

Configurazione e convalida delle configurazioni di Workgroup Bridge (WGB)

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritta la procedura per configurare un bridge di gruppi di lavoro (WGB) su un access point Cisco e per convalidare le configurazioni.

Prerequisiti

Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

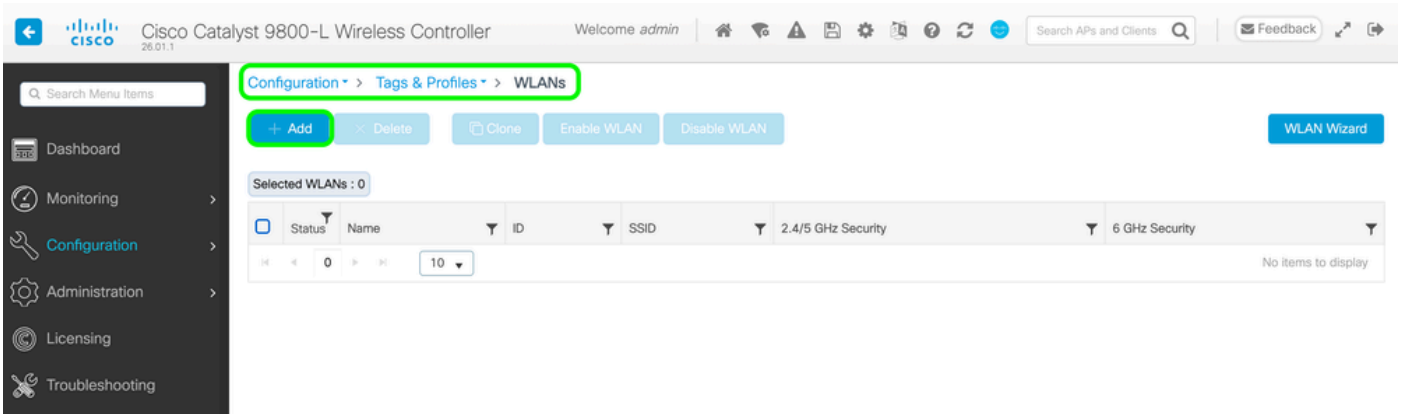
Configurazione

Esempio di rete

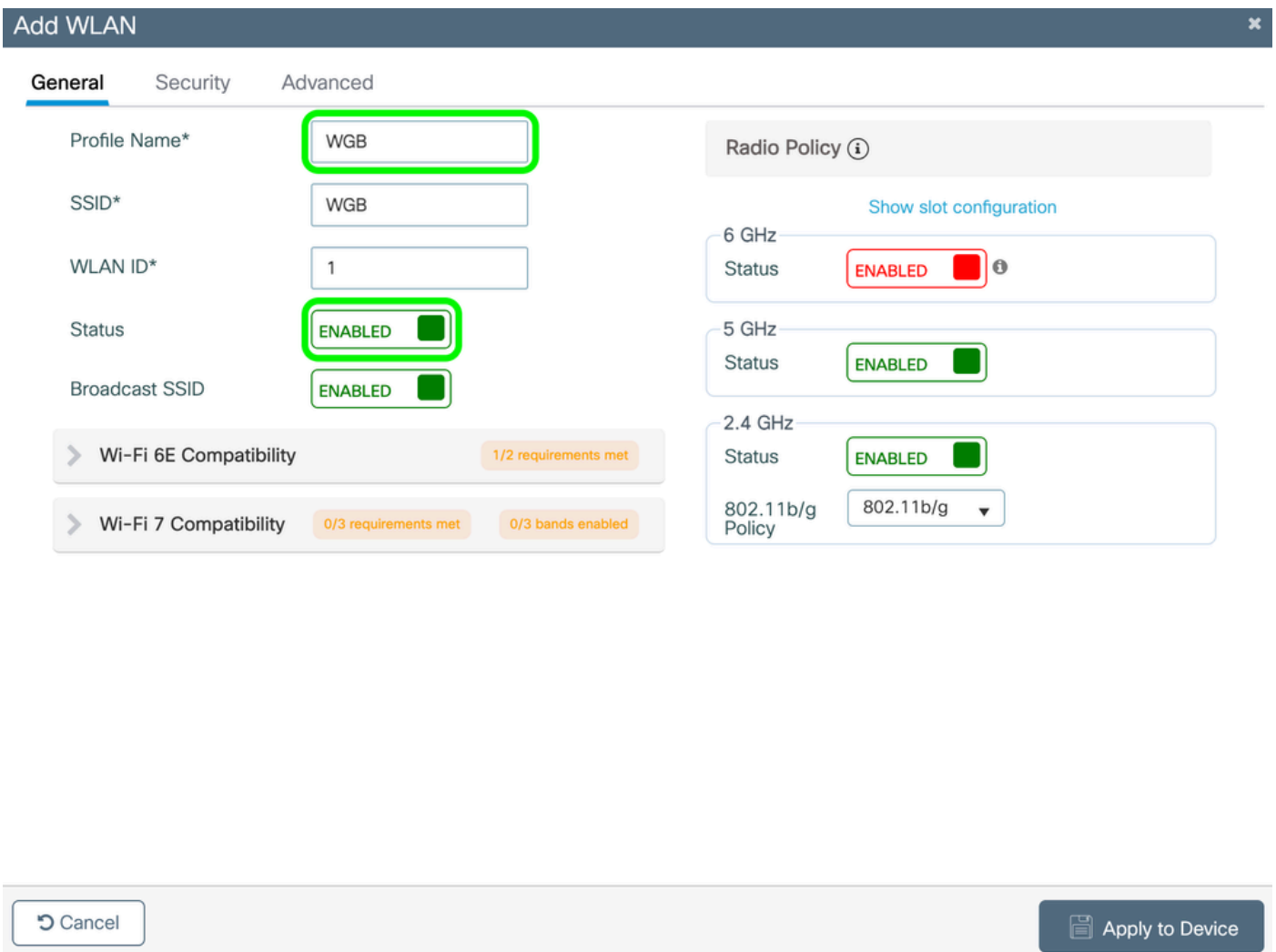
Configurazioni

Passaggio 1. Configurare una WLAN sul WLC da utilizzare per il WGB.

Sul WLC, selezionare Configuration > Tags & Profiles > WLAN > click + Add come mostrato nell'immagine.



Assegnare un nome alla WLAN e verificare che sia abilitata.



Passare alla scheda Protezione e selezionare le impostazioni di protezione desiderate per l'SSID WGB creato. Ai fini del presente documento è stato creato un SSID aperto. Tuttavia, è possibile creare anche altre opzioni di protezione.



Avviso: Verificare che le impostazioni di sicurezza corrispondano tra il SSID sul WLC e il profilo SSID del WGB AP (questo profilo è configurato più avanti nel documento sul 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

Andare alla scheda Advanced (Avanzate) e verificare che CCX Aironet IE sia abilitato. Quindi fare clic su Applica al dispositivo.

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)

Deny LAA (RCM) clients

6 GHz Client Steering

Latency Measurements Announcements

Off Channel Scanning Defer

Defer Priority 0 1 2

3 4 5

6 7

Scan Defer Time

Assisted Roaming (11k)

Dopo aver creato il profilo WLAN, creare un profilo criteri per la WLAN. A tale scopo, selezionare Configurazione > Tag e profili > Criterio > fare clic su + Aggiungi.

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

Immettere un nome per il profilo dei criteri nella scheda Generale e verificare che il profilo dei criteri sia abilitato.

⚠ 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

Passare alla scheda Criteri di accesso e assegnare una VLAN al profilo della policy.

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

Search or Select ▼ ⓘ

VLAN

VLAN/VLAN Group

BACKBONE-V... x ▼ ⓘ

Multicast VLAN

Enter 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

Search or Select ▼ ⓘ

IPv6 ACL

Search or Select ▼ ⓘ

URL Filters ⓘ

Pre Auth

Search or Select ▼ ⓘ

Post Auth

Search or Select ▼ ⓘ

↶ Cancel

📄 Apply to Device

Passare alla scheda Advanced (Avanzate), scorrere verso il basso fino alla sezione WGB Parameters (Parametri WGB) e selezionare Broadcast Tagging (Tagging trasmissione) e WGB VLAN options (Opzioni VLAN WGB). Quindi fare clic su Applica al dispositivo.

Add Policy Profile

DHCP Server VRF

Show more >>>

AAA Policy

Allow AAA Override

NAC State

Policy Name

Accounting List

Interim Accounting

WGB Parameters

Broadcast Tagging

WGB VLAN

Policy Proxy Settings

ARP Proxy

IPv6 Proxy

DNS Layer Security Parameter Map

Flex DHCP Option for DNS

Flex DNS Traffic Redirect

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

Quindi, mappare il profilo dei criteri al profilo WLAN. Selezionare Configurazione > Tag e profili > Tag > clic + Aggiungi.

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

Immettere un nome per il tag dei criteri. Quindi fare clic su + Aggiungi.

Add Policy Tag ×

Name*

Description

✓ WLAN-POLICY Maps : 0

+ Add × Delete

<input type="checkbox"/>	WLAN Profile	Policy Profile
No records available.		

◀ ◁ ▷ ▶ 10 items per page 0 - 0 of 0 items

> RLAN-POLICY Maps : 0

↶ Cancel 📄 Apply to Device

Scorrere verso il basso fino alla sezione Mappa WLAN e criteri e selezionare i profili dei criteri WLAN creati in precedenza. Quindi fare clic su .

Add Policy Tag ×

+ Add × Delete

<input type="checkbox"/>	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

Dopo aver verificato che il mapping sia stato aggiunto alla tabella, fare clic su Applica al dispositivo.

Add Policy Tag ×

▼ WLAN-POLICY Maps : 1

+ Add × Delete

<input type="checkbox"/>	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

Passaggio 2. Configurare un access point in modalità WGB.

Convertire l'access point da CAPWAP al tipo WGB.

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

Configurare un indirizzo IP per l'access point WGB.

Per un indirizzo IP DHCP:

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

Per un indirizzo IP statico:

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

Configurare un profilo SSID nell'access point WGB.

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

```
ssid
```

```
authentication
```

Collegare il profilo SSID a un'interfaccia radio.

```
WGB_AP#configure dot11Radio
```

```
mode wgb ssid-profile
```

Abilitare la radio configurata nell'access point WGB.

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

Quindi, il punto di accesso WGB si connette al punto di accesso principale. È possibile verificare dal WLC che la configurazione sia stata completata correttamente.

Sul WLC, l'access point WGB è visto come un client wireless connesso. Nella stessa tabella vengono visualizzati anche i client cablati connessi tramite l'access point WGB.

Esempio:

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Selected 0 out of 2 Clients

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



Suggerimento: Prima di procedere con le configurazioni sull'access point WGB, verificare che sull'access point sia configurato un codice paese (è possibile verificare il codice con il comando "show controllers dot11Radio"), ad esempio:

```
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)
```



Suggerimento: Se il codice paese non è configurato, convertire l'access point in modalità CAPWAP, aggiungerlo a un WLC e verificare che il codice paese sia configurato. Quindi, convertire l'access point in modalità WGB e procedere con le configurazioni.

Verifica

È possibile utilizzare questi comandi per verificare le configurazioni correnti.

Nell'access point WGB:

```
#show wgb ssid
```

Esempio di output di configurazione riuscito:

```
Configured SSIDs details:
```

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

```
#show wgb dot11 associazioni
```

Esempio di output di configurazione riuscito:

```
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
```

Risoluzione dei problemi

Raccogli debug

Nell'access point WGB:

Dopo aver applicato le configurazioni, se l'access point WGB non si connette all'access point radice, abilitare il debug per ottenere ulteriori dettagli sulla causa dell'errore:

```
#debug wgb uplink all
```

Esempio di output di una connessione riuscita:

```
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:

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).