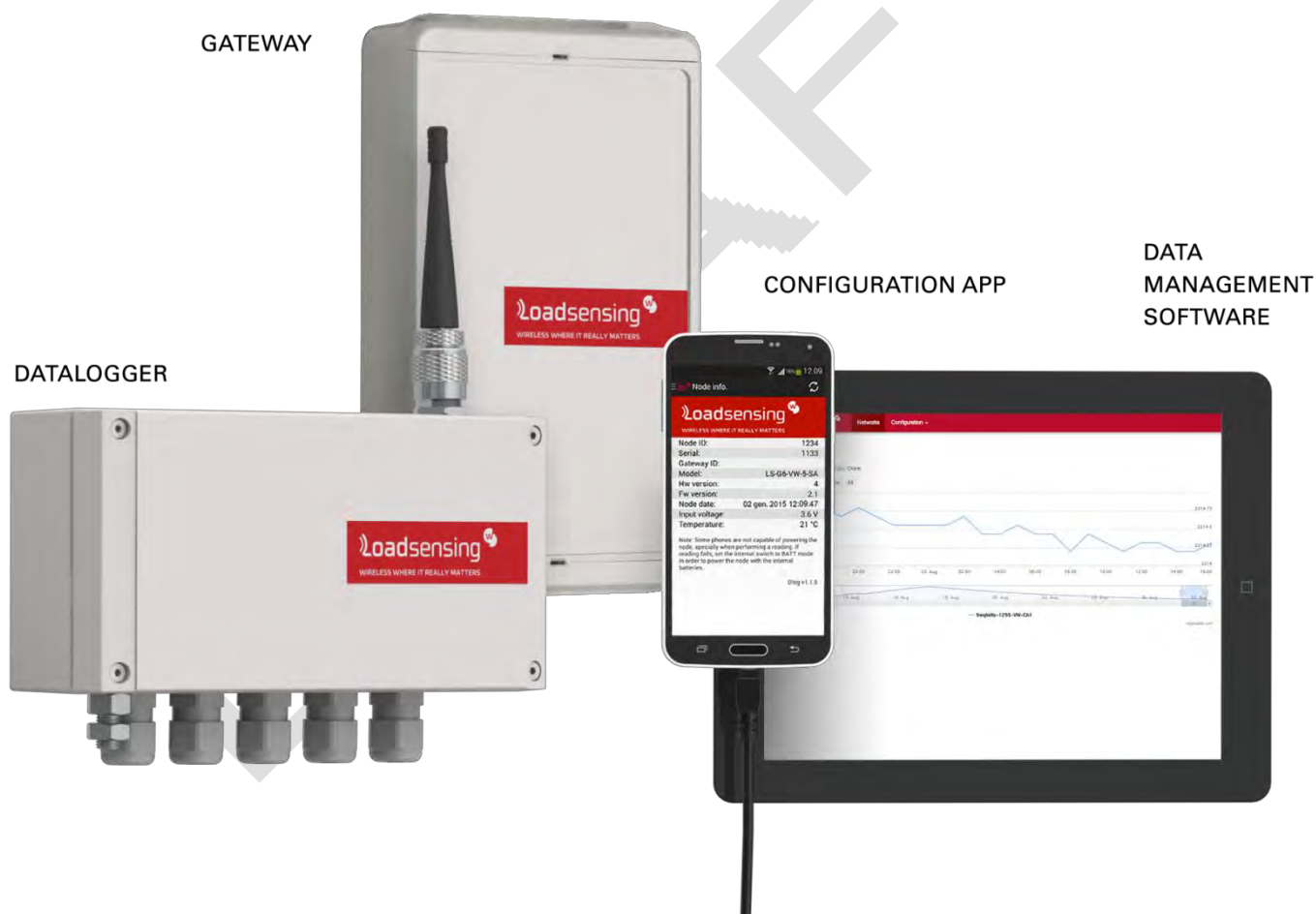


LS-G6

USER GUIDE V1.6

February 2016



INDEX

1. INTRODUCTION.....	6
1.1. About this document.....	6
1.2. Product overview.....	6
2. QUICK START	6
2.1. Equipment.....	6
2.2. Datalogger installation.....	7
2.2.1. Initialize datalogger	7
2.2.2. Sensor connection.....	9
2.2.3. Datalogger mounting	9
2.3. Datalogger configuration.....	10
2.4. Gateway installation.....	17
2.4.1. Gateway overview	17
2.4.2. Powering the Gateway	19
2.4.3. Mounting of the enclosure.....	21
2.4.4. SIM Card	24
2.4.5. Ethernet connection	25
2.5. Gateway configuration.....	25
2.5.1. Connecting to the Gateway	25
2.5.2. The Gateway's configuration and data access interface	26
2.6. Data visualization and retrieval	37
2.7. Maintenance.....	42
2.7.1. General Maintenance	42
2.7.2. Periodical maintenance.....	42
2.7.3. Return material authorization.....	43
3. LS-G6 DATALOGGERS	44
3.1. LS-G6-VW	44
3.1.1. Sensor connection.....	44
3.1.2. Barometric measurements	45
3.1.3. Battery lifespan	45
3.1.4. Configuration	46
3.1.5. Data storage	46
3.2. LS-G6-DIG.....	46
3.2.1. Sensor Connection	46
3.2.2. Battery lifespan	47
3.2.3. Configuration	48
3.2.4. Data storage.....	48
3.3. LS-G6-ANALOG	48
3.3.1. Sensor Connection	48
3.3.2. Battery lifespan	50
3.3.3. Configuration	50

3.3.4. Data storage	50
4. WIRELESS RADIO	51
4.1. Maximum number of dataloggers connected in a network	51
4.2. Radio configuration	52
4.3. Results of signal coverage test.....	53
5. CONTACT WORLDSENSING.....	55
Annex 1: Details of mounting systems	56
Mounting brackets.....	56
Strong magnets	56
Pole mounting.....	57
Annex 2: Android compatibility	59
Annex 3: LS-G6 water tightness	60
Annex 4: Recommended batteries.....	61
Annex 5: Communications security.....	62
Long range radio communication from dataloggers to gateway	62
Security.....	62
Encryption	62
Gateway user access.....	62
Remote access	62
Local administration.....	63
Annex 6: Troubleshooting reference table	64
Gateway.....	64
Dataloggers.....	65



FIGURES

Figure 1: View of the recommended positions to open the datalogger.....	7
Figure 2: Removal of the upper enclosure of the battery holder.....	8
Figure 3: Detail of power switch (SW A).	9
Figure 4: Detail of the grounding screw.	10
Figure 5: a) Main screen of Android Configuration App and b) Node configuration screen, which has to be accessed for the configuration of the datalogger.....	10
Figure 6: Network size configuration.....	11
Figure 7: Sensor configuration options of LS-G6-VW-5ch.	12
Figure 8: Sensor configuration options of LS-G6-DIG-2ch.....	12
Figure 9: Sensor configuration options of LS-G6-ANALOG-4ch.....	13
Figure 10: Data readings of active sensors.	14
Figure 11: Radio configuration screen.....	14
Figure 12: Radio signal coverage performed at the end of the datalogger setup (using the Setup wizard).	17
Figure 13: LS-G6 Gateway, with all the parts indicated.....	18
Figure 14: LS-G6 Gateway opened.	19
Figure 15: Detail of the connections for the Power through PoE.....	20
Figure 16: Wiring of the cable at the RJ45 connector (following T-568A/B specification) to be inserted in the PoE Injector.	20
Figure 17: DC terminal block.	21
Figure 18: Gateway mounted in a pole.	21
Figure 19: Gateway mounted on the Wall.....	22
Figure 20: Gateway's antenna mounting.	23
Figure 21: Connection of the antenna cable to the connector.	23
Figure 22: Fixing of the antenna cable.	24
Figure 23: SIM card slot. Indicated the Extraction button.	24
Figure 24: PoE. Left port (Data & Power Out) is for the Power Cable and right port (Data in) is for the Data transmission.....	25
Figure 25: Initial page of the gateway. This is the first page when entering the Web's Configuration Interface.	27
Figure 26: Summary of the datalogger status and the historical received/lost messages.	28
Figure 27: Gateway status page.....	30
Figure 28: View of the Internet configuration tab of the Gateway. The present configuration is the one by default.....	31
Figure 29: Options for manual configuration.....	32
Figure 30: Settings for the configuration of the GPRS/3G connection.....	33
Figure 31: Remote Access tab, inside the gateway interface.	34
Figure 32: Radio config tab, inside the gateway interface.....	36
Figure 33: Delete all tab, inside the gateway interface.	36
Figure 34: Reboot tab, inside the gateway interface.	37

Figure 35: In the “Last readings” tab, it appears a gear icon in the right, to edit the formula of the sensor.....	37
Figure 36: Menu to edit the formulae to transform the raw data of the sensors into engineering units.....	38
Figure 37: Circled in red, the icon to display the charts of each of the sensors.	39
Figure 38: Example of a chart of one datalogger.	39
Figure 39: View of the screen where the .csv files of the raw data and the data transformed into engineering units (of the complete network) can be downloaded.	39
Figure 40: View of the screen where the data of a specific datalogger can be downloaded.	40
Figure 41: View of the screen where the FTP can be configured.....	41
Figure 42: View of last messages recieved by the gateway, displayed in API format.....	41
Figure 43: Detail of a terminal block.....	44
Figure 44: View of the inside of the digital datalogger.	47
Figure 45: View of the LS-G6-ANALOG datalogger internally where the four channels can be identified.	49
Figure 46: View of the wiring of the different types of analogue sensors, indicated in the Android Configuration App.....	49
Figure 47: Summarized scheme of the data transmission over time in a LS-G6 network.	51
Figure 48: View of the geographical display (in the software of the gateway) indicating the results of the signal coverage tests.	54

TABLES

Table 1: Connections of the terminal block.....	44
Table 2: Indicative lifespan for LS VW-datalogger 1 ch and LSVW- datalogger 5 ch. Estimations using 4 c-size cells.....	45
Table 3: Times of data storage (without overwriting) for LS VW-datalogger 1 ch and LS VW- datalogger 5 ch.....	46
Table 4: Indicative lifespan for LS-DIG datalogger. Estimations using 4 c-size cells.....	47
Table 5: Idicative storage capacity of the LS-DIG datalogger. Estimations using 5 sensors.	48
Table 6: Indicative lifespan for LS-ANALOG datalogger. Estimations using 4 c-size cells.	50
Table 7: Indicative storage capacity of the LS-ANALOG datalogger. Estimations using 4 sensors.	50
Table 8: Slot times table. Columns are the number of nodes, rows are sampling rate. Slot times are in seconds.	51

1. INTRODUCTION

1.1. About this document

This user guide explains the basic procedure for data acquisition with the Loadsensing LS-G6 family of dataloggers from Worldsensing Industrial (WSI). Further technical description is available in the datasheets.

The family of dataloggers LS-G6 from Worldsensing Industrial comprises 5 different dataloggers which may be used as standalone dataloggers (without remote communications) and radio dataloggers (with remote communications through a gateway). The models are listed in the following:

Radio dataloggers

- LS-G6-VW-1
- LS-G6-VW-1P
- LS-G6-VW-5
- LS-G6-DIG-2
- LS-G6-ANALOG-4

Gateway

- LS-G6-GW¹

1.2. Product overview

Worldsensing's LS-G6 dataloggers are low power, easy to use and field-friendly dataloggers used for data acquisition from a great range of sensors in the market. Moreover, radio models are characterized by long range communications, up to 15 km in open-field scenarios, and 4 km in urban scenarios.

LS-G6 dataloggers are battery powered, and easy configured through the Android Configuration App. The dataloggers and the gateway are robust (IP68 dataloggers, IP67 gateway) and they don't need recasing.

LS-G6 dataloggers are used in many sectors, such as civil engineering, mining, environmental or industrial monitoring among others.

2. QUICK START

2.1. Equipment

Worldsensing's LS-G6 system ship with the following accessories:

- LS datalogger accessories:

Included:

¹ Gateways adjust to different geographic areas

- **RTC battery ½ AA-size bobbin cell:** Required to keep the time. If no RTC battery installed, the datalogger loses the time.
- **Antenna** (only for radio models)

Not included:

- **Micro USB OTG to USB 2.0**
 - **External mounting brackets** (set of 2) for wall mounting (see Annex 1 for details)
 - **Plate** for pole mounting (see Annex 1 for details)
 - **Strong magnets** for mounting in metallic structures (see Annex 1 for details)
 - **Batteries C-size spiral cell** (see Annex 4 for details): 1 to 4 batteries can be connected.
- Gateway accessories (included):
 - **Antenna**
 - **Cable antenna**
 - **PoE**
 - **USB Local Administration Interface**

2.2. Datalogger installation

2.2.1. Initialize datalogger

The datalogger is shipped closed and without batteries installed. In order to initialize it, the user may follow these steps:

- Open the datalogger (using allen wrench -2.5 mm-) following the recommended positions (Figure 1) in order to avoid damaging the lateral gore valve. The batteries are held on the cover, so be careful not to snap the cable between the cover and the main board.

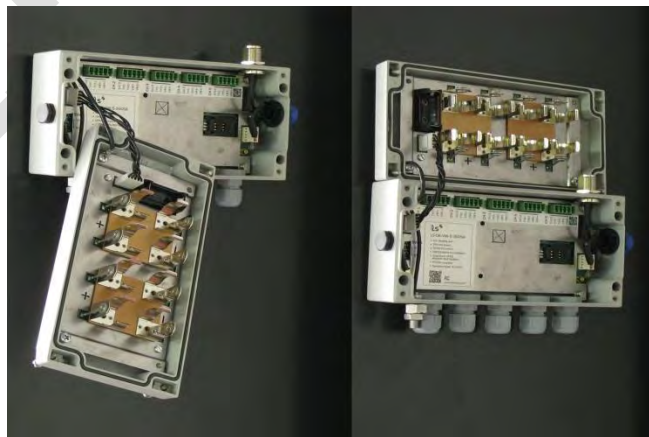


Figure 1: View of the recommended positions to open the datalogger.

- Insert RTC battery (small battery included). First remove the upper enclosure of the battery holder (Figure 2). Polarity is indicated inside the holder.

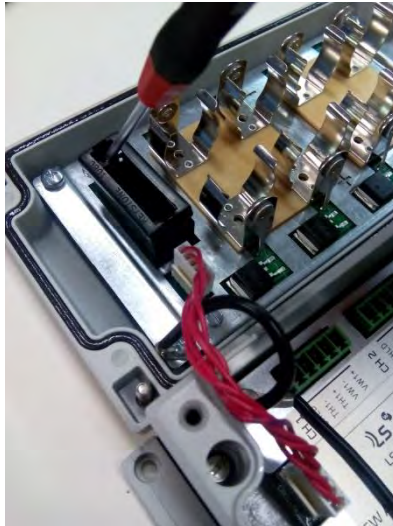


Figure 2: Removal of the upper enclosure of the battery holder.

- c. Insert C-type batteries in the battery holders. 1 to 4 batteries can be connected. Polarity is indicated (see Annex 4 for further information on the batteries).

Note that battery reverse protections exist but it is not safe to keep batteries reversed in the datalogger for a long time.

WARNING: RISK OF EXPLOSION IF THE BATTERIES ARE SUBSTITUTED FOR AN INCORRECT MODEL. DISPOSE OF THE BATTERIES ACCORDING TO THE INSTRUCTIONS. THIS EQUIPMENT IS MEANT TO BE INSTALLED IN RESTRICTED ACCESS AREAS.

- d. Check that power switch (SW A, Figure 3) is in the correct position. USB: the datalogger is powered by the USB cable connected to any other Android device/ BATT (default): the datalogger is powered by the batteries.

Note that some Android devices are not capable of powering the datalogger, specially when performing a reading. If reading fails, set the switch to BATT mode in order to power the datalogger with batteries.



Figure 3: Detail of power switch (SW A).

2.2.2. Sensor connection

Sensors are connected to the datalogger at the datalogger terminal blocks. Each terminal block corresponds to one channel of the data logger. The terminal blocks accept wires that are prepared by stripping a short length of insulation from the end.

Each datalogger type has specific instructions for sensor wiring. The specifications for each model can be found at sections: 3.1. (vibrating wire dataloggers), 3.2. (digital dataloggers) and 3.3. (analogue dataloggers).

2.2.3. Datalogger mounting

Dataloggers can be mounted (see Annex 1 for specific details):

- On the wall: mounting brackets can be supplied as additional accessories,
- On a metallic structure: strong magnets can be supplied as additional accessories,
- On a pole: a plate for 35 and 50 mm pole diameter can be supplied as additional accessory for this mounting type,
- Inside a manhole (with plastic or metallic cover): no special accessories are available for this mounting type. Even though the dataloggers are IP68 certified, we recommend to install them in holes with proper drainage, so they won't be permanently covered in water.

