Dickson LoRa® Gateways

Firmware version 6.x
(starting December 2022)

DICKSON
Environmental Monitoring + Compliance Experts

Notices and safety

Disclaimer and limitation of liability

Dickson assumes no liability for any loss or claims by third parties which may arise through the use of this product. Users must not use the product in any manner not specifically indicated by Dickson.

Dickson shall not be held liable for improper use of this product.

This document is non-contractual and subject to change without notice.

Safety instructions

The latest safety instructions document is available for download from the Dickson website. Flash this QR code to access the document:

https://docs.oceaview.com/dickson_safety.pdf

Certifications and compliance

Caution: Any changes or modifications made to this product not expressly approved in writing by Dickson could void the user's authority to operate the equipment.

FCC statement

This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference received, including interference that may cause undesired operation: FCC Part 15 §107 - §109 - §207 - §247 (Ed 2008).

FCC RF Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

IC statement

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device. Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

CE - Conformity with European regulations

This device is compliant with the essential requirements and other relevant requirements of the following directives.

- 2014/53/EU Radio Equipment Directive (RED)
- 2014/30/EU EMC Directive
- 2014/35/EU Low Voltage Directive
- 2011/65/EU Restriction of Hazardous Substances Directive

WEEE compliance

This device complies with the essential requirements and other relevant provisions of the Waste Electrical and Electronic Equipment Directive 2002/96/EC (WEEE Directive).

Environmental protection

Please respect local regulations concerning disposal of packaging, unused wireless devices, and their accessories, and promote their recycling.

RoHS compliance

This device is compliant with the restriction of the use of certain hazardous substances in electrical and electronic equipment Directive 2002/95/EC (RoHS Directive). Do not dispose of this product with household trash. Dickson recycles this product under certain conditions. Please contact us for more information.

Dickson Europe
Montpellier – France
Tel: +33 499 13 67 30

Dickson North America
Addison, IL – USA
Tel: +1 (630) 543-3747

Dickson Asia
Petaling Jaya – Malaysia
Tel: +6019 880 6438

This is a non-contractual document. Features and specifications mentioned here are subject to change. Document updated for firmware v6.x.x.

June 2023 Ref: ING-INS-142-EN Rev. 14

Table of Contents

1 Introduction

Congratulations and thank you for choosing the Dickson LoRaWAN wireless monitoring solution. This document describes how to set up and use the Dickson LoRaWAN-enabled gateways, a key component for collecting data in your monitoring solution.

> The functionality of the Advanced and Pro models (shown below) is strictly identical. The two models only vary somewhat in terms of hardware aspects.

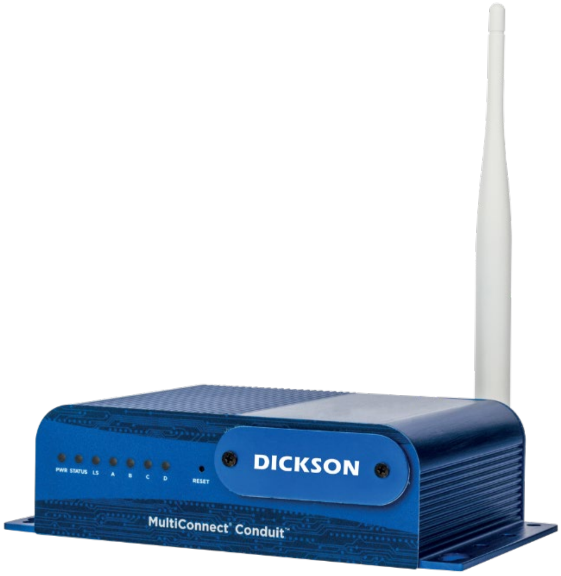


Figure 1 – Dickson Advanced LoRaWAN enabled gateway

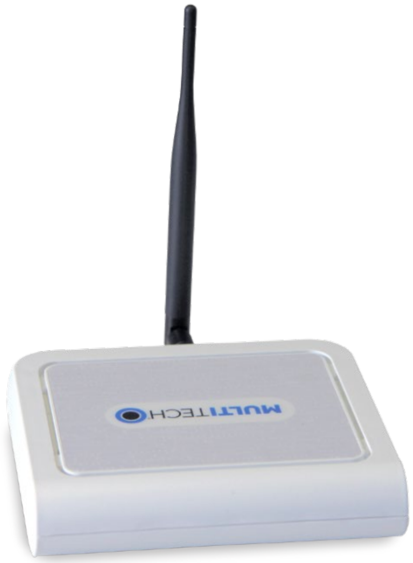


Figure 2 – Dickson Pro LoRaWAN enabled gateway

1.1 Overview

Designed for use with Dickson wireless data loggers featuring LoRaWAN connectivity, the Dickson LoRaWAN gateway is a wireless gateway that leverages new-generation LoRaWAN Internet of Things technology to offer exceptionally long-range wireless communication.

This gateway can be connected to your local network via either a wired Ethernet or a Wi-Fi connection, or to a cellular data network with the optional cellular data option.

1.2 Detailed description

1.2.1 Key features

- Compatible with Dickson LoRaWAN data loggers
- Low energy technology preserves data logger battery
- LED status indicators
- Software updates via integrated web interface

1.2.2 Data management

- Collects/forwards data from data loggers to Cloud or On-premises server

1.2.3 Connectivity

- LoRaWAN long-range wireless technology
- Range up to about 15 km/10 miles
- Automatic data logger detection
- LoRaWAN channel plans in ISM spectrum (depending on model):

  EU868, US915, AU915, IN865, KR920, AS923-1, AS923-2, AS923-3, AS923-4, and RU864

1.2.4 Hardware details (both Pro and Advanced models)

- Antenna (+3dBi default; +5dBi or +8dBi optional)
- External power supply (110-240V AC adapter)

  Note: the LoRa Pro Gateway is available with Power-over-Ethernet (POE) to take power directly from a connected Ethernet cable (as supported by your router)
- ARM9 400MHz; 256 MB DDR RAM; 256 MB Flash
- Storage conditions: -40 °C to +85 °C (-40 °F to +185 °F); 20 to 90% RH (non-condensing)
- Wall-mount, screw attachment
- LoRaWAN / Wi-Fi / Cellular data: FCC, CE, IC
- ROHS 3, REACH, PROP-65

1.2.5 Hardware details – Advanced model (blue)

- Connectivity options: Ethernet; Wi-Fi (802.11 a/b/n/g, 2.4 & 5 GHz); and/or 4G-LTE cellular

  Note: cellular connection requires standard sized SIM card
- Operating conditions: -30 °C to +70 °C (-22 °F to +158 °F); 20 to 90% RH (non-condensing)
- Anodized aluminum, IP30 rating
- Dimensions: 161.3 x 107.4 x 42.8 mm (6.4 x 4.2 x 1.7 in.); weight: 450 g (16 oz.)

1.2.6 Hardware details – Pro model (gray)

- POE (Power-over-Ethernet) available as option
- Connectivity options: Ethernet or Ethernet/4G-LTE cellular

  Note: cellular connection requires micro-SIM)
- Operating conditions: 0 °C to +70 °C (32 °F to +158 °F); 20 to 90% RH (non-condensing)
- PC-ABS (polycarbonate-ABS), IP30 rating
- Dimensions: 165 x 135 x 36 mm (6.5 x 5.3 x 1.4 in.)
- Weight: 284 g (10 oz.)

1.2.7 Technical highlights

- Wireless range up to about 10 miles (16 km) line-of-sight
- 2-way wireless communications
- Available LoRaWAN protocol frequencies: 915 MHz, 868 MHz, 434 MHz
- Wired Ethernet or Wi-Fi network connection
- Optional cellular data module

1.2.8 Package contents

- Dickson LoRaWAN enabled gateway
- AC adapter (110-240 v)
- LoRaWAN antenna
- Ethernet cable

Optional and to be ordered separately

- Wi-Fi wireless module
- Cellular data module, antenna, and SIM card (standard or micro-SIM depending on the gateway model)

1.3 Architecture and technologies

Installed locally at your site, the Dickson LoRaWAN enabled gateway collects data from compatible Dickson data loggers within wireless range.

The gateway is connected permanently via the Internet to the OCEAView Cloud or On-premises platform, where collected data is transferred by the gateway, and accessed using the OCEAView web application. The diagram below shows the overall solution organization, with the gateway collecting data from modules and forwarding it to the OCEACloud platform.

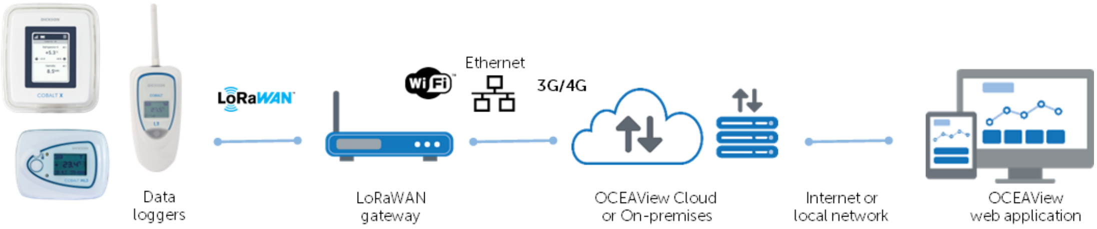


Figure 3 – Gateway connecting LoRaWAN data loggers to OCEAView

2 Setting up your gateway

The Dickson LoRaWAN gateway is configured using an integrated web interface, which you must use to determine how your gateway connects to the Internet, that is, via an Ethernet or Wi-Fi , or cellular data connection, as well as how it reaches your OCEAView Cloud or On-premises solution. This chapter describes how to set up your gateway as necessary.

