Initial configuration of the unit in Provisioning Mode

Initial configuration of devices in provisioning mode

Initial configuration of devices in provisioning mode is a process that

- allows access points with no configuration to receive initial configuration from Industrial Wireless (IW) Service
- enables network configuration using DHCP when network connectivity exists, and
- provides local configuration options through GUI or CLI when network connectivity is unavailable.

Note From UIW Release 17.16.1, IoT OD IW changes to IW Service.

Provisioning mode behavior

This section provides provisioning mode behavior, default access credentials, DHCP addressing behavior, fallback IP behavior, cloud connectivity requirements, and CLI examples.

Catalyst IW Access Points running in URWB mode support configuration from Cisco Industrial Wireless (IW) Service 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 Industrial Wireless (IW) Service.

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

Default login credentials

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

- Username: Cisco
- Password: Cisco

DHCP addressing and IW service cluster selection

The DHCP server assigns a default gateway and domain name system (DNS) server. Industrial Wireless (IW) Service 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 Industrial Wireless (IW) Service organization is configured to the correct cluster.

Static IP requirement for normal operation

DHCP is only used in provisioning mode. A static IP address must be assigned for normal operation. If DHCP is unavailable and configuration through Industrial Wireless (IW) Service 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.

Verify provisioning mode using GUI

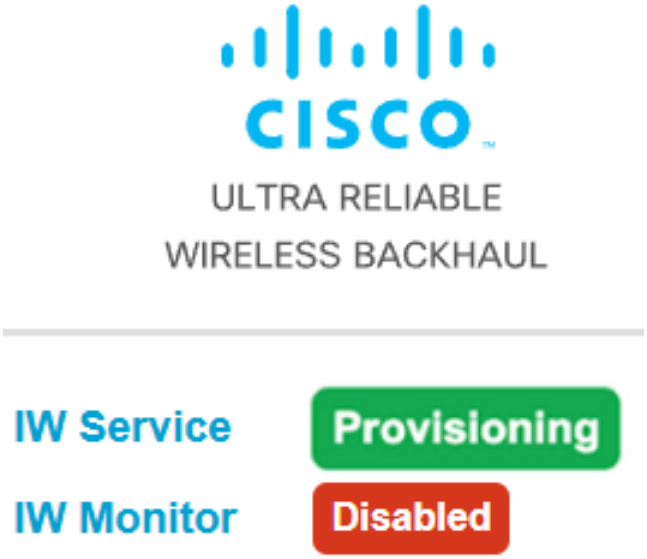
These steps show how to verify if the device is in provisioning mode:

Procedure

Step 1 To verify if the device is in provisioning mode, go to the device configurator interface. The status is shown as **Provisioning**:

Example:

Figure 1: Provisioning mode page



Step 2 If the status is shown as **Cloud-Managed** or **Offline**, choose either of these options:

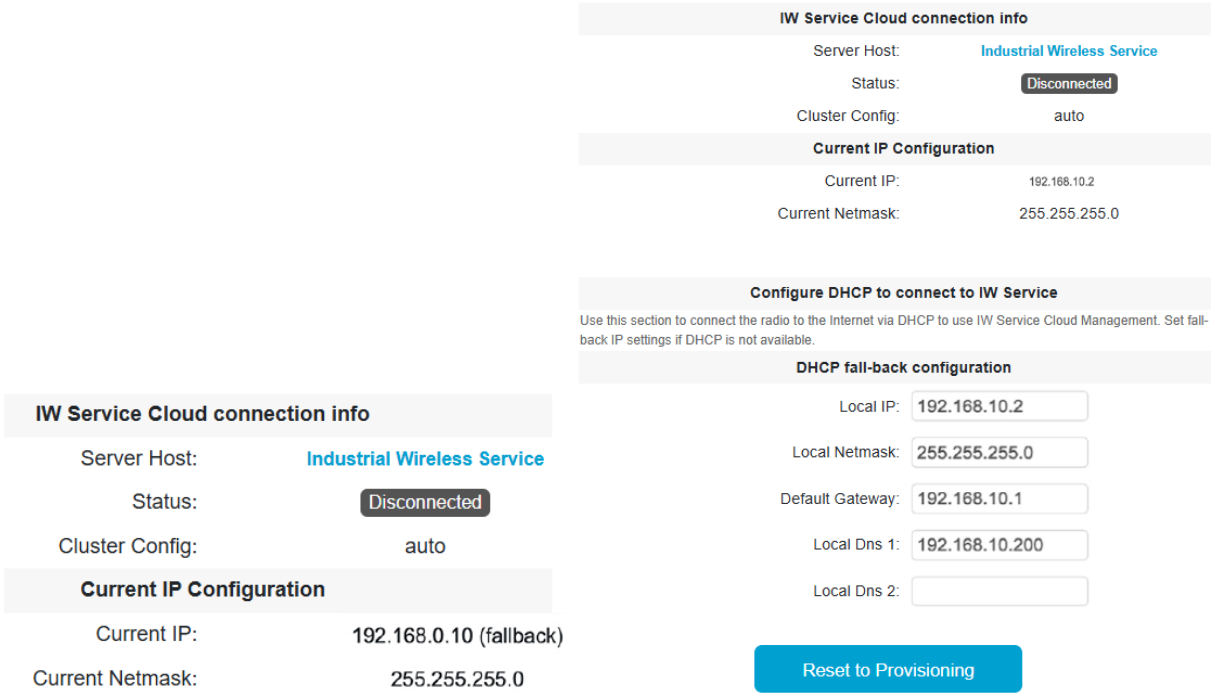
- To configure a new device, revert the wireless device to provisioning mode and reset the device, see Reset the device to factory default using GUI, on page 7.
- To change the connection settings with current configuration, see Configure GENERAL SETTINGS, on page 11.

