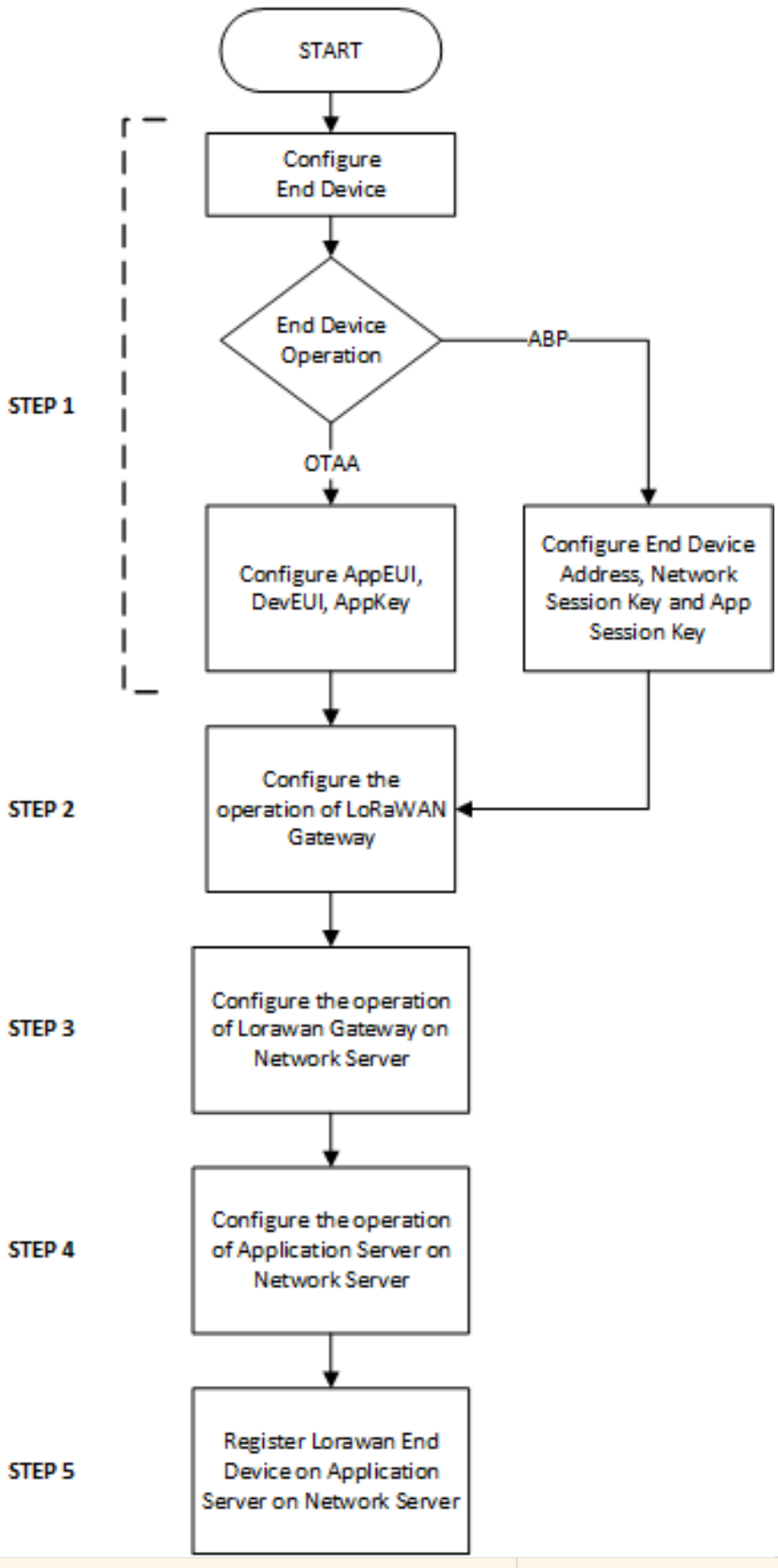
USER GUIDE FOR LORAWAN SENSOR WSLRW

WSLRW-MN-EN-01	DEC-2023

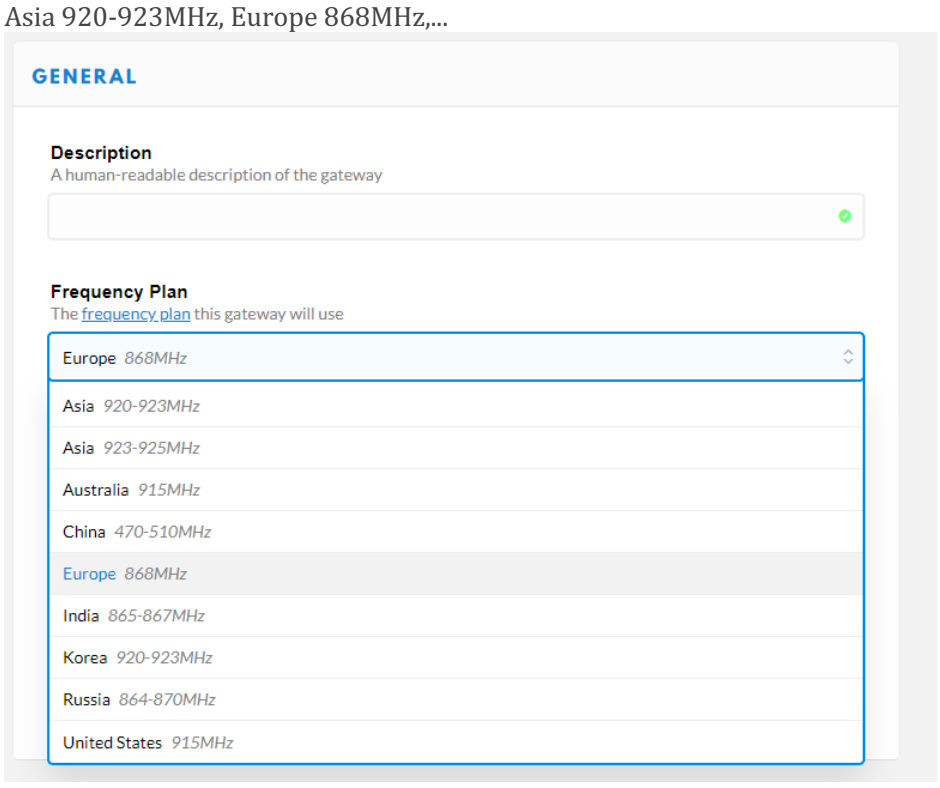
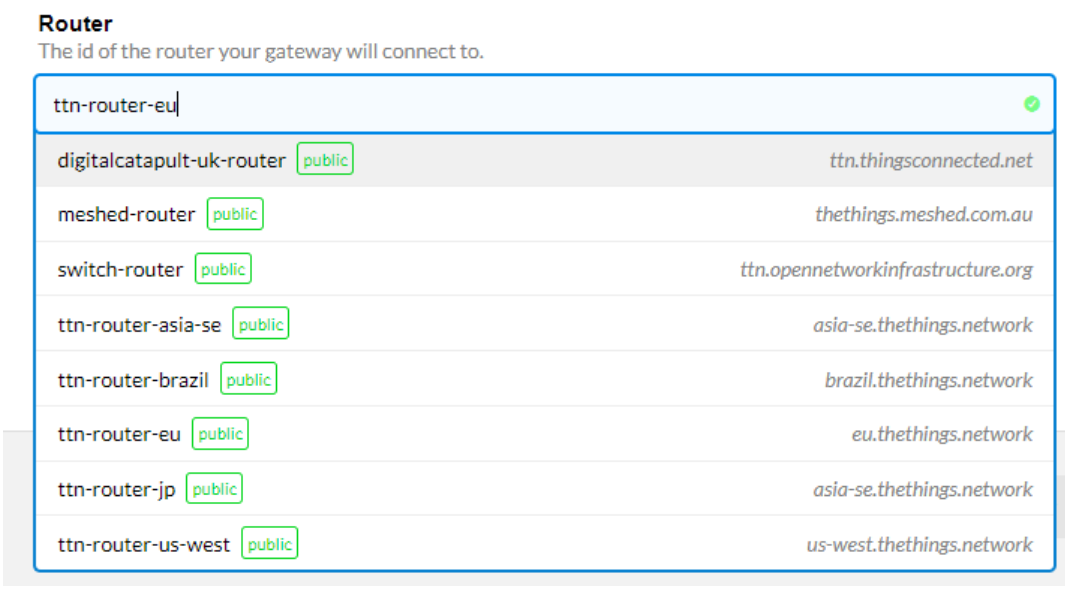
This document is applied for the following products

SKU	WSLRW				

1. Configuration Check List



STEP 1: Configure End Device (Using Modbus Configuration Cable)	**Setting value (Example)**
1. Select region	AS923, IN865, EU868,.. (refer to register address **317**)
2. End Device Operation	OTAA or ABP
• ○ OTAA	1. Write AppEUI information from Application Server to Lorawan End Device; 2. Write AppKey (created by user) information for Lorawan End Device and Application Server.
• ○ ABP	1. Write DevEUI information from Application Server to Lorawan end device;

	2. write Network Session Key and App Session Key (created by user) information to Lorawan end device (and Application Server).
3. Configure "cycle send data"	900 sec (Defaut)
4. Configure "sensor sampling rate"	120 sec (Defaut)
5. Configure parameters of sensor	**(Refer to Check data configuration table)**
STEP 2: Configure the operation of LoRaWAN Gateway	**(Ex: URSALINK Gateway)**
1. Configure the information in the General tab	Server address, Server port **(For more information)**