2.1 Getting started

2.1.1 Plug in the LoRaWAN antenna

Advanced model

1. Plug the provided LoRaWAN radio antenna on the "RF" connector (the location may vary according to your unit's options).
2. Hand-tighten the antenna by rotating the ring clockwise.

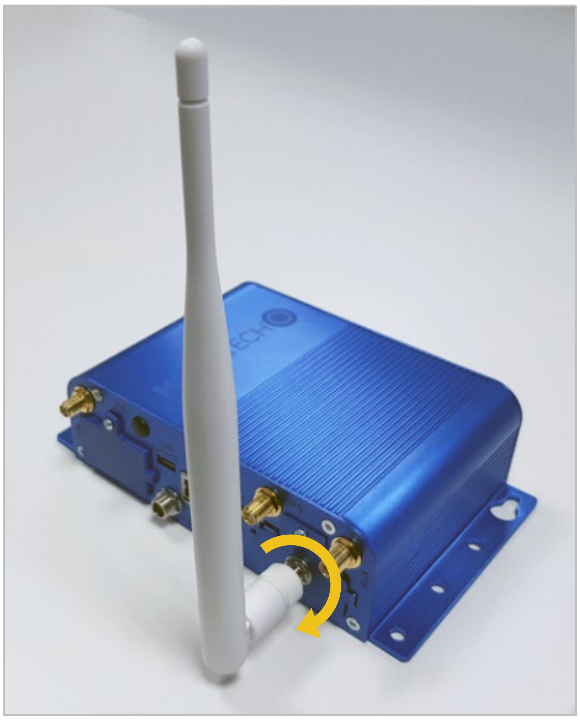


Figure 4 – Attach LoRaWAN antenna to connector labeled "RF"

Pro model

1. Plug the provided LoRaWAN radio antenna on the connector on the back of the device
2. Hand-tighten the antenna by rotating the ring clockwise.

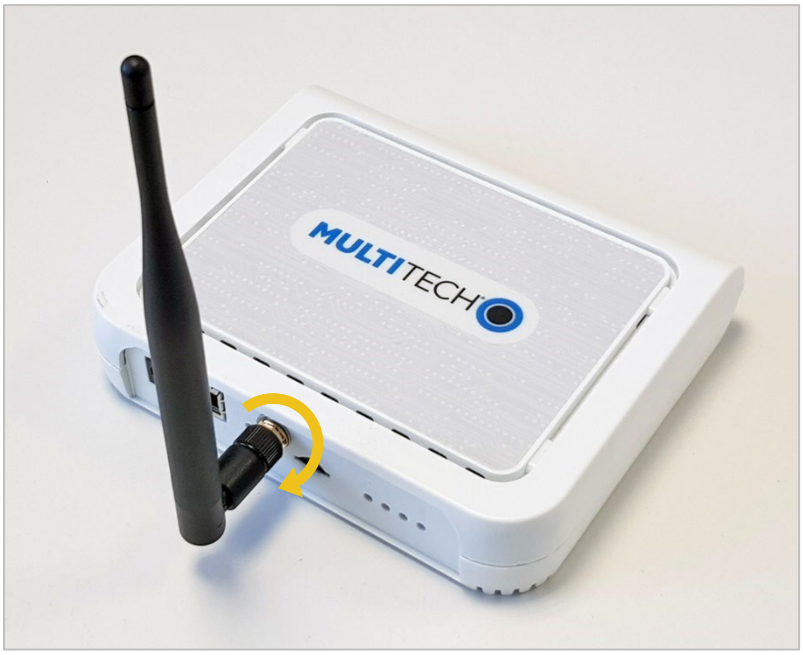


Figure 5 – Attach LoRaWAN antenna to the connector

2.1.2 Plug in the power cable

Advanced model

1. Plug the screw-on power cable on the stainless-steel connector on the back of the gateway. The cable only fits correctly onto one of the connectors.
2. Hand-tighten the cable by rotating the steel ring clockwise to attach it firmly to the unit.

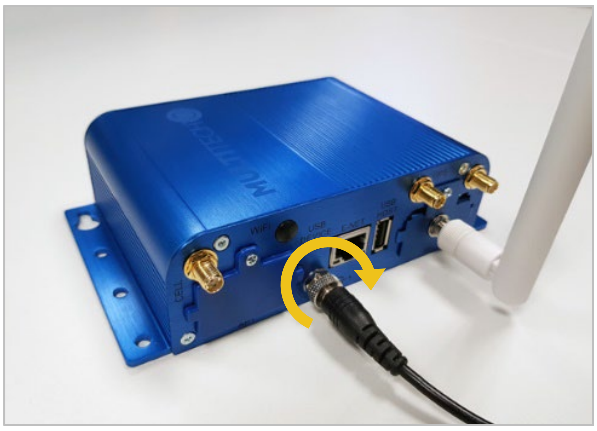


Figure 6 – Plug in the power cable to the stainless-steel connector

3. Plug the AC adapter into a power socket to boot the gateway. The startup process may take up to 5 minutes to complete. When the unit is ready for use, the left-hand LED remains lit as shown here (the Status LED may continue to blink):

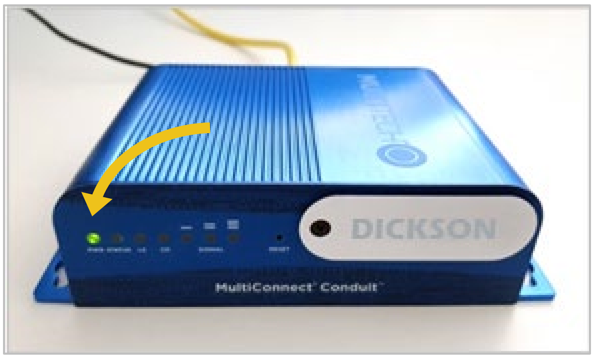


Figure 7 – Power indicator remains on when gateway is ready to use

Pro model

1. Plug the power cable firmly into the power plug on the back of the device.

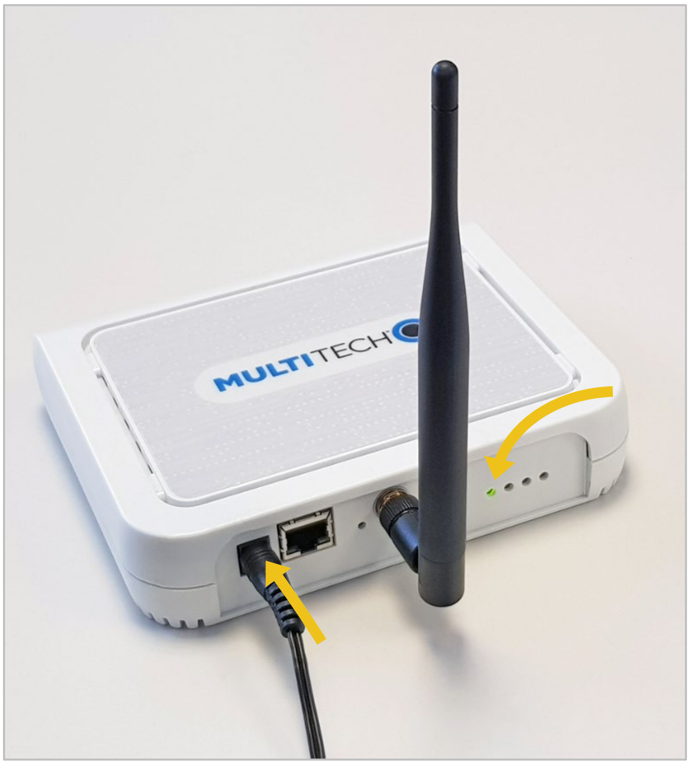


Figure 8 – Plug in the power cable into the power plug

2. Plug the AC adapter into a power socket to boot the gateway. The startup process may take up to 5 minutes to complete. When the unit is ready for use, the status LED turns green. LED activity will vary depending on the connection type.

2.1.3 Connect your computer to the gateway for configuration

1. Plug the Ethernet network cable into the Ethernet port on the back of the gateway.

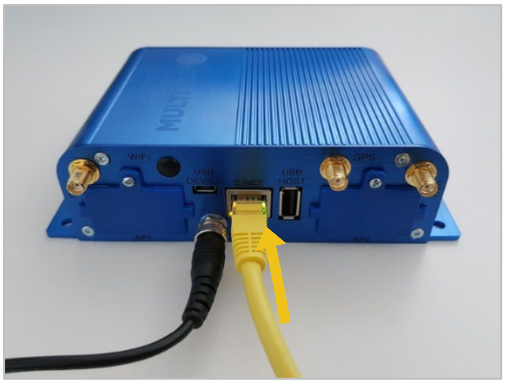


Figure 9 – Advanced model with Ethernet cable

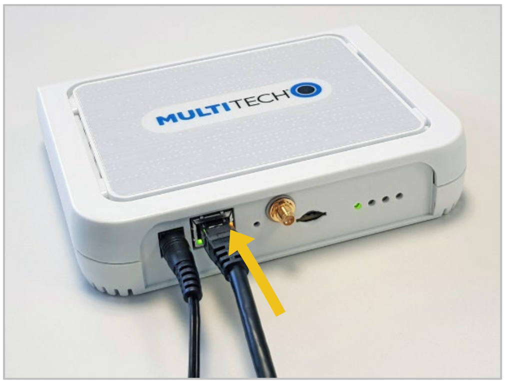


Figure 10 – Pro model with Ethernet cable

2. Plug the other end of the cable into your computer. In your computer's network settings, assign the following IP information temporarily (make sure you change it back when done configuring your gateway):

   IP: 192.168.2.199

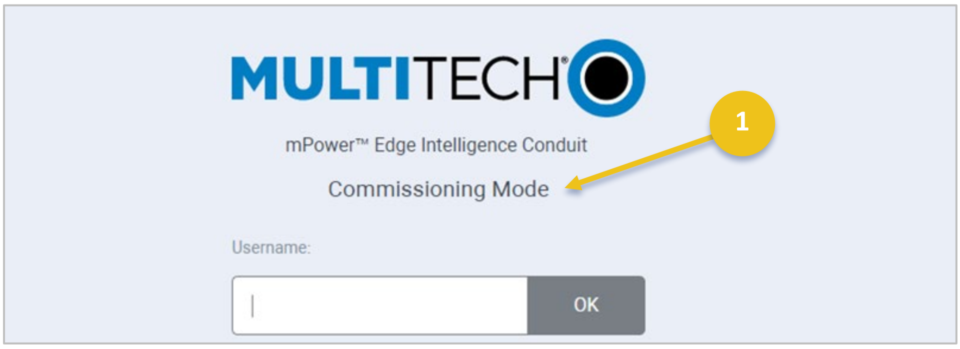
   Mask: 255.255.255.0

3. Use your web browser to connect to the gateway's default IP address: http://192.168.2.1

> ! We recommend that you use the Google Chrome web browser.

