Milesight

5G Dongle

UF31

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.
- ❖ 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.
- ❖ Do not pull the antenna or power supply cable, detach them by holding the connectors.

Declaration of Conformity

UF31 is in conformity with the essential requirements and other relevant provisions of 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
May 11, 2022	V 1.0	Initial version
July 27, 2022	V 1.1	Change default cellular antenna, delete Ethernet cable
March 20, 2023	V 1.2	1. Accessories adjustment 2. Web GUI design change 3. Add firewalls, OpenVPN, IPsec VPN and GPS feature

Contents

1. Product Introduction

1.1 Overview

Milesight UF31 5G Dongle is designed as an easy-to-use solution providing for 5G wireless networking application. It supports 5G NSA & SA, 4G LTE and 3G networks from telecom service providers of most countries in the world. The USB type-C port and Ethernet port are adopted to provide high-speed internet access for field devices.

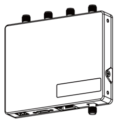
With a compact size and industrial design, UF31 is easy to carry out or embed to any equipment, which is particularly suitable for smart offices, video surveillance, digital media implementations, industrial automation, traffic applications, robots and so on.

1.2 Key Features

- Support global 5G NSA&SA/4G LTE/WCDMA network, enables up to 4.13 Gbps download speeds
- Plug and play, provide lightning transmission via Gigabit Ethernet port or USB 3.0
- Embeds hardware watchdog to automatically recover from various failure, ensure highest level of availability
- Wide operating temperature range from -20°C to 50°C and industrial design for harsh environment
- USB or DC power supply optional
- Easy to deploy anywhere with compact size, suit for embedded installation
- Iptables firewall and VPN tunnels to ensure security data transmission
- WEB GUI and CLI enable the admin to achieve simple management and quick configuration among a large quantity of devices
- DeviceHub provides remote monitoring, bulk configuration, and centralized management

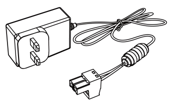
2. Hardware Introduction

2.1 Packing List



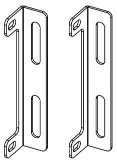
1 ×

UF31 Device



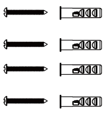
1 ×

Power Adapter



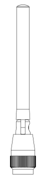
2 ×

Mounting Ear Kits

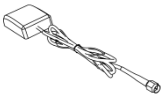


4 × Wall Mounting

Kits



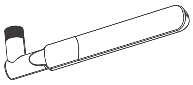
4 × Mini Stubby Cellular Antennas



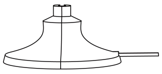
1 x GPS Antenna

1 × Quick Guide

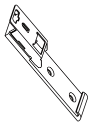
1 × Warranty Card



4 × Stubby Cellular Antennas(Optional)



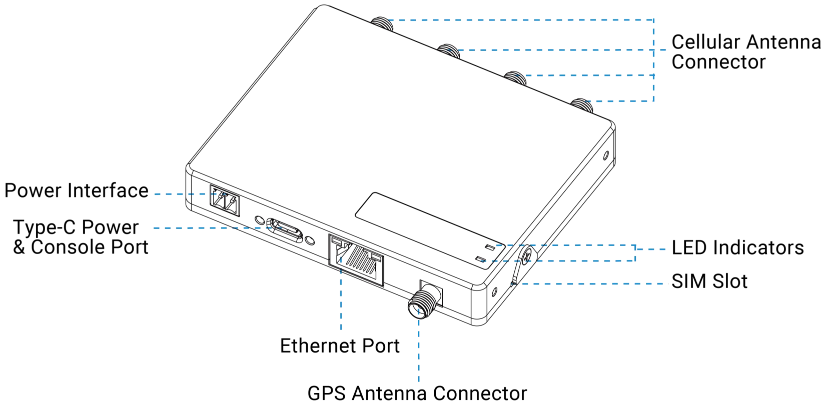
4 × Antenna Magnetic Mounts(Optional)



1 x DIN Rail Clip (Optional)

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

2.2 Hardware Overview

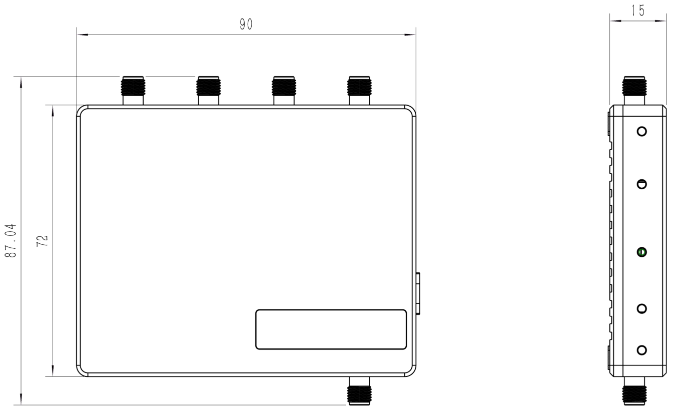


2.3 LED Indicators

LED	Indication	Status	Description
STATUS	Power & System Status	Off	The power is switched off
		Orange	Static: The system is startup
		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

2.4 Dimensions (mm)



2.5 Reset Button

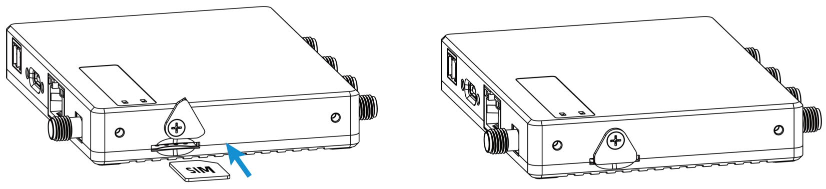
The reset button is inside the device.

Function	Description	
	STATUS & 5G LED	Action
Reset	Static	Press and hold the reset button for more than 5 seconds.
	Static → Blinking	Release the button and wait.
	Off → Static Green	The device resets to factory default.

3. Hardware Installation

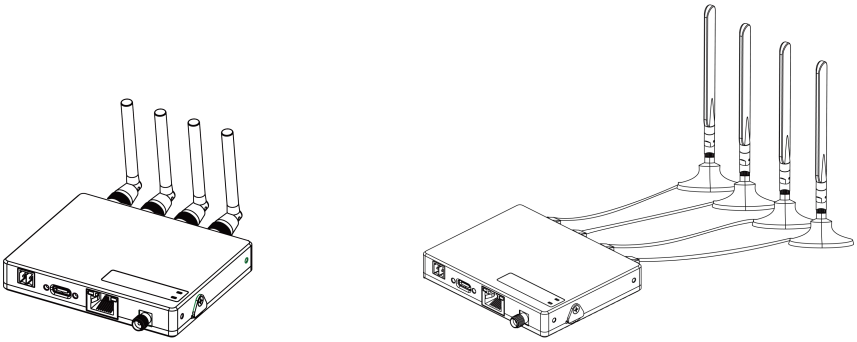
3.1 SIM Installation

Remove the sheet on the SIM slot, insert the SIM card into the slot according to the direction icon on the device, then fix the sheet on the slot with screw.



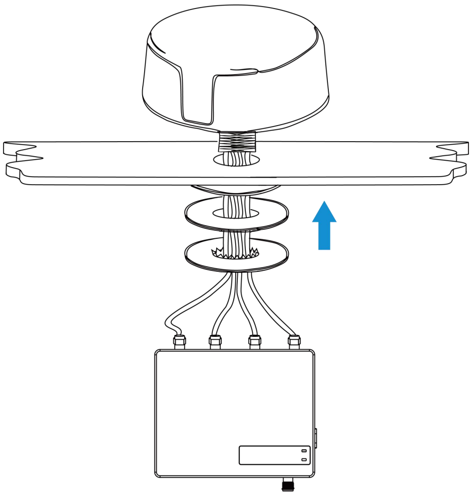
3.2 Antenna Installation

Rotate the antenna into the antenna connector accordingly. Antennas should be installed vertically always on a site with a good signal.



If an antenna box is being used, the installation position should be drilled a hole to fix the antenna box.

- Recommended hole size: ϕ28.0 ± 0.5 mm
- Recommended thickness size: 3.0 ± 1.0 mm

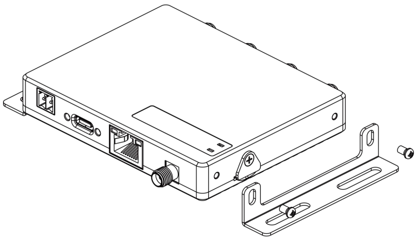


3.3 Device Installation

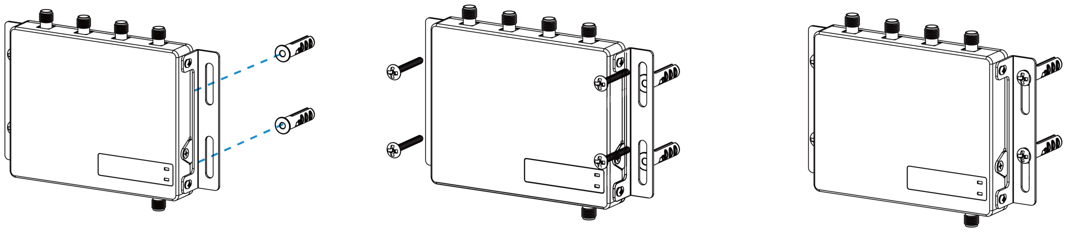
UF31 device can be placed on a desktop or mounted to a wall or a DIN rail.

3.3.1 Wall Mounting

1. Fix the two mounting ears to both side of the device with screws.

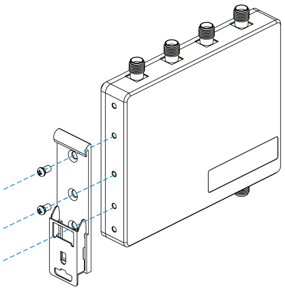


2. Drill 4 holes on the wall according to the mounting ear's hole and fix the wall plugs into the wall holes, then fix the device to the wall plugs with mounting screws. When installation, it's suggested to fix the two screws on the top at first.

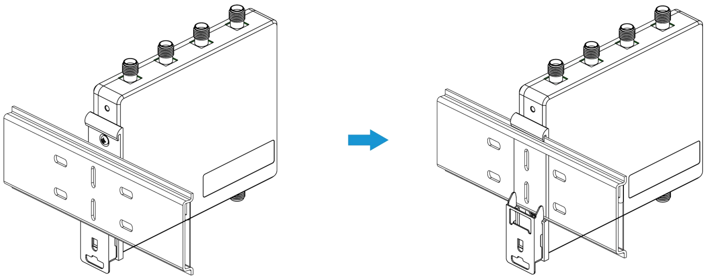


3.3.2 DIN Rail Mounting

1. Fix the mounting clip to the device with 3 screws.

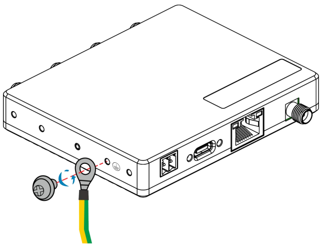


2. Hang the device to the DIN rail. The width of DIN rail is 3.5 cm.



3.4 Protective Grounding Installation

Connect the grounding ring of the cabinet's grounding wire onto the grounding stud and screw up the grounding nut.



4. Access to Web GUI

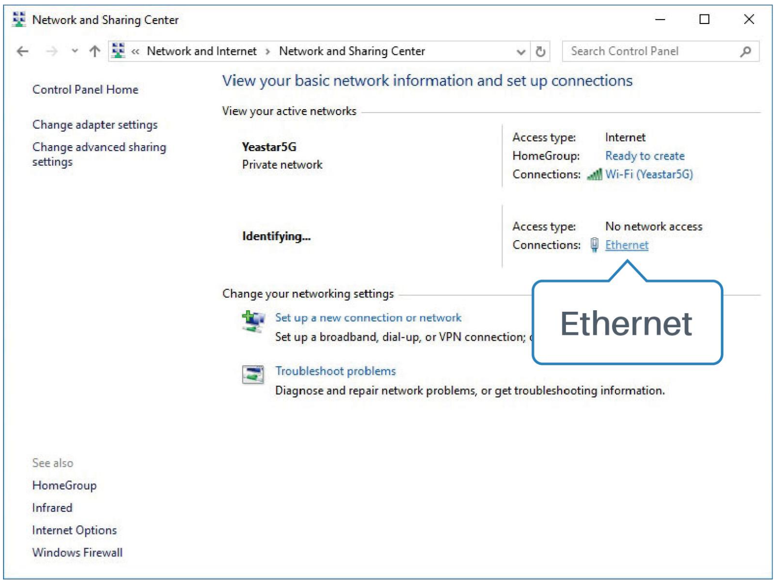
UF31 provides user-friendly web GUI for configuration and users can access it via LAN port or USB. This chapter explains how to access to Web GUI of the UF31 device.

Username: **admin**

Password: **password**

Connect PC to the LAN port or USB port directly to access the web GUI of device. 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...

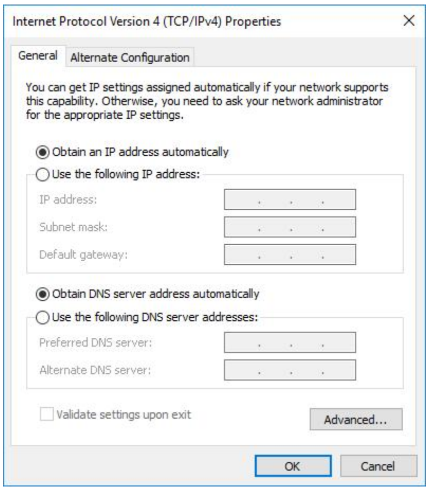
Access type: No network access
Connections: Ethernet

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.

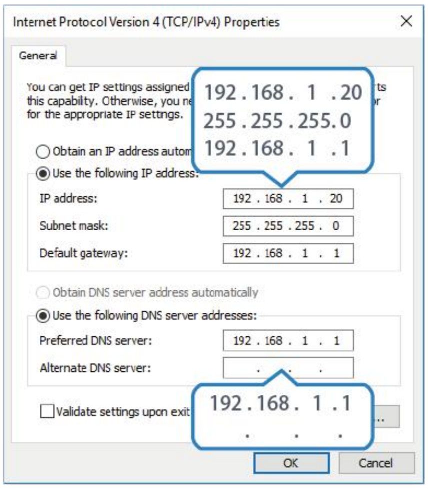


You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit



You can get IP settings assigned this capability. Otherwise, you n for the appropriate IP settings.

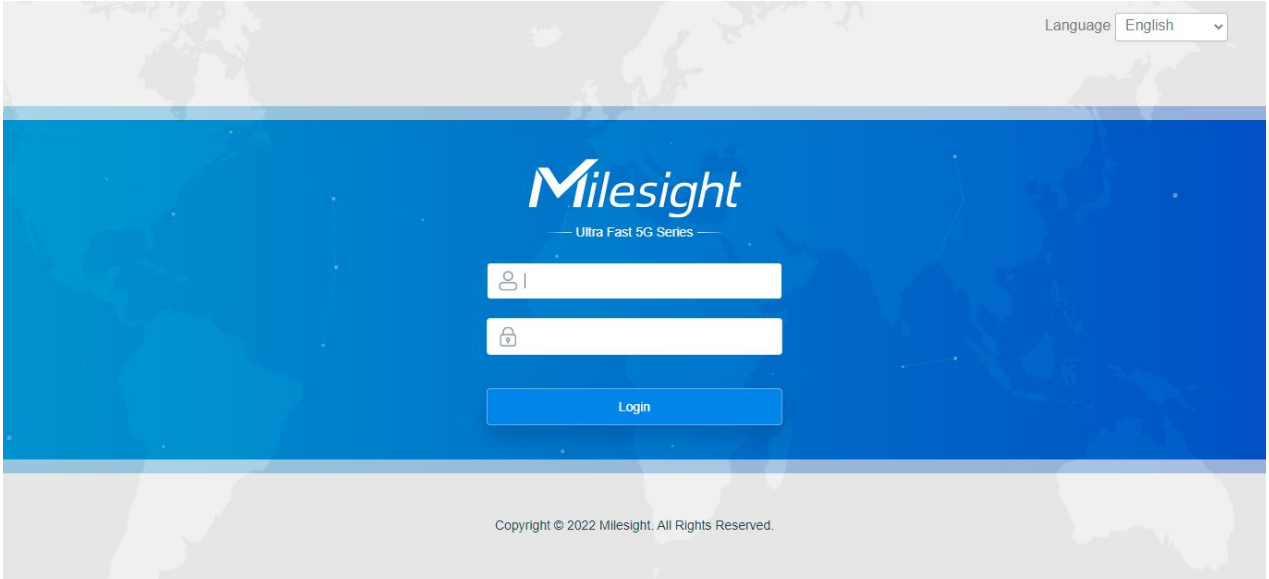
○ Obtain an IP address autom
● Use the following IP address:
IP address: 192 . 168 . 1 . 20
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1

○ 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) and type in the IP address **192.168.1.1** to access the web GUI.

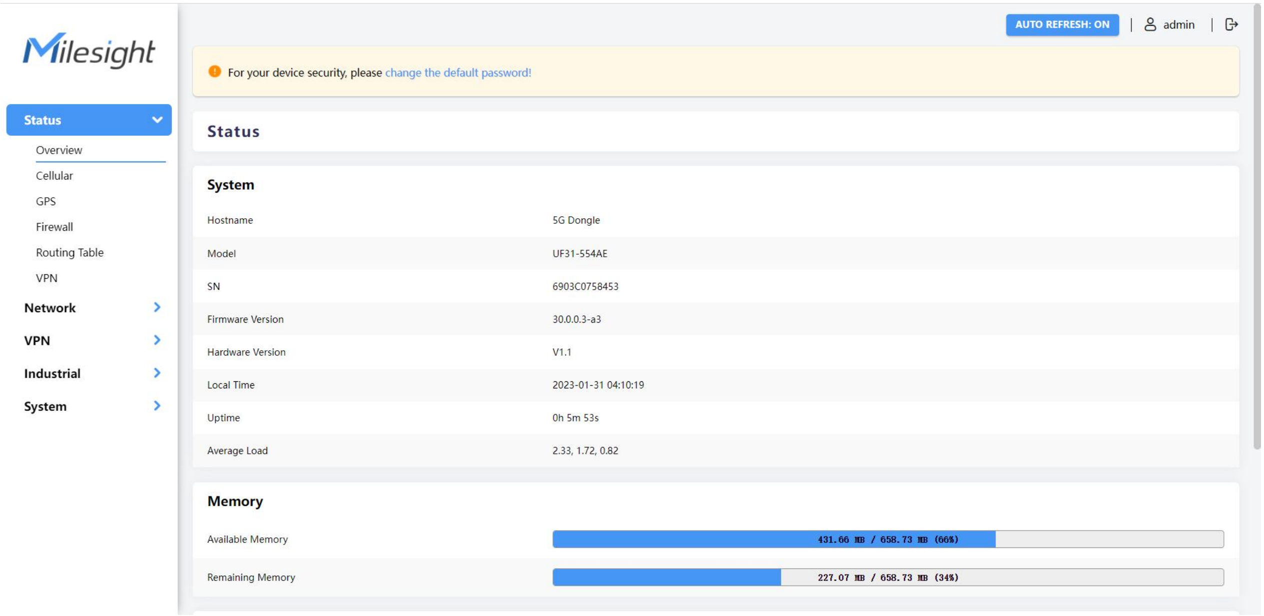
4. Enter the username and password, click “Login”.



Copyright © 2022 Milesight. All Rights Reserved.

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

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



For your device security, please change the default password!

