

Mini LoRaWAN[®] Gateway

IOT-G63

User Guide

Preface

Thanks for choosing IOT-G63 LoRaWAN® gateway. IOT-G63 delivers tenacious connection over network with full-featured design such as extended hardware watchdog, VPN, fast Ethernet and beyond.

This guide shows you how to configure and operate the IOT-G63 LoRaWAN® gateway. You can refer to it for detailed functionality and gateway configuration.

Readers

This guide is mainly intended for the following users:

- Network Planners
- On-site technical support and maintenance personnel
- Network administrators responsible for network configuration and maintenance

Contents

Chapter 1 Product Introduction.....	6
1.1 Overview.....	6
1.2 Advantages.....	6
1.3 Specifications.....	7
1.4 Dimensions.....	8
Chapter 2 Access to Web GUI.....	9
Chapter 3 Web Configuration.....	11
3.1 Status.....	11
3.1.1 Overview.....	11
3.1.2 Network.....	12
3.1.3 VPN.....	12
3.2 LoRaWAN.....	14
3.2.1 Packet Forwarder.....	14
3.2.1.1 General.....	14
3.2.1.2 Radios.....	15
3.2.1.3 Noise Analyzer.....	17
3.2.1.4 Advanced.....	17
3.2.1.5 Custom.....	20
3.2.1.6 Traffic.....	20
3.2.2 Network Server.....	21
3.2.2.1 General.....	21
3.2.2.2 Application.....	23
3.2.2.3 Profiles.....	27
3.2.2.4 Device.....	30
3.2.2.5 Multicast Groups.....	33
3.2.2.6 Packets.....	34
3.3 Network.....	37
3.3.1 Interface.....	37
3.3.1.1 Port.....	37
3.3.1.2 Loopback.....	40
3.3.2 VPN.....	41
3.3.2.1 DMVPN.....	41
3.3.2.2 IPSec.....	43
3.3.2.3 GRE.....	46
3.3.2.4 L2TP.....	47
3.3.2.5 PPTP.....	49
3.3.2.6 OpenVPN Client.....	51
3.3.2.7 Certifications.....	52
3.4 System.....	53
3.4.1 General Settings.....	53
3.4.1.1 General.....	53

3.4.1.2 System Time.....	55
3.4.1.3 SMTP.....	56
3.4.1.4 Email.....	57
3.4.2 User Management.....	58
3.4.2.1 Account.....	58
3.4.2.2 User Management.....	58
3.4.3 SNMP.....	59
3.4.3.1 SNMP.....	59
3.4.3.2 MIB View.....	60
3.4.3.3 VACM.....	61
3.4.3.4 Trap.....	61
3.4.3.5 MIB.....	62
3.4.4 Device Management.....	62
3.4.5 Events.....	63
3.4.5.1 Events.....	63
3.4.5.2 Events Settings.....	64
3.5 Maintenance.....	65
3.5.1 Tools.....	65
3.5.1.1 Ping.....	65
3.5.1.2 Traceroute.....	65
3.5.2 Schedule.....	66
3.5.3 Log.....	66
3.5.3.1 System Log.....	67
3.5.3.2 Log Settings.....	67
3.5.4 Upgrade.....	68
3.5.5 Backup and Restore.....	69
3.5.6 Reboot.....	69
Chapter 4 Application Examples.....	71
4.1 Restore Factory Defaults.....	71
4.1.1 Via Web Interface.....	71
4.1.2 Via Hardware.....	72
4.2 Firmware Upgrade.....	72
4.3 Ethernet Connection.....	73
4.4 Packet Forwarder Configuration.....	74
4.5 Connect to Linovision IoT Cloud.....	75
4.6 Application Configuration.....	77
4.7 Device Configuration.....	80
4.8 Send Data to Device.....	81
4.9 Connect to UG65/UG67 Gateway.....	83

Chapter 1 Product Introduction

1.1 Overview

IOT-G63 is a robust 8-channel indoor LoRaWAN® gateway. Adopting SX1302 LoRa chip and high-performance CPU, IOT-G63 supports connection with more than 2000 nodes. IOT-G63 has line of sight up to 15 km and can cover about 2 km in urbanized environment, which is ideally suited to smart office, parking lots, campuses, hotels, exhibition centers and many other indoor areas. It also applies to provide coverage for indoor blind spots.

IOT-G63 has integrated with mainstream network servers (such as TTI, ChirpStack, etc.) and Linovision IoT Cloud. Besides, it also supports a built-in network server for easy deployment.

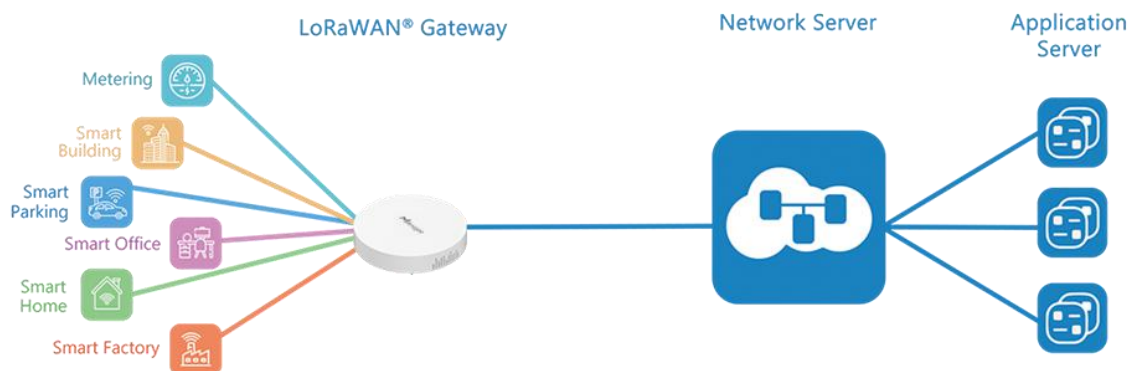


Figure 1-1

1.2 Advantages

Benefits

- High performance NXP industrial processor with big memory
- Embedded network server and compliant with several third party network servers
- MQTT, HTTP or HTTPS protocol for data transmission to application server
- Rugged enclosure, optimized for wall or pole mounting
- 3-year warranty included

Security & Reliability

- Enable unit with security frameworks like IPsec/OpenVPN/GRE/L2TP/PPTP/ DMVPN
- Embedded hardware watchdog to automatically recover from various failure and ensure highest level of availability

Easy Maintenance

- Linovision DeviceHub provides easy setup, bulk configuration, and centralized management of remote devices
- The user-friendly web interface design and various upgrading options help administrator to manage the device as easy as pie
- Web GUI and CLI enable the admin to achieve quick configuration and simple management among a large quantity of devices
- Users can efficiently manage the remote devices on the existing platform through the industrial standard SNMP

Capabilities

- Link remote devices in an environment where communication technologies are constantly changing
- Industrial ARM Cortex-A7 processor, high-performance operating up to 528 MHz with low power consumption, and 4 GB eMMC available to support more applications
- Support wide operating temperature ranging from -20°C to 50°C/-4°F to 122°F

1.3 Specifications

Hardware System	
CPU	528 MHz, ARM Cortex-A7
Memory	4 GB eMMC Flash, 256 MB DDR4 RAM
LoRaWAN	
Antenna	2 × Internal Antennas
Channel	8 (Half/Full-duplex)
Frequency Band	CN470/IN865/EU868/RU864/US915/AU915/KR920/AS923-1&2&3&4
Sensitivity	-140dBm Sensitivity @292bps
Output Power	27dBm Max
Protocol	V1.0 Class A/Class B/Class C and V1.0.2 Class A/Class B/Class C
LBT	Support
Ethernet	
Ports	1 × RJ-45 (PoE PD supported)
Physical Layer	10/100 Base-T (IEEE 802.3)
Data Rate	10/100 Mbps (auto-sensing)
Interface	Auto MDI/MDIX
Mode	Full or half duplex (auto-sensing)

Software

Network Protocols	PPPoE, SNMP v1/v2c/v3, TCP, UDP, DHCP, DDNS, HTTP, HTTPS, DNS, SNTP, Telnet, SSH, MQTT, etc.
VPN Tunnel	DMVPN/IPsec/OpenVPN/PPTP/L2TP/GRE
Management	Web, CLI, DeviceHub, Linovision IoT Cloud, Yeastar Workplace Platform

Power Supply and Consumption

Power Supply	1. 1 × 802.3 af PoE input 2. 5V by Type-C Port
--------------	---

Consumption	Max 3.3 W
-------------	-----------

Physical Characteristics

Ingress Protection	IP30
Dimensions	Φ 115 x 21 mm
Color & Material	White, PC+ABS
Mounting	Desktop, Wall or Ceiling Mounting

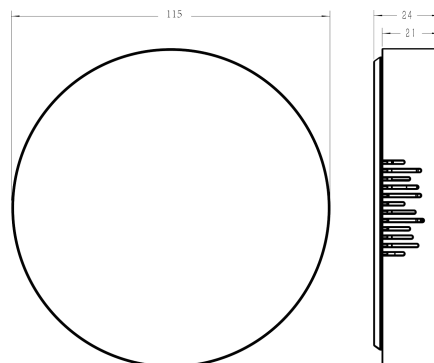
Others

Reset Button	1 × RST
LED Indicators	1 × SYS, 1 × LoRa
Built-in	Watchdog, RTC, Timer

Environmental

Operating Temperature	-20°C to +50°C (-4°F to +122°F)
Storage Temperature	-40°C to +85°C (-40°F to +185°F)
Ethernet Isolation	1.5 kV RMS
Relative Humidity	0% to 95% (non-condensing) at 25°C/77°F

1.4 Dimensions (mm)



Chapter 2 Access to Web GUI

This chapter explains how to access to Web GUI of the IOT-G63. Username:

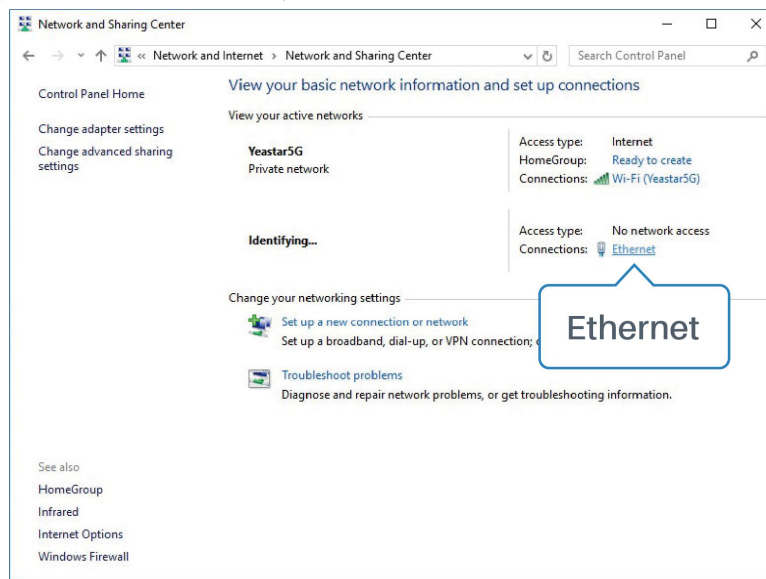
admin

Password: **password**

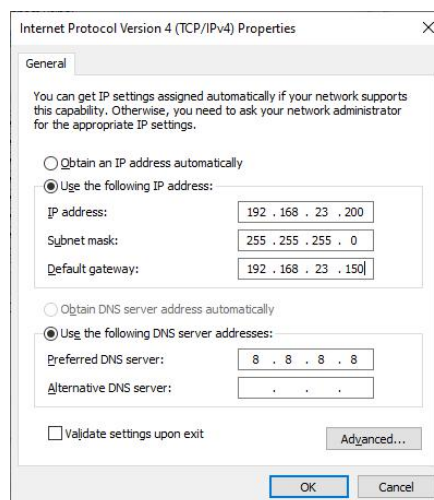
Connect PC to IOT-G63 ETH port directly or through PoE injector to access the web GUI of gateway.

The following steps are based on Windows 10 system for your reference.

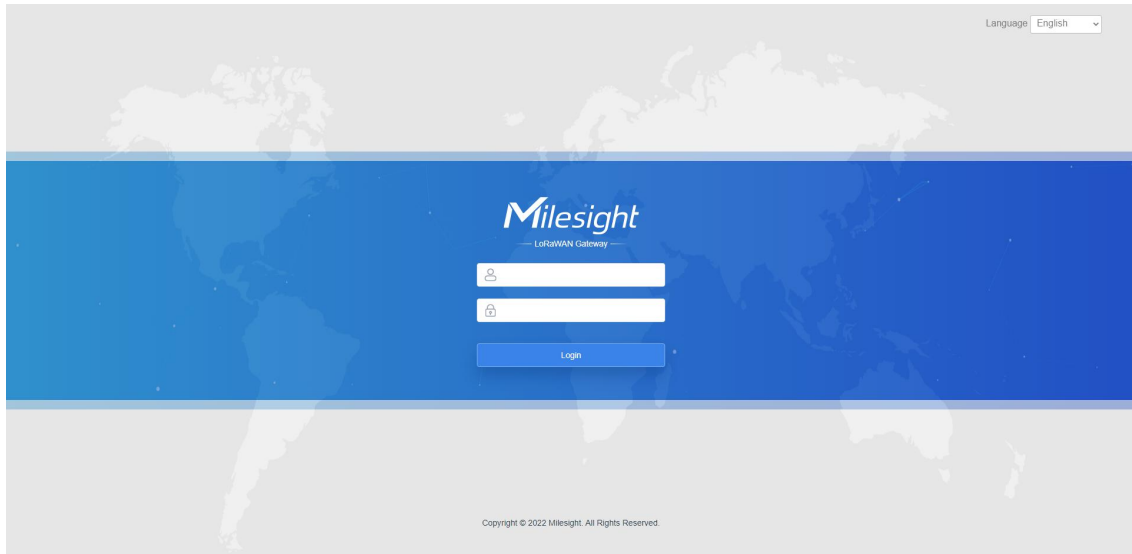
1. Go to “Control Panel” → “Network and Internet” → “Network and Sharing Center”, then click “Ethernet” (May have different names).



2. Go to “Properties” → “Internet Protocol Version 4 (TCP/IPv4)” and select “Use the following IP address”, then assign a static IP manually within the same subnet of the gateway.

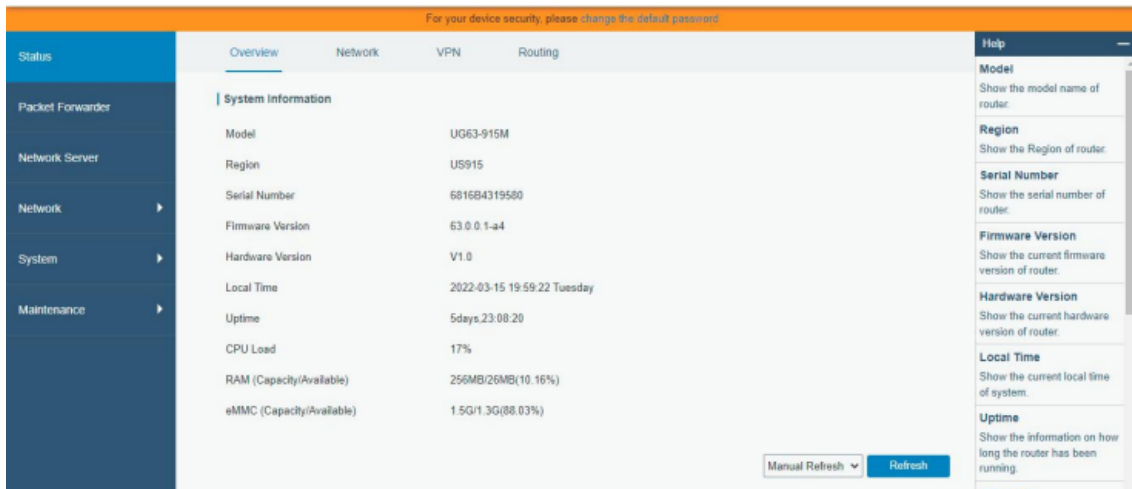


3. Open a Web browser on your PC (Chrome is recommended) and type in the IP address **192.168.23.150** to access the web GUI.
4. Enter the username and password, click “Login”.



⚠ If you enter the username or password incorrectly more than 5 times, the login page will be locked for 10 minutes.

5. After logging in the web GUI, you can view system information and perform configuration of the gateway. It's suggested that you change the password for the sake of security.

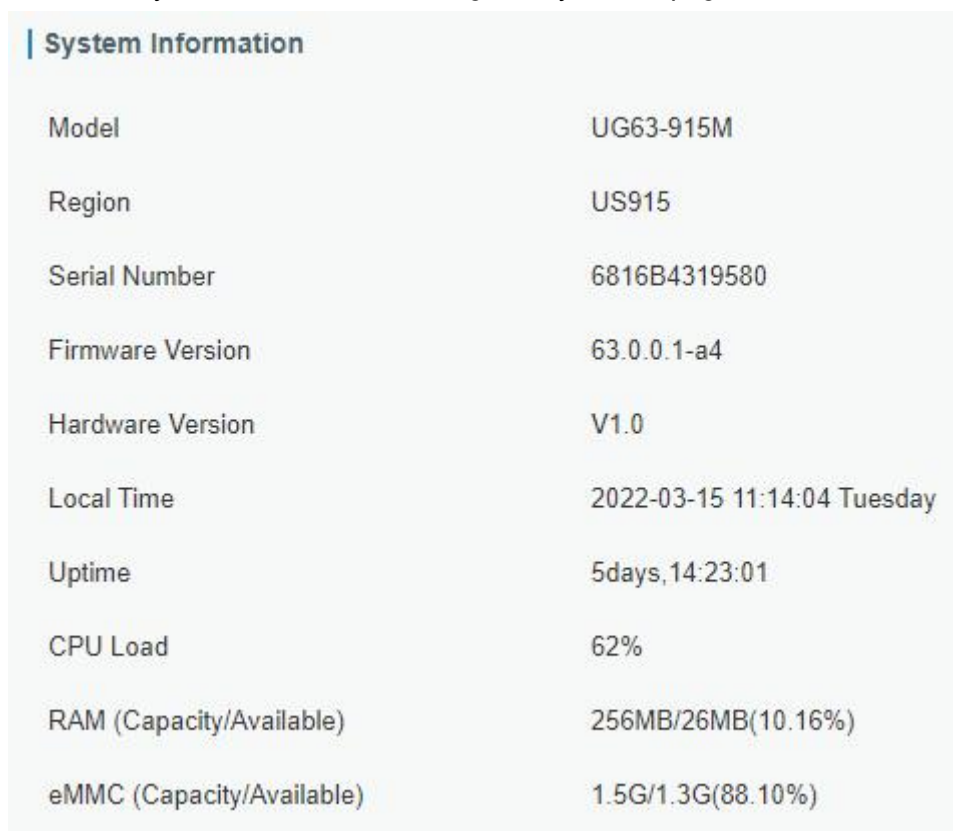


Chapter 3 Web Configuration

3.1 Status

3.1.1 Overview

You can view the system information of the gateway on this page.



System Information	
Model	UG63-915M
Region	US915
Serial Number	6816B4319580
Firmware Version	63.0.0.1-a4
Hardware Version	V1.0
Local Time	2022-03-15 11:14:04 Tuesday
Uptime	5days,14:23:01
CPU Load	62%
RAM (Capacity/Available)	256MB/26MB(10.16%)
eMMC (Capacity/Available)	1.5G/1.3G(88.10%)

Figure 3-1-1-1

System Information	
Item	Description
Model	Show the model name of gateway.
Region	Show the LoRaWAN® frequency region of gateway.
Serial Number	Show the serial number of gateway.
Firmware Version	Show the currently firmware version of gateway.
Hardware Version	Show the currently hardware version of gateway.
Local Time	Show the currently local time of system.
Uptime	Show the information on how long the gateway has been running.
CPU Load	Show the current CPU utilization of the gateway.
RAM (Capacity/Available)	Show the RAM capacity and the available RAM memory.
eMMC (Capacity/Available)	Show the eMMC capacity and the available eMMC memory.

Table 3-1-1-1 System Information

3.1.2 Network

On this page you can check the Ethernet port status of the gateway.

The screenshot shows a navigation bar with 'Overview', 'Network' (selected), 'VPN', and 'Routing'. Below it, a 'WAN' section contains a table with the following data:

Port	Status	Type	IP Address	Netmask	Gateway	DNS	Duration
eth 0	up	Static	192.168.45.161	255.255.255.0	192.168.45.1	8.8.8.8	5days,23h 07m 56s

Figure 3-1-2-1

Network	
Item	Description
Port	Show the name of the Ethernet port.
Status	Show the status of the Ethernet port. "Up" refers to a status that WAN is enabled and Ethernet cable is connected. "Down" means Ethernet cable is disconnected or WAN function is disabled.
Type	Show the dial-up type of the Ethernet port.
IP Address	Show the IP address of the Ethernet port.
Netmask	Show the netmask of the Ethernet port.
Gateway	Show the gateway of the Ethernet port.
DNS	Show the DNS of the Ethernet port.
Duration	Show the information about how long the Ethernet cable has been connected to the Ethernet port when the port is enabled. Once the port is disabled or Ethernet cable is disconnected, the duration will stop.

Table 3-1-2-1 WAN Status

3.1.3 VPN

You can check VPN status on this page, including GRE, PPTP, L2TP, IPsec, OpenVPN and DMVPN.

The screenshot shows a navigation bar with 'Overview', 'Network', 'VPN' (selected), and 'Routing'. Below it, three sections show the status of different VPN tunnel types:

PPTP Tunnel

Name	Status	Local IP	Remote IP
pptp_1	Disconnected	-	-
pptp_2	Disconnected	-	-
pptp_3	Disconnected	-	-

L2TP Tunnel

Name	Status	Local IP	Remote IP
l2tp_1	Disconnected	-	-
l2tp_2	Disconnected	-	-
l2tp_3	Disconnected	-	-

IPsec Tunnel

Name	Status	Local IP	Remote IP
ipsec_1	Disconnected	-	-
ipsec_2	Disconnected	-	-
ipsec_3	Disconnected	-	-

Figure 3-1-3-1

OpenVPN Client				
Name	Status	Local IP	Remote IP	
openvpn_1	Disconnected	-	-	
openvpn_2	Disconnected	-	-	
openvpn_3	Disconnected	-	-	

GRE Tunnel				
Name	Status	Local IP	Remote IP	
gre_1	Disconnected	-	-	
gre_2	Disconnected	-	-	
gre_3	Disconnected	-	-	

DMVPN Tunnel				
Name	Status	Local IP	Remote IP	
dmypn	Disconnected	-	-	

Figure 3-1-3-2

VPN Status	
Item	Description
Name	Show the name of the VPN tunnel.
Status	Show the status of the VPN tunnel.
Local IP	Show the local tunnel IP of VPN tunnel.
Remote IP	Show the remote tunnel IP of VPN tunnel.

Table 3-1-3-1 VPN Status

3.1.4 Routing

You can check routing status on this page, including the routing table and ARP cache.

Overview	Network	VPN	Routing	
Routing Table				
Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.45.1	eth 0	1
127.0.0.0	255.0.0.0	-	Loopback	-
192.168.45.0	255.255.255.0	-	eth 0	-

ARP Cache			
IP	MAC	Interface	
192.168.45.17	8c:16:45:57:58:d3	eth 0	
192.168.45.7	00:e0:4c:68:00:5a	eth 0	
192.168.45.150	24:e1:24:f0:de:07	eth 0	
192.168.45.1	b8:e3:b1:90:fd:01	eth 0	
192.168.45.22	00:0e:c6:5a:60:e4	eth 0	

Figure 3-1-4-1

Item	Description
Routing Table	
Destination	Show the IP address of destination host or destination network.
Netmask	Show the netmask of destination host or destination network.
Gateway	Show the IP address of the gateway.
Interface	Show the outbound interface of the route.
Metric	Show the metric of the route.
ARP Cache	

IP	Show the IP address of ARP pool.
MAC	Show the IP address's corresponding MAC address.
Interface	Show the binding interface of ARP.

Table 3-1-4-1 Routing Information

3.2 LoRaWAN

3.2.1 Packet Forwarder

3.2.1.1 General

The screenshot displays the 'General' settings for a LoRaWAN Packet Forwarder. It includes fields for Gateway EUI (24E124FFFEF12257), Gateway ID (24E124FFFEF12257), and Frequency-Sync (Disabled). Below these is a 'Multi-Destination' table with columns for ID, Enable, Type, Server Address, Connect Status, and Operation. One entry is shown with ID 0, Enabled, Embedded NS, localhost, and Connected status.

Figure 3-2-1-1

General Settings		
Item	Description	Default
Gateway EUI	Show the identifier of the gateway.	Generated from MAC address of the gateway and cannot be changed.
Gateway ID	Fill in the corresponding ID which you've used for register gateway on the remote network server, such as TTN. It is usually the same as gateway EUI and can be changed.	The same as gateway EUI.
Frequency-Sync	Sync frequency configurations from network server by selecting the corresponding ID.	Disabled
Multi-Destination	The gateway will forward the data to the network server address that was created and enabled in the list.	Local host
Connection Status	Show the connection status of package forwarder.	---

Table 3-2-1-1 General Setting Parameters

Related Configuration Example

[Packet forwarder configuration](#)

3.2.1.2 Radios

Radio Channel Setting

Region: US915 Noise Analyzer

Name	Center Frequency/MHz
Radio 0	904.3
Radio 1	905.1

Figure 3-2-1-2

Radios-Radio Channel Setting		
Item	Description	Default
Region	Choose the LoRaWAN® frequency plan used for the upstream and downlink frequencies and datarates. Available channel plans depend on the gateway's model.	Based on the gateway's model
Center Frequency	Radio 0 : supports transmitting and receiving packet. Radio 1 : only supports receiving packet from nodes.	Based on what is specified in the LoRaWAN® regional parameters document

Table 3-2-1-2 Radio Channels Setting Parameters

Multi Channels Setting

Enable	Index	Radio	Frequency/MHz
<input checked="" type="checkbox"/>	0	Radio 0	923.2
<input checked="" type="checkbox"/>	1	Radio 0	923.4
<input checked="" type="checkbox"/>	2	Radio 0	923.6
<input checked="" type="checkbox"/>	3	Radio 1	922.2
<input checked="" type="checkbox"/>	4	Radio 1	922.4
<input checked="" type="checkbox"/>	5	Radio 1	922.6
<input checked="" type="checkbox"/>	6	Radio 1	922.8
<input checked="" type="checkbox"/>	7	Radio 1	923.0

Figure 3-2-1-3

Radios-Multi Channel Setting		
Item	Description	Default
Enable	Click to enable this channel to transmit packets.	Enabled
Index	Indicate the ordinal of the list.	/
Radio	Choose Radio 0 or Radio 1 as center frequency.	Radio 0
Frequency/MHz	Enter the frequency of this channel.	Based on the

	Range: center frequency ± 0.4625 .	LoRaWAN® regional document
--	--	----------------------------

Table 3-2-1-3 Multi Channel Setting Parameters

LoRa Channel Setting

Enable	Radio	Frequency/MHz	Bandwidth/KHz	Spread Factor
<input checked="" type="checkbox"/>	Radio 0	923.8	250KHZ	SF7

Figure 3-2-1-4

Radios-LoRa Channel Setting		
Item	Description	Default
Enable	Click to enable this channel to transmit packets.	Enabled
Radio	Choose Radio 0 or Radio 1 as center frequency.	Radio 0
Frequency/MHz	Enter the frequency of this channel. Range: center frequency ± 0.9 .	Based on the supported frequency
Bandwidth/MHz	Enter the bandwidth of this channel. Recommended value: 125KHz, 250KHz, 500KHz	500KHz
Spread Factor	Choose the selectable spreading factor. The channel with large spreading factor corresponds to a low rate, while the small one corresponds to a high rate.	Based on what is specified in the LoRaWAN® regional parameters document

Table 3-2-1-4 LoRa Channel Setting Parameters

FSK Channel Setting

Enable	Radio	Frequency/MHz	Bandwidth/KHz	DataRate
<input checked="" type="checkbox"/>	Radio 0	924.0	125KHZ	50000

Figure 3-2-1-5

Radios-FSK Channel Setting		
Item	Description	Default
Enable	Click to enable this channel to transmit packets.	Disabled
Radio	Choose Radio 0 or Radio 1 as center frequency.	Radio 0
Frequency/MHz	Enter the frequency of this channel. Range: center frequency ± 0.9 .	Based on the supported frequency
Bandwidth/kHz	Enter the bandwidth of this channel. Recommended value: 125 kHz, 250 kHz, 500 kHz	Based on the supported frequency
Data Rate	Enter the data rate. Range: 500-25000.	500

Table 3-2-1-5 FSK Channel Setting Parameters

3.2.1.3 Noise Analyzer

Noise analyzer is used for scanning the noise of every frequency channel and giving a diagram for users to analyze the environment interference condition and select best deployment. RSSI indicates the sensitivity for every channel. **Lower the RSSI value, better the signal. It's not suggested to enable this feature when using package forwarder since it will affect the downlink transmission.**

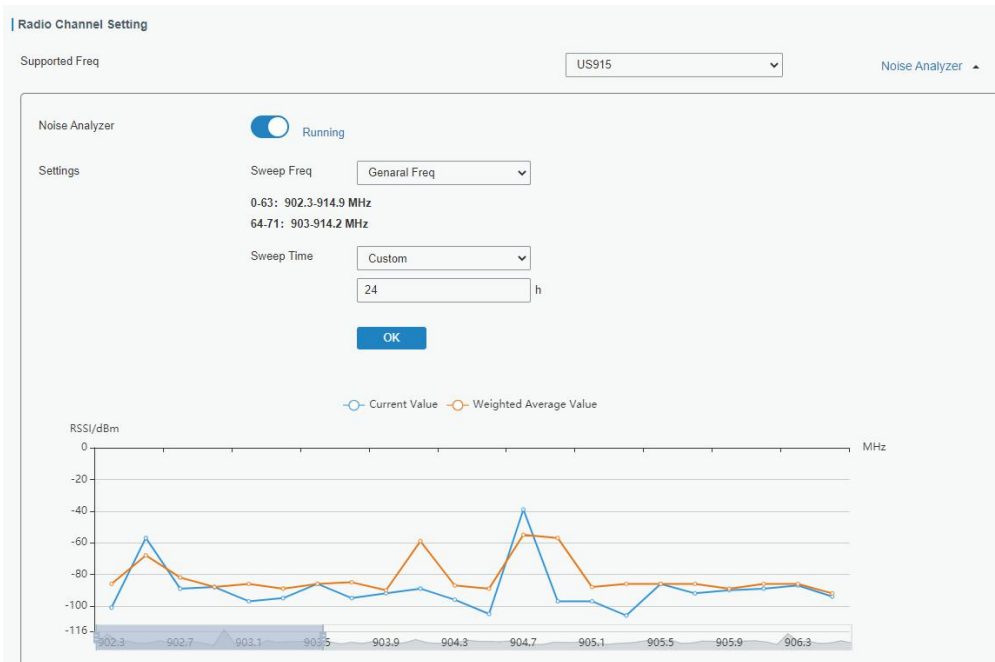


Figure 3-2-1-6

Noise Analyzer		
Item	Description	Default
Enable	Click to enable noise analyzer feature.	Disabled
Sweep Freq	Select the frequency sweeping range. General Freq: frequencies based on the LoRaWAN® regional parameters document Custom: custom the frequency range	General Freq
Sweep Time	Enable the noise analyzer continuously or within a period of time. If Custom is selected, the noise analyzer will stop automatically after the pre-configured time. Note: It's suggested to custom the time since noise analyzer feature will affect the normal data transmission.	Custom/24h

Table 3-2-1-6 Noise Analyzer Setting Parameters

3.2.1.4 Advanced

This section is about settings in details of beacon transmitting and validating.

General	Radios	Advanced	Custom	Traffic
Beacon Setting				
Beacon Period		0	s	
Beacon Freq		923300000	Hz	
Beacon Datarate		SF12		
Beacon Channel Number		8		
Beacon Freq Step		600000	Hz	
Beacon Bandwidth		500000	Hz	
Beacon TX Power		27	dBm	

Figure 3-2-1-7

Advanced-Beacon Setting		
Item	Description	Default
Beacon Period	Interval of gateway sending beacons for Class B device time synchronization. 0 means the gateway will not send beacons.	0
Beacon Freq	The frequency of beacons.	Based on the supported frequency
Beacon Datarate	The datarate of beacons.	Based on the supported frequency
Beacon Channel Number	When selecting Custom, it allows users to custom range from 1 to 8.	1
Beacon Freq Step	Frequency interval of beacons. Unit: Hz	200000 Hz
Beacon Bandwidth	The bandwidth of beacons. Unit: Hz	12500 Hz
Beacon TX Power	The TX power of beacons.	Based on the supported frequency

Table 3-2-1-7 Advanced-Beacon Parameters

Intervals Setting

Keep Alive Interval s

Stat Interval s

Push Timeout ms

Forward CRC Setting

Forward CRC Disabled

Forward CRC Error

Forward CRC Valid

Figure 3-2-1-8

Item	Description	Default
Keep Alive Interval	Enter the interval of keep alive packet which is sent from gateway to network server to keep the connection stable and alive. Range: 1-3600.	10 s
Stat Interval	Enter the interval to update the network server with gateway statistics. Range: 1-3600.	30 s
Push Timeout	Enter the timeout to wait for the response from server after the gateway sends data of node. Rang: 1-1999.	100 ms
Forward CRC Disabled	Enable to send packets received with CRC disabled to the network server.	Disabled
Forward CRC Error	Enable to send packets received with CRC errors to the network server.	Disabled
Forward CRC Valid	Enable to send packets received with CRC valid to the network server.	Enabled

Table 3-2-1-8 Advanced Parameters

LBT Settings

Enable

RSSI Target dBm

Figure 3-2-1-9

Item	Description	Default
Enable	Enable to scan occupancy of current channels before transmission. Note: AU915 and US915 do not support LBT feature.	Disabled
RSSI Target	Enter the criteria of an idle channel. If actual RSSI of	-80

	a channel is less than the criteria/target, the channel is considered as idle. Range: -120~0	
--	--	--

Table 3-2-1-9 Advanced-LBT Parameters

3.2.1.5 Custom

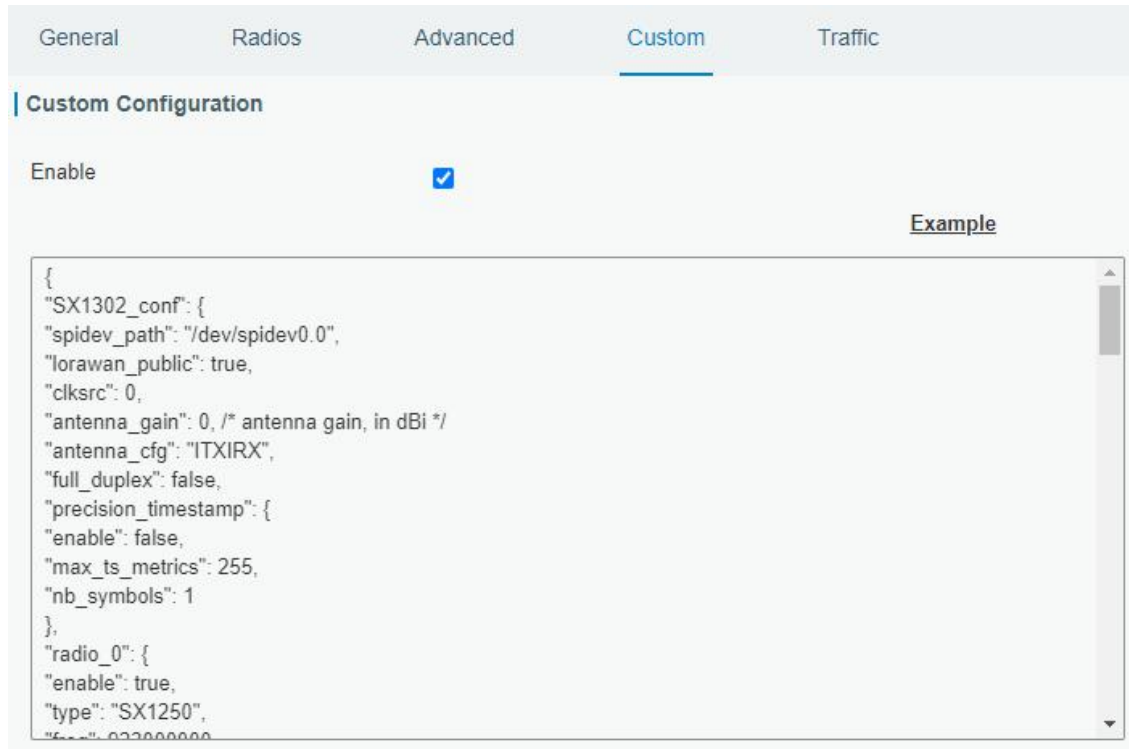


Figure 3-2-1-10

When Custom Configuration mode is enabled, you can write your own packet forwarder configuration file in the edit box to configure packet forwarder. Click “Save” to save your custom configuration file content, and click “Apply” to take effect. You can click “Clear” to erase all content in the edit box. If you don’t know how to write configuration file, please click “Example” to go to reference page.

3.2.1.6 Traffic

When navigating to the traffic page, any recent traffic received by the gateway will display. To watch live traffic, click “Refresh”.

Traffic Setting									
Refresh Clear									
Rfch	Direction	Time	Ticks	Frequency	Datarate	Coderate	RSSI	SNR	
1	up	-	83002508	922.8	SF9BW125	4/5	-103	-13.2	
1	up	-	71108156	922.6	SF9BW125	4/5	-102	-13.2	
1	up	-	35426956	922.8	SF9BW125	4/5	-103	-9.8	
1	up	-	3171639508	922.6	SF9BW125	4/5	-100	-10.5	
1	up	-	3159744804	922.6	SF9BW125	4/5	-102	-13.0	
1	up	-	3155781348	922.6	SF9BW125	4/5	-101	-12.2	
1	up	-	3147851660	922.6	SF9BW125	4/5	-102	-13.8	
1	up	-	3143888916	922.8	SF9BW125	4/5	-102	-13.2	
1	up	-	3139922740	922.8	SF9BW125	4/5	-100	-12.2	
1	up	-	3124065788	922.8	SF9BW125	4/5	-100	-12.8	

Figure 3-2-1-11

Item	Description
Refresh	Click to obtain the latest data.
Clear	Click to clear all data.
Rfch	Show the channel of this packet.
Direction	Show the direction of this packet.
Time	Show the receiving time of this packet.
Ticks	Show the ticks of this packet.
Frequency	Show the frequency of the channel.
Datarate	Show the datarate of the channel.
Coderate	Show the coderate of this packet.
RSSI	Show the received signal strength.
SNR	Show the signal to noise ratio of this packet.

Table 3-2-1-10 Traffic Parameters

3.2.2 Network Server

3.2.2.1 General

General Applications Profiles Device

General Setting

Enable

Cloud Mode

NetID

Join Delay sec

RX1 Delay sec

Lease Time hh-mm-ss

Log Level

Global Channel Plan Setting

Channel Plan

Channel

Figure 3-2-2-1

Item	Description	Default
General Setting		
Enable	Click to enable Network Server mode.	Enabled
Cloud Mode	Enabled to connect gateway to Linovision IoT Cloud or Yeastar Workplace platform .	Disabled
NetID	Enter the network identifier.	010203
Join Delay	Enter the interval time between when the end-device sends a Join_request_message to network server and when the end-device prepares to open RX1 to receive the Join_accept_message sent from network server.	5
RX1 Delay	Enter the interval time between when the end-device sends uplink packets and when the end-device prepares to open RX1 to receive the downlink packet.	1
Lease Time	Enter the amount of time till a successful join expires. The format is hours-minutes-seconds. If the join-type is OTAA, then the end-devices need to join the network server again when it exceeds the lease time.	876000-00-00
Log level	Choose the log level.	Info

Channel Plan Setting		
Channel Plan	Choose LoRaWAN® channel plan used for the upstream and downlink frequencies and datarates. Available channel plans depend on the gateway's model.	Depend on the gateway's frequency
Channel	<p>Enabled frequencies are controlled using channel mask.</p> <p>Leave it blank means using all the default standard usable channels specified in the LoRaWAN® regional parameters document.</p> <p>It allows to enter the index of the channels.</p> <p>Examples:</p> <p>1, 40: Enabling Channel 1 and Channel 40</p> <p>1-40: Enabling Channel 1 to Channel 40</p> <p>1-40, 60: Enabling Channel 1 to Channel 40 and Channel 60</p> <p>All: Enabling all channels</p> <p>Null: Indicates that all channels are disabled</p>	Depend on the gateway's frequency

Table 3-2-2-1 General Parameters

Note: 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, as the following picture shows:

Frequency(MHz)	Min Datarate	Max Datarate	Operation

Figure 3-2-2-2

Additional Channels		
Item	Description	Default
Frequency/MHz	Enter the frequency of the additional plan.	Null.
Max Datarate	Enter the max datarate for the end-device. The range is based on what is specified in the LoRaWAN® regional parameters document.	DR0 (SF12,125 kHz)
Min Datarate	Enter the min datarate for the end-device. The range is based on what is specified in the LoRaWAN® regional parameters document.	DR3 (SF9,125 kHz)

Table 3-2-2-2 Additional Plan Parameters

3.2.2.2 Application

An application is a collection of devices with the same purpose/of the same type. All

devices with the same “Payload Codec” and data transmission destination can be added under the same application.

You can edit the application by clicking  or create a new application by clicking .

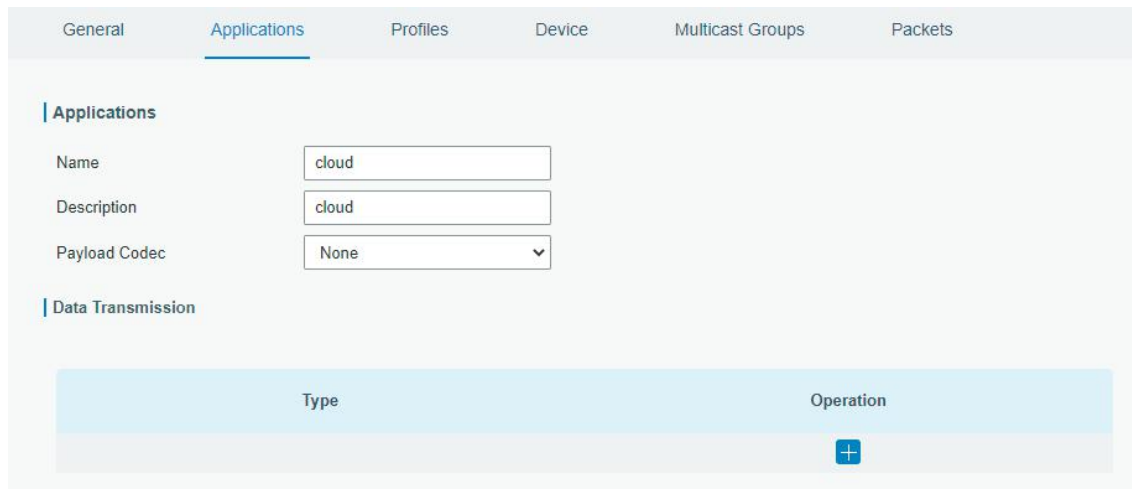


Figure 3-2-2-3

Item	Description
Name	Enter the name of the application profile. E.g Smoker-sensor-app.
Description	Enter the description of this application. E.g a application for smoker sensor.
Payload Codec	Select from: “None”, “Cayenne LPP”, “Custom”. None: This mode enables devices not to encode data. Cayenne LPP: This mode enables devices to encode data with the Cayenne Low Power Payload (LPP). Custom: This mode enables devices to encode data with the decoder function and the encoder function which you have entered the code.
Data Transmission	Data will be sent to your custom server using the MQTT,HTTP or HTTPS protocol.

Table 3-2-2-3 Application Parameters

Type

Status -

General

Broker Address

Broker Port

Client ID

Connection Timeout/s

Keep Alive Interval/s

User Credentials

Enable

Username

Password

Figure 3-2-2-4

TLS

Enable

Mode

Topic

Data Type	topic	
Uplink data	<input type="text"/>	QoS 0
Downlink data	<input type="text"/>	QoS 0
Multicast downlink data	<input type="text"/>	QoS 0
Join notification	<input type="text"/>	QoS 0
ACK notification	<input type="text"/>	QoS 0
Error notification	<input type="text"/>	QoS 0

Figure 3-2-2-5

MQTT Settings		
Item	Description	Default
General		
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 message 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	30
Keep Alive Interval/s	After the client is connected with the server, the client will send heartbeat packet to the server regularly to keep alive. Range: 1-65535	60
User Credentials		
Enable	Enable user credentials.	
Username	The username used for connecting to MQTT broker.	
Password	The password used for connecting to MQTT broker.	
TLS		
Enable	Enable the TLS encryption in MQTT communication.	
Mode	Select from "Self signed certificates", "CA signed server certificate". CA signed server certificate: verify with the certificate issued by Certificate Authority (CA) that pre-loaded on device. Self signed certificates: upload the custom CA certificates, client certificates and secret key for verification.	
Topic		
Data Type	Data type sent to MQTT broker.	
Topic	Topic name of the data type using for publish.	
QoS	<p>QoS 0 – Only Once This is the fastest method and requires only 1 message. It is also the most unreliable transfer mode.</p> <p>QoS 1 – At Least Once This level guarantees that the message will be delivered at least once, but may be delivered more than once.</p> <p>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.</p>	

Table 3-2-2-4 MQTT Settings Parameters

HTTP Header

Header Name	Header Value	Operation

URL

Data Type	URL
Uplink data	<input style="width: 90%;" type="text"/>
Join notification	<input style="width: 90%;" type="text"/>
ACK notification	<input style="width: 90%;" type="text"/>
Error notification	<input style="width: 90%;" type="text"/>

Figure 3-2-2-6

HTTP/HTTPS Settings	
Item	Description
HTTP Header	
Header Name	A core set of fields in HTTP header.
Header Value	Value of the HTTP header.
URL	
Data Type	Data type sent to HTTP/HTTPS server.
Topic	Topic name of the data type using for publish.
URL	HTTP/HTTPS server URL to receive data.

Table 3-2-2-5 HTTP/HTTPS Settings Parameters

Related Configuration Example

[Application configuration](#)

3.2.2.3 Profiles

A Profile defines the device capabilities and boot parameters that are needed by the Network Server for setting the LoRaWAN® radio access service. These information elements shall be provided by the end-device manufacturer.

You can edit the device profile by clicking or create a new device profile by clicking




General	Applications	Profiles	Device	Multicast Groups	Packets
Device Profiles					
Name	Max TXPower	Join Type	Class Type	Operation	
ClassA-OTAA	0	OTAA	Class A	 	
ClassB-OTAA	0	OTAA	Class A Class B	 	
ClassC-OTAA	0	OTAA	Class A Class C	 	
					

Figure 3-2-2-7

Device Profiles

Name

Max TXPower

Join Type

Class Type Class A Class B Class C

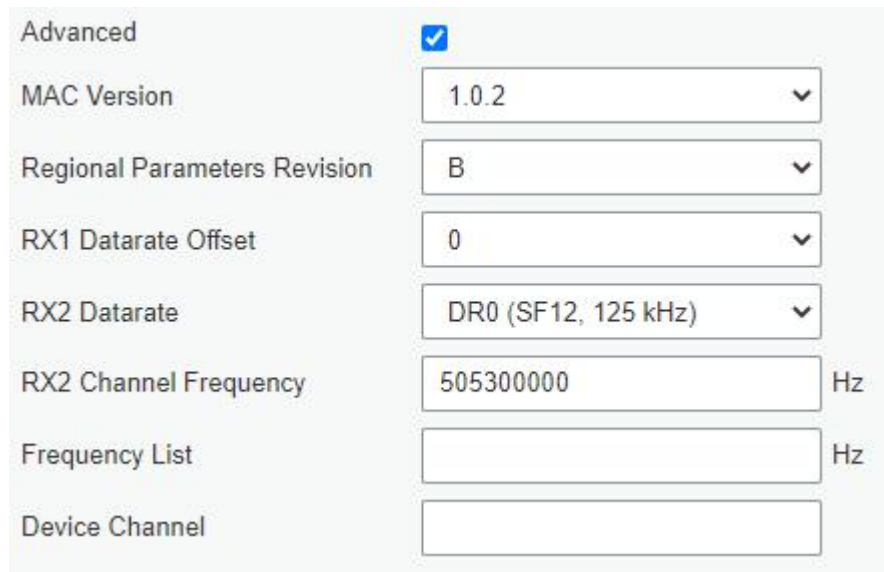
Advanced

Figure 3-2-2-8

Device Profiles Settings		
Item	Description	Default
Name	Enter the name of the device profile. E.g. Smoker-sensor-app.	Null
Max TXPower	Enter the maximum transmit power. The TXPower indicates power levels relative to the Max EIRP level of the end-device. 0 means using the max EIRP. EIRP refers to the Equivalent Isotropically Radiated Power.	0
Join Type	Select from: "OTAA" and "ABP". OTAA:Over-the-Air Activation. For over-the-air activation, end-devices must follow a join procedure prior to participating in data exchanges with the network server. An end-device has to go through a new join procedure every time as it has lost the session context information. ABP: Activation by Personalization. Under certain circumstances, end-devices can be activated by personalization. Activation by	OTAA

	personalization directly ties an end-device to a specific network bypassing the join request - join accept procedure.	
Class Type	Device type is Class A by default. Users can check the box of Class B or Class C to add the class type. Note: Beacon period should be set to nonzero value in Packet Forwarder->Advanced if you use Class B.	---

Table 3-2-2-6 Device Profiles Setting Parameters



Advanced

MAC Version

Regional Parameters Revision

RX1 Datarate Offset

RX2 Datarate

RX2 Channel Frequency Hz

Frequency List Hz

Device Channel

Figure 3-2-2-9

Device Profile Advanced Settings		
Item	Description	Default
MAC Version	Choose the version of the LoRaWAN® supported by the end-device.	1.0.2
Regional Parameter Revision	Revision of the Regional Parameters document supported by the end-device.	B
RX1 Datarate Offset	The offset which used for calculating the RX1 data-rate, based on the uplink data-rate.	Based on what is specified in the LoRaWAN® regional parameters document
RX2 Datarate	Enter the RX2 datarate which used for the RX2 receive-window.	
RX2 Channel Frequency	RX2 channel frequency which used for the RX2 receive-window.	
Frequency List	List of factory-preset frequencies. The range is based on what is specified in the LoRaWAN® regional parameters document.	Null
Device Channel	Change this device frequency channel by typing the channel indexes. When configured, it takes precedence over the global channel. This setting	Null

	only works for CN470/US915/AU915 gateway.	
PingSlot Period	Period of opening the pingslot.	Every Second
PingSlot DataRate	Datarate of the node receiving downlinks.	Based on the supported frequency
PingSlot Freq	Frequency of the node receiving downlinks.	Based on the supported frequency
ACK Timeout	The time for confirmed downlink transmissions. This option is only applicable to class B and class C.	Class B: 10 Class C: 10

Table 3-2-2-7 Device Profiles Advanced Setting Parameters

3.2.2.4 Device

A device is the end-device connecting to, and communicating over the LoRaWAN® network. **Due to memory limitation, it's suggested to add not more than 20 devices.**

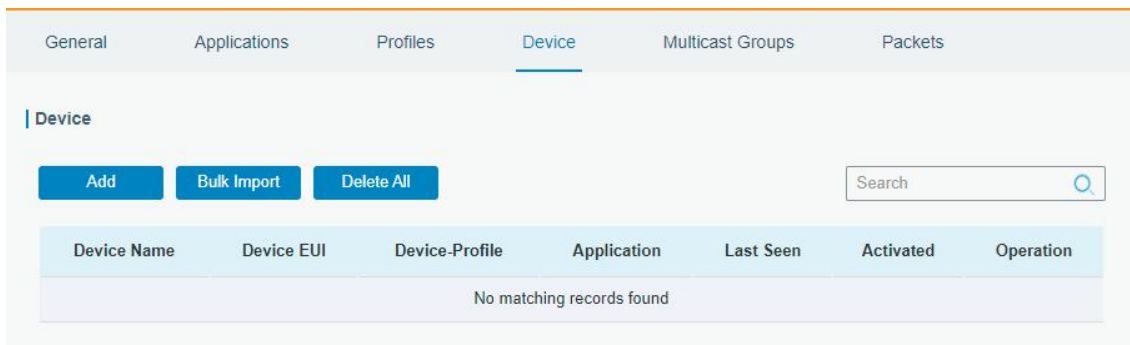


Figure 3-2-2-10

Item	Description
Add	Add a device.
Bulk Import	Download template and import multiple devices.
Delete All	Delete all devices in the list.
Device Name	Show the name of the device.
Device EUI	Show the EUI of the device.
Device-Profile	Show the name of the device's device profile.
Application	Show the name of the device's application.
Last Seen	Show the time of last packet received.
Activated	Show the status of the device. ✓ means that the device has been activated.
Operation	Edit or delete the device.

Table 3-2-2-8 Device Parameters

Device Name	lora-sensor
Description	a short description of your node
Device EUI	24e1641194784358
Device-Profile	OTAA
Application	app
Modbus RTU Data Transmission	Modbus RTU to TCP
Fport	
TCP Port	
Frame-counter Validation	<input type="checkbox"/>
Application Key	
Device Address	
Network Session Key	
Application Session Key	
Uplink Frame-counter	0
Downlink Frame-counter	0

Figure 3-2-2-11

Device Configuration		
Item	Description	Default
Device Name	Enter the name of this device.	Null
Description	Enter the description of this device.	Null
Device EUI	Enter the EUI of this device.	Null
Device-Profile	Choose the device profile.	Null
Application	Choose the application profile.	Null
Modbus RTU Data Transmission	Choose from: "Disable", "Modbus RTU to TCP", "Modbus RTU over TCP". This feature is only applicable to Linovision class C type LoRaWAN® controllers.(UC300/UC501/UC1152, etc.) -Modbus RTU to TCP: TCP client can send Modbus TCP commands to ask for controller Modbus data. -Modbus RTU over TCP: TCP client can send Modbus RTU commands to ask for controller Modbus data.	Disable
Fport	Enter the LoRaWAN® frame port for transparent transmission between Linovision LoRaWAN®	Null

	<p>controllers and UG63. Range: 2-84, 86-223. Note: this value must be the same as the Linovision LoRaWAN® controller's Fport.</p>	
TCP Port	<p>Enter the TCP port for data transmission between the TCP Client and UG63 (as TCP Server). Range: 1-65535.</p>	Null
Frame-Counter Validation	<p>If disable the frame-counter validation, it will compromise security as it enables people to perform replay-attacks.</p>	Enabled
Application Key	<p>Whenever an end-device joins a network via over-the-air activation, the application key is used for derive the Application Session key.</p>	Null
Device Address	<p>The device address identifies the end-device within the current network.</p>	Null
Network Session Key	<p>The network session key 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.</p>	Null
Application Session Key	<p>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.</p>	Null
Uplink Frame-counter	<p>The number of data frames which sent uplink to the network server. It will be incremented by the end-device and received by the end-device. Users can reset the 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.</p>	Null
Downlink Frame-counter	<p>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 the 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.</p>	Null

Table 3-2-2-9 Device Setting Parameters

Related Configuration Example

[Device configuration](#)

3.2.2.5 Multicast Groups

Linovision gateways support for creating Class B or Class C multicast groups to send downlink messages to a group of end devices. A multicast group is a virtual ABP device (i.e. shared session keys), does not support uplink, confirmed downlink nor MAC commands.

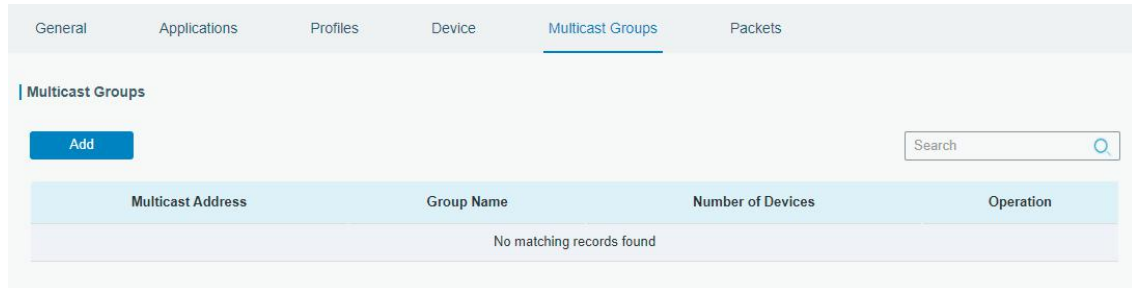


Figure 3-2-2-12

Item	Description
Add	Add a multicast group.
Group Name	Show the name of the group.
Number of Devices	Show the device number of the group.
Operation	Edit or delete the multicast group.

Table 3-2-2-10 Multicast Group Parameters

Group Name	<input type="text"/>
Multicast Address	<input type="text"/>
Multicast Network Session Key	<input type="text"/>
Multicast Application Session Key	<input type="text"/>
Class Type	Class C <input type="button" value="v"/>
Datarate	DR8(SF12,500KHz) <input type="button" value="v"/>
Frequency	<input type="text" value="923300000"/> Hz
Frame-counter	<input type="text" value="0"/>
Selected Devices	<div style="border: 1px solid #ccc; height: 60px;"></div>
Add Device	<input type="text"/>

Figure 3-2-2-13

Multicast Group Configuration		
Item	Description	Default
Group Name	Enter the name of this multicast group.	Null
Multicast	Device address (Dev Addr) of all devices in this group.	Null

Address		
Multicast Network Session Key	The network session key (Netwks Key) of all devices in this group.	Null
Multicast Application Session Key	The application session key (AppSKey) of all devices in this group.	Null
Class Type	Class B and Class C are optional.	Class C
Datarate	Datarate of the node receiving downlinks	Based on the supported frequency
Frequency	Downlink frequency of all devices in this group.	Based on the supported frequency
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.	0
Ping Slot Periodicity	Period of opening the pingslot. This is only applied to Class B end devices.	Every 4 second
Selected Devices	Show all device names in this group.	Null
Add Device	Add devices in the pull-down list.	Null

Table 3-2-2-11 Multicast Group Setting Parameters

3.2.2.6 Packets

The screenshot displays a user interface for sending data. It is divided into three main sections:

- Send Data To Device:** Contains a form with fields for 'Device EUI' (text input with '0000000000000000'), 'Type' (dropdown menu set to 'ASCII'), 'Payload' (text input), 'Port' (text input with '85'), and 'Confirmed' (checkbox). A 'Send' button is located to the right.
- Send Data to Multicast Group:** Contains a form with fields for 'Multicast Group' (dropdown menu), 'Type' (dropdown menu set to 'ASCII'), 'Payload' (text input), and 'Port' (text input with '85'). A 'Send' button is located to the right.
- Network Server:** Features a 'Clear' button, a search bar with a magnifying glass icon, and a table with columns: 'Device EUI/Group', 'Gateway ID', 'Frequency', 'Datarate', 'RSSI/SNR', 'Size', 'Fcnt', 'Type', 'Time', and 'Details'. Below the table, it states 'No matching records found'.

Figure 3-2-2-14


Send Data To Device/Multicast Group		
Item	Description	Default

Device EUI	Enter the EUI of the device to receive the payload.	Null
Multicast Group	Select the multicast group to send downlinks. Multicast groups can be added under Multicast Groups tab.	Null
Type	Choose from: "ASCII", "hex", "base64". Choose the payload type to enter in the payload Input box.	ASCII
Payload	Enter the message to be sent to this device.	Null
Port	Enter the LoRaWAN® frame port for packet transmission between device and Network Server.	Null
Confirmed	After enabled, the end device will receive downlink packet and should answer "confirmed" to the network server. Multicast feature does not support confirmed downlink.	Disabled

Table 3-2-2-12 Send Data to Device Parameters

Network Server	
Item	Description
Device EUI/Group	Show the EUI of the device or multicast group.
Frequency	Show the used frequency to transmit packets.
Datarate	Show the used datarate to transmit packets.
SNR	Show the signal-noise ratio.
RSSI	Show the received signal strength indicator.
Size	Show the size of payload.
Fcnt	Show the frame counter.
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	Show the time of packet was sent or received.

Table 3-2-2-13 Packet Parameters

Click  to get more details about the packet. As shown:

Packet Details	
Dev Addr/Multicast Addr	0614B991
GwEUI	24E124FFFEF0E225
AppEUI	24E124C0002A0001
Device EUI/Group Name	24E124126A210644
Class Type	Class C
Immediately	-
Timestamp	2721022973
Type	UpUnc
Adr	false
AdrAckReq	false
Ack	false
Fcnt	969
Port	85

Figure 3-2-2-15

Item	Description
Dev Addr/Multicast Addr	Show the address of the device/multicast group.
GwEUI	Show the EUI of the gateway.
AppEUI	Show the EUI of the application.
DevEUI/Group Name	Show the EUI of the device/multicast group name.
Class Type	Show the class type of the device or multicast group.
Immediately	True: Device may transmit an explicit (possibly empty) acknowledgement data message immediately after the reception of a data message requiring a confirmation.
Timestamp	Show the timestamp 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
Adr	True: The end-node has enabled ADR. False: The end-node has not enabled 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	True: This frame is ACK. False: This frame is not ACK.
Fcnt	Show the frame-counter of this packet. The network server tracks the uplink frame counter and generates the downlink counter for each end-device.
FPort	FPort is a multiplexing port field. If the frame payload field is not empty, the port field must be present. If present, a FPort 16 value of 0 indicates that the FRMPayload contains MAC commands only. When this is the case, the FOptsLen field must be zero. FOptsLen is the length of the FOpts field in bytes.
Modulation	LoRa means the physical layer uses the LoRa modulation.
Bandwidth	Show the bandwidth of this channel.
SpreadFactor	Show the spreadFactor of this channel.
Bitrate	Show the bitrate of this channel.
CodeRate	Show the coderate of this channel.
SNR	Show the SNR of this channel.
RSSI	Show the RSSI of this channel.
Power	Show the transmit power of the device.
Payload (b64)	Show the application payload of this packet.
Payload (hex)	Show the application payload of this packet.
MIC	Show the MIC of this packet. MIC is a cryptographic message integrity code, computed over the fields MHDR, FHDR, FPort and the encrypted FRMPayload.

Table 3-2-2-14 Packets Details Parameters

Related Topic

[Send Data to Device](#)

3.3 Network

3.3.1 Interface

3.3.1.1 Port

The Ethernet port can be connected with Ethernet cable to get Internet access. It supports 3 connection types.

- **Static IP:** configure IP address, netmask and gateway for Ethernet WAN interface.
- **DHCP Client:** configure Ethernet WAN interface as DHCP Client to obtain IP address automatically.
- **PPPoE:** configure Ethernet WAN interface as PPPoE Client.

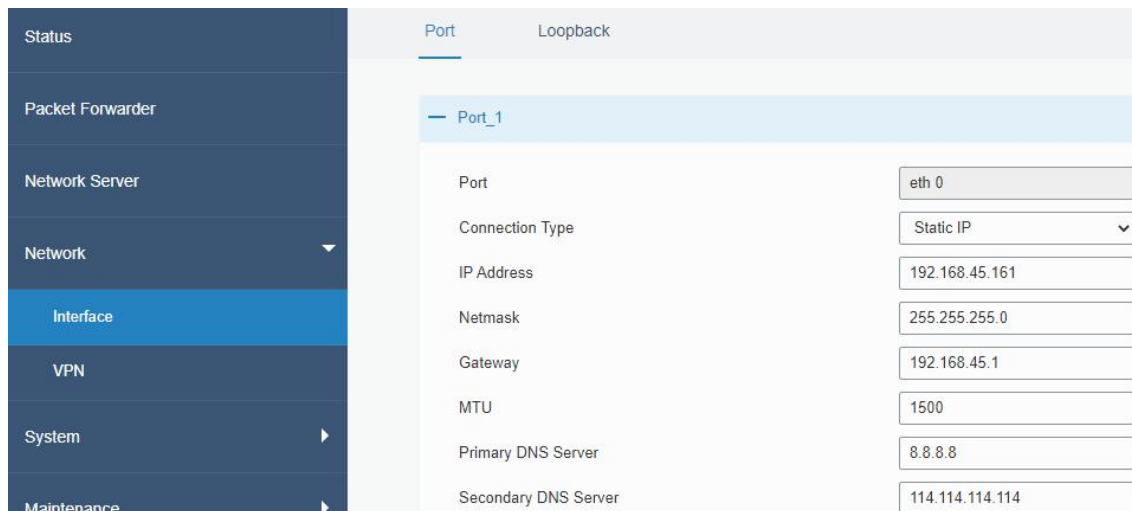


Figure 3-3-1-1

Port Setting		
Item	Description	Default
Port	The port that is fixed as eth0 port and enabled.	eth 0
Connection Type	Select from "Static IP", "DHCP Client" and "PPPoE".	Static IP
MTU	Set the maximum transmission unit.	1500
Primary DNS Server	Set the primary DNS.	8.8.8.8
Secondary DNS Server	Set the secondary DNS.	114.114.114.1 14

Table 3-3-1-1 Port Parameters

Related Configuration Example

[Ethernet Connection](#)

1. Static IP Configuration

If the external network assigns a fixed IP for the Ethernet port, user can select "Static IP" mode.

Figure 3-3-1-2

Static IP		
Item	Description	Default
IP Address	Set the IP address which can access Internet.	192.168.23.150
Netmask	Set the Netmask for Ethernet port.	255.255.255.0
Gateway	Set the gateway's IP address for Ethernet port.	192.168.23.1
Multiple IP Address	Set the multiple IP addresses for Ethernet port.	Null

Table 3-3-1-2 Static IP Parameters

2. DHCP Client

If the external network has DHCP server enabled and has assigned IP addresses to the Ethernet WAN interface, user can select “DHCP client” mode to obtain IP address automatically.

Figure 3-3-1-3

DHCP Client	
Item	Description
Use Peer DNS	Obtain peer DNS automatically during PPP dialing. DNS is necessary when user visits domain name.

Table 3-3-1-3 DHCP Client Parameters

3. PPPoE

PPPoE refers to a point-to-point protocol over Ethernet. User has to install a PPPoE client on the basis of original connection way. With PPPoE, remote access devices can get control of each user.

The screenshot shows a configuration window for 'Port_1'. The settings are as follows:

- Port: eth 0
- Connection Type: PPPoE (dropdown menu)
- Username: (empty text field)
- Password: (empty text field)
- Link Detection Interval(s): 60
- Max Retries: 0
- MTU: 1500
- Use Peer DNS:
- Primary DNS Server: 8.8.8.8
- Secondary DNS Server: 114.114.114.114

Figure 3-3-1-4

PPPoE	
Item	Description
Username	Enter the username provided by your Internet Service Provider (ISP).
Password	Enter the password provided by your Internet Service Provider (ISP).
Link Detection Interval (s)	Set the heartbeat interval for link detection. Range: 1-600.
Max Retries	Set the maximum retry times after it fails to dial up. Range: 0-9.
Use Peer DNS	Obtain peer DNS automatically during PPP dialing. DNS is necessary when user visits domain name.

Table 3-3-1-4 PPOE Parameters

3.3.1.2 Loopback

Loopback interface is used for replacing gateway's ID as long as it is activated. When the interface is DOWN, the ID of the gateway has to be selected again which leads to long convergence time of OSPF. Therefore, Loopback interface is generally recommended as

the ID of the gateway.

Loopback interface is a logic and virtual interface on gateway. Under default conditions, there's no loopback interface on gateway, but it can be created as required.

Figure 3-3-1-5

Loopback		
Item	Description	Default
IP Address	Unalterable	127.0.0.1
Netmask	Unalterable	255.0.0.0
Multiple IP Addresses	Apart from the IP above, user can configure other IP addresses.	Null

Table 3-3-1-5 Loopback Parameters

3.3.2 VPN

Virtual Private Networks, also called VPNs, are used to securely connect two private networks together so that devices can connect from one network to the other network via secure channels.

UG63 supports DMVPN, IPsec, GRE, L2TP, PPTP, OpenVPN, as well as GRE over IPsec and L2TP over IPsec.

3.3.2.1 DMVPN

A dynamic multi-point virtual private network (DMVPN), combining mGRE and IPsec, is a secure network that exchanges data between sites without passing traffic through an organization's headquarter VPN server or gateway.

DMVPN	IPsec	GRE	L2TP	PPTP	OpenVPN Client
DMVPN Settings					
Enable		<input checked="" type="checkbox"/>			
Hub Address		<input type="text"/>			
Local IP Address		<input type="text"/>			
GRE HUB IP Address		<input type="text"/>			
GRE Local IP Address		<input type="text"/>			
GRE Mask		<input type="text" value="255.255.255.0"/>			
GRE Key		<input type="text"/>			
Negotiation Mode		<input type="text" value="Main"/>			
Authentication Algorithm		<input type="text" value="DES"/>			
Encryption Algorithm		<input type="text" value="MD5"/>			
DH Group		<input type="text" value="MODP768-1"/>			
Key		<input type="text"/>			
Local ID Type		<input type="text" value="Default"/>			
IKE Life Time(s)		<input type="text" value="10800"/>			
SA Algorithm		<input type="text" value="DES-MD5"/>			
PFS Group		<input type="text" value="NULL"/>			
Life Time(s)		<input type="text" value="3600"/>			

Figure 3-3-2-1

DPD Time Interval(s)	<input type="text" value="30"/>
DPD Timeout(s)	<input type="text" value="150"/>
Cisco Secret	<input type="text"/>
NHRP Holdtime(s)	<input type="text" value="7200"/>

Figure 3-3-2-2

DMVPN	
Item	Description
Enable	Enable or disable DMVPN.
Hub Address	The IP address or domain name of DMVPN Hub.
Local IP address	DMVPN local tunnel IP address.
GRE Hub IP Address	GRE Hub tunnel IP address.
GRE Local IP Address	GRE local tunnel IP address.
GRE Netmask	GRE local tunnel netmask.
GRE Key	GRE tunnel key.
Negotiation Mode	Select from "Main" and "Aggressive".
Authentication Algorithm	Select from "DES", "3DES", "AES128", "AES192" and "AES256".
Encryption Algorithm	Select from "MD5" and "SHA1".

DH Group	Select from "MODP768_1", "MODP1024_2" and "MODP1536_5".
Key	Enter the preshared key.
Local ID Type	Select from "Default", "ID", "FQDN", and "User FQDN"
IKE Life Time (s)	Set the lifetime in IKE negotiation. Range: 60-86400.
SA Algorithm	Select from "DES_MD5", "DES_SHA1", "3DES_MD5", "3DES_SHA1", "AES128_MD5", "AES128_SHA1", "AES192_MD5", "AES192_SHA1", "AES256_MD5" and "AES256_SHA1".
PFS Group	Select from "NULL", "MODP768_1", "MODP1024_2" and "MODP1536-5".
Life Time (s)	Set the lifetime of IPsec SA. Range: 60-86400.
DPD Interval Time (s)	Set DPD interval time
DPD Timeout (s)	Set DPD timeout.
Cisco Secret	Cisco Nhrp key.
NHRP Holdtime (s)	The holdtime of Nhrp protocol.

Table 3-3-2-1 DMVPN Parameters

3.3.2.2 IPsec

IPsec is especially useful for implementing virtual private networks and for remote user access through dial-up connection to private networks. A big advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers.

IPsec provides three choices of security service: Authentication Header (AH), Encapsulating Security Payload (ESP), and Internet Key Exchange (IKE). AH essentially allows authentication of the senders' data. ESP supports both authentication of the sender and data encryption. IKE is used for cipher code exchange. All of them can protect one and more data flows between hosts, between host and gateway, and between gateways.

DMVPN **IPsec** GRE L2TP PPTP OpenVPN Client

IPsec Settings

— IPsec_1

Enable

IPsec Gateway Address

IPsec Mode

IPsec Protocol

Local ID Type

Remote Subnet

Remote Subnet Mask

Remote ID Type

Figure 3-3-2-3

IPsec	
Item	Description
Enable	Enable IPsec tunnel. A maximum of 3 tunnels is allowed.
IPsec Gateway Address	Enter the IP address or domain name of remote IPsec server.
IPsec Mode	Select from "Tunnel" and "Transport".
IPsec Protocol	Select from "ESP" and "AH".
Local ID Type	Select from "Default", "ID", "FQDN", and "User FQDN".
Remote Subnet	Enter the remote subnet IP address that IPsec protects.
Remote Subnet Mask	Enter the remote netmask that IPsec protects.
Remote ID type	Select from "Default", "ID", "FQDN", and "User FQDN".

Table 3-3-2-2 IPsec Parameters

IKE Parameter	<input checked="" type="checkbox"/>
IKE Version	IKEv1
Negotiation Mode	Main
Encryption Algorithm	DES
Authentication Algorithm	MD5
DH Group	MODP768-1
Local Authentication	PSK
Local Secrets	
XAUTH	<input type="checkbox"/>
Lifetime(s)	10800
SA Parameter	<input checked="" type="checkbox"/>
SA Algorithm	DES-MD5
PFS Group	NULL
Lifetime(s)	3600
DPD Time Interval(s)	30
DPD Timeout(s)	150
IPsec Advanced	<input checked="" type="checkbox"/>
Enable Compression	<input type="checkbox"/>
VPN Over IPsec Type	NONE

Figure 3-3-2-4

IKE Parameter	
Item	Description
IKE Version	Select from "IKEv1" and "IKEv2".
Negotiation Mode	Select from "Main" and "Aggressive".
Encryption Algorithm	Select from "DES", "3DES", "AES128", "AES192" and "AES256".
Authentication Algorithm	Select from "MD5" and "SHA1"
DH Group	Select from "MODP768_1", "MODP1024_2" and "MODP1536_5".
Local Authentication	Select from "PSK" and "CA".
Local Secrets	Enter the preshared key.
XAUTH	Enter XAUTH username and password after XAUTH is enabled.
Lifetime (s)	Set the lifetime in IKE negotiation. Range: 60-86400.
SA Parameter	
SA Algorithm	Select from "DES_MD5", "DES_SHA1", "3DES_MD5", "3DES_SHA1", "AES128_MD5", "AES128_SHA1", "AES192_MD5", "AES192_SHA1", "AES256_MD5" and "AES256_SHA1".
PFS Group	Select from "NULL", "MODP768_1", "MODP1024_2" and "MODP1536_5".
Lifetime (s)	Set the lifetime of IPsec SA. Range: 60-86400.

DPD Interval Time(s)	Set DPD interval time to detect if the remote side fails.
DPD Timeout(s)	Set DPD timeout. Range: 10-3600.
IPsec Advanced	
Enable Compression	The head of IP packet will be compressed after it's enabled.
VPN Over IPsec Type	Select from "NONE", "GRE" and "L2TP" to enable VPN over IPsec function.

Table 3-3-2-3 IPsec Parameters

3.3.2.3 GRE

Generic Routing Encapsulation (GRE) is a protocol that encapsulates packets in order to route other protocols over IP networks. It's a tunneling technology that provides a channel through which encapsulated data message can be transmitted and encapsulation and decapsulation can be realized at both ends.

In the following circumstances the GRE tunnel transmission can be applied:

- GRE tunnel can transmit multicast data packets as if it were a true network interface. Single use of IPsec cannot achieve the encryption of multicast.
- A certain protocol adopted cannot be routed.
- A network of different IP addresses shall be required to connect other two similar networks.

The screenshot displays the 'GRE Settings' configuration page. At the top, there are tabs for 'DMVPN', 'IPsec', 'GRE' (selected), 'L2TP', and 'PPTP'. Below the tabs, the 'GRE Settings' section is visible, with a sub-section for 'GRE_1'. The configuration includes the following items:

- Enable:** A checked checkbox.
- Remote IP Address:** An empty text input field.
- Local IP Address:** An empty text input field.
- Local Virtual IP Address:** An empty text input field.
- Netmask:** A text input field containing '255.255.255.0'.
- Peer Virtual IP Address:** An empty text input field.
- Global Traffic Forwarding:** An unchecked checkbox.
- Remote Subnet:** An empty text input field.
- Remote Netmask:** An empty text input field.
- MTU:** A text input field containing '1500'.
- Key:** An empty text input field.

Figure 3-3-2-5

GRE	
Item	Description
Enable	Check to enable GRE function.

Remote IP Address	Enter the real remote IP address of GRE tunnel.
Local IP Address	Set the local IP address.
Local Virtual IP Address	Set the local tunnel IP address of GRE tunnel.
Netmask	Set the local netmask.
Peer Virtual IP Address	Enter remote tunnel IP address of GRE tunnel.
Global Traffic Forwarding	All the data traffic will be sent out via GRE tunnel when this function is enabled.
Remote Subnet	Enter the remote subnet IP address of GRE tunnel.
Remote Netmask	Enter the remote netmask of GRE tunnel.
MTU	Enter the maximum transmission unit. Range: 64-1500.
Key	Set GRE tunnel key.

Table 3-3-2-4 GRE Parameters

3.3.2.4 L2TP

Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by an Internet service provider (ISP) to enable the operation of a virtual private network (VPN) over the Internet.

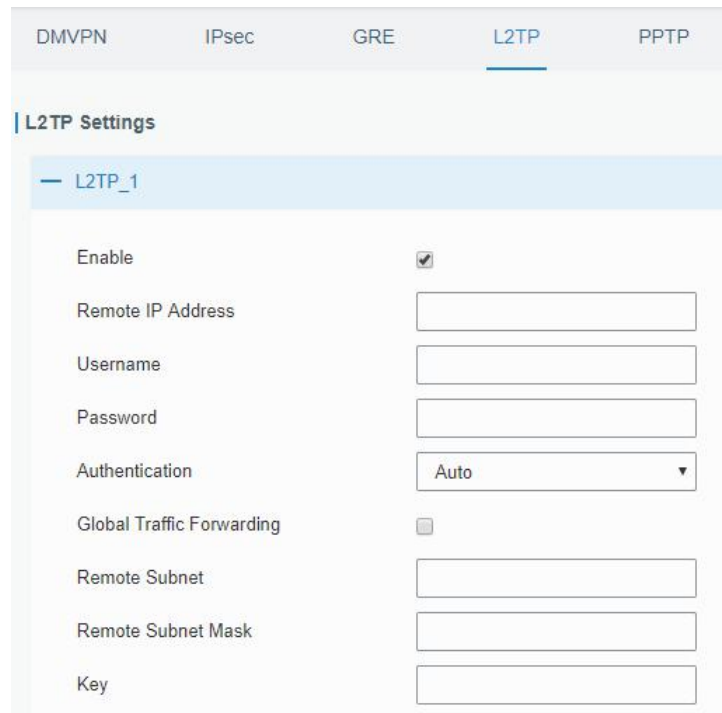


Figure 3-3-2-6

L2TP	
Item	Description
Enable	Check to enable L2TP function.
Remote IP Address	Enter the public IP address or domain name of L2TP server.
Username	Enter the username that L2TP server provides.
Password	Enter the password that L2TP server provides.
Authentication	Select from "Auto", "PAP", "CHAP", "MS-CHAPv1" and

	"MS-CHAPv2".
Global Traffic Forwarding	All of the data traffic will be sent out via L2TP tunnel after this function is enabled.
Remote Subnet	Enter the remote IP address that L2TP protects.
Remote Subnet Mask	Enter the remote netmask that L2TP protects.
Key	Enter the password of L2TP tunnel.

Table 3-3-2-5 L2TP Parameters

Advanced Settings	<input checked="" type="checkbox"/>
Local IP Address	<input type="text"/>
Peer IP Address	<input type="text"/>
Enable MPPE	<input type="checkbox"/>
Address/Control Compression	<input type="checkbox"/>
Protocol Field Compression	<input type="checkbox"/>
Asyncmap Value	<input type="text" value="ffffff"/>
MRU	<input type="text" value="1500"/>
MTU	<input type="text" value="1436"/>
Link Detection Interval(s)	<input type="text" value="60"/>
Max Retries	<input type="text" value="0"/>
Expert Options	<input type="text"/>

Figure 3-3-2-7

Advanced Settings	
Item	Description
Local IP Address	Set tunnel IP address of L2TP client. Client will obtain tunnel IP address automatically from the server when it's null.
Peer IP Address	Enter tunnel IP address of L2TP server.
Enable MPPE	Enable MPPE encryption.
Address/Control Compression	For PPP initialization. User can keep the default option.
Protocol Field Compression	For PPP initialization. User can keep the default option.
Asyncmap Value	One of the PPP protocol initialization strings. User can keep the default value. Range: 0-ffffff.
MRU	Set the maximum receive unit. Range: 64-1500.
MTU	Set the maximum transmission unit. Range: 64-1500
Link Detection Interval	Set the link detection interval time to ensure tunnel

(s)	connection. Range: 0-600.
Max Retries	Set the maximum times of retry to detect the L2TP connection failure. Range: 0-10.
Expert Options	User can enter some other PPP initialization strings in this field and separate the strings with blank space.

Table 3-3-2-6 L2TP Parameters

3.3.2.5 PPTP

Point-to-Point Tunneling Protocol (PPTP) is a protocol that allows corporations to extend their own corporate network through private "tunnels" over the public Internet. Effectively, a corporation uses a wide-area network as a single large local area network.

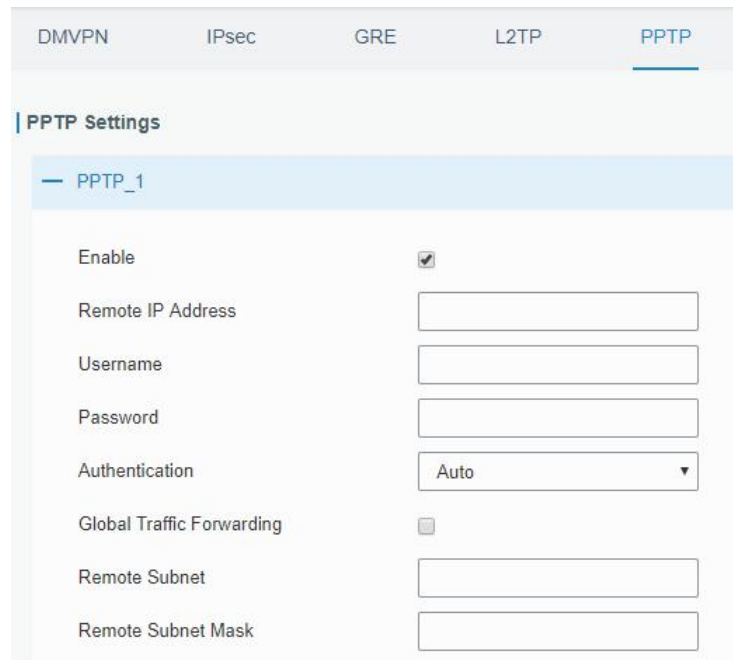


Figure 3-3-2-8

PPTP	
Item	Description
Enable	Enable PPTP client. A maximum of 3 tunnels is allowed.
Remote IP Address	Enter the public IP address or domain name of PPTP server.
Username	Enter the username that PPTP server provides.
Password	Enter the password that PPTP server provides.
Authentication	Select from "Auto", "PAP", "CHAP", "MS-CHAPv1", and "MS-CHAPv2".
Global Traffic Forwarding	All of the data traffic will be sent out via PPTP tunnel once enable this function.
Remote Subnet	Set the peer subnet of PPTP.
Remote Subnet Mask	Set the netmask of peer PPTP server.

Table 3-3-2-7 PPTP Parameters

Advanced Settings	<input checked="" type="checkbox"/>
Local IP Address	<input type="text"/>
Peer IP Address	<input type="text"/>
Enable MPPE	<input type="checkbox"/>
Address/Control Compression	<input type="checkbox"/>
Protocol Field Compression	<input type="checkbox"/>
Asyncmap Value	<input type="text" value="ffffff"/>
MRU	<input type="text" value="1500"/>
MTU	<input type="text" value="1436"/>
Link Detection Interval(s)	<input type="text" value="60"/>
Max Retries	<input type="text" value="0"/>
Expert Options	<input type="text"/>

Figure 3-3-2-9

PPTP Advanced Settings	
Item	Description
Local IP Address	Set IP address of PPTP client.
Peer IP Address	Enter tunnel IP address of PPTP server.
Enable MPPE	Enable MPPE encryption.
Address/Control Compression	For PPP initialization. User can keep the default option.
Protocol Field Compression	For PPP initialization. User can keep the default option.
Asyncmap Value	One of the PPP protocol initialization strings. User can keep the default value. Range: 0-ffffff.
MRU	Enter the maximum receive unit. Range: 0-1500.
MTU	Enter the maximum transmission unit. Range: 0-1500.
Link Detection Interval (s)	Set the link detection interval time to ensure tunnel connection. Range: 0-600.
Max Retries	Set the maximum times of retrying to detect the PPTP connection failure. Range: 0-10.
Expert Options	User can enter some other PPP initialization strings in this field and separate the strings with blank space.

Table 3-3-2-8 PPTP Parameters

3.3.2.6 OpenVPN Client

OpenVPN is an open source virtual private network (VPN) product that offers a simplified security framework, modular network design, and cross-platform portability.

Advantages of OpenVPN include:

- Security provisions that function against both active and passive attacks.
- Compatibility with all major operating systems.
- High speed (1.4 megabytes per second typically).
- Ability to configure multiple servers to handle numerous connections simultaneously.
- All encryption and authentication features of the OpenSSL library.
- Advanced bandwidth management.
- A variety of tunneling options.
- Compatibility with smart cards that support the Windows Crypt application program interface (API).

The screenshot shows the 'OpenVPN Client Settings' page with the following configuration for 'OpenVPN_1':

- Enable:
- Protocol: UDP
- Remote IP Address: (empty)
- Port: 1194
- Interface: tun
- Authentication: None
- Local Tunnel IP: (empty)
- Remote Tunnel IP: (empty)
- Compression: LZO
- Link Detection Interval(s): 60
- Link Detection Timeout(s): 300
- Cipher: None
- MTU: 1500
- Max Frame Size: 1500
- Verbose Level: ERROR
- Expert Options: (empty)

Figure 3-3-2-10

OpenVPN Client	
Item	Description
Enable	Enable OpenVPN client. A maximum of 3 tunnels is allowed.
Protocol	Select from "UDP" and "TCP".
Remote IP Address	Enter remote OpenVPN server's IP address or domain name.
Port	Enter the listening port number of remote OpenVPN server. Range: 1-65535.
Interface	Select from "tun" and "tap".
Authentication	Select from "None", "Pre-shared", "Username/Password", "X.509 cert", and "X.509 cert+user".

Local Tunnel IP	Set local tunnel address.
Remote Tunnel IP	Enter remote tunnel address.
Global Traffic Forwarding	All the data traffic will be sent out via OpenVPN tunnel when this function is enabled.
Enable TLS Authentication	Check to enable TLS authentication.
Username	Enter username provided by OpenVPN server.
Password	Enter password provided by OpenVPN server.
Compression	Select LZO to compress data.
Link Detection Interval (s)	Set link detection interval time to ensure tunnel connection. Range: 10-1800.
Link Detection Timeout (s)	Set link detection timeout. OpenVPN will be reestablished after timeout. Range: 60-3600.
Cipher	Select from "NONE", "BF-CBC", "DE-CBC", "DES-EDE3-CBC", "AES-128-CBC", "AES-192-CBC" and "AES-256-CBC".
MTU	Enter the maximum transmission unit. Range: 128-1500.
Max Frame Size	Set the maximum frame size. Range: 128-1500.
Verbose Level	Select from "ERROR", "WARNING", "NOTICE" and "DEBUG".
Expert Options	User can enter some other PPP initialization strings in this field and separate the strings with blank space.

Table 3-3-2-9 OpenVPN Client Parameters

3.3.2.7 Certifications

User can import/export certificate and key files for OpenVPN and IPsec on this page.

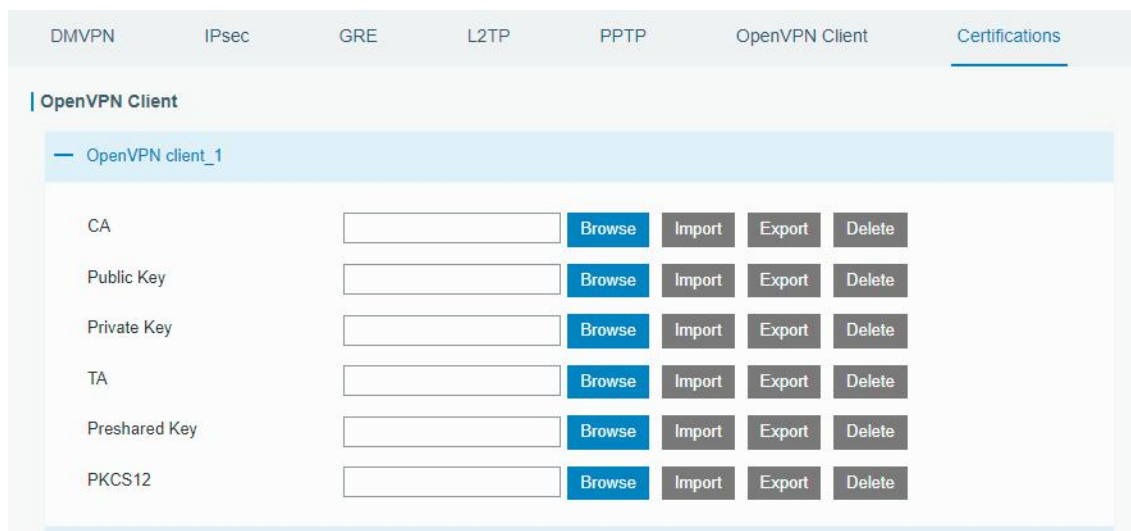


Figure 3-3-2-13

OpenVPN Client	
Item	Description
CA	Import/Export CA certificate file.
Public Key	Import/Export public key file.

Private Key	Import/Export private key file.
TA	Import/Export TA key file.
Preshared Key	Import/Export static key file.
PKCS12	Import/Export PKCS12 certificate file.

Table 3-3-2-11 OpenVPN Client Certification Parameters

The screenshot shows a web-based configuration interface for IPsec. At the top, there is a header 'IPsec' and a sub-header 'IPsec_1'. Below this, there are five rows of configuration fields:

- CA:** A text input field followed by a blue 'Browse' button and three grey buttons labeled 'Import', 'Export', and 'Delete'.
- Client Key:** A text input field followed by a blue 'Browse' button and three grey buttons labeled 'Import', 'Export', and 'Delete'.
- Server Key:** A text input field followed by a blue 'Browse' button and three grey buttons labeled 'Import', 'Export', and 'Delete'.
- Private Key:** A text input field followed by a blue 'Browse' button and three grey buttons labeled 'Import', 'Export', and 'Delete'.
- CRL:** A text input field followed by a blue 'Browse' button and three grey buttons labeled 'Import', 'Export', and 'Delete'.

Figure 3-3-2-14

IPsec	
Item	Description
CA	Import/Export CA certificate.
Client Key	Import/Export client key.
Server Key	Import/Export server key.
Private Key	Import/Export private key.
CRL	Import/Export certificate recovery list.

Table 3-3-2-12 IPsec Parameters

3.4 System

This section describes how to configure general settings, such as administration account, access service, system time, common user management, SNMP, event alarms, etc.

3.4.1 General Settings

3.4.1.1 General

General settings include system info, access service and HTTPS certificates.

General System Time SMTP Email

| System

Hostname

Web Login Timeout(s)

| Access Service

Enable	Service	Port
<input checked="" type="checkbox"/>	HTTP	<input type="text" value="80"/>
<input checked="" type="checkbox"/>	HTTPS	<input type="text" value="443"/>
<input type="checkbox"/>	TELNET	<input type="text" value="23"/>
<input checked="" type="checkbox"/>	SSH	<input type="text" value="22"/>

| HTTPS Certificates

Certificate

Key

Figure 3-4-1-1

General		
Item	Description	Default
System		
Hostname	User-defined gateway name, needs to start with a letter.	GATEWAY
Web Login Timeout (s)	You need to log in again if it times out. Range: 100-3600.	1800
Access Service		
Port	Set port number of the services. Range: 1-65535.	--
HTTP	Users can log in the device locally via HTTP to access and control it through Web after the option is checked.	80
HTTPS	Users can log in the device locally and remotely via HTTPS to access and control it through Web after option is checked.	443
TELNET	Users can log in the device locally and remotely via TELNET to access and control it through Web after option is checked.	23
SSH	Users can log in the device locally and remotely via SSH after the option is checked.	22
HTTPS Certificates		
Certificate	Click "Browse" button, choose certificate file on the PC, and then click "Import" button to upload the file into gateway. Click "Export" button will export the file to the	--

	PC. Click "Delete" button will delete the file.	
Key	Click "Browse" button, choose key file on the PC, and then click "Import" button to upload the file into gateway. Click "Export" button will export file to the PC. Click "Delete" button will delete the file.	--

Table 3-4-1-1 General Setting Parameters

3.4.1.2 System Time

This section explains how to set the system time including time zone and time synchronization type.

Note: to ensure that the gateway runs with the correct time, it's recommended that you set the system time when configuring the gateway.

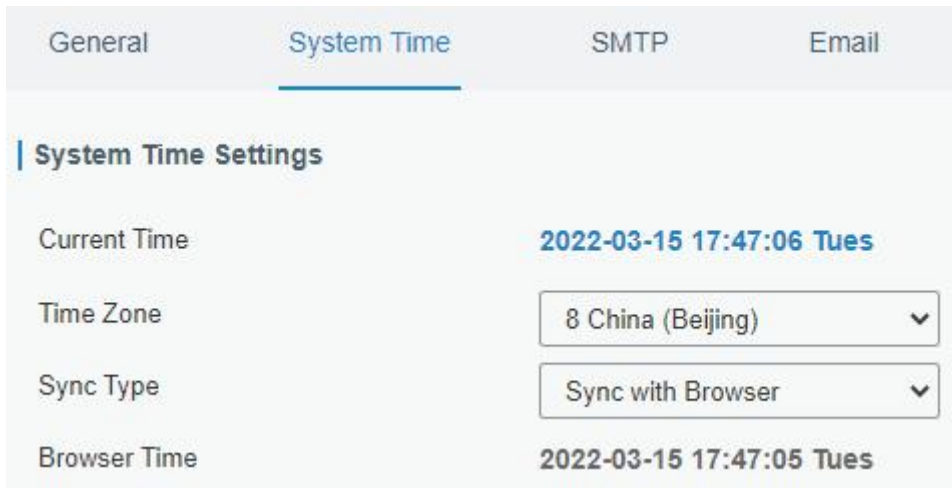


Figure 3-4-1-2



Figure 3-4-1-3

Figure 3-4-1-4

System Time	
Item	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.
Browser Time	Show the current time of browser.
Set up Manually	Manually configure the system time.
Sync with NTP Server	Synchronize time with NTP server so as to achieve time synchronization of all devices equipped with a clock on network.
Sync with NTP Server	
NTP Server Address	Set NTP server address (domain name/IP).
Enable NTP Server	NTP client on the network can achieve time synchronization with gateway after "Enable NTP Server" option is checked.

Table 3-4-1-2 System Time Parameters

3.4.1.3 SMTP

SMTP, short for Simple Mail Transfer Protocol, is a TCP/IP protocol used in sending and receiving e-mail. This section describes how to configure email settings.

Figure 3-4-1-5

SMTP	
Item	Description
SMTP Client Settings	
Enable	Enable or disable SMTP client function.
Email Address	Enter the sender's email account.
Password	Enter the sender's email password.
SMTP Server Address	Enter SMTP server's domain name.
Port	Enter SMTP server port. Range: 1-65535.
Enable TLS	Enable or disable TLS encryption.

Table 3-4-1-3 SMTP Setting

Related Topics

[Events Setting](#)

3.4.1.4 Email

Email settings involve email alarm for events.

Figure 3-4-1-6

Email	
Item	Description
Email List	

Name	Set Email group name.
Email Address	Enter the Email address. You can divide multiple Email addresses by “;”.

Table 3-4-1-4 Email Settings

3.4.2 User Management

3.4.2.1 Account

Here you can change the login username and password of the administrator.

Note: it is strongly recommended that you modify them for the sake of security.

The screenshot shows a web interface with two tabs: 'Account' (selected) and 'User Management'. Under the 'Account' tab, there is a section titled 'Change Account Info'. This section contains four input fields: 'Username' (with the value 'admin'), 'Old Password', 'New Password', and 'Confirm New Password'. Below these fields is a blue 'Save' button.

Figure 3-4-2-1

Account	
Item	Description
Username	Enter a new username. You can use characters such as a-z, 0-9, "_", "-", "\$". The first character can't be a digit.
Old Password	Enter the old password.
New Password	Enter a new password.
Confirm New Password	Enter the new password again.

Table 3-4-2-1 Account Information

3.4.2.2 User Management

This section describes how to create common user accounts.

The common user permission includes Read-Only and Read-Write.

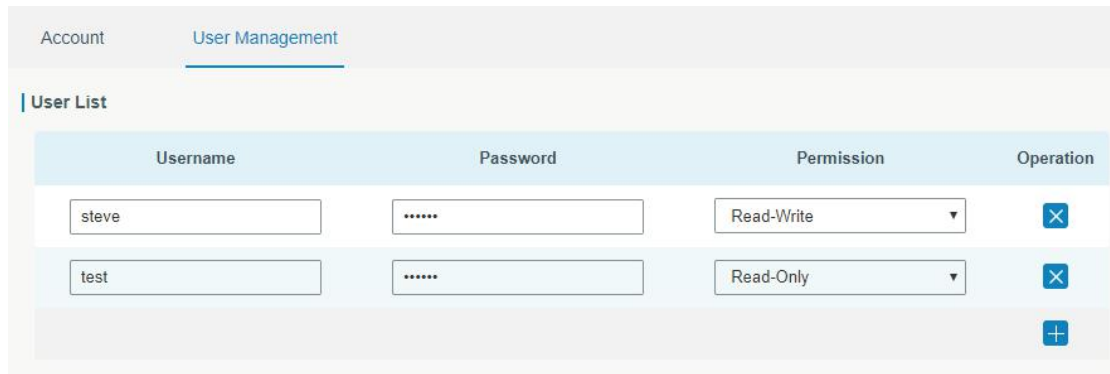


Figure 3-4-2-2

User Management	
Item	Description
Username	Enter a new username. You can use characters such as a-z, 0-9, "_", "-", "\$". The first character can't be a digit.
Password	Set password.
Permission	Select user permission from "Read-Only" and "Read-Write". <ul style="list-style-type: none"> - Read-Only: users can only view the configuration of gateway in this level. - Read-Write: users can view and set the configuration of gateway in this level.

Table 3-4-2-2 User Management

3.4.3 SNMP

SNMP is widely used in network management for network monitoring. SNMP exposes management data with variables form in managed system. The system is organized in a management information base (MIB) which describes the system status and configuration. These variables can be remotely queried by managing applications.

Configuring SNMP in networking, NMS, and a management program of SNMP should be set up at the Manager.

Configuration steps are listed as below for achieving query from NMS:

1. Enable SNMP setting.
2. Download MIB file and load it into NMS.
3. Configure MIB View.
4. Configure VCAM.

3.4.3.1 SNMP

UG63 supports SNMPv1, SNMPv2c and SNMPv3 version. SNMPv1 and SNMPv2c employ community name authentication. SNMPv3 employs authentication encryption by username and password.

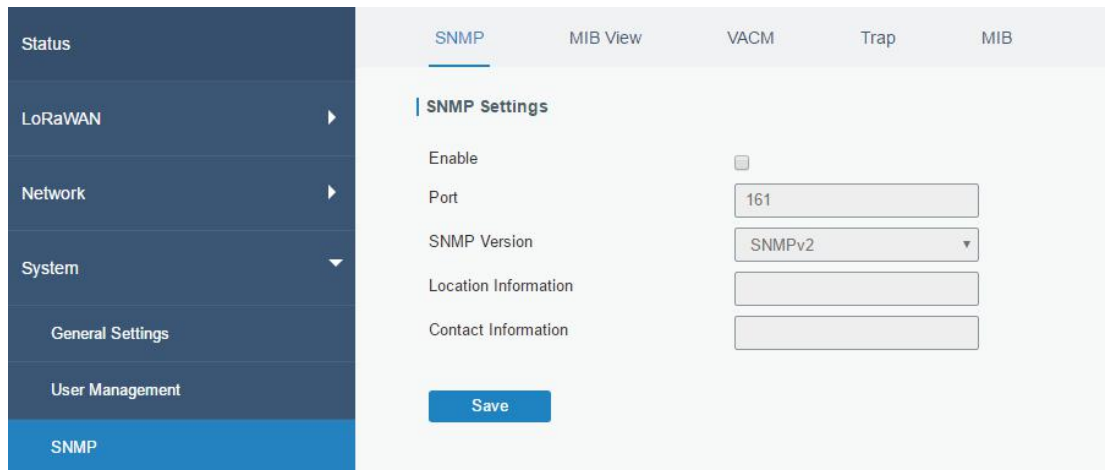


Figure 3-4-3-1

SNMP Settings	
Item	Description
Enable	Enable or disable SNMP function.
Port	Set SNMP listened port. Range: 1-65535. The default port is 161.
SNMP Version	Select SNMP version; support SNMP v1/v2c/v3.
Location Information	Fill in the location information.
Contact Information	Fill in the contact information.

Table 3-4-3-1 SNMP Parameters

3.4.3.2 MIB View

This section explains how to configure MIB view for the objects.

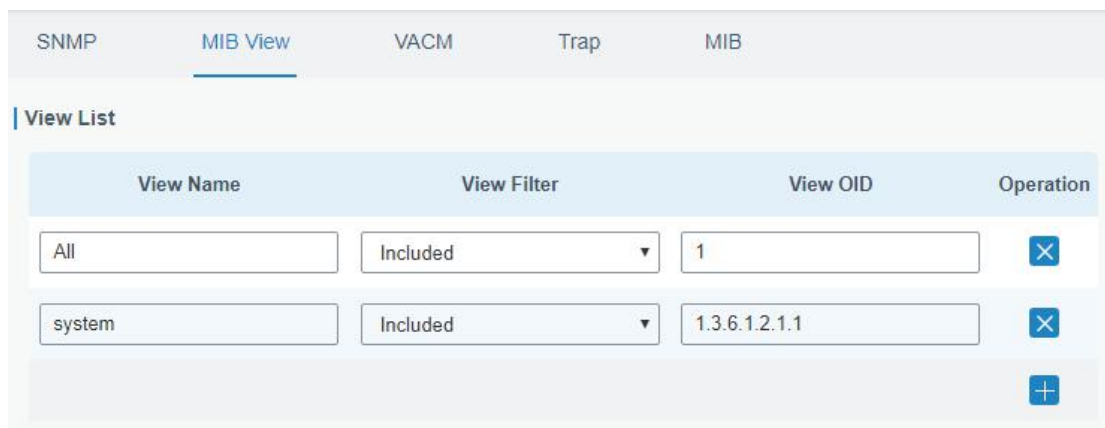


Figure 3-4-3-2

MIB View	
Item	Description
View Name	Set MIB view's name.
View Filter	Select from "Included" and "Excluded".
View OID	Enter the OID number.

Included	You can query all nodes within the specified MIB node.
Excluded	You can query all nodes except for the specified MIB node.

Table 3-4-3-2 MIB View Parameters

3.4.3.3 VACM

This section describes how to configure VACM parameters.

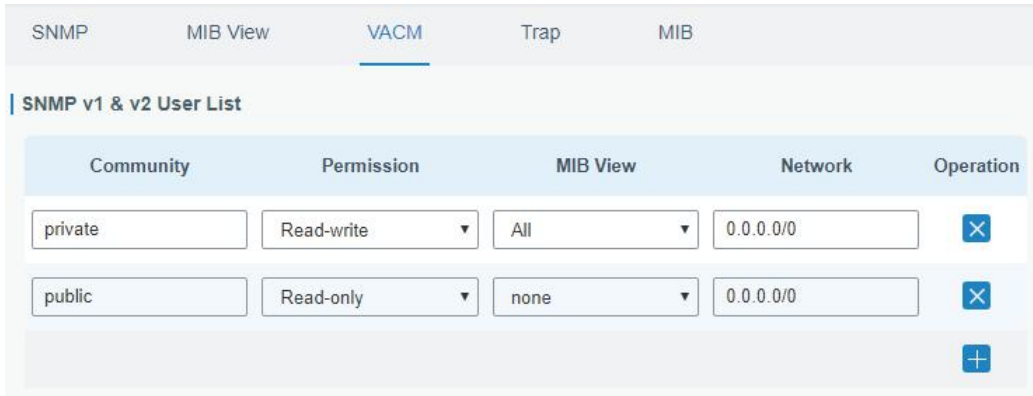


Figure 3-4-3-3

VACM	
Item	Description
SNMP v1 & v2 User List	
Community	Set the community name.
Permission	Select from "Read-Only" and "Read-Write".
MIB View	Select an MIB view to set permissions from the MIB view list.
Network	The IP address and bits of the external network accessing the MIB view.
Read-Write	The permission of the specified MIB node is read and write.
Read-Only	The permission of the specified MIB node is read only.
SNMP v3 User List	
Group Name	Set the name of SNMPv3 group.
Security Level	Select from "NoAuth/NoPriv", "Auth/NoPriv", and "Auth/Priv".
Read-Only View	Select an MIB view to set permission as "Read-only" from the MIB view list.
Read-Write View	Select an MIB view to set permission as "Read-write" from the MIB view list.
Inform View	Select an MIB view to set permission as "Inform" from the MIB view list.

Table 3-4-3-3 VACM Parameters

3.4.3.4 Trap

This section explains how to enable network monitoring by SNMP trap.

Figure 3-4-3-4

SNMP Trap	
Item	Description
Enable	Enable or disable SNMP Trap function.
SNMP Version	Select SNMP version; support SNMP v1/v2c/v3.
Server Address	Fill in NMS's IP address or domain name.
Port	Fill in UDP port. Port range is 1-65535. The default port is 162.
Name	Fill in the group name when using SNMP v1/v2c; fill in the username when using SNMP v3.
Auth/Priv Mode	Select from "NoAuth & No Priv", "Auth & NoPriv", and "Auth & Priv".

Table 3-4-3-4 Trap Parameters

3.4.3.5 MIB

This section describes how to download MIB files.

Figure 3-4-3-5

MIB	
Item	Description
MIB File	Select the MIB file you need.
Download	Click "Download" button to download the MIB file to PC.

Table 3-4-3-5 MIB Download

3.4.4 Device Management

You can connect the device to the DeviceHub on this page so as to manage the gateway centrally and remotely. For details refer to DeviceHub User Guide.

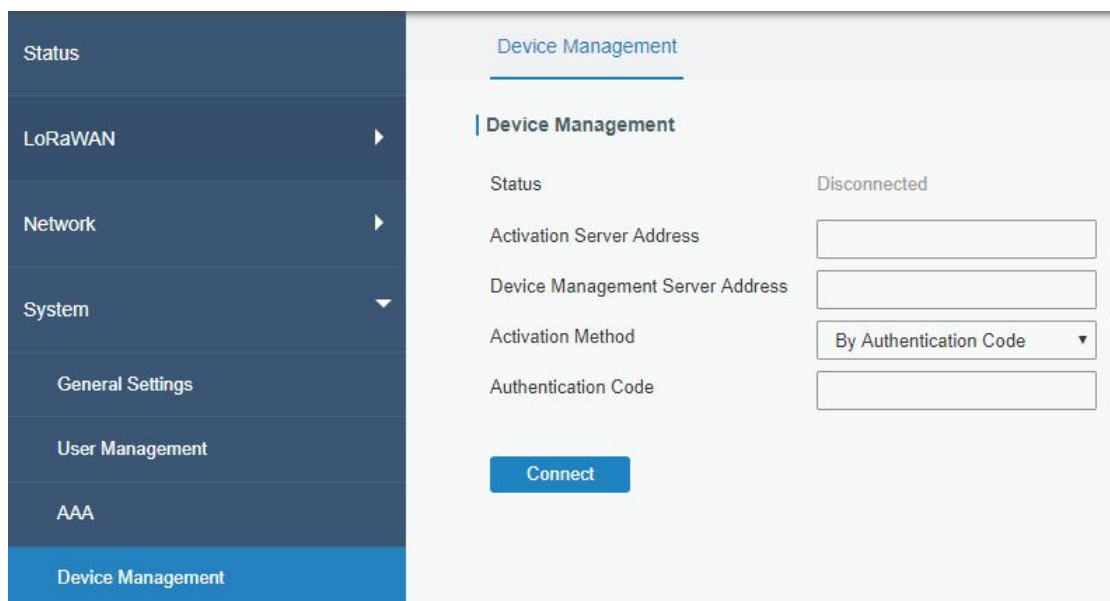


Figure 3-4-4-1

DeviceHub	
Item	Description
Status	Show the connection status between the gateway and the DeviceHub.
Disconnected	Click this button to disconnect the gateway from the DeviceHub.
Activation Server Address	IP address or domain of the DeviceHub.
DeviceHub Server Address	The URL address for the device to connect to the DeviceHub, e.g. http://220.82.63.79:8080/acs.
Activation Method	Select activation method to connect the gateway to the DeviceHub server, options are "By Authentication ID" and "By ID".
Authentication Code	Fill in the authentication code generated from the DeviceHub.
ID	Fill in the registered DeviceHub account (email) and password.
Password	

Table 3-4-4-1

3.4.5 Events

Event feature is capable of sending alerts by Email when certain system events occur.

3.4.5.1 Events

You can view alarm messages on this page.

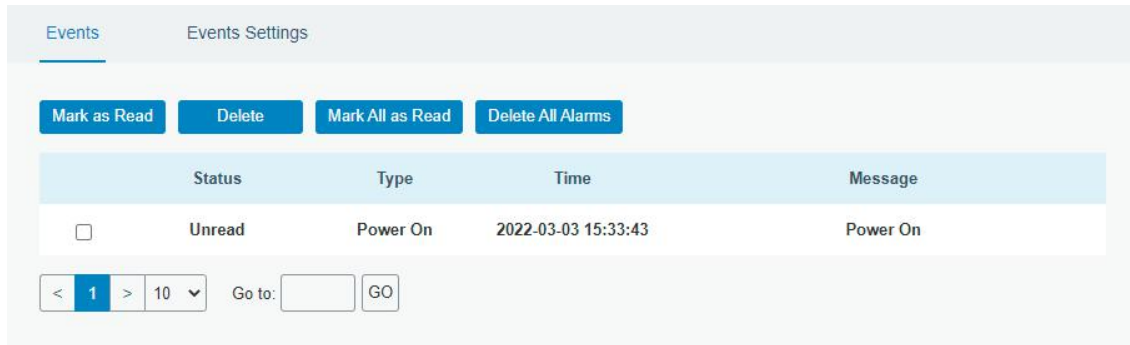


Figure 3-4-5-1

Events	
Item	Description
Mark as Read	Mark the selected event alarm as read.
Delete	Delete the selected event alarm.
Mark All as Read	Mark all event alarms as read.
Delete All Alarms	Delete all event alarms.
Status	Show the reading status of the event alarms, such as “Read” and “Unread”.
Type	Show the event type that should be alarmed.
Time	Show the alarm time.
Message	Show the alarm content.

Table 3-4-5-1 Events Parameters

3.4.5.2 Events Settings

In this section, you can decide what events to record and whether you want to receive email and SMS notifications when any change occurs.

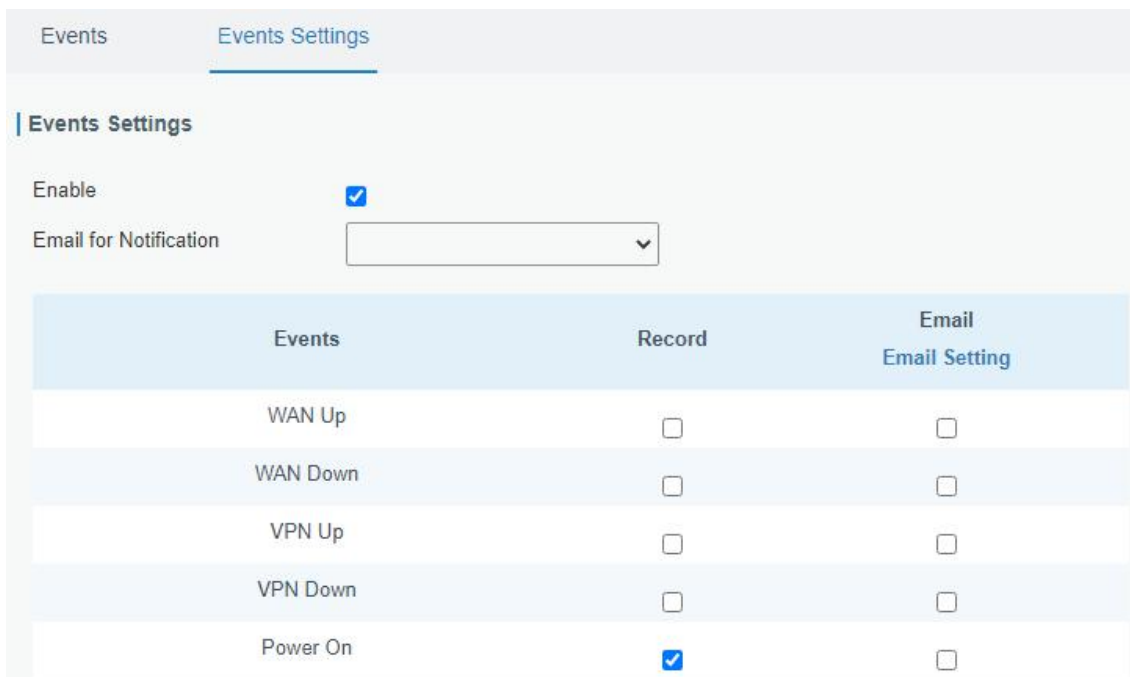


Figure 3-4-5-2

Event Settings	
Item	Description
Enable	Check to enable "Events Settings".
WAN Up	Ethernet cable is connected to WAN port.
WAN Down	Ethernet cable is disconnected to WAN port.
VPN Up	VPN is connected.
VPN Down	VPN is disconnected.
Power On	The gateway has powered on.
Record	The relevant content of event alarm will be recorded on "Event" page if this option is checked.
Email	The relevant content of event alarm will be sent out via email if this option is checked.
Email Setting	Click and you will be redirected to the page "Email" to configure the Email group.

Table 3-4-5-2 Events Parameters

Related Topics

[Email Setting](#)

3.5 Maintenance

This section describes system maintenance tools and management.

3.5.1 Tools

Troubleshooting tools includes ping and traceroute.

3.5.1.1 Ping

Ping tool is engineered to ping outer network.

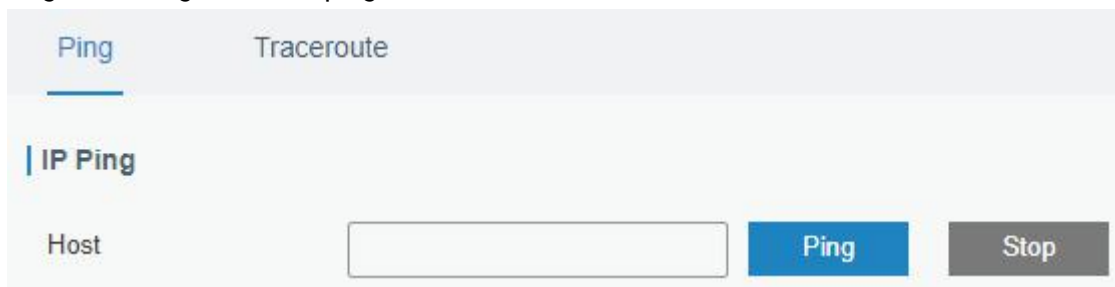


Figure 3-5-1-1

PING	
Item	Description
Host	Ping outer network from the gateway.

Table 3-5-1-1 IP Ping Parameters

3.5.1.2 Traceroute

Traceroute tool is used for troubleshooting network routing failures.

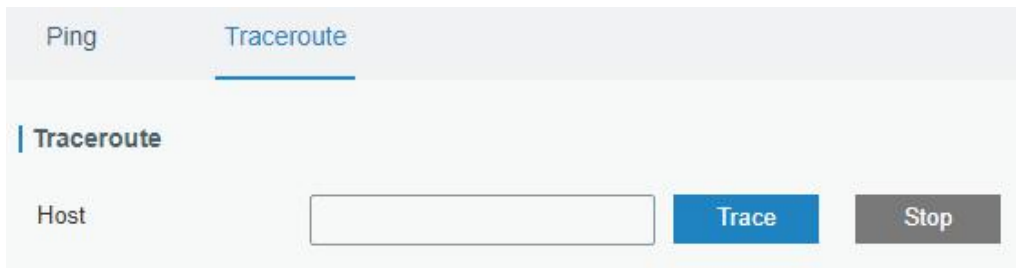


Figure 3-5-1-2

Traceroute	
Item	Description
Host	Address of the destination host to be detected.

Table 3-5-1-2 Traceroute Parameters

3.5.2 Schedule

This section explains how to configure scheduled reboot on the gateway.

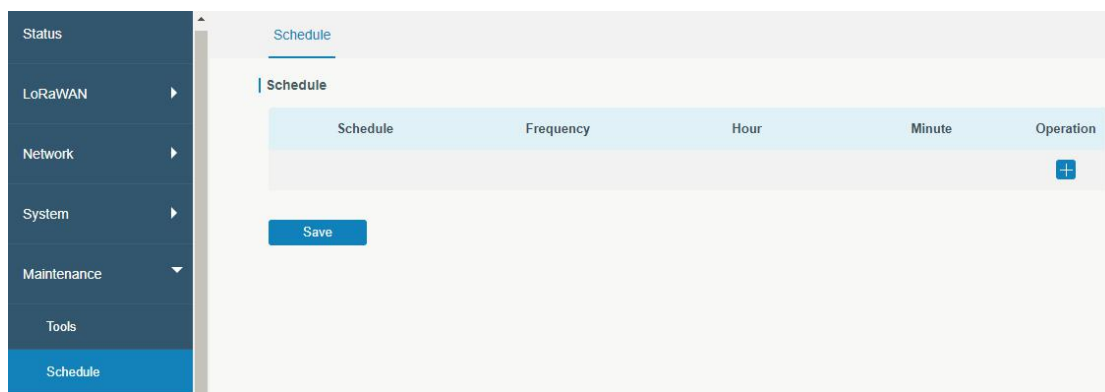


Figure 3-5-2-1

Schedule	
Item	Description
Schedule	Select schedule type.
Reboot	Reboot the gateway regularly.
Frequency	Select the frequency to execute the schedule.
Hour & Minute	Select the time to execute the schedule.

Table 3-5-2-1 Schedule Parameters

3.5.3 Log

The system log contains a record of informational, error and warning events that indicates how the system processes. By reviewing the data contained in the log, an administrator or user troubleshooting the system can identify the cause of a problem or whether the system processes are loading successfully. Remote log server is feasible, and gateway will upload all system logs to remote log server such as Syslog Watcher.

3.5.3.1 System Log

This section describes how to download log file and view the recent log on web.

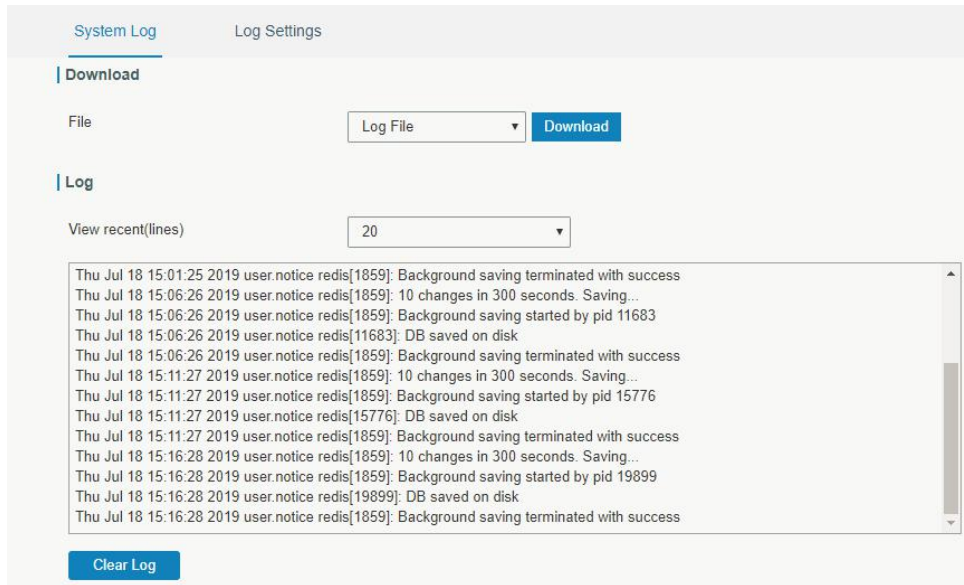


Figure 3-5-3-1

System Log	
Item	Description
Download	Download log file.
View recent (lines)	View the specified lines of system log.
Clear Log	Clear the current system log.

Table 3-5-3-1 System Log Parameters

3.5.3.2 Log Settings

This section explains how to enable remote log server and local log setting.

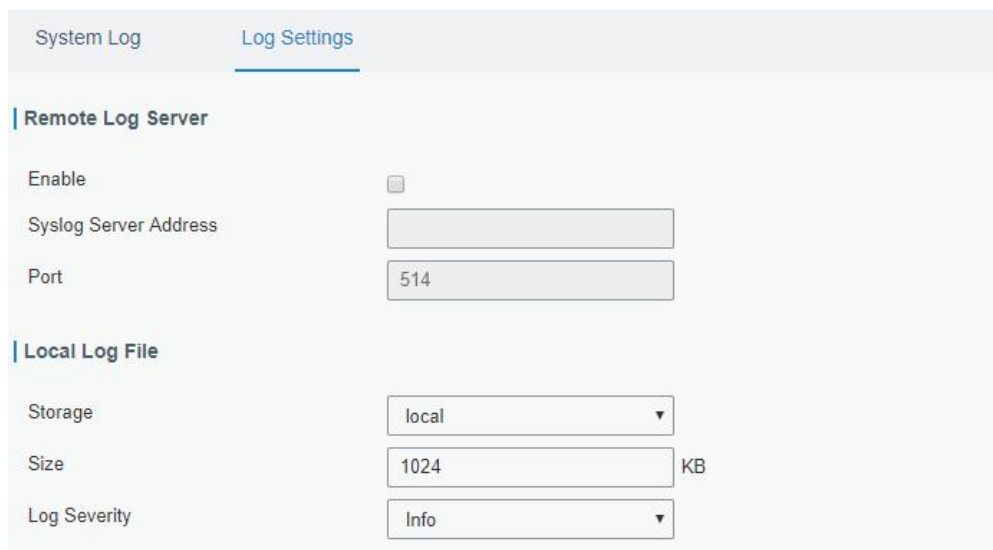


Figure 3-5-3-2

Log Settings	
Item	Description
Remote Log Server	
Enable	With "Remote Log Server" enabled, gateway will send all system logs to the remote server.
Syslog Server Address	Fill in the remote system log server address (IP/domain name).
Port	Fill in the remote system log server port.
Local Log File	
Storage	User can store the log file in memory or TF card.
Size	Set the size of the log file to be stored.
Log Severity	The list of severities follows the syslog protocol.

Table 3-5-3-2 System Log Parameters

3.5.4 Upgrade

This section describes how to upgrade the gateway firmware via web GUI. Generally, you don't need to do the firmware upgrade.

Note: any operation on web page is not allowed during firmware upgrade, otherwise the upgrade will be interrupted, or even the device will break down.

Figure 3-5-4-1

Upgrade	
Item	Description
Firmware Version	Show the current firmware version.
Reset Configuration to Factory Default	When this option is checked, the gateway will be reset to factory defaults after upgrade.
Upgrade Firmware	Click "Browse" button to select the new firmware file, and click "Upgrade" to upgrade firmware.

Table 3-5-4-1 Upgrade Parameters

Related Configuration Example

[Firmware Upgrade](#)

3.5.5 Backup and Restore

This section explains how to create a backup of the whole system configurations to a file, replicate parts of important configuration only for batch backup, restore the config file to the gateway and reset to factory defaults.

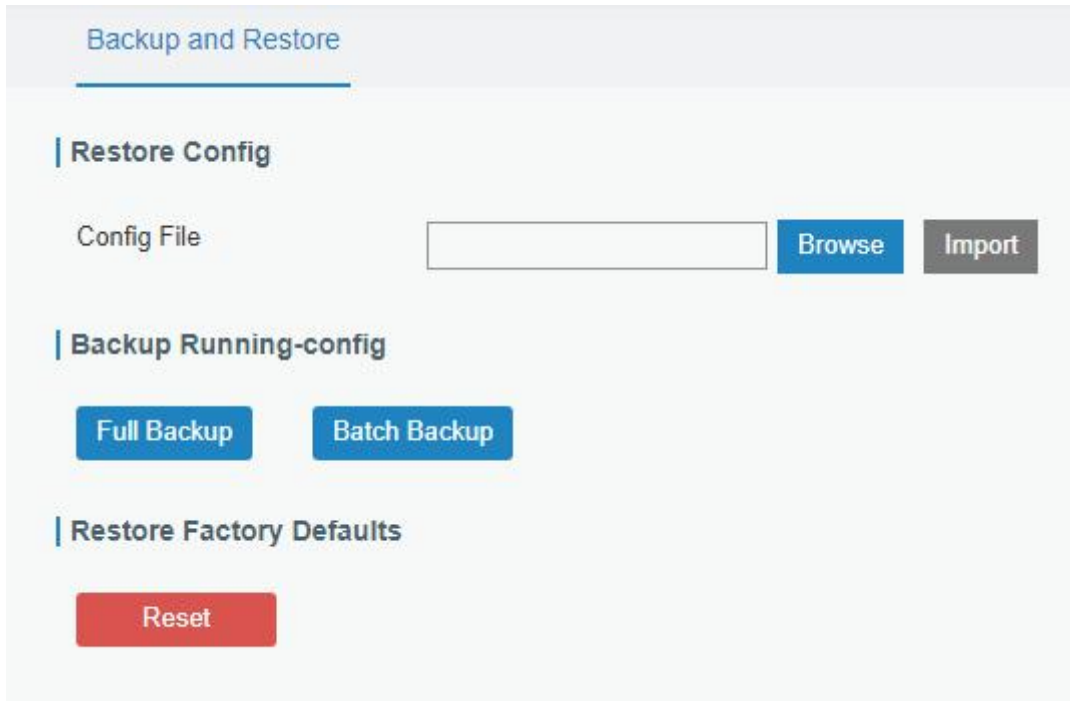


Figure 3-5-5-1

Backup and Restore	
Item	Description
Config File	Click "Browse" button to select configuration file, and then click "Import" button to upload the configuration file to the gateway.
Full Backup	Click "Full Backup" to export the current configuration file to the PC.
Batch Backup	Click "Batch Backup" to export current configuration except gateway ID of packet forwarder, all embedded NS settings, static IP address of WAN, user management settings, DeviceHub authentication code.
Reset	Click "Reset" button to reset factory default settings. gateway will restart after reset process is done.

Table 3-5-5-1 Backup and Restore Parameters

Related Configuration Example

[Restore Factory Defaults](#)

3.5.6 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.

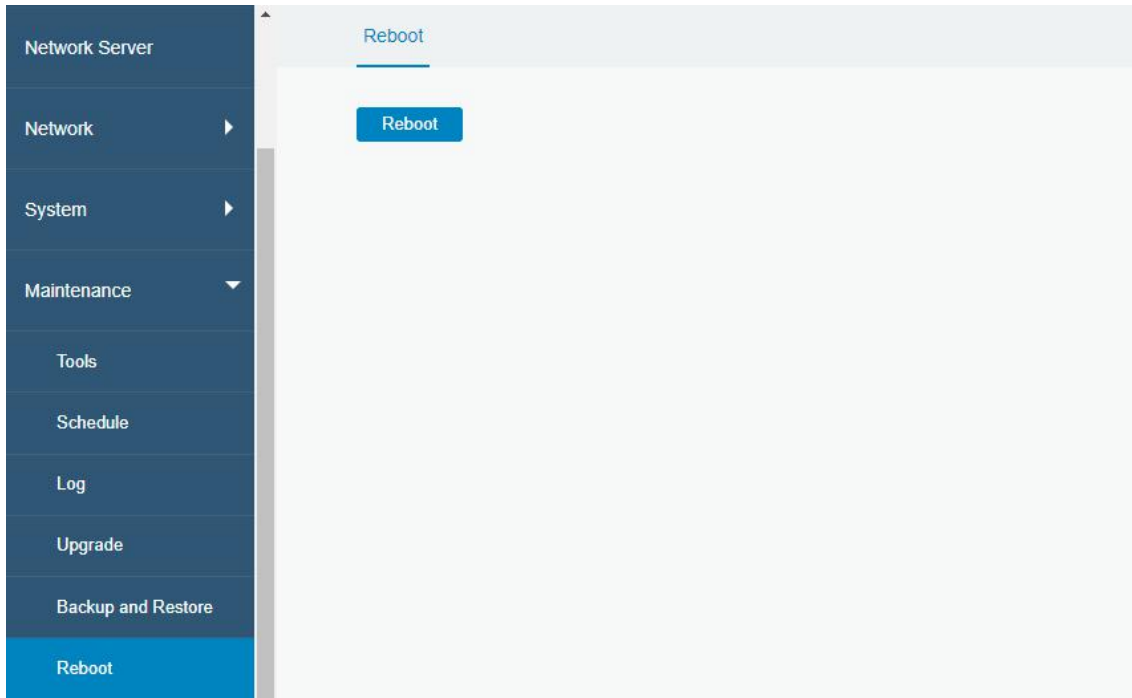


Figure 3-5-6-1

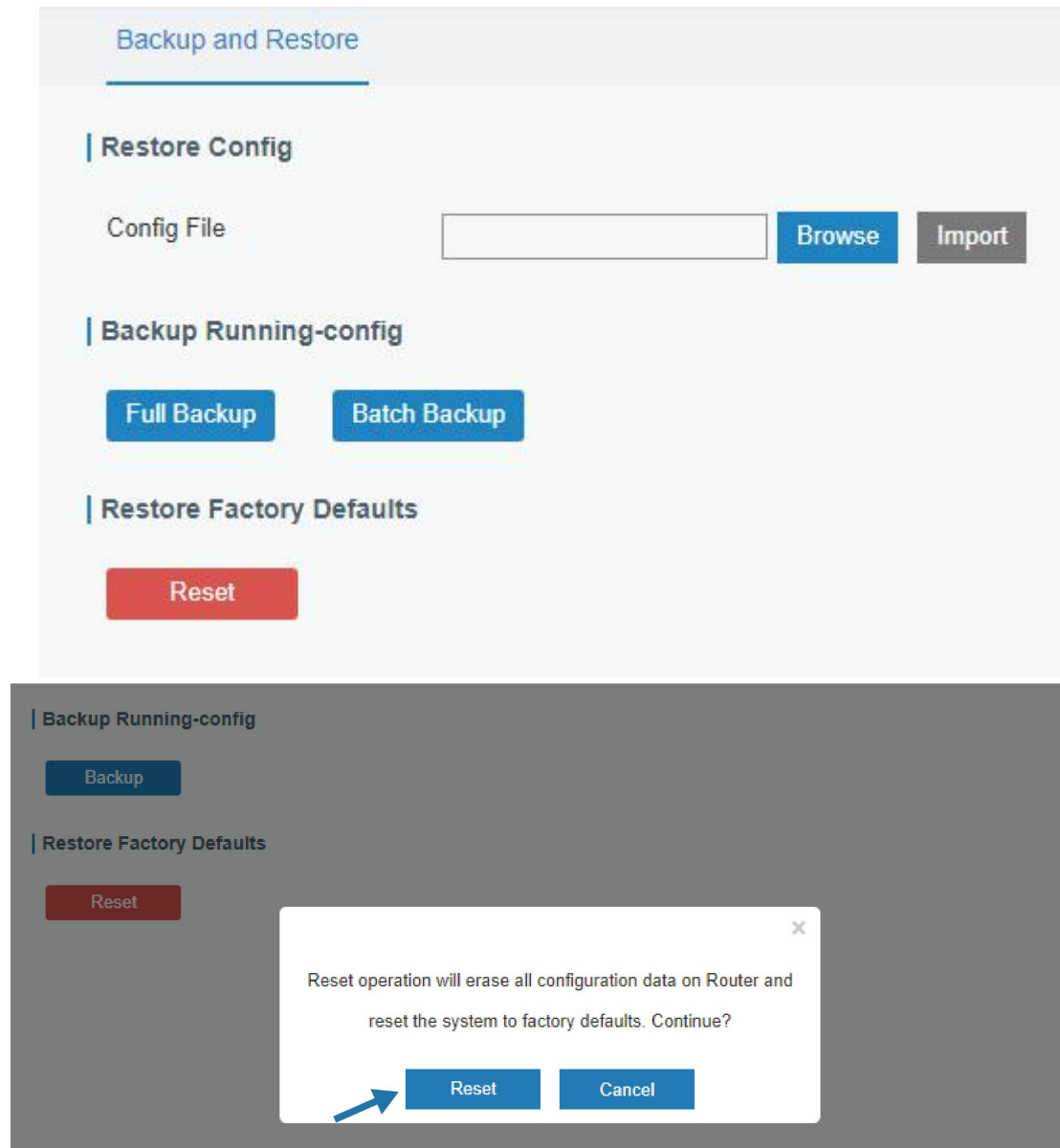
Chapter 4 Application Examples

4.1 Restore Factory Defaults

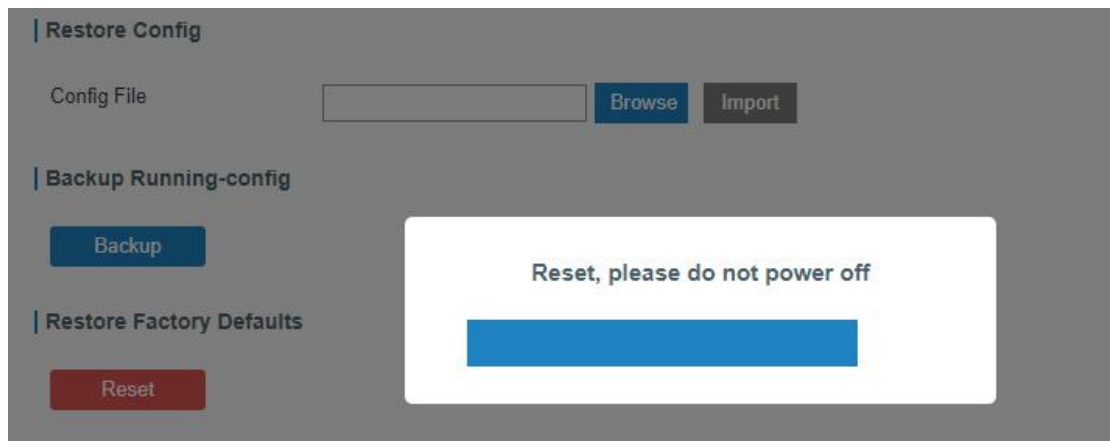
4.1.1 Via Web Interface

1. Log in web interface, and go to “Maintenance → Backup and Restore”.
2. Click “Reset” button under the “Restore Factory Defaults”.

You will be asked to confirm if you’d like to reset it to factory defaults. Then click “Reset” button.



Then the gateway will reboot and restore to factory settings immediately.



Please wait till SYS light staticly and the login page pops up again, which means the gateway has already been reset to factory defaults successfully.

Related Topic

[Restore Factory Defaults](#)

4.1.2 Via Hardware

Locate the reset button on the gateway, and take corresponding actions based on the status of SYS LED.

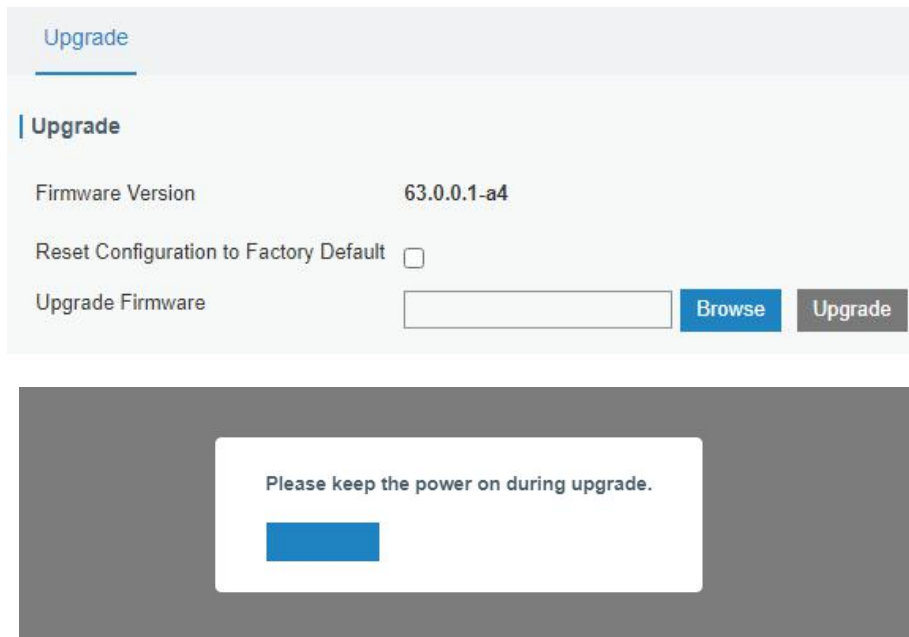
SYS LED	Action
Static Green	Press and hold the reset button for more than 5 seconds.
Static Green → Rapidly Blinking	Release the button and wait.
Off → Static Green	The gateway is now reset to factory defaults.

4.2 Firmware Upgrade

It is suggested that you contact Linovision technical support first before you upgrade gateway firmware. Gateway firmware file suffix is “.bin”.

After getting firmware file please refer to the following steps to complete the upgrade.

1. Go to “Maintenance > Upgrade”.
2. Click “Browse” and select the correct firmware file from the PC.
3. Click “Upgrade” and the gateway will check if the firmware file is correct. If it’s correct, the firmware will be imported to the gateway, and then the gateway will start to upgrade.

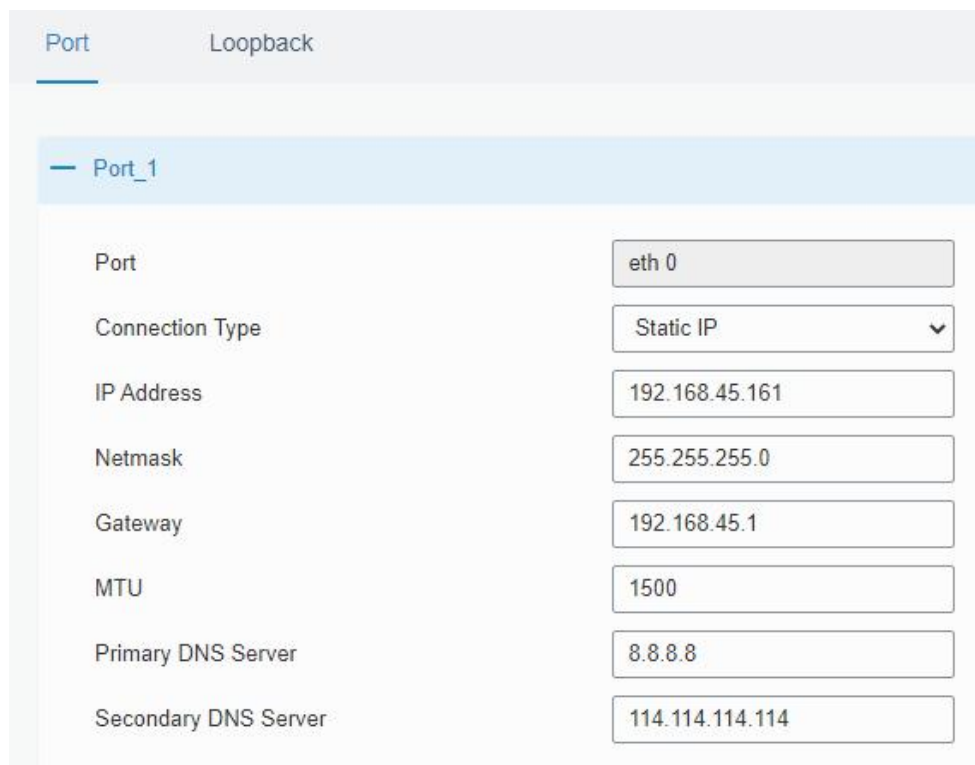


Related Topic

[Upgrade](#)

4.3 Ethernet Connection

1. Go to “Network → Interface → Port” page to select the connection type and configure Ethernet port configuration.
2. Click “Save & Apply” for configuration to take effect.



3. Connect Ethernet port of gateway to devices like router or modem.
4. Log in the web GUI via the newly assigned IP address and go to "Status -> Network" to check Ethernet port status.

Port	Status	Type	IP Address	Netmask	Gateway	DNS	Duration
eth 0	up	Static	192.168.45.161	255.255.255.0	192.168.45.1	8.8.8.8	5days,21h 19s




Related Topic


[Port Setting](#)

4.4 Packet Forwarder Configuration

UG63 gateway has installed multiple packet forwarders including Semtech, Basic station, Chirpstack-Generic MQTT broker, etc. Before connecting make sure the gateway has connected to network.

1. Go to "Packet Forwarder → General".

General	Radios	Advanced	Custom	Traffic	
General Setting					
Gateway EUI	24E124FFFEF12257				
Gateway ID	<input type="text" value="24E124FFFEF12257"/>				
Frequency-Sync	<input type="text" value="Disabled"/>				
Multi-Destination					
ID	Enable	Type	Server Address	Connect Status	Operation
0	Enabled	Embedded NS	localhost	Connected	 
					

2. Click  to add a new network server. Fill in the network server information and enable this server.

Enable	<input checked="" type="checkbox"/>
Type	<input type="text" value="Semtech"/>
Server Address	<input type="text" value="eu1.cloud.thethings.network"/>
Port Up	<input type="text" value="1700"/>
Port Down	<input type="text" value="1700"/>
<input type="button" value="Save"/>	

3. Go to “Packet Forwarder → Radio” page to configure antenna type, center frequency and channels. The channels of the gateway and network server need to be the same.

Region

Name	Center Frequency/MHz
Radio 0	<input type="text" value="904.3"/>
Radio 1	<input type="text" value="905.0"/>

Multi Channels Setting

Enable	Index	Radio	Frequency/MHz
<input checked="" type="checkbox"/>	0	<input type="text" value="Radio 0"/>	<input type="text" value="903.9"/>
<input checked="" type="checkbox"/>	1	<input type="text" value="Radio 0"/>	<input type="text" value="904.1"/>
<input checked="" type="checkbox"/>	2	<input type="text" value="Radio 0"/>	<input type="text" value="904.3"/>
<input checked="" type="checkbox"/>	3	<input type="text" value="Radio 0"/>	<input type="text" value="904.5"/>
<input checked="" type="checkbox"/>	4	<input type="text" value="Radio 1"/>	<input type="text" value="904.7"/>
<input checked="" type="checkbox"/>	5	<input type="text" value="Radio 1"/>	<input type="text" value="904.9"/>
<input checked="" type="checkbox"/>	6	<input type="text" value="Radio 1"/>	<input type="text" value="905.1"/>
<input checked="" type="checkbox"/>	7	<input type="text" value="Radio 1"/>	<input type="text" value="905.3"/>

4. Add the gateway on network server page. For more details about the network server connection please refer to [Linovision IoT Support portal](#).

5. Go to “Traffic” page to view the data communication of UG63.

General Radios Advanced Custom Traffic

Traffic Setting

Rfch	Direction	Time	Ticks	Frequency	Datarate	Coderate	RSSI	SNR
0	up	05:57:30	212136749 3	903.9	SF10BW125	4/5	-51	13.2
0	up	05:57:29	211944923 1	904.5	SF7BW125	4/5	-95	8.5
0	up	05:57:13	210431205 7	904.6	SF8BW500	4/5	-51	11.5
0	up	05:57:06	209699855 6	903.9	SF7BW125	4/5	-65	14.2

4.5 Connect to Linovision IoT Cloud

1. Go to “Packet Forwarder → General” page to enable the embedded network server.

The screenshot shows the configuration interface for a Packet Forwarder. The left sidebar contains navigation options: Status, Packet Forwarder (selected), Network Server, Network, System, Maintenance, and APP. The main content area has tabs for General, Radios, Advanced, Custom, and Traffic. Under the 'General Setting' tab, the following fields are visible:

- Gateway EUI: 24E124FFFEF12257
- Gateway ID: 24E124FFFEF12257
- Frequency-Sync: Disabled

Below these settings is a 'Multi-Destination' table:

ID	Enable	Type	Server Address	Connect Status	Operation
0	Enabled	Embedded NS	localhost	Connected	[Edit] [Delete] [Add]

2. Go to “Packet Forwarder → Radio” page to select the center frequency and channels. The channels of the gateway and nodes need to be the same.

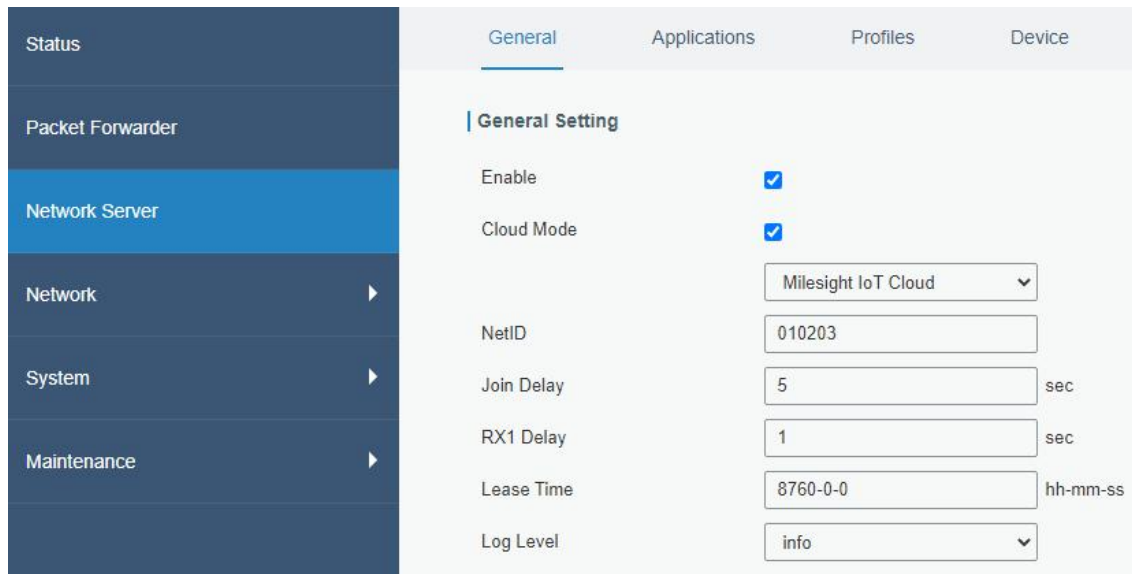
The screenshot shows the 'Radio' configuration page. At the top, the 'Region' is set to 'US915'. Below this, there are two rows for radio configuration:

Name	Center Frequency/MHz
Radio 0	904.3
Radio 1	905.0

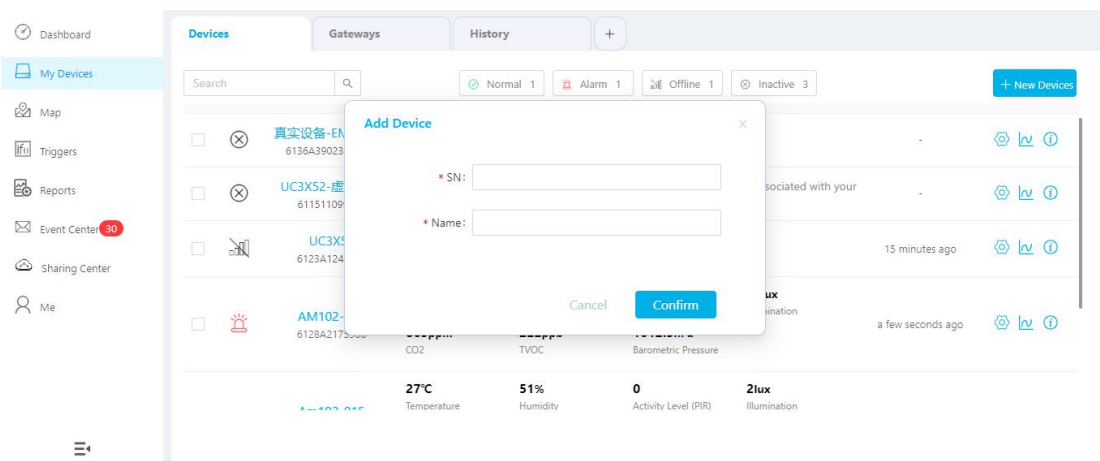
Below this is the 'Multi Channels Setting' table:

Enable	Index	Radio	Frequency/MHz
<input checked="" type="checkbox"/>	0	Radio 0	903.9
<input checked="" type="checkbox"/>	1	Radio 0	904.1
<input checked="" type="checkbox"/>	2	Radio 0	904.3
<input checked="" type="checkbox"/>	3	Radio 0	904.5
<input checked="" type="checkbox"/>	4	Radio 1	904.7
<input checked="" type="checkbox"/>	5	Radio 1	904.9
<input checked="" type="checkbox"/>	6	Radio 1	905.1
<input checked="" type="checkbox"/>	7	Radio 1	905.3

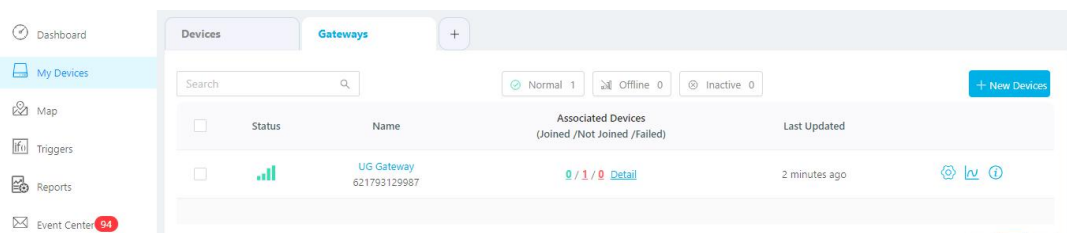
3. Go to “Network Server” → “General” page to enable the network server and “Cloud mode”, then select “Linovision IoT Cloud”.



4. Log in the Linovision IoT Cloud. Then go to “My Devices” page and click “+New Devices” to add gateway to Linovision IoT Cloud via SN. Gateway will be added under “Gateways” menu.




5. The gateway is online on Linovision IoT Cloud. For UG63, it's suggested to bind not more than 20 devices.

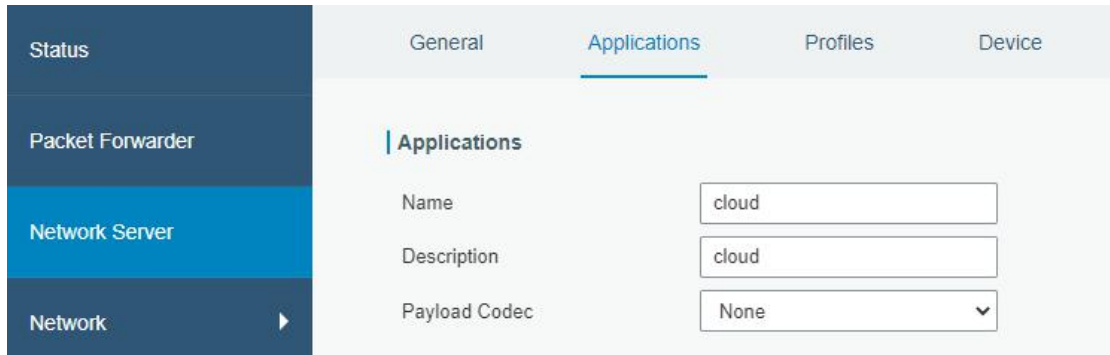


4.6 Application Configuration


You can create a new application on this page, which is mainly used to define the method of decoding the data sent from end-device and choosing the data transport protocol to send data to another server address. The data will be sent to your custom server address using MQTT, HTTP or HTTPS protocol.

1. Go to “Network Server → Application”.

2. Click  to enter the configuration page, displayed as the following picture:

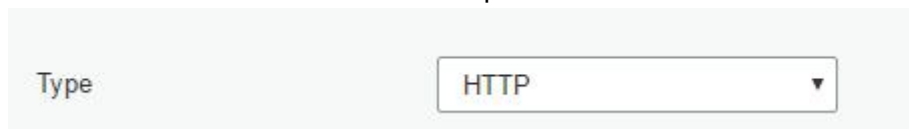


3. Click "Save" to create this application.

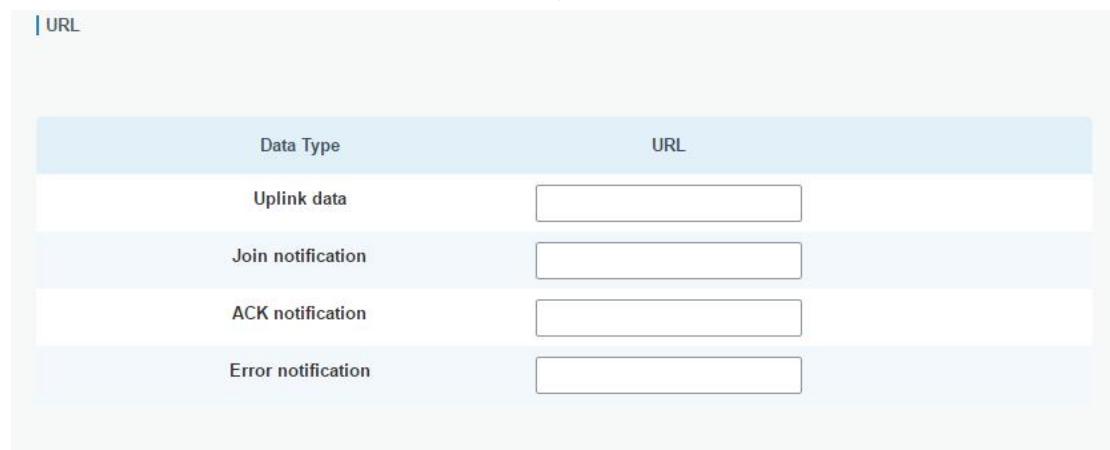
4. Click  to add a data transmission type.

HTTP or HTTPS:

Step 1: select HTTP or HTTPS as transmission protocol.

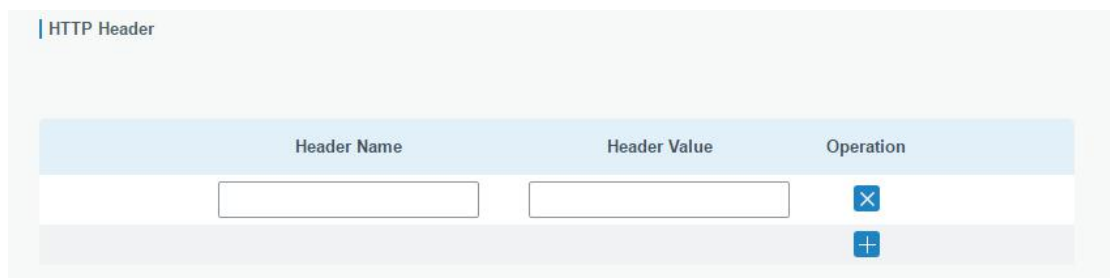



Step 2: Enter the destination URL. Different types of data can be sent to different URLs.



Data Type	URL
Uplink data	<input type="text"/>
Join notification	<input type="text"/>
ACK notification	<input type="text"/>
Error notification	<input type="text"/>

Enter the header name and header value if there is user credentials when accessing the HTTP(s) server.



Header Name	Header Value	Operation
<input type="text"/>	<input type="text"/>	

MQTT:

Step 1: select the transmission protocol as MQTT.

Type MQTT

Step 2: Fill in MQTT broker general settings.

General

Broker Address

Broker Port

Client ID

Connection Timeout/s

Keep Alive Interval/s

Step 3: Select the authentication method required by the server.

If you select user credentials for authentication, you need to enter the username and password for authentication.

User Credentials

Enable

Username

Password

If certificate is necessary for verification, please select mode and import CA certificate, client certificate and client key file for authentication.

TLS

Enable

Mode Self signed certificates

CA File Browse Import Delete

Client Certificate File Browse Import Delete

Client Key File Browse Import Delete

Step 4: Enter the topic to receive data and choose the QoS.

Data Type	topic	QoS
Uplink data	<input type="text" value="devices/UR67/messages/event"/>	QoS 0
Downlink data	<input type="text"/>	QoS 0
Multicast downlink data	<input type="text"/>	QoS 0
Join notification	<input type="text"/>	QoS 0
ACK notification	<input type="text"/>	QoS 0
Error notification	<input type="text"/>	QoS 0

4.7 Device Configuration

Go to “Device” page and click “Add” to add LoRaWAN® node devices. **Due to memory limitation, it’s suggested to add not more than 20 devices.** Please select correct device profile according to device type.



Device Name:

Description:

Device EUI:

Device-Profile:

Application:

Frame-counter Validation:

Application Key:

Device Address:

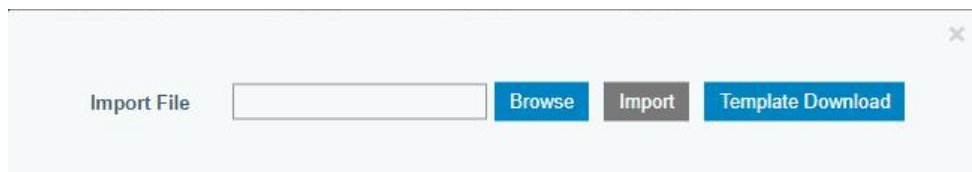
Network Session Key:

Application Session Key:

Uplink Frame-counter:

Downlink Frame-counter:

You can also click “Bulk Import” if you want to add many nodes all at once.



Click “Template Download” to download template file and add device information to this file. Application and device profile should be the same as you created on web page.

	A	B	C	D	E	F	G	H	I
1	name	description	deveui	application	deviceprofile	appkey	devaddr	appskey	nwkskey
2	24e1242191323266		24e1242191323266	cloud	ClassC-OTAA	112233445566778899aa112233445566			
3									
4									
5									

Import this file to add bulks of devices.

4.8 Send Data to Device

1. Go to “Network Server → Packets”, check the packet in the network server list to make sure that the device has joined the network successful.

1122612191	868100000	SF7BW125	-	-	17	0	JnAcc	2019-08-06T09:22:29+08:00	
112261219	868100000	SF7BW125	9.5	-77	18	0	JnReq	2019-08-06T09:22:29+08:00	

2. Fill in the device EUI or select the multicast group which you need to send downlinks. Then fill in the downlink commands, ports.

Send Data To Device

Device EUI	Type	Payload	Fport	Confirmed
<input type="text" value="11226121913"/>	ASCII	<input type="text" value="15"/>	<input type="text" value="15"/>	<input checked="" type="checkbox"/>

3. Click “Send”.



4. Check the packet in the network server list to make sure that the device has received this message successful. It's suggested to enable “Confirmed”. Multicast feature does not support confirmed downlinks.

Send Data To Device

Device EUI	Type	Payload	Fport	Confirmed
<input type="text" value="11226121913"/>	ASCII	<input type="text" value="15"/>	<input type="text" value="15"/>	<input checked="" type="checkbox"/>

You can click “Refresh” to refresh the list or set automatic refreshing frequency for the list. **If the device's class type is Class C, then the device will constantly receive packets.**

This packet's type is DnCnf (Downlink Confirmed Packet) and if the packet's color is gray, then it means the packet cannot be transmitted now because at least one message has been in the queue. If the packet record is white, it means the packet has been delivered successfully.

1122612191311123	869525000	SF12BW125	-	-	6	2	DnCnf	2019-08-06T09:22:55+08:00	Success
1122612191311123	0				6	2	DnCnf		Pending

If the device receives this downlink confirmed packet, then the device will reply “ACK” when delivering next.

Device EUI	Frequency	Datarate	SNR	RSSI	Size	Fcnt	Type	Time	Details
11226121913	868300000	SF10BW125	-	-	0	3	DnUnc	2019-08-06T09:23:44+08:00	
1122612191	868300000	SF10BW125	10.5	-75	64	2	UpCnf	2019-08-06T09:23:44+08:00	
112261219	869525000	SF12BW125	-	-	6	2	DnCnf	2019-08-06T09:22:55+08:00	
112261219	0				6	2	DnCnf		
112261219	868500000	SF10BW125	-	-	0	1	DnUnc	2019-08-06T09:22:49+08:00	

Packets Details	
Dev Addr	07e7
GwEUI	24e124ff
AppEUI	557240
DevEUI	1122612191311123
Immediately	-
Timestamp	874346044
Type	UpCnf
Adr	false
AdrAckReq	false
Ack	true
Fcnt	21
Fport	55
Modulation	LORA

Ack is "true" means that the device has received this packet.

If the device's class type is Class A, only after the device sends out an uplink packet will the network server sends out data to the device.

Device EUI	Frequency	Datarate	SNR	RSSI	Size	Fcnt	Type	Time	Details
1122612191311123	868300000	SF10BW125	-	-	0	19	DnUnc	2019-08-06T09:49:38+08:00	!
1122612191311123	868300000	SF10BW125	10.8	-76	64	21	ACK	2019-08-06T09:49:38+08:00	!
1122612191311123	868300000	SF10BW125	10.8	-76	64	21	UpCnf	2019-08-06T09:49:38+08:00	!
1122612191311123	868100000	SF10BW125	-	-	6	18	DnCnf	2019-08-06T09:48:43+08:00	Success
1122612191311123	868100000	SF10BW125	9.8	-77	64	20	UpCnf	2019-08-06T09:48:43+08:00	!
1122612191311123	0				6	18	DnCnf		Pending
1122612191311123	868500000	SF10BW125	-	-	0	17	DnUnc	2019-08-06T09:47:38+08:00	!
1122612191311123	868500000	SF10BW125	8.0	-76	64	19	UpCnf	2019-08-06T09:47:38+08:00	!
1122612191311123	868100000	SF10BW125	-	-	0	16	DnUnc	2019-08-06T09:46:38+08:00	!
1122612191311123	868100000	SF10BW125	11.2	-74	64	18	UpCnf	2019-08-06T09:46:37+08:00	!

Device EUI	Frequency	Datarate	SNR	RSSI	Size	Fcnt	Type	Time	Details
1122612191311123	868300000	SF10BW125	-	-	0	19	DnUnc	2019-08-06T09:49:38+08:00	!
1122612191311123	868300000	SF10BW125	10.8	-76	64	21	ACK	2019-08-06T09:49:38+08:00	!
1122612191311123	868300000	SF10BW125	10.8	-76	64	21	UpCnf	2019-08-06T09:49:38+08:00	!
1122612191311123	868100000	SF10BW125	-	-	6	18	DnCnf	2019-08-06T09:48:43+08:00	!
1122612191311123	868100000	SF10BW125	9.8	-77	64	20	UpCnf	2019-08-06T09:48:43+08:00	!
1122612191311123	0				6	18	DnCnf		!
1122612191311123	868500000	SF10BW125	-	-	0	17	DnUnc	2019-08-06T09:47:38+08:00	!
1122612191311123	868500000	SF10BW125	8.0	-76	64	19	UpCnf	2019-08-06T09:47:38+08:00	!
1122612191311123	868100000	SF10BW125	-	-	0	16	DnUnc	2019-08-06T09:46:38+08:00	!
1122612191311123	868100000	SF10BW125	11.2	-74	64	18	UpCnf	2019-08-06T09:46:37+08:00	!

means the device has received the packet you send

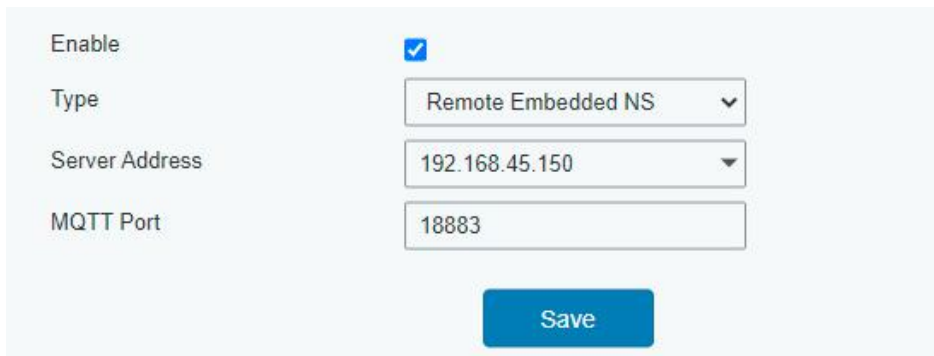
Related Topic

[Packets](#)

4.9 Connect to UG65/UG67 Gateway

Linovision UG6x LoRaWAN® gateway can set up multi-gateway architecture, which can make different gateway failover each other and extend signal coverage, while make one node device roams in multiple gateways. One UG65/UG67 gateway can be used as network server and other UG6x series gateways can be used as packet forwarder and transmit all data to the main gateway.

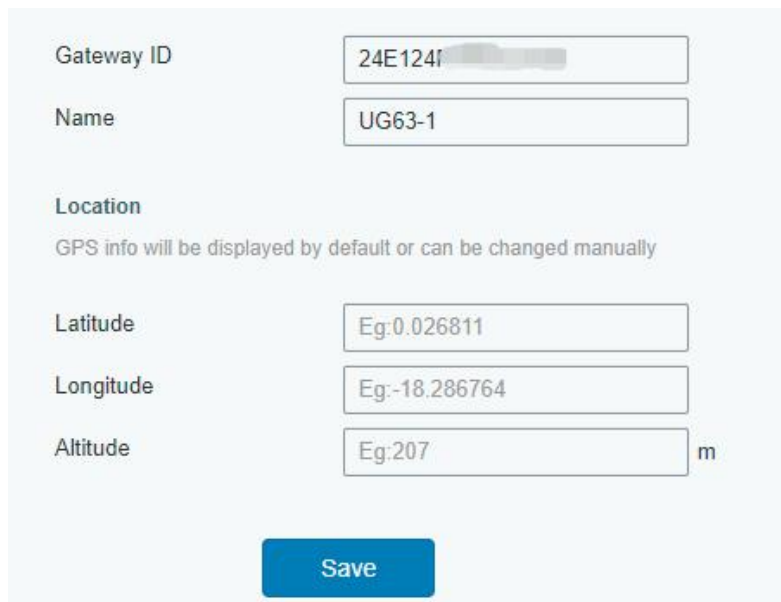
1. Go to “Packet Forwarder” → “General” page to enable the “Remote Embedded NS” and fill in the main gateway IP address which can reach.



Enable	<input checked="" type="checkbox"/>
Type	Remote Embedded NS
Server Address	192.168.45.150
MQTT Port	18883

Save

2. Go to “Network Server” → “Gateway Fleet” page of UG65/UG67 to add the gateway ID of UG63 gateway and define a name, then save the settings.



Gateway ID	24E124f...
Name	UG63-1
Location GPS info will be displayed by default or can be changed manually	
Latitude	Eg:0.026811
Longitude	Eg:-18.286764
Altitude	Eg:207 m

Save

3. After connected, the UG63 can transfer node data to UG65/UG67 and you can check the data details on “Network Server” → “Packets” page of UG65/UG67.

Status	General	Applications	Profiles	Device	Multicast Groups	Gateway Fleet	Packets
	Packet Forwarder	Gateway Fleet					
	Network Server	Gateway ID	Name	Status	Last Seen	Operation	
	Network	24E124[REDACTED]	Local Gateway	Connected	2022-03-10 19:13:54	<input checked="" type="checkbox"/> <input type="checkbox"/>	
System	24E124[REDACTED]	UG63-1	Connected	2022-03-10 19:13:54	<input checked="" type="checkbox"/> <input type="checkbox"/>		
					<input type="checkbox"/>	<input type="checkbox"/>	

[END]