



Ultra Low Power Solar LoRaWAN Gateway

SG50

User Guide

Contents

Chapter 1. About this Guide.....	3
Chapter 2. Product Introduction.....	6
Overview.....	6
Packing List.....	6
Hardware Introduction.....	7
Chapter 3. First Start.....	11
Chapter 4. Hardware Installation.....	15
Chapter 5. Power Management.....	23
Chapter 6. Web GUI Configuration.....	24
Status.....	24
Packet Forward.....	30
Network Server.....	43
Network.....	60
Cellular.....	60
WLAN.....	64
OpenVPN.....	68
Service.....	70
Device Management.....	70
System.....	72
General.....	72
Event & Notification.....	76
Low Power Mode.....	81
Maintenance.....	82
Chapter 7. Services.....	89

Chapter 1. About this Guide

This guide provides instructions for setting up, deploying, configuring, operating, and maintaining the SG50 gateway.

Readers

This guide is intended for installers, system integrators, network administrators, and other personnel responsible for deploying or managing the gateway.

Copyright Statement

This guide may not be reproduced in any form or by any means to create any derivative such as translation, transformation, or adaptation without the prior written permission of Xiamen Milesight IoT Co., Ltd (Hereinafter referred to as Milesight).

 reserves the right to change this guide and the specifications without prior notice. The latest specifications and user documentation for all Milesight products are available on our official website <http://www.milesight.com>

Safety Instruction

These instructions are intended to ensure that users can use the product correctly to avoid danger or property loss. Milesight will not take responsibility for any loss or damage resulting from failure to follow the instructions in this operating guide.



Warning:

Serious injury or death may be caused if any of these warnings is neglected.

- This installation must be conducted by a qualified service person and should strictly comply with the electrical safety regulations of the local region.
- Do not power the device or connect it to other electrical devices during installation.
- Do not connect or power the device using damaged cables.
- Make sure the device is firmly fixed when installing.



CAUTION:

Injury or equipment damage may be caused if any of these cautions are neglected.



- 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 drop the device or subject it to physical shock.

Revision History

Release Date	Version	Description
Oct. 15, 2023	V1.0	Initial version
Jan. 15, 2024	V1.1	1. Add remote embedded NS packet forwarder type; 2. Compatible with Milesight Development Platform and DeviceHub V2.
Apr. 3, 2025	V1.2	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 cellular protocol parameter option. 6. Add Proprietary Message filter. 7. Add sleep mode. 8. Add weather protection and lightning protection.
Aug. 4, 2025	V1.2.1	1. Add syncing time with the browser. 2. Add gateway info to report via MQTT. 3. Add solar panel maintenance note.
Sept. 22, 2025	V1.3	1. Add HTTPS access feature. 2. Add OpenVPN client feature. 3. Add password change prompt upon first login

Release Date	Version	Description
Aug. 21, 2026	V1.4	1. Add displaying battery power and DC input power, and support power consumption history export. 2. Add radio noise scan. 3. Add advanced parameters for embedded NS devices. 4. Add HTTP/HTTPS data reporting via applications. 5. Add gateway event data report type via applications. 6. Add an SSL security option in TLS authentication for Chirpstack packet forwarder or embedded NS MQTT transmission. 7. Add cellular IMS option and DNS server parameters. 8. Add WLAN client mode. 9. Add global routing option for OpenVPN. 10. Optimize the display of Device Management page. 11. Add battery event notification via email or SMS. 12. Adjust sleep mode to low power mode. 13. Add remote log transmission.

Chapter 2. Product Introduction

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 place with hard access to power resource.

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

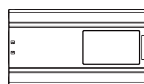
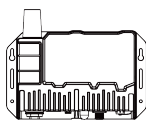
Benefiting from its robust structural design and high IP67 protection rate, SG50 can work smoothly in harsh environments. It is specifically tailored for applications such as oil and gas, mining, forestry, and remote industries where power consumption must be carefully managed.

The device has the following 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.
- Embedded 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

Packing List

After unboxing, please check the package contents against the following list to ensure all items are included. If any of the below items are missing or damaged, please contact your sales representative.



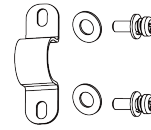
1 × SG50 Gateway



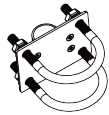
1 × Battery Pack



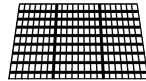
1 × SIM Card Ejector Tool



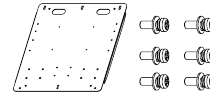
1 × LoRaWAN[®]
Antenna (60cm)



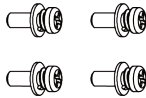
1 × Antenna Coaxial Cable (1m)



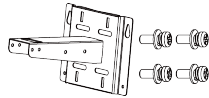
1 × Antenna U-strap Kit



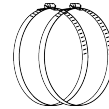
1 × Antenna U-bolt Clamp Kit



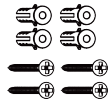
1 × Solar Panel (with
50cm M12 Power Cable)



1 × Solar Panel Bracket Kit



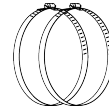
4 × Mounting Screws



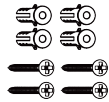
1 × Mounting Bracket Kit



2 × Hose Clamps (Ø 67-127mm)



4 × Wall Mount Screw Sets



1 × Warranty Card



1 × Quick Guide Card



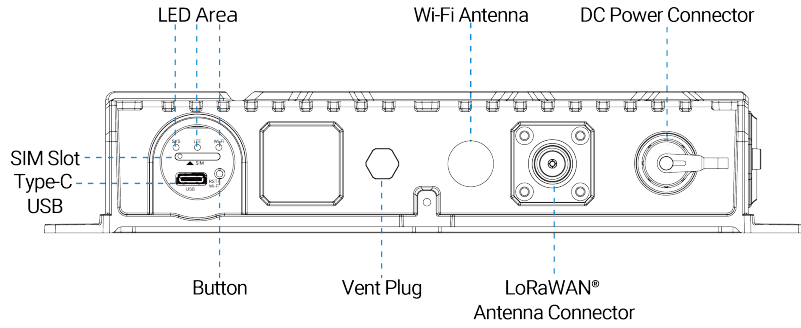
Hardware Introduction

This chapter describes the hardware design of the device.

Hardware Overview

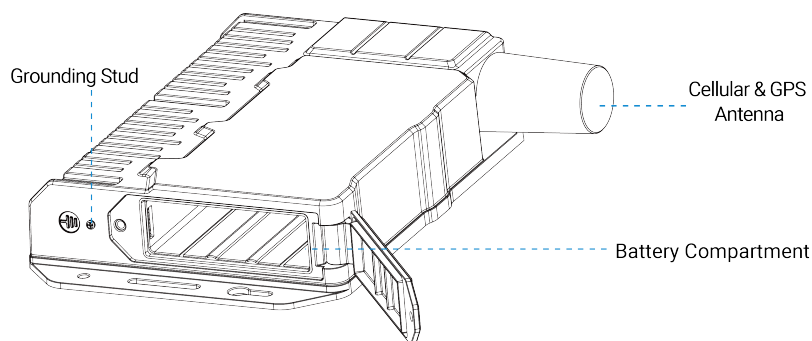
The following figure shows the main components of the device.

Bottom View



Part	Description
DC Power Connector	Connect a solar panel or an external DC source to supply power to the device.
LoRaWAN® Antenna Connector	Allows connection of an external antenna to enhance wireless communication range and reliability.
Wi-Fi Antenna	Enhance wireless communication range and reliability.
Vent Plug	Equalizes the internal pressure and prevents moisture build-up.
LED Area	See LED Patterns .
Button	See Button Patterns .
SIM Slot	Allows to insert a SIM card to connect to the cellular network.
Type-C USB Port	Used for device console or device power supply.

Side View



Part	Description
Cellular & GPS Antenna	Enhance wireless communication range and reliability.
Battery Compartment	Install battery pack to supply power to the device.

Part	Description
Grounding Stud	Used to connect to an earth ground to protect the device from power surges.

LED Patterns

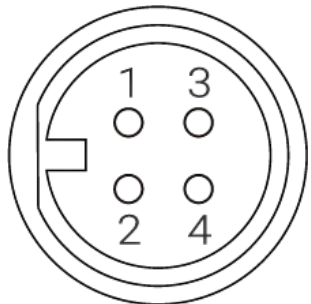
LED	Status	Description
SYS	Off	The power is switched off or in sleep mode
	Green Static On	The power is switched on and the system is working well
	Red Static On	The power is switched on and the system malfunctions
LTE	Off	SIM card is registering or failed to register (or there are no SIM cards inserted)
	Slowly Blinks	SIM card has been registered and is ready for dial-up
	Quickly Blinks	SIM card has been registered and is dialing up now
	Static On	SIM card has been registered and dialed up successfully
Wi-Fi	Off	Wi-Fi is off
	Slowly Blinks	Wi-Fi is starting
	Static On	Wi-Fi is on

Button Patterns

Function	Action	LED Status
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 Low Power Mode	When low power mode is enabled and the gateway detects not enough solar power.	SYS: Quickly Blinks → Off
Wake Up	Under low power mode, quickly press the button once to wake up for 10 minutes.	SYS: Off → On
Factory Reset	Press and hold the button for more than 5 seconds.	SYS: Quickly Blinks

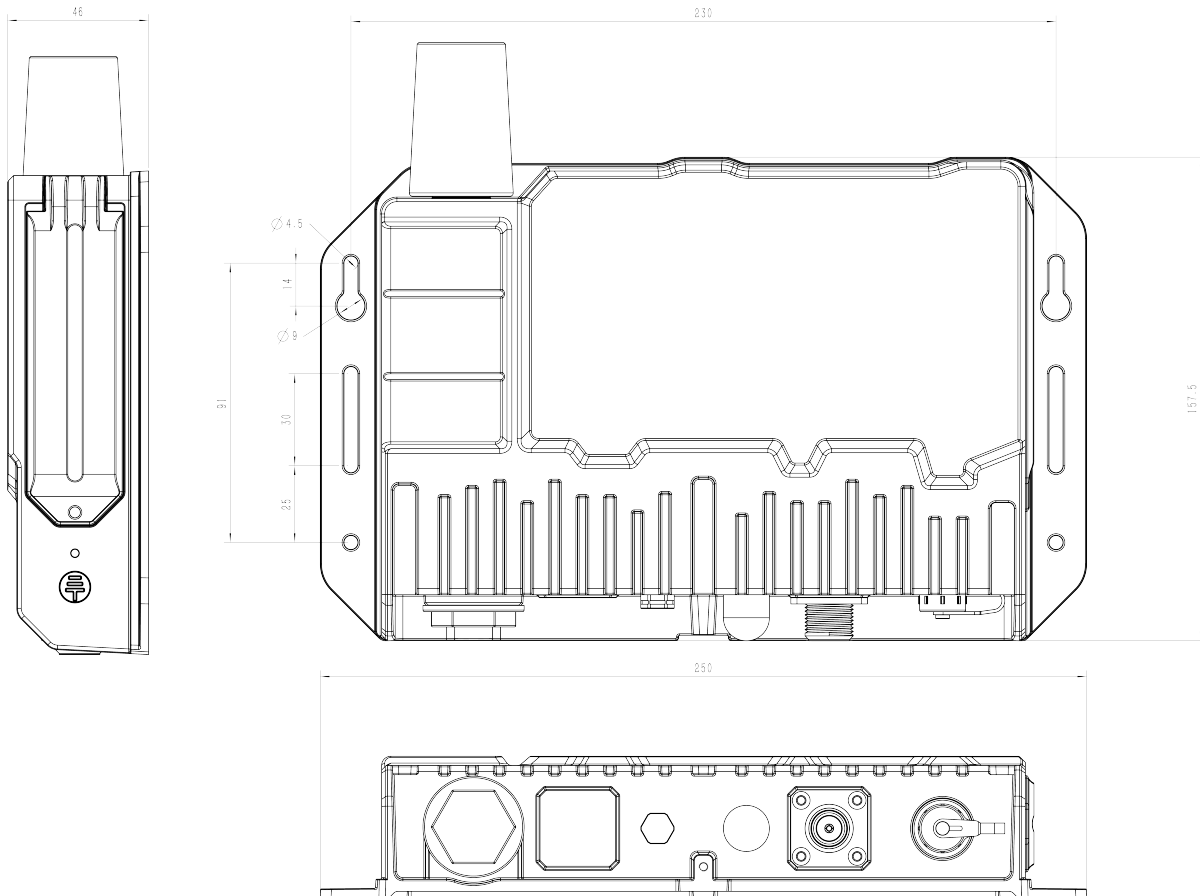
DC Power Connector Definition

The following table shows the pin definition of the DC power connector.

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

Device Dimensions

The following figure shows the device dimensions (unit:mm).



Chapter 3. First Start

This chapter describes the required steps to complete the basic setup, and verify that the gateway is ready for deployment.

Prerequisites

Prepare the following items and information before commissioning the gateway.

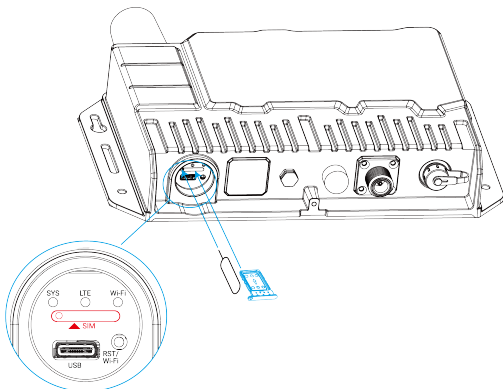
- An activated Nano (4FF) SIM card. APN and PIN information are provided upon demand.
- SIM Card Ejector Tool
- Battery Pack
- LoRaWAN[®] Antenna
- Solar Panel or supported 12-24 VDC external power supply with the M12 cable
- Computer
- (Optional) A working LoRaWAN[®] network server. Recommended that NS adds the gateway first.

Prepare the Gateway

Complete the minimum hardware preparation required for first-time commissioning.

