

User Guide

Loadsensing CMT Edge

Version 2.9.0

CMT Edge^W



Table of contents

| | |
|--|-----------|
| 1. Purpose | 3 |
| 2. Edge devices network | 4 |
| 2.1 Loadsensing network | 4 |
| 2.2 Network Main Page | 6 |
| 2.2.1 Edge devices list general view | 7 |
| 2.2.2 Operations | 11 |
| 2.3 Edge devices (detail) | 14 |
| 2.3.1 Edge devices general view | 15 |
| 2.3.2 Operations | 19 |
| 2.4 Repeaters devices (detail) | 21 |
| 2.4.1 Repeaters general view | 22 |
| 3. Status | 26 |
| 3.1 Gateway status | 26 |
| 3.2 Logs | 30 |
| 4. Configuration | 31 |
| 4.1 General settings | 31 |
| 4.2 CSV data files configuration | 34 |
| 4.2.1 Creating and deleting a Compacted Custom CSV file | 35 |
| 4.2.2 Adding parameters to an existing Compacted Custom CSV file | 37 |
| 4.2.3 Modifying or deleting an existing parameter | 39 |
| 4.3 Internet configuration | 41 |
| 4.3.1 Interface selection | 41 |
| 4.3.2 Cellular configuration | 43 |
| 4.3.3 Other relevant information | 46 |
| SMTP | 46 |
| NTP | 46 |
| Network watchdog | 47 |
| Required network ports | 48 |
| 4.4 Edge devices network radio (LoRa) | 49 |
| 4.4.1 Disable downlink messages | 51 |
| 4.5 Remote Access configuration | 51 |
| 4.5.1 Passwords management | 51 |

| | |
|--|-----------|
| Administrator user password | 51 |
| View Only user password | 52 |
| 4.5.2 Remote tunnel management | 52 |
| 4.6 Repeater plugin | 54 |
| 4.7 Data Output | 55 |
| 4.7.1 FTP | 55 |
| 4.7.2 Modbus TCP | 62 |
| 4.7.3 REST API Calls | 67 |
| 4.7.4 MQTT Push | 69 |
| 4.8 Maintenance | 74 |
| 4.8.1 Configuration import and export process | 74 |
| 4.8.2 Gateway firmware update | 74 |
| 4.8.3 License manager | 77 |
| 4.8.4 Delete all | 78 |
| 4.8.5 Reboot | 80 |
| 5. CMT Dual Management | 80 |
| 5.1 Tunnel for CMT Dual Management Feature: | 81 |
| 5.2 CMT Dual Management Key Features: | 81 |
| 5.3 How does it work | 82 |
| 6. Good Practices | 82 |
| 6.1 Select appropriate Internet access interface | 82 |
| 6.2 Setting the reporting period remotely | 83 |
| 6.3 Solution deployment procedure (step by step) | 84 |
| Contact Worldsensing | 86 |

1. Purpose

This document describes the content and configuration of the Loadsensing CMT Edge solution.

CMT Edge solution is the piece of software embedded in the CMT Edge gateway, which enables connectivity with edge devices, data storage and Internet connection for remote access or third-party applications.

This is a specific document updated to the specific firmware version 2.7 available only on 4G gateways (LS-G6-KIO-GW). **The 3G Gateways (LS-G6-KO-GW) cannot be updated to version 2.7.** Please look for the specific document if you are using a different firmware version.

This document is divided into three main sections, according to the CMT Edge gateway menu:

- Network: This tab displays the edge devices network, their status and readings.
- Status: Here all relevant information related to the gateway is displayed, as well as all logs registered while the gateway is operating.
- Configuration: The tab where all configurations are done: Internet and radio access configuration, data output for third-party software, etc...

It also describes the most relevant good practices to deploy a Loadsensing CMT Edge system.

More information about this solution is available at our knowledge base at <https://worldsensing.zendesk.com/>, where a specific guide for each gateway model can be found, as well as the quick start guide and other more specific annexe documents.

2. Edge devices network

2.1 Loadsensing network

This is the main page, the one displayed when the gateway is accessed. It can also be accessed by clicking on the "NETWORKS" menu.

It displays the information about the different networks created on this gateway under its Network ID number.

A personalized name may be given to the network under the feature "Name" (see "Network main page" below).

It also displays the number of both active and inactive edge devices, in a green square if active (connected) or red, if inactive (disconnected).

| CMT Edge ^W | | |
|-----------------------------------|-------|-------|
| Networks Status Configuration | | |
| Networks | | |
| / Networks | | |
| Id | Name | Nodes |
| 23466 | 23466 | 1 |

CMT Edge can only have a unique network operative, even though more than one network may appear on the system. This means the software will only accept (receive, process and store) incoming data from a unique radio, the one configured on the "Configuration / Network" tab.

This radio may be modified or re-configured (by modifying the type of radio, password or network ID). In case of modifying these parameters (on the configuration tab or in the edge devices during the network commissioning process), a new network may appear in the software, containing the edge device as disconnected.

All messages received by the gateway with the wrong radio ID will automatically be discarded, and the readings of the edge device broadcasting the messages will not be processed or stored.

CMT Edge^W

Networks

Status

Configuration

Networks

/ Networks

| Id | Name | Nodes |
|-------|-------|-------|
| 23466 | 23466 | 1 |
| 12345 | 12345 | 1 |

*12345 is an incorrect network (not configured on the gateway) with an edge device. This device will not communicate

The Loadsensing CMT Edge is delivered with a default Network ID, which matches with the Gateway ID, and a unique specific password. This information is delivered in the Gateway Information Sheet (GIS), provided with the gateway.

Refer to the specific section for more information about network credentials management.

Finally, clicking on the network ID or name (if available) will display the network where the data can be visualized and the devices can be configured.

2.2 Network Main Page

The network main page is accessible by clicking on the network ID or Name on the previous screen.

By accessing the network, the network menu is displayed, where this information can be accessed:

- 1) Network general information (Name, comments. Check "Operations" tab for more info)
- 2) Compacted custom files of the network
- 3) Signal coverage test map access button
- 4) Edge devices and repeaters detail and reporting period operation buttons
- 5) Copyright and data server version information

CMT Edge ^W

Networks Status Configuration

1— Network: CMT Edge

/ Networks / 23466

Comments Gateway 23466

2— Compacted custom CSV files compacted-custom-readings-23466-Tilt90E_periodical_readings-current.dat

3— Signal coverage test map

4— Nodes

Id, name, serial or model Search

☐ All 0 nodes selected of 1

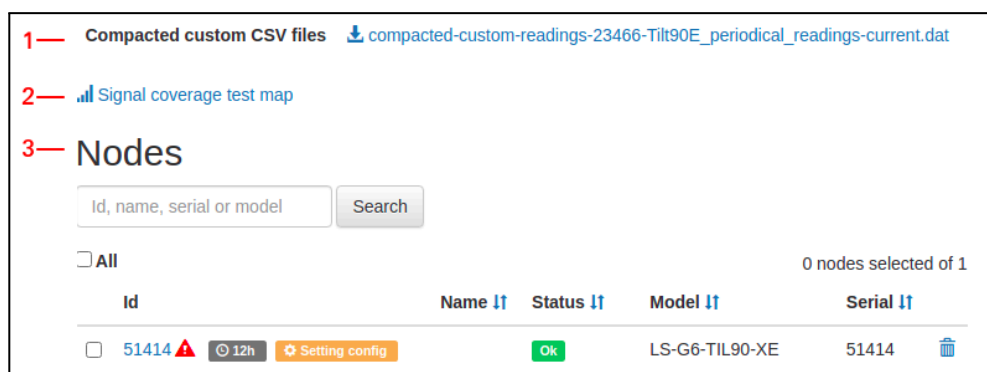
| Id | Name | Status | Model | Serial |
|--|------|--------|----------------|--------|
| <input type="checkbox"/> 51414 12h Setting config | | Ok | LS-G6-TIL90-XE | 51414 |

Change sampling rate Cancel sampling rate changes

5— All rights reserved. WorldSensing © 2021
Version 1.6.9.5

2.2.1 Edge devices list general view

The network main page displays the information related to the edge devices and repeaters connected to the whole network, such as compacted custom files [1], coverage test access button [2] or devices list with relevant information for a quick check [3].

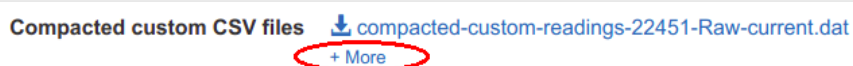


[1] The Loadsensing CMT Edge solution allows configuring monthly Compacted Custom CSV (Comma Separated File) files. This CSV file structure and configuration are explained in the “[CSV Data files configuration](#)” tab. They are available to be downloaded manually to be analysed using a CSV editor (eg, MS Excel or similar), or can be pushed via FTP to an FTP server.

The system will feed the configured files and close them by the end of the month, renaming them with the year and month number, and creating a current file with the readings generated during the current month.

The current month's file will be available for FTP upload, while all older files will remain on the gateway available for direct download.

Up to five compacted CSV files can be created, which will be kept stored until the gateway is flashed again by the Worldsensing operations team, or if the “Delete all” option is applied. The oldest files are zipped to save space on the gateway and hidden. The full list can be displayed by clicking on the + More button



[2] The signal coverage test map button redirects to a new page, where all the results of the coverage tests of that network previously performed using the configuration Android app are displayed (the ones where messages reach the gateway). Results are geographically plotted if the GPS option is enabled in the Android device used to configure the device. A comma-separated (CSV) file is available for download with all results



Clicking on the coverage test located on the map, displays the device ID and all relevant information of the test, such as spreading factor messages received vs sent, location, token and timestamp.

The test will be coloured according to the shortest spreading factor with more than 50% of the messages received by the gateway.

Also, all the results of the network can be downloaded by clicking on the “DOWNLOAD ALL TESTS OF THIS NETWORK” icon, which will download a CSV file. This is especially useful for indoor tests, or those done without GPS location or offline tests. In this case, the Token ID will be displayed in the Android application.

Finally, by clicking on the button “DELETE TESTS” all the tests of the network will be deleted, leaving the map blank.

[3] Devices general overview

In this tab a general overview of all the devices that have been connected to the network is displayed.

Nodes

The search box is now permanently available. By setting the device ID and clicking “Search” the specific device will appear. Leaving the box blank, and clicking the “Search” button will display the full list of devices again.

The “All” checkbox will select all the devices available on the list. This feature may be used to apply changes to all the devices of the list (See operations paragraph)

Finally, a list of devices is displayed. This list can be ordered by any of the columns displayed by clicking on the arrows next to the column








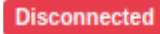
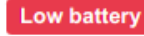


| <input type="checkbox"/> All | 0 nodes selected of 1 | | | |
|------------------------------|-----------------------|--------|-------|--------|
| Id | Name | Status | Model | Serial |

- **ID:** This is the Device ID configured in the device. By default, it is the same as the serial number. It can be modified on the nodes using the Android application, for example for replacing a device. The ID of the Repeaters can't be changed and it will be the same as the Serial Number.

All readings on CSV files are pointed using this parameter.

Several operations can be done with the connected nodes. This may provoke displaying a specific tag (icon) to inform about the reporting period status if this parameter has been

modified from the CMT Edge. The tag will not be shown if the reporting period has only been modified from the mobile application:

-  A change in the reporting period is pending. While the orange label is active, the changes may be cancelled.
-  The reporting period of the device has been set through the CMT Edge.
-  Reporting period Dishonored. The reporting period set or pending exceeds the maximum frequency recommended by the internal algorithm. This may provoke data loss due to messages on air collision and should be avoided.
-  Alarm is active on TIL360-E edge device
-  A change in the configuration is pending for the TILT90-E edge device from the CMT Edge platform.
-  A configuration is set for the TILT90-E edge device from the CMT Edge platform.
- **Name:** It is a text to easily identify the device. This parameter is configurable.
- **Status:** Current status of the device, shown using a specific TAG.
 -  At least one radio message has been received from the device in the last 15 hours.
 -  No radio message has been received from the device in the last 15 hours (no reading message nor 2 consecutive healths).
 -  Piconode and Analog data loggers 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.
 -  Exclusive for the DIG2 data logger with MDT SmartLink sensor connected to the DIG device which **does** have the Initial Reading set.
 -  Exclusive for the DIG2 data logger with MDT SmartLink sensor connected to the DIG device which **does not** have the Initial Reading set.
- **Model** Device model. Firmware coded, can not be modified.
- **Serial number** Firmware coded, can not be modified.

2.2.2 Operations

Three operations are available on this screen; Network configuration, edge devices reporting period management and devices deletion.

CMT Edge Networks Status Configuration

Network: CMT Edge

/ Networks / 23466

Comments Gateway 23466

Compacted custom CSV files [download compacted-custom-readings-23466-Tilt90E_periodical_readings-current.dat](#)

[Signal coverage test map](#)

Nodes

Id, name, serial or model

☐ All 0 nodes selected of 1

| Id | Name | Status | Model | Serial |
|--|------|--------|----------------|--------|
| <input type="checkbox"/> 51414 Setting config | | | LS-G6-TIL90-XE | 51414 |

[1] Clicking on the pen icon allows modifying the network name and setting comments related to the network. This information is displayed on this screen.

Edit

/ Networks / 22451 / Edit

Name Network Name

Comments Comments related to the network.

Changes saved

Network: Network Name

/ Networks / 22451

Comments Comments related to the network.

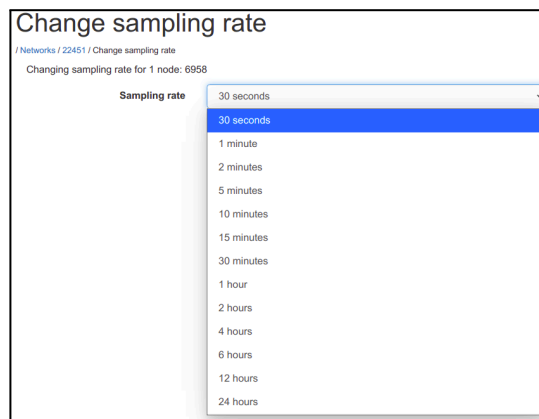
Once the required information is updated, the “Save” button must be clicked. This process will redirect to the initial screen, with the new parameters set and a “Changes saved” message in green.


[2] Remote edge devices reporting period management.


This feature allows setting or modifying the current reporting period of the edge devices connected to the network. The reporting period management can not be applied to a Repeater device.

For this purpose, the required devices checkbox must be marked ("All" checkbox can be used if all the edge devices have to be modified with the reporting period) and the "Change reporting period" button must be selected.

This button redirects to the reporting period configuration screen, where the available reporting periods can be selected.



Clicking on the "Save" button will apply these changes. As soon as a radio message is received from an edge device, the gateway will send the appropriate command to modify the reporting period. During this period the reporting period modification icon will appear in orange, and the operation may be cancelled. 

Once the gateway identifies the reporting period has been modified, the icon will change its color to grey, indicating the reporting period modification has succeeded . At this point, the changes can not be undone. The reporting period can be modified as many times as required.

Depending on the size of the network or the device model, the shortest reporting periods may not be available, in order to avoid data collisions on the network which may provoke data loss. This limitation may be avoided by enabling the checkbox of the message. This way the unavailable reporting periods will be available.

