Configuring Cisco URWB Operation Mode

Configuring Cisco URWB Operation Mode

Catalyst IW9167E Access Point supports three wireless technologies on a single hardware platform, such as Cisco Catalyst Wi-Fi, Cisco URWB, and Cisco Workgroup Bridge (WGB). These access point have the flexibility to change their operating mode from Wi-Fi mode to Cisco URWB mode and vice versa.

To identify the image mode (AP mode or Cisco URWB mode) on IW9167E, the following method is used:

- Determining from CLI

Determining from CLI

IW9167E supports two different OS (Cisco URWB and CAPWAP Stack) for different feature sets and data plane logic. To determine Cisco URWB mode on IW9167E use the following show command.

```
Device# show version
Cisco AP Software, (ap1g6j), C9167, RELEASE SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2022 by Cisco Systems, Inc.
Compiled Thu Aug 18 01:01:29 PDT 2022
ROM: Bootstrap program is U-Boot boot loader
BOOTLDR: U-Boot boot loader Version 2022010100
```

```
APFC58. 9A16.E464 uptime is 1 days, 3 hours, 58 minutes
Last reload time : Wed Sep 7 11:17:00 UTC 2022
Last reload reason: reload command
```

If the show version displays Cisco AP Software **(ap1g6j)**, it means that the image supports Cisco URWB mode.

Cisco URWB LED Pattern

The IW9167E Cisco URWB mode follow the below LED pattern during booting process (Blinking Green during a normal booting process).

Table 1: Definition of Booting LED Pattern

Events	LED State
Boot loader status sequence: DRAM memory test in progress DRAM memory test OK Board initialization in progress Initialization FLASH file system FLASH memory test OK Initializing Ethernet Ethernet OK Starting AP OS Initialization Successful	Blinking GREEN
To press Reset button less than 20 s	Blinking RED
To press Reset button more than 20 s	Solid RED
When Reset button is released Or Reset button is pressed more than 60 sec	Blinking GREEN

After the access point boots up, the IW9167E Cisco URWB mode follows the below LED pattern.

Table 2: Definition of Cisco URWB OS LED Pattern

AP State	LED State
General warning: Insufficient inline power	Cycling through RED, GREEN, and AMBER
Limbo (Provisioning) mode: Fallback	Chirping AMBER
Limbo (Provisioning) mode: DHCP(Dynamic Host Configuration Protocol)	AMBER

AP State	LED State
SNR(Signal to Noise Ratio) Excellent (>=25 dB)	Blinking GREEN
SNR Good (15<=X<25 dB)	Fade-in GREEN
SNR Bad (10<=X<15 dB)	Fade-in AMBER
SNR Unbearable (<10 dB)	Fade-in RED

Reset Button Settings

The following reset actions are performed in the Cisco URWB when the LED turns to blinking RED (after the boot loader gets the reset signal):

- If reset button pressed for less than 20 seconds, configuration gets cleared.
- If reset button pressed for more than 20 seconds and less than 60 seconds, factory reset triggered.
- If reset button pressed for more than 60 seconds, nothing will be cleared.

Configuring Image Conversion

To convert an IW9167E Access Point from Wi-Fi mode (CAPWAP AP) to Cisco URWB mode and vice versa follow below procedures:

1. To convert from CAPWAP to Cisco URWB enter the following CLI command. Access Point will reboot and boot with Cisco URWB mode.

   ```
   configure boot mode urwb
   ```

2. To convert from Cisco URWB to CAPWAP enter the following CLI command. Access Point will reboot and boot with Cisco CAPWAP Access Point mode.

