Configuring URWB Operation Mode

Configuring URWB Operation Mode

Catalyst Industrial Wireless access points support multiple wireless technologies, such as Catalyst Wi-Fi (AP), Cisco Ultra-Reliable Wireless Backhaul (URWB), and Workgroup Bridge (WGB). The modes supported vary by specific access point.

The access point OS supports two different software images: Catalyst Wi-Fi (AP) and Unified Industrial Wireless (UIW). Both URWB and WGB are part of the UIW software. The access point mode is determined at boot time based on the mode the access point is configured to operate in.

Determining from CLI

The access point OS supports two different software images: Catalyst Wi-Fi (AP) and UIW. Use the following show command to determine which software is running and look for the indicated platform code:

```
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 `ap1g6a` or `ap1g6b`, it means that the access point OS is running. If the show version displays `ap1g6j` or `ap1g6m`, it means the UIW software is running.

To check if the access point is running in URWB mode, use the following CLI command:

```
Device# show iotod-iw status
```

If the command exists, then the access point is running in URWB mode, otherwise the access point is running in WGB mode.

Reset Button Settings

The following reset actions are performed in the URWB mode when the LED turns to blinking red (after the boot loader gets the reset signal). Ensure you to press the device's reset button before the device is powering on.

- If you press the reset button for < 20 seconds, it clears the existing configuration.
- If you press the reset button for > 20 seconds and < 60 seconds, it triggers the factory reset.
- If you press the reset button for > 60 seconds, it does not clear the configuration.

Configuring Image Conversion

To convert a Catalyst IW9167E access point either from Wi-Fi mode (CAPWAP AP) to URWB mode or from URWB mode to Wi-Fi mode (CAPWAP AP), follow these steps:

1. To convert from CAPWAP to URWB mode or from WGB/uWGB to URWB mode, use the following CLI command. The access point then reboots and starts up in URWB mode.

   configure boot mode urwb

2. To convert from URWB to CAPWAP mode or from WGB/uWGB to CAPWAP mode, use the following CLI command. The access point then reboots and starts up in CAPWAP mode.

   configure boot mode capwap

3. To convert from CAPWAP to WGB/uWGB mode or from URWB to WGB/uWGB mode, use the following CLI command:

   configure boot mode wgb

Note Image conversion performs a full factory reset which completely erases the configuration and data.

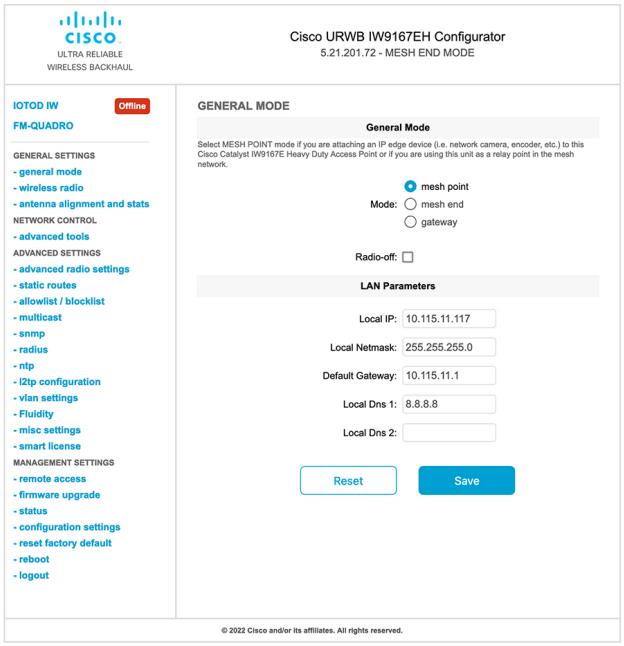
Instructions to Access the GUI

To access the Web UI (Web User Interface), use the following procedure:

1. To access a Web UI, open the web browser and enter the following URL: https://<IP address of unit>/

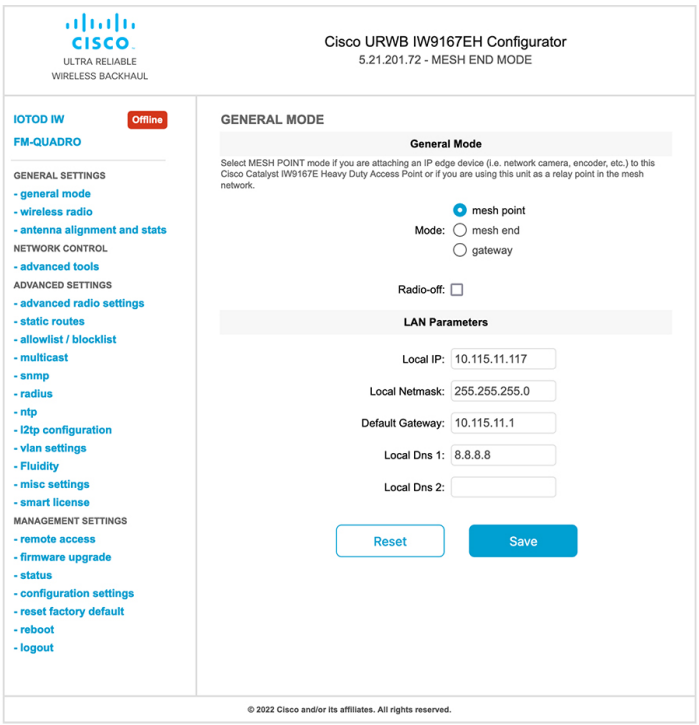
   The **IW9167E or IW9165 Configurator** window appears.

2. To access the configuration page, use the credentials as follows: **Username** and **Enable password**.
3. Once you successfully log into the GUI, the URWB configurator displays:



URWB Catalyst IW9167E Configuration from GUI

The following image shows the configuration of the Catalyst IW9167E configurator:



Committing CLI Configuration

To save the current or running configuration settings to local storage or memory, type `write` CLI command. The modified value is in the cache configuration file, once the `write` command is entered, re-boot the device to take effect of the current configuration. To make the configuration effective, use the following CLI commands:

```
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 IoT OD Online 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 network. In offline mode the device is configured in local mode using CLI and GUI, and it is not connected to the cloud.

When the device is configured in offline mode, choose following options:

- Configure the device manually using CLI and GUI.
- Configure the device on IoT OD cloud service and select the configuration file exported from IoT OD IW and upload the configuration file using upload configuration button at the end of IoT OD IW management page.

To activate or deactivate IoT OD IW (IoT Industrial Wireless) configuration capability, use the following CLI command:

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

Online - To set up IoT OD IW mode to online. The device can be managed from IoT OD IW cloud server (if it is connected to the network).

Offline - To set up IoT OD IW mode to offline. The device is disconnected from IoT OD IW and must be manually configured using the CLI, or offline configurator interface.

Configuring Password (after first login) from CLI

Once the device switches to offline mode (after the initial login), you need to set up new login credential. To configure login credentials using GUI or CLI, the login credentials should follow these criteria:

- The username length must be from 1 to 32 characters.
- The password length must be from 8 to 120 characters.
- The password must include the following:
    - At least one uppercase letter
    - At least one lowercase character,
    - At least one digit
    - At least one special character
- The password can contain alphanumeric characters and special characters (ASCII decimal code from 33 to 126), but the following special characters are not allowed:

  " [double quote]

  ' [single quote]

  ? [question mark]
- The password must not contain:
    - Three sequential characters or digits (ABC/ CBA)

- The same three characters or digits consecutively (AAA) or (666)
- Same as the current or existing password
- Same as or the reverse of the username

Example:

Default credentials:

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

To reset the credentials, use the following sample credentials:

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

Example of configuring password using 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, reset the 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
```

Once the credentials are changed, 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 the real scenario, they are hidden behind asterisks (*).

Configuring IoT OD IW from GUI

The following image shows the configuration of IoT OD IW: