

User Guide

Connectivity Management Tool - CMT Cloud

Version 1.1



Document Information

Author:	Worldsensing	Client:	All
Creation Date	11/03/2020	Document description	This document describes the CMT Cloud solution.

Version	Date	Author	Description
1.0	17/11/2020	Customer Success	CMT Cloud user guide
1.1	22/04/2022	Customer Success	Minor changes



Contents

Document Information	1
Contents	1
Confidentiality Agreement	6
System Architecture	6
Unique data server Per Project Scheme	7
Edge Devices	9
Loadsensing Mobile App (Dlog)	9
Gateways	10
Upgrade embedded gateway	11
Network Server	12
Data server	13
Multi-gateway Feature	15
System Deployment	16
Data Server Deployment	16
Data server deployment request	16
Data server Initial Configuration	17
Security access passwords modification	17
Time Zone modification	17
Network (devices) status monitoring via email	18
Gateway Commissioning	19
Local access	19
Gateway local access commissioning	19
Gateway Status	23

General info:	23
Application status:	23
Network info:	24
GPRS Modem Info:	24
Internet Configuration	25
Network Watchdog:	26
Network connection:	26
NTP Server:	27
Cellular configuration	28
Low-Power Radio Configuration	30
Password Change And Tunnel Settings	32
Admin password	32
Remote tunnel	32
Gateway Registration On Data server	33
Procedure	33
Data logger Commissioning	36
Requirements	36
Online Registration Commissioning Procedure	37
Step 1: Physical installation	38
Step 2: Loadsensing Mobile App (Dlog) first steps: Firmware upgrade and time synchronization	38
Step 3: Sensor configuration [Setup Wizard]	40
Step 4: Radio configuration (Setup Wizard)	41
A. Radio type → MultiGW	41

B. Sampling rate	42
C. Region	43
D. Data server ID	45
E. Network Encrypt Password	46
F. Advanced options	47
Step 5. Register node on data server	48
Step 6: Radio signal coverage	50
Offline Registration Commissioning Procedure	51
Registration on the data server	52
Loadsensing Mobile App (Dlog) Setup wizard	53
Data Server Features	58
Dashboard	58
Network	63
Coverage Tests Page	65
Data Logger Page	65
Last readings and Time-series graphs	66
Status	66
Last messages	67
Loadsensing Devices Configuration	68
Loadsensing Data Loggers Management	68
New node registration	68
Nodes List	70
Loadsensing Gateways Management	72
New gateway registration	72

Gateway List	74
Logs History	75
System Configuration	76
General settings	76
Timezone	76
Monitoring notification emails	76
FTP Client Configuration	77
Compacted CSV deployment	80
Error data	81
Compacted options	81
MQTT server	81
REST API calls	83
Standard API calls	83
Troubleshooting	84
Node Reconfiguration	84
Other Troubleshooting	85
CONTACT WORLDSENSING	85

Confidentiality Agreement

All information, products, services, licenses and, in general, whatever revealed by Worldsensing is considered as confidential unless otherwise expressly stated by it. In addition to this confidentiality, no information, product, service, or license can be disclosed, communicated, disseminated, distributed, stored, in whole or in part, or transformed. All information, as well as the products, services, and licenses, are and will be the property of Worldsensing, which is and will also be the propriety of all intellectual, industrial, patent, and trademark rights. The use of any Software of Worldsensing will be subject to the application of EULA (End User License Agreement) document in force at any time, as well as the General T&C in force. Worldsensing reserves the right to revise and change this publication, the information, the products, and/or the services given by it when deemed necessary.

Any issues or queries arising should be addressed to industrial_support@worldsensing.com.

The content presented in this document will be binding only after the signature of a formal contract between the parties.

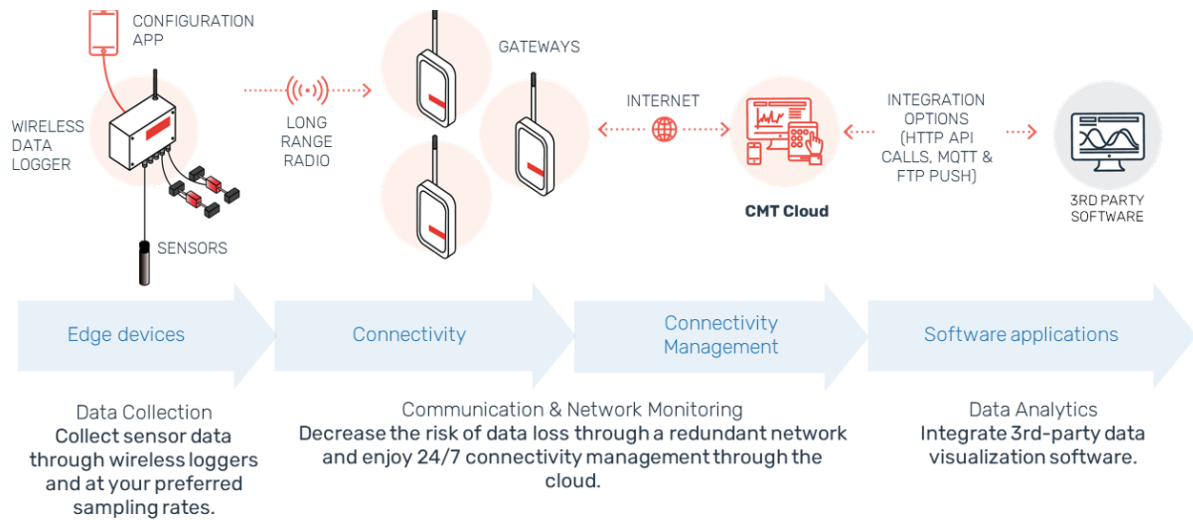
System Architecture



Unique data server Per Project Scheme

CMT Cloud provides full data digitization, easy to deploy, in near-real-time, with high reliability and easy to integrate with third-party monitoring software platforms.

Multi-gateway System Architecture



Sensors are installed at their specific locations and wired to data loggers which collect data from these sensors. The data is broadcasted via radio signal to the multiple gateways. The data is saved in the cloud and may be integrated with 3rd party software.

Most sensors of the market can be connected to Loadsensing nodes, which is easily configured using our Android Dlog Application.

The nodes periodically read the instruments as configured, store the data, and broadcast them using our LoadSensing LoRaWAN® radio to the project data server.

A network of indoor and/or outdoor gateways will provide full radio coverage to all the nodes existing in a specific project, redirecting the received readings via radio to the LoadSensing network server, which will handle these readings to be finally stored in the data server.

This architecture ensures data acquisition, as several gateways will redirect the same readings received via radio from the same nodes and send them to the data server. Unlike the CMT Edge architecture, the data server is located out of the gateway. This feature avoids data loss in case of gateway failure.

This architecture simplifies monitoring tasks in those cases where more than one gateway is required to cover the nodes of the project.

The data server ensures high data availability, secure data backup, and new features deployment.

Edge Devices

Edge devices are data loggers or nodes in charge of powering the connected sensors, digitizing the reading, storing locally and broadcasting it to the gateways. Edge devices also include wireless sensors such as tiltmeters and the laser distance meter node.

All the current Loadsensing nodes (both data loggers and wireless sensors) are fully compatible with the CMT Cloud.

The CMT Cloud nodes use LoRaWAN[®] network to communicate with the gateways.

In case the node is not on the latest firmware version, an updated Dlog Android application (Version 1.7.30 or higher) will request the node to upgrade.

Nodes will require the latest firmware version. Worldsensing technical support department will advise about the compatible firmware versions.

Loadsensing Mobile App (Dlog)

Several changes have been applied to Loadsensing Dlog Android application to make it compatible with both CMT Edge and CMT Cloud solutions.

As well as the nodes requiring a minimum firmware version, a minimum Dlog Android application version is also required to configure nodes using the new radio.

Dlog v.1.7.30 is the first firmware version which allows selecting both CMT Edge radio (Loadsensing Radio) or CMT Cloud radio (MultiGW Radio). It also allows configuring nodes in standalone mode (Radio off).

In any case, it is highly recommended to upgrade the Dlog Application to the latest version which will have the latest features and fixes to avoid any kind of issue.

Loadsensing Mobile App

Radio configuration	
Radio type	Radio off
Sampling rate	LS Radio
Network Config	MultiGW
Region	Europe
Network Size	1-4 nodes
Edit network ID and password	<input type="checkbox"/>
Network ID	21145
Password	
Advanced options	
ETSI limit duty cycle	<input checked="" type="checkbox"/>

The multi-gateway radio configuration may be selected in the Loadsensing Mobile App.

Loadsensing Dlog Android application can be downloaded from our repository at <http://wsop.cat/industrial/Dlog/Dlog.apk>.

These are the minimum requirements for the Android device to correctly use the application:

- Android 5.1 Lollipop or higher
- USB-OTG Compatible device
- USB-OTG cable (provided by Worldsensing and available under request)

Gateways

The CMT Cloud requires a gateway or gateway infrastructure to provide connectivity to the nodes. This device will receive the radio messages broadcasted by the nodes and redirect them to the Network server. Please check zendesk or the [Worldsensing website](#) for the latest gateways compatible with CMT.

Upgrade embedded gateway

The gateways of the CMT Edge solution can be updated for use on CMT Cloud.

In case this update is needed, please, contact your Sales Manager and the [Customer Success team](#) will take care of it.

CMT Edge gateways must be at least on the 2.0 firmware version, and connected to the Internet, in order for it to be updated by the Worldsensing Customer Success department.

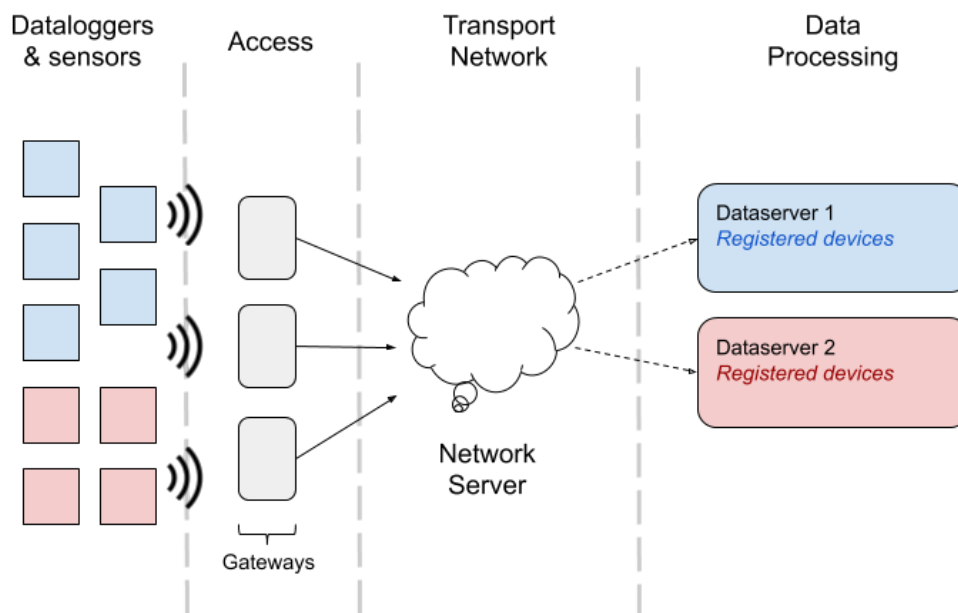


Network Server

The network server connects sensors and nodes through gateways with the end-user data server.

It ensures a reliable and secure routing of the messages broadcasted by nodes which are received by the gateway and redirected to the network server.

Data Flow Diagram



This network server acts as a stack, redirecting the received messages, such as readings and health messages, to the data server where the node has been registered previously. It represents the transport network of the solution.

The network server is factory configured in the gateways. Therefore, no configuration is required in the system. All deployed gateways will redirect the received messages to it, redirecting them to the appropriate data server.

Data server

The data server is the CMT software element where messages arrive. It is connected to the network server, and accepts, decrypts and saves all messages received from the nodes registered previously (during the node commissioning, via Dlog or directly in the data server).

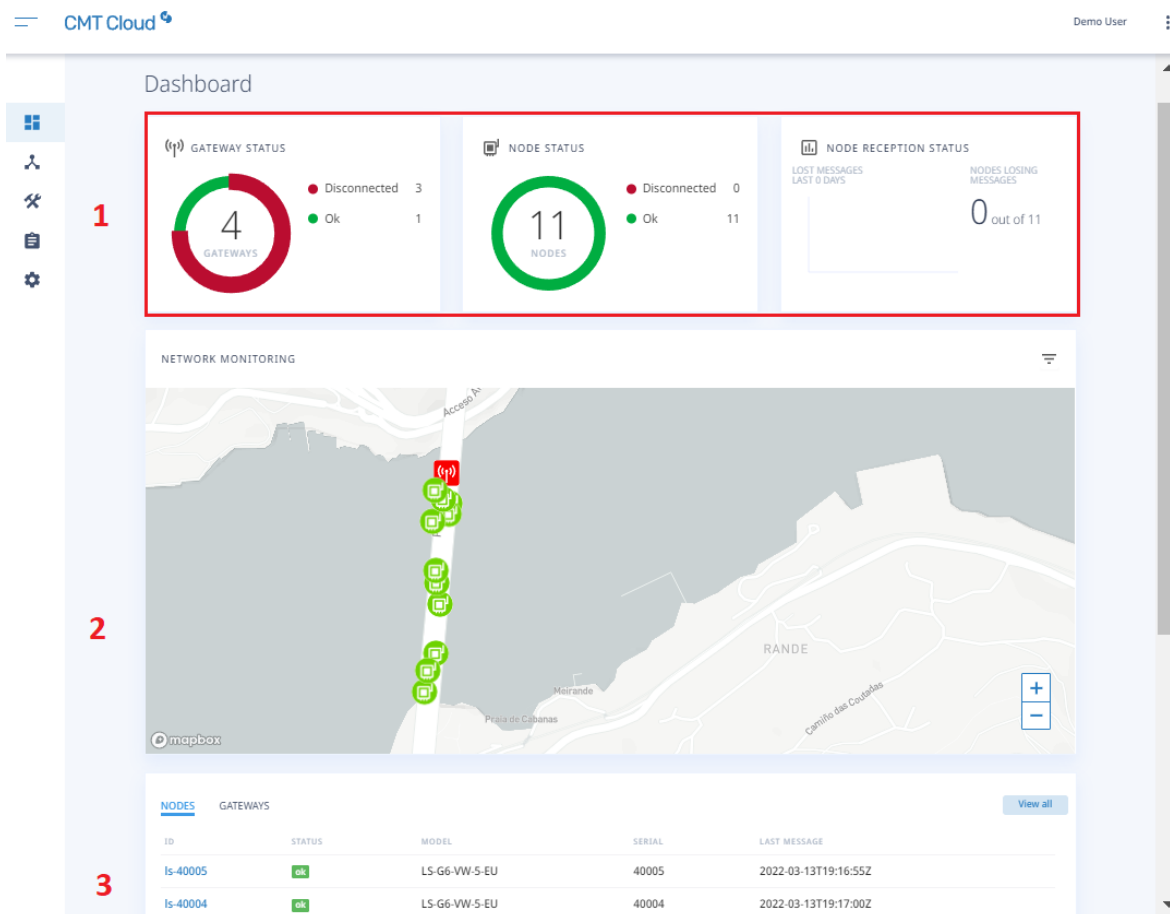
Unlike the CMT Edge solution, the data server is installed out of the gateway. This ensures high data availability, as it does not depend on the device operational status. It also reduces the gateway resources usage, which is now focused on networking tasks, allowing a bigger amount of node connection at shorter sampling rates.

It can be installed in a cloud-based system, which ensures better performance in server-to-server integrations, and increases user experience as it is installed in higher resources hardware, such as servers or cloud systems.

The main features of the data server are:

- Instruments and sensor network management
- Secure data (instruments readings) storage
- Graphical view of the latest readings
- Connected nodes and gateways status management and reporting via email
- Third-party connectivity (against backup systems or monitoring platforms)

CMT Cloud Dashboard



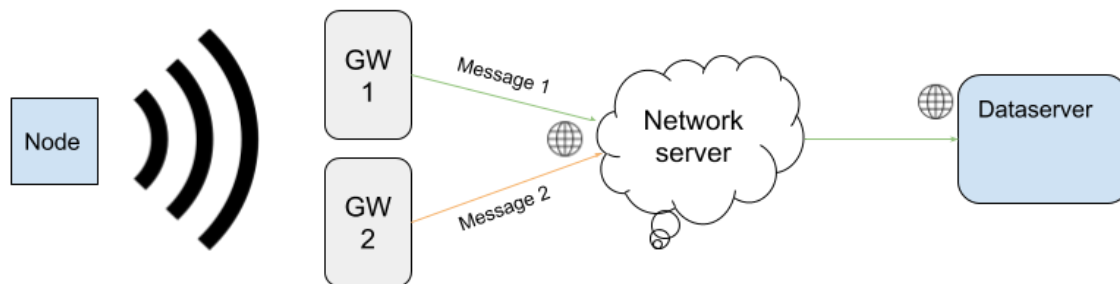
The CMT dashboard provides a quick view of the top 3 main KPIs monitored by the software. The first two are the Gateway and Nodes Status that show you the number of gateways or nodes that are online or offline. The third KPI is the Nodes Reception Status which shows how many nodes are losing messages per day for the last 5 days. Next is the Map View where you may zoom in and out on a map. Finally, at the lower part of the dashboard is the Device list which shows all the nodes and the gateways that are registered in the system and an overview of their status.

Multi-gateway Feature

The CMT Cloud infrastructure allows using the system in Multi-gateway mode.

This feature is available because all gateways redirect the received messages to the same network server, instead of parsing the message according to a preconfigured network password.

Multi-gateway network data flow



When a node broadcasts a message, it will be received by two or more gateways which are in the node coverage area. In case the message is sent using the same radio specifications than configured in the gateway, both gateways will redirect this message to the network server.

The LoRaWAN Network services will identify both incoming messages, delete duplicate ones and redirect it to the appropriate data server, where it will finally be decrypted and stored. All received messages metadata is stored in case downlink messages are required (Spreading factor modification etc.).

This feature allows not only greater flexibility during gateway network deployment, but also sets a second gateway near the first one to have a redundant network. This could be useful to allow data acquisition on critical areas of a specific project.

It is recommended to use a separated power and Internet connectivity sources for both gateways (for example, mains connected vs solar kit connected, Ethernet vs Mobile connectivity, to avoid both gateway malfunction due to a unique external issue. An example of this would be two gateways connected to the same Internet wired network may stop communicating in case of network failure).

System Deployment

This section explains the procedure to deploy a CMT Cloud project.

Main steps are:

- Data server deployment (under request to Worldsensing)
- Gateways installation
- Nodes commissioning

Data Server Deployment

Data server deployment request

Each project is managed by a single data server, regardless of the number of gateways, nodes, or sensors associated with it.

The data server is deployed by Worldsensing. Therefore it should be requested via the Sales manager. A previous registration is required.

<https://www.worldsensing.com/support/>

Once it is registered, a new request has to be made, asking for a new data server. In order to optimize the data server deployment some minimum data is required:

- Customer name
- Project name
- Project location (Country/City)
- Email contact (if different to the one registered on support platform)
- CMT Cloud User List

Worldsensing will accept the request and deploy and provide the web access of the data server. At least two weeks after accepting the request is required to deploy and check the system.

A URL link will be provided via the Customer Success support request platform and login credentials for each user provided in the CMT Cloud User List (user and password) will be sent to the provided email contact using a secure password sharing platform to comply with GDPR requirements.

The data server URL will be accessed to the Loadsensing servers with a data server ID provided by Worldsensing.

`loadsensing.wocs3.com/connectivity/{Dataserver_ID}`

Data server Initial Configuration

Once the data server is deployed and delivered it is ready to be used. In any case, it is recommended that a minimal configuration before the devices (both gateways and nodes) for a better or network deployment.

Security access passwords modification

Worldsensing will provide access settings to as many users as necessary. If required, the password can be modified by Worldsensing. For this, please contact the Customer Success department.

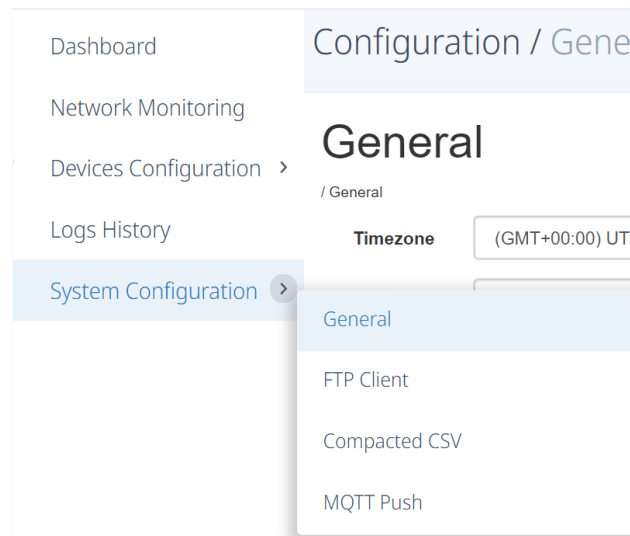
Time Zone modification

All radio messages are time-stamped in UTC at the nodes when generated. The radio message is sent through the whole system with this timestamp, and finally, the data server converts it to the configured local time zone. Data server default configuration will show data in UTC unless this configuration is modified.

Modifying the time zone before deploying the nodes ensures all data shown by the system, and stored in CSV files will be presented in local time (except for the custom compacted files which will always be in UTC). On the other hand, modifying the time zone after nodes deployment may cause a time-jump on CSV files between UTC and local time.

Check the General settings section of this guide for deployment information.

How to modify the time zone in CMT Cloud



Go to System Configuration tab and select the General option to update the timezone.

Network (devices) status monitoring via email

On the same tab, several email accounts can be configured.

These email addresses will be subscribed to the data server monitoring service and will get information such as:

- A status changes notification email whenever a node gets disconnected (a node is considered disconnected after no messages have been received for 14 hours)
- A daily reminder of the disconnected nodes, if there are any
- A monthly status report with the status of all the nodes
- A punctual email for every reconnected gateway and a disconnected email after no ping from the gateway has been received in the last 40 minutes

This will provide relevant information to the person/team in charge of the node network maintenance, by getting network status modifications as soon as the alarms are created.

Gateway Commissioning

Local access

The first step for gateway deployment is accessing locally to the gateway using the local web interface. This connection gives full access to the gateway configuration options to configure the WAN interface, which can be deployed over a 3G/4G or wired (ethernet) interface.

The local administration interface shall be used for:

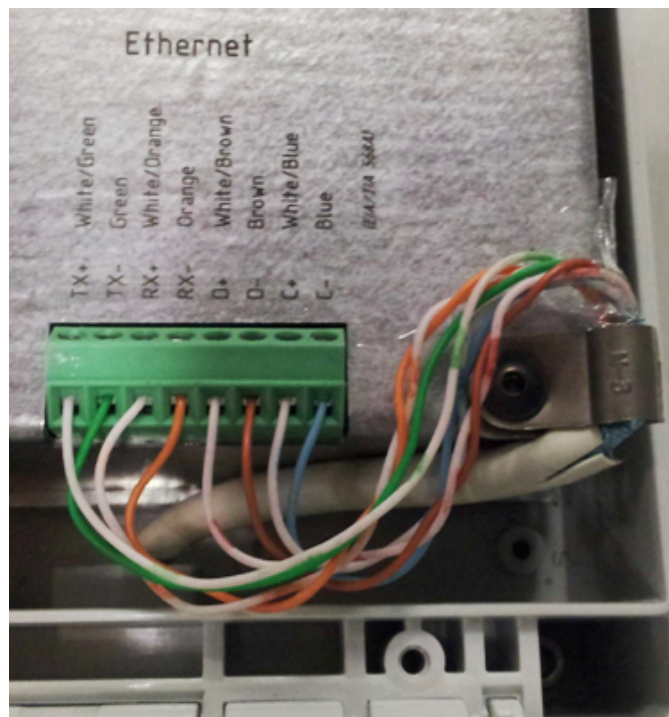
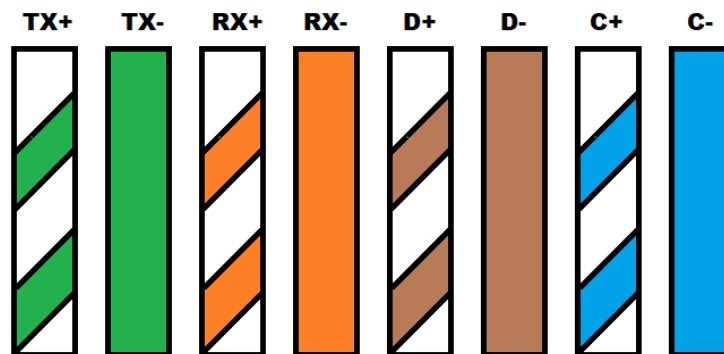
- Initial configuration of a new gateway
- On-site data retrieval and configuration of a gateway without an internet connection
- In the case of a forgotten remote access password, for the 3G gateways the local administration interface has a fixed password provided by Worldsensing in the Gateway Information Sheet (for the 4G gateway contact Customer Success department)

In case of using 3G/4G interface for Internet connection, the SIM card should be installed before the local connection process (before powering-up the device).

Gateway local access commissioning

In order to use the local administration interface, the gateway should be powered via PoE injector. For this purpose, the gateway enclosure must be opened using a flat-head screwdriver.

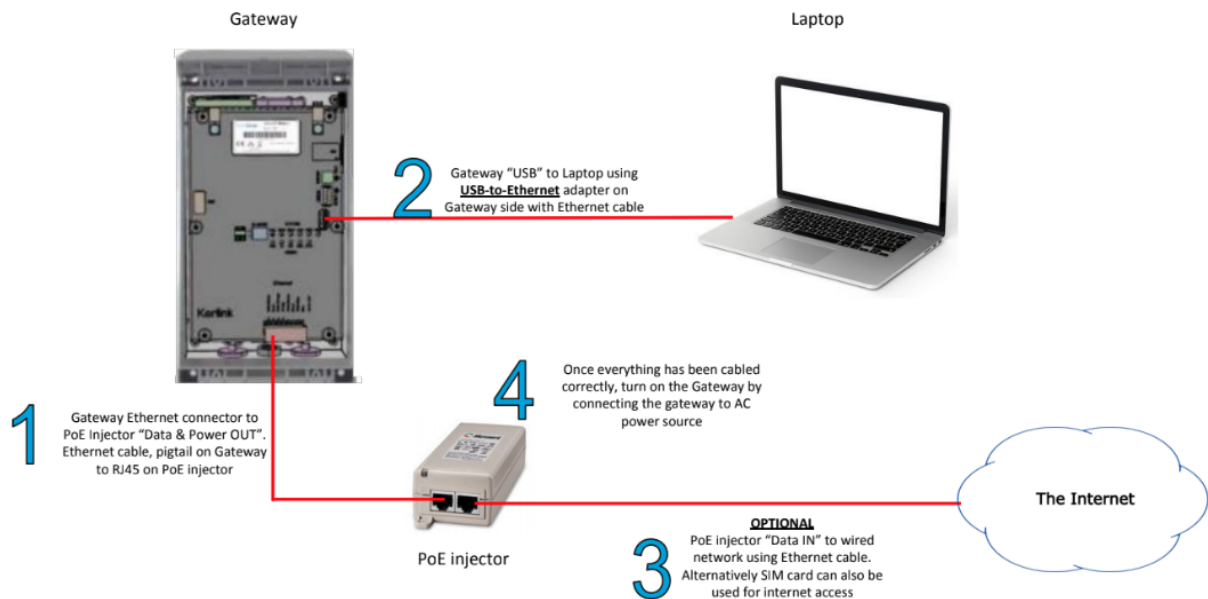
An Ethernet cable must be connected between the Data & Power OUT port of the PoE injector and the ethernet connection pad. To connect to this port, one of the RJ45 connectors of the Ethernet cable must be cut, passed through the gateway cable gland, and connected to the Ethernet connection pad following the scheme printed on the gateway. (Step 1)



The gateway must be connected to the computer through the Local Interface. A USB-ETHERnet adapter is provided with the gateway to connect the USB side on the USB port inside the gateway and attach an ethernet cable on the other side, connected to the gateway (Step 2).

Set the Internet connection. This means inserting the SIM card for GPRS/3G connectivity or wiring the DATA IN port of the PoE injector to the local network using an Ethernet cable (Step 3).

Once everything is cabled, power up the gateway connecting the PoE injector to mains. A correctly powered gateway will show a green led on the PoE injector. Orange led means the gateway has not been correctly wired to the PoE injector or a problem happens on the cable. (Step 4).



Ensure that the computer is configured to acquire an IP address automatically using DHCP. Local interface of the gateway will provide a dynamic IP address to the gateway, in the network 169.254.0.0/16.

Check the gateway connectivity is working correctly by pinging the gateway IP address:

ping 169.254.0.1

Once the connectivity is successful, open the following website on your Internet browser and access with the default access settings:

<http://169.254.0.1>

- user: admin

- password: VMjG6z

Note: This user and password are for exclusive use for the Local (USB) interface. They can't be modified nor disabled (Kerlink 3G gateway).

An SSL certification error will appear. This is normal as this gateway uses a self-signed certificate for SSL authentication. Adding a security exception for this certificate to allow the connection is required (self-signed certificate). Check your browser's documentation for instructions on how to do this (normally following the steps).

Should you experience difficulty connecting, check these steps:

- Use the USB-to-Ethernet adapter provided by Worldsensing (other adapters may not work depending on the driver)
- If the computer used to configure the gateway does not have an Ethernet port, use two USB-to-Ethernet adapters of the same model
- Check if the USB-to-Ethernet adapter associated network Interface has received a valid IP address (169.254.XXX.YYY with Subnet Mask 255.255.0.0)

If not, manually set a valid IP address on the same network range.

For example, IP address: 169.254.0.2 and Subnet Mask 255.255.0.0. Default gateway and DNS are not required as it is a direct communication without Internet access.

Gateway Status

Next steps show the gateway configuration once the device has been accessed via the gateway website. The Status tab displays the general information related to the gateway, updated every five minutes. It is the main page shown when accessing the gateway.

This tab has different sections, each one related to different features of the gateway:

General info:

This section displays general information of the gateway, such as serial number, model or firmware version. Gateway uptime, given in minutes, allows checking possible gateway reboots in a fast way.

General Info

Gateway serial number	20649
Gateway Model	LS-M6-KO-GW-FCC
Firmware version	1.0
Date	Wed Nov 4 10:58:12 UTC 2020
Uptime (minutes)	791
Input voltage	12.1503 V
Voltage history	gwVoltages_1.csv

Application status:

This section displays information related to the gateway connectivity status of the gateway:

- Internet connection: a ping against our servers (loadsensing.wocs3) is done to define if the gateway is Internet-connected.
- Status reporting: the gateway periodically sends information about its status parameters (voltage input, CPU & RAM usage, uptime) to our monitoring system (via port TCP-80)
- Remote access: displays the status of the VPN connection between the gateway and Worldsensing servers. This VPN connection is required for accessing via <https://loadsensing.wocs3.com/GWID>. In case the remote tunnel is disabled it will appear as Connection KO

Application status

Internet connection (ping)	Ping OK
Status reporting	Connection OK
Remote access	Connection OK

Network info:

This paragraph displays technical information about your network, such as type of connection (Ethernet or Mobile), interface status and IP parameters.

Network Info

Selected interface	Ethernet - DHCP
Ethernet Status	Up
Ethernet IP	192.168.7.76
Ethernet Netmask	255.255.252.0
Gprs/3g Status	Not connected
Gprs IP	none
Default Gateway	192.168.4.1
Primary DNS	192.168.4.12
Secondary DNS	8.8.8.8

GPRS Modem Info:

This paragraph displays the mobile connection information in case the gateway is Internet-connected using a SIM card. Note this information is provided by the ISP. Depending on the ISP and the APN settings used this information may not be available. Not showing this information does not mean a lack of mobile connectivity (Check Network Info and Application status paragraphs)

Gprs Modem Info

Status	Registered
IMSI	228017000984377
Operator	Swisscom
Roaming	Not roaming
Mode	HSDPA
Signal	77 %

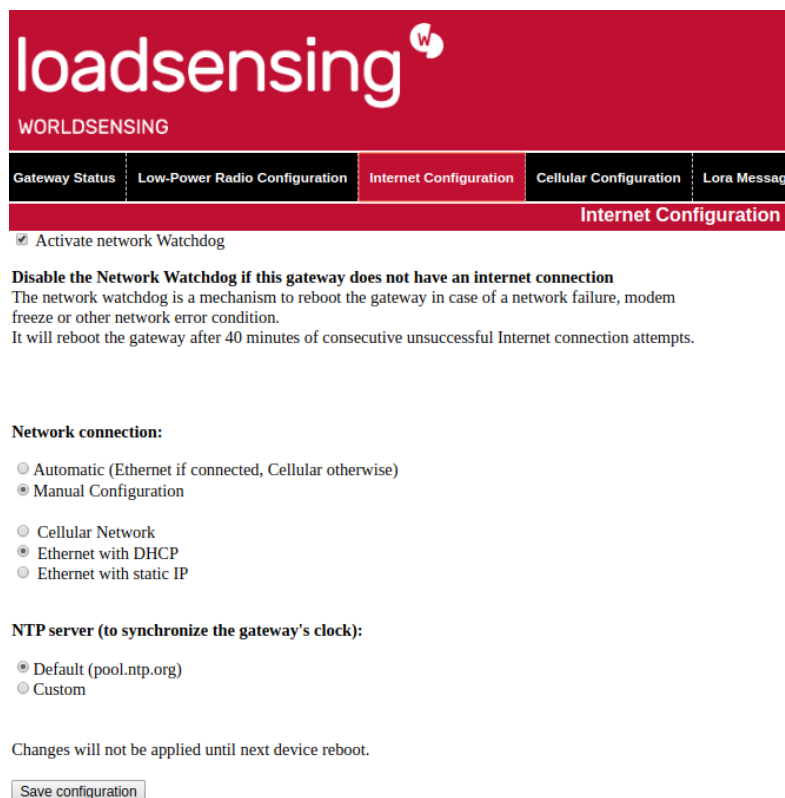
Internet Configuration

The Internet configuration tab allows selecting and configuring the Internet access configuration mode.

The gateway is factory-configured to allow Internet access without any configuration, by connecting to the Ethernet using configuration provided by the DHCP server or, if Ethernet connection (link) is not detected, by connecting to a mobile network using the SIM card with a default configuration; PIN number deactivated and using one of the APNs (mobile network configuration settings) stored in the internal database of the device. In case of not getting a Dynamic IP address via Ethernet, not getting successful mobile connectivity, it will remain disconnected until the next reboot.

It also comes with a network Watchdog which will reboot the gateway in case of lack of connectivity.

Time synchronization is also configured by default against an NTP server.



The screenshot shows the 'Internet Configuration' tab selected in the top navigation bar. The main content area has a red header with the 'loadsensing' logo and 'WORLDSENSING' text. Below the header, there are five tabs: 'Gateway Status', 'Low-Power Radio Configuration', 'Internet Configuration' (selected), 'Cellular Configuration', and 'Lora Message'. The 'Internet Configuration' tab is active, showing a checkbox for 'Activate network Watchdog' which is checked. Below this, there is a warning message: 'Disable the Network Watchdog if this gateway does not have an internet connection'. The text explains that the network watchdog is a mechanism to reboot the gateway in case of a network failure, modem freeze or other network error condition, and it will reboot the gateway after 40 minutes of consecutive unsuccessful Internet connection attempts. Under the heading 'Network connection:', there are two radio button options: 'Automatic (Ethernet if connected, Cellular otherwise)' and 'Manual Configuration'. Under the heading 'NTP server (to synchronize the gateway's clock):', there are two radio button options: 'Default (pool.ntp.org)' and 'Custom'. At the bottom, there is a note: 'Changes will not be applied until next device reboot.' and a 'Save configuration' button.

Network Watchdog:

The network Watchdog checks the gateway Internet connection. The gateway pings our servers (loadsensing.wocs3.com) every five minutes. In case it fails eight times the network watchdog will be triggered, after 40 minutes of consecutive unsuccessful Internet connection attempts, rebooting the gateway.

☒ Activate network Watchdog

Note: It should be deactivated in case of using the gateway in local environments (no Internet access), to avoid periodical reboots which may affect the solution performance. Disabling it on Internet-connected gateways will not trigger a reboot in case of lack of Internet connection.

Network connection:

The connection is set to automatic mode according to factory defaults. This configuration has some benefits, such as automatic interface selection, but Worldsensing recommends modifying it to select the appropriate interface as a best practice.

- Automatic mode
 - When the gateway is turned on, if a connected Ethernet cable is detected, a dynamic IP address will be requested to the network via DHCP. If a DHCP server provides connection settings, these will be used to ensure the Internet connection.
 - If no Ethernet cable connection is detected, the gateway will switch to mobile connection using the SIM card, trying to connect without PIN number and selecting the most appropriate APN settings listed at the internal database of the gateway.

Network connection:

- ☒ Automatic (Ethernet if connected, Cellular otherwise)
- ☐ Manual Configuration

Note:

- This method does not act as a failover; it won't switch back to Ethernet in case of mobile network failure
- Installing a SIM card with PIN number enabled won't allow Internet connection
- Not all ISP APN settings are available on the gateway database

- Manual configuration.

Network connection:

- ☐ Automatic (Ethernet if connected, Cellular otherwise)
- ☒ Manual Configuration
- ☒ Cellular Network
- ☐ Ethernet with DHCP
- ☐ Ethernet with static IP

NTP server (to synchronize the gateway's clock):

- ☒ Default (pool.ntp.org)
- ☐ Custom

- **Cellular Network:** Discards automatic network detection and always launches a Cellular (mobile) connection with the setting configured in the CELLULAR CONFIGURATION area
- **Ethernet with DHCP:** This setting overrides auto-detection and always launches an Ethernet connection, receiving configuration automatically through DHCP (Dynamic IP)
 - This option is the easiest to configure for an Ethernet interface but it may not be ideal for connecting directly to the gateway as the IP address may vary
- **Ethernet with static IP:** This setting overrides auto-detection and always launches an Ethernet connection. In this mode, it is required manually setting all network parameters

- ☒ Ethernet with static IP

IP Address:

Netmask:

Default gateway:

Primary DNS server:

Secondary DNS server:

NTP Server:

The NTP (Network Time Protocol) server synchronizes the gateway's clock automatically. By default it is connected to an NTP server. A different NTP server can be configured. This is recommended for

LAN environments, where usually an NTP server is deployed for all internal devices time synchronization.

NTP server (to synchronize the gateway's clock):

- ☐ Default (pool.ntp.org)
- ☒ Custom

NTP Server:

Settings saving and gateway reboot is required to apply any changes in this tab.

Cellular configuration

The Cellular configuration tab shows some configuration parameters specific to this type of connection. It should only be configured in case of selecting cellular network option at network connection, or automatic mode using a SIM card. It is discarded in all other cases.

- ☒ PIN Off (Sim card is unlocked)
- ☐ PIN On (Sim card needs PIN code)

- ☒ APN Auto selection (will select based on the SIM card operator)
- ☐ Manual APN Configuration

PIN settings:

- Off (default)
 - The gateway will not attempt to unlock the SIM card
 - The Cellular connection will fail If the SIM card is PIN code protected
- On
 - This setting allows entering the PIN code for a PIN-locked SIM card
 - A wrong PIN configuration will block the SIM card as the gateway will automatically attempt to unlock the SIM card, and exhaust the three possible attempts
 - There is no way to enter the PUK code in the gateway. If the SIM card gets PUK-locked, a mobile terminal will be required to unlock it
- APN settings
 - APN Auto selection (default)
 - Every mobile operator must set a specific configuration for connection to its network

- The gateway features a database of the correct configurations for hundreds of operators around the world. This setting will attempt 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 allows manual input of the mobile operator configuration values
 - Use this setting if auto-selection didn't work, or if specific, non-standard configuration values are required

☐ APN Auto selection (will select based on the SIM card operator)

☒ Manual APN Configuration

Authentication Method

Connection Mode

APN:

Username:

Password:

Settings saving and gateway reboot is required to apply any changes in this tab.

Low-Power Radio Configuration

This tab allows configuring the parameters of the radio parameters to communicate the nodes with the gateway. Different gateways will allow different radio communications, as gateways are built to optimize specific frequency ranges for specific countries, according to local radio regulations.

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

☒ Europe

Changes will not be applied until next device reboot.

Change Country and frequency

The chosen region on the Dlog Application for every node must match with the one configured in the Gateway Network configuration in order to be able to establish communications.

Loadsensing Mobile App

Radio configuration	
Radio type	MultiGW (be..
Sampling rate	1 h
Network Config	
Region	Europe Multi..
Network Size	1-15 nodes
Datasever ID	105
Device data encryption	
Network encrypt password	random



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

☒ Europe

Changes will not be applied until next device reboot.

Change Country and frequency

LoRa Server parameters define the network server where the gateway will redirect all incoming radio messages.

Change Lora Server parameters:

Lora Server URL:	worldsensing.net/ings.industri
Lora Server Port:	1700

Changes will not be applied until next device reboot.

[Change Lora Server Parameters](#)

Warning: These parameters should only be modified under Worldsensing supervision. Modifying it will provoke data loss as messages won't arrive at the appropriate network server.

Password Change And Tunnel Settings

This tab allows you to change the password for remote access to the Web Configuration Interface and enable or disable the remote tunnel against our servers (VPN).

A strong password is provided by Worldsensing to access the gateway with the admin user. The default factory password is printed on the Gateway Information Sheet. Once it has been changed, there is no way to recover it remotely, just local connection allows setting it back.

This password can be modified by accessing the gateway via the website. In case of accessing via loadsensing.wocs3.com or LAN IP address, the previous password must be entered. This is not required if you are connected through the local administration interface.

Note: Worldsensing securely saves the default access settings. If you require a copy of this document, which includes access passwords, advise us via the support platform at <http://worldsensing.com/support>.

Admin password

This is the section where the admin password can be modified.

Admin password

This is the password for the "admin" user

Current password:

New password:

Repeat new password:

Remote tunnel

This is the section where the tunnel between Loadsensing server and the gateway can be disabled.

Deactivating this tunnel means:

- https://loadsensing.wocs3.com/Gateway_ID link will be disabled, allowing access via IP only.

- Connections through "loadsensing.wocs3.com" will be deactivated and it will not be possible for the Technical Support team to remotely connect to the gateway for any maintenance required
- No gateway performance will be registered in our servers for troubleshooting
- You will only have access remotely through the Gprs/3G when having a public IP (ensure you have one), and locally through the gateway's local Ethernet
- The firewall for the 3G modem will be also deactivated and it could generate a huge data usage in case of being exposed to an external attack. When the tunnel is activated the firewall discards all connections from the cellular modem except the ones coming from the remote tunnel

Gateway Registration On Data server

At this moment both the data server and gateway (or several gateways) are deployed and communicating. Next step should be registering the gateways in the data server.

This procedure will inform about the gateway status to the data server, showing monitoring information such as Gateway status (Online, Critical). This information will be sent to the list of email addresses configured at the data server General tab.

It will also provide a list of linked gateways, the status, and direct access which will redirect to the gateway.

Note:

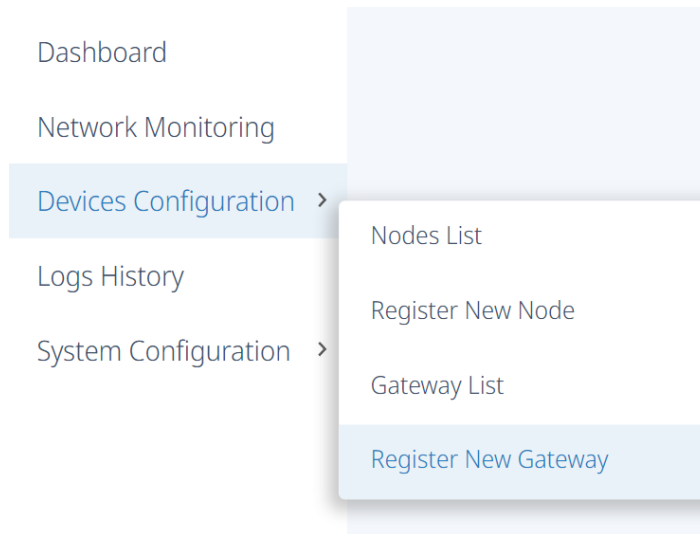
- This step is not required but highly recommended
- Registering a gateway does not imply that all messages received by the gateway will be redirected to the data server. This step is done in the node during the commissioning

Procedure

Access the data server through the URL and admin settings provided by Worldsensing

<https://loadsensing.wocs3.com/connectivity/123>

Click on the Devices Configuration tab, then Register New Gateway.



Set the requested parameters for every gateway to be registered in the data server:

- **Gateway ID:** the Gateway ID can be found in the gateway itself or gateway information sheet (GIS) provided by Worldsensing
- **Gateway name:** setting a name will allow an easier recognition of the gateway (optional)
- **Gateway password:** the password you use to access in your gateway via the website using the admin user. (Available at the GIS)

Example:

GATEWAY ID

12345

Gateway ID can be found printed on a sticker of the device.

GATEWAY NAME

Gateway 1

GATEWAY PASSWORD

.....|

Register

Once the gateway is registered the system indicates if the registration process failed or succeeded, in which case it shows a list of registered gateways with the link to the gateway configuration web.



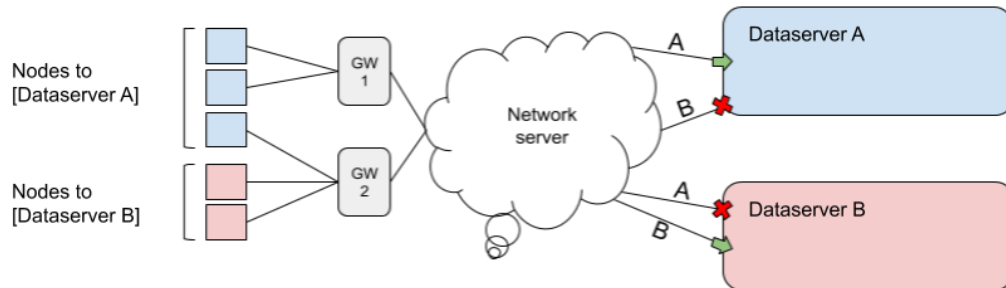
Gateway successfully registered: **12345**



Unable to register New Gateway

Data logger Commissioning

The CMT Cloud architecture is based on the communication between the node to the data server.



To ensure the communications between nodes and data server, each node must be registered on the data server first. In this way the network server will be aware of the nodes list each data server has registered (and is waiting for messages) and redirect the message accordingly.

Once this step is done, the node will send radio messages, which will be redirected to the network server through the Loadsensing gateway's network, and will be redirected to the specific data server.

The registering step is done on the data server. This can be done using the Dlog app, during the setup wizard process, as it sends an order via the Internet to the data server. In case of not having an Internet connection (i.e., deploying nodes inside a tunnel) or not having the gateway access password (nodes are commissioned by a third party) nodes can be previously registered on the data server, through the website.

Therefore, two ways of commissioning a node exist: Offline or Online Registering.

Requirements

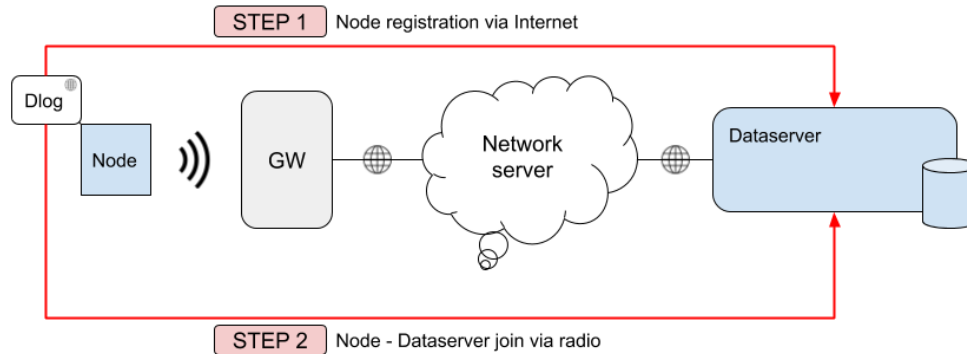
Nodes can be configured to a CMT Cloud platform using the latest published Dlog version, which allows Multi-gateway radio configuration. Initial Loadsensing Dlog Version with Multi-gateway support is 1.7.21, published in November 2019.

Anyway it is highly recommended to upgrade the Dlog Application to the latest version which will have the latest features and fixes to avoid any kind of issue.

All loadsensing G6 nodes are compatible with this solution, but they require a specific firmware version to connect to this platform. Nodes must be upgraded at least to firmware version 2.41.

Online Registration Commissioning Procedure

Online registration commissioning of a node requires Dlog application to be used in an Android device with Internet access, as the Dlog will proceed to register the node during the commissioning.





Step 1: Physical installation

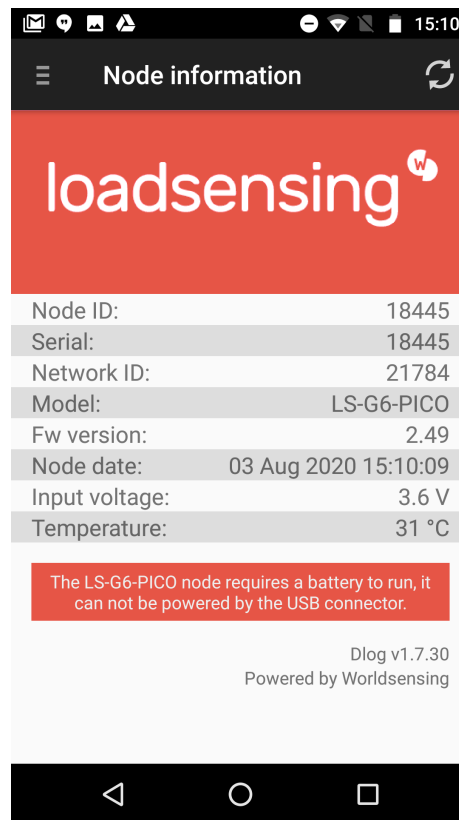
- Install batteries according to the indications on the node electrical board. SAFT LSH14 batteries are recommended
- Set the internal switch of the node in BATT mode (if exists). This switch will power the node and connected instruments using the batteries instead of powering it using the Android device
- Note: Nodes without an internal switch will only work with batteries inserted. A node with the internal switch in EXT PWR mode will be powered by the Android device during commissioning. It will be turned off when the device is disconnected, even batteries are installed
- Connect the instrument to the node, passing the node through the cable glands and closing them accordingly

Step 2: Loadsensing Mobile App (Dlog) first steps: Firmware upgrade and time synchronization

Connect the provided USB-OTG cable to the Android device with the latest Android Loadsensing Dlog Application installed.

The node configuration application will be launched automatically showing the main screen, where the main information such as Node ID, serial number, model, firmware version, date and time, battery voltage and temperature are shown.

Loadsensing Mobile App



At this step, the application may ask for a firmware upgrade. Accept and follow the steps without disconnecting the USB-otg cable during the firmware upgrade.

In case of failure disconnect the cable, restart the application and connect the node again. This step will be restarted and the node will ask for the firmware upgrade again.

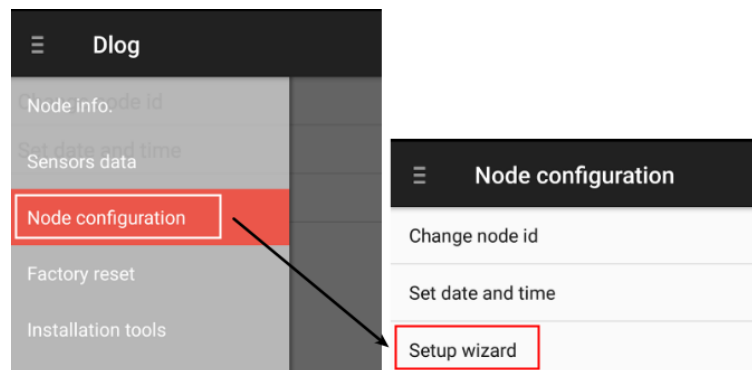
In case the node is up to date, the application will ask to synchronize date and time. It is important to synchronize the node DateTime will timestamp all readings. This can be manually done by selecting Set Date and Time on the Node Configuration tab.

In case the node loses the timestamp, it will be set to defaults (1970-01-01 00:00:00). Health messages sent periodically to the gateway (every seven hours) will allow synchronizing the node and gateway timestamp.

Step 3: Sensor configuration [Setup Wizard]

Node commissioning is done at the set-up wizard. This wizard can be found by clicking on Node Configuration on the left menu, then clicking on Setup Wizard. This will start the commissioning process.

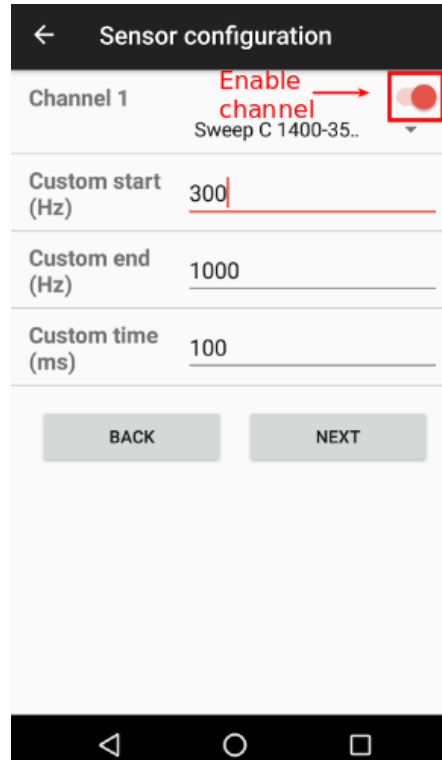
Loadsensing Mobile App



The first step at Setup wizard is related to instrument configuration. At this step, the channels to be used can be enabled or disabled. Selecting the output type of the instrument will show a wiring scheme and will allow configuring all the parameters associated with it. Check the Nodes user guide at our knowledge base for specific nodes.

Example of a one-channel vibrating wire node:

Loadsensing Mobile App



Once the instrument is wired and configured, clicking the Next button will provide a test reading and show it on the screen. As many readings as required can be taken if troubleshooting is required.

Note: The node commissioning may vary depending on the sensor or data logger model.

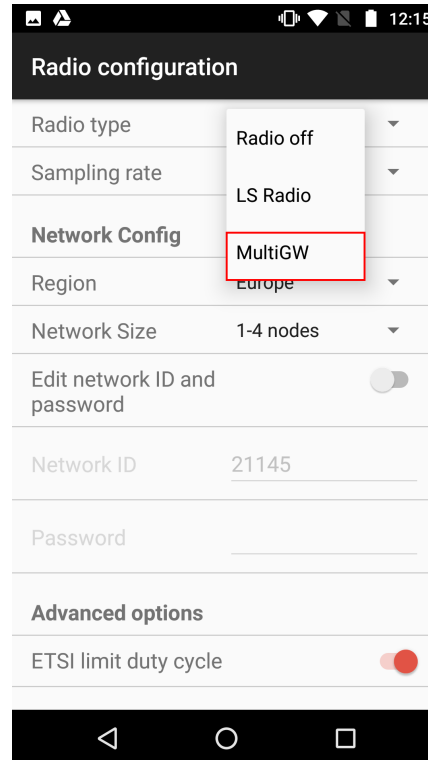
Step 4: Radio configuration (Setup Wizard)

Next step of the setup wizard will configure the radio settings.

A. Radio type → MultiGW

Dlog application can be used to commission offline nodes (without being connected to the gateway), Loadsensing radio (CMT Edge networks where data server is installed in the gateway) or CMT Cloud (MultiGW option).

Loadsensing Mobile App

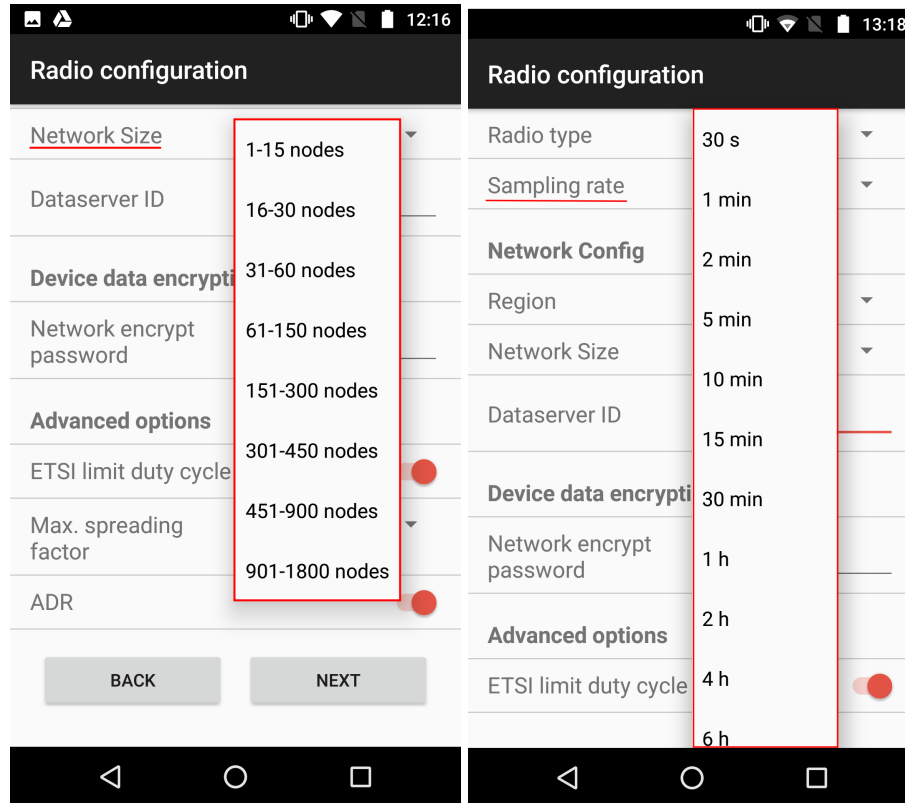


B. Sampling rate

The sampling rate is unique to the whole node, can't be configured independently for every channel of the node.

