WisGate OS 2 User Manual

Overview

This document describes in detail the functionality of the WisGateOS 2. The system builds on top of OpenWRT and runs on all RAK WisGate Edge V2 gateways. The guide presents general overview and provides guides and detailed configuration of the gateway. It functions as reference for several products with similar functionality. Thus, some sections will apply to certain products and not others.

Gateway Start-up

To power up the gateway, check the Quick Start guide of the respective device. There are two ways to access the gateway (**Wi-Fi AP Mode** and **WAN Port (Ethernet)**) explained in the corresponding document.

> 📝 **NOTE**
>
> Make sure all the antennas are connected before powering the Gateway.

Access the WisGateOS 2 Web UI

1. For security reasons, upon first login, the user must set a login password. This is done by filling in the desired password and confirming it in the provided fields.

The password needs to comply with the following rules:

- Should be at least 12 characters long;
- Has at least one special character (!“#$%&\‘()*+,-./:;<=>?@[]^_`{|}~);
- Has at least one number;
- Has at least one standard Latin letter (used in the English alphabet).

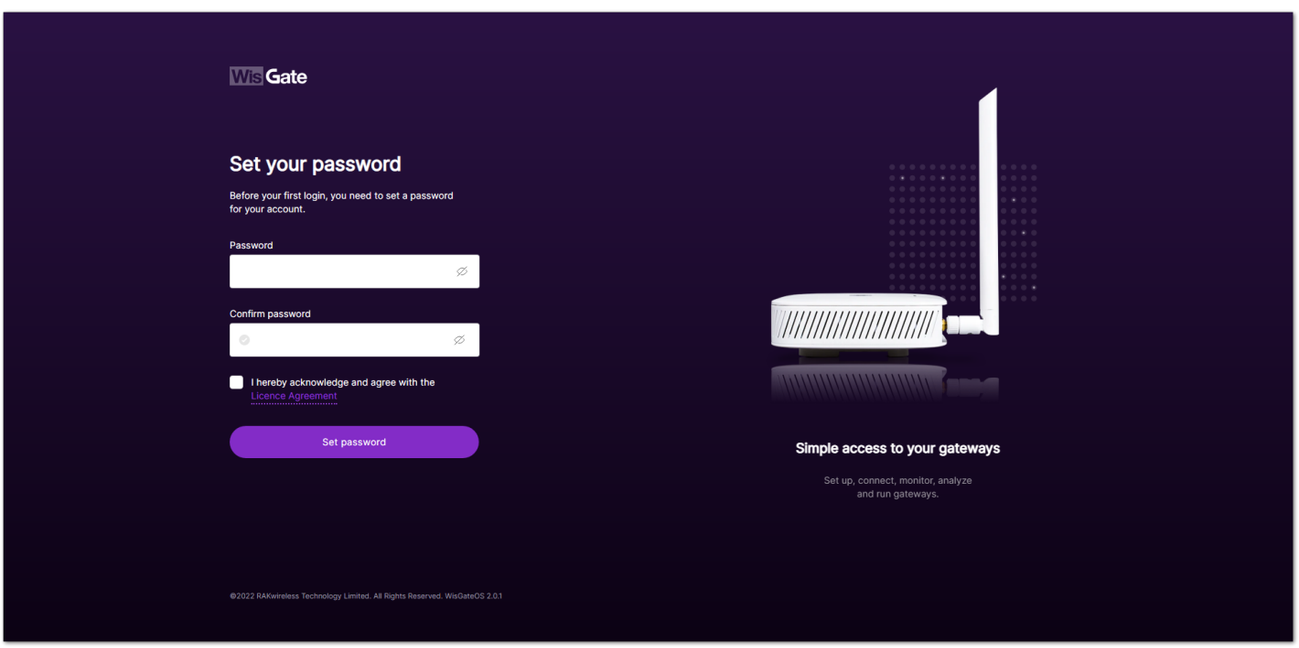

Figure 1: First login page

2. When the fields are filled in, click the **Set password** button to apply it. The Web UI is now accessible and it will load the **LoRaWAN Statistics** page (Figure 4).

3. On the next login, the user needs to use the set password for access. The default login username is **root**.

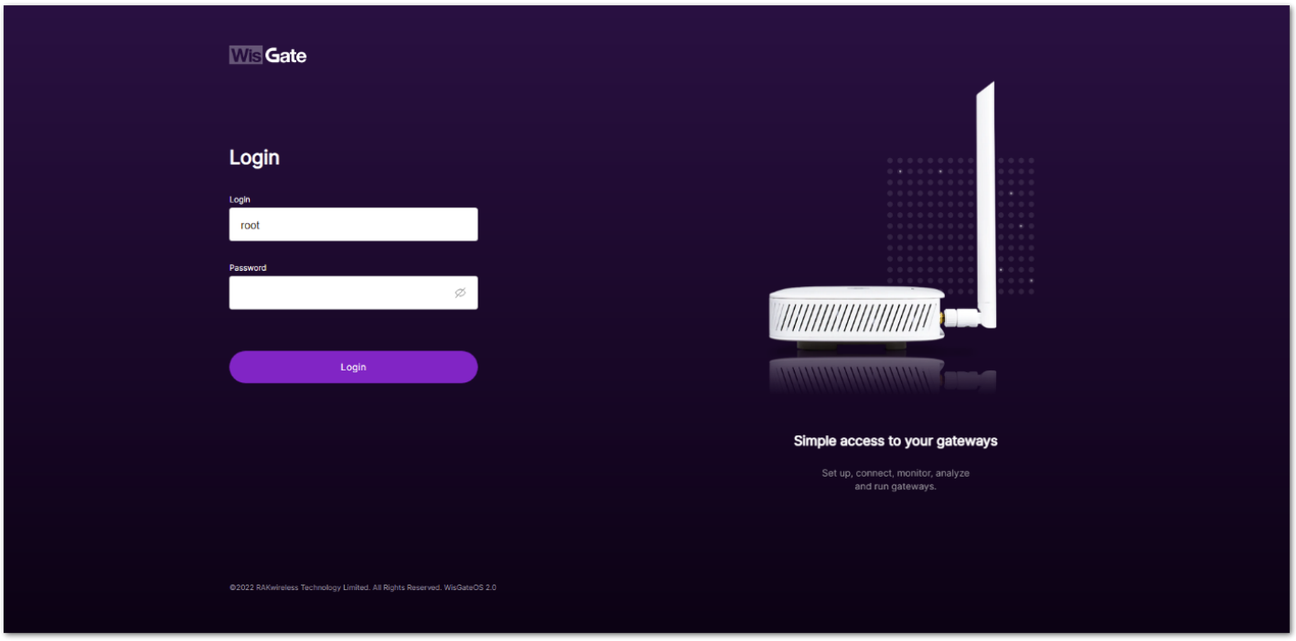

Figure 2: Login page

Web Management Platform

After the user have entered the correct credentials and logged in the gateway, they can start exploring the configuration and monitoring interface of the device starting with the **LoRaWAN Statistics** page that opens automatically.

> 📝 **NOTE**
>
> In WisGateOS 2, the menu names are hidden for esthetic reasons and only the icons are visible.

The user can click on the WisGate logo (WisGate) in the upper left corner to expand the menu on the left and see the full names of the tabs. When the user clicks anywhere else on the page, the menu folds again.

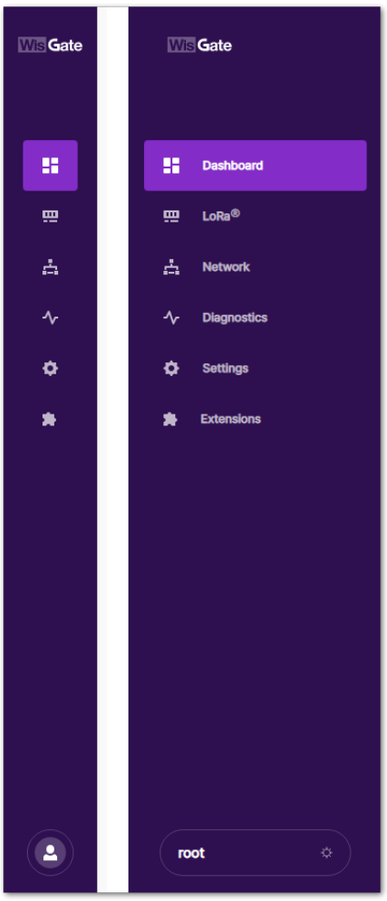

Figure 3: Folded and unfolded sidebar

Dashboard

This is where statistics about the gateway behavior can be monitored in real time.

LoRaWAN Statistics

The page consists of several blocks where the user can see the overview of some metrics and basic information about the traffic of messages.

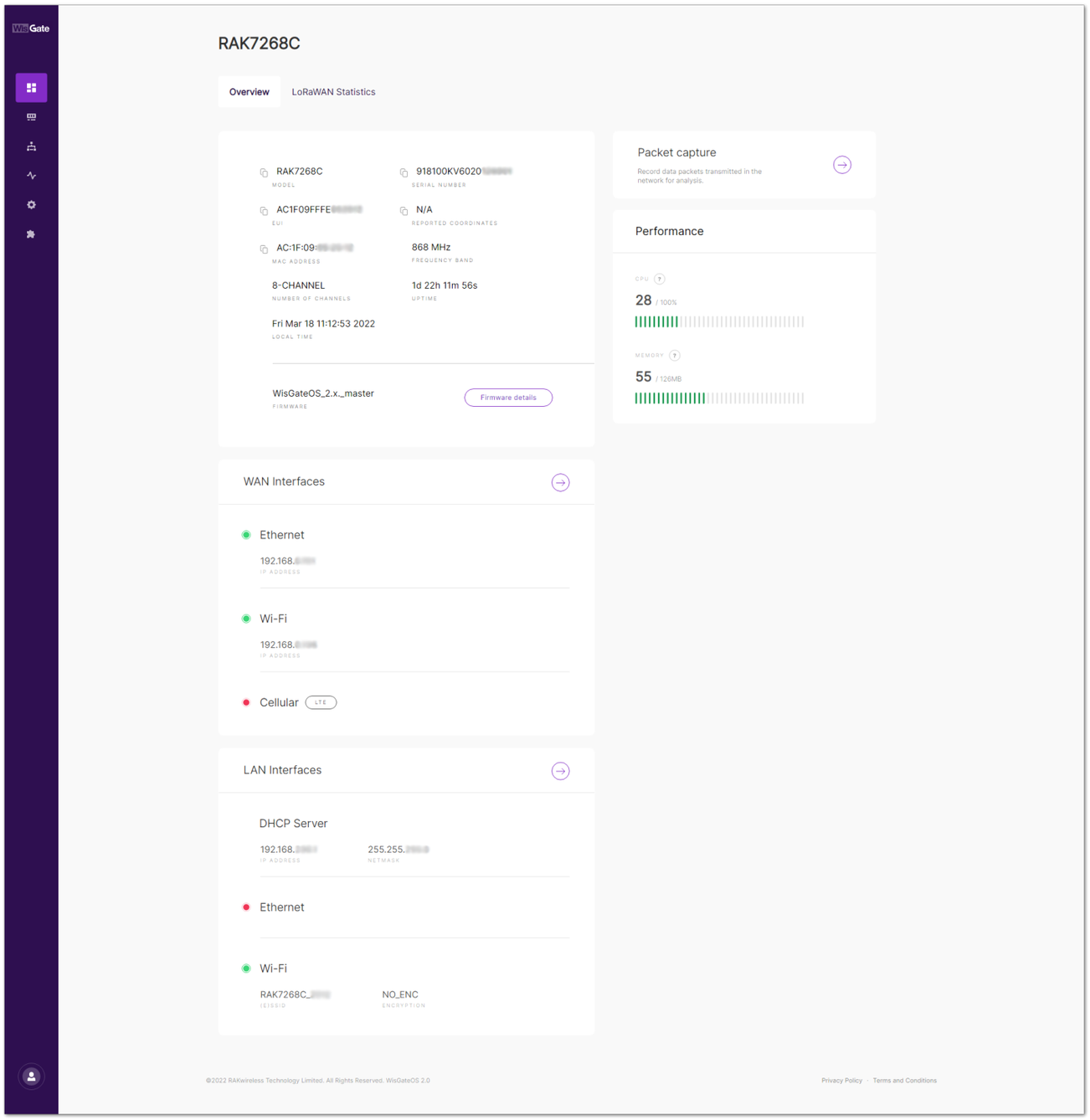

Figure 4: LoRaWAN Statistics tab

- **Packets** - Shows the total number of received and transmitted packets by the gateway (uplinks and downlinks). Here are displayed not only messages from devices connected to the gateway directly but from any device that is within the coverage of the gateway and transmitting LoRa messages.
- **End devices** - Shows the number of end devices within the gateway's coverage that sent data:
  - **Active** - The number of the end devices that have sent data in the past hour.
  - **Busy** – The number of the end devices that have sent an average of 1 uplink packet every minute in the past 10 minutes.
- **Channel Usage** - Shows the frequency channel load. The green color indicates low load and the red color indicates high load. The user can use the **Timespan** drop-down menu and **Range** scale to set timespan and range for the channel usage to be shown in the graph.
- **SNR & RSSI** - These graphs show the total number of packets with RSSI/SNR value within a specific range. This is also shown in a pie chart to the side of the graphs.
- **Uplink Traffic** - Shows the packet per minute rate as a function of time and airtime (sec) per minute. Above the graphs, the user can see the color-coding of the different Data Rates, where the actual height of the values is a sum of all the packets overall data rates for the time sample. The user can set a time span to be shown for the uplink traffic via the **Timespan** drop-down menu.
- **Downlink Traffic** - Shows the packet per minute rate as a function of time and airtime (sec) per minute. Above the graphs, the user can see the color-coding of the different Data Rates, where the actual height of the values

is a sum of all the packets overall data rates for the time sample. The user can set a different time span to be shown for the downlink traffic via the **Timespan** drop-down menu.

Overview

The page consists of several blocks where the user can see information about the gateway model, firmware, WAN and LAN interfaces. In addition, the user can monitor the performance of the gateway or its packet traffic.

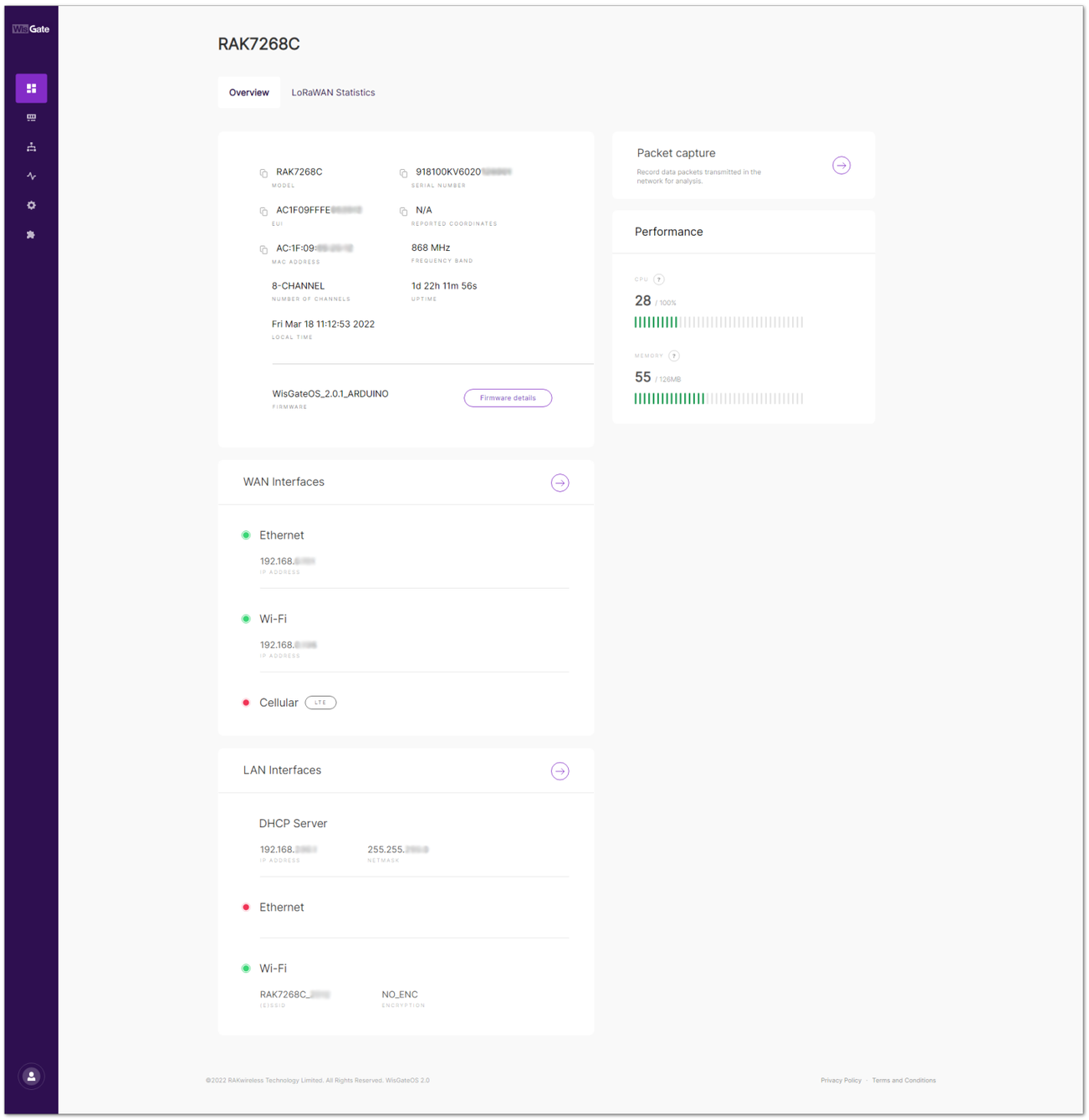

Figure 5: Overview tab

- In the first block, the user can see the general information about the gateway:
  - **Model** – The model of the gateway.
  - **Serial number** – The serial number of the gateway.
  - **EUI** - The Extended Unique Identifier of the gateway. It is used to register the gateway in LoRaWAN Network servers.
  - **Coordinates** – Coordinates of the gateway.
  - **MAC address** - The Media Access Control address of the gateway.
  - **Frequency band** – The frequency band set on the gateway.
  - **Number of channels** – The number of the channels of the gateway (8-channel/16-channel).
  - **Uptime –** The time the gateway has been working for.

- **Local time**- The local time set to the gateway**.**
- **Firmware** – The details about the firmware version. The **Firmware details** button will redirect the user to the **General settings**, which are explained in the **Settings** menu further down this document.

- **Packet capture** - This is the feature that records data packets transmitted in the network. By clicking the arrow ( ), the user will be redirected to the **Gateway Packet Capture** menu.

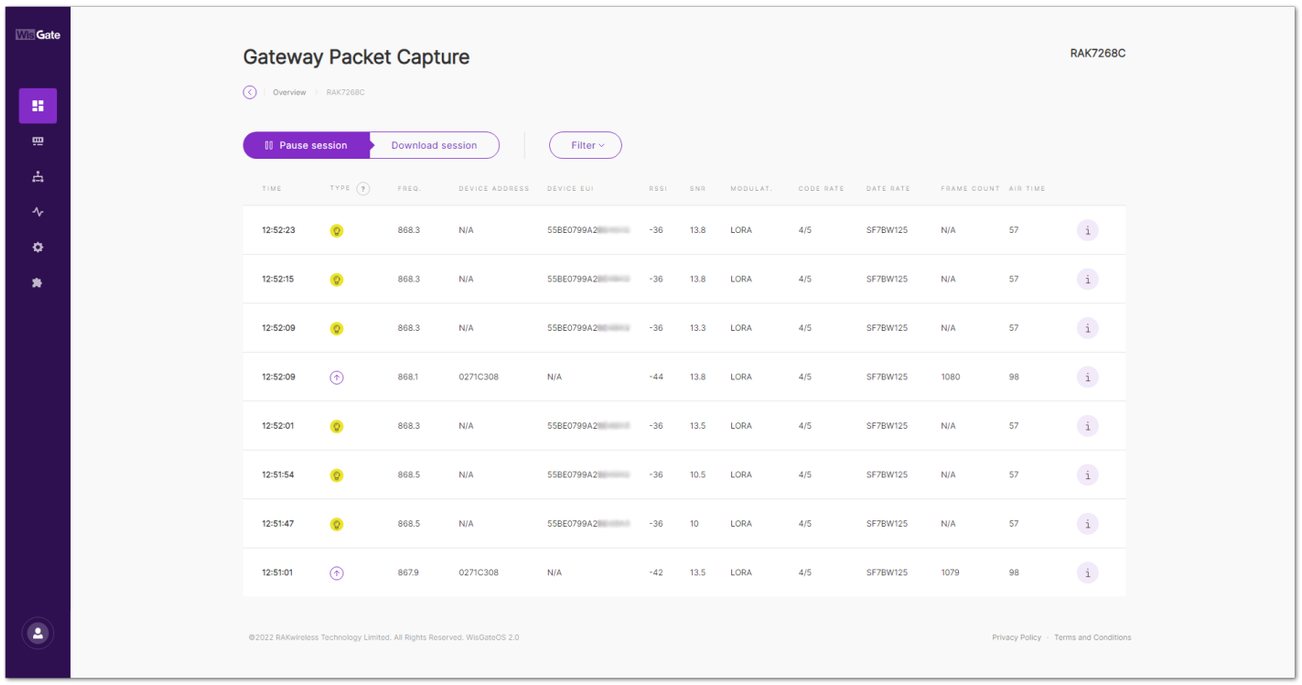

Figure 6: Gateway Packet Capture page

- Gateway Packet Capture menu:
  - **Pause/Restart session** – The button pauses or restarts the session.
  - **Download session** – The button downloads a .json file with packets data in it.
  - **Filter** – The button drops-down a filter menu. The **Reset filter** text, will reset the filter to default. The user can filter the packets by:
    - **Type** – Type of the packet.
    - **Frequency** – The frequency on which the packet is received/sent.
    - **RSSI** – Range of the RSSI.
    - **SNR** – Range of the SNR.
    - **Device address** – In the **Search Device address** field, the user can manually type a device address and the packets sent by that devices will be filtered.
    - **Hide CRC_ERR Packets** – When enabled, the filter will hide all packets with CRC Error.
- **Performance** - This block shows the CPU load and memory used by the gateway in real time.

- **WAN Interfaces** - Shows the available and active interfaces. Clicking the arrow ( ), will redirect the user to the **Network** menu that is explained in detail further down this document.

- **LAN Interfaces** - Shows the available and LAN interfaces and the active one. Clicking the arrow ( ), will redirect the user to the **Network** menu that is explained in detail further down this document.

LoRa

Configuration

In the Configuration tab, the user can set the working mode of the gateway. In the **Work mode** setting the user can set the mode to **Packet forwarder**, **Basics station** or **Built-in network server**.

In addition, the user can set the **Log Level** to **Error** (shows only error logs), **Warning** (shows warnings logs), **Notice** (shows notice logs), **Info** (shows all notice, error, and warning logs) or **Debug**** (this is full log, it shows all types of logs, it is used for debugging).

Depending on the chosen mode, the other available settings and tabs change. By default, the gateway is configured to work in **Built-in network server**.

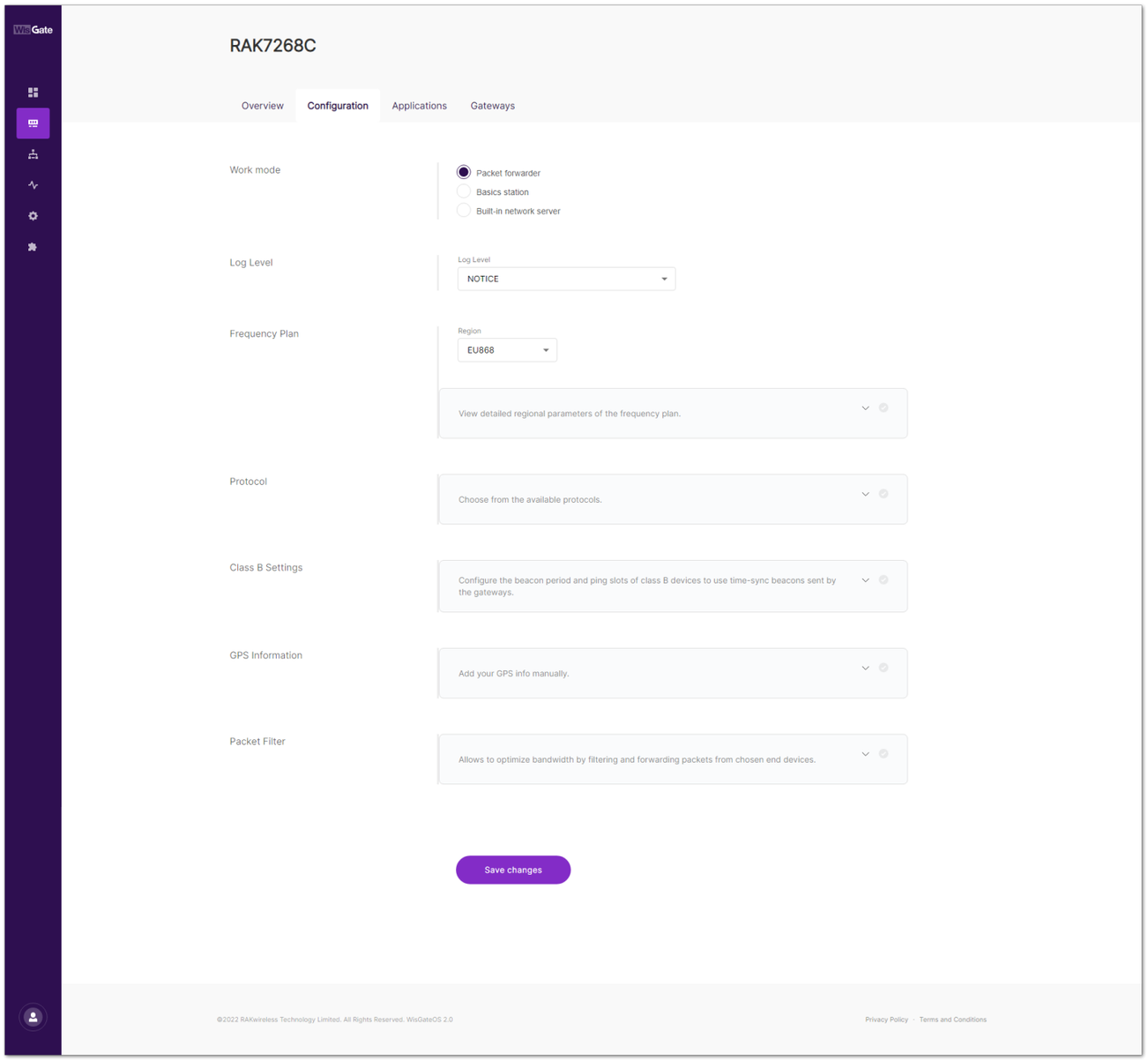

Figure 7: Configuration tab

Packet Forwarder Mode Settings

When you choose **Packet forwarder** work mode, the settings will change to the corresponding ones for this mode. The user can set a packet forwarder and point to a chosen third-party LoRaWAN Network Server.

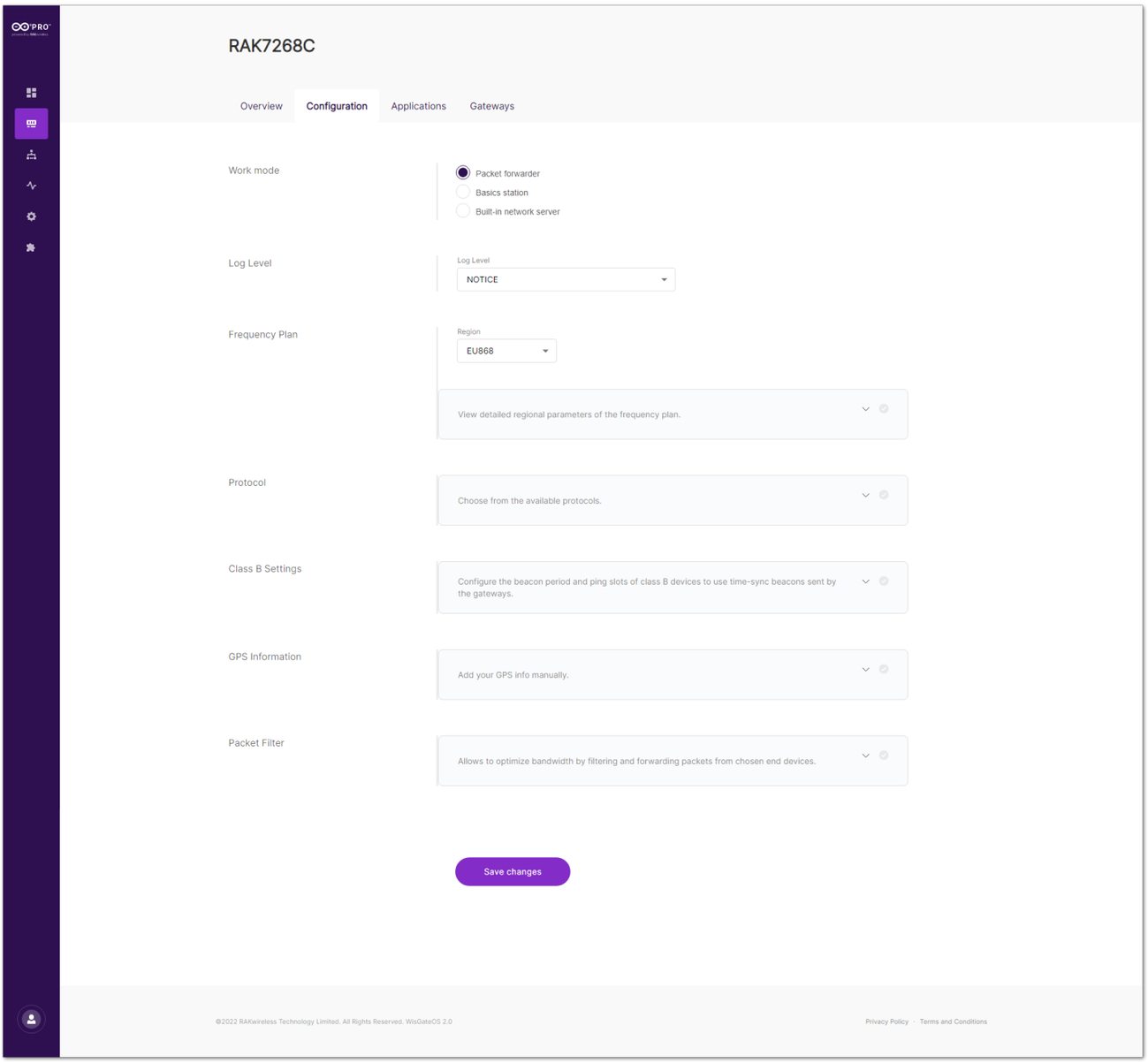

Figure 8: Packet forwarder settings

- **Frequency Plan** - Here, the user can change the frequency plan of the gateway. Click on **View detailed regional parameters of the frequency plan** to expand the options.

  For middle band gateways (supporting **RU864**, **IN865**, and **EU868** LoRaWAN regions) and for high band gateways (supporting **US915**, **AU915**, **KR920**, and **AS923** LoRaWAN regions) there are differences in the frequency sub-bands section.

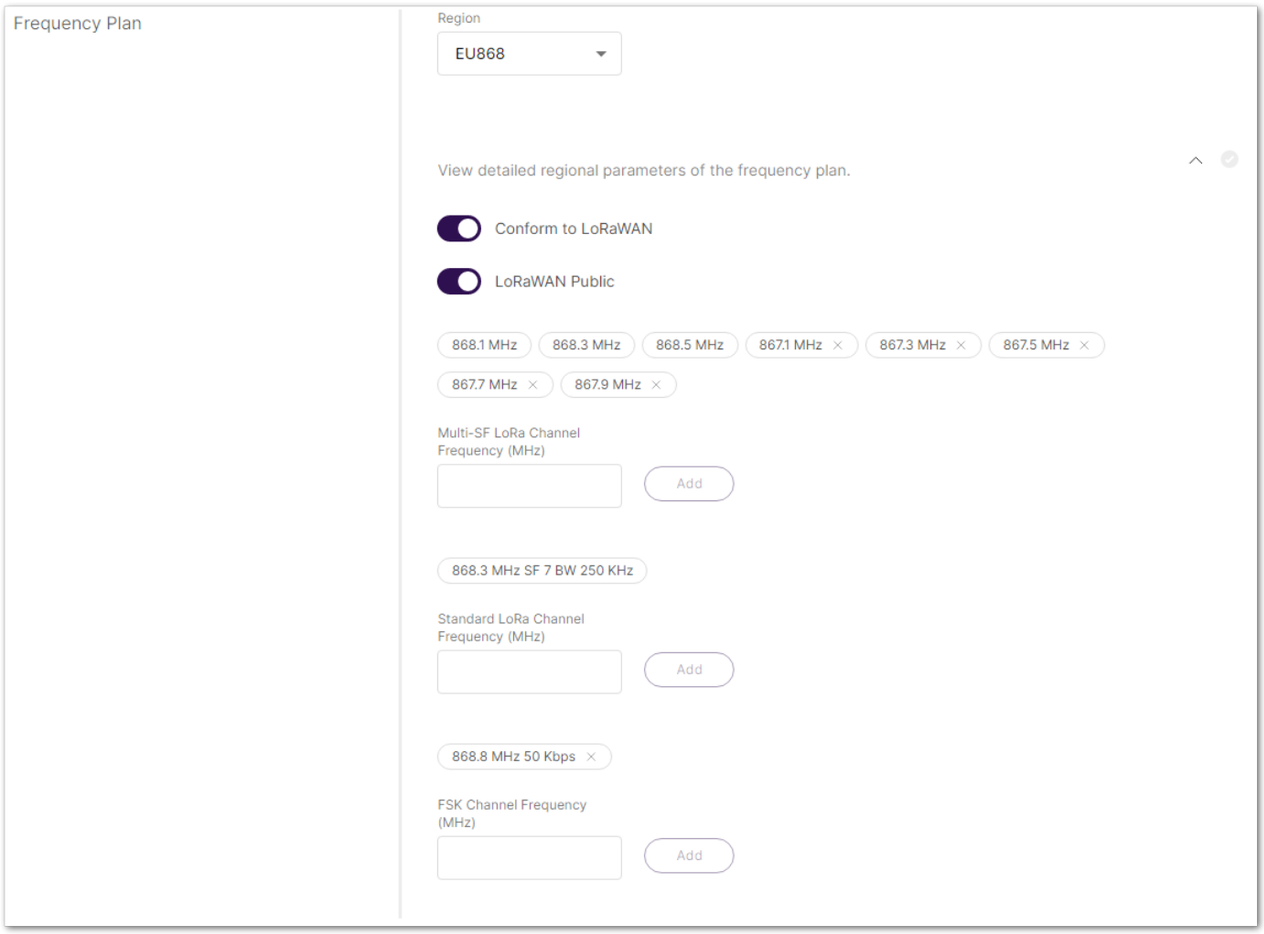

Figure 11: Frequency plan settings for different LoRaWAN regions

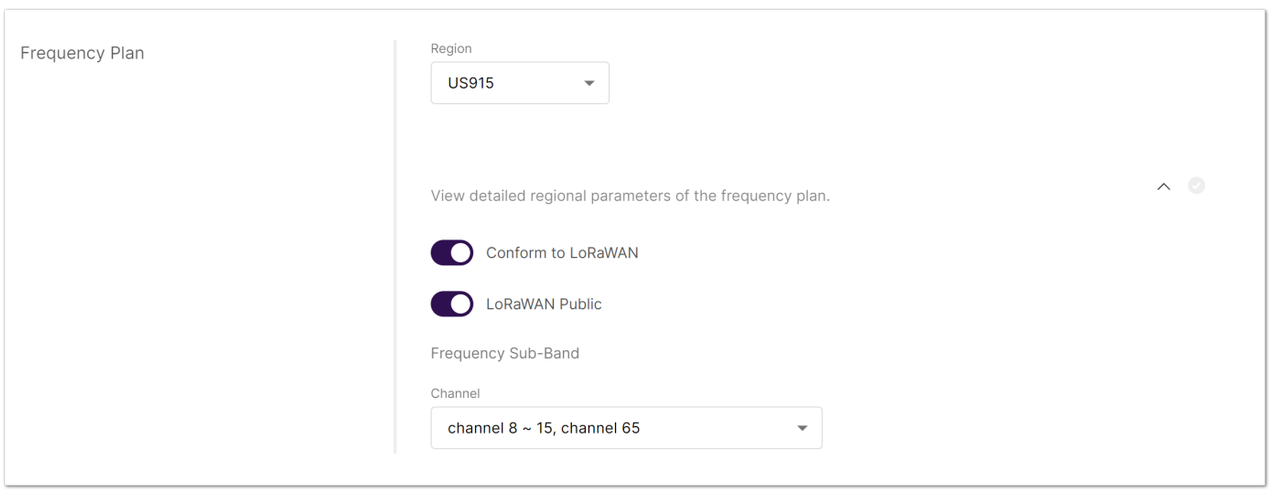

Figure 12: Frequency plan settings for different LoRaWAN regions

- **Region** - Here is where the region is set. Note that different hardware supports different LoRaWAN regions.
- **Conform to LoRaWAN** - When enabled (by default), the gateway will comply to the LoRaWAN protocol. The user can disable it and set their own channels.

  When **Conform to LoRaWAN** is disabled, you can either **Select a template** or manually **Edit** the LoRa channels for each concentrator.

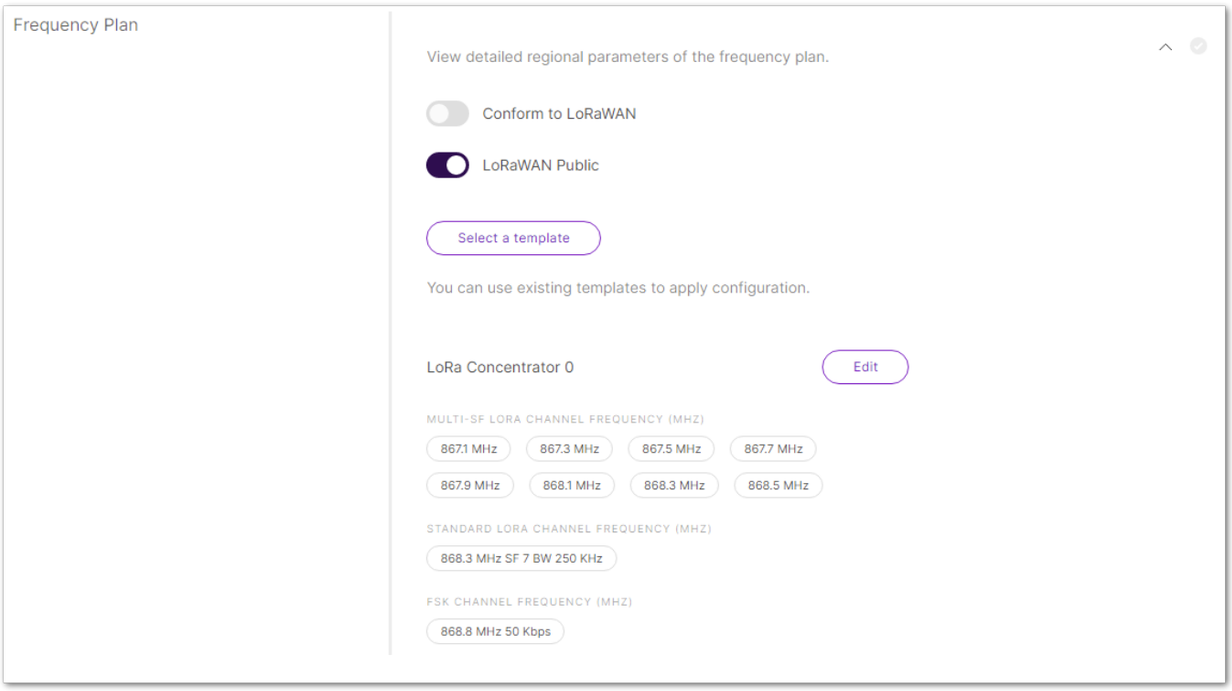

Figure 10: Confirm to LoRaWAN is disabled

- **Select a template** - The user have a list of templates for frequency plans to choose from depending on the LoRaWAN region that the gateway supports.
- **Edit** button - Clicking the button will redirect the user to the LoRa Concentrator settings, where they can set custom channels.

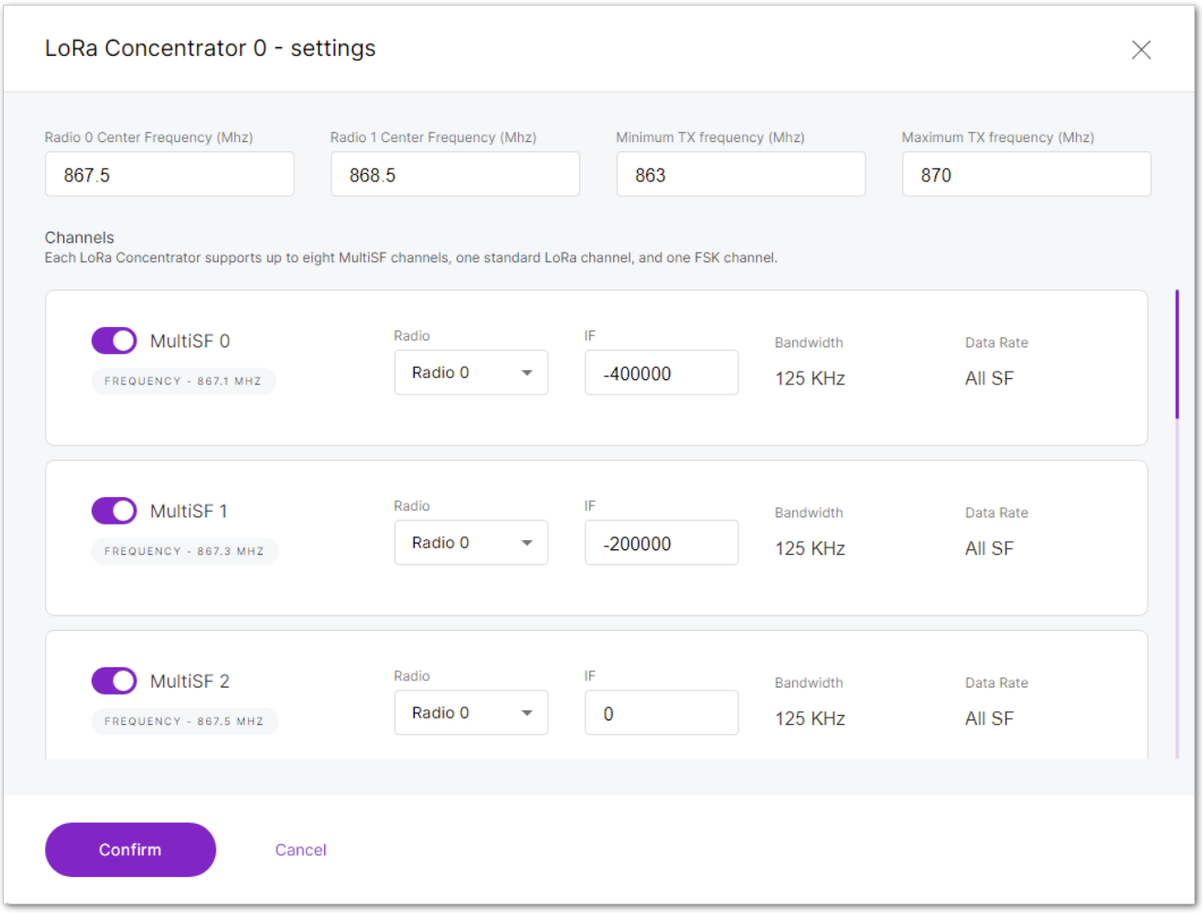

Figure 9: LoRa Concentrator settings

- **Radio 0 Center Frequency (Mhz)** – The center frequency for radio 0.
- **Radio 1 Center Frequency (Mhz)** - The center frequency for radio 1.
- **Minimum TX frequency (Mhz)** – The minimum frequency for transmission.
- **Maximum TX frequency (Mhz)** – The maximum TX frequency for transmission.

        - **Channels** - The user can enable/disable channels with the corresponding switch. In the **Radio** field, the user can select what radio the channel must use. In the **IF** field, the difference of the frequency of the selected radio center frequency in kHz is written.

    - **LoRaWAN Public** - When enabled (by default), the gateway will process data from all end devices. If you want to create a private network, you can turn it off. The gateway will process the data only from the end devices, which sync word is changed to private.

    - **Additional for the middle band gateways** (supporting **RU864**, **IN865**, and **EU868** LoRaWAN regions) - Under the **LoRaWAN Public** switch, the user sees the default channels and can remove them by clicking on the **X** next to each.

        - **Multi-SF LoRa Channel Frequency (MHz)** – The user can add a frequency for the Multi-SF LoRa channel.
        - **Standard LoRa Channel Frequency (MHz)** – The user can add a frequency for the standard LoRa channel.
        - **FSK Channel Frequency (MHz)** – The user can add a frequency for the FSK channel.

    - **Additional for the high band gateways** (supporting **US915**, **AU915**, **KR920**, and **AS923** LoRaWAN regions) - Under the **LoRaWAN Public** switch, the user sees the **Frequency Sub-band** section. From the drop-down menu, the user can choose sub-bands to use for the uplink traffic.

- **Protocol** - Here, click on **Choose from the available protocols** and expand the options, the user can choose which protocol to use as well as the **Static Interval (sec)** (the time interval of how often statistics are pushed to the server).

- **Semtech UDP GWMP Protocol** - Choosing this option will give the user the ability to set **UDP Protocol Parameters**.

    - **Server address** – The address of the LoRa Network Server (LNS).

    - **Server Port Up/Down** – The ports of the LoRa Server that are going to be used for inbound and outbound traffic.

    - **Push Timeout (sec)** - The time delay for the server response after sending uplink data.

    - **Keepalive Interval (sec)** - The interval of which the gateway sends data to make sure that the server is aware that the gateway is online.

    - **Auto-restart Threshold** - This variable defines how many times the Keepalive Interval can expire before the Packet Forwarder restarts.

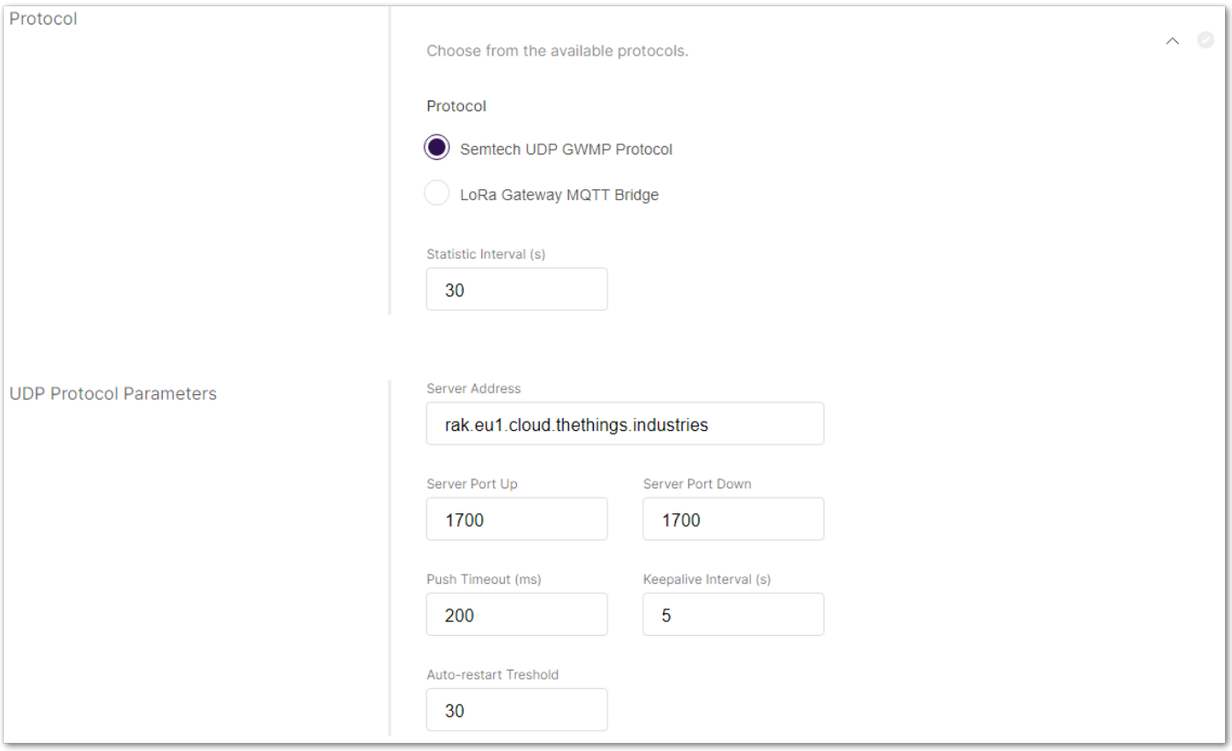

Figure 13: UDP Protocol Parameters

- **LoRa Gateway MQTT Bridge** - Choosing this option will give the user the ability to set **LoRa Gateway MQTT Bridge Parameters**.
  - **MQTT Protocol** – From the drop-down menu, the user can choose the MQTT protocol of the MQTT bridge (**MQTT for Built-in LoRa Network Server**, **MQTT for ChirpStack 2.x**, **MQTT for ChirpStack 3.x (JSON)** or **MQTT for ChirpStack 3.x (Protobuf)**). Note that the MQTT topics change depending on the chosen protocol.
  - **MQTT Broker Address** - The IP address of the gateway where the MQTT Broker is hosted.
  - **MQTT Broker Port** – The corresponding port (default port is 1883).
  - **MQTT Protocol Version -** You can choose between V3.1 and V3.1.1. There is very little difference between them, more information can be found here .
  - **QoS** - You can set the desired Quality of Service level.
  - **Keepalive Interface (sec)** - The keepalive interval in seconds (10 default).
  - **Clean Session** - When this function is enabled, the Broker will not store any subscription information or undelivered messages.
  - **Retain** - When this function is enabled, the last message published will be retained.
  - **Enable User Authentication** - This function enables user authentication via username and password.
  - **SSL/TLS Mode -** When enabled (disabled by default), you can choose between three modes **CA signed server certificate**, **Self-signed server certificate**, and **Self-signed server & client certificate**, with their corresponding options.
  - **Uplink/Downlink/Downlink Acknowledge/Gateway Statistic Topic** – MQTT template topics. These topics cannot be changed.

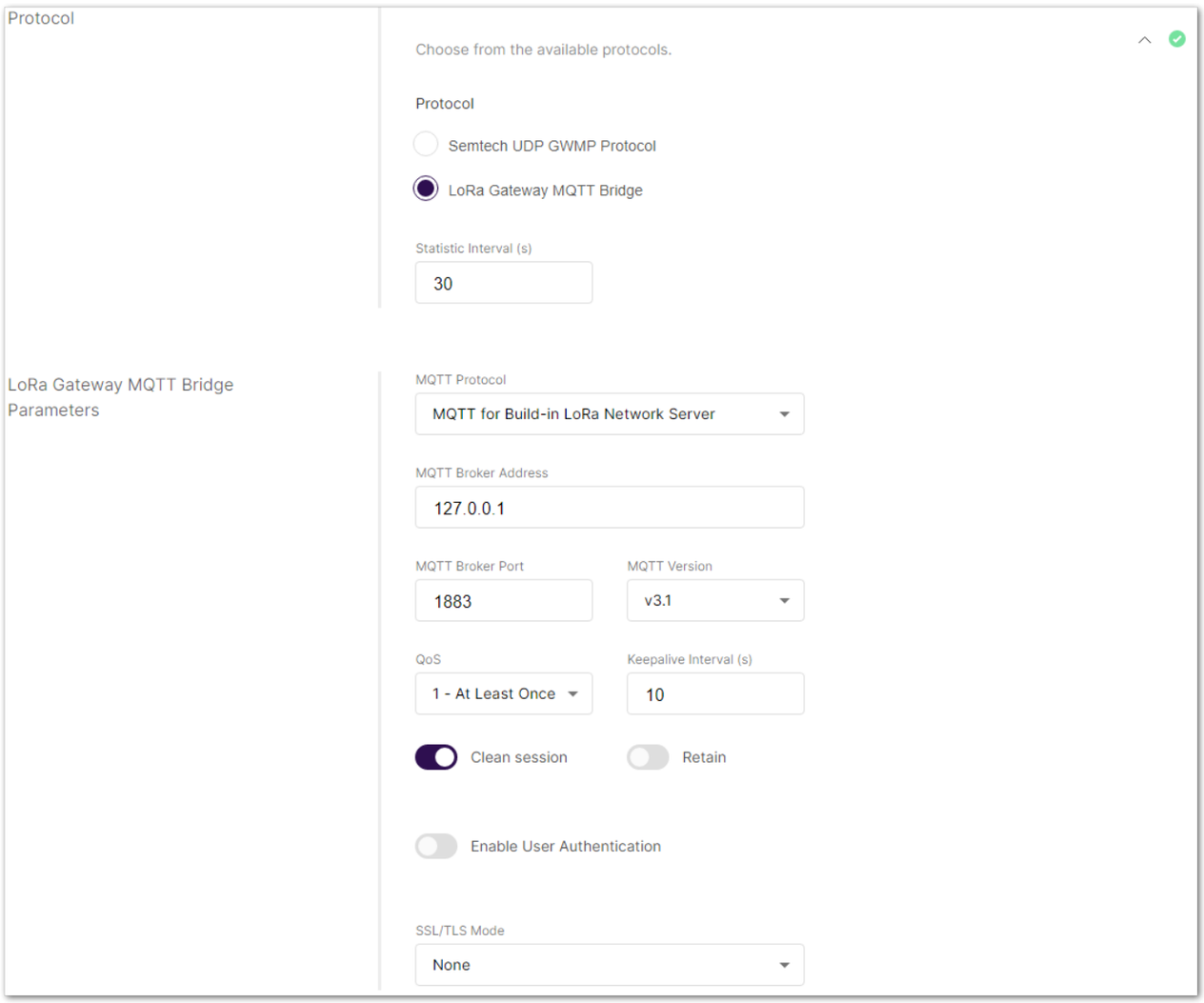

Figure 14: LoRa Gateway MQTT Bridge Parameters

- **Class B Settings** - Here, the user can enable/disable the class B beaconing. Click on **Configure the beacon period and ping slots of class B devices to use time-sync beacons sent by the gateways** to expand class B settings.
  - **Enable Beacon** – Enables the class B beacon.
  - **Beacon Tx Power** – The power for transmitting the beacon ping.

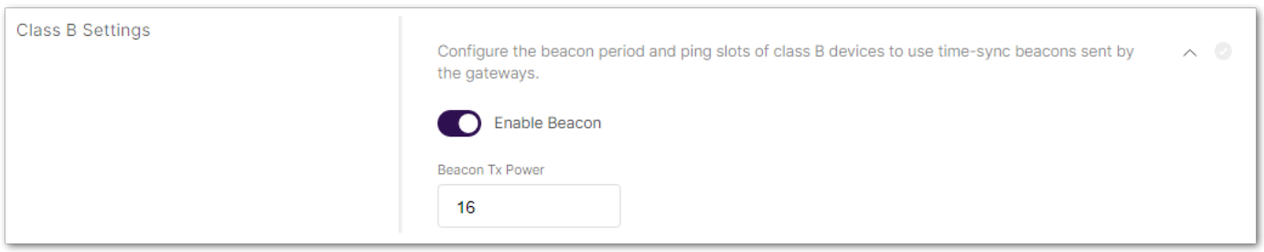

Figure 15: Class B Settings

- **GPS Information** Here, the user can set fake GPS coordinates (disabled by default). Click on **Add your GPS info manually** to expand the GPS settings and enable **Fake GPS** with the switch.

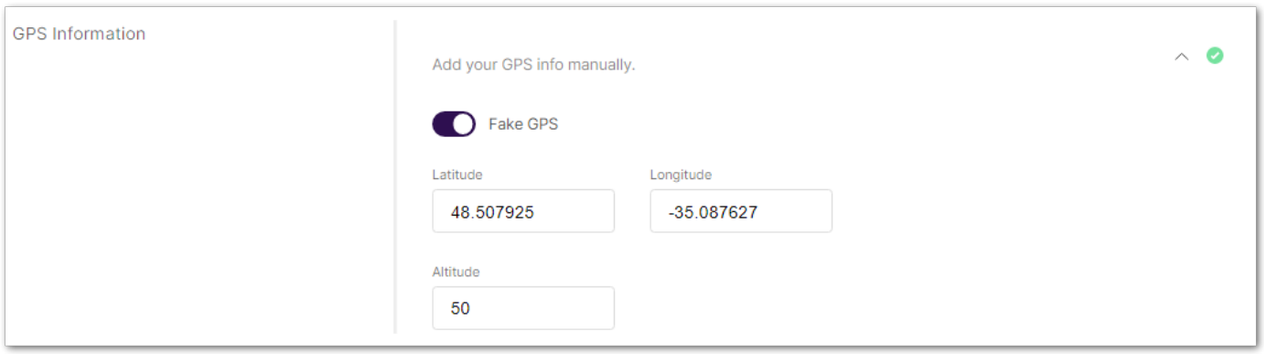

Figure 16: GPS Information

- **Packet Filter** - Here, the user can set a filter for the packets from chosen devices (disabled by default). Click on **Allows to optimize bandwidth by filtering and forwarding packets from chosen end devices** to expand packet filter settings. If **White List Mode** and **Auto Filter** are enabled, the user have the options:
  - **OUI** – This is white list filtering option to filter by Organizationally Unique Identifier of the end device.
  - **Network ID** – This is a white list filtering option to filter by Network ID.
  - **Discard Period (s)** – This is a period threshold of discard time for nodes (in seconds).
  - **Join Period (s)** – This is a period threshold of Statistics on the latest join request (in seconds).
  - **Join Interval (s)** – This is a time interval threshold of the same device EUI twice-consecutive join request (in seconds).
  - **Join Count 1** – This is the maximum count of join requests allowed during Join Interval.
  - **Join Count 2** – this is the maximum count of join requests allowed during the Join Period.

Basics Station Mode Settings

When the **Basics station** work mode is chosen, the corresponding settings pop up replacing the ones for other work modes.

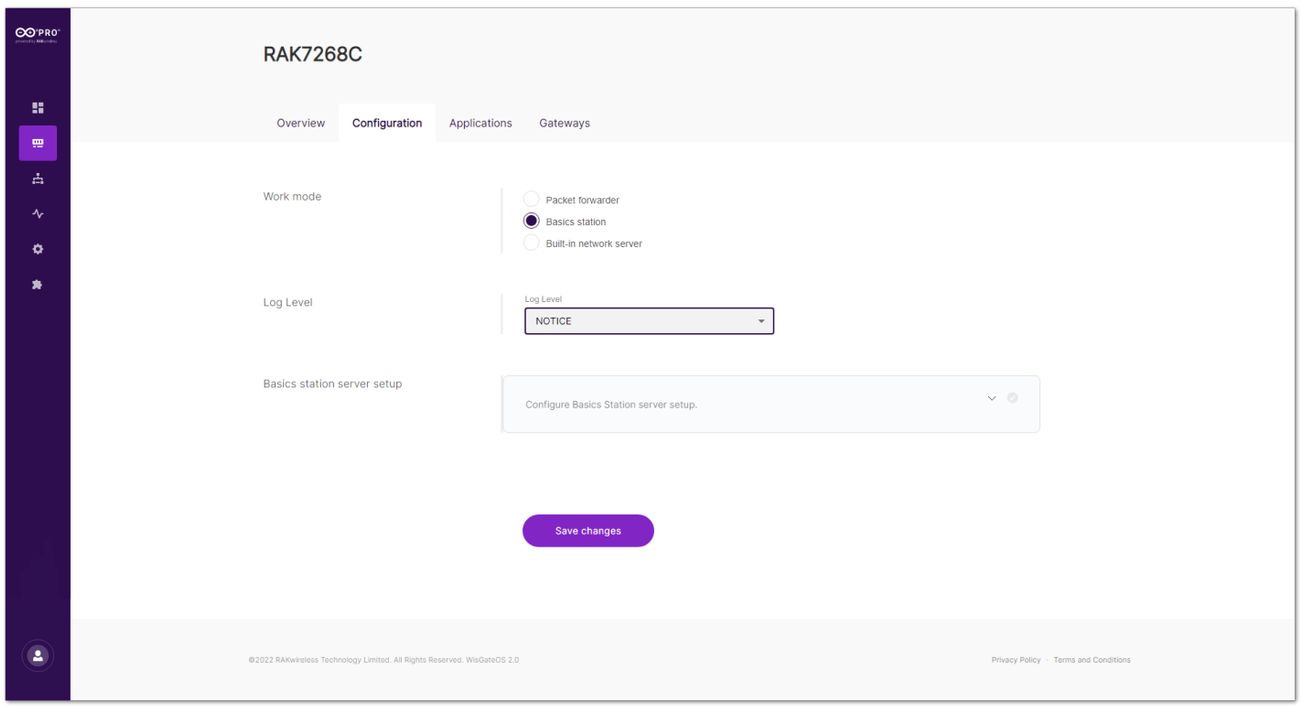

Figure 17: Basics station settings

- To expand the **Basics station server setup** menu, the user needs to click on **Configure Basics Station server setup.**

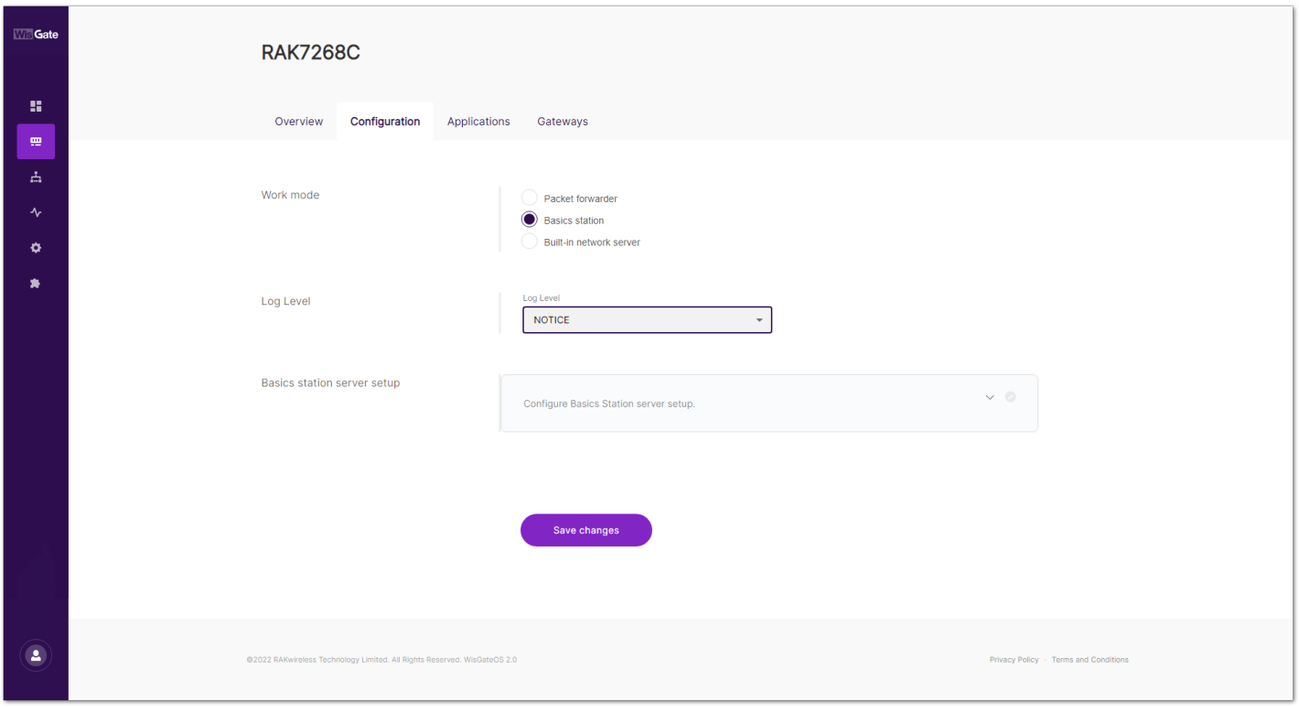

Figure 18: Basics station server setup

- **Basics Station Server Type** - The user can choose between **CUPS-BOOT Server**, **CUPS Server**, **LNS Server**.
- **Server URL** – The address of the server to which the gateway is going to connect.
- **Server Port** – This is the corresponding port of the server.
- **Authentication Mode** – The user can choose between four options with their corresponding fields:
  - **No Authentication** - The server requires no authentication.
  - **TLS Server Authentication** - The server requires a **trust** file for authentication.
  - **TLS Server and Client Authentication** - The server requires **trust**, **certificate**, and **key** files for authentication.
  - **TLS Server Authentication and Client Token** - The server requires a **trust** file and a client **token**.

Built-in Network Server Mode Settings

When the **Built-in network server** work mode is chosen, the corresponding settings pop up replacing the ones for other work modes.

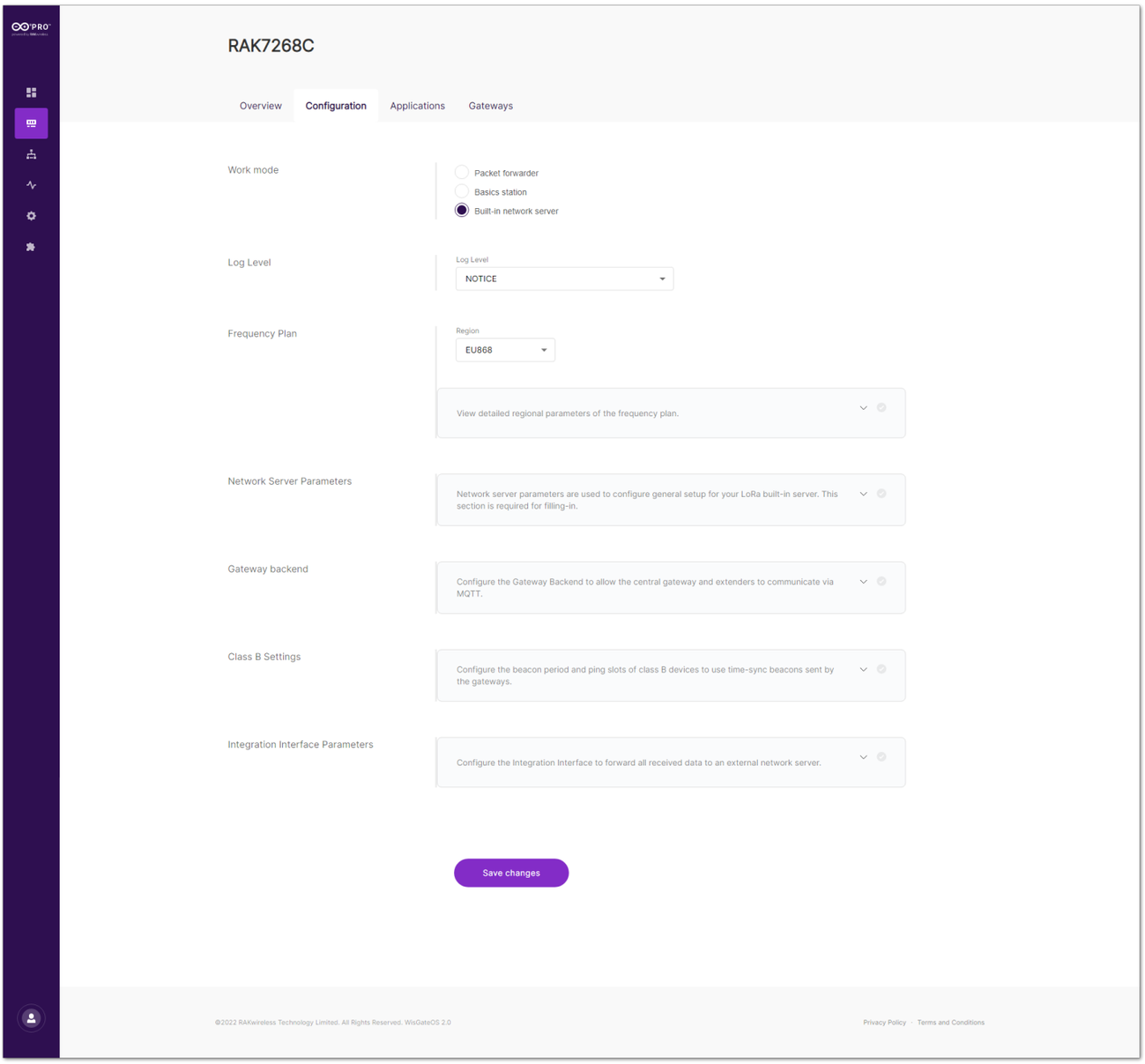

Figure 19: Built-in network server settings

- **Frequency Plan** - Here, the user can change the frequency plan of the gateway. Click on **View detailed regional parameters of the frequency plan** to expand the options.

  For middle band gateways (supporting **RU864**, **IN865**, and **EU868** LoRaWAN regions) and for high band gateways (supporting **US915**, **AU915**, **KR920**, and **AS923** LoRaWAN regions) there are differences in the frequency sub-bands section.

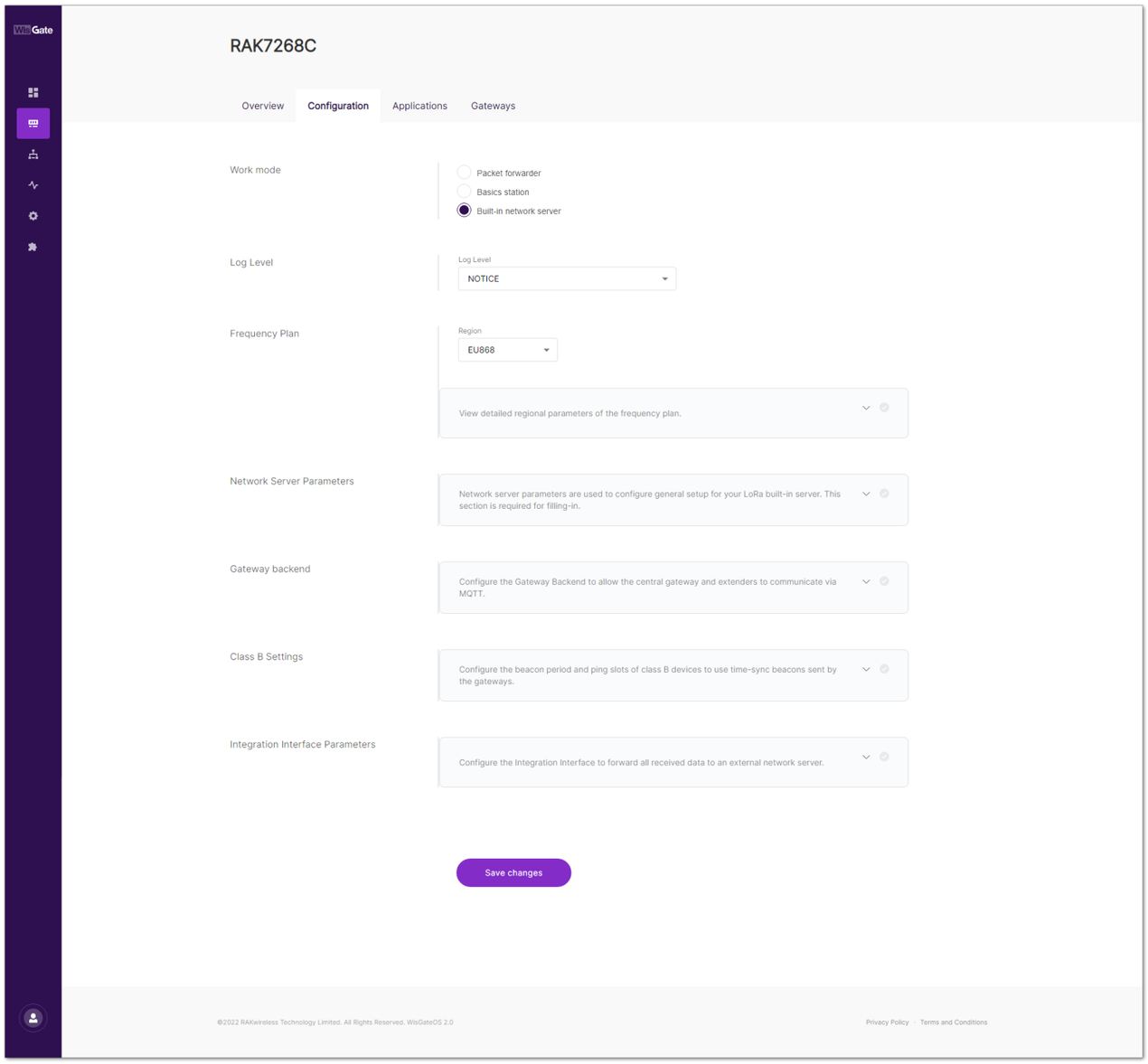

Figure 20: Frequency plan settings for different LoRaWAN regions

- **Region** - Here is where the region is set. Note that different hardware supports different LoRaWAN regions.
- **LoRaWAN Public** - When enabled (by default), the gateway will process data from all end devices. If you want to create a private network, you can turn it off. The gateway will process the data only from the end devices, which sync word is changed to private.
- **Additional for the middle band gateways** (supporting **RU864**, **IN865**, and **EU868** LoRaWAN regions) - Under the **LoRaWAN Public** switch, the user sees the default channels and can remove them by clicking on the **X** next to each.
  - **Multi-SF LoRa Channel Frequency (MHz)** – The user can add a frequency for the Multi-SF LoRa channel.
  - **Standard LoRa Channel Frequency (MHz)** – The user can add a frequency for the standard LoRa channel.
  - **FSK Channel Frequency (MHz)** – The user can add a frequency for the FSK channel.
- **Additional for the high band gateways** (supporting **US915**, **AU915**, **KR920**, and **AS923** LoRaWAN regions) - Under the **LoRaWAN Public** switch, the user sees the **Frequency Sub-band** section. From the drop-down menu, the user can choose sub-bands to use for the uplink traffic.

- **Network Server Parameters** - The user needs to click on **Network server parameters are used to configure general setup for your LoRa built-in server. This section is required for filling-in.** to expand the settings menu.

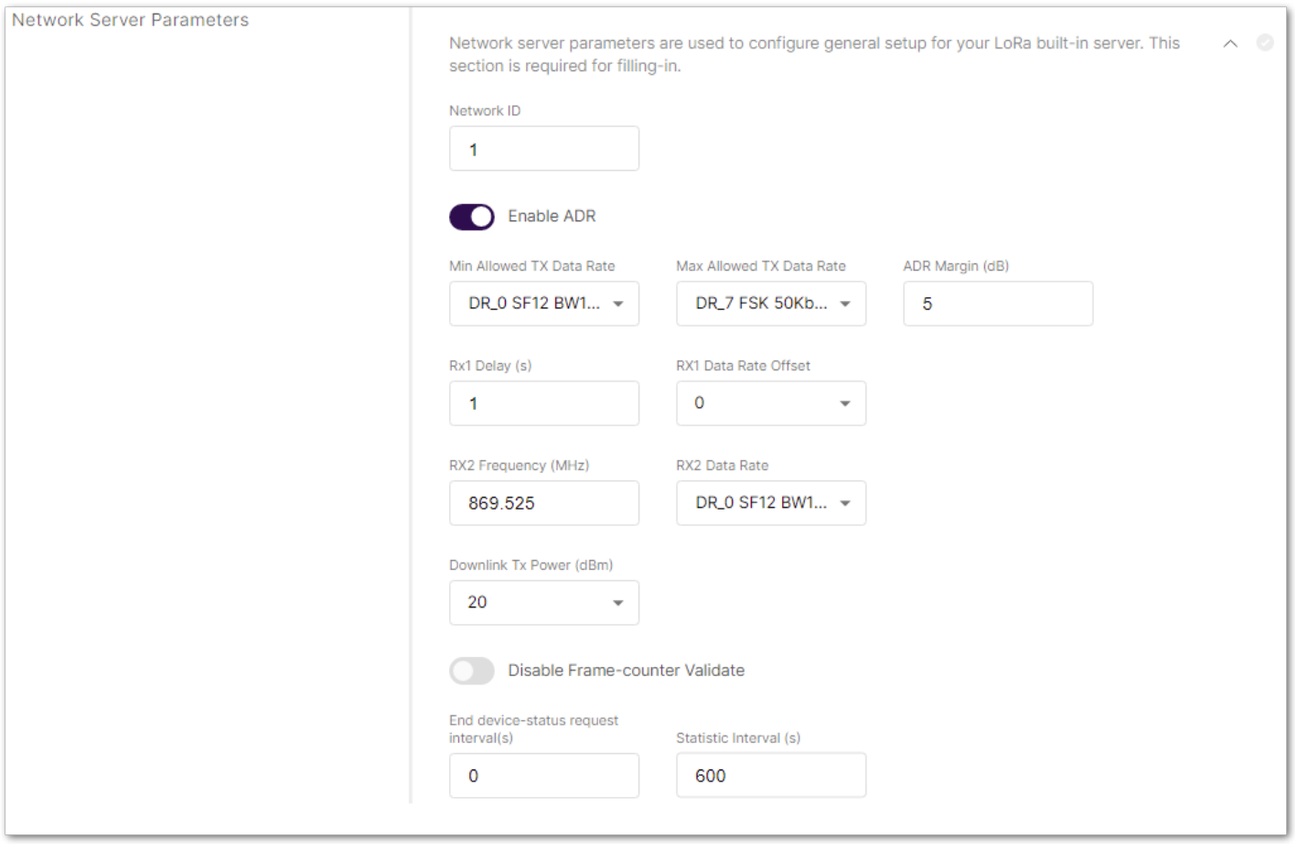

Figure 21: Network Server Parameters

- **Network ID** – This is a decimal number to distinguish between networks if the user is deploying multiple ones.
- **Enable ADR** – The switch enables/disables Adaptive Data Rate. The built-in server will optimize the data rates, airtime, and energy consumption in the network depending upon the prevailing channel conditions.
- **Minimum/Maximum Allowed TX Data-Rate** - DR0 to DR7 can be selected to limit the ADR possible values range. Depends on the Region.
- **ADR Margin (dB)** – This is visible only when ADR is enabled. It is a value to keep in dB to make sure that the data rate is not overestimated resulting in poor performance (error rate and range).
- **Rx1 Delay (s)** – This is the delay of the first receive window in seconds.
- **RX1 Data Rate Offset** - This determines the data rate of the downlink frames originating from the Gateway for the Rx1 window. By default, it is 0 – identical to the uplink.
- **RX2 Frequency (MHz)** – This is the frequency of the second receive window in Hz.
- **RX2 Data Rate** - The Data Rate of the frames to be sent in the second receive window.
- **Downlink Tx Power (dBm)** – It is useful, if you want to use a larger antenna with more gain. Values from -6 to 20 are permissible.
- **Disable Frame-counter Validate** - this function turns on/off the Frame counter validation.
- **End device-status request interval (s)** - This shows how often should the end-devices be polled for their status Log Level.
- **Statistic Interval (sec)** – This shows how often the statistics will be gathered.
- **Gateway backend** - To extend the settings field, the user needs to click on **Configure the Gateway Backend to allow the central gateway and extenders to communicate via MQTT**.

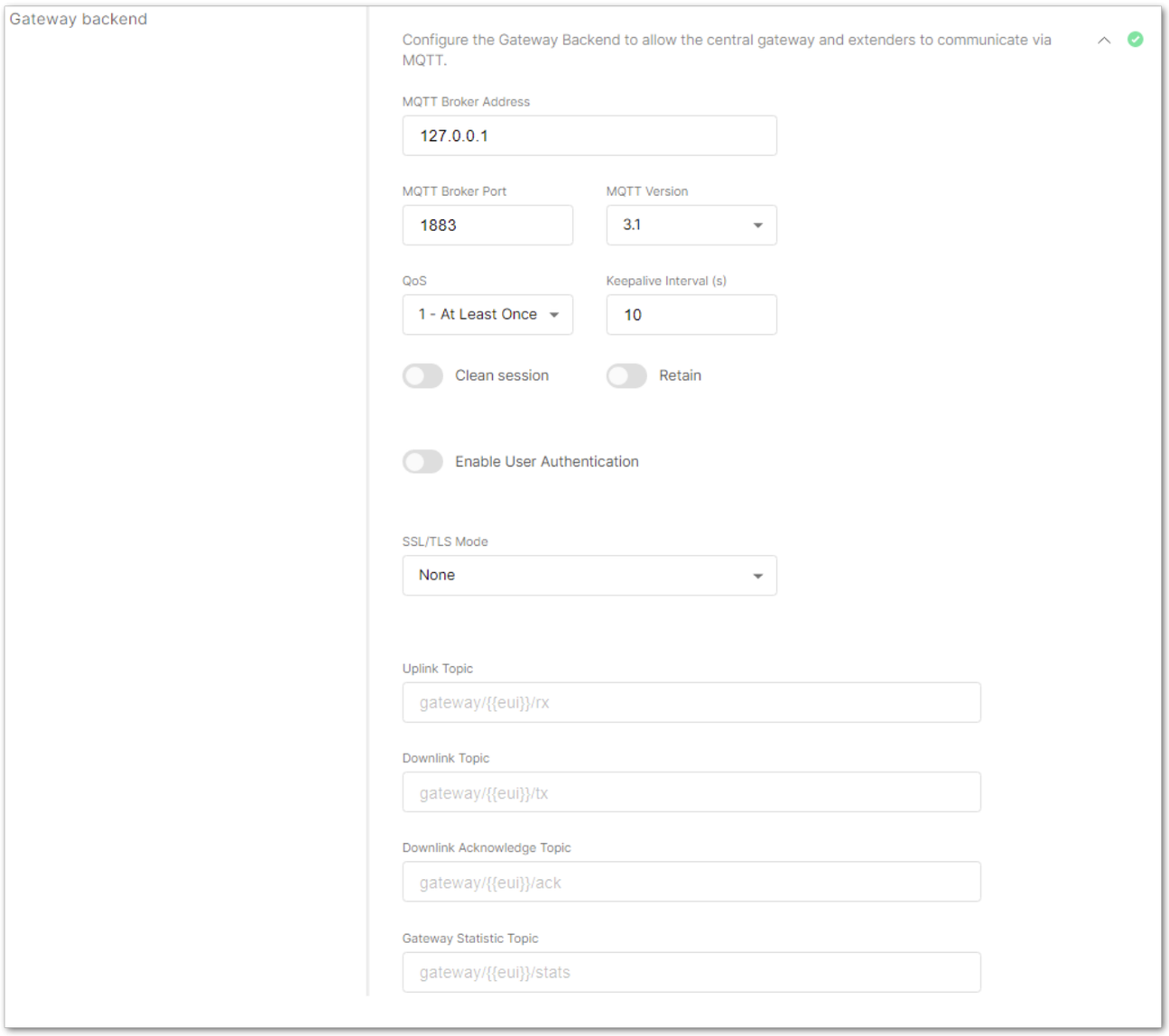

Figure 22: Gateway backend

- **MQTT Broker Address** - The IP address of the machine where the MQTT Broker is hosted (default is 127.0.0.1 for the built-in one).
- **MQTT Broker Port** - The corresponding port (default port is 1883).
- **MQTT Protocol Version** - You can choose between V3.1 and V3.1.1. There is very little difference between them, more information can be found here .
- **QoS** - You can set the desired Quality of Service level. More information about QoS can be found here .
- **Keepalive Interval (s)** - The keepalive interval in seconds (10 default).
- **Clean session** – When this function is enabled (disabled by default), the Broker will not store any subscription information or undelivered messages.
- **Retain** – When this function is enabled (disabled by default), the last message published will be retained.
- **Enable User Authentication** – This function enables Encryption of the transmitted data (disabled by default). The user needs to configure the credentials (username and password) used to encrypt the data to secure authentication being performed.
- **SSL/TLS Mode** - When this mode is enabled (disabled by default), you can choose between three modes **CA signed server certificate**, **Self-signed server certificate**, **Self-signed server & client certificate**, with their corresponding options.

- **Uplink/Downlink/Downlink Acknowledge/Gateway Statistic Topic** – These are MQTT topic templates. They cannot be changed.
- **Class B Settings** - Here. the user can enable/disable the class B beaconing. To expand the menu, click on **Configure the beacon period and ping slots of class B devices to use time-sync beacons sent by the gateways**.

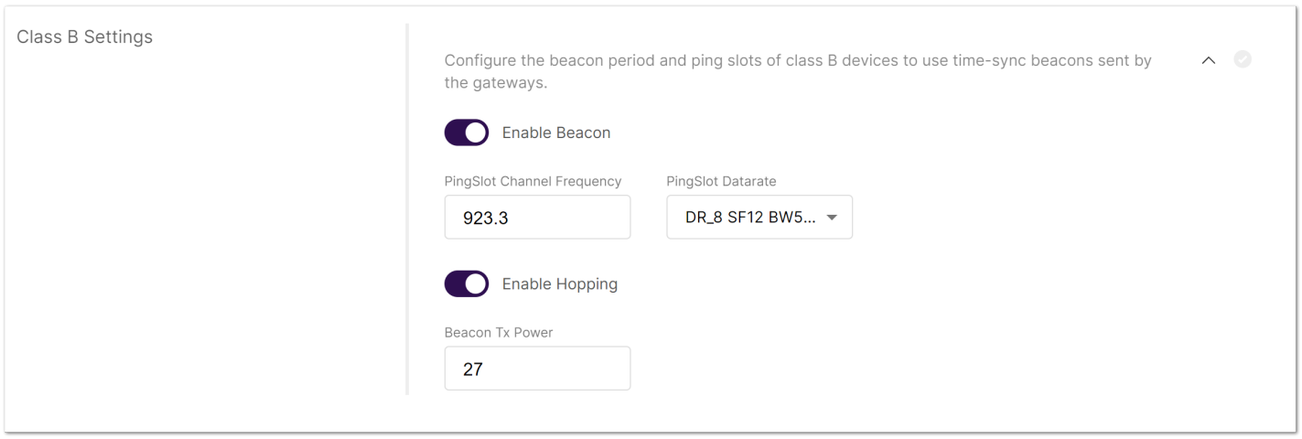

Figure 23: Class B Settings

- **Enable Beacon** – The switch enables/disables Class B beaconing.
- **PingSlot Channel Frequency** – The frequency used for the beacon ping.
- **PingSlot Datarate** – The minimum duration of each beacon ping slot.
- **Enable Hopping** - Enables/disables Class B hopping as the class B beacon is transmitted following a frequency hopping pattern.
- **Beacon TX Power** – This is the transmit power of the beacon ping.
- **Integration Interface Parameters** - Here, the user can configure an integration to an external server. To expand the menu, the user needs to click on **Configure the Integration Interface to forward all received data to an external network server**. The settings change depending on the chosen **Integration mode.**

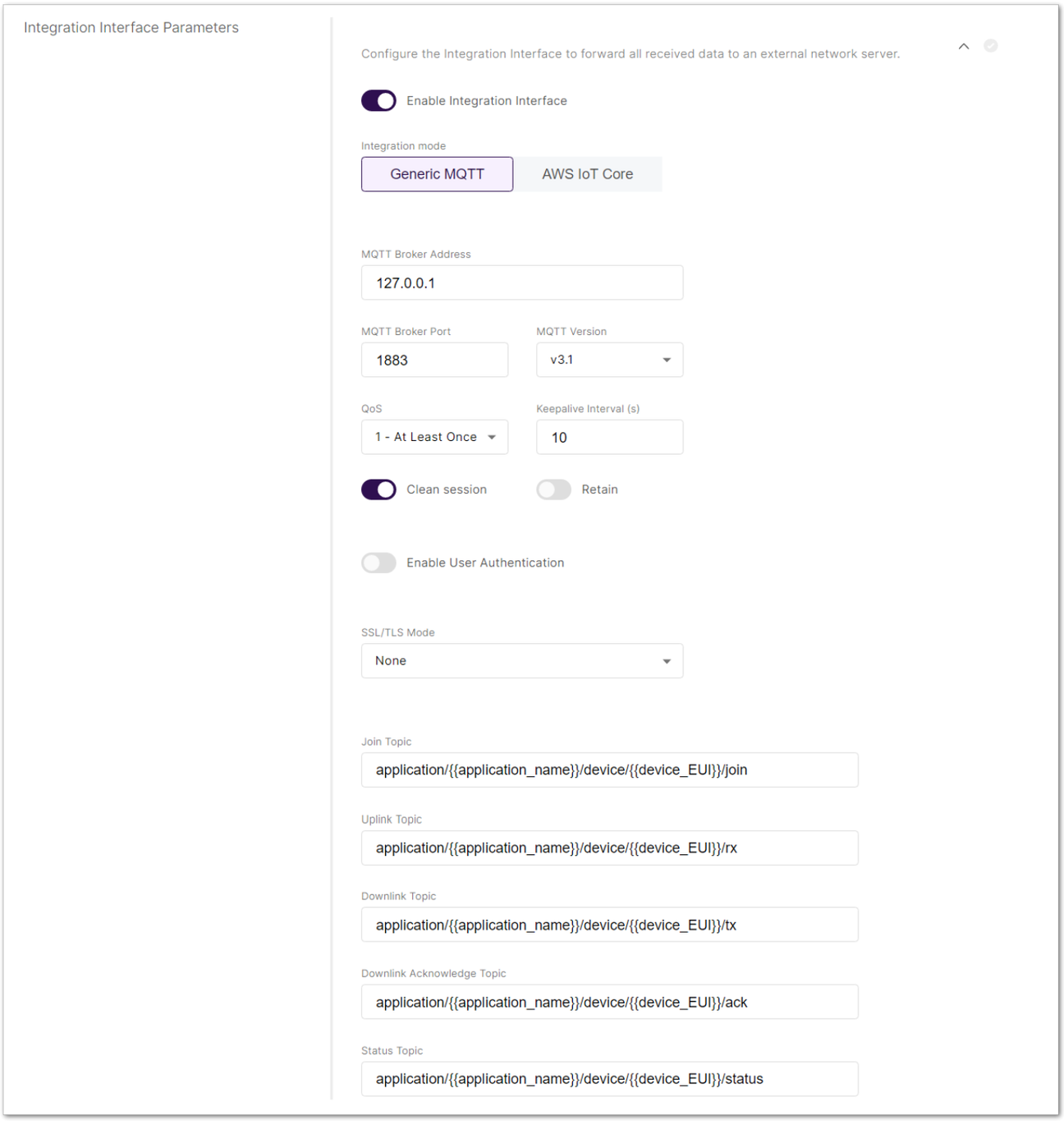

Figure 24: Integration Interface Parameters

- **Enable Integration Interface** – This switch enables the Integration Interface switch enables/disables the integration.
- **Generic MQTT** integration mode:
  - **MQTT Broker Address** - The IP address of the machine where the MQTT Broker is hosted (default is 127.0.0.1 for the built-in one).
  - **MQTT Broker Port** - The corresponding port (default port is 1883).
  - **MQTT Protocol Version** - You can choose between V3.1 and V3.1.1. There is very little difference between them, more information can be found here .
  - **QoS** - You can set the desired Quality of Service level. More information about the QoS can be found here .
  - **Keepalive Interval (s)** - The keepalive interval in seconds (10 default).
  - **Clean session** – When this function is enabled, the Broker will not store any subscription information or undelivered messages.
  - **Retain** – When this function is enabled, the last message published will be retained
  - **Enable User Authentication** - This function enables user authentication via username and password.
  - **SSL/TLS Mode** - When this mode is enabled (disabled by default), you can choose between three modes **CA signed server certificate**, **Self-signed server certificate**, **Self-signed server & client certificate**, with

their corresponding options.
    - **Join/Uplink/Downlink/Downlink Acknowledge/Status Topic** – These are MQTT topic templates. They cannot be changed.
- **AWS IoT Core** integration mode:
    - **AWS IoT Core endpoint URL** – This is the address of the AWS.
    - **AWS IoT Core endpoint Port** – The corresponding port of the server.
    - **Root CA** - CA certificate provided by the AWS IoT Core.
    - **Certificate** - Certificate for the gateway, generated by AWS IoT Core.
    - **Key** - Private key for the gateway, generated by AWS IoT Core.

Applications

In this tab, the user can create an application and register end devices in the Built-in Network Server. By default, there will be no created Applications. Note that this tab is available only when the gateway is in Built-in Network Server working mode.

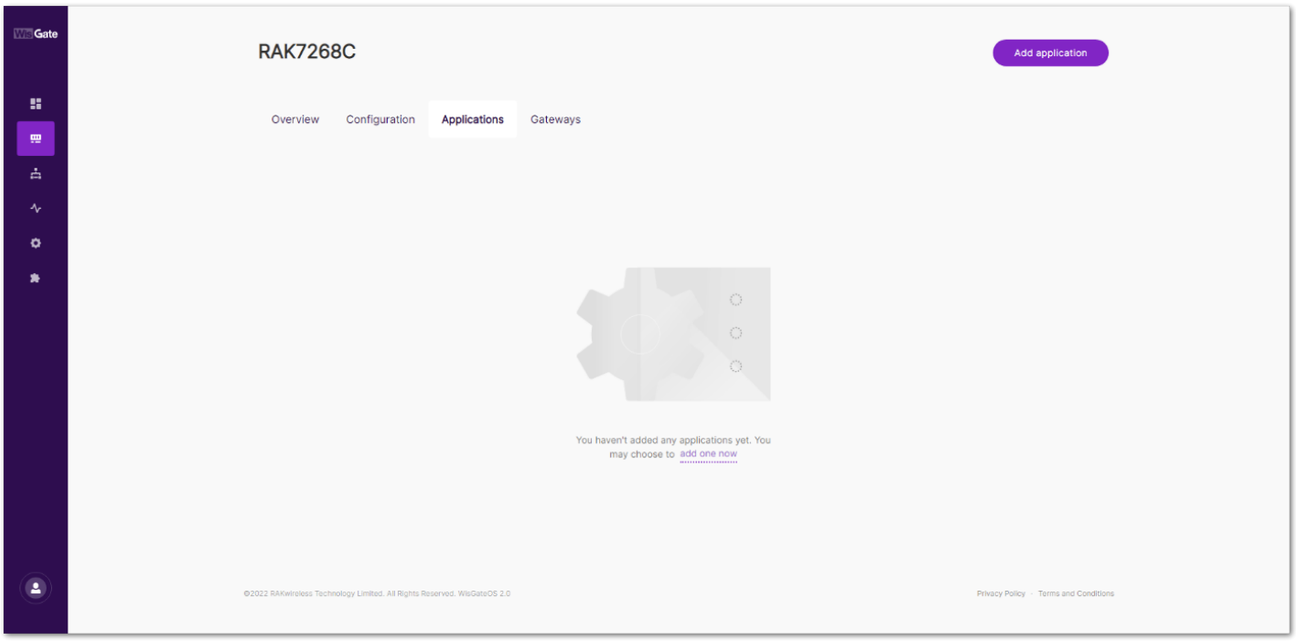

Figure 25: Applications tab

Gateways

In this tab, the user can add **extender** gateways to work with the LNS. The current gateway do not need to be added as the Network Server is working on it and it acts as the **central** gateway. Note that this tab is available only when the gateway is in Built-in Network Server working mode.

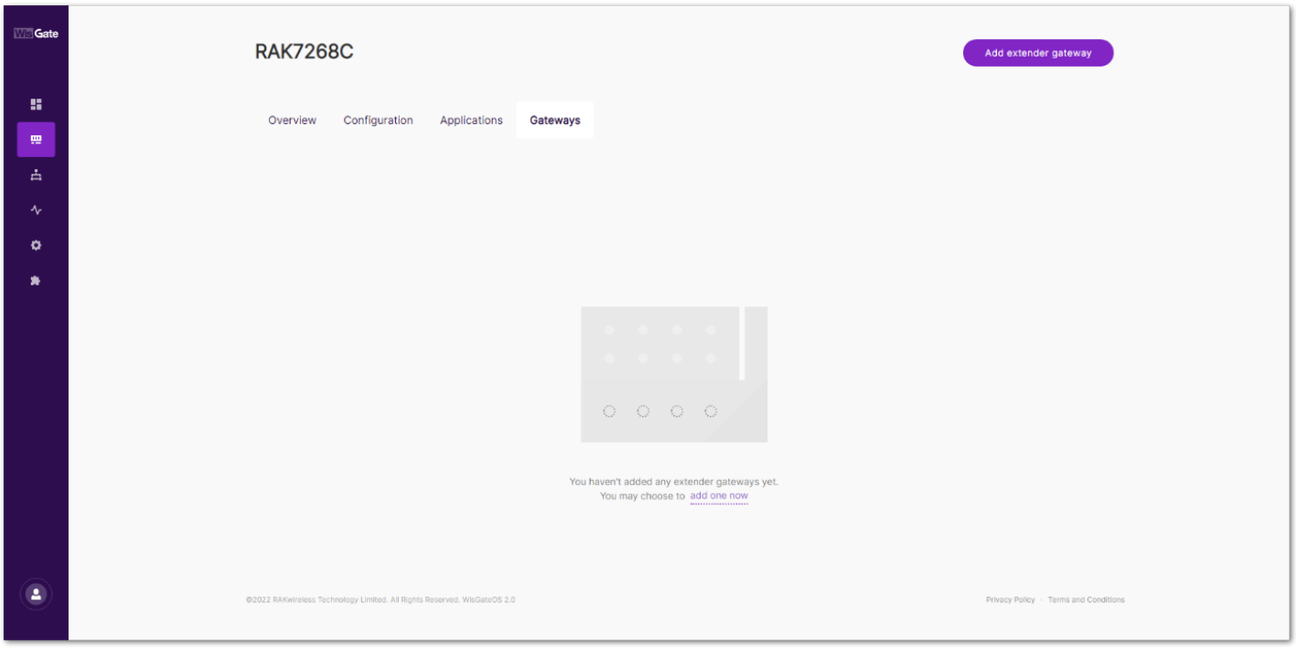

Figure 26: Gateways tab

Overview

In this tab, the user can see information about the end devices and traffic going thru the extender gateways and the central gateway. Note that this tab is available only when the gateway is in Built-in Network Server working mode.

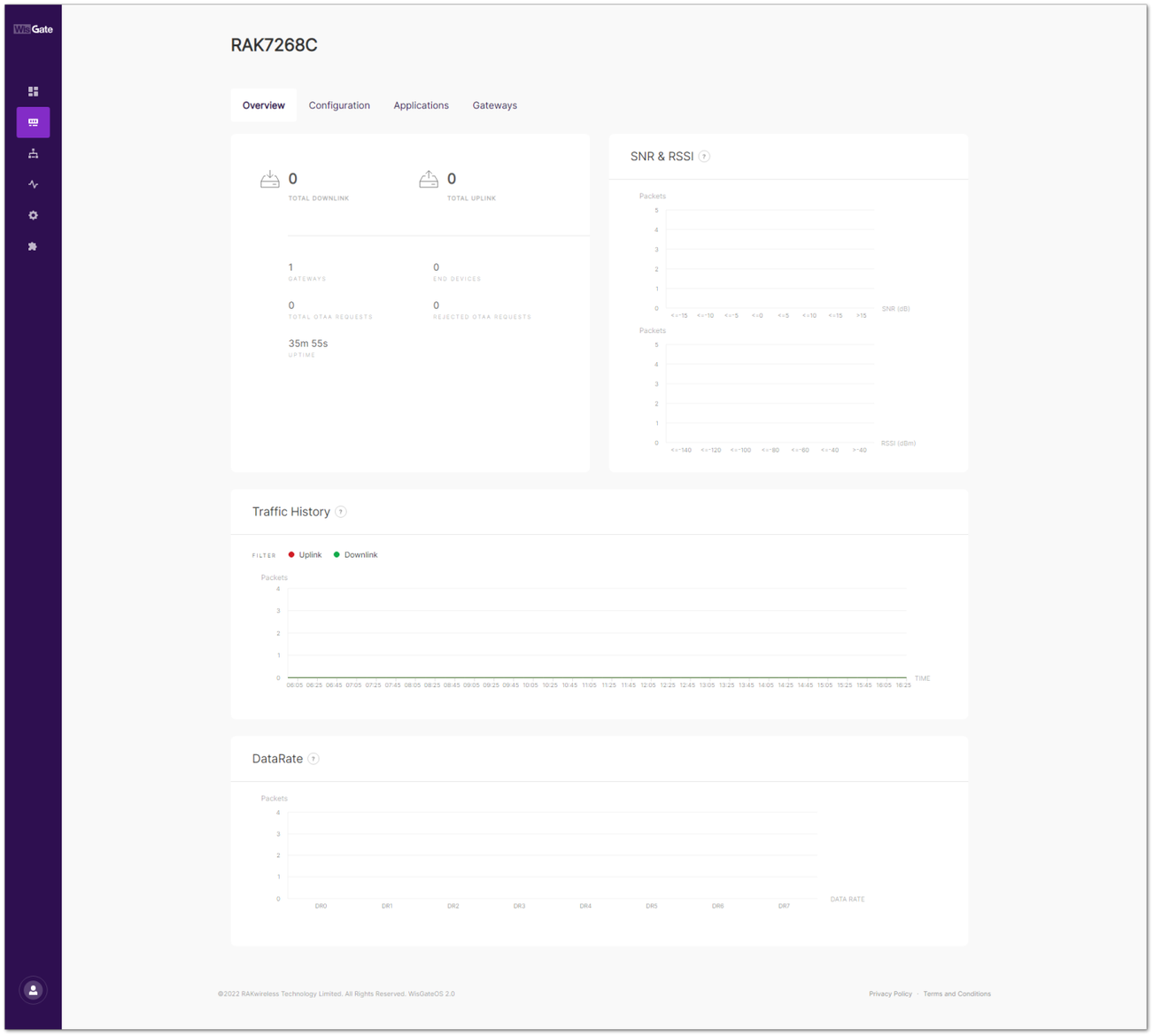

Figure 27: Overview tab

- In the first block, the user can see information about the traffic and the end devices of the central gateway and all extender gateways if any.
  - **Total Downlink** – Total downlink frames transmitted.
  - **Total uplinks** – Total uplink frames transmitted.
  - **Gateways** - The total amount of extender gateways that are forwarding frames to the built-in server plus the central one.
  - **End Devices** - The total amount of end-devices that are currently authenticated with the server.
  - **Total OTAA Requests** - The total authentication requests submitted by end-nodes.
  - **Rejected OTAA Request** - The total authentication requests that were rejected.
  - **Uptime** - The time the built-in server has been working without interruption.
- **SNR & RSSI** - In the SNR & RSSI block, the user can see information about the Signal to Noise Ratio (SNR) and Received Signal Strength Indicator (RSSI) of the packets in a grapf form.
- **Traffic History** - This block shows a general graph of the amount of traffic in packets versus time.
- **DataRate** - In this block, the user can see the number of packets as per Data Rate (DR0 to DR7).

Network

In the Network menu, the user can do changes on the **WAN** (Wide Area Network) and **LAN** (Local Area Network) interfaces. The WAN menu contains the interfaces for communication with the Internet. The LAN menu contains the interfaces for the local networking.

WAN

In the WAN menu, the user can change the priority of the WAN interfaces. If the highest priority interface goes down, the next in line will be used to access the Internet. The red/green light on the left of the WAN interface name shows if that interface is available.

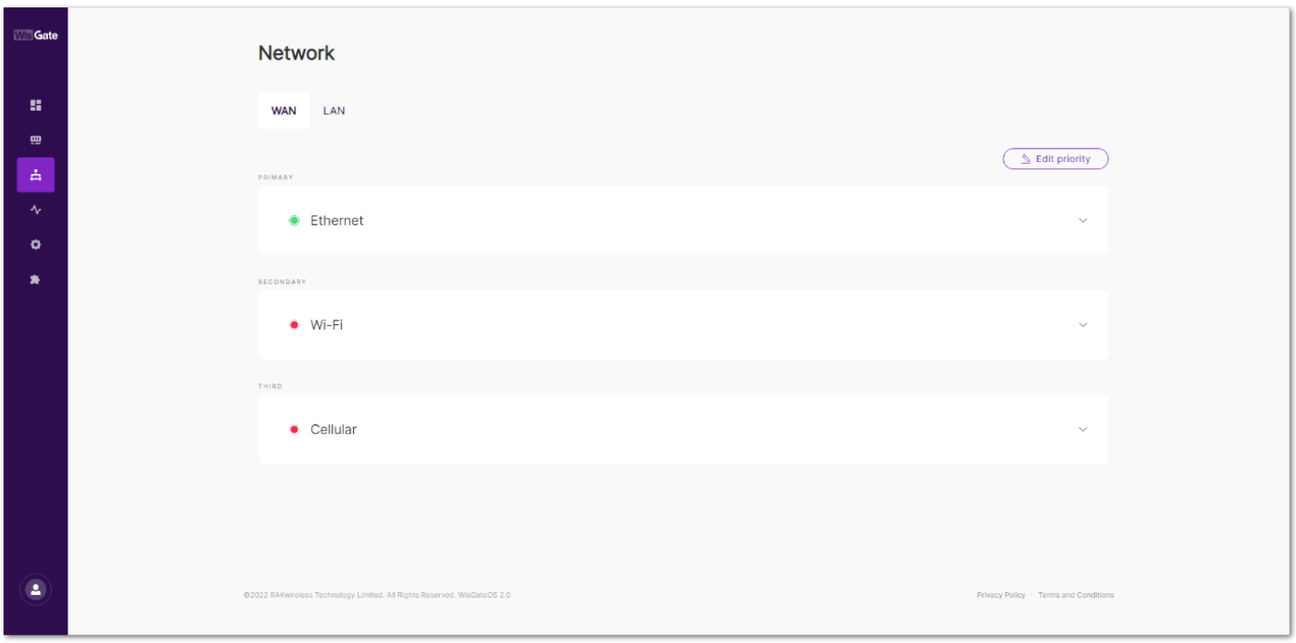

Figure 28: WAN tab

To rearrange the default order click on the **Change priority** button. The priority is changed with the arrows left of the interface name(). The arrow pointing up will increase the priority, and the arrow pointing down – will lower it. To save the changes, you need to click on **Save priorities.**

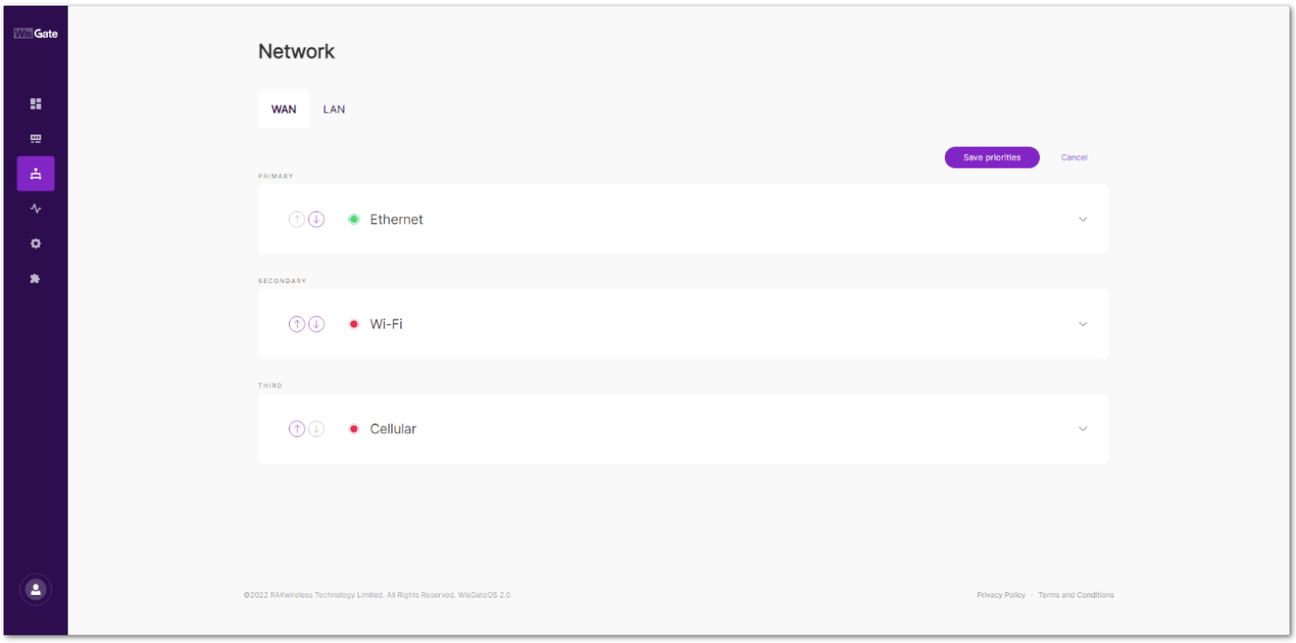

Figure 29: Editing WAN interface's priority

The user can expand each interface window by clicking on the name of the interface or the arrow on the left of the interface (⌄).

- **Ethernet** - The user can see information about the selected interface. There is also a **Settings** button which redirects to the selected interface’s settings.

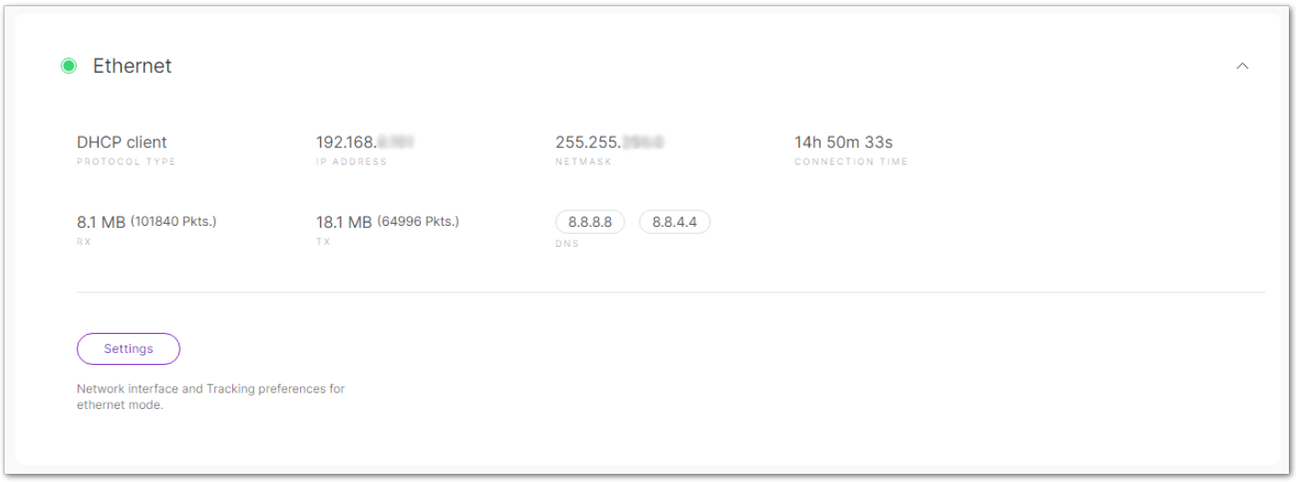

Figure 30: Ethernet

- **Protocol client** – The type of the protocol.
- **IP Address** – The address assigned to the gateway.
- **Netmask** – The netmask of the gateway.
- **Connection time** – The time of the gateway's connection to that interface.
- **RX** – Packets received.
- **TX** – Packets sent.
- **DNS** – DNS server addresses.
- **Ethernet settings General tab**

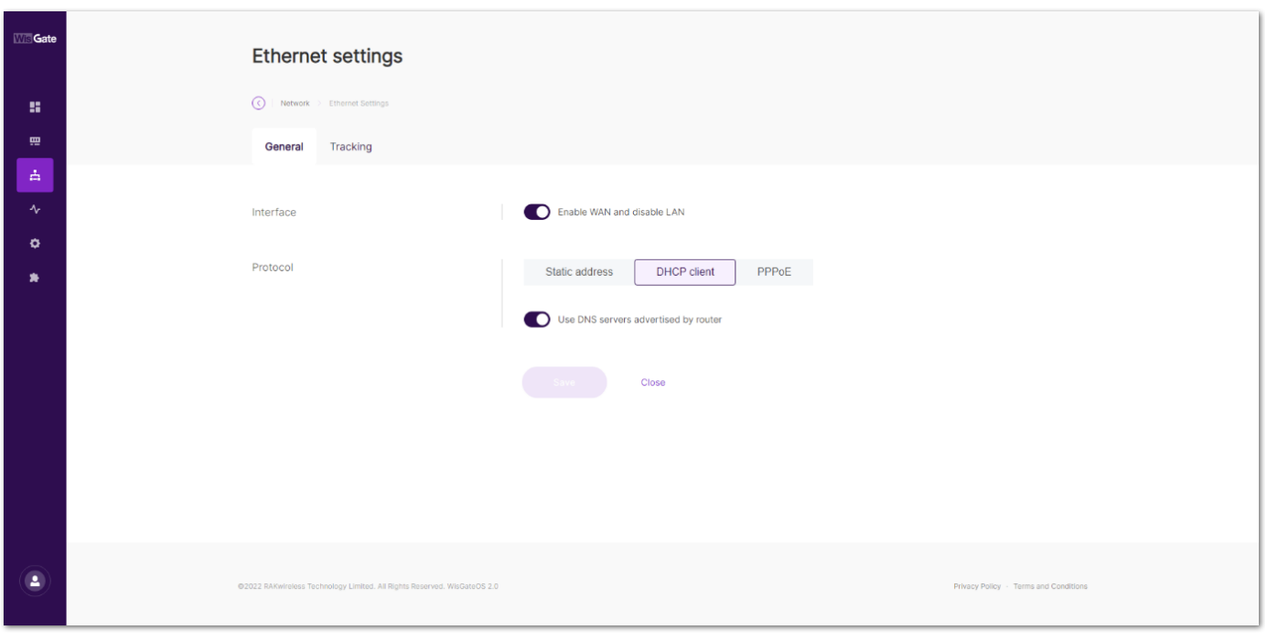

Figure 31: Ethernet settings General tab

- **Interface** - When switched on, this option enables the WAN and disables the LAN interface.
- **Protocol** - The user can choose the type of the protocol. By default, DHCP client is selected.

- **Static address** - The user can set a static address for the gateway.
  - **IPv4 Address** – The desired static address of the gateway in IPv4.
  - **IPv4 Netmask** - The netmask of the gateway in IPv4.
  - **IPv4 Router** – The address of the router in IPv4.
  - **DNS Server** – Custom DNS server address.
- **DHCP client** - The router's DHCP server will assign an IP to the gateway. The **Use DNS server advertised by router** switch allows the gateway to assign DNS address from the router. If the user wants to use custom one, they need to disable it.
- **PPPoE** - The user can set Point-to-Point Protocol over Ethernet, with **username** and **password** provided by the internet provider. The **DNS server advertised by router** switch allows the gateway to assign DNS address from the router. If you want to use custom one, you need to disable it.

- **Ethernet settings Tracking tab** - Here, the user can set up continuous tracking of the interface to automatically switch the gateway to the next available interface when the current interface is no longer stable.

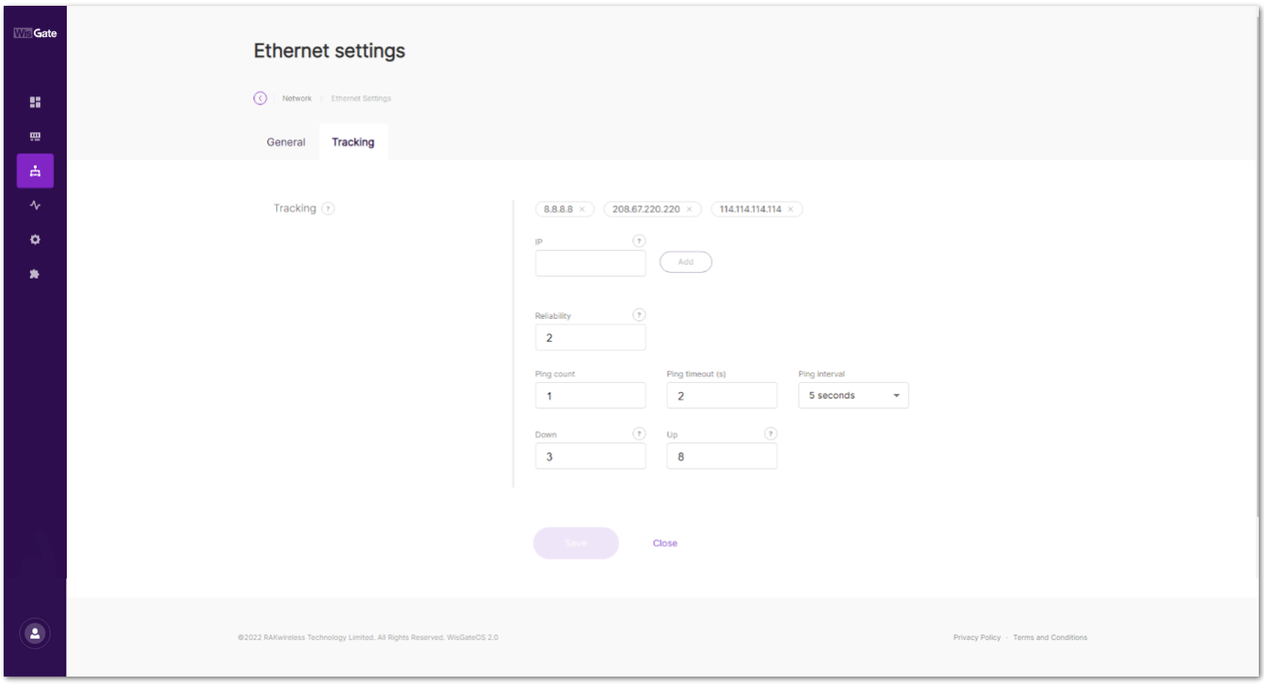

Figure 32: Ethernet settings Tracking tab

  - **IP** – The user can add an IP address to send the ping test.
  - **Reliability** – The added minimum number of IP addresses that must respon to confirm a successful ping test.
  - **Ping count** – Counter of the pings.
  - **Ping timeout (s)** – Timeout of the pings.
  - **Ping interval** – The ping interval.
  - **Down** – The number of the ping test that must fail consecutively to confirm the interface is down.
  - **Up** – The number of the ping test that must fail consecutively to confirm the interface is up.

- **Wi-Fi** - The user can see information about the selected interface. There is also a **Settings** button which redirects to the selected interface's settings.

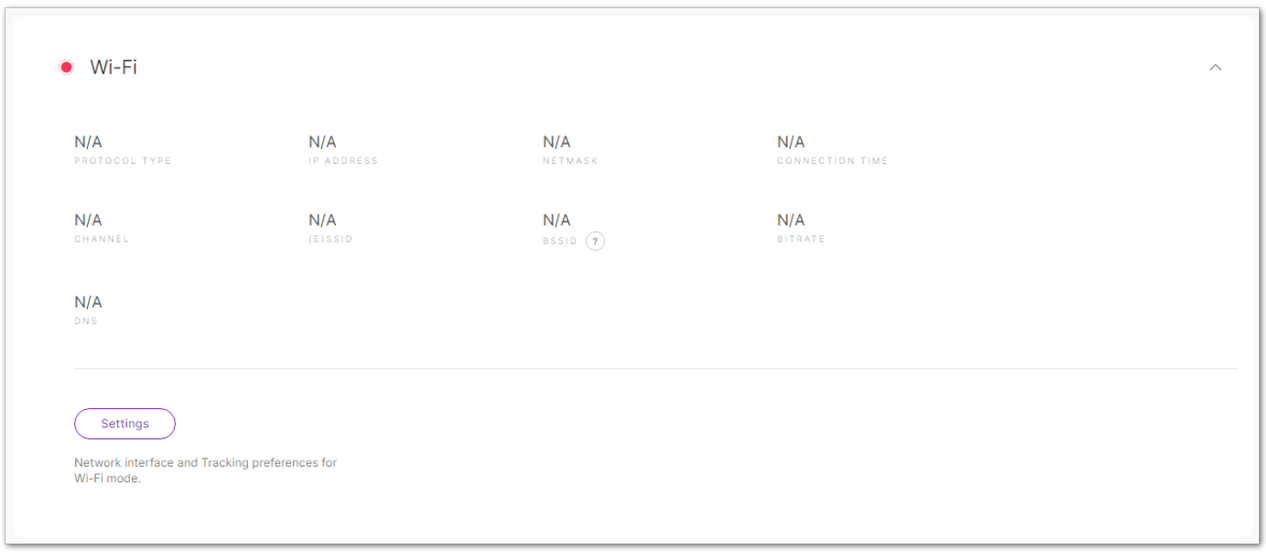

Figure 33: Wi-Fi

- **Protocol Type** – The type of the protocol.
- **IP Address** – The IP assigned to the gateway.
- **Netmask** – The netmask assigned to the gateway.
- **Connection time** – The time the gateway is connected to the Wi-Fi interface.
- **Channel** – This field shows which operating frequency will be used.
- **(E)SSID** – The SSID of the Wi-Fi network.
- **BSSID** – The MAC address of the wireless access point or a router in the wireless network.
- **Bitrate** – The bitrate of the wireless network.

- **Wi-Fi settings General tab** - Here, the user can set a connection to the wireless network.

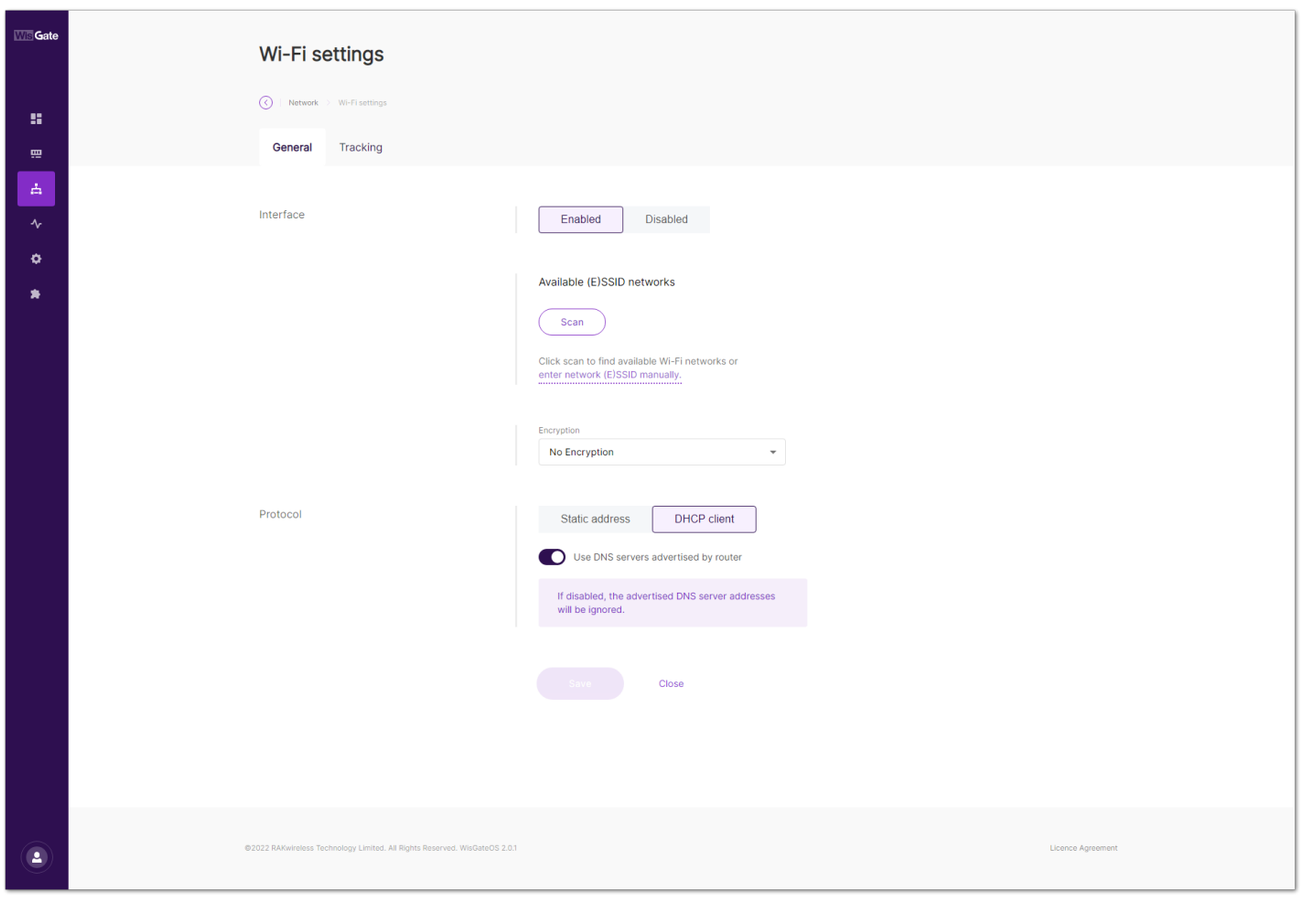

Figure 34: Wi-Fi settings General tab

- **Interface**
  - **Enabled/Disabled** – The user can turn the interface on/off.

  - **Available (E)SSID networks** – The **Scan** button scans for available wireless networks. The user can select the desired network or enter it manually.
  - **Encryption** – The user can choose what encryption the wireless network uses and type in the password in the **Key** field. The options are **No Encryption**, **WPA-PSK, WPA2-PSK**, and **WPA-PSK/WPA2-PSK Mixed Mode** (recommended).

- **Protocol** - The user can set a static IP address for the gateway or let the router's DHCP address to assign one.

  - **Static address** - Here, the user can set a static address for the gateway.
    - **IPv4 Address** – The desired static address of the gateway in IPv4.
    - **IPv4 Netmask** – The netmask of the gateway in IPv4.
    - **IPv4 Router** – The address of the router in IPv4.
    - **DNS Server** – Custom DNS server address.
  - **DHCP client** - The router's DHCP server will assign IP to the gateway.
    - **Use custom DNS server** – When disabled, the DNS server addresses advertised from the router will be ignored.
    - **DNS Server** – The user can add custom DNS.

- **Wi-Fi settings Tracking tab** - Here, the user can set up continuous tracking of the interface to automatically switch the gateway to the next available interface when the current interface is no longer stable.

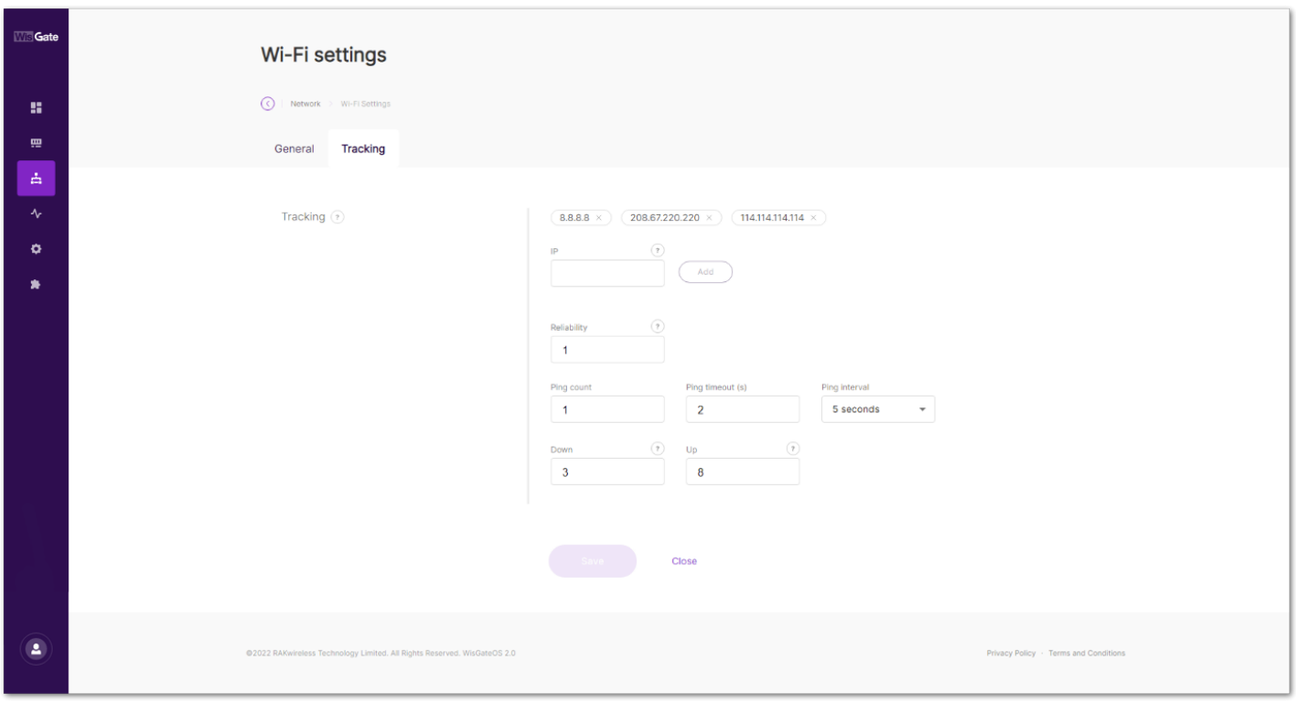

Figure 35: Wi-Fi settings Tracking tab

- **IP** – The user can add IP address to send the ping test.
- **Reliability** – The added minimum number of IP addresses that must respond to confirm a successful ping test.
- **Ping count** – The counter of the pings.
- **Ping timeout (s)** – timeout of the pings.
- **Ping interval** – The ping interval.
- **Down** – The number of the ping test that must fail consecutively to confirm the interface is down.
- **Up** – The number of the ping test that must fail consecutively to confirm the interface is up.
- **Cellular** - The user can see information about the selected interface. There is also a **Settings** button which redirects to the selected interface's settings.

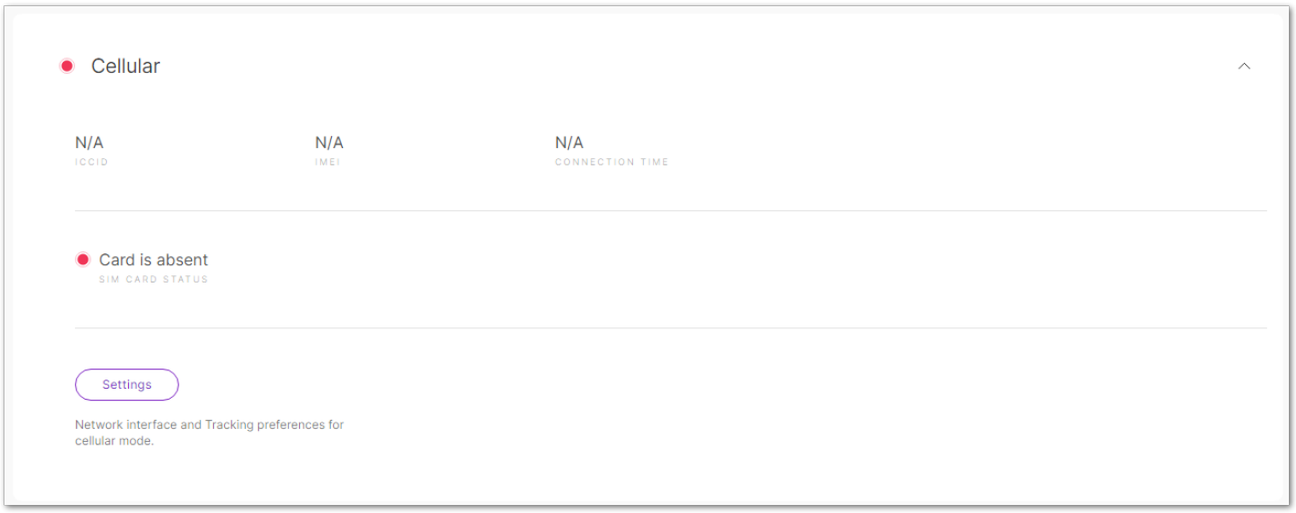

Figure 36: Cellular

- **ICCID** – The Integrated Circuit Card Identifier.
- **IMEI** – The International Mobile Equipment Identity.
- **Connection time** – The time the gateway was connected to the interface.
- **SIM Card Status** – The status of the SIM card.
- **Cellular settings General tab** - Here, the user can set a cellular connection.

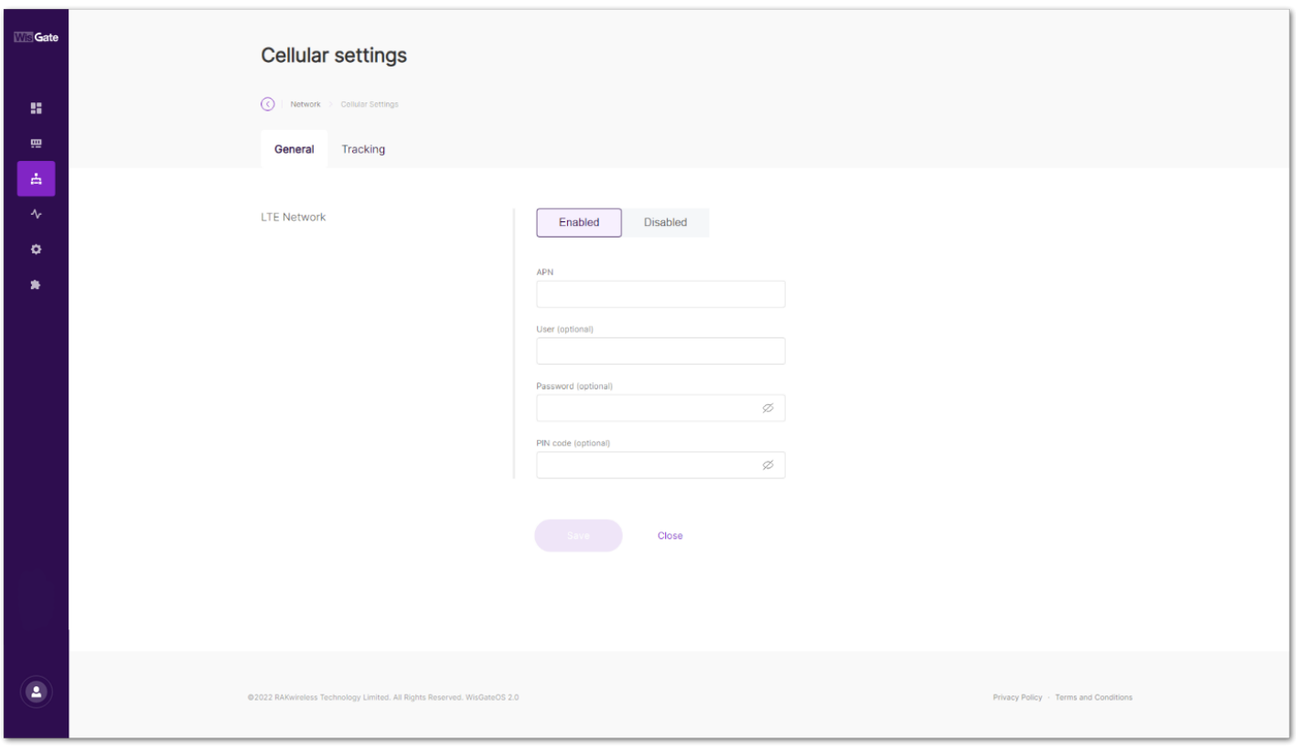

Figure 37: Cellular settings General tab

- **Enable/Disable** – The user can enable/disable the interface.
- **APN** – The Access Point Name.

- **User (optional)** – Username used for authorization (leave empty if there is none).
- **Password (optional)** – Password used for authorization (leave empty if there is none).
- **PIN code (optional)** - The PIN code of the SIM Card (leave empty if there is none).
- **Cellular settings Tracking tab** - Here, the user can set up continuous tracking of the interface to automatically switch the gateway to the next available interface when the current interface is no longer stable.

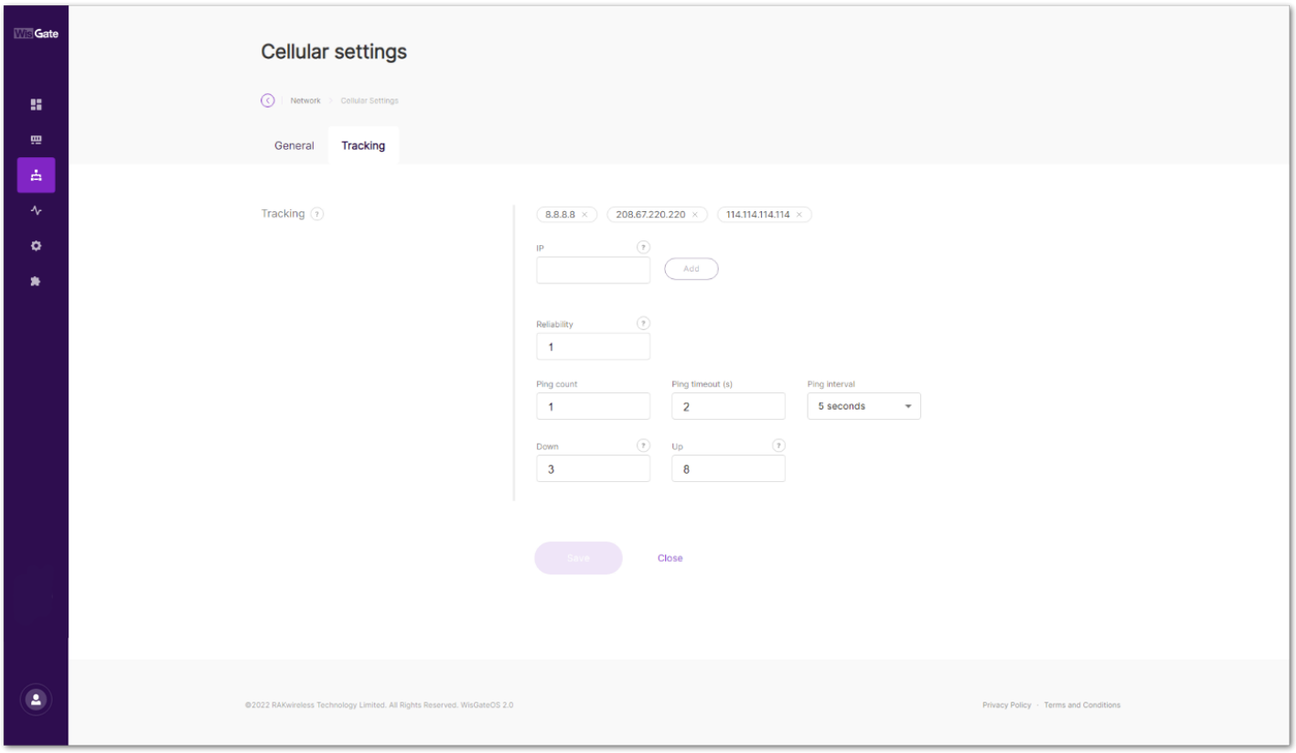

Figure 38: Cellular settings Tracking tab

- **IP** – The user can add IP address to send the ping test.
- **Reliability** – The added minimum number of IP addresses that must respond to confirm a successful ping test.
- **Ping count** – Counter of the pings.
- **Ping timeout (s)** – Timeout of the pings.
- **Ping interval** – The ping interval.
- **Down** – The number of the ping test that must fail consecutively to confirm the interface is down.
- **Up** – The number of the ping test that must fail consecutively to confirm the interface is up.

LAN

In the LAN tab, the user can see and edit information about the Local Area Network.

The red/green light on the left shows if the interface is enabled/disabled. You can expand each LAN interface window, by clicking on its name or the arrow on the right (⌄) of the interface.

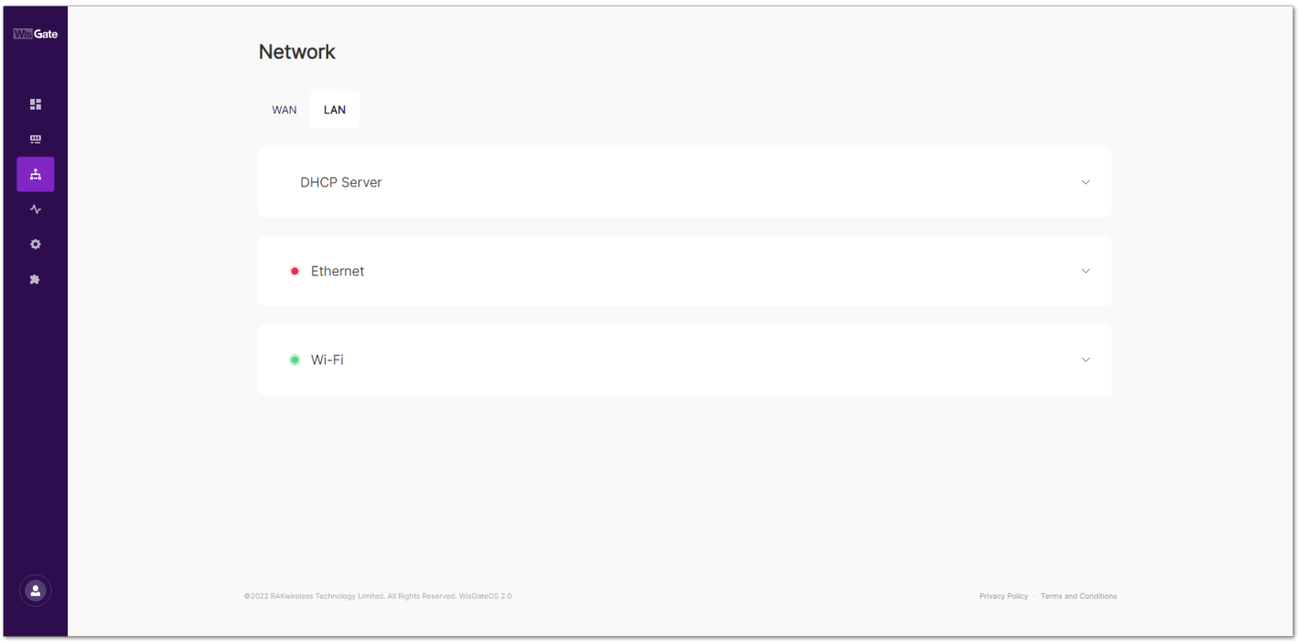

Figure 39: LAN tab

- **DHCP Server**

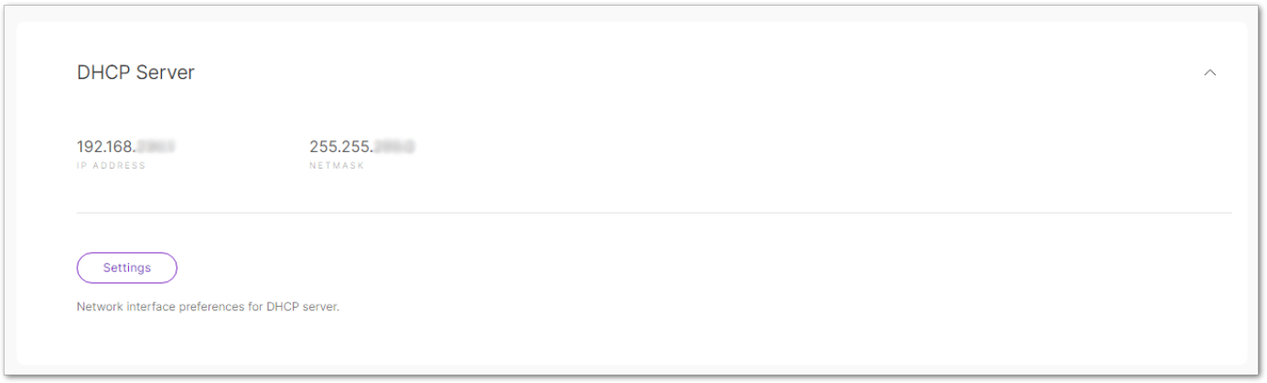

Figure 40: DHCP Server

  - **IP Address** – The IP address of the gateway DHCP server.
  - **Netmask** – The netmask of the DHCP server of the server.
  - The **Settings** button redirects you to the LAN DHCP settings.

- **DHCP Settings** - Here, the user can change the **IPv4 address** of the LAN DHCP server.

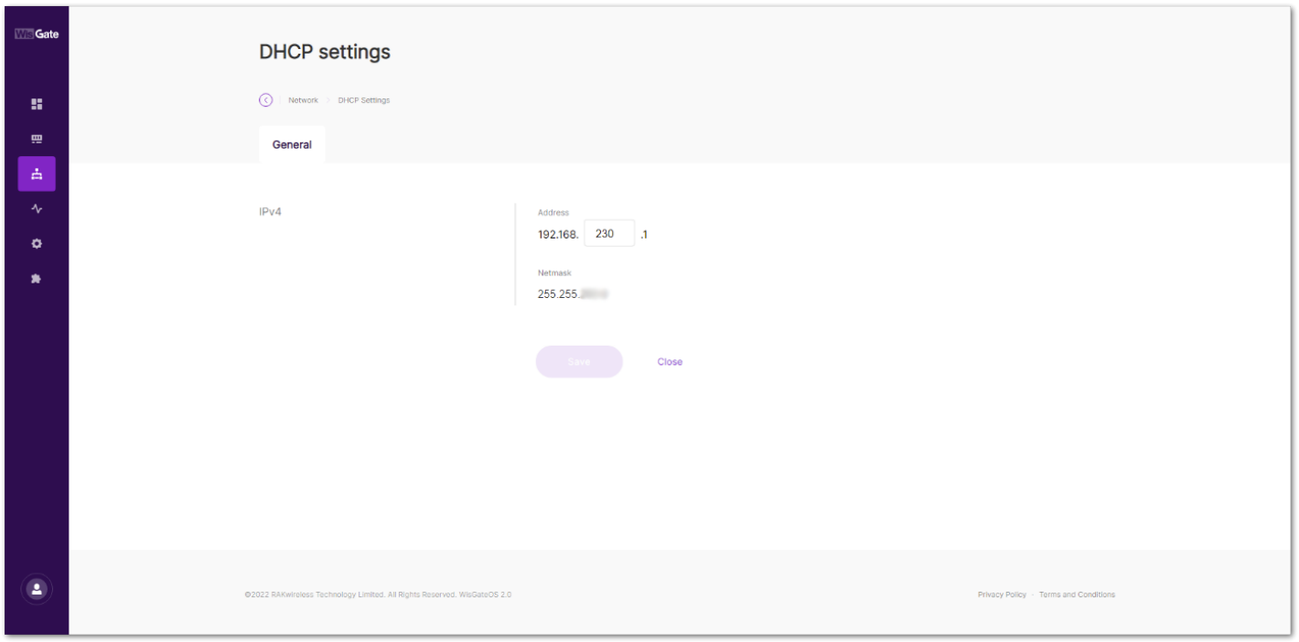

Figure 41: DHCP Settings

- **Ethernet** - The field only shows if the interface is active. The **Settings** button redirects you to the LAN Ethernet settings.

Figure 42: Ethernet

- **Ethernet settings** - Here, the user can enable the LAN Ethernet interface and disable the WAN Ethernet interface.

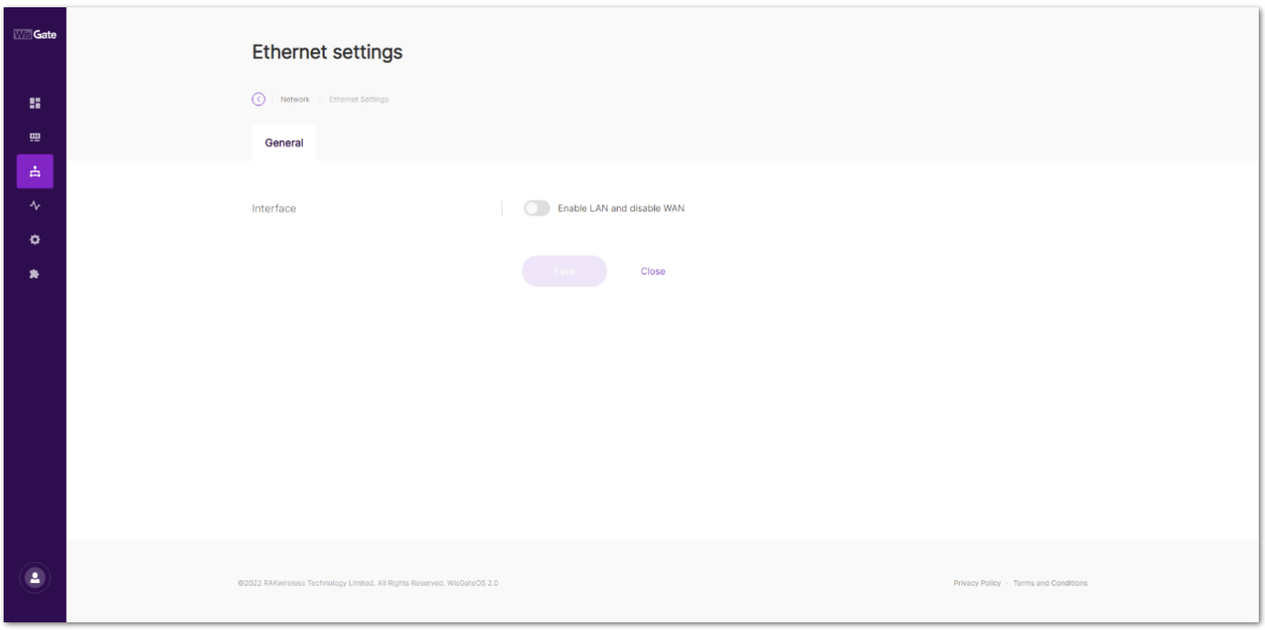

Figure 43: Ethernet settings

- **Wi-Fi**

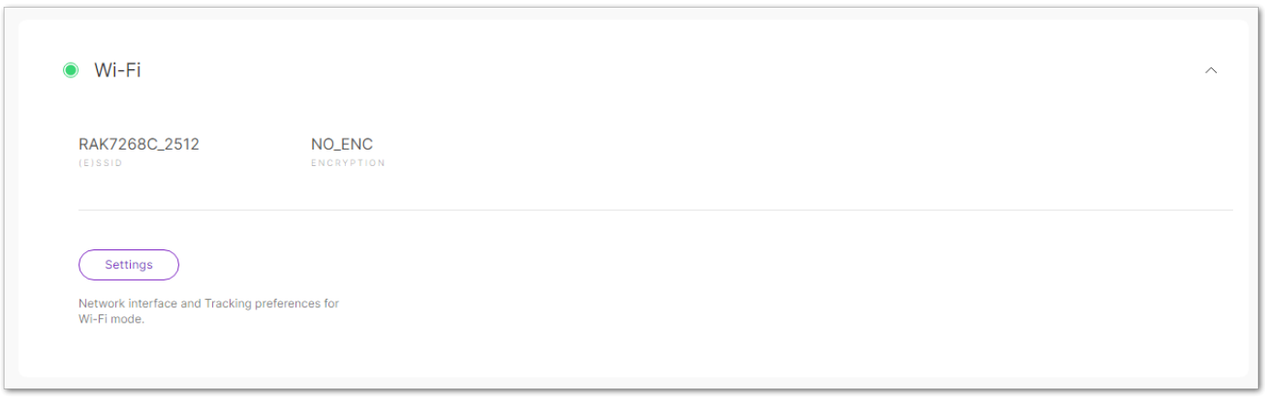

Figure 44: Wi-Fi

  - **(E)SSID –** SSID of the Access Point (AP) of the gateway.
  - **Encryption** – Encryption of the AP.
  - The **Settings** button redirects you to the LAN Wi-Fi settings.

- **Wi-Fi settings** - Here, the user can manage the LAN Wi-Fi settings.

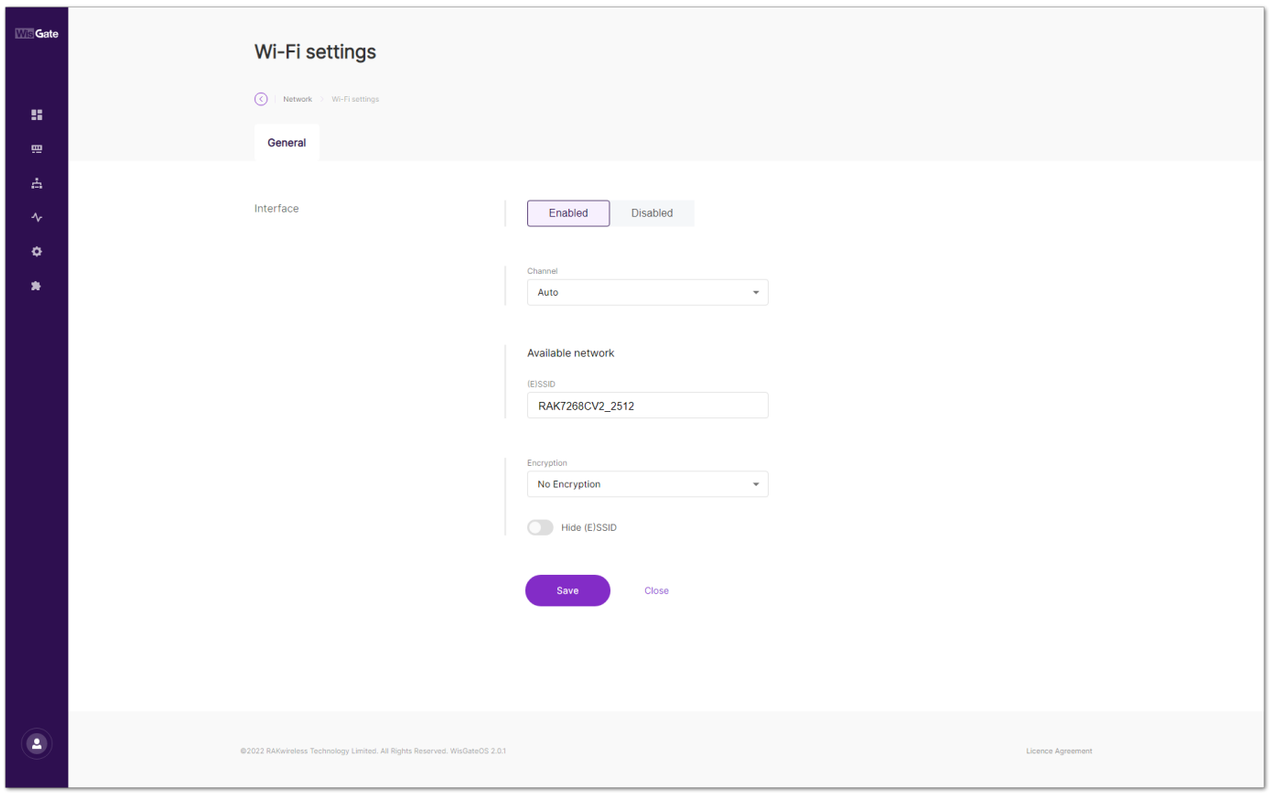

Figure 45: Wi-Fi settings

- **Enabled/Disabled** – Enables/disables the LAN Wi-Fi interface.
- **Channel** – The user can set a channel for the Wi-Fi. Default is **Auto**, the gateway will automatically choose a channel.
- **(E)SSID** – The name of the AP.
- **Encryption** – The user can set an encryption of the AP with a password written in the **Key** field. The options are **No Encryption**, **WPA-PSK**, **WPA2-PSK**, and **WPA-PSK/WPA-PSK2 Mixed Mode** (recommended).
- **Hidden** – The user can hide the AP.

Diagnostics

In the **Diagnostics** menu, the user can review the logs on the gateway and perform checks.

System log

On this page, the user can see the complete system logs. It is mainly used for debugging purposes. The System Log reports both system information and actual data from LoRa frames coming from the end nodes.

At the top right corner there is the **Auto Refresh** button. Depending on the state (ON or OFF) the auto-refresh will be enabled or disabled.

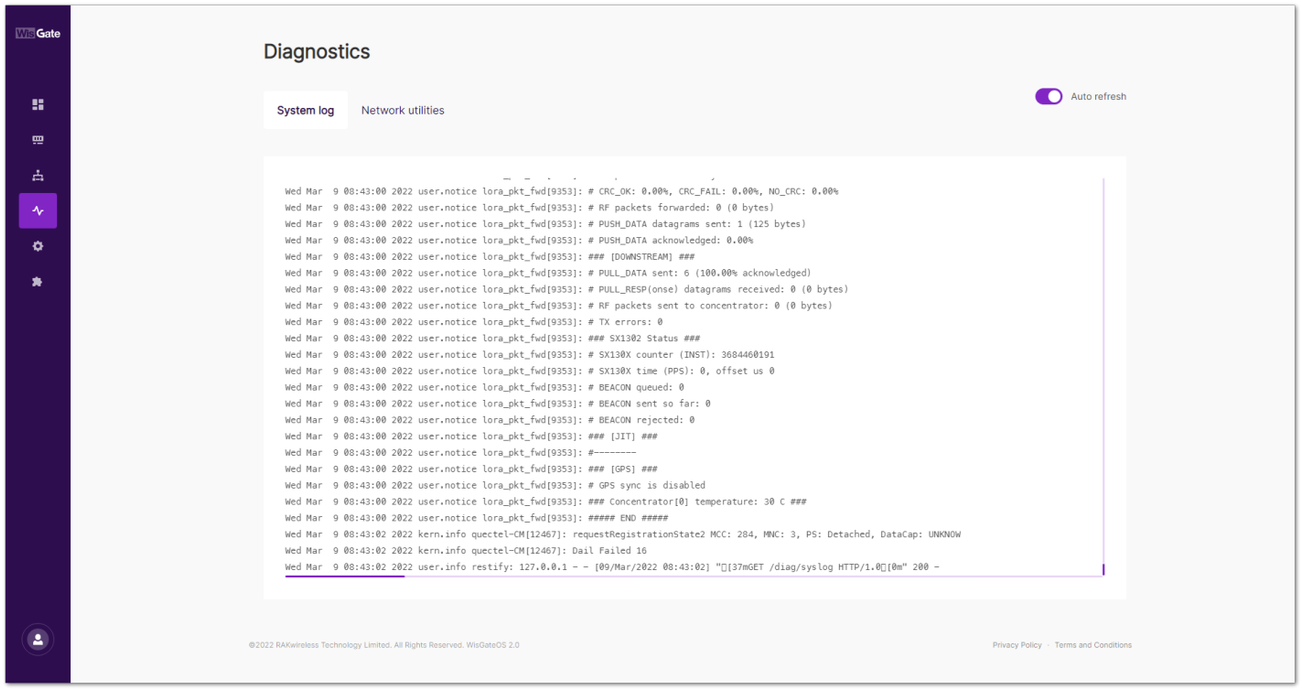

Figure 46: System log tab

Network utilities

This is where the user can perform checks via the built-in tools: **Ping**, **Trace**, **Nslookup**. The user can either enter an URL or an IP Address in the text box and execute the command with one of the buttons. The results are conveniently displayed in a CLI box.

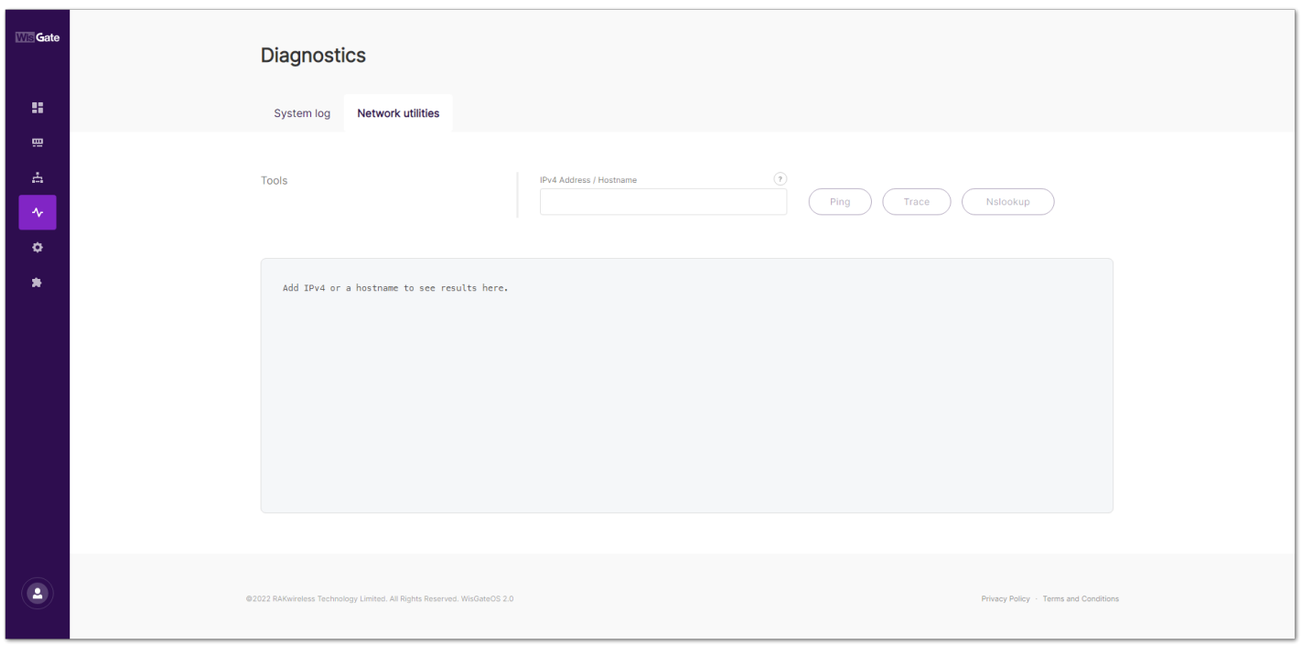

Figure 47: Network utilities tab

Settings

General settings

In this tab, the user can change the name of the gateway, setup a system log server or reboot the device.

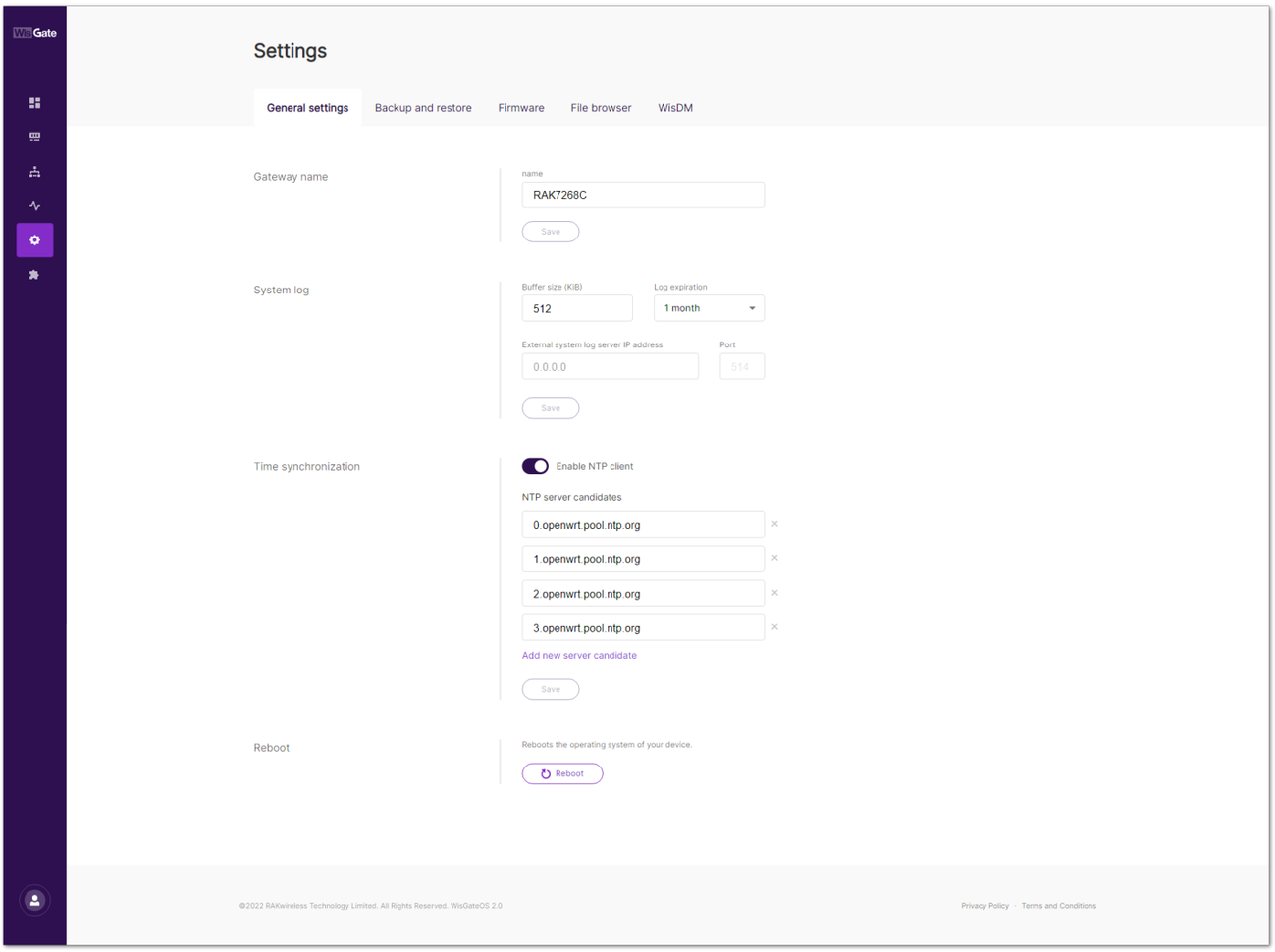

Figure 48: General settings tab

- **Gateway name** – The user can change the default name of the gateway by typing the desired name in the **Name** field and clicking the **Save** button.
- **System log** – The user can point the gateway to a system log server where they can save logs.
  - **Buffer size (KiB)** – This is the maximum size of the log file to be saved.
  - **Log expiration** – How long does it take for the log file to be saved.
  - **External system log server IP address** – The address of the external system log server.
  - **Port** – corresponding port of the system log server.
- **Time synchronization** - The switch enables/disables the time synchronization from a Network Time Protocol (NTP) server. In the **NTP server candidates** area, the user can add or remove NTP candidates. To add a new candidate, the user needs to click on the **Add new server candidate** text. A new field pops up, where the user needs to fill the server candidate.
- **Reboot** – Here you can reboot the gateway. All unsaved changes will be discarded.

