User Guide

Sentrius RG1xx

Version 4.1

REVISION HISTORY

Ver.	Date	Notes	Contributor(s)	Approver
1.0	20 July	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 the 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

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

CONTENTS

3
Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

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.

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

Laird'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 Laird'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 Laird'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.

Figure 1: Top of the Sentrius™ RG1xx gateway
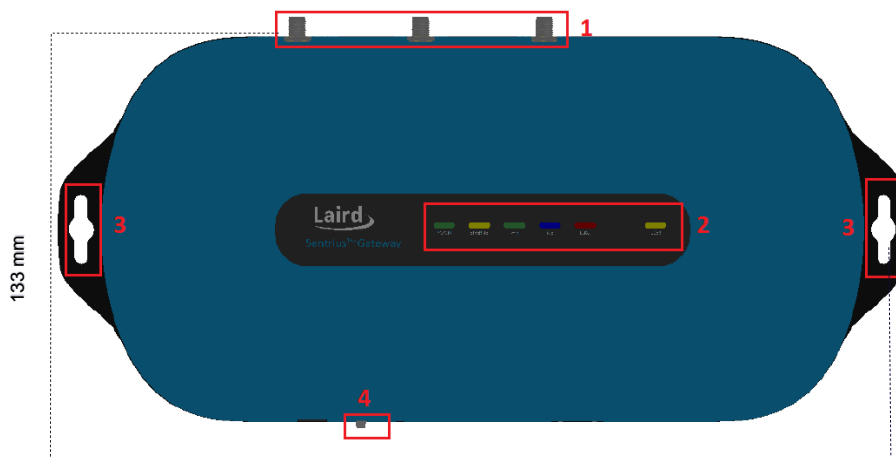
1. LoRa and Wi-Fi antennas
2. LEDs
3. Mounting holes
4. User button

Figure 2: Side panel of the Sentrius™ RG1xx gateway

5. DC power input
6. User button
7. Reset button
8. SD card slot
9. Ethernet connector

5

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

2.2 Specification

Category	Feature	Specification
Chipset	**LoRa®**	Semtech SX1301/SX1257
	Bluetooth®	Cambridge Silicon Radio CSR8811 A08
	Wi-Fi	Qualcomm Atheros QCA6004
Wireless Characteristics	**Wi-Fi Spatial Streams**	2x2 MIMO
	Wi-Fi Frequencies	2.4 and 5 GHz operation
	Conducted Maximum Transmit Power *Note: Transmit power on each channel varies according to individual country regulations. All values for lowest data rate are nominal, +/-2 dBm. Others are +/-2.5 dBm* *Note:* *HT40 – 40 MHz-wide channels* *HT20 – 20 MHz-wide channels*	**802.11a (UNII-1, UNII-2A, UNII-2C) or CH 36 – CH140** 6 Mbps — 17 dBm 54 Mbps — 14 dBm **802.11a (UNII-3) or CH 148 – CH 165** 6 Mbps — 15 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) (UNII-1, UNII-2A, UNII-2C) or CH 36 – CH140** 6.5 Mbps (MCS0, HT20) — 17 dBm 65 Mbps (MCS7, HT20) — 13 dBm (MCS0, HT40) — 14 dBm (MCS7, HT40) — 11 dBm **802.11n (5 GHz) (UNII-3) or CH 148 – CH 165** 6.5 Mbps (MCS0, HT20) — 15 dBm 65 Mbps (MCS7, HT20) — 12 dBm (MCS0, HT40) — 14 dBm (MCS7, HT40) — 11 dBm **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 54 Mbps — -74 dBm (PER <= 10%) **802.11n (2.4 GHz)** 6.5 Mbps (MCS0) — -91 dBm 65 Mbps (MCS7) — -71 dBm

Category	Feature	Specification		
		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		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	
	LoRa Frequencies, LoRaWAN Region, UL/DL, Laird part number	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	
		MY	919 – 924 MHz (LoRaWAN AS923, UL/DL) – 455-00101	
		SG	920 – 925 MHz (LoRaWAN AS923, UL/DL) – 455-00102	
		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	
	LoRa Radio Conducted TX Power (at -40°C) (RG191 plus AS915 & AU923 variants)	TWN	25 dBm (max entry in Radio TX Power Table)	
		HK	25 dBm (max entry in Radio TX Power Table)	
		MY	25 dBm (max entry in Radio TX Power Table)	
		SG	27 dBm (max entry in Radio TX Power Table)	
		US, NZ, AUS, TWN, HK, MY, 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	Wireless		
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		

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

Category	Feature	Specification
	LoRa	Packet Network Forwarder with default support for the following: ▪ The Things Network with Semtech Basic Station or UDP forwarder ▪ Stream communications with UDP forwarder ▪ ChirpStack with UDP forwarder or Semtech Basic Station ▪ Senet through legacy Semtech UDP or proprietary Senet forwarder
	Configuration	Web-based interface via Ethernet/Wi-Fi
Physical	Dimensions	133 x 275 x 30 mm (enclosure only)
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 **Malaysia –** TBC **Singapore –** TBC
Wi-Fi Antenna	Model	Laird 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	Laird 001-0028 (863-870 MHz) used with RG186 Laird 001-0002 (902-928 MHz) used with RG191 plus AS915 and AU923 variants
	Type	Dipole
	Connector	RP-SMA
	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
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 1 x External DC power adapter

Category	Feature	Specification
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
RG186	Sentrius™ RG191 US (US902-928) 915 MHz Gateway - LoRaWAN, Wi-Fi, and Ethernet – US Power Adapter
RG191	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™ RG191 US (US902-928) 915 MHz Gateway – LoRaWAN, Wi-Fi, and Ethernet – IP67
450-0191	Sentrius™ RG186 Europe (EU868) 868 MHz Gateway – LoRaWAN, Wi-Fi, and Ethernet – IP67
455-00054	Sentrius™ RG191 New Zealand (AS923) 923 MHz Gateway – LoRaWAN, Wi-Fi, and Ethernet – NZ Power Adapter
455-00055	Sentrius™ RG191 Hong Kong (AS923) 923 MHz Gateway – LoRaWAN, Wi-Fi, and Ethernet – HK Power Adapter
455-00056	Sentrius™ RG191 Australia (AU915+AS923) 923 MHz Gateway – LoRaWAN, Wi-Fi, and Ethernet – AU Power Adapter
455-00057	Sentrius™ RG191 US (US902-928) 915 MHz Gateway - LoRaWAN, Wi-Fi, and Ethernet – US Power Adapter
The following regions orderable from - TBD	
455-00101	Sentrius™ RG191 Malaysia (AS923) 923 MHz Gateway – LoRaWAN, Wi-Fi, and Ethernet – UK Power Adapter
455-00102	Sentrius™ RG191 Singapore (AS923) 923 MHz Gateway – LoRaWAN, Wi-Fi, and Ethernet – UK Power Adapter
Accessories	
690-1002	Pole Mount Bracket - Accessory for 450-0190 or 450-0191
690-1003	Wall Mount Bracket - Accessory for 450-0190 or 450-0191

https://www.lairdconnect.com/
9
© Copyright 2020 Laird Connectivity.
All Rights Reserved

Americas: +1-800-492-2320
**Europe**: +44-1628-858-940
Hong Kong: +852 2923 0610

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 antennas. Refer to *Antenna Configuration* 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.
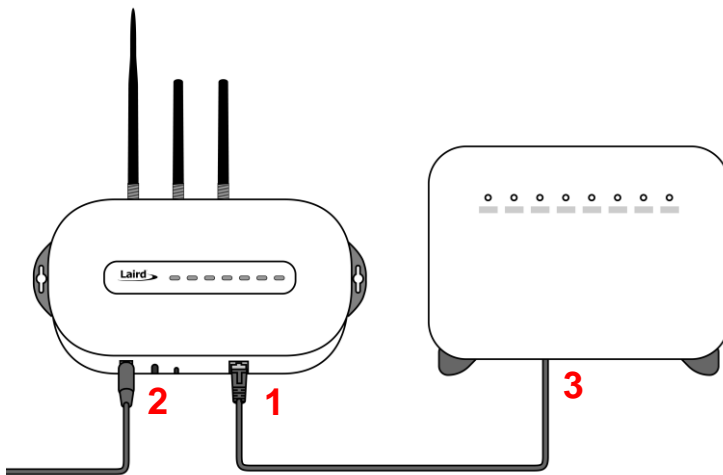
Figure 3: Connecting the gateway

3.1.1   Antenna Configuration

To configure the antenna properly, do the following:

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.
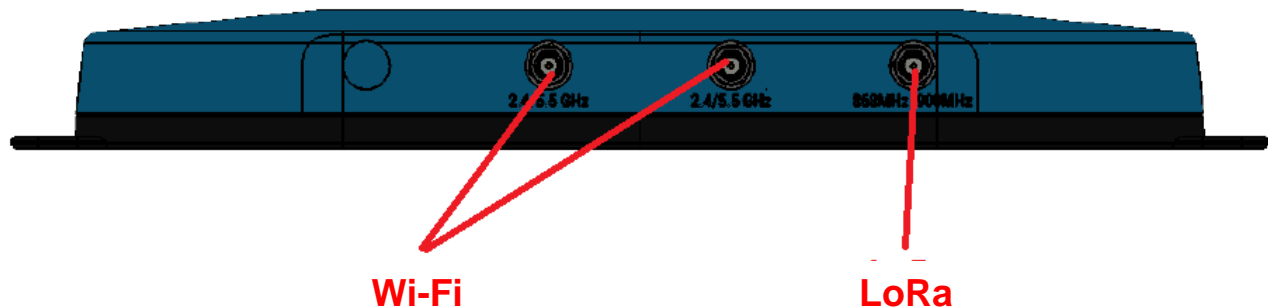
3.1.2 Wi-Fi Quick Configuration

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.

The gateway includes a mode to allow you to configure without ethernet access, in the case that you wish to join a wireless network.

Apply power to the gateway and allow to start, then perform the following:

1. Depress and hold the user button (see #2 in Figure 2) for seven seconds.
2. From a wirelessly enabled device perform a scan.
3. Connect to the access point rg1xx**29378B**, where *29378B* are the last six digits of the Ethernet MAC address found on the label on the bottom of the gateway (*Figure 4*).

   The network is secured with WPA2 with 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 on the
   Wi-Fi > Advanced web page.

Upon logout or client disassociation, 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 4*).


Figure 4: 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 5).
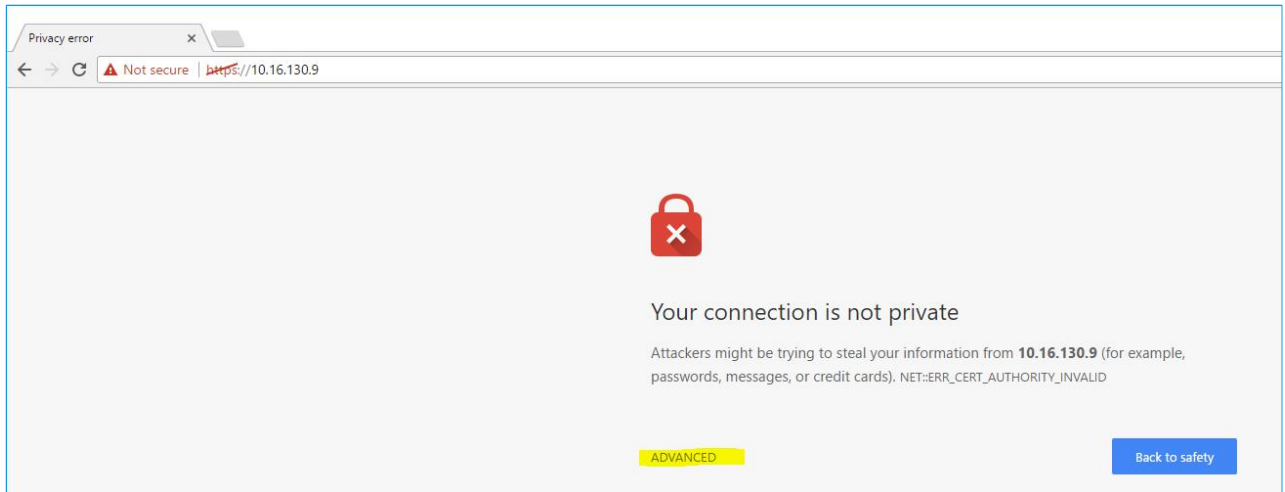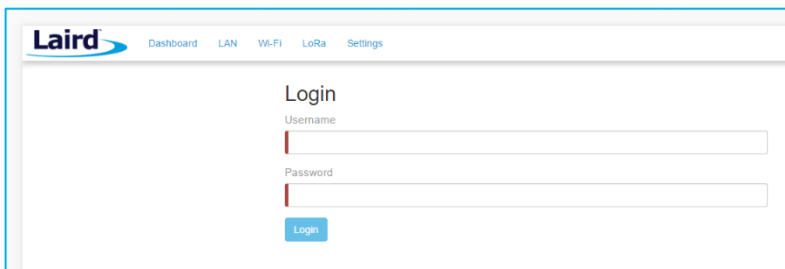
Figure 5: Web interface – first screen