All LS-G6 dataloggers are protected against lightning, and there is an easy to use grounding screw (Figure 4), next to the cable glands, which may be connected to guarantee the protection.



Figure 4: Detail of the grounding screw.

Note that in order to protect the datalogger from surges (especially on installations with long cable runs) the datalogger must be installed with proper grounding connected to the grounding screw.

2.3. Datalogger configuration

Different configuration parameters are required for each type of datalogger (Vibrating Wire, Digital, Analogue). The complete configuration of the datalogger is done through the Android Configuration App (see Annex 2 for Android compatibility). When a new version of the app is available, a message appears automatically when connecting the datalogger by USB.

The configuration of the sensors and the radio is accessed by clicking the Setup wizard (in the tab menu “Node configuration”, Figure 5). Inside the Node configuration menu, there are also other parameters of the configuration of the node that can be changed by the user, such as the node id or the date and time (especially important when accessed for the first time in the node, or after installing the RTC battery).

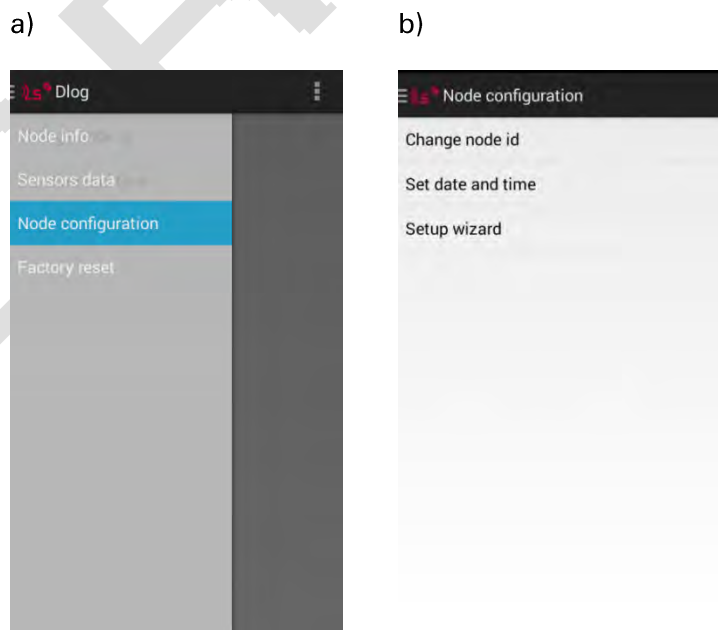


Figure 5: a) Main screen of Android Configuration App and b) Node configuration screen, which has to be accessed for the configuration of the datalogger.

By selecting the Setup wizard, a step-by-step configuration of the sensors and the radio is started:

- 1) **Network size.** The size of the network (Figure 6) defines the slot time for each of the dataloggers to send the data to the gateway in order to avoid data collision (see section 4.1. of this user guide).

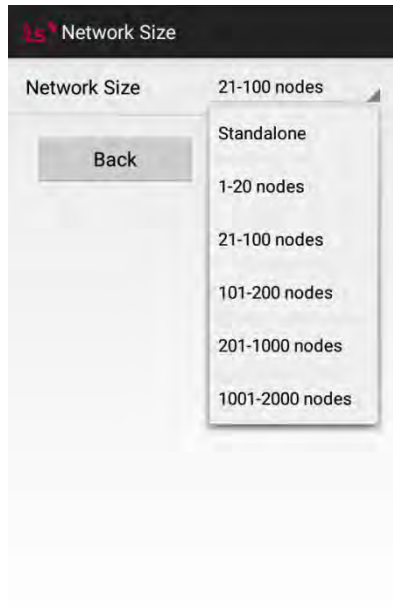


Figure 6: Network size configuration.

- 2) **Sensor configuration.** Each type of datalogger has its own parameters for configuration:
- VW datalogger (Figure 7): activation of channels, sampling rate interval and VW sweep frequency for each sensor. For more information on the configuration, see Section 3.1.

Sensor Configuration

Sampling rate: 30 min

Channel 1: ☒ On Sweep C 1400-3500

Channel 2: ☐ Off Sweep C 1400-3500

Channel 3: ☐ Off Sweep C 1400-3500

Channel 4: ☐ Off Sweep C 1400-3500

Channel 5: ☐ Off Sweep C 1400-3500

Custom start (Hz): 1400

Custom end (Hz): 3500

Figure 7: Sensor configuration options of LS-G6-VW-5ch.

- DIG datalogger (Figure 8): sampling rate, communication protocol with sensors (from given options), bus addresses of the sensors (if connected through RS485 by digital bus). Be aware that all the readings are kept according the bus addresses introduced. Therefore, the number of columns of data will fit with the records indicated by the inserted addresses, and not with the real number of sensors connected. If you don't keep track of the different addresses over time, we strongly recommend a factory reset. The last configuration is saved in the datalogger.

Sensor Configuration

Sampling rate: 5 min

Protocol: RST

Addresses
(separated by comma)
26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45

Be aware that all the recorded readings are kept even if you change the configuration. The readings are stored in the same order than the inserted addresses. If you don't keep track of the different addresses over time, we strongly recommend a factory reset. The last configuration is saved in the datalogger.

Set configuration

Figure 8: Sensor configuration options of LS-G6-DIG-2ch.

- ANALOGUE datalogger (Figure 9): this datalogger supports six different analogic sensor types: voltage, full Wheatstone bridge, thermistor, current loop, PT100,

potentiometer. The interface for the sensor configuration in the Setup wizard requires the user to choose between the different sensor types in each channel (Figure 9a). For each specific sensor type, the details of the sensor wiring appear in the screen, and the configuration parameters (specific for each sensor type) have to be selected by the user (Figure 9b). Each channel can be configured independently, with specific requirements for each sensor (sensor power, warm up times, etc).

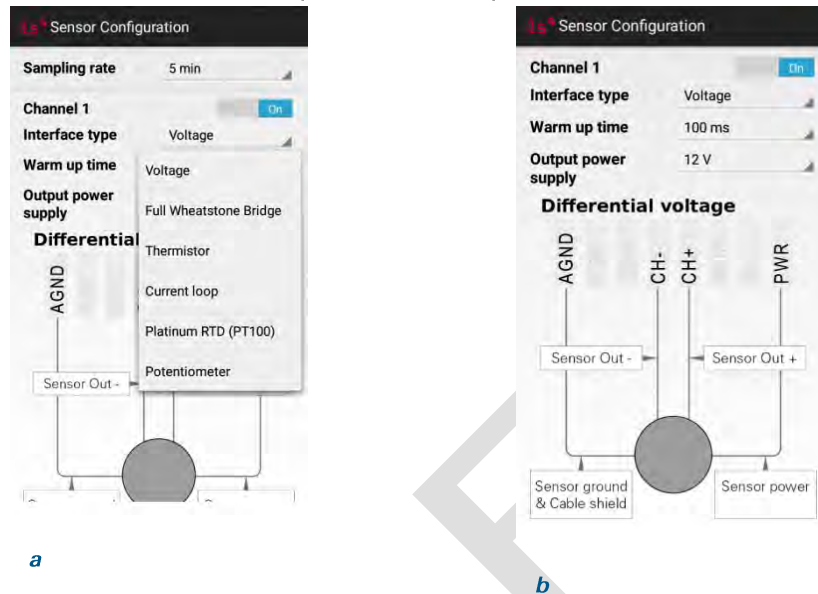


Figure 9: Sensor configuration options of LS-G6-ANALOG-4ch

- 3) **Sensors data.** A reading of the active channels is displayed (Figure 10). In this stage, the user can see the readings of the sensors in this specific moment, to check if the sensors have been properly configured.

Note that this action may take some time, depending on the sensor, and specially for the sensor strings of digital sensors connected to RS485 port of LS-G6-DIG.

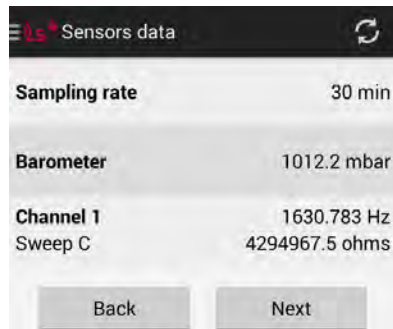


Figure 10: Data readings of active sensors.

- 4) **Radio configuration.** This is the panel where radio configurations are set. You are required to set the correct region and country to comply with local regulations. The network is identified by a Network ID, and protected with a password. All dataloggers and the gateway of an installation need to have identical settings (country and password). The default credentials of the radio network are specified in the Gateway Information Sheet (Figure 11). The advanced options should not be changed in the majority of installations. For more details on the advanced options, check Section 4 of this manual.

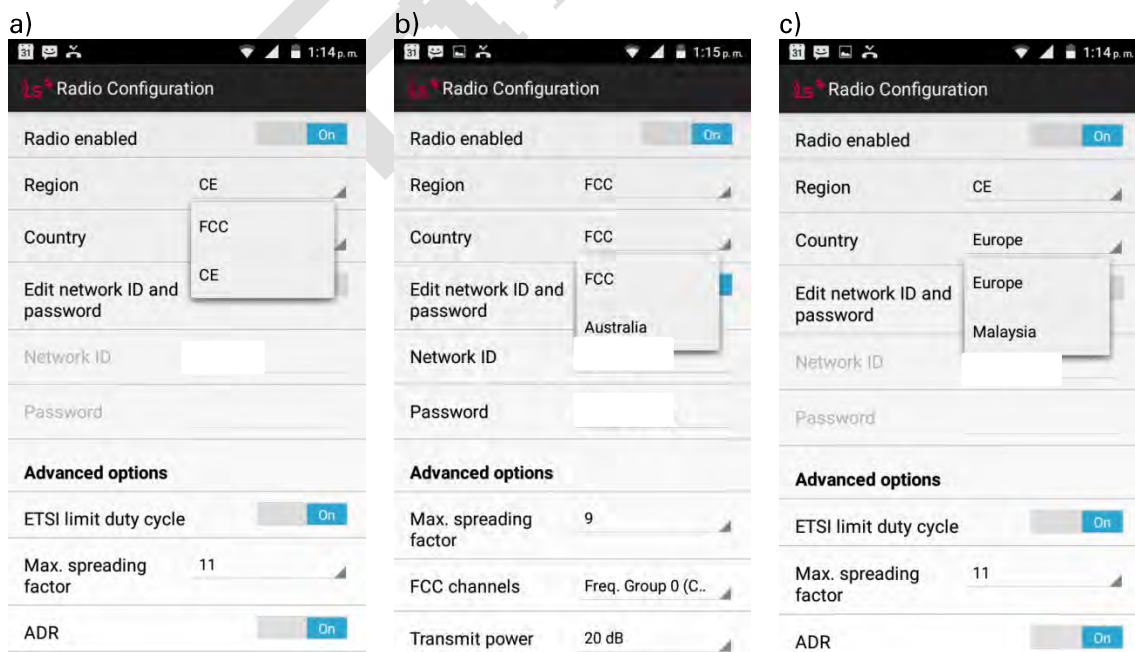


Figure 11: Radio configuration screen.

Note that in order to simplify the datalogger configuration tasks, especially in large installations, the network ID and password of the last datalogger configured are saved into the Android app. The option of editing them has to be activated by the user, otherwise the credentials that will be introduced in the configuration of the datalogger will be the ones that were introduced the last time the Android app was used.

5) Radio signal coverage test (only for radio models). Once the gateway is configured, a signal coverage test can be performed (Figure 12). This test will check for correct connectivity between the datalogger and the gateway. Some test packets will be sent by the datalogger, and then the Android app will check on the gateway (using the Internet connection) for the reception of these packets. Hence, the test will check for:

- Correct gateway operation and communication
- Correct radio configuration on both gateway and datalogger (including matching country and id/password configurations)
- Quality of the signal received by the gateway from the datalogger

For the results of this test to be immediately displayed in the Android device, the gateway needs to be installed with a working Internet connection, and the Android device also needs to be connected to the Internet. This is what we call an “online test”.

In order to perform an Online test, the Dlog app needs to be supplied with the gateway’s serial number and remote access password.

The remote access password is used to protect access to the gateway from the local network or the Internet. It is separate from the radio network password, even though it’s set to the same value by default.

The gateway ID and default password are specified in the Gateway Information Sheet. Before starting the test itself, the gateway connectivity is checked, and in case of any problem with the credentials an error message will appear.

The displayed results are listed for each Spreading Factor (SF). The SF represents a way of data modulation. The gateway is capable of receiving at the same time all the frequencies with several SF. The lower the SF number is, the shorter is the message, thus more messages can be sent on the network. The SF is proportional to the distance between datalogger and gateway: higher spreading factors are capable of transmitting data at higher distances, while lower spreading factors are reaching lower distances.

During the radio signal coverage test, the datalogger sends 10 or 5 packages of data at SF7 to SF12. In the results, it can be viewed how many reached the gateway, to ensure that the communications are working fine. The Australian version of the radio works differently, see section 4 of this manual.

When doing the Radio signal coverage test, the position of the Android device is kept (if the user allowed the permission of the app to access to the GPS data), and a “token” number identifies each test.

If the Gateway and/or the Android device don’t have Internet connectivity during the test, the online test will fail (since the gateway cannot be contacted over the Internet), and you will need to perform an “Offline test”. In this mode however, the results of the test can not be displayed in the Android device. The “token number” identifies each test. You need to write down the token number along

with a description of where and in what conditions the test was taken. You will have to check the results of the coverage test on the gateway's web interface (under network->Signal coverage test map->Download all tests of this network). A coverage test is considered correct if any of the Spreading Factors is able to deliver at least half the packets sent.

Note that performing the Radio signal coverage test takes approximately 2 minutes.

DRAFT

a)

b)

Field	Value
Date	
Token	
Node ID	
Network ID	
Latitude	
Longitude	
SF7	1 / 10
SF8	3 / 10
SF9	2 / 10
SF10	1 / 5
SF11	1 / 5

Figure 12: Radio signal coverage performed at the end of the datalogger setup (using the Setup wizard).

2.4. Gateway installation

2.4.1. Gateway overview

Dataloggers equipped with a radio communication system can transmit their readings to the Gateway, and make them available for real-time access. Readings can be accessed over the Internet, via a private network, or stored on the gateway for local retrieval.

The LS-G6 Gateway (Figure 13) is made of a high impact resistant polycarbonate, engineered to withstand harsh industrial and outdoor environments. It offers excellent flammability rating, good UV resistance and also good chemical resistance, and is rated IP67.

We advise that the gateway should be setup and configured in an office environment, rather than doing the startup procedure in an outdoor or industrial environment.



Figure 13: LS-G6 Gateway, with all the parts indicated.

The LS-G6 Gateway is composed of:

1. The Casing
2. Cable gland for RJ45 PoE, or DC Power cable
3. N connector, for the sensor network radio antenna
4. Pressure stabilizer for protection against condensation
5. Sensor network radio antenna, with N connector
6. The mounting kit
7. A PoE injector, and its power supply cable

The Gateway casing can be opened (Figure 14) by putting a flat-head screwdriver in the small holes on either side of the door. You will need to open the Gateway to perform the initial installation and configuration procedure.



Figure 14: LS-G6 Gateway opened.

Note that PoE power supply should be installed inside a box or indoor, since it is not waterproof.

2.4.2. Powering the Gateway

The Gateway can be powered by either PoE (Power over Ethernet), or via DC in. Only one power source is necessary. The nominal power consumption is about 3,2W (270 mA at 12V); peaks are up to 3,84 W of consumption, while idle is 2,16 W.

- Power through PoE
 - The PoE in the LS-G6 Gateway is IEEE 802.11af compliant. It's supplied with a compatible PoE power supply, but it's also possible to use another compatible adapter, or a PoE switch or router.
 - On the Gateway side, the Ethernet cable (not included) must first be inserted into the case through the cable gland. Then, the cables must be unshielded and stripped, and connected into the terminal blocks in the correct order, as described on the Figure 15.



Figure 15: Detail of the connections for the Power through PoE.

- The cable gland allows external cable diameter from 4 mm to 8 mm.
- On the other side of the PoE cable, the RJ45 connector must be inserted into the PoE injector. The PoE injector must be connected to 230VAC.
- The RJ45 cable must be wired according to the T-568A/B specification (Figure 16).

Note that a suitable weatherproof Ethernet cable should be used if the gateway is going to be placed outdoors (e.g. Ubiquity ToughCable). Alternatively, a normal Ethernet cable could be used, but using a protection tube.

