Initial Configuration of the Device in Provisioning Mode

Catalyst IW Access Points running in URWB mode support configuration from Cisco IoT Operations Dashboard (IoT OD) or using local management interfaces. An access point (AP) with no configuration defaults to provisioning mode, which allows the initial configuration to be sent to the access point from IoT OD.

Provisioning mode is a special mode where the AP attempts to request network configuration using dynamic host configuration protocol (DHCP) and connect to IoT OD. If network connectivity exists, the AP connects to IoT OD. If there is no network connectivity, the AP can be configured locally using the GUI or CLI, accessible using the console port or SSH.

Note Use these default credentials to log into either the GUI or CLI:

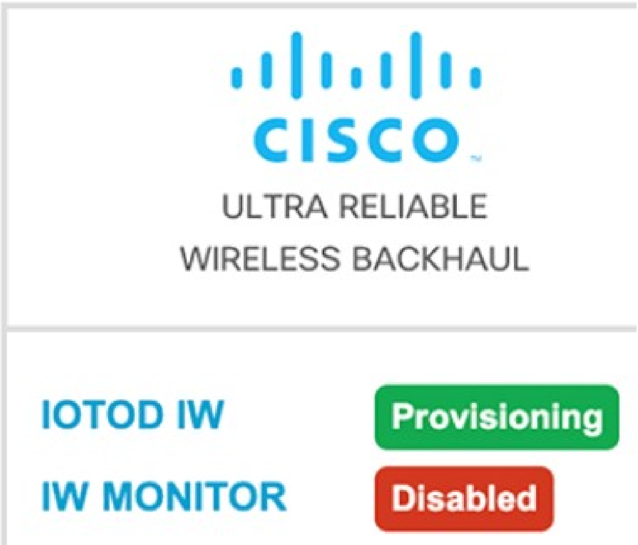
- Username: Cisco
- Password: Cisco

The DHCP server assigns a default gateway and domain name system (DNS) server. IoT OD uses DNS geo-location to direct AP in the United States to the US cluster. Other locations are directed to the EU cluster. Ensure your IoT OD organization is configured to the correct cluster.

DHCP is only used in provisioning mode. A static IP address must be assigned for normal operation. If DHCP is unavailable and configuration through IoT OD is required, the IP address, subnet, default gateway, and DNS can be manually configured.

Note When the device is in provisioning mode, the AP attempts to get an IP address from a DHCP server. If the device fails to receive an IP address through DHCP, the AP reverts to a fallback IP address of 192.168.0.10/24.

- To verify if the device is in provisioning mode, go to the device configurator interface and the status of IoT OD is shown as **Provisioning**:



ULTRA RELIABLE
WIRELESS BACKHAUL

IOTOD IW Provisioning

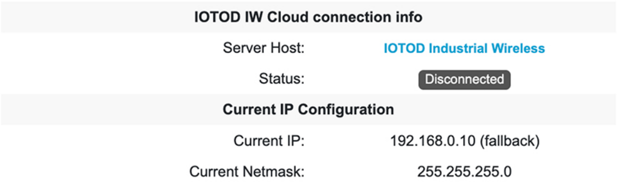
IW MONITOR Disabled

- To verify if the device is in provisioning mode, use the following show command:

```
Device#show iotod-iw status
  IOTOD IW mode: Provisioning
  Status: Connected
```

- If the status of IoT OD is shown as **Online** or **Offline**, choose either of the following options:
  - To configure a new device, revert the wireless device to provisioning mode and reset the device, see Reset the Device to Factory Default using GUI, on page 6.
  - To change the connection settings with current configuration, see Configuring General Settings, on page 9.

