User Guide

Sentrius RG1xx / RG191+LTE

Version 7.1

Revision History

Version	Date	Notes	Contributors	Approver
1.0	20 July 2017	Initial Release		Jonathan Kaye
1.1	3 Aug 2017	Clarified web interface URL. Identified separate mDNS address.		Shewan Yitayew
1.2	29 Nov 2017	Update info for compatibility with GA2 (93.7.2.x) firmware. Add compliance information. Add IP67 Rated Version Specs		Jonathan Kaye
2.0	13 Dec 2017	Changed Rev # to 2.0 to match engineering release		Jonathan Kaye
2.1	04 Jan 2018	Miscellaneous text and grammatical edits		Shewan Yitayew
2.2	10 Jan 2018	Adding Ordering Information		Jonathan Kaye
3.0	28 Feb 2018	Adding UAE Certification Compliance, Firmware update info		RG, RDE
3.1	15 Mar 2018	Added note to Wi-Fi Quick Configuration section regarding available firmware version. Updated to new template		Jonathan Kaye
3.2	29 Mar 2018	Removed inapplicable Firmware update URLs	Sue White	Jonathan Kaye
3.3	13 Apr 2018	Important update to firmware upgrade procedure	Ryan Erickson	Shewan Yitayew
3.4	30 May 2018	Updates for GA3 firmware. Add section for web session timeout. Update firmware upgrade section.	Ryan Erickson	Jonathan Kaye
3.5	20 Aug 2018	Updated Outdoor Enclosure Connector Layout	Robert Gosewehr	Jonathan Kaye
3.6	19 Dec 2018	Updated logos and URL	Sue White	Jonathan Kaye
3.7	7 Mar 2019	Updated Section 9.4.2 for clarity Updated template	Robert Gosewehr Sue White	Jonathan Kaye
3.8	11 Oct. 19	Added AS923/AU915 Region Support	Robert Gosewehr Adam Ruehl Raj Khatri Chris Boorman	Jonathan Kaye
3.9	8 Nov 19	Update remote management section to include information about uploading and downloading configuration files for LoRa and Wi-Fi.	Adam Ruehl	Chris Boorman
4.0	4 Feb 2020	Updates for GA5	Adam Ruehl	Chris Boorman
4.1	17 April 2020	Added URL for GA4.1	Adam Ruehl	Chris Boorman
5.0	19 Dec 2020	Updated all regulatory information	Maggie Teng Ryan Urness	Jonathan Kaye
5.1	5 Jan 2021	Updates for GA5.2	Adam Ruehl	Chris Boorman
5.2	6 Apr 2021	Updated regulatory definition/detail	Chris Boorman	Jonathan Kaye
6.0	25 May 2021	Updated for GA6 + migration of RG191+LTE gateway user guide content	Adam Ruehl Robert Gosewehr	Chris Boorman
6.1	20 Dec 2021	Updated firmware update section for new release	Adam Ruehl	Chris Boorman
6.2	4 Feb 2022	Added New RG1xx+LTE Generation Support	Brian Petted Robert Gosewehr	Jonathan Kaye
6.3	9 Nov 2022	Updated part 450-00107-K2 in 2.3 Ordering Information.	Adam Ruehl	Jonathan Kaye
6.4	2 Feb 2023	Revised and updated section 3.1.3 Wi-Fi Quick Configuration.	Adam Ruehl Robert Gosewehr Florian Baumgartl	Jonathan Kaye

Version	Date	Notes	Contributors	Approver
6.5	21 Mar 2023	Updated the cellular node in the The Sentrius Gateway's TR-069 Data Model and IP67 Rated Enclosure sections.	Adam Ruehl Robert Gosewehr	Senthooran Ragavan
6.6	3 June 2024	Updated for firmware v6.5.	Dave Drogowski	Senthooran Ragavan
6.7	11 Sept 2024	Updated URL for updating firmware to incorporate ezurio.com	Seokwoo Yoon	Senthooran Ragavan
7.0	8 May 2025	Updated to Ezurio branding	Dave Drogowski	Dave Drogowski
7.1	21 July 2025	Updated for GA8 (LRD12)	Seokwoo Yoon	Jonathan Kaye

Contents

1 About this Guide

This document is the parent guide of the ***RG1xx Quick Start Guide*** and provides a comprehensive guide on how to configure the **Sentrius™ RG1xx** gateways to suit the intended application. It covers all the **Sentrius™ RG1xx** functionality, including Ethernet, Wi-Fi and LoRa configurations. It also provides instructions for setting up the gateway on a LoRa network server.

All sections describing LTE operation are for features only available on the RG191+LTE model.

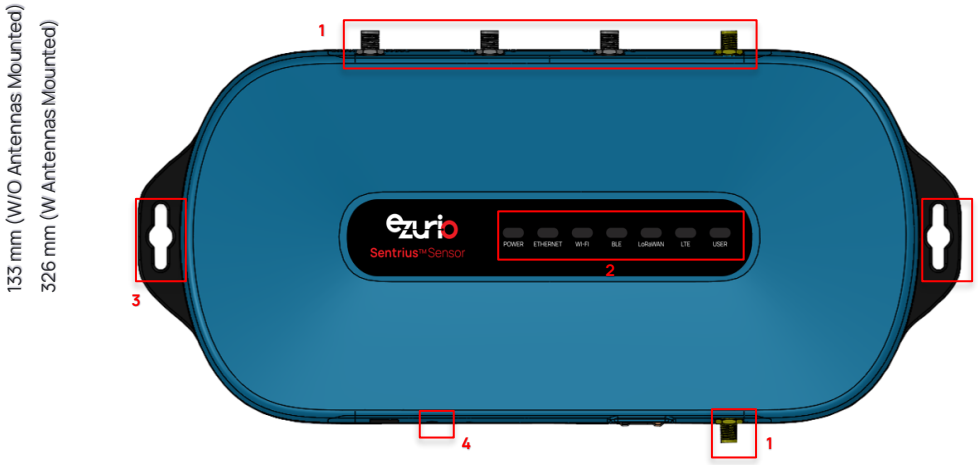
All other hardware models **Do Not** contain the required LTE modem.

Note: Step-by-step instruction, screen shots, and pictures are based on the **Sentrius™ RG191**, but the same is applicable for the **Sentrius™ RG186** and other AS915, AU923 variants; differences are highlighted in the notes.

2 Introduction

2.1 Product Overview

Ezurio's **Sentrius™ RG1xx** LoRa-Enabled Gateway is the ultimate in secure, scalable, robust LoRa solutions for end-to-end control of your private LoRaWAN network. Leveraging Ezurio's field-proven and reliable 50 Series *Wireless Bridge* certified module, it also offers enterprise dual-band Wi-Fi and wired Ethernet for complete design freedom. Based on the Semtech SX1301/SX1257 chipset designs, it offers a LoRa range up to ten miles and pre-loaded LoRa Packet Forwarder software, perfect for highly scalable, flexible IoT networks. The Sentrius RG1xx Gateway works with Ezurio's **Sentrius™ RM1xx Series LoRa+BLE** certified modules for simple out-of-the-box integration and is compatible with third-party cloud and LoRa partners, as well as any LoRaWAN-certified client devices. **LTE hardware and connectivity only available on RG191+LTE models.**



1. LoRa, Wi-Fi and LTE Antenna Ports **(LTE only available on RG191+LTE model)**
2. LEDs
3. Mounting Holes
4. User Button

Figure 1: Top of the Sentrius™ RG1xx Gateway

1. DC Power Input
2. User Button
3. Reset Button
4. SD Card Slot
5. Ethernet Connector
6. LTE Antenna Port

Figure 2: Side panel of the Sentrius™ RG1xx gateway

2.2 Specification

Category	Feature	Specification
Chipset	**LoRa®**	Semtech SX1301/SX1257
	Bluetooth®	Cambridge Silicon Radio CSR8811 A08
	Wi-Fi	Qualcomm Atheros QCA6004
	LTE CAT 1 (Only within RG191+LTE)	Quectel EG91-NA
Wireless Characteristics	**Wi-Fi Spatial Streams**	2x2 MIMO
	Wi-Fi Frequencies	2.4 and 5 GHz operation
	FCC/IC conducted WiFi transmit power (for single stream) ***Note:*** *Transmit power on each channel varies according to individual country regulations. All values for lowest data rate are nominal, +/-2.0dB.* ***Note:*** *HT40 – 40 MHz-wide channels* *HT20 – 20 MHz-wide channels*	**802.11a** 6 Mbps | 17 dBm 54 Mbps | 14 dBm **802.11b** 1 Mbps | 17 dBm 11 Mbps | 17 dBm **802.11g** 6 Mbps | 17 dBm 54 Mbps | 14 dBm **802.11n (2.4 GHz)** 6.5 Mbps (MCS0) | 17 dBm 65 Mbps (MCS7) | 13 dBm **802.11n (5 GHz)** 6.5 Mbps (MCS0, HT20) | 17 dBm 65 Mbps (MCS7, HT20) | 13 dBm (MCS0, HT40) | 14 dBm (MCS7, HT40) | 11 dBm
	ETSI (CE) RG186 conducted WiFi transmit power (for single stream) ***Note:*** *Transmit power on each channel varies according to individual country regulations. All values for lowest data rate are nominal, +/-2.0dB.* ***Note:*** *HT40 – 40 MHz-wide channels* *HT20 – 20 MHz-wide channels*	**802.11a (5GHz band)** 6 Mbps | 14 dBm 54 Mbps | 14 dBm **802.11b (2.4GHz band)** 1 Mbps | 10 dBm 11 Mbps | 10 dBm **802.11g (2.4GHz band)** 6 Mbps | 11dBm 54 Mbps | 11dBm **802.11n (2.4GHz band)** 6.5 Mbps (MCS0) | 11dBm 65 Mbps (MCS7) | 11dBm **802.11n (5GHz band)** 6.5Mbps (MCS0, HT20) | 14dBm 65 Mbps (MCS7, HT20) | 13dBm 6.5 Mbps (MCS0, HT40) | 14dBm 65 Mbps (MCS7, HT40) | 11dBm
	Note: *Bluetooth support not included at a software level within the RG1xx*	**Bluetooth Low Energy** 1 Mbps | 6 dBm
	Wi-Fi Radio Conducted Typical Receiver Sensitivity ***Note:*** *All values nominal, ±3 dBm. Variant by channels.*	**802.11a** 6 Mbps | -92 dBm 54 Mbps | -74 dBm (PER < = 10%) **802.11b** 1 Mbps | -94 dBm 11 Mbps | -87 dBm (PER < = 8%) **802.11g** 6 Mbps | -91 dBm

Category	Feature	Specification	
		54 Mbps	-74 dBm (PER < = 10%)
		802.11n (2.4 GHz)	
		6.5 Mbps (MCS0)	-91 dBm
		65 Mbps (MCS7)	-71 dBm
		802.11n (5 GHz HT20)	
		6.5 Mbps (MCS0)	-92 dBm
		65 Mbps (MCS7)	-71 dBm
		Bluetooth Low Energy	
		1 Mbps	-86 dBm
LoRa - Wireless Characteristics	**LoRa Frequencies, LoRaWAN Region, UL/DL, Ezurio part number**	EU	863 – 870 MHz (LoRaWAN EU863-870, UL/DL) –RG186
		US	902 – 928 MHz (LoRaWAN US902-928, UL) – RG191
		NZ	918.2 – 927.6 MHz (LoRaWAN AS923 UL/DL) – 455-00055
		AU	923.3 – 927.5 MHz (LoRaWAN AU915-928, UL) – 455-00057
		AU	915.4 – 927.7 MHz (LoRaWAN AS923, UL/DL) – 455-00057
		TWN	920.2 – 924.8 MHz (LoRaWAN AS923, UL/DL) – 455-00054
		HK	920.2 – 924.8 MHz (LoRaWAN AS923, UL/DL) – 455-00056
		SG	920 – 925 MHz (LoRaWAN AS923, UL/DL) – 455-00102
	LoRa Radio Conducted TX Power (at -40°C) (RG191 plus AS915 & AU923 variants)	US	28 dBm (max entry in Radio TX Power Table)
		NZ	24 dBm (max entry in Radio TX Power Table)
		AUS	27 dBm (max entry in Radio TX Power Table), AU915 and AS923
		TWN	25 dBm (max entry in Radio TX Power Table)
		HK	25 dBm (max entry in Radio TX Power Table)
		SG	27 dBm (max entry in Radio TX Power Table)
		US, NZ, AUS, TWN, HK, SG	0 dBm (min entry in Radio TX Power Table)
	LoRa Radio Conducted RX Sensitivity (RG191 plus AS915 & AU923 variants)	-127 dBm (Bandwidth = 125 kHz, Spreading Factor = 7, DR0)	
	LoRa Radio Conducted TX Power (at -40°C) (RG186)	Supports TX power as per ETSI Frequency bands 25 dBm (max entry in Radio TX Power Table) -3 dBm (min entry in Radio TX Power Table)	
	LoRa Radio Conducted RX Sensitivity (RG186)	-125 dBm (Bandwidth = 125 kHz, Spreading Factor = 7, DR0) -123 dBm (Bandwidth = 250 kHz, Spreading Factor = 7, DR6)	
Interfaces	**Wired**	Ethernet - RJ45 Connector	
	Wireless	LoRa, 802.11a/b/g/n, Cellular LTE (**Only RG191+LTE model**)	
Power	**Supply Voltage**	12V/1A	
	Power Adapter	External DC Power Supply (has 12V /2A rating) with regional plug adapter	
Security	**Wi-Fi**	Standards – WEP, WPA, WPA2 Encryption – WEP, TKIP, AES EAP Types – EAP-FAST, EAP-TLS, EAP-TTLS, PEAP-GTC, PEAP-MSCHAP, PEAP-MSCHAPv2, PEAP-TLS, LEAP	
Software	**Operating System**	Embedded Linux, 4.x Kernel	
	LoRa	Packet Network Forwarder with default support for the following: The Things Network with Semtech Basics Station or UDP forwarder Stream communications with UDP forwarder ChirpStack with UDP forwarder or Semtech Basics Station Senet through legacy Semtech UDP or proprietary Senet forwarder	
	Configuration	Web-based interface via Ethernet/Wi-Fi or remote via TR-069 protocol (requires ACS)	
Physical	**Dimensions**	133 x 275 x 30 mm (enclosure only)	

Category	Feature	Specification
Environmental	**Operating Temperature**	-30° to +70°C ***Note:*** *The RG1xx gateway operating temperature range is limited to -30° to +70°C due to the supplied external power supply. The RG1xx gateway without the external power supply is certified for -40° to +85°C.*
Regulatory	**Approvals (RG186)**	**CE** Health and Safety – IEC 60950-1 V2.0 Radio – EN300 220-1 V3.1.1 (2017-02); EN300-220-2 V3.1.1 (2017-02) EMC – EN301 489-1 V2.2.0 (2017-03); EN301 489-3 V2.1.1 (2017-03)
	Approvals (RG191)	**FCC –** Contains FCC ID: SQG-WB50NBT **IC –** Contains IC ID: 3147A-WB50NBT **FCC –** Contains FCC ID: SQG-1001 **IC –** Contains IC ID: 31347A-1001 **NZ –** AS/NZS 4268:2017 **AUS –** AS/NZS 4268:2017 **TWN –** NCC LP0002 **SG –** DA107248 **PTCRB (LTE Version) –** Covers Bands 2, 4, 5, 12, & 13
Wi-Fi Antenna	**Model**	Ezurio MAF94051
	Type	Dipole
	Connector	RP-SMA
	Antenna Gain	2.1 dBi (2.4-2.5 GHz), 2.4 dBi (4.9 GHz) 2.6 dBi (5.25 GHz), 3.4 dBi (5.875 GHz)
LoRa Antenna	**Model**	Ezurio 001-0028 (863-870 MHz) used with RG186 Ezurio 001-0002 (902-928 MHz) used with RG191 plus AS915 and AU923 variants
	Type	Dipole
	Connector	RP-SMA (001-0002 & 001-0028)
	Antenna Gain	2.0 dBi (863-870 MHz) used with RG186 2.0 dBi (902-928 MHz) used with RG191 plus AS915 and AU923 variants
LTE Antenna	**Model**	Ezurio DBA6927C1-FSMAM
	Type	Dipole
	Connector	SMA-Male
	Antenna Gain	0.5 dBi (698-960 MHz) – 2.2 dBi (1710-2700 MHz) used with RG191+LTE
Accessories	**Included**	1 x 863-870 MHz antenna (with RG186) or 1 x 902-928 MHz antenna (with RG191, AS915 and AU923 variants) 2 x 2.4/5 GHz Wi-Fi antennas 2 x 698-960/1710-2700 MHz LTE antenna (**with RG191+LTE**) 1 x External DC power adapter
Enclosure	**Standard**	Moulded plastic housing
Warranty		One-year warranty

2.3 Ordering Information

Important Note: **The region setting of the radio cannot be changed.** The user must purchase the appropriate model for the desired region of operation and only use the model **appropriate for the location in which they will install the gateway.**

Table 1: Ordering information

Part Number	Description
RG191	Sentrius™ RG191 US (US902-928) 915 MHz Gateway - LoRaWAN, Wi-Fi, and Ethernet – US Power Adapter
RG186	Sentrius™ RG186 Europe (EU868) 868 MHz Gateway - LoRaWAN, Wi-Fi, and Ethernet – EU Power Adapter
455-00028	Sentrius™ RG186 United Kingdom (EU868) 868 MHz Gateway - LoRaWAN, Wi-Fi, and Ethernet – UK Power Adapter
450-0190	Sentrius™ RG186 Europe (EU868) 868 MHz Gateway – LoRaWAN, Wi-Fi, and Ethernet – IP67
450-0191	Sentrius™ RG191 US (US902-928) 915 MHz Gateway – LoRaWAN, Wi-Fi, and Ethernet – IP67
455-00054	Sentrius™ RG191 Taiwan (AS923) 923 MHz Gateway - LoRaWAN, Wi-Fi, and Ethernet – TW Power Adapter
455-00055	Sentrius™ RG191 New Zealand (AS923) 923 MHz Gateway – LoRaWAN, Wi-Fi, and Ethernet – NZ Power Adapter
455-00056	Sentrius™ RG191 Hong Kong (AS923) 923 MHz Gateway – LoRaWAN, Wi-Fi, and Ethernet – HK Power Adapter
455-00057	Sentrius™ RG191 Australia (AU915+AS923) 923 MHz Gateway – LoRaWAN, Wi-Fi, and Ethernet – AU Power Adapter
455-00102	Sentrius™ RG191 Singapore (AS923) 923 MHz Gateway – LoRaWAN, Wi-Fi, and Ethernet – UK Power Adapter
450-00107-K2	Sentrius™ RG191 US (US902-928) 915 MHz Gateway - LoRaWAN, Wi-Fi, Ethernet and LTE, CAT-1, NA
450-00109-K2	Sentrius™ RG191 US (US902-928) 915 MHz Gateway - LoRaWAN, Wi-Fi, Ethernet and LTE, CAT-1, NA – IP67
Accessories	
690-1002	Pole Mount Bracket - Accessory for IP67 Gateways
690-1003	Wall Mount Bracket - Accessory for IP67 Gateways

3 Connecting the Hardware

3.1 Connect the Gateway

To use the gateway, you must power up the gateway and access the web interface via the Ethernet port. To do this, follow these steps:

1. Follow the label on the box and connect the three (or five with RG1xx+LTE) antennas. Refer to Antenna Configuration section for additional information.
2. Connect the power supply (see #2 in Figure 3).
3. Connect the gateway to your router (#3 in Figure 3) using the Ethernet cable (#1 in Figure 3).

Alternatively use the Wi-Fi Quick Config mechanism. Refer to Wi-Fi Quick Configuration for additional information.
Your gateway is now connected and ready.

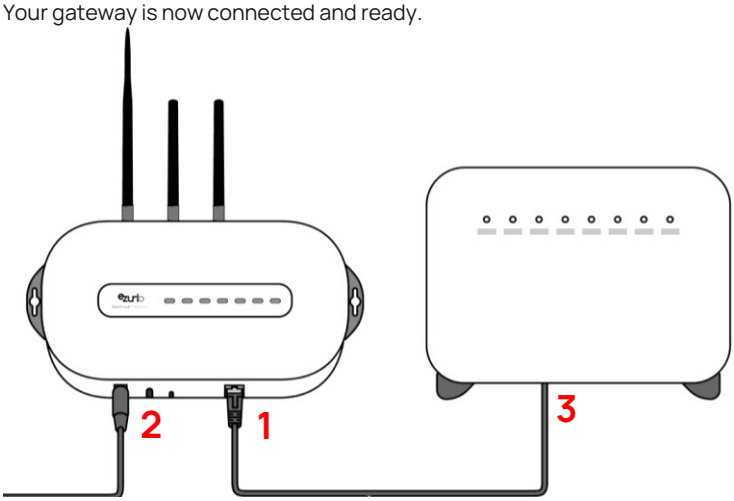


Figure 3: Connecting the gateway

Note: The figure above depicts the standard RG1xx gateway, please refer to Figure 1 for depiction of LTE-equipped gateway. The steps described in the section above pertains to the LTE-equipped gateway as well.

3.1.1 SIM Card Installation

Note: This is only available with the RG191+LTE hardware for the US market only, see Ordering Information for product part numbers.

To utilize the LTE functionality, a cellular network provider's SIM card needs to be installed into the gateway. The recommended SIM card to purchase shall support LTE-CAT 1, to utilize the full capabilities of the LTE gateway.

Note: The RG191+LTE production units come with a Truphone SIM card pre-installed. The SIM will need to be registered and activated, see section 5.2.

To install the SIM card, follow these steps:

1. Unscrew the four (4) back Torx screws using a T8 Torx screwdriver for the non-IP67 gateway version.
   Unscrew the thirteen (13) screws using a Philips screwdriver for the IP67 gateway version.

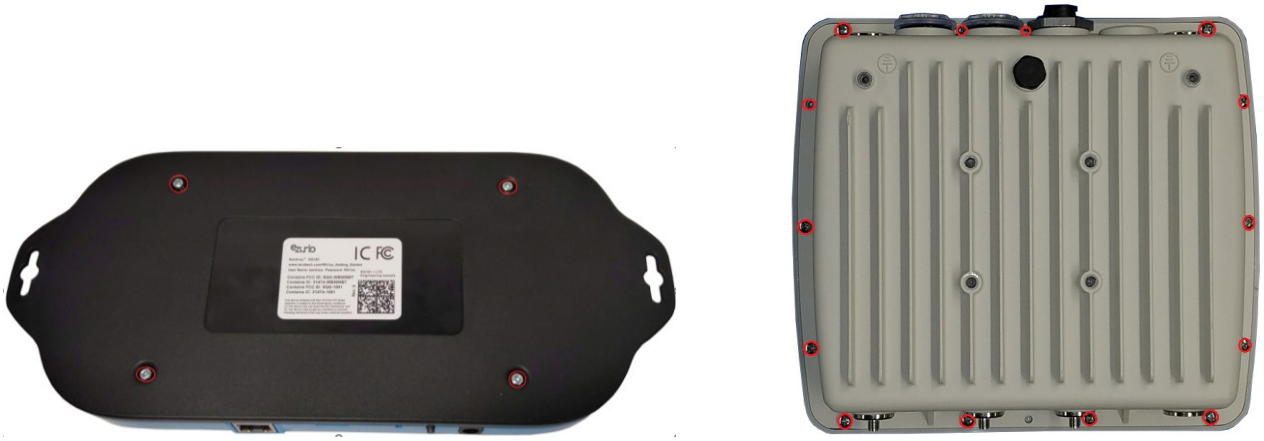


Figure 4: Gateway Screw Locations (Left: Standard; Right: IP67)

2. Carefully move the top enclosure lid to the back of the gateway for the indoor (non-IP67) version as seen below.
   Remove the top lid for the IP67 gateway version (RF cables are not connected to the top cover on the IP67 gateway).

Figure 5: Opened Gateway (indoor (non-IP67) gateway shown)

Note: The RF cables are connected to the modules and glued in position. If the antennas are installed, remove the antennas before moving the top enclosure in position for the indoor (non-IP67) gateway.

---

3. If replacing the production installed SIM card, punch out the Micro-SIM (3FF size) from the Main Sim card (secondary set of punch out lines from the center moving outward).

Figure 6: SIM Card Punch-Out

4. Install the SIM card into the SIM card slot in the upper right location near the LTE modem making sure the copper contact side of the SIM card is facing down (follow Blue Arrow). Re-close the gateway and screw down the screws when complete.

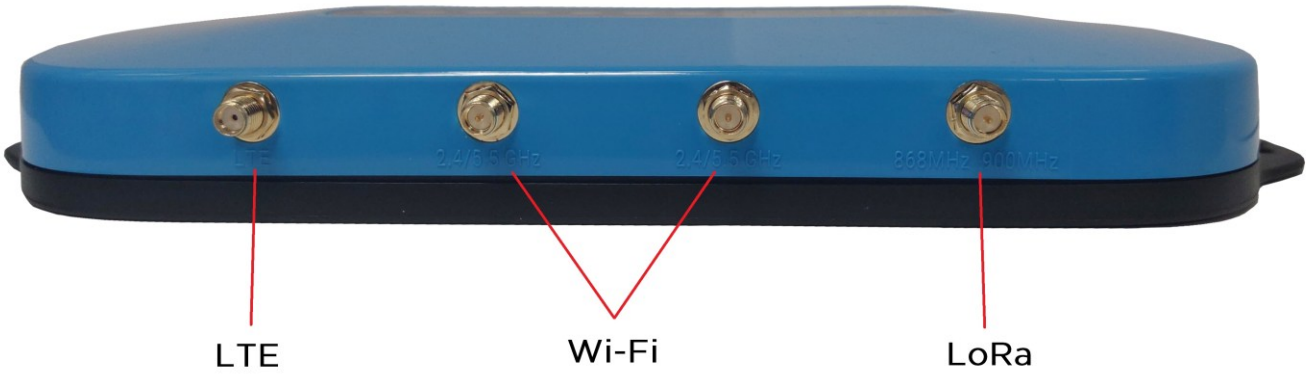
Figure 7: SIM Install (Right: Picture of SIM card contact side)

Note: To remove the SIM card, push the card out from Red Arrow side and remove SIM.

3.1.2 Antenna Configuration

To configure the antenna properly, take the following steps:

1. Attach the two shorter antennas to the 2.4/5.5 GHz (Wi-Fi) ports.
2. Attach the third and longer antenna to the 868 MHz/900 MHz (LoRa) port.
3. Attach the fourth and fifth wider blade antennas to the LTE ports. **Notice the different connector types**. The LTE antennas will only fit in the designated ports. The fifth port is in front of the gateway. This is only available on RG191+LTE hardware.



3.1.3 Wi-Fi Quick Configuration

Note: **This feature only works with firmware version 93.7.2.9 and newer**. Please verify your Gateway firmware version number and, if required, upgrade to a current version. Refer to **Updating Gateway Firmware** for additional information regarding this upgrade.

For configuration reasons, the RG1xx gateway supports a mode allowing you to access its web UI through a wireless network (Wi-Fi access point) without Ethernet and LAN access. Please follow manually the instructions below to enable it temporarily.
Apply power to the gateway and allow it to start (this might take a few minutes), then perform the following steps:

1. Press, hold and release the User button (Figure 2) after seven seconds. The Wi-Fi LED will now start blinking.
2. Perform a scan from a wireless-enabled device such as a smartphone, tablet, or laptop which you would like to use.
3. Connect to rg1xx**29378b**, where *29378b* are the last six digits of the Ethernet MAC address of your RG1xx gateway.

The Wi-Fi network and access point of the RG1xx gateway is secured with WPA2 and a password that is the same as the SSID. We recommend that you change the default password for security reasons. The password can be changed in the web UI under Wi-Fi → Advanced → Wi-Fi Quick Config Settings → SoftAP Password (Figure 26) at any time.

You can find the Ethernet MAC address and the last six digits of it on the product label on the bottom of your RG1xx gateway (Figure 8). Please note that both SSID and password are in lowercase only. Do not use any uppercase characters. In this example, **rg1xx29378b** is correct whereas **rg1xx29378B** would be incorrect and not work.
Please be aware that upon logout or client disassociation, the Wi-Fi Quick Config shuts down and normal operation resumes.

4 Log into the Gateway

To log into the gateway web interface, follow these steps:

1. Determine the last three bytes of your gateway's Ethernet MAC address. This can be found on the label on the bottom of the gateway; the last three bytes are highlighted (Figure 8).

Figure 8: Bottom label (Standard GW – Left, AS923 & AU915 Region Supported/Latest Version – Right) – last three bytes of the Ethernet MAC address highlighted

2. Enter the URL into the web browser to access the web interface. For example, for the gateway used in this guide, the URL is https://rg1xx**29378B**.local, where "*29378B*" are the last six digits of the Ethernet MAC address. In Wi-Fi quick config mode, the gateway can also be accessed via the IP address at https://192.168.1.1.
3. Accept the self-signed security certificate in the browser.
4. Click **Advanced** (Figure 9).

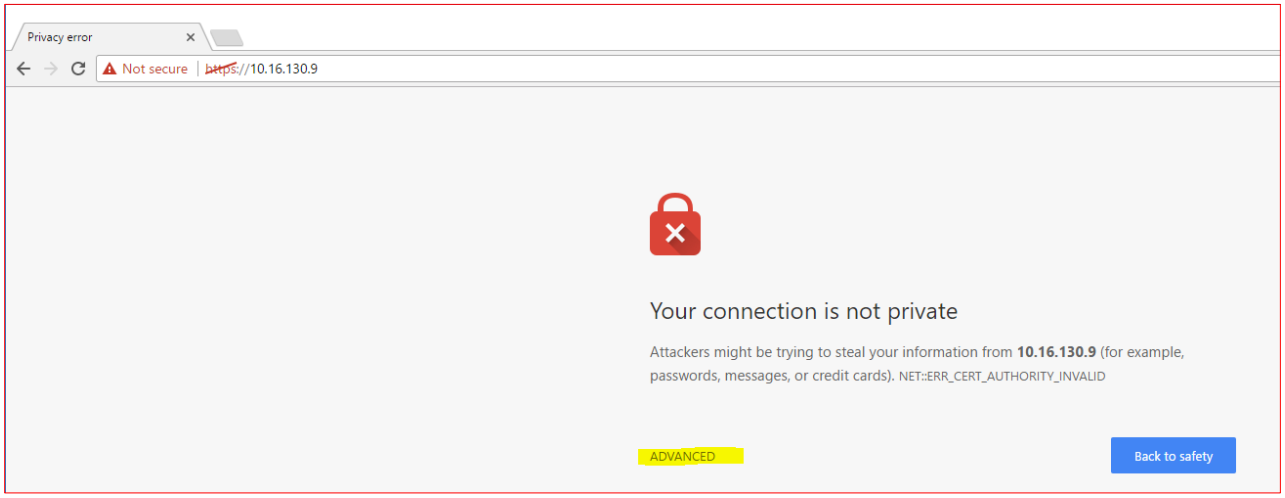


Figure 9: Web interface – first screen

5. Click **Proceed** (Figure 10).

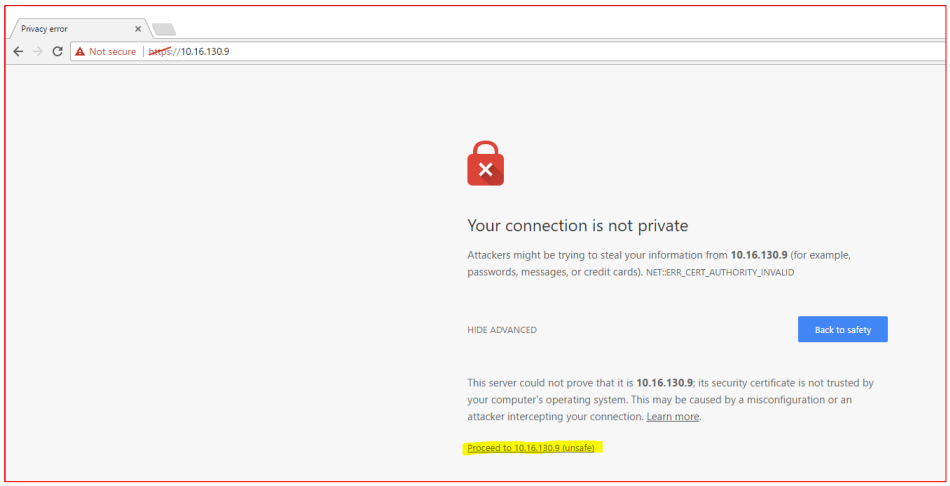


Figure 10: Web interface – second screen

6. Log on using the following default credentials:

   Username: sentrius

   Password: RG1xx

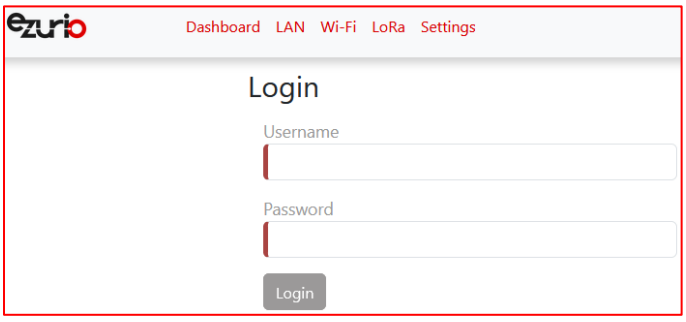


Figure 11: Gateway interface login screen

After logging in, the program warns you to change the default credentials for security reasons (Figure 12).

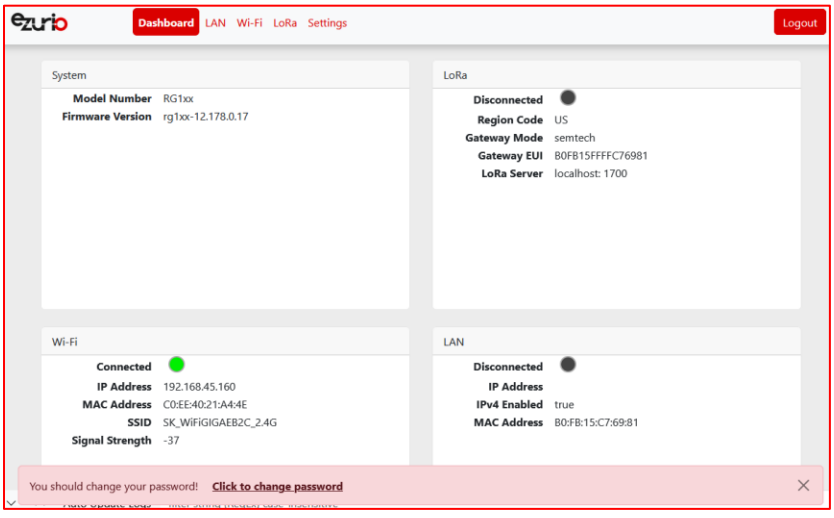


Figure 12: Change the default credentials

Only one login session is allowed at a time. If there is another active session active, the program warns you before allowing you to take over the session (Figure 13).

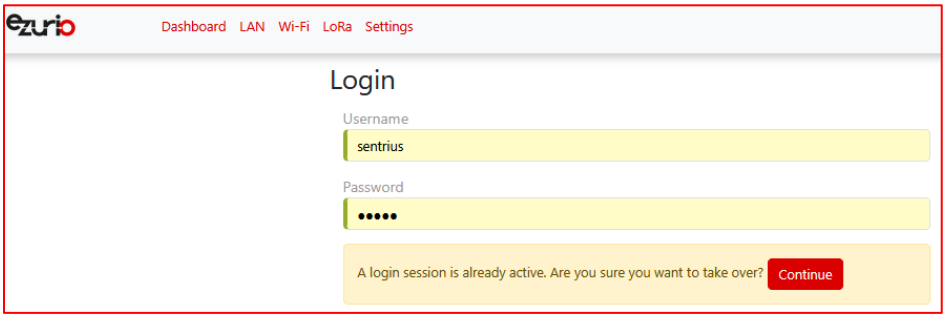


Figure 13: Active session warning

7. Click **Continue** to log in.

5 LTE Connection setup

Note: This feature only works with the RG191+LTE hardware for the US market only, see Ordering Information for product part numbers.

The Cellular menu supports modem configuration. The status of the integrated Cellular modem is also displayed. To access this section, click the **Cellular** tab from the ribbon at the top of the page.

In the sidebar on the left (Figure 14*)* you can navigate various Cellular pages. Further, you will find a button to enable/disable the Cellular modem.

Note: By default, the Cellular modem within the gateway is disabled!! **Users will need to enable it!**

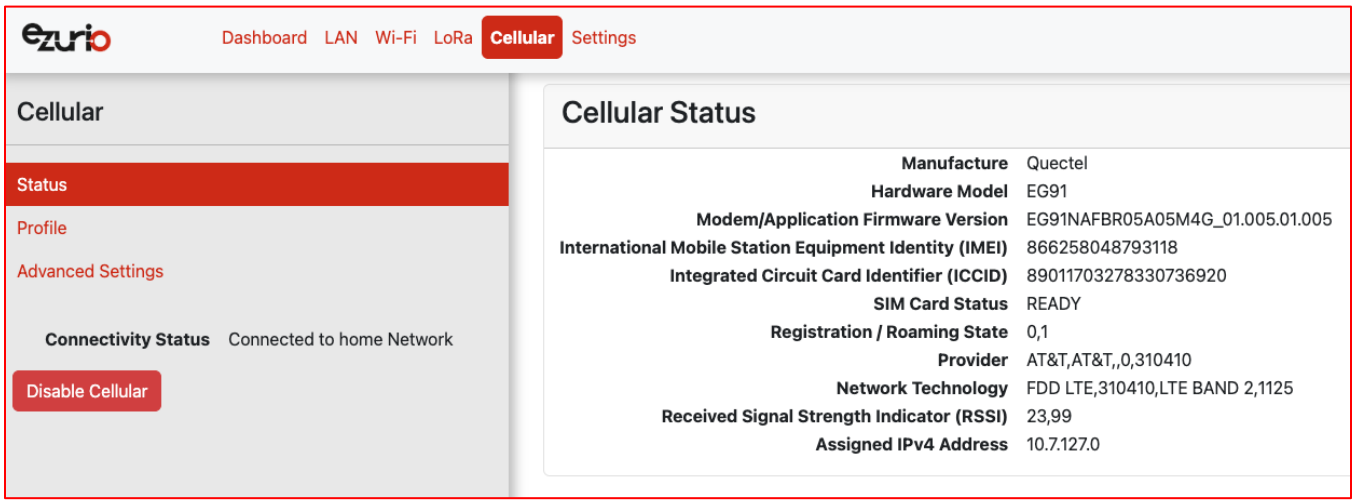


Figure 14: Enable/Disable Cellular Button

5.1 Status – Modem and Network Information

The first page when clicking on the Cellular menu is the **Status** page (Figure 15). You cannot change anything on this page.

This page will provide you with information about the Cellular modem, inserted SIM card, and your network connection.

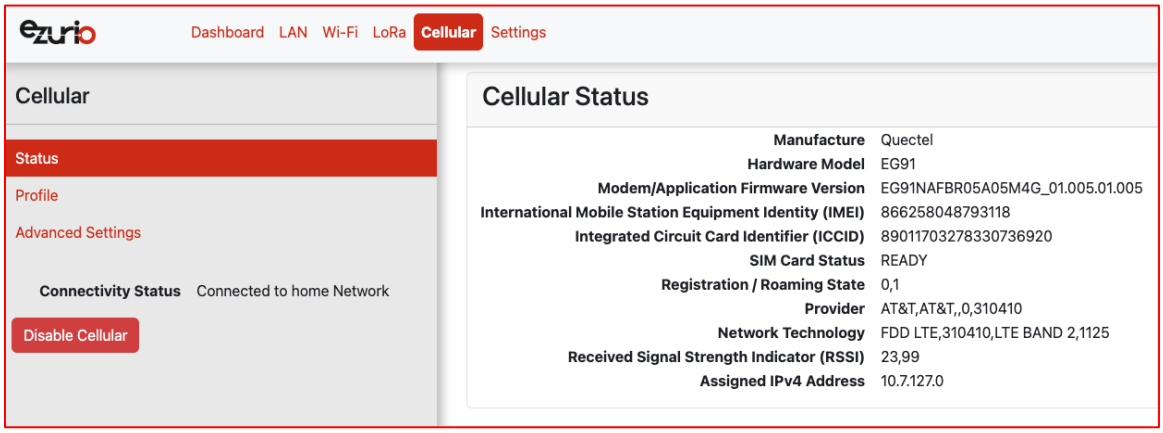


Figure 15: Cellular Status page

- **Manufacturer** – Shows the manufacturer identification of the integrated Cellular modem.
- **Hardware Model** – Shows the hardware model identification of the integrated Cellular modem.
- **Firmware Revision** – Shows the current firmware revision of the integrated Cellular modem.
- **International Mobile Station Equipment Identity (IMEI)** – Shows the IMEI number of the integrated Cellular modem.
- **Integrated Circuit Card Identifier (ICCID)** – Shows the ICCID number of the attached (U) SIM card (only if not locked).
- **SIM Card Status** – Shows the current state of the SIM card and whether a password (PIN/PUK) is required.
- **Registration / Roaming State** – Shows information about the network registration and roaming state.
- **Provider** – Shows information about the current service provider which the Cellular modem is attached to.
- **Network Technology** – Shows information about the current access technology and network frequency / band.
- **Received Signal Strength Indicator (RSSI)** – Shows information about the current received signal strength and channel bit error rate.

Note: A value of 99 indicates unknown or not detectable.

- **Assigned IPv4 Address** – Shows information about the public IPv4 address of the current mobile data connection.

Note: ***N/A*** means ***Not Available***. In this case either parts of the Cellular modem are not fully initiated, or some information could not be obtained. Wait a few seconds and try it again by refreshing the page. If all fields show N/A, please make sure that the Cellular modem is turned on and installed properly.

5.2 Profile – APN (User) Profile Configuration

Select the Modem Configuration page by clicking the **Settings** menu item in the side menu of the Cellular view (Figure 16).

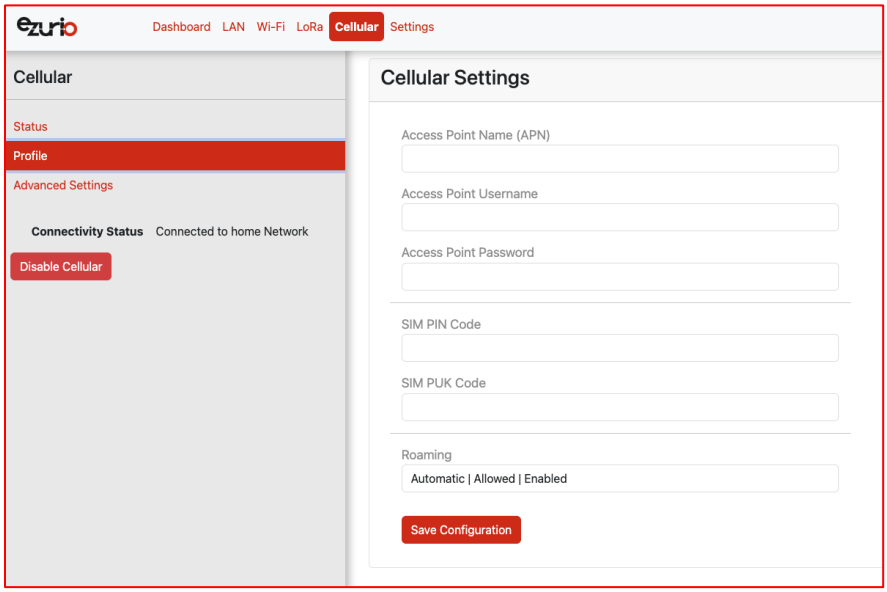


Figure 16: Cellular Settings page

1. Depending on your service provider that issued the SIM card you may have to add extra information about your **Access Point Name** (APN), Access Point Username and Access Point Password for authentication purposes. If you are unsure about these settings, please contact your mobile service provider and/or SIM card provider. However, most providers do not require this information to be entered.

Note1: The RG191+LTE gateway comes with a preinstalled Truphone SIM card:
Navigate to https://iot.truphone.com to register and activate your SIM card.
Select a data plan that meets your data needs for your application. This is a subscription plan.

Enter Truphone's APN: **iot.truphone.com** in the APN field and save the configuration to start the cellular service. This requires a reboot. ***** Cellular must be enabled to utilize the cellular feature. *****

2. If your SIM card is protected, you should add your **PIN** and/or **PUK** code where needed (**otherwise leave these fields empty**). Reference the SIM card and/or mobile service provider documentation for more details on the necessary settings to configure.

Note: The RG191+LTE gateway comes with a preinstalled Truphone SIM card which, once registered and activated following the link above, does **NOT** require a PIN and/or PUK code by default. If using the preinstalled Truphone SIM card, leave these fields blank. ***** Cellular must be enabled to utilize the cellular feature. *****

---

3. Choose a **Roaming option**. By default, roaming is enabled, and in most cases, it is recommended. For Roaming there are two options available – **Allowed** and **Disallowed**. When roaming is Disallowed, your network preference is restricted to home-only; no resources from other operator's network will be used in that case.
4. Apply your settings by clicking on the **Save Configuration** button and **reboot** the gateway when requested.

5.3 Advance Settings

Select the Advanced Modem Configuration page by clicking the **Advanced Settings** menu item in the side menu of the Cellular view (Figure 17)

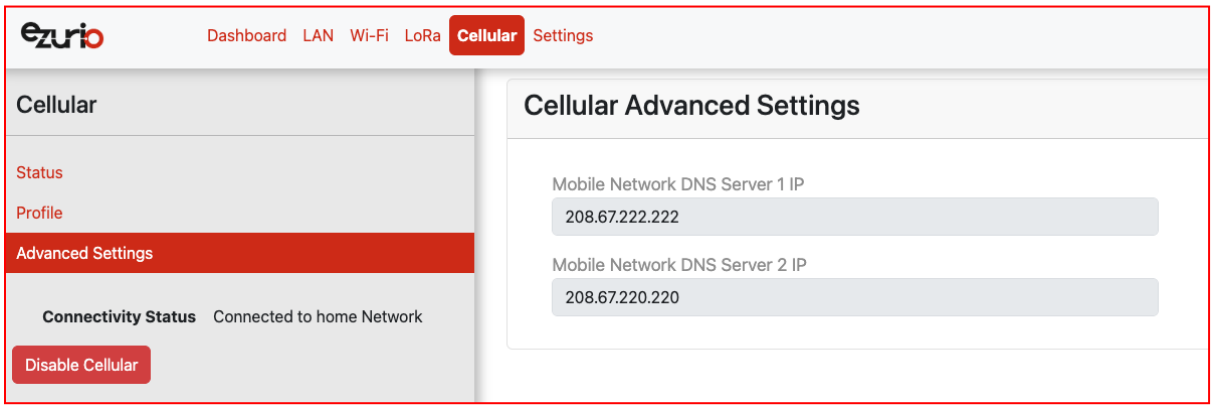


Figure 17: Cellular Advanced Settings page

This page will provide information about Cellular DNS Server(s) assigned by your service provider.

6 LAN Connection Setup

The LAN menu allows selections for configuration and status of the IPv4/IPv6 wired network. The status of the IPv4 network is also displayed. To access this section, click **LAN** in the page menu.

6.1 IPv4 Configuration

The first page for configuring the Ethernet LAN connection is the IPv4 Configuration page. There are two basic modes of operation – DHCP and Static. These are selected in the IP Address Acquisition Method drop-down box (Figure 18). The gateway factory default setting is DHCP.

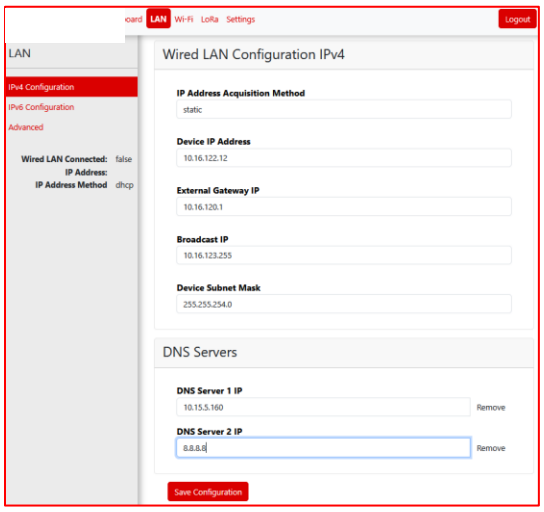


Figure 18: IPv4 Configuration page

DHCP – When in DHCP mode, all settings are provided by the DHCP server. All configuration settings (except IP Address Acquisition Method) are greyed out. IP values provided by DHCP are displayed but cannot be changed.

Static – When the IP Address Acquisition Method is set to static, all IP settings are fixed and saved in the device. The external Gateway IP address is optional and may be left blank. DNS Server IP addresses are also optional. Zero, one, or two DNS servers may be specified.

6.2 IPv6 Configuration

Select the IPv6 configuration by clicking the IPv6 menu item in the side menu of the LAN view (Figure 18). The IPv6 configuration settings are shown below.

There are two fully supported modes for IPv6 addressing:

DHCP – In DHCP mode, all settings are provided through communication with an IPv6 server on the network.

Auto – In auto mode, you have the option of selecting the auto DHCP method (either stateless or SLAAC). Currently, IPv6 static mode is only partially supported.

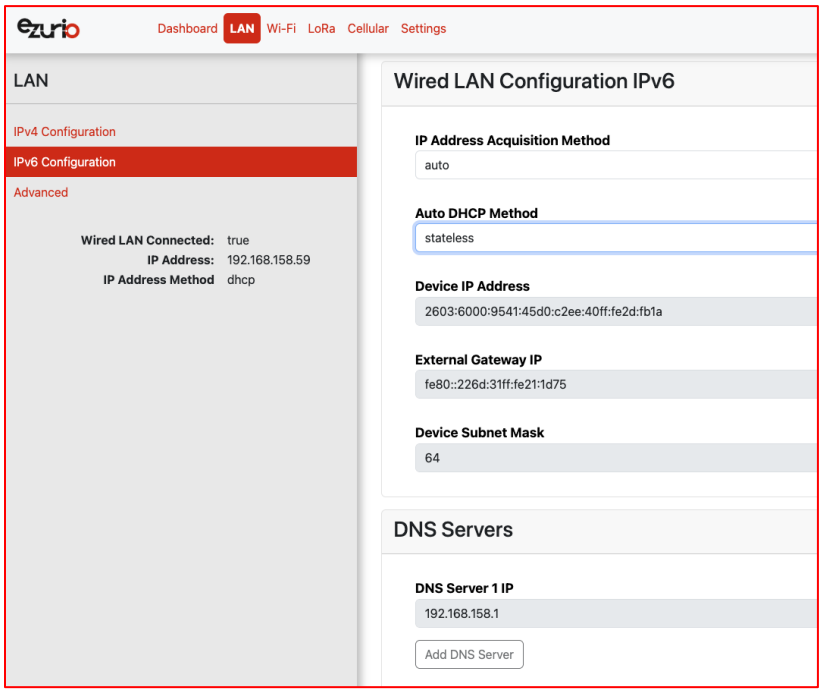


Figure 19: IPv6 Configuration page

6.3 Advanced View

Select the advanced view by clicking the Advanced menu item in the LAN sidebar (Figure 20). The Advanced view shows all network information provided by the Wi-Fi module in the gateway. Depending on the settings of the network and the gateway, not all settings may apply to the current mode of operation. This view is intended to support advanced users in troubleshooting their network.

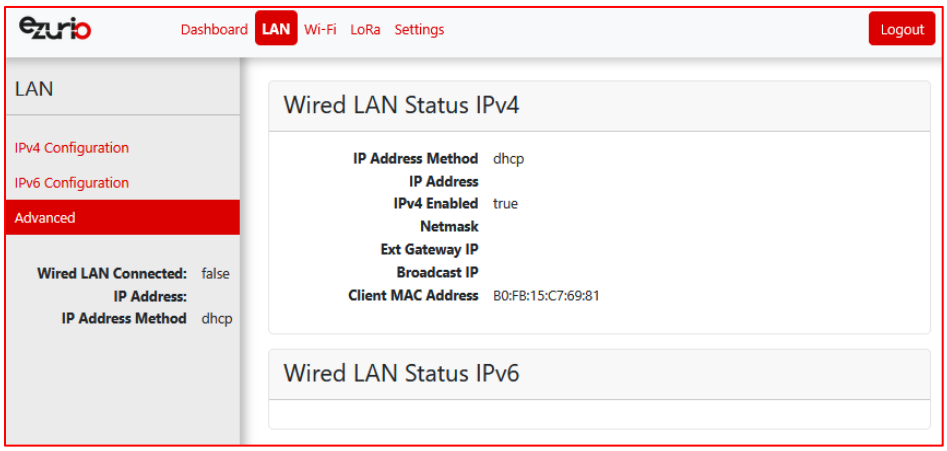


Figure 20: Advanced view

7 Wi-Fi Connection Setup

By default, the gateway's Wi-Fi radio is not configured to connect to a Wi-Fi network. The user must access the web interface on the gateway via the Ethernet interface to setup the Wi-Fi connection.

To setup a Wi-Fi connection, click the **Wi-Fi** tab in the main menu (Figure 21).

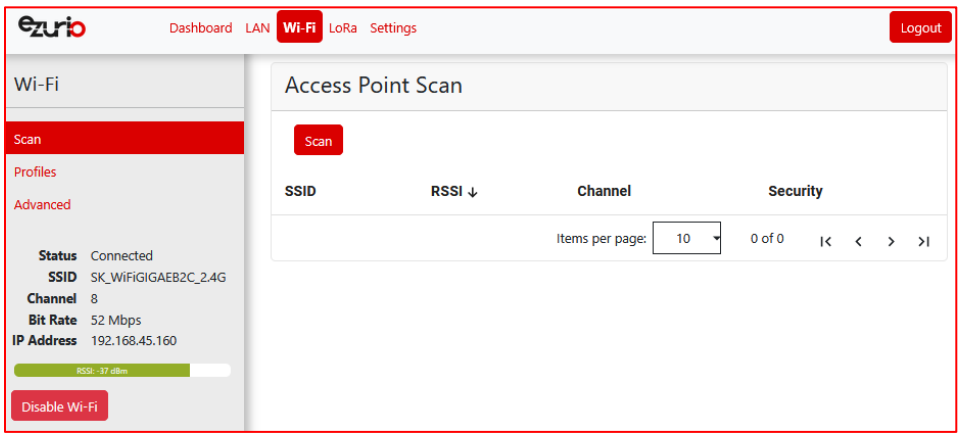


Figure 21: Wi-Fi connection setup

In the sidebar on the left, you can navigate to various Wi-Fi pages and see the status of the Wi-Fi interface. There is also a button to enable/disable the Wi-Fi radio.

7.1 Use Scan to Add a Profile

To use the scan function to add a profile, follow these steps:

1. **Connect to a Wi-Fi network** – click **Scan** to scan for nearby Wi-Fi networks. Scanning continues until you click **Stop** or click on one of the listed scan results (Figure 22).

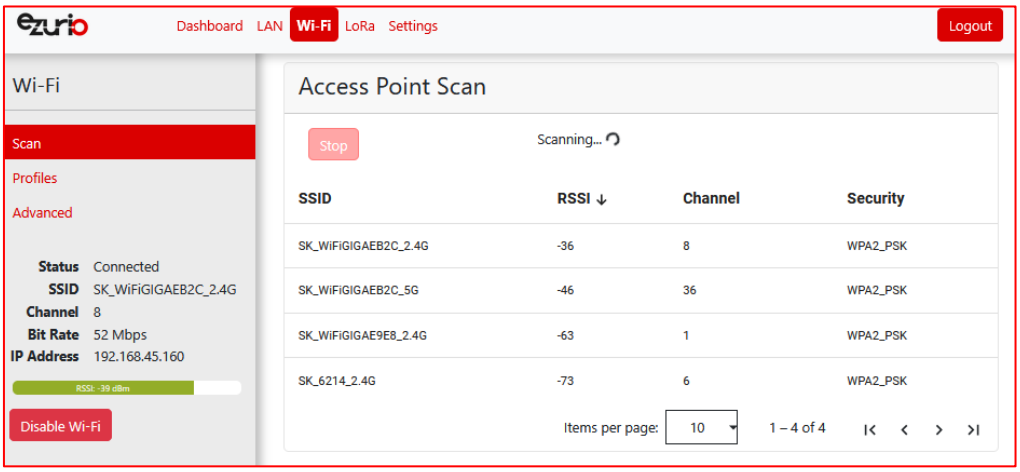


Figure 22: Scan function

2. Click on the applicable scan result.

3. In the Wi-Fi profile window, enter the appropriate credential information for your chosen Wi-Fi network (Figure 23).

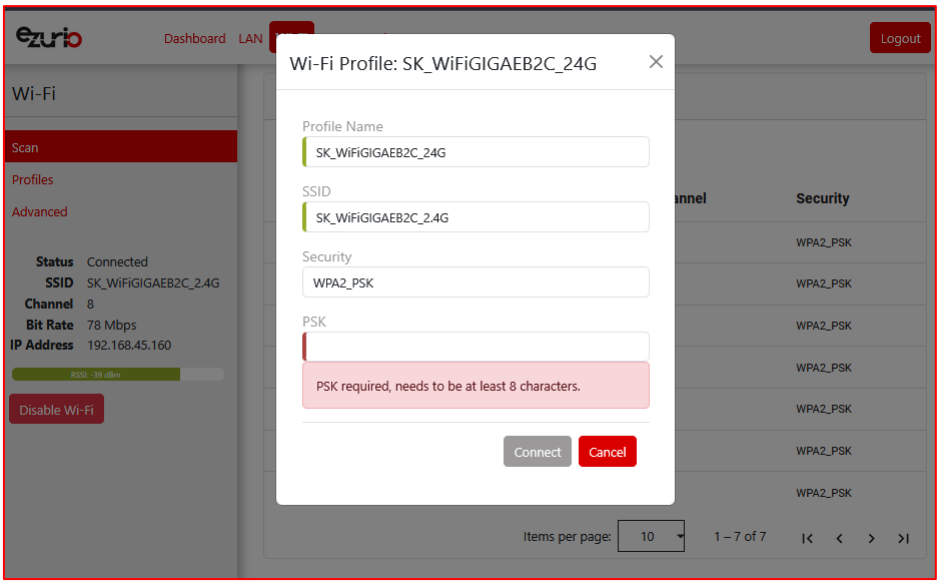


Figure 23: Wi-Fi profile window

7.2 Manually Adding a Profile

To add a Wi-Fi network profile manually, follow these steps:

1. Click the **LAN** button in the main menu, then click the **Profiles** button on the top. This page is useful for adding a hidden Wi-Fi network that is not broadcasting its SSID (Figure 24).

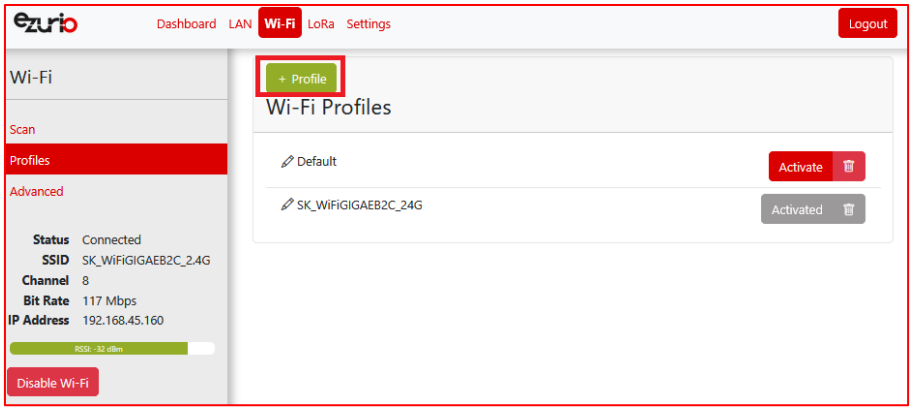


Figure 24: Wi-Fi profiles page

The profile page shows all Wi-Fi profiles that are saved in the gateway. You can add, activate, or delete the profiles shown on this page.

2. Click **+ Profile** to display the Wi-Fi profile dialog (*Figure 25*).

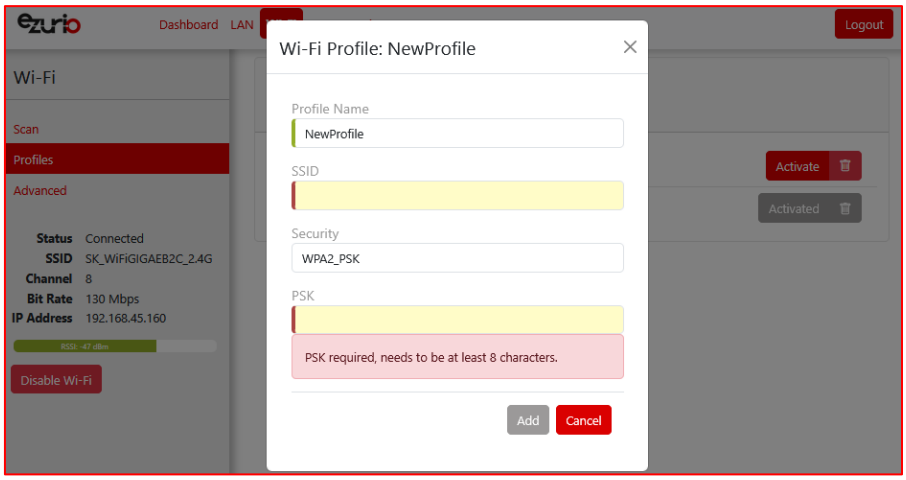


Figure 25: Wi-Fi profile dialog

3. Enter the appropriate information for the new profile.
4. Click **Add**.

7.3 Wi-Fi Advanced Page

The Wi-Fi advanced page shows more detailed information about the Wi-Fi radio status and allows the user to configure the Quick Config AP mode password (Figure 26).

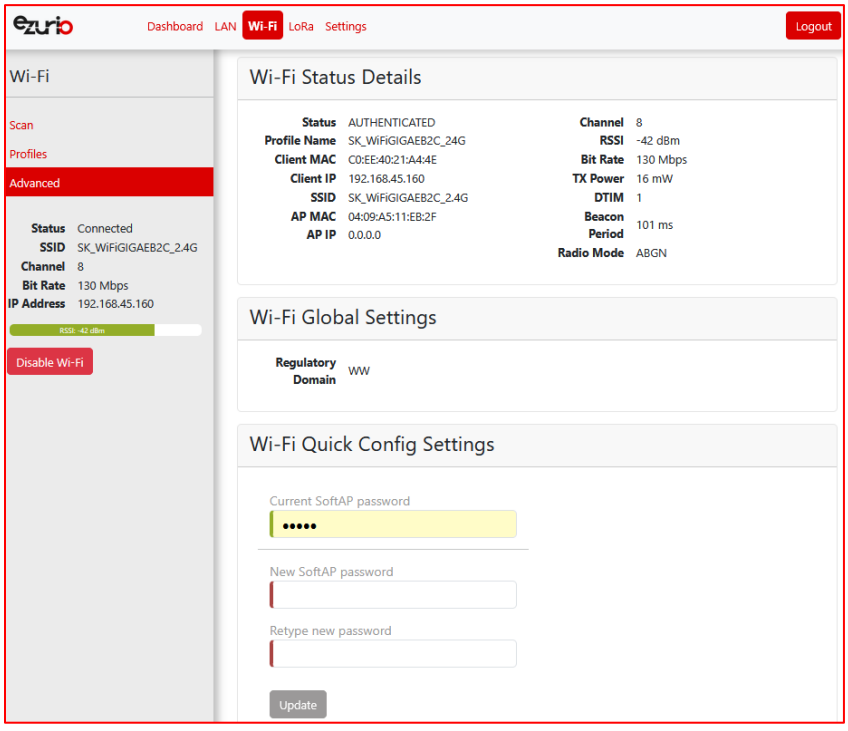


Figure 26: Wi-Fi Advanced page

8 LoRa Connection Setup

The side panel for the LoRa Gateway allows selections for configuration and status of the LoRa network card. The status of the LoRa Network is also displayed (Figure 27).

Note: *The LoRa Region Code is displayed here. Be sure that the gateway you are operating matches the region in which you are operating it.*

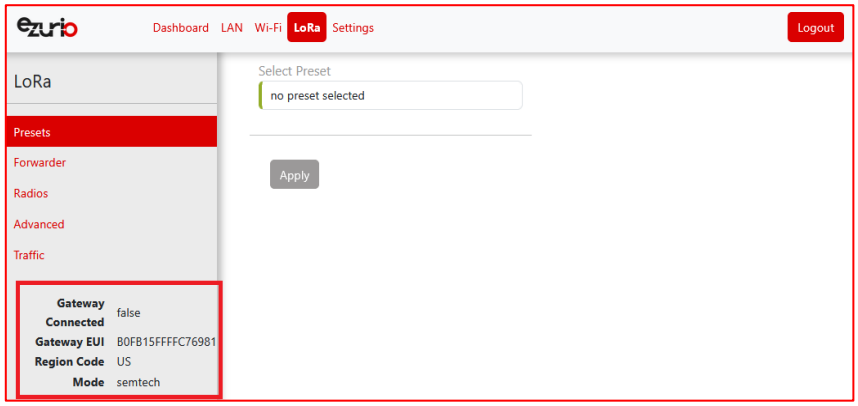


Figure 27: LoRa connection setup page

The Gateway ID (also known as the gateway DevEUI), is used to uniquely identify the RG1xx gateway. It is required when registering the gateway on a LoRa network server. The gateway EUI is also printed on the bottom label of the gateway, with the label *M2 EUI or DevEUI*.

Figure 28: Gateway label (Standard GW – Left, AS923 & AU915 Region Supported/Latest Version – Right)

8.1 Using Presets

The **Sentrius™ RG1xx** contains multiple preset configurations for connecting to a third-party server or as the basis for a private network. These presets configure the forwarder and the channel plan.

To apply a preset configuration, follow these steps:

1. Click the **LoRa** tab in the main menu. The default page of the LoRa menu is the **Presets** page (also accessible in the left side menu of the LoRa pages).
2. Select the preset from the drop down. Information about this preset is displayed in a panel to the right (Figure 29).
3. Click **Apply** to apply the preset configuration. After a few moments, a green confirmation appears on the bottom of the page.

Note: After applying a preset, further changes can be made on the other screens. Some presets use a custom forwarder and may not be modified.

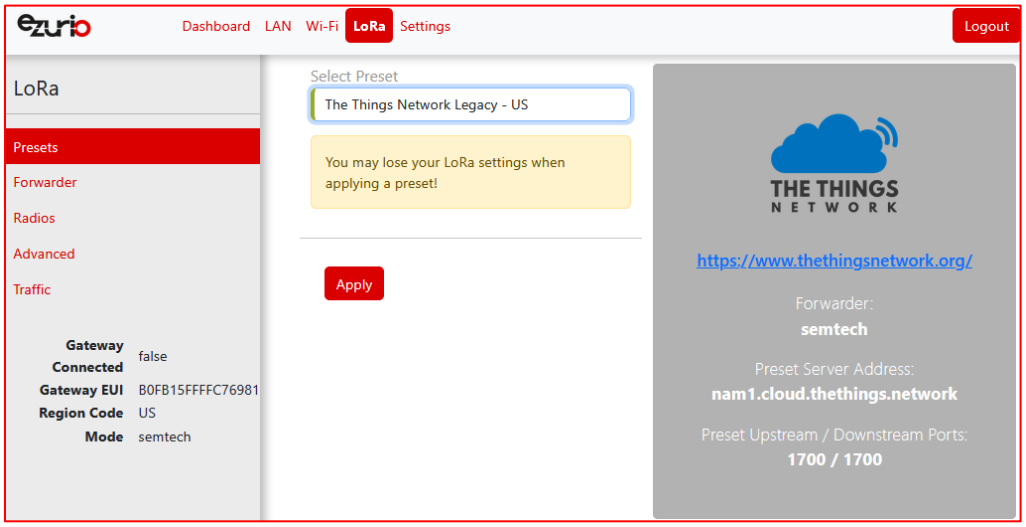


Figure 29: Selecting a preset configuration

8.2 Semtech Basic Station

Semtech's Basic Station replaces most other forwarders that were included in prior releases of the gateway. Basic station uses secure web sockets to communicate with the LoRa Network Server. It also has the capability to connect to a CUPS server to allow the device to configure the LNS connection remotely. All configuration settings beyond this are handled by the Lora Network Server. This includes the channel plan. An appropriate channel plan must be selected in the LNS that corresponds to the region of operation for your specific gateway.

8.2.1 Mode

The forwarder page allows configuration of the packet forwarder. The mode allows the user to change to different packet forwarders.

8.2.2 Servers

The user must enter in a valid LNS server to allow for operation as a packet forwarder. The CUPS servers are optional but should be kept blank if you do not want to communicate with the CUPS servers to provision the LNS certificates.

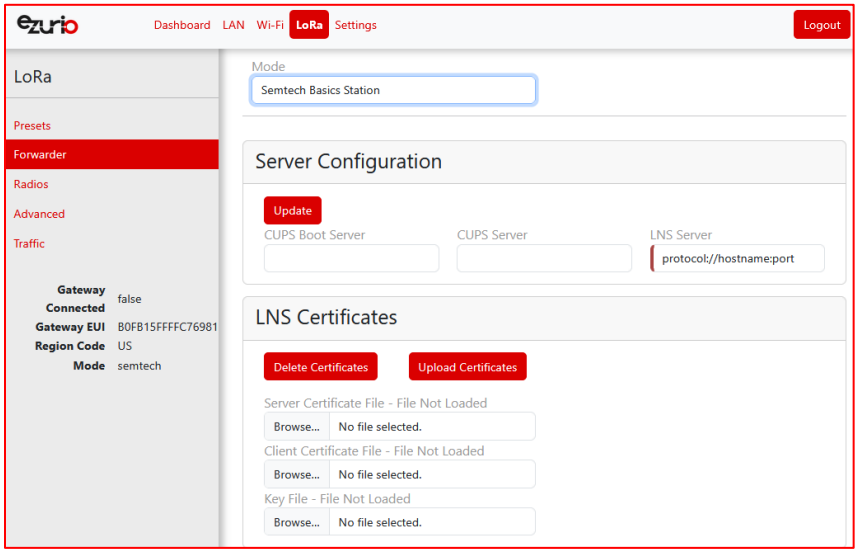


Figure 30: LNS server

8.2.3 Certificates

Each of the three servers has a set of certificates used to authenticate the server to the gateway and the other way around. It is possible to function in a mode where only the server is authenticated with the gateway in which case you would only install the server certificate.