Status

System

Hostname	5G Dongle
Model	UF31-554AE
SN	6903C0758453
Firmware Version	30.0.0.3-a3
Hardware Version	V1.1
Local Time	2023-01-31 04:10:19
Uptime	0h 5m 53s
Average Load	2.33, 1.72, 0.82

Memory

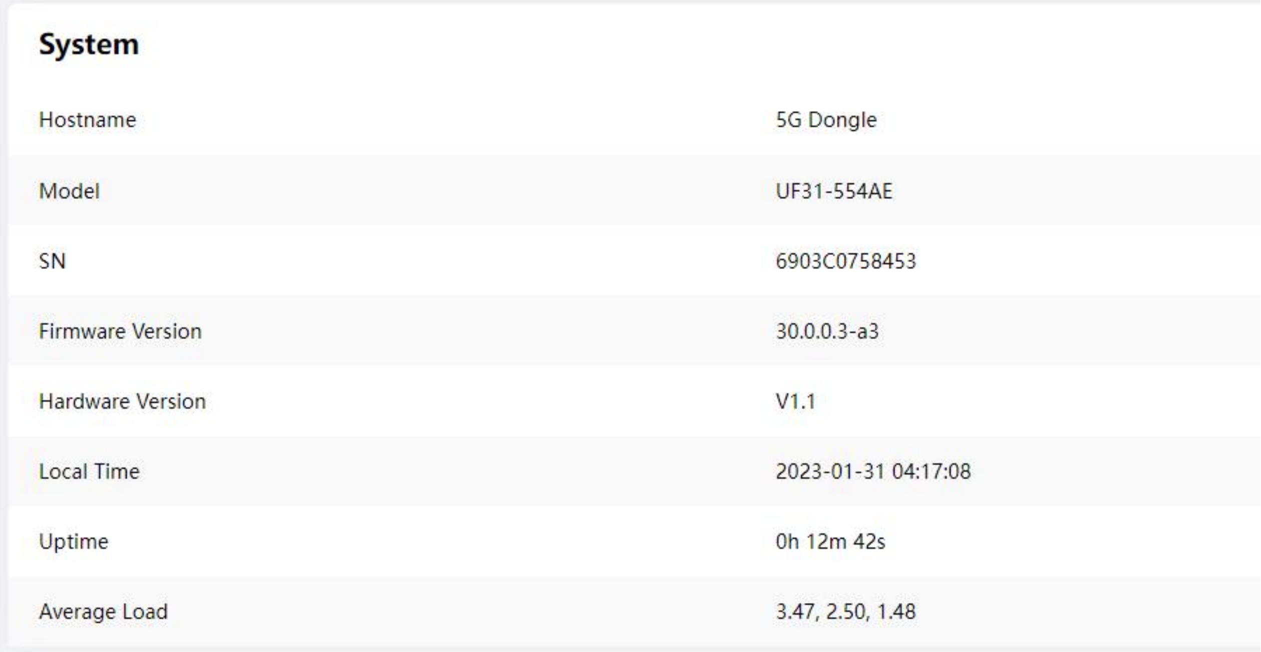
Available Memory	431.66 MB / 658.73 MB (66%)
Remaining Memory	227.07 MB / 658.73 MB (34%)

5. Web Configuration

5.1 Status

5.1.1 Overview

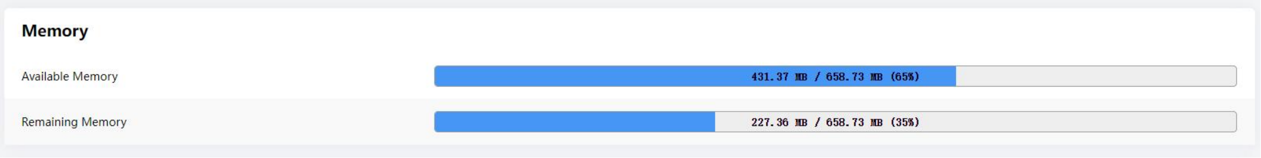
You can view the system information of the device on this page.



System

Hostname	5G Dongle
Model	UF31-554AE
SN	6903C0758453
Firmware Version	30.0.0.3-a3
Hardware Version	V1.1
Local Time	2023-01-31 04:17:08
Uptime	0h 12m 42s
Average Load	3.47, 2.50, 1.48

System	
Item	**Description**
Hostname	Show the hostname of device, it can be modified on **System > System > General Settings**.
Model	Show the model name of device.
SN	Show the serial number of device.
Firmware Version	Show the current firmware version of device.
Hardware Version	Show the current hardware version of device.
Local Time	Show the current system time of device.
Uptime	Show the time since device has been powered and running.
Average Load	Averages over progressively longer periods of time (1, 5 and 15 minute averages), lower numbers are better.

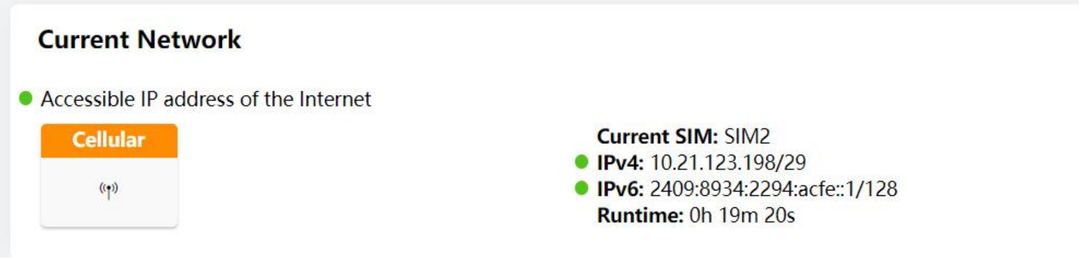


Memory

Available Memory	431.37 MB / 658.73 MB (65%)
Remaining Memory	227.36 MB / 658.73 MB (35%)

Memory	
Item	**Description**
Available Memory	Show the percentage of available RAM.
Remaining Memory	Show the percentage of used RAM.

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



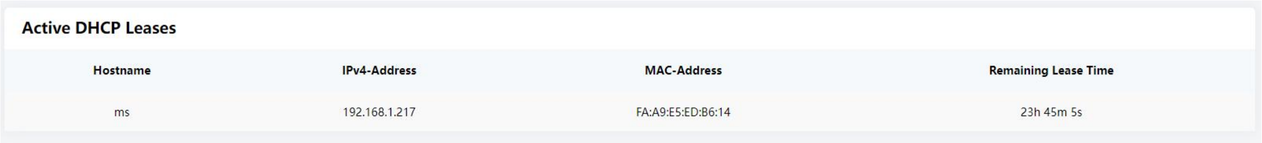
Current Network

● Accessible IP address of the Internet

Cellular

Current SIM: SIM2
● **IPv4:** 10.21.123.198/29
● **IPv6:** 2409:8934:2294:acfe::1/128
Runtime: 0h 19m 20s

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



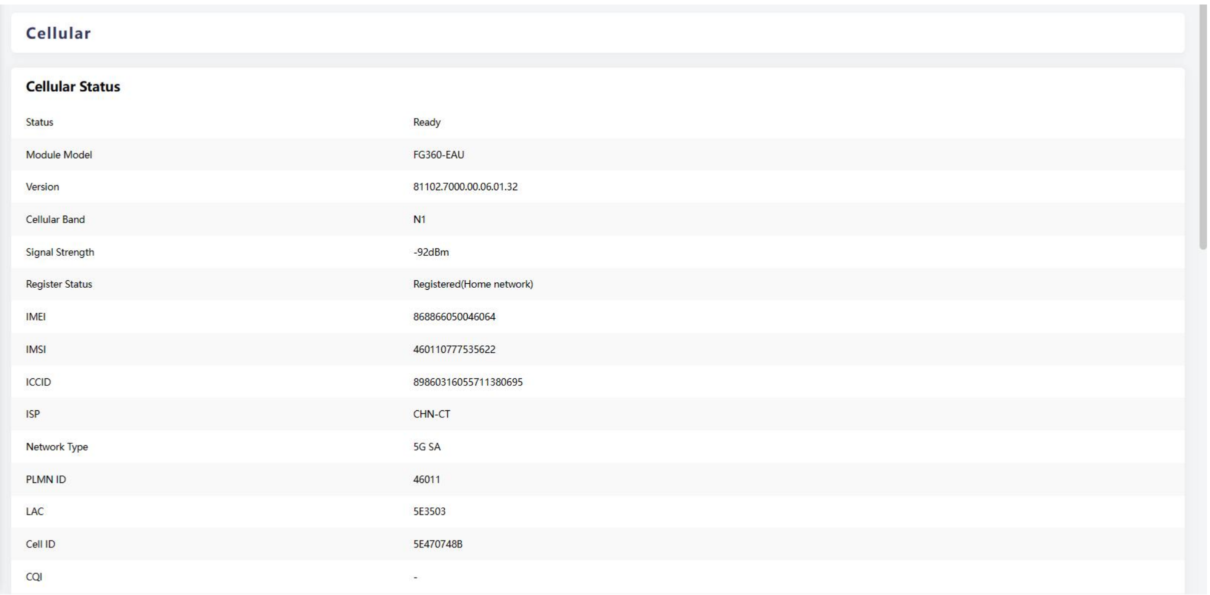
Active DHCP Leases

Hostname	IPv4-Address	MAC-Address	Remaining Lease Time
ms	192.168.1.217	FA:A9:E5:ED:B6:14	23h 45m 5s

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

5.1.2 Cellular

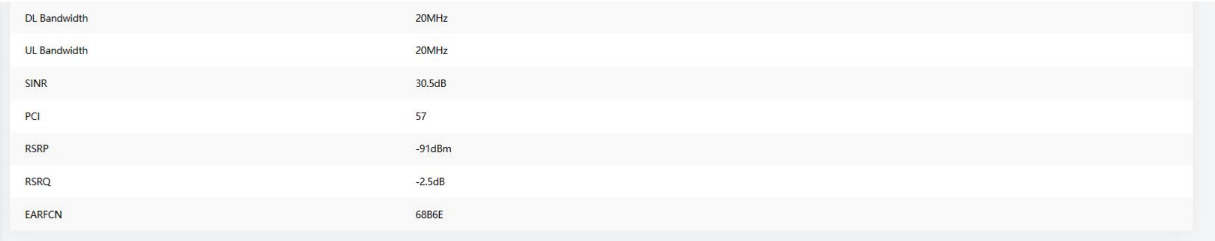
You can view the cellular network status of device on this page.



Cellular

Cellular Status

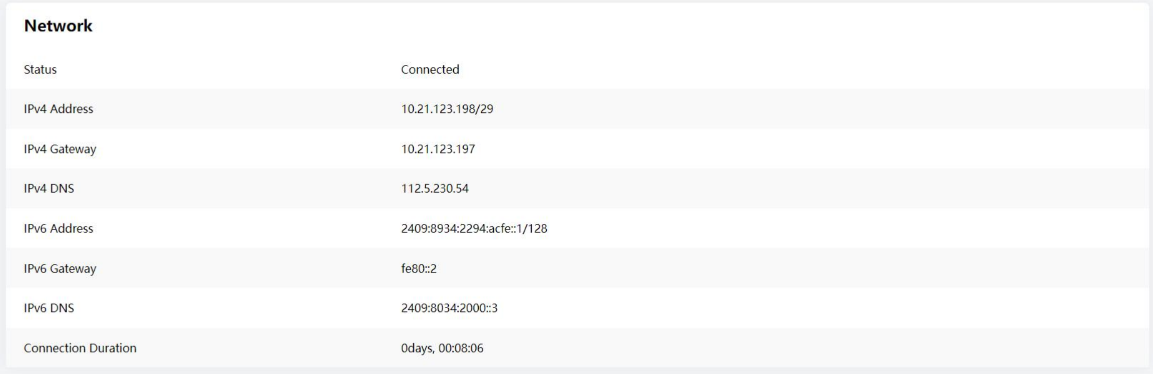
Status	Ready
Module Model	FG360-EAU
Version	81102.7000.00.06.01.32
Cellular Band	N1
Signal Strength	-92dBm
Register Status	Registered(Home network)
IMEI	868866050046064
IMSI	460110777535622
ICCID	89860316055711380695
ISP	CHN-CT
Network Type	5G SA
PLMN ID	46011
LAC	5E3503
Cell ID	5E470748B
CQI	-



DL Bandwidth	20MHz
UL Bandwidth	20MHz
SINR	30.5dB
PCI	57
RSRP	-91dBm
RSRQ	-2.5dB
EARFCN	68B6E

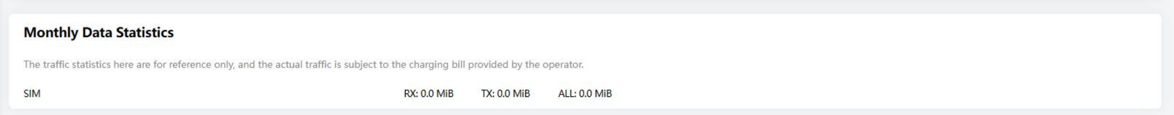
Modem Information

Item	Description
Status	Show corresponding detection status of module and SIM card.
Module Model	Show the name of cellular module.
Version	Show the cellular module firmware version.
Cellular Band	The cellular band which the device used to register to network.
Signal Strength	Show the cellular signal level.
Register Status	Show the registration status of SIM card.
IMEI	Show the IMEI of the module.
IMSI	Show IMSI of the SIM card.
ICCID	Show ICCID of the SIM card.
ISP	Show the network provider which the SIM card registers on.
Network Type	Show the connected network type, such as 5G NR, LTE, etc.
PLMN ID	Show the current PLMN ID, including MCC, MNC, LAC and Cell ID.
LAC	Show the location area code of the SIM card.
Cell ID	Show the Cell ID of the SIM card location.
CQI	Show the Channel Quality Indicator of the cellular network.
DL Bandwidth	Show the DL bandwidth of the cellular network.
UL Bandwidth	Show the UL bandwidth of the cellular network.
SINR	Show the Signal Interference + Noise Ratio of the cellular network.
PCI	Show the physical-layer cell identity of the cellular network.
RSRP	Show the Reference Signal Received Power of the cellular network.
RSRQ	Show the Reference Quality Received Power of the cellular network.
ECGI	Show the E-UTRAN Cell Global Identifier of the cellular network.
EARFCN	Show the E-UTRA Absolute Radio Frequency Channel Number.



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



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	RX: 0.0 MiB	TX: 0.0 MiB	ALL: 0.0 MiB

Network

Item	Description
Status	Show the connection status of cellular network.
IPv4/IPv6 Address	Show the IPv4/IPv6 address and netmask of cellular network.
IPv4/IPv6 Gateway	Show the IPv4/IPv6 gateway and netmask of cellular network.

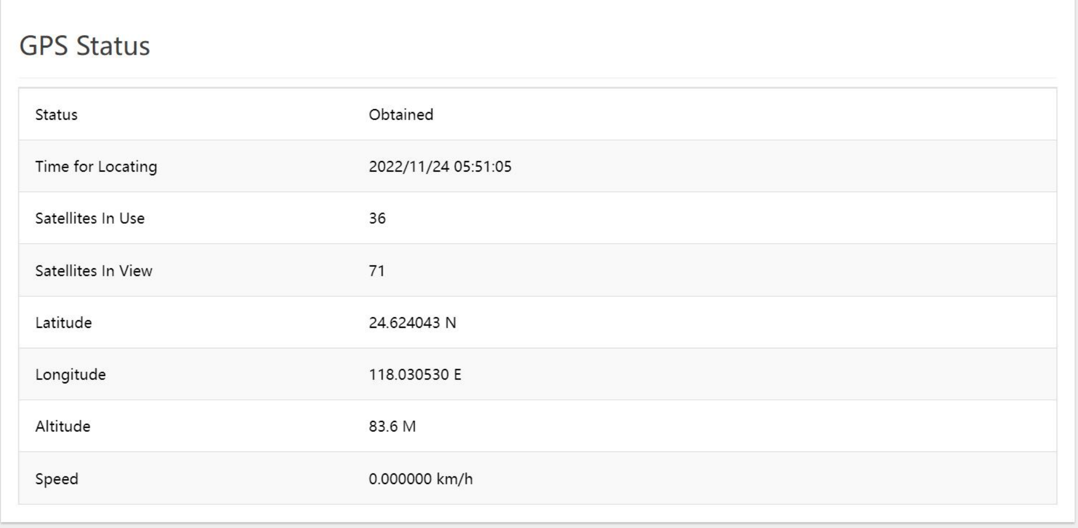
IPv4/IPv6 DNS	Show the DNS of cellular network.
Connection Duration	Show information on how long the cellular network has been connected.
RX	The data volume and packets received of this month.
TX	The data volume and packets transmitted of this month.
ALL	Total data volume and packets of this month.

Related Application

Cellular Application

5.1.3 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.



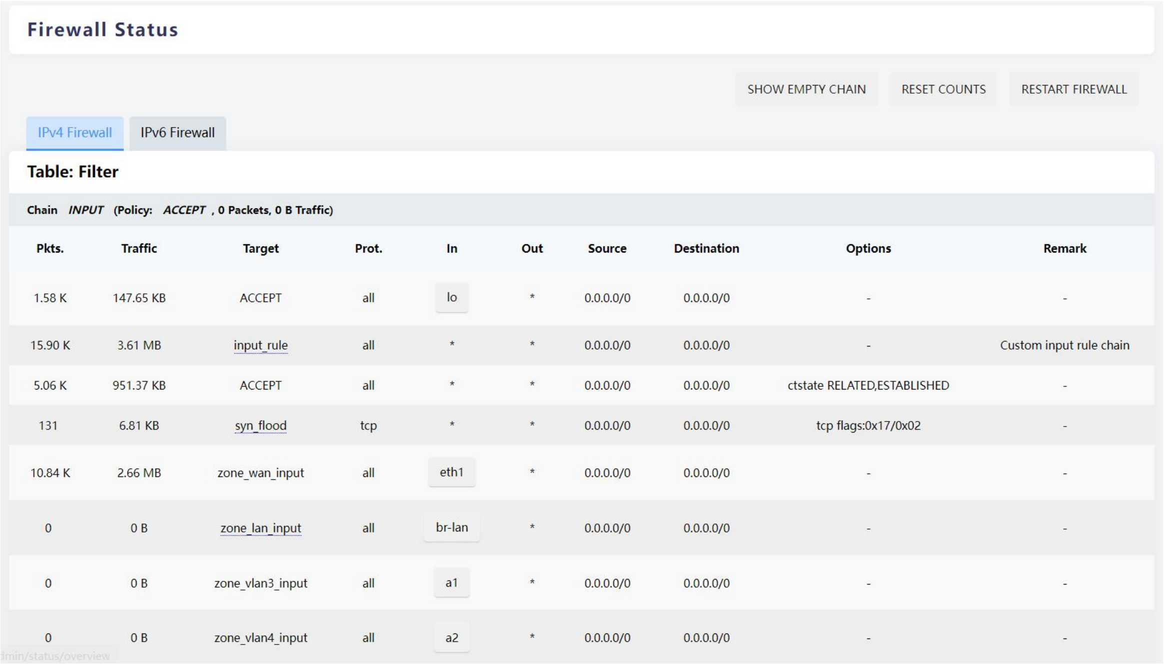
GPS Status

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.

5.1.4 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.



Firewall Status

SHOW EMPTY CHAIN RESET COUNTS RESTART FIREWALL

IPv4 Firewall IPv6 Firewall

Table: Filter

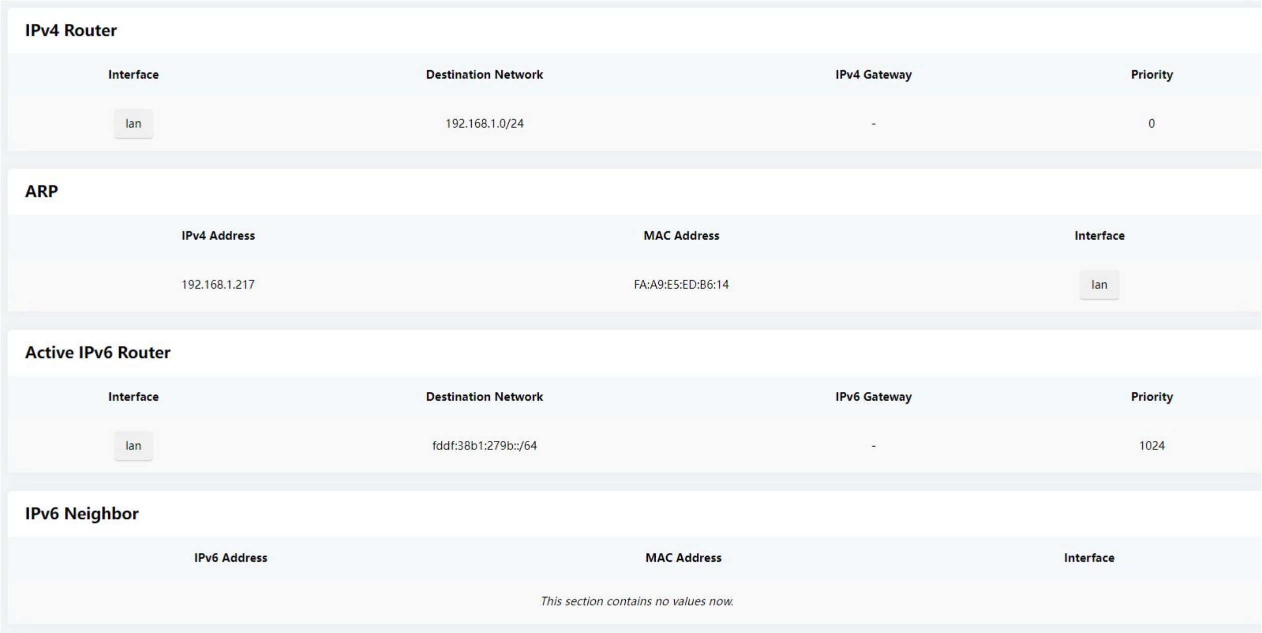
Chain *INPUT* (Policy: *ACCEPT* , 0 Packets, 0 B Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Remark
1.58 K	147.65 KB	ACCEPT	all	lo	*	0.0.0.0/0	0.0.0.0/0	-	-
15.90 K	3.61 MB	input_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom input rule chain
5.06 K	951.37 KB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	-
131	6.81 KB	syn_flood	tcp	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02	-
10.84 K	2.66 MB	zone_wan_input	all	eth1	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	zone_lan_input	all	br-lan	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	zone_vlan3_input	all	a1	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	zone_vlan4_input	all	a2	*	0.0.0.0/0	0.0.0.0/0	-	-

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.

5.1.5 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
lan	192.168.1.0/24	-	0

ARP

IPv4 Address	MAC Address	Interface
192.168.1.217	FA:A9:E5:ED:B6:14	lan

Active IPv6 Router

Interface	Destination Network	IPv6 Gateway	Priority
lan	fddf:38b1:279b::/64	-	1024

IPv6 Neighbor

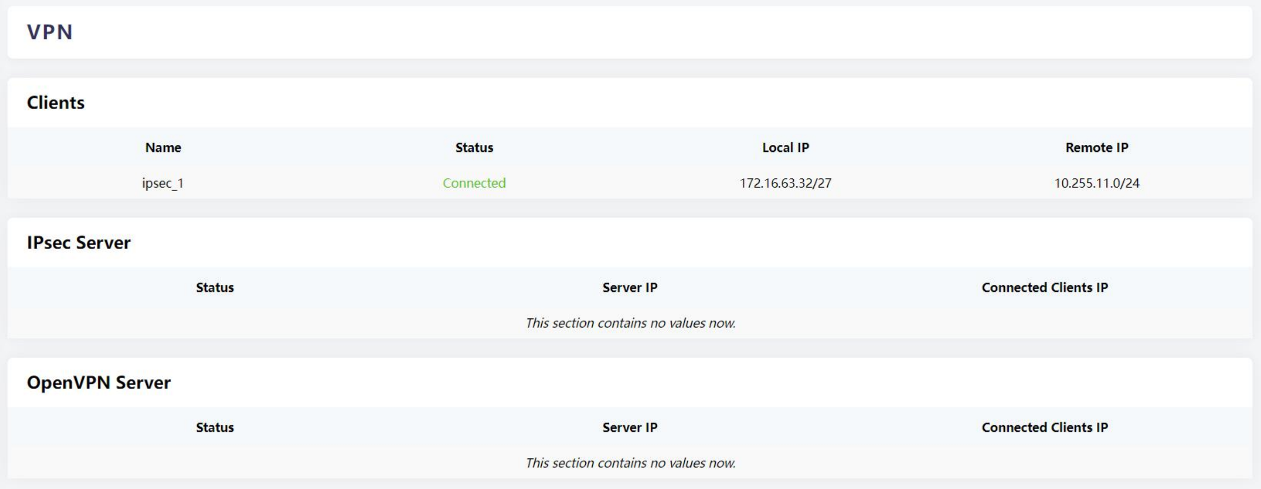
IPv6 Address	MAC Address	Interface

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	
IPv4 Address	The IP address of ARP pool.
MAC Address	The IP address's corresponding MAC address.
Interface	The binding interface of ARP.
IPv6 Neighbor	
IPv6 Address	The IP address of neighbor.
MAC Address	The IP address's corresponding MAC address.
Interface	The binding interface of neighbor.

5.1.6 VPN

You can check VPN status on this page.



VPN

Clients

Name	Status	Local IP	Remote IP
ipsec_1	Connected	172.16.63.32/27	10.255.11.0/24

IPsec Server

Status	Server IP	Connected Clients IP

This section contains no values now.

OpenVPN Server

Status	Server IP	Connected Clients IP

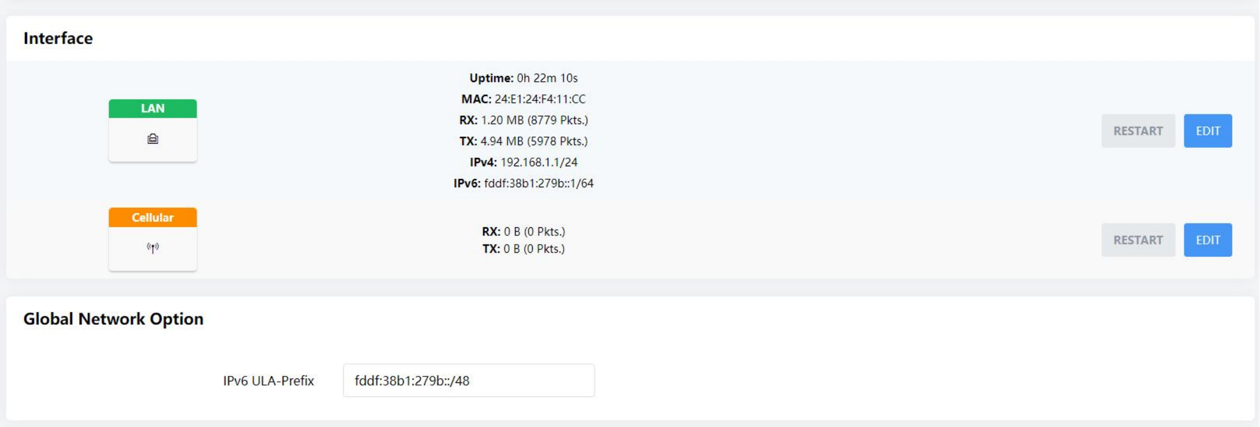
This section contains no values now.

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.

5.2 Network

5.2.1 Interfaces

This menu allows to configure the basic settings of cellular and LAN interface.



Interface

LAN

Uptime: 0h 22m 10s
MAC: 24:E1:24:F4:11:CC
RX: 1.20 MB (8779 Pkts.)
TX: 4.94 MB (5978 Pkts.)
IPv4: 192.168.1.1/24
IPv6: fddf:38b1:279b::1/64

Cellular

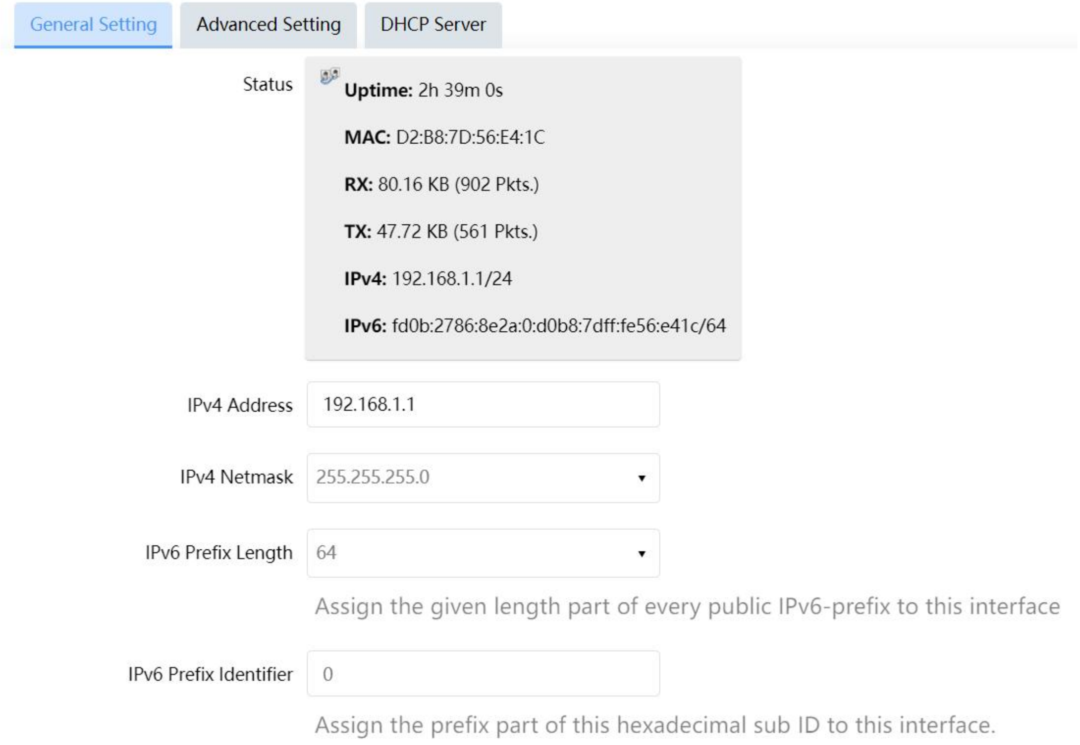
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)

Global Network Option

IPv6 ULA-Prefix: fddf:38b1:279b::/48

Item	Description
Interfaces	
Restart	Click to restart this network interface.
Edit	Click to edit general settings of this network interface.
Global Network Options	
IPv6 ULA-Prefix	The IPv6 unique local address (ULA) prefix of this device.

5.2.1.1 LAN/DHCP Server



Status

Uptime: 2h 39m 0s
MAC: D2:B8:7D:56:E4:1C
RX: 80.16 KB (902 Pkts.)
TX: 47.72 KB (561 Pkts.)
IPv4: 192.168.1.1/24
IPv6: fd0b:2786:8e2a:0:d0b8:7dff:fe56:e41c/64

IPv4 Address: 192.168.1.1

IPv4 Netmask: 255.255.255.0

IPv6 Prefix Length: 64

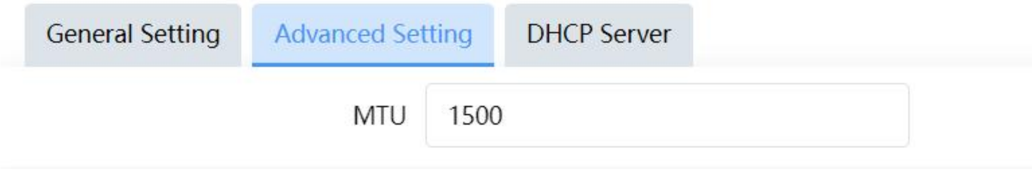
Assign the given length part of every public IPv6-prefix to this interface

IPv6 Prefix Identifier: 0

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

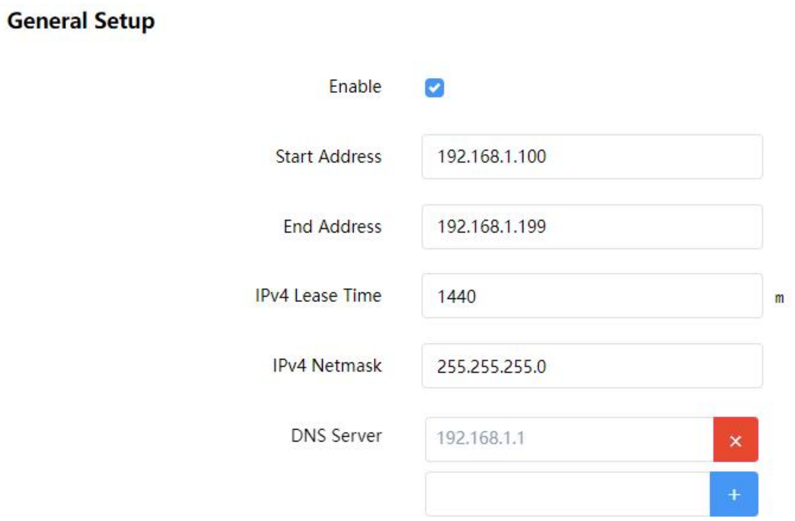
LAN - General Settings	
Item	**Description**
Status	**Uptime:** how long has the device been running.
	MAC: MAC address of LAN interfaces.
	RX: the data volume and packets received in this interface.

	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

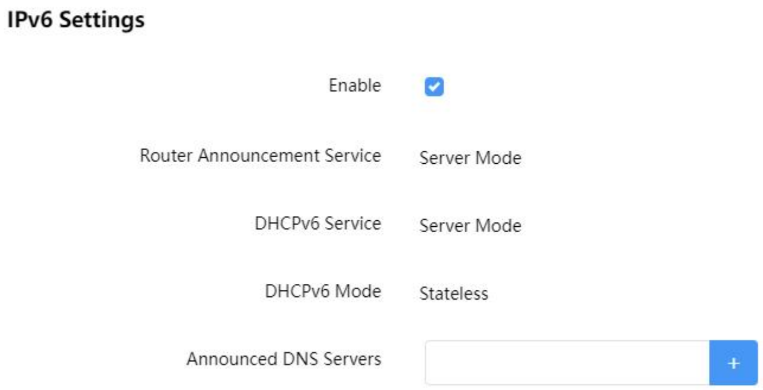
IPv4 Lease Time 1440 m

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

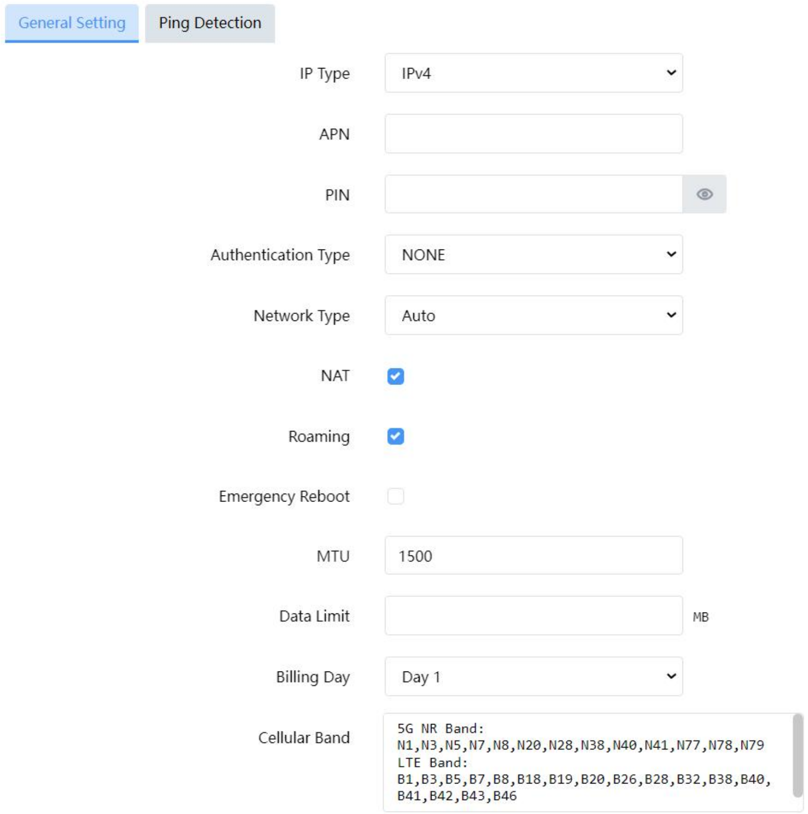
DHCPv6 Service: Server Mode

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.

5.2.1.1 Cellular



General Setting | Ping Detection

IP Type: IPv4

APN:

PIN:

Authentication Type: NONE

Network Type: Auto

NAT ☑

Roaming ☑

Emergency Reboot ☐

MTU: 1500

Data Limit: MB

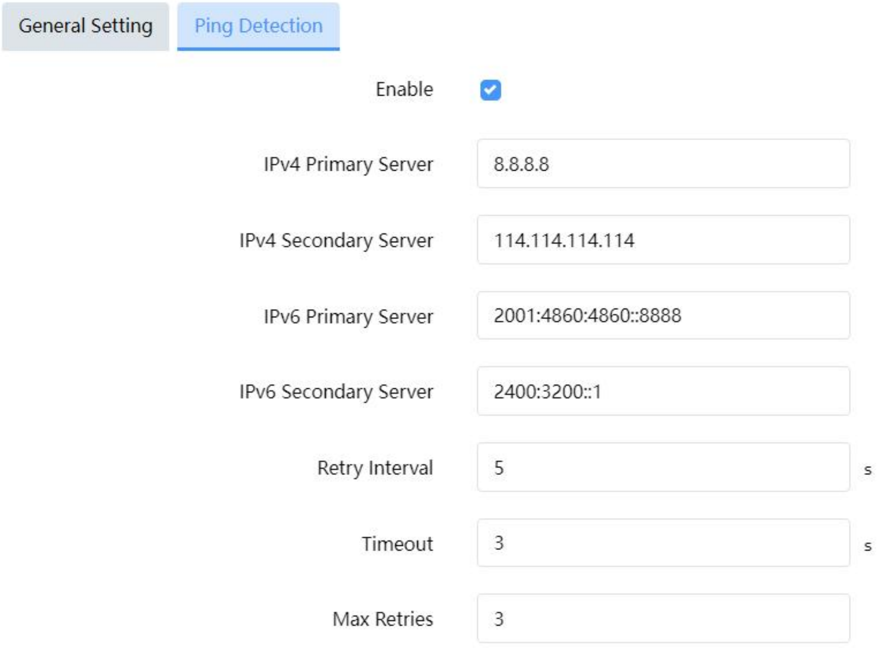
Billing Day: Day 1

Cellular Band:

```
5G NR Band:
N1,N3,N5,N7,N8,N20,N28,N38,N40,N41,N77,N78,N79
LTE Band:
B1,B3,B5,B7,B8,B18,B19,B20,B26,B28,B32,B38,B40,
B41,B42,B43,B46
```

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.
NAT	Enable or disable NAT.
Emergency Reboot	Enable to reboot the device if ping detection fails. This will only reboot 3 times at most.
Roaming	Enable or disable roaming.
MTU	Set the maximum transmission units. IPv4 Range: 68-1500; IPv4/IPv6 or IPv6 Range: 1280-1500.
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.



Enable ☑

IPv4 Primary Server: 8.8.8.8

IPv4 Secondary Server: 114.114.114.114

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

IPv6 Secondary Server: 2400:3200::1

Retry Interval: 5 s

Timeout: 3 s

Max Retries: 3

Ping Detection	
Item	**Description**
Enable	If enabled, the device will periodically detect the connection status of the link.
IPv4 Primary Server	The device will send ICMP packet to the IPv4 address or hostname to determine whether the Internet connection is still available or not.
IPv4 Secondary Server	The device will try to ping the secondary server if primary server is not available.
IPv6 Primary Server	The device will send ICMP packet to the IPv6 address or hostname to determine whether the Internet connection is still

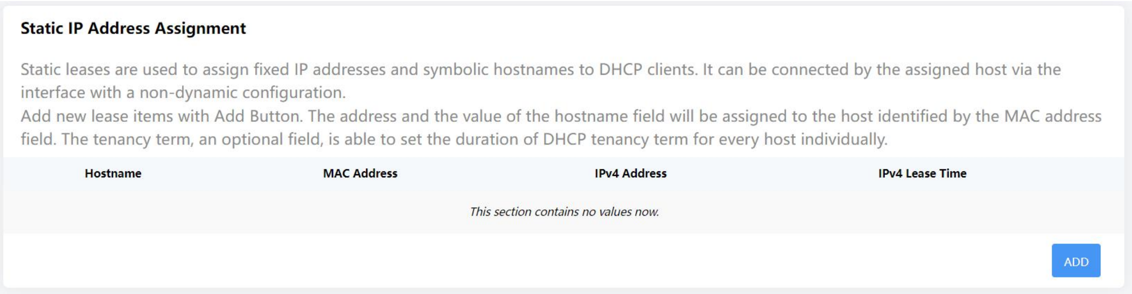
	available or not.
IPv6 Secondary Server	The device will try to ping the secondary server if primary server is not available.
Retry Interval	Set the ping retry interval. When ping failed, the device will ping again in every retry interval.
Timeout	The maximum amount of time the device will wait for a response to a ping request. If it does not receive a response for the amount of time defined in this field, the ping request will be considered to have failed.
Max Retries	The retry times of the device sending ping request until determining that the connection has failed.

Related Application

Cellular Application

5.2.1.3 Static IP Address Assignment

When LAN 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

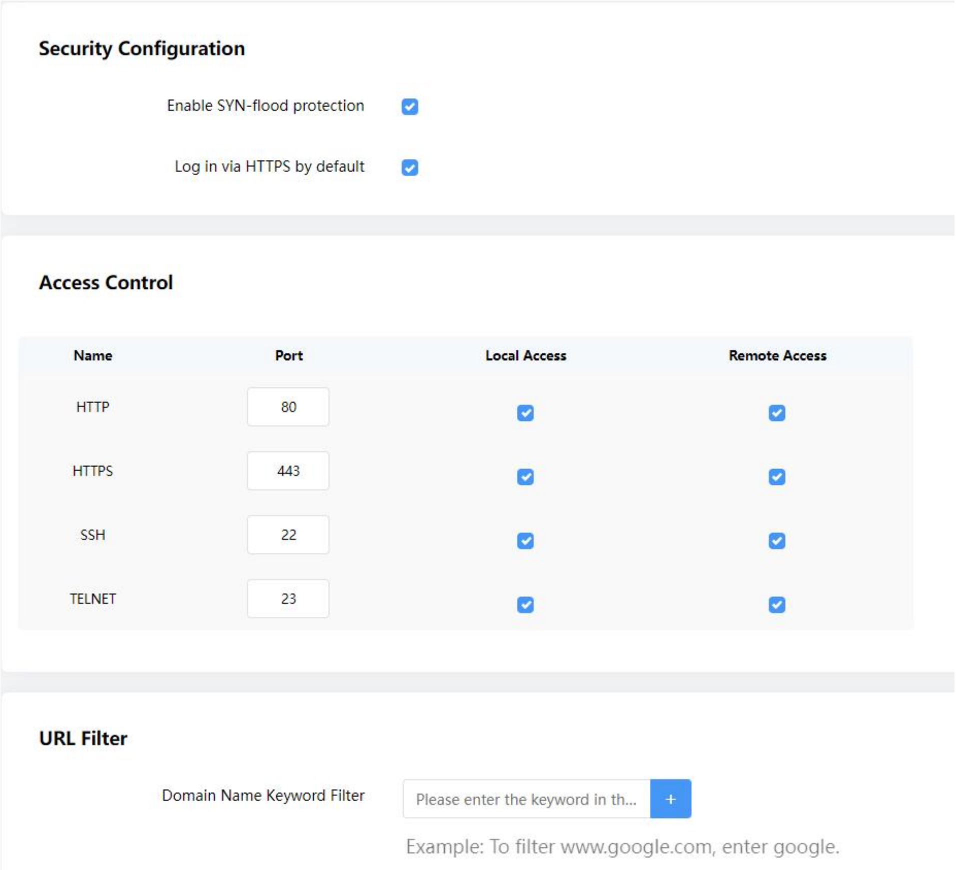
This section contains no values now.

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.

5.2.2 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.

5.2.2.1 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 th... +

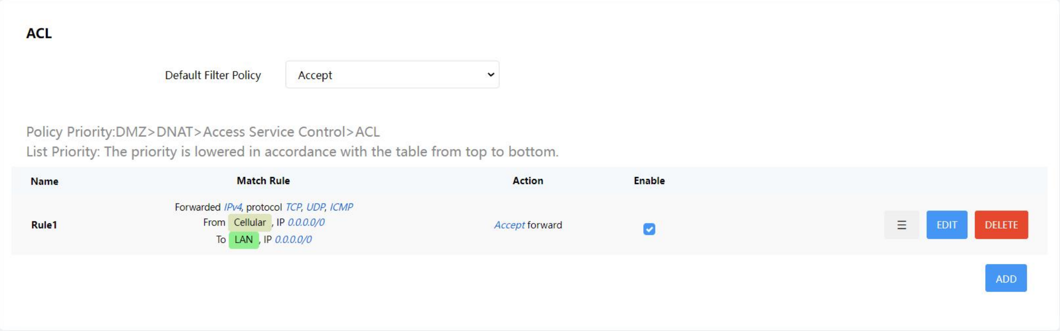
Example: To filter www.google.com, enter google.

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 is checked.	80
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 Filtering	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.

5.2.2.2 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.



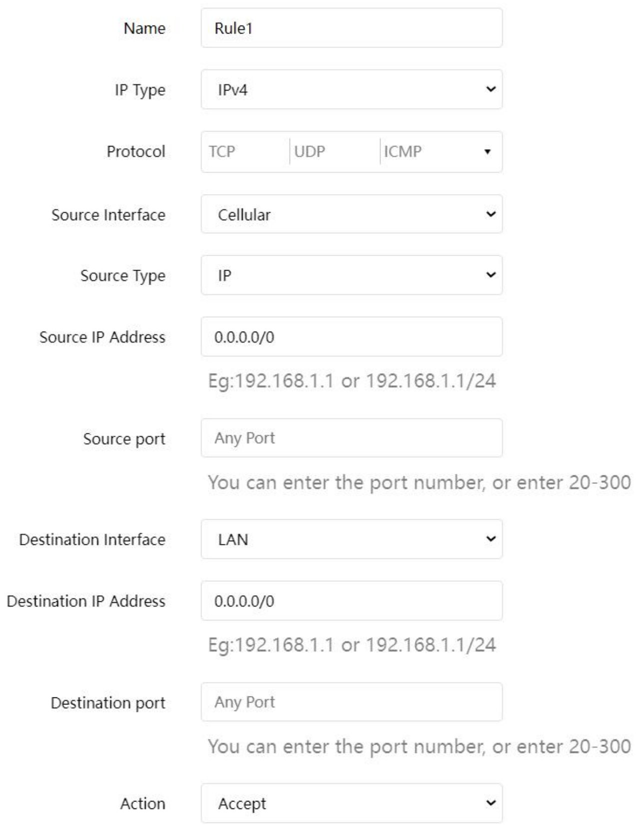
ACL

Default Filter Policy: Accept

Policy Priority:DMZ>DNAT>Access Service Control>ACL
List Priority: The priority is lowered in accordance with the table from top to bottom.

Name	Match Rule	Action	Enable	
Rule1	Forwarded *IPv4*, protocol *TCP, UDP, ICMP* From 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.

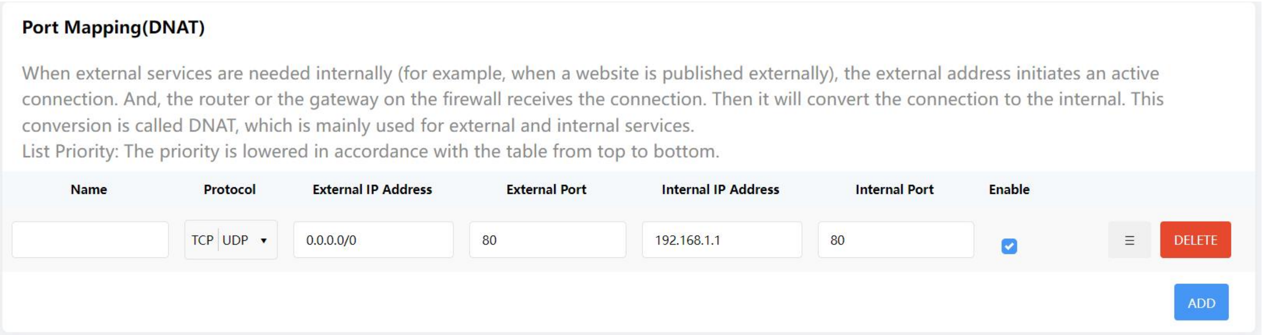


Name	Rule1
IP Type	IPv4
Protocol	TCP UDP ICMP
Source Interface	Cellular
Source Type	IP
Source IP Address	0.0.0.0/0 Eg:192.168.1.1 or 192.168.1.1/24
Source port	Any Port You can enter the port number, or enter 20-300
Destination Interface	LAN
Destination IP Address	0.0.0.0/0 Eg:192.168.1.1 or 192.168.1.1/24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

5.2.2.3 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	80	192.168.1.1	80	☑	☰	DELETE

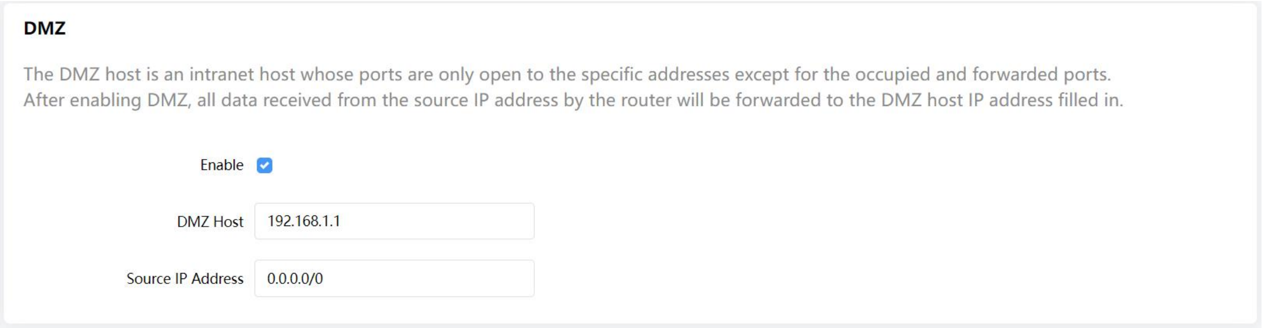
Port Mapping (DNAT)	
Item	**Description**
Name	Define a unique name of the port mapping rule.
Protocol	Select TCP or UDP for your application requirements.
External IP Address	Specify the host or network which can access local IP address. 0.0.0.0/0 means all.
External Port	Set the port or port range 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]

5.2.2.4 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

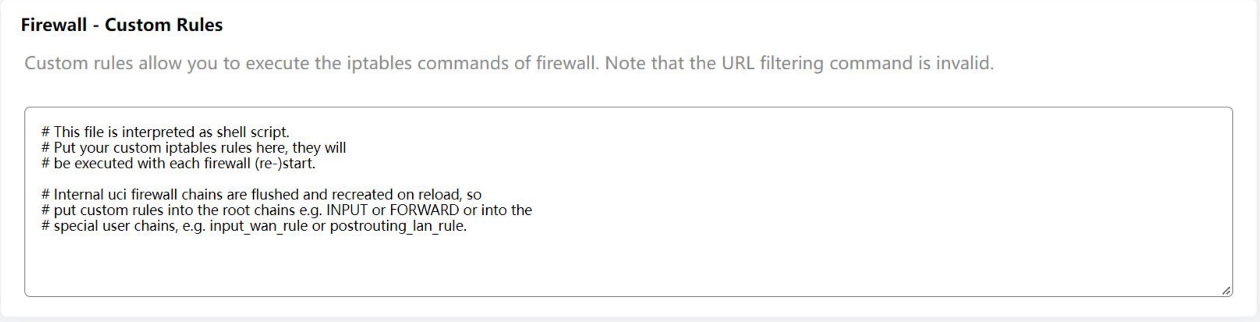
Source IP Address 0.0.0.0/0

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.

5.2.2.5 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

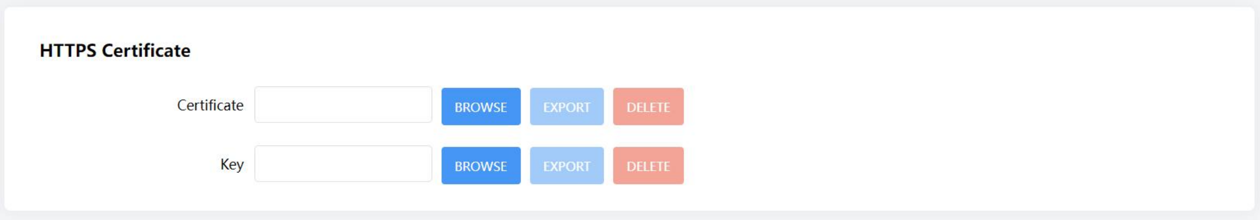
Custom rules allow you to execute the iptables commands of firewall. Note that the URL filtering command is invalid.

```
# 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.
```

5.2.2.6 Certificates

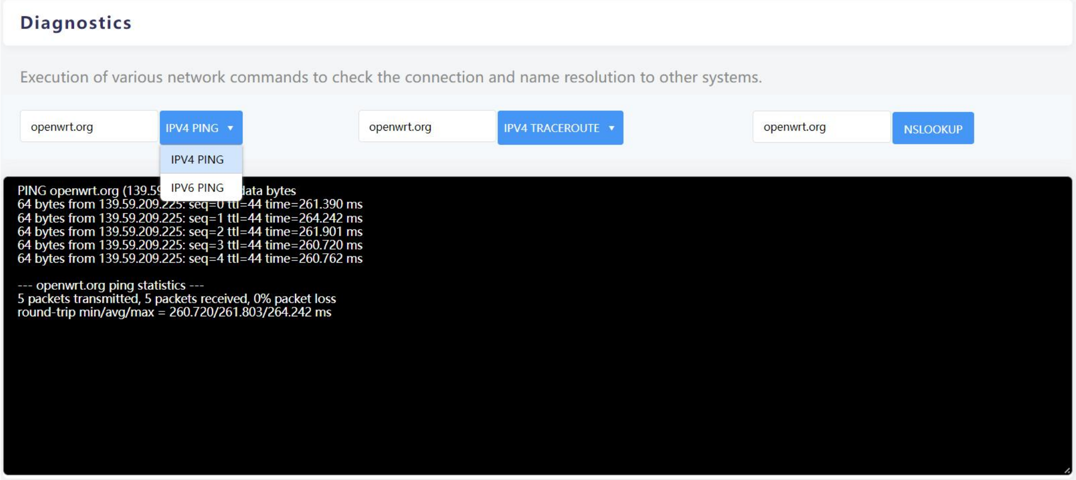
In this page, you can import the HTTPS certificates for device web GUI secure access.



HTTPS Certificate

5.2.3 Diagnostics

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



Diagnostics

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

```
PING openwrt.org (139.59                    data bytes
64 bytes from 139.59.209.225: seq=0 ttl=44 time=261.390 ms
64 bytes from 139.59.209.225: seq=1 ttl=44 time=264.242 ms
64 bytes from 139.59.209.225: seq=2 ttl=44 time=261.901 ms
64 bytes from 139.59.209.225: seq=3 ttl=44 time=260.720 ms
64 bytes from 139.59.209.225: seq=4 ttl=44 time=260.762 ms

--- openwrt.org ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 260.720/261.803/264.242 ms
```

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.

5.3 VPN

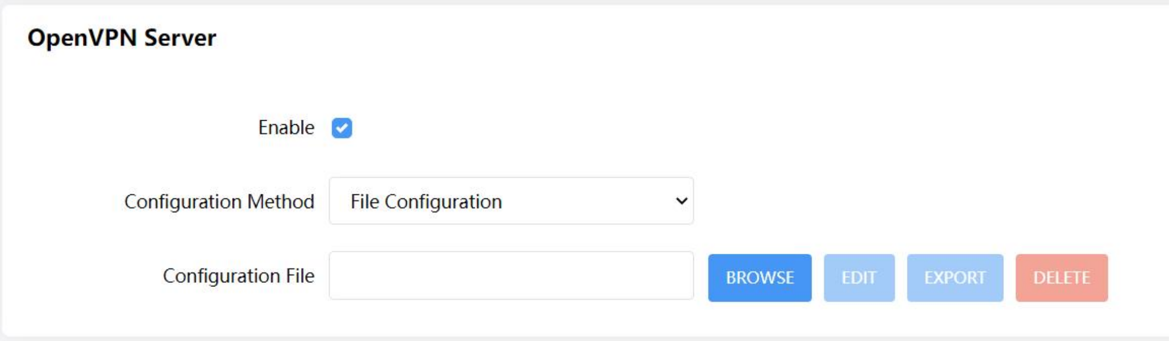
Virtual Private Networks, also called VPNs, are used to securely connect two private networks together so that devices can connect from one network to the other network via secure channels.

5.3.1 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 UF31 is 2.5.3.

5.3.1.1 OpenVPN Server

UF31 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.



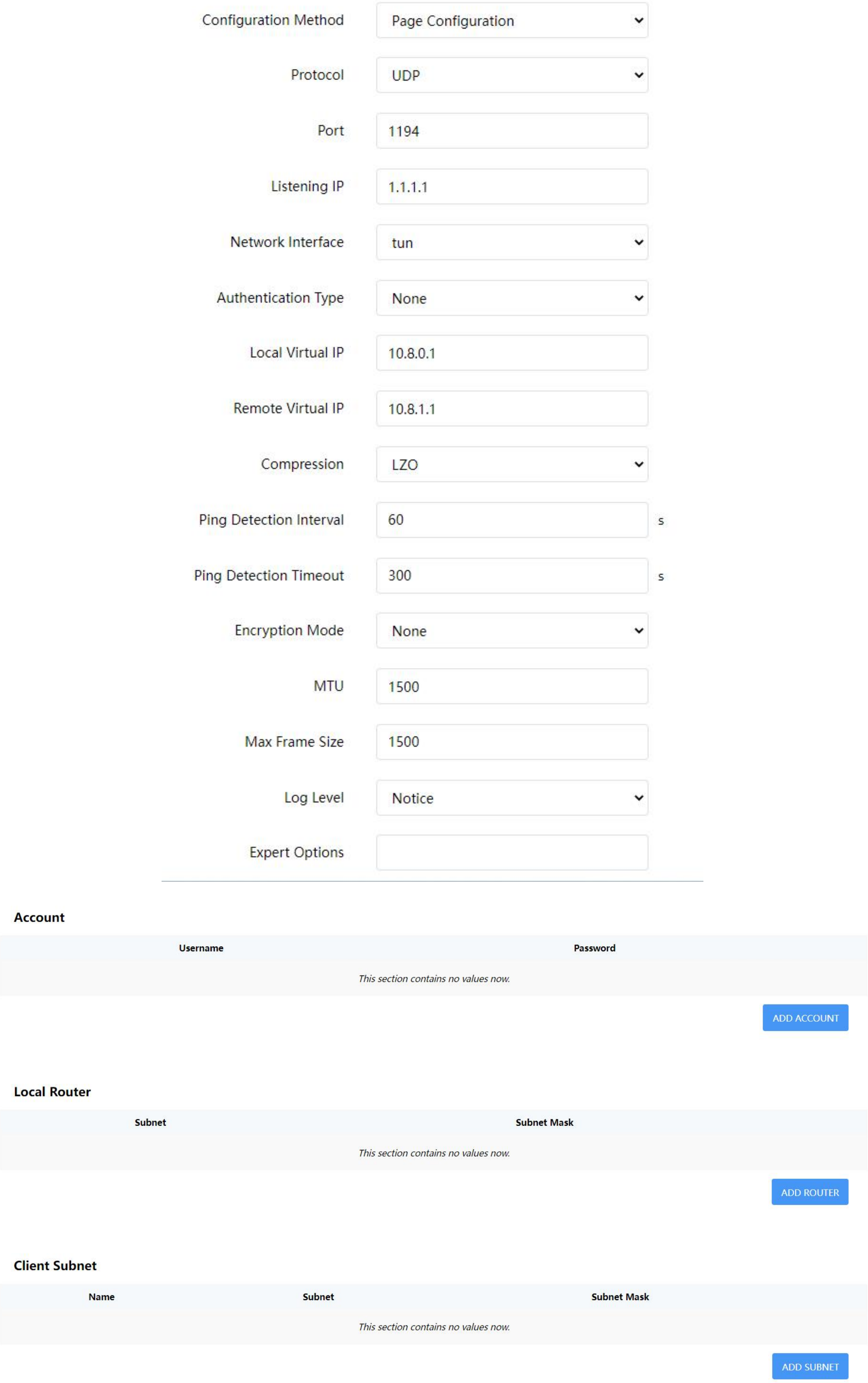
OpenVPN Server

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	1.1.1.1
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

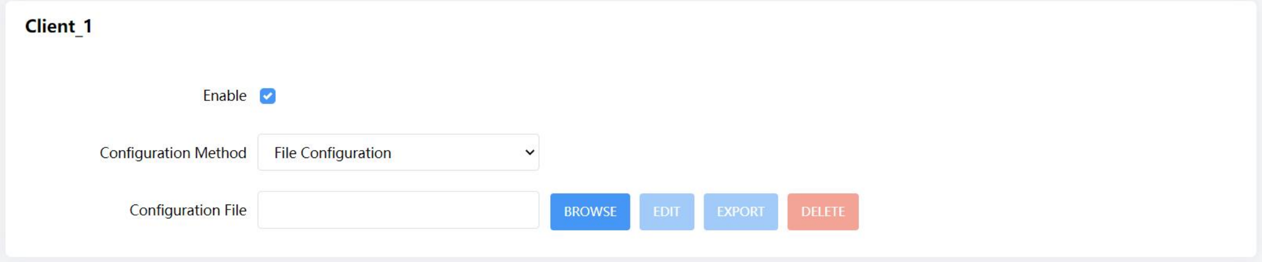
Name	Subnet	Subnet Mask
This section contains no values now.		

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.

5.3.1.2 OpenVPN Client

UF31 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.



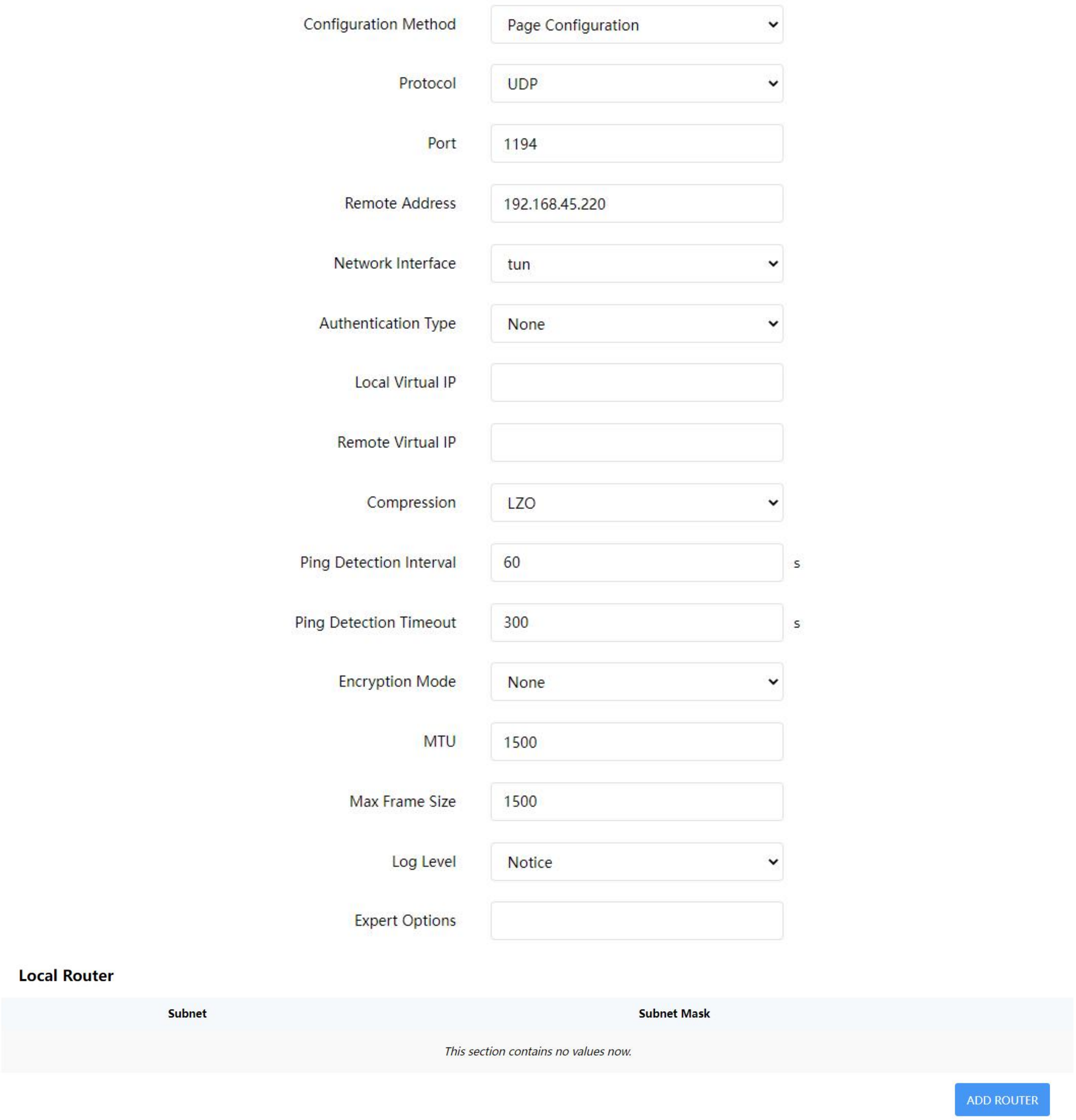
Client_1

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	192.168.45.220
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.

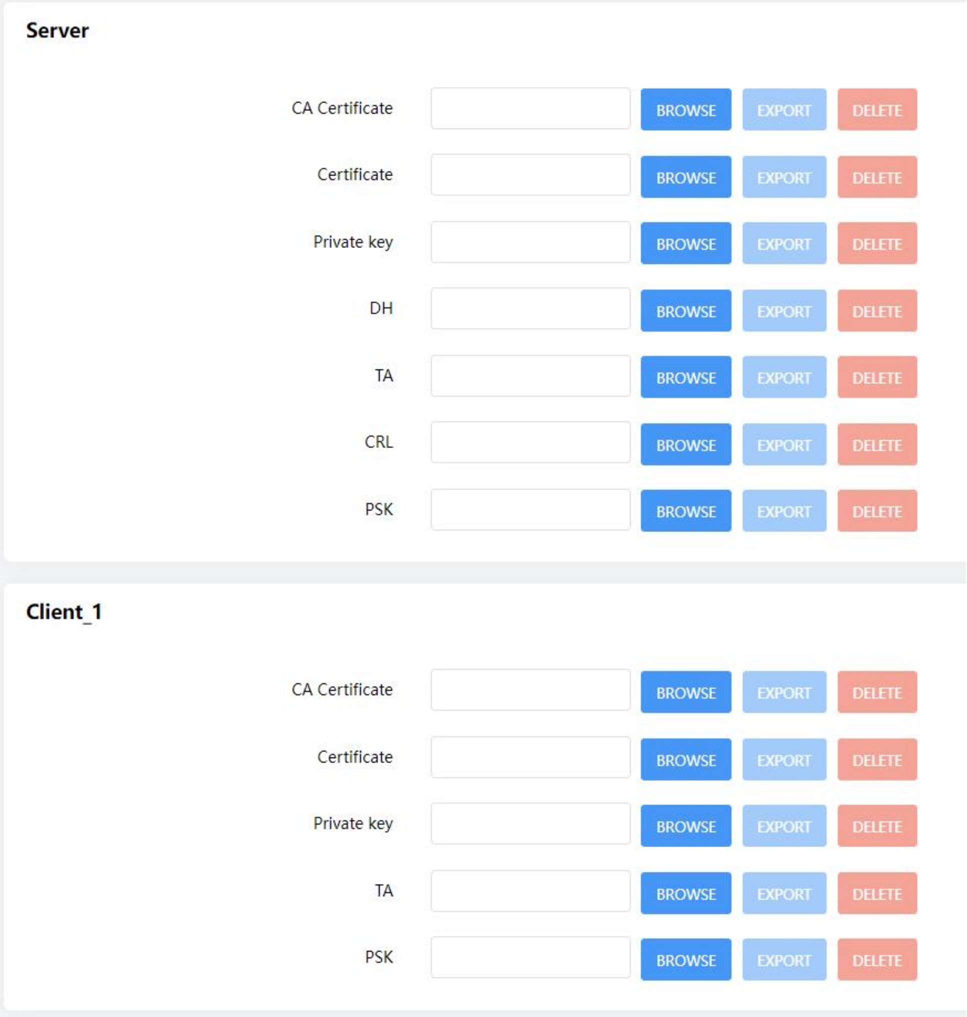
	X.509 cert: use X.509 type certificate to complete the authentication. After selecting, go to **VPN > OpenVPN > Certifications** page to import CA certificate, client certificate and client private key to corresponding fields. **X.509 cert + user:** use both username/password and X.509 cert authentication 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

5.3.1.3 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.

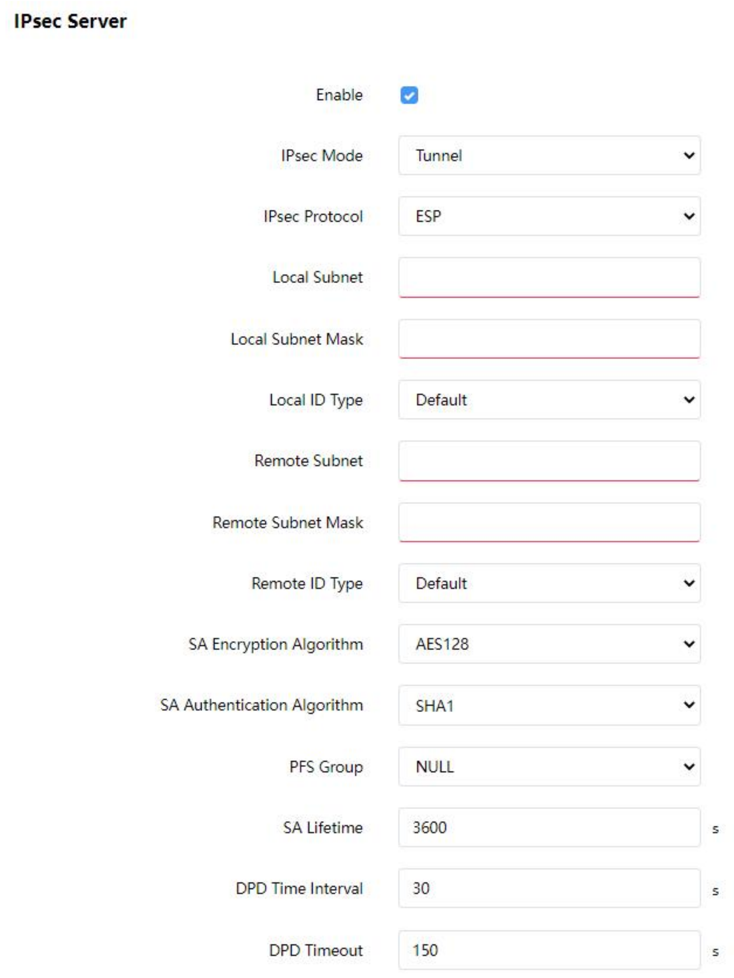


5.3.2 IPsecVPN

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.

5.3.2.1 IPSec Server

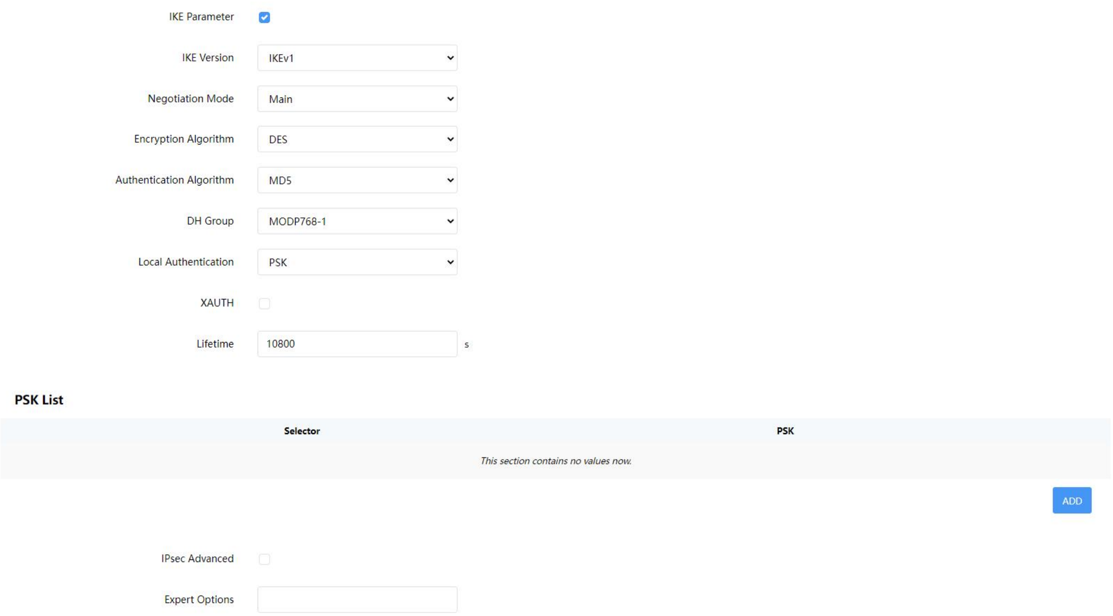


IPsec Server

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 ☐

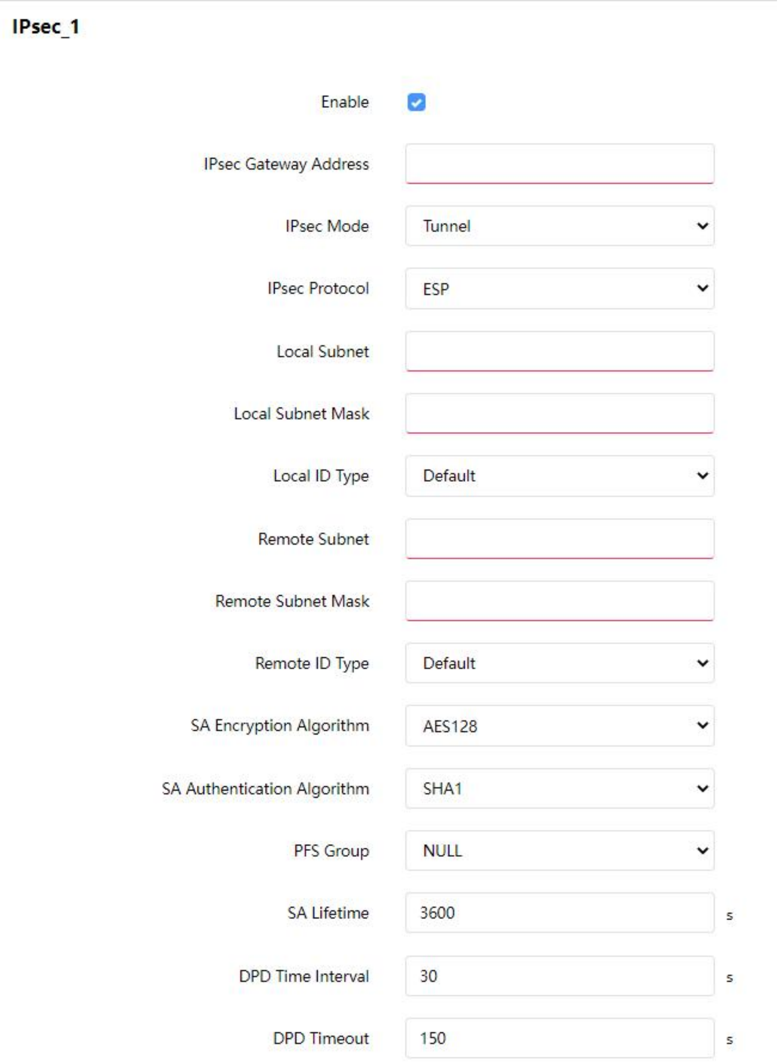
Expert Options:

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.

5.3.2.2 IPSec Client

UF31 supports running at most 3 IPsec clients at the same time.

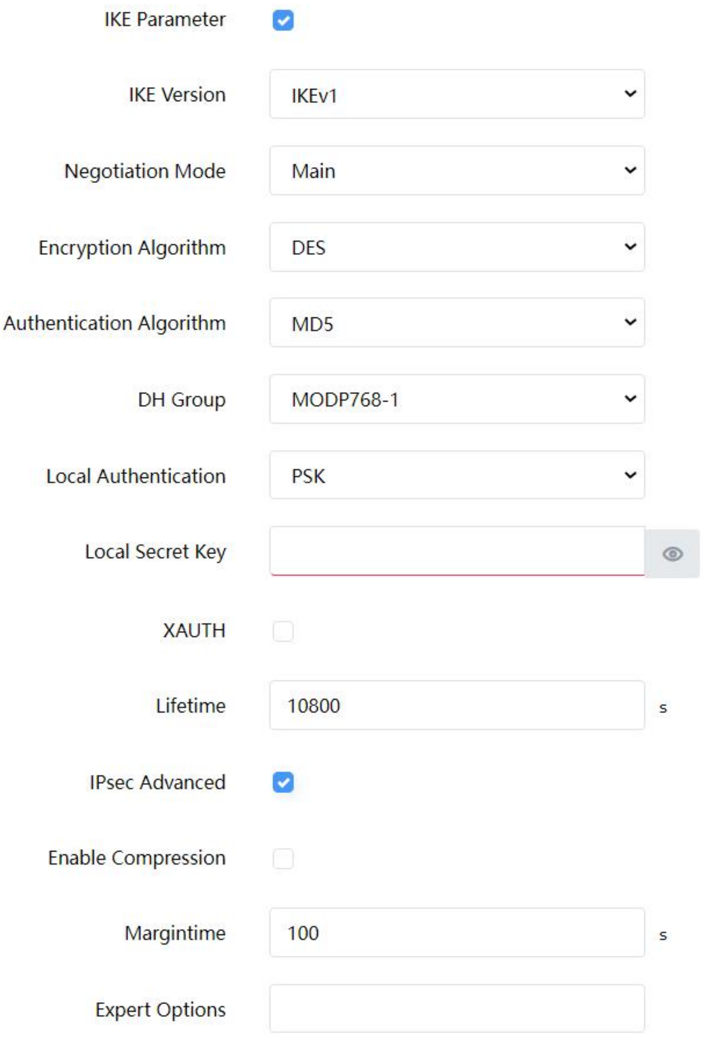


IPsec_1

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



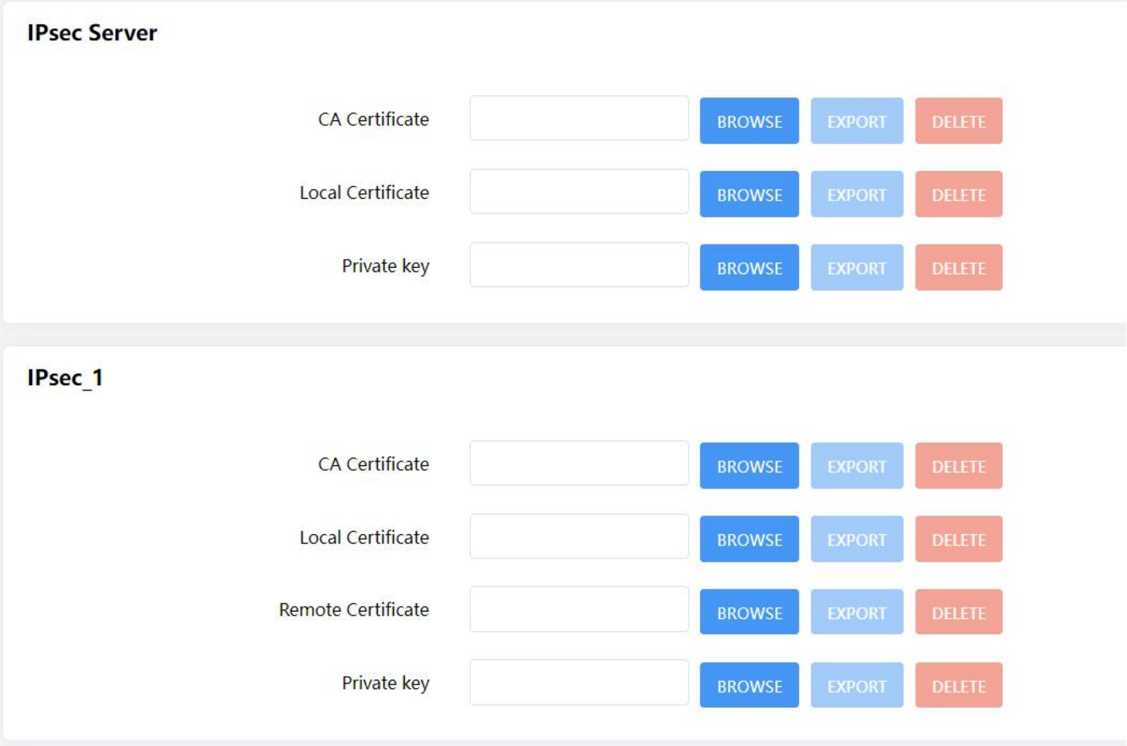
IKE Parameter	☑
IKE Version	IKEv1
Negotiation Mode	Main
Encryption Algorithm	DES
Authentication Algorithm	MD5
DH Group	MODP768-1
Local Authentication	PSK
Local Secret Key	
XAUTH	☐
Lifetime	10800 s
IPsec Advanced	☑
Enable Compression	☐
Margintime	100 s
Expert Options	

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.

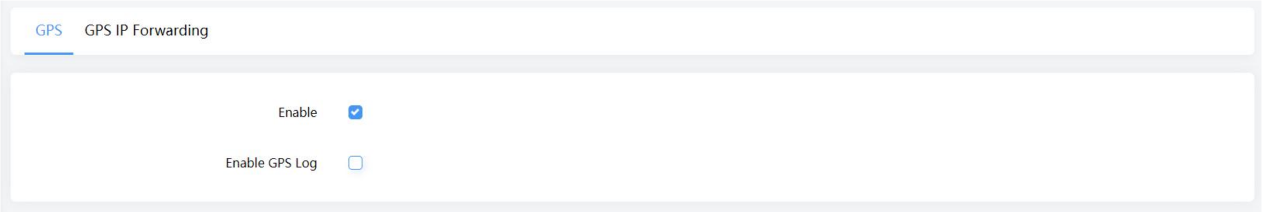
5.3.2.3 Certificate

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



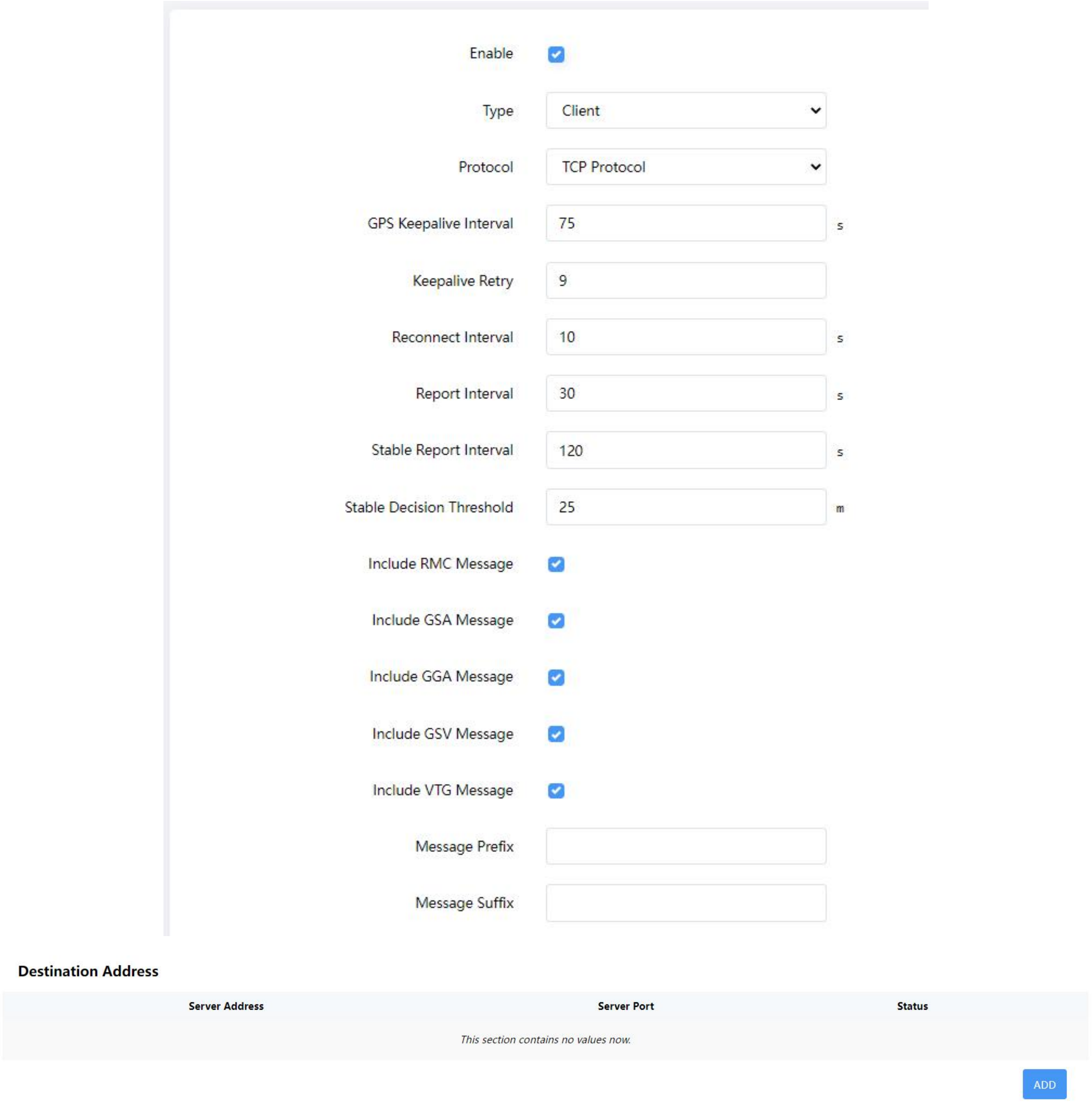
5.4 GPS

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



Enable ☑

Enable GPS Log □



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 m

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
This section contains no values now.		

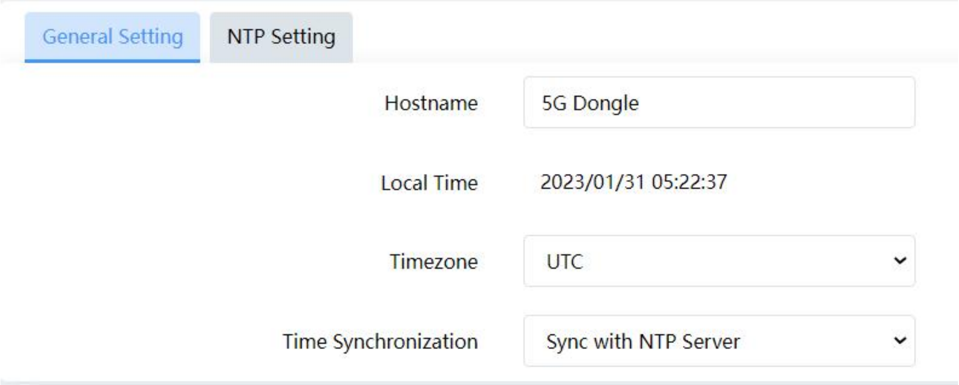
GPS IP Forwarding		
Item	**Description**	**Default**
Enable	Forward the GPS data to the client or server.	Disable
Type	Select connection type as Client or Server.	Client
Protocol	Select protocol of data transmission as TCP or UDP.	TCP

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 Retry	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
Local Port	Set the listening port when using as a Server. Range: 1-65535.	
Reconnect Interval	When the connection failes, 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.	--

5.5 System

This section describes how to configure general settings, such as administration account, system time, system maintenance tools and management.

5.5.1 System



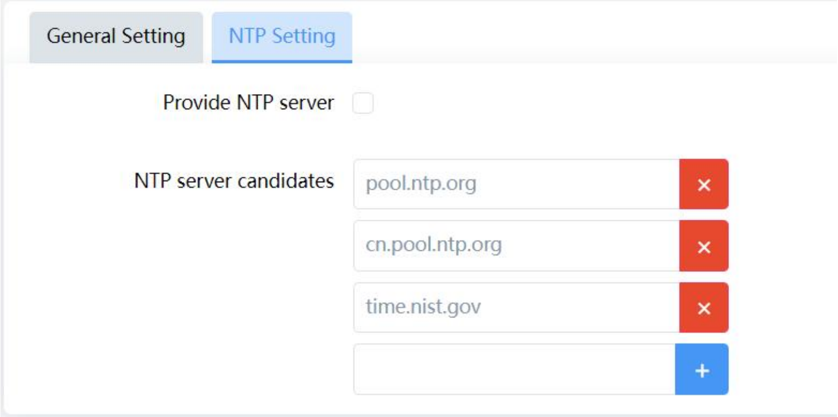
Hostname: 5G Dongle

Local Time: 2023/01/31 05:22:37

Timezone: UTC

Time Synchronization: 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 **Industrial > GPS >GPS**. **Manual:** configure the time manually.



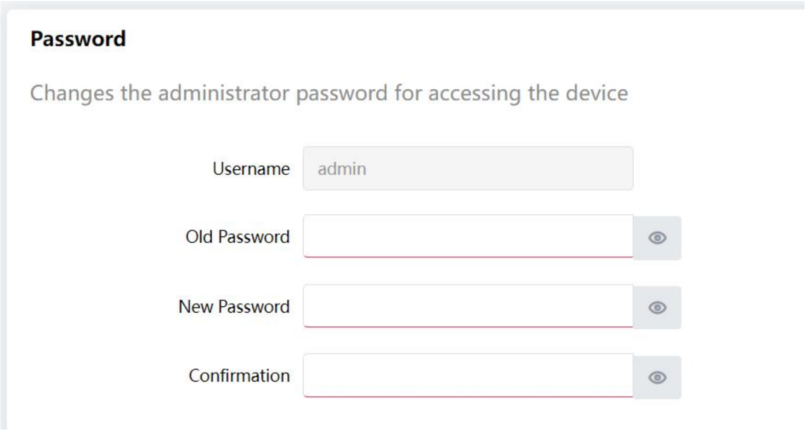
Provide NTP server □

NTP server candidates: pool.ntp.org, cn.pool.ntp.org, time.nist.gov

System - NTP Setting	
Item	**Description**
Provide 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.

5.5.2 Password

You can change the administrator password for accessing the device.



Password

Changes the administrator password for accessing the device

Username: admin

Old Password:

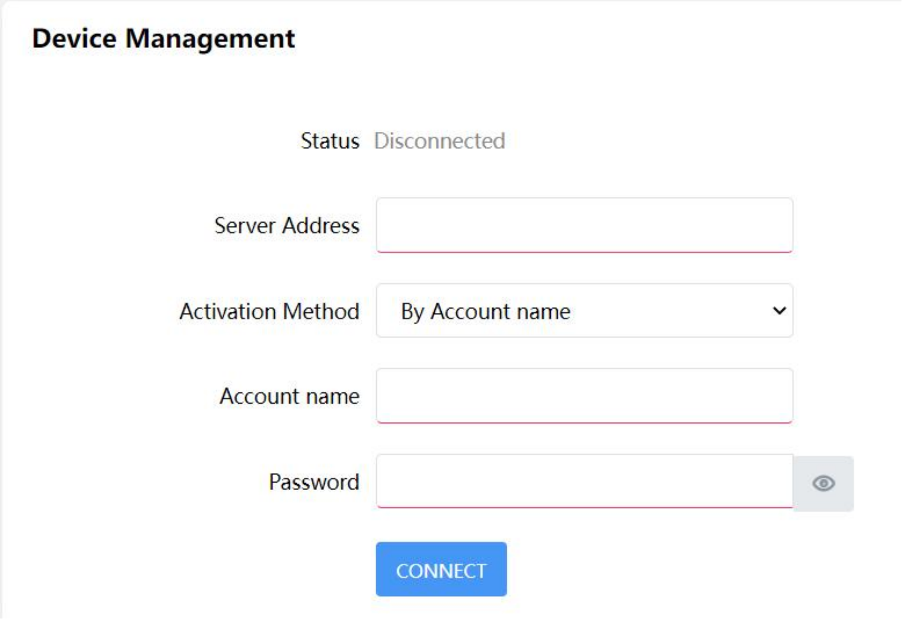
New Password:

Confirmation:

Password	
Item	**Description**
Username	It's fixed as admin.
Old Password	Enter the old password to verify the authority.
New Password	Enter a new password.
Confirmation	Enter the new password again.

5.5.3 Device Management

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



Device Management

Status: Disconnected

Server Address:

Activation Method: By Account name

Account name:

Password:

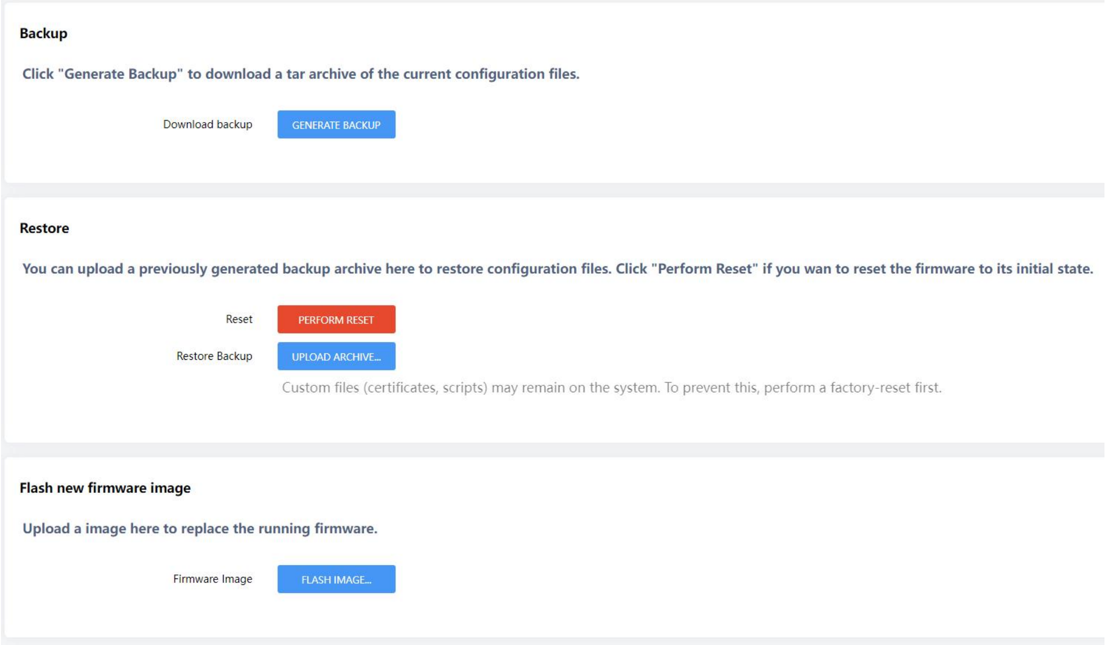
Device Management	
Item	**Description**
Status	Show the connection status between the device and the DeviceHub.
Server Address	IP address or domain of the DeviceHub management server.
Activation Method	Select activation method to connect the device to the DeviceHub server, options are "**By Authentication 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.

5.5.4 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 web. Generally, you don't need to do the firmware upgrade.

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



Backup

Click "Generate Backup" to download a tar archive of the current configuration files.

Download backup GENERATE BACKUP

Restore

You can upload a previously generated backup archive here to restore configuration files. Click "Perform Reset" if you wan to reset the firmware to its initial state.

Reset PERFORM RESET

Restore Backup UPLOAD ARCHIVE...

Custom files (certificates, scripts) may remain on the system. To prevent this, perform a factory-reset first.

Flash new firmware image

Upload a image here to replace the running firmware.

Firmware Image FLASH IMAGE...

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.
Upload Archive...	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.
Flash Image...	Upload an image here to replace the running firmware.

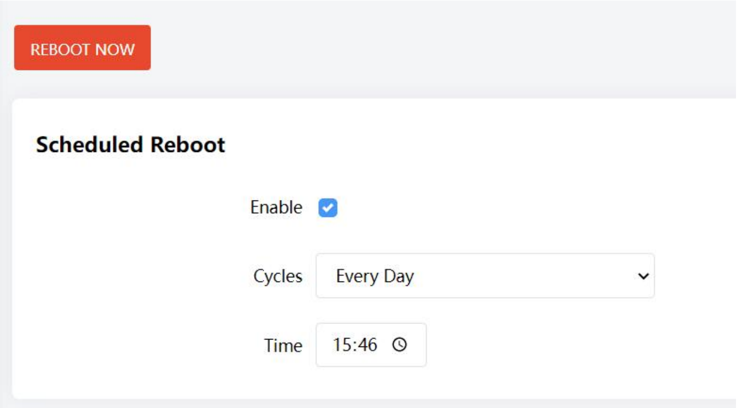
Related Configuration Example

Firmware Upgrade

Restore Factory Defaults

5.5.5 Reboot

This page allows to reboot the device immediately or regularly.



REBOOT NOW

Scheduled Reboot

Enable ☑

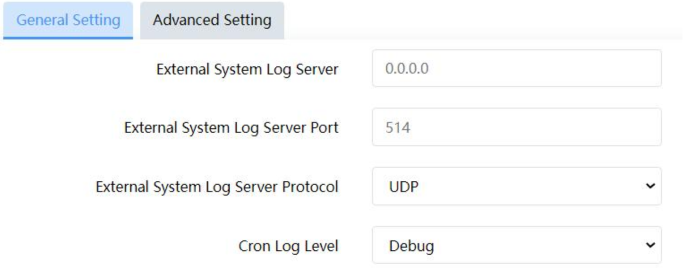
Cycles Every Day

Time 15:46

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.

5.5.6 Log

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



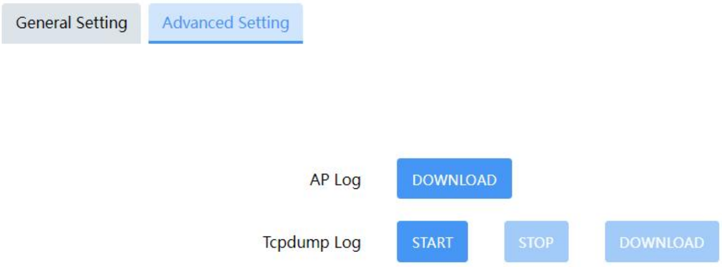
External System Log Server 0.0.0.0

External System Log Server Port 514

External System Log Server Protocol UDP

Cron Log Level Debug

Log Control - 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.

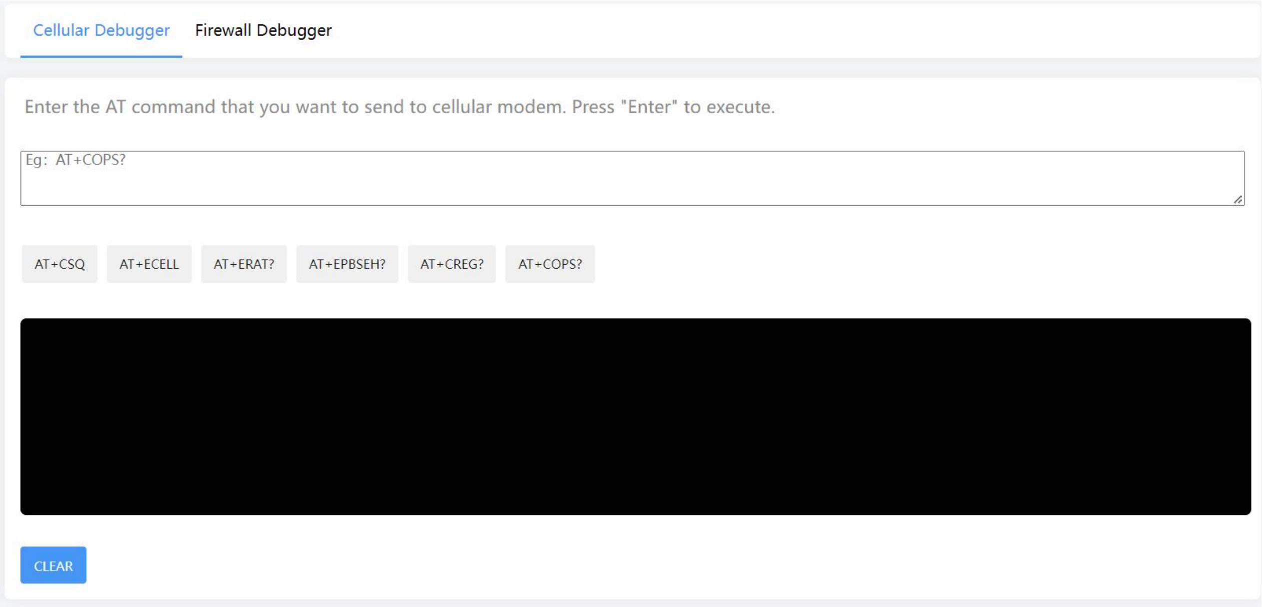


Log Control - Advanced Settings	
Item	**Description**
AP log	
Download	Click to download the last AP log recorded.
Tcpdump log	
Start	Click to start recording tcpdump log.
Stop	Click to stop recording tcpdump log.
Download	Click to download the last tcpdump log recorded.

5.5.7 Debugger

5.5.7.1 Cellular Debugger

This tool allows to use AT commands to check cellular debug information. You can press the buttons on the top of black frame directly to execute common commands directly or enter the AT command that you want to send to cellular modem and press **Enter** to execute.



Enter the AT command that you want to send to cellular modem. Press "Enter" to execute.

Common command description:

AT+CSQ?----Get cellular network signal

AT+ECELL?----Get current cell information

AT+ERAT?----Get RAT status and network type

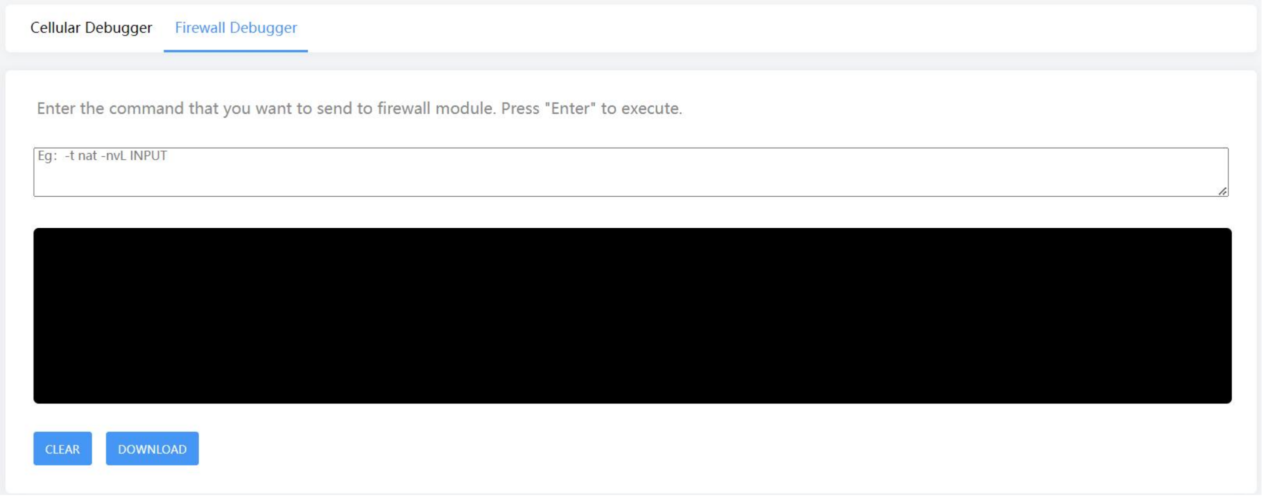
AT+EPBSEH? ----Get using bands

AT+CREG?----Get network registration status

AT+COPS?----Get operator and access technology info

5.5.7.2 Firewall Debugger

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



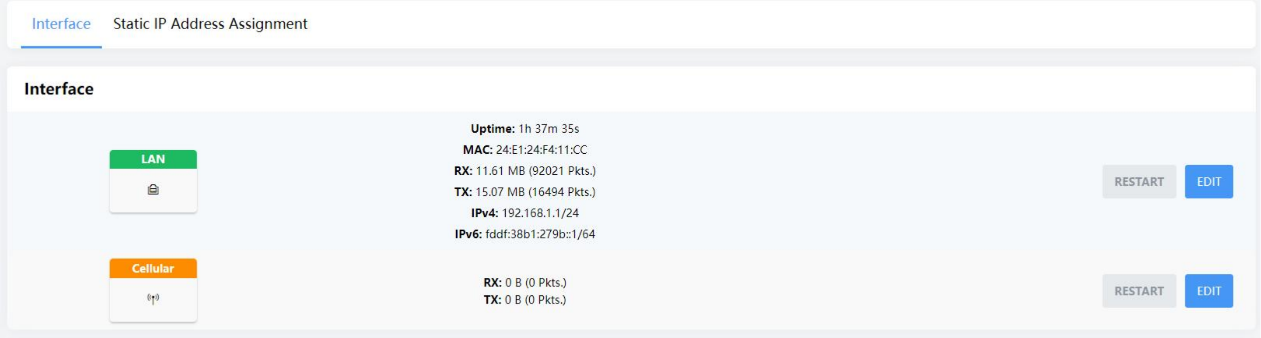
Enter the command that you want to send to firewall module. Press "Enter" to execute.

Eg： -t nat -nvL INPUT

Application Examples

6.1 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.



Interface | Static IP Address Assignment

Interface

LAN

Uptime: 1h 37m 35s
MAC: 24:E1:24:F4:11:CC
RX: 11.61 MB (92021 Pkts.)
TX: 15.07 MB (16494 Pkts.)
IPv4: 192.168.1.1/24
IPv6: fddf:38b1:279b::1/64

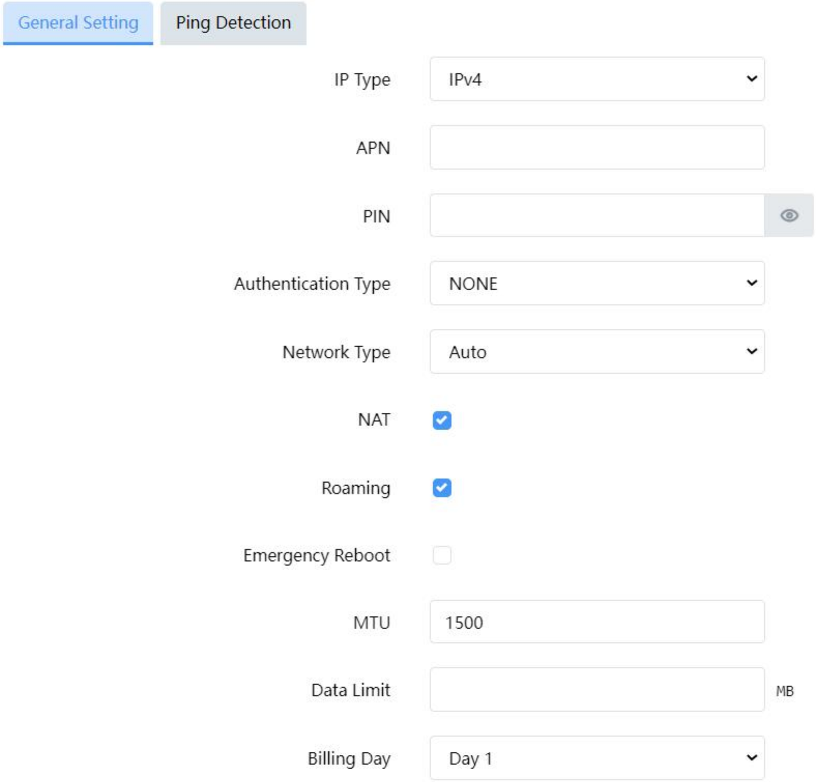
RESTART EDIT

Cellular

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

RESTART EDIT

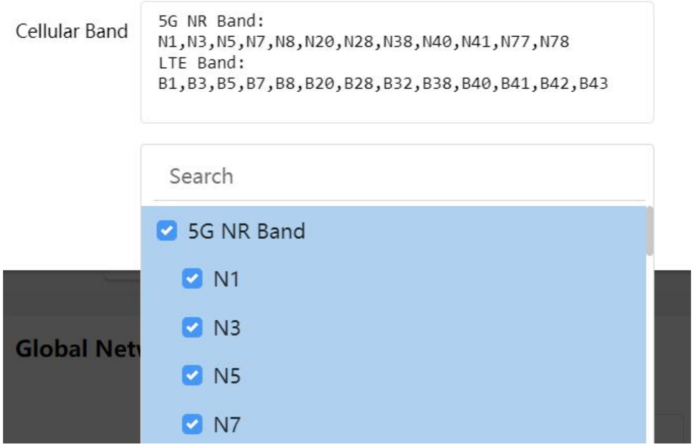
3. Select the SIM card you need to configure and fill in the necessary info of SIM card, then save all settings.



General Setting | Ping Detection

IP Type	IPv4
APN	
PIN	
Authentication Type	NONE
Network Type	Auto
NAT	☑
Roaming	☑
Emergency Reboot	□
MTU	1500
Data Limit	MB
Billing Day	Day 1

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
```

Search

☑ 5G NR Band

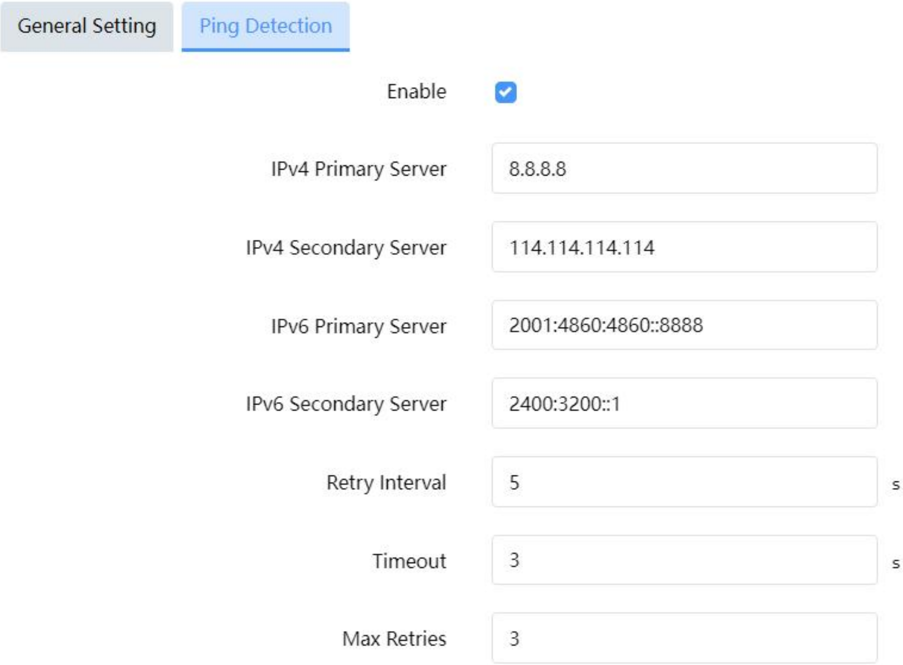
☑ N1

☑ N3

☑ N5

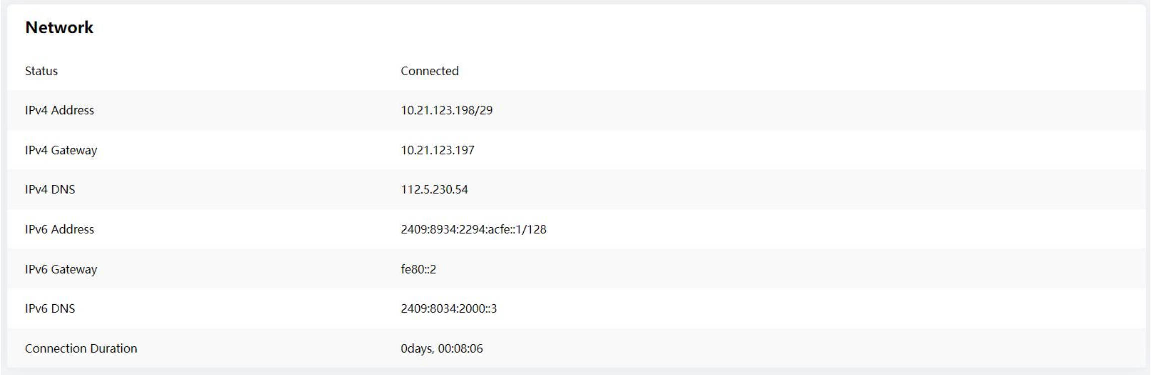
☑ N7

4. Click **Ping Detection** to configure ICMP ping detection information. UF31 will send ICMP packages to check network connection regularly.



Enable	☑
IPv4 Primary Server	8.8.8.8
IPv4 Secondary Server	114.114.114.114
IPv6 Primary Server	2001:4860:4860::8888
IPv6 Secondary Server	2400:3200::1
Retry Interval	5 s
Timeout	3 s
Max Retries	3

5. 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.

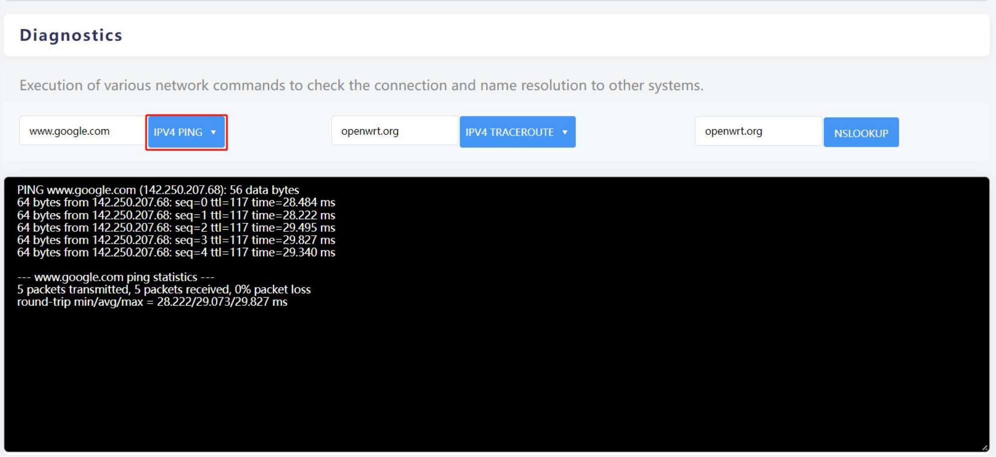


Network

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

6. Go to **Network > Diagnostics** to ping a valid address or domain to check network connection. You

can also open a browser on PC, type any available web address into address bar and see if it is able to visit Internet via the UF31 device.



Diagnostics

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

```
PING www.google.com (142.250.207.68): 56 data bytes
64 bytes from 142.250.207.68: seq=0 ttl=117 time=28.484 ms
64 bytes from 142.250.207.68: seq=1 ttl=117 time=28.222 ms
64 bytes from 142.250.207.68: seq=2 ttl=117 time=29.495 ms
64 bytes from 142.250.207.68: seq=3 ttl=117 time=29.827 ms
64 bytes from 142.250.207.68: seq=4 ttl=117 time=29.340 ms

--- www.google.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 28.222/29.073/29.827 ms
```

Related Topic

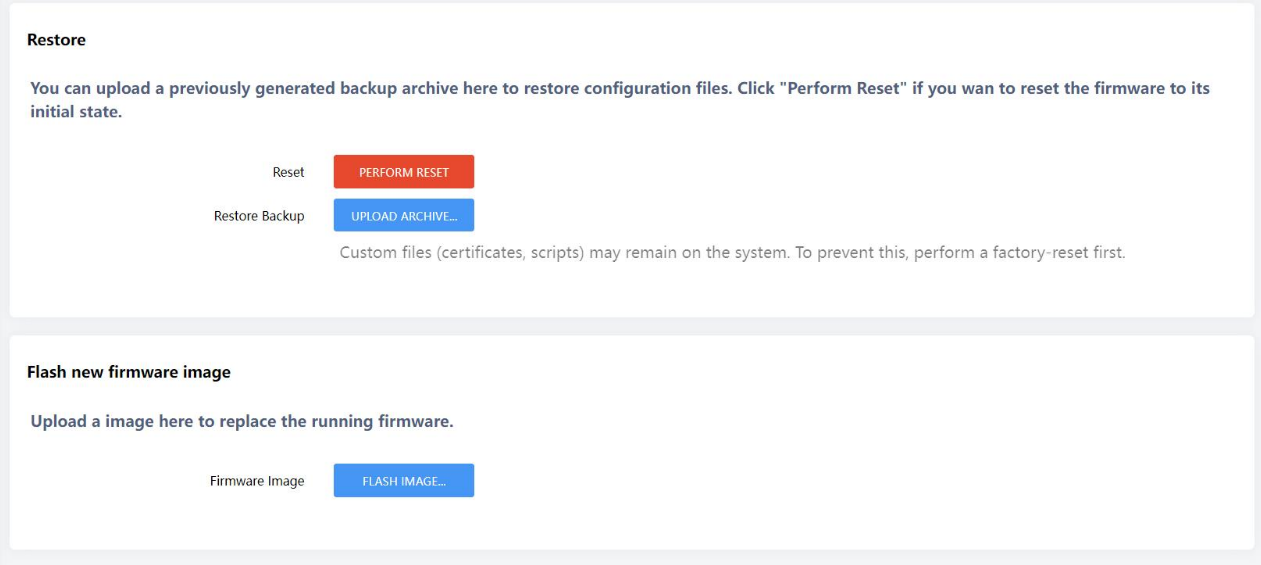
Cellular Settings

Cellular Status

6.2 Firmware Upgrade

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

1. Go to **System > Backup/Upgrade** page, and click **Flash image….**



Restore

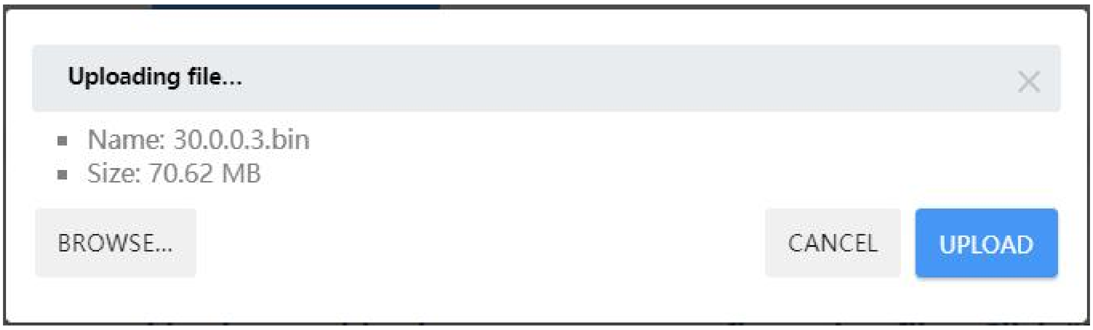
You can upload a previously generated backup archive here to restore configuration files. Click "Perform Reset" if you wan to reset the firmware to its initial state.

Custom files (certificates, scripts) may remain on the system. To prevent this, perform a factory-reset first.

Flash new firmware image

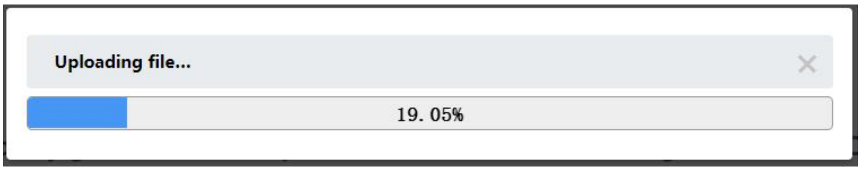
Upload a image here to replace the running firmware.

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.



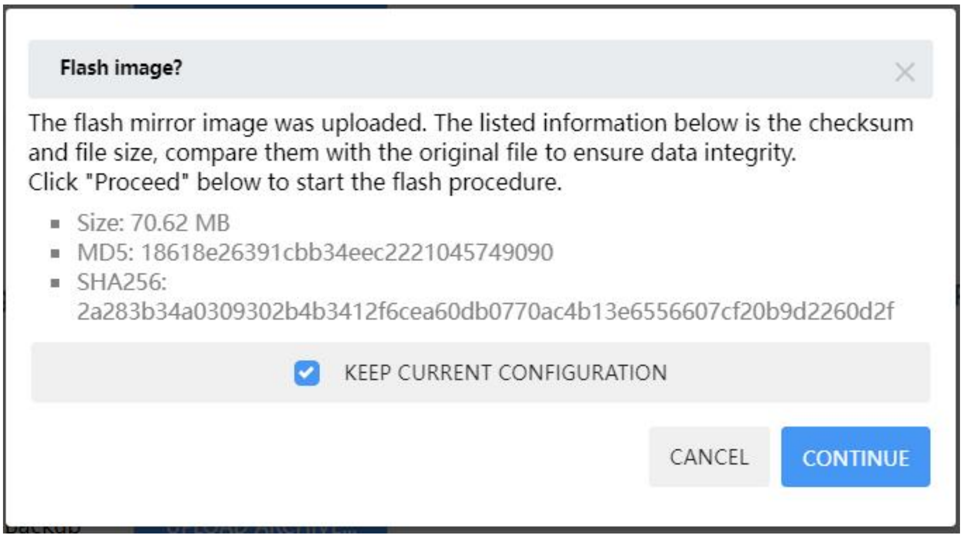
Uploading file...

- Name: 30.0.0.3.bin
- Size: 70.62 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.

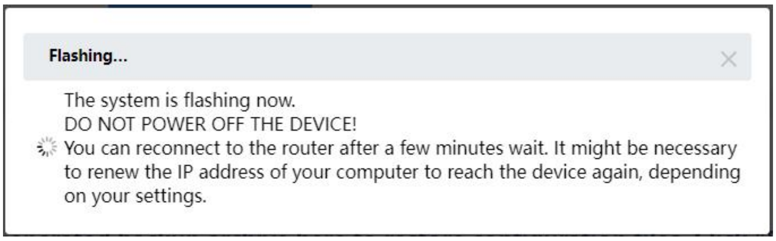


Flash image?

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: 70.62 MB
- MD5: 18618e26391cbb34eec2221045749090
- SHA256: 2a283b34a0309302b4b3412f6cea60db0770ac4b13e6556607cf20b9d2260d2f

☑ KEEP CURRENT CONFIGURATION



Flashing...

The system is flashing now.
DO NOT POWER OFF THE DEVICE!
You can reconnect to the router after a few minutes wait. It might be necessary to renew the IP address of your computer to reach the device again, depending on your settings.

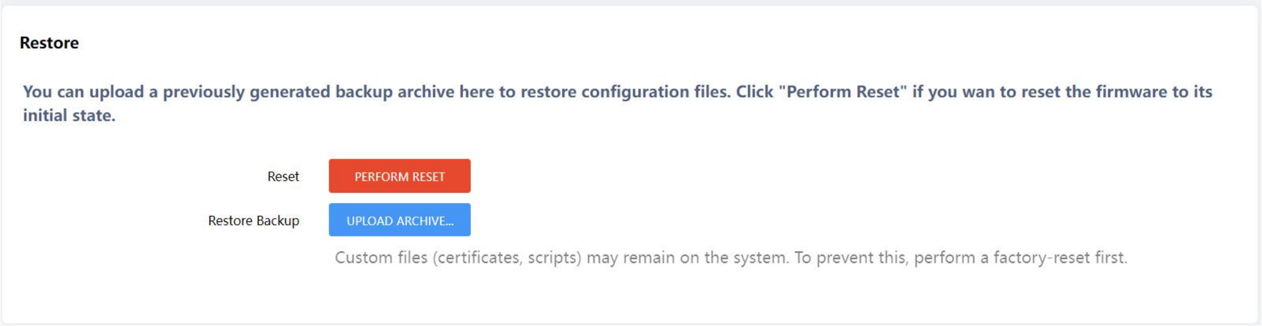
Related Topic

Backup / Upgrade

6.3 Restore Factory Defaults

Method 1:

Go to **System > 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

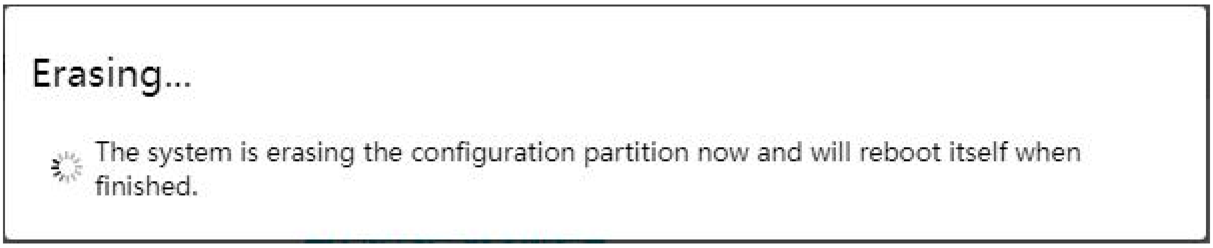
You can upload a previously generated backup archive here to restore configuration files. Click "Perform Reset" if you wan to reset the firmware to its initial state.

Reset PERFORM RESET

Restore Backup UPLOAD ARCHIVE...

Custom files (certificates, scripts) may remain on the system. To prevent this, perform a factory-reset first.

Then UF31 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 STATUS LED shines in green, which means the device has already been reset to factory defaults successfully.

Related Topic

Backup / Upgrade

Method 2:

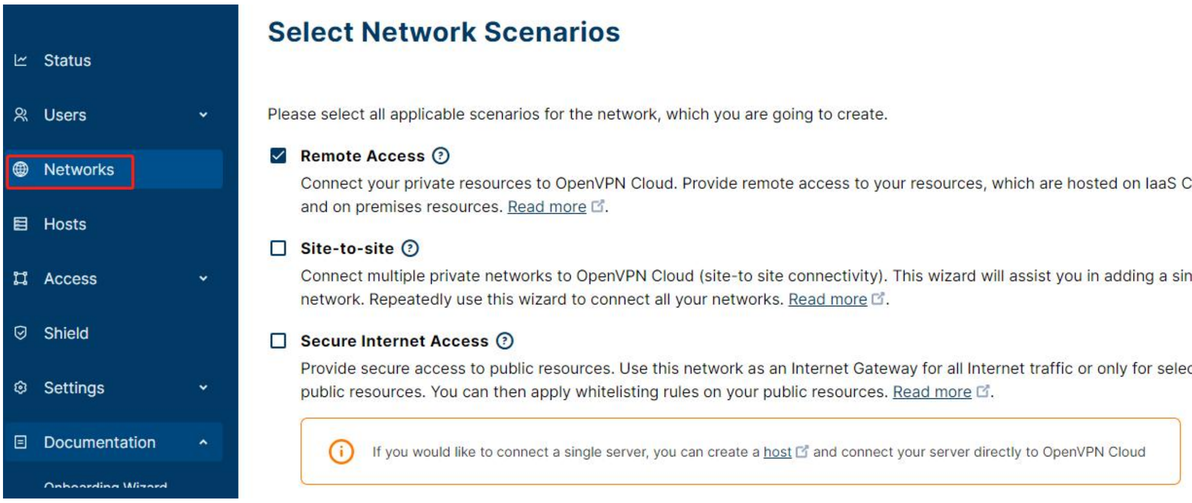
Release the metal case and find the reset button on the mainboard, press and hold the reset button for more than 5 seconds until LED blinks.

6.4 Configure OpenVPN Client

UF31 can work as OpenVPN clients or OpenVPN servers. We are about to take an example of configuring OpenVPN client to connect to OpenVPN cloud.

Configuration Steps

1. Ensure the device has gotten access to the Internet.
2. Log in the openVPN cloud 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, which you are going to create.

☑ Remote Access

Connect your private resources to OpenVPN Cloud. Provide remote access to your resources, which are hosted on IaaS Cloud, and on premises resources. Read more.

□ Site-to-site

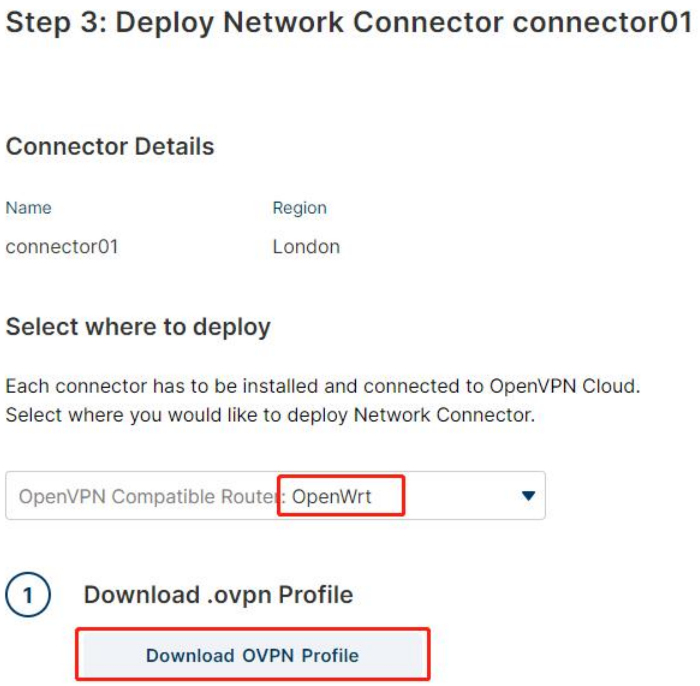
Connect multiple private networks to OpenVPN Cloud (site-to site connectivity). This wizard will assist you in adding a single network. Repeatedly use this wizard to connect all your networks. Read more.

□ 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 on 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 OpenVPN Cloud

3. Select the location as OpenWrt and download the OVPN file.



Step 3: Deploy Network Connector connector01

Connector Details

Name	Region
connector01	London

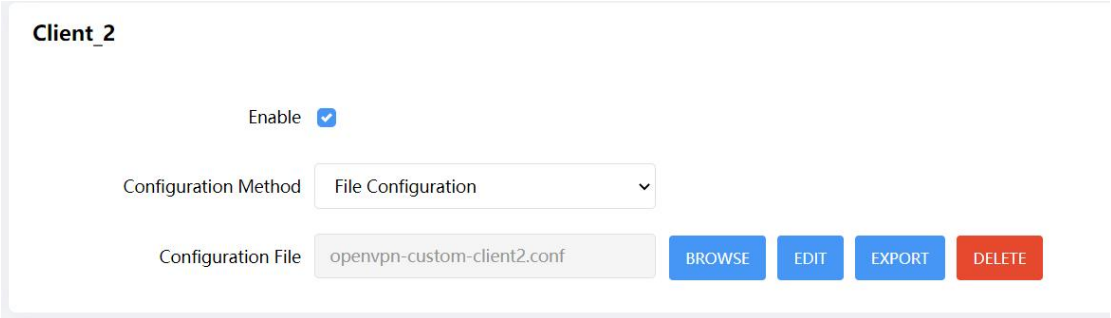
Select where to deploy

Each connector has to be installed and connected to OpenVPN Cloud.
Select where you would like to deploy Network Connector.

OpenVPN Compatible Router: OpenWrt

1 Download .ovpn Profile

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



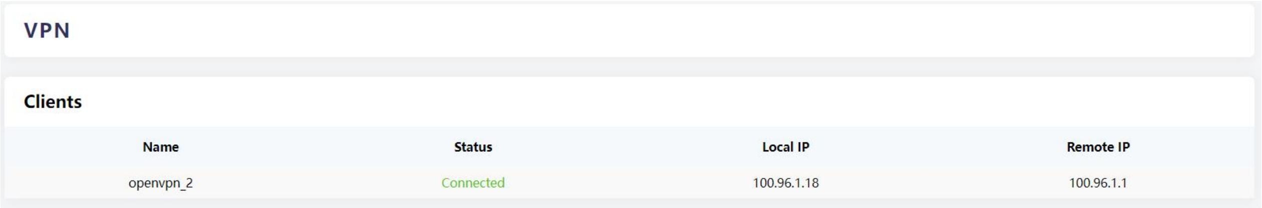
Client_2

Enable ☑

Configuration Method: File Configuration

Configuration File: openvpn-custom-client2.conf

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

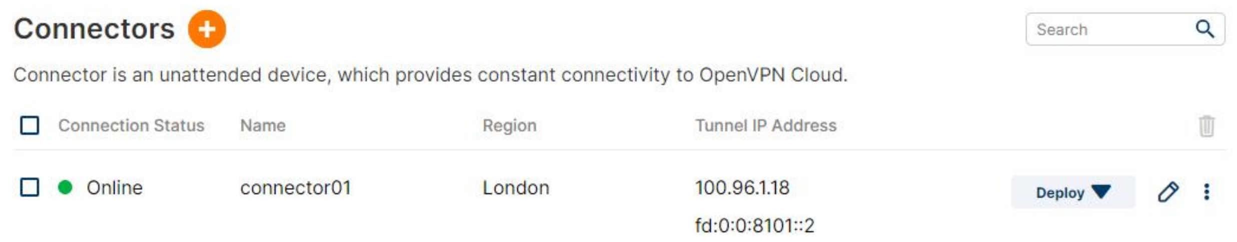


VPN

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 OpenVPN cloud.

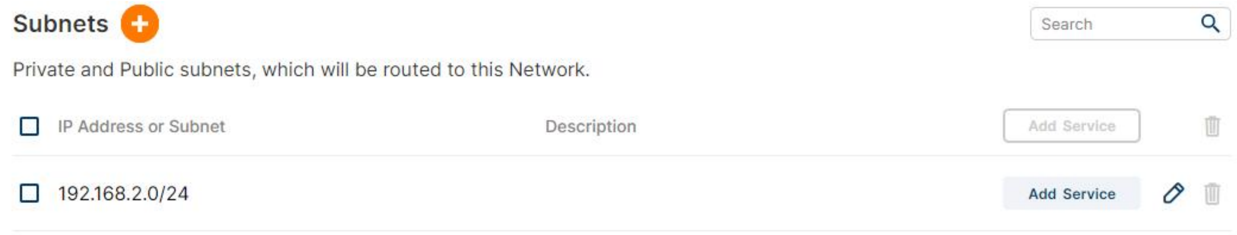


Connectors

Connector is an unattended device, which provides constant connectivity to OpenVPN Cloud.

□	Connection Status	Name	Region	Tunnel IP Address	
□	● Online	connector01	London	100.96.1.18 fd:0:0:8101::2	Deploy

6. You can remotely get access to this router via OpenVPN Connect software. If you need to access the terminal devices under device subnet, it’s necessary to assign the subnet on OpenVPN cloud.



Subnets

Private and Public subnets, which will be routed to this Network.

□	IP Address or Subnet	Description	
□	192.168.2.0/24		Add Service

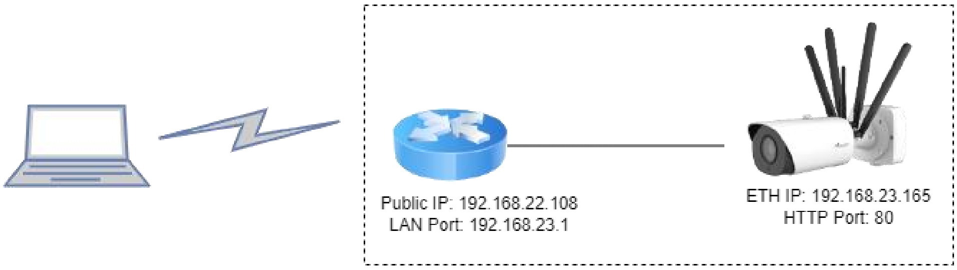
Related Topic

OpenVPN Client

6.5 Configure NAT Rule

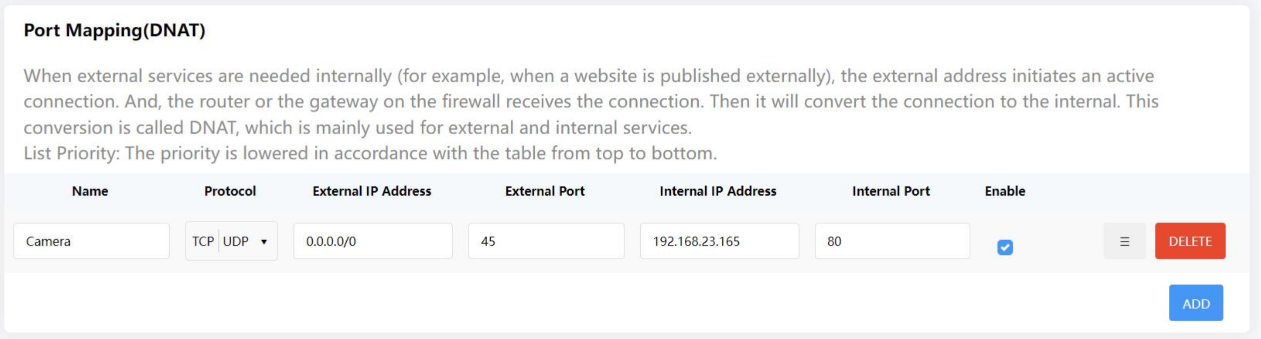
Example

UF31 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.



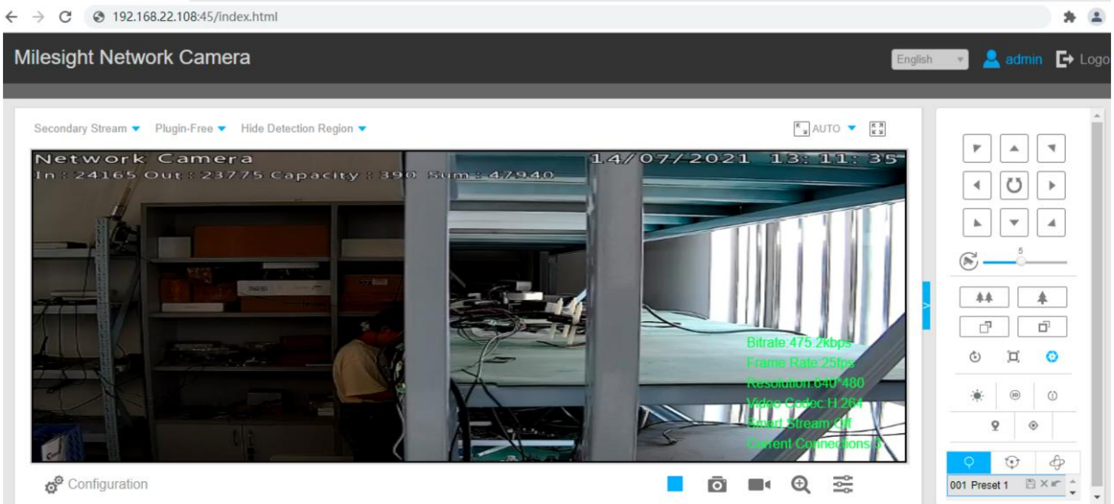
Port Mapping(DNAT)

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



192.168.22.108:45/index.html

Related Topic

Port Mapping

[END]