Customer IT Requirements —
EcoSync Gen2 LoraWan GateWay
Quick Startup Guide

v 2.9.1

TLDR: **Set up unrestricted internet access (subnetwork or VLAN) **OR** set IPs, ports etc described below for the GateWay mac address on an ethernet cable. GW needs power unless you requested a POE device.**

Introduction

Smart heating controller IOT gateway (HUB) utilising the **LoRaWan** (**Lo**ng **Ra**nge low-power radio **W**ide **A**rea **N**etwork modulation technique)

The GateWay (GW) device EcoSync uses is a version of the MultiTech MTCAP2-L4E1-868-042A LoraWan gateway with significant Software (SW) modifications.

This gateway connects our IoT Valve Actuator devices using low energy long range radio communication to our cloud software stack.

The gateway contains custom configurations, settings and software for EcoSync services.
The gateway cannot be replaced with any other third-party gateway devices.

IMPORTANT: NEVER RESET THE GATEWAY! DO NOT PRESS THE RESET BUTTON!
If you press the reset button the gateway device will lose all the configurations and will not be able to communicate with our servers and the IOT valve actuator devices will not be able to communicate with it.
In case of accidental reset, please get in touch with us ASAP so we can ship you another fully configured gateway device.

How it works:

When the GW is powered on and has access to the internet it automatically does the following:

- creates a **secure VPN connection.** This VPN connection enables us to securely connect to the GW for monitoring and maintenance purposes.
- **connects to our cloud stack** platform automatically and will continue communicating with it continuously throughout its lifespan
- starts accepting communication requests from our IoT valve actuator devices via low-power radio communication (NOT WIFI!)
- start sending sensor data and other network data to and receive user settings from our cloud stack

ETHERNET & GSM enabled gateway devices

Requirements:

- ELECTRICITY THROUGH MAINS (adapter included) or POE[1]
- INTERNET ACCESS (UTP Ethernet cable included)

Note: In certain cases SIM only service is also possible.

The Ethernet enabled devices require an Ethernet INTERNET connection to our cloud based stack. The built-in security measures and firewall makes it impossible to access any data or functions on the device. The uniqueness of our SW solution also makes it a very unlikely target for misuse.

THIS DEVICE WILL NOT WORK ON A RESTRICTED IOT BMS NETWORK.
IT NEEDS INTERNET ACCESS.

PLEASE MAKE SURE THAT THE ETHERNET SOCKET YOU WILL USE FOR THE DEVICE IS ONLINE AND HAS INTERNET ACCESS.

[1]Not every gateway includes Power over Ethernet (PoE) capability. Please specify if you require this feature before installation. Availability of devices may vary based on current stock.

Internet access

There are three ways to set up internet access for our devices:

Version 1. physical subnetwork

If your switch allows, set up a physical **subnetwork** that has no routing to anything else on the network allowing Egress. This is safe because there is no ingress into the GW and there is no connection between the devices on the network and the GW.

Version 2. VLAN

If your switch does not allow a subnetwork, set up a **VLAN** with similar characteristics.

Version 3. Firewall settings

Set up connection to our services through restricting access only to the following devices on the internet:

ONLY ONE SETTING MISSING OR NOT BEING SET PROPERLY
WILL CAUSE OUR SERVICES TO FAIL[2]

Details for the Firewall:

- MAC address will be provided
- Port forwarding requirements: NONE
- Inbound/Ingress firewall settings: NONE
- Outbound/Egress filters to be set in the firewall:
    - Table gw_t1: Preferred firewall settings
    - Table gw_t2: Backup firewall settings if the firewall is not capable of handling domain names. This is not recommended because third party ip addresses might change any time.

[2] Wrong firewall settings will activate the failover secondary SIM (LTE/4G) connection

Name	Destination domain	Destination port	Protocol
clearblade_mqtt	europe-west1-mqtt.clearblade.com	443	TCP
vpn_tcp	vpn.ecosync.energy	443	TCP
vpn_udp	vpn.ecosync.energy	1194	UDP
google_dns1	8.8.8.8	53	UDP
google_dns2	8.8.4.4	53	UDP
room_mt_80	room.mt	80	TCP
room_mt_443	room.mt	443	TCP
time.google.com	time.google.com	123	UDP
time.facebook.com	time.facebook.com	123	UDP
time.apple.com	time.apple.com	123	UDP
time.windows.com	time.windows.com	123	UDP
ds.devicehq.com	ds.devicehq.com	5798	TCP

[gw_t1] Preferred OUTBOUND firewall settings for version 3)

Name	Destination IP	Destination port	Protocol
clearblade_mqtt	34.140.42.104	443	TCP
vpn1_tcp	35.195.174.0	443	TCP
vpn1_udp	35.195.174.0	1194	UDP
vpn2_tcp	35.228.208.188	443	TCP
vpn2_udp	35.228.208.188	1194	UDP
vpn3_tcp	34.77.55.211	443	TCP
vpn3_udp	34.77.55.211	1194	UDP
google_dns1	8.8.8.8	53	UDP
google_dns2	8.8.4.4	53	UDP
Ping ICMP	8.8.8.8	7	TCP/UDP
room_mt_80	87.229.69.179	80	TCP
room_mt_443	87.229.69.179	443	TCP
vpn_loadbalancer_tcp	104.199.21.122	443	TCP
vpn_loadbalancer_udp	104.199.21.122	1194	UDP
time.google.com_1	216.239.35.0	123	UDP
time.google.com_2	216.239.35.4	123	UDP
time.google.com_3	216.239.35.12	123	UDP
time.google.com_4	216.239.35.8	123	UDP
time.facebook.com	129.134.26.123	123	UDP
time.apple.com_1	17.253.52.253	123	UDP
time.apple.com_2	17.253.14.253	123	UDP
time.apple.com_3	40.119.148.38	123	UDP
time.windows.com	40.119.148.38	123	UDP
ds.devicehq.com	52.72.160.94	80	TCP
ds.devicehq.com	52.72.160.94	443	TCP

ds.devicehq.com	52.72.160.94	5798	TCP
ds.devicehq.com	52.72.160.94	5799	TCP
ds.devicehq.com	52.201.177.144	80	TCP
ds.devicehq.com	52.201.177.144	443	TCP
ds.devicehq.com	52.201.177.144	5798	TCP
ds.devicehq.com	52.201.177.144	5799	TCP
ds.devicehq.com	52.55.24.204	80	TCP
ds.devicehq.com	52.55.24.204	443	TCP
ds.devicehq.com	52.55.24.204	5798	TCP
ds.devicehq.com	52.55.24.204	5799	TCP

[gw_t1] OUTBOUND firewall settings for version without domains 3)[3]

[3] YELLOW: details updated in Feb. 2024
GREEN: details updated in Apr. 2024

PLEASE INFORM ECOSYNC ABOUT YOUR DECISION ON THE TYPE OF SETUP YOU CHOSE.

Changes may occur, we need to be able to adjust settings.

This SIM ONLY service can be utilised if one of the following conditions appear:

- There is **no ethernet socket** available in the building to provide **unrestricted internet access**
- The existing ethernet **internet access is unreliable** and loses connectivity from time to time

In the above situations the device will use the built-in sim card and GSM radio to communicate with our cloud stack. The data plan is usually data usage based which means that the **monthly costs** of using such a device **can vary** depending on the time the GSM functionality is used and the amount of data transmitted. The latter can be estimated from the number of EcoSync IOT devices connected to the GW. Please contact us for a quote or assistance.

These devices work **with the local ethernet** cable and can also work **without ethernet** using **ONLY THE GSM network**, which means no ethernet cable connection is required.

We offer the first 30 days of GSM service for free. After the first 30 days, we will be charging for the data use if no Ethernet connection is enabled. Using the GSM only option incurs **additional monthly costs.**

Monitoring, script and Firmware updates

The Gateway establishes an outbound **secure VPN connection.** This VPN connection enables us to securely connect to the GW for monitoring and maintenance purposes.

We utilise a aforementioned VPN connection to facilitate the seamless delivery of updates. In terms of monitoring and management, we have a dual approach. We leverage both the manufacturer's monitoring solution and our in-house system.

This same VPN is used to transfer sensitive information to the GW such as IoT sensor and actuator security keys.

Our primary service involves collecting gateway telemetry data from the devices every five minutes, which is then stored in a database. The gateways collect the telemetry data from multiple sources and send the data to a dedicated API endpoint on a dedicated VPS. This data serves as the foundation for our online HTML-based monitoring platform. Additionally, it empowered us to successfully implement automatic processes, such as reboots in case of malfunctions, as well as automatic notifications through SMS, email, and other channels when needed. One such use of the HTML platform is in the closing section of this document in the Quick start guide and can be reached by scanning the QR sticker on the GW itself.

Placement of the gateway

TLDR: **CENTRE OF THE MIDDLE FLOOR**

Place it in the centre of the middle floor of your building.

