Cisco IEC6400 Edge Compute Appliance Installation and Configuration Guide, Release 1.0.1

First Published: 2023-11-28

Last Modified: 2024-04-05

C O N T E N T S

Preface

This preface describes this guide and provides information about the installation and configuration of IEC6400 Edge Compute Appliance, and related documentation.

It includes the following sections:

- About this Guide, on page v
- Related Documentation, on page v
- Communications, Services, and Additional Information, on page v

About this Guide

This guide details the installation and configuration of the IEC6400 Edge Compute Appliance. The IEC6400 Edge Compute Appliance uses the Ultra-Reliable Wireless Backhaul (URWB) technology with Cisco UCS C220 M6 Rack Server. The IEC6400 Release 1.0.1 fixes the following issues:

- The SNMP v3 encryption protocols mentioned in the GUI are now same as those configured using CLI.

- The NTP authentication methods mentioned in the GUI are now same as the authentication methods configured using CLI.

Related Documentation

For more details about Regulatory Compliance and Safety Information, see Regulatory Compliance and Safety Information.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.

- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.

- To submit a service request, visit Cisco Support.

- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.

- To obtain general networking, training, and certification titles, visit Cisco Press.

- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

CHAPTER 1

Overview of Cisco IEC6400 Gateway

Overview of Edge Compute Appliance

The IEC6400 Edge Compute Appliance acts as the MPLS gateway in a URWB network. One of the most important functionalities of the IEC6400 gateway is to handle aggregated throughput up to 40 Gbps.

The IEC6400 gateway uses the Ultra-Reliable Wireless Backhaul (URWB) technology with Cisco UCS C220 M6 Rack Server that enables you to extend the benefits of URWB to large-scale, high-capacity-demanding wireless networks. The IEC6400 gateway is designed to operate in URWB Layer 2 and 3 networks. It serves as an aggregation point for all the MPLS-over-the-communications within networks with numerous industrial wireless (IW) gateways requiring multi-Gbps aggregated throughput. IEC6400 gateway is part of the IW product's family with Wi-Fi 6 capability.

The Cisco UCS C220 M6 server supports:

- 2x 10GBase-T Ethernet LAN on Motherboard (LOM) ports used as data ports

- Support for an optional Cisco VIC, providing 4x 10/25G SFP28 data ports, which extends the throughput capability up to 40 Gbps

- 1x Gigabit Ethernet dedicated management port to access the UCS Cisco Integrated Management Controller (IMC) interface. The IMC offers CLI and web interface to manage configurations of the gateway hardware.

- 2x power supply connectors

- 1 KVM port

- Secure Boot

The following table lists the UCS C220 M6 server details:

Feature	Description
Chassis	One rack-unit (1RU) chassis
Hard disk	480 GB SSD SATA

Feature	Description
Central processor	Intel 4310 2.1 GHz/120 W 12C/18 MB DDR4 2667 MHz
Memory	16 GB
Power specification	2x 1050 W AC Power Supply

Note   Each power supply in the server has a power cord. Standard power cords or jumper power cords are available for connection to the server. The shorter jumper power cords, for use in racks, are available as an optional alternative to the standard power cords.

For more details about UCS C220 M6 server physical, environmental, power and power cord specifications, see *Cisco UCS C220 M6 Server Installation and Service Guide - Server Specifications*.

Architecture

Below is the sample architecture on how the IEC6400 gateway operates in a URWB Fluidity L3 network:

Figure 1: IEC6400 Gateway Architecture
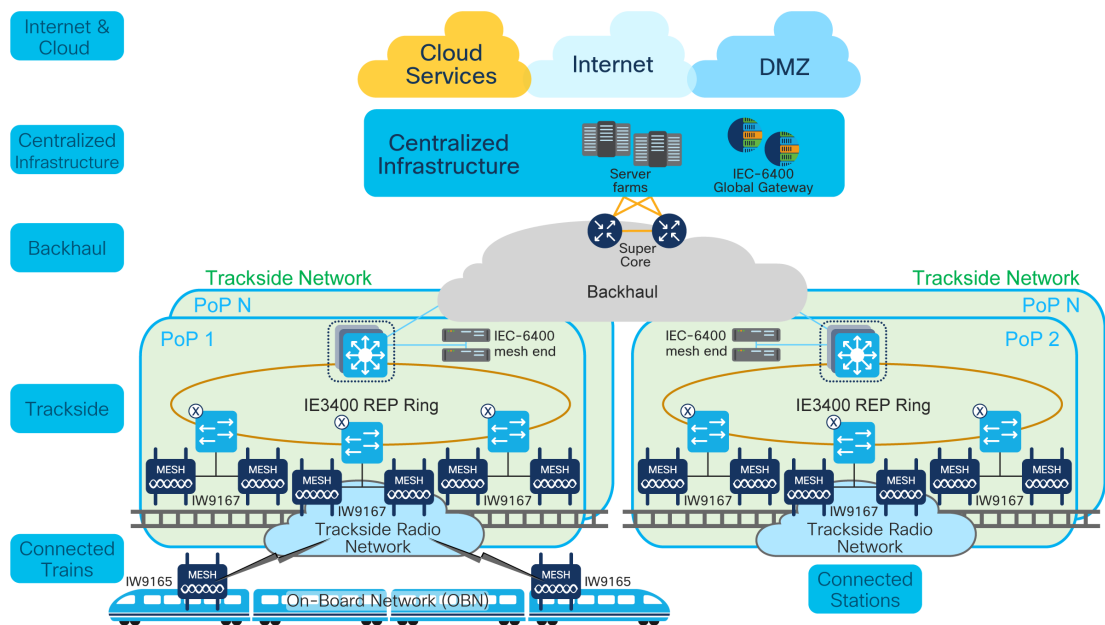
The IEC6400 gateway establishes a fixed architecture and implements the multiprotocol label switching (MPLS) protocol which uses labels rather than network addresses to guide data from one node to another node. This functionality increases the IP packet delivery rate.

Identifying Gateway Mesh Capability

Although the wireless access points can be configured in both Mesh Point and Mesh End modes, the IEC6400 gateway can only be configured as a Mesh End. Irrespective of its configuration and operational mode, each gateway is shipped from the factory with a unique mesh identification (ID) number (also called the Mesh ID), and it is in the form of 5.a.b.c.

The triplet a.b.c uniquely identifies the individual physical hardware gateway. The Mesh ID number serves as the identifier for the configurator interface that is used to configure the gateway. The mesh ID number is permanent and cannot be changed.

IEC6400 Gateways

The IEC6400 gateway is deployed at the data center level to ensure IP address reachability throughout the entire network. The gateway has total three LAN interfaces (see Figure 3: Rear Panel View):

- One dedicated to CIMC management port (port 9) to access the CIMC CLI

- Two dedicated ethernet data ports (ports 10 and 11) to access the gateway's GUI and CLI

The gateway and all other edge gateways must be provided with a private LAN IP address, and they are accessed through the private IP addresses.

External Features

Front Panel Overview

The following figure shows the front panel features of the IEC6400 gateway:

Figure 2: Front Panel View
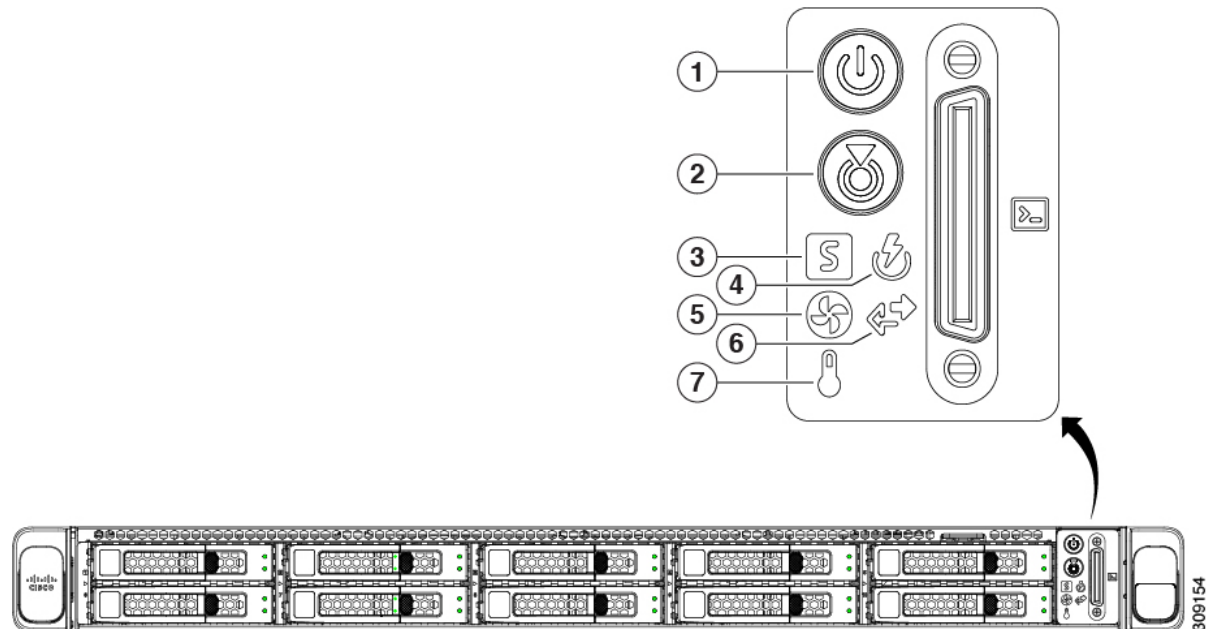
Identification Number in the Front Panel	LED/Button Details
(1)	Power button/LED
(2)	Unit identification
(3)	System health status
(4)	Power supply status
(5)	Fan status
(6)	Network link activity
(7)	Temperature status

Rear Panel Overview

The following figure shows the rear panel features of the IEC6400 gateway:

Figure 3: Rear Panel View
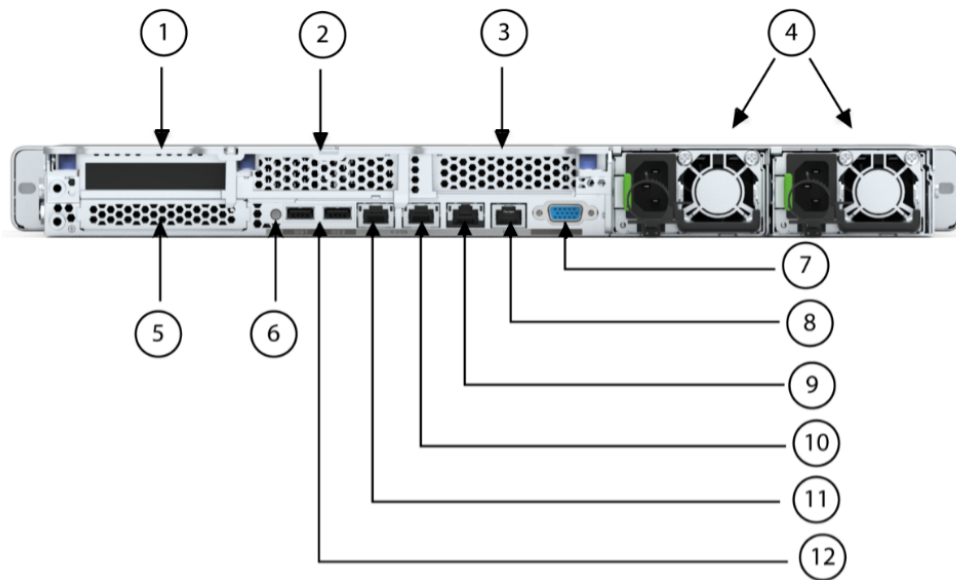
Identification Number in the Rear Panel	Slot Details
(1)	Riser 1, which is controlled by CPU 1: • Supports one PCIe slot • Slot 1 is half height, ¾ length, x16
(2)	Riser 2 (blanking panel)
(3)	Riser 3 (blanking panel)

Identification Number in the Rear Panel	Slot Details
(4)	Power supply units (2x which can be redundant when configured in 1+1 power mode)
(5)	Modular LAN-on-motherboard (mLOM)
(6)	System identification button/LED
(7)	VGA video port (DB-15 connector)
(8)	COM port (RJ-45 connector)
(9)	1 GbE dedicated Ethernet IMC management port
(10) and (11)	Dual 1 Gb/10 GbE Ethernet data ports (LAN1 and LAN2) LAN1 is left connector LAN2 is left connector
(12)	USB 3.0 ports (2x)

UCS C220 M6 server LED pattern

For more details about UCS C220 M6 server LED pattern, see Status LEDs and Buttons.

Installing Gateway in the Rack

Installing Gateway in the Rack

To install the UCS C220 M6 Rack Server in the rack, see Installing the Server.

CHAPTER 3

Initial Gateway Setup

You can perform the initial gateway setup using either of the following methods:

- Using KVM, see Connecting to Gateway for Setup, on page 9, or

- Using CIMC GUI, see Configuring the Cisco Integrated Management Controller, on page 10

Connecting to Gateway for Setup

Before you begin

In this procedure, connect a keyboard and monitor directly to the system for setup. This procedure will use a KVM cable (Cisco PID N20-BKVM) or the ports on the rear panel.

Step 1   Attach a power cord to each power supply ports, and then attach each power cord to a grounded power outlet.

Wait for approximately two minutes to let the gateway boot to standby power during the first bootup. You can verify system power status by looking at the system Power Status LED on the front panel. The system is in standby power mode when the LED is amber.

Step 2   Connect a USB keyboard and VGA monitor to the gateway using one of the following methods:

- Connect an optional KVM cable (Cisco PID N20-BKVM) to the KVM connector on the front panel. Connect your USB keyboard and VGA monitor to the KVM cable.

- Connect a USB keyboard and VGA monitor to the corresponding connectors on the rear panel.

Step 3   To connect with the Cisco IMC Configuration interface:

a)   Press and hold the front panel power button for four seconds to boot the gateway.

b)   During bootup, press **F8** when prompted to open the Cisco IMC Configuration interface.

Note   The first time that you enter the Cisco IMC Configuration interface, you are prompted to change the default password. The default password is *password*.

The password feature is enabled. The following are the requirements for password:

- The password can have a minimum of 8 characters and a maximum of 14 characters.

- The password must not contain the user's name.
- The password must contain characters from three of the following four categories:

  - English uppercase letters (A through Z)

  - English lowercase letters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic character:

    - ! (Exclamation mark)

    - @ (At sign)

    - # (Hashtag)

    - $ (Dollar)

    - % (Percentage)

    - ^ (Circumflex)

    - & (Ampersand)

    - * (Asterisk)

    - - (Minus sign)

    - _ (Underscore)

    - = (Equal)

    - , (Comma)

Step 4   By default, the Cisco IMC uses DHCP to receive the IP address of the device. To assign static IP address to CIMC using CLI, see the latest CLI configuration guide at Cisco UCS C-Series Servers Integrated Management Controller.

Configuring the Cisco Integrated Management Controller

Intially, the Cisco Integrated Management Controller (IMC) management port must be configured with a static IP address. To configure Cisco IMC, follow these steps:

Step 1   Connect the power cord to each power supply port, and then connect each power cord to the grounded power outlet.

Wait for approximately two minutes during the first bootup for the gateway to enter standby power mode. The LED on the front panel turns to amber when the system is in standby power mode.

Step 2   Plug your management ethernet cable into the dedicated management interface (port 9) on the rear panel.

Step 3   Connect through the CIMC LAN management interface (port 9) to the network, which has a DHCP server, to obtain the IP address <a.b.c.d> of the device. Open the web browser and enter the following URL: https//:<A.B.C.D>/

Step 4   (Or) Press and hold the power button for four seconds to boot the gateway.

> **Note**   The first time that you enter the Cisco IMC configuration interface, you are prompted to change the default password. The default password is *password*.

The following are the requirements for password:

- The password must have minimum of 8 characters and a maximum of 14 characters.

- The password must not contain the user's name.
- The password must contain characters from three of the following four categories:

    - English uppercase letters (A through Z)

    - English lowercase letters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic character:

        - ! (Exclamation mark)

        - @ (At sign)

        - # (Hashtag)

        - $ (Dollar)

        - % (Percentage)

        - ^ (Circumflex)

        - & (Ampersand)

        - * (Asterisk)

        - - (Minus sign)

        - _ (Underscore)

        - = (Equal)

        - , (Comma)

Step 5	Click [icon] at the left corner.
	A left pane appears.
Step 6	Go to **Admin** > **Networking**.
	A new **Network** page appears.

Step 7 In the **IPv4 Properties**, uncheck the **Use DHCP** check box.

