Cisco IEC6400 Edge Compute Appliance Installation and Configuration Guide, Release 1.2.0

First Published: 2025-12-19

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

PREFACE

CHAPTER 1

CHAPTER 2

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 vii
- Related Documentation, on page vii
- Communications, Services, and Additional Information, on page viii

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 1.1.0 introduces these new features:

- IW Monitor Management
- Layer 2 Mesh Transparency
- Multipath Operation
- URWB Telemetry Protocol

Related Documentation

- For more information about Cisco IEC6400 Release Notes, see the release notes documentation landing page Cisco IEC6400 Edge Compute Appliance.
- For more information about Cisco IEC6400 Installation and Configuration Guide, see the documentation landing page Cisco IEC6400 Edge Compute Appliance Installation and Configuration Guide.
- For more details about Regulatory Compliance and Safety Information, see Regulatory Compliance and Safety Information.
- For more details about UCS Firmware Upgrade Guide, see Cisco IEC6400 Edge Compute Appliance UCS Firmware Upgrade Guide.

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

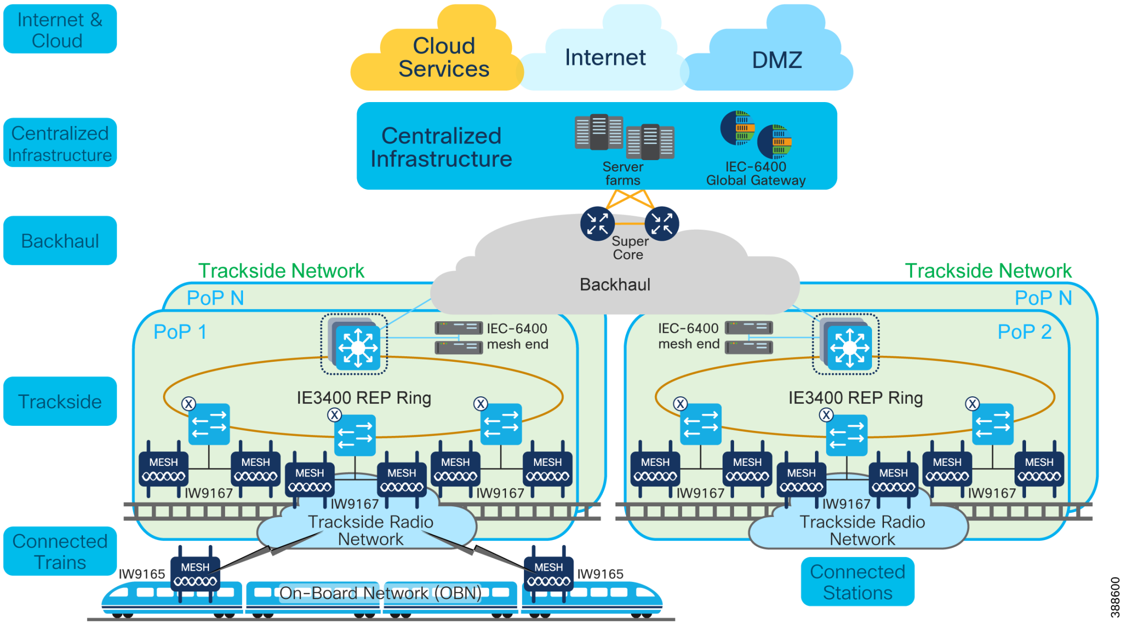
Note Each power supply in the server has a power cord. Standard power cords or jumper power cords are available for connection to the server. The shorter jumper power cords, for use in racks, are available as an optional alternative to the standard power cords.

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

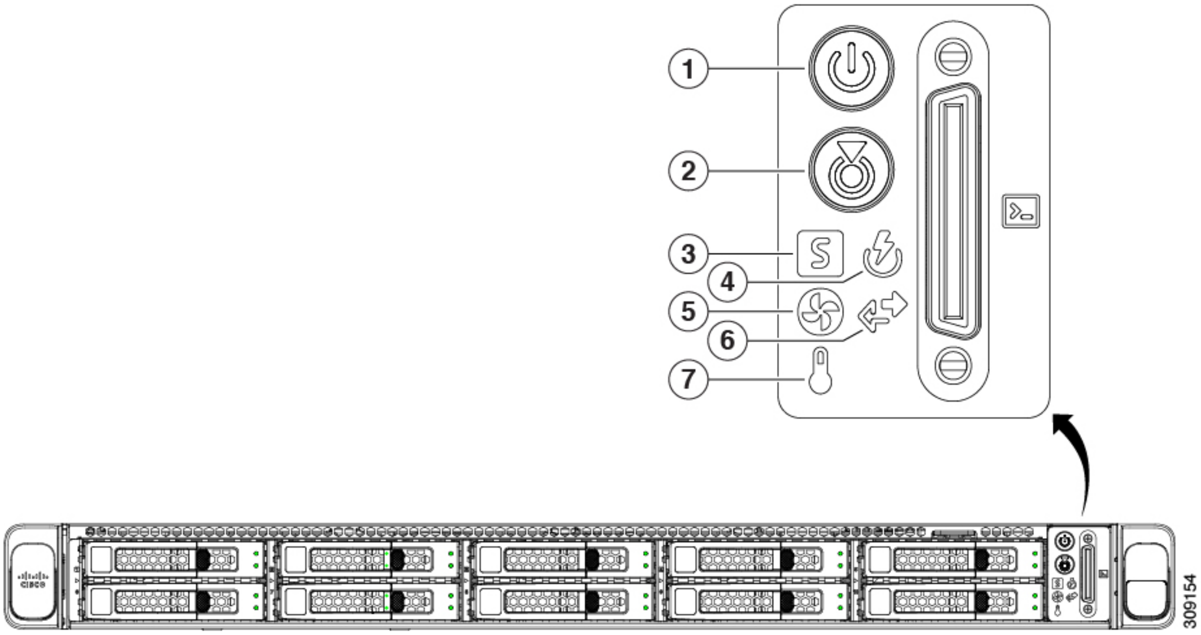
The gateway and all other edge gateways must be provided with a private LAN IP address, and they are accessed through the private IP addresses.

External Features

Front Panel Overview

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

Figure 2: Front Panel View

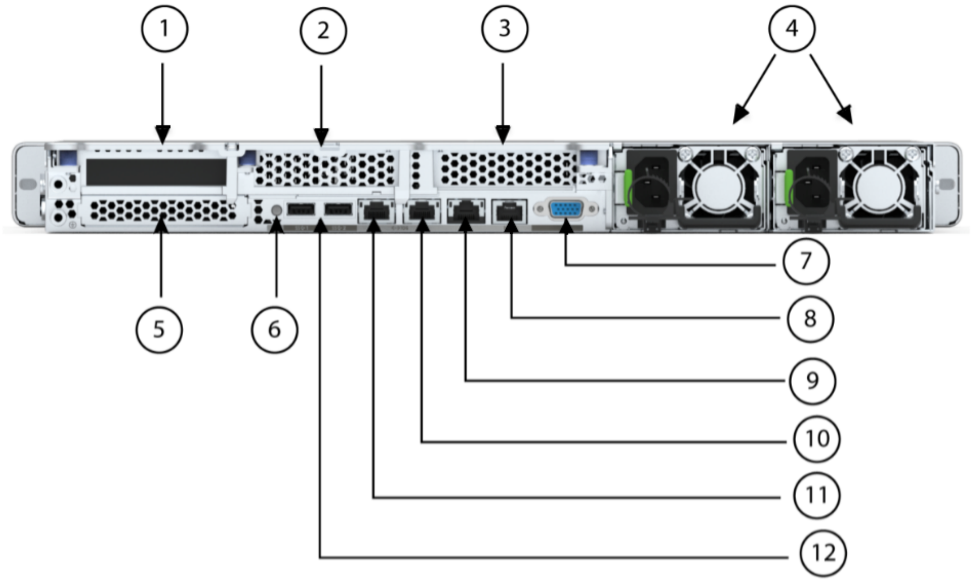


Identification Number in the Front Panel	LED/Button Details
(1)	Power button/LED
(2)	Unit identification
(3)	System health status
(4)	Power supply status
(5)	Fan status
(6)	Network link activity
(7)	Temperature status

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.

CHAPTER 2

Virtual Interface Card

Overview of virtual interface card

Cisco UCS Virtual Interface Card (VIC) 1455 is a Quad Port 10/25G SFP28 Converged Network Adapter (CNA) Peripheral Component Interconnect Express (PCIe) card that is designed for UCS C-Series M5 and M6 rack servers. From IEC6400 Release 1.1.0, use the Cisco Integrated Management Controller (CIMC) to configure the VIC 1455 adapter card.

VIC

A VIC is a physical hardware component in the UCS system. It is a type of network adapter that creates multiple Virtual Network Interface Card (vNICs) on a single physical card.

vNIC

In the UCS environment, you can create and manage vNICs, which are logical interfaces assigned to virtual machines or service profiles.

Specifications of Cisco UCS VIC

- Quad Port: The VIC 1455 has four ports, allowing multiple network connections.
- 10/25G SFP28: The VIC ports support both 10 and 25 Gigabit Ethernet speeds using SFP28 transceivers.
- CNA: The VIC handles both Ethernet and Fibre Channel over Ethernet (FCoE) traffic, combining network and storage traffic onto a single adapter.
- PCIe: The VIC uses a PCIe interface to connect to the server's motherboard, ensuring high-speed data transfer.

Verify VIC status using gateway's CLI

Use the **ethernet** command to view the VIC status in the gateway.

```
Device#ethernet
Ethernet port status:
eth0/0 UP Full-duplex 1000
eth0/1 DOWN
SFP+ port status:
sfp1/0 DOWN
sfp1/1 DOWN
sfp1/2 DOWN
sfp1/3 DOWN

link aggregation: backup
Ethernet interface MTU:  1530
```

If the **ethernet** command output does not show the **SFP+ port status** section, assume that the gateway either does not recognize the VIC or is not configured with the VIC. To configure vNIC, refer either Configure the vNIC using CIMC GUI or Configure the vNIC using CIMC CLI.

Configure the vNIC using the CIMC GUI

Follow this procedure if any of the following conditions apply:

- If the VIC is installed after the product delivery.
- If the URWB software does not recognize the card.

Note Repeat these two configuration procedures to configure the vNIC properties for eth1, eth2, and eth3.

Before you begin

Ensure the gateway is powered on.

Configure the adapter card general settings using GUI

Procedure

Step 1 Log into the CIMC web application using your credentials.

Step 2 On the home page, click ☰ at the top left to open the **Networking** menu.

Step 3 Click **Networking** > **Adapter Card 1**.
General tab appears.

Step 4 From the **General** tab, expand **Adapter Card Properties** to update these fields:

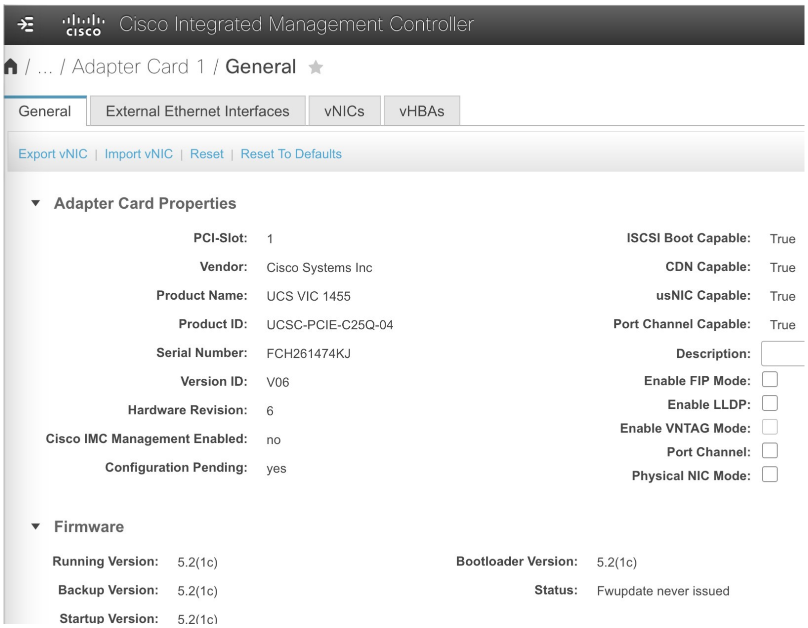
a) Uncheck the **Enable FIP Mode** check box.

b) Uncheck the **Enable LLDP** check box.

c) Uncheck the **Port Channel** check box.

Note

All other settings in **Adapter Card Properties** and **Firmware** section should be same as in the screenshot.



Cisco Integrated Management Controller
/ ... / Adapter Card 1 / General
General | External Ethernet Interfaces | vNICs | vHBAs
Export vNIC | Import vNIC | Reset | Reset To Defaults

Adapter Card Properties

PCI-Slot:	1	ISCSI Boot Capable:	True
Vendor:	Cisco Systems Inc	CDN Capable:	True
Product Name:	UCS VIC 1455	usNIC Capable:	True
Product ID:	UCSC-PCIE-C25Q-04	Port Channel Capable:	True
Serial Number:	FCH261474KJ	Description:	
Version ID:	V06	Enable FIP Mode:	☐
Hardware Revision:	6	Enable LLDP:	☐
Cisco IMC Management Enabled:	no	Enable VNTAG Mode:	☐
Configuration Pending:	yes	Port Channel:	☐
		Physical NIC Mode:	☐

Firmware

Running Version:	5.2(1c)	Bootloader Version:	5.2(1c)
Backup Version:	5.2(1c)	Status:	Fwupdate never issued
Startup Version:	5.2(1c)		

Step 5 Click **Save Changes**.

Configure the adapter card vNIC settings using GUI

Before you begin

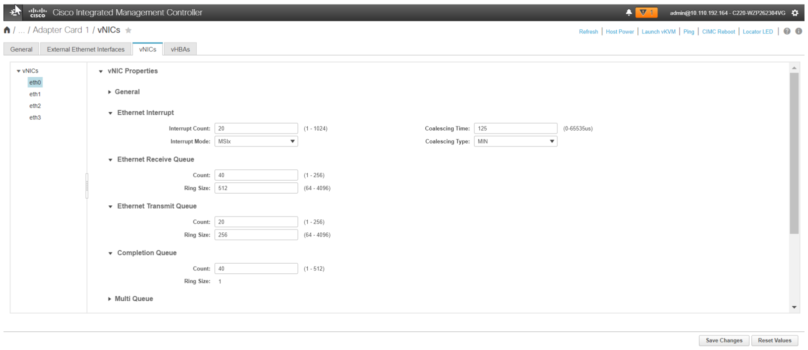
Perform steps 1 to 3 as mentioned in the Configure the adapter card general settings using GUI to reach the **Adapter Card 1** window and click **vNICs** tab.

Procedure

Step 1 In the **vNICs** section, click **Add vNIC** to create a new vNIC.

Note

You must create four vNIC interfaces and name them as eth0, eth1, eth2, and eth3. Ensure the vNIC settings should be same as shown in the screenshot.


Cisco Integrated Management Controller
admin@10.110.192.164 - C220-WZP262304VG
/ ... / Adapter Card 1 / vNICs
Refresh | Host Power | Launch vKVM | Ping | CIMC Reboot | Locator LED
General
External Ethernet Interfaces
vNICs
vHBAs
vNICs
eth0
eth1
eth2
eth3
Save Changes
Reset Values

vNIC Properties

General

Ethernet Interrupt

Interrupt Count: 20 (1 - 1024)

Interrupt Mode: MSIx

Coalescing Time: 125 (0-65535us)

Coalescing Type: MIN

Ethernet Receive Queue

Count: 40 (1 - 256)

Ring Size: 512 (64 - 4096)

Ethernet Transmit Queue

Count: 20 (1 - 256)

Ring Size: 256 (64 - 4096)

Completion Queue

Count: 40 (1 - 512)

Ring Size: 1

Multi Queue

Step 2 Expand **vNICs** drop-down list from left menu and click **eth0**.

Step 3 Expand **vNIC Properties** to display following sections:

- **General**
- **Ethernet Interrupt**
- **Ethernet Receive Queue**
- **Ethernet Transmit Queue**
- **Completion Queue**

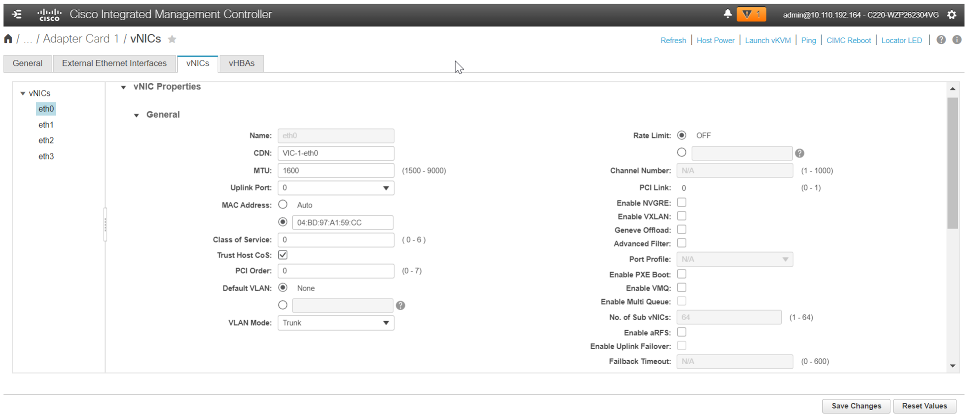
Step 4 Expand **General** to update these fields:

a) Enter 1600 in the **MTU** field.

b) Check the **Trust Host CoS** check box.

Note

- Set the MTU value to 1600. Using any other value may lead to unexpected results.
- All other settings in **General** section should be same as shown in the screenshot.


Cisco Integrated Management Controller
admin@10.110.192.164 - C220-WZP262304VG
/ ... / Adapter Card 1 / vNICs
Refresh | Host Power | Launch vKVM | Ping | CIMC Reboot | Locator LED
General
External Ethernet Interfaces
vNICs
vHBAs
vNICs
eth0
eth1
eth2
eth3
Save Changes
Reset Values

vNIC Properties

General

Name: eth0

CDN: VIC-1-eth0

MTU: 1600 (1500 - 9000)

Uplink Port: 0

MAC Address: ○ Auto
● 04:BD:97:A1:59:CC

Class of Service: 0 (0 - 6)

Trust Host CoS: ☑

PCI Order: 0 (0 - 7)

Default VLAN: ● None
○

VLAN Mode: Trunk

Rate Limit: ● OFF
○

Channel Number: N/A (1 - 1000)

PCI Link: 0 (0 - 1)

Enable NVGRE: □

Enable VXLAN: □

Geneve Offload: □

Advanced Filter: □

Port Profile: N/A

Enable PXE Boot: □

Enable VMQ: □

Enable Multi Queue: □

No. of Sub vNICs: 64 (1 - 64)

Enable aRFS: □

Enable Uplink Failover: □

Failback Timeout: N/A (0 - 600)

Step 5 Expand **Ethernet Interrupt** to update these fields:

a) Enter 20 in the **Interrupt Count** field.

b) Choose **MSIx** from the **Interrupt Mode** drop-down list.

Step 6 Expand **Ethernet Receive Queue** to update these fields:

a) Enter 40 in the **Count** field.

b) Enter 512 in the **Ring Size** field.

Step 7 Expand **Ethernet Transmit Queue** to update these fields:

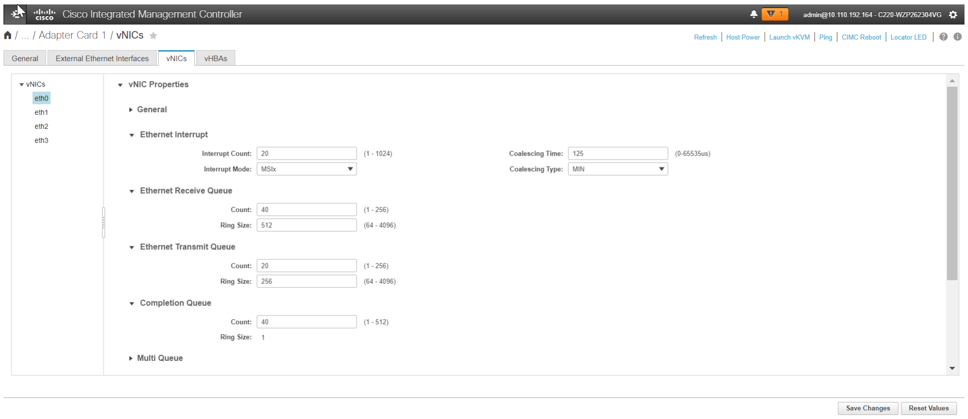
a) Enter 20 in the **Count** field.

b) Enter 256 in the **Ring Size** field.

Step 8 Expand **Completion Queue** to enter 40 in the **Count** field.

Note

All other settings in **Ethernet Interrupt, Ethernet Receive Queue**, **Ethernet Transmit Queue**, and **Completion Queue** sections should be same as shown in the screenshot.


Cisco Integrated Management Controller
admin@10.110.192.164 - C220-WZP262304VG
/ ... / Adapter Card 1 / vNICs
Refresh | Host Power | Launch vKVM | Ping | CIMC Reboot | Locator LED
General
External Ethernet Interfaces
vNICs
vHBAs
vNICs
eth0
eth1
eth2
eth3
vNIC Properties
General
Multi Queue
Save Changes
Reset Values

Ethernet Interrupt

Interrupt Count: 20 (1 - 1024)

Interrupt Mode: MSIx

Coalescing Time: 125 (0-65535us)

Coalescing Type: MIN

Ethernet Receive Queue

Count: 40 (1 - 256)

Ring Size: 512 (64 - 4096)

Ethernet Transmit Queue

Count: 20 (1 - 256)

Ring Size: 256 (64 - 4096)

Completion Queue

Count: 40 (1 - 512)

Ring Size: 1

Step 9 Click **Save Changes**.

Note

Repeat the configuration steps in the topic Configure the vNIC using the CIMC GUI to configure the vNIC properties for eth1, eth2, and eth3.

Step 10 Click **Host Power** > **Power Cycle** to reboot the gateway.

When gateway reboots, log into the CIMC through SSH using your credentials to check the VIC adapter status. For information on how to check VIC adapter status, see Verify VIC status using CIMC CLI.

Configure the vNIC using the CIMC CLI

Follow this procedure if any of the following conditions apply:

- If the VIC is installed after the product delivery.
- If the URWB software does not recognize the card.

Note Repeat these two CLI configuration procedures to configure the vNIC properties for eth1, eth2, and eth3.

Before you begin

Ensure the gateway is powered on.

Configure the adapter card general settings using CLI

Procedure

Step 1 Use the **scope chassis** command to enter the gateway.

```
Device# scope chassis
```

Step 2 Use the **scope adapter 1** command to enter the gateway's adapter.

```
Device /chassis# scope adapter 1
```

Step 3 Use the **set fip-mode disabled** command to disable FCoE initialization protocol (FIP) mode.

```
Device /chassis/adapter# set fip-mode disabled
```

Step 4 Use the **set lldp disabled** command to disable Link layer discovery protocol (LLDP) mode.

```
Device /chassis/adapter *# set lldp disabled
```

Step 5 Use the **set portchannel disabled** command to disable the port channel.

```
Device /chassis/adapter *# set portchannel disabled
```

Step 6 Use the **commit** command to update the changes.

```
Device /chassis/adapter *# commit
```

Configure the adapter card vNIC settings using CLI

If the gateway either does not recognize the VIC or is not configured with the VIC, update the following settings of vNIC Properties:

Procedure

Step 1 Configure the general settings using CLI

Step 2 Configure the ethernet receive queue settings using CLI

Step 3 Configure the ethernet transmit queue settings using CLI

Step 4 Configure the completion queue settings using CLI

Step 5 Configure the ethernet interrupt settings using CLI

Configure the general settings using CLI

Before you begin

Perform steps 1 and 2 of the Configure the adapter card general settings using CLI to reach the Adapter card 1 settings.

Procedure

Step 1 Use the **scope host-eth-if eth0** command to enter the eth0 mode.

```
Device /chassis/adapter *# scope host-eth-if eth0
```

Step 2 Use the **set mtu 1600** command to configure the MTU value as 1600.

```
Device /chassis/adapter/host-eth-if *# set mtu 1600
```

Step 3 Use the **set trust-host-cos enable** command to enable the Trust Host CoS.

```
Device /chassis/adapter/host-eth-if *# set trust-host-cos enable
```

Configure the ethernet receive queue settings using CLI

Before you begin

Perform steps 1 and 2 of the Configure the adapter card general settings using CLI to reach the Adapter card 1 settings.

Procedure

Step 1 Use the **scope recv-queue** command to enter the ethernet receive queue mode.

```
Device /chassis/adapter/host-eth-if *# scope recv-queue
```

Step 2 Use the **set rq-count 40** command to configure the ethernet receive queue count value as 40.

```
Device /chassis/adapter/host-eth-if/recv-queue *# set rq-count 40
```

Step 3 Use the **set rq-ring-size 512** command to configure the ethernet receive queue ring size as 512.

```
Device /chassis/adapter/host-eth-if/recv-queue *# set rq-ring-size 512
```

Step 4 Use the **exit** command to exit from the ethernet receive queue.

```
Device /chassis/adapter/host-eth-if/recv-queue *# exit
```

Configure the ethernet transmit queue settings using CLI

Before you begin

Perform steps 1 and 2 of the Configure the adapter card general settings using CLI to reach the Adapter card 1 settings.

Procedure

Step 1 Use the **scope trans-queue** command to enter the ethernet transmit queue mode.

```
Device /chassis/adapter/host-eth-if *# scope trans-queue
```

Step 2 Use the **set wq-count 20** command to configure the ethernet transmit queue count value as 20.

```
Device /chassis/adapter/host-eth-if/trans-queue *# set wq-count 20
```

Step 3 Use the **set wq-ring-size 256** command to configure the ethernet transmit queue ring size as 256.

```
Device /chassis/adapter/host-eth-if/trans-queue *# set wq-ring-size 256
```

Step 4 Use the **exit** command to exit from the ethernet transmit queue.

```
Device /chassis/adapter/host-eth-if/trans-queue *# exit
```

Configure the completion queue settings using CLI

Before you begin

Perform steps 1 and 2 of the Configure the adapter card general settings using CLI to reach the Adapter card 1 settings.

Procedure

Step 1 Use the **scope comp-queue** command to enter the completion queue mode.

```
Device /chassis/adapter/host-eth-if *# scope comp-queue
```

Step 2 Use the **set cq-count 40** command to configure the completion queue count value as 40.

```
Device /chassis/adapter/host-eth-if/comp-queue *# set cq-count 40
```

Step 3 Use the **exit** command to exit from the completion queue.

```
Device /chassis/adapter/host-eth-if/comp-queue *# exit
```

Configure the ethernet interrupt settings using CLI

Before you begin

Perform steps 1 and 2 of the Configure the adapter card general settings using CLI to reach the Adapter card 1 settings.

Procedure

Step 1 Use the **scope interrupt** command to enter the ethernet interrupt mode.

```
Device /chassis/adapter/host-eth-if # scope interrupt
```

Step 2 Use the **set interrupt-count 20** command to configure the ethernet interrupt count value as 20.

```
Device /chassis/adapter/host-eth-if/interrupt # set interrupt-count 20
```

Step 3 Use the **exit** command to exit from the ethernet interrupt mode.

```
Device /chassis/adapter/host-eth-if/interrupt *# exit
```

Step 4 Use the **exit** command to exit from the eth0 mode.

```
Device /chassis/adapter/host-eth-if *# exit
```

Note
Repeat the steps as mentioned in the Configure the vNIC using the CIMC CLI to modify the vNIC properties for eth1, eth2, and eth3.

Step 5 Use the **commit** command to reflect the updates.

```
Device /chassis/adapter *# commit
```

Step 6 Use the **exit** command to exit from the adapter properties.

```
Device /chassis/adapter # exit
```

Step 7 Use the **exit** command to exit from the gateway.

```
Device /chassis # exit
```

Step 8 Upon successful configuration, use the **power cycle** command to reboot the gateway.

```
Device /chassis # power cycle
```

CHAPTER 3

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 4

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 19, or
- Using CIMC GUI, see Configuring the Cisco Integrated Management Controller, on page 20

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.

Procedure

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:

Procedure

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.

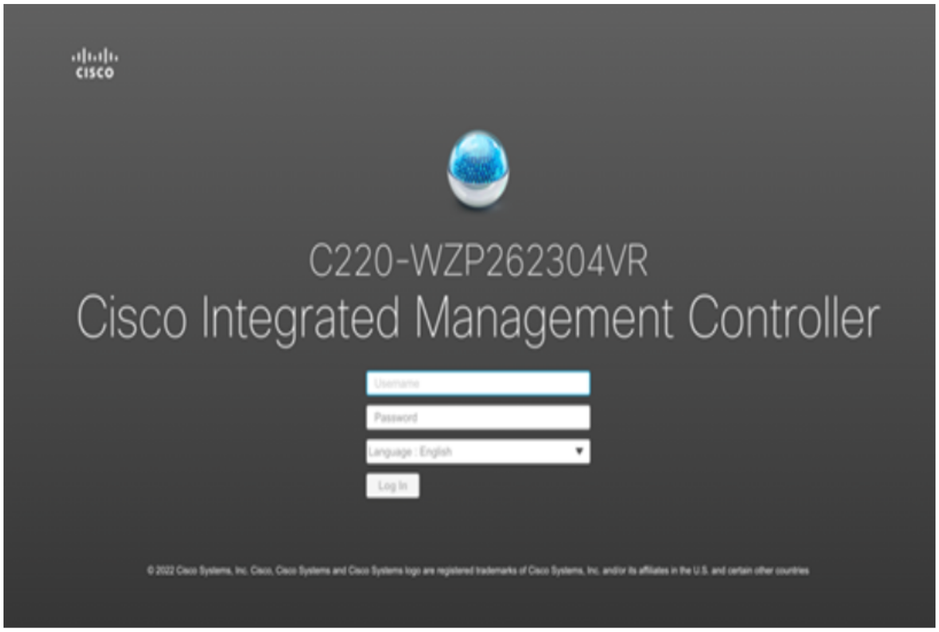
Step 3 Connect through the CIMC LAN management interface (port 9) to the network, which has a DHCP server, to obtain the IP address <a.b.c.d> of the device. Open the web browser and enter the following URL: https//:<A.B.C.D>/

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:

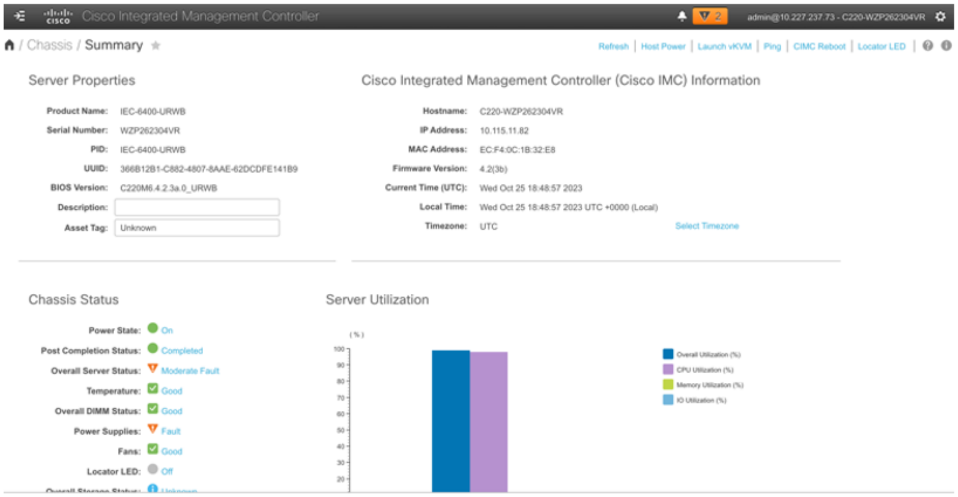
- The password must have minimum of 8 characters and a maximum of 14 characters.
- The password must not contain the user's name.
- The password must contain characters from three of the following four categories:
  - English uppercase letters (A through Z)
  - English lowercase letters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic character:
    - ! (Exclamation mark)
    - @ (At sign)
    - # (Hashtag)
    - $ (Dollar)
    - % (Percentage)
    - ^ (Circumflex)
    - & (Ampersand)
    - * (Asterisk)
    - - (Minus sign)
    - _ (Underscore)
    - = (Equal)
    - , (Comma)



C220-WZP262304VR

Cisco Integrated Management Controller

© 2022 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries



Cisco Integrated Management Controller
2
admin@10.227.237.73 - C220-WZP262304VR
Refresh | Host Power | Launch vKVM | Ping | CIMC Reboot | Locator LED

/ Chassis / Summary

Server Properties

Product Name: IEC-6400-URWB
Serial Number: WZP262304VR
PID: IEC-6400-URWB
UUID: 366B12B1-C882-4807-8AAE-62DCDFE141B9
BIOS Version: C220M6.4.2.3a.0_URWB
Description:
Asset Tag: Unknown

Cisco Integrated Management Controller (Cisco IMC) Information

Hostname: C220-WZP262304VR
IP Address: 10.115.11.82
MAC Address: EC:F4:0C:1B:32:E8
Firmware Version: 4.2(3b)
Current Time (UTC): Wed Oct 25 18:48:57 2023
Local Time: Wed Oct 25 18:48:57 2023 UTC +0000 (Local)
Timezone: UTC Select Timezone

Chassis Status

Power State: On
Post Completion Status: Completed
Overall Server Status: Moderate Fault
Temperature: Good
Overall DIMM Status: Good
Power Supplies: Fault
Fans: Good
Locator LED: Off
Overall Storage Status: Unknown

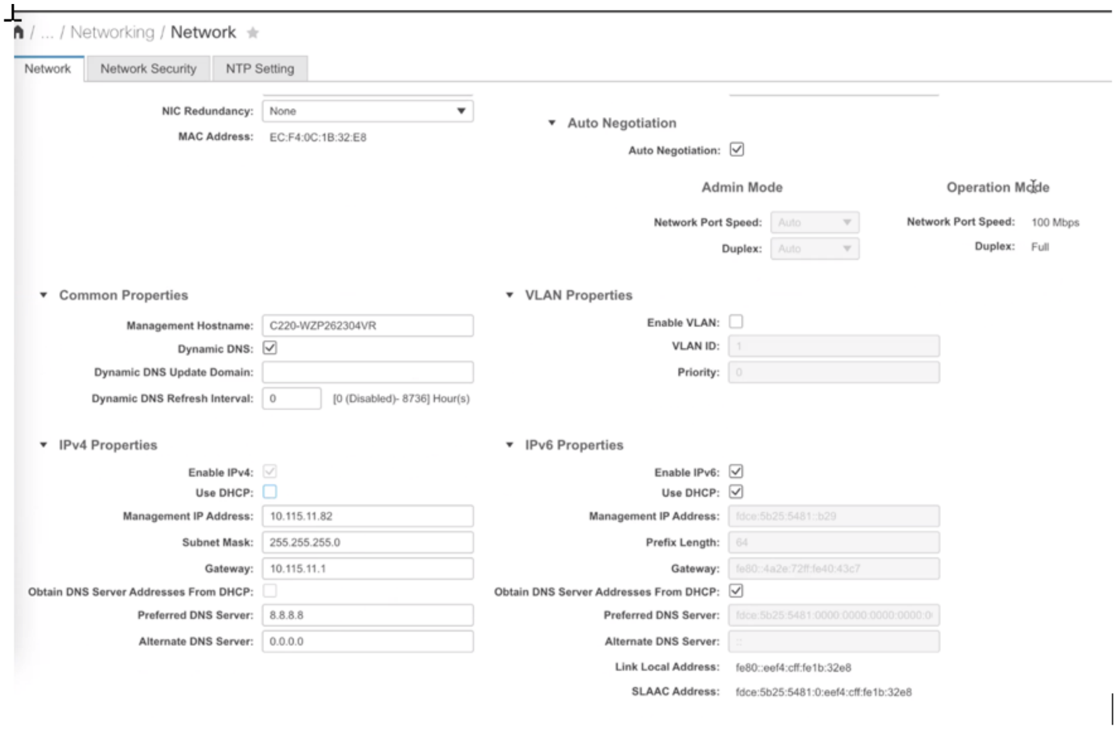
Server Utilization

Step 5 Click ⇶ at the left corner.

A left pane appears.

Step 6 Go to **Admin** > **Networking**.

A new **Network** page appears.



NIC Redundancy: None
MAC Address: EC:F4:0C:1B:32:E8

Auto Negotiation

Auto Negotiation: ☑

Admin Mode

Network Port Speed: Auto
Duplex: Auto

Operation Mode

Network Port Speed: 100 Mbps
Duplex: Full

Common Properties

Management Hostname: C220-WZP262304VR
Dynamic DNS: ☑
Dynamic DNS Update Domain:
Dynamic DNS Refresh Interval: 0 [0 (Disabled)- 8736] Hour(s)

VLAN Properties

Enable VLAN: □
VLAN ID: 1
Priority: 0

IPv4 Properties

Enable IPv4: ☑
Use DHCP: □
Management IP Address: 10.115.11.82
Subnet Mask: 255.255.255.0
Gateway: 10.115.11.1
Obtain DNS Server Addresses From DHCP: □
Preferred DNS Server: 8.8.8.8
Alternate DNS Server: 0.0.0.0

IPv6 Properties

Enable IPv6: ☑
Use DHCP: ☑
Management IP Address: fdce:5b25:5481::b29
Prefix Length: 64
Gateway: fe80::4a2e:72ff:fe40:43c7
Obtain DNS Server Addresses From DHCP: ☑
Preferred DNS Server: fdce:5b25:5481:0000:0000:0000:0000:0
Alternate DNS Server: ::
Link Local Address: fe80::eef4:cff:fe1b:32e8
SLAAC Address: fdce:5b25:5481:0:eef4:cff:fe1b:32e8

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:

Procedure

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.

CHAPTER 5

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 26
- Using CIMC CLI, see Accessing Gateway's CLI from CIMC CLI, on page 25

Accessing Gateway's CLI from CIMC CLI

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

Procedure

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 29.

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.

Procedure

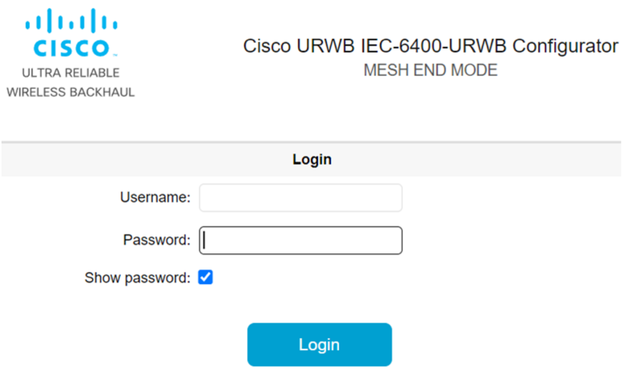
Step 1 Power on the gateway and wait for atleast five minutes to allow the boot sequence to finish.

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.



Cisco URWB IEC-6400-URWB Configurator
MESH END MODE

Show password: ☑

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

- Configuring new login credentials using GUI
- Configuring new login credentials using CLI

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:

Procedure

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.

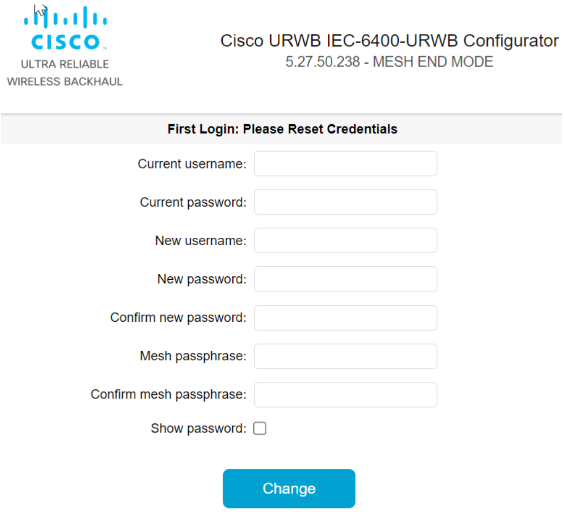
Step 4 Enter the new password in the **New password** field. For rules on creating the new login credentials, see Rules to Reset the Login Credentials.

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**.



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

First Login: Please Reset Credentials

Current username:

Current password:

New username:

New password:

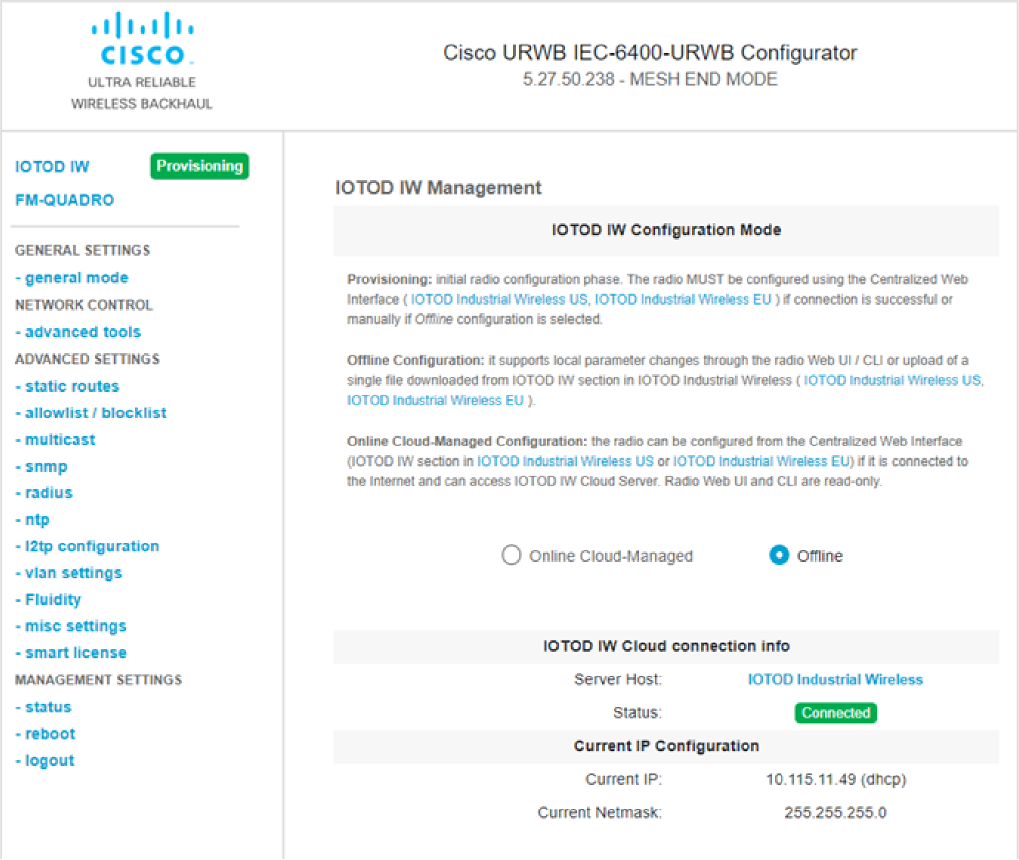
Confirm new password:

Mesh passphrase:

Confirm mesh passphrase:

Show password: □

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



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

IOTOD IW Management

IOTOD IW Configuration Mode

Provisioning: initial radio configuration phase. The radio MUST be configured using the Centralized Web Interface (IOTOD Industrial Wireless US, IOTOD Industrial Wireless EU) if connection is successful or manually if *Offline* configuration is selected.

Offline Configuration: it supports local parameter changes through the radio Web UI / CLI or upload of a single file downloaded from IOTOD IW section in IOTOD Industrial Wireless (IOTOD Industrial Wireless US, IOTOD Industrial Wireless EU).

Online Cloud-Managed Configuration: the radio can be configured from the Centralized Web Interface (IOTOD IW section in IOTOD Industrial Wireless US or IOTOD Industrial Wireless EU) if it is connected to the Internet and can access IOTOD IW Cloud Server. Radio Web UI and CLI are read-only.

○ Online Cloud-Managed ● Offline

IOTOD IW Cloud connection info

Server Host:	IOTOD Industrial Wireless
Status:	Connected

Current IP Configuration

Current IP:	10.115.11.49 (dhcp)
Current Netmask:	255.255.255.0

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 26
- Through CIMC CLI, see Accessing Gateway's CLI from CIMC CLI, on page 25

To know the default IP address for SSH connection, see Configuring the Gateway Initially in Provisioning Mode, on page 32.

Procedure

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 this criteria:

- The username length must be between 3 to 32 characters long.
- The password length must be between 8 to 32 characters long.
- 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

CHAPTER 6

Configuring the Gateway Initially in Provisioning Mode

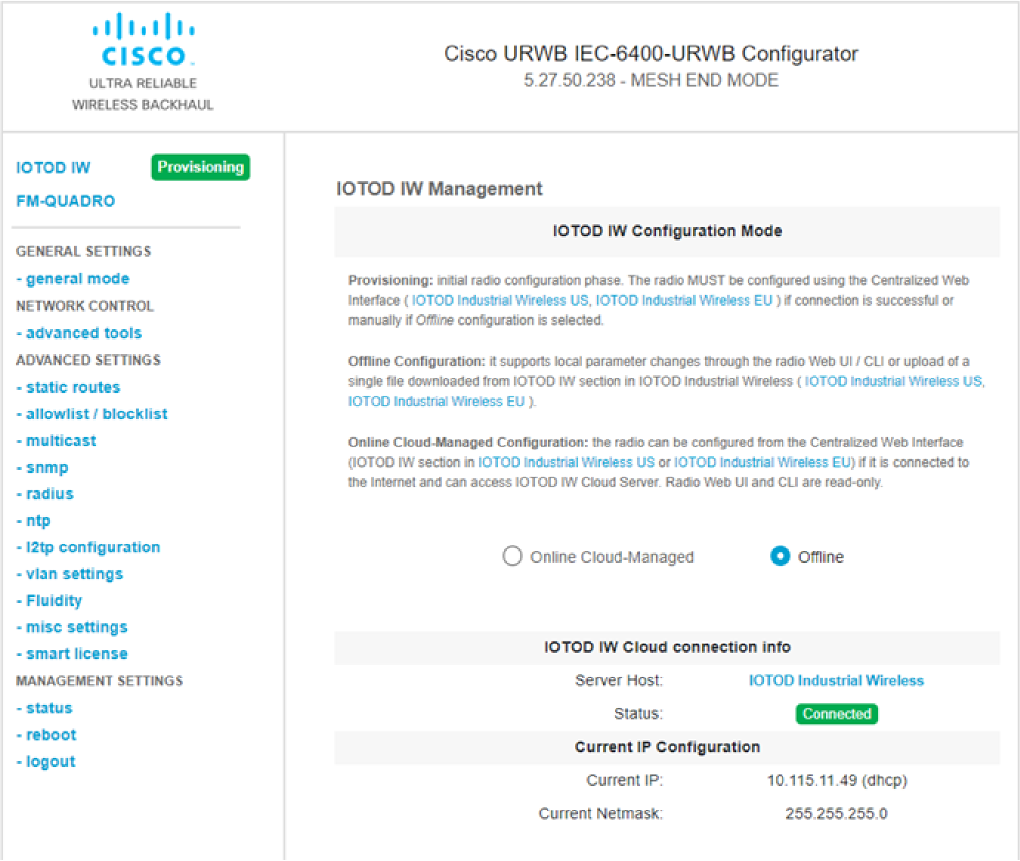
You can use IoT OD IW for online cloud configuration or alternatively you can switch to offline mode for configuring the gateway manually using the CLI or web UI.

Switching Between Offline and Online modes

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

Procedure

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



ULTRA RELIABLE WIRELESS BACKHAUL

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

IOTOD IW Provisioning
FM-QUADRO

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
- status
- reboot
- logout

IOTOD IW Management

IOTOD IW Configuration Mode

Provisioning: initial radio configuration phase. The radio MUST be configured using the Centralized Web Interface (IOTOD Industrial Wireless US, IOTOD Industrial Wireless EU) if connection is successful or manually if *Offline* configuration is selected.

Offline Configuration: it supports local parameter changes through the radio Web UI / CLI or upload of a single file downloaded from IOTOD IW section in IOTOD Industrial Wireless (IOTOD Industrial Wireless US, IOTOD Industrial Wireless EU).

Online Cloud-Managed Configuration: the radio can be configured from the Centralized Web Interface (IOTOD IW section in IOTOD Industrial Wireless US or IOTOD Industrial Wireless EU) if it is connected to the Internet and can access IOTOD IW Cloud Server. Radio Web UI and CLI are read-only.

○ Online Cloud-Managed ● Offline

IOTOD IW Cloud connection info

Server Host:	IOTOD Industrial Wireless
Status:	Connected

Current IP Configuration

Current IP:	10.115.11.49 (dhcp)
Current Netmask:	255.255.255.0

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.

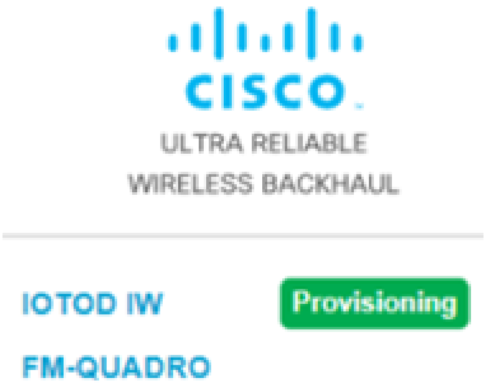
Note When the gateway is in provisioning mode, the gateway attempts to get an IP address from a DHCP server. If the gateway fails to receive an IP address using DHCP, the gateway reverts to a fallback IP address of 192.168.0.10/24. For easier accessibility, the gateway is also assigned an additional 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 IEC-6400-URWB 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 35
If the gateway is not able to connect to the network.	Gateway Fails to Connect to the Network, on page 36

Gateway in Provisioning Mode

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



CISCO

ULTRA RELIABLE
WIRELESS BACKHAUL

IOTOD IW Provisioning

FM-QUADRO

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.
- 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:

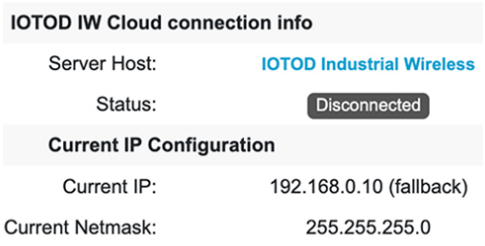
```
Device# iotod-iw show status

IOTOD IW mode: Provisioning

Status: Connected
```

Gateway in Disconnected Mode

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



IOTOD IW Cloud connection info

Server Host: IOTOD Industrial Wireless

Status: Disconnected

Current IP Configuration

Current IP: 192.168.0.10 (fallback)

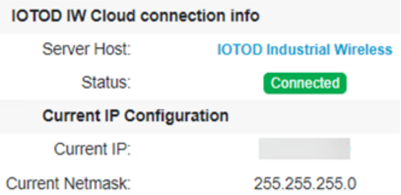
Current Netmask: 255.255.255.0

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: [redacted]

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:

Procedure

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:

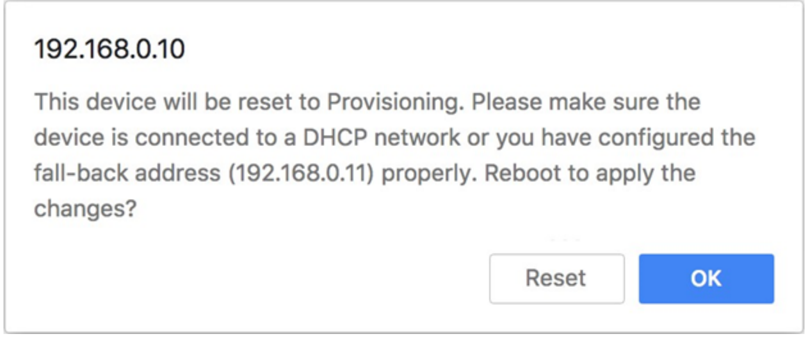
Procedure

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.

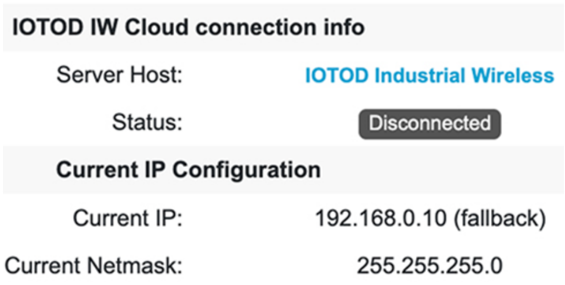


192.168.0.10

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?

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.

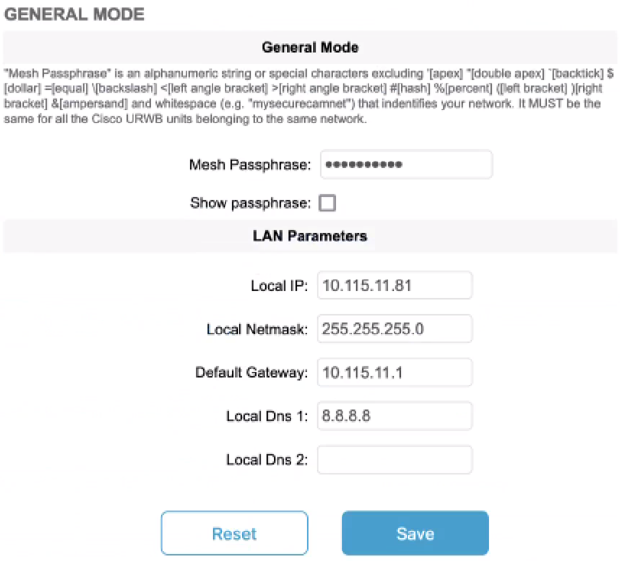
The general mode window contains controls on how to monitor and/or change the following settings:

- Shared network passphrase
- Gateway's LAN parameters

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

Procedure

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:

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:

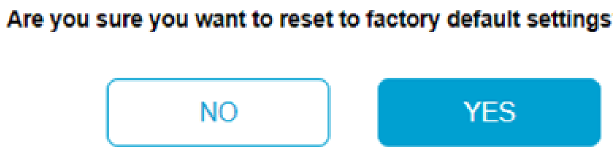
```
ip addr 192.168.10.2 netmask 255.255.255.0 gateway 192.168.10.1 dns1
192.168.10.200 dns2 192.168.10.201
```

Resetting the Gateway to Factory Default using GUI

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

Procedure

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?

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.

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.

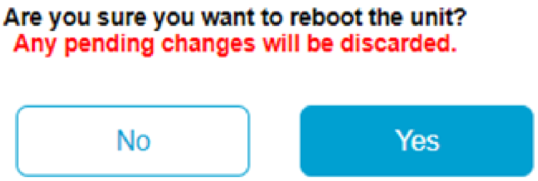
Rebooting the Gateway using GUI

Before you begin

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

Procedure

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.

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.

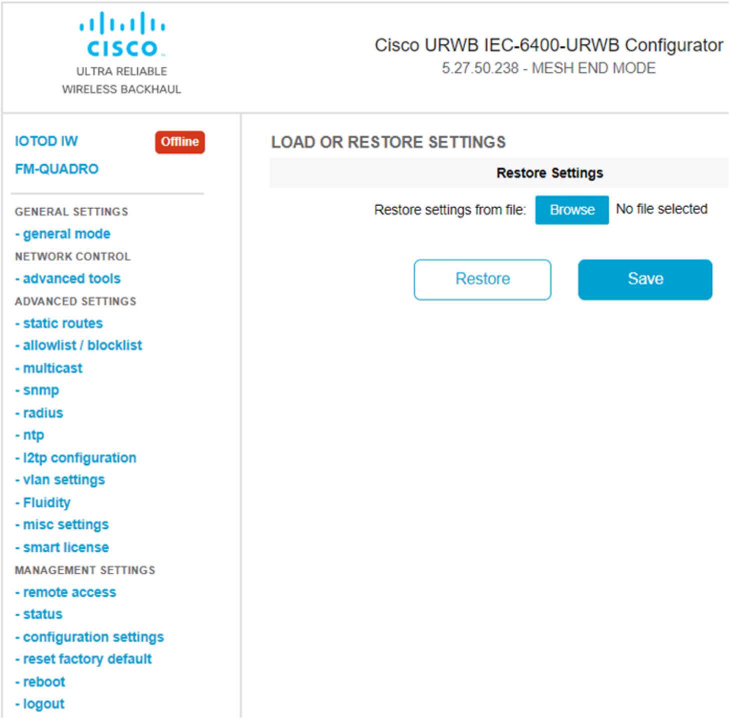
Downloading the Gateway's Current Configuration Settings

Before you begin

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

Procedure

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.

Procedure

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.

CHAPTER 7

Recommended Settings for Interoperability with Catalyst APs in URWB Mode

Restrictions on deploying IEC6400 as Coordinator (Mesh End)

When deploying the IEC6400 as Coordinator or as Mesh end node, ensure these requirements are met:

- IEC6400 must be deployed only in Layer-2 mobility systems (without a Global Gateway). Legacy URWB Layer-3 architectures that rely on multi-subnet routing and L2TP tunneling are not supported.
- IEC6400 must be monitored using the FMQuadro interface when it is used as the mesh coordinator.
- When the IEC6400 operates as the mesh Coordinator, the network topology is not displayed on the controller WebUI and must be monitored through the FMQuadro interface on the IEC6400 unit.
- If the URWB network includes both Catalyst access points operating as fixed infrastructure and mobility nodes, disable the MPLS reduce-broadcast feature. Disabling this feature prevents association issues for access points that cannot join the controller.

VLAN configuration for Catalyst APs in URWB mode

This section explains how to configure VLANs so that Catalyst APs in URWB mode can communicate with the IEC6400 controller.

It includes:

- **Untagged VLAN setup**: configuration steps for the IEC6400, connected Catalyst APs in URWB mode, and switch ports when CAPWAP VLAN Tag feature is not configured on the APs.
- **Tagged VLAN setup**: configuration requirements for deployments using CAPWAP VLAN Tag feature on the APs, including the list of allowed VLANs for both the IEC6400 and Catalyst APs in URWB mode.

Make sure wired clients use a VLAN that is different from the controller's VLAN. Update your configurations to maintain network segmentation and connectivity. For configuration instructions, see Add a VLAN for Wired Clients.

Untagged VLAN setup

Use this configuration when the Catalyst APs in URWB mode do not use CAPWAP VLAN tags. In this scenario, traffic between the controller and the APs uses the native VLAN.

Before you begin

To enable communication between Catalyst APs that operate in URWB mode and the IEC6400, enable VLAN functionality on the IEC6400 using the **vlan status enabled** command.

Procedure

Step 1 Set the management and native VLAN IDs to 1.

a) Use the **vlan mgm-vid** *management-id* to set the management ID.

Example:

```
Device# vlan mgm-vid 1
```

b) Use the **vlan native-vid** *native-vlan-id* to set the VLAN ID.

Example:

```
Device# vlan native-vid 1
```

Step 2 Configure the switch port connected to the IEC6400 to use the controller VLAN as the native VLAN.

Note
The examples given in this section assume that the IEC6400 is connected to the switch port Te1/0/5 and that the controller is on VLAN 87.

a) Use the **interface TenGigabitEthernet** *interface* command on the switch CLI to enter interface configuration mode by specifying the slot and port number of the interface.

Example:

```
Device# interface TenGigabitEthernet 1/0/5
```

b) Use the **switchport trunk native vlan** *vlan* command to configure the native VLAN on a trunk port. This specifies which VLAN will be treated as the default (untagged) VLAN on the trunk.

Example:

```
Device# switchport trunk native vlan 87
```

c) Use the **switchport trunk allowed vlan** *vlan* command to specify which VLANs are allowed to pass through a trunk port. This controls which VLAN traffic can traverse the trunk.

Example:

```
Device# switchport trunk allowed vlan 87
```

d) Use the **switchport mode trunk** command to configure a switch port to operate as a trunk. A trunk port can carry traffic for multiple VLANs between network devices.

Example:

```
Device# switchport mode trunk
```

Step 3 Configure the switch port connected to the local Catalyst AP in URWB mode.

Note
The examples given in this section assume that the Catalyst AP is connected to port Te1/0/9 of the backbone switch.

a) Use the **interface TenGigabitEthernet** *interface* command to enter interface configuration mode by specifying the slot and port number of the interface.

Example:

```
Device# interface TenGigabitEthernet1/0/9
```

b) Use the **switchport trunk native vlan** *vlan* command to configure the native VLAN on a trunk port. This specifies which VLAN will be treated as the default (untagged) VLAN on the trunk.

Example:

```
Device# switchport trunk native vlan 87
```

c) Use the **switchport trunk allowed vlan** *vlan* command to specify which VLANs are allowed to pass through a trunk port. This controls which VLAN traffic can traverse the trunk.

Example:

```
Device# switchport trunk allowed vlan 87
```

d) Use the **switchport mode trunk** command to configure a switch port to operate as a trunk. A trunk port can carry traffic for multiple VLANs between network devices.

Example:

```
Device# switchport mode trunk
```

e) Use the **spanning-tree portfast** command to enable PortFast on a switch port.

Example:

```
Device# spanning-tree portfast
```

Tagged VLAN setup

Use this configuration when the Catalyst APs in URWB mode use a specific CAPWAP VLAN tag, such as VLAN 87, to communicate with the controller.

Before you begin

To enable communication between Catalyst APs that operate in URWB mode and the IEC6400, enable VLAN functionality on the IEC6400 using the **vlan status enabled** command.

Procedure

Step 1 Set the management VLAN ID to the Controller's VLAN and native VLAN ID to 1.

Note
The examples given in this section assume that the controller is on VLAN 87.

a) Use the **vlan mgm-vid** *management-id* command to set the management VLAN ID so that it matches the controller's VLAN.

Example:

```
Device# vlan mgm-vid 87
```

b) Use the **vlan native-vid** *native-vlan-id* to specify the native VLAN ID.

Example:

```
Device# vlan native-vid 1
```

Step 2 Configure the switch port connected to the IEC6400 to allow the controller VLAN.

Note
The examples given in this section assume that the IEC6400 is connected to the switch port Te1/0/5.

a) Use the **interface TenGigabitEthernet** *interface* command to enter interface configuration mode by specifying the slot and port number of the interface.

Example:

```
Device# interface TenGigabitEthernet 1/0/5
```

b) Use the **switchport trunk native vlan** *vlan* command to configure the native VLAN on a trunk port.

Example:

```
Device# switchport trunk native vlan 87
```

c) Use the **switchport mode trunk** command to configure a switch port to operate as a trunk. A trunk port can carry traffic for multiple VLANs between network devices.

Example:

```
Device# switchport mode trunk
```

Step 3 Configure the switch port connected to the local Catalyst AP.

Note
The examples given in this section assume that the Catalyst AP is connected to port Te1/0/9 of the backbone switch.

a) Use the **interface TenGigabitEthernet** *interface* command to enter interface configuration mode by specifying the slot and port number of the interface.

Example:

```
Device# interface TenGigabitEthernet1/0/9
```

b) Use the **switchport trunk native vlan** *vlan* command to configure the native VLAN on a trunk port. This specifies which VLAN will be treated as the default (untagged) VLAN on the trunk.

Example:

```
Device# switchport trunk native vlan 87
```

c) Use the **switchport mode trunk** command to configure a switch port to operate as a trunk. A trunk port can carry traffic for multiple VLANs between network devices.

Example:

```
Device# switchport mode trunk
```

d) Use the **spanning-tree portfast** command to enable PortFast on a switch port.

Example:

```
Device# spanning-tree portfast
```

Add a VLAN for Wired Clients

Wired clients must be on a VLAN different from the controller. To support wired clients on a separate VLAN (for example, VLAN 90), update the switch port configurations to allow the new VLAN.

Procedure

Step 1 Update the switch port connected to the IEC6400 to allow the client VLAN.

a) Use the **interface TenGigabitEthernet** *interface* command to enter interface configuration mode by specifying the slot and port number of the interface.

Example:

```
Device# interface TenGigabitEthernet1/0/5
```

b) Use the **switchport trunk native vlan** *vlan* command to configure the native VLAN on a trunk port. The native VLAN is treated as the default (untagged) VLAN on the trunk.

Example:

```
Device# switchport trunk native vlan 87,90
```

c) Use the **switchport mode trunk** command to configure a switch port to operate as a trunk. A trunk port carries traffic for multiple VLANs between network devices.

Example:

```
Device# switchport mode trunk
```

Step 2 Update the switch port connected to the local Catalyst AP to allow the client VLAN.

a) Use the **interface TenGigabitEthernet** *interface* command to enter interface configuration mode by specifying the slot and port number of the interface.

Example:

```
Device# interface TenGigabitEthernet1/0/9
```

b) Use the **switchport trunk native vlan** *vlan* command to configure the native VLAN on a trunk port. This specifies which VLAN will be treated as the default (untagged) VLAN on the trunk.

Example:

```
Device# switchport trunk native vlan 87,90
```

c) Use the **switchport mode trunk** command to configure a switch port to operate as a trunk. A trunk port can carry traffic for multiple VLANs between network devices.

Example:

```
Device# switchport mode trunk
```

d) Use the **spanning-tree portfast** command to enable PortFast on a switch port.

Example:

```
Device# spanning-tree portfast
```

CHAPTER 8

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`

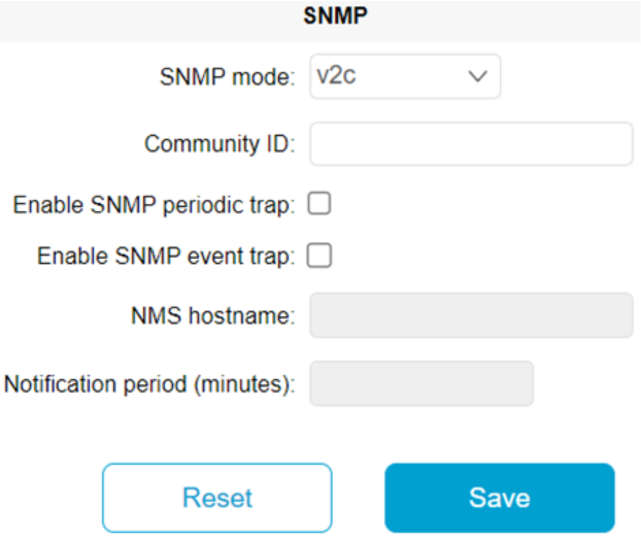
Configuring SNMP Version v2c using GUI

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:

Procedure

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



SNMP

SNMP mode: v2c

Community ID:

Enable SNMP periodic trap: □

Enable SNMP event trap: □

NMS hostname:

Notification period (minutes):

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**.

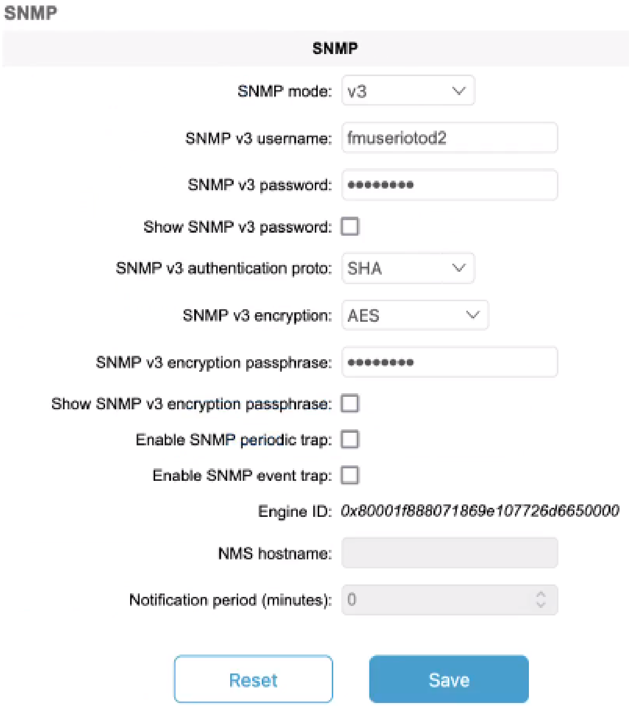
Configuring SNMP Version v3 using GUI

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:

Procedure

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



SNMP

SNMP

SNMP mode: v3

SNMP v3 username: fmuseriotod2

SNMP v3 password: ●●●●●●●●●

Show SNMP v3 password: □

SNMP v3 authentication proto: SHA

SNMP v3 encryption: AES

SNMP v3 encryption passphrase: ●●●●●●●●●

Show SNMP v3 encryption passphrase: □

Enable SNMP periodic trap: □

Enable SNMP event trap: □

Engine ID: *0x80001f8880718 69e107726d6650000*

NMS hostname:

Notification period (minutes): 0

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

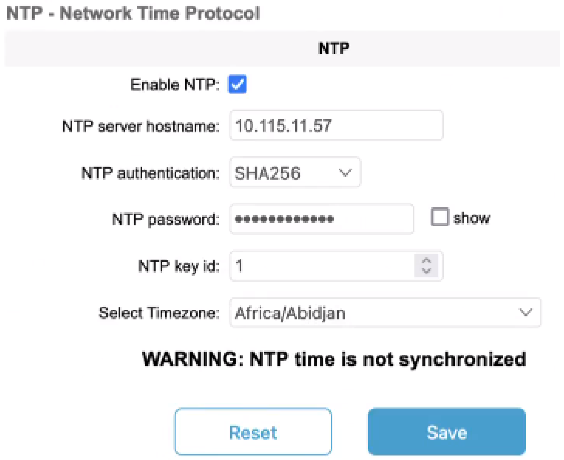
The gateway has NTP functionality that allows it to synchronize the time settings with a chosen network time server.

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:

Procedure

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



NTP - Network Time Protocol

NTP

Enable NTP: ☑

NTP server hostname: 10.115.11.57

NTP authentication: SHA256

NTP password: ●●●●●●●●●●●●● □ show

NTP key id: 1

Select Timezone: Africa/Abidjan

WARNING: NTP time is not synchronized

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
```

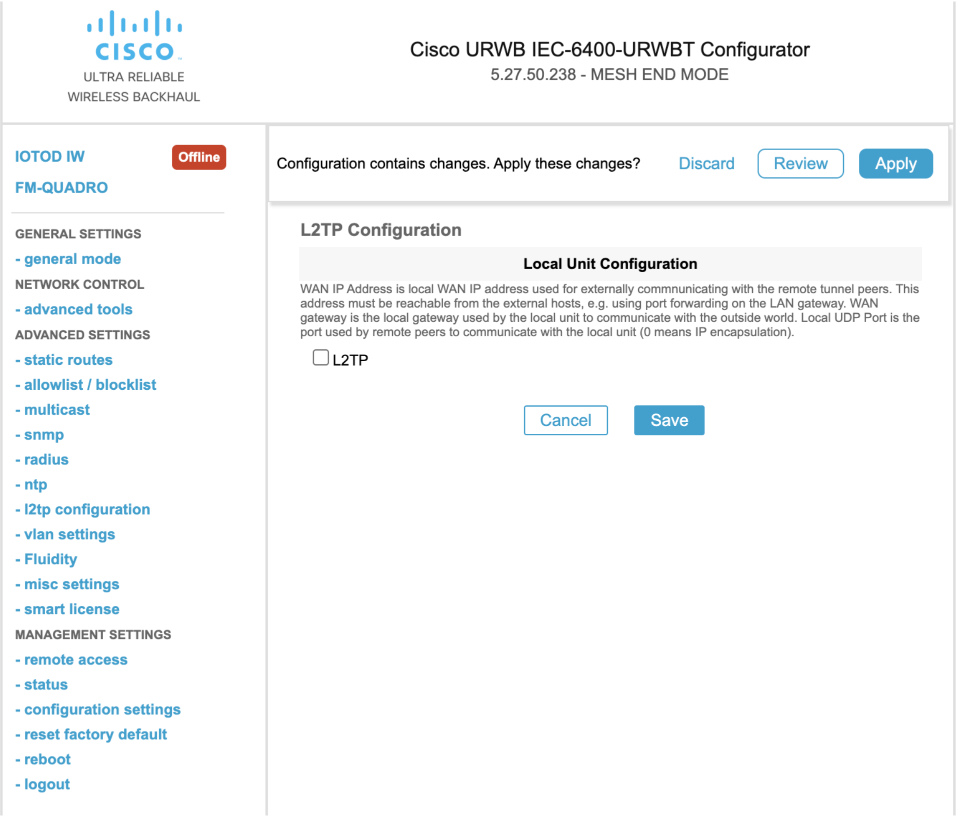
Configuring L2TP using GUI

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:

Procedure

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

The **L2TP Configuration** window appears.



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

Configuration contains changes. Apply these changes?

L2TP Configuration

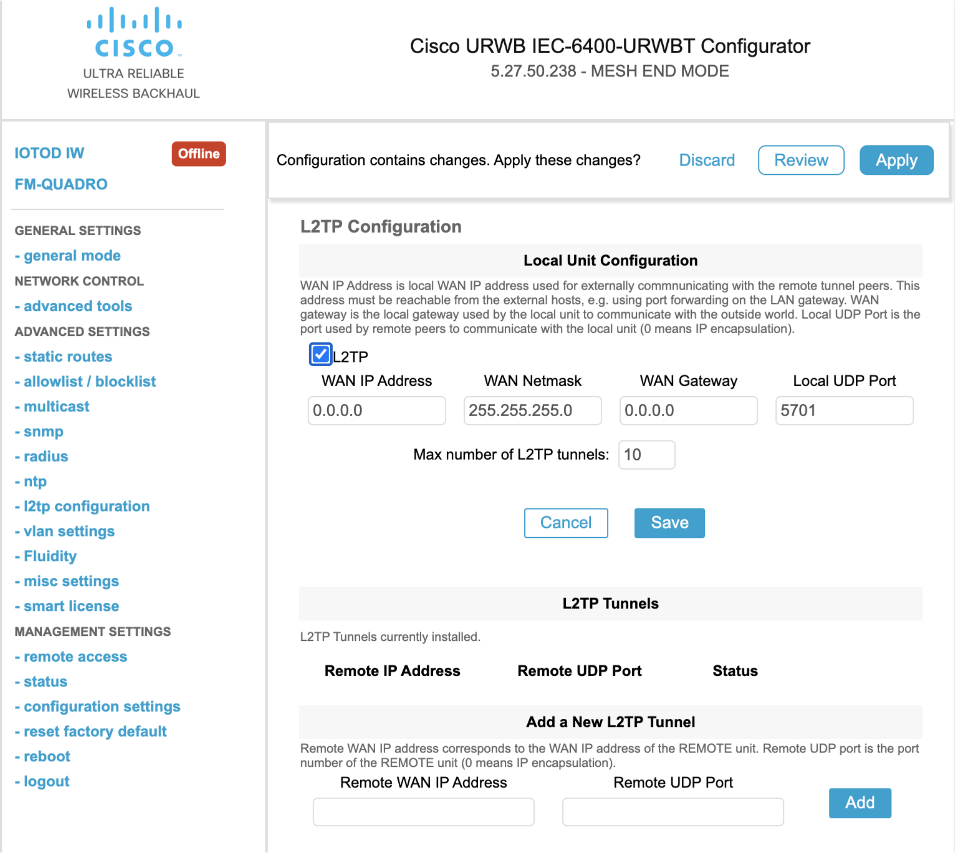
Local Unit Configuration

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

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

The L2TP detailed configuration settings appears.



Cisco URWB IEC-6400-URWBT Configurator

5.27.50.238 - MESH END MODE

Configuration contains changes. Apply these changes?

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

WAN IP Address	WAN Netmask	WAN Gateway	Local UDP Port
0.0.0.0	255.255.255.0	0.0.0.0	5701

Max number of L2TP tunnels: 10

L2TP Tunnels

L2TP Tunnels currently installed.

Remote IP Address	Remote UDP Port	Status

Add a New L2TP Tunnel

Remote WAN IP address corresponds to the WAN IP address of the REMOTE unit. Remote UDP port is the port number of the REMOTE unit (0 means IP encapsulation).

Remote WAN IP Address

Remote UDP Port

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:

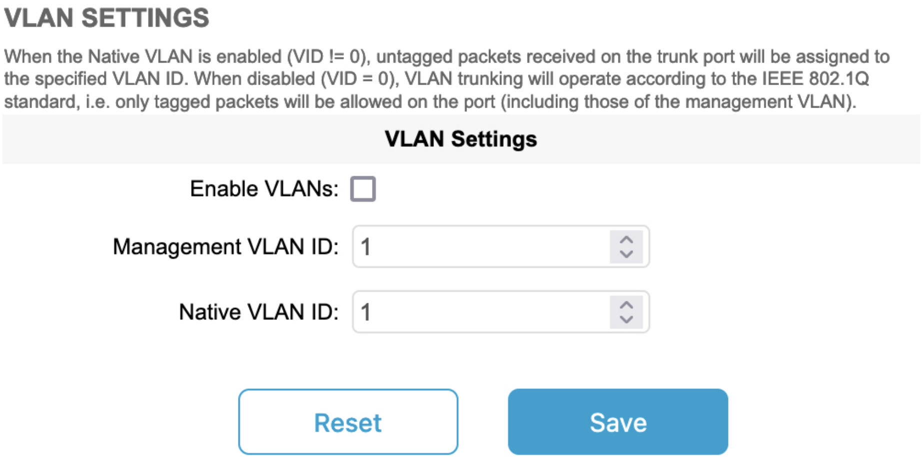
Parameter	Default value
Management VLAN ID (MVID)	1
Native VLAN ID (NVID)	1

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

Procedure

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

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

Access port rules management for outgoing packets with a gateway in smart mode	
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

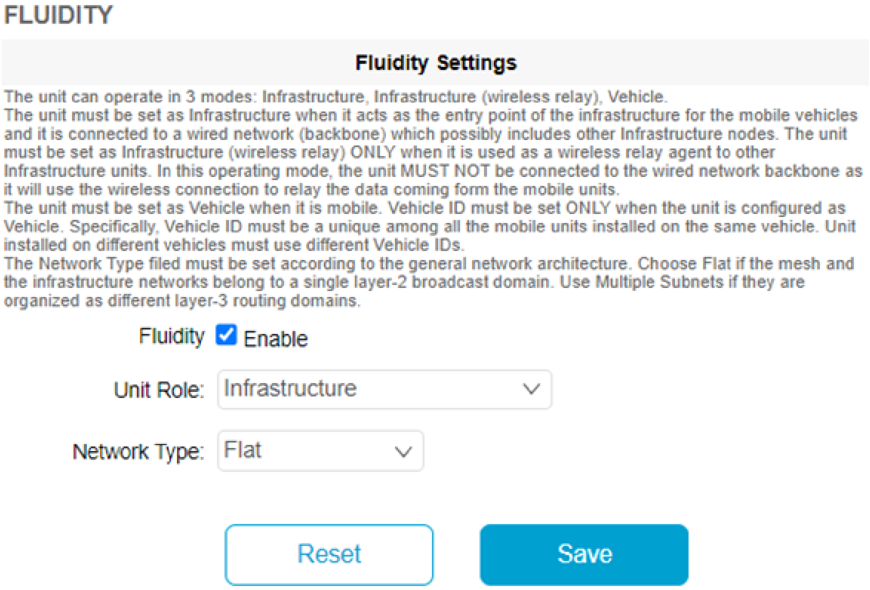
To change the fluidity settings, follow these steps:

Before you begin

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

Procedure

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

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:

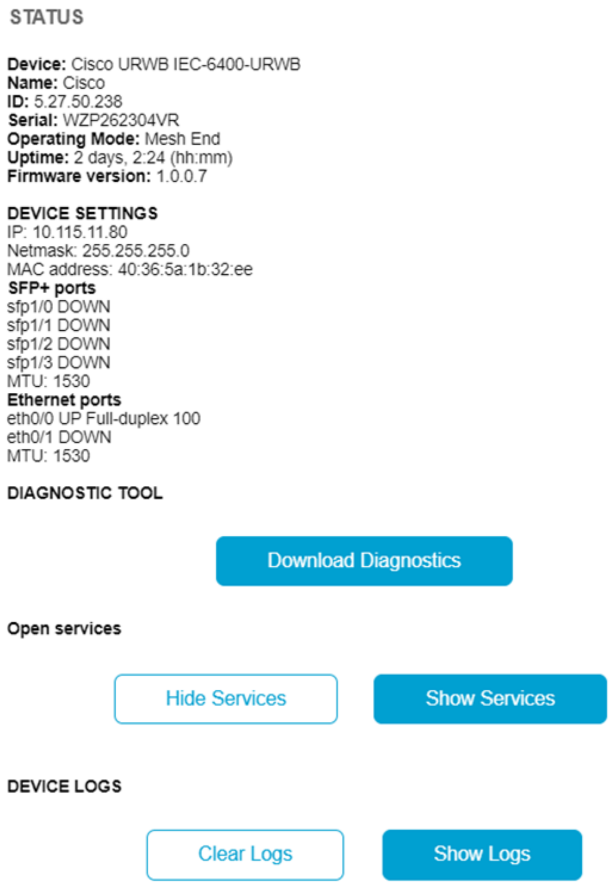
```
Device# fluidity status enabled
```

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

Open services

DEVICE 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.

CHAPTER 9

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`

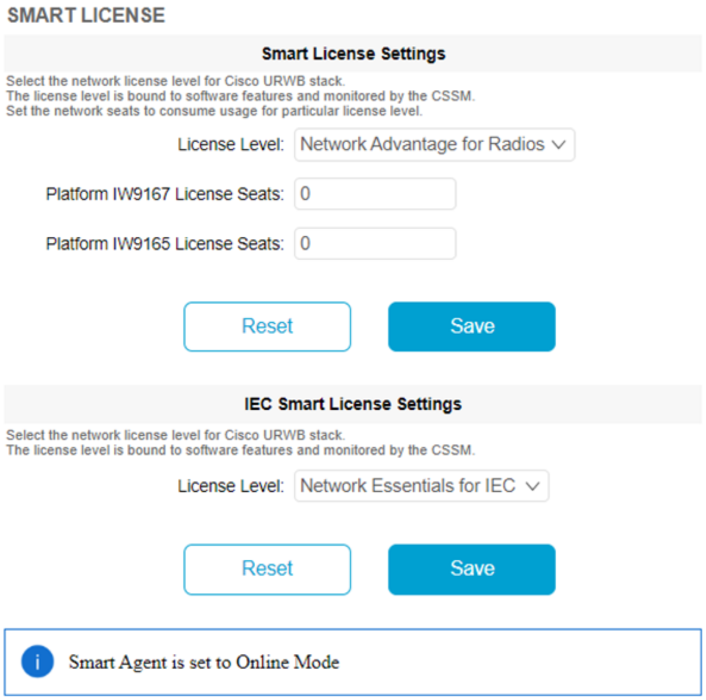
Configuring Smart Licensing using GUI

Before you begin

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

Procedure

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



SMART LICENSE

Smart License Settings

Select the network license level for Cisco URWB stack.
The license level is bound to software features and monitored by the CSSM.
Set the network seats to consume usage for particular license level.

License Level: Network Advantage for Radios

Platform IW9167 License Seats: 0

Platform IW9165 License Seats: 0

IEC Smart License Settings

Select the network license level for Cisco URWB stack.
The license level is bound to software features and monitored by the CSSM.

License Level: Network Essentials for IEC

Smart Agent is set to Online Mode

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
```

CHAPTER 10

Layer 2 Mesh Transparency

Overview of Layer 2 mesh transparency

From IEC6400 Release 1.1.0, the IEC6400 gateway supports Layer 2 Mesh Transparency feature. Layer 2 mesh transparency feature allows to forward non-IPv4 Layer 2 protocols across the URWB network by selectively filtering which ether-types are permitted. The selection of allowed ether-types can be performed from either the CLI or the GUI.

Features of URWB MPLS Layer 2 mesh networks

The URWB mesh data plane supports these functionalities when used in MPLS Layer 2 mode:

- Detects and reports Ethertype present in the URWB network automatically.
- Supports the configurable list of Ethertypes allowed in the network.
- Manages transparency of Layer 2 protocols in a convenient manner.

List of reserved Ethertypes

These Ethertypes are reserved and cannot be added to the allow list:

Ethertype (value)	Forwardable	Additional Information
0x0000 – 0x05FF	User-configurable	Ethernet-I frames: STP and CDP are subject to other configuration options
0x0800	Yes	IPv4
0x0806	Yes	ARP
0x0900 – 0x09FF	No	URWB signaling protocols
0x8100	Yes	IEEE 802.1Q VLAN encapsulation

Ethertype (value)	Forwardable	Additional Information
0x8847 – 0x8848	No	MPLS
0xFFFF	No	IANA reserved

Advantages of Layer 2 mesh transparency

- Provides detailed control over the forwarding of Layer 2 protocols.
- Ensures backward compatibility with existing deployments by default.
- Allows for full transparency to enable all Layer 2 protocols, if needed.
- Facilitates MAC address learning for generic Ethernet types.

Manage Ethertypes using GUI

Perform these tasks to manage Layer 2 protocols parameters on the gateway:

Add an Ethertype to allowed Ethernet list using GUI

Procedure

Step 1 Launch your computer's web browser and enter the URL to open the configurator login page.

Step 2 Enter your username and password in the respective **Username** and **Enable Password** fields.

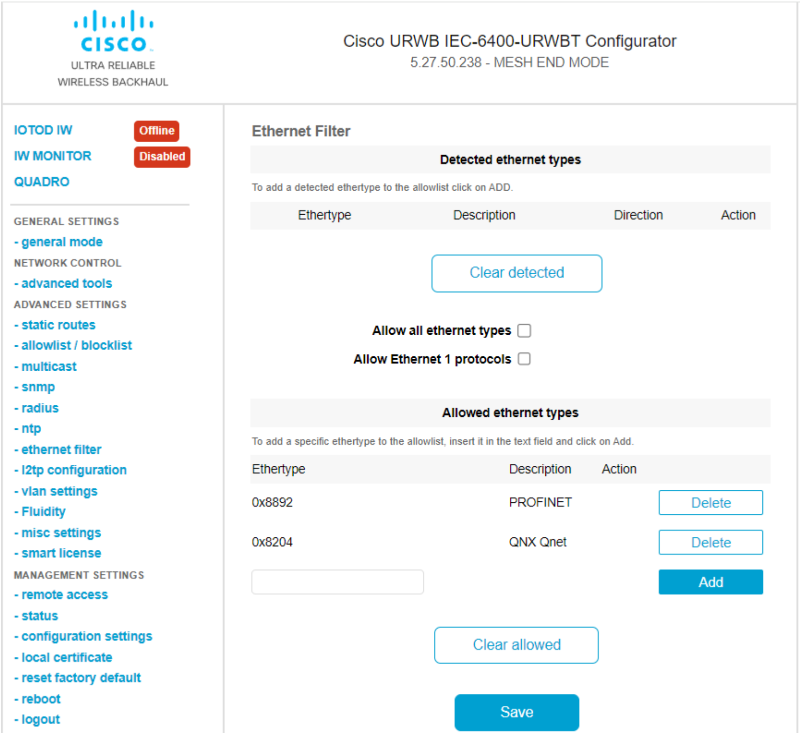
Step 3 Click **Login**.
Once you have successfully logged into the GUI, the URWB configurator is displayed.

Step 4 From the **ADVANCED SETTINGS**, click **ethernet filter** to open the **Ethernet Filter** window.

Step 5 In the **Detected ethernet types** section, click **Add** to add an Ethertype to the **Allowed ethernet types** section.

Step 6 In the **Allowed ethernet types** section, to add an Ethertype that has not been detected yet, enter the specific Ethertype value in the text box and click **Add**.

Step 7 Click **Save** and **Apply** to update the configuration.
The gateway reboots to apply the changes.



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

Ethernet Filter

Detected ethernet types

To add a detected ethertype to the allowlist click on ADD.

Ethertype	Description	Direction	Action

Allow all ethernet types □

Allow Ethernet 1 protocols □

Allowed ethernet types

To add a specific ethertype to the allowlist, insert it in the text field and click on Add.

Ethertype	Description	Action
0x8892	PROFINET	Delete
0x8204	QNX Qnet	Delete
		Add

Allow all Ethertypes to the allow list using GUI

Procedure

Step 1 Launch your computer's web browser and enter the URL to open the configurator login page.

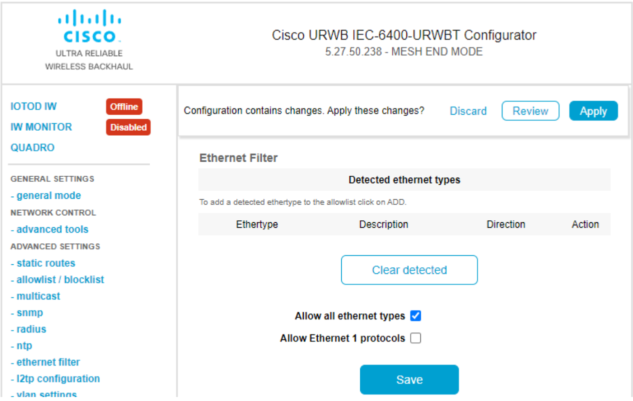
Step 2 Enter your username and password in the respective **Username** and **Enable Password** fields.

Step 3 Click **Login**.
Once you have successfully logged into the GUI, the URWB configurator is displayed.

Step 4 From the **ADVANCED SETTINGS**, click **ethernet filter** to open the **Ethernet Filter** window.

Step 5 Check the **Allow all ethernet types** check box in the **Ethernet Filter** section to allow all Ethertypes.

Step 6 Click **Save** and **Apply** to update the configuration.
The gateway reboots to apply the changes.



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

Configuration contains changes. Apply these changes?

Ethernet Filter

Detected ethernet types

To add a detected ethertype to the allowlist click on ADD.

Ethertype	Description	Direction	Action

Allow all ethernet types ☑

Allow Ethernet 1 protocols □

Clear list of allowed Ethertypes from the allowed Ethernet list using GUI

Procedure

Step 1 Launch your computer's web browser and enter the URL to open the configurator login page.

Step 2 Enter your username and password in the respective **Username** and **Enable Password** fields.

Step 3 Click **Login**.

Once you have successfully logged into the GUI, the URWB configurator is displayed.

Step 4 From the **ADVANCED SETTINGS**, click **ethernet filter** to open the **Ethernet Filter** window.