2. Configure the information in the Radio tab	Select the Region Region (Other parameters to default)
STEP 3: Configure the operation of LoRaWAN Gateway on Network Server	**(Ex: URSALINK Gateway with Thethingsnetwork)**
1. Gateway ID registration	Gateway ID is the GatewayEUI information on the Gateway
2. Frequency Plan parameters configuration	Asia 920-923MHz, Europe 868MHz,... 
3. Router parameters configuration	
4. Check the connection of the gateway to the network server	The Gateway status LED lights up and displays the message "Status: conneted" on the Thethingsnetwork
STEP 4: Configure the operation of Application Server on Network Server	
1. App ID registration	
2. Handler parameters configuration	
STEP 5: Register Lorawan End Device on Application Server on Thethingsnetwork	
1. ID Registration	
2.Select operation mode	OTAA or ABP

• ○ OTAA	Configure parameters DevEUI and AppKEY
• ○ ABP	Configure parameters Device Address, Network Session Key, App Session Key

2. Introduction

WSLRW is LoRaWAN Sensor that support multiple sensor types via I2C, SPI, UART... input signal. With Ultra-low Power design and smart firmware allow the sensor can last up to 10 years with 02 x AA-type battery (depends on configuration). The sensor will transmit data in kilo-meters distance to LoRaWAN gateway, any brand on the market.