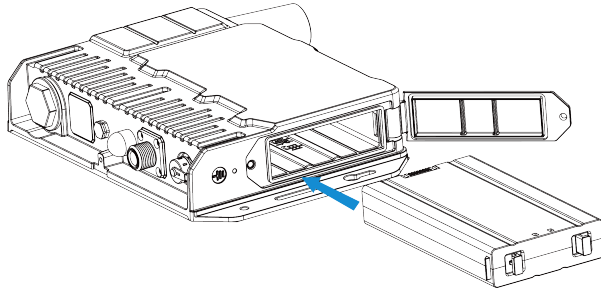
Insert the SIM Card

1. Remove the SIM cover.
2. Use the SIM card ejector tool to open the SIM card tray.
3. Insert the Nano (4FF) SIM card and put the tray back into the gateway.
4. Rotate the SIM cover back into position.

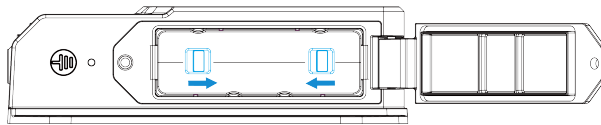


Install the Battery Pack

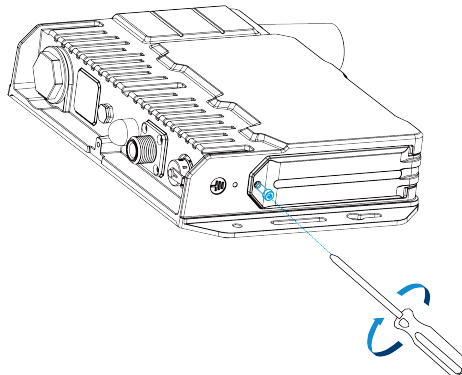
1. Release the fixing screw on the side of the gateway and remove the battery compartment cover.
2. Push the battery pack into the battery compartment.



To remove the battery pack, hold on the latches on the battery.



3. Reinstall the battery compartment cover and secure it with the fixing screw.



i Tip:

- Installing the battery pack does not power on the gateway automatically.
- The battery can only be charged through the DC power connector. USB charging is not supported.

Connect the LoRaWAN[®] Antenna

Connect the LoRaWAN[®] antenna to the LoRaWAN[®] antenna connector for end device communication testing.

Power On the Gateway

1. Connect the M12 power cable of the solar panel to the DC power connector.
2. Wait for the gateway to start. The startup status can be checked via LED indicators.

LED	Expected Status
SYS	A green light indicates that the system is running properly.
Wi-Fi	A static green light indicates that Wi-Fi is on.
LTE	A static green light indicates that the SIM card has registered and cellular dial-up has completed successfully.

**Note:**

If Wi-Fi is disabled, quickly press the button once to turn on Wi-Fi for 10 minutes.

Access the Web GUI

1. Enable Wi-Fi on the computer and connect to the gateway default access point: **Gateway_XXXXXX**.
The SSID can be found on the gateway label.
2. Open a web browser (Chrome is recommended) and enter **https://192.168.23.1**.
3. Enter the default credentials to log in.

Username: **admin**

Password: **password**

4. Change the default password when prompted. The new password must contain at least one letter and one number.

5. Log in to the web GUI using the new credentials.

Complete the Setup Wizard

Follow the setup wizard to complete the basic settings. The wizard can also be skipped or exited if you want to configure the gateway manually.

1. Configure the cellular settings. In most cases, enter the APN required by the cellular operator.
2. Configure the correct system time.
3. Configure the gateway to connect to the required LoRaWAN[®] network server.
4. Configure packet filtering if required.
5. Configure the WLAN settings.

**Note:**

Detailed Cellular, Packet Forward, Packet Filters, and WLAN parameters are described in their corresponding configuration chapters.

Verify the Commissioning Result

After completing the basic configuration, open the **Status** page and check the gateway information.

- Check the configured LoRaWAN[®] region.
- Check the cellular network information and IP address.
- Check the LoRaWAN[®] Packet Forward connection status.
- Add a LoRaWAN[®] end device to the network server and check if it can join the network.

**Note:**

To power off the gateway after commissioning, remove the M12 power cable from the DC power connector.

Chapter 4. Hardware Installation

This chapter describes the preparation and installation procedures for mounting the gateway and its accessories at the deployment site.

**Tip:**

It is suggested to install the gateway on a sunny day for solar panel adjustment and charging.

Prerequisites

Check the Accessories

The gateway with the solar panel can be mounted on a wall or a pole. Select the required mounting method and prepare the corresponding mounting accessories.

Check the SIM Card

Make sure the Nano (4FF) SIM card is installed and the SIM cover is tightened to prevent water from entering the gateway. The specified tightening torque is 0.7 N.m. See [Insert the SIM Card](#).

Check the Battery Pack

Make sure the battery pack is installed in the battery compartment and the compartment cover is secured with the fixing screw. See [Install the Battery Pack](#).

Check the Power Supply

The gateway can be powered by a 12-24 VDC external power supply or the solar panel. The internal battery pack is charged when an external power source is available and can power the gateway when the external supply is disconnected or solar power is insufficient.

Select Installation Location

- The antennas must extend beyond the wall or pillar surface and not be close to the poles or walls. If there are still walls nearby, please keep the antennas at least 35cm away from them.
- Ensure there are no obstacles or metal objects around.
- For better coverage, it is recommended to position the gateway at a higher location, but not the highest position.
- The wall or pole structure shall be sufficiently solid and stable to ensure overall mounting stability.

- Screw mounting positions must avoid internal wall electrical wiring, water pipes and other concealed utilities to prevent structural damage and potential safety hazards.
- Avoid installing the gateway where the device may be exposed to excessive heat. The battery cannot be charged when the device temperature exceeds 50°C.

Install the Mounting Bracket

Select one of the following mounting methods.

Wall Mounting

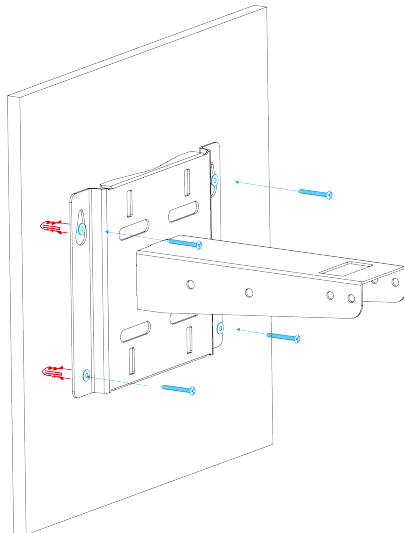
1. Align the mounting bracket horizontally to the target surface, use a pencil to mark four mounting holes.



Note:

The connecting lines of adjacent points are at right angles.

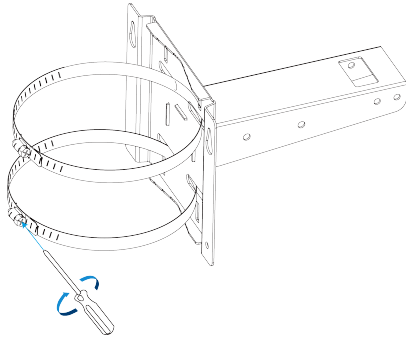
2. Drill four holes in the wall according to the mounting bracket.
3. Insert the wall plugs into the holes.
4. Secure the mounting bracket to the wall with the wall mounting screws.



Pole Mounting

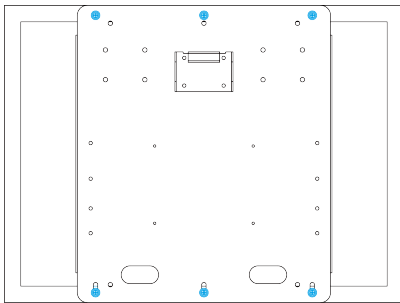
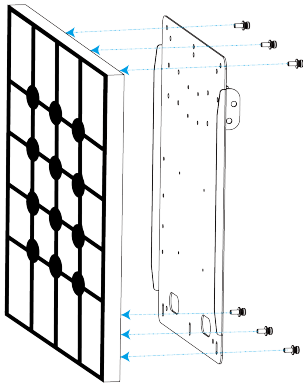
1. Straighten the hose clamps and slide them through the rectangular rings in the mounting bracket.
2. Wrap the hose clamps around the pole.

3. Use a screwdriver to tighten the locking mechanism clockwise.

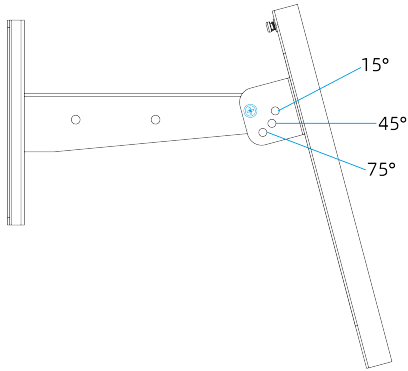


Install the Solar Panel

1. Remove the protective plastics from the four corners of the solar panel.
2. Secure the solar panel to the solar panel bracket with six fixing screws.



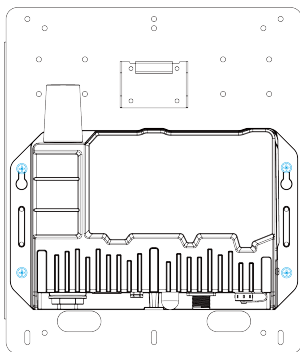
3. Hang the solar panel bracket on the mounting bracket and secure the two parts with two fixing screws first.
4. Adjust the solar panel bracket angle according to the installation environment. The supported installation angles are 15°, 45°, and 75°.



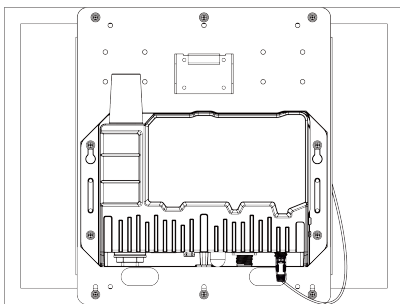
5. Install the remaining two screws to secure the solar panel bracket.

Mount the Gateway

1. Secure the gateway to the opposite side of the solar panel bracket with four screws. It is suggested to install the two upper screws first.



2. Install the LoRaWAN[®] antenna using one of the supported mounting methods.
3. After completing the required hardware installation, connect the M12 power cable of the solar panel to the DC power connector. The gateway powers on automatically.

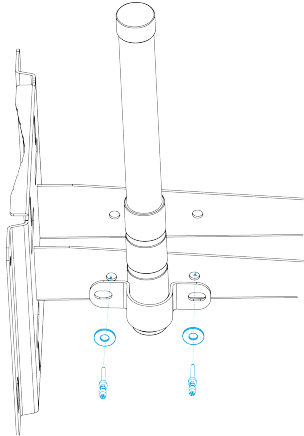


Install the LoRaWAN[®] Antenna

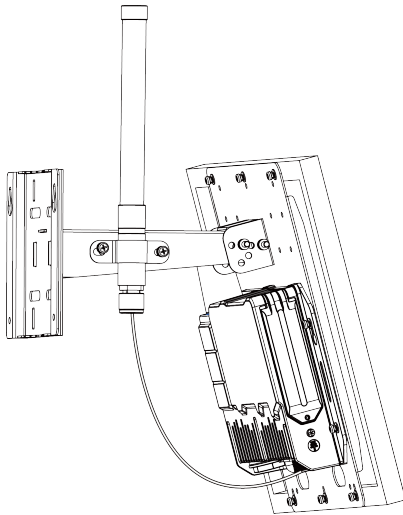
Select the U-strap or U-bolt mounting method according to the deployment.

U-strap Mounting

1. Pass the LoRaWAN[®] antenna through the U-strap clamp.
2. Secure the U-strap clamp to the side of the mounting bracket with two flat washers and two screws.

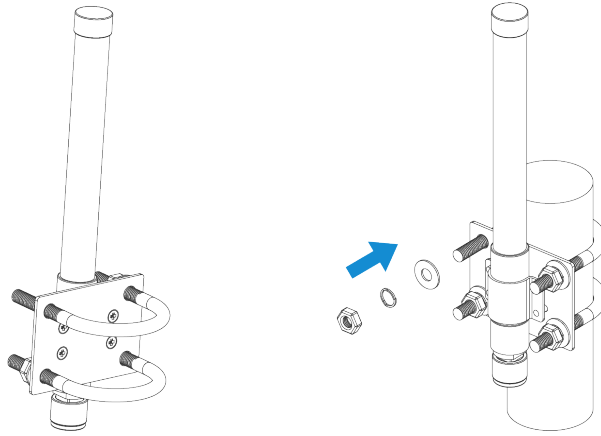


3. Connect one end of the antenna coaxial cable to the LoRaWAN[®] antenna and the other end to the gateway antenna connector.



U-bolt Mounting

1. Pass the LoRaWAN[®] antenna through the antenna clamp and secure it with four screws.
2. Wrap the U-bolt around the pole and secure the clamp with the nuts and other accessories.

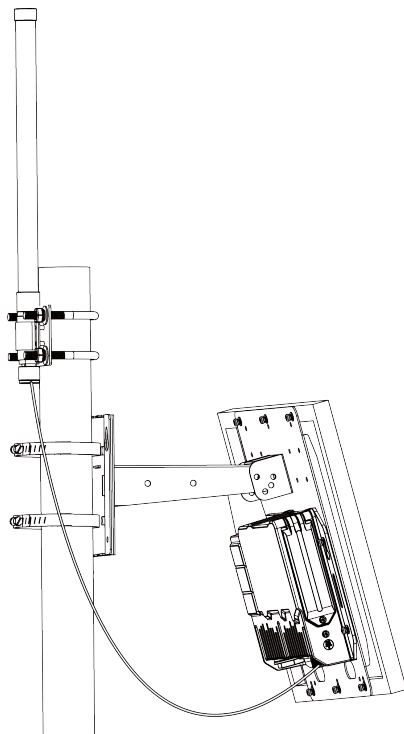


3. Connect one end of the antenna coaxial cable to the LoRaWAN[®] antenna and the other end to the gateway antenna connector.



Tip:

For better antenna signal, it is suggested to install the antenna at the top of the metal pole.



Weatherproof the Antenna Connection

Cover the antenna connector with tape to protect the outdoor connection from bad weather.

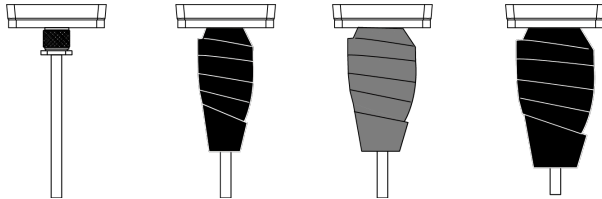
Prerequisites: Electrical Insulation Tapes, 3M Waterproof Tapes



Note:

Install the lightning arrester on the connector before wrapping the tapes if required.

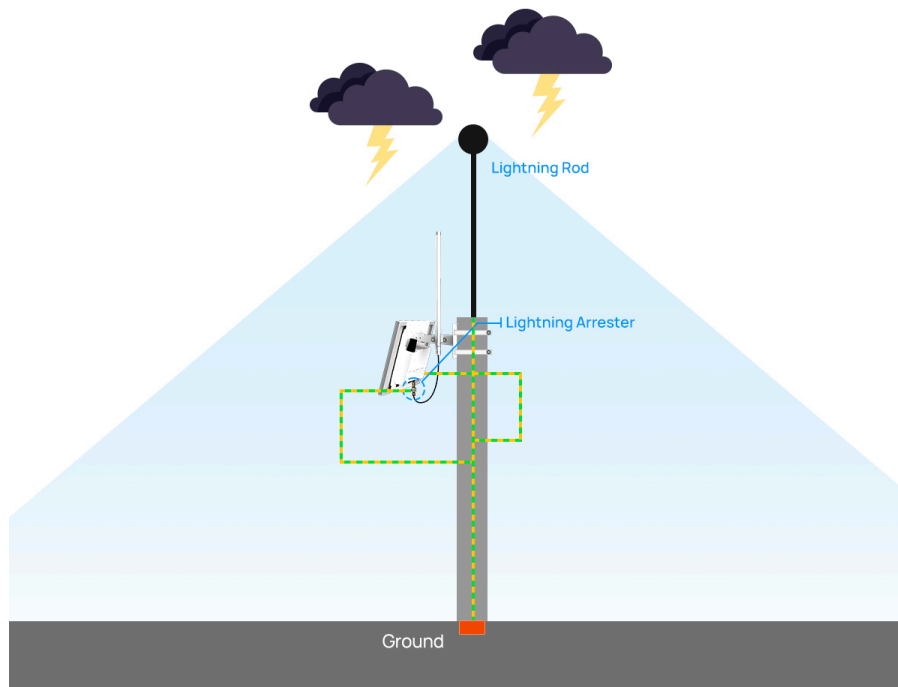
1. Make sure the antenna is installed tightly and clean the connector surfaces.
2. Wrap one layer of electrical insulation tape tightly around the connector, overlapping the previous wrap by 50%.
3. Wrap one layer of 3M waterproof tape tightly around the connector, overlapping the previous wrap by 50%. Stretch the waterproof tape to twice its length while wrapping.
4. Wrap one final layer of electrical insulation tape around the connector with natural uncoiling force, overlapping the previous wrap by 50% and covering the head and tail of the connector.



Lightning Protection and Grounding

Take lightning protection measures, including but not limited to:

- Connect the gateway to earth ground.
- Add a lightning arrester to the antenna connector.
- Make sure the antennas are lower than the highest position of the building and the gateway and antennas are within the protection range of the lightning rod.
- If there is no lightning rod nearby, make sure the gateway is not installed in an area influenced by lightning, or install a lightning rod above the antennas.
- The cross-sectional area of the earthing wire should be more than 10 AWG.



Chapter 5. Power Management

This chapter describes how the SG50 uses external power, the solar panel, and the internal battery, and provides battery and solar panel maintenance information.

Power Supply

The SG50 can be powered by either a 12-24 VDC external power supply or a solar panel. When an external power source is available, the internal battery pack is also charged. If the external power supply is disconnected or the solar panel cannot provide enough power, the internal battery pack can supply power to the gateway.

Battery Charging and Operating Conditions

Observe the following conditions when charging and operating the internal battery pack.

Condition	Description
Charging Interface	The battery can only be charged through the DC power connector. USB charging is not supported.
Temperature above 50°C	The battery cannot be charged when the device temperature is above 50°C. Avoid direct exposure of the device to sunlight.
Temperature below 0°C	If the device temperature is below 0°C and the solar panel provides more than 7 W, the gateway heats the battery until the temperature reaches 10°C. If the battery is not fully charged, charging then starts.

Battery Care and Storage

If the battery is not used for an extended period, it may become over-discharged and its health may be affected. Charge the battery regularly, at least once every three months, to avoid over-discharge.

Solar Panel Maintenance

Clean the solar panel surface regularly or according to local environmental conditions. Dust, sand, bird droppings, and other environmental factors on the solar panel surface can reduce charging efficiency.

Chapter 6. Web GUI Configuration

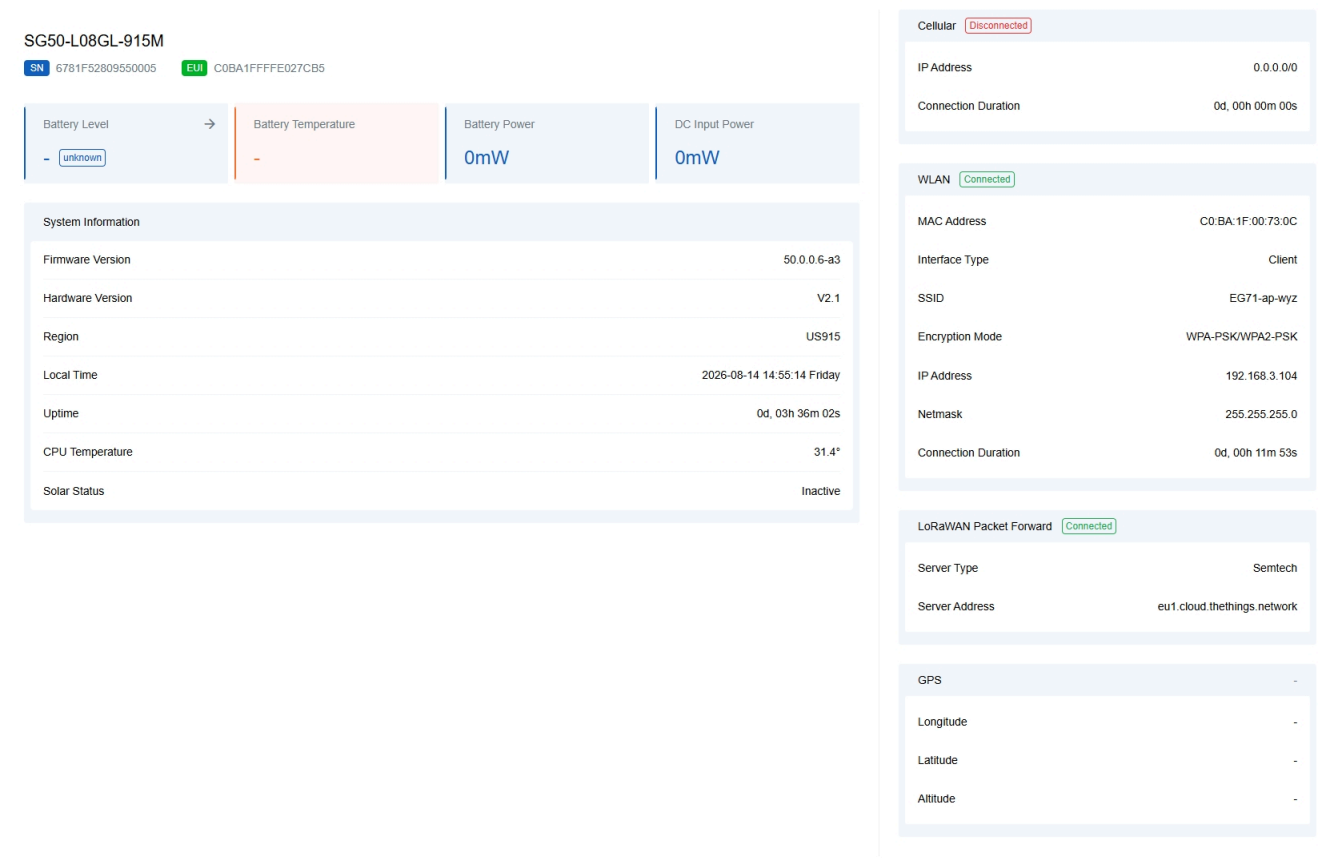
This chapter describes the web GUI configuration for the gateway. Before starting configuration, make sure you have [accessed the web GUI](#).

Status

The Status page displays the device's basic information and operational status.

Overview

The top of the page displays the model, serial number, and EUI. Click the widgets in the figure to learn more.



1. [#unique_9_Connect_42_battery-power-info](#)
2. [System Information](#)
3. [Cellular](#)
4. [WLAN](#)

5. [LoRaWAN Packet Forward](#)

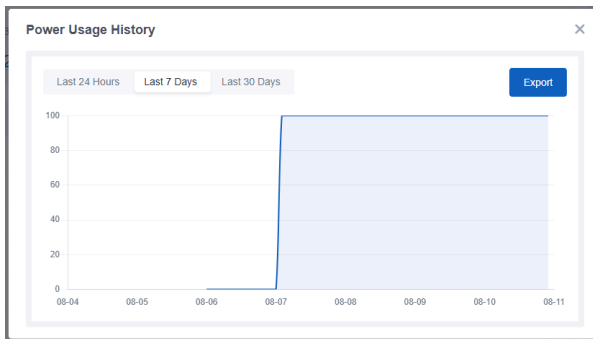
6. [GPS](#)

Battery & Power Information

The widget displays the current battery and power information.



Battery Level: The level of the battery and charging status. Click this to check the power usage history and export the hourly history record as a CSV file. The history record can store data for up to 30 days.



Battery Temperature: The temperature of the battery.

Battery Power: Battery input/output power. A positive value indicates charging, and a negative value indicates discharging.

DC Input Power: The input power when the gateway is connected to an external DC input or a solar panel.

System Information

The widget displays the basic system information and solar powering status.

System Information	
Firmware Version	50.0.0.6
Hardware Version	V2.1
Region	US915
Local Time	2026-08-14 14:55:14 Friday
Uptime	0d, 03h 36m 02s
CPU Temperature	31.4°
Solar Status	Inactive

Cellular

The widget displays the cellular connection status, IP address and connection duration.

Cellular	Connected
IP Address	10.160.123.117
Connection Duration	0d, 12h 05m 52s

WLAN

The widget displays the WLAN MAC address, working status and connection information.

WLAN Connected	
MAC Address	C0:BA:1F:00:73:0C
Interface Type	Client
SSID	EG71-ap-wyz
Encryption Mode	WPA-PSK/WPA2-PSK
IP Address	192.168.3.221
Netmask	255.255.255.0
Connection Duration	0d, 12h 06m 20s

LoRaWAN Packet Forward

The widget displays the packet forwarder connection status, server type and the server address.

LoRaWAN Packet Forward Connected	
Server Type	Semtech
Server Address	eu1.cloud.thethings.network

GPS

The widget displays the location of the gateway. The values are displayed only when the gateway is outdoors.

GPS	-
Longitude	-
Latitude	-
Altitude	-

Cellular

The page displays the cellular connection status and cellular network information. Click the widgets in the figure to learn more.

The screenshot displays the Cellular configuration page with two main sections: SIM and NET.

SIM Section:

- Status: Ready
- Register Status: Registered (Home network)
- Modem Information Table:

Modem	
Model	EG915Q-NA
Version	EG915QNALCR01A05M04_01.003.01.003
Signal Level	23 asu(-67 dbm)
IMEI	867507066654670
IMSI	460115212149201
ICCID	89860325245924625528
ISP	CHN-CT
Network Type	FDD LTE
PLMN ID	46011
LAC	5F0C
Cell ID	E6D915

NET Section:

- Status: Connected
- Connection Duration: 0d, 11h 27m 28s
- Network Information Table:

Network	
IPv4 Address	10.160.123.117/32
IPv4 Gateway	10.64.64.64
IPv4 DNS	8.8.8.8

1. [Modem](#)
2. [Network](#)

Modem

The widget displays the SIM registration status, SIM registration information, and cellular module information.

SIM

Ready

Register Status: Registered (Home network)

Modem	
Model	EG915Q-NA
Version	EG915QNALCR01A05M04_01.003.01.003
Signal Level	23 asu(-67 dbm)
IMEI	867507066654670
IMSI	460115212149201
ICCID	89860325245924625528
ISP	CHN-CT
Network Type	FDD LTE
PLMN ID	46011
LAC	5F0C
Cell ID	E6D915

SIM status reference:

- 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

Network

This widget displays the cellular network connection status and the connected IP information.

NET

Connected

Connection Duration: 0d, 11h 27m 28s

Network	
IPv4 Address	10.160.123.117/32
IPv4 Gateway	10.64.64.64
IPv4 DNS	8.8.8.8

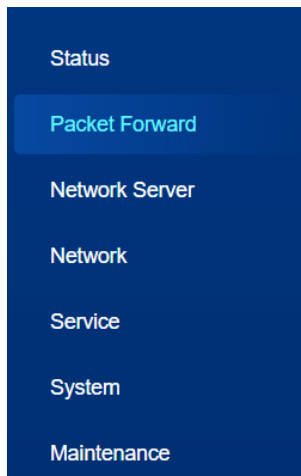
Packet Forward

The gateway can work as a packet forwarder to set up communication between LoRaWAN[®] end devices and a LoRaWAN[®] network server. This chapter describes how to configure and monitor the packet forwarder.

General

This section is used to configure the packet forwarding destination and the connection parameters for the selected network server type.

1. On the left bar, select **Packet Forward** page.



2. On the top bar, select **General** tab.
3. Configure the packet forward parameters as required.

EUI

C0BA1FFFE027CB5

Gateway ID *

C0BA1FFFE027CB5

Destination

Enable

☒

Type

Embedded NS

Connected

Parameter	Description
EUI	The unique identifier of the gateway. This value is not editable.
Gateway ID	The customizable ID used to register the gateway to a network server, such as The Things Network. By default, it is the same as the gateway EUI.
Destination	
Enable	Enable or disable the packet forward feature.
Type	Select the packet forward type. Semtech: Connect to a network server through the Semtech UDP protocol. It supports most mainstream network servers. ChirpStack-Generic: Connect to ChirpStack v3 through a generic MQTT gateway bridge. ChirpStack-v4: Connect to ChirpStack v4 through an MQTT forwarder. Basic Station: Connect to a network server through TCP. LNS and CUPS do not both need to be configured. Remote Embedded NS: Connect to the embedded network server of a Milesight controller gateway like UG65. Embedded NS: Connect to the embedded network server of this gateway. DeviceHub LNS: Connect to Milesight DeviceHub LNS. Enable DeviceHub 2.0 on the Service > Device Management page first. Milesight Development Platform LNS: Connect to Milesight Development Platform LNS. Enable Milesight Development Platform on the Service > Device Management page.
Semtech	
Server Address	The IP address or domain name of the LoRaWAN [®] network server.

Parameter	Description
Port Up	The UDP port used to forward uplinks from end devices to the network server.
Port Down	The UDP port used to forward downlinks from the network server to end devices.
Data Re-transmission	When the network is disconnected, the gateway can store up to 500 uplink packets and retransmit them to the network server after the network recovers. Pending Data: Display the number of packets to be retransmitted.  Note: The gateway does not save Join Request packets.
Basic Station	
URI	The URL of the LoRaWAN[®] network server. Use the following format and replace the server address and port with the actual values. LNS URI: wss://<server-address>:<port> Or ws://<server-address>:<port> CUPS URI: https://<server-address>:<port>
CA File	The CA certificate used to secure the server domain.  Note: Change the certificate file format to .trust before importing it.
Client Certificate File	The client certificate used to verify the identity of the gateway.
Client Key File	The private key used to verify the identity of the gateway.
GPS	When connecting through LNS, enable or disable forwarding the gateway GPS data to the network server.
Data Re-transmission	When the network is disconnected, the gateway can store up to 500 uplink packets and retransmit them to the network server after the network recovers. Pending Data: Display the number of packets to be retransmitted.

Parameter	Description
	 Note: The gateway does not save Join Request packets.
ChirpStack-Generic/ChirpStack-v4	
Server Address	The IP address or domain name of the LoRaWAN [®] network server.
MQTT Port	The network server port used for the MQTT connection.
Region ID	The region ID for a ChirpStack-v4 server. This value is entered automatically when Supported Freq is changed on the Packet Forward > Radios page.
User Credentials	When enabled, enter the username and password used for authentication.
TLS Authentication	Enable or disable TLS authentication. Mode: Select the certificate mode as CA Signed Server Certificate to use pre-loaded certificates, or Self Signed Certificates to import the custom CA certificate, client Certificate and client key for verification. SSL Security: After enabled, the gateway will verify the certificate's validity.
Data Re-transmission	When the network is disconnected, the gateway can store up to 500 uplink packets and retransmit them to the network server after the network recovers. Pending Data: Display the number of packets to be retransmitted.  Note: The gateway does not save Join Request packets.
Remote Embedded NS	
Server Address	The IP address or domain name of the Mulesight controller gateway.
MQTT Port	The communication port of the Mulesight controller gateway.
Data Re-transmission	When the network is disconnected, the gateway can store up to 500 uplink packets and retransmit them to the network server after the network recovers. Pending Data: Display the number of packets to be retransmitted.

Parameter	Description
	 Note: The gateway does not save Join Request packets.

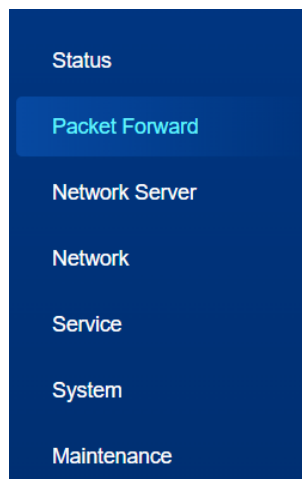
- Click **Save & Apply** to save the settings.
- Check if both the gateway and the network server show the status is **Connected**.

Radios

This section is used to configure the LoRaWAN[®] frequency plan and radio channels.

Basic Settings

- On the left bar, select **Packet Forward** page.



- On the top bar, select **Radios** tab.
- Configure the radio channel parameters as required.

Radio Channel Setting

Supported Freq
US915
Noise Scan

Radio 0
905.7

Radio 1
905.5

Multi Channels Setting

Enable	Radio	Frequency/MHz
☒	Radio 0	905.5
☒	Radio 0	905.7
☒	Radio 0	905.9
☒	Radio 0	906.1
☒	Radio 1	906.3
☒	Radio 1	906.5

Parameter	Description
Radio Channel Setting	
Support- ed Freq	The LoRaWAN[®] frequency plan used for uplink and downlink frequencies and data rates. The available options depend on the gateway model. -470M: CN470 -868M: EU868, RU864, IN865 -915M: US915, AU915, KR920, AS923-1&2&3&4
Radio 0/Radio 1	The center frequencies used to receive packets from LoRaWAN [®] end devices.
Noise Scan	Sweep the noise of specific frequency change and give a diagram for users to analyze the environmental interference condition and select the best deployment. See here for details.
Multi Channels Setting	
Enable	Enable or disable this channel to receive packets.
Radio	Select Radio 0 or Radio 1 as the center frequency.
Frequen- cy/MHz	Set the frequency of this channel. Range: center frequency $\pm$ 0.4625.

- (Optional) Configure the LoRa/FSK channel settings if you require the private communication.

| LoRa Channel Setting

Enable	☒
Radio	Radio 0
Frequency/MHz	904.6
Bandwidth/kHz	500KHz
Data Rate/Bit	SF8

| FSK Channel Setting

Enable	☐
Radio	Radio 0
Frequency/MHz	904.6
Bandwidth/kHz	250KHz
Data Rate/Bit	50000

Parameter	Description
Enable	Enable or disable this channel to transmit packets.
Radio	Select 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.

- Click **Save & Apply** to save the settings.

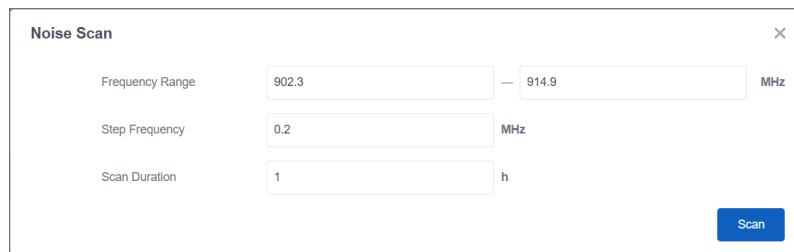
Noise Scan

Prerequisites

- The device is placed to the target location. If the installation location is changed, reproduce the noise scan.
- This feature will impact LoRaWAN[®] downlink transmission, so do not send downlink commands to devices during sweeping.

Steps

1. Click **Noise Scan**.
2. In the pop-up window, configure the scan conditions.

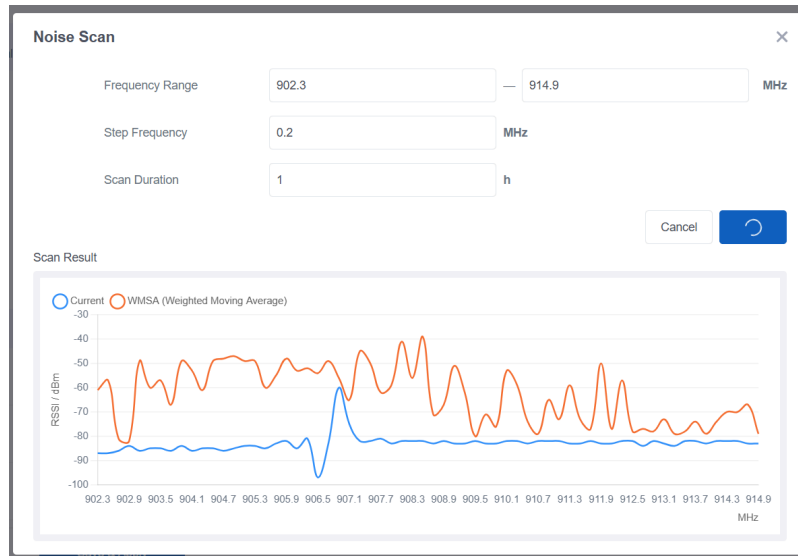


The image shows a 'Noise Scan' configuration window with a close button (X) in the top right corner. It contains three input fields: 'Frequency Range' with values 902.3 and 914.9, 'Step Frequency' with value 0.2, and 'Scan Duration' with value 1. Each field has a unit indicator (MHz for frequency, h for duration). A blue 'Scan' button is located at the bottom right.

Parameter	Description
Frequency Range	The frequency range to scan.
Step Frequency	The step for each frequency channel to be scanned.
Scan Duration	Custom the time to sweep the frequencies.  Tip: To ensure the accurate result, it is recommended to set the sweep time as 24h.

3. Click **Scan**. The gateway will scan until the scan duration reaches. To stop scanning in advance, click **Cancel**.

4. Check the scan result. The lower the RSSI value, the better the signal.



Packet Filters

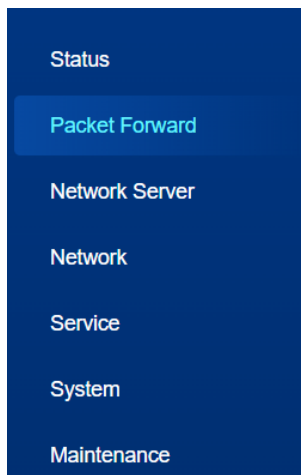
This section is used to filter uplink packets by different conditions to reduce network congestion, save network traffic, and help ensure safe operation.



Note:

When the destination type is **Embedded NS**, this feature does not work.

1. On the left bar, select **Packet Forward** page.



2. On the top bar, select **Packet Filters** tab.
3. Configure the packet filter parameters as required.

Proprietary Message Filter ☒

Filters by NetID ⓘ

Mode ☐ White List ☒ Black List

List +

Filters by JoinEUI ⓘ

Mode ☒ White List ☐ Black List

List To +

Filters by DevEUI ⓘ

Mode ☒ White List ☐ Black List

List To +

Parameter	Description
Proprietary Message Filter	Enable to prevent proprietary message packets (Mtype=111) from being forwarded.
Filters by NetID	Forward or do not forward uplink packets that match the NetID.
Filters by JoinEUI	Forward or do not forward Join Request packets that match the JoinEUI range.
Filters by DevEUI	Forward or do not forward Join Request packets that match the DevEUI range.
Mode	Select the filter mode as black list or white list. White List: Only forward packets included in the list to the network server. Black List: Forward packets other than those included in the list to the network server.
List	Set the specific filtering value or range. Each condition supports up to five lists.

4. Click **Save & Apply** to save the settings.

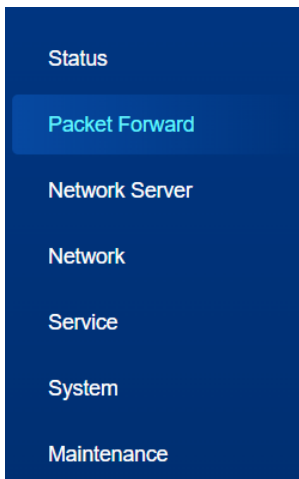
**Note:**

1. When JoinEUI and DevEUI are both configured, only packets that meet both conditions are forwarded.
2. When a third-party network server assigns filter conditions to the gateway, the gateway prioritizes to the network server settings.

Advanced

This section is used to configure beacon, keepalive, LBT, and expert packet forwarder settings.

1. On the left bar, select **Packet Forward** page.



2. On the top bar, select **Advanced** tab.
3. Configure the advanced parameters as required.

| Beacon Setting

Beacon Period ☒ 0 ☐ 128

| Intervals Setting

Keep Alive Interval/s

Stat Interval/s

Push Timeout/ms

| LBT Settings

Enable ☐

RSSI Target

| Expert Options ⓘ

Enable ☐

Parameter	Description
Beacon Setting	
Beacon Period	The interval at which the gateway sends beacons for Class B device time synchronization. A value of 0 means that the gateway does not send beacons. Select 128 when the end device type is Class B.
Intervals Setting	
Keep Alive Interval	The interval at which the gateway sends keepalive packets to the network server to keep the connection active.
Start Interval	The interval at which the gateway updates the network server with gateway statistics.
Push Timeout	The timeout for waiting for a response from the server after the gateway sends data.
LBT Setting	
Enable	Enable or disable LBT. Listen before talk (LBT) detects whether the downlink channel is idle to help avoid channel access conflicts.

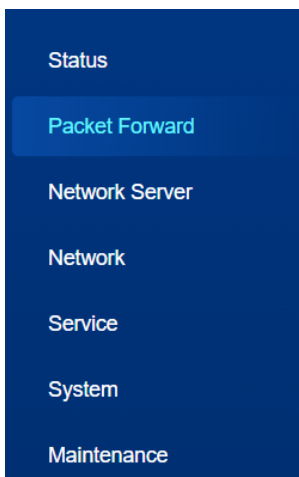
Parameter	Description
	 Note: AU915 and US915 do not support LBT.
RSSI Target	The criterion for determining an idle channel. If the actual RSSI of a channel is lower than the target, the channel is considered idle.
Expert Options	
Enable	When enabled, the gateway supports a customized configuration file for the packet forwarder. The customized configuration overrides the packet forward settings in the web GUI. Click Example to open the reference page for the correct configuration file format.

- Click **Save & Apply** to save the settings.

Traffic

This section is used to view the latest traffic received from end devices or the network server. The gateway displays up to 30 traffic records.

- On the left bar, select **Packet Forward** page.



- On the top bar, select **Traffic** tab.
- View the traffic records.

General	Radios	Packet Filters	Advanced	Traffic				Refresh
Direction	Time	Frequency	Datarate	Channel	RSSI	SNR	Data	
Down	0000-00-00T00:00:00.000000Z	924.500000	SF9BW500	0			YFkFIQcgLjpSNk7N	
Up	0000-00-00T00:00:00.000000Z	905.900000	SF9BW125	2	-79	12.5	gFkFIQcAOUIARue9gBop	
Up	0000-00-00T00:00:00.000000Z	905.700000	SF7BW125	1	-100	-6.2	gA4VTwaAlgVBduyah6Vuf9naiaKDnw02QgLEhmyT...	
Down	0000-00-00T00:00:00.000000Z	925.700000	SF9BW500	0			YFkFIQeLTofA2jijLjKjwU=	
Up	0000-00-00T00:00:00.000000Z	906.300000	SF9BW125	4	-86	9.5	gFkFIQcAOEJVdKD3HlwPoBpTknq7vqERDIXAw+S...	
Down	0000-00-00T00:00:00.000000Z	927.500000	SF9BW500	0			YCiGqwYgFDZ0vS4o	
Up	0000-00-00T00:00:00.000000Z	906.900000	SF9BW125	7	-87	8.8	gCiGqwYAIT8A6Zw6Dp4T	
Down	0000-00-00T00:00:00.000000Z	926.900000	SF9BW500	0			YCw9wYghDSI1tyY	
Up	0000-00-00T00:00:00.000000Z	906.700000	SF9BW125	6	-84	10.8	gCw9wYAKEEA3t3W7vm0	
Down	0000-00-00T00:00:00.000000Z	923.900000	SF9BW500	0			YCiGqwalEzYFA2jijKuvPL4=	
Down	0000-00-00T00:00:00.000000Z	923.300000	SF9BW500	0			YHuXywelbTYFA2jijN6k6GQ=	
Up	0000-00-00T00:00:00.000000Z	905.700000	SF9BW125	1	-82	9.2	gCiGqwYAlD9VdnlRNlq1oEJjdDorjUa5Lny+JaW38S...	

Parameter	Description
Refresh/Stop	Refresh: Click to refresh the page and update the latest data automatically. Stop: Click to stop automatic page updates.
Direction	The transmission direction of the packet.
Time	The time when the packet is received.
Frequency	The frequency used to receive or send the packet.
Datarate	The data rate of the packet.
Channel	The frequency channel used to receive or send the packet.
RSSI	The received signal strength of the packet.
SNR	The signal-to-noise ratio of the packet.
Data	The encrypted data of the packet.

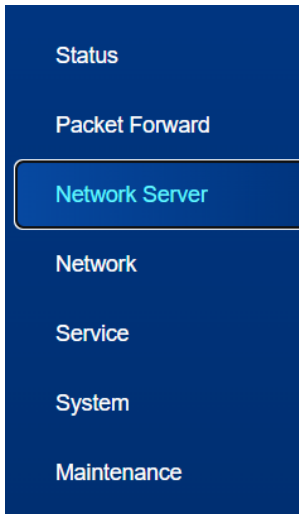
Network Server

The gateway can work as a LoRaWAN[®] network server when the packet forwarder type is set to **Embedded NS**. This chapter describes how to use the gateway embedded network server.

General

This section is used to configure the global channel plan settings for the network server.

1. On the left bar, select **Network Server** page.



2. On the top bar, select **General** tab.
3. Configure the global channel plan parameters as required.

Global Channel Plan Setting

Channel Plan: KRS20

If you want to modify Channel Plan, please go to [Packet forwarder]-[Radio] .

Channel: 0-2

Additional Channels

Frequency(MHz)	Min Datarate	Max Datarate
+		

Parameter	Description
Channel Plan	Display the current channel plan. This can be changed in Packet Forward > Radio page.
Channel	Allow end devices to communicate via specific frequency channels by entering the channel indexes. Examples: 1,40: Enable Channel 1 and 40 1-40: Enable Channel 1-40 1-40, 60: Enable Channel 1-40 and 60 Null: Enable all channels

Parameter	Description
Addition- al Channels	Click plus icon to add channels not defined by the LoRaWAN [®] Regional Parameters. This parameter only works with channel plans other than US915/AU915/CN470.

4. Click **Save & Apply** to save the settings.

Devices

This section is used to add and manage LoRaWAN[®] end devices. The gateway supports up to 100 devices.

Prerequisites:

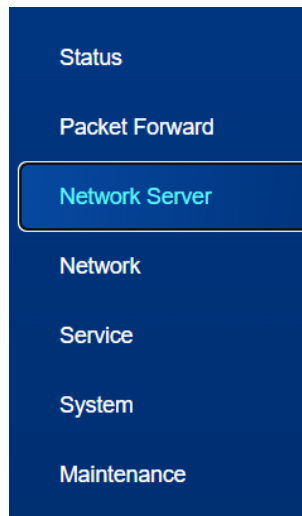
- The end device class type is Class A or Class C.
- Obtain the device information from the vendor.

Add Batch Import Delete DeviceEUI									
☐	DeviceName	DeviceEUI		Class	Join Type	Application	Activated	Create Time	Last Seen
☐	50	24e124		Class C	OTAA		✓	2026-08-07 10:39:29+0100	49 seconds ago
☐	49	24e124		Class C	OTAA		✓	2026-08-07 10:39:29+0100	34 seconds ago
☐	48	24e124		Class C	OTAA		✓	2026-08-07 10:39:29+0100	44 seconds ago
☐	47	24e124		Class C	OTAA		✓	2026-08-07 10:39:29+0100	1 mins ago
☐	46	24e124		Class C	OTAA		✓	2026-08-07 10:39:29+0100	38 seconds ago
☐	45	24e124		Class C	OTAA		✓	2026-08-07 10:39:29+0100	26 seconds ago
☐	44	24e124		Class C	OTAA		✓	2026-08-07 10:39:29+0100	1 mins ago
☐	43	24e124		Class C	OTAA		✓	2026-08-07 10:39:29+0100	1 seconds ago
☐	42	24e124		Class C	OTAA		✓	2026-08-07 10:39:29+0100	53 seconds ago
☐	41	24e124		Class C	OTAA		✓	2026-08-07 10:39:29+0100	33 seconds ago

The gateway supports adding a device individually or batch importing devices. Please select one method to add devices.

Add a Single Device

1. On the left bar, select **Network Server** page.



2. On the top bar, select **Device** tab.
3. Click **Add** and configure the device related parameters.

Add Devices
✕

* DeviceName

Description

* DeviceEUI

* Class

Class A ▾

* Join Type

OTAA ▾

* Appkey

* DevAddr

* NwkSkey

* AppSkey

▼ Advanced Settings

* RX1 Datarate Offset

0 ▾

* RX2 Datarate

DR8 (SF12, 500kHz) ▾

RX2 Channel Frequency/Hz

923300000

Device Channel

Range 0-63, separate multiple val

* Uplink Frame-counter

0

* Downlink Frame-counter

0

* FPort

1

Cancel

Add Next

Add

Parameter	Description
Device Name	Define a unique name for the device.
Description	For noting this device.
Device EUI	The unique 16-digit hexadecimal EUI of the device.
Class	Select the device class type from Class A and Class C .
Join Type	Select the device join type from OTAA and ABP .

Parameter	Description
App Key	When join type is OTAA, set the 32-digit hexadecimal Application Key value.
DevAddr	When the join type is ABP, set the 8-digit hexadecimal Device Address.
NwkSKey	When the join type is ABP, set the 32-digit hexadecimal Network Session Key value.
AppSKey	When the join type is ABP, set the 32-digit alphanumeric Application Session Key value.
Advanced Settings	RX1 Datarate Offset: The offset used to calculate the RX1 data rate based on the uplink data rate.
	RX2 Datarate: The data rate of RX2 window.
	RX2 Channel Frequency: The frequency of RX2 window.
	Device Channel: Allow the device to communicate via specific frequency channels by entering the channel indexes. This parameter only works with CN470/US915/AU915 channel plans. Examples: 1,40: Enable Channel 1 and 40 1-40: Enable Channel 1-40 1-40, 60: Enable Channel 1-40 and 60 Null: Enable all channels
	Class C ACK Timeout: The time to wait for a downlink response from class C devices. If no response is received within this time, the gateway will retransmit the downlink command.
Uplink Frame-counter	When the join type is ABP, set the uplink frame-counter.
Downlink Frame-counter	When the join type is ABP, set the downlink frame-counter.
FPort	FPort (Frame Port) is a single-byte field in the MAC payload that identifies the type or destination of the data. For Mile-sight end devices with default settings, the FPort is 85.

Parameter	Description
Frame-counter Validation	Enable or disable to prevent replay attacks.

- Click **Add** to complete the addition, or click **Add Next** to add a new device.
- Check if the device status is activated. If not, navigate to **Network Server > Packets** to check for communication between the device and the gateway.

Batch Import Devices

- On the left bar, select **Network Server** page.

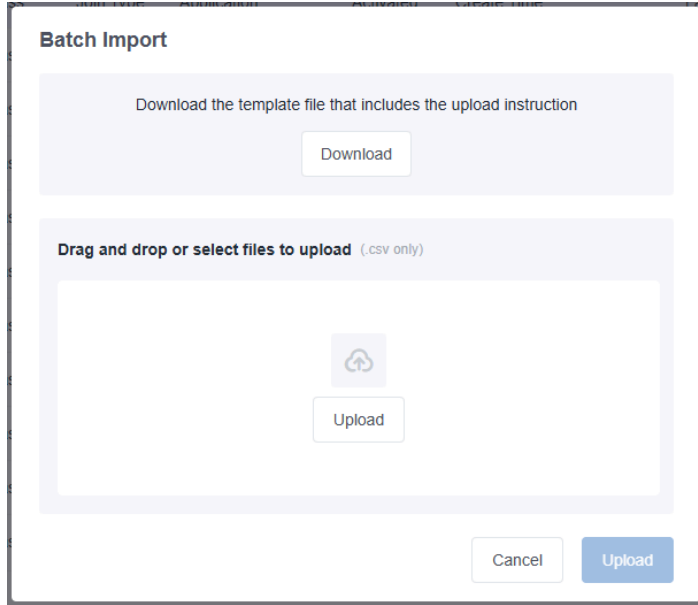


- On the top bar, select **Device** tab.
- Click **Batch Import**.
- In the pop-up window, download the template file and add the device information to the template file.



Note:

When editing template files, do not delete the table headers or the instructions at the top.



The image shows a 'Batch Import' dialog box. At the top, it says 'Batch Import'. Below this, there is a light blue box with the text 'Download the template file that includes the upload instruction' and a 'Download' button. Below that, there is another light blue box with the text 'Drag and drop or select files to upload (.csv only)'. Inside this box is a large white area with a cloud icon and an 'Upload' button. At the bottom right of the dialog, there are 'Cancel' and 'Upload' buttons.

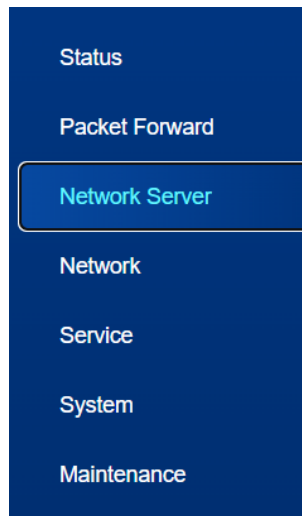
5. Select the device file to upload or drag the file to the target box.
6. Click **Upload**. If upload failed, an error message will pop-up; if upload successfully, the devices will be added to the **Devices** page.

Application

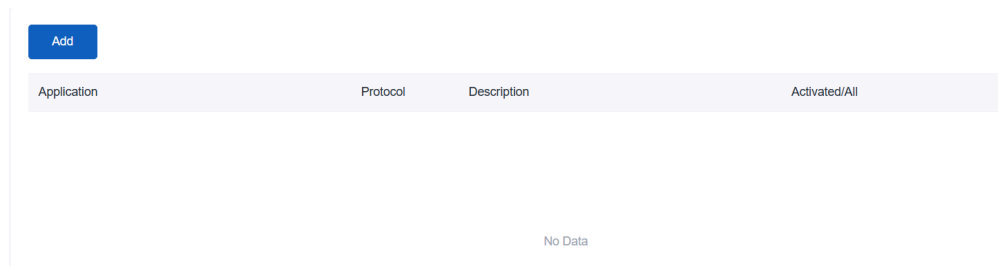
This section is used to add and manage applications. An application is a collection of devices with the same purpose/of the same type. Users can add a series of devices to the same application that need to send data to the same server. The gateway supports adding up to three applications, and each application can only connect to one server.

Add an Application

1. On the left bar, select **Network Server** page.



2. On the top bar, select **Application** tab.
3. Click **Add** to add a new application.



4. Configure the application basic info, then click **Next**.

← Add Application

1

2

Basic Information

Add Device

Application

Description

Protocol

MQTT

Parameter	Description
Application	Define a unique name for the application.
Description	For noting this application.
Protocol	Select the transmission protocol to connect to the remote server from MQTT , HTTP and HTTPS .

5. Select the devices to add to this application, or click plus icon in the top right to add a new device. Then click **Save**.

Device Name	Description	Device EUI	Join Type	Class	Activated
☒ 50		24e1244060574a64	Class C	OTAA	✓
☐ 49		24e1244060573876	Class C	OTAA	✓
☐ 48		24e1244060578c9c	Class C	OTAA	✓
☐ 47		24e124406057d96d	Class C	OTAA	✓
☐ 46		24e124406057bd03	Class C	OTAA	✓
☐ 45		24e124406057ab94	Class C	OTAA	✓

6. Navigate **Device** page to add or delete devices, or navigate to **HTTP/HTTPS/MQTT** page to configure server info. For details, refer to the following content.