To select a certificate, follow these steps:

1. Click **Choose File**.
2. Select the desired .pem file and press upload.

You can optionally select to upload your client certificate and key files when necessary.

All files can be uploaded at once with one click of the Upload Certificate button. After uploading the Basic Station restarts and should attempt to connect to the server. You may also delete the certificates for each server by pressing **Delete Certificate**. This clears out all three files at once for the server. The text box indicates which files are already present.

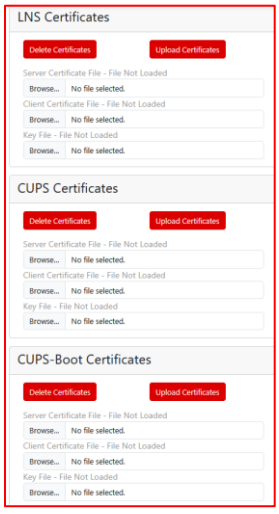


Figure 31: Certificate selection

8.2.4 Connection Status

8.2.4.1 LoRa View

The status of the connection to the LNS is shown on the sidebar when in the LoRa view.

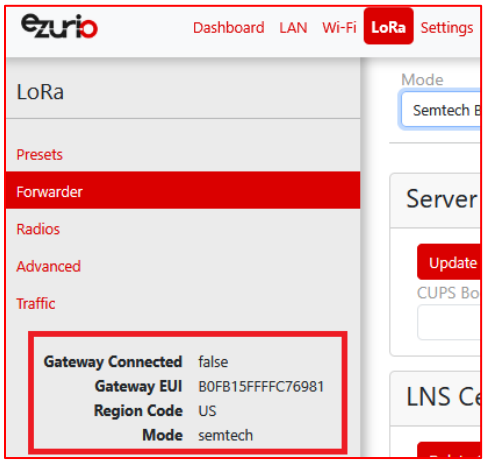


Figure 32: LoRa view

8.2.4.2 Dashboard View

In the Dashboard view, the status is shown with a circle that will be green when connected and black when disconnected.

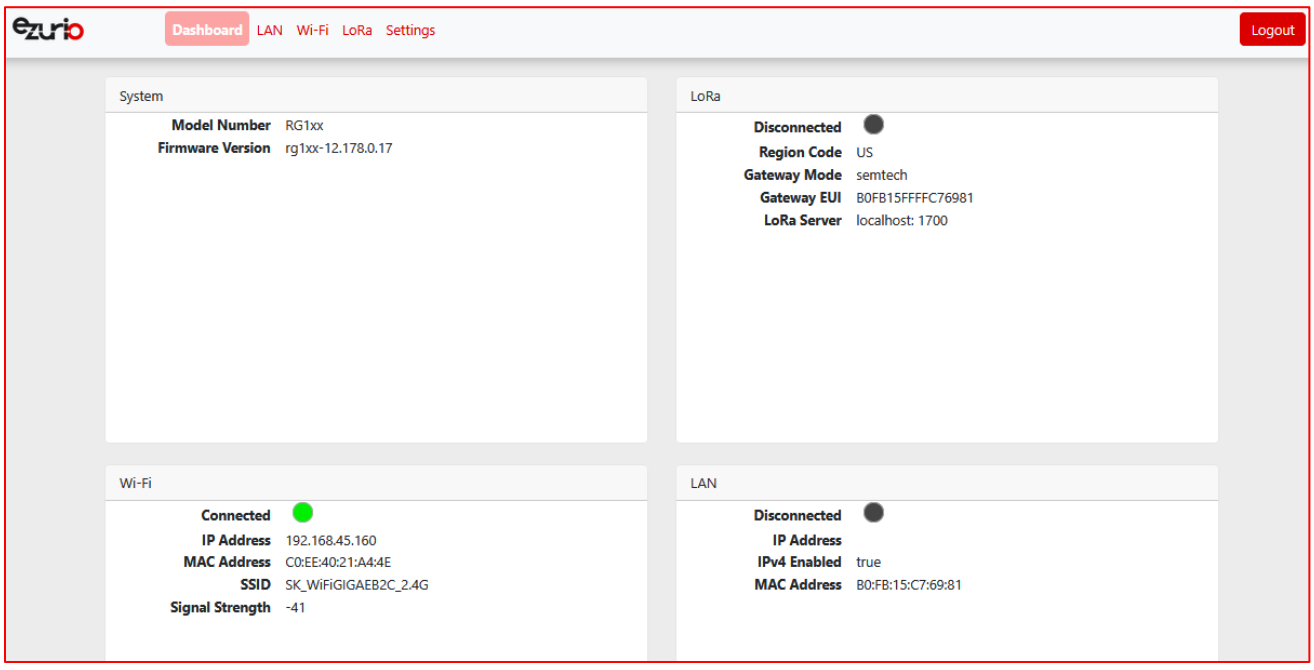


Figure 33: Dashboard view

8.3 Senet

Senet provides two modes of operation: Senet DEV and Senet RAN. In Senet DEV mode the web UI is enabled. **When in Senet RAN mode, the Web UI is disabled and the only way out of that mode is by performing a factory reset** (see Factory Reset section). After a factory reset, you must contact Senet to be able to reconnect the gateway with the same EUI.

8.4 Semtech Legacy UDP Forwarder

NOTE: This forwarder should not be used for production purposes. Contact Ezurio if you have questions.

Click **Forwarder** in the left-hand menu of the LoRa pages to access the Forwarder settings.

8.4.1 Mode

The forwarder page allows configuration of the packet forwarder. The mode allows the user to change to different packet forwarders.

8.4.2 Configuration

The configuration changes based on what packet forwarder is used.

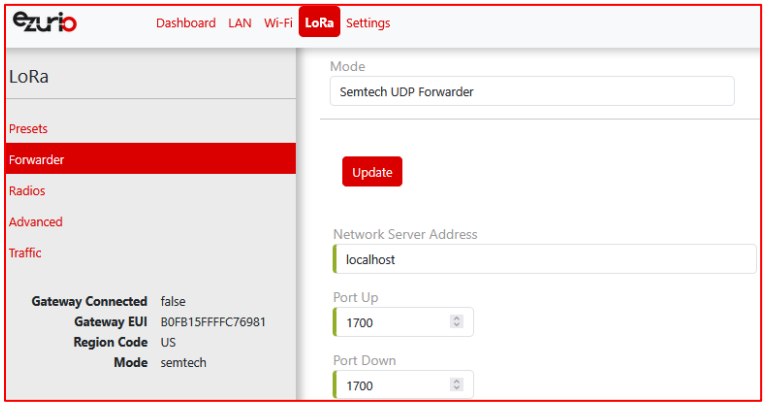


Figure 34: Semtech packet forwarder configuration

8.4.3 Radios

The radio page provides configuration of the radios and channels. The LoRa card has two radios (Radio 0 and Radio 1). This interface allows advanced users to change radio and channel assignments within the allowed range per the gateway region. Depending on the forwarder being used, the radio configuration may not be available.

8.4.3.1 Channel Plan Graphic

At the top of the Radios page is a graphic representation of the full bandwidth range, channels, and radios. This graphic is different for gateways operating in US mode and EU mode.

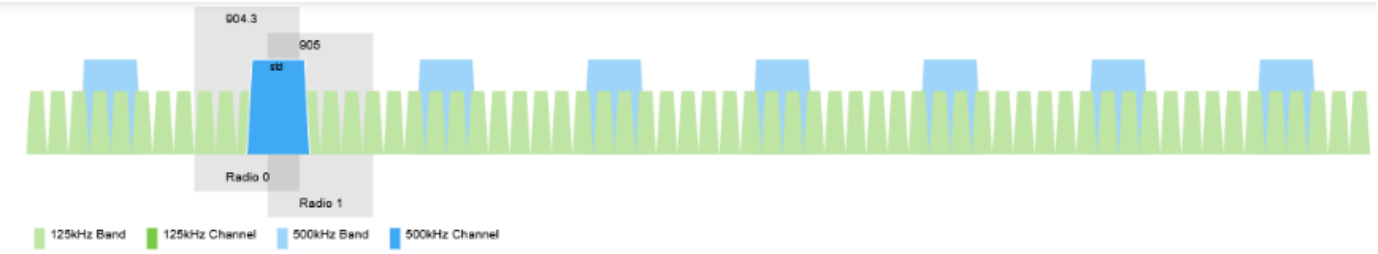


Figure 35: Channel plan graphic

8.4.3.2 Radio Center Frequencies

Each radio is assigned a center frequency. Channels are then assigned to each radio and given an offset from the center (Figure 36).

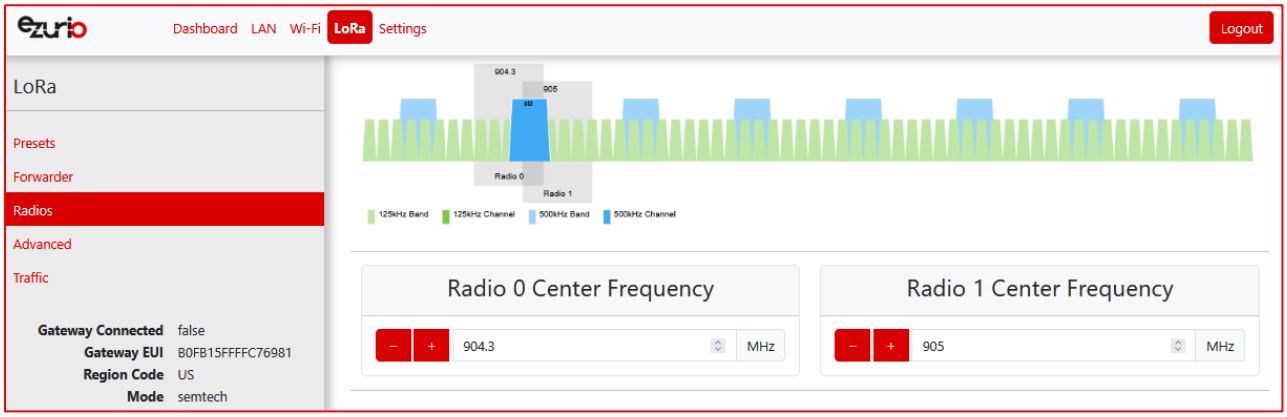


Figure 36: Channel assignments

8.4.3.3 Channels

Channels are enabled and assigned to either radio. Each radio can have up to five channels assigned to it.

The channel's frequency is an offset of its radio's center frequency. For most channels with a 125-kHz bandwidth, the offset can be -0.4 to +0.4 MHz.

LoRa STD and FSK channels have configurable bandwidth. For these channels, when operating in 250-kHz or 500-kHz bandwidth, the offset can be -0.3 to +0.3 MHz.

Each channel should be placed at least 200 kHz from any other channel, otherwise the channel's bandwidth overlaps. While this configuration still functions, there is wasted bandwidth. The interface displays a warning and marks each channel in red if they overlap (Figure 38). Channel configuration is shown in Figure 37.

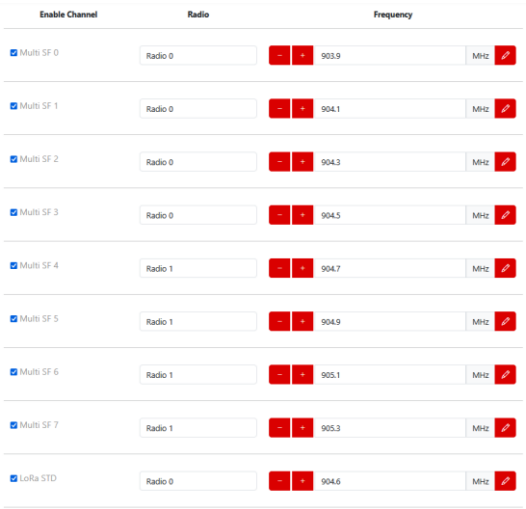


Figure 37: Channels window

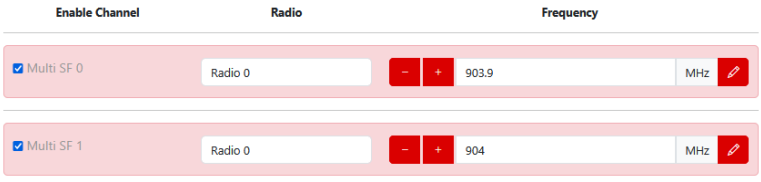


Figure 38: Overlapping channels

8.4.3.4 LoRa Radio Card (US)

Gateways that operate in the US region should have a 500-kHz channel. In Figure 39, the allowed placement of these channels displays larger and blue.

If a 500-kHz channel is not configured, the interface displays a warning.

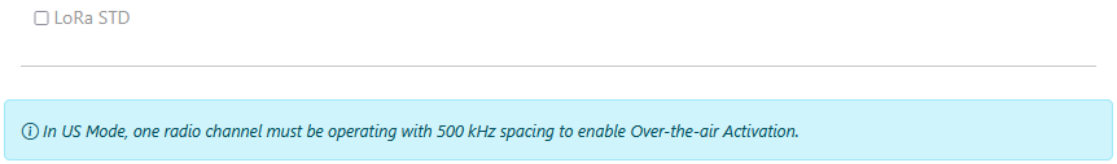


Figure 39: US region gateways

8.4.3.5 LoRa Radio Card (EU)

There are three mandatory channels for gateways that operate in the EU region. These channels are 868.1, 868.3, and 868.5.

The EU region bands have different duty cycles. This is indicated with a grey background box and label in Figure 40. A higher duty cycle allows higher throughput.

The EU region specifies *keep out* areas in the allowed frequencies. These are highlighted in red on the illustration. The interface displays a warning if a channel lies in a keep-out area.

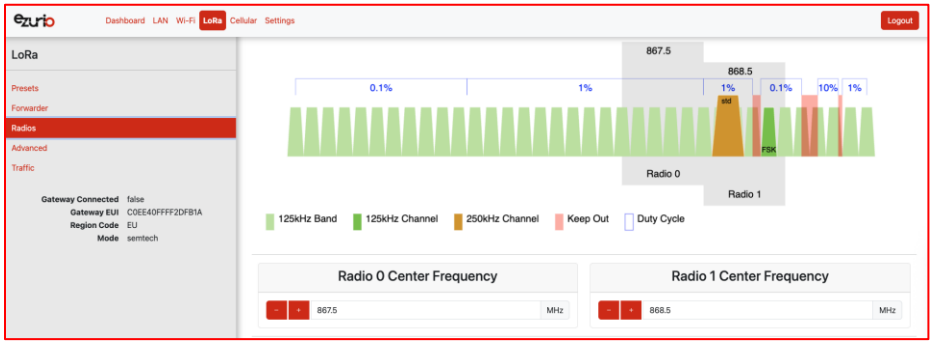


Figure 40: EU region gateways – keep out channels

8.4.4 LoRa Radio Card (Australia)

If the gateway is the Australia variant, the user may toggle between the AU915 and AU923 regions through the web UI on the gateway. A factory reset must be performed on the device after toggling between AU915 and AU923. No other regions are end-user selectable.

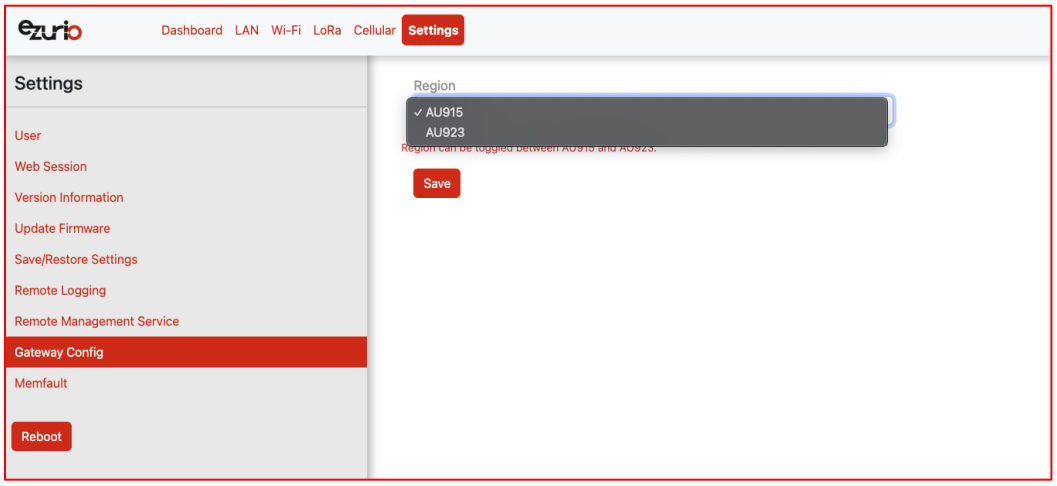


Figure 41: Australia region selector

8.4.4.1 AU915

The region code is AU915. This is not an AS923 region with no mandatory channel requirements. The firmware will restrict the operation to the legal regulatory limits for this region. These limits include frequency, duty cycle, dwell time, and power restrictions. If the network server requests to transmit in an illegal manner, the packet will be dropped. In the case of TX power, the TX power will be clipped to the highest allowable power if the requested power exceeds the legal limit for this region.

8.4.4.2 AU923

The region code is AU923. This is an AS923 region, therefore there are two mandatory channels: 923.2 and 923.4. The firmware will restrict the operation to the legal regulatory limits for this region. These limits include frequency, duty cycle, dwell time, and power restrictions. If the network server requests to transmit in an illegal manner, the packet will be dropped. In the case of TX power, the TX power will be clipped to the highest allowable power if the requested power exceeds the legal limit for this region.

8.4.5 LoRa Radio Card (New Zealand)

The region code is NZ. This is an AS923 region, therefore there are two mandatory channels: 923.2 and 923.4. The firmware will restrict the operation to the legal regulatory limits for this region. These limits include frequency, duty cycle, dwell time, and power restrictions. If the network server requests to transmit in an illegal manner, the packet will be dropped. In the case of TX power, the TX power will be clipped to the highest allowable power if the requested power exceeds the legal limit for this region.

8.4.6 LoRa Radio Card (Taiwan)

The region code is TW. This is an AS923 region, therefore there are two mandatory channels: 923.2 and 923.4. The firmware will restrict the operation to the legal regulatory limits for this region. These limits include frequency, duty cycle, dwell time, and power restrictions. If the network server requests to transmit in an illegal manner, the packet will be dropped. In the case of TX power, the TX power will be clipped to the highest allowable power if the requested power exceeds the legal limit for this region.

8.4.7 LoRa Radio Card (Hong Kong)

The region code is HK. This is an AS923 region, therefore there are two mandatory channels: 923.2 and 923.4. The firmware will restrict the operation to the legal regulatory limits for this region. These limits include frequency, duty cycle, dwell time, and power restrictions. If the network server requests to transmit in an illegal manner, the packet will be dropped. In the case of TX power, the TX power will be clipped to the highest allowable power if the requested power exceeds the legal limit for this region.

8.4.8 LoRa Radio Card (Singapore)

The region code is SG. This is an AS923 region, therefore there are two mandatory channels: 923.2 and 923.4. The firmware will restrict the operation to the legal regulatory limits for this region. These limits include frequency, duty cycle, dwell time, and power restrictions. If the network server requests to transmit in an illegal manner, the packet will be dropped. In the case of TX power, the TX power will be clipped to the highest allowable power if the requested power exceeds the legal limit for this region.

8.5 Advanced Configuration

The Advanced page provides additional configuration options for the specific forwarder.

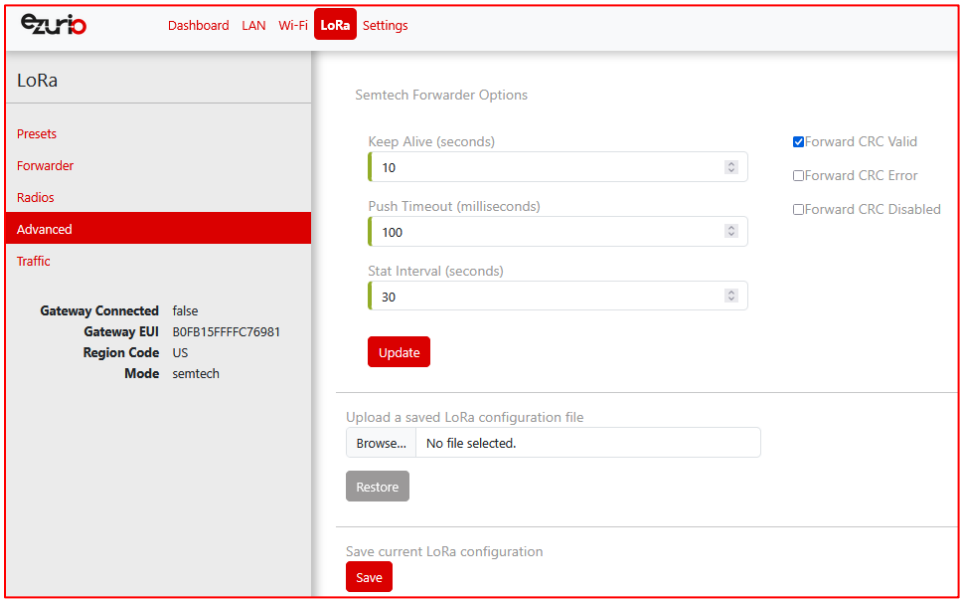


Figure 42: Advanced configuration page

The current configuration may be saved as a JSON text file. This file can also be uploaded to restore the saved configuration. This feature is useful for configuring multiple gateways with the same configuration (Figure 43).

Note: If the forwarder settings contain credentials, these are not saved in the configuration file for security reasons. **The user must take care to set the appropriate credentials when restoring the saved configuration to a gateway**.

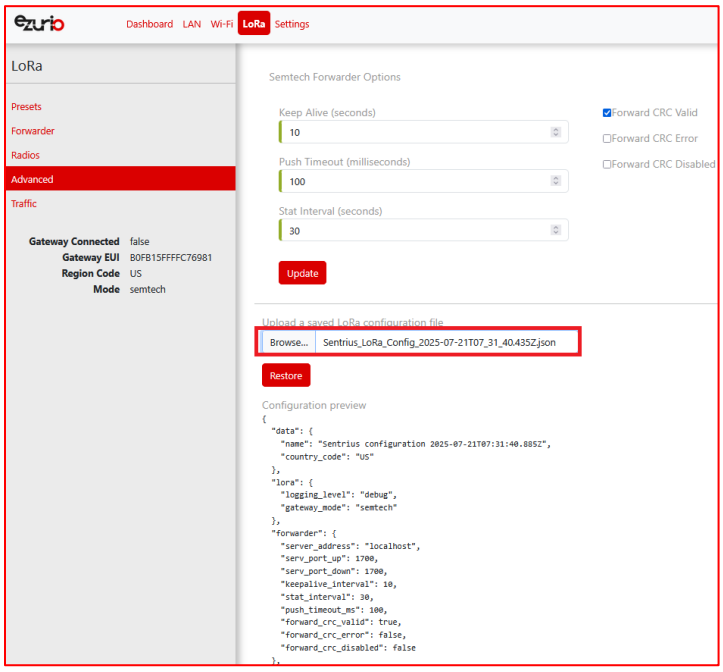


Figure 43: Current configuration file

8.6 Traffic

The traffic page is only available when using certain forwarders. When navigating to the traffic page, any recent traffic that has been seen by the gateway displays. To watch live traffic, click **Poll Traffic**. Traffic columns can be sorted, and filters can be applied to one column at a time.

