Ultra Low Power Solar LoRaWAN® Gateway

SG50

User Guide

Safety Precautions

Milesight will not shoulder responsibility for any loss or damage resulting from not following the instructions of this operating guide.

- The device must not be disassembled or remodeled in any way.
- Do not place the device close to objects with naked flames.
- Do not place the device where the temperature is below/above the operating range.
- Do not power on the device or connect it to other electrical device when installing.
- Check lightning and water protection when used outdoors.
- Do not connect or power the equipment using cables that have been damaged.

Declaration of Conformity

SG50 is in conformity with the essential requirements and other relevant provisions of the CE, FCC, and RoHS.

Copyright © 2011-2025 Milesight. All rights reserved.

All information in this guide is protected by copyright law. Whereby, no organization or individual shall copy or reproduce the whole or part of this user guide by any means without written authorization from Xiamen Milesight IoT Co., Ltd.

For assistance, please contact

Milesight technical support:

Email: iot.support@milesight.com

Support Portal: support.milesight-iot.com

Tel: 86-592-5085280

Fax: 86-592-5023065

Address: Building C09, Software Park Phase III, Xiamen 361024, China

Revision History

Date	Doc Version	Description
Oct. 15, 2023	V 1.0	Initial version
Jan. 15, 2024	V 1.1	1. Support connecting to Milesight gateway embedded network server; 2. Support to connect to Milesight Development platform and DeviceHub V2.
April 3, 2025	V 1.2	1. Add embedded network server. 2. Compatible with ChirpStack v4 packet forwarder. 3. Add data retransmission for packet forwarder. 4. Add scheduled reboot, ping tool and hostname configuration. 5. Add protocol parameter to cellular configuration. 6. Add Proprietary Message filter. 7. Add sleep mode. 8. Add weather protection and lightning protection.
Aug. 4, 2025	V 1.2.1	1. Add syncing time with the browser. 2. Add gateway info to report via MQTT. 3. Add solar panel maintenance note.
Sept. 22, 2025	V 1.3	1. Add HTTPS access feature. 2. Add OpenVPN client feature. 3. Add password change prompt upon first login.

Contents

1. Product Introduction

1.1 Overview

SG50 is an energy-efficient solar LoRaWAN® gateway designed for outdoor environments with limited power availability and ample solar energy resources. With built-in batteries and accessorial solar panel, SG50 can work independently in various scenarios, especially the places with hard access to power resources.

Besides the high adaptability, SG50 is highly compatible with mainstream network servers and supports remote management via remote network servers which provides both convenience and secured management.

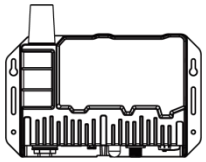
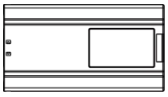
Benefiting from its robust structural design and high IP67 protection rate, SG50 can work smoothly in harsh environments. It is specifically tailored for applications such as oil and gas, mining, forestry, and remote industries where power consumption must be carefully managed.

1.2 Key Features

- IP67 enclosure and robust structural design promote its strength and working lifespan
- Equip with SX1302 chip, handling a higher amount of traffic with lower consumption
- Support 8 channels for more than 2000 end-nodes connections
- Equip with GPS for simple remote management and deployment
- Fast deployment with the all-in-one design and standard accessories
- Built-in rechargeable batteries & accessorial solar panel for wireless usage
- Support cellular for backhaul network enabling independent networking
- Compatible with mainstream network servers like The Things Stack, ChirpStack, etc.
- Built-in network server and MQTT API for easily integration
- Equip with high-efficient power management design prolonging its battery life up to 4 days
- Compatible with remote management system for simple deployment even in remote regions

2. Hardware Introduction

2.1 Packing List

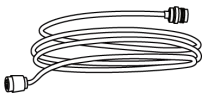



1 × SG50 Device

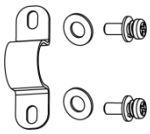
1 × Battery Pack

1 × SIM Card Ejector Tool

1 × LoRaWAN® Antenna (60 cm)

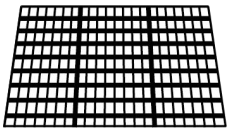


1 × Antenna Coaxial Cable (1m)

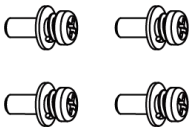


1 × Antenna U-strap Kit

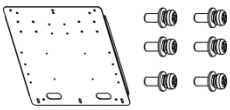
1 × Antenna U-bolt Kit



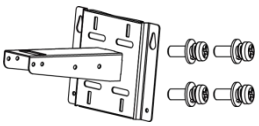
1 × Solar Panel (with 50cm M12 Power Cable)



4 × Mounting Screws

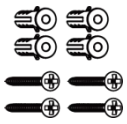


1 × Solar Panel Bracket Kit



1 × Mounting Bracket Kit

2 × Hose Clamps (⌀ 67-127mm)



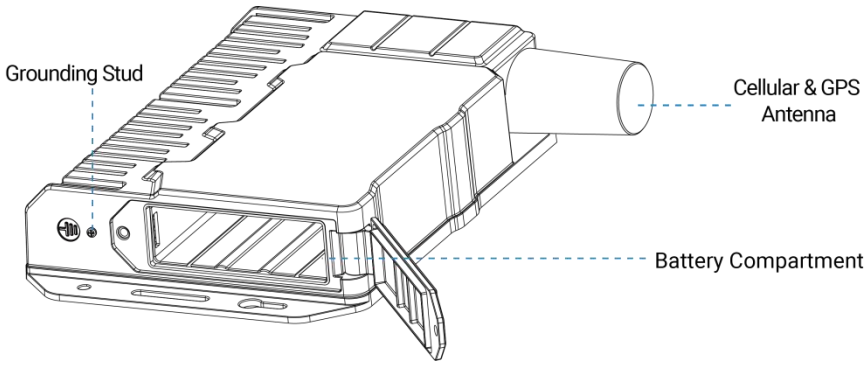
4 × Wall Mount Screw Kits

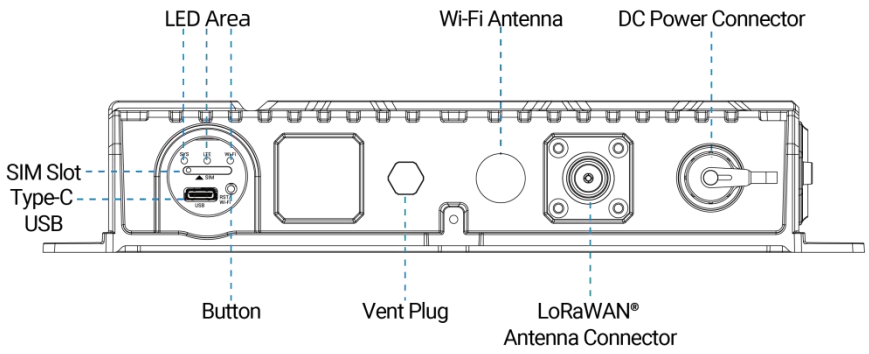
1 × Quick Guide

1 × Warranty Card

If any of the above items is missing or damaged, please contact your sales representative.

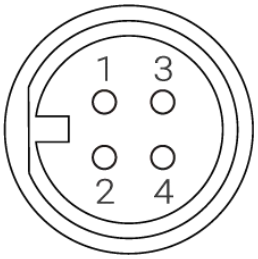
2.2 Hardware Overview





DC Power Connector

Pin	Description	
1	DC-	DC 12-24V
2	DC+	
3	Connect/disconnect the pins together to power on/off the device.	
4		



2.3 Button and LED Indicator

LED Indicators

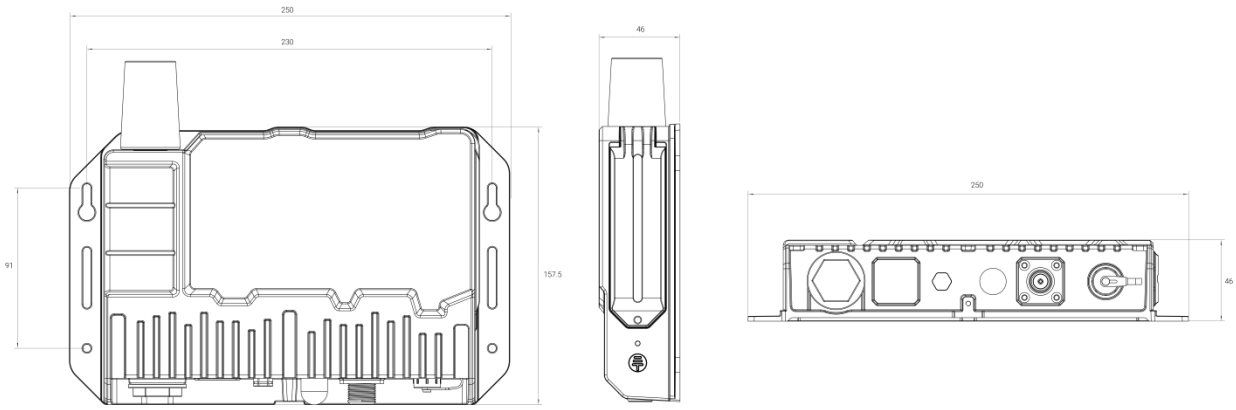
LED	Indication	Status	Description
SYS	Power & System Status	Off	The power is off or in sleep mode
		Green Light	The system is running properly
		Red Light	The system goes wrong
LTE	Cellular Status	Off	SIM card is registering or failed to register (or there are no SIM cards inserted)
		Green Light	Blinking slowly: SIM card has been registered and is ready for dial-up
			Blinking rapidly: SIM card has been registered and is dialing up now
			Static: SIM card has been registered and dialed up successfully
Wi-Fi	Wi-Fi Status	Off	Wi-Fi is off
		Green Light	Blinking slowly: Wi-Fi is starting
			Static: Wi-Fi is on

Wi-Fi/Reset Button

Function	Action	LED Indication
Turn On Wi-Fi	When Wi-Fi is disabled, quickly press the button once to turn on Wi-Fi for 10 minutes.	Wi-Fi: Off → On

Turn Off Wi-Fi	When Wi-Fi is enabled, quickly press the button once to turn off Wi-Fi for 10 minutes.	Wi-Fi: On → Off
Enter Sleep Mode	When the sleep mode is enabled and the gateway detects not enough solar power.	SYS: blinks rapidly → Off
Wake up	Under sleep mode, quickly press the button once to wake up for 10 minutes.	SYS: Off → On
Reset to Factory Default	Press and hold the button for more than 5 seconds	SYS: blinks rapidly.

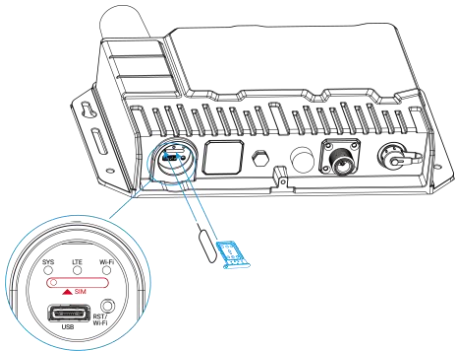
2.4 Dimensions (mm)



3. Hardware Installation

3.1 SIM Card Installation

1. Take the SIM cover down, and use an ejector tool to open the SIM card tray. Insert the nano (4FF) SIM card, then put the slot with the SIM card back into the device.
2. Rotate back the cover and tighten it with a wrench to prevent water from entering the device (Tightening Torque: 0.7 N.m).

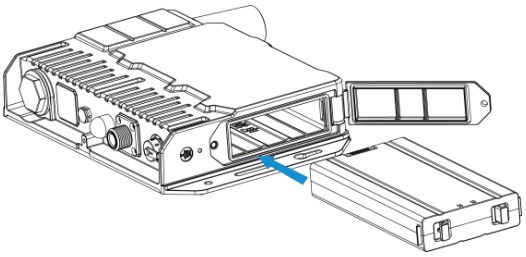


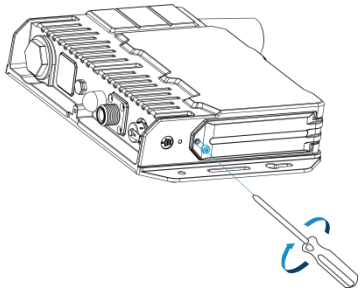
3.2 Power Supply

SG50 can be powered by either a 12-24 VDC external supply or a solar panel. In the meantime, the internal battery pack will also be charged. When the external supply is disconnected or there is not enough power for the solar panel, SG50 can be powered by the internal battery pack.

Battery Installation

1. Release the fixing screw on the side of the device, and remove the battery compartment cover.
2. Push the battery into the battery compartment as the icon shows. If you need to take out the battery, hold on the latches on the battery to pull it out.
3. Fix the cover back to the device using the fixing screw.





Note:

- After installing the battery, the device will not power on automatically. Please connect the power cable of the solar panel to turn the device on. When the power cable is disconnected, the device will power off.
- **The battery can only be charged by the DC power connector, USB charge is not supported.**
- The device can not be charged when its temperature is more than 50°C. Please avoid direct exposure of the device to sunlight.
- When the device detects the temperature is lower than 0°C and solar panel power is enough (more than 7W), the device will heat the battery until the temperature reaches to 10°C, then charge the battery if the battery level is not full.
- The battery will be over-discharged if it is not used for an extended period, which will impact the battery's health. Please charge the battery regularly (at least every 3 months) to avoid over-discharge.

Solar Panel Installation

Refer to Solar Panel Installation chapter.

Note: Clean the solar panel surface on schedule or according local environmental conditions. The solar panel may be affected by environmental factors such as dust, sand, and bird droppings, which can reduce their charge efficiency.

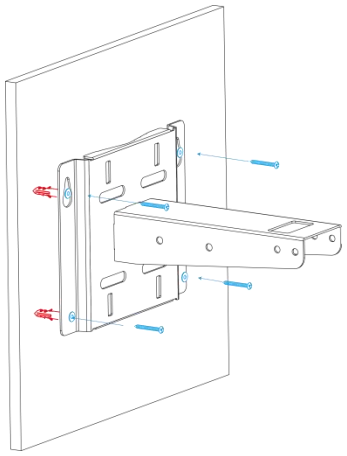
3.3 Gateway Installation

SG50 with solar panel can be mounted either to a wall or pole. It is suggested to install the device on sunny days for solar panel adjustment and charging.