Backup and restore

In this tab, the user can backup, restore or reset the gateway's settings.

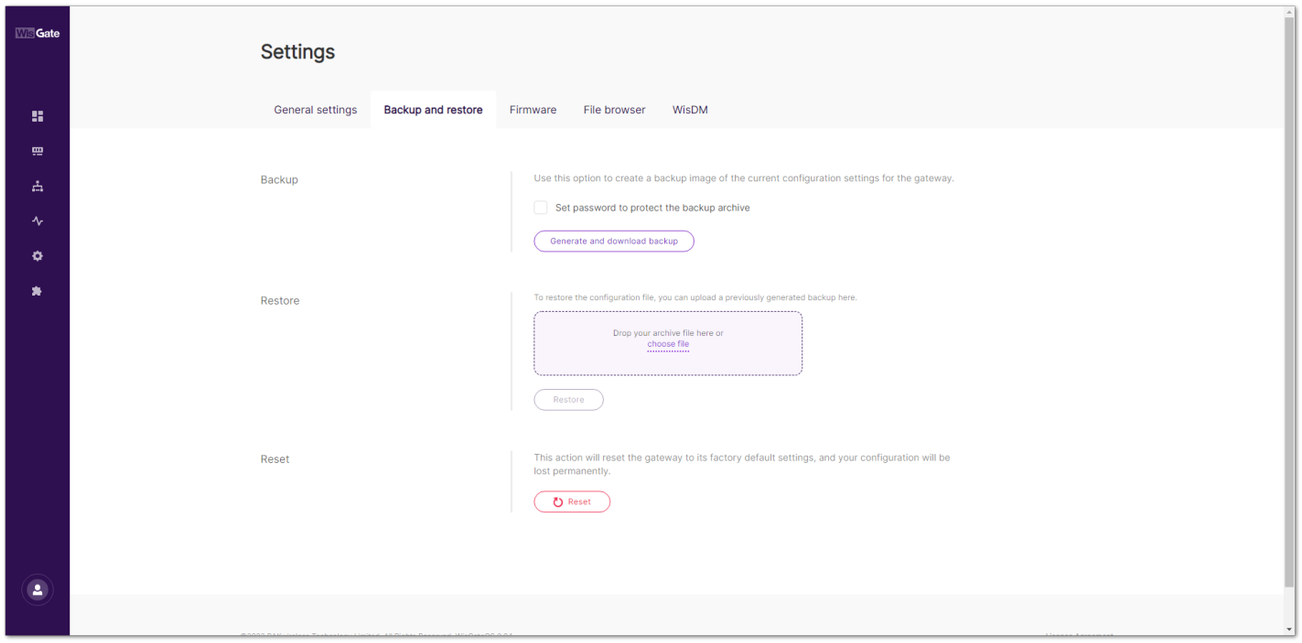

Figure 49: Backup and restore tab

- **Backup** – The **Generate and download backup** button creates and downloads an archive file with all current settings.
- **Restore** – Here, the user can upload an archive file by clicking **choose file** or drag-and-dropping it in the area and restore the previous settings.
- **Reset** – With the **Reset** button, the user can restore the factory settings.

Firmware

In this tab, the user can see the current version of the firmware and update it.

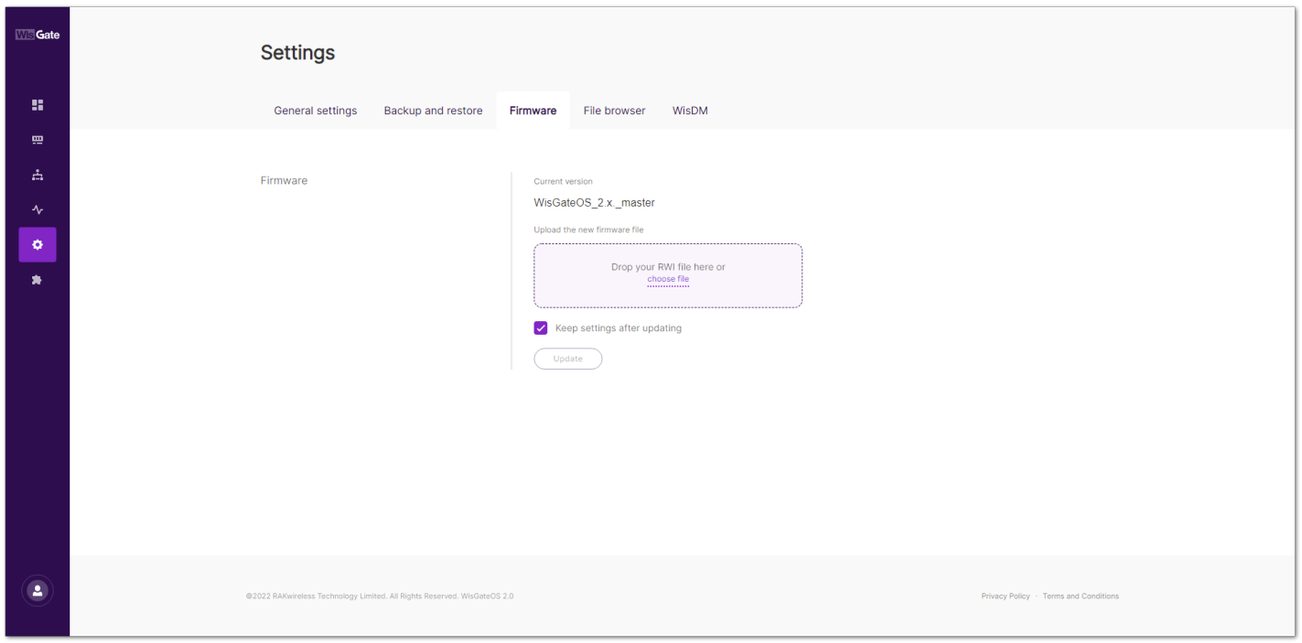

Figure 50: Firmware tab

To update the firmware, the user needs to flash a **RWI** file. This is done by using the **choose file** button to select the location of the new firmware file and the **Update** button to initiate the flashing process. There is a tick box to toggle the option of keeping the current settings of the gateway.

> 📝 **NOTE**
>
> The **Keep settings after updating** check box is selected by default, as unchecking it will results in having a gateway with stock settings after the firmware update.

When the **Enable FOTA** option from the **WisDM tab** is active, the user will not be able to update the firmware, as it is done via WisDM.

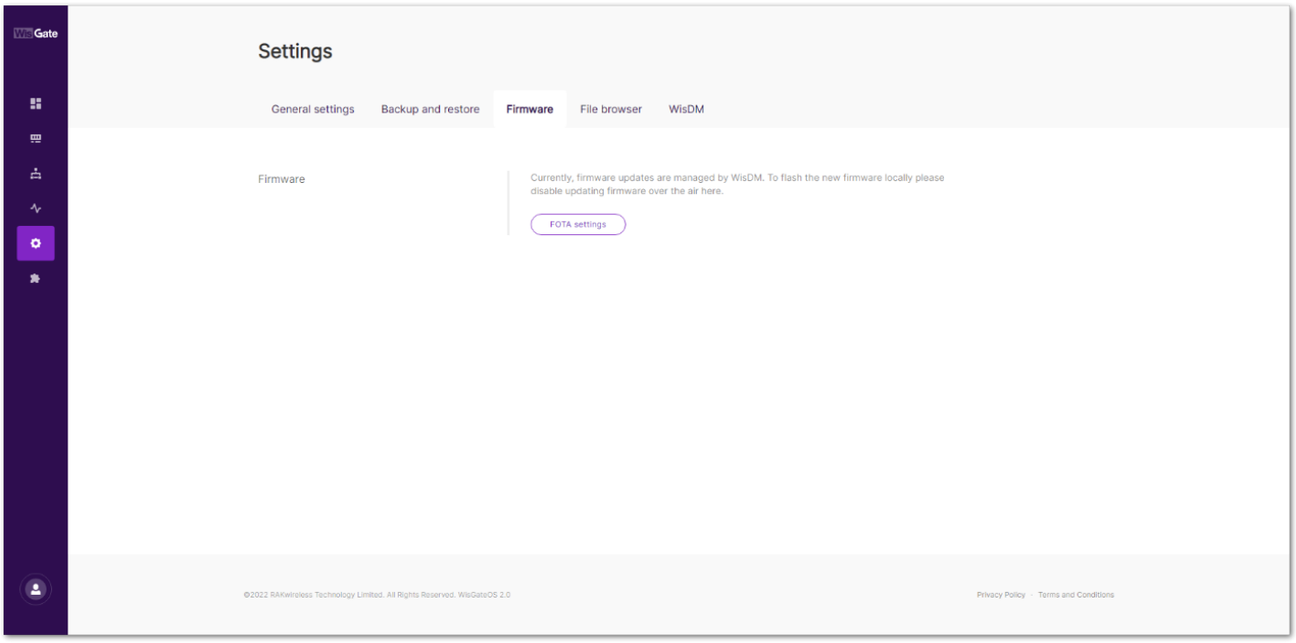

Figure 51: Firmware tab inactive

File browser

Through the **File browser** tab, the user can access the files in the **root** partition. System logs are saved there and can be downloaded from here.

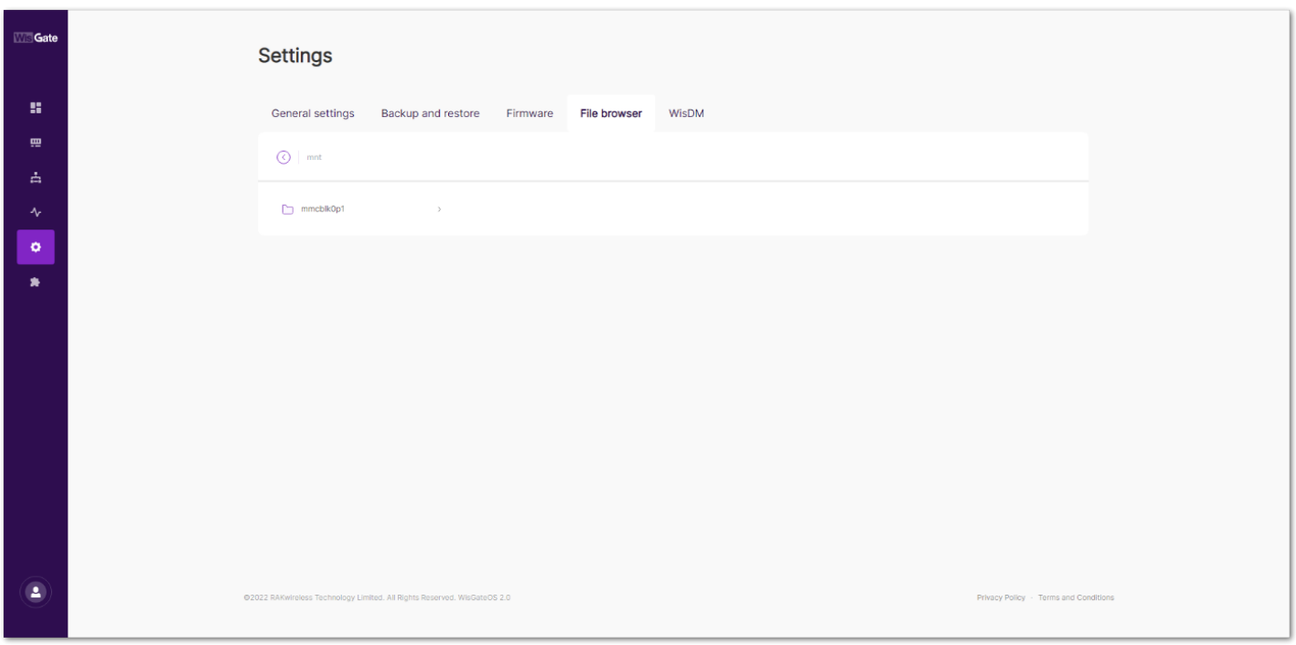

Figure 52: File browser tab

WisDM

Here, the user can enable/disable WisDM integration and FOTA (Firmware over the air).

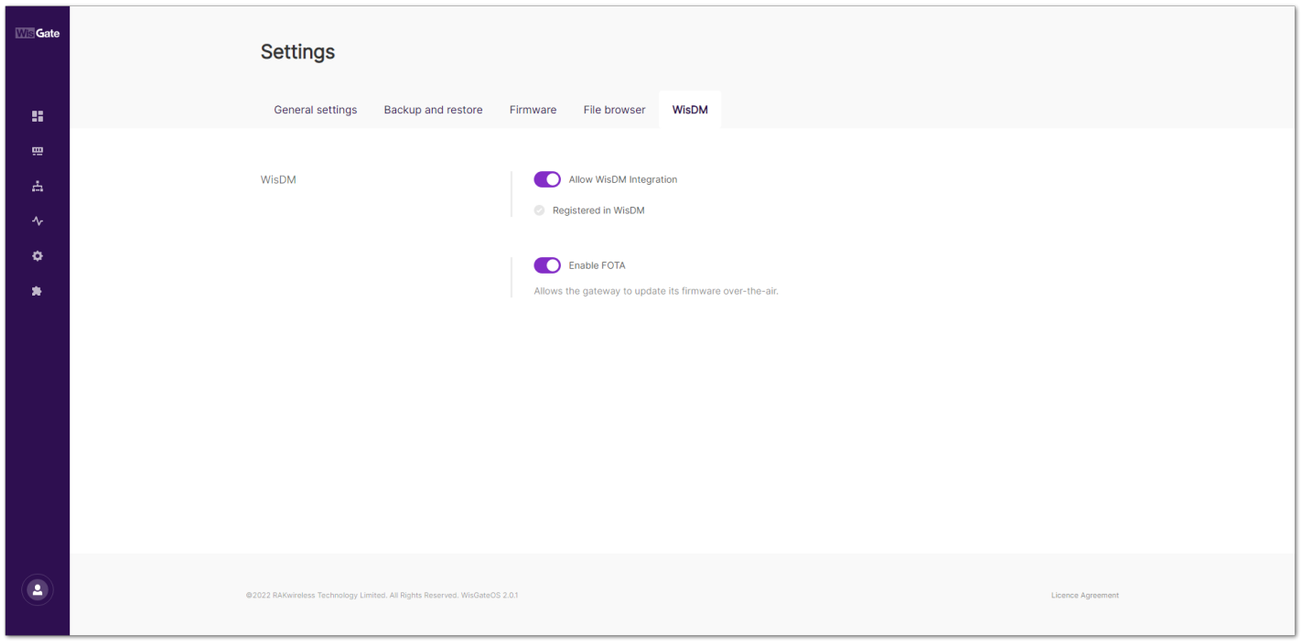

Figure 53: WisDM tab

- **Allow WisDM Integration** – Enables the WisDM. The gateway can be managed via the WisDM Platform .
- **Enable FOTA** - When enabled, the gateway can be upgraded to a newer firmware version via the WisDM platform. If you want to upgrade the firmware via the Web UI, this function must be disabled.

Extensions

Here, the user can install extensions to the gateway via drag-and-drop of an existing IPK file, the **Add new extension** button or **install one now** link.

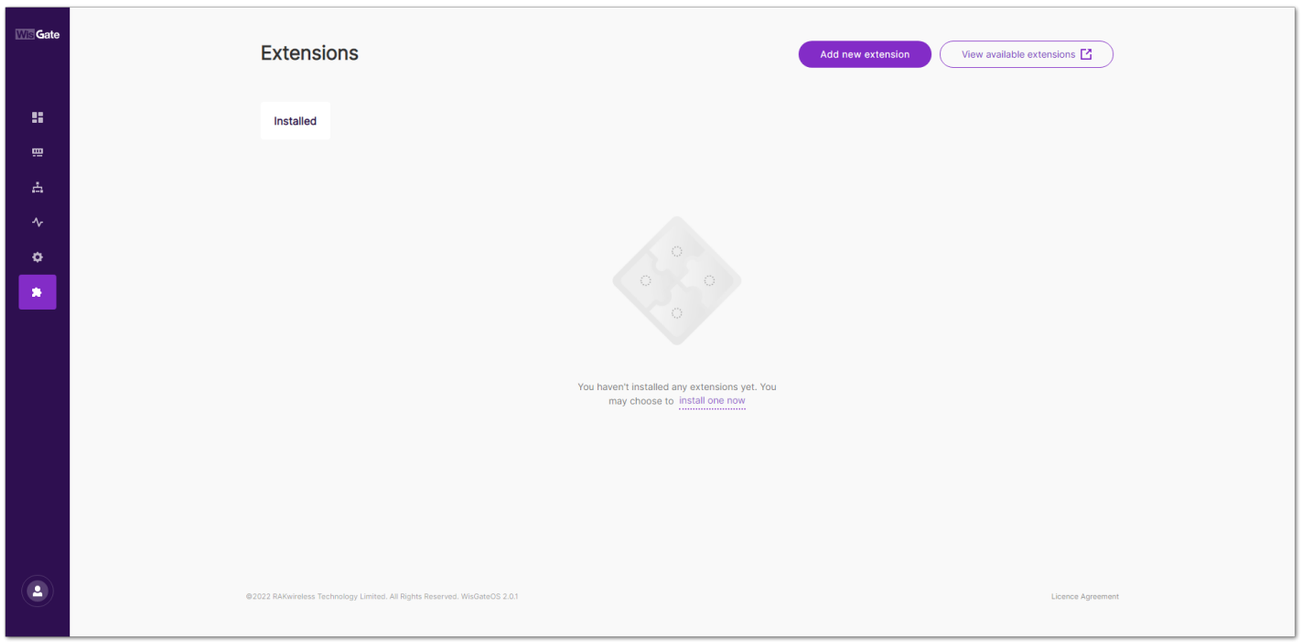

Figure 54: Extension

User preferences

In the bottom left corner, the user can logout from the Web UI or choose User preferences.

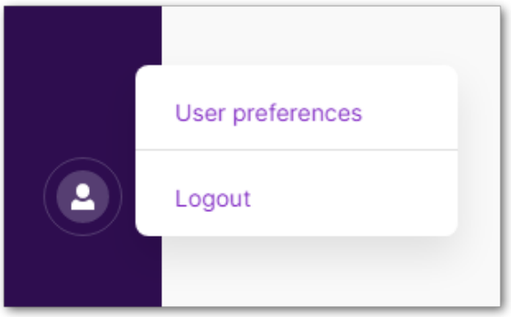

Figure 55: User button

Choosing the **User preferences** option will redirect the user to the corresponding page.

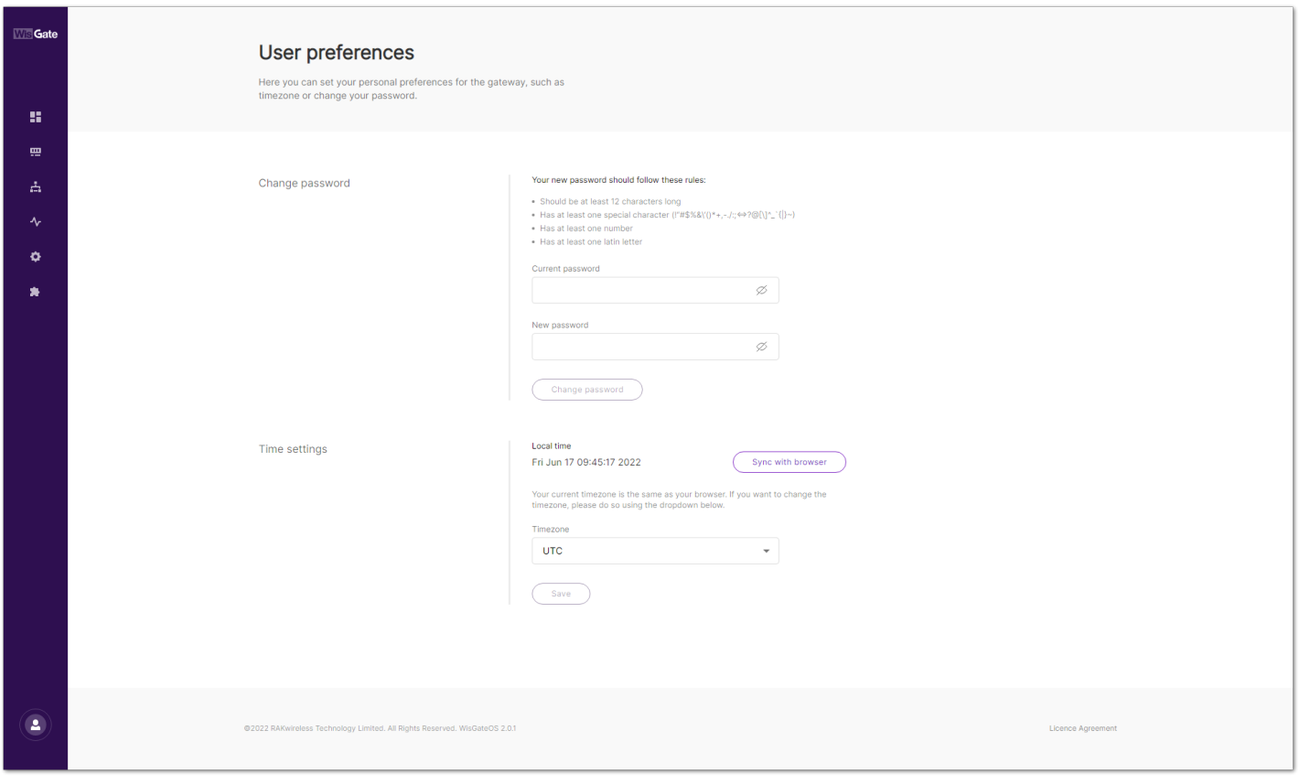

Figure 56: User preferences

- **Change password** – Here, the user can change the password for access for the Web UI.
- **Time settings** – Here, the user can set local time to the gateway.

Last Updated: 9/29/2022, 2:03:34 PM