

# Configuration et validation des configurations WGB (Workgroup Bridge)

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Composants utilisés](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérifier](#)

[Dépannage](#)

---

## Introduction

Ce document décrit la procédure de configuration du pont de groupe de travail (WGB) sur un point d'accès (AP) Cisco et de validation des configurations.

## Conditions préalables

### Composants utilisés

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

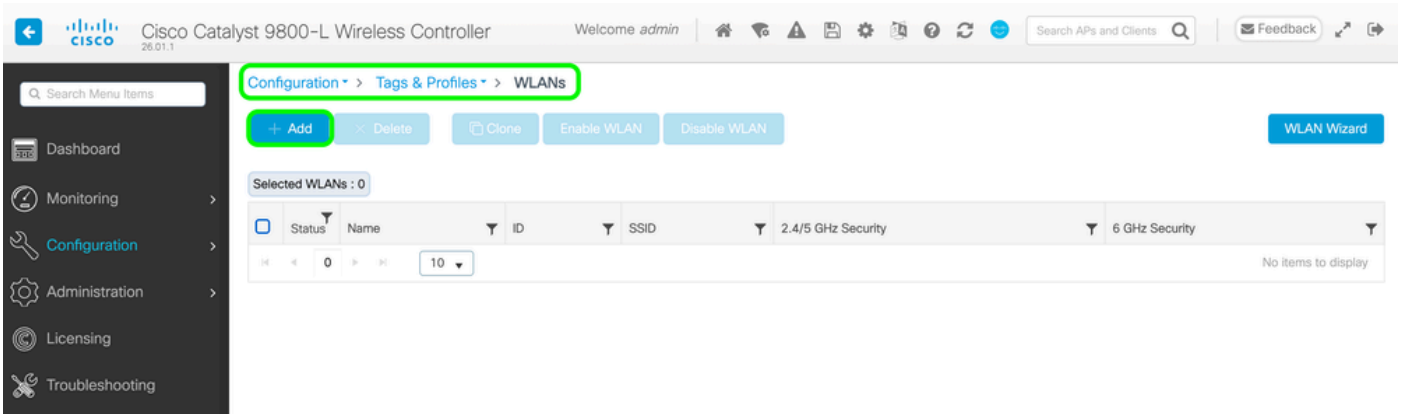
## Configurer

### Diagramme du réseau

### Configurations

## Étape 1 : configuration d'un WLAN sur le WLC à utiliser pour le WGB

Sur le WLC, accédez à Configuration > Tags & Profiles > WLANs > cliquez sur + Add comme indiqué dans l'image.



Donnez un nom à votre WLAN et assurez-vous qu'il est activé.

The 'Add WLAN' configuration form is shown with three tabs: General, Security, and Advanced. The General tab is active. The form contains the following fields and controls:

- Profile Name\*: WGB (highlighted with a green box)
- SSID\*: WGB
- WLAN ID\*: 1
- Status: ENABLED (checkbox checked, highlighted with a green box)
- Broadcast SSID: ENABLED (checkbox checked)
- Wi-Fi 6E Compatibility: 1/2 requirements met
- Wi-Fi 7 Compatibility: 0/3 requirements met, 0/3 bands enabled
- Radio Policy (i):
  - Show slot configuration
  - 6 GHz Status: ENABLED (checkbox checked, highlighted with a red box)
  - 5 GHz Status: ENABLED (checkbox checked)
  - 2.4 GHz Status: ENABLED (checkbox checked)
  - 802.11b/g Policy: 802.11b/g (dropdown menu)

At the bottom of the form, there are two buttons: 'Cancel' and 'Apply to Device'.

Accédez à l'onglet Security et sélectionnez les paramètres de sécurité souhaités pour le SSID WGB créé. Dans le cadre de ce document, un SSID ouvert a été créé. Néanmoins, d'autres options de sécurité peuvent également être créées.



Avertissement : Assurez-vous que les paramètres de sécurité correspondent entre le SSID sur le WLC et le profil SSID du WGB AP (ce profil est configuré plus loin dans le document sur le WGB AP).

### Add WLAN ✕

General **Security** Advanced

**Layer2** Layer3 AAA

WPA + WPA2     WPA2 + WPA3     WPA3     Static WEP     None

MAC Filtering

OWE Transition Mode     Transition Mode WLAN ID\*

Lobby Admin Access

Accédez à l'onglet Advanced et vérifiez que l'IE Aironet CCX est activé. Cliquez ensuite sur Apply to Device.

**Add WLAN**

General Security **Advanced**

Coverage Hole Detection  Universal Admin

**CCX Aironet IE**  OKC

Advertise AP Name  Load Balance

P2P Blocking Action  Band Select

Multicast Buffer  IP Source Guard

Media Stream Multicast-direct  WMM Policy

11ac MU-MIMO  mDNS Mode

Wi-Fi to Cellular Steering

Wi-Fi Alliance Agile Multiband

Fastlane+ (ASR)

Defer Priority

Deny LAA (RCM) clients

6 GHz Client Steering

Latency Measurements Announcements

Scan Defer Time

Off Channel Scanning Defer

Assisted Roaming (11k)

Une fois le profil WLAN créé, créez un profil de stratégie pour ce WLAN. Pour cela, accédez à Configuration > Tags & Profiles > Policy > cliquez sur + Add.

Cisco Catalyst 9800-L Wireless Controller Welcome admin

Configuration > Tags & Profiles > Policy

+ Add Delete Clone

Selected Rows : 0

| Admin Status                        | Associated Policy Tags | Policy Profile Name    | Description            |
|-------------------------------------|------------------------|------------------------|------------------------|
| <input checked="" type="checkbox"/> |                        | default-policy-profile | default policy profile |

10 items per page 1 - 1 of 1 Items

Entrez un nom pour le profil de stratégie dans l'onglet Général et assurez-vous que le profil de stratégie est activé.

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

**General**   Access Policies   QOS and AVC   Mobility   Advanced

Name\*

WGB\_profile

Description

Enter Description

Status

ENABLED

Passive Client

DISABLED

IP MAC Binding

ENABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

2-65519

WLAN Switching Policy

Central Switching

ENABLED

Central Authentication

ENABLED

Central DHCP

ENABLED

Flex NAT/PAT

DISABLED

↶ Cancel

📄 Apply to Device

Accédez à l'onglet Access Policies et attribuez un VLAN à votre profil de stratégie.

## Add Policy Profile



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

General **Access Policies** QOS and AVC Mobility Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

### WLAN Local Profiling

Global State of Device Classification **Disabled** ⓘ

Local Subscriber Policy Name

### VLAN

VLAN/VLAN Group **BACKBONE-V...** ⓘ

Multicast VLAN

*Note : Selecting a VLAN Group is a valid config only for Central Switching SSIDs. Do not use with SSIDs enabled for Flex Local Switching*

### WLAN ACL

IPv4 ACL

IPv6 ACL

### URL Filters ⓘ

Pre Auth

Post Auth

↶ Cancel

📄 Apply to Device

Accédez à l'onglet Advanced, faites défiler jusqu'à la section WGB Parameters et sélectionnez les options Broadcast Tagging et WGB VLAN. Cliquez ensuite sur Apply to Device.

### Add Policy Profile

DHCP Server VRF

Show more >>>

**AAA Policy**

Allow AAA Override

NAC State

Policy Name

Accounting List

Interim Accounting  ENABLED

**WGB Parameters**

Broadcast Tagging

WGB VLAN

**Policy Proxy Settings**

ARP Proxy  DISABLED

IPv6 Proxy

DNS Layer Security Parameter Map

Flex DHCP Option for DNS  ENABLED

Flex DNS Traffic Redirect  IGNORE

**WLAN Flex Policy**

VLAN Central Switching

Split MAC ACL

**Air Time Fairness Policies**

2.4 GHz Policy

5 GHz Policy

**EoGRE Tunnel Profiles**

Tunnel Profile

Ensuite, mappez le profil de stratégie au profil WLAN. Accédez à Configuration > Tags & Profiles > Tags > cliquez sur + Add.

Cisco Catalyst 9800-L Wireless Controller | Welcome admin

Configuration > Tags & Profiles > Tags

Policy | Site | RF | AP

Selected Rows : 0

| Policy Tag Name                             | Description        |
|---|--------------------|
| <input type="checkbox"/> default-policy-tag | default policy-tag |

10 items per page | 1 - 1 of 1 Items

Entrez un nom pour la balise de stratégie. Cliquez ensuite sur + Ajouter.

**Add Policy Tag** ✕

Name\*

Description

▼ WLAN-POLICY Maps : 0

+ Add ✕ Delete

| WLAN Profile                           | Policy Profile |
|--|----------------|
| No records available.                  |                |
| ⏪ ⏩ 10 items per page 0 - 0 of 0 items |                |

> RLAN-POLICY Maps : 0

↶ Cancel
📄 Apply to Device

Faites défiler jusqu'à la section Map WLAN and Policy et sélectionnez les profils de stratégie WLAN précédemment créés. Cliquez ensuite sur ✓.

**Add Policy Tag** ✕

+ Add ✕ Delete

| WLAN Profile                           | Policy Profile |
|--|----------------|
| No records available.                  |                |
| ⏪ ⏩ 10 items per page 0 - 0 of 0 items |                |

**Map WLAN and Policy**

WLAN Profile\*

✕ ▼
📄

Policy Profile\*

✕ ▼
📄

✕
✓

> RLAN-POLICY Maps : 0

↶ Cancel
📄 Apply to Device

Après vous être assuré que le mappage a été ajouté à la table, cliquez sur Apply to Device.

Add Policy Tag ✕

▼ WLAN-POLICY Maps : 1

+ Add
✕ Delete

|                          | WLAN Profile |  | Policy Profile |
|--------------------------|--------------|--|----------------|
| <input type="checkbox"/> | WGB          |  | WGB_policy     |

⏪ ⏩ 1 ⏪ ⏩
10 items per page
1 - 1 of 1 Items

Map WLAN and Policy

WLAN Profile\*

Policy Profile\*

✕
✓

↶ Cancel
Apply to Device

## Étape 2 : configuration d'un point d'accès en mode WGB

Convertissez le point d'accès CAPWAP en type WGB.

```
WGB_AP#ap-type workgroup-bridge
```

Configurez une adresse IP pour le point d'accès WGB.

Pour une adresse IP DHCP :

```
WGB_AP#configure ap address ipv4 dhcp
```

Pour une adresse IP statique :

```
WGB_AP#configure ap address ipv4 static
```

Configurez un profil SSID sur le point d'accès WGB.

```
WGB_AP#configure ssid-profile
```

```
ssid
```

```
authentication
```

Connectez le profil SSID à une interface radio.

```
WGB_AP#configure dot11Radio
```

```
mode wgb ssid-profile
```

Activez la radio configurée sur le point d'accès WGB.

```
WGB_AP#configure dot11Radio 1 enable
```

Ensuite, le point d'accès WGB se connecte au point d'accès racine. Il est possible de vérifier à partir du WLC que la configuration a réussi.

Sur le WLC, l'AP WGB est considéré comme un client sans fil connecté. Dans le même tableau, les clients filaires qui sont connectés via le point d'accès WGB sont également visibles.

## Exemple :

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller interface. The breadcrumb navigation is 'Monitoring > Wireless > Clients'. The 'Clients' tab is selected. A table displays two clients:

| Client MAC Address | IPv4 Address | IPv6 Address | AP Name       | Slot ID | SSID | WLAN ID | Client Type      |
|--------------------|--------------|--------------|---------------|---------|------|---------|------------------|
| [Redacted]         | [Redacted]   | [Redacted]   | AP-[Redacted] | 1       | WGB  | 1       | WLAN (WGB)       |
| [Redacted]         | N/A          | N/A          | AP-[Redacted] | 1       | WGB  | 1       | WLAN (WGB Wired) |