3.3.1 Mounting Bracket Installation

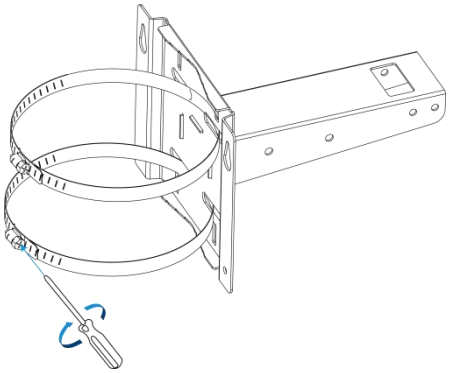
Wall Mounting:

Drill 4 holes on the wall according to the mounting bracket and insert the wall plugs into these holes. Then fix the mounting bracket to the wall by fixing the wall mounting screws into the wall plugs.



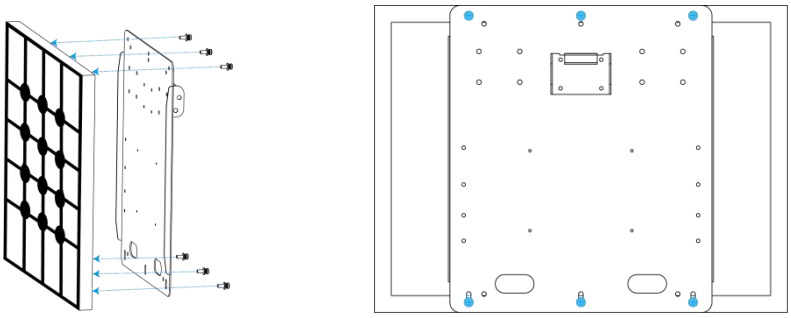
Pole Mounting:

Straighten the hose clamps and slide them through the rectangular rings in the mounting bracket. Wrap the hose clamps around the pole, then use a screwdriver to tighten the locking mechanism by turning it clockwise.

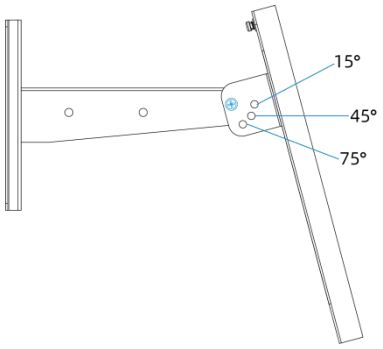


3.3.2 Solar Panel Installation

1. Remove the protective plastics on the four corners of the solar panel.
2. Fix the solar panel to the solar panel bracket using 6 fixing screws.

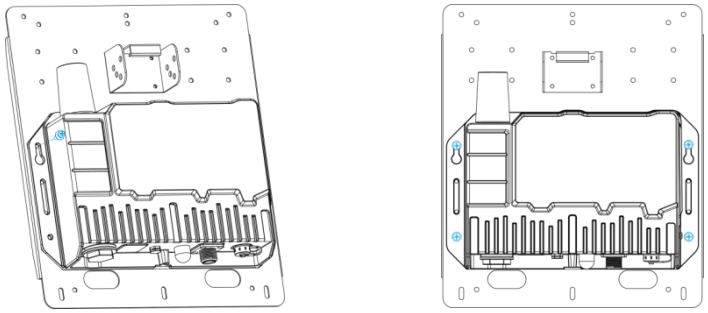


3. Hang the solar panel bracket onto the mounting bracket and fix both parts using 2 fixing screws first. Adjust the angle of the solar panel bracket (15°, 45°, and 75° is optional) based on the installation environment. Then fix the remaining two screws to the solar panel bracket.

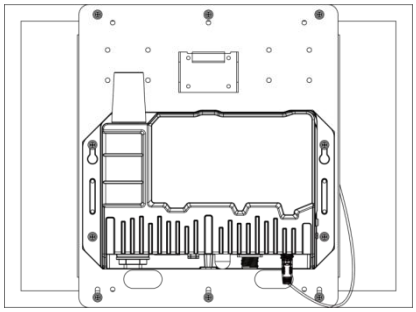


3.3.3 Device Installation

1. Fix the device to the opposite side of the solar panel bracket using 4 screws. When installation, it is suggested to fix the 2 screws on the top at first.
2. Install antennas as Antenna Installation chapter.



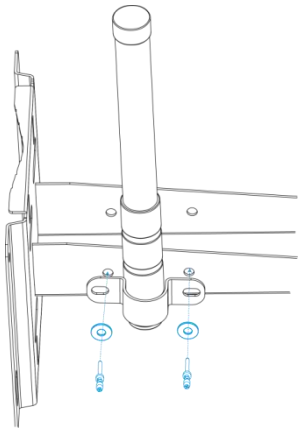
2. Connect M12 power cable of the solar panel to DC power connector of the device, then the device will power on automatically.



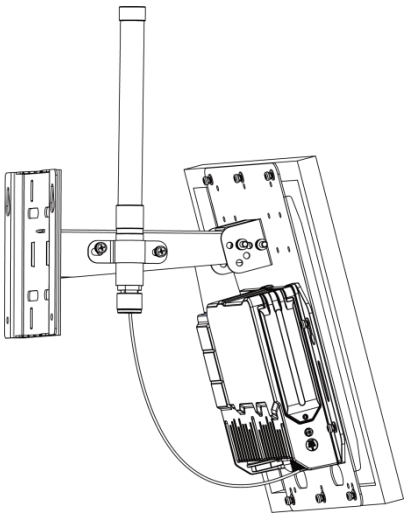
3.3.4 Antenna Installation

U-strap Mounting:

1. Pass the LoRaWAN® antenna through the U-strap clamp and fix the U-strap clamp to the side of the mounting bracket using 2 flat washers and 2 screws.



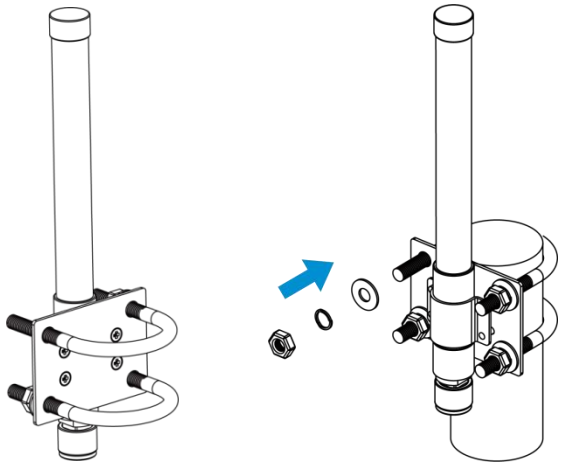
2. Connect one end of the antenna coaxial cable to the LoRaWAN® antenna, the opposite end to the device's antenna connector.



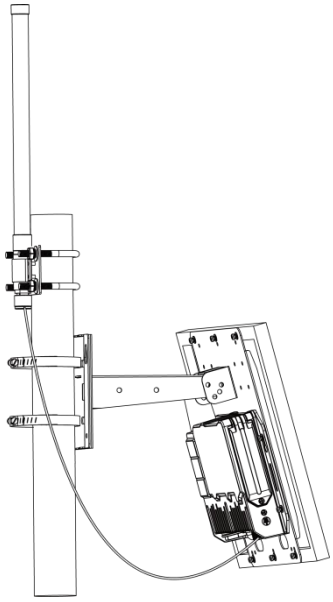
U-bolt Mounting:

1. Pass the LoRaWAN® antenna through the antenna clamp and fix it using 4 screws, then wrap the U-bolt around the pole and fix the clamp with nuts and other accessories.

Note: To make sure good signals of antennas, it is suggested to install the antenna to the top of the metal pole.



2. Connect one end of the antenna coaxial cable to the LoRaWAN® antenna, the opposite end to the device's antenna connector.

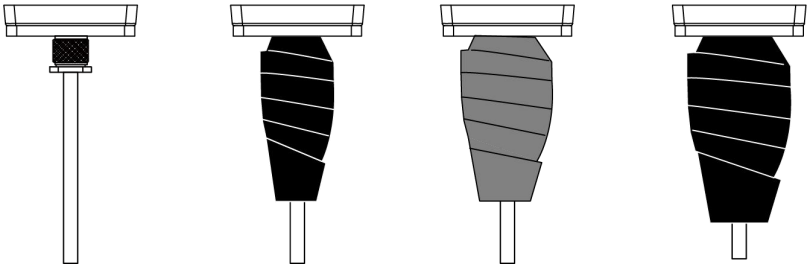


3.4 Weather Protection

To protect the gateway from outdoor bad weather, it is necessary to cover the antenna connector with tapes.

Note: Install the lightning arrester to the connector before wrapping tapes if required.

1. Ensure the antenna is installed tightly, then clean the surfaces of the connector.
2. Wrap a layer of electrical insulation tape tightly around the connector and overlap the previous wrap by 50%.
3. Wrap a layer of 3M waterproof tape tightly around the connector and overlap the previous wrap by 50%. Note that the tapes should be stretched to double their length when using.
4. Wrap a layer of electrical insulation tape with natural uncoiling force around the connector and overlap the previous wrap by 50%, ensure them to cover the head and tail of the connector.

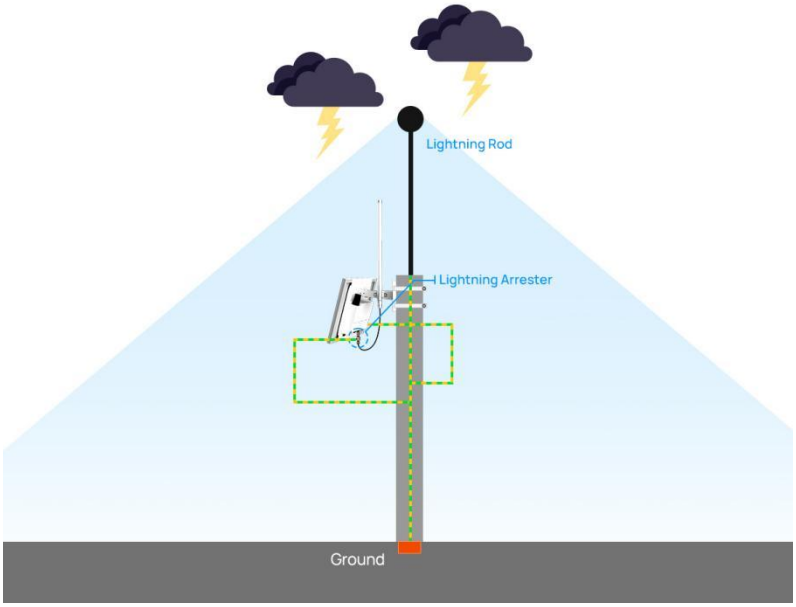


3.5 Lightning Protection

It is suggested to follow below notes to achieve lightning protection:

- Connect the gateway to the earth ground.
- Add a lightning arrester on the antenna connector.
- Ensure the antennas are lower than the highest position of the building, and the gateway with antennas is within the protection range of the lighting rod.
- If there is no lightning rod around, ensure the location of the gateway is not in the influence area of the lightning, or fix a lightning rod above the antennas.
- The cross-sectional area of the earthing wire should be more than 10 AWG.

Lightning Protection Example:



4. Access the Gateway

SG50 provides user-friendly web GUI for configuration and users can get access to it via Wi-Fi connection. The default settings are listed below:

Wi-Fi SSID: **Gateway_XXXXXX** (can be found on the label)

Wi-Fi IP Address: **192.168.23.1**

Browser: **Chrome (Recommended)**

Username: **admin**
Password: **password**

Configuration Steps:

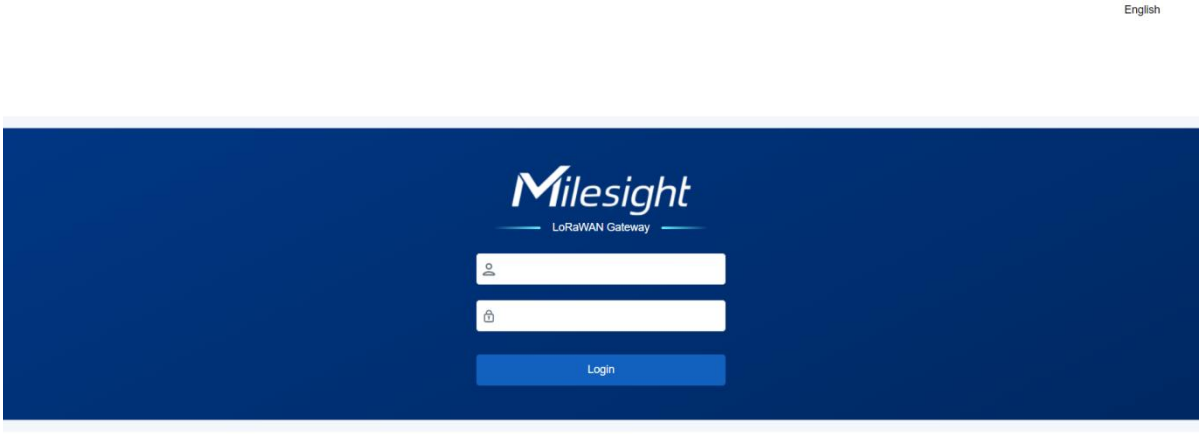
Step 1: Connect the M12 power cable to power on the device and ensure the Wi-Fi LED is statically on.

Step 2: Enable Wi-Fi on your computer and search for the gateway access point, then connect the computer to this access point.

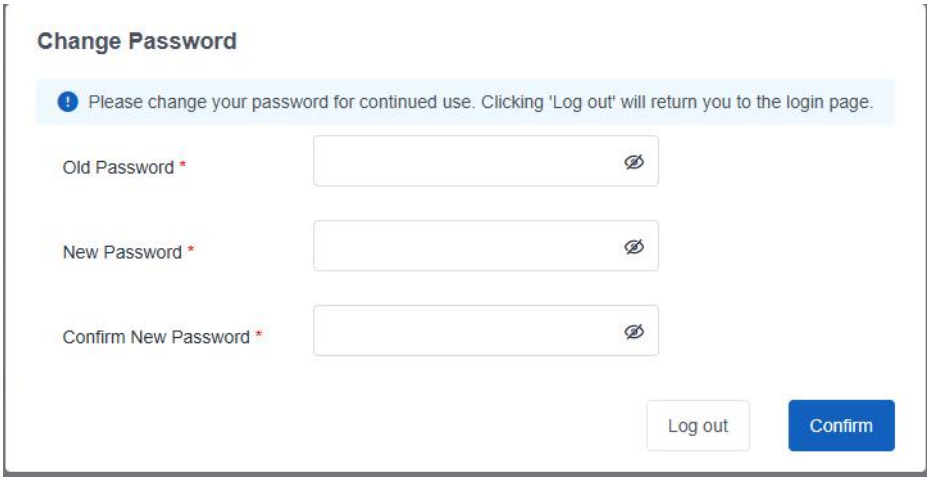
Step 3: Open the browser and type *https://192.168.23.1* to access the web GUI.

Step 4: Select the language.

Step 5: Enter the default username and password to log in the web GUI.



Step 6: Change the default password. The new password must contain at least one letter and one number.



Step 7: It is recommended to follow the setup wizard to complete basic settings. Users can also skip all steps or exit the wizard to configure the device.

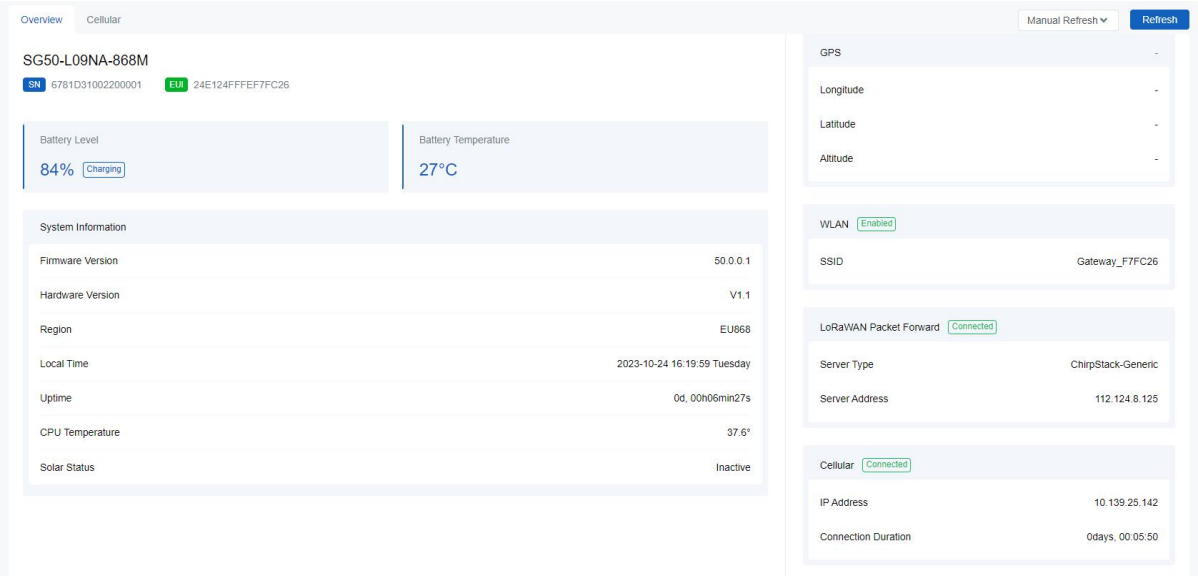
1) Configure the cellular settings to set up cellular connections. Usually, it is necessary to type the APN parameter to register to cellular networks. For details please refer to Cellular chapter.

2) Configure correct system time. For details please refer to Time chapter.

3) Configure the device to connect a LoRaWAN® network server. For details please refer to Packet Forward-General chapter.
4) Configure the packet filter. For details please refer to Packet Forward-Packet Filters chapter.
5) Configure the WLAN settings. For details please refer to WLAN chapter.

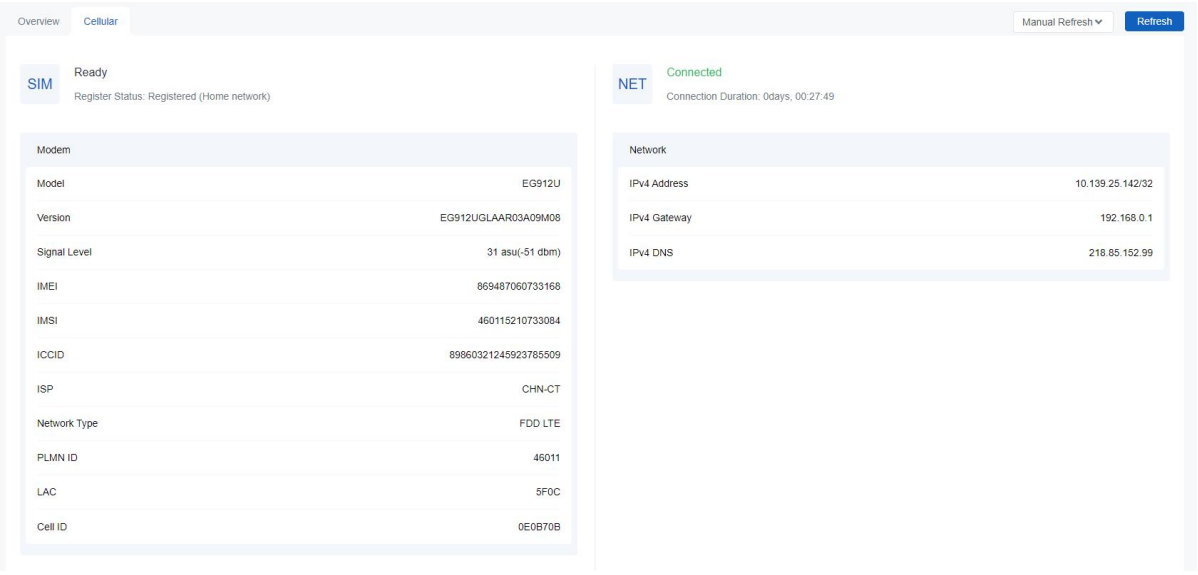
5. Operation Guide

5.1 Status



Overview	
Parameters	**Description**
Model	The whole model name of the gateway.
SN	The serial number of the gateway.
EUI	The unique identifier of the gateway and it's non-editable.
Battery Level & Status	The internal battery level and current charging status.
Battery Temperature	The temperature of the internal battery.
System Information	
Firmware Version	The current firmware version of the gateway.
Hardware Version	The current hardware version of the gateway.
Region	The LoRaWAN® frequency of the gateway. This can be changed on **Packet Forward > Radios** page.
Local Time	The current local time of the system.
Uptime	The information on how long the gateway has been running.

CPU Temperature	The temperature of CPU.
Solar Status	The current solar powering status.
GPS	
Longitude	The latitude of the location.
Latitude	The longitude of the location.
Altitude	The altitude of the location.
WLAN	
SSID	The SSID of the WLAN access point.
LoRaWAN® Packet Forward	
Server Type	The LoRaWAN® packet forward connection type.
Server Address	The LoRaWAN® network server address. When server type is Basic Station, this will show LNS URI and CUPS URI.
Cellular	
IP Address	The IP address of cellular network.
Connection Duration	The information on how long the cellular network has been connected.



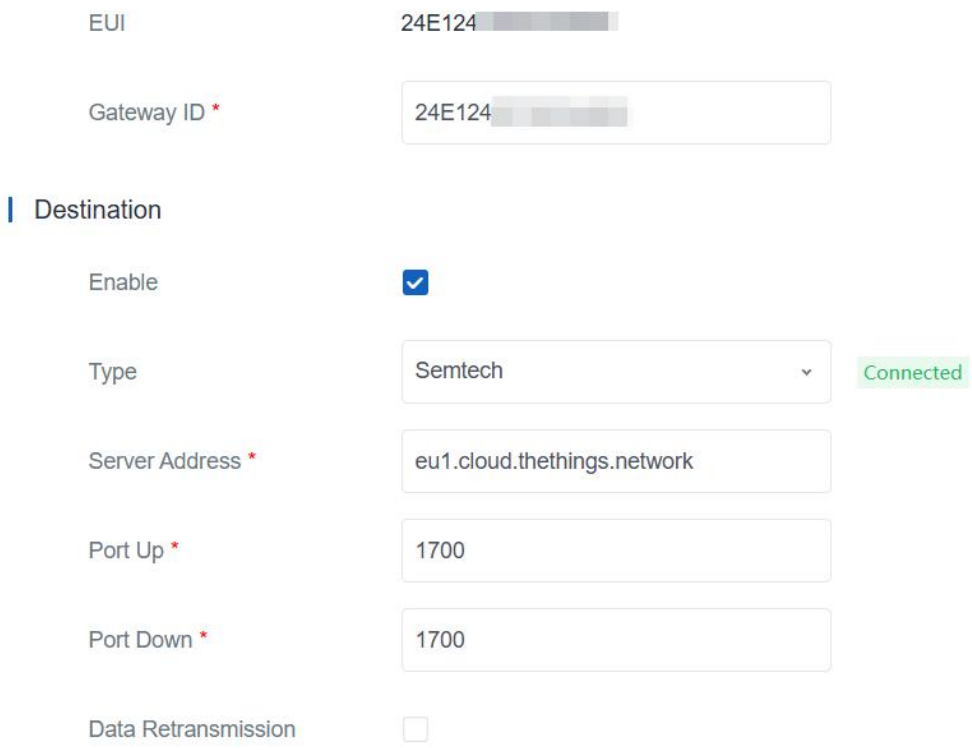
Cellular	
Parameters	**Description**
Modem	
SIM Status	Corresponding detection status of module and SIM card. ● No SIM Card: the SIM card is not inserted ● SIM Card Error: the SIM card is error ● PIN Error: the PIN code is error

	• PIN Required: the SIM card requires to type PIN code • PUK Required: the SIM card requires to be unlocked by PUK code • No Signal: no cellular signal • Ready: the SIM card is inserted • Down: the SIM card is deactivated
Register Status	The registration status of SIM card.
Model	The name of cellular module.
Version	The firmware version of cellular module.
Signal Level	The RSSI (Received Signal Indicator) of registered cellular network.
IMEI	The IMEI of the cellular module.
IMSI	The IMSI of the SIM card.
ICCID	The ICCID of the SIM card.
ISP	The network provider on which the SIM card registers.
Network Type	The connected network type, such as FDD LTE.
PLMN ID	The current PLMN ID, including MCC, MNC, LAC and Cell ID.
LAC	The location area code of the SIM card.
Cell ID	The Cell ID of the SIM card location.
Network	
Connection Status	The connection status of the cellular network.
Connection Duration	The information on how long the cellular network has been connected.
IPv4 Address	The IPv4 address of the cellular network.
IPv4 Gateway	The IPv4 gateway of the cellular network.
IPv4 DNS	The IPv4 DNS sever of the cellular network.

5.2 Packet Forward

SG50 supports to work as a packet forwarder to set up communication between LoRaWAN® end devices and LoRaWAN® network server.

5.2.1 General

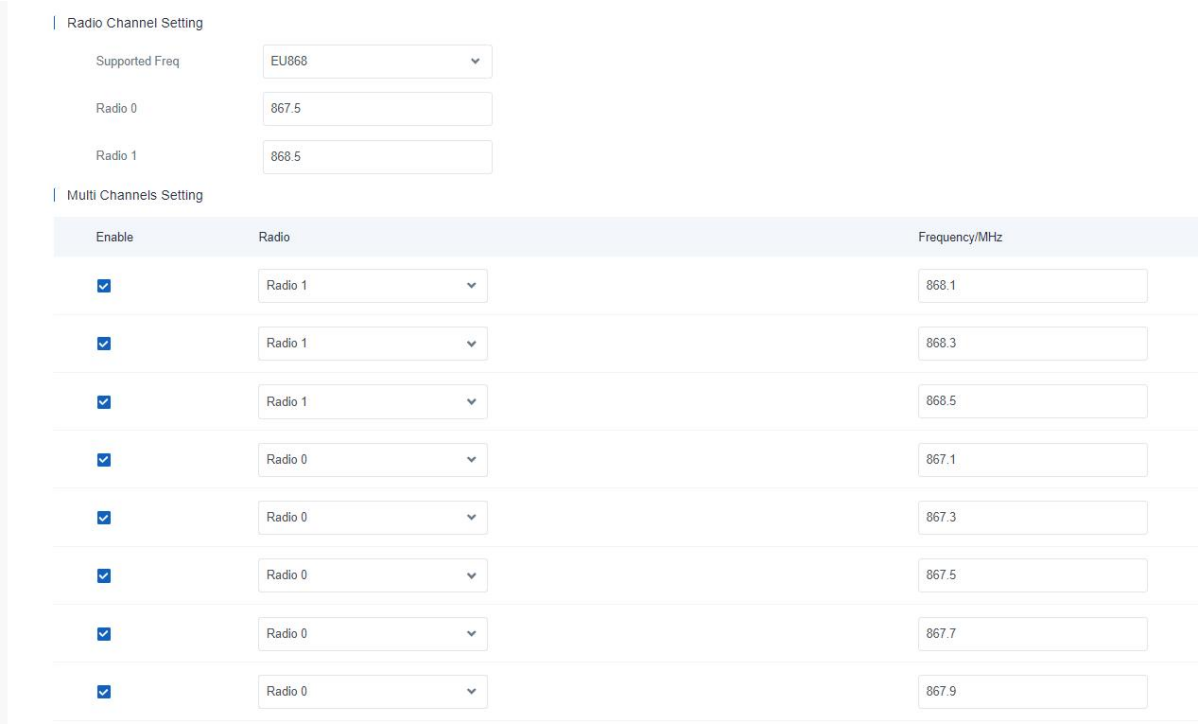


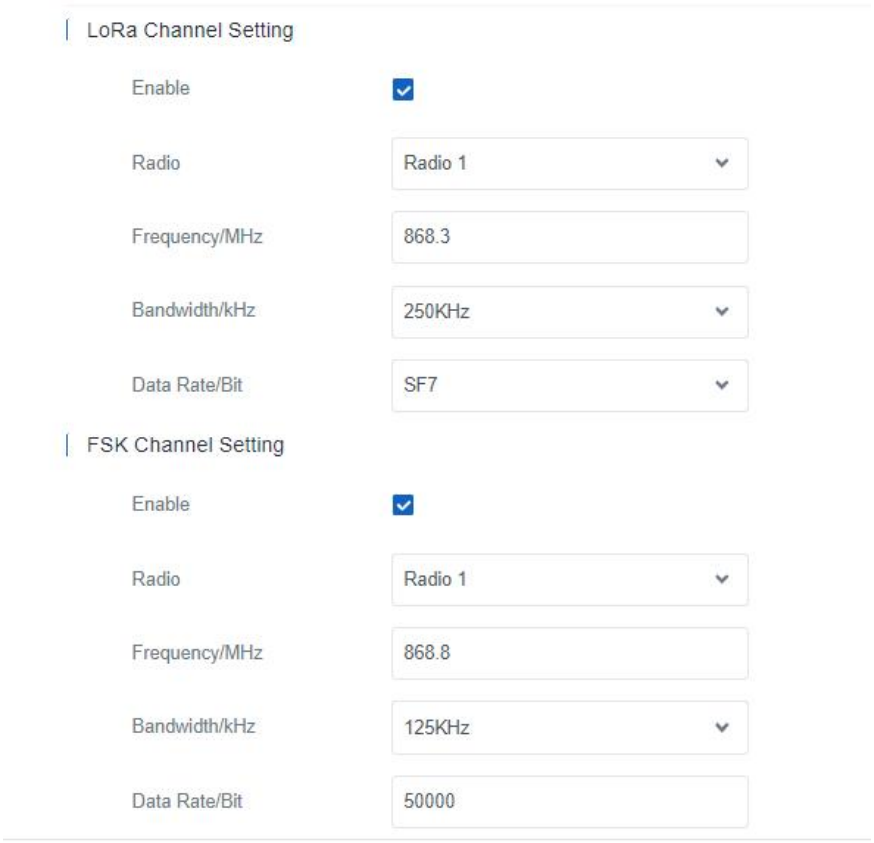
General	
Parameters	**Description**
EUI	The unique identifier of the gateway and it's non-editable.
Gateway ID	The customizable ID for registering gateway to network server, such as The Things Network. It is the same as gateway EUI by default.
Destination	
Enable	Enable or disable the packet forward feature.
Type	Select packet forward type among Semtech, Chirpstack-Generic or Basic Station, Remote Embedded NS, DeviceHub LNS or Milesight Development Platform LNS. **Semtech:** connect to network server through the Semtech UDP protocol. It supports to connect to most mainstream network servers. **Chirpstack-Generic:** connect to Chirpstackv3 via generic MQTT gateway bridge. **Chirpstack-v4:** connect to Chirpstackv4 via MQTT forwarder. **Basic Station:** connect to network server through TCP protocol. When configuring, there is no need to configure both LNS and CUPS settings. **Remote Embedded NS:** connect to embedded network server of Milesight UG65/UG67/UG56 gateways. **Embedded NS:** connect to the embedded network server. **DeviceHub LNS:** connect to Milesight DeviceHub LNS. This needs to select and enable DeviceHub 2.0 option on **Service** page and type the platform address. **Milesight Development Platform LNS:** connect to Milesight Development

	Platform LNS. This needs to select and enable Milesight Development Platform option on **Service** page and add the gateway to your platform account.
Semtech	
Server Address	The LoRaWAN® network server IP address or domain.
Port Up	The UDP port to forward uplinks from end device to network server.
Port Down	The UDP port to forward downlinks from network server to end device.
Data Retransmission	When network is disconnected, the device supports to store up to 500 pieces of Uplink type packets and re-transmit the data to network server after network recovery. **Note:** The device will not save Join Request packets.
Basic Station	
URI	The URL of LoRaWAN® network server. Please type as below format and replace *<server-address>* and *<port>* as real server address and server port. **LNS URI:** *wss://<server-address>:<port>* or *ws://<server-address>:<port>* **CUPS URI:** *https://<server-address>:<port>*
CA File	CA certificate to secure the server domain. **Note:** Change the certificate file format as *.trust* before import.
Client Certificate File	Client certificate file to verify the identity of the gateway.
Client Key File	Private key file to verify the identity of the gateway.
GPS	When connecting via LNS, enable or disable it to forward gateway GPS data to network server.
Data Retransmission	When network is disconnected, the device supports to store up to 500 pieces of Uplink type packets and re-transmit the data to network server after network recovery. **Note:** The device will not save Join Request packets.
ChipStack-Generic/ChirpStack-v4	
Server Address	The LoRaWAN® network server IP address or domain.
MQTT Port	The LoRaWAN® network server port.
Region ID	The region ID for ChirpStack-v4 server. This value will be typed automatically when changing the **Supported Freq** on **Packet Forward > Radios** page.
User Credentials	After enabled, username and password are required to type for verification.
TLS Authentication	Select from “Self signed certificates” or “CA signed server certificate”. **CA signed server certificate:** verify with the certificate issued by Certificate Authority (CA) that pre-loaded on the device. **Self signed certificates:** upload the custom CA certificates, client certificates and secret key for verification.
Data Retransmission	When network is disconnected, the device supports to store up to 500 pieces of Uplink type packets and re-transmit the data to network server after

	network recovery. **Note:** The device will not save Join Request packets.
Remote Embedded NS	
Server Address	The IP address or domain name of Milesight controller gateway.
MQTT Port	The communication port to Milesight controller gateway.
Data Retransmission	When network is disconnected, the device supports to store up to 500 pieces of Uplink type packets and re-transmit the data to network server after network recovery. **Note:** The device will not save Join Request packets.

5.2.2 Radios





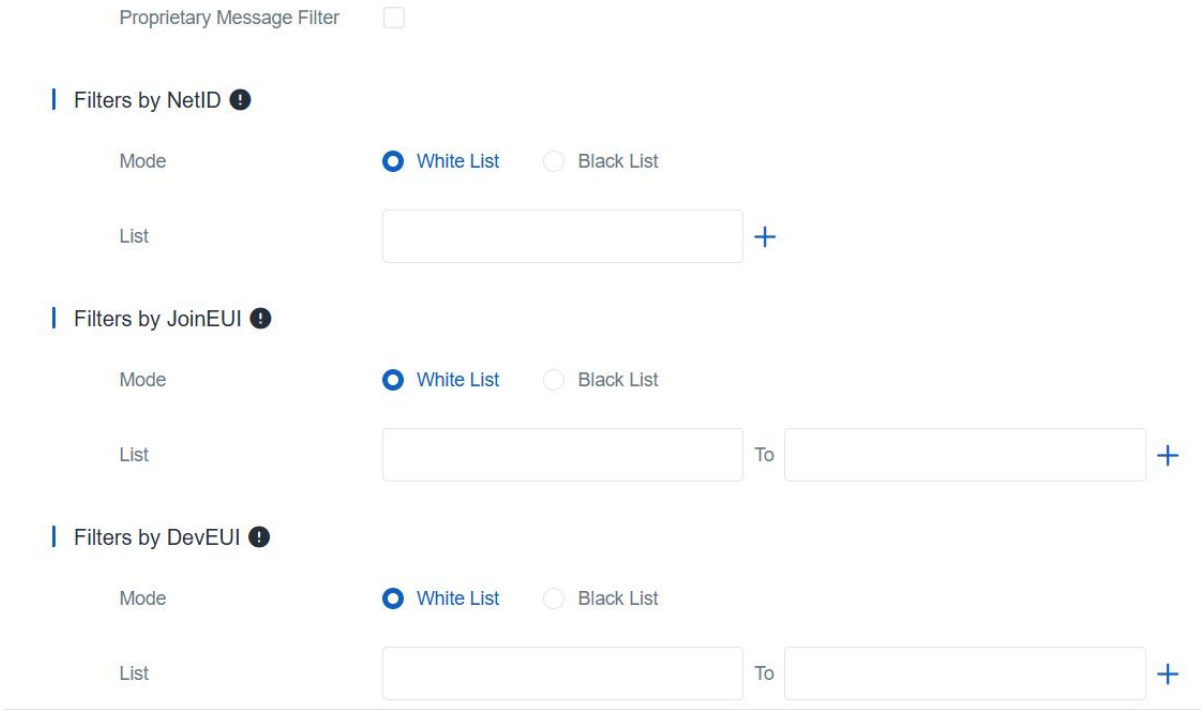
Radios	
Parameters	**Description**
Radio Channel Setting	
Supported Freq	The LoRaWAN® frequency plan used for the uplink and downlink frequencies and datarates. Available options depend on the gateway's model: **-470M:** CN470 **-868M:** EU868, RU864, IN865 **-915M:** US915, AU915, KR920, AS923-1&2&3&4
Radio 0/Radio 1	The center frequencies to receive packets from LoRaWAN® nodes.
Multi Channels Setting	
Enable	Enable or disable this channel to transmit packets.
Radio	Choose Radio 0 or Radio 1 as the center frequency.
Frequency/MHz	Set the frequency of this channel. Range: center frequency ± 0.4625.
LoRa/FSK Channel Setting	
Enable	Enable or disable this channel to transmit packets.
Radio	Choose Radio 0 or Radio 1 as the center frequency.
Frequency/MHz	Set the frequency of this channel.
Bandwidth/kHz	Set the bandwidth of this channel.

Data Rate/Bit	Set the data rate.

5.2.3 Packet Filters

SG50 supports to filter uplink packets via different conditions to reduce network congestion, save network traffic and ensure the safe operations.

Note: When the destination type is Embedded NS, this feature will not work.



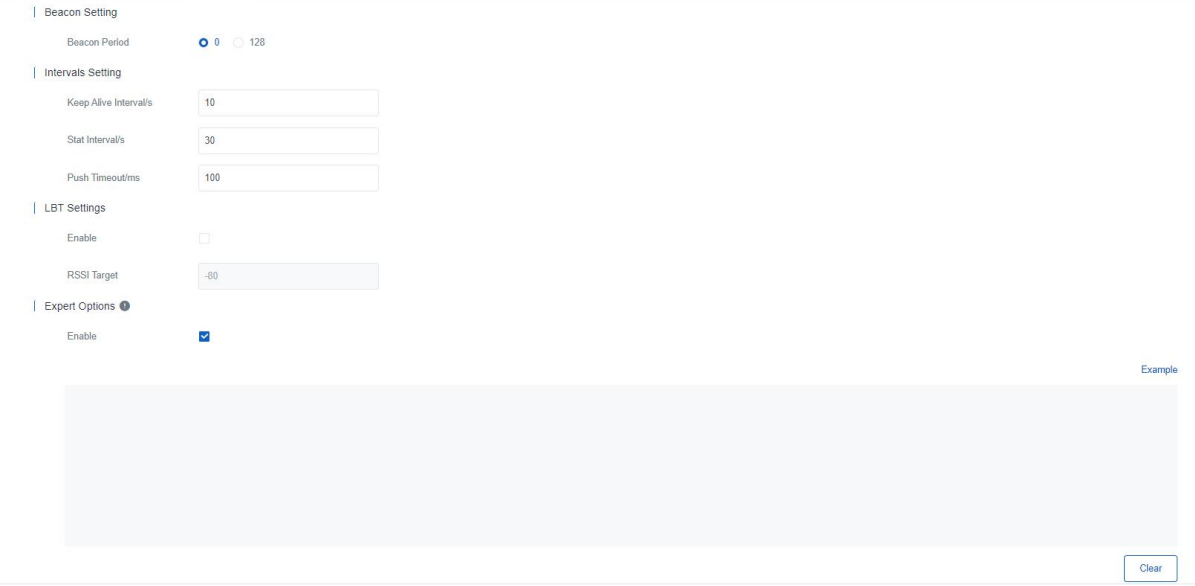
Packet Filters	
Parameters	**Description**
Proprietary Message Filter	Enable to not forward the proprietary message packets (Mtype=111).
Filters by NetID	Forward/Not forward the uplink packets that meet the NetID.
Filters by JoinEUI	Forward/Not forward the join request packets that meet the JoinEUI range.
Filters by DevEUI	Forward/Not forward the join request packets that meet the DevEUI range.
Mode	Select the filter mode as black list or white list. **White List:** Only forward the packets in this list to the network server. **Black List:** Only forward the packets except this list to the network server.
List	Set the specific filtering value or range list. Every condition supports to add 5 lists at most.

Note:

1. When join EUI and devEUI are both configured, only packets that meet both conditions will be forwarded.
2. When a third-party network server assigns filter condition to gateway, the gateway will use

network server settings in priority.

5.2.4 Advanced

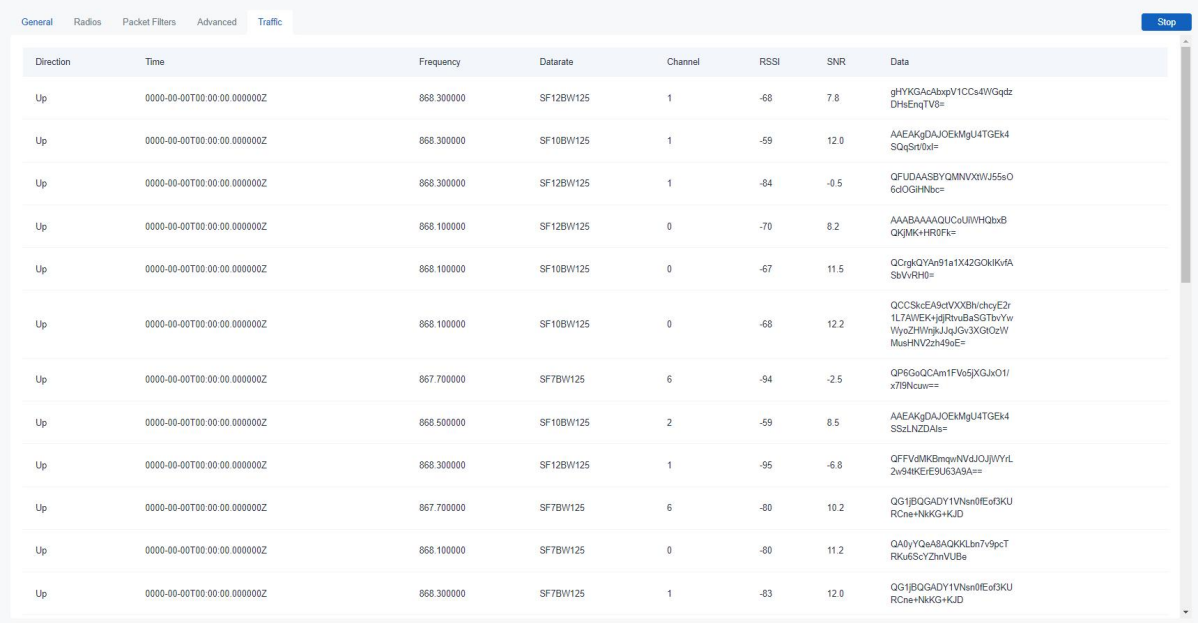


Advanced	
Parameters	**Description**
Beacon Setting	
Beacon Period	Interval of gateway sending beacons for Class B device time synchronization. 0 means the gateway will not send beacons. Please select the value as 128 if end device type is Class B.
Intervals Setting	
Keep Alive Interval/s	The interval of keepalive packet which is sent from gateway to network server to keep the connection stable and alive.
Start Interval/s	The interval to update the network server with gateway statistics.
Push Timeout/ms	The timeout to wait for the response from server after the gateway sends data.
LBT Setting	
Enable	Enable or disable LBT feature. Listen before talk (LBT) is used to detect whether the downlink channel is idle and avoid channel access conflicts. Note: AU915 and US915 do not support LBT feature.
RSSI Target	The criteria of an idle channel. If actual RSSI of a channel is less than the criteria/target, the channel is considered as idle.
Expert Options	
Enable	After enabled, the device supports customizing the configuration file to configure packet forwarder and customized configuration will overwrite the packet forward configurations of web GUI. To customize configuration file with correct format, click “Example” to go to

	reference page.