Change sampling rate


/ Networks / 21246 / Change sampling rate

Changing sampling rate for 15 nodes: [View](#)

Sampling rate: 30 seconds

☒ I want to use a higher frequency sampling rate, and I acknowledge that I have read the limitations of sampling rate related to number of nodes in my network, as explained in section 4.1 of the manual

[Save](#)

Devices with the reporting period modified to a higher frequency than the one recommended by the system will be permanently marked with the dishonored icon .

Note: Changing the reporting period using the Android device will not modify the parameters displayed on the gateway.

It is highly recommended to set the definitive reporting period from the gateway interface for all the devices. This procedure confirms that radio communications are OK in both directions (gateway to device and vice versa).

It also decreases the compacted files generation delay, which may be up to one hour, as it optimizes message-sending timings. Any new device should also be configured in this way.

Setting the reporting period from the gateway also optimizes the performance of the whole system.

[3] Device deletion.

Any of the devices on the list can be deleted, either edge devices or repeaters devices. Deleting a device will also delete all related reading, health and error CSV files associated with it. On compacted custom files blank spaces will be registered on the columns related to them.

Devices can easily be deleted by clicking on the bin icon on the left side of the row assigned to it. A popup window will appear asking to literally type **"Yes, delete node"** text to avoid any misclicking.

loadsensing.wocs3.com dice

Are you sure you want to delete this node? Id: 51414

To confirm, write "Yes, delete node" on the box below.

[Cancelar](#) [Aceptar](#)

2.3 Edge devices (detail)

Clicking on an edge device ID or name (if it has been configured before) redirects to the edge device detailed screen. Here the device information is displayed, and data (readings and data logger health information) can be viewed and downloaded, as well as configuring some parameters.

CMT Edge

Networks

Status

Configuration

Node 51414

/ Networks / 23466 / Node 51414

Name

Installation date

Comments

ModelLS-G6-TIL90-XE

Firmware version2.64

Serial number51414

Health CSV files[51414-health-current.csv](#)

LS-G6-TIL90E CSV files[51414-readings-current.csv](#)

Last readings and Time series graphs

| Temp (°C) | X Axis (°) | Y Axis (°) | Z Axis (°) | Alerts Configured |
|-----------|------------|------------|------------|-------------------|
| 24.4 | -1.3733 | 88.6230 | | Yes |

| X Broken Threshold | X Threshold Value (°) | Y Broken Threshold | Y Threshold Value (°) | Z Broken Threshold | Z Threshold Value (°) |
|--------------------|-----------------------|--------------------|-----------------------|--------------------|-----------------------|
| | | Upper | 10.00 | | |

Received on 2021-11-17T10:44:57Z

Status

Metadata

Last messages

2.3.1 Edge devices general view

These are the different items available in the site:

CMT Edge Networks Status Configuration

Node 51414

/ Networks / 23466 / Node 51414

Name

Installation date

Comments

Model LS-G6-TIL90-XE

Firmware version 2.64

Serial number 51414

1

Health CSV files [51414-health-current.csv](#)

LS-G6-TIL90E CSV files [51414-readings-current.csv](#)

2

Last readings and Time series graphs

| Temp (°C) | X Axis (°) | Y Axis (°) | Z Axis (°) | Alerts Configured |
|-----------|------------|------------|------------|-------------------|
| 24.4 | -1.3733 | 88.6230 | | Yes |

| X Broken Threshold | X Threshold Value (°) | Y Broken Threshold | Y Threshold Value (°) | Z Broken Threshold | Z Threshold Value (°) |
|--------------------|-----------------------|--------------------|-----------------------|--------------------|-----------------------|
| | | Upper | 10.00 | | |

Received on 2021-11-17T10:44:57Z

Status

Metadata

Last messages

[1] Edge device information: Some of the information displayed in this area is directly sent by the data logger, such as the Model, Firmware version and serial number.

Some others can be entered manually, such as an Identifier (name), Installation date and other comments.




[2] Edge device CSV files: All devices store different information in monthly files. These files are available to download by clicking them and are stored in CSV format. All readings belonging to the current month are stored in the first file, generally named as DEVICE_ID-FILETYPE-current.csv.

Clicking +More will expand the list of the previous months. The second one containing the information of the previous month will be stored in the same format, with the data in the filename instead of Current, (YYYY-MM), while all other files are stored in a zipped format for space saving.

- **XXXX-readings-ZZZZ.csv:** Stores all readings taken by the data logger at the chosen frequency.
- **XXXX-health-ZZZZ.csv:** Stores all data logger status messages sent automatically every 7 hours. This frequency cannot be changed.
- **XXXX-reading-errors-ZZZZ.csv:** from firmware version 2.1 and above. Some devices may report timestamped errors. These errors may be registered due to out of range situations, unresponsive sensors or other more specific errors reported by digital sensors. (Check the specific edge device user guide for more information.

[3] Last readings and Time-series graphs:

Displays the last readings taken from all sensor channels configured.

| Last readings and Time series graphs | | | | |
|--------------------------------------|--|--|--|---|
| Channel | Temperature (°C)  | Axis A (°)  | Axis B (°)  | |
| 1 | 24.4 | 3.7416 | -2.0514 |  |
| Received on 2021-05-28 02:00:17 CEST | | | | |

In addition, clicking on the graph icon next to each reading will display a graph of the last 400 readings.

If available, clicking the Gear icon at the left will redirect to the Engineering units configuration menu for the device.

[4] Status: Displays relevant information about the device's radio performance.

| Status | | | |
|---|--------------------------|----|------------|
| Status | OK | | |
| Last status change date | 2021-05-10 16:27:12 CEST | | |
| Monitoring status emails | ✓ Yes | | |
| Messages received: today | 3 | 0 | |
| Messages received: 1 day ago | 4 | 0 | |
| Messages received: 2 days ago | 5 | 0 | |
| Messages received: 3 days ago | 4 | 0 | |
| Messages received: 4 days ago | 5 | 0 | |
| Messages received: 5 days ago | 4 | 0 | |
| Total number of messages since gateway installation | 853 | 9 | 11 |
| 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) |
| 2021-05-24 02:27:58 CEST | -72.0 | 11 | 868.850 |
| 2021-05-24 09:27:48 CEST | -74.0 | 11 | 868.100 |
| 2021-05-24 16:27:32 CEST | -72.0 | 11 | 869.525 |
| 2021-05-24 23:27:45 CEST | -72.0 | 11 | 869.050 |

- **Status:** May appear as OK or DISCONNECTED. In case the gateway doesn't receive any radio message for 15 hours (two missing health files) the status will change from OK to DISCONNECTED. When a message is received the status will return to OK.
- **Messages received:** Displays the number of messages received during the last 5 days (per day) as well as the total number of messages received and missed. Depending on the colour, the reason for the data loss will be displayed:



- **Power:** Displays a timestamped list of the radio parameters of the latest received messages:
 - **RSSI (dBm):** Received Signal strength indicator
 - **SF:** Spreading factor
 - **Freq (MHz):** Frequency used to send the message

| Date | RSSI (dBm) | SF | Freq (MHz) |
|--------------------------|------------|----|------------|
| 2021-05-24 02:27:58 CEST | -72.0 | 11 | 868.850 |

[5] Metadata: Reserved. No information is currently displayed on this tab.

[6] Last messages: last messages received from the edge device in JSON format.

4 different messages may be displayed in this area:

- **healthV2** message, containing information related to the health message sent by the edge device every 7 hours, such as battery voltage, device uptime, temperature, etc...
- **coverateTestV1** message. This one contains information related to the coverage tests carried out using the Android application. The Token ID is the most relevant value sent by this message.
- **xxxReadingsVy** message. This message contains information related to the readings done by the edge device, such as the readings themselves and timestamp when it has been done. The name and parameters of this message may vary depending on the type of edge device and a sensor configured/connected.
- **spstAggCfgV1** message. This message is displayed when the reporting period is modified from the CMT Edge user interface. It contains relevant parameters such as the new slot time and reporting period configured by doing this operation.
- **til90EChAggCfgV1** message. This message is displayed when the Tilt90-E edge device configuration is modified from the CMT Edge user interface and it has been correctly applied. The new configuration parameters are registered in this message.

2.3.2 Operations

Several customizations of the device are available on this page, such as edge device info customization and engineering units configuration:

- CUSTOMIZATION:** Main information configuration option is available by clicking the pen icon. This tab opens a submenu where NAME, INSTALLATION DATE and COMMENTS can be added. This menu also allows deactivating the Monitoring status emails, enabled by default. Deactivating this option by selecting “No” in the scroll menu ignores the status of this specific edge device for status reports sent by email. Useful if the logger is definitely disconnected and does not require any specific monitoring.

The screenshot shows the 'Edit' configuration page for Node 7060. On the left, there is a summary card for 'Node 7060' with a red circle and arrow pointing to a pen icon. An arrow points from this card to the main 'Edit' form on the right. The 'Edit' form has the following fields:

- Name:** 12 Bridge
- Installation date:** 2021-05-23
- Comments:** A text area for adding comments.
- Monitoring status emails:** A dropdown menu currently set to 'Yes'.
- Save:** A button at the bottom to apply changes.

The save button must be clicked to apply the changes.

- ENGINEERING UNITS:** All readings taken by the sensors and sent by the edge device to the gateway are sent in raw data. These readings can be converted by the gateway to a configured engineering unit so they can be stored in the CSV files and displayed in the gateway. EG: A Vibrating wire piezometer will send readings in Hertz. The gateway will convert them to digits, and the engineering units option allows converting them to MAMSL or any other required measurement.

The engineering units menu will be displayed by clicking on the gear icon. “USE ENGINEERING UNITS” checkbox must be enabled to allow the configuration options. This step is independent for every channel of measurement.

Engineering units

[/ Networks / 22451 / Node 7060 / Engineering units](#)

Channel 1

☐ Use engineering units

Save

Channel 1

☒ Use engineering units

Formula:

- Angle variation with axes rotation (°)
- Angle variation (°)
- Angle variation with axes rotation (°)
- Change units (tangent formula)
- Change units (sinus formula)

It is relevant to understand that CH0 Logical = CH1 physical. Once the configuration is done, click SAVE. Each type of edge device will display different options. Check the edge device user guide at our knowledge base for more information.

Once configured, engineering units will also be displayed in the Last readings and Time Series graphs, as well as stored in CSV files. (Example of a INC15 Tiltmeter with Axis variation)

| Last readings and Time series graphs | | | | | |
|--------------------------------------|------------------|------------|------------|-----------|----------|
| Channel | Temperature (°C) | Axis A (°) | Axis B (°) | ΔA (°) | ΔB (°) |
| 1 | 26.3 | -7.1810 | 4.7153 | -9.181000 | 3.715300 |

Received on 2021-06-08 02:00:01 CEST

Alternatively, some edge devices will have a gear icon next to the Device customization icon, which will allow specific configurations, such as thresholds in the case of the TILT90-XE device, which allows configuring the Event mode parameters, such as alarm Thresholds and automatic reporting period modification when alarms are triggered. Check the specific Edge device user guide for more information.

Node 51414

[/ Networks / 23466 / Node 51414](#)

2.4 Repeaters devices (detail)

Clicking on a repeater device ID or name (if it has been configured previously) redirects to the repeater device detailed screen. Here the device information is displayed, and data can be viewed and downloaded, as well as configuring some parameters such as name, installation date and comments.

CMT Edge

[Networks](#)
[Status](#)
[Configuration](#)

Node 688

/ Networks / 26016 / Node 688

| | | |
|-------------------|-------------------------------|--|
| Name | Repeater #1 | |
| Installation date | 2022-11-14 | |
| Comments | First repeater of the branch. | |
| Model | RPK20E868HW | |
| Firmware version | 1.0 | |
| Serial number | 688 | |

LS-R6-KIO-GW CSV files
 [688-health-current.csv](#)

Last readings and Time series graphs

| | | |
|---------------------|---------------------------|---------------|
| Uptime | 120 s | |
| Hardware Indicators | CPU load (last 15 min) | 0.2 |
| | RAM usage | 55 % |
| | % Root partition used | 1 % |
| | Root partition free bytes | 6011695 bytes |
| | % R/W partition used | 1 % |
| | R/W partition free bytes | 6011695 bytes |

2.4.1 Repeaters general view

These are the different items available in the site:

| Name | Repeater #1 |
|-------------------|-------------------------------|
| Installation date | 2022-11-14 |
| Comments | First repeater of the branch. |
| Model | RPK20E868HW |
| Firmware version | 1.0 |
| Serial number | 688 |

LS-R6-KIO-GW CSV files [688-health-current.csv](#)

[1] Repeater information: Some of the information displayed in this area is directly sent by the repeater, such as the Model, Firmware version and Serial number.

Some others can be entered manually, such as an Identifier (name), Installation date and other comments.

[2] Repeater CSV file: the repeater automatically sends status messages every 7 hours (this frequency cannot be changed) and is stored in monthly files.

These files are available to download by clicking them and are stored in CSV format. All readings belonging to the current month are stored in the first file, generally named REPEATER_ID-health-current.csv.

Clicking +More will expand the list of the previous months. The second one containing the information of the previous month will be stored in the same format, with the data in the filename instead of Current, (YYYY-MM), while all other files are stored in a zipped format for space saving.

[3] Last readings and Time-series graphs:

Displays the last health message that arrived.

| Last readings and Time series graphs | | |
|--------------------------------------|---------------------------|---------------------|
| Uptime | | 120 s |
| Hardware Indicators | CPU load (last 15 min) | 0.2 |
| | RAM usage | 55 % |
| | % Root partition used | 1 % |
| | Root partition free bytes | 6011695 bytes |
| | % R/W partition used | 1 % |
| | R/W partition free bytes | 6011695 bytes |
| | Gateway input voltage | 12.1 V |
| | Temperature (°C) | No sensor connected |
| | | |
| Networking | Interface configured | ETH0 |
| | IP address | 10.20.20.91 |
| | USB connected | Not connected |
| | VPN connected | Connected |
| Application status | Packet forwarder uptime | 0 h |
| | Repeater daemon uptime | 0 h |
| | MAC layer daemon uptime | 0 h |
| | App layer daemon uptime | 0 h |

Received on 2022-11-14T13:30:30Z

[4] Status: Displays relevant information about the device's radio performance.

| Status | | | |
|---|----------------------|----|------------|
| Status | OK | | |
| Last status change date | 2022-11-11T12:14:42Z | | |
| Monitoring status emails | ✓ Yes | | |
| Messages received: today | 9 | 0 | |
| Messages received: 1 day ago | 16 | 0 | |
| Messages received: 2 days ago | 15 | 0 | |
| Messages received: 3 days ago | 7 | 0 | |
| Messages received: 4 days ago | 0 | 0 | |
| Messages received: 5 days ago | 0 | 0 | |
| Total number of messages since gateway installation | 47 | 0 | |
| 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) |
| 2022-11-13T10:15:47Z | 0.0 | 7 | 868.300 |
| 2022-11-13T10:56:53Z | 1.0 | 7 | 868.300 |
| 2022-11-13T11:37:59Z | 0.0 | 7 | 868.500 |
| 2022-11-13T12:25:17Z | 1.0 | 7 | 868.300 |
| 2022-11-13T15:31:46Z | -2.0 | 7 | 868.500 |
| 2022-11-13T16:33:25Z | 0.0 | 7 | 868.300 |

- **Status:** May appear as OK or DISCONNECTED. In case the gateway doesn't receive any radio message for 15 hours (two missing health files) the status will change from OK to DISCONNECTED. When a message is received the status will return to OK.
- **Messages received:** Displays the number of messages received during the last 5 days (per day) as well as the total number of messages received and missed. Only messages sent directly from the repeater, that is, health messages, are counted. Not those forwarded from nodes or other repeaters.
Depending on the colour, the reason for the data loss will be displayed:



- **Power:** Displays a timestamped list of the radio parameters of the latest received messages:
 - **RSSI (dBm):** Received Signal strength indicator
 - **SF:** Spreading factor
 - **Freq (MHz):** Frequency used to send the message

| Date | RSSI (dBm) | SF | Freq (MHz) |
|----------------------|------------|----|------------|
| 2022-11-13T10:15:47Z | 0.0 | 7 | 868.300 |

[5] Metadata: Reserved. No information is currently displayed on this tab.