If the device is in provisioning mode, the device configurator interface is shown:



IOTOD IW Cloud connection info

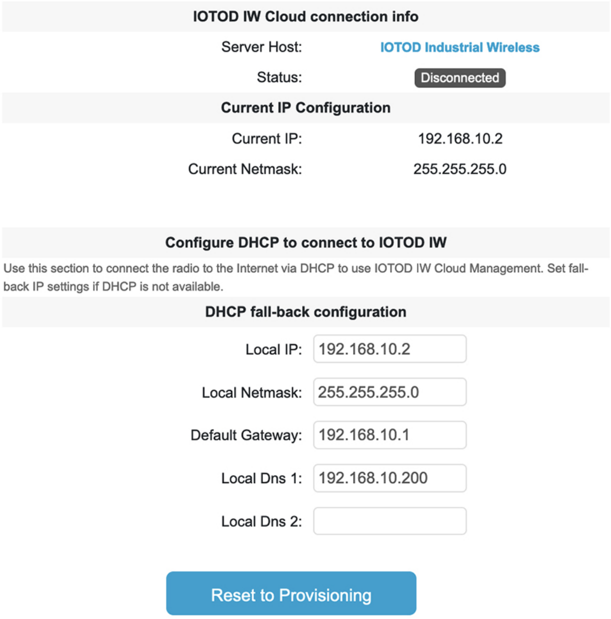
Server Host: IOTOD Industrial Wireless

Status: Disconnected

Current IP Configuration

Current IP: 192.168.0.10 (fallback)

Current Netmask: 255.255.255.0



IOTOD IW Cloud connection info

Server Host:	IOTOD Industrial Wireless
Status:	Disconnected

Current IP Configuration

Current IP:	192.168.10.2
Current Netmask:	255.255.255.0

Configure DHCP to connect to IOTOD IW

Use this section to connect the radio to the Internet via DHCP to use IOTOD IW Cloud Management. Set fall-back IP settings if DHCP is not available.

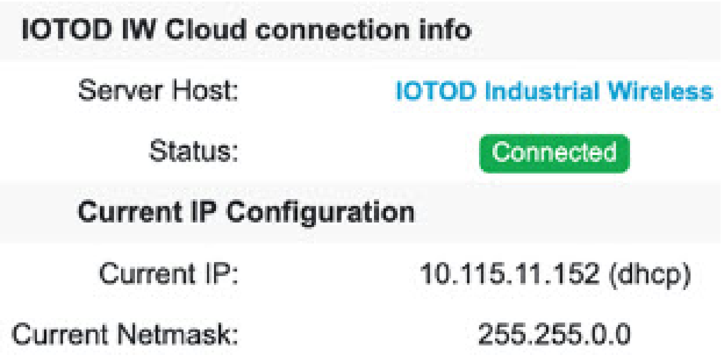
DHCP fall-back configuration

Local IP:	192.168.10.2
Local Netmask:	255.255.255.0
Default Gateway:	192.168.10.1
Local Dns 1:	192.168.10.200
Local Dns 2:	

The device's status and LEDs blink continuously and LEDs repeat this cycle until the device either enters a fallback condition, or enters **Online**, or **Offline** mode. To know more about LED status, see LED Pattern for Catalyst IW9165 or LED Pattern for Catalyst IW9167.

Note DHCP is used only in provisioning mode. A static IP address must be assigned for normal operation.

Ensure that the device is connected to a network that supports DHCP. If the connection to IoT OD is successful, the cloud connection info status is shown as **Connected**.



IOTOD IW Cloud connection info

Server Host:	IOTOD Industrial Wireless
Status:	Connected

Current IP Configuration

Current IP:	10.115.11.152 (dhcp)
Current Netmask:	255.255.0.0

To configure the fallback address, use the following CLI command:

Note In the provisioning mode, the IP, netmask, default gateway, primary DNS, and secondary DNS configuration (IP command) are allowed.

```
Device# configure ip address ipv4 [ static IP address [ static netmask [ IP address of
default gateway [ dns1 ip [ dns2 ip ] ] ] ] ]
```

For example:

```
Device# configure ip address ipv4 static 192.168.10.2 255.255.255.0 192.168.10.1
192.168.10.200 192.168.10.201
```

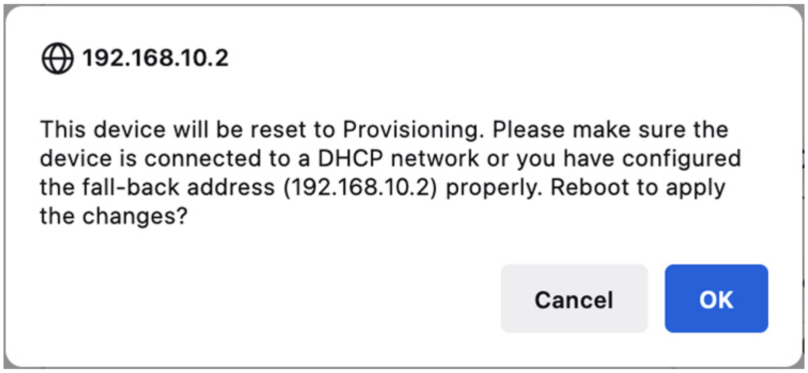
The device sets the fallback address (192.168.0.10 by default) or the configured IP address automatically if it does not receive an address from the DHCP server. If the device fails to connect to IoT OD, verify the following to reach IoT OD:

1. Check if the ethernet cable leading to the device is connected correctly.
2. Check if the local DNS server can fix the IP address of IoT OD cloud server and if the address can be reached.
3. Check if access point uses an outbound HTTPS connection on tcp/443 for the following domains:
    - device.ciscoiot.com
    - us.ciscoiot.com
    - eu.ciscoiot.com
4. If IoT OD is still offline, perform a local (offline) configuration using the device's configurator interface.

If the device fails to connect to the network in provisioning mode, follow these steps:

1. Enter alternative **Local IP**, **Local Netmask**, **Default Gateway**, **Local Dns 1**, and **Local Dns 2** values as needed, using IoT OD IW image and click the **Save fallback IP**.

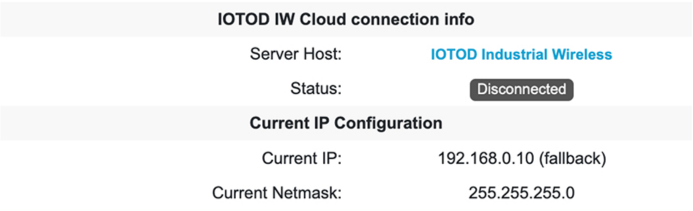
   A reboot confirmation pop-up appears:

   192.168.10.2

   This device will be reset to Provisioning. Please make sure the device is connected to a DHCP network or you have configured the fall-back address (192.168.10.2) properly. Reboot to apply the changes?

2. Click **OK** or **Reset** to go back to IoT OD IW and adjust the settings.
    - Once you click **OK**, the device reboots and remains in provisioning mode.
    - The device attempts to connect to the network using the new connection values.
3. If the device fails to connect to the network using the **DHCP** settings, **IoT OD IW Cloud connection Status** is shows as **Disconnected**.



IOTOD IW Cloud connection info

Server Host: IOTOD Industrial Wireless

Status: Disconnected

Current IP Configuration

Current IP: 192.168.0.10 (fallback)

Current Netmask: 255.255.255.0

4. To verify if the device is in provisioning mode and not connected to IoT OD, use the following CLI command:

```
Device#show iotod-iw status
 IOTOD IW mode: Provisioning
 Status: Disconnected
```

The following CLI example shows that the device is in provisioning mode and retrieved the IP address from the DHCP server:

```
Device#show ip
 IP:              192.168.0.10
 Network:         255.255.255.0
 Gateway:
 Nameservers:

 DHCP Address (PROVISIONING Mode):
 IP:              10.0.0.2
 Network:         255.255.255.0
 Gateway:         10.0.0.1
 Nameservers:     8.8.8.8

 Fallback Address (PROVISIONING Mode):
 IP:              169.254.201.72
 Network:         255.255.0.0
```

The following CLI example shows the device in provisioning mode fails to retrieve the IP address from the DHCP server and using the default fallback IP address 192.168.0.10:

```
Device#show ip
 IP:              192.168.0.10
 Network:         255.255.255.0
 Gateway:
 Nameservers:

 DHCP Address (PROVISIONING Mode):
 IP:              192.168.0.10
 Network:         255.255.255.0
 Gateway:
 Nameservers:     127.0.0.1

 Fallback Address (PROVISIONING Mode):
 IP:              169.254.201.72
 Network:         255.255.0.0
```

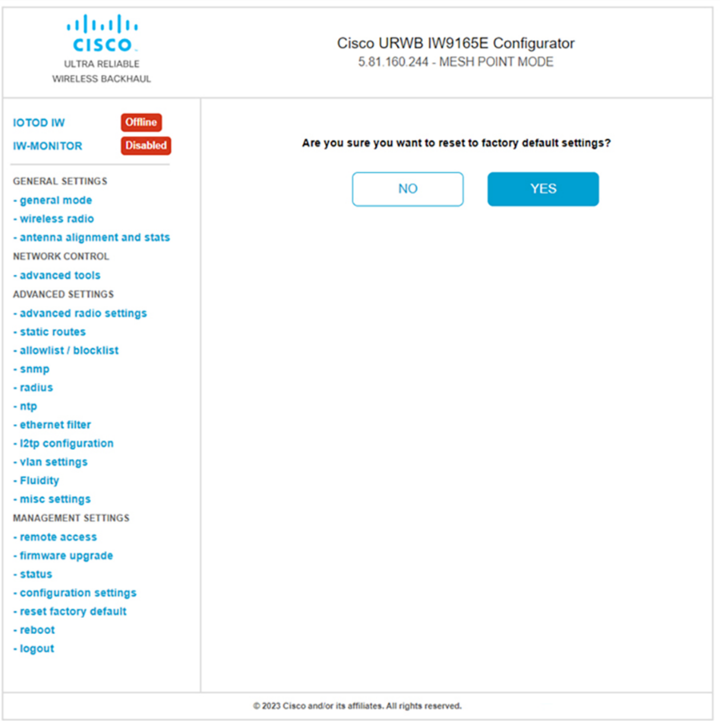
- Reset the Device to Factory Default using GUI, on page 6
- Reboot the Device using GUI, on page 7
- Saving and Restoring the Device Settings, on page 8
- Configuring General Settings, on page 9
- Connecting to the Access Point Console Port, on page 11

Reset the Device to Factory Default using GUI

You can reset the device to factory default either by pressing a reset button for 30 seconds when power is supplied to the access point or through configurator interface. For more information about reset button, see Using the Reset Button.

Note A hard reset reverts all device configuration settings, including the device IP address and administrator password to factory defaults. Instead if you want to reboot the device, see Reboot the Device using GUI, on page 7.

1. In the **MANAGEMENT SETTINGS**, click **reset factory default**.



Cisco URWB IW9165E Configurator
5.81.160.244 - MESH POINT MODE

Are you sure you want to reset to factory default settings?

2. Click **YES** in the confirmation pop-up window. To abort the factory reset, click **NO**.

3. If you have previously saved a configuration file for the device, you can restore the saved configuration settings to the device, see Saving and Restoring the Device Settings, on page 8.

Note Do not perform a hard reset unless the device requires reconfiguration using its factory configuration as the starting point. Hard reset resets the device's IP address, administrator password, and it disconnects the device from the network.

Reset the Device to Factory Default using CLI

To reset of the device configuration, use the following CLI command:

```
device#configure factory reset config
WARNING: "configure factory reset config" will clear config and reboot.
Do you want to proceed? (y/n)
```

Enter `y` in the CLI command to start the device reset process or alternatively enter `n` to abort the process.

To reset the device configuration and data wipe, use the following CLI command:

```
Device#configure factory reset default
WARNING: "configure factory reset default" will take minutes to perform DATA WIPE.
```

The following files are cleared as part of this process:

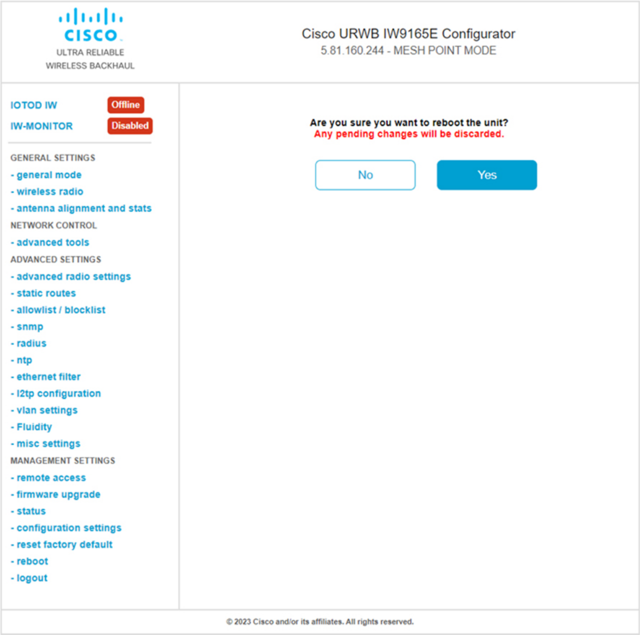
```
1) Config, Bak config files
2) Crashfiles
3) syslogs
4) Boot variables
5) Pktlogs
6) Manually created files
Do you want to proceed? (y/n)
```

Enter `y` in the CLI command to start the device reset of the configuration and data wipe or alternatively enter `n` to abort the process.

Reboot the Device using GUI

To reboot the device's operating system, follow these steps:

1. In the **MANAGEMENT SETTINGS**, click **reboot**.



Cisco URWB IW9165E Configurator
5.81.160.244 - MESH POINT MODE

Are you sure you want to reboot the unit?
Any pending changes will be discarded.

2. In the confirmation pop-up window, click **Yes**. To abort the reboot, click **No**.

Reboot the Device using CLI

To perform reboot, use the following CLI command:

```
Device#reload
Proceed with reload command (cold)? [confirm]
```

Enter `confirm` in the CLI command to start the device reboot process.

Saving and Restoring the Device Settings

The **LOAD OR RESTORE SETTINGS** window allows you to perform the following tasks:

- Save the device's existing software configuration as a configuration (*.conf) file.
- Upload and apply a saved configuration file to the current device.

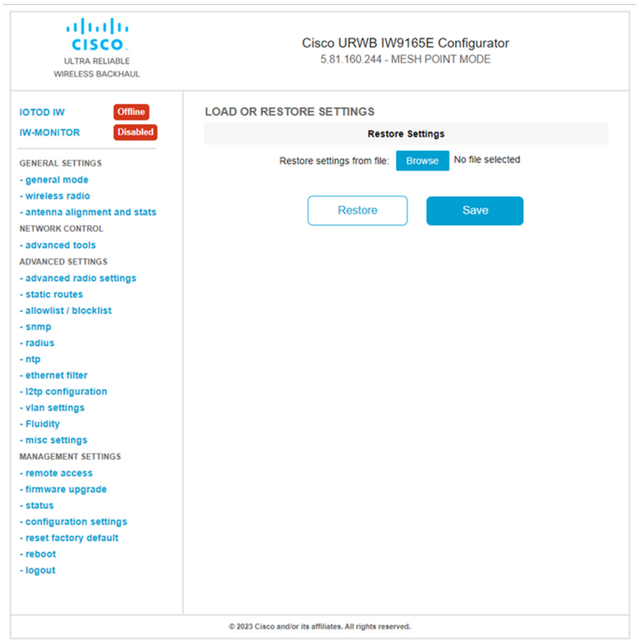
Note Device software configuration (*.conf) files are not interchangeable with IoT OD configuration setup (*.iwconf) files.

Tip Saved configuration files are reused for all devices of the same type. These saved configuration files act as configuration backup files to speed up redeployment if you need to replace the damaged device with a new device of the same type.

To download the device's existing configuration settings to your computer, follow these steps:

1. In the **MANAGEMENT SETTINGS**, click **configuration settings**.

   The **LOAD OR RESTORE SETTINGS** window appears.



Restore settings from file: No file selected

2. Click **Save** to download the device configuration (*.conf).

To upload a saved configuration file to the device, follow these steps:

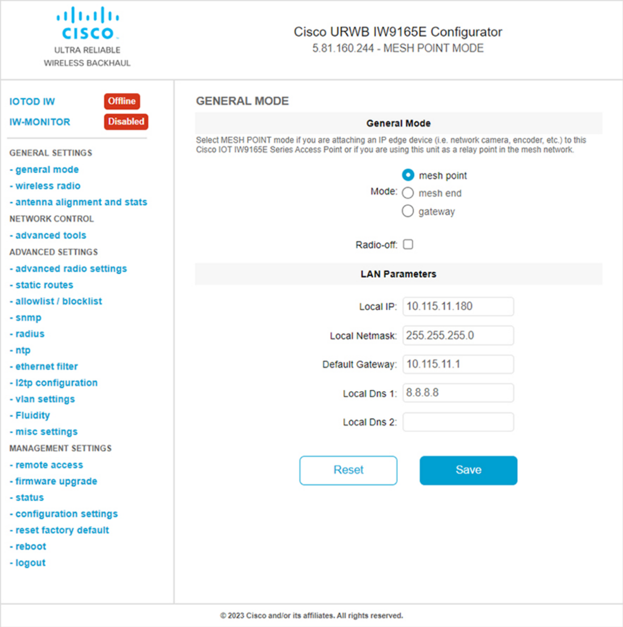
1. Click **Browse** to upload the configuration (*.conf) file to the device.

2. Click **Restore** to apply the configuration settings to the device.

Configuring General Settings

To change the **General Mode** settings, follow these steps:

1. In the **GENERAL SETTINGS**, click **general mode**.



Cisco URWB IW9165E Configurator
5.81.160.244 - MESH POINT MODE

GENERAL MODE

General Mode

Select MESH POINT mode if you are attaching an IP edge device (i.e. network camera, encoder, etc.) to this Cisco IOT IW9165E Series Access Point or if you are using this unit as a relay point in the mesh network.

Mode: ● mesh point ○ mesh end ○ gateway

Radio-off: □

LAN Parameters

Local IP: 10.115.11.180
Local Netmask: 255.255.255.0
Default Gateway: 10.115.11.1
Local Dns 1: 8.8.8.8
Local Dns 2:

© 2023 Cisco and/or its affiliates. All rights reserved.

The **General Mode** has the operational mode controls. Devices capable of operating in a mesh radio network are shipped in **mesh point** mode.

Note When designing the required network layout, there must be at least one mesh end device. This device performs control and administrative functions, such as license management. This is necessary for correct network operation, even if the network consists of only two devices.

To change the device's operational mode, select any one of the following mode:

- **Gateway** - This mode is applicable for advanced Layer 3 mobility deployments, and it is not used in most networks.
- **Mesh Point** - This mode is applicable for the remaining access points in the network. These access points establish links to other access points with the same network passphrase configured as mesh end or mesh point using wireless links or wired links. In this scenario, the access point has Layer 2 visibility of other access points.
- **Mesh End** - This mode configures the access point to perform control and administrative network functions. There must be at least one mesh end in each network. This access point is typically installed in the most central point where the wireless and wired networks converge.

Configuring General Settings using CLI

To configure general settings, use the following CLI command:

```
Device#configure modeconfig mode
  gateway    layer 3 global gateway mode
  meshend    mesh end mode
  meshpoint  mesh point mode
```

```
Device#configure modeconfig mode meshend
  mpls       MPLS support
  radio-off  disable radio interfaces
```

Changing the LAN Parameters

The LAN parameters has entry controls for local address setting. Perform the following to change the LAN parameters:

1. Once the **General Mode** window is opened for the first time, the **Local IP** and **Local Netmask** LAN parameters are shown with factory-set default values.
2. If needed, enter the local primary DNS address in the **Dns 1** field, and enter the local secondary DNS address in the **Dns 2** field.
3. Click **Save** to save the LAN settings. To clear the settings, click **Reset**.

Configuring LAN Parameters using CLI

To configure LAN parameters, use the following CLI command:

Example:

```
device#configure ip address ipv4 static
192.168.10.2 255.255.255.0 192.168.10.1 192.168.10.200 192.168.10.201
```

Connecting to the Access Point Console Port

To configure the access point locally (without connecting to a wired LAN), connect the computer to the access point's console port using a DB-9 to RJ-45 serial cable and to open the CLI by connecting to the access point's console port, follow these steps:

1. Connect a nine-pin, female DB-9 to RJ-45 serial cable to the RJ-45 serial port on the access point and to the COM port on a computer.
2. Set up a terminal emulator to communicate with the access point. In the terminal emulator, use the following settings:

Parameter	Value
Baud rate	115200 bps
Data	Eight bits
Parity	No
Stop	One stop bit
Flow Control	No

3. There are two available command-prompt modes: standard command prompt (>) and privileged command prompt (#). When logged in for the first time, it directs you to standard command prompt (>) mode to execute unprivileged commands.

   To access privileged command-prompt (#) mode, enter the enable command (abbreviated as en) and enter the enable password (the privilege mode login password is different from the standard login password).

Use these default credentials to log in:

- Username: Cisco
- Password: Cisco

Note Once the initial configuration completes, ensure to remove the serial cable from the access point.