   ```
   configure boot mode capwap
   ```

3. To convert from CAPWAP to WGB/uWGB enter the following CLI command.

   ```
   configure boot mode wgb
   ```

4. To convert from URWB to WGB/uWGB enter the following CLI command.

   ```
   configure boot mode wgb
   ```

5. To convert from WGB/uWGB to CAPWAP enter the following CLI command.

   ```
   configure boot mode capwap
   ```

6. To convert from WGB/uWGB to URWB enter the following CLI command.

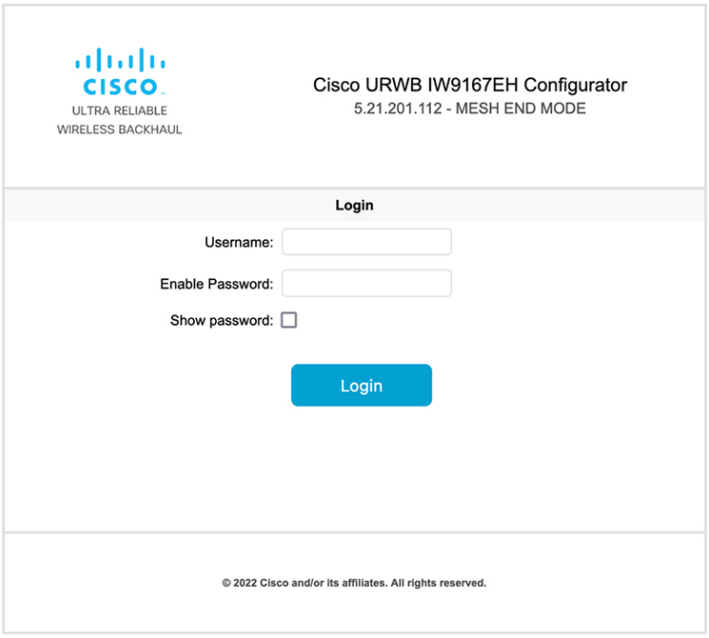
   ```
   configure boot mode urwb
   ```

Note Image conversion performs full factory reset (any configuration and data will be removed completely).

Instructions to Access the GUI

To access the Web UI, use the following procedures:

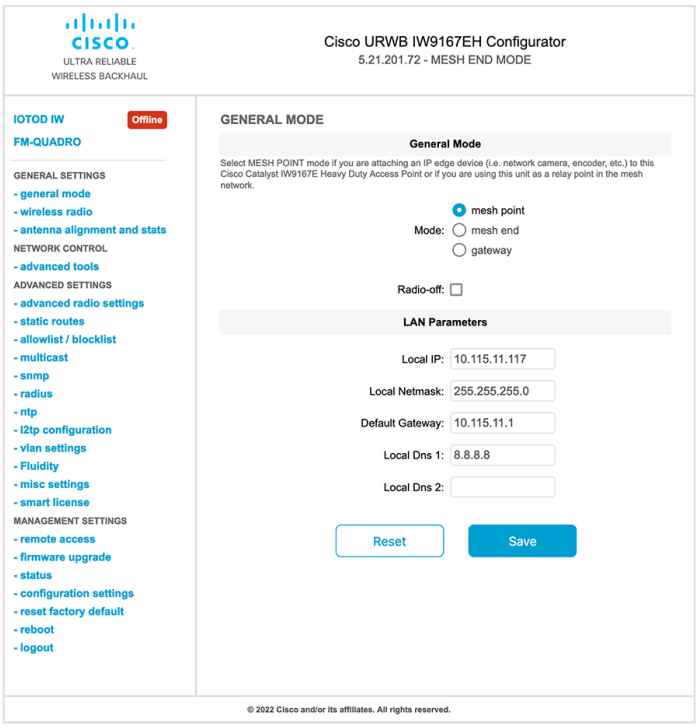
1. To access a Web UI, open the web browser and enter the following URL: https://<IP address of unit>/
2. After successfully open the login page, you will see the Cisco URWB IW9167EH Configurator as below.



3. To access the configuration page, user need to use the credentials as follows: username and enable password.

Cisco URWB IW9167E Configuration from GUI

The following image shows the GUI configuration of Cisco URWB IW9167E layout.



Committing CLI Configuration

To save the current or running configuration settings to local storage or memory, user need to type ***'write'*** CLI command. The modified value is in the cache configuration file so after the ***'write'*** command is entered, user must re-boot the device for the current configuration to take effect. To make the configuration effective, use the following CLI comments to write the configuration and reload the device.

```
Device# write
```

or

```
Device# wr
```

write or wr: commit the current configuration settings to memory.

```
Device# reload
```

reload: reload the device.

Example:

```
Device# write
```

!!! Please reboot to take effect

```
Device# reload
```

Proceed with reload? [confirm]

(enter to confirm)

Configuring and Verifying Regulatory Domain from CLI

To configure country code for ROW (Rest of the World) domain, use the following CLI command.

```
Device# configure countrycode [countrycode]
```

Example:

```
Configure countrycode GB
```

The above CLI will report error if configured country code is not included in ROW and wireless interface does not work properly if the user does not configure the country code.

