



## USER GUIDE

# JRI LoRA GATEWAY



Products N°12706-12707-12708-12709-13191





## TABLE OF CONTENTS

1.	DESCRIPTION.....	1
1.1.	Important information .....	1
1.2.	Regulatory and Environmental information.....	2
1.3.	Product content.....	2
2.	INSTALLATION RECOMMENDATIONS .....	3
2.1.	Sources of attenuation and disturbances.....	3
2.2.	Positioning .....	3
3.	HARDWARE DESCRIPTION .....	4
4.	TECHNICAL PREREQUISITES .....	5
4.1.	General: .....	5
4.2.	DHCP mode:.....	5
4.3.	Fixed IP mode: .....	5
5.	CONFIGURATION .....	5
5.1.	Start and login on the configuration portal:.....	5
5.2.	IP Configuration .....	8
5.3.	WAN Failover Priority .....	9
5.4.	Cellular configuration .....	10
5.5.	Date and time: (To be modified only if ≠ from the PC time):.....	11
5.6.	Check the Configuration Access parameters:.....	<b>Erreur ! Signet non défini.</b>
5.7.	LoRaWAN Parameters (SF and Packet Forwarder mode configuration).....	11
5.8.	Save changes and restart.....	13
6.	RESTART AND RESTORE CONFIGURATION .....	13
7.	NODE RED CONFIGURATION FOR MYSIRIUS SERVER USE .....	14
8.	ADD THE GATEWAY IN MYSIRIUS .....	17

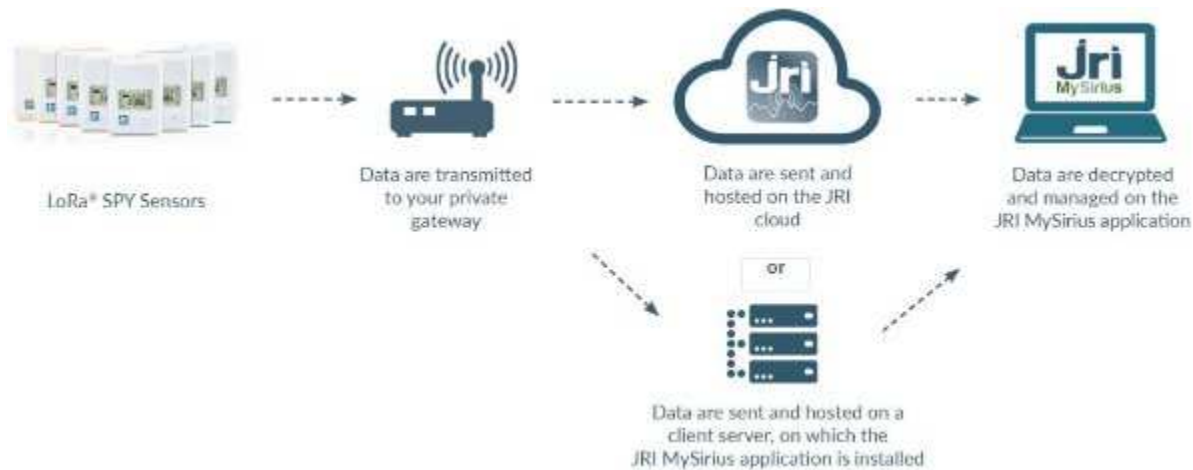


## 1. DESCRIPTION

This document describes the installation procedure and utilization of the JRI LoRa Gateways.

### 1.1. Important information

The JRI LoRa gateways default configuration ensures communication between JRI LoRa devices (LoRa SPYs, LoRa Temp's) and JRI-MySirius Cloud. For a use with MySirius Server version, a modification is required in the built-in NodeRed server [\(see part 7\)](#).






- **NEVER CONNECT A NEW GATEWAY ON A CUSTOMER'S ETHERNET NETWORK WITH A DHCP SERVER IF IT IS MEANT TO BE USED IN FIXED IP MODE.**
- LORA GATEWAYS ARE CONFIGURED BY DEFAULT IN DHCP; A RESERVATION OF AN IP ADDRESS CAN BE MADE BY PROVIDING THE GATEWAY'S MAC ADDRESS. (SEE BACKSIDE STICKER)



- **TO SWITCH TO FIXED IP MODE, DO A SHORT RESET OF 10 SECONDS (>5 SEC AND <30 SEC) AND SEE [STEP 5.2](#). NEVER DO A HARD RESET > 30 SEC (FACTORY RESET).**
- CONNECTING A JRI LORA GATEWAY TO THE CUSTOMER'S NETWORK ALLOWS REMOTE MANAGEMENT OF THE GATEWAY THROUGH ITS CONFIGURATION PORTAL. FOR THE ETHERNET VERSION, IT IS THE MEDIUM OF DATA COMMUNICATION, WHEREAS THE 4G VERSION USES THE ETHERNET NETWORK FOR COMMUNICATION BUT CAN SWITCH TO THE CELLULAR NETWORK IN CASE OF ETHERNET NETWORK FAILURE.

## 1.2. Regulatory and Environmental information

	Do not dispose of with other waste. Instead, hand it over to a designated collection point for the recycling of waste electrical and electronic equipment. The separate collection and recycling of your waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment.
	Compliant with European Council Directives 2011/65/EU and 2014/53/EU for electrical safety, flammability, disruptive electromagnetic emissions, and immunity to environmental electrical disturbances.
<b>RoHS</b>	Embedded products comply with the chemical concentration limitations set forth in the directive 2015/863 of the European Parliament (Restriction of the use of certain Hazardous Substances in electrical and electronic equipment - RoHS). This product does not contain the banned chemicals.
	This device complies with part 15 of the FCC rules. Operation is subject to conditions. Contact us for more details. The grantee is not responsible for any changes or modification not expressly approved by the party responsible for compliance. The antenna(s) used for this transmitter, must be installed to provide a separation distance of at least 20 cm from all persons. Installers and end-users must be provided with operating conditions for satisfying RF exposure compliance.

## 1.3. Product content

- JRI LoRa Gateway
- LoRa Antenna 20 cm 3db. Can be replaced by Outdoor antenna 8db 1m20 with 10 m extension cable (see product 12524)
- Power supply
- Ethernet cable
- Mounting bracket

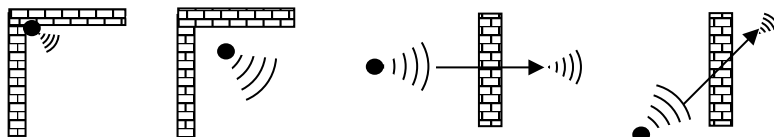


## 2. INSTALLATION RECOMMENDATIONS

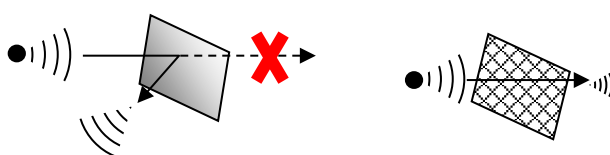
To ensure optimal radio transmission, a certain number of recommendations must be respected, as any wireless transmission is subject to disturbances.

### 2.1. Sources of attenuation and disturbances

- The presence of obstacles between the LoRa recorders and the LoRa Gateway (wall, furniture, vehicles...) or near the antenna.
- The thickness of an obstacle. The attenuation is greater diagonally than perpendicularly.

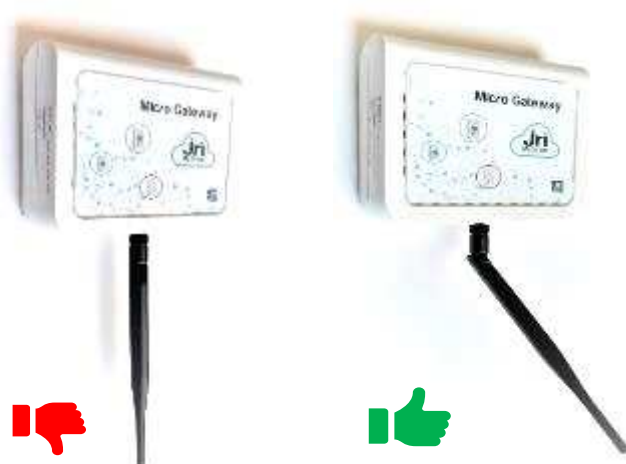


- A solid metal wall without any openings will not allow transmission by radio. Small openings in the wall will attenuate the signal. Recommended size of openings is 35cm minimum.



### 2.2. Positioning

- Position the Gateway's LoRa antenna at 45° degrees from the wall (avoid being in parallel). Place the Gateway in a high and central position according to the distribution of LoRa SPYs sensors. A LoRa SPY TEST (Ref: 12146/12308) can be used to determine the gateway's best location onsite.



- A large external antenna with 8dB gain (ref 12524) can be installed instead of the antenna provided by default. A cable of 10m long can be used for remote installation.



- Use the mounting bracket provided for an easier installation.



To ensure your safety during installation or an intervention on a device placed in a high position, use proper equipment which provides adequate stability, wear appropriate non-slip shoes and install warning signs around the work area if the intervention takes place in an area of foot traffic.

### 3. HARDWARE DESCRIPTION



The above image shows the model with all features (ETHERNET and Cellular). For models that don't have a cellular radio, the chassis will not have a SIM slot.

Item	Description
<b>Connectors</b>	
Power	5 Volt power jack.
Ethernet	RJ45 Ethernet jack.
Reset	Reset button. Reboots device or restores factory defaults. see Resetting the Device P.1
LoRa antenna	Connect external 3db LoRa antenna or extension cable for 8db LoRa antenna
SIM	<i>Cellular models only.</i> SIM slot. Refer to <i>Installing SIM Card</i> for details.
<b>LEDs</b>	
STATUS	Blinks when operating system is fully loaded.
LORA	Lights when LoRa software (node Red) is active.
CELL	<i>Cellular models only.</i> Lights when there is power to the radio. Blinks when the SIM is registered with the carrier.
Ethernet Link	Left LED on the Ethernet connector. Blinks when data is sent or received on the Ethernet link. Steady light when there is a valid Ethernet connection.
Ethernet Speed	Right LED on the Ethernet connector. Lit when the Ethernet is linked at 100 Mbps. If not lit, the Ethernet is linked at 10 Mbps.

## 4. TECHNICAL PREREQUISITES

### 4.1. General:

- A 220V electrical outlet is required within 1.5m from the Gateway location
- 4G cellular coverage or RJ45 network socket depending on the Gateway chosen.
- For MySirius CLOUD use: Open TCP port **8443** to [device.jri-mysirius.com](https://device.jri-mysirius.com) platform.
- For MySirius SERVUR use: Open TCP port **13252** to the IP address of the MySirius server.
- For remote management: Open TCP **5798** port to [ds.devicehq.com](https://ds.devicehq.com) platform.



**CAUTION:** Depending on the generation of the Gateway, some are still configured to work on port **13252** in classic **HTTP**, and not on port **8443** which is the **HTTPS** port. JRI strongly recommends to switch the configuration for MySirius CLOUD to **HTTPS** only (port 8443 - see chapter on NodeRED Configuration)

### 4.2. DHCP mode:

It is recommended to set Gateways in DHCP (default configuration). A DHCP server is required for an automated IP configuration but it is mandatory to know the IP address that will be allocated to the Gateway for future modification. Otherwise, the Gateway IP address is only recoverable from [www.devicehq.com](https://www.devicehq.com).

### 4.3. Fixed IP mode:

For a fixed IP usage, the user should provide the information below:

- IP address
- Subnetwork mask
- Gateway
- DNS

## 5. CONFIGURATION

### 5.1. Start and login on the configuration portal:

#### DHCP configuration:

- Power the Gateway.
- Connect the Gateway on a customer network with a DHCP server (Request a reservation of an IP address by providing the Gateway MAC address - backside label).
- Open an internet browser at the GATEWAY IP address.
- In the login page that appears, provide the following default credentials:
  - **User name:** admin
  - **Password:** Admin1234. (Password is "admin" for former versions)

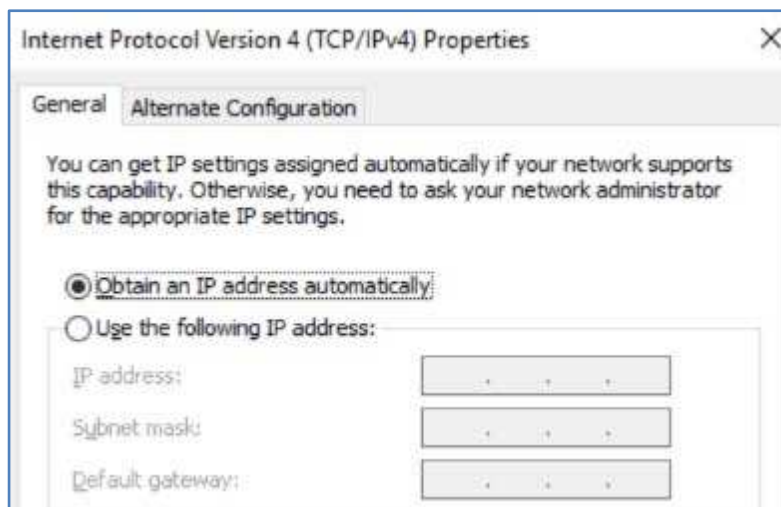
Depending on the Gateway version, access customization may be requested.

#### FIXED IP configuration (if the IP address has not been configured by JRI):

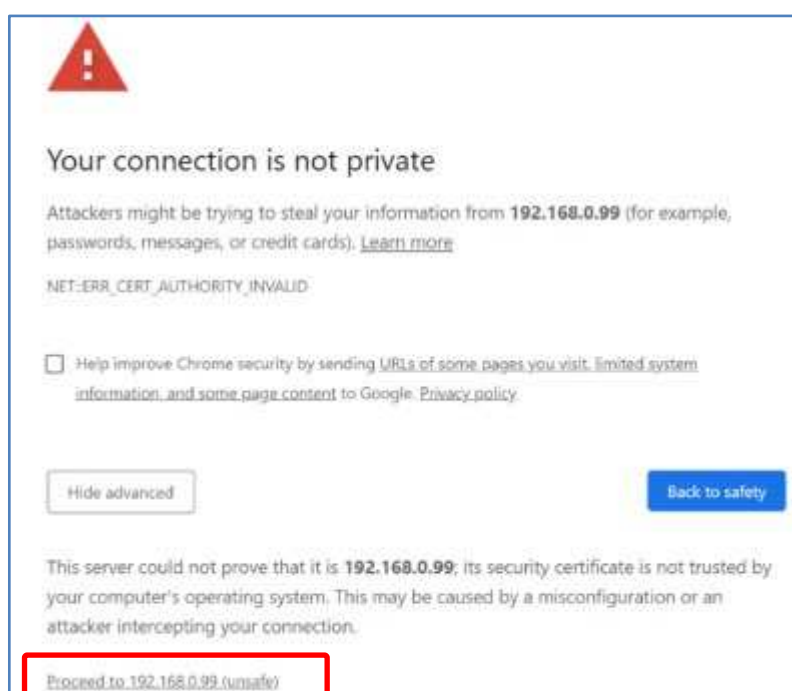
- Power the Gateway.
- Wait for the Gateway to completely start: LoRa LED is steady / STATUS LED is blinking.
- Remove the sticker on the RESET button and press for 10 seconds with a paperclip.
- Wait for the full reboot of the Gateway: LoRa LED is steady / STATUS LED is blinking.