It is directly related to Network size for CMT Edge system, as there are some limitations in this system. The bigger the network (number of nodes) is, bigger sampling rates will only be available

Loadsensing Mobile App



C. Region

As LoRaWAN radios are regulated by countries, different regions have been implemented in the system to meet with local regulations. The appropriate network type (region) must be selected to meet with local regulations.

Loadsensing Mobile App

Radio configuration

Radio type: MultiGW (be..)

Sampling rate: 1 h

Network Config

Region: Europe MultiGW

Network Size: FCC MultiGW

Dataserver ID: 923A MultiGW

Device data encryption: 922S MultiGW

Network encryption password: test

Advanced options

ETSI limit duty cycle: ☒

Nodes can be configured with all the existing regions, but it is important to choose the same region on the nodes rather than the region which is configured in the gateway. Otherwise, the gateway will discard the radio messages received from those nodes.

Loadsensing Mobile App

Radio configuration	
Radio type	MultiGW (be..
Sampling rate	1 h
Network Config	
Region	Europe Multi..
Network Size	1-15 nodes
Dataserver ID	105
Device data encryption	
Network encrypt password	random

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

☒ Europe

Changes will not be applied until next device reboot.

Change Country and frequency

D. Data server ID

This space is reserved to set the data server ID number where the nodes will be registered. At the next step, the nodes will be registered in this data server, using the Network encrypt password.

Loadsensing Mobile App

Radio configuration	
Radio type	MultiGW (be.. ▾
Sampling rate	1 h ▾
Network Config	
Region	Europe Multi.. ▾
Network Size	1-15 nodes ▾
Dataserver ID	105
Device data encryption	
Network encrypt password	random

E. Network Encrypt Password

During online commissioning, Dlog will directly register the node in the data server using the network encryption password. This means there is no need to previously register the nodes in the data server.

The Dlog configures the encryption keys used by the Node to securely communicate with the CMT Cloud through the gateway and network server. The Node Network Encryption Password is used in combination with the Node ID to generate the mentioned encryption keys.

The same Node Network Encryption password specified here in the configuration step must be used in the CMT Cloud Node register. When the Dlog is also used for the Node register the same Node Network Encryption password is automatically used, but when the Node is registered in CMT Cloud using the web interface the user must specify the same Node Network Encryption password (required for offline registering).

In this example, the node will be registered in the next step of the setup wizard in the data server 105 using the password 'random'.

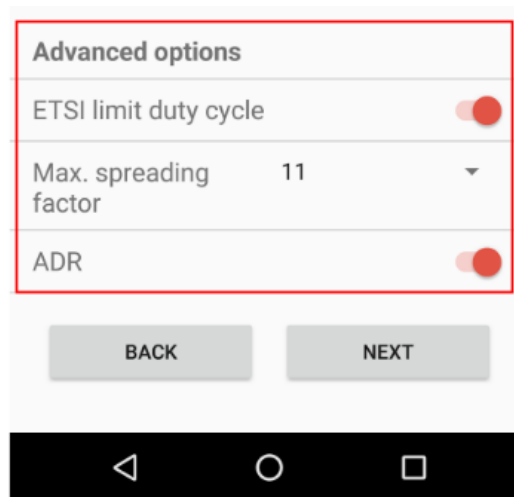
Loadsensing Mobile App

Radio configuration	
Radio type	MultiGW (be.. ▾
Sampling rate	1 h ▾
Network Config	
Region	Europe Multi.. ▾
Network Size	1-15 nodes ▾
Dataserver ID	105
Device data encryption	
Network encrypt password	random

F. Advanced options

Options by default are configured to meet with local regulations. These settings can be modified to get better signal strength. Check the radio annexe at Worldsensing knowledge base for more information.

Loadsensing Mobile App



Example of a valid configuration to register a node in data server 105 using 'random' password. The node will sample a reading every hour and broadcast it using the European radio model. Any Loadsensing gateway configured with this radio model that receives its radio messages will redirect it to the network server, which will redirect them to the 105 data server to be decrypted and processed.

Loadsensing Mobile App

Radio configuration	
Radio type	MultiGW (be.. ▾
Sampling rate	1 h ▾
Network Config	
Region	Europe Multi.. ▾
Network Size	1-15 nodes ▾
Dataserver ID	105
Device data encryption	
Network encrypt password	random

Advanced options	
ETSI limit duty cycle	<input checked="" type="checkbox"/>
Max. spreading factor	11 ▾
ADR	<input checked="" type="checkbox"/>

Step 5. Register node on data server

Registering the node on the data server allows the data server to receive data from that specific node with its Network encryption password.

This step can be performed immediately, and directly from the Dlog Android application, in case of having an Internet connection in the Android device. Otherwise (no internet access on the device) it will be required to previously register the node (Check Offline procedure).

Required information for Online node registering:

- Data server ID: ID of the data server where the node will be registered. Can't be modified as it has been configured in the previous step

- Data server password: node registration password. Provided by Worldsensing under a data server deployment request

Click Next to proceed to registration. This procedure may take up to 20 seconds.

Loadsensing Mobile App

Register node in dataserver

Dataserver ID	300
Dataserver Password	<u>Node registration</u>

No data will be visualized until this node is registered in the dataserver.

The registration process can be performed now if internet access is reliable or else we suggest performing it via the dataserver's website.

BACK NEXT

SKIP

Once the process has been completed, the node will appear in the gateway Network Management tab, Authorised Nodes option.

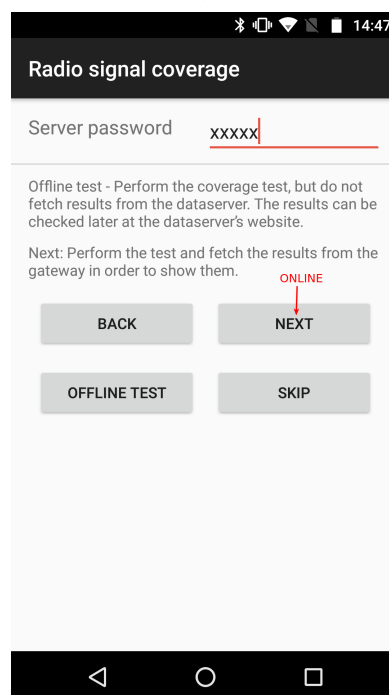
Step 6: Radio signal coverage

The last step is doing a coverage test for checking the LoRaWAN radio coverage between the node and the gateway. The node will send ten messages at Spreading factor 7, 8 and 9; and 5 more messages at SF 10, 11 and 12. This procedure may take up to two minutes.

As full connectivity is available at the Android device, all options are available:

- Offline Test: Radio coverage will be done. Then the Dlog application will show a Token ID. Radio coverage results can be checked in the gateway using this Token
- Skip: No coverage test is done
 - Next: An online coverage test is done, showing the results at Dlog application.

Loadsensing Mobile App



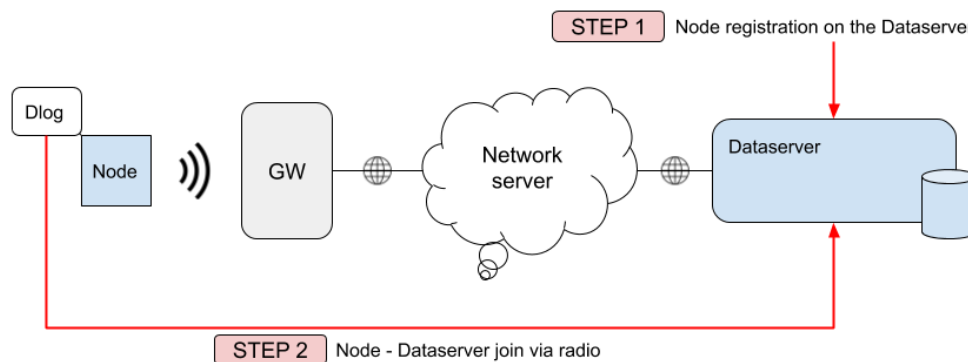
The results for Online procedure are shown when the procedure is finished. We can define the current spreading factor as the shortest SF with at least 50% of the received messages (five messages for SF7, SF8 and SF9; three messages received for SF10 and SF11. SF12 is discarded for a correct performance).

Loadsensing Mobile App

Radio signal coverage	
Date	20 Nov 2019 13:16:42
Token	1574252202
Node ID	6905
Network ID	105
Latitude	
Longitude	
SF7	10 / 10
SF8	10 / 10
SF9	10 / 10
SF10	5 / 5
SF11	5 / 5
SF12	5 / 5
<div>BACK</div> <div>NEXT</div>	

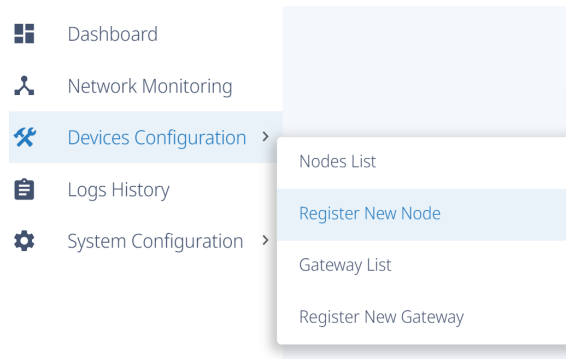
Offline Registration Commissioning Procedure

Offline registration of the node on the data server, without an Internet connection on the Dlog Application, requires two steps. First, the node must be registered on the data server previous to the node connection. Then, the set-up must be done using the Dlog application.




Registration on the data server

The node (or nodes) to be registered has to be registered using a specific password at the data server, at Devices Configuration tab, selecting "Register New Node" option.




NODE ID


122 

Node ID can be found printed on a sticker of the device.

NODE NETWORK PASSWORD

..... 

REPEAT NODE NETWORK PASSWORD

..... 

Register

- Node ID - In this box, the node ID to be registered must be set. A unique node can be registered using at a time
- Node Network Password (and Repeat Node Network Password) - Same as Network password Encrypt on the Dlog Application. The password set in this box is the one to be used in the next step (node commissioning using Dlog application)

Clicking on the Register button will register the nodes at the data server.

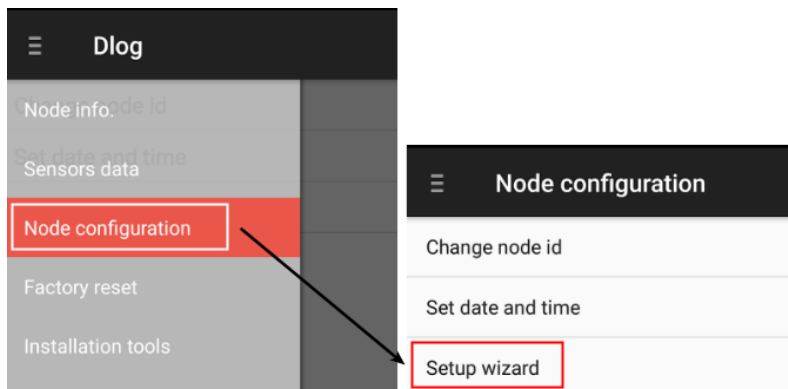
Successful registering can be checked by clicking at Devices Configuration tab, Nodes List option.

+ Register new Node - Unregister selected Node	
<input type="checkbox"/> All	NODE ID
<input type="checkbox"/>	Is-19426
<input type="checkbox"/>	Is-24082

Loadsensing Mobile App (Dlog) Setup wizard

Once the node has been pre-registered, node commissioning procedure is the same as configuration as when doing the online procedure.

1. Connect the node to the Android device and once Dlog application self-launches click Setup Wizard on Node configuration tab.



Note: Node must be battery powered with an internal Switch set to BATT (for powering the node using batteries). Dlog app may ask for node date and time setting, or node firmware version upgrade. Both operations should be done without disconnecting the Android device, to avoid firmware corruption.

2. Configure the **sensor** with the appropriate parameters.
First screen of the setup wizard Sensor Configuration will ask for each channel configuration parameters. Check nodes user guide for more information.

At the end of the sensor configuration, Dlog will display a reading for every configured node to ensure the configuration has been correctly done.

3. Radio configuration

This step will ask to configure all nodes to data server communication parameters.

A- Radio type -> MultiGW

Select this radio type to connect the node against a data server

B- Sampling rate

This feature (not related to radio settings) will allow the available sampling rate for the node. Network size parameters will limit shortest sampling rates for bigger network sizes. Using the smallest Network size available will allow the shortest sampling rates.

Example: At a network size of 901-1800 nodes, Dlog Application will only allow choosing a one hour sampling rate or higher. On the contrary, a 1-15 node Network size will allow 30 seconds sampling rates.

Note: Setting a smaller network size, and setting the shortest sampling rates should not affect the network performance. These features must be correctly set in Loadsensing radio mode only.

C- Region

Select the region depending on which geographical location you are in. Each location will use a different radio configuration, to meet with local regulations.

Note: It is mandatory to choose the same region on the nodes than the region which is the gateway. Otherwise, the gateway will discard any incoming messages from those nodes.

D- Network size

Related to the sampling rate. Network size will limit the sampling rate.

E- Data Server ID

Data server's ID number, provided by Worldsensing.

F- Network Encrypt Password

At this point, the password used to register the node previously at the data server must be set. This will be the password to encrypt data and decrypt it at the data server. Setting a different password will make the data server discard any incoming message.

Note: Network encryption password loss may require commissioning the node again.

Radio configuration	
Radio type	MultiGW (be..)
Sampling rate	1 h
Network Config	
Region	Europe Multi..
Network Size	1-15 nodes
Dataserver ID	105
Device data encryption	
Network encrypt password	random

ls_ids
9336 12455 3695

Network Password
.....

Repeat Password
.....