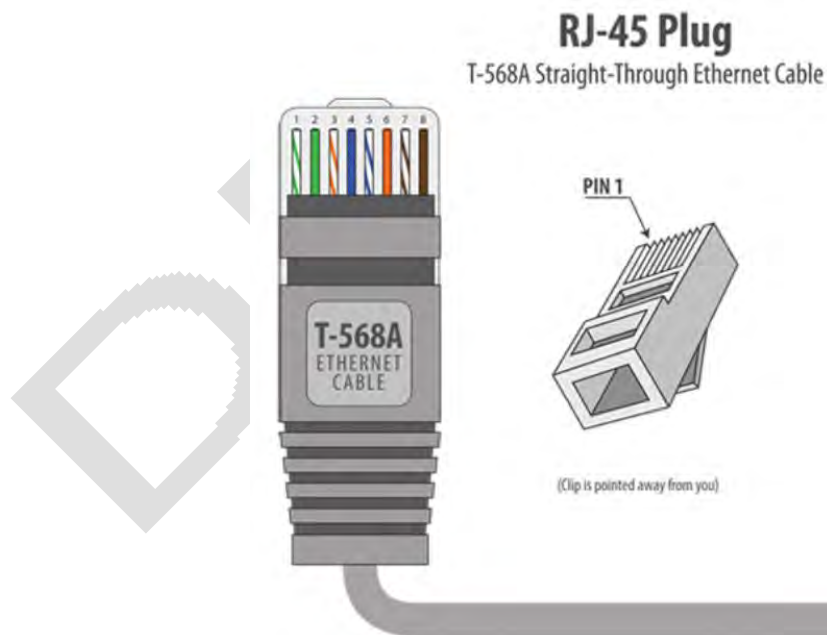


Figure 16: Wiring of the cable at the RJ45 connector (following T-568A/B specification) to be inserted in the PoE Injector.

- The Gateway can also be powered with a DC power supply, such as a solar panel. The input voltage range is 11 to 30 VDC.
- On the Gateway side, the cable must first be inserted through the cable gland. The DC in is the terminal block shown as in Figure 17.

Note that if the gateway is powered using a generator or another source that may induce surges or spikes, a voltage stabilizer may be installed in the power input of the gateway.

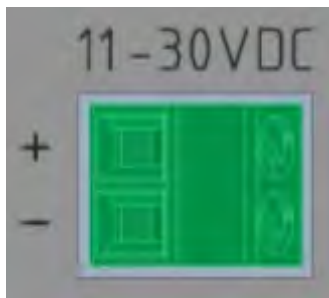


Figure 17: DC terminal block.

- The cable gland allows external cable diameter from 4 mm to 8 mm.

Note that when powering out the gateway, the shutting down process takes some time. Therefore, even if the power is disconnected, the gateway may be active.

2.4.3. Mounting of the enclosure

The gateway enclosure comes with a mounting kit, which is designed for various configurations:

- Pole mounting by U-bolt (Figure 18)

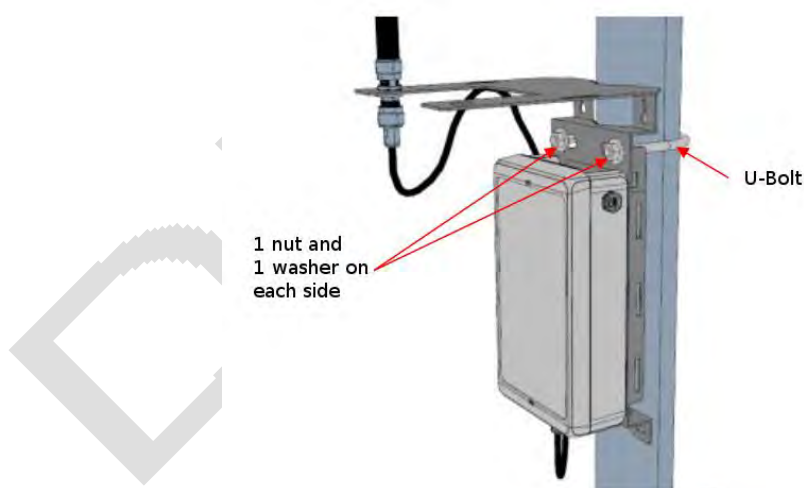


Figure 18: Gateway mounted in a pole.

- Wall mounting (Figure 19)

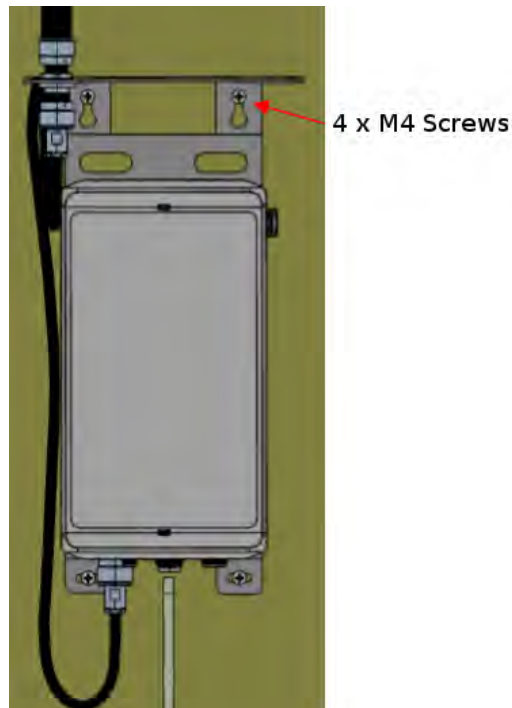
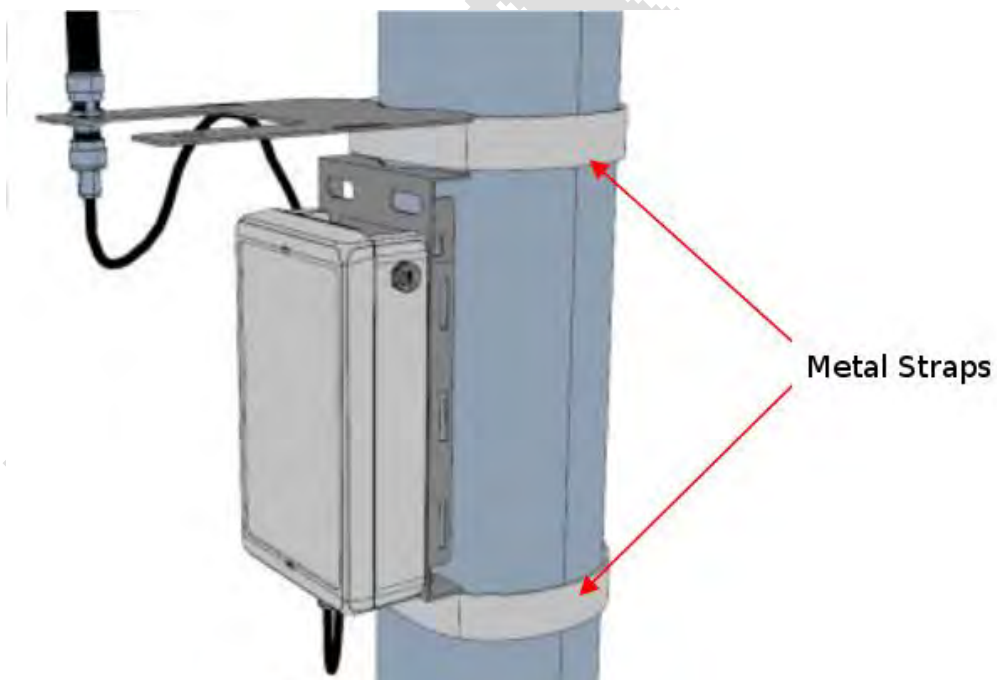


Figure 19: Gateway mounted on the Wall.

- Metallic strapping mounting (tube, pipe, flue..)



The metallic mounting kit must be grounded for safety reasons.

The antenna must also be mounted in its place on the mounting kit (Figure 20).



Figure 20: Gateway's antenna mounting.

The supplied antenna cable must be connected to the gateway enclosure, as shown on Figure 21:

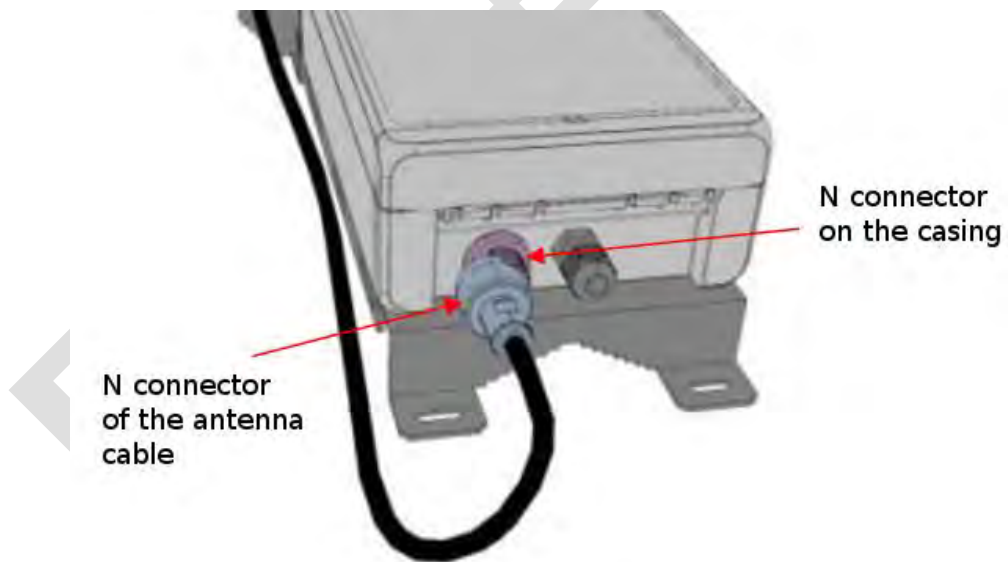


Figure 21: Connection of the antenna cable to the connector.

Finally, the antenna cable must be strapped to the mounting kit to reduce accidental wear.

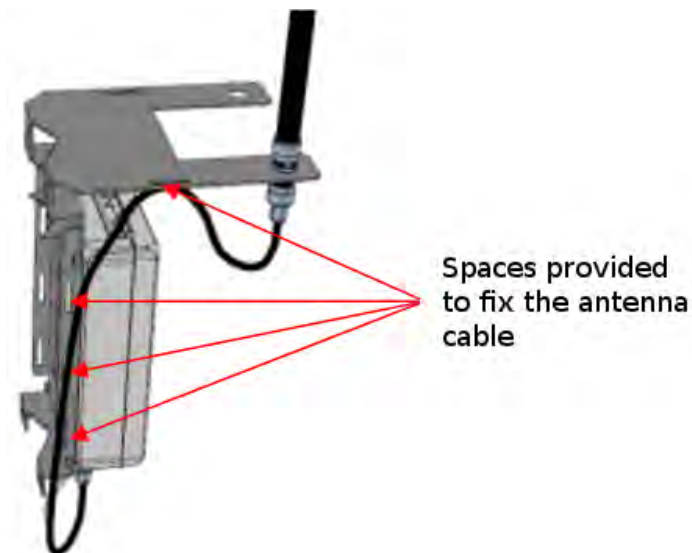


Figure 22: Fixing of the antenna cable.

Note that the gateway does not ship with surge protection out of the box as the dataloggers do. However, if this kind of protection is desired, it is possible to achieve it by using external devices (Ethernet Link and Antenna Link). Contact Worldsensing technical support for further information.

2.4.4. SIM Card

If the Gateway is meant to use a Gprs/3G connection, you will need to insert the SIM card in its place (Figure 23).

To insert a SIM card:

- Open the Gateway enclosure, using a flat-head screwdriver
- Push the SIM extraction button, using a small screwdriver, or the point of a pen
- Put the SIM in the tray, with the contacts facing out
- Put the tray back into the Gateway

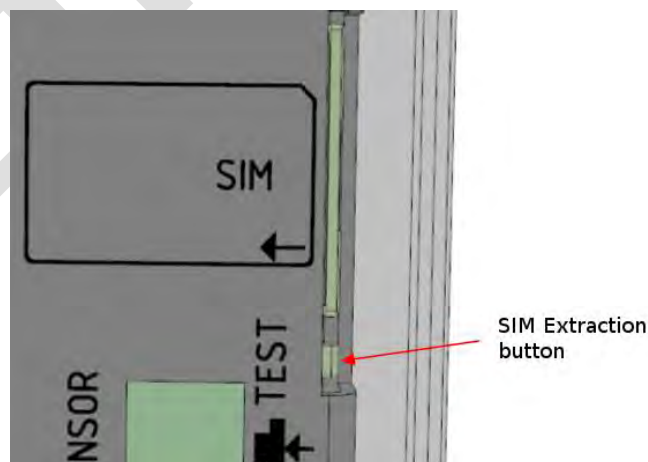


Figure 23: SIM card slot. Indicated the Extraction button.

2.4.5. Ethernet connection

If the Gateway is meant to be connected to the Internet by Ethernet cable, it will be done through the PoE injector (Figure 24).

Note that Ethernet cable should be connected before plugging in the PoE injector to 230VAC. Once the gateway is initialized, Ethernet connection should be established in order to avoid problems with the default Internet access configuration (see section 2.5.2.2.).



Figure 24: PoE. Left port (Data & Power Out) is for the Power Cable and right port (Data in) is for the Data transmission.

2.5. Gateway configuration

Configuration is done with a desktop or laptop computer. The LS-G6 Gateway provides a web interface for all configuration and data retrieval tasks. The interface is accessible through **any** of the gateway's network connections, which will be explained in this section.

2.5.1. Connecting to the Gateway

2.5.1.1. Local administration interface

In order to connect to the Gateway onsite, without depending on any external network, you may use the Local administration interface. This interface provides all features of the web administration, including the network configuration and access to the LS-G6 data.

In order to use the local administration interface, you must:

- Open the Gateway box, using a flat-head screwdriver
- Connect the supplied USB Ethernet adapter to the USB port on the front plate of the Gateway
- Connect an ethernet cable between the gateway's USB adapter and your laptop computer.
- Your computer must be configured to acquire an IP address automatically using DHCP
- Open the following website on your Internet Browser:
 - <http://169.254.0.1>
 - user: admin
 - password: VMjG6z
 - An SSL certification error will appear. This is normal, as this Gateway uses a self-signed certificate for SSL authentication. Add a security exception

for this certificate so the connection is allowed. Check your browser's documentation for instructions on how to do this.

The Local administration interface should be used for:

- Initial configuration of a new Gateway
- Onsite data retrieval and gateway configuration of a gateway without an internet connection
- In case the remote access password is forgotten. The local administration interface has a fixed password, which cannot be changed

2.5.1.2. Remote Access connection

If the gateway has a SIM card or it is connected to a router through Ethernet, the remote access to the gateway is habilitated.

2.5.2. The Gateway's configuration and data access interface

In order to access the gateway's web configuration interface, you need a working network connection to the Gateway. There are 3 access methods to the interface:

- Using the Local administration interface
 - Explained earlier in this chapter, the local administration interface is meant to be used for initial configuration of the other interfaces, and onsite access to the gateway
 - The credentials for local access are fixed and cannot be changed
- Using the public network interface
 - If the Gateway has a working network interface (Ethernet or 3G) and its public IP is known, it's possible to access the web interface through it.
 - The password for this type of access is the remote web access password.
 - The default remote web access password is printed on your Gateway Information Sheet
 - The password can be changed from the web configuration interface
- Using the Loadsensing Remote Access Service
 - If the Gateway has a working Internet connection (Through Ethernet or 3G), it's possible to use the Loadsensing Remote Access Service.
 - This service allows secure remote access to a Gateway using an easy address, even if the network is inside a private network or is connected through a 3G connection.
 - The remote access address for a given Gateway is <http://loadsensing.wocs3.com/XXXX>, where XXXX corresponds to the gateway's serial number.
 - The password for this type of access is the remote web access password.
 - The default remote web access password is printed on your Gateway Information Sheet
 - The password can be changed from the web configuration interface

2.5.2.1. Networks

The first page shown when entering the gateway's Web Configuration Interface shows the network ID and three different menus: networks, status and configuration. In case that

the network ID has been changed for a specific gateway (the same serial number), several networks will appear in this tab, under different IDs. A personalized name may be given to the network under the feature "Name". Finally, the number of dataloggers, active and inactive are shown, and displayed in green or red according their status (active/inactive).

When entering the network, several features of the nodes are visible: status, model, serial number. Serial and node ID coincide by default but Id may be changed (Figure 25). Through this page it is possible to:

- Download the compacted .dat/.csv files of the data collected by the network (raw data or engineering units (see section 2.5.3. for further information).
- View the signal coverage test map, where the results of the signal coverage tests are geographically plotted.
- See datalogger basic information: status, Id, Serial number, model
- Access to all the menus of the gateway Gateway configuration interface.
- Access to the visualization of the data sent from the dataloggers. Also the messages lost and received by the gateway are counted (under status tab). The green number indicates the messages received, the red number corresponds to the radio lost messages and the orange to the lost ones due to gateway power interruption (Figure 26).
- Remotely change the sampling rate of the dataloggers*

**This feature requires minimum gateway software version 1.7. and minimum dataloggers firmware version 2.15. Please contact Worldsensing for further information on firmware and software versions.*

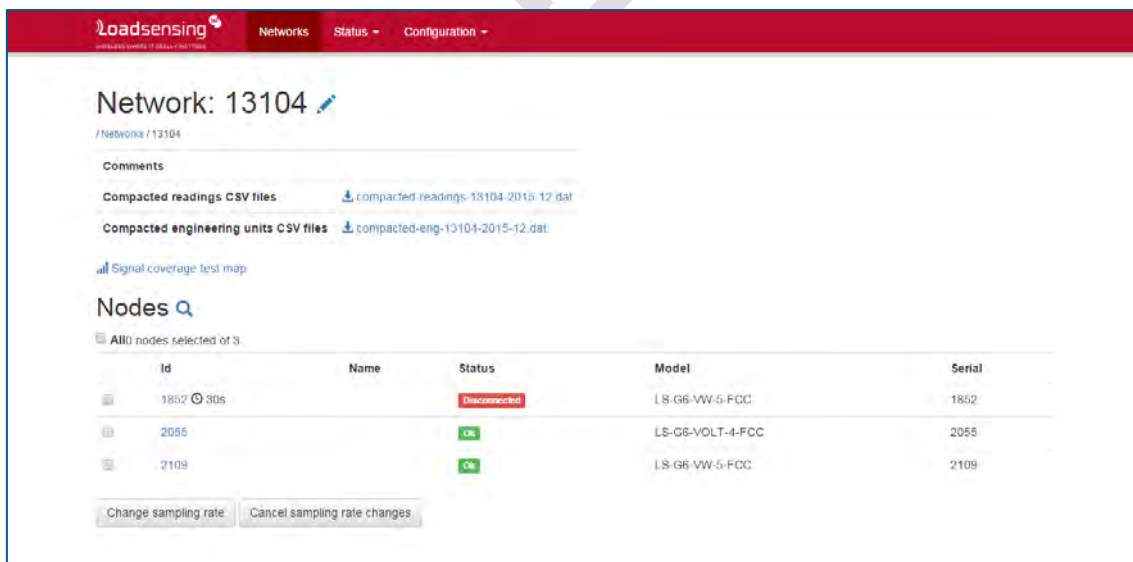


Figure 25: Initial page of the gateway. This is the first page when entering the Web's Configuration Interface.

Status	
Status	Ok
Last status change date	2016-01-13 01:55:13 AEDT
Monitoring status emails	✓ Yes
Messages received: today	368 1
Messages received: 1 day ago	107 5 2
Messages received: 2 days ago	74 1
Messages received: 3 days ago	0 0
Messages received: 4 days ago	0 0
Messages received: 5 days ago	0 0
Total number of messages since gateway installation	549 7 2

Note: all messages not received are stored in the node, and can be retrieved with the dlog app

Figure 26: Summary of the datalogger status and the historical received/lost messages.

Remote change of sampling rate

- The sampling rate can be remotely changed for one or several dataloggers.
- When selecting the check box in the left of the corresponding line and apply "Change sampling rate" the new sampling rate option has to be selected from a pop up menu.
- Once done and changes saved, a clock icon with the value of the new sampling rate next to it will appear at the Id column of the node.
- When it appears with an orange label, it means that the change has still not been applied.
- If the orange label disappears, it means that the change is effective.
- While the orange label is active, the changes can be cancelled.
- If the user tries to introduce a sampling rate not suitable according to the slot times required for the network, a message will appear where the user will have to accept that he/she understands the risk (Table 8).

2.5.2.2. Status

In the status tab, the user can view the Gateway status or the Logs of the gateway.

➤ Gateway status

In the gateway status menu, the following information is displayed (Figure 27).

- General Information
 - Gateway serial number
 - Shows the hardware's serial number. This value cannot be changed.
 - Gateway Model
 - Shows the hardware model.
 - Firmware version
 - Shows the current Firmware version. The Gateway's firmware can be remotely updated by Worldsensing Technical Support, as long

as the Gateway has an Internet connection, and remote access is working (see below)

- Date
 - Shows the current date, according to the gateway's internal clock, always in UTC
- Uptime in minutes
 - Shows the time in minutes since the gateway was connected or rebooted
- Input voltage
 - Shows the voltage that powers the gateway. This reading has a precision of +/- 0.35V
- Application status
 - Network ID
 - Shows the current sensor radio network ID
 - Internet connection (ping)
 - Shows if the gateway is able to connect to the Loadsensing server, in order to check for connectivity.
 - Check the "Internet configuration" section for more information on this check.
 - Status reporting
 - Shows if the gateway is able to send status reports to Worldsensing.
 - These reports are sent via HTTP (port 80) to loadsensing.wocs3.com, and will provide information on the gateway's status to Worldsensing Technical Support
 - Remote access
 - Shows if the gateway is able to open a remote access connection to the Worldsensing server.
 - This service uses a TCP connection to loadsensing.wocs3.com, on port 22
 - The remote access mechanism is used:
 - To provide the Loadsensing Remote Access Service, which allows remote access to the Web Configuration Interface
 - To provide remote access capability to Worldsensing Technical Support, which allows for remote support and remote updates of deployed Gateways
- Network information
 - Ethernet status, IP and Netmask
 - Shows the status of the Ethernet interface (up/down), and the current address if there is one
 - Gprs/3G status and IP
 - Shows the status of the Gprs/3G interface (up/down), and the current address if there is one
 - Default Gateway and DNS servers
 - Shows the parameters of the currently active network configuration

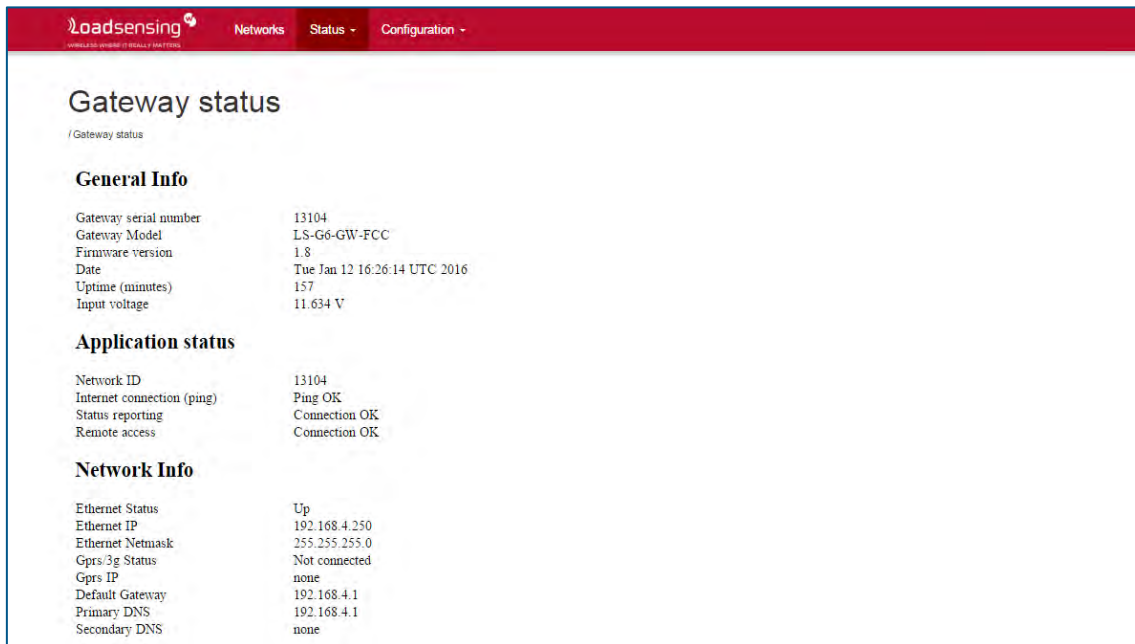


Figure 27: Gateway status page.

➤ Logs

In the Logs page, the status actions are reported and the user can select by dates the logs to be displayed.

2.5.2.3. Configuration

The configuration tab shows the different configuration options.

➤ General

The gateway has an internal clock configured in UTC, however, the user can introduce the time zone in the gateway software interface. By doing so the user will be able to retrieve and visualize the data in local time.

LoadSensing
WIRELESS WHERE IT REALLY MATTERS

Networks Status Configuration

General

/ General

Timezone UTC

Monitoring notification emails

One email per line, without semicolon or commas.

Save

➤ FTP client

In the configuration tab, the user can configure a FTP client, in order to push the data stored in the gateway automatically to the server (see 2.6 Data visualization and retrieval).

➤ Internet

Also in the configuration tab, the user can change the details of the Internet connectivity (Figure 28). By default, it is set in the automatic mode (Figure 28).

LoadSensing
WIRELESS WHERE IT REALLY MATTERS

Networks Status Configuration

Internet

/ Internet

☒ Activate network Watchdog

Disable the Network Watchdog if this gateway does not have an internet connection
The network watchdog is a mechanism to reboot the gateway in case of a network failure, modem freeze or other network error condition.
It will reboot the gateway after 40 minutes of consecutive unsuccessful Internet connection attempts.

Network connection:

☒ Automatic (Ethernet if connected, gprs/3g otherwise)

☐ Manual Configuration

Changes will not be applied until next device reboot.

Save configuration

Figure 28: View of the Internet configuration tab of the Gateway. The present configuration is the one by default.

- **Network Watchdog**
 - The Network Watchdog is the mechanism that checks if the Internet connection is working properly.
 - This mechanism is checking for Internet connectivity every minute, by sending a ping request to `loadsensing.wocs3.com`
 - If the Gateway is unable to communicate with the server for 40 minutes, it will assume there is a problem with the connection, and reboots the Gateway

- The Network Watchdog must be disabled if the Gateway does not have an Internet connection
 - If a Gateway with no Internet connection is left with the Network Watchdog enabled, it will start a reboot cycle every 40 minutes. This will lead to sensor data loss, as data incoming during the reboot cycle will not be stored.
- The Network Watchdog is enabled by default
- Network connection
 - Automatic (default)
 - In automatic mode, the network connection mode is automatically configured on Gateway startup
 - If a connected Ethernet cable is detected, an Ethernet connection with DHCP will be used
 - An Ethernet cable is connected if there is some kind of network equipment (for example router or a switch) on the other side of the cable. The PoE injector doesn't count.
 - If no Ethernet cable connection is detected, the Gprs connection will be launched, with its configured parameters

Network connection:

- ☐ Automatic (Ethernet if connected, gprs/3g otherwise)
- ☒ Manual Configuration
- ☒ Gprs/3G
- ☐ Ethernet with DHCP
- ☐ Ethernet with static IP

Manual configuration (Figure 29)

- Figure 29).

Network connection:

- ☐ Automatic (Ethernet if connected, gprs/3g otherwise)
- ☒ Manual Configuration
- ☒ Gprs/3G
- ☐ Ethernet with DHCP
- ☐ Ethernet with static IP

Figure 29: Options for manual configuration.

This setting will override autodetection, and always launch a gprs/3G connection

- Ethernet with DHCP
 - This setting will override autodetection, and always launch an Ethernet connection, getting the configuration automatically through DHCP
- Ethernet with Static IP
 - This setting will override autodetection, and always launch an Ethernet connection.
 - In this mode, you need to manually set all parameters of the network configuration:

- IP Address
- Netmask
- Default gateway
- DNS servers

➤ GPRS/3G

The GPRS/3G configuration tab (Figure 30) contains some configuration parameters specific to this type of connection.

The screenshot shows the 'GPRS / 3G' configuration page. At the top, there's a red navigation bar with 'LoadSensing' logo and tabs for 'Networks', 'Status', and 'Configuration'. Below the header, the title 'GPRS / 3G' is displayed. The settings include:

- PIN:** Two radio buttons: 'PIN Off (Sim card is unlocked)' (selected) and 'PIN On (Sim card needs PIN code)'.
- APN:** Two radio buttons: 'APN Auto selection (will select based on the SIM card operator)' (selected) and 'Manual APN Configuration'.
- Manual Configuration Fields:** Three input fields for 'APN:', 'Username:', and 'Password:'.
- Footer:** A message 'Changes will not be applied until next device reboot.' and a 'Save configuration' button.

Figure 30: Settings for the configuration of the GPRS/3G connection.

This configuration will be applied whenever a GPRS/3G connection is used, regardless of it was the result of an automatic or manual configuration in the Internet tab

- PIN setting
 - Off (default)
 - In this mode, the Gateway will not try to unlock the SIM card.
 - If the SIM card is protected by a PIN code, the GPRS/3G connection will fail.
 - On
 - This setting will allow you to enter the PIN code for use with a PIN-locked SIM card.
 - Be careful not to boot the Gateway with a PIN-protected SIM card, and the wrong PIN set here. The Gateway will automatically retry unlocking, and exhaust the 3 tries.
 - There is no way to enter the PUK code in the Gateway. If your card gets PUK-locked, you will have to unlock it using a mobile terminal.

- APN settings
 - APN Auto selection (default)
 - Every mobile operator requires the setting of a specific configuration for connection to its network.
 - The LS-G6 Gateway features a database of the correct configuration for hundreds of operators around the world. This setting will try to configure the connection automatically based on the SIM card that is inserted.
 - This setting may fail if your operator is not in the database, or your configuration is non-standard.
 - Manual APN configuration
 - This setting will allow manual input of the mobile operator configuration values.
 - Use this setting if auto selection didn't work for you, or you need to input specific, non-standard configuration values.

➤ Remote access

This page will allow you to change the password used for remote access to the Web Configuration Interface (Figure 31).

The new or the initial provided password will be required to access the gateway either through the public network interface, or through the Loadsensing Remote Access Service.

Be careful on setting weak passwords. This will make your Gateway accessible from anywhere on the public network, or anywhere on the Internet if you have an Internet connection.

In order to change the password from the public interface or from the Remote Access Service, you will need to input the previous password. This is not required if you are connected through the local administration interface.

The default factory password is printed on the Gateway Information Sheet. Once you change the password, there is no way to recover it.

In case of a lost or forgotten remote access password, you will have to use the Local Administration Interface to change it to a known one (section 2.5.2).

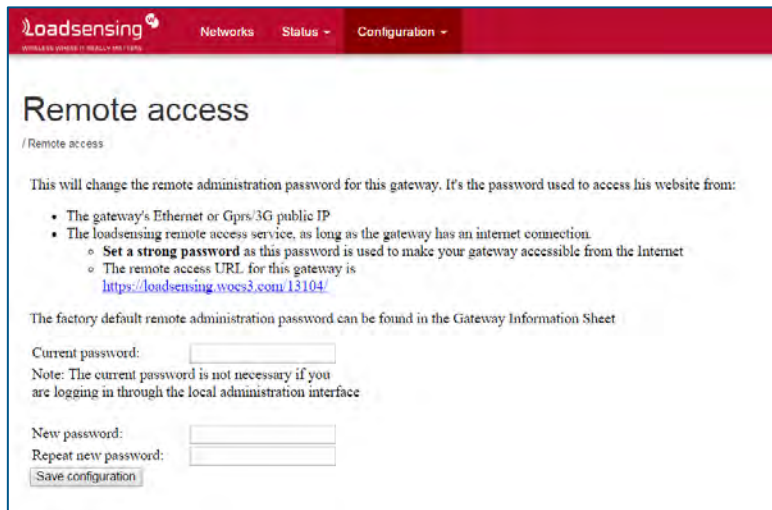


Figure 31: Remote Access tab, inside the gateway interface.

➤ Radio

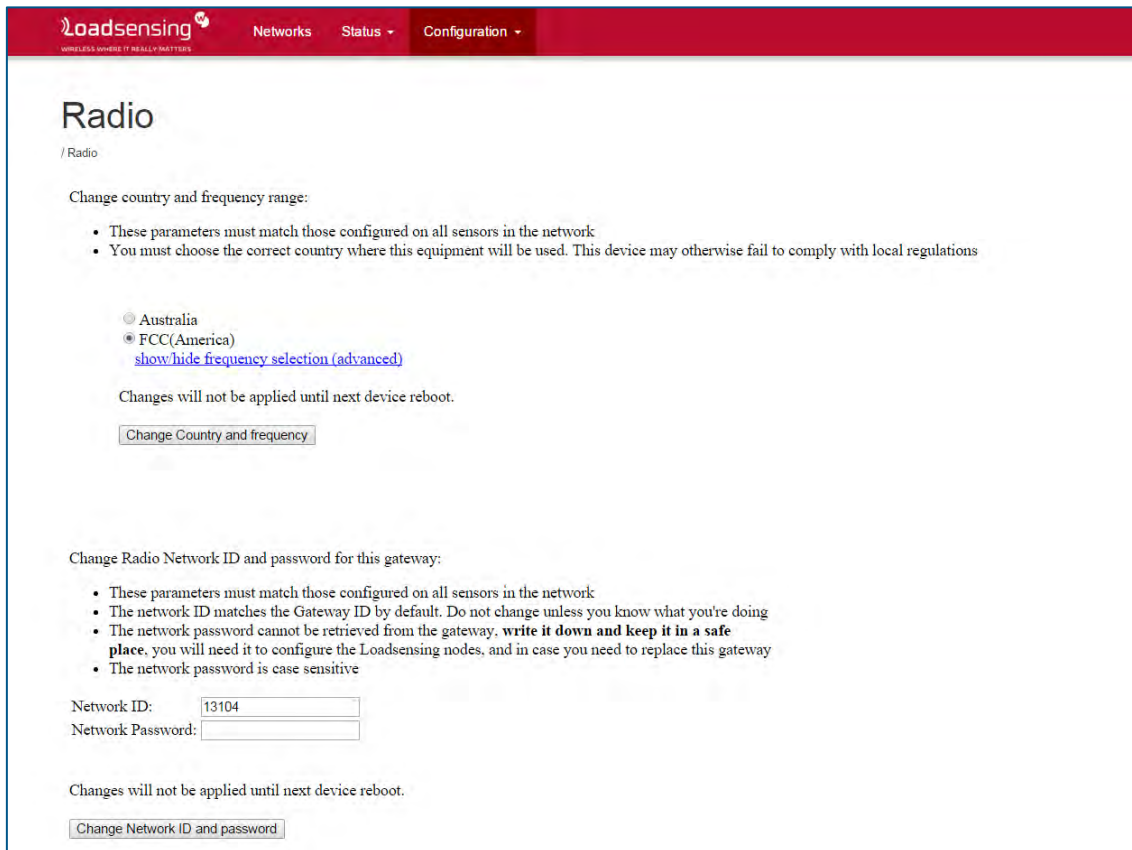
This page will allow you to configure the parameters of the Wireless Sensor Radio Network (Figure 32). There are three different gateway models, according to geographical areas where they are going to be placed. In addition, depending on the country regulations, the radio configuration will be set specifically.

Note that for some countries, an advanced menu can be displayed. It refers to the possibility of choosing different channels through the ones the data can be sent, in each spreading factor. This could be useful for a project with many dataloggers (hundreds), sampling at a high rate, to set some of the dataloggers at one group (and also one gateway) and some other nodes at a different frequency group (and also a second gateway configured to this other group) for avoiding any possible collision.

Note that if the user changes the default configuration of the advanced options, this should be also changed in the datalogger configuration (see sections 2.3. and 4).

In order for the LS-G6 dataloggers to be able to connect to this Gateway and send data, both the Gateway and all participating dataloggers need to be configured with the same parameters.

- Network ID
 - A numeric identifier of the wireless sensor network
 - It's set by default to the serial number of the Gateway
 - You should only change it if you're replacing a Gateway and don't want to reconfigure all dataloggers in the network
- Network Password
 - This password is used to encrypt all data in transit on the Wireless Sensor Network.
 - The default factory password is printed on the Gateway Information Sheet.
 - Once you change the password, there is no way to recover it. You will have to change it to a known one in the Gateway and in all dataloggers in the network.



Radio

/ Radio

Change country and frequency range:

- These parameters must match those configured on all sensors in the network
- You must choose the correct country where this equipment will be used. This device may otherwise fail to comply with local regulations

☐ Australia
☒ FCC(America)
[show/hide frequency selection \(advanced\)](#)

Changes will not be applied until next device reboot.

Change Radio Network ID and password for this gateway:

- These parameters must match those configured on all sensors in the network
- The network ID matches the Gateway ID by default. Do not change unless you know what you're doing
- The network password cannot be retrieved from the gateway. **write it down and keep it in a safe place**, you will need it to configure the LoadSensing nodes, and in case you need to replace this gateway
- The network password is case sensitive

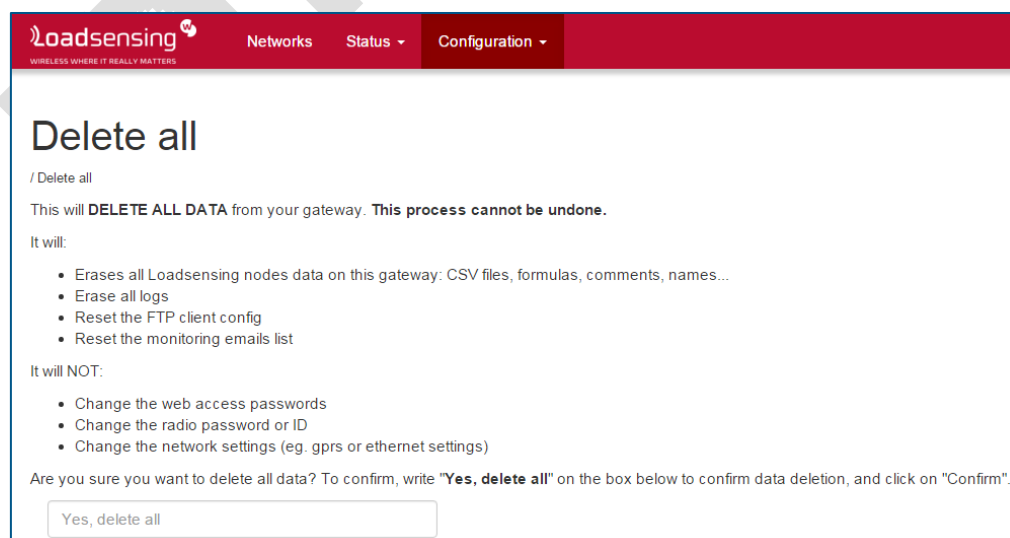
Network ID:
 Network Password:

Changes will not be applied until next device reboot.

Figure 32: Radio config tab, inside the gateway interface.

➤ Delete all

In order to delete all the data contained in the gateway (but not all the configuration), the user has to access the tab “Delete all data” (Figure 33) and follow the instructions.



Delete all

/ Delete all

This will **DELETE ALL DATA** from your gateway. **This process cannot be undone.**

It will:

- Erases all LoadSensing nodes data on this gateway: CSV files, formulas, comments, names...
- Erase all logs
- Reset the FTP client config
- Reset the monitoring emails list

It will NOT:

- Change the web access passwords
- Change the radio password or ID
- Change the network settings (eg. gprs or ethernet settings)

Are you sure you want to delete all data? To confirm, write **"Yes, delete all"** on the box below to confirm data deletion, and click on "Confirm".

Figure 33: Delete all tab, inside the gateway interface.

➤ Reboot

After changing some of the configuration parameters of the gateway, it needs to be rebooted to apply the changes (Figure 34).

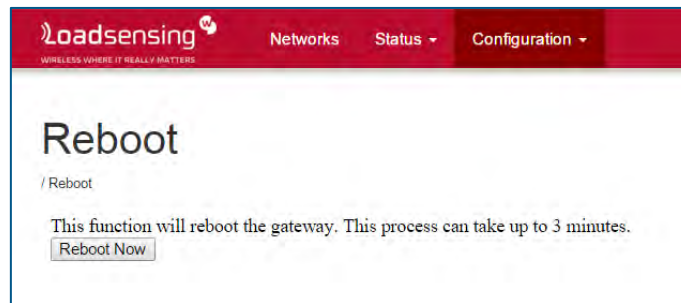


Figure 34: Reboot tab, inside the gateway interface.

2.6. Data visualization and retrieval

For all the models, data files (.csv) can be retrieved by USB cable from the datalogger using the OTG USB cable, through the Android application DLOG. The option for downloading data is in the "Sensors data" tab, using the arrow pointing down. The data files can also be sent via email.

For the radio models only, the data is sent to the gateway and is retrieved from there. In the gateway it is possible to display the data collected in the nodes, transformed into engineering units and with a graphical interface.

For the transformation into engineering units, the user has to introduce the suitable formula, depending on the sensor. In the Last readings tab, when selecting a node, a gear icon is placed in the most right of each channel's last reading (Figure 35). By clicking this icon, the menu to edit the formula corresponding to the sensor is displayed (Figure 36).

The formula has to be selected from a drop-down menu of several Linear and Polynomial formulae available.

Last readings and Time series graphs			
Channel	Thermistor (Ohms) ↕	Frequency (Hz) ↕	
1	4294967.295	1529.097	⚙
Pressure (mBar) ↕		Pressure (kPa)	
1011.1		101.11	⚙
Received on 2015-09-01T09:47:30Z			

Figure 35: In the "Last readings" tab, it appears a gear icon in the right, to edit the formula of the sensor.

LoadSensing Networks Configuration

Engineering units

/ Networks / 13004 / Node 1140 / Engineering units

Channel 1

☒ Use engineering units

Polynomial A with compensation

$$P = AR_i^2 + BR_i + C + K(T_i - T_0) - F(S_i - S_0) + D$$

P: Converted data in units
 R_i: Current Reading in digit during observation
 T_i: Temperature during the observation
 S_i: Current barometric pressure in kPa

Units: Magnitude that is measuring the sensor (ie: mBars, mm)

kPa

A: Polynomial gage factor (from calibration)
4.6290E-08

B: Polynomial gage factor (from calibration)
-1.5185E-01

C: Polynomial gage factor (from calibration)
9.6881E+02

K: Thermal factor in units/°C
0.015

T₀: Temperature at the time of taking zero reading in °C
20

F: Conversion factor in units/kPa
1

S₀: Barometric pressure at time of installation in kPa
101.1

D: Offset in units
0

Thermistor YSI44005 (°C)

$$T = \frac{1}{A + B(\ln R) + C(\ln R)^3} - 273.2$$

T: Temperature in °C
 LnR: Natural log of thermistor resistance
 A: 1.4051×10^{-3}
 B: 2.389×10^{-4}
 C: 1.019×10^{-7}
 Note: Coefficients calculated over the -50°C to +150°C span,

Figure 36: Menu to edit the formulae to transform the raw data of the sensors into engineering units.

The gateway data visualization and retrieval is possible by accessing to the gateway (locally or through the server) and clicking the icon next to each header (Figure 37).

The data visualization in the charts supports only the last 400 readings of each sensor. In each chart, all the sensors connected to a datalogger are displayed. Some sensors may be deactivated from the chart by the user (Figure 38).

Under the Configuration tab, the timezone of the gateway can be configured. It is important for the correct display of the charts, since otherwise they will be shown in UTC.

Channel	Thermistor (Ohms) ↗	Frequency (Hz) ↗	Engineering units ↗	T (°C) ↗	
1	3165.588	2207.994	98.546 mm	23.7	⚙

Figure 37: Circled in red, the icon to display the charts of each of the sensors.

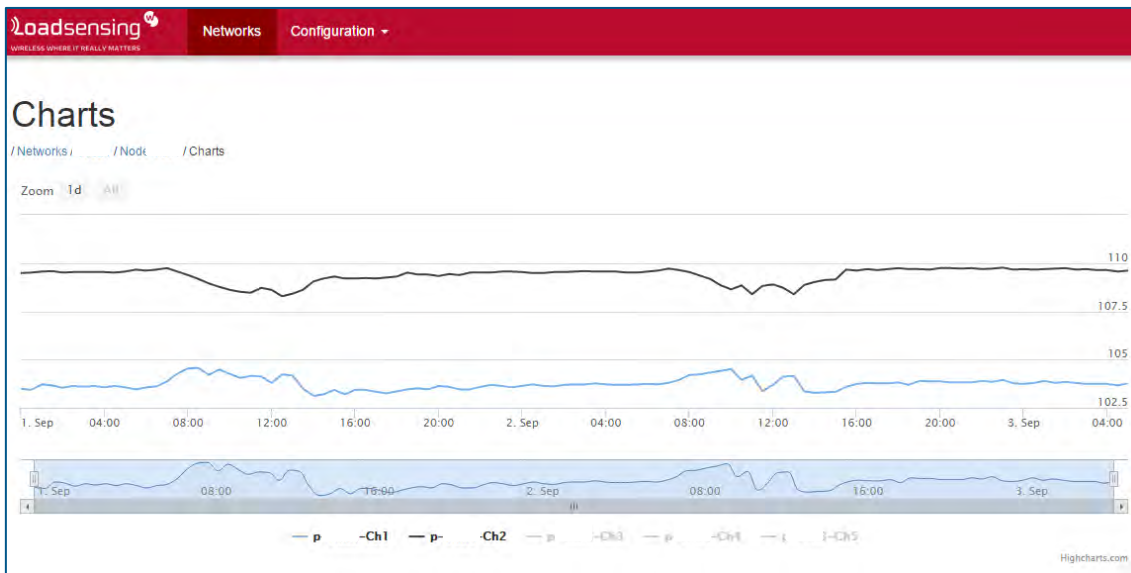


Figure 38: Example of a chart of one datalogger.

The retrieval of the data can be done into two different ways:

- General file of the network: two .dat files are available to download (Figure 39):
 - compacted readings of raw data from the dataloggers
 - compacted readings in engineering units

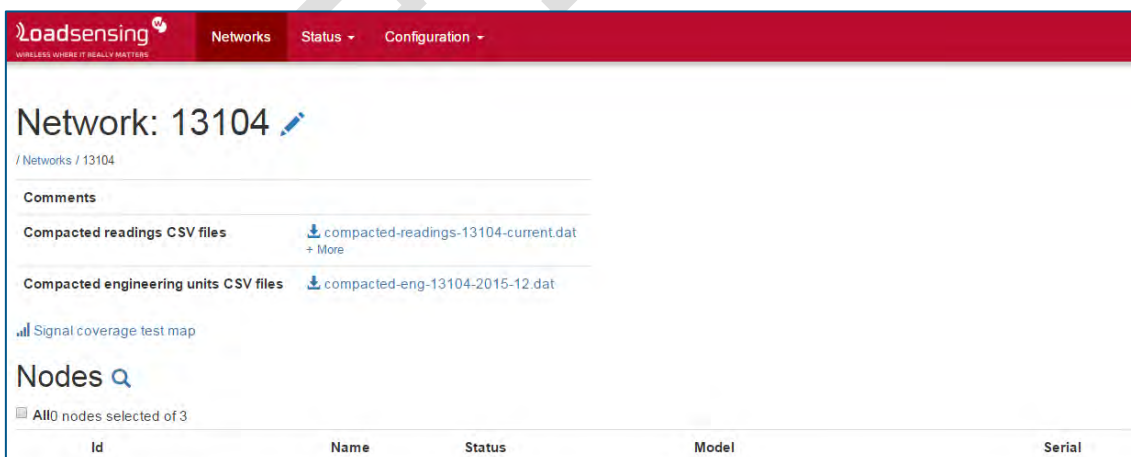


Figure 39: View of the screen where the .csv files of the raw data and the data transformed into engineering units (of the complete network) can be downloaded.

Note that the file where the new data is saved is called xxxxx-current.dat. The current file is prepared to support up to 520 columns.

At the end of the month, the file is closed and named xxxxx-yyyy-mm.dat (yyyy: year; mm: month). Files of past months can be retrieved by clicking "+ More" below the

current file. During the process of closing the file and changing the name, a delay of 1.5 hours appear.

- Specific file for each of the nodes: two csv files are available to download (Figure 40):
 - health (containing battery in V, temperature in Celsius and uptime node in seconds)
 - data readings (raw data)

Node 1852

/ Networks / 13104 / Node 1852

Name

Installation date

Comments

Model LS-G6-VW-5-FCC

Firmware version 2.15

Serial number 1852

Health CSV files [1852-health-2015-12.csv](#)

Vibrating wire CSV files [1852-readings-2015-12.csv](#)

▼ Last readings and Time series graphs

Channel	Thermistor (Ohms)	Frequency (Hz)	Engineering units	T (°C)
1	4294967.295	1571.536	-3.738 mm	-87.5
2	4294967.295	1584.172	160.158 mm	-87.5

Pressure	Pressure (kPa)
988	98.8

Received on 2015-12-17T20:53:32Z

► Status

► Metadata

► Last messages

Figure 40: View of the screen where the data of a specific datalogger can be downloaded.

In the configuration tab, also the FTP can be configured (Figure 41). The user can specify the FTP settings and the files that want to be uploaded. When the FTP is first configured in the gateway, an upload test is performed.