5.2.5 Traffic

SG50 supports to display latest 30 pieces of traffic received from end devices or network server.

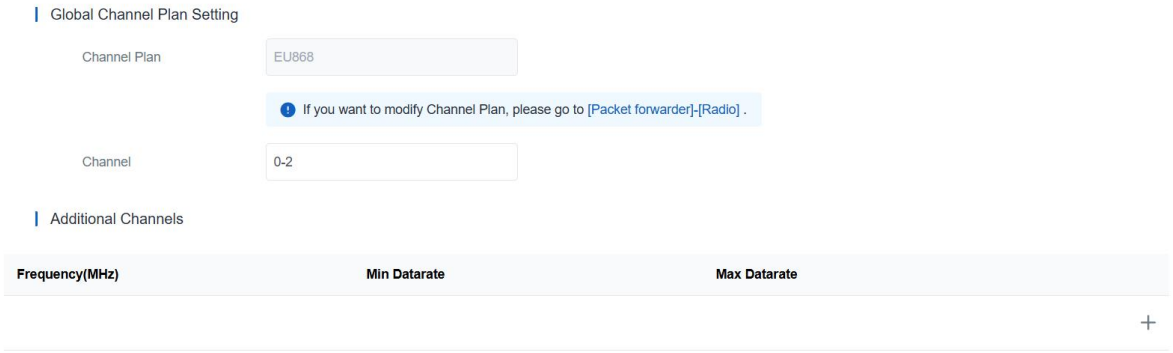


Traffic	
Parameters	**Description**
Fresh/Stop	**Fresh:** click to fresh this page to update latest data automatically. **Stop:** click to stop fresh this page to update latest data.
Direction	The transmission direction of this packet.
Time	The receiving time of this packet.
Frequency	The frequency of receiving or sending this packet.
Datarate	The datarate of this packet.
Channel	The frequency channel of receiving or sending this packet.
RSSI	The received signal strength of this packet.
SNR	The signal-to-noise ratio of this packet.
Data	The encrypted data of this packet.

5.3 Network Server

SG50 supports to work as a LoRaWAN® network server when the packet forwarder type is selected to **Embedded NS**.

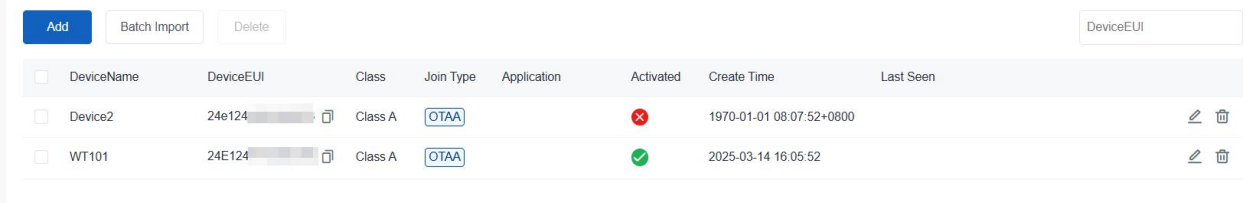
5.3.1 General Setting



General	
Parameters	**Description**
Channel Plan	Show the LoRaWAN® frequency plan used for the uplink and downlink frequencies and data rates.
Channel	Allow end devices to communicate with specific frequency channels. Leaving it blank means using all the default standard usable channels specified in the LoRaWAN® regional parameters document. It allows entering the index of the channels. **Examples:** 1, 40: Enabling Channel 1 and Channel 40 1-40: Enabling Channel 1 to Channel 40 1-40, 60: Enabling Channel 1 to Channel 40 and Channel 60
Additional Channels	For some regional variants, if allowed by your LoRaWAN® region, you can use Additional Plan to configure additional channels undefined by the LoRaWAN® Regional Parameters, like EU868 and KR920.

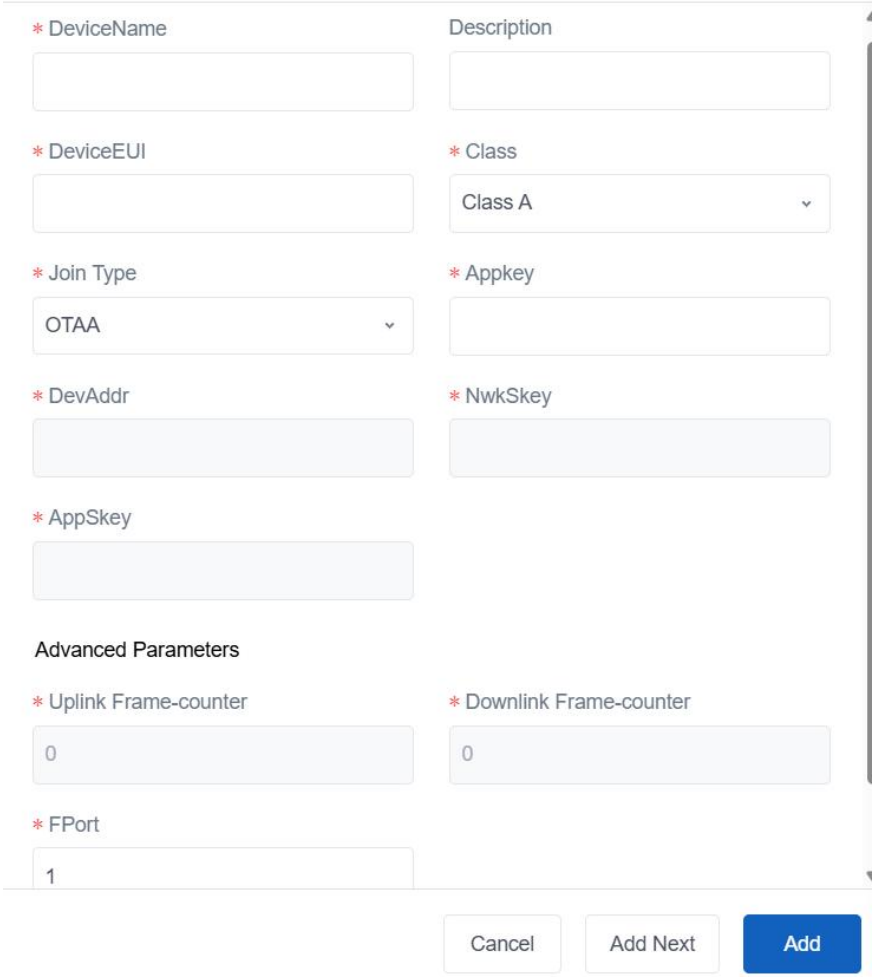
5.3.2 Devices

A device is the end-device connecting to, and communicating over the LoRaWAN® network. The gateway supports to add 100 devices at most.



Devices	
Parameters	**Description**
Add	Click to add a device.
Batch Import	Click to add bulk devices. You can download and adjust the template file, and then upload the file to add multiple devices.
Delete	Check the boxes of devices to delete.
Device Name	Show the name of the device.

Device EUI	Show the EUI of the device.
Class	Show the class type of the device.
Join Type	Show the join type of the device.
Application	Show the name of the device's application.
Activated	Show the network status of the device.
Create Time	Show the create time of the device.
Last Seen	Show the time of the last packet received.
Operation	Edit or delete the device.



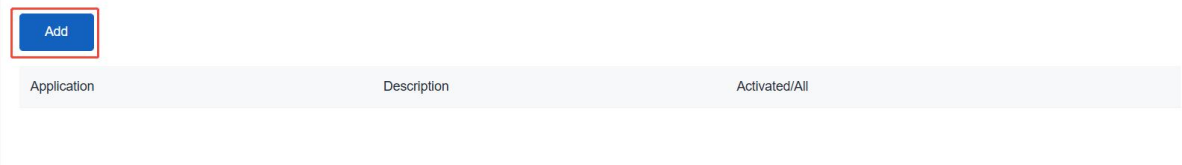
Add Device Configuration	
Parameter	**Description**
Device Name	Enter the name of this device.
Description	Enter the description of this device.
Device EUI	Enter the EUI of this device.
Class	Choose class type as Class A or Class C.
Join Type	Choose join type as OTAA or ABP.
App Key	Whenever an end-device joins a network via over-the-air activation, the application key is used for derive the Application Session key.
Dev Addr	The device address identifies the end-device within the current network.
NwkS Key	The network session key is specific for the end-device. It is used by

	the end-device to calculate the MIC or part of the MIC (message integrity code) of all uplink data messages to ensure data integrity.
AppS Key	The AppSKey is an application session key specific for the end-device. It is used by both the application server and the end-device to encrypt and decrypt the payload field of application-specific data messages.
Uplink Frame-counter	The number of data frames that sent uplink to the network server. It will be incremented by the end-device and received by the end-device. Users can reset a personalized end-device manually, then the frame counters on the end-device and the frame counters on the network server for that end-device will be reset to 0.
Downlink Frame-counter	The number of data frames which received by the end-device downlink from the network server. It will be incremented by the network server. Users can reset a personalized end-device manually, then the frame counters on the end-device and the frame counters on the network server for that end-device will be reset to 0.
FPort	Enter the downlink port of device, it's 85 by default for Milesight devices.
Frame-Counter Validation	If disable the frame-counter validation, it will compromise security as it enables people to perform replay-attacks.

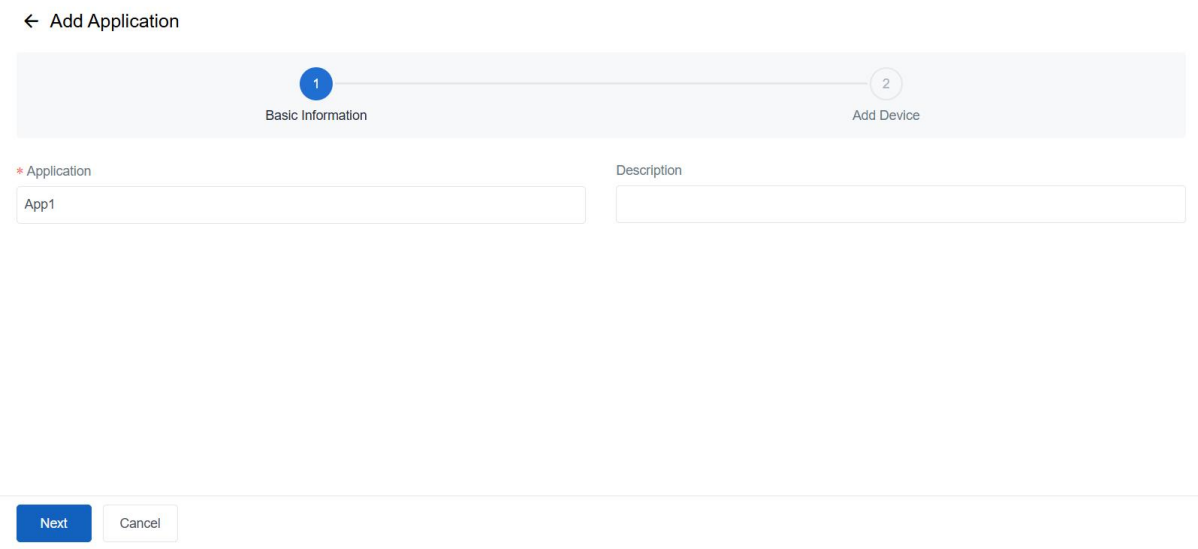
5.3.3 Application

An application is a collection of devices with the same purpose/of the same type. Users can add a series of devices to the same application which needs to send to the same server. The gateway supports to add 5 applications at most and every application can only connect to one MQTT broker.