Register

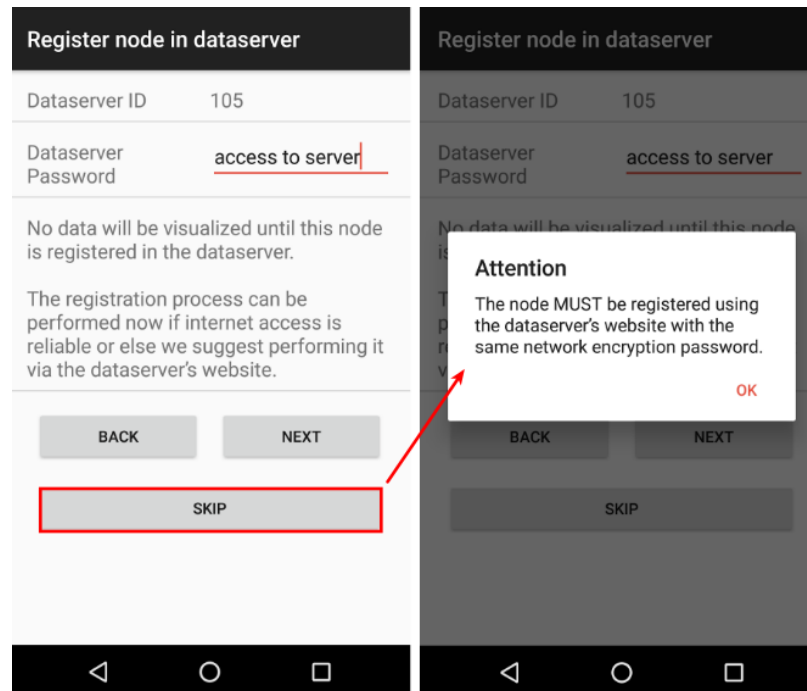
4. Register node in data server

This step has previously been done. Therefore, this step is not required, and the Skip button should be pressed. This option does not require a data server Password to be inserted, as no Dlog-data server direct communications will happen.

Clicking the Next button will show an error as no Internet connection exists on the Android device.

Clicking Skip button the Dlog Application will show an advertisement reminding the need to register the node on the data server (step already done).

Loadsensing Mobile App



5. Coverage test

The next step is to perform the coverage test, as the Dlog Application doesn't have an Internet connection, an Offline Test should be done.

This test will make the node broadcast coverage test messages. In case of being received by one of the gateways, these messages will be redirected to the network server. The network server will redirect all these messages to the data server, which will decrypt them using the network encryption password, parse and store them.

Loadsensing Mobile App

Radio signal coverage		Radio signal coverage	
Server password	xxxxx	Date	20 Nov 2019 13:10:38
<p>Offline test - Perform the coverage test, but do not fetch results from the dataserver. The results can be checked later at the dataserver's website.</p> <p>Next: Perform the test and fetch the results from the gateway in order to show them.</p> <p>ONLINE</p> <p>BACK NEXT</p> <p>OFFLINE TEST SKIP</p>		Token	1574251838
		Node ID	6905
		Network ID	105
		Latitude	
		Longitude	
		<p>This test was performed in offline mode, so the results could not be fetched from the gateway. Write down the Token ID to identify this test, and check the results on the gateway.</p> <p>BACK NEXT</p>	

Dlog application will provide a Token ID. Coverage test results can be checked at the data server by accessing the network and clicking on Signal Coverage Test Map.

Network: 105

/ Networks / 105

Comments

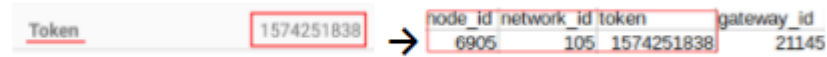
Compacted custom CSV files

Signal coverage test map

A CSV file can be downloaded with the results.

- The node will send ten radio messages on SF7, SF8 and SF9, and 5 messages at SF10, SF11 and SF12. We can define the current spreading factor as the shortest SF with at least 50% of

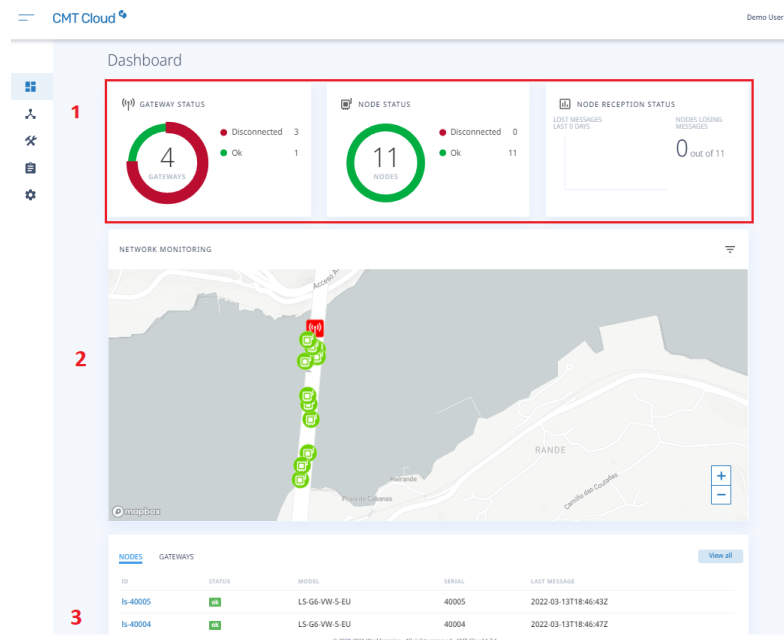
the received messages (five messages for SF7, SF8 and SF7; three messages received for SF10 and SF11. SF12 is discarded for a correct performance).



Data Server Features

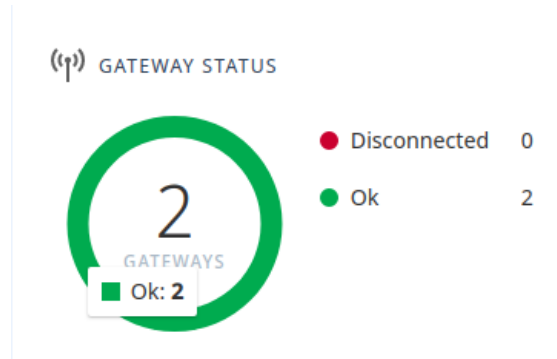
Dashboard

The dashboard shows an overview of the project status as well as the geographical position of the devices if it has been previously configured.

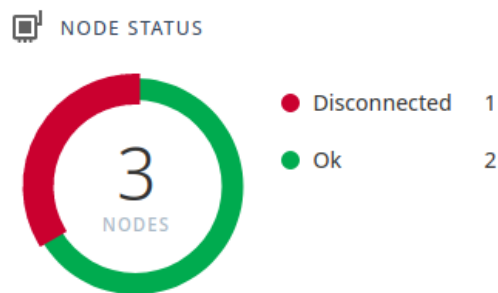


Status graphs: the graphics show the general status of the gateway, the nodes and the lost messages.

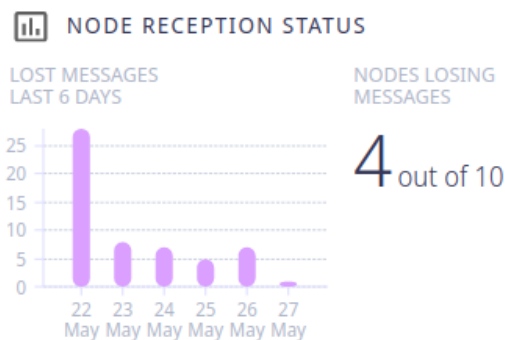
1. Gateway Status: number of gateways connected or disconnected.



2. Nodes status: number of nodes connected or disconnected.



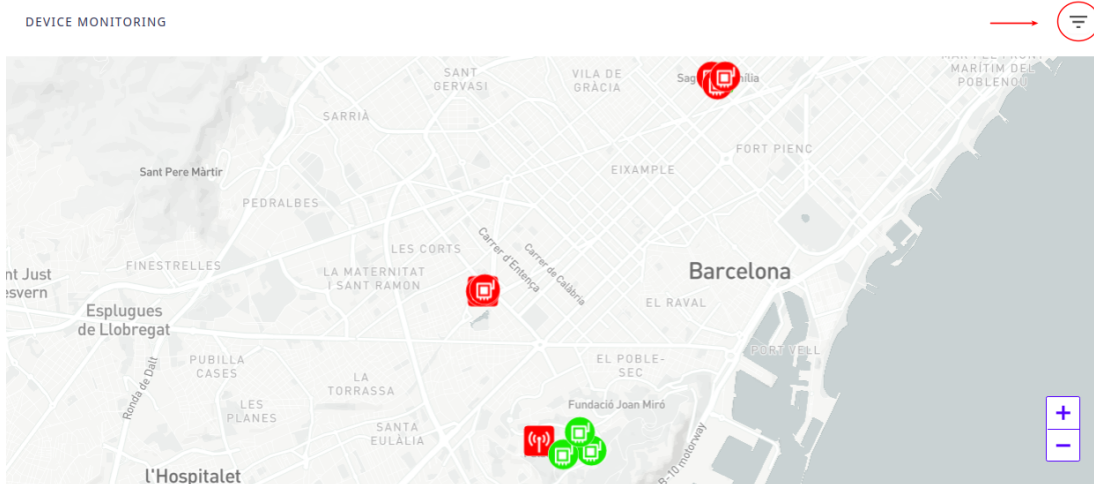
3. Node reception status: number of messages lost in the last 6 days and the number of nodes with data lost.



For more detail about the disconnection or data loss check the Network section or contact the Customer Success department.

Device monitoring: a map with the devices located geographically. To do this it is necessary to perform the online coverage test of the node via the Dlog app or add the location later via API call.

You can filter by clicking on the filter icon at the top right.



Allows you to filter by device (gateway/node) and by status (online/disconnected) Once filtered the map will show us the filters applied and the results.

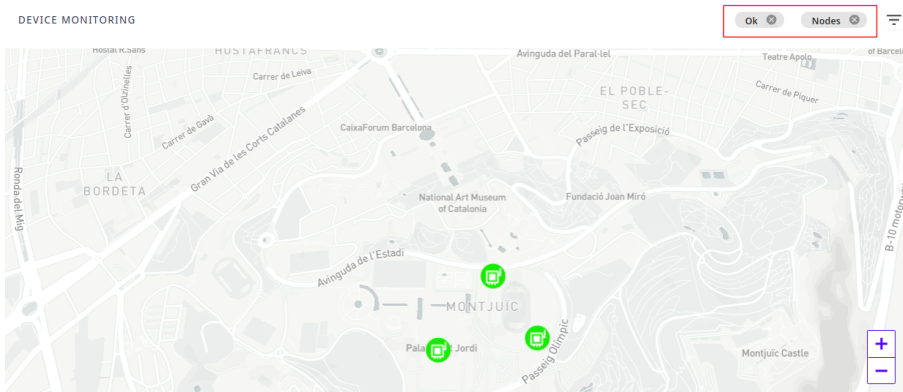
Filter Devices

TYPE OF DEVICES

- ☒ All types
- ☐ Gateways
- ☐ Nodes

STATUS

- ☒ Disconnected
- ☒ Ok



Nodes/Gateway status: information and status of previously registered nodes or gateways (different tabs).

1. Nodes: nodes tab shows ID (SN by default, can be changed), status (OK/disconnected), model, serial number and date and hour of the last received message in UTC

NODES		GATEWAYS		
ID	STATUS	MODEL	SERIAL	LAST MESSAGE
Is-19426	OK	LS-G6-INC15	19426	2020-10-07T14:52:33Z
Is-7060	DISCONNECTED	LS-G6-INC15	7060	2020-10-02T13:52:10Z
Is-24922	OK	LS-G6-INC15	24922	2020-10-07T14:52:57Z

10 rows per page Previous 1 Next

By clicking the View All button it will show the nodes registered list.

2. Gateways: Gateway tab shows Gateway ID, name (not necessary), model, status (ok/disconnected) and uptime.


NODES		GATEWAYS		
ID	NAME	MODEL	STATUS	UPTIME
20791	CSI Test TI GW 2	LS-G7-TI-GW-EU	OK	5d 1h 16m
20790	CSI Test TI GW 1	LS-G7-TI-GW-EU	OK	3d 22h 57m

10 rows per page Previous 1 Next

By clicking the View All button it will show the gateways registered list.



Network


Accessing the network tab, the data server will present all the main characteristics of the network and the nodes connected to the Network.


Network: 302 

/ 302

Comments Network management test
















1 **Compacted custom CSV files**  compacted-custom-readings-302-test-current.dat 

2  Signal coverage test map

Nodes 

Id, name, serial or model

☐ All 0 nodes selected of 11

Id	Name 	Status 	Model 	Serial 
<input type="checkbox"/> 32018			LS-G6-INC15	0
<input type="checkbox"/> 32019			LS-G6-INC15	0
<input type="checkbox"/> 32020			LS-G6-INC15	0
<input type="checkbox"/> 36001	TILT90		LS-G6-TIL90-X	0
<input type="checkbox"/> 40000	Laser node		LS-G6-LASER	0
<input type="checkbox"/> 40001			LS-G6-VW-5-EU	0
<input type="checkbox"/> 40002			LS-G6-VW-5-EU	0
<input type="checkbox"/> 40003			LS-G6-VW-5-EU	0
<input type="checkbox"/> 40004			LS-G6-VW-5-EU	0
<input type="checkbox"/> 40005	Crackmeters		LS-G6-VW-5-EU	0
<input type="checkbox"/> 40006	Piconode		LS-G6-PICO	0

4

Clicking on the pen icon will allow modifying the network name and set comments related to the network.

Edit

/ 302 / Edit

Name

302

Comments

Network management test

Network view features:

1. Monthly Compacted CSV files available to be downloaded
 - Compacted custom CSV files:

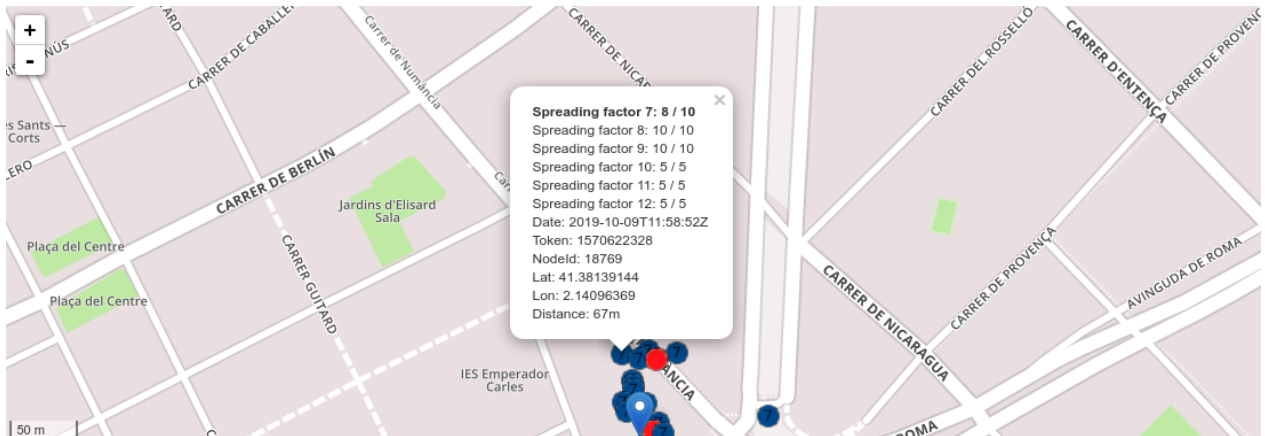
CSV files must be previously configured with the specific data available in all sensors of the network (raw data, engineering units or errors). Several files can be created. The system will feed these files and close them by the end of the month

2. Review signal coverage tests done in a map where results are geographically plotted (requires GPS being enabled at the Android device used for nodes commissioning)
3. Check basic data logger information, such as:
 - Node ID: Same as the serial number by default. It can be modified using the Dlog Android application, for example for replacing a node. A specific tag will inform about the sampling rate status if this one has been modified from the gateway. (Tag will not be shown if the sampling rate has only been modified from Dlog application)
 - In the ID column. A change in the sampling rate is pending
 - In the ID column. The sampling rate of the node has been set through the GW
 - In the ID column. The sampling rate set or pending exceeds the maximum frequency recommended
 - Name (configurable from the data server)
 - Status: Current status of the node, shown using a specific TAG
 - In the status column. Data is received from the node
 - In the status column. No data received from the node on the last day. (Really is 15h ~ 2 healths)
 - Piconode and Analog nodes with sensors powered to 12/24VDC will be marked as Low Battery when sensors are incorrectly powered. This may provoke erratic reading acquisition. In this case, the batteries should be replaced
 - In the status column. The MDT SmartLink sensor connected to the DIG node does have the InitialReading set
 - In the status column. The MDT SmartLink sensor connected to the DIG node does not have the InitialReading set
 - Node model (Firmware coded, can not be modified)
 - Serial number (Firmware coded, can not be modified)
4. Sampling rate of the nodes remote modification

Coverage Tests Page

Clicking on the Signal Coverage TestMap button will redirect the gateway to a map where all coverage tests done are shown in a map. Online coverage tests with GPS location enabled on the Android device are required to show information in this map.