Note Users need to reboot the device before configuring other wireless parameters (e.g., frequency, channel width), and after configuring country code. The country code is changeable or varying only for IW9167EH-ROW.

To verify status of regulatory domain, use the following show command.

```
Device# show version | in Product
Product/Model Number: IW9167EH-ROW
```

To verify status of ROW (Rest of the World) country code, use the following show command.

```
Device# show dot11Radio <interface> config
```

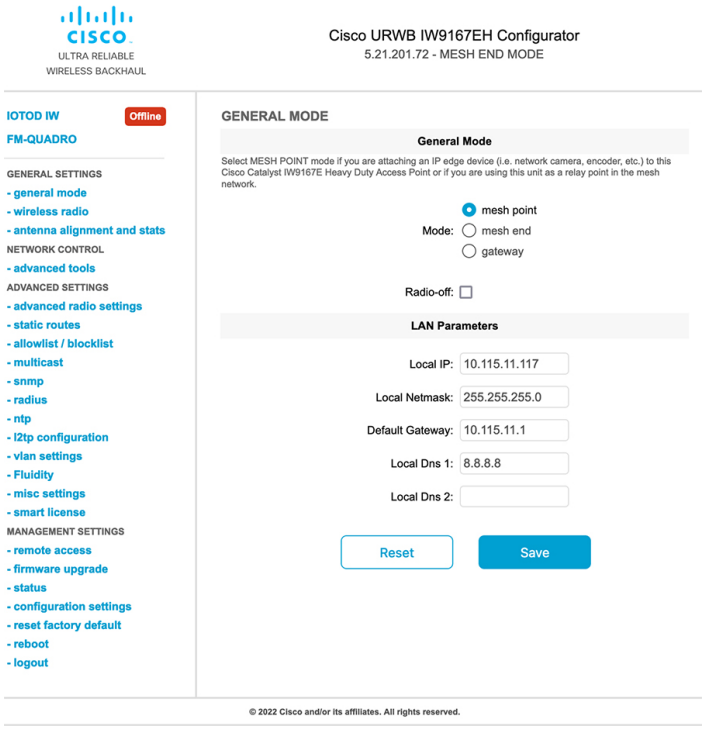
Example:

```
Device# show dot11Radio 1 config
…….
DFS region : GB
DFS radar role : auto
Radar Detected : 0
Indoor deployment: disable
```

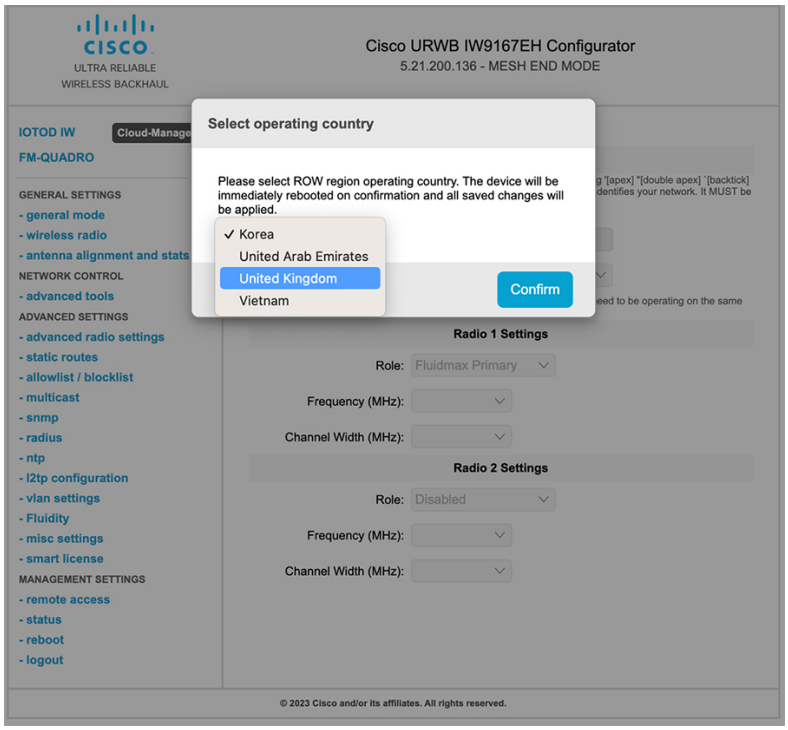
Configuring Regulatory Domain from GUI

Wireless interfaces do not work if user does not configure country code. Use the following procedure to configure a regulatory domain from GUI.

