that do not support enhanced open and newer clients with enhanced open to co-exist. Transition Mode is introduced specifically to cater to this scenario.

This requires configuration of two SSIDs - one hidden SSID to support OWE and a second SSID that is Open and is broadcasted.

The Opportunistic Wireless Encryption (OWE) transition mode enables OWE and non-OWE STAs to connect to the same SSID simultaneously. When all the OWE STAs see an SSID in OWE transition mode, they connect with the OWE.

Both the open WLAN and the OWE WLAN transmit beacon frames. Beacon and probe response frames from the OWE WLAN include the Wi-Fi Alliance vendor IE to encapsulate the BSSID and SSID of the open WLAN, and similarly, the open WLAN also includes for OWE WLAN.

An OWE STA shall only display to the user in the list of available networks the SSID of the Open BSS of an OWE AP operating in OWE Transition Mode, and shall suppress the display of the OWE BSS SSID of that OWE AP.

## Guidelines and Restrictions:

- Enhanced open requires WPA3 only Policy. WPA3 is not supported in Cisco Wave 1 (Cisco IOS®-

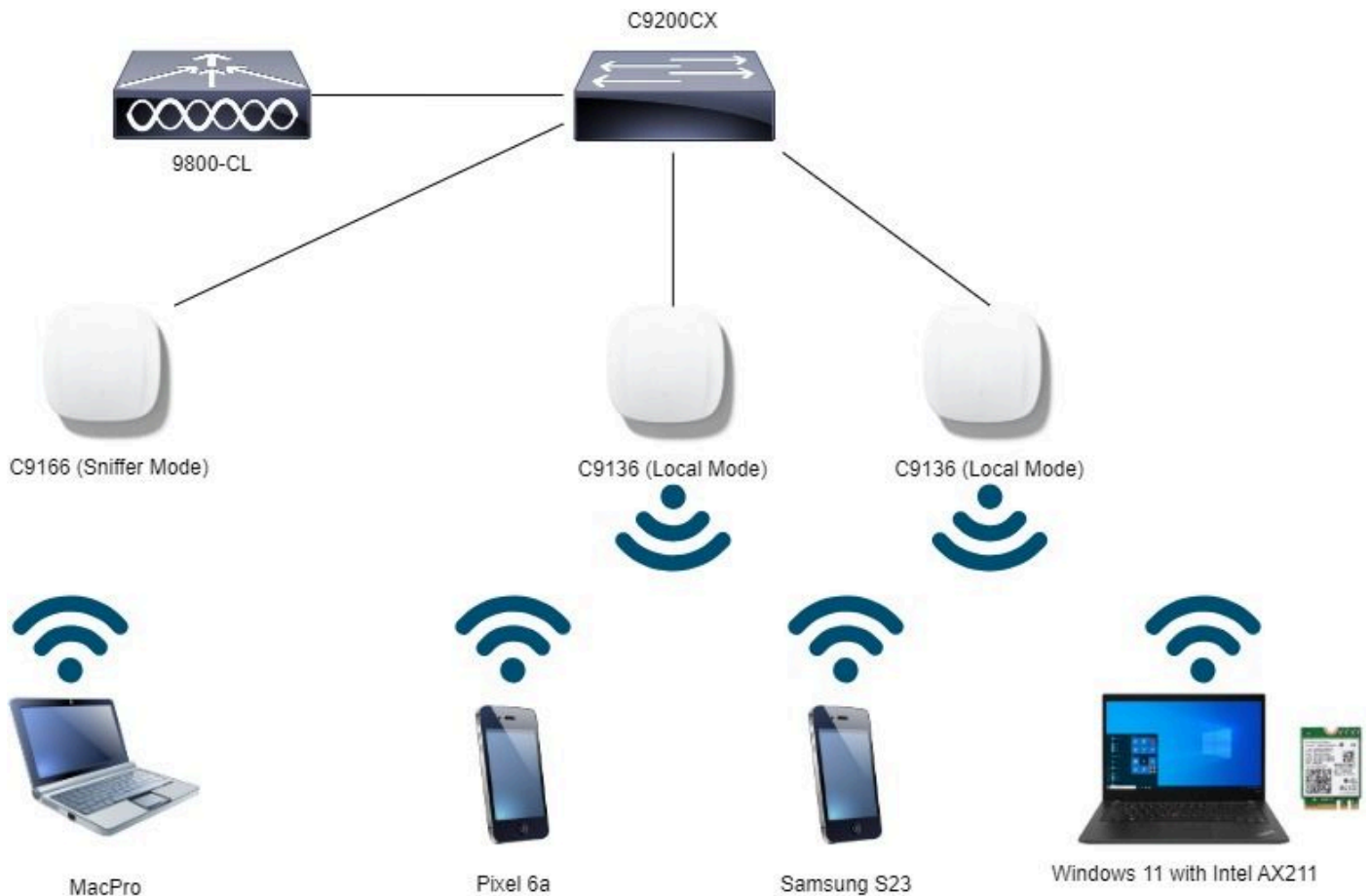
based) APs.

- Protected Management Frame (PMF) must be set to Required. This is set by default with WPA3 only Layer 2 Security.
- Enhanced Open only works on end clients that run the newer versions that support Enhanced Open.

## Configure

Typical use case where the administrator wants to configure Enhanced Open but still allow for older clients to be able to connect to the guest SSID.

### Network Diagram



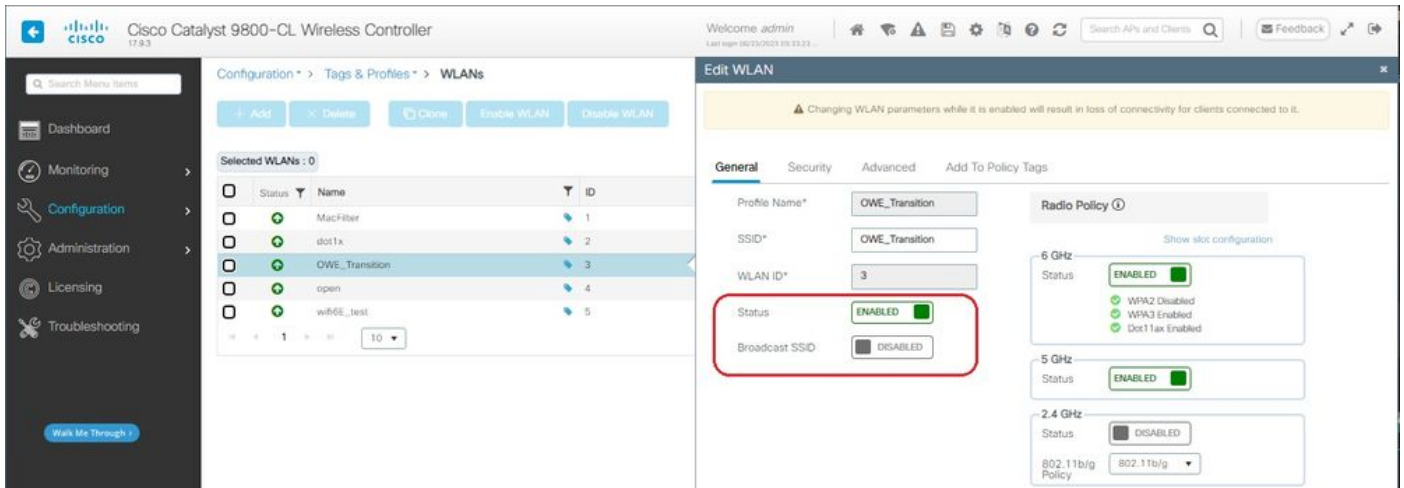
*Network Topology*

### Configuration steps for GUI:

Create first SSID, hereby called "OWE\_Transition". In this example WLAN ID 3, and ensure it is hidden with the option "Broadcast SSID" disabled:

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs** to open the WLANs page.

Step 2 Click **Add** to add new WLAN > add WLAN name "OWE\_Transition" > change **Status** to **Enable** > ensure **Broadcast SSID** is **Disabled**.