> **Note** Before you enable DHCP, you must preconfigure your DHCP server with the range of MAC addresses for this gateway.
>
> The NIC mode is **Dedicated** as there is a dedicated ethernet management port and it must not be changed.

Step 8 Enter the **Management IP Address**, **Subnet Mask**, **Gateway**, **Preferred DNS Server**, and **Alternate DNS Server** fields.

The static IPv4 and IPv6 settings include the following:

- Cisco IMC IPv4 address

- Gateway IPv4 address

  For IPv6, if you do not know the gateway, you can set it as none by entering :: (two colons).

- Preferred DNS server address

  For IPv6, you can set this as none by entering :: (two colons).

Step 9 (Optional) Update the **VLAN Properties**.

Step 10 (Optional) Set a hostname for the server.

Step 11 (Optional) Enable dynamic DNS and set a dynamic DNS (DDNS) domain.

Step 12 Click **Save Changes**.

The device reboots and you must refresh the browser to establish connection with the new management IP address.

Connecting to Gateway Console Port

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

Step 1   Connect a nine-pin female DB-9 to RJ-45 serial cable on one side to the RJ-45 serial port on the gateway and the other side to the COM port on a computer.

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

Step 3   If you are logging in for the first time, use the standard command prompt (>) mode to execute unprivileged commands. Use the default username and password to login: Cisco.

Note   Once the initial configuration completes, ensure that you remove the serial cable from the gateway.

Log into Gateway Configurator for the First Time

You can log into the gateway configurator using any three of the following methods:

- Using configurator interface or through SSH from data ports using CLI, see Log into the Gateway Configurator for the First Time, on page 15

- Using CIMC CLI, see Accessing Gateway's CLI from CIMC CLI, on page 15

Accessing Gateway's CLI from CIMC CLI

Use CIMC CLI to access the server for configuring the IEC6400 gateway:

Step 1 To connect with the server through the serial console, use the following CLI command: `device# connect host`

Step 2 Enter the username and password.

Credentials are *Cisco/Cisco*.

Step 3 To retrieve the details of DHCP address in the provisioning mode, use the following CLI command: `device# ip`

Step 4 At first, use the CLI command to set new username and password: `device# credentials`

Step 5 Login with default login credentials and then enter the new username and password. For rules on creating the new login credentials, see Rules to Reset the Login Credentials, on page 19.

After successful login, the device is in provisioning mode.

Log into the Gateway Configurator for the First Time

Follow the steps to access the IEC-6400-URWB Configurator:

Before you begin

Before you login, disable the Wi-Fi on your computer to prevent routing issues between the computer's wired and wireless network interfaces. The IEC-6400-URWB configurator allows you to configure the IEC6400 gateway.

Step 1 Power on the gateway and wait for atleast five minutes to allow the boot sequence to finish.

Step 2 Connect one end of a CAT5/6 ethernet cable to the computer and the other end of the cable to the LAN port on the gateway.

> **Note** The configurator interface and SSH can be accessible through the data ports 10 and 11 (see Figure 3: Rear Panel View).

Step 3 Launch the computer's web browser.

Step 4 To access the configurator, open the web browser and enter the following URL: https://<IP address of gateway>/
The **IEC-6400-URWB Configurator** login window appears.

> **Note** The web browser may display security warnings because the IEC6400 gateway is connected to the computer using an unsecured CAT5/6 cable connection. Ignoring these warnings is safe and expected during the configuration process.

Step 5 Enter the username and password in the respective fields. Following are the factory-set login details:

- **Username**: Cisco

- **Password**: Cisco

Step 6 Click **Login**.

Changing the Default Login Credentials

Before you begin

After your initial login, the configurator prompts you to change the gateway's login credentials and mesh passphrase. You can perform this task using either of the following methods:

Configuring New Login Credentials using GUI

To change the login credentials, follow these steps:

Step 1   Enter the current username in the **Current username** field.

Step 2   Enter the current password in the **Current password** field.

Step 3   Enter the new username in the **New username** field.

Step 4   Enter the new password in the **New password** field. For rules on creating the new login credentials, see Rules to Reset the Login Credentials.

Step 5   Re-enter the new password in the **Confirm new password** field.

Step 6   Enter the current mesh passphrase in the **Mesh passphrase** field.

Step 7   Enter the new mesh passphrase in the **Confirm mesh passphrase** field.

Step 8   Click **Change**.

The **IEC-6400- URWB Configurator** window appears.

Configuring New Login Credentials using CLI

You can access the gateway's CLI using either of the following methods:

- Through SSH from data ports, see Log into the Gateway Configurator for the First Time, on page 15

- Through CIMC CLI, see Accessing Gateway's CLI from CIMC CLI, on page 15

To know the default IP address for SSH connection, see Configuring the Gateway Initially in Provisioning Mode, on page 22.

Step 1 To configure new login credentials using the GUI or CLI, see Rules to Reset the Login Credentials.

Note The default login credentials are:

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

Step 2 To reset the login credentials, use the following example credentials:

```
username: demouser
password: DemoP@ssw0rd
```

• Example of configuring a password from the CLI:

```
Device# # iotod-iw configure offline
Switching to IOTOD IW Offline mode...
```

Step 3   After the first login, reset your credentials:

```
Old username:Cisco
Old Password:Cisco
New username:demouser
New Password:DemoP@ssw0rd
Confirm Password:DemoP@ssw0rd
Mesh Passphrase:
Confirm Mesh Passphrase:
YES
```

Step 4   After successful credentials change, login again:

```
User access verification
Username: demouser
Password: DemoP@ssw0rd
```

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

Rules to Reset the Login Credentials

When the gateway is switched to offline mode (after the initial login), you need to set a new login credential for the gateway. To configure a new password using a GUI or CLI, the login credentials should follow the criteria:

• The username length must be from 1 to 32 characters.

• The password length must be from 8 to 32 characters.

• The password must include at least one uppercase character, one lowercase character, one digit, and one special character.

• The following special characters are permitted:

    • ! (Exclamation mark)

    • * (Asterisk)

    • + (Plus sign)

    • - (Minus sign)

    • , (Comma)

    • - (Hyphen)

    • @ (At sign)

    • ^ (Circumflex)

    • _ (Underscore)

- The password must not contain:
    - White spaces
    - Name like Cisco, such as CiSc0 or 0cSiC
    - Three sequential characters or digits (ABC/ CBA) or (123/321)
    - The same three characters or digits consecutively (AAA) or (666)
    - Same as or the reverse of the username
    - Same as the current or existing password

C H A P T E R **5**

Configuring the Gateway Initially in Provisioning Mode

You can use IoT OD IW for online cloud configuration or alternatively you can switch to offline mode for configuring the gateway manually using the CLI or web UI.

Switching Between Offline and Online modes

To switch between offline and online mode, follow these steps:

Step 1 Log into the configurator interface, see Log into the Gateway Configurator for the First Time.
The **URWB IEC-6400-URWB Configurator** window appears.

Step 2   Click **IOTOD IW**.
IOT OD IW Configuration Mode window appears.

Step 3   **IOT OD IW Configuration Mode** section has two options. Click the option you need:

• **Online Cloud-Managed** mode

• **Offline** mode

Step 4   Click **Confirm**.

• If you select **Online Cloud-Managed mode**, a 10 second countdown pop-up appears.

• If you select **Offline mode**, a five second countdown pop-up appears.

Configuring the Gateway Initially in Provisioning Mode

The IEC6400 gateway running on URWB mode supports configuration from IoT OD IW or using local management configurator interface. IoT OD is the cloud management portal, where the gateway connects to the online cloud through the network. In the offline mode, the gateway is configured using the CLI or web

UI. A gateway with no configuration settings defaults to provisioning mode, which allows the initial configuration to be sent to the gateway from IoT OD IW.

- The provisioning mode where the gateway attempts to request network configuration using the DHCP and connects to IoT OD IW.

- If there is no network connectivity, the gateway can be configured locally using either GUI, or CLI and it is accessible through console port.

The DHCP server assigns a default gateway and domain name system (DNS) server. IoT OD uses DNS geo-location to direct the gateway 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 used only in provisioning mode. A static IP address must be assigned for normal operation. If DHCP is unavailable and configuration using IoT OD IW is required, the IP address, subnet, default gateway, and DNS can be manually configured.

