

# **LoRaWAN Stack for VAS sensors**

- Overview of LoRaWAN Stack for VAS sensors -

Document version: 1.0

Last modified: 14/05/2024 15:50:00

# Contents

- Overview of the LoRaWAN Stack .....2**
  - 1. GNU/Linux server .....2
  - 2. LoRaWAN Gateway .....2
  - 3. LoRaWAN Network Server.....2
  - 4. IoT Platform .....3
  - 5. Reverse Proxy.....3
  - 6. Mandatory configuration and requirements .....3
- Configuration of the LoRaWAN Network Server (ChirpStack) .....4**
  - 1. Example of Docker installation on Debian 12 .....4
  - 2. Clone LoRaWAN Stack for VAS applications example repository and start it.....5
  - 3. Add LoRaWAN Gateway to the ChirpStack .....6
  - 4. Create certificates for the LoRaWAN gateway .....7
  - 5. Add VAS devices .....8
- Configuration of the LoRaWAN Gateway (RAK7289CV2 WisGate Edge Pro).....10**
  - 1. Initial configuration .....10
  - 2. Configure LoRa settings.....14
- References:.....16**

## Revision History

Version 0.1

Initial version: 25 April 2024

Version 1.0

Added Configuration and Usage Guide: 14 May 2024

# 1.

## Overview of the LoRaWAN Stack

A stack was implemented to connect the VAS sensors over the LoRaWAN network, collect data from these sensors, and visualise it. The main components of the stack are:

- GNU/Linux server (Debian);
- LoRaWAN Gateway (RAK7289CV2 WisGate Edge Pro);
- LoRaWAN Network Server (ChirpStack);
- IoT Platform (ThingsBoard);
- Reverse Proxy (Traefik).

### 1. GNU/Linux server

All software components are installed on a Debian GNU/Linux 12 (Bookworm) server.

The server is running with the following hardware configuration:

- 4 CPU cores;
- 8 GB RAM;
- 2 Hard disks (32 GB for system disk and 200 GB disk for data).
  - NOTE: 2<sup>nd</sup> HDD is optional, everything can be stored on one hard drive.

All ChirpStack components, ThingsBoard, and Traefik are installed on Docker, running in rootless mode using Docker Compose.

The following firewall ports are opened:

- 22 for SSH;
- 443 for HTTPS;
- 8883 for MQTT.

The following firewall ports can be opened for debugging:

- 8080 for ChirpStack Web GUI without TLS;
- 9090 for ThingsBoard Web GUI without TLS.

### 2. LoRaWAN Gateway

RAK7289CV2 WisGate Edge Pro is used as a LoRaWAN Gateway [1]. The following hardware configuration is employed:

- 8 Channels;
- No LTE;
- EU868 Frequency Region.

The gateway communicates with ChirpStack using an MQTT v3.1 Bridge with TLS encryption on port 8883.

### 3. LoRaWAN Network Server

ChirpStack v4 is used as the LoRaWAN Network Server [2]. All of its components (chirpstack, chirpstack-rest-api, postgres, redis, mosquitto) are installed on Docker, which is running in rootless mode using Docker Compose. Only the EU region is enabled for LoRaWAN communication.

The LoRaWAN device repository has been imported into ChirpStack.

An MQTT connection with TLS encryption is enabled on port 8883. Port 1883 for external connections without encryption is disabled, although it can be used internally within the mosquitto container for testing and debugging.

## 4. IoT Platform

The ThingsBoard Community Edition is installed as an IoT platform for data collection, processing, and visualisation [3]. An instance with a Cassandra database and Kafka queue service is used, as recommended by ThingsBoard developers for a production environment [4]. 8 GB of RAM is recommended for this setup.

## 5. Reverse Proxy

Out of the box, ChirpStack and ThingsBoard do not have HTTPS capabilities – they only support unencrypted connections to access their Web Dashboards. Therefore, Traefik is used as a reverse proxy to implement connections with TLS encryption [5].

Self-signed certificates are utilized, however, there is also the option to use Let's Encrypt certificates with valid domain names.

The following domains are used:

- ChirpStack Dashboard: <https://chirpstack.vas.internal/>
- ThingsBoard Dashboard: <https://thingsboard.vas.internal/>
- Traefik Dashboard: <https://traefik.vas.internal/>

The Traefik Dashboard is password-protected using the basicAuth middleware from Traefik.

## 6. Mandatory configuration and requirements

- The LoRaWAN Gateway and ChirpStack must be on the same network.
- Static IP addresses are required.
- The correct IP address of the ChirpStack must be set on the LoRaWAN Gateway.
- Domains used for the reverse proxy must be configured on the DNS server, which is not included in this setup.

# 2.

## Configuration of the LoRaWAN Network Server (ChirpStack)

Docker compose is used to run LoRaWAN Network Server (ChirpStack), therefore docker and docker compose should be installed on the system.

Installation instructions for various operating systems can be found at the following page:  
<https://docs.docker.com/engine/install/>

Installation example on Debian 12 using the apt repository is presented in chapter 2.1.  
Also, as mentioned in the Chapter 1, ports 22, 443, 8883, 8080, 9090 should be open.

### 1. Example of Docker installation on Debian 12

Uninstall old versions, if installed:

```
for pkg in docker.io docker-doc docker-compose podman-docker  
containerd runc; do apt-get remove $pkg; done
```

Update apt package index

```
apt update
```

Install packages to allow apt to use a repository over HTTPS:

```
apt install apt-transport-https ca-certificates curl gnupg lsb-  
release software-properties-common
```

Set up Docker's apt repository.

```
# Add Docker's official GPG key:  
apt update  
apt install ca-certificates curl  
install -m 0755 -d /etc/apt/keyrings  
curl -fsSL https://download.docker.com/linux/debian/gpg -o /etc/  
apt/keyrings/docker.asc  
chmod a+r /etc/apt/keyrings/docker.asc  
# Add the repository to Apt sources:  
echo \  
    "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/  
keyrings/docker.asc] https://download.docker.com/linux/debian \  
    $(. /etc/os-release && echo "$VERSION_CODENAME") stable" | \  
    tee /etc/apt/sources.list.d/docker.list > /dev/null  
apt update
```

Install latest version

```
apt install docker-ce docker-ce-cli containerd.io docker-buildx-  
plugin docker-compose-plugin
```

## LoRaWAN Stack for VAS sensors

Verify that the installation is successful by running the hello-world image:

```
docker run hello-world
```

Install the Compose plugin

```
sudo apt update
```

```
sudo apt install docker-compose-plugin
```

Install Compose standalone.

```
sudo curl -SL https://github.com/docker/compose/releases/download/v2.24.6/docker-compose-linux-x86_64 -o /usr/local/bin/docker-compose
```

```
sudo chmod +x /usr/local/bin/docker-compose
```

Note that Compose standalone uses the `-compose` syntax instead of the current standard syntax `compose`.

For example type `docker-compose up` when using Compose standalone, instead of `docker compose up`.

## 2. Clone LoRaWAN Stack for VAS applications example repository and start it

Configuration example of LoRaWAN Stack for VAS applications is provided in the following git repository:

<https://github.com/...>

Clone this repository

```
cd ~
```

```
git clone https://github.com/...
```

Start LoRaWAN Stack for VAS applications:

```
cd vas-lora-docker-dev
```

```
docker-compose up
```

OR:

```
docker-compose up -d
```

To stop LoRaWAN Stack for VAS applications:

```
cd vas-lora-docker-dev
```

```
docker-compose stop
```

OR:

```
docker-compose down
```

NOTE: last command will discard the containers and the networks they were utilizing

All services should be accessible:

- ChirpStack Dashboard: <https://chirpstack.vas.internal/>
  - OR: `http://<IP_OF_THE_SERVER>:8080`
- ThingsBoard Dashboard: <https://thingsboard.vas.internal/>
  - OR: `http://<IP_OF_THE_SERVER>:9090`
- Traefik Dashboard: <https://traefik.vas.internal/>

As mentioned in Chapter 1, **all used \*.vas.internal domain names should be resolvable to the IP address of the server**. System administrator must ensure that by editing settings of the used DNS server or host files or any other means.