Step 3 If the device is in provisioning mode, the device configurator interface is shown:

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

Example:

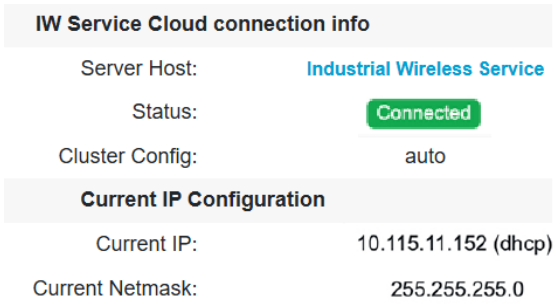
Figure 2: Cloud connection info



If the connection to Industrial Wireless (IW) Service is successful, the cloud connection info status is shown as **Connected**.

Example:

Figure 3: Cloud connection info



Verify provisioning mode using CLI

These steps show how to verify if the device is in provisioning mode:

Procedure

Use the **show iw-service status** command to verify whether the device is in provisioning mode.

Example:

```
Device#show iw-service status
  IW Service mode: Provisioning
  Status: Connected
```

This 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
```

This example shows the device in provisioning mode failed 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
```

Configure the fallback address

This task ensures that the device remains reachable on the network by using either the default fallback IP address or a user-configured static IP address.

This task is used in provisioning mode to assign a fallback IPv4 address configuration to the device when DHCP is unavailable or does not provide an address.

Procedure

Use the **configure ip address ipv4** *static-IP-address static-netmask default-gateway-ip* [*dns-ip*] command to configure fallback address.

Note
In provisioning mode, the IP address, netmask, default gateway, primary DNS, and secondary DNS can be configured using the IP command.

The device automatically sets the fallback address (192.168.0.10 by default) or the configured IP address if it does not receive an address from the DHCP server.