FCC Warning

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: 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.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

3. Specification

Sensor Input	I2C, SPI, UART, Digital Input 0-3.3V, Analog input 0-3V
Data rate	250bps .. 5470bps
Antenna	Internal Antenna 2.0 dbi
Battery	02 x AA size 1.5VDC, battery not included
RF Frequency and Tx Power	US915, max +20 dBm Tx
Protocol	LoRaWAN, class A
Data sending modes	interval time, alarm occurred and manually triggering by magnetic key
Working temperature	-40oC..+60oC
Dimensions	H106xW73xD42
Net-weight	190 grams
Housing	Aluminum + Polycarbonate plastic

4. Operation Principle

4.1 LoRaWAN protocol specifications

4.1.1 LoRaWAN Sensor protocol specifications

- LoRaWAN Protocol Version 1.0.3
- Application Server Version 1.3.0.0
- MAC Layer Version 4.4.2.0
- Radio Standards: LoRa Alliance Certified
- LoRaWAN Zone: US915
- Class A
- Join Active: OTAA / ABP
- Network Mode: Public Network / Private Network
- Tx Power: up to 20 dBm
- Spreading factor: SF10 - SF7
- Bandwidth: 125 kHz
- Unconfirmed-data message
- LoRaWAN application port for certification: 224

4.1.2 Data rate of LoRaWAN Sensor

Data rate name	Data rate (bps)	Spreading factor (SF)	Bandwidth (kHz)	Region
DR0	980	SF10	125	US915
DR1	1760	SF9	125	
DR2	3125	SF8	125	
DR3	5470	SF7	125	

4.1.3 Tx power of LoRaWAN sensor

Max EIRP (dBm)	Max Tx Power (dBm)	Region
30	20	US915

4.2 The principle of operation of the LoRaWAN sensor

When starting the power supply, the LoRaWAN sensor has 60 seconds to allow configuration to operate via the Configuration Cable with the Modbus RTU protocol. After 60 seconds, the first packet will be sent, then the LoRaWAN sensor will send the next packets in the following cases:

- **Case 1:**
  - When it reaches the frequency of taking data, the LoRaWAN sensor will wake up to measure and calculate. Then:
    - If the measured value exceeds the High or Low setting thresholds, the packet will be sent to the Gateway and then asleep;
    - If NOT then sleep without sending data.

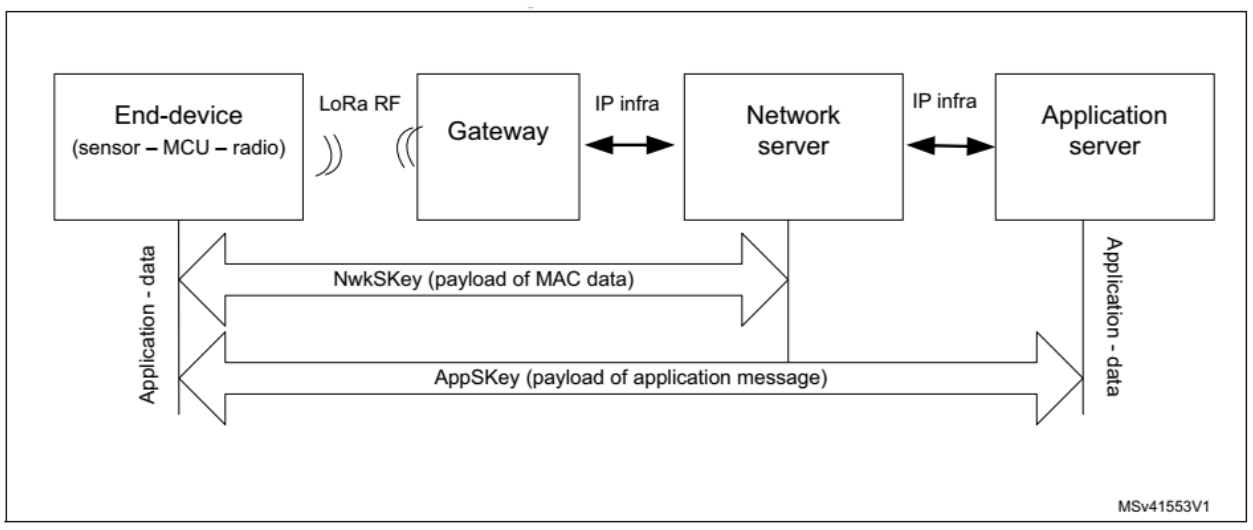
> **NOTE:**
>
> Once sending the data to Gateway by this alarm event, the timer of sending time interval will be reset;

- **Case 2:** When the sending time interval is reached, the LoRaWAN sensor wakes up to measure and calculate and send data to Gateway immediately, regardless of value.
- **Case 3:** By using the magnet key, the LoRaWAN sensor can be triggered to send data to Gateway immediately.

NOTE:

The time between sending data for Class A is at least 3 seconds

4.3 Principle of operation LoRaWAN Network



The LoRaWAN Gateway function is Packet Forwarder so:

- **Between Gateway and End Device:** Gateway receives data packets from End Device via RF connection, so it is recommended to configure Radio parameters (**Note:** the packet that Gateway receives is encrypted)
- **Between Gateway and Network Server:** Gateway forwards data packets to the Network server via an IP connection, so it is recommended to configure Network parameters such as Server Address, Server Uplink Port, Server Downlink Port,...

LoRaWAN Network is secured as follows:

- Network section key (NwkSKey) to ensure the security of communications on the Network
- The application session key (AppSKey) to ensure data security between End Device and Application Server
- Special keys of the device such as DevEUI, AppEUI, Gateway EUI, Device Address. *Therefore, the data packet that the Gateway receives is encrypted and decrypted on the Application server.*

To End Device connect to the Network server, you need to register in the following two ways:

- **Activation with OTAA (Over-the-Air activation):** is the process of joining the Network automatically. Previously, both End Device and Application Server installed the same DevEUI code, AppEUI, and AppKey. During activation, AppKey will generate 2 security keys for End Device and Network, which are:

    - The network session key (NwkSKey): is the key to secure communication commands on the MAC layer between the End Device and the Network server.
    - The application session key (AppSKey): is the key to secure data packets between the End Device and Application server.

ATTENTIONS:

** OTAA mode must be successfully activated in order for the End Device to send data packets to the Network through the Gateway;*

** OTAA mode only need to activate once, if the device is reset or battery replacement, it will activate OTAA again;*

** When the End Device is connected to the Network server, whether the Gateway is reset or the power is restarted, it will not need to activate OTAA.*

- **Activation by ABP (Activation by Personalization):** is the process of joining the Network manually. Device Address, Network session key (NwkSKey), and Application session key (AppSKey) codes must be stored inside the End Device and Application server, so when the End Device sends data packets to the network server, it will also send the security codes to activate.