5. Click **Proceed** (Figure 6).
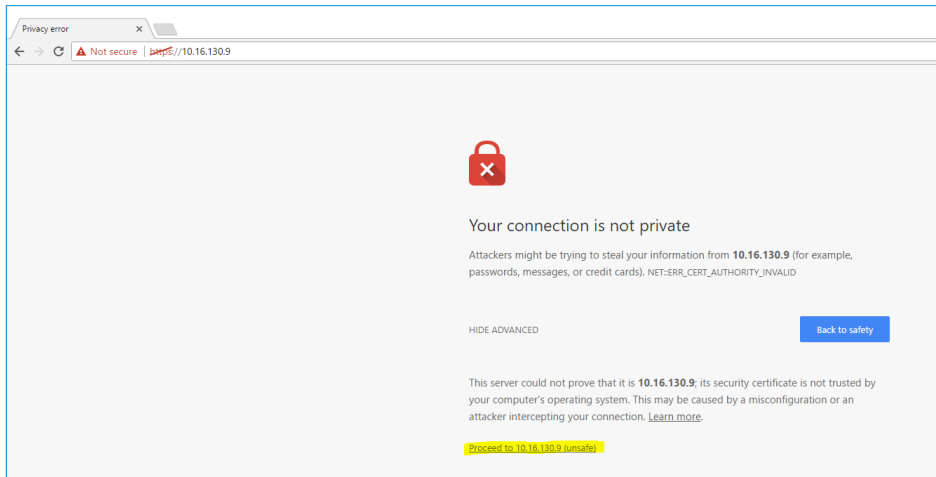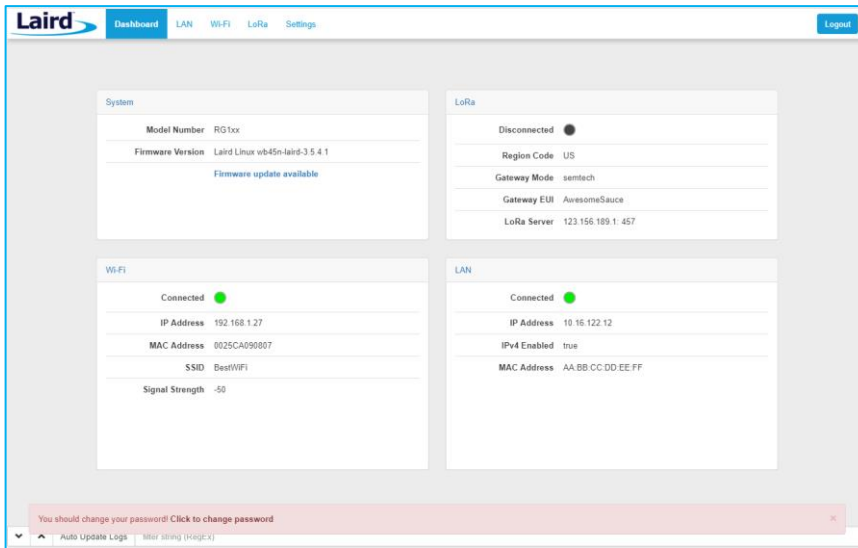

Figure 6: Web interface – second screen

6. Log on using the following default credentials:
   Username: sentrius
   Password: RG1xx

Figure 7: Gateway interface login screen

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

After logging in, the program warns you to change the default credentials for security reasons (Figure 8).

Figure 8: 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 9).
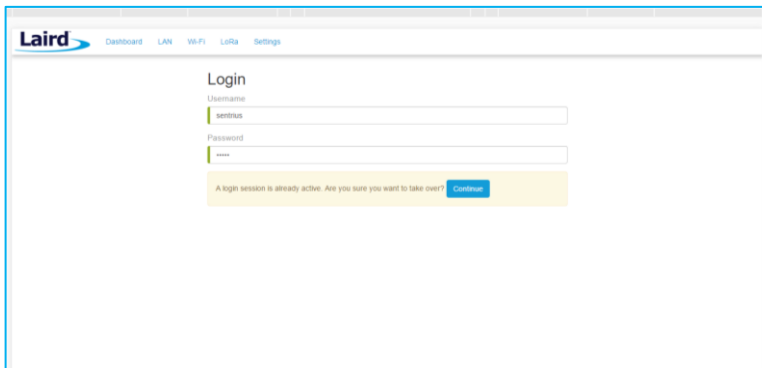
Figure 9: Active session warning

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

5   LAN CONNECTION SETUP

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

5.1   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 10). The gateway factory default setting is DHCP.

Figure 10: 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.

5.2   IPv6 Configuration

Select the IPv6 configuration by clicking the IPv6 menu item in the side menu of the LAN view (Figure 10). 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). As of June 2017, IPv6 static mode is only partially supported. Please see the software release notes for current information.

Figure 11: IPv6 Configuration page

5.3   Advanced View

Select the advanced view by clicking the Advanced menu item in the LAN sidebar (Figure 12). 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 12: Advanced view

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

6 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 13).
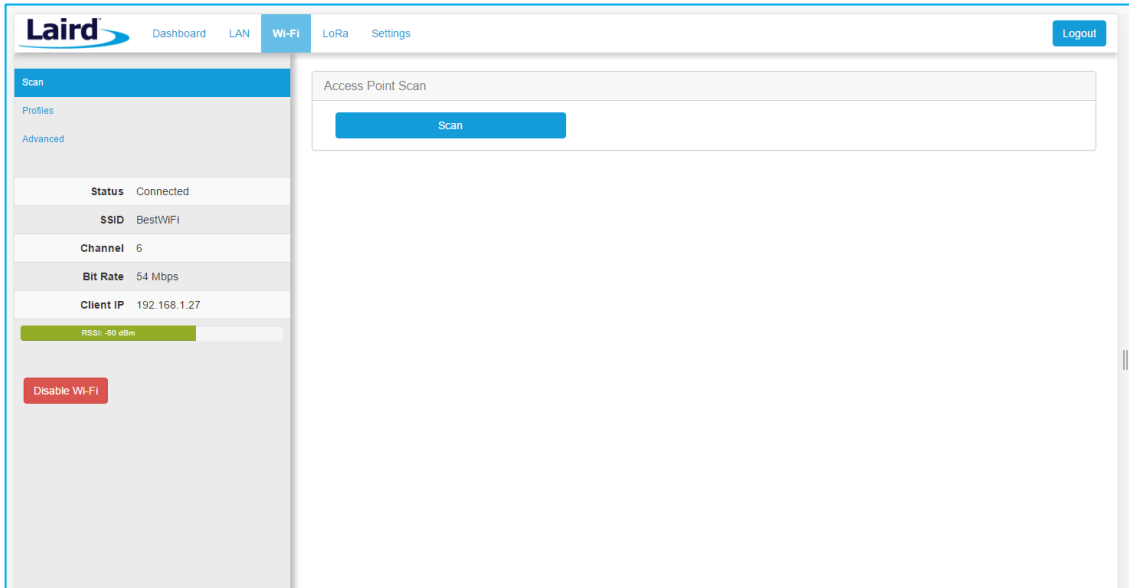
Figure 13: Wi-Fi connection setup

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.

6.1 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 14).
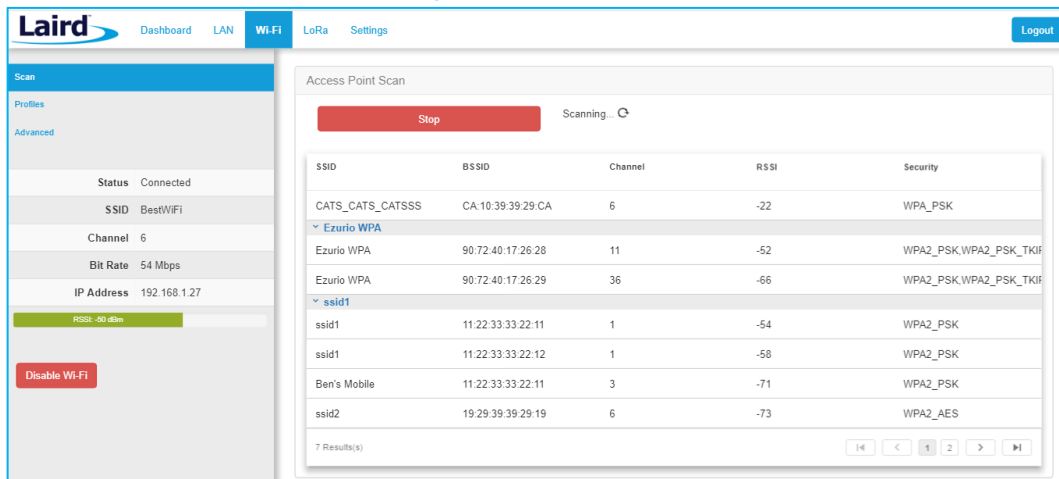
Figure 14: Scan function

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 15).
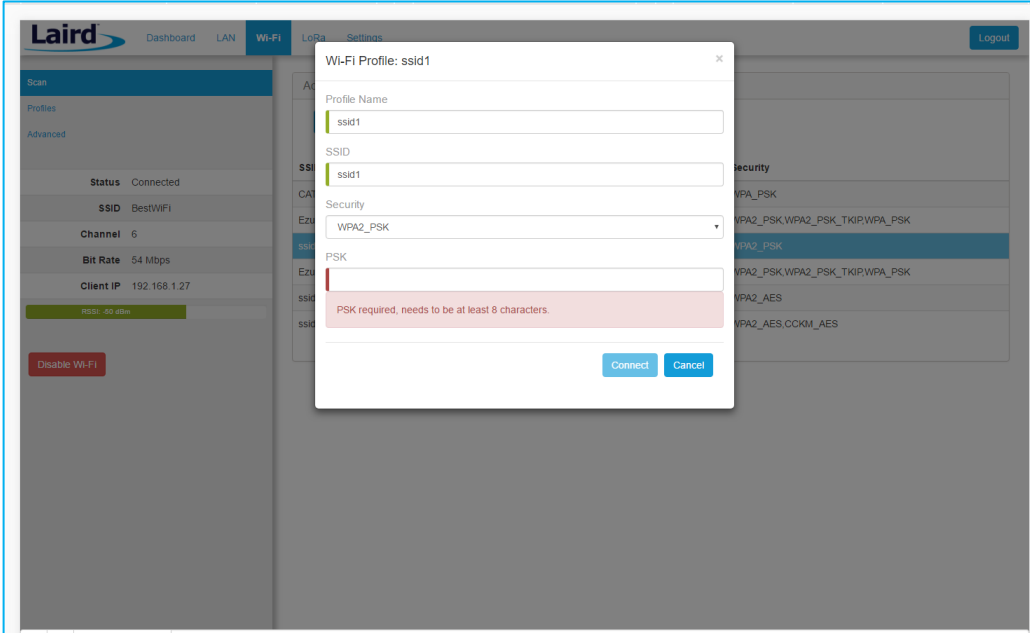
Figure 15: Wi-Fi profile window