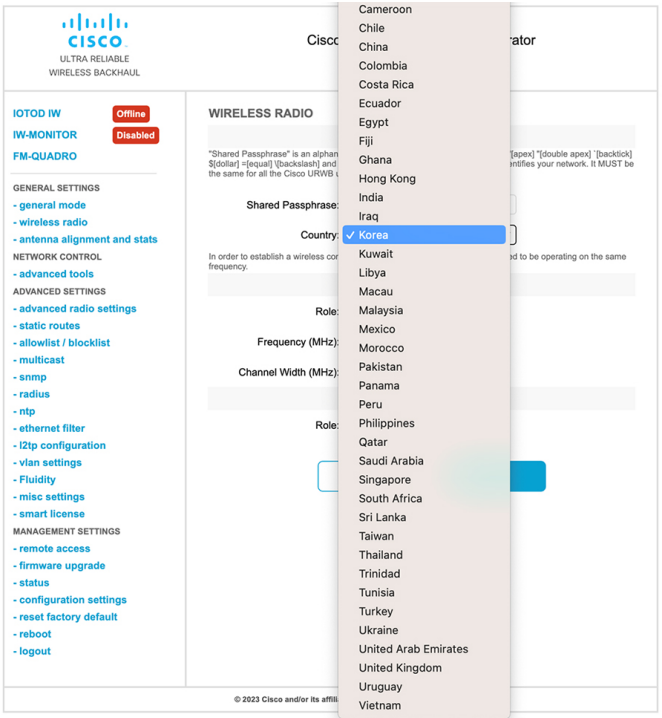
1. Select a Mesh Point mode if you are attaching an IP edge device to Cisco IW9167EH Access Point or if you are using this unit as a relay point in the mesh network.



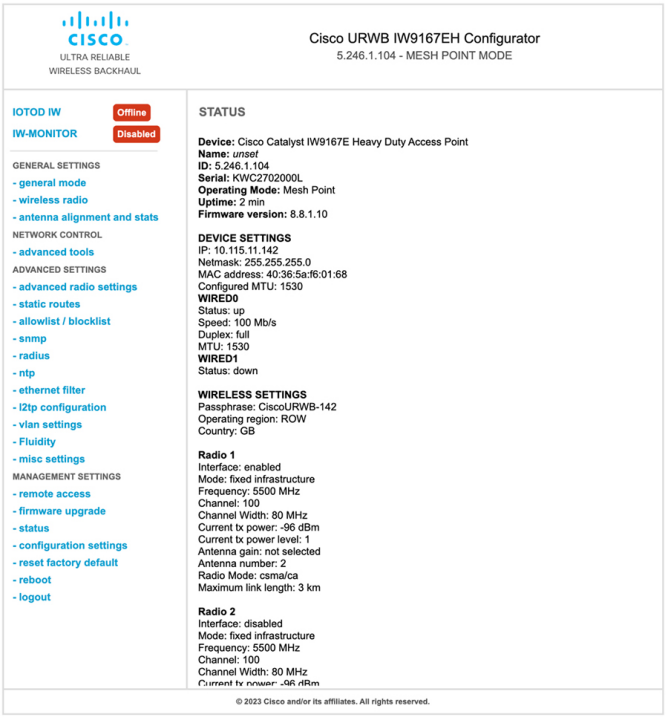
2. For ROW domain, if the country code is not selected, the Web UI will display an alert toast as follows.



3. To select a country code, click the alert toast displays in the below image then the user will be redirected to Web UI wireless section for selecting country code.

