Milesight

Wi-Fi HaLow Gateway

HL31

User Guide

Safety Precautions

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

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

Declaration of Conformity

HL31 is in conformity with the essential requirements and other relevant provisions of the CE, FCC, and RoHS.

For assistance, please contact
Milesight technical support:
Email: iot.support@milesight.com
Support Portal: support.milesight-iot.com
Tel: 86-592-5085280
Fax: 86-592-5023065
Address: Building C09, Software Park III,
Xiamen 361024, China

Revision History

Date	Doc Version	Description
Feb. 22, 2024	V1.0	Initial version

Contents

Chapter 1 Product Introduction

1.1 Overview

HL31 is a lightweight indoor Wi-Fi HaLow gateway. Adopting Wi-Fi HaLow technology and a high-performance quad-core CPU, HL31 supports setting up more than 200 node transmission at the same time with low power consumption. HL31 has a line of sight up to 1 km and supports data rates up to 32 Mbps, which is suitable for IoT sensors and picture camera applications. HL31 supports not only multiple back-haul backups with Ethernet and cellular, but also provides multiple VPN solutions to secure the data transmission to remote servers.

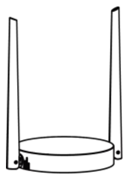
With compact size and various kinds of power supply options, it is an ideal supplement for wide indoor areas such as offices, parking lots, campuses, etc.

1.2 Key Features

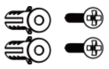
- Industrial-grade quad-core CPU with ARM Cortex-A35 processor, providing high performance for data transmission
- Support up to 200 end-node connections
- Small in size for easy carrying & Deployment
- Desktop, wall, or ceiling mounting support
- Equipped with Wi-Fi for web GUI configuration
- Multi-backhaul backups with Ethernet and Cellular (4G)
- Secure transmission with VPN tunnels like IPsec/OpenVPN /GRE/L2TP/PPTP/DMVPN
- Function well with standard Wi-Fi HaLow sensors

Chapter 2 Hardware Introduction

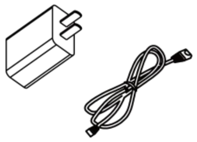
2.1 Packing List



1 × HL31 Device



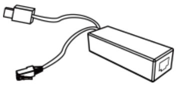
2 × Wall Mounting Kits



1 × Type-C Cable & Power Adapter

1 × Quick Guide

1 × Warranty Card

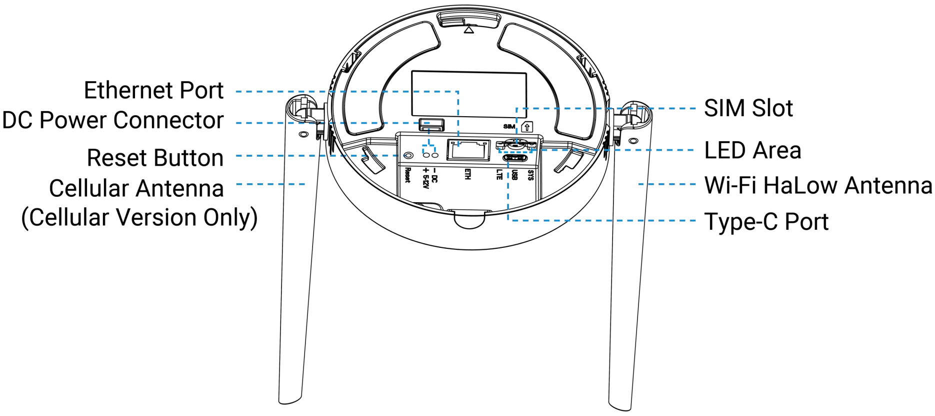


1 × PoE Splitter

(Optional)

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

2.2 Hardware Overview



2.3 LED Indicator and Reset Button

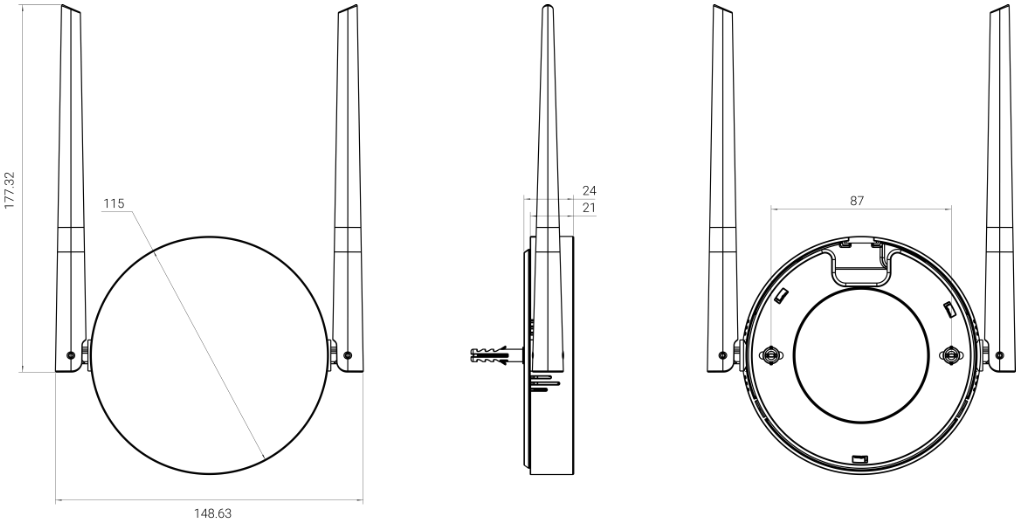
LED Indicators

LED	Indication	Status	Description
SYS	Power & System Status	Off	The power is off
		Green Light	The system is running properly
		Red Light	The system goes wrong
LTE	Cellular Status	Off	SIM card is registering or failed to register (or there are no SIM cards inserted)
		Green Light	Blinking slowly: SIM card has been registered and is ready for dial-up
			Blinking rapidly: SIM card has been registered and is dialing up now
			Static: SIM card has been registered and dialed up successfully
Ethernet Port	Link Indicator	Off	Disconnected or connect failure
		Yellow Blinking	Transmitting data
	Connection Indicator	Off	Ethernet port is disconnected
		Green Light	Ethernet port is connected

Reset Button

Function	Action	LED Indication
Reset to Factory Default	Press and hold the button for more than 5 seconds	SYS: blinks rapidly.

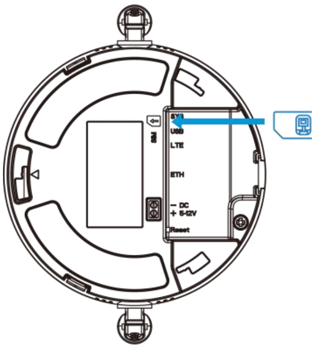
2.4 Dimensions (mm)



Chapter 3 Hardware Installation

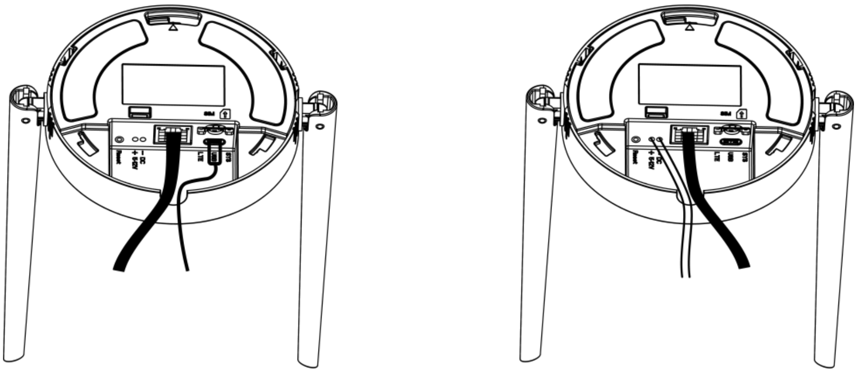
3.1 SIM Card Installation (Cellular Version Only)

Insert the micro (3FF) SIM card into the device according to arrows as follows. If you need to take out the SIM card, press the SIM card and it will pop up automatically.

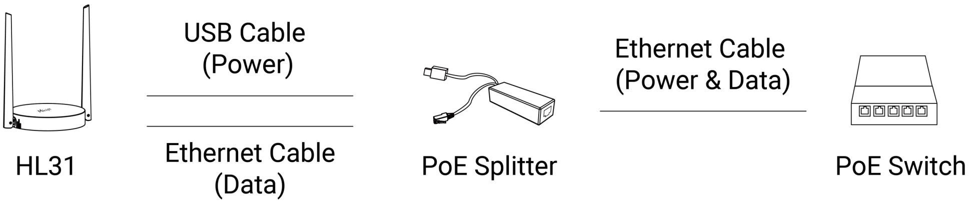


3.2 Power Supply

HL31 can be powered by USB (5V) or a DC power connector (5-12V) by default. When installing the power cables, pass them with Ethernet cables through the groove.



Additionally, it can also be powered by an 802.3af standard PoE source via a PoE splitter.



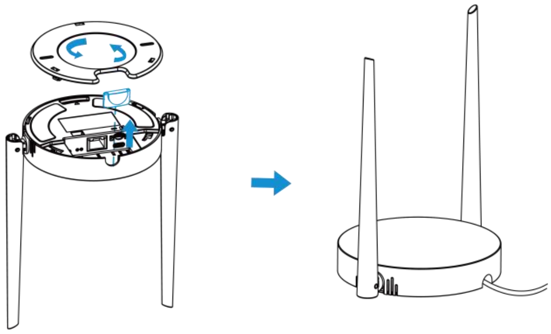
3.3 Gateway Installation

HL31 supports multiple installation methods like desktop, wall mounting, ceiling mounting, etc. Before you start, make sure that all cables have been installed and configurations are completed.

Note: Do not connect device to power supply or other devices when installing.

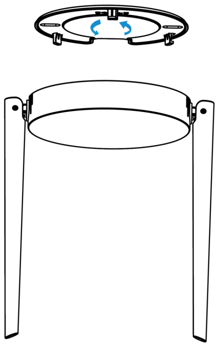
3.3.1 Desktop

Take off the baffle and mounting plate on the back of the device, then you can place the device on the desktop.

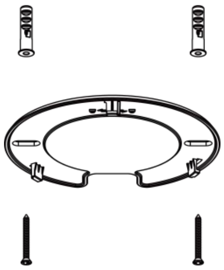


3.3.2 Wall/Ceiling Mounting

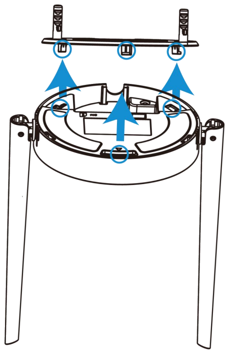
1. Take off the mounting plate on the back of the device.



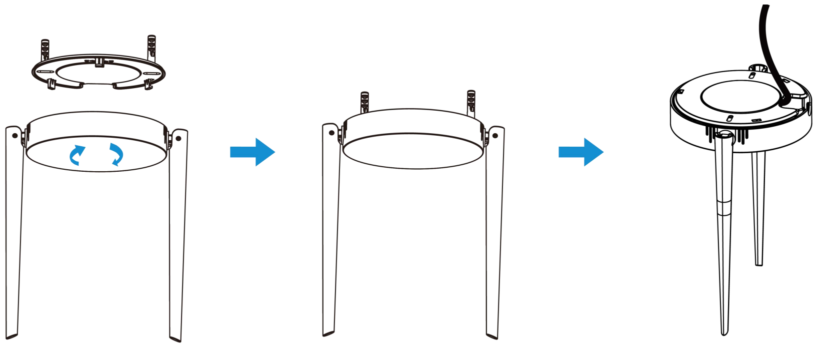
2. Align the mounting plate horizontally to the desired position on the wall or ceiling to mark two mounting holes, drill two holes as these marks, insert wall plugs into the holes respectively.



3. Fix the mounting plate to the wall plugs with screws.



4. Turn the device clockwise to lock it to the mounting plate.



Chapter 4 Access to Web GUI

This chapter explains how to access to Web GUI of the HL31.

Username: **admin**

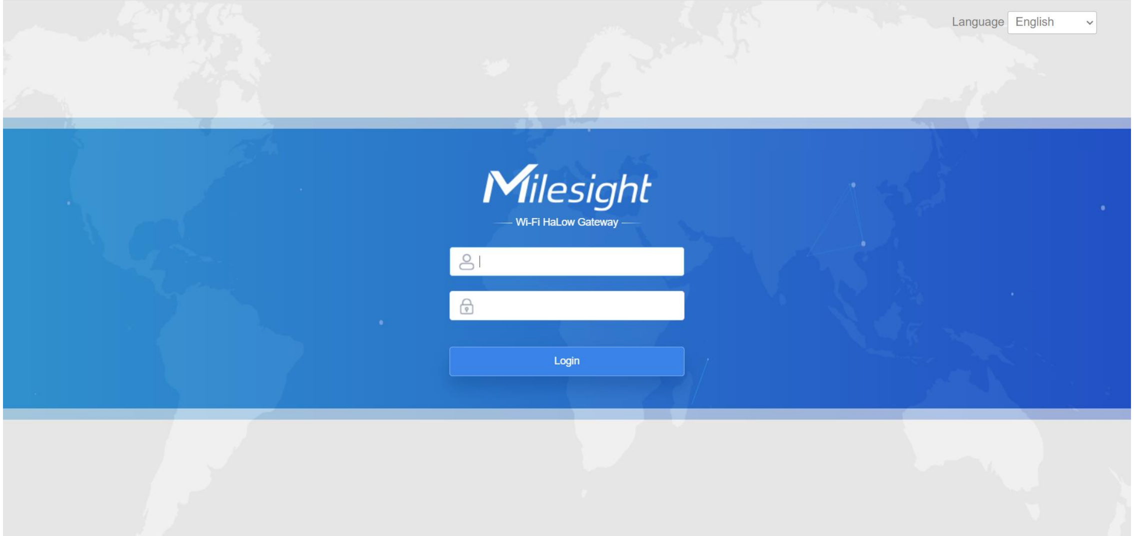
Password: **password**

4.1 Wireless Access

1. Enable Wireless Network Connection on your computer and search for access point **Gateway_XXXXXX_2.4G**, type default password **iotpassword** to connect it. (XXXXXX=last 6 digits of MAC address)

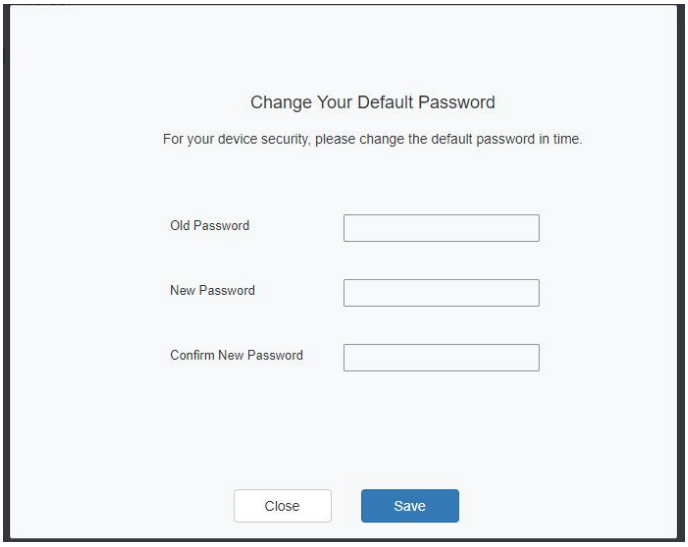
2. Open a Web browser on your PC (Chrome is recommended) and type in the IP address **192.168.1.1** to access the web GUI.

3. 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.

4. After logging the web GUI, follow the guide to complete the basic configurations. It's suggested that you change the password for the sake of security.



Change Your Default Password

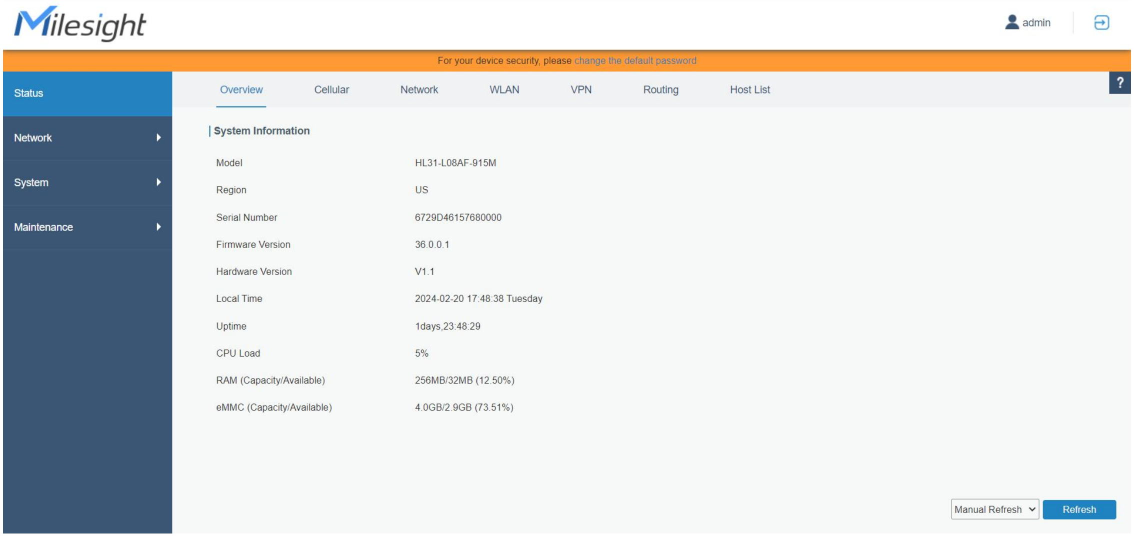
For your device security, please change the default password in time.

Old Password

New Password

Confirm New Password

5. You can view system information and perform configuration of the gateway.



For your device security, please change the default password

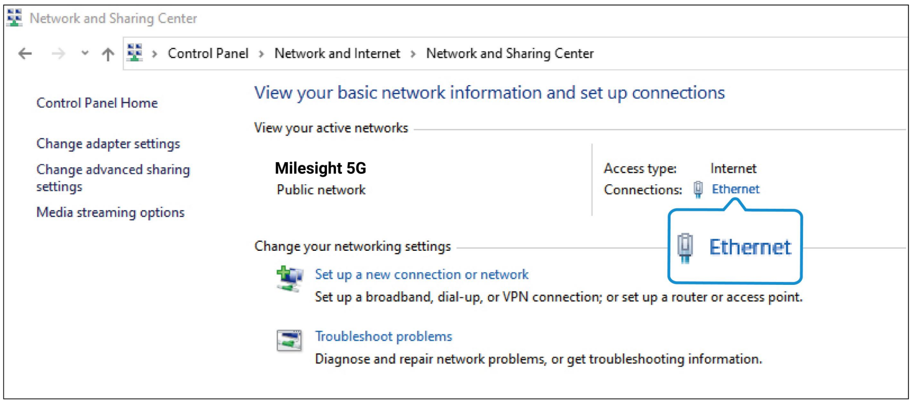
System Information

Model	HL31-L08AF-915M
Region	US
Serial Number	6729D46157680000
Firmware Version	36.0.0.1
Hardware Version	V1.1
Local Time	2024-02-20 17:48:38 Tuesday
Uptime	1days,23:48:29
CPU Load	5%
RAM (Capacity/Available)	256MB/32MB (12.50%)
eMMC (Capacity/Available)	4.0GB/2.9GB (73.51%)

4.2 Wired Access

Connect PC to HL31 ETH port directly 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).



Network and Sharing Center

Control Panel › Network and Internet › Network and Sharing Center
Control Panel Home
Change adapter settings
Change advanced sharing settings
Media streaming options

View your basic network information and set up connections

View your active networks

Milesight 5G
Public network

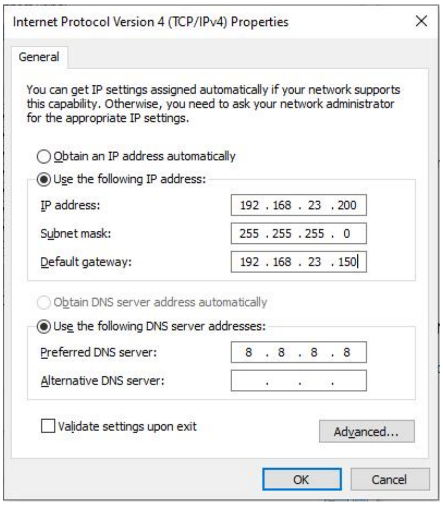
Access type: Internet
Connections: Ethernet

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

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.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 23 . 200

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 23 . 150

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

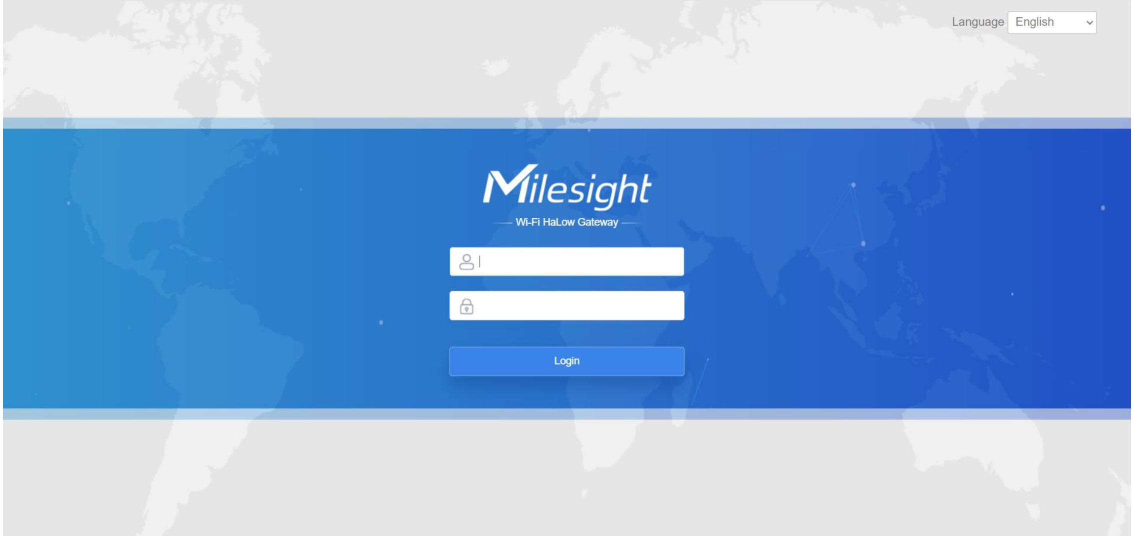
Preferred DNS server: 8 . 8 . 8 . 8

Alternative DNS server: . . .

□ Validate settings upon exit

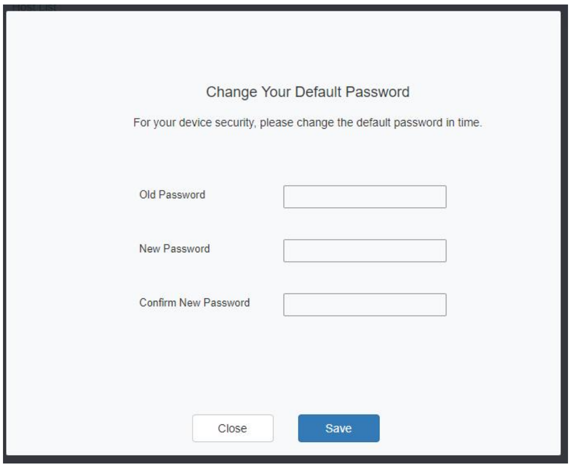
3. Open a Web browser on your PC (Chrome is recommended) and type in the IP address **192.168.23.150** to access the web GUI.

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 the web GUI, follow the guide to complete the basic configurations. It’s suggested that you change the password for the sake of security.



Change Your Default Password

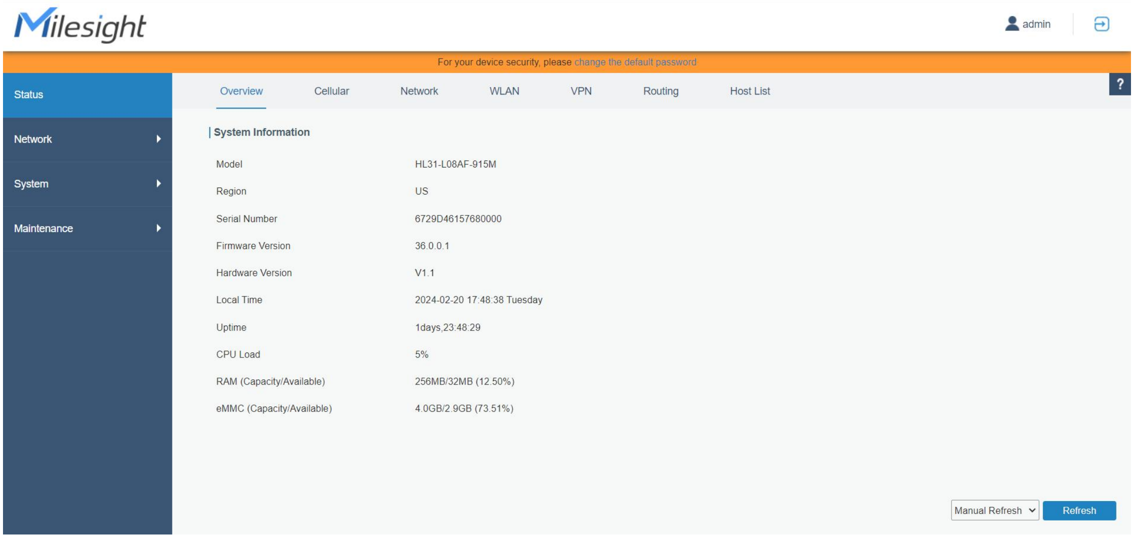
For your device security, please change the default password in time.

Old Password

New Password

Confirm New Password

6. You can view system information and perform configuration of the gateway.



For your device security, please change the default password

System Information

Model	HL31-L08AF-915M
Region	US
Serial Number	6729D46157680000
Firmware Version	36.0.0.1
Hardware Version	V1.1
Local Time	2024-02-20 17:48:38 Tuesday
Uptime	1days,23:48:29
CPU Load	5%
RAM (Capacity/Available)	256MB/32MB (12.50%)
eMMC (Capacity/Available)	4.0GB/2.9GB (73.51%)

Chapter 5 Application Examples

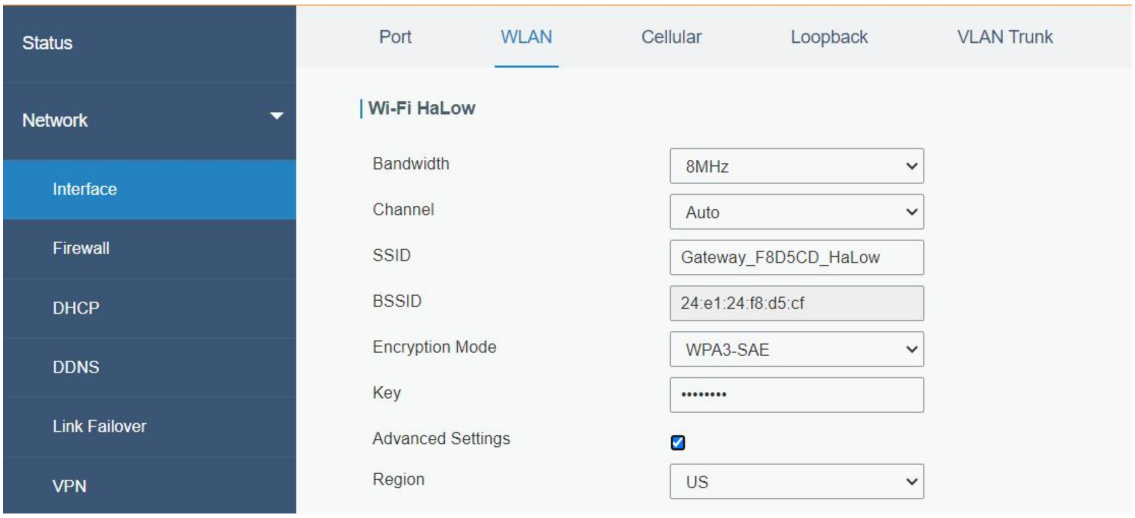
5.1 Wi-Fi HaLow Access Point

Application Example

Configure HL31 as Wi-Fi HaLow AP to allow connection from X1 Wi-Fi HaLow cameras.

Configuration Steps

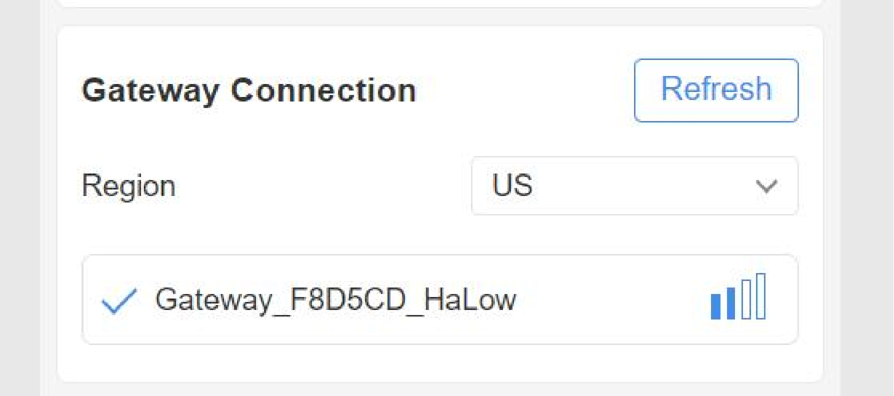
1. Go to **Network > Interface > WLAN** to configure wireless parameters and save the settings.



Wi-Fi HaLow

Bandwidth	8MHz
Channel	Auto
SSID	Gateway_F8D5CD_HaLow
BSSID	24:e1:24:f8:d5:cf
Encryption Mode	WPA3-SAE
Key	••••••••
Advanced Settings	☑
Region	US

2. Select the region parameter of X1 camera the same as the gateway, search and connect to the access point of HL31.

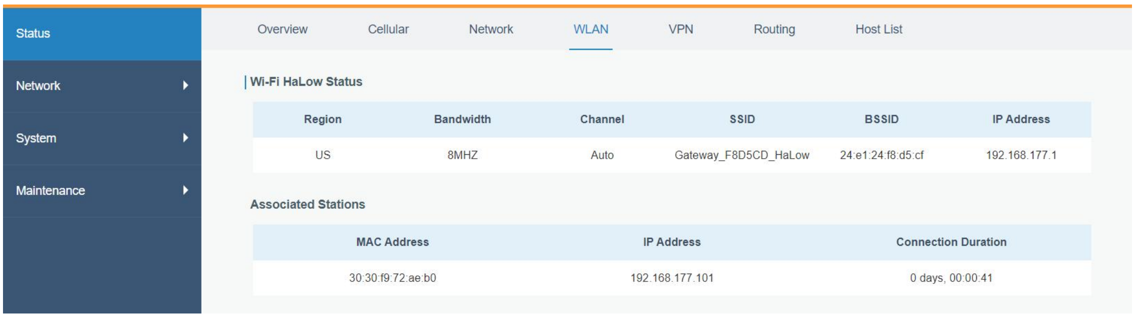


Gateway Connection

Region: US

✓ Gateway_F8D5CD_HaLow

3. Go to **Status > WLAN** of HL31 gateway, and you can check the AP settings and information of the connected client/user.



Wi-Fi HaLow Status

Region	Bandwidth	Channel	SSID	BSSID	IP Address
US	8MHZ	Auto	Gateway_F8D5CD_HaLow	24:e1:24:f8:d5:cf	192.168.177.1

Associated Stations

MAC Address	IP Address	Connection Duration
30:30:f9:72:ae:b0	192.168.177.101	0 days, 00:00:41

Related Topic

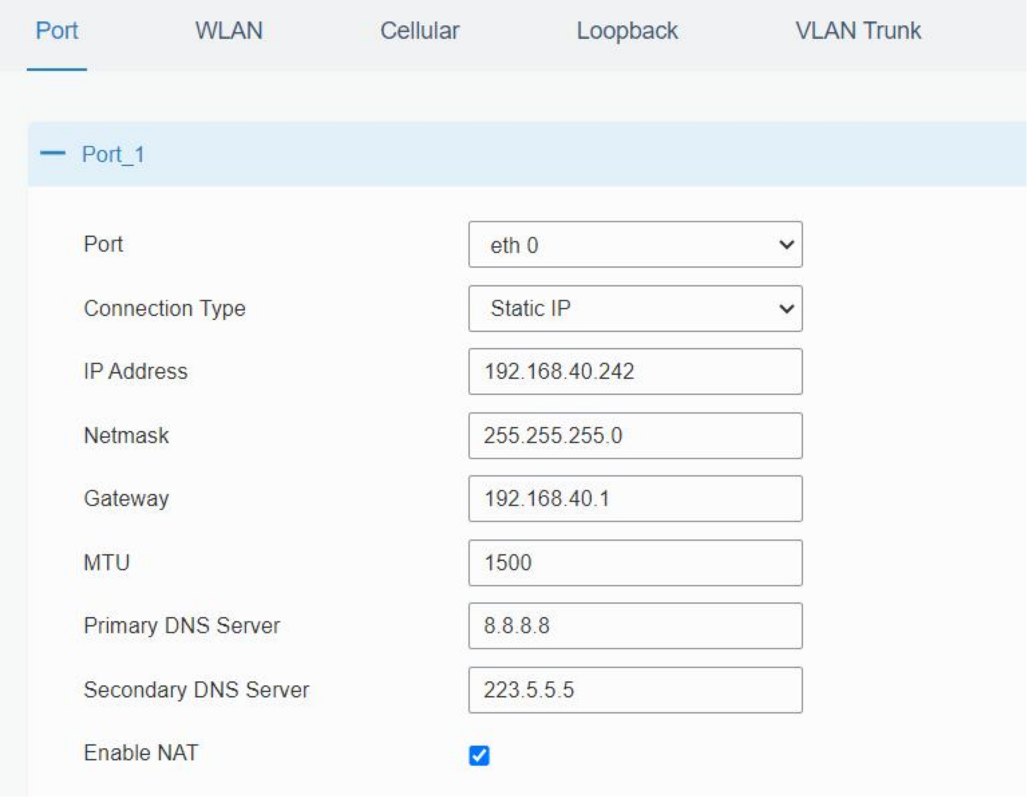
WLAN Setting

WLAN Status

5.2 Ethernet Connection

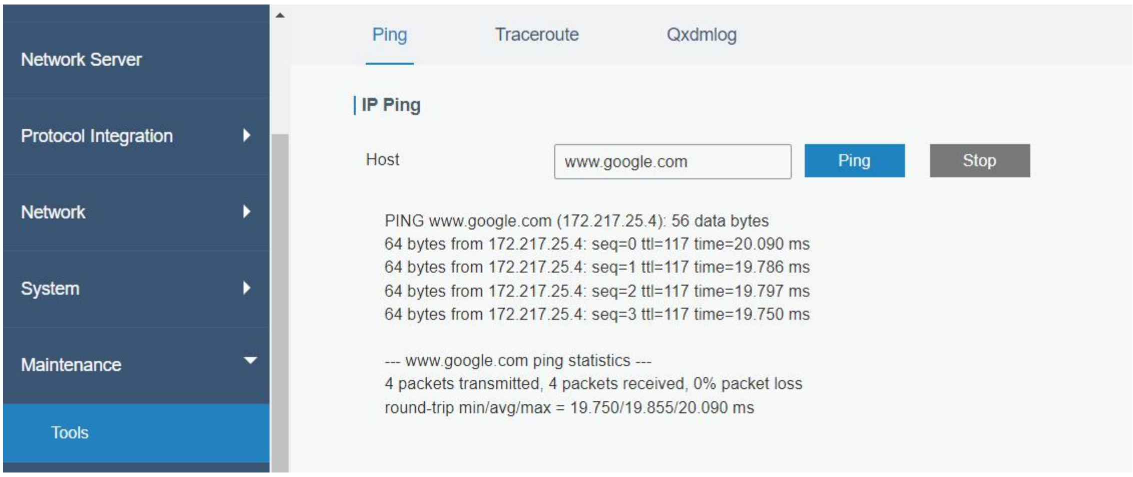
We are about to take an example of configuring the gateway to get access to the Internet through Ethernet port.

1. Go to **Network > Interface > Port** page to select the connection type and configure Ethernet port configuration, then save the settings.



Port	eth 0
Connection Type	Static IP
IP Address	192.168.40.242
Netmask	255.255.255.0
Gateway	192.168.40.1
MTU	1500
Primary DNS Server	8.8.8.8
Secondary DNS Server	223.5.5.5
Enable NAT	☑

2. Connect Ethernet port of gateway to network devices like router or modem.
3. Go to **Maintenance > Tools > Ping** page to check network connectivity.



Host: www.google.com

```
PING www.google.com (172.217.25.4): 56 data bytes
64 bytes from 172.217.25.4: seq=0 ttl=117 time=20.090 ms
64 bytes from 172.217.25.4: seq=1 ttl=117 time=19.786 ms
64 bytes from 172.217.25.4: seq=2 ttl=117 time=19.797 ms
64 bytes from 172.217.25.4: seq=3 ttl=117 time=19.750 ms

--- www.google.com ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 19.750/19.855/20.090 ms
```

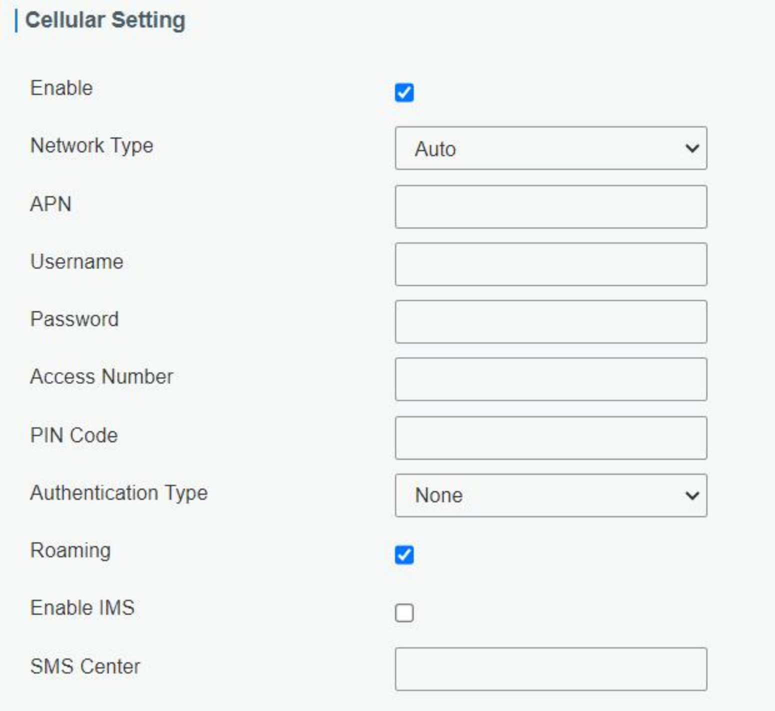
Related Topic

Port Setting

5.3 Cellular Connection (Cellular Version Only)

We are about to take an example of configuring the gateway to get access to the Internet through cellular.

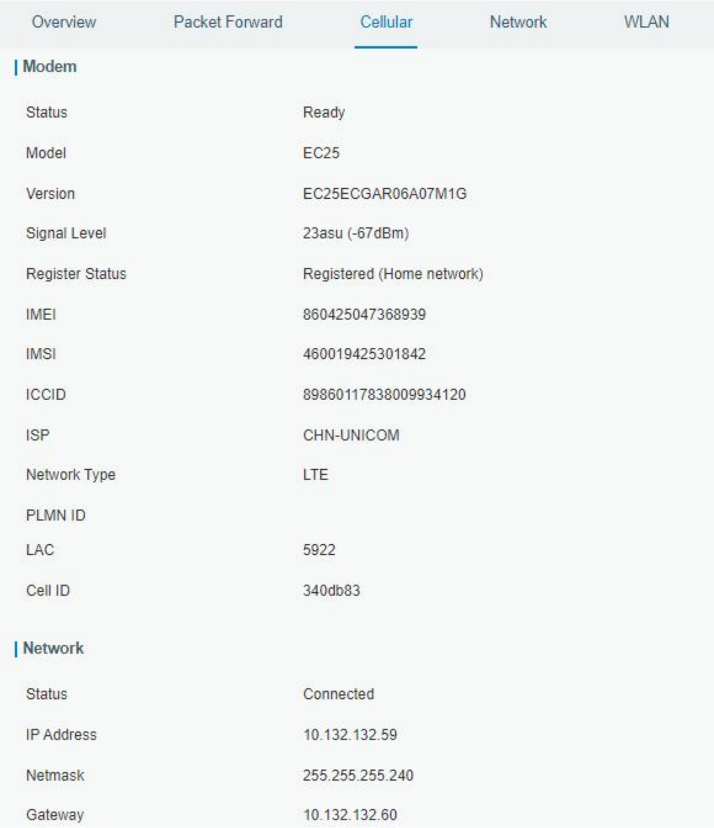
1. Go to **Network > Interface > Cellular > Cellular Setting** and configure the necessary info of SIM card, then save the settings.



Cellular Setting

Enable	☑
Network Type	Auto
APN	
Username	
Password	
Access Number	
PIN Code	
Authentication Type	None
Roaming	☑
Enable IMS	□
SMS Center	

2. Click **Status > Cellular** to view the status of the cellular connection. If it shows 'Connected', SIM has dialed up successfully.



Modem

Status	Ready
Model	EC25
Version	EC25ECGAR06A07M1G
Signal Level	23asu (-67dBm)
Register Status	Registered (Home network)
IMEI	860425047368939
IMSI	460019425301842
ICCID	89860117838009934120
ISP	CHN-UNICOM
Network Type	LTE
PLMN ID	
LAC	5922
Cell ID	340db83

Network

Status	Connected
IP Address	10.132.132.59
Netmask	255.255.255.240
Gateway	10.132.132.60

Related Topic

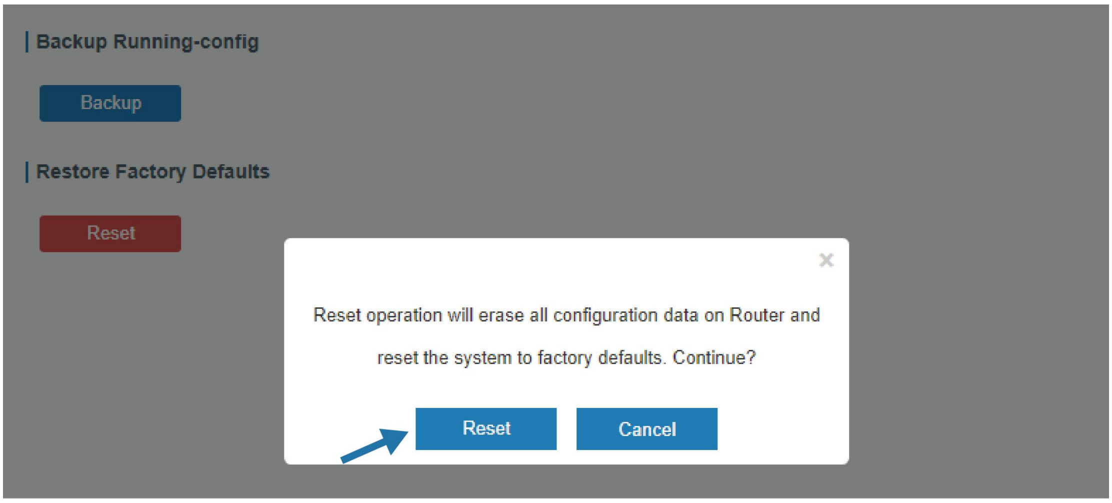
Cellular Setting

Cellular Status

5.4 Restore Factory Defaults

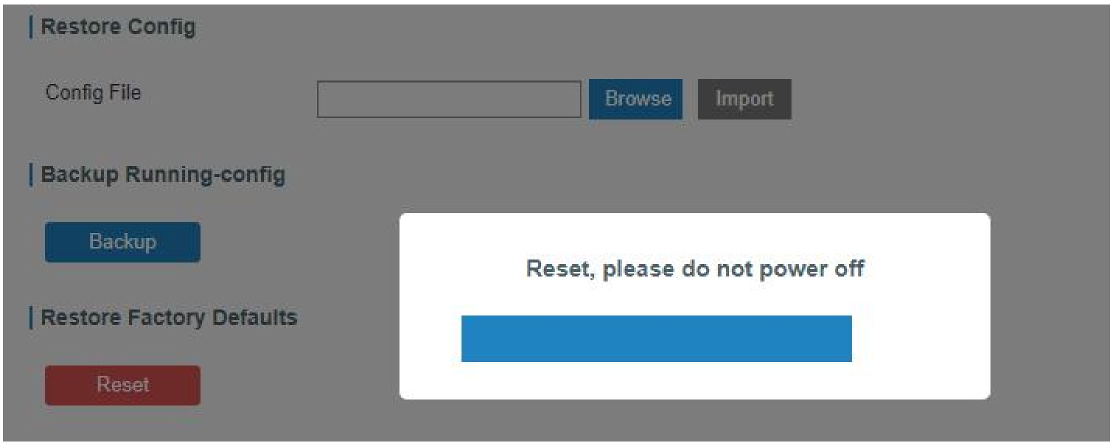
Method 1:

Log in web interface, and go to **Maintenance > Backup and Restore**, click **Reset** button, you will be asked to confirm if you'd like to reset it to factory defaults. Then click **Reset** button.



Reset operation will erase all configuration data on Router and reset the system to factory defaults. Continue?

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



Reset, please do not power off

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

Related Topic

Restore Factory Defaults

Method 2:

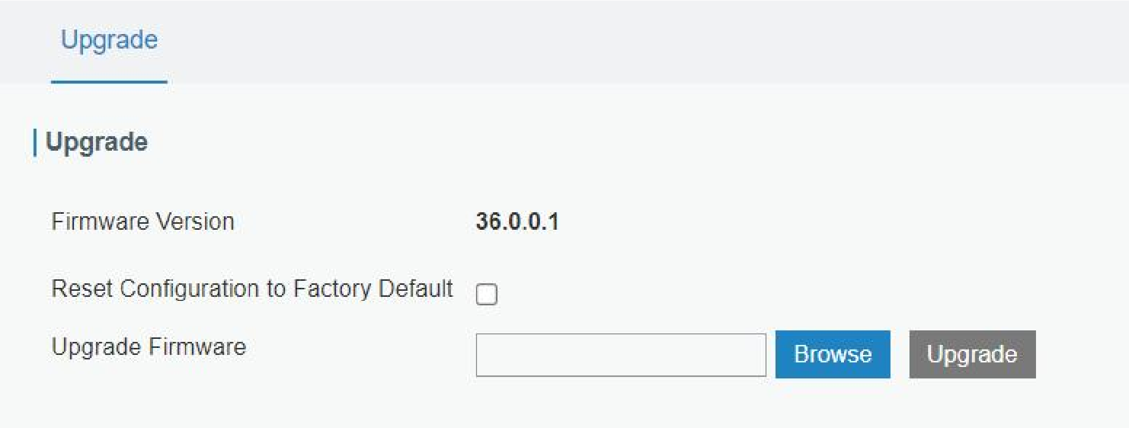
Locate the reset button on the gateway, press and hold the reset button for more than 5s until the SYS LED blinks.

5.5 Firmware Upgrade

It is suggested that you contact Milesight technical support first before you upgrade gateway firmware. The gateway firmware file suffix is ".bin".

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

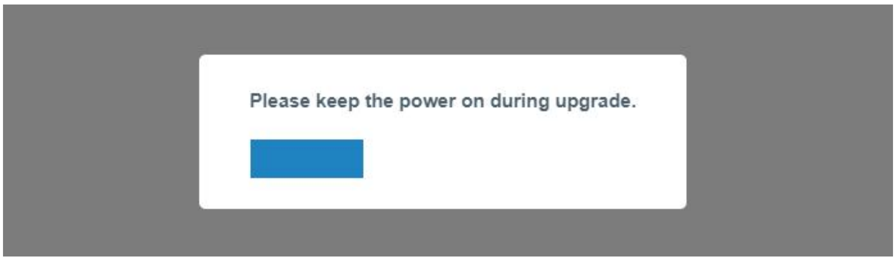
1. Go to **Maintenance > Upgrade** page, click **Browse** and select the correct firmware file from the PC.
2. Click **Upgrade** and the gateway will check if the firmware file is correct. If it's correct, the firmware will be imported to the gateway, and then the gateway will start to upgrade.



Firmware Version 36.0.0.1

Reset Configuration to Factory Default □

Upgrade Firmware



Please keep the power on during upgrade.

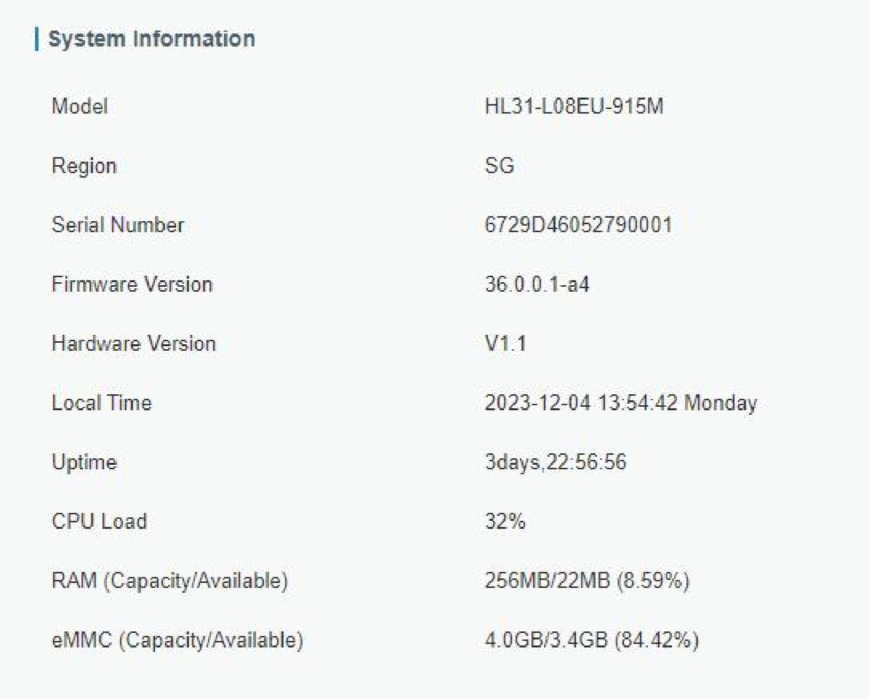
Related Topic

Upgrade

Chapter 6 Operation Guide

6.1 Status

6.1.1 Overview



System Information

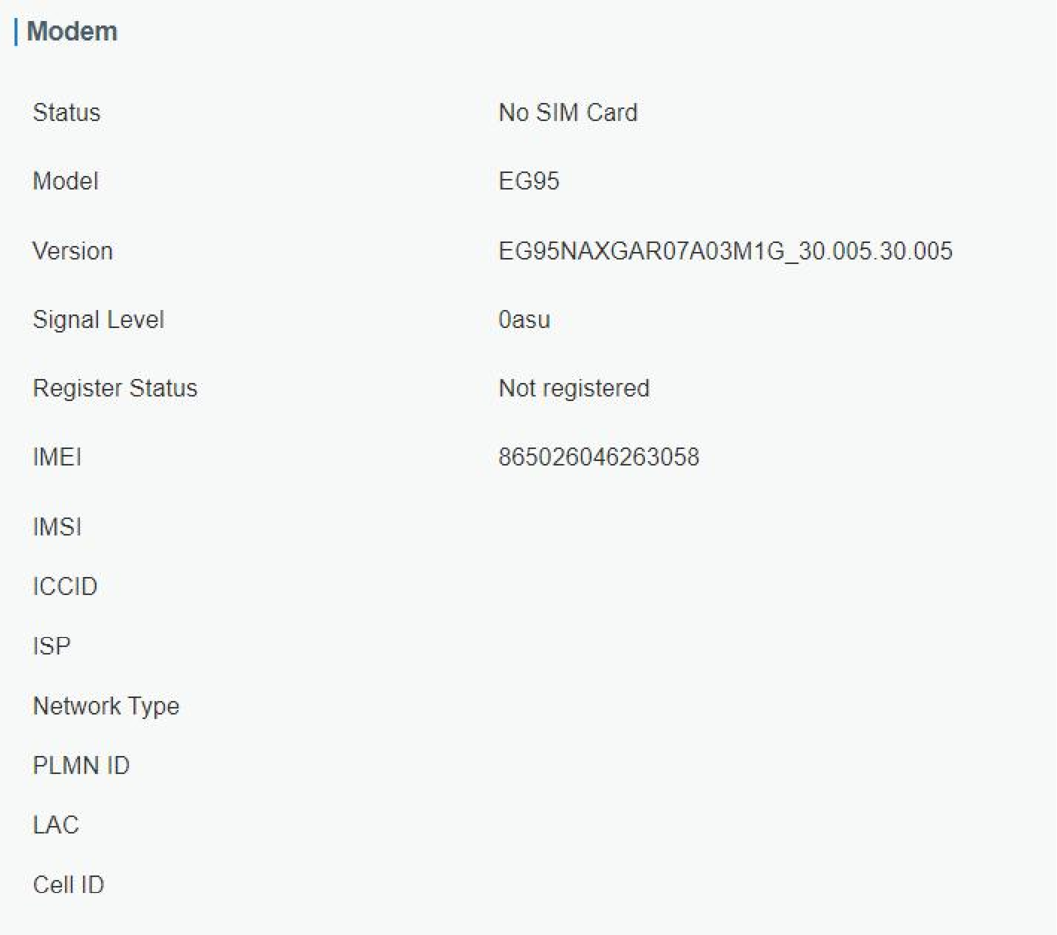
Model	HL31-L08EU-915M
Region	SG
Serial Number	6729D46052790001
Firmware Version	36.0.0.1-a4
Hardware Version	V1.1
Local Time	2023-12-04 13:54:42 Monday
Uptime	3days,22:56:56
CPU Load	32%
RAM (Capacity/Available)	256MB/22MB (8.59%)
eMMC (Capacity/Available)	4.0GB/3.4GB (84.42%)

System Information	
Item	**Description**
Model	Show the model name of gateway.
Region	Show the Wi-Fi HaLow 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.

6.1.2 Cellular (Cellular Version Only)

You can view the cellular network status of gateway on this page.

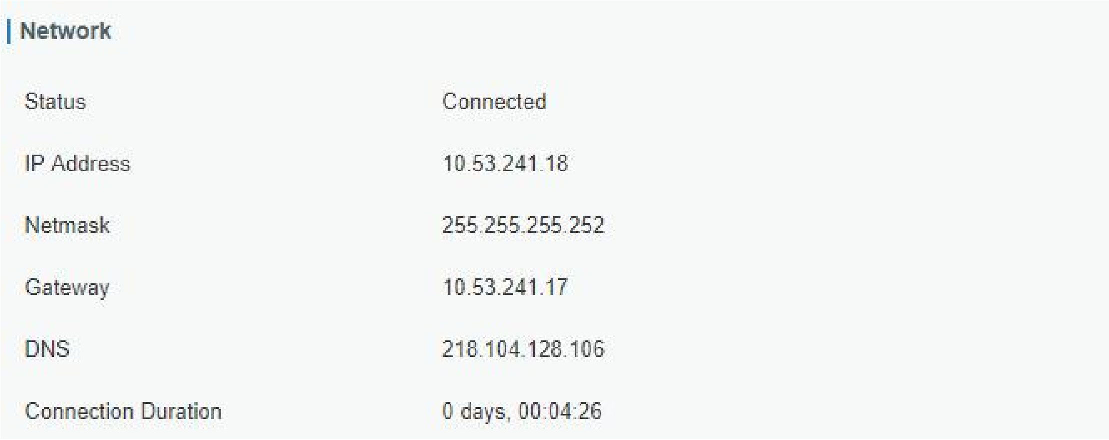


Modem

Status	No SIM Card
Model	EG95
Version	EG95NAXGAR07A03M1G_30.005.30.005
Signal Level	0asu
Register Status	Not registered
IMEI	865026046263058
IMSI	
ICCID	
ISP	
Network Type	
PLMN ID	
LAC	
Cell ID	

Modem Information	
Item	Description
Status	Show corresponding detection status of module and SIM card.
Model	Show the model name of cellular module.
Version	Show the version of cellular module.
Signal Level	Show the cellular signal level.
Register Status	Show the registration status of SIM card.
IMEI	Show the IMEI of the module.
IMSI	Show IMSI of the SIM card.
ICCID	Show ICCID of the SIM card.
ISP	Show the network provider which the SIM card registers on.
Network Type	Show the connected network type, such as LTE, 3G, etc.

PLMN ID	Show the current PLMN ID, including MCC, MNC, LAC and Cell ID.
LAC	Show the location area code of the SIM card.
Cell ID	Show the Cell ID of the SIM card location.



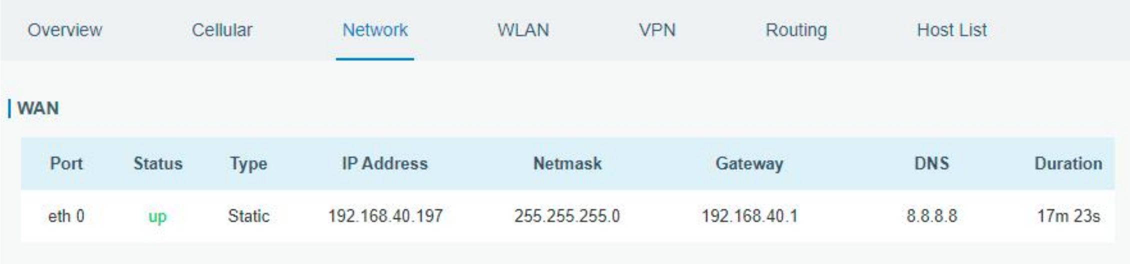
Network

Status	Connected
IP Address	10.53.241.18
Netmask	255.255.255.252
Gateway	10.53.241.17
DNS	218.104.128.106
Connection Duration	0 days, 00:04:26

Network Status	
Item	**Description**
Status	Show the connection status of cellular network.
IP Address	Show the IP address of cellular network.
Netmask	Show the netmask of cellular network.
Gateway	Show the gateway of cellular network.
DNS	Show the DNS of cellular network.
Connection Duration	Show information on how long the cellular network has been connected.

6.1.3 Network

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



WAN

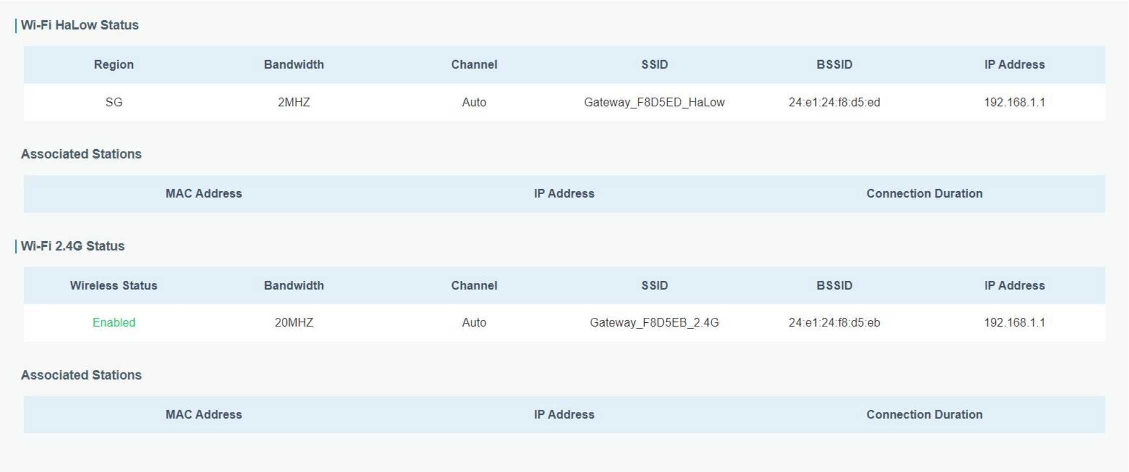
Port	Status	Type	IP Address	Netmask	Gateway	DNS	Duration
eth 0	up	Static	192.168.40.197	255.255.255.0	192.168.40.1	8.8.8.8	17m 23s

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.

6.1.4 WLAN

You can check the Wi-Fi status on this page, including the information of the access point and client.



Wi-Fi HaLow Status

Region	Bandwidth	Channel	SSID	BSSID	IP Address
SG	2MHZ	Auto	Gateway_F8D5ED_HaLow	24:e1:24:f8:d5:ed	192.168.1.1

Associated Stations

MAC Address	IP Address	Connection Duration

Wi-Fi 2.4G Status

Wireless Status	Bandwidth	Channel	SSID	BSSID	IP Address
Enabled	20MHZ	Auto	Gateway_F8D5EB_2.4G	24:e1:24:f8:d5:eb	192.168.1.1

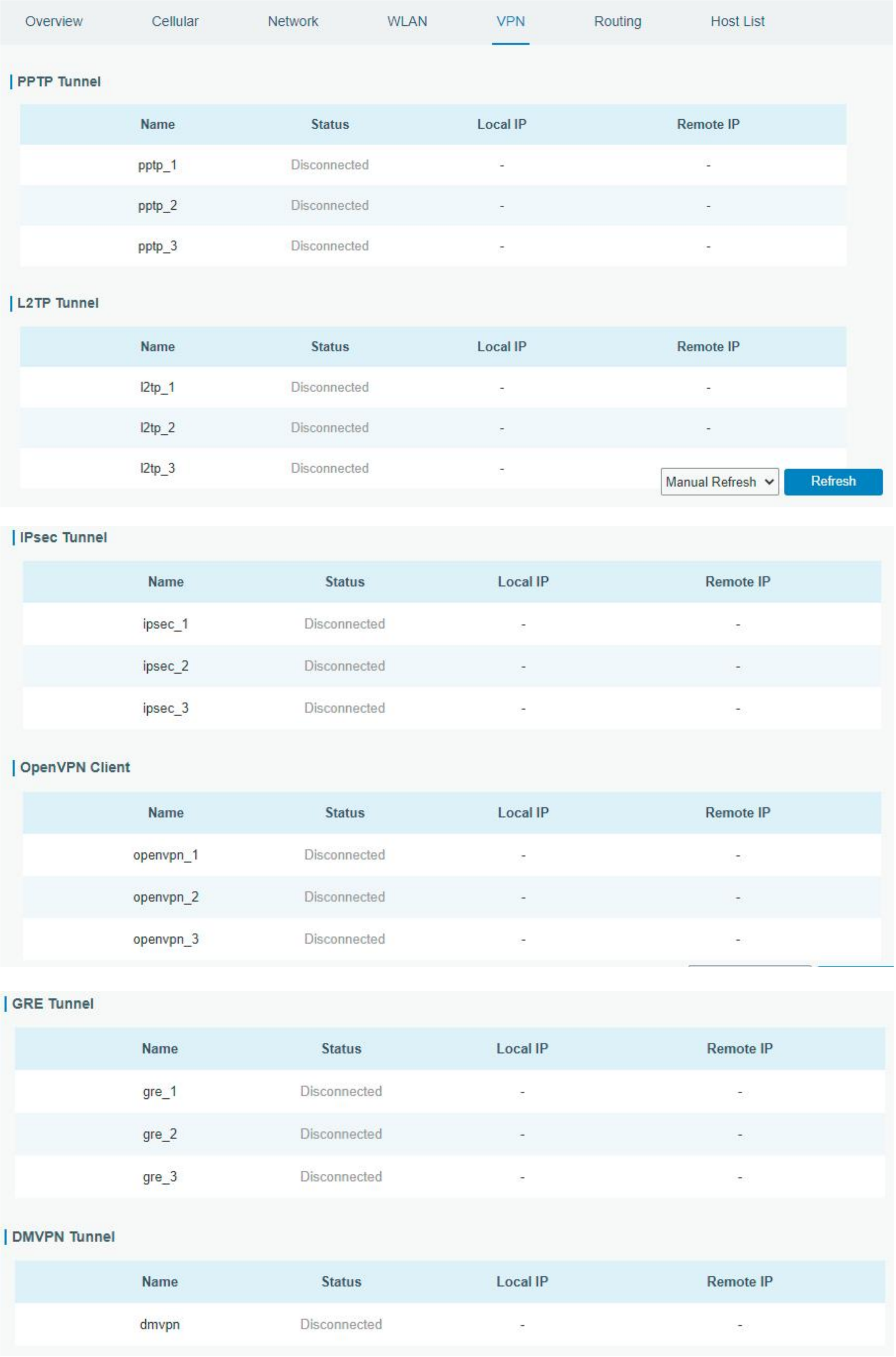
Associated Stations

MAC Address	IP Address	Connection Duration

WLAN Status	
Item	**Description**
Wi-Fi HaLow/Wi-Fi 2.4G Status	
Region	Show the using region of Wi-Fi HaLow.
Wireless Status	Show the 2.4G Wi-Fi status.
Bandwidth	Show the working bandwidth.
Channel	Show the wireless channel.
SSID	Show the SSID.
BSSID	Show the BSSID.
IP Address	Show the IP address of the gateway.
Status	Show the connection status.
Associated Stations	
MAC Address	Show the MAC address of the client.
IP Address	Show the IP address of client.
Connection Duration	Show information on how long the Wi-Fi network has been connected.

6.1.5 VPN

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



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	-	-

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

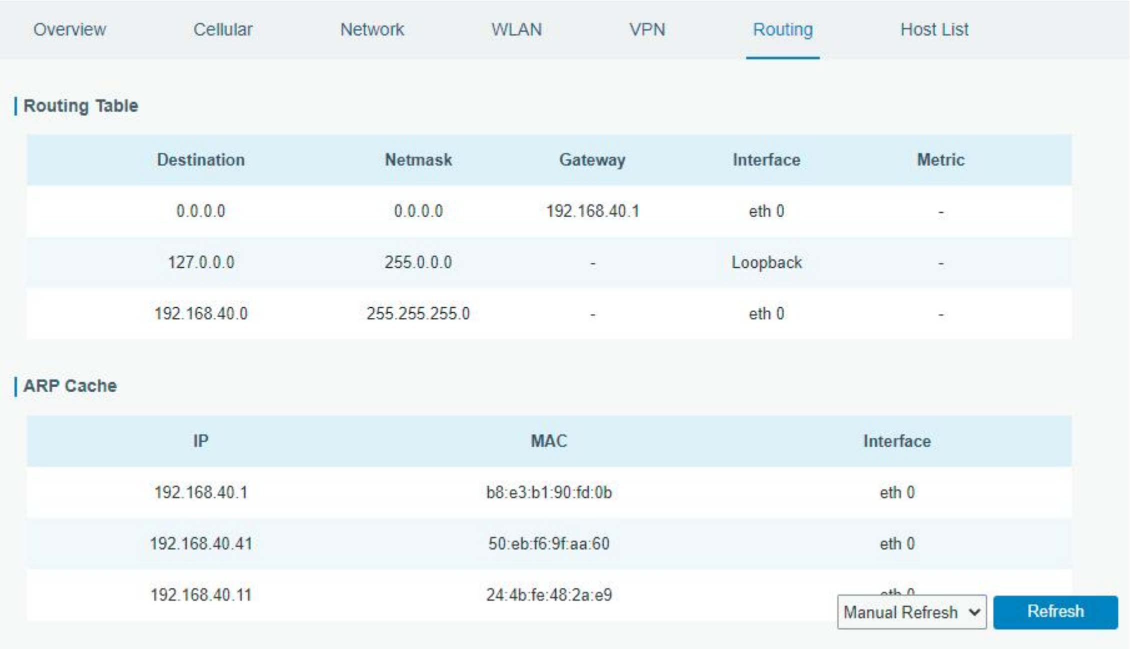
Name	Status	Local IP	Remote IP
dmvpn	Disconnected	-	-

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.

6.1.6 Routing

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



Routing Table

Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.40.1	eth 0	-
127.0.0.0	255.0.0.0	-	Loopback	-
192.168.40.0	255.255.255.0	-	eth 0	-

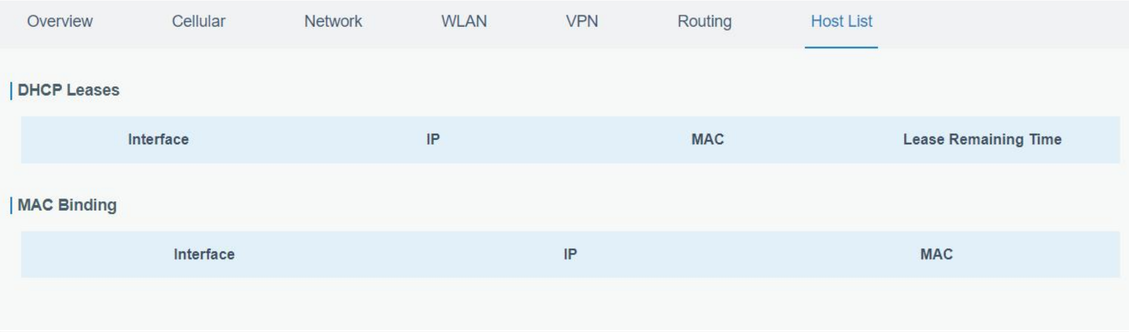
ARP Cache

IP	MAC	Interface
192.168.40.1	b8:e3:b1:90:fd:0b	eth 0
192.168.40.41	50:eb:f6:9f:aa:60	eth 0
192.168.40.11	24:4b:fe:48:2a:e9	eth 0

Item	Description
Routing Table	
Destination	Show the IP address of destination host or destination network.
Netmask/Prefix Length	Show the netmask or prefix length 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.

6.1.7 Host List

You can view the host information on this page.



DHCP Leases

Interface	IP	MAC	Lease Remaining Time

MAC Binding

Interface	IP	MAC

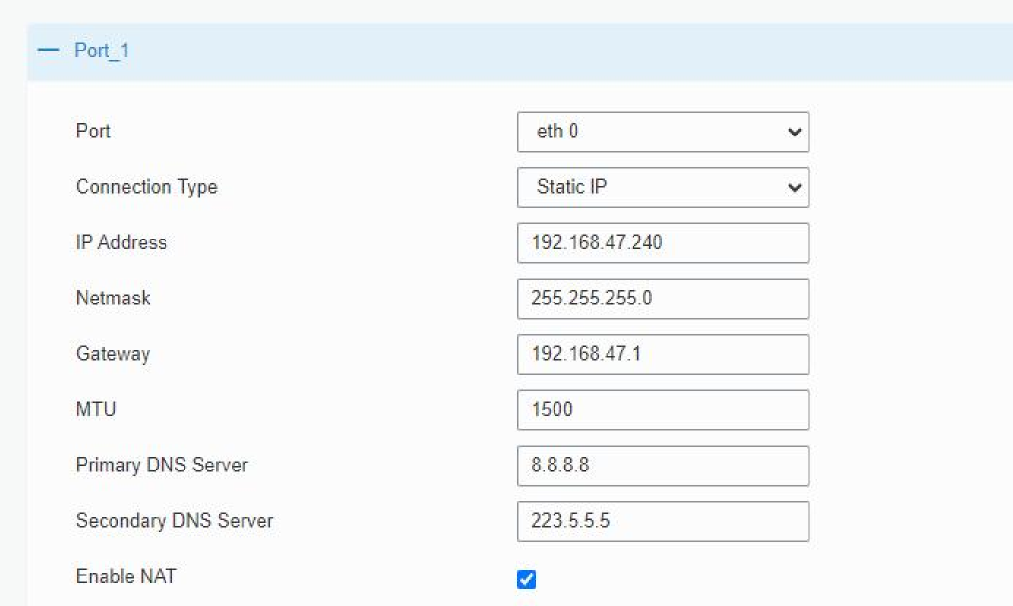
Host List	
Item	**Description**
DHCP Leases	
Interface	Show the interface: Wi-Fi HaLow or Wi-Fi 2.4G.
IP	Show IP address of DHCP client
MAC Address	Show MAC address of DHCP client
Lease Time Remaining	Show the remaining lease time of DHCP client.
MAC Binding	
Interface	Show the interface: Wi-Fi HaLow or Wi-Fi 2.4G.
IP & MAC	Show the IP address and MAC address set in the Static IP list of DHCP service.

6.2 Network

6.2.1 Interface

6.2.1.1 Port

The Ethernet port can be connected with Ethernet cable to get Internet access.



Port	eth 0
Connection Type	Static IP
IP Address	192.168.47.240
Netmask	255.255.255.0
Gateway	192.168.47.1
MTU	1500
Primary DNS Server	8.8.8.8
Secondary DNS Server	223.5.5.5
Enable NAT	☑

Port Setting

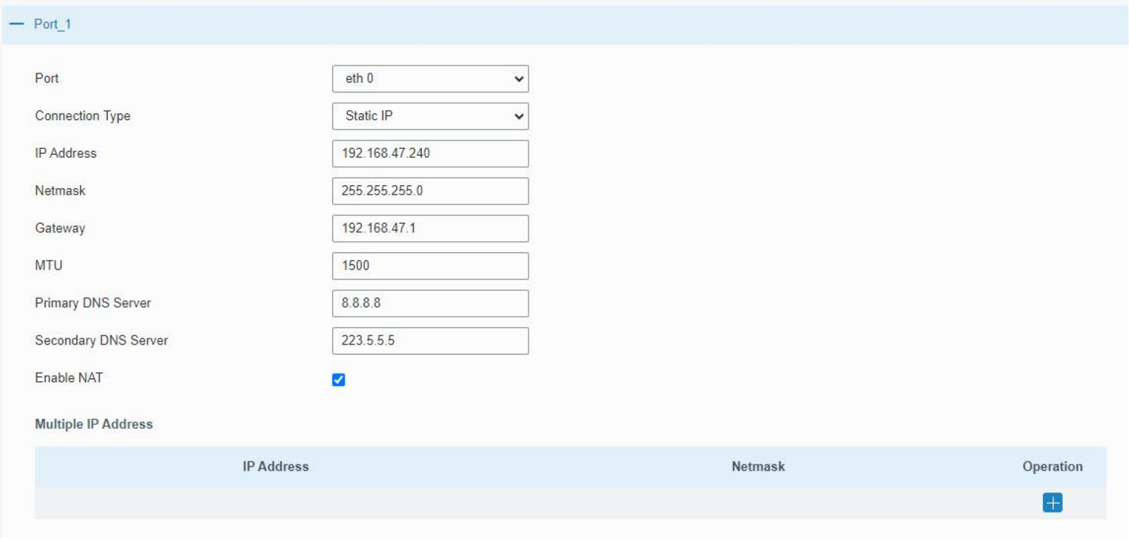
Item	Description	Default
Port	The port that is fixed as eth0 port and enabled.	eth 0
Connection Type	Select from Static IP, DHCP Client and PPPoE. **Static IP**: configure IP address, netmask and gateway for Ethernet WAN interface. **DHCP Client**: configure Ethernet WAN interface as DHCP Client to obtain IP address automatically. **PPPoE**: configure Ethernet WAN interface as PPPoE Client.	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.	223.5.5.5
Enable NAT	Enable or disable NAT function. When enabled, a private IP can be translated to a public IP.	Enable

Related Configuration Example

Ethernet Connection

1. Static IP Configuration

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



— Port_1

Port: eth 0

Connection Type: Static IP

IP Address: 192.168.47.240

Netmask: 255.255.255.0

Gateway: 192.168.47.1

MTU: 1500

Primary DNS Server: 8.8.8.8

Secondary DNS Server: 223.5.5.5

Enable NAT: ☑

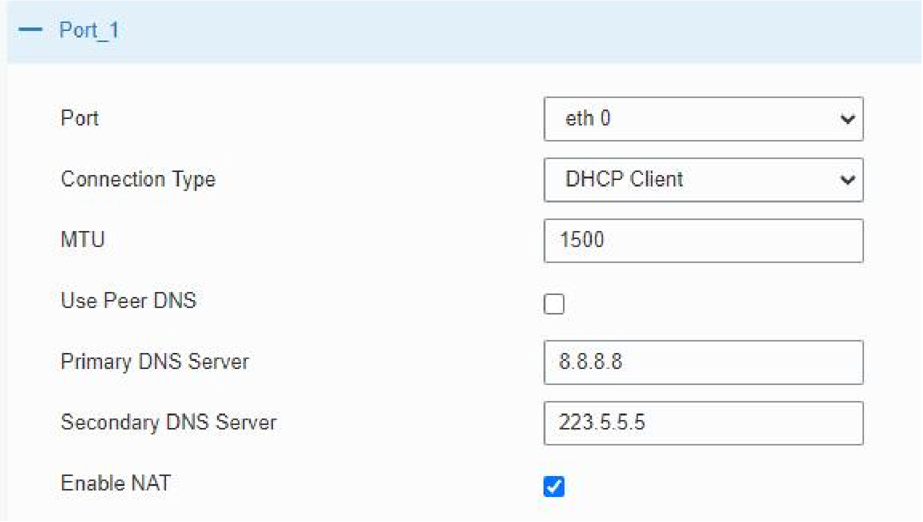
Multiple IP Address

IP Address	Netmask	Operation
		+

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

2. DHCP Client

If the external network has DHCP server enabled and has assigned IP addresses to the Ethernet WAN interface, select this mode to obtain IP address automatically.



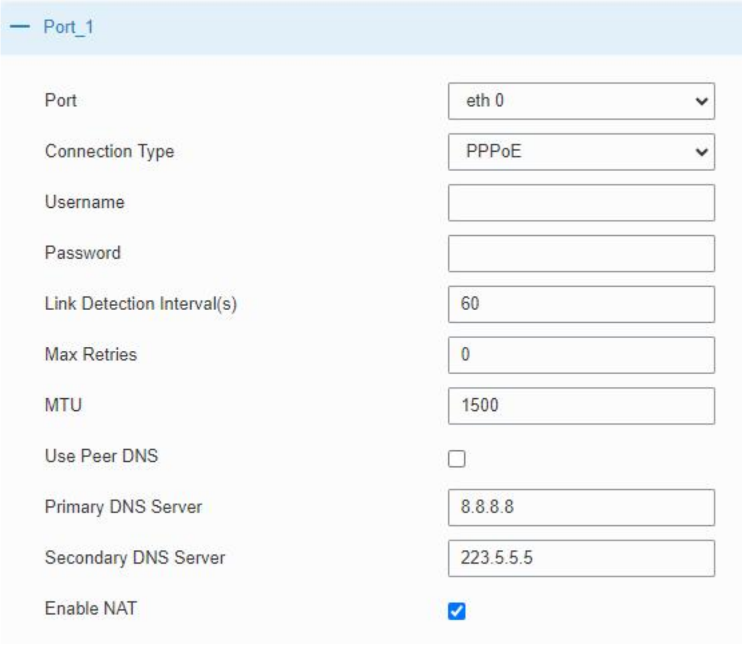
— Port_1

Port	eth 0
Connection Type	DHCP Client
MTU	1500
Use Peer DNS	□
Primary DNS Server	8.8.8.8
Secondary DNS Server	223.5.5.5
Enable NAT	☑

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

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.



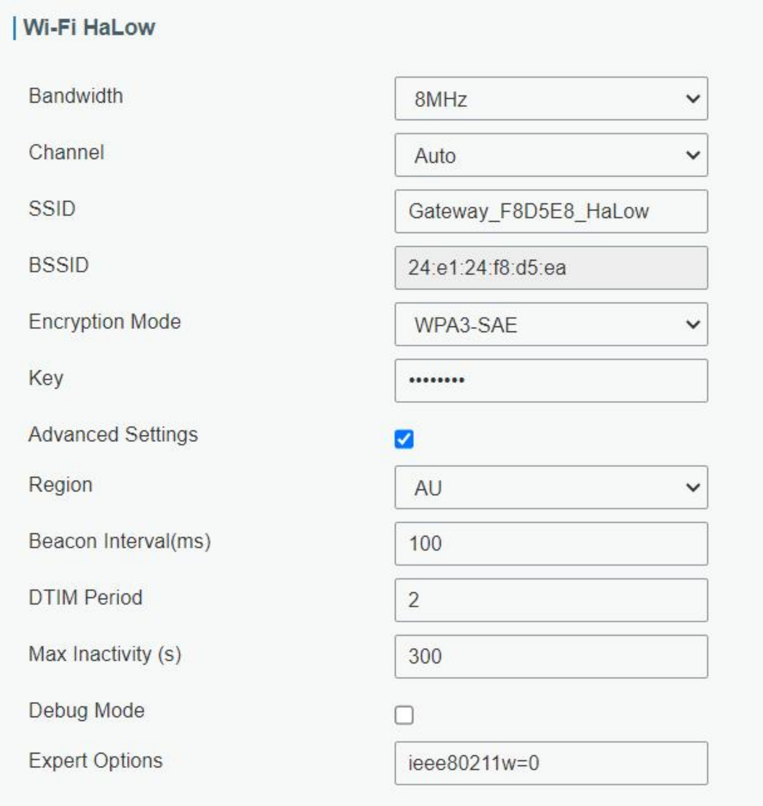
— Port_1

Port	eth 0
Connection Type	PPPoE
Username	
Password	
Link Detection Interval(s)	60
Max Retries	0
MTU	1500
Use Peer DNS	□
Primary DNS Server	8.8.8.8
Secondary DNS Server	223.5.5.5
Enable NAT	☑

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.

6.2.1.2 WLAN

This section explains how to set the related parameters for Wi-Fi 2.4G and Wi-Fi HaLow network. HL31 can work as Wi-Fi 2.4G or Wi-Fi HaLow access point to allow connections.

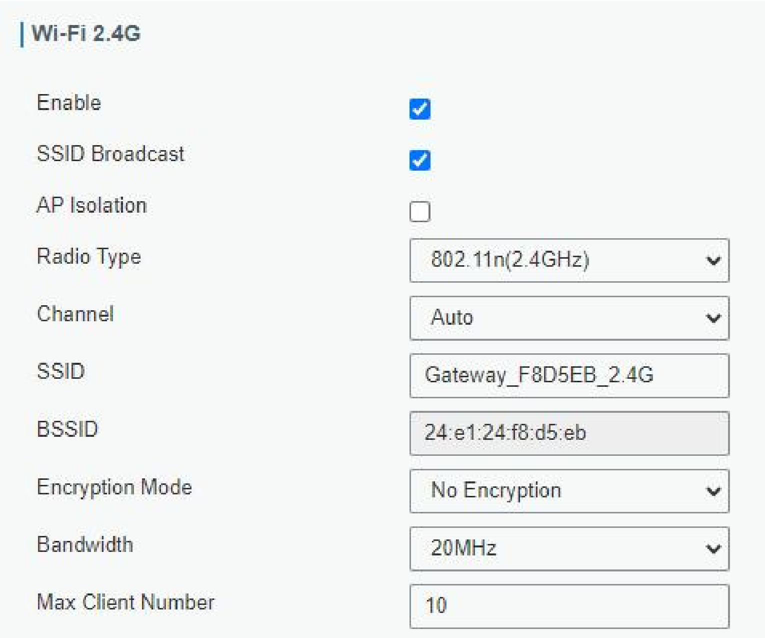


Wi-Fi HaLow

Bandwidth	8MHz
Channel	Auto
SSID	Gateway_F8D5E8_HaLow
BSSID	24:e1:24:f8:d5:ea
Encryption Mode	WPA3-SAE
Key	••••••••
Advanced Settings	☑
Region	AU
Beacon Interval(ms)	100
DTIM Period	2
Max Inactivity (s)	300
Debug Mode	□
Expert Options	ieee80211w=0

Wi-Fi HaLow Settings	
Item	**Description**
Bandwidth	Select working bandwidth. The options differ based on region. Higher bandwidth increases the data rate, and the transmission distance becomes shorter.
Channel	Select the wireless channel. The options differ based on region.
SSID	Fill in the SSID of the access point. Default: Gateway_XXXXXX_HaLow (XXXXXX=last 6 digits of MAC address)
BSSID	The MAC address of the access point. Either SSID or BSSID can be filled to join the network.

Encryption Mode	Select encryption mode. The options are “No Encryption", and “WPA3-SAE".
Key	Fill in the pre-shared key of WPA3 encryption.
Advanced Settings	
Region	The region of the frequency. This parameter should be the same as Wi-Fi HaLow clients.
Beacon Interval (ms)	The interval to broadcast the beacons to Wi-Fi HaLow clients.
DTIM Period	The period to send DTIM messages to Wi-Fi HaLow clients. DTIM is a message that is sent with beacons to “wake up” Wi-Fi HaLow clients from a sleeping state.
Max Inactivity (s)	If a client does not send anything within this interval, the gateway will send a frame to the client to check connectivity. If no response, the gateway will disconnect the connection with this client.
Debug Mode	After enabled, the gateway log files will print debug log information.
Expert Options	Enter some other PPP initialization strings to achieve advanced settings.

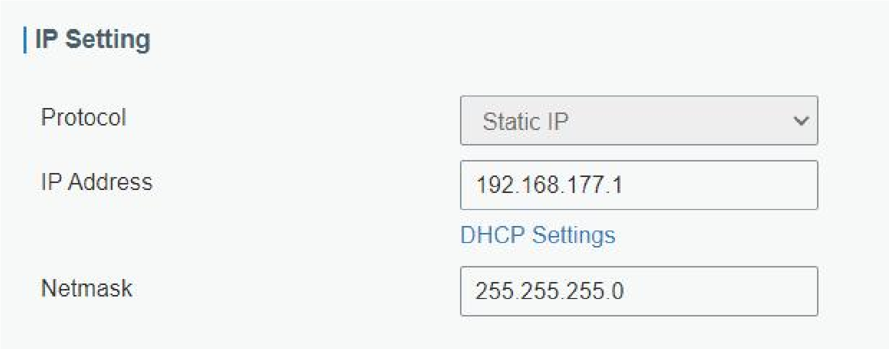


Wi-Fi 2.4G

Enable	☑
SSID Broadcast	☑
AP Isolation	□
Radio Type	802.11n(2.4GHz)
Channel	Auto
SSID	Gateway_F8D5EB_2.4G
BSSID	24:e1:24:f8:d5:eb
Encryption Mode	No Encryption
Bandwidth	20MHz
Max Client Number	10

Wi-Fi 2.4G Settings	
Item	**Description**
Enable	Enable/disable Wi-Fi 2.4G.
SSID Broadcast	When SSID broadcast is disabled, other wireless devices can't find the SSID, and users have to enter the SSID manually to access the wireless network.
AP Isolation	When AP isolation is enabled, all users which access the AP are isolated without communication with each other.
Radio Type	Select Radio type. The options are “802.11b (2.4 GHz)", “802.11g

	(2.4 GHz)", “802.11n (2.4 GHz)”.
Channel	Select the wireless channel. The options are "Auto", "1", "2"......"13".
BSSID	The MAC address of the access point. Either SSID or BSSID can be filled to join the network.
SSID	Fill in the SSID of the access point. Default: Gateway_XXXXXX_2.4G (XXXXXX=last 6 digits of MAC address)
Encryption Mode	Select encryption mode. The options are “No Encryption", “WEP Open System" , “WEP Shared Key", “WPA-PSK", “WPA2-PSK" and “WPA-PSK/WPA2-PSK".
Cipher	Select cipher. The options are “Auto", “AES", “TKIP" and “AES/TKIP".
Key	Fill in the pre-shared key of WEP/WPA encryption. Default: iotpassword
Bandwidth	Select bandwidth. The options are "20MHz" and "40MHz".
Max Client Number	Set the maximum number of client to connect this access point. Range: 1-15



IP Setting

Protocol: Static IP

IP Address: 192.168.177.1

DHCP Settings

Netmask: 255.255.255.0

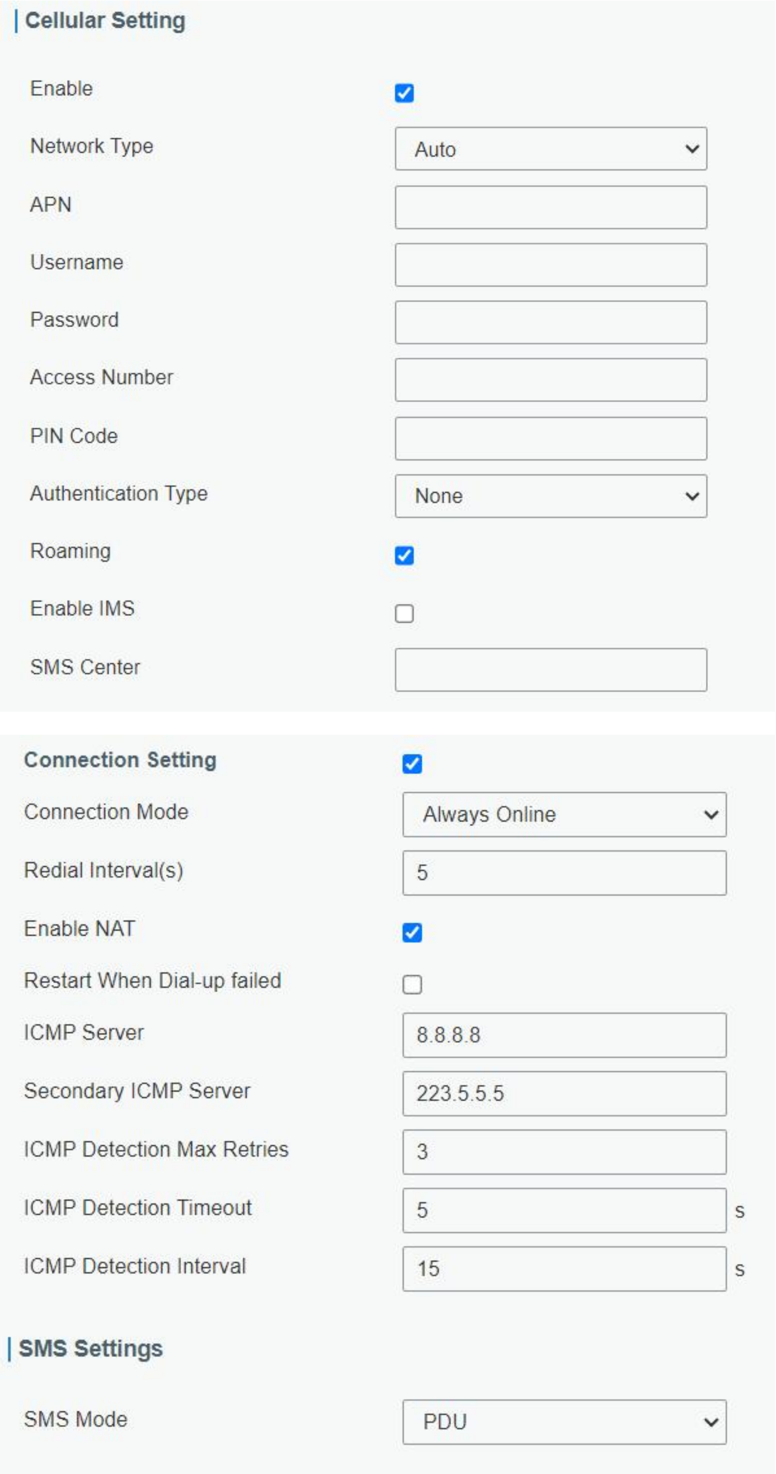
IP Setting	
Item	**Description**
Protocol	It is fixed as Static IP.
IP Address	Set the Wi-Fi IP address of this device. Wi-Fi HaLow and Wi-Fi 2.4G uses the same IP address.
Netmask	Set the netmask of the IP address.

Related Topic

Wi-Fi Application Example

6.2.1.3 Cellular (Cellular Version Only)

This section explains how to set the related parameters for cellular network.



Cellular Setting

Enable	☑
Network Type	Auto
APN	
Username	
Password	
Access Number	
PIN Code	
Authentication Type	None
Roaming	☑
Enable IMS	☐
SMS Center	

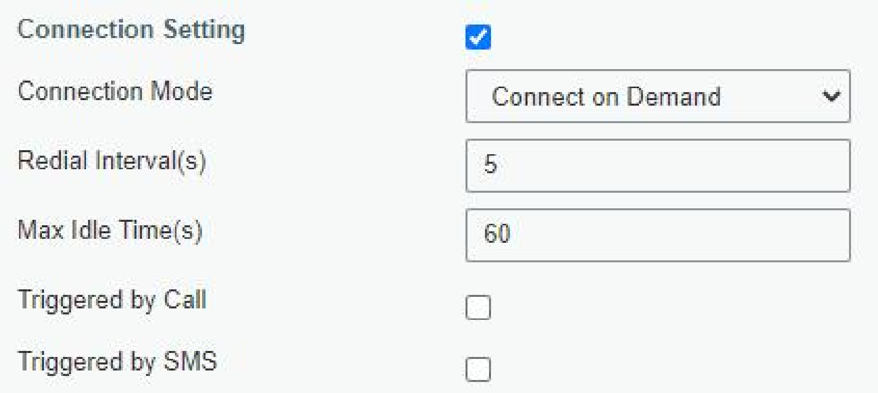
Connection Setting	☑
Connection Mode	Always Online
Redial Interval(s)	5
Enable NAT	☑
Restart When Dial-up failed	☐
ICMP Server	8.8.8.8
Secondary ICMP Server	223.5.5.5
ICMP Detection Max Retries	3
ICMP Detection Timeout	5 s
ICMP Detection Interval	15 s

SMS Settings

SMS Mode	PDU

General Settings	
Item	**Description**
Enable	Enable or disable the device to register to cellular network.
Network Type	Select from Auto, Auto 3G/4G, 4G Only and 3G Only. Auto: connect to the network with the strongest signal automatically. 4G Only: connect to 4G network only. And so on.
APN	Enter the Access Point Name for cellular dial-up connection provided

	by local ISP.
Username	Enter the username for cellular dial-up connection provided by local ISP.
Password	Enter the password for cellular dial-up connection provided by local ISP.
Access Number	Enter the dial-up center NO. For cellular dial-up connection provided by local ISP.
PIN Code	Enter a 4-8 characters PIN code to unlock the SIM.
Authentication Type	Select from NONE, PAP and CHAP.
Roaming	Enable or disable roaming.
Enable IMS	Enable or disable IMS function.
SMS Center	Enter the local SMS center number for storing, forwarding, converting and delivering SMS message.
Enable NAT	Enable or disable NAT function.
Restart When Dial-up failed	When this function is enabled, the gateway will restart automatically if the dial-up fails several times.
ICMP Server	Set the ICMP detection server's IP address.
Secondary ICMP Server	Set the secondary ICMP detection server's IP address.
ICMP Detection Max Retries	Set max number of retries when ICMP detection fails.
ICMP Detection Timeout	Set timeout of ICMP detection.
ICMP Detection Interval	Set interval of ICMP detection.
SMS Mode	Select SMS mode from TEXT and PDU.



Connection Setting ☑

Connection Mode: Connect on Demand

Redial Interval(s): 5

Max Idle Time(s): 60

Triggered by Call □

Triggered by SMS □

Item	Description
Connection Mode	
Connection Mode	Select from Always Online and Connect on Demand.
Redial Interval(s)	Set the time interval between redials. Range: 0-3600.
Max Idle Time(s)	Set the maximum duration of the gateway when current link is under idle status. Range: 10-3600.

Triggered by Call	The gateway will switch from offline mode to cellular network mode automatically when it receives a call from the specific phone number.
Call Group	Select a call group for call trigger. Go to **System > General Settings > Phone** to set up phone group.
Triggered by SMS	The gateway will switch from offline mode to cellular network mode automatically when it receives a specific SMS from the specific mobile phone.
SMS Group	Select a SMS group for trigger. Go to **System > General Settings > Phone** to set up SMS group.
SMS Text	Fill in the SMS content for triggering.

Related Topics

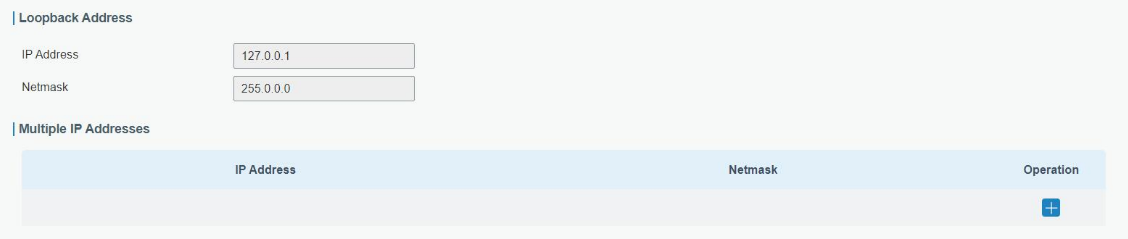
Cellular Connection Application Example

Phone Group

6.2.1.4 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.


Loopback Address

IP Address: 127.0.0.1

Netmask: 255.0.0.0

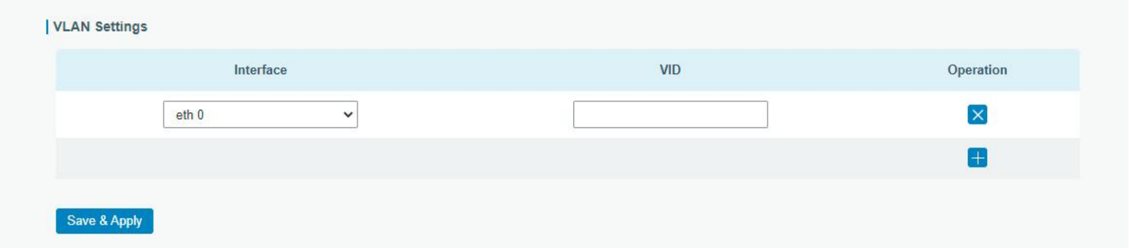
Multiple IP Addresses

IP Address	Netmask	Operation
		⊞

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

6.2.1.5 VLAN Trunk

HL31 gateway supports the Ethernet port working as VLAN Trunk client and be assigned a VLAN ID, which easy to traffic classification. When VLAN ID is set, port on **Network > Interface > Port** can be chosen as eth0.x with x being VLAN ID. VLAN Setting is blank by default, you can add a new VLAN label to certain interface by clicking ⊞.



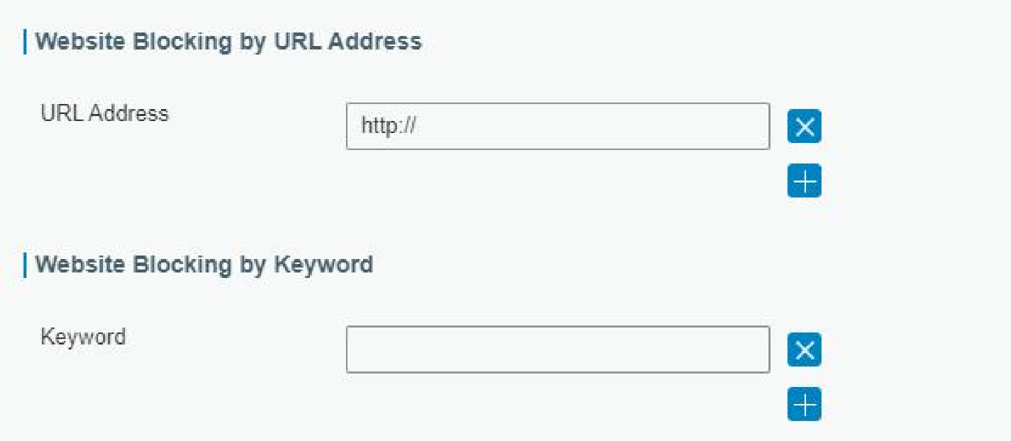
VLAN Trunk	
Item	**Description**
Interface	Select the VLAN interface, it’s fixed as eth0.
VID	Set the label ID of the VLAN. Range: 1-4094.

6.2.2 Firewall

This section describes how to set the firewall parameters, including website block, ACL, DMZ, Port Mapping and MAC Binding.

The firewall implements corresponding control of data flow at entry direction (from Internet to local area network) and exit direction (from local area network to Internet) according to the content features of packets, such as protocol style, source/destination IP address, etc. It ensures that the gateway operate in a safe environment and host in local area network.

6.2.2.1 Security

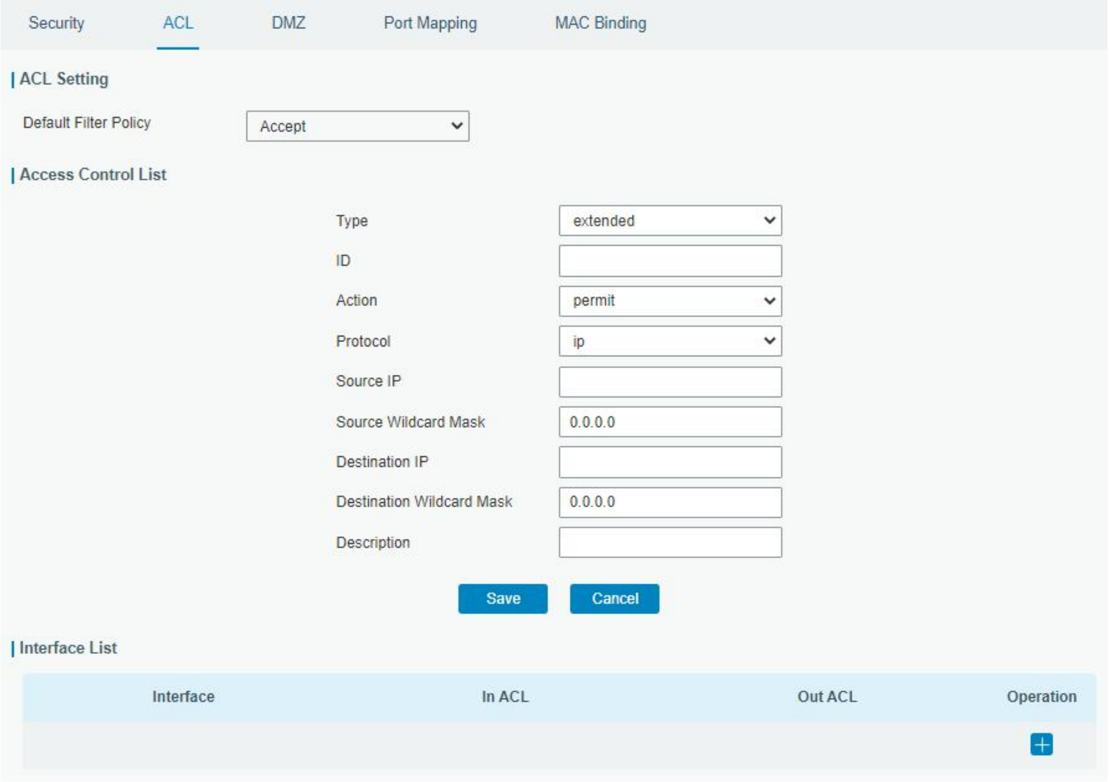


Website Blocking	
URL Address	Enter the HTTP address which you want to block.
Keyword	You can block specific website by entering keyword. The maximum number of character allowed is 64.

6.2.2.2 ACL

Access control list, also called ACL, implements permission or prohibition of access for specified network traffic (such as the source IP address) by configuring a series of matching rules so as to filter the network interface traffic. When gateway receives packet, the field will be analyzed according to the ACL rule applied to the current interface. After the special packet is identified, the permission or prohibition of corresponding packet will be implemented according to preset strategy.

The data package matching rules defined by ACL can also be used by other functions requiring flow distinction.



| ACL Setting

Default Filter Policy: Accept

| Access Control List

Type: extended

ID:

Action: permit

Protocol: ip

Source IP:

Source Wildcard Mask: 0.0.0.0

Destination IP:

Destination Wildcard Mask: 0.0.0.0

Description:

| Interface List

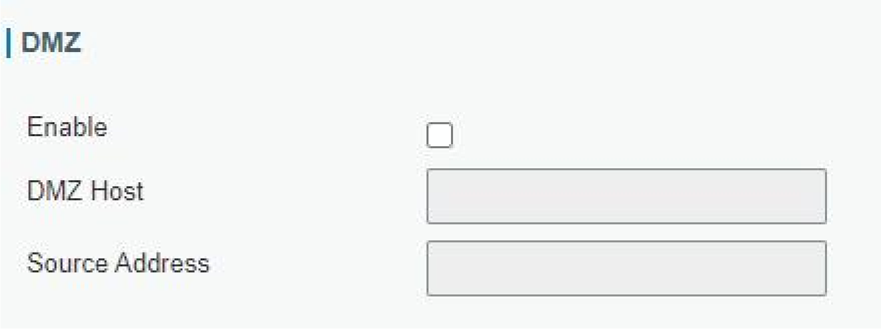
Interface	In ACL	Out ACL	Operation
			⊞

Item	Description
ACL Setting	
Default Filter Policy	Select from "Accept" and "Deny". The packets which are not included in the access control list will be processed by the default filter policy.
Access Control List	
Type	Select type from "Extended" and "Standard".
ID	User-defined ACL number. Range: 1-199.
Action	Select from "Permit" and "Deny".
Protocol	Select protocol from "ip", "icmp", "tcp", "udp", and "1-255".
Source IP	Source network address (leaving it blank means all).
Source Wildcard Mask	Wildcard mask of the source network address.
Destination IP	Destination network address (0.0.0.0 means all).
Destination Wildcard Mask	Wildcard mask of destination address.
Description	Fill in a description for the groups with the same ID.
ICMP Type	Enter the type of ICMP packet. Range: 0-255.
ICMP Code	Enter the code of ICMP packet. Range: 0-255.
Source Port Type	Select source port type, such as specified port, port range, etc.

Source Port	Set source port number. Range: 1-65535.
Start Source Port	Set start source port number. Range: 1-65535.
End Source Port	Set end source port number. Range: 1-65535.
Destination Port Type	Select destination port type, such as specified port, port range, etc.
Destination Port	Set destination port number. Range: 1-65535.
Start Destination Port	Set start destination port number. Range: 1-65535.
End Destination Port	Set end destination port number. Range: 1-65535.
More Details	Show information of the port.
Interface List	
Interface	Select network interface for access control.
In ACL	Select a rule for incoming traffic from ACL ID.
Out ACL	Select a rule for outgoing traffic from ACL ID.

6.2.2.3 DMZ

DMZ is a host within the internal network that has all ports exposed, except those forwarded ports in port mapping.



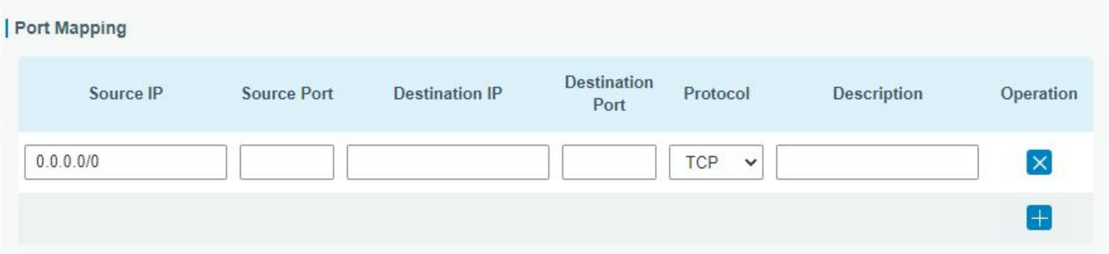
DMZ

Enable	□
DMZ Host	
Source Address	

DMZ	
Item	**Description**
Enable	Enable or disable DMZ.
DMZ Host	Enter the IP address of the DMZ host on the internal network.
Source Address	Set the source IP address which can access to DMZ host. "0.0.0.0/0" means any address.

6.2.2.4 Port Mapping (DNAT)

When external services are needed internally (for example, when a website is published externally), the external address initiates an active connection. And, the router or the gateway on the firewall receives the connection. Then it will convert the connection into the an internal connection. This conversion is called DNAT, which is mainly used for external and internal services.



Port Mapping

Source IP	Source Port	Destination IP	Destination Port	Protocol	Description	Operation
0.0.0.0/0				TCP		☒

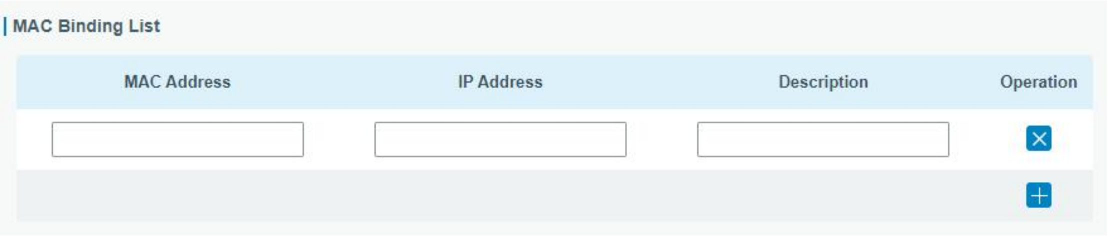
Port Mapping	
Item	**Description**
Source IP	Specify the host or network which can access local IP address. 0.0.0.0/0 means all.
Source Port	Enter the TCP or UDP port from which incoming packets are forwarded. Range: 1-65535.
Destination IP	Enter the IP address that packets are forwarded to after receiving from the incoming interface.
Destination Port	Enter the TCP or UDP port that packets are forwarded to after receiving from the incoming port(s). Range: 1-65535.
Protocol	Select TCP or UDP for your application requirements.
Description	The description of this rule.

Related Configuration Example

NAT Application Example

6.2.2.5 MAC Binding

MAC Binding is used for specifying hosts by matching MAC addresses and IP addresses that are in the list of allowed outer network access.



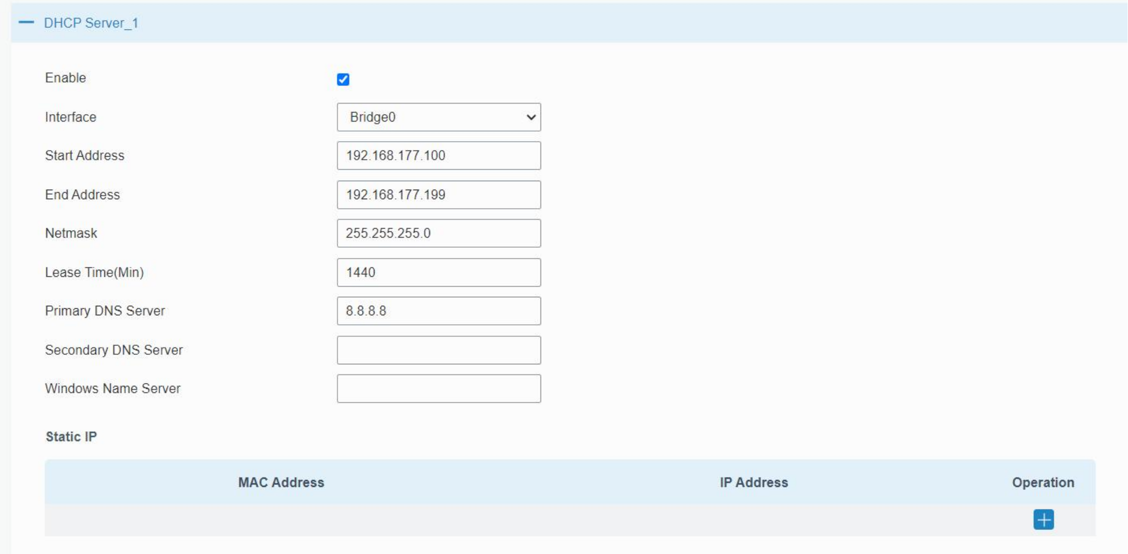
MAC Binding List

MAC Address	IP Address	Description	Operation
			☒

MAC Binding List	
Item	**Description**
MAC Address	Set the binding MAC address.
IP Address	Set the binding IP address.
Description	Fill in a description for convenience of recording the meaning of the binding rule for each piece of MAC-IP.

6.2.3 DHCP

HL31 can be set as a DHCP server to distribute IP address to Wi-Fi clients. Wi-Fi HaLow and Wi-Fi 2.4G uses the same DHCP IP address range.



DHCP Server_1

Enable	☑
Interface	Bridge0
Start Address	192.168.177.100
End Address	192.168.177.199
Netmask	255.255.255.0
Lease Time(Min)	1440
Primary DNS Server	8.8.8.8
Secondary DNS Server	
Windows Name Server	

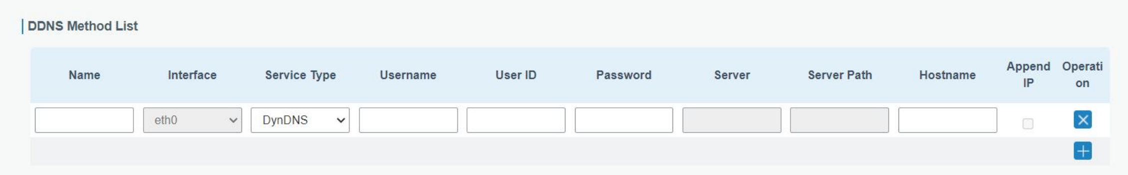
Static IP

MAC Address	IP Address	Operation
		+

DHCP Server		
Item	**Description**	**Default**
Enable	Enable or disable DHCP server.	Enable
Interface	The interface to assign IP addresses.	Bridge0
Start Address	Define the beginning of the pool of IP addresses which will be leased to DHCP clients.	192.168.1.100
End Address	Define the end of the pool of IP addresses which will be leased to DHCP clients.	192.168.1.199
Netmask	Define the subnet mask of IP address obtained by DHCP clients from DHCP server.	255.255.255.0
Lease Time (Min)	Set the lease time on which the client can use the IP address obtained from DHCP server. Range: 1-10080.	1440
Primary DNS Server	Set the primary DNS server.	8.8.8.8
Secondary DNS Server	Set the secondary DNS server.	Null
Windows Name Server	Define the Windows Internet Naming Service obtained by DHCP clients from DHCP sever. Generally you can leave it blank.	Null
Static IP		
MAC Address	Set a static and specific MAC address for the DHCP client (it should be different from other MACs so as to avoid conflict).	Null
IP Address	Set a static and specific IP address for the DHCP client (it should be outside of the DHCP range).	Null

6.2.4 DDNS

Dynamic DNS (DDNS) is a method that automatically updates a name server in the Domain Name System, which allows user to alias a dynamic IP address to a static domain name. DDNS serves as a client tool and needs to coordinate with DDNS server. Before starting configuration, user shall register on a website of proper domain name provider and apply for a domain name.



DDNS Method List

Name	Interface	Service Type	Username	User ID	Password	Server	Server Path	Hostname	Append IP	Operation
	eth0	DynDNS							□	☒

DDNS	
Item	**Description**
Name	Give the DDNS a descriptive name.
Interface	Set interface bundled with the DDNS.
Service Type	Select the DDNS service provider.
Username	Enter the username for DDNS register.
User ID	Enter User ID of the custom DDNS server.
Password	Enter the password for DDNS register.
Server	Enter the name of DDNS server.
Hostname	Enter the hostname for DDNS.
Append IP	Append your current IP to the DDNS server update path.

6.2.5 Link Failover

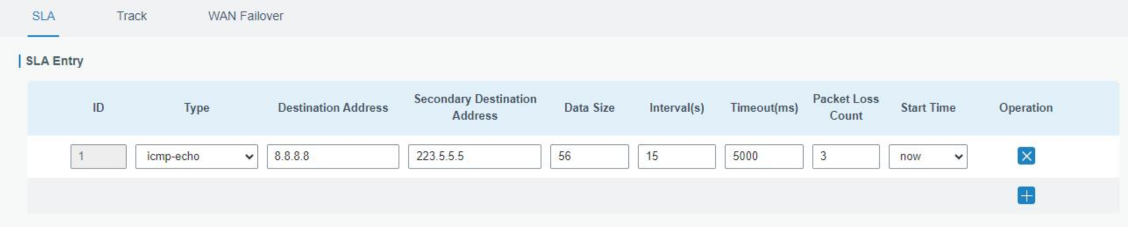
This section describes how to configure link failover strategies, such as VRRP strategies.

Configuration Steps

1. Define one or more SLA operations (ICMP probe).
2. Define one or more track objects to track the status of SLA operation.
3. Define applications associated with track objects, such as VRRP or static routing.

6.2.5.1 SLA

SLA setting is used for configuring link probe method. The default probe type is ICMP.



SLA Entry

ID	Type	Destination Address	Secondary Destination Address	Data Size	Interval(s)	Timeout(ms)	Packet Loss Count	Start Time	Operation
1	icmp-echo	8.8.8.8	223.5.5.5	56	15	5000	3	now	☒

SLA		
Item	**Description**	**Default**
ID	SLA index. Up to 10 SLA settings can be added. Range: 1-10.	1

Type	ICMP-ECHO is the default type to detect if the link is alive.	icmp-echo
Destination Address	The detected IP address.	8.8.8.8
Secondary Destination Address	The secondary detected IP address.	223.5.5.5
Data Size	User-defined data size. Range: 0-1000.	56
Interval (s)	User-defined detection interval. Range: 1-608400.	30
Timeout (ms)	User-defined timeout for response to determine ICMP detection failure. Range: 1-300000.	5000
Packet Loss Count	Define packet loss count in each SLA probe. SLA probe fails when the preset packet loss count is exceeded.	5
Start Time	Detection start time; select from "Now" and blank character. Blank character means this SLA detection doesn't start.	now

6.2.5.2 Track

Track setting is designed for achieving linkage among SLA module, Track module and Application module. Track setting is located between application module and SLA module with main function of shielding the differences of various SLA modules and providing unified interfaces for application module.

Linkage between Track Module and SLA module

Once you complete the configuration, the linkage relationship between Track module and SLA module will be established. SLA module is used for detection of link status, network performance and notification of Track module. The detection results help track status change timely.

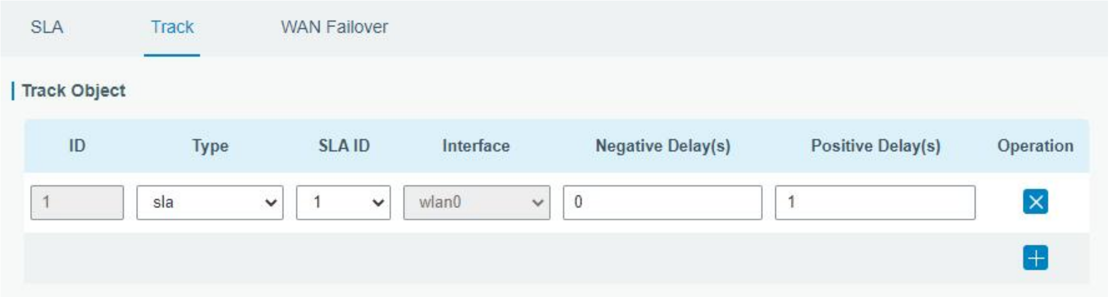
- For successful detection, the corresponding track item is Positive.
- For failed detection, the corresponding track item is Negative.

Linkage between Track Module and Application Module

After configuration, the linkage relationship between Track module and Application module will be established. When any change occurs in track item, a notification that requires corresponding treatment will be sent to Application module.

Currently, the application modules like VRRP and static routing can get linkage with track module.

If it sends an instant notification to Application module, the communication may be interrupted in some circumstances due to routing's failure like timely restoration or other reasons. Therefore, user can set up a period of time to delay notifying application module when the track item status changes.



SLA Track WAN Failover

Track Object

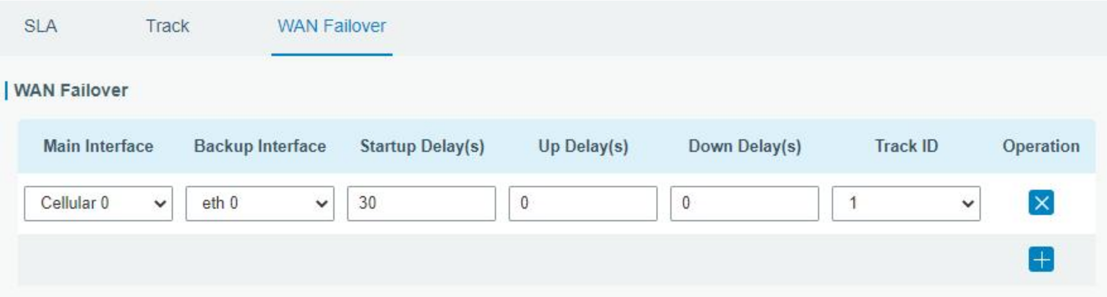
ID	Type	SLA ID	Interface	Negative Delay(s)	Positive Delay(s)	Operation
1	sla	1	wlan0	0	1	☒

Item	Description	Default
Index	Track index. Up to 10 track settings can be configured. Range: 1-10.	1
Type	The options are "sla" and "interface".	SLA
SLA ID	Defined SLA ID.	1
Interface	Select the interface whose status will be detected.	----
Negative Delay (s)	When interface is down or SLA probing fails, it will wait according to the time set here before actually changing its status to Down. Range: 0-180 (0 refers to immediate switching).	0
Positive Delay (s)	When failure recovery occurs, it will wait according to the time set here before actually changing its status to Up. Range: 0-180 (0 refers to immediate switching).	1

6.2.5.3 WAN Failover

WAN failover refers to failover between Ethernet WAN interface and cellular interface. When service transmission can’t be carried out normally due to malfunction of a certain interface or lack of bandwidth, the rate of flow can be switched to backup interface quickly. Then the backup interface will carry out service transmission and share network flow so as to improve reliability of communication of data equipment.

When link state of main interface is switched from up to down, system will have the pre-set delay works instead of switching to link of backup interface immediately. Only if the state of main interface is still down after delay, will the system switch to link of backup interface. Otherwise, system will remain unchanged.



SLA Track WAN Failover

WAN Failover

Main Interface	Backup Interface	Startup Delay(s)	Up Delay(s)	Down Delay(s)	Track ID	Operation
Cellular 0	eth 0	30	0	0	1	☒

WAN Failover		
Parameters	**Description**	**Default**
Main Interface	Select a link interface as the main link.	--
Backup Interface	Select a link interface as the backup link.	--
Startup Delay (s)	Set how long to wait for the startup tracking detection policy to take effect. Range: 0-300.	30
Up Delay (s)	When the primary interface switches from failed detection to successful detection, switching can be delayed based on the set time. Range: 0-180 (0 refers to immediate switching)	0
Down Delay (s)	When the primary interface switches from successful detection to failed detection, switching can be delayed based on the set time. Range: 0-180 (0 refers to immediate switching).	0
Track ID	Track detection, select the defined track ID.	--

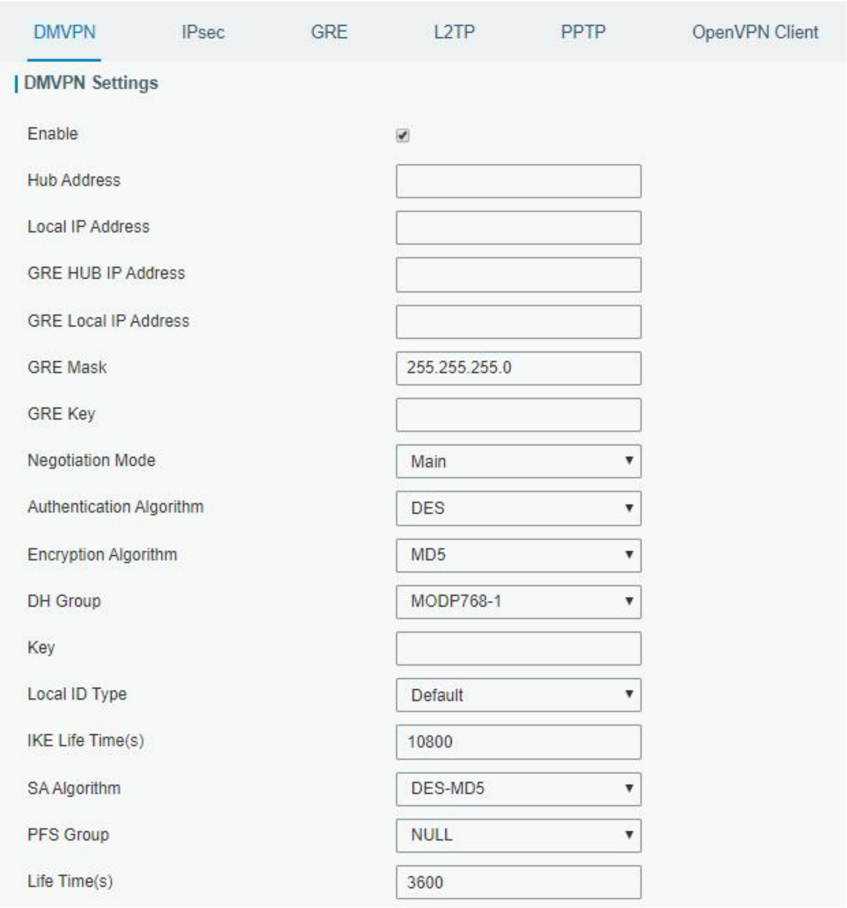
6.2.6 VPN

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.

HL31 supports DMVPN, IPsec, GRE, L2TP, PPTP, OpenVPN, as well as GRE over IPsec and L2TP over IPsec.

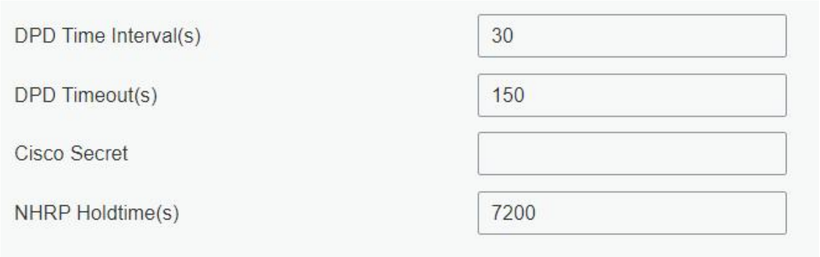
6.2.6.1 DMVPN

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 Settings

Enable	☑
Hub Address	
Local IP Address	
GRE HUB IP Address	
GRE Local IP Address	
GRE Mask	255.255.255.0
GRE Key	
Negotiation Mode	Main
Authentication Algorithm	DES
Encryption Algorithm	MD5
DH Group	MODP768-1
Key	
Local ID Type	Default
IKE Life Time(s)	10800
SA Algorithm	DES-MD5
PFS Group	NULL
Life Time(s)	3600



DPD Time Interval(s)	30
DPD Timeout(s)	150
Cisco Secret	
NHRP Holdtime(s)	7200

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".

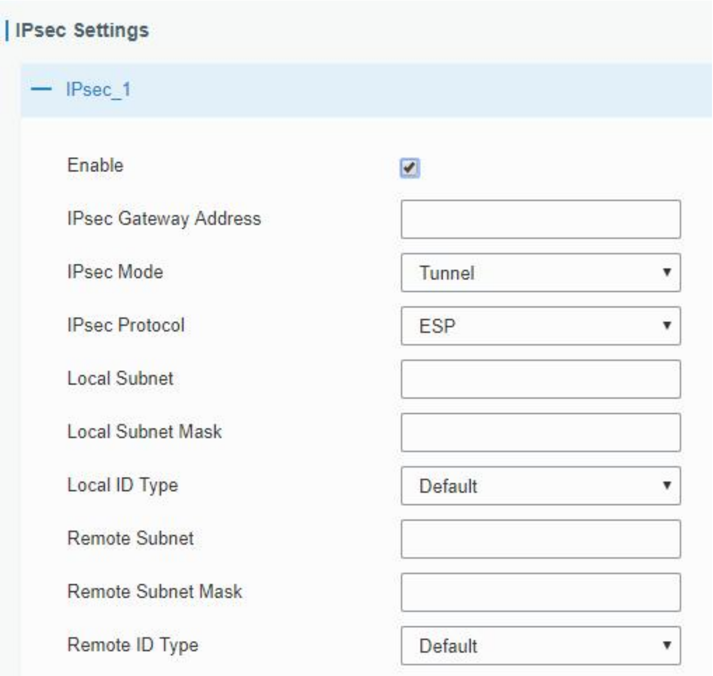
Key	Enter the preshared key.
Local ID Type	Select from "Default", "ID", "FQDN", and "User FQDN"
IKE Life Time (s)	Set the lifetime in IKE negotiation. Range: 60-86400.
SA Algorithm	Select from "DES_MD5", "DES_SHA1", "3DES_MD5", "3DES_SHA1", "AES128_MD5", "AES128_SHA1", "AES192_MD5", "AES192_SHA1", "AES256_MD5" 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.

6.2.6.2 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.

HL31 supports running at most 3 IPsec clients at the same time.

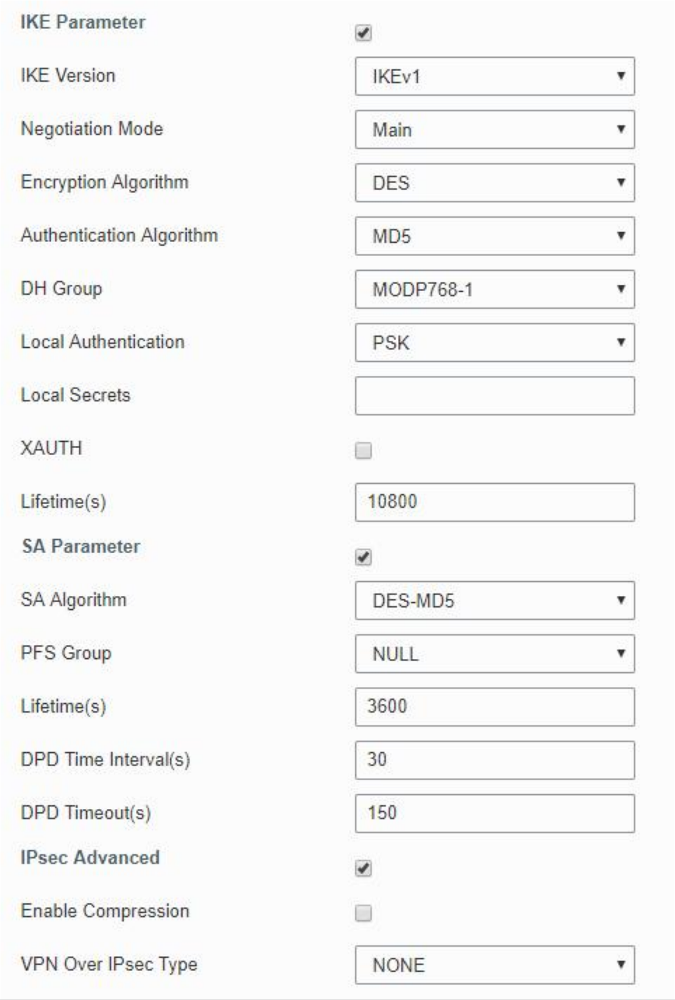


IPsec Settings

— IPsec_1

Enable	☑
IPsec Gateway Address	
IPsec Mode	Tunnel
IPsec Protocol	ESP
Local Subnet	
Local Subnet Mask	
Local ID Type	Default
Remote Subnet	
Remote Subnet Mask	
Remote ID Type	Default

IPsec	
Item	**Description**
Enable	Enable or disable IPsec tunnel. A maximum of 3 tunnels is allowed.
IPsec Gateway Address	Enter the IP address of remote IPsec server.
IPsec Mode	Select Tunnel or Transport.
IPsec Protocol	Select ESP or AH.
Local Subnet	Enter the local LAN subnet IP address on the IPsec tunnel.
Local Subnet Netmask	Enter the local LAN netmask on the IPsec tunnel.
Local ID Type	Select the identifier type to send to remote peer. **Default:** None **ID:** use local subnet IP address as ID **FQDN:** fully qualified domain name, example: test.user.com **User FQDN:** fully qualified username string with email address format, example:test@user.com
Remote Subnet	Set the remote LAN subnet that on the IPsec tunnel.
Remote Subnet Mask	Enter the remote LAN netmask on the IPsec tunnel.
Remote ID type	Select the identifier type that is the same as remote peer local ID. **Default:** None **ID:** use remote subnet IP address as ID **FQDN:** fully qualified domain name, example: test.user.com **User FQDN:** fully qualified username string with email address format, example: test@user.com



IKE Parameter ☑
IKE Version: IKEv1
Negotiation Mode: Main
Encryption Algorithm: DES
Authentication Algorithm: MD5
DH Group: MODP768-1
Local Authentication: PSK
Local Secrets:
XAUTH □
Lifetime(s): 10800
SA Parameter ☑
SA Algorithm: DES-MD5
PFS Group: NULL
Lifetime(s): 3600
DPD Time Interval(s): 30
DPD Timeout(s): 150
IPsec Advanced ☑
Enable Compression □
VPN Over IPsec Type: NONE

IKE Parameter	
Item	**Description**
IKE Version	Select the method of key exchange of IKEv1 or IKEv2.
Negotiation Mode	Select from Main and Aggressive.
Encryption Algorithm	Select DES, 3DES, AES128, AES192 or AES256.
Authentication Algorithm	Select from MD5 and SHA1.
DH Group	Select MODP768_1, MODP1024_2 or MODP1536_5.
Local Authentication	Select PSK or CA. **PSK:** use pre-shared key to complete the authentication. **CA:** use certificate to complete the authentication. After selecting, go to **Network > VPN > Certifications** page to import CA certificate, local certificate and private key to corresponding fields.
Local Secrets	Enter the preshared key.
Remote Authentication	Enter the pre-shared key which is defined on serer side.
Remote Secrets	Select PSK or CA. **PSK:** use pre-shared key to complete the authentication. **CA:** use certificate to complete the authentication.

XAUTH	When using IKEv1, define 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.

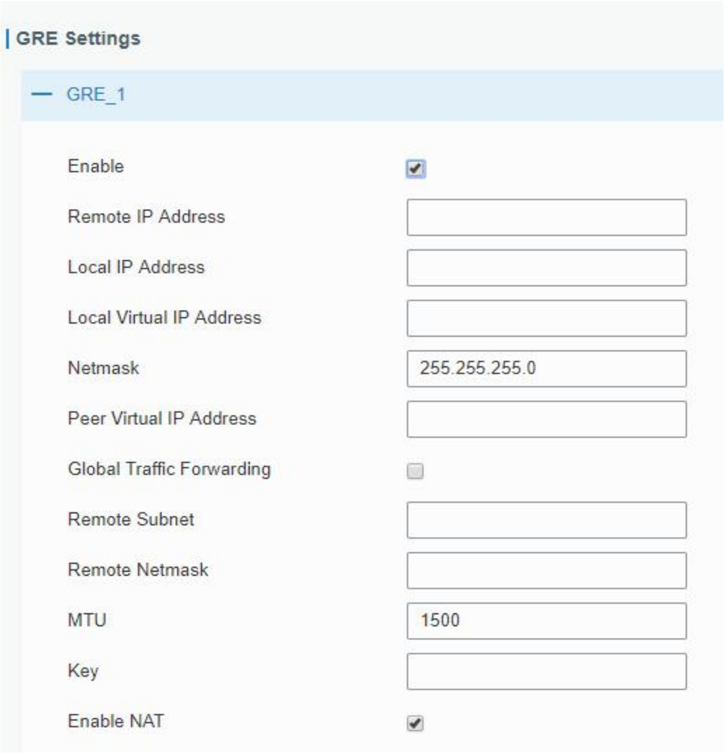
6.2.6.3 GRE

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.

HL31 supports running at most 3 GRE clients at the same time.



GRE Settings

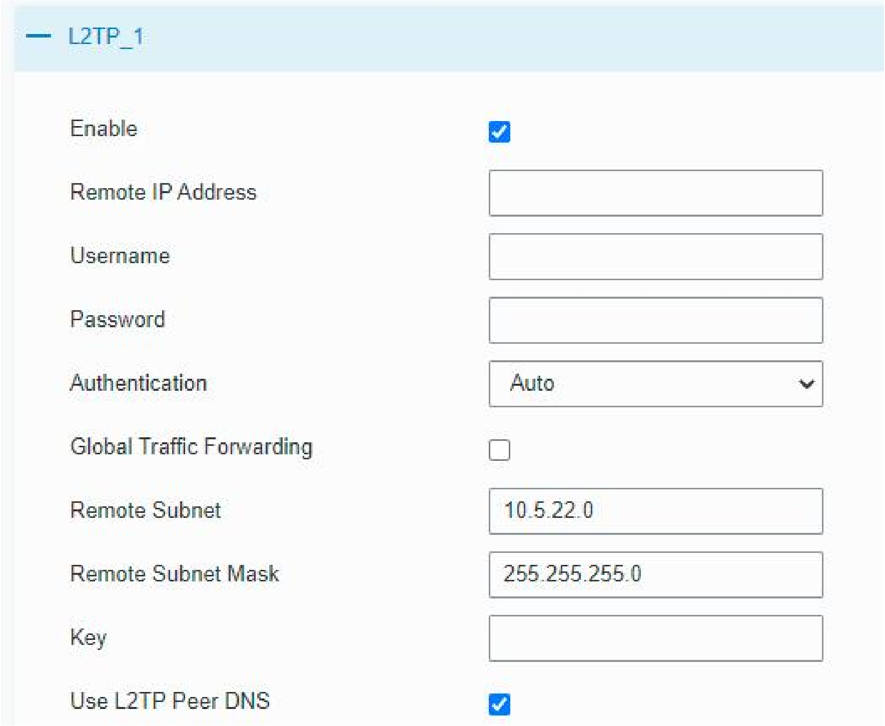
— GRE_1

Enable	☑
Remote IP Address	
Local IP Address	
Local Virtual IP Address	
Netmask	255.255.255.0
Peer Virtual IP Address	
Global Traffic Forwarding	□
Remote Subnet	
Remote Netmask	
MTU	1500
Key	
Enable NAT	☑

GRE	
Item	**Description**
Enable	Check to enable GRE function. A maximum of 3 tunnels is allowed.
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.
Enable NAT	Enable NAT traversal function.

6.2.6.4 L2TP

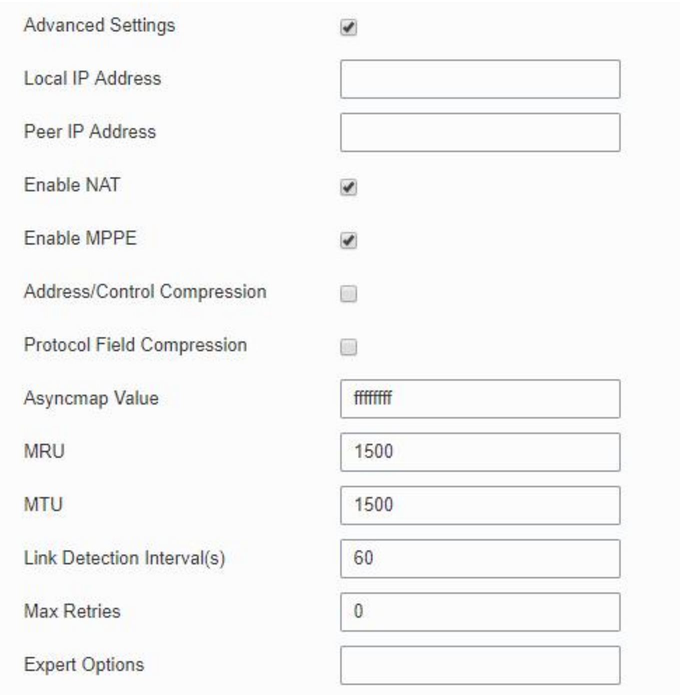
Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by an Internet service provider (ISP) to enable the operation of a virtual private network (VPN) over the Internet.



— L2TP_1

Enable	☑
Remote IP Address	
Username	
Password	
Authentication	Auto
Global Traffic Forwarding	□
Remote Subnet	10.5.22.0
Remote Subnet Mask	255.255.255.0
Key	
Use L2TP Peer DNS	☑

L2TP	
Item	**Description**
Enable	Enable or disable L2TP client. A maximum of 3 tunnels is allowed.
Remote IP Address	Enter remote L2TP server's IP address or domain name.
Username	Enter the username that L2TP server provides.
Password	Enter the password that L2TP server provides.
Authentication	Select authentication type used to secure data sessions.
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.
Use L2TP Peer DNS	Enable to use the DNS address of peer L2TP server .

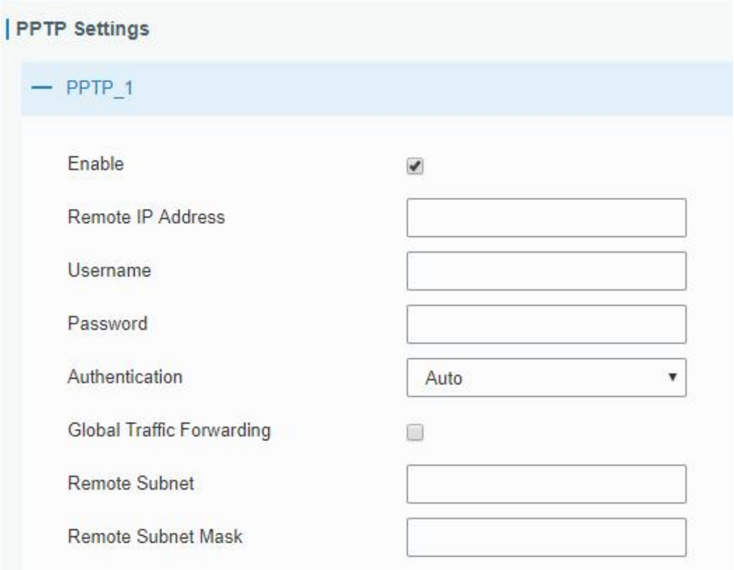


Advanced Settings	☑
Local IP Address	
Peer IP Address	
Enable NAT	☑
Enable MPPE	☑
Address/Control Compression	□
Protocol Field Compression	□
Asyncmap Value	ffffffff
MRU	1500
MTU	1500
Link Detection Interval(s)	60
Max Retries	0
Expert Options	

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 NAT	Enable NAT traversal function.
Enable MPPE	Enable or disable MPPE(Microsoft Point to Point 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-ffffffff.
MRU	Set the maximum receive unit. Range: 64-1500.
MTU	Set the maximum transmission unit. Range: 64-1500
Link Detection Interval (s)	Set the link detection interval time to ensure tunnel connection. Range: 0-600.
Max Retries	Set the maximum times of 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.

6.2.6.5 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.

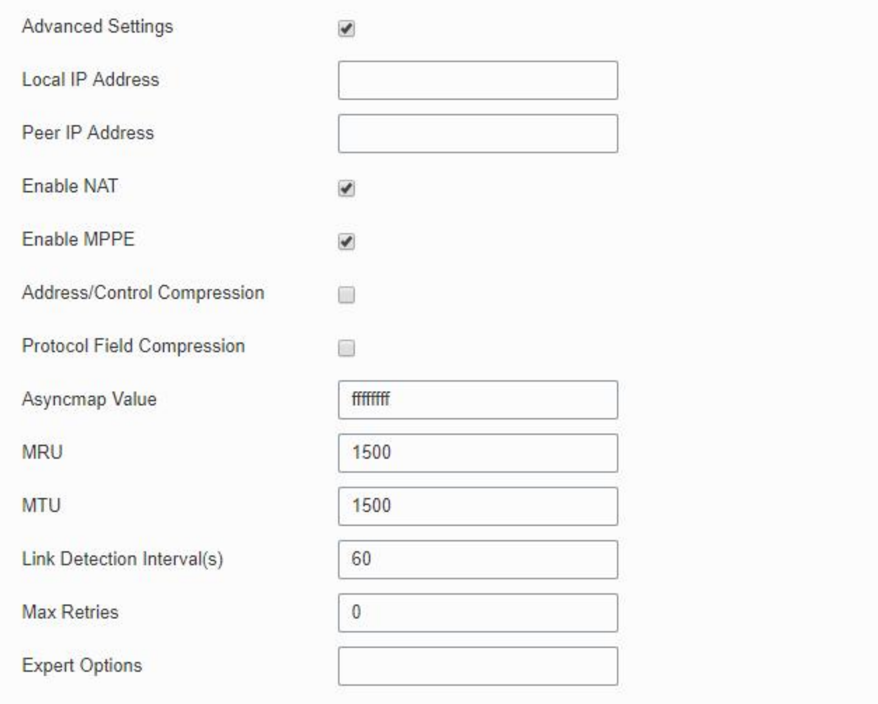


PPTP Settings

— PPTP_1

Enable	☑
Remote IP Address	
Username	
Password	
Authentication	Auto ▾
Global Traffic Forwarding	□
Remote Subnet	
Remote Subnet Mask	

PPTP	
Item	**Description**
Enable	Enable or disable PPTP client. A maximum of 3 tunnels is allowed.
Remote IP Address	Enter remote PPTP server's IP address or domain name.
Username	Enter the username that PPTP server provides.
Password	Enter the password that PPTP server provides.
Authentication	Select authentication type used to secure data sessions.
Global Traffic Forwarding	All of the data traffic will be sent out via PPTP tunnel once enable this function.
Remote Subnet	Enter the remote subnet of PPTP VPN server.
Remote Subnet Mask	Enter the remote netmask of PPTP VPN server.

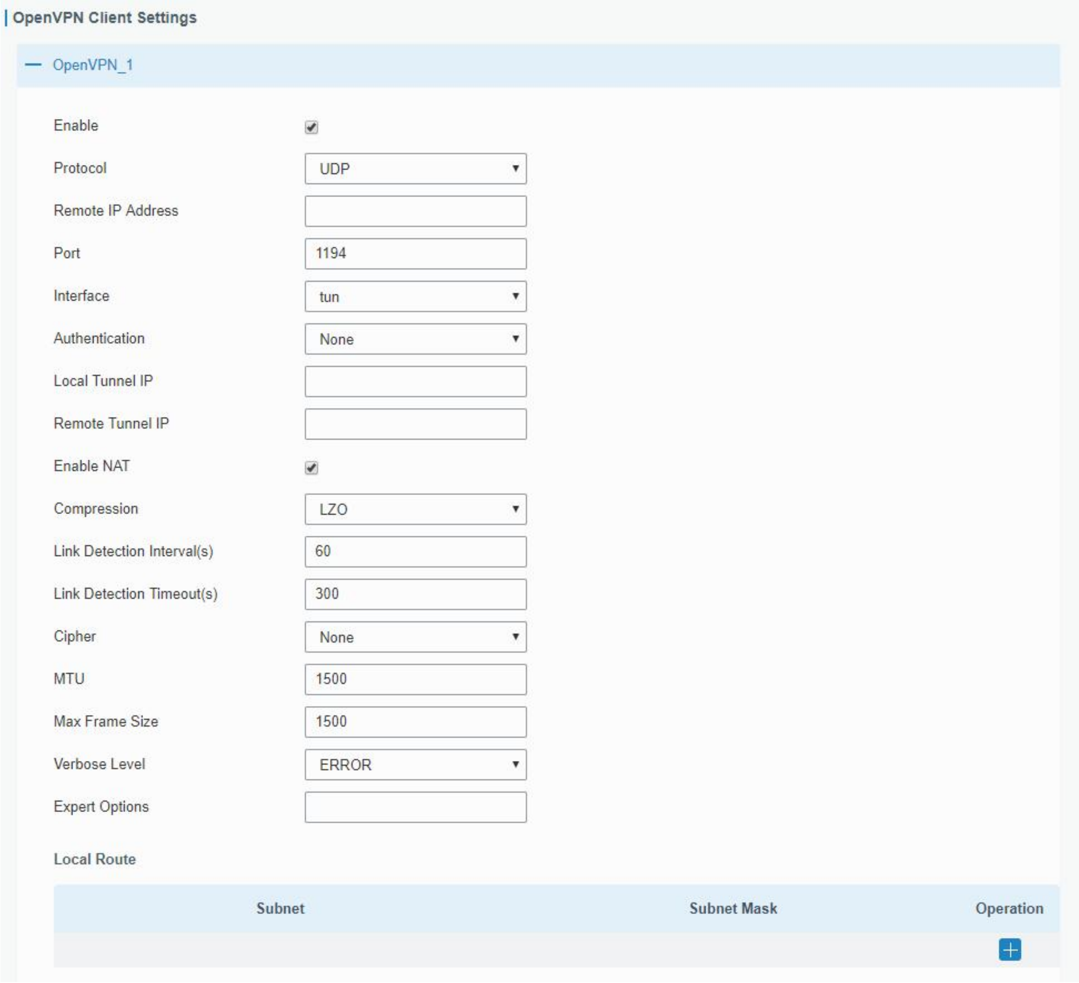


Advanced Settings	☑
Local IP Address	
Peer IP Address	
Enable NAT	☑
Enable MPPE	☑
Address/Control Compression	□
Protocol Field Compression	□
Asyncmap Value	ffffffff
MRU	1500
MTU	1500
Link Detection Interval(s)	60
Max Retries	0
Expert Options	

PPTP Advanced Settings	
Item	**Description**
Local IP Address	Set tunnel IP address of PPTP client. Client will obtain tunnel IP address automatically from the server when it's null.
Peer IP Address	Enter tunnel IP address of PPTP server.
Enable NAT	Enable the NAT faction of PPTP.
Enable MPPE	Enable MPPE(Microsoft Point to Point 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-ffffffff.
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.

6.2.6.6 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. HL31 supports running at most 3 OpenVPN clients at the same time.



OpenVPN Client Settings

— OpenVPN_1

Enable	☑
Protocol	UDP ▾
Remote IP Address	
Port	1194
Interface	tun ▾
Authentication	None ▾
Local Tunnel IP	
Remote Tunnel IP	
Enable NAT	☑
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	

Local Route

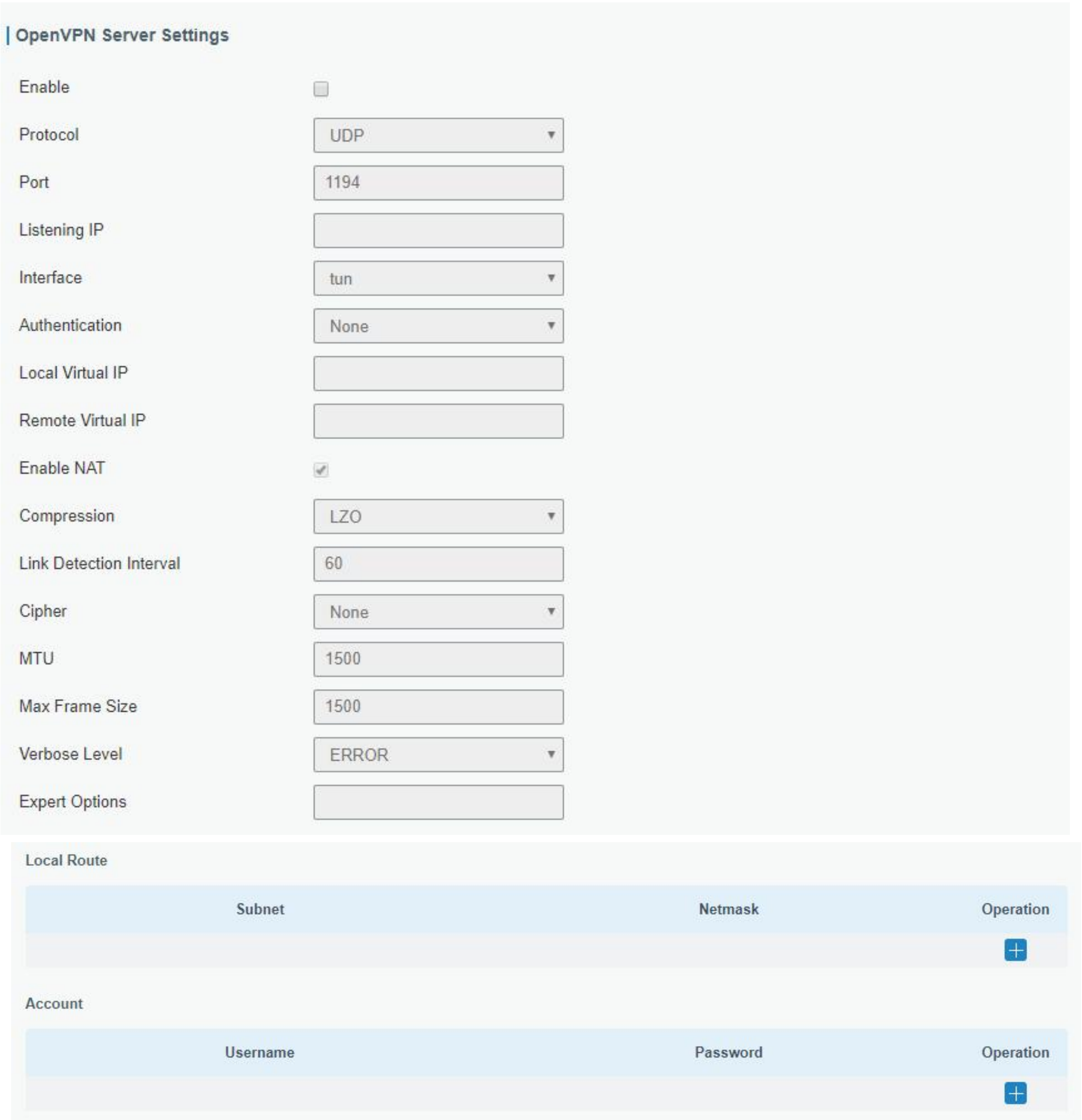
Subnet	Subnet Mask	Operation
		+

OpenVPN Client	
Item	**Description**
Enable	Enable OpenVPN client. A maximum of 3 tunnels is allowed.
Protocol	Select a transport protocol used by connecting UDP and TCP.
Remote IP Address	Enter remote OpenVPN server's IP address or domain name.
Port	Enter the TCP/UCP service number of remote OpenVPN server. Range: 1-65535.
Interface	Select virtual VPN network interface type from TUN and TAP. TUN devices encapsulate IPv4 or IPv6 (OSI Layer 3) while TAP devices encapsulate Ethernet 802.3 (OSI Layer 2).
Authentication	Select authentication type used to secure data sessions. **Pre-shared:** use the same secret key as server to complete the authentication. After selecting, go to **Network > VPN > Certifications** page to import a static.key to **PSK** field. **Username/Password:** use username/password which is preset in server side to complete the authentication. **X.509 cert:** use X.509 type certificate to complete the authentication. After selecting, go to **Network > VPN > Certifications** page to import CA certificate, client certificate

	and client private key to corresponding fields. **X.509 cert + user:** use both username/password and X.509 cert authentication type.
Local Tunnel IP	Set local tunnel address when authentication type is **None** or **Pre-shared**.
Remote Tunnel IP	Set remote tunnel address when authentication type is **None** or **Pre-shared**.
Global Traffic Forwarding	All the data traffic will be sent out via OpenVPN tunnel when this function is enabled.
Enable TLS Authentication	Disable or enable TLS authentication when authentication type is X.509 cert. After being enabled, go to **Network > VPN > Certifications** page to import a ta.key to **TA** field. Note: this option only supports tls-auth. For tls-crypt, please add this format string on expert option: tls-crypt /etc/openvpn/openvpn-client1-ta.key
Enable NAT	Enable NAT traversal function.
Compression	Select LZO to compress data.
Link Detection Interval (s)	Set link detection interval time to ensure tunnel connection. If this is set on both server and client, the value pushed from server will override the client local values. Range: 10-1800 s.
Link Detection Timeout (s)	OpenVPN will be reestablished after timeout. If this is set on both server and client, the value pushed from server will override the client local values. Range: 60-3600 s.
Cipher	Select from NONE, BF-CBC, DES-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, WARING, NOTICE and DEBUG.
Expert Options	User can enter some initialization strings in this field and separate the strings with semicolon. **Example:** auth SHA256; key direction 1
Local Route	
Subnet	Set the local route's IP address.
Subnet Mask	Set the local route's netmask.

6.2.6.7 OpenVPN Server

HL31 supports OpenVPN server to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities.



OpenVPN Server Settings

Enable	□
Protocol	UDP
Port	1194
Listening IP	
Interface	tun
Authentication	None
Local Virtual IP	
Remote Virtual IP	
Enable NAT	☑
Compression	LZO
Link Detection Interval	60
Cipher	None
MTU	1500
Max Frame Size	1500
Verbose Level	ERROR
Expert Options	

Local Route

Subnet	Netmask	Operation
		+

Account

Username	Password	Operation
		+

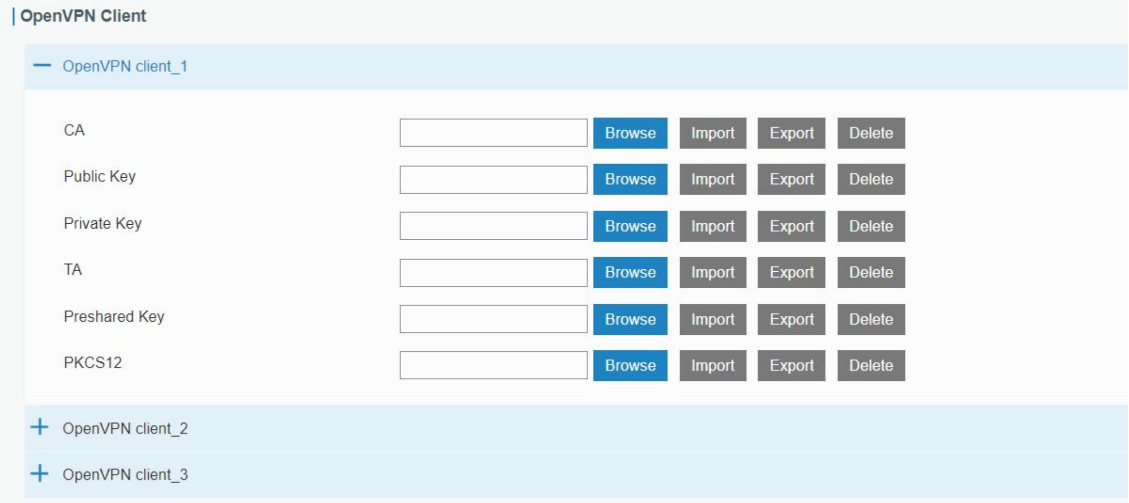
OpenVPN Server	
Item	**Description**
Enable	Enable/disable OpenVPN server.
Protocol	Select a transport protocol used by connection from UDP and TCP.
Port	Enter the TCP/UCP service number for OpenVPN client connection. Range: 1-65535.
Listening IP	Enter the local hostname or IP address for bind. If left blank, OpenVPN server will bind to all interfaces.
Interface	Select virtual VPN network interface type from TUN and TAP. TUN devices encapsulate IPv4 or IPv6 (OSI Layer 3) while TAP devices encapsulate Ethernet 802.3 (OSI Layer 2).
Authentication	Select authentication type used to secure data sessions. **Pre-shared:** use the same secret key as server to complete the authentication. After selecting, go to **Network > VPN >**

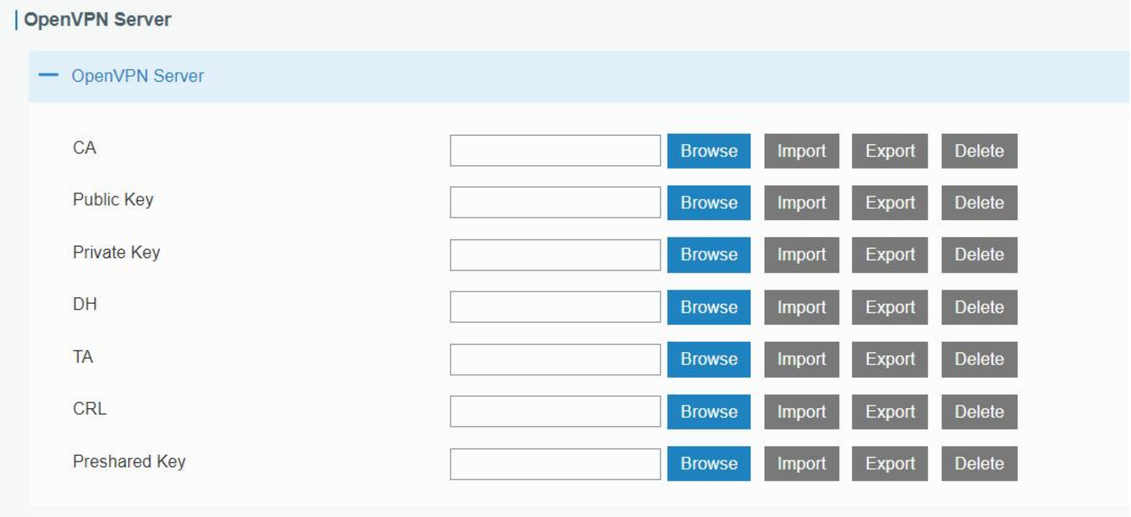
	Certifications page to import a static.key to **PSK** field. **Username/Password:** use username/password which is preset in server side to complete the authentication. **X.509 cert:** use X.509 type certificate to complete the authentication. After selecting, go to **Network > VPN > Certifications** page to import CA certificate, client certificate and client private key to corresponding fields. **X.509 cert + user:** use both username/password and X.509 cert authentication type.
Local Virtual IP	Set local tunnel address when authentication type is **None** or **Pre-shared**.
Remote Virtual IP	Set remote tunnel address when authentication type is **None** or **Pre-shared**.
Client Subnet	Define an IP address pool for openVPN client.
Client Netmask	Set the client subnet netmask to limit the IP address range.
Renegotiation Interval(s)	Renegotiate data channel key after this interval. 0 means disable. Range: 0-86400.
Max Clients	Maximum OpenVPN client number. Range: 1-128.
Enable TLS Authentication	Disable or enable TLS authentication when authentication type is X.509 cert. After being enabled, go to **Network > VPN > Certifications** page to import a ta.key to **TA** field. Note: this option only supports tls-auth. For tls-crypt, please add this format string on expert option: tls-crypt /etc/openvpn/openvpn-client1-ta.key
Enable CRL	Enable or disable CRL verify.
Enable Client to Client	When enabled, openVPN clients can communicate with each other.
Enable Dup Client	Allow multiple clients to connect with the same common name or certification.
Enable NAT	Check to enable the NAT traversal function.
Compression	Select LZO to compress data.
Link Detection Interval (s)	Set link detection interval time to ensure tunnel connection. If this is set on both server and client, the value pushed from server will override the client local values. Range: 10-1800 s.
Link Detection Timeout (s)	OpenVPN will be reestablished after timeout. If this is set on both server and client, the value pushed from server will override the client local values. Range: 60-3600 s.
Cipher	Select from NONE, BF-CBC, DES-CBC, DES-EDE3-CBC, AES-128-CBC, AES-192-CBC and AES-256-CBC.
MTU	Enter the maximum transmission unit. Range: 64-1500.
Max Frame Size	Set the maximum frame size. Range: 64-1500.
Verbose Level	Select from ERROR, WARING, NOTICE and DEBUG.
Expert Options	User can enter some initialization strings in this field and

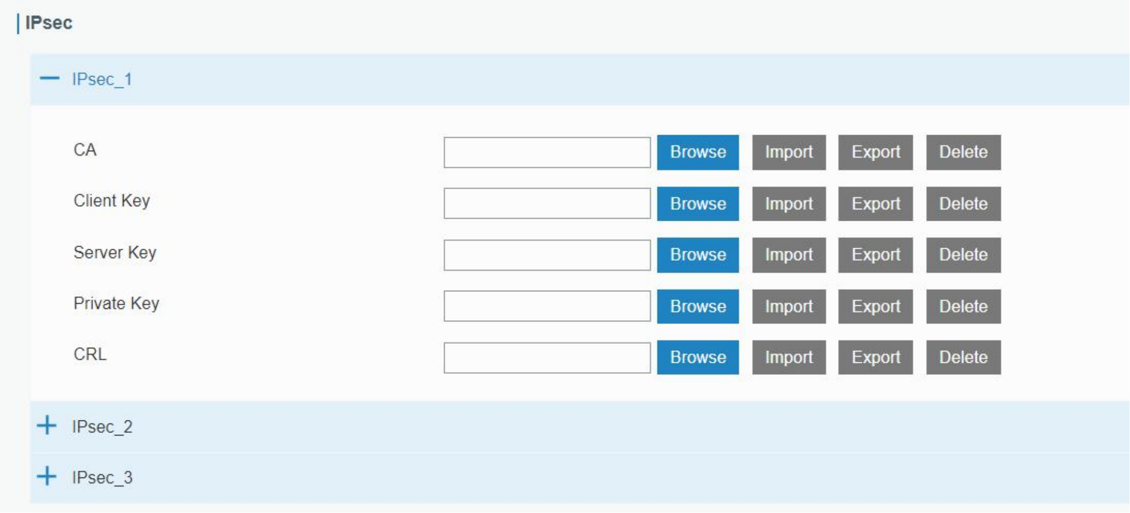
	separate the strings with semicolon. **Example:** auth SHA256; key direction 1
Local Route	
Subnet	The real local IP address of OpenVPN client.
Netmask	The real local netmask of OpenVPN client.
Account	
Username & Password	Set username and password for OpenVPN client when authentication type is username/password.
Client Subnet	
Name	Set the name as OpenVPN client certificate common name.
Subnet	Set the subnet of OpenVPN client.
Subnet Mask	Set the subnet netmask of OpenVPN client.

6.2.6.8 Certifications

When working as OpenVPN server, OpenVPN client or IPsec Server, user can import/export necessary certificate and key files to this page according to the authentication types.







IPsec

— IPsec_1

CA		Browse	Import	Export	Delete
Client Key		Browse	Import	Export	Delete
Server Key		Browse	Import	Export	Delete
Private Key		Browse	Import	Export	Delete
CRL		Browse	Import	Export	Delete

+ IPsec_2

+ IPsec_3

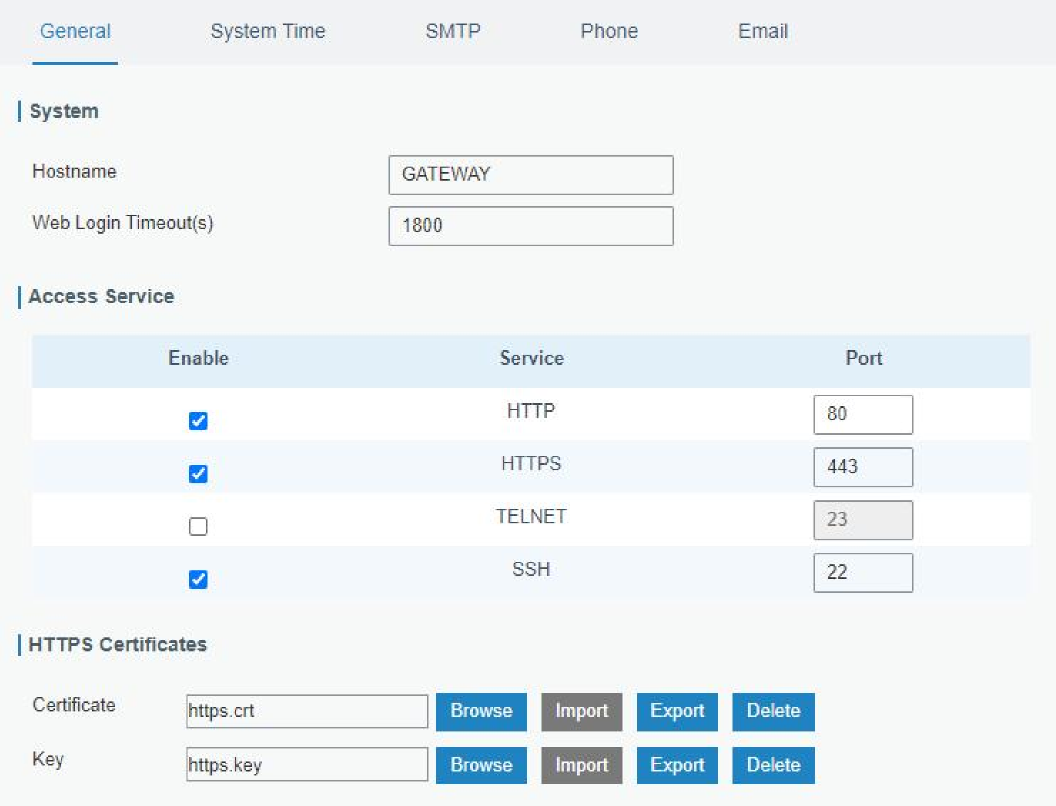
6.3 System

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

6.3.1 General Settings

6.3.1.1 General

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



System

Hostname: GATEWAY

Web Login Timeout(s): 1800

Access Service

Enable	Service	Port
☑	HTTP	80
☑	HTTPS	443
□	TELNET	23
☑	SSH	22

HTTPS Certificates

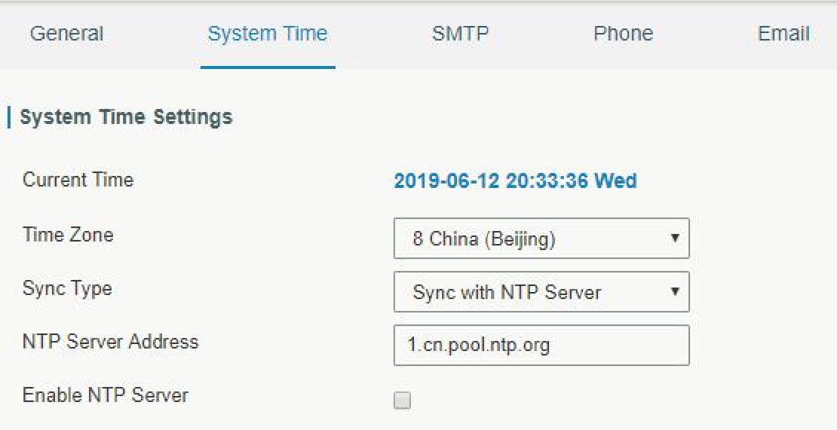
Certificate	https.crt	Browse	Import	Export	Delete
Key	https.key	Browse	Import	Export	Delete

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.	--

6.3.1.2 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.



System Time Settings

Current Time 2019-06-12 20:33:36 Wed

Time Zone 8 China (Beijing)

Sync Type Sync with NTP Server

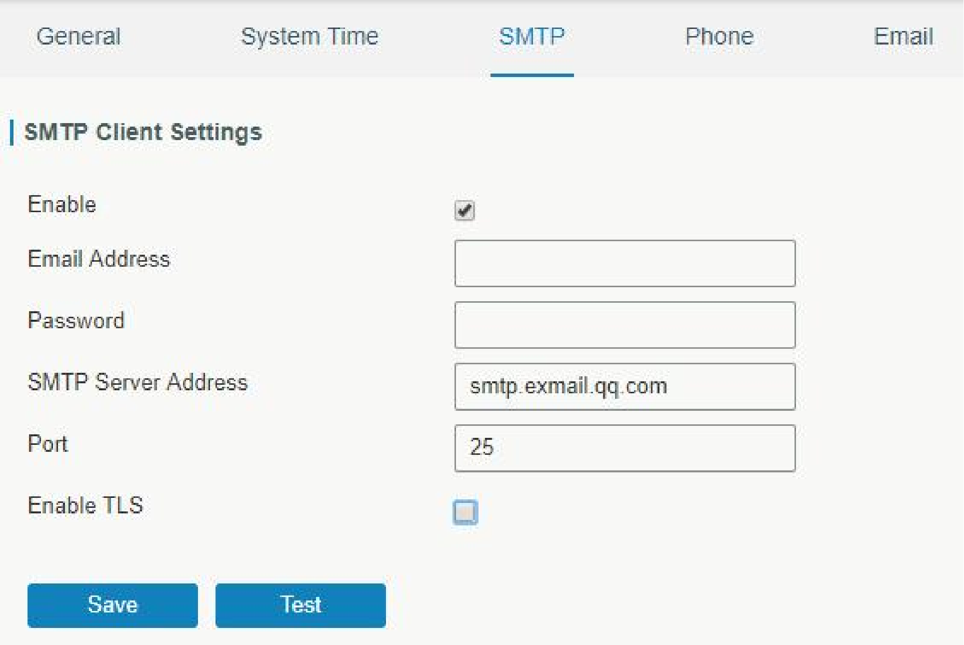
NTP Server Address 1.cn.pool.ntp.org

Enable NTP Server □

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. **Sync with NTP Server:** Synchronize time with NTP Server. **Set up Manually:** configure the time manually.
Sync with NTP Server	
NTP Server Address	Set NTP server address (domain name/IP).
Enable NTP Server	After checked, NTP client on the network can achieve time synchronization with gateway.

6.3.1.3 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 the gateway to work as a SMTP client to send emails.



SMTP Client Settings

Enable	☑
Email Address	
Password	
SMTP Server Address	smtp.exmail.qq.com
Port	25
Enable TLS	□

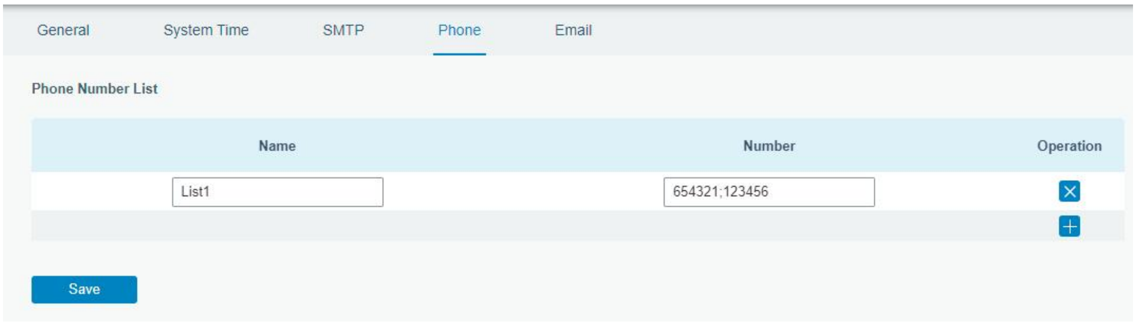
SMTP	
Item	**Description**
SMTP Client Settings	
Enable	Enable or disable SMTP client function.
Email Address	Enter the sender's email account.
Password	Enter the sender's email password.
SMTP Server Address	Enter SMTP server's domain name.
Port	Enter SMTP server port. Range: 1-65535.
Enable TLS	Enable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

Related Topics

Events Setting

6.3.1.4 Phone

Phone settings involve in call/SMS trigger and SMS alarm for events. This is only applied to gateway with cellular feature.



Phone Number List

Name	Number	Operation
List1	654321;123456	☒
		⊞

Phone	
Item	**Description**

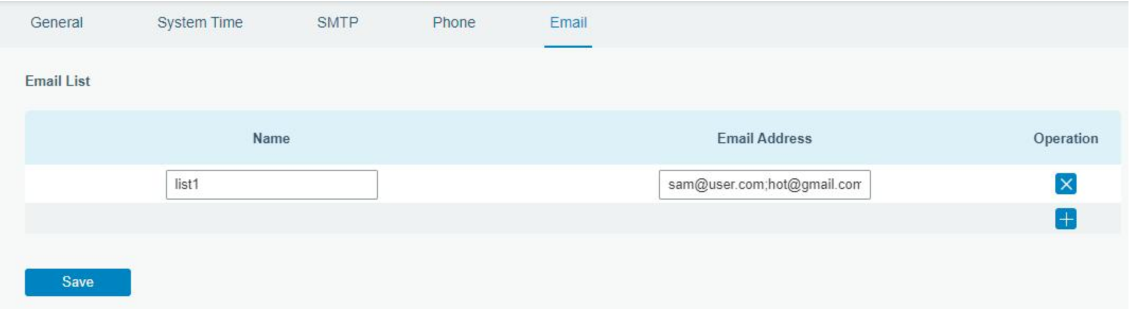
Phone Number List	
Name	Set phone group name.
Number	Enter the telephone number. Digits, "+" and "-" are allowed. You can divide multiple numbers by “;”.

Related Topic

Connect on Demand

6.3.1.5 Email

Email settings involve email alarm for events.



Email List

Name	Email Address	Operation
list1	sam@user.com;hot@gmail.com	☒
		⊞

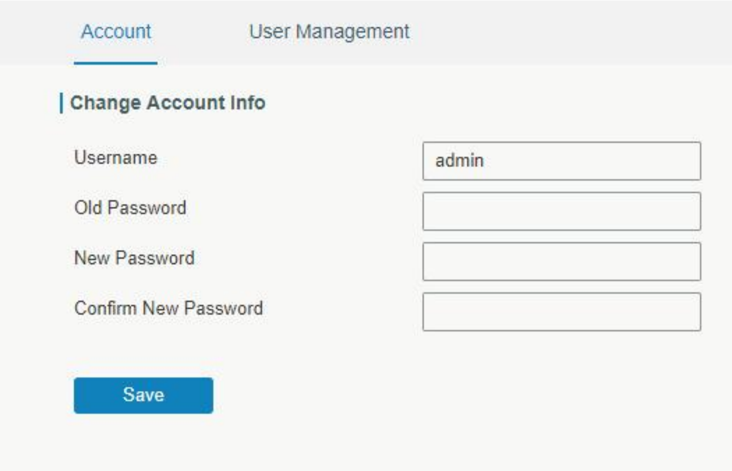
Email	
Item	**Description**
Email List	
Name	Set Email group name.
Email Address	Enter the Email address. You can divide multiple Email addresses by “;”.

6.3.2 User Management

6.3.2.1 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.



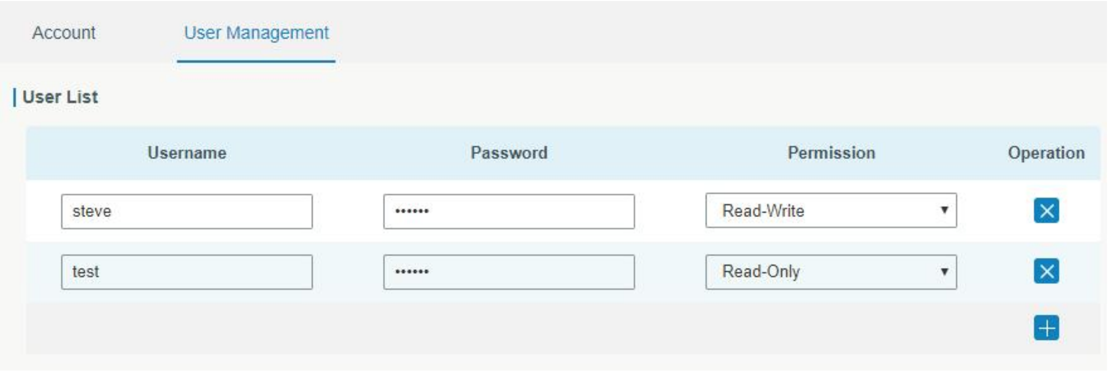
Change Account Info

Username	admin
Old Password	
New Password	
Confirm New Password	

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.

6.3.2.2 User Management

This section describes how to create common user accounts.
The common user permission includes Read-Only and Read-Write.



User List

Username	Password	Permission	Operation
steve	••••••	Read-Write	☒
test	••••••	Read-Only	☒
			⊞

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”. - 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.

6.3.3 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.

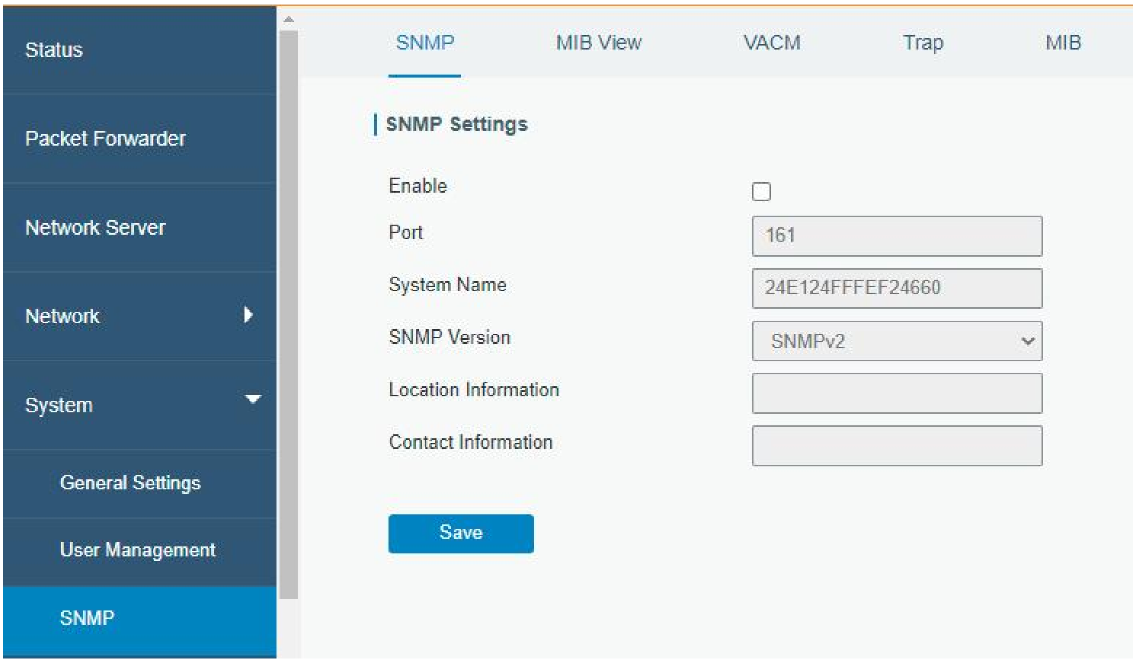
Configuration steps are listed as below for achieving query from NMS:

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

4. Configure VCAM.

6.3.3.1 SNMP

HL31 supports SNMPv1, SNMPv2c and SNMPv3 version. SNMPv1 and SNMPv2c employ community name authentication. SNMPv3 employs authentication encryption by username and password.



SNMP Settings

Enable □

Port 161

System Name 24E124FFFEF24660

SNMP Version SNMPv2

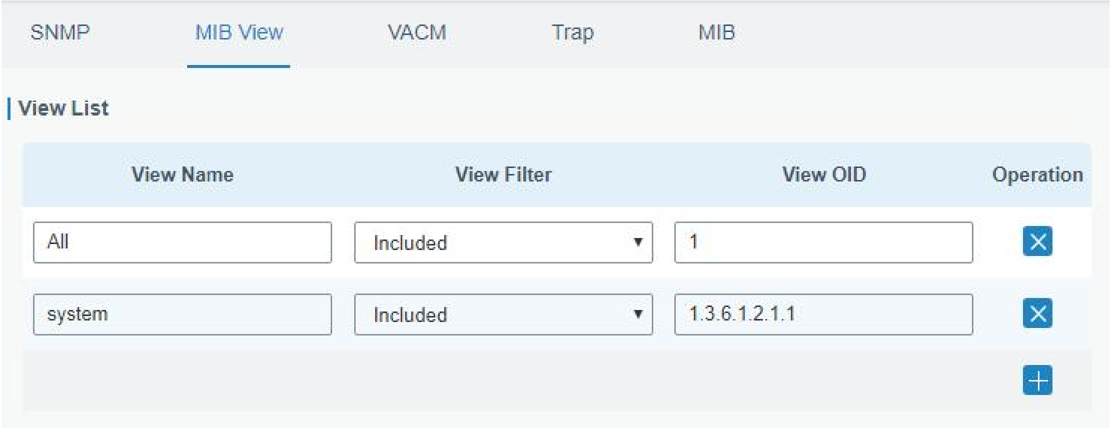
Location Information

Contact Information

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

6.3.3.2 MIB View

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



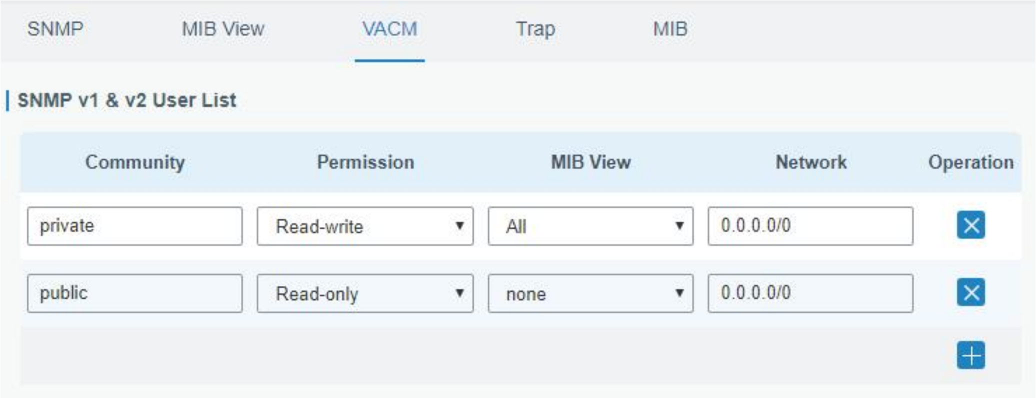
View List

View Name	View Filter	View OID	Operation
All	Included	1	☒
system	Included	1.3.6.1.2.1.1	☒
			⊞

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.

6.3.3.3 VACM

This section describes how to configure VCAM parameters.



SNMP v1 & v2 User List

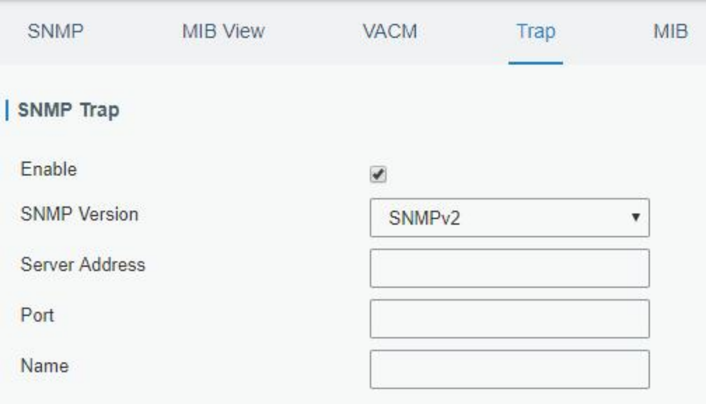
Community	Permission	MIB View	Network	Operation
private	Read-write	All	0.0.0.0/0	☒
public	Read-only	none	0.0.0.0/0	☒
				⊞

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.

6.3.3.4 Trap

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



SNMP Trap

Enable ☑

SNMP Version: SNMPv2

Server Address

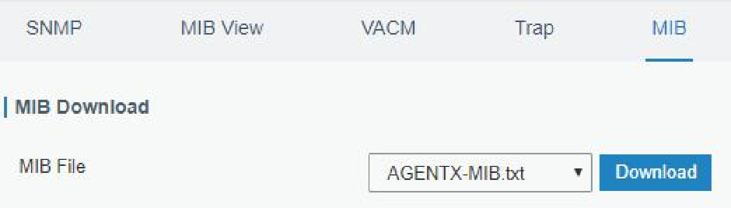
Port

Name

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".

6.3.6.3 MIB

This section describes how to download MIB files.



MIB Download

MIB File: AGENTX-MIB.txt

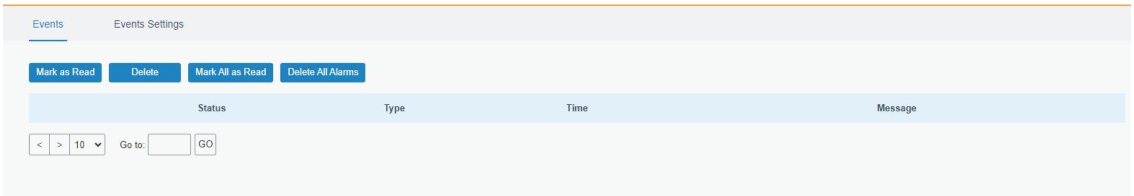
MIB	
Item	**Description**
MIB File	Select the MIB file you need.
Download	Download the MIB file to PC.

6.3.5 Events

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

6.3.5.1 Events

You can view alarm messages on this page.

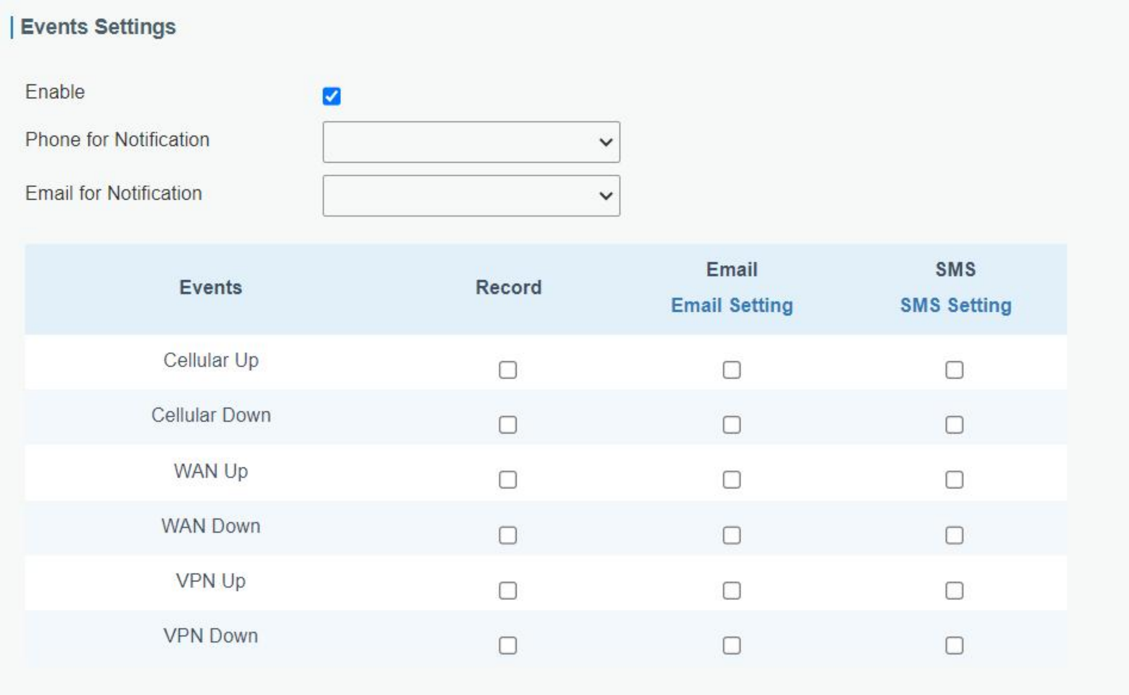


Status	Type	Time	Message

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.

6.3.5.2 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.



Events Settings

Enable	☑
Phone for Notification	
Email for Notification	

Events	Record	Email Email Setting	SMS SMS Setting
Cellular Up	☐	☐	☐
Cellular Down	☐	☐	☐
WAN Up	☐	☐	☐
WAN Down	☐	☐	☐
VPN Up	☐	☐	☐
VPN Down	☐	☐	☐

Event Settings	
Item	**Description**
Enable	Check to enable events settings.
Phone for Notification	Select phone group to receive SMS alarm.
Email for Notification	Select Email group to receive Email alarm.
Events	Event type the gateway supports to record.
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.
SMS	The relevant content of event alarm will be sent out via SMS if this option is checked.
SMS Setting	Click and you will be redirected to the page of "Phone" to configure phone group list.

Related Topics

Email Setting

Phone Setting

6.4 Maintenance

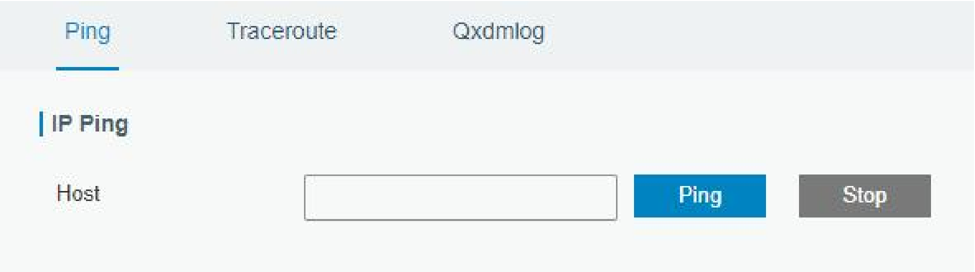
This section describes system maintenance tools and management.

6.4.1 Tools

Troubleshooting tools includes ping and traceroute.

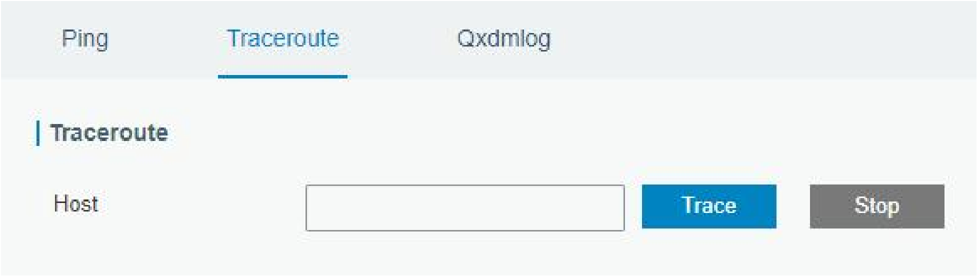
6.4.1.1 Ping

Ping tool is engineered to ping IP address or domain name of outer network.



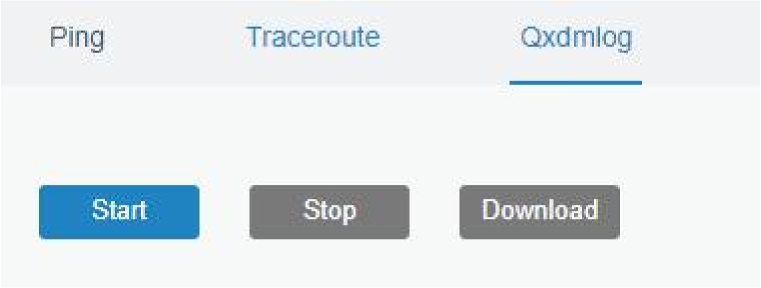
6.4.1.2 Traceroute

Traceroute tool is used for troubleshooting network routing failures.



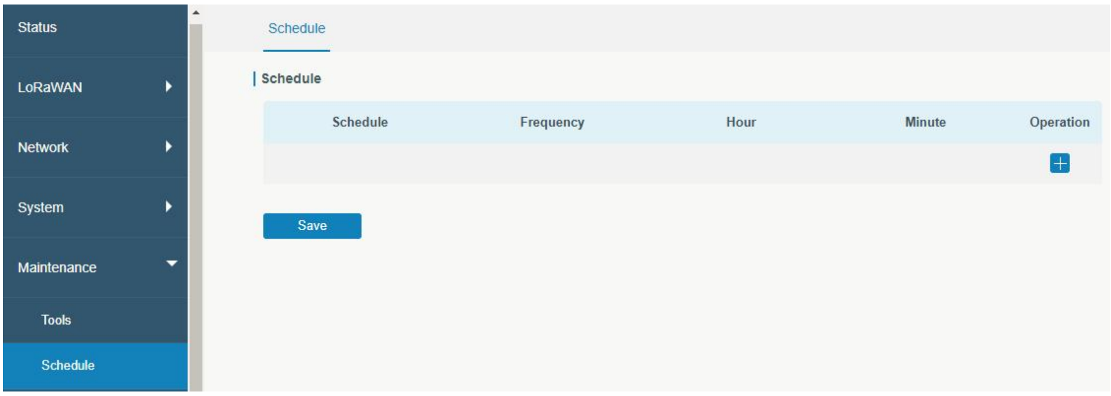
6.4.1.3 Qxdmlog

This section allow collecting diagnostic logs of cellular module via QXDM tool.



6.4.2 Schedule

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



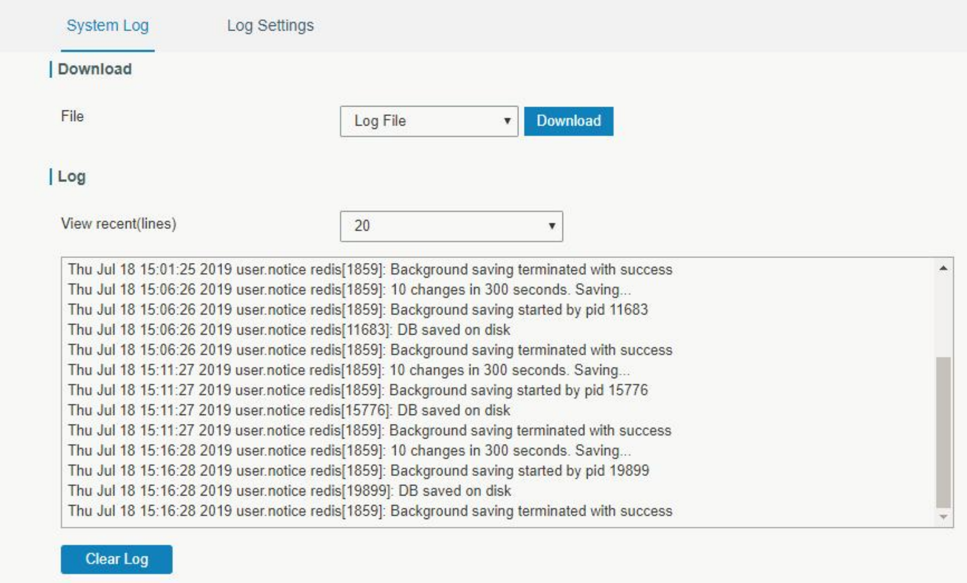
Schedule	
Item	**Description**
Schedule	Select schedule event: Reboot: Reboot the gateway regularly.
Frequency	Select the frequency to execute the schedule.
Hour & Minute	Select the time to execute the schedule.

6.4.3 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.

6.4.3.1 System Log

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



File: Log File

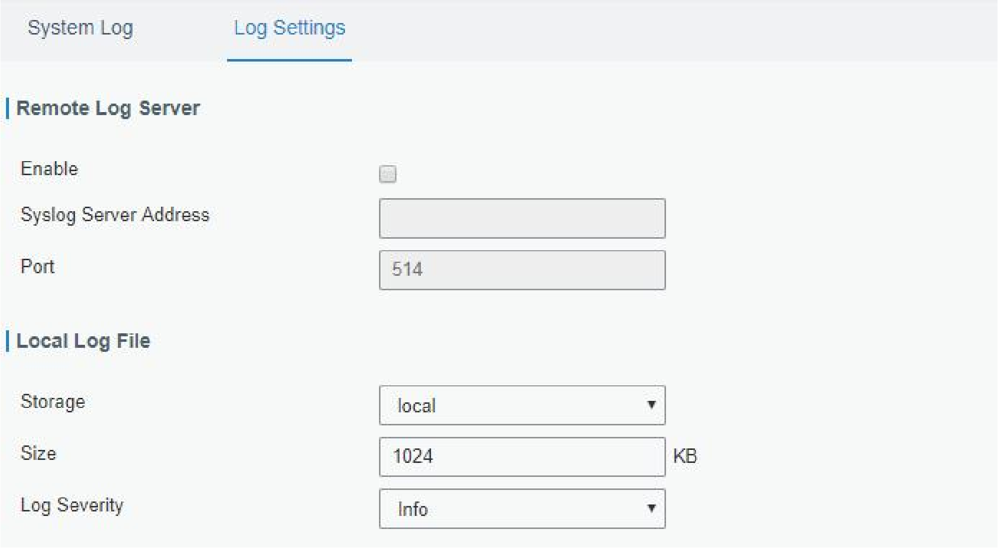
View recent(lines): 20

```
Thu Jul 18 15:01:25 2019 user.notice redis[1859]: Background saving terminated with success
Thu Jul 18 15:06:26 2019 user.notice redis[1859]: 10 changes in 300 seconds. Saving...
Thu Jul 18 15:06:26 2019 user.notice redis[1859]: Background saving started by pid 11683
Thu Jul 18 15:06:26 2019 user.notice redis[11683]: DB saved on disk
Thu Jul 18 15:06:26 2019 user.notice redis[1859]: Background saving terminated with success
Thu Jul 18 15:11:27 2019 user.notice redis[1859]: 10 changes in 300 seconds. Saving...
Thu Jul 18 15:11:27 2019 user.notice redis[1859]: Background saving started by pid 15776
Thu Jul 18 15:11:27 2019 user.notice redis[15776]: DB saved on disk
Thu Jul 18 15:11:27 2019 user.notice redis[1859]: Background saving terminated with success
Thu Jul 18 15:16:28 2019 user.notice redis[1859]: 10 changes in 300 seconds. Saving...
Thu Jul 18 15:16:28 2019 user.notice redis[1859]: Background saving started by pid 19899
Thu Jul 18 15:16:28 2019 user.notice redis[19899]: DB saved on disk
Thu Jul 18 15:16:28 2019 user.notice redis[1859]: Background saving terminated with success
```

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.

6.4.3.2 Log Settings

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



Enable: □

Syslog Server Address:

Port: 514

Storage: local

Size: 1024 KB

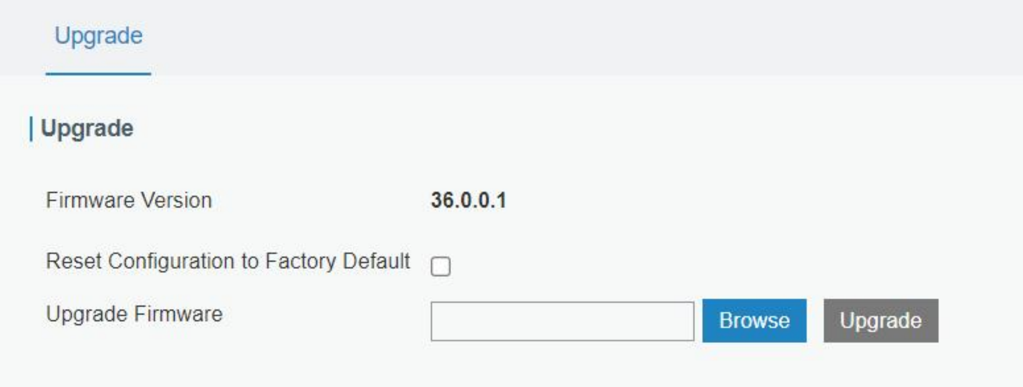
Log Severity: Info

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.

6.4.4 Upgrade

This section describes how to upgrade the gateway firmware via web. 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.



Upgrade

Firmware Version 36.0.0.1

Reset Configuration to Factory Default □

Upgrade Firmware

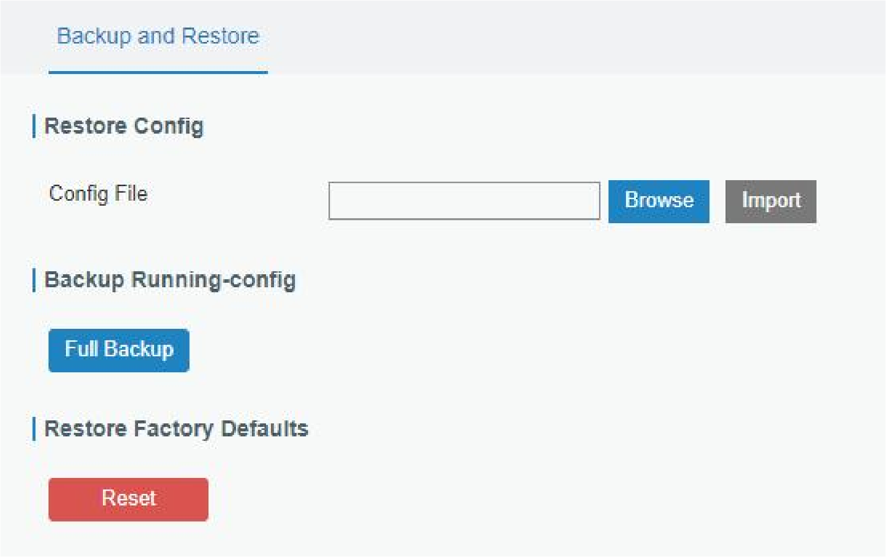
Upgrade	
Item	**Description**
Firmware Version	Show the current firmware version.
Reset Configuration to Factory Default	When this option is checked, the gateway will be reset to factory defaults after upgrade.
Upgrade Firmware	Click "Browse" button to select the new firmware file, and click "Upgrade"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

Related Configuration Example

Firmware Upgrade

6.4.5 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.



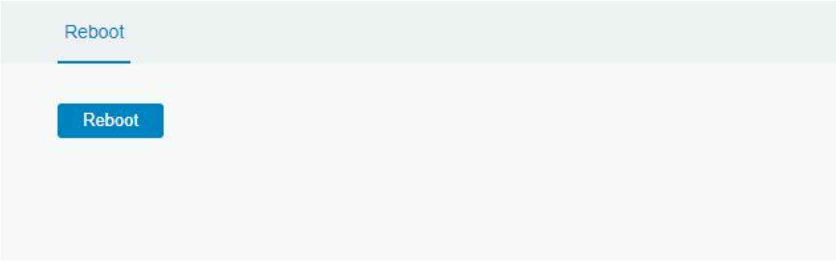
Backup and Restore	
Item	**Description**
Config File	Click "Browse" button to select configuration file, and then click "Import" button to upload the configuration file to the gateway.
Full Backup	Click "Full Backup" to export the current configuration file to the PC.
Reset	Click "Reset" button to reset factory default settings. gateway will restart after reset process is done.

Related Configuration Example

Restore Factory Defaults

6.4.6 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.



[END]