4.4 Configure the LoRaWAN Network

4.4.1 Configure End Device operation according to OTAA

Configuration parameters for the End Device to be activated by OTAA as the table below:

Parameter settings	Setting value (example)	Description
Join Mode	OTAA	Device activation type on Network Server
DevEUI	34 35 31 31 4B 37 75 12	Device ID's unique ID number => Set this ID number for the Application server
AppEUI	70 B3 D5 7E D0 02 D5 0B	Application server's unique ID number (random or user-generated) => Set this ID number for End Device
AppKey	2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C	Key Number for generating 2 NwkSKey and AppSKey security keys created by the user (factory-created by default) => Used to install for both the Device and Application Server End

ATTENTIONS:

** The AppEUI number from Application Server => then installed for the End Device. AppEUI is randomly generated by the Application server or by the user;*

** The number of AppKeys during OTAA activation will generate two security keys, Lora NwkSKey and AppSKey, which are used for both End Device and Network.*

4.4.2 Configure End Device operation according to ABP

Configuration parameters for the End Device to be activated by ABP as the table below:

Parameter settings	Setting value (example)	Description
Join Mode	ABP	Device activation type on Network Server
Device Address	12 34 56 78	End Device Address created by the Application server => Set Device Address for End Device
NwkSKey (Network session key)	2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C	NwkSKey number created by the user to install and use for both End Device and Application Server
AppSKey (Application session key)	2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C	AppSKey number generated by the user to install for both End Device and Application Server

4.5 LED meaning

- RED LED:
  - **Fixed ON:** due to noise caused peripheral components (i2c, spi, uart, timer, rtc, wdt, ...) do not initialize.
  - **Flashing 10ms ON / 10s OFF:** Activation by OTAA on the Network server failed.
  - **Flashing 10ms ON / 2s OFF:** Sending a data packet to Gateway failed.
- GREEN LED: Flashing 100ms ON / OFF when sending a data packet to Gateway.
- BLUE LED:
  -
  - **Flashing 1s ON / 1s OFF** for the first 60 seconds when booting (insert batteries or connected external sources), after 60 seconds OFF.
  - **ON** during the LoRaWAN sensor receives data packets from the Network server and **OFF** when received.

4.6 Process of measurement

When the LoRa sensor wakes up, it will supply power to the internal or external sensor so that the sensor can start measuring. After measuring successfully it will turn off the power to the sensor for energy saving.

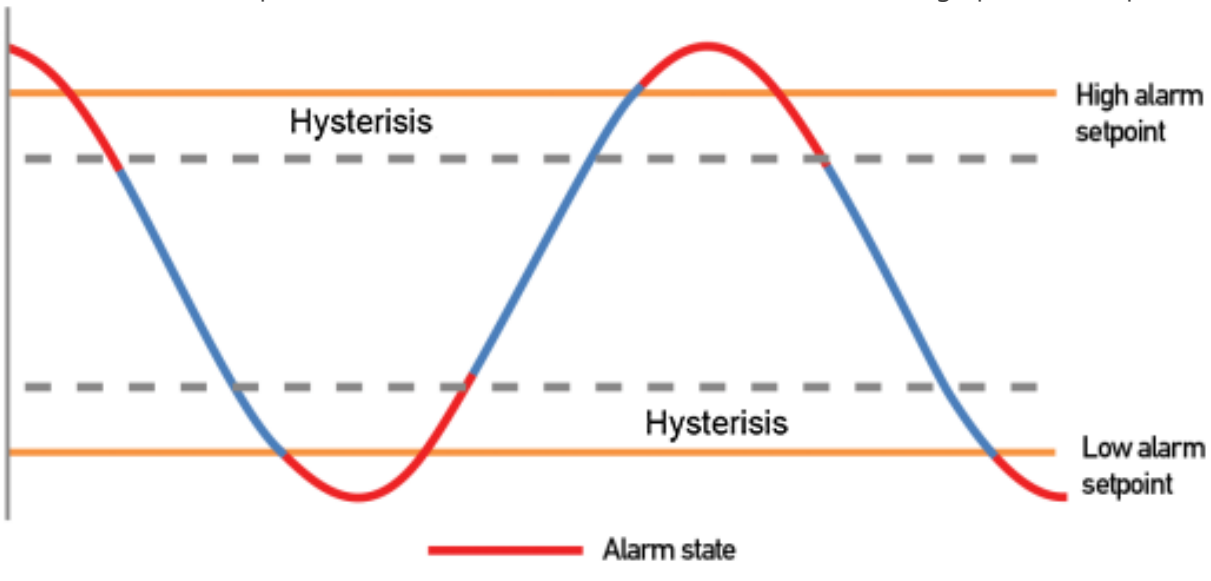
The measured value is the raw value of the sensor. The measured value can be scaled according to the following formula:

$$Y = aX + b$$

-
  -
    -
      -
      - **X:** the raw value from the sensor

- **Y:** the calculated value will be sent to LoRaWAN Gateway in the payload data.
- **a:** constant (default value is 1)
- **b:** constant (default value is 0)

So, if there is no user setting for **a** and **b** ==> **Y** = **X**
The **Y** value will be compared with Lo and Hi threshold. Please refer below the graph of alarm processing.



4.7 Payload Data

The following is the format of payload data that will be sent to the LoRaWAN Gateway.