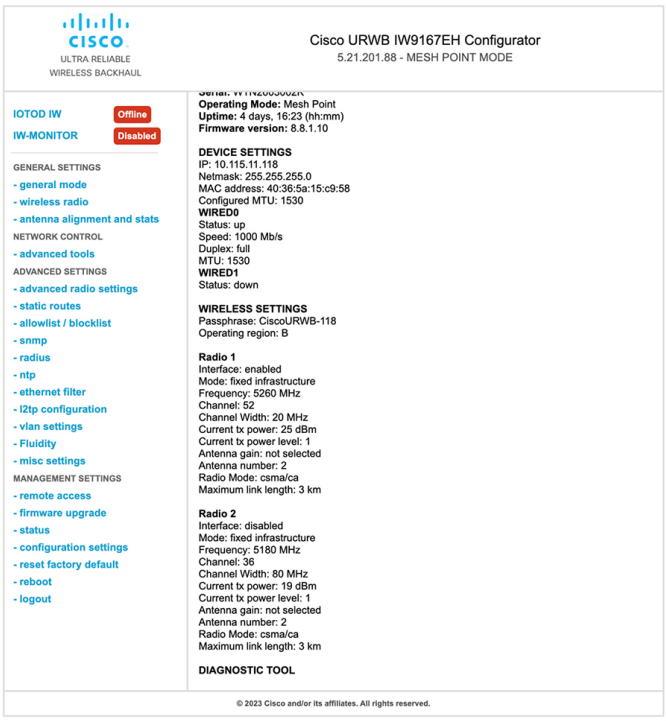


4. User must click on "status" link on the left side of menu page and check operating region and country code availability in wireless setting status page.



5. To establish a wireless connection between Cisco URWB units, set a same operating frequency in radio units.“Shared Passphrase” must be the same for all the Cisco URWB units belonging to the same network.

6. The below image shows the configuration of regularity domain from GUI.



Configuring IOT-OD and Offline Mode from CLI

IOT-OD (IoT Operations Dashboard) is the cloud management portal, and the device is connected to the online cloud through the internet. In offline mode the device is configured in local mode by CLI and web UI, and it is not connected to the cloud.

When the device is configured in offline mode, the user can choose following options.

- configure the device manually using CLI and web UI.
- configure the device on IOTOD cloud service and select the configuration file exported from IOD-OD industrial wireless and upload the configuration file by using upload configuration button at the end of IOT-IW management page.

To activate or deactivate IOTOD-IW (IOT Industrial Wireless) configuration capability, use the following CLI command.

```
Device# configure iotod-iw {offline | online}
```

online - set up IOTOD IW mode to online. The device can be managed from the IOTOD IW cloud server (if it is connected to the Internet).

offline - set up IOTOD IW mode to offline. (The device is disconnected from IOTOD-IW and must be manually configured using the CLI, or its offline Configurator interface.)

Configuring Strong Password (after first login) from CLI

When the device is turned to offline mode, it is required to set a strong password for the device after the first login. To configure a strong password from the CLI, the username and password should follow the procedures listed below:

- The username length is between 1 and 32 characters.
- The password length should be from 8 to 120 characters.
- The password must contain at least one uppercase character, one lowercase character, one digit, and one punctuation mark.
- The password can contain alphanumeric characters and special characters (ASCII decimal code from 33 to 126), but the following special characters are not permitted:

  " [double quote]

  ' [single quote]

  ? [question mark]
- The password should not contain three sequential characters.
- The password cannot contain the same three characters consecutively.
- The password cannot be the same as or the reverse of the username.
- A new password cannot be the same as the current or existing password.

Example:

The default credential is,

```
username: Cisco
password: Cisco
enable password: Cisco
```

To reset the credential with strong password, use the following sample credentials.

```
username: demouser
password: DemoP@ssw0rd
enable password: DemoE^aP@ssw0rd
```

Example of configuring strong password from CLI.

```
Device# configure iotod-iw {offline}
Switching to IOTOD IW Offline mode...
Will switch from Provisioning Mode to IOTOD IW offline Mode, device need to reboot:Y/N?
Y
User access verification.
[Device rebooting...]

User Access Verification:
Username: Cisco
Password: Cisco
```

After first login, Please reset credentials

```
Current Password:Cisco
Current Enable Password:Cisco
New User Name:demouser
New Password:DemoP@ssw0rd
Confirm New Password:DemoP@ssw0rd
New Enable Password:DemoE^aP@ssw0rd
Confirm New Enable Password:DemoE^aP@ssw0rd
```

After credentials changed, Please re-login

```
User access verification
Username: demouser
Password: DemoP@ssw0rd
Device> enable
Password:DemoE^aP@ssw0rd
Device#
```

Note In the above example, all passwords are in plain text. This is for demo purposes (sample credential). In real case or configuration, they are hidden behind asterisks (*).

Configuring IOT-OD IW from GUI

The following image shows the GUI page of IOT-OD IW management.