Upon first boot, the gateway is in "Commissioning mode" (1) and you will be prompted to create a new username and password. There is no default username or password.

4. Create a default **Username** and press **OK**.



MULTITECH

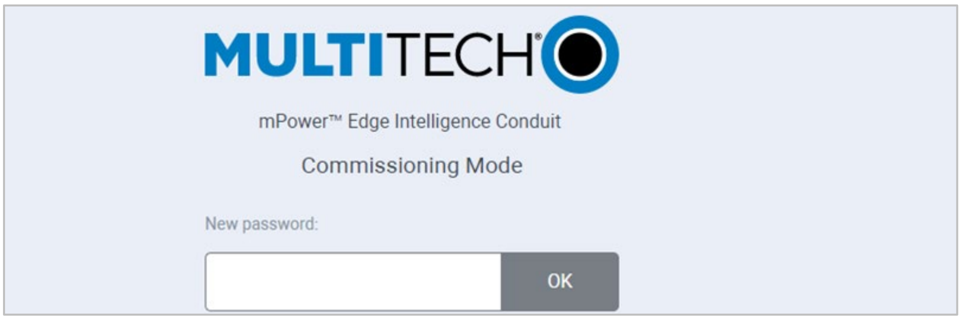
mPower™ Edge Intelligence Conduit

Commissioning Mode

Username:

Figure 11 – Creating a Username in Commissioning Mode

5. Enter a **Password** and press **OK**, then confirm the password and press **OK** again:



MULTITECH

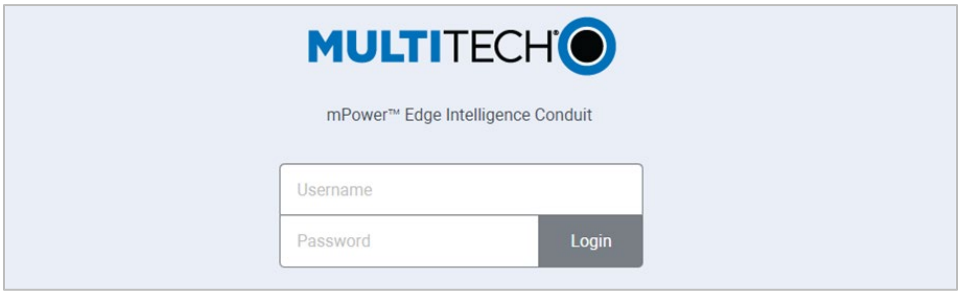
mPower™ Edge Intelligence Conduit

Commissioning Mode

New password:

Figure 12 – Assigning a password for the Username

6. You may then login using the information you just entered.



MULTITECH

mPower™ Edge Intelligence Conduit

Username

Password

Figure 13 – Login with the new Username and Password

! When you connect to the gateway for the first time, a First-Time Setup Wizard runs automatically.

We recommend that you close the Wizard and proceed with gateway set-up manually as described here.

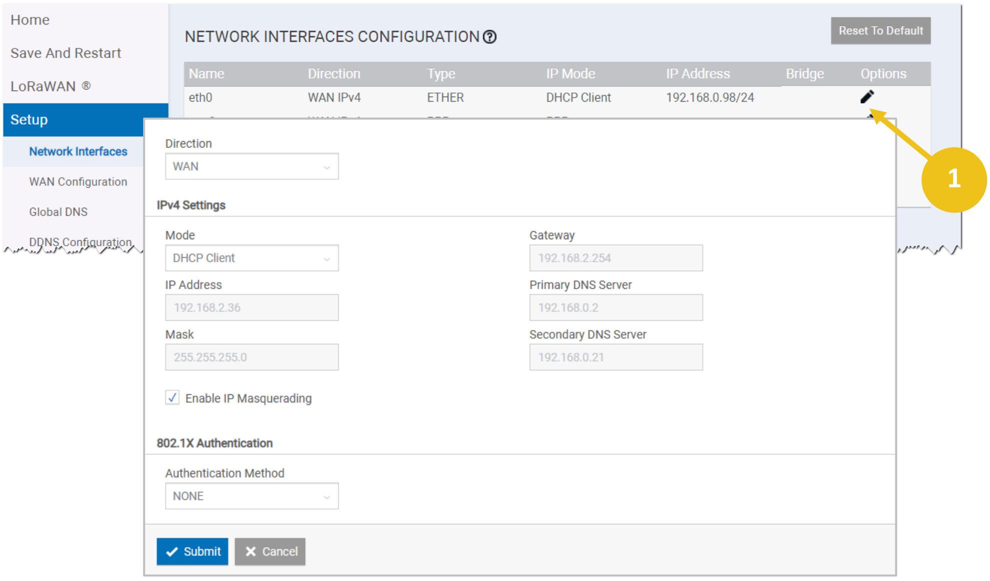
2.2 Setting up network connections

The next step in the setup process is to configure the network connection.

2.2.1 Ethernet connection to your network

This section describes how to configure your gateway with a wired Ethernet connection. The gateway does not need to be placed in its final location for this operation, but it does need to be accessible over your network.

1. Click on **Setup** ➔ **Network Interfaces** ➔ 🖉 (**Options**) for “eth0” (1):



NETWORK INTERFACES CONFIGURATION

Name	Direction	Type	IP Mode	IP Address	Bridge	Options
eth0	WAN IPv4	ETHER	DHCP Client	192.168.0.98/24		🖉

Direction: WAN

IPv4 Settings

Mode: DHCP Client

IP Address: 192.168.2.36

Mask: 255.255.255.0

Gateway: 192.168.2.254

Primary DNS Server: 192.168.0.2

Secondary DNS Server: 192.168.0.21

☑ Enable IP Masquerading

802.1X Authentication

Authentication Method: NONE

Figure 14 – Adapt Ethernet settings for your network

2. Adjust the various settings in the **Network Interface Configuration** window to match your network:

Option	Setting
Direction	**WAN**
Mode	You may choose **Static** (in which case you must set the IP Address in the field below), or **DHCP Client** (the gateway gets its IP address from your network’s DHCP server).
IP Address, Mask, Gateway, Primary DNS Server, Secondary DNS Server…	Enter the IP addresses according to your network configuration. Tick the **Enable IP Masquerading** checkbox and leave Authentication Method set to **NONE**.

3. Click on **Submit** when you are done.

   If you connected your computer directly to the gateway with an Ethernet cable, remember to plug the gateway into your Local Area Network.

❗ It is essential to leave the DHCP Server option disabled on your gateway (**Setup → DHCP**). Enabling that option could create a conflict with your network's regular DHCP server.

This is not to be confused with the DHCP Client option described above. You do not need to configure other options in the **Network Interfaces** section.

2.2.2 Wi-Fi connection to your network (Advanced model only)

This section describes how to configure your gateway with a Wi-Fi wireless connection using DCHP automatic IP address assignment.

> If you need to use your LoRaWAN router in Wi-Fi mode with a static IP address, please see *section 2.2.2.1 –*
>
> *Workaround for Wi-Fi connection with static* IP address*, p. 22.*

To set up Wi-Fi wireless access for your gateway:

1. Plug the provided Wi-Fi antenna on the Wi-Fi connector and rotate the ring clockwise to fasten the antenna securely:

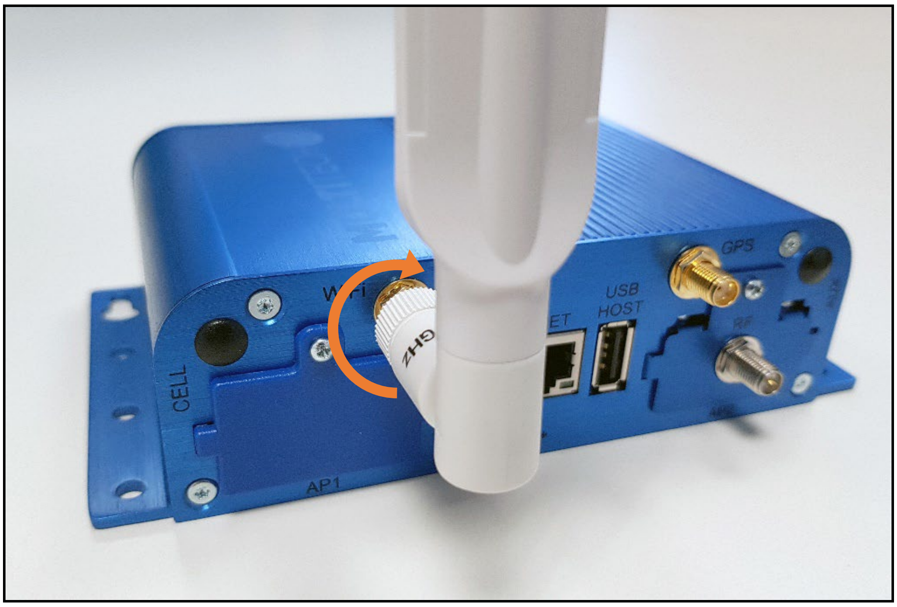
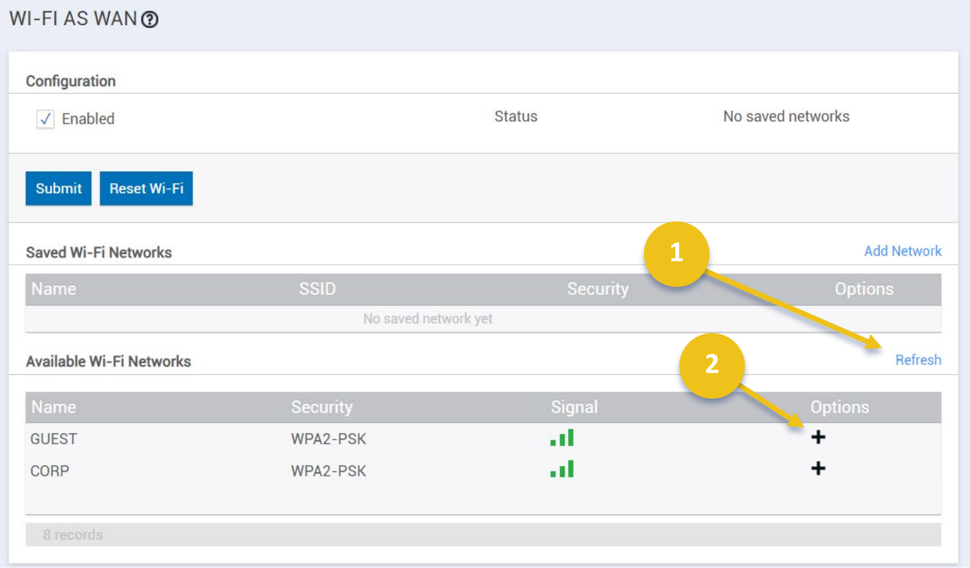


Figure 15 – Attaching antenna for Wi-Fi network

2. Click on **Wireless** (in the left-hand menu) ➔ **Wi-Fi as WAN**, as shown here:



WI-FI AS WAN

Configuration

☑ Enabled | Status | No saved networks

Submit | Reset Wi-Fi

Saved Wi-Fi Networks | Add Network

Name	SSID	Security	Options
No saved network yet			

Available Wi-Fi Networks | Refresh

Name	Security	Signal	Options
GUEST	WPA2-PSK	▂▄▆	+
CORP	WPA2-PSK	▂▄▆	+

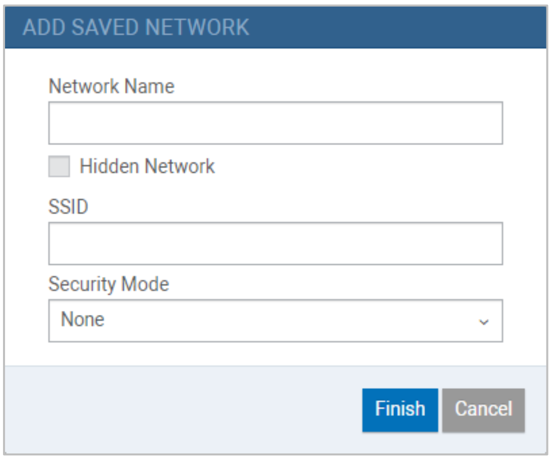
8 records

Figure 16 – Adding a Wi-Fi network

3. Click on **Enabled** to activate WiFi, then on **Refresh** to display available WiFi networks.

   If your network is listed, click on the corresponding ✚ icon and enter the required security information (notably the **Shared key** to access the network). Then click on **Finish** ➔ **Submit** to save your changes.

   If your network is not listed, click on **Add Network** and fill in the information as required:



ADD SAVED NETWORK

Network Name

□ Hidden Network

SSID

Security Mode

None

Finish | Cancel

Figure 17 – Wi-Fi network settings

Option	Setting
Network Name	Assign a “friendly” name for the network.
SSID	Enter the exact real network name.
Security Mode	Choose the security and key encryption methods used by your Wi-Fi network

Click on **Finish ➔ Submit** (2) to save these settings.

4. If this is the only change you are making to your configuration, click on **Save and Apply**.

   Otherwise, we recommend waiting until you have made all your changes and do a global **Save and Apply** when you are done (or **Save and Restart** depending on the settings you changed). The process takes several minutes and there is no reason to launch it multiple times.

2.2.2.1 Workaround for Wi-Fi connection with static IP address

As of this writing, the Dickson LoRaWAN gateway does not support the use of a static IP address for Wi-Fi communications.

If you need to use your Dickson LoRaWAN gateway in Wi-Fi mode with a static IP address, you must implement a workaround solution using an intermediary Wi-Fi repeater or router whose setup allows a fixed IP address, as shown below, to connect to your network.

> ! The Wi-Fi router or repeater must also support being configured as a Wi-Fi *client* in order to connect to your organization's Wi-Fi *access point*.

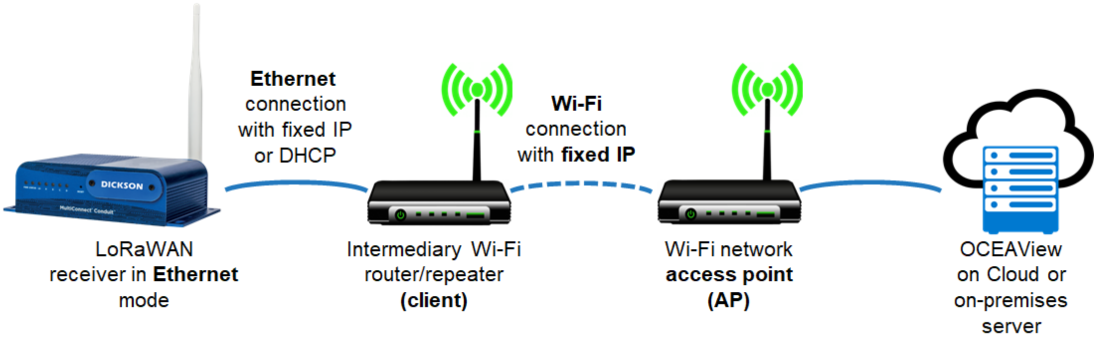

Ethernet connection with fixed IP or DHCP
Wi-Fi connection with fixed IP
LoRaWAN receiver in Ethernet mode
Intermediary Wi-Fi router/repeater (client)
Wi-Fi network access point (AP)
OCEAView on Cloud or on-premises server
DICKSON

Figure 18 – Using an intermediary Wi-Fi router or repeater to provide a static IP address

To implement this workaround:

1. Set up an intermediary Wi-Fi router/repeater whose configuration options allow you to set a static IP address for connecting to your network. That device must also be configurable as a Wi-Fi *client* (and not just as an *access point* (AP).
2. Connect the router to your network.

   Note: We recommend that you test the router using a laptop computer plugged into an Ethernet port (as the Dickson LoRaWAN gateway will be)
3. Set up the Dickson LoRaWAN gateway to use an **Ethernet** connection (as described in *section 2.2.1 – Ethernet connection to your network, p. 17*) either with a static IP address or using DHCP, according to your requirements.
4. Connect the Dickson LoRaWAN gateway to the Wi-Fi router using an Ethernet cable.

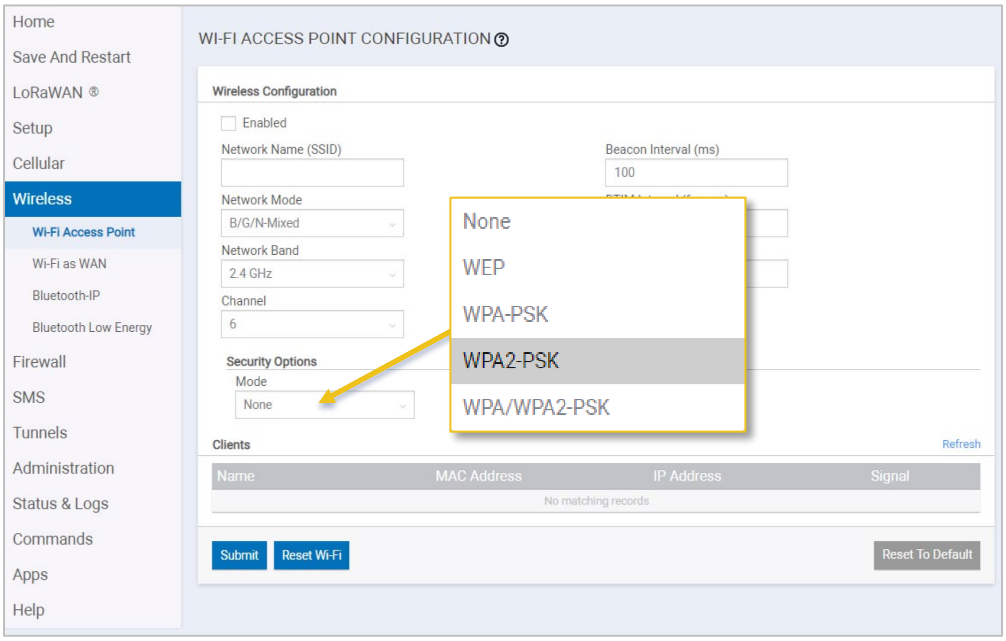
2.2.2.2 Using a pre-shared WPA/WPA2 key

Wi-Fi Protected Access Pre-Shared Key (WPA-PSK) is an encryption method for authenticating users or devices on wireless local area networks.