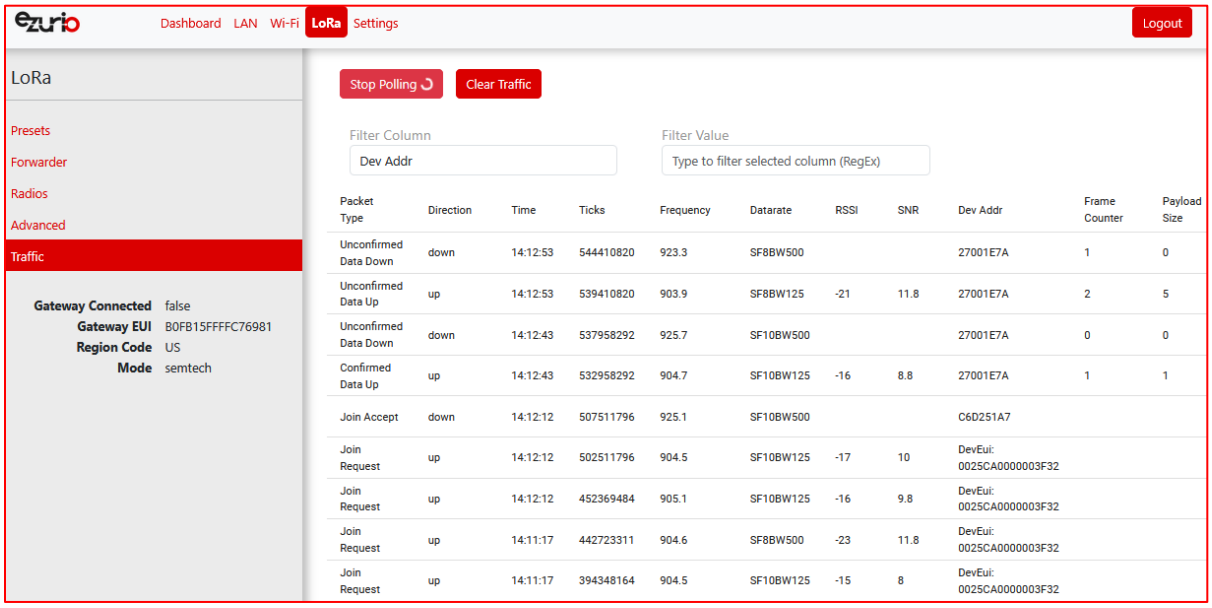


Figure 44: LoRa traffic

Clicking on a traffic row displays packet details.

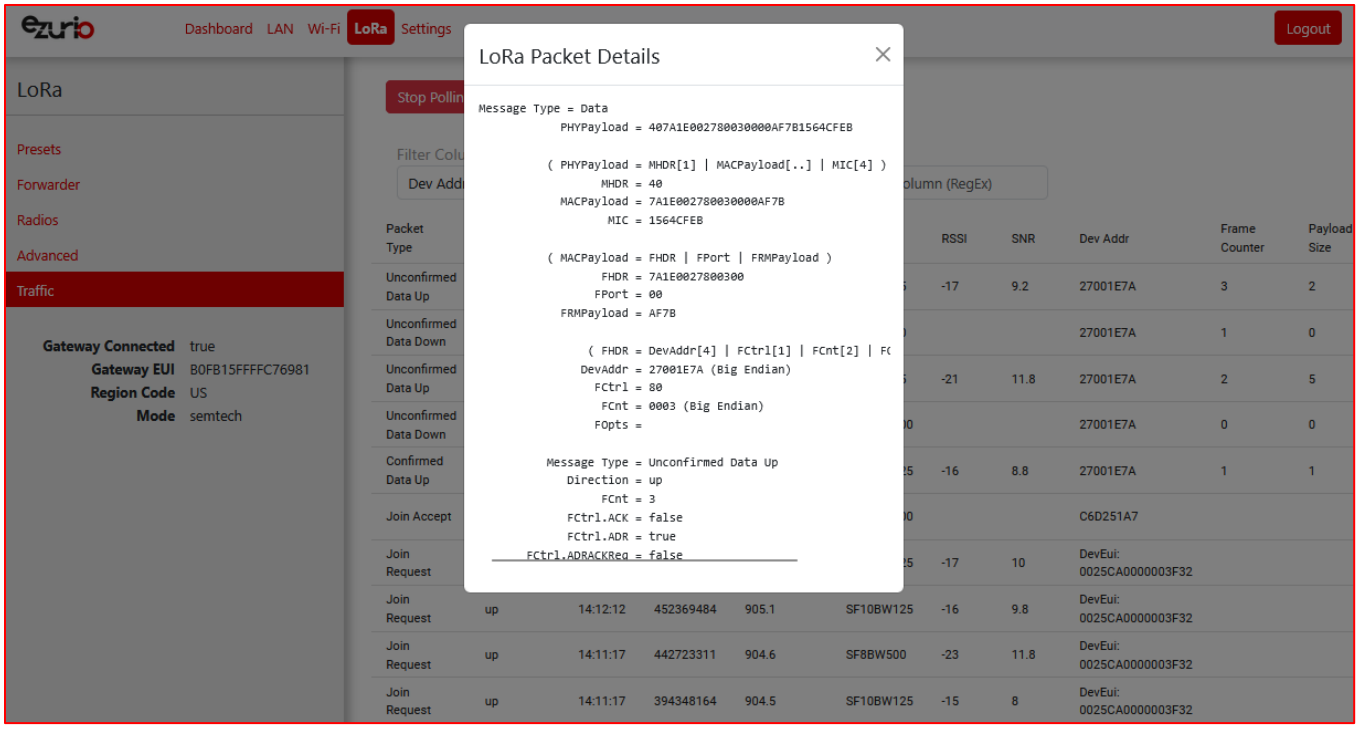


Figure 45: LoRa packet details

9 Manage the Gateway

9.1 Changing Username and Password

To change the login credentials of the gateway, follow these steps:

1. In the main menu, click the **Settings** tab. Then in the left menu, click the **User** tab (Figure 46).
2. Enter the current password, and then the new desired username and password.
3. Click **Update**.

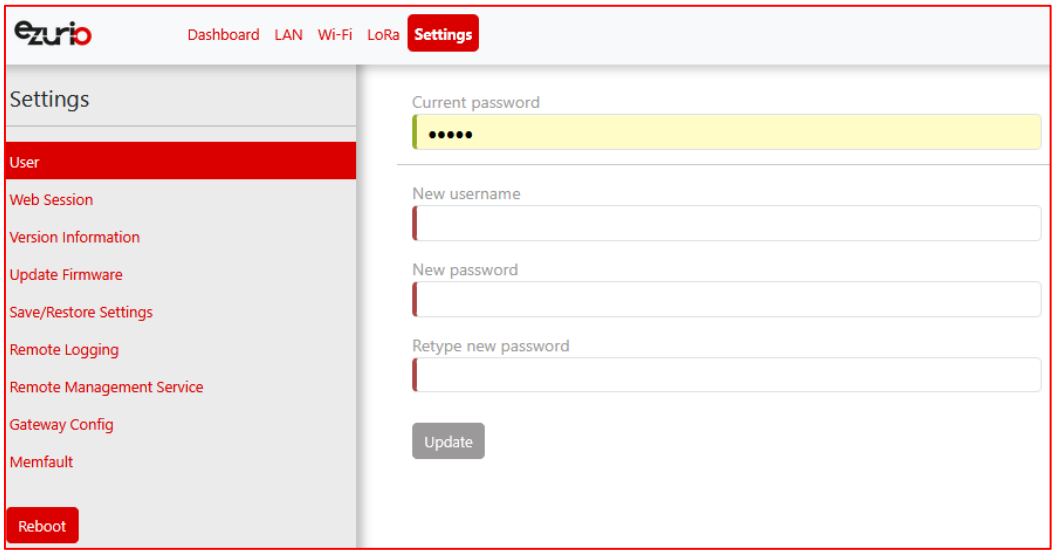


Figure 46: Change username and password

9.2 Web Session

The user can change the web session timeout. The web session timeout is the amount of time before the user will be warned and automatically logged out if there is no web activity. Activity is defined as navigating between pages, changing any settings, or polling LoRa traffic. The minimum time, and default, is 5 minutes and the maximum time is 60 minutes. When polling LoRa traffic, the time is set to the maximum of 60 minutes. When polling is stopped, the time out is set back to the saved setting.

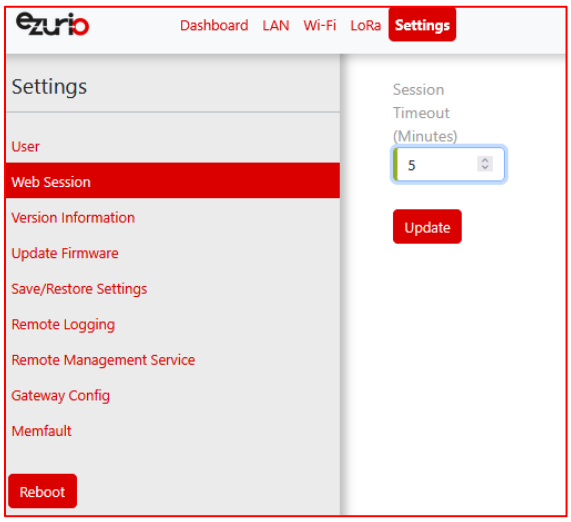


Figure 47: Change web session time out

9.3 Version Information

The **Settings** › **Version Information** page shows detailed software/firmware information of various components in the gateway.

The Build string is the overall firmware version for the gateway software package.

If a firmware update is available a New Build Available row is displayed.

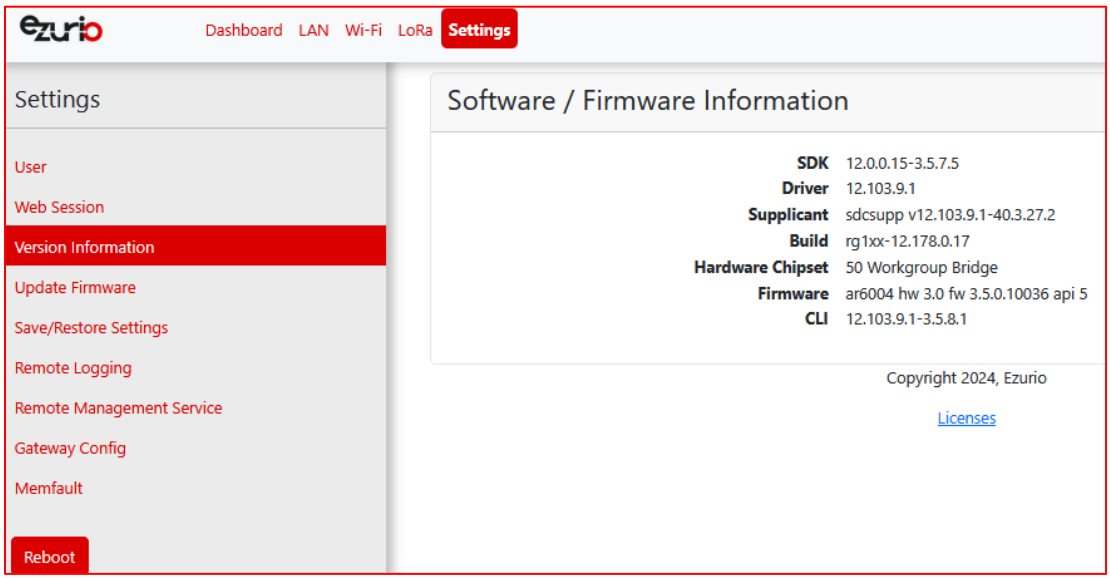


Figure 48: Version information

9.3.1 Modem Version Information

Note: This information is only available with the RG191+LTE hardware for the US market only, see Ordering Information for product part numbers.

The **Cellular** › **Status** page shows detailed software/firmware information of the cellular modem in the gateway.

The **Firmware Revision** string is the firmware version for the LTE modem software package.

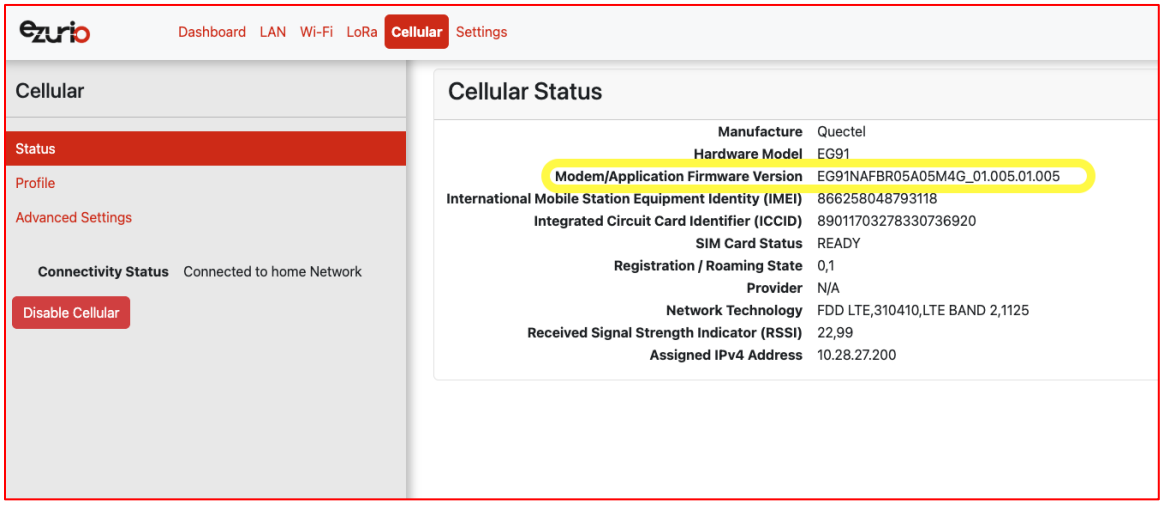


Figure 49: Modem Version information

9.4 Updating Gateway Firmware

To update the firmware in the gateway, follow these steps:

Warning: Updating the firmware ***MAY*** restore the gateway to factory default settings. We advise you to save/backup or make note of any settings the user does not wish to lose beforehand.

1. Click the **Settings** tab in the main menu. Then click **Update Firmware** in the left menu.
2. Enter the proper URL. Information about which URL is to be used can be found below.
3. Click **Start Update**.

   The firmware update process downloads the firmware to the gateway and then flashes it.

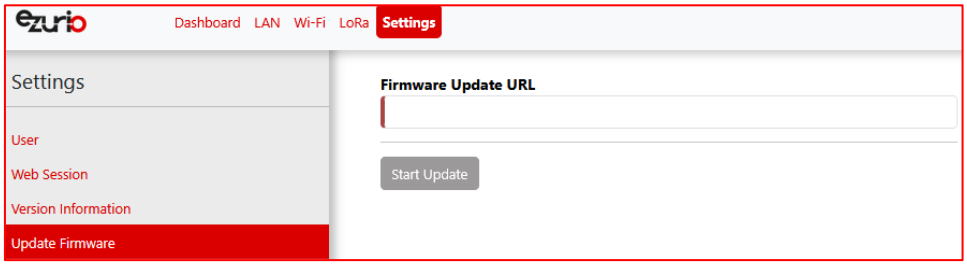


Figure 50: Updating gateway firmware window

During the firmware update, the progress displays as shown in (Figure 51).

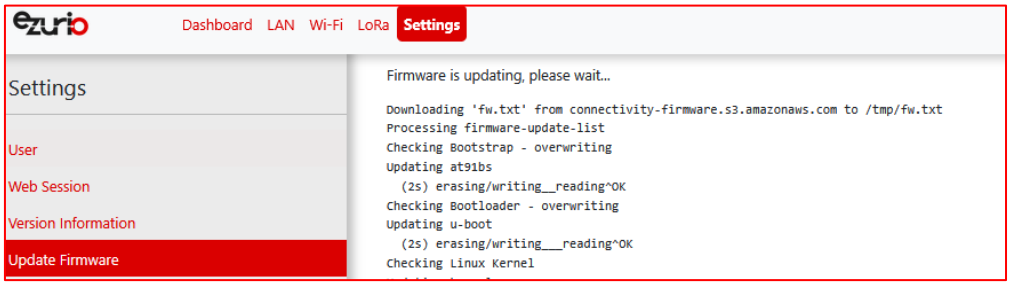


Figure 51: Progress indicator

4. At the end of the update, you are prompted to reboot the gateway.

Click **Reboot**. The gateway must be rebooted for the update to take effect (Figure 52).

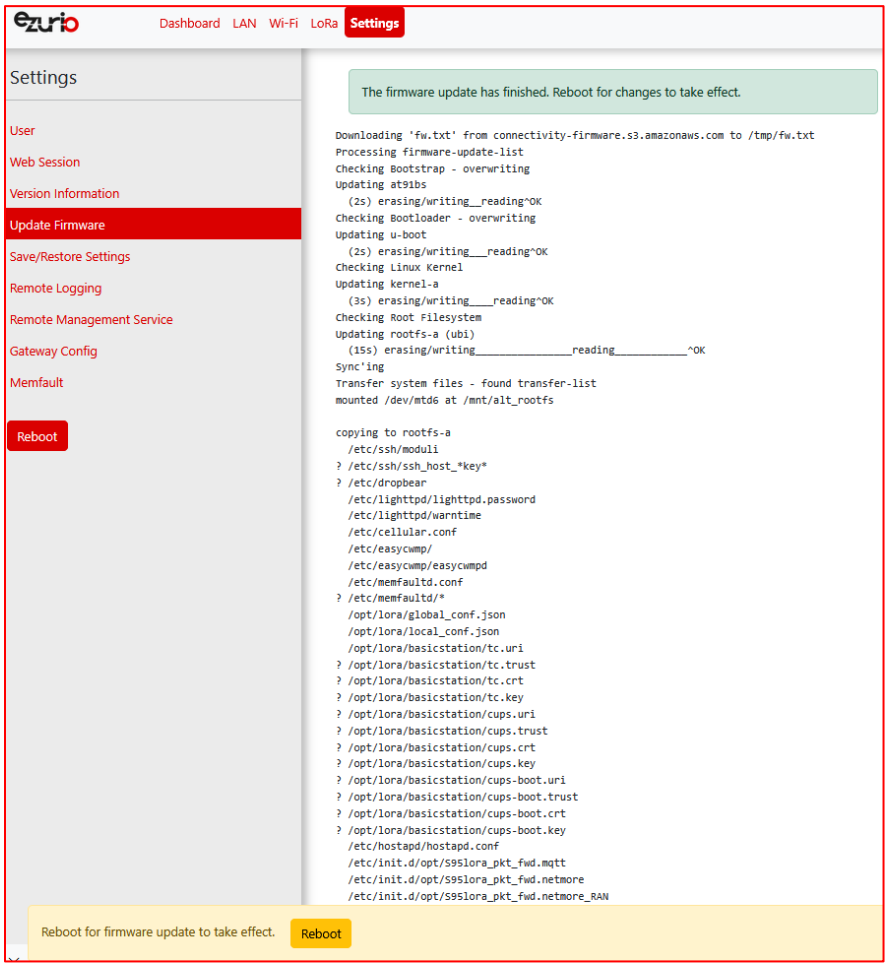


Figure 52: Reboot prompt

9.4.1 Firmware Update URLs

IMPORTANT: Please follow the instructions based on the firmware version ***currently*** running on the gateway.

9.4.1.1 93.7.1.13 (GA1) Firmware

If the gateway is running version **93.7.1.13** firmware the user should use this link to upgrade to the next version:

https://www.ezurio.com/products/rg1xx-lora-gateway/firmware/GA1.1/fw.txt

After updating with this link, the gateway will be running version 93.7.1.14. Follow the instructions for that version to update to the latest version of firmware.

9.4.1.2 93.7.1.14 Firmware

If the gateway is running version **93.7.1.14** firmware the user should use this link to upgrade to the next version:

https://www.ezurio.com/products/rg1xx-lora-gateway/firmware/GA2.1/fw.txt

After updating with this link, the gateway will be running version 93.7.2.10. Follow the instructions for that version to update to the latest version of firmware.

WARNING: This upgrade performs a factory reset on the gateway.

9.4.1.3 93.7.2.9 (GA2) Firmware

If the gateway is running version **93.7.2.9** firmware the user should use this link to upgrade to the next version:

https://www.ezurio.com/products/rg1xx-lora-gateway/firmware/GA2.1/fw.txt

After updating with this link, the gateway will be running version 93.7.2.10. Follow the instructions for that version to update to the latest version of firmware.

WARNING: This upgrade performs a factory reset on the gateway.

9.4.1.4 93.7.2.10 (GA2.1) Firmware

If the gateway is running version **93.7.2.10** firmware the user should use this link to upgrade to the latest version:

https://www.ezurio.com/products/rg1xx-lora-gateway/firmware/newest/fw.txt

---

Note: This requires users to manually update the URL!

9.4.1.5 93.7.3.4 (GA3) Firmware and Newer

GA3 firmware (93.7.3.x) and newer versions have a feature to automatically notify the user if new firmware is available and what link to download the firmware from.

9.4.1.6 GA4 Firmware (93.8.4.28)

9.4.1.7 GA4.1 Firmware (93.8.4.37)

9.4.1.8 GA5 Firmware (93.8.5.18)

9.4.1.9 GA5.1 Firmware (93.8.5.21)

9.4.1.10 GA5.2 Firmware (93.8.5.25) - Engineering Release

9.4.1.11 GA6 Firmware (93.9.6.12)

9.4.1.12 GA6.1 Firmware (93.9.6.14)

9.4.1.13 GA6.2 Firmware (93.9.6.30)

9.4.1.14 GA6.3 Firmware (93.9.6.44)

9.4.1.15 GA6.4 Firmware (93.9.6.57)

9.4.1.16 GA6.5 Firmware (93.9.6.77)

9.4.1.17 GA8 Firmware (12.178.0.18) - Latest Production Release.

https://connectivity-firmware.s3.amazonaws.com/rg1xx-lora-gateway/firmware/newest/fw.txt

9.5 Save/Restore Settings

All the settings in the gateway can be saved and restored. This is useful for backing up all settings before a factory reset or firmware upgrade. Settings are saved to a JSON file and can be restored on another gateway.

Note: Any security related settings like credentials and security certificates are not saved in the JSON file for security reasons. That means security-related settings cannot be restored onto a separate gateway. Security related settings are only saved on the current gateway and can be restored on the same gateway.