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
```

Troubleshoot connectivity

This task guides you through basic connectivity checks, including Ethernet, DNS resolution, HTTPS access on TCP port 443, and fallback IP configuration, so the device can reconnect or remain reachable for offline setup.

This task helps you when a device cannot connect to IoT Operations Dashboard Industrial Wireless Service or cannot reach the network while in provisioning mode.

Procedure

Step 1 If the device fails to connect to Industrial Wireless (IW) Service, verify these items to reach Industrial Wireless (IW) Service:

a. Check if the ethernet cable leading to the device is connected correctly.

b. Check if the local DNS server can fix the IP address of Industrial Wireless (IW) Service cloud server and if the address can be reached.

c. Check if access point uses an outbound HTTPS connection on tcp/443 for these domains:

- device.ciscoiot.com
- US.ciscoiot.com
- EU.ciscoiot.com

d. If Industrial Wireless (IW) Service is still offline, perform a local (offline) configuration using the device's configurator interface.

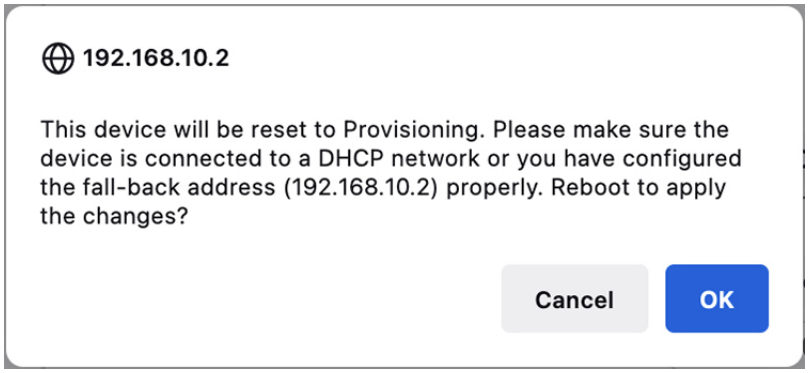
Step 2 If the device fails to connect to the network in provisioning mode, follow these steps:

a) Enter alternative **Local IP**, **Local Netmask**, **Default Gateway**, **Local DNS 1**, and **Local DNS 2** values as needed, using Industrial Wireless (IW) Service image and click the **Save fallback IP**.

A reboot confirmation pop-up appears:

Example:

Figure 4: Reboot confirmation popup



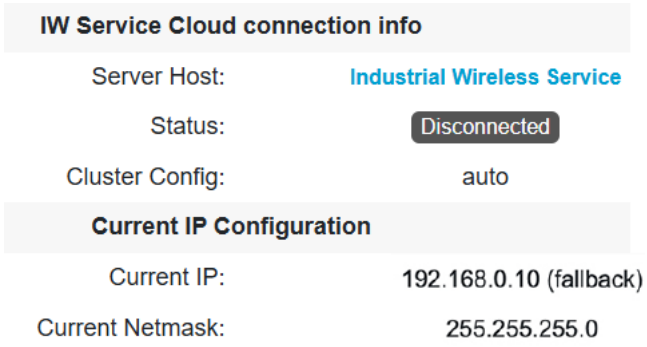
b) Click **OK** or **Reset** to go back to Industrial Wireless (IW) Service and adjust the settings.

- 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.

If the device fails to connect to the network using the **DHCP** settings, **IW Service Cloud connection Status** is shown as **Disconnected**.

Example:

Figure 5: Connection Status



Reset the device to factory default using GUI

Reset the device to factory default to revert all device configuration SETTINGS, including the device IP address and administrator password, to factory defaults.

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.

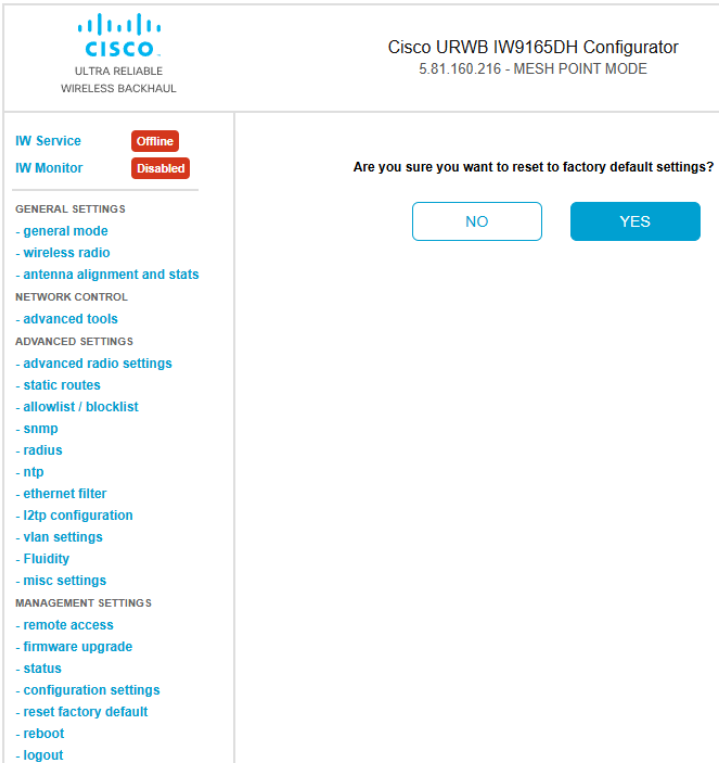
Note A hard reset reverts all device configuration SETTINGS, including the device IP address and administrator password to factory defaults. Instead if you want to reboot the device, see Reboot the device using GUI, on page 9.

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.

To reset of the device configuration, use the steps:

Procedure

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



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

Step 3 If you have previously saved a configuration file for the device, you can restore the saved configuration SETTINGS to the device, see Save and RESTORE the device SETTINGS, on page 10.

Reset the device to factory default using CLI

Reset the device to factory default to revert all device configuration SETTINGS, including the device IP address and administrator password, to factory defaults.

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

Procedure

Step 1 Use the **configure factory reset config** command to reset of the device configuration.

Example:

```
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.

Step 2 Use the **configure factory reset default** command to reset the device configuration and data wipe.

Example:

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

Example:

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.