Following default usernames and passwords are used:

- ChirpStack:
  - User: admin
  - Password: LoRaChirpStack2)@\$
- ThingsBoard:
  - System Administrator:
    - User: sysadmin@thingsboard.org
    - Password: sysadmin
  - Tenant Administrator:
    - User: tenant @thingsboard.org
    - Password: tenant
  - Customer User:
    - User: customer @thingsboard.org
    - Password: customer
- Traefik Dashboard:
  - User: vasuser
  - Password: LoRaChirpStack2)@\$

NOTE:

Docker automatically resolves addresses of the services defined in the docker-compose file. But sometimes it does not work e.g. chirpstack can't resolve postgres address. As a workaround these names can be added to the hosts file of the server. E.g.:

Edit hosts file

```
sudo nano /etc/hosts
```

Append to the hosts file:

```
127.0.0.1 chirpstack mosquitto postgres
```

### 3. Add LoRaWAN Gateway to the ChirpStack

Open Web GUI of the ChirpStack by loading following web page:

<https://chirpstack.vas.internal/>

OR:

http://<IP\_OF\_THE\_SERVER>:8080/

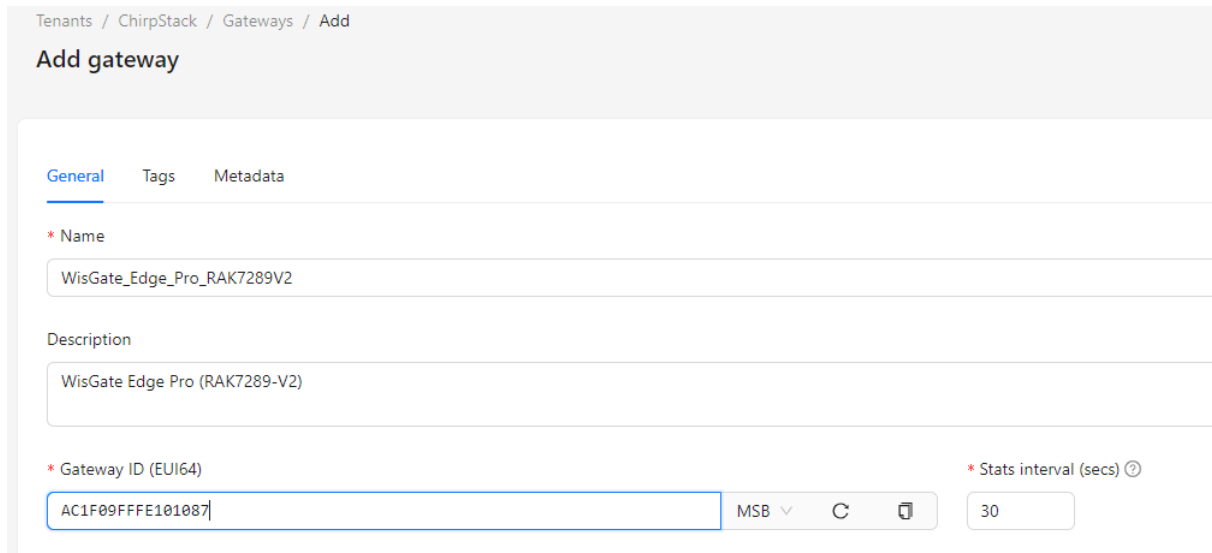
Navigate to: Tenant → Gateways

Press “Add gateway” button at the top right corner of the page.