The files can be uploaded to the FTP:

- a) Separately, per node type. Files are pushed every 15 minutes, in real time.
- b) Compacted in one file. Files are pushed every 15 minutes; however this option is delayed one hour respect to the real time. The reason of this delay is that the compacted file is generated every hour, and in order to avoid conflicts between the data receiving and the file creation, the file is created with 1 hour delay.

The folder where the data is uploaded can be directed by a relative path, or by the full path. Data can be accessed through http calls.

LoadSensing
WIRELESS WHERE IT REALLY MATTERS

Networks Status Configuration

FTP client

/ FTP client

Data is pushed to the FTP every 15 minutes

Hostname

Port number

☐ Use anonymous FTP

Username

Password

FTP mode

Type of file	Enabled	Full path (starting with /) or Relative path (starting with ./)
Health	<input type="checkbox"/>	<input type="text"/>
Vibrating wire data	<input type="checkbox"/>	<input type="text"/>
Inclinometer data	<input type="checkbox"/>	<input type="text"/>
Volt data	<input type="checkbox"/>	<input type="text"/>
SHM data	<input type="checkbox"/>	<input type="text"/>
Weather data	<input type="checkbox"/>	<input type="text"/>
Compacted data	<input type="checkbox"/>	<input type="text"/>

Save and test

Figure 41: View of the screen where the FTP can be configured.

Alternatively, the last messages received by the gateway are displayed in API format. This can be viewed under the tab “Last Messages” of the software interface (Figure 42).

Type	Message
coverageTestV1	<pre>{ "nodeModel": "LS-G6-VW-5-EU", "commMetaData": { "networkId": "13012", "macAddress": "57673283", "receivedTimestamp": "2015-09-01T09:35:20Z", "frequencyHertz": 868.85, "snr": 11, "sequenceCounter": [53] }, "gatewayId": 13012, "rssi": -51, "type": "longRangeRadioMetaDataV1", "sf": 12, "macType": "ETSIV1" }</pre>

Figure 42: View of last messages received by the gateway, displayed in API format.

2.7. Maintenance

Proper maintenance of LS-G6 components is essential to obtain accurate data. Equipment must be in good operating condition, which requires a program of regular inspection and maintenance. The person in charge of the logging system can accomplish routine and simple maintenance. More difficult maintenance such as datalogger calibration, datalogger performance testing, and datalogger component replacement, should be done by Worldsensing technical support or by a certified distributor.

A station log should be maintained for each monitoring site that includes serial numbers, dates of site inspections, and maintenance performed.

2.7.1. General Maintenance

- Check sensor leads and cables for cracking, deterioration, proper routing, and strain relief. Replace sensor cables if required.
- Check that the box junction and cable gland are dry and completely tightened.
- Check that the screws are correctly locked and the enclosure lid is in perfect conditions.
- Check battery life periodically. Replace when less than 20% remaining.

2.7.2. Periodical maintenance

1 Month

- a. Monitor data values collected by the units periodically. Abnormal or out of range sensor values may indicate problems with the unit.
- b. Monthly visual inspection of the station to observe any apparent problems.
- c. Do a visual inspection of the sensors and boxes position.

6 Months

- a. Inspect the enclosure seal.

12 Months

- a. Check battery life periodically. Replace when less than 20% remaining.

2-3 years

- a. Battery replacement. The lifetime of the battery depends on the use of each node, number of channels, sensors, etc.

2.7.3. Return material authorization

Products may not be returned to WS without prior authorization. To obtain a Return Material Authorization (RMA), please contact WS technical support. After the nature of the problem is determined, an RMA number will be issued. Please write this number clearly on the outside of the shipping container. The following contact information is for international customers residing in countries served by Worldsensing S.L. directly. Worldsensing's shipping address is:

WORLDSENSING, S.L.

Aragó 383, 4th

08013 Barcelona

(Spain)

3. LS-G6 DATALOGGERS

3.1. LS-G6-VW

3.1.1. Sensor connection

Most of the vibrating wire sensors can be interfaced to the LS-G6-VW.

The datalogger is supplied with cable glands (one for each channel), for the adjustment to different cable diameters.

After each terminal block is connected, it is recommended taking a sensor reading in order to ensure that the connections have been correctly done. This reading should be compared with the reading of the sensor on installation with a portable readout unit, before connecting to the LS datalogger. Note that some configuration is required during the installation (see section 3 of this manual).

Cables must be connected in accordance to the following table:

Each terminal block has a group of 5 connectors.

Each group has:

- 1x Vibrating wire channel
- 1x Thermistor channel
- 1 shield terminal

An example of the connections for one terminal block (Table 1 and Figure 43) is listed below.

Table 1: Connections of the terminal block.

Name	Function
SHLD	Used to connect the sensor shield if needed
TH2-	Thermistor input 2. No polarity.
TH2+	Thermistor input 2. No polarity.
VW2-	Differential voltage input 2.
VW2+	Differential voltage input 2.

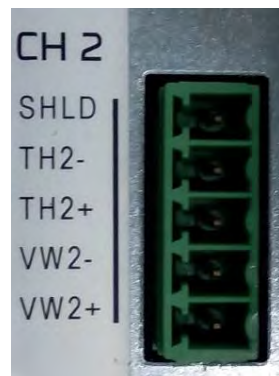


Figure 43: Detail of a terminal block.

3.1.2. Barometric measurements

The datalogger includes a barometer (BOSCH BMP180 device). It is important to avoid placing the datalogger inside any type of container. This would affect the correct readings of the barometer through the gore valve.

If the Vibrating Wire sensor requires barometric pressure compensation (such as piezometers installed in locations which can be affected by changes in barometric pressure), the current pressure readings from the barometer are usually used directly. The transformed data (compensated by the barometric pressure) is displayed if the user selects the option "Polynomial A with compensation" in the "Engineering Units" drop-down menu (see section 2.6).

In case that the desired measurement is the atmospheric pressure at the sea level (commonly used in meteorology), a correction of the barometric readings is needed.

The formula for the correction of the barometer readings in order to provide atmospheric pressure at the sea level is:

$$p_0 = \frac{p}{\left(1 - \frac{\text{altitude}}{44330}\right)^{5.255}}$$

p_0 = pressure at the sea level in mbars

p = current pressure reading

altitude= altitude in m.a.s.l.

3.1.3. Battery lifespan

The following table gives the indicative battery lifespan for channel (Table 2). User should take into account that consumption varies depending on the sensor used, the sampling rate and the environmental conditions.

*Table 2: Indicative lifespan for LS VW-datalogger 1 ch and LSVW- datalogger 5 ch.
Estimations using 4 c-size cells*

Number of sensors	Sampling rate			
	1 hour	30 minutes	5 minutes	10 sec
1	>10 years	>10 years	>10 years	1,2 years
5	>10 years	>10 years	7 years	3 months

NOTE: Extreme temperatures could cut down the capacity from 20 to 40%, check the specifications of your batteries. USB not used

3.1.4. Configuration

The vibrating wire node requires configuring the sweep frequency before starting. There are several existing sweep frequencies predefined:

- Sweep Frequency A (450-1125 Hz),
- Sweep Frequency B (800-2000 Hz),
- Sweep Frequency C (1400-3500 Hz),
- Sweep Frequency D (2300-6000 Hz)
- Custom Sweep Frequency (min value: 300 Hz max value: 7000 Hz).

For the configuration of the radio communications of the datalogger, see section 2.3 of this manual.

3.1.5. Data storage

The internal node memory size is 4 MB. The 5-channel datalogger connected to 5 sensors stores up to 73.500 readings. The 1-channel datalogger stores up to 200.000 readings. Times of data storage for LS datalogger 1 ch and LS datalogger 5 ch are indicated in Table 3. Memory mode is a circular buffer. When memory is full, logging continues by overwriting earliest readings. Besides the data from the sensor, health data is collected hourly, which indicates the battery voltage, the internal temperature of the node and the node uptime.

Table 3: Times of data storage (without overwriting) for LS VW-datalogger 1 ch and LS VW- datalogger 5 ch.

Number of sensors	Sampling rate		
	60 minutes	30 minutes	10 minutes
1	more than 10 years	more than 20 years	3,5 years
5	8 years	4 years	17 months

3.2. LS-G6-DIG

3.2.1. Sensor Connection

LS-G6-DIG datalogger supports 2 different sensor models by default (RS485 port):

- Geosense Inclinometer (<http://www.geosense.co.uk/products/details/mems-inclinometer-vertical-in-place>)
- RST inclinometer (<http://www.rstinstruments.com/In-place%20Vertical%20MEMS%20Inclinometer.html>)
- More models can be added with the development of the drivers by Worldsensing developers. Contact Worldsensing technical support.

Regarding power consumption Worldsensing ensures that up to 30 inclinometers can be safely powered from the datalogger. However up to 60 sensors may be read and transmitted by the datalogger. If more sensors are to be supplied, an external 12 V battery should be connected. In this case, contact Worldsensing.

The wiring is indicated in the RS485 port of the datalogger. The datalogger has to be placed at HALF to read the inclinometers. For the connection of digital dataloggers at SDI ports the wiring has to be checked at the sensor specifications.



Figure 44: View of the inside of the digital datalogger.

LS-G6-DIG dataloggers (Figure 44) can also support other digital sensors, with SDI interface connection. These type of sensors are not supported by default by the datalogger, but drivers can be developed by Worldsensing engineers. The wiring for the sensors with SDI interfaces will depend on the model of the sensor; however, the label of each terminal is indicated.

3.2.2. Battery lifespan

The following table gives the indicative battery lifespan for channel (Table 4). User should take into account that consumption varies depending on the sensor used, the sampling rate and the environmental conditions.

Table 4: Indicative lifespan for LS-DIG datalogger. Estimations using 4 c-size cells

Number of sensors	Sampling rate			
	6 hour	2 hour	30 minutes	5 minutes
10 (RS485)	>20 years	5,5 years	2,5 years	4 months
30 (RS485)	5,2 years	10 months	4 months	26 days

3.2.3. Configuration

The configuration of the digital datalogger requires specifying the protocol of communication (from given options) and the bus addresses of the sensors connected in the RS485 port. This action is done through the Android Configuration App. The bus addresses of the digital sensors are specified by the manufacturers. Up to 30 sensors can be connected in a bus chain. When connecting the sensors, we recommend using resistors. In some cases is clearly specified by manufacturer of the sensors.

For the configuration of the radio communications of the datalogger, see section 2.3 of this manual.

3.2.4. Data storage

Capacity for up to 90.000 readings from the inclinometers (each one with 2 axes and temperature, grouped by 5 sensors) (Table 5).

Table 5: Indicative storage capacity of the LS-DIG datalogger. Estimations using 5 sensors.

Number of sensors	Sampling rate		
	60 minutes	30 minutes	10 minutes
5	more tan 10 years	5 years	20 months

3.3. LS-G6-ANALOG

3.3.1. Sensor Connection

LS-G6-ANALOG datalogger supports 6 different sensor models that can be connected independently to four different channels (Figure 45):

- Voltage (+/- 10 V peak to peak)
- Full Wheatstone Bridge (39.06 mV)
- Thermistor (-40 to 85 °C for a standard 3K ohms)
- Current Loop (4-20 mA, 2 or 3 wires)
- Potentiometer (5 V)
- PT100 (-40 to 85°C)



Figure 45: View of the LS-G6-ANALOG datalogger internally where the four channels can be identified.

The wiring of the sensors is indicated in the Android configuration app, once selected the type of sensor connected to the channel (Figure 46).

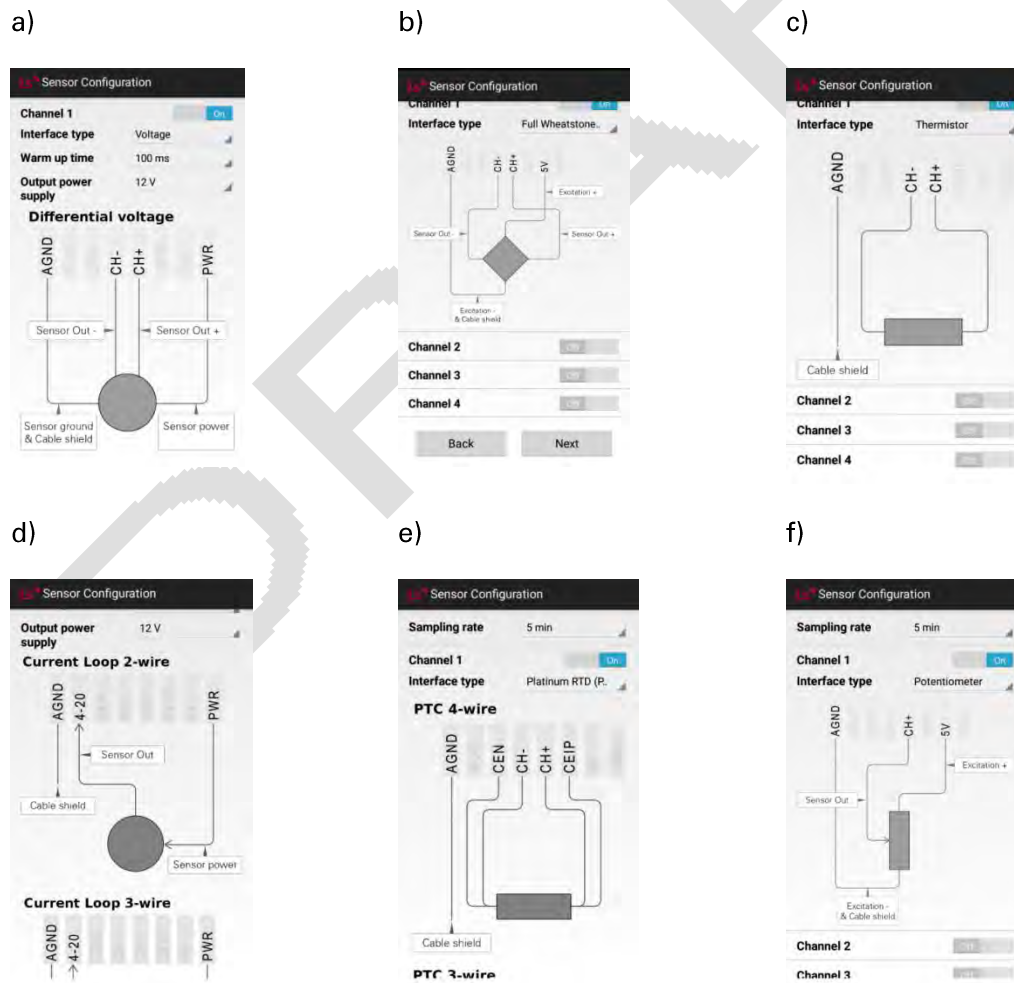


Figure 46: View of the wiring of the different types of analogue sensors, indicated in the Android Configuration App.

The datalogger can measure both voltage differential and single ended voltage sensors outputs. The standard wiring is for differential, and for single ended is needed to wire the negative input of the datalogger to datalogger ground.

The wiring can be connected once the Setup Wizard in the Android Configuration App has been initialized, and therefore when the wiring schemes appear.

3.3.2. Battery lifespan

The following table gives the indicative battery lifespan for channel (Table 6). User should take into account that consumption varies depending on the sensor used, the sampling rate and the environmental conditions.

Table 6: Indicative lifespan for LS-ANALOG datalogger. Estimations using 4 c-size cells

Number of sensors	Sampling rate			
	6 hour	1 hour	30 minutes	5 minutes
1 sensor Full Wheatstone Bridge/Thermistor/Potentiometer/PT100 @ 350ohms	>10 years	>10 years	8,5 years	1,5 year
1 sensor Voltage@12V@10mA	>10 years	9,4 years	4,9 years	10 months
1 sensor Current Loop @ 24V@24mA	>10 years	7,5 years	4 years	8 months
4 sensors Full Wheatstone Bridge/Thermistor/Potentiometer/PT100 @ 350ohms	>10 years	5,31 years	2,7 years	5,6 months
4 sensors Voltage@12V@10mA	>10 years	3,8 years	2 years	4 months
4 sensors Current Loop @ 24V@24mA	>10 years	2,2 years	1 year	2 months

3.3.3. Configuration

The configuration requires specifying the excitation power voltage and the warm-up time for the sensors that need power supply (voltage and current loop sensors). For the other sensors, 5V excitation supply is present in all channels connectors.

Excitation power voltage can be 12 V or 24 V, and warm-up times: 100, 300, 500 milliseconds or 1, 2, 5 seconds.

See section 2.3 for the configuration of the radio communications of the datalogger.

3.3.4. Data storage

Capacity for up to 130.000 readings with 4 sensors connected (Table 5).

Table 7: Indicative storage capacity of the LS-ANALOG datalogger. Estimations using 4 sensors.

Number of sensors	Sampling rate		
	60 minutes	30 minutes	10 minutes
4	more tan 10 years	7 years	2,4 years

4. WIRELESS RADIO

4.1. Maximum number of dataloggers connected in a network

The number of dataloggers that can be connected in a radio network is limited by the number of messages that can be transmitted over a period of time. All nodes in the network take their readings at a synchronized time (eg. if reading every 5 minutes, it's every hour, at minute 0,5,10,15 and so on.). These messages are then written to internal node memory, but are not transmitted immediately. The readings are transmitted to the gateway at a random time inside a communication slot (Figure 47).

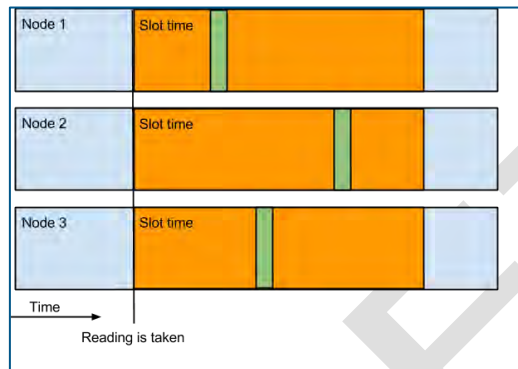


Figure 47: Summarized scheme of the data transmission over time in a LS-G6 network.

The length of the communication slot depends on the number of nodes in a network (Table 8), and is chosen automatically by the Android Configuration App when a node gets configured. There are also combinations of network size and sampling rate which are not supported. This is to prevent all nodes from sending at the same time and saturating the network.

Table 8: Slot times table. Columns are the number of nodes, rows are sampling rate. Slot times are in seconds.

	0-20	20-100	100-200	200-1000	1000-2000
10 seg	NO	NO	NO	NO	NO
30 seg	20	NO	NO	NO	NO
1 min	40	NO	NO	NO	NO
5 min	60	240	NO	NO	NO
15 min	60	600	600	NO	NO
30 min	60	600	900	NO	NO
1h	60	600	900	2700	NO
6h	60	600	900	2700	3600
12h	60	600	900	2700	3600
24h	60	600	900	2700	3600

Note that LS-DIG doesn't fulfill the slot times table (Table 8) because reading may take longer times than VW or ANALOG dataloggers.

4.2. Radio configuration

- Region and country: These values have to match the location where the dataloggers are deployed, in order to comply with the local regulations. There is a specific gateway model for each region, and the gateway must also be configured to the correct country. In order to achieve communication, the gateway and all the dataloggers on a network need to be configured in the same way.
 - Australian radio: The radio for Australia has some differences to the radios on other countries. On the rest of the countries, the gateway is always listening to all Spreading Factors, and on different frequencies. The datalogger can choose which SF and frequency to transmit on. On Australia, this is not possible. The gateway and all dataloggers must be configured to a Specific Spreading Factor and channel, which must be the same for all devices on the network. The default values are Channel 1, Spreading Factor 9, so these will be the values used if the Advanced options were ignored on both the Gateway and the Dataloggers.
- Network ID and password:
 - These values are used to identify a radio network, and to protect (encrypt) the data in transit. A strong password will prevent a malicious attacker from both reading data from your sensors and from inserting bogus data posing as a sensor.
 - The radio network ID is set by default to the gateway's serial number, but it can be changed. For example, if you are replacing a gateway, you might want to set the new gateway (with a new serial number) to the old gateway's network ID, so that the dataloggers don't have to be reconfigured.
 - The network password is set by default to a randomly generated value, which is printed on your Gateway Information sheet. The generated password is unique to each gateway unit, so it can be used safely.
 - In order to achieve communication, the gateway and all the dataloggers on a network need to be configured with the same network ID and password.
 - For security reasons, the network password cannot be read from a datalogger by the Dlog Android app. For this reason, when entering the radio configuration dialog, the password displayed is the last one that was set using this Android device.
- Advanced options:
 - (Europe only) ETSI limit duty cycle: The European Telecommunications Standards Institute (ETSI) defines a time limit during which a radio device may transmit on a given frequency over a 1-hour period. In some rare cases (high sampling rates on high SF), the datalogger may exhaust its radio time, and it will stop transmitting until next hour. This option can be disabled for testing purposes, or for use on places where the norm doesn't apply (eg. Inside a mine)
 - Maximum Spreading Factor: Defines the maximum spreading factor the datalogger is allowed to transmit to.
 - Lower spreading factors allow for faster data transmission, so more dataloggers can share the same radio space.

- Higher spreading factors allow for more reliable data transmission, allowing for longer distances and better immunity to interference.
- These are the maximum Spreading Factors allowed by the regulations:
 - Europe: SF 11
 - FCC: SF 9
 - Malaysia: SF 9
 - Australia: SF 11
- ADR (All countries except Australia): ADR (Adaptive Data Rate) is the mechanism which allows the datalogger to automatically negotiate the lowest viable spreading factor with the gateway. When the ADR is off, the datalogger will always use the highest SF (as set on the previous selector).
- Transmit power: Allows adjusting of the transmit power, in dB. The maximum allowed transmit power is specific to each country.
- Channel (Australia only): It's possible to choose between 4 different channels in Australia:
 - Channel 1: 921,9 MHz
 - Channel 2: 922,5 MHz
 - Channel 3: 923,7 MHz
 - Channel 4: 924,3 MHz
- Channel group (FCC only): In FCC mode, the radio will use frequency hopping on a group of 8 channels. You may want to use a different channel group in order to move away from interferences on specific channels. All devices on a network (the gateway and all dataloggers) must be set to the same configuration. There are 8 groups to choose from:
 - Group 0 (Channels 00-07) – 902,3 to 903,7 MHz
 - Group 1 (Channels 08-15) – 903,9 to 905,3 MHz
 - Group 2 (Channels 16-23) – 905,5 to 906,9 MHz
 - Group 3 (Channels 24-31) – 907,1 to 908,5 MHz
 - Group 4 (Channels 32-39) – 908,7 to 910,1 MHz
 - Group 5 (Channels 40-47) – 910,3 to 911,7 MHz
 - Group 6 (Channels 48-55) – 911,9 to 913,3 MHz
 - Group 7 (Channels 56-63) – 913,5 to 914,9 MHz

4.3. Results of signal coverage test

In section 2.3, the signal coverage tests are presented. There are several ways to get the results of the signal coverage tests:

- 1) Receiving the results of the signal coverage tests in the Android Configuration App (Figure 11).
- 2) They are also displayed geographically in the software of the gateway (Figure 48). In this case, your computer has to be connected to the Internet, to get the map. The position where the tests have been carried out is displayed with a specific symbol that related to the coverage at the specific point. The symbol selected (color legend) indicates the maximum SF from which >50% of the information packages sent by the datalogger have reached the gateway. In red, the places where ≤50% of the packages of SF 12 are indicated.
- 3) Moreover, the results of the signal coverage tests can be downloaded from the gateway in a .csv file (Figure 48, lower right corner). If the test is done "offline", the results only appear in this .csv.

Note that independently if the gateway has received the data from the tests, all the tests are saved in a .csv file inside the Android device (DLOG directory). Geographical data is also saved there (if GPS is activated in the Android).

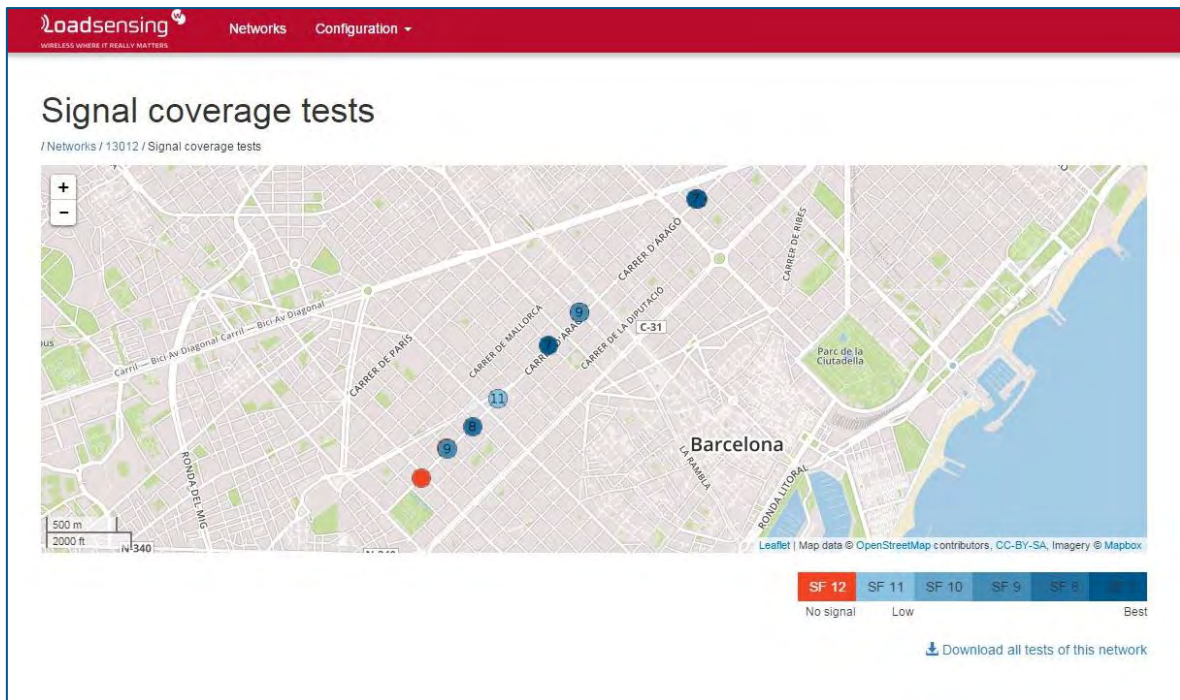


Figure 48: View of the geographical display (in the software of the gateway) indicating the results of the signal coverage tests.

5. CONTACT WORLDSENSING

Phone: +34 93 418 05 85 (08.30h - 16.30h UTC)

Technical support: support@worldsensing.com

General information: info@worldsensing.com

Worldsensing SL

Aragó 383, 4th

08013 Barcelona

(Spain)

DRAFT

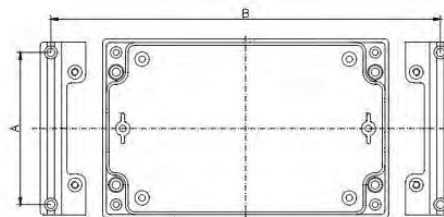
Annex 1: Details of mounting systems

Mounting brackets



External mounting brackets (set = 2 pcs.)
for mounting without opening the lid

Order No.	A	B	for Type	Order No.	A	B	for Type
04.00 00 80	65	92	04.08 08 08	04.00 01 40	125	152	04.14 14 07
04.00 00 80	65	132	04.08 12 08	04.00 01 40	125	192	04.14 18 07
04.00 01 00	85	112	04.10 10 06	04.00 01 40	125	232	04.14 22 07
04.00 01 00	85	172	04.10 16 06	04.00 01 60	145	172	04.16 16 08
04.00 01 00	85	212	04.10 20 06	04.00 01 60	145	252	04.16 24 08
04.00 01 20	105	132	04.12 12 08	04.00 02 00	185	212	04.20 20 07
04.00 01 20	105	172	04.12 16 08	04.00 02 00	185	292	04.20 28 07



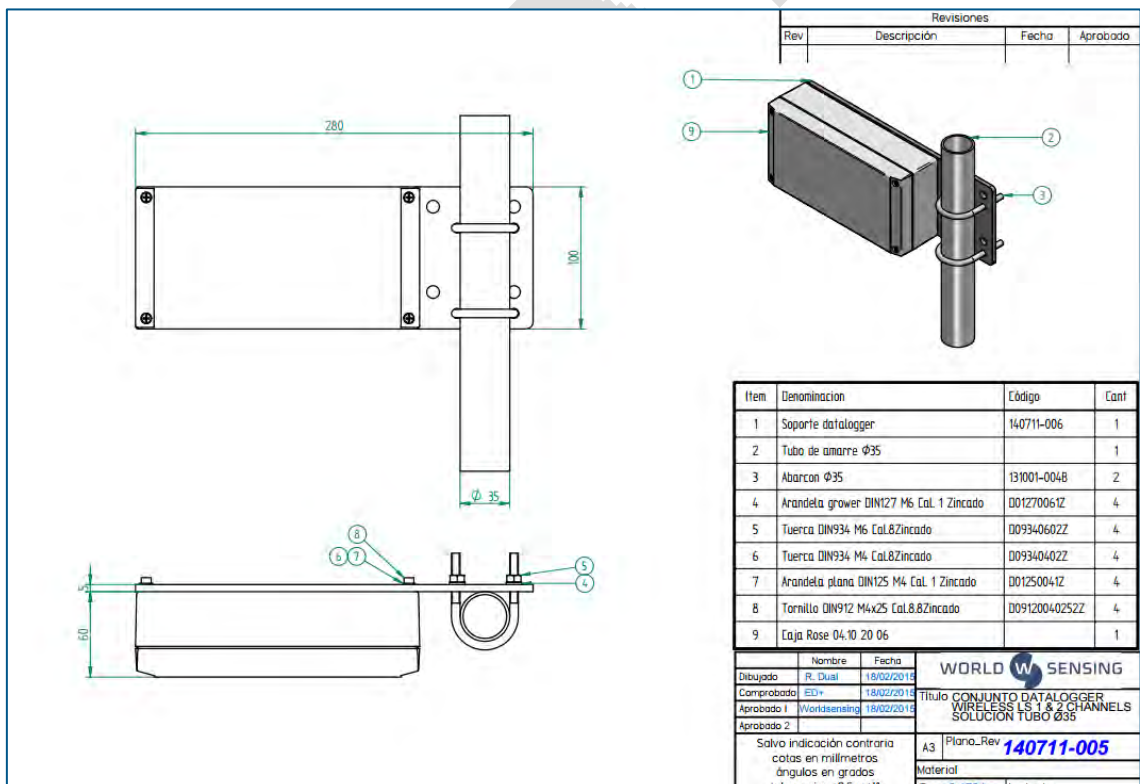
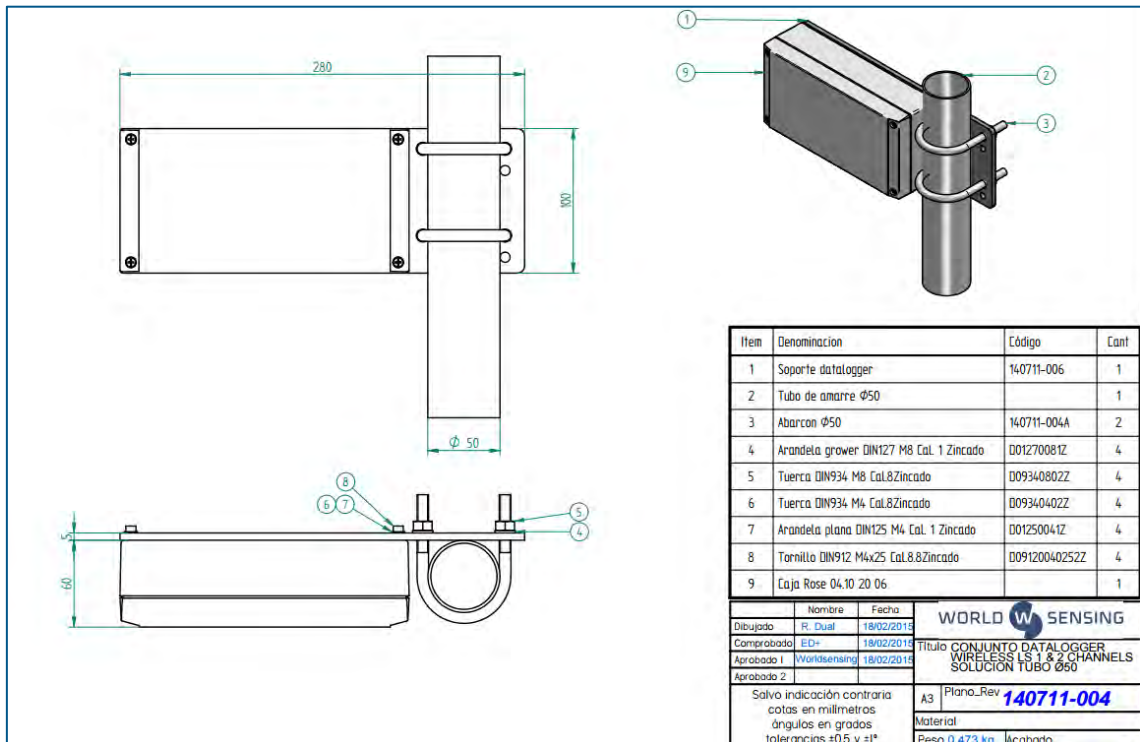
Strong magnets