*OWE Transition Enhanced Open SSID hidden*

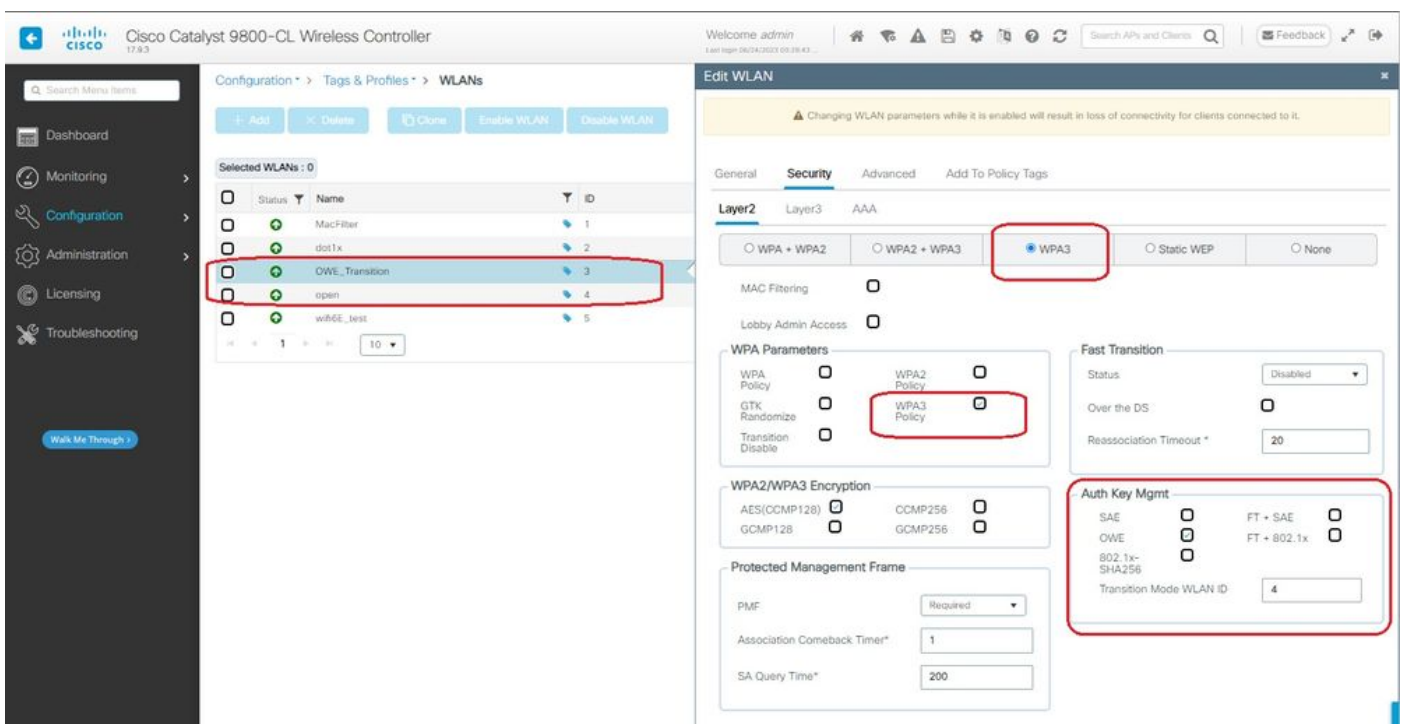
Step 3 Choose the **Security > Layer 2** tab > Select **WPA3**.

Step 4 Set Protected Management Frame (PMF) to **Required**.

Step 5 Under **WPA Parameters** > Check the WPA3 Policy. Select **AES(CCMP128)** Encryption and **OWE** Auth Key Management.

Step 6 Add WLAN ID 4 (open WLAN) to "**Transition Mode WLAN ID**" box.

Step 7 Click **Apply to Device**.



*OWE Transition Mode - OWE SSID*

Create second SSID, call it "open" in this example WLAN ID 4, and ensure you enable "Broadcast SSID":

Step 1 Choose **Configuration > Tags & Profiles > WLANs** to open the WLANs page.

Step 2 Click **Add** to add new WLAN > add WLAN name "open" > change **Status** to **Enable** > ensure

## Broadcast SSID is Enabled.

The screenshot shows the 'Edit WLAN' configuration page for WLAN ID 4. The 'General' tab is selected. The 'Broadcast SSID' checkbox is checked and highlighted with a red box. The 'Status' checkbox is also checked. The 'Radio Policy' section shows the 5 GHz status as 'ENABLED'.

*OWE Transition Open SSID*

Step 3 Choose the **Security > Layer 2** tab > Choose **None**.

Step 4 Add WLAN ID 4 (OWE\_Transition) to "**Transition Mode WLAN ID**" box.

Step 5 Click **Apply to Device**.

The screenshot shows the 'Edit WLAN' configuration page for WLAN ID 4. The 'Security' tab is selected, and the 'Layer2' section is active. The 'OWE Transition Mode' checkbox is checked, and the 'Transition Mode WLAN ID' field is set to 3, both highlighted with a red box.

*OWE Transition Mode Open WLAN Security*

This screenshot shows the final result: one WLAN is secured and configured for WPA3+OWE+WPA3 named "OWE\_Transition" and the other is a fully open SSID named "open". Only the fully open SSID called "open" has its SSID broadcasted in the beacons while "OWE\_Transition" is hidden.

The screenshot shows the 'WLANs' configuration page. The table below shows the configuration for the WLANs:

Status	Name	ID	SSID	Security
<input type="checkbox"/>	MacFilter	1	MacFilter	[open]MAC Filtering [Web Auth]
<input type="checkbox"/>	dot1x	2	dot1x	[WPA2][802.1x][AES]
<input type="checkbox"/>	OWE_Transition	3	OWE_Transition	[WPA3][OWE][AES]
<input checked="" type="checkbox"/>	open	4	open	[open]
<input type="checkbox"/>	wifiE_test	5	wifiE_test	[WPA3][OWE][AES]

*OWE Transition Mode WLANs*

Step 6 Map the **WLANs** created to the desired **Policy Profiles** into the **Policy Tag** and apply it to the APs.

Warning: Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name\*

Description

WLAN-POLICY Maps: 2

+ Add X Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> OWE_Transition	CentralSwPolicyProfile
<input type="checkbox"/> open	CentralSwPolicyProfile

1 - 2 of 2 items

*Policy Tag*

## Configure for CLI:

### Enhanced Open 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
```

### Open 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
```

#### Policy Profile:

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

## Verify

This is the verification section.

Verify the WLANs configuration on CLI:

```
<#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  
[...]

In the WLC you can go to the AP Configuration and verify that both WLANs are active on the AP:



*OWE Transition Mode AP Operational Configuration Viewer*

When enabled, the AP only beacons with Open SSID but carry an OWE Transition Mode Information Element (IE). When a client capable of enhanced open connects to this SSID, it automatically uses OWE to encrypt all traffic post association.

Here is what you can observe over the air (OTA):



09:03

30%

# Wi-Fi



Ligado



## Rede atual



Ligado



## Redes disponíveis



MEO-WiFi

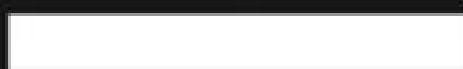
É necessário iniciar sessão.



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

And we can observe the same in the WLC GUI:

Cisco Catalyst 9800-CL Wireless Controller

Welcome admin

Monitoring > Wireless > Clients

Client Properties

Client Properties	AP Properties	Security Information	Client Statistics	QOS
MAC Address		286b.3598.580f		
Client MAC Type		Universally Administered Address		
Client DUID		NA		
IPv4 Address		192.168.1.159		
IPv6 Address		2001:8a0:fb91:1c00:d0cb:dd1b:71e4:f29d fe80::ac5b:e1e1:67ba:c353 2001:8a0:fb91:1c00:edb2:8d62:d379:c53b		
User Name		N/A		
Policy Profile		CentralSwPolicyProfile		
Flex Profile		N/A		
Wireless LAN Id		3		
WLAN Profile Name		OWE_Transition		
Wireless LAN Network Name (SSID)		OWE_Transition		
RSSID		00df14d4d742e		

Cisco Catalyst 9800-CL Wireless Controller

Welcome admin

Monitoring > Wireless > Clients

Client Properties

Client Properties	AP Properties	Security Information	Client Statistics	QOS
Client State Servers		None		
Client ACLs		None		
Client Entry Create Time		424 seconds		
Policy Type		WPA3		
Encryption Cipher		CCMP (AES)		
Authentication Key Management		OWE		
EAP Type		Not Applicable		
Session Timeout		1800		

For clients that do not support Enhanced Open, they only see and connect to the open SSID, with no encryption.

As illustrated here, these are clients that do not support Enhanced Open (respectively an iPhone on IOS 15 and a MacBook on Mac OS 12) and only see the open guest SSID and do not use encryption.

Wi-Fi



open

Unsecured Network

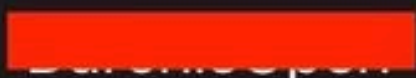


MY NETWORKS



OTHER NETWORKS

apr0v0



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

## Troubleshoot

1. Ensure that client supports OWE, as not all clients support it. Check the client vendor documentation, for example Apple documented the support for their devices [here](#).
2. Some older clients possibly do not even accept the Open ssid beacons due to the presence of the OWE Transition Mode IE and not present the SSID in the networks in range. If your client cannot see the Open SSID, remove the Transition VLAN (set to 0) from the WLAN configuration and check if it sees the WLAN then.
3. If clients see open SSID, support OWE, but they still connect without WPA3, then verify if the transition VLAN id is correct and being broadcasted in the beacons of both WLANs. You can use AP in sniffer mode to capture OTA traffic. Please execute these steps to configure an AP in sniffer mode: [APs Catalyst 91xx in Sniffer Mode](#) .

- The beacon is sent with SSID "open" contains the OWE Transition Mode IE with the enhanced



open SSID details inside, like BSSID and SSID name "OWE\_Transition":

*OWE Transition Open SSID Beacon*

- There are also beacons OTA with the SSID hidden and if we filter by bssid, the frames are sent to the BSSID **00:df:1d:dd:7d:3e** which is the BSSID inside the OWE Transition Mode IE:





## [WPA3 Deployment Guide](#)