PROFINET Traffic Passthrough With QoS

Revised: October 21, 2021

PROFINET Traffic Passthrough With QoS

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Information About Configuring PROFINET

PROFINET is the PROFIBUS International (PI) open Industrial Ethernet Standard that uses TCP/IP and IT standards for automation control. It emphasizes data exchange and defines communication paths to meet speed requirements.

PROFINET communication is scalable on three levels:

- Normal non-real-time communication uses TCP/IP and enables bus cycle times of approximately 100 ms.
- Real-Time (RT): Real-time communication enables cycle times of approximately 10 ms. Real-time data are treated with a higher priority than TCP (UDP)/IP data. It uses the standard existing protocol components (using Ethernet with special frame ether-type = 0x8892 and priority value in the VLAN tag) to achieve deterministic and cyclic data transfer.
- Isochronous Real-Time (IRT): Isochronous real-time communication enables cycle times of approximately 1 ms. IRT is out of the scope of this document.

PROFINET I/O is a modular communication framework for distributed automation applications. PROFINET I/O uses cyclic data transfer to exchange data, alarms, and diagnostic information with programmable controllers, input/output (I/O) devices, and other automation controllers (for example, motion controllers).

PROFINET I/O recognizes three classes of devices:

- I/O devices: a distributed input/output device such as a sensor, an actuator, or a motion controller.
- I/O controllers: a programmable logic controller (PLC) that controls I/O devices and exchanges data such as configuration, alarms, and I/O data through an automation program. The I/O controller and the I/O supervisor exchange diagnostic information. The I/O controller shares configuration and input/output information with the I/O device and receives alarms from the I/O device.
- I/O supervisors: an engineering station, such as a human machine interface (HMI) or PC, used for commissioning, monitoring, and diagnostic analysis. The I/O supervisor exchanges diagnostic, status, control, and parameter information with the I/O device.

PROFINET Traffic Passthrough With QoS

This feature implements the ability of transparent PROFINET RT traffic over wireless on the IW6300 and ESW6300 access points. With this feature, PROFINET RT traffic, including PROFINET Class of Service (CoS) value, can be transparently relayed via Wi-Fi network.

PROFINET packet sent by PLC or I/O device contains a frame with ether-type 0x8892. On the Ethernet deployment, the PROFINET frame will be encoded in an 802.1q trunk and prioritize the traffic as high priority by setting the priority bits in the 802.1q header to

6 on Cisco switches (for example, the Cisco IE switches). The PROFINET frame on wireless network needs to follow the same priority 6 to prioritize it over regular traffic.

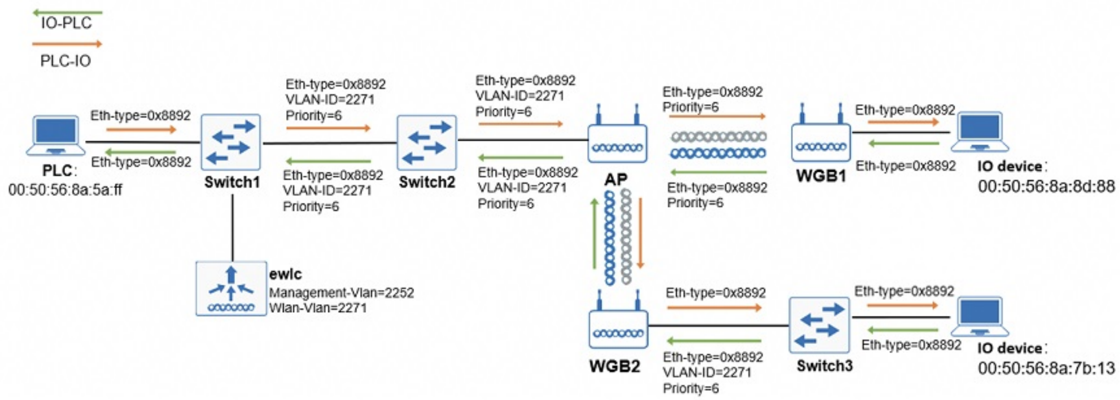
Note COS AP and WGB (IW6300 and ESW6300) will recognize ether-type 0x8892 and pass through PROFINET frame with priority 6. In the case of IOS AP and IOS WGB (IW3702) deployment, IOS WGB/AP will follow the original priority of PROFINET frame. Below use cases will focus on the COS AP/WGB behavior.