Note When the gateway is in provisioning mode, the gateway attempts to get an IP address from a DHCP server. If the gateway fails to receive an IP address using DHCP, the gateway reverts to a fallback IP address of 192.168.0.10/24. For easier accessibility, the gateway is also assigned an additional backup IP address as 169.254.C.D, where C and D are the last two octets of the Mesh ID.

Initial Mode	Gateway Status	Solution	Gateway Mode	Refer
Provisioning mode	Gets an IP address from DHCP	Yes (Received IP address)	Configure the gateway using IoT OD IW (Online mode)	If the gateway status is shown as Online, do the next step by Configuring the gateway using IoT OD IW
		No (Reverts to fallback IP address)	Configure the gateway using the configurator Web UI or CLI (Offline mode)	If the gateway status is shown as Offline, do the next step by Log into the Gateway Configurator for the First Time

Troubleshooting: Gateway Status in Provisioning Mode	Refer topic
If the gateway connects to the network in provisioning mode, but not able to connect to IoT OD IW.	Gateway Fails to Connect to IoT OD IW, on page 25
If the gateway is not able to connect to the network.	Gateway Fails to Connect to the Network, on page 26

Gateway in Provisioning Mode

The gateway is in provisioning mode if the status is shown as **Provisioning**.

Alternatively, if the status of IoT OD IW is shown as **Online** or **Offline**, you must choose between two further options:

- To configure the gateway as a new gateway, revert the gateway to provisioning mode and reset the gateway, see Resetting the Gateway to Factory Default using GUI.

- To change the connection settings with the current configuration, see Configuring General Settings using GUI.

To verify if the gateway is in provisioning mode, use the following CLI command:

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

Gateway in Disconnected Mode

If the gateway is in provisioning mode, IoT OD IW status is shown as:

When the gateway fails to receive an IP address from the DHCP server, it reverts to the fallback IP address (192.168.0.10/24).

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

Gateway in Connected Mode

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

IOTOD IW Cloud connection info	
Server Host:	**IOTOD Industrial Wireless**
Status:	Connected
Current IP Configuration	
Current IP:	
Current Netmask:	255.255.255.0

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

✎

Note   IP, Netmask, Default Gateway, Primary DNS, and Secondary DNS configuration (**ip** command) must be allowed when provisioning mode is on.

```
Device# ip [ addr <static IP address> [ netmask <static netmask> [ gateway <IP
address of default gateway[ dns1 <IP of primary DNS server> [ dns2 <IP of
alternate DNS server> ] ] ] ] ]
```

Example:

```
Device# ip addr 192.168.10.2 netmask 255.255.255.0 gateway 192.168.10.1 dns1
192.168.10.200 dns2 192.168.10.201
```

Gateway Fails to Connect to IoT OD IW

If the gateway obtains an IP address through DHCP but cannot connect to IoT OD IW, it will retain the DHCP-assigned IP address instead of reverting to the fallback IP address. To connect the gateway to IoT OD IW, follow these steps:

Step 1   Check if the ethernet cable leading to the gateway is connected properly.

Step 2   Check if the local DNS server can fix the IP address of an IoT OD IW cloud server and verify if the IP address can be reached.

Step 3   Check if the gateway uses an outbound HTTPS connection on tcp/443 for the following domains:

- gateway.ciscoiot.com

- us.ciscoiot.com

- eu.ciscoiot.com

Step 4   During the provisioning mode, if the gateway fails to connect to IoT OD IW, the device remains in provisioning mode. You must manually configure the gateway in offline mode to change the state.

Gateway Fails to Connect to the Network

Before you begin

Verify the following for the gateway:

- It is in the correct VLAN.

- It can reach the DHCP server.

- The DHCP server has an IP address assigned to the gateway.

To connect to the network, follow these steps:

Step 1 If needed, enter the values for the following fields in **IOT OD IW** window:

- **Local IP**

- **Local Netmask**

- **Default Gateway**

- **Local Dns 1**

- **Local Dns 2**

Step 2 Click **Save fallback IP**.

The web browser shows the gateway reboot window appears.

192.168.0.10

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 (192.168.0.11) properly. Reboot to apply the changes?

Reset   OK
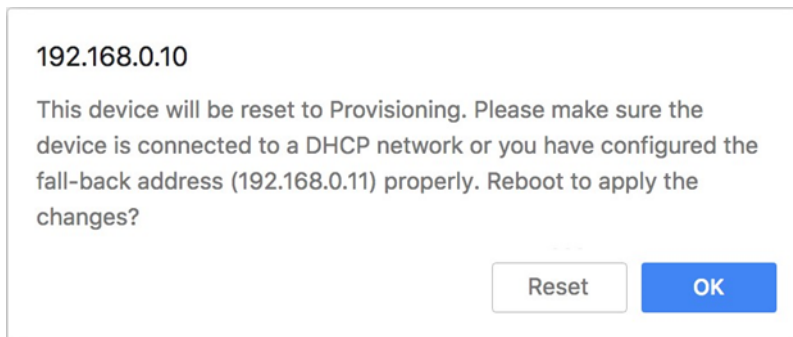
Step 3 Click **OK**, then the gateway reboots and remains in provisioning mode and the gateway tries to connect to the network using the new connection values.

Step 4 If the gateway cannot connect to the network using the **DHCP** settings, **IOT OD IW Cloud connection** info status is shown 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

To verify if the gateway is in provisioning mode and it is not connected to IoT OD IW, use the following CLI command:

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

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

```
Device# ip
IP: 192.168.0.10
Network: 255.255.255.0
Device:
Nameservers:
DHCP Address (PROVISIONING Mode):
IP: 10.115.11.29
Network: 255.255.255.0
Device: 10.115.11.1
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 gateway in provisioning mode but not able to retrieve the IP address from the DHCP server, so it uses the fallback IP address of 192.168.0.10:

```
Device# ip
IP: 192.168.0.10
Network: 255.255.255.0
Device:
Nameservers:
DHCP Address (PROVISIONING Mode):
IP: 192.168.0.10
Network: 255.255.255.0
Device:
Nameservers: 127.0.0.1
Fallback Address (PROVISIONING Mode):
IP: 169.254.201.72
Network: 255.255.0.0
```

Configuring General Settings using GUI

Before you begin

By default, when the **General Mode** window is opened for the first time, the **Local IP**, **Local netmask**, and **LAN parameters** fields are with factory-set default values.

The general mode window contains controls on how to monitor and/or change the following settings:

- Shared network passphrase

- Gateway's LAN parameters

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

Step 1   In the **GENERAL SETTINGS**, click **general mode**.
The **GENERAL MODE** window appears.

GENERAL MODE

General Mode

"Mesh Passphrase" is an alphanumeric string or special characters excluding '[apex] "[double apex] `[backtick] $ [dollar] =[equal] \[backslash] <[left angle bracket] >[right angle bracket] #[hash] %[percent] ([left bracket])[right bracket] &[ampersand] and whitespace (e.g. "mysecurecamnet") that indentifies your network. It MUST be the same for all the Cisco URWB units belonging to the same network.

Mesh Passphrase: ●●●●●●●●●●

Show passphrase: ☐

LAN Parameters

Local IP: 10.115.11.81

Local Netmask: 255.255.255.0

Default Gateway: 10.115.11.1

Local Dns 1: 8.8.8.8

Local Dns 2:

Reset   Save

Step 2   In the **General Mode** section, verify that the **Mesh Passphrase** field is set as desired.

Check the **Show passphrase** check box to see the **Mesh Passphrase** field.

Step 3   In the **LAN Parameters** section, enter the following details:

- Enter the local IP address in the **Local IP** field.

- Enter the local netmask address in the **Local Netmask** field.

- Enter the default gateway IP address in the **Default Gateway** field.

- Enter the local primary DNS IP address value in the **Local Dns 1** field.

- Enter the local secondary DNS IP address value in the **Local Dns 2** field.

Step 4   Click **Save**.

Configuring LAN Parameters using CLI

To configure LAN parameters, use the following CLI command:

Example:

```
ip addr 192.168.10.2 netmask 255.255.255.0 gateway 192.168.10.1 dns1
192.168.10.200 dns2 192.168.10.201
```

Resetting the Gateway to Factory Default using GUI

To reset the gateway to its factory defaults, follow these steps:

Step 1   In the **MANAGEMENT SETTINGS**, click **reset factory defaults**.
The gateway reset window appears.

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

NO	YES

Step 2   Click **YES** to reset the gateway with the factory reset or click **NO**.

Note   If you have previously saved the gateway configuration file, you can restore the saved configuration settings to the gateway as described in Saving and Restoring the Gateway Settings.

Note   Perform a hard reset only if the gateway needs to be reconfigured using its factory configuration as an unpacked gateway. A hard reset performs the reset of the gateway's IP address, administrator password, and then it disconnects the gateway from the network. Instead, if you want to reboot the gateway, see Rebooting the Gateway using GUI.

Resetting the Gateway to Factory Default using CLI

To perform reset the configuration, use the following CLI command:

```
Device# factory reset config
Factory reset configuration and reboot? Type YES to continue.
```

Enter YES in the CLI command to start the device reset.

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

```
Device# factory reset default
WARNING: Secure data wipe will be performed on the next reboot. This could take a long time
```

```
 DO NOT POWER OFF THE DEVICE DURING THIS OPERATION!
Perform DATA WIPE (Configuration, logs, crashfiles) and reboot? Type YES to continue.
```

These 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 enter `n` to abort the process.

Rebooting the Gateway using GUI

Before you begin

This procedure allows you to reboot the gateway's operating system.

Step 1 In the **MANAGEMENT SETTINGS**, click **reboot**.
The gateway reboot window appears.

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

| No | Yes |

Step 2 Click **Yes** to reboot.

Rebooting the Gateway using CLI

To perform a reboot, use the following CLI command:

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

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

Saving and Restoring the Gateway Settings

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

• Save the gateway's current software configuration as a configuration (*.conf) file.

• Upload and apply a saved configuration file to the current gateway.

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

Tip	Saved configuration files can be reused for all gateways of the same type. It simplifies the configuration task.
	These saved configuration files act as configuration backup files to speed up redeployment if you need to replace the damaged gateway with a new gateway of the same type.

Downloading the Gateway's Current Configuration Settings

Before you begin

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

Step 1 In the **MANAGEMENT SETTINGS**, click **configuration settings**.
The **LOAD OR RESTORE SETTINGS** window appears.

Step 2 Click **Save** to download the gateway's configuration (*.conf) file.

Uploading a Saved Configuration File to the Gateway

To upload the saved configuration file on to the gateway, follow these steps:

Before you begin

Before initiating the restoration process using the configuration file, ensure you have the file stored on your computer. For downloading the file, see Downloading the Gateway's Current Configuration Settings.

Step 1   In the **MANAGEMENT SETTINGS**, click **configuration settings**.
The **LOAD OR RESTORE SETTINGS** window appears.

Step 2   Click **Browse** to upload the configuration (*.conf) file.
The selected configuration file is shown next to the **Browse** button.

Step 3   Click **Restore** to apply the configuration settings to the gateway.
Once you apply the configuration, the gateway starts rebooting.

Configuring IoT OD IW Online and Offline Mode using CLI

To configure the gateway using IoT OD IW, use the following CLI command:

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

Online – It sets up IoT OD IW to online mode. The gateway can be managed from an IoT OD IW cloud server.

Offline – It sets up IoT OD IW in offline mode. The gateway is disconnected from IoT OD IW and must be manually configured.

To configure the gateway using IoT OD IW, see Configure IW gateways in online / offline mode.

Configuring Advanced Settings

Configuring SNMP using CLI

URWB software for network management functionalities uses SNMP applications. The SNMP implementation supports queries (solicited) and traps (unsolicited). If you enable SNMP traps, specify the server address to which the monitoring information is sent.

Note   The same SNMP configuration must be set for all gateways in the network.

To configure SNMP, use the following CLI commands:

Note   All parameters of SNMP are required to be configured before enabling SNMP feature using CLI:

```
snmp enabled
```

Table 1: SNMP CLI Commands

Purpose	Command or Action
To enable or disable SNMP functionality	`Device# snmp [enabled	disabled]`

Purpose	Command or Action
To specify the SNMP protocol version	`Device# snmp version {v2c	v3}`
To specify the SNMP v2c community ID number (SNMP v2c)	`Device# snmp community-id <length 1-64>`
To specify the SNMP v3 username (SNMP v3)	`Device# snmp username <length 32>`
To specify the SNMP v3 user password (SNMP v3)	`Device# snmp password <length 8-64>`
To specify the SNMP v3 authentication protocol (SNMP v3)	`Device# snmp auth-method <MD5|SHA|SHA-224|SHA-256|SHA-384|SHA-512>`
To specify the SNMP v3 encryption protocol (SNMP v3)	`Device# snmp encryption {aes	none}` **Note** Possible encryption value is aes. Alternatively, enter none if the v3 encryption protocol is not needed.
To specify the SNMP v3 encryption passphrase (SNMP v3)	`Device# snmp secret <length 8-64>`
To specify the SNMP periodic trap settings	`Device# snmp periodic-trap {enabled	disabled}`
To specify the notification trap period for periodic SNMP traps	`Device# snmp trap-period <1-2147483647>` **Note** Notification value trap period measured in minutes.
To enable or disable SNMP event traps	`Device# snmp event-trap {enabled	disabled}`
To specify the SNMP NMS hostname or IP address	`Device# snmp nms-hostname {hostname |Ip Address}`
To disable SNMP configuration	`Device# snmp disabled`

Table 2: Example of SNMP configuration:

Purpose	Command or Action

To configure SNMP v2	`Device# snmp community-id <length 1-64>`
	`Device # snmp nms-hostname hostname/Ip Address`
	`Device # snmp trap-period <1-2147483647>`
	`Device # snmp periodic-trap enabled/disabled`
	`Device # snmp event-trap enabled/disabled`
	`Device # snmp version v2c`
	`Device # snmp enabled`

Purpose	Command or Action

To configure SNMP v3	`Device # snmp nms-hostname hostname/Ip Address`
	`Device # snmp trap-period <1-2147483647>`
	`Device # snmp username <length 32>`
	`Device # snmp password <length 8-64>`
	`Device # snmp auth-method`
	`<MD5|SHA|SHA-224|SHA-256|SHA-384|SHA-512>`
	`Device # snmp encryption <aes| none>`
	`Device # snmp secret <length 8-64>`
	`Device # snmp periodic-trap enabled/disabled`
	`Device # snmp event-trap enabled/disabled`

Configuring SNMP Version v2c using GUI

By default, the gateways are shipped from the factory with SNMP in disabled mode.

To change the gateway's SNMP mode to version **v2c** and configure the gateway, follow these steps:

Step 1   Choose the version **v2c** from the **SNMP mode** drop-down list.
The **SNMP** window appears.

Step 2   Enter the community identity value in the **Community ID** field.

    Important   The same community identity value must be set for all the gateways in the network.

Step 3   Check the **Enable SNMP event trap** check box to enable SNMP event traps for significant system-related events, and then enter the network management station (NMS) host name in the **NMS hostname** field.

    Important   The NMS host to which traps are sent must have an SNMP agent that is configured to collect SNMP v2c traps.

Step 4   Check the **Enable SNMP periodic trap** check box to enable periodic SNMP traps to send SNMP traps at defined periodic intervals and then enter the host name of NMS in the **NMS hostname** field. Enter the notification period (minutes) in the **Notification period**.

Step 5   Click **Save**.

Configuring SNMP Version v3 using GUI

By default, the gateways are shipped from the factory with SNMP in disabled mode.

To change the gateway's SNMP mode to version **v3** and then configure the gateway, follow these steps:

Step 1   Choose the version **v3** from the **SNMP mode** drop-down list.
The **SNMP** window appears.

Step 2   Enter the SNMP v3 username in the **SNMP v3 username** field.

Note   The same SNMP v3 username must be set for all the gateways in the network.

Step 3   To change the current SNMP v3 password, enter the new password in the **SNMP v3 password** field.

Check the **Show SNMP v3 password** check box to see the **SNMP v3 password** field.

Step 4   Choose the authentication type from the **SNMP v3 authentication proto** drop-down list. The available options are:

• **MD5**

        • **SHA**

        • **SHA-224**

        • **SHA-256**

        • **SHA-384**

        • **SHA-512**

Important   The same SNMP authentication protocol must be set for all the gateways in the network.

Step 5   Choose the appropriate encryption protocol from the **SNMP v3 encryption** drop-down list. The available options are:

        • **No Encryption**

        • **AES** (Advanced Encryption Standard)

Note   The same encryption protocol must be set for all the gateways in the network.

Step 6   To change the encryption passphrase, enter a new passphrase in the **SNMP v3 encryption passphrase** field.

Step 7   Check the **Enable SNMP event trap** check box to enable the SNMP event traps for significant system-related events and then enter the host name of NMS in the **NMS hostname** field.

Note   The NMS host to which traps are sent must have an SNMP agent configured to collect v3 traps.

Step 8   Check the **Enable SNMP periodic trap** check box to enable the periodic SNMP traps to send SNMP traps at defined periodic intervals and then enter the host name of NMS in the **NMS hostname** field. Enter the notification period (minutes) in the **Notification period**.

Step 9   Click **Save**.

Configuring NTP using GUI

The gateway has NTP functionality that allows it to synchronize the time settings with a chosen network time server.

☞

Important   The same NTP configuration must be set for all the gateways in the network. If the same NTP settings are not applied to all gateways, the network may encounter timestamp conflicts and/or device malfunctions.

To change the NTP settings, follow these steps:

Step 1   In the **ADVANCED SETTINGS**, click **ntp**.
The **NTP - Network Time Protocol** window appears.

Step 2   Check the **Enable NTP** check box to enable the NTP synchronization.

Step 3   Enter the host name of a chosen primary NTP server in the **NTP server hostname** field.

Step 4   Choose the authentication method from the **NTP authentication** drop-down list. Following are the available options:

- **None** (does not require an NTP password)

- **SHA1**

- **SHA256**

- **SHA512**

Step 5   Enter the password in the **NTP password** field.

Check the **show** check box to see the **NTP password** field.

Note	To configure a new password using a GUI or CLI, the password should match the following criteria:

- The password must be at least 10 characters.

- The following special characters are not allowed:

    - ' (apex)

    - " (double apex)

    - ` (backtick)

    - $ (dollar)

    - = (equal)

    - \ (backslash)

    - # (number sign)

    - & (ampersand)

    - < > (angle brackets)

    - % (percent sign)

    - white spaces

Step 6   Enter the NTP key id in the **NTP key id** field.

Step 7   Choose the time zone from the **Select Timezone** drop-down list.

Step 8   Click **Save**.

Configuring NTP using CLI

To configure an NTP server address, use the following CLI command:

```
Device# ntp server <string>
```

String - IP address or domain name.

Example:

```
Device# ntp server 192.168.216.201
```

To configure an NTP authentication, use the following CLI command:

```
Device# ntp server-auth None
Device# configure ntp server-auth SHA1 <password> <keyid>
Device# configure ntp server-auth SHA256 <password> <keyid>
Device# configure ntp server-auth SHA512 <password> <keyid>
```

none - disable NTP authentication md5

sha1 - authentication method

Example:

```
Device# # ntp server-auth SHA1 test12345 65535
```

| Note | To configure a new password using a GUI or CLI, the password should match the following criteria: |

- The password must be at least 10 characters.

- The following special characters are not allowed:

  - ' (apex)

  - " (double apex)

  - ` (backtick)

  - $ (dollar)

  - = (equal)

  - \ (backslash)

  - # (number sign)

  - & (ampersand)

  - < > (angle brackets)

  - % (percent sign)

  - white spaces

To enable or disable the NTP service, use the following CLI command:

```
Device# ntp { enabled|disabled }
```

To configure the NTP timezone, use the following CLI command:

```
Device# ntp timezone <string>
```

Example:

```
Device# ntp timezone Asia/Shanghai
```

To validate NTP configuration and status, use the following CLI commands:

```
Device# ntp
NTP: enabled
NTP: 192.168.216.201
Server auth: SHA1
Timezone: Asia/Shanghai
Current date: Thu 02 Nov 2023 07:15:02 PM CET
```
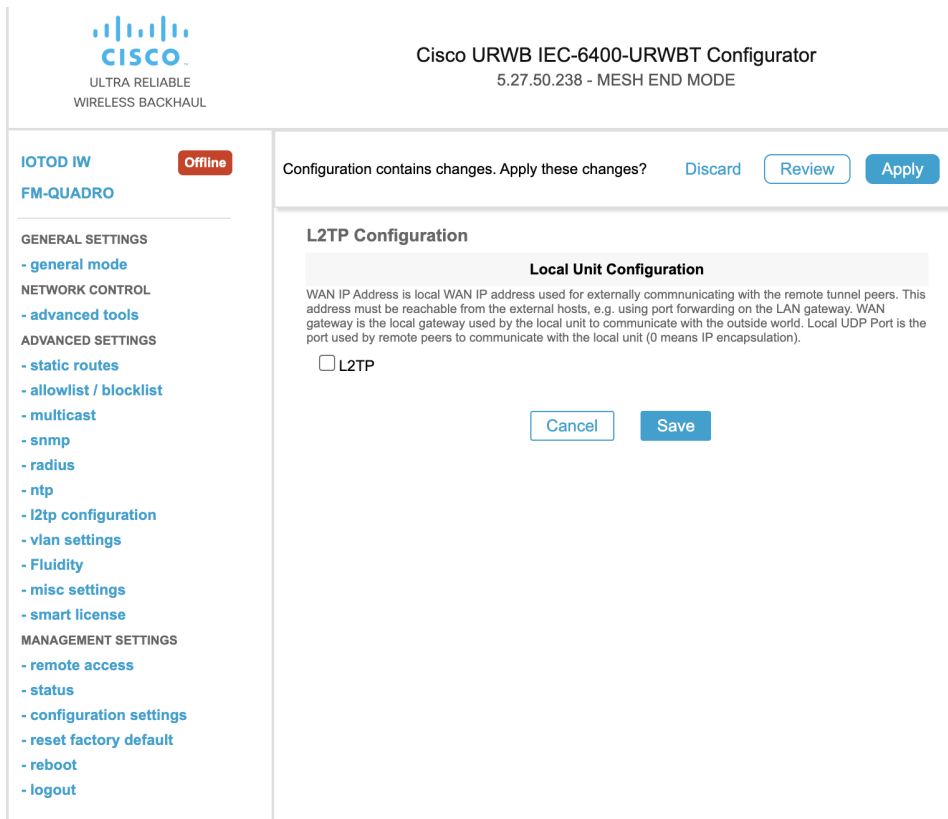
Configuring L2TP using GUI

Layer 2 Tunneling Protocol (L2TP) functionality allows the devices to support integration of URWB Fluidity technology in Layer 3 networks. To configure L2TP links, follow these steps:

Step 1 In the **ADVANCED SETTINGS**, click **lt2p configuration**.

The **L2TP Configuration** window appears.

CISCO

ULTRA RELIABLE
WIRELESS BACKHAUL

Cisco URWB IEC-6400-URWBT Configurator
5.27.50.238 - MESH END MODE

IOTOD IW   Offline
FM-QUADRO

Configuration contains changes. Apply these changes?   Discard   Review   Apply

GENERAL SETTINGS
- general mode
NETWORK CONTROL
- advanced tools
ADVANCED SETTINGS
- static routes
- allowlist / blocklist
- multicast
- snmp
- radius
- ntp
- l2tp configuration
- vlan settings
- Fluidity
- misc settings
- smart license
MANAGEMENT SETTINGS
- remote access
- status
- configuration settings
- reset factory default
- reboot
- logout

L2TP Configuration

Local Unit Configuration

WAN IP Address is local WAN IP address used for externally commnunicating with the remote tunnel peers. This address must be reachable from the external hosts, e.g. using port forwarding on the LAN gateway. WAN gateway is the local gateway used by the local unit to communicate with the outside world. Local UDP Port is the port used by remote peers to communicate with the local unit (0 means IP encapsulation).

☐ L2TP

Cancel   Save

Step 2   Check the **L2TP** check box to enable the configuration.

The L2TP detailed configuration settings appears.

Step 3   Enter the following details:

- • WAN IP Address

   • WAN Netmask

   • WAN Gateway

   • Local UDP Port

   • Max number of L2TP tunnels

Step 4   Click **Save**.

Step 5   To add a L2TP tunnel to remote host:

a)   Enter the **Remote WAN IP Address** and **Remote UDP Port** details.

b)   Click **Add**.

Configuring L2TP using CLI

To enable or disable the L2TP configuration, use the following CLI command:

```
Device# l2tp status <enable or disable>
```

Example:

```
l2tp status enable
```

To set the interface port for the L2TP communication with the gateway, use the following CLI command:

```
Device# l2tp interface <1 or 2>
```

Port 1 = ethernet LAN ports bridge

Port 2 = SFP+ ports bridge

Example:

```
Device# l2tp interface 1
```

To configure L2TP WAN parameters, use the following CLI command:

```
Device# l2tp wan <WAN IP address> <WAN netmask> <WAN gateway address>
```

Example:

```
Device# l2tp wan 192.168.0.20 255.255.255.0 192.168.0.1
```

To configure L2TP WAN interface port, use the following CLI command:

```
Device# l2tp port <UDP port>
```

Example:

```
Device# l2tp port 5701
```

Note The unsigned integer range of UDP port of remote peer is [1-65535].

To add a L2TP tunnel to remote host, use the following CLI command:

```
Device# l2tp add <IP address of remote peer> <UDP port number of remote peer>
```

Example:

```
Device# l2tp add 192.168.20.20 5701
```

Note The unsigned integer range of UDP port of remote peer is [1-65535].

To print the current list of L2TP tunnels, use the following CLI command:

```
Device# l2tp
```

To delete the L2TP tunnel, use the following CLI command:

```
Device# l2tp del <tunnel-ID>
```

tunnel-ID – It is shown in the list of L2TP tunnels. Use command `l2tp` to print the list.

Configuring VLAN Settings

Default VLAN configuration factory-set parameters for the gateway are:

Parameter	Default value
Management VLAN ID (MVID)	1
Native VLAN ID (NVID)	1

To connect the gateway to a VLAN that is part of the local wireless network, follow these steps:

Step 1 In the **ADVANCED SETTINGS**, click **vlan settings**.

The **VLAN SETTINGS** window appears.

VLAN SETTINGS

When the Native VLAN is enabled (VID != 0), untagged packets received on the trunk port will be assigned to the specified VLAN ID. When disabled (VID = 0), VLAN trunking will operate according to the IEEE 802.1Q standard, i.e. only tagged packets will be allowed on the port (including those of the management VLAN).

VLAN Settings

Enable VLANs: ☐

Management VLAN ID: 1

Native VLAN ID: 1

Reset   Save

Step 2 Check the **Enable VLANs** check box to connect the gateway to a VLAN that is part of the local wireless network.

Step 3 Enter the management identification number of the VLAN in the **Management VLAN ID** field. For detailed info about vlan settings and packet management, see Rules for Packet Management.

Note The same Management VLAN ID must be used on all the gateways that are part of the same mesh network.

Step 4 Enter the native identification number of the VLAN in the **Native VLAN ID** field.

Step 5 Click **Save**.

Rules for Packet Management

Parameter	Default value
Native VLAN processing	Enabled
Port mode (all Ethernet ports)	Smart

Traffic Management

The incoming data packets are classified based on the following parameter values:

Parameter	Default value
Signaling	Ethernet protocol type
User	All other traffic
Packet tagged with MVID	Packet allowed

Access port rules for incoming packets	
Untagged packet from the gateway	Packet allowed
Untagged packet with VLAN ID (VID) is not configured	Packet allowed
Untagged packet with VID is configured	Packet tagged with specified VID
Tagged packet with valid VID	Packet dropped
Tagged packet with null (0) VID	Packet dropped

Access port rules for outgoing packets	
Tagged packet with configured and allowed VID	Packet allowed
Packet from the gateway	Packet allowed
Tagged packet with VID is not configured	Packet allowed

Parameter	Default value
Tagged packet with valid VID, but not allowed	Packet dropped
Tagged packet with null (0) VID	Packet dropped

Access port rules management for incoming packets with a gateway in smart mode	
Untagged packet	If native VLAN is ON, then the packet is allowed (tagged with NVID) If native VLAN is OFF, then the packet is dropped
Tagged packet (any VID without any check)	Packet allowed with original tag

Access port rules management for outgoing packets with a gateway in smart mode	
Packets from the gateways (for example: IoT OD IW interface)	Packet tagged with MVID
Signaling traffic	Packet tagged with MVID
Tagged with valid VID (1–4095), but not with NVID	Packet allowed (tagged)
Tagged with null VID (0) or NVID	Packet allowed (untagged)

✎

Note   The packets transmitted through the Cisco VIC SFP+ interface is always tagged with a VLAN header. The outgoing packets from the interface are classified as untagged with an IEEE 802.1p header and VLAN ID tag of 0.

Configuring Fluidity Settings using GUI

To change the fluidity settings, follow these steps:

Before you begin

By default, the gateways are shipped from the factory with Fluidity functionality in disabled mode.

Step 1   In the **ADVANCED SETTINGS**, click **Fluidity**.
The **FLUIDITY** window appears.

FLUIDITY

Fluidity Settings

The unit can operate in 3 modes: Infrastructure, Infrastructure (wireless relay), Vehicle.
The unit must be set as Infrastructure when it acts as the entry point of the infrastructure for the mobile vehicles and it is connected to a wired network (backbone) which possibly includes other Infrastructure nodes. The unit must be set as Infrastructure (wireless relay) ONLY when it is used as a wireless relay agent to other Infrastructure units. In this operating mode, the unit MUST NOT be connected to the wired network backbone as it will use the wireless connection to relay the data coming form the mobile units.
The unit must be set as Vehicle when it is mobile. Vehicle ID must be set ONLY when the unit is configured as Vehicle. Specifically, Vehicle ID must be a unique among all the mobile units installed on the same vehicle. Unit installed on different vehicles must use different Vehicle IDs.
The Network Type filed must be set according to the general network architecture. Choose Flat if the mesh and the infrastructure networks belong to a single layer-2 broadcast domain. Use Multiple Subnets if they are organized as different layer-3 routing domains.

Fluidity ☑ Enable

Unit Role: | Infrastructure ⌄ |

Network Type: | Flat ⌄ |

[Reset]   [Save]

Step 2   Check the **Fluidity** check box to enable the fluidity functionality.

Note   The **Unit Role** drop-down is set to **Infrastructure** mode, and it cannot be changed.

Step 3   Choose the network type designation for the gateway from the **Network Type** drop-down list and it must be set in accordance with the general network architecture. Following are the available options from the network type:

- **Flat**: Choose this option, if both the mesh network and the infrastructure network belong to a single layer 2 broadcast domain.

- **Multiple Subnets**: Choose this option, if the mesh network and the infrastructure network are organized as separate layer 3 routing domains.

Step 4   Click **Save**.

Configuring Fluidity Settings using CLI

To enable fluidity, at least one radio interface should be in fluidity mode:

```
Device# fluidity status enabled
```

Configuring Gateway Status

The gateway status window shows information on basic settings (including the gateway's MAC address) and allows you to download diagnostic data files and view event logs.

In the **MANAGEMENT SETTINGS**, click **status**.

• The **STATUS** window appears.

STATUS

Device: Cisco URWB IEC-6400-URWB
Name: Cisco
ID: 5.27.50.238
Serial: WZP262304VR
Operating Mode: Mesh End
Uptime: 2 days, 2:24 (hh:mm)
Firmware version: 1.0.0.7

DEVICE SETTINGS
IP: 10.115.11.80
Netmask: 255.255.255.0
MAC address: 40:36:5a:1b:32:ee
SFP+ ports
sfp1/0 DOWN
sfp1/1 DOWN
sfp1/2 DOWN
sfp1/3 DOWN
MTU: 1530
Ethernet ports
eth0/0 UP Full-duplex 100
eth0/1 DOWN
MTU: 1530

DIAGNOSTIC TOOL

Download Diagnostics

Open services

Hide Services   Show Services

DEVICE LOGS

Clear Logs   Show Logs

The following details are shown in the **STATUS** section:

• Device details

- Device settings

- Ethernet ports

Following are the sections available in other part of the **STATUS** section:

- **DIAGNOSTIC TOOL**: To download diagnostics of the device.

- **Open services**: To show or hide services.

- **DEVICE LOGS**: To show or clear logs.

Configuring and Validating Smart Licensing

Overview of Smart Licensing Support

Smart licensing for the gateway running in URWB mode supports the following scenarios:

- Smart license management provides a seamless experience with the various aspects of licensing.

- Gateway controls the feature based on the license type:

    - Essentials

    - Advantage

    - Premier

- The platform can specify the number of license seats reserved. The system reports the higher value between the reserved license count and the actual licenses consumed. You can specify the number of purchased licenses for a deployment to avoid triggering a reporting event as the number fluctuates, provided that it remains equal to or less than the number of seats reserved.

- Smart transport mode connects to smart software manager (SSM) (formerly it was CSSM) directly to sync license usage.

- Airgap mode uses the downloaded file to sync with SSM manually.

- All radio devices in URWB mode (such as Catalysts IW9167E and IW9165) in the same URWB network require the same license level. This license level is set globally at the Mesh End or Global Mesh end. The license levels for gateways is configured independently on each gateway. It can be configured at a different level than the radio devices in the network.

Table 3: Smart license level for IEC6400 Gateway

License Type	Features
Essentials	• 5 Gbps fixed throughput • 5 Gbps gateway mobility throughput • 5 Gbps vehicle mobility throughput
Advantage	• 10 Gbps fixed throughput • 10 Gbps gateway mobility throughput • 10 Gbps vehicle mobility throughput
Premier	• 40 Gbps fixed throughput • 40 Gbps gateway mobility throughput • 40 Gbps vehicle mobility throughput

Note Industrial protocols support and Titan (High Availability) capabilities are always included in all the license tiers.

Configuring and Validating Smart Licensing Using CLI

To configure a smart license for the IEC6400 gateway, use the following CLI command:

Command or Action	Purpose
To configure a smart license	```Device# license iec-level [advantage
essentials	premier]
advantage   Network Advantage for Gateway
essentials Network Essentials for Gateway
premier   Network Premier for Gateway``` **Note** The IEC license must be configured on each IEC6400 gateway in the network.
To configure a smart license for Catalyst IW916x devices	```Device# license iw-level [advantage
essentials	premier]
advantage   Network Advantage for Radios
essentials Network Essentials for Radios
premier   Network Premier for Radios```
To configure the smart license Seats number for Catalyst IW916x devices	```Device# license iw-network platform [iw9165
iw9167] seats 6
iw9165 iw9165 Platform
iw9167 iw9167 Platform```

Command or Action	Purpose

To configure the smart license online deployment	`Device# license smart transport smart`
	`Device# license smart proxy address`
	`192.168.1.1 (Optional)`
	`Device# license smart proxy port 3128`
	`(Optional)`
	`Device# license smart trust idtoken`
	`<id_token_generate_from_SSM> local [force]`
	`  force      Force CSSM to generate new trust`
	` code`
	`Device# license smart usage interval 50`
	`(Optional)`

To configure smart license offline deployment	`Device# license smart transport off`
	`Device# license smart save usage all`
	`tftp://192.168.216.201/rum_report_all.xml`
	`Device# license smart import`
	`tftp://192.168.216.201/rum_report_ack.xml`

To configure the reset license configuration as default	`Device# license smart factory reset` **Note**　　Do not give CLI command as reload, it clears all the license configuration.

To validate smart license type	`Device# license show usage`
	`License Authorization:`
	`  Status: Not Applicable`
	
	`IEC6400_URWB_NW_E (IEC6400_URWB_NW_E):`
	`  Description: Cisco URWB Network Essentials`
	` for IEC6400 Edge Compute Platform`
	`  Count: 1`
	`  Version: 01`
	`  Status: IN USE`
	`  Export status: NOT RESTRICTED`
	`  Feature Name: IEC6400_URWB_NW_E`
	`  Feature Description: Cisco URWB Network`
	`Essentials for IEC6400 Edge Compute Platform`
	`  Enforcement type: NOT ENFORCED`
	`  License type: Perpetual`

To validate the smart license gateway number	`Device# license show iw seats`
	`    Platform   Configured      Current`
	`      IW9167          0               0`
	`      IW9165          0               0`

To validate the smart license usage count	`Device# license show summary`
	`Account Information:`
	`  Smart Account: <none>`
	`  Virtual Account: <none>`
	
	`License Usage:`
	`  License                  Entitlement Tag`
	`            Count Status`
	
	`_____`
	
	`  IEC6400_URWB_NW_E      (IEC6400_URWB_NW_E)`
	`                  1 IN USE`

Configuring Smart Licensing using GUI

Before you begin

To select the network license level for the URWB network, follow these steps:

Step 1 In the **ADVANCED SETTINGS**, click **smart license**.
The **SMART LICENSE** window appears.

Step 2 In the **Smart License Settings** section, configure the following parameters:

   a. Choose license level from the **License Level** drop-down list.

   b. Enter the platform iw9167 license seats value in the **Platform IW9167 License Seats** field.

   c. Enter the platform iw9165 license seats value in the **Platform IW9165 License Seats** field.

   Note   There are no seats defined for the IEC6400 license.

Step 3 Click **Save**.

Step 4 In the **IEC Smart License Settings** section, choose license level from the **License Level** drop-down list.

Step 5 Click **Save**.

Configuring Smart License Seats Management using CLI

To configure a smart license seat, use the following CLI command:

```
Device# license iw-network platform [ iw9165 | iw9167 ] seats
```

Example:

```
Device# license iw-network platform iw9165 seats 12
Device# license iw-network platform iw9167 seats 15
```

Configuring Running License Level using CLI

The license level, for Catalyst IW916x devices, is configured by the primary Mesh End (ME) or GGW gateway (based on network configuration) then the license level applied to all the gateways connected to the network.

To configure a license level for ME and GGW (license distributor), use the following CLI command:

```
Device# license iw-level [ advantage | essentials | premier ]
  advantage   Network Advantage for Radios
  essentials  Network Essentials for Radios
  premier     Network Premier for Radios
```

The license level for IEC6400 devices needs to be configured on each IEC device.

To configure a license level for an IEC device, use the following CLI command:

```
Device# license iec-level
advantage   Network Advantage for Gateway
  essentials  Network Essentials for Gateway
  premier     Network Premier for Gateway
```

Verifying License Smart License Seat using CLI

To verify the configured smart license seat, use the following CLI command:

```
Device# show license iw seats
Platform Configured Current
IW9167 0 15
IW9165 0 12
Device# write
Device# reboot
Device# license iw seats
Platform Configured Current
IW9167 0 15
IW9165 0 12
```

Configuring Running License Level for Gateway using CLI

To configure the license level for the gateway, use the following CLI command:

```
Device# license iec-level [ advantage | essentials | premier ]
advantage: Network Advantage for Radios
essentials: Network Essentials for Radios
premier: Network Premier for Radios
```

Shutting Down and Powering off the Gateway

The gateway can run in either of two power modes:

- Main power mode - Power is supplied to all server components and any operating system on your drives can run.

- Standby power mode - Power is supplied only to the service processor and certain components. It is safe for the operating system and data to remove power cords from the server in this mode.

⚠️

Caution After the IEC6400 gateway is shut down to standby power, electric current is still present in the IEC6400 gateway. To completely remove power as directed in some service procedures, you must disconnect all power cords from all power supplies in the server.

Shutting Down using the Power Button

Step 1   Check the color of the Power button/LED:

- Amber - The gateway is already in standby mode, and you can safely remove the power.

- Green - The gateway is in main power mode and must be shut down before you can safely remove the power.

Step 2   Initiate either a graceful shutdown or a hard shutdown:

Caution   To avoid data loss or damage to your operating system, you should always invoke a graceful shutdown of the operating system.

- Graceful shutdown - Press and release the **Power** button. The operating system performs a graceful shutdown, and the gateway goes to standby mode, which is indicated by an amber Power button/LED.

• Emergency shutdown - Press and hold the **Power** button for four seconds to force the main power off and immediately enter standby mode.

Shutting Down using the Cisco IMC GUI

Before you begin

You must log in with user or admin privileges to perform this task.

Step 1 In the Cisco IMC home page, click **Host Power** > **Power Off**.
A confirmation pop-up appears.

Step 2 Click **OK**.
The operating system performs a graceful shutdown, and the gateway goes to standby mode, which is indicated by an amber Power button/LED.

Shutting Down using Cisco IMC CLI

Before you begin

You must log in with user or admin privileges to perform this task.

Step 1 Click **Launch vKVM** in the Cisco IMC interface.
The **Launch vKVM** opens in a new window.

Step 2 At the server prompt, enter: `device# scope chassis`

Step 3 At the chassis prompt, enter: `device/chassis# power shutdown`

Step 4 (Optional) You can also directly shut down the gateway using the **Power off** option in **Launch vKVM**, click **Power** > **Power Off System**.
A confirmation warning appears.

Step 5 (Optional) Click **Confirm**.
The operating system performs a graceful shutdown, and the gateway goes to standby mode, which is indicated by an amber Power button/LED.