Fill mandatory fields as shown in Figure 1:

- Name: can be any, e.g. WisGate\_Edge\_Pro\_RAK7289V2
- Description: can be any, e.g.: WisGate Edge Pro (RAK7289-V2)
- Gateway ID (EUI64): should match EUI of the used LoRaWAN gateway.
  - In the case of the RAK7289CV2 WisGate Edge Pro, it can be found in the Overview page of its Web GUI, as shown at the end of the Chapter 3.1.





The screenshot shows the 'Add gateway' form in the ChirpStack Web GUI. The breadcrumb navigation at the top is 'Tenants / ChirpStack / Gateways / Add'. The form has three tabs: 'General' (selected), 'Tags', and 'Metadata'. Under the 'General' tab, there are three fields: 'Name' with the value 'WisGate\_Edge\_Pro\_RAK7289V2', 'Description' with the value 'WisGate Edge Pro (RAK7289-V2)', and 'Gateway ID (EUI64)' with the value 'AC1F09FFFE101087'. To the right of the Gateway ID field is a 'Stats interval (secs)' field with the value '30'. There are also buttons for 'MSB', 'C', and a trash icon.

Figure 1. Add LoRaWAN Gateway

#### 4. Create certificates for the LoRaWAN gateway

Certificates are needed to allow MQTT connection with TLS encryption.

Open the Web GUI of the ChirpStack.

Navigate to: Tenant → Gateways → <GATEWAY\_ADDED\_IN\_PREVIOUS\_STEP> → TLS certificate

Press “Generate certificate”.

Following fields of the generated certificate should be shown (examples of these certificates are shown in Figure 2 and Figure 3):

- CA certificate
  - Copy everything, including “-----BEGIN CERTIFICATE-----” and “-----END CERTIFICATE-----” lines to the text file and save it as **ca.pem** file.
- TLS certificate
  - Save everything, including “-----BEGIN CERTIFICATE-----” and “-----END CERTIFICATE-----” lines to the text file and save it as **client\_cert.pem** file.
- TLS key
  - Save everything, including “-----BEGIN CERTIFICATE-----” and “-----END CERTIFICATE-----” lines to the text file and save it as **client\_key.pem** file.

These three certificate files will be needed while configuring LoRaWAN gateway in Chapter 3.2.