Sensor type (1 byte)	Status1 (1 byte)	Status2 (1 byte)	1st - Parameter (Int16)	2nd - Parameter (Int16)	3rd - Parameter (Int16)

Meaning of Data in the Payload

Data	Size (byte)	Bit	Format	Meaning
Sensor type	1	all	Uint8	Sensor type = 0x0D means LoRaWAN Tilt Sensor. Sensor type = 0xFF means no sensor
Status1: battery level	1	Bit 7 and 6	Uint8	Battery capacity in 04 levels 11: battery level 4 (99%) 10: battery level 3 (60%) 01: battery level 2 (30%) 00: battery level 1 (10%)
Status1: error		Bit 5 and 4		Node status 01: error 00: no error
Status1: alarm 1		Bit 3 and 2		Alarm status of 1st - Parameter (X Tilt value) 11 : Hi alarm 01 : Lo alarm 00 : No alarm
Status1: alarm 2		Bit 1 and 0		Alarm status of 2nd - Parameter (Y Tilt value) 11 : Hi alarm 01 : Lo alarm 00 : No alarm
	1	Bit 7 and 2	Uint8	Not Applicable
Status2: alarm 3		Bit 1 and 0		Alarm status of 3rd - Parameter (Z Tilt value) 11 : Hi alarm 01 : Lo alarm 00 : No alarm
1st - Parameter	2	all	Int16	Measured value 1
2nd - Parameter	2	all	Int16	Measured value 2
3rd - Parameter	2	all	Int16	Measured value 3

5. Configuration

Using the configuration cable to connect to the sensor as below picture.

Serial port configuration on the computer:

* COMPort, Baudrate: **9600**, Parity: **None**, Stop bit: **1**, Data bit: **8**

* Modbus RTU: Reading data by **Function 3** / Writing data by **Function 16**.

5.1 Step to configure

NOTE:

The Modbus configuration can only be performed in the first 60s after power up the LoRaWAN sensor. After 60s, if user can not finish the configuration process, user need to reset the power of LoRaWAN sensor again, by removing battery in at least 15s.

Step 1: Install the Modbus Configurator Software in the link below

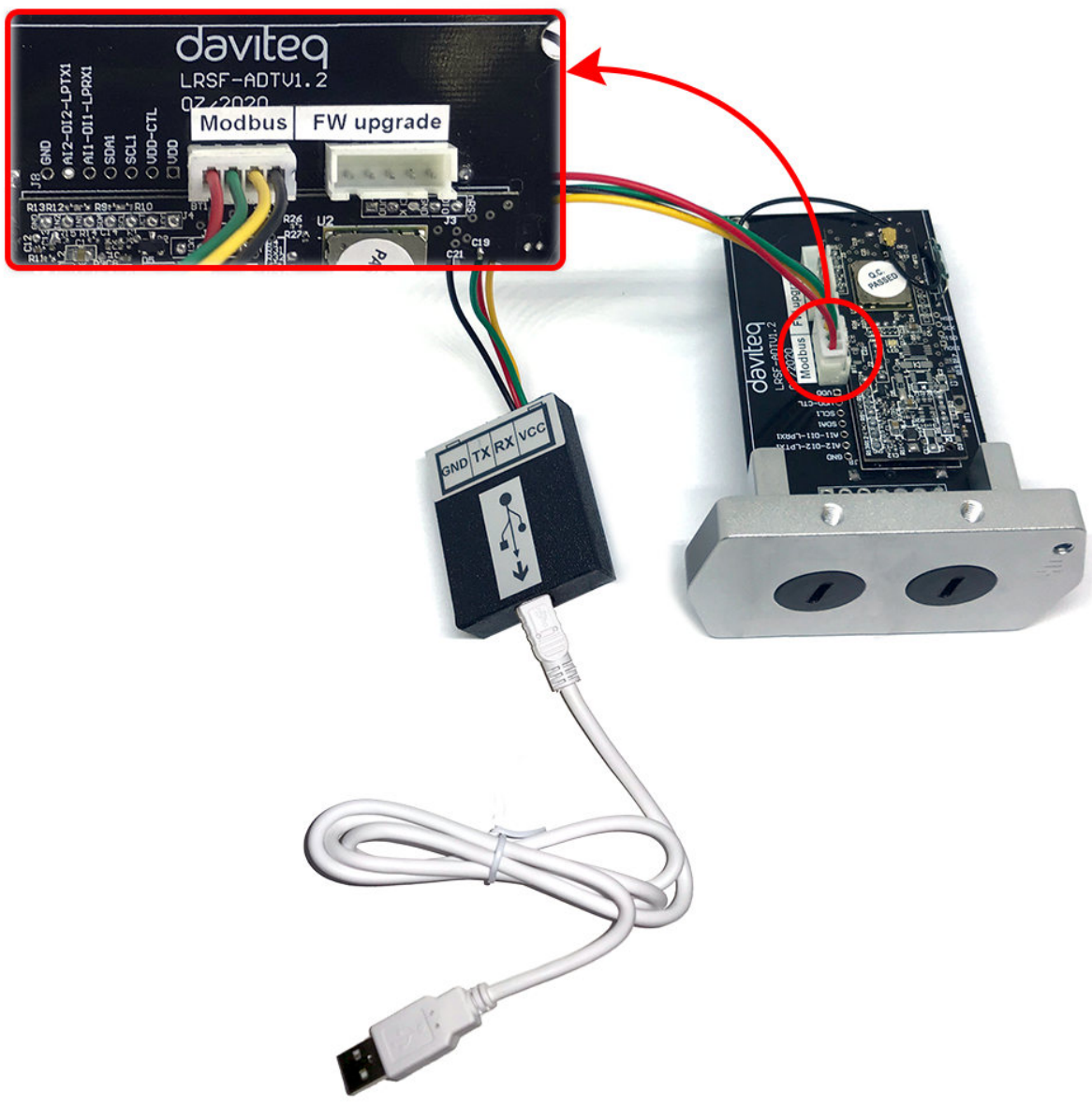
https://filerun.daviteq.com/wl/?id=qK0PGNbY1g1fuxTqbFW9SXtEvCw7bpc6

How to use the Modbus configuration software

Step 2: Plug the configuration cable to computer via USB port and install the driver;