Manage Device in an Application

1. Select the desired application, click .
2. Under **Device** tab, click **Add** to add devices to this application, or select target devices and click **Delete** to remove them from the application.

DeviceName	DeviceEUI	Class	Join Type	Application	Activated
☐ 50	24e1244060574a64	Class C	OTAA	test	✓

Configure MQTT/HTTP/HTTPS Settings

1. Select the desired application, click .
2. Under **MQTT/HTTP/HTTPS** tab, configure the server parameters.

HTTP/HTTPS

Parameter	Description
Name	Define a unique name for this server.

Parameter	Description
Enable	Enable or disable to forward data to a HTTP(s) server.
HTTP Headers	Click plus icon to add an HTTP header name and value.
Data Topic	Set the URL to send different types of data. For more details, refer to MQTT&HTTP Application Guide. Uplink Data: Device data uplinks. Join Notification: Device join request packets. ACK Notification: ACK notification after sending confirmed downlink commands to LoRaWAN[®] devices. Gateway Info: Gateway basic information and network status. Gateway Event: Gateway alarm event.

MQTT

Parameter	Description
Name	Define a unique name for this server.
Enable	Enable or disable to set up the communication with a MQTT broker.
General	
Broker Address	The IP address or domain name of the MQTT broker.
Broker Port	The service port of the MQTT broker.
Client ID	The unique identifier of the gateway.
Keep Alive Interval	The interval to send heartbeat packets regularly to keep alive.
Data Re-transmission	When enabled, it supports storing up to 100 packets when the network is disconnected and re-transmits the data after network recovery.
Auto Re-connect	If the connection is lost, the attempt to reconnect will be made automatically.

Parameter	Description
	Reconnect Period: The interval to reconnect the server.
Clean Session	When enabled, the connection will create a temporary session, and all information will be lost when the client is disconnected from the broker; when disabled, the connection will create a persistent session that will remain and save offline messages until the session logs out over time.
User Credentials	Enable or disable to authenticate with username and password. Username: The username for authentication. Password: The password for authentication.
TLS	Enable or disable TLS authentication. Mode: Select the certificate mode as CA Signed Server Certificate to use preloaded certificates, or Self Signed Certificates to import the custom CA certificates(.crt or .pem), client Certificates(.crt) and client key(.key) for verification. SSL Security: After enabled, the gateway will verify the certificate's validity.  Tip: If MQTT broker type is HiveMQ, enable TLS and set the mode as CA signed Server Certificate.
Last Will and Testament	Enable or disable sending a will message. The last will message will be sent automatically when the MQTT client is disconnected abnormally. It is typically used to send device status information or notify other devices or proxy servers of the device's offline status.

Parameter	Description
	Last-Will Topic: The topic to receive last will messages. Last-Will QoS: QoS0, QoS1 and QoS2 are optional. Last-Will Retain: Enable or disable to set last will message as retain message. Last-Will Payload: The content of the last will message.
Data Topic	
Data Type	The data type to communicate with MQTT broker. For more details, refer to MQTT&HTTP Application Guide. Uplink Data: Receive device uplink packets. Downlink Data: Send downlink commands to devices. Join Notification: Receive device join request packets. ACK Notification: Receive ACK packets after sending confirmed downlink commands to devices. Gateway Info: Receive gateway basic information and network status. Gateway Event: Receive gateway event. Request data: Send request commands to enquire or configure the gateway. Response data: Receive the replies after sending request to Request data topic.
Topic	Topic name of the data type used for publishing.
Period	Display the report condition of the uplink data. Among them, Gateway Info supports configuring the report period.
Retain	Enable or disable to set the latest message of this topic as retain message.
QoS	QoS0, QoS1 or QoS2 is optional. QoS 0 –Only Once This is the fastest method and requires only one message. It is also the most

Parameter	Description
	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.

3. Click **Save & Apply** to save the settings.

Packets

This section is used to view communication packets between the connected devices and the gateway.

The gateway supports displaying 500 packets.

DeviceEUI	Gateway ID	Frequency	DataRate	RSSI/SNR	Size	Cnt	Type	Time	
24e1244060572ac5	c0ba1fff0e027cb5	926300000	SF9BW500	-/-	0	15678	DnUnc	2026-08-13 04:04:37+0100	
24e1244060572ac5	c0ba1fff0e027cb5	906500000	SF9BW125	-81/7.8	21	16448	UpCnf	2026-08-13 04:04:37+0100	
24e1244060571869	c0ba1fff0e027cb5	925100000	SF9BW500	-/-	0	15476	DnUnc	2026-08-13 04:04:36+0100	
24e1244060571869	c0ba1fff0e027cb5	906100000	SF9BW125	-87/8.5	21	16579	UpCnf	2026-08-13 04:04:36+0100	
24e1244060572667	c0ba1fff0e027cb5	923300000	SF9BW500	-/-	0	14492	DnUnc	2026-08-13 04:04:34+0100	
24e1244060572667	c0ba1fff0e027cb5	905500000	SF9BW125	-73/11.8	0	15863	UpCnf	2026-08-13 04:04:34+0100	
24e124406057c3b8	c0ba1fff0e027cb5	926300000	SF9BW500	-/-	0	14902	DnUnc	2026-08-13 04:04:33+0100	
24e124406057c3b8	c0ba1fff0e027cb5	906500000	SF9BW125	-79/9.2	0	16459	UpCnf	2026-08-13 04:04:33+0100	
24e124406057c3b8	c0ba1fff0e027cb5	926900000	SF9BW500	-/-	0	14901	DnUnc	2026-08-13 04:04:32+0100	
24e124406057c3b8	c0ba1fff0e027cb5	906700000	SF9BW125	-78/13.8	20	16458	UpCnf	2026-08-13 04:04:32+0100	

Total: 500

< 1 2 3 4 5 6 7 ... 50 >
10 / page
Go To
Page

Parameter	Description
Refresh	Update the latest data packet records.
Clear Data	Clears all data packet records on this page.
Device EUI	The device EUI of the packet.
Gateway ID	The ID of the gateway that sends the packet.

Parameter	Description
Frequency	The frequency used to receive or send the packet.
Data Rate	The data rate of the packet.
RSSI/SNR	The received signal strength and signal-to-noise ratio.
Size	The size of the packet.
Fcnt	The frame counter of the packet.
Type	Display the data type. • JnAcc - Join Accept Packet • JnReq - Join Request Packet • UpUnc - Uplink Unconfirmed Packet • UpCnf - Uplink Confirmed Packet; ACK response from the network is requested. • DnUnc - Downlink Unconfirmed Packet • DnCnf - Downlink Confirmed Packet; ACK response from the end device is requested.
Time	The time when the packet was received.
	Opens the packet details.

Detail ×	
DevAddr	07128624
GwEUI	c0ba1ffffe027cb5
AppEUI	24e124c0002a0001
DeviceEUI	24e1244060572ac5
Class Type	Class C
Immediately	-
Timestamp	1631740125
Type	UpCnf
Adr	false
AdrAckReq	false
Ack	false
Fcnt	16448
Port	85
Modulation	LORA
Bandwidth	125
SpreadFactor	9
Bitrate	0
CodeRate	4/5
SNR	7.8
RSSI	-81
Power	-
Payload(b64)	AccIAiYCA6QGBAAFEAYABwAl/2cB
Payload(hex)	01c70802260203a40604000510060007000 8ff6701
MIC	892238e6

Parameter	Description
DevAddr	The device address of the device that sends the packet.
GwEUI	The ID of the gateway that sends the packet.
App EUI	The App EUI of the device that sends the packet.
Device EUI	The device EUI of the packet.
Class Type	The class type of the device that sends the packet.
Immediately	Indicates whether the downlink packet is sent immediately.

Parameter	Description
Timestamp	The time when the packet is received after the packet forwarder starts running. Unit: ms.
Type	Display the data type. • JnAcc - Join Accept Packet • JnReq - Join Request Packet • UpUnc - Uplink Unconfirmed Packet • UpCnf - Uplink Confirmed Packet; ACK response from the network is requested. • DnUnc - Downlink Unconfirmed Packet • DnCnf - Downlink Confirmed Packet; ACK response from the end device is requested.
Adr	Indicates whether the device enables ADR.
AdrAckReq	Nodes periodically transmit ADRACKReq to validate that the network is receiving uplink messages. True means the network should respond within ADR_ACK_DELAY. False means ADR is disabled or the network does not respond within ADR_ACK_DELAY.
Ack	Indicates whether the packet is an ACK packet.
Fcnt	The frame counter of the packet.
Port	The FPort used to transmit the packet. MAC commands use port 0; application data uses ports 1-233.
Modulation	LORA means the physical layer uses LoRa modulation.
Bandwidth	The bandwidth of the frequency channel.
Spread Factor	The spreading factor of the packet.
Bitrate	The bitrate of the frequency channel.
CodeRate	The code rate of the frequency channel.
SNR	The signal-to-noise ratio of the packet.
RSSI	The received signal strength of the packet.
Power	The TX power of the device.
Payload (b64)	The payload in Base64 format.
Payload (hex)	The payload in hexadecimal format.

Parameter	Description
MIC	The cryptographic message integrity code computed over MHDR, FHDR, FPort, and the encrypted FRMPayload.

Related information

[Packet Forward](#)

Network

Cellular

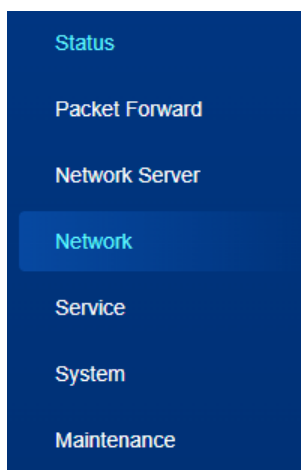
This chapter describes how to configure the settings to register to cellular network.

Prerequisites

- The supported frequencies of the SIM card matches the device model.
- Ensure the SIM card has sufficient balance and works properly in other devices.
- Ensure the device has installed the SIM card.
- Gather SIM information from the cellular operator.

Basic Settings

1. On the left bar, select **Network** page.



2. On the top bar, select **Cellular** tab.
3. Configure the cellular settings as required.

Protocol	IPv4
APN	ctnet-1.apn
Username	user
Password	
Authentication Type	CHAP
PIN Code	
Enable IMS	☐
Primary DNS Server	
Secondary DNS Server	
AT Command	EG:AT+CGREG?
	Send
Emergency Reboot	☐

Parameter	Description
Protocol	Select IPv4 or IPv4/IPv6 .
APN	The Access Point Name for cellular registration and defining which external network to connect. Only letters, digits, "-" and "." are allowed, and the first character must not be "_" or ".". The maximum length is 63 characters.
Username	The username for cellular dial-up connection provided by local ISP.
Password	The password for cellular dial-up connection provided by local ISP.
PIN Code	A 4-8 characters PIN code to unlock the SIM.
Enable IMS	Enable or disable IMS feature. This parameter is only available for -L08GL model.
Primary DNS Server	Customize the cellular primary DNS server. If left blank, the device will use operator's settings.
Secondary DNS Server	Customize the cellular secondary DNS server. If left blank, the device will use operator's settings.

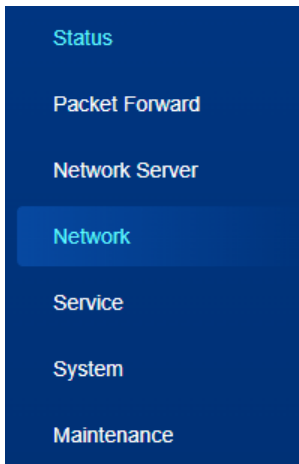
Parameter	Description
AT Command	Send AT Command to get cellular information or configure advanced settings
Emergency Reboot	Enable the gateway to reboot if no network link is available.

- Click **Save & Apply** to save the settings.
- Navigate to **Status > Cellular** page to check if the register status is **Ready** and if there is cellular IP address.

Ping Detection

Ping detection allows the gateway to detect the cellular connection regularly to ensure stable connectivity.

- On the left bar, select **Network** page.



- On the top bar, select **Cellular** tab.
- Enable ping detection and configure the related parameters.

| Ping Detection

Enable ⓘ



Primary Server (IPv4)

8.8.8.8

Secondary Server (IPv4)

223.5.5.5

Interval/s

300

Retry Interval/s

5

Timeout/s

3

Max Ping Retries

3

Parameter	Description
Enable	After enabled, the device will periodically detect the connection status of the link by sending ICMP packets.  Note: It is suggested to disable this option if the gateway is connected to a private, non-Internet network.
Primary Server (IPv4)	The IPv4 server address that the gateway pings to determine whether the connection is still available.
Secondary Server (IPv4)	The IPv4 server address that the gateway tries to ping if the primary server is unavailable.
Interval	The interval between two Ping attempts.
Retry Interval	The interval to retry the ping if the previous ping reaches the timeout and does not reach the max retry times.
Timeout	The maximum time that the gateway waits for a ping response. If no response is received within this time, the ping request is considered failed.

Parameter	Description
Max Ping Retries	The number of times that the gateway retries sending a ping request before determining that the connection has failed.

- Click **Save & Apply** to save the settings.

Related information

[Status](#)

[Tools](#)

WLAN

The gateway can work Wi-Fi as either access point or client. This chapter describes how to configure Wi-Fi settings.

Access Point Settings

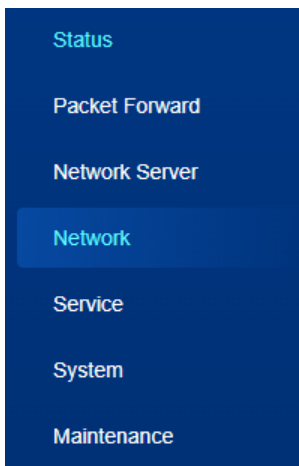
The device can work as an Access Point for device web access.



Note:

One gateway only supports 2 devices' WLAN connection to login this device at the same time.

