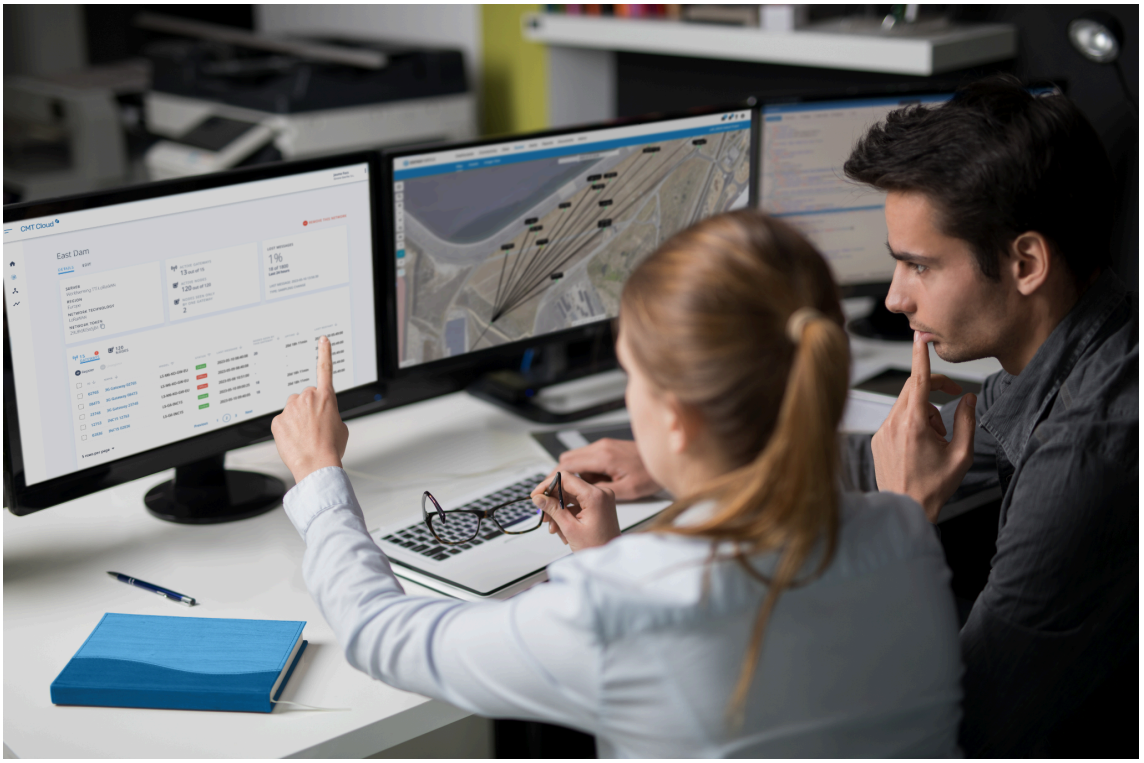
User Guide

CMT Cloud V2 Deployment guide

Version 2.10



Document Information

Author:	Worldsensing	Client:	All
Creation Date	01/06/2023	Document description	This document describes the CMT Cloud V2 solution deployment steps.

Version	Date	Author	Description
1.0	14/07/2023	Technical Support	Initial version, based on the 2.3 version.
2.5	25/01/2024	Technical Support	CMT Cloud 2.5 Version
2.7	01/11/2024	Technical Support	- CMT Cloud 2.7 Version -CMT dual management -LasTil scheduling tool -Vibration nodes integration -UI modifications -V1 Compatibility
2.10	26/05/2025	Technical Support	-UI improvements -Role management -Add-ons implementation

Contents

WORLD SENSING

BARCELONA
Viriat 47, Edificio Numancia 1, 10th floor,
08014 Barcelona, Spain
(+34) 93 418 05 85
www.worldsensing.com
connect@worldsensing.com

London Los Angeles Singapore

Confidentiality Agreement

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

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

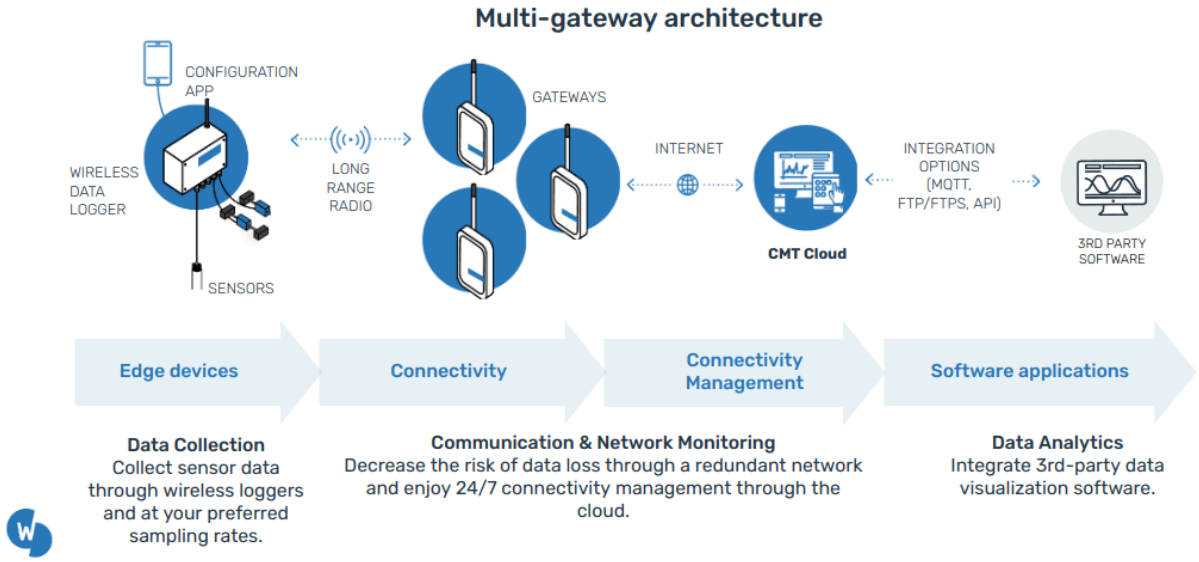
The content presented in this document will be binding only after the signature of a formal contract between the parties.

Purpose

The purpose of this document is explaining the main parts of the Worldsensing CMT Cloud v2 version. This document also details the networking possibilities and the procedure to deploy a full Worldsensing network, and the steps to connect edge devices and sensors to it.

System Architecture

CMT Cloud is a cloud based application. It provides full data digitization, easy to deploy, in near-real-time, with high reliability and easy to integrate with third-party monitoring software platforms in different ways.



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

Most sensors of the market can be connected to our data loggers, which are easily configured using our Worldsensing Mobile Android App (WS Mobile app onwards).

The edge devices periodically read the instruments as configured, store the data, and broadcast readings and other messages using our LoRaWAN© radio to the project data server.

A network of gateways will provide full radio coverage to all the edge devices existing in a specific project, redirecting the received readings via radio to the network server, which will handle these readings to be finally stored in the data server.

This architecture ensures data acquisition, as several gateways may redirect the same readings received via radio from the same edge devices and send them to the data server. Unlike the CMT

Edge architecture, the data server is located out of the gateway. This feature avoids data loss in case of gateway failure among other benefits and features.

This architecture simplifies monitoring tasks in those cases where more than one gateway is required to cover the edge devices of the project, due to the area to cover, or those projects monitoring different locations..

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

Edge Devices

Edge devices are data loggers and/or data loggers with embedded sensors, which act as nodes in the network topology. They are in charge of powering the connected instruments, digitizing the reading, storing locally and broadcasting the message through the radio network. Edge devices may also include wireless sensors such as Tilt 90 series, and are an active part of solutions such as event detection system.

All the current Gen6 edge devices, as well as some Gen7 devices (both data loggers and wireless sensors) are fully compatible with the CMT Cloud. Check compatibility appendix for more information.

The CMT Cloud edge devices use LoRaWAN© network to communicate with the gateways.

These devices are easy to deploy using the WS Mobile App

Gateways

The CMT Cloud requires at least one gateway, or gateways network to provide connectivity to the edge devices. This device will receive the radio messages broadcasted by the edge devices and redirect them to the Network server. It also establishes connectivity in the reverse direction, which allows remote actions being performed from the Cloud software.

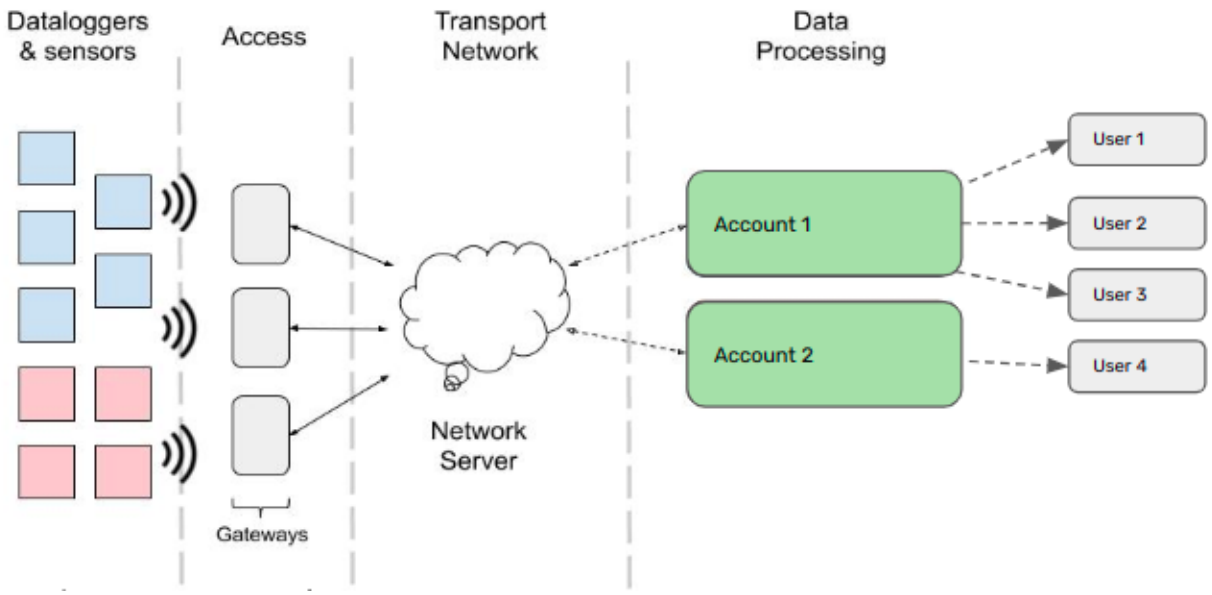
Please check zendesk or the Worldsensing website for the latest gateways compatible with CMT Cloud.

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

Network Server

The network server is a communications layer in charge of connecting edge devices and gateways with the end-user cloud based software.

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



This network server acts as a stack, redirecting the received messages, such as readings and health messages, to the data server where the edge devices have been registered previously. It represents the transport network of the solution, and it is transparent to the user.

Data server

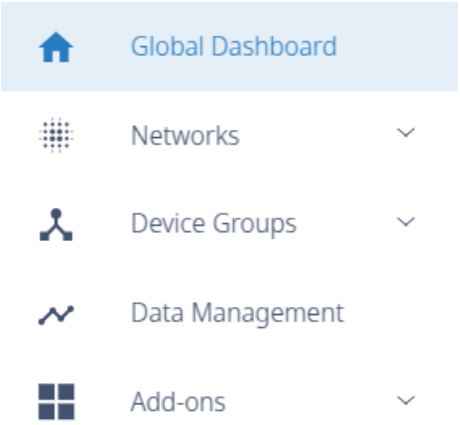
The data server is the CMT software element where messages arrive. It is connected to the network server, and accepts, decrypts and stores all messages received from the edge devices registered previously.

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

The main features of the data server are:

- Network management
- Connected edge devices and Gateways status management and reporting
- Device groups organization and management
- Secure data (instruments readings) storage
- Graphical view of the latest readings
- Third-party integrations deployment (against backup systems or monitoring platforms)

For this purpose, CMT Cloud is divided into 5 different areas:



Global dashboard with a general view of all the networks and device groups deployed

Networks: Connectivity layer. All devices are connected to a specific network.

Device groups: Edge devices are grouped as required by the user in this area.

Data management is in charge of handling with sensors connected to devices, and includes all the integrations of different device groups with third party software (via MQTT, FTP ,etc..)

Add-Ons: Specific add-ons to be deployed on demand, such as WorkFlow Builder, Thread Manager, Network monitoring and more.

Account implementation and management

This chapter of the document explains how the CMT Cloud account is designed, how users and accounts are managed and deployed, and all initial steps needed to be done. It also describes how to interact with the platform prior to starting implementing a new network.

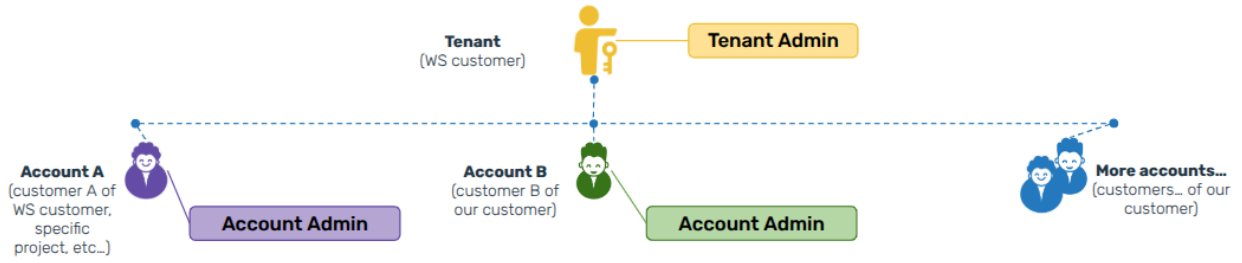
Platform structure and role management

The CMT Cloud account is created by the Worldsensing team on the first interaction, creating a new Tenant, associated to at least one user with Tenant admin permissions. This tenant is unique for the company, and will involve all accounts required for the customer. All users registered as Tenant admins will be able to create as many accounts as needed, as well as the associated Account admins and end users.

On the initial interaction,, an account has to be created. The account will also have a user with Account manager permissions. Each account may include a specific project, separated from the other ones (other accounts created by Tenant admins), each one with its own users.

This way, the company may manage a large number of projects (accounts) using the same credentials (tenant admins), and each project (account) will be totally independent of each other, keeping the account users blind from other accounts.

Finally, each account may implement as many networks, devices groups, and integrations as required.



Worldsensing will remain as System administrator, which has the resources for solving any issue or specific request required regarding this structure implementation.

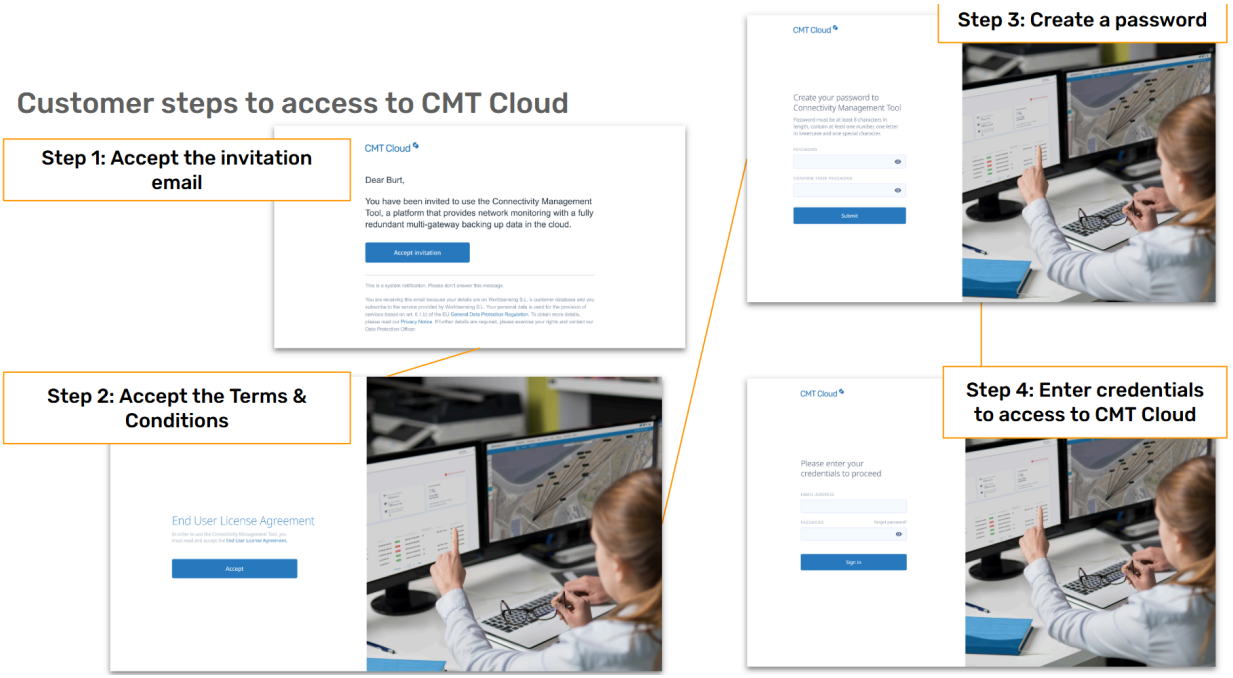
Login

Worldsensing CMT Cloud platform is accessed on this URL: https://cmt.wocs3.com/login i

Prior to the first access, the platform will send an automatic email, which will ask to end the self-registration by setting a secure password, as well as accepting the End User Licence Agreement.

Once the user is registered, this URL should be used, instead of the link provided by the email received.

This login process also allows receiving an email in case the password is lost or forgotten, and is unique for all type of users (Tenant admins, Account admins and Account users)



Tenant admin management

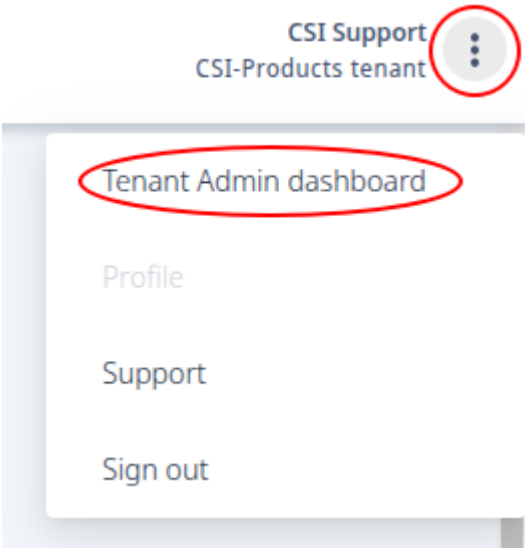
Once the Tenant admin user has logged in, the platform is displayed. The Global dashboard will be displayed, where all Networks and Devices groups can be checked. Also, Data management and enabled Add-Ons are available.

At this point, the user can navigate through the device groups, check the networks, data, etc.. for monitoring purposes.

In case a specific account needs to be accessed for specific implementations or tasks, such as reporting period modifications, sensor configuration and many other operations, the specific account has to be accessed.

This dashboard will also allow creating new accounts for new end customers, as well as managing the account users.

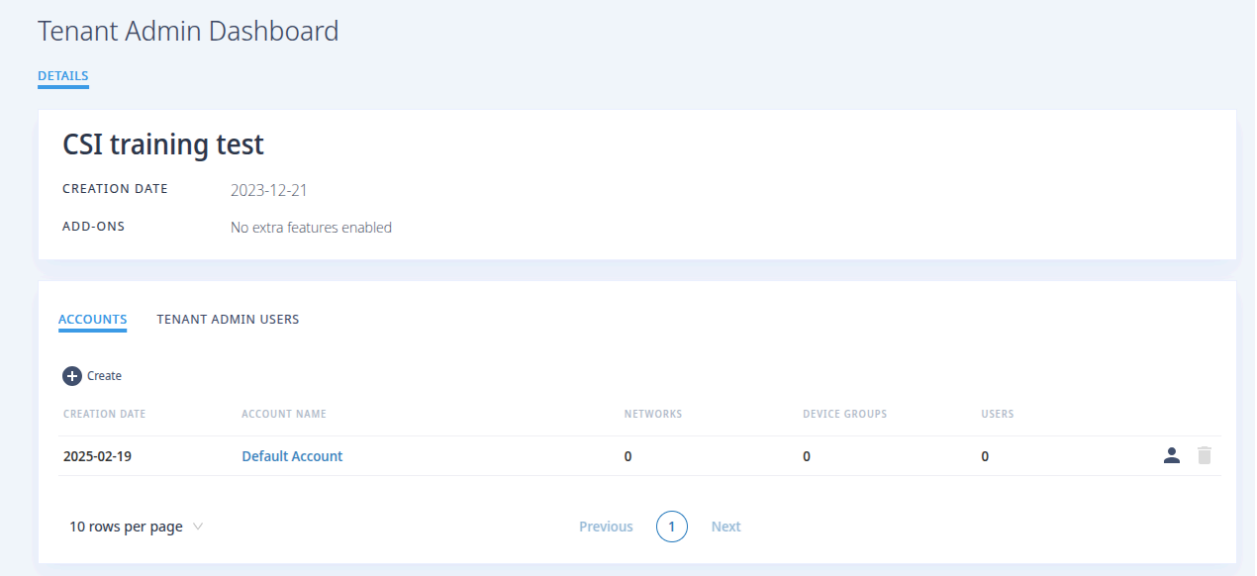
The Tenant Admin Dashboard, is available by clicking on the top right three dots icon, selecting Tenant Admin Dashboard.



This dashboard displays the Creation date, as well as the list of ADD-ONS associated with this tenant, as well as some other specific features such as Compatibility with V1, etc..

Also, two different areas are displayed:

1) ACCOUNTS: Allows creating new accounts, adding or modifying users associated to it (ACCOUNT users), and joining the account. Deleting the account will be available in future releases.
2) TENANT ADMIN USERS: Allows creation of new TENANT admin users. Deleting them will be available in future releases.

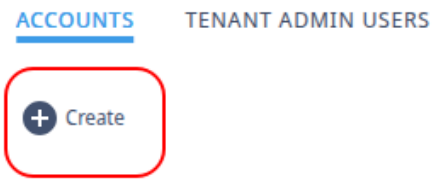


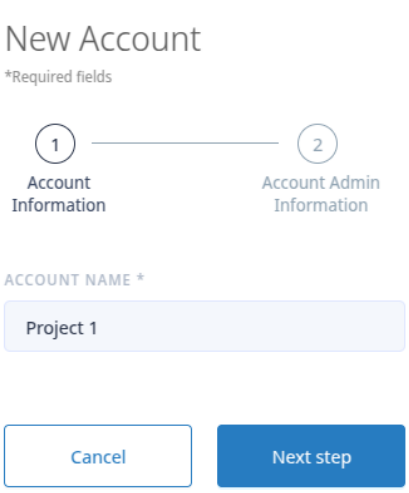
New account creation

A new project, for a new end customer, will require a new account, to be a fully independent space from other end customers. Tenant admins have the option to create it, and assign the required account users, which will be able to access their own account.

For this step, a new account needs to be created, with an associated Account admin user. For this purpose, Account name, and Account admin email and identification is required.

The new account creation setup wizard is triggered by selecting the ACCOUNTS tab, and clicking in the Create button.

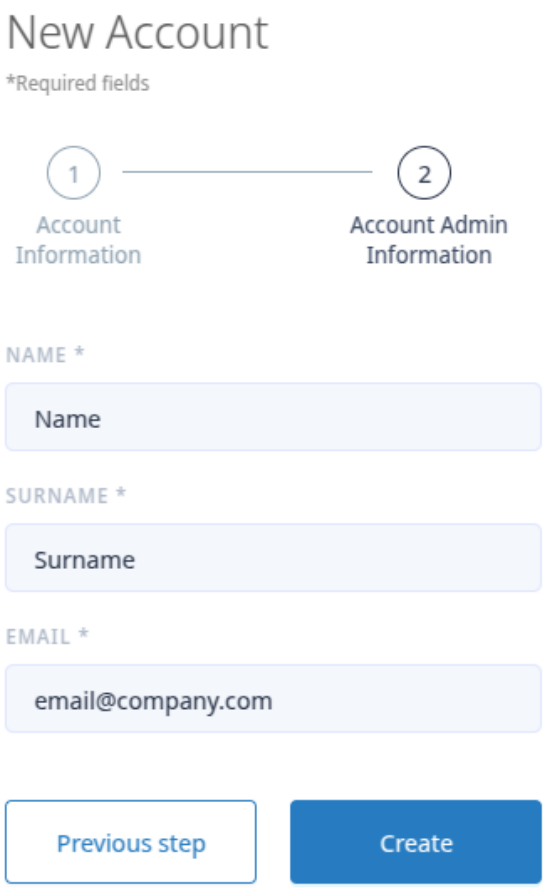




The first step will require assigning a name to the Account.

This name indicates how the account will be identified in the Global dashboard for Tenant admins.

Clicking next will display the Account admin user generation.

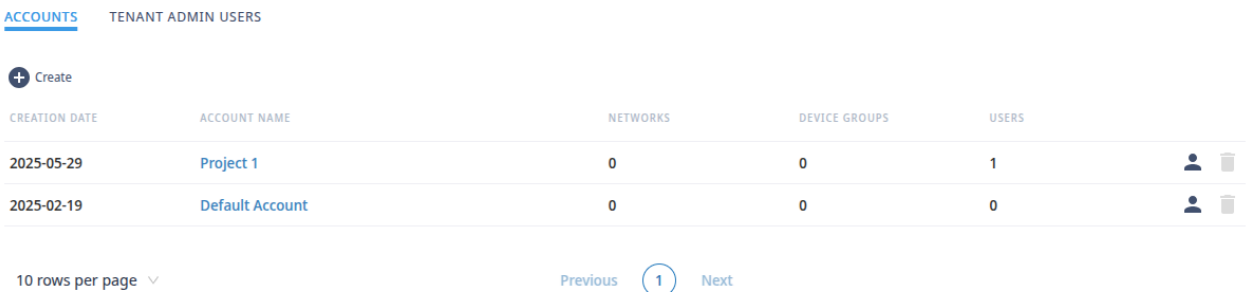


The second step requires Name, Surname and Email account of the account manager. Fill the information requested and click on the Create button

At this point an automatic email will be delivered to the end customer email account to end the self registration at the platform.

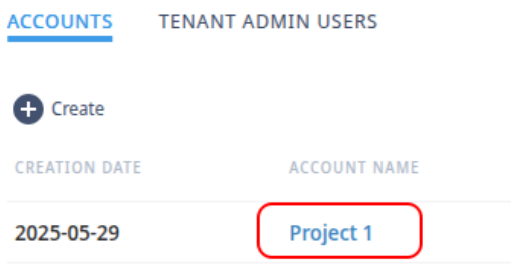
As indicated in the Login chapter, Once finished, the Account admin will be able to login through the platform url: https://cmt.wocs3.com/

Once finished, the dashboard will display the new account.

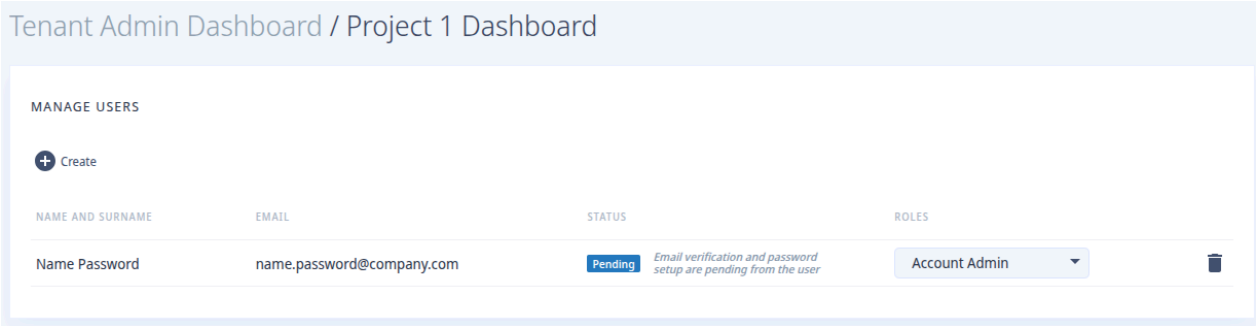


Account users management

Once the account is created, the rest of users can be created by clicking on the Account name.



This link will redirect the Tenant to the account management dashboard, which displays the list of users created, as well as the registration status, and role.



New users can be created by clicking on the **+ CREATE** icon, existing users (including account managers) can be deleted by clicking on the **Bin** icon of the specific user, and roles (permissions within the account) can be modified by selecting the appropriate ones from the dropdown list of available roles (Save button has to be selected to confirm).

NOTE: Only Tenant admin users are allowed to manage account users. Any user management (Creation, Deletion or role modification) is managed by the Tenant admin users. Account users (even Account admins) are not permitted to create new account users and modify the existing ones role, and will have to contact the Tenant for these tasks.

This table shows the actions each user can perform according to the role or roles selected.

Action	Account Admin	Network Manager	Network Viewer	Device Manager	Device Viewer
Manage networks	✔	✔	-	-	-
Manage device groups	✔	-	-	✔	-
Create/edit integrations	✔	-	-	✔	-
View/download custom CSV	✔	-	-	✔	✔
Manage engineering units	✔	-	-	✔	-
Use and access to ADD-ONS	-	-	-	-	-

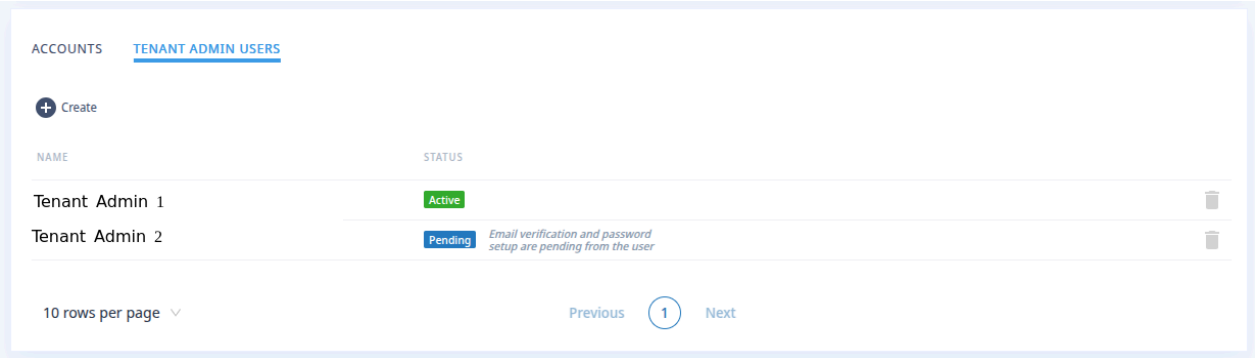
Role management offers granular control over user interactions. For instance, users can be restricted to specific network layer functionalities like Device manager or Network Viewer. Additionally, certain operations, such as creating engineering units or modifying the Reporting period, can be disallowed by assigning users the Device Viewer role.

An account administrator possesses all the permissions of both a Network Manager and a Device Manager.

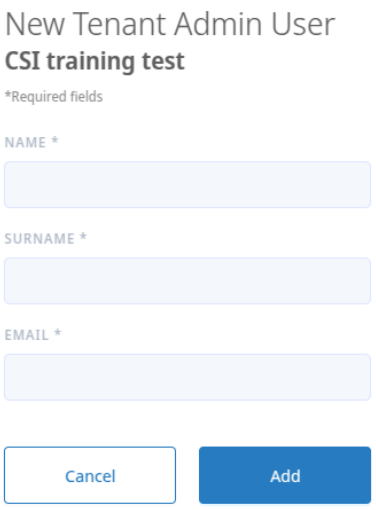
Account users cannot access ADD-ONs; this functionality is exclusively for Tenant administrators.

Tenant admin management

Back in the Tenant admin dashboard, the TENANT ADMIN USERS tab displays the list of created Tenant admin users, as well as the Status (Active or self-registration process pending)



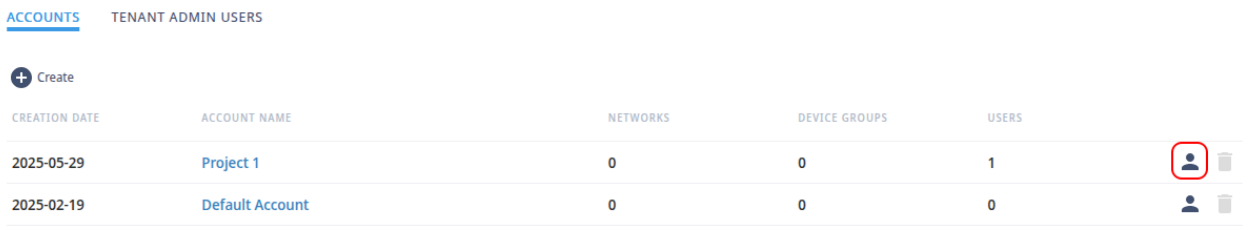
Upon clicking "Create," a new tenant administrator user form appears. Similar to other user creation procedures, an email is dispatched to the new user for email verification and password configuration.



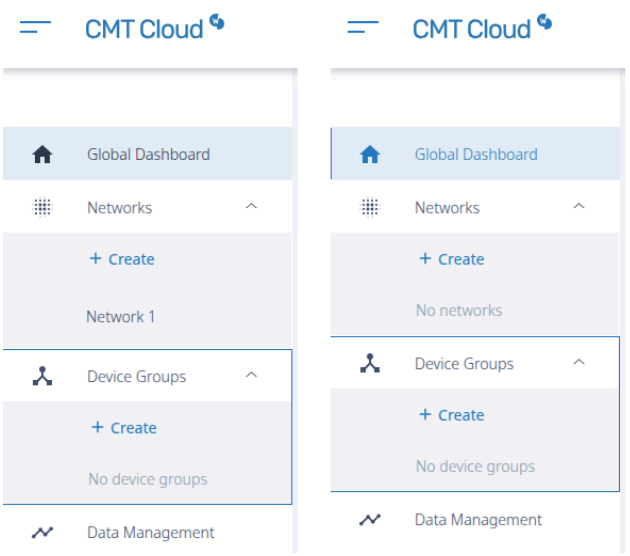
Joining an Account

A Tenant admin user may operate with any of the existing accounts with Account admin permissions.

These tasks, such as gateways and edge devices connection, networks and device groups creation, and any other configuration, requires accessing the specific account. This step is done by clicking the USER icon on the Tenant Admin Dashboard / Accounts tab



Once clicked, a new tab will appear in the navigator, displaying the Global dashboard as default page. Unlike the previous tab, where the user acts as Tenant admin, and therefore all networks and devices groups deployed on all accounts can be managed, this one will only display the existing networks and devices groups in the specific account.



Tenant administrators viewing the lateral panel will see a list of accounts, as shown in the left image. In this example, "Project 1" and "Default account" are visible. The "Default account" contains one network, "Network 1".

Upon accessing a specific account, such as "Project 1" (right image), the lateral panel updates to show the contents of that account. In this instance, no networks or device groups are displayed within "Project 1" because none have been created yet.

New project deployment

This part of the document details all the requirements and steps to be done to deploy a project from the beginning to the end on Worldsensing CMT Cloud.

Most edge devices are compatible with this platform, as well as CMT Cloud gateways (LS-M6-KIO-XXX).

CMT Edge gateways are not compatible with this structure, although the CMT Edge projects can be linked to CMT Cloud for data centralization and management, using the CMT Dual management feature (chapter below).

Also, The 2.8 version of WS Mobile App or higher is required. This version can be downloaded from Google Play by searching Worldsensing. Once the WS Mobile App and the devices are ready, access the CMT Cloud platform via https://cmt.wocs3.com/login .

In case of using a Tenant admin user, access the Tenant admin dashboard and join the required Account.

As a general rule, there is a list of steps to be done to deploy a project. This means connecting all devices to start monitoring them correctly.

1) Access the platform and join the required account.
2) Create a network: All gateways and edge devices must be connected to a network, which will manage and provide the connectivity layer. This could be a Cloud (LoRaWAN) network, or either a CMT Edge (LoRA) gateway linked using Dual Management Feature (explained below)
3) Link devices (Only for Cloud networks): At least one gateway must be connected to the network, to provide radio level connectivity to the edge devices. Once a gateway is connected, more gateways, or edge devices can be connected.
4) Create device groups: All the devices registered and connected in the previous step must be added to a device group. Once created, edge devices and gateways have to be linked to the Device Groups. This is mandatory to receive readings from the nodes, and data management.
5) At this point all data is being processed and stored at the cloud instance. In case of requiring connectivity with a third party software, a new integration can be created. Integrations allow connecting CMT Cloud with a third party software, sending readings from a specific device group. MQTT, API calls and FTP are available. Some other features such as Custom CSV files are available.
6) Alternatively, ADD-ONs can be used for specific features, such as applying rules for automatic threshold alert email delivery, Thread X3 connection, etc…

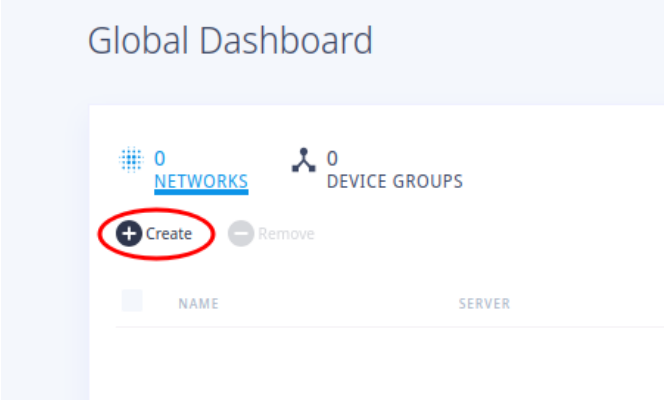
CMT Cloud network (LoRaWAN project deployment)

Network creation

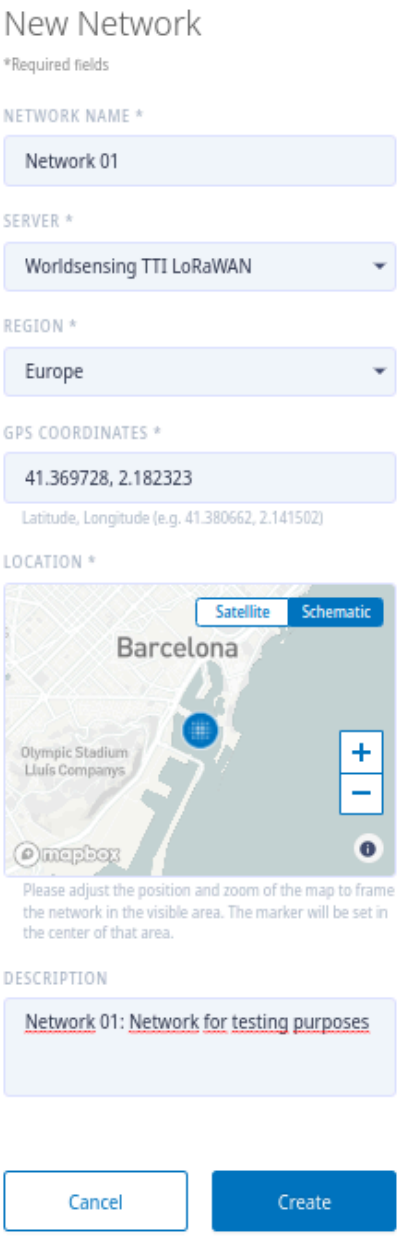
The first step is creating a network. CMT Cloud allows creating as many networks as required, which can be useful to organize the connected sensors according to the project requirements, or creating different networks for different projects within the same account, etc.

It is recommended defining the networks structure before devices deployment due to these points:

- There is no possibility of moving gateways and edge devices from one network to another: The device should be removed and configured again. This would provoke the loss of all data related to the device.
- Selecting a network is a mandatory step during device commissioning.



To create a new network it is necessary to click on CREATE button on the NETWORKS option at the CMT Cloud dashboard and complete the steps of the wizard:



NETWORK NAME: Name of the network (to be displayed)

SERVER: Network server selection. Select **LoRaWAN** for standard cloud based edge devices network. LoRa server should be used for Dual management configuration (check specific chapter for more information)

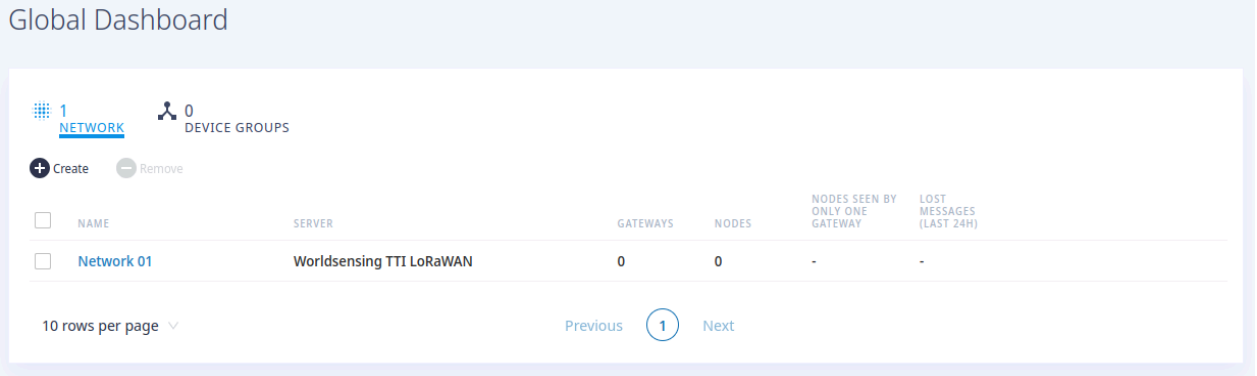
REGION: Europe / North America / Australia. This option is related to the network server to be used. A relation between Region, Gateway radio model and App radio model to be used is detailed at the end of the document (Appendix 2) Ask customer support in case of doubt.

GPS COORDINATES: Location of the network icon in the map. It can be selected with the map below.

DESCRIPTION: Text area reserved for adding information related to the network (not a mandatory field)

Once all options are selected, click Create to create a new network.

At this point a new network has been created, and devices can start being connected to it.



NOTE: It is relevant to understand that connecting devices to a network does not imply receiving messages, as messages arrival must be ensured.

Readings, as well as Health information will be stored once linked to a network, but will not be displayed until these devices are added to a devices group (Step explained in the Devices group section).

Gateway commissioning

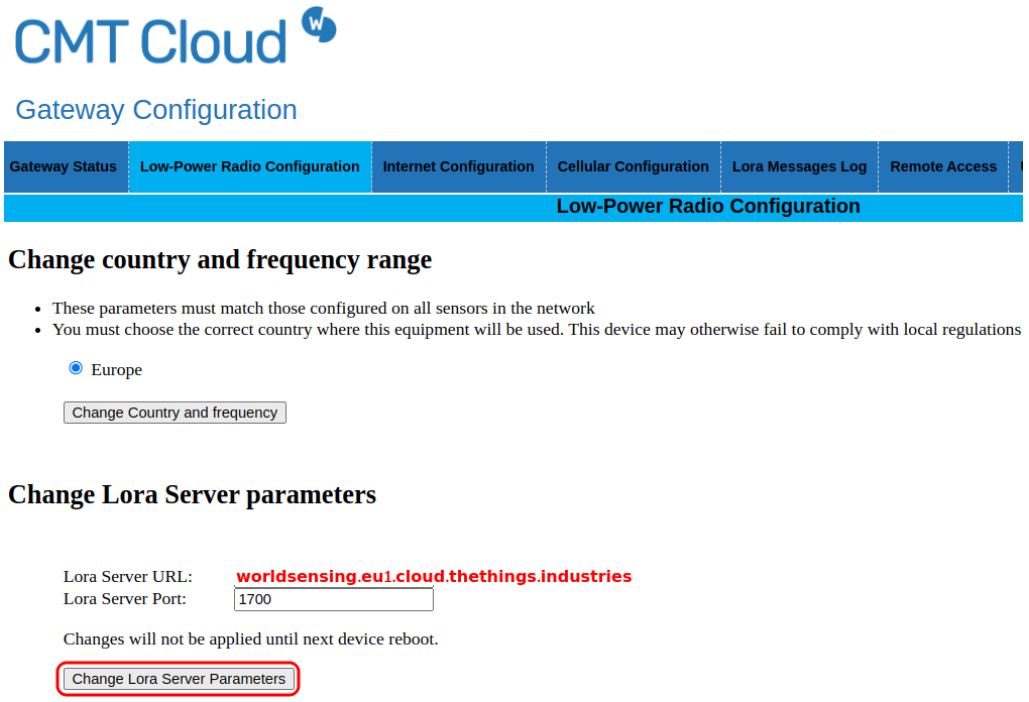
Next step in a project deployment is connecting the gateways, which will provide the connectivity to the edge devices. Only those gateways that have Cloud firmware are compatible with this solution, the ones named as LS-M6-KIO-XXX. The initial firmware version (1.0) is valid for it, even though we recommend checking the upgrades to ensure no required features are missing and any possible bugfix is applied. Contact Worldsensing support platform for the firmware upgrade files.

The gateway configuration consists of two different parts:

- Gateway configuration
- Cloud connection

For the first step, it is required powering and connecting the gateway to the Internet (These steps are detailed in the gateway user guide at our knowledge base).

Once the gateway is available and accessible from the internet, we recommend checking the LoRa Server and radio model at the “Low Power Radio Configuration” tab



Each gateway may have different radio models and a different network server will be required, depending on the local radio regulations. The cloud account will be created according to these regulations, and the information will be provided by Worldsensing.

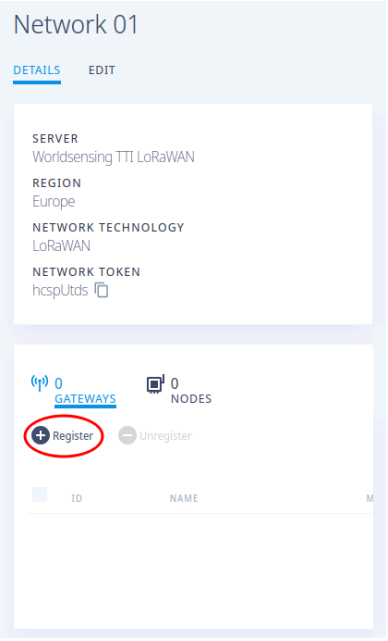
Currently, these three options are available, according to the region where the project is deployed:

Gateway model	LoRa server
LS-M6-KI0-868	worldsensing.eu1.cloud.thethings.industries
LS-M6-KI0-915	worldsensing.nam1.cloud.thethings.industries
LS-M6-KI0-923	worldsensing.au1.cloud.thethings.industries

Once the correct radio has been selected, and the appropriate LoRa Server has been configured, the gateway is ready to be registered at CMT Cloud.

The configuration of the Gateway must be replicated in the CMT Cloud account.

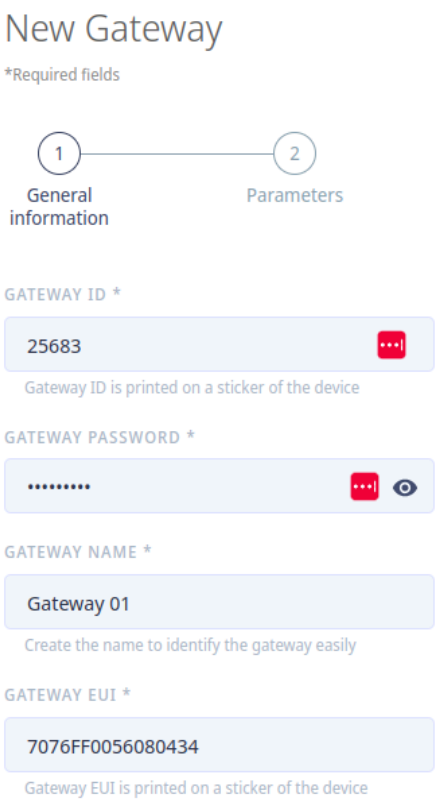
For this purpose, click on the recently created network, select Gateways option and click on Register



Fill the options on the setup wizard displayed.

There are three main group of parameters to configure in this case:

- Related to the Gateway parameters
- Related to the Location and info
- Related to the Radio parameters used

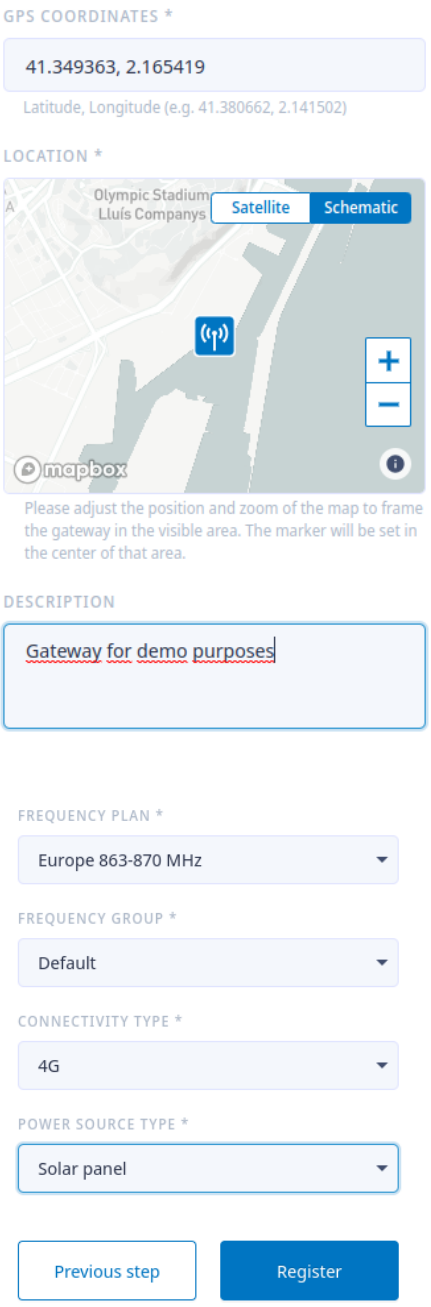


GATEWAY ID: This is a unique ID hard coded on the system. Information available at the Gateway Information Sheet.

GATEWAY PASSWORD: Password created to access the gateway remotely. This parameter can be modified. Information available at the Gateway Information Sheet.

GATEWAY NAME: The name used to display the gateway on the platform.

GATEWAY EUID: This is a hard coded parameter. It is available in a sticker in the gateway, as well as in the Gateway information sheet.
Contact the worldsensing support team to get the ID if not available.



GPS COORDINATES: In this part, the GPS coordinates can be selected, the same way it is done with the network.
This will help display the exact location of the gateway.
It can be modified remotely at any moment.

DESCRIPTION: Text area reserved for adding information related to the gateway (not a mandatory field)

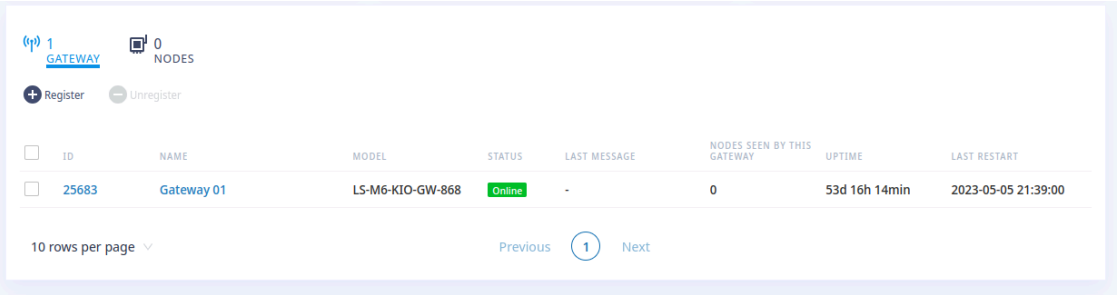
FREQUENCY PLAN: Must match with the radio model configured in the gateway(check appendix II).

FREQUENCY GROUP: The frequency group must match with the one configured in the gateway.

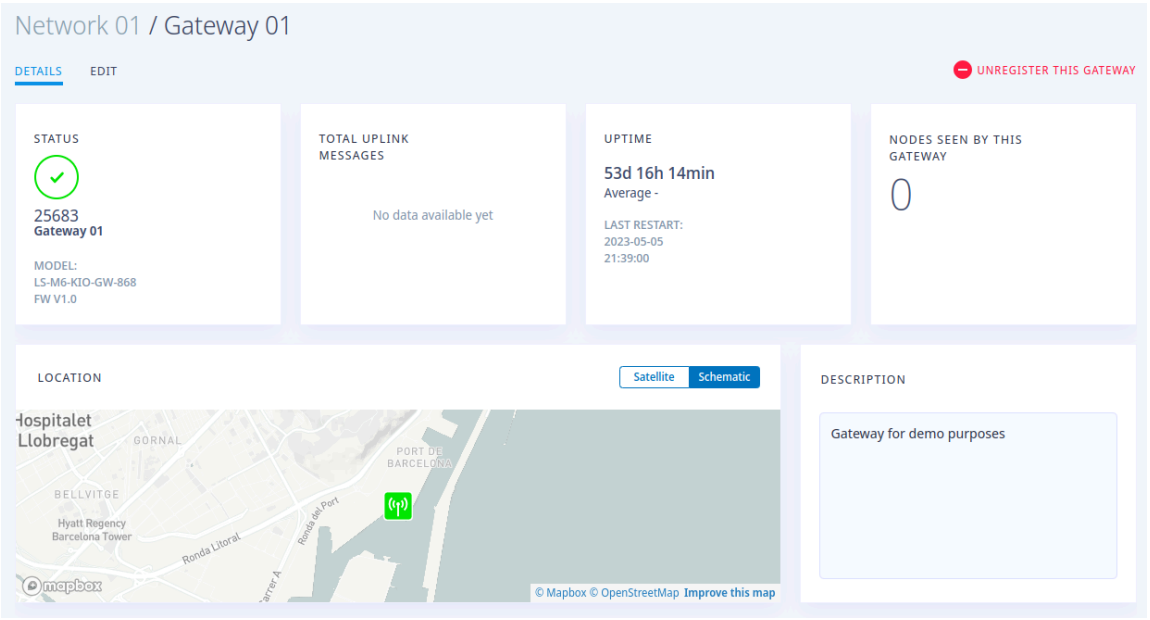
CONNECTIVITY and POWER SOURCE TYPE: These parameters are not used for any specific task, just for informative purposes. Does not affect the performance of the device.

Once configured, click REGISTER. A message with a green background will be displayed in case the configuration has been done correctly.

Once the gateway is connected, it will be displayed in the network list, appearing as online with the gateway monitoring data. Getting Online may take some time, displaying Pending status until messages arrive from the network server. Force a reboot if the gateway does not get online.



Selecting the device displays all the connectivity parameters of the device, such as the number of uplink messages, uptime, map location etc…



Gateway management (register and unregistering gateways) is now carried out directly from the software platform, not requiring Worldsensing support for this purpose.

Edge devices commissioning

Edge devices (data loggers and sensors) are fully compatible with the CMT platform . The registration of these devices requires using the WS Mobile App, which can be downloaded from Google Play.

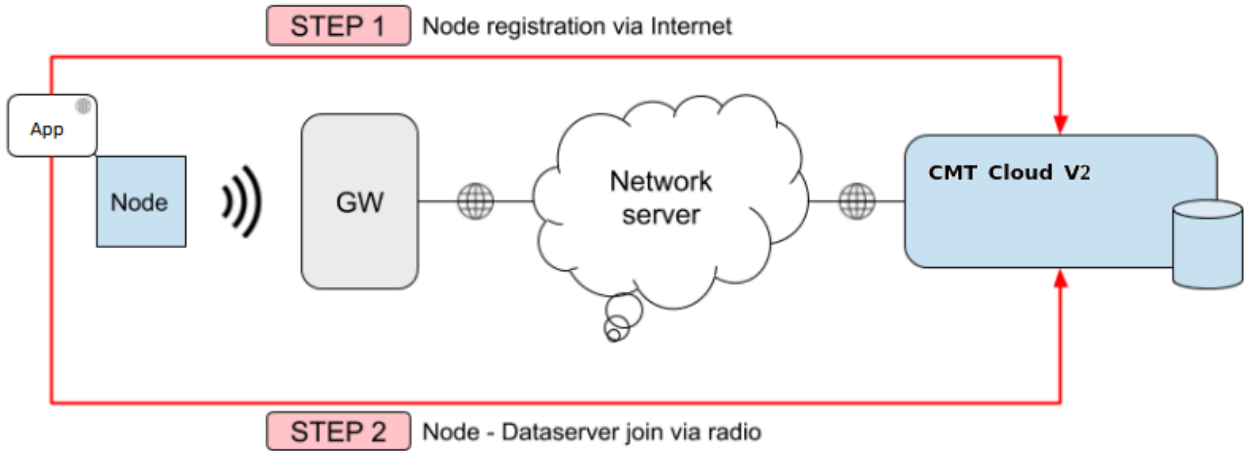
Once the sensors are connected to the device (if applied), batteries installed and the internal switch set to batt (if exists), the commissioning will require connecting the device to an Android device with the application installed (WS Mobile App). We strongly recommend checking the specific user guide of the device to connect, in order to ensure the configuration, wiring and other relevant details. This section is focused on the radio connectivity of the commissioning. Check the user guide for sensor configuration.

Depending on the Internet connection of the device, there are two different ways to register an edge device on the CMT Cloud platform:

- Online registration: The Android device with the Worldsensing App has Internet connection.
- Offline registration: The Android device is not Internet connected.

Online registration

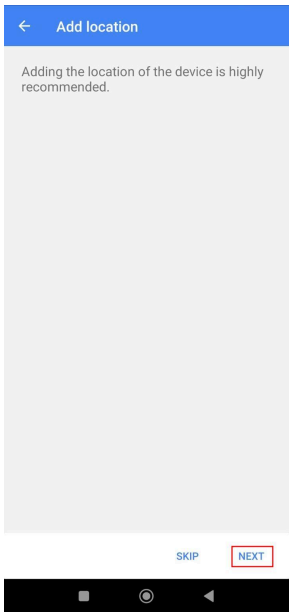
This is the recommended option. Having Internet access on the Android device allows getting instant information related to the coverage of the device, and the commissioning is done in a unique step using the app only.



For this commissioning method, once the device is connected it is required setting it on time and upgrading the firmware version if needed. Once this step is done click on Setup wizard and pass the setup wizard process to connect it to CMT Cloud. This process will pass through these steps:

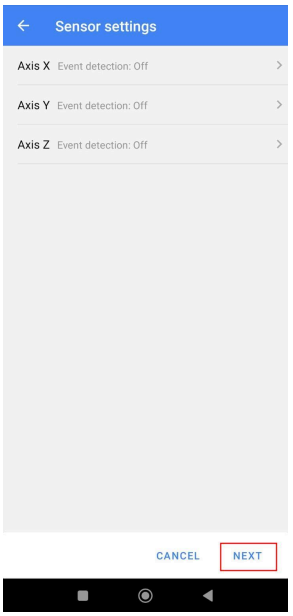
- Data logger location, sensor configuration, reading test and results
- Radio model configuration
- Cloud Account and network selection
- Coverage test
- Network size and Reporting Period configuration

For more information related to the WS App features please refer to the Worldsensing knowledge base at https://worldsensing.zendesk.com

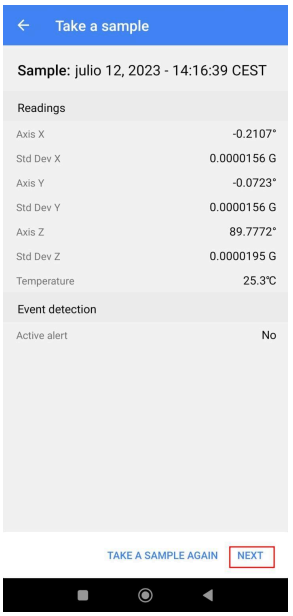


Click next to select the location of the device, to be shown in the map.

Select the location. This can be done automatically (Android device location) or set manually. This step can be avoided if needed.

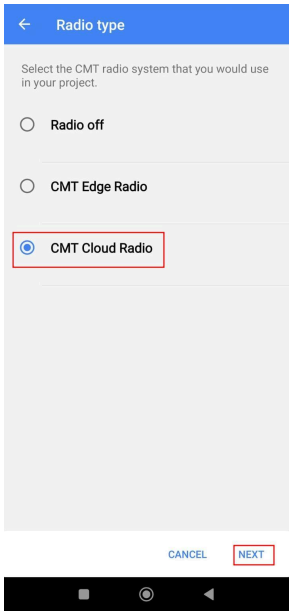


Configure the channels of the device. For devices with sensors included this can be automatic, or a specific configuration may be required. Check the device user guide for more information.

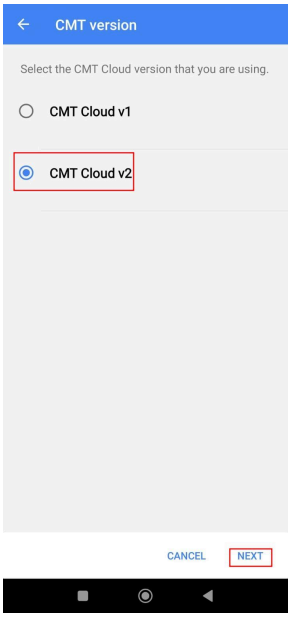


Take a sample to ensure the readings are correct.

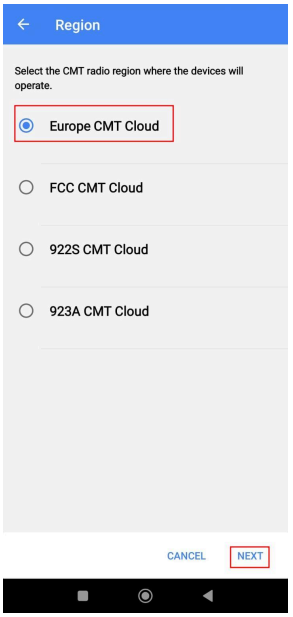
STEP 1: Data logger location, sensor configuration, reading test and resultsSTEP 2: Radio model configuration



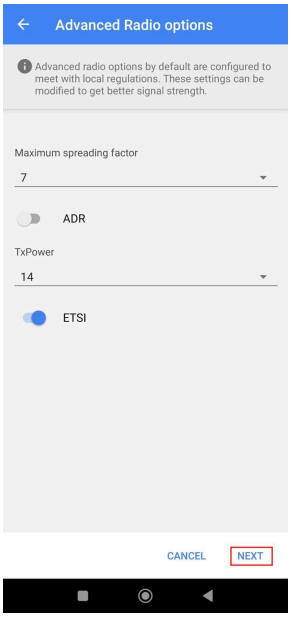
Select the appropriate solution, in this case **CMT Cloud Radio**.



Select **CMT Cloud V2** option.

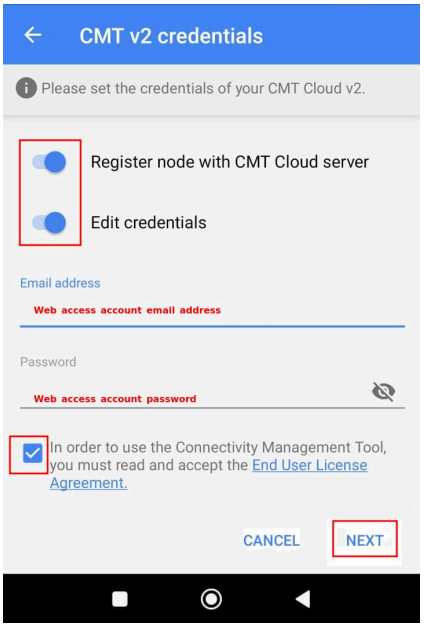


Select the Radio region of the Cloud account. This information is provided with the account credentials and **matches with the gateway configuration.**



Select the advanced radio options. These parameters will vary depending on the radio selected. **It should be left by default, unless radio coverage isn't good enough.**

STEP 3: Cloud Account and network selection



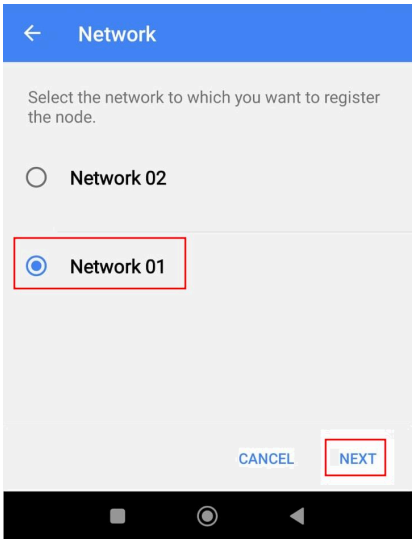
In this step, the edge device will be registered on the Cloud instance.

Once registered, the device will join the Cloud account on the selected network.

For this purpose it is needed enabling the Register Node option in the app (enabled by default).

Enabling the "Edit Credentials" option will allow introducing the Email address and password used to login our Cloud account.

EULA must be accepted to enable the NEXT button.



Once the next button is clicked, the app will access the Cloud platform with the indicated credentials, and will display all existing networks.

The appropriate network must be selected, to register the edge device in that specific one.

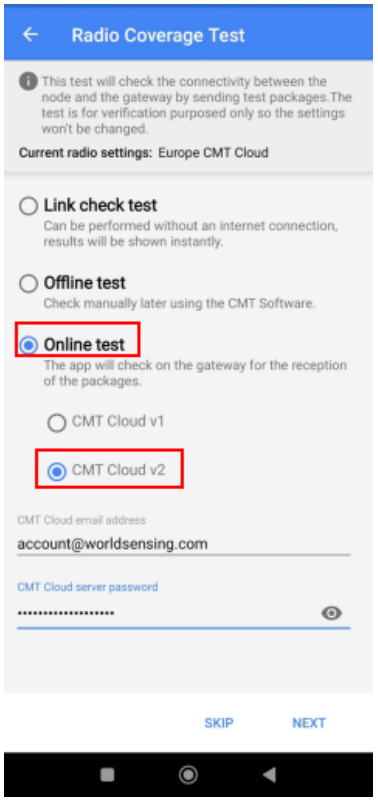
Click the NEXT button to proceed with the Coverage test.

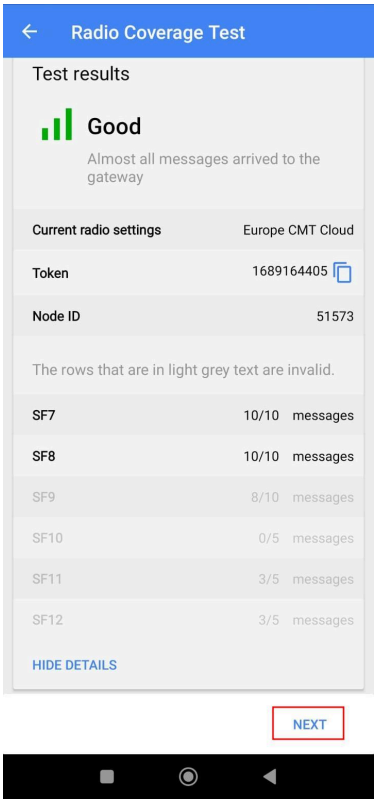
Note: "Register node with CMT Cloud server" option should be selected only in case the edge device being configured is not linked to the required nor any other network nor account (First deployment)

In case the device has already been registered, and therefore linked to a network, this option should be unchecked. Alternatively the device can be deleted from the network, to start a clean new installation. Note that this step will delete the device from the network, Devices group, and data will not remain available.

The WS App allows several independent testings for the device to avoid using the setup wizard, such as taking a sensor reading sample, or forcing a coverage test.

STEP 4: Coverage Test

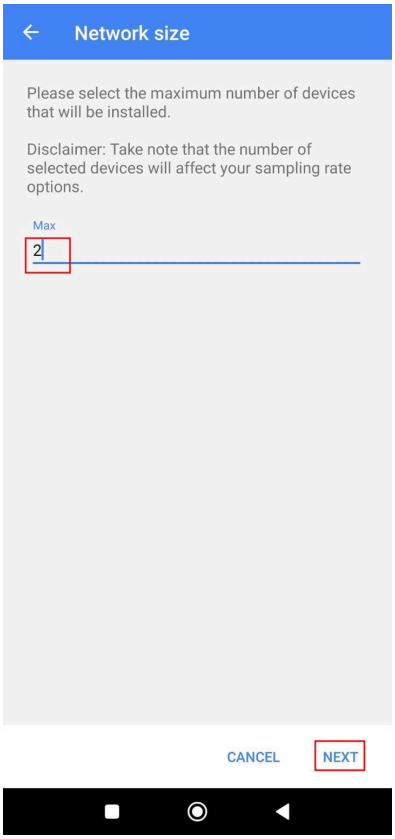




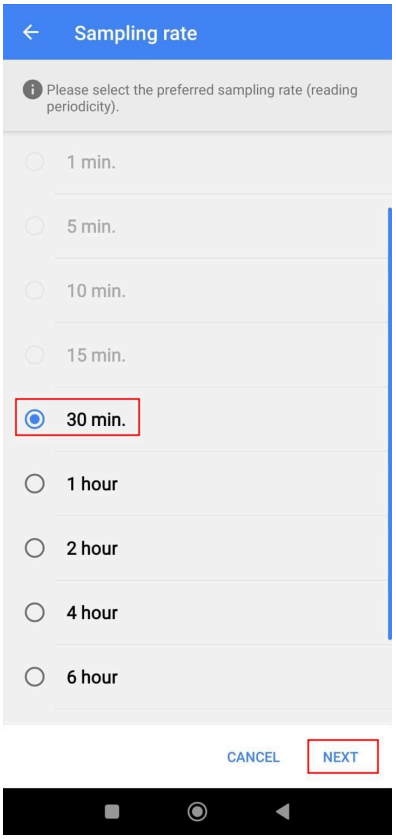
This step is common to all configuration possibilities. Worldsensing recommends using the Online test method, as it displays the results in the app. For this purpose it is needed selecting CMT Cloud option, using the same account credentials used in the previous step.

Alternatively the Link check test may be used, which may take more time in case of limited radio coverage.

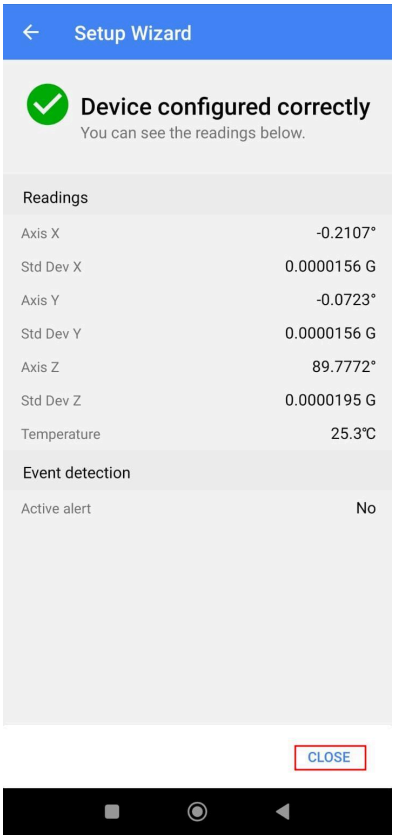
STEP 5: Network size and Reporting Period configuration



Select the network size. This refers to the number of edge devices connected to the specific network, and will discard the shortest reporting periods available. Note that this is CMT Edge oriented, which may limit the next step. Contact Worldsensing if more information is needed.

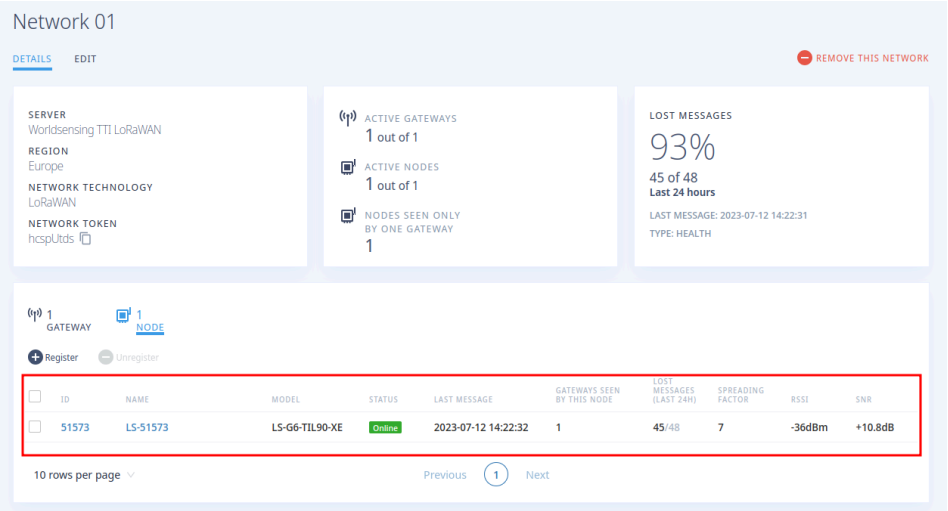


Set the reporting period required for the connected edge device.
It is strongly recommended forcing it from the Cloud platform once the device is connected.



Once the NEXT button is clicked a device resume is displayed, indicating the device has been correctly configured.

Once the setup wizard is complete, the device will appear in the selected network connected at the selected network.



NOTE: The edge device is now connected, but only data related to the Network will be displayed. This means no readings nor Health messages will be available until it gets connected to a Device Group, even data (readings, etc.) is being already registered. This step is described below.