## LoRaWAN Stack for VAS sensors

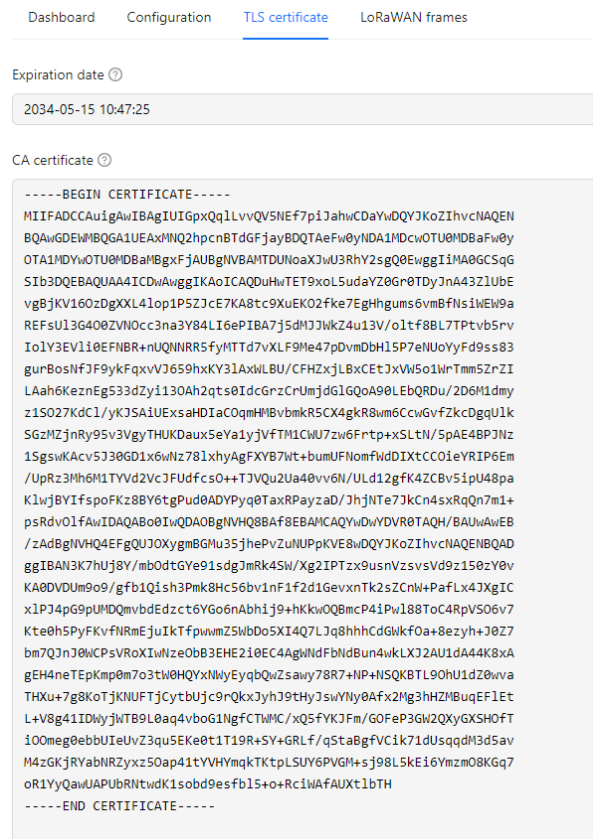


Figure 2. Example of the generated certificate for the gateway – CA certificate

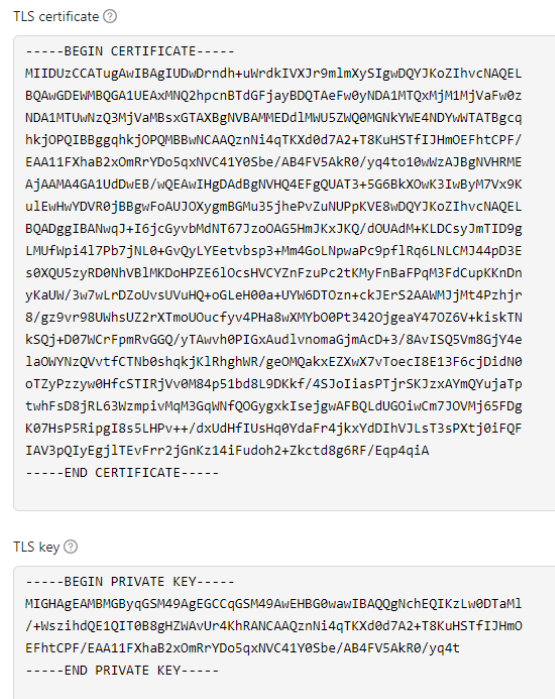


Figure 3. Example of the generated certificate for the gateway – TLS certificate and TLS key

## 5. Add VAS devices

## LoRaWAN Stack for VAS sensors

TBD...

# 3.

## Configuration of the LoRaWAN Gateway (RAK7289CV2 WisGate Edge Pro)

Manufacturer's quick start guide is available at:

<https://docs.rakwireless.com/Product-Categories/WisGate/RAK7289-V2/Quickstart/>

### 1. Initial configuration

Power on Gateway using included PoE Injector.

Wi-Fi AP Mode is used to make initial configuration of the gateway.

Connect to the gateway's default Wi-Fi network.

By default, gateway will create a Wi-Fi Network named RAK7289\_XXXX, where "XXXX" is the last two bytes of the Gateway MAC address.

Open any Web Browser and navigate to the following address: <https://192.168.230.1/>

Web GUI of the Gateway should open.

Set password for access to the gateway's Web GUI as shown in Figure 4.