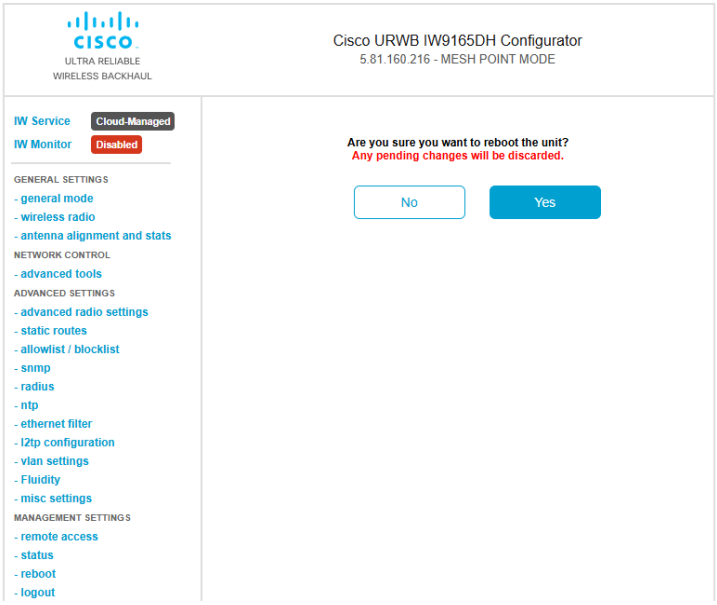
Reboot the device using GUI

Reboot the device's operating system to restart all system processes and apply configuration changes.

Use this procedure when you need to restart the device after making configuration changes or when troubleshooting system issues.

Procedure

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



Step 2 In the confirmation pop-up window, click **Yes**.

To abort the reboot, click **No**.

Step 3 To perform reboot using CLI, use the following command:

Example:

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

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

Save and RESTORE 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.

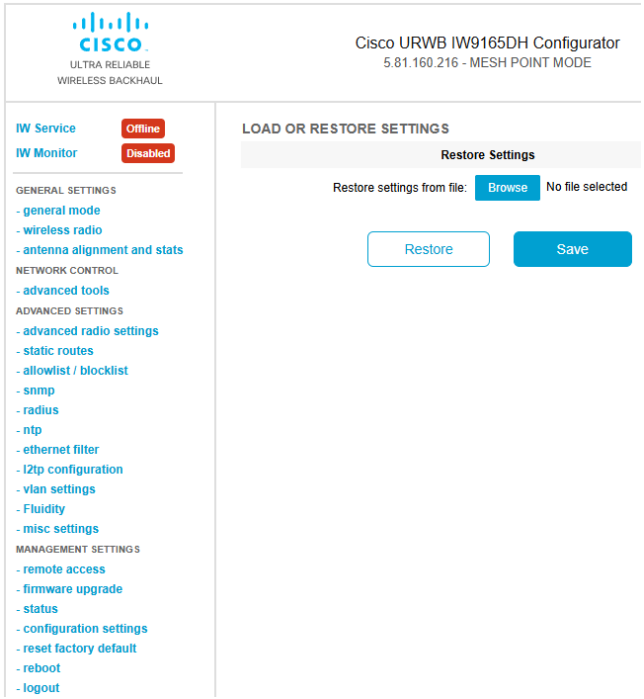
Note Device software configuration (*.conf) files are not interchangeable with IW Service configuration setup (*.iwconf) files.

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.

Procedure

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

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



Step 2 To download the device's existing configuration SETTINGS to your computer, click **Save** to download the device configuration (*.conf).

Step 3 To upload a saved configuration file to the device, click **Browse** to upload the configuration (*.conf) file to the device.

Step 4 Click **RESTORE** to apply the configuration SETTINGS to the device.

Configure GENERAL SETTINGS

Configure the operational mode and LAN parameters to establish proper mesh network functionality and device connectivity.

Devices capable of operating in a mesh radio network are shipped in mesh point mode. The GENERAL Mode has operational mode controls that determine how the device functions within the network.

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 General Mode settings, follow these steps:

Procedure

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

Step 2 Select the device's operational mode from the following options:

- **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.

Step 3 Change the LAN parameters by entering the local primary DNS address in the **DNS 1** field, and enter the local secondary DNS address in the **DNS 2** field if needed.

The **Local IP** and **Local Netmask** LAN parameters are shown with factory-set default values when the GENERAL Mode window is opened for the first time.

Step 4 Click **Save** to save the LAN SETTINGS.

To clear the SETTINGS, click **Reset**.

Step 5 Alternatively, configure GENERAL SETTINGS using CLI commands.

Example:

```
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
```

Step 6 Configure LAN parameters using CLI commands.

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
```

Connect to the access point console port

Configure the access point locally without connecting to a wired LAN by establishing a console connection and accessing the command-line interface.

This task enables local configuration of the access point when network connectivity is not available or when initial setup is required.

Before you begin

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. Then, open the CLI by connecting to the access point's console port.

Procedure

Step 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.

Step 2 Set up a terminal emulator to communicate with the access point.

In the terminal emulator, use these settings:

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

Step 3 Log in using the default credentials and access the appropriate command-prompt mode.

There are two available command-prompt modes: standard command prompt (>) and privileged command prompt (#). When you log in for the first time, the system directs you to standard command prompt (>) mode, where you can 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.