Supported platforms:

- WLC: Cisco Catalyst 9800 Series Wireless Controllers
- AP: IW6300/ESW6300, IW3702
- WGB: IOS WGB (IW3700) and COS WGB (IW6300/ESW6300)
- Software version: Cisco IOS XE 17.4.1
- AP mode:
  - Flex (local switching)
  - Flex+Bridge (local switching+ Ethernet bridging)—only for IW6300/ESW6300

WGB Stationary Use Case

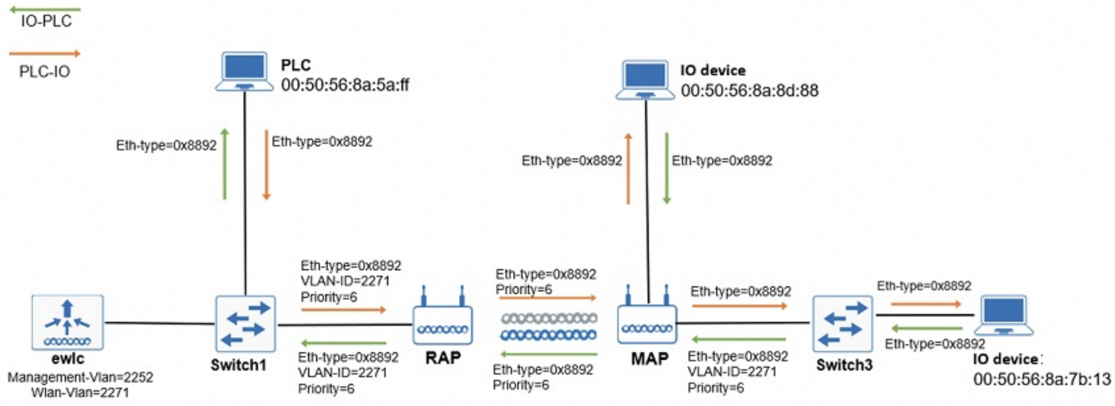
In the stationary use case, the IO device is connected to the PLC using a WGB, but it is fixed at this location.Two scenarios are supported, a switch is between WGB and IO device, or the IO device directly connects to WGB. AP and WGBs evaluate the traffic encoded with ether-type of 0x8892 and treat this traffic as higher priority than other types of traffic. When an IO device sends a frame with ether-type 0x8892, WGB sends the PROFINET packet to AP with priority 6, which is carried all along the path. The same operation is repeated when a PLC sends RT traffic back to the IO Device.



Flex+Bridge Stationary Use Case

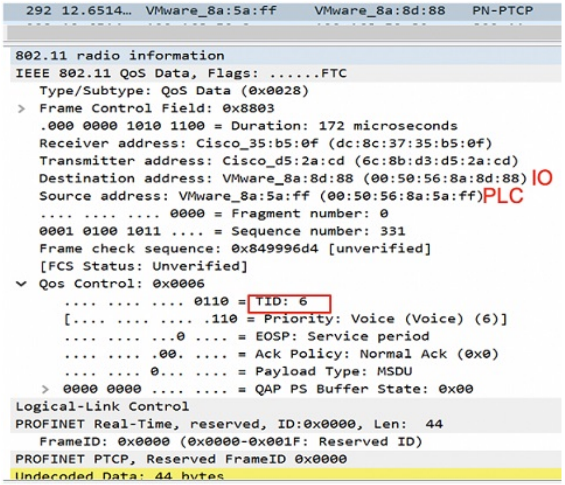
In this use case, an IO deviceis attached to MAP by ethernet bridging. The PROFINET traffic goes through the Ethernet bridging network with priority 6. RAP and MAP evaluate the traffic encoded with ether-type 0x8892 and treat as higher priority than other types of traffic. When an IO device sends a frame with ether-type 0x8892, the MAP sends the PROFINET packet to RAP with priority 6, which is carried all along the path. The same operation is repeated when a PLC sends RT channel traffic back to the IO Device.

Note The Ethernet VLAN configuration of MAP should be different from the RAP's native VLAN. The VLAN between RAP and IE switch is the VLAN set on the MAP's Ethernet port.