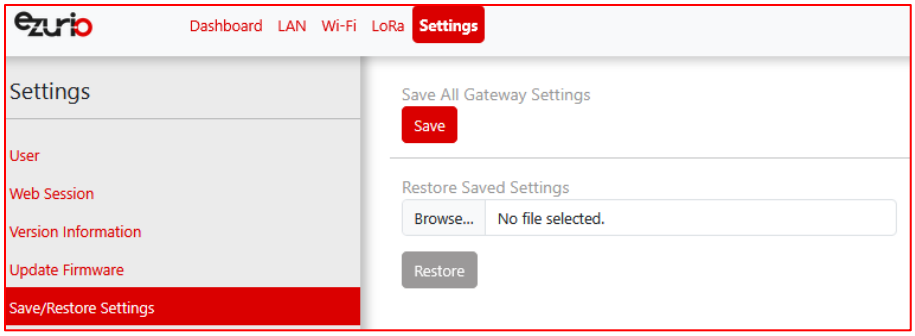


Figure 53: Save/Restore settings

After restoring settings, the gateway must be rebooted for changes to take effect.

9.6 Remote Management

The gateway can be managed remotely via TR-069. It requires an externally hosted Auto Configuration Server (ACS) to use this feature. This allows a system administrator to access the gateways without needing physical access to the gateway or access behind a firewall. The gateway will periodically initiate connections with the ACS allowing a user to remotely update LoRa configuration settings, update firmware, download logs, etc.

9.6.1 Configuring the Gateway for Remote Management

The user must point the device to your external ACS. This is done under **Settings > Remote Management Service**.
This is a one-time setting that is preserved across firmware updates.
The URL must be updated, including the port number. In a standard ACS installation, this is usually **port 7547** but that can vary. Consult your ACS provider for the URL, port number, username, and password. The username and password fields are for connections initiated by the gateway. Not for connections initiated by the ACS. The parameter key is optional. Press the update button when all parameters are correctly entered.

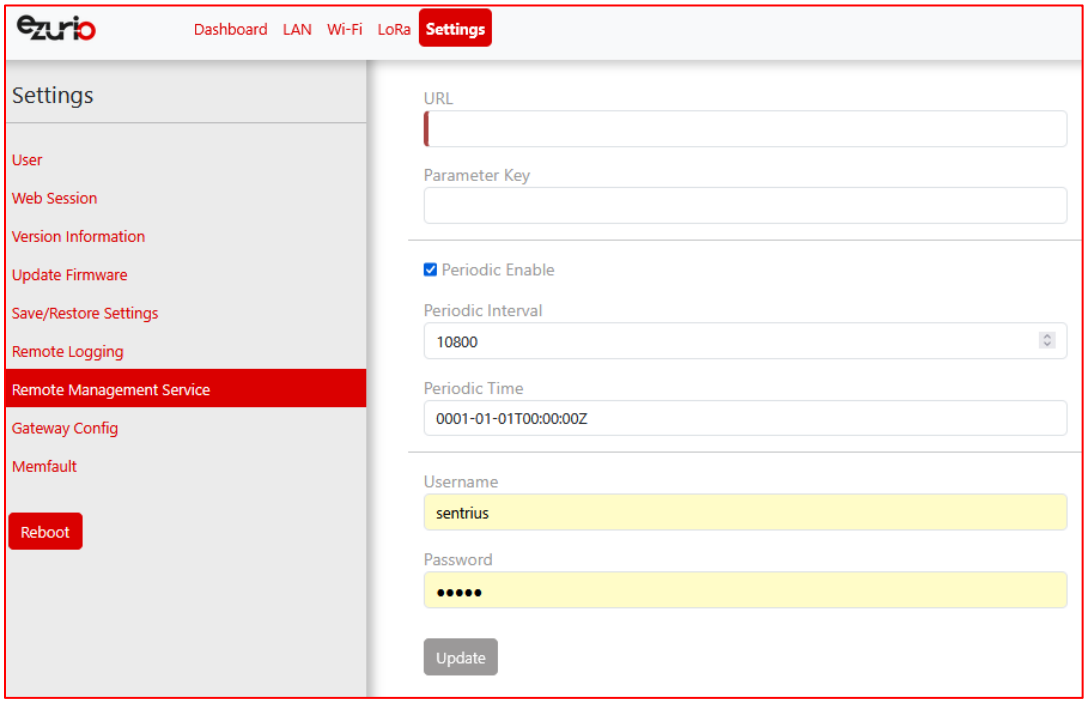


Figure 54: Save/Restore settings

9.6.2 Updating Firmware Remotely

This works much like it does with the web User Interface (UI). When the system administrator has a new firmware release to load, they will update the InternetGatewayDevice.Rfpros.GatewayManagement.Versions.FirmwareUpdateURL. The value is the link to download the firmware. This link always points to a fw.txt file. Once that is done, the gateway will respond with success and download the firmware in the background. A remote user would then poll for InternetGatewayDevice.Rfpros.GatewayManagement.Versions.FirmwareUpdateStatus to be set to "1" indicating that the firmware was successfully downloaded and is ready to reboot to switch to the new firmware. The system administrator would then issue the TR-069 "Reboot" command to reboot the device. After the reboot, the gateway will check in again and be running the new version. Note that settings (including remote management) are preserved across a firmware update.

9.6.3 Configuration File Upload

9.6.3.1 Configuration Files

Configuration files and certificates can be uploaded to the device. These configuration files are called '**vendor configuration files**' in TR-069 terminology. An ACS can be commanded to push these to a device or group of devices. The vendor configuration file can change a number of settings in bulk. It is useful to (re)configure a batch of new devices in the field. These settings include, LAN, WiFi, and LoRa radio settings (including the channel plan and other radio settings).
A strategy to deploy configurations to the field is to modify a unit locally to the way you want it. Download the configuration file via TR-069 from a locally configured gateway, then upload that generated configuration file to be pushed to all the units once the system administrator is satisfied that all of the settings are correct on the 'golden unit'. A download is initiated by the ACS with the type "**3 Vendor Configuration File**", and an upload is also initiated by the ACS with the type "**3 Vendor Configuration File**". The ACS will not put a file extension on the downloaded file. It is a compressed tarball (.tar.gz) file.
See the documentation for your ACS to determine how to initiate the '**3 Vendor Configuration File**" upload command.

9.6.4 Configuration File Download

9.6.4.1 Log File

Initiate a download by the ACS with type ***2 Vendor Log File***. This returns the log data. The same log data that can be obtained by the web interface. It is viewable with a text editor.

9.6.4.2 Configuration Files

The device configuration can be downloaded by the ACS with type ***3 Vendor Configuration File***. This allows a user to configure a device locally to their specification, then save the settings for distribution to a larger group of deployed units. This file will include LoRa settings, Wi-Fi settings, and IP settings. This includes the channel plan used by the Semtech UDP packet forwarder. This file can be uploaded to deployed gateways to update their configuration to match the device that was updated locally. It is always good practice to locally test any configuration changes you make, so that you know it works the way you want it to before deploying the changes to more units deployed in the field. See the documentation for your ACS to determine how to initiate the ***3 Vendor Configuration File*** download command.

9.6.5 The Sentrius Gateway's TR-069 Data Model

The following tables show all of the parameters supported by the gateway along with a description of each. Each entry in the table is designated as read (R), write (W), or object (O). The items designated as objects are nodes in the data model. All parameters are designated with an R, W, or both.

The root of the data model is InternetGatewayDevice.

9.6.5.1 InternetGatewayDevice.Rfpros.DeviceInfo

Table 2: InternetGatewayDevice.Rfpros.DeviceInfo

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.DeviceInfo	O	Device info node	N/A
InternetGatewayDevice.DeviceInfo.SpecVersion	R	Version of the TR-069 spec referenced by this implementation	N/A
InternetGatewayDevice.DeviceInfo.ProvisioningCode	R	Code set by the ACS to indicate completed provisioning	N/A
InternetGatewayDevice.DeviceInfo.Manufacturer	R	Device manufacturer	N/A
InternetGatewayDevice.DeviceInfo.ManufacturerOUI	R	MAC address OUI value for the manufacturer	N/A
InternetGatewayDevice.DeviceInfo.ProductClass	R	Product type	N/A
InternetGatewayDevice.DeviceInfo.SerialNumber	R	Unique value assigned to each device at production	N/A
InternetGatewayDevice.DeviceInfo.HardwareVersion	R	Hardware version	N/A
InternetGatewayDevice.DeviceInfo.SoftwareVersion	R	Software version	N/A
InternetGatewayDevice.DeviceInfo.MemoryStatus	O	MemoryStatus node	N/A
InternetGatewayDevice.DeviceInfo.MemoryStatus.Total	R	Total system memory	N/A
InternetGatewayDevice.DeviceInfo.MemoryStatus.Free	R	Total free system memory	N/A
InternetGatewayDevice.DeviceInfo.UpTime	R	Total up time	N/A
InternetGatewayDevice.DeviceInfo.DeviceLog	R	Unused in our implementation. Request an upload of type *4 Vendor Log File* via the ACS	N/A
InternetGatewayDevice.DeviceInfo.ModelName	R	Model name	N/A

9.6.5.2 InternetGatewayDevice.Rfpros.ActiveProfileSettings

Table 3: InternetGatewayDevice.Rfpros.ActiveProfileSettings

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.Rfpros.ActiveProfileSettings	O	Active Wi-Fi profile node	N/A
InternetGatewayDevice.Rfpros.ActiveProfileSettings.ProfileName	R/W	Wi-Fi profile name (not SSID)	String representing the profile name
InternetGatewayDevice.Rfpros.ActiveProfileSettings.SSID	R/W	Wi-Fi network SSID	String representing the SSID
InternetGatewayDevice.Rfpros.ActiveProfileSettings.PSK	W	Wi-Fi network preshared key	String representing the PSK
InternetGatewayDevice.Rfpros.ActiveProfileSettings.ClientName	R/W	Wi-Fi network client name	A string representing name client name.
InternetGatewayDevice.Rfpros.ActiveProfileSettings.TxPower	R	TX power	A numeric value representing TX power
InternetGatewayDevice.Rfpros.ActiveProfileSettings.AuthType	R/W	Wi-Fi network authentication type	open, shared, or eap
InternetGatewayDevice.Rfpros.ActiveProfileSettings.EAPType	R/W	Wi-Fi network EAP type	leap, eap-fast, peap-mschapv2, eap-tls, peap-tls
InternetGatewayDevice.Rfpros.ActiveProfileSettings.WEPType	R/W	Wi-Fi network WEP type	none, wep, wep-eap, psk, tkip, wpa2-psk, wpa2-aes, cckm-tkip, cckm-aes, wpa-psk-aes, wpa-aes
InternetGatewayDevice.Rfpros.ActiveProfileSettings.Mode	R/W	Wi-Fi network mode	BGN
InternetGatewayDevice.Rfpros.ActiveProfileSettings.Powersave	R	Is power save enabled	off,max,fast
InternetGatewayDevice.Rfpros.ActiveProfileSettings.PSPDelay	R	Power save delay	A value 10 - 500 in milliseconds
InternetGatewayDevice.Rfpros.ActiveProfileSettings.Username	R/W	Username used by some authentication methods	A string representing the username
InternetGatewayDevice.Rfpros.ActiveProfileSettings.Password	W	Password used by some authentication methods	A string representing the password

9.6.5.3 InternetGatewayDevice.Rfpros.WIFIGlobalSettings

Table 4: InternetGatewayDevice.Rfpros.WIFIGlobalSettings

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.Rfpros.WIFIGlobalSettings	O	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Rfpros.WIFIGlobalSettings.UAPSD	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Rfpros.WIFIGlobalSettings.WMM	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Rfpros.WIFIGlobalSettings.AChannelSet	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Rfpros.WIFIGlobalSettings.AuthServerType	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Rfpros.WIFIGlobalSettings.AutoProfile Off	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Rfpros.WIFIGlobalSettings.BGChannelSet	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Rfpros.WIFIGlobalSettings.BeaconMissTime	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Rfpros.WIFIGlobalSettings.CCXFeatures	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Rfpros.WIFIGlobalSettings.CertificatePat	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Rfpros.WIFIGlobalSettings.DateCheck	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Rfpros.WIFIGlobalSettings.DefaultAdhocCh	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Rfpros.WIFIGlobalSettings.DFSChannels	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Rfpros.WIFIGlobalSettings.FIPSMode	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Rfpros.WIFIGlobalSettings.IgnoreNullSSID	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Rfpros.WIFIGlobalSettings.PMKCaching	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Rfpros.WIFIGlobalSettings.ProbeDelay	R	Hardcoded Wi-Fi settings in the gateway	N/A

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.Rfpros.WIFIGlobalSettings.RegulatoryDomain	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Rfpros.WIFIGlobalSettings.RoamPeriodMs	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Rfpros.WIFIGlobalSettings.RoamTrigger	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Rfpros.WIFIGlobalSettings.RTSThreshold	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Rfpros.WIFIGlobalSettings.ScanDFSTime	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Rfpros.WIFIGlobalSettings.TTLSInnerMethod	R	Hardcoded Wi-Fi settings in the gateway	N/A

9.6.5.4 InternetGatewayDevice.Rfpros.LORASettings

Table 5: InternetGatewayDevice.Rfpros.LORASettings

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.Rfpros.LORASettings	O	The LoRa settings for the gateway.	N/A
InternetGatewayDevice.Rfpros.LORASettings.EUI	R	This is the unique identifier for your gateway.	N/A
InternetGatewayDevice.Rfpros.LORASettings.Mode	R/W	This is the chosen packet forwarder type.	semtech, sbs
InternetGatewayDevice.Rfpros.LORASettings.Region	R/W	This is the region of operation your gateway is configured to. It is only writable one time and is set before leaving the factory. Attempting to change this after it is locked, will result in no change and an error being returned.	The following strings representing country codes: MY, SG, TW, HK, AU915, AU923, NZ, US, EU
InternetGatewayDevice.Rfpros.LORASettings.STServer	R/W	This is the URL for the network server when using the legacy Semtech UDP packet forwarder.	The URL of the server.
InternetGatewayDevice.Rfpros.LORASettings.STPortUp	R/W	This is the port used by the Semtech packet forwarder	A 2-4 digit port number.
InternetGatewayDevice.Rfpros.LORASettings.STPortDown	R/W	This is the port used by the Semtech packet forwarder	A 2-4 digit port number.
InternetGatewayDevice.Rfpros.LORASettings.STKeepAlive	R/W	This is the keep alive timeout used by the Semtech packet forwarder.	A value in milliseconds
InternetGatewayDevice.Rfpros.LORASettings.STPushTimeout	R/W	This is the push timeout used by the Semtech packet forwarder.	A value in milliseconds
InternetGatewayDevice.Rfpros.LORASettings.STStatInterval	R/W	This is the stat interval used by the Semtech packet forwarder.	A value in milliseconds
InternetGatewayDevice.Rfpros.LORASettings.STForwardCRCValid	R/W	This determines if packets with CRC errors are forwarded.	true, false
InternetGatewayDevice.Rfpros.LORASettings.STForwardCRCError	R/W	This determines if packets with CRC errors are forwarded.	true, false

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.Rfpros.LORASettings.STForwardCRCDisabled	R/W	This determines if packets with CRC errors are forwarded.	true, false
InternetGatewayDevice.Rfpros.LORASettings.SBSCUPSBootURL	R/W	This is the CUPS-Boot URL used by Basic Station.	A string representing the URL of the CUPS-Boot server.
InternetGatewayDevice.Rfpros.LORASettings.SBSCUPSURL	R/W	This is the CUPS URL used by Basic Station.	A string representing the URL of the CUPS server.
InternetGatewayDevice.Rfpros.LORASettings.SBSLNSURL	R/W	This is the URL to the LNS server used by Basic Station.	A string representing the URL of the LNS server.
InternetGatewayDevice.Rfpros.LORASettings.SBSStatus	R	This is the status of the connection to the LNS server. 0 - Disconnected, 1 - Connected.	N/A
InternetGatewayDevice.Rfpros.LORASettings.RadioConfig	R	This is the radio settings including channel plan used by the Legacy Semtech UDP packet forwarder.	N/A – This can be updated via vendor config file upload.

9.6.5.5 InternetGatewayDevice.Rfpros.LANSettings

Table 6: InternetGatewayDevice.Rfpros.LANSettings

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.Rfpros.LANSettings	O	This node contains the LAN settings. These are not writeable as parameters	N/A
InternetGatewayDevice.Rfpros.LANSettings.IPv4	O	IPv4 settings	N/A
InternetGatewayDevice.Rfpros.LANSettings.IPv4.DNSServer1	R	The first DNS server	N/A
InternetGatewayDevice.Rfpros.LANSettings.IPv4.DNSServer2	R	The second DNS server	N/A
InternetGatewayDevice.Rfpros.LANSettings.IPv4.DeviceAddr	R	Gateway IP address	N/A
InternetGatewayDevice.Rfpros.LANSettings.IPv4.NetMask	R	The netmask	N/A
InternetGatewayDevice.Rfpros.LANSettings.IPv4.Broadcast	R	The broadcast IP address	N/A
InternetGatewayDevice.Rfpros.LANSettings.IPv4.ExtGWIP	R	Gateway IP address (not necessarily external)	N/A
InternetGatewayDevice.Rfpros.LANSettings.IPv4.IPMethod	R	IP mode (DHCP or static)	N/A
InternetGatewayDevice.Rfpros.LANSettings.IPv6	O	IPv6 settings	N/A
InternetGatewayDevice.Rfpros.LANSettings.IPv6.DeviceAddr	R	IPv6 address	N/A
InternetGatewayDevice.Rfpros.LANSettings.IPv6.Mask	R	IPv6 net mask	N/A
InternetGatewayDevice.Rfpros.LANSettings.IPv6.IPMethod	R	IPv6 mode	N/A
InternetGatewayDevice.Rfpros.LANSettings.IPv6.AutoDHCPMethod	R	IPv6 auto DHCP mode	N/A

9.6.5.6 InternetGatewayDevice.Rfpros.GatewayManagement

Table 7: InternetGatewayDevice.Rfpros.GatewayManagement

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.Rfpros.GatewayManagement	O	Version information and how to initiate a firmware update	N/A
InternetGatewayDevice.Rfpros.GatewayManagement.Password	W	Set the password.	A string indicating a space separated value: current_password new_password
InternetGatewayDevice.Rfpros.GatewayManagement.ProvisioningComplete	R	Has provisioning been completed.	1 = completed, 0 = not completed
InternetGatewayDevice.Rfpros.GatewayManagement.Versions	O	Contains version information	N/A
InternetGatewayDevice.Rfpros.GatewayManagement.Versions.SDK	R	SDK version	N/A
InternetGatewayDevice.Rfpros.GatewayManagement.Versions.Driver	R	Driver package version	N/A
InternetGatewayDevice.Rfpros.GatewayManagement.Versions.Supplicant	R	Wi-Fi supplicant version	N/A
InternetGatewayDevice.Rfpros.GatewayManagement.Versions.Build	R	Build version	N/A
InternetGatewayDevice.Rfpros.GatewayManagement.Versions.HardwareChipset	R	Hardware chipset	N/A
InternetGatewayDevice.Rfpros.GatewayManagement.Versions.Firmware	R	Wi-Fi firmware version	N/A
InternetGatewayDevice.Rfpros.GatewayManagement.Versions.CLI	R	SDC CLI version	N/A
InternetGatewayDevice.Rfpros.GatewayManagement.Versions.FirmwareUpdateURL	R/W	URL to point to a new firmware version	String with the URL pointing to a *fw.txt* file with the firmware hosted on an external server
InternetGatewayDevice.Rfpros.GatewayManagement.Versions.FirmwareUpdateStatus	R	Status of the firmware update (1 = complete, 0 = not complete)	N/A

9.6.5.7 InternetGatewayDevice.Rfpros.SavedProfileSettings

Table 8: InternetGatewayDevice.Rfpros.SavedProfileSettings

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.Rfpros.SavedProfileSettings	O	Node to modify saved profile settings	N/A
InternetGatewayDevice.Rfpros.SavedProfileSettings.ListProfiles	R	List of all gateway Wi-Fi profiles	N/A
InternetGatewayDevice.Rfpros.SavedProfileSettings.ProfileName	R/W	Wi-Fi profile alias that the user wants to modify	String representing the profile name
InternetGatewayDevice.Rfpros.SavedProfileSettings.AddProfile	R/W	Adds a new profile	String representing the profile name
InternetGatewayDevice.Rfpros.SavedProfileSettings.DeleteProfile	R/W	Deletes a profile	String representing the profile name
InternetGatewayDevice.Rfpros.SavedProfileSettings.SSID	R/W	SSID for the selected Wi-Fi profile	String representing the SSID
InternetGatewayDevice.Rfpros.SavedProfileSettings.PSK	R/W	PSK for the selected Wi-Fi profile	String representing the PSK
InternetGatewayDevice.Rfpros.SavedProfileSettings.ClientName	R/W	Client name for the selected Wi-Fi profile	String representing name client name
InternetGatewayDevice.Rfpros.SavedProfileSettings.TxPower	R/W	TX power for the selected Wi-Fi profile	A numeric value representing TX power
InternetGatewayDevice.Rfpros.SavedProfileSettings.AuthType	R/W	Authentication type for the selected Wi-Fi profile	open, shared, or eap
InternetGatewayDevice.Rfpros.SavedProfileSettings.EAPType	R/W	EAP type for the selected Wi-Fi profile	leap, eap-fast, peap-mschapv2, eap-tls, peap-tls
InternetGatewayDevice.Rfpros.SavedProfileSettings.WEPType	R/W	WEP type for the selected Wi-Fi profile	none, wep, wep-eap, psk, tkip, wpa2-psk, wpa2-aes, cckm-tkip, cckm-aes, wpa-psk-aes, wpa-aes
InternetGatewayDevice.Rfpros.SavedProfileSettings.Mode	R/W	Selected Wi-Fi profile mode	BGN
InternetGatewayDevice.Rfpros.SavedProfileSettings.Powersave	R/W	Displays the enabled power save mode	off,max,fast
InternetGatewayDevice.Rfpros.SavedProfileSettings.PSPDelay	R/W	Selected Wi-Fi profile's power save delay	A value 10 - 500 in units of milliseconds.
InternetGatewayDevice.Rfpros.SavedProfileSettings.Username	R/W	Wi-Fi profile username used by some authentication methods	Username string
InternetGatewayDevice.Rfpros.SavedProfileSettings.Password	W	Wi-Fi profile password used by some authentication methods	Password (write only) string

9.6.5.8 InternetGatewayDevice.ManagementServer

Table 9: InternetGatewayDevice.ManagementServer

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.ManagementServer	O	Standard TR-069 Management Server node	
InternetGatewayDevice.ManagementServer.ConnectionRequestURL	R/W	URL for the ACS to use to initiate a connection	URL used by the ACS to initiate a connection with the gateway
InternetGatewayDevice.ManagementServer.ParameterKey	R/W		String representing the parameter key (opt.)
InternetGatewayDevice.ManagementServer.PeriodicInformTime	R/W	Time of the last inform message	String representing the time of the last inform message
InternetGatewayDevice.ManagementServer.PeriodicInformInterval	R/W	Interval for the periodic inform message	Numeric value representing the periodic inform interval
InternetGatewayDevice.ManagementServer.PeriodicInformEnable	R/W	Enables periodic inform	true, false
InternetGatewayDevice.ManagementServer.Password	W	Password used to initiate a connection with the ACS	String representing the password for connections initiated by the gateway
InternetGatewayDevice.ManagementServer.ConnectionRequestUsername	R/W	Username used for the ACS to initiate a connection with the gateway	String representing the username for connections initiated by the ACS
InternetGatewayDevice.ManagementServer.ConnectionRequestPassword	W	Password used for the ACS to initiate a connection with the gateway	String representing the password for connections initiated by the ACS