Conseil : Avant de procéder aux configurations sur le point d'accès WGB assurez-vous que le point d'accès a un code de pays configuré dessus (peut être vérifié avec la commande "show controllers dot11Radio"), par exemple :

```
WGB_AP#show controllers dot11Radio 1
wifi1 Link encap:Ethernet HWaddr XX:XX:XX:XX:XX:XX
BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:2699
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
```

Radio Info Summary:

```
=====
Radio: 5.0GHz
Carrier Set: (-E) Belgium ( BE)
```



Conseil : Si le code de pays n'est pas configuré, convertissez l'AP en mode CAPWAP, joignez-le à un WLC et assurez-vous que le code de pays est configuré. Ensuite, convertissez le point d'accès en mode WGB et continuez avec les configurations.

## Vérifier

Vous pouvez utiliser ces commandes pour vérifier les configurations actuelles.

Sur l'AP WGB :

#show wgb ssid

Exemple de résultat de configuration réussie :

Configured SSIDs details:

| SSID-Profile     | SSID  | Authentication | DTIM |
|------------------|-------|----------------|------|
| WGB_ssid_profile | "WGB" | OPEN           | 1    |

#show wgb dot11 associations

Exemple de résultat de configuration réussie :

Uplink Radio ID : 1  
Uplink Radio MAC : XX:XX:XX:XX:XX:XX  
SSID Name : WGB  
Connected Duration : 0 hours, 2 minutes, 14 seconds  
Parent AP Name : APXXXX.XXXX.XXXX  
Parent AP MAC : XX:XX:XX:XX:XX:XX  
Uplink State : CONNECTED  
Auth Type : OPEN  
Dot11 type : 11ax  
Channel : 112  
Bandwidth : 40 MHz  
Current Datarate (Tx/Rx) : 309/195 Mbps  
Max Datarate : 1147 Mbps  
RSSI : 65  
IP : XX.XX.XX.XXX/24  
Default Gateway : XX.XX.XX.XXX  
IPV6 : ::/128  
Assoc timeout : 5000 Msec  
Auth timeout : 5000 Msec  
Dhcp timeout : 60 Sec  
Country-code : BE

#show wgb event all

## Dépannage

Collecter les débogages

Sur l'AP WGB :

Après avoir appliqué les configurations, si l'AP WGB ne se connecte pas à l'AP racine, activez le débogage pour obtenir plus de détails sur la raison de la défaillance :

```
#debug wgb uplink all
```

Exemple de résultat de connexion réussie :

```
Jun 19 12:57:39 WGB_AP kernel: [*06/19/2026 12:57:39.0356] DOT11_UPLINK_EV: Scan Started ON SLOT 1
Jun 19 12:57:39 WGB_AP kernel: [*06/19/2026 12:57:39.0357] DOT11_UPLINK_EV: Uplink state changed [DOT11
Jun 19 12:57:39 WGB_AP kernel: [*06/19/2026 12:57:39.0358] DOT11_UPLINK_EV: Set BH root port(hop 00:00:
Jun 19 12:57:39 WGB_AP kernel: [*06/19/2026 12:57:39.0358] DOT11_UPLINK_SCAN: Uplink Scan Started in Do
Jun 19 12:57:39 WGB_AP kernel: [*06/19/2026 12:57:39.0362] DOT11_UPLINK_SCAN: Enable passive scan on ch
Jun 19 12:57:39 WGB_AP kernel: [*06/19/2026 12:57:39.0632] Radio configuration has been saved successf
Jun 19 12:57:39 WGB_AP kernel: [*06/19/2026 12:57:39.0633]
Jun 19 12:57:39 WGB_AP kernel: [*06/19/2026 12:57:39.1492] DOT11_UPLINK_SCAN: Enable passive scan on ch
Jun 19 12:57:39 WGB_AP kernel: [*06/19/2026 12:57:39.2895] DOT11_UPLINK_SCAN: Enable passive scan on ch
Jun 19 12:57:39 WGB_AP kernel: [*06/19/2026 12:57:39.4298] DOT11_UPLINK_SCAN: Enable passive scan on ch
Jun 19 12:57:39 WGB_AP kernel: [*06/19/2026 12:57:39.4933] DOT11_UPLINK_SCAN:[*06/19/2026 13:17:00.6489
[*06/19/2026 13:17:00.6494] DOT11_UPLINK_EV: parent_rssi: -65, configured low rssi: -70
Rcvd Beacon from XX:XX:XX:XX:XX:XX channel 112 Time 36143
Jun 19 12:57:39 WGB_AP kernel: [*06/19/2026 12:57:39.4934] DOT11_UPLINK_SCAN: Received Beacon and going
Jun 19 12:57:39 WGB_AP kernel: [*06/19/2026 12:57:39.4934] DOT11_UPLINK_SCAN: Sending probe request on
Jun 19 12:57:39 WGB_AP kernel: [*06/19/2026 12:57:39.4934] WGB Classifier: Dot11UplinkClassifier: Downs
Jun 19 12:57:39 WGB_AP kernel: [*06/19/2026 12:57:39.4935] WGB Classifier: Dot11UplinkClassifier: Tx se
Jun 19 12:57:39 WGB_AP kernel: [*06/19/2026 12:57:39.4952] DOT11_UPLINK_SCAN: Rcvd Probe Response from
Jun 19 12:57:39 WGB_AP kernel: [*06/19/2026 12:57:39.4952] DOT11_UPLINK_SCAN: WGB_SCAN_STATUS: Received
Jun 19 12:57:39 WGB_AP kernel: [*06/19/2026 12:57:39.5266] DOT11_UPLINK_SCAN: Enable passive scan on ch
Jun 19 12:57:39 WGB_AP kernel: [*06/19/2026 12:57:39.6657] DOT11_UPLINK_SCAN: Enable passive scan on ch
Jun 19 12:57:39 WGB_AP kernel: [*06/19/2026 12:57:39.8046] DOT11_UPLINK_SCAN: Enable passive scan on ch
Jun 19 12:57:39 WGB_AP kernel: [*06/19/2026 12:57:39.9436] DOT11_UPLINK_SCAN: Enable passive scan on ch
Jun 19 12:57:40 WGB_AP kernel: [*06/19/2026 12:57:40.0827] DOT11_UPLINK_SCAN: Enable passive scan on ch
Jun 19 12:57:40 WGB_AP kernel: [*06/19/2026 12:57:40.2218] DOT11_UPLINK_SCAN: Enable passive scan on ch