- Default user is: root

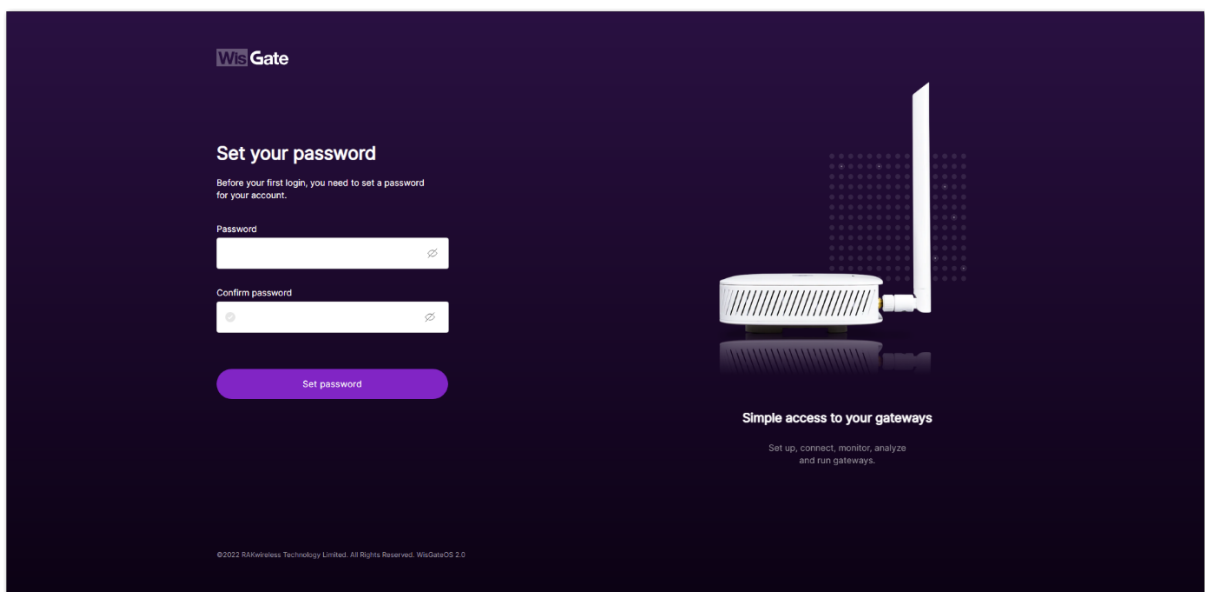


Figure 4. Set password on the RAK Gateway

After setting the password, the dashboard of the gateway should open.

If needed, you can click on the WisGate logo at the top left corner of the Web GUI, to show names of the menu entries, as shown in Figure 5.

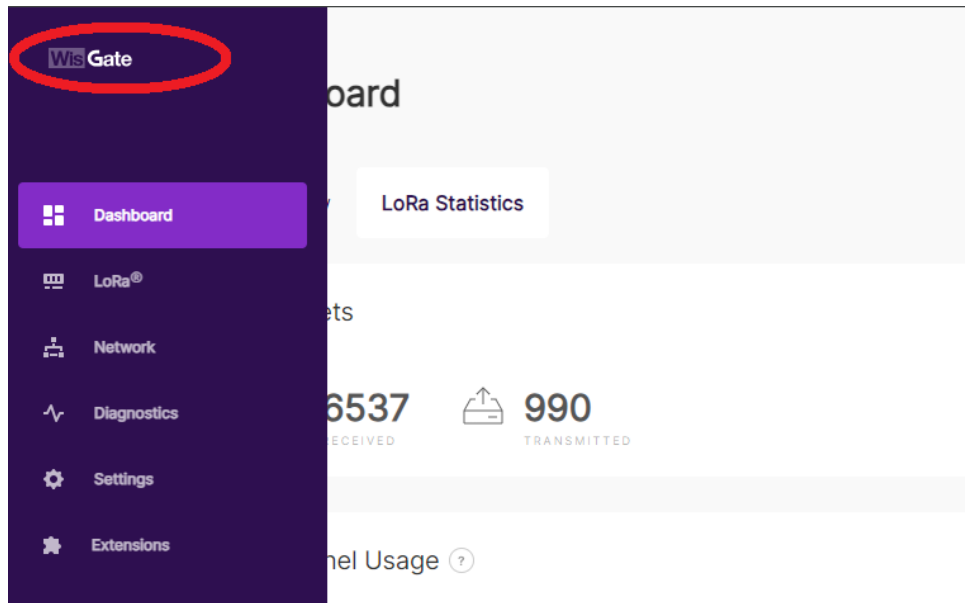


Figure 5. Press on WisGate logo, to show names of the menu entries

Set Wi-Fi password:

- Navigate to: Network → LAN (at the top of the network menu) → Expand (press arrow down) Wi-Fi entry → Settings
- Settings of the Wi-Fi interface should open, as shown in Figure 6. Change following settings:
  - Encryption: WPA2-PSK
  - Key: <YOUR\_PASSWORD>

Figure 6. Settings of the Wi-Fi interface

Set static IP on the LAN interface:

- Navigate to: Network → WAN (at the top of the network menu) → Expand (press arrow down) Ethernet entry → Settings
- Settings of the Ethernet interface should be opened as shown in Figure 7.
  - Enable WAN and disable LAN: enabled
  - Static address: selected
  - IPv4 address: <YOUR\_IP>
  - IPv4 netmask: <YOUR\_NETMASK>
  - IPv4 router: <YOUR\_DEFAULT\_GATEWAY>
  - DNS Server: <YOUR\_DNS\_SERVER>
    - NOTE: Don't forget to press Add button after entering DNS address.