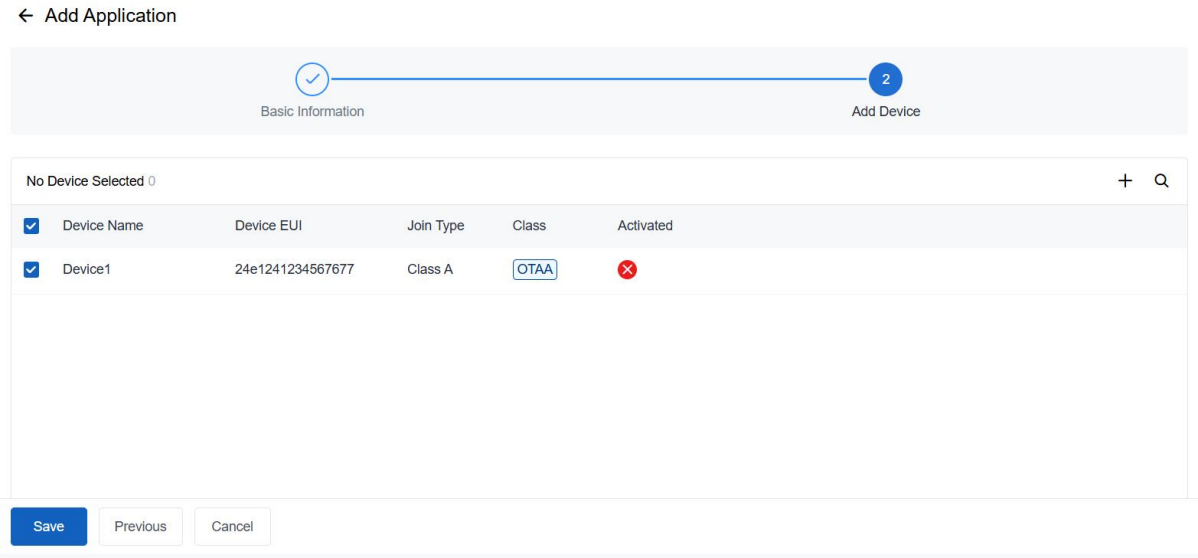
1. Click **Add** to add an application.



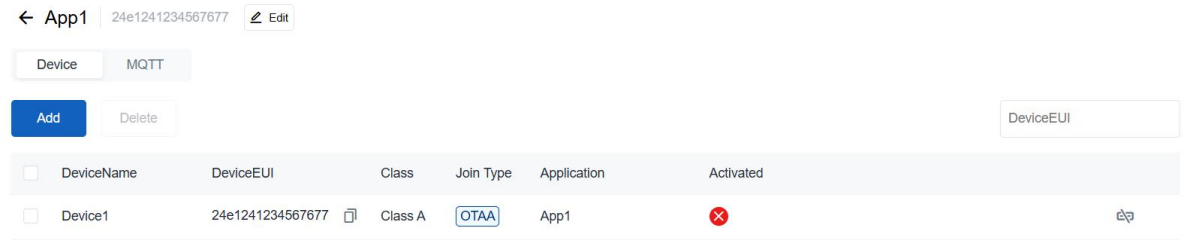
2. Customize an application name and type the description, then click **Next**.



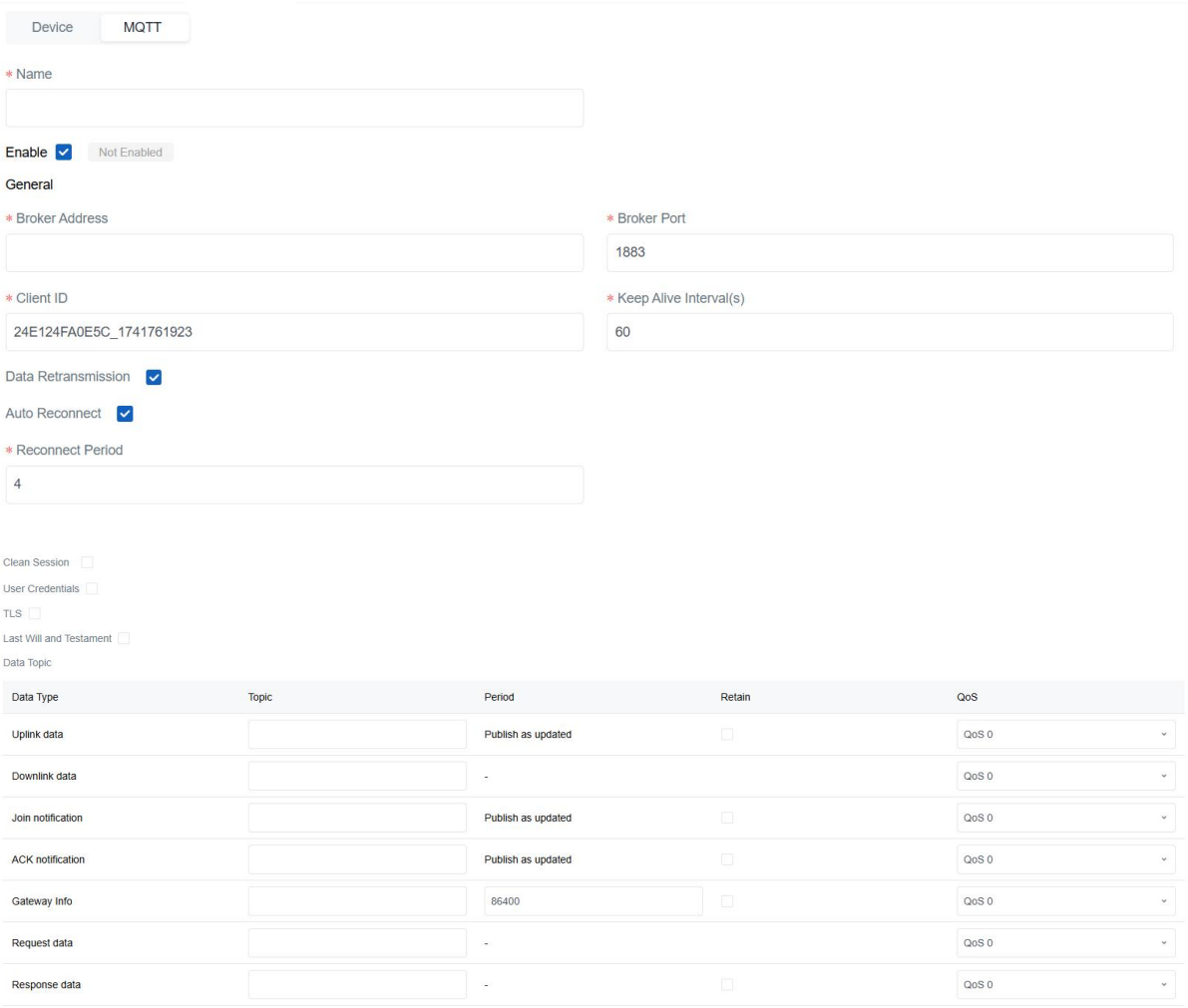
3. Select the devices to add to this application, then click **Save**. You can also click "+" to add a new device to this list if there is not suitable device.



4. Go to **Device** page to add or delete the devices in this application.



5. Go to **MQTT** page to configure the MQTT broker information to set up the communication between end devices and the MQTT broker.

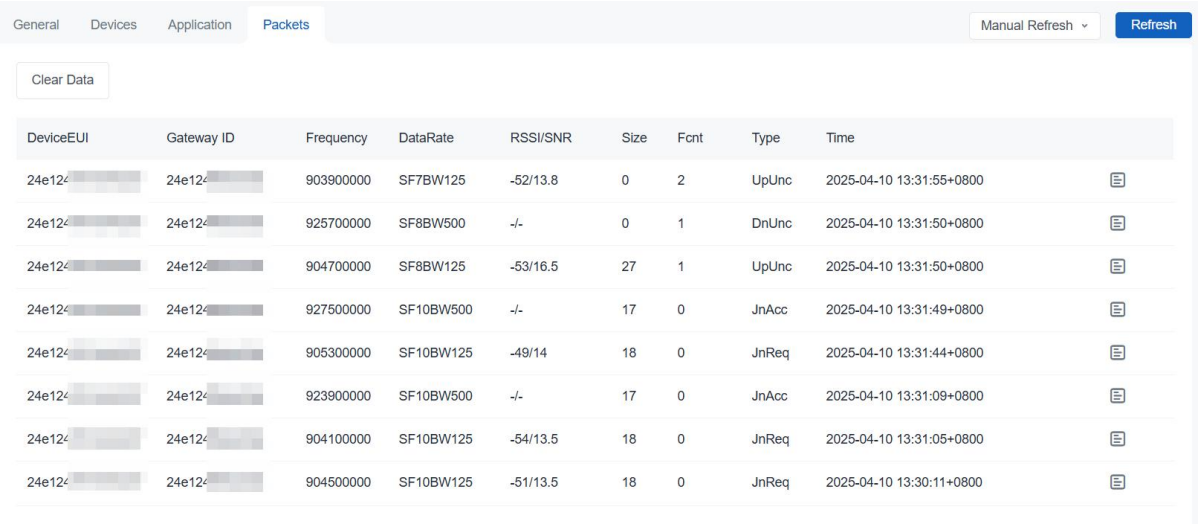


MQTT Settings	
Parameter	**Description**
Name	Customize a name for this MQTT connection.
Enable	Enable or disable this MQTT connection.
Broker Address	MQTT broker address to receive data.
Broker Port	MQTT broker port to receive data.
Client ID	Client ID is the unique identity of the client to the server. It must be unique when all clients are connected to the same server, and it is the key to handle messages at QoS 1 and 2.
Connection Timeout/s	If the client does not get a response after the connection timeout, the connection will be considered as broken. The Range: 1-65535
Keep Alive Interval/s	After the client is connected to the server, the client will send heartbeat packet to the server regularly to keep alive. Range: 1-65535
Data Retransmission	When network is disconnected, the device supports to store up to 100 pieces of all types of packets and re-transmit the data to MQTT broker after network recovery.
Auto Reconnect	When connection is broken, try to reconnect the server automatically. **Reconnect Period:** The interval to reconnect the server.

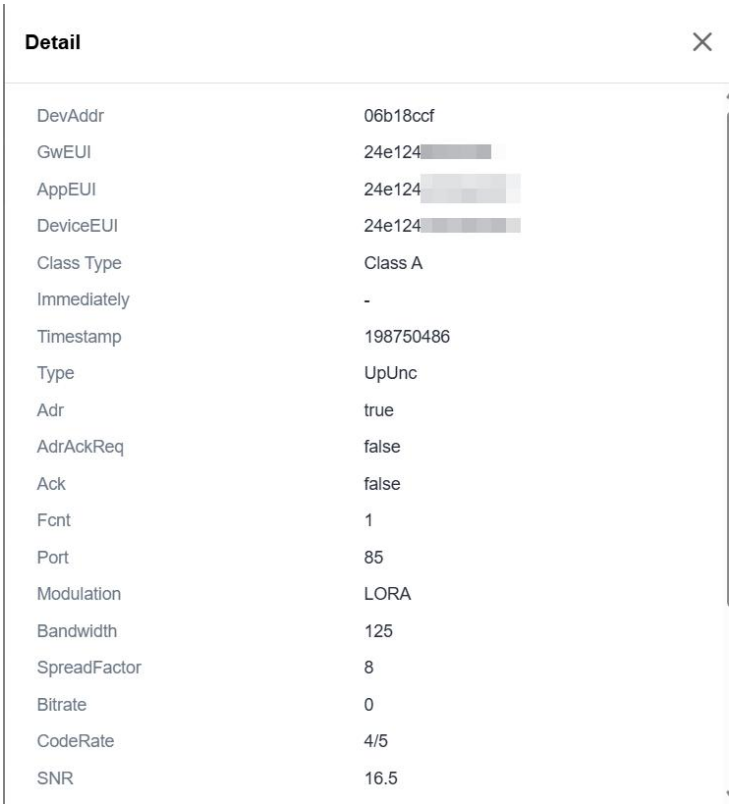
Clean Session	When enabled, the connection will create a temporary session and all information will lose when the client is disconnected from broker; when disabled, the connection will create a persistent session that will remain and save offline messages until the session logs out overtime.
User Credentials	Enable or disable user credentials for connecting to the MQTT broker.
TLS	Enable the TLS encryption in MQTT communication. **CA-signed server certificate:** verify with the certificate issued by Certificate Authority (CA) that pre-loaded on the device. **Self-signed certificates:** upload the custom CA certificates (.crt or .pem), client Certificates(.crt) and secret key(.key) for verification. **Note:** if MQTT broker type is HiveMQ, please enable **TLS** and set the option as **CA signed server certificate.**
Last Will and Testament	Last will message is automatically sent when the MQTT client is abnormally disconnected. It is usually used to send device status information or inform other devices or proxy servers of the device's offline status. **Last-Will Topic:** Customize the topic to receive last will messages. **Last-Will QoS:** QoS0, QoS1 or QoS2 are optional. **Last-Will Retain:** Enable to set last will message as retain message. **Last-Will Payload:** Customize the last will message contents.
Data Topics	
Data Type	Data type to communicate with MQTT broker: **Uplink Data:** receive device uplink packets **Downlink Data:** send downlink commands to device **Join Notification:** receive join request packets from devices **ACK Notification:** receive ACK packets from devices **Gateway Info:** receive basic information of the gateway **Request data:** send requests to enquire and configure the gateway **Response data:** receive the requested responses
Topic	Topic name of the data type used for publishing.
Period	The period to report data to MQTT broker.
Retain	Enable to set the latest message of this topic as retain message.
QoS	QoS 0 – Only Once This is the fastest method and requires only 1 message. It is also the most unreliable transfer mode. QoS 1 – At Least Once This level guarantees that the message will be delivered at least once, but may be delivered more than once. QoS 2 – Exactly Once QoS 2 is the highest level of service in MQTT. This level guarantees that each message is received only once by the intended recipients. QoS 2 is the safest and slowest quality of service level.

5.3.4 Packets

SG50 supports to display latest 500 pieces of packets.



Packets	
Parameters	**Description**
Clear Data	Click to clear the data in this page.
Device EUI	The device EUI of the packet.
Gateway ID	The ID of the gateway to send this packet.
Frequency	The frequency of receiving or sending this packet.
Datarate	The datarate of this packet.
RSSI/SNR	The received signal strength and signal-to-noise ratio of this packet.
Size	The size of this packet.
Fcnt	The frame counter of this packet.
Type	Show the type of the packet: JnAcc - Join Accept Packet JnReq - Join Request Packet UpUnc - Uplink Unconfirmed Packet UpCnf - Uplink Confirmed Packet - ACK response from network requested DnUnc - Downlink Unconfirmed Packet DnCnf - Downlink Confirmed Packet- ACK response from end-device requested
Time	The receiving time of this packet.
	Check the details of this packet.