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.ManagementServer.Username	R/W	Username for the gateway to initiate a connection with the ACS	String representing the username for connections initiated by the gateway
InternetGatewayDevice.ManagementServer.URL	R/W	URL for the gateway to initiate a connection with the ACS	URL used by the gateway to initiate a connection with the ACS

9.6.5.9 InternetGatewayDevice.WANDevice

Table 10: InternetGatewayDevice.WANDevice

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.WANDevice	O	Standard node for Wi-Fi endpoint configuration. Only one Wi-Fi connection is allowed on this gateway	N/A
InternetGatewayDevice.WANDevice.{x}	O	Sub-node for each Wi-Fi device. Only one Wi-Fi connection allowed on this gateway	N/A
InternetGatewayDevice.WANDevice.{x}.WANConnectionDevice	O	Sub-node for each Wi-Fi device. Only one Wi-Fi connection is allowed on this gateway	N/A
InternetGatewayDevice.WANDevice.{x}.WANConnectionDevice.{y}	O	Sub-node for each WiFi device. Only one Wi-Fi connection is allowed on this gateway	N/A
InternetGatewayDevice.WANDevice.{x}.WANConnectionDevice.{y}.WANIPConnection	O	Sub-node for each Wi-Fi device. Only one Wi-Fi connection is allowed on this gateway	N/A
InternetGatewayDevice.WANDevice.{x}.WANConnectionDevice.{y}.WANIPConnection.{z}	O	Sub-node for each Wi-Fi device. Only one Wi-Fi connection is allowed on this gateway	N/A
InternetGatewayDevice.WANDevice.{x}.WANConnectionDevice.{y}.WANIPConnection.{z}.ConnectionStatus	R	Connection status	N/A
InternetGatewayDevice.WANDevice.{x}.WANConnectionDevice.{y}.WANIPConnection.{z}.ExternalIPAddress	R	IP address (not necessarily external)	N/A
InternetGatewayDevice.WANDevice.{x}.WANConnectionDevice.{y}.WANIPConnection.{z}.MACAddress	R	MAC address	N/A

9.6.5.10 InternetGatewayDevice.IPPingDiagnostics

Table 11: InternetGatewayDevice.IPPingDiagnostics

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.IPPingDiagnostics	O	Diagnostic data for the IP connections	N/A
InternetGatewayDevice.IPPingDiagnostics.DiagnosticsState	R	Diagnostic data for the IP connections	N/A
InternetGatewayDevice.IPPingDiagnostics.Host	R	Diagnostic data for the IP connections	N/A
InternetGatewayDevice.IPPingDiagnostics.NumberOfRepetitions	R	Diagnostic data for the IP connections	N/A
InternetGatewayDevice.IPPingDiagnostics.Timeout	R	Diagnostic data for the IP connections	N/A
InternetGatewayDevice.IPPingDiagnostics.DataBlockSize	R	Diagnostic data for the IP connections	N/A
InternetGatewayDevice.IPPingDiagnostics.SuccessCount	R	Diagnostic data for the IP connections	N/A
InternetGatewayDevice.IPPingDiagnostics.AverageResponseTime	R	Diagnostic data for the IP connections	N/A
InternetGatewayDevice.IPPingDiagnostics.MinimumResponseTime	R	Diagnostic data for the IP connections	N/A
InternetGatewayDevice.IPPingDiagnostics.MaximumResponseTime	R	Diagnostic data for the IP connections	N/A
InternetGatewayDevice.IPPingDiagnostics.FailureCount	R	Diagnostic data for the IP connections	N/A

9.6.5.11 InternetGatewayDevice.LANDevice

Table 11: InternetGatewayDevice.LANDevice

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.LANDevice	O	Defines Wi-Fi settings	N/A
InternetGatewayDevice.LANDevice.{x}	O	Defines Wi-Fi settings	N/A
InternetGatewayDevice.LANDevice.{x}.WLANConfiguration	O	Defines Wi-Fi settings	N/A
InternetGatewayDevice.LANDevice.{x}.WLANConfiguration.{y}	O	Defines Wi-Fi settings	N/A
InternetGatewayDevice.LANDevice.{x}.WLANConfiguration.{y}.Enable	R/W	Enables the specific Wi-Fi device	true, false
InternetGatewayDevice.LANDevice.{x}.WLANConfiguration.{y}.RadioEnable	R/W	Enables the specific Wi-Fi device	true, false
InternetGatewayDevice.LANDevice.{x}.WLANConfiguration.{y}.SSID	R/W	Enables the specific Wi-Fi device	Represents the SSID of the active Wi-Fi profile

9.6.5.12 InternetGatewayDevice.Cellular

Note: Provisioning of these data fields is only supported with the RG191+LTE hardware for the US market only, see Ordering Information for product part numbers.

Table 12: InternetGatewayDevice.Cellular

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.Cellular	O	This is the TR-181 cellular node.	N/A
InternetGatewayDevice.Cellular	O	This is the TR-181 cellular node.	N/A
InternetGatewayDevice.Cellular.Manufacturer	R	This is the manufacturer of the installed modem.	N/A
InternetGatewayDevice.Cellular.Model	R	This is the model number of the installed modem.	N/A
InternetGatewayDevice.Cellular.Firmware	R	This is the firmware version of the installed modem.	N/A
InternetGatewayDevice.Cellular.RoamingEnabled	R/W	This indicates if roaming is enabled on the modem.	true,false
InternetGatewayDevice.Cellular.RoamingStatus	R	This is the roaming status	N/A
InternetGatewayDevice.Cellular.InterfaceNumberOfEntries	R	This is the number of cellular network interfaces (always 1 in our gateway)	N/A
InternetGatewayDevice.Cellular.AccessPoint.{x}	O	This is the subnode for each access point supported. Currently only 1 is supported by this platform.	N/A
InternetGatewayDevice.Cellular.AccessPoint.{x}.APN	R/W	The APN used to route data traffic from this cellular modem.	A string representing the APN.
InternetGatewayDevice.Cellular.AccessPoint.{x}.UserName	R/W	The username for the cellular account. This is optional. Not all network operators require a username and password.	A string representing the username.
InternetGatewayDevice.Cellular.AccessPoint.{x}.Password	W	The password for the cellular account. This is optional. Not all network operators require a username and password.	A string representing the password.
InternetGatewayDevice.Cellular.Interface.{x}	O	This is the subnode for each interface (cellular modem) supported. Currently only 1 modem is supported by this platform.	N/A
InternetGatewayDevice.Cellular.Interface.{x}.CurrentAccessTechnology	R	The radio access technology currently in use. This platform only supports LTE.	N/A
InternetGatewayDevice.Cellular.Interface.{x}.DNS1	R/W	The first DNS server override.	A string representing the IP address of a DNS server.

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.Cellular.Interface.{x}.DNS2	R/W	The second DNS server override.	A string representing the IP address of a DNS server.
InternetGatewayDevice.Cellular.Interface.{x}.Enable	R/W	Enable or disable the modem.	true = enabled, false = disabled.
InternetGatewayDevice.Cellular.Interface.{x}.IMEI	R	The IMEI of the modem.	N/A
InternetGatewayDevice.Cellular.Interface.{x}.IPV4	R	The IPv4 address acquired from the network.	N/A
InternetGatewayDevice.Cellular.Interface.{x}.NetworkInUse	R	The name of the network operator and mcc and mnc of the network.	N/A
InternetGatewayDevice.Cellular.Interface.{x}.RSSI	R	The RSSI in dBm.	N/A
InternetGatewayDevice.Cellular.Interface.{x}.Status	R	The status of the connection. true = connected, false = not connected.	N/A
InternetGatewayDevice.Cellular.Interface.{x}.Stats	O	This is the subnode reporting the data usage statistics for the interface.	N/A
InternetGatewayDevice.Cellular.Interface.{x} .Stats.BytesReceived	R	The number of bytes (RX).	N/A
InternetGatewayDevice.Cellular.Interface.{x} .Stats.BytesSent	R	The number of bytes (TX).	N/A
InternetGatewayDevice.Cellular.Interface.{x} .Stats.ErrorsReceived	R	The number of RX errors.	N/A
InternetGatewayDevice.Cellular.Interface.{x} .Stats.ErrorsSent	R	The number of TX errors.	N/A
InternetGatewayDevice.Cellular.Interface.{x }.Stats.PacketsReceived	R	The number of Packets (RX)	N/A
InternetGatewayDevice.Cellular.Interface.{x} .Stats.PacketsSent	R	The number of Packets (TX)	N/A
InternetGatewayDevice.Cellular.Interface.{x}.USIM	O	This is the subnode reporting USIM data for this interface.	N/A
InternetGatewayDevice.Cellular.Interface.{x}.USIM.ICCID	R	This is the ICCID of the SIM card that is inserted.	N/A
InternetGatewayDevice.Cellular.Interface.{x}.USIM.IMSI	R	This is the IMSI stored on the SIM card that is inserted.	N/A

9.6.5.13 InternetGatewayDevice.WiFi

Table 12: InternetGatewayDevice.WiFi

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.WiFi	O	The TR-181 Wi-Fi node.	N/A
InternetGatewayDevice.WiFi.Radio	O	Sub-node for each Wi-Fi radio (only one on the gateway)	N/A
InternetGatewayDevice.WiFi.Radio.{x}	O	Sub-node for the Wi-Fi radio settings for each Wi-Fi radio (only one on the gateway)	N/A
InternetGatewayDevice.WiFi.Radio.{x}.AutoChannelEnable	R	Whether/not auto channel is enabled	N/A
InternetGatewayDevice.WiFi.Radio.{x}.Enable	R	Whether/not the interface is enabled	N/A
InternetGatewayDevice.WiFi.Radio.{x}.Status	R	Interface status	N/A
InternetGatewayDevice.WiFi.Radio.{x}.Name	R	Interface name	N/A
InternetGatewayDevice.WiFi.Radio.{x}.SupportedFrequencyBands	R	Supported Wi-Fi frequencies	N/A
InternetGatewayDevice.WiFi.Radio.{x}.OperatingFrequencyBand	R	Currently used Wi-Fi frequencies	N/A
InternetGatewayDevice.WiFi.Radio.{x}.ChannelsInUse	R	Whether/not the channel is in use	N/A
InternetGatewayDevice.WiFi.Radio.{x}.Channel	R	Indicates the applicable channel	N/A
InternetGatewayDevice.WiFi.Radio.{x}.AutoChannelSupported	R	Whether/not auto channel is supported	N/A

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.WiFi.Radio.{x}.OperatingStandards	R	Supported Wi-Fi modes	N/A
InternetGatewayDevice.WiFi.SSID	O	SSID node	N/A
InternetGatewayDevice.WiFi.SSID.{x}	O		N/A
InternetGatewayDevice.WiFi.SSID.{x}.Enable	R/W	Whether/not SSID is enabled	true, false
InternetGatewayDevice.WiFi.SSID.{x}.Status	R	SSID status	N/A
InternetGatewayDevice.WiFi.SSID.{x}.Name	R/W	SSID profile name	The profile name string
InternetGatewayDevice.WiFi.SSID.{x}.LowerLayers	R/W	Reference to the radio in the data model	Reference in the data model to the active radio string
InternetGatewayDevice.WiFi.SSID.{x}.SSID	R/W	SSID	SSID for your Wi-Fi network string
InternetGatewayDevice.WiFi.SSID.{x}.X_IPInterface	R/W	Reference to the IP interface in the data model	The reference to the IP interface in the data model string
InternetGatewayDevice.WiFi.EndPoint	O	Defines each endpoint (Wi-Fi profile)	N/A
InternetGatewayDevice.WiFi.EndPoint.{x}	O		N/A
InternetGatewayDevice.WiFi.EndPoint.{x}.Profiles	O		
InternetGatewayDevice.WiFi.EndPoint.{x}.Profiles.{y}	O		N/A
InternetGatewayDevice.WiFi.EndPoint.{x}.Profiles.{y}.Security	O	Sub-node that defines the security settings used in the Wi-Fi profile.	N/A
InternetGatewayDevice.WiFi.EndPoint.{x}.Profiles.{y}.Security.WEPKey	R/W	WEP key when WEP mode is enabled	A string representing the WEP key.
InternetGatewayDevice.WiFi.EndPoint.{x}.Profiles.{y}.Security.PreSharedKey	W	PSK used for various security modes. Either	A string representing the PSK.

Parameter Name	R/W	Description	Input Data
		the passphrase or pre-shared key can be entered here.	
InternetGatewayDevice.WiFi.EndPoint.{x}.Profiles.{y}.Security .KeyPassphrase	W	Passphrase for the WPA/WPA2 security. Either the passphrase or pre-shared key can be entered here.	A string representing the PSK.
InternetGatewayDevice.WiFi.EndPoint.{x}.Profiles.{y}.Security .ModeEnabled	R/W	Displays the enabled security mode. These are the standard TR-181 security type strings	A string selected from InternetGatewayDevice.WiFi.EndPoint.{x}.Security.ModesSupported.
InternetGatewayDevice.WiFi.EndPoint.{x}.Profiles.{y}.Security .EAPType	R/W	Indicates which EAP mode is enabled	leap, eap-fast, peap-mschapv2, eap-tls, peap-tls
InternetGatewayDevice.WiFi.EndPoint.{x}.Profiles.{y}.Security .Username	R/W	Username used for authentication	A string representing the username.
InternetGatewayDevice.WiFi.EndPoint.{x}.Profiles.{y}.Security .Password	W	Password used for authentication	A string representing the password.
InternetGatewayDevice.WiFi.EndPoint.{x}.Profiles.{y}.Security .CACertificate	R/W	Certificate file path	A string representing the path to the CA certificate.
InternetGatewayDevice.WiFi.EndPoint.{x}.Profiles.{y}.Security .UserCertName	R/W	Certificate name	A string representing the certificate name.
InternetGatewayDevice.WiFi.EndPoint.{x}.Profiles.{y}.Security .UserCertPassword	W	Certificate password	A string representing the certificate path.
InternetGatewayDevice.WiFi.EndPoint.{x}.Profiles.{y}.Security .PACName	R/W	PAC file name	A string representing the PAC name.
InternetGatewayDevice.WiFi.EndPoint.{x}.Profiles.{y}.Security .PACPassword	W	The PAC file password	A string representing the PAC password.
InternetGatewayDevice.WiFi.EndPoint.{x}.Profiles.{y}.Enable	R/W	Whether/not the profile is enabled	true, false

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.WiFi.EndPoint.{x}.Profiles.{y}.Alias	R/W	Profile name	A string representing the Wi-Fi profile name.
InternetGatewayDevice.WiFi.EndPoint.{x}.Profiles.{y}.SSID	R/W	Profile SSID	A string representing the Wi-Fi network SSID.
InternetGatewayDevice.WiFi.EndPoint.{x}.Profiles.{y}.Status	R	Connection status	N/A
InternetGatewayDevice.WiFi.EndPoint.{x}.Security	O	Defines security supported by the gateway	N/A
InternetGatewayDevice.WiFi.EndPoint.{x}.Security.ModesSupported	R	Comma-separated list of supported security modes	N/A
InternetGatewayDevice.WiFi.EndPoint.{x}.ProfileNumberOfEntries	R	Number of profiles	N/A
InternetGatewayDevice.WiFi.EndPoint.{x}.SSIDReference	R	Data model reference to the SSID for the currently active profile	N/A
InternetGatewayDevice.WiFi.EndPoint.{x}.ProfileReference	R	Profile reference for the currently active profile	N/A
InternetGatewayDevice.WiFi.EndPoint.{x}.Status	R	Profile status	N/A
InternetGatewayDevice.WiFi.EndPoint.{x}.Enable	R/W		true, false

9.6.5.14 InternetGatewayDevice.IP

Table 13: InternetGatewayDevice.IP

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.IP	O	This node provides stats for all the IP interfaces. There are 2 on the gateway, eth0 and wlan0.	N/A
InternetGatewayDevice.IP.Interface	O		N/A
InternetGatewayDevice.IP.Interface.{x}	O		N/A
InternetGatewayDevice.IP.Interface.{x}.Stats	O		N/A
InternetGatewayDevice.IP.Interface.{x}.Stats.DiscardPacketsReceived	R	The number of discarded packets (RX).	N/A
InternetGatewayDevice.IP.Interface.{x}.Stats.DiscardPacketsSent	R	The number of discarded packets (TX).	N/A
InternetGatewayDevice.IP.Interface.{x}.Stats.ErrorsReceived	R	The number of RX errors.	N/A
InternetGatewayDevice.IP.Interface.{x}.Stats.PacketsReceived	R	The number of packets (RX).	N/A
InternetGatewayDevice.IP.Interface.{x}.Stats.PacketsSent	R	The number of packets (TX).	N/A
InternetGatewayDevice.IP.Interface.{x}.Stats.BytesReceived	R	The number of bytes (RX).	N/A
InternetGatewayDevice.IP.Interface.{x}.Stats.BytesSent	R	The number of bytes (TX).	N/A
InternetGatewayDevice.IP.Interface.{x}.Stats.ErrorsSent	R	The number of TX errors.	N/A
InternetGatewayDevice.IP.Interface.{x}.IPv4Address	O	IPv4 Settings for the particular IP interface.	N/A
InternetGatewayDevice.IP.Interface.{x}.IPv4Address.{y}	O		N/A
InternetGatewayDevice.IP.Interface.{x}.IPv4Address.{y}.SubnetMask	R	The subnet mask.	N/A
InternetGatewayDevice.IP.Interface.{x}.IPv4Address.{y}.Enable	R	Is this interface enabled.	N/A
InternetGatewayDevice.IP.Interface.{x}.IPv4Address.{y}.AddressingType	R	The addressing type.	N/A
InternetGatewayDevice.IP.Interface.{x}.IPv4Address.{y}.IPAddress	R	The current IP address.	N/A
InternetGatewayDevice.IP.Interface.{x}.IPv4AddressNumberOfEntries	R	The number of IPv4 entries in this node (only 1 for the gateway)	N/A
InternetGatewayDevice.IP.Interface.{x}.Type	R	The type of IP interface.	N/A

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.IP.Interface.{x}.Name	R	The name of the interface.	N/A
InternetGatewayDevice.IP.Interface.{x}.Enable	R	Is the interface enabled.	N/A

9.7 Memfault

MEMFAULT is a remote diagnostic and fleet management feature integrated into the RG1xx firmware (starting with version 12.x and later). It enables users to monitor and troubleshoot devices in the field through a secure, cloud-based dashboard—eliminating the need for physical access.

MEMFAULT is designed as a remote observability platform. Once a device is enabled and actively syncing, it continuously sends telemetry data that helps users track:

- CPU and memory usage
- Uptime and reboot history
- Crash reports and software faults
- Firmware/software versions
- Sync health (heartbeat data)

To enable Memfault, navigate to Settings → Memfault in the RG1xx Web UI and click the Enable button.

By default, the device will connect to Ezurios's Memfault portal. You can setup your own account to get a project key and connect your gateways.

Please contact Ezurio if you have any questions.

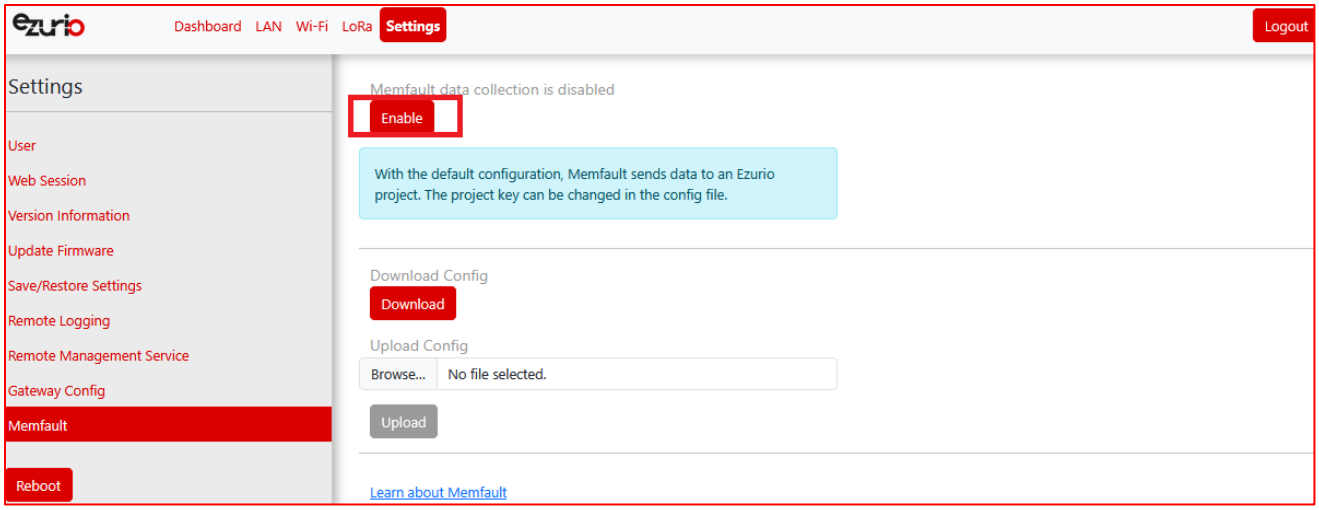


Figure 55: Memfault setting

The MEMFAULT dashboard provides a visual summary of each device's operational health. Below is a breakdown of the key sections as seen in this screenshot:

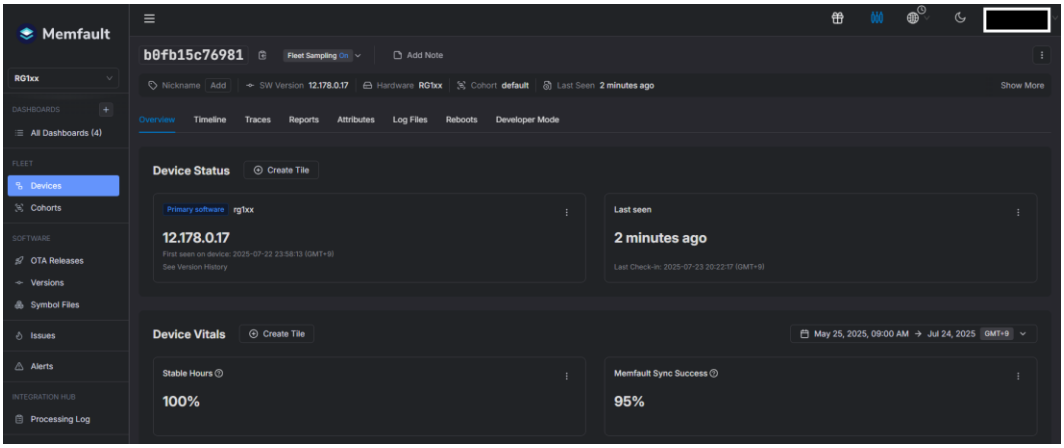


Figure 56: Memfault dashboard

9.8 Debug

At the bottom of the web UI is a debug pane that can be used to view system logs on the gateway. Click the arrow buttons to expand or collapse the debug pane. To start or stop debug log polling, click **Auto Update Logs**.

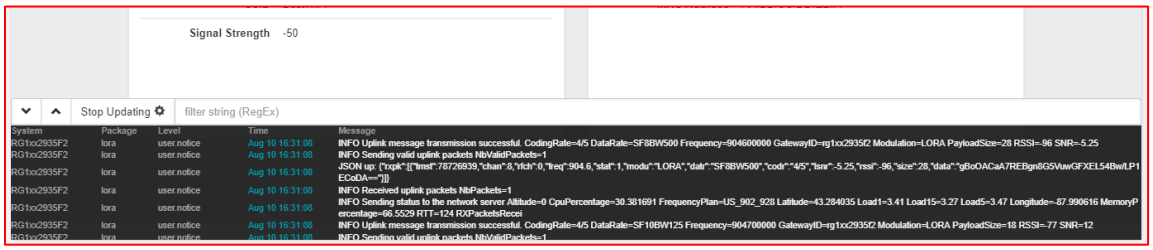


Figure 57: Debug info

9.9 Factory Reset

To factory reset the gateway back to default settings, complete the following steps:

1. Hold the user button while power is applied *OR* hold the user button while you press the reset button (Figure 58).

1 – User Button

2 – Reset Button

Figure 58: Performing a factory reset

2. Continue to hold the user button until ALL the LEDs on the top begin to flash.
3. Once the LEDs start flashing, release the user button.
4. The factory defaults are applied, the gateway reboots, and it is ready to use.

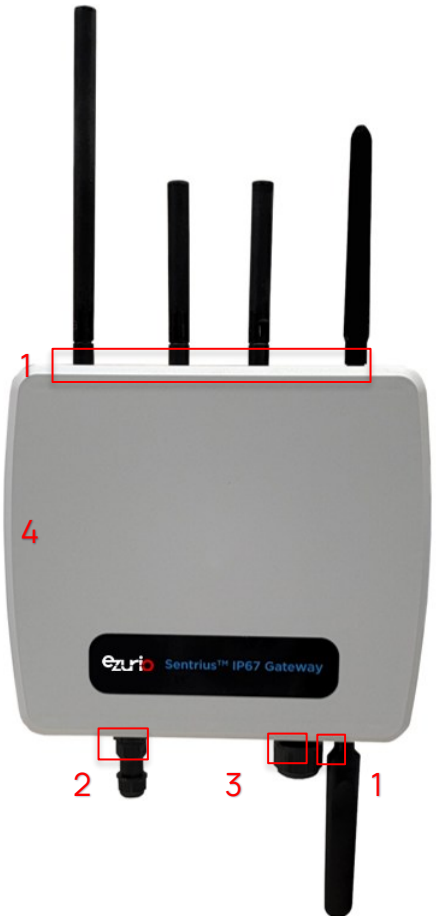
9.10 Bluetooth

Currently the Bluetooth and Bluetooth Low Energy functionality onboard the RG1xx Gateway is not enabled.
Please visit the RG1xx page on ezurio.com for more information: https://www.ezurio.com/wireless-modules/lorawan-solutions/sentrius-rg1xx-lora-enabled-gateway-wi-fi-bluetooth-ethernet.

10 IP67 Rated Enclosure

Reference	Description
1	LoRa and Wi-Fi antennas
2	Power supply module
3	CAT6 Ethernet module
4	Moulded plastic cover

Figure 59: Top of the IP67 Rated Sentrius™ RG1xx Gateway



Reference	Description
1	LoRa, Wi-Fi and LTE antennas (**LTE on RG191+LTE model only**)
2	Power supply module
3	CAT6 Ethernet module
4	Moulded plastic cover

Figure 60: Top of the IP67 Rated Sentrius™ RG191+LTE Gateway

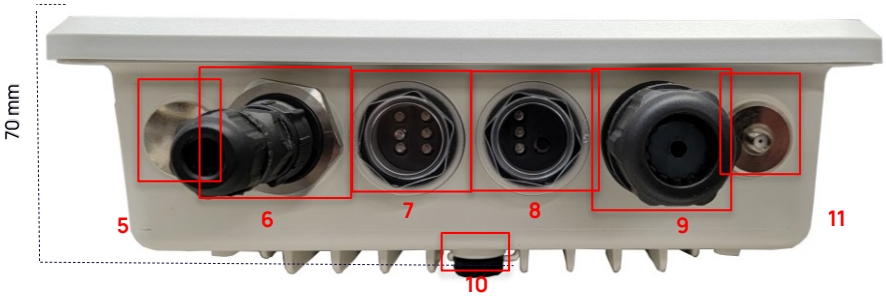


Figure 61: Side panel of the IP67 Rated Sentrius™ RG1xx LTE Gateway (Current Generation)

Ref.	Description
5	Metal cover plug (1-2 Ports) – Available data/power ports for expansion
6	Power supply module
7	Six LED displays with transparent dust cover
8	Three LED display and User button with transparent dust cover
9	CAT6 Ethernet module
10	Plastic gore ventilation plug
11	LTE Antenna Port (**RG191+ LTE only**)

11 Regulatory

11.1 Current Regulatory Certifications

The RG1xx holds current certifications in the following countries:

Country/Region	Regulatory ID
USA (FCC)	Contains the following: RG191-M2 – SQG-1001 WB50NBT – SQG-WB50NBT
EU (CE)	Contains the following: RG186-M2 – SQG-1002 WB50NBT – 3147A-WB50NBT
UK	UKCA
UAB (TRA)	TRA Registered No: ER61585/18 Dealer No: DA72940/18
Canada (ISED)	Contains the following: RG191-M2 – 3147A-1001 WB50NBT – 3147A-WB50NBT
Taiwan (NCC)	CCAF19LP1820T2
Australia	C-Tick
New Zealand	C-Tick (R-NZ)
Singapore (IMDA)	DA107248

11.2 Documentation Requirements

To ensure regulatory compliance, when integrating the RG1xx into a host device, it is necessary to meet the documentation requirements set forth by the applicable regulatory agencies. The following sections (FCC, ISED Canada, European Union, and others) outline the information that may be included in the user's guide and external labels.

11.3 FCC Regulatory

11.3.1 RG191

The RG191 contains the RG191-M2 and the WB50NBT from Ezurio.

Model	US/FCC
RG191-M2	SQG-1001
WB50NBT	SQG-WB50NBT

11.3.2 RG191+LTE

Note: For complete regulatory information, refer to the RG191+LTE Regulatory Information document which is also available from the RG191+LTE product page.

The RG191+LTE contains the RG191-M2, the WB50NBT from Ezurio, and the Quectel Wireless Solutions EG91-NA. It holds current certifications in the following countries:

Model	US/FCC	CANADA/IC
RG191+LTE	SQG-RG191NALTE	3147A-RG191NALTE
contains…		
RG191-M2	SQG-1001	3147A-1001
WB50NBT	SQG-WB50NBT	3147A-WB50NBT
EG91-NA	XMR201807EG91NA	10224A-2018EG91NA

11.3.3 LTE Network Certification

The RG191+LTE gateway operates on LTE networks based on PTCRB certification.

11.3.3.1 PTCRB Certification

Manufacturer	Model	Supported Technologies and Frequencies	Hardware Version	Software Version	Web Link
Ezurio	RG191+LTE Series	**E-UTRA FDD:** Band 2 Band 4 Band 5 Band 12 Band 13	v750.03.224	v93.9.5.1	Link

11.3.4 Power Exposure Information

To comply with FCC RF exposure limits for general population/uncontrolled exposure, the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and operating in conjunction with any other antenna or transmitter.

IMPORTANT NOTE: If these conditions cannot be met (for certain configurations or co-location with another transmitter), then the FCC and Industry Canada authorizations are no longer considered valid, and the FCC ID and IC Certification Number cannot be used on the final product. In these circumstances, the OEM integrator is responsible for re-evaluating the end product (including the transmitter) and obtaining a separate FCC and Industry Canada authorization.

11.3.5 OEM Responsibilities

To comply with FCC and Industry Canada RF exposure limits for general population/uncontrolled exposure, the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and operating in conjunction with any other antenna or transmitter, except in accordance with FCC multi-transmitter product procedures.

WARNING: Changes or modifications not expressly approved by Ezurio could void the user's authority to operate the equipment.

11.3.6 FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in an installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to correct the interference by one or more of the following measures:
Re-orient or relocate the receiving antenna
Increase the separation between the equipment and the receiver
Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
Consult the dealer or an experienced radio/TV technician for help.

11.3.7 FCC Warning

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, and (2) this device must accept any interference received, including interference that may cause undesired operation.

11.4 ISED (Canada) Regulatory

The RG191 contains the RG191-M2 and the WB50NBT from Ezurio.

Model	CANADA/ISED
RG191-M2	3147A-1001
WB50NBT	3147A-WB50NBT

11.4.1 ISED Warning

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.
French equivalent is:
Le présent appareil est conforme aux CNR d'Industrie Canada applicable aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

11.4.2 ISED Radiation Exposure Statement

To comply with ISED Canada RF exposure limits for general population / uncontrolled exposure, the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be operating in conjunction with any other antenna or transmitter.
French equivalent is:
Déclaration IC d'exposition aux radiations
Pour se conformer à Industrie Canada RF limites d'exposition pour la population générale / exposition non contrôlée, l'antenne utilisée pour ce transmetteur doit être installée pour fournir une distance d'au moins 20 cm de toutes les personnes et ne doit pas fonctionner en conjonction avec toute autre antenne ou transmetteur.

11.5 Australia and New Zealand Regulatory

RCM: Pending Compliant to standards EN 300 328 V1.9.1, AS/NZS 4268: 2012-A1:2013, and EN 55022:2010/AC:2011
If this device is used in a product, the OEM has responsibility to verify compliance of the final end product to the Australia/New Zealand (RCM) Standards. All end-products require their own certification (SDoc). You will not be able to leverage the module certification and ship product into the country.

11.6 Taiwan (NCC) Regulatory

The RG191 is approved for use in the Taiwan market.

Model	Certificate Number
RG191	CCAF19LP1820T2

第十二條→經型式認證合格之低功率射頻電機，非經許可，公司，商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
第十四條→低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信法規定作業之無線電通信。 低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Note: You must place "本產品內含射頻模組：**CCAF19LP1820T2**" on the host product in such a location that it can be seen by an operator at the time of purchase.

11.7 EU Regulatory

The RG186 has been tested for compliance with relevant standards for the EU market. The RG186 module was tested with a 2 dBi antenna. The OEM can operate the RG186 module with any other type of antenna but must ensure that the gain does not exceed 2 dBi to maintain the Ezurio approval.
The OEM should consult with a qualified test house before entering their device into an EU member country to make sure all regulatory requirements have been met for their complete device.

11.7.1 User's Guide Requirements

The integrator must include specific information in the user's guide for the device into which the BT85x is integrated. In addition to the required FCC and IC statements outlined above, the following Radio Equipment Directive (RED) statements must be added in their entirety and without modification into a prominent place in the user's guide for the device into which the RG186 is integrated:
This device complies with the essential requirements of the 2014/53/EU – Radio Equipment Directive (RED). The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the 2014/53/EU – Radio Equipment Directive (RED):

- **EN 62368-1:2014/A11:2017**
- Safety requirements for audio/video, information, and technology equipment
- **EN 300 328 v2.2.2 (2019-07)**
- Electromagnetic compatibility and Radio Spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
- **EN 62311:2008 I EN 50665:2017 I EN 50385:2017**
- RF exposure
- **EN 301 489-1 v2.2.0 (2017-03)**
- Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements
- **EN 301 489-17 V3.2.0 (2017-03)**
- Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment
- **EU 2015/863 (RoHS 3)**
- Declaration of Compliance – EU Directive 2015/863; Reduction of Hazardous Substances (RoHS)
- This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.
- In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

- This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

български [Bulgarian]	С настоящото *[име на производителя]* декларира, че това устройство *[вид оборудване]* е в съответствие със съществените изисквания и други приложими разпоредби на Директиви 2014/53/EC
Hrvatski [Croatian]	*[naziv proizvođača]* ovim putem izjavljuje da je ovaj uređaj *[vrsta opreme]* sukladan osnovnim zahtjevima i ostalim bitnim odredbama Direktiva 2014/53/EU
Česky [Czech]	*[Jméno výrobce]* tímto prohlašuje, že tento *[typ zařízení]* je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.
Dansk [Danish]	Undertegnede *[fabrikantens navn]* erklærer herved, at følgende udstyr *[udstyrets typebetegnelse]* overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU.
Deutsch [German]	Hiermit erklärt *[Name des Herstellers]*, dass sich das Gerät *[Gerätetyp]* in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet.
Eesti [Estonian]	Käesolevaga kinnitab *[tootja nimi]* seadme *[seadme tüüp]* vastavust direktiivi 2014/53/EL põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, *[name of manufacturer]*, declares that this *[type of equipment]* is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
Español [Spanish]	Por medio de la presente *[nombre del fabricante]* declara que el *[clase de equipo]* cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/UE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *[όνομα του κατασκευαστή]* ΔΗΛΩΝΕΙ ΟΤΙ *[εξοπλισμού]* ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/ΕΕ.
Français [French]	Par la présente *[nom du fabricant]* déclare que l'appareil *[type d'appareil]* est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/UE.
Íslenska [Icelandic]	Hér, *[Nafn framleiðanda]*, því yfir að þetta *[gerð búnaðar]* tæki er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipana 2014/53/ ESB
Italiano [Italian]	Con la presente *[nome del costruttore]* dichiara che questo *[tipo di apparecchio]* è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/UE.
Latviešu valoda [Latvian]	Aršo *[izgatavotājanosaukums]* deklarē, ka *[iekārtas tips]* atbilstDirektīvas 2014/53/ES būtiskajāmprasībām un citiemar to saistītajiemnoteikumiem.
Lietuvių kalba [Lithuanian]	Šiuo *[gamintojo pavadinimas]* deklaruoja, kad šis *[įrangos tipas]* atitinka esminius reikalavimus ir kitas 2014/53/ES Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart *[naam van de fabrikant]* dat het toestel *[type van toestel]* in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU.
Malti [Maltese]	Hawnhekk, *[isem tal-manifattur]*, jiddikjara li dan *[il-mudel tal-prodott]* jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/UE.
Magyar [Hungarian]	Alulírott, *[gyártó neve]* nyilatkozom, hogy a *[... típus]* megfelel a vonatkozó alapvetõ követelményeknek és az 2014/53/EU irányelv egyéb elõírásainak.
Norsk [Norwegian]	Herved *[navnet på produsenten]*, erklærer at denne *[type utstyr]* enheten, er i samsvar med de grunnleggende kravene og andre relevante bestemmelser i direktivene 2014/53/EU
Polski [Polish]	Niniejszym *[nazwa producenta]* oświadcza, że *[nazwa wyrobu]* jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/UE.
Português [Portuguese]	*[Nome do fabricante]* declara que este *[tipo de equipamento]* está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/UE.
Română [Romanian]	Prin prezenta, *[numele producătorului]* declară că acest dispozitiv *[tipul de echipament]* este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivelor 2014/53/UE
Slovenščina [Slovenian]	*[Ime proizvajalca]* izjavlja, da je ta *[tip opreme]* v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU.
Slovenčina [Slovak]	*[Menovýrobcu]* týmtovyhlasuje, že *[typzariadenia]* spĺňazákladnépožiadavky a všetkypríslušnéustanovenia Smernice 2014/53/EU.
Suomi [Finnish]	*[Valmistaja]* vakuuttaa täten että *[laitteen tyyppimerkintä]* tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar *[företag]* att denna *[utrustningstyp]* står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU.

11.7.2 EU Declarations of Conformity

Manufacturer	Ezurio
Products	RG186
Product Description	LoRa/Wi-Fi/BT and BLE RF module
EU Directives	2014/53/EU – Radio Equipment Directive (RED)

Reference standards used for presumption of conformity:

Article Number	Requirement	Reference standard(s)
3.1a	Low voltage equipment safety	EN 62368-1:2014
3.1b	Protection requirements – Electromagnetic compatibility	EN 301 489-1 v2.2.0 (2017-03) EN 301 489-3 v2.1.1 (2017-03) EN 301 489-17 v3.2.0 (2017-03)
3.2	Means of the efficient use of the radio frequency spectrum (ERM)	EN 300 220-1 v3.1.1 (2017-02) EN 300 220-2 v3.1.1 (2017-02) EN 300 328 v2.1.1 (2016-11) EN 301 893-v2.1.1 (2017-05)

Declaration:

We, Ezurio, declare under our sole responsibility that the essential radio test suites have been carried out and that the above product to which this declaration relates is in conformity with all the applicable essential requirements of Article 3 of the EU Radio Equipment Directive 2014/53/EU, when used for its intended purpose.

The minimum distance between the user and/or any bystander and the radiating structure of the transmitter is 20 cm.

Place of Issue:	Ezurio W66N220 Commerce Court, Cedarburg, WI 53012 USA tel: +1-262-375-4400 fax: +1-262-364-2649
Date of Issue:	2020, June 3
Name of Authorized Person:	Ryan Urness
Signature of Authorized Person:	

12 Telecommunications Regulatory Authority (TRA) Compliance

The RG186 has been tested for compliance with the relevant standards for the United Arab Emirates (UAE) market.

12.1 Labelling Requirements

The RG186 will contain the following information on the back of the gateway serial number label:
Registered No (ER61585/18): Registration number allocated by the TRA to the equipment.
RG186 TRA Registered Number: **ER61585/18**
Dealer No (DA72940/18): Dealer registration number allocated by the TRA to the dealer.
RG186 Dealer Registration Number: **DA72940/18**

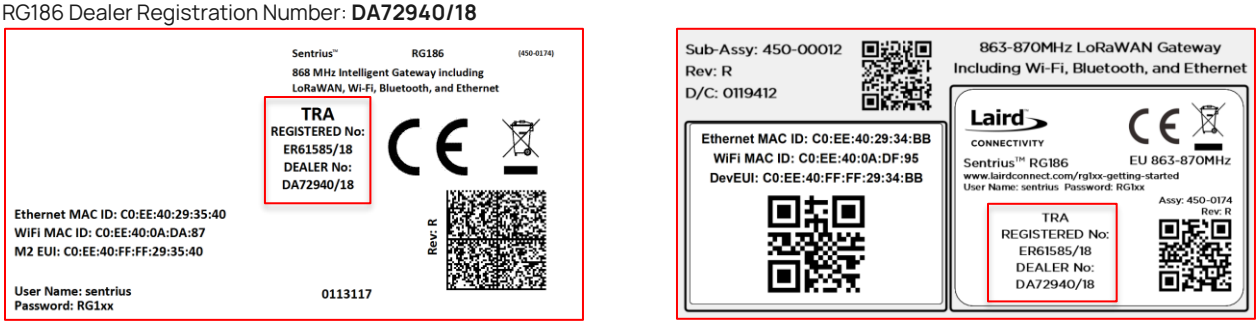


Figure 62: TRA Label Information (Standard GW – Left, AS923 & AU915 Region Supported/Latest Revision – Right)

13 Region Supported Labels

13.1 RG186 Version

The RG186 is compliant with UKCA & CE standards.

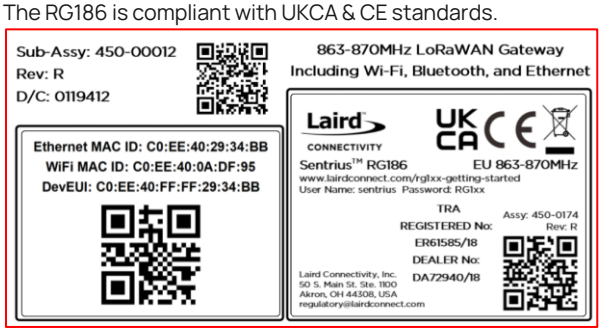


Figure 63: RG186 Region Supported Label

13.2 RG191 Version

The RG191 is the base for all current country variants:

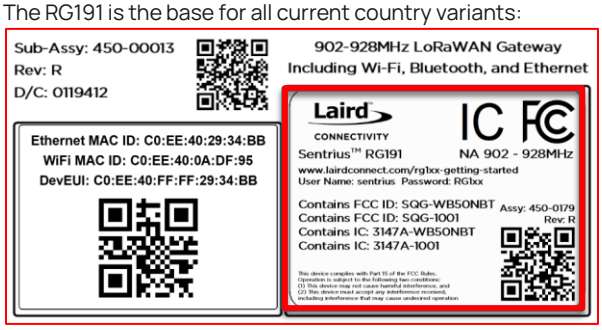


Figure 64: RG191 Region Supported Label

13.3 RG191+LTE Version

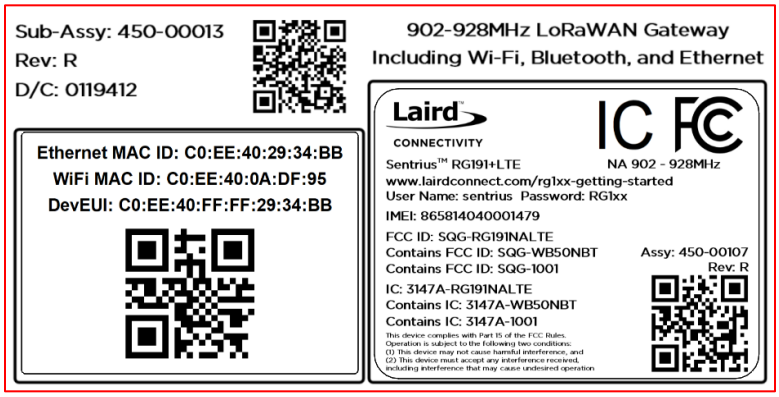


Figure 65: RG191+LTE Supported Label

13.4 AU915 & AS923 Regions

All region gateways will have a unique Product ID label which describes the region, any region certification label requirements, and frequency the gateway supports. This label is placed in the blue border shown in Figure 64. All labels are printed in black and white color.

13.4.1 Taiwan (TW)

Figure 66: Taiwan 923MHz Region Supported Label

13.4.2 New Zealand (NZ)

Figure 67: New Zealand 923MHz Region Supported Label

13.4.3 Hong Kong (HK)

Figure 68: Hong Kong 923MHz Region Supported Label

13.4.4 Australia (AU)

Figure 69: Australia 915 or 923MHz Region Supported Label (Frequency changes depending on setting)

13.4.5 Singapore (SG)

Figure 70: Singapore 923MHz Region Supported Label

14 Appendix: Outbound Network Services and Ports

Service	FQDN/IP	Port(s)	Protocol	Notes
Firmware update	ezurio.com, connectivity-firmware.s3.amazonaws.com	443	HTTPS	Used for over-the-air (OTA) firmware updates.
LoRaWAN forwarder	Dependent on forwarder and server selection	Dependent on forwarder and server selection	UDP, TCP/TLS	Handles transmission of LoRaWAN packets between the gateway and the configured LoRaWAN network server.
DNS client	Dependent on DHCP or static IP configuration	53	DNS/UDP	Used for resolving domain names to IP addresses across all network-related operations.
Time Synchronization (NTP)	time.google.com, time.aws.com, time.cloudflare.com	123	NTP/UDP	Required for time synchronization. LoRaWAN forwarders rely on this.
Internet connectivity check	cloudflare.com, openwrt.org, github.com, google.com	53	DNS/UDP, ICMP	Performs basic internet health checks by resolving hostnames and pinging IPs from each active network interface.
TR069 device management (easycwmpd)	Dependent on customer server	80, 443	HTTP, HTTPS	Optional service for remote device provisioning and management via TR-069 protocol, if configured by the customer.
Memfault (memfaultd)	memfault.com	443	HTTPS	Enables remote diagnostics and performance monitoring. Only active if enabled by the customer.

15 Additional Information

Please contact your local sales representative or our support team for further assistance:

Headquarters	Ezurio 50 S. Main St. Suite 1100 Akron, OH 44308 USA
Website	http://www.ezurio.com
Technical Support	http://www.ezurio.com/resources/support
Sales Contact	http://www.ezurio.com/contact

Note: Information contained in this document is subject to change.

Ezurio's products are subject to standard Terms & Conditions.