Interface

Enable WAN and disable LAN

Protocol

Static address DHCP client PPPoE

IPv4 address

192.168.10.100

IPv4 netmask

255.255.255.0

IPv4 router

192.168.10.100

Use custom DNS servers

192.168.10.1 x

DNS Server

Add

Figure 7. Settings of the Ethernet interface

Update Firmware

- Navigate to: Settings → Firmware
- Check currently installed version of the firmware. In the example, shown in Figure 8, current version is 2.2.2. Also, the version of the firmware should be shown at the bottom of the Web GUI.

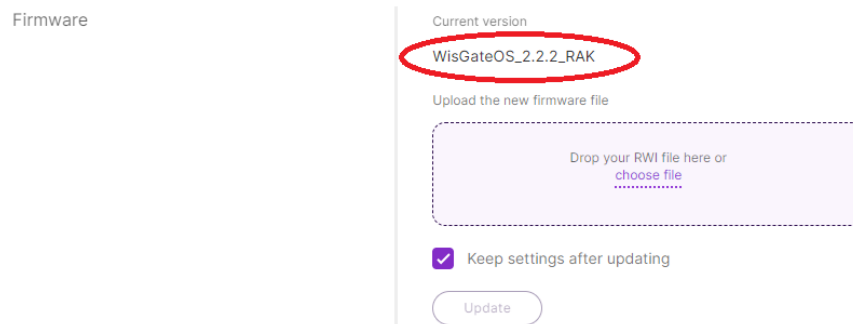


Figure 8. Current version of the firmware

- Check latest available firmware and release notes at the following web page: <https://downloads.rakwireless.com/#LoRa/WisGateOS2/>
- If newer firmware is available download and unzip it.
- Then navigate to the firmware page on the Web GUI (Settings → Firmware) and upload the new firmware file (.rwi), enable “Keep setting after updating” option and make an update.
- Wait for the update to finish.

Take a note of the Gateway’s EUI:

- EUI is needed to connect LoRaWAN gateway to the ChirpStack.
- Navigate to: Dashboard → Overview
- Various parameters of the gateway is shown, as can be seen in the example provided in Figure 9.