Jun 19 12:57:40 WGB_AP kernel: [*06/19/2026 12:57:40.3609] DOT11_UPLINK_SCAN: Enable passive scan on ch
Jun 19 12:57:40 WGB_AP kernel: [*06/19/2026 12:57:40.4983] DOT11_UPLINK_SCAN: End of channel list
Jun 19 12:57:40 WGB_AP kernel: [*06/19/2026 12:57:40.4984] DOT11_UPLINK_SCAN: An AP responded, try to a
Jun 19 12:57:40 WGB_AP kernel: [*06/19/2026 12:57:40.4984] DOT11_UPLINK_SCAN: Uplink Scan stopped in Do
Jun 19 12:57:40 WGB_AP kernel: [*06/19/2026 12:57:40.4984] DOT11_UPLINK_SCAN: Choosing best AP
Jun 19 12:57:40 WGB_AP kernel: [*06/19/2026 12:57:40.4985] DOT11_UPLINK_SCAN: Selected best AP : XX:XX
Jun 19 12:57:40 WGB_AP kernel: [*06/19/2026 12:57:40.4985] DOT11_UPLINK_SCAN: Best AP : XX:XX:XX:XX:XX:
Jun 19 12:57:40 WGB_AP kernel: [*06/19/2026 12:57:40.4985] DOT11_UPLINK_SCAN: HD IE not present!
Jun 19 12:57:40 WGB_AP kernel: [*06/19/2026 12:57:40.4986] DOT11_UPLINK_SCAN: WME capable 1
Jun 19 12:57:40 WGB_AP kernel: [*06/19/2026 12:57:40.4986] DOT11_UPLINK_SCAN: Scan done.Starting Authen
Jun 19 12:57:40 WGB_AP kernel: [*06/19/2026 12:57:40.4987] DOT11_UPLINK_EV: Uplink state changed [DOT11
Jun 19 12:57:40 WGB_AP kernel: [*06/19/2026 12:57:40.4988] DOT11_UPLINK_EV: Set BH root port(hop 00:00:
Jun 19 12:57:40 WGB_AP kernel: [*06/19/2026 12:57:40.4995] DOT11_UPLINK_EV: existing channel 140, targe
Jun 19 12:57:40 WGB_AP kernel: [*06/19/2026 12:57:40.5001] DOT11_UPLINK_EV: existing channel 140, targe
Jun 19 12:57:40 WGB_AP kernel: [*06/19/2026 12:57:40.5168] DOT11_UPLINK_CONFIG: get tx_pow_lvl 1 by txp
Jun 19 12:57:40 WGB_AP kernel: [*06/19/2026 12:57:40.5433] DOT11_UPLINK_EV: Channel event on slot 1 cha
Jun 19 12:57:40 WGB_AP kernel: [*06/19/2026 12:57:40.5541] DOT11_UPLINK_EV: Channel event on slot 1 cha
Jun 19 12:57:40 WGB_AP kernel: [*06/19/2026 12:57:40.5655] DOT11_UPLINK_EV: Handling auth delay for cha
Jun 19 12:57:40 WGB_AP kernel: [*06/19/2026 12:57:40.5718] DOT11_UPLINK_CONFIG: get tx_pow_lvl 1 by txp
Jun 19 12:57:40 WGB_AP kernel: [*06/19/2026 12:57:40.5719] DOT11_UPLINK_EV: Starting Connection (uplink
Jun 19 12:57:40 WGB_AP kernel: [*06/19/2026 12:57:40.5719] WGB_UPLINK_SEC: New roamed parent : XX:XX:XX
Jun 19 12:57:40 WGB_AP kernel: [*06/19/2026 12:57:40.5719] WGB_UPLINK_SEC: WPAS process does not exist
Jun 19 12:57:40 WGB_AP kernel: [*06/19/2026 12:57:40.5719] DOT11_UPLINK_EV: Uplink state changed [DOT11
Jun 19 12:57:40 WGB_AP kernel: [*06/19/2026 12:57:40.5721] WGB Classifier: Dot11UplinkClassifier: Downs
Jun 19 12:57:40 WGB_AP kernel: [*06/19/2026 12:57:40.5721] WGB Classifier: Dot11UplinkClassifier: Tx se
```

Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.5723] DOT11\_UPLINK\_EV: Auth request sent!  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.5753] DOT11\_UPLINK\_EV: Channel event on slot 1 cha  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.5753] DOT11\_UPLINK\_EV: Channel 112 set response fr  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.5764] DOT11\_UPLINK\_EV: Channel event on slot 1 cha  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.5765] DOT11\_UPLINK\_EV: Channel 112 set response fr  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.6035] WGB Classifier: Dot11UplinkClassifier: Rx se  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.6036] DOT11\_UPLINK\_EV: Auth Response (uplink)addr1  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.6036] DOT11\_UPLINK\_EV: Uplink state changed [DOT11  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.6038] DOT11\_UPLINK\_EV: Assoc. Req. addr1[XX:XX:XX:  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.6038] DOT11\_UPLINK\_EV: set\_ht\_cap\_ie\_fields: Addin  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.6038] DOT11\_UPLINK\_EV: set\_vht\_cap\_ie\_fields: Addi  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.6038] DOT11\_UPLINK\_EV: VhtCapInfo=865069494  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.6039] DOT11\_UPLINK\_EV: set\_he\_cap\_ie\_fields: Addin  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.6039] DOT11\_UPLINK\_EV: set\_he\_cap\_ie\_fields: Setti  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.6039] DOT11\_UPLINK\_EV: Added system name : in ass  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.6039] DOT11\_UPLINK\_EV: Added static IP address : X  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.6040] WGB Classifier: Dot11UplinkClassifier: Downs  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.6040] WGB Classifier: Dot11UplinkClassifier: Tx se  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.6041] DOT11\_UPLINK\_EV: Sent Assoc. Req. (uplink)ad  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.6100] WGB Classifier: Dot11UplinkClassifier: Rx se  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.6101] DOT11\_UPLINK\_EV: Assoc Response (uplink)addr  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.6102] DOT11\_UPLINK\_EV: Uplink state changed [DOT11  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.6108] DOT11\_UPLINK\_EV: Set BH root port(hop XX:XX:  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.6118] wlan: [10239:I:ANY] ieee80211\_ucfg\_setparam\_  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.6124] DOT11\_UPLINK\_EV: Set BH root port(hop XX:XX:  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.6130] DOT11\_UPLINK\_EV: Static IP address configure  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.6131] DOT11\_UPLINK\_EV: Uplink state changed [DOT11  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.6241] route: SIOCADDRT: File exists  
Jun 19 12:57:40 WGB\_AP odhcp6c[186731]: in timer\_init.  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.6761] odhcp6c[186731]: in timer\_init.  
Jun 19 12:57:40 WGB\_AP odhcp6c[186735]: (re)starting transaction on srcr2  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.6782] DOT11\_UPLINK\_EV: Odhcp6c process started  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.6784] DOT11-UPLINK\_ESTABLISHED: Interface Dot11Rad  
Jun 19 12:57:40 WGB\_AP kernel: [\*06/19/2026 12:57:40.6786] DOT11\_UPLINK\_EV: Peer assoc event received f  
Jun 19 12:57:41 WGB\_AP odhcp6c[186735]: Starting SOLICIT transaction (timeout 4294967295s, max rc 0)  
Jun 19 12:57:41 WGB\_AP odhcp6c[186735]: odhcp6c\_update\_entry state = 16, valid = 1800, preferred = 1800  
Jun 19 12:57:41 WGB\_AP odhcp6c[186735]: odhcp6c\_update\_entry state = 16, valid = 2592000, preferred = 6  
Jun 19 12:57:41 WGB\_AP odhcp6c[186735]: odhcp6c\_update\_entry state = 17, valid = 2592000, preferred = 6  
Jun 19 12:57:43 WGB\_AP kernel: [\*06/19/2026 12:57:43.6386] ip6\_port srcr2, ip6local XXXX:XXXX:XXXX:XXX  
Jun 19 12:58:00 WGB\_AP kernel: [\*06/19/2026 12:58:00.6134] DOT11\_UPLINK\_EV: Calling RSSI get for XX:XX:  
Jun 19 12:58:00 WGB\_AP kernel: [\*06/19/2026 12:58:00.6138] DOT11\_UPLINK\_EV: parent\_rssi: -63, configure  
Jun 19 12:58:20 WGB\_AP kernel: [\*06/19/2026 12:58:20.6140] DOT11\_UPLINK\_EV: Calling RSSI get for XX:XX:  
Jun 19 12:58:20 WGB\_AP kernel: [\*06/19/2026 12:58:20.6145] DOT11\_UPLINK\_EV: parent\_rssi: -63, configure  
Jun 19 12:58:40 WGB\_AP kernel: [\*06/19/2026 12:58:40.6147] DOT11\_UPLINK\_EV: Calling RSSI get for XX:XX:  
Jun 19 12:58:40 WGB\_AP kernel: [\*06/19/2026 12:58:40.6152] DOT11\_UPLINK\_EV: parent\_rssi: -64, configure  
Jun 19 12:59:00 WGB\_AP kernel: [\*06/19/2026 12:59:00.6154] DOT11\_UPLINK\_EV: Calling RSSI get for XX:XX:  
Jun 19 12:59:00 WGB\_AP kernel: [\*06/19/2026 12:59:00.6158] DOT11\_UPLINK\_EV: parent\_rssi: -64, configure  
Jun 19 12:59:20 WGB\_AP kernel: [\*06/19/2026 12:59:20.6161] DOT11\_UPLINK\_EV: Calling RSSI get for XX:XX:

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.