Step 5 In the **Allowed ethernet types** section, click **Clear allowed** to clear all the Ethertypes from the **Allowed ethernet types** section.

When you click **Clear allowed**, the **Allowed ethernet types** section is cleared.

Step 6 Click **Save** and **Apply** to update the configuration.

The gateway reboots to apply the changes.

Delete list of detected Ethertypes in the detected Ethernet list using GUI

Procedure

Step 1 Launch your computer's web browser and enter the URL to open the configurator login page.

Step 2 Enter your username and password in the respective **Username** and **Enable Password** fields.

Step 3 Click **Login**.

Once you have successfully logged into the GUI, the URWB configurator is displayed.

Step 4 From the **ADVANCED SETTINGS**, click **ethernet filter** to open the **Ethernet Filter** window.

Step 5 In the **Detected ethernet types** section, click **Clear detected** to clear all the detected Ethertypes from the list.

When you click **Clear detected**, the **Detected ethernet types** section is cleared.

Manage Ethernet 1 protocols using GUI

Procedure

Step 1 Launch your computer's web browser and enter the URL to open the configurator login page.

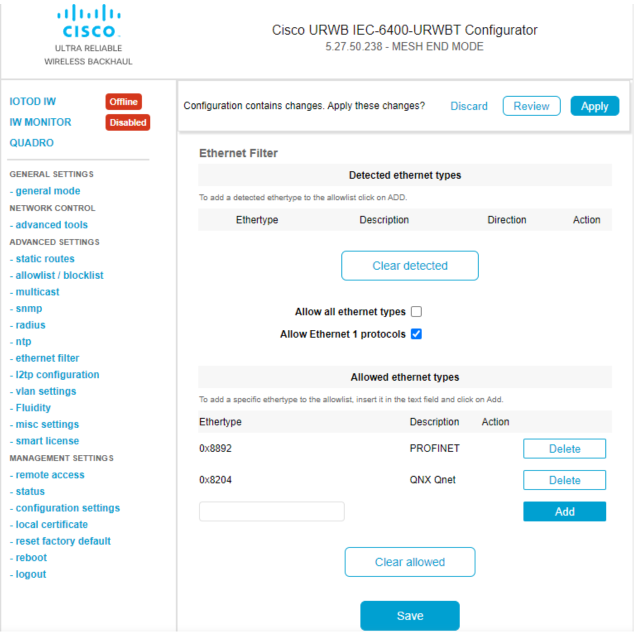
Step 2 Enter your username and password in the respective **Username** and **Enable Password** fields.

Step 3 Click **Login**.
Once you have successfully logged into the GUI, the URWB configurator is displayed.

Step 4 From the **ADVANCED SETTINGS**, click **ethernet filter** to open the **Ethernet Filter** window.

Step 5 Check the **Allow Ethernet 1 protocols** check box in the **Ethernet Filter** window to enable Ethernet 1 protocols.

Step 6 Click **Save** and **Apply** to update the configuration.
The gateway reboots to apply the changes.



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

Configuration contains changes. Apply these changes?

Ethernet Filter

Detected ethernet types

To add a detected ethertype to the allowlist click on ADD.

Ethertype	Description	Direction	Action

Allow all ethernet types ☐

Allow Ethernet 1 protocols ☑

Allowed ethernet types

To add a specific ethertype to the allowlist, insert it in the text field and click on Add.

Ethertype	Description	Action
0x8892	PROFINET	Delete
0x8204	QNX Qnet	Delete
		Add

Manage Ethertypes using CLI

Perform these tasks to manage Layer 2 protocols parameters on the gateway:

Add an Ethertype to the allow list using CLI

Use the **mpls ether-filter allow-list add** *Ethertype value* command to add a specific Ethertype to the allow list.

```
Device#mpls ether-filter allow-list add 0x86DD
```

Delete an Ethertype from the allow list using CLI

Use the **mpls ether-filter allow-list delete** *Ether-type value* command to delete a specific Ethertype from the allow list.

```
Device#mpls ether-filter allow-list delete 0x86DD
```

Verify list of allowed Ethertypes using CLI

Use the **mpls** command to view the list of allowed Ethertypes from the Ethernet filter allow list.

```
Device#mpls
.
.
.
Ethernet Filter allow-list: 0x8892 0x8204 0x86dd, ethernet-I block
.
.
.
```

Note If Ethernet-I is enabled, the **mpls** show output is shown with **Ethernet Filter allow-list: 0x8892 0x8204 0x86dd**.

Clear all Ethertypes from the allow list using CLI

Use the **mpls ether-filter allow-list clear** command to delete all the detected and allowed Ethertypes from the allow list.

```
Device#mpls ether-filter allow-list clear
```

Verify removed Ethernet filter allow list status using CLI

Use the **mpls** command to view the Ethernet filter allow list.

```
Device#mpls
.
.
.
Ethernet Filter allow-list: none, ethernet-I block
.
.
.
```

Note If the allowed ethertypes has been cleared the **mpls** show output is shown with **Ethernet Filter allow-list: none**.

Add all Ethertypes to the allow list using CLI

Use the **mpls ether-filter allow-list add all** command to add all the Ethertypes to allow list.

```
Device#mpls ether-filter allow-list add all
```

Verify all Ethertypes in the allow list using CLI

Use **mpls** command to view the Ethernet filter allow list.

```
Device#mpls
.
.
.
Ethernet Filter allow-list: all, ethernet-I block
```

Note If all Ethertypes are allowed, the **mpls** show output is shown with **Ethernet Filter allow-list: all**.

Enable Ethernet 1 protocol using CLI

Use the **mpls ether-filter ethernet-I forward** command to enable Ethernet 1 protocol.

```
Device#mpls ether-filter ethernet-I forward
```

Block Ethernet 1 protocol using CLI

Use the **mpls ether-filter ethernet-I block** command to block the Ethernet 1 protocol.

```
Device#mpls ether-filter ethernet-I block
```

Verify Ethernet 1 allowed Ethertypes using CLI

Use the **mpls** command to view the list of allowed Ethertypes from the Ethernet filter allow list.

```
Device#mpls
.
.
.
Ethernet Filter allow-list: 0x8892 0x8204 0x86dd, ethernet-I block
.
.
.
```

Note If Ethernet-I is enabled, the **mpls** show output is shown with **ethernet-I forward**.

Clear all detected Ethertypes using CLI

Use the **mpls ether-filter table clear** command to delete all the detected Ethertypes.

```
Device#mpls ether-filter table clear
```

Note The detection process works in background after clearing the detected Ethernet types.

Verify list of detected Ethertypes using CLI

Use the **mpls ether-filter table** command to view the list of detected Ethertypes from the Ethernet filter allow list.

```
Device#mpls ether-filter table
Ether-type Direction Description
0x8899     INGRESS   ---
0x86DD     INGRESS   IPv6
```

CHAPTER 11

Multipath Operation

Overview of Multipath operation

From IEC6400 Release 1.1.0, Multipath Operation (MPO) is supported on the IEC6400 gateway. MPO is a patented technology that enables the simultaneous transmission of high-priority packets over multiple paths. It enhances the reliability and efficiency of wireless communication in fast-moving mobile systems like trains, buses, and other vehicles.

Note

- Gateway licensing policy enables the MPO feature for all license levels.
- Gateway supports up to four redundant paths for MPO-protected traffic.
- Gateway supports receiving duplicate packets. However, the number of replicas is decided by mobile nodes.
- MPO is supported only in Fluidity MPLS Layer 2 configurations.

Overview of MPO data redundancy

The MPO data redundancy enhances the availability and reliability of wireless communication systems. Each wireless link replicates MPO-protected traffic. Even if one wireless link fails, the other links continue to replicate the traffic. This method ensures uninterrupted communication.

Advantages of MPO

- It is useful in environments where network conditions are dynamic and can lead to packet losses.

- It distributes traffic across multiple paths to optimize network performance.
- It removes duplicate packets, so only one copy is processed, reducing unnecessary load.
- It sorts packets by priority by sending critical packets through multiple paths and non-critical packets through a single path.

MPO packet duplication and deduplication

Duplication

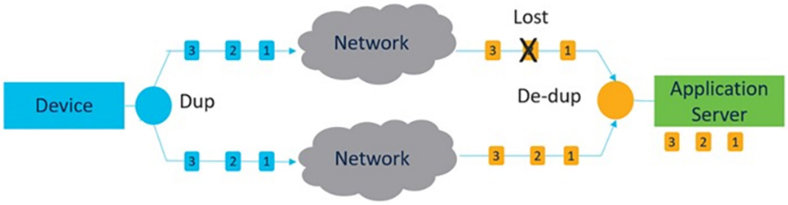
MPO sends the same data across multiple paths in the network. This increases the chances of the data reaching its destination even if some paths fail. It sends duplicate packets using multiple wireless paths to different devices. This enhances the chances of successful packet reception, even if some paths experience losses or delays.

Note For upstream traffic, gateway is in charge of managing the deduplication, whereas duplication is performed only on wireless links by IW devices. For downstream traffic, the roles are inverted.

Deduplication

This process ensures that only one copy of each packet is processed, even if multiple copies are received. It removes duplicate packets using sequence numbers assigned to the packets.

Figure 4: Process of Duplication and Deduplication



Duplication and Deduplication algorithm:

- Handles packet loss and paths with high or variable delays.
- Removes additional packet delays created by buffering.
- Removes duplicate and out-of-sequence packets.

Manage MPO parameters using CLI

Perform these steps to enable MPO, manage MPO CoS, and MPO telemetry.

Note By default, this feature is disabled on the gateway.

Procedure

Step 1 Use the **fluidity mpo status enable** command to enable the MPO feature on the gateway.

```
Device#fluidity mpo status enable
```

Note
Use the **fluidity mpo status disable** command to disable the MPO feature on the gateway.

Step 2 Use the **fluidity mpo cos** *CoS value* command to manage MPO Class-of-Service (CoS) on the gateway.

```
Device#fluidity mpo cos C
```

Configure class-of-service (CoS) of traffic to protect with MPO redundancy, you can use only one CoS at a time. Valid cos range is from zero to seven and the default value is six.

Step 3 Use the **fluidity mpo telemetry enable** command to enable MPO telemetry on the gateway.

```
Device#fluidity mpo telemetry enable
```

Note
- Use the **fluidity mpo telemetry disable** command to disable MPO telemetry on the gateway.
- By default, MPO telemetry is disabled on the gateway.

Step 4 Use the **write** command to apply the configuration in a permanent way.

```
Device#write
```

Step 5 Use the **reboot** command to reboot the device.

```
Device#reboot
```

Manage rx-only MPO from CLI

Rx-Only deduplicates incoming MPLS traffic. However, it does not duplicate outgoing traffic.

Use the **fluidity mpo status rx-only** command to enable RX-Only on the gateway.

```
Device#fluidity mpo status rx-only
```

MPO configuration example

```
Device#fluidity mpo status enabled
Device#fluidity mpo cos 6
Device#fluidity mpo telemetry 1
```

```
Device#write
Device#reboot
```

Verify MPO configuration from CLI

Use the **fluidity mpo** command to view the status of MPO configuration on the gateway.

```
Device#fluidity mpo
Status: enabled
CoS: 6
Telemetry: enabled
```

Verify MPLS configuration from CLI

Use the **mpls** command to view the status of MPLS configuration on the gateway.

```
Device#mpls
layer 2
unicast-flood: enabled (limited rate)
arp-unicast: enabled (broadcasting not allowed)
reduce-broadcast: disabled
pwlist: all
Cluster ID: disabled
Ethernet Filter allow-list: 0x8892 0x8204, ethernet-I block
MPLS fast failover:  enabled
Node failover timeout:  50 ms
L2TP WAN update delay:  100 ms
Preemption delay:  100 s
Virtual IP:  0.0.0.0
ARP limit: rate 0 grace 30000 block 0

MPLS tunnels:
ldp_id 1365673902 debug 0 auto_pw 1
local_gw 5.27.50.238 global_gw 0.0.0.0 pwlist { }
mobility true vehicle_id -2 v2v_handoff 0 v2v_pws false auto_en true static_pws { 0.0.0.0
}
lsps 2
<5.27.50.238 5.212.77.176 233907170> ESTABLISHED ftn 256 ilm 178016 pim- 46.364051233 ka 0
 { 5.27.50.238 5.81.160.244 5.212.77.176 }
<5.27.50.238 5.81.160.244 1316742122> ESTABLISHED ftn 1 ilm 178015 pi-- 2.383096885 ka 0 {
 5.27.50.238 5.81.160.244 }
MPLS Multipath tunnels:
5.212.77.176:
   path_id 0 ilm 178016 nhlfe 48 lbr 5.81.160.244 age 46.432595279 { 5.27.50.238 5.81.160.244
 5.212.77.176 }
   path_id 1 ilm 178017 nhlfe 50 lbr 5.81.160.244 age 46.421394799 { 5.27.50.238 5.81.160.244
 5.212.77.176 }
```

Verify fluidity MPO statistics from CLI

Use the **fluidity mpo statistics** command to view the MPO fluidity statistics of the gateway.

```
Device#fluidity mpo statistics
table-size 2:
MAC address : 40:36:5A:15:C8:50 8C:89:A5:83:EB:71
Tx-1 : 0 208
```

```
Tx-2 : 0 208
Rx-Accept-1 : 178 0
Rx-Accept-2 : 30 0
Rx-Drop-1 : 30 0
Rx-Drop-2 : 178 0
Lost-1-only : 0 0
Lost : 0 0
```

MPO Statistics	Description
MAC address	The source Layer 2 address of the external network device that sends packets.
Tx-1 and Tx-2	Shows the total count of packets that are eligible for duplication.
Rx-Accept-1 and Rx-Accept-2	Shows the total count of packets received and dropped during the de-duplication process. This can happen on either the primary or secondary path.
Lost-1-only	Shows the total count of packets received and accepted during the de-duplication process on the secondary path.
Lost	Shows the cumulative number of packets lost on both the primary and secondary paths.

CHAPTER 12

URWB Telemetry Protocol

Overview of URWB telemetry protocol

From IEC6400 Release 1.1.0, the IEC6400 gateway supports the URWB Telemetry Protocol feature. It performs the external monitoring of real-time wireless performance. Third-party and custom applications can use the telemetry data. This feature sends pre-defined structured UDP packets at regular intervals and it contains network metrics. An application which receives this data can interpret this data live or capture and process it later. This telemetry packet from the gateway contains the packet throughput and migration rate.

For information about the Type-Length-Values (TLVs) for the gateway, contact Cisco Support.

Manage URWB telemetry export parameters using CLI

Before you begin

By default, this feature is disabled on the gateway. Perform these steps to enable the telemetry export.

Procedure

Step 1 Use one of the following commands:

- Use the **telemetry server** *IP-address UDP-port-value* command to enter the IP address and UDP port of the telemetry receiver.

  ```
  Device#telemetry server 192.168.0.100 1234
  ```

  Multicast IP addresses are supported.

  Or

- Use the **telemetry live server** *IP-address UDP-port-value* command to manage the IP address and UDP port of the telemetry receiver.

  ```
  Device#telemetry live server 192.168.0.100 1234
  ```

Step 2 Use one of the following commands:

- Use the **telemetry export enable** command to enable the telemetry transmission to the configured telemetry receiver.

  ```
  Device#telemetry export enable
  ```

  Note

  - Use the **telemetry export disable** command to disable the telemetry transmission to the configured telemetry receiver.
  - When you run the **telemetry export disable** command, the device defaults the IP address to 0.0.0.0, but retains with the UDP port value.