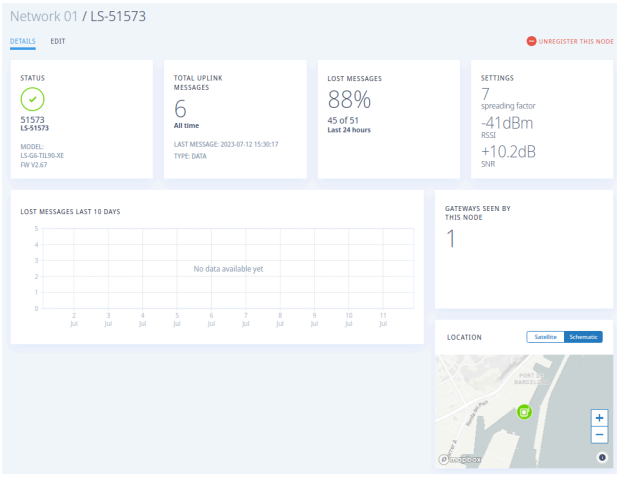
NOTE: Once the edge devices are linked to the network, it is highly recommended setting the reporting period from the platform, to optimize the radio performance, as a good practice.

This method of adding edge devices to the network displays the default reporting period set as 24 Hour, even the configured one is different.

Setting the reporting period from the platform (remotely) will shorten data acquisition time and display the Reporting period correctly, and indicate any possible downlink message issue.

In any case, radio messages will be received as configured with the Worldsensing App.

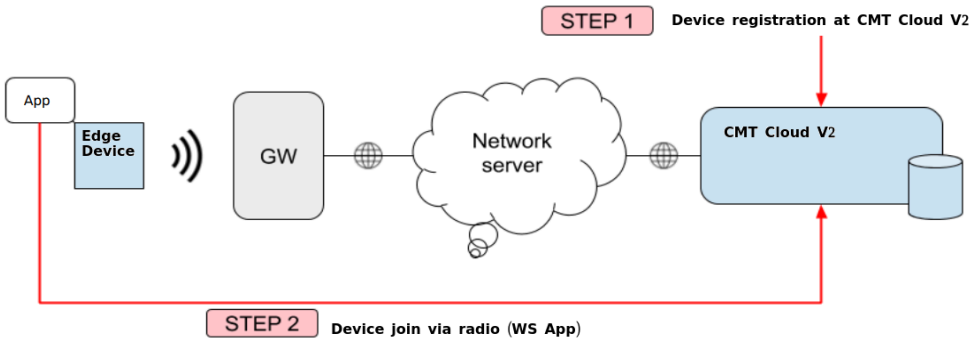
Clicking on the edge device ID or name redirects to the device connectivity status page.



Offline registration

In case the Android device has no Internet connection, the commissioning of the devices will have to be done in two steps. Firstly, the edge device has to be pre registered directly on the CMT Cloud instance.

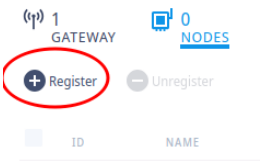
Once this step is completed, use the WS Mobile App to join the edge device. In this specific case, as there is no Internet connection on the device, a network token (automatically generated when the network is created) will be required, as well as the access credentials. In this case the edge device will not be registered, just joined, as this step has been previously done.

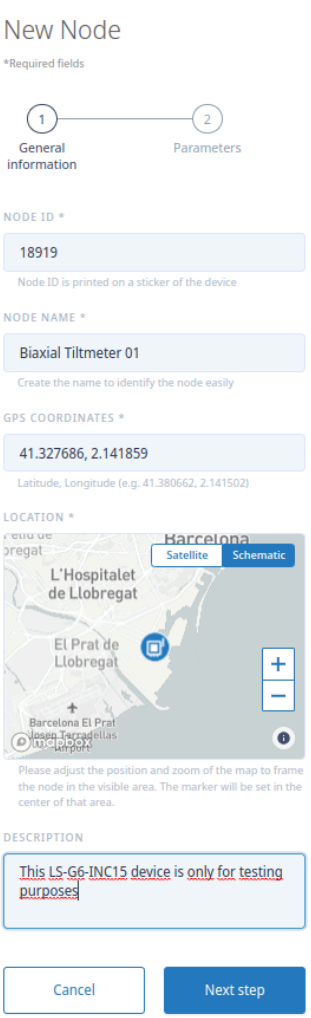


STEP 1: Register the edge device in the CMT Cloud instance

For this step select the network where the edge device is expected to be connected, click on NODES Option, and finally click on the REGISTER button. Once clicked, a setup wizard will be displayed. Click the "Start Registering" button to start the process.

The edge device ID and Radio model will be required as mandatory parameters.





The setup wizard is divided into two different parts.

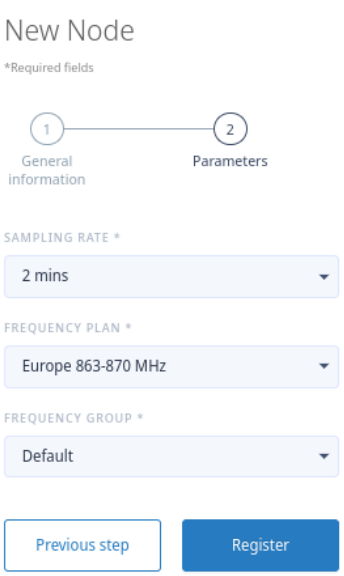
The first one will require edge device and installation related data such as:

NODE ID: By default, this configuration parameter is the same as the serial number.
It can be modified with the WS App if needed, for example for edge device replacement.

NODE NAME: The name used to identify the edge device on the Network.

GPS COORDINATES: In this part, the GPS coordinates can be selected, the same way it is done with the gateways.
This will help display the exact location of the edge device in the maps.
It can be modified remotely at any moment.

DESCRIPTION: Text area reserved for adding information related to the edge device (not a mandatory field)



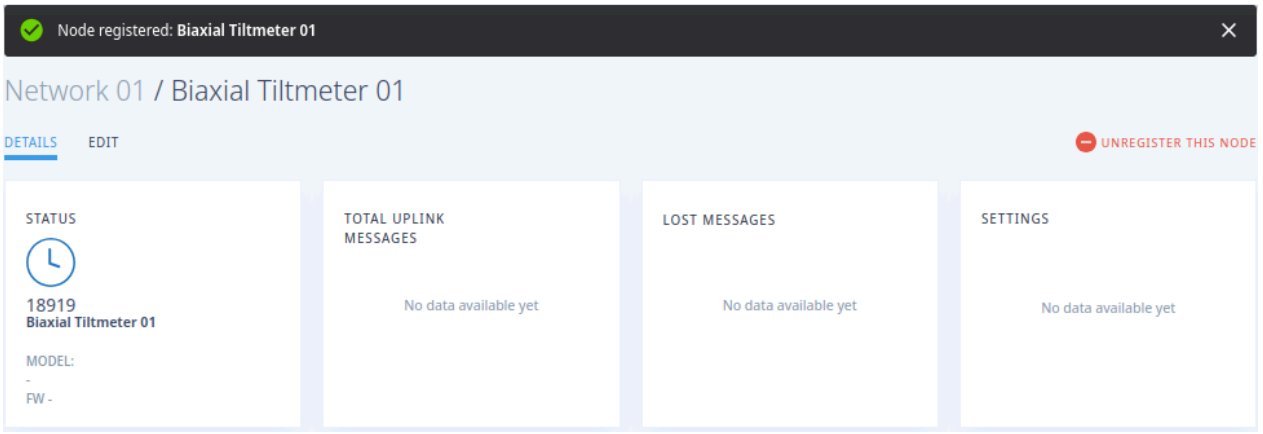
At this second step of the setup wizard, the information related to the edge device configuration will be configured, such as:

REPORTING PERIOD: Frequency of readings of the sensors connected to the edge device

FREQUENCY PLAN: Radio model used by the network. This parameter must match with the Gateway configuration.

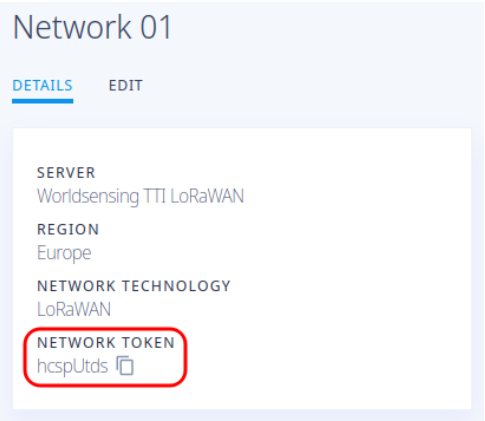
FREQUENCY GROUP: Same as Frequency plan. This parameter may vary depending on the Frequency plan selected.

At this point, the edge device has been registered on the system, but it is not yet operative, as these same parameters need to be configured on the device side. A clock displayed in the Status indicates the edge device is not yet fully operational.



STEP 2: Join the edge device to the network using WS App:

At this stage, using the WS App the same way as the online method, the device must be configured to join the network following the steps indicated below. Instead of logging CMT Cloud using access credentials, the Network token is required. This token is displayed in the network once created at the platform, and is unique for every network created.

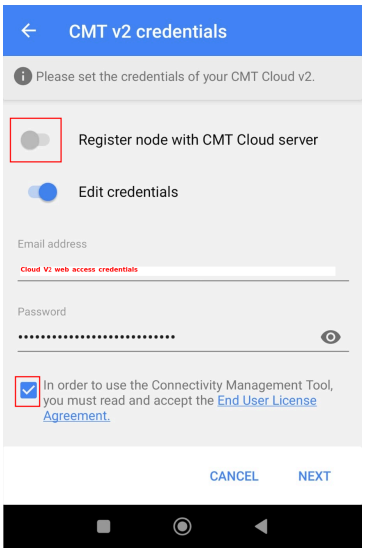


For this commissioning method, the next step will be carried out with the Android device in flight mode. These are the steps on the WS App to be carried out during the commissioning, which is done following the setup wizard option:

- Data logger location, sensor configuration, reading test and results: This step is equal to the one carried out during the online commissioning, except the Location step, which is not available in the app, as it has been configured during the registration from the platform at the first step.

- Radio model configuration: This step is exactly the same as in the online commissioning procedure.

- Cloud Account and network selection: This step requires a different configuration:

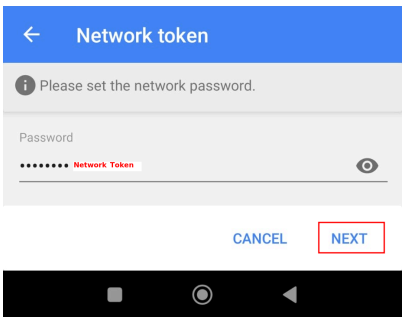


At the "CMT credentials" option, some changes are needed:

Disable the Registration of the edge device, as this step has been done directly on the CMT Cloud platform.

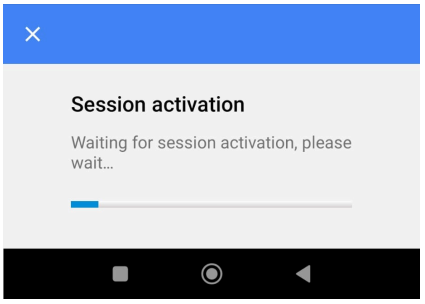
Same credentials must be inserted.

Please read and confirm your acceptance of the EULA by ticking the appropriate box. In this case we're in compliance with the legal requirements.



At the next step, the network token must be inserted.

This token will associate the edge device with the Network where it was registered previously.



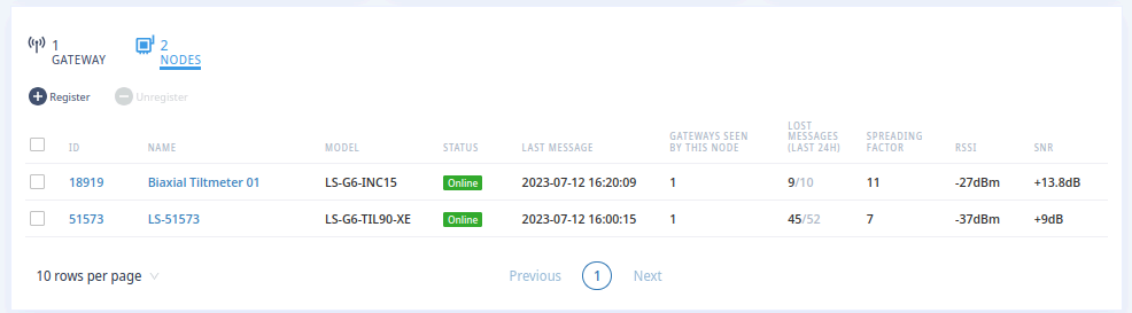
Once the Next button is clicked, the session is activated.

If all parameters have been correctly configured, this step will redirect to the coverage test steps. Otherwise, an error message may be displayed.

- Coverage test: As there is no way to connect the WS App to the Cloud platform, Online coverage is not available. Offline and Link check test options are available only. Check the WS App user guide available at our knowledge base for more information.

- Network size and reporting period configuration: This step is exactly the same as in the online commissioning procedure.

Once the setup wizard is finished, and the system starts receiving radio messages, the node appears online and connected.



NOTE: It is highly recommended setting the same Reporting period in both cases:

At the CMT Cloud platform during the edge device registration

At the WS Mobile App during the commissioning.

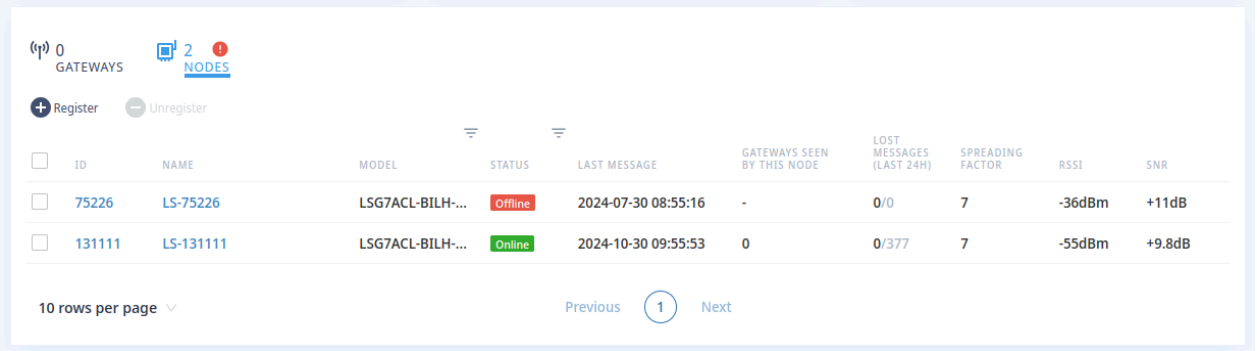
This way the configured reporting period (via WS App) and the reporting period modification window (the one set during the registration on the software) will match, having a real reporting period displayed on the software from the beginning.

The CMT Cloud system will define an edge device as **Offline, showing it in RED** color in the network, as soon as two expected messages are not received at the cloud account. For example, it will turn red and show as offline in two hours for a one hour reporting period configured edge device.

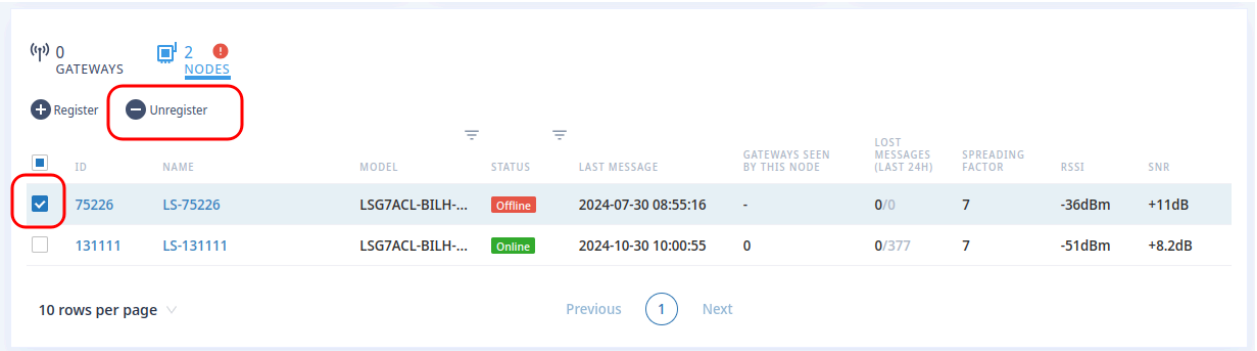
In the same way, an edge device will be displayed as **Pending (blue)** in case the device has been registered in the network (via App or manually on the platform) but no radio message has been

received. This could indicate a misconfiguration or either a lack of LoRaWAN coverage during the commissioning.

Connected Gateways and Edge devices can be checked and listed in the Network. The Network, as a connectivity layer, will display information and allow sorting by different parameters.



Selecting a specific Gateway or Edge device will allow checking (but not modifying) the network configuration, as well as radio status parameters. Modifying radio parameters for a specific device will require deleting the device from the network, and commissioning it again, selecting and deleting it.



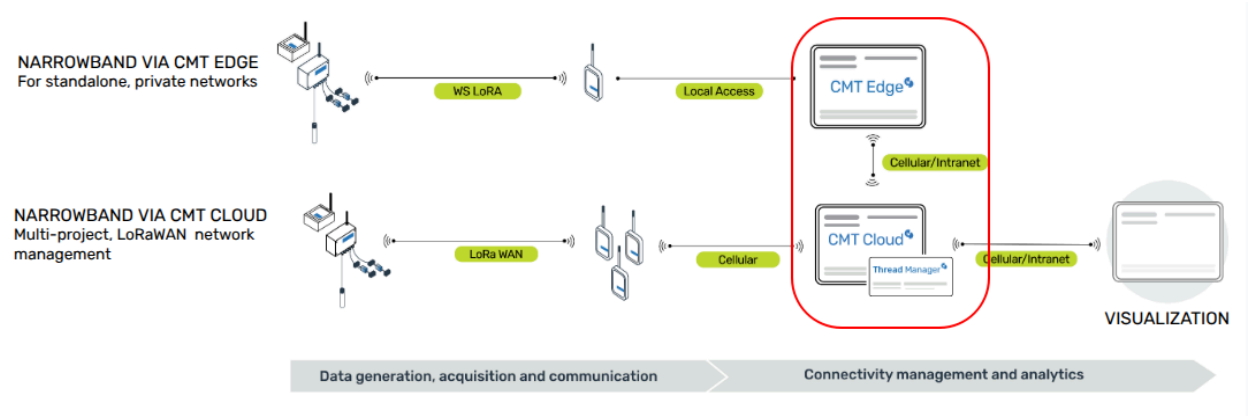
Dual Management: CMT EDGE network link (LoRa network)

CMT Edge gateways can be linked to the CMT Cloud account as a specific network.

This allows joining as many Edge gateways as needed to an account, and manage the measurements taken by the data loggers grouped in device groups. This aims to achieve the end to end connectivity among all our products in the portfolio, where now CMT Edge is one end and CMT Cloud is another one.

From a CMT Cloud perspective, CMT Edge gateway will be added to the platform as a network. This way, it will be possible to mix both LoRa (edge) and LoRaWAN (cloud) networks in a unique site or devices group, simplifying the big projects network monitoring and integration, unifying all measurements.

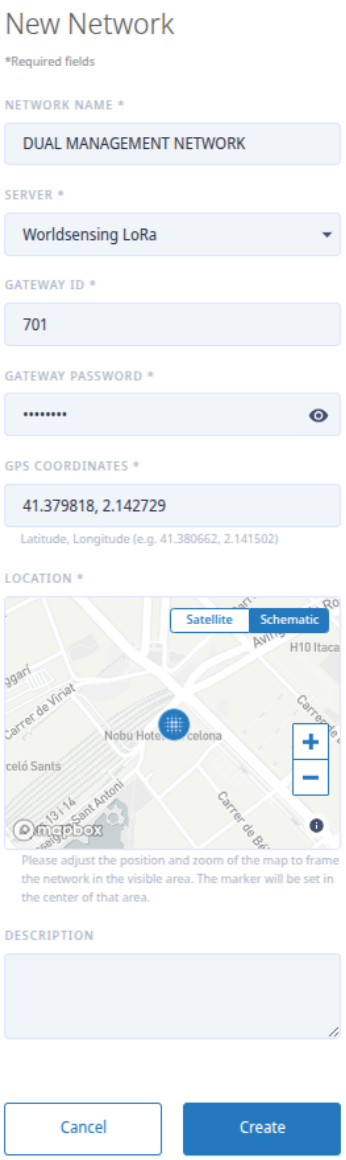
The scheme below represents a CMT Edge gateway linked to an existing project.



All CMT Edge gateways, with Firmware version 2.10 onwards are preconfigured to be added to a CMT Cloud account as a network. All data between CMT Edge gateway and CMT Cloud platform is encrypted and secured.

NETWORK DEPLOYMENT

A new network must be created to link a gateway to the system. The gateway must be online (Internet connected, Remote tunnel enabled) for a successful network deployment.



The CMT Edge Network deployment proceeds as outlined below:

NETWORK NAME: Set a network name which will identify the gateway. Gateway ID can be set for faster identification.

SERVER: Select "Worldsensing LoRa" Server option.

GATEWAY ID: Set the Gateway of the CMT Edge Gateway. This parameter can not be modified in the gateway, it is a fixed parameter available in the Gateway stickers, and the Gateway information sheet.

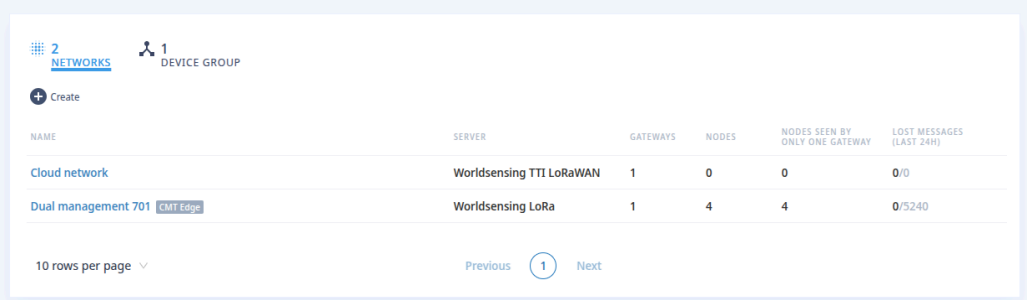
GATEWAY PASSWORD: Password used for 'admin' user login via web.
NOTE: Modifying this parameter after linking the gateway will provoke network disconnection.

GPS COORDINATES: Network location in the map.

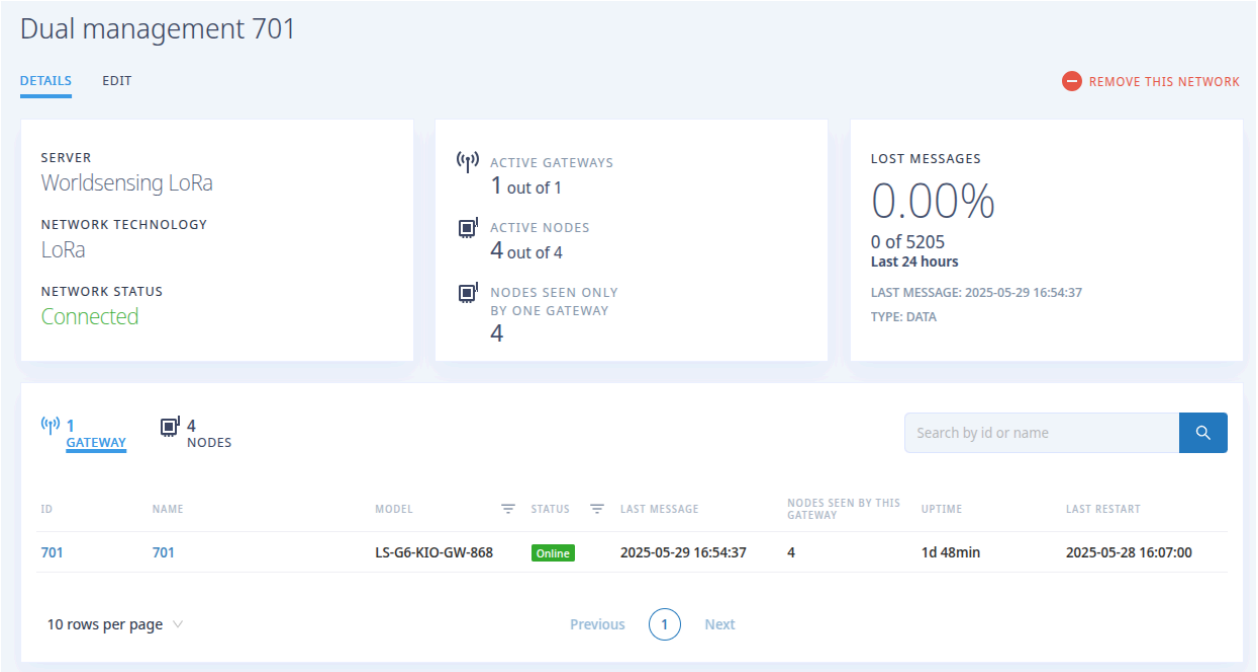
DESCRIPTION: Not mandatory text field.