[6] Last messages: last message received from the repeater in JSON format.

- **repHealthV1** message, containing information related to the health message sent by the repeater device every 7 hours, such as battery voltage, device uptime, temperature, etc...

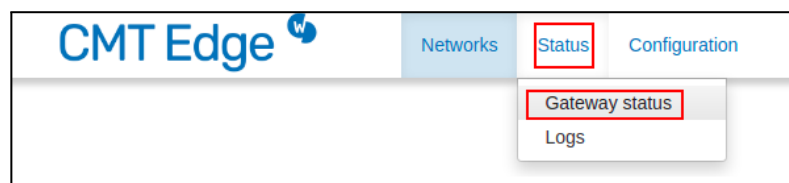
| Last messages | |
|---------------|--|
| Type | Message |
| repHealthV1 | <pre>{ "msgVersion": 0, "diskFree": 6011695, "commMetaData": { "networkId": "26016", "macAddress": "688", "receivedTimestamp": "2022-11-14T13:30:29Z", "frequencyHertz": 868.1, "messageFrames": 1, "snr": 11, "sequenceCounter": [0], "gatewayId": 26016, "rssi": -2, "type": "longRangeRadioMetaDataV2", "sf": 7, "macType": "ETSIIV1" }, "diskUsedPct": 1, "timeDeltaUnits": "seconds", "netip": "10.20.20.91", "vpnConnected": true, "macUptime": 0, "uptime": 120, "temperature": null, "timeDelta": 3, "pktFwdUptime": 0, "nodeld": 688, "repeaterUptime": 0, "fwVersion": "1.0", "type": "repHealthV1", "ramUsage": 55, "appUptime": 0, "diskRwUsedPct": 1, "mainVolt": 12.1, "cpuUsage": 0.2, "readTimestamp": "2022-11-14T13:30:24Z", "nodeModel": "RPK20E868HW", "netIfConfigured": "ETH0", "usbConnected": false, "diskRwFree": 6011695 }</pre> |

3. Status

This paragraph details the STATUS tab at the CMT Edge user interface, where all the status Information is displayed, as well as the event logs register.

3.1 Gateway status

This paragraph, available in the STATUS tab displays all the relevant information related to the gateway main details, applications and connectivity.



The status is automatically self-updated every 5 minutes.

- **General**

Displays general information about the device and the CMT Edge status

- Gateway serial number (coded by Worldsensing, different to manufacturer S/N)
- Gateway model (Identifies the hardware model, as well as the frequency range)
- Firmware version (Displays the current version, it can be upgraded)
- Date: Displays the current time and date set on the gateway.
- Uptime in minutes: Amount of minutes since the gateway was connected or rebooted last time.
- Input voltage: Displays the voltage that powers the gateway. This reading has a precision of +/- 0.35 V.
- Gateway Health history: file named GW_ID-gwhealth-YYYY-MM.csv.
This file contains relevant information related to the device, such as uptime (in minutes), CPU Usage, GPS coordinates, Network interface parameters and general voltage. This information can be uploaded by FTP if required.
- Gateway EUI: The Extended Unique Identifier is a 64-bit unique identifier as defined by IEEE.

- **Application**

Displays information related to the different applications of the gateway, and how they are performing

- Network ID: Displays the current radio network ID configured. It matches with the Gateway Serial Number by default, but it can be modified.
- Internet connection (ping): Indicates whether or not the gateway is able to connect to the Loadsensing servers. Used for connectivity check.
- Status reporting: Indicates whether or not the gateway is able to send status reports to Worldsensing. These reports are sent via HTTP (port 80) to loadsensing.wocs3.com and provide monitoring information of the gateway's status to Worldsensing Technical Support.
- Remote access: Indicates whether or not the gateway is able to open a remote access connection to the Worldsensing server. This Remote access allows the user to access the CMT Edge via web, through [https://loadsensing.wocs3.com/\[Gateway_Serial_Number\]](https://loadsensing.wocs3.com/[Gateway_Serial_Number]), as well as the Worldsensing technical support department remotely for maintenance purposes.

● Network

Displays the parameters configured on the active network interface.

- Selected interface: Displays Internet connection selected (Cellular or Ethernet).
- Ethernet status: Indicates if the Ethernet interface is active (up) or inactive (not connected)
- Ethernet IP and Netmask: Displays the Ethernet configuration in case of being active when monitored.
- Cellular modem status: Same as Ethernet status for Cellular connection.
- Cellular modem IP: IP address assigned to the cellular interface, if enabled.
- Default gateway and DNS servers: Displays associated addresses.

● Cellular Modem

This information is provided by the ISP, it may not be shown even if the interface is active.

- Status: Indicates whether or not the current cellular modem status is correct.
- IMSI: Identification number of a given user in a cellular network.
- Operator: Telecommunication operator used for the cellular modem (ISP).
- Roaming: Indicates whether or not roaming mode is activated on the SIM card (The roaming function is enabled by default on the gateway, to be controlled by the SIM card provider)

- Mode: Indicates the technology (algorithm) used in telecommunications to define the channels and bandwidth to be used.
- Signal: Indicates the signal coverage of the telecommunications operator in percentages.

Gateway status

/ Gateway status

Status checked 1 minute ago

General

| | |
|------------------------|--|
| Gateway serial number | 26016 |
| Gateway model | LS-G6-KIO-GW-868 |
| Firmware version | 2.7.0-Alpha |
| Date | Mon Nov 14 16:05:25 UTC 2022 |
| Uptime (minutes) | 4574 |
| CPU Load | 19% |
| Input voltage | 12.247 V |
| Gateway Health history | 26016-gwhealth-2022-11.csv |

Application

| | |
|----------------------------|---------------|
| Network ID | 26016 |
| Internet connection (ping) | Ping OK |
| Status reporting | Connection OK |
| Remote access | Not connected |

Network

| | |
|-----------------------|-----------------|
| Selected interface | Ethernet - DHCP |
| Ethernet Status | Up |
| Ethernet IP | 10.20.20.36 |
| Ethernet netmask | 255.255.255.0 |
| Cellular modem Status | Up |
| Cellular modem IP | Unknown |
| Default Gateway | 10.20.20.1 |
| Primary DNS | 192.168.1.12 |
| Secondary DNS | 1.1.1.1 |

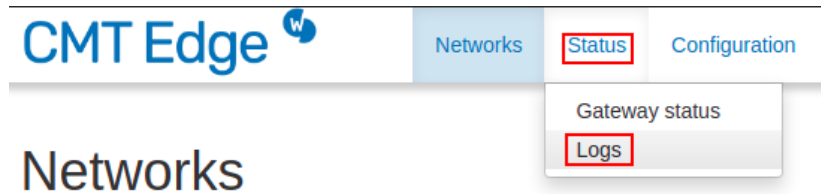
Cellular Modem

| | |
|----------|-----------------|
| Status | Registered |
| IMSI | 214036682390555 |
| Operator | Orange |
| Roaming | Not roaming |
| Mode | HSDPA |
| Signal | 100 % |



3.2 Logs

Logs tab displays registered actions or events, and are selectable by day. A maximum of 10 daily log files are available.



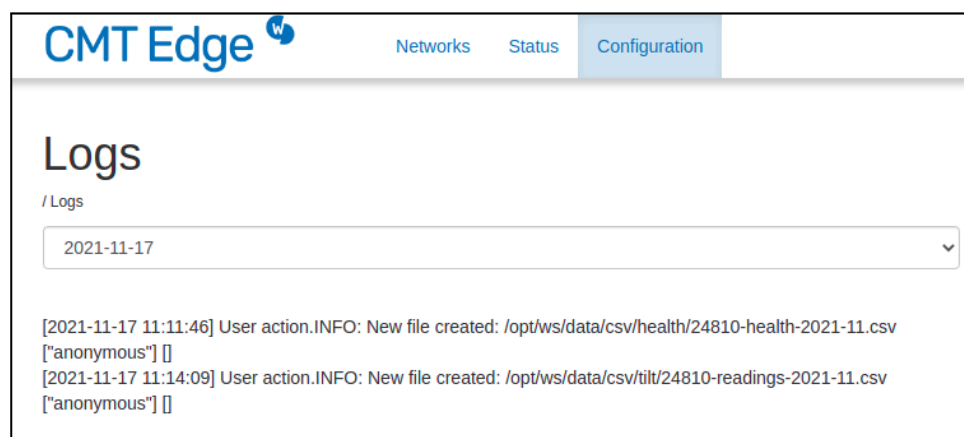
This tab provides information about:

- **System actions:** edge device deletion, time update, geographical area modification...
- **Edge device irregularities:** edge device time synchronization issues, etc...
- **Unsuccessful actions:** FTP data upload failure, etc...
- **Regular actions carried out manually or automatically by the device:** file overwriting on gateway memory, new data file creation, etc.

Records are organized by two types:

- **INFO:** event information.
- **ALERT:** events that should not occur, usually due to some misconfiguration.

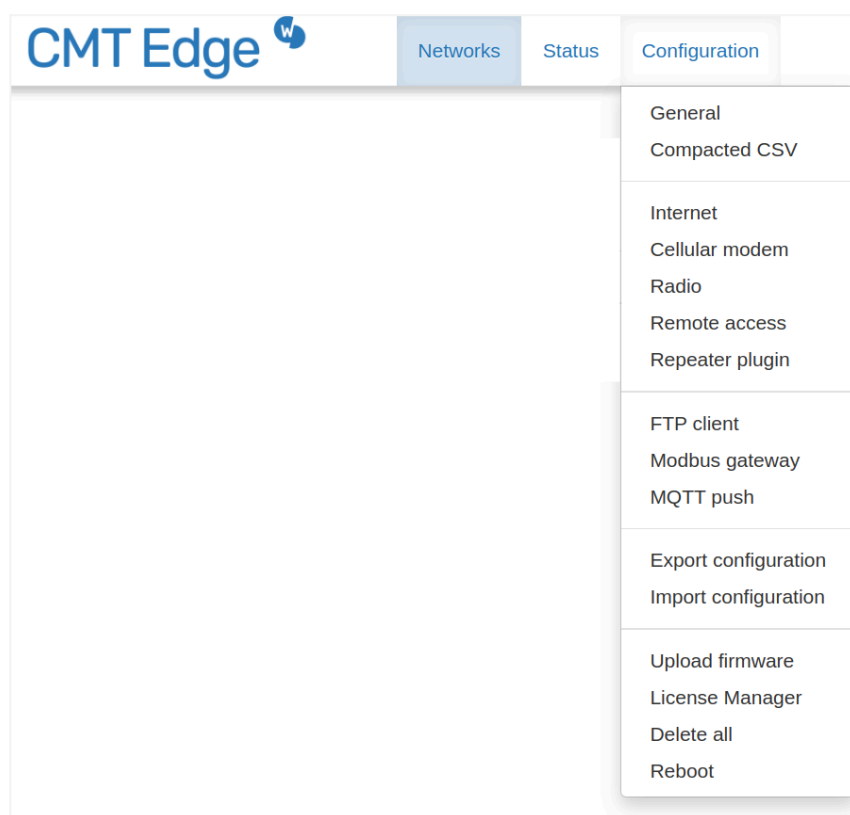
All records are time-stamped in UTC



4. Configuration

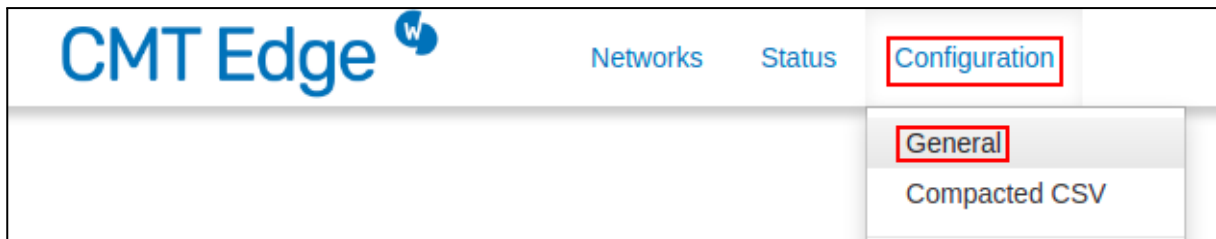
The CONFIGURATION tab displays different gateway configuration options. These options are separated into 5 blocks:

- General configuration: General purpose and CSV configuration
- Communication interfaces: Network interface and radio interface related configurations.
- 3rd party connectivity: FTP, Modbus TCP and MQTT options.
- Export / Import: Configuration management tasks.
- Maintenance tasks: Basic maintenance operations and license manager tool.



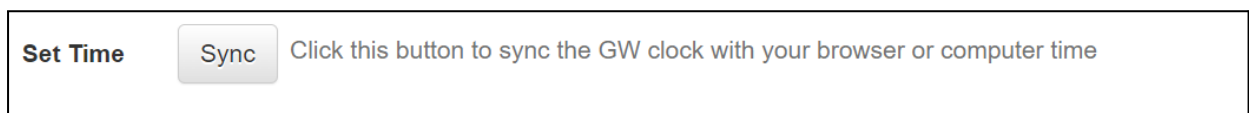
4.1 General settings

This option is available at [Configuration]>[General]. It allows modifying the time zone and configuring the monitoring email list.



The CMT Edge gateway has an internal clock configured in UTC used to register all sensor readings, events and possible incidents. This clock is protected with an internal battery and synchronized via NTP.

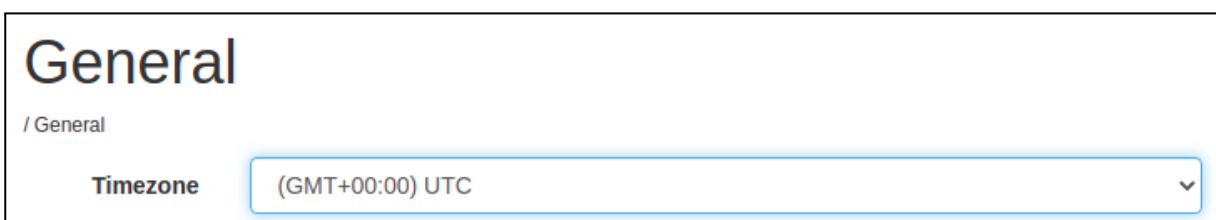
In situations where it is not possible to reach an NTP server because the Gateway is installed offline, it is possible to synchronize the date/time with the computer's browser using the following button.