- Set the PC network adapter to automatic mode (Disconnect the PC from Ethernet or Wifi network)



- Connect the Gateway to the PC using the Ethernet cable (disable the Firewall or antivirus if necessary).
- Open an internet browser and enter the address <http://192.168.2.1>



- If a security message appears (depending on the browser) Click on more details and continue to the site 192.168.2.1





- In the login page, enter the following default credentials:

- **User name** : admin
  - **Password** : Admin1234.
- Click on **Login**

The login page features the MULTITECH logo at the top, followed by the product name 'mPower™ Edge Intelligence Conduit AP'. Below this, there are two input fields: 'Username' and 'Password'. A 'Login' button is positioned to the right of the password field.

- After connection, the configuration page below opens.
- The left menu gives access to the different configuration panels.

The configuration page displays the MULTITECH logo and the product name 'mPower™ Edge Intelligence Conduit AP - Application Enablement Platform'. The user is logged in as 'admin as administrator'. The page is divided into a left sidebar menu and a main content area.

**Left Sidebar Menu:**

- Home
- Save And Restart
- LoRaWAN ®
- Setup
- Firewall
- Tunnels
- Administration
- Status & Logs
- Commands
- Apps
- Help

**DEVICE INFORMATION**

Device	
Model Number	MTCAP-868-001A
Serial Number	19791620
Firmware	5.0.0-AEP
Current Time	03/04/2020 11:10:34
Up Time	7 days 21:45:26
WAN Transport	None
Current DNS	192.168.0.239, 192.168.4.239

**LAN**

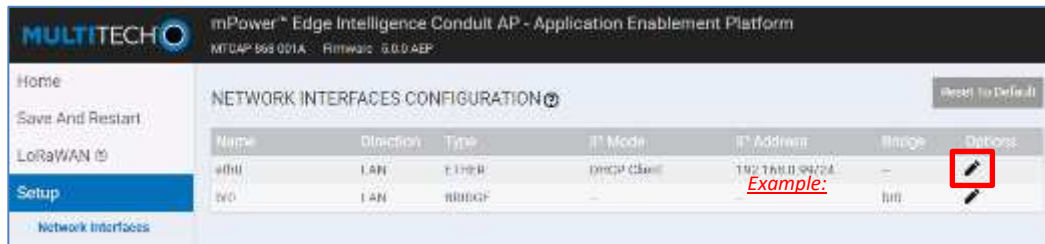
Bridge (br0)	
MAC Address	
IPv4 Address	
Mask	255.255.255.0
DHCP State	Disabled
Interfaces	

Ethernet (eth0)	
Mode	DHCP Client
Bridge	-
MAC Address	00:08:00:4A:58:2E
IPv4 Address	192.168.0.99
Mask	255.255.255.0
DHCP State	Disabled
Lease Range	192.168.2.100-192.168.2.150

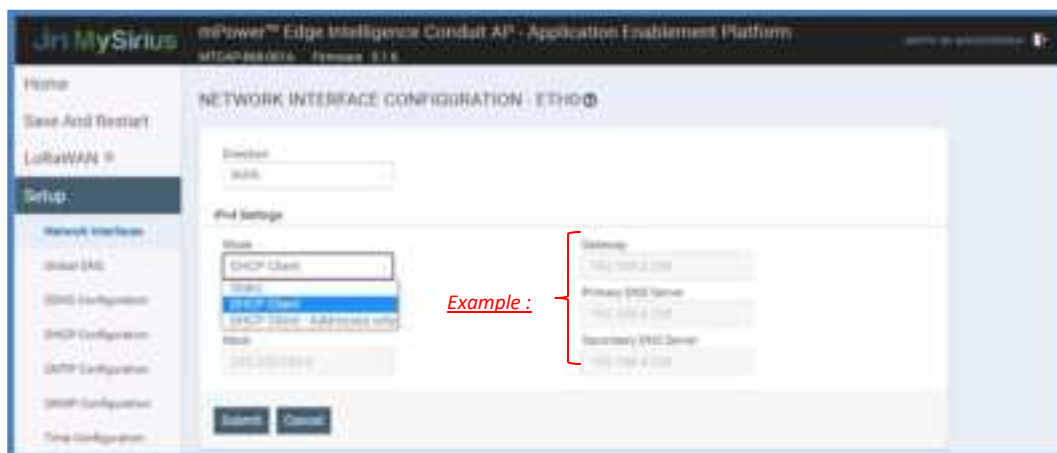


## 5.2. IP Configuration

- Setup Menu > Network Interfaces.
- Click on the pencil in the Options column to modify "eth0".



- Fill in the fields according to the desired configuration:
  - Let direction on LAN for default Ethernet configuration and select WAN for Ethernet with cellular failover utilization
  - Select DHCP client (default) for dynamic IP configuration
  - Or select Static IP for fixed IP configuration and enter the IP/Mask/Gateway/DNS information.
- Click on "submit"




To connect to the Gateway configuration page again, enter its new IP address in the browser if it has been modified (fixed IP given by the client or IP allocated by the client's DHCP server).

### 5.3. WAN Failover Priority

Failover mode regulates which medium (Ethernet or Cellular) is used for the Internet connection and switches from one to another if a connectivity failure is detected. Priority can be set either on Ethernet or Cellular connection.

If Ethernet connection (eth0) is set as priority 1 by default, cellular connection can be set as a failover connection by setting its priority to 2. Both connections should be set as WAN.

- Click Setup > WAN Configuration.
- Under Options, click the up and down arrows to change the priority of the appropriate connection.
- Click Save and Apply to save the change.



**WAN CONFIGURATION**

General Configuration

Mode: **FAILOVER**

WANS:

Priority	Status	Name	Type	Options
1	Enabled	ppp0	CELLULAR	⬆ ⬇ ⬆
2	Enabled	eth0	ETHERNET	⬆ ⬇ ⬆

Reset To Default

To edit failover configuration:

- Under the Options column at the right, click the pencil icon (edit) for the selected WAN. The Failover Configuration page is displayed.
- Make the desired changes. Refer to Failover Configuration Fields for details.
- Click Finish.



**FAILOVER CONFIGURATION**

Monitoring Mode: **ACTIVE**

Interval (secs): **60**

Hostname: **www.google.com**

Mode Type: **ICMP**

ICMP Count: **10**

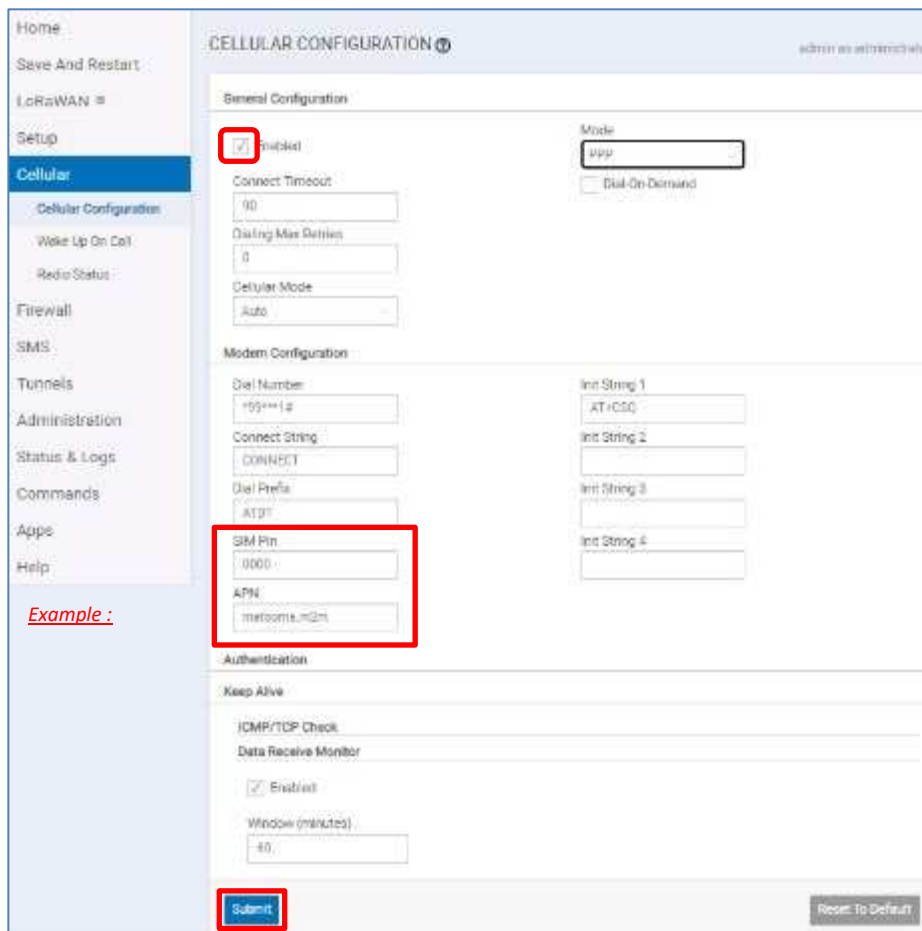
Save Cancel



**CAUTION:** To detect network availability (Ethernet or 4G) and thus be able to switch from one connection mode to another, the Gateway needs to send a ping or an ICMP frame to an address (by default [www.google.fr](http://www.google.fr)). You must ensure that this address is accessible to the Gateway.

## 5.4. Cellular configuration

- Insert a micro SIM card before starting the Gateway.
- Use Machine to Machine sim cards with data connection service of minimum 5Mb/month for small installations (ex: 10 monitored units with default JRI configuration)
- Go to the Cellular > Cellular Configuration menu.
- In the General Configuration tab, check that the "Enabled" box is checked.
- In the Modem Configuration tab, complete the PIN and APN fields according to the SIM card used.
- Let all other settings with default values and click on «submit».

Home  
Save And Restart  
LoRaWAN  
Setup  
**Cellular**  
Cellular Configuration  
Wake Up On Cell  
Radio Status  
Firewall  
SMS  
Tunnels  
Administration  
Status & Logs  
Commands  
Apps  
Help

*Example :*

**CELLULAR CONFIGURATION**

General Configuration

☒ Enabled

Mode  
app  
Dial-On Demand

Connect Timeout  
90

Dialing Max Retries  
0

Cellular Mode  
Auto

Modem Configuration

Dial Number  
+554412

Connect String  
CONNECT

Dial Prefix  
ATDT

SIM Pin  
0000

APN  
m2mcom.m2m

Init String 1  
AT+CSQ

Init String 2

Init String 3

Init String 4

Authentication

Keep Alive

ICMP/TCP Check

Data Receive Monitor

☒ Enabled

Window (minutes)  
-60

Submit

Reset To Default



According to the SIM card provider chosen and the coverage level, the connection to the cellular network can take up to 1h30. In optimized conditions, this process is done within 15 minutes.



## 5.5. Date and time: (To be modified only if ≠ from the PC time):

- Setup menu > Time: choose UTC > then submit.

Home  
Save And Restart  
LoRaWAN ®  
**Setup**  
Network Interfaces  
WAN Configuration  
Global DNS  
DDNS Configuration  
DHCP Configuration  
SMTP Configuration  
SNMP Configuration  
**Time Configuration**  
Cellular  
Firewall  
SMS  
Tunnels  
Administration  
Status & Logs  
Commands

### TIME CONFIGURATION ⓘ

admin as administrator

Settings

Current Date and Time: 11/24/2020 17:37:18 (Europe/Paris)

Date  
MM/DD/YYYY

Time  
HH:MM

Time Zone  
Europe/Paris

SNTP Configuration

☒ Enabled

Polling Time (5 to 1440 minutes)  
120

Server  
time.nist.gov

Backup Server 1  
Backup Server 2  
Backup Server 3  
Backup Server 4

Submit Reset To Default

## 5.6. LoRaWAN Parameters (SF and Packet Forwarder mode configuration)

- JRI recommends to set the SF between 9 and 12 for the 868MHz version (12706/12707) to optimize radio communications: → Lora WAN Menu → Network Settings → Settings → change the value of the Max Data rate to 3 (SF9). Minimum Data rate is set by default to 0 (SF12). For the 915MHz version, the default values of SF are set from 7 to 10.

Settings

Tx Power (dBm)	Rx 1 DR Offset	ADR Step (dB)	Min Datarate
26	0	30	0 - SF12BW125
Antenna Gain (dBi)	Rx 2 Datarate	ACK Timeout	Max Datarate
8	0 - SF12BW125	5000	3 - SF9BW125

- By default, the JRI Gateways are configured as Network servers: Each Gateway uses the built-in Node Red server to communicate with MySirius (Cloud or Server) via TCP port 13252.

Home  
Save And Restart  
LoRaWAN ®  
**Network Settings**  
Key Management  
Gateways

### LORAWAN NETWORKING ⓘ

LoRa Mode

Mode	Packet Forwarder	Network Server
NETWORK SERVER	192.168.0.1	192.168.0.1
Status	Status	
RUNNING	RUNNING	

Restart LoRa Services

It is possible to set the Packet Forwarder mode to send the measurements of LoRa devices from a “slave” Gateway (Packet forwarder) to the “master” Gateway (Network Server) which must always be configured in fixed IP.



→ Administration Menu → LoRaWAN → LoRa mode → select PACKET FORWARDER mode → Restart LoRa services.

Go to the bottom of the page and configure the Gateway Network Server information:

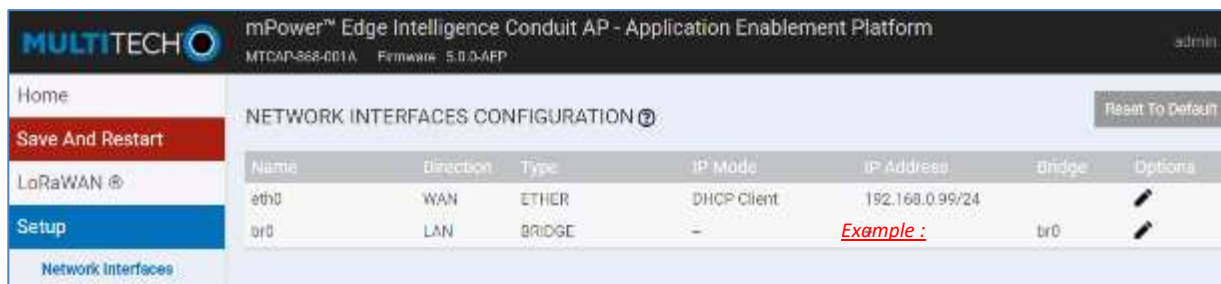
→ Select Network Manual → Enter the IP address of the GateWay Network Server → Save & Restart.

Example :



## 5.7. Save changes and restart

- To save modifications, restart the Gateway by clicking on "Save and Restart" in the menu on the left.



- After restarting, the Gateway can be disconnected from the PC and connected to the customer's network (optional for 4G versions).

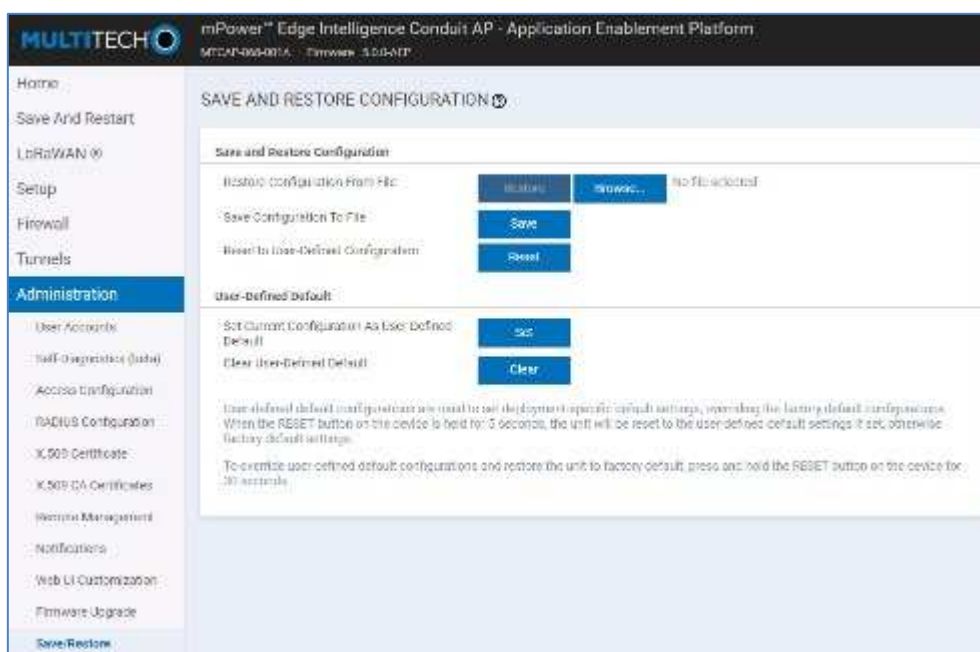


To connect to the Gateway configuration page again, enter its new IP address in the browser if it has been modified (fixed IP given by the client or IP allocated by the client's DHCP server).

## 6. RESTART AND RESTORE CONFIGURATION

- To restart a Gateway: Disconnect then reconnect the power supply or click on Save / Restart
- When the RESET button is pressed for less than 5 seconds, the Gateway can be restarted without losing its entire configuration (Ex: Node Red Server).
- Pressing the RESET button for 10 seconds (>5 sec; < 30 sec) allows you to restore the JRI default configuration.
- It is possible to create your own backup point:

Go to Administration > Save / Restore > User Defined Default > click on Set in the User Defined Default.



A 30 second reset completely removes the configuration of the Gateway and requires general reprogramming by JRI including the configuration of the Node Red server. It is not recommended to do this action.





## 7. NODE RED CONFIGURATION FOR MYSIRIUS SERVER USE

To use a LoRa JRI Gateway with a private server, a modification of the NodeRed embedded software is required.

- When connecting to the GateWay for the first time, access to the NodeRed settings must be enabled via LAN and WAN. Administration Access configuration NodeRed settings

The screenshot shows the 'ACCESS CONFIGURATION' page in the JRI Gateway Administration interface. The left sidebar contains a menu with options: Home, Save And Restart, LoRaWAN, Setup, Firewall, Tunnels, Administration (highlighted), User Accounts, Self-Diagnostics (beta), Access Configuration (highlighted), RADIUS Configuration, X.509 Certificate, X.509 CA Certificates, Remote Management, Notifications, Web UI Customization, and Firmware Upgrade. The main content area is titled 'ACCESS CONFIGURATION' and contains several sections: 'Web Server' with 'HTTP Redirect to HTTPS' (Enabled), 'HTTPS' (Via WAN, Port 443), and 'Authorization' (Session Timeout: 5 minutes); 'HTTPS Security'; 'SSH Settings' (Enabled, Port 22, Via LAN); 'SSH Security'; 'ICMP Settings' (Enabled, Respond to LAN); and 'Node-RED Settings' (Via LAN and Via WAN).

- Connect to the Gateway LoRa interface and go to the Apps section → Launch Node RED

The screenshot shows the 'MANAGE APPS' section of the mPower Edge Intelligence Conduit AP - Application Enablement Platform. The top header indicates 'MTCAP-868-001A Firmware 5.1.6'. The 'MANAGE APPS' section has a 'Launch Node-RED' button. Below this, there are two sections: 'Node-RED Apps' and 'Custom Apps'. In the 'Node-RED Apps' section, the 'Enabled' checkbox is checked. Below this is a table with columns: Name, Version, Status, and Actions. The table contains one entry: 'Development' with version '0.0.0' and status 'Running'. In the 'Custom Apps' section, the 'Enabled' checkbox is also checked, and there is a table with columns: Name, Version, Status, Info, and Actions, which currently shows 'No items found.'

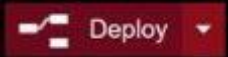



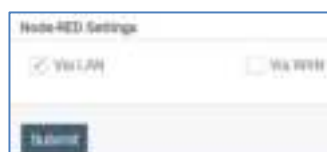
- Connect to the Node-RED interface with the same identifiers used to connect to the configuration page of the Gateway:



- Select SET CONFIG tab → Double click on the “Change MySirius Server URL”.



- Replace the name of the JRI cloud (<https://device.jri-mysirius.com:8443>) by the IP address of the local MySirius server (Example: <http://192.168.0.150:13252>).
- Click on « DONE » to validate the changes and close the window.
- Click on  to apply the modified FLOW.
- When the green "Operation successful" message is displayed, use the button  to apply the changes.
- Disable access to the NodeRed settings for security reasons, apply the changes, then click "Save and Restart" and wait for the GateWay to restart.

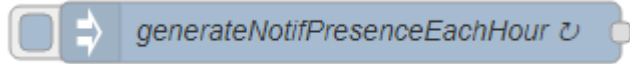


- If it is necessary to change this configuration again, perform a 10-second reset on the GateWay, and repeat the whole process described in section 7.

Checking the connection with the MySirius server:

It is possible to check the connection of the gateway with the MySirius server directly in Node-RED, if the gateway is connected to the client network (not possible if connected directly to the PC).

- Go to the "MySirius" tab and click on the "GenerateNotifPresenceEachHour" block button



- If an error message appears in the "Debug" tab (on the right of the screen), it means that there is a problem either in the server URL or in the client network which has not correctly opened the port
- If no message in the "Debug" tab -> the gateway is working correctly

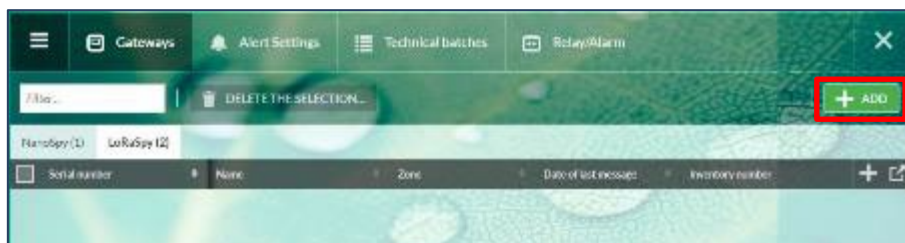


## 8. ADD THE GATEWAY IN MY SIRIUS

- Log in to MySirius with an ADMINISTRATOR account
- Open the configuration dashboard by clicking on the “Administration” tab



- Click on the « Gateways » tile.
- Click on +ADD and follow the wizard



- Select GateWay LoRa® SPY, enter the required information then click on SAVE.

**Caution:** It is important to enter the correct serial number. It will be used to link your gateway with your MySirius account.

Device Type	Gateway LoRa® SPY
Serial number	12345678
Name	GateWay TEST
Inventory number	Ex: 192.168.10.75/MAC: C8.3B.45.FA.0B.8D
Zone	DEMO
<div>CANCEL SAVE</div>	

- Once added on MySirius, the gateway will appear in the LoRa® Spy gateways list.



- You can now start your LoRa SPY / LoRa temp' devices within the radio coverage area of the gateway. An automatic detection is done for an easy installation.
- The gateway installation is a success if the “Date of last message” of the gateway is filled with the current date. Note that it may take a few minutes to get a connection between the gateway and MySirius. You may refresh your web page until the date of last message shows up.



Traçabilité, surveillance et métrologie

© JRI SAS au capital de 4 000 000 € - RCS Pontoise 380 332 858 - Date : 08/04/2022

[www.jri-corp.com](http://www.jri-corp.com) | [info@group-mms.com](mailto:info@group-mms.com)

Technical support : 0892680933 | [support@group-mms.com](mailto:support@group-mms.com)