Profinet Traffic Over the Air

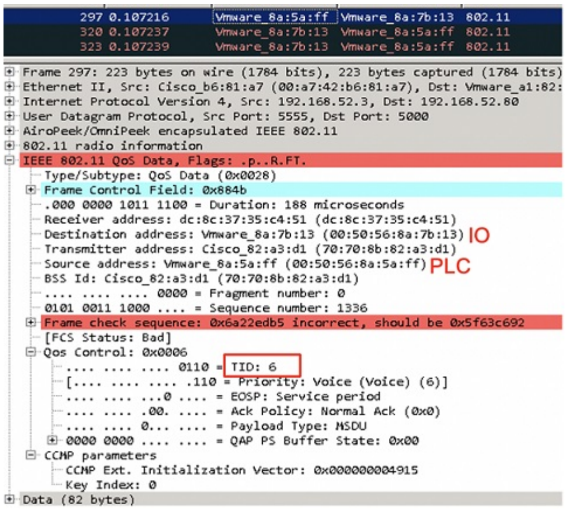
The following figure shows the PROFINET packet from AP to WGB:



```
  292 12.6514…  VMware_8a:5a:ff     VMware_8a:8d:88    PN-PTCP

802.11 radio information
IEEE 802.11 QoS Data, Flags: ......FTC
   Type/Subtype: QoS Data (0x0028)
 > Frame Control Field: 0x8803
   .000 0000 1010 1100 = Duration: 172 microseconds
   Receiver address: Cisco_35:b5:0f (dc:8c:37:35:b5:0f)
   Transmitter address: Cisco_d5:2a:cd (6c:8b:d3:d5:2a:cd)
   Destination address: VMware_8a:8d:88 (00:50:56:8a:8d:88) IO
   Source address: VMware_8a:5a:ff (00:50:56:8a:5a:ff)PLC
   .... .... .... 0000 = Fragment number: 0
   0001 0100 1011 .... = Sequence number: 331
   Frame check sequence: 0x849996d4 [unverified]
   [FCS Status: Unverified]
 ˅ Qos Control: 0x0006
      .... .... .... 0110 = TID: 6
      [.... .... .... .110 = Priority: Voice (Voice) (6)]
      .... .... ...0 .... = EOSP: Service period
      .... .... .00. .... = Ack Policy: Normal Ack (0x0)
      .... .... 0... .... = Payload Type: MSDU
    > 0000 0000 .... .... = QAP PS Buffer State: 0x00
Logical-Link Control
PROFINET Real-Time, reserved, ID:0x0000, Len:  44
   FrameID: 0x0000 (0x0000-0x001F: Reserved ID)
PROFINET PTCP, Reserved FrameID 0x0000
Undecoded Data: 44 bytes
```

The following figure shows the Profinet packet from RAP to MAP:



```
     297 0.107216   Vmware_8a:5a:ff Vmware_8a:7b:13 802.11
     320 0.107237   Vmware_8a:7b:13 Vmware_8a:5a:ff 802.11
     323 0.107239   Vmware_8a:7b:13 Vmware_8a:5a:ff 802.11

⊞ Frame 297: 223 bytes on wire (1784 bits), 223 bytes captured (1784 bits)
⊞ Ethernet II, Src: Cisco_b6:81:a7 (00:a7:42:b6:81:a7), Dst: Vmware_a1:82:
⊞ Internet Protocol Version 4, Src: 192.168.52.3, Dst: 192.168.52.80
⊞ User Datagram Protocol, Src Port: 5555, Dst Port: 5000
⊞ AiroPeek/OmniPeek encapsulated IEEE 802.11
⊞ 802.11 radio information
⊟ IEEE 802.11 QoS Data, Flags: .p..R.FT.
    Type/Subtype: QoS Data (0x0028)
  ⊞ Frame Control Field: 0x884b
    .000 0000 1011 1100 = Duration: 188 microseconds
    Receiver address: dc:8c:37:35:c4:51 (dc:8c:37:35:c4:51)
    Destination address: Vmware_8a:7b:13 (00:50:56:8a:7b:13)
    Transmitter address: Cisco_82:a3:d1 (70:70:8b:82:a3:d1)
    Source address: Vmware_8a:5a:ff (00:50:56:8a:5a:ff)
    BSS Id: Cisco_82:a3:d1 (70:70:8b:82:a3:d1)
    .... .... .... 0000 = Fragment number: 0
    0101 0011 1000 .... = Sequence number: 1336
  ⊞ Frame check sequence: 0x6a22edb5 incorrect, should be 0x5f63c692
    [FCS Status: Bad]
  ⊟ Qos Control: 0x0006
      .... .... .... 0110 = TID: 6
      [.... .... .... .110 = Priority: Voice (Voice) (6)]
      .... .... ...0 .... = EOSP: Service period
      .... .... .00. .... = Ack Policy: Normal Ack (0x0)
      .... .... 0... .... = Payload Type: MSDU
    ⊞ 0000 0000 .... .... = QAP PS Buffer State: 0x00
  ⊟ CCMP parameters
      CCMP Ext. Initialization Vector: 0x000000004915
      Key Index: 0
⊞ Data (82 bytes)
```

Wireless Controller Configuration

There is no specific configurations on the Cisco Catalyst 9800 Series Wireless Controller for this feature. For more detailed configuration, see the Cisco Catalyst 9800 configuration guide .

The following procedure provides example of wireless controller configuration from CLI and GUI:

Procedure

Step 1 Configure IP address on the AP management interface by DHCP server in the infrastructure to automatically get IP address. The following example shows the switch interface configuration which the AP is connected.

Configuration from CLI:

Example:

```
interface GigabitEthernet0/2
 description profinet-ap1
 switchport trunk native vlan 2252
 switchport mode trunk
end
```

Step 2 Create or modify a WLAN profile.

Configuration from CLI:

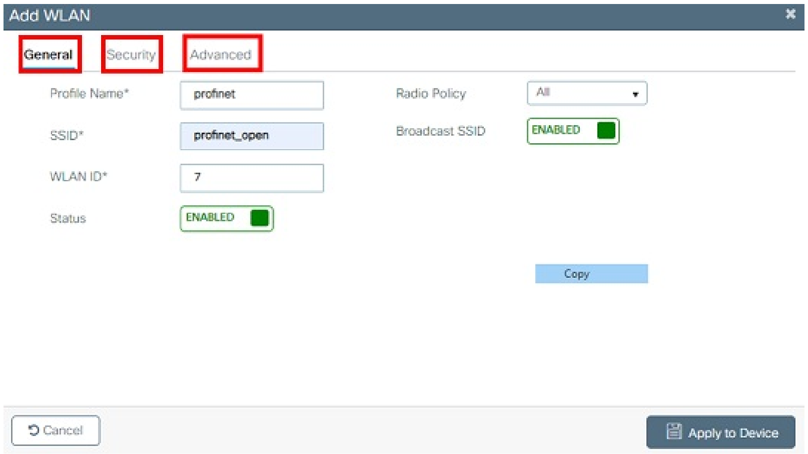
Example:

```
wlan profinet_open 1 profinet_open
 ccx aironet-iesupport
 no security ft adaptive
 no security wpa
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 no security wpa akm dot1x
 no shutdown
wlan profinet_psk 2 profinet_psk
 ccx aironet-iesupport
 security wpa psk set-key ascii 0 <key>
 no security wpa akm dot1x
 security wpa akm psk
 no shutdown
wlan profinet_1x 3 profinet_1x
 ccx aironet-iesupport
 security dot1x authentication-list profinet_1x
 no shutdown
```

Configuration from GUI:

a) Navigate to **Configuration** > **Tags & Profiles** > **WLANs**. Either select the name of a pre-existing one or click **+ Add** to add a new one.

b) Create WLAN with Profile Name, SSID, WLAN ID, and set Status to ENABLED.



Profile Name*: profinet

SSID*: profinet_open

WLAN ID*: 7

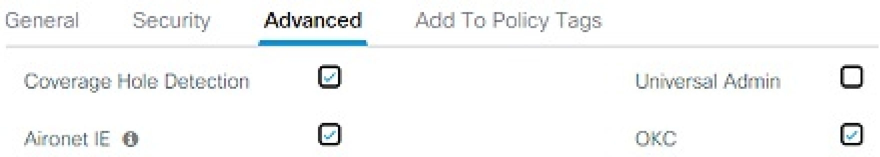
Status: ENABLED

Radio Policy: All

Broadcast SSID: ENABLED

c) Choose corresponding security.

d) Enable Aironet IE on Advanced page for WGB wired client.



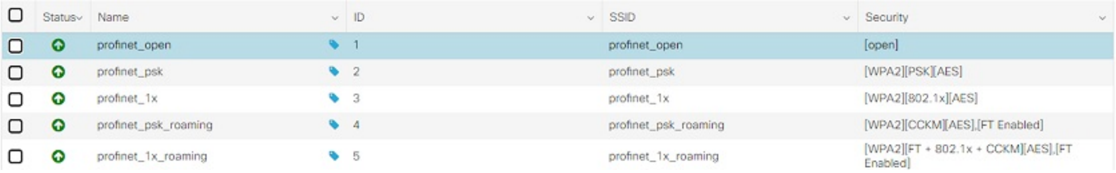
Coverage Hole Detection ☑

Universal Admin □

Aironet IE ☑

OKC ☑

You can find created WLANs listed in the following figure.



□	Status	Name	ID	SSID	Security
□	●	profinet_open	1	profinet_open	[open]
□	●	profinet_psk	2	profinet_psk	[WPA2][PSK][AES]
□	●	profinet_1x	3	profinet_1x	[WPA2][802.1x][AES]
□	●	profinet_psk_roaming	4	profinet_psk_roaming	[WPA2][CCKM][AES],[FT Enabled]
□	●	profinet_1x_roaming	5	profinet_1x_roaming	[WPA2][FT + 802.1x + CCKM][AES],[FT Enabled]

Step 3 Create Policy profile.

Configuration from CLI:

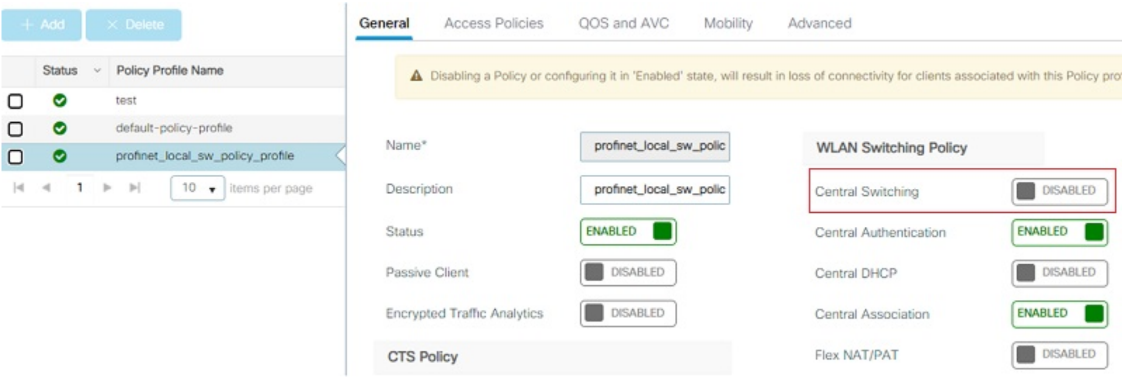
Example:

```
wireless profile policy profinet_local_sw_policy_profile
 aaa-override
 no central dhcp
 no central switching
 description profinet_local_sw_policy_profile
 no exclusionlist
 idle-timeout 30000
 nac
 session-timeout 0
 vlan VLAN2271
 wgb broadcast-tagging
 wgb vlan
 no shutdown
```

Configuration from GUI:

a) Navigate to **Configuration** > **Tags & Profiles** > **Policy**. Either select the name of a pre-existing one or click **+ Add** to add a new one.

b) Disable Central Switching on General page.



	Status	Policy Profile Name
□	✓	test
□	✓	default-policy-profile
□	✓	profinet_local_sw_policy_profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy pro

Name* profinet_local_sw_polic

Description profinet_local_sw_polic

Status ENABLED

Passive Client DISABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

WLAN Switching Policy

Central Switching DISABLED

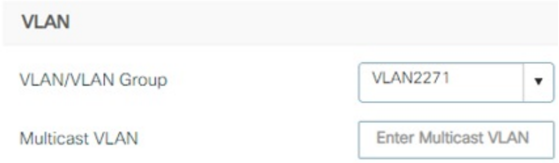
Central Authentication ENABLED

Central DHCP DISABLED

Central Association ENABLED

Flex NAT/PAT DISABLED

c) Click on Access Policies tab and choose client to be assigned with VLAN 2271.

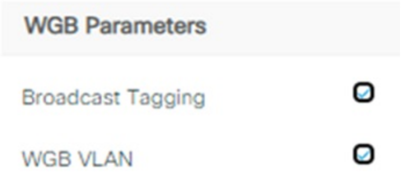


VLAN

VLAN/VLAN Group VLAN2271

Multicast VLAN Enter Multicast VLAN

d) For WGB, click on Advanced tab, and enable WGB VLAN.



WGB Parameters

Broadcast Tagging ☑

WGB VLAN ☑

Step 4 Create or modify a Policy Tag.

Configuration from CLI:

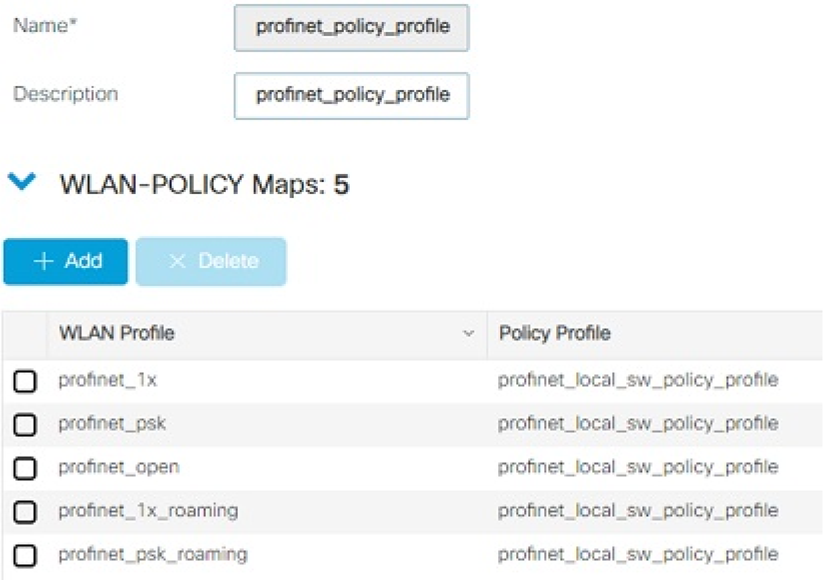
Example:

```
wireless tag policy profinet_policy_profile
 description profinet_policy_profile
 wlan profinet_1x policy profinet_local_sw_policy_profile
 wlan profinet_psk policy profinet_local_sw_policy_profile
 wlan profinet_open policy profinet_local_sw_policy_profile
 wlan profinet_1x_roaming policy profinet_local_sw_policy_profile
 wlan profinet_psk_roaming policy profinet_local_sw_policy_profile
```

Configuration from GUI:

a) Navigate to **Configuration** > **Tags & Profiles** > **Tags** > **Policy**. Either select the name of a pre-existing one or click **+ Add** to add a new one.

b) Inside the Policy Tag, click **+Add**. From the drop down list, select the WLAN Profile name you want to add to the Policy Tag and the policy profile that you want to link to it. Then click the check mark.



Name* profinet_policy_profile

Description profinet_policy_profile

WLAN-POLICY Maps: 5

	WLAN Profile	Policy Profile
□	profinet_1x	profinet_local_sw_policy_profile
□	profinet_psk	profinet_local_sw_policy_profile
□	profinet_open	profinet_local_sw_policy_profile
□	profinet_1x_roaming	profinet_local_sw_policy_profile
□	profinet_psk_roaming	profinet_local_sw_policy_profile

Step 5 Create or modify AP Join profile.

Configuration from CLI:

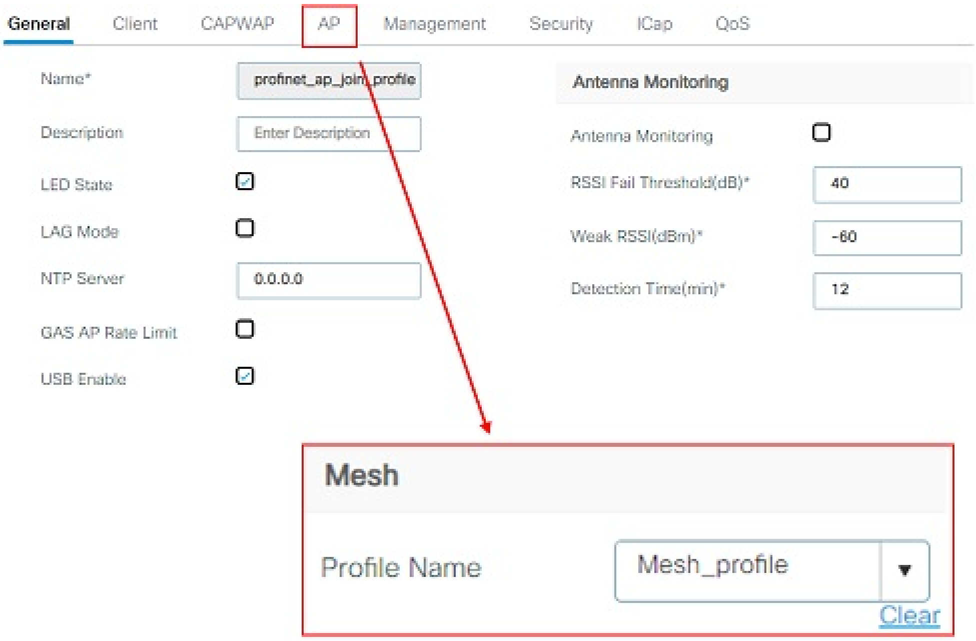
Example:

```
ap profile profinet_ap_join_profile
 mesh-profile Mesh_profile
 mgmtuser username admin password 0 <key >secret 0 <key>
 oeap
 no tcp-adjust-mss enable
```

Configuration from GUI:

a) Navigate to **Configuration** > **Tags & Profiles** > **AP Join**. Either select the name of a pre-existing one or click **+ Add** to add a new one.

b) For Flex + Bridge AP, configure mesh profile on AP page.



Name* profinet_ap_join_profile

Description Enter Description

LED State ☑

LAG Mode □

NTP Server 0.0.0.0

GAS AP Rate Limit □

USB Enable ☑

Antenna Monitoring

Antenna Monitoring □

RSSI Fail Threshold(dB)* 40

Weak RSSI(dBm)* -60

Detection Time(min)* 12

Mesh

Profile Name Mesh_profile

Step 6 Configure Flex Profile.

Configuration from CLI:

Example:

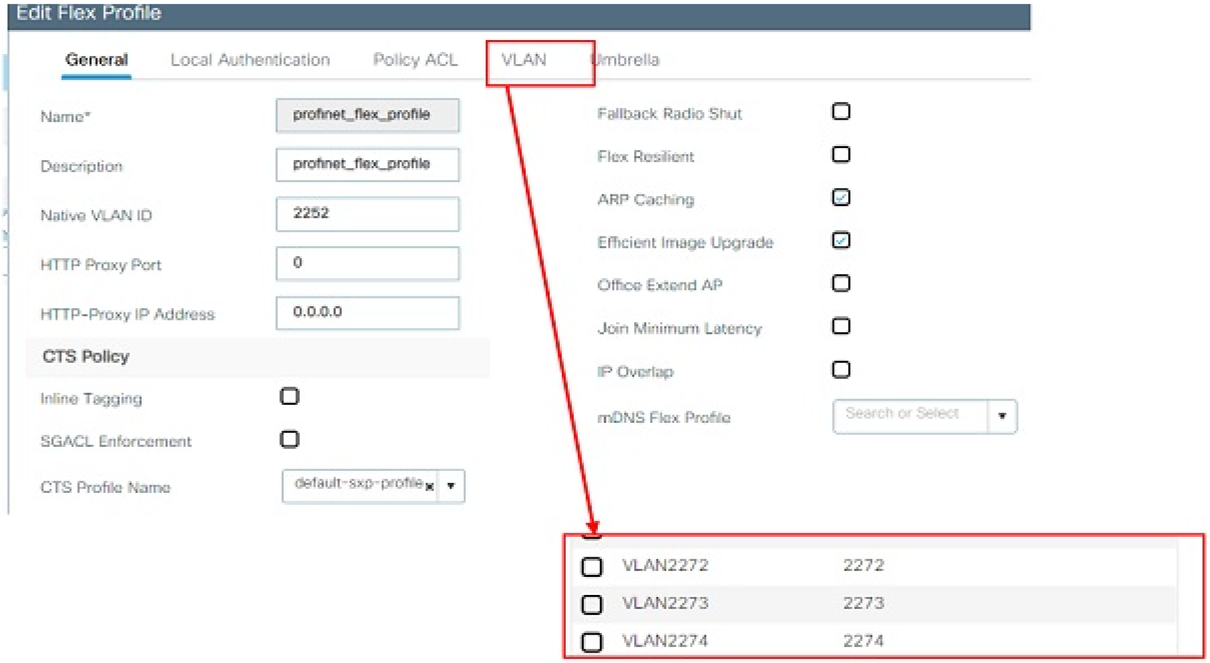
```
wireless profile flex profinet_flex_profile
 description profinet_flex_profile
native-vlan-id 2252
 vlan-name VLAN2252
  vlan-id 2252
 vlan-name VLAN2271
  vlan-id 2271
 vlan-name VLAN2272
  vlan-id 2272
 vlan-name VLAN2273
  vlan-id 2273
```

Configuration from GUI:

a) Navigate to **Configuration** > **Tags & Profiles** > **Flex**. Either select the name of a pre-existing one or click **+ Add** to add a new one.

b) Define a name for your Flex profile and specify the AP's VLAN (Native VLAN ID). Configure AP management vlan 2252 on Native VLAN ID.

c) Navigate to the VLAN tab and specify the needed VLAN. Add non-native client vlan 2272 on VLAN page.



Name* profinet_flex_profile

Description profinet_flex_profile

Native VLAN ID 2252

HTTP Proxy Port 0

HTTP-Proxy IP Address 0.0.0.0

CTS Policy

Inline Tagging □

SGACL Enforcement □

CTS Profile Name default-sxp-profile

Fallback Radio Shut □

Flex Resilient □

ARP Caching ☑

Efficient Image Upgrade ☑

Office Extend AP □

Join Minimum Latency □

IP Overlap □

mDNS Flex Profile Search or Select

□	VLAN2272	2272
□	VLAN2273	2273
□	VLAN2274	2274

Step 7 Configure Site Tag.

Configuration from CLI:

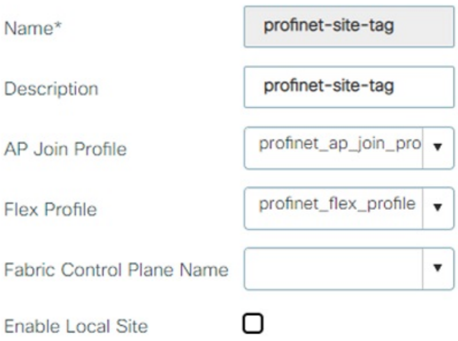
Example:

```
wireless tag site profinet-site-tag
 ap-profile profinet_ap_join_profile
 description profinet-site-tag
 flex-profile profinet_flex_profile
 no local-site
```

Configuration from GUI:

a) Navigate to **Configuration** > **Tags & Profiles** > **Tags** > **Site**. Either select the name of a pre-existing one or click **+ Add** to add a new one.

b) Inside the Site Tag, disable Enable Local Site option. Once it is disabled, you can also select the Flex Profile. Then click **Save & Apply to Device**.



Name* profinet-site-tag

Description profinet-site-tag

AP Join Profile profinet_ap_join_pro

Flex Profile profinet_flex_profile

Fabric Control Plane Name

Enable Local Site □

Step 8 Policy Tag Assignment to AP.