The gateway is a radio transmitter / receiver very much like a wifi routers, although using different radio frequencies, it is similar in a way that distance is the enemy of good signal.

Whenever possible, place the gateway in the middle of the building. In a multi floor building choose the middle floor and place the device in the centre of said middle floor.

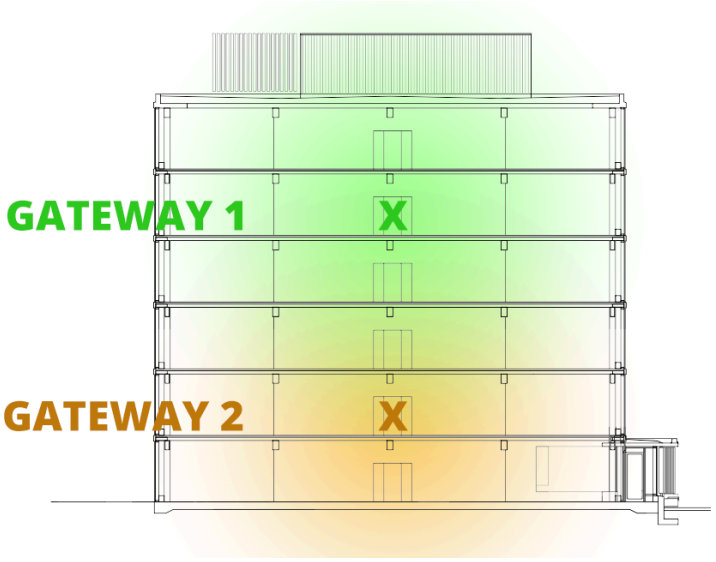
The gateway needs to be out of reach of occupants at all times. We suggest a dedicated power outlet that is out of reach and that will not be used for cleaning equipment or any other purposes. Each gateway come with a wall mount please make sure the device is securely fastened to the wall if need be and is out of reach. Do not place the gateway into a metal cabinet because such a Faraday cage may **hinder the signal.**

The gateway is typically capable of covering 2 floors up and 2 floors down and if placed in the centre of a floor it usually can reach the furthest rooms as well.

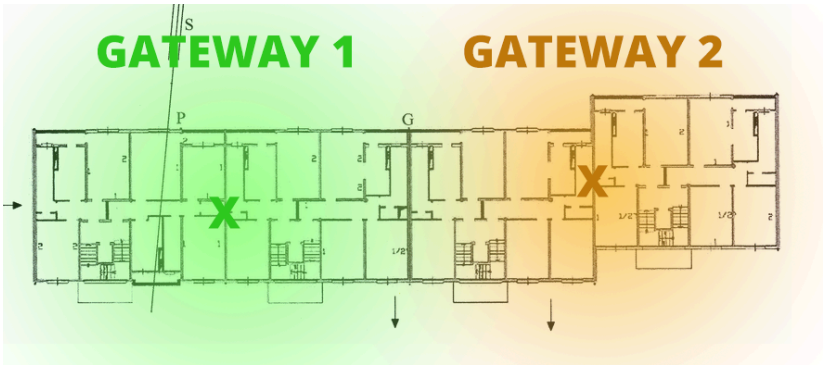
GATEWAY RANGE CHECK

In order to find the best location for your gateway TEST YOUR SIGNAL using one of our valve actuators! In buildings made of concrete or in buildings with multiple staircases, or more than 4 floors it might be necessary to use multiple gateways. The gateway location is not acceptable if there is at least one radiator with a wrong reading. In this case consider another location. If you find that you will need multiple gateways, try not using the two ends of the building. Eg. in a building with 6 floors instead of having one gateway on the ground floor and one on the top floor, place one on the first floor and the other on the fourth floor thus creating a more even signal coverage throughout the building. Same goes with horizontally aligned buildings.

Gateway location suggestions:



Suggested GW placement in a multi store building (Vertical segment of a building)



Suggested GW placement in a long building (Horizontal segment of a building)

Quick start guide

1. Connect the included antenna to the back of the device.
2. Connect the device using the cables included to the wall sockets for electricity and internet.
   The device will take a few minutes to boot up and connect to the internet.
   Note: **Do not place the device inside a metal cabinet because it may hinder the signal.**
3. To check if the device is indeed connected to the internet scan the QR code on the device.

Note: The gateway may take about 5 minutes to fully boot up.

Example QR:

mts1

SCAN QR
TO CHECK DEVICE
CONNECTVITY

OR TO READ MORE

The connectivity page shows the connection type (**CELLULAR / ETHERNET**), the last pint time and the device ID. Example: