Milesight

5G CPE
UF51

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.
- To avoid risk of fire and electric shock, do keep the product away from rain and moisture before installation.
- In outdoor applications, please install the device under thunder lightning rod and add lightning arrseters.
- Do not place the device where the temperature or humidity is below/above the operating range.
- The device must never be subjected to drops, shocks or impacts.
- Make sure the device is firmly fixed when installing.
- Make sure the plug is firmly inserted into the power socket.

Declaration of Conformity

UF51 is in conformity with the essential requirements and other relevant provisions of the CE and RoHS.

CE 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
Jan. 19, 2023	V 2.0	Initial version
Apr. 20, 2024	V 2.1	1. Add Node-RED, DDNS, IP Passthrough, SMS, SNMP feature 2. Rename Modbus Master as Modbus Client 3. Support customized cellular MTU, IMS and SMS center number 4. Add NAT option on WAN and cellular interfaces 5. Support to customize AT debug command 6. Support hard reset
Sept. 20, 2024	V 2.2	1. Add WLAN client mode and support to configure WLAN country code; 2. Add WLAN status page; 3. Add MQTT, event alarm and multi-user features; 4. Adjust the System menu.

Contents

Chapter 1 Product Introduction 7

1.1 Overview 7

1.2 Advantages 7

Chapter 2 Hardware Introduction 9

2.1 Packing List 9

2.2 Hardware Overview 9

2.3 Serial & IO & Power Pinouts 10

2.4 LED Indicators 10

2.5 Dimensions (mm) 11

2.6 Reset Button 11

Chapter 3 Power Supply 11

Chapter 4 Hardware Installation 12

4.1 SIM Installation 12

4.2 Waterproof Cover & Ethernet Cable Installation 12

4.3 Device Installation 13

4.3.1 Desktop 13

4.3.2 Wall Mounting 14

4.3.3 Pole Mounting 14

Chapter 5 Access to Web GUI 15

Chapter 6 Application Examples 17

6.1 Configure Cellular Connection 17

6.2 Configure Ethernet Connection 19

6.3 Configure Wi-Fi Access Point 21

6.4 Configure OpenVPN Client 22

6.5 Configure NAT Rule 24

6.6 Restore Factory Defaults 25

6.7 Firmware Upgrade 26

Chapter 7 Web Configuration 27

7.1 Status 27

7.1.1 Overview 27

7.1.2 Cellular 29

7.1.3 WLAN (Wi-Fi Version Only) 32

7.1.4 GPS 33

7.1.5 Firewall 34

7.1.6 Routing Table 35

7.1.7 VPN 36

7.2 Network 36

7.2.1 Interfaces 36

7.2.1.1 WAN 37

7.2.1.2 LAN/DHCP Server 40

7.2.1.3 Cellular 43

7.2.1.4 Interface Settings 44

7.2.1.5 Link Failover 44
7.2.1.6 Static IP Address Assignment 46
7.2.2 WLAN (Wi-Fi Version Only) 47
7.2.2.1 WLAN 47
7.2.2.2 Advanced Settings 49
7.2.3 Firewall 50
7.2.3.1 General Settings 50
7.2.3.2 ACL 51
7.2.3.3 Port Mapping (DNAT) 52
7.2.3.4 DMZ 53
7.2.3.5 Custom Rules 54
7.2.3.6 Certificates 54
7.2.4 Static Routes 54
7.2.5 IP Passthrough 55
7.2.6 DDNS 55
7.2.7 Diagnostics 56
7.3 VPN 57
7.3.1 OpenVPN 57
7.3.1.1 OpenVPN Server 57
7.3.1.2 OpenVPN Client 60
7.3.1.3 Certificate 63
7.3.2 IPsecVPN 64
7.3.2.1 IPSec Server 64
7.3.2.2 IPSec Client 66
7.3.2.3 Certificate 69
7.3.3 L2TP 70
7.3.4 PPTP 72
7.4 Service 73
7.4.1 Serial Port 73
7.4.2 I/O 77
7.4.2.1 DI 77
7.4.2.2 DO 78
7.4.3 Modbus Client (Master) 79
7.4.3.1 Modbus Client 79
7.4.3.2 Channel 79
7.4.4 GPS 82
7.4.4.1 GPS IP Forwarding 82
7.4.4.2 GPS Serial Forwarding 84
7.4.4.3 GPS MQTT Forwarding 85
7.4.5 Phone&SMS 86
7.4.5.1 Phone 86
7.4.5.2 SMS 87
7.4.6 SNMP 88
7.4.6.1 SNMP 89

7.4.6.2 MIB View 89
7.4.6.3 VACM 90
7.4.6.4 Trap 90
7.4.6.5 MIB Download 91
7.4.7 MQTT 91
7.5 App 94
7.5.1 Node-RED 94
7.6 System 96
7.6.1 Administration 97
7.6.1.1 System Settings 97
7.6.1.2 User Settings 98
7.6.1.3 Multi User Management 98
7.6.2 Maintenance 99
7.6.2.1 Log 99
7.6.2.2 Cellular Debugger 100
7.6.2.3 Firewall Debugger 101
7.6.2.4 Backup/Upgrade 102
7.6.2.5 Reboot 102
7.6.3 Event Alarm 103
7.6.3.1 Event Alarm 103
7.6.3.2 Events Settings 103
7.6.4 Device Management 104
7.6.4.1 Device Management 104
7.6.4.2 Cloud VPN 105

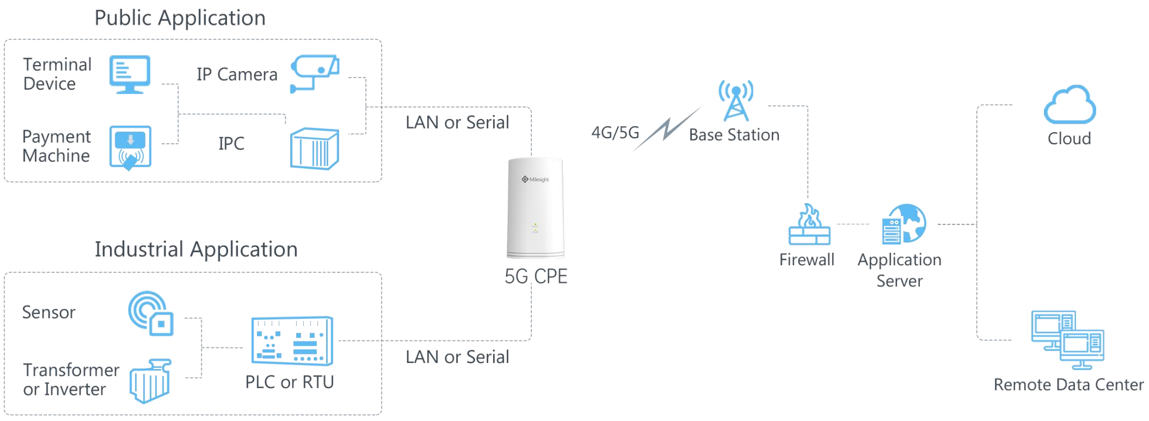
Chapter 1 Product Introduction

1.1 Overview

UF51 5G CPE is dedicated to cost effective solutions for 5G wireless networking applications. Adopting a high-performance and low power consumption industrial platform of quad-core CPU and 5G cellular module, UF51 supports the global WCDMA, 4G LTE, 5G Sub-6 GHz and NSA network and WiFi-6, to provide ultra-fast network to ensure the extremely safe and reliable connection to the wireless network. With IP67 waterproof enclosure, various kinds of installation methods, and authentic design, UF51 is competent to both indoor and outdoor applications.

Meanwhile, UF51 also supports 2-port Gigabit Ethernet switch, RS232/RS485 serial ports and Digital input/Digital output, which enable to scale up M2M applications combining data collection and high-speed transmission in a limited time and budget.

UF51 is particularly suitable for smart offices, video surveillance, digital media implementations, industrial automation, traffic applications, robots and so on.



1.2 Advantages

Ultra Fast Connectivity

- Industrial-grade quad-core CPU ARM Cortex-A55 with big memory, providing high performance for data transmission
- Global 5G (NSA/SA)/4G LTE network
- Dual carrier aggregation (2CC CA) is supported in the 5G Sub-6GHz, enabling wider signal coverage with superb download speed up to 4.67 Gbps
- Plug& play, supply lightning transmission via Gigabit Ethernet ports or USB Type-C interface

- Support Wi-Fi 6, allows 2.4G & 5G dual band concurrent connections up to 3.6 Gbps download speed
- Embedded eight 5G antennas and four Wi-Fi antennas for best signal reception

Security & Reliability

- Automated failover/failback backup via Ethernet, Cellular and Wi-Fi
- Secure transmission with VPN tunnels like IPsec/OpenVPN/L2TP/PPTP
- Embedded with hardware watchdog to automatically recover from various failures, ensuring the highest level of availability
- Equipped with multiple security protection measures such as ACL, DMZ, SYN-Flood protection, and data filtering to ensure that the network is secured
- Support policy routing and NAT for more secure intranet access

Easy Maintenance

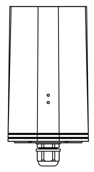
- Milesight DeviceHub provides easy setup, mass configuration, and centralized management of remote devices
- The user-friendly web interface design and several upgrade options help administrator to manage the device easily
- Support multilevel user authorities for security management
- Fast and user-friendly programming by Node-RED development tool

Industrial-Grade Design

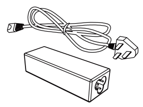
- Equipped with I/O, serial port, and GPS for industrial transmission applications
- Wide operating temperature range from -30°C to 60°C and industrial design for harsh environments
- IP67 waterproof and UV-protective enclosure for outdoor applications
- PoE, DC or USB power supply optional
- Equipped with a vent plug to prevent condensation in the enclosure
- Pole mounting, wall mounting, desktop, bottom screw mounting for various applications
- 3-year warranty included

Chapter 2 Hardware Introduction

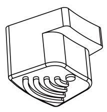
2.1 Packing List



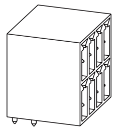
1 ×
UF51 Device



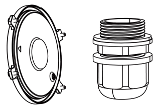
1 ×
Power Adapter



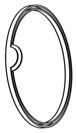
1 × Rubber Feet



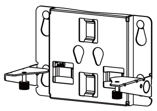
1 × 8-pin Serial & IO &
Power Terminal Block



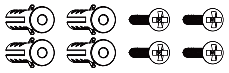
1 × Bottom Cover
with Cable Grand



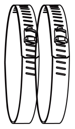
1 × Waterproof
Rubber Ring



1 × Mounting Bracket

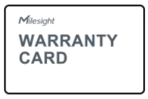


4 × Wall Mounting
Kits



2 × Hose Clamp

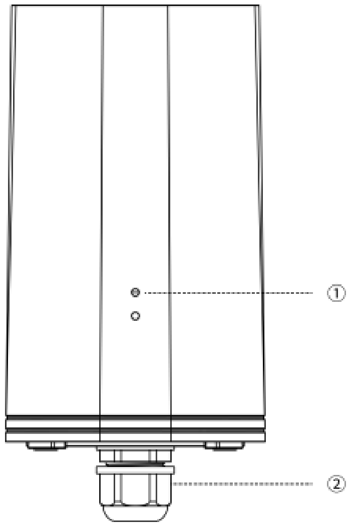
1 × Quick Start Guide



1 × Warranty Card

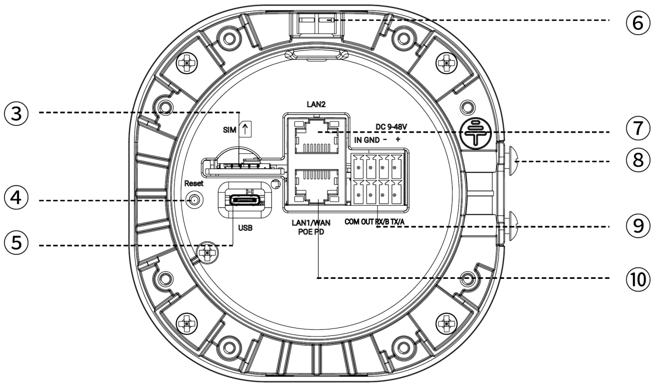
⚠ **If any of the above items is missing or damaged, please contact your sales representative.**

2.2 Hardware Overview



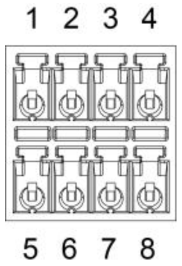
① LED Indicator Area
STATUS: Power & System Indicator
5G: Cellular Indicator

② Waterproof Connector



③ SIM Slot
④ Reset Button
⑤ USB Type-C Port
⑥ Vent Plug
⑦ LAN2 Port
⑧ Bracket Mounting Screws
⑨ Serial & IO Power Interface
⑩ LAN1/WAN Port (PoE PD)

2.3 Serial & IO & Power Pinouts



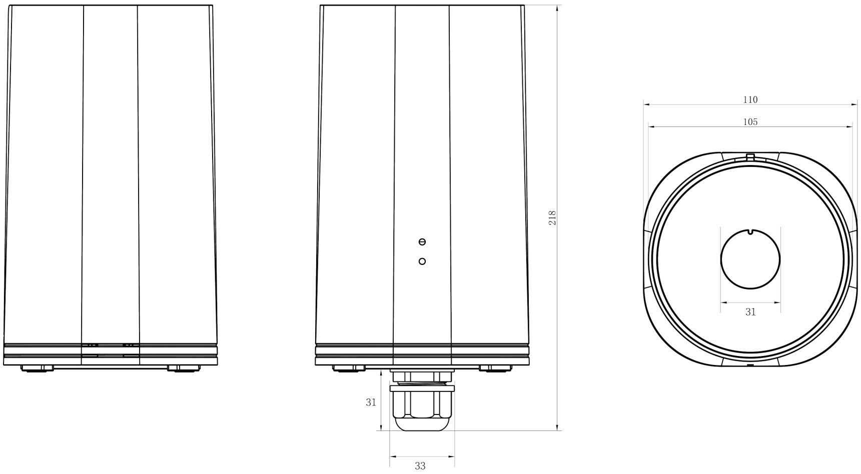
PIN	RS232 /RS485	DI	DO	Power	Description
1	---	IN	---	---	Digital Input
2	GND	GND	---	---	Ground
3	---	---	---	(-)	Negative
4	---	---	---	(+)	Positive (9-48V)
5	---	---	COM	---	Common Ground
6	---	---	OUT	---	Digital Output
7	RXD/B	---	---	---	RS232-RXD RS485-B
8	TXD/A	---	---	---	RS232-TXD RS485-A

2.4 LED Indicators

LED	Indication	Status	Description
STATUS	Power & System Status	Off	The power is switched off
		Orange	Static: The system is booting
		Green	Static: The system is running properly
		Red	Static: The system goes wrong
5G	Cellular Status	Off	SIM card is registering or fails to register (or there are no SIM cards inserted)
		Green	Blinking rapidly: SIM card has been registered and is dialing up now
			Static: SIM card has been registered and dialed up to 5G network
		Orange	Static: SIM card has been registered and dialed up to 4G network

Ethernet Port	Link Indicator (Orange)	Off	Disconnected or connect failure
		On	Connected
		Blinking	Transmitting data
	Rate Indicator (Green)	Off	100 Mbps mode
		On	1000 Mbps mode

2.5 Dimensions (mm)



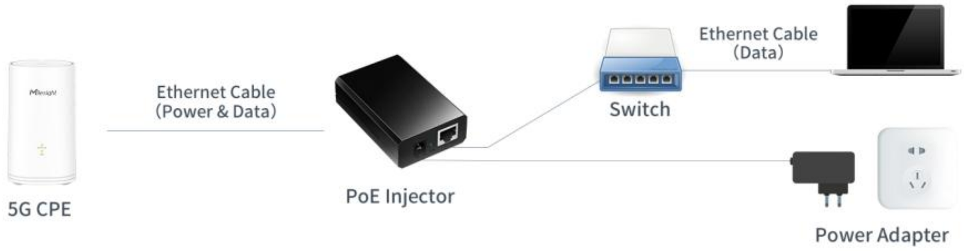
2.6 Reset Button

Function	Description	
	LED Indicator	Action
Soft Reset	Static	When the device is powered on, press and hold the reset button for more than 5 seconds.
	Static →All Blinking	Release the button and wait.
	Off →STATUS Static Green	The device resets to factory default.
Hard Reset	Off	When the device is powered off, press and hold the reset button.
	Static →All Blinking	Power on the device while keeping holding the reset button for more than 5 seconds, then release the button.
	Off →STATUS Static Green	The device resets to factory default.

Chapter 3 Power Supply

UF51 can be powered by 802.3af standard PoE or 9-48V DC. Both power supplies can’t be used at the same time.

PoE Supply: provide power supply via PoE injector as follows. Besides, it can also be powered by PoE switch.

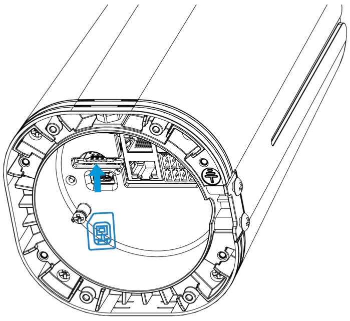


DC Supply: Connect the DC power cable to terminal block, then connect the terminal block to DC interface to power the device.

Chapter 4 Hardware Installation

4.1 SIM Installation

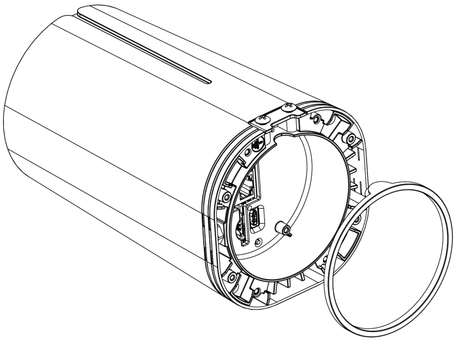
Insert the SIM card into the device according to the direction icon on the device. If you need to take ut the SIM card, press into the SIM card tray and it will pop out automatically.



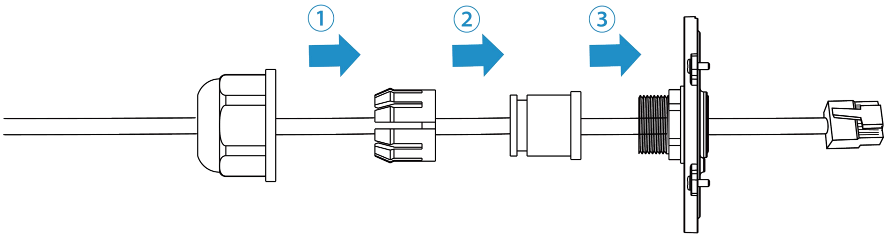
4.2 Waterproof Cover & Ethernet Cable Installation

Please use round Ethernet cable and install as follows if UF51 needs to be placed outdoors:

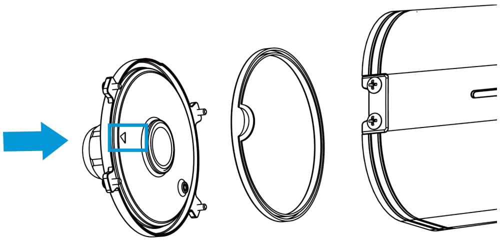
1. Install the rubber ring into the bottom of the device. Note that the round part needs to face the gap of bottom when installing, otherwise it may cause waterlogged.



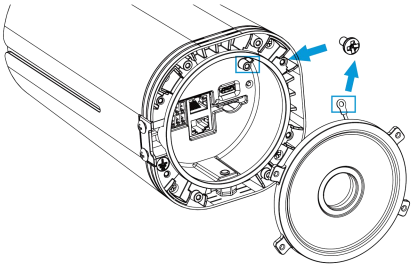
2. Connect a round Ethernet cable to LAN1/WAN port, then pass the Ethernet cable through the bottom cover and all parts of the cable gland.



3. Fix the bottom cover to the bottom of the device with 4 screws. Note the arrow behind the cover need to face the bracket mounting screws.



Note: Bottom cover can be fixed with the device via the wiring behind the cover.



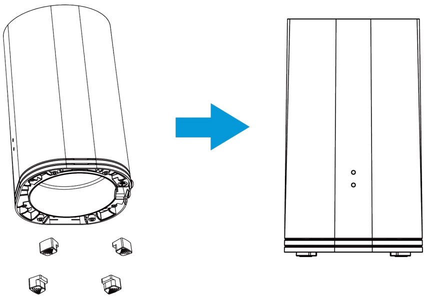
4.3 Device Installation

UF51 supports multiple installation methods like desktop, wall mounting, pole mounting, etc. Before you start, make sure that all fittings have been installed.

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

4.3.1 Desktop

When using indoors, pile 4 rubber feet into the gaps at the bottom of the device. The rough surface of rubber feet should face desktop.



4.3.2 Wall Mounting

Preparation: mounting bracket(with 2 screws), wall plugs, wall mounting screws and other required tools.

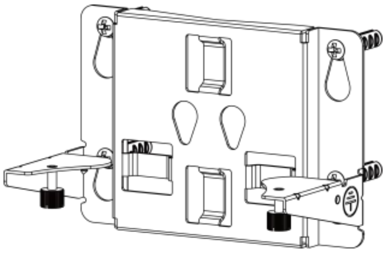
A. Align the mounting bracket horizontally to the desired position on the wall, use a marker pen to mark four mounting holes on the wall, and then remove the mounting bracket from the wall.

Note: The connecting lines of adjacent points are at right angles.

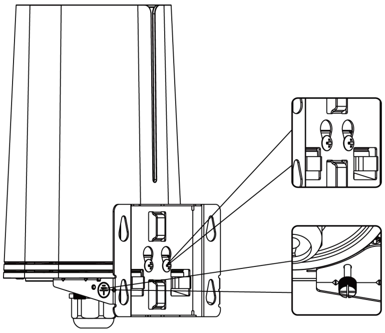
B. Drill four holes with a depth of 32 mm by using your drill with a 6 mm drill bit on the positions you marked previously on the wall.

C. Insert four wall plugs into the holes respectively.

D. Mount the mounting bracket horizontally to the wall by fixing the wall mounting screws into the wall plugs.



E. Hang the device to the mounting bracket via bracket mounting screws on the back of device, then screw the 2 bracket screws to the bottom of the device.



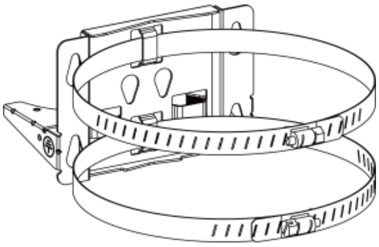
4.3.3 Pole Mounting

Preparation: mounting bracket(with 2 screws), hose clamps and other required tools.

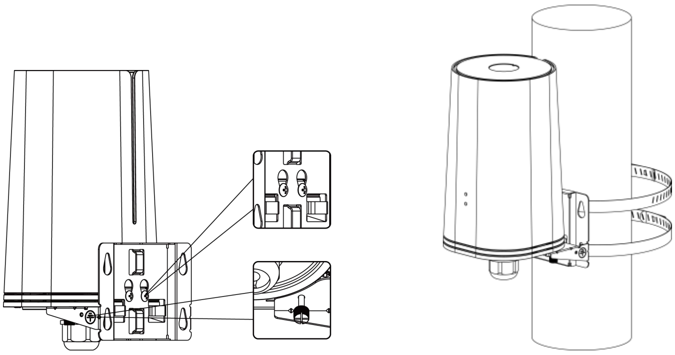
A. Loosen the hose clamp by turning the locking mechanism counter-clockwise.

B. Straighten out the hose clamp and slide it through the rectangular rings in the mounting bracket, wrap the hose clamp around the pole.

C. Use a screwdriver to tighten the locking mechanism by turning it clockwise.



D. Hang the device to the mounting bracket via bracket mounting screws on the back of device, then screw the 2 bracket screws to the bottom of the device.



Chapter 5 Access to Web GUI

UF51 provides user-friendly web GUI for configuration and users can access it via LAN port. This chapter explains how to access to Web GUI of the UF51 device.

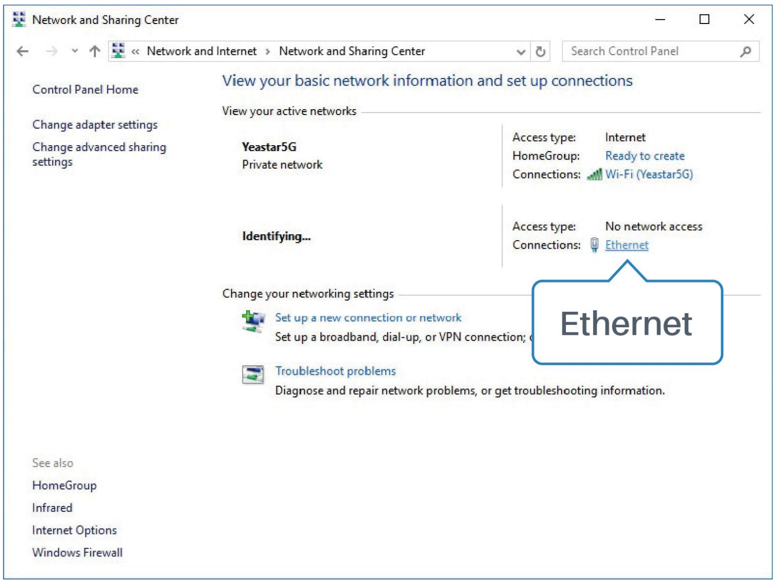
Username: **admin**

Password: **password**

IP Address: **192.168.1.1**

Connect PC to LAN port or USB port of UF51 directly. The following steps are based on Windows 10 operating system for your reference.

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



View your basic network information and set up connections

View your active networks

Yeastar5G
Private network

Access type: Internet
HomeGroup: Ready to create
Connections: Wi-Fi (Yeastar5G)

Identifying...

Access type: No network access
Connections: Ethernet

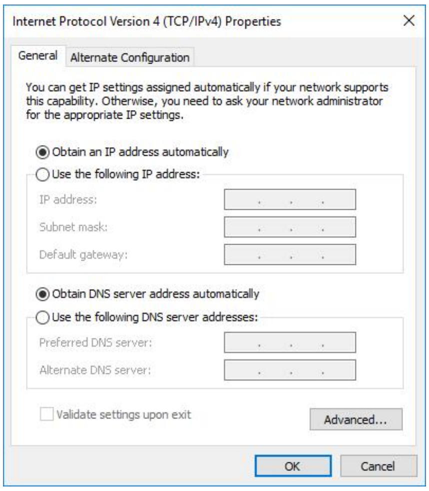
Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection;

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

2. Go to **Properties** → **Internet Protocol Version 4(TCP/IPv4)**, select **Obtain an IP address automatically** or **Use the following IP address**, then assign a static IP manually within the same

subnet of the device.



Internet Protocol Version 4 (TCP/IPv4) Properties

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.

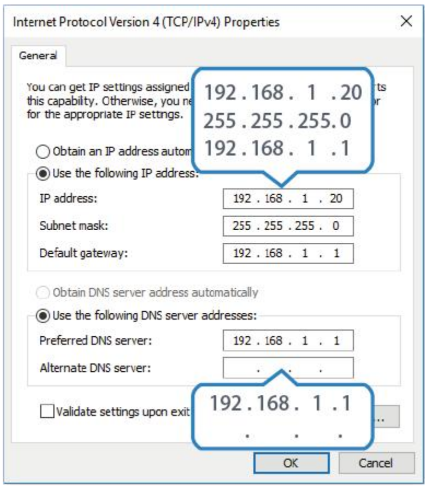
● Obtain an IP address automatically

○ Use the following IP address:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

□ Validate settings upon exit



Internet Protocol Version 4 (TCP/IPv4) Properties

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 20

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

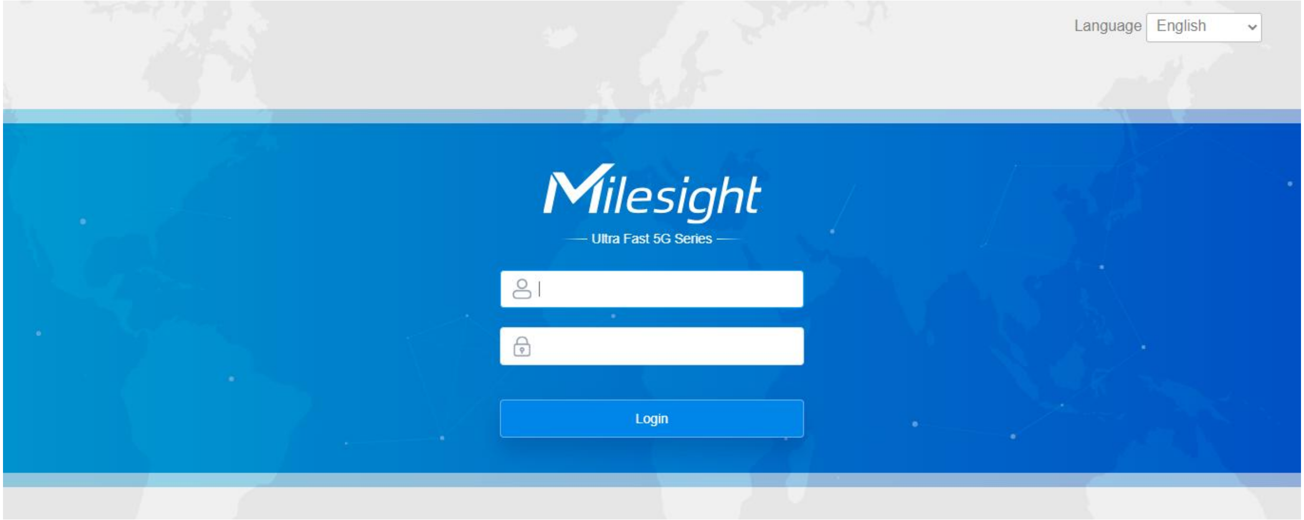
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 1 . 1

Alternate DNS server:

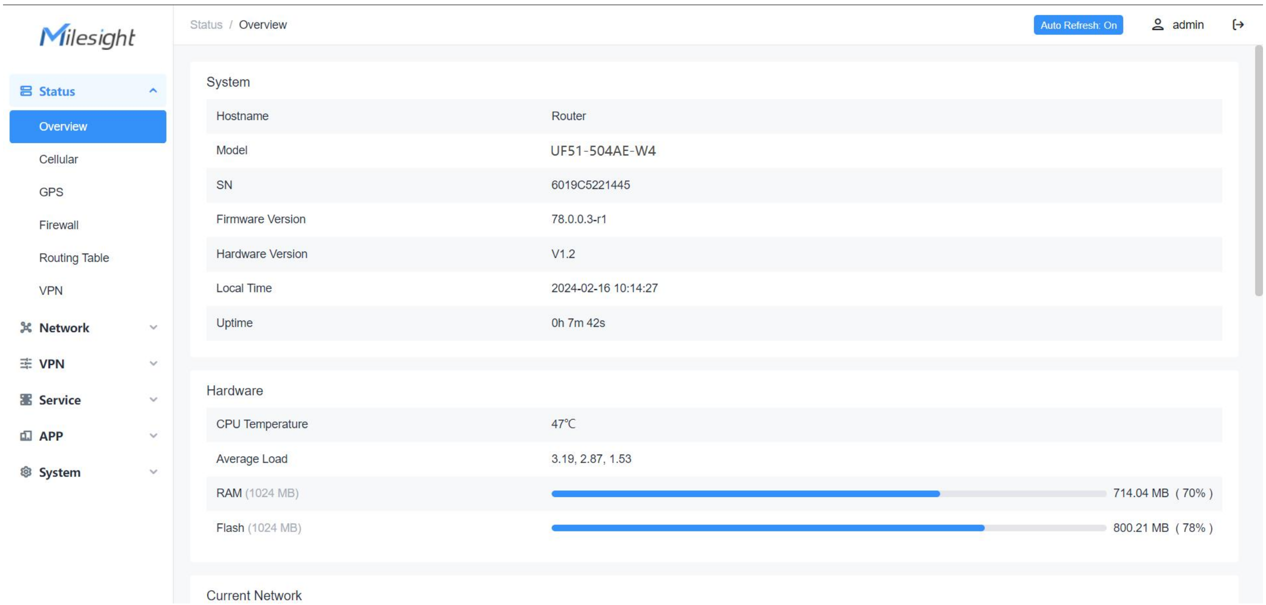
□ Validate settings upon exit

3. Open a Web browser on your PC (Chrome is recommended), type in the IP address 192.168.1.1 to access the web GUI, then enter the default username and password, and 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 you login the Web GUI, you can view system information and perform configuration.



System

Hostname	Router
Model	UF51-504AE-W4
SN	6019C5221445
Firmware Version	78.0.0.3-r1
Hardware Version	V1.2
Local Time	2024-02-16 10:14:27
Uptime	0h 7m 42s

Hardware

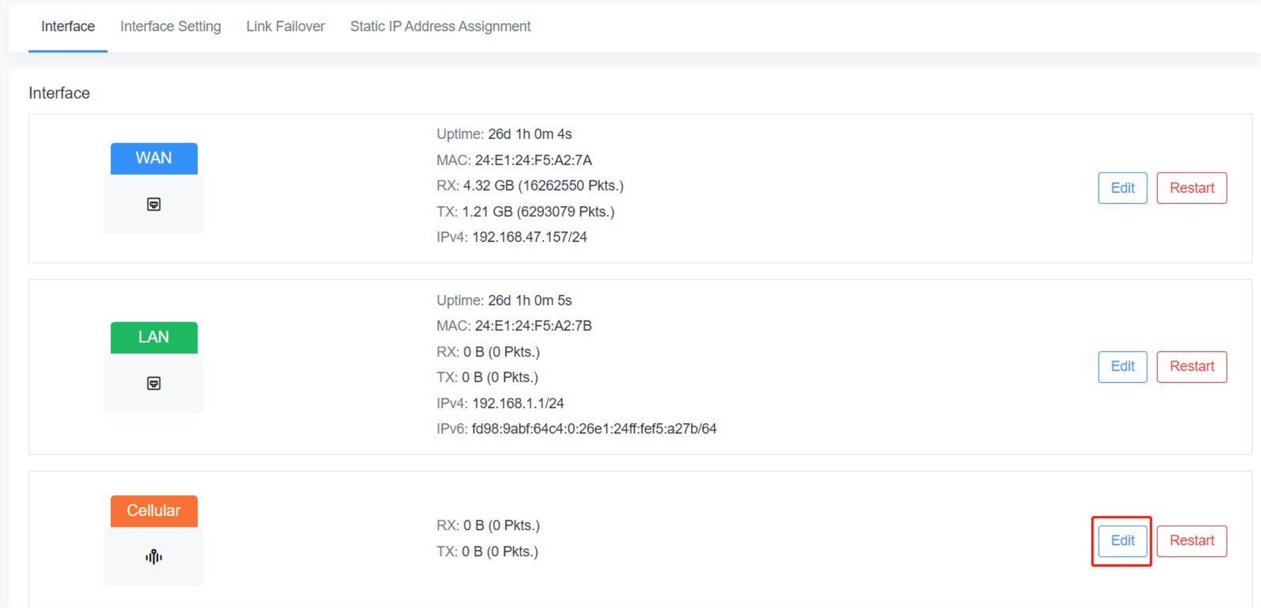
CPU Temperature	47℃
Average Load	3.19, 2.87, 1.53
RAM (1024 MB)	714.04 MB (70%)
Flash (1024 MB)	800.21 MB (78%)

Current Network

Chapter 6 Application Examples

6.1 Configure Cellular Connection

1. Ensure the SIM card is inserted well and all cellular antennas are connected to the correct connectors.
2. Go to **Network > Interface > Interface** page, find the cellular interface and click **Edit** button.

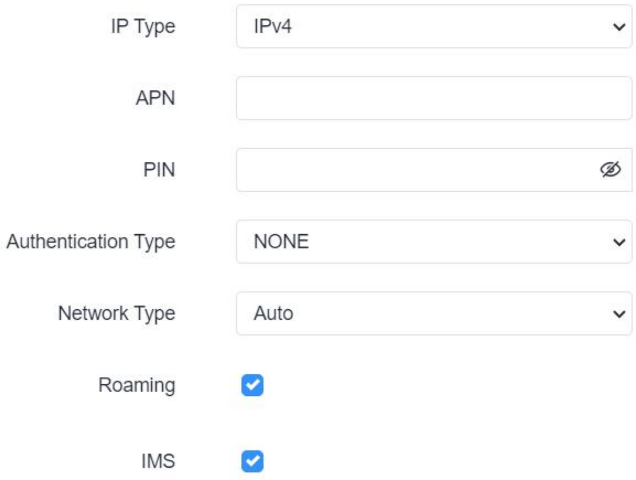


WAN
Uptime: 26d 1h 0m 4s
MAC: 24:E1:24:F5:A2:7A
RX: 4.32 GB (16262550 Pkts.)
TX: 1.21 GB (6293079 Pkts.)
IPv4: 192.168.47.157/24

LAN
Uptime: 26d 1h 0m 5s
MAC: 24:E1:24:F5:A2:7B
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)
IPv4: 192.168.1.1/24
IPv6: fd98:9abf:64c4:0:26e1:24ff:fef5:a27b/64

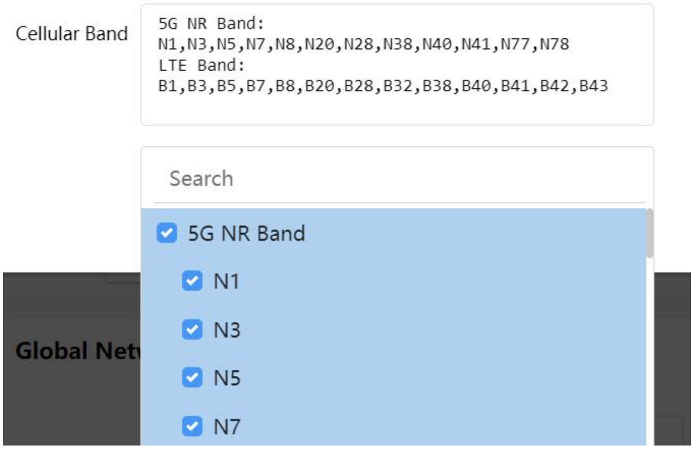
Cellular
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)

3. Fill in the necessary info of SIM card, then save all settings.



IP Type	IPv4
APN	
PIN	
Authentication Type	NONE
Network Type	Auto
Roaming	☑
IMS	☑

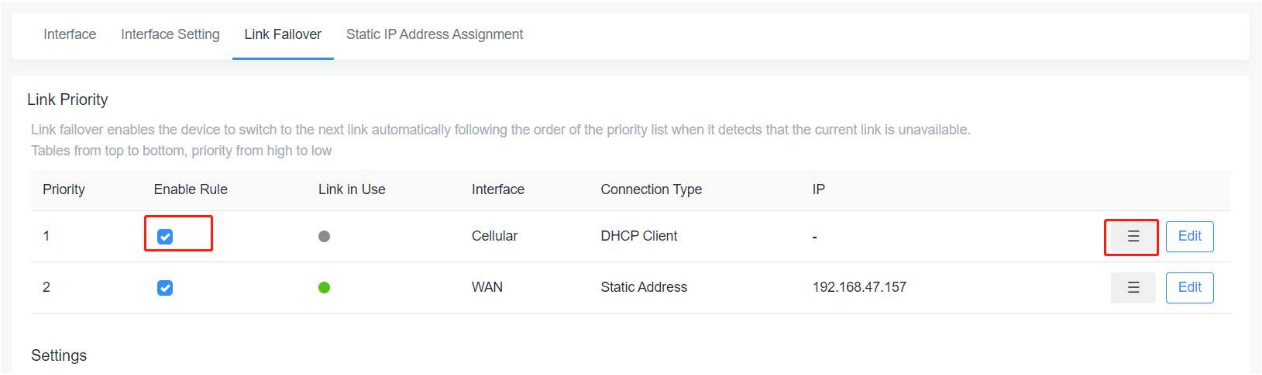
For 5G connection, you can choose specific bands to ensure high network speed.



Cellular Band

```
5G NR Band:
N1,N3,N5,N7,N8,N20,N28,N38,N40,N41,N77,N78
LTE Band:
B1,B3,B5,B7,B8,B20,B28,B32,B38,B40,B41,B42,B43
```

4. Go to **Network > Interface > Link Failover** to enable cellular and drag the buttons to change link priority.



Link Priority

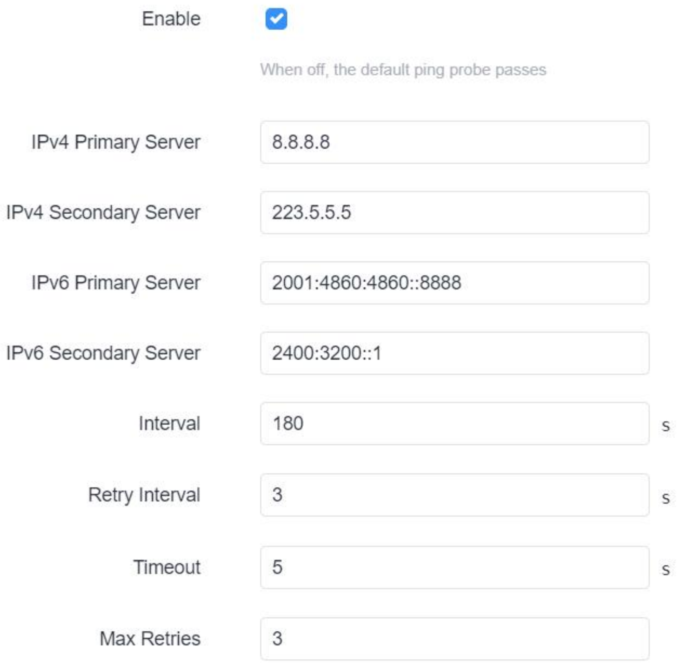
Link failover enables the device to switch to the next link automatically following the order of the priority list when it detects that the current link is unavailable.
Tables from top to bottom, priority from high to low

Priority	Enable Rule	Link in Use	Interface	Connection Type	IP	
1	☑	●	Cellular	DHCP Client	-	☰ Edit
2	☑	●	WAN	Static Address	192.168.47.157	☰ Edit

Settings

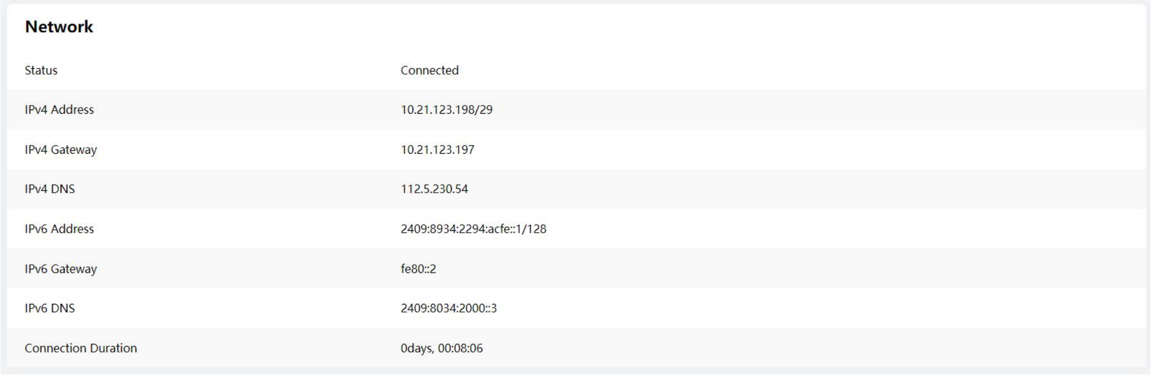
5. Click **Edit** of a link to configure ICMP ping detection information. When ping probe is enabled, the device will send ICMP packets to detection server to check if this link is valid. If no response and exceeding max retries, it will switch to the lower priority link.

Note: if you use private SIM card, please change a private server address or disable the ping probe.



Enable	☑ When off, the default ping probe passes	
IPv4 Primary Server	8.8.8.8	
IPv4 Secondary Server	223.5.5.5	
IPv6 Primary Server	2001:4860:4860::8888	
IPv6 Secondary Server	2400:3200::1	
Interval	180	s
Retry Interval	3	s
Timeout	5	s
Max Retries	3	

6. Go to **Status > Cellular** to check the status of the cellular connection. If modem status is ready and network status shows **Connected**, the SIM has been dialed up successfully.



Network

Status	Connected
IPv4 Address	10.21.123.198/29
IPv4 Gateway	10.21.123.197
IPv4 DNS	112.5.230.54
IPv6 Address	2409:8934:2294:acfe::1/128
IPv6 Gateway	fe80::2
IPv6 DNS	2409:8034:2000::3
Connection Duration	0days, 00:08:06

Related Topic

Cellular Setting

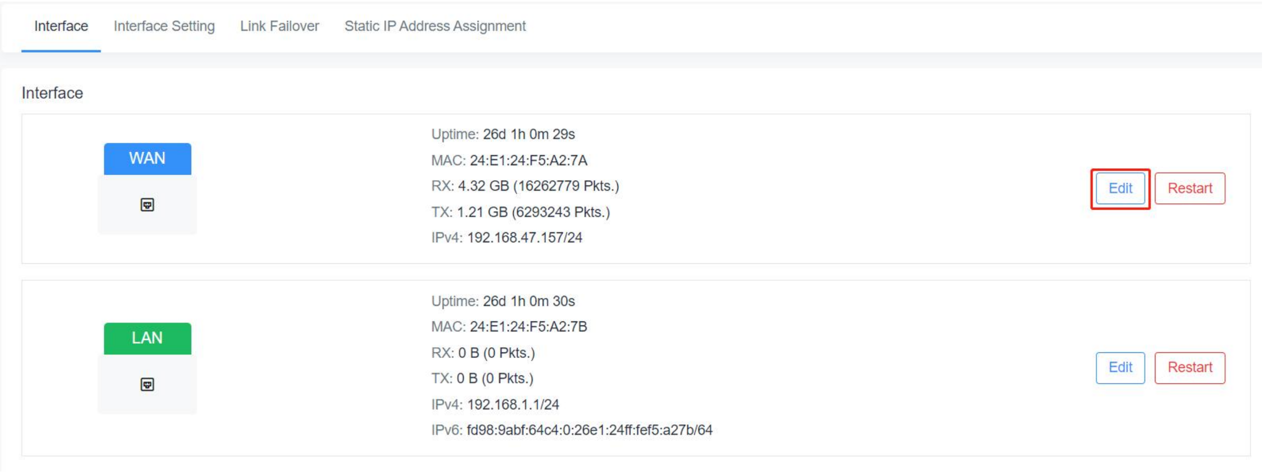
Cellular Status

6.2 Configure Ethernet Connection

UF51 supports getting network access via WAN port.

Configuration Steps

1. Go to **Network > Interface > Interface** page, find the WAN interface and click **Edit** button.



Interface | Interface Setting | Link Failover | Static IP Address Assignment

Interface

WAN

Uptime: 26d 1h 0m 29s
MAC: 24:E1:24:F5:A2:7A
RX: 4.32 GB (16262779 Pkts.)
TX: 1.21 GB (6293243 Pkts.)
IPv4: 192.168.47.157/24

Edit | Restart

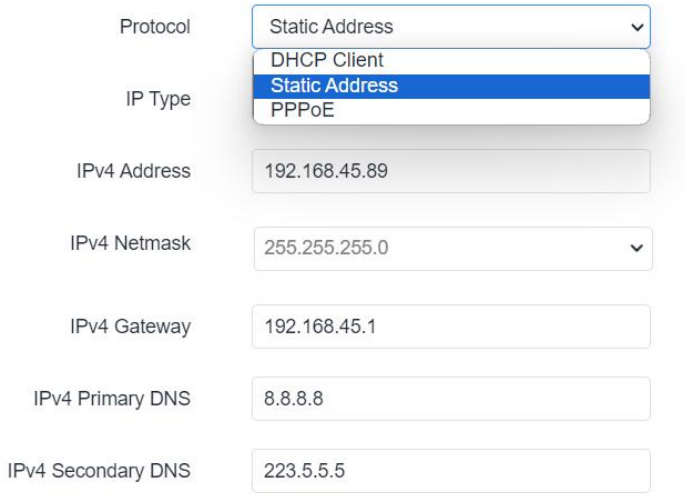
LAN

Uptime: 26d 1h 0m 30s
MAC: 24:E1:24:F5:A2:7B
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)
IPv4: 192.168.1.1/24
IPv6: fd98:9abf:64c4:0:26e1:24ff:fef5:a27b/64

Edit | Restart

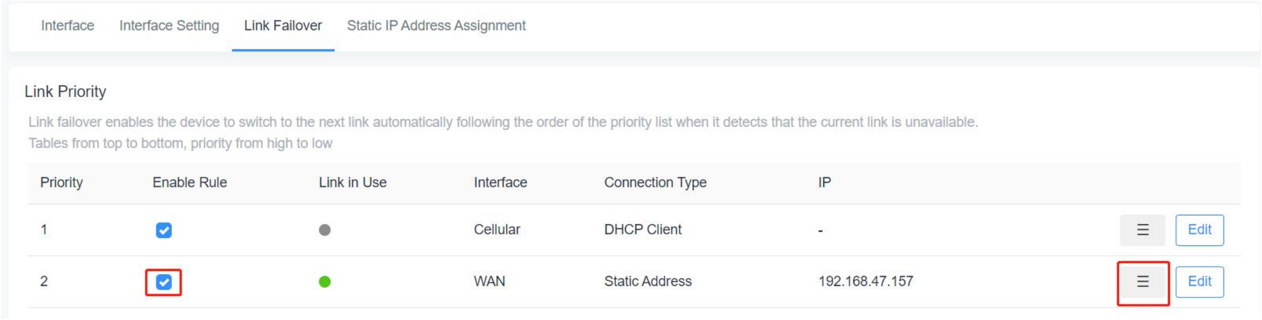
2. Select the protocol according to your network router mode or network provider types and configure the corresponding parameters, then save all settings.

- **DHCP:** upper network router will assign an IP address to UF51 WAN port. This is the easiest way and requires the upper route to enable the DHCP server.
- **Status Address:** assign a static IP address with the same subnet as the LAN subnet of the upper network router. Besides, it's necessary to configure at least one DNS server.
- **PPPoE:** type your PPPoE account username and password, this should contact your network provider.



Protocol	Static Address
	DHCP Client Static Address PPPoE
IP Type	
IPv4 Address	192.168.45.89
IPv4 Netmask	255.255.255.0
IPv4 Gateway	192.168.45.1
IPv4 Primary DNS	8.8.8.8
IPv4 Secondary DNS	223.5.5.5

3. Go to **Network > Interface > Link Failover** to enable WAN and drag the button to change link priority.



Interface | Interface Setting | Link Failover | Static IP Address Assignment

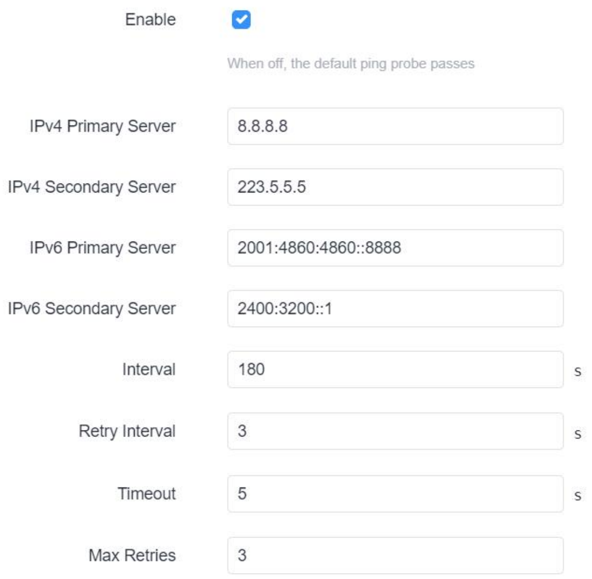
Link Priority

Link failover enables the device to switch to the next link automatically following the order of the priority list when it detects that the current link is unavailable.
Tables from top to bottom, priority from high to low

Priority	Enable Rule	Link in Use	Interface	Connection Type	IP	
1	☑	●	Cellular	DHCP Client	-	☰ Edit
2	☑	●	WAN	Static Address	192.168.47.157	☰ Edit

4. Click **Edit** of a link to configure ICMP ping detection information. When ping probe is enabled, the device will send ICMP packets to detection server to check if this link is valid. If no response and exceeding max retries, it will switch to the lower priority link.

Note: if you use private network, please change a private server address or disable the ping probe.



Enable ☑

When off, the default ping probe passes

IPv4 Primary Server: 8.8.8.8

IPv4 Secondary Server: 223.5.5.5

IPv6 Primary Server: 2001:4860:4860::8888

IPv6 Secondary Server: 2400:3200::1

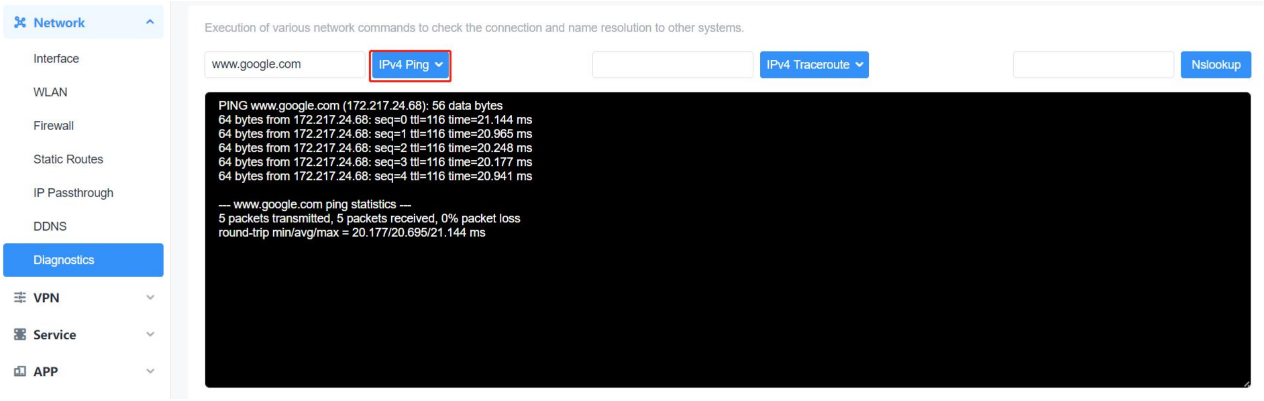
Interval: 180 s

Retry Interval: 3 s

Timeout: 5 s

Max Retries: 3

5. Click **Network > Diagnostics** to check the network connectivity.



Execution of various network commands to check the connection and name resolution to other systems.

www.google.com

```
PING www.google.com (172.217.24.68): 56 data bytes
64 bytes from 172.217.24.68: seq=0 ttl=116 time=21.144 ms
64 bytes from 172.217.24.68: seq=1 ttl=116 time=20.965 ms
64 bytes from 172.217.24.68: seq=2 ttl=116 time=20.248 ms
64 bytes from 172.217.24.68: seq=3 ttl=116 time=20.177 ms
64 bytes from 172.217.24.68: seq=4 ttl=116 time=20.941 ms

--- www.google.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 20.177/20.695/21.144 ms
```

Related Topic

WAN Setting

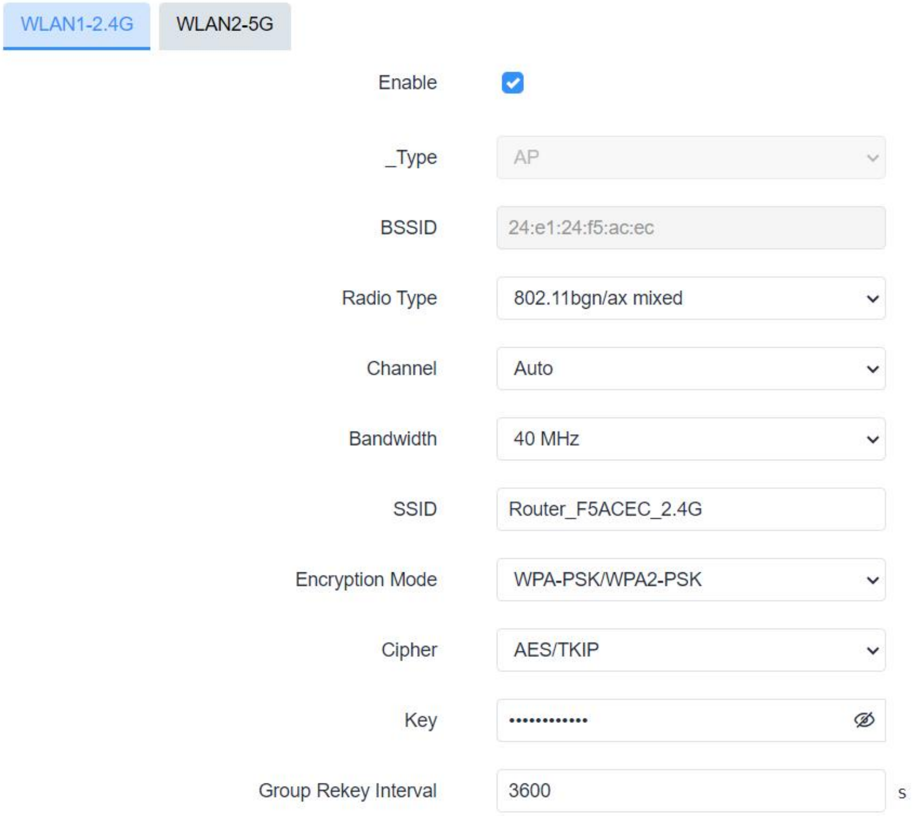
6.3 Configure Wi-Fi Access Point

UF51 supports both 2.4G and 5G Wi-Fi and they can work as access points to provide network access to other devices at the same time. We are about to take an example of configuring a 2.4G Wi-Fi access point.

Configuration Steps

1. Ensure the device supports Wi-Fi and the Wi-Fi antennas are connected to the correct connectors.
2. Go to **Network > WLAN** page to enable 2.4G Wi-Fi mode, then users can modify the radio type, SSID and other parameters. For security access, it's suggested to select an encryption mode and

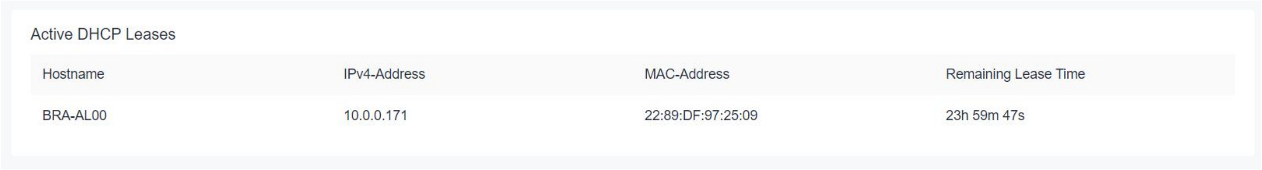
define a key for devices to connect to Wi-Fi.



WLAN1-2.4G | WLAN2-5G

Enable	☑
_Type	AP
BSSID	24:e1:24:f5:ac:ec
Radio Type	802.11bgn/ax mixed
Channel	Auto
Bandwidth	40 MHz
SSID	Router_F5ACEC_2.4G
Encryption Mode	WPA-PSK/WPA2-PSK
Cipher	AES/TKIP
Key	••••••••••••
Group Rekey Interval	3600 s

3. Use a smart phone to connect the access point of UF51. You can check the information of the connected client/user on **Status > Overview** page.



Active DHCP Leases

Hostname	IPv4-Address	MAC-Address	Remaining Lease Time
BRA-AL00	10.0.0.171	22:89:DF:97:25:09	23h 59m 47s

Related Topic

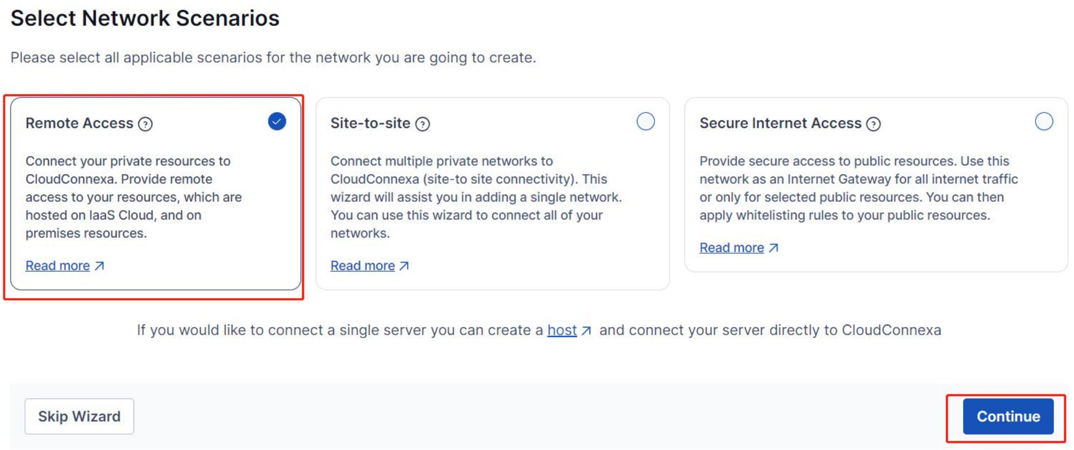
WLAN Setting

6.4 Configure OpenVPN Client

UF51 can work as OpenVPN clients or OpenVPN servers. We are about to take an example of configuring OpenVPN client to connect to CloudConnexa.

Configuration Steps

1. Ensure the UF51 has gotten access to the Internet.
2. Log in the CloudConnexa account, select Network section and select the service depending on your requirement and follow the wizard to continue the settings.



Select Network Scenarios

Please select all applicable scenarios for the network you are going to create.

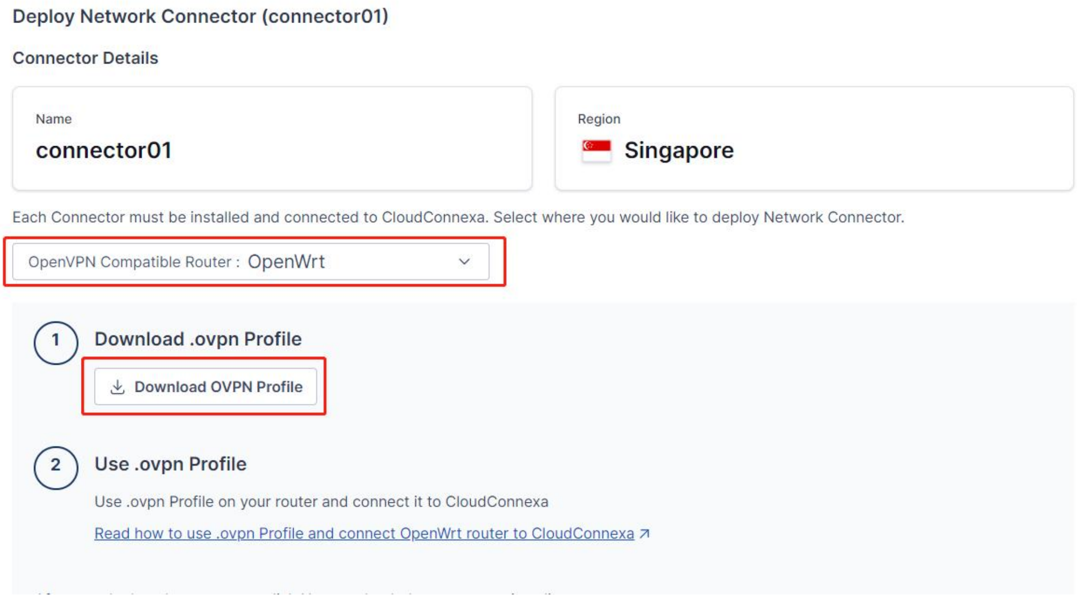
Remote Access ☑
Connect your private resources to CloudConnexa. Provide remote access to your resources, which are hosted on IaaS Cloud, and on premises resources.
Read more ↗

Site-to-site ○
Connect multiple private networks to CloudConnexa (site-to site connectivity). This wizard will assist you in adding a single network. You can use this wizard to connect all of your networks.
Read more ↗

Secure Internet Access ○
Provide secure access to public resources. Use this network as an Internet Gateway for all internet traffic or only for selected public resources. You can then apply whitelisting rules to your public resources.
Read more ↗

If you would like to connect a single server you can create a host ↗ and connect your server directly to CloudConnexa

3. Select the provider type as OpenWrt and download the OVPN file.



Deploy Network Connector (connector01)

Connector Details

Name: connector01

Region: Singapore

Each Connector must be installed and connected to CloudConnexa. Select where you would like to deploy Network Connector.

OpenVPN Compatible Router : OpenWrt

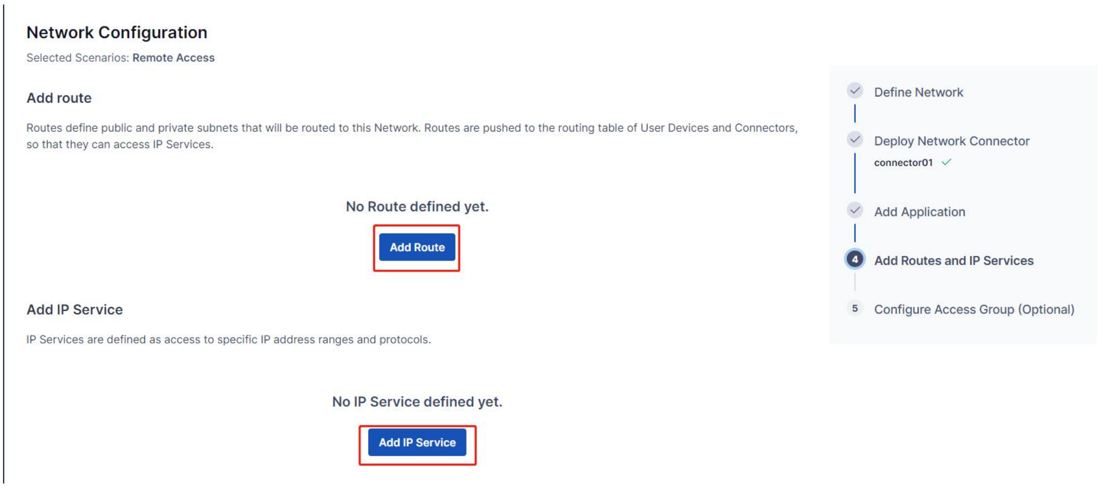
1 Download .ovpn Profile

2 Use .ovpn Profile

Use .ovpn Profile on your router and connect it to CloudConnexa

Read how to use .ovpn Profile and connect OpenWrt router to CloudConnexa ↗

4. If you need to access the terminal devices under subnet, it's necessary to add the route and IP service as LAN subnet of the router.



Network Configuration

Selected Scenarios: Remote Access

Add route

Routes define public and private subnets that will be routed to this Network. Routes are pushed to the routing table of User Devices and Connectors, so that they can access IP Services.

No Route defined yet.

Add IP Service

IP Services are defined as access to specific IP address ranges and protocols.

No IP Service defined yet.

✓ Define Network

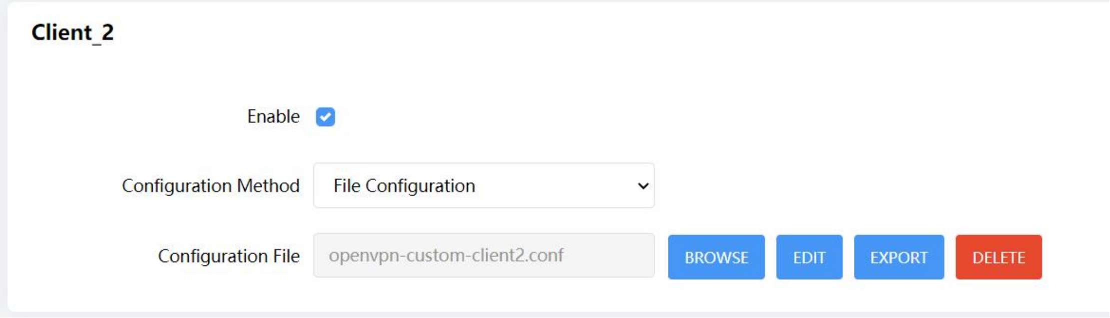
✓ Deploy Network Connector
connector01 ✓

✓ Add Application

4 Add Routes and IP Services

5 Configure Access Group (Optional)

5. Go to **VPN > OpenVPN > OpenVPN Client** page of device, select configuration method as File Configuration, then import the OVPN file.



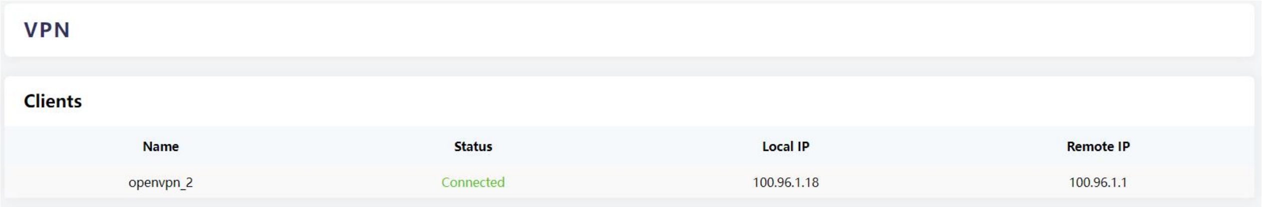
Client_2

Enable ☑

Configuration Method: File Configuration

Configuration File: openvpn-custom-client2.conf

6. Go to **Status > VPN** page to check if the client is connected.

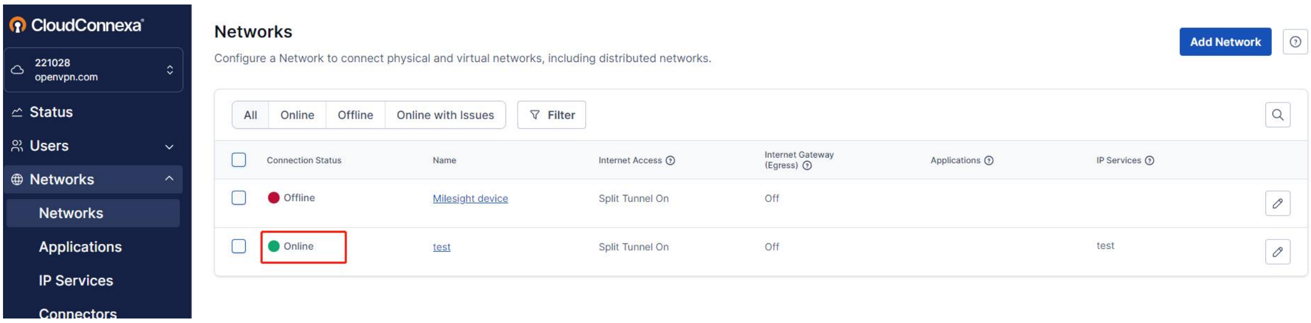


VPN

Clients

Name	Status	Local IP	Remote IP
openvpn_2	Connected	100.96.1.18	100.96.1.1

You can also check the connection status on CloudConnexa.



Networks

Configure a Network to connect physical and virtual networks, including distributed networks.

	Connection Status	Name	Internet Access	Internet Gateway (Egress)	Applications	IP Services
□	● Offline	Milesight device	Split Tunnel On	Off		
□	● Online	test	Split Tunnel On	Off		test

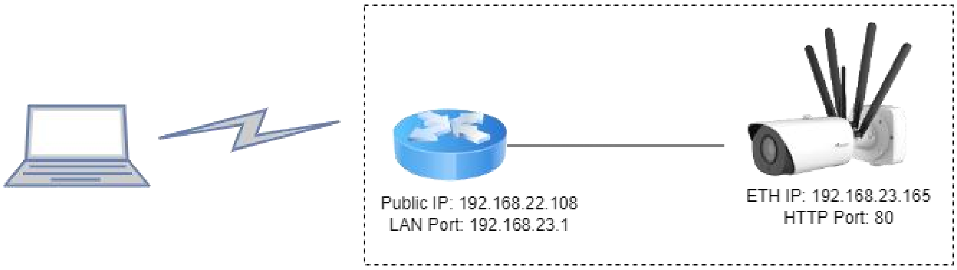
Related Topic

OpenVPN Client

6.5 Configure NAT Rule

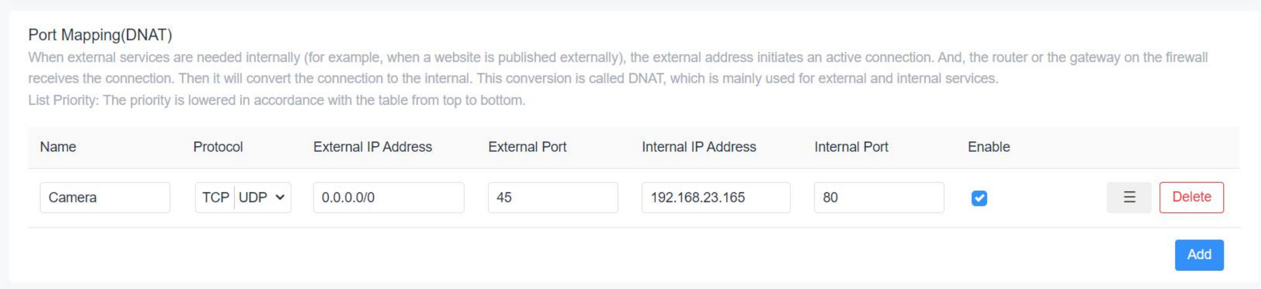
Example

A UF51 device can access to the Internet via cellular and get a public IP address. LAN port is connected with an IP camera whose IP address is 192.168.23.165 and HTTP port is 80. This IP camera can be accessed by public IP address via the below port mapping settings.



Configuration Steps

Go to **Network > Firewall > Port Mapping** and configure port mapping parameters as below. External IP address 0.0.0.0/0 means all external addresses are allowed to access. After that, users can use public IP: external port to access the IP camera.



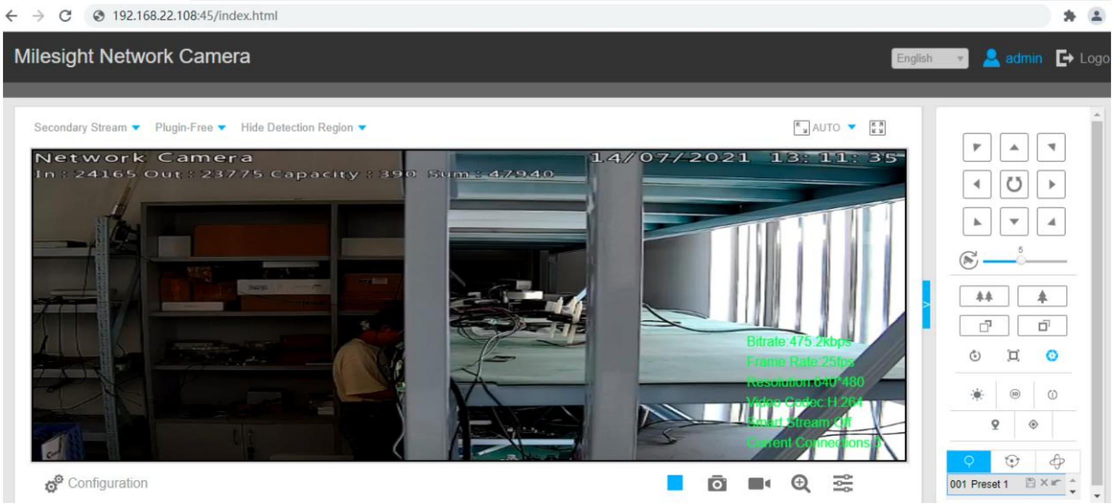
Port Mapping(DNAT)

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 to the internal. This conversion is called DNAT, which is mainly used for external and internal services.

List Priority: The priority is lowered in accordance with the table from top to bottom.

Name	Protocol	External IP Address	External Port	Internal IP Address	Internal Port	Enable	
Camera	TCP UDP	0.0.0.0/0	45	192.168.23.165	80	☑	☰ Delete

Add



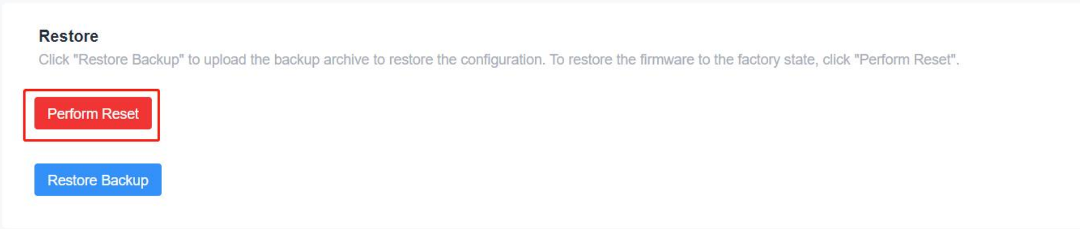
Related Topic

Port Mapping

6.6 Restore Factory Defaults

Method 1:

Go to **System > Maintenance > Backup/Upgrade** page, click **Perform Reset** button, you will be asked to confirm if you'd like to reset it to factory defaults. Then click **OK** button.



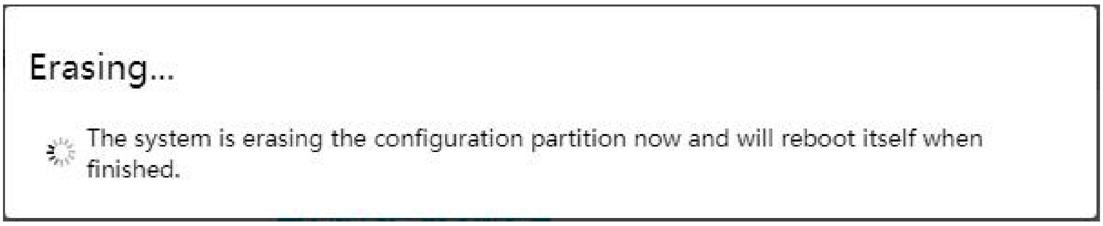
Restore

Click "Restore Backup" to upload the backup archive to restore the configuration. To restore the firmware to the factory state, click "Perform Reset".

Perform Reset

Restore Backup

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



Erasing...

The system is erasing the configuration partition now and will reboot itself when finished.

Please wait till the SYSTEM LED shines in green, which means the device has already been reset to factory defaults successfully.

Related Topic

Backup / Flash Firmware

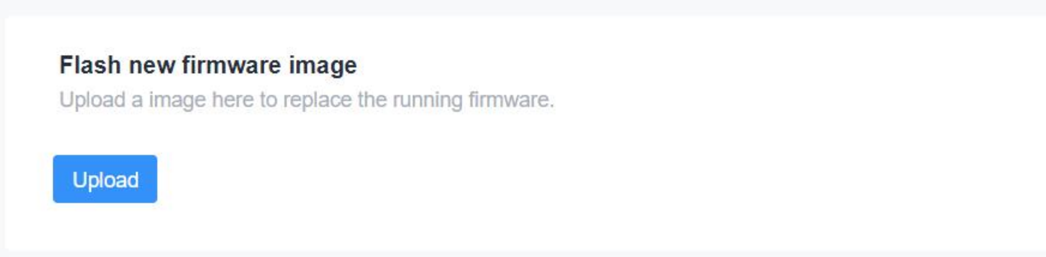
Method 2:

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

6.7 Firmware Upgrade

It is suggested that you contact Milesight technical support first before you upgrade the device. After getting the image file please refer to the following steps to complete the upgrade.

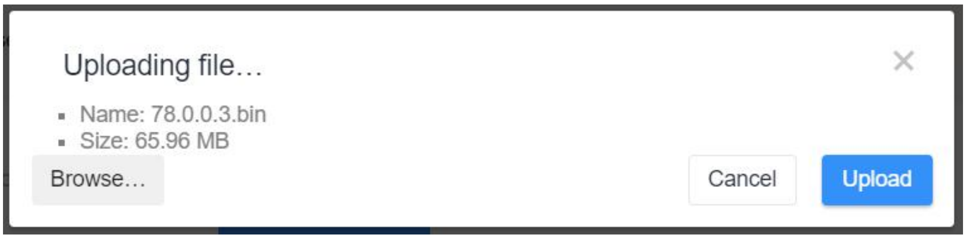
1. Go to **System > Maintenance > Backup/Upgrade** page, and click **Upload.**



Flash new firmware image

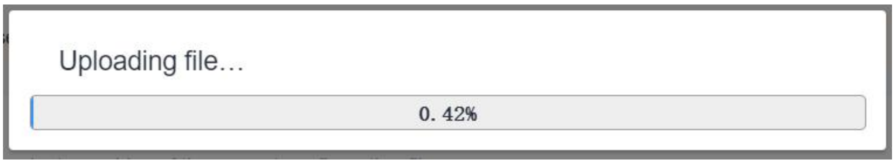
Upload a image here to replace the running firmware.

2. Browse the correct firmware file from the PC, click **Upload** and the device will check if the firmware file is correct. If it's correct, the firmware will be imported to the device.



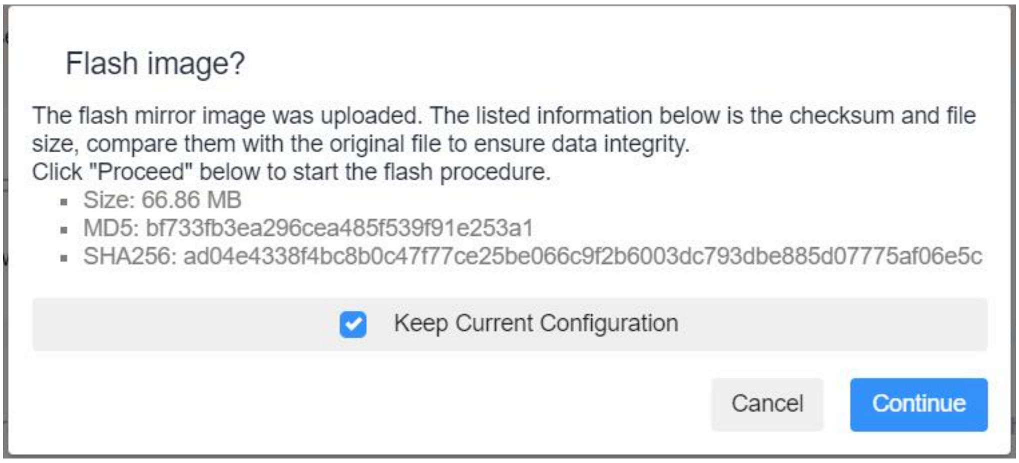
Uploading file…

- Name: 78.0.0.3.bin
- Size: 65.96 MB



Uploading file…

3. After upload, click **Continue** to upgrade the device. When SYS LED changes from orange to green and stay statically, the upgrade is completed. Do not perform any operation or disconnect the power during the upgrade.

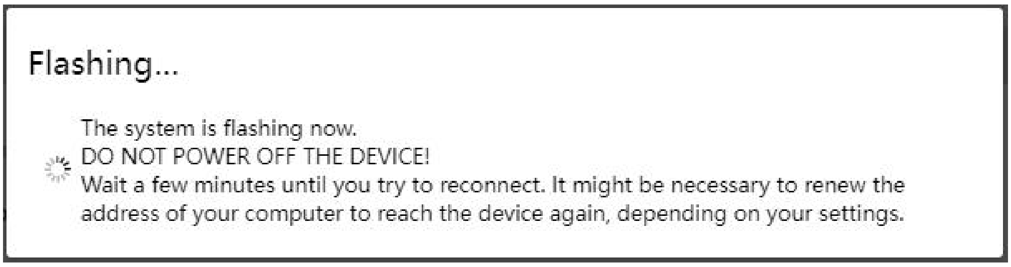


Flash image?

The flash mirror image was uploaded. The listed information below is the checksum and file size, compare them with the original file to ensure data integrity.
Click "Proceed" below to start the flash procedure.

- Size: 66.86 MB
- MD5: bf733fb3ea296cea485f539f91e253a1
- SHA256: ad04e4338f4bc8b0c47f77ce25be066c9f2b6003dc793dbe885d07775af06e5c

☑ Keep Current Configuration



Flashing...

The system is flashing now.
DO NOT POWER OFF THE DEVICE!
Wait a few minutes until you try to reconnect. It might be necessary to renew the address of your computer to reach the device again, depending on your settings.

Related Topic

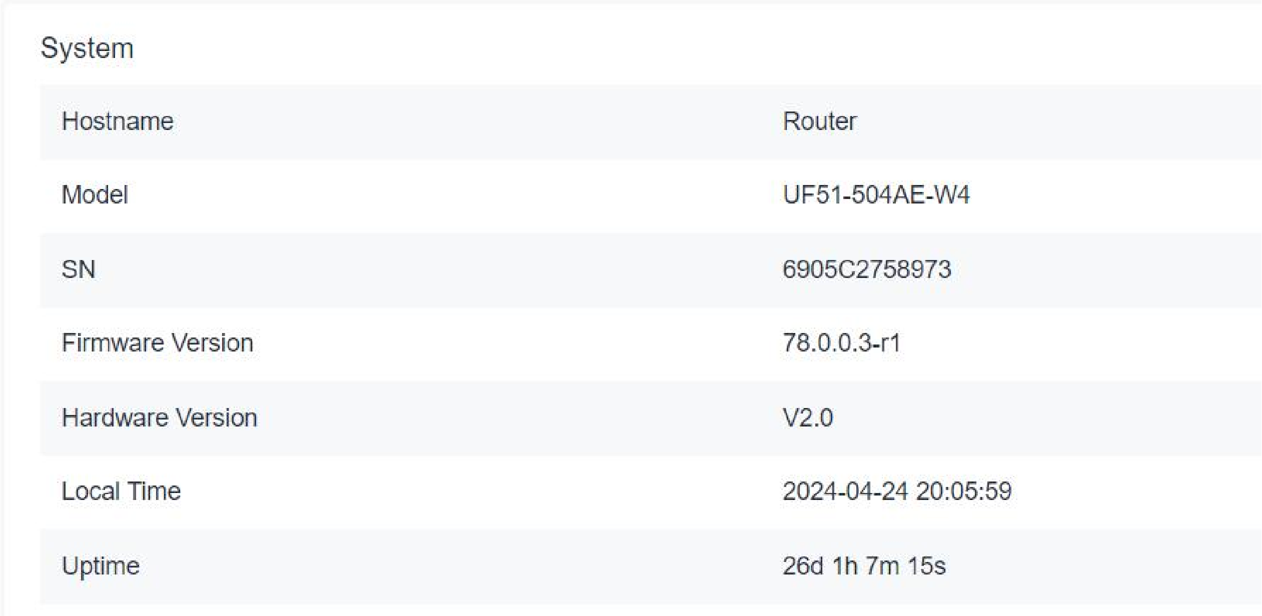
Backup / Flash Firmware

Chapter 7 Web Configuration

7.1 Status

7.1.1 Overview

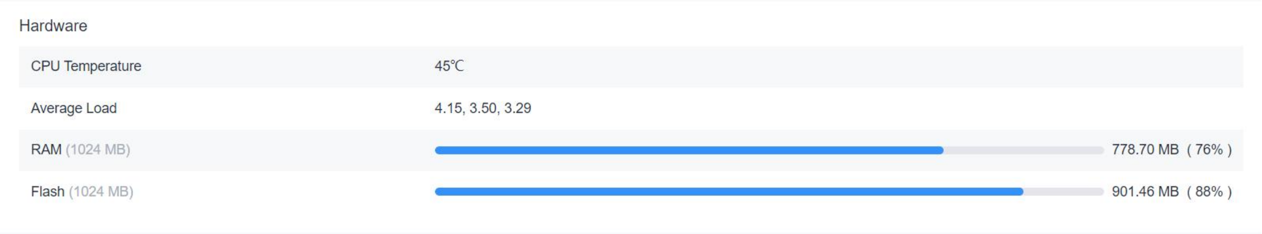
The System tab contains the basic information of the device on this page.



System

Hostname	Router
Model	UF51-504AE-W4
SN	6905C2758973
Firmware Version	78.0.0.3-r1
Hardware Version	V2.0
Local Time	2024-04-24 20:05:59
Uptime	26d 1h 7m 15s

System	
Item	**Description**
Hostname	The hostname of device, it can be modified on **System > Administration > System Settings**.
Model	The model name of the device.
SN	The serial number of the device.
Firmware Version	The current firmware version of the device.
Hardware Version	The current hardware version of the device.
Local Time	The current system time of the device , it can be modified on **System > Administration > System Settings**.
Uptime	The time since the device has been powered and running.

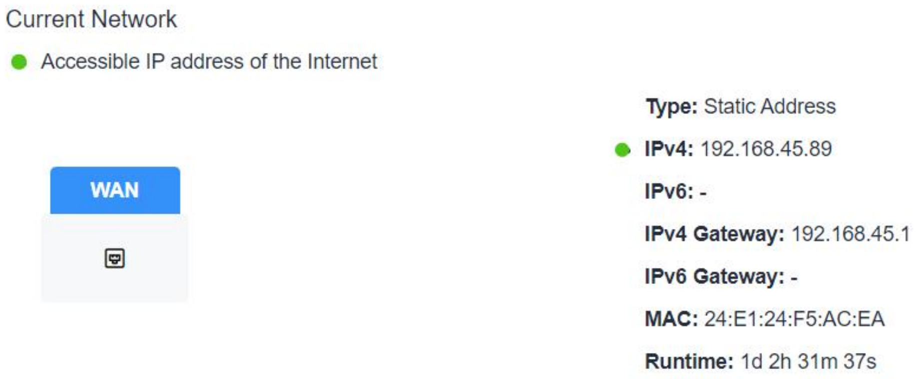


Hardware

CPU Temperature	45℃
Average Load	4.15, 3.50, 3.29
RAM (1024 MB)	778.70 MB (76%)
Flash (1024 MB)	901.46 MB (88%)

Hardware	
Item	**Description**
CPU Temperature	The temperature of CPU.
Average Load	Averages over progressively longer periods of time (1, 5 and 15 minutes averages), the smaller numbers are better.
RAM	the RAM capacity and the available RAM memory.
Flash	the flash capacity and the available flash memory.

The **Current Network** tab displays the basic information of link in use, click Interface chapter for details.



Current Network

● Accessible IP address of the Internet

Type: Static Address

● **IPv4:** 192.168.45.89

IPv6: -

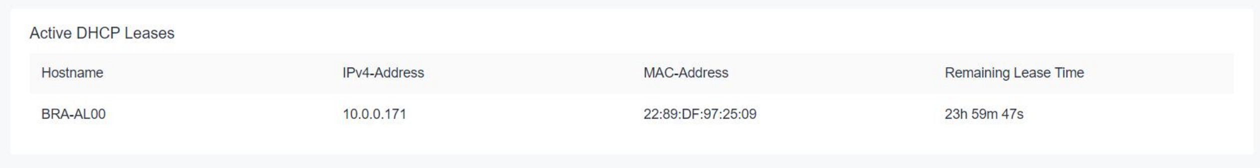
IPv4 Gateway: 192.168.45.1

IPv6 Gateway: -

MAC: 24:E1:24:F5:AC:EA

Runtime: 1d 2h 31m 37s

The Active DHCP Leases tab displays the basic information of connected devices.

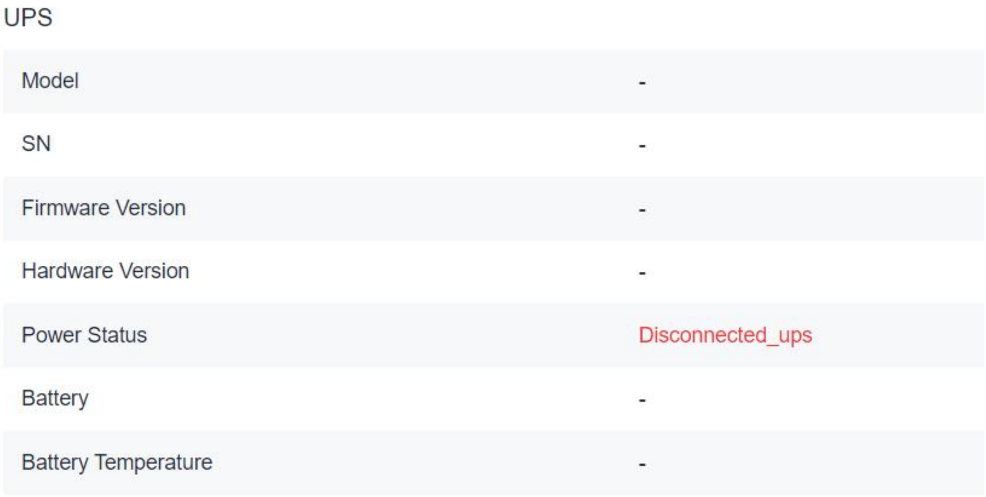


Active DHCP Leases

Hostname	IPv4-Address	MAC-Address	Remaining Lease Time
BRA-AL00	10.0.0.171	22:89:DF:97:25:09	23h 59m 47s

Active DHCP Leases	
Item	**Description**
Hostname	The hostname of the connected device.
IPv4-Address	Tthe IPv4 address of the connected device.
MAC-Address	The MAC address of the connected device.
Remaining Lease Time	The time remaining for this lease.

When Milesight UPS is connected to the device, the UPS basic information will also show on the Status page. For more details please refer to *Milesight UPS User Guide*.

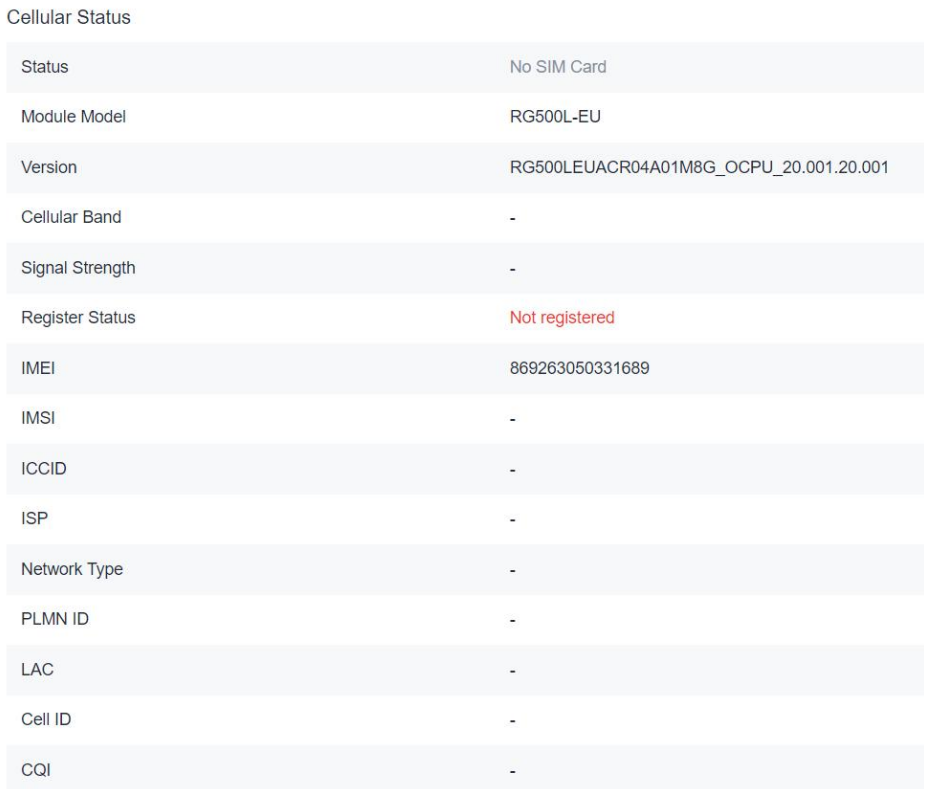


UPS

Model	-
SN	-
Firmware Version	-
Hardware Version	-
Power Status	Disconnected_ups
Battery	-
Battery Temperature	-

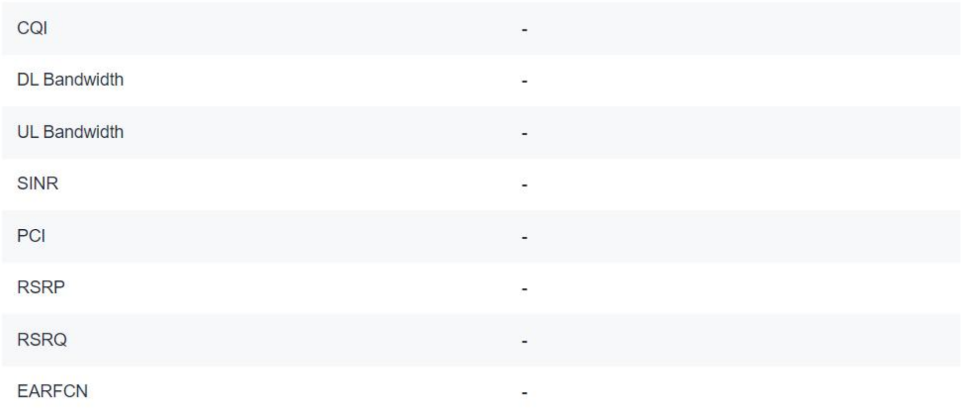
7.1.2 Cellular

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



Cellular Status

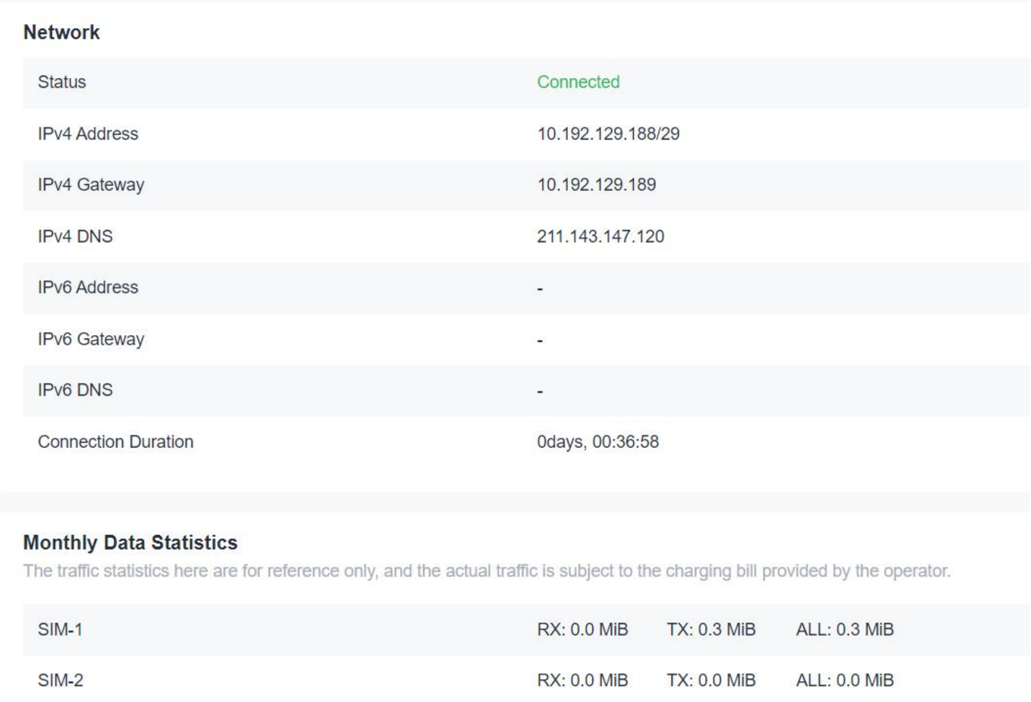
Status	No SIM Card
Module Model	RG500L-EU
Version	RG500LEUACR04A01M8G_OCPU_20.001.20.001
Cellular Band	-
Signal Strength	-
Register Status	Not registered
IMEI	869263050331689
IMSI	-
ICCID	-
ISP	-
Network Type	-
PLMN ID	-
LAC	-
Cell ID	-
CQI	-



CQI	-
DL Bandwidth	-
UL Bandwidth	-
SINR	-
PCI	-
RSRP	-
RSRQ	-
EARFCN	-

Modem Information	
Item	**Description**
Status	Corresponding detection status of module and SIM card. ● No SIM Card: the SIM card is not inserted ● PIN Error: the PIN code is error ● PIN Required: the SIM card requires to type PIN code ● PUK Required: the SIM card requires to be unlocked by PUK code ● No Signal: no cellular signal ● Ready: the SIM card is inserted ● Down: the SIM card is deactivated or data overage
Module Model	The model name of cellular module.
Version	The firmware version of cellular module.

Cellular Band	The cellular band which the device used to register to network.
Signal Strength	The RSSI (Received Signal Indicator) of registered cellular network.
Register Status	The registration status of SIM card.
IMEI	The IMEI of the cellular module.
IMSI	The IMSI of the SIM card.
ICCID	The ICCID of the SIM card.
ISP	The network provider which the SIM card registers on.
Network Type	The connected network type, such as LTE, 3G, etc.
PLMN ID	The current PLMN ID, including MCC, MNC, LAC and Cell ID.
LAC	The location area code of the SIM card.
Cell ID	The Cell ID of the SIM card location.
CQI	The Channel Quality Indicator of the cellular network.
DL Bandwidth	The DL bandwidth of the cellular network.
UL Bandwidth	The UL bandwidth of the cellular network.
SINR	The Signal Interference + Noise Ratio of the cellular network.
PCI	The physical-layer cell identity of the cellular network.
RSRP	The Reference Signal Received Power of the cellular network.
RSRQ	The Reference Quality Received Power of the cellular network.
EARFCN	The E-UTRA Absolute Radio Frequency Channel Number.



Network

Status	Connected
IPv4 Address	10.192.129.188/29
IPv4 Gateway	10.192.129.189
IPv4 DNS	211.143.147.120
IPv6 Address	-
IPv6 Gateway	-
IPv6 DNS	-
Connection Duration	0days, 00:36:58

Monthly Data Statistics

The traffic statistics here are for reference only, and the actual traffic is subject to the charging bill provided by the operator.

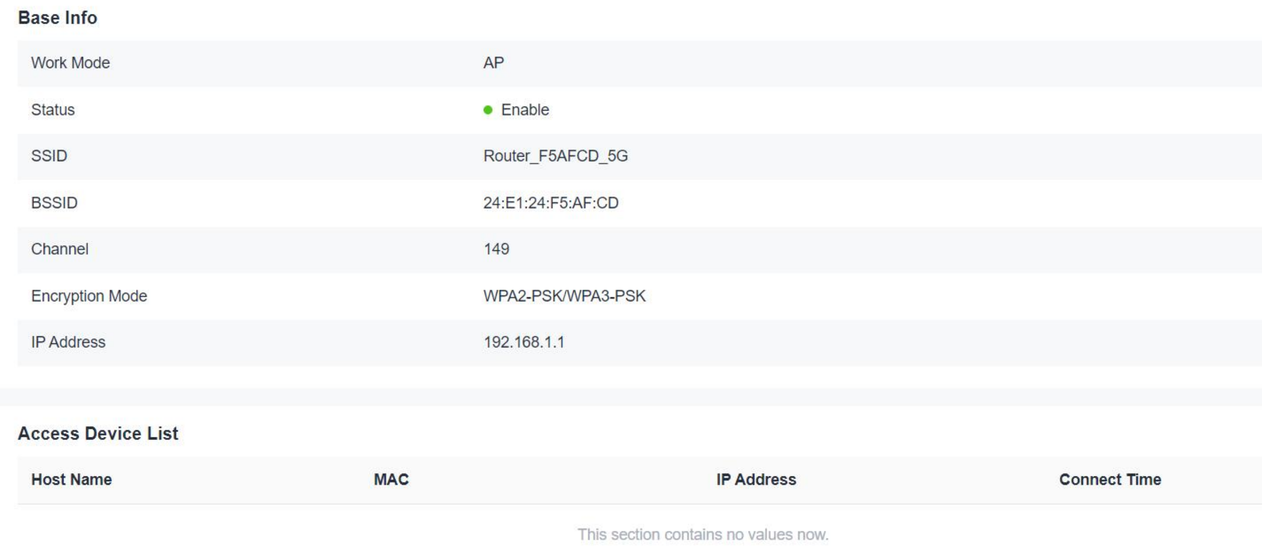
SIM-1	RX: 0.0 MiB	TX: 0.3 MiB	ALL: 0.3 MiB
SIM-2	RX: 0.0 MiB	TX: 0.0 MiB	ALL: 0.0 MiB

Network	
Item	**Description**
Status	The connection status of cellular network.
IPv4/IPv6 Address	The IPv4/IPv6 address and netmask of cellular network.
IPv4/IPv6 Gateway	The IPv4/IPv6 gateway and netmask of cellular network.

IPv4/IPv6 DNS	The DNS sever of cellular network.
Connection Duration	The information on how long the cellular network has been connected.
RX	The data volume and packets received of this month.
TX	The data volume and packets transmitted of this month.
ALL	Total data volume and packets of this month.

7.1.3 WLAN (Wi-Fi Version Only)

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



Base Info

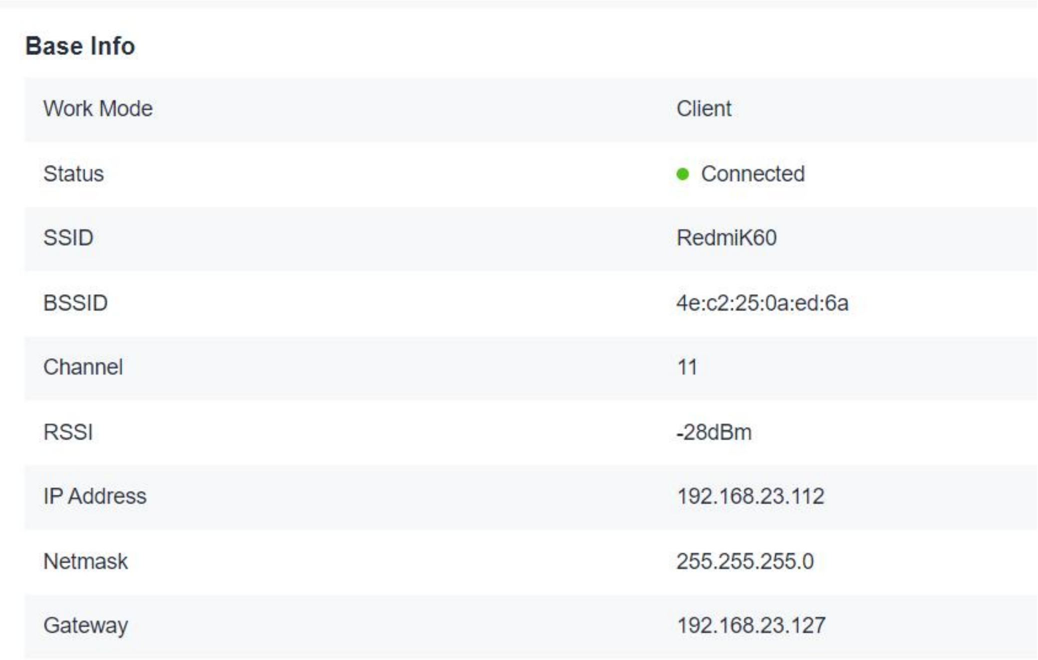
Work Mode	AP
Status	● Enable
SSID	Router_F5AFCD_5G
BSSID	24:E1:24:F5:AF:CD
Channel	149
Encryption Mode	WPA2-PSK/WPA3-PSK
IP Address	192.168.1.1

Access Device List

Host Name	MAC	IP Address	Connect Time

This section contains no values now.

WLAN Status-AP Mode	
Item	**Description**
Base Info	
Work Mode	Show the work mode of this WLAN interface.
Status	Show the enable status of this WLAN interface.
Type	Show the Wi-Fi interface type.
SSID	Show the SSID of this device.
Channel	Show the used channel of this WLAN interface.
Encryption Mode	Show the encryption mode of this WLAN interface.
IP Address	Show the IP address of this device.
Associated Device List	
Hostname	Show the hostname of the client which connected to this device.
MAC Address	Show the MAC address of the client which connected to this device.
IP Address	Show the IP address of the client which connected to this device.
Connect Time	Show the connection duration between client device and this device.



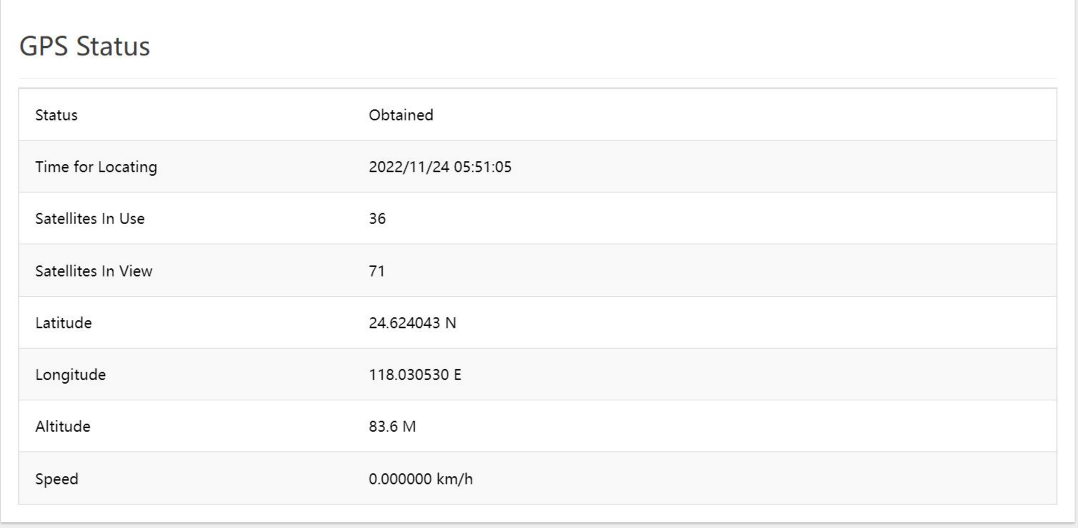
Base Info

Work Mode	Client
Status	● Connected
SSID	RedmiK60
BSSID	4e:c2:25:0a:ed:6a
Channel	11
RSSI	-28dBm
IP Address	192.168.23.112
Netmask	255.255.255.0
Gateway	192.168.23.127

WLAN Status-Client Mode	
Item	**Description**
Base Info	
Work Mode	Show the work mode of this WLAN interface.
Status	Show the connection status with WLAN access point.
SSID	Show the SSID of AP which the device connected to.
BSSID	Show the MAC address of AP which the device connected to.
Channel	Show the used channel of this WLAN interface.
RSSI	Show the signal of this WLAN interface.
IP Address	Show the IP address of this device assigned from WLAN AP.
Netmask	Show the netmask of this device assigned from WLAN AP.
Gateway	Show the IP address of WLAN AP.

7.1.4 GPS

When GPS function is enabled and the GPS information is obtained successfully, you can view the latest GPS information including GPS time, latitude, longitude and speed on this page.



GPS Status

Status	Obtained
Time for Locating	2022/11/24 05:51:05
Satellites In Use	36
Satellites In View	71
Latitude	24.624043 N
Longitude	118.030530 E
Altitude	83.6 M
Speed	0.000000 km/h

GPS Status	
Item	**Description**
Status	The obtain status of GPS.
Time for Locating	The time for locating.
Satellites In Use	The quantity of satellites in use.
Satellites In View	The quantity of satellites in view.
Latitude	The Latitude of the location.
Longitude	The Longitude of the location.
Altitude	The Altitude of the location.
Speed	The speed of movement.

7.1.5 Firewall

On this page you can check all IPv4/IPv6 chains of iptables. Users can click the targets with dashed line to jump to the corresponding chains.

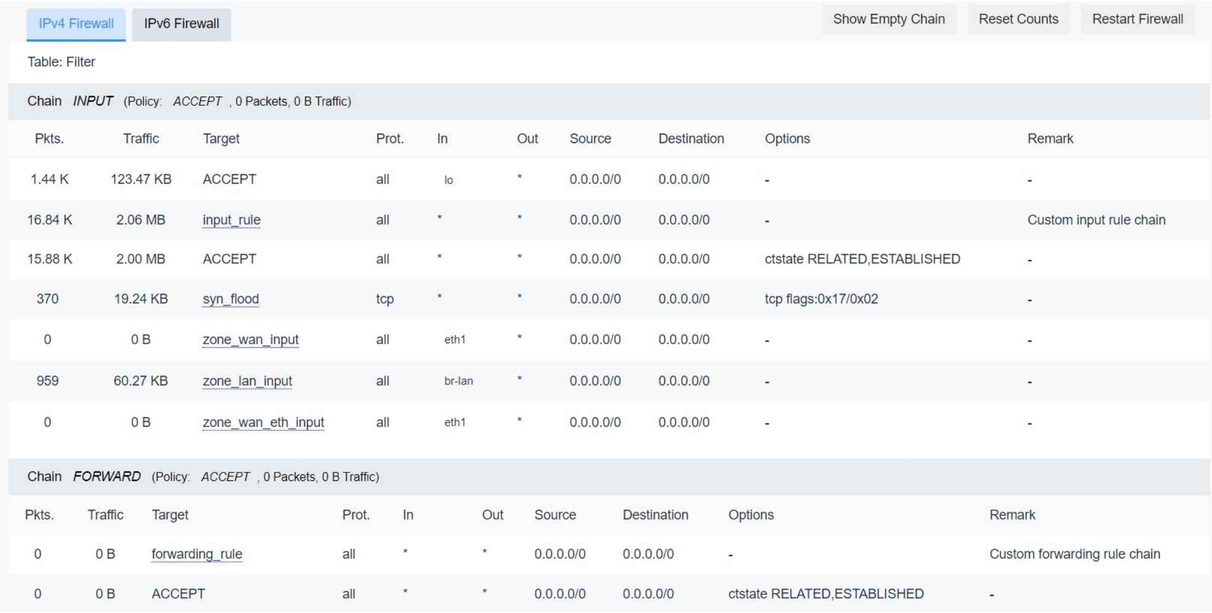


Table: Filter

Chain *INPUT* (Policy: *ACCEPT* , 0 Packets, 0 B Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Remark
1.44 K	123.47 KB	ACCEPT	all	lo	*	0.0.0.0/0	0.0.0.0/0	-	-
16.84 K	2.06 MB	input_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom input rule chain
15.88 K	2.00 MB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	-
370	19.24 KB	syn_flood	tcp	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02	-
0	0 B	zone_wan_input	all	eth1	*	0.0.0.0/0	0.0.0.0/0	-	-
959	60.27 KB	zone_lan_input	all	br-lan	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	zone_wan_eth_input	all	eth1	*	0.0.0.0/0	0.0.0.0/0	-	-

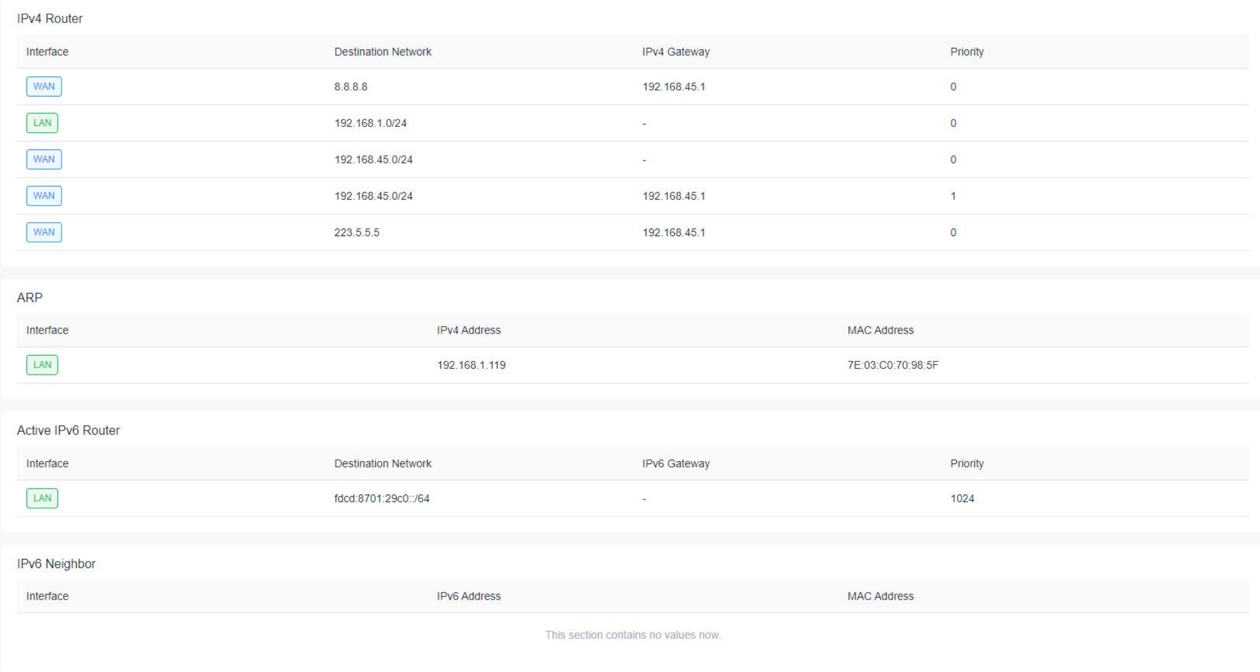
Chain *FORWARD* (Policy: *ACCEPT* , 0 Packets, 0 B Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Remark
0	0 B	forwarding_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom forwarding rule chain
0	0 B	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	-

Firewall Status	
Item	**Description**
Table: Filter	The default table for handing network packets.
Table: NAT	Used to alter packets that create a new connection and used for Network Address Translation (NAT).
Table: Mangle	Used for specific types of packet alternation.
Show/Hide Empty Chain	Show/hide the chain without any rule.
Reset Counts	Reset the traffic counts of all chains.
Restart Firewall	Restart the whole firewall process.

7.1.6 Routing Table

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



IPv4 Router

Interface	Destination Network	IPv4 Gateway	Priority
WAN	8.8.8.8	192.168.45.1	0
LAN	192.168.1.0/24	-	0
WAN	192.168.45.0/24	-	0
WAN	192.168.45.0/24	192.168.45.1	1
WAN	223.5.5.5	192.168.45.1	0

ARP

Interface	IPv4 Address	MAC Address
LAN	192.168.1.119	7E:03:C0:70:98:5F

Active IPv6 Router

Interface	Destination Network	IPv6 Gateway	Priority
LAN	fdcd:8701:29c0::/64	-	1024

IPv6 Neighbor

Interface	IPv6 Address	MAC Address

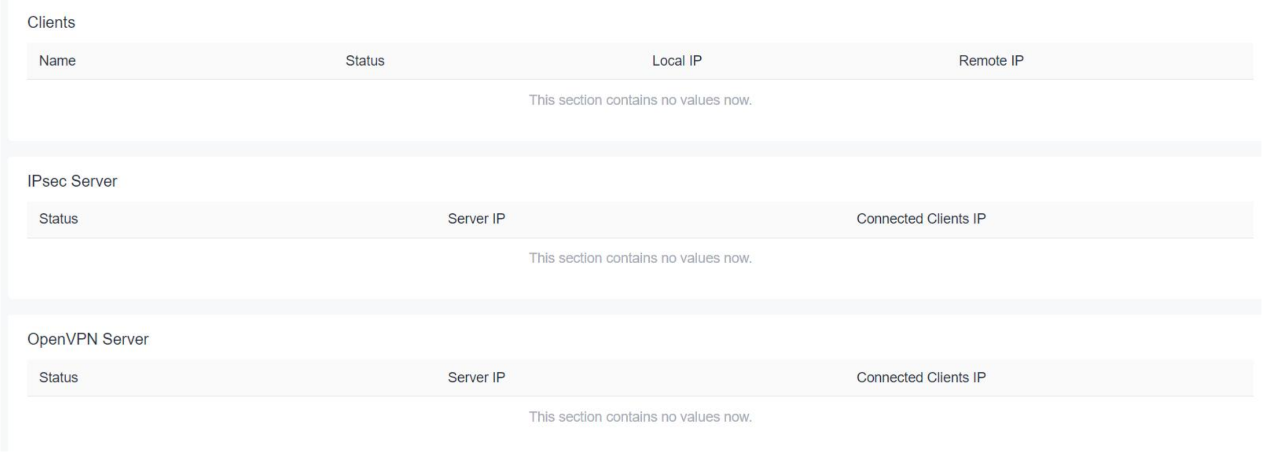
This section contains no values now.

Item	Description
Active IPv4/IPv6 Router	
Interface	The outbound interface of the route.
Destination Network	The IP address and netmask of destination host or destination network.
IPv4/IPv6 Gateway	The IP address of the gateway to send packets from.
Priority	The metric number indicating interface priority of usage.
ARP Cache	
Interface	The binding interface of ARP.
IPv4 Address	The IP address of ARP pool.
MAC Address	The IP address's corresponding MAC address.
IPv6 Neighbor	
Interface	The binding interface of neighbor.

IPv6 Address	The IP address of neighbor.
MAC Address	The IP address's corresponding MAC address.

7.1.7 VPN

You can check VPN status on this page.



Clients

Name	Status	Local IP	Remote IP

This section contains no values now.

IPsec Server

Status	Server IP	Connected Clients IP

This section contains no values now.

OpenVPN Server

Status	Server IP	Connected Clients IP

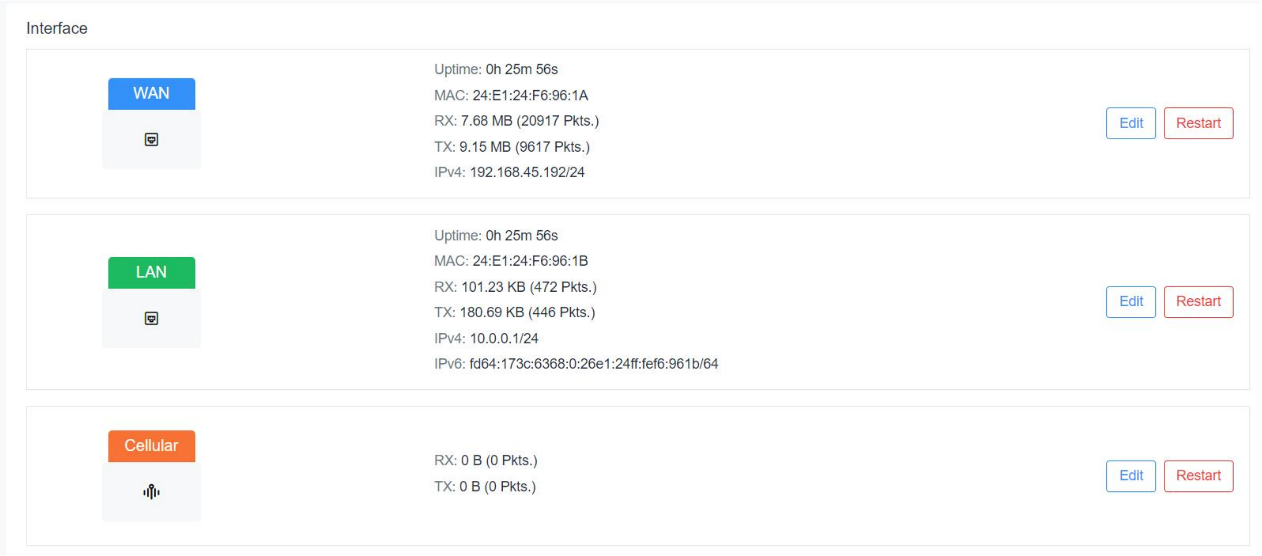
This section contains no values now.

VPN Status	
Item	**Description**
Clients	
Name	The name of the enabled VPN clients.
Status	The connection status of client.
Local IP	The local IP address and subnet of the VPN tunnel.
Remote IP	The real remote IP address and subnet of the VPN tunnel.
IPsec/OpenVPN Server	
Status	The status of Server.
Server IP	The server IP address and subnet of the VPN tunnel.
Connected Clients IP	The IP address of the client which is connected to the server.

7.2 Network

7.2.1 Interfaces

This menu allows to configure the basic settings of cellular, WAN and LAN interfaces.



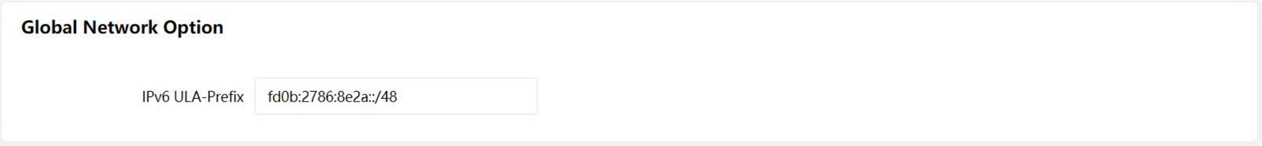
Interface

Uptime: 0h 25m 56s
MAC: 24:E1:24:F6:96:1A
RX: 7.68 MB (20917 Pkts.)
TX: 9.15 MB (9617 Pkts.)
IPv4: 192.168.45.192/24

Uptime: 0h 25m 56s
MAC: 24:E1:24:F6:96:1B
RX: 101.23 KB (472 Pkts.)
TX: 180.69 KB (446 Pkts.)
IPv4: 10.0.0.1/24
IPv6: fd64:173c:6368:0:26e1:24ff:fef6:961b/64

RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)

Interfaces	
Item	**Description**
Restart	Click to restart this network interface.
Edit	Click to edit general settings of this network interface.



Global Network Option

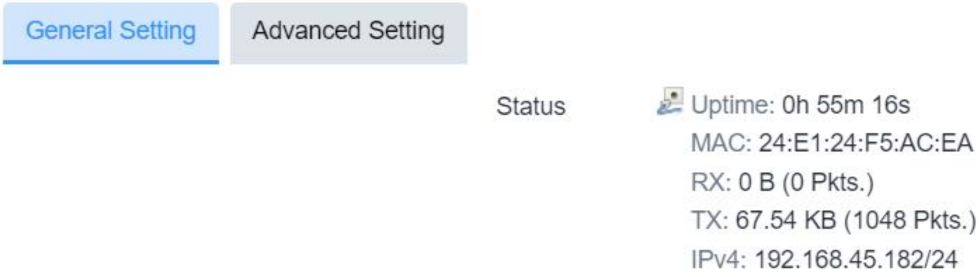
IPv6 ULA-Prefix: fd0b:2786:8e2a::/48

Global Network Options	
Item	**Description**
IPv6 ULA-Prefix	The IPv6 unique local address (ULA) prefix of this device.

7.2.1.1 WAN

The WAN port can be connected with an Ethernet cable to get Internet access. It supports 3 connection types which can work with both IPv4 and IPv6.

- **Static IP**: configure IPv4 address, netmask and gateway for Ethernet WAN interface.
- **DHCP Client**: configure Ethernet WAN interface as DHCP Client to obtain IPv4 address automatically.
- **PPPoE**: configure Ethernet WAN interface as PPPoE or PPPoEv6 Client.

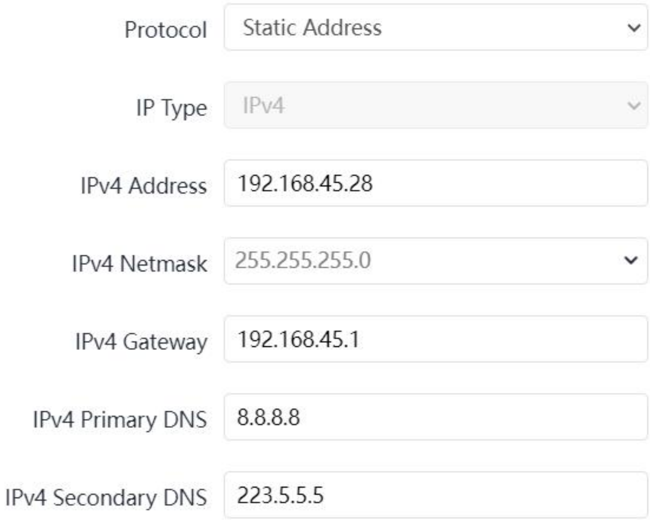


Status: Uptime: 0h 55m 16s
MAC: 24:E1:24:F5:AC:EA
RX: 0 B (0 Pkts.)
TX: 67.54 KB (1048 Pkts.)
IPv4: 192.168.45.182/24

WAN - Status	
Item	**Description**
Uptime	How long has the device been running.
MAC	MAC address of WAN interface.
RX	RX: the data volume and packets received in this interface.
TX	TX: the data volume and packets transmitted from this interface.
IPv4	IPv4 address of WAN interface.

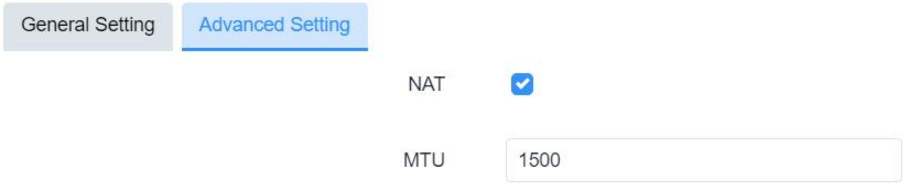
1. Static IP Configuration

If the external network assigns a fixed IP for the WAN interface, please select this mode.



Protocol: Static Address
IP Type: IPv4
IPv4 Address: 192.168.45.28
IPv4 Netmask: 255.255.255.0
IPv4 Gateway: 192.168.45.1
IPv4 Primary DNS: 8.8.8.8
IPv4 Secondary DNS: 223.5.5.5

Static Address - General Settings		
Item	**Description**	**Default**
IP Type	It's fixed as IPv4.	IPv4
IPv4 Address	Set the IPv4 address of the WAN port.	--
IPv4 Netmask	Set the Netmask for WAN port.	255.255.255.0
IPv4 Gateway	Set the gateway for WAN port's IPv4 address.	--
IPv4 Primary DNS	Set the primary IPv4 DNS server.	8.8.8.8
IPv4 Secondary DNS	Set the secondary IPv4 DNS server.	223.5.5.5



NAT ☑

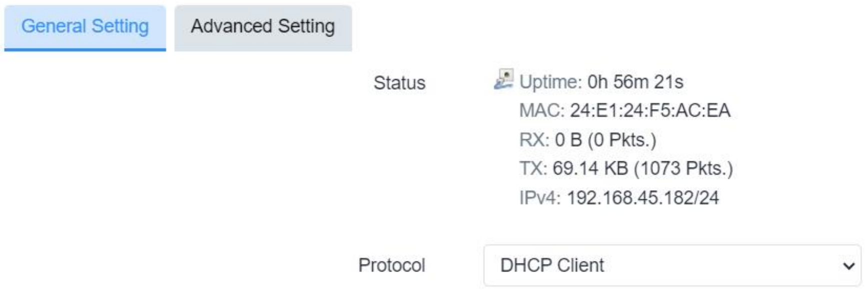
MTU: 1500

Static Address - Advanced Settings	
Item	**Description**

NAT	Enable or disable NAT function. When enabled, a private IP can be translated to a public IP.
MTU	Set the maximum transmission unit. Range: 68-1500.

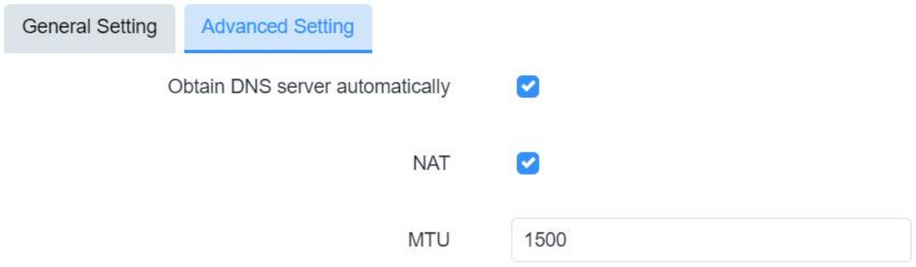
2. DHCP Client

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



Status
Uptime: 0h 56m 21s
MAC: 24:E1:24:F5:AC:EA
RX: 0 B (0 Pkts.)
TX: 69.14 KB (1073 Pkts.)
IPv4: 192.168.45.182/24

Protocol: DHCP Client



Obtain DNS server automatically ☑

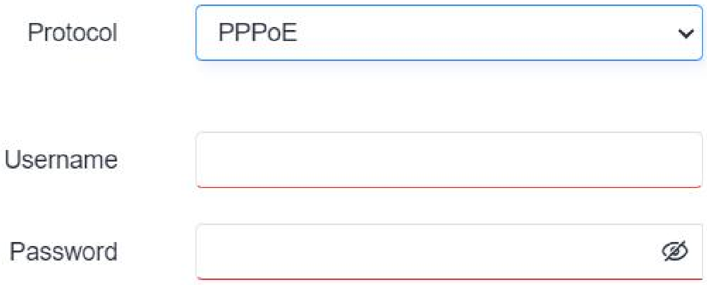
NAT ☑

MTU 1500

DHCP Client - Advanced Settings	
Item	**Description**
Obtain DNS server automatically	Obtain peer DNS automatically. DNS is necessary when visiting domain name.
NAT	Enable or disable NAT function. When enabled, a private IP can be translated to a public IP.
MTU	Set the maximum transmission unit. Range: 68-1500.

3. PPPoE/PPPoEv6

PPPoE refers to a point to point protocol over Ethernet. If IPv6 negotiation is enabled, device can get both IPv4 and IPv6 address.

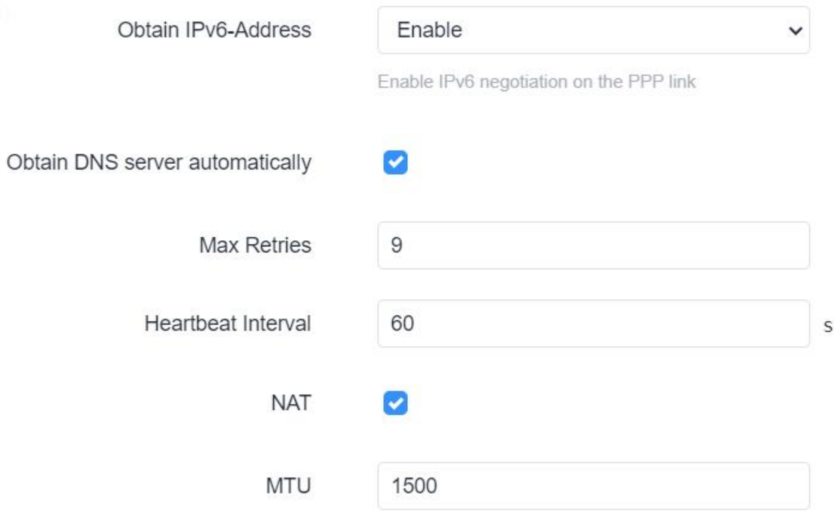


Protocol: PPPoE

Username

Password

PPPoE - General Settings	
Item	**Description**
PAP/CHAP Username	Enter the username provided by your Internet Service Provider (ISP).
PAP/CHAP Password	Enter the password provided by your Internet Service Provider (ISP).

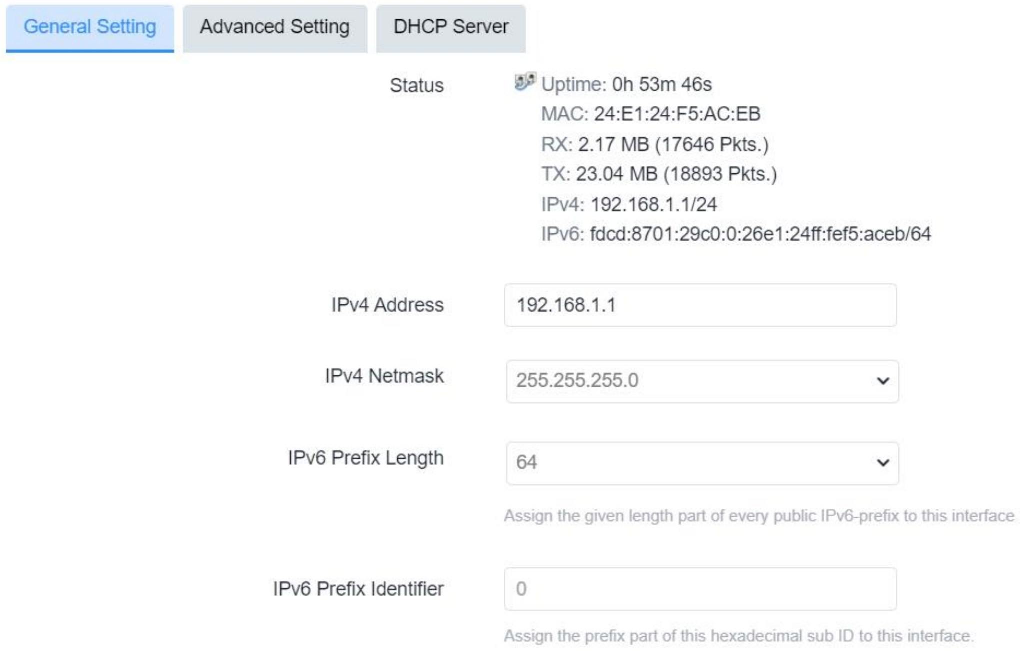

Obtain IPv6-Address: Enable
Enable IPv6 negotiation on the PPP link
Obtain DNS server automatically: ☑
Max Retries: 9
Heartbeat Interval: 60 s
NAT: ☑
MTU: 1500

PPPoE - Advanced Settings	
Item	**Description**
Obtain IPv6-Address	Enable IPv6 negotiation on the PPP link.
Obtain DNS server automatically	Obtain peer DNS automatically during PPP dialing. DNS is necessary when visiting domain name.
Max Retries	Set the maximum retry times after it fails to dial up. Range: 0-9.
Heartbeat Interval (s)	Set the heartbeat interval for link detection. Range: 1-600.
NAT	Enable or disable NAT function. When enabled, a private IP can be translated to a public IP.
MTU	Set the maximum transmission unit. Range: 68-1500.

Related Configuration Example

Ethernet WAN Connection

7.2.1.2 LAN/DHCP Server



Status
Uptime: 0h 53m 46s
MAC: 24:E1:24:F5:AC:EB
RX: 2.17 MB (17646 Pkts.)
TX: 23.04 MB (18893 Pkts.)
IPv4: 192.168.1.1/24
IPv6: fdcd:8701:29c0:0:26e1:24ff:fef5:aceb/64

IPv4 Address: 192.168.1.1

IPv4 Netmask: 255.255.255.0

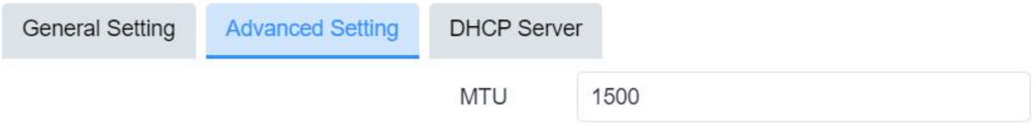
IPv6 Prefix Length: 64

Assign the given length part of every public IPv6-prefix to this interface

IPv6 Prefix Identifier: 0

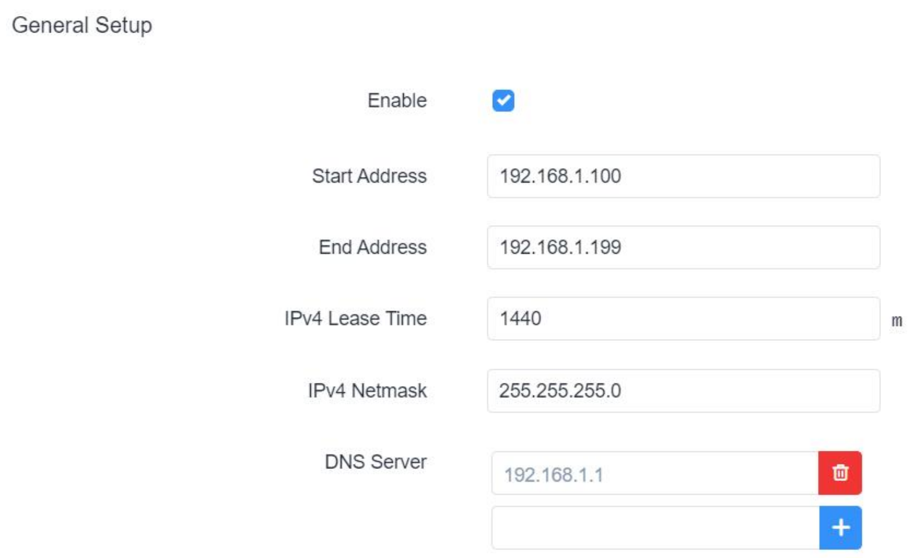
Assign the prefix part of this hexadecimal sub ID to this interface.

LAN - General Settings	
Item	**Description**
Status	**Uptime:** how long has the device been running.
	MAC: MAC address of LAN interfaces.
	RX: the data volume and packets received in this interface.
	TX: the data volume and packets transmitted from this interface.
	IPv4/IPv6: IPv4/IPv6 address of LAN interfaces.
IPv4 Address	Set the IPv4 address of LAN interface.
IPv4 Netmask	Set the netmask for LAN interface.
IPv6 Prefix Length	Assign a part of given length of every public IPv6-prefix to this interface.
IPv6 Prefix Identifier	Assign prefix parts using this hexadecimal sub-prefix ID for this interface.



MTU: 1500

LAN - Advanced Settings	
Item	**Description**
MTU	Set the maximum transmission unit. Range: 68-1500.



General Setup

Enable ☑

Start Address 192.168.1.100

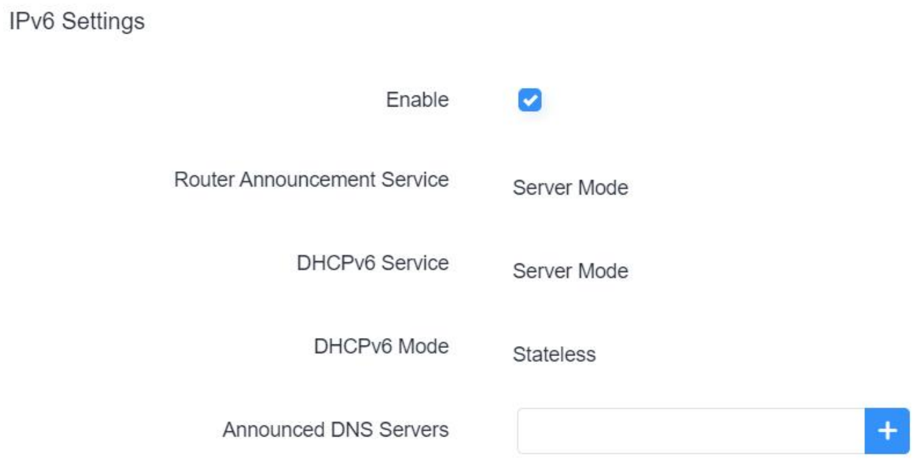
End Address 192.168.1.199

IPv4 Lease Time 1440 m

IPv4 Netmask 255.255.255.0

DNS Server 192.168.1.1

DHCP Server-General Setup	
Item	**Description**
Enable	Enable to disable DHCP for this interface.
Start Address	Define the beginning of the pool of IP addresses which will be leased to DHCP clients.
End Address	Define the end of the pool of IP addresses which will be leased to DHCP clients.
IPv4 Lease time	Set the expiry time of leased addresses, the minimum is 2 minutes (2m).
IPv4-Netmask	Set to override the netmask sent to clients. Normally it is calculated from the subnet that is served.
DNS Server	Set the DNS server list for clients.



IPv6 Settings

Enable ☑

Router Announcement Service Server Mode

DHCPv6 Service Server Mode

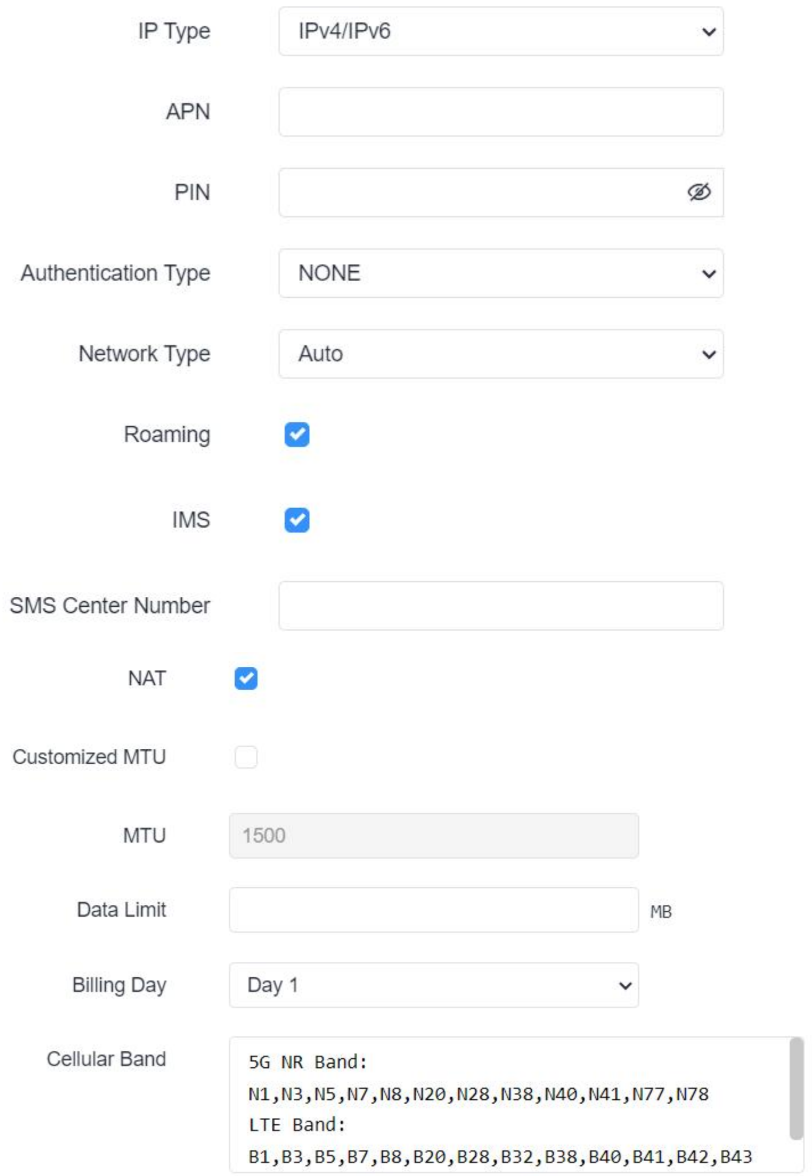
DHCPv6 Mode Stateless

Announced DNS Servers

DHCP Server-IPv6 Settings	
Item	**Description**
Enable	Choose to enable DHCPv6 server when using cellular IPv6 or PPPoE v6.
Router Advertisement Service	It’s fixed as server mode.
DHCPv6 Service	It’s fixed as server mode.

DHCPv6 Mode	It’s fixed as stateless mode.
Announced DNS Servers	Set the DNS server list for clients.

7.2.1.3 Cellular



IP Type: IPv4/IPv6

APN:

PIN:

Authentication Type: NONE

Network Type: Auto

Roaming: ☑

IMS: ☑

SMS Center Number:

NAT: ☑

Customized MTU: □

MTU: 1500

Data Limit: MB

Billing Day: Day 1

Cellular Band:

```
5G NR Band:
N1,N3,N5,N7,N8,N20,N28,N38,N40,N41,N77,N78
LTE Band:
B1,B3,B5,B7,B8,B20,B28,B32,B38,B40,B41,B42,B43
```

Cellular	
Item	**Description**
IP Type	Show the Internet protocol type to use for this interface. Option: IPv4, IPv6 and IPv4/IPv6.
APN	Enter the Access Point Name for cellular dial-up connection provided by local ISP.
PIN	Enter a 4-8 characters PIN code to unlock the SIM.
Authentication Type	Select from NONE, PAP, CHAP and PAP/CHAP.
Network Type	Select from Auto, 5G Only, 4G Only and 3G Only.

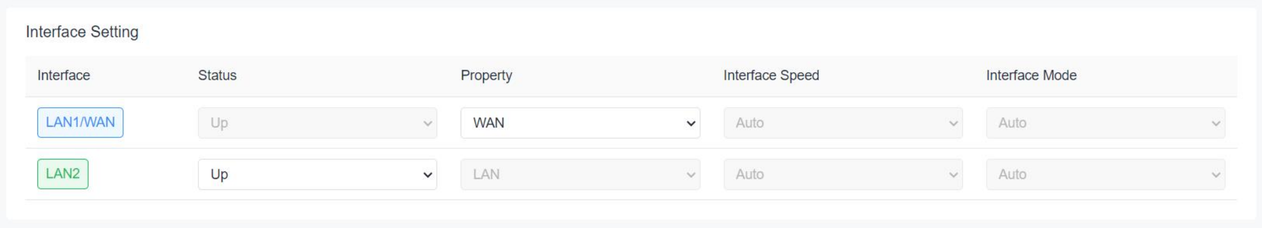
	Auto: connect to the network with the strongest signal automatically. 5G Only: connect to 5G network only. And so on.
Roaming	Enable or disable roaming.
IMS	Enable or disable IMS function.
SMS Center Number	Enter the local SMS center number for storing, forwarding, converting and delivering SMS message.
NAT	Enable or disable NAT function.
Customized MTU	Enable or disable to customize the maximum transmission units. When disabled, the device will use operator’s MTU settings.
MTU	Set the maximum transmission units. Range: 68-1500.
Data Limit	Set the data limit of this month. If data traffic exceeds the limit, the SIM card will be forbidden this month. The default is blank (no limited).
Billing Day	Clear the monthly data statistics when reaching the billing day of this month.
Cellular Band	Select the 5G NR and 4G LTE bands used to register cellular network. It can be used to optimize cellular speeds by selecting specific bands.

Related Application

Cellular Application

7.2.1.4 Interface Settings

UF51supports 2 Gigabit Ethernet ports. This page display the properties of all Ethernet ports and allows to control the status of these ports.



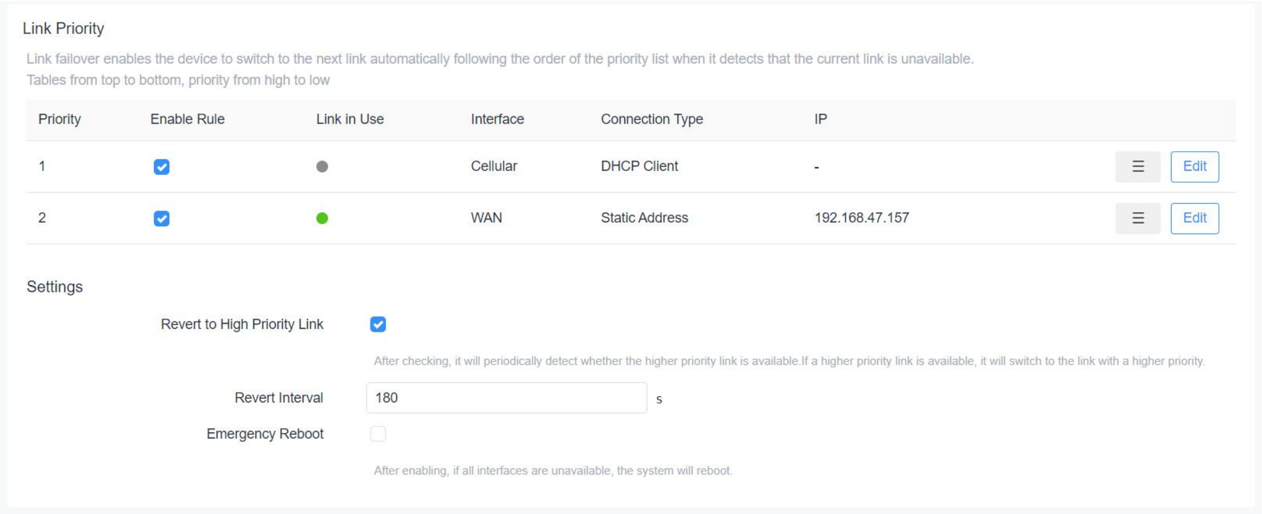
Interface Setting

Interface	Status	Property	Interface Speed	Interface Mode
LAN1/WAN	Up	WAN	Auto	Auto
LAN2	Up	LAN	Auto	Auto

Interface Setting	
Item	**Description**
Interface	Users can define the Ethernet ports according to their needs.
Status	Set the status of Ethernet port; select **Up** to enable and **Down** to disable.
Property	The Ethernet port's type, fixed as a WAN port or a LAN port.
Interface Speed	Ethernet port speed is fixed as Auto.
Interface Mode	Ethernet port mode is fixed as Auto.

7.2.1.5 Link Failover

This section describes how to configure link failover strategies, their priority and the ping settings, each rule owns its ping rules by default. The device will follow the priority to choose the next available interface to access the internet, make sure you have enabled the full interface that you need to use here. If priority 1 can only use IPv4, UF51 will select a second link in which IPv6 works as the main IPv6 link and vice versa.



Link Priority

Link failover enables the device to switch to the next link automatically following the order of the priority list when it detects that the current link is unavailable.
Tables from top to bottom, priority from high to low

Priority	Enable Rule	Link in Use	Interface	Connection Type	IP	
1	☑	●	Cellular	DHCP Client	-	☰ Edit
2	☑	●	WAN	Static Address	192.168.47.157	☰ Edit

Settings

Revert to High Priority Link ☑

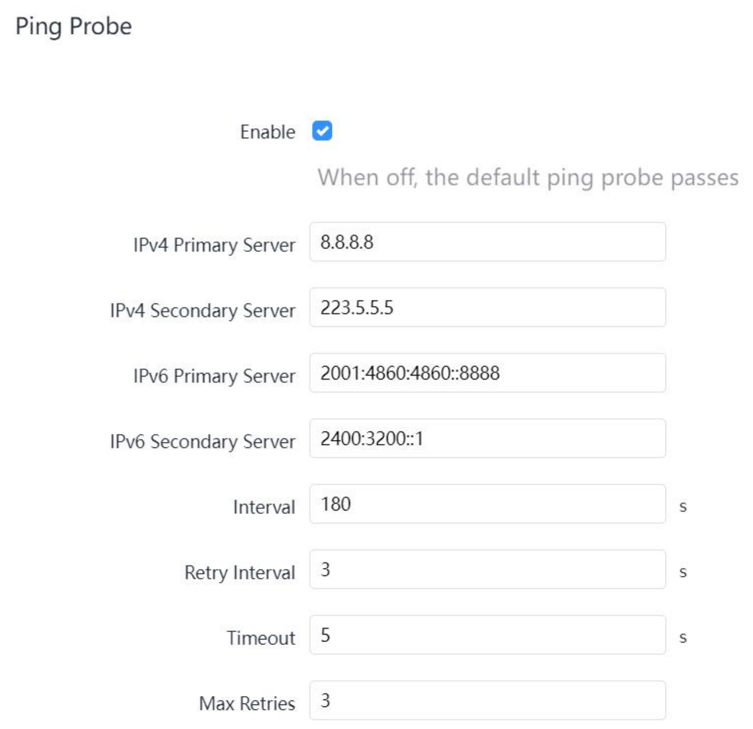
After checking, it will periodically detect whether the higher priority link is available.If a higher priority link is available, it will switch to the link with a higher priority.

Revert Interval 180 s

Emergency Reboot □

After enabling, if all interfaces are unavailable, the system will reboot.

Link Failover	
Item	**Description**
Link Priority	
Priority	Display the priority of each interface, you can modify it by the operation's **up** and **down** button.
Enable Rule	If enabled, the device will choose this interface into its switching rule. For the Cellular interface, if it's not enabled here, the interface will be disabled as well.
Link in Use	Mark whether this interface is in use with Green color.
Interface	Display the name of the interface.
Connection type	Display how to obtain the IP address in this interface, like static IP or DHCP. For cellular interface, it only supports as DHCP client.
IP	Display the IP address of the interface.
☰	Drag this button to adjust the priority of network links. The top of the list has the highest priority.
Edit	Click to edit ping probe settings of every network link.
Settings	
Revert to High Priority Link	When enabled, periodically detect whether the high-priority link can be pinged, and if so, switch the link with a higher priority.
Revert Interval	Specify the number of seconds that you should wait for switching to the link with higher priority, range: 1 - 21600s.
Emergency Reboot	Enable to reboot the device if not any link is available.



Ping Probe

Enable ☑

When off, the default ping probe passes

IPv4 Primary Server 8.8.8.8

IPv4 Secondary Server 223.5.5.5

IPv6 Primary Server 2001:4860:4860::8888

IPv6 Secondary Server 2400:3200::1

Interval 180 s

Retry Interval 3 s

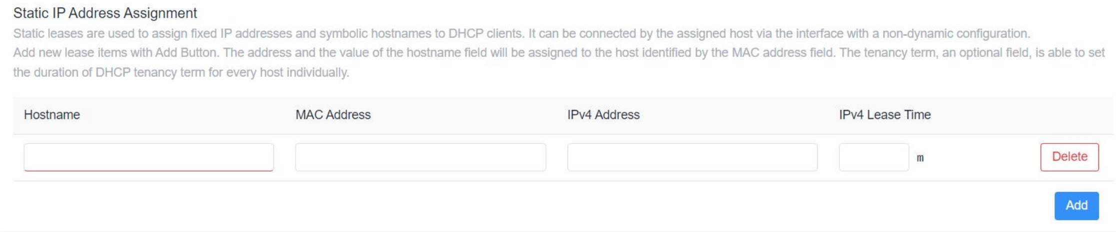
Timeout 5 s

Max Retries 3

Ping Probe	
Item	**Description**
Enable	If enabled, the device will periodically detect the connection status of the link by sending ICMP packets.
IPv4/IPv6 Primary Server	The device will send ICMP packet to the IPv4/IPv6 address to determine whether the network connection is still available or not.
IPv4/IPv6 Secondary Server	The device will try to ping the alternative server address if primary server is not available.
Interval	Time interval (in seconds) between two Pings.
Retry Interval	Set the ping retry interval. When ping failed, the device will ping again in every retry interval.
Timeout	The maximum amount of time the device will wait for a response to a ping request. If it does not receive a response for the amount of time predefined in this field, the ping request will be considered as fail.
Max Retries	The retry times of the device sending ping request until determining that the connection has failed.

7.2.1.6 Static IP Address Assignment

When LAN interface works as DHCP server, users can assign fixed IP addresses and symbolic hostnames to devices with fixed MAC addresses.



Static IP Address Assignment

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. It can be connected by the assigned host via the interface with a non-dynamic configuration.

Add new lease items with Add Button. The address and the value of the hostname field will be assigned to the host identified by the MAC address field. The tenancy term, an optional field, is able to set the duration of DHCP tenancy term for every host individually.

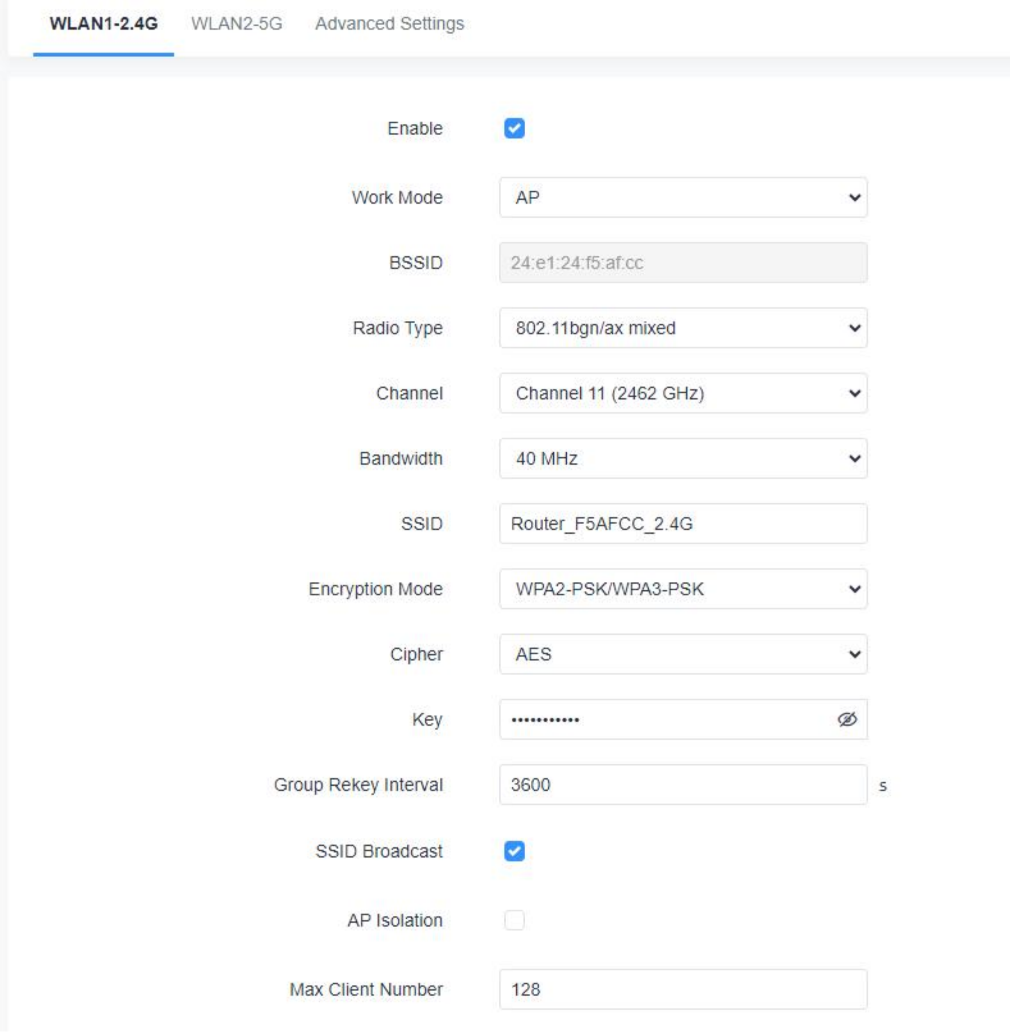
Hostname	MAC Address	IPv4 Address	IPv4 Lease Time	
			m	Delete

Static IP Address Assignment	
Item	**Description**
Hostname	The hostname of static leases.
MAC Address	The MAC address of the DHCP client.
IPv4 Address	The IPv4 address assigned to the client.
IPv4 Lease time	Time remaining for the client.

7.2.2 WLAN (Wi-Fi Version Only)

7.2.2.1 WLAN

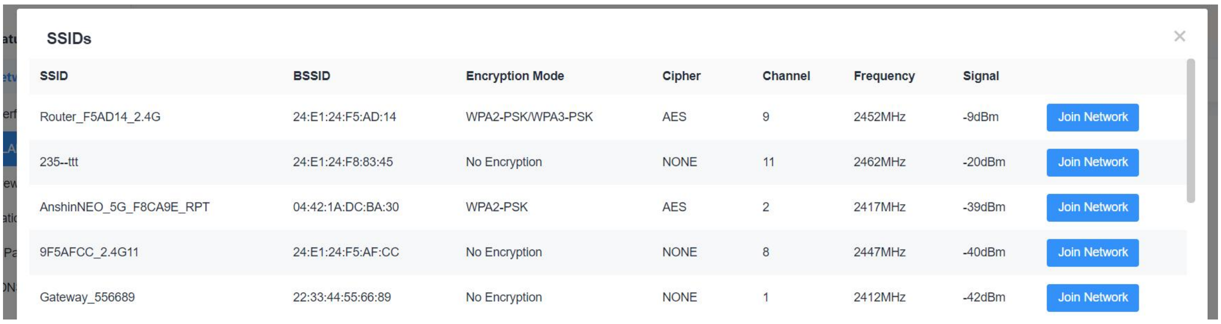
This section explains how to set the related parameters for Wi-Fi network. UF51 supports both 2.4G and 5G Wi-Fi and they can work at the same time.



Enable	☑
Work Mode	AP
BSSID	24:e1:24:f5:af:cc
Radio Type	802.11bgn/ax mixed
Channel	Channel 11 (2462 GHz)
Bandwidth	40 MHz
SSID	Router_F5AFCC_2.4G
Encryption Mode	WPA2-PSK/WPA3-PSK
Cipher	AES
Key	•••••••••••
Group Rekey Interval	3600 s
SSID Broadcast	☑
AP Isolation	□
Max Client Number	128

WLAN	
Item	**Description**
Enable	Enable/disable WLAN.
Work Mode	Select router's work mode. The options are "Client" or "AP".
AP Mode	
BSSID	Show the MAC address of this WLAN interface.
Radio Type	Select Radio type.
Channel	Select wireless channel from 1 to 13 or select Auto.
Bandwidth	Select bandwidth. The options are 20MHz and 40MHz.
SSID	Fill in the SSID of the access point.
Encryption Mode	Select encryption mode. The options are No Encryption, WEP Open System , WEP Auto, WEP Shared Key, WPA-PSK, WPA2-PSK, WPA3-PSK, WPA-PSK/WPA2-PSK and WPA2-PSK/WPA3-PSK.
Cipher	Select the cipher when using PSK type encryption mode. The options are AES, TKIP and AES/TKIP.
Key	Fill the key to connect to this access point. The default key is **iotpassword**.
Group Rekey Interval	The interval of changing the cipher key.
SSID Broadcast	When SSID broadcast is disabled, other wireless devices can't not find the SSID, and users have to enter the SSID manually to access to the wireless network.
AP Isolation	When AP Isolation is enabled, all users who access to the AP are isolated and cannot communication with each other.
Max Client Number	Set the maximum number of clients to access when the router is configured as AP.
MAC Filtering	Enable to filter the clients to connect to this access point.
Type	Choose the filter type of devices connected to this router's wireless access point. **Whitelist:** Only the listed MAC addresses are allowed to connect to the router's wireless access point. **Blacklist:** The listed MAC addresses are not allowed to connect to the router's wireless access point.
MAC Address	The device MAC addresses which need to be blocked or allowed.
Description	The description of this MAC address.
Client Mode	
Scan	Click to scan the access points around this device.
SSID	Fill in the SSID of the access point.
BSSID	Fill in the MAC address of the access point. Either SSID or BSSID can be filled to join the network.
Channel	Select wireless channel from 1 to 13 or select Auto.
Encryption Mode	Select encryption mode. The options are No Encryption, WPA-PSK, WPA2-PSK, WPA3-PSK, WPA-PSK/WPA2-PSK and WPA2-PSK/WPA3-PSK.

Cipher	Select the cipher of WPA encryption. The options are “AES", “TKIP" and “AES/TKIP".
Key	Fill the key to connect to this access point.
IP Setting	
Protocol	Set the protocol to get the WLAN IP address.
IPv4 Address	Set the IP address in wireless network when protocol is Static IP. Note that the subnet of this IP address should be different from WAN port.
Netmask	Set the netmask in wireless network when protocol is Static IP.
Gateway	Set the gateway in wireless network when protocol is Static IP.
Preferred DNS	Set the primary IPv4 DNS server.
Alternative DNS	Set the secondary IPv4 DNS server.



SSIDs

SSID	BSSID	Encryption Mode	Cipher	Channel	Frequency	Signal	
Router_F5AD14_2.4G	24:E1:24:F5:AD:14	WPA2-PSK/WPA3-PSK	AES	9	2452MHz	-9dBm	Join Network
235--ttt	24:E1:24:F8:83:45	No Encryption	NONE	11	2462MHz	-20dBm	Join Network
AnshinNEO_5G_F8CA9E_RPT	04:42:1A:DC:BA:30	WPA2-PSK	AES	2	2417MHz	-39dBm	Join Network
9F5AFCC_2.4G11	24:E1:24:F5:AF:CC	No Encryption	NONE	8	2447MHz	-40dBm	Join Network
Gateway_556689	22:33:44:55:66:89	No Encryption	NONE	1	2412MHz	-42dBm	Join Network

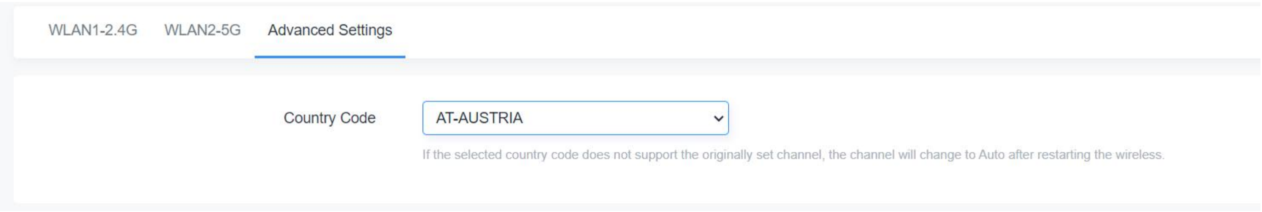
WLAN-Scan	
Item	**Description**
SSID	Show SSID.
BSSID	Show the MAC address of the access point.
Encryption Mode	Show the encryption mode.
Cipher	Show the cipher of the access point.
Channel	Show wireless channel.
Frequency	Show the frequency of radio.
Signal	Show wireless signal.
Join Network	Click the button to join the wireless network.

Related Topic

Wi-Fi Application Example

7.2.2.2 Advanced Settings

The device supports to select the country code to adjust the channel and TX power.



WLAN1-2.4G WLAN2-5G Advanced Settings

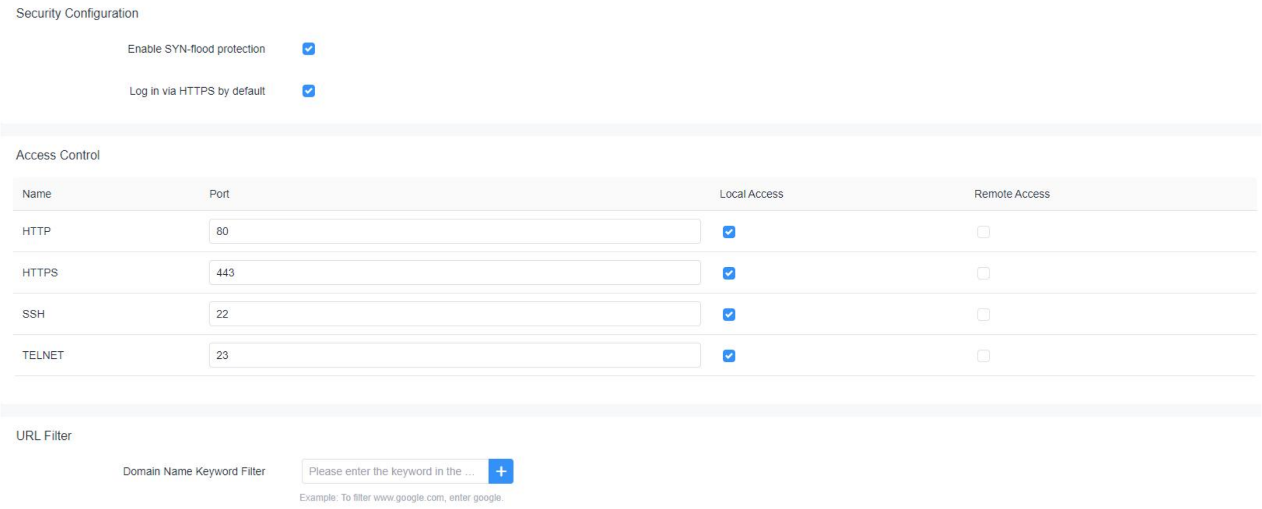
Country Code: AT-AUSTRIA

If the selected country code does not support the originally set channel, the channel will change to Auto after restarting the wireless.

7.2.3 Firewall

This section describes how to set the firewall parameters, including security, ACL, DMZ, Port Mapping and custom iptables rules. After setting, users can go to **Status > Firewall** to check if firewall settings work.

7.2.3.1 General Settings



Security Configuration

Enable SYN-flood protection ☑

Log in via HTTPS by default ☑

Access Control

Name	Port	Local Access	Remote Access
HTTP	80	☑	☐
HTTPS	443	☑	☐
SSH	22	☑	☐
TELNET	23	☑	☐

URL Filter

Domain Name Keyword Filter: Please enter the keyword in the ... +

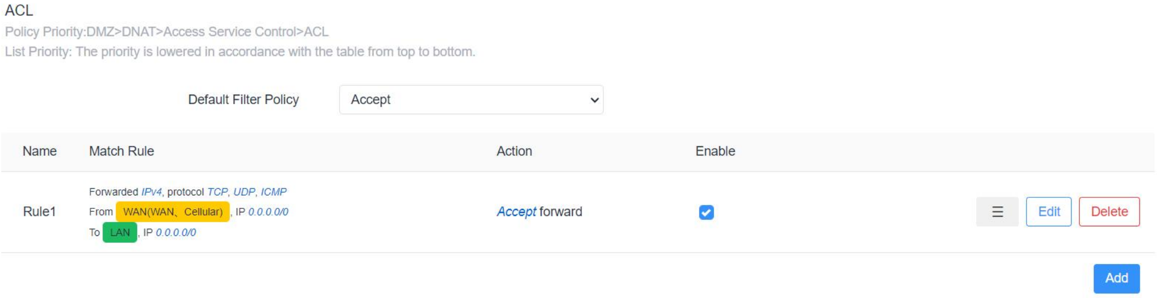
Example: To filter www.google.com, enter google.

General Setting		
Item	**Description**	**Default**
Security Configuration		
Enable SYN-flood Protection	Enable/disable SYN-flood protection. SYN-flood protection allows to protect from a DDoS attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive.	Enable
Log in using HTTPS by default	Log in the web GUI of device via HTTPS by default.	Enable
Access Control		
Port	Set port number of the services. Range: 1-65535.	--
Local Access	Access the device locally.	Enable
Remote Access	Access the device remotely.	Disable
HTTP	Users can log in the device locally via HTTP to access and control it through Web after the option	80

	is checked.	
HTTPS	Users can log in the device locally and remotely via HTTPS to access and control it through Web after the option is checked.	443
TELNET	Users can log in the device locally and remotely via Telnet after the option is checked.	23
SSH	Users can log in the device locally and remotely via SSH after the option is checked.	22
URL Filter		
Domain Name Keyword Filter	You can block specific website by entering keyword from a domain name. After filtering, the devices under LAN ports can not access corresponding websites. The maximum number of characters allowed is 64.	

7.2.3.2 ACL

The 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 a device receives a 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

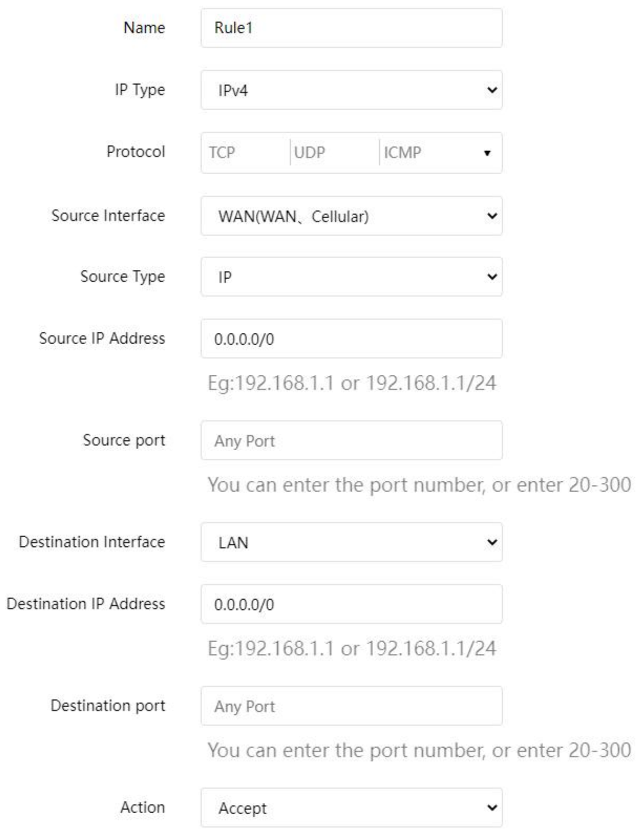
Policy Priority:DMZ>DNAT>Access Service Control>ACL

List Priority: The priority is lowered in accordance with the table from top to bottom.

Default Filter Policy: Accept

Name	Match Rule	Action	Enable	
Rule1	Forwarded IPv4, protocol TCP, UDP, ICMP From WAN(WAN、Cellular), IP 0.0.0.0/0 To LAN, IP 0.0.0.0/0	Accept forward	☑	☰ Edit Delete

ACL	
Item	**Description**
Default Filter Policy	The packets which are not included in the access control list will be processed by the default filter policy. **Accept:** allow all traffic out of devices under LAN ports. **Drop:** deny all traffic out of devices under LAN ports.
Enable	Enable this ACL rule.
☰	Drag this button to adjust the priority of ACL rules. The top of the list has the highest priority.
Edit	Click to edit the details of this ACL rule.
Delete	Delete this ACL rule.

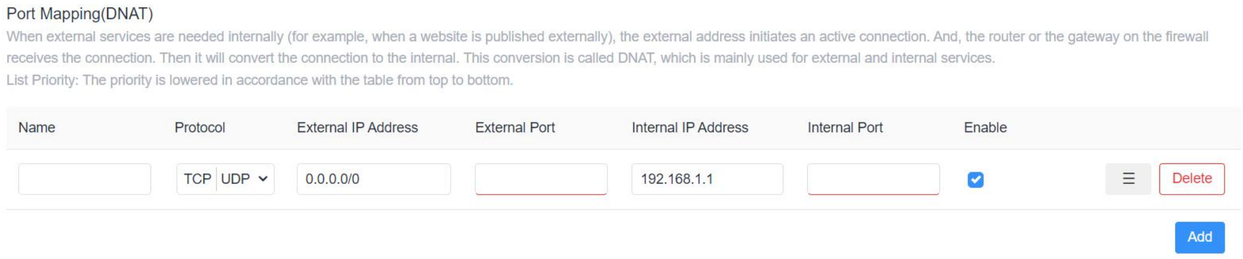


Name	Rule1
IP Type	IPv4
Protocol	TCP UDP ICMP
Source Interface	WAN(WAN、Cellular)
Source Type	IP
Source IP Address	0.0.0.0/0 Eg:192.168.1.1 or 192.168.1.1/24
Source port	Any Port You can enter the port number, or enter 20-300
Destination Interface	LAN
Destination IP Address	0.0.0.0/0 Eg:192.168.1.1 or 192.168.1.1/24
Destination port	Any Port You can enter the port number, or enter 20-300
Action	Accept

ACL - Add/Edit	
Name	Define a unique name for this ACL rule.
Type	Select type as IPv4 or IPv6.
Protocol	Select protocol among TCP, UDP and ICMP.
Source Interface	Select the source interface type from Device Output, LAN, VLAN or WAN (WAN, Cellular, WLAN). Device Output means the packets coming from device itself.
Source Type	When using IPv4 type, select the address type as IP, MAC or IP+MAC.
Source IP/MAC Address	Set source network address according to address type. (0.0.0.0/0 means all).
Source Port	Set specific source port number or port range, example: 20-300.
Destination Interface	Select the destination interface type from LAN, WAN (WAN, Cellular, WLAN), VLAN or Device Input. Device Input means the packets going to device itself.
Destination IP Address	Set destination network address (0.0.0.0/0 means all).
Destination Port	Set specific source port number or port range, example: 20-300.
Action	Select action as Accept or Drop.

7.2.3.3 Port Mapping (DNAT)

When external services are needed internally (for example, when a website is published externally), th e external address initiates an active connection. And, the device or the gateway on the firewall receiv es 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(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 to the internal. This conversion is called DNAT, which is mainly used for external and internal services.

List Priority: The priority is lowered in accordance with the table from top to bottom.

Name	Protocol	External IP Address	External Port	Internal IP Address	Internal Port	Enable		
	TCP UDP	0.0.0.0/0		192.168.1.1		☑	☰	Delete

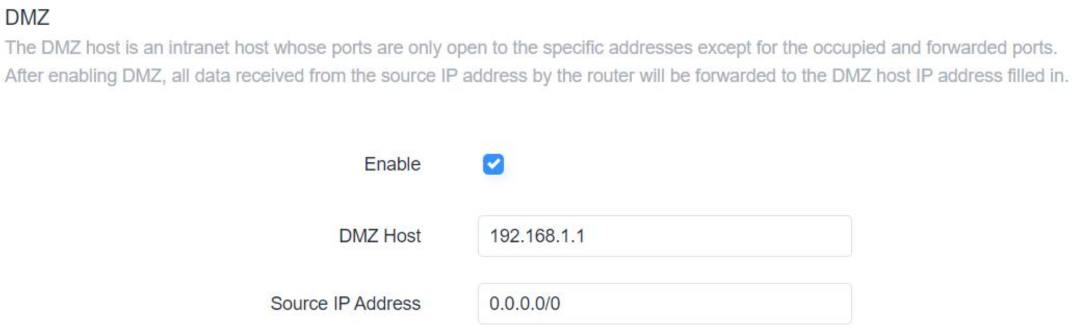
Port Mapping (DNAT)	
Item	**Description**
Name	Define a unique name of the port mapping rule.
Protocol	Select TCP or UDP for your application requirements.
External IP Address	Specify the host or network which can access local IP address. 0.0.0.0/0 means all.
External Port	Set the port or port range from which incoming packets are forwarded, example: 20-300.
Internal IP Address	Enter the IP address that packets are forwarded to after receiving from the incoming interface.
Internal Port	Enter the port or port range that packets are forwarded to after receiving from the incoming port(s). When setting port range, the value should be the same as external port range.
Enable	Enable or disable this port mapping rule.
☰	Drag this button to adjust the priority of port mapping rules. The top of the list has the highest priority.
Delete	Delete this rule.

Related Configuration Example

NAT Application Example

7.2.3.4 DMZ

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



DMZ

The DMZ host is an intranet host whose ports are only open to the specific addresses except for the occupied and forwarded ports. After enabling DMZ, all data received from the source IP address by the router will be forwarded to the DMZ host IP address filled in.

Enable ☑

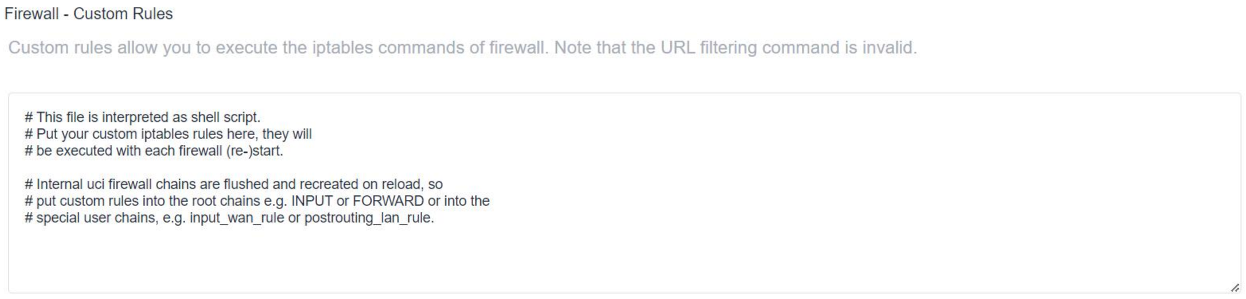
DMZ Host 192.168.1.1

Source IP Address 0.0.0.0/0

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

7.2.3.5 Custom Rules

In this page, you can enter your own custom firewall iptables rules and these will get executed as a Linux shell script.



Firewall - Custom Rules

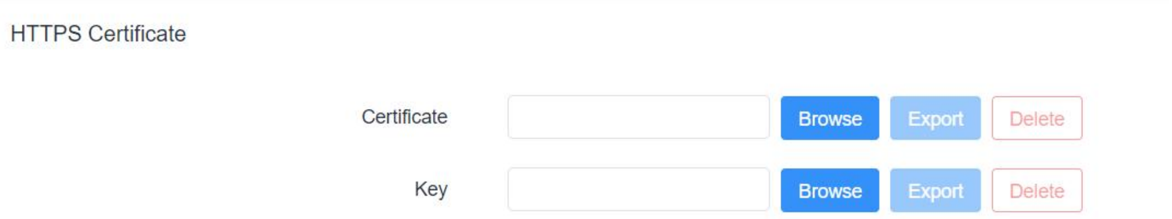
Custom rules allow you to execute the iptables commands of firewall. Note that the URL filtering command is invalid.

```
# This file is interpreted as shell script.
# Put your custom iptables rules here, they will
# be executed with each firewall (re-)start.

# Internal uci firewall chains are flushed and recreated on reload, so
# put custom rules into the root chains e.g. INPUT or FORWARD or into the
# special user chains, e.g. input_wan_rule or postrouting_lan_rule.
```

7.2.3.6 Certificates

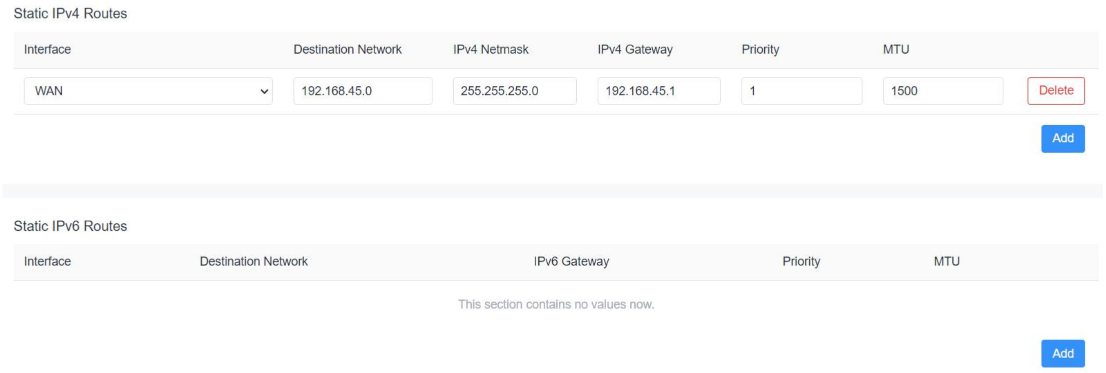
In this page, you can import the HTTPS certificates for device web GUI secure access.



HTTPS Certificate

7.2.4 Static Routes

A static routing is a manually configured routing entry. Information about the routing is manually entered rather than obtained from dynamic routing traffic. After setting static routing, the package for the specified destination will be forwarded to the path designated by users.



Static IPv4 Routes

Interface	Destination Network	IPv4 Netmask	IPv4 Gateway	Priority	MTU
WAN	192.168.45.0	255.255.255.0	192.168.45.1	1	1500

Static IPv6 Routes

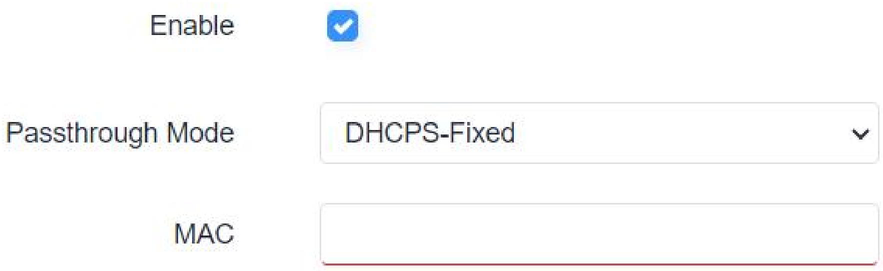
Interface	Destination Network	IPv6 Gateway	Priority	MTU

This section contains no values now.

Static Routes	
Item	**Description**
Interface	The interface allows the data to reach the destination address.
Destination Network	Enter the destination IPv4/IPv6 address.
IPv4 Netmask	Enter the subnet mask of IPv4 destination address.
IPv4/IPv6 Gateway	IPv4/IPv6 address of the next device that will be passed by before the input data reaches the destination address.
Priority	Smaller value refers to higher priority. Range: 1-255.
MTU	Set the maximum transmission unit. Range: 68-1500.

7.2.5 IP Passthrough

IP Passthrough mode shares or "passes" the Internet providers assigned IP address to a single LAN client device connected to the device.



Enable ☑

Passthrough Mode: DHCPS-Fixed

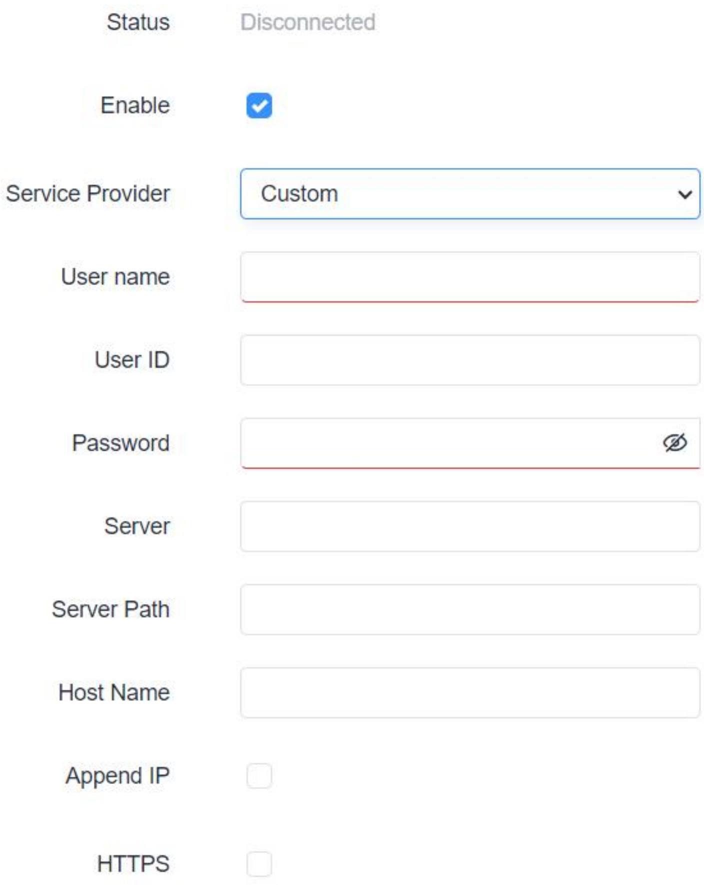
MAC

IP Passthrough	
Item	**Description**
Enable	Enable or disable IP Passthrough.
Passthrough Mode	Select passthrough mode from “DHCPS-Fixed” and “DHCPS-Dynamic”.
MAC	Set MAC address when passthrough mode is “DHCPS-Fixed”.

7.2.6 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.

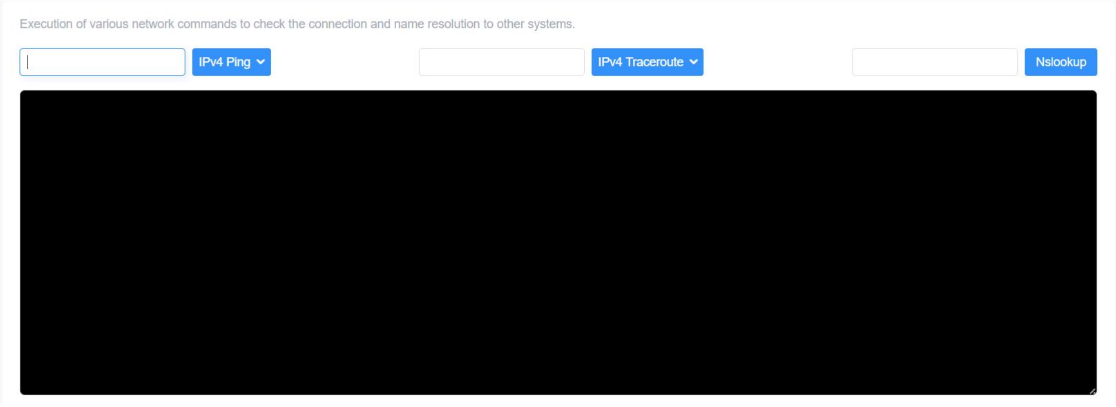


Status	Disconnected
Enable	☑
Service Provider	Custom
User name	
User ID	
Password	
Server	
Server Path	
Host Name	
Append IP	☐
HTTPS	☐

DDNS	
Item	**Description**
Status	Show connection status of DDNS.
Enable	Enable/disable DDNS.
Service Provider	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.
Server Path	By default the hostname is appended to the path.
Hostname	Enter the hostname for DDNS.
Append IP	Append your current IP to the DDNS server update path.
HTTPS	Enable HTTPS for some DDNS providers.

7.2.7 Diagnostics

Network Utilities includes IPv4/IPv6 ping, IPv4/IPv6 traceroute, nslookup the command-line tool.



Execution of various network commands to check the connection and name resolution to other systems.

Network Utilities	
Item	**Description**
IPv4 Ping	Click to ping outer network from the device in IPv4.
IPv6 Ping	Click to ping outer network from the device in IPv6.
IPv4 Traceroute	Address of the destination host to be detected in IPv4.
IPv6 Traceroute	Address of the destination host to be detected in IPv6.
Nslookup	Click to obtain the mapping between domain name and IP address, or other DNS records.

7.3 VPN

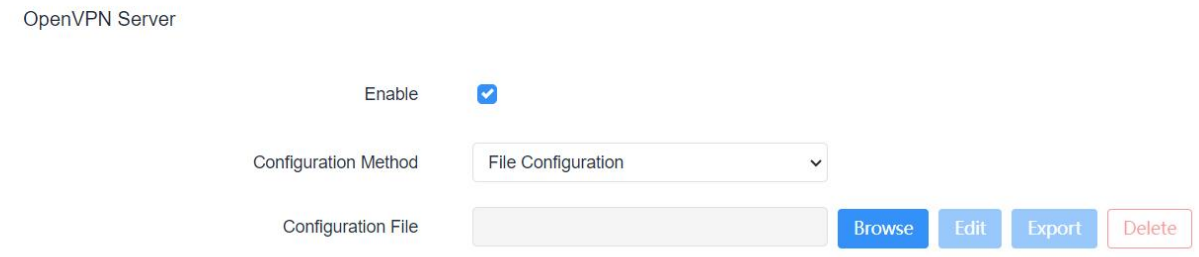
Virtual Private Networks, also called VPNs, are used to securely connect two private networks together so that devices can connect from one network to the other network via secure channels.

7.3.1 OpenVPN

OpenVPN is an open source virtual private network (VPN) product that offers a simplified security framework, modular network design, and cross-platform portability. The default OpenVPN version of UF51 is 2.5.3.

7.3.1.1 OpenVPN Server

UF51 supports OpenVPN server to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. You can import the ovpn file directly or configure the parameters on this page to set this server.



OpenVPN Server

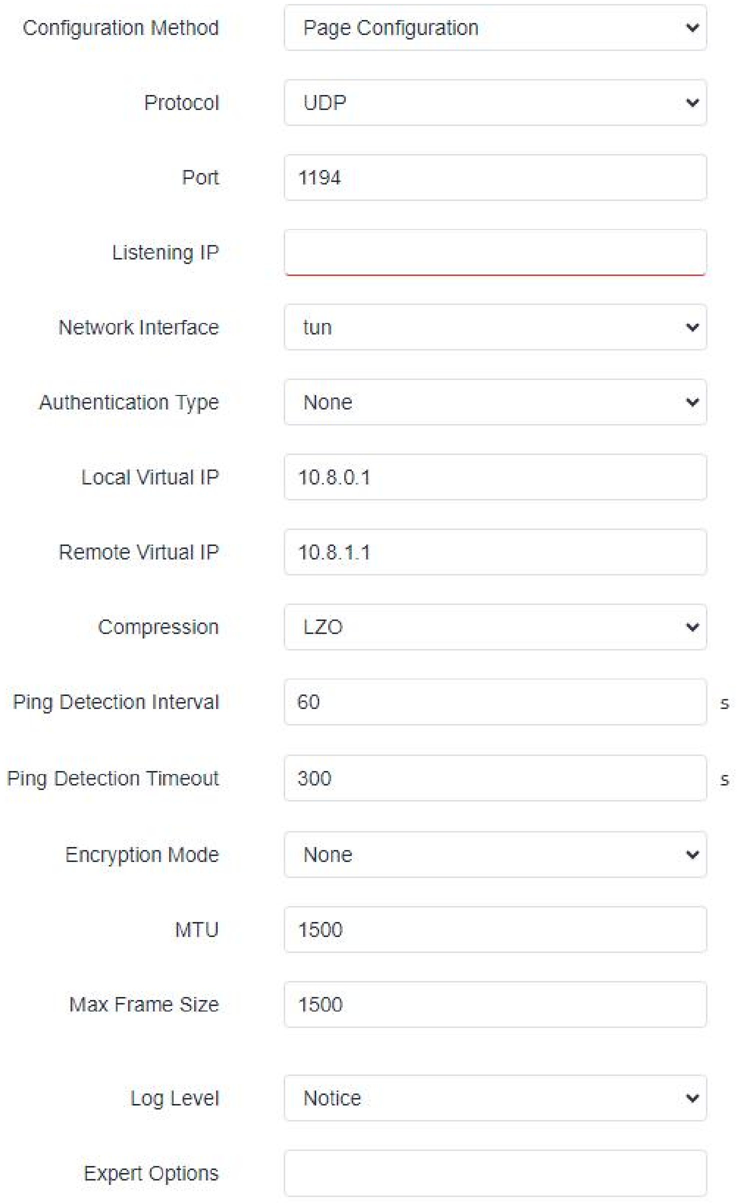
Enable ☑

Configuration Method: File Configuration

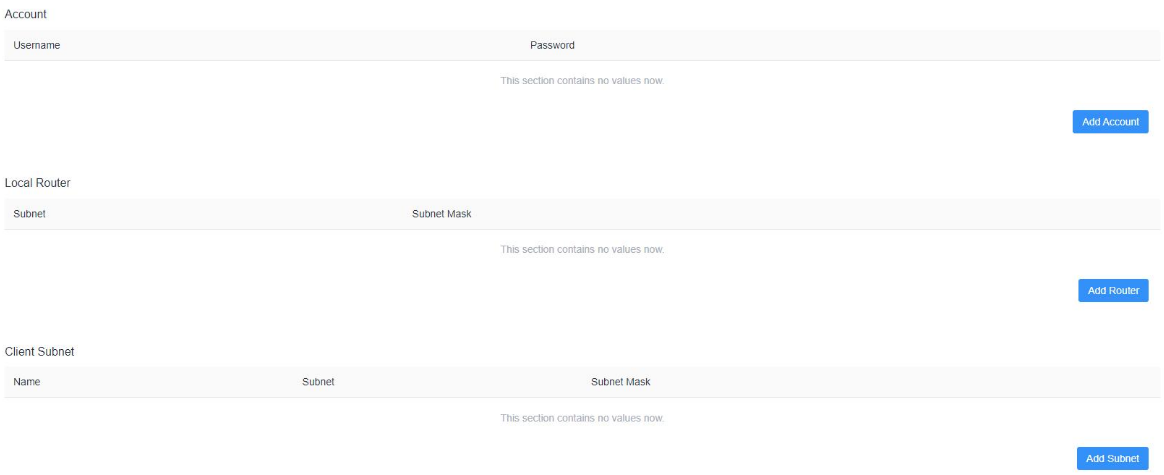
Configuration File

OpenVPN Server - File Configuration

Item	Description
Browse	Click to browse the server configuration ovpn format file including the settings and certificate contents. Please refer to the server configuration file according to sample: server.conf
Edit	Click to edit the imported file.
Export	Export the server configuration file.
Delete	Click to delete the configuration file.



Configuration Method	Page Configuration
Protocol	UDP
Port	1194
Listening IP	
Network Interface	tun
Authentication Type	None
Local Virtual IP	10.8.0.1
Remote Virtual IP	10.8.1.1
Compression	LZO
Ping Detection Interval	60 s
Ping Detection Timeout	300 s
Encryption Mode	None
MTU	1500
Max Frame Size	1500
Log Level	Notice
Expert Options	



Account

Username	Password

This section contains no values now.

Local Router

Subnet	Subnet Mask

This section contains no values now.

Client Subnet

Name	Subnet	Subnet Mask

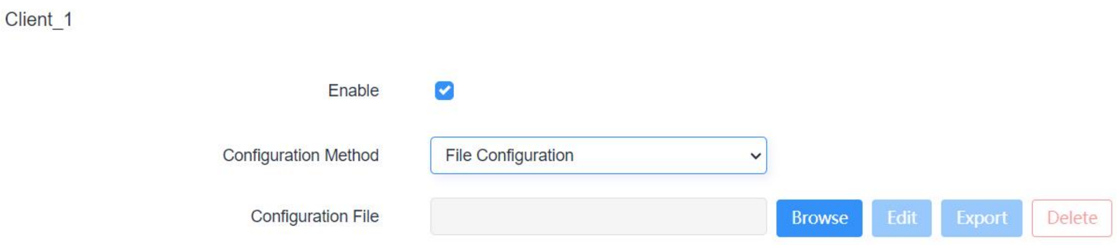
This section contains no values now.

OpenVPN Server - Page Configuration	
Item	**Description**
Protocol	Select a transport protocol used by connection from UDP and TCP.
Listening IP	Enter the local hostname or IP address for bind. If left blank, OpenVPN server will bind to all interfaces.
Port	Enter the TCP/UCP service number for OpenVPN client connection. Range: 1-65535.
Network 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 Type	Select authentication type used to secure data sessions. **Pre-shared:** use the same secret key as server to complete the authentication. After select, go to **VPN > OpenVPN > 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 select, go to **VPN > OpenVPN > 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	Renegotiate data channel key after this interval. 0 means disable.
Max Clients	Limit server to a maximum of concurrent clients, range: 1-128. **Note:** please adjust log severity to Info if you need to connect many clients.
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 TLS Authentication	Disable or enable TLS authentication when authentication type is X.509 cert. After being enabled, go to **VPN > OpenVPN > 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
Compression	Select to enable or disable LZO to compress data.
Ping Detection Interval	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.
Ping Detection Timeout	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.
Encryption Mode	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: 68-1500.
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
Account	
Username & Password	Set username and password for OpenVPN client when authentication type is username/password.
Local Router	
Subnet	Set the local route's IP address.
Subnet Mask	Set the local route's netmask.
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.

7.3.1.2 OpenVPN Client

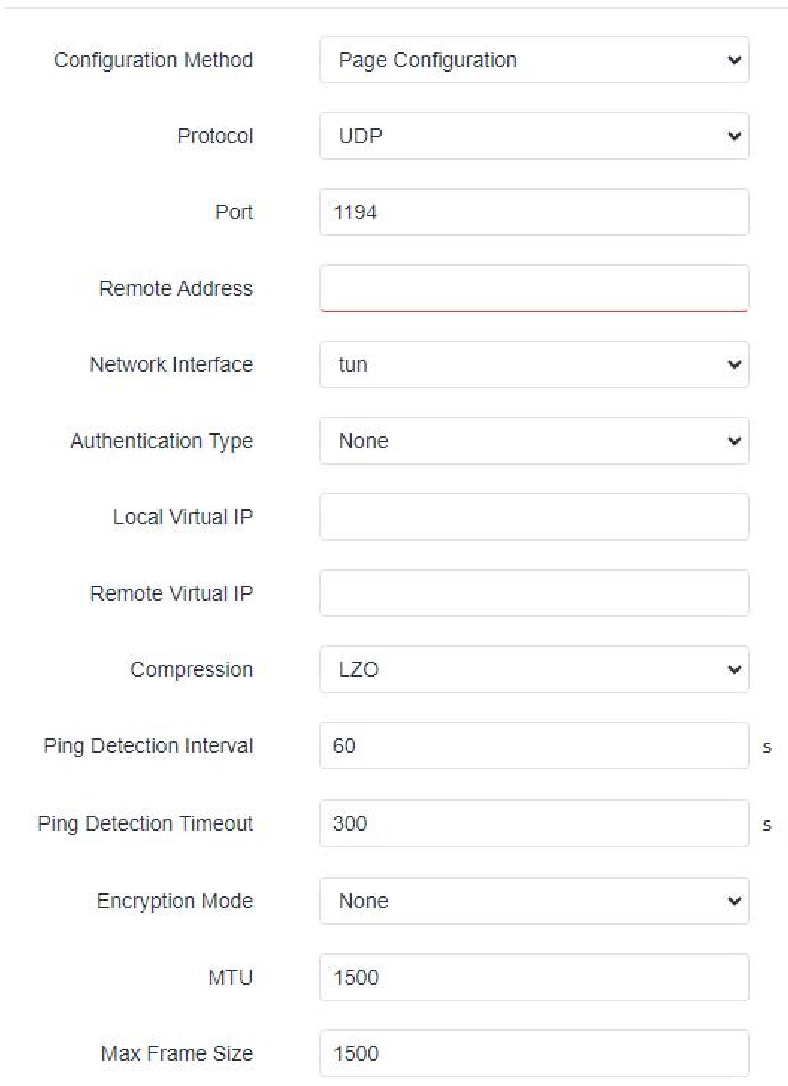
UF51 supports running at most 3 OpenVPN clients at the same time. You can import the ovpn file directly or configure the parameters on this page to set clients.



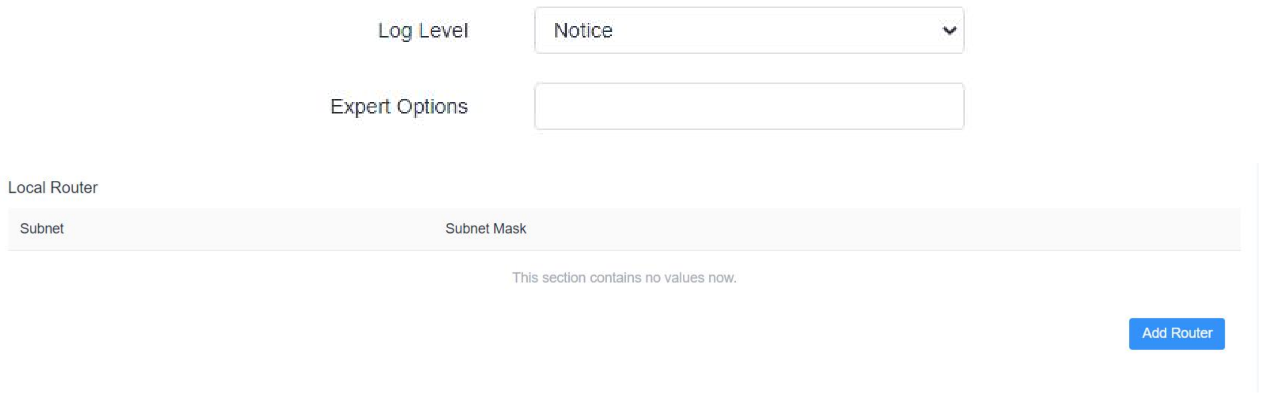
Client_1

Enable	☑
Configuration Method	File Configuration
Configuration File	

OpenVPN Client - File Configuration	
Item	**Description**
Browse	Click to browse the client configuration ovpn format file including the settings and certificate contents. Please refer to the client configuration file according to sample: client.conf
Edit	Click to edit the imported file.
Export	Export the server configuration file.
Delete	Click to delete the configuration file.



Configuration Method	Page Configuration
Protocol	UDP
Port	1194
Remote Address	
Network Interface	tun
Authentication Type	None
Local Virtual IP	
Remote Virtual IP	
Compression	LZO
Ping Detection Interval	60 s
Ping Detection Timeout	300 s
Encryption Mode	None
MTU	1500
Max Frame Size	1500



Log Level: Notice

Expert Options:

Local Router

Subnet	Subnet Mask

This section contains no values now.

OpenVPN Client - Page Configuration	
Item	**Description**
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.
Network 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 Type	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 **VPN > OpenVPN > 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 **VPN > OpenVPN > 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**.
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 **VPN > OpenVPN > 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
Compression	Select to enable or disable LZO to compress data.
Ping Detection Interval	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

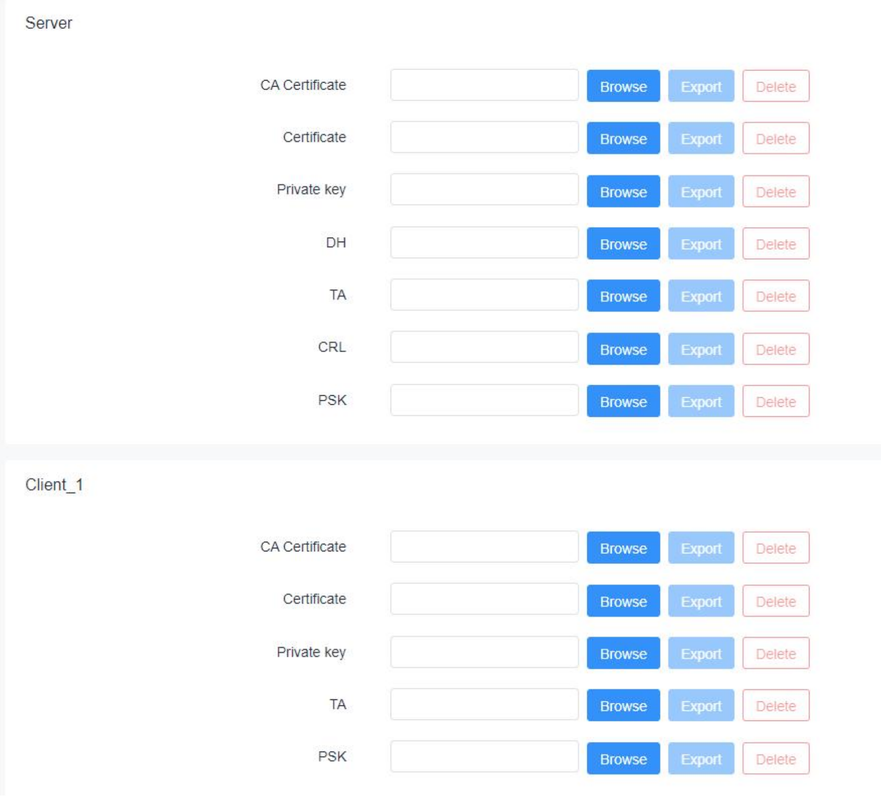
	client local values. Range: 10-1800 s.
Ping Detection Timeout	OpenVPN will be reestablished after timeout. If this is set on both server and client, the value pushed from server will override the client local values. Range: 60-3600 s.
Encryption Mode	Select from NONE, BF-CBC, DES-CBC, DES-EDE3-CBC, AES-128-CBC, 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.

Related Configuration Example

OpenVPN Client Application Example

7.3.1.3 Certificate

When using page configuration of OpenVPN server or client, user can import/export necessary certificate and key files to this page according to the authentication types.

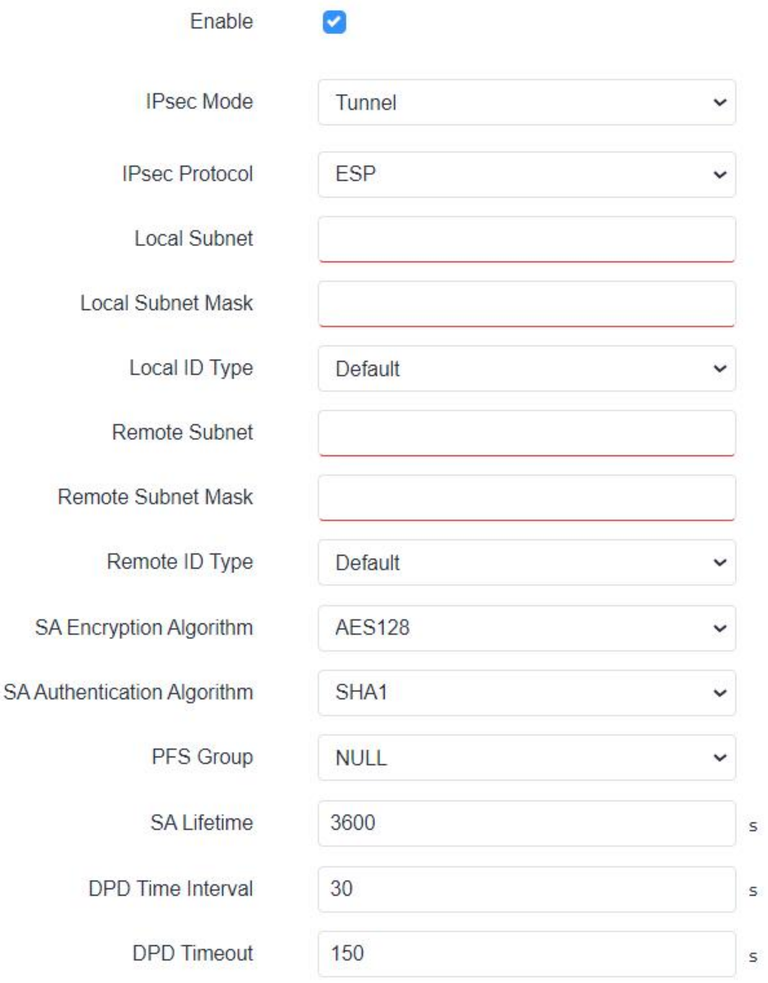


7.3.2 IPsecVPN

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 computer.

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 authentications 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.

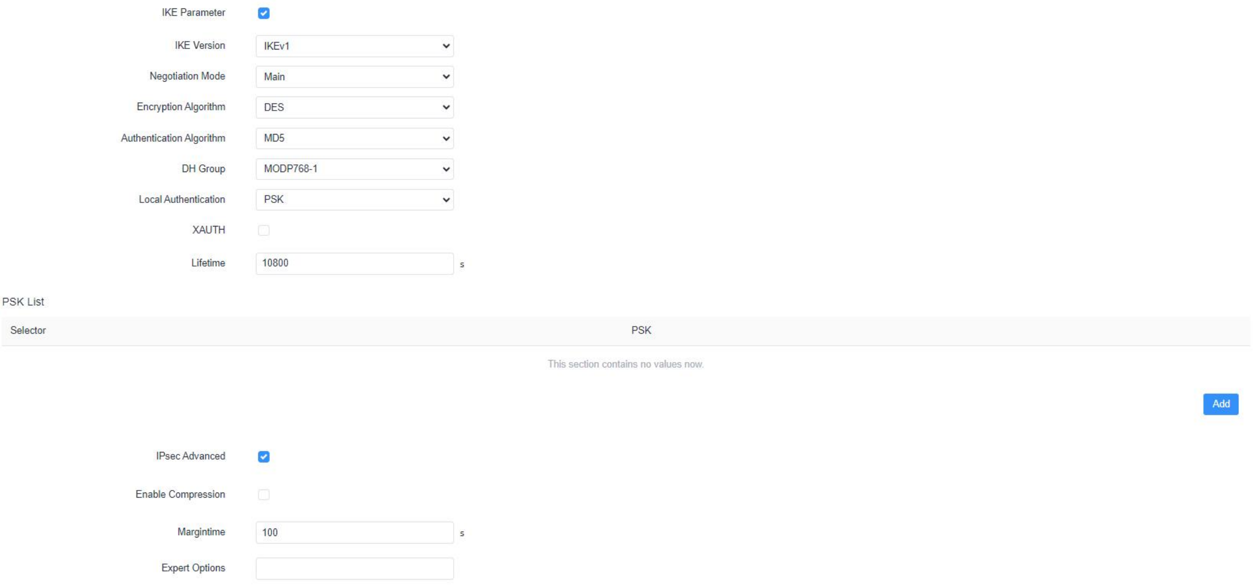
7.3.2.1 IPSec Server



Enable	☑	
IPsec Mode	Tunnel	
IPsec Protocol	ESP	
Local Subnet		
Local Subnet Mask		
Local ID Type	Default	
Remote Subnet		
Remote Subnet Mask		
Remote ID Type	Default	
SA Encryption Algorithm	AES128	
SA Authentication Algorithm	SHA1	
PFS Group	NULL	
SA Lifetime	3600	s
DPD Time Interval	30	s
DPD Timeout	150	s

IPsec Server	
Item	**Description**
Enable	Enable or disable IPsec server mode.
IPsec Mode	Select Tunnel or Transport.
IPsec Protocol	Select from 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, and send it 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 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
SA Encryption Algorithm	Select AES128, AES192 or AES256.
SA Authentication Algorithm	Select SHA1 or SHA2-256.
PFS Group	Select NULL, MODP768_1 , MODP1024_2 or MODP1536_5.
SA Lifetime	Set the lifetime of IPsec SA. Range: 60-86400 s.
DPD Interval Time	Set DPD retry interval to send DPD requests. Range: 2-60 s
DPD Timeout	When using IKE V1, set DPD timeout to detect the remote side fails. Range: 10-3600s.



IKE Parameter ☑

IKE Version: IKEv1

Negotiation Mode: Main

Encryption Algorithm: DES

Authentication Algorithm: MD5

DH Group: MODP768-1

Local Authentication: PSK

XAUTH □

Lifetime: 10800 s

PSK List

Selector	PSK

This section contains no values now.

IPsec Advanced ☑

Enable Compression □

Margintime: 100 s

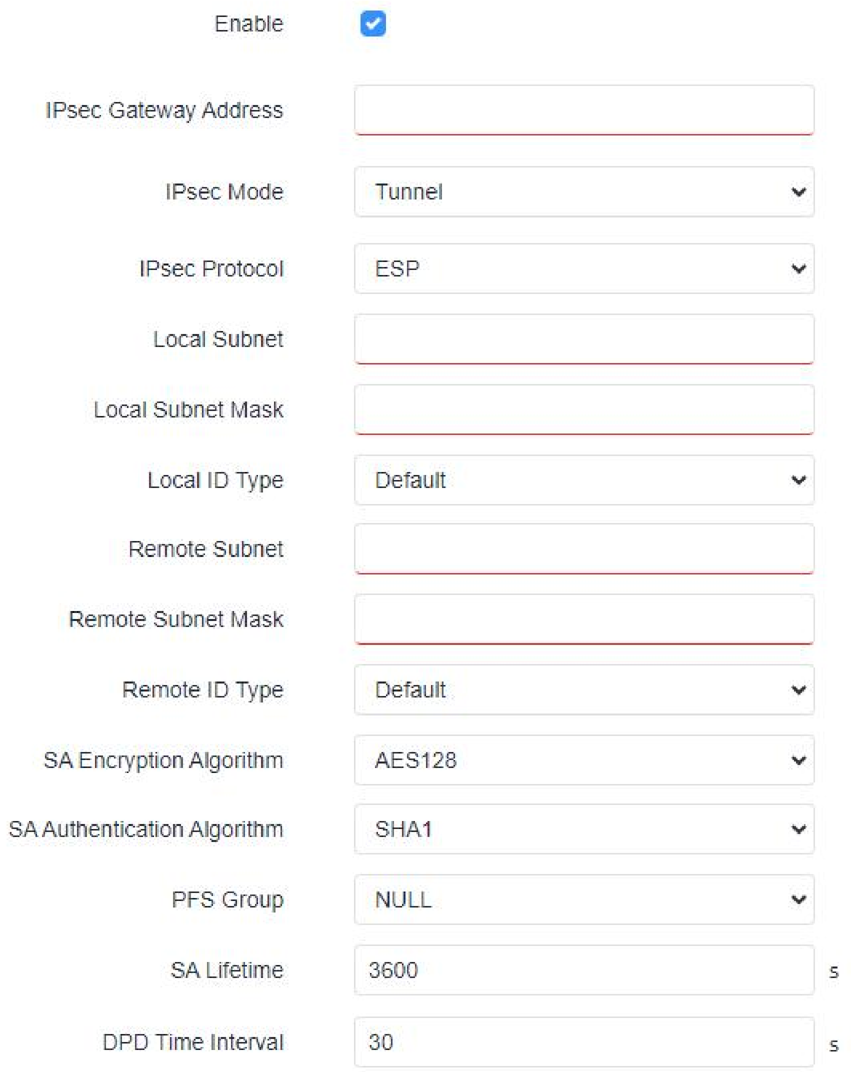
Expert Options:

IKE Parameter

Item	Description
IKE Version	Select the method of key exchange from IKEv1 and IKEv2.
Negotiation Mode	When using IKEv1, select Main or Aggressive.
Encryption Algorithm	Select DES, 3DES, AES128, AES192 or AES256.
Authentication Algorithm	Select MD5, SHA1 or SHA2-256.
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 **VPN > IPsec > Certifications** page to import CA certificate, local certificate and private key to corresponding fields.
Remote Authentication	When using IKEv2, 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	Set the lifetime in IKE negotiation. Range: 60-86400 s.
XAUTH List	
Username	Define the username used for the client xauth authentication.
Password	Define the password used for the client xauth authentication.
PSK List	
Selector	Set the selector as IP address or local ID of IPsec client. If it is left blank, all clients can use this PSK to complete authentication.
PSK	Define the pre-shared key.
IPsec Advanced	
Enable Compression	The head of IP packet will be compressed after it's enabled.
Margintime	Set advanced time before the lifetime expires to begin the re-negotiation.
Expert Options	User can enter some other initialization strings in this field to add extra settings and separate the strings with semicolon.

7.3.2.2 IPSec Client

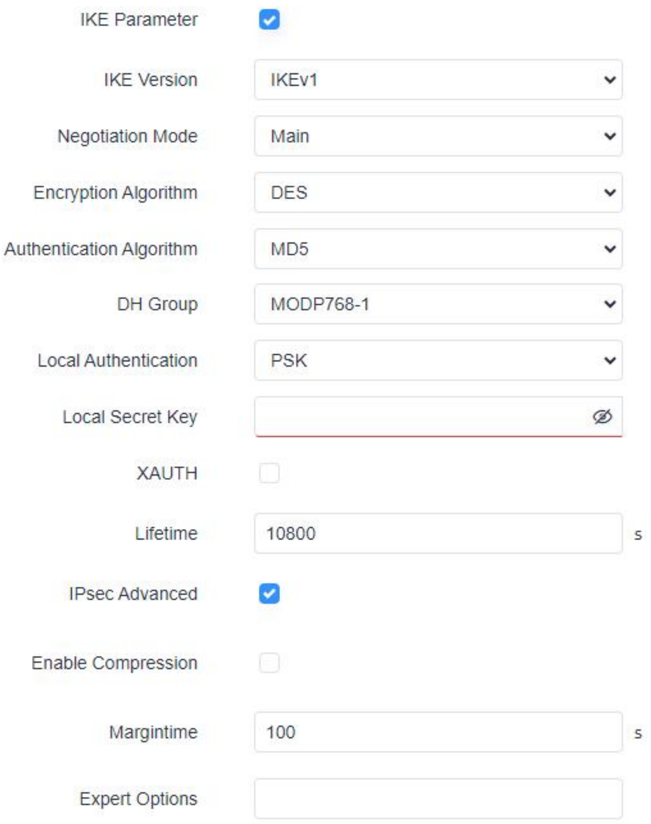
UF51 supports running at most 3 IPsec clients at the same time.



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
SA Encryption Algorithm	AES128
SA Authentication Algorithm	SHA1
PFS Group	NULL
SA Lifetime	3600 s
DPD Time Interval	30 s

IPsec Client	
Item	**Description**
Enable	Enable or disable IPsec client mode. A maximum of 3 tunnels is allowed.
IP Gateway Address	Enter the remote IPsec server address.
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
SA Encryption Algorithm	Select AES128, AES192 or AES256.
SA Authentication Algorithm	Select SHA1 or SHA2-256.
PFS Group	Select NULL, MODP768_1 , MODP1024_2 or MODP1536_5.
SA Lifetime	Set the lifetime of IPsec SA. Range: 60-86400 s.
DPD Interval Time	Set DPD retry interval to send DPD requests. Range: 2-60 s
DPD Timeout	When using IKEv1, set DPD timeout to detect the remote side fails. Range: 10-3600 s.



IKE Parameter ☑

IKE Version: IKEv1

Negotiation Mode: Main

Encryption Algorithm: DES

Authentication Algorithm: MD5

DH Group: MODP768-1

Local Authentication: PSK

Local Secret Key:

XAUTH □

Lifetime: 10800 s

IPsec Advanced ☑

Enable Compression □

Margintime: 100 s

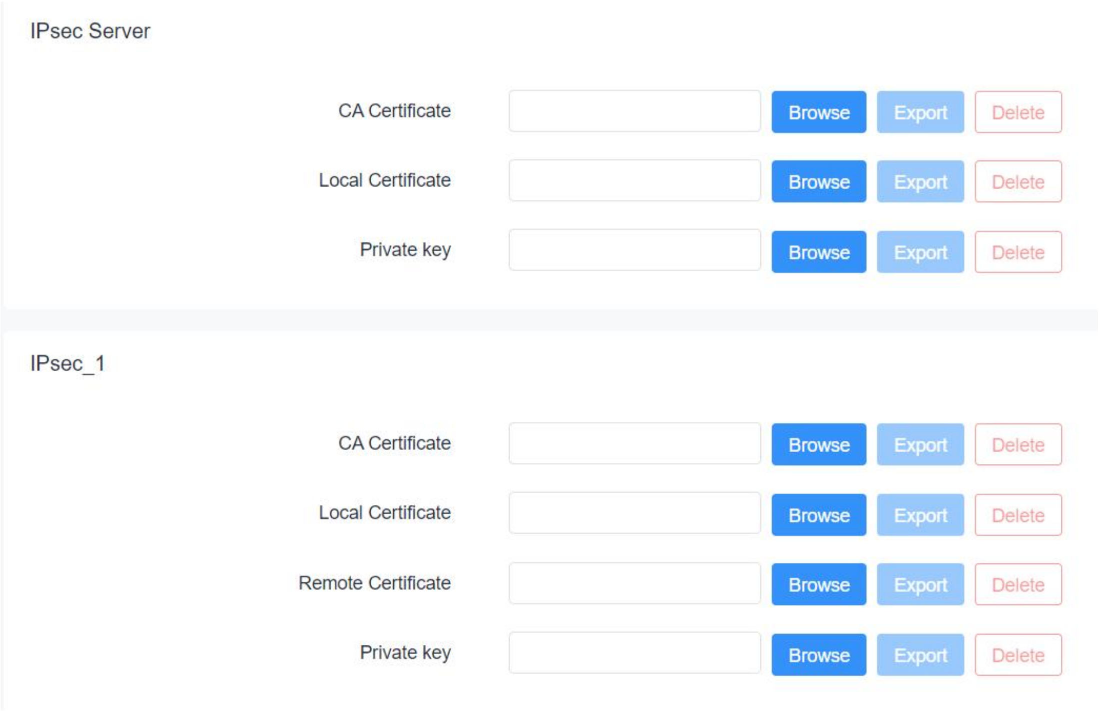
Expert Options:

IKE Parameter	
Item	**Description**
IKE Version	Select the method of key exchange of IKEv1 or IKEv2.
Negotiation Mode	When using IKEv1, select Main or Aggressive.
Encryption Algorithm	Select DES, 3DES, AES128, AES192 or AES256.
Authentication Algorithm	Select MD5, SHA1 or SHA2-256.

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 **VPN > IPsec > Certifications** page to import CA certificate, local certificate and private key to corresponding fields.
Local Secret Key	Enter the pre-shared key which is defined on serer side.
Remote Authentication	Select PSK or CA. **PSK:** use pre-shared key to complete the authentication. **CA:** use certificate to complete the authentication.
Remote Key	Enter the pre-shared key which is defined on server side.
XAUTH	When using IKEv1, define XAUTH username and password after XAUTH is enabled.
Lifetime	Set the lifetime in IKE negotiation. Range: 60-86400 s.
IPsec Advanced	
Enable Compression	The head of IP packet will be compressed after it's enabled.
Margintime	Set advanced time before the lifetime expires to begin the re-negotiation.
Expert Options	User can enter some other initialization strings in this field to add extra settings and separate the strings with semicolon.

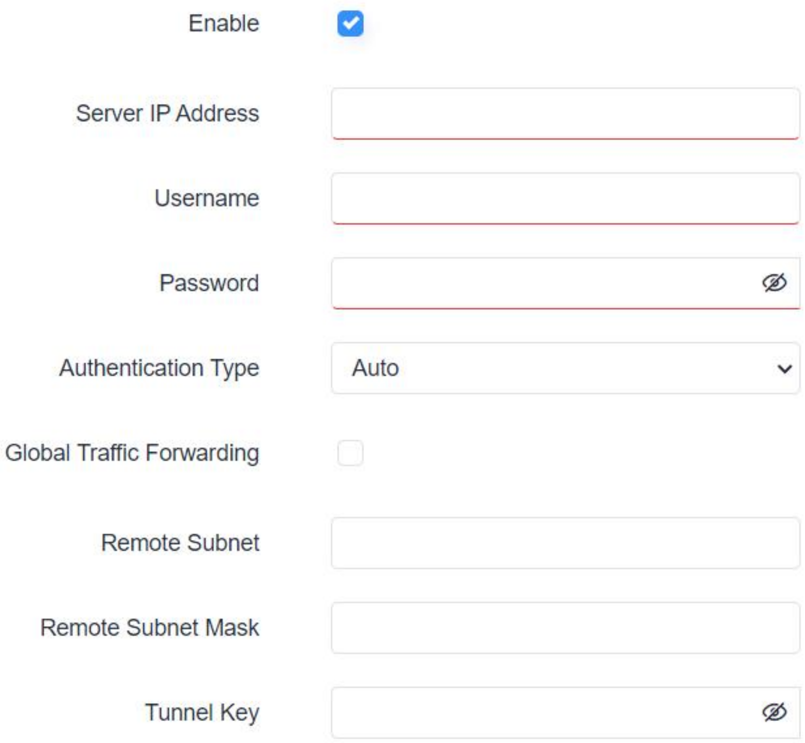
7.3.2.3 Certificate

When using local authentication of IPsec server or client as CA, user can import/export necessary certificate and key files to this page.

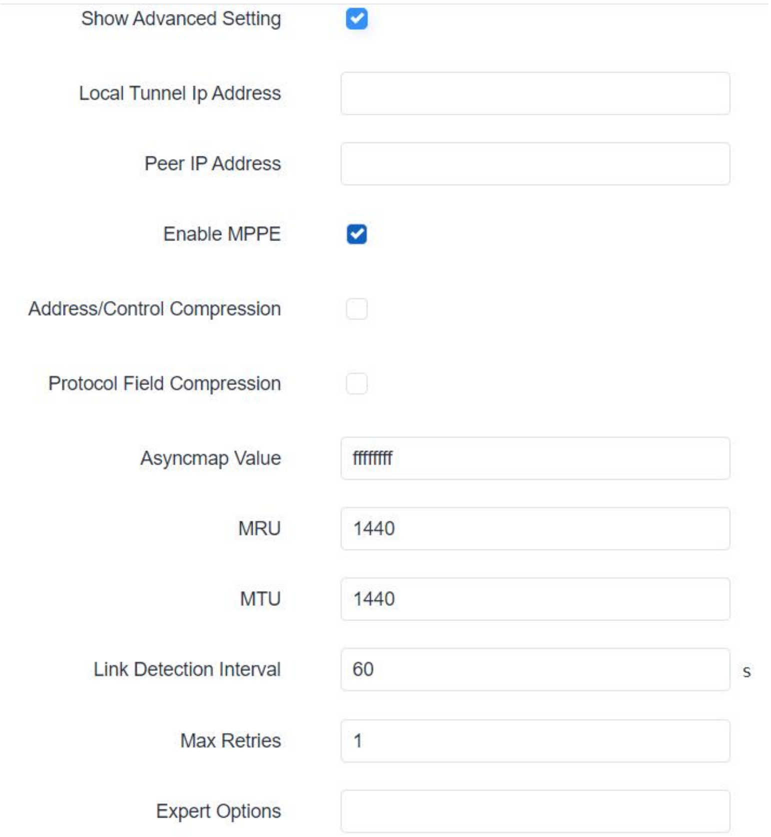


7.3.3 L2TP

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.



Enable	☑
Server IP Address	
Username	
Password	
Authentication Type	Auto
Global Traffic Forwarding	☐
Remote Subnet	
Remote Subnet Mask	
Tunnel Key	



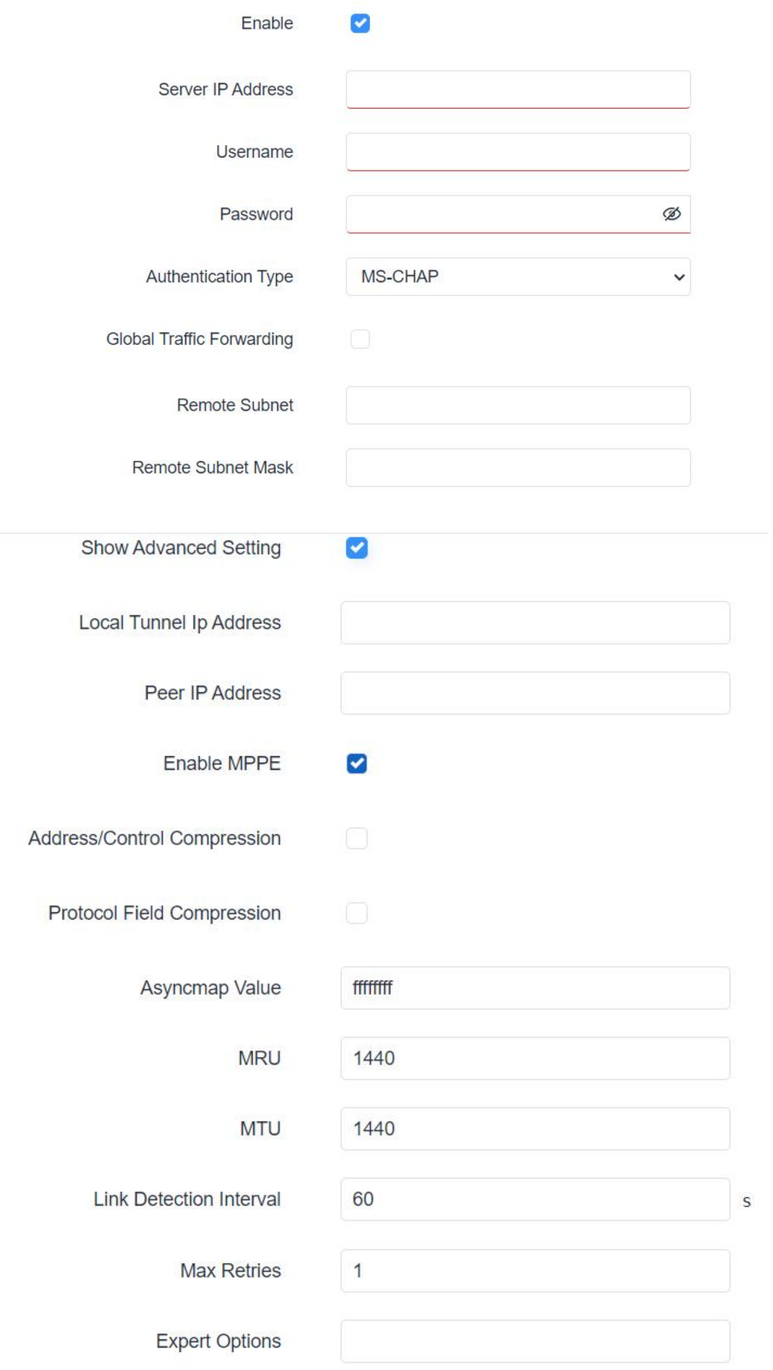
Show Advanced Setting	☑
Local Tunnel Ip Address	
Peer IP Address	
Enable MPPE	☑
Address/Control Compression	□
Protocol Field Compression	□
Asyncmap Value	ffffffff
MRU	1440
MTU	1440
Link Detection Interval	60 s
Max Retries	1
Expert Options	

L2TP	
Item	**Description**
Enable	Enable or disable L2TP client.
Server 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 Type	Select authentication type used to secure data sessions.
Global Traffic Forwarding	All the data traffic will be sent out via L2TP VPN tunnel when this function is enabled.
Remote Subnet	Enter the remote subnet of L2TP VPN server.
Remote Subnet Mask	Enter the remote netmask of L2TP VPN server.
Tunnel Key	Enter the password of L2TP tunnel.
Local Tunnel IP Address	Set tunnel IP address of L2TP client. Client will obtain tunnel IP address automatically from the server when it's null.
Peer IP Address	Enter tunnel IP address of L2TP server.
Enable MPPE	Enable 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 L2TP 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: 68-1500.
Link Detection Interval	Set the link detection interval time to ensure tunnel connection. Range: 0-600.
Expert Options	User can enter some initialization strings in this field and separate the strings with semicolon.

7.3.4 PPTP

Point-to-Point Tunneling Protocol (PPTP) is a protocol that uses a TCP control channel and a Generic Routing Encapsulation tunnel to encapsulate PPP packets.



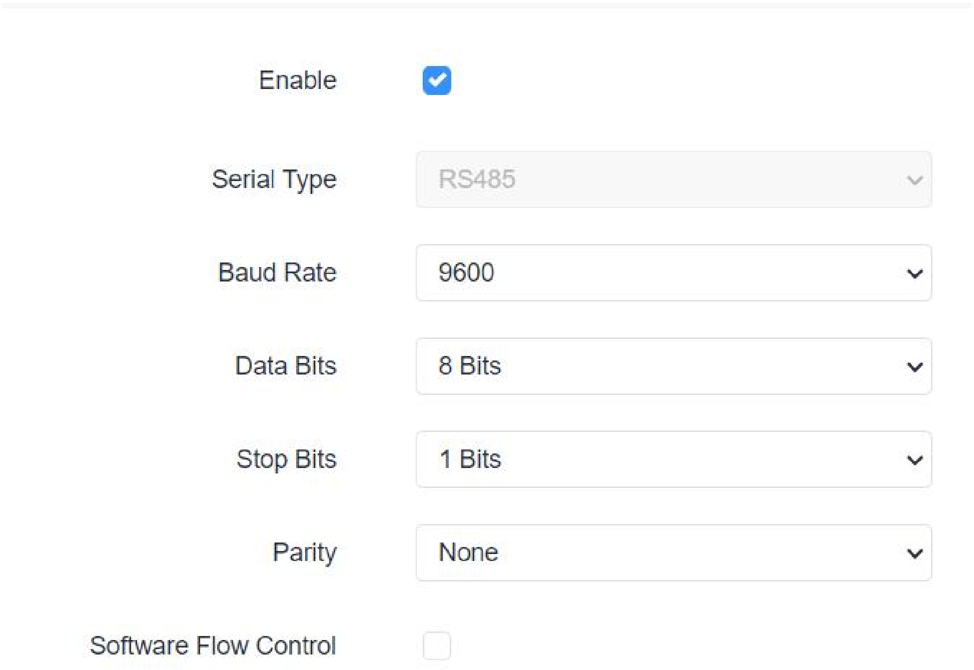
Enable	☑
Server IP Address	
Username	
Password	
Authentication Type	MS-CHAP
Global Traffic Forwarding	□
Remote Subnet	
Remote Subnet Mask	
Show Advanced Setting	☑
Local Tunnel Ip Address	
Peer IP Address	
Enable MPPE	☑
Address/Control Compression	□
Protocol Field Compression	□
Asyncmap Value	ffffffff
MRU	1440
MTU	1440
Link Detection Interval	60 s
Max Retries	1
Expert Options	

PPTP	
Item	**Description**
Enable	Enable or disable PPTP client.
Server 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 Type	Select authentication type used to secure data sessions.
Global Traffic Forwarding	All the data traffic will be sent out viaPPTP VPN tunnel when this function is enabled.
Remote Subnet	Enter the remote subnet of PPTP VPN server.
Remote Subnet Mask	Enter the remote netmask of PPTP VPN server.
Local Tunnel 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 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 PPTP initialization strings. User can keep the default value. Range: 0-ffffffff.
MRU	Set the maximum receive unit. Range: 64-1440.
MTU	Set the maximum transmission unit. Range: 68-1440.
Link Detection Interval	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 initialization strings in this field and separate the strings with semicolon.

7.4 Service

7.4.1 Serial Port

This section explains how to configure serial port parameters to achieve communication with serial terminals, and configure work mode to achieve communication with the remote data centers, so as to achieve two-way communication between serial terminals and remote data centers.



Enable ☑

Serial Type: RS485

Baud Rate: 9600

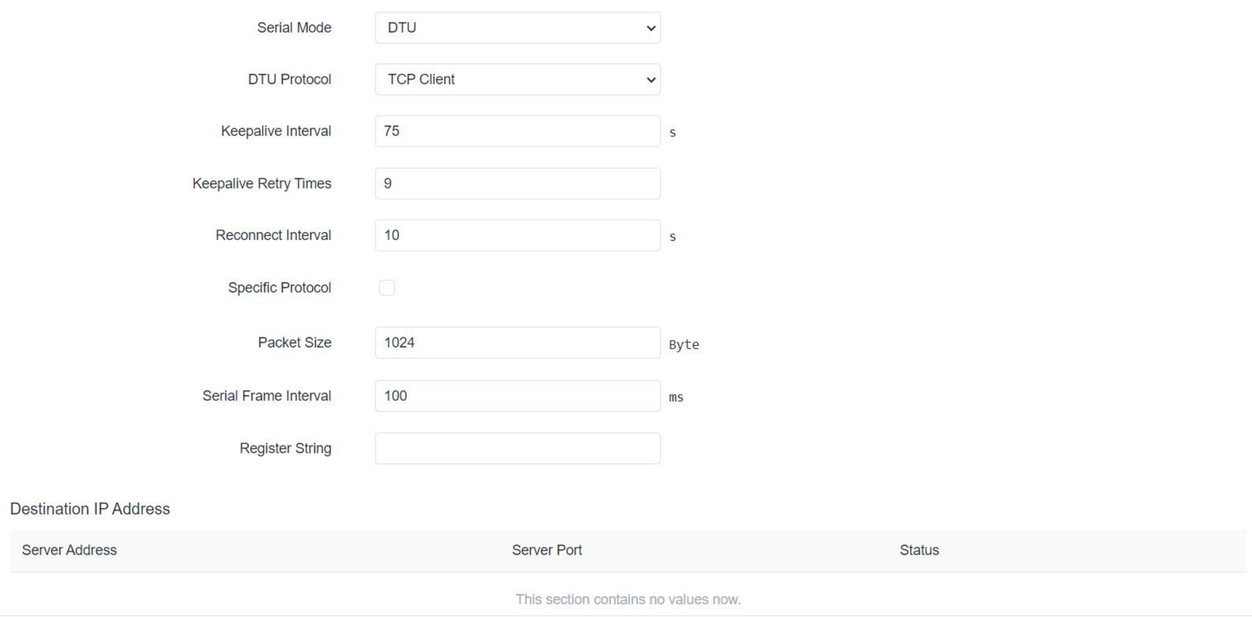
Data Bits: 8 Bits

Stop Bits: 1 Bits

Parity: None

Software Flow Control □

Serial Setting		
Item	**Description**	**Default**
Enable	Enable or disable serial port function.	Disable
Serial Type	It is fixed as RS485 by default. If you want RS232 port, please contact sales before ordering.	--
Baud Rate	The range is 300-230400. Same with the baud rate of the connected terminal device.	9600
Data Bits	8 bits or 7 bits optional. Same with the data bits of the connected terminal device.	8
Stop Bits	1 bit or 2 bits optional. Same with the stop bits of the connected terminal device.	1
Parity	Options are None, Odd and Even. Same with the parity of the connected terminal device.	None
Software Flow Control	Enable or disable software flow control.	Disable
Serial Mode	Select work mode of the serial port. **DTU Mode:** In DTU mode, the serial port can establish communication with the remote server/client. **GPS:** In GPS mode, go to **Service > GPS > GPS Serial Forwarding** to configure basic parameters to send GPS data to serial port. **Modbus Client:** In Modbus Client mode, go to **Service > Modbus Client** to configure basic parameters and channels.	Disable



Serial Mode	DTU	
DTU Protocol	TCP Client	
Keepalive Interval	75	s
Keepalive Retry Times	9	
Reconnect Interval	10	s
Specific Protocol	□	
Packet Size	1024	Byte
Serial Frame Interval	100	ms
Register String		

Destination IP Address

Server Address	Server Port	Status

This section contains no values now.

DTU Mode		
Item	**Description**	**Default**
DTU Protocol	Select from below protocols: **TCP Client:** the device is used as TCP client and transmits data to TCP server transparently. **UDP Client:** the device is used as UDP client and transmits data to UDP server transparently. **TCP server:** the device is used as TCP server to wait for polling data. **UDP server:** the device is used as UDP server to wait for polling data. **Modbus:** the device will be used as Modbus gateway, which can achieve conversion between Modbus RTU and Modbus TCP. **Node-RED:** the device will forward the data to the Serial Input node when Node-RED is installed. **MQTT:** the router will be used as MQTT client to forward data to MQTT broker or forward downlink to serial port.	--
TCP/UDP Server		
Local port	Set the local port of this TCP/UDP server. Range: 1-65535.	502
Keepalive Interval	After TCP connection is established, client will send heartbeat packet regularly by TCP to keep alive. The interval range is 1-3600 s.	75
Max Retries	When TCP heartbeat times out, device will resend heartbeat. After it reaches the limitation of the preset retry times, TCP connection will be reestablished. The retry times range is 1-16.	9
Packet Size	Set the size of the serial data frame. Packet will be sent out when preset frame size reaches the limitation. The size range is 1-1024 byte.	1024
Serial Frame Interval	The interval that the device sends out real serial data stored in the buffer area to public network. The range is 10-65535 ms. **Note:** data will be sent out to public network when real serial data size reaches the preset packet size, even though it's within the serial	100

	frame interval.	
TCP/UDP Client		
Keepalive Interval	After TCP client is connected with TCP server, the client will send heartbeat packet by TCP regularly to keep alive. The interval range is 1-3600 s.	75
Keepalive Retry Times	When TCP heartbeat times run out, the device will resend heartbeat. After it reaches the preset retry times, device will reconnect to TCP server. The range is 1-16.	9
Reconnect Interval	When connection fails, device will reconnect to the server at the preset interval. The range is 10-60 s.	10
Specific Protocol	With Specific Protocol, the device will be able to connect to the TCP2COM software.	Disable
Heartbeat Interval	With Specific Protocol, the device will send heartbeat packet to the server regularly to keep alive. The interval range is 1-3600s.	30
ID	Define unique ID of each device. No longer than 63 characters and do not contain space character.	--
Packet Size	Set the size of the serial data frame. Packet will be sent out when preset frame size is reached. The range is 1-1024 byte.	1024
Serial Frame Interval	The interval that the device sends out real serial data stored in the buffer area to public network. The range is 10-65535 ms. **Note:** data will be sent out to public network when real serial data size reaches the preset packet size, even though it's within the serial frame interval.	100
Register String	When setting UDP client, define register string for connection with the server.	Null
Server Address	Fill in the TCP or UDP server address (IP/domain name).	Null
Server Port	Fill in the TCP or UDP server port. Range: 1-65535.	Null
Status	Show the connection status between the device and the server.	--
Modbus		
Local Port	Set the device listening port. Range: 1-65535.	502
Max TCP Clients	Specify the maximum number of TCP clients allowed to connect the device which act as a TCP server.	32
Connection Timeout	If the TCP server does not receive any data from the slave device within the connection timeout period, the TCP connection will be broken.	60
Read Interval	Set the interval for reading remote channels. When a read cycle ends, the new read cycle begins until this interval expires. If it is set to 0, the device will restart the new read cycle after all channels have been read.	100
Response Timeout	Set the maximum response time that the device waits for the response to the command. If the device does not get a response after the maximum response time, it's determined that the command has run out of time.	3000
Max Retries	Set the maximum retry times after it fails to read.	3
Node-RED		

Packet Size	Set the size of the serial data frame. Packet will be sent out when preset frame size is reached. The range is 1-1024 byte.	1024
Serial Frame Interval	The interval that the device sends out real serial data stored in the buffer area to public network. The range is 10-65535 ms. **Note:** data will be sent out to public network when real serial data size reaches the preset packet size, even though it's within the serial frame interval.	100

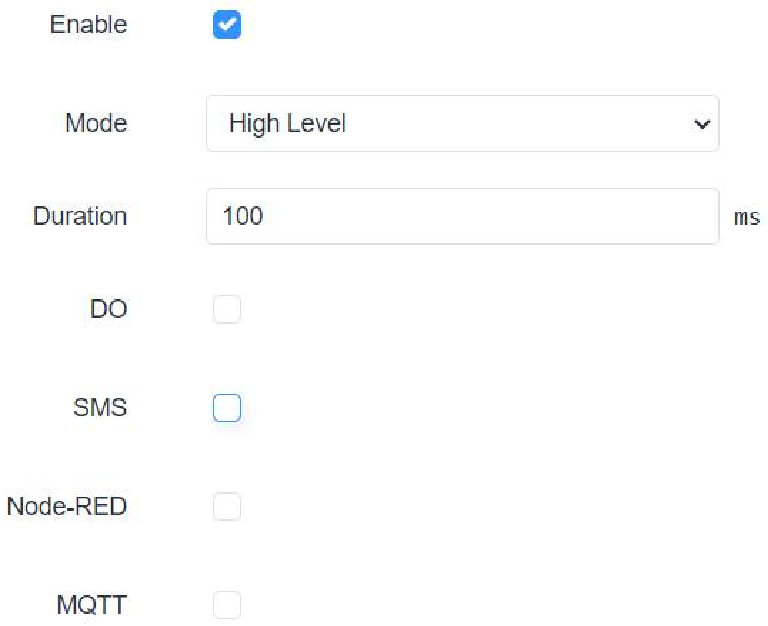
Related Configuration Example

DTU Application Example

7.4.2 I/O

7.4.2.1 DI

This section explains how to configure monitoring condition on digital input, and take certain actions once the condition is reached.



Enable ☑

Mode: High Level

Duration: 100 ms

DO □

SMS □

Node-RED □

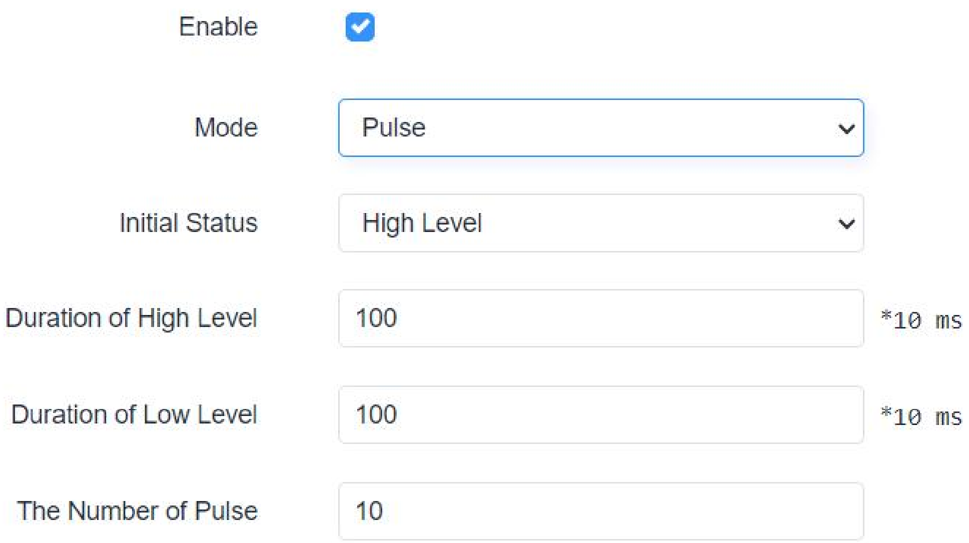
MQTT □

DI	
Item	**Description**
Enable	Enable or disable DI.
Mode	Select the working mode of DI. **High Level:** when it detects high level, trigger the action. **Low Level:** when it detects low level, trigger the action. **Counter:** when it detects a pulse, the counter value will increase by 1.
Duration (ms)	When the mode is high/low level, set the continuous duration of high/low level. Range: 1-10000.
Trigger	When mode is counter, select the counter trigger condition.

Condition	**Low->High:** The counter value will increase by 1 if digital input's status changes from low level to high level. **High->Low:** The counter value will increase by 1 if digital input's status changes from high level to low level.
Trigger Counter	The system will take actions accordingly when the counter value reach the preset one, and then reset the counter value to 0. Range: 1-100.
Action	Select the corresponding actions that the system will take when digital input mode meets the preset condition or duration. **DO:** Control output status of DO. **SMS:** select phone group to send SMS alarms. **Node-RED:** send the DI status to Digital Input node when Node-RED is installed. **MQTT**: enable to send message to MQTT broker. The MQTT connection is set up on **Service > MQTT** page.

7.4.2.2 DO

This section describes how to configure digital output mode.



Enable ☑

Mode: Pulse

Initial Status: High Level

Duration of High Level: 100 *10 ms

Duration of Low Level: 100 *10 ms

The Number of Pulse: 10

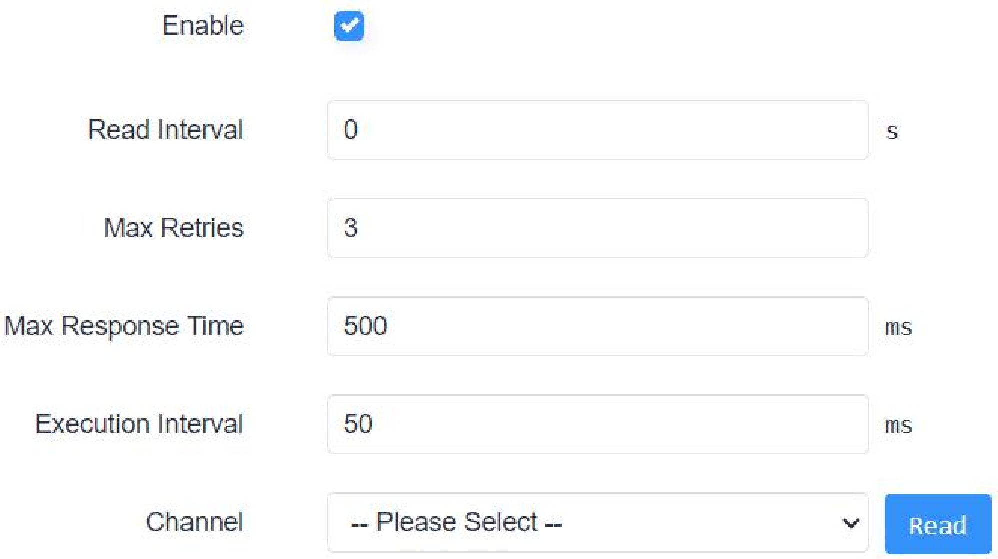
DO	
Item	**Description**
Enable	Enable or disable DO.
Mode	Select the working mode of DO. **High Level:** trigger the DO to send high level signal. **Low Level:** trigger the DO to send low level signal. **Counter:** trigger the DO to send pulses.
Initial Status	Select high level or low level as the initial status of the pulse.
Duration of High Level (*10ms)	Set the duration of pulse's high level. Range: 1-10000.
Duration of Low Level (*10ms)	Set the duration of pulse's low level. Range: 1-10000.
The Number of Pulse	Set the quantity of pulse. Range: 1-100.

7.4.3 Modbus Client (Master)

UF51 can be set as Modbus RTU/TCP Client to poll the remote Modbus Server and send data to TCP server.

7.4.3.1 Modbus Client

You can configure Modbus Client's parameters on this page.



Enable ☑

Read Interval: 0 s

Max Retries: 3

Max Response Time: 500 ms

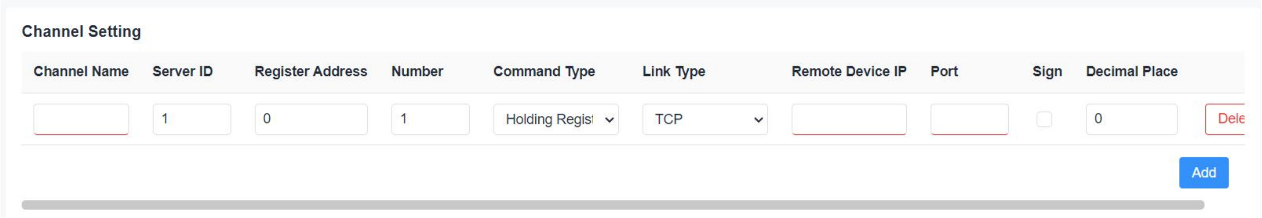
Execution Interval: 50 ms

Channel: -- Please Select --

Modbus Client		
Item	**Description**	**Default**
Enable	Enable/disable Modbus master.	--
Read Interval	Set the interval for reading remote channels. When the read cycle ends, the commands which haven't been sent out will be discard, and the new read cycle begins. If it is set as 0, the device will restart the new read cycle after all channels have been read. Range: 0-600 s.	0
Max Retries	Set the maximum retry times when it fails to read, range: 0-5.	3
Max Response Time	Set the maximum response time that the device waits for the response to the command. If the device does not get a response after the maximum response time, it's determined that the command has run out of time. Range: 10-1000 ms.	500
Execution Interval	The execution interval between each command. Range: 10-1000 ms.	50
Channel	Select a readable channel form **Service > Channel > Channel.**	--

7.4.3.2 Channel

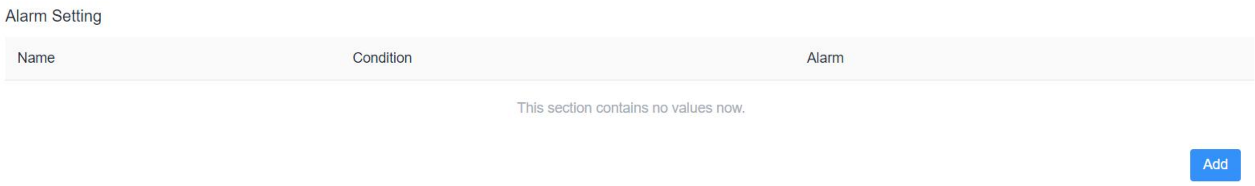
You can add the channels and configure alarm setting on this page, so as to connect the device to the remote Modbus Server to poll the address on this page and receive alarms from the device in different conditions.



Channel Setting

Channel Name	Server ID	Register Address	Number	Command Type	Link Type	Remote Device IP	Port	Sign	Decimal Place	
	1	0	1	Holding Regisi	TCP			□	0	Dele

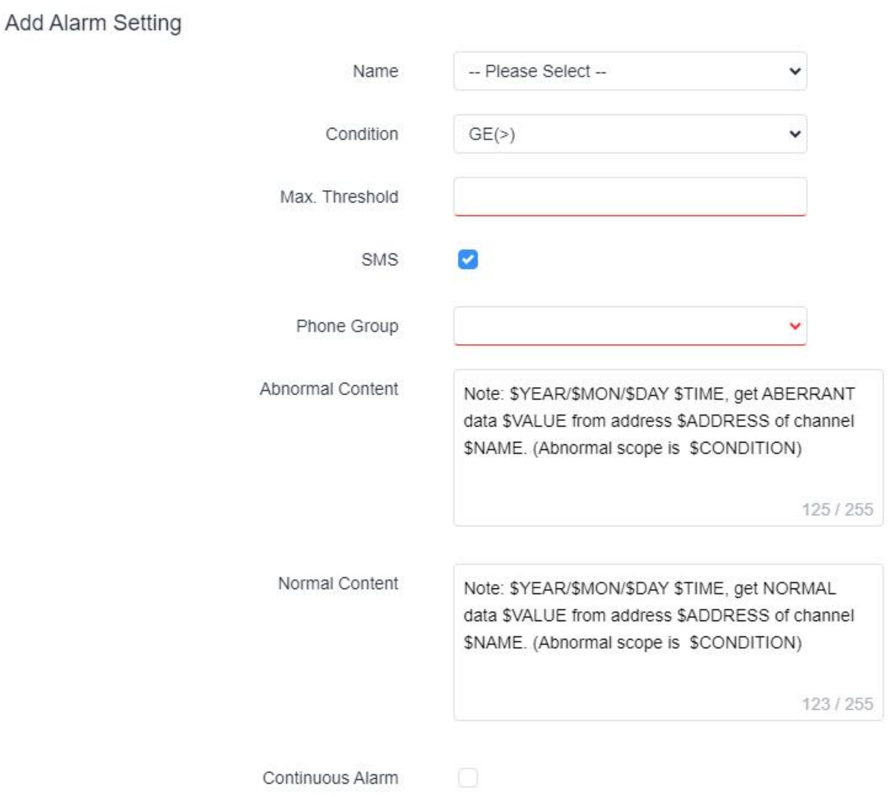
Channel Setting	
Item	**Description**
Channel Name	Set the name to identify the remote channel. It cannot be blank.
Server ID	Set Modbus server ID.
Register Address	The starting address for Modbus reading.
Number	The reading quantity from starting address.
Command Type	Read command data type, options are Coil, Discrete, Holding Register (INT16), Input Register (INT16), Holding Register (INT32) and Holding Register (Float).
Link Type	Select serial port or TCP connection. **Serial Port:** the device communicate with devices via Modbus RTU protocol. **TCP:** the device communicate with devices via Modbus TCP protocol.
Remote Device IP	When link is TCP, fill in the IP address of the remote Modbus TCP device.
Port	When link is TCP, fill in the port of the remote Modbus TCP device.
Sign	When command data type is holding register or input register, enable or disable to identify whether this channel is signed.
Decimal Place	When command data type is holding register or input register, indicate a dot in the read into the position of the channel. For example: read the channel value is 1234 and a Decimal Place is equal to 2, then the actual value is 12.34.



Alarm Setting

Name	Condition	Alarm

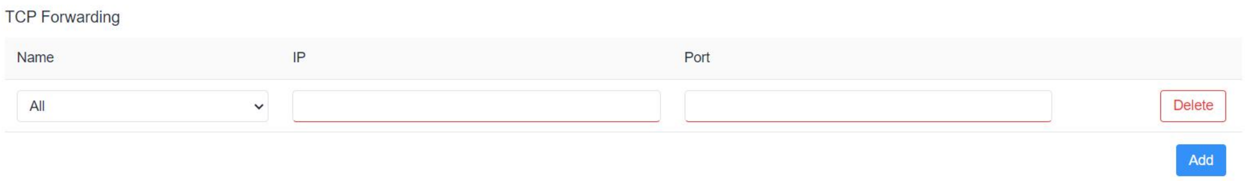
This section contains no values now.



Add Alarm Setting

Name	-- Please Select --
Condition	GE(>)
Max. Threshold	
SMS	☑
Phone Group	
Abnormal Content	Note: $YEAR/$MON/$DAY $TIME, get ABERRANT data $VALUE from address $ADDRESS of channel $NAME. (Abnormal scope is $CONDITION) 125 / 255
Normal Content	Note: $YEAR/$MON/$DAY $TIME, get NORMAL data $VALUE from address $ADDRESS of channel $NAME. (Abnormal scope is $CONDITION) 123 / 255
Continuous Alarm	□

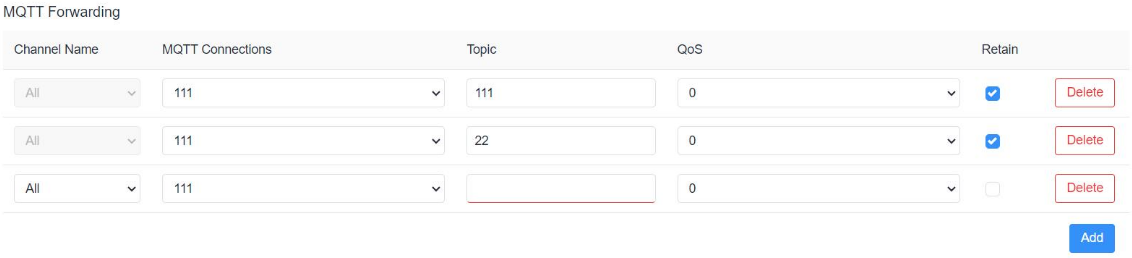
Alarm Setting	
Item	**Description**
Channel Name	Select the Modbus channel.
Condition	The condition that triggers alert.
Min. Threshold	Set the min. value to trigger the alert. When the actual value is less than this value, the alarm will be triggered.
Max. Threshold	Set the max. value to trigger the alert. When the actual value is more than this value, the alarm will be triggered.
SMS	Enable or disable SMS alarm when Modbus channel meets the condition.
Phone Group	Select the phone group to receive the alarm SMS. The phone group can be added on **Service > Phone&SMS > Phone page**.
Abnormal Content	When the actual value meets the preset condition, the device will automatically trigger the alarm and send the preset abnormal content to the specified phone group.
Normal Content	When the actual value is restored to the normal value from exceeding the threshold value, the device will automatically cancel the abnormal alarm and send the preset normal content to the specified phone group.
Continuous Alarm	Once enabled, the same alarm will be continuously reported. Otherwise, the same alarm will be reported only one time.



TCP Forwarding

Name	IP	Port	
All			Delete

TCP Forwarding	
Item	**Description**
Name	The name of Modbus Client's channel.
IP	The IP address of the server to which the packets are forwarded .
Port	The port of the server's to which the packets are forwarded.



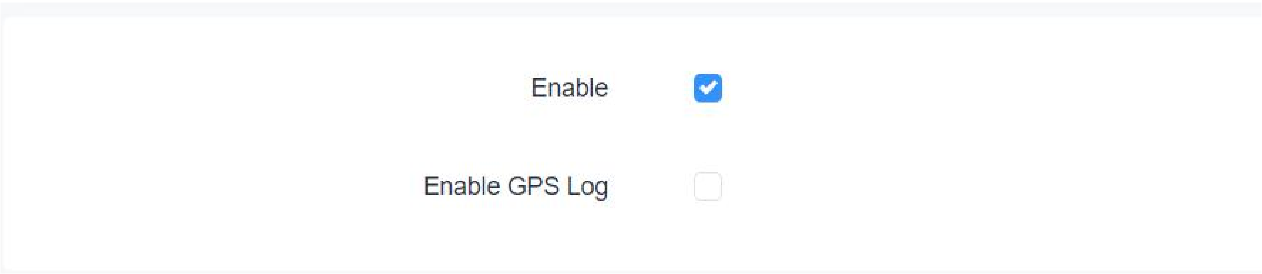
MQTT Forwarding

Channel Name	MQTT Connections	Topic	QoS	Retain	
All	111	111	0	☑	Delete
All	111	22	0	☑	Delete
All	111		0	□	Delete

MQTT Forwarding	
Item	**Description**
Channel Name	The name of Modbus Client's channel.
MQTT Connections	Select the MQTT connection to send Modbus channel data, it’s set up on **Service > MQTT** page.
Topic	Topic name used for publishing Modbus channel data.
Retain	Enable to set the latest message of this topic as retain message.
QoS	QoS0, QoS1 or QoS2 are optional.

7.4.4 GPS

Users can enable GPS feature here. For more debug information, please also enable GPS log.

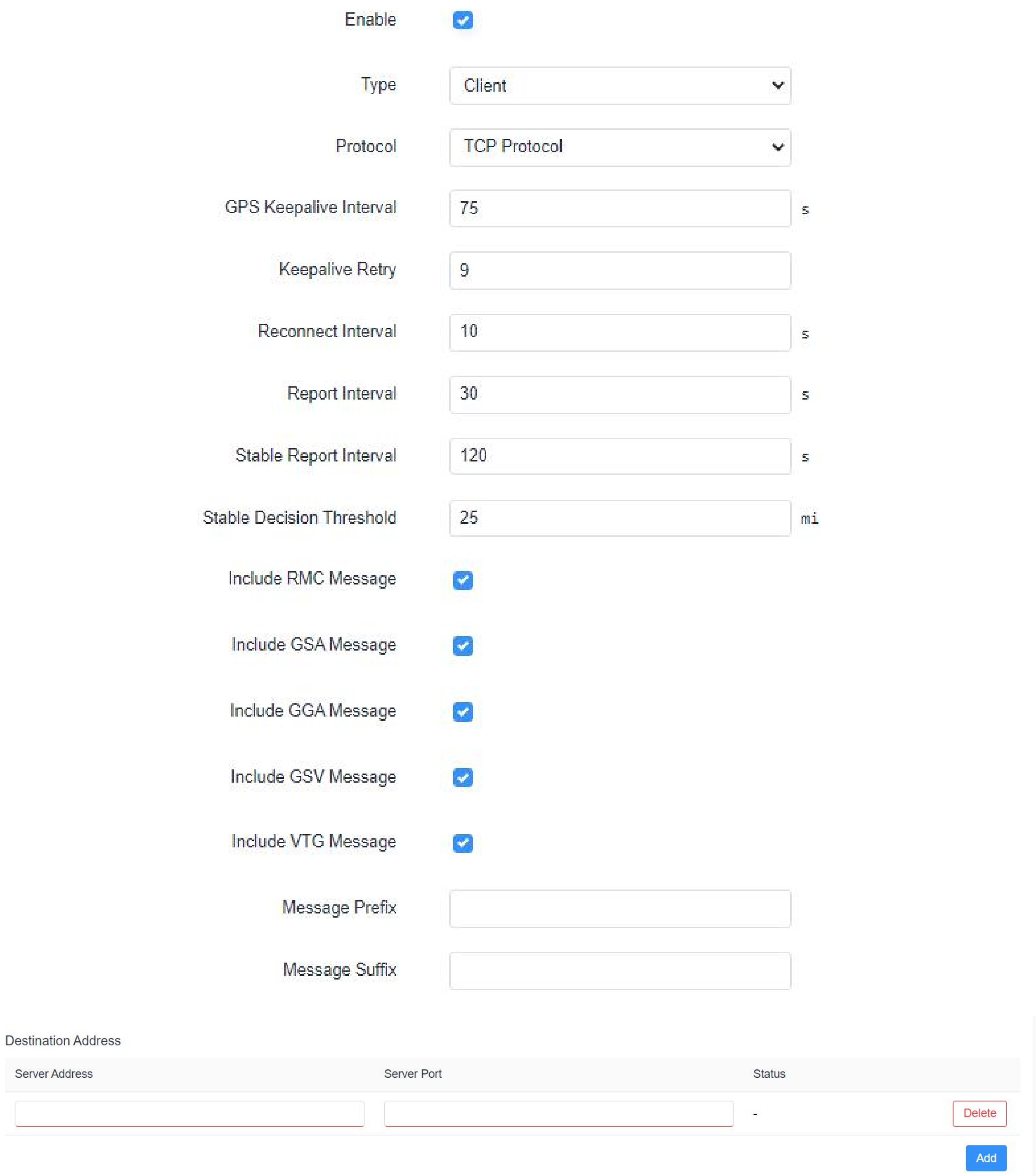


Enable ☑

Enable GPS Log □

7.4.4.1 GPS IP Forwarding

GPS IP forwarding means that GPS data can be forwarded over the Internet.



Enable	☑
Type	Client
Protocol	TCP Protocol
GPS Keepalive Interval	75 s
Keepalive Retry	9
Reconnect Interval	10 s
Report Interval	30 s
Stable Report Interval	120 s
Stable Decision Threshold	25 mi
Include RMC Message	☑
Include GSA Message	☑
Include GGA Message	☑
Include GSV Message	☑
Include VTG Message	☑
Message Prefix	
Message Suffix	

Destination Address

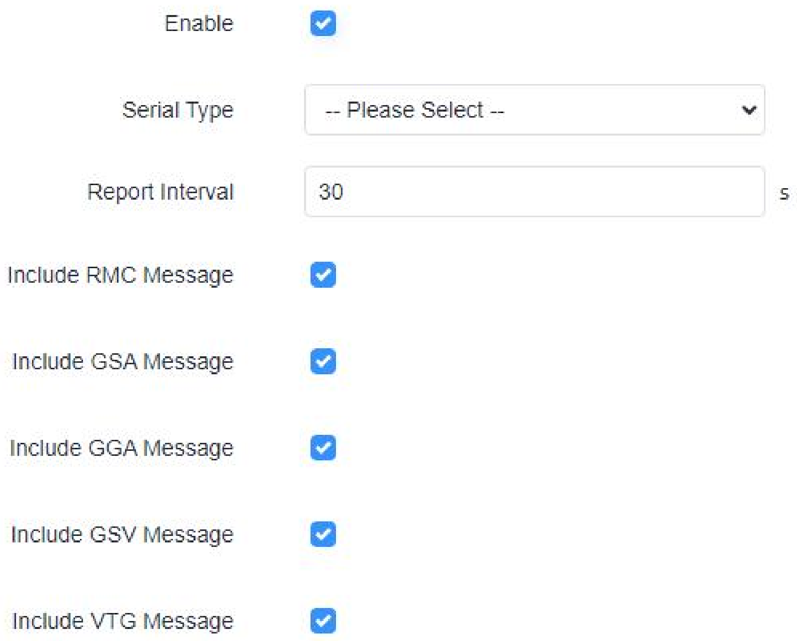
Server Address	Server Port	Status	
		-	Delete

GPS IP Forwarding		
Item	**Description**	**Default**
Enable	Forward the GPS data to the client or server.	Disable
Type	Select connection type of the device as Client or Server.	Client
Protocol	Select protocol of data transmission as TCP or UDP.	TCP
GPS Keepalive Interval	When it's connected with server/client, the device will send heartbeat packet regularly to the server/client to keep alive. The interval range is 1-3600s.	75
Keepalive	When TCP heartbeat times run out, the device will resend heartbeat.	9

Retry	After it reaches the preset retry times, device will reconnect to TCP server. The range is 1-16.	
Local Port	Set the device listening port when using as a Server. Range: 1-65535.	
Reconnect Interval	When the connection fails, device will reconnect to the server at the preset interval. The range is 10-60 s.	10
Report Interval	The device will send GPS data to the server/client according to this interval if it reaches the stable decision threshold. The range is 1-65535 s.	30
Stable Report Interval	The device will send GPS data to the server/client according to this interval if it does not reach the stable decision threshold. The range is 1-65535 s.	120
Stable Decision Threshold	The GPS location deviation within this distance can be regarded as no change. The range is 1-65535 m.	25
Include RMC Message	RMC includes time, date, position, course and speed data.	Enable
Include GSA Message	GSA includes GPS receiver operating mode, satellites used in the position solution, and DOP values.	Enable
Include GGA Message	GGA includes time, position and fix type data.	Enable
Include GSV Message	GSV includes the number, elevation, azimuth of GPS satellites and SNR values.	Enable
Include VTG Message	VTG includes course and speed information relative to the ground.	Enable
Message Prefix	Add a prefix to the GPS data.	Null
Message Suffix	Add a suffix to the GPS data.	Null
Destination Address		
Server Address	Fill in the server address to receive GPS data (IP/domain name).	--
Server Port	Fill in the server port to receive GPS data. Range: 1-65535.	--
Status	Show the connection status between the device and the server.	--

7.4.4.2 GPS Serial Forwarding

GPS serial forwarding means that GPS data can be forwarded to the serial port.

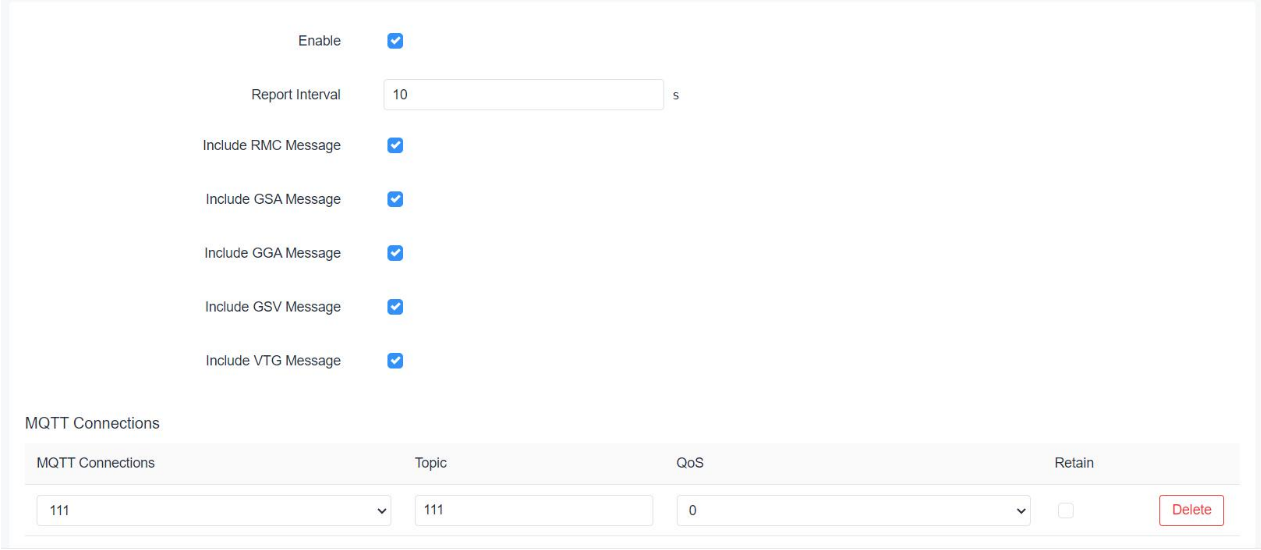


Enable	☑
Serial Type	-- Please Select --
Report Interval	30 s
Include RMC Message	☑
Include GSA Message	☑
Include GGA Message	☑
Include GSV Message	☑
Include VTG Message	☑

GPS Serial Forwarding		
Item	**Description**	**Default**
Enable	Forward the GPS data to the preset serial port.	Disable
Serial Type	Select the serial port to receive GPS data. Ensure that the serial port is enabled on **Service > Serial Port**.	--
Report Interval	The device will forward the GPS data to the serial port according to this interval. The range is 1-65535s.	30
Include RMC Message	RMC includes time, date, position, course and speed data.	Enable
Include GSA Message	GSA includes GPS receiver operating mode, satellites used in the position solution, and DOP values.	Enable
Include GGA Message	GGA includes time, position and fix type data.	Enable
Include GSV Message	GSV includes the number, elevation, azimuth of GPS satellites and SNR values.	Enable
Include VTG Message	VTG includes course and speed information relative to the ground.	Enable

7.4.4.3 GPS MQTT Forwarding

GPS MQTT forward means that GPS raw data can be forwarded to MQTT broker automatically.



Enable ☑

Report Interval 10 s

Include RMC Message ☑

Include GSA Message ☑

Include GGA Message ☑

Include GSV Message ☑

Include VTG Message ☑

MQTT Connections

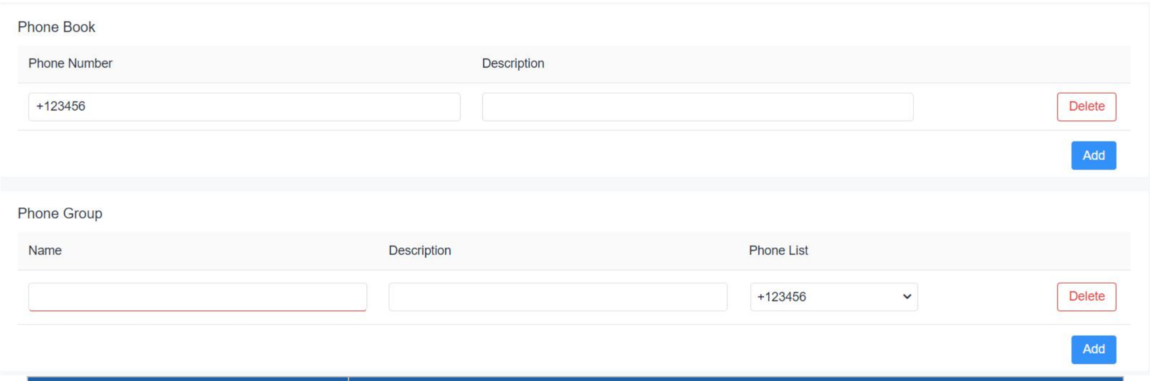
MQTT Connections	Topic	QoS	Retain	
111	111	0	☐	Delete

GPS MQTT Forwarding		
Item	**Description**	**Default**
Enable	Forward the GPS data to MTT broker automatically.	Disable
Report Interval	The interval to locate and forward the GPS data to the MQTT broker. The range is 1-60 s.	30
Include RMC Message	RMC includes time, date, position, course and speed data.	Enable
Include GSA Message	GSA includes GPS receiver operating mode, satellites used in the position solution, and DOP values.	Enable
Include GGA Message	GGA includes time, position and fix type data.	Enable
Include GSV Message	GSV includes the number, elevation, azimuth of GPS satellites and SNR values.	Enable
Include VTG Message	VTG includes course and speed information relative to the ground.	Enable
MQTT Connections		
MQTT Connections	Select the MQTT connection to send GPS data, it's set up on **Service > MQTT** page.	
Topic	Topic name for publishing GPS raw data.	
Retain	Enable to set the latest message of this topic as retain message.	
QoS	QoS0, QoS1 or QoS2 are optional.	

7.4.5 Phone&SMS

7.4.5.1 Phone

Phone settings involve in call/SMS trigger, SMS control and SMS alarm for events.



Phone Book

Phone Number	Description	
+123456		Delete

Add

Phone Group

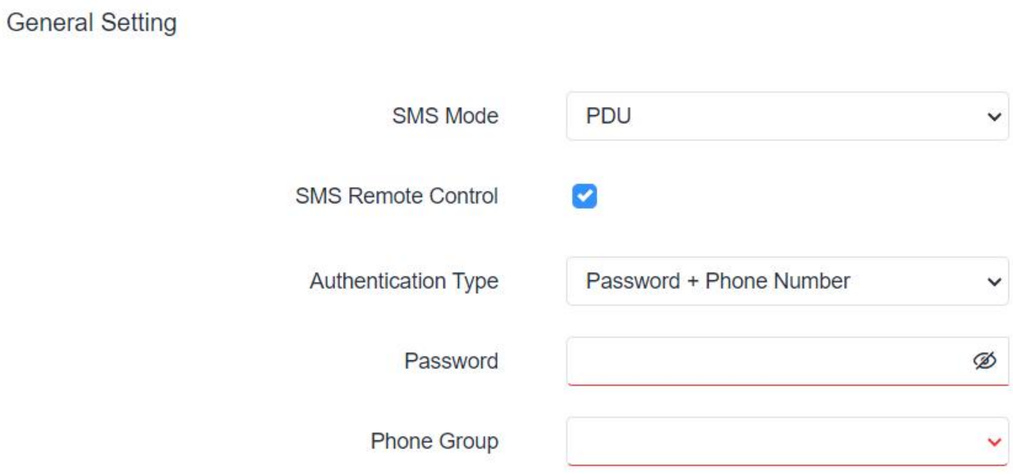
Name	Description	Phone List	
		+123456	Delete

Add

Item	Description
Phone Book	
Phone Number	Enter the telephone number. Digits, "+" and "-" are allowed.
Description	The description of the telephone number.
Phone Group List	
Group Name	Set name for phone group.
Description	The description of the phone group.
Phone List	Select the phone numbers to the list.

7.4.5.2 SMS

SMS settings involve in remote SMS control, sending SMS and SMS receiving and sending status.



General Setting

SMS Mode: PDU

SMS Remote Control: ☑

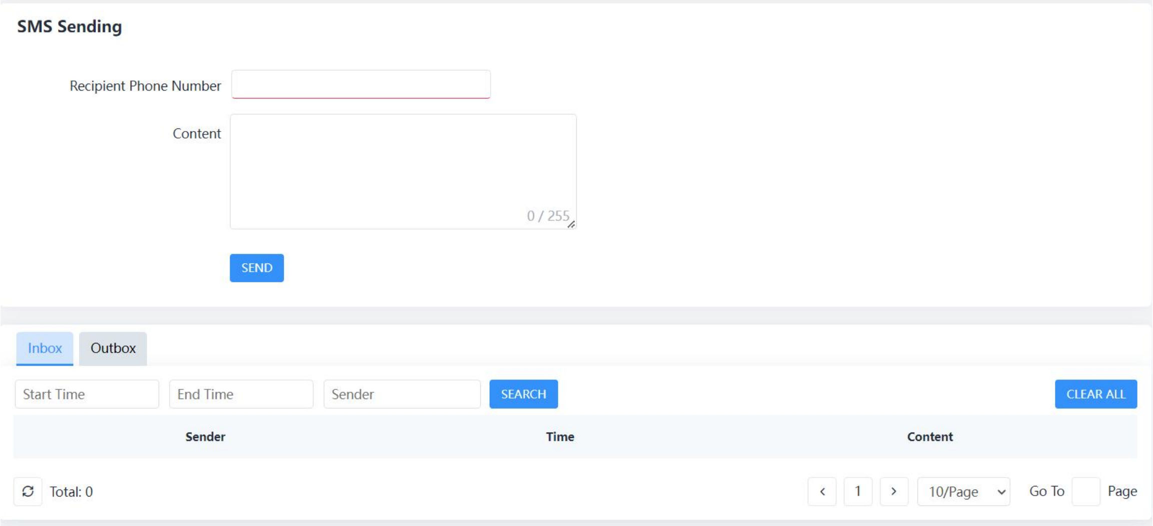
Authentication Type: Password + Phone Number

Password:

Phone Group:

SMS	
Item	**Description**
SMS Mode	Select SMS mode: **Text:** Pure text mode, mainly used in Europe and America. Technical ly, it can also be used to send Short Messages in Chinese. **PDU:** It’s the default encoding Mode for mobile phones, which confo rm to all mobile phones SMS format and can use any character.
SMS Remote Control	Enable/disable SMS Remote Control. Click here to check SMS control commands.
Authentication Type	Choose the authentication type to check whether the SMS is from valid controller.

	Phone number: only the phone numbers on phone groups support remote control. **Password + phone number:** only the phone numbers on phone groups support remote control; besides, control SMS should be sent as format password+”;”+command content.
Password	Set password for authentication.
Phone Group	Select the Phone group which used for remote control.


SMS Sending

Recipient Phone Number

Content

0 / 255

Sender	Time	Content

SMS	
Item	**Description**
SMS Sending	
Recipient Phone Number	Enter the number to receive the SMS.
Content	SMS content.
Inbox/Outbox	
Search	Search for SMS record.
Clear All	Clear the SMS inbox/outbox records.

7.4.6 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.

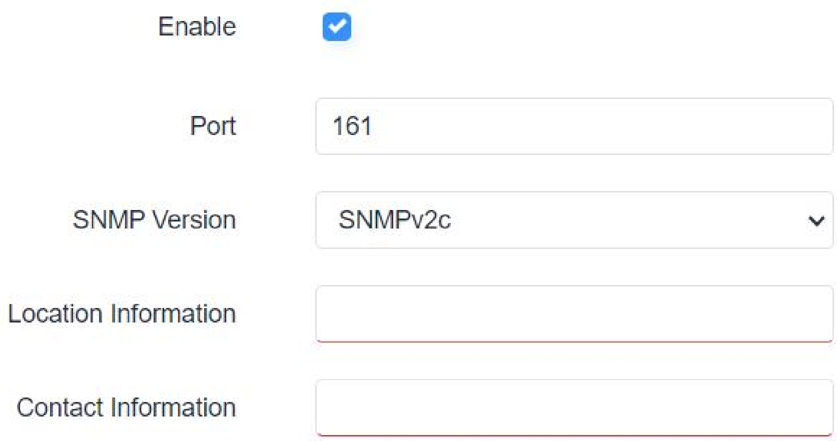
Configuring SNMP in networking, NMS, and a management program of SNMP should be set up at the Manager.

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.

7.4.6.1 SNMP

UF51 supports SNMPv1, SNMPv2c and SNMPv3 version. SNMPv3 employs authentication encryption by username and password.



Enable ☑

Port 161

SNMP Version SNMPv2c

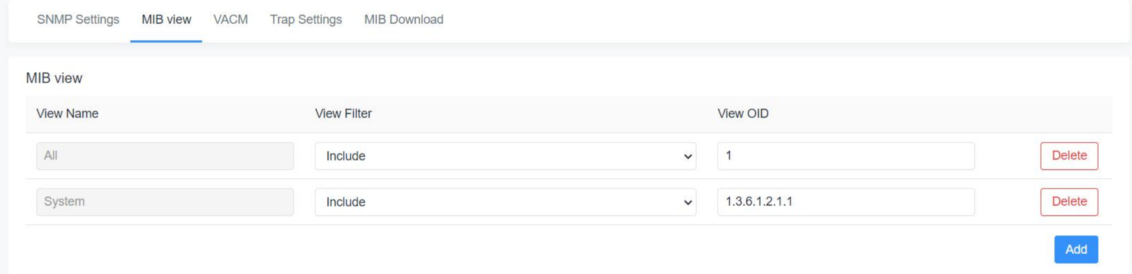
Location Information

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.
SNMP Version	It’s fixed as SNMP v3.
Location Information	Fill in the location information.
Contact Information	Fill in the contact information.

7.4.6.2 MIB View

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



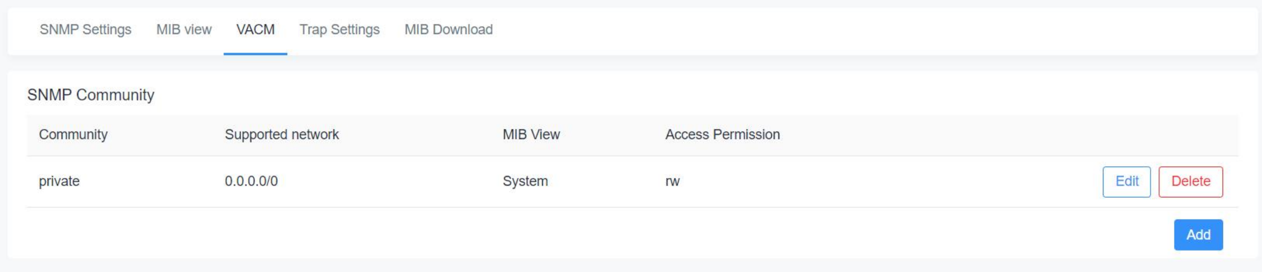
MIB view

View Name	View Filter	View OID	
All	Include	1	Delete
System	Include	1.3.6.1.2.1.1	Delete

MIB View	
Item	**Description**
View Name	Set MIB view's name.
View Filter	Select from "Included" and "Excluded". Included: query all nodes within the specified MIB node. Excluded: query all nodes except for the specified MIB node.
View OID	Enter the OID number.
Add/Delete	Click to add or delete a MIB view.

7.4.6.3 VACM

This section describes how to configure VCAM parameters.



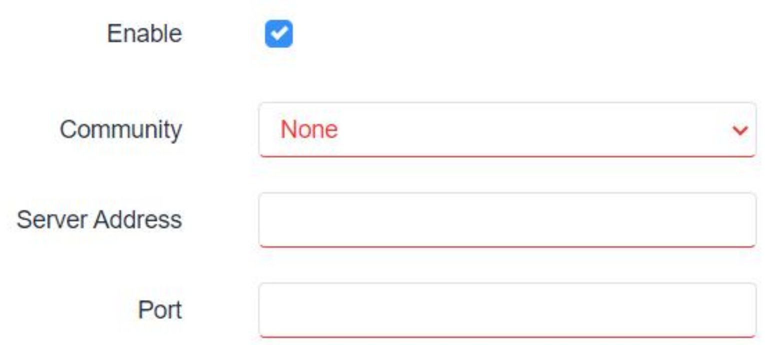
SNMP Community

Community	Supported network	MIB View	Access Permission
private	0.0.0.0/0	System	rw

VACM	
Item	**Description**
SNMP v1 & v2c Supported Network	
Community	Set the community name.
IP Address/Netmask	The external IP address range to access this MIB view.
MIB View	Select an MIB view to set permissions from the MIB view list.
Access Permission	Select from "Read-Only" and "Read-Write".
SNMP v3 User	
Username	Set the name of SNMPv3 user.
Security Level	Select from "None", "Auth/NoPriv", and " Auth/Priv".
Authentication Algorithm	Select from "MD5" or "SHA" when Auth is selected.
Authentication Password	The password should be filled in.
Encryption Algorithm	Select from "AES" or "DES" when “Auth/Priv” is selected.
Encryption Password	The password should be filled in.
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.
Notify View	Select an MIB view to set permission as "Notify" from the MIB view list.

7.4.6.4 Trap

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

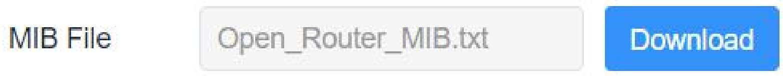


Enable	☑
Community	None
Server Address	
Port	

SNMP Trap	
Item	**Description**
Enable	Enable or disable SNMP Trap function.
Community	Select the community of SNMP v1/v2c.
User	Select the user of SNMPv3.
Server Address	Fill in NMS's IP address or domain name.
Port	Fill in UDP port. Port range is 1-65535.

7.4.6.5 MIB Download

This section describes how to download MIB files.

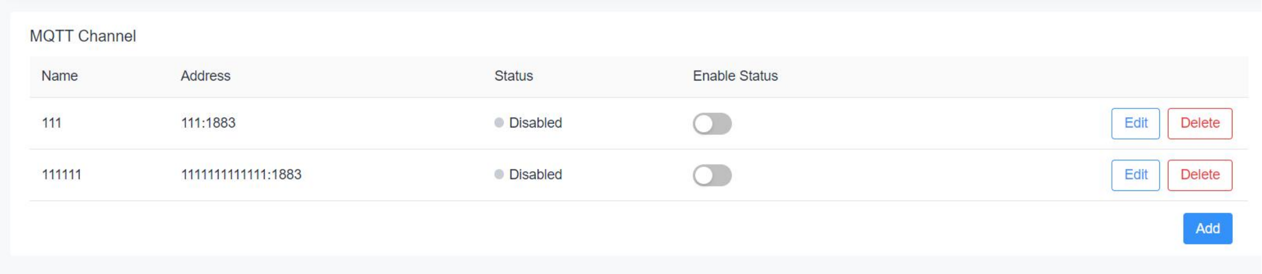


MIB File: Open_Router_MIB.txt

7.4.7 MQTT

The device supports to work as MQTT client to forward data and router information to MQTT broker in two ways:

1. Users send requests to the router to enquire the router information;
2. The router publishes the data automatically.

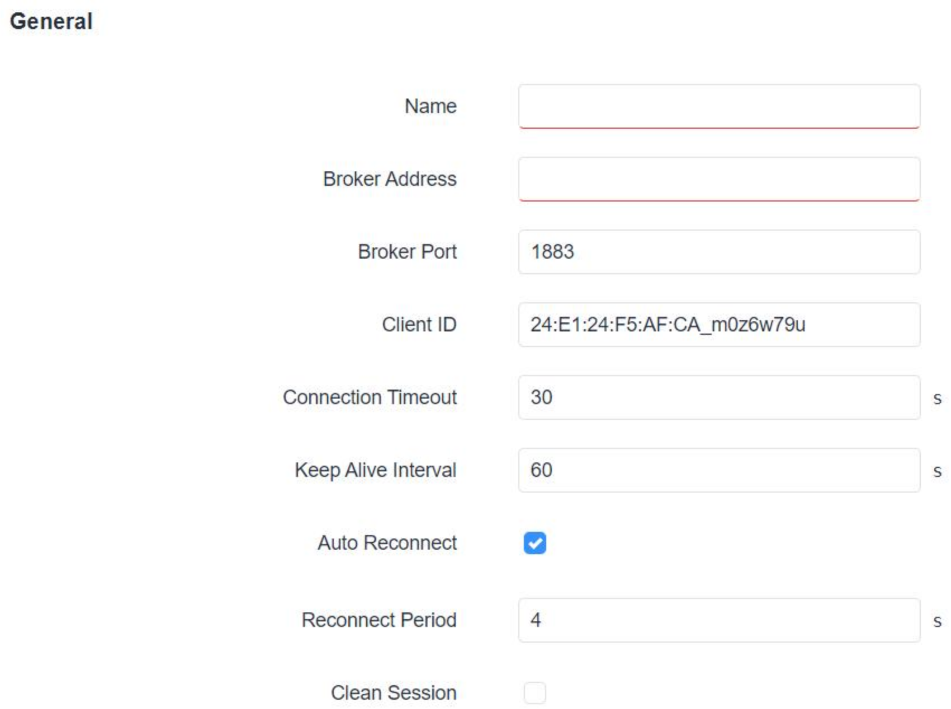


MQTT Channel

Name	Address	Status	Enable Status	
111	111:1883	● Disabled	○	Edit Delete
111111	1111111111111:1883	● Disabled	○	Edit Delete

MQTT Channel	
Item	**Description**
Name	The unique name of MQTT channel.
Address	MQTT broker address and port to receive data.
Status	Show connection status between router and MQTT broker.
Enable Status	Enable or disable this MQTT channel.

Edit	Edit this MQTT channel.
Delete	Delete this MQTT channel.
Add	Add a new MQTT channel.



General

Name:

Broker Address:

Broker Port: 1883

Client ID: 24:E1:24:F5:AF:CA_m0z6w79u

Connection Timeout: 30 s

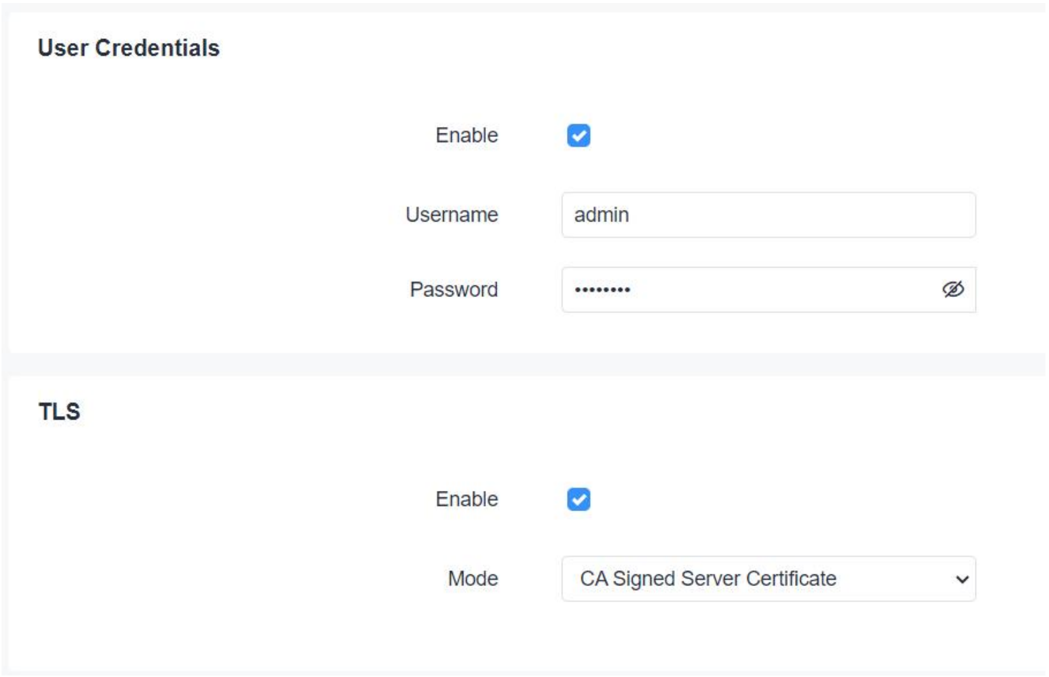
Keep Alive Interval: 60 s

Auto Reconnect: ☑

Reconnect Period: 4 s

Clean Session: □

\



User Credentials

Enable: ☑

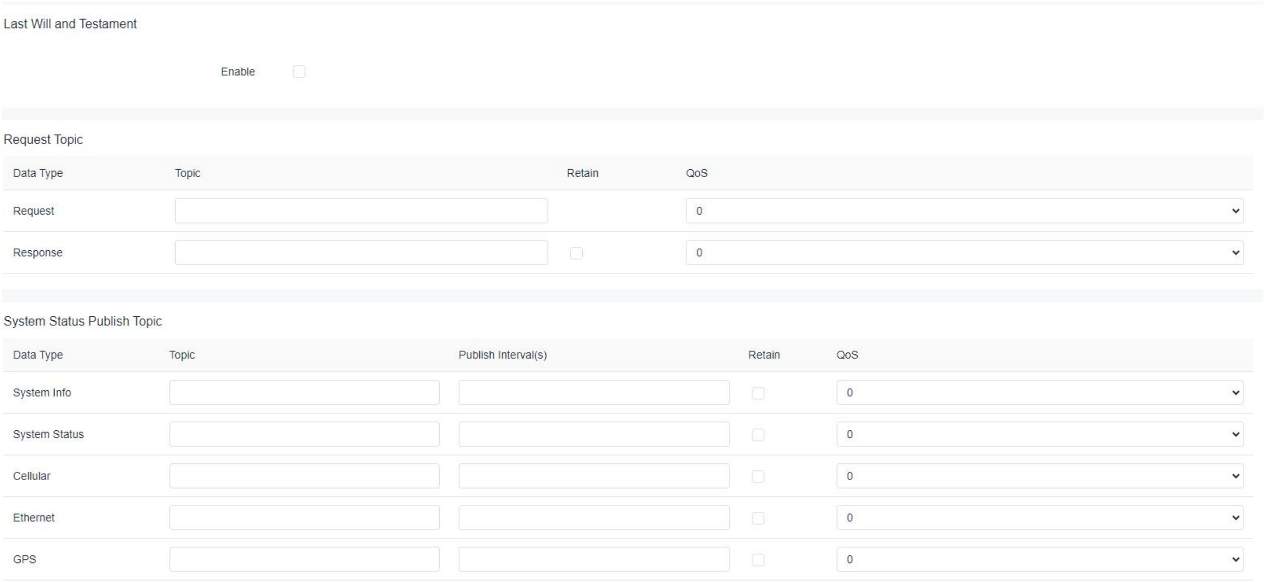
Username: admin

Password: ••••••••

TLS

Enable: ☑

Mode: CA Signed Server Certificate



Last Will and Testament

Enable □

Request Topic

Data Type	Topic	Retain	QoS
Request			0
Response		□	0

System Status Publish Topic

Data Type	Topic	Publish Interval(s)	Retain	QoS
System Info			□	0
System Status			□	0
Cellular			□	0
Ethernet			□	0
GPS			□	0

MQTT Settings	
Item	**Description**
General	
Name	Customize a unique connection name.
Broker Address	MQTT broker address to receive data.
Broker Port	MQTT broker port to receive data.
Client ID	Client ID is the unique identity of the client to the server. It must be unique when all clients are connected to the same server, and it is the key to handle messages at QoS 1 and 2.
Connection Timeout/s	If the client does not get a response after the connection timeout, the connection will be considered as broken. The Range: 1-65535.
Keep Alive Interval/s	After the client is connected to the server, the client will send heartbeat packet to the server regularly to keep alive. Range: 1-65535.
Auto Reconnect	When connection is broken, try to reconnect the server automatically.
Reconnect Period	When connection is broken, the period to reconnect the server periodically.
Clean Session	When enabled, the connection will create a temporary session and all information will lose when the client is disconnected from broker; when disabled, the connection will create a persistent session that will remain and save offline messages until the session logs out overtime.
User Credentials	
Enable	Enable user credentials.
Username	The username used for connecting to the MQTT broker.
Password	The password used for connecting to the MQTT broker.
TLS	
Enable	Enable the TLS encryption in MQTT communication.
Mode	Select from Self signed certificates, CA signed server certificate. **CA signed server certificate:** verify with the certificate issued by

	Certificate Authority (CA) that pre-loaded on the device. **Self signed certificates:** upload the custom CA certificates, client certificates and secret key for verification.
Last Will and Testament	
Enable	Last will message is automatically sent when the MQTT client is abnormally disconnected. It is usually used to send device status information or inform other devices or proxy servers of the device's offline status.
Last-Will Topic	Customize the topic to receive last will messages.
Last-Will QoS	QoS0, QoS1 or QoS2 are optional.
Last-Will Retain	Enable to set last will message as retain message.
Last-Will Payload	Customize the last will message contents.
Request and Response Topic	

Topic	The router supports to send requests to enquire router information.
	Request: users is able to send requests to this topic to enquire router information. Request format:
	{
	    "id":"1",
	    "status":"systeminfo",
	    "sn": "64E1213132456",
	    "need_response":1 //1 means need response
	}
	The id is a random value, and the status can be set as 5 types: systeminfo, systemstatus, cellular, ethernet, gps.
	Response: users is able to subscribe this topic to get the replies.

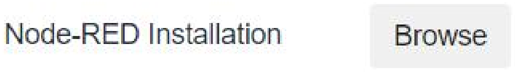
Retain	Enable to set the latest message of this topic as retain message.
QoS	QoS0, QoS1 or QoS2 are optional.
System Status Publish Topic	
Data Type	Data type sent to MQTT broker automatically. Note that the GPS in this page is not raw data but decoded location data.
Topic	Topic name of the data type used for publishing.
Publish Interval (s)	The interval to publish data to MQTT broker automatically.
Retain	Enable to set the latest message of this topic as retain message.
QoS	QoS0, QoS1 or QoS2 are optional.

7.5 App

7.5.1 Node-RED

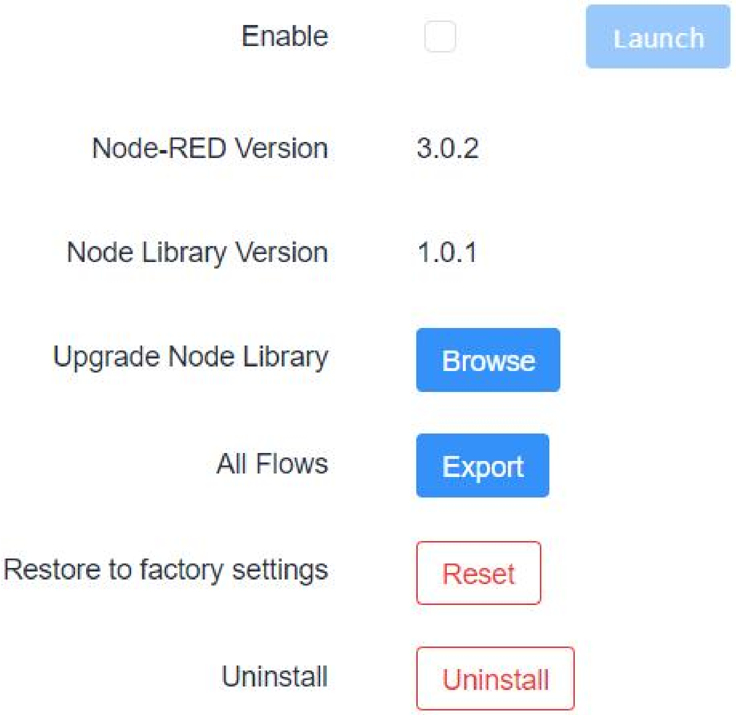
Node-RED is a flow-based development tool for visual programming and wiring together hardware devices, APIs and online services as part of the Internet of Things. Node-RED provides a

web-browser-based flow editor, which can easily wire together flows using the wide range of nodes in the palette. For more guidance and documentation please refer to Node-RED official website.
If the Node-RED is not installed, please download the Node-RED App from Milesight website and install it to the device.



Node-RED Installation Browse

After installation, it will show below status.



Enable □ Launch

Node-RED Version 3.0.2

Node Library Version 1.0.1

Upgrade Node Library Browse

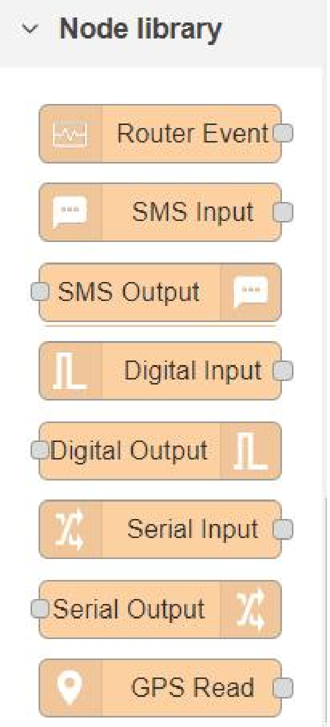
All Flows Export

Restore to factory settings Reset

Uninstall Uninstall

Node-RED	
Item	**Description**
Enable	Enable the Node-RED.
Launch	Click to launch the web GUI of Node-RED. The login authority of Node RED web GUI is the same as the admin account of web GUI.
Node-RED Version	Show the version of the Node-RED.
Node Library Version	Show the version of the node library provided by Milesight.
Upgrade Node Library	Upgrade the node library by importing the library package.
All Flows Export	Export all flows as a JSON format file.
Restore to Factory Settings	Erase all flows data of Node-RED.
Uninstall	Uninstall the Node-RED App from this device.

Milesight provides a customized node library to use the interfaces of the device.



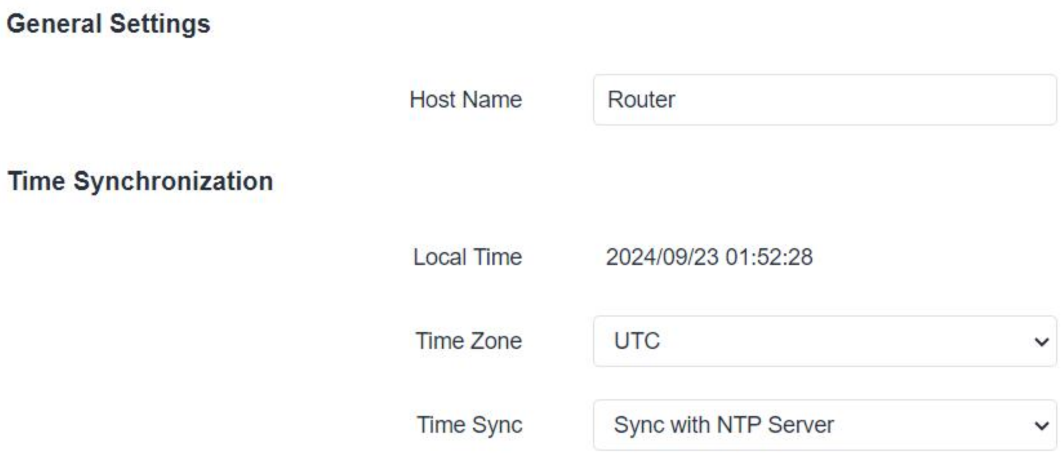
Node Library	
Node	**Description**
Router Event	Monitor alarm events of the device.
SMS Input	Receive SMS message. This only works when the cellular is connected.
SMS Output	Send an SMS message. This only works when the cellular is connected.
Digital Input	Receive DI status. This only works when DI is enabled and Action is Node-RED on **Service > I/O > DI** web GUI.
Digital Output	Trigger DO status. This only works when DO is enabled on **Service > I/O > DO** web GUI.
Serial Input	Receive serial port data. This only works when the serial port is enabled, Serial Mode is DTU and DTU protocol is Node-RED on **Service > Serial Port > Serial Port** web GUI.
Serial Output	Send command to the serial port. This only works when the serial port is enabled, Serial Mode is DTU and DTU protocol is Node-RED on **Service > Serial Port > Serial Port** web GUI.
GPS Read	Receive GPS data. This only works when GPS is enabled on **Service > GPS > GPS** web GUI.

7.6 System

This section describes how to configure general settings and debugs, such as administration account, system time, common user management, device management, download logs, etc.

7.6.1 Administration

7.6.1.1 System Settings



General Settings

Host Name: Router

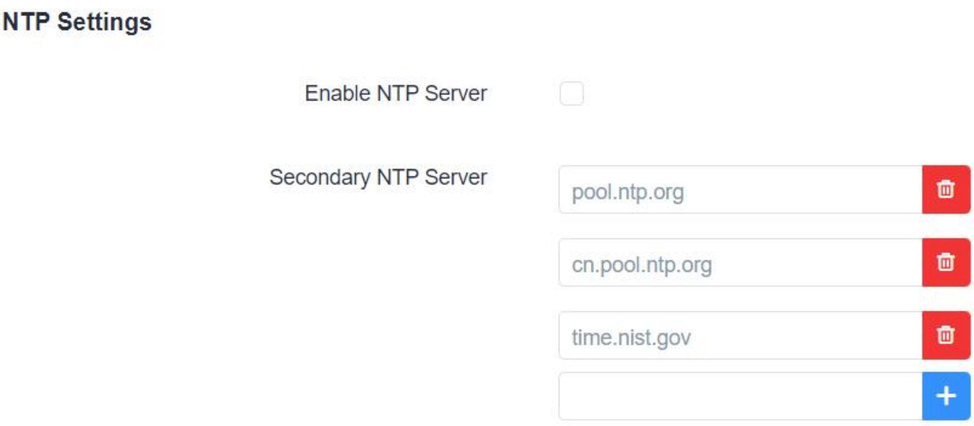
Time Synchronization

Local Time: 2024/09/23 01:52:28

Time Zone: UTC

Time Sync: Sync with NTP Server

System - General Setting	
Item	**Description**
Hostname	Define the device name, needs to start with a letter.
Local Time	Show the current system time.
Timezone	Click the drop-down list to select the time zone you are in.
Time Synchronization	Select the time synchronization mode. **Sync Browser Time:** Synchronize time with browser. **Sync with NTP Server:** Synchronize time with NTP Server. **GPS Time Synchronization:** Synchronize time with GPS per hour. Ensure that GPS is enabled on **Service > GPS >GPS**. **Manual:** configure the time manually.



NTP Settings

Enable NTP Server: □

Secondary NTP Server: pool.ntp.org

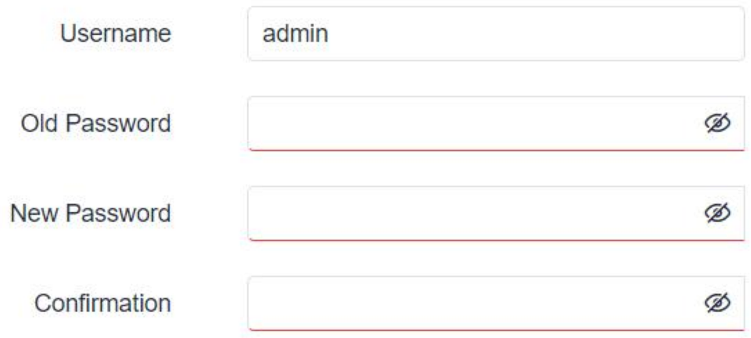
cn.pool.ntp.org

time.nist.gov

System - NTP Setting	
Item	**Description**
Enable NTP server	Enable to provide NTP server for connected devices.
NTP server candidates	Enter NTP Server's IP address or domain name to synchronize time. It can add 5 servers at most.

7.6.1.2 User Settings

You can change the administrator username or password for accessing the device.

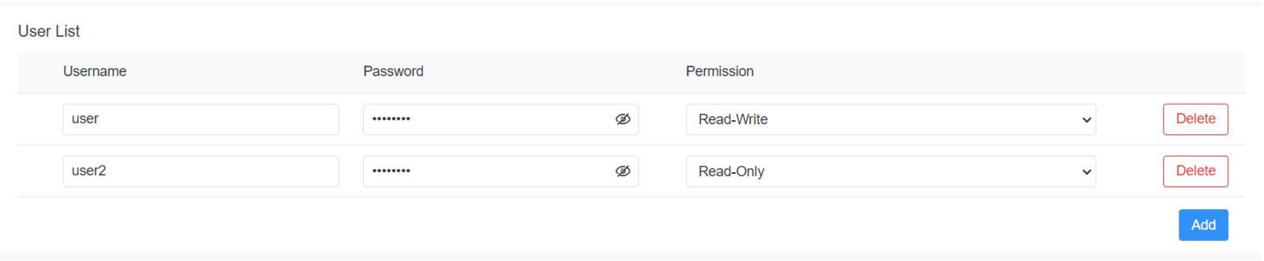


Username	admin
Old Password	
New Password	
Confirmation	

Change Account Info	
Item	**Description**
Username	Enter the username of administrator account.
Old Password	Enter the old password to verify the authority.
New Password	Enter a new password. You can use any ASCII characters except blank.
Confirmation	Enter the new password again.

7.6.1.3 Multi User Management

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



User List

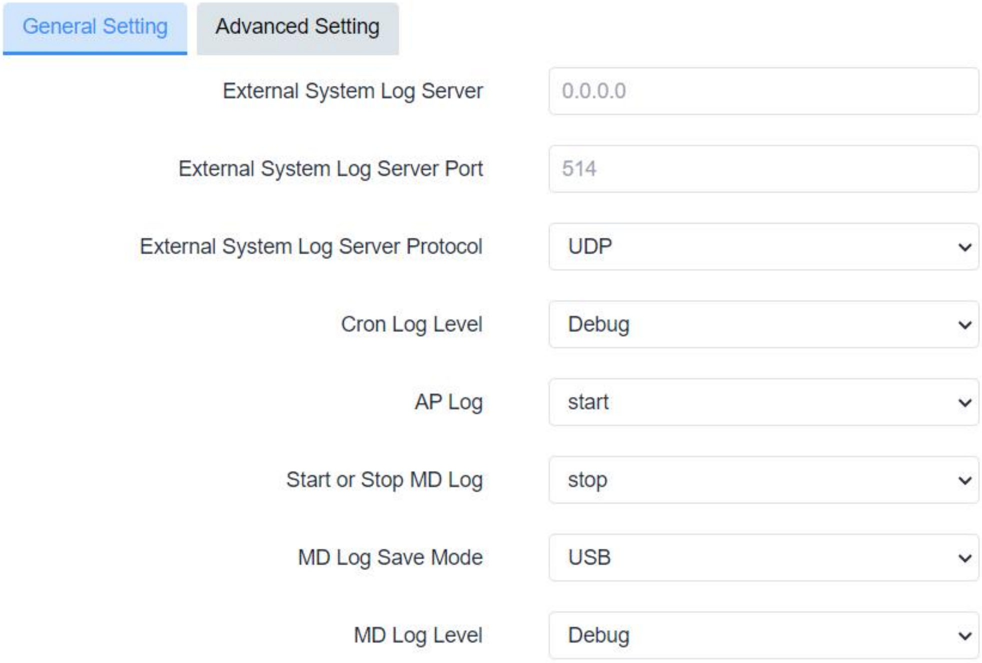
Username	Password	Permission	
user	••••••••	Read-Write	Delete
user2	••••••••	Read-Only	Delete

User List	
Item	**Description**
Username	Enter a new username. You can use characters such as a-z, 0-9, "_", "-". The first character must be a letter or "_".
Password	Set password. You can use any ASCII characters except blank.
Permission	Select user permission from "Read-Only" and "Read-Write". **Read-Only:** users can only view the configuration of router in this level. **Read-Write:** users can view and set the configuration of router in this level.

7.6.2 Maintenance

7.6.2.1 Log

Users can download logs contains a record of informational, error and warning events that indicates how the system processes. By reviewing the data 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 the device will upload all system logs to remote log server such as Syslog Watcher.



External System Log Server: 0.0.0.0

External System Log Server Port: 514

External System Log Server Protocol: UDP

Cron Log Level: Debug

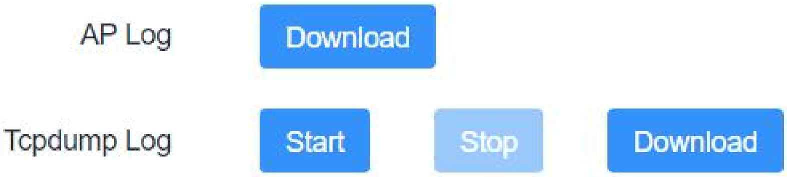
AP Log: start

Start or Stop MD Log: stop

MD Log Save Mode: USB

MD Log Level: Debug

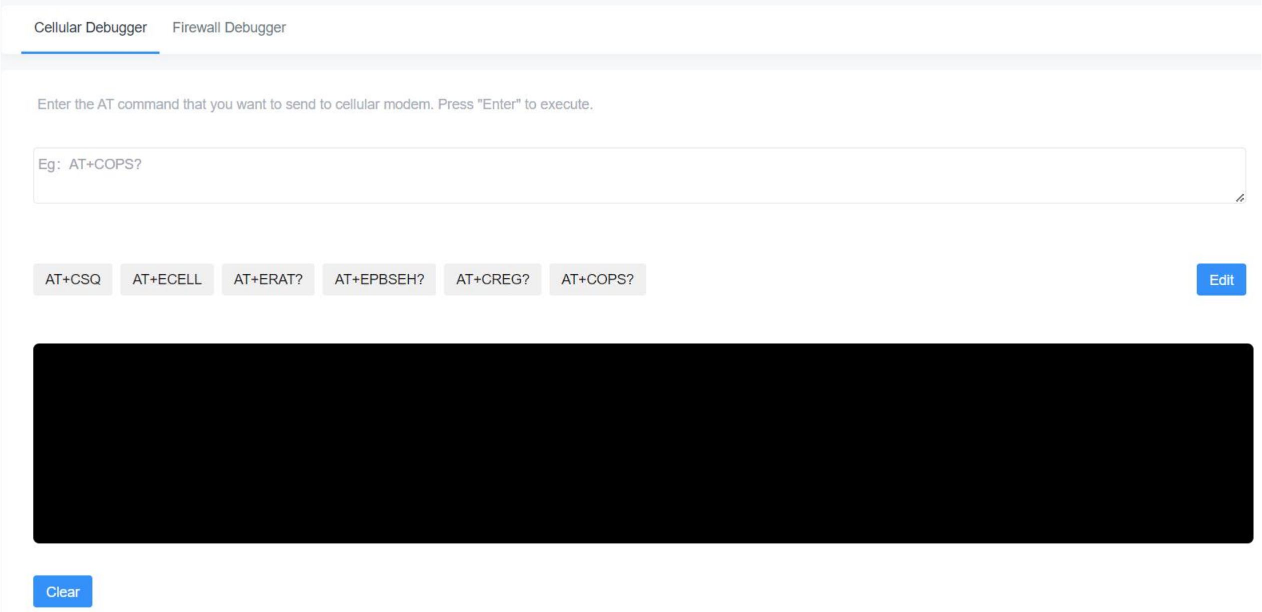
Log - General Settings	
Item	**Description**
External system log server	Fill in the remote log server address (IP/domain name) which the device sends.
External system log server port	Fill in the remote log server port which the device sends.
External system log server protocol	Choose UDP or TCP from the drop-down list to transmit log file in corresponding protocol.
Cron Log Level	The severities to print the AP log: Normal, Warning, Debug.
AP Log	Select to start or stop recording system log.
Start or Stop MD Log	Select to start or stop recording cellular module log.
MD Log Save Mode	Select the save and output mode of MD log.
MD Log Level	The severities to print the MD log: Info, Notice, Warning, Error, Critical, Alert, Emergency, Debug.



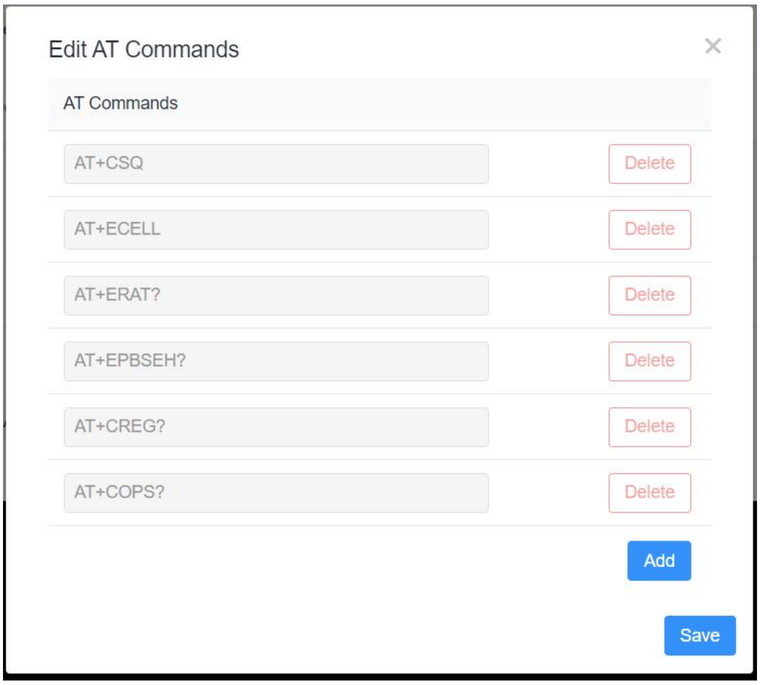
Log- Advanced Settings	
Item	**Description**
AP log	
Download	Click to download the last AP log recorded.
Tcpdump log	
Start	Click to start recording tcpdump log.
Stop	Click to stop recording tcpdump log.
Download	Click to download the last tcpdump log recorded.

7.6.2.2 Cellular Debugger

This tool allows to use AT commands to enter the AT command and press **Enter** to execute and check cellular debug information..



Besides, click **EDIT** to customize the common AT commands, then press the buttons on the top of black frame directly to execute common commands directly.



Edit AT Commands

AT Commands

AT+CSQ

AT+ECELL

AT+ERAT?

AT+EPBSEH?

AT+CREG?

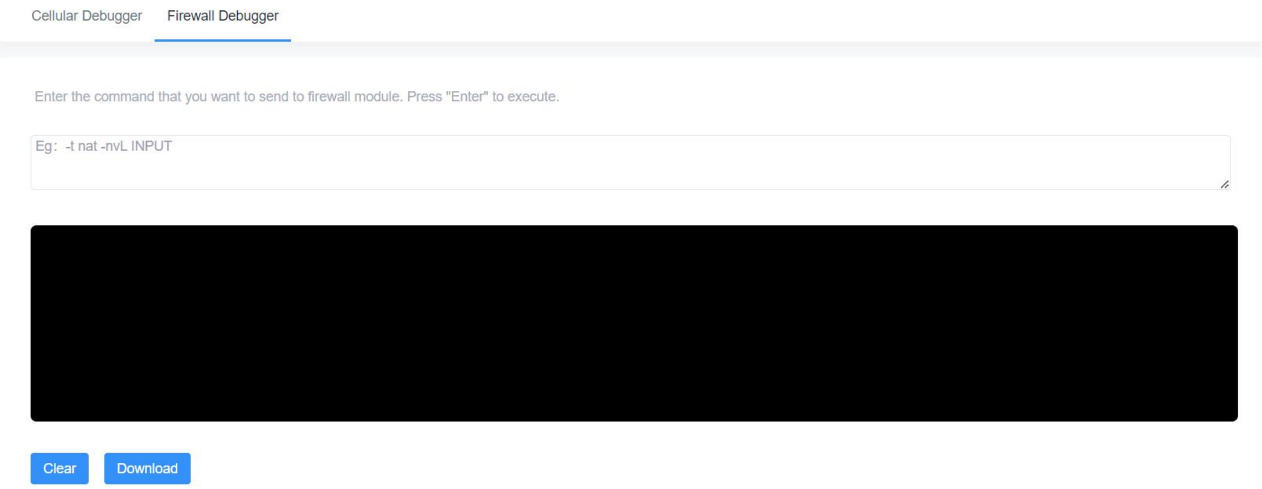
AT+COPS?

Common command description:

AT+CSQ?----Get cellular network signal
AT+ECELL?----Get current cell information
AT+ERAT?----Get RAT status and network type
AT+EPBSEH? ----Get using bands
AT+CREG?----Get network registration status
AT+COPS?----Get operator and access technology info

7.6.2.3 Firewall Debugger

This tool allows to use iptables commands to check firewall information and download results.



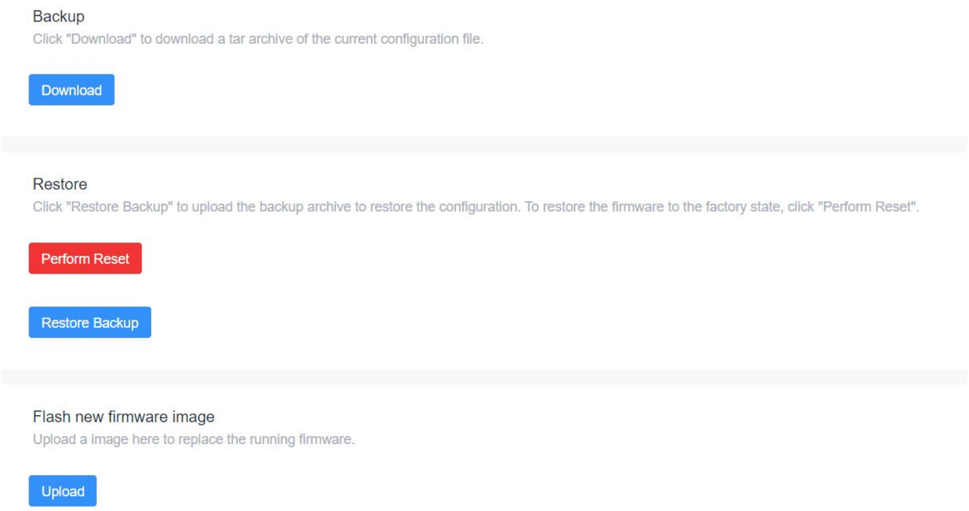
Enter the command that you want to send to firewall module. Press "Enter" to execute.

Eg：-t nat -nvL INPUT

7.6.2.4 Backup/Upgrade

This section describes how to create a complete backup of the system configurations to a file, reset to factory defaults, restore the config file to the device and upgrade the flash image via the 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 worse the device will break down.



Backup

Click "Download" to download a tar archive of the current configuration file.

Restore

Click "Restore Backup" to upload the backup archive to restore the configuration. To restore the firmware to the factory state, click "Perform Reset".

Flash new firmware image

Upload a image here to replace the running firmware.

Backup/Upgrade	
Item	**Description**
Generate Backup	Click to download a tar archive of the current configuration file.
Perform Reset	Click to reset the device to factory default.
Restore Backup	To restore configuration files, you can upload a previously generated backup archive here. Custom files (certificates, scripts) may remain on the system. To prevent this, you can perform a factory-reset first.
Upload	Upload an image here to replace the running firmware.

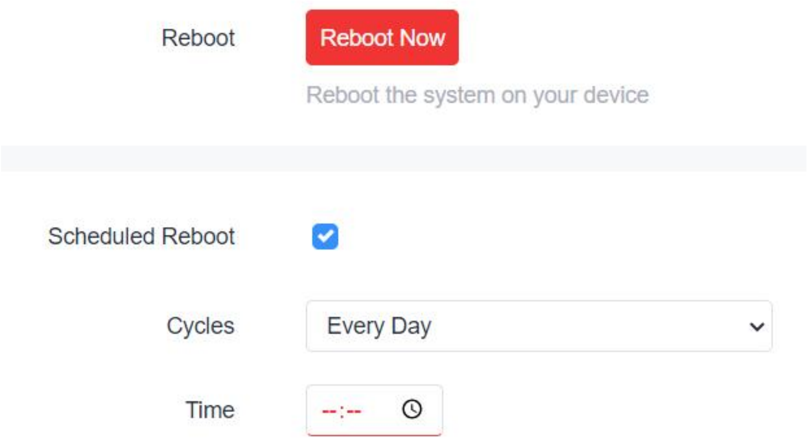
Related Configuration Example

Firmware Upgrade

Restore Factory Defaults

7.6.2.5 Reboot

This page allows to reboot the device immediately or regularly.



Reboot

Reboot the system on your device

Scheduled Reboot ☑

Cycles: Every Day

Time: --:--

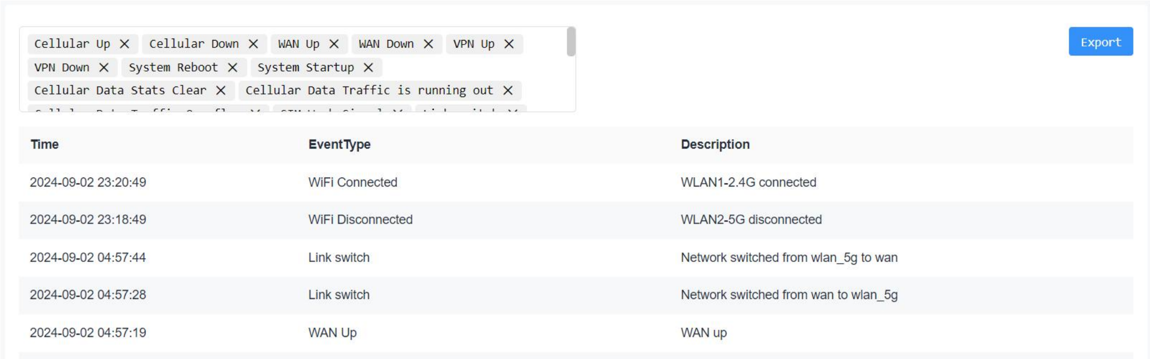
Reboot	
Item	**Description**
Reboot Now	Reboot the device immediately.
Schedule	
Enable	Click to enable reboot schedule.
Cycles	Reboot the device at a scheduled frequency.
Time	Select the time to execute the schedule.

7.6.3 Event Alarm

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

7.6.3.1 Event Alarm

You can view alarm messages on this page.



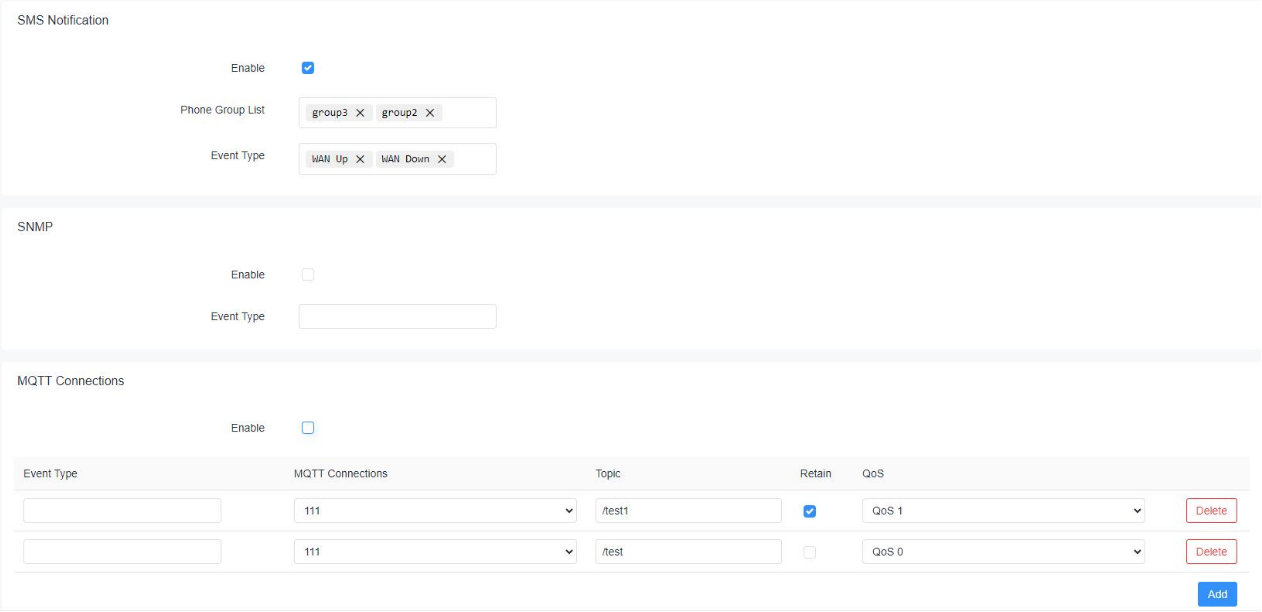
Cellular Up ✕ Cellular Down ✕ WAN Up ✕ WAN Down ✕ VPN Up ✕
VPN Down ✕ System Reboot ✕ System Startup ✕
Cellular Data Stats Clear ✕ Cellular Data Traffic is running out ✕
Export

Time	EventType	Description
2024-09-02 23:20:49	WiFi Connected	WLAN1-2.4G connected
2024-09-02 23:18:49	WiFi Disconnected	WLAN2-5G disconnected
2024-09-02 04:57:44	Link switch	Network switched from wlan_5g to wan
2024-09-02 04:57:28	Link switch	Network switched from wan to wlan_5g
2024-09-02 04:57:19	WAN Up	WAN up

Event Alarm	
Item	**Description**
Search	Select the event alarm you need to display on this list.
Export	Export the event alarm list to A CSV format file.
Time	Show the alarm time.
Event Type	Show the type of event alarms.
Description	Show the details of event alarms.

7.6.3.2 Events Settings

In this section, you can decide whether you want to receive SMS, SNMP or MQTT notifications when any change occurs.



SMS Notification

Enable ☑

Phone Group List: group3 × group2 ×

Event Type: WAN Up × WAN Down ×

SNMP

Enable □

Event Type

MQTT Connections

Enable □

Event Type	MQTT Connections	Topic	Retain	QoS	
	111	/test1	☑	QoS 1	Delete
	111	/test	□	QoS 0	Delete

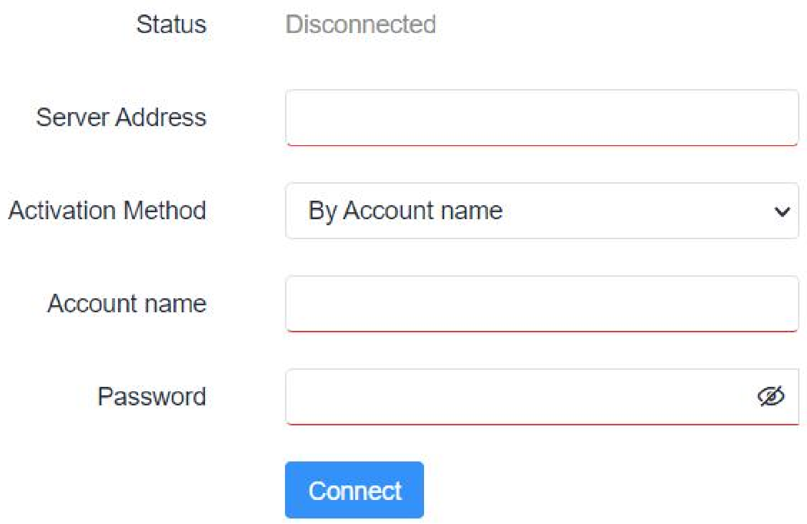
Add

Event Settings	
Item	**Description**
SMS Notification	
Enable	Check to enable SMS notification when event is triggered.
Phone Group List	Select phone group to receive SMS notifications.
Event Type	Select the event type which need to send SMS notifications.
SNMP	
Enable	Check to enable SNMP notification when event is triggered.
Event Type	Select the event type which need to record via SNMP.
MQTT Connections	
Enable	Check to enable MQTT notification when event is triggered.
Event Type	Select the event type which need to send MQTT notifications.
MQTT Connection	Select the MQTT connection to send notifications, it's set up on **Service > MQTT** page.
Topic	Topic name used for publishing serial port data.
Retain	Enable to set the latest message of this topic as retain message.
QoS	QoS0, QoS1 or QoS2 are optional.

7.6.4 Device Management

7.6.4.1 Device Management

You can connect the device to the Milesight DeviceHub management platform on this page so as to manage the device centrally and remotely. For more details, please refer to ***DeviceHub User Guide***.



Status Disconnected

Server Address

Activation Method By Account name

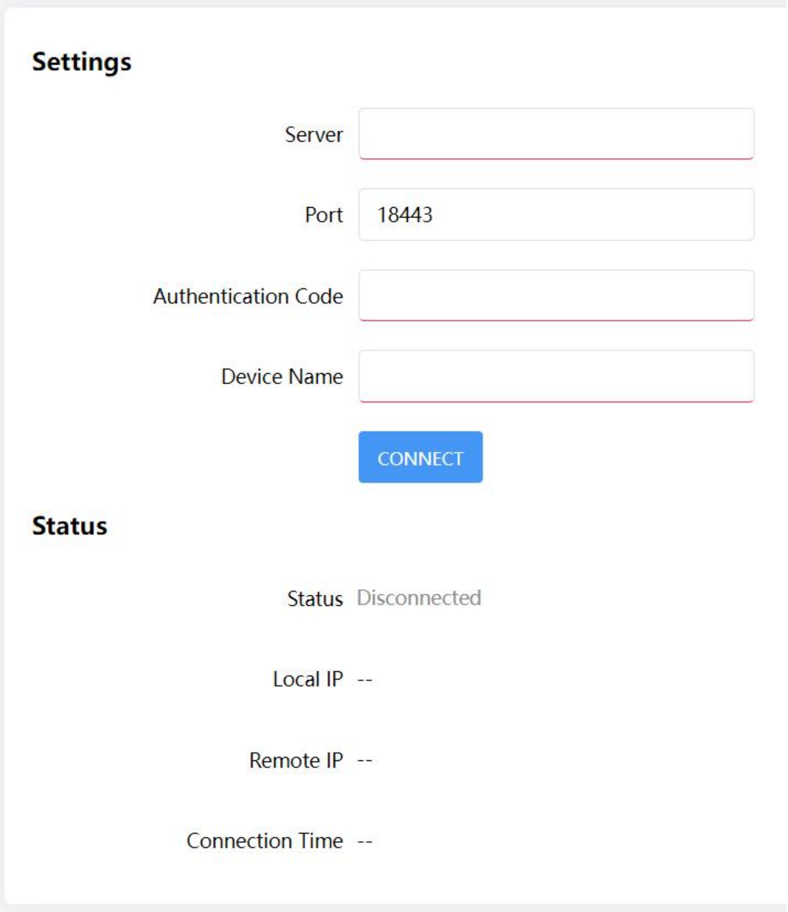
Account name

Password

Device Management	
Item	**Description**
Status	Show the connection status between the device and the DeviceHub.
Server Address	IP address or domain of the DeviceHub management server.
Activation Method	Select activation method to connect the device to the DeviceHub server, options are "**By Authentication Code**" and "**By Account name**".
Authentication Code	Fill in the authentication code generated from the DeviceHub.
Account Name	Fill in the registered DeviceHub account (email) and password.
Password	
Connect/Disconnect	Click this button to connect/disconnect the device from the DeviceHub.

7.6.4.2 Cloud VPN

You can connect the device to the MilesightVPN on this page so as to manage the device and connected devices centrally and remotely. For more details please refer to ***MilesightVPN User Guide***.



Settings

Server

Port 18443

Authentication Code

Device Name

Status

Status Disconnected

Local IP --

Remote IP --

Connection Time --

Cloud VPN	
Item	**Description**
Settings	
Server	Enter the IP address or domain name of MilesightVPN.
Port	Enter the HTTPS port number.
Authorization code	Enter the authorization code which generated by MilesightVPN.
Device Name	Enter the name of the device.
Status	
Status	Show the connection information about whether the device is connected to the MilesightVPN.
Local IP	Show the virtual IP of the device.
Remote IP	Show the virtual IP of the Milesight VPN server.
Connection Time	Show the information on how long has the device been connected to the Milesight VPN.

[END]