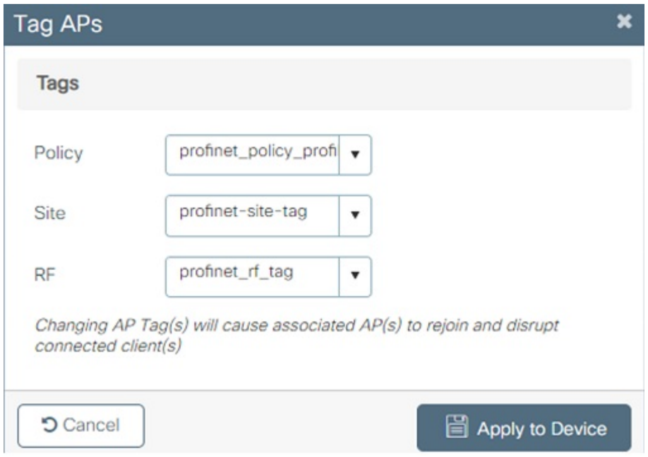
Configuration from CLI:

Example:

```
ap <ethernet-mac-addr>
 policy-tag profinet_policy_profile
 rf-tag profinet_rf_tag
 site-tag profinet-site-tag
```

Configuration from GUI:

Navigate to **Configuration** > **Wireless** > **Access Points** > **AP name** > **General** > **Tags**. From the **Site** dropdown list, select the desired Tags and click **Apply to Device**. Or navigate to **Configuration** > **Wireless Setup** > **Advanced** > **Start Now** to configure multiple APs at the same time.



Tag APs

Tags

Policy: profinet_policy_profi

Site: profinet-site-tag

RF: profinet_rf_tag

Changing AP Tag(s) will cause associated AP(s) to rejoin and disrupt connected client(s)

IOS WGB Configuration

There is no specific configuration for this feature on IOS WGB.

Security: Open

```
dot11 ssid <profinet_open>
  authentication open
  no ids mfp client
interface Dot11Radio0
  no ip address
  ssid <profinet_open>
  station-role workgroup-bridge
  bridge-group 1
  bridge-group 1 spanning-disabled
```

Security: WPA2 PSK

```
dot11 ssid <profinet_psk>
  authentication open
  authentication key-management wpa version 2
  wpa-psk ascii <PASSWORD>
  no ids mfp client
```

```
interface Dot11Radio0
  no ip address
  ssid <profinet_psk>
  encryption mode ciphers aes-ccm
  station-role workgroup-bridge
  bridge-group 1
  bridge-group 1 spanning-disabled
```

Security: 802.1x cckm

```
dot11 ssid <profinet_1x_cckm>
  authentication open eap eap
  authentication network-eap eap
  authentication key-management cckm
  dot1x credentials <profinet_1x>
  dot1x eap profile <profinet_1x_fast>
  no ids mfp client
eap profile <profinet_1x_fast>
  method fast
dot1x credentials <profinet_1x>
  username profinet_user1
  password 7  <password>
interface Dot11Radio0
  no ip address
  ssid <profinet_1x_cckm>
  encryption mode ciphers aes-ccm
  station-role workgroup-bridge
  bridge-group 1
  bridge-group 1 spanning-disabled
```

COS WGB Configuration

There is no specific configuration for this feature on COS WGB.

Open

```
configure ssid-profile <profile-name> ssid <ssid-name> authentication open
```

PSK

```
configure ssid-profile <profile-name> ssid <ssid-name> authentication psk <key> key-management <wpa2/dot11r>
```

802.1x

```
Configure dot1x credentials <dot1x-profile-name> <username/delete> <user-name> password <password>
Configure eap-profile <eap-profile-name> method <fast/leap/peap/tls>
Configure eap-profile <eap-profile-name> dot1x-credentials <dot1x-profile-name>
Configure ssid-profile <ssid-profile-name> ssid <ssid-name> authentication eap eap-profile <eap-profile-name>
 key-management <wpa2/dot11r>
```

Troubleshooting

The following command output shows the Profinet packet count on COS AP in Flex local switching mode:

```
#show dot11 qos
profinet-ap1#show dot11 qos
......
Profinet packet
Downstream: 10 <-Downstream profinet traffic, received from radio side
Upstream:   10 <-Upstream profinet traffic, received from wired side
```

The following command output shows the Profinet packet count on COS AP in Flex+Bridge local switching mode:

```
#show dot11 qos
profinet-ap1#show dot11 qos
......
Profinet packet
Downstream: 10
Upstream:   10
==========
  rx from wireless client: 5 <-Upstream profinet traffic, received from wireless client
  rx from non root port:   5 <-Upstream profinet traffic, received from LAN port
```

The following command output shows the Profinet packet count on COS WGB:

```
#show dot11 qos
......
Profinet packet
Downstream: 10 <-Downstream profinet traffic, received from radio side
Upstream:   10 <-Upstream profinet traffic, received from wired side
```

To clear the counter of Profinet packet on COS AP or WGB, use the **clear counters profinet** command.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.