Some Wi-Fi networks may require you to enter a pre-shared WPA/WPA2 key in order to connect the LoRaWAN gateway.

In the gateway's administration interface:

1. Click on **Wireless**, then click in the **Security Options** field.



□ Enabled

Network Name (SSID):

Beacon Interval (ms): 100

Network Mode: B/G/N-Mixed

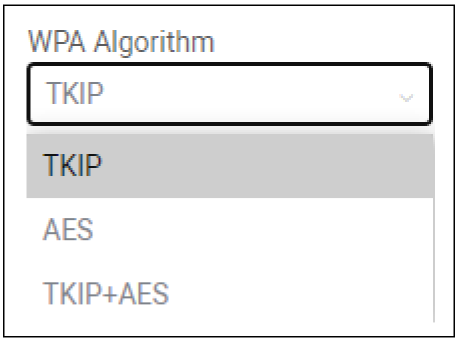
Network Band: 2.4 GHz

Channel: 6

Mode: None

Figure 19 – Assigning a pre-shared Wi-Fi key

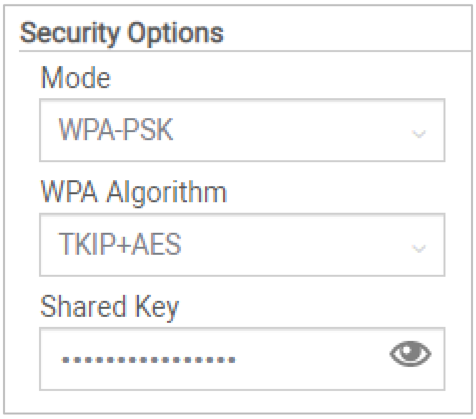
2. Choose the security option used for your network. For example, if you choose WPA or WPA2, click to select the appropriate WPA Algorithm:



WPA Algorithm: TKIP

Figure 20 – Assigning a pre-shared Wi-Fi key

3. Enter the key in the **Shared Key** field.



Security Options

Mode

WPA-PSK

WPA Algorithm

TKIP+AES

Shared Key

•••••••••••••••••

Figure 21 – Entering the shared key information

4. Click on **Submit** in the lower left-hand corner of the screen when done.
5. If this is the only change you are making to your configuration, click on **Save and Apply**.

   Otherwise, we recommend waiting until you have made all your changes and do a global **Save and Apply** when you are done (or **Save and Restart** depending on the settings you changed). The process takes several minutes and there is no reason to launch it multiple times.

2.2.3 Cellular data connection (optional)

This section describes how to configure your compatible gateway with a cellular data connection.

2.2.3.1 Inserting standard sized SIM card in Advanced model

1. Plug the provided cellular antenna on the cellular radio connector (marked "**Cell**") and rotate the ring clockwise to fasten the antenna securely:

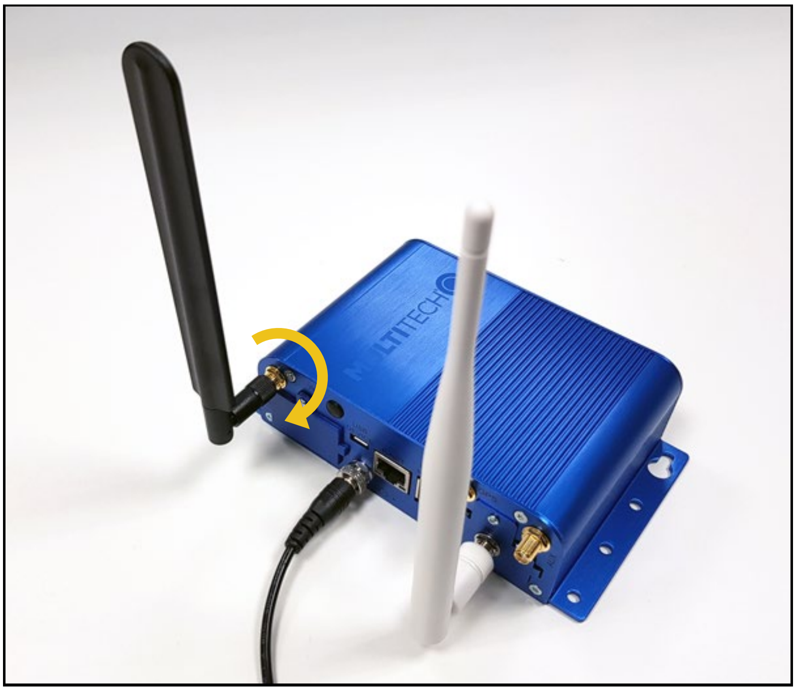


Figure 22 – Fasten the cellular radio antenna (on left)

2. Remove the front cover plate and insert your SIM card in the slot:

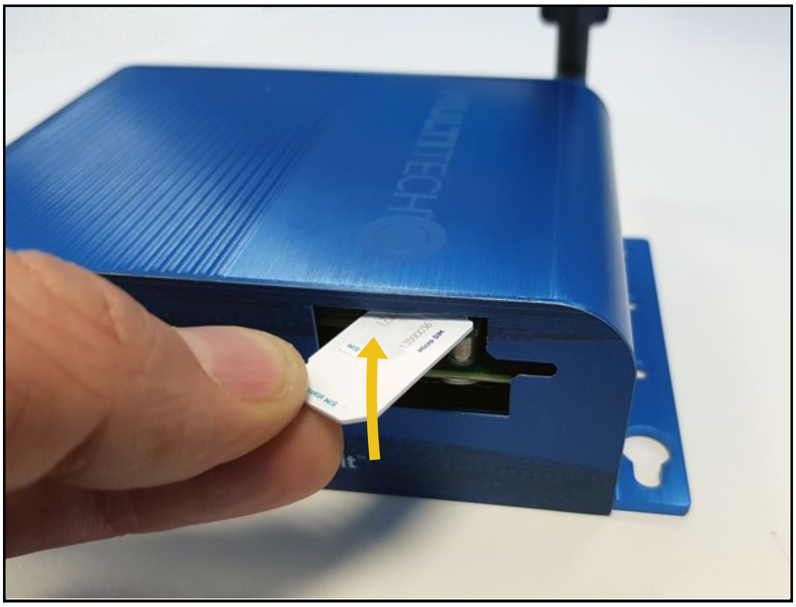


Figure 23 – Insert SIM card completely into slot

2.2.3.2 Inserting micro-SIM card in Pro model

1. The cellular antenna is integrated inside the gateway casing, so you do not need to connect an external antenna.
2. Insert the SIM card completely into the slot on the back of the gateway as shown below. The slot is "keyed", so the SIM card can only be inserted with the cut corner on the left-hand side, facing forward.

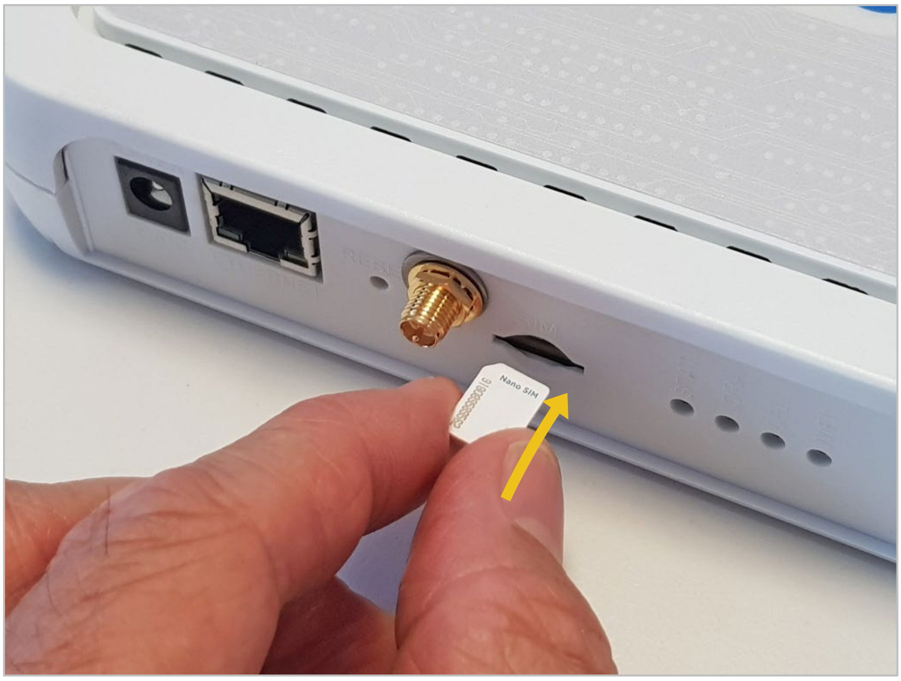
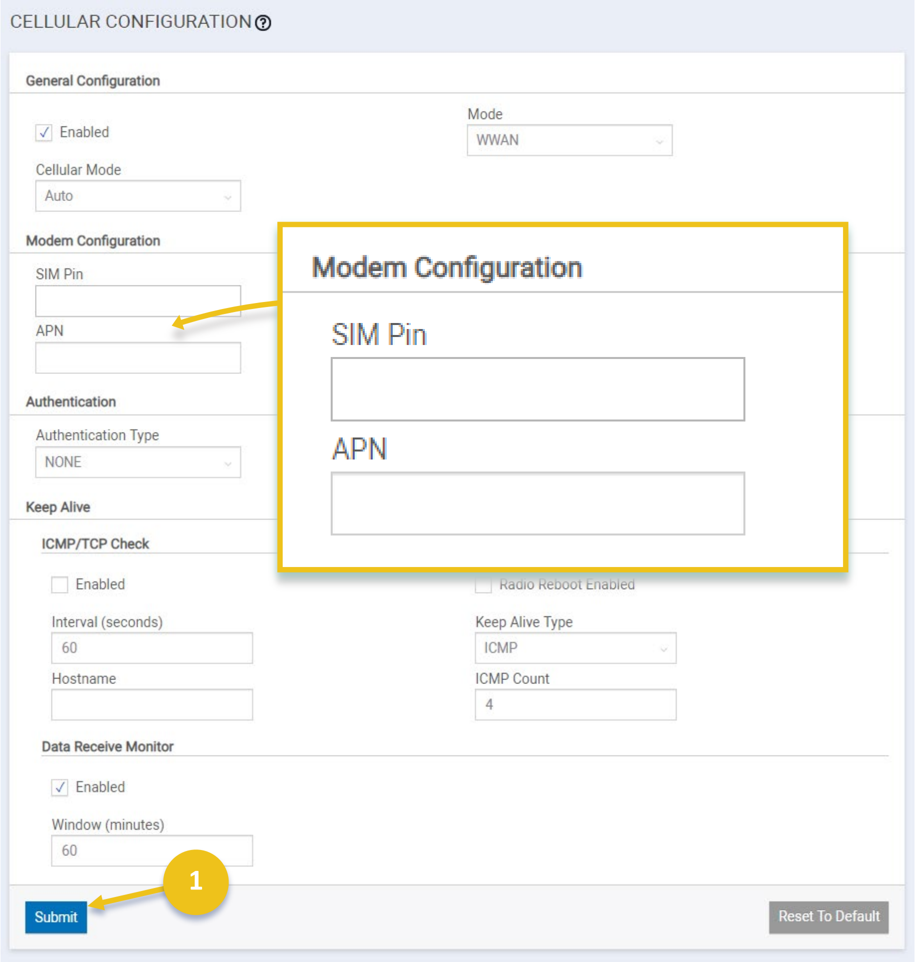


Figure 24 – Insert SIM card completely into slot

2.2.3.3 Software configuration

1. In the administration interface, select **Cellular → Cellular Configuration**:



CELLULAR CONFIGURATION

General Configuration

☑ Enabled

Mode: WWAN

Cellular Mode: Auto

Modem Configuration

SIM Pin:

APN:

Authentication

Authentication Type: NONE

Keep Alive

ICMP/TCP Check

□ Enabled

□ Radio Reboot Enabled

Interval (seconds): 60

Keep Alive Type: ICMP

Hostname:

ICMP Count: 4

Data Receive Monitor

☑ Enabled

Window (minutes): 60

Figure 25 – Edit SIM Pin and APN fields for cellular communications

2. In this screen, the only fields you should need to edit are:

   SIM Pin If necessary, enter the PIN number to unlock access to your SIM card. Many data-only (Internet of Things) solutions do not require a SIM code.

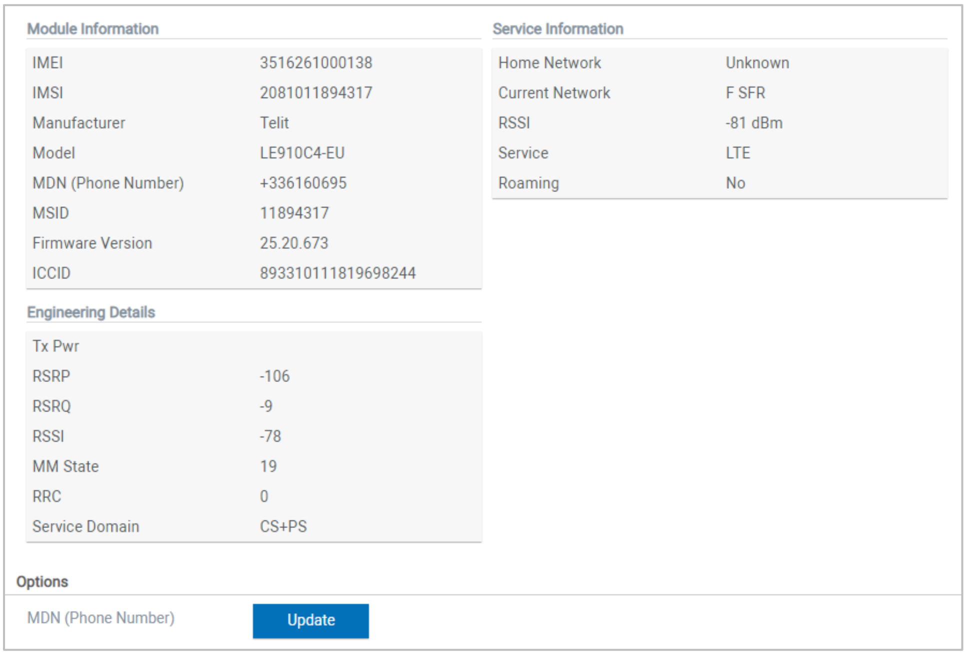
   APN Enter the code provided by your cellular service provider.

   All other fields may be left with their default values.

3. Click on **Submit** (1) to save your settings.
4. If this is the only change you are making to your configuration, click on **Save and Apply**.

   Otherwise, we recommend waiting until you have made all your changes and do a global **Save and Apply** when you are done (or **Save and Restart** depending on the settings you changed). The process takes several minutes and there is no reason to launch it multiple times.

5. You may check the gateway's cellular status by clicking on **Cellular → Radio Status**:



Module Information

IMEI	3516261000138
IMSI	2081011894317
Manufacturer	Telit
Model	LE910C4-EU
MDN (Phone Number)	+336160695
MSID	11894317
Firmware Version	25.20.673
ICCID	893310111819698244

Service Information

Home Network	Unknown
Current Network	F SFR
RSSI	-81 dBm
Service	LTE
Roaming	No

Engineering Details

Tx Pwr	
RSRP	-106
RSRQ	-9
RSSI	-78
MM State	19
RRC	0
Service Domain	CS+PS

Options

MDN (Phone Number)

Figure 26 – Checking cellular communication status

2.3 Configuring “failover” order for network access

If you have more than one Internet connectivity option installed in your gateway, the gateway can switch from one to another in case of failure.

As a reminder:

- The Advanced model supports Ethernet, WiFi, and 4G/cellular
- The Pro model supports Ethernet and 4G/cellular

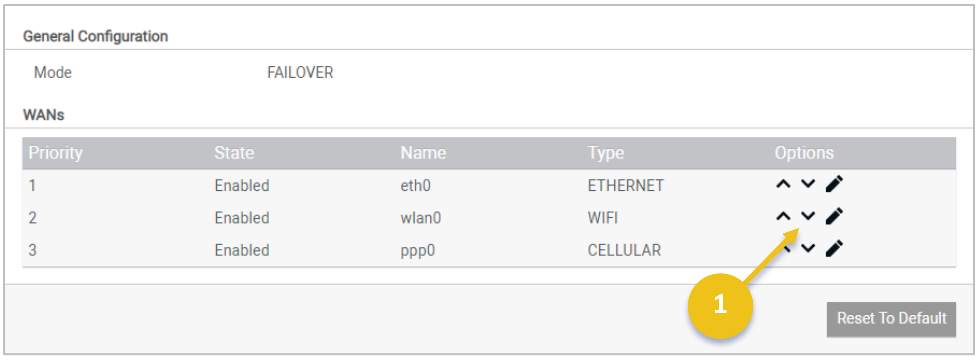
Connectivity options are specified at the time of purchase.

For example, if you choose to run Ethernet as your primary connection and the connection fails at some point, you could backup the communication channel by also configuring the optional cellular data connection as described below:

1. Click on **Setup ➔ WAN Configuration**

   The list below shows the priority order in which connectivity options are used. In the case below, Ethernet is used as the priority connection. The gateway would switch automatically to WiFi if communication via Ethernet fails, and then cellular data if WiFi fails.

2. Click on the up/down arrows (1) to change network priority order.



General Configuration

Mode FAILOVER

WANs

Priority	State	Name	Type	Options
1	Enabled	eth0	ETHERNET	^ ˅ ✎
2	Enabled	wlan0	WIFI	^ ˅ ✎
3	Enabled	ppp0	CELLULAR	^ ˅ ✎

Figure 27 – Determine network “failover” order

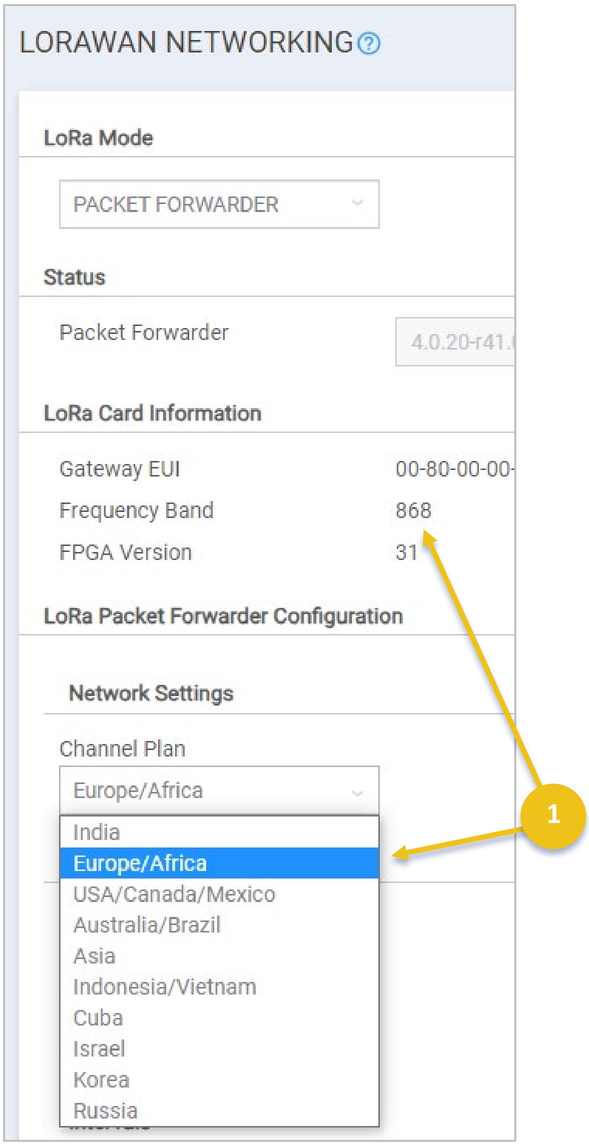
2.4 LoRaWAN configuration

After configuring your gateway's TCP/IP network settings (Ethernet, Wi-Fi, or cellular), the next step is to set up and verify LoRaWAN networking settings.