6.2   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 in the left menu. This page is useful for adding a hidden Wi-Fi network that is not broadcasting its SSID (Figure 16).
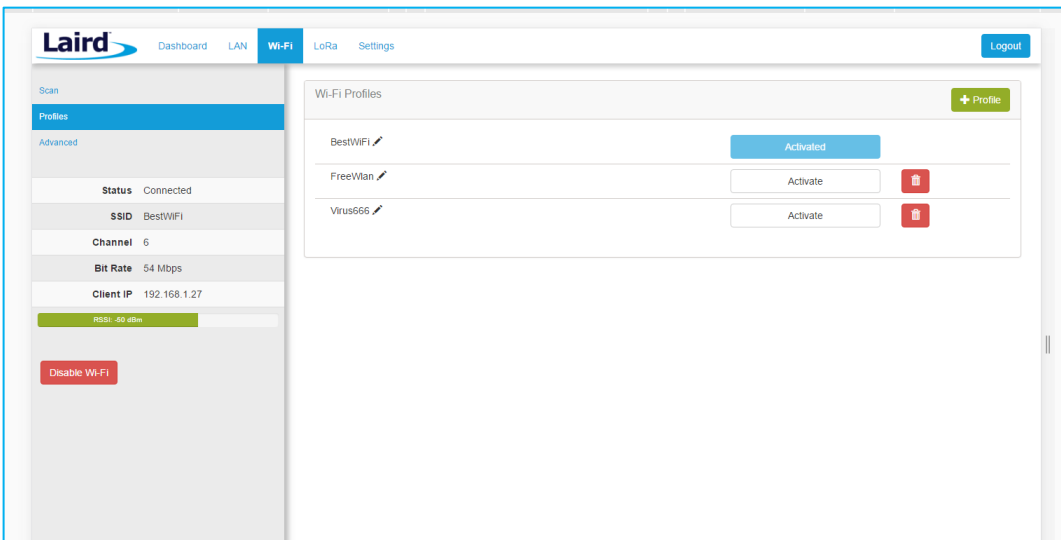
Figure 16: Wi-Fi profiles page

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 17).
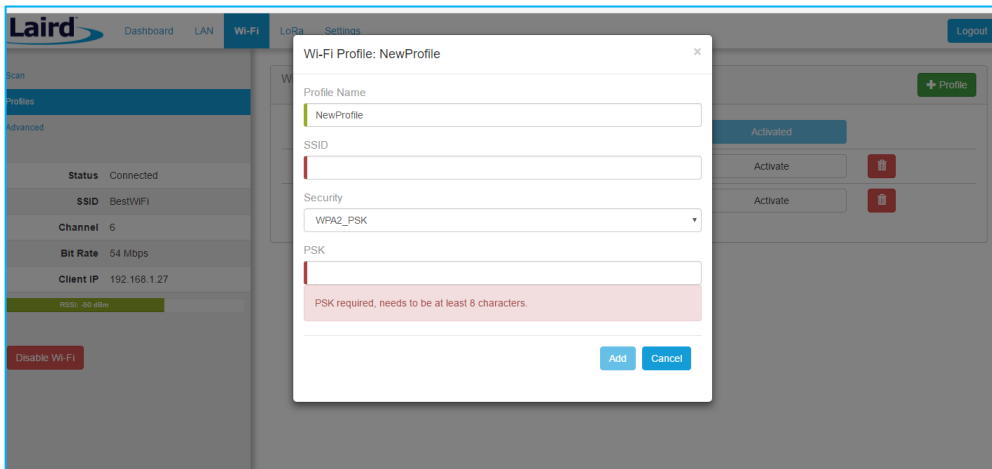
Figure 17: Wi-Fi profile dialog

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

6.3 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 18).
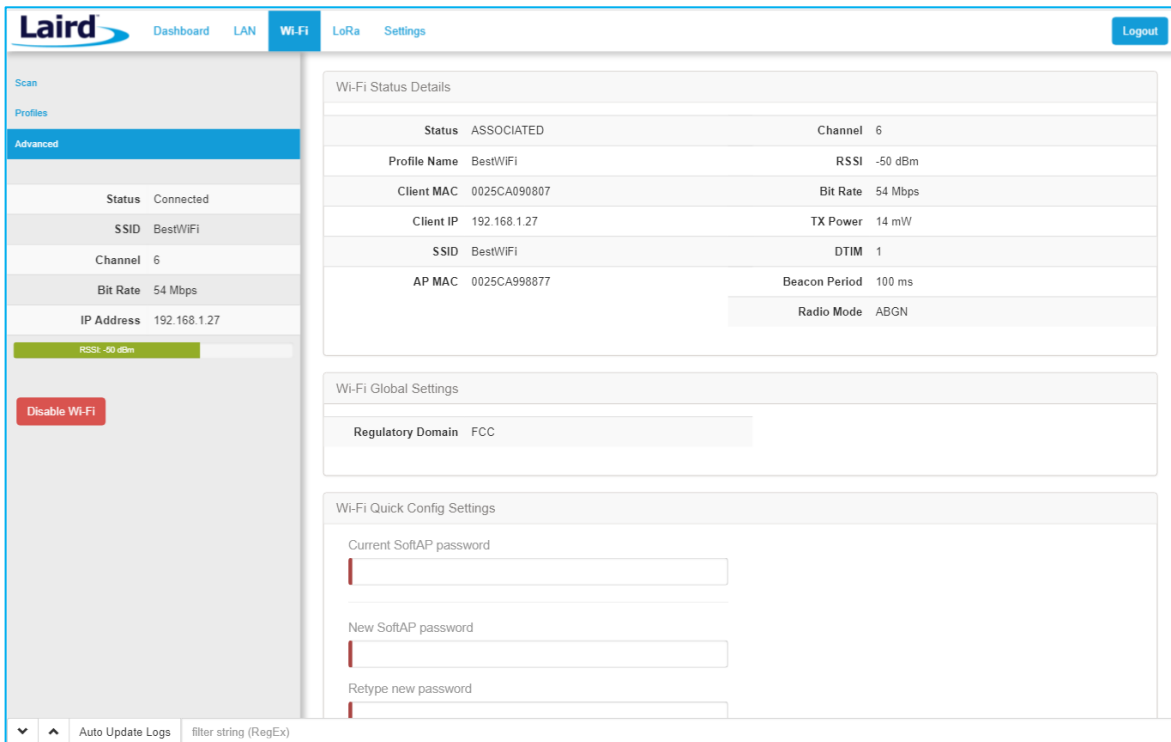
Figure 18: Wi-Fi Advanced page

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

7 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 19).

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.
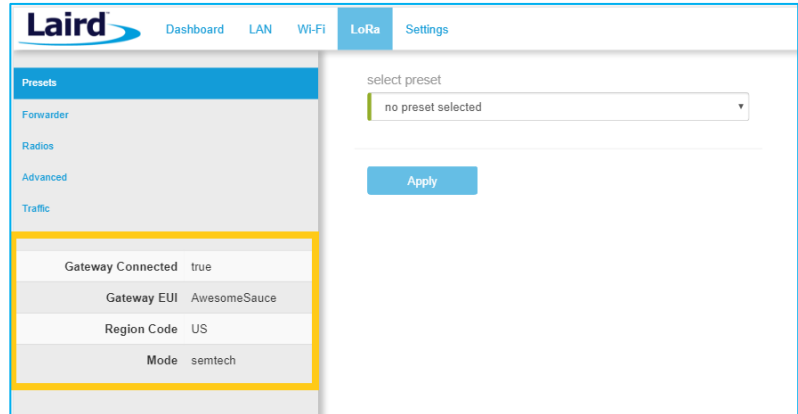
Figure 19: LoRa connection setup page

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

7.1 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 21).
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.
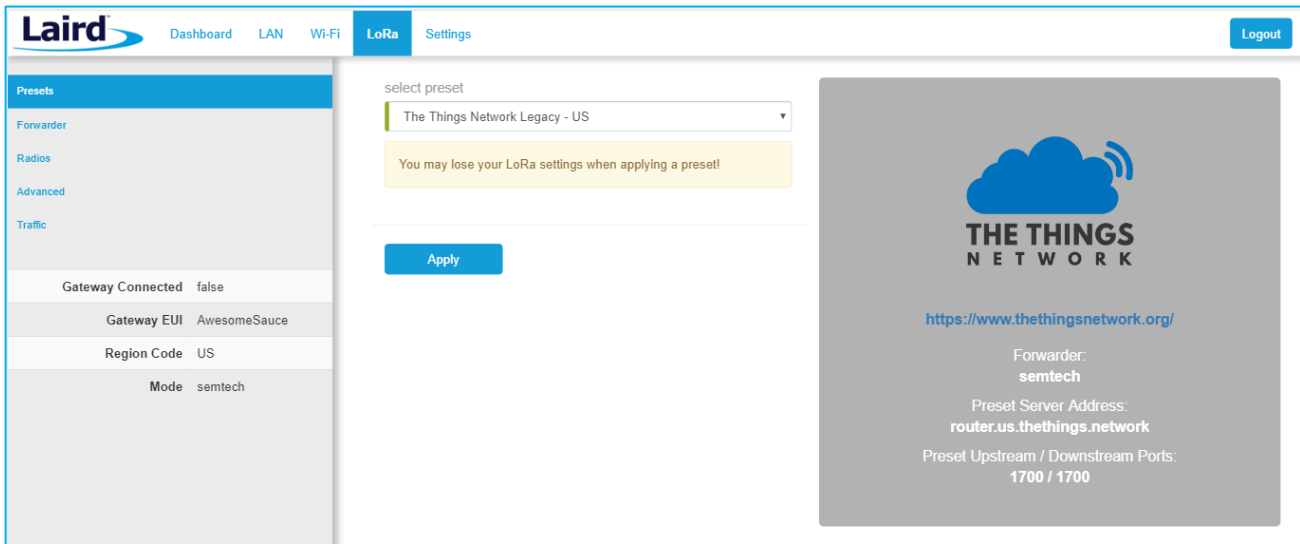
Figure 21: Selecting a preset configuration

7.2 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.

7.2.1 Mode

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

7.2.2 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 22: LNS server

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610
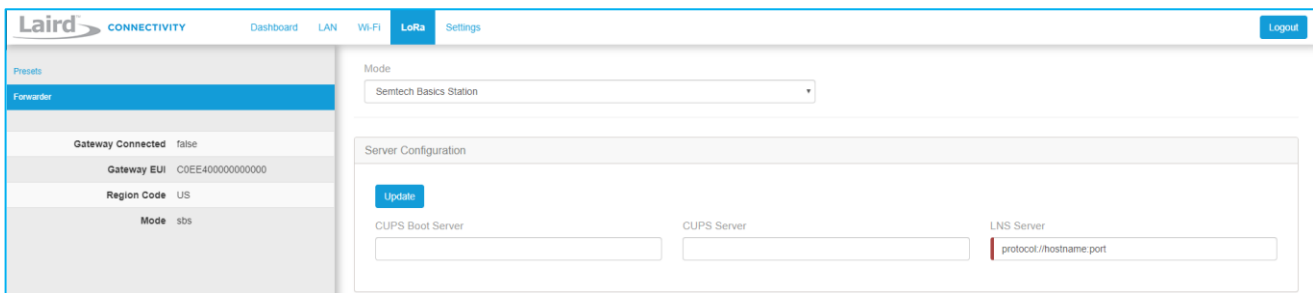
7.2.3 Certificates

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 upload 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 23: Certificate selection

7.2.4 Connection Status

7.2.4.1 LoRa View

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

Figure 24: LoRa view

7.2.4.2 Dashboard View

In the Dashboard view, the status is shown with a circle that will be green when connected and black when disconnected.
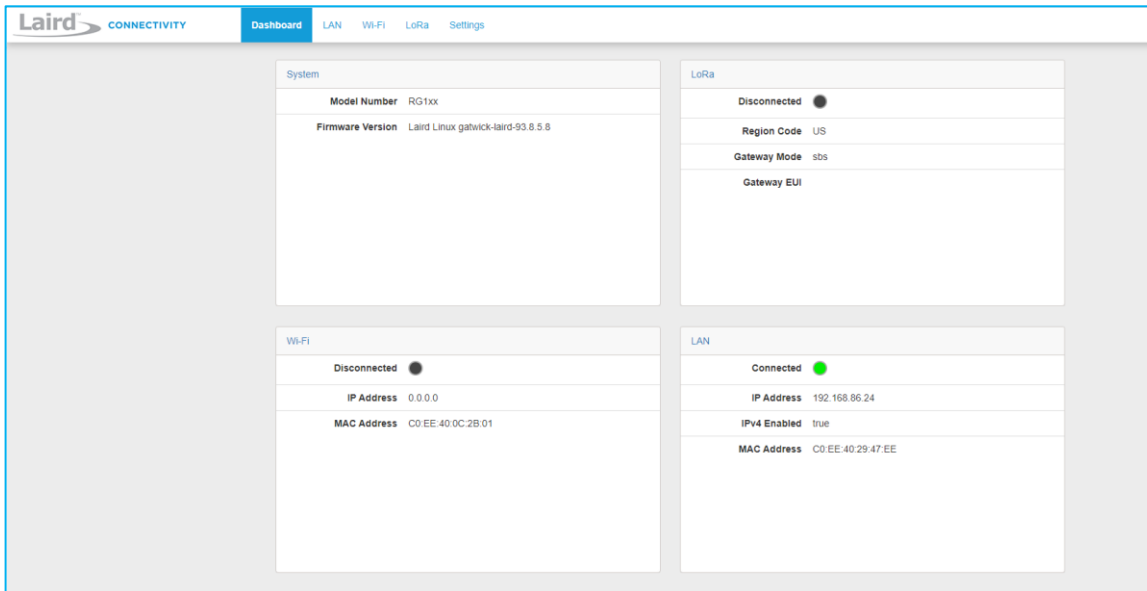
Figure 25: Dashboard view

7.3 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.