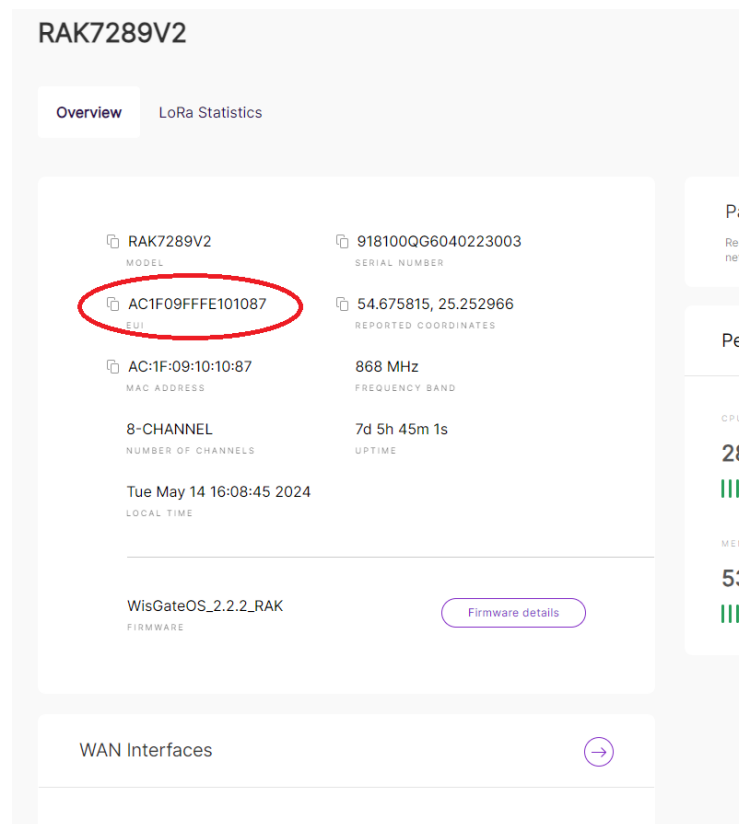


Figure 9. EUI of the Gateway in the Overview page

- As it is seen, in this example EUI is: AC1F09FFFE101087

## 2. Configure LoRa settings

Main LoRa settings are shown in Figure 10.

Open Web GUI of the Gateway.

Open LoRa settings

- Work mode: Packet forwarder
- Log Level: NOTICE
- Frequency Plan:
  - Country: Lithuania
  - Regio: EU868
- Protocol:
  - Protocol: LoRa Gateway MQTT Bridge
  - Statistic interval (s): 30
  - LoRa Gateway MQTT Bridge Parameters
    - MQTT Protocol: MQTT for ChirpStack 4.x (protobuf)
    - MQTT Broker Address: chirpstack.vas.internal
    - MQTT Broker Port: 8883
    - MQTT Version: 3.1.1
    - QoS: 1 - At Least Once
    - Keepalive interval (s): 10
    - Clean session: enabled
    - Retain: disabled
    - Enable User Authentication: disabled
    - SSL/TLS Mode: Self-signed server & client certification
    - TLS Version: TLS v1.2
    - CA certificate: upload **ca.pem** generated in Chapter 2.4
    - Client certificate: upload **client\_cert.pem** generated in Chapter 2.4
    - Client key: upload **client\_key.pem** generated in Chapter 2.4



LoRaWAN Stack for VAS sensors

Protocol

Choose from the available protocols.

Protocol

☐ Semtech UDP GWMP Protocol

☒ LoRa Gateway MQTT Bridge

Statistic interval (s)

30

LoRa Gateway MQTT Bridge Parameters

MQTT Protocol

MQTT for ChirpStack 4.x (Protobuf)

MQTT Broker Address

chirpstack.vas.internal

MQTT Broker Port

8883

MQTT Version

v3.1.1

QoS

1 - At Least Once

Keepalive interval (s)

10

☒ Clean session

☐ Retain

☐ Enable User Authentication

SSL/TLS Mode

Self-signed server & client certification

TLS Version

TLS v1.2

CA certificate

Upload a new certificate

Figure 10. Main Settings of the LoRaWAN gateway

## References:

- [1] RAK Wireless, “8 or 16 channel Outdoor LoRaWAN Gateway.” Accessed: Apr. 26, 2024. [Online]. Available: <https://store.rakwireless.com/products/rak7289-8-16-channel-outdoor-lorawan-gateway?variant=42334687789254>
- [2] ChirpStack, “ChirpStack, open-source LoRaWAN® Network Server.” Accessed: Apr. 26, 2024. [Online]. Available: <https://www.chirpstack.io/>
- [3] The ThingsBoard Authors, “ThingsBoard. Open-source IoT Platform.” Accessed: Apr. 26, 2024. [Online]. Available: <https://thingsboard.io/>
- [4] The ThingsBoard Authors, “Installing ThingsBoard using Docker (Linux or Mac OS).” Accessed: Apr. 26, 2024. [Online]. Available: <https://thingsboard.io/docs/user-guide/install/docker/>
- [5] Traefik Labs, “Traefik, The Cloud Native Application Proxy.” Accessed: Apr. 26, 2024. [Online]. Available: <https://traefik.io/traefik/>