- On the left bar, select **Network** page.



- On the top bar, select **WLAN** tab.
- Enable WLAN feature.
- Select the interface type as **Access Point** and configure the related parameters.

| WLAN

Enable ☒Disable When Discharged ⓘ ☒Timing Turnoff ⓘ ☐Interface Type SSID * Encryption Mode

| IP Settings

Protocol IP Address * Netmask *

Parameter	Description
Disable When Discharged	Enable or disable turning off the Wi-Fi when the battery is discharging to save power.
Timing Turnoff	Enable or disable turning off the Wi-Fi during a preset time range.
SSID	Define the Service Set Identifier (SSID) to identify this access point. The default value is Gateway_XXXXXX (XXXXXX=last 6 digits of WLAN MAC address).
BSSID	Display the MAC address of WLAN interface.
Encryption Mode	Select the encryption mode for connection. Options: No Encryption, WPA-PSK.
Key	Set the key to connect to this access point when encryption mode is WPA-PSK. Only ASCII characters without spaces are allowed. The length is 8 to 63 characters.
IP Settings	

Parameter	Description
Protocol	It's fixed as Static IP.
IP Address	Set the IP address of this WLAN interface. The default value is 192.168.23.1 .
Netmask	Set the subnet mask of this WLAN interface.

- Click **Save & Apply** to save the settings.
- Connect a smart phone or a computer to the access point. This requires the parameters the same as the access point.

Client Settings

The device can work as a Client to connect to another Access Point for Internet access.

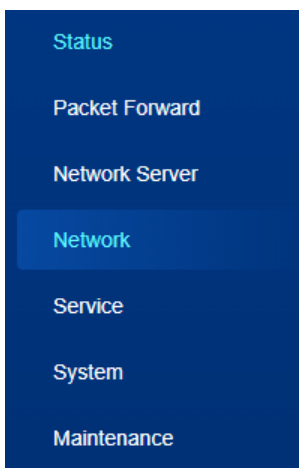
Prerequisites: A 2.4 GHz WLAN access point and the gateway is within its coverage area.



Note:

If you access the device's web GUI via Wi-Fi, you will no longer be able to access it through Wi-Fi after setting the WLAN to client mode. Please connect your computer to the same WLAN access point as the device and use the IP address assigned to the device by the AP.

- On the left bar, select **Network** page.



- On the top bar, select **WLAN** tab.
- Enable WLAN feature.
- Select the interface type as **Client** and configure the related parameters.

| WLAN

Enable	☒
Interface Type	Client
SSID	
BSSID	
Encryption Mode	No Encryption

| IP Settings

Protocol *	Static IP
IP Address *	
Netmask *	255.255.255.0
Gateway *	192.168.1.1
Primary DNS Server	
Secondary DNS Server	

Parameter	Description
SSID	Set the Service Set Identifier (SSID) of the WLAN access point.
BSSID	Set the MAC address of the WLAN access point. Typically, enter either the SSID or the BSSID.
Encryption Mode	Select the encryption mode for connection. Options: No Encryption, WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK.
Key	Set the key to connect to the WLAN access point when encryption mode is not No Encryption .
IP Setting	
Protocol	Select the mode to get the WLAN IP address. DHCP Client: Receive IP address from the access point. Static IP: Assign the IP address manually.

Parameter	Description
IP Address	Set the WLAN interface IP address with the same subnet as the access point.
Subnet Mask	Set the subnet mask of the WLAN interface IP address.
Gateway	Set the IP address of the connected gateway.
Primary DNS Server	The primary DNS server address to send the ICMP packet.
Secondary DNS Server	The secondary DNS server address to send the ICMP packet if the device does not receive the replies from the primary server.

5. Click **Save & Apply** to save the settings.
6. After connected, go to **Status** page to check if the status is Connected.

Related information

[Status](#)

[Tools](#)

OpenVPN

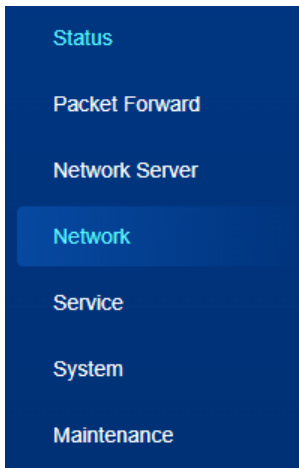
Virtual Private Network (VPN) is a feature to set up encrypted tunnels to ensure data secure transmission, and allow the access between two private networks. This chapter introduces the OpenVPN feature to ensure secure communication.

Prerequisites

- A working OpenVPN server.
- The gateway has accessed the network to reach the OpenVPN server.
- A OpenVPN client configuration file according to sample: [client.conf](#). The parameters can be referred [here](#).

Step

1. On the left bar, select **Network** page.



2. On the top bar, select **OpenVPN** tab.
3. Enable OpenVPN and configure the related parameters.

Enable	☒
File Configuration	openvpn.ovpn Import Export Delete
Status	Connected
Error Log	☐
Device Virtual IP	10.10.0.7
Server Virtual IP	10.10.0.1
Connection Duration	0d, 00h 02m 59s

Parameter	Description
File Configuration	Click Import to upload the <code>.ovpn</code> configuration file.
Status	Display the connection status between the gateway and the OpenVPN server.
VPN Global Route	When enabled, all data traffic will be sent out via this OpenVPN tunnel; otherwise, only the data traffic under the subnet of the VPN tunnel will be sent out.
Error Log	Display the connection and configuration error logs.

Parameter	Description
Device Virtual IP	Display the device virtual IP address after VPN connected.
Server Virtual IP	Display the server virtual IP address after VPN connected.
Connection Duration	Display the connection time after connecting to the VPN server.

4. Click **Save & Apply** to save the settings.
5. Check if the Status shows connected and if there are virtual IP addresses. If not, check error logs for troubleshooting.

Service

Device Management

This chapter describes how to connect the device to Milesight remote management platform.

Prerequisites

For Milesight Development Platform

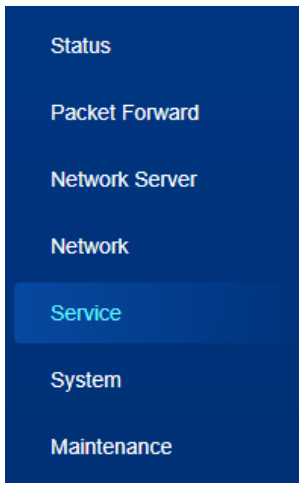
- The device has accessed the Internet network.
- Milesight Development Platform account and enterprise have been created, and device addition is supported.

For Milesight DeviceHub Platform

- A DeviceHub platform is deployed.
- The device can access the DeviceHub platform.

Steps

1. On the left bar, select **Service** page.



2. Configure the platform related parameters.

Auto Provision

Enable ☐

Management Platform

Enable ☒

Platform Type Milesight Development Platform Connected

Sync Platform LNS ☐

When "Sync Platform LNS" is enabled, the gateway will connect to Milesight Development Platform LNS, and data forwarding to other NS will be disabled.

Parameter	Description
Auto Provision	
Enable	Enable to receive the configurations from Milesight Development Platform once after the device is connected to Internet. This will work even Management Platform is disabled.
Management Platform	
Enable	Enable the device to be managed by Milesight management platforms.
Platform Type	Milesight DeviceHub 2.0 or Milesight Development Platform is optional.

Parameter	Description
DeviceHub Address	Fill in the DeviceHub server IP address or domain name.
Sync Platform LNS	After enabled, the gateway will use the platform LNS, and the packet forwarder type will be switched to Milesight Development Platform LNS or DeviceHub LNS .

3. Click **Save & Apply** to save the settings.
4. Add the device to the platform. For more details, refer to [Milesight Development Platform Guide](#) or [Milesight DeviceHub User Guide](#).
5. Check if connection status changes to **Connected** on the platform and the gateway.

System

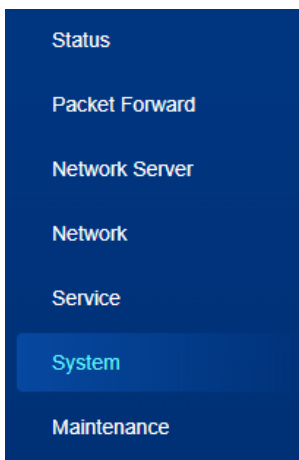
General

This chapter describes the general access settings and time settings.

General

This section is used to change the gateway hostname.

1. On the left bar, select **System** page.



2. On the top bar, select **General** tab.
3. Change the hostname as required.

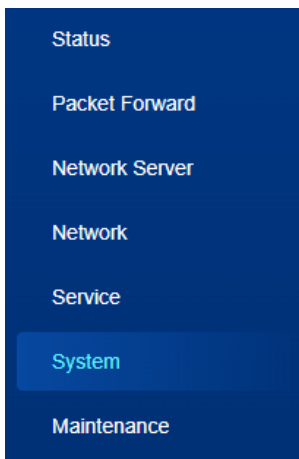
Hostname	Gateway
----------	--------------------------------------

- Click **Save & Apply** to save the settings.

User

This section is used to change account info.

- On the left bar, select **System** page.



- On the top bar, select **User** tab.
- Change the username and password as required.

Username	admin
Old Password *	
New Password *	
Confirm New Password *	

Parameter	Description
Username	Enter a new username. Only letters, digits, "-" and "_" are allowed, and the first character must be a letter or "_". Length limitation: 3-31 characters.
Old Password	Enter the old password.

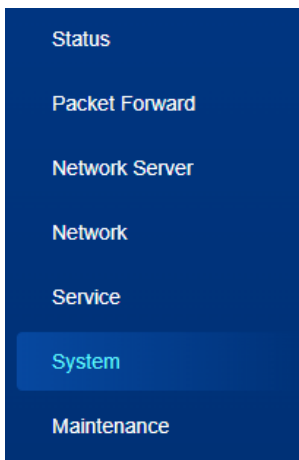
Parameter	Description
New Password	Enter a new password. Only ASCII characters are allowed except spaces. The password must contain at least one letter and one number, and be 8 to 31 characters long.
Confirm New Password	Enter the new password again.

- Click **Save & Apply** to save the settings.
- Log in to the gateway with new account info.

Time

This page is used to configure the device system time.

- On the left bar, select **System** page.



- On the top bar, select **Time** tab.
- Configure the general parameters as required.

Current Time	2026-08-11 12:46:43
Time Zone	0 Europe/London ▼
Sync Type	Sync with NTP Server ▼
NTP Server Address	pool.ntp.org

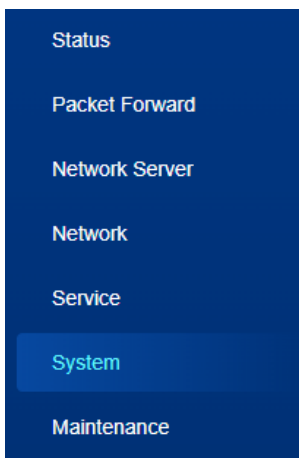
Parameter	Description
Current Time	Displays the current device time.
Timezone	Select the time zone of the device.
Sync Type	Select the time sync source from Sync with Browser and Sync with NTP server .
Sync with NTP Server	
NTP Server Address	Set the NTP server address (domain name/IP) to synchronize the time. This requires the gateway to be able to access this server.
Sync with Browser	
Browser Time	Display the browser time.

- Click **Save & Apply** to save the settings.

Access Service

This page is used to configure access parameters.

- On the left bar, select **System** page.



- On the top bar, select **Access Service** tab.
- Configure the parameters for web access.

| HTTPS / HTTP

Enable



Local Access

HTTPS

Access Port

443

Parameter	Description
Enable	Enable or disable the web access service.
Local Access	Select the local access protocol from HTTPS or HTTP .
Access Port	Select the port for local web access.

- Click **Save & Apply** to save the settings.

Event & Notification

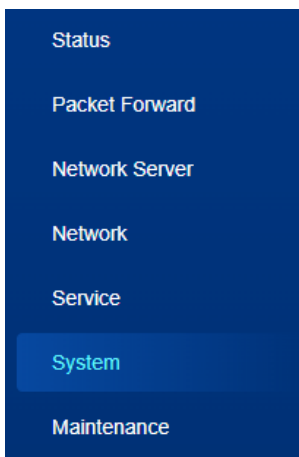
The gateway supports recording and sending event alarms. This chapter describes the event and notification settings.

Step 1. Configure SMTP Server

The gateway supports adding an email address as a SMTP server to send alarm emails.

Prerequisites: A working email address information, and ensure the email address allows third-party app access.

- On the left bar, select **System** page.



2. On the top bar, select **SMTP** tab.
3. Enable **SMTP Server Settings** and configure the related parameters.

| SMTP Server Settings

Enable ☒

Email Address *

Username

Password * 

SMTP Server *

Port *

Enable TLS

| Test Email Settings

Send Test

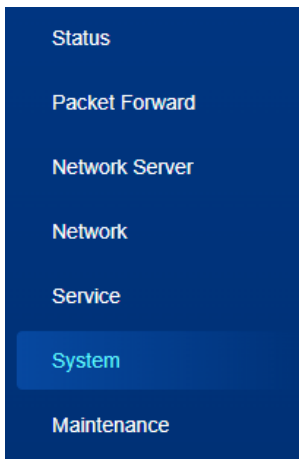
Parameter	Description
Enable	Enable or disable SMTP server settings.
Email Address	The address used for sending emails. Format: xxx@xxx.xx
Username	Username for authentication on SMTP server.
Password	Password for authentication on SMTP server.
SMTP Server	The address of the email service provider's SMTP server.
Port	The port of the email service provider's SMTP server.
Enable TLS	Select the authentication type from None , TLS/SSL and STARTTLS .

4. Click **Save & Apply** to save the settings.
5. Click **Send Test**. If the settings take effect, a test email can be sent out successfully.

Step 2. Configure Email Group

The gateway supports managing email groups to send email alarms.

1. On the left bar, select **System** page.



2. On the top bar, select **Email** tab.
3. Click plus icon to add an email group and configure the related parameters. Up to 15 email groups can be added.