7.4 Semtech Legacy UDP Forwarder

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

7.4.1 Mode

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

https://www.lairdconnect.com/ 22
© Copyright 2020 Laird Connectivity.
All Rights Reserved
Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

7.4.2 Configuration

The configuration changes based on what packet forwarder is used.

Figure 26: Semtech packet forwarder configuration

7.4.3 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.

7.4.3.1 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.
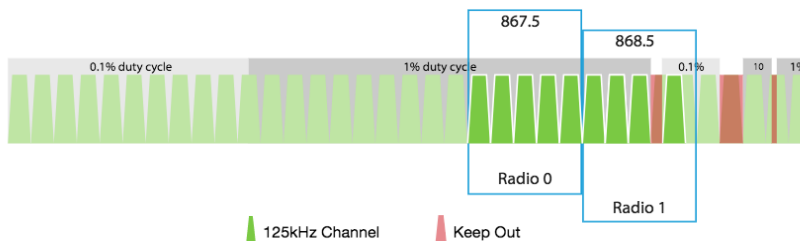
Figure 27: Channel plan graphic

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

7.4.3.2 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 28).
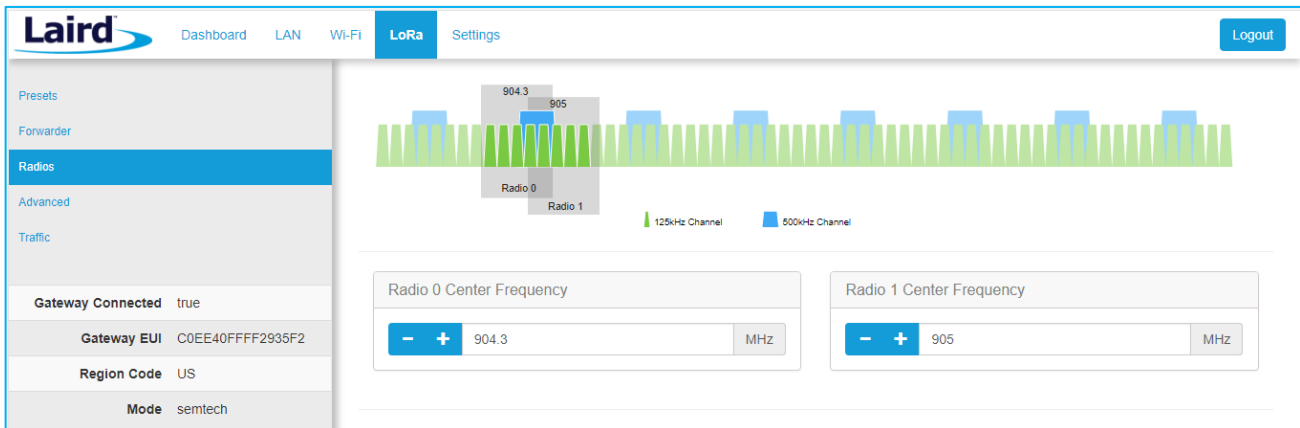
Figure 28: Channel assignments

7.4.3.3 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 30). Channel configuration is shown in Figure 29.
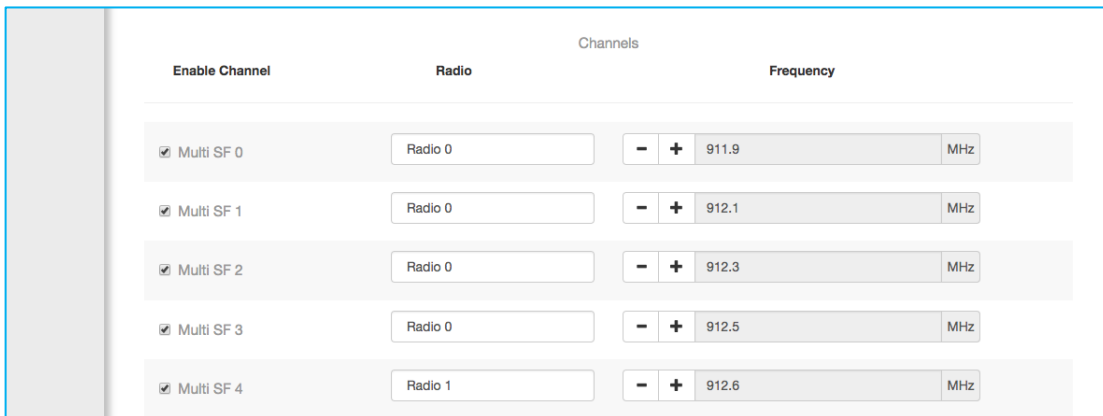
Figure 29: Channels window

https://www.lairdconnect.com/ 24
© Copyright 2020 Laird Connectivity.
All Rights Reserved

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610
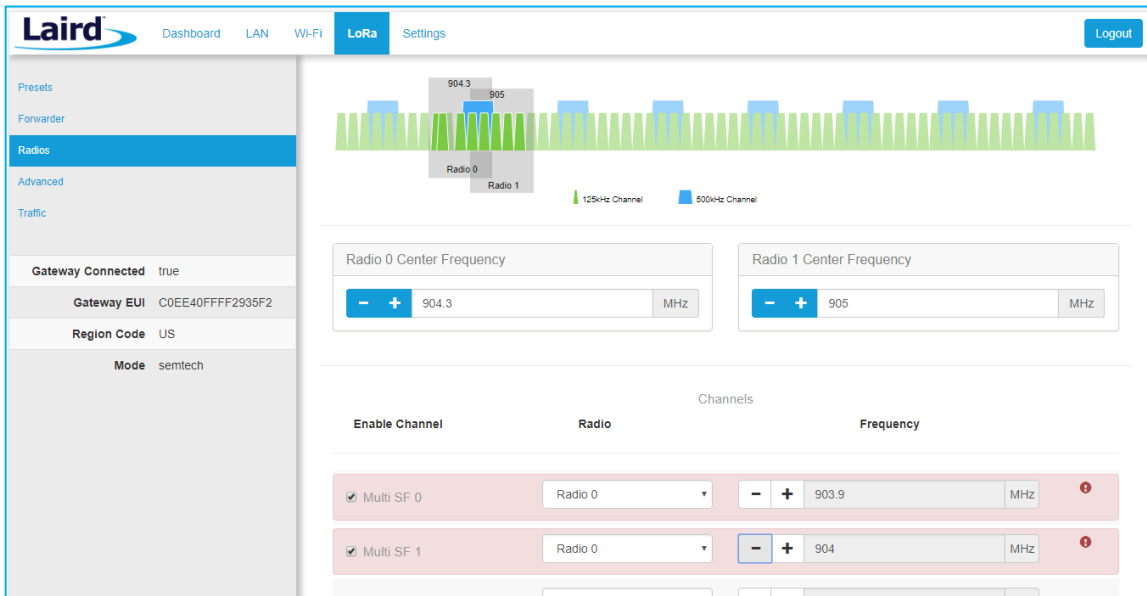
Figure 30: Overlapping channels

7.4.3.4 LoRa Radio Card (US)

Gateways that operate in the US region should have a 500-kHz channel. In Figure 31, the allowed placement of these channels displays larger and blue.

If a 500-kHz channel is not configured, the interface displays a warning.
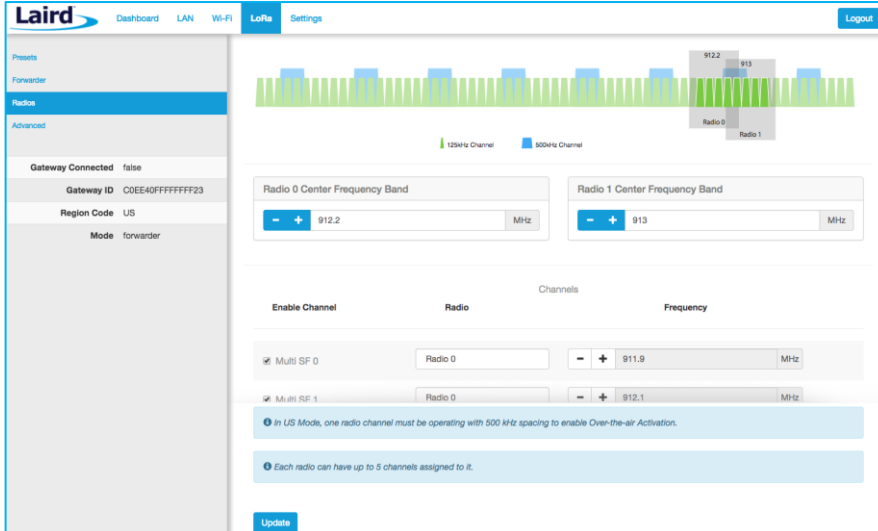
Figure 31: US region gateways

7.4.3.5 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 32. A higher duty cycle allows higher throughput.

https://www.lairdconnect.com/
25
© Copyright 2020 Laird Connectivity.
All Rights Reserved

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

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.
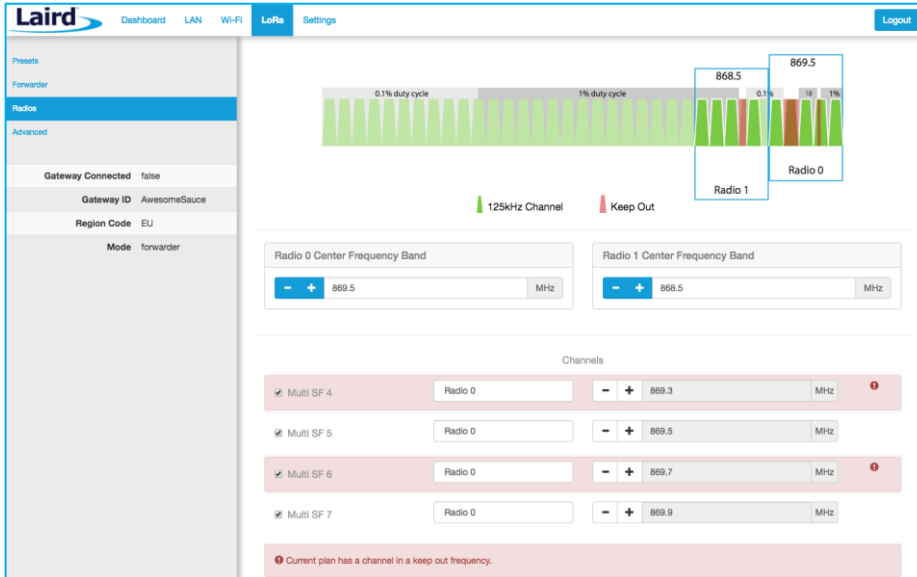
Figure 32: EU region gateways – keep out channels

7.4.4 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.
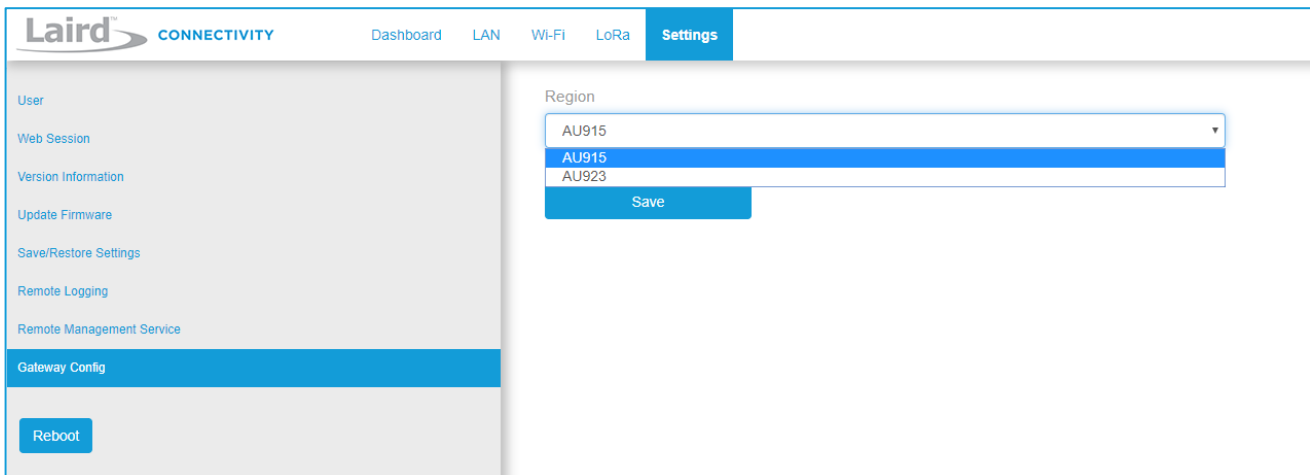
Figure 33: Australia region selector

7.4.4.1 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.

7.4.4.2 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.

7.4.5 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.

7.4.6 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.

7.4.7 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.

7.4.8 LoRa Radio Card (Malaysia)

The region code is MY. 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.

7.4.9 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.

7.5 Advanced Configuration

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

Figure 34: 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 35).

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 35: Current configuration file

https://www.lairdconnect.com/ 28

© Copyright 2020 Laird Connectivity.
All Rights Reserved

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

7.6   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 36: LoRa traffic

Clicking on a traffic row displays packet details.

Figure 37: LoRa packet details

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

8 MANAGE THE GATEWAY

8.1 Changing Username and Password

To change the login credentials of the gateway, follow these steps:
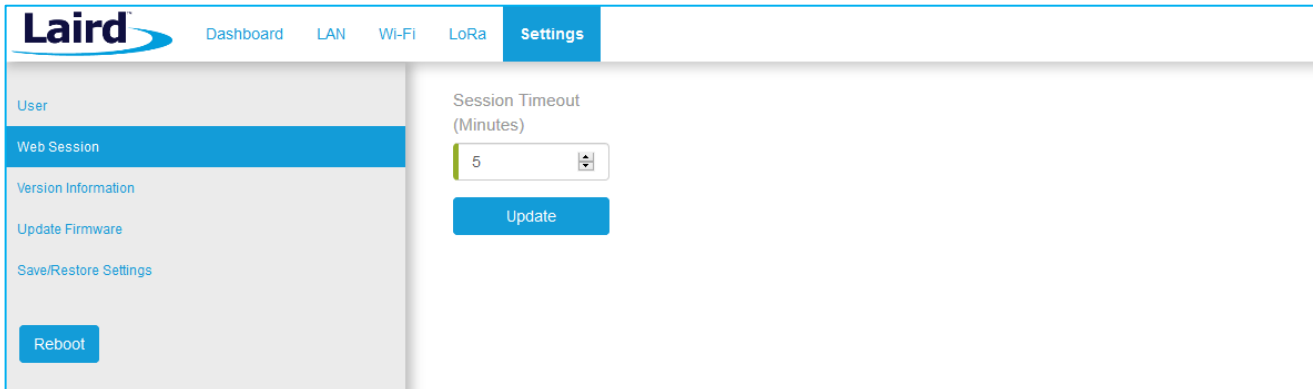
1. In the main menu, click the **Settings** tab. Then in the left menu, click the **User** tab (Figure 38).
2. Enter the current password, and then the new desired username and password.
3. Click **Update**.

Figure 38: Change username and password

8.2 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 39: Change web session time out

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

8.3   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, New Build Available row displays.
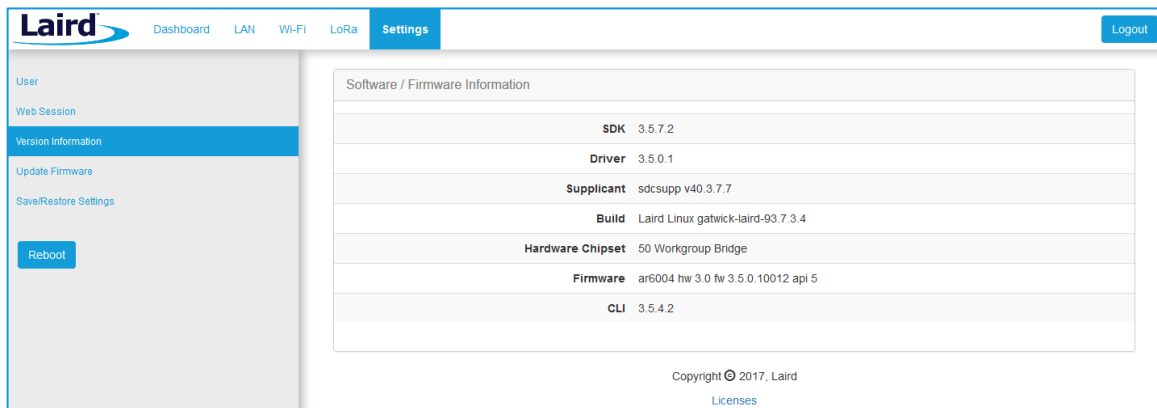
Figure 40: Version information

8.4   Updating Gateway Firmware

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

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

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

8.4.1 Firmware Update URLs

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

8.4.1.1   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.lairdtech.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.

8.4.1.2   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.lairdtech.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.**

8.4.1.3   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.lairdtech.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.**

8.4.1.4   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 next version:

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

Note: This requires users to manually update the URL!

After updating with this link, the gateway will be running GA3 firmware (93.7.3.x) or newer. Follow the instructions for that version to update to the latest version of firmware.

8.4.1.5   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.

8.4.1.6   *GA4 Firmware (93.8.4.28)*

8.4.1.7   *GA4.1 Firmware (93.8.4.37)*

`https://www.lairdtech.com/products/rg1xx-lora-gateway/firmware/GA4.1/fw.txt`

8.4.1.8   *GA5 Firmware (93.8.5.18)*

8.4.1.9   *GA5.1 Firmware (93.8.5.21) is the latest release*

The firmware update process downloads the firmware to the gateway and then flashes it.
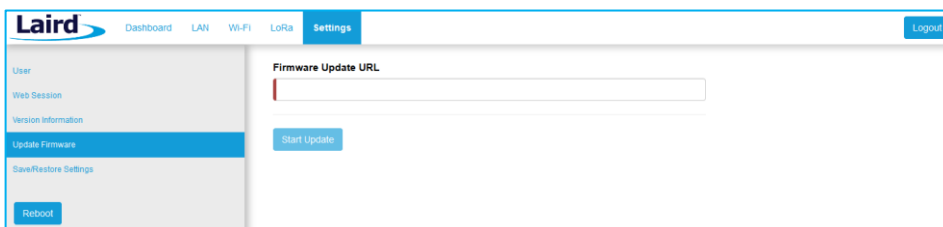
Figure 41: Updating gateway firmware window

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

During the firmware update, the progress displays as shown in Figure 42.
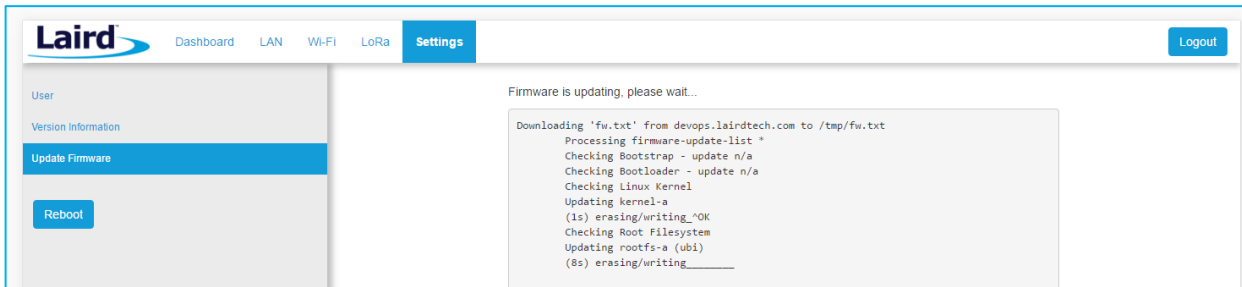
Figure 42: Progress indicator

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 43).
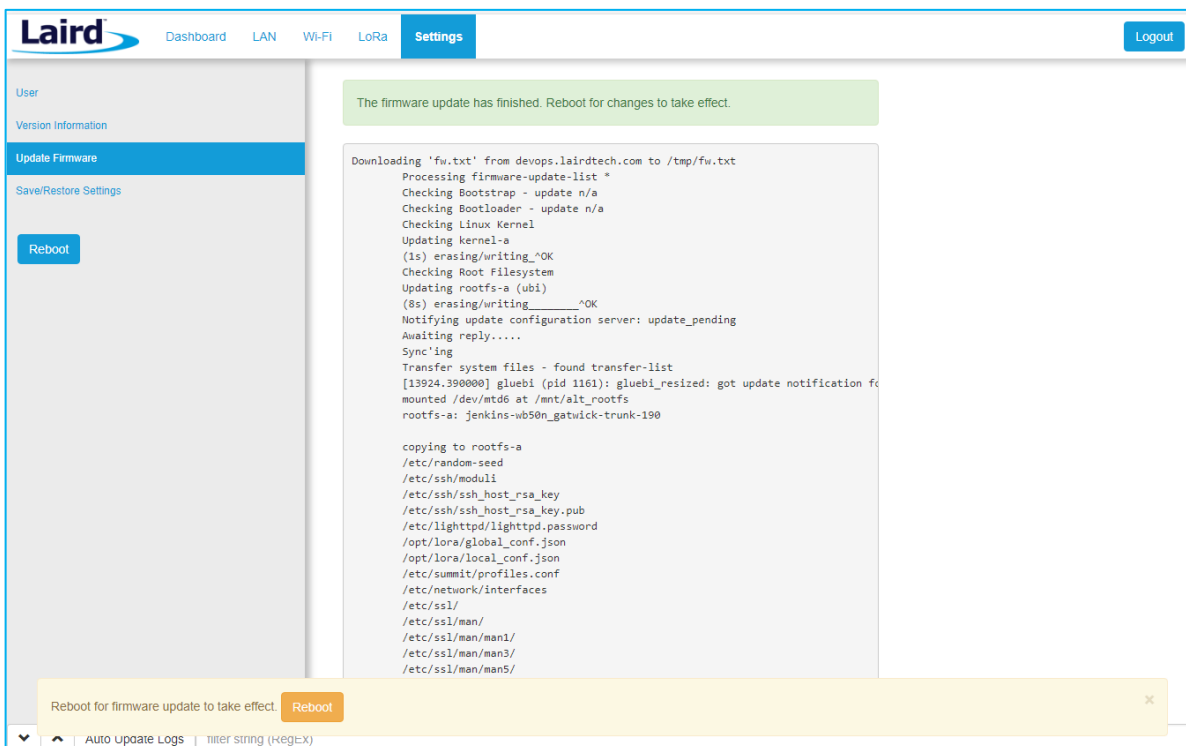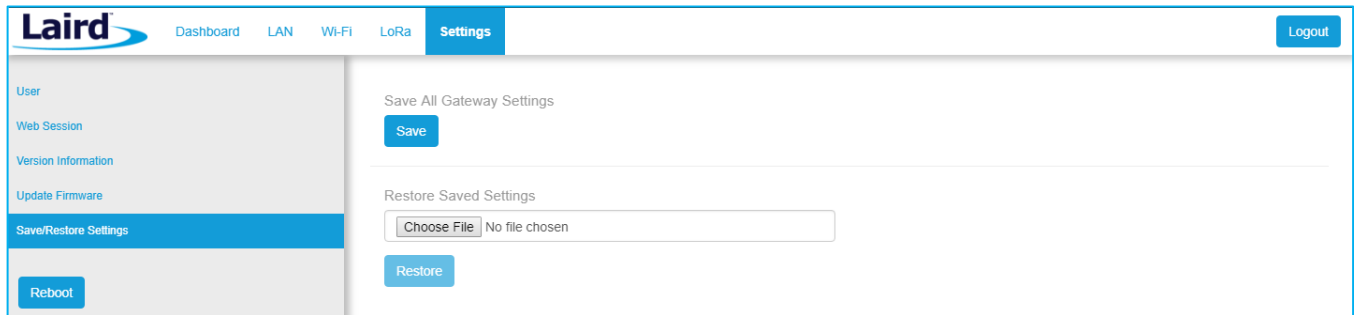
Figure 43: Reboot prompt

8.5   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 44: Save/Restore settings

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

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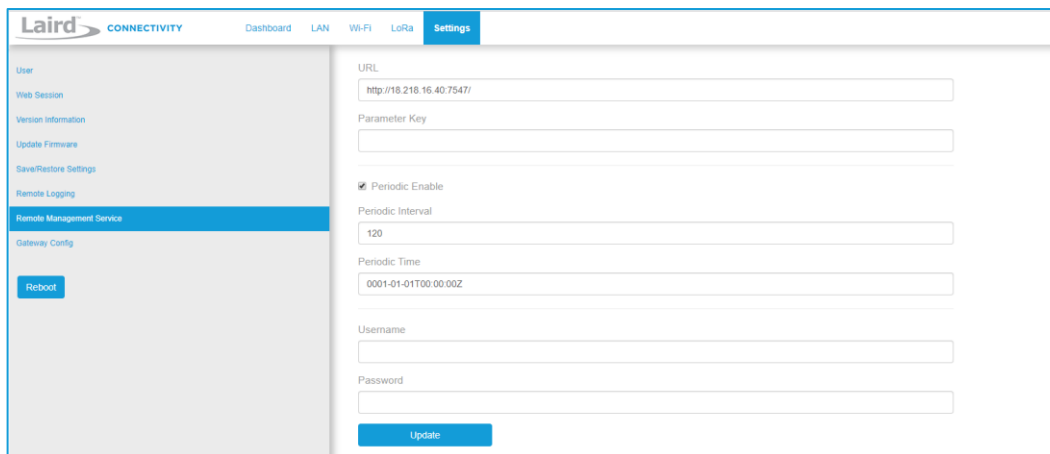
The gateway can be managed remotely via TR-069. It requires an externally hosted Auto Configuration Server (ACS) to use this feature. This allows a system administrator to access the gateways without needing physical access to the gateway or access behind a firewall. The gateway will periodically initiate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

8.6.1 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 45: Save/Restore settings

8.6.2 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.Laird.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.Laird.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.

8.6.3 Configuration File Upload

8.6.3.1 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.

8.6.4 Configuration File Download

8.6.4.1 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.

8.6.4.2 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.

8.6.5 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.

8.6.5.1 InternetGatewayDevice.Laird.DeviceInfo

Table 2: InternetGatewayDevice.Laird.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

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

Parameter Name	R/W	Description	Input Data
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

8.6.5.2 *InternetGatewayDevice.Laird.ActiveProfileSettings*

Table 3: InternetGatewayDevice.Laird.ActiveProfileSettings

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.Laird.ActiveProfileSettings	O	Active Wi-Fi profile node	N/A
InternetGatewayDevice.Laird.ActiveProfileSettings.ProfileName	R/W	Wi-Fi profile name (not SSID)	String representing the profile name
InternetGatewayDevice.Laird.ActiveProfileSettings.SSID	R/W	Wi-Fi network SSID	String representing the SSID
InternetGatewayDevice.Laird.ActiveProfileSettings.PSK	W	Wi-Fi network preshared key	String representing the PSK
InternetGatewayDevice.Laird.ActiveProfileSettings.ClientName	R/W	Wi-Fi network client name	A string representing name client name.
InternetGatewayDevice.Laird.ActiveProfileSettings.TxPower	R	TX power	A numeric value representing TX power
InternetGatewayDevice.Laird.ActiveProfileSettings.AuthType	R/W	Wi-Fi network authentication type	open, shared, or eap
InternetGatewayDevice.Laird.ActiveProfileSettings.EAPType	R/W	Wi-Fi network EAP type	leap, eap-fast, peap-mschapv2, eap-tls, peap-tls
InternetGatewayDevice.Laird.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.Laird.ActiveProfileSettings.Mode	R/W	Wi-Fi network mode	BGN
InternetGatewayDevice.Laird.ActiveProfileSettings.Powersave	R	Is power save enabled	off,max,fast
InternetGatewayDevice.Laird.ActiveProfileSettings.PSPDelay	R	Power save delay	A value 10 - 500 in milliseconds
InternetGatewayDevice.Laird.ActiveProfileSettings.Username	R/W	Username used by some authentication methods	A string representing the username
InternetGatewayDevice.Laird.ActiveProfileSettings.Password	W	Password used by some authentication methods	A string representing the password

8.6.5.3 InternetGatewayDevice.Laird.WIFIGlobalSettings

Table 4: InternetGatewayDevice.Laird.WIFIGlobalSettings

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

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.Laird.WIFIGlobalSettings.DefaultAdhocCh	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Laird.WIFIGlobalSettings.DFSChannels	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Laird.WIFIGlobalSettings.FIPSMode	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Laird.WIFIGlobalSettings.IgnoreNullSSID	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Laird.WIFIGlobalSettings.PMKCaching	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Laird.WIFIGlobalSettings.ProbeDelay	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Laird.WIFIGlobalSettings.RegulatoryDomain	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Laird.WIFIGlobalSettings.RoamPeriodMs	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Laird.WIFIGlobalSettings.RoamTrigger	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Laird.WIFIGlobalSettings.RTSThreshold	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Laird.WIFIGlobalSettings.ScanDFSTime	R	Hardcoded Wi-Fi settings in the gateway	N/A
InternetGatewayDevice.Laird.WIFIGlobalSettings.TTLSInnerMethod	R	Hardcoded Wi-Fi settings in the gateway	N/A

8.6.5.4 InternetGatewayDevice.Laird.LORASettings

Table 5: InternetGatewayDevice.Laird.LORASettings

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.Laird.LORASettings	O	The LoRa settings for the gateway.	N/A
InternetGatewayDevice.Laird.LORASettings.EUI	R	This is the unique identifier for your gateway.	N/A
InternetGatewayDevice.Laird.LORASettings.Mode	R/W	This is the chosen packet forwarder type.	semtech, sbs
InternetGatewayDevice.Laird.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.Laird.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.Laird.LORASettings.STPortUp	R/W	This is the port used by the Semtech packet forwarder	A 2-4 digit port number.
InternetGatewayDevice.Laird.LORASettings.STPortDown	R/W	This is the port used by the Semtech packet forwarder	A 2-4 digit port number.
InternetGatewayDevice.Laird.LORASettings.STKeepAlive	R/W	This is the keep alive timeout used by the Semtech packet forwarder.	A value in milliseconds
InternetGatewayDevice.Laird.LORASettings.STPushTimeout	R/W	This is the push timeout used by the Semtech packet forwarder.	A value in milliseconds
InternetGatewayDevice.Laird.LORASettings.STStatInterval	R/W	This is the stat interval used by the Semtech packet forwarder.	A value in milliseconds
InternetGatewayDevice.Laird.LORASettings.STForwardCRCValid	R/W	This determines if packets with CRC errors are forwarded.	true, false
InternetGatewayDevice.Laird.LORASettings.STForwardCRCError	R/W	This determines if packets with CRC errors are forwarded.	true, false
InternetGatewayDevice.Laird.LORASettings.STForwardCRCDisabled	R/W	This determines if packets with CRC errors are forwarded.	true, false
InternetGatewayDevice.Laird.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.Laird.LORASettings.SBSCUPSURL	R/W	This is the CUPS URL used by Basic Station.	A string representing the URL of the CUPS server.
InternetGatewayDevice.Laird.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.

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.Laird.LORASettings.SBSStatus	R	This is the status of the connection to the LNS server. 0 - Disconnected, 1 - Connected.	N/A
InternetGatewayDevice.Laird.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.

8.6.5.5 InternetGatewayDevice.Laird.LANSettings

Table 6: InternetGatewayDevice.Laird.LANSettings

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

8.6.5.6 InternetGatewayDevice.Laird.GatewayManagement

Table 7: InternetGatewayDevice.Laird.GatewayManagement

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.Laird.GatewayManagement	O	Version information and how to initiate a firmware update	N/A
InternetGatewayDevice.Laird.GatewayManagement.Versions	O	Contains version information	N/A
InternetGatewayDevice.Laird.GatewayManagement.Versions.SDK	R	SDK version	N/A
InternetGatewayDevice.Laird.GatewayManagement.Versions.Driver	R	Driver package version	N/A
InternetGatewayDevice.Laird.GatewayManagement.Versions.Supplicant	R	Wi-Fi supplicant version	N/A
InternetGatewayDevice.Laird.GatewayManagement.Versions.Build	R	Build version	N/A
InternetGatewayDevice.Laird.GatewayManagement.Versions.HardwareChipset	R	Hardware chipset	N/A
InternetGatewayDevice.Laird.GatewayManagement.Versions.Firmware	R	Wi-Fi firmware version	N/A
InternetGatewayDevice.Laird.GatewayManagement.Versions.CLI	R	SDC CLI version	N/A

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.Laird.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.Laird.GatewayManagement.Versions.FirmwareUpdateStatus	R	Status of the firmware update (1 = complete, 0 = not complete)	N/A

8.6.5.7 InternetGatewayDevice.Laird.SavedProfileSettings

Table 8: InternetGatewayDevice.Laird.SavedProfileSettings

Parameter Name	R/W	Description	Input Data
InternetGatewayDevice.Laird.SavedProfileSettings	O	Node to modify saved profile settings	N/A
InternetGatewayDevice.Laird.SavedProfileSettings.ListProfiles	R	List of all gateway Wi-Fi profiles	N/A
InternetGatewayDevice.Laird.SavedProfileSettings.ProfileName	R/W	Wi-Fi profile alias that the user wants to modify	String representing the profile name
InternetGatewayDevice.Laird.SavedProfileSettings.AddProfile	R/W	Adds a new profile	String representing the profile name
InternetGatewayDevice.Laird.SavedProfileSettings.DeleteProfile	R/W	Deletes a profile	String representing the profile name
InternetGatewayDevice.Laird.SavedProfileSettings.SSID	R/W	SSID for the selected Wi-Fi profile	String representing the SSID
InternetGatewayDevice.Laird.SavedProfileSettings.PSK	R/W	PSK for the selected Wi-Fi profile	String representing the PSK
InternetGatewayDevice.Laird.SavedProfileSettings.ClientName	R/W	Client name for the selected Wi-Fi profile	String representing name client name
InternetGatewayDevice.Laird.SavedProfileSettings.TxPower	R/W	TX power for the selected Wi-Fi profile	A numeric value representing TX power
InternetGatewayDevice.Laird.SavedProfileSettings.AuthType	R/W	Authentication type for the selected Wi-Fi profile	open, shared, or eap
InternetGatewayDevice.Laird.SavedProfileSettings.EAPType	R/W	EAP type for the selected Wi-Fi profile	leap, eap-fast, peap-mschapv2, eap-tls, peap-tls
InternetGatewayDevice.Laird.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.Laird.SavedProfileSettings.Mode	R/W	Selected Wi-Fi profile mode	BGN
InternetGatewayDevice.Laird.SavedProfileSettings.Powersave	R/W	Displays the enabled power save mode	off,max,fast
InternetGatewayDevice.Laird.SavedProfileSettings.PSPDelay	R/W	Selected Wi-Fi profile's power save delay	A value 10 - 500 in units of milliseconds.
InternetGatewayDevice.Laird.SavedProfileSettings.Username	R/W	Wi-Fi profile username used by some authentication methods	Username string
InternetGatewayDevice.Laird.SavedProfileSettings.Password	W	Wi-Fi profile password used by some authentication methods	Password (write only) string

8.6.5.8 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.)

Parameter Name	R/W	Description	Input Data
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
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

8.6.5.9 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	N/A

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

Parameter Name	R/W	Description	Input Data
		allowed on this gateway	
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

8.6.5.10 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

8.6.5.11 InternetGatewayDevice.LANDevice

Table 12: 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

https://www.lairdconnect.com/ 41
© Copyright 2020 Laird Connectivity.
All Rights Reserved

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

8.6.5.12 InternetGatewayDevice.WiFi

Table 13: 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
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 the passphrase or pre-shared key can be entered here.	A string representing the PSK.
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 InternetGatewa

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

Parameter Name	R/W	Description	Input Data
			yDevice.WiFi.EndPoint.{x}.Security.ModesSupported.
InternetGatewayDevice.WiFi.EndPoint.{x}.Profiles.{y}.Security.AuthType	R/W	Indicates which authentication mode is enabled	open, shared, or eap
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
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

8.6.5.13 InternetGatewayDevice.IP

Table 14: 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
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

8.7 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 46: Debug info

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

8.8 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 47).

1 – User Button

2 – Reset Button

Figure 47: 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.

8.9 Bluetooth

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

For the latest version of this manual, quick start guide, regulatory information and firmware updates, please see the Documentation tab the RG1xx page on Lairdconnect.com: https://www.lairdconnect.com/wireless-modules/lorawan-solutions/sentrius-rg1xx-lora-enabled-gateway-wi-fi-bluetooth-ethernet

9 IP67 RATED ENCLOSURE
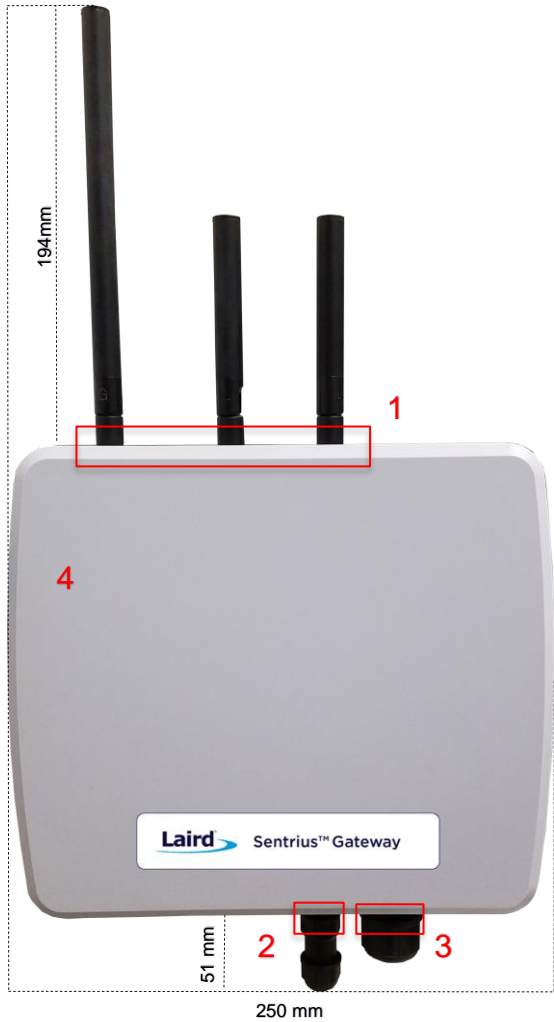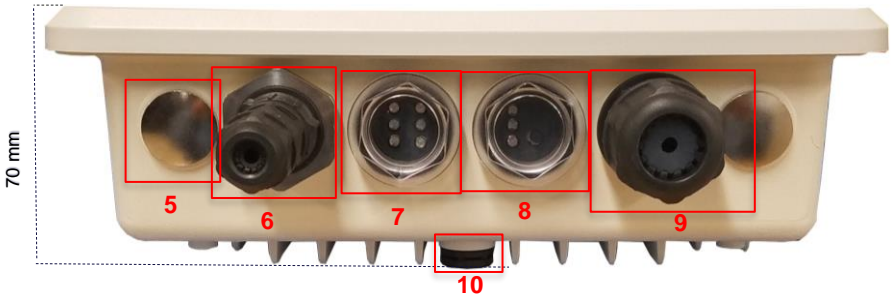

Reference	Description
1	LoRa and Wi-Fi antennas
2	Power supply module
3	CAT6 Ethernet module
4	Moulded plastic cover

Figure 48: Top of the IP67 Rated Sentrius™ RG1xx Gateway

Figure 49: Side panel of the IP67 Rated Sentrius™ RG1xx Gateway (Current Generation)

Ref.	Description
5	Metal cover plug (2) – 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

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

9.1 Specification

| Category	Feature	Specification
Interfaces	Wired	CAT6 Ethernet - RJ45 Connector
		LED Data Communication Ports (2)
		Optional Data Communication/Power Ports Available for Expansion (2)
	Wireless	Wireless
Power	Supply Voltage	12V/1A
	Power Adapter/Cable	External DC Power Supply (12V/2A rating) with regional plug adapter – Industrial Temperature Rated (supplied by end-user)
	Configuration	Web-based interface via Ethernet/Wi-Fi
Physical	Dimensions	220 x 250 x 70 mm (enclosure only)
Environmental	Operating Temp.	-40° to +85°C
Wi-Fi Antenna	Model	Laird 001-0012 IP67-rated
	Type	Dipole
	Connector	RP-SMA
	Antenna Gain	2.0 dBi (2.4–2.5 GHz), 2.0 dBi (4.9–5.875 GHz)
LoRa Antenna	Model	Laird 001-0029 IP67-rated (863–870 MHz) used with RG186
		Laird 001-0011 IP67-rated (902–928 MHz) used with RG191
	Type	Dipole
	Connector	RP-SMA
	Antenna Gain	2.0 dBi (863–870 MHz) used with RG186
		2.0 dBi (902–928 MHz) used with RG191
Accessories	Included	▪ 1 x 863-870 MHz antenna (with RG186) or 1 x 902-928 MHz antenna (with RG191) ▪ Two 2.4/5 GHz Wi-Fi antennas *Note: Mounting hardware (wall mount or pole mount available) – sold separately*
Enclosure	IP67 Rated	▪ External enclosure housing for Main Gateway PCB ▪ Molded plastic cover ▪ Anti-corrosive ▪ Die Cast Alloy Frame (Al-Si-Mg)
Warranty		One-year warranty

9.2   LED Display Reference

9.2.1 Three LED Display with User Button
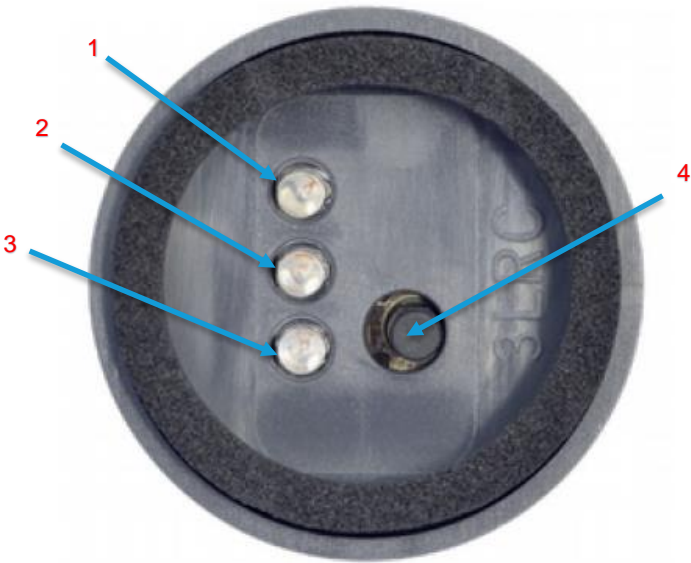
Reference	Description
1	Power (green)
2	LoRa (green)
3	BLE (green)
4	User Button

Figure 50: LED displays with User button (#6 from Figure 49)

9.2.2 Six LED Display
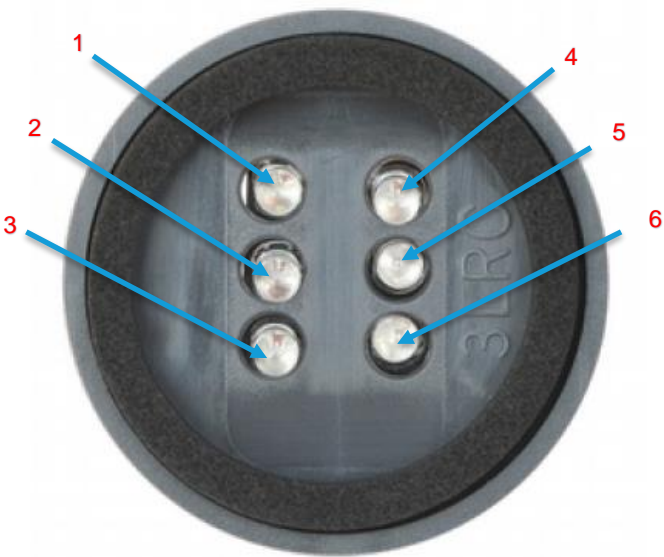
Reference	Description
1	Power
2	Ethernet
3	Wi-Fi
4	N/A
5	User
6	N/A (Future Use)

Note: *All LEDs are green.*

Figure 51: Six LED display (#7 from Figure 49)

48
Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

9.3 Previous Generation Connector Adapter Layout
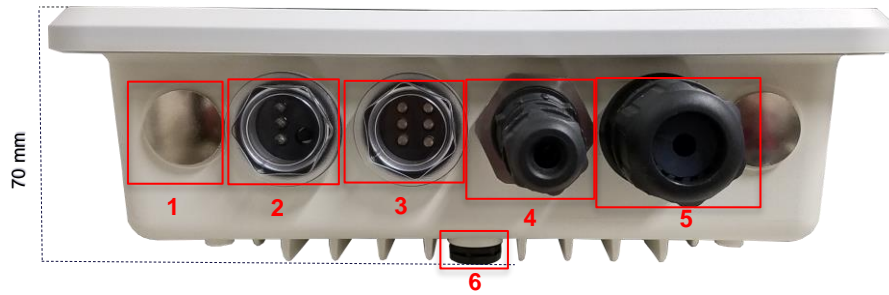
Figure 52: Side panel of the IP67 Rated *Sentrius™ RG1xx* Gateway (Revision 1 & 2)

Ref.	Description
1	Metal cover plug (2) – Available data/power ports for expansion
2	Three LED display and User button with transparent dust cover
3	Six LED displays with transparent dust cover
4	Power supply module
5	CAT6 Ethernet module
6	Plastic gore ventilation plug

9.4 Cable Assemblies

9.4.1 Power Supply and Ethernet Module
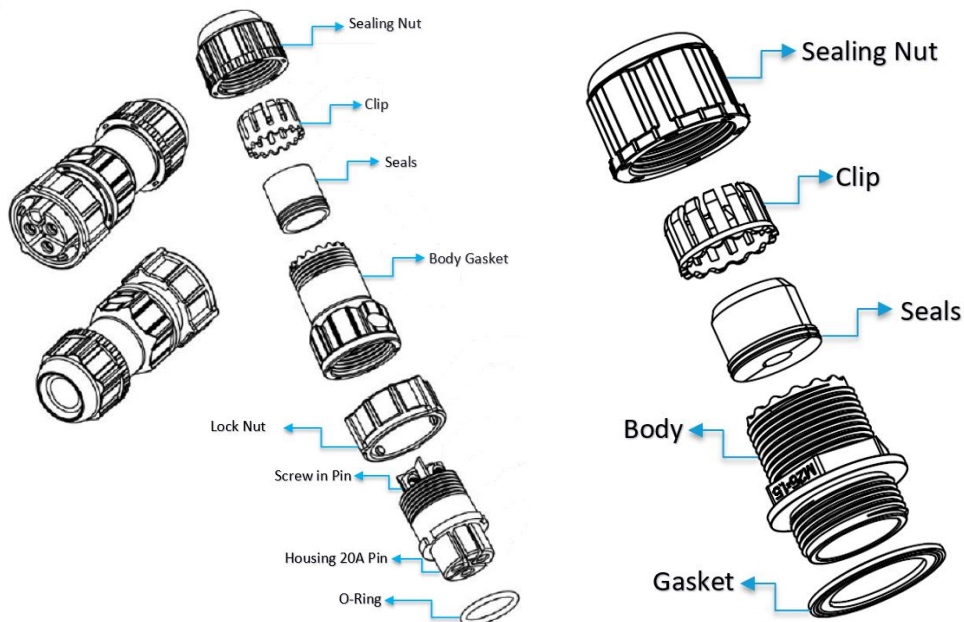
Figure 53: Power cable (left) and Ethernet (right) assembly components

9.4.2 Assembly Steps

The steps explained below cover the power cable assembly process in detail. The ethernet cable assembly is very similar, however less complex, to work with. In general, place the Ethernet cord through each component and mount to the enclosure. Tighten the Sealing Nut with a **Torque Force of 8 ~ 10 kgf.cm**. The rest of the guide covers the power cord assembly.

Note: To ensure the IP67 rating, the Ethernet cable diameter must be in the range of 4.5 mm – 6.5 mm. If the cable is too small, there is a potential risk of environment factors potentially damaging the internal hardware.