Once the form is correctly filled, click on the CREATE button.

Once the procedure has been finished, a new network, marked as CMT EDGE will appear in the Networks list, displaying the same parameters a LoRaWAN network does.



Selecting the Network also displays the same parameters a LoRaWAN network does, except the Network Status option, which may appear as Pending (no data has arrived yet to the gateway), Connected (OK) or Disconnected (gateway offline, only displayed after Connected status)



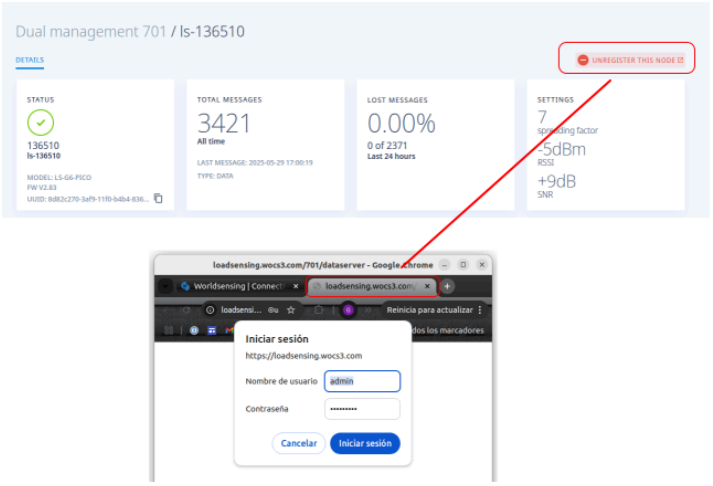
This network has a unique Gateway (The edge gateway itself), and does not allow adding any other Gateway or data logger, which should be connected to a LoRaWAN network.

Dual management feature allows receiving data from CMT Edge gateways to the Cloud platform for data management, but it does not allow bidirectional communications. Data flows from the gateway to the Cloud, but no orders can be sent in the reverse direction.

This means there are some operations that can not be managed from the Cloud platform, such as:

- Reporting period modification
- Sensor configuration (eg, vibration meter node, Event detection system)
- Network elements modification (deleting and adding nodes)

All these operations have to be done in the CMT Edge gateway directly. Trying to apply them from the Cloud platform will open the Gateway URL in an independent tab of the navigator. For example, trying to unregister a data logger from the network associated with the gateway XXX will open a new tab at https://loadsensing.wocs3.com/XXX to manually delete the mentioned node.



Also, no historical data will be dumped to the CMT Cloud account. Only new measurements will be registered in the associated LoRa network. Configured engineering units are not eigher transmitted.

Deleting the network will delete all the devices linked to the gateway, and the gateway itself.

Device Groups creation and management

Device groups are the part of the platform where edge devices and gateways are grouped to organize them in groups required by the project. These groups will later be used to create integrations (MQTT and FTP integrations with third party platforms, such as monitoring software, etc.)

Creating device groups and adding the devices to one of them is mandatory to start getting messages (Readings, Health…) on the platform. Also, it is a mandatory step to integrate CMT Cloud with third party software.

Each edge device or gateway can be assigned to a unique device group, organizing the devices as required (For example, by geographical location, type of sensors installed, specific part of a project, etc.). It is recommended planning both Network and Device groups scheme before starting the deployment.

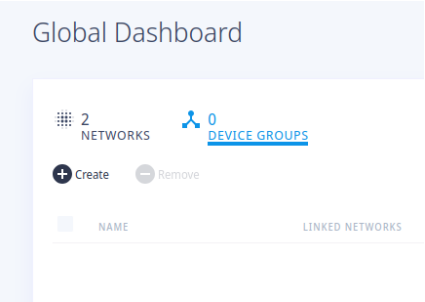
There is no limitation on the Network and device groups link:

- A unique network can be linked to a unique Device Group (Simple configuration)
- A unique network can be shared by different Device Groups
- Multiple networks can be linked to a unique Device Group
- Device Groups configuration can be duplicated (Two different Device Groups may have the same networks linked)

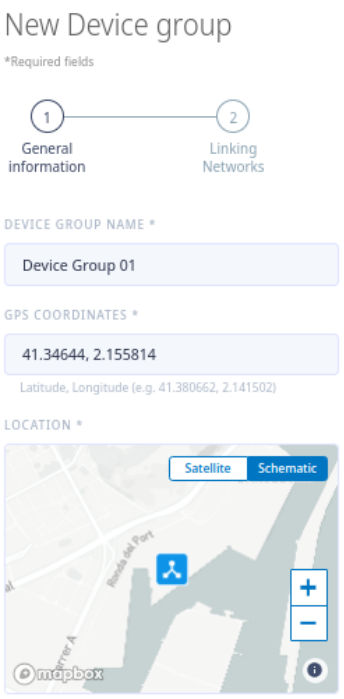
The only limitation is that a specific Edge Device or Gateway can only be linked to a unique Device group. Once a device is added to a Device Group, this device will not be available for other Devices groups, even the network it belongs to is linked to this second one.

Device Groups deployment

Device groups are created at the dashboard, selecting “DEVICE GROUPS” option and clicking “+ CREATE” button



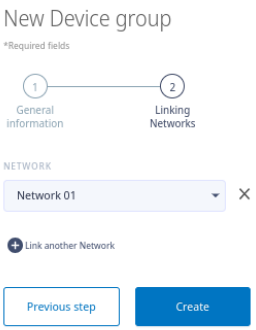
Add the required fields in the wizard displayed to create the group:



DEVICE GROUP NAME: Name of the Device group (to be displayed)

GPS COORDINATES: Location of the network icon in the map. It can be selected with the map below.

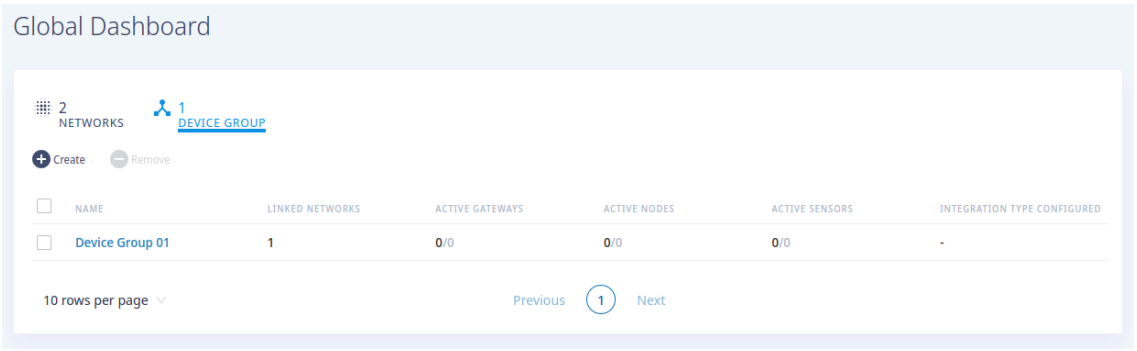
DESCRIPTION: Text area reserved for adding information related to the network (not a mandatory field)



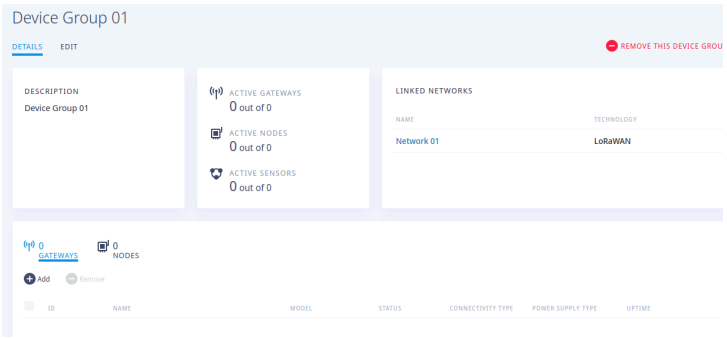
NETWORK: Select the network to link to this device group. More networks can be linked by selecting the " + LINK ANOTHER NETWORK" button.

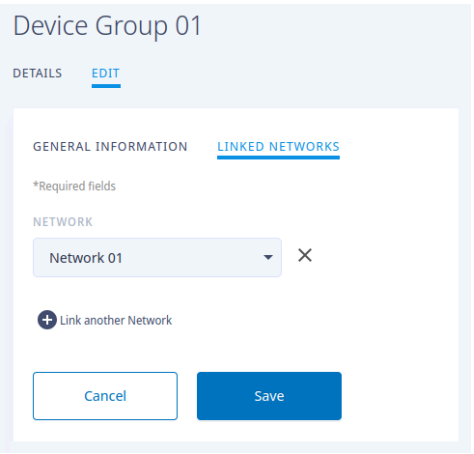
The edge devices registered in these networks will be applicable to be grouped in the Device Group.

Once clicking the Create BUTTON, the devices group is created.



The information related to this item can be checked by selecting it. Also, the configured parameters, as well as the linked networks can be modified, added or deleted by at the Edit menu, at GENERAL INFORMATION and LINKED NETWORK submenus .



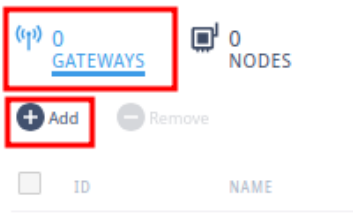


Device Groups management

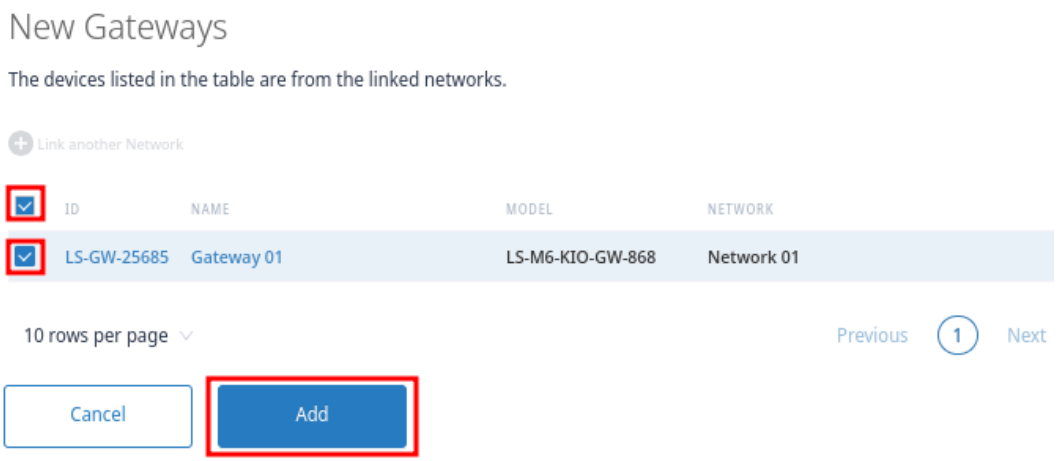
The next step of the project deployment is adding the edge devices to the Device groups. Adding them will allow monitoring data (readings and health messages) of all the sensors connected to the devices, creating integrations to redirect them to third party software platforms and creating business rules. This step is mandatory to get data on the system.

Adding Gateways and Edge Devices

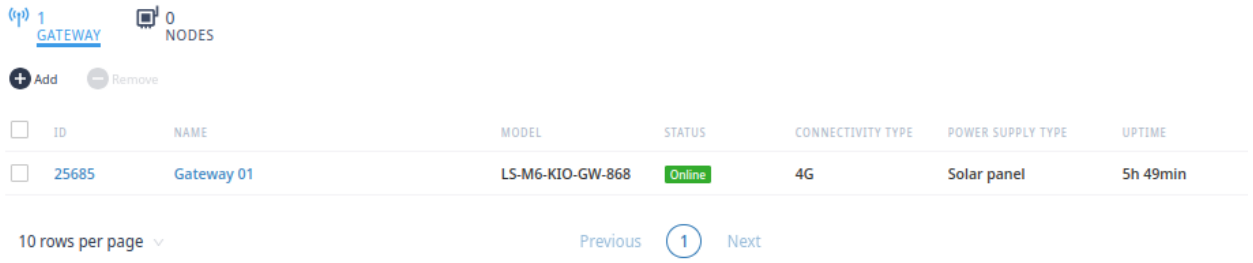
Adding both Gateways and devices to a specific device group is done by clicking on the "+ Add" button on both Gateways and Nodes option, and selecting the devices to be added to the group.



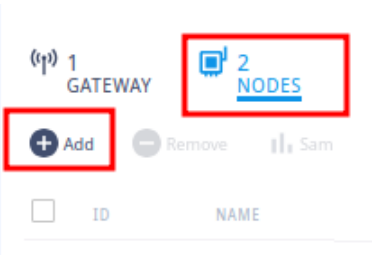
Once the type of device to connect is selected, a list of devices will be displayed. Only the devices not added previously to any other device group will be applicable to be added.

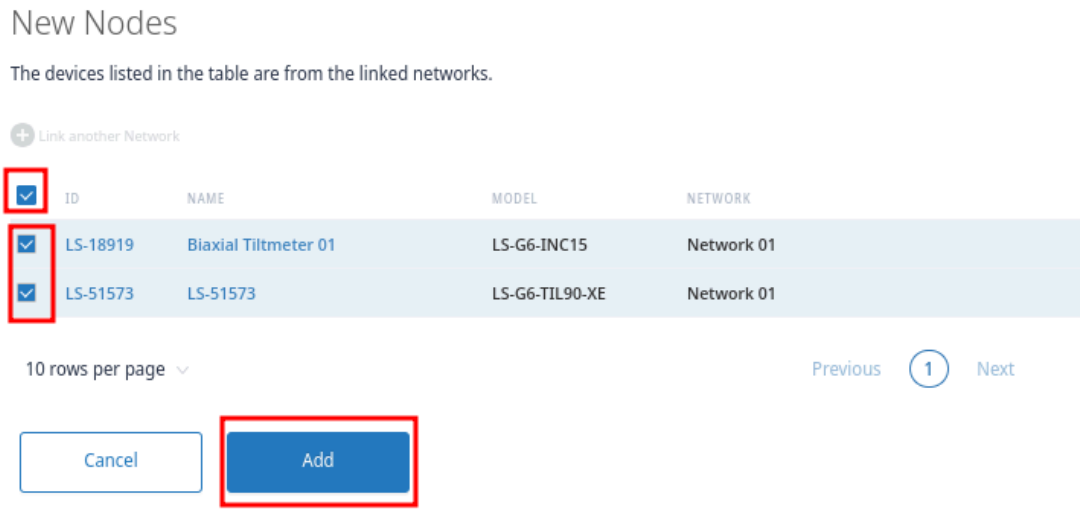


Clicking ID will select all the devices listed below. Alternatively specific devices can be selected and added to the device group by clicking add. For this specific case, Gateway 01, connected to Network 01 will be added to the device Group 01.



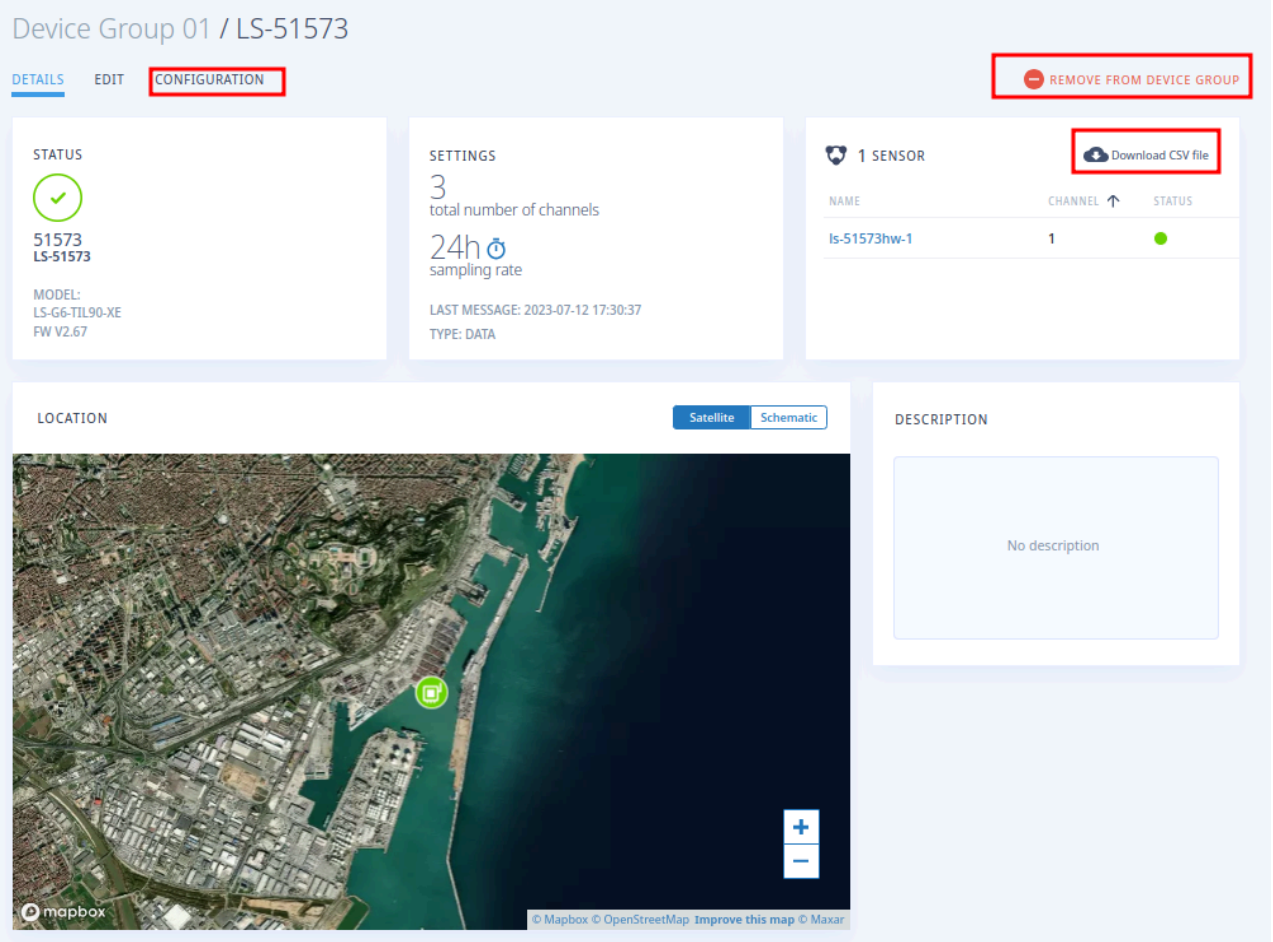
The same procedure is required for edge devices; This process will add Both Biaxial Tiltmeter 01 and LS-51572, connected to the Network 01, to the Devices group 01





NOTE: Registered (directly from the server) but not commissioned yet edge devices can be added to the devices group. This allows creating a software level structure before commissioning devices on field, ready to receive information.

Once all gateways and edge devices are linked to the devices group, all these devices will start registering readings on the Cloud platform. This information is available at the page displayed by clicking the specific edge device, where several tasks can be carried out, such as CSV files manual download and reporting period modification, among others.



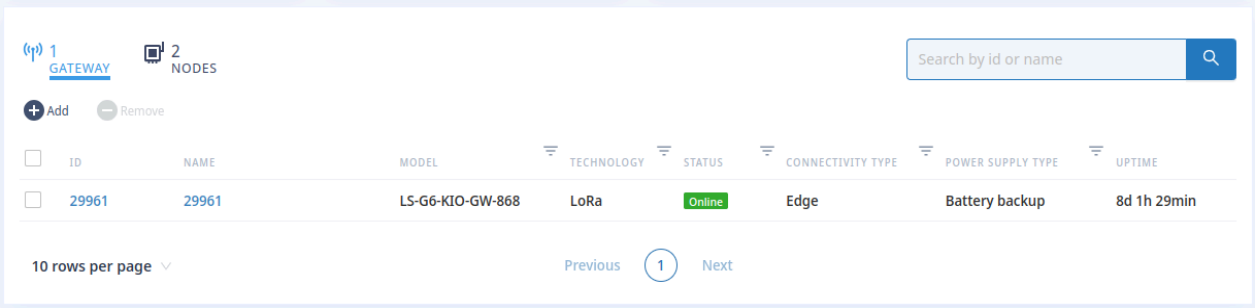
Other operations with Gateways and Edge Devices

GATEWAY AND EDGE DEVICES SEARCH AND LISTING

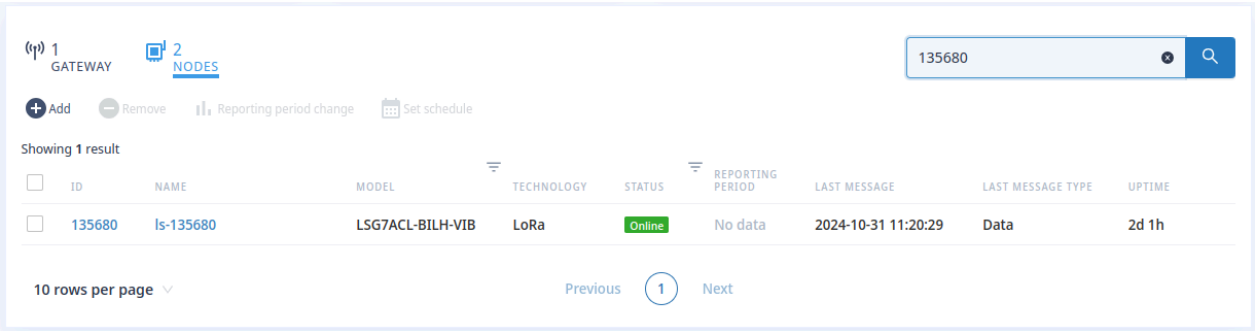
CMT Cloud platform allows ordering and filtering both Gateways and Edge devices by different parameters of the tables.

Gateway list can be filtered by all of the parameters of the table (except ID and name).

The Text box in the top right corner allows searching for a specific gateway by selecting the ID (Gateway ID) or NAME (name added during the gateway commissioning)



In the same way, edge devices can be searched and filtered according to different parameters shown in the list, such as Model, technology and Status



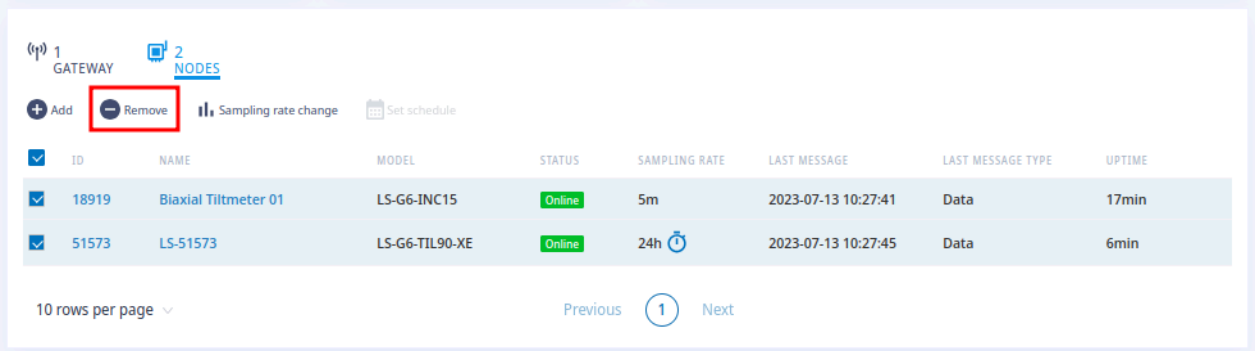
GATEWAYS AND EDGE DEVICES REMOVAL

All devices can be removed from a specific Devices Group, or even moved from one to another.

Edge devices are deleted by clicking the REMOVE FROM DEVICE GROUP button and accepting the alert message.

Note that deleting a gateway or edge device from a devices group will not unregister the device from the network, which means it will remain connected and available to be added to a different device group.

Alternatively, the devices can be deleted in batch, by selecting them from the Device group list and clicking on Remove button.



Once edge devices are deleted, no new data relative to the edge devices will be stored on the system, until they are connected to a new one. The existing data will be stored, but not available, until the edge device is connected again to an existing device group.

