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 1

- Using CIMC CLI, see Accessing Gateway's CLI from CIMC CLI, on page 1

Accessing Gateway's CLI from CIMC CLI

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

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

Step 2 Enter the username and password.

Credentials are *Cisco/Cisco*.

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

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

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

After successful login, the device is in provisioning mode.

Log into the Gateway Configurator for the First Time

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

Before you begin

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

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

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

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

Step 3   Launch the computer's web browser.

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

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

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

- **Username**: Cisco

- **Password**: Cisco

Step 6   Click **Login**.

# Changing the Default Login Credentials

Before you begin

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

Configuring New Login Credentials using GUI

To change the login credentials, follow these steps:

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

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

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

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

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

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

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

Step 8 Click **Change**.
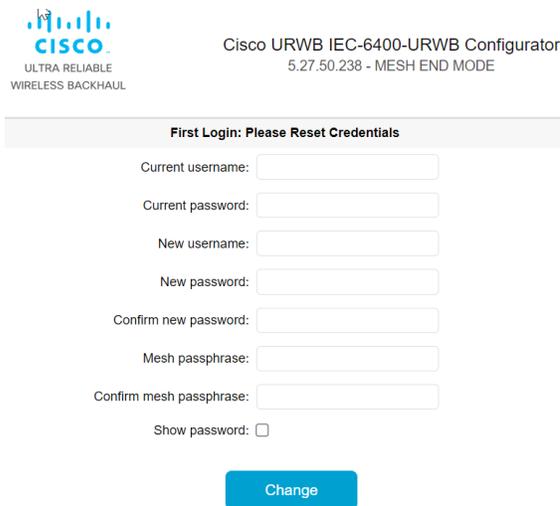
CISCO
ULTRA RELIABLE
WIRELESS BACKHAUL

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: ☐

Change

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

Configuring New Login Credentials using CLI

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

- Through SSH from data ports, see Log into the Gateway Configurator for the First Time, on page 1

- Through CIMC CLI, see Accessing Gateway's CLI from CIMC CLI, on page 1

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

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

Note The default login credentials are:

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

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

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

• Example of configuring a password from the CLI:

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

Step 3   After the first login, reset your credentials:

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

Step 4   After successful credentials change, login again:

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

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

Rules to Reset the Login Credentials

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

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

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

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

• The following special characters are permitted:

　　• ! (Exclamation mark)

　　• * (Asterisk)

　　• + (Plus sign)

　　• - (Minus sign)

　　• , (Comma)

　　• - (Hyphen)

　　• @ (At sign)

　　• ^ (Circumflex)

　　• _ (Underscore)

- The password must not contain:

  - White spaces

  - Name like Cisco, such as CiSc0 or 0cSiC

  - Three sequential characters or digits (ABC/ CBA) or (123/321)

  - The same three characters or digits consecutively (AAA) or (666)

  - Same as or the reverse of the username

  - Same as the current or existing password