To assemble the power cable, follow these steps:

1. Insert the Ethernet cord through each component – sealing nut (i), clip (ii), sealing (iii), sealing body (iv), gasket (v), and lock nut (vi) (Figure 54).
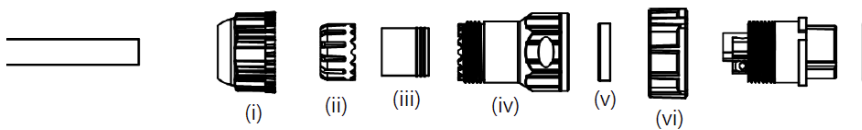

Figure 54: Insert Ethernet cord

Note: To ensure the IP67 rating, the **cable diameter must be in the range of 5.5 mm – 8.0 mm**. If the cable is too small, there is a potential risk of environment factors potentially damaging the internal hardware.

---

2. Use a 1.5 mm screwdriver, preferably an allen wrench, to fix the core wire(s) into the screw fixing point (Figure 55).
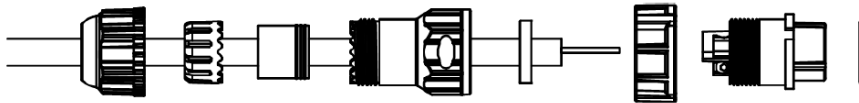

Figure 55: Core wire fixed into the screw fixing point

Note: The cable core wires for the power cable assembly need to be in the range of 14 AWG to 18 AWG to fit properly in the screw points. We recommend that you strip and tin the ends of the core cable wires to make the install easier when inserting the wire into the screw points. Range of length tinning wire: 5 mm– 6 mm.

Pin 2 should be negative (black wire) and Pin 1 should be positive (red wire). It is recommended to install an Earth Ground Wire. There are positions available on the enclosure for this (*Figure 61*).

---
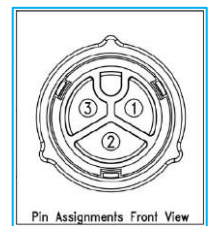
3. Fit the gasket (v), sealing (iii), and clip (ii) onto the sealing body (iv) (Figure 56).
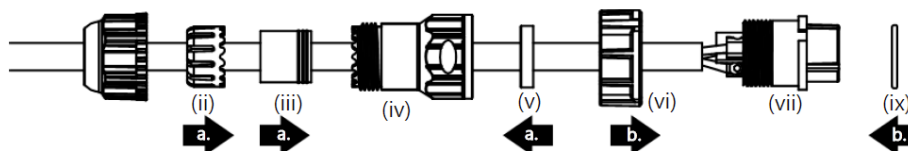4. Fit the lock (vi) and o-ring (ix) onto the housing (vii) (Figure 56).

Figure 56: Steps 3 and 4

5. Screw the sealing nut (i) and the assembled housing (x) onto the assembled sealing body (xi) with a torque force of 8–10 kgf-cm (Figure 57).

(i)   (xi)   (x)

Figure 57: Step 5

The assembly is now complete (*Figure 58*).

Figure 58: Completed assembly

3. Mount the completed cables into the keyed power module slot and the Ethernet module slot #8 and #9 from Figure 49.

9.5 Mounting Hardware

9.5.1 Wall Mount

Figure 59: Wall Mount
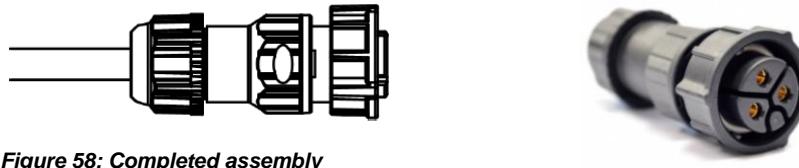
Included Mounting Hardware
M6x0.8x10.0 mm, stainless steel screws with washers – 4
5/16 x 11 self-tapping screws, L=25.00 mm – 4
3/4" wall anchors – 4
4" hose clamps – 2
M5x1.0x10.0 mm, stainless steel screws with washers (optional) – 4

Figure 60: Wall mount dimensions
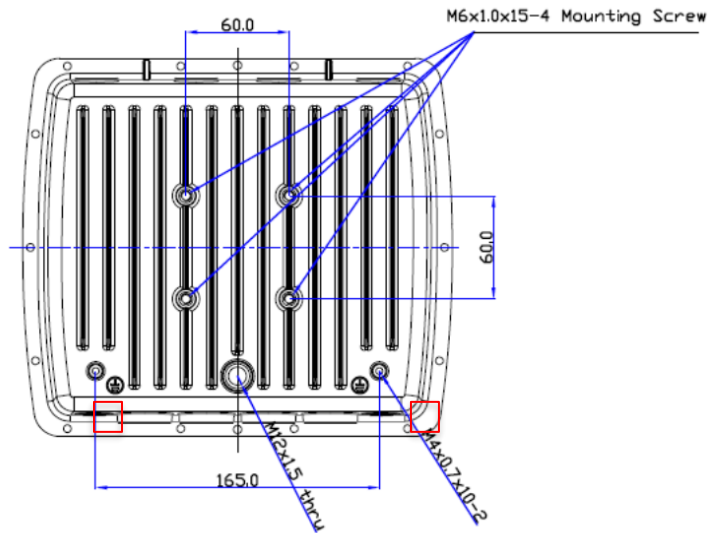
Figure 61: Enclosure placement dimensions (mm)

9.5.2 Pole Mount

Included Mounting Hardware
M6x0.8x10.0 mm, stainless steel screws with washers – 4
5/16 x 11 Self-tapping screws, L=25.00 mm – 4
3/4" wall anchors – 4
M8x1.25x80.0 mm stainless steel screws with washers – 2
M8x1.25x90.0 mm Stainless Steel Screws with washers and nut – 1
M5x1.0mm Stainless Steel Screws, L = 10.0 mm with washers (optional) – 4

Figure 62: Pole mount (pole diameter range ~34 mm – 90 mm)
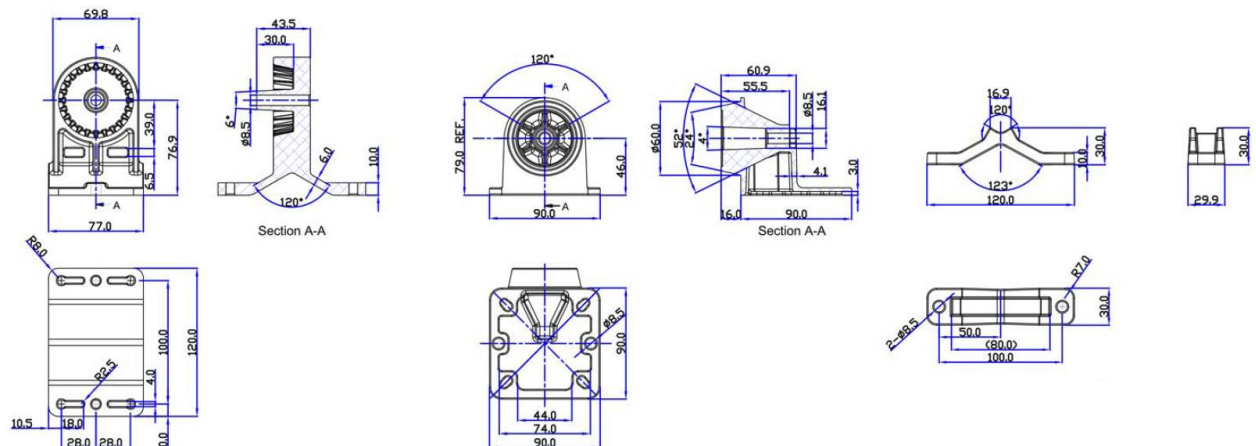
9.5.2.1 Dimensions

Figure 63: Pole mount dimensions

10   FCC AND ISED CANADA REGULATORY STATEMENTS

This product contains the RG191-M2 and the WB50NBT from Laird.

Model	US/FCC	CANADA/IC
RG191-M2	SQG-1001	3147A-1001
WB50NBT	SQG-WB50NBT	3147A-WB50NBT

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.

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 Laird could void the user's authority to operate the equipment.**

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.

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.

Industry Canada (IC) 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.

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 CE REGULATORY

The RG186 has been tested for compliance with relevant standards for the EU market.

Reference the Declaration of Conformities listed below for a full list of the standards that the modules were tested to. Test reports are available upon request.

11.1 EU Declarations of Conformity

Manufacturer	Laird
Products	RG186
Product Description	LoRa/Wi-Fi/BT and BLE RF module
EU Directives	2014/53/EU – Radio Equipment Directive (RED)
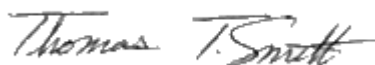
Reference standards used for presumption of conformity:

Article Number	Requirement	Reference standard(s)
3.1a	Health and Safety	EN60950-1:2006+A2:2013
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, Laird, 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.

Place of Issue:	Laird W66N220 Commerce Court, Cedarburg, WI 53012 USA tel: +1-262-375-4400 fax: +1-262-364-2649
Date of Issue:	20 Dec 2017
Name of Authorized Person:	Thomas T Smith, Director of EMC Compliance
Signature of Authorized Person:	

12 TAIWAN NCC REGULATORY

NCC Warning

802.11b/802.11g/BT 警語：

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。

13 TELECOMMUNICATIONS REGULATORY AUTHORITY (TRA) COMPLIANCE

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

13.1 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.
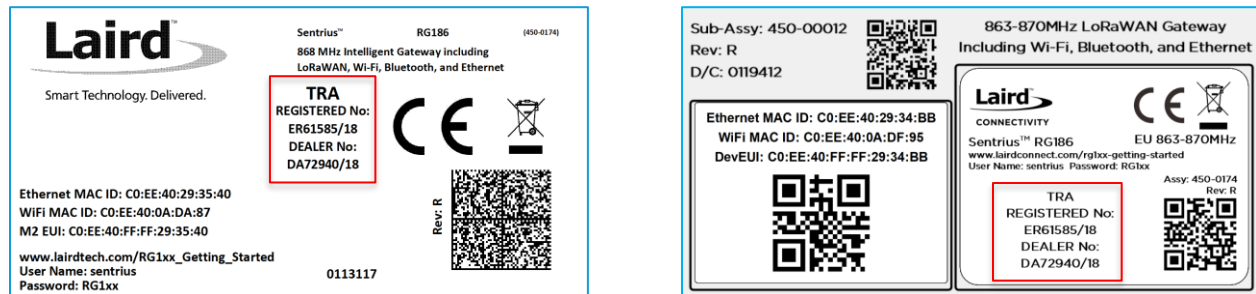   – RG186 Dealer Registration Number: DA72940/18

Figure 64: TRA Label Information (Standard GW – Left, AS923 & AU915 Region Supported/Latest Revision – Right)

14 REGION SUPPORTED LABELS

14.1 RG191 Version

The RG191 is the base for all current country variants:

Figure 65: RG191 Region Supported Label

14.2 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 65. All labels are printed in black and white color.

14.2.1 Taiwan (TW)

Figure 66: Taiwan 923MHz Region Supported Label
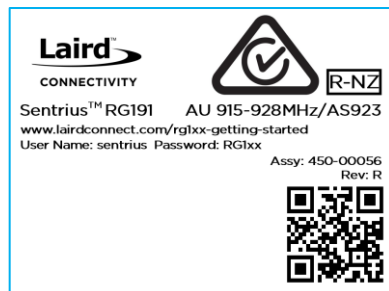
14.2.2 New Zealand (NZ)

Figure 67: New Zealand 923MHz Region Supported Label

14.2.3 Hong Kong (HK)
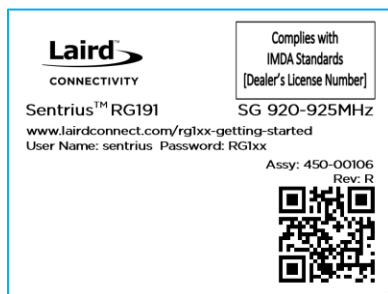

Figure 68: Hong Kong 923MHz Region Supported Label

14.2.4 Australia (AU)

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

14.2.5 Singapore (SG)

Figure 70: Singapore 923MHz Region Supported Label (Pending Certification)

14.2.6 Malaysia (MY)

Figure 71: Malaysia 923MHz Region Supported Label (Pending Certification)

Mouser Electronics

Authorized Distributor

Click to View Pricing, Inventory, Delivery & Lifecycle Information:

[Ezurio](#):

[455-00102](#) [455-00097](#)