The gateway will be located by a pointer if GPS coverage is available on the installation site, and nodes will indicate coverage using a colour scheme and the detailed results by clicking it.



Note: This map does not show the real (final) node location. Several coverage tests with the same node will display different points related to the same node.

In case of not meeting one of these two requirements (Offline test or No GPS position granted by the Android device), coverage test will not be shown in the map but will appear in the CSV accessible by clicking the test download button.

This CSV file will show all coverage tests, both located and unlocated ones, pointed by Token ID, timestamp, and Node ID.

[Download all tests of this network](#)

Data Logger Page







Clicking over a node ID displays the information related to the data logger or node. Clicking in the pen allows configuring a specific name, setting the installation date and some comments to help to identify the node.

This screen shows monthly readings and health files. Readings files include timestamped rows with all generated readings, and conversion to engineering units if done. Health files store timestamped rows with information related to the node status, like battery voltage or node uptime.

Node 32018

/ 302 / Node 32018

Name	
Installation date	
Comments	
Model	LS-G6-INC15
Firmware version	unkonwn
Serial number	0
Health CSV files	
LS-G6-INC15 CSV files	32018-readings-current.csv + More

Last readings and Time series graphs					
Channel	Temperature (°C) 	Axis A (°) 	Axis B (°) 	ΔA (°) 	ΔB (°) 
1	2822.7	1628.1210	-32.8908	1583.121000	-62.890800 
Received on 2022-03-13T21:11:15Z					
Status					
Metadata					
Last messages					

Different tabs will show different information related to the node:

Last readings and Time-series graphs

This tab displays the last reading for every channel enabled in the node, including engineering units (if configured). Engineering units editor can be accessed by clicking the gear icon and selecting the appropriate formula. Selecting the Graph close to the titles will show a graph of the selected parameter created with the latest 400 readings.

Status

This tab displays the status of the node, the last message received timestamp, a general view of the received vs lost messages, and a list of the radio quality of the latest received messages.

Last readings and Time series graphs			
Status			
Status	OK		
Last status change date	2022-03-02T16:38:11Z		
Monitoring status emails	✓ Yes		
Messages received: today	2626	0	
Messages received: 1 day ago	2975	0	
Messages received: 2 days ago	2975	0	
Messages received: 3 days ago	2973	0	
Messages received: 4 days ago	2975	0	
Messages received: 5 days ago	2974	0	
Total number of messages since gateway installation	521435	670951877	
Note: all messages not received are stored in the node, and can be retrieved with the Android app			
Power			
Date	RSSI (dBm)	SF	Freq (MHz)
2022-03-13T21:01:58Z	-21.0	4	862.300
2022-03-13T21:02:27Z	-21.0	4	862.300

Last messages

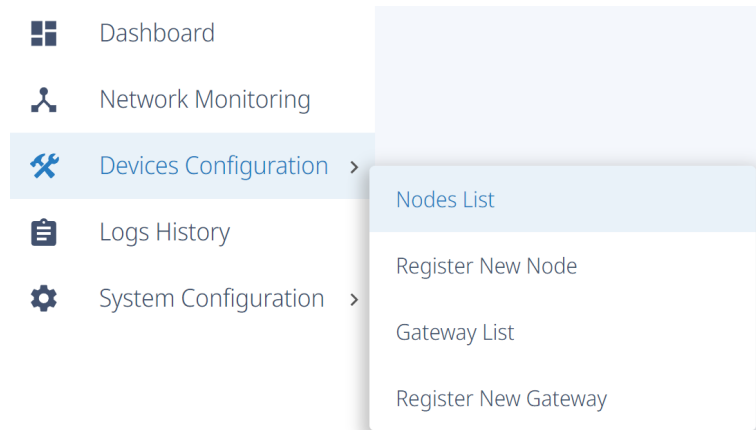
This tab will show the latest received message of each type related to this node.

The received messages can be:

- Reading
- Health (healthV2)
- Coverage test (coverageTestV1)
- Sampling rate modification request (request from gateway) (spstAggCfgV1)

Loadsensing Devices Configuration

The Devices Configuration tab allows registering and unregistering nodes (required for offline node commissioning), as well as associating gateways to the data server for status monitoring. It also displays the relation of registered nodes and linked gateways and their associated status.



Loadsensing Data Loggers Management

Per LoRaWAN requirements, Nodes previous registration in the data server is a mandatory step to do. Otherwise reading messages, incoming from the network server, won't be accepted by the data server.

The data server will only accept, decrypt and manage all those messages incoming from the Network server originated at a registered node.

Two ways of registering nodes are available at this system: Using Dlog Android application (check Online registration commissioning procedure) and directly on the data server.

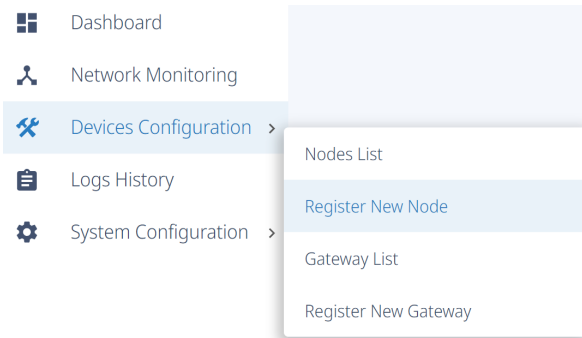
New node registration

Node registration on the data server is done at Devices Configuration tab, by selecting the Register New Node option.

This will allow node registering previously to node commissioning on the field. Even if it is not a mandatory step (it can be done using Dlog application if it has an Internet connection), It can be useful in these situations:

- Lack of internet access: Node commissioning with Android device offline (underground installations, devices without Internet access such as Tablets)
- Security reasons: The engineer in charge of node commissioning should not have the Admin password of the data server.

Clicking at this tab will ask for some parameters:



NODE ID

122

Node ID can be found printed on a sticker of the device.

NODE NETWORK PASSWORD

.....

REPEAT NODE NETWORK PASSWORD

.....

Register

- Node id
Set the list of nodes to be registered. More than one node ID (not serial number) can be set, separated by a blank space, i.e. 9336 12455 3695
- Network password (and Repeat network password)
Set the network password. This password is a random password but must match with the one configured at Dlog application when commissioning it (for more information check "Network

password Encrypt" paragraph).

The section explains this password:

"The same network encryption password used to register the node in the data server MUST be used to configure the node using the Dlog App."

Loadsensing Mobile App

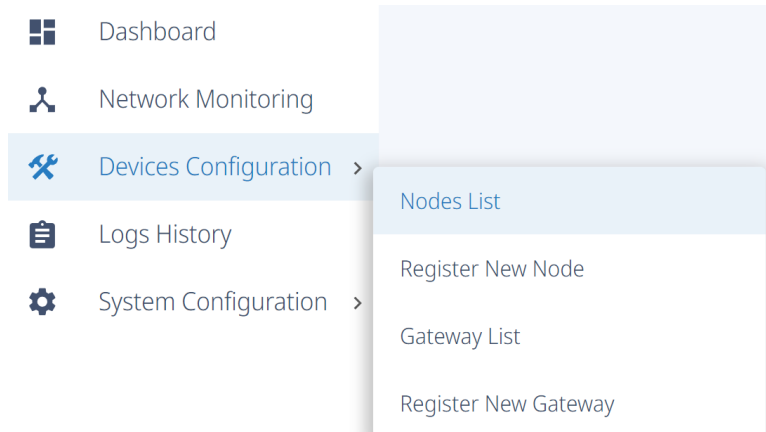
A Successful node registration message will be shown when clicking the Register button.

✓ Successfully unregistered 1 datalogger

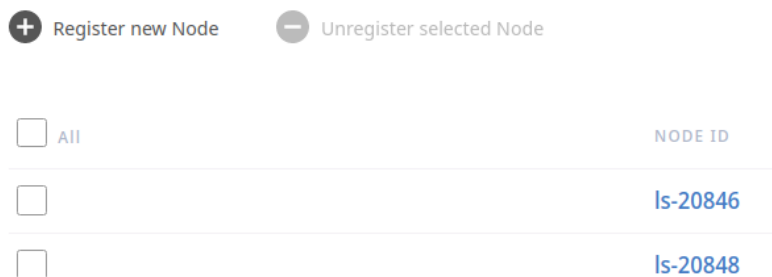
Alternatively, the password can be left blank. In this case, the registration password will be the one configured in the data server (check update Network Password paragraph below).

Nodes List

All the correctly registered nodes will be authorized to send messages to the data server. They can be found listed at the Nodes List section on the Devices Configuration tab.



A list with all the node IDs (not serial number) is displayed.



The Nodes List section explains its performance, showing this message:

- Every time a node is registered, the keys are generated based on the chosen network password and device id of the node
- Only nodes from this list can send data to this network

Also, a node can be deleted by clicking the checkbox, then pressing the Delete Selected button.

When this operation is done, the node will continue sending messages to the data server because it's still configured pointing to that data server, but the data server will reject the data because the node is not in the authorized nodes list.

+ Register new Node
- Unregister selected Node

- All

NODE ID

<input checked="" type="checkbox"/>	Is-19426
<input type="checkbox"/>	Is-24082

+ Register new Gateway
- Unregister selected Gateways

- All

NAME

GATEWAY LINK

<input checked="" type="checkbox"/>	Test Demo	21264
<input checked="" type="checkbox"/>	GW-1	20649
<input type="checkbox"/>	GW-2	20791

✓
Successfully unregistered 1 gateway

Note: Deleting a node from this list does not erase the node from the Network Monitoring list, nor does it erase all the related CSV files. It only disables the connectivity between both sides.

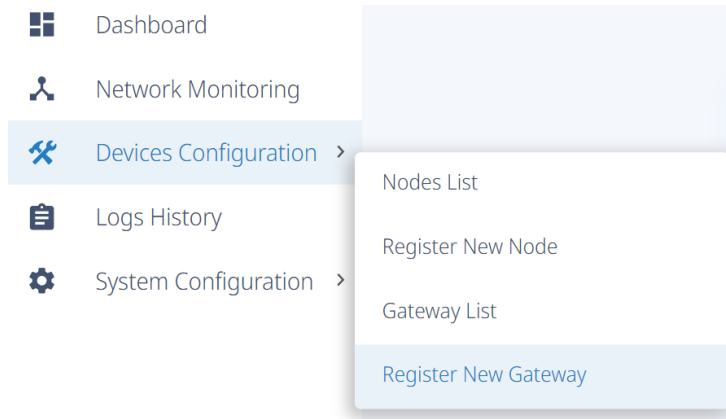
Loadsensing Gateways Management

The data server has the possibility to register the gateway. Linking the gateways to the data server allows monitoring gateways to get the full control of the network. This way the data server will achieve the gateway status information from the network server, where gateways are connected.

Note: This step is not mandatory. Linking a gateway to the data server does not automatically redirect incoming messages to the data server: Nodes are registered directly to the data server, independently of which loadsensing gateway redirects the message.

New gateway registration

All the gateways associated with a project can be registered in the data server at Devices Configuration tab, selecting Register New Gateway.



Gateway connection settings must be entered. This information can be found on the gateway information sheet.

- Gateway ID
- Gateway name: Field with information purposes only. This field will associate a known name to the gateway.
- Gateway password: Web access password for Admin user (the one to access the gateway through loadsensing.wocs3.com/GATEWAY_ID)

GATEWAY ID

12345

Gateway ID can be found printed on a sticker of the device.

GATEWAY NAME

Gateway 1

GATEWAY PASSWORD

.....

Register

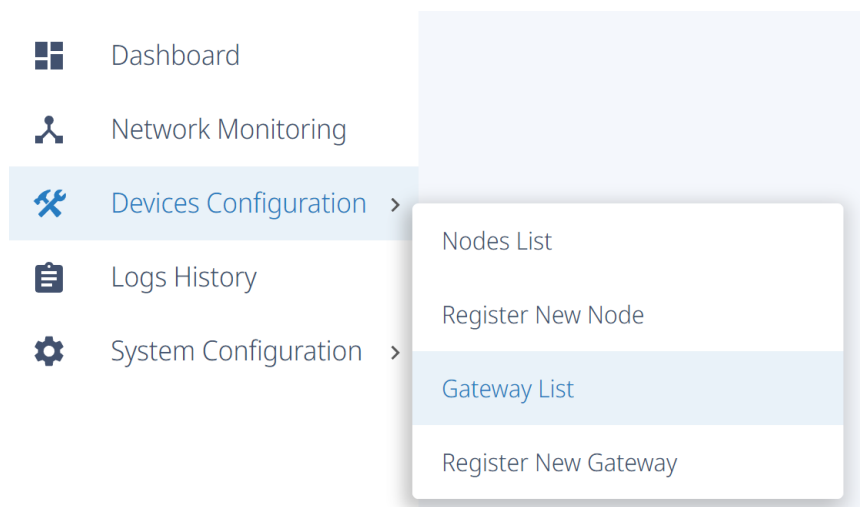
Clicking the Register button shows registration failure or success. In case of successful registration, it shows all the gateways registered with the link to the gateway configuration web.



Gateway List

This section, the data server displays all the gateways previously registered on it with a direct link to its configuration web access and current status. It also allows unregistering them.

This list can be accessed on the Gateway List section on the Devices Configuration tab.



A gateway can be erased from the data server authorized list, by clicking the checkbox of the desired gateway and clicking the Unregister selected Gateways button.

Logs History

Clicking on the Logs item in the Status drop-down menu brings up the Logs interface. On the Logs interface, a historical record of the logs is registered. A typical log is of the following form:

Logs

/ Logs

```
[2019-11-18 13:50:08] User action.INFO: New file created: /var/www/html/public/csv/health/23442-health-2019-11.csv ["anonymous"] []
[2019-11-18 13:57:06] User action.INFO: New file created: /var/www/html/public/csv/laser/23442-readings-2019-11.csv ["anonymous"] []
[2019-11-18 13:57:06] User action.INFO: New file created: /var/www/html/public/csv/errors/23442-reading-errors-2019-11.csv ["anonymous"] []
[2019-11-18 14:02:20] User action.INFO: New file created: /var/www/html/public/csv/health/6920-health-2019-11.csv ["anonymous"] []
[2019-11-18 14:05:32] User action.INFO: New file created: /var/www/html/public/csv/vw/6920-readings-2019-11.csv ["anonymous"] []
[2019-11-18 14:09:11] User action.INFO: New file created: /var/www/html/public/csv/health/6958-health-2019-11.csv ["anonymous"] []
[2019-11-18 14:16:33] User action.INFO: New file created: /var/www/html/public/csv/vw/6958-readings-2019-11.csv ["anonymous"] []
[2019-11-18 14:19:44] User action.INFO: New file created: /var/www/html/public/csv/health/6905-health-2019-11.csv ["anonymous"] []
[2019-11-18 14:25:39] User action.INFO: New file created: /var/www/html/public/csv/vw/6905-readings-2019-11.csv ["anonymous"] []
[2019-11-18 14:38:41] User action.INFO: New file created: /var/www/html/public/csv/health/7648-health-2019-11.csv ["anonymous"] []
[2019-11-18 15:00:54] User action.INFO: New file created: /var/www/html/public/csv/inclinometer/7648-readings-2019-11.csv ["anonymous"] []
```

By default, the most recent log is displayed. Clicking into the drop-down list allows choosing an older log.

Each entry gives information on the status item for such parameters as date, type of file, which action is taken, file path and identity in the following format:

```
[2019-11-18 13:50:08] User action.INFO: New file created:
/var/www/html/public/csv/health/23442-health-2019-11.csv ["anonymous"] []
```

This log will register relevant information like new file creation, FTP client upload errors and low battery alarms among others.

System Configuration

The System Configuration tab allows modifying the data server configuration parameters such as the timezone, monitoring emails receivers list, creating several customs compacted CSV or configuring different ways to send data out of the data server. It also allows configuring a second user and exporting configuration management.

General settings

Timezone

The gateway gets the time and date from the preconfigured NTP server and keeps it thanks to the internal battery. This time is used for readings timestamping, by default in UTC.

However, a different time zone can be configured in the data server interface at System configuration/General. By doing so, readings will be retrieved in UTC and visualized in local time, thus simplifying monitoring tasks.

Note: It is recommended setting the time zone when connecting to the gateway for the first time in order to avoid any timestamp issues with CSV file generation, as explained in data server initial configuration paragraph.

Monitoring notification emails

Several Email addresses can be set in this same area. The selected email addresses will receive different emails advising about the network status. Notifications will provide information related to:

- A status change notification email whenever a node gets disconnected (a node is considered disconnected after no messages have been received for 15 hours)
- A daily reminder of the disconnected nodes, if there are any
- A monthly status report with the status of all the nodes
- A punctual email for every disconnected and reconnected gateway

Hello,

The monitoring service has been set up correctly.

You will now receive:

- *A status change notification email whenever a data logger gets disconnected (A data logger is considered disconnected after no messages have been received for 15 hours).*
- *A daily reminder of the disconnected data loggers, if there are any.*

- A monthly status report with the status of all the data loggers.

Regards

FTP Client Configuration

FTP client tab, permits connecting the data server FTP client against an FTP server to push data from the data server automatically.

Node CSV files are pushed every three minutes at most, while compacted CSV files are pushed every 15 minutes. The most common use of this feature is automatically uploading data to a monitoring server to create and display reading charts, but can also be used for data backup. These are the configurable features of the FTP client:

- **HOSTNAME:** IP or URL of the FTP server where data are going to be uploaded
- **PORT NUMBER:** TCP PORT. 21 by default. It can be changed according to FTP server configuration.
- **USERNAME & PASSWORD:** User and password for login to the FTP server. An anonymous user is also available. ("Use anonymous FTP" must be checked to use an anonymous user, leaving User and Password in the blank.)
- **PROTOCOL:** FTP protocol to use. The data server supports 3 different types:
 - **FTP:** Standard FTP server, without data encryption of communication. We do not recommend sending data through the Internet, except for controlled LAN environment servers or VPN connected networks.
 - **FTPS:** This option allows configuration of data upload to a secure FTP server. It requires an authentication certificate issued by a Certification Authority (CA) such as Thawte, Verisign, etc. All communication is encrypted using SSH protocol.
 - **FTPS (ignoring self-signed certificates).** This option allows configuration of the connection to a secure FTP server with self-signed certificates not issued by a Certification Authority. This option eliminates the display of invalid certificate messages, which should be manually accepted, to allow automatic data upload. This method has the same security level as the FTPS.
- **FTP MODE:** This may be configured in passive or extended passive mode, depending on server configuration. Should you have questions, contact the server administrator or IT department. Most servers are configured in passive mode.
- **OUTPUT:** Select how node readings are to be uploaded to the FTP server. One file per reading can be generated at the server (Create a unique file at every upload), a line for each new reading sent can be added to an existing file (Append to the end of file) or overwrite the file on every data upload (Overwrite every upload). This last method dumps the whole file again in

the case of errors (unable to read the file to be overwritten stored in the server, file writing error, file unavailable, etc.).

- **TYPE OF FILE:** In this area, the files to be uploaded to the server are selected by clicking the appropriate checkbox. Checking a file type enables the Path to upload the file or data. You can set a full path by typing '/', or a relative path (associated with the login user) by typing './' (most common configuration, as it saves the files in the folder assigned by the FTP server). Files can also be stored in specific folders inside the relative path. For example, Health files may be set at ./Health/, while customized files may be set in a different folder ./Customized_readings. All paths must be set without commas.

The file to FTP Server upload process is as follows:

- The FTP client connects to the server and checks the last file or data uploaded.
- It then uploads the latest data (appends to an existing file or creates a new file).
- Should an error occur in the previous step, the reading file is uploaded again, or the full file from the beginning of the month (append mode) is uploaded.

When configuring the FTP client for the first time, the client should test the server connection by uploading a test file and deleting it once the test is done. If this procedure is

completed successfully, the web interface will show a configuration OK message.

Enable FTP ☒

Hostname

Port number

☐ Use anonymous FTP

Username

Password

Protocol

FTP mode

Output

Type of file	Enabled	Full path (starting with /) or Relative path (starting with .)
Health	<input checked="" type="checkbox"/>	<input type="text" value="/"/>
LS-G6-VW data	<input checked="" type="checkbox"/>	<input type="text" value="/"/>
LS-G6-DIG data	<input type="checkbox"/>	<input type="text"/>
LS-G6-VOLT data	<input type="checkbox"/>	<input type="text"/>
LS-G6-PICO data	<input type="checkbox"/>	<input type="text"/>
LS-G6-INC15 data	<input type="checkbox"/>	<input type="text"/>
LS-G6-DIG MDT data	<input type="checkbox"/>	<input type="text"/>
LS-G6-DIG Sisgeo data	<input type="checkbox"/>	<input type="text"/>
LS-G6-DIG GeoFlex/GeoSmart/GeoString data	<input type="checkbox"/>	<input type="text"/>
LS-G6-VOLT DGSI IPI data	<input type="checkbox"/>	<input type="text"/>
LS-G6-LASER data	<input type="checkbox"/>	<input type="text"/>
SHM data	<input type="checkbox"/>	<input type="text"/>
Weather data	<input type="checkbox"/>	<input type="text"/>
Custom compacted data	<input checked="" type="checkbox"/>	<input type="text" value="/"/>

Compacted CSV deployment

The CMT Cloud data server doesn't create a Compacted CSV by default, it gives the option to create several files, maximum 15.

Networks

105 ▼

Filenames

1 ▼

Filename

NewCustomCompacted

Add

Delete

- Networks: Select the network to need to be taken from.
- Filenames: This box shows all the existing files, one must be checked to configure it. To create a new one add a new one at Filename box and click Add, then select it. Select a filename and click Delete to delete it.

- Adding a new column:

- Node: select the node to get the reading from
- Column: Select the variable to store in the CSV
- Header name: The variable name can be personalized
- Press Add and once you finish, press Save

Node 6905 ▼ Column thermResInOhms-6905-VW-Ch1 ▼ Header name 6905-Ohms Add

	Column	Node	Data source	Header name	
↑	1	6905	tInCelsius-6905-Ch1	6905-Celsius	🗑

Save

- Deleting an existing column:
 - Press on the bin next to the existing column

○ Press Save

Node Column Header name

	Column	Node	Data source	Header name
↑	1	6905	tInCelsius-6905-Ch1	6905-Celsius

The time zone used in Compacted custom files is UTC even though a different time zone has been set. Configured time will be applied in node readings and health files.

Error data

In the Custom compacted file, a column can be set to register information related to the errors from each node. This way the reading file won't have any blank space or strange data that can affect your visualization software but you will have the information.

Compacted options

This option allows for changing the maximum number of columns from the default 600 to 1000. This feature has been kept according to CMT Edge system, to ensure compatibility in case of upgrading the system.

Maximum columns

Changing this parameter may corrupt data files on the FTP server if the FTP client functionality is used. In case you are using the FTP, before modifying this value you must:

- Disable the ftp from the FTP client tab
- Rename the current files of your FTP

This function will reboot the gateway. This process can take up to 3 minutes.

MQTT server

The data server has the option of enabling an MQTT pusher under demand on the data server request, available which, when enabling it, sends data to an MQTT broker as soon as the data server receives it. This ensures a real-time visualization of the data.

This is a reliable method to integrate CMT Cloud against a third party software like monitoring platforms.

These are the configurable features of the MQTT broker:

- Server IP / hostname: IP or URL of the MQTT broker where data is going to be sent
- Server port: Port from where the MQTT broker needs to be accessed. The MQTT communication has two ports by default, namely, 8883 which works with SSL security and 1883 which does not use SSL
- Topic: defines the location to which the incoming data belongs on the MQTT broker. Depends on the broker configuration
- Server validation: depending on the server configuration you use your own certificate or upload one to the gateway
- Authentication: login to the MQTT broker that depends on the server configuration. If you use a certificate and key authentication, the certificate and the key must be uploaded to the gateway

This feature will push data received from data nodes to a MQTT server.

Enable MQTT push	<input checked="" type="checkbox"/>
Server ip / hostname	<input type="text" value="35.210.111.196"/>
Server port	<input type="text" value="8883"/>
Topic	<input type="text" value="cmt-test"/>
Server validation	<input type="text" value="No validation"/>
CA certificate	<input type="button" value="Choose file"/> No file chosen
Authentication	<input type="text" value="User + password"/>
Username	<input type="text" value="guest"/>
Password	<input type="password" value="*****"/>
Certificate	<input type="button" value="Choose file"/> No file chosen
key	<input type="button" value="Choose file"/> No file chosen
<input type="button" value="Save configuration"/>	

Check the MQTT annexe for more information and detail.

REST API calls

The data server implements a REST API calls pack which allows sending information in real-time. This feature is enabled by default, and allows, as the FTP client and MQTT Client do, easy integration with third-party software, such as monitoring or management platforms.

Standard API calls

They are organised into three different types:

- Inventory (related to the radio network status and its components, gateway and nodes)
- Data (information received by the gateway related to the latest readings)
- Monitoring (receives data monitoring of network elements, such as lost messages, node uptime, coverage test, etc.)

At the same time, these calls can carry out different actions:

- GET (shows the information required depending on the API call)
- POST (valid only at Monitoring, allows data creation, like GPS location coordinates when offline test coverage is done, to be shown in the coverage test map)

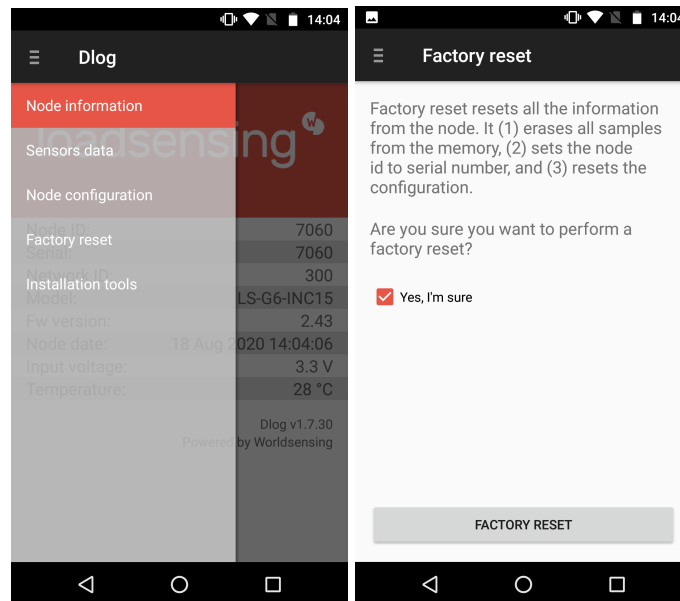
All the related API calls can be found at our knowledge base, in the specific API calls annexe (annexe 03). Ask the Worldsensing Customer Success team for access to the knowledge base.

Troubleshooting

Node Reconfiguration

In case a node needs to be commissioned again, a full reset is recommended to avoid any malfunction or communication issue. This procedure is done by following these steps:

1. Factory reset in the Dlog Application



2. Disconnect the mobile phone from the node (remove the OTG cable)
3. Make sure the node is in BATT mode (battery-powered and not EXT PWR) if it has a power switch



4. Remove all batteries, including RTC

5. Configure the node again from the beginning (put the batteries, set date and time) with the Dlog Application

Other Troubleshooting

For any other troubleshooting contact our support department at <https://worldsensing.com/support>.

CONTACT WORLDSENSING

Need more support? Get in touch with our Customer Success team:

Web: <https://worldsensing.com/support>

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

Want to stay up-to-date about Worldsensing? Sign up for our newsletter:

www.worldsensing.com

Visit our blog for interesting content:

blog.worldsensing.com

Download the latest datasheets and infographics:

www.worldsensing.com/download-center

Follow us online