2.4.1 Regional frequency

Select your geographical region, which automatically assigns the correct wireless frequency for communications:

1. Login to the gateway as described in the previous section.
2. Select **LoRaWAN® ➔ Network settings**
3. Click on the **Channel Plan** drop down menu (1) and select the appropriate region.



LORAWAN NETWORKING

LoRa Mode

PACKET FORWARDER

Status

Packet Forwarder 4.0.20-r41.

LoRa Card Information

Gateway EUI 00-80-00-00-

Frequency Band 868

FPGA Version 31

LoRa Packet Forwarder Configuration

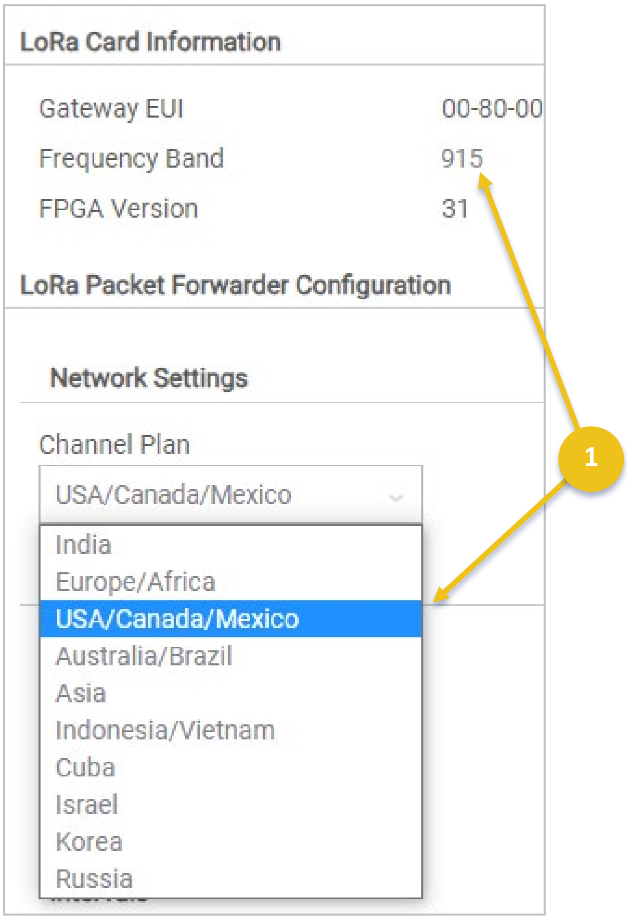
Network Settings

Channel Plan: Europe/Africa

Figure 28 – Choose the option that matches your region's frequency band

On this screen you only need to make sure that the Channel Plan value corresponds to your gateway hardware and geographical region. You may leave all other fields with their default values.

Here is an example for a 915 MHz LoRaWAN radio:



LoRa Card Information

Gateway EUI	00-80-00
Frequency Band	915
FPGA Version	31

LoRa Packet Forwarder Configuration

Network Settings

Channel Plan: USA/Canada/Mexico

Figure 29 – Example of a Channel Plan using 915 MHz

Note regarding the FPGA version:

The FPGA version in your gateway is set at the factory based on the region in which you intend to use it. The version is either 31 or 35.

- **FPGA Version 31**: India, Europe, Africa, Russia
- **FPGA Version 35**: USA, Canada, Mexico, Australia, Brazil, Asia, Indonesia/Vietnam, Cuba, Israel, Korea

  If you want to use your gateway in one of these regions, and the FGPA version is not correct, click on **Upgrade** to change the version, or contact Dickson Technical Support.

4. Click on **Submit** when done to save your changes.

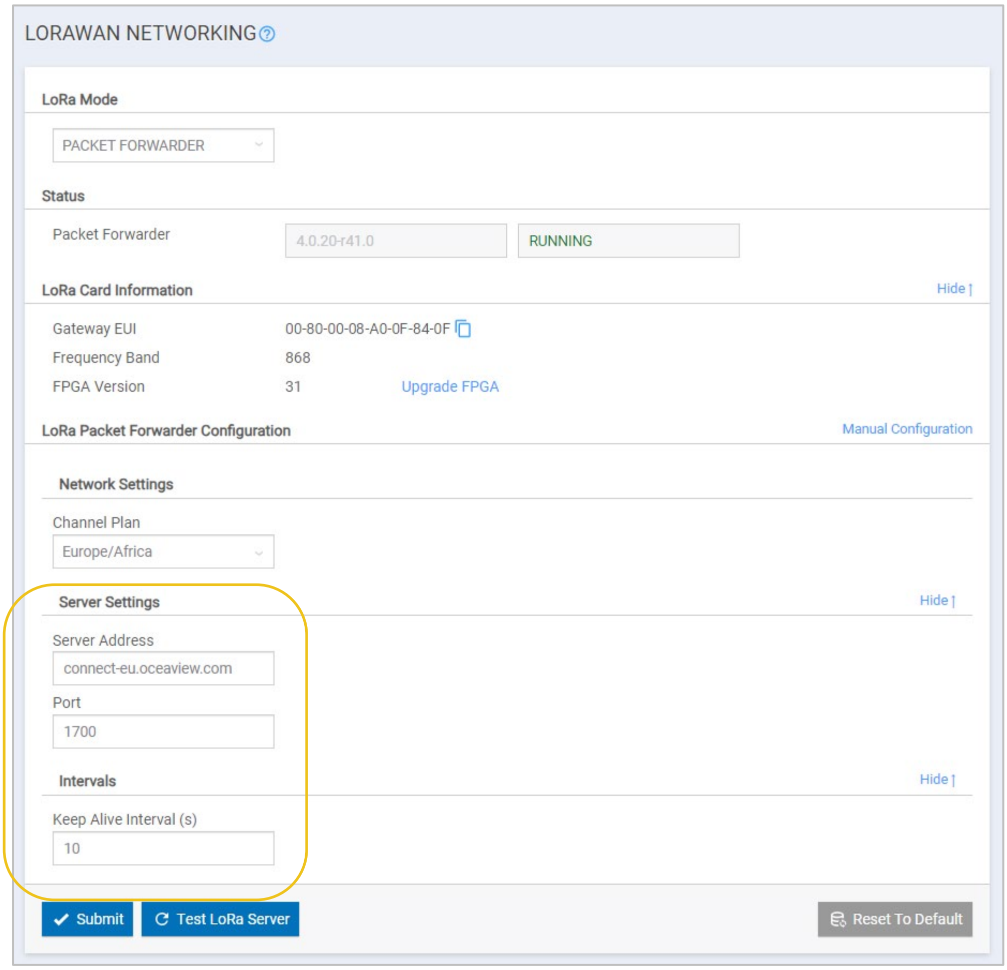
5. If this is the only change you are making to your configuration, click on **Save and Apply**.

Otherwise, we recommend waiting until you have made all your changes and do a global **Save and Apply** when you are done (or **Save and Restart** depending on the settings you changed). The process takes several minutes and there is no reason to launch it multiple times.

2.4.2 Server connection information

Follow these steps to set how the gateway connects to your OCEAView server.

1. Click on **LoRaWAN (Network Settings)**



LORAWAN NETWORKING

LoRa Mode

PACKET FORWARDER

Status

Packet Forwarder 4.0.20-r41.0 RUNNING

LoRa Card Information

Gateway EUI 00-80-00-08-A0-0F-84-0F

Frequency Band 868

FPGA Version 31

LoRa Packet Forwarder Configuration

Network Settings

Channel Plan: Europe/Africa

Server Settings

Server Address: connect-eu.oceaview.com

Port: 1700

Intervals

Keep Alive Interval (s): 10

Figure 30 – LoRaWAN configuration screen

2. Enter the following (or make sure they are present):
   - **Keep Alive Interval**:
     - If you are using 4G connectivity, set this to **1** second
     - If you are not using 4G connectivity, set this to **10** seconds
   - **Port** (up & down): 1700

For OCEAView Cloud platform

- Server Address: enter the URL that corresponds to your geographic region:
  Americas: **connect-us.oceaview.com**
  Europe: **connect-eu.oceaview.com**
  Asia: **connect-asia.oceaview.com**

For OCEAView On-premises platform

- Enter the domain name or IP address of your OCEAView server

---

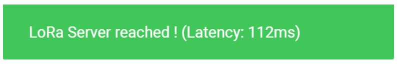
If you enter a domain name rather than an IP address, the DHCP client in the gateway must be able to resolve the name to connect to the Internet.

2.5 Finalizing your configuration

1. Assuming your gateway is correctly connected to the network (as described in the previous sections), you may click on the Test LoRa Server button in the lower right-hand corner to verify the connection between the gateway and the OCEAView platform. This function only works if your network is configured properly.

Your gateway must have a reasonably fast Internet connection to operate correctly and avoid communication errors.

The Test LoRa Server function must show a maximum latency time of 200 ms. The latency is indicated on the screen as shown here:



LoRa Server reached ! (Latency: 112ms)

If the latency value is higher than 200 ms, please check with your IT department to increase speed for the gateway.

---

2. When the test has succeeded, click on **Submit** to apply your changes
3. You must restart gateway services for settings to be saved. Click on **Save and Apply** in the menu on the left-hand side of the screen (or **Save and Restart**) to complete configuration. This process takes several minutes.
4. Once the services are restarted, LoRaWAN networking status is updated.

3 Troubleshooting

If you are having difficulties with your configuration, look at these frequently asked questions before contacting technical support.

How can I test my LoRaWAN network connection?

In the **Setup ➔ LoRa** window, there is a **Test LoRa Server** button. When you click on that button, you should receive acknowledgment that the connection is up and running.

> ❗ The latency indicated by this function must not be higher than 200 ms.

I would like to see how well LoRaWAN wireless coverage works at my site. Is there an easy way to perform tests?

You may test the wireless connection between your gateway and a Dickson LoRaWAN module as described in the module User Guide. For more information, or to conduct a more complete site survey, please contact your Dickson representative.

I want to use my gateway with a cellular data connection. I think I have done everything correctly, but the gateway does not seem to be able to obtain an IP from the network.

Connect to the gateway interface with your login name and password, then select **Cellular ➔ Wake up on call** in the left-hand menu. Remove the Init String “AT+WS46=28”.

I’d like to test LoRaWAN wireless coverage at my site. The gateway is in place, but I don’t want to use it on the Internet yet, just LoRaWAN to check coverage. Is that possible?

There is an auto-acknowledgment wireless testing feature in recent X2 data logger firmware. If you want to test on-site coverage without an Internet connection (that is, just the LoRaWAN part), you may configure the X2 data logger as follows: select **Menu ➔ Advanced ➔ LoRaWAN ➔ Network ➔ Customer.** Select the region and enter this 8-digit number via the keypad: “00000000”. On the LoRaWAN gateway, click on **LoRaWAN (Network Settings),** change the “Server Address” to 127.0.0.1, then click on Submit ➔ Restart LoRa Services. You may then use the **Range test** feature on the X2 data logger to test LoRaWAN connectivity with your gateway.

I forgot my gateway's IP address or username/password and cannot connect to the administrator interface. Is there a way to restore factory settings?

The Dickson LoRaWAN gateways both have a reset button that can be pressed to restore factory settings. For example, you may choose to do this if you have forgotten the IP address you entered in network configuration, or if you forgot the username/password and can no longer connect to the administration interface.

To perform a factory reset:

1. Insert a blunt tool (such as a paper clip) to press and hold the button recessed inside the "Reset" hole.
2. Continue holding the button for over 30 seconds, at which point the LEDs light up again.
3. Release the button and wait while the gateway reboots.
4. You may then connect to the gateway using the default settings (and default IP address).

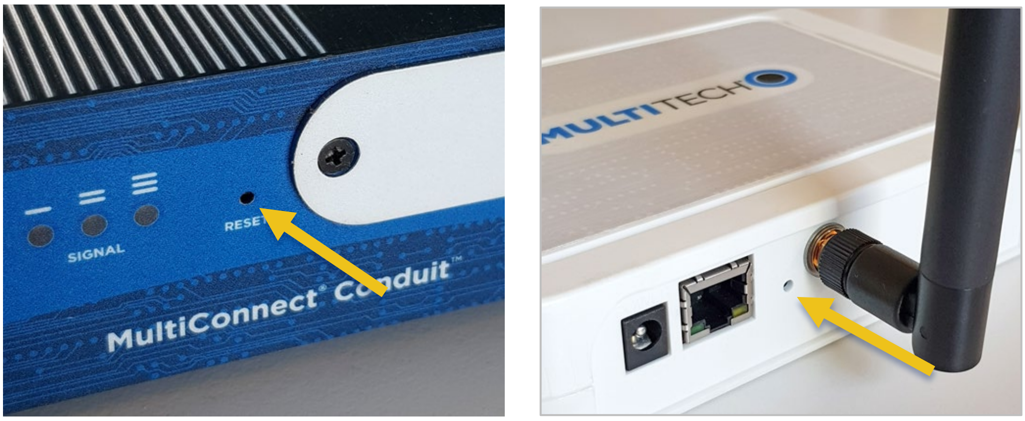


Figure 31 – Restoring LoRaWAN gateway factory settings

4 Firmware upgrade from version 1.4.17 to 6.x.x or higher

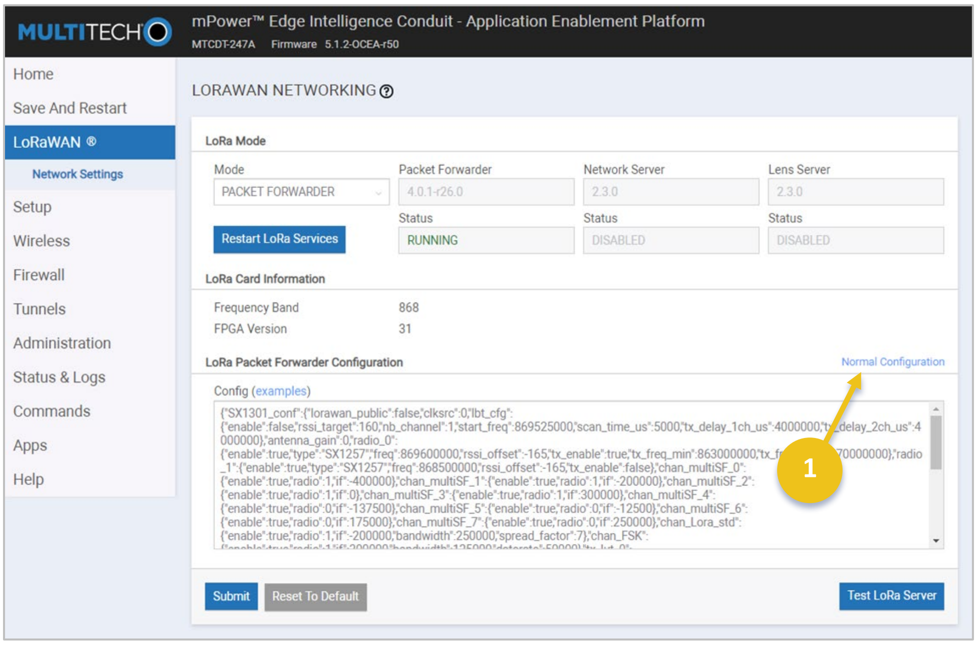
This section provides specific information when upgrading your gateway's firmware from version 1.4.17 to version 6.x.x or higher.

To upgrade the firmware in your gateway, typically following notification from Dickson or contact with our technical support team, follow these steps:

1. Connect to your gateway with your login name and password.
2. Select **Administration ➔ Firmware upgrade**
3. Select **Choose Firmware Upgrade File** and browse your computer to locate the firmware file provided to you by Dickson.

> ! Only use official firmware files provided by Dickson. Never install firmware that you may find elsewhere on the web.

4. Select **Start upgrade** and continue the process as directed on the screen.
5. When upgrading from 1.x.x firmware, this process resets your previous LoRaWAN configuration. You must then click on **LoRaWAN** in the main menu, then click on the **Normal Configuration** link (1) on the right-hand side of the screen to open **Manual Configuration**.



MTCDT-247A Firmware 5.1.2-OCEA-r50

LoRa Mode

Mode	Packet Forwarder	Network Server	Lens Server
PACKET FORWARDER	4.0.1-r26.0	2.3.0	2.3.0
	Status	Status	Status
	RUNNING	DISABLED	DISABLED

LoRa Card Information

Frequency Band	868
FPGA Version	31

LoRa Packet Forwarder Configuration

```
{"SX1301_conf":{"lorawan_public":false,"clksrc":0,"lbt_cfg":
{"enable":false,"rssi_target":160,"nb_channel":1,"start_freq":869525000,"scan_time_us":5000,"tx_delay_1ch_us":4000000,"t[illegible]delay_2ch_us":4
000000},"antenna_gain":0,"radio_0":
{"enable":true,"type":"SX1257","freq":869600000,"rssi_offset":-165,"tx_enable":true,"tx_freq_min":863000000,"tx_f[illegible]70000000},"radio
_1":{"enable":true,"type":"SX1257","freq":868500000,"rssi_offset":-165,"tx_enable":false},"chan_multiSF_0":
{"enable":true,"radio":1,"if":-400000},"chan_multiSF_1":{"enable":true,"radio":1,"if":-200000},"chan_multiSF_2":
{"enable":true,"radio":1,"if":0},"chan_multiSF_3":{"enable":true,"radio":1,"if":300000},"chan_multiSF_4":
{"enable":true,"radio":0,"if":-137500},"chan_multiSF_5":{"enable":true,"radio":0,"if":-12500},"chan_multiSF_6":
{"enable":true,"radio":0,"if":175000},"chan_multiSF_7":{"enable":true,"radio":0,"if":250000},"chan_Lora_std":
{"enable":true,"radio":1,"if":-200000,"bandwidth":250000,"spread_factor":7},"chan_FSK":
```

6. You may then proceed with LoRaWAN configuration as described earlier. This specific behavior is caused by the migration from firmware 1.x.x to a higher version. After this upgrade, you should not have to perform the same procedure again in the future.

DICKSON

Environmental Monitoring + Compliance Experts

Dickson North America
Addison, IL - USA

+1 (630) 543-3747
contact@dicksondata.com

Dickson Europe
Montpellier - France

+33 (0)4 99 13 67 30
contact@dicksondata.fr

Dickson Asia
Petaling Jaya - Malaysia

+6019 880 6438
lcrepin@dicksondata.fr

www.dicksondata.com