 A configuration interface for email groups. It features a table with two columns: 'Name' and 'Email'. The first row contains the value '1' in the 'Name' column and 'user1@milesight.com;user2@milesight.com' in the 'Email' column. To the right of the 'Email' input field is a trash icon. Below the table is a plus sign icon to add a new group.

Parameter	Description
Name	Set a unique name to identify this email group.
Email Address	Enter email addresses into the email group, separating each address with a semicolon.
	Delete this email group.

4. Click **Save & Apply** to save the settings.

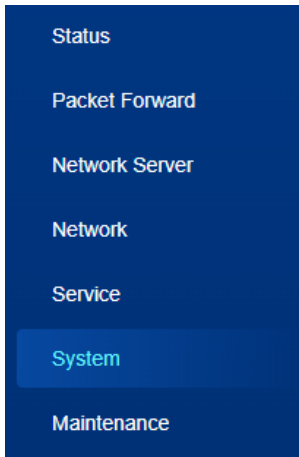
Step 3. Configure Phone Group

The gateway supports managing phone groups to send SMS alarms.

Prerequisites

- This feature is only available for -L08GL model.
- Ensure the used SIM card supports SMS services.

1. On the left bar, select **System** page.



2. On the top bar, select **Phone** tab.
3. Click plus icon to add a phone group and configure the related parameters. Up to 15 phone groups can be added.

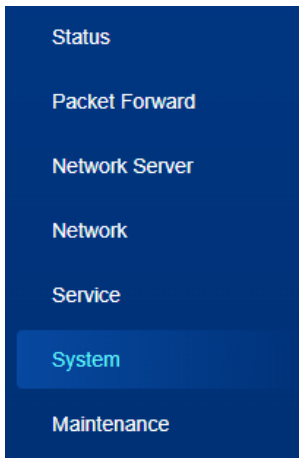
Name	Phone Number	
1	12345678;87654321	
		+

Parameter	Description
Name	Set a unique name to identify this phone group.
Phone Number	Enter phone numbers into the phone group, separating each number with a semicolon.
	Delete this phone group.

4. Click **Save & Apply** to save the settings.

Step 4. Configure Event

1. On the left bar, select **System** page.



2. On the top bar, select **Events** tab.
3. Select the target phone group or email group to send alarms, and configure the power parameters.

Alert Phone

Alert Email

Charging Status Debounce Time * s

Low Power Detect Debounce Time * s

Event	Email	SMS
Battery Status & Low Power Alarm	☐	☐

Parameter	Description
Charging Status Debounce Time	The minimum duration that a change in charging status must persist before it is recognized and reported as an event.
Low Power Detect Debounce Time	The minimum duration that a change in low power status must persist before it is recognized and reported as an event.

4. Select the target event to enable **Email** or **Phone** alarms.

Event	Description
Battery Status & Low Power Alarm	Send notifications when battery working status changes, low power alarm triggering or releasing.

5. Click **Save & Apply** to save the settings.

Related information

[Cellular](#)

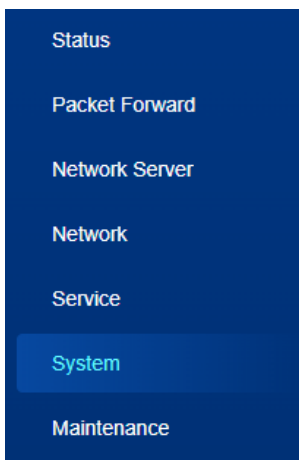
Low Power Mode

The gateway supports low power mode to save battery power and extend the battery life. This chapter describes how to enable the low power mode.

Prerequisites: The battery is installed and operating normally.

Steps:

1. On the left bar, select **System** page.



2. On the top bar, select **Low Power Mode** tab.

3. Enable or disable the **Low Power Mode** option. When enabled, the gateway will only turn on LoRa, communication, data storage and retransmission programs. Cellular, WLAN, GPS and web access will be disabled.

Enable Low Power Mode  

4. Click **Save & Apply** to save the settings.

Maintenance

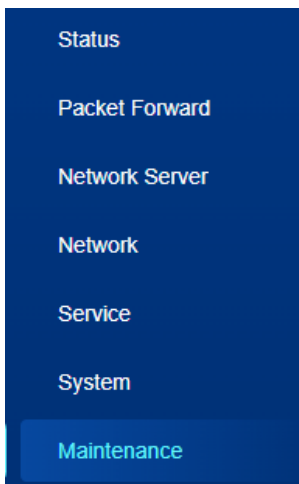
This chapter describes the logs, maintenance tools and features.

Log

The log files can be used for troubleshooting if any problem.

Prerequisites: The device system time is correct.

1. On the left bar, select **Maintenance** page.



2. Configure the log related parameters.

| Remote Log Server

Enable ☒

Server Address *

Port *

| Local Log Storage

Log Severity

Log File

Core dump 

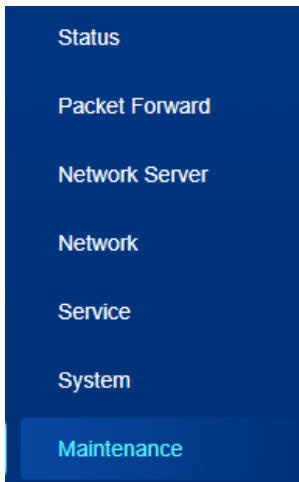
Parameter	Description
Remote Log Server	
Enable	Enable or disable to send the system log file to a remote server.
Server Address	Set the remote log UDP server address (IP/domain name).
Port	Set the remote log server port.
Local Log Storage	
Log Severity	Select the severity to display the logs. To submit logs to technical support, it is recommended to set the log severity to Debug.  Note: After changing the log severity, please replicate the issue to ensure the logs capture the details.
Log File	Download system 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.

3. Click **Save & Apply** to save the settings.
4. Click **Download** to download the log file. You can check the log file directly or send it to Milesight technical support.

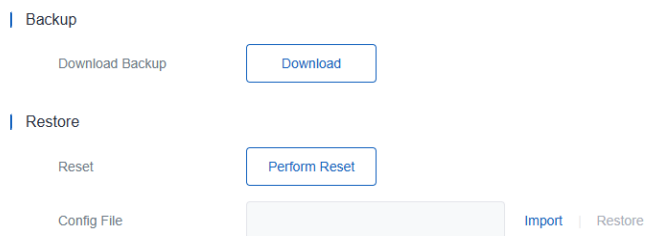
Backup and Restore

This section is used to backup and restore settings.

1. On the left bar, select **Maintenance** page.



2. On the top bar, select **Backup/Upgrade** tab.
3. Click **Download** to download the configuration file of current device.



4. Open the web GUI of a new gateway with the same model, click **Import** to select the configuration file from the local path.
5. Click **Restore** to import the configurations to a new device.

Upgrade

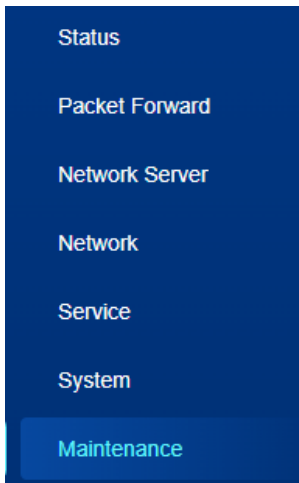
This section is used to upgrade the gateway.

Prerequisites:

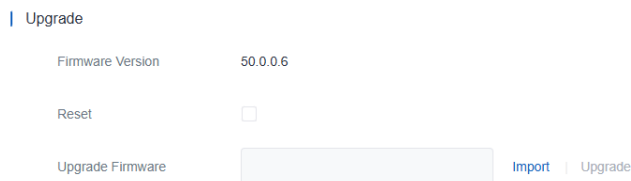
- Download the correct gateway firmware file from Milesight official website. It is recommended to consult technical support before upgrading to ensure a safe and successful upgrade.
- Ensure the network connection is stable enough for remote upgrade.

Steps:

1. On the left bar, select **Maintenance** page.



2. On the top bar, select **Backup/Upgrade** tab.
3. Click **Import** to select the firmware file from the local path.



4. Enable **Reset** as required. After enabled, the device will reset factory default settings after upgrade.
5. Click **Upgrade** to upgrade the device.



CAUTION:

Any operation on web page is not allowed during firmware upgrade; otherwise, the upgrade will be interrupted, or the device may even become inoperable.

- When the SYS LED of the device turns to steady green, log in to the web GUI to verify that the upgrade was successful.



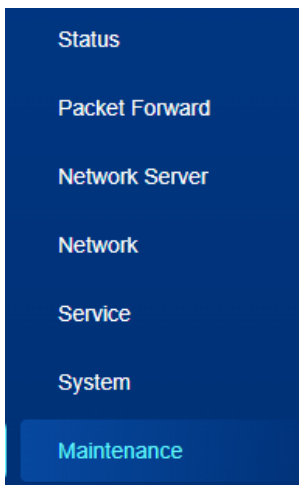
Troubleshooting:

If the web GUI displays abnormally after the upgrade, clear your browser cache.

Factory Reset

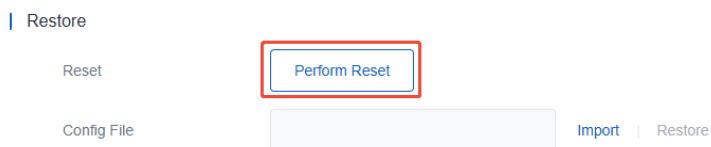
This section is used to reset the device to factory settings.

- On the left bar, select **Maintenance** page.



- On the top bar, select **Backup/Upgrade** tab.

- Click **Perform Reset**.

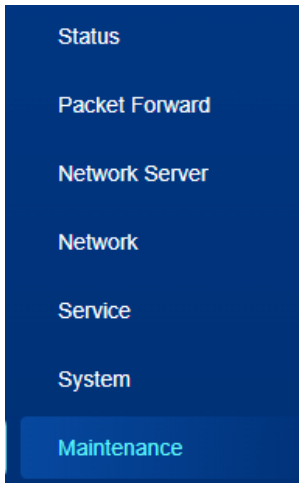


- In the pop-up window, click **Confirm**. The device will reset and reboot.

Reboot

This section is used to reboot the device.

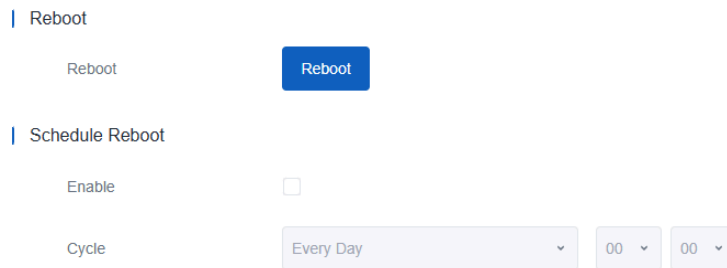
1. On the left bar, select **Maintenance** page.



2. On the top bar, select **Reboot** tab.
3. Select the option to reboot the device.

Reboot Immediately: Click **Reboot** to reboot this device.

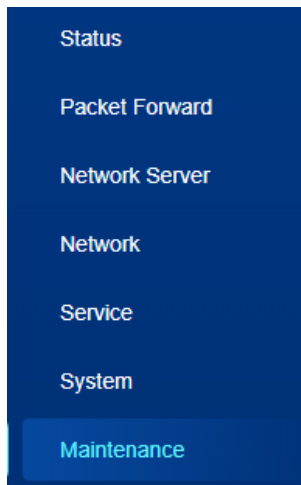
Reboot on Schedule: Enable **Schedule Reboot** and configure the rebooting cycle.

A screenshot of the 'Reboot' configuration page. It has two tabs: 'Reboot' and 'Schedule Reboot'. The 'Reboot' tab is active, showing a 'Reboot' button. The 'Schedule Reboot' tab is also visible, showing an 'Enable' checkbox (which is unchecked) and a 'Cycle' section with a dropdown menu set to 'Every Day' and two time input fields both set to '00'.

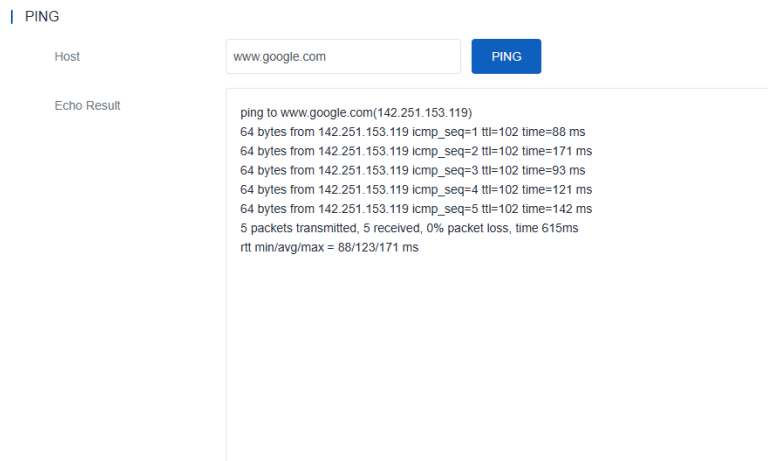
Tools

This section is used to check network connectivity via ping tool.

1. On the left bar, select **Maintenance** page.



2. On the top bar, select **Tools** tab.
3. Enter an IP address or a domain name.
4. Click **Ping** to check the network connectivity and latency between the device and target hosts.



Chapter 7. Services

Milesight provides customers with timely and comprehensive technical support services. End-users can contact their local dealer to obtain technical support. Distributors and resellers can contact Milesight directly for technical support.

Technical Support Mailbox: iot.support@milesight.com

Online Support Portal: <https://support.milesight-iot.com>

Resource Download Center: <https://www.milesight.com/iot/resources/download-center/>

MILESIGHT CHINA

TEL: +86-592-5085280

FAX: +86-592-5023065

Add: Building C09, Software Park Phase III, Xiamen 361024, Fujian, China