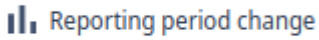
Moving edge devices from one group to another can only be carried out in two steps:

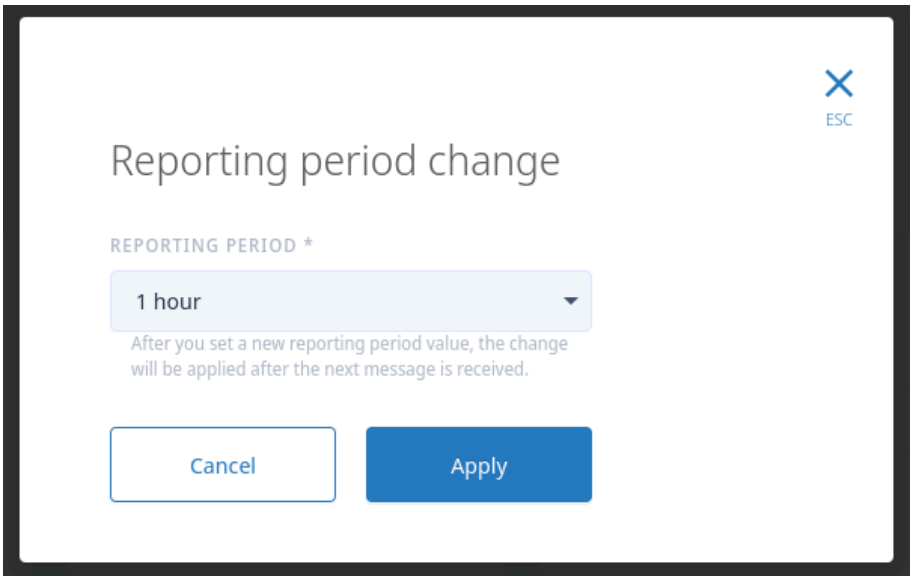
- Delete the required gateways and edge devices as described in this section
- Add them to a new Device Group as described in the previous section

REPORTING PERIOD MODIFICATION

As well as Devices add and removal, reporting period can also be modified.

Clicking the Reporting period change button with several edge devices selected allows modifying the reporting period to all selected devices.





Once applied, the Cloud platform will send downlink messages to the edge devices to apply the change. This message may be sent several times until it is applied, displaying an icon in case it has been or has not been applied.

This feature is available for all devices connected using LoRaWAN technology (CMT v2 direct connection, not available for Dual management connected nodes)

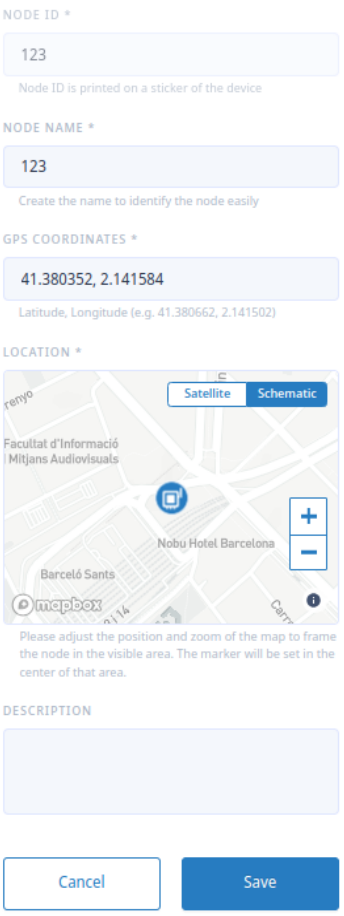
NOTE: Specific edge devices may display different features such as configuration of the sensor on this tab.All these features are also available on Edge device configuration.

EG:LS-G6-LAS-TIL90 devices, with firmware 2.79 or higher also allow configuring the laser schedule.

Edge devices configuration

There are several operations that can be done on Edge devices at Devices Groups paragraph. These operations are available at EDIT and CONFIGURATION tabs

EDIT TAB OPTIONS



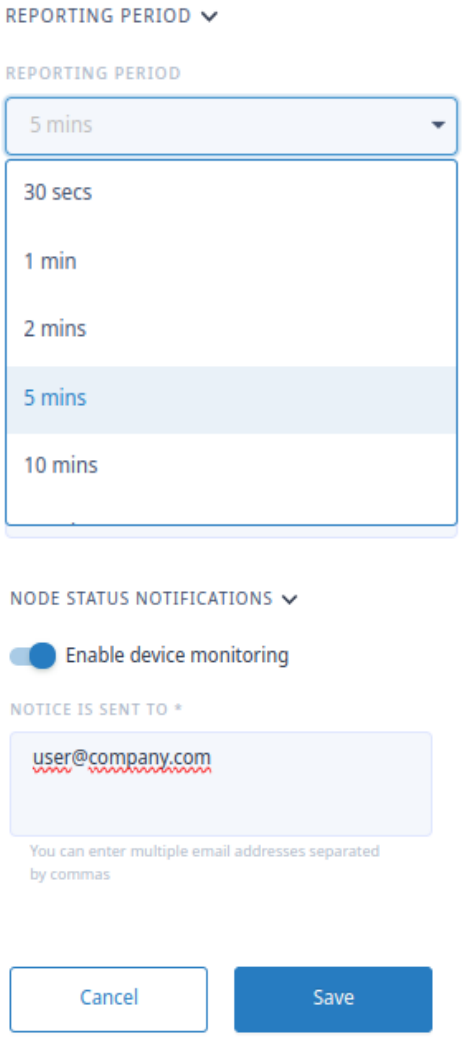
On this area general information that is displayed on the Devices group can be modified, such as:

NODE NAME: Name of the edge device to be displayed at the device group.

GPS COORDINATES: Location of the edge device icon in the map. It can be selected with the map below.

DESCRIPTION: Text area reserved for adding information related to the edge device (not a mandatory field)

CONFIGURATION TAB / GENERAL SETTINGS



In this area, specific information related to the edge device can be configured.

REPORTING PERIOD:
This scroll option will allow modifying the reporting period of the specific edge device.

The shortest reporting period is every 30 seconds, while the highest one is providing a reading every 24 Hours. Dishonored RP may be configured if required.

NOTE: The reporting period modification window is the one configured on the device via app.

The CMT platform will display 24 Hours by default for online configured edge devices, until the reporting period is modified remotely.

NODE STATUS NOTIFICATIONS:
Turning on this option enables edge devices notifications, related to the status of the device within the device group.

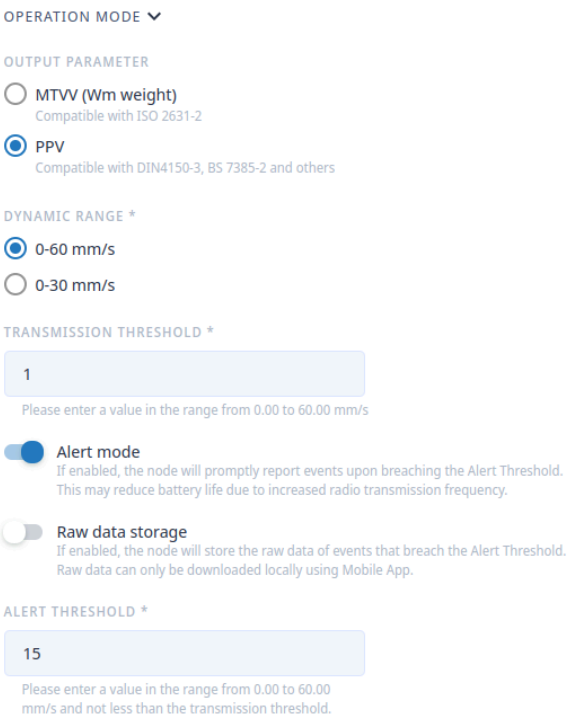
Main monitoring notifications refer to the connected and disconnected status of the device in the group.

An email account must be set to receive the notifications.

Specific sensors also may allow specific configurations on this tab. Check the edge device user guide for more information related to the specific device.

As an example, the LSG7ACL-BILH-VIB (Vibration meter device) allows configuring the protocols and thresholds remotely, including the alert threshold in case the device firmware version is 3.3 or higher.

Note that this tab may or may not contain any configuration options, depending on the edge device model, as well as the firmware version running.



In this area, the operation mode and thresholds can be configured:

OUTPUT PARAMETER: Allows configuring MTVV or PPV method.

DYNAMIC RANGE: Selects the range for the data to be used with PPV.

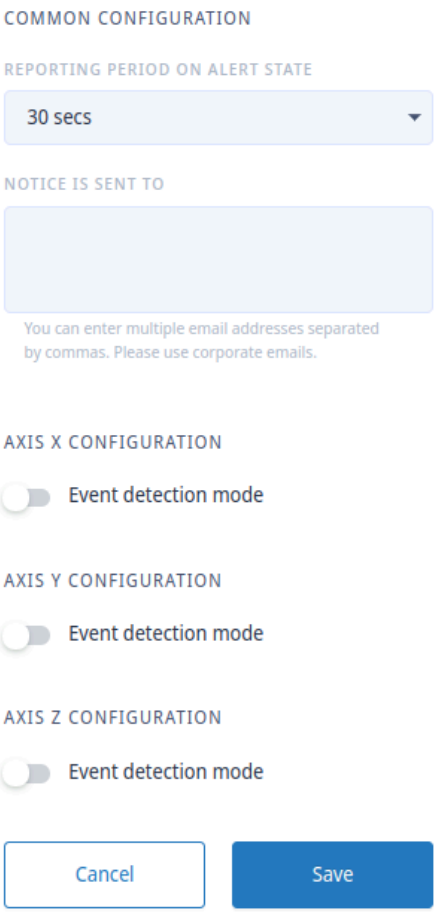
TRANSMISSION THRESHOLD: All data above this threshold will be registered.

ALERT MODE/RAW DATA STORAGE: enables the alert mode (priority messages above an alert threshold) and allows storing RAW data on the device.

ALERT THRESHOLD: (Any event above this second threshold will be broadcasted via radio with high priority message (near real time)

CONFIGURATION TAB / EVENT DETECTION

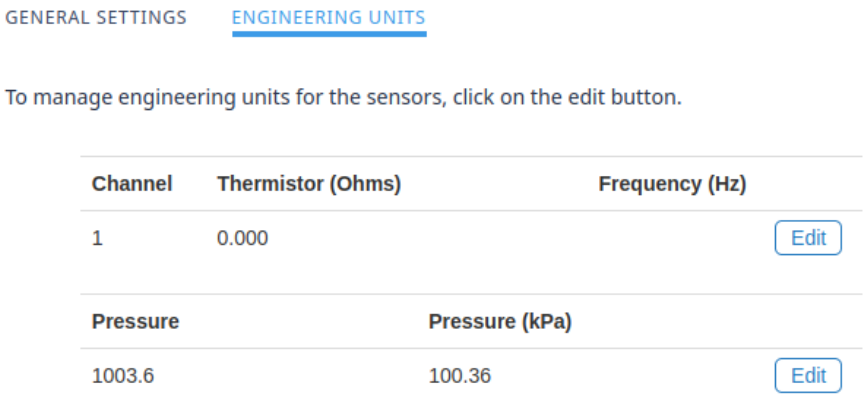
Specific data loggers may also be remotely configurable from a specific tab. This is the case of the event detection solution, which has a specific tab for Event detection thresholds configuration, as well as the new reporting period on alert state.



CONFIGURATION TAB / ENGINEERING UNITS

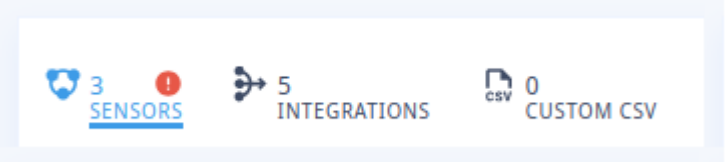
This tab is available on CMT Cloud V2 with V1 compatibility enabled. It allows enabling and configuring Engineering units. Note that this feature is configured on the Data management tab, selecting the sensor for standard CMT Cloud deployments (without V1 Compatibility).

Clicking the Edit button on the sensor to be configured, redirects to the engineering unit setup page. This setup page will require enabling and configuring the sensor selected the same way it is configured on CMT Edge



Data Management

This section of the CMT Cloud platform manages the information at sensor level, and allows managing integrations with third party software platforms. It is divided in three different areas:



Sensors

This part displays all sensors configured on the existing edge devices. Lists all instruments sending readings to the system to manage them as required. Unlike Networks (connectivity layer) and Device Groups (Device layer) this one lists all sensors independently from the devices.

It is accessible from the Devices groups tab, by selecting the sensor of a specific edge device.

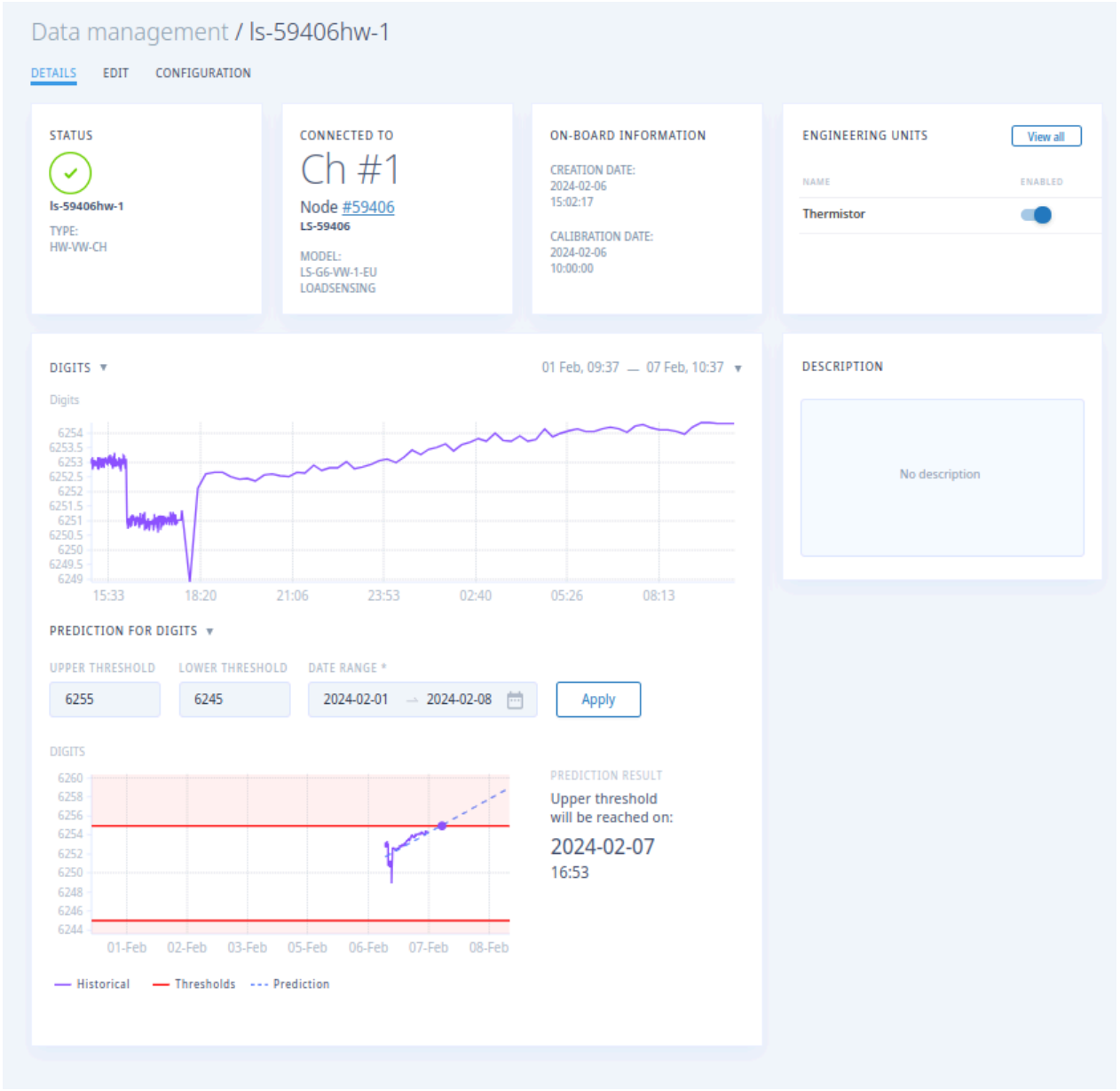
This sensor level layer allows monitoring and managing a specific instrument connected to a specific channel of the device independently.

At this point, some features can be implemented, such as engineering unit conversion, event detection system (EDS) alert threshold configuration, etc..

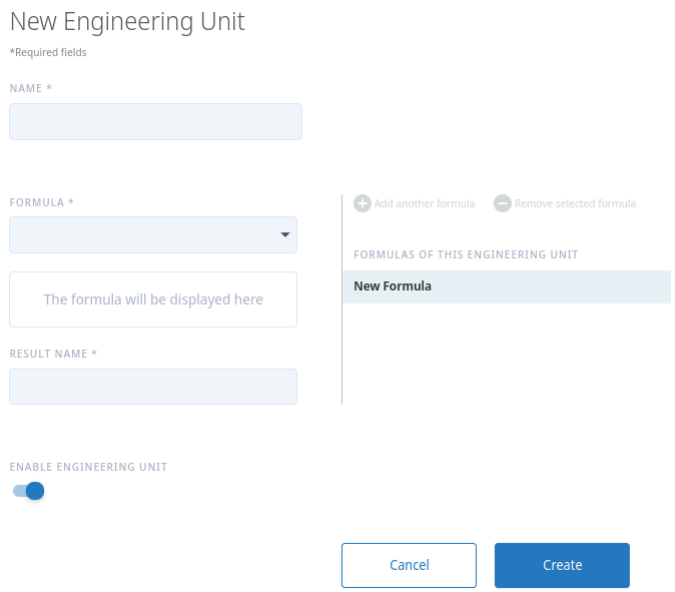
A time graph is available to display the different parameters of the selected device, where the specific parameter and time period can be displayed. For example, Thermistor, Pressure and Frequency (both Hz and digits) could be displayed for a Vibrating wire device, as well as the configured engineering units.

In parallel, a LINEAR prediction tool is available for every one of the parameters registered by the system. This tool allows configuring a time period (date rage) and two (upper and lower) thresholds. According to the data registered, this tool will predict and display an expected threshold reach date.

In the EDIT tab, the user can add specific information about the sensor: name, calibration date and time, and sensor description, if needed.


Data management / ls-59406hw-1
DETAILS
EDIT
CONFIGURATION
STATUS
ls-59406hw-1
TYPE:
HW-VW-CH
CONNECTED TO
Ch #1
Node #59406
LS-59406
MODEL:
LS-G6-VW-1-EU
LOADSENSING
ON-BOARD INFORMATION
CREATION DATE:
2024-02-06
15:02:17
CALIBRATION DATE:
2024-02-06
10:00:00
ENGINEERING UNITS
View all
NAME
ENABLED
Thermistor
DIGITS
01 Feb, 09:37 — 07 Feb, 10:37
Digits
6254
6253.5
6253
6252.5
6252
6251.5
6251
6250.5
6250
6249.5
6249
15:33
18:20
21:06
23:53
02:40
05:26
08:13
DESCRIPTION
No description
PREDICTION FOR DIGITS
UPPER THRESHOLD
6255
LOWER THRESHOLD
6245
DATE RANGE *
2024-02-01
2024-02-08
Apply
DIGITS
6260
6258
6256
6254
6252
6250
6248
6246
6244
01-Feb
02-Feb
03-Feb
05-Feb
06-Feb
07-Feb
08-Feb
PREDICTION RESULT
Upper threshold
will be reached on:
2024-02-07
16:53
Historical
Thresholds
Prediction

The CONFIGURATION tab allows configuring Engineering units



Each device will have available the associated Engineering configuration formulas, which can be implemented with the calibration sheet information of the sensor, and saved by clicking on the Create button. These engineering units may be disabled or even removed at any moment.

Important! The NAME field will be included in the CSV header and will determine the sorting of the columns in alphabetical order. If a specific sorting order is required for the engineering units in the node reading CSV file, it is important to properly introduce the names, taking into consideration the sorting criteria.

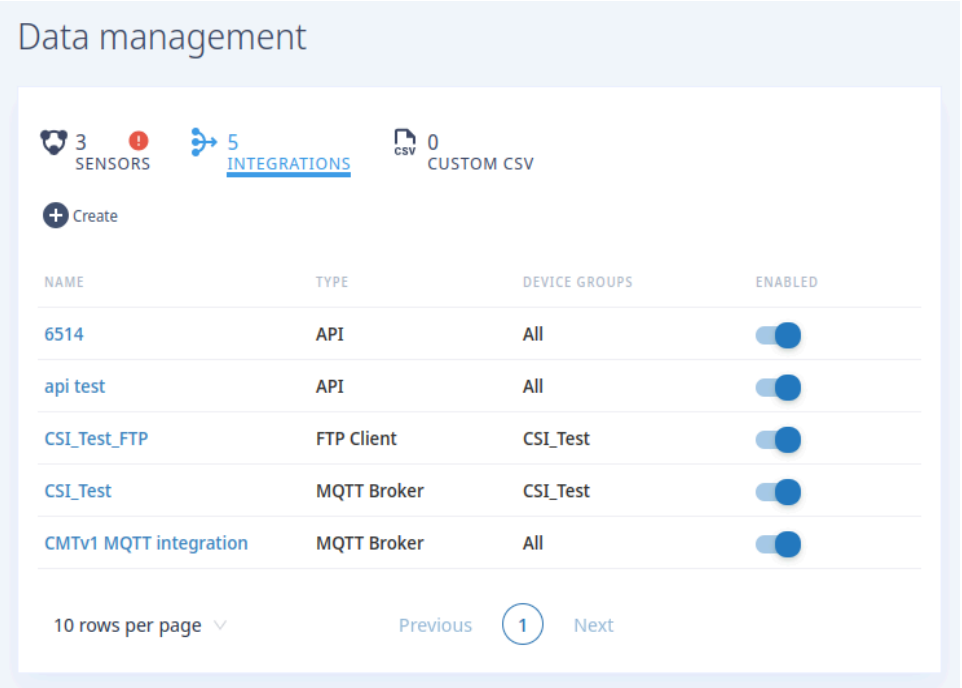
Integrations

This area allows configuring a connection between CMT Cloud V2 and third party software platforms. This could be a monitoring platform, data backup system, etc.. It can be done using two different methods: FTP, API and MQTT.

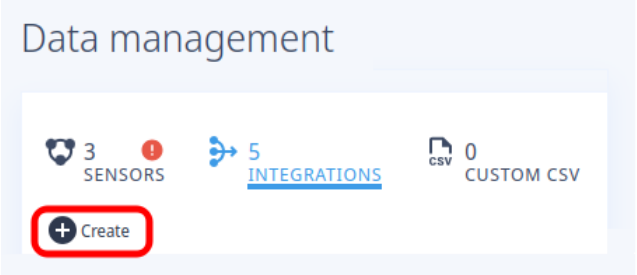
MQTT BROKER: This integration will create a MQTT broker connection and provide the information needed to connect the monitoring platform to it (url, topic, credentials, etc…)

FTP CLIENT: This integration method will configure a FTP Client on the Cloud software. It will allow connecting to any FTP Server, with different configurations (FTP/FTPS, connected sensors and path selection, file upload method and storage period among others).

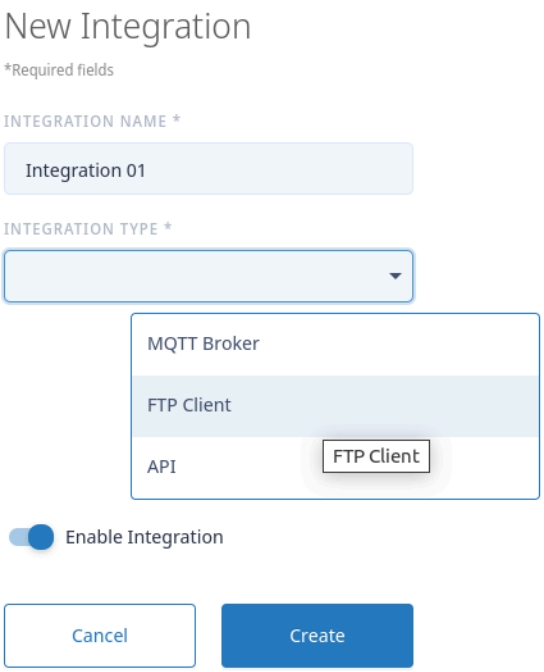
API: Will enable the REST API Calls integration and will generate the required API key. Check Worldsensing Knowledge base to get the detail of the available API calls. API Calls are only available at CMT V1 Compatibility mode. All data stored in Cloud server databases is also available through the Historical API, which allows getting all readings available in the database in a specific period of time.



Data sharing with third party software requires a new integration. For this purpose it is necessary to Click on + CREATE button and follow the wizard displayed. This process will vary depending on the type of integration to be implemented.



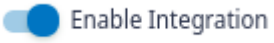
Integration method selection



The initial screen requires setting a name to the integration to identify it in the integration list.

Also, the available methods will be displayed. Currently three different options are available: API calls, FTP Client and MQTT Broker

Ensure the integration is enabled to start working as soon as it is implemented:

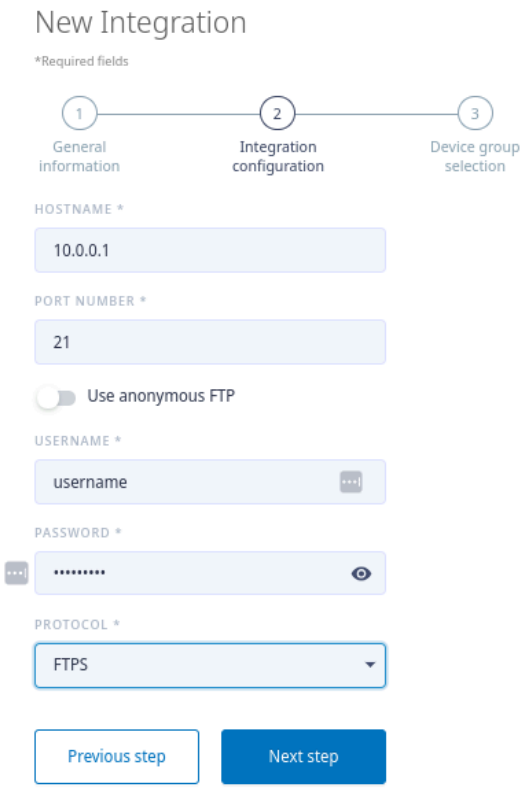


FTP Integration configuration

The FTP integration will redirect all reading related to a specific Device group or batch of Device groups to a specific FTP server.

As many integrations can be implemented, which means that readings from different groups of devices can be redirected to different FTP Servers with different configurations.

FTP Client will upload the newly arrived data every 10 minutes. In case new readings are not uploaded, this information will be stored in a buffer and uploaded in the next try, avoiding data loss due to lack of connectivity or any other possible issue.



The next step will request the FTP Server parameters. It is mandatory having the FTP server already deployed, with the FTP User, folders and subfolders created with the appropriate permissions and ports open.

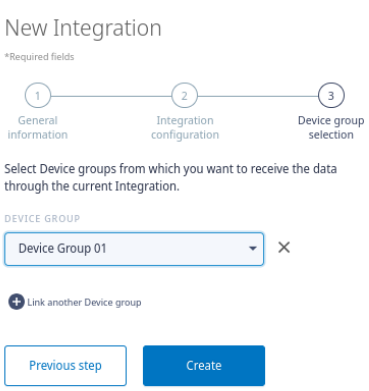
HOSTNAME: Host name of the FTP server, could be an IP or a url

PORT NUMBER: TCP Port open for the FTP communication

USERNAME & PASSWORD: Credentials of the FTP User implemented on the server.

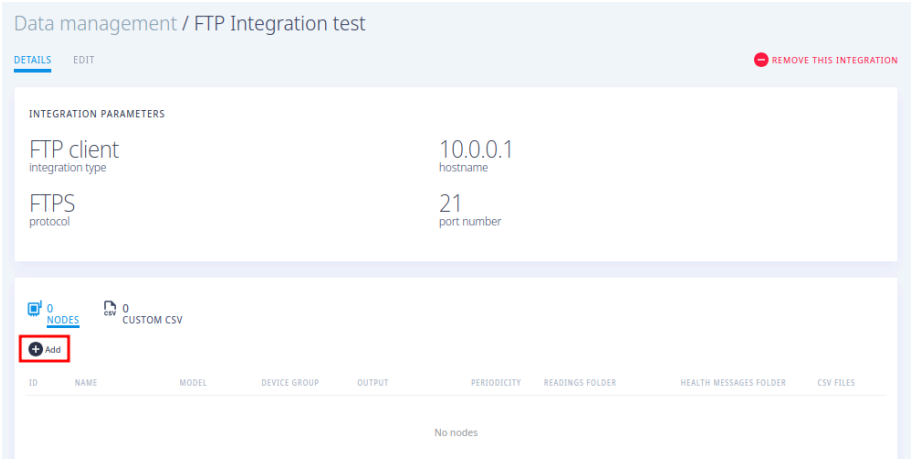
PROTOCOL: At this point both FTP or FTPS can be selected.

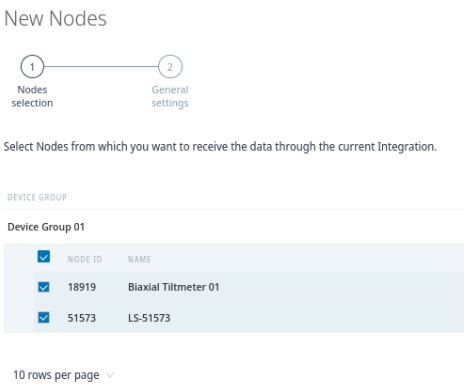
Click the NEXT STEP button to proceed with the final configuration.



Once the FTP Server connection settings have been configured, the next step will require indicating the Device groups associated with this integration. Several device Groups can be added to the integration by clicking + LINK ANOTHER DEVICE GROUP button.

At this point the integration is created, but not finished. Edge devices must be added to the integration, Selecting the appropriate path. Also, Custom CSV files can be added to the integration (explained in the section below), This is done by clicking + ADD button.

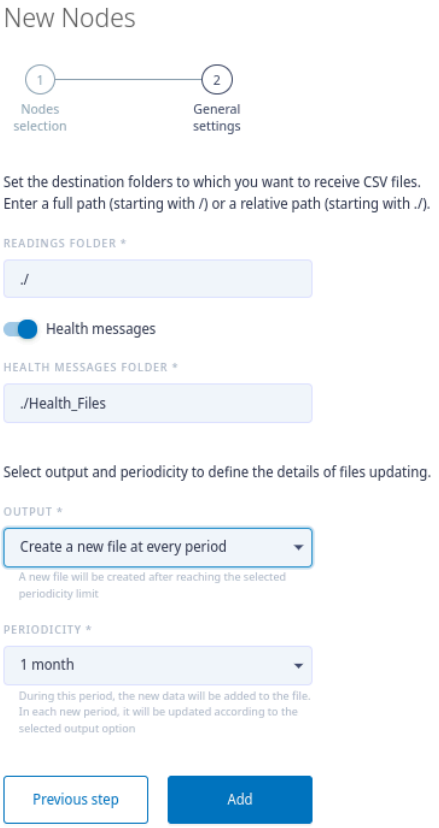




At this stage, the sensors of the previously selected device groups can be selected.

Clicking the first check box named NODE ID, all devices are selected.

Click Next to set the paths.



At this step, the paths at the FTP Server to store data, as well as data push methods are implemented.

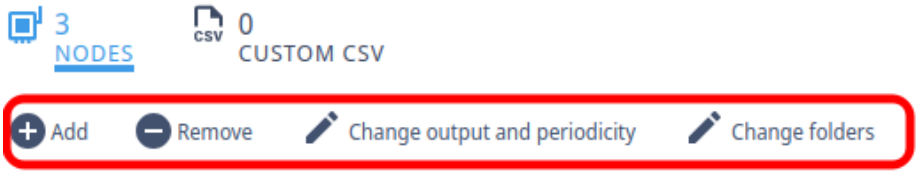
All the files will be redirected to a unique FTP folder, unless health files, that can be uploaded if selected, and added to a different subfolder in the server.

OUTPUT: This indicates the method to upload data, and there are currently two methods available: “Create a new file at every period” and “Overwrite the file at every period”, which will maintain the file name but delete the existing data after the period.

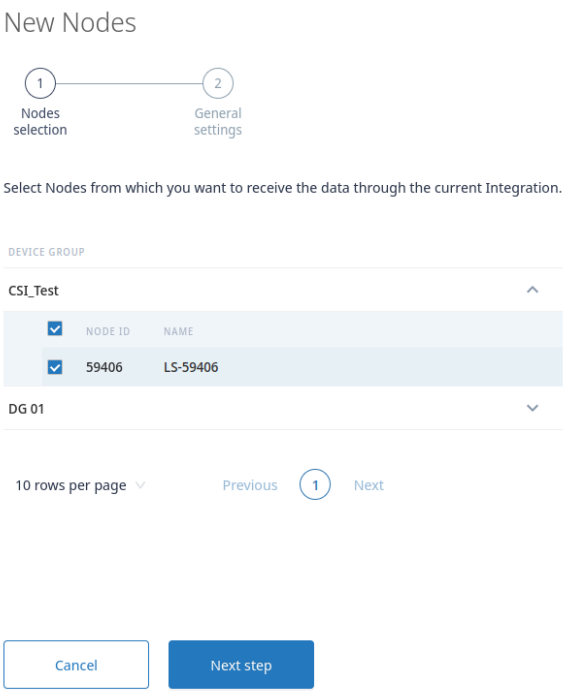
PERIODICITY: Refers to the period of time a file will be maintained. Options available: 1 Hour, 1 Day, 1 Month.

NOTE: The example on the left will create a new monthly file with all readings per each edge device, and another one for the health information, simulating the “Append at the end of file” implemented at CMT Cloud V1 and CMT Edge solutions.

Once the devices are added to the FTP integration list, some modifications can be carried out at any moment. Just selecting them permits different modifications.



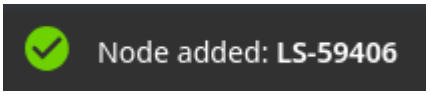
These features are available by selecting the device or group of edge devices listed in the integration and following the setup once selected the modification to be done.

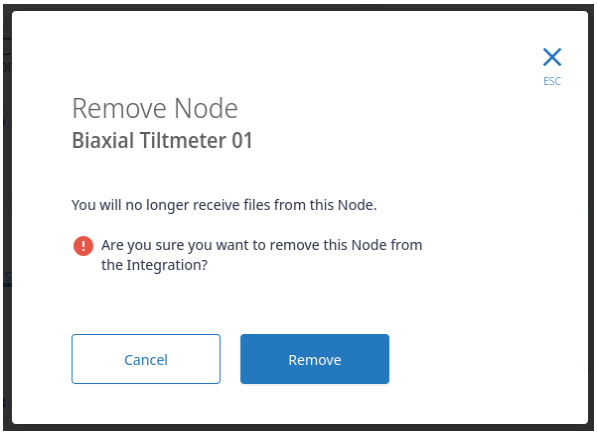


Add a new edge device to the FTP integration.

This feature is the same displayed in the previous steps, by clicking the Add button.

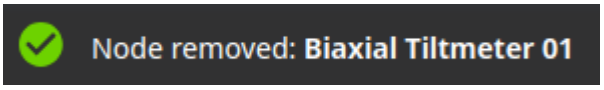
The device must be previously added to one of the Device groups listed in the integration.

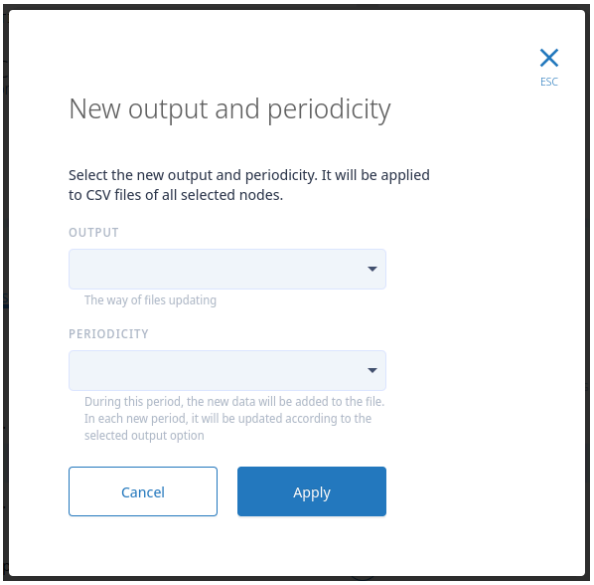




Remove edge devices from the FTP integration.

Ege devices can be bulk deleted (including all the previously selected ones to modify the configuration)

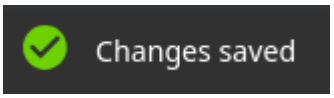


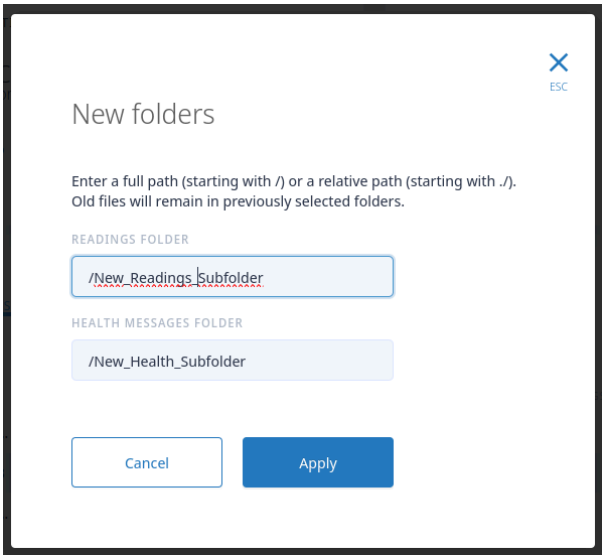


Change the Output and periodicity for a given edge device.

Both Output and Periodicity parameters may be different for a specific or group of edge devices in the same integration.

This feature allows using different methods of upload on the same FTP server. As an example, some files could be used for backup purposes while other devices files may be optimized for feeding a monitoring platform database.

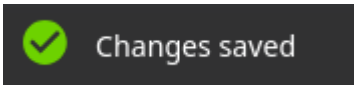




Modify the path for Readings and Health messages files in the FTP server

The path for both Readings and health files can be configured independently for each edge device.

NOTE: The subfolder must be previously created on the FTP server, and the appropriate permissions must be given in order to receive readings as expected.



MQTT Integration configuration

In case MQTT integration has been selected on the step 1, Only the device group configuration will be required. Unlike previous CMT Cloud versions, in this case the MQTT integration feature already implements a MQTT broker which receives all data received from the CMT Cloud account, and data can be shared with the third party software.

This way, the integration can be carried out directly from the third party software against Cloud platform, using the indicated parameters. The integration is done much more easily as there is no need to deploy and maintain an MQTT broker. A specific port is used: TCP 8423, networking rules may be needed on the software side.

Only a unique Device group can be selected per integration. This limitation may require creating different integrations for different Device Groups to cover the whole project, in case this one is divided into different groups.

Also, once a Device group has been used for a MQTT integration, this one can not be used again for a new MQTT integration. This does not affect the FTP implementation.

Configuration note: Client **keepalive** must be configured **< 30s**.

CMT Cloud V1 Compatibility also allows using this integration method, based on device groups.

Using the same structure, CMT Cloud account creates a MQTT broker sending all messages to it, allowing third party MQTT clients subscribing to the topic for data reception.

In this case, due to the different internal structure, the topic shared by the integration configuration has to be preceded by "**v1push/**". This will ensure a correct link.

By default, a unique CMT Cloud V1 MQTT integration will be permitted, which will integrate messages of all devices of the platform. In case of requiring different MQTT integrations for different device groups, V1 compatibility per device groups should be requested, instead of default general V1 compatibility. This would allow sending different edge devices readings listed in separate device groups, to different topics, which would allow different projects monitoring separately.

All the other configurations remain the same as the default configuration.

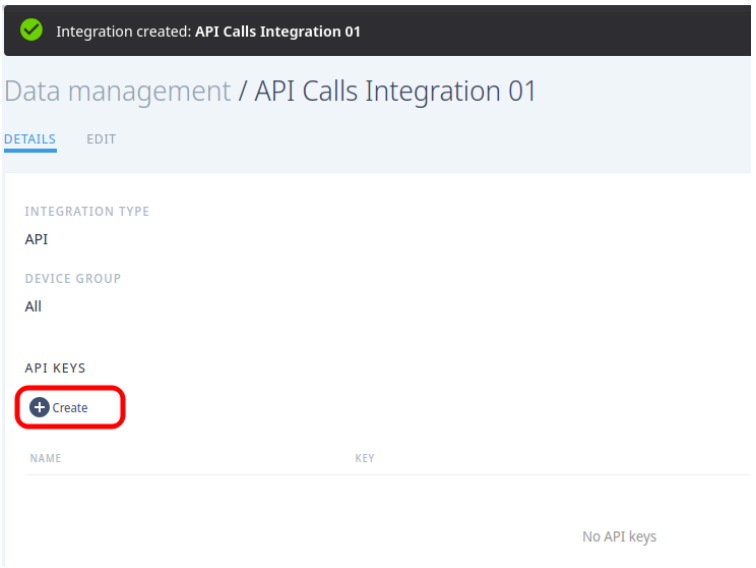
API Calls Integration configuration

API Calls can be used to integrate CMT Cloud with other softwares. This requires enabling this integration method, which provides a key that enables the communication between both systems.

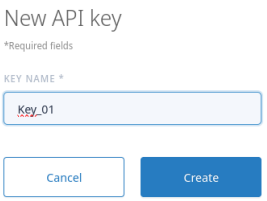
This integration method is available for Compatibility with V1 tenants or devices groups, using the CMT Edge or Cloud V1 JSON format.

Once a new integration has been created, selecting API integration type, a new integration is created.

At this point a new API Key must be created, by selecting the Create button.

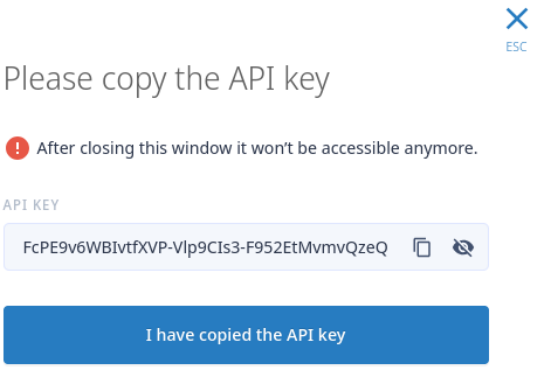


This button will require a name for the key, which will generate a key to be used for the deployment.



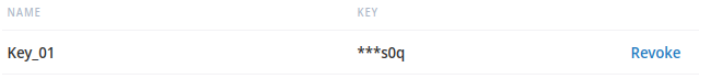
The platform will be blocked with a pop-up message that requires copying the key before continuing.

NOTE: This key will not be accessible anymore. We recommend copying and saving it to have it available when required.



This key is generated in the system, and can be revoked when needed, by clicking the Revoke button.

As many keys as required may be implemented in the system.

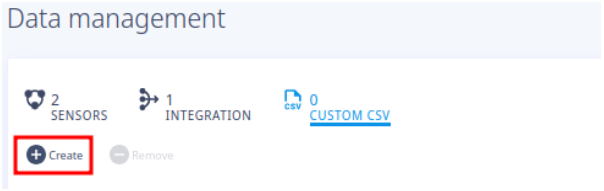


The detail of the available APIs, as well as the detail of the messaging (in JSON format) are available at Worldsensing knowledge base.

NOTE: API Calls are only available in V1 format by using CMT Cloud V1 Compatibility mode.

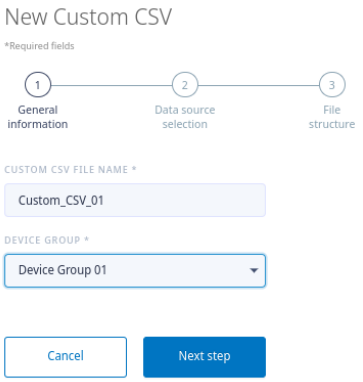
Custom CSV

CMT Cloud implements the custom CSV files management. The solution allows creating as much Custom CSV as required with a maximum of 50 columns each. Each column may represent any of the values of any of the sensors from the edge devices linked to a Device Group. This includes both raw data and Engineering units.



This feature is implemented in the Data Management section.

Selecting the CUSTOM CSV option and clicking the + Create button displays a configuration wizard to create a new custom CSV file.



The first step will ask to set a name for the file and associate a Device Group to the new Custom CSV file.

A unique Device Group can be added from the dropdown menu to each specific Custom CSV file.

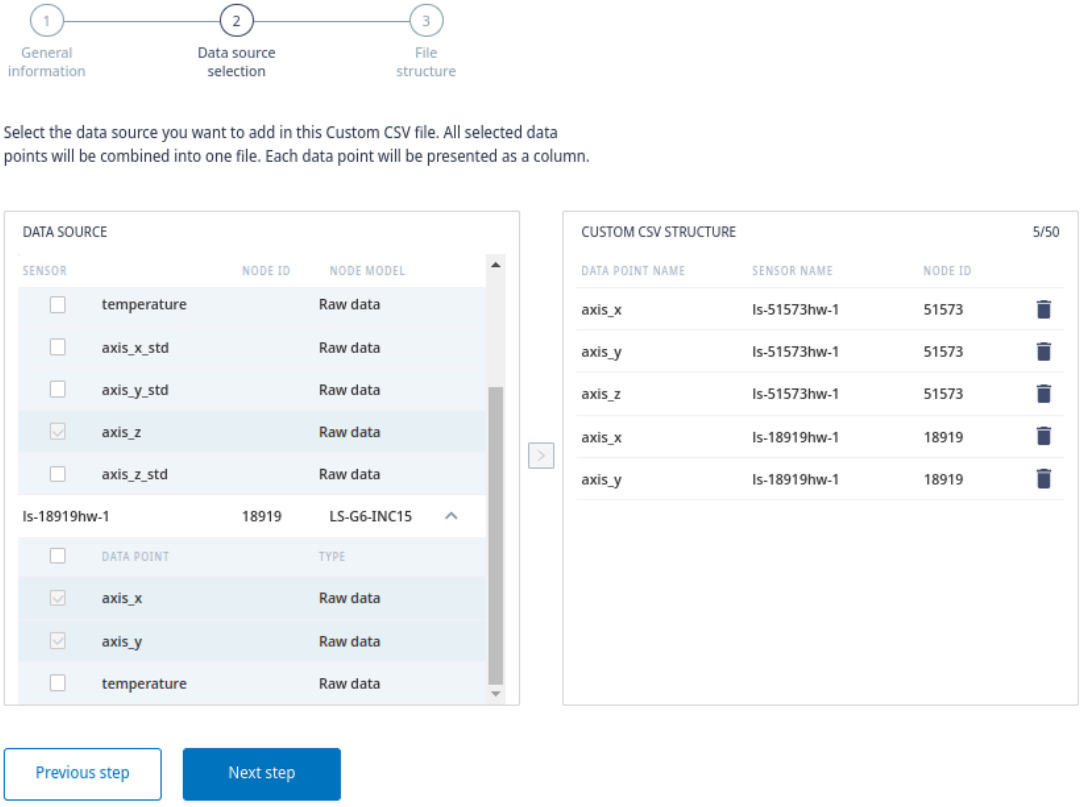
Click Next to follow to the next step.

The next step displays two columns.

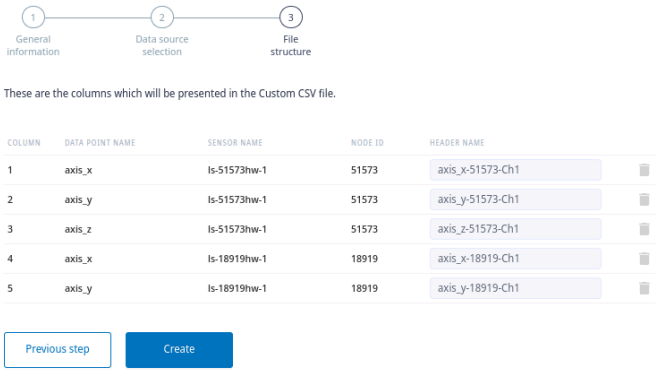
The first one contains all sensors (not edge devices) of the device group. Selecting each one of them displays a tree with all the registered readings (Raw data and engineering units) of that specific sensor.

These elements can be added to the second column, adding it to the Custom CSV file structure.

Click next once the Custom CSV columns have been added.



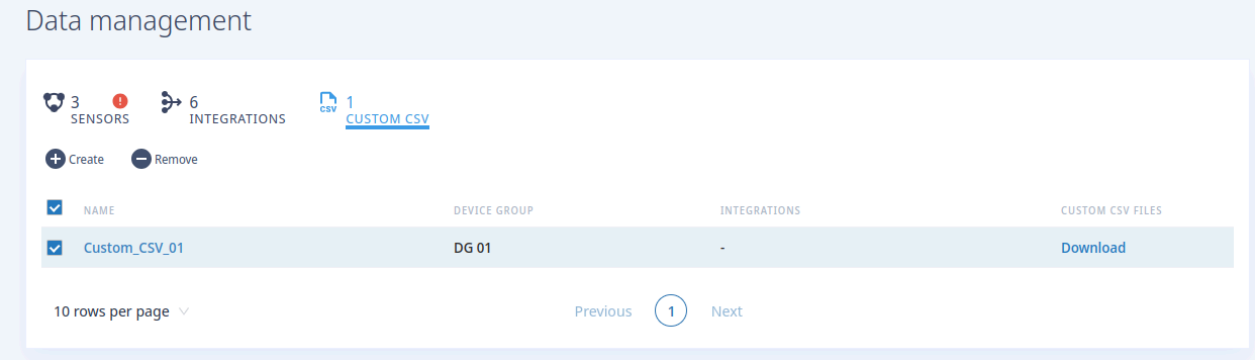
The last step displays the list of elements that will feed the Custom CSV columns.



These CSV files can be used for manual download, and also implemented in the FTP integrations.

Once the create button is clicked, the new Custom CSV File will be created. It is displayed in the Custom CSV main menu, and several operations can be performed:

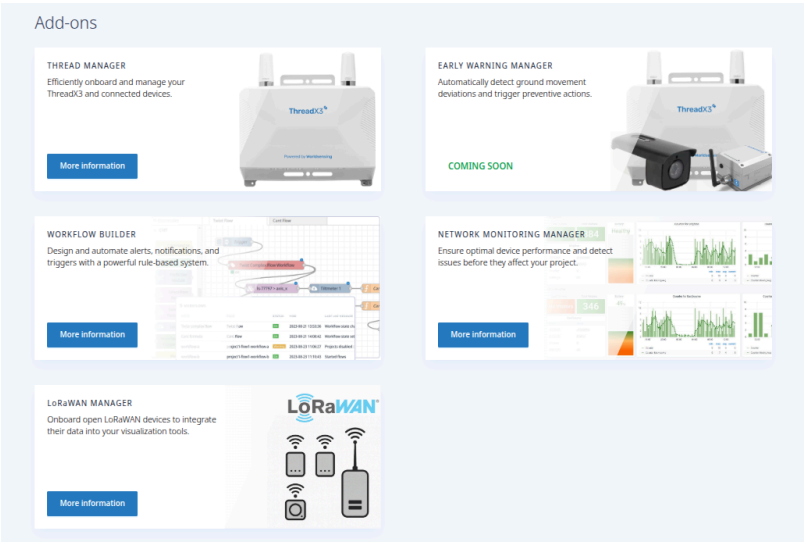
- Create a new Custom CSV by clicking on the Create button
- Delete one or several Custom files, by selecting them and clicking on the Remove button
- Download a selected Custom CSV File by clicking on the Download option. This option asks for a specific time period to generate the Custom CSV file with the timestamps available during that period of time.



ADD-ONS

Add-Ons is a new module that enhances the Loadsensing CMT Cloud system adding more features to the system. They need to be requested and enabled on demand, but the available ones, as well as the new ones coming soon can be checked by clicking on the Add-Ons icon in the top right corner.

Actually, these are the available ones:



WorkFlow builder: Design automatic alerts and notifications, triggers etc… using visual programming.

Thread manager: Allows connecting and managing Thread X3, and monitoring the connected devices.

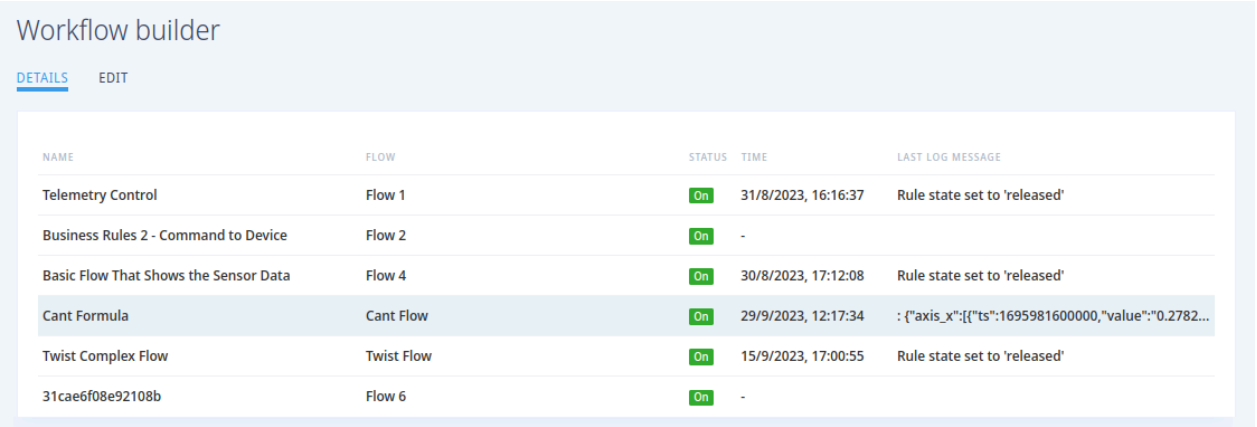
Network Monitoring: Loadsensing LoRaWAN network monitoring for network optimization.

LoRaWAN Manager: Onboarding of LoRaWAN sensors (third party sensors)

Workflow Builder

The Workflow Builder tool is a feature that provides the ability to perform actions based on identification of specific conditions previously defined by the user automatically. This allows not requiring a third party software integration for a wide range of actions.

As an example, it could calculate the cant in rail track geometry monitoring using the measurement of the angle of two different devices, and send an early warning alert, set thresholds on specific instruments and trigger an **email** notification when reached, etc…



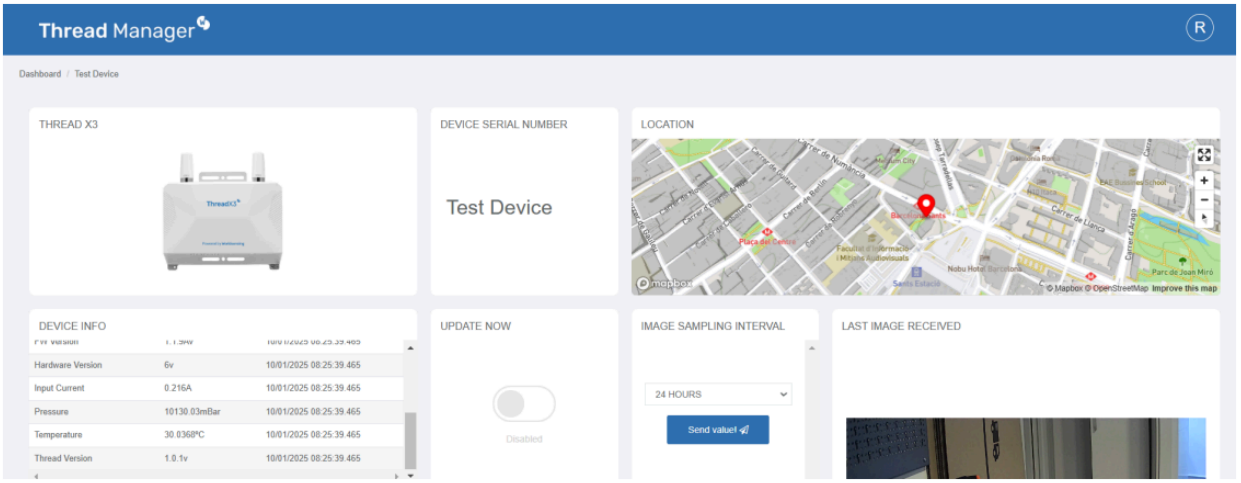
A specific user guide of this tool can be found on the Worldsensing Knowledge base.

Thread manager

Thread Manager is an affordable alternative for using Thread X3 devices, designed for customers who do not require the advanced visualization tools. Seamlessly integrated into CMT Cloud, ensuring a seamless user experience. It provides a streamlined solution with the flexibility to integrate and receive data from devices via MQTT or API integrations.

The initial release offers essential functionality, with enhancements planned for future updates. Currently, the platform supports three types of connected sensors:

- Field Camera.
- Campbell AVW200 interface with Geosense crackmeters.-
- Senix ToughSonic Ultrasonic Distance Sensor.
- Vaisala Weather station
- Relay



A Thread manager user guide is available in the Knowledge base.

Network Monitoring

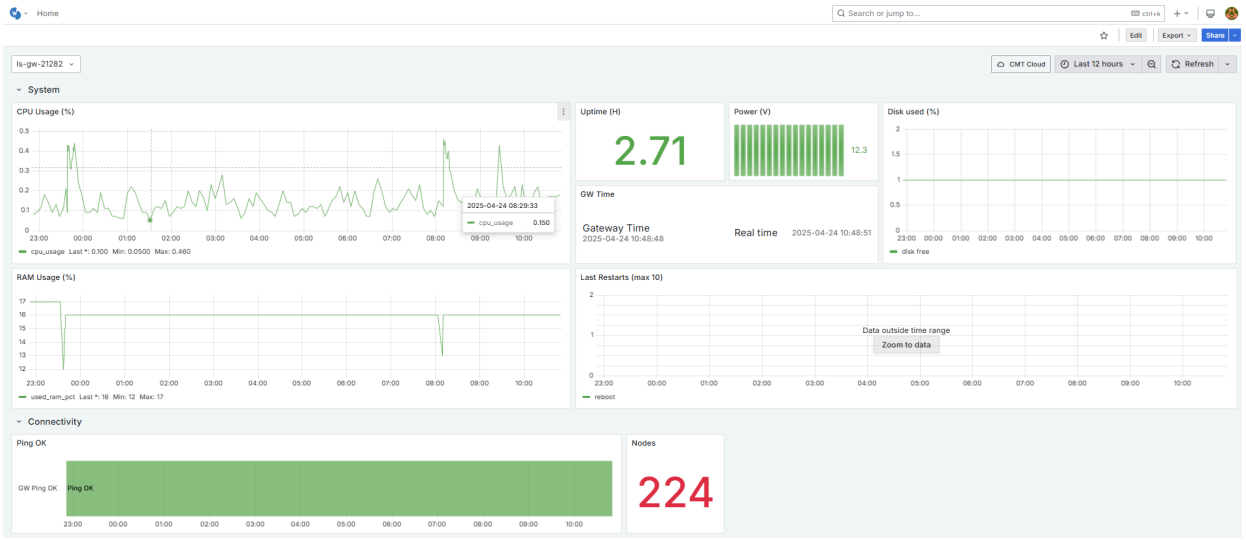
The Network Monitoring Manager is a CMT Cloud add-on designed to give operations and support teams deep visibility into the performance of the deployed LoRa and LoRaWAN gateways. This tool provides detailed diagnostics per gateway — helping users optimize wireless network reliability and performance by monitoring the hardware at the heart of every deployment.

It delivers clear dashboards with real-time and historical data, enabling proactive troubleshooting and efficient system maintenance. Some of the information it may provide:

1. Gateway Health Monitoring, such as CPU and RAM usage, Dis space, Uptime and gateway reboots, Power supply.

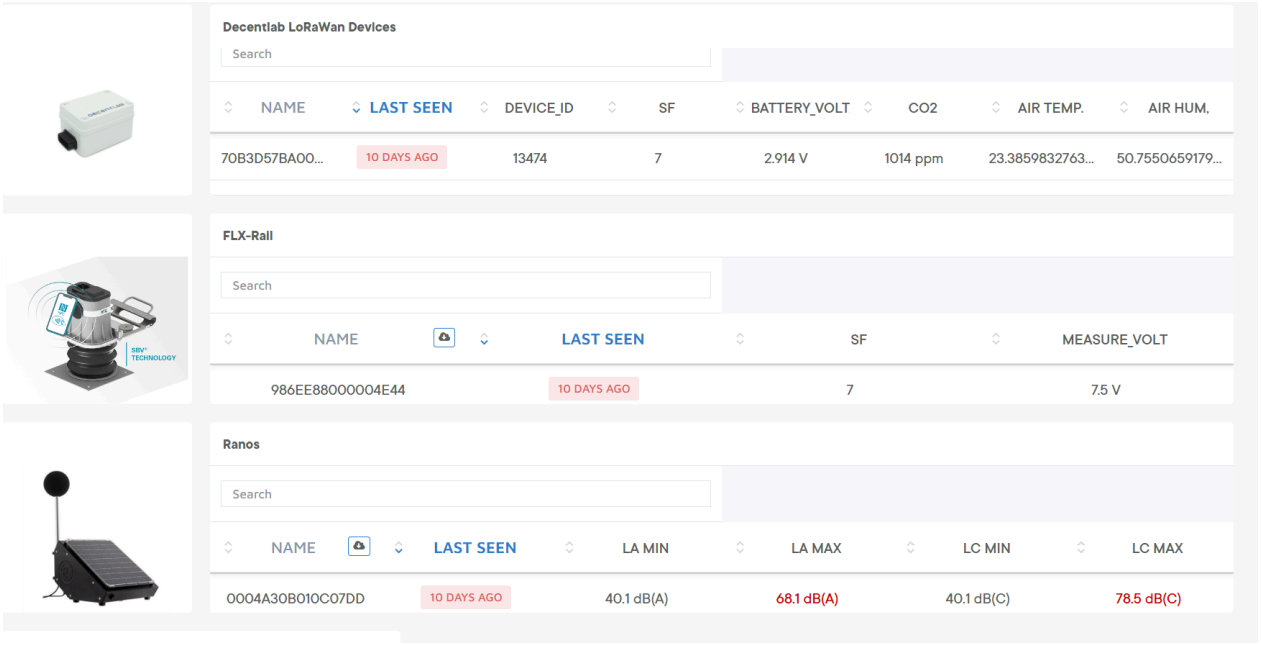
2. Gateway Connectivity (Ping, Number of connected nodes)

3. Gateway-Specific LoRa Communication Metrics (Spreading factor distribution, Radio packets per hour, RSSI, SNR, etc…)



LoRaWAN manager

The LoRaWAN Manager Add-On for CMT Cloud enables seamless integration, registration, and monitoring of third-party LoRaWAN devices within the Worldsensing ecosystem. This module extends CMT Cloud's native capabilities by allowing operators to incorporate a broader range of LoRaWAN sensors — including those not manufactured by Worldsensing — into their projects.



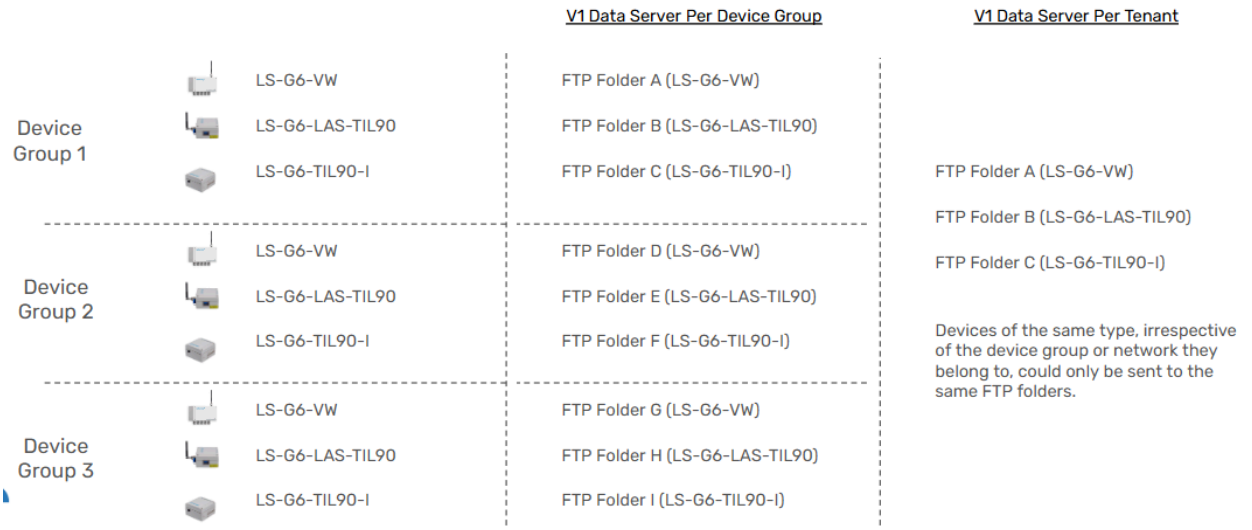
Appendix 1: CMT Cloud V1 Compatibility

The current Loadsensing CMT Cloud version is V2. This version has some differences compared to CMT Cloud V1 (deprecated) and CMT Edge in terms of CSV management. While Edge and V1 systems share the same Edge devices based CSV files format, the V2 platform is sensor oriented, which requires some differences between both CSV file formats.

For those already deployed networks, which require being migrated to CMT Cloud V2, with CSV based third party integrations (FTP Integrations mostly), the V2 integration would require modifying most of the CSV parameters (columns) on the monitoring platforms. V1 compatibility has been implemented to avoid these tasks, maintaining the same CSV structure.

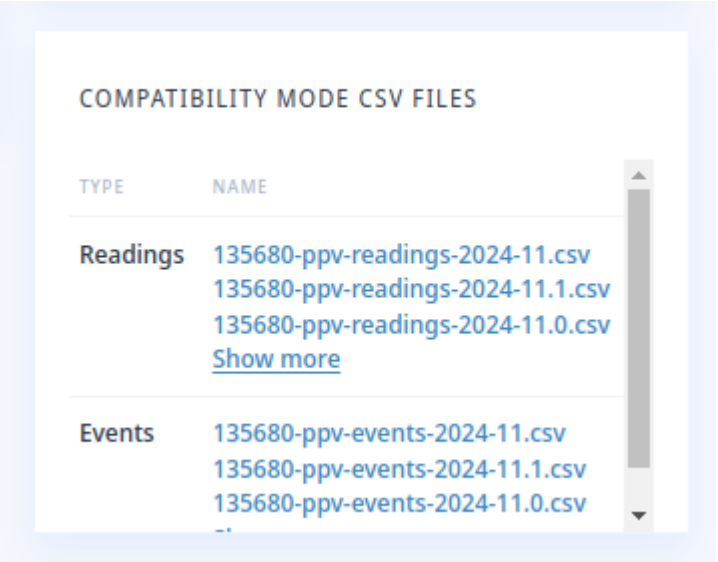
This feature implementation requires being requested prior to the account implementation, and will remain available for all the device groups deployed on the account.

This V1 compatibility may be implemented **for the tenant** (the whole account will work in compatibility mode **or by specific device groups**. In any case, a maximum of three device groups may be available in V1 on each account, and any additional device group will require a separate request to Worldsensing customer support team.



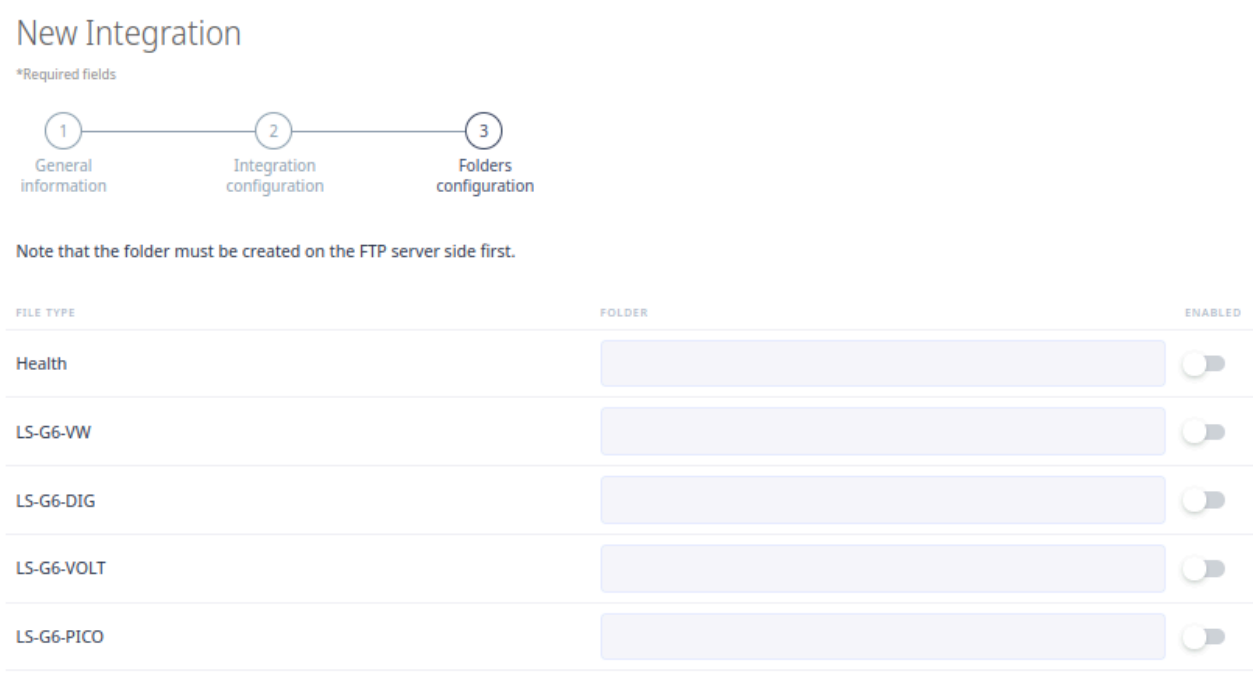
These V1 compatible accounts, in addition to the standard data storage on databases, also store the readings in monthly CSV files, keeping the same CSV file structure. These CSV files (all Health, Readings, Errors and node specific files such as Events) are available for direct download on the

COMPATIBILITY MODE CSV FILES widget at the DEVICES GROUPS/EDGE DEVICE page, the same way it is displayed at the older version.



This allows configuring FTP integrations based on the created device groups using the same CSV file structure, upload methods and paths, which makes it 100% compatible with the integration done with Edge and older versions of CMT (V1).

Same three FTP Upload methods (Append, create unique file and overwrite), as well as the same path structure is maintained.



The main difference remains on the amount of FTP Integrations available. A FTP integration may be created for each existing device group, which may connect to different FTP servers using different paths.

In the same way, in order to maintain the compatibility with Edge and V2 integrations, the same REST API calls have also been implemented. In this case data acquisition method will require generating and enabling an API Key on the platform, but keeps the same API call structure (Check REST API Calls chapter for more information)

Some other differences may be implemented for specific integration methods, such as MQTT. Please check the MQTT chapter for the specific information.

Appendix 2: Gateway - Network configuration scheme

GATEWAY MODEL	GATEWAY RADIO MODEL	NETWORK SERVER	CMT CLOUD NETWORK REGION	CMT CLOUD FREQUENCY PLAN	FREQUENCY GROUP
LS-G6-GW-868	Europe	eu1	Europe	Europe 863-868 Mhz	-
LS-G6-GW-915	FCC Group 0	nam1	North America	United States 902-928 MHz	Group 0
LS-G6-GW-923	923A	au1	Australia	Australia 915-928 MHZ	Group 0
LS-G6-GW-923	922S	au1	Australia	Asia 923 MHz	-

Appendix 3: Sensor and integrations table

This is the list of sensors and digital integrations available on CMT Cloud

EDGE DEVICE MODEL	INTEGRATION (if applies)
LS-G6-VW (Vibrating wire data logger)	-
LS-G6-VOLT4 (Analog data logger)	-
LS-G6-PICO (Pico Node data logger)	-
LS-G6-DIG2 (Digital data logger	DGSI Geoflex KELLER PR36 XV/XIV VAISALA WXT563 MEASURAND (max 200 segments) POSITION CONTROL PC-HSD4 V2 IN-SITU Level/BaroTROLL, AquaTROLL 200 YIELDPOINT d6EXTO & d15EXTO ENCARDIO EAN-56 OSPREY IPX-08 BAUER Load Cell MDT DIG4+, SmartLink MPBX GEOSINERGIA Modbus, Logger HI, Rebar-D SISGEO V3 RST / Geosense AQUALABO METER Teros 32 GEOKON IPI, Thermistor chain, Triaxial IPI MAXIMET
LS-G6-TIL90 (TILT90 series)	-
LS-G6-TIL90-X (Event Detection System)	-
LS-G6-LAS-TIL90 (Laser tiltmeter)	-
LSG7ACL-BILH (GEN 7 Vibrations Meter)	-
tiltmeter90XE (GEN7 til90 series)	-

Contact Worldsensing

Download the latest datasheets and infographics:

www.worldsensing.com

Contact our Customer Support team, and access the latest user guides, video tutorials and other documentation at our Knowledge Base:

https://worldsensing.com/support

Follow us online

WORLD SENSING

BARCELONA
Viriat 47, Edificio Numancia 1, 10th floor,
08014 Barcelona, Spain
(+34) 93 418 05 85
www.worldsensing.com
connect@worldsensing.com

London
Los Angeles
Singapore