Revisiones			
Rev	Descripción	Fecha	Aprobada

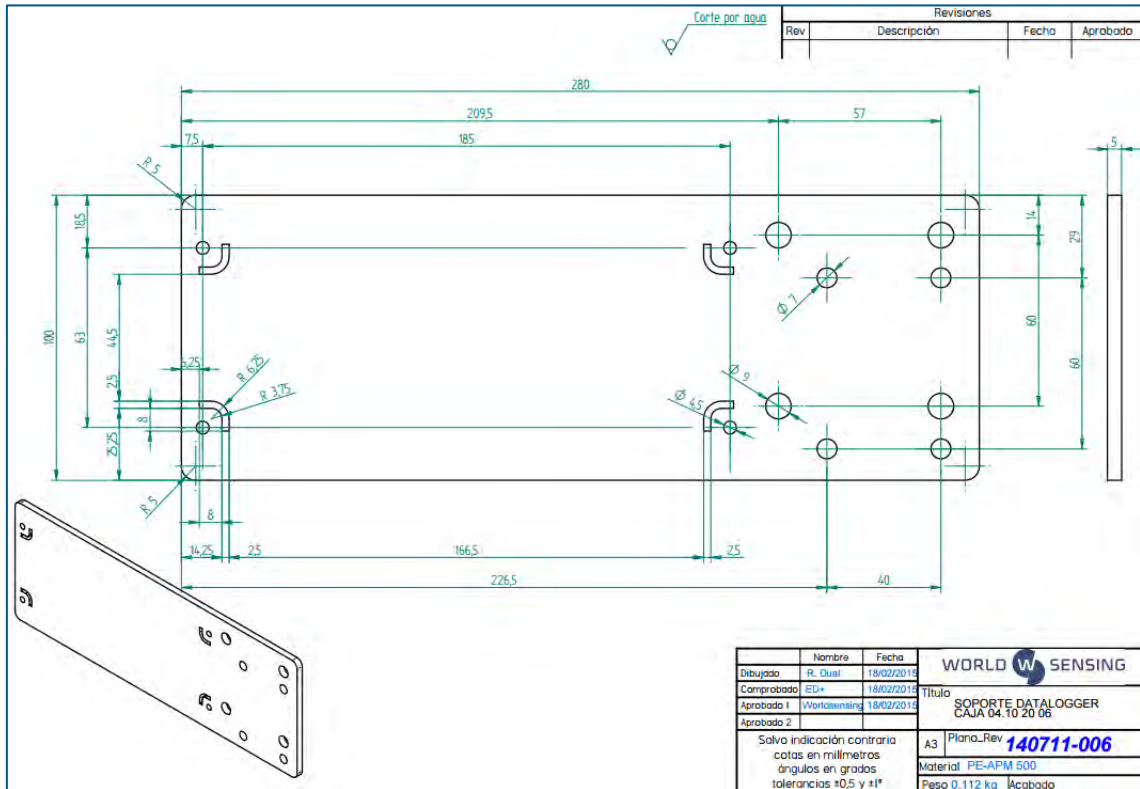
Item	Denominación	Código	Cant
1	Caja Rose 04.10 20 06		1
2	Tornillo DIN912 M4x15 Cal.8.8Zincado	D0912004015Z2	4
3	Iman roscado SUPERMAGNETE ITNG-16	ITNG-16	4
4	Arandela de caucho Ø12/Ø4 x 2	SAR00400120	4

Nombre	Fecha	WORLD SENSING
Dibujado: R. Duil	12/05/2019	Título CONJUNTO DATALOGGER WIRELESS LS-1 & 2 CHANNELS SOLUCIÓN IMANTADA
Comprobado: ED+	12/05/2019	
Aprobado 1: Workstermink	12/05/2019	
Aprobado 2:		
Salvo indicación contraria cotas en milímetros ángulos en grados tolerancias ±0,5 y ±1°		A3 Plano_Rev 140711-007 Material Peso 0,473 kg Acabado

Pole mounting



LS-G6 USER GUIDE V1.5



Annex 2: Android compatibility

The Android Configuration app specifically developed to connect locally with the LS-G6 (LS-G6) dataloggers, allowing configuration, data display and download. This document provides the basic information to know which Android devices are compatible with the LS-G6 dataloggers, and the USB cable that must be used for this local connection.

To download the Android Configuration App in your Android device, go the following link: <http://wsop.cat/industrial/dlog/Dlog.apk>. Information on how to use the application can be found in the LS-G6 user guide.

In order to be compatible with the LS-G6 dataloggers, an Android device must have the following specifications: USB on the go (OTG) + Android at least 3.1. From early 2013 most of the Android devices on the market fulfill these requirements. To check if your Android device includes the USB OTG feature, just search in the web "<model of the smartphone> specifications USB OTG" and ensure that the Android version is at least 3.1 (API version 12). Some Android devices may have the USB OTG feature locked. An example of unlocking process for Samsung SIII mini can be found in this tutorial: <https://www.youtube.com/watch?v=JevEyrilXZ0>.

The connection between the LS-G6 datalogger and the Android device is done with "USB on the go" cable (OTG). This cable allows an Android device to act as "master", meaning that other devices can be controlled from it. The LS-G6 dataloggers have a mini USB connection, while most Android devices have a micro USB connection. In order to connect the Android device to the datalogger an USB OTG cable from micro USB to mini USB is needed.

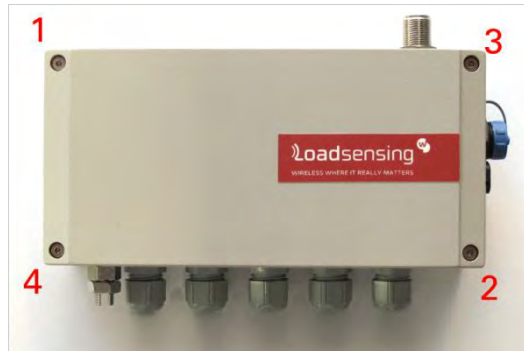


Annex 3: LS-G6 water tightness

The LS-G6 family of dataloggers from Worldsensing Industrial (WSI) are rated IP67. The dataloggers can also pass the IP68 tests for extended immersion (1 meter for 3 days) if the installer uses extreme caution.

To ensure this condition, the user should be sure that:

- After sensor connection, the box is closed following a cross-shape order.



- The box is screwed at 2 Nm, using a torque screwdriver (e.g. Ref. 1227107 from WERA)
- The cable glands are closed using a 19 mm open spanner (e.g. Bahco 19 mm Single Ended Open Spanner; RS Amidata code 717-8992) (holding the internal nut using a 22 mm open spanner (e.g. Bahco 22 mm Single Ended Open Spanner; RS Amidata code 717-8995)).
- The antenna is mounted. If it is not, the antenna connector should be covered with a cap.
- The sealing ring is not manipulated, neither physically or chemically.

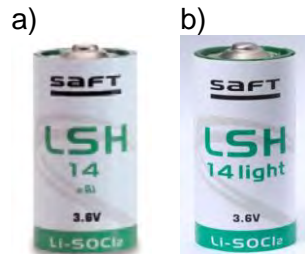
If any of these conditions are not given, or if one or several components (e.g. gore valve) are damaged, the IP67 and superior are not guaranteed.

In case that it is required that the datalogger is further sealed because it is going to be placed in a very harsh environment or in an floodable manhole, additional sealants would be required to close the box (e.g. Sikaflex products).

Annex 4: Recommended batteries

LS-G6 can work with only one cell battery or more than one (up to four). As much batteries are used, the longer the autonomy is.

The recommended batteries are LSH 14 models from Saft.



This equipment can work with only one cell of specified battery in the next link. (Saft model). More paralleled batteries increase the node autonomy.

If another model of battery is required it must to meet the same specifications than saft batteries. Typical issues will be:

- Cell voltage: must be at least 2,7V to 5V
- Cell continuous current: Must be high current from 500 mA to 1 A

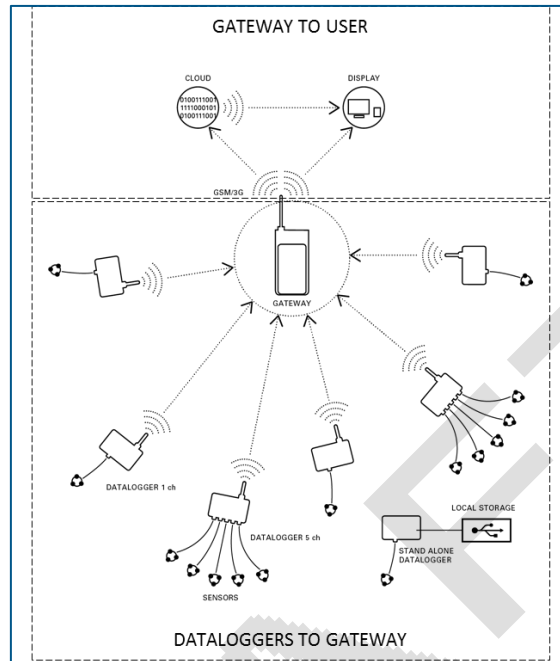
Cell voltage and continuous current change with temperature. Previous specs must to be checked in the desired temperature range. Also common batteries (alkaline) doesn't work on extreme temperatures.

WARNING: RISK OF EXPLOSION IF THE BATTERIES ARE SUBSTITUTED FOR AN INCORRECT MODEL. DISPOSE OF THE BATTERIES ACCORDING TO THE INSTRUCTIONS. THIS EQUIPMENT IS MEANT TO BE INSTALLED IN RESTRICTED ACCESS AREAS.

Annex 5: Communications security

Long range radio communication from dataloggers to gateway

This part explains the security of the radio communication from dataloggers to gateway.



Security

Each LS radio network uses an own identifier and password. The ID and password provide authentication and encryption to all radio communications within the network. This means this ID and password are set on both the gateway and the dataloggers (via the USB Dlog Android app). By default, the gateway comes with a randomized password.

Encryption

The radio network has a special need for secure communication, as many of its applications imply critical data of key infrastructures. This has been solved applying three encryption layers:

- Unique Network key ([EUI64](#)) at network level.
- Unique Application key ([EUI64](#)) at application level.
- Network specific key to encrypt all data using [AES-128](#) (AES-EUI128).

Gateway user access

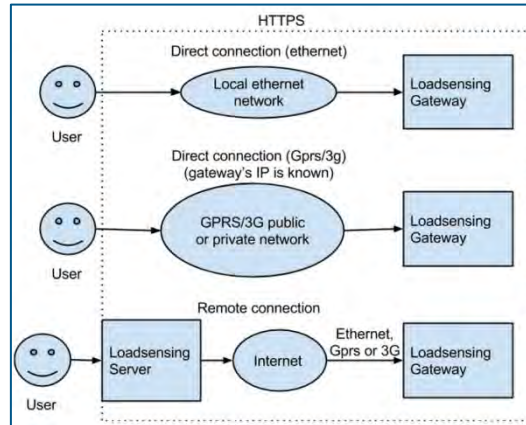
This part explains how the communication between the user and the gateway is secured.

Remote access

This is the method used to access the gateway over the internet or a local network. The gateway has two interfaces integrated for remote access:

- Ethernet interface
- 3G/GPRS interface

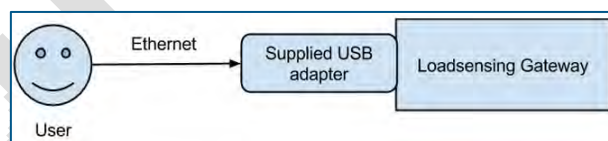
Both interfaces use HTTPS protocol for secure communication, and both interfaces use the remote access password. This password is unique and is randomly generated at production: it can be changed by the user using the gateway administration web. The different methods for remote access to the gateway (for more information please refer to the LS-G6 user guide) are shown here:



Local administration

The gateway offers the possibility of direct local connection, using gateway's internal USB port (for more information please refer to the LS-G6 user guide). When accessed by this method, the connection is also secured using https. However, this connection will ask for a password which is not unique (is the same for all gateways). This is done taking two important considerations into account:

- A direct recovery method of the data is needed if remote access password is lost.
- The gateway cannot be physically reached by users other than the customer.



Note: If your gateway is located where it might be physically accessed by alien users, please contact Worldsensing technical support.

Data protection and communications security is highly emphasized in Worldsensing's products:

- The radio communication from the dataloggers to the gateway is encrypted with AES.
- All remote communications to allow user's access to the gateways are done with https protocols.

Both security methods are proved standards applied in all industries, from bank transactions to most accessed internet services.

Annex 6: Troubleshooting reference table

Gateway

Fault	Possible cause	Remedy
Gateway not visible via 3G/GPRS	Poor signal	Move location
Gateway not visible via 3G/GPRS	No SIM card	Insert SIM card
Gateway not visible via 3G/GPRS	SIM configuration problem	Contact service provider
Gateway not visible via 3G/GPRS	SIM pin code on	Disable SIM pin or change configuration 3G/GPRS by local connection
Gateway not visible via 3G/GPRS	No power supply	Check/connect power supply.
Gateway not visible via 3G/GPRS	Gateway not configured to 3G/GPRS	Configure to 3G/GPRS by local connection
Gateway not visible via 3G/GPRS	Network configuration	Check firewalls, Routing, IPs
Gateway not visible via 3G/GPRS (gateway software version prior to 1.9.1)	Application frozen	Reboot the gateway: https://loadsensing.wocs3.com/XXXX/reboot.htm
Gateway not visible via Ethernet	Cable	Check Ethernet cable
Gateway not visible via Ethernet	No power supply	Check/connect power supply. Check board LEDs
Gateway not visible via Ethernet	Network configuration	Check firewalls, Routing, IPs
Gateway not visible via Ethernet	Gateway not configured to Ethernet	Configure to Ethernet by local connection

"Internal server error" is displayed on the browser (gateway software version prior to 1.9.1)	Application frozen	Reboot the gateway: https://loadsensing.wocs3.com/XXXX/reboot.htm
---	--------------------	--

Dataloggers

Fault	Possible cause	Remedy
Datalogger not visible to Gateway	Datalogger isolated/not visible for anyone	Move location
Datalogger not visible to Gateway. Cannot be accessed with Dlog unless switch is set to "USB".	Datalogger battery is dead	Check battery
Datalogger not visible to Gateway	Radio configuration	Check radio configuration using DLOG. Check carefully that the radio configuration is the same on all devices.
Datalogger not visible to Gateway	Antenna	Check connection & orientation
Datalogger not visible to Gateway	Gateway	Check Gateway is UP
Datalogger not visible to Gateway	Gateway antenna	Check connection & orientation

CONFORMITY ASSESSMENT ISSUES

FCC/IC Regulatory notices

Modification statement

Worldsensing, S.L. has not approved any changes or modifications to this device by the user. Any changes or modifications could void the user's authority to operate the equipment.

Worldsensing, S.L. n'approuve aucune modification apportée à l'appareil par l'utilisateur, quelle qu'en soit la nature. Tout changement ou modification peuvent annuler le droit d'utilisation de l'appareil par l'utilisateur.

Interference statement

This device complies with Part 15 of the FCC Rules and Industry Canada's licence-exempt RSS standards. 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.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables 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.

Wireless notice

This equipment complies with FCC and ISCED radiation exposure limits set forth for an uncontrolled environment. The antenna should be installed and operated with minimum distance of 20 cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Cet appareil est conforme aux limites d'exposition aux rayonnements de l'ISDE pour un environnement non contrôlé. L'antenne doit être installée de façon à garder une distance minimale de 20 centimètres entre la source de rayonnements et votre corps. L'émetteur ne doit pas être colocalisé ni fonctionner conjointement avec à autre antenne ou autre émetteur.

Permitted Antenna

This radio transmitter LS-G6-VW has been approved by FCC and ISCED to operate with the antenna types listed below with the maximum permissible gain indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Type	Max Gain
AR017 GSM Quad Band Antenna (WellShow)	3 dBi

Le présent émetteur radio (identifier le dispositif par son numéro de certification) a été approuvé par ISDE pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Type	Gain maximal
AR017 GSM Quad Band Antenna (WellShow)	3 dBi



FCC Class B digital device notice

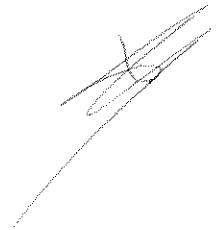
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate 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 a particular 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 try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into 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.

CAN ICES-3 (B) / NMB-3 (B)

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de classe B est conforme à la norme canadienne ICES-003.

A handwritten signature or mark, possibly a stylized 'A' or 'S', located in the bottom right corner of the page.