However, a different **time zone** can be configured in the CMT Edge. By doing so, data will be retrieved and visualized in local time, thus simplifying monitoring tasks.

This time zone modification implies automatic modification of the time zone, as well as summer time modification. This only applies to visualization and csv timestamping, as an internal task of the software. Radio messages are always sent/received in UTC, just like edge devices do.

Worldsensing strongly recommends setting the appropriate time zone during the initial deployment, prior to field installation, in order to avoid any timestamp issues with CSV file generation. Modifying the Time Zone once readings have already arrived to the CMT edge solution modifies future readings timestamp, but previous timestamps remain, creating an inconsistency in the CSV files.



Furthermore, the CMT Edge solution allows sending automatic emails as a monitoring service, by registering mail addresses in the "Monitoring notification emails" section.

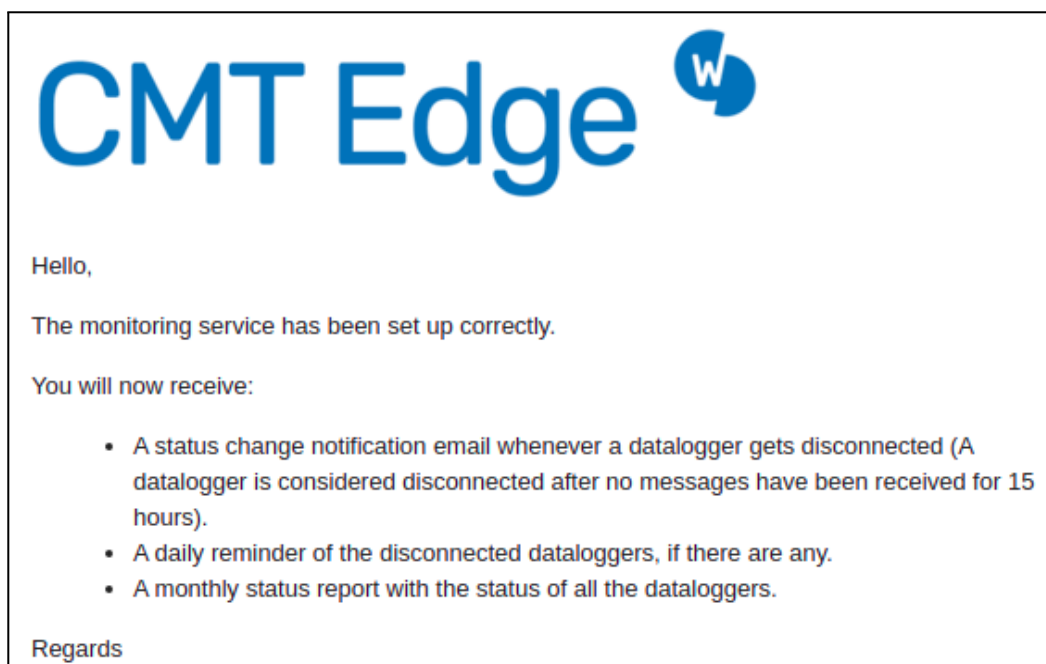
Monitoring
notification
emails

One email per line, without semicolon or commas.

Save

This service is enabled by setting at least one email account, without any account limit. A unique email account should be set per line, without any semicolon or similar icon. By doing this, the email accounts will receive periodical emails indicating the following events:

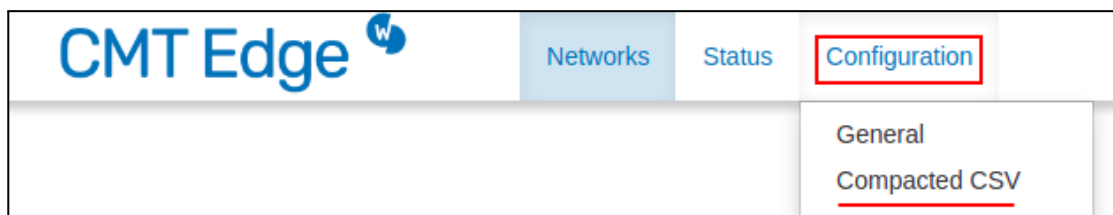
- Notification in case of edge device status change: gets disconnected (after no messages have been received for 15 hours) or connected again.
- Daily reminder of the disconnected edge devices, if they exist.
- Monthly status report with the status of all existing edge devices.



Initial email example

4.2 CSV data files configuration

This tab is available at [Configuration]>[Compacted CSV] tab. It allows creating of up to 5 personalized CSV with any received reading information from any device connected to the network. This includes raw data readings, engineering units converted readings, error messages and repeater health messages. No health information from the edge devices can be added to these files.



These files are complementary to the edge devices and repeaters CSV files already explained in [their section](#). They can be used to mix different data from different devices, to include all readings from a specific area, and type of sensor, or simplify the data output for third-party monitoring software, as it allows header customization. As well as edge device files, these files will be time-stamped using the timezone configured at CONFIGURATION > General tab

Custom-compacted

You can generate up to 5 custom-compacted CSV files by giving each one a unique filename. Select the network you require from the relevant dropdown menu and then add a unique filename. Once the file has been created, the data columns of the different nodes of that network can be configured.

Remember: When new nodes are added to the network you will need to register them on the custom-compacted CSV files. New nodes will not be automatically registered.

Network

22451

Filename

All

Node

6920

Column

Message-type-6920

Header name

Message-type-6920

Add

Add raw

Add eng

| | Column | Node | Data source | Header name | |
|---|--------|------|--------------------------|------------------|--|
| ↑ | 1 | 6920 | AtmPressure-6920-in-mbar | Pressure | |
| ↑ | 2 | 6920 | Message-type-6920 | Error_(msg_type) | |

Save

Once a file is created, it will keep the structure, not adding or deleting columns if a new device is added to or deleted from the network. It will keep the same monthly structure as edge device files do, creating a current file for the current month and renaming it with year-month at the end of the month. These files are displayed at the Network main page. Deleted edge devices will be displayed

as "Unknown" in the devices list, with empty data values being written as no info is available on the platform.

These files may be modified during the entire life of the project. When a specific Compacted custom CSV file is modified, the previous one is closed and renamed as "compacted-custom-readings-<net_id>-<name>-<year>-<month>.change0.dat", leaving the new modified version with the default name, "compacted-custom-readings-<net_id>-<name>-current.dat". Future modifications of this file throughout the current month will apply the same criteria, renaming previous versions as change01, change02, etc.

This process is restarted the next month, creating change0 files again, as the Year and the Month are both available on the header of the file, for fast identification.

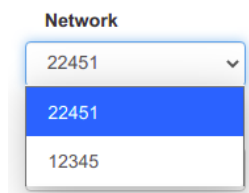
4.2.1 Creating and deleting a Compacted Custom CSV file

This guide explains the steps to create a new CSV file

1 Network selection

Each file is associated with an existing device's network. Even though a unique network may be enabled on the system, this can be changed in Radio settings, for example, to create a new network keeping readings from an older installation in the CMT edge platform.

The required network must be selected on the Network box, where all existing networks are available.



2 File name creation

Click on the + icon next to the filename list. A pop-up window will appear requesting the name for the new file. Click Accept to create the new file.

Network
22451

Filename
All

loadsensing.wocs3.com dice

Please enter the new filename

New Example File

Cancel Acceptar

Note: The filename is limited to a maximum length of 30 characters. We suggest using Roman alphabet characters without accents.

Immediately a blank new file will be created and displayed in the file list. Any blank spaces will be underscored, to minimize integration issues.

Filename

New_Example_File

New_Example_File

All

ENG-Units

Raw

This way, a new File has been created (New_Example_File)

3 Deleting a file

Deleting a file requires two steps; Selecting the network the file belongs to (step 1) and clicking - icon. A new window will pop-up asking about the task to be done. Accept button must be clicked to delete the file.

Network
22451

Filename
New_Example_File

loadsensing.wocs3.com dice

Are you sure you want to delete this custom-compacted file?

Cancel Acceptar

Once any of these procedures is completed, a green message will be displayed indicating the operation has been successfully done.

Filename configuration succesful deleted

4.2.2 Adding parameters to an existing Compacted Custom CSV file

Once the file has been created, the next step is adding all required readings (both raw or converted) or error messages. First of all, an existing CSV file must be selected. Automatically all available devices ID of that network and the selectable parameters will appear in a drop down form

The screenshot shows a web interface for configuring a CSV file. At the top, there are three dropdown menus: 'Node' (set to 6920), 'Column' (set to 'AtmPressure-6920-in-m...'), and 'Header name' (set to 'AtmPressure-6920-in-m'). To the right of these are three buttons: 'Add', 'Add raw', and 'Add eng'. Below this is a table with the following headers: 'Column', 'Node', 'Data source', 'Header name', and a trash icon. The table is currently empty. Below the table, there is a text box that says 'Empty custom column list. Add columns using the form above.' and a 'Save' button.

This form contains these parameters:

- **Node:** The Edge device or repeater ID of the devices available on the network
- **Column:** It contains all the available variables to store in the CSV file. Same column name as present in the corresponding readings or health CSV file.
- **Header name:** Box to assign a name to the header for the column of the variable selected. Blank spaces will be replaced by an underscore. Same as the column field by default.

Once a variable is selected and configured, the Add button must be clicked.

Filename

New_Example_File

+

-

Node

6920

Column

tInCelsius-6920-Ch1

Header name

tInCelsius-6920-Ch1

Add

Add raw

Add eng

| | Column | Node | Data source | Header name | |
|---|--------|------|---------------------------|------------------|--|
| ↑ | 1 | 6920 | freqSqlnDigit-6920-VW-Ch1 | 6920-Ch1-Digits | |
| ↑ | 2 | 6920 | tInCelsius-6920-Ch1 | 6920-Ch1_Celsius | |

Save

Alternatively, all RAW readings from the edge device or the repeater, or all engineering units of the edge device previously configured on the CMT Edge platform can be selected by clicking “add raw” or “add eng” buttons. This option will add all the selected parameters with default header names, which can be modified later.

In this example, Add Eng button has been clicked, adding all the engineering units configured for the Edge device 6920, a 1-channel Vibrating Wire data logger.

Node

6920

Column

tInCelsius-6920-Ch1

Header name

tInCelsius-6920-Ch1

Add

Add raw

Add eng

| | Column | Node | Data source | Header name | |
|---|--------|------|----------------------------------|----------------------------------|--|
| ↑ | 1 | 6920 | atmPressureSeaLevel-6920-in-mbar | atmPressureSeaLevel-6920-in-mbar | |
| ↑ | 2 | 6920 | p-6920-Ch1 | p-6920-Ch1 | |
| ↑ | 3 | 6920 | tInCelsius-6920-Ch1 | tInCelsius-6920-Ch1 | |

Once all the required parameters have been added to the CSV file, **SAVE** button must be clicked to save the configuration. This will automatically create the CSV file. This file may not be immediately available on the edge devices network page, it will appear as soon as enough readings arrive to the platform to create a new timestamped line on a new CSV file. This process may take up to one hour if reporting periods of the devices have not been remotely set from the platform.

A green bar will be displayed if the process has been completed.

Changes saved

4.2.3 Modifying or deleting an existing parameter

Any CSV can be modified after it has been created by the user, adding, deleting or modifying the order or the header name of any of the existing parameters.

Adding and deleting a parameter (column) of the CSV file

A new parameter can be added following the steps in the previous paragraph. Once created, it can be deleted by clicking the Trash icon in the right side of the parameter.

A message must be accepted to apply changes.

loadsensing.wocs3.com dice

Are you sure you want to remove this column?

Cancelar

Aceptar

Modifying a parameter name (column header name) of the CSV file.

A column may be modified by clicking the pen icon next to the trash icon at the right side of the parameter to be modified. Any blank space will be replaced by an underscore.

loadsensing.wocs3.com dice

Please enter the new header name (max. length 30)

New Header Name|

Cancelar

Aceptar

Modifying the parameter order (column order) of the CSV file.

Any parameter can be moved to any position if required. This will modify the order of that specific parameter at the CSV file. This configuration is done by clicking the selected

parameter and moving to the desired position. This step may require doing it in several steps in long CSV files.

Note: Modifying the order or header name, and deleting any parameter from an existing CSV will alter its structure, which may affect any integration done with a third party software, if this compacted custom CSV file is uploaded.

Finally, once all required modifications are done, "SAVE" button must be clicked. A "Changes saved" green bar will be displayed, and the list of parameters of the CSV file will be updated. Otherwise the changes will be lost once another operation is done.

Changes saved

4.3 Internet configuration

The Internet configuration option is available in the [CONFIGURATION] > [Internet] tab.

It allows selecting the interface the gateway will use to connect to the Internet. It can be done via Ethernet physical interface using an ethernet cable with an RJ-45 connector (either LAN or WAN) or Cellular, by inserting a SIM card.

4.3.1 Interface selection

By default, the interface selection is set on automatic mode.

Network connection:

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

The gateway is factory-configured to communicate with the Internet as fast as possible. When booting, the device will try connecting to the Internet by using the Ethernet configuration using a DHCP configuration. In case the Ethernet connection (link) is not detected, it will switch to Cellular interface, by connecting to a mobile network using the SIM card with a default configuration and PIN number deactivated. An APN database is stored in the internal memory, the device will select the most appropriate one and try to connect. In case of not connecting to any network, the gateway will remain standalone, without internet connection.

Internet communication is available with this setup. However, this configuration is not the most appropriate one. Worldsensing recommends configuring the deployed interface once the gateway has connected to the Internet in automatic mode, or in a previous step using the local interface for the initial setup. (Check gateway user guide at our knowledge base)

This modification is done at the Network connection option, by selecting the Manual configuration, and selecting the deployed network.

Network connection:

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

Network connection

- Automatic (default)
 - The network connection mode is automatically configured upon gateway startup.
 - The device will configure the Internet connection as described in the previous paragraph.

- Manual Configuration.

Note: This setting overrides auto-detection and launches the selected connection type.

- Cellular modem
 - Launches a cellular connection with the settings configured in the CONFIGURATION > CELLULAR MODEM.
 - Ethernet interface is deactivated but can be used for feeding the device with a PoE injector.
- Ethernet with DHCP
 - Ethernet interface is deactivated but can be used for feeding the device with a PoE injector.
 - Receives an IP automatically from an existing DHCP server on the network.

Note: This option is the easiest to configure for an Ethernet interface but it may not be ideal for connecting directly to the gateway in a LAN environment, as the IP address may vary. Dynamic IP addresses may affect any routing or firewalling configuration, such as port forwarding. Static IP address configuration is recommended for this kind of installation.

- Ethernet with Static IP
 - This mode requires manually setting of the network parameters:
 - IP address
 - Subnet mask
 - Default gateway
 - DNS servers

Once the changes on this web have been made, it is required pressing the “SAVE CONFIGURATION” button and applying a reboot of the device. Otherwise the previous configuration will remain, even if it has been saved.

4.3.2 Cellular configuration

The cellular modem configuration tab contains some configuration parameters specific to this type of connection.

Note: This tab should be checked when deploying a cellular interface only, if required. This configuration is applied whenever a Cellular connection is used, regardless of whether it was the result of an automatic or manual configuration in the Internet tab.

Cellular modem

/ Cellular modem

☒ 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

Roaming is allowed by default. If you want to block the connection via roaming, please contact your telecommunications service provider to disable the roaming. Changes will not be applied until next device reboot.

Save configuration

In case the Gateway suddenly loses connection to the Internet via cellular modem and it is located in a network where a 3G shutdown is in process, a workaround is possible via Advanced APN Settings. It is strongly recommended to contact the customer support team and check related documentation before proceeding. [Advanced Modem Configuration](#)

These are the options available to configure in this tab:

- **PIN** (personal identification number) setting
 - Off (selected by default)
 - The gateway will not attempt to unlock the SIM card.
 - The cellular connection will fail in case the SIM card is PIN protected
 - On
 - This setting allows configuring the PIN code for a PIN-locked SIM card.

- **Important:** the gateway will automatically attempt to unlock the SIM card. In case the configured PIN and the real one are different, the SIM card will get blocked once the system exhausts the three possible attempts.
 - There is no way to enter the PUK code in the gateway. A PUK-locked SIM card needs to be installed in a mobile device for unlocking.
- **APN** (access point name) settings
 - APN Auto selection (default)
 - Every mobile operator requires a specific configuration for connection to its network. The CMT Edge gateway has a database with hundreds of operator configurations worldwide. The CMT edge will try to recognize and configure the SIM card connection accordingly.
 - The configuration may be wrong for non-standard and some other operators not available on the list.
 - Manual APN configuration
 - This setting allows manual input of the mobile operator configuration values.
 - This feature should be used in case auto-selection does not configure the connection properly.

Important: roaming is allowed by default in the CMT Edge gateway. This feature can not be disabled in the device, it should be blocked on the service provider side to avoid using this feature, which may incur on unwanted expenses.

Cellular modem

/ Cellular modem

☒ 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

Roaming is allowed by default. If you want to block the connection via roaming, please contact your telecommunications service provider to disable the roaming. Changes will not be applied until next device reboot.

[Save configuration](#)

In case the Gateway suddenly loses connection to the Internet via cellular modem and it is located in a network where a 3G shutdown is in process, a workaround is possible via Advanced APN Settings. It is strongly recommended to contact the customer support team and check related documentation before proceeding. [Advanced Modem Configuration](#) ←

The advanced modem configuration can be used in those cases where the 3G has been shutdown and the Gateway lost connection to the internet via the cellular modem.

The procedure to enter the APN in these cases is first from the menu Configuration -> Cellular modem set the APN to Manual APN configuration, then enter the APN parameters (APN name, etc.), and save the configuration.

Once it is saved, then get into the Cellular modem menu again and click on Advanced modem configuration, and enter the same APN settings again, and save the configuration.

Then disconnect the LAN cable from the gateway that you may have connected and reboot the GW.

For support on how to configure this feature, please contact support@worldsensing.com.

Cellular modem

/ Cellular modem

Advanced Modem Configuration

This page should be only used under the Worldsensing permission. Be sure that the SIM is inserted in the gateway and reboot it before executing the following fixes:

- APN Fix: Update the APN hostname to the modem.

After submitting it is recommended to reboot the gateway.

There is no previous APN configured.

Insert APN: [Apply Changes](#) [Reset](#)

4.3.3 Other relevant information

Some other parameters and features are available on the CMT Edge, which can be configured to personalize the system according to the requirements of the deployment.

SMTP

CMT Edge uses a preconfigured SMTP configuration to send monitoring emails to the list of email addresses configured at GENERAL tab.

This configuration is available at [CONFIGURATION] > [INTERNET] tab, at SMTP Server option:

SMTP server:

☐ Default (Internet service)

☒ Custom

SMTP Server:

Port:

"From" email address:

Use TLS/SSL: ☐

Use Authentication: ☐

Username:

Password:

The platform allows setting a custom configuration of this parameter. This way, the monitoring emails will be sent from the configured email address instead of being sent by a Worldsensing account, which has been specially deployed for this specific CMT Edge instance.

This configuration requires the "Save configuration" button to be clicked and the gateway rebooted to take effect.

NTP

Each CMT Edge instance periodically synchronizes with a NTP (Network time protocol) server to have the date and time updated. This is required to display and register readings correctly.

This server can be configured at [CONFIGURATION] > [INTERNET] tab, at NTP Server option. It can be configured to use a different NTP server, which may be useful in offline deployments (where the system is not Internet connected), by selecting the local network NTP server IP address.

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

☐ Default (pool.ntp.org)
☒ Custom

NTP Server:

This configuration requires the “Save configuration” button to be clicked and the gateway rebooted to take effect.

Worldsensing recommends leaving this parameter by default for Internet connected deployments.

Network watchdog

The Internet interface (both ethernet and cellular) are by default protected by a watchdog. This network watchdog monitors the status of the Internet connection by triggering a controlled gateway reboot, which will close and restart correctly the gateway, restarting the Internet access connection.

This watchdog is triggered when the CMT Edge identifies a connectivity issue. The CMT Edge pings every 5 minutes to Worldsensing servers. In case of not receiving a positive response during 8 consecutive tries, this means, 40 minutes, the reboot is triggered.

CMT Edge^W

[Networks](#)
[Status](#)
[Configuration](#)

Internet

/ Internet

☒ Activate network Watchdog

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

This feature should be deactivated ONLY in offline deployments, as the system will not be able to ping external servers.

It increases the reliability level, specially for remote installations, as it minimizes the Internet access issues due to device malfunction.

Required network ports

The CMT Edge gateway requires some generic ports to be open for a normal performance. Also some other ones may be required for specific features, such as integration with third party software.

Most of these ports are open by default in most of the networks, and the user should not face networking issues in most of them, but in managed networks these port openings may be required to the IT department.

Cellular networks normally allow communicating through these ports without any other configuration.

- **TCP 80** (HTTP port): This port is required for gateway monitoring. The gateway will periodically send a message to the Worldsensing monitoring platform with relevant information, such as input voltage, messages received/lost, CPU and RAM usage, etc...
This information is available for Worldsensing Technical support department, which is useful for troubleshooting in case of raising an incident in our support platform.
- **TCP 443** (HTTPS port): This port is the one used to access the gateway via the web. Also used for REST API call integrations.
- **UDP 1194** (VPN port): This port is used to enable remote access. Check the Remote Access Configuration paragraph for more information.
- **UDP 123** (NTP port): Required for time synchronization. May use an internal address for LAN environments.
- **TCP/UDP 53** (DNS): require to translate domain names to IP addresses.

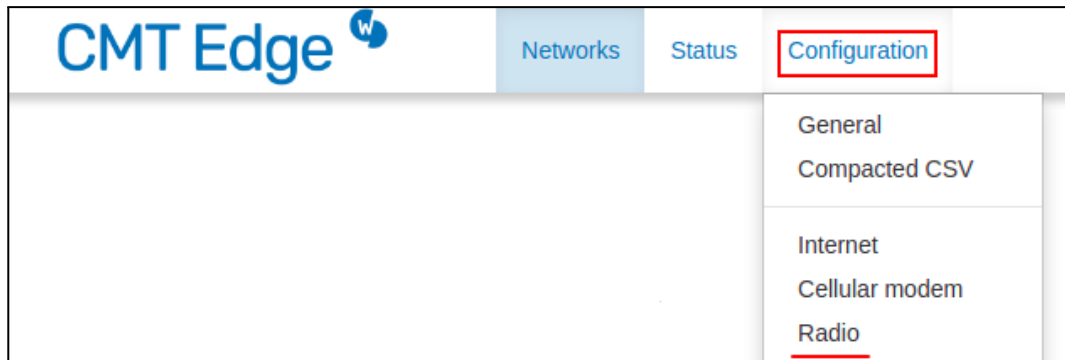
Other ports may also be required depending on the project requirements.

- **TCP 502** (Modbus TCP): Required for Modbus TCP communication with third party software.
- **TCP 21** (FTP): Required for FTP communication with third party software. This port is configurable by the user at the FTP client.

Note: More ports may be required to be open depending on the FTP configuration.

4.4 Edge devices network radio (LoRa)

This page allows configuring Wireless Sensor Radio Network parameters.



There are three different gateway models, with different radio models available, according to the geographical areas where they may be placed. The radio model will be selected based on the local regulations defined by the country where the device will be located.

For some countries, an advanced menu may be displayed. This refers to the possibility of choosing one of the multiple channel groups available for data transmission. A group, usually 0, is set by default, but it can be modified on each gateway. This configuration may avoid or minimize data packet collisions in environments where several gateways are communicating with large amounts of edge devices at high reporting periods, as each group of edge devices will communicate with the gateway in different frequency groups.

Note: changing the default configuration, even the channel group at advanced options, requires modifying these parameters at the edge devices during the setup using the Android application. Otherwise, the CMT Edge gateway may not receive the radio message, and data will not be registered on the system.

Network type, ID and password must match at both CMT Edge and edge devices.

The available parameters to configure are:

Country and frequency (Network type)

- Varies depending on the gateway model. Check the appropriate radio model according to the country regulations.

- Depending on the network model, different channel groups, channels or specific spreading factors may be chosen.

☐ 866I
☒ Europe

Changes will not be applied until next device reboot.

Change Country and frequency

- **Network ID**

- It is a numeric identifier for the wireless sensor network.
- Same as the Gateway Serial number by default.

- **Network Password**

- This password is used to encrypt all data in transit on the Wireless Sensor Network.
- The default factory password is printed on the Gateway Information Sheet.

Network ID:

Network Password:

Show Password ☐

Changes will not be applied until next device reboot.

Change Network ID and password

The parameters displayed in this page may be modified under the user risk. Worldsensing recommends modifying them only in case of gateway replacement. In this case, a new CMT Edge gateway with the same radio configuration as the replaced ones will continue receiving messages from all connected edge devices, without any need of re-configuring them.

Note: The password can not be recovered once modified. Worldsensing keeps a digital copy of the GIS which contains the factory parameters, including the original password. Setting and losing a new password may require setting a new one and re-configuring all connected edge devices.

The process which manages radio message reception is protected by a watchdog, which reboots the gateway in case of not being able to parse any radio message during 8 Hours (no message during 1 Health message period). Rebooting the CMT Edge gateway minimizes data loss as the process is correctly started again, in case of service failure.

If no messages are received for 8 hours, the gateway will restart due to the radio watchdog.

4.4.1 Disable downlink messages

Since firmware version 2.7.0 it is possible to disable the downlink communication from a Gateway.

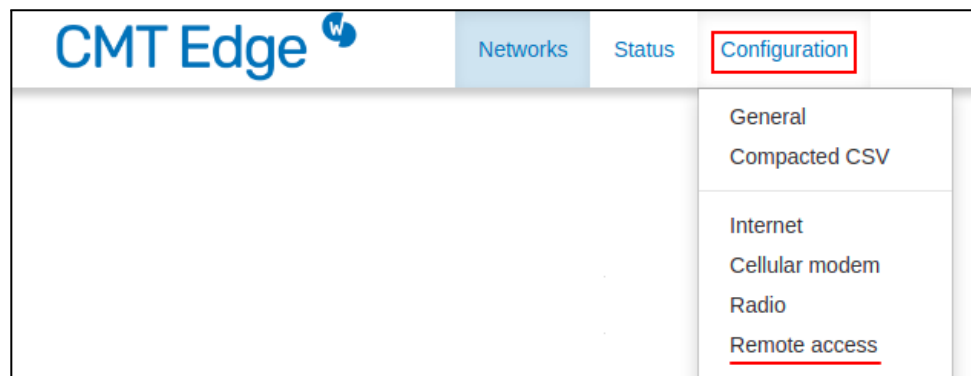
That means that two Gateways could be configured by using the same Network and receive all the messages from nodes that are connected to it within the radio coverage area.

This feature allows the creation of a redundant or secondary gateway to guarantee operations in case of failure of the primary gateway.

Refer to the Secondary gateway document on our [knowledge base](#) for more information.

4.5 Remote Access configuration

This page is available in the Configuration tab, by clicking the Remote access option. It allows configuring how the users access the CMT edge platform, including both methods, users and passwords.



4.5.1 Passwords management

CMT Edge is delivered together with a preconfigured user with administrator privileges and a predefined password. This user (Admin) and the password are used to access the gateway from all the interfaces available: Internet access via Public IP address (regardless of the physical interface used), Remote access tunnel (https://loadsensing.wocs3.com/GW_ID) or Local interface, by using the USB-C to Ethernet adapter.

Administrator user password

Here the Admin user password can be modified.

The previous Admin password will be required when the device is accessed remotely (IP or Remote tunnel), but no previous password will be required when modifying it through the local access.

Admin password

This is the password for the "admin" user

Current password:

Note: Changing the current admin password will also change the password if you are logging in through the local administration interface.
In order to recover the original Admin password contact the customer support team.

New password:

Repeat new password:

"Change Admin password" button must be clicked to apply changes.

Note: Keep the new password safely. The Worldsensing support team only keeps a digital copy of the default password, provided on the Gateway information sheet.

Changing the default passwords also affects the local interface (unlike previous firmware versions).

The Worldsensing support department may set the passwords to defaults remotely. Contact us by opening a support ticket on our support platform to recover the original one.

View Only user password

A view-only user may be enabled. This user named "viewonly" allows access to the CMT edge with limited privileges: All configuration options will be disabled in the User Interface.

User enabled: ☒

New password:

Repeat new password:

This user is disabled by default. It needs to be enabled by ticking the checkbox, setting a new password, and clicking the "Set viewonly configuration" button.

This user can be disabled by an Admin user remotely.

4.5.2 Remote tunnel management

CMT Edge platform is deployed locally on the gateway, but it may be connected to the Worldsensing platform using a VPN connection. This VPN tunnel service allows accessing the gateway through a

known URL instead of accessing via a Public IP address, which may be variable, especially when using dynamic IP addresses, as most SIM cards do. This known URL is https://loadsensing.wocs3.com/{Gateway_ID}, unique for every instance deployed, and accessible with the credentials provided at the GIS.

This VPN tunnel also allows Worldsensing technical support team remote access for troubleshooting and support purposes.

This feature is enabled by default, but may be disabled if required.

Remote tunnel

By disabling the remote tunnel you acknowledge that:

- **Connections through "loadsensing.wocs3.com" will be deactivated** and it will not be possible for Technical Support team to connect to the gateway for any maintenance required.
- You will only have access remotely through the cellular modem when having a **public IP** (ensure you have one), and locally through the gateway's local Ethernet.
- The firewall for the cellular 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.

☒ Activate remote tunnel

Changes will be applied immediately. If connecting through tunnel, connection will be lost and you will need to connect through the public IP.

[Save tunnel configuration](#)

There are two main scenarios where this tunnel should be disabled only:

- Offline environments without Internet access (together with the network watchdog)
- When using a public IP address. Sim cards providing a public IP address must be requested specifically, and are usually more expensive than the ones available in the market. In this case, it is relevant requesting a fixed IP address, to have a known IP address to access the system

Note: tunnel deactivation is done immediately, once the "save tunnel configuration" button is applied. This may provoke connection loss if the operation is done through the tunnel URL. Worldsensing recommends disabling this function (if required) from the local interface to avoid any connectivity issue.

Firewall rules for the Cellular interface

For the Cellular interface connected gateways some firewall rules are applied, which only accepts incoming traffic from the tunnel. Deactivating the tunnel when using this interface could generate a huge data usage in case of being exposed to an external attack.

These firewall rules are not applied when the device is connected via Ethernet, as the security is provided by the network where it has been connected.

Important note: Fail2Ban has been implemented in CMT Edge to enhance security and prevent brute-force attacks. Under the new configuration, any authentication failed (401 Unauthorized requests) to <https://loadsensing.wocs3.com/#####> will be blocked after 5 failed attempts. The block will last for 2 hours, after which the IP address will be unblocked automatically.

4.6 Repeater plugin

The repeater plugin feature allows the possibility of covering more area with the complete network, circumventing obstacles or including locations where internet access is not available by adding Edge Repeaters between the Main Gateway (CMT Edge) and the nodes which had no direct connection to the Main Gateway. Meaning that the Main gateway can receive data from Edge Repeaters, from nodes connected to them and from nodes connected directly to this gateway.

To use this functionality the Repeater plugin must be enabled on the CMT Edge.

Important: this feature can't be used without Edge Repeaters so enable this plugin only when there's at least one Edge Repeater in the same network.

Repeater plugin

/ Repeater plugin

Enabling the repeater plugin allows this gateway to send and receive messages from other repeaters, meaning that you can receive data from gateways, from nodes connected to them and nodes connected directly to this gateway.

Enable this plugin **only** when there's at least one repeater gateway in the same network.

☒ Enable Repeater Plugin

Once the [Enable Repeater Plugin] is selected, the Downstream devices list must be configured with the serial number of **all** the devices on the network that will communicate with the Main Gateway, both nodes and Edge Repeaters.

List of Downstream devices:

- This is the list of Loadsensing Nodes that belong to a repeater gateway further down the chain away from the main gateway.
- Insert the Loadsensing Node Serial Numbers, one per line.

Downstream devices:

101
102
12345
23456
34567

Save configuration

Edge repeaters SNs: 101 and 102 / Nodes SNs: 12345, 23456 and 34567

For more information about Edge repeaters and their configuration check the manual in our [knowledge base](#) or contact the [technical support](#) team.

4.7 Data Output

CMT Edge platform is designed to easily integrate with third party software platforms, for monitoring or data backup purposes. Three main options are available to automate data acquisition by external platforms.

4.7.1 FTP

At [CONFIGURATION]>[FTP client], an FTP client can be enabled and configured. This feature allows sending data to a configured FTP Server, and it is the most commonly used method for automatically uploading data to a monitoring software platform, to create and display reading charts, threshold alarms configuration, etc... It can also be used for backup purposes, by sending all readings received by the CMT Edge platform to a backup server.

The FTP client uploads all new readings received periodically. Readings stored on Edge device CSV files are pushed every 3 minutes if they exist, while compacted CSV file readings are pushed every 15 minutes. This means a FTP upload may not happen if no new readings exist, or more than one reading will be uploaded if the reporting period rate is lower than this period. This option is not configurable.

FTP SERVER CONFIGURATION

The FTP client requires configuring a FTP server, where data is going to be uploaded.

This information may be provided by the monitoring software provider or by the IT department in charge of the FTP server deployment.

These parameters must be filled to configure and enable the FTP client:

-Enable FTP: This checkbox will enable or disable the FTP client. A correct configuration will not work until this option is enabled. Any incorrect configuration of the FTP client will pass the FTP test if this checkbox is not enabled.

-Hostname: Box to set the URL or IP address of the FTP site. Temporarily, the IP address of a FTP site may be set if the URL does not work due to DNS issues.

-Port number: FTP uses Port TCP21 by default, and it is predefined in the system. This port may be modified according to the FTP site requirements.

-Credentials (Username & Password): The FTP client allows uploading data using anonymous login, or using a predefined Username and Password. Leave "Use anonymous FTP" checkbox unmarked for login using predefined credentials. Enabling this option will disable Username and Password options.

-Protocol: FTP, FTPS or FTPS (ignoring self-signed certificates) options are available. This information should be provided by the IT department in charge of the FTP site.

- The first one (FTP) refers to the unsecured system, which does not use any encryption method.
- FTPS option is used for connecting to secured FTP servers, when a CA certificate provided by a certification authority is used, such as Verisign, Thawte, etc...
- FTPS (ignoring self-signed certificates) option is used to connect to those secured FTP servers where the certificates have been generated locally, instead of by a CA.

NOTE: The Edge Gateway FTP client does not support the SFTP protocol. SFTP is not an FTP-based protocol, it is based on SSH.

-FTP mode: Passive or Extended passive modes are available. To be defined by the IT department in charge of the FTP server.

| | |
|--------------------|--|
| Enable FTP | <input type="checkbox"/> |
| Hostname | <input type="text"/> |
| Port number | <input type="text" value="21"/> |
| | <input type="checkbox"/> Use anonymous FTP |
| Username | <input type="text"/> |
| Password | <input type="password"/> |
| Protocol | <input type="text" value="FTP"/> ▼ |
| FTP mode | <input type="text" value="Passive"/> ▼ |

DATA UPLOAD METHOD AND PATHS

The second part of the configuration is related to how data will be transferred to the FTP site. Three different ways to upload data are possible, depending on the **Output** method selected

- **Append to the end of file:** This option creates a monthly file on the FTP server, similar to the Edge device and compacted files, named as current, and renamed with the Month and Year at the end of the month. Adds a line for each new reading uploaded.

This method dumps the whole file again in the case the file is not found on the server during the upload process. This method is useful for backup purposes.

- **Create unique file name at every upload:** This option creates a new file on every upload, with the device ID, date and time stamped on the file name, with all new readings generated since the last upload process.

This process may generate a lot of files, which may increase data consumption on the gateway side (part of the upload process requires listing all files existing on the FTP server folder). The user will be asked to mark a checkbox accepting the file management on the server side.

Output

Create unique file name at every upload

☐ This output method will generate a lot of files, and you are responsible to delete them from the FTP server. Each file uploaded has its own header.

This option is usually selected for data uploading to monitoring platforms, where the file is parsed as soon as it is uploaded to the FTP site, and deleted once data is registered.

- **Overwrite at every upload:** This option uploads a unique file to the FTP site. Similar to the Append mode, but it will overwrite all existing readings in the file on every upload, leaving only the new ones available. Useful for monitoring platforms which require a fixed name for the file, as no time nor date are modified on the file name.

As well as the Create unique file option, it will also be asked to mark a checkbox explaining the performance of this method.

Output

Overwrite at every upload

☐ This output method will overwrite the last uploaded file each time, keeping the same file name. This will have its own header and the new data since the last upload.

In all the cases, a file (or bunch of files if "Create unique file at every upload" option is selected) will be created for every edge device available on the network, if the type of file has been selected. Previously configured Custom compacted files can also be uploaded if this option is marked.

Different paths are available on the FTP client configuration option. Each one refers to a specific type of file. A different path may be set to each file to be uploaded, in order to store them in different subfolders on the FTP site.

Enabling the checkbox and setting a correct path is mandatory to upload that type of file.

Note: Default paths may be set as full path "/" or relative path "./" (without quotes). Any configured subfolder must be previously created on the FTP site, and correct permissions must be set.

| | | |
|------------------------------|---|-----|
| Output | Append to end of file | |
| Type of file | Append to end of file | |
| Health | Create unique file name at every upload | |
| | Overwrite at every upload | |
| LS-G6-VW data | <input type="checkbox"/> | |
| LS-G6-DIG data | <input type="checkbox"/> | |
| | | ... |
| Custom compacted data | <input type="checkbox"/> | |

This list describes the list of available types of files available at this firmware version.

Health: Uploads and stores any Health information of all the existing edge devices. A Health file will be created for every edge device connected.

LS-G6-VW data: Uploads and stores any information sent by any Loadsensing Vibrating Wire data logger available on the network.

LS-G6-DIG data: Uploads and stores any information related to any Geosense IPI, RST ASCII IPI, or Sisgeo V2 (Legacy) instrument sent by any Digital data logger available on the network.

LS-G6-VOLT data: Uploads and stores any information sent by any Loadsensing Analog (4 channel) data logger available on the network (Excluding DGSI Serial HD IPIs).

LS-G6-PICO data: Uploads and stores any information sent by any Loadsensing Piconode data logger available on the network.

LS-G6-INC15 data: Uploads and stores any information sent by any Loadsensing 15° biaxial tiltmeter available on the network.

LS-G6-DIG MDT data: Uploads and stores any information related to any MDT MPBX instrument sent by any Digital data logger available on the network.

LS-G6-DIG Sisgeo data: Uploads and stores any information related to any Sisgeo instrument with V3 firmware version sent by any Digital data logger available on the network.

LS-G6-DIG GeoFlex/GeoSmart/GeoString data: Uploads and stores any information related to any GeoFlex, GeoSmart or GeoSmart IPI sent by any Digital data logger available on the network.

LS-G6-DIG Modbus RTU: Uploads and stores any information related to any Geokon IPI or thermistor, Insitu Level Troll / Baro Troll and Aqua troll, Keller PR36XW and PR36XiW CTD, Vaisala WXT563, Position Control PC-HSD4 v2 or RST Modbus IPI sensor sent by any Digital data logger available on the network.

LS-G6-DIG Measurand SAA: Uploads and stores any information related to any Measurand ShapeArray instrument sent by any Digital data logger available on the network.

LS-G6-DIG YieldPoint: Uploads and stores any information related to any YieldPoint instrument using the ASCII protocol sent by any Digital data logger available on the network.

LS-G6-VOLT DGSI IPI data: Uploads and stores any information related to any DGSI Serial HD IPI sent by any Analog data logger available on the network.

LS-G6-LASER data: Uploads any information sent by any Loadsensing Laser distance meter available on the network.

Tiltmeter data: Uploads any information sent by any Loadsensing triaxial tiltmeter available.

LS-G6-LAS-TIL90 data: Uploads and stores any information sent by any Loadsensing Laser distance meter + Triaxial tiltmeter available on the network.

LS-G6-TIL90-E data: Uploads and stores any information sent by any Loadsensing triaxial tiltmeter with Event mode feature available on the network.

RPK20E data: Uploads and stores all Edge Repeaters-related monitoring information.

LSG7ACL-BILH-VIB data: Uploads and stores data from any Loadsensing Vibration meter.

LSG7ACL-BILH-VIB events: Uploads and stores the events from any Loadsensing Vibration meter.

SHM data: Reserved, not to be used.

Weather data: Reserved, not to be used.

Custom compacted data: Uploads and stores all custom files stored.

Gateway Health data: Uploads and stores all gateway-related monitoring information.

LSG7GNS-SXLH data: Uploads and stores data from any Loadsensing GNSS available in the network. NOT yet implemented.

LSG7GNS-SXLH statistics: Uploads and stores data from any Loadsensing GNSS statistics available in the network. NOT yet implemented.

TEST PROCEDURE AND ERROR LOGS

Once all configurations are done, the "SAVE AND TEST" button has to be clicked. By doing this, the FTP client will try to connect to the server, following this process:

1. The platform creates a connection to the FTP server using the credentials configured.
2. A test file is created, filled with data, and finally deleted on the server, in order to test the connectivity is OK.
3. CMT Edge checks the last file or data uploaded to the server.
4. It then uploads the latest data (with the selected output method to the selected paths).

A green bar with a success message will be displayed if the process is successfully completed.

FTP configuration has been saved

A red bar with a fail message will be displayed if the process is unsuccessful, as well as a message indicating the issue at the FTP Client configuration page, under Output configuration option.

FTP test failed, see details below

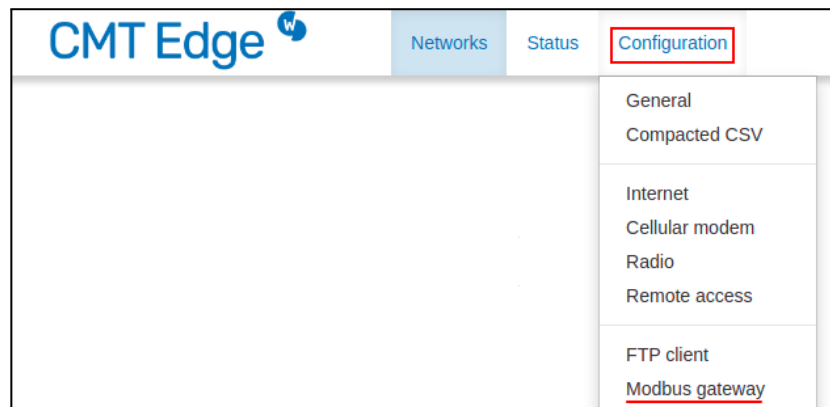
Last result ❌ Failed on 2021-08-03 12:25:17 CEST cURL (upload operation): Couldn't resolve host 'hostname'

During the service normal performance, should an error occur, the reading file should be uploaded again, or the full file from the beginning of the month (for append mode) should be uploaded. The error will be logged in the platform logs page.

Note: Both FTP server or CMT Edge internet access may require additional network ports to be open for a correct performance, due to passive mode port usage.

4.7.2 Modbus TCP

Loadsensing CMT Edge may also be connected to a Modbus TCP client by configuring the Modbus gateway at CONFIGURATION / MODBUS GATEWAY tab.



This protocol uses TCP502 port, which should be enabled in the network to allow communication. There is no possibility of modifying this feature.

This option is only available for wired network configurations, to be used in LAN environments, and SIM connected gateways with public IP addresses as it requires a known IP address to connect to the client. Anyway, it is recommended only to be used in LAN environments, as this protocol is insecure by design, without no user and password requirements, nor data encryption.

Unlike using FTP protocol, no historical information is available. Latest readings and edge device status is stored in the CMT Edge platform database, and it has to be periodically read by the ModBUS TCP Client.

The loadsensing network is organized by assigning a Unit ID to each edge device, and all available data (timestamps, last reading, etc...) related to each Unit ID is stored in registers assigned to each Unit ID.

Due to the loadsensing CMT Edge Modbus configuration, up to 246 Unit ID may be configured, to achieve information from 246 edge devices. Unit ID 247 is reserved for edge device status acquisition.

The ModBUS registers have a size of 16 bit , and may be accessed by using Function code 4 (Read input registers). This size may not be enough to display some information, such as timestamps or long readings; in these cases two consecutive registers may be required to get the data.

Once a reading from a specific edge device arrives at the CMT Edge platform, The associated registers are updated, overwriting the previous information.

Modbus TCP gateway configuration

Modbus TCP Gateway configuration is enabled by selecting the appropriate interface, Wired (Ethernet) or All (including cellular modem interface)

Status

Select the required status for your Modbus TCP gateway.

Disabled

Disabled

Enabled - Wired interfaces only

Enabled - All interfaces, including WAN (GPRS/3G)

Once the interface is selected, "SAVE" button next to the selected option must be pressed. This will enable the connectivity with external Modbus TCP clients using the selected one. A configuration saved message will be displayed. Access again to the Modbus gateway page to continue with the configuration.



Next required step is configuring the Message Timeout. This timeout refers to the time data will be available at the registers. A radio message arrives to the CMT Edge platform, and it is stored in the register for the period of time configured in this parameter. Once this time has passed, the information stored will be deleted. If this reading has been updated due to a new message arrival, the timeout restarts.

If the data of the register has not been renewed, an error will be sent to the ModBUS TCP request due to the empty register.

Setting this parameter to "NEVER" keeps the latest reading received from the edge device, even if it is offline. This option avoids receiving error messages at the ModBUS client, but may provoke receiving duplicate readings.

Therefore, it is recommended setting the message timeout at least equal to the highest reporting period configured on the network, as this feature is common to all the UNIT IDs configured.

Available timeout periods match with the reporting period configurable at the edge devices.

Save button next to the scroll menu must be pressed to apply the changes, and a Configuration saved menu will be displayed, same as in the previous operation.

12 hours ▾

Save

30 seconds

1 minute

5 minutes

15 minutes

30 minutes

1 hour

6 hours

12 hours

24 hours

Never

Unit ID configuration

This second part of the ModBUS gateway configuration will assign Unit IDs to the connected edge devices by creating a list with Unit IDs. Once created, the edge devices can be assigned to the UNIT ids. It is mandatory for Edge devices to be online while this configuration is done, as disconnected devices are not eligible for this list.

A specific Unit ID can be typed at Unit ID option (not necessarily sequential). Once typed, "Add row" Button must be pressed to add the Unit ID to the list. A scroll menu will appear next to the recently created Unit ID, where an Edge device ID can be assigned.

Unit ID

| Unit ID | Node ID - Type | |
|---------|--|--|
| 1 | <input type="text" value="7060 - tiltReadingsV1"/> | |
| 55 | <input type="text" value="Unconfigured"/> | |

As unit IDs are unique, CMT Edge platform does not allow duplication by mistake, displaying an error message.

Finally, a Unit ID can be deleted by pressing the "Trash" icon

Save button under the Unit ID list must be pressed to apply the changes, and a Configuration saved menu will be displayed, same as in both previous operations.

At this moment, a list of Unit IDs associated with the Edge devices is accessible in the CMT Edge platform.

NOTE: All detailed information, including the Modbus memory map and example videos is available at Worldsensing knowledge base.

IMPORTANT: from version 2.7, for 4G gateways (LS-G6-KIO-GW), the functionality of sending alerts from TIL90-XE nodes with Event Detection Mode via ModBus is added.

Take into account that polling alert registers at high frequency can increase the CPU usage from the Gateway.

According to Worldsensing load tests we can say that the Gateway supports requests at 4Hz, taking into account the following limitations to ensure correct operation and not to exceed the CPU maximum values:

- Polling to up to 20 TILT90E devices alert registers (this limits the number of TILT90E devices on a network, but does not refer to the total number of devices that could be connected on a Network)
- Periodic reading in alert state of 2 minutes
- FTP and MQTT disabled.

An increase in these values can lead to a CPU overload causing restarts and data loss. We recommend checking the CPU usage, also available as a modbus register, to ensure that there is no CPU overhead.

In case a different casuistic is needed please contact the support team.

4.7.3 REST API Calls

The CMT Edge platform is also accessible via REST API calls. This integration method allows receiving information from the platform such as latest readings and network status. It also allows some other operations such as edge devices and a full edge devices network deletion.

Requests can be done to both URL (https://loadsensing.wocs3.com/{CMT_Edge_ID}) or directly to the IP address, so it is available for any Internet connected or LAN environment deployment. Admin credentials will be required for this purpose.

Messages responding to GET requests are received in JSON format, with all the information displayed in a similar way to the Last messages explained in the Edge devices (Detail) paragraph.

The available REST API calls available are organized in three different types:

- INVENTORY: Calls included in this group return information about the networks created in the platform, list of edge devices at each network, and detailed general information of each edge device.
- DATA: Two specific calls will return the latest reading of all the devices connected to a specific network, or just the latest reading of a specific device in the platform.
- MONITORING: Displays peripheral information related to the network, related to the radio network quality. Some of these API calls allow receiving information such as coverage tests, lost/received messages, RSSI and other radio parameters of a whole network or specific edge device, etc...

IMPORTANT NOTE: A detailed article with detailed information related to integration with third party software using REST API calls can be found at [Worldsensing knowledge base](#).

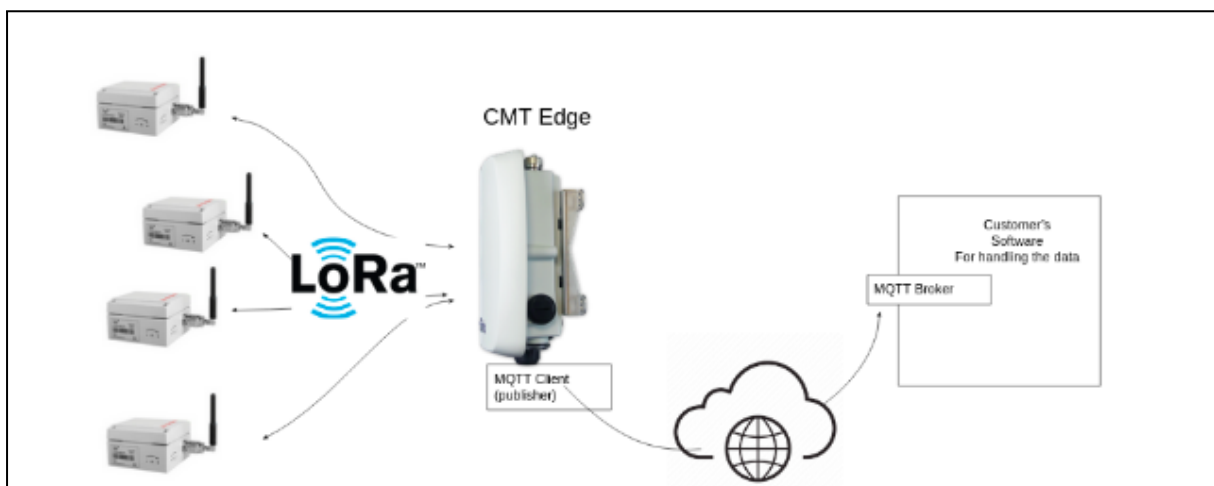
4.7.4 MQTT Push

The MQTT Push option has been implemented on the CMT Edge platform. MQTT is a lightweight data push system using TCP/IP protocol.

Unlike ModBUS TCP and REST API calls methods, this system redirects all the received readings and health messages to a configured broker as soon as they are received and processed by the gateway, allowing real time acquisition of the readings. Gateway uptime messages and gateway health data with the complete gateway information can also be sent.

Available message types are:

- Edge devices default data
- Edge devices engineering units
- Gateway KeepAlive message (can be manually activated/deactivated. Sent every 30s.)
- Gateway Callhome data with complete gateway info (user activable)
- Event mode alarms for TILT90-XE edge devices



This protocol allows pushing messages from different CMT Edge instances to the same broker using the same topic, centralizing all the gateways associated to a project in a unique point. Different clients may access this information at the same time, which makes this system much more flexible than all the others implemented.

A persistent buffering system has been implemented to avoid data loss in case the connection gets temporarily lost or in case the gateway gets rebooted.

This buffer is limited to a reserved space of 20MB or 10240 messages. See the following table.

| Max Reserved Space | Max Stored Messages |
|--------------------|---------------------|
| No swap 20MB limit | 10240 |

| 15 nodes with reporting period of 30 sec (30 msg/min) | 30 nodes with reporting period of 1 min (30 msg/min) | 120 nodes with reporting period of 15 min (8 msg/min) | 120 nodes with reporting period of 1 hour (8 msg/min) |
|---|--|---|---|
| 0.24 days (5.7h) | 0.24 days (5.7h) | 0.88 days (21h) | 3.55 days |

Note: A license activation is required to use the MQTT service. Refer to the [4.8.3 License manager](#) section for more information.

CONFIGURATION

At Configuration > MQTT Push tab the connection parameters between the CMT Edge instance and MQTT Broker are set.

Enable MQTT push

☒

Send Gateway Health data

☒

Send keep-alive data

☒

ClientID

Hostname

Port number

Topic

Server validation

No validation

Authentication

Username

Add

Enable bridge notifications

☒

Notifications topic

Save configuration

-Enable MQTT push: This checkbox must be selected to enable the connectivity

-Send callhome and Keep-alive data: Enabling this checkbox allows periodically pushing a message with gateway full health information to the broker (callhome) or a basic keepalive message with the uptime information of the gateway.

-ClientID: configurable field of the MQTT client ID. The default shall be ls-g6-gw[GW_ID], i.e. ls-g6-gw12345.

-Hostname & Port number: In these textbox the Hostname or IP address of the MQTT broker, and the used TCP/IP port number must be set

-Topic: String that the broker uses to filter messages for each connected client. It will also be used by the subscriber to receive all messages assigned to this topic. All devices connected to a CMT Edge instance will use the same topic, but several CMT Edge instances can use the same topic.

-Server validation: Three different methods may be used to validate the connectivity; No validation (Default), Using Own certificate, and using System certificates. This configuration must match with the configuration on the broker side.

In case of using an own certificate, a file browser will be enabled to upload the CA Certificate to the CMT Edge instance.

-Authentication: by default there is no authentication. Choose the desired type from the list (Username, Password, Certificate, Key) and click the ADD button to add it to the methods the MQTT client will use to authenticate.

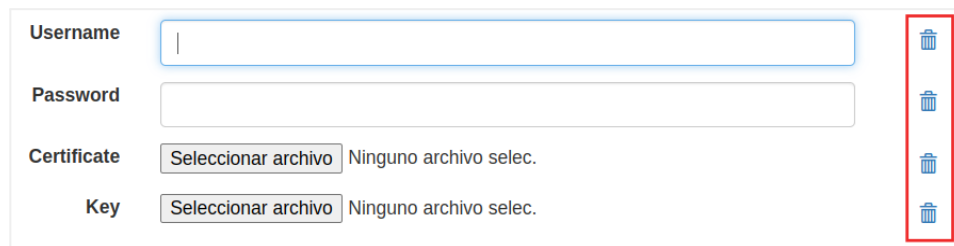
All authentications types can be used if required by the authentication system.

Important: although the different authentications are added separately, there are options that must both be chosen to be used together. E.g. username and password.

Selecting the Username and Password option will enable two text boxes to type the user and the password configured at the MQTT broker.

In case the certificate or key option is selected, two new buttons will be displayed to upload the certificate and the key.

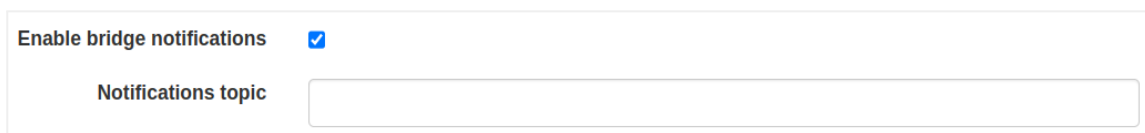
In case you don't want to use an already added authentication, clicking on the trash icon will delete it.



If you want to connect the MQTT client to an Azure IoT Hub, check the 'How to configure Azure IoT Hub to work with Loadsensing Gateway' user guide in our [Knowledge Base](#).

-Bridge notifications: by enabling the Bridge notifications, messages giving information about the state of the bridge connection will be sent.

-Notifications topic: Choose the topic on which notifications will be published for this bridge.



Note: The option "Enable bridge notifications" must be disabled if Azure IoT Hub is going to be used as a broker.

Once the configuration is done, SAVE CONFIGURATION button must be clicked to apply the configuration. A message will be displayed indicating that changes have been applied.



4.8 Maintenance

Different Maintenance tasks can be carried out at the configuration tab at CMT Edge platform

4.8.1 Configuration import and export process

CMT Edge allows exporting the entire configuration into a file, which can be used for backup purposes, or for loading this configuration in another gateway.

This feature is specially useful for gateway replacement, as it simplifies the task and reduces operational times. It will only require manual configuration for the Internet access, and previous Radio network configuration.

It also allows migrating from old 3G gateways to new Loadsensing Rugged 4G Gateways, and from 1.X firmware version to the latest firmware versions, which includes new features and latest integrations.

- The Export option is not available in Gateways prior to firmware version 1.16.2
- The Export/Import function is not available in Gateways prior to firmware version 2.3

Important note: Check Worldsensing Knowledge base to download the document with the detailed procedure.

4.8.2 Gateway firmware update

The CMT Edge platform allows updating the firmware using OTA files published at Worldsensing Knowledge base. These files vary depending on the gateway hardware type (3G or 4G gateway). The appropriate firmware version file should be used depending on the hardware and current firmware version.

This procedure allows adding new radios to the CMT Edge, new features or new compatibilities. The three different available gateway models are:

- 1) Loadsensing 3G gateway 1.X. 3G gateway model with firmware versions lower than 1.16.2. Can only be upgraded up to 1.16.2 firmware version. Future versions will not include new features and developments, and will be published just for bug fixing.
- 2) Loadsensing 3G gateway 2.X. Same hardware than previous version with 2.0 firmware version. Available on version 2.0 onwards. Future versions will include bugfix and new features.

- 3) Loadsensing rugged 4G Gateway. Available on 2.4.1 firmware version onwards. Include bug fixes and new features.

This information is available on Gateway status tab:

General

| | |
|-----------------------|------------------|
| Gateway serial number | 26016 |
| Gateway model | LS-G6-KIO-GW-868 |
| Firmware version | 2.7.0 |

- a. 3G model: LS-G6-GW-X (*X refers to the region*)
- b. 4G model: LS-G6-KIO-GW-X (*X refers to the region*)

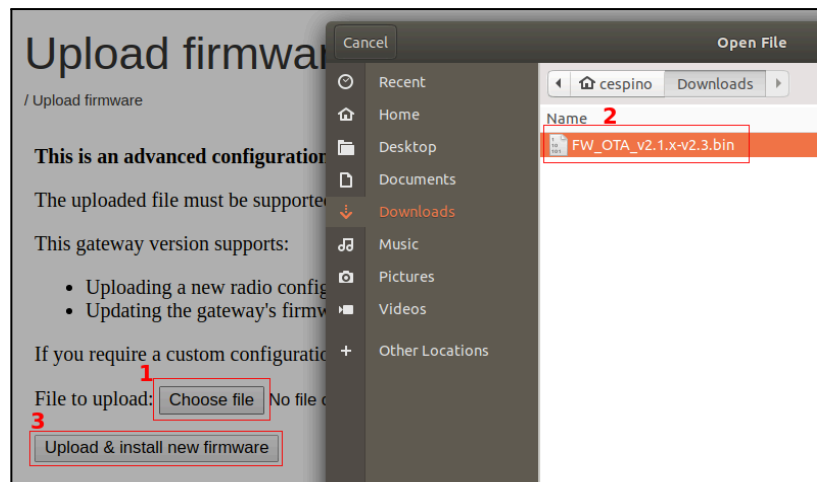
Firmware upgrades are done version by version. This means upgrading it from 2.3 to 2.6 will require three steps: from 2.3 to 2.4.1, 2.4.1 to 2.5 and from 2.5 to 2.6.

Note: Worldsensing strongly recommends reading the notes and communications about the update prior to proceeding with it, as it may contain relevant information.

Note: This feature is available in version 1.14 or higher. For lower version gateways, this feature is only available after upgrading remotely by Worldsensing to version 1.14.

This procedure is done, once required OTA files are locally downloaded, at Configuration tab, Upload firmware section.

Pressing the "Select file" button [1] and selecting the OTA file [2] stored locally is required. Then, pressing "Upload & install new firmware" button [2] uploads the OTA file to the platform and starts the upgrade.



The platform will check the uploaded file and display an error message if the file does not fit with a valid radio or firmware version (in the case of corrupted files or another file type selected by mistake).

CMT Edge will remain unavailable during the upgrade process, which may take up to 30 minutes. Once upgraded the gateway is rebooted and it goes back to normal.

Note: Upgrading a 3G gateway from 1.x to 2.x version cannot be done remotely. It is necessary to do it with physical access to the gateway by Worldensing engineers. Please contact your sales manager for a quotation.

4.8.3 License manager

The License Manager feature can be used to activate different software application(s) that require a license for their use. It is currently only available for activating MQTT licenses.

License Manager

/ License Manager

The License Manager can be used to activate different software application(s) that require a license for their use. If you need or are interested in the activation and use of any of these services please contact the Customer Support team.

| Service | Feature | Status | Activation Date | Expiration Date |
|---------|---------|-------------|-----------------|-----------------|
| MQTT | Pusher | Deactivated | None | None |

Activation

In order to activate any service/feature a valid license key is required. Please introduce the provided license key in the following form and press the button 'Activate' in order to proceed with the license activation.

License key

LICENSE ACTIVATION

If a license is needed, please contact the Product Sales Area Manager to get the license key required to activate the desired feature.

This license key is unique for the CMT Edge instance requested. Once the activation license is received, it should be inserted in the text box at the bottom of the License manager section available at the CONFIGURATION > LICENSE MANAGER tab, and the "Activate" button must be clicked.

Activation

In order to activate any service/feature a valid license key is required. Please introduce the provided license key in the following form and press the button 'Activate' in order to proceed with the license activation.

License key

Once a valid license key has been activated, a "success" message will be displayed at the top of the screen if the license is successful as well as the new license will be displayed in the system with the related information (service, feature, status, activation date and expiration date) or an error message if there has been a problem during the license activation.

In this case, check that the license has been copied correctly and that no blanks have been copied. If the error persists, please contact our technical support team.

Success: The new license has been successfully activated.

The License Manager can be used to activate different software application(s) that require a license for their use. If you need or are interested in the activation and use of any of these services please contact the Customer Support team.

| Service | Feature | Status | Activation Date | Expiration Date |
|---------|---------|-----------|---------------------|---------------------|
| MQTT | Pusher | Activated | 2022-11-23 11:48:46 | 2023-01-01 00:00:00 |

Success message and new MQTT license activated

Error: Invalid license format. The new license is not valid.

The License Manager can be used to activate different software application(s) that require a license for their use. If you need or are interested in the activation and use of any of these services please contact the Customer Support team.

| Service | Feature | Status | Activation Date | Expiration Date |
|---------|---------|-------------|-----------------|-----------------|
| MQTT | Pusher | Deactivated | None | None |

Error message

IMPORTANT NOTE: MQTT push feature will stop working once the date displayed at “Expiration date” arrives. Make sure the license key is not expired in case data is not received.

The “Delete all” option will also delete the license keys, together with the configured parameters and may require installing it again for enabling the feature.

4.8.4 Delete all

“Delete all” option deletes all data contained in the CMT Edge. This feature is useful for deleting all readings and networks generated during any test carried out prior to the final deployment. It is also useful for leaving a blank instance for a new project, and reusing the CMT Edge gateway.

This process will erase the whole existing network, including CSV files, formulas and peripheral configuration. It will also delete all logs and reset Compacted CSV, FTP client, General and ModBus gateway configurations.

It will NOT modify any credentials, radio configuration nor network settings, which should be manually configured if required.

Note: This process can not be undone

This process requires typing "Yes, delete all" as seen on the image below, and pressing the "Confirm" button to proceed, as it is a critical process that can not be reverted.

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

Yes, delete all

Confirm

Even if this option erases all the edge devices and the networks, as the devices still communicate with the gateway (Radio configuration isn't modified), the configured network and the devices will appear once they send a new radio message.

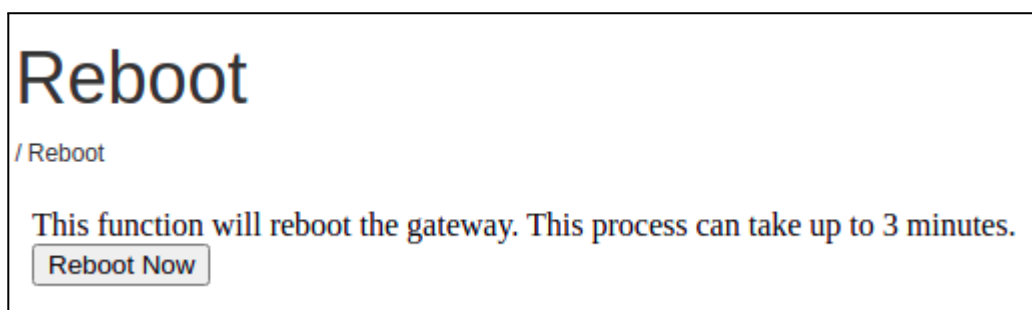
Edge devices require being unpowered, reconfigured, or factory reset before this process to avoid generating unwanted devices or readings.

4.8.5 Reboot

Rebooting the gateway may be required to apply some configuration changes at the CMT Edge platform. The CMT Edge will inform you about this requirement when required. This option is available at the Configuration / Reboot option.

Rebooting the CMT Edge may take several minutes depending on the Firmware version and performance. It may also take some extra time enabling remote access depending on the Internet connection.

Reboot Now button should be pressed and accept the displayed message.

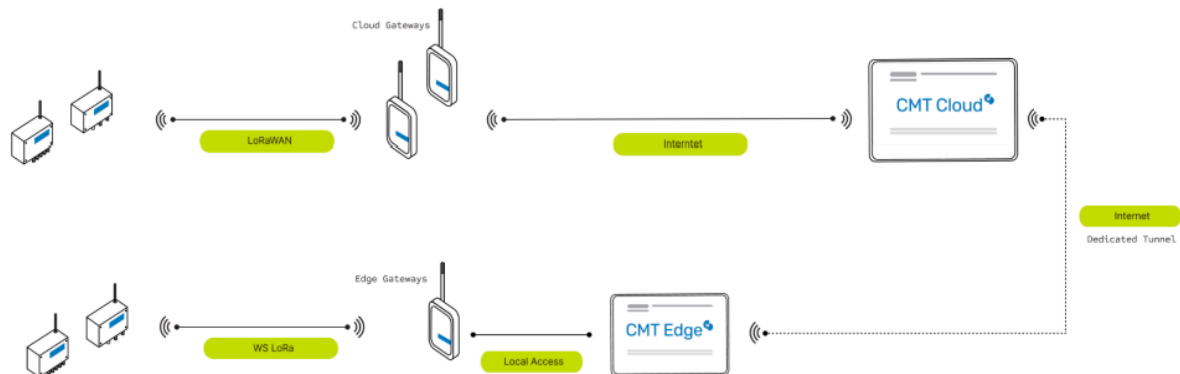


5. CMT Dual Management

This feature allows network operators to have full visibility of CMT Edge gateways in CMT Cloud.

It allows merging both single-networks and multi-networks deployments in one platform (CMT Cloud), while maintaining full independence of network and device management locally for CMT Edge users. When this function is activated in CMT Edge, users will be able to onboard Edge gateways in CMT Cloud as a separate network through the standard Network creation dialog box.

CMT Edge version 2.9.0 fully supports the CMT Dual Management feature from CMT Cloud 2.6.



5.1 Tunnel for CMT Dual Management Feature:

Please note that the dedicated tunnel that connects CMT Edge 2.9 to CMT Cloud is not enabled by default. It activates when the gateway is onboarded in CMT Cloud and it gets disabled automatically when the gateway and the associated network in CMT Cloud is deleted.

5.2 CMT Dual Management Key Features:

- Full visibility of Edge gateways and associated nodes:
 - New CMT Edge gateways are created as new networks in CMT Cloud and all nodes connected to them automatically become part of this network.
- Full data management over edge devices:
 - Data from all nodes in CMT Edge networks are fully operable in CMT Cloud. Create export files, set engineering units and use the workflow builder for more advanced data processing.
- Quick access to CMT Edge for network and device management:
 - Network and Device management are performed in CMT Edge. You can access CMT Edge locally or using a quick unified online access through CMT Cloud.
- Ability to create device groups or create new hybrid device groups:
 - Adding CMT Edge gateways and nodes to existing device groups.

5.3 How does it work

1. The CMT Dual Management feature works as a unidirectional link based in a dedicated tunnel between CMT Edge and CMT Cloud. In order to onboard a CMT Edge system in the CMT Cloud, the user has to provide internet connectivity to the gateway, either through Ethernet or cellular SIM card.
2. CMT Edge gateways are set up as Edge Networks. Edge Networks are easily created following the same user interface as other CMT Cloud networks.
3. Each CMT Edge Gateway is onboarded and presented as a separate LoRa network. From the CMT Cloud, nodes are automatically populated in the new network created, and data from them is received according to the reporting period set in CMT Edge.
4. Data from nodes can be used in the Data Management module for data export purposes.
5. Network and device management from CMT Edge Network remains independent from CMT Cloud. All network related features are fully functional in CMT Edge. You can access CMT Edge from CMT Cloud through a dedicated link.

6. Good Practices

6.1 Select appropriate Internet access interface

As explained in the Internet section ([refer to it for more information](#)) the CMT Edge gateway is factory-configured to communicate with the Internet without prior configuration by using Automatic mode. When booting, the device will try connecting to the Internet by using the Ethernet configuration using a DHCP configuration. In case the Ethernet connection (link) is not detected, it will switch to the Cellular interface. In case of not connecting to any network, the gateway will remain standalone, without an internet connection.

Network connection:

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

Internet communication is available with this setup. However, this configuration **is not the most appropriate one**.

Worldsensing strongly recommends configuring the Network connection in Manual Configuration Mode at the Configuration / Internet tab, and selecting the appropriate option.

Network connection:

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

- ☐ Cellular modem
- ☒ Ethernet with DHCP
- ☐ Ethernet with static IP

The “Cellular modem” option should be selected for SIM card based deployments, while Ethernet option (both DHCP or static IP configuration) in deployments providing Internet connectivity via Ethernet cable.

This configuration will ensure a faster and more reliable connection after reboots.

It will also decrease CPU usage, which may be critical to ensure a good performance of the deployment, specially on big networks, short reporting periods, and API Call integrations, as they require a high CPU usage.

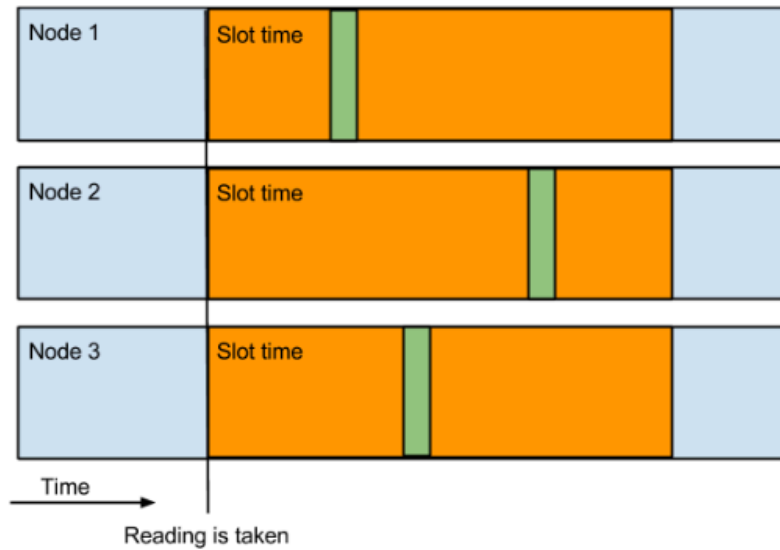
6.2 Setting the reporting period remotely

Setting the reporting period from the CMT Edge platform is considered to be a good practice. The reporting period is initially set to the edge devices using the Loadsensing Android application. At this point, and depending on the network size and reporting period selected, the Android app will assign a predefined maximum slot time to the connected device.

Setting the reporting period to the device remotely will shorten the slots time, getting reading from the devices sooner in the platform.

This configuration allows optimizing the radio network performance, getting the readings added in near-real time in the Compacted CSV files (and FTP servers if the FTP feature is configured), and also decreasing the CPU usage.

The maximum slot time refers to the maximum period of time an edge device may take between the reading is taken and the message is sent via radio. This time is considerably higher than the time used to send the message, and is necessary to avoid radio messages collisions.



This procedure is already explained in this document [HERE](#)

Important: since CMT Edge firmware version 2.6 the slot time calculation has been adapted to the processing capacity of the 4G Gateway (LS-G6-KIO-GW) and 30 messages per minute are being considered instead of 8 messages/minute (3G Gateway -LS-G6-KO-GW- maximum capacity). This decreases the time for data reception on the Gateway and file generation process.

Please make sure to reapply the reporting period from the CMT Edge again once you have updated the Gateway's firmware, if not the new calculation will not be applied.

6.3 Solution deployment procedure (step by step)

This procedure is a step-by-step short guide to be carried out for correctly deploying CMT Edge on a project. Worldsensing recommends following these steps to avoid misconfigurations during the deployment.

- 1) Connect the gateway to the Internet, following the steps on the appropriate Gateway user guide available on our knowledge base. It should be installed on the previously planned place; a coverage test may be required to select the optimal place. It is relevant to setting the correct Internet access interface as described in the [paragraph 5.1](#). It is also relevant to reconfigure the radio settings if required (gateway replacement, etc...)

- 2) Configure general tab, specially setting the timezone and monitoring emails, as described in the [paragraph 4.1](#)
- 3) Check the Status of the gateway. Upgrade the gateway to the latest version if required, as described in the annex available in the knowledge base and in the [paragraph](#). The configuration file may be imported if required at this moment if required.
- 4) Edge devices deployment on field using the Android application. Check our knowledge base for more information.
- 5) Remotely set the reporting period of the edge devices to optimize the network as described in [paragraph 5.2](#)
- 6) Once readings are arriving to the gateway engineering units and other minor configurations can be implemented.
- 7) Data export configuration if required, such as Compacted Custom CSV files creation, FTP client or Modbus TCP implementation, etc...



Contact Worldsensing

Need more support? Check our knowledge base at <https://https://www.worldsensing.com/support/>

Get in touch with our Customer Success team by opening a ticket at the Worldsensing support page or by email:

Email: support@worldsensing.com

Want to stay up-to-date about Worldsensindustrialsupport@worldsensing.coming?

Sign up for our newsletter: https://info.worldsensing.com/subscribe_loadsensing_maillist

Visit our blog for interesting content:

blog.worldsensing.com

Download the latest datasheets and infographics:

www.worldsensing.com/download-center

Follow us online