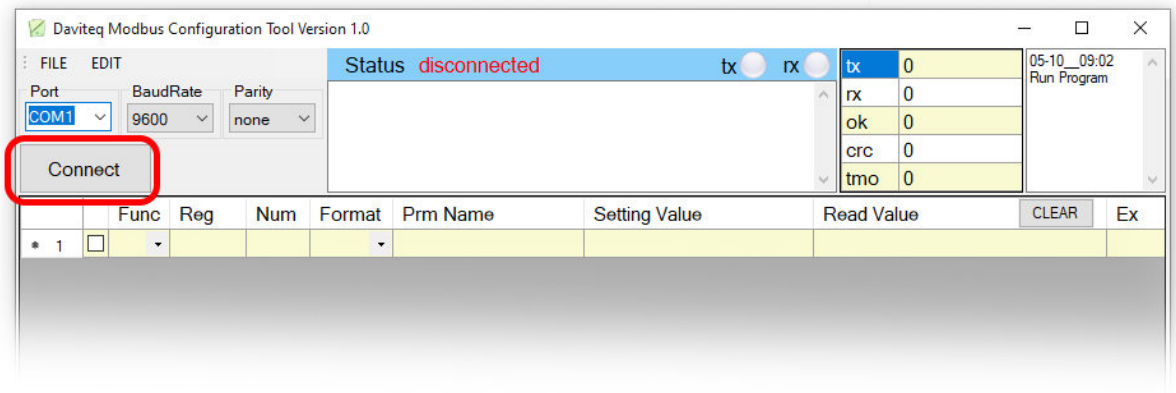
Step 3: Open the plastic housing with L hex key to unscrew M4 screws at the side of the housing

Step 4: Plug the connector to the configuration port;



Step 5: Import the configuration file by importing the csv file: Go to MENU: **FILE / Import New /** => select the file with name CONFIGURATION TEMPLATE FILE FOR LORAWAN SENSOR FW1.0.csv (in the link below). Then click **Connect**;

CONFIGURATION TEMPLATE FILE FOR LORAWAN SENSOR FW1.0



> **To write new value to the device:**
>
> First, you need to write the password in "password for setting", after reading the value to check ok, you can write the new value AppEUI, AppKey, ...
>
> You only have 60 seconds after plugging the configuration cable or the power supply into the device for configuration.

5.2 Register table

Here is the table of Data will be read by Modbus tool

Modbus Register (Decimal)	Modbus Register (Hex)	Function Code	# of Registers	Description	Range	Default	Format	Property	Comment
0	0	3	5	device info		WSLRW-I2C	string	Read	Wireless Sensor LoRaWAN - I2C
5	5	3	4	firmware version		1.00ddmm	string	Read	ddmm = day / month
9	9	3	2	hardware version		1.10	string	Read	
11	B	3	4	lorawan protocol version		01.00.03	string	Read	lorawan v1.0.3
15	F	3	6	application version		01.03.00.00	string	Read	application server v1.3.0.0
21	15	3	6	mac layer version		04.04.02.00	string	Read	mac layer v4.4.2.0
27	1B	3	4	deviceEUI			hex	Read	End Device's EUI number, used to register the product on the Network Server by OTAA
31	1F	3	4	lora appEUI			hex	Read	Application server's EUI number is used to register the product on the Network Server by OTAA
35	23	3	8	lora appKey			hex	Read	The number of keys used to create two security keys of the End Device, used to register the product on the

									Network Server by OTAA
43	2B	3	8	lora nwkSkey			hex	Read	key number encrypts the communicatio n command of the MAC layer of the End Device, which is used to register the product on the Network Server by ABP
51	33	3	8	lora appSkey			hex	Read	End Device data encryption key number, used to register the product on the Network Server by ABP
59	3B	3	2	device address		0	uint32	Read	End Device address created by Application server, used to register the product on the Network server by ABP
61	3D	3	2	network ID		0	uint32	Read	Network server ID number, used to register the product on the Network server by ABP
63	3F	3	2	join mode		OTAA	string	Read	OTAA: Over-the-Air activation, ABP: Activation by Personalizatio n
65	41	3	4	network mode		PUBLIC	string	Read	PUBLIC, PRIVATE
76	4C	3	3	bandwidth		BW125	string	Read	BW125
79	4F	3	2	spread factor		SF10	string	Read	SF10, SF9, SF8, SF7
81	51	3	4	activation of ADR		ADR OFF	string	Read	ADR ON, ADR OFF
85	55	3	1	class		A	string	Read	
103	67	3	1	sensor type	1-255		uint16	Read	1-254: sensor type, 255: no sensor
104	68	3	1	battery level	0-3		uint16	Read	4 levels of battery capacity status

105	69	3	1	error status	0-1		uint16	Read	Error code of sensor, 0: no error, 1: error
106	6A	3	1	prm1 alarm status	0-2		uint16	Read	Alarm status of parameters 1, 0: none, 1: Low, 2: High
107	6B	3	1	prm2 alarm status	0-2		uint16	Read	Alarm status of parameter 2
108	6C	3	2	prm1 value			float	Read	Value of parameter 1
110	6E	3	2	prm2 value			float	Read	Value of parameter 2
112	70	3	1	battery %	10%, 30%, 60%, 99%		uint16	Read	% Value of battery capacity
113	71	3	2	battery voltage	0-3.67 vdc		float	Read	Value of battery voltage
115	73	3	2	mcu temperature	oC		float	Read	Temperature value of RF module
117	75	3	1	mcu vref	0-3.67 vdc		uint16	Read	Vref value of RF module
118	76	3	1	button1 status	0-1		uint16	Read	Button state, 0: No button pressed, 1: Button pressed
119	77	3	1	button2 status	0-1		uint16	Read	Button status, 0: No magnetic sensor detected, 1: Magnetic sensor detected
126	78	3	2	prm3 value			float	Read	Value of parameter 3
128	7A	3	1	prm3 alarm status	0-2		uint16	Read	Report the alarm status of parameter 3

Here is the table for Configuration:

Modbus Register (Decimal)	Modbus Register (Hex)	Function Code	# of Registers	Description	Range	Default	Format	Property	Comment
256	100	3 / 16	1	modbus address	1-247	1	uint16	R/W	Modbus address of the device
257	101	3 / 16	1	modbus baudrate	0-1	0	uint16	R/W	0: 9600, 1: 19200
258	102	3 / 16	1	modbus parity	0-2	0	uint16	R/W	0: none, 1: odd, 2: even
259	103	3 / 16	9	serial number			string	R/W (Password)	

268	10C	3 / 16	2	password for setting			uint32	R/W (Password)	password 190577
270	10E	3 / 16	4	lora appEUI			hex	R/W (Password)	Application server's EUI number, used to register the product on the Network Server by OTAA
274	112	3 / 16	8	lora appKey			hex	R/W (Password)	The number of keys used to create two security keys of the End Device, used to register the product on the Network server by OTAA
282	11A	3 / 16	8	lora nwkSkey			hex	R/W (Password)	key number encrypts the communication command of the MAC layer of the End Device, which is used to register the product on the Network Server by ABP
290	122	3 / 16	8	lora appSkey			hex	R/W (Password)	End Device data encryption key number, used to register the product on the Network Server by ABP
298	12A	3 / 16	2	device address			uint32	R/W (Password)	End Device address created by Application server, used to register the product on the Network server by ABP
300	12C	3 / 16	2	network ID			uint32	R/W (Password)	Network server ID number, used to register the product on the Network server by ABP
302	12E	3 / 16	1	activation mode	0-1	1	uint16	R/W (Password)	1: OTAA (Over-the-Air Activation), 0: ABP (Activation by Personalization)
304	130	3 / 16	1	application port	1-255	1	uint16	R/W (Password)	Port 224 is reserved for certification
319	13F	3 / 16	1	tx power	2-20	16	uint16	R/W (Password)	tx power: 2,4,6,8,10,12,14,16,18,20

320	140	3 / 16	1	adaptative data rate	0-1	0	uint16	R/W (Password)	Automatically adjust data rate, 0: disable, 1: enable
334	14E	3 / 16	2	cycle send data		900	uint32	R/W	sec (data sending cycle)
338	152	3 / 16	1	alarm limt		44	uint16	R/W	limit the number of events / day
340	154	3 / 16	2	sensor1: sampling_rate		120	uint32	R/W	sec (frequency of data taken from sensor 1)
348	15C	3 / 16	2	prm1: a		1	float	R/W	Scale parameter "a" of Measured value 1
350	15E	3 / 16	2	prm1: b		0	float	R/W	Scale parameter "b" of Measured value 1
354	162	3 / 16	2	prm1: High Threshold		100000	float	R/W	High threshold value of Measured value 1
356	164	3 / 16	2	prm1: High Hysteresis		10000	float	R/W	High hysteresis value of Measured value 1
358	166	3 / 16	2	prm1: Low Threshold		0	float	R/W	Low threshold value of Measured value 1
360	168	3 / 16	2	prm1: Low Hysteresis		10000	float	R/W	Low hysteresis value of Measured value 1
362	16A	3 / 16	2	prm1: High Cut		100000	float	R/W	Upper limit value of Measured value 1
364	16C	3 / 16	2	prm1: Low Cut		0	float	R/W	Lower limit value of Measured value 1

6. Installation

6.1 Installation location

To maximize the distance of transmission, the ideal condition is Line-of-sight (LOS) between the LoRaWAN sensor and Gateway. In real life, there may be no LOS condition. However, the LoRaWAN sensor still communicates with Gateway, but the distance will be reduced significantly.

> **ATTENTION:**
>
> **DO NOT** install the LoRaWAN sensor or its antenna inside a completed **metallic** box or housing, because the RF signal can not pass through the metallic wall. The housing is made from Non-metallic materials like plastic, glass, wood, leather, concrete, cement…is acceptable.

WSLRW-AG-H5.PNG

6.2 Battery installation

WSLRW-AG-H7.PNG

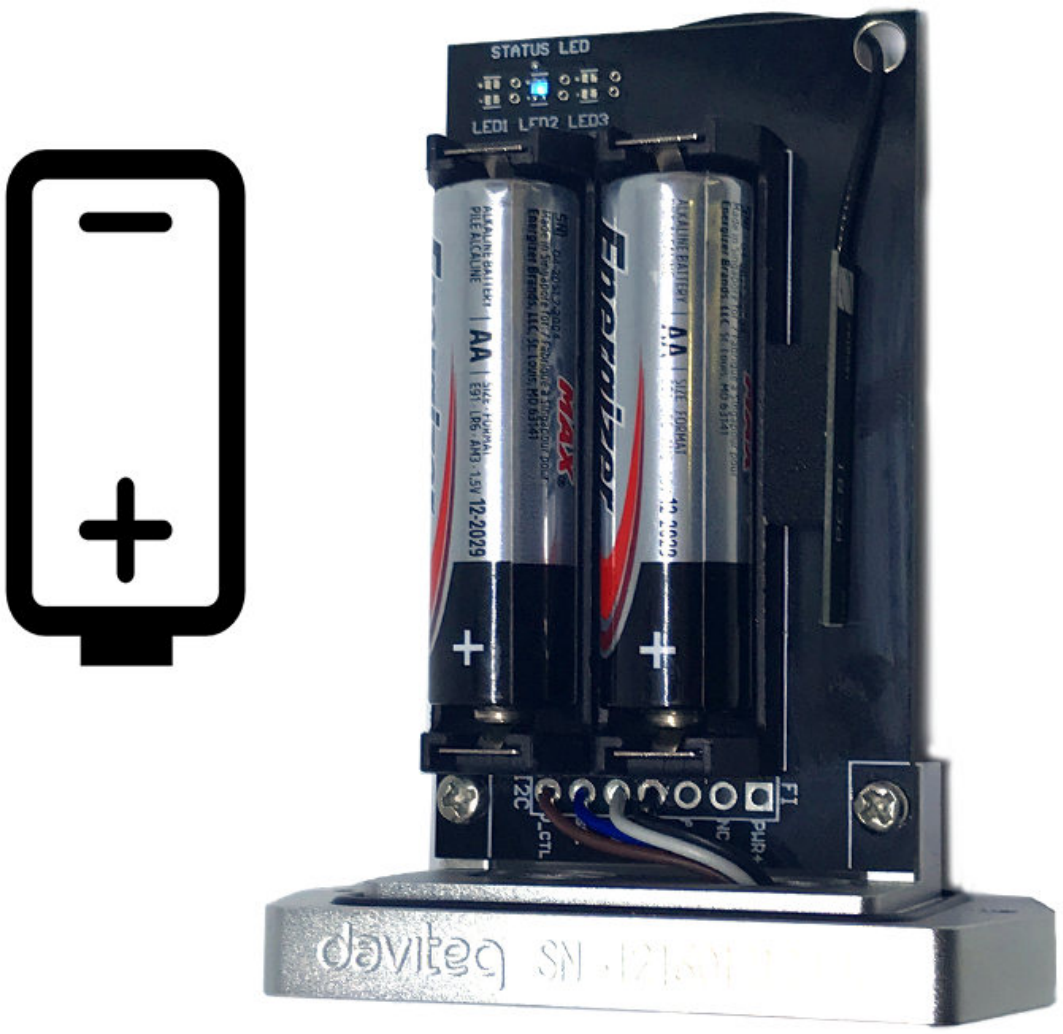
Steps for battery installation:

Step 1: Using L hex key to unscrew M4 screws at the side of the housing and carefully pull out the top plastic housing in the vertical direction

Step 2: Insert 02 x AA 1.5VDC battery, please take note the poles of the battery

ATTENTION:

REVERSED POLARITY OF BATTERIES IN 10 SECONDS CAN DAMAGE THE SENSOR CIRCUIT!!!



Step 3: Insert the top plastic housing and locking by L hex key

ATTENTION:

When reinstalling the cover, pay attention to put the PCB edge into the middle slot of the box inside as shown below)

7. Troubleshooting

No.	Phenomena	Reason	Solutions
1	The BLUE LED does not blink when the battery is installed	Insert the battery in the opposite direction	Insert the battery in the correct way
2	The RED LED is always on	Due to noise, the peripheral components (i2c, spi, uart, ..) of RF module cannot be initialized	After 30s the node will automatically reset. If the noise causes the Watchdog not to initialize, remove the battery and wait for more than 10 seconds, then insert the battery again
3	The RED LED blinks continuously (10ms ON / 2s OFF) and the Node does not send RF. After more than 10 sending cycles, the Node will automatically reset	• Operating frequency in that country is prohibited • Operating frequency in that country is limited to Data rate, Tx Power	• Reconfigure the allowed frequency of operation • Reconfigure Data rate = DR5 / SF07, Tx Power
4	RED LED blinks continuously (10ms ON / 2s OFF) and Node sends RF continuously 3s / time but no data. After more than 10 sending cycles, the Node will automatically reset	Node runs dummy sending mode => sent by Gateway to send Downlink packets when users clear Uplink and Downlink counter values on Network Server (build-in Gateway) when activated by ABP	Configuration enabled by OTAA
5	The RED LED flashes 10ms ON / 10s OFF and the Node does not send RF	Node activation by OTAA on Network server has not been successful	Using Magnet-Key to force Node to send RF continuously for 3 seconds/time => when activating by OTAA successfully, the GREEN LED will blink after sending RF
6	The node sent RF successfully but the GREEN LED did not blink	LED is broken	Warranty to replace LED
7	The data packet taken from the Gateway has an incorrect value	The data package is encrypted	Get the decoded packet on the Application Server
8	The node sends RF and activates by ABP, on Gateway receives data but the Application server has no data	The application server still stores the counter values of the previous Uplink and Downlink	Delete the counter values of Uplink and Downlink on the Application server
9	The node does not send RF and the RF module is hot	• Insert the battery in the opposite direction • Short circuit	Warranty or replacement

10	The node does not send RF to Gateway according to the alarm, LED does not blink	• The alarm configuration is incorrect • Running out of the number of alarms set for the day	• Check alarm configuration • Check the configuration for the maximum number of alarms per day
11	The node does not send RF to Gateway when activated by the magnetic key, LED does not blink	The magnetic sensor has malfunctioned	Read the status of the magnetic sensor via Modbus (when powering or attaching the battery) to see if the magnetic sensor is working.
12	Node has blinked LED GREEN when sending RF but the Gateway or Application server cannot receive	• LoRa module on the Gateway is faulty • The IP connection (4G / WiFi / ...) on the Gateway is faulty	• Check Gateway's LoRa status lights on Gateway • Check 4G / WiFi status lights on Gateway
13	The value of the sensor is 0 and sensor_type = 0xFF	Lost connection with the sensor	• Check sensor connection • Replace the module sensor
14	RSSI is weak and often loses data	• The distance between Node and Gateway is far or there are many obstructions • Connection to Antenna problem • Install metal nodes or in metal cabinets	• Configure Data rate = DR0 / SF12 • Check Antenna position • Install Node in a well-ventilated location

8. Support contacts

Manufacturer

Daviteq Technologies Inc
No.11 Street 2G, Nam Hung Vuong Res., An Lac Ward, Binh Tan Dist., Ho Chi Minh City, Vietnam.
Tel: +84-28-6268.2523/4 (ext.122)
Email: info@daviteq.com | www.daviteq.com