Or

- Use the **telemetry live export enable** command to enable the telemetry transmission to the configured telemetry receiver.

  ```
  Device#telemetry live export enable
  ```

Step 3 **Note**

- If you include **live** keyword in the command, the configuration takes effect immediately.
- If you do not include **live** keyword in the command, you need to run **write** and **reboot** commands.

Use the **write** command to apply the configuration permanently.

```
Device#write
```

Step 4 Use the **reboot** command to reboot the device.

```
Device#reboot
```

URWB telemetry protocol configuration example

CLI command without live:

Use these commands to export the telemetry data when you do not include **live** keyword in the command.

```
Device#telemetry server 192.168.0.100 1234
Device#telemetry export enable
Device#write
Device#reboot
```

CLI command with live:

Use these commands to export the telemetry data when you include **live** keyword in the command.

```
Device#telemetry live server 192.168.0.100 1234
Device#telemetry live export enable
```

Manage telemetry level

Telemetry level default

Use the **telemetry level default** command to send the default statistics to the telemetry server.

```
Device#telemetry level default
```

Telemetry level detailed

Use the **telemetry level detailed** command to send the detailed statistics to the telemetry server. Detailed telemetry includes information for each handoff occurring in the network.

```
Device#telemetry level detailed
```

Verify telemetry configuration

Use the **telemetry** command to view the telemetry configuration.

```
Device#telemetry
Telemetry export: enabled, current (live): disabled
Telemetry server: 192.168.0.100 1234, current (live): 0.0.0.0 30000
```

Note The **current (live)** status in the show output section reflects the current status, which may differ from the stored status due to the live command.

- If you use live option to disable **telemetry** export, the telemetry output shows **current (live): disabled**.
- If you use live option to enable **telemetry** export, the telemetry output shows **current (live): enabled**.
- If you do not use live option to configure **telemetry** server, the telemetry output shows **current(live): 0.0.0.0 30000**.
- If you use live option to configure telemetry server to 192.168.0.100 1234, the telemetry output shows **current(live): 192.168.0.100 1234**.

CHAPTER 13

IW Monitor Management

Overview of IW monitor

From IEC6400 Release 1.1.0, the Industrial Wireless (IW) Monitor feature is introduced on the IEC6400 gateway. IW Monitor is a standalone, on-premise monitoring application for IW devices. It displays real-time data and alerts for URWB devices in the network. This application provides robust monitoring, management, and optimization of industrial wireless networks. IW Monitor can log multiple events and in this release IW monitor logs only ethernet or fiber link change events. For more information about IW Monitor, see the IW Monitor User Guide.

Primary attributes of IW monitor

- Dashboard to monitor network status
- Topology view of the network
- Real-time history charts for wireless Key Performance Indicators (KPIs)
- Real-time performance monitoring
- Process the telemetry data sent by IW devices
- Network events logs

IW monitor dashboard support

The IW Monitor dashboard provides comprehensive support.

- Attach, manage, and detach devices
- Telemetry protocol support
- CLI and GUI management

Attach IW Monitor

Attaching IW Monitor to the device configurator does not require any configuration. You can add gateways and IW devices to the IW Monitor dashboard. For information about adding devices to the IW Monitor application, see Adding Devices to the IW Monitor.

Detach IW monitor using GUI

Procedure

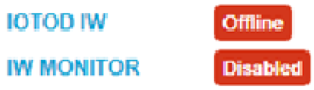
Step 1 Launch your computer's web browser and enter the URL to open the configurator login page.

Step 2 Enter your username and password in the respective **Username** and **Enable Password** fields.

Step 3 Click **Login**.
Upon successful GUI login, the URWB configurator is displayed.

Note
On the URWB configurator home page:

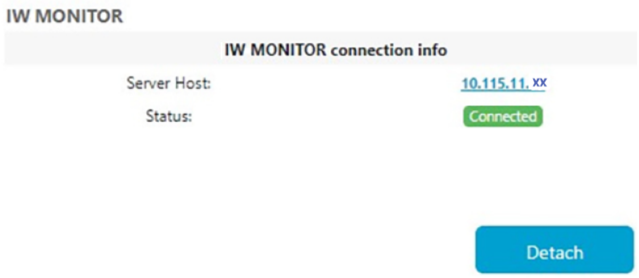
- If the gateway is attached to the IW Monitor server, the **IW Monitor** status is shown as **Enabled** on the left menu.
- If the gateway is detached from the IW Monitor server, the **IW Monitor** status is shown as **Disabled** on the left menu.



IOTOD IW Offline
IW MONITOR Disabled

Step 4 From the left menu, click **IW Monitor** to open the **IW Monitor** window.

Step 5 Click **Detach** to disconnect the device from the IW Monitor server.
In the **IW Monitor** window, **Status** is shown as **Disconnected**.



IW MONITOR

IW MONITOR connection info

Server Host: 10.115.11.xx
Status: Connected

Detach

Detach IW monitor using CLI

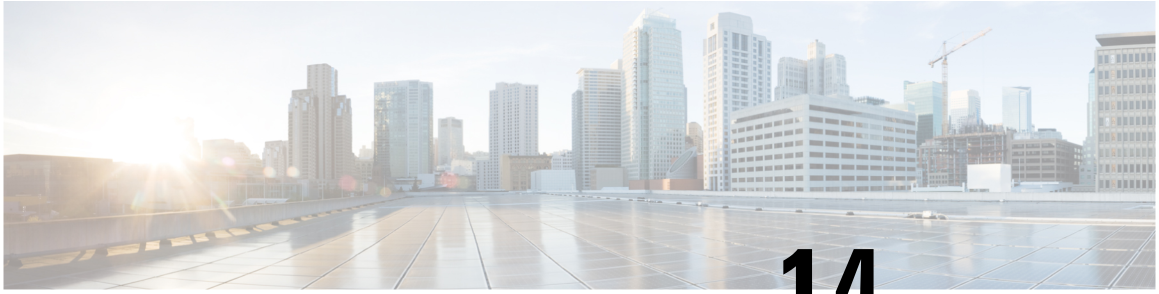
Use the **monitor detach** command to detach the gateway from the IW Monitor server.

```
Device#monitor detach
```

Verify IW Monitor Status using CLI

Use the **monitor** command to view the status of IW Monitor.

```
Device#monitor
IW MONITOR: enabled
Status: Connected
```



CHAPTER 14

Link-Aggregation Modes

Link-Aggregation Modes

Link-aggregation modes are categories that define different methods for combining multiple network connections into a single logical link.

These modes enable network devices to use several physical links together, improving performance, redundancy, and load balancing. Common terms associated with link-aggregation include LACP (Link Aggregation Control Protocol), balance mode, backup mode, and broadcast mode.

This approach distributes traffic across several links, which increases bandwidth and ensures network availability if a link fails. The Link Aggregation Control Protocol (LACP) dynamically manages link aggregation based on the IEEE 802.3ad standard, making it a widely adopted solution for Ethernet networks.

IEC6400 has two 10GBASE-T ports. If it is configured with the optional VIC card, it also has four SFP28 ports. These ports are configured into two logical groups by port type. The first group consists of the two 10GBASE-T ports. The second group consists of the four SFP28 ports.

Link-aggregation manages network traffic among the physical ports belonging to the same group, improving the efficiency of packet transfer. The device supports simultaneous use of Ethernet ports, which increases redundancy, balances network load, and enhances overall performance. Balance mode and LACP mode are specifically designed to optimize packet transfer performance.

By default, the device operates in Backup mode.

Types of Link-Aggregation Modes

These modes define how the device manages aggregated links:

- Backup mode
- Broadcast mode
- Balance mode
- LACP mode

Backup mode

Backup mode is one of the link-aggregation methods, where one link is designated as the primary (active) link, and the others act as backups (standby). Normally, all network traffic flows through the primary link. If the primary link fails, a backup link automatically takes over, ensuring continuous network connectivity.

Broadcast mode

Broadcast mode is one of the link-aggregation methods, where all links belonging to the same group are active and can be used to connect to other equipment.

- In this mode, you should not create loops.
- Broadcast mode does not increase bandwidth efficiency, as all links carry the same traffic, but it maximizes reliability in mission-critical networks.

This mode is ideal for critical network connections where reliability is essential, and bandwidth requirements can be met by a single link.

Sample use case

First Ethernet port is connected to the external device (Switch) on the customer side, and the other Ethernet port is connected to the laptop device.

Balance mode

Balance mode is one of the link-aggregation methods, that distributes network traffic evenly across all available member links in an aggregation group. This helps optimize bandwidth usage and improves overall network performance by preventing any single link from becoming a bottleneck. Hashing on the on the header of the packet decides which part to assign.

LACP mode

LACP mode is one of the link-aggregation methods, that enables the multiple physical Ethernet links to combine into a single logical link. These protocols increase network bandwidth and provide redundancy.

Benefits

- Increased Reliability: Multiple network links are combined, so network connectivity is maintained even if one or more links fail.
- Redundancy: Backup paths for data transmission are automatically provided, significantly reducing the risk of network downtime.
- Simplified Management: Aggregated links are managed as a single logical connection, streamlining configuration and ongoing management tasks.
- Scalability: Network capacity can be easily expanded by adding more links to the aggregation group, supporting growing traffic demands.
- Flexibility: Link aggregation can be configured to meet different networking needs such as load balancing, high availability, or ensuring reliable data delivery, depending on the selected mode.

Prerequisites

- Compatible Network Devices: Both ends of the aggregated links (such as switches, routers, or servers) must support link aggregation and the specific aggregation mode you plan to deploy.
- Uniform Link Speed and Duplex Settings: All physical links within the aggregation group must operate at the same speed (for example, 1 Gbps or 10 Gbps) and have matching duplex settings to ensure stable and consistent performance.
- Port Availability: Ensure that enough free ports are available on both devices to create the desired aggregation group.
- LACP Support and Configuration: Both devices should support IEEE 802.3ad (Link Aggregation Control Protocol, or LACP). LACP must be enabled on both devices when using this dynamic aggregation mode.

Configure Link-aggregation modes using CLI

Configure link aggregation modes to optimize network performance, enhance bandwidth, and provide redundancy for network links.

Link aggregation combines multiple physical Ethernet links into a single logical link. This task describes how to configure the various link aggregation modes available on your device using CLI

Procedure

Step 1 Use the **ethernet link-aggregation** command to display the available link aggregation modes on the device.

```
Device# ethernet link-aggregation
```

The device supports these link aggregation modes:

```
Device# ethernet link-aggregation
 lacp       dynamic link aggregation (802.3ad) mode
balance    XOR balanced mode
broadcast  broadcast mode
backup     backup mode
```

Example:

- Enable LACP mode:

  ```
  Device# ethernet link-aggregation lacp
  ```

- Enable balance mode:

  ```
  Device# ethernet link-aggregation balance
  ```

- Enable broadcast mode:

  ```
  Device# ethernet link-aggregation broadcast
  ```

- Enable backup mode:

  ```
  Device# ethernet link-aggregation backup
  ```

Step 2 Use the **write** command to save the current configuration settings to the device's persistent memory.

```
Device# write
```

Step 3 Use the **reboot** command to restart the device.

```
Device# reboot
```

Configure Backup mode using CLI

Perform this task to enable a backup mechanism for link aggregation, ensuring network resilience and continued operation in case of primary link failure.

This procedure outlines the steps to configure and apply backup mode settings using the CLI, that is crucial for maintaining network availability and stability.

Procedure

Step 1 Use the **ethernet link-aggregation backup** command to configure backup mode on the device.

```
Device# ethernet link-aggregation backup
```

Step 2 Use the **write** command to apply the current configuration settings to the device.

```
Device# write
```

Step 3 Use the **reboot** command to restart the device.

```
Device# reboot
```

Configure Broadcast mode using CLI

Configure the broadcast mode to define how broadcast traffic is handled across the aggregated Ethernet link.

Procedure

Step 1 Use the **ethernet link-aggregation broadcast** command to configure broadcast mode on the device.

```
Device# ethernet link-aggregation broadcast
```

Step 2 Use the **write** command to apply the current configuration settings to the device.

```
Device# write
```

Step 3 Use the **reboot** command to restart the device.

```
Device# reboot
```

Configure Balance mode using CLI

Perform this task to effectively configure the balance mode on your device. This process allows you to optimize network traffic distribution across aggregated links, enhancing bandwidth utilization and providing redundancy.

Configure the balance mode to distribute network traffic across aggregated links, optimizing bandwidth utilization and providing redundancy.

Procedure

Step 1 Use the **ethernet link-aggregation balance** command to configure balance mode on the device.

Example:

```
Device# ethernet link-aggregation balance
```

Step 2 Use the **ethernet link-aggregation balance policy** command to configure any specific policy on the balance mode of the device.

Example:

```
Device# ethernet link-aggregation balance policy
l2   l2 policy: src_mac XOR dst_mac
l23  l23 policy: src_mac XOR dst_mac XOR src_ip XOR dst_ip
l34  l34 policy: src_ip XOR dst_ip XOR src_port XOR dst_port
```

Note

- The l2 policy operates at Layer 2, using source and destination MAC addresses.
- The l23 policy operates at Layer 2 and Layer 3, using source and destination MAC and IP addresses.

- The l34 policy operates only on IP traffic, supporting data transfer through TCP or UDP ports. It does not accept Ethernet traffic.

Policy options are same for both balance and LACP modes.

Step 3 Use the **write** command to apply the current configuration settings to the device.

```
Device# write
```

Step 4 Use the **reboot** command to restart the device.

```
Device# reboot
```

Configure LACP mode using CLI

Use this procedure to enable and customize LACP on your device, which improves network performance and redundancy.

This procedure guides you through configuring LACP mode and its associated load-balancing policies using the CLI.

Procedure

Step 1 Use the **ethernet link-aggregation lacp** command to configure LACP mode on the device.

Example:

```
Device# ethernet link-aggregation lacp
```

Step 2 Use the **ethernet link-aggregation lacp policy** command to configure any specific policy on the lacp mode of the device.

Example:

```
Device# ethernet link-aggregation lacp policy
l2   l2 policy: src_mac XOR dst_mac
l23  l23 policy: src_mac XOR dst_mac XOR src_ip XOR dst_ip
l34  l34 policy: src_ip XOR dst_ip XOR src_port XOR dst_port
```

Note

- The l2 policy operates at Layer 2, using source and destination MAC addresses.
- The l23 policy operates at Layer 2 and Layer 3, using source and destination MAC and IP addresses.
- The l34 policy operates only on IP traffic, supporting data transfer through TCP or UDP ports. It does not accept Ethernet traffic.

Policy options are same for both balance and LACP modes.

Step 3 Use the **write** command to apply the current configuration settings to the device.

```
Device# write
```

Step 4 Use the **reboot** command to restart the device.

```
Device# reboot
```

CHAPTER 15

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, on page 103
- Shutting Down using the Cisco IMC GUI, on page 104
- Shutting Down using Cisco IMC CLI, on page 104

Shutting Down using the Power Button

Procedure

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.

Procedure

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.

Procedure

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.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.