Packets-Detail	
Parameters	**Description**
DevAddr	Click to clear the data in this page.
GwEUI	The ID of the gateway to send this packet.
AppEUI	The app EUI of the device which sending this packet.
Device EUI	The device EUI of the packet.
Class Type	The class type of the device which sending this packet.
Immediately	Whether to send this downlink packet immediately.
Timestamp	Show the time to receive this packet after packet forwarder starts running. Unit: ms
Type	Show the type of the packet: JnAcc - Join Accept Packet JnReq - Join Request Packet UpUnc - Uplink Unconfirmed Packet UpCnf - Uplink Confirmed Packet - ACK response from network requested DnUnc - Downlink Unconfirmed Packet DnCnf - Downlink Confirmed Packet- ACK response from end-device requested
Adr	Whether the device enables ADR.
AdrAckReq	In order to validate that the network is receiving the uplink messages, nodes periodically transmit ADRACKReq message. This is 1 bit long. True: Network should respond in ADR_ACK_DELAY time to confirm that it is receiving the uplink messages.

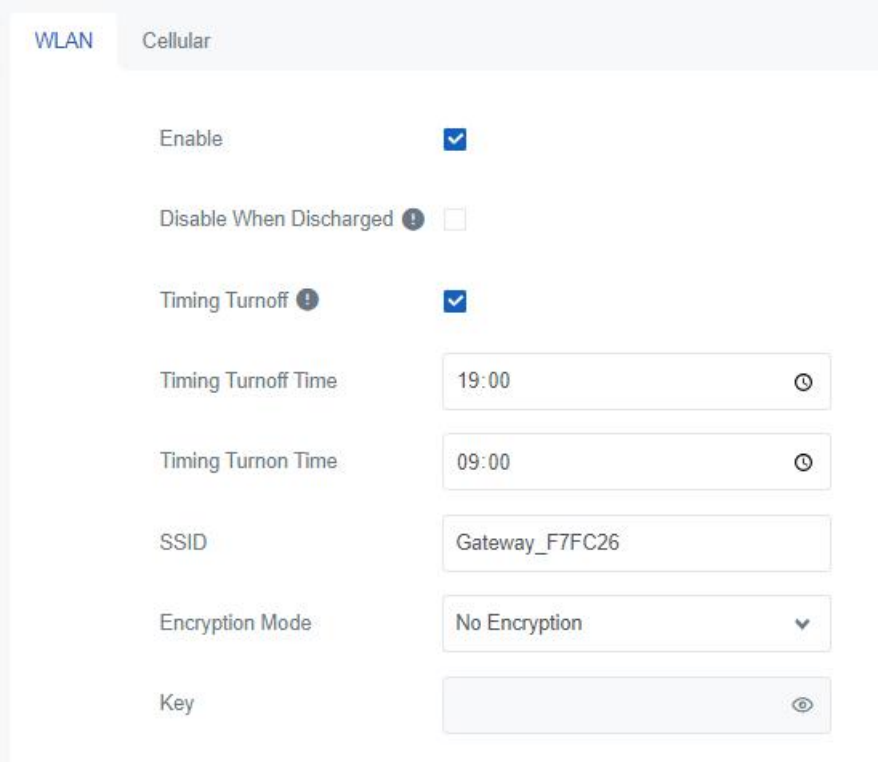
	False: ADR is disabled or Network does not respond in ADR_ACK_DELAY.
Ack	Whether this is ACK packet.
Fcnt	The frame counter of this packet.
Port	The FPort to transmit this packet. If this packet is MAC command, the port is 0; if this packet contains application data, the port is not 0 (1-233).
Modulation	LoRa means the physical layer uses the LoRa modulation.
Bandwidth	The bandwidth of this frequency channel.
Spreading Factor	The SF of this packet.
Bitrate	The bitrate of this frequency channel.
CodeRate	The coderate of this frequency channel.
RSSI	The received signal strength of this packet.
SNR	The signal-to-noise ratio of this packet.
Power	The TX power of this device.
Payload (b64)	The payload of this packet with base64 format.
Payload (hex)	The payload of this packet with HEX format.
MIC	The MIC of this packet. MIC is a cryptographic message integrity code, computed over the fields MHDR, FHDR, FPort and the encrypted FRMPayload.

5.4 Network

5.4.1 WLAN

SG50 supports wlan feature to work as AP mode to configure device and it can not connect to other access points.

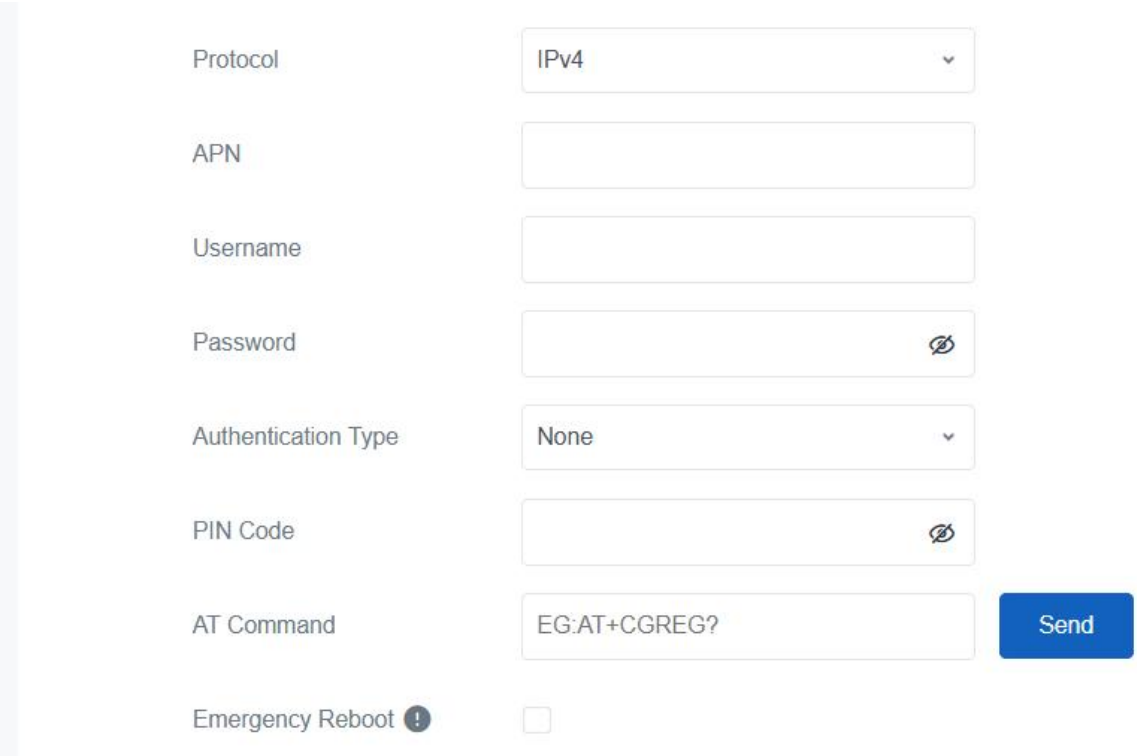
Note: one SG50 device only supports 2 devices' WLAN connection to login this device at the same time.



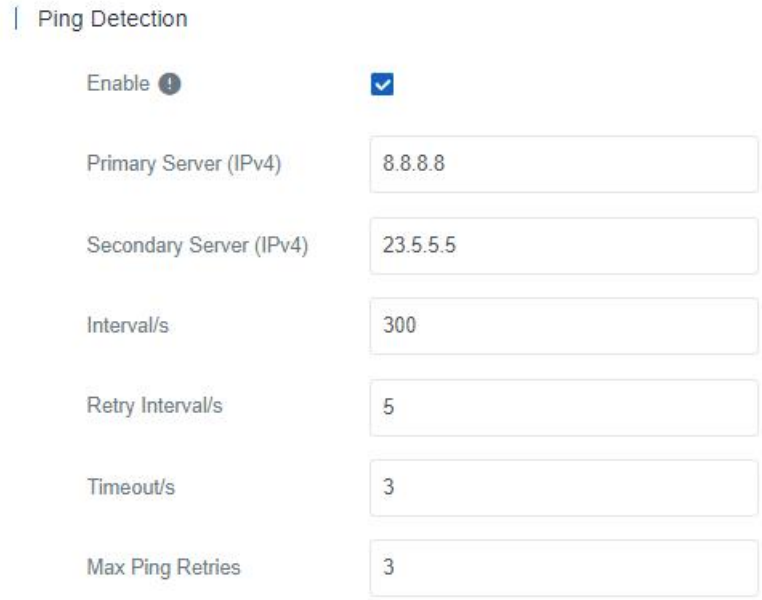
WLAN	
Parameters	**Description**
Enable	Enable or disable Wi-Fi feature.
Disable When Discharged	After enabled, the device will turn off the Wi-Fi when the battery is discharging to save power.
Timing Turnoff	If this option is enabled, the device will turn off and turn on the Wi-Fi at preset time points of a day.
SSID	The unique name for this device Wi-Fi access point. The default SSID is Gateway_XXXXXX. (XXXXX=last 6 digits of MAC address)
Encryption Mode	No Encryption and WPA-PSK are optional.
Key	Customize the Wi-Fi password when security mode is WPA-PSK. Length: 8--63. Limitation: any ASCII characters except blank.

5.4.2 Cellular

SG50 supports to insert a SIM card to get cellular network connections.



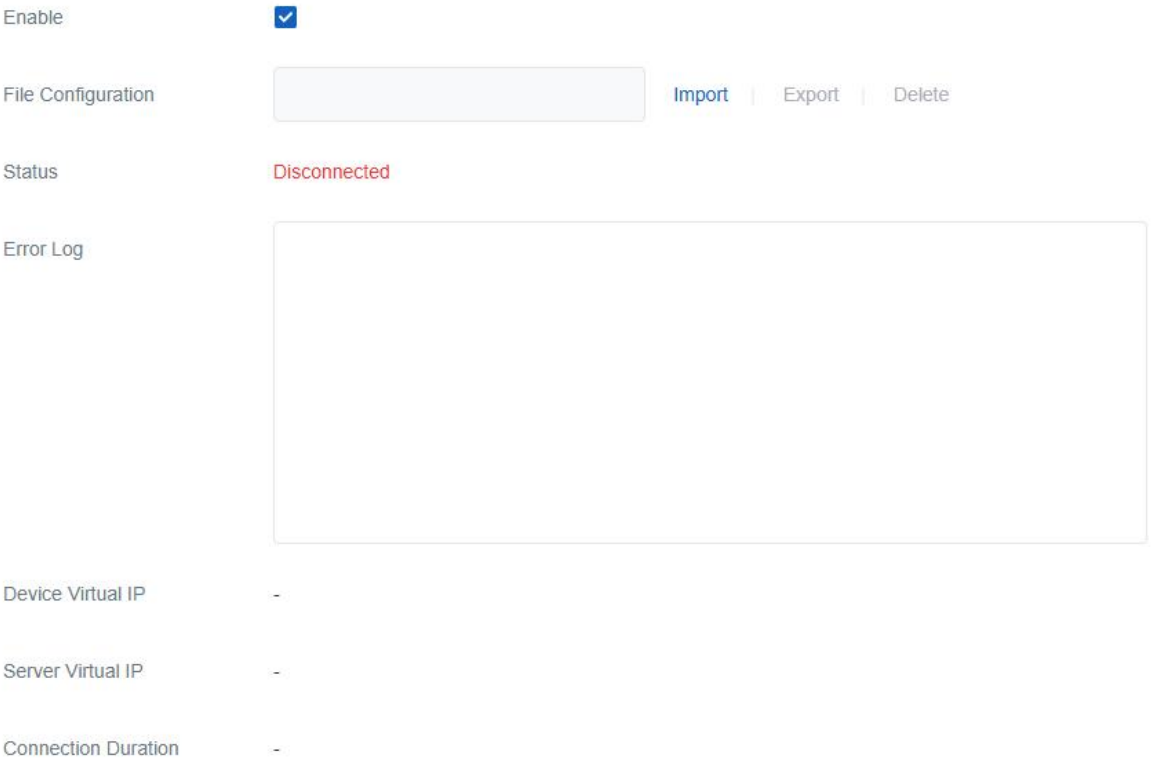
Cellular	
Parameters	**Description**
Protocol	Select from "IPv4", and "IPv4/IPv6".
APN	The Access Point Name for cellular dial-up connection provided by local ISP. Please contact cellular operator or search for the Internet to get it.
Username	The username for cellular dial-up connection provided by local ISP.
Password	The password for cellular dial-up connection provided by local ISP.
Authentication Type	Select from None, PAP and CHAP.
PIN Code	A 4-8 characters PIN code to unlock the SIM.
AT Command	Send AT Command to get cellular information or configure advanced settings.
Emergency Reboot	Enable to reboot the device if cellular connection is not available.



Ping Detection	
Parameters	**Description**
Enable	After enabled, the device will send ICMP packets to corresponding servers to detect the connection periodically. **Note:** Disable this option if the device is connected to a private (non-internet) network.
Primary Server (IPv4)	The device will send ICMP packet to this server address or domain name to determine whether the Internet connection is still available or not.
Secondary Server (IPv4)	The device will try to ping the secondary server name if primary server is not available.
Interval/s	Time interval between two ping attempts.
Retry Interval/s	When ping failed, the device will ping again at every retry interval.
Timeout/s	The maximum time the device will wait for a ping response. If it does not receive a response for the timeout, the ping request will be considered to have failed.
Max Ping Retries	The number of times the device will retry sending a ping request until determining that the connection has failed.

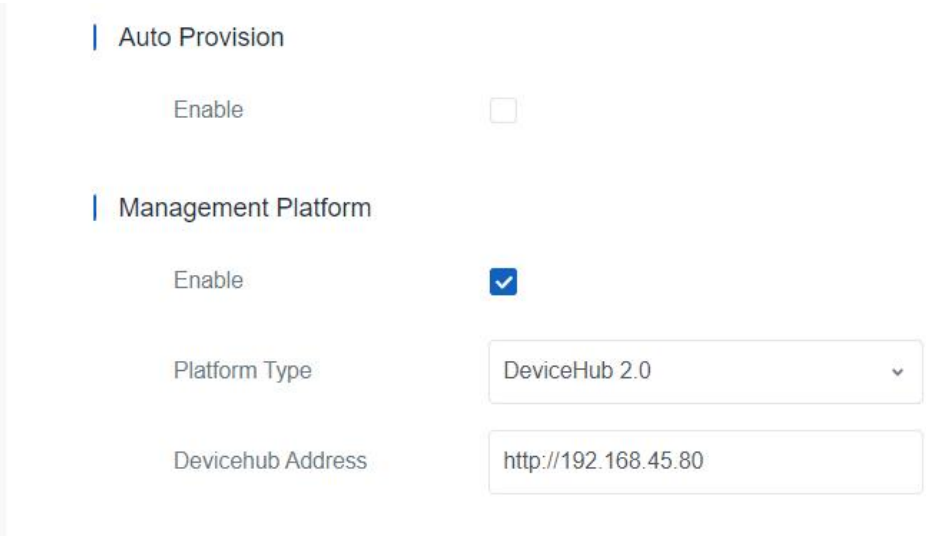
5.4.3 OpenVPN

SG50 supports working as an OpenVPN client to set up security private network connection.



OpenVPN	
Parameters	**Description**
Enable	Enable or disable OpenVPN client.
File Configuration	Upload a .ovpn client configuration file including the settings and certificate information. Please refer to the client configuration file according to sample: client.conf
Status	Show the connection status between the gateway and the OpenVPN server.
Error Log	Show the connection and configuration error logs.
Device Virtual IP	Show the virtual IP address of the device after VPN setup.
Server Virtual IP	Show the virtual IP address of the server after VPN setup.
Connection Duration	Show how long the gateway has been connected to the OpenVPN server.

5.5 Service



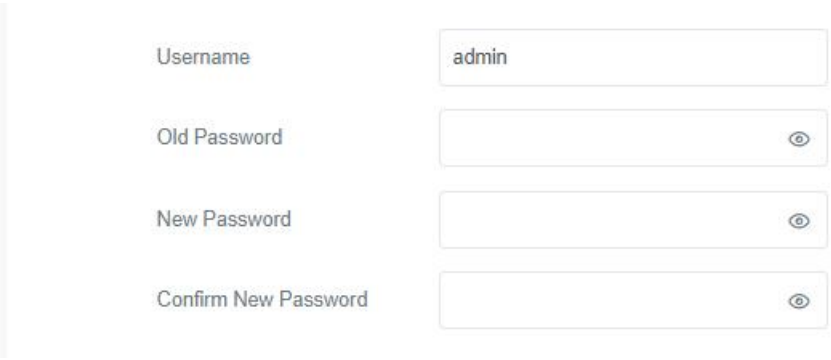
Parameters	Description
Auto Provision	Enable to receive the configurations from Milesight Development Platform once after the device is connected to Internet. This will work even management platform mode is disabled.
Management Platform	
Enable	Enable the device to be managed by Milesight management platforms.
Platform	Milesight DeviceHub 2.0 or Milesight Development Platform is optional.
DeviceHub Address	Set the DeviceHub server IP address or domain name.

5.6 System

5.6.1 General

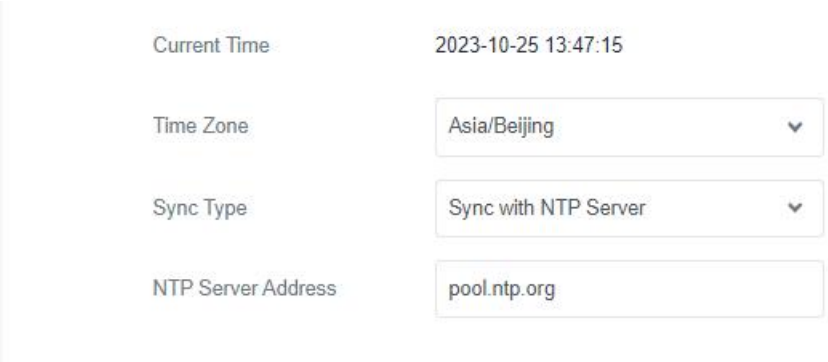
The gateway supports to change the hostname.

5.6.2 User



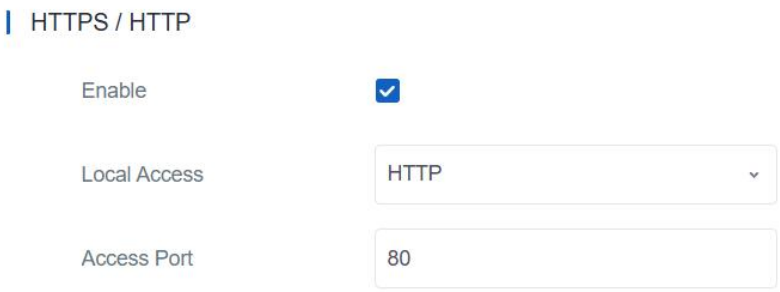
Parameters	Description
Username	Enter a new username. Only letters, digits, underscores(_) , and hyphens (-) are allowed.
Old Password	Enter the old password.
New Password	Enter a new password. The password must contain at least one letter and one number.
Confirm New Password	Enter the new password again.

5.6.3 Time



Parameters	Description
Current Time	Show the current system time.
Time Zone	Click the drop-down list to select the time zone you are in.
Sync Type	Click the drop down list to select the time synchronization type. **Sync with Browser:** Synchronize time with browser. **Sync with NTP Server:** Synchronize time with NTP Server.
NTP Server Address	Set the NTP Server's IP address or domain name.

5.6.4 Access Service



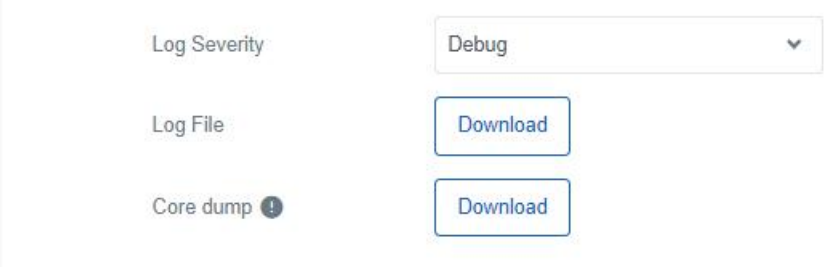
Parameters	Description
Enable	Enable or disable the local access.
Local access	Select the access protocol as HTTP or HTTPS.
Access port	Set the port number for HTTP or HTTPS access.

5.6.5 Sleep Mode

Parameters	Description
Enable	Enable the gateway to enter sleep mode when insufficient solar power is detected. During the sleep mode, the gateway will turn off all programs and activates the power detection program every 10 minutes.
Maximum Sleep Time without Light	Set the maximum days to go to sleep mode without sunlight. Note: When hardware version is 1.x, this time is fixed at 10 days and not support to be configured.

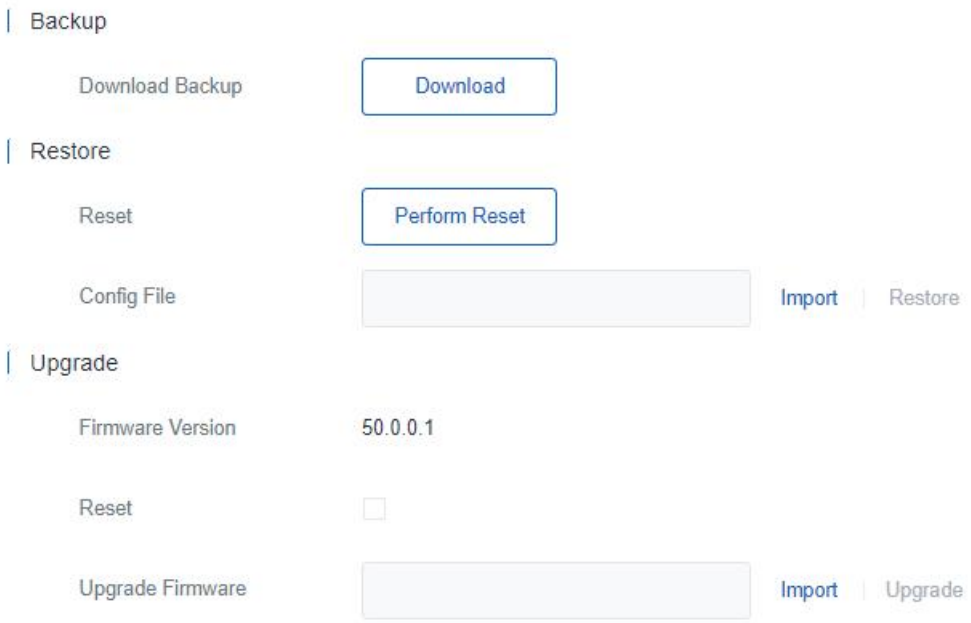
5.7 Maintenance

5.7.1 Log



Parameters	Description
Log Severity	The list of severities follows the syslog protocol.
Log File	Download log file.
Core dump	Core dump file contains a snapshot of a program's memory at a specific point in time when the program encounters a critical error or crashes, which can be used for debugging and troubleshooting purposes.

5.7.2 Backup/Upgrade

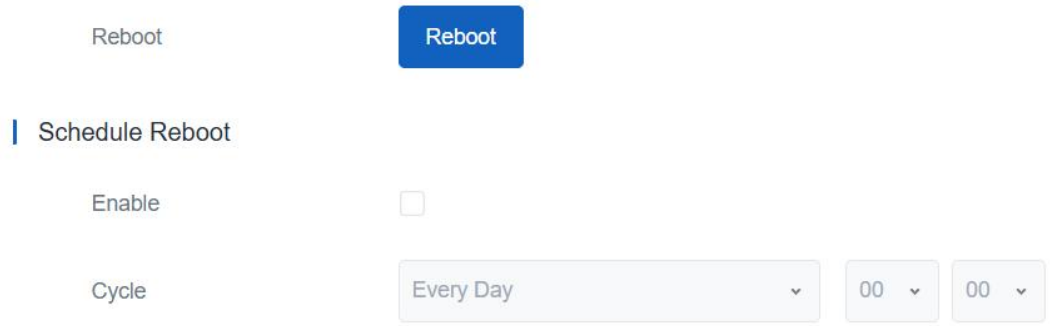


Backup/Upgrade	
Parameters	**Description**
Backup	
Backup	Export the current configuration file to the PC.
Restore	
Reset	Reset device to factory default settings. The device will restart after reset process is done.
Config File	Click "Import" button to select configuration file, and then click "Restore" button to upload the configuration file to the device.
Upgrade	
Firmware	Show the current firmware version.

Version	
Reset	When this option is enabled, the device will be reset to factory defaults after upgrade.
Upgrade Firmware	Click "Import" button to select the new firmware file, and click "Upgrade" to upgrade firmware. **Note:** 1) Ensure that the distance between the computer and the SG50 device is not too far during the upgrade; otherwise, the upgrade process may fail. 2) After upgrade, the device will restart automatically. Please reconnect Wi-Fi to access the web GUI. 3) After upgrade, clean the caches of the browser if there is abnormal display of web GUI.

5.7.3 Reboot

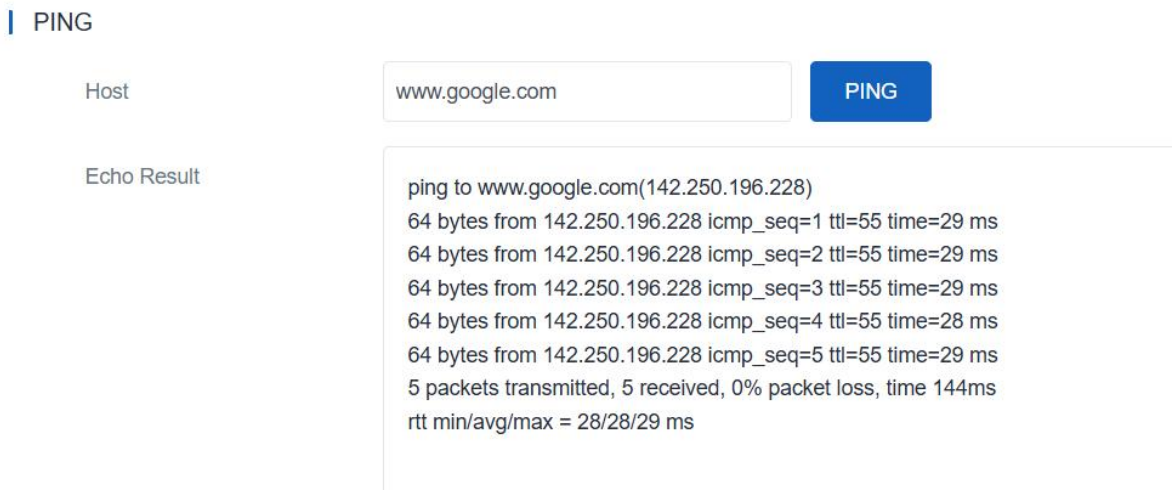
On this page you can reboot the gateway and return to the login page. We strongly recommend clicking “Save” button before rebooting the gateway so as to avoid losing the new configuration.



Reboot	
Parameters	**Description**
Reboot	Reboot the device immediately.
Schedule Reboot	
Enable	Enable or disable to reboot regularly.
Cycle	Select the reboot cycle as day/week/month and configure the time.

5.7.4 Ping

Ping tool is engineered to check the outer network connectivity by typing IPv4 address or domain name.



Appendix

Default Frequency

Supported Freq	Channel/MHz
CN470	471.9, 472.1, 472.3, 472.5, 472.7,472.9, 473.1, 473.3 (8~15)
EU868	868.1, 868.3, 868.5, 867.1, 867.3, 867.5, 867.7, 867.9
IN865	865.0625, 865.4025, 865.6025, 865.985, 866.185, 866.385, 866.585, 866.785
RU864	868.9, 869.1, 869.3, 867.3, 867.5, 867.7, 867.9, 868.1
AU915	916.8, 917, 917.2, 917.4, 917.6, 917.8, 918, 918.2 (8~15)
US915	903.9, 904.1, 904.3, 904.5, 904.7, 904.9,905.1, 905.3 (8~15)
KR920	922.1, 922.3, 922.5, 922.7, 922.9, 923.1, 923.3, 923.5
AS923-1	923.2, 923.4, 922, 922.2, 922.4, 922.6, 922.8, 923
AS923-2	921.2, 921.4, 921.6, 921.8, 922, 922.2, 922.4, 922.6
AS923-3	916.6, 916.8, 917, 917.3, 917.4, 917.6, 917.8, 918
AS923-4	917.3, 917.5, 917.7, 917.9, 918.1